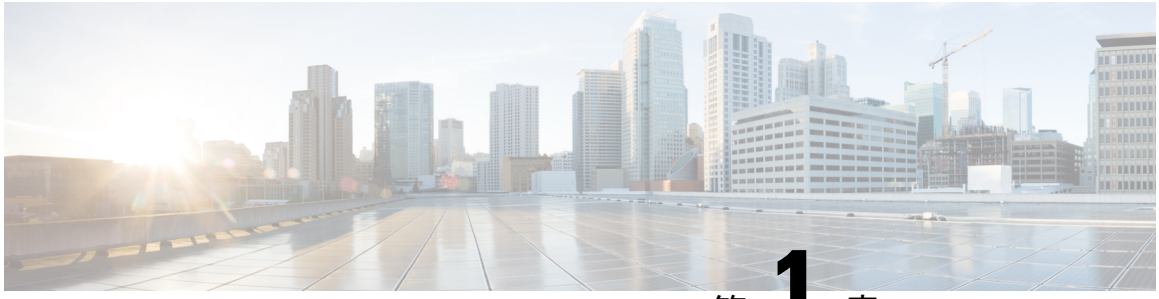
Firepower Management Center バージョン 6.4 コンフィギュレーション ガイド

初版：2019 年 4 月 30 日

最終更新：2019 年 9 月 26 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/



第 1 章

Firepower の概要

Cisco Firepowerは、専用プラットフォームで展開されるか、ソフトウェア ソリューションとして展開される、ネットワーク セキュリティおよびトラフィック管理製品の統合スイートです。このシステムは、組織のセキュリティ ポリシー（ネットワークを保護するためのガイドライン）に準拠する方法でネットワーク トラフィックを処理できるように設計されています。

標準的な展開では、ネットワーク セグメントにインストールされた複数のトラフィック検知管理対象デバイスが分析対象のトラフィックをモニタし、マネージャにレポートします。

- Firepower Management Center
- Firepower Device Manager
- Adaptive Security Device Manager（ASDM）

マネージャでは、集中管理コンソールのグラフィカル ユーザ インターフェイスを使用して管理、分析、およびレポート タスクを実行できます。

このガイドでは、*Firepower Management Center* 管理アプライアンスについて説明します。ASDMを介して管理される Firepower Device Manager または ASA with FirePOWER Services については、これらの管理手法のガイドを参照してください。

- *Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager*
- *ASA with FirePOWER Services Local Management Configuration Guide*

クイック スタート：基本設定

Firepower の機能セットには、基本設定および詳細設定をサポートできるだけの強力さと柔軟性があります。以降に説明する手順に従って、Firepower Management Center とその管理対象デバイスを迅速に設定し、トラフィックの制御と分析を開始することができます。

物理アプライアンスでの初期セットアップのインストールと実行

目的のアプライアンスに対応するドキュメンテーションを使用して、すべての物理アプライアンスで初期セットアップをインストールおよび実行します。

- **Firepower Management Center**
  - ハードウェア モデルについては、『*Cisco Firepower Management Center Getting Started Guide*』を参照してください。次のサイトから入手できます。

    http://www.cisco.com/go/firepower-mc-install

- **Firepower Threat Defense 管理対象デバイス**

  重要　　次のページの Firepower Device Manager ドキュメントは無視してください。

  - Cisco Firepower 1010 Getting Started Guide
  - Cisco Firepower 1100 Series Getting Started Guide
  - sco Firepower 2100 Series Getting Started Guide
  - Cisco Firepower 4100 Getting Started Guide
  - Cisco Firepower 9300 Getting Started Guide
  - Cisco Firepower Threat Defense for the ASA 5508-X and ASA 5516-X Using Firepower Management Center Quick Start Guide
  - Cisco Firepower Threat Defense for the ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, and ASA 5555-X Using Firepower Management Center Quick Start Guide
  - Cisco Firepower Threat Defense for the ISA 3000 Using Firepower Management Center Quick Start Guide

- **従来型管理対象デバイス**
  - Cisco ASA FirePOWER Module Quick Start Guide
  - Cisco Firepower 8000 Series Getting Started Guide
  - Cisco Firepower 7000 Series Getting Started Guide

仮想アプライアンスの展開

展開に仮想アプライアンスが含まれている場合は、以下の手順に従います。ドキュメンテーション ロードマップを使用して、http://www.cisco.com/c/en/us/td/docs/security/firepower/roadmap/firepower-roadmap.html にリストされているドキュメントを見つけます。

ステップ 1 Management Center とデバイスで使用する、サポートされている仮想プラットフォームを決定します（これらは同一とは限りません）。詳細については、『*Cisco Firepower Compatibility Guide*』を参照してください。

ステップ 2 ご使用の環境に応じたドキュメンテーションを使用して、仮想 Firepower Management Center を展開します。

- VMware で実行されている Firepower Management Center Virtual：*Cisco Firepower Management Center Virtual for VMware Deployment Quick Start Guide*
- AWS で実行されている Firepower Management Center Virtual：*Cisco Firepower Management Center Virtual for AWS Deployment Quick Start Guide*
- KVM で実行されている Firepower Management Center Virtual：*Cisco Firepower Management Center Virtual for KVM Deployment Quick Start Guide*

ステップ 3 ご使用のアプライアンスに応じたドキュメンテーションを使用して、仮想デバイスを展開します。

- VMware で実行されている NGIPSv：*Cisco Firepower NGIPSv Quick Start Guide for VMware*
- VMware で実行されている Firepower Threat Defense Virtual：*Cisco Firepower Threat Defense for the ASA 5508-X and ASA 5516-X Using Firepower Management Center Quick Start Guide*
- AWS で実行されている Firepower Threat Defense Virtual：*Cisco Firepower Threat Defense Virtual for AWS Deployment Quick Start Guide*
- KVM で実行されている Firepower Threat Defense Virtual：*Cisco Firepower Threat Defense Virtual for KVM Deployment Quick Start Guide*
- Azure で実行されている Firepower Threat Defense Virtual：*Cisco Firepower Threat Defense Virtual for Azure Deployment Quick Start Guide*

最初のログイン

始める前に

- アプライアンスを準備します。詳細については、物理アプライアンスでの初期セットアップのインストールと実行 （2 ページ）または仮想アプライアンスの展開 （3 ページ）を参照してください。

ステップ 1 ユーザ名として **admin**、パスワードとして **Admin123** を使用して、Firepower Management Center の Web インターフェイスにログインします。このアカウントのパスワードは、ご使用のアプライアンスの『クイック スタート ガイド』の説明に従って変更してください。

ステップ 2 このアカウントのタイム ゾーンを設定します。詳細については、デフォルト タイム ゾーンの設定 （49 ページ）を参照してください。

ステップ 3 ライセンスを追加します。詳細については、Firepower システムのライセンス （93 ページ）を参照してください。

ステップ 4 管理対象デバイスを登録します。詳細については、Firepower Management Center へのデバイスの追加 （293 ページ）を参照してください。

ステップ 5 管理対象デバイスを設定します。手順については、次を参照してください。

- IPS デバイスの展開と設定の概要 （663 ページ）：7000 シリーズまたは 8000 シリーズのデバイスで、パッシブ インターフェイスまたはインライン インターフェイスを設定する場合。
- Firepower Threat Defense のインターフェイスの概要 （785 ページ）：Firepower Threat Defense デバイスで、トランスペアレント モードまたはルーテッド モードを設定する場合。
- Firepower Threat Defense のインターフェイスの概要 （785 ページ）：Firepower Threat Defense デバイスで、インターフェイスを設定する場合。

次のタスク

- 基本ポリシーを設定することで、トラフィックの制御と分析を開始します。詳細については、基本ポリシーの設定 （4 ページ）を参照してください。

基本ポリシーの設定

ダッシュボード、コンテキスト エクスプローラ、およびイベント テーブルにデータを表示するには、基本ポリシーを設定し、展開する必要があります。

（注） これはポリシーや機能に関する完全な説明ではありません。その他の機能とより高度な設定については、このガイドの他のセクションを参照してください。

始める前に

- 最初のログイン （3 ページ）の説明に従って、Web インターフェイスにログインして、タイム ゾーンを設定し、ライセンスを追加し、デバイスを登録し、デバイスを設定します。

ステップ 1 基本的なアクセス コントロール ポリシーの作成 （1673 ページ）の説明に従って、アクセス コントロール ポリシーを設定します。

- ほとんどの場合、デフォルトのアクションとして、セキュリティと接続のバランスの取れた侵入ポリシーを設定することが提案されます。詳細については、アクセス コントロール ポリシーのデフォルト アクション （1668 ページ）およびシステム提供のネットワーク分析ポリシーと侵入ポリシー （2033 ページ）を参照してください。
- ほとんどの場合、組織のセキュリティとコンプライアンスのニーズを満たすために接続のロギングを有効にすることが提案されます。表示を整理したり、システムに負担をかけないために、ログに記録する接続を決定する際はネットワークのトラフィックを考慮してください。詳細については、接続ロギングについて （3001 ページ）を参照してください。

ステップ 2 正常性ポリシーの適用 （363 ページ）の説明に従って、システムが提供するデフォルトの正常性ポリシーを適用します。

ステップ 3 いくつかのシステム設定をカスタマイズします。

- サービス（SNMP や syslog など）の受信接続を許可する場合は、アクセス リストの設定 （1291 ページ）の説明に従ってアクセス リストのポートを変更します。
- データベース イベント数の制限の設定 （1264 ページ）の説明に従って、データベース イベント制限の編集について理解し、検討します。
- 表示言語を変更する場合は、 Web インターフェイスの言語の設定 （1304 ページ）の説明に従って言語設定を編集します。
- 組織がプロキシ サーバを使用してネットワーク アクセスを制限しており、初期設定時にプロキシを設定しなかった場合は、「Firepower Management Center 管理インターフェイスの設定 （1273 ページ）」の説明に従ってプロキシ設定を編集します。

ステップ 4 ネットワーク検出ポリシーの設定 （2649 ページ）の説明に従って、ネットワーク検出ポリシーをカスタマイズします。デフォルトでは、ネットワーク検出ポリシーは、ネットワークのすべてのトラフィックを分析します。ほとんどの場合、RFC 1918 のアドレスに検出を制限することが提案されます。

ステップ 5 次の他の一般的な設定のカスタマイズを検討します。

- メッセージ センターのポップアップを表示しない場合は、通知動作の設定 （418 ページ）の説明に従って通知を無効にします。
- システム変数のデフォルト値をカスタマイズする場合は、変数セット （538 ページ）の説明に従ってそれらの用途を理解します。
- 地理位置情報データベースを更新する場合は、地理位置情報データベース（GeoDB）の更新 （183 ページ）の説明に従って手動またはスケジュールに基づいて更新します。
- アプライアンスにアクセスする追加のローカル認証ユーザ アカウントを作成する場合は、社内ユーザ アカウントの追加 （57 ページ）を参照してください。

- LDAP または RADIUS 外部認証を使用してアプライアンスへのアクセスを許可する場合は、外部認証の設定 （62 ページ）を参照してください。

ステップ 6 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

次のタスク

- Firepower 機能 （7 ページ）およびこのガイドの他のセクションに記載されているその他の機能の設定について確認し、検討してください。

Firepower デバイス

一般的な展開では、複数のトラフィック処理デバイスが、アドミニストレーション、管理、分析、および報告タスクの実行に使用される 1 つの Firepower Management Center に報告します。

従来のデバイス

従来のデバイスは、次世代 IPS（NGIPS）ソフトウェアを実行します。具体的には以下のとおりです。

- Firepower 7000 シリーズおよび Firepower 8000 シリーズの物理デバイス。
- VMware でホストされている NGIPSv。
- ASA with FirePOWER Services は、一部の ASA 5500-X シリーズ デバイス（ISA 3000 も含む）で使用できます。ASA は最も重要なシステム ポリシーを提供し、検出およびアクセス コントロールのためにトラフィックを ASA FirePOWER モジュールに渡します。

  ASA FirePOWER デバイスで ASA ベースの機能を設定するには、ASA CLI または ASDM を使用する必要があります。これには、デバイスのハイ アベイラビリティ、スイッチング、ルーティング、VPN、NAT などが含まれます。FMC を使用して ASA FirePOWER インターフェイスを設定することはできません。また、ASA FirePOWER が SPAN ポート モードで展開されている場合、FMC GUI は ASA インターフェイスを表示しません。また、FMC を使用して ASA FirePOWER プロセスのシャットダウン、再起動、またはその他の管理を行うことはできません。

Firepower Threat Defense デバイス

Firepower Threat Defense（FTD）デバイスは、NGIPS 機能も備えた次世代ファイアウォール（NGFW）です。NGFW およびプラットフォーム機能には、サイト間およびリモート アクセス VPN、堅牢なルーティング、NAT、クラスタリング、およびアプリケーション インスペクションとアクセス制御におけるその他の最適化が含まれています。

FTD は、幅広い物理プラットフォームおよび仮想プラットフォームで使用できます。

互換

特定のデバイス モデル、仮想ホスティング環境、オペレーティング システムなどと互換性のあるソフトウェアを含むマネージャとデバイスの互換性の詳細については、『Cisco Firepower Release Notes』および『Cisco Firepower Compatibility Guide』を参照してください。

Firepower 機能

次の表には、一般的に使用されるいくつかの Firepower 機能が一覧表示されています。

アプライアンスおよびシステム管理の機能

未知のドキュメントを検索するには、http://www.cisco.com/c/en/us/td/docs/security/firepower/roadmap/firepower-roadmap.html を参照してください。

目的	設定	参照先
Firepower アプライアンスへのログイン用のユーザ アカウントを管理する	Firepower 認証	ユーザ アカウントについて（51 ページ）
システム ハードウェアとシステム ソフトウェアの状況をモニタする	ヘルス モニタリング ポリシー	ヘルス モニタリングについて （349 ページ）
アプライアンスのデータをバックアップする	バックアップと復元	バックアップと復元 （199 ページ）
新しい Firepower バージョンにアップグレードする	システムの更新プログラム	Cisco Firepower Management Center Upgrade Guide Firepower Release Notes
物理アプライアンスを基準に合わせる	工場出荷時の初期状態に復元（再イメージ化）する	Cisco Firepower Management Center Upgrade Guide、新規インストールの実行に関する説明へのリンクの一覧。
VDB を更新する、侵入ルールを更新する、またはアプライアンスの GeoDB を更新する	脆弱性データベース（VDB）の更新、侵入ルールの更新、地理位置情報データベース（GeoDB）の更新	システム ソフトウェアの更新 （179 ページ）
ライセンス制御機能を利用するためにライセンスを適用する	従来のライセンスまたはスマート ライセンス	Firepower ライセンスについて （93 ページ）

目的	設定	参照先
アプライアンスの動作の継続性を確保する	管理対象デバイスの高可用性または Firepower Management Center の高可用性（あるいはその両方）	7000 および 8000 シリーズ デバイスのハイ アベイラビリティについて （679 ページ） ハイ アベイラビリティ Firepower Threat Defense について （873 ページ） Firepower Management Center のハイ アベイラビリティについて （263 ページ）
複数の 8000 シリーズのデバイスの処理リソースを結合する	デバイス スタッキング	デバイス スタックについて （699 ページ）
複数のインターフェイス間のトラフィックをルーティングするようにデバイスを設定する	ルーティング	仮想ルータ （1581 ページ） Firepower Threat Defense のルーティングの概要 （953 ページ）
複数のネットワーク間のパケットスイッチングを設定する	デバイス スイッチング	仮想スイッチ（1569ページ） の□ブリッジ グループ インターフェイスの設定 （813 ページ）
インターネット接続のプライベート アドレスをパブリック アドレスに変換する	ネットワーク アドレス変換（NAT）	NAT ポリシーの設定 （1427 ページ） Firepower Threat Defense 用のネットワーク アドレス変換（NAT） （1449 ページ）
管理対象の Firepower Threat Defense デバイスまたは 7000/8000 シリーズ デバイス間のセキュアなトンネルを確立する	サイト間バーチャル プライベート ネットワーク（VPN）	Firepower Threat Defense の VPN の概要 （1053 ページ）
リモート ユーザと管理対象 Firepower Threat Defense デバイス間のセキュアなトンネルを確立する	リモート アクセス VPN	Firepower Threat Defense の VPN の概要 （1053 ページ）
管理対象デバイス、設定、およびイベントへのユーザ アクセスをセグメント化する	ドメインを使用したマルチテナンシー	ドメインを使用したマルチテナンシーの概要 （433 ページ）

目的	設定	参照先
REST API クライアントを使用してアプライアンスの設定を表示および管理する	REST API および REST API エクスプローラ	REST API 設定 （1324 ページ） *Firepower REST API Quick Start Guide*
問題のトラブルシューティング	該当なし	システムのトラブルシューティング （409 ページ）

プラットフォーム別のハイ アベイラビリティとスケーラビリティの機能

（フェールオーバーとも呼ばれる）ハイ アベイラビリティ構成により、操作の継続性が確保されます。クラスタ化構成とスタック構成では、複数のデバイスが単一の論理デバイスとしてグループ化され、スループットと冗長性が向上します。

プラットフォーム	高可用性	クラスタリング	スタック構成
Firepower Management Center	あり MC750 を除く	—	—
Firepower Management Center Virtual	—	—	—
Firepower Threat Defense： • Firepower 1000 シリーズ • Firepower 2100 シリーズ • ASA 5500-X シリーズ • ISA 3000	あり	—	—
Firepower Threat Defense： • Firepower 4100/9300 シャーシ	あり	あり	—
Firepower Threat Defense Virtual： • VMware • KVM	あり	—	—
Firepower Threat Defense Virtual（パブリッククラウド）： • AWS • Azure	—	—	—

プラットフォーム	高可用性	クラスタリング	スタック構成
• Firepower 7010、7020、7030、7050 • Firepower 7110、7115、7120、7125 • Firepower 8120、8130 • AMP 7150、8050、8150	あり	—	—
• Firepower 8140 • Firepower 8250、8260、8270、8290 • Firepower 8350、8360、8370、8390 • AMP 8350	あり	—	あり
ASA FirePOWER	—	—	—
NGIPSv	—	—	—

関連トピック

7000 および 8000 シリーズ デバイスのハイ アベイラビリティについて （679 ページ）
ハイ アベイラビリティ Firepower Threat Defense について （873 ページ）
Firepower Management Center のハイ アベイラビリティについて （263 ページ）

潜在的な脅威を検出、防御、および処理するための機能

未知のドキュメントを検索するには、http://www.cisco.com/c/en/us/td/docs/security/firepower/roadmap/firepower-roadmap.html を参照してください。

目的	設定	参照先
ネットワーク トラフィックのインスペクション、記録、およびアクションを実行する	アクセス コントロール ポリシー、他のいくつかのポリシーの親	アクセス制御の概要 （1665 ページ）
IP アドレス、URL、またはドメイン名との間でブラックリスト接続する	アクセス コントロール ポリシー内のセキュリティ インテリジェンス	セキュリティ インテリジェンスについて （1741 ページ）
ネットワークのユーザがアクセスできる Web サイトを制御する	ポリシー ルール内の URL フィルタリング	URL Filtering （1717 ページ）
ネットワーク上の悪意のあるトラフィックと侵入をモニタする	侵入ポリシー	侵入ポリシーの基本 （2063 ページ）

目的	設定	参照先
インスペクションを実行せずに、暗号化されたトラフィックをブロックする 暗号化または複合されたトラフィックのインスペクション	SSL ポリシー	SSL ポリシーの概要 （1837 ページ）
ディープ インスペクションをカプセル化トラフィックに合わせて調整し、高速パス処理でのパフォーマンスを向上させる	プレフィルタ ポリシー	プレフィルタリングについて （1767 ページ）
アクセス コントロールによって許可または信頼されたネットワーク トラフィックのレート制限	サービス品質（QoS）ポリシー	QoS ポリシーについて （864 ページ）
ネットワーク上のファイル（マルウェアを含む）を許可またはブロックする	ファイル/マルウェア ポリシー	ファイル ポリシーと高度なマルウェア防御 （1911 ページ）
脅威インテリジェンス ソースからデータを運用可能にします。	Cisco Threat Intelligence Director（TID）	Cisco Threat Intelligence Director（TID） の概要 （1967 ページ）
ユーザの認知およびユーザ制御を実行するためにパッシブまたはアクティブなユーザ認証を設定する	ユーザ認識、ユーザ アイデンティティ、アイデンティティ ポリシー	ユーザ アイデンティティ ソースについて （2482 ページ） アイデンティティ ポリシーについて （2637 ページ）
ユーザ認識を実行するために、ネットワークのトラフィックからホスト、アプリケーション、およびユーザ データを収集する	ネットワーク検出ポリシー	概要：ネットワーク検出ポリシー （2647 ページ）
外部ツールを使用してネットワーク トラフィックと潜在的な脅威に関するデータを収集して分析する	外部ツールとの統合	外部ツールを使用したイベントの分析 （2881 ページ）
アプリケーション検出およびコントロールを実行する	アプリケーション ディテクタ	概要：アプリケーション検出 （2547 ページ）
問題のトラブルシューティング	該当なし	システムのトラブルシューティング （409 ページ）

外部ツールとの統合

未知のドキュメントを検索するには、http://www.cisco.com/c/en/us/td/docs/security/firepower/roadmap/firepower-roadmap.html を参照してください。

目的	設定	参照先
ネットワークの条件が、関連付けられたポリシーに違反した場合、自動的に修復を起動する	修復	修復の概要 （2755 ページ） *Firepower System Remediation API Guide*
Firepower Management Center からカスタム開発されたクライアント アプリケーションにイベント データをストリームする	eStreamer 統合	eStreamer サーバ ストリーミング （2906 ページ） *Firepower System eStreamer Integration Guide*
サードパーティ クライアントを使用して Firepower Management Center のデータベース テーブルを照会する	外部データベース アクセス	外部データベース アクセスの設定 （1262 ページ） *Firepower System Database Access Guide*
サードパーティ ソースからデータをインポートすることによって検出データを増やす	ホスト入力	ホスト入力データ （2507ページ） *Firepower System Host Input API Guide*
外部イベント データ ストレージ ツールその他のデータ リソースを使用してイベントを調査します。	外部イベント分析ツールとの統合	外部ツールを使用したイベントの分析 （2881 ページ）
問題のトラブルシューティング	該当なし	システムのトラブルシューティング （409 ページ）

Firepower Management Center のドメインの切り替え

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン数	アクセス
該当なし	任意	FMC	任意	任意

マルチドメイン導入環境では、ユーザ ロール権限によって、ユーザがアクセスできるドメインと、そのドメイン内でのユーザの権限が決まります。単一のユーザ アカウントを複数のドメインに関連付けて、各ドメインでそのユーザに異なる権限を割り当てることができます。たとえば、あるユーザにグローバル ドメインでは読み取り専用権限を割り当て、子孫ドメインでは管理者権限を割り当てることができます。

複数のドメインに関連付けられているユーザは、同じ Web インターフェイス セッション内でドメインを切り替えることができます。

ツールバーのユーザ名の下に、利用可能なドメインのツリーが表示されます。ツリーの表示は次のようになります。

- 先祖ドメインは表示されますが、使用しているユーザアカウントに割り当てられた権限に応じて、先祖ドメインへのアクセスが無効である場合があります。
- 兄弟ドメインや子孫ドメインを含め、使用しているユーザアカウントでアクセスできない他のドメインは非表示になります。

ドメインを切り替えると、以下の項目が表示されます。

- そのドメインのみに関連するデータ。
- そのドメインで割り当てられたユーザ ロールに応じて定められたメニュー オプション。

アクセスするドメインは、ユーザ名の下にあるドロップダウン リストから選択します。

コンテキスト メニュー

Firepower システム Web インターフェイスの特定のページでは、右クリック（最も一般的）および左クリックでコンテキスト メニューを表示できます。コンテキスト メニューは、Firepower システム内の他の機能にアクセスするためのショートカットとして使用できます。コンテキスト メニューの内容はどこでこのメニューにアクセスするか（どのページかだけでなく特定のデータにアクセスしているか）によって異なります。

次に例を示します。

- IP アドレスのホットスポットでは、そのアドレスに関連付けられているホストに関する情報（使用可能な whois とホスト プロファイル情報を含む）が表示されます。
- SHA-256 ハッシュ値のホットスポットでは、ファイルの SHA-256 ハッシュ値をクリーン リストまたはカスタム検出リストに追加したり、コピーするためにハッシュ値全体を表示したりできます。

Firepower システム コンテキスト メニューをサポートしていないページや場所では、ブラウザの通常のコンテキスト メニューが表示されます。

ポリシー エディタ

多くのポリシーエディタには、各ルールのホットスポットが含まれています。新しいルールとカテゴリの挿入、ルールの切り取り、コピー、貼り付け、ルール状態の設定、ルールの編集などを行うことができます。

侵入ルール エディタ

侵入ルールエディタには、各侵入ルールのホットスポットが含まれています。ルールの編集、ルール状態の設定、しきい値および抑止オプションの設定、ルールのドキュメンテーションの表示などを行うことができます。必要に応じて、コンテキストメニューで、**ルールのドキュメント**をクリックするより具体的なルールの詳細を表示するドキュメントのポップアップ ウィンドウで、**ルールのドキュメント**をクリックすることができます。

イベント ビューア

イベントページ（[分析（Analysis）]ページにあるドリルダウンページとテーブル ビュー）には、各イベント、IP アドレス、URL、DNS クエリ、特定のファイルの SHA-256 ハッシュ値のホットスポットが含まれています。ほとんどのイベントタイプでは、表示中に以下の操作を行うことができます。

- Context Explorer で関連情報を表示する。
- 新しいウィンドウでイベント情報をドリルダウンする。
- イベント フィールドに含まれているテキスト（ファイルの SHA-256 ハッシュ値、脆弱性の説明、URL など）が長すぎてイベント ビューですべて表示できない場合、テキスト全体を表示する。
- コンテキスト クロス起動機能を使用し、Firepower の外部のソースからのエレメントに関する情報が表示されている Web ブラウザ ウィンドウを開きます。詳細については、Webベースのリソースを使用したイベントの調査（2890ページ）を参照してください。
- （組織で Cisco Security Packet Analyzer が展開されている場合）イベントに関連するパケットを調べます。詳細については、を使用したイベント調査 Cisco Security Packet Analyzer （2882 ページ）を参照してください。

接続イベントの表示中は、デフォルトのセキュリティインテリジェンスのホワイトリストとブラックリストに以下の項目を追加できます。

- IP アドレスのホットスポットの場合、IP アドレス。
- URL のホットスポットの場合、URL またはドメイン名。
- DNS クエリのホットスポットの場合、DNS クエリ。

キャプチャ ファイル、ファイル イベント、マルウェア イベントの表示中は、以下の操作を行うことができます。

- クリーン リストまたはカスタム検出リストのファイルを追加または削除する。
- ファイルのコピーをダウンロードする。
- アーカイブ ファイル内のネストされたファイルを表示する。
- ネストされたファイルの親アーカイブ ファイルをダウンロードする。
- ファイルの構成を表示する。

- ローカル マルウェア分析およびダイナミック分析対象のファイルを送信する。

侵入イベントの表示中は、侵入ルール エディタまたは侵入ポリシーで実行できるようなタスクを行うことができます。

- トリガー ルールを編集する。
- ルールの無効化を含め、ルールの状態を設定する。
- しきい値および抑止オプションを設定する。
- ルールのドキュメンテーションを表示する。必要に応じて、コンテキストメニューの [Rule documentation] をクリックした後、ドキュメント ポップアップ ウィンドウの [Rule Documentation] をクリックするとより具体的なルールの詳細情報を表示できます。

侵入イベントのパケット ビュー

侵入イベントのパケット ビューには、IP アドレスのホットスポットが含まれています。パケット ビューでは、左クリックによるコンテキスト メニューを使用します。

ダッシュボード

多くのダッシュボード ウィジェットには、関連する情報を Context Explorer で表示するためのホットスポットが含まれています。ダッシュボード ウィジェットには、IP アドレスと SHA-256 ハッシュ値のホットスポットが含まれる場合もあります。

Context Explorer

Context Explorer には、図、表、グラフのホットスポットが含まれています。Context Explorer よりも詳細なグラフまたはリストのデータを調べたい場合は、関連するデータのテーブル ビューにドリルダウンすることができます。また、関連するホスト、ユーザ、アプリケーション、ファイル、および侵入ルールの情報を表示できます。

Context Explorer でも左クリックのコンテキスト メニューを使用します。これには、Context Explorer に特有のフィルタリングおよび他のオプションも含まれています。

関連トピック

セキュリティ インテリジェンスのリストとフィード （557 ページ）

シスコとのデータの共有

次の機能を使用して、シスコとデータを共有することを選択できます。

- Cisco Success Network

  Cisco Success Network （162 ページ）を参照してください

- Web 分析

  （オプション）Web 分析トラッキングのオプトアウト （1326 ページ）を参照してください

Firepowerのオンラインヘルプ、ハウツー、およびドキュメント

オンライン ヘルプには、Web インターフェイスからアクセスできます。

- 各ページで状況依存ヘルプのリンクをクリックする。
- **[ヘルプ（Help）]** > **[オンライン（Online）]** を選択する。

ハウツーは、Firepower Management Center 上でタスク間を移動するためのウォークスルーを提供するウィジェットです。ウォークスルーでは、タスクを実行するために移動する必要があるかもしれない各種 UI 画面かどうかを問わず、各ステップを順次体験することでタスクを完遂するために必要なステップを実行します。デフォルトで [ハウツー（How To）] ウィジェットは有効になっています。このウィジェットを無効にするには、自分のユーザ名の下にあるドロップダウン リストから [ユーザ設定（User Preferences）] を選択し、[ハウツーの設定（How-To Settings）] タブの [ハウツーを有効にする（Enable How-Tos）] をオフにします。

（注） 通常、ウォークスルーはすべての UI ページで利用でき、ユーザ ロールは区別されていません。ただし、ユーザの権限によっては Firepower Management Center のインターフェイスに表示されないメニュー項目もあります。そのため、そのようなページではウォークスルーは実行されません。

Firepower Management Center では次のウォークスルーを使用できます。

- [Cisco スマート アカウントへの FMC の登録（Register FMC with Cisco Smart Account）]：このウォークスルーでは、Cisco スマート アカウントに Firepower Management Center を登録する手順について説明します。
- [デバイスのセットアップと FMC への追加（Set up a Device and add it to FMC）]：このウォークスルーでは、デバイスをセットアップし、そのデバイスを Firepower Management Center に追加する手順について説明します。
- [日付と時刻の設定（Configure Date and Time）]：このウォークスルーでは、プラットフォーム設定ポリシーを使用して Firepower Threat Defense デバイスの日付と時刻を設定する手順について説明します。
- [インターフェイスの設定（Configure Interface Settings）]：このウォークスルーでは、Firepower Threat Defense デバイス上のインターフェイスを設定する手順について説明します。
- [アクセス コントロール ポリシーの作成（Create an Access Control Policy）]：アクセス コントロール ポリシーは上から下へと評価される、順序付けられた一連のルールから構成されています。このウォークスルーでは、アクセス コントロール ポリシーを作成する手順について説明します。

- [アクセス コントロール ルールの追加（Add an Access Control Rule）] - 機能のウォークスルー：このウォークスルーでは、アクセス コントロール ルールのコンポーネントと、Firepower Management Center でのそれらの使用方法について説明します。
- [ルーティングの設定（Configure Routing Settings）]：Firepower Threat Defense ではさまざまなルーティング プロトコルがサポートされています。スタティック ルートは、特定の宛先ネットワークのトラフィックの送信先を定義します。このウォークスルーでは、デバイスのスタティック ルーティングを設定する手順について説明します。
- [NAT ポリシーの作成（Create a NAT Policy）] - 機能のウォークスルー：このウォークスルーでは、NAT ポリシーを作成する手順とともに、NAT ルールのさまざまな機能について説明します。

ドキュメントのロードマップを使用して Firepower システムに関連する他のドキュメントについてはhttp://www.cisco.com/c/en/us/td/docs/security/firepower/roadmap/firepower-roadmap.html を参照してください。

FMC 展開に関するトップレベルのドキュメントのリスト ページ

Firepower Management Center 展開のバージョン 6.0+ を設定するときは、次のドキュメントが役立つ可能性があります。

（注） リンクされたドキュメントの一部は、Firepower Management Center 展開には適用できません。たとえば、Firepower Threat Defense ページの一部のリンクは Firepower Device Manager によって管理される展開に固有の内容で、ハードウェア ページの一部のリンクは FirePOWER とは無関係です。混乱を避けるために、ドキュメントのタイトルには十分に注意してください。また、一部のドキュメントは複数の製品を対象としているため、複数の製品のページに記載されていることがあります。

Firepower Management Center

- Firepower Management Center ハードウェア アプライアンス：

  http://www.cisco.com/c/en/us/support/security/defense-center/tsd-products-support-series-home.html

- Firepower Management Center Virtual アプライアンス：
  - http://www.cisco.com/c/en/us/support/security/defense-center-virtual-appliance/tsd-products-support-series-home.html
  - http://www.cisco.com/c/en/us/support/security/defense-center/tsd-products-support-series-home.html

NGFW（次世代ファイアウォール）デバイスとも呼ばれる Firepower Threat Defense

- Firepower Threat Defense ソフトウェア：

http://www.cisco.com/c/en/us/support/security/firepower-ngfw/tsd-products-support-series-home.html

- Firepower Threat Defense Virtual：

  http://www.cisco.com/c/en/us/support/security/firepower-ngfw-virtual/tsd-products-support-series-home.html

- FirePOWER 1000 シリーズ：

  https://www.cisco.com/c/en/us/support/security/firepower-1000-series/tsd-products-support-series-home.html

- FirePOWER 2100 シリーズ：

  https://www.cisco.com/c/en/us/support/security/firepower-2100-series/tsd-products-support-series-home.html

- Firepower 4100 シリーズ：

  https://www.cisco.com/c/en/us/support/security/firepower-4100-series/tsd-products-support-series-home.html

- FirePOWER 9300：

  https://www.cisco.com/c/en/us/support/security/firepower-9000-series/tsd-products-support-series-home.html

- ASA 5500-X シリーズ：
  - https://www.cisco.com/c/en/us/support/security/asa-firepower-services/tsd-products-support-series-home.html
  - https://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/tsd-products-support-series-home.html

- ISA 3000：

  https://www.cisco.com/c/en/us/support/security/industrial-security-appliance-isa/tsd-products-support-series-home.html

NGIPS（次世代侵入防御システム）デバイスとも呼ばれる従来型デバイス

- ASA with FirePOWER Services：
  - ASA 5500-X with FirePOWER Services：
    - https://www.cisco.com/c/en/us/support/security/asa-firepower-services/tsd-products-support-series-home.html
    - https://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/tsd-products-support-series-home.html
  - ISA 3000 with FirePOWER Services：

    https://www.cisco.com/c/en/us/support/security/industrial-security-appliance-isa/tsd-products-support-series-home.html

- FirePOWER 8000 シリーズ：

  https://www.cisco.com/c/en/us/support/security/firepower-8000-series-appliances/tsd-products-support-series-home.html

- FirePOWER 7000 シリーズ：

  https://www.cisco.com/c/en/us/support/security/firepower-7000-series-appliances/tsd-products-support-series-home.html

- AMP for Networks：

  https://www.cisco.com/c/en/us/support/security/amp-appliances/tsd-products-support-series-home.html

- NGIPSv（バーチャル デバイス）：

  https://www.cisco.com/c/en/us/support/security/ngips-virtual-appliance/tsd-products-support-series-home.html

ドキュメンテーションのライセンス ステートメント

項の先頭に記載されているライセンス ステートメントは、項で説明される機能を有効にするために Firepower システムの管理対象デバイスに割り当てる必要があるのは従来のライセンスかスマート ライセンスかを示します。

ライセンス付きの機能の多くは追加的であるため、ライセンス ステートメントでは、各機能で最も必要なライセンスについてのみ記載しています。

ライセンス文の「または」という語は、その項に記載されている機能を有効にするには特定のライセンスを管理対象デバイスに指定する必要があることを示していますが、追加のライセンスで機能を追加できます。たとえば、ファイル ポリシー内では、一部のファイル ルール アクションではデバイスに保護ライセンスを指定する必要がありますが、他方ではマルウェア ライセンスを指定する必要があります。

ライセンスの詳細については、Firepower ライセンスについて （93 ページ）を参照してください。

関連トピック

Firepower ライセンスについて （93 ページ）

ドキュメント内のサポート対象デバイスに関する記述

章または項目の先頭に記載されているサポート対象デバイスに関する記述は、ある機能が特定のデバイス シリーズ、ファミリ、またはモデルでのみサポートされていることを示しています。たとえば、多くの機能は Firepower Threat Defense デバイスのみでサポートされています。

このリリースでサポートされているプラットフォームの詳細については、リリース ノートを参照してください。

ドキュメント内のアクセス ステートメント

このドキュメントの各手順の先頭に記載されているアクセス ステートメントは、手順の実行に必要な事前定義のユーザ ロールを示しています。記載されている任意のロールを使用して手順を実行することができます。

カスタム ロールを持っているユーザは、事前定義されたロールとは異なる権限セットを持つことができます。事前定義されたロールを使用して手順のアクセス要件が示されている場合は、同様の権限を持つカスタム ロールにもアクセス権があります。カスタム ロールを持っているユーザは、設定ページにアクセスするために使用するメニュー パスが若干異なる場合があります。たとえば、侵入ポリシー権限のみが付与されているカスタム ロールを持つユーザは、アクセス コントロール ポリシーを使用する標準パスではなく侵入ポリシーを経由してネットワーク分析ポリシーにアクセスします。

ユーザ ロールの詳細については、ユーザ ロール （54 ページ）およびWeb インターフェイス用のユーザ ロールのカスタマイズ （81 ページ）を参照してください。

Firepower システムの IP アドレス表記法

IPv4 Classless Inter-Domain Routing（CIDR）の表記、および IPv6 と同様のプレフィックス長の表記を使用して、Firepower システムのさまざまな場所でアドレス ブロックを定義することができます。

CIDR またはプレフィックス長の表記を使用して IP アドレスのブロックを指定する場合、Firepower システムは、マスクまたはプレフィックス長で指定されたネットワーク IP アドレスの部分**のみ**を使用します。たとえば、10.1.2.3/8 と入力した場合、Firepower システムでは 10.0.0.0/8 が使用されます。

つまり、Cisco では CIDR またはプレフィックス長の表記を使用する場合に、ビット境界上でネットワーク IP アドレスを使用する標準の方法を推奨していますが、Firepower システムではこれは必要ありません。

関連リソース

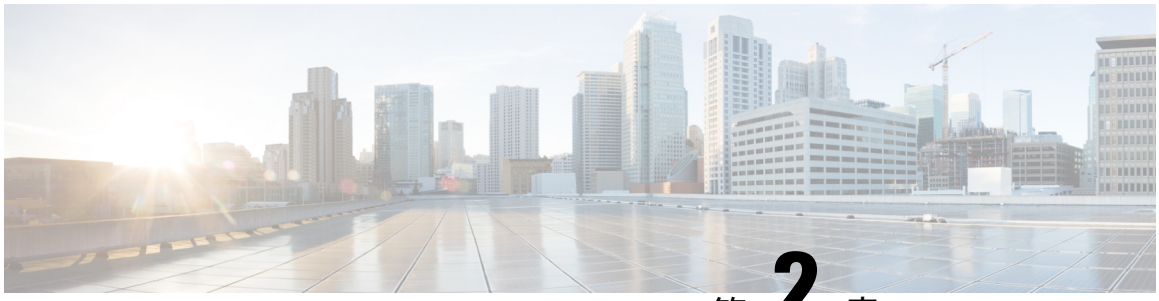
ファイアウォール コミュニティは、参考資料の包括的リポジトリで、シスコの広範にわたるドキュメンテーションを補完します。これには、シスコのハードウェアの3Dモデル、ハードウェア構成セレクタ、製品販促アイテム、設定例、トラブルシューティングに関するテクニカル ノート、トレーニング ビデオ、ラボおよび Cisco Live セッション、ソーシャル メディア チャネル、Cisco ブログおよび技術文書チームによって公開されたすべてのドキュメンテーションへのリンクが含まれます。

管理人等、コミュニティ サイトや動画共有サイトに情報を掲載する個人が、シスコの社員であることがあります。それらのサイトおよび対応するコメントで表明される意見は、投稿者本人の個人的意見であり、シスコの意見ではありません。掲載内容は、情報の提供のみを目的としており、シスコや他の関係者による推奨または異議を目的としたものではありません。

（注） ファイアウォール コミュニティ の動画、テクニカル ノート、および参考資料の中には、古いバージョンの Firepower Management Center に言及しているものがあります。ご使用のバージョンの Firepower Management Center と動画やテクニカル ノートで参照されているバージョンとではユーザ インターフェイスに違いがあるために、手順も異なる場合があります。

第 I 部

ユーザ アカウント



第 2 章

Firepower システムへのログイン

以下のトピックでは、Firepower システムにログインする方法を示します。

Firepower システム ユーザ アカウント

ユーザ名とパスワードを入力して、FMC または管理対象デバイスの Web インターフェイス、シェル、または CLI へのローカル アクセスを取得する必要があります。管理対象デバイスでは、Config レベルのアクセス権を持つ CLI ユーザは、`expert` コマンドを使用して Linux シェルにアクセスできます。FMC では、すべての CLI ユーザが `expert` コマンドを使用できます。FTD と FMC は、外部 LDAP や RADIUS サーバでユーザ クレデンシャルを保存する外部認証を使用するように設定できる場合があります。その場合、外部ユーザに対し、CLI またはシェルへのアクセスを禁止または許可することができます。

FMC CLI は、すべてのコマンドにアクセスできる単一の **admin** ユーザを提供します。FMC Web インターフェイスのユーザがアクセスできる機能は、管理者がユーザ アカウントに付与する権限によって制御されます。管理対象デバイスでは、ユーザがアクセスできる機能（CLI と Web インターフェイス用の）は、管理者がユーザ アカウントに付与する権限によって制御されます。

（注） システムはユーザ アカウントに基づいてユーザ アクティビティを監査するため、ユーザが正しいアカウントでシステムにログインしていることが保証されます。

注意 すべての FMC CLI ユーザ、および管理対象デバイスで Config レベルの CLI アクセス権を持つユーザは、Linux シェルの root 権限を取得できます。このため、セキュリティ上のリスクが生じる可能性があります。システム セキュリティ上の理由から、次の点を強くお勧めします。

- 外部認証を確立した場合は、CLI またはシェルへのアクセス権があるユーザのリストを適切に制限してください。
- 管理対象デバイスで CLI アクセス権限を付与する場合は、Config レベルの CLI アクセス権を付与された内部ユーザのリストを制限します。
- Linux シェルユーザは確立しないでください。事前定義された **admin** ユーザおよび CLI 内で **admin** ユーザが作成したユーザのみを使用します。

注意 Cisco TAC または Firepower ユーザ マニュアルの明示的な手順による指示がない限り、Linux シェルを使用しないことを強くお勧めします。

アプライアンスが異なれば、サポートするユーザアカウントのタイプは異なり、搭載される機能もさまざまです。

Firepower Management Centerについて

Firepower Management Center では、次のユーザ アカウント タイプをサポートします。

- Web インターフェイス アクセス用に事前定義された **admin** アカウント。このアカウントは管理者ロールを保有し、Web インターフェイスから管理できます。
- カスタム ユーザ アカウント。このアカウントは Web インターフェイスへのアクセスが可能で、**admin** ユーザおよび管理者権限を持つユーザが作成および管理できます。
- CLI またはシェルへのアクセス権に事前に定義されている **admin** アカウント。このアカウントはルート権限を取得できます。デフォルトでは、デバイスにログインすると、この **admin** アカウントはシェルにダイレクトアクセスできるようになります。ただし、Firepower Management Center CLI が有効になっている場合、このアカウントでログインするユーザは `expert` コマンドを使用してシェルにアクセスする必要があります。

注意 システム セキュリティ上の理由から、アプライアンスでは追加の Linux シェル ユーザを確立しないことを強く推奨します。

7000 & 8000 シリーズ デバイス

7000 & 8000 シリーズ デバイスでは、次のユーザ アカウント タイプをサポートします。

- 事前定義された **admin** アカウント。このアカウントはデバイスにアクセスするすべての形態で使用できます。
- カスタム ユーザ アカウント。このアカウントは、**admin** ユーザおよび管理者ロールのユーザが作成、管理できます。

7000 & 8000 シリーズは、ユーザの外部認証をサポートしています。

NGIPSv デバイス

NGIPSv デバイスでは、次のユーザ アカウント タイプをサポートします。

- 事前定義された **admin** アカウント。このアカウントはデバイスにアクセスするすべての形態で使用できます。
- カスタム ユーザ アカウント。このアカウントは、**admin** ユーザおよび Config アクセス権をもつユーザが作成、管理できます。

NGIPSv は、ユーザの外部認証をサポートしていません。

Firepower Threat Defense および Firepower Threat Defense Virtual デバイス

Firepower Threat Defense および Firepower Threat Defense Virtual デバイスでは、次のユーザ アカウント タイプをサポートします。

- 事前に定義された **admin** アカウント。このアカウントはデバイスにアクセスするすべての形態で使用できます。
- カスタム ユーザ アカウント。このアカウントは、**admin** ユーザおよび Config アクセス権をもつユーザが作成、管理できます。

Firepower Threat Defense は、SSH ユーザの外部認証をサポートしています。

ASA FirePOWER デバイス

ASA FirePOWER モジュールでは、次のユーザ アカウント タイプをサポートします。

- 事前定義された **admin** アカウント。
- カスタム ユーザ アカウント。このアカウントは、**admin** ユーザおよび Config アクセス権をもつユーザが作成、管理できます。

ASA FirePOWER モジュールは、ユーザの外部認証をサポートしていません。ASA CLI および ASDM を介した ASA デバイスへのアクセスについては、『*Cisco ASA Series General Operations CLI Configuration Guide*』および『*Cisco ASA Series General Operations ASDM Configuration Guide*』に記載されています。

Firepower システム ユーザ インターフェイス

アプライアンスのタイプに応じて、Web ベースの GUI、補助的な CLI、または Linux シェルを使用して Firepower アプライアンスを操作できます。Firepower Management Center 展開では、ほとんどの設定タスクを FMC の GUI から実行します。CLI または Linux シェルを使用してアプライアンスに直接アクセスすることが必要なタスクは、ごく一部のタスクのみです。Cisco TAC または Firepower ユーザ マニュアルの明示的な手順による指示がない限り、Linux シェルを使用しないことを強くお勧めします。

ブラウザの要件については、『Firepower Release Notes』を参照してください。

（注） いずれのアプライアンスでも、SSH を介した CLI またはシェルへのログイン試行が 3 回連続して失敗すると、SSH 接続が終了します。

アプライアンス	Web ベースの GUI	補助的な CLI	Linux シェル
Firepower Management Center	• 事前定義された **admin** ユーザとカスタム ユーザ アカウントでサポートされます。 • アドミニストレーティブ タスク、管理タスク、分析タスクに使用することができます。	• 事前定義された **admin** ユーザとカスタム外部ユーザ アカウントでサポートされます。 • 有効な場合にのみアクセスできます。Firepower Management Center CLI の有効化（3364ページ）を参照してください。 • SSH 接続、シリアル接続、またはキーボードおよびモニタ接続を使用してアクセス可能です。 • Cisco TAC の指示に従って管理およびトラブルシューティングを行う場合にのみ、使用してください。	• 事前定義された **admin** ユーザとカスタム外部ユーザ アカウントでサポートされます。 • サポート対象ユーザのアクセスのデフォルト形式ですが、Firepower Management Center CLI が有効な場合は `expert` コマンド経由でアクセスする必要があります。Firepower Management Center CLI の有効化（3364ページ）を参照してください。 • SSH 接続、シリアル接続、またはキーボードおよびモニタ接続を使用してアクセス可能です。 • Cisco TAC または FMC マニュアルの明示的な手順による指示に従って管理およびトラブルシューティングを行う場合にのみ、使用してください。

アプライアンス	Web ベースの GUI	補助的な CLI	Linux シェル
7000 & 8000 シリーズ デバイス	• 事前定義された **admin** ユーザとカスタム ユーザ アカウントでサポートされます。 • 初期設定、基本的な分析、および設定タスクにのみ使用することができます。	• 事前定義された **admin** ユーザとカスタム ユーザ アカウントでサポートされます。 • SSH 接続、シリアル接続、またはキーボードおよびモニタ接続を使用してアクセス可能です。 • Cisco TAC の指示に従って設定およびトラブルシューティングを行う場合にのみ、使用できます	• 事前定義された **admin** ユーザとカスタム ユーザ アカウントでサポートされます。 • Config アクセス権を持つ CLI ユーザが `expert` コマンドを使用してアクセスできます。 • Cisco TAC または FMC マニュアルの明示的な手順による指示に従って管理およびトラブルシューティングを行う場合にのみ、使用してください。
Firepower Threat Defense Firepower Threat Defense Virtual	—	• 事前定義された **admin** ユーザとカスタム ユーザ アカウントでサポートされます。 • SSH、シリアル、またはキーボードとモニタ接続を使用してアクセスできます。仮想デバイスでは、SSH または VM コンソール経由でアクセスできます。 • Cisco TAC の指示に従って設定およびトラブルシューティングを行う場合にのみ、使用できます	• 事前定義された **admin** ユーザとカスタム ユーザ アカウントでサポートされます。 • Config アクセス権を持つ CLI ユーザが `expert` コマンドを使用してアクセスできます。 • Cisco TAC または FMC マニュアルの明示的な手順による指示に従って管理およびトラブルシューティングを行う場合にのみ、使用してください。

アプライアンス	Web ベースの GUI	補助的な CLI	Linux シェル
NGIPSv	—	• 事前定義された **admin** ユーザとカスタム ユーザ アカウントでサポートされます • SSH 接続または VM コンソールを使用してアクセスできます。 • Cisco TAC の指示に従って設定およびトラブルシューティングを行う場合にのみ、使用できます	• 事前定義された **admin** ユーザとカスタム ユーザ アカウントでサポートされます • Config アクセス権を持つ CLI ユーザが `expert` コマンドを使用してアクセスできます • Cisco TAC または FMC マニュアルの明示的な手順による指示に従って管理およびトラブルシューティングを行う場合にのみ、使用してください。
ASA FirePOWERモジュール	—	• 事前定義された **admin** ユーザとカスタム ユーザ アカウントでサポートされます。 • SSH 接続を使用してアクセスできます。また、ASA 5585-X デバイス（ハードウェア モジュール）の場合はキーボードおよびモニタ接続を使用して、その他の ASA 5500-X シリーズ デバイス（ソフトウェア モジュール）の場合はコンソール ポートを使用してアクセスできます。 • 設定タスクおよび管理タスクに使用することができます。	• 事前定義された **admin** ユーザとカスタム ユーザ アカウントでサポートされます • Config アクセス権を持つ CLI ユーザが `expert` コマンドを使用してアクセスできます • Cisco TAC または FMC マニュアルの明示的な手順による指示に従って管理およびトラブルシューティングを行う場合にのみ、使用してください。

関連トピック

社内ユーザ アカウントの追加 （57 ページ）

Web インターフェイスの考慮事項

- 組織が認証に共通アクセスカード（CAC）を使用している場合は、LDAP で認証されている外部ユーザは CAC クレデンシャルを使用してアプライアンスの Web インターフェイスにアクセスすることができます。
- Web セッション時にアプライアンスのホーム ページに初めてアクセスした際に、そのアプライアンスに対する最後のログインセッションに関する情報を表示できます。最後のログインについて、次の情報を表示できます。
  - ログインの年、月、日、曜日
  - ログイン時のアプライアンスのローカル時間（24 時間表記）
  - アプライアンスにアクセスするために最後に使用されたホストとドメイン名
- デフォルトのホーム ページの上部に表示されるメニューおよびメニュー オプションは、ユーザアカウントの権限に基づきます。ただし、デフォルトホームページのリンクには、ユーザアカウントの権限の範囲に対応するオプションが含まれています。アカウントに付与されている権限とは異なる権限が必要なリンクをクリックすると、システムから警告メッセージが表示され、そのアクティビティがログに記録されます。
- プロセスの中には長時間かかるものがあります。このため、Web ブラウザで、スクリプトが応答しなくなっていることを示すメッセージが表示されることがあります。このメッセージが表示された場合は、スクリプトが完了するまでスクリプトの続行を許可してください。

関連トピック

ホームページの指定 （43 ページ）

セッション タイムアウト

セッション タイムアウトが適用されないように設定しない限り、デフォルトでは、非アクティブな状態が 1 時間続くと、Firepower システムが自動的にセッションからユーザをログアウトします。

管理者ロールを割り当てられたユーザは、以下の設定を使用して、アプライアンスのセッション タイムアウト間隔を変更できます。

アプライアンス	設定
Firepower Management Center	**[システム（System）] > [設定（Configuration）] > [シェル タイムアウト（Shell Timeout）]**
7000 & 8000 シリーズ デバイス	**[デバイス（Devices）] > [プラットフォーム設定（Platform Settings）] > [シェル タイムアウト（Shell Timeout）]**

関連トピック

セッション タイムアウトの設定 （1315 ページ）

Firepower Management Center Web インターフェイスへのログイン

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
該当なし	任意	FMC	任意	任意

ユーザは単一のアクティブなセッションに制限されます。すでにアクティブセッションがあるユーザアカウントにログインしようとすると、もう一方のセッションを終了するか、または別のユーザとしてログインするように求められます。

複数の FMC が同じ IP アドレスを共有する NAT 環境の場合

- 各 FMC が一度にサポートできるログイン セッションは 1 つだけです。
- 異なる FMC にアクセスするには、ログインごとに別のブラウザ（Firefox や Chrome など）を使用するか、ブラウザをシークレットモードまたはプライベートモードに設定します。

始める前に

- Web インターフェイスにアクセスできない場合は、システム管理者に連絡してアカウントの特権を変更してもらうか、管理者アクセス権を持つユーザとしてログインし、アカウントの特権を変更します。
- Web インターフェイスでの内部ユーザの追加 （57 ページ）の説明に従って、ユーザ アカウントを作成します。

ステップ 1 ブラウザで **https://***ipaddress_or_hostname/* に移動します。ここで、*ipaddress* または *hostname* は使用している FMC に対応します。

ステップ 2 [ユーザ名（Username）] および [パスワード（Password）] フィールドに、ユーザ名とパスワードを入力します。次の注意事項に注意を払ってください。

- ユーザ名は大文字/小文字を区別しません。
- マルチドメイン導入環境では、ユーザ アカウントが作成されたドメインをユーザ名の前に付加します。先祖ドメインを前に付加する必要はありません。たとえばユーザ アカウントを SubdomainB で作成し、そのドメインの先祖ドメインが DomainA である場合、次の形式でユーザ名を入力します。

  ```
  SubdomainB\username
  ```

- 組織でログイン時に SecurID® トークンが使用されている場合、ログインするには SecurID PIN にトークンを付加してパスワードとして使用します。たとえば PIN が `1111` で、SecurID トークンが `222222` の

場合は、1111222222 と入力します。Firepower システムにログインする前に、SecurID PIN を生成しておく必要があります。

ステップ 3 [ログイン（Login）] をクリックします。

関連トピック

セッション タイムアウト （31 ページ）

7000 または 8000 シリーズ デバイスの Web インターフェイスへのログイン

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
該当なし	任意	7000 & 8000 シリーズ	該当なし	任意

ユーザは単一のアクティブなセッションに制限されます。すでにアクティブセッションがあるユーザアカウントにログインしようとすると、もう一方のセッションを終了するか、または別のユーザとしてログインするように求められます。

始める前に

- Web インターフェイスにアクセスできない場合は、システム管理者に連絡してアカウントの特権を変更してもらうか、管理者アクセス権を持つユーザとしてログインし、アカウントの特権を変更します。
- デバイスに該当する Firepower クイック スタート ガイドおよびWeb インターフェイスでの内部ユーザの追加 （57 ページ）の説明に従って、初期設定プロセスを完了し、ユーザ アカウントを作成します。

ステップ 1 ブラウザで https://*hostname*/ にアクセスします。ここで、*hostname* はアクセスする管理対象デバイスのホスト名に対応します。

ステップ 2 [ユーザ名（Username）] および [パスワード（Password）] フィールドに、ユーザ名とパスワードを入力します。次の注意事項に注意を払ってください。

- ユーザ名は大文字/小文字を区別しません。
- 組織でログイン時に SecurID® トークンが使用されている場合、ログインするには SecurID PIN にトークンを付加してパスワードとして使用します。たとえば PIN が 1111 で、SecurID トークンが 222222 の場合は、1111222222 と入力します。Firepower システムにログインする前に、SecurID PIN を生成しておく必要があります。

ステップ 3 [ログイン（Login）] をクリックします。

関連トピック

セッション タイムアウト （31 ページ）

CAC クレデンシャルを使用した Firepower Management Center へのログイン

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
該当なし	任意	FMC	任意	任意

ユーザは単一のアクティブなセッションに制限されます。すでにアクティブセッションがあるユーザアカウントにログインしようとすると、もう一方のセッションを終了するか、または別のユーザとしてログインするように求められます。

複数の FMC が同じ IP アドレスを共有する NAT 環境の場合

- 各 FMC が一度にサポートできるログイン セッションは 1 つだけです。
- 異なる FMC にアクセスするには、ログインごとに別のブラウザ（Firefox や Chrome など）を使用するか、ブラウザをシークレット モードまたはプライベート モードに設定します。

⚠

注意 ブラウズ セッションがアクティブな間は、CAC を削除**しない**でください。セッション中に CAC を削除または交換すると、Web ブラウザでセッションが終了し、システムにより Web インターフェイスから強制的にログアウトされます。

始める前に

- Web インターフェイスにアクセスできない場合は、システム管理者に連絡してアカウントの特権を変更してもらうか、管理者アクセス権を持つユーザとしてログインし、アカウントの特権を変更します。
- Web インターフェイスでの内部ユーザの追加 （57 ページ）の説明に従ってユーザ アカウントを作成します。
- LDAP を使用した共通アクセス カード認証の設定 （80 ページ）の説明に従って、CAC の認証と認可を設定します。

ステップ 1 組織の指示に従って CAC を挿入します。

ステップ 2 ブラウザで **https://***ipaddress_or_hostname/* に移動します。ここで、*ipaddress* または *hostname* は使用している FMC に対応します。

ステップ 3 プロンプトが表示されたら、ステップ 1 で挿入した CAC に関連付けられた PIN を入力します。

ステップ 4 プロンプトが表示されたら、ドロップダウン リストから該当する証明書を選択します。

ステップ 5 [続行（Continue）] をクリックします。

関連トピック

LDAP を使用した共通アクセス カード認証の設定 （80 ページ）
セッション タイムアウト （31 ページ）

CAC クレデンシャルを使用した 7000 または 8000 シリーズ デバイスへのログイン

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
該当なし	任意	7000 & 8000 シリーズ	該当なし	任意

ユーザは単一のアクティブなセッションに制限されます。

⚠

注意 ブラウズ セッションがアクティブな間は、CAC を削除**しない**でください。セッション中に CAC を削除または交換すると、Web ブラウザでセッションが終了し、システムにより Web インターフェイスから強制的にログアウトされます。

始める前に

- Web インターフェイスにアクセスできない場合は、システム管理者に連絡してアカウントの特権を変更してもらうか、管理者アクセス権を持つユーザとしてログインし、アカウントの特権を変更します。
- Web インターフェイスでの内部ユーザの追加 （57 ページ）の説明に従って、ユーザ アカウントを作成します。
- LDAP を使用した共通アクセス カード認証の設定 （80 ページ）の説明に従って、CAC の認証と認可を設定します。

ステップ 1 組織の指示に従って CAC を挿入します。

ステップ 2 ブラウザで `https://hostname/` にアクセスします。ここで、*hostname* はアクセスするアプライアンスのホスト名に対応します。

ステップ 3 プロンプトが表示されたら、ステップ 1 で挿入した CAC に関連付けられた PIN を入力します。
ステップ 4 プロンプトが表示されたら、ドロップダウン リストから該当する証明書を選択します。
ステップ 5 [続行（Continue）] をクリックします。

関連トピック

LDAP を使用した共通アクセス カード認証の設定 （80 ページ）
セッション タイムアウト （31 ページ）

FMC コマンドライン インターフェイスへのログイン

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
該当なし	任意	FMC	任意	任意

管理CLI ユーザと特定のカスタム外部ユーザは、FMC CLI/シェルにログインできます。

注意 Cisco TAC または FMC マニュアルの明示的な手順による指示がない限り、Linux シェルを使用しないことを強くお勧めします。

（注） すべてのアプライアンスでは、SSH を介した CLI またはシェルへのログイン試行が 3 回連続して失敗すると、SSH 接続は終了します。

始める前に

admin ユーザとして初期設定プロセスを完了します。を参照してください。最初のログイン（ 3 ページ）

ステップ 1 **admin** ユーザ名とパスワードを使用して、SSH またはコンソールポート経由で FMC に接続します。

組織でログイン時に SecurID® トークンが使用されている場合、ログインするには SecurID PIN にトークンを付加してパスワードとして使用します。たとえば PIN が `1111` で、SecurID トークンが `222222` の場合は、`1111222222` と入力します。ログインする前に、SecurID PIN を生成しておく必要があります。

ステップ 2 CLI アクセスが有効になっている場合は、利用可能な CLI コマンドのいずれかをします。

7000/8000 シリーズ、ASA FirePOWER、および NGIPSv デバイスの CLI へのログイン

基本的な CLI 設定へのアクセスを最低限保有していれば、従来の管理対象デバイスに直接ログインできます。

（注） すべてのアプライアンスでは、SSH を介した CLI またはシェルへのログイン試行が 3 回連続して失敗すると、SSH 接続は終了します。

始める前に

- 最初のログインにデフォルトの **admin** ユーザを使用して初期設定プロセスを完了します。
- **configure user add** コマンドを使用して、CLI にログインできる追加のユーザ アカウントを作成します。
- 7000 & 8000 シリーズ デバイスでは、Web インターフェイスでの内部ユーザの追加 （57 ページ）の説明に従って、Web インターフェイスでユーザ アカウントを作成します。

ステップ 1 デバイスの管理インターフェイスに SSH 接続するか（ホスト名または IP アドレス）、コンソールを使用します。

専用の ASA FirePOWER コンソールポートをもつ ASA 5585-X デバイスを除いて、コンソールを介してアクセスされる ASA FirePOWER デバイスは、デフォルトのオペレーティングシステム CLI に設定されます。これには、Firepower CLI にアクセスするための追加の手順（**`session sfr`**）が必要です。

組織でログイン時に SecurID® トークンが使用されている場合、ログインするには SecurID PIN にトークンを付加してパスワードとして使用します。たとえば PIN が `1111` で、SecurID トークンが `222222` の場合は、`1111222222` と入力します。ログインする前に、SecurID PIN を生成しておく必要があります。

ステップ 2 CLI プロンプトで、コマンド ライン アクセスのレベルで許可されている任意のコマンドを使用します。

FTD デバイスのコマンドライン インターフェイスへのログイン

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	該当なし	FTD	該当なし	CLI の基本設定

FTD 管理対象デバイスのコマンドライン インターフェイスに直接ログインできます。

（注） すべてのアプライアンスでは、SSH を介した CLI またはシェルへのログイン試行が 3 回連続して失敗すると、SSH 接続は終了します。

始める前に

最初のログインにデフォルトの **admin** ユーザを使用して初期設定プロセスを完了します。**configure user add** コマンドを使用して、CLI にログインできる追加のユーザ アカウントを作成します。

ステップ 1 コンソール ポートまたは SSH を使用して、FTD CLI に接続します。

FTD デバイスの管理インターフェイスに SSH で接続できます。SSH 接続用のインターフェイスを開いている場合、データ インターフェイス上のアドレスにも接続できます。データ インターフェイスへの SSH アクセスはデフォルトで無効になっています。特定のデータ インターフェイスへの SSH 接続を許可する方法については、セキュア シェルの設定 （1375 ページ）を参照してください。

デバイスのコンソール ポートに直接接続できます。デバイスに付属のコンソール ケーブルを使用し、9600 ボー、8 データ ビット、パリティなし、1 ストップ ビット、フロー制御なしに設定されたターミナル エミュレータを用いて PC をコンソールに接続します。コンソール ケーブルの詳細については、デバイスのハードウェア ガイドを参照してください。

コンソール ポートでアクセスする最初の CLI は、デバイス タイプによって異なります。

- ASA シリーズ デバイス：コンソール ポートの CLI は通常の FTD CLI です。
- Firepower シリーズ デバイス：コンソール ポートの CLI は FXOS です。**connect ftd** コマンドを使用して FTD CLI にアクセスできます。FXOS CLI はシャーシ レベルの設定およびトラブルシューティングにのみ使用します。基本設定、モニタリング、および通常のシステムのトラブルシューティングには FTD CLI を使用します。FXOS コマンドの詳細については、FXOS のマニュアルを参照してください。

ステップ 2 **admin** のユーザ名とパスワードでログインします。

ステップ 3 CLI プロンプト（>）で、コマンド ライン アクセス レベルで許可されている任意のコマンドを使用します。

ステップ 4 （オプション）診断 CLI にアクセスします。

system support diagnostic-cli

この CLI を使用して、高度なトラブルシューティングを行います。この CLI では、追加の **show** コマンドや、ASA 5506W-X ワイヤレス アクセス ポイントの CLI へのアクセスに必要な **session wlan console** コマンドなど、その他のコマンドが利用できます。

この CLI には 2 つのサブモード、ユーザ EXEC モードと特権 EXEC モードがあります。特権 EXEC モードではより多くのコマンドが利用できます。特権 EXEC モードを開始するには、**enable** コマンドを入力し、プロンプトに対してパスワードを入力せずに Enter を押します。

例：

```
> system support diagnostic-cli
firepower> enable
Password:
firepower#
```

通常の CLI に戻るには、**Ctrl+a**、**d** を入力します。

Firepower システム Web インターフェイスからのログアウト

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
該当なし	任意	任意	任意	任意

Firepower システムの Web インターフェイスをアクティブに使用しなくなった場合、シスコでは、少しの間 Web ブラウザから離れるだけであっても、ログアウトすることを推奨しています。ログアウトすることで Web セッションを終了し、別のユーザが自分の資格情報を使用してインターフェイスを使用できないようにします。

ユーザ名の下にあるドロップダウンリストから、[Logout] を選択します。

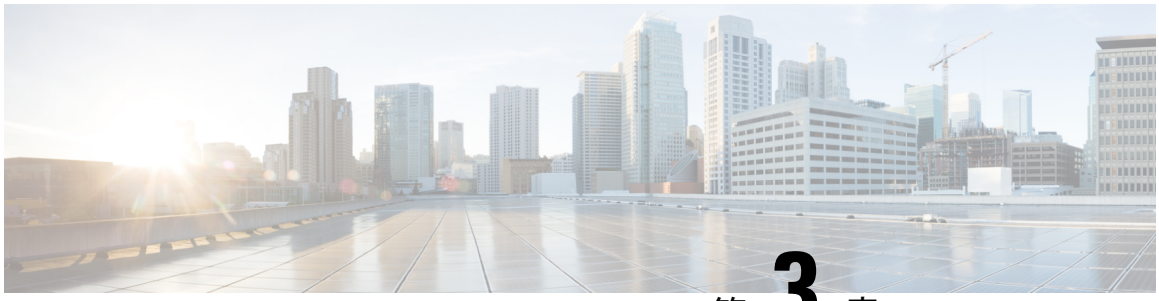
関連トピック

セッション タイムアウト （31 ページ）

Firepower システムへのログイン履歴

機能	バージョン	詳細
SSH ログイン失敗の制限数	6.3	ユーザが SSH 経由でデバイスにアクセスし、ログイン試行を 3 回続けて失敗すると、デバイスは SSH セッションを終了します。

機能	バージョン	詳細
のCLIアクセスを有効化および無効化する機能 FMC	6.3	新しい/変更された画面： FMC の Web インターフェイスで管理者が使用可能な新しいチェックボックス：**[System]** > **[Configuration]** の [CLI アクセスの有効化（Enable CLI Access）] > [コンソール設定（Console Configuration）] ページ。 • オン： SSH を使用して FMC にログインすると CLI にアクセスします。 • オフ：SSH を使用して FMC にログインすると Linux シェルにアクセスします。これは、バージョン 6.3 の新規インストールと、以前のリリースからバージョン 6.3 にアップグレードした場合のデフォルトの状態です。 サポートされるプラットフォーム FMC



第 3 章

ユーザ設定の指定

以下のトピックでは、ユーザ設定を指定する方法について説明します。

ユーザ設定の概要

ホーム ページ、アカウント パスワード、タイム ゾーン、ダッシュボード、イベント ビューの各設定など、単一のユーザ アカウントに関連付けられた設定を構成できます。

ユーザ ロールに応じて、パスワード、イベント ビューの設定、タイム ゾーンの設定、ホーム ページの設定など、ユーザ アカウントにある特定の設定を指定できます。

マルチドメイン展開では、ユーザ設定は、アカウントでアクセスできるすべてのドメインに適用されます。ホーム ページ設定とダッシュボード設定を指定した場合、特定のページとダッシュボード ウィジェットがドメインから制約を受けることに留意してください。

パスワードの変更

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	任意	任意	任意	任意

すべてのユーザ アカウントはパスワードで保護されています。パスワードはいつでも変更することができ、ユーザ アカウントの設定によっては定期的にパスワードを変更しなければならない場合もあります。

パスワードの強度チェックが有効の場合、パスワードは大文字と小文字が混在する少なくとも 8 つの英数字で、少なくとも 1 つの数字が含まれている必要があります。パスワードは、辞書に出現する単語であったり、連続する繰り返し文字を含んでいたりすることができません。

LDAP または RADIUS ユーザの場合、Web インターフェイスを介してパスワードを変更することはできません。

ステップ 1 ユーザ名の下にあるドロップダウン リストから、[ユーザ プリファレンス（User Preferences）] を選択します。

ステップ 2 [現在のパスワード（Current Password）] を入力して、[変更（Change）] をクリックします。

ステップ 3 [新しいパスワード（New Password）] および [確認（Confirm）] フィールドに、新しいパスワードを入力します。

ステップ 4 [変更（Change）] をクリックします。

失効パスワードの変更

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	任意	任意	任意	任意

ユーザアカウントの設定によっては、パスワードが期限切れになることがあります。パスワードの有効期間は、アカウントが作成されたときに設定されます。パスワードが期限切れになった場合、[パスワードの有効期限の警告（Password Expiration Warning）] ページが表示されます。

パスワードの有効期限の警告のページには 2 つの選択肢があります。

- すぐにパスワードを変更するには、[パスワードの変更（Change Password）] をクリックします。残りの警告日数がゼロの場合は、パスワードを変更する**必要があります**。

  ヒント パスワードの強度チェックが有効の場合、パスワードは大文字と小文字が混在する少なくとも 8 つの英数字で、少なくとも 1 つの数字が含まれている必要があります。パスワードは、辞書に出現する単語であったり、連続する繰り返し文字を含んでいたりすることができません。

- 後でパスワードを変更するには、[後で（Skip）] をクリックします。

ホームページの指定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	任意	任意	任意	External Database User を除くすべてのユーザ

Webインターフェイス内のページをアプライアンスのホームページに指定できます。ダッシュボードへのアクセス権がないユーザ アカウントを除いて、デフォルトのホームページは、デフォルト ダッシュボード（**[Overview]** > **[Dashboards]**）です（デフォルト ダッシュボードの設定については、「デフォルトのダッシュボードの指定（50ページ）」を参照してください）。

マルチドメイン環境では、選択したデフォルトのホームページは、ユーザアカウントがアクセスできるすべてのドメインに適用されます。複数のドメインに頻繁にアクセスするアカウントのホームページを選択する際、特定のページはグローバル ドメインに制限されることに注意してください。

ステップ 1 ユーザ名の下にあるドロップダウン リストから、[ユーザ設定（User Preferences）] を選択します。

ステップ 2 [ホームページ（Home Page）] をクリックします。

ステップ 3 ホーム ページとして使用するページをドロップダウン リストから選択します。

ドロップダウン リスト内のオプションは、ユーザアカウントのアクセス権限に基づいて表示されます。詳細については、Web インターフェイスのユーザ ロール （54 ページ）を参照してください。

ステップ 4 **[保存（Save）]** をクリックします。

イベント ビュー設定の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン数	アクセス
任意	任意	任意	任意	機能に応じて異なる

[イベント ビュー設定（Event View Settings）] ページを使用して、Firepower Management Center のイベント ビューの特性を設定します。イベント ビュー設定は、特定のユーザ ロールでのみ使用可能であることに注意してください。External Database User ロールを持つユーザは、イベント ビュー設定のユーザ インターフェイスの一部を表示できますが、それらの設定を変更しても意味のある結果は生じません。

ステップ 1 ユーザ名の下にあるドロップダウン リストから、[ユーザ設定（User Preferences）] を選択します。

ステップ 2 [イベント ビュー設定（Event View Settings）] をクリックします。

ステップ 3 [イベント設定（Event Preferences）] セクションで、イベント ビューの基本特性を設定します。イベント ビュー設定 （44 ページ）を参照してください。

ステップ 4 [ファイル設定（File Preferences）] セクションで、ファイル ダウンロードを設定します。ファイル ダウンロード設定 （45 ページ）を参照してください。

ステップ 5 [デフォルト時間帯（Default Time Windows）] セクションで、デフォルトの時間帯を設定します。デフォルト時間枠 （46 ページ）を参照してください。

ステップ 6 [デフォルト ワークフロー（Default Workflow）] セクションで、デフォルト ワークフローを設定します。デフォルト ワークフロー （48 ページ）を参照してください。

ステップ 7 **[保存（Save）]** をクリックします。

イベント ビュー設定

[イベント ビュー設定（Event View Settings）] ページの [イベント設定（Event Preferences）] セクションを使用して、Firepower システムのイベント ビューの基本特性を設定します。このセクションはすべてのユーザ ロールで使用可能ですが、イベントを表示できないユーザには、ほとんどまたはまったく意味がありません。

以下のフィールドが [Event Preferences] セクションに示されます。

- [Confirm “All” Actions] フィールドは、イベント ビューのすべてのイベントに影響を与える操作について、アプライアンスがユーザに確認を要求するかどうかを制御します。

  たとえば、この設定が有効である場合、イベント ビューで [Delete All] をクリックすると、アプライアンスがデータベースからの削除を実行する前に、現在の制約を満たすすべてのイベント（現在のページに表示されていないイベントを含む）を削除することをユーザが確認する必要があります。

- [Resolve IP Addresses] フィールドは、可能な場合には常に、アプライアンスがイベント ビューで IP アドレスの代わりにホスト名を表示するようにします。

  多数の IP アドレスが含まれている場合、このオプションを有効にすると、イベント ビューの表示に時間がかかる可能性があることに注意してください。また、この設定を有効にするには、管理インターフェイス設定を使用して、システム設定で DNS サーバを確立する必要があることにも注意してください。

- [パケット ビューの展開（Expand Packet View）] フィールドでは、侵入イベントのパケット ビューをどのように表示するかを設定できます。デフォルトでは、アプライアンスによるパケット ビューの表示は折りたたまれた状態になっています。

  - [なし（None）] : パケット ビューの [パケット情報（Packet Information）] セクションのサブセクションをすべて折りたたんだ状態にします。

- [パケット テキスト（Packet Text）]：[パケット テキスト（Packet Text）] サブセクションだけを展開します。
- [パケット バイト（Packet Bytes）]：[パケット バイト（Packet Bytes）] サブセクションだけを展開します。
- [すべて（All）]：すべてのセクションを展開します。

デフォルト設定に関係なく、パケット ビューのセクションを手動で展開することで、キャプチャされたパケットに関する詳細情報を常に表示することができます。

- [1 ページあたりの行数（Rows Per Page）] フィールドは、ドリル ダウン ページとテーブル ビューに表示する、ページごとのイベントの行数を制御します。
- [更新間隔（Refresh Interval）] フィールドは、イベント ビューの更新間隔を分単位で設定します。0 を入力すると、更新オプションが無効になります。この間隔はダッシュボードに適用されないことに注意してください。
- [Statistics Refresh Interval] は、[Intrusion Event Statistics] や [Discovery Statistics] ページなどのイベントのサマリー ページの更新間隔を制御します。0 を入力すると、更新オプションが無効になります。この間隔はダッシュボードに適用されないことに注意してください。
- [ルールの非アクティブ化（Deactivate Rules）] フィールドは、標準テキスト ルールによって生成される侵入イベントのパケット ビューに、どのリンクを表示させるかを次のように制御します。
  - [すべてのポリシー（All Policies）]：すべてのローカルで定義されたカスタム侵入ポリシーで標準テキスト ルールを非アクティブにする単一リンク
  - [現在のポリシー（Current Policy）]：現在展開中の侵入ポリシーだけで標準テキスト ルールを非アクティブにする単一リンク。デフォルトのポリシーのルールは非アクティブにできないことに注意してください。
  - [質問（Ask）]：これらの個々のオプションへのリンク

パケット ビューでこれらのリンクを表示するには、Administrator または Intrusion Admin のアクセス権があるユーザ アカウントが必要です。

関連トピック

管理インターフェイス （1266 ページ）

ファイル ダウンロード設定

[イベント ビュー設定（Event View Settings）] ページの [ファイル設定（File Preferences）] セクションを使用して、ローカル ファイル ダウンロードの基本特性を設定します。このセクションは、Administrator、Security Analyst、または Security Analyst（読み取り専用）ユーザ ロールを持つユーザのみが使用できます。

キャプチャされたファイルのダウンロードをアプライアンスがサポートしていない場合、これらのオプションは無効になることに注意してください。

以下のフィールドが [ファイル設定（File Preferences）] セクションに示されます。

- [Confirm 'Download File' Actions] チェックボックスは、ファイルをダウンロードするたびに [File Download] ポップアップウィンドウが表示され、警告が示されて続行するかキャンセルするかを選択するためのプロンプトが出されるようにするかどうかを制御します。

  ⚠

  注意 シスコでは、有害な結果が発生することがあるため、マルウェアをダウンロード**しない**ように強くお勧めします。ファイルをダウンロードする際は、マルウェアが含まれている可能性があるので注意してください。ファイルをダウンロードする前に、ダウンロード先をセキュアにするために必要な予防措置を行っていることを確認します。

  ファイルをダウンロードする際には、いつでもこのオプションを無効にできることに注意してください。

- キャプチャされたファイルをダウンロードすると、そのファイルを含むパスワード保護された .zip アーカイブがシステムによって作成されます。[Zip File Password] フィールドは、zip ファイルへのアクセスを制限するためにユーザが使用するパスワードを定義します。このフィールドを空欄にすると、パスワードなしのアーカイブ ファイルがシステムによって作成されます。

- [Show Zip File Password] チェック ボックスによって、[Zip File Password] フィールドにプレーンテキストを表示するかまたは不明瞭な文字を表示するかを切り替えます。このフィールドをオフにすると、[zip ファイル パスワード（Zip File Password）] には不明瞭な文字が表示されます。

デフォルト時間枠

時間枠（時間範囲と呼ばれることもある）は、任意のイベント ビューでイベントに時間制約を課します。[Event View Settings] ページの [Default Time Windows] セクションを使用して、時間枠のデフォルトの動作を制御します。

このセクションへのユーザ ロール アクセスは以下のとおりです。

- Administrators と Maintenance Users は、セクション全体にアクセスできます。

- Security Analysts と Security Analysts（読み取り専用）は、[Audit Log Time Window] 以外のすべてのオプションにアクセスできます。

- Access Admins、Discovery Admins、External Database Users、Intrusion Admins、Network Admins、および Security Approvers は、[Events Time Window] オプションにのみアクセスできます。

デフォルトの時間枠設定に関係なく、イベントの分析中にいつでも手動で個別のイベント ビューの時間枠を変更できることに注意してください。また、時間枠の設定は、現在のセッションにだけ有効であることにも注意してください。ログアウトしてから再びログインすると、時間枠は、このページで設定したデフォルトにリセットされます。

以下のように、デフォルトの時間枠を設定できる 3 つのタイプのイベントがあります。

- [Events Time Window] は、時間で制約できるほとんどイベントのために単一のデフォルトの時間枠を設定します。
- [Audit Log Time Window] は、監査ログのためにデフォルトの時間枠を設定します。
- [Health Monitoring Time Window] は、ヘルス イベントのためにデフォルトの時間枠を設定します。

時間枠は、ユーザ アカウントがアクセスできるイベント タイプにのみ設定できます。すべてのユーザ タイプは、イベントの時間枠を設定できます。Administrators、Maintenance Users、および Security Analysts は、ヘルス モニタリングの時間枠を設定できます。Administrators と Maintenance Users は、監査ログの時間枠を設定できます。

すべてのイベント ビューが時間で制約できるとは限らないので、時間枠の設定によって、ホスト、ホスト属性、アプリケーション、クライアント、脆弱性、ユーザの ID、ホワイトリスト違反を表示するイベント ビューは影響を受けないことに注意してください。

複数の時間枠を使用して、上記の各タイプのイベントに 1 つずつ適用するか、または**単一の**時間枠を使用して、それをすべてのイベントに適用することができます。単一の時間枠を使用すると、3 つのタイプの時間枠用の設定が非表示になり、新しく [Global Time Window] 設定が表示されます。

以下の 3 つのタイプの時間枠があります。

- 静的は、特定の開始時刻から特定の終了時刻までに生成されたすべてのイベントを表示します
- 拡張は、特定の開始時刻から現在までに生成されたすべてのイベントを表示します。時間の進行と共に時間枠が拡張され、新しいイベントがイベント ビューに追加されます。
- スライディングは、特定の開始時刻（たとえば 1 日前）から現在までに生成されたすべてのイベントを表示します。時間の進行と共に時間枠は「スライド」し、設定した範囲内（この例では直前の 1 日）のイベントだけが表示されます。

すべての時間枠の最大時間範囲は、1970 年 1 月 1 日午前 0 時（UTC）～ 2038 年 1 月 19 日午前 3 時 14 分 7 秒です。

次のオプションは、[Time Window Settings] ドロップダウン リストに表示されます。

- [Show the Last - Sliding] オプションにより、指定した長さのスライドするデフォルトの時間枠を設定できます。

  アプライアンスは、特定の開始時刻（たとえば 1 時間前）から現在までに生成されたすべてのイベントを表示します。イベント ビューの変更と共に、時間枠は「スライド」して、常に最後の 1 時間内のイベントが表示されます。

- [Show the Last - Static/Expanding] により、指定した長さのデフォルトの時間枠を静的または拡張のどちらかに設定できます。

  静的時間枠にするには、[Use End Time] チェック ボックスをオンにします。アプライアンスは、特定の開始時間（1 時間前など）から現在までに生成されたすべてのイベントを表示します。イベント ビューを変更しても時間枠は固定されており、静的な時間枠の間に発生したイベントのみが表示されます。

  拡張時間枠にするには、[Use End Time] チェック ボックスをオフにします。アプライアンスは、特定の開始時刻（たとえば 1 時間前）から現在までに生成されたすべてのイベントを表示します。イベント ビューを変更すると、時間枠は現在まで拡張されます。

- [Current Day - Static/Expanding] オプションにより、現在の日付のデフォルトの時間枠を静的または拡張のどちらかに設定できます。現在の日付は、現行セッションのタイム ゾーン設定に基づいて午前 0 時に始まります。

  静的時間枠にするには、[Use End Time] チェック ボックスをオンにします。アプライアンスは、午前 0 時からユーザがイベントを初めて確認した時刻までに生成されたすべてのイベントを表示します。イベント ビューを変更しても時間枠は固定されており、静的な時間枠の間に発生したイベントのみが表示されます。

  拡張時間枠にするには、[Use End Time] チェック ボックスをオフにします。アプライアンスは、午前 0 時から現在までに生成されたすべてのイベントを表示します。イベント ビューを変更すると、時間枠は現在まで拡張されます。ログアウトする前に 24 時間を超えて分析を続けた場合、この時間枠は 24 時間よりも長くなる可能性があることに注意してください。

- [Current Week - Static/Expanding] オプションにより、現在の週のデフォルトの時間枠を静的または拡張のどちらかに設定できます。現在の週は、現行セッションのタイム ゾーン設定に基づいて直前の日曜日の午前 0 時に始まります。

  静的時間枠にするには、[Use End Time] チェック ボックスをオンにします。アプライアンスは、午前 0 時からユーザがイベントを初めて確認した時刻までに生成されたすべてのイベントを表示します。イベント ビューを変更しても時間枠は固定されており、静的な時間枠の間に発生したイベントのみが表示されます。

  拡張時間枠にするには、[Use End Time] チェック ボックスをオフにします。アプライアンスは、日曜日の午前 0 時から現在までに生成されたすべてのイベントを表示します。イベント ビューを変更すると、時間枠は現在まで拡張されます。ログアウトする前に 1 週間を超えて分析を続けた場合、この時間枠は 1 週間よりも長くなる可能性があることに注意してください。

デフォルト ワークフロー

ワークフローは、アナリストがイベントの評価に使用するデータが示された一連のページです。アプライアンスには、各イベント タイプに少なくとも 1 つの定義済みのワークフローが付属しています。たとえば、Security Analyst の場合、実行する分析のタイプに応じて、それぞれ

が侵入イベントのデータを別の形式で示している、10の異なる侵入イベントのワークフローから選択できます。

アプライアンスは、イベントタイプごとのデフォルトのワークフローによって設定されます。たとえば、[Events by Priority and Classification（優先度および分類に基づいたイベント）] ワークフローが、侵入イベントのデフォルトになります。つまり、侵入イベント（確認済みの侵入イベントを含む）を表示するたびに、アプライアンスは [優先順位および分類に基づいたイベント（Events by Priority and Classification）] ワークフローを表示します。

ただし、イベント タイプごとにデフォルト ワークフローは変更できます。設定可能なデフォルトのワークフローは、ユーザ ロールによって異なります。たとえば、侵入イベントのアナリストがデフォルトのディスカバリ イベント ワークフローを設定することはできません。

デフォルト タイム ゾーンの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	任意	任意	任意	任意

Firepower Management Center とその管理対象デバイスは正確な時刻に大きく依存しています。システム クロックはFirepowerシステムの時刻を維持するシステム機能です。システム クロックは協定世界時（UTC）に設定されています。これは、時計と時刻を管理するために世界で使用されている基本的な標準時間です。

イベントの表示に使用するタイム ゾーンを、アプライアンスが使用している標準 UTC 時間から変更できます。設定したタイム ゾーンは現在のユーザ アカウントにのみ適用され、タイム ゾーンをさらに変更するまで有効になります。

制約事項

タイムゾーン機能（[ユーザ設定（User Preferences）]）は、デフォルトのシステム クロックがUTC時間に設定されていることを前提としています。システム時刻を変更しようとしないでください。システム時刻の UTC からの変更はサポートされていません。また、システム時刻を変更した場合はデバイスを再イメージ化してサポートされていない状態から回復させる必要があります。

ステップ 1 ユーザ名の下にあるドロップダウン リストから、[ユーザ設定（User Preferences）] を選択します。

ステップ 2 [タイムゾーン設定（Time Zone Preference）] タブをクリックします。

ステップ 3 左側のリスト ボックスで、使用するタイム ゾーンを含む大陸または地域を選択します。

ステップ 4 右側のリスト ボックスで、使用するタイム ゾーンに対応するゾーン（都市名）を選択します。

ステップ 5 **[保存（Save）]** をクリックします。

デフォルトのダッシュボードの指定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	任意	任意	任意	Admin/Maint/Any Security Analyst

[Overview] > **[Dashboards]** を選択すると、デフォルトのダッシュボードが表示されます。変更しない限り、すべてのユーザのデフォルト ダッシュボードは、[サマリー（Summary）] ダッシュボードです。

マルチドメイン環境では、選択したデフォルトのダッシュボードは、ユーザアカウントがアクセスできるすべてのドメインに適用されます。複数のドメインに頻繁にアクセスするアカウントのダッシュボードを選択する際、ドメインが特定のダッシュボードウィジェットを制限することに注意してください。

ステップ 1 ユーザ名の下にあるドロップダウン リストから、[ユーザ設定（User Preferences）] を選択します。

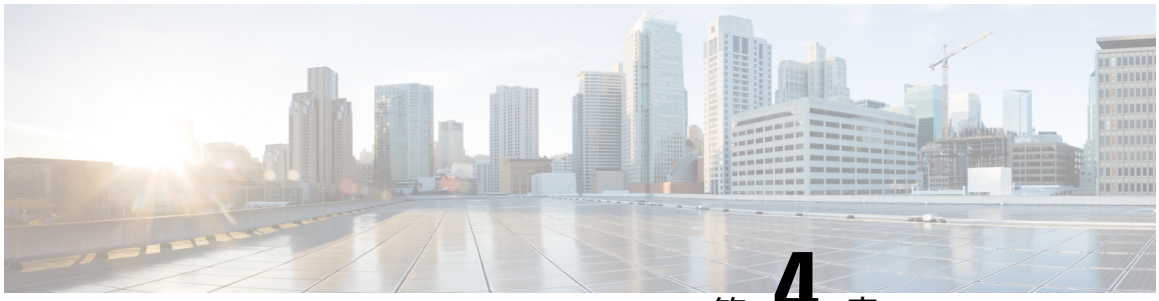
ステップ 2 [ダッシュボード設定（Dashboard Settings）] をクリックします。

ステップ 3 デフォルトとして使用するダッシュボードをドロップダウン リストから選択します。[なし（None）] を選択した場合、**[Overview]** > **[Dashboards]** を選択するときに、表示するダッシュボードを選択できます。

ステップ 4 **[保存（Save）]** をクリックします。

関連トピック

ダッシュボードの表示 （346 ページ）



第 4 章

管理アクセス用のユーザ アカウント

Firepower Management Center と管理対象デバイスには、管理アクセス用のデフォルトの**管理者**アカウントが含まれています。この章では、サポートされているモデル用のカスタム ユーザ アカウントを作成する方法について説明します。ユーザ アカウントを使用して Firepower Management Center または管理対象デバイスにログインする方法の詳細については、Firepower システムへのログイン （25 ページ）を参照してください。

この章では、Cisco Security Manager（CSM）で ASA を管理し、Firepower Management Center で FirePOWER サービス モジュールを管理する場合の、CSM シングル サインオンについても説明します。

ユーザ アカウントについて

内部ユーザとして、またはモデルでサポートされている場合は LDAP または RADIUS サーバの外部ユーザとして、Firepower Management Center および管理対象デバイスにカスタム ユーザ アカウントを追加できます。各 Firepower Management Center と各管理対象デバイスは、個別のユーザ アカウントを保持します。たとえば、Firepower Management Center にユーザを追加した場合は、そのユーザは FMC にのみアクセスできます。そのユーザ名を使用して管理対象デバイスに直接ログインすることはできません。管理対象デバイスにユーザを別途追加する必要があります。

内部および外部ユーザ

Firepower デバイスは次の 2 つのタイプのユーザをサポートしています。

- 内部ユーザ：デバイスは、ローカルデータベースでユーザ認証を確認します。内部ユーザの詳細については、社内ユーザ アカウントの追加 （57 ページ）を参照してください。
- 外部ユーザ：ユーザがローカルデータベースに存在しない場合は、システムは外部 LDAP または RADIUS の認証サーバに問い合わせます。外部ユーザの詳細については、外部認証の設定 （62 ページ）を参照してください。

Web インターフェイス、CLI またはシェルによるアクセス

ユーザ アカウントを設定する際に、Web インターフェイス アクセスと CLI またはシェル アクセスを個別に有効にします。 Firepower デバイスには、Linux の上部で実行する Firepower CLI が含まれます。CLI ユーザは、TAC の監督のもとで、または Firepower ユーザ マニュアルに明示的な手順がある場合、Linux シェルにアクセスすることもできます。管理 UI の詳細については、「Firepower システム ユーザ インターフェイス （28 ページ）」を参照してください。

注意 すべてのデバイス上で、CLI の Config レベルのアクセス権またはシェルへのアクセス権があるユーザは、Linux シェルの `sudoers` 権限を取得できます。このため、セキュリティ上のリスクが生じる可能性があります。システム セキュリティ上の理由から、次の点を強くお勧めします。

- 外部認証を確立した場合は、CLI またはシェルへのアクセス権があるユーザのリストを適切に制限してください。
- CLI アクセス権限を付与する場合は、構成レベルのアクセス権を付与されたユーザのリストを制限します。
- Linux シェルでユーザを直接追加しないでください。この章の手順のみを使用してください。
- Cisco TAC による指示または Firepower ユーザ マニュアルの明示的な手順による指示がない限り、Linux シェルや CLI エキスパート モードを使用して Firepower デバイスにアクセスしないでください。

各デバイス タイプでサポートされているアクセス形式は異なります。次に詳細を示します。

- FTD、 ASA FirePOWER、および NGIPSv では、デバイスの直接管理に CLI アクセスを使用できます。
  - これらのデバイスでは CLI を使用して内部ユーザを作成できます。
  - Firepower Threat Defense デバイスでは外部ユーザを確立できます。

- 管理インターフェイスを通じてこれらのデバイスにログインしているユーザはCLIにアクセスします。CLI Config レベルのアクセス権を持つユーザは、CLI **expert** コマンドを使用して Linux シェルにアクセスできます。

  ⚠

  注意 Cisco TAC または Firepower ユーザ マニュアルの明示的な手順による指示がない限り、Linux シェルを使用しないことを強くお勧めします。

- FMC にはデバイスを直接管理するための Web インターフェイス、CLI、および Linux シェルがあります。
  - FMC は 2 種類の内部 **admin** ユーザをサポートします。つまり Web インターフェイスのユーザと、 CLI またはシェル アクセス権が付与されたユーザが対象になります。これら 2 つの **admin** ユーザは異なるアカウントであり、同じパスワードを共有しません。システム初期化プロセスでは、これら 2 つの**admin** アカウントのパスワードが同期されるため、アカウントは同じように開始されますが、これらのアカウントは異なる内部メカニズムによって追跡され、初期設定後に分岐する場合があります。システム初期化の詳細については、ご使用のモデルの『*Getting Started Guide*』を参照してください。（Web インターフェイスの **admin** のパスワードを変更するには、**[System]** > **[Users]** > [ユーザ（Users）] を使用します。CLI またはシェルの **admin** のパスワードを変更するには、FMCCLI コマンド **configure password** を使用します）。
  - FMC Web インターフェイスで追加された内部ユーザには、Web インターフェイスのアクセス権のみが付与されます。
  - CLI またはシェルへのアクセス権を FMC の外部ユーザに付与できます。
  - FMC のデフォルトでは、シェルまたは CLI へのアクセス権を持つアカウントが管理インターフェイスにログインすると、そのアカウントは Linux シェルに直接アクセスします。FMC CLI を有効にすると、それらのユーザはログイン時にまず CLI へのアクセス権を取得すると、**expert** コマンドを使用してシェルへのアクセス権を取得できる場合があります。「Firepower Management Center のコマンド ライン リファレンス（3363 ページ）」を参照してください。
- 7000 および 8000 シリーズ デバイスには、デバイスを直接管理するための Web インターフェイスと CLI の両方が備わっています。
  - 7000 および 8000 シリーズ デバイスの内部ユーザには Web インターフェイスと CLI アクセス権があります。
  - 7000 および 8000 シリーズ デバイスの外部ユーザに対して CLI またはシェルへのアクセスを有効にできます。
  - 管理インターフェイスを通じてこれらのデバイスにログインしているユーザはCLIにアクセスします。CLI Config レベルのアクセス権を持つユーザは、シェルの **expert** コマンドを使用してシェルにアクセスできます。

⚠

注意 Cisco TAC またはFMC マニュアルの明示的な手順による指示がない限り、Linux シェルを使用しないことを強くお勧めします。

ユーザ ロール

ユーザ権限は、割り当てられたユーザ ロールに基づいています。たとえば、アナリストに対してセキュリティ アナリストや検出管理者などの事前定義ロールを付与し、デバイスを管理するセキュリティ管理者に対して管理者ロールを予約することができます。また、組織のニーズに合わせて調整されたアクセス権限を含むカスタム ユーザ ロールを作成できます。

Web インターフェイスのユーザ ロール

7000 および 8000 シリーズのデバイスは、管理者、メンテナンス ユーザ、およびセキュリティ アナリストのユーザ ロールへのアクセス権を持っています。

Firepower Management Center には、次の定義済みユーザ ロールが含まれています。

アクセス管理者（Access Admin）

[ポリシー（Policies）] メニューでアクセス制御ポリシー機能や関連する機能へのアクセスが可能です。アクセス管理者は、ポリシーを展開できません。

管理者

管理者は製品内のすべてのものにアクセスできるため、セッションでセキュリティが侵害されると、高いセキュリティ リスクが生じます。このため、ログイン セッション タイムアウトから管理者を除外することはできません。

セキュリティ上の理由から、管理者ロールの使用を制限する必要があります。

Discovery Admin

[ポリシー（Policies）] メニューのネットワーク検出機能、アプリケーション検出機能、相関機能にアクセス可能です。検出管理者は、ポリシーを展開できません。

外部データベース ユーザ

JDBC SSL 接続に対応しているアプリケーションを用いて、Firepower System データベースに対して読取り専用のアクセスが可能です。Firepower システム アプライアンスの認証を行うサードパーティのアプリケーションについては、システム設定内でデータベースへのアクセスを有効にする必要があります。Web インターフェイスでは、外部データベース ユーザは、[ヘルプ（Help）] メニューのオンライン ヘルプ関連のオプションのみにアクセスできます。このロールの機能には Web インターフェイスが含まれていないため、容易なサポートとパスワード変更の目的でのみアクセスが提供されます。

侵入管理者（Intrusion Admin）

[ポリシー（Policies）] メニューと [オブジェクト（Objects）] メニューの侵入ポリシー機能、侵入ルール機能、ネットワーク分析ポリシー機能のすべてにアクセスが可能です。侵入管理者は、ポリシーを展開できません。

メンテナンス ユーザ（Maintenance User）

監視機能と保守機能へのアクセスを提供します。メンテナンスユーザは、[ヘルス（Health）] メニューや[システム（System）] メニューのメンテナンス関連オプションにアクセスできます。

ネットワーク管理者

[ポリシー（Policies）] メニューのアクセス制御機能、SSL インスペクション機能、DNS ポリシー機能、アイデンティティ ポリシー機能、および [デバイス（Devices）] メニューのデバイス設定機能へのアクセスが可能です。ネットワーク管理者は、デバイスへの設定の変更を展開できます。

Security Analyst

セキュリティ イベント分析機能へのアクセスと [概要（Overview）] メニュー、[分析（Analysis）] メニュー、[ヘルス（Health）] メニュー、[システム（System）] メニューのヘルス イベントに対する読み取り専用のアクセスが可能です。

Security Analyst (Read Only)

[概要（Overview）] メニュー、[分析（Analysis）] メニュー、[ヘルス（Health）] メニュー、[システム（System）] メニューのセキュリティ イベント分析機能とヘルス イベント機能への読み取り専用アクセスを提供します。

Security Approver

[ポリシー（Policies）] メニューのアクセス制御ポリシーや関連のあるポリシー、ネットワーク検出ポリシーへの制限付きのアクセスが可能です。セキュリティ承認者はこれらのポリシーを表示し、展開できますが、ポリシーを変更することはできません。

Threat Intelligence Director（TID）ユーザ

[Intelligence] メニューの Threat Intelligence Director 設定にアクセスできます。Threat Intelligence Director（TID）ユーザは、TID の表示および設定が可能です。

CLI ユーザ ロール

管理対象デバイスでは、CLI のコマンドへのユーザのアクセス権は割り当てるロールによって異なります。

（注） FMC の CLI 外部ユーザにはユーザ ロールがありません。そのため、それらのユーザは使用可能なすべてのコマンドを使用できます。

None

ユーザは、コマンド ラインでデバイスにログインすることはできません。

Config

ユーザは、設定コマンドを含むすべてのコマンドにアクセスできます。このアクセス レベルをユーザに割り当てるときには注意してください。

Basic

ユーザは、非設定コマンドにのみアクセスできます。

（注） 管理対象デバイス上の外部CLIユーザには常にConfigユーザ ロールが備わっています。RADIUSを使用している Firepower Threat Defense の場合、Config または Basic のいずれかを指定できます。

ユーザ アカウントの要件と前提条件

モデルのサポート

外部ユーザ認証は、次のモデルでサポートされています。

- Firepower Management Center
- Firepower Threat Defense
- 7000 および 8000 シリーズ

ユーザ アカウントの注意事項および制約事項

デフォルト

すべてのデバイスには、すべてのアクセス形式のローカルユーザアカウントとして**admin**ユーザが含まれています。**admin**ユーザは削除できません。デフォルトの初期パスワードは**Admin123**です。初期化プロセス中に、この初期パスワードの変更が強制されます。システム初期化の詳細については、ご使用のモデルの『*Getting Started Guide*』を参照してください。

Global Settings

デフォルトでは、Firepower Management Center のすべてのユーザ アカウントに次の設定が適用されます。

- パスワードの再利用に制限はありません。
- システムは正常なログインを追跡しません。

- システムは、不正なログイン クレデンシャルを入力したユーザに対して時間が指定された一時的なロックアウトを適用しません。

すべてのユーザのこれらの設定は、システム設定として変更できます。（**[System]** > **[Configuration]** > **[User Configuration]**）グローバル ユーザ構成時の設定 （1312 ページ）を参照してください。

社内ユーザ アカウントの追加

各デバイスは、個別のユーザ アカウントを保持します。Firepower Management Center と 7000 および 8000 シリーズ の Web インターフェイスは似ています。Firepower Threat Defense、NGIPSv、および ASA FirePOWER では、CLI で社内ユーザを追加する必要があります。Firepower Management Center および 7000 および 8000 シリーズ では、CLI でユーザを追加することはできません。

Web インターフェイスでの内部ユーザの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	任意	FMC 7000 & 8000 シリーズ	任意	管理者

この手順では、Firepower Management Center または 7000 & 8000 シリーズ デバイスの Web インターフェイスでカスタム内部ユーザ アカウントを追加する方法について説明します。

[システム（System）] > **[ユーザ（Users）]** > **[ユーザ（Users）]** タブには、手動で追加した内部ユーザと、LDAP または RADIUS 認証でユーザがログインしたときに自動的に追加された外部ユーザの両方が表示されます。外部ユーザについては、より高い権限を持つロールを割り当てると、この画面のユーザ ロールを変更できます。パスワード設定を変更することはできません。

Firepower Management Center のマルチドメイン展開では、ユーザは作成されたドメインでのみ表示されます。グローバル ドメインにユーザを追加してから、リーフ ドメインのユーザ ロールを割り当てると、そのユーザがリーフ ドメインに「所属」していても、追加されたグローバル [ユーザ（Users）] ページにそのユーザが表示されることに注意してください。

デバイスでセキュリティ認定コンプライアンスまたは Lights-Out Management（LOM）を有効にすると、異なるパスワード制限が適用されます。セキュリティ認定コンプライアンスの詳細については、セキュリティ認定準拠 （1411 ページ）を参照してください。

リーフ ドメインにユーザを追加した場合、そのユーザはグローバル ドメインからは表示されません。

ステップ 1 **[System]** > **[Users]**を選択します。

[ユーザ（Users）] タブはデフォルトで表示されます。

ステップ 2 [Create User] をクリックします。

ステップ 3 [ユーザ名（User Name）] に入力します。

ユーザ名は、次のように Linux に対して有効である必要があります。

- 英数字、ハイフン（-）、およびアンダースコア（_）が使用可で、最大 32 文字
- すべて小文字
- 最初の文字にハイフン（-）は使用不可、すべて数字は不可、ピリオド（.）、アットマーク（@）、またはスラッシュ（/）は使用不可

ステップ 4 LDAP または RADIUS によりログインしたときに自動的に追加されたユーザに対しては、[外部認証方式の使用（Use External Authentication Method）] チェックボックスがオンになっています。外部ユーザを事前設定する必要はないため、このフィールドは無視できます。外部ユーザについては、このチェックボックスをオフにすることで、そのユーザを内部ユーザに戻すことができます。

ステップ 5 [パスワード（Password）] および [パスワードの確認（Confirm Password）] フィールドに値を入力します。

この値は、このユーザに設定したパスワード オプションに準拠している必要があります。

ステップ 6 [ログイン失敗の最大回数（Maximum Number of Failed Logins）] を設定します。

各ユーザが、ログイン試行の失敗後に、アカウントがロックされるまでに試行できるログインの最大回数を示す整数を、スペースなしで入力します。デフォルト設定は 5 回です。ログイン失敗回数を無制限にするには、**0** を使用します。**管理者**アカウントは、ログイン失敗回数が最大数に達してもロックアウトされません（ただし、セキュリティ認定コンプライアンスを有効にした場合は除きます）。

ステップ 7 [パスワードの最小長（Minimum Password Length）] を設定します。

ユーザのパスワードの必須最小長（文字数）を示す整数を、スペースなしで入力します。デフォルト設定は **8** です。値 **0** は、最小長が必須ではないことを示します。

ステップ 8 [パスワードの有効期限までの日数（Days Until Password Expiration）] を設定します。

ユーザのパスワードの有効期限までの日数を入力します。デフォルト設定は **0** で、パスワードは期限切れにならないことを示します。デフォルトから変更すると、[ユーザ（Users）] リストの [パスワードのライフタイム（Password Lifetime）] 列に、各ユーザのパスワードの残っている日数が表示されます。

ステップ 9 [パスワードの有効期限を事前に警告する日数（Days Before Password Expiration Warning）] を設定します。

パスワードが実際に期限切れになる何日前に、ユーザがパスワードを変更する必要があるという警告が表示されるかを入力します。デフォルト設定は **0** 日間です。

ステップ 10 ユーザの [オプション（Options）] を設定します。

- [ログイン時にパスワードのリセットを強制（Force Password Reset on Login）]：次回のログイン時にユーザにパスワード変更を強制します。
- [パスワードの強度のチェック（Check Password Strength）]：強力なパスワードを必須にします。強力なパスワードは8文字以上の英数字からなり、大文字と小文字を使用し、1つ以上の数字と1つ以上の特殊文字を使用する必要があります。辞書に記載されている単語や、同じ文字を連続して繰り返し使用することはできません。
- [ブラウザセッションタイムアウトの適用除外（Exempt from Browser Session Timeout）]：非アクティブ状態が原因で、ユーザのログイン セッションが終了しないようにします。Administrator ロールが割り当てられているユーザを除外することはできません。

ステップ 11 （7000 または 8000 シリーズ）CLI ユーザ ロール （55 ページ）の説明に従い、適切なレベルの [コマンドラインインターフェイスアクセス（Command-Line Interface Access）] を割り当てます。

（注） 7000 または 8000 シリーズ の場合とは異なり、Firepower Management Center 内部ユーザのシェルアクセスを有効にすることはできません（FMC では、外部ユーザのシェルアクセスを有効にできますが、システム セキュリティ上の理由から、有効にしないことを推奨します）。

ステップ 12 [ユーザロールの設定（User Role Configuration）] エリアで、ユーザ ロールを割り当てます。ユーザ ロールの詳細については、Web インターフェイス用のユーザ ロールのカスタマイズ （81 ページ）を参照してください。

外部ユーザについては、グループまたはリストのメンバーシップによってユーザ ロールが割り当てられている場合、最小限のアクセス権限を削除することはできません。ただし、追加の権限を割り当てることはできます。ユーザ ロールがデバイスで設定したデフォルトのユーザ ロールの場合は、ユーザ アカウントのロールを制限なしに変更できます。ユーザ ロールを変更すると、[ユーザ（Users）] タブの [認証方式（Authentication Method）] 列に、[外部-ローカル変更（External - Locally Modified）] のステータスが表示されます。

表示されるオプションは、デバイスが単一ドメイン展開かマルチドメイン展開（Firepower Management Center のみ）かによって異なります。

- 単一ドメイン：ユーザを割り当てるユーザ ロールをオンにします。
- マルチドメイン（Firepower Management Center のみ）：マルチドメイン展開では、管理者アクセス権限があるドメインでユーザ アカウントを作成できます。ユーザは各ドメインで異なる権限を持つことができます。先祖ドメインと子孫ドメインの両方でユーザ ロールを割り当てることができます。たとえば、あるユーザにグローバル ドメインでは読み取り専用権限を割り当て、子孫ドメインでは管理者権限を割り当てることができます。次の手順を参照してください。

  1. [ドメインの追加（Add Domain）] をクリックします。
  2. [ドメイン（Domain）] ドロップダウン リストからドメインを選択します。
  3. ユーザを割り当てるユーザ ロールをオンにします。
  4. [保存（save）] をクリックします。

ステップ 13 **[保存（Save）]** をクリックします。

CLI での内部ユーザの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	任意	FTD ASA FirePOWER NGIPSv	任意	Config

CLI を使用して、FTD、ASA FirePOWER、および NGIPSv デバイスで内部ユーザを作成します。これらのデバイスには Web インターフェイスがないため、内部（および外部）ユーザは管理のために CLI にのみアクセスできます。

ステップ 1 設定権限を持つアカウントを使用してデバイス CLI にログインします。

admin ユーザ アカウントには必要な権限がありますが、設定権限を持つ任意のアカウントで作業できます。SSH セッションまたはコンソール ポートを使用できます。

特定の FTD モデルの場合、コンソール ポートで FXOS CLI に入ります。**connect ftd** を使用して FTD の CLI にアクセスします。

ステップ 2 ユーザ アカウントを作成します。

configure user add *username* {**basic** | **config**}

- *username*：ユーザ名を設定します。ユーザ名は、次のように Linux に対して有効である必要があります。
  - 英数字、ハイフン（-）、およびアンダースコア（_）が使用可で、最大 32 文字
  - すべて小文字
  - 最初の文字にハイフン（-）は使用不可、すべて数字は不可、ピリオド（.）、アットマーク（@）、またはスラッシュ（/）は使用不可
- **basic**：ユーザに基本的なアクセス権を付与します。このロールはユーザに設定コマンドの入力を許可しません。
- **config**：ユーザに設定アクセス権を付与します。このロールはユーザにすべてのコマンドへの完全な管理者権限を与えます。

例：

次の例では、johncrichton という名前の設定アクセス権を持つユーザ アカウントを追加します。パスワードは入力時に非表示となります。

```
> configure user add johncrichton config
Enter new password for user johncrichton: newpassword
Confirm new password for user johncrichton: newpassword
> show user
Login             UID   Auth Access  Enabled Reset    Exp Warn  Str Lock Max
admin            1000  Local Config  Enabled    No  Never  N/A  Dis   No N/A
johncrichton     1001  Local Config  Enabled    No  Never  N/A  Dis   No   5
```

（注） 自分のパスワードを **configure password** コマンドを使用して変更できることをユーザに伝えます。

ステップ 3 （任意） セキュリティ要件を満たすようにアカウントの性質を調整します。

アカウントのデフォルト動作を変更するには、次のコマンドを使用できます。

- **configure user aging** *username max_days warn_days*

  ユーザ パスワードの有効期限を設定します。パスワードの最大有効日数と、有効期限が近づいたことをユーザに通知する警告を期限切れとなる何日前に発行するかを指定します。どちらの値も 1 ~ 9999 ですが、警告までの日数は最大日数以内にする必要があります。アカウントを作成した場合、パスワードの有効期限はありません。

- **configure user forcereset** *username*

  次回ログイン時にユーザにパスワードを強制的に変更するよう要求します。

- **configure user maxfailedlogins** *username number*

  アカウントがロックされる前の連続したログイン失敗の最大回数を1~9999までで設定します。**configure user unlock** コマンドを使用してアカウントのロックを解除します。新しいアカウントのデフォルトは、5 回連続でのログインの失敗です。

- **configure user minpasswdlen** *username number*

  パスワードの最小長を 1 ~ 127 までで設定します。

- **configure user strengthcheck** *username* {**enable** | **disable**}

  パスワードの変更時にユーザに対してパスワード要件を満たすように要求する、パスワードの強度確認を有効または無効にします。ユーザパスワードの有効期限が切れた場合、または **configure user forcereset** コマンドを使用した場合は、ユーザが次にログインしたときにこの要件が自動的に有効になります。

ステップ 4 必要に応じてユーザ アカウントを管理します。

ユーザをアカウントからロックアウトしたり、アカウントを削除するか、またはその他の問題を修正したりしなければならない可能性があります。システムのユーザ アカウントを管理するには、次のコマンドを使用します。

- **configure user access** *username* {**basic** | **config**}

  ユーザ アカウントの権限を変更します。

- **configure user delete** *username*

  指定したアカウントを削除します。

- **configure user disable** *username*

  指定したアカウントを削除せずに無効にします。ユーザは、アカウントを有効にするまでログインできません。

- **configure user enable** *username*

  指定したアカウントを有効にします。

- **configure user password** *username*

  指定したユーザのパスワードを変更します。ユーザは通常、**configure password** コマンドを使用して自分のパスワードを変更する必要があります。

- **configure user unlock** *username*

  ログイン試行の最大連続失敗回数の超過が原因でロックされたユーザ アカウントをロック解除します。

外部認証の設定

外部認証を有効にするには、1 つ以上の外部認証オブジェクトを追加する必要があります。

外部認証について

Firepowerシステムの管理ユーザの外部認証を有効にすると、デバイスにより外部認証オブジェクトで指定された LDAP または RADIUS サーバを使用してユーザ クレデンシャルが検証されます。

外部認証オブジェクトは、Firepower Management Center、7000 および 8000 シリーズ、 および FTD デバイスで使用できます。さまざまなアプライアンス/デバイス タイプで同じオブジェクトを共有することも、別々のオブジェクトを作成することもできます。

FMC では、**[システム（System）] > [ユーザ（Users）] > [外部認証（External Authentication）]** タブで外部認証オブジェクトを直接有効にします。この設定は、FMC の使用にのみ影響し、管理対象デバイスを使用する場合には、このタブで有効にする必要はありません。 7000 および 8000 シリーズ および FTD のデバイスでは、デバイスに展開するプラットフォーム設定で外部認証オブジェクトを有効にする必要があります。

外部認証オブジェクト内の CLI/シェル ユーザから Web インターフェイスのユーザが個別に定義されます。 7000 または 8000 シリーズ および Firepower Management Center の RADIUS の CLI/シェル ユーザの場合、外部認証オブジェクト内に RADIUS ユーザ名のリストを事前に設定しておく必要があります。FTD では、RADIUS サーバのユーザを定義する（Service-Type 属性を使用）か、または他のプラットフォームの場合と同じように外部認証オブジェクト内にユーザ リストを事前に定義できます。LDAP では、LDAP サーバの CLI ユーザと一致するようにフィルタを指定できます。

CAC 認証用にも設定されている CLI/シェル アクセスの LDAP オブジェクトは使用できません。

（注） Linux シェルへのアクセス権があるユーザはルート権限を取得できるため、セキュリティ上のリスクが生じる可能性があります。次のことを実行してください。

- Linux シェルへのアクセス権を持つユーザのリストを制限します。
- Linux シェル ユーザを作成しないでください。

Firepower Management Center および 7000 および 8000 シリーズ の外部認証

Webインターフェイスアクセス用に複数の外部認証オブジェクトを設定できます。たとえば、5 つの外部認証オブジェクトがある場合、いずれかのオブジェクトのユーザを Web インターフェイスにアクセスするために認証できます。

CLI またはシェル アクセスに使用できる外部認証オブジェクトは 1 つのみです。複数の外部認証オブジェクトが有効になっている場合、ユーザはリスト内の最初のオブジェクトのみを使用して認証できます。7000 または 8000 シリーズ デバイス上の外部 CLI ユーザは常に Config 権限を持っています。他のユーザ ロールはサポートされません。

Firepower Threat Defense の外部認証

FTD では、1 つの外部認証オブジェクトのみをアクティブ化できます。

FTD SSH アクセスでは、外部認証オブジェクト内のフィールドのサブセットのみが使用されます。その他のフィールドに値を入力しても無視されます。このオブジェクトを他のデバイス タイプにも使用する場合は、それらのフィールドが使用されます。

LDAP ユーザには常に Config 権限があります。RADIUS ユーザは、Config ユーザまたは Basic ユーザとして定義できます。

LDAP について

Lightweight Directory Access Protocol（LDAP）により、ユーザ クレデンシャルなどのオブジェクトをまとめるためのディレクトリをネットワーク上の一元化されたロケーションにセットアップできます。こうすると、複数のアプリケーションがこれらのクレデンシャルと、クレデンシャルの記述に使用される情報にアクセスできます。ユーザのクレデンシャルを変更する必要がある場合も、常に 1 箇所でクレデンシャルを変更できます。

RADIUS について

Remote Authentication Dial In User Service（RADIUS）は、ネットワーク リソースへのユーザ アクセスの認証、認可、およびアカウンティングに使用される認証プロトコルです。RFC 2865 に準拠するすべての RADIUS サーバで、認証オブジェクトを作成できます。

FirePOWER デバイスは、SecurID トークンの使用をサポートします。SecurID を使用したサーバによる認証を設定した場合、そのサーバに対して認証されるユーザは、自身の SecurID PIN の末尾に SecurID トークンを追加したものをログイン時にパスワードとして使用します。SecurID をサポートするために、FirePOWER デバイスで追加の設定を行う必要はありません。

LDAP 外部認証オブジェクトの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	任意	FTD 7000 および 8000 シリーズ FMC	任意	管理者

デバイス管理用に外部ユーザをサポートするために、LDAP サーバを追加します。

FTD では、CLI アクセスには一部のフィールドのみが使用されます。どのフィールドが使用されるかについては、SSH の外部認証の設定 （1361 ページ）を参照してください。

マルチドメイン展開では、外部認証オブジェクトは作成されたドメインでのみ使用できます。

始める前に

- デバイス上にドメイン名ルックアップの DNS サーバを指定する必要があります。この手順で LDAP サーバのホスト名ではなく IP アドレスを指定した場合、ホスト名に含めることができる認証用の URI を LDAP サーバが返す場合があります。ホスト名を解決するには DNS ルックアップが必要です。DNS サーバを追加するには管理インターフェイスの設定 （1273 ページ）を参照してください。
- CAC 認証に使用する LDAP 認証オブジェクトを設定する場合は、コンピュータに挿入されている CAC を取り外さないでください。ユーザ証明書を有効にした後では、CAC が常に挿入された状態にしておく必要があります。

ステップ 1 **[System]** > **[Users]**を選択します。

ステップ 2 [外部認証（External Authentication）] タブをクリックします。

ステップ 3 [外部認証オブジェクトの追加（Add External Authentication Object）] をクリックします。

ステップ 4 [認証方式（Authentication Method）] を [LDAP] に設定します。

ステップ 5 （任意） CAC 認証および認可にこの認証オブジェクトを使用する予定の場合は、[CAC] チェックボックスをオンにします。

CAC 認証および認可を完全に設定するには、LDAP を使用した共通アクセス カード認証の設定 （80 ページ）の手順にも従う必要があります。このオブジェクトは、CLI ユーザには使用できません。

ステップ 6 [名前（Name）] とオプションの [説明（Description）] を入力します。

ステップ 7 ドロップダウン リストから [サーバタイプ（Server Type）] を選択します。

ヒント [デフォルトの設定（Set Defaults）] をクリックした場合は、デバイスにより [ユーザ名テンプレート（User Name Template）]、[UIアクセス属性（UI Access Attribute）]、[シェルアクセス属性（Shell Access Attribute）]、[グループメンバー属性（Group Member Attribute）]、および [グループメンバーURL属性（Group Member URL Attribute）] フィールドに、サーバ タイプのデフォルト値が入力されます。

ステップ 8 [プライマリサーバ（Primary Server）] の場合は、[ホスト名/IPアドレス（Host Name/IP Address）] を入力します。

証明書を使用し、TLS または SSL 経由で接続する場合は、証明書のホスト名が、このフィールドに入力するホスト名と一致している必要がりあります。また、暗号化接続では IPv6 アドレスはサポートされていません。

ステップ 9 （任意） [ポート（Port）] をデフォルトから変更します。

ステップ 10 （任意） [バックアップサーバ（Backup Server）] パラメータを入力します。

ステップ 11 [LDAP固有のパラメータ（LDAP-Specific Parameters）] を入力します。

a) ユーザがアクセスする LDAP ディレクトリの [ベースDN（Base DN）] を入力します。たとえば、Example 社のセキュリティ（Security）部門の名前を認証するには、`ou=security,dc=example,dc=com` と入力します。または、[DNの取得（Fetch DNs）] をクリックし、ドロップダウン リストから適切なベース識別名を選択します。

b) （任意） [基本フィルタ（Base Filter）] を入力します。たとえば、ディレクトリ ツリー内のユーザ オブジェクトに `physicalDeliveryOfficeName` 属性が設定されており、New York 支店のユーザに対しこの属性に値 `NewYork` が設定されている場合、New York 支店のユーザだけを取得するには、`(physicalDeliveryOfficeName=NewYork)` と入力します。

c) LDAP サーバを参照するために十分なクレデンシャルを持つユーザの [ユーザ名（User Name）] を入力します。たとえば、ユーザ オブジェクトに `uid` 属性が含まれている OpenLDAP サーバに接続し、Example 社のセキュリティ（Security）部門の管理者のオブジェクトの `uid` に値 `NetworkAdmin` が設定されている場合は、`uid=NetworkAdmin,ou=security,dc=example,dc=com` と入力します。

d) [パスワード（Password）] および [パスワードの確認（Confirm Password）] フィールドにユーザ パスワードを入力します。

e) （任意） [詳細オプションを表示（Show Advanced Options）] をクリックして、次の詳細オプションを設定します。

- [Encryption]：[None]、[TLS]、または [SSL] をクリックします。

  ポートを指定した後で暗号化方式を変更すると、ポートがその方式のデフォルト値にリセットされます。[なし（None）] または [TLS] の場合、ポートはデフォルト値の 389 にリセットされます。[SSL] 暗号化を選択した場合、ポートは 636 にリセットされます。

- [SSL証明書アップロードパス（SSL Certificate Upload Path）]：SSL または TLS 暗号化の場合は、[ファイルの選択（Choose File）] をクリックして証明書を選択する必要があります。

  以前にアップロードした証明書を置き換えるには、新しい証明書をアップロードし、設定をデバイスに再展開して、新しい証明書を上書きコピーします。

（注） TLS 暗号化には、すべてのプラットフォームで証明書が必要です。SSL の場合、FTD も証明書を必要とします。他のプラットフォームの場合、SSL は証明書を必要としません。ただし、中間者攻撃を防ぐため、SSL 証明書を常にアップロードしておくことをお勧めします。

- [ユーザ名テンプレート（User Name Template）]：[UIアクセス属性（UI Access Attribute）] に対応するテンプレートを入力します。たとえば、UI アクセス属性が `uid` である OpenLDAP サーバに接続し、Example 社のセキュリティ（Security）部門で働くすべてのユーザを認証するには、[ユーザ名テンプレート（User Name Template）] フィールドに `uid=%s,ou=security,dc=example,dc=com` と入力します。Microsoft Active Directory Server の場合は `%s@security.example.com` と入力します。

  CAC 認証では、このフィールドは必須です。

- [タイムアウト（Timeout）]：バックアップ接続にロールオーバーするまでの秒数を入力します。デフォルトは 30 です。

ステップ 12 （任意）[属性照合（Attribute Matching）] を設定して、属性に基づいてユーザを取得します。

- [UIアクセス属性（UI Access Attribute）] を入力するか、[属性の取得（Fetch Attrs）] をクリックして利用可能な属性のリストを取得します。たとえば Microsoft Active Directory Server では、Active Directory Server ユーザ オブジェクトに `uid` 属性がないため、[UI アクセス属性（UI Access Attribute）] を使用してユーザを取得することがあります。代わりに [UI アクセス属性（UI Access Attribute）] フィールドに `userPrincipalName` と入力して、`userPrincipalName` 属性を検索できます。

  CAC 認証では、このフィールドは必須です。

- ユーザ識別タイプ以外のシェル アクセス属性を使用する場合は、[シェルアクセス属性（Shell Access Attribute）] を設定します。たとえば、Microsoft Active Directory Server で、`sAMAccountName` シェル アクセス属性を使用して CLI/シェル アクセス ユーザを取得するには、`sAMAccountName` と入力します。

ステップ 13 （任意）[グループ制御アクセスロール（Group Controlled Access Roles）] を設定します。

グループ制御アクセス ロールを使用してユーザの権限を事前に設定していない場合、ユーザには、外部認証ポリシーでデフォルトで付与される権限だけが与えられています。

a) （任意）ユーザ ロールに対応するフィールドに、これらのロールに割り当てる必要があるユーザを含む LDAP グループの識別名を入力します。

   参照するグループはすべて LDAP サーバに存在している必要があります。スタティック LDAP グループまたはダイナミック LDAP グループを参照できます。スタティック LDAP グループとは、特定のユーザを指し示すグループ オブジェクト属性によってメンバーシップが決定されるグループであり、ダイナミック LDAP グループとは、ユーザ オブジェクト属性に基づいてグループ ユーザを取得する LDAP 検索を作成することでメンバーシップが決定されるグループです。ロールのグループ アクセス権は、グループのメンバーであるユーザにのみ影響します。

   ダイナミック グループを使用する場合、LDAP クエリは、LDAP サーバで設定されているとおりに使用されます。この理由から、検索構文エラーが原因で無限ループが発生することを防ぐため、FirePOWER デバイスでは検索の再帰回数が 4 回に制限されています。

例：

Example 社の情報テクノロジー（Information Technology）部門の名前を認証するには、[管理者（Administrator）] フィールドに次のように入力します。

```
cn=itgroup,ou=groups, dc=example,dc=com
```

b) 指定したグループのいずれにも属していないユーザの [デフォルトユーザロール（Default User Role）] を選択します。

c) スタティック グループを使用する場合は、[グループ メンバー属性（Group Member Attribute）] を入力します。

例：

デフォルトの Security Analyst アクセスのためのスタティック グループのメンバーシップを示すために `member` 属性を使用する場合は、`member` と入力します。

d) ダイナミック グループを使用する場合は、[グループ メンバー URL 属性（Group Member URL Attribute）] を入力します。

例：

デフォルトの管理者アクセスに対して指定したダイナミック グループのメンバーを取得する LDAP 検索が `memberURL` 属性に含まれている場合は、`memberURL` と入力します。

ユーザ ロールを変更する場合は、変更した外部認証オブジェクトを保存/展開し、[ユーザ（Users）] 画面からユーザを削除する必要があります。次回のログイン時に、ユーザが自動的に再度追加されます。

ステップ 14 （任意） CLI/シェル ユーザを許可するように [シェルアクセスフィルタ（Shell Access Filter）] を設定します。

CLI/シェル アクセスの LDAP 認証を防止するには、このフィールドを空白にします。CLI/シェル ユーザを指定するには、次のいずれかの方法を選択します。

- 認証設定の設定時に指定したものと同じフィルタを使用するには、[基本フィルタと同じ（Same as Base Filter）] を選択します。
- 属性値に基づいて管理ユーザ項目を取得するには、属性名、比較演算子、およびフィルタとして使用する属性値を、カッコで囲んで入力します。たとえば、すべてのネットワーク管理者の `manager` 属性に属性値 `shell` が設定されている場合は、基本フィルタ `(manager=shell)` を設定できます。

ユーザ名は、次のように Linux に対して有効である必要があります。

- 英数字、ハイフン（-）、およびアンダースコア（_）が使用可で、最大 32 文字
- すべて小文字
- 最初の文字にハイフン（-）は使用不可、すべて数字は不可、ピリオド（.）、アットマーク（@）、またはスラッシュ（/）は使用不可

（注） 7000 または 8000 シリーズ および Firepower Management Center では、[シェルアクセスフィルタ（Shell Access Filter）] に含まれているユーザと同じユーザ名を持つ内部ユーザを作成しないでください。唯一の内部 FMC ユーザは **admin** である必要があります。[シェルアクセスフィルタ（Shell Access Filter）] に **admin** ユーザを含めないでください。

FTD では、内部ユーザに同じユーザ名を以前に設定している場合、FTD は内部ユーザに対して最初にパスワードを確認し、失敗した場合は LDAP サーバを確認します。後から外部ユーザと同じ名前の内部ユーザを追加できないことに注意してください。既存の内部ユーザしかサポートされません。

ステップ 15 （任意） LDAP サーバへの接続をテストするには、[テスト（Test）] をクリックします。

テスト出力には、有効なユーザ名と無効なユーザ名が示されます。有効なユーザ名は一意のユーザ名であり、アンダースコア（_）、ピリオド（.）、ハイフン（-）、英数字を使用できます。UI のページ サイズ制限のため、ユーザ数が 1000 を超えているサーバへの接続をテストする場合、返されるユーザの数は 1000 であることに注意してください。テストが失敗した場合は、LDAP 認証接続のトラブルシューティング （88 ページ）を参照してください。

ステップ 16 （任意） [追加のテストパラメータ（Additional Test Parameters）] を入力して、認証できるようにするユーザのユーザ クレデンシャルをテストすることもできます。[ユーザ名（User Name）] `uid` と [パスワード（Password）] を入力してから、[テスト（Test）] をクリックします。

Microsoft Active Directory Server に接続して `uid` の代わりに UI アクセス属性を指定する場合は、ユーザ名としてこの属性の値を使用します。ユーザの完全修飾識別名も指定できます。

ヒント テスト ユーザの名前とパスワードを誤って入力すると、サーバ設定が正しい場合でもテストが失敗します。サーバ設定が正しいことを確認するには、最初に [Additional Test Parameters] フィールドにユーザ情報を入力せずに [Test] をクリックします。正常に完了した場合は、テストする特定ユーザのユーザ名とパスワードを指定します。

例：

Example 社の `JSmith` ユーザ クレデンシャルを取得できるかどうかをテストするには、`JSmith` と正しいパスワードを入力します。

ステップ 17 [保存（Save）] をクリックします。

ステップ 18 このサーバの使用を有効にします。

- Firepower Management Center：Firepower Management Center でのユーザの外部認証の有効化 （78 ページ）
- FTD：SSH の外部認証の設定 （1361 ページ）
- 7000 および 8000 シリーズ：7000/8000 シリーズ デバイスの外部認証について （1342 ページ）

ステップ 19 LDAP サーバで後からユーザを追加または削除する場合は、ユーザ リストを更新し、管理対象デバイスのプラットフォーム設定を再展開する必要があります。Firepower Management Center では、この手順は必要ありません。

a) 各 LDAP サーバの横にある[Refresh] アイコン（）をクリックします。

ユーザ リストが変更された場合は、デバイスの設定変更を展開するように促すメッセージが表示されます。

b) 7000 および 8000 シリーズ デバイスの場合は、プラットフォーム設定を少し変更して、設定が古いとマークされるようにします。LDAP シェルユーザ リストの更新のために、7000 および 8000 シリーズ のプラットフォーム設定が自動的に古いとマークされることはありません。

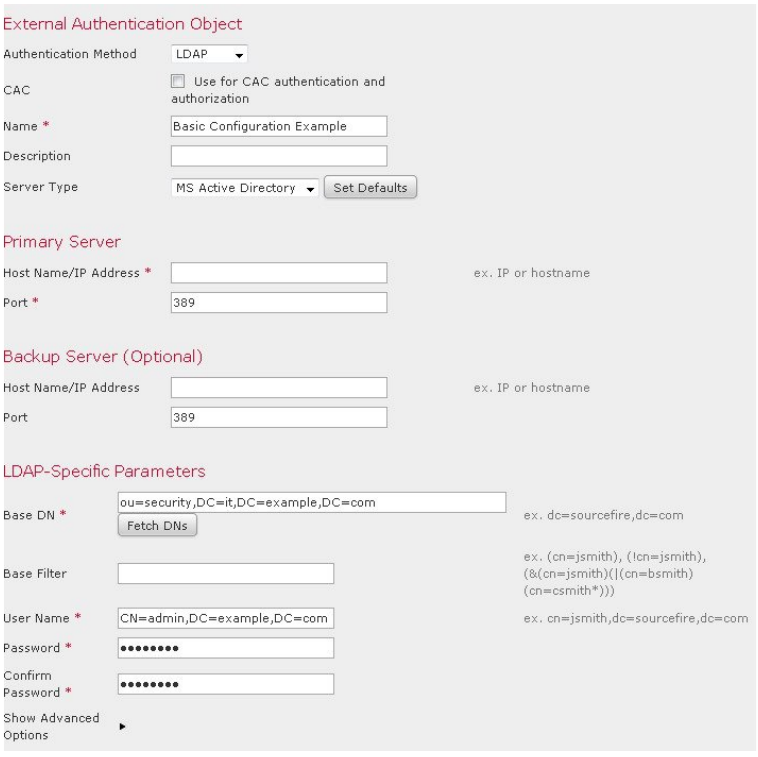
Firepower Threat Defense のプラットフォーム設定は自動的に古いとマークされるため、この回避策を実行する必要はありません。

c) 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

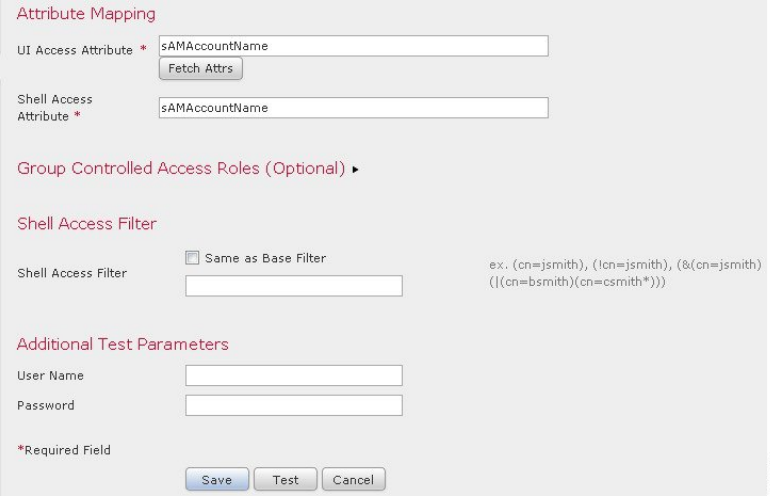
例

基本的な例

次の図は、Microsoft Active Directory Server の LDAP ログイン認証オブジェクトの基本設定を示します。この例の LDAP サーバの IP アドレスは 10.11.3.4 です。接続ではアクセスのためにポート 389 が使用されます。



この例では、Example 社の情報テクノロジー ドメインで、セキュリティ部門のベース識別名として `OU=security,DC=it,DC=example,DC=com` を使用した接続を示しています。



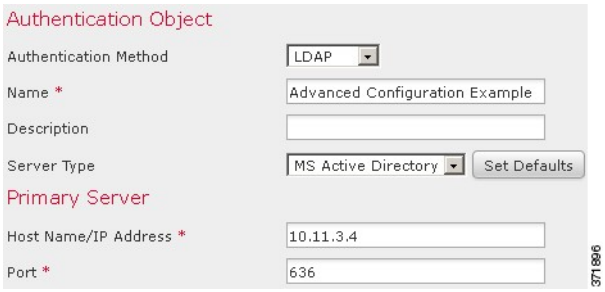
ただし、このサーバが Microsoft Active Directory Server であるため、ユーザ名の保存に `uid` 属性ではなく `sAMAccountName` 属性が使用されます。サーバのタイプとして MS Active Directory を選択し、[デフォルトの設定（Set Defaults）] をクリックすると、[UI アクセス属性（UI Access Attribute）] が `sAMAccountName` に設定されます。その結果、ユーザが Firepower システムへのログインを試行すると、Firepower システムは各オブジェクトの `sAMAccountName` 属性を検査し、一致するユーザ名を検索します。

また、[シェルアクセス属性（Shell Access Attribute）] が `sAMAccountName` の場合、ユーザがアプライアンスでシェル アカウントまたは CLI アカウントにログインすると、ディレクトリ内のすべてのオブジェクトの各 `sAMAccountName` 属性が検査され、一致が検索されます。

基本フィルタはこのサーバに適用されないため、Firepower システムはベース識別名により示されるディレクトリ内のすべてのオブジェクトの属性を検査することに注意してください。サーバへの接続は、デフォルトの期間（または LDAP サーバで設定されたタイムアウト期間）の経過後にタイムアウトします。

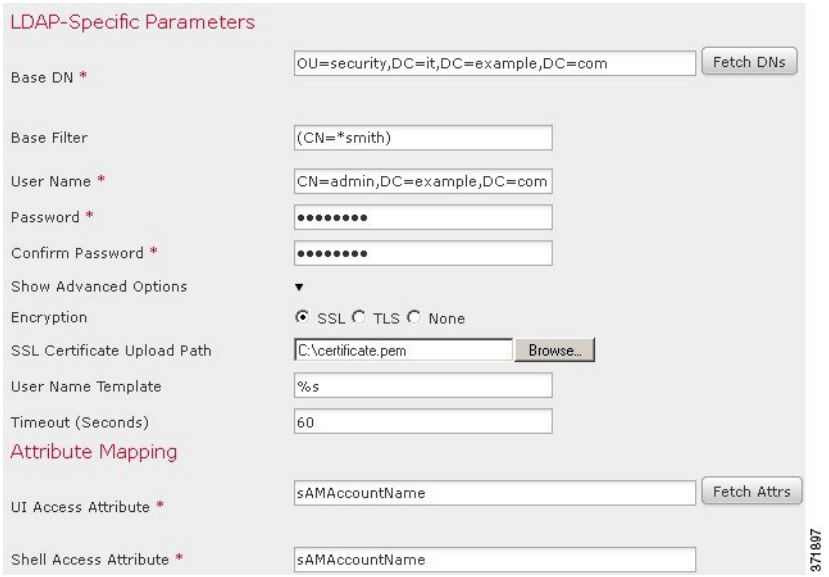
高度な例

次の例は、Microsoft Active Directory Server の LDAP ログイン認証オブジェクトの詳細設定を示します。この例の LDAP サーバの IP アドレスは 10.11.3.4 です。接続ではアクセスのためにポート 636 が使用されます。



この例では、Example 社の情報テクノロジー ドメインで、セキュリティ部門のベース識別名として `OU=security,DC=it,DC=example,DC=com` を使用した接続を示しています。

ただし、このサーバに基本フィルタ（`cn=*smith`）が設定されていることに注意してください。このフィルタは、サーバから取得するユーザを、一般名が `smith` で終わるユーザに限定します。

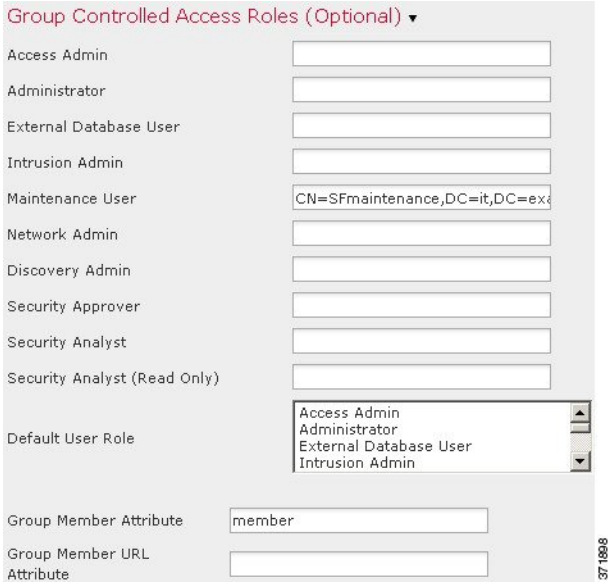


サーバへの接続が SSL を使用して暗号化され、`certificate.pem` という名前の証明書が接続に使用されます。また、[Timeout] の設定により、60 秒経過後にサーバへの接続がタイムアウトします。

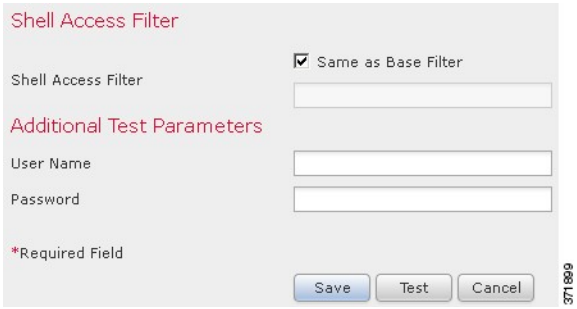
このサーバが Microsoft Active Directory Server であるため、ユーザ名の保存に `uid` 属性ではなく `sAMAccountName` 属性が使用されます。設定では、[UI アクセス属性（UI Access Attribute）] が `sAMAccountName` であることに注意してください。その結果、ユーザが Firepower システムへのログインを試行すると、Firepower システムは各オブジェクトの `sAMAccountName` 属性を検査し、一致するユーザ名を検索します。

また、[シェルアクセス属性（Shell Access Attribute）] が `sAMAccountName` の場合、ユーザがアプライアンスで CLI/シェルアカウントにログインすると、ディレクトリ内のすべてのオブジェクトの各 `sAMAccountName` 属性が検査され、一致が検索されます。

この例では、グループ設定も行われます。[メンテナンス ユーザ（Maintenance User）] ロールが、`member` グループ属性を持ち、ベース ドメイン名が `CN=SFmaintenance,=it,=example,=com` であるグループのすべてのメンバーに自動的に割り当てられます。



シェル アクセス フィルタは、基本フィルタと同一に設定されます。このため、同じユーザが Web インターフェイスを使用する場合と同様に、シェルまたは CLI を介してアプライアンスにアクセスできます。



RADIUS 外部認証オブジェクトの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	任意	FTD 7000 および 8000 シリーズ FMC	任意	管理者

デバイス管理用に外部ユーザをサポートするために、RADIUS サーバを追加します。

FTD では、CLI アクセスには一部のフィールドのみが使用されます。どのフィールドが使用されるかについては、SSH の外部認証の設定 （1361 ページ）を参照してください。

マルチドメイン展開では、外部認証オブジェクトは作成されたドメインでのみ使用できます。

ステップ 1 **[System]** > **[Users]**を選択します。

ステップ 2 [外部認証（External Authentication）] タブをクリックします。

ステップ 3 [外部認証オブジェクトの追加（Add External Authentication Object）] をクリックします。

ステップ 4 [認証方式（Authentication Method）] を [RADIUS] に設定します。

ステップ 5 [名前（Name）] とオプションの [説明（Description）] を入力します。

ステップ 6 [プライマリサーバ（Primary Server）] の場合は、[ホスト名/IPアドレス（Host Name/IP Address）] を入力します。

ステップ 7 （任意） [ポート（Port）] をデフォルトから変更します。

ステップ 8 [RADIUS秘密キー（RADIUS Secret Key）] を入力します。

ステップ 9 （任意） [バックアップサーバ（Backup Server）] パラメータを入力します。

ステップ 10 （任意） [RADIUS固有のパラメータ（RADIUS-Specific Parameters）] を入力します。

a) プライマリ サーバを再試行するまでの [タイムアウト（Timeout）] を秒単位で入力します。デフォルトは 30 です。

b) バックアップ サーバにロールオーバーするまでの [再試行（Retries）] を入力します。デフォルトは 3 です。

c) ユーザ ロールに対応するフィールドに、各ユーザの名前を入力するか、またはこれらのロールに割り当てる必要がある属性と値のペアを指定します。

ユーザ名と属性と値のペアは、カンマで区切ります。

例：

セキュリティ アナリストとする必要があるすべてのユーザの `User-Category` 属性の値が `Analyst` である場合、これらのユーザにそのロールを付与するには、[セキュリティアナリスト（Security Analyst）] フィールドに `User-Category=Analyst` と入力します。

例：

ユーザ `jsmith` と `jdoe` に管理者ロールを付与する場合は、[管理者（Administrator）] フィールドに `jsmith, jdoe` と入力します。

例：

`User-Category` の値が `Maintenance` であるすべてのユーザにメンテナンス ユーザ ロールを付与するには、[メンテナンスユーザ（Maintenance User）] フィールドに `User-Category=Maintenance` と入力します。

d) 指定したグループのいずれにも属していないユーザの [デフォルトユーザロール（Default User Role）] を選択します。

ユーザ ロールを変更する場合は、変更した外部認証オブジェクトを保存/展開し、[ユーザ（Users）] 画面からユーザを削除する必要があります。次回のログイン時に、ユーザが自動的に再度追加されます。

ステップ 11 （任意） [カスタムRADIUS属性を定義する（Define Custom RADIUS Attributes）]。

RADIUS サーバが、/etc/radiusclient/ 内の dictionary ファイルに含まれていない属性の値を返し、これらの属性を使用してユーザにユーザ ロールを設定する予定の場合は、これらの属性を定義する必要があります。RADIUS サーバでユーザ プロファイルを調べると、ユーザについて返される属性を見つけることができます。

a) [属性名（Attribute Name）] を入力します。

属性を定義する場合は、英数字からなる属性名を指定します。属性名の中の単語を区切るには、スペースではなくダッシュを使用することに注意してください。

b) [属性ID（Attribute ID）] を整数で入力します。

属性 ID は整数にする必要があり、etc/radiusclient/dictionary ファイルの既存の属性 ID と競合していてはなりません。

c) ドロップダウン リストから [属性タイプ（Attribute Type）] を選択します。

属性のタイプ（文字列、IP アドレス、整数、または日付）も指定します。

d) [追加（Add）] をクリックして、カスタム属性を追加します。

RADIUS 認証オブジェクトの作成時に、そのオブジェクトの新しいディクショナリ ファイルがデバイスの /var/sf/userauth ディレクトリに作成されます。追加したすべてのカスタム属性は、ディクショナリ ファイルに追加されます。

例：

シスコルータが接続しているネットワーク上でRADIUSサーバが使用される場合に、Ascend-Assign-IP-Pool 属性を使用して、特定のIPアドレスプールからログインするすべてのユーザに特定のロールを付与するとします。Ascend-Assign-IP-Pool は、ユーザがログインできるアドレス プールを定義する整数属性であり、割り当てられる IP アドレス プールの番号を示す整数が指定されます。

そのカスタム属性を宣言するには、属性名が Ascend-IP-Pool-Definition、属性 ID が 218、属性タイプが integer のカスタム属性を作成します。

次に、Ascend-IP-Pool-Definition 属性値が 2 のすべてのユーザに対し、読み取り専用の Security Analyst 権限を付与するには、Ascend-Assign-IP-Pool=2 を [セキュリティ アナリスト（読み取り専用）（Security Analyst (Read Only)）] フィールドに入力します。

ステップ 12 （任意）（7000 または 8000 シリーズ および Firepower Management Center）[シェルアクセスフィルタ（Shell Access Filter）] エリアの [管理者シェルアクセスユーザリスト（Administrator Shell Access User List）] フィールドに、CLI/シェルへのアクセス権を付与する必要があるユーザ名をカンマで区切って入力します。

これらのユーザ名が RADIUS サーバのユーザ名と一致していることを確認します。名前は、次のように Linux に対して有効である必要があります。

- 英数字、ハイフン（-）、およびアンダースコア（_）が使用可で、最大 32 文字
- すべて小文字
- 最初の文字にハイフン（-）は使用不可、すべて数字は不可、ピリオド（.）、アットマーク（@）、またはスラッシュ（/）は使用不可

FTD では、この方法を必要に応じて使用して CLI ユーザを定義するか、または各ユーザに対して Service-Type 属性を設定することで RADIUS サーバの CLI ユーザを定義できます。Service-Type 属性の詳細については、SSH の外部認証の設定（1361 ページ）を参照してください。FTD で [シェルアクセスフィルタ（Shell Access Filter）] メソッドを使用すると、FTD およびその他のプラットフォーム タイプで同一の外部認証オブジェクトを使用できます。RADIUS 定義ユーザを使用する場合は、[シェル アクセス フィルタ（Shell Access Filter）] を空のままにする必要があります。

FTD に対して Service-Type 属性メソッドを使用しているときに 、FTD、7000 または 8000 シリーズ、 および FMC に同じ RADIUS サーバを使用するには、同じ RADIUS サーバを識別する外部認証オブジェクトを 2 つ作成します。一方のオブジェクトには事前に定義した [シェルアクセスフィルタ（Shell Access Filter）] ユーザを含め（FMC と 7000 または 8000 シリーズ で使用）、もう一方のオブジェクトの [シェルアクセスフィルタ（Shell Access Filter）] は空のままにします（FTD で使用）。

このフィールドを空のままにするのは、7000 または 8000 シリーズ および Firepower Management Center のユーザに対して CLI/シェル アクセスの RADIUS 認証を防止するためです。

（注） 7000 または 8000 シリーズ および Firepower Management Center では、[シェルアクセスフィルタ（Shell Access Filter）] に含まれているユーザと同じユーザ名を持つ内部ユーザを削除します。Firepower Management Center の場合、内部 CLI/シェル ユーザのみが **admin** です。そのため、**admin** 外部ユーザを作成しないでください。

FTD では、内部ユーザに同じユーザ名を以前に設定している場合、FTD は内部ユーザに対して最初にパスワードを確認し、失敗した場合は RADIUS サーバを確認します。後から外部ユーザと同じ名前の内部ユーザを追加できないことに注意してください。既存の内部ユーザしかサポートされません。

ステップ 13 （任意） RADIUS サーバへの FMC 接続をテストするには、[テスト（Test）] をクリックします。

この機能は、RADIUS サーバへの FMC 接続のみをテストできます。管理対象デバイスの RADIUS サーバへの接続をテストする機能はありません。

ステップ 14 （任意） [追加のテストパラメータ（Additional Test Parameters）] を入力して、認証できるようにするユーザのユーザ クレデンシャルをテストすることもできます。[ユーザ名（User Name）] と [パスワード（Password）] を入力してから、[テスト（Test）] をクリックします。

ヒント テスト ユーザの名前とパスワードを誤って入力すると、サーバ設定が正しい場合でもテストが失敗します。サーバ設定が正しいことを確認するには、最初に [Additional Test Parameters] フィールドにユーザ情報を入力せずに [Test] をクリックします。正常に完了した場合は、テストする特定ユーザのユーザ名とパスワードを指定します。

例：

Example 社の `JSmith` ユーザ クレデンシャルを取得できるかどうかをテストするには、`JSmith` と正しいパスワードを入力します。

ステップ 15 [保存（Save）] をクリックします。

ステップ 16 このサーバの使用を有効にします。

- Firepower Management Center：Firepower Management Center でのユーザの外部認証の有効化 （78 ページ）

- FTD：SSH の外部認証の設定 （1361 ページ）
- 7000 および 8000 シリーズ：7000/8000 シリーズ デバイスの外部認証について （1342 ページ）

例

単純なユーザ ロールの割り当て

次の図は、IP アドレスが 10.10.10.98 で FreeRADIUS が稼働しているサーバのサンプル RADIUS ログイン認証オブジェクトを示します。接続ではアクセスのためにポート 1812 が使用されること、および不使用期間が 30 秒を経過するとサーバ接続がタイムアウトになり、バックアップ認証サーバへの接続試行前に、サーバ接続が 3 回再試行されることに注意してください。

次の例は、RADIUS ユーザ ロール設定の重要な特徴を示します。

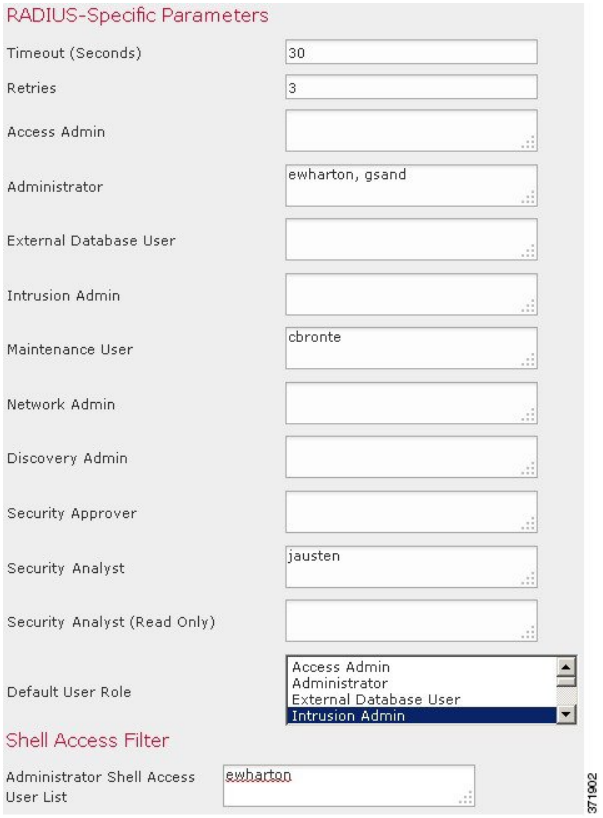
ユーザ `ewharton` および `gsand` には、Web インターフェイスの管理アクセスが付与されます。

ユーザ `cbronte` には、Web インターフェイスのメンテナンス ユーザ アクセスが付与されます。

ユーザ `jausten` には、Web インターフェイスのセキュリティ アナリスト アクセスが付与されます。

ユーザ `ewharton` は、CLI/シェル アカウントを使用してデバイスにログインできます。

次の図に、この例のロール設定を示します。

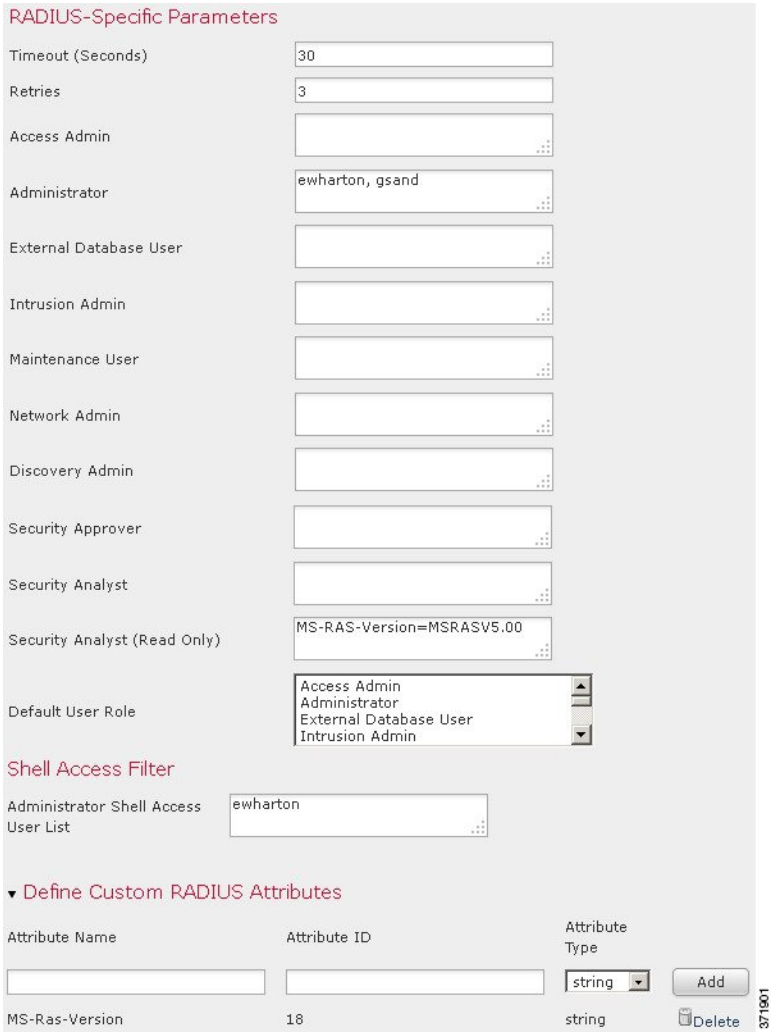


属性と値のペアに一致するユーザのロール

属性と値のペアを使用して、特定のユーザ ロールが付与される必要があるユーザを示すこともできます。使用する属性がカスタム属性の場合、そのカスタム属性を定義する必要があります。

次の図は、前述の例と同じ FreeRADIUS サーバのサンプル RADIUS ログイン認証オブジェクトでのロール設定とカスタム属性の定義を示します。

ただしこの例では、Microsoft リモート アクセス サーバが使用されているため、1 つ以上のユーザの `MS-RAS-Version` カスタム属性が返されます。`MS-RAS-Version` カスタム属性は文字列であることに注意してください。この例では、Microsoft v. 5.00 リモート アクセス サーバ経由で RADIUS にログインするすべてのユーザに対し、[セキュリティ アナリスト（読み取り専用）（Security Analyst (Read Only)）] ロールが付与される必要があります。このため、属性と値のペア `MS-RAS-Version=MSRASV5.00` を [セキュリティ アナリスト（読み取り専用）（Security Analyst (Read Only)）] フィールドに入力します。



Firepower Management Center でのユーザの外部認証の有効化

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	任意	FMC	任意	Admin

管理ユーザの外部認証を有効にすると、Firepower Management Center により外部認証オブジェクトで指定された LDAP または RADIUS サーバを使用してユーザ クレデンシャルが検証されます。

始める前に

LDAP 外部認証オブジェクトの追加 （64 ページ）およびRADIUS 外部認証オブジェクトの追加 （72 ページ）に従って 1 つまたは複数の外部認証オブジェクトを追加します。

ステップ 1 **[System]** > **[Users]**を選択します。

ステップ 2 [外部認証（External Authentication）] タブをクリックします。

ステップ 3 外部 Web インターフェイスのユーザにデフォルトのユーザ ロールを設定します。

ロールがないユーザは、アクションを実行できません。外部認証オブジェクトで定義されたユーザ ロールは、このデフォルトのユーザ ロールをオーバーライドします。

a) [デフォルトのユーザ ロール（Default User Roles）] の値をクリックします（デフォルトでは何も選択されていません）。

a) [デフォルトのユーザロール設定（Default User Role Configuration）] ダイアログ ボックスで、使用するロールをオンにします。

b) [保存（Save）] をクリックします。

ステップ 4 使用する外部認証オブジェクトそれぞれの横にあるスライダ（  ）をクリックします。複数のオブジェクトを有効にすると、ユーザは指定された順序でサーバと照合されます。サーバの順序を変更する場合は、次の手順を参照してください。

シェル認証を有効にする場合は、[シェルアクセスフィルタ（Shell Access Filter）] を含む外部認証オブジェクトを有効にする必要があります。また、CLI/シェル アクセスのユーザは、認証オブジェクトがリストの順序で最も高いサーバに対してのみ認証できます。

ステップ 5 （任意）認証要求が行われたときに認証サーバがアクセスされる順序を、サーバをドラッグアンドドロップして変更できます。

ステップ 6 外部ユーザに CLI/シェル アクセスを許可する場合は、**[シェル認証（Shell Authentication）]** > **[有効（Enabled）]** を選択します。

1 番目の外部認証オブジェクト名は、CLI/シェル アクセスに使用されるのは 1 番目のオブジェクトだけであることを示すため、[有効（Enabled）] オプションの横に表示されます。

ステップ 7 [Save and Apply] をクリックします。

管理対象デバイスのユーザに対する外部認証の有効化

デバイスのプラットフォーム設定で外部認証を有効にして、管理対象デバイスに設定を展開します。使用している管理対象デバイス タイプに応じて、次の手順を参照してください。

- Firepower Threat Defense：SSH の外部認証の設定 （1361 ページ）
- 7000 および 8000 シリーズ：7000/8000 シリーズ デバイスの外部認証について （1342 ページ）

LDAP を使用した共通アクセス カード認証の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	任意	FMC 7000 および 8000 シリーズ	任意	管理者 ネットワーク管理者

組織で共通アクセス カード（CAC）を使用している場合は、Web インターフェイスにログインしている FMC ユーザまたは 7000 および 8000 シリーズ ユーザを認証するように LDAP 認証を設定できます。CAC 認証により、ユーザは、デバイスに個別のユーザ名とパスワードを指定せずに直接ログインすることができます。

CAC 認証ユーザは、Electronic Data Interchange Personal Identifier（EDIPI）番号により識別されます。

非アクティブ状態が 24 時間続くと、デバイスにより CAC 認証ユーザが [ユーザ（Users）] タブから削除されます。その後のログインのたびにユーザが再度追加されますが、ユーザ ロールに対する手動の変更は再設定する必要があります。

始める前に

CAC 設定プロセスの一部としてユーザ証明書を有効にするには、ブラウザに有効なユーザ証明書（この場合は CAC を介してユーザのブラウザに渡される証明書）が存在している必要があります。CAC 認証および認可の設定後に、ネットワーク上のユーザはブラウズ セッション期間にわたって CAC 接続を維持する必要があります。セッション中に CAC を削除または交換すると、Web ブラウザでセッションが終了し、システムにより Web インターフェイスから強制的にログアウトされます。

ステップ 1 組織の指示に従い CAC を挿入します。

ステップ 2 ブラウザで **https://***ipaddress_or_hostname/* に移動します。ここで、*ipaddress* または *hostname* は使用しているデバイスに対応します。

ステップ 3 プロンプトが表示されたら、ステップ 1 で挿入した CAC に関連付けられた PIN を入力します。

ステップ 4 プロンプトが表示されたら、ドロップダウン リストから該当する証明書を選択します。

ステップ 5 ログイン ページで、[ユーザ名（Username）] フィールドと [パスワード（Password）] フィールドに、管理者権限を持つユーザとしてログインします。CAC クレデンシャルを使用してログインすることは、まだ**できません**。

ステップ 6 **[システム（System）] > [ユーザ（Users）] > [外部認証（External Authentication）]** を選択します。

ステップ 7 LDAP 外部認証オブジェクトの追加 （64 ページ）の手順に従い、CAC 専用の LDAP 認証オブジェクトを作成します。次の設定を行う必要があります。

- **[CAC]** チェックボックス。

- **[LDAP固有のパラメータ（LDAP-Specific Parameters）] > [詳細オプションを表示（Show Advanced Options）] > [ユーザ名テンプレート（User Name Template）]**。
- **[属性マッピング（Attribute Mapping）] > [UIアクセス属性（UI Access Attribute）]**。

ステップ 8 [保存（Save）] をクリックします。

ステップ 9 「Firepower Management Center でのユーザの外部認証の有効化 （78 ページ）」または「7000/8000 シリーズ デバイスへの外部認証の有効化 （1341 ページ）」の説明に従って、外部認証と CAC 認証を有効にします。

ステップ 10 **[System] > [Configuration]** を選択し、[HTTPS証明書（HTTPS Certificate）] をクリックします。

ステップ 11 HTTPS サーバ証明書をインポートし、必要に応じて HTTPS サーバ証明書のインポート （1259 ページ）で説明する手順に従います。

使用する予定の CAC で、HTTPS サーバ証明書とユーザ証明書が同じ認証局（CA）により発行される必要があります。

ステップ 12 [HTTPS ユーザ証明書設定（HTTPS User Certificate Settings）] の [ユーザ証明書を有効にする（Enable User Certificates）] を選択します。詳細については、有効な HTTPS クライアント証明書の強制 （1260 ページ）を参照してください。

ステップ 13 「CAC クレデンシャルを使用した Firepower Management Center へのログイン （34 ページ）」または「CAC クレデンシャルを使用した 7000 または 8000 シリーズ デバイスへのログイン （35 ページ）」に従い、デバイスにログインします。

Webインターフェイス用のユーザ ロールのカスタマイズ

各ユーザアカウントは、ユーザ ロールで定義する必要があります。このセクションでは、ユーザ ロールを管理する方法と、Web インターフェイス アクセス用のカスタム ユーザ ロールを設定する方法について説明します。ユーザ ロールの詳細については、Web インターフェイスのユーザ ロール （54 ページ）を参照してください。

（注） 管理対象デバイスの CLI/シェル ユーザ ロールは、設定ロールと基本ロールに制限されています。詳細については、「CLI ユーザ ロール （55 ページ）」を参照してください。

カスタム ユーザ ロールの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	任意	FMC 7000 & 8000 シリーズ	任意	管理者

カスタム ユーザ ロールには、メニューベースのアクセス許可とシステム アクセス許可の任意のセットを持たせることができます。また、完全にオリジナルのものを作成することや、定義済みのユーザ ロールまたは別のカスタム ユーザ ロールからコピーすることや、別のデバイスからインポートすることができます。

ステップ 1 **[System]** > **[Users]**を選択します。

ステップ 2 [User Roles] タブをクリックします。

ステップ 3 次のいずれかの方法で新しいユーザ ロールを追加します。

- [ユーザ ロールの作成（Create User Role）] をクリックします。
- コピーするユーザ ロールの横にある[Copy] アイコン（  ）をクリックします。
- 別のデバイスからカスタム ユーザ ロールをインポートします。
  1. 古いデバイスで、[Export] アイコン（  ）をクリックしてロールを PC に保存します。
  2. 新しいデバイスで、**[システム（System）]** > **[ツール（Tools）]** > **[インポート/エクスポート（Import/Export）]** を選択します。
  3. [パッケージのアップロード（Upload Package）] をクリックし、指示に従って保存したユーザ ロールを新しいデバイスにインポートします。

ステップ 4 新しいユーザ ロールの [名前（Name）] を入力します。ユーザ ロール名では、大文字と小文字が区別されます。

ステップ 5 （任意） [説明（Description）] を追加します。

ステップ 6 新しいロールの [メニューベースのアクセス許可（Menu-Based Permissions）] を選択します。

アクセス許可を選択すると、その下位にあるアクセス許可もすべて選択され、複数値を持つアクセス許可では最初の値が使用されます。上位のアクセス許可をクリアすると、下位のアクセス許可もすべてクリアされます。アクセス許可を選択しても、下位のアクセス許可を選択しない場合、アクセス許可がイタリックのテキストで表示されます。

カスタム ロールのベースとして使用する事前定義ユーザ ロールをコピーすると、その事前定義ロールに関連付けられているアクセス許可が事前選択されます。

カスタム ユーザ ロールに制限付き検索を適用できます。これらの検索では、[分析（Analysis）] メニューの下にあるテーブルやページでユーザが確認できるデータが制限されます。制限付き検索を設定するには、

最初に、プライベートの保存済み検索を作成し、該当するメニュー ベースのアクセス許可の下で [制限付き検索（Restrictive Search）] ドロップダウン メニューからその検索を選択します。

ステップ 7 （任意）新しいロールのデータベースアクセス権限を設定するには、[外部データベースアクセス（External Database Access）] チェックボックスをオンにします。

このオプションにより、JDBC SSL 接続に対応しているアプリケーションを用いて、データベースに対して読み取り専用アクセスが可能になります。デバイスの認証を行うサードパーティのアプリケーションについては、システム設定内でデータベース アクセスを有効にする必要があります。

ステップ 8 （任意）新しいユーザ ロールのエスカレーション権限を設定するには、ユーザ ロール エスカレーションの有効化 （84 ページ）を参照してください。

ステップ 9 [保存（Save）] をクリックします。

例

アクセス コントロール関連機能のカスタム ユーザ ロールを作成して、ユーザのアクセス コントロールおよび関連付けられたポリシーの表示、変更権限の有無を指定できます。

次の表に、作成可能なカスタム ロールと例として挙げたロールでそれぞれ与えられるユーザ権限を示します。表にはそれぞれのカスタム ロールに必要な権限が記載されています。この例では、ポリシー承認者はアクセス コントロール ポリシーと侵入ポリシーの表示が可能です（変更はできません）。また、ポリシー承認者は設定の変更をデバイスに展開することもできます。

表 *1*: アクセス制御のカスタム ロールの例

カスタム ロールの権限	例：アクセスコントロール編集者	例：侵入およびネットワーク分析編集者	例：ポリシー承認者
アクセス制御	あり	なし	あり
アクセス コントロール ポリシー	あり	なし	あり
アクセス コントロール ポリシーの変更	あり	なし	なし
侵入ポリシー	なし	あり	あり
侵入ポリシーの変更	なし	あり	なし
設定をデバイスに展開	なし	なし	あり

ユーザ ロールの非アクティブ化

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	任意	FMC 7000 & 8000 シリーズ	任意	管理者

ロールを非アクティブにすると、そのロールが割り当てられているすべてのユーザから、そのロールと関連するアクセス許可が削除されます。事前定義ユーザ ロールは削除できませんが、非アクティブにすることができます。

マルチドメイン展開では、現在のドメインで作成されたカスタム ユーザ ロールが表示されます。これは編集できます。先祖ドメインで作成されたカスタム ユーザ ロールも表示されますが、これは編集できません。下位のドメインのカスタム ユーザ ロールを表示および編集するには、そのドメインに切り替えます。

ステップ 1 **[System]** > **[Users]**を選択します。

ステップ 2 [User Roles] タブをクリックします。

ステップ 3 アクティブまたは非アクティブにするユーザ ロールの横にあるスライダをクリックします。

コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

Lights-Out Management を含むロールが割り当てられているユーザがログインしているときに、このロールを非アクティブにしてから再度アクティブにする場合、またはユーザのログイン セッション中にバックアップからユーザまたはユーザ ロールを復元する場合、そのユーザはWebインターフェイスに再度ログインして、IPMItool コマンドへのアクセスを再度取得する必要があります。

ユーザ ロール エスカレーションの有効化

Firepower Management Center の場合、カスタム ユーザ ロールにアクセス許可を付与し、パスワードを設定することで、ベース ロールの特権に加え、他のターゲット ユーザ ロールの特権を一時的に取得できます。この機能により、あるユーザが不在であるときにそのユーザを別のユーザに容易に置き換えることや、拡張ユーザ特権の使用状況を緊密に追跡することができます。デフォルトのユーザ ロールでは、エスカレーションはサポートされません。

たとえば、ユーザのベース ロールに含まれている特権が非常に限られている場合、そのユーザは管理アクションを実行するために管理者ロールにエスカレーションできます。ユーザが各自のパスワードを使用するか、または指定された別のユーザのパスワードを使用することができるように、この機能を設定できます。2 番目のオプションでは、該当するすべてのユーザのための 1 つのエスカレーション パスワードを容易に管理できます。

ユーザ ロール エスカレーションを設定するには、次のワークフローを参照してください。

ステップ 1 エスカレーション ターゲット ロールの設定 （85 ページ）。エスカレーション ターゲット ロールにすることができるユーザ ロールは一度に 1 つだけです。

ステップ 2 エスカレーション用のカスタム ユーザ ロールの設定 （85 ページ）。

ステップ 3 （ログイン後のユーザの場合）ユーザ ロールのエスカレーション （86 ページ）

エスカレーション ターゲット ロールの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	任意	FMC	任意	管理者

各自のユーザ ロール（事前定義またはカスタム）をシステム全体でのエスカレーション ターゲット ロールとして機能するように割り当てることができます。これは、カスタム ロールのエスカレーション先となるロールです（エスカレーションが可能な場合）。エスカレーション ターゲット ロールにすることができるユーザ ロールは一度に 1 つだけです。各エスカレーションはログイン セッション期間中保持され、監査ログに記録されます。

ステップ 1 **[System]** > **[Users]**を選択します。

ステップ 2 [ユーザ ロール（User Roles）] をクリックします。

ステップ 3 [アクセス許可エスカレーションの設定（Configure Permission Escalation）] をクリックします。

ステップ 4 [エスカレーションターゲット（Escalation Target）] ドロップダウン リストからユーザ ロールを選択します。

ステップ 5 [OK] をクリックして変更を保存します。

エスカレーション ターゲット ロールの変更は即時に反映されます。エスカレーションされたセッションのユーザには、新しいエスカレーション ターゲットのアクセス許可が付与されます。

エスカレーション用のカスタム ユーザ ロールの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	FMC	いずれか（Any）	管理者

エスカレーションを有効にするユーザは、エスカレーションを有効にしたカスタム ユーザ ロールに属している必要があります。この手順では、カスタム ユーザ ロールのエスカレーションを有効にする方法について説明します。

カスタム ロールのエスカレーション パスワードを設定するときには、部門のニーズを考慮してください。多数のエスカレーションユーザを容易に管理するには、別のユーザを選択し、そのユーザのパスワードをエスカレーション パスワードとして使用することができます。そのユーザのパスワードを変更するか、またはそのユーザを非アクティブにすると、そのパスワードを必要とするすべてのエスカレーションユーザが影響を受けます。この操作により、特に一元管理できる外部認証ユーザを選択した場合に、ユーザ ロール エスカレーションをより効率的に管理できます。

始める前に

エスカレーション ターゲット ロールの設定 （85 ページ）に従って対象ユーザ ロールを設定します。

ステップ 1 カスタム ユーザ ロールの作成 （82 ページ）の説明に従って、カスタム ユーザ ロールの設定を開始します。

ステップ 2 [システム権限（System Permissions）] エリアで、[このロールをエスカレーションする：（Set this role to escalate to:）] チェック ボックスをオンにします。

現在のエスカレーション ターゲット ロールは、チェックボックスの横に表示されます。

ステップ 3 このロールがエスカレーションするときに使用するパスワードを選択します。次の 2 つのオプションから選択できます。

- このロールを持つユーザがエスカレーション時に自分のパスワードを使用するようにするには、[割り当てられたユーザのパスワードを使用して認証（Authenticate with the assigned user's password）] を選択します。
- このロールを持つユーザが別のユーザのパスワードを使用するようにするには、[指定したユーザのパスワードを使用して認証（Authenticate with the specified user's password）] を選択して、そのユーザ名を入力します。

（注） 別のユーザのパスワードで認証するときには、任意のユーザ名（非アクティブなユーザまたは存在しないユーザを含む）を入力できます。エスカレーションにパスワードが使用されるユーザを非アクティブにすると、そのパスワードを必要とするロールが割り当てられているユーザのエスカレーションが不可能になります。この機能を使用して、必要に応じてエスカレーション機能をただちに削除できます。

ステップ 4 **[保存（Save）]** をクリックします。

ユーザ ロールのエスカレーション

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン数	アクセス
任意	任意	FMC	任意	任意

エスカレーション権限のあるカスタムユーザ ロールを割り当てられたユーザは、いつでもターゲット ロールの権限にエスカレーションできます。エスカレーションはユーザ設定に影響しないことに注意してください。

ステップ 1 ユーザ名の下にあるドロップダウン リストから、[アクセス許可のエスカレーション（Escalate Permissions）] を選択します。

このオプションが表示されない場合は、管理者はユーザ ロールのエスカレーションを有効にしていません。

ステップ 2 認証パスワードを入力します。

ステップ 3 [Escalate] をクリックします。これで、現行ロールに加え、エスカレーション ターゲット ロールのすべてのアクセス許可が付与されました。

エスカレーションはログイン セッションの残り期間にわたって保持されます。ベース ロールの特権だけに戻すには、ログアウトしてから新しいセッションを開始する必要があります。

Cisco Security Manager のシングル サインオンの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	任意	ASA FirePOWER	任意	管理者

シングル サインオンにより、Cisco Security Manager（CSM）バージョン 4.7 以上と Firepower Management Center を統合して、ログインの追加認証なしで CSM から Firepower Management Center にアクセスできるようにすることができます。ASA FirePOWER モジュールを使用して ASA を管理するときは、モジュールに展開したポリシーの変更が必要となる場合もあります。CSM でFirepower Management Centerを管理することを選択し、Web ブラウザで起動します。

（注） 組織で認証に CAC が使用されている場合は、シングル サインオンでログインできません。

始める前に

- NAT 環境では、Firepower Management Centerと CSM は NAT 境界の同じ側に存在している必要があります。

ステップ 1 CSM から、接続を識別するシングル サインオン共有暗号キーを生成します。詳細については、CSM のマニュアルを参照してください。

ステップ 2 Firepower Management Center から、**[System]** > **[Users]** を選択します。

ステップ 3 [CSM シングル サインオン（CSM Single Sign-on）] を選択します。

ステップ 4 CSM ホスト名または IP アドレスとサーバのポートを入力します。

ステップ 5 CSM から生成した**共有キー**を入力します。

ステップ 6 （任意） Firepower Management Center のプロキシ サーバを使用して CSM と通信する場合は、[接続にプロキシを使用（Use Proxy For Connection）] チェックボックスをクリックします。

ステップ 7 [送信（Submit）] をクリックします。

ステップ 8 [証明書の確認（Confirm Certificate）] をクリックして証明書を保存します。

LDAP 認証接続のトラブルシューティング

LDAP認証オブジェクトを作成したが、選択したサーバへの接続が失敗したか、または必要なユーザのリストが取得されなかった場合は、そのオブジェクトの設定を調整できます。

接続のテストで接続が失敗する場合は、設定のトラブルシューティングに関する次の推奨手順を試してください。

- Web インターフェイス画面上部とテスト出力に示されるメッセージから、問題の原因となっているオブジェクトの部分を確認します。
- オブジェクトに使用したユーザ名とパスワードが有効であることを確認します。
  - サードパーティのLDAPブラウザを使用してLDAPサーバに接続し、ベース識別名に示されているディレクトリを参照する権限がユーザにあることを確認します。
  - ユーザ名が、LDAP サーバのディレクトリ情報ツリーで一意であることを確認します。
  - テスト出力に LDAP バインド エラー 49 が示される場合は、ユーザのユーザ バインディングが失敗しています。サードパーティアプリケーションを使用してサーバ認証を試行し、その接続でも同様にバインディングが失敗するかどうかを確認します。
- サーバを正しく指定していることを確認します。
  - サーバの IP アドレスまたはホスト名が正しいことを確認します。
  - ローカル アプライアンスから、接続する認証サーバに TCP/IP でアクセスできることを確認します。
  - サーバへのアクセスがファイアウォールによって妨げられないこと、およびオブジェクトで設定されているポートがオープンしていることを確認します。
  - 証明書を使用してTLSまたはSSL経由で接続する場合は、証明書のホスト名が、サーバに使用されているホスト名と一致している必要があります。
  - シェル アクセスを認証する場合は、サーバ接続に IPv6 アドレスを使用していないことを確認します。

- サーバ タイプのデフォルトを使用している場合は、正しいサーバ タイプであることを確認し、[デフォルトを設定（Set Default）] をもう一度クリックしてデフォルト値をリセットします。

- ベース識別名を入力した場合は、[DN を取得（Fetch DNs）] をクリックし、サーバで使用可能なすべてのベース識別名を取得し、リストから名前を選択します。
- フィルタ、アクセス属性、または詳細設定を使用している場合は、それぞれが有効であり正しく入力されていることを確認します。
- フィルタ、アクセス属性、または詳細設定を使用している場合は、各設定を削除し、設定なしでオブジェクトをテストしてみます。
- 基本フィルタまたはシェル アクセス フィルタを使用している場合は、フィルタがカッコで囲まれており、有効な比較演算子を使用していることを確認します。
- より制限された基本フィルタをテストするには、特定のユーザだけを取得するため、フィルタにそのユーザのベース識別名を設定します。
- 暗号化接続を使用する場合：
  - 証明書の LDAP サーバの名前が、接続に使用するホスト名と一致していることを確認します。
  - 暗号化されたサーバ接続で IPv6 アドレスを使用していないことを確認します。
- テストユーザを使用する場合、ユーザ名とパスワードが正しく入力されていることを確認します。
- テストユーザを使用する場合、ユーザ資格情報を削除してオブジェクトをテストします。
- LDAP サーバに接続し、次の構文を使用して、使用しているクエリをテストします。

```
ldapsearch -x -b 'base_distinguished_name'
-h LDAPserver_ip_address -p port -v -D
'user_distinguished_name' -W 'base_filter'
```

たとえば、`domainadmin@myrtle.example.com` ユーザと基本フィルタ (`cn=*`) を使用して `myrtle.example.com` のセキュリティ ドメインに接続する場合は、次のステートメントを使用して接続をテストできます。

```
ldapsearch -x -b 'CN=security,DC=myrtle,DC=example,DC=com'
-h myrtle.example.com -p 389 -v -D
'domainadmin@myrtle.example.com' -W '(cn=*)'
```

接続のテストが正常に完了したが、プラットフォーム設定ポリシーの適用後に認証が機能しない場合は、使用する認証とオブジェクトの両方が、デバイスに適用されるプラットフォーム設定ポリシーで有効になっていることを確認します。

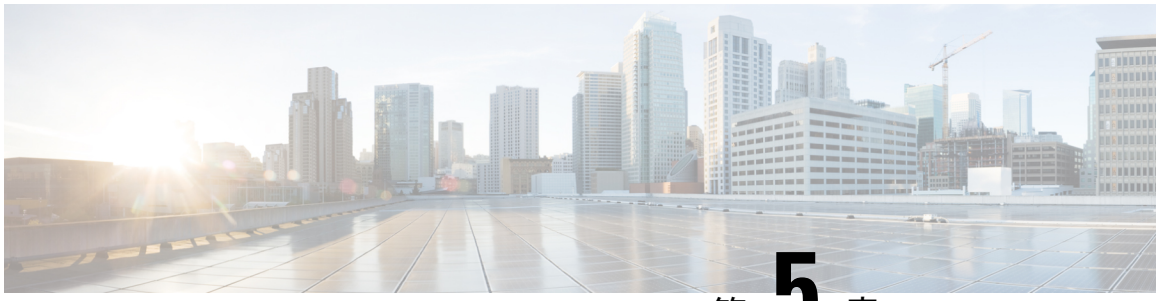
正常に接続したが、接続で取得されたユーザ リストを調整する必要がある場合は、基本フィルタまたはシェル アクセス フィルタを追加または変更するか、ベース DN をさらに制限するかまたは制限を緩めて使用することができます。

ユーザ アカウントの履歴

機能	バージョン	詳細
RADIUS サーバに定義されている FTD ユーザの Service-Type 属性のサポート	6.4	FTD CLI ユーザの RADIUS の認証では、以前は RADIUS 外部認証オブジェクトにユーザ名を定義してから、RADIUS サーバに認証されているユーザ名とリストが一致していることを手動で確認する必要がありました。Service-Type 属性を使用して RADIUS サーバで CLI ユーザを定義できるようになりました。また、Basic と Config の両方のユーザ ロールも定義できます。このメソッドを使用するには、外部認証オブジェクトのシェルアクセス フィルタを空白のままにしてください。 新しい/変更された画面： **[システム（System）] > [ユーザ（Users）] > [外部認証（External Authentication）] > [外部認証オブジェクトの追加（Add External Authentication Object）] > [シェル アクセス フィルタ（Shell Access Filter）]** サポートされるプラットフォーム FTD
FTD SSH アクセスの外部認証	6.2.3	LDAP または RADIUS認証を使用して FTD への SSH の外部認証を設定できるようになりました。 新しい/変更された画面： **[デバイス（Devices）] > [プラットフォームの設定（Platform Settings）]> [外部認証（External Authentication）]** サポートされるプラットフォーム FTD

第 II 部

Firepower システムの管理



第 5 章

Firepower システムのライセンス

ここでは、Firepower システムのライセンスを適用する方法について説明します。

Firepower ライセンスについて

Firepower 製品（Firepower Management Center と管理対象デバイス）には基本的な操作のライセンスが含まれていますが、一部の機能については、この章で説明するように、個別のライセンスまたはサービス サブスクリプションが必要です。

「使用権」ライセンスに有効期限はありませんが、サービス サブスクリプションは定期的に更新する必要があります。

製品に必要なライセンスのタイプ（スマートまたはクラッシック）はそれを実行するハードウェアではなく、使用するソフトウェアによって異なります。

Firepower Management Center のライセンス要件

Firepower Management Center 管理対象デバイスにライセンスを割り当ててシステムのライセンスを管理できます。

単一の Firepower Management Center でクラッシック ライセンスを必要とするデバイスと、スマート ライセンスを必要とするデバイスの両方を管理できます。

ハードウェア FMC

ハードウェアの Firepower Management Center では、デバイスを管理するために追加のライセンスやサービス サブスクリプションを購入する必要はありません。

Virtual FMC

Firepower Management Center Virtual の場合には追加のライセンス要件があります。Firepower Management Center Virtual ライセンス （94 ページ）を参照してください。

Firepower Management Center Virtual ライセンス

通常、Firepower Management Center Virtual の場合は管理するデバイスごとにライセンスの付与資格が必要です。

高可用性ペア内に設定されている Firepower Threat Defense デバイスを FMCv で管理する場合にも、（ペアに 1 つではなく）デバイスごとに 1 つの付与資格が必要です。

複数インスタンスの展開では、セキュリティ モジュールごとに 1 つの付与資格が必要です。

標準的な接続されているスマート ライセンスでは、これらは永続ライセンスです。

特定の永続ライセンスでは、これらは期間ベースのライセンスとなります。

この付与資格は、異なる数の付与資格を持つ **Firepower MCv デバイス ライセンス**として Cisco Smart Software Manager に表示されます。

評価ライセンスに関する注意事項

評価ライセンスではすべての機能を使用できるわけではありません。評価ライセンスで使用できるのは機能の一部であり、評価ライセンスから標準ライセンスへの移行もシームレスに行われない場合があります。

たとえば、クラスタ内に Firepower Threat Defense のデバイスを設定している場合、評価ライセンスからスマートライセンスに切り替えると変更を展開した時点でサービスが中断されます。

このライセンスに関する章と、各機能の展開に関連する章の情報にある評価ライセンスについての注意事項の情報を確認してください。

スマート ライセンスとクラシック ライセンス

管理対象デバイスの場合、必要なライセンス（スマートまたはクラシック）は、デバイスで実行されるソフトウェアによって異なります。いずれの FMC でも、スマートライセンスのデバイスと従来のライセンスのデバイスを同時に管理できます。各タイプのライセンスを個別に設定する必要があります。

ソフトウェア	ライセンスのタイプ	詳細情報
Firepower Management Center（ハードウェア）	なし	FMC ハードウェア モデル自体にはライセンスは必要ありません。
Firepower Management Center Virtual	デバイスの権限	Firepower Management Center Virtual ライセンス （94 ページ）を参照してください。
Firepower Threat Defense Firepower Threat Defense Virtual	スマート	Firepower Threat Defense デバイスのライセンス （96 ページ）を参照してください。
NGIPS ソフトウェア： • Firepower 7000/8000 シリーズ • ASA FirePOWER • NGIPSv	従来型	Firepower 7000/8000 シリーズのライセンス、ASA FirePOWER、および NGIPSv デバイス（従来のライセンス） （142 ページ）を参照してください。
その他すべてのソフトウェア（Firepower ハードウェア上で実行するものを含む）	ソフトウェア製品のライセンス情報を参照してください。	

Firepower Threat Defense デバイスでの展開のライセンス（スマート ライセンス）

Firepower Threat Defense デバイスにはスマート ライセンスが必要です。

Cisco Smart Licensing によって、ライセンスを購入し、ライセンスのプールを一元管理することができます。製品認証キー（PAK）ライセンスとは異なり、スマート ライセンスは特定のシリアル番号またはライセンス キーに関連付けられません。Smart Licensing を利用すれば、ライセンスの使用状況やニーズをひと目で評価できます。

また、Smart Licensing では、まだ購入していない製品の機能を使用できます。Cisco Smart Software Manager に登録すると、すぐにライセンスの使用を開始することも、後でライセンスを購入することもできます。これによって、機能の展開および使用が可能になり、発注書の承認による遅延がなくなります。

Firepower Threat Defense デバイスのライセンス

Firepower Threat Defense デバイスでは Smart Licensing が使用されます。

ステップ 1 Firepower の展開にスマート ライセンスが必要なことを確認してください。

スマート ライセンスとクラシック ライセンス （95 ページ）を参照してください。

展開に両方のタイプのライセンスが必要な場合は、スマート ライセンスが必要なデバイスについてはこの手順に従い、従来のライセンスを使用するデバイスについてはFirepower 7000/8000 シリーズのライセンス、ASA FirePOWER、および NGIPSv デバイス（従来のライセンス） （142 ページ）に記載の手順に従います。

ステップ 2 スマート アカウントをまだ持っていない場合は、1 つ作成します。

ライセンスを購入する前にスマートアカウントを取得することをお勧めします。新しいスマートアカウントを作成するには、ライセンスを保持するためのスマート アカウントの作成 （110 ページ）を参照してください。

（注） アカウント担当者が、ユーザのためにスマート アカウントを作成していることもあります。その場合は、https://software.cisco.com/#module/SmartLicensingで、Cisco Smart Software Manager（CSSM）のアカウントにアクセスできることを確認します。

ステップ 3 組織に必要なプラットフォーム ライセンスを把握します。

- Firepower Management Center 物理ハードウェア：

  このアプライアンスには必要なライセンスが付属しています。ライセンスを有効化するための操作は不要です。

- Firepower Management Center Virtual：

  追加のライセンスが必要です。詳細については、Firepower Management Center Virtual ライセンス （94 ページ）を参照してください。

  （クラシック ライセンスを使用するデバイスを FNCv でも管理する場合、クラッシク ライセンスを設定する際にそれらのデバイスにもこれらの付与資格が必要になります。）

- Firepower Threat Defense デバイス：

  各デバイスには、基本的な機能のためのライセンスが自動的に含まれています。詳細は、基本ライセンス （104 ページ）を参照してください。

  ベースのライセンスをアクティブ化するのに何も実行する必要はありませんが、次で説明するように、多くの機能で個別のライセンスが必要です。

ステップ 4 組織に必要な機能ライセンス（サービス サブスクリプションと呼ばれることもある）を把握します。

スマート ライセンスのタイプと制約事項 （101 ページ）およびサブトピックを参照してください。

ステップ 5 組織に必要な機能ライセンスまたはサービス サブスクリプションの数を確認してください。

- 一般に、各管理対象デバイスには、使用する各機能のライセンスが必要です。
- 高可用性ペアの Firepower Management Center の場合：

  FMC HA のライセンス要件 （265 ページ）を参照してください。
- 高可用性ペアの Firepower Threat Defense デバイスの場合：

  各デバイス（アクティブまたはスタンバイ）には、使用する各機能のライセンスが必要です。追加のライセンスは必要ありません。

  高可用性ペアでの FTD デバイスのライセンス要件 （875 ページ）を参照してください。
- シャーシ間またはシャーシ内クラスタ化 Firepower Threat Defense デバイスの場合：

  クラスタリングのライセンス （916 ページ）を参照してください。
- 複数インスタンス展開の場合：

  複数インスタンス展開のライセンス （110 ページ）を参照してください。

ステップ 6 変換または移動の必要がある既存のライセンスがある場合：

- 従来のライセンスを Firepower Threat Defense に使用できるライセンスに変換するには：

  クラシック ライセンスまたは PAK からスマート ライセンスへの変換 （152 ページ）を参照してください。
- 別の Firepower Management Center に現在登録されているスマート ライセンスを転送するには：

  別の にスマート ライセンスを転送します。 Firepower Management Center （139 ページ）およびCisco Smart Software Manager から Firepower Management Center の登録解除 （140 ページ）を参照してください。
- 別の Firepower Threat Defense に現在登録されているスマート ライセンスを移動するには：

  管理対象デバイスからのスマート ライセンスの移動または削除 （138 ページ）を参照してください。

ステップ 7 Firepower アプライアンスのインターネット アクセスが制限されている場合：

状況に最も適したソリューションを決定します。

- エアギャップ展開のライセンスのオプション （117 ページ）を参照してください。
- Firepower Management Center はインターネットに接続されていないが、シスコのライセンス認証局に接続できる内部サーバに接続できるか、または手動でライセンスの更新を受信できる場合：

  Smart Software Satellite Server を展開します。詳細については、Smart Software Satellite Server の概要 （117 ページ）およびSmart Software Satellite Server の展開方法 （118 ページ）を参照してください。

- 展開が完全にエアギャップになっていて、ライセンス認証局や、ライセンス認証局に接続する Satellite Server に接続できない場合、または手動でライセンスの更新を受信できる場合：

  特定のライセンスの予約の概要 （119 ページ）を参照し、この手順の残りはスキップします。

ステップ 8 複数の Firepower Management Center アプライアンスがあり、1 つのプロキシでシスコのライセンス認証局に接続する場合は、次の手順を実行します。

Smart Software Satellite Server を展開します。詳細については、Smart Software Satellite Server の概要 （117 ページ）を参照してください。

ステップ 9 強力な暗号化を使用する機能を有効にしたいが、地理的な領域によって制限されている場合：

輸出規制対象の機能のライセンス （108 ページ）を参照してください。

ステップ 10 必要なライセンスを購入します。

シスコのセールス担当者または認定再販業者に問い合わせてください。

ステップ 11 再販業者やシスコのセールス担当者によってスマート アカウントにライセンスが追加されたことを確認します。

CSSM で https://software.cisco.com/#SmartLicensing-Inventory を参照します。[インベントリ（Inventory）] をクリックした後、[ライセンス（Licenses）] タブをクリックします。必要に応じてリストをフィルタリングします。ライセンスの名前を把握するために購入確認が必要な場合があります。

表示されると予想していたライセンスが表示されない場合は、正しい仮想アカウントを確認していることを確認します。この点についてサポートが必要な場合は、CSSM のリソース リンクを参照してください。

引き続きライセンスが表示されないか、またはライセンスが正しくない場合は、そのライセンスを購入した担当者に問い合わせてください。

ステップ 12 仮想アカウント（スマートアカウント）に予想していたライセンスが表示されたら、Firepower Management Center を CSSM に登録します。

Web インターフェイスを使用して、Firepower Management Center にライセンスを設定する必要があります。

- Firepower Management Center が CSSM に直接接続している場合：

  次のトピックを参照してください。

  - スマート ライセンス用の製品ライセンス登録トークンの取得 （112 ページ）および
  - スマート ライセンスの登録 （113 ページ）

- Firepower Management Center が Smart Software Satellite Server に接続している場合：

  Smart Software Satellite Server への接続の設定 （118 ページ）を参照してください。

- Firepower Management Center がインターネットから完全に分離されている場合：

  特定のライセンスの予約ステータス （130 ページ）およびサブトピックを参照してください。

ステップ 13 登録が正常に実行されたことを確認します。

Firepower Management Center Web インターフェイスで、[システム（System）]>[ライセンス（Licenses）]>[スマートライセンス（Smart Licenses）]に移動します。[製品登録（Product Registration）]に緑のチェックマークが表示されている必要があります。

ステップ 14 まだ実行していない場合は、デバイスを管理対象デバイスとして Firepower Management Center に追加します。

Firepower Management Center へのデバイスの追加 （293 ページ）を参照してください

ステップ 15 管理対象 Firepower Threat Defense デバイスへのライセンスの割り当て：

複数の管理対象デバイスへのライセンスの割り当て （135 ページ）を参照してください

ステップ 16 デバイスにライセンスが正常に追加されたことを確認します。

スマート ライセンスおよびスマート ライセンス ステータスの表示 （136 ページ）を参照してください。

ステップ 17 必要に応じて、高可用性とクラスタ化された展開のライセンスをセットアップします。

- 高可用性ペアの Firepower Management Center の場合：

  Firepower Management Center ハイ アベイラビリティの確立 （272 ページ）の前提条件を参照してください。

  FMC 高可用性ペアを設定すると、デバイスのライセンスはアクティブからスタンバイ管理センターに自動的に転送されます。ライセンスに固有の設定は不要です。

- 高可用性ペアの Firepower Threat Defense デバイスの場合：

  高可用性を設定する前に、アクティブとスタンバイの両方のデバイスに使用する機能のライセンスを割り当てます。デバイスにさまざまな機能のライセンスがある場合、スタンバイ デバイスのライセンスがアクティブなデバイスと同じ一連のライセンスで置き換えられます。

- クラスタ化 Firepower Threat Defense デバイスの場合：

  クラスタリングのライセンス （916 ページ）を参照してください。ライセンスの手順は、FMC：クラスタの追加 （931 ページ）に含まれています。

次のタスク

- （オプション）従来のデバイス（7000/8000 シリーズ、ASA FirePOWER、NGIPSv）を管理する必要がある場合は、それらのデバイスにライセンスを設定します。

  Firepower 7000/8000 シリーズのライセンス、ASA FirePOWER、および NGIPSv デバイス（従来のライセンス） （142 ページ）を参照してください。

- 有効期間と期限を把握します。FirePOWER のライセンスとサービス サブスクリプションの期限切れ （156 ページ）を参照してください。

Smart Software Manager

Firepower機能のスマートライセンスを複数購入する場合は、それらのライセンスをCisco Smart Software Manager（http://www.cisco.com/web/ordering/smart-software-manager/index.html）で管理できます。Smart Software Manager では、組織のマスター アカウントを作成できます。

デフォルトでは、ライセンスはマスターアカウントの下のデフォルトの仮想アカウントに割り当てられます。アカウントの管理者として、たとえば、地域、部門、または子会社ごとに、追加の仮想アカウントを作成できます。複数の仮想アカウントを使用することで、多数のライセンスおよびアプライアンスの管理を行うことができます。

ライセンスとアプライアンスは、バーチャル アカウント別に管理します。バーチャル アカウントに割り当てられているライセンスを使用できるのは、そのバーチャルカウントのアプライアンスのみです。追加のライセンスが必要な場合は、別の仮想アカウントから未使用のライセンスを転用できます。また、仮想アカウント間でのアプライアンスの譲渡も可能です。

バーチャル アカウントごとに、製品インスタンス登録トークンを作成できます。各 Firepower Management Center を展開するか、または既存の FMC を登録する場合は、このトークン ID を入力します。既存のトークンの有効期限が切れている場合は、新しいトークンを作成できます。トークンの有効期限が切れても、そのトークンを使用して登録された FMC には影響しませんが、有効期限が切れたトークンを使用して FMC を登録することはできません。また、登録済み FMC は、使用するトークンに基づいてバーチャル アカウントに関連付けられます。

Cisco Smart Software Manager の詳細については、*Cisco Smart Software Manager User Guide*または https://www.cisco.com/c/en/us/buy/smart-accounts/software-manager.html を参照してください。あるいは https://www.cisco.com/web/fw/softwareworkspace/smartlicensing/SSMCompiledHelps/ からもアクセスできる CSSM 内のオンライン ヘルプを参照してください。

License Authority との定期通信

製品ライセンスの権限付与を維持するために、製品は Cisco ライセンス認証局と定期的に通信する必要があります。

Firepower Management Center の登録に製品インスタンス登録トークンを使用すると、このアプライアンスがシスコのライセンス認証局に登録されます。ライセンス認証局は、Firepower Management Center とライセンス認証局の間の通信用に ID 証明書を発行します。この証明書の有効期間は 1 年ですが、6 か月ごとに更新されます。ID 証明書の期限が切れた場合（通常は、9 ヵ月または 1 年間通信がない状態）、Firepower Management Center は登録解除状態に戻り、ライセンス機能の使用は中断されます。

Firepower Management Center は、定期的にライセンス認証局と通信します。Smart Software Manager で変更を加えた場合は、Firepower Management Center 上で認証を更新すると、その変更がすぐに適用されます。また、スケジュールどおりにアプライアンスが通信するのを待つこともできます。

Firepower Management Center は、Cisco Smart Software Manager を介してライセンス認証局に直接インターネットでアクセスするか、スケジュールした期間でスマート ソフトウェア サテライト サーバを介してアクセスする必要があります。通常のライセンスに関する通信は 30 日ごとに行われますが、これには猶予期間があり、アプライアンスはホームをコールすることなく

最大で 90 日間は動作します。90 日が経過する前にライセンス認証局と連絡を取る必要があります。

オプションで、ライセンス認証局との通信用プロキシとして機能するように Smart Software サテライト サーバを設定することができます。詳細については、Smart Software Satellite Server の概要 （117 ページ）を参照してください。

Firepower機能のサービスサブスクリプション（スマートライセンス）

一部の機能にはサービス サブスクリプションが必要です。

サービス サブスクリプションは、所定の時間内限定で、管理対象デバイス上の特定の Firepower 機能を有効にします。サービス サブスクリプションは、1 年、3 年、または 5 年単位で購入できます。サブスクリプションの期限が切れると、サブスクリプションの更新が必要であることが通知されます。Firepower Threat Defense デバイスのサブスクリプションの期限が切れた場合でも、関連する機能は引き続き使用できます。

表 *2:* サブスクリプションおよび対応するスマート ライセンス

購入するサブスクリプション	Firepower システム内で割り当てるスマート ライセンス
T	脅威
TC	脅威 + URL フィルタリング
TM	脅威 + マルウェア
TMC	脅威 + URL フィルタリング + マルウェア
URL	URL フィルタリング（脅威に追加するか、脅威なしで使用できます）
AMP	マルウェア（脅威に追加するか、脅威なしで使用できます）

スマート ライセンスを使用する管理対象デバイスを購入すると、基本ライセンスが自動的に提供されます。このライセンスは無制限であり、システム アップデートを使用可能にします。Firepower Threat Defense デバイスでは、すべてのサービス サブスクリプションがオプションです。

スマート ライセンスのタイプと制約事項

ここでは、Firepower システムの導入環境で使用可能なスマート ライセンスのタイプについて説明します。Firepower Management Center では、Firepower Threat Defense のデバイスを管理するためスマート ライセンスが必要です。

次の表に、Firepower システムのスマート ライセンスの概要を示します。

表 *3 : Firepower* システムのスマート ライセンス

Firepowerシステムで割り当てるライセンス	購入するサブスクリプション	期間	付与される機能
基本 （特定のライセンスの予約を除き、基本ライセンスがすべての Firepower Threat Defenseデバイスに自動的に割り当てられます）	サブスクリプションは不要（デバイスにライセンスが含まれています）	永久	ユーザおよびアプリケーション制御 スイッチングとルーティング NAT 詳細は、基本ライセンス （104ページ）を参照してください。
脅威	• T • TC（脅威 + URL） • TMC（脅威 + マルウェア + URL）	期間ベース	侵入検知と防御 ファイル制御 セキュリティ インテリジェンス フィルタリング 詳細については、脅威ライセンス （106 ページ）を参照してください。
マルウェア	• TM（脅威 + マルウェア） • TMC（脅威 + マルウェア + URL） • AMP	期間ベース	ネットワーク向け AMP（ネットワーク ベースの高度なマルウェア防御） Cisco Threat Grid ファイル ストレージ 詳細については、Firepower Threat Defense デバイスのマルウェア ライセンス （105 ページ）およびファイルおよびマルウェア ポリシーのライセンス要件 （1913 ページ） を参照してください。

Firepower システムで割り当てるライセンス	購入するサブスクリプション	期間	付与される機能
URL フィルタリング	• TC（脅威 + URL） • TMC（脅威 + マルウェア + URL） • URL	期間ベース	カテゴリとレピュテーションに基づく URL フィルタリング 詳細は、Firepower Threat Defense デバイスの URL フィルタリング ライセンス（106ページ）を参照してください。
仮想 Firepower Management Center	ライセンス タイプに基づいています。	ライセンス タイプに基づき期間ベースまたは永久	プラットフォーム ライセンスによって、仮想アプライアンスが管理できるデバイスの数が決まります。 詳細は、Firepower Management Center Virtual ライセンス （94 ページ）を参照してください。
輸出管理機能	ライセンス タイプに基づいています。	ライセンス タイプに基づき期間ベースまたは永久	国家安全保障、外交政策、反テロリズムに関する法律や規制の対象となる機能。輸出規制対象の機能のライセンス （108 ページ） を参照してください。

Firepower システムで割り当てるライセンス	購入するサブスクリプション	期間	付与される機能
リモート アクセス VPN： • AnyConnect Apex • AnyConnect Plus • AnyConnect VPN Only	ライセンス タイプに基づいています。	ライセンス タイプに基づきタームベースまたは永久	リモート アクセス VPN の設定。リモート アクセス VPN を設定するには、基本ライセンスがエクスポート制御機能を許可する必要があります。デバイスの登録時に、輸出要件を満たしているかどうかを選択します。Firepower Threat Defense は有効な AnyConnect ライセンスを使用できます。使用できる機能はライセンス タイプによって異なります。 詳細については、AnyConnect ライセンス （107 ページ）およびVPN ライセンス （1057 ページ）を参照してください。

基本ライセンス

基本ライセンスは、Firepower Threat Defense または Firepower Threat Defense Virtual デバイスを購入するごとに自動的に提供されます。

基本ライセンスでは、次のことができます。

- スイッチングおよびルーティング（DHCP リレーおよび NAT を含む）を実行するように FTD デバイスを設定する
- FTD デバイスをハイ アベイラビリティ ペアとして設定する
- Firepower 9300 シャーシ内のクラスタとしてセキュリティ モジュールを設定する（シャーシ内クラスタリング）
- Firepower Threat Defense を実行している Firepower 9300 または Firepower 4100 シリーズ デバイスをクラスタとして設定する（シャーシ間クラスタリング）
- アクセス コントロール ルールにユーザとアプリケーションの条件を追加することで、ユーザとアプリケーションの制御を実装する

脅威とマルウェアの検出および URL のフィルタリング機能には追加のオプション ライセンスが必要です。

特定のライセンスの予約を使用する展開の場合を除き、基本ライセンスは登録した Firepower Threat Defense デバイスごとに Firepower Management Center に自動的に追加されます。

複数インスタンス展開については、複数インスタンス展開のライセンス（110ページ）を参照してください。

Firepower Threat Defense デバイスのマルウェア ライセンス

Firepower Threat Defense デバイス用のマルウェア ライセンスを使用すると、ネットワーク向け AMP および Cisco Threat Grid を使用して Cisco Advanced Malware Protection（AMP）を実行することができます。この機能では、Firepower Threat Defense デバイスを使用して、ネットワーク上で伝送されるファイルのマルウェアを検出してブロックできます。この機能ライセンスをサポートするために、スタンドアロン サブスクリプションとしてマルウェア（AMP）サービス サブスクリプションを購入できます。また、脅威（TM）や脅威および URL フィルタリング（TMC）サブスクリプションと組み合わせて購入することもできます。

（注） マルウェア ライセンスが有効になっている Firepower Threat Defense 管理対象デバイスは、動的分析を設定していない場合でも、定期的に AMP クラウドへの接続を試行します。このため、デバイスの [インターフェイス トラフィック（Interface Traffic）] ダッシュボード ウィジェットには、送信済みトラフィックが表示されます。これは正常な動作です。

ファイル ポリシーの一部として ネットワーク向け AMP を設定し、その後 1 つ以上のアクセス コントロール ルールを関連付けます。ファイル ポリシーでは、特定のアプリケーション プロトコルを介した特定のタイプのユーザによるファイルのアップロードとダウンロードを検出できます。ネットワーク向け AMP では、ローカル マルウェア分析とファイルの事前分類を使用して、それらの限られた一連のファイルタイプを検査できます。特定のファイル タイプをダウンロードして Cisco Threat Grid クラウドにアップロードして、動的 Spero 分析でマルウェアが含まれているかどうかを判別することもできます。これらのファイルでは、ファイルがネットワーク内で経由する詳細なパスを示すネットワーク ファイル トラジェクトリを表示できます。マルウェア ライセンスでは、ファイル リストに特定のファイルを追加し、そのファイル リストをファイル ポリシー内で有効にすることもできます。これにより、検出時にこれらのファイルを自動的に許可またはブロックできます。

マルウェア ライセンスをすべて無効にすると、システムは AMP への問い合わせを停止し、AMP クラウドから送信される遡及的イベントの確認応答も停止します。既存のアクセス コントロール ポリシーに ネットワーク向け AMP 構成が含まれている場合は、それらのポリシーを再展開することができません。マルウェア ライセンスが無効にされた後、システムが既存のキャッシュ ファイルの性質を使用できるのは極めて短時間のみであることに注意してください。この時間枠の経過後、システムは `Unavailable` という性質をこれらのファイルに割り当てます。

マルウェア ライセンスが必要なのは、ネットワーク向け AMP および Cisco Threat Grid を展開する場合のみであることに注意してください。マルウェア ライセンスがなければ、Firepower Management Center は AMP クラウドからエンドポイント向け AMP マルウェア イベントおよび侵害の兆候（IOC）を受信できます。

ファイルおよびマルウェア ポリシーのライセンス要件（1913ページ）の重要な情報も参照してください。

脅威ライセンス

脅威ライセンスでは、侵入の検出と防御、ファイル制御、およびセキュリティインテリジェンスのフィルタリングを実行することができます。

- 侵入検知および防御により、侵入とエクスプロイトを検出するためネットワークトラフィックを分析できます。またオプションで違反パケットをドロップできます。
- ファイル制御により、特定のアプリケーションプロトコルを介した特定タイプのファイルを検出し、オプションでこれらのファイルのアップロード（送信）またはダウンロード（受信）をユーザからブロックできます。マルウェア ライセンスが必要な ネットワーク向け *AMP* では、マルウェアの性質に基づいて限られたファイル タイプを検査およびブロックすることもできます。
- セキュリティインテリジェンスフィルタリングにより、トラフィックをアクセス制御ルールによる分析対象にする前に、特定の IP アドレス、URL、および DNS ドメイン名をブラックリストに追加（その IP アドレスとの間のトラフィックを拒否）できます。ダイナミック フィードにより、最新の情報に基づいて接続を直ちにブラックリストに追加できます。オプションで、Security Intelligence フィルタリングに「監視のみ」設定を使用できます。

脅威ライセンスは、スタンドアロン サブスクリプション（T）として、または URL フィルタリング（TC）、マルウェア（TM）、またはその両方（TMC）と組み合わせて購入することができます。

管理対象デバイスで脅威ライセンスを無効にすると、Firepower Management Center で、影響を受けたデバイスからの侵入イベントとファイルイベントの確認応答が停止されます。結果として、トリガー条件としてこれらのイベントを使用する相関ルールがトリガーしなくなります。また、Firepower Management Center はシスコ提供またはサードパーティのセキュリティインテリジェンス情報を取得するためにインターネットに接続しなくなります。脅威ライセンスを再度有効にするまでは、既存の侵入ポリシーを適用し直すことができません。

Firepower Threat Defense デバイスの URL フィルタリング ライセンス

URL フィルタリング ライセンスにより、モニタ対象ホストにより要求される URL に基づいて、ネットワーク内を移動できるトラフィックを判別するアクセス制御ルールを作成することができます。この機能ライセンスをサポートするために、スタンドアロンサブスクリプションとして URL フィルタリング（URL）サービス サブスクリプションを購入できます。また、脅威（TM）や脅威およびマルウェア（TMC）サブスクリプションと組み合わせて購入することもできます。

ヒント　URL フィルタリング ライセンスがない状態で、許可またはブロックする個別 URL または URL グループを指定できます。これにより、Web トラフィックをカスタムできめ細かく制御できますが、URL カテゴリおよびレピュテーション データをネットワーク トラフィックのフィルタリングに使用することはできません。

URL フィルタリング ライセンスがない状態でも、アクセス制御ルールにカテゴリ ベースの URL 条件およびレピュテーション ベースの URL 条件を追加できますが、Firepower Management Center は URL 情報をダウンロードしません。最初に URL フィルタリング ライセンスを Firepower Management Center に追加し、ポリシー適用対象デバイスで有効にするまでは、アクセス コントロール ポリシーを適用できません。

管理対象デバイスで URL フィルタリング ライセンスを無効にすると、URL フィルタリングへのアクセスが失われる可能性があります。ライセンスが期限切れになるか、ライセンスを無効にすると、URL 条件が含まれているアクセス制御ルールは URL フィルタリングを直ちに停止し、Firepower Management Center は URL データのアップデートをダウンロードできなくなります。既存のアクセス コントロール ポリシーに、カテゴリ ベースまたはレピュテーション ベースの URL 条件を含むルールが含まれている場合は、それらのポリシーを再展開することができません。

AnyConnect ライセンス

Firepower Threat Defense デバイスを使用して、Cisco AnyConnect セキュア モビリティ クライアント（AnyConnect）と標準規格に準拠した IPSec/IKEv2 を使用するリモート アクセス VPN を設定できます。

Firepower Threat Defense リモート アクセス VPN 機能を有効にするは、次のライセンスのいずれかを購入し、有効にしておく必要があります。[AnyConnect Plus]、[AnyConnect Apex]、または [AnyConnect VPN のみ（AnyConnect VPN Only）]。AnyConnect の任意のライセンス（[Plus]、[Apex]、[VPN のみ（VPN Only）]）を使用できます。両方のライセンスがあり、どちらも使用する場合は、[AnyConnect Plus] と [AnyConnect Apex] を選択できます。[Apex] または [Plus] と一緒に [AnyConnect VPN のみ（AnyConnect VPN Only）] ライセンスを使用することはできません。AnyConnect ライセンスは、スマート アカウントと共有する必要があります。手順については、http://www.cisco.com/c/dam/en/us/products/collateral/security/anyconnect-og.pdfを参照してください。

指定されたデバイスに指定された AnyConnect ライセンス タイプの権限が 1 つ以上ない場合、リモート アクセス VPN 設定を FTD デバイスに展開することはできません。登録されたライセンスがコンプライアンスに従っていない、または権限の有効期限が切れている場合は、システムにライセンス アラートとヘルス イベントが表示されます。

リモート アクセス VPN を使用する際は、スマート ライセンス アカウントでエクスポート制御機能（高度な暗号化）を有効にしておく必要があります。AnyConnect クライアントとのリモート アクセス VPN 接続を確立するために、FTD はより強力な暗号化を要求します（これは DES よりも高い暗号化です）。デバイスを登録する際に、エクスポート制御機能に対して有効化された Smart Software Manager アカウントによってエクスポートを制御する必要があります。エクスポート制御機能の詳細については、スマート ライセンスのタイプと制約事項 （101 ページ）を参照してください。

次の条件に当てはまる場合、リモート アクセス VPN を展開できません。

- Firepower Management Center でスマート ライセンスが評価モードで実行されている。

- スマートアカウントがエクスポート制御機能（高度な暗号化）を使用するように設定されていない。エクスポート制御機能を持つ基本ライセンスを適用した後に、FTDデバイスを再起動する必要があることに注意してください。

輸出規制対象の機能のライセンス

輸出規制対象の機能が必要な機能

特定のソフトウェア機能は、国家安全保障、外交政策、反テロリズムに関する法律や規制の対象となります。これらの輸出規制対象の機能は次のとおりです。

- セキュリティ認定コンプライアンス
- Firepower Threat Defense リモート アクセス VPN
- 強力な暗号化によるサイト間 VPN
- 強力な暗号化による SSH プラットフォーム ポリシー
- 強力な暗号化による SSL ポリシー
- 強力な暗号化による SNMPv3 などの機能

輸出規制対象の機能がシステムに対して現在有効になっているかどうかを判断する方法

輸出規制対象の機能がシステムに対して現在有効になっているかどうかを判断するには、[システム（System）] > [ライセンス（Licenses）] > [スマート ライセンス（Smart Licenses）] に移動し、[輸出規制対象の機能（Export-Controlled Features）] に [有効（Enabled）] と表示されているかどうかを確認します。

輸出規制対象の機能の有効化について

[輸出規制対象の機能（Export-Controlled Features）] に [無効（Disabled] と表示されており、強力な暗号化が必要な機能を使用する場合：

強力な暗号化機能を有効にする方法は2つあります。組織はどちらか一方を使用する（またはどちらも使用しない）ことができますが、両方を使用することはできません。

- Cisco Smart Software Manager（CSSM）で新しい製品インスタンス登録トークンを生成したときに輸出規制対象の機能を有効にするオプションがない場合は、次のようになります。

  代理店に問い合わせてください。

  Firepower Management Center では、スマート アカウントが輸出規制対象の機能の付与資格がある場合は輸出規制対象の機能を使用することができます。シスコによって承認されると、輸出規制ライセンスが仮想アカウントに追加されるため、輸出規制対象お機能を使用できます。詳細については、輸出規制機能の有効化（グローバル権限のないアカウントの場合）（115 ページ）を参照してください。

- Cisco Smart Software Manager（CSSM）で新しい製品インスタンス登録トークンを生成したときに輸出規制対象の機能を使用するためのオプションが表示された場合：

- これは永続的な付与資格であり、サブスクリプションは必要ありません。
- 輸出規制対象の機能を使用するには、Firepower Management Center にライセンスを取得する前にスマート アカウントがこの機能を使用できるように有効になっている必要があります。
- Cisco Smart Software Manager（CSSM）のスマート アカウントに対して輸出規制対象の機能を有効にした後、新しい製品インスタンス登録トークンを使用して Firepower Management Center を再登録する必要があります。
- 新しい製品インスタンス登録トークンを作成する際に、[このトークンで登録された製品で輸出規制対象の機能を許可する（Allow export-controlled functionality on the products registered with this token）] オプションを選択する必要があります。この機能がスマート アカウントに許可されている場合には、このオプションがデフォルトで有効になっています。
- 輸出規制対象の機能を持つトークンを Firepower Management Center にインストールし、管理対象の Firepower Threat Defense デバイスに関連するライセンスを割り当てた後、次の手順を実行します。
  - 各デバイスを再起動し、新たに有効にした機能を使用できるようにします。
  - 高可用性展開では、アクティブ デバイスとスタンバイ デバイスを一緒に再起動してアクティブ/アクティブの状態を回避する必要があります。

詳細情報

輸出規制に関する一般情報については https://www.cisco.com/c/en/us/about/legal/global-export-trade.html を参照してください。

高可用性構成のライセンス

参照先：

- 高可用性ペア内の Firepower Management Center アプライアンスの場合：

  ライセンス要件 （265 ページ）

- 高可用性ペア内の Firepower Threat Defense デバイスの場合：

  高可用性ペアでの FTD デバイスのライセンス要件 （875 ページ）

また、スマート ライセンスのタイプと制約事項 （101 ページ）のトピックの特定のライセンス タイプについてのトピックも参照してください。

FTD クラスタのライセンス

このライセンス章の情報の他に次を参照してください。

- クラスタリングのライセンス （916 ページ）

- FMC：クラスタの追加 （931 ページ）。

複数インスタンス展開のライセンス

すべてのライセンスがコンテナ インスタンスごとではなく、セキュリティ エンジン/シャーシ（Firepower 4100 の場合）またはセキュリティ モジュール（Firepower 9300 の場合）ごとに適用されます。

基本ライセンス

各セキュリティ エンジンまたはモジュールが 1 つの基本ライセンスを使用します。このライセンスは、特定のライセンスの予約を使用している場合を除き、すべての展開に自動的に割り当てられます。

仮想 Firepower Management Center

Firepower Management Center の仮想アプライアンスが管理するセキュリティ エンジン/モジュールごとに 1 つの付与資格が必要です。

機能ライセンス

ライセンス（マルウェア、脅威、URL フィルタリング、AnyConnect Apex、AnyConnect Plus、および AnyConnect VPN 専用）を取得する各機能に、セキュリティ エンジン/モジュール単位で 1 つのライセンスが必要です。エンジン/モジュールのすべてのインスタンスで同じ機能ライセンスを共有できます。

インスタンスごとにライセンスを割り当てる必要があります。

ハイ アベイラビリティ展開

高可用性ペア内のインスタンスは機能ライセンスを相互に共有することはできませんが、各インスタンスがそれぞれのエンジン/モジュール上の他のインスタンスと機能ライセンスを共有することはできます。

ライセンスの例

上記のライセンス要件の連動については、コンテナインスタンスのライセンス （748 ページ）を参照してください。

ライセンスを保持するためのスマート アカウントの作成

スマート アカウントはスマート ライセンスのために必要です。また、従来のライセンスを保持することもできます。

スマート ライセンスを購入する前に、スマート アカウントを設定する必要があります。

始める前に

アカウント担当者または再販業者が、ユーザのためにスマートアカウントを設定していることがあります。その場合は、この手順を使用するのではなく、その担当者からアカウントへのアクセスに必要な情報を取得してから、アカウントにアクセスできることを確認してください。

スマート アカウントに関する一般情報については http://www.cisco.com/go/smartaccountsを参照してください。

ステップ 1 スマート アカウントのリクエスト：

この説明については、https://community.cisco.com/t5/licensing-enterprise-agreements/request-a-smart-account-for-customers/ta-p/3636515?attachment-id=150577 を参照してください。

詳細については、https://communities.cisco.com/docs/DOC-57261を参照してください。

ステップ 2 スマート アカウントの設定準備ができたことを知らせる電子メールが届くのを待ちます。電子メールが届いたら、指示に従って、メールに含まれているリンクをクリックします。

ステップ 3 スマート アカウントの設定：

https://software.cisco.com/software/company/smartaccounts/home?route=module/accountcreation を参照してください。

この説明については、https://community.cisco.com/t5/licensing-enterprise-agreements/complete-smart-account-setup-for-customers/ta-p/3636631?attachment-id=132604 を参照してください。

ステップ 4 Cisco Smart Software Manager（CSSM）でアカウントにアクセスできることを確認します。

https://software.cisco.com/#module/SmartLicensing に移動してサインインします。

次のタスク

長いワークフローに従っている場合は、そのワークフローに戻ります。

Firepower Threat Defense デバイスのライセンス （96 ページ）

ダイレクト インターネット アクセスによるスマート ライセンスの設定方法

始める前に

展開が複雑な場合、または必要なライセンスについてご不明な点がある場合は、Firepower Threat Defense デバイスのライセンス （96 ページ）を参照してください。

ステップ 1 Cisco Smart Software Manager ライセンス ポータルでトークンを取得します。

スマート ライセンス用の製品ライセンス登録トークンの取得 （112 ページ）を参照してください。

ステップ 2 スマート ライセンス ポータルに Firepower Management Center を登録します。

スマート ライセンスの登録 （113 ページ）を参照してください。このトピックの前提条件が満たされていることを確認してください。

ステップ 3 FMC がスマート ライセンス ポータルに正常に登録されたことを確認します。

Firepower Management Center Web インターフェイスで、[システム（System）] > [ライセンス（Licenses）] > [スマートライセンス（Smart Licenses）] に移動します。

[製品登録（Product Registration）] に緑のチェックマークが表示されている必要があります。

ステップ 4 FMC にまだデバイスを追加していない場合は、追加します。

Firepower Management Center へのデバイスの追加 （293 ページ）を参照してください。

ステップ 5 FMC によって管理されているデバイスにライセンスを割り当てます。

複数の管理対象デバイスへのライセンスの割り当て （135 ページ）を参照してください。

ステップ 6 ライセンスが正常にインストールされたことを確認します。

スマート ライセンスおよびスマート ライセンス ステータスの表示 （136 ページ）を参照してください。

次のタスク

必要に応じて、高可用性展開およびクラスタ化展開のライセンスをセットアップします。

Firepower Threat Defense デバイスのライセンス （96 ページ）の最後の手順を参照してください。

スマート ライセンス用の製品ライセンス登録トークンの取得

始める前に

- まだ作成していない場合は、スマート アカウントを作成します。https://software.cisco.com/smartaccounts/setup#accountcreation-accountを参照してください。詳細については、https://www.cisco.com/c/en/us/buy/smart-accounts.htmlを参照してください。
- 必要なライセンスのタイプおよびライセンス数を購入したことを確認します。
- 必要ライセンスがスマート アカウントに表示されていることを確認します。

  ライセンスがスマートアカウントに表示されない場合は、注文した担当者（シスコのセールス担当者または認定再販業者など）にそのライセンスをスマートアカウントに転送するように依頼します。
- 可能ならば、スマート ライセンスの登録 （113 ページ）の前提条件を確認して、登録プロセスがスムーズに進むようにします。
- Cisco Smart Software Manager にサインインするためのクレデンシャルがあることを確認します。

ステップ 1 https://software.cisco.com に進みます。

ステップ 2 （[ライセンシング（Licensing）] セクションで）[スマート ソフトウェア ライセンシング（Smart Software Licensing）] をクリックします。

ステップ 3 Cisco Smart Software Manager にサインインします。

ステップ 4 [インベントリ（Inventory）] をクリックします。

ステップ 5 [General] をクリックします。

ステップ 6 [新規トークン（New Token）] をクリックします。

ステップ 7 [説明（Description）] に、このトークンを使用する Firepower Management Center を一意かつ明確に特定する名前を入力します。

ステップ 8 365 日以内の期限を入力します。

この期限により、トークンを Firepower Management Center に登録しておく必要がある期間が決まります（ライセンスの権限付与期間はこの設定とは関係ありませんが、トークンをまだ登録していない場合でも、カウント ダウンが開始されることがあります）。

ステップ 9 エクスポート制御機能を有効にするオプションが表示されていて、強力な暗号化を必要とする機能を使用する予定の場合は、このオプションを選択します。

重要 このオプションが表示された場合は、この機能を使用する予定かどうかをここで選択する必要があります。輸出規制対象の機能を後で有効にすることはできません。

このオプションが表示されていない場合で、輸出規制対象の機能のライセンスを組織が取得している場合は、輸出規制機能の有効化（グローバル権限のないアカウントの場合） （115 ページ）で説明したように、この機能を後で有効にします。

ステップ 10 [トークンの作成（Create Token）] をクリックします。

ステップ 11 リストで新しいトークンを見つけて、[アクション（Actions）] をクリックして、[コピー（Copy）] または [ダウンロード（Download）] を選択します。

ステップ 12 必要に応じて、Firepower Management Center にトークンを入力する準備ができるまで、トークンを安全な場所に保存します。

次のタスク

スマート ライセンスの登録 （113 ページ）の手順に進みます。

スマート ライセンスの登録

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	該当なし	Firepower Threat Defense	グローバルだけ	Admin

Cisco Smart Software Manager で Firepower Management Center を登録します。

始める前に

- Smart Software Satellite Server または特定のライセンスの予約を使用している場合は、この手順を使用しないでください。代わりに、Smart Software Satellite Server への接続の設定（118ページ）または特定のライセンスの予約の実装方法（120ページ）をそれぞれ参照してください。
- Firepower Management Center が tools.cisco.com:443 で Cisco Smart Software Manager（CSSM）サーバにアクセスできることを確認します。
- Firepower Management Center で NTP デーモンが実行されていることを確認します。登録時に、NTP サーバと Cisco Smart Software Manager の間でキー交換が実行されるため、適切な登録には時刻の同期が必要です。

  Firepower 4100/9300 シャーシに FTD を展開する場合は、Firepower Management Center と同じ NTP サーバをシャーシに使用して Firepower シャーシに NTP を設定する必要があります。
- 組織に複数の Firepower Management Center アプライアンスがある場合は、各 FMC に明確に識別できる一意の名前が付いていて、同じバーチャルアカウントに登録されている可能性がある他の Firepower Management Center アプライアンスと区別できることを確認します。この名前は、スマート ライセンスの権限付与の管理にとって重要です。あいまいな名前だと後で問題が発生することがあります。
- Cisco Smart Software Manager から必要な製品ライセンス登録トークンを生成します。スマート ライセンス用の製品ライセンス登録トークンの取得（112ページ）を参照してください（すべての前提条件を含む）。Firepower Management Center にアクセスするマシンからトークンにアクセスできることを確認します。

ステップ 1 **[System]** > **[Licenses]** > **[Smart Licenses]**を選択します。

ステップ 2 Firepower Management Center の Web インターフェイスで、[登録（Register）] をクリックします。

ステップ 3 生成されたトークンを [製品インスタンス登録トークン（Product Instance Registration Token）] フィールドに貼り付けます。

テキストの前後にスペースや空白の行がないことを確認します。

ステップ 4 使用状況データをシスコに送信するかどうかを決定します。

- [Cisco Success Networkの有効化（Enable Cisco Success Network）] は、デフォルトで有効です。シスコによって収集されるデータの種類を表示するには、[サンプルデータ（sample data）] をクリックします。Cisco Success Network の情報ブロックを読むと、判断に役立ちます。
- （注）
  - 有効にすると、Cisco Support Diagnostics は、次の同期サイクルで Firepower Threat Defense（FTD）デバイスで有効になります。FTD と FMC との同期は、30 分ごとに 1 回実行されます。
  - 有効にすると、今後この FMC に登録される新しい FTD では、Cisco Support Diagnostics が自動的に有効になります。

ステップ 5 [変更を適用（Apply Changes）] をクリックします。

次のタスク

- Firepower Threat Defense デバイスを Firepower Management Center に追加します。Firepower Management Center へのデバイスの追加 （293 ページ）を参照してください。
- ライセンスを Firepower Threat Defense デバイスに割り当てます。複数の管理対象デバイスへのライセンスの割り当て （135 ページ）を参照してください。

輸出規制機能の有効化（グローバル権限のないアカウントの場合）

重要 この手順は、スマートアカウントに強力な暗号が承認されていない場合にのみ使用します。アカウントが承認されていない場合、またはわからない場合は輸出規制対象の機能のライセンス（108 ページ）を参照してください。

始める前に

- 展開でまだ輸出規制対象の機能がサポート**されていない**ことを確認します。

（注） 展開で輸出規制対象の機能がサポートされている場合、Cisco Smart Software Manager の [登録トークンの作成（Create Registration Token）] ページに輸出規制対象の機能を有効にできるオプションが表示されます。詳細については、https://www.cisco.com/c/en/us/buy/smart-accounts/software-manager.htmlを参照してください。

- 展開で評価ライセンスが使用されていないことを確認します。
- Cisco Smart Software Manager の **[インベントリ（Inventory）]** > **[ライセンス（Licenses）]** ページで、Firepower Management Center に対応するライセンスがあることを確認します。

輸出規制ライセンス	Firepower Management Center モデル
Cisco Virtual FMC シリーズの強力な暗号化（3DES/AES）	すべての仮想 Firepower Management Center
Cisco FMC 1K シリーズの強力な暗号化（3DES/AES）	750、1000、1500、1600
Cisco FMC 2 K シリーズの強力な暗号化（3DES/AES）	2000、2500、2600

輸出規制ライセンス	Firepower Management Center モデル
Cisco FMC 4K シリーズの強力な暗号化（3DES/AES）	3500、4000、4500、4600

ステップ 1 **[システム（System）] > [ライセンス（Licenses）] > [スマート ライセンス（Smart Licenses）]** を選択します。

（注） [輸出キーの要求（Request Export Key）] が表示されている場合は輸出規制対象の機能がアカウントに承認されています。そのため、必要な機能の使用に進むことができます。

ステップ 2 [エクスポート キーの要求（Request Export Key）] をクリックして、エクスポート キーを生成します。

ヒント エクスポート制御キーの要求に失敗した場合は、バーチャル アカウントに有効なエクスポート制御ライセンスがあることを確認します。

次のタスク

これで、輸出規制対象の機能を使用する設定またはポリシーを展開できるようになります。

メモ これによって有効にされた新しい輸出規制対象のライセンスとすべての機能は、Firepower Threat Defense デバイスが再起動されるまでそのデバイスでは有効になりません。それまでは、前のライセンスでサポートされていた機能のみがアクティブになります。

高可用性展開では、アクティブ/アクティブの状態を避けるために両方の Firepower Threat Defense デバイスを再起動する必要があります。

輸出規制対象の機能の無効化（グローバル権限のないアカウントの場合）

輸出規制機能の有効化（グローバル権限のないアカウントの場合） （115 ページ） で説明した機能を使用して輸出規制対象の機能を有効にした場合は、この手順を使用してこの機能を無効にできます。

ステップ 1 **[システム（System）] > [ライセンス（Licenses）] > [スマート ライセンス（Smart Licenses）]** を選択します。

これによって、このライセンスが開放されて仮想アカウント内の使用可能なライセンスのプールに戻り、再利用できるようになります。

ステップ 2 [輸出キーの返却（Return Export Key）] をクリックして、輸出規制ライセンスを無効にします。

エアギャップ展開のライセンスのオプション

次の表に、インターネットアクセスがない環境でのライセンスの展開に使用できるオプションを比較して示します。特定の状況については、販売担当者が他のアドバイスをできる場合があります。

表 4: エアギャップ ネットワークのライセンス オプションの比較

Smart Software Satellite Server	特定のライセンスの予約
大量の製品に対する拡張性	少数のデバイスに最適
ライセンス管理、使用状況、および資産管理の可視性を自動化	使用状況および資産管理の可視性の制限
デバイスを追加するための運用コストの増加なし	デバイスを追加するための経時的な運用コストが線形
柔軟性、使いやすさ、少ないオーバーヘッド	移動、追加、および変更の際の管理および手動によるオーバーヘッドの多さ
初期およびさまざまな期限切れ状態でコンプライアンス不適合ステータスが許可される	コンプライアンス不適合ステータスはシステムの動作に影響を与える
詳細については、Smart Software Satellite Server の概要 （117 ページ）を参照してください。	詳細については、特定のライセンスの予約の概要 （119 ページ）を参照してください。

Smart Software Satellite Server の概要

License Authority との定期通信 （100 ページ） の説明に従って、ライセンス権限を維持するため、システムは Cisco と定期的に通信する必要があります。次の状況のいずれかの場合、ライセンス認証局と接続するためのプロキシとして Smart Software Satellite Server を使用できます。

- Firepower Management Center がオフラインである、接続が制限されている、または接続がない（つまり、エアギャップ ネットワークに展開されている）場合。
- Firepower Management Center に固定接続があるが、ネットワークからの単一の接続によってスマート ライセンスを制御する場合。

スマート ソフトウェア サテライト サーバを使用すると、同期スケジュールを設定、またはスマート ライセンス認証を Smart Software Manager と手動で同期させることができます。

スマート ソフトウェア サテライト サーバの詳細については、https://www.cisco.com/c/en/us/buy/smart-accounts/software-manager-satellite.html を参照してください。

エアギャップ ネットワークの場合の代替ソリューションは特定ライセンスの予約です。詳細については、特定のライセンスの予約の概要 （119 ページ）を参照してください。

Smart Software Satellite Server の展開方法

始める前に

ネットワークがエアギャップの場合、Smart Software Satellite Server または特定ライセンスの予約が展開に最適なソリューションであるかどうかを判断します。詳細については、Smart Software Satellite Server の概要 （117 ページ）および特定のライセンスの予約の概要 （119 ページ）を参照してください。

ステップ 1 Smart Software Satellite Server を展開して設定します。

https://www.cisco.com/c/en/us/buy/smart-accounts/software-manager-satellite.htmlにある『*Smart Software Manager Satellite User Guide*』を参照してください。

ステップ 2 Firepower Management Center を Satellite に接続し、登録トークンを取得して、管理センターを Satellite に登録します。

Smart Software Satellite Server への接続の設定 （118 ページ）を参照してください。

ステップ 3 デバイスを管理対象に追加します。

Firepower Management Center へのデバイスの追加 （293 ページ）を参照してください。

ステップ 4 管理対象デバイスへのライセンスの割り当て

複数の管理対象デバイスへのライセンスの割り当て （135 ページ）を参照してください

ステップ 5 Satellite を Cisco Smart Software Management Server（CSSM）に同期させます。

上記で使用した『*Smart Software Manager Satellite User Guide*』を参照してください。

ステップ 6 継続的な同期時刻をスケジュールします。

Smart Software Satellite Server への接続の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	該当なし	Firepower Threat Defense	グローバルのみ	管理者

始める前に

- Smart Software Satellite Server を設定します。詳細については、Smart Software Satellite Server の展開方法 （118 ページ）を参照してください。
- サテライト サーバの TLS/SSL 証明書の CN をメモします。

- FMC が Smart Software Satellite Server に到達できることを確認します。たとえば、サテライト サーバの call-home URL として設定された FQDN が内部 DNS サーバによって解決できることを確認します。
- http://www.cisco.com/security/pki/certs/clrca.cer に移動し、TLS/SSL 証明書の本文全体（"-----BEGIN CERTIFICATE-----" から "-----END CERTIFICATE-----" まで）を、設定中にアクセスできる場所にコピーします。

ステップ 1 **[System]** > **[Integration]**を選択します。

ステップ 2 [Smart Software Satellite] タブをクリックします。

ステップ 3 [Cisco Smart Software Satellite Serverに接続（Connect to Cisco Smart Software Satellite Server）] を選択します。

ステップ 4 この手順の前提条件で収集した CN 値を使用して、Smart Software Satellite Server の **URL** を次の形式で入力します。

`https://FQDN_or_hostname_of_Satellite/Transportgateway/services/DeviceRequestHandler`

FQDN またはホスト名は、サテライトによって提示された証明書の CN 値と一致している必要があります。

ステップ 5 新しい [SSL証明書（SSL Certificate）] を追加し、この手順の前提条件でコピーした証明書テキストを貼り付けます。

ステップ 6 [適用（Apply）] をクリックします。

ステップ 7 [システム（System）] > [ライセンス（Licenses）] > [スマートライセンス（Smart Licenses）] を選択し、[登録（Register）] をクリックします。

ステップ 8 Smart Satellite Server で新しいトークンを作成します。

ステップ 9 トークンをコピーします。

ステップ 10 トークンを管理センター ページのフォームに貼り付けます。

ステップ 11 [変更を適用（Apply Changes）] をクリックします。

これで、管理センターが Smart Software Satellite Server に登録されました。

次のタスク

Smart Software Satellite Server の展開方法 （118 ページ）の残りの手順を実行します。

特定のライセンスの予約の概要

特定のライセンスの予約機能を使用して、エアギャップ ネットワークにスマート ライセンスを展開できます。

特定のライセンスの予約が有効になっている場合、Firepower Management Center は、Cisco Smart Software Manager または Smart Software サテライト サーバにアクセスせずに仮想アカウントからライセンスを予約します。

Firepower Management Center では、標準クラシック ライセンスを使用するデバイスを同時に管理することもできます。ただし、これらのデバイスは特定のライセンスの予約を使用しません。

インターネットへのアクセスが必要なパブリック Web サイトに対する URL ルックアップや状況に応じた相互起動などの機能は動作しません。

シスコは、特定のライセンスの予約を使用する展開に関する Web 分析やテレメトリのデータを収集しません。

関連トピック：

- 特定のライセンスの予約のベスト プラクティス （120 ページ）
- 特定のライセンスの予約の要件 （120 ページ）
- 特定のライセンスの予約の実装方法 （120 ページ）
- 特定のライセンスの予約ステータス （130 ページ）
- 特定のライセンスの予約の更新 （127 ページ）
- 特定のライセンスの予約の非アクティブ化と返却 （131 ページ）
- 特定のライセンスの予約のトラブルシューティング （133 ページ）

特定のライセンスの予約のベスト プラクティス

特定のライセンスの予約を正常に実装するには、このドキュメントを必ず読んでください。

試行が失敗した場合は TAC に連絡する必要が生じる可能性があります。

問題を避けるには、前提条件や確認手順を含めて、手順に慎重に従ってください。

特定のライセンスの予約の要件

特定のライセンスの予約の使用状況は、シスコによる承認と認証が必要です。

特定のライセンスの予約の前提条件 （121 ページ）も参照してください。

特定のライセンスの予約の実装方法

	操作手順	詳細情報
ステップ 1	この機能の前提条件を満たします。	特定のライセンスの予約の前提条件 （121 ページ）

	操作手順	詳細情報
ステップ 2	スマートアカウントで特定のライセンスの付与資格を展開する準備が整っていることを確認します。	スマート アカウントが特定のライセンスの予約の展開の準備が整っているかどうかの確認 （122 ページ）
ステップ 3：	Firepower Management Center を使用して特定のライセンスの予約を有効にします。	[特定のライセンス（Specific Licenses）] メニュー オプションの有効化 （123 ページ）
ステップ 4：	Firepower Management Center から予約要求コードを生成します。	Firepower Management Center からの予約要求コードの生成 （124 ページ）
ステップ 5：	予約要求コードを使用して、Cisco Smart Software Manager から予約承認コードを生成します。	Cisco Smart Software Manager からの予約承認コードの生成 （124 ページ）
ステップ 6：	Firepower Management Center に予約承認コードを入力します。	Firepower Management Center に予約承認コードを入力します。 （125 ページ）
ステップ 7	特定のライセンスを管理対象の Firepower Threat Defence デバイスに割り当てます。	管理対象デバイスへの特定のライセンスの割り当て （126 ページ）
ステップ 9	（Firepower Management Center 外）進行中のメンテナンス タスクのリマインダのスケジュールを設定します。	エアギャップ展開の維持 （197 ページ）

特定のライセンスの予約の前提条件

- スマート アカウントをセットアップします。

  ライセンスを保持するためのスマートアカウントの作成（110ページ）を参照してください。

- Firepower Management Center で標準スマート ライセンスを現在使用している場合は、特定のライセンスの予約を実装する前に Firepower Management Center の登録を解除します。詳細については、Cisco Smart Software Manager から Firepower Management Center の登録解除（140 ページ）を参照してください。

  Firepower Management Center に現在展開されているすべてのスマート ライセンスがアカウントで使用可能なライセンスのプールに戻され、特定のライセンスの予約を実装すると再利用できるようになります。

- 特定のライセンスの予約には、標準スマートライセンスと同じ数およびタイプのライセンスが必要です。展開するデバイスと機能に必要な標準ライセンスとサービスサブスクリプションの数を特定します。必要に応じて、Firepower Management Center Virtual の付与資格を含めてください。

  Firepower のライセンスとサービス サブスクリプションについては、スマート ライセンスのタイプと制約事項 （101 ページ）およびそのサブトピック（特にFirepower Management Center Virtual ライセンス （94 ページ））を参照してください。

- 必要なライセンスを購入します。
- 必要であり、組織にその付与資格がある場合は、輸出規制対象の強力な暗号化機能を手配します。アカウントでその機能が使用できること、または必要な Firepower Management Centerの事前ライセンスが仮想アカウントに表示されていることを確認します。アカウント担当者がサポートします。

  詳細については、輸出規制対象の機能のライセンス （108 ページ）を参照してください。

- Firepower製品の特定ライセンス予約（SLR）の承認を得るため、アカウント担当者が協力いたします。
- 特定のライセンスの予約が使用できる状態になっており、スマートアカウントに反映されていることをアカウント担当者に確認してください。
- 管理対象デバイスを Firepower Management Center に追加します。この説明については、Firepower Management Center へのデバイスの追加 （293 ページ）を参照してください。（管理対象デバイスはいつでも追加できますが、今追加すると、このプロセスが簡単になります。）これを実行するには、評価ライセンスを有効にする必要があります（[システム（System）] から [ライセンス（Licenses）] > [スマート ライセンス（Smart Licenses）]）。評価ライセンスは、ライセンス認証局への接続を必要としません。
- （推奨）高可用性構成で Firepower Management Center ペアを展開する場合は、ライセンスを割り当てる前にその設定をします（高可用性構成の FMC で必要なライセンスの数は、単一の FMC の場合と同じです）。すでにセカンダリ アプライアンスにライセンスを展開している場合は、そのアプライアンスからライセンスを登録解除します。

スマート アカウントが特定のライセンスの予約の展開の準備が整っているかどうかの確認

特定のライセンスの予約の展開時の問題を防ぐため、Firepower Management Center に変更を加える前にこの手順を実行します。

始める前に

- 特定のライセンスの予約の前提条件 （121 ページ）で説明した要件を満たしていることを確認します。
- Cisco Smart Software Manager のクレデンシャルがあることを確認します。

ステップ 1 Cisco Smart Software Manager にサインインします。

https://software.cisco.com/#SmartLicensing-Inventory

ステップ 2 必要に応じて、[インベントリ（Inventory）] をクリックします。

ステップ 3 [ライセンス（Licenses）] タブをクリックします。

ステップ 4 次のことを確認してください。

- [ライセンスの予約（License Reservation）] ボタンが表示されている。
- 該当する場合は、デバイスの Firepower Management Center Virtual の付与資格を含めて展開するデバイスおよび機能に十分なプラットフォーム ライセンスと機能ライセンスがある。

ステップ 5 これらのアイテムがないか、または誤っている場合は、アカウント担当者に連絡して問題を解決します。

重要 問題が修正されるまではこのプロセスは続行**しないでください**。

[特定のライセンス（Specific Licenses）] メニュー オプションの有効化

Specific License	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	Firepower Management Center	グローバルだけ	管理者

この手順では、Firepower Management Center の [スマート ライセンス（Smart Licenses）] メニュー オプションを [特定のライセンス（Specific Licenses）] に変更します。

ステップ 1 USB キーボードと VGA モニタを使用して Firepower Management Center コンソールにアクセスするか、または SSH を使用して管理インターフェイスにアクセスします。

ステップ 2 Firepower Management Center の **admin** アカウントにログインします。デフォルトでは、これによって Linux シェルへのアクセス権が付与されます。Firepower Management Center の CLI が有効になっている場合は、これによってコマンド ライン インターフェイスへのアクセス権が付与されます。

ステップ 3 CLI が有効になっている Firepower Management Center の場合は、**expert** コマンドを入力して Linux シェルにアクセスします。

ステップ 4 特定のライセンスの予約のオプションにアクセスするには、次のコマンドを実行します。

sudo manage_slr.pl

例：

```
admin@fmc63betaslr: ~$ sudo manage_slr.pl
Password:


*************** Configuration Utility **************

1   Show SLR Status
2   Enable SLR
3   Disable SLR
0   Exit
```

```
************************************************************
Enter choice:
```

ステップ 5 オプション 2 を選択して、Specific License Reservation を有効にします。

ステップ 6 オプション 0 を選択して manage_slr ユーティリティを終了します。

ステップ 7 **exit** と入力し、Linux シェルを終了します。

ステップ 8 CLI が有効になっている Firepower Management Center では、入力 **exit**してコマンドライン インターフェイスを終了します。

ステップ 9 Firepower Management Center の Web インターフェイスの [特定のライセンスの予約（Specific License Reservation）] ページにアクセスできることを確認します。

- [システム（System）] > [ライセンス（Licenses）] > [スマート ライセンス（Smart Licenses）] ページが現在表示されている場合は、ページを更新します。
- それ以外の場合は、[システム（System）] > [ライセンス（Licenses）] > [特定のライセンス（Specific Licenses）] を選択します。

Firepower Management Center からの予約要求コードの生成

Specific License	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	Firepower Management Center	グローバルだけ	管理者

ステップ 1 [特定のライセンスの予約（Specific License Reservation）] ページが表示されていない場合は、[システム（System）] > [ライセンス（Licenses）] > [特定のライセンス（Specific Licenses）] を選択します。

ステップ 2 [生成（Generate）] をクリックします。

ステップ 3 **予約要求コード**をメモします。

Cisco Smart Software Manager からの予約承認コードの生成

ステップ 1 Cisco Smart Software Manager に移動します。

https://software.cisco.com/#SmartLicensing-Inventory

ステップ 2 必要に応じて、[インベントリ（Inventory）] をクリックします。

(このページは自動的に表示されることがあります。)

ステップ 3 [ライセンス（Licenses）] タブをクリックします。

ステップ 4 [ライセンスの予約（License Reservation）] をクリックします。

ステップ 5 生成したコードを Firepower Management Center から [予約要求コード（Reservation Request Code）] ボックスに入力します。

ステップ 6 [次へ（Next）] をクリックします。

ステップ 7 [特定のライセンスの予約（Reserve a specific license）] を選択します。

ステップ 8 下にスクロールしてライセンス グリッド全体を表示します。

ステップ 9 [予約する数量（Quantity To Reserve）] に、展開に必要な各プラットフォームと機能の数を入力します。

重要

- 管理対象デバイスごとに **Firepower Threat Defense Base Features** ライセンスを、マルチインスタンス展開の場合は **Firepower Threat Defense ベース機能**ライセンスを明示的に含める必要があります。
- 仮想管理センターを使用している場合は、各モジュール（マルチインスタンス展開）か、または各管理対象デバイス（その他のすべての展開）に **Firepower MCv デバイス ライセンス**の資格を組み込む必要があります。
- 強力な暗号化機能を使用する場合：
  - スマート アカウント全体が輸出規制対象機能に対して有効になっている場合は、ここで何もする必要はありません。
  - 組織の資格が Firepower Management Center 単位の場合は、アプライアンス向けに適切なライセンスを選択する必要があります。

  デバイスに適切なライセンス名を選択するには、輸出規制機能の有効化（グローバル権限のないアカウントの場合） （115 ページ）の前提条件を参照してください。

ステップ 10 [次へ（Next）] をクリックします。

ステップ 11 [承認コードを生成（Generate Authorization Code）] をクリックします。

この時点で、ライセンスは、Smart Software Manager に従って使用中です。

ステップ 12 Firepower Management Center に入力するための準備として承認コードをダウンロードします。

Firepower Management Center に予約承認コードを入力します。

Specific License	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	Firepower Management Center	グローバルだけ	管理者

ステップ 1 [特定のライセンスの予約（Specific License Reservation）] ページが表示されていない場合は、Firepower Management Center の Web インターフェイスで [システム（System）] > [ライセンス（Licenses）] > [特定のライセンス（Specific Licenses）] を選択します。

ステップ 2 [参照（Browse）] をクリックして、承認コード ファイル（.txt）をアップロードします。

ステップ 3 [Install（インストール）] をクリックします。

ステップ 4 [特定のライセンスの予約（Specific License Reservation）] ページに [使用の承認（Usage Authorization）] ステータスが [承認済み（authorized）] と表示されていることを確認します。

ステップ 5 [予約済みライセンス（Reserved Licenses）] タブをクリックして、[承認コード（Authorization Code）] の生成時に選択したライセンスを確認します。

必要なライセンスが表示されていない場合は、必要なライセンスを追加します。詳細については、「特定のライセンスの予約の更新」を参照してください。

管理対象デバイスへの特定のライセンスの割り当て

Specific License	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	Firepower Management Center	グローバルだけ	管理者

この手順を使用して、複数の管理対象デバイスにライセンスを一度にすばやく割り当てます。

また、この手順を使用してライセンスを無効にするか、または 1 つの Firepower Threat Defense デバイスから別のデバイスに移動できます。デバイスのライセンスを無効にすると、ライセンスに関連付けられた機能をそのデバイスで使用できません。

ステップ 1 [システム（System）] > [ライセンス（Licenses）] > [個別ライセンス（Specific Licenses）] を選択します。

ステップ 2 [ライセンスの編集（Edit Licenses）] をクリックします。

ステップ 3 各タブをクリックし、必要に応じてデバイスにライセンスを割り当てます。

ステップ 4 [適用（Apply）] をクリックします。

ステップ 5 [割り当て済みのライセンス（Assigned Licenses）] タブをクリックし、各デバイスでライセンスが正しくインストールされていることを確認します。

次のタスク

- 輸出規制対象の機能が有効になっている場合は、各デバイスを再起動します。高可用性ペアにデバイスが設定されている場合、両方のデバイスを同時に再起動してアクティブ/アクティブの状態を回避します。
- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

特定のライセンスの予約の更新

Specific License	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	Firepower Management Center	グローバルだけ	管理者

Firepower Management Center で特定のライセンスが正常に展開された後は、この手順を使用して付与資格をいつでも追加または削除できます。

ステップ 1 Firepower Management Center で、このアプライアンスの一意の製品インスタンス識別子を取得します。

a) [システム（System）] > [ライセンス（Licenses）] > [特定のライセンス（Specific Licenses）] を選択します。

b) [製品インスタンス（Product Instance）] の値をメモします。

この値はこのプロセス中に何度か必要になります。

ステップ 2 Cisco Smart Software Manager で、更新する Firepower Management Center のアプライアンスを識別します。

a) Cisco Smart Software Manager に移動します。

https://software.cisco.com/#SmartLicensing-Inventory

b) 必要に応じて、[インベントリ（Inventory）] をクリックします。

(このページは自動的に表示されることがあります。)

c) [製品インスタンス（Product Instances）] タブをクリックします。

d) [タイプ（Type）] 列に **FP**、[名前（Name）] 列に一般的な SKU（ホスト名ではない）が設定されている製品インスタンスを探します。また他のテーブル列の値を使用すると、どの Firepower Management Center が正しい Firepower Management Center かを判断するのに役立ちます。名前をクリックします。

e) **UUID** を調べ、変更しようとしている Firepower Management Center の UUID かどうかを確認します。

違う場合は、正しい Firepower Management Center が見つかるまで、これらの手順を繰り返す必要があります。

ステップ 3 Cisco Smart Software Manager で適切な Firepower Management Center アプライアンスが見つかったら、予約したライセンスを更新し、新しい承認コードを生成します。

a) 正しい UUID が表示されているページで、[アクション（Actions）] > [予約済みのライセンスの更新（Update Reserved Licenses）] を選択します。

b) 必要に応じて、予約済みライセンスを更新します。

重要

- 管理対象デバイスごとに **Firepower Threat Defense Base Features** ライセンスを、マルチインスタンス展開の場合は **Firepower Threat Defense ベース機能**ライセンスを明示的に含める必要があります。
- 仮想管理センターを使用している場合は、各モジュール（マルチインスタンス展開）か、または各管理対象デバイス（その他のすべての展開）に **Firepower MCv デバイス ライセンス**の資格を組み込む必要があります。
- 強力な暗号化機能を使用する場合：
  - スマート アカウント全体が輸出規制対象機能に対して有効になっている場合は、ここで何もする必要はありません。
  - 組織の資格が Firepower Management Center 単位の場合は、アプライアンス向けに適切なライセンスを選択する必要があります。

    デバイスに適切なライセンス名を選択するには、輸出規制機能の有効化（グローバル権限のないアカウントの場合）（115 ページ）の前提条件を参照してください。

c) [次へ（Next）] をクリックして詳細を確認します。
d) [承認コードを生成（Generate Authorization Code）] をクリックします。
e) Firepower Management Center に入力するための準備として承認コードをダウンロードします。
f) [予約の更新（Update Reservation）] ページを開いたままにしておきます。この手順の後半でこのページに戻ります。

ステップ 4 Firepower Management Center での特定のライセンスを更新するには、次の手順を実行します。

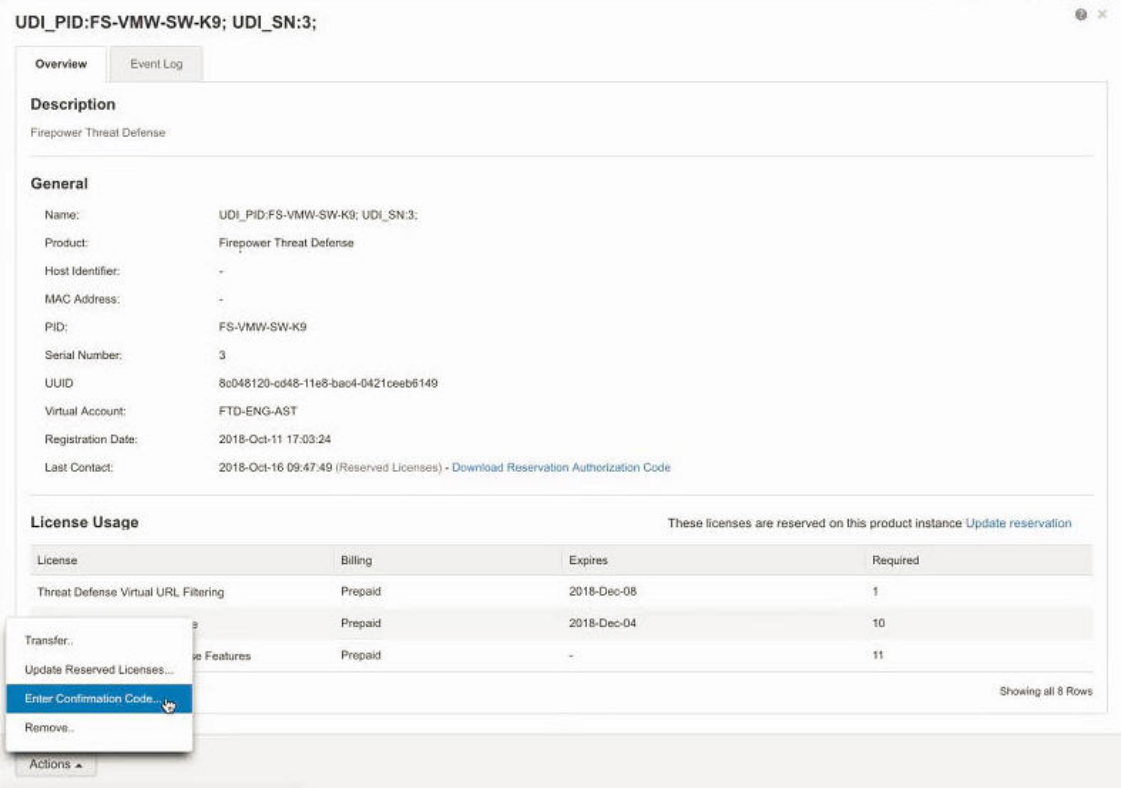
a) [システム（System）] > [ライセンス（Licenses）] > [特定のライセンス（Specific Licenses）] を選択します。
b) [SLR の編集（Edit SLR）] をクリックします。
c) [参照（Browse）] をクリックして、新たに生成された承認コードをアップロードします。
d) [インストール（Install）] をクリックしてライセンスを更新します。

   承認コードが正常にインストールされたら、Firepower Management Center の [予約済み（Reserved）] 列に表示されたライセンスが、Cisco Smart Software Manager で予約したライセンスと一致していることを確認します。

e) **確認コード**をメモします。

ステップ 5 Cisco Smart Software Manager に承認コードを入力するには、次の手順を実行します。

a) この手順の前半で開いたままにしておいた Cisco Smart Software Manager のページに戻ります。
b) [アクション（Actions）] > [確認コードの入力（Enter Confirmation Code）] を選択します。



c) Firepower Management Center から生成したコードを入力します。

ステップ 6 Firepower Management Center で、ライセンスが予期したとおりに予約されていること、および各管理対象デバイスの各機能にチェックマークが付いた緑色の丸（）が表示されていることを確認します。

必要に応じて、詳細については特定のライセンスの予約ステータス （130 ページ）を参照してください。

次のタスク

展開に輸出規制対象の機能が含まれている場合は各デバイスを再起動します。高可用性ペアにデバイスが設定されている場合、両方のデバイスを同時に再起動してアクティブ/アクティブの状態を回避します。

設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

重要：SLR 展開の維持

展開を有効に保つ脅威に関するデータとソフトウェアを更新するには、エアギャップ展開の維持 （197 ページ）を参照してください。

すべての機能が中断せずに動作し続けるようにするには、ライセンスの有効期限を（[予約済みライセンス（Reserved Licenses）] タブ）で監視します。

特定のライセンスの予約ステータス

次に示すように、[システム（System）]>[Licenses（ライセンス）]>[特定のライセンス（Specific Licenses）] ページには Firepower Management Center でのライセンスの使用状況の概要が表示されます。

使用の認証

可能なステータス値は次のとおりです。

- [承認済み（Authorized）]：Firepower Management Center は、アプライアンスのライセンスの付与資格を承認したライセンス認証局に準拠しており、正常に登録されています。
- [コンプライアンス不適合（Out-of-compliance）]：ライセンスの期限が切れているか、または Firepower Management Center が予約していないにもかかわらずライセンスを過剰に使用している場合、[コンプライアンス不適合（Out-of-Compliance）] がステータスに表示されます。[特定のライセンスの予約（Specific License Reservation）] にライセンスの付与資格が適用されるため、アクションを実行する必要があります。

製品登録

特定の登録ステータスと、Firepower Management Center で承認コードが最後にインストールされたか、または更新された日付を指定します。

輸出管理機能

Firepower Management Center の輸出規制対象機能を有効にしたかどうかを指定します。

輸出規制対象機能の詳細については、輸出規制対象の機能のライセンス （108 ページ）を参照してください。

製品インスタンス

この Firepower Management Center のユニバーサル一意識別子 (UUID)。この値は Cisco Smart Software Manager でこのデバイスを識別します。

確認コード

特定のライセンスを更新するか、または非アクティブ化して返却する場合に [確認コード（Confirmation Code）] が必要です。

[割り当て済みライセンス（Assigned Licenses）] タブ

各デバイスとそれぞれのステータスに割り当てられているライセンスを表示します。

[予約済みライセンス（Reserved Licenses）] タブ

割当に使用されているライセンスと使用可能なライセンスの数、およびライセンスの有効期限を表示します。

期限切れと特定のライセンスの予約

必要なライセンスが使用できないか、または期限が切れている場合、次のアクションは制限されています。

- デバイス登録に使用
- ポリシーの展開

特定のライセンスの予約の資格を更新するには、必要なライセンスを購入し、特定のライセンスの予約の更新 （127 ページ）の手順を実行します。

特定のライセンスの予約資格の更新

特定のライセンスの予約資格を更新する時期になったら、必要なライセンスを購入し、特定のライセンスの予約の更新 （127 ページ）の手順を実行します。

特定のライセンスの予約の非アクティブ化と返却

特定のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	Firepower Management Center	グローバルのみ	管理者

特定のライセンスが不要になった場合は、そのライセンスをスマートアカウントに戻す必要があります。

重要 この手順のすべてのステップを実行しないと、ライセンスは使用中の状態のままとなり、再利用できません。

この手順で、Firepower Management Center と関連付けられていたすべてのライセンスの付与資格が仮想アカウントに開放されます。登録を解除すると、ライセンスが付与された機能への更新や変更が許可されなくなります。

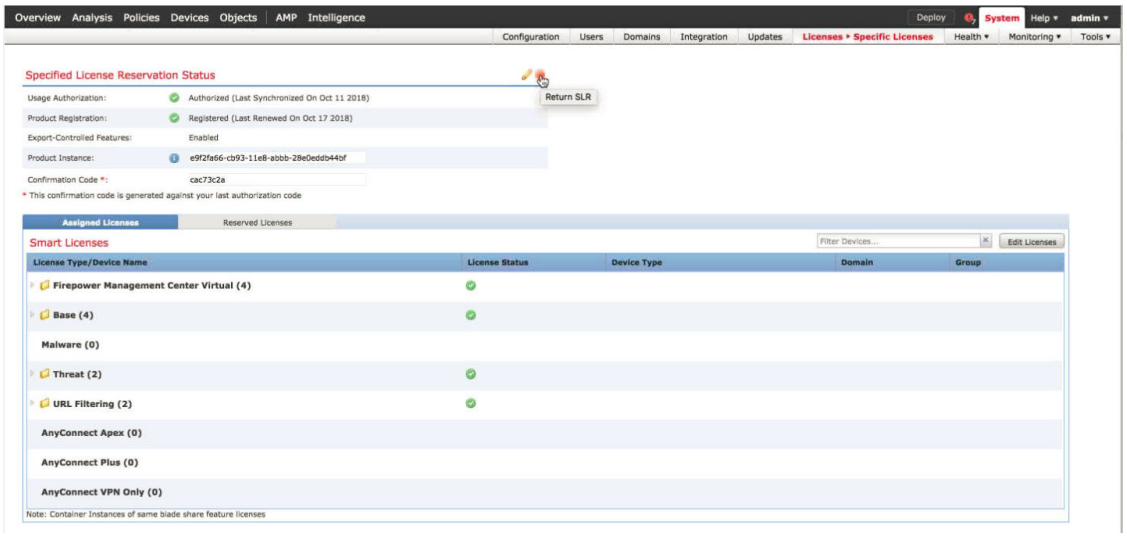
ステップ 1 Firepower Management Center の Web インターフェイスで、[システム（System）]>[ライセンス（Licenses）]>[特定のライセンス（Specific License）] を選択します。

ステップ 2 この Firepower Management Center の [製品インスタンス（Product Instance）] の識別子をメモします。

ステップ 3 Firepower Management Center から返却コードを生成するには、次の手順を実行します。

a) [SLR の返却（Return SLR）]] ボタンをクリックします。

次の図に、[SLR の返却（Return SLR）] ボタンを示します。



Firepower Threat Defense デバイスのライセンスが無効になり、Firepower Management Center が登録解除の状態に移行します。

b) **返却コード**をメモします。

ステップ 4 Cisco Smart Software Manager で、登録を解除する Firepower Management Center のアプライアンスを識別します。

a) Cisco Smart Software Manager に移動します。

https://software.cisco.com/#SmartLicensing-Inventory

b) 必要に応じて、[インベントリ（Inventory）] をクリックします。

(このページは自動的に表示されることがあります。)

c) [製品インスタンス（Product Instances）] タブをクリックします。

d) [タイプ（Type）] 列に **FP**、[名前（Name）] 列に一般的な SKU（ホスト名ではない）が設定されている製品インスタンスを探します。また他のテーブル列の値を使用すると、どの Firepower Management Center が正しい Firepower Management Center かを判断するのに役立ちます。名前をクリックします。

e) **UUID** を調べ、変更しようとしている Firepower Management Center の UUID かどうかを確認します。

違う場合は、正しい Firepower Management Center が見つかるまで、これらの手順を繰り返す必要があります。

ステップ 5 正しい Firepower Management Center が特定されたら、ライセンスをスマート アカウントに戻します。

a) 正しい UUID が表示されたページで、[アクション（Actions）] > [削除（Remove）] を選択します。

b) Firepower Management Center から生成した予約返却コードを [製品インスタンスの削除（Remove Product Instance）] ダイアログボックスに入力します。

c) [製品インスタンスの削除（Remove Product Instance）] をクリックします。

特定の予約済みライセンスがスマート アカウントの使用可能プールに戻り、この Firepower Management Center が Cisco Smart Software Manager の製品インスタンス リストから削除されます。

ステップ 6 Firepower Management Center の Linux シェルで、特定のライセンスを無効にします。

a) USB キーボードと VGA モニタを使用して Firepower Management Center コンソールにアクセスするか、または SSH を使用して管理インターフェイスにアクセスします。

b) Firepower Management Center の **admin** アカウントにログインします。デフォルトでは、これによって Linux シェルへのアクセス権が付与されます。Firepower Management Center の CLI が有効になっている場合は、これによってコマンドライン インターフェイスへのアクセス権が付与されます。

c) CLI が有効になっている Firepower Management Center の場合は、**expert** コマンドを入力して Linux シェルにアクセスします。

d) makecall ディレクトリで、次のコマンドを実行します。

```
sudo manage_slr.pl
```

例：

```
admin@fmc63betaslr: ~$ sudo manage_slr.pl
Password:


*************** Configuration Utility *************

1   Show SLR Status
2   Enable SLR
3   Disable SLR
0   Exit

************************************************************
Enter choice:
```

e) オプション 3 を選択して、特定のライセンスの予約を無効にします。

f) オプション 0 を選択して manage_slr ユーティリティを終了します。

g) **exit** と入力し、Linux シェルを終了します。

h) CLI が有効になっている Firepower Management Center では、入力 **exit** してコマンドライン インターフェイスを終了します。

特定のライセンスの予約のトラブルシューティング

Cisco Smart Software Manager の製品インスタンス リストから特定の Firepower Management Center を識別する方法を教えてください。

Cisco Smart Software Manager の [製品インスタンス（Product Instances）] ページで、テーブル内の列のいずれかの値に基づいて製品インスタンスが識別できない場合は、**FP** タイプの汎用製品インスタンスそれぞれの名前をクリックする必要があります。このページの **UUID** の値は 1 つの Firepower Management Center を一意に識別します。

Firepower Management Center の Web インターフェイスでは、Firepower Management Center の UUID は [システム（System）] > [ライセンス（Licenses）] > [特定のライセンス（Specific License）] ページに表示される [製品インスタンス（Product Instance）] の値です。

Cisco Smart Software Manager の [ライセンスの予約（License Reservation）] ボタンが表示されません。

[ライセンス予約（License Reservation）] ボタンが表示されない場合、お使いのアカウントでは個別ライセンスの予約が承認されていません。Linux シェルで特定のライセンスの予約をすでに有効にし、要求コードを生成している場合は、次の手順を実行します。

1. Firepower Management Center の Web インターフェイスですでに**要求コード**を生成している場合は、その要求コードをキャンセルします。
2. 「特定のライセンスの予約の非アクティブ化と返却（131 ページ）」のセクションで説明しているように、Firepower Management Center の Linux シェルで特定のライセンスの予約を無効にします。
3. スマート トークンを使用して、通常モードで Firepower Management Center を Cisco Smart Software Manager に登録します。
4. Cisco TAC に連絡して、自分のスマート アカウントの個別ライセンスを有効にします。

ライセンス プロセスの最中に中断が発生しました。中断した場所を取得する方法を教えてください。

承認コードは生成したが、Cisco Smart Software Manager からまだダウンロードしていない場合は、Cisco Smart Software Manager の [製品インスタンス（Product Instance）] ページに移動し、製品インスタンスをクリックした後、[予約承認コードのダウンロード（Download Reservation Authorization Code）] をクリックします。

Firepower Threat Defense デバイスをFirepower Management Center Virtual に登録できません。

登録するデバイスをカバーするのに十分な MCv の資格がスマート アカウントにあることを確認してから展開を更新し、必要な資格を追加します。

特定のライセンスの予約の更新（127 ページ）を参照してください。

特定のライセンスを有効にしていましたが、[スマート ライセンス（Smart License）] ページが表示されなくなりました。

これは予期されている動作です。[特定のライセンス（Specific Licensing）] を有効にすると、スマート ライセンスは無効になります。[特定のライセンス（Specific License）] ページを使用してライセンスの操作を実行できます。

スマート ライセンスを使用する場合は、特定のライセンスを返却する必要があります。詳細については、特定のライセンスの予約の非アクティブ化と返却（131 ページ）を参照してください。

Firepower Management Center に [特定のライセンス（Specific License）] ページが表示されません。

[特定のライセンス（Specific License）] ページを表示するには、特定のライセンスを有効にする必要があります。詳細については、[特定のライセンス（Specific Licenses）] メニュー オプションの有効化 （123 ページ）を参照してください。

特定のライセンスを無効にしましたが、返却コードをコピーするのを忘れてしまいました。どうすればよいでしょうか。

[戻りコード（Return Code）] は Firepower Management Center に保存されています。Linux シェルから特定のライセンスをもう一度有効にし（「[特定のライセンス（Specific Licenses）] メニュー オプションの有効化 （123 ページ）」を参照）、Firepower Management Center の Web インターフェイスを更新します。[戻りコード（Return Code）] が表示されます。

複数の管理対象デバイスへのライセンスの割り当て

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	該当なし	Firepower Threat Defense	グローバルのみ	管理者

Firepower Management Center によって管理されるデバイスは、ライセンスを、Cisco Smart Software Manager から直接ではなく Firepower Management Center 経由で取得します。

複数の Firepower Threat Defense デバイスでスマート ライセンスまたは特定のライセンスを一度に有効にするには、次の手順を実行します。

（注） 同じ セキュリティ モジュール/エンジン のコンテナ インスタンスの場合は、ライセンスを各インスタンスに適用します。ただし、セキュリティ モジュール/エンジン のすべてのインスタンスについては、セキュリティ モジュール/エンジン は機能ごとに 1 つのライセンスのみを使用します。

（注） FTD クラスタの場合は、クラスタ全体にライセンスを適用します。ただし、クラスタ内の各ユニットが機能ごとに個別のライセンスを使用します。

始める前に

- まだ割り当てていない場合、Firepower Management Center でデバイスを登録します。Firepower Management Center へのデバイスの追加 （293 ページ）を参照してください。
- 管理対象デバイスに配布するためのライセンスを準備するには、次を参照してくださいスマート ライセンスの登録 （113 ページ）

ステップ 1 **[System]** > **[Licenses]** > **[Smart Licenses]** または [特定のライセンス（Specific Licenses）] を選択します。

ステップ 2 [ライセンスの編集（Edit Licenses）] をクリックします。

ステップ 3 デバイスに追加するライセンスのタイプごとに、次の手順を実行します。

a) 該当するライセンスのタイプのタブをクリックします。

b) 左側のリスト内のデバイスをクリックします。

c) [追加（Add）] をクリックして、デバイスを右側のリストに移動させます。

d) 各デバイスが該当するタイプのライセンスを受信するまで、この手順をデバイスごとに繰り返します。

ここでは、追加するすべてのデバイスのライセンスをユーザが保持しているかどうかを気にする必要はありません。

e) 追加するライセンスのタイプごとに、この手順を繰り返します。

f) [適用（Apply）] をクリックします。

次のタスク

- ライセンスが正しくインストールされていることを確認します。スマート ライセンスおよびスマート ライセンス ステータスの表示 （136 ページ） の手順に従います。
- 輸出規制対象の機能が新たに有効になった場合は、各デバイスを再起動します。高可用性ペアにデバイスが設定されている場合、両方のデバイスを同時に再起動してアクティブ/アクティブの状態を回避します。
- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

スマート ライセンスおよびスマート ライセンス ステータスの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	該当なし	Firepower Threat Defense	グローバルのみ	管理者

[スマート ライセンス（Smart Licenses）] ページで、Firepower Management Center とその管理対象 Firepower Threat Defense デバイスのスマート ライセンスを表示します。このページには、展開におけるライセンスのタイプごとに、使用されているライセンスの総数、そのライセンスのコンプライアンスの適合または不適合の状態、デバイス タイプ、およびデバイスが展開されているドメインとグループが表示されます。また、Firepower Management Center のスマート ライセンス ステータスを表示できます。同じ セキュリティ モジュール/エンジン 上の コンテナ インスタンスは セキュリティ モジュール/エンジン ごとに 1 つのライセンスを使用します。したがって、ライセンス タイプごとに各コンテナ ライセンスが個別に FMC に表示されても、機能ライセンス タイプに使用されているライセンスの数は 1 つのみです。

[スマート ライセンス（Smart Licenses）] ページ以外にも、ライセンスを表示できる方法がいくつかあります。

- [製品ライセンス（Product Licensing）] ダッシュボード ウィジェットはライセンスの概要を示します。

  ダッシュボードへのウィジェットの追加 （340 ページ）、ユーザ ロール別のダッシュボード ウィジェットの可用性 （324 ページ）、および[製品ライセンス（Product Licensing）] ウィジェット （336 ページ）を参照してください。

- [デバイス管理（Device Management）] ページ（**[Devices]** > **[Device Management]**）は、各管理対象デバイスに適用されているライセンスをリストします。
- ヘルス ポリシーで使用される際に、スマート ライセンス モニタのヘルス モジュールはライセンス ステータスを伝達します。

ステップ 1 **[System]** > **[Licenses]** > **[Smart Licenses]**を選択します。

ステップ 2 [スマート ライセンス（Smart Licenses）] テーブルで、各 [ライセンス タイプ（License Type）] フォルダの左側にある矢印をクリックしてそのフォルダを展開します。

ステップ 3 各フォルダで、各デバイスの [ライセンス ステータス（License Status）] 列にチェックマーク付きの緑の円（）が表示されていることを確認します。

（注） Firepower Management Center 仮想ライセンスが重複している場合は、それぞれが 1 つの管理対象デバイスを表します。

すべてのデバイスにチェックマーク付きの緑の円（）が表示されている場合、デバイスには適切なライセンスがあり、使用できる状態にあります。

チェックマーク付きの緑の円（）以外のライセンス ステータスが表示されている場合は、ステータス アイコンにマウスオーバーしてメッセージを確認します。

次のタスク

- チェックマーク付きの緑の円（）が表示されているデバイスがない場合は、追加ライセンスの購入が必要な可能性があります。

スマート ライセンスのステータス

[システム（System）] > [ライセンス（Licenses）] > [スマート ライセンス（Smart Licenses）] ページの [スマート ライセンスのステータス（Smart License Status）] セクションでは、次に示すとおり、Firepower Management Center でのライセンスの使用状況の概要が提供されます。

使用の認証

可能なステータス値は次のとおりです。

- [コンプライアンス適合（In-compliance）]：管理対象デバイスに割り当てられているすべてのライセンスが要求を満たしており、 Firepower Management Center がシスコのライセンス認証局と正常に通信しています。
- ：デバイスのライセンスは要求を満たしていますが、Firepower Management Center がシスコのライセンス認証局と通信できません。
- [コンプライアンス不適合（Out-of-compliance）]またはライセンス認証局と通信できない：1 つ以上の管理対象デバイスがコンプライアンス不適合のライセンスを使用しているか、Firepower Management Center がシスコのライセンス認証局と通信していない期間が 90 日を超えています。

製品登録

Firepower Management Center がライセンス認証局に連絡し登録された最終日を指定します。

割当済みの仮想アカウント

製品インスタンス登録トークンの生成に使用したスマートアカウントの下の仮想アカウントを指定し、Firepower Management Center を登録します。この展開がスマート アカウント内の特定の仮想アカウントに関連付けられていない場合は、この情報は表示されません。

輸出管理機能

このオプションが有効になっている場合、制限機能を展開できます。詳細は、輸出規制対象の機能のライセンス （108 ページ）を参照してください。

Cisco Success Network

Firepower Management Centerの Cisco Success Network を有効にしたかどうかを指定します。このオプションを有効にすると、テクニカルサポートを提供するために不可欠な使用状況に関する情報と統計がシスコに提供されます。また、この情報により、シスコは製品を向上させ、未使用の使用可能な機能を認識させるため、ネットワーク内にある製品の価値を最大限に生かすことができます。詳細については、「Cisco Success Network （162 ページ）」を参照してください。

管理対象デバイスからのスマート ライセンスの移動または削除

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	該当なし	Firepower Threat Defense	グローバルのみ	管理者

1 つの Firepower Threat Defense デバイスから、同じ Firepower Management Center に登録されている別のデバイスにライセンスを移動するか、またはそのデバイスからライセンスを削除するには、次の手順を実行します。デバイスのライセンスを削除（無効化）すると、そのライセンスに関連付けられた機能をそのデバイスで使用できなくなります。

重要 別の Firepower Management Centerで管理されているデバイスにライセンスを移動する必要がある場合は、別の にスマート ライセンスを転送します。 Firepower Management Center （139 ページ）を参照してください。

ステップ 1 **[System]** > **[Licenses]** > **[Smart Licenses]**を選択します。

ステップ 2 [ライセンスの編集（Edit Licenses）] をクリックします。

ステップ 3 [マルウェア（Malware）]、[脅威（Threat）]、[URL フィルタリング（URL Filtering）]、[AnyConnect Plus]、[AnyConnect Apex]、または [AnyConnect VPN のみ（AnyConnect VPN Only）] のいずれかのタブをクリックします。

ステップ 4 ライセンスを付与するデバイスを選択して [追加（Add）] をクリックするか、ライセンスを削除する各デバイス形式をクリックして [Delete] アイコン（） をクリックします。

ステップ 5 [適用（Apply）] をクリックします。

次のタスク

変更内容を管理対象デバイスに展開します。

別の にスマート ライセンスを転送します。 Firepower Management Center

スマート ライセンスを Firepower Management Center に登録すると、バーチャル アカウントでそのライセンスが FMC に割り当てられます。スマート ライセンスを他の Firepower Management Center に移転する必要がある場合は、現在ライセンスが適用されている FMC の登録を解除する必要があります。これにより、バーチャルアカウントからスマート ライセンスが削除され、既存のライセンスが解放されるので、そのライセンスを新しい FMC に登録できるようになります。登録を解除しないと、これらのライセンスを再利用できず、バーチャルアカウントで使用可能なライセンスの数が足りなくなるために、コンプライアンス不適合通知を受け取る場合があります。この説明については、Cisco Smart Software Manager から Firepower Management Center の登録解除 （140 ページ） を参照してください。

その後、目的の Firepower Management Center にライセンスを登録できます。

[スマートライセンスのステータス（Smart License Status）] が [コンプライアンス不適合（Out of Compliance）] の場合

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	該当なし	Firepower Threat Defense	グローバルだけ	管理者

[スマートライセンス（Smart Licenses）] ページ（**[System]** > **[Licenses]** > **[Smart Licenses]**）の [使用の承認（Usage Authorization）] ステータスが [コンプライアンス不適合（Out of Compliance）] の場合はアクションを実行する必要があります。

ステップ 1 このページの下部にある [スマート ライセンス（Smart Licenses）] セクションを確認し、必要なライセンスを判断します。

ステップ 2 必要なライセンスを通常のチャネルを通じて購入します。

ステップ 3 Cisco Smart Software Manager (https://software.cisco.com/#SmartLicensing-Inventory)で、仮想アカウントにライセンスが表示されていることを確認します。

必要なライセンスがない場合はスマート ライセンスのトラブルシューティング （141 ページ）を参照してください。

ステップ 4 Firepower Management Center で、**[System]** > **[Licenses]** > **[Smart Licenses]** を選択します。

ステップ 5 [再承認（Re-Authorize）] ボタンをクリックします。

Cisco Smart Software Manager から Firepower Management Center の登録解除

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	該当なし	Firepower Threat Defense	グローバルのみ	管理者

アプライアンスを再インストール（再イメージ化）する前か、または何らかの理由ですべてのライセンスの付与資格を開放してスマート アカウントに戻す必要がある場合は、Cisco Smart Software Manager から Firepower Management Center の登録を解除（未登録に）します。

登録を解除すると、仮想アカウントから FMC が削除されます。Firepower Management Center リリースに関連付けられているライセンス権限はすべて、ご使用のバーチャルアカウントに戻ります。登録解除後、Firepower Management Center は適用モードになり、ライセンスが適用される機能に対する更新および変更が許可されなくなります。

管理対象の Firepower Threat Defense の一部のデバイスからライセンスを削除する必要がある場合は、複数の管理対象デバイスへのライセンスの割り当て（135ページ）または[デバイス管理（Device Management）] ページで管理対象デバイスにライセンスを割り当てる （154 ページ）を参照してください。

ステップ 1 **[System]** > **[Licenses]** > **[Smart Licenses]**を選択します。

ステップ 2 登録解除アイコン（）をクリックします。

Cisco Smart Software Manager と Firepower Management Center の同期

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	該当なし	Firepower Threat Defense	グローバルのみ	管理者

Cisco Smart Software Manager に変更を加えた場合は、すぐに変更が有効になるように Firepower Management Center 上で認証を更新できます。

ステップ 1 **[System]** > **[Licenses]** > **[Smart Licenses]**を選択します。

ステップ 2 更新アイコン（）をクリックします。

スマート ライセンスのトラブルシューティング

予期していたライセンスがスマート アカウントに表示されません。

表示されると思っていたライセンスがスマート アカウントにない場合は、次を試してください。

- 他の仮想アカウントにないことを確認します。この問題について、組織のライセンス管理者によるサポートが必要な場合があります。
- ライセンスを販売した担当者と、アカウントへの譲渡が完了していることを確認します。

予期していなかったコンプライアンス不適合の通知またはその他のエラー

- デバイスが別の FMC にすでに登録されている場合は、新しい FMC にデバイスのライセンスを付与する前に元の FMC の登録を解除する必要があります。Cisco Smart Software Manager から Firepower Management Center の登録解除 （140 ページ）を参照してください。

- 同期を試行します。Cisco Smart Software Manager と Firepower Management Center の同期 （141 ページ）を参照してください。

Firepower 7000/8000 シリーズのライセンス、ASA FirePOWER、および NGIPSv デバイス（従来のライセンス）

7000 および 8000 シリーズ デバイス、NGIPSv デバイス、および ASA FirePOWER モジュールには従来のライセンスが必要です。このドキュメントでは、これらのデバイスは多くの場合、クラッシク デバイスと呼ばれています。

重要 Firepower ハードウェアを稼働しているが Firepower ソフトウェアは実行していない場合は、使用しているソフトウェア製品のライセンス情報を参照してください。このドキュメントでは扱っていません。

クラシック ライセンスは、製品認証キー（PAK）をアクティブにする必要があり、デバイスごとに必要です。クラシック ライセンスは、「従来のライセンス」と呼ばれることもあります。

製品ライセンス登録ポータル

Firepower 機能のクラシック ライセンスを 1 つ以上購入する場合は、それらのライセンスを Cisco Product License Registration ポータルで管理します。

http://www.cisco.com/web/go/license

このポータルの使用方法の詳細については、次を参照してください。

https://www.cisco.com/web/fw/tools/swift/xui/html/help.html

Firepower 機能のサービス サブスクリプション（クラシック ライセンス）

一部の機能にはサービス サブスクリプションが必要です。

サービス サブスクリプションは、所定の時間内限定で、管理対象デバイス上の特定の Firepower 機能を有効にします。サービス サブスクリプションは、1 年、3 年、または 5 年単位で購入できます。サブスクリプションの期限が切れると、サブスクリプションの更新が必要であることが通知されます。クラシック デバイスのサブスクリプションの期限が切れた場合、機能のタイプによっては、関連機能を使用できなくなることがあります。

表 *5:* サブスクリプションおよび対応するクラシック ライセンス

購入するサブスクリプション	Firepower システム内で割り当てるクラシック ライセンス
TA	制御 + 保護（別名「脅威 & アプリ」、システム更新に必要）
TAC	制御 + 保護 + URL フィルタリング
TAM	制御 + 保護 +マルウェア
TAMC	制御 + 保護 + URL フィルタリング + マルウェア
URL	URL フィルタリング（TA が既に存在する場合はアドオン）
AMP	マルウェア（TA が既に存在する場合はアドオン）

クラシック ライセンスを使用する管理対象デバイスを購入すると、制御および保護のライセンスが自動的に提供されます。これらのライセンスは無期限ですが、システムの更新を有効にするには、TA サービス サブスクリプションを購入する必要があります。追加機能のサービス サブスクリプションはオプションです。

従来のライセンスのタイプと制約事項

ここでは、Firepower システム展開環境で使用可能な従来のライセンスのタイプについて説明します。デバイスで有効にできるライセンスは、デバイスのモデル、バージョン、および他の有効なライセンスによって異なります。

7000 および 8000 シリーズ デバイス、NGIPSv デバイス、および ASA FirePOWER モジュールの場合、ライセンスはモデル固有です。ライセンスがデバイスのモデルと完全に一致しない限り、管理対象デバイスでライセンスを有効にすることはできません。たとえば、Firepower 8250 マルウェア ライセンス（FP8250-TAM-LIC=）を使用して 8140 デバイスでマルウェア関連の機能を有効にすることはできません。Firepower 8140 マルウェア ライセンス（FP8140-TAM-LIC=）を購入する必要があります。

（注） NGIPSv または ASA FirePOWER では、制御ライセンスを使用してユーザとアプリケーションの制御を実行できますが、それらのデバイスはスイッチング、ルーティング、スタッキング、または 7000 および 8000 シリーズ デバイスの高可用性をサポートしていません。

Firepower システムでライセンス付き機能にアクセスできなくなる状況がいくつかあります。

- Firepower Management Center から従来のライセンスを削除することができますが、そのようにすると、すべての管理対象デバイスに影響します。
- 特定の管理対象デバイスでライセンス付き機能を無効にすることができます。

いくつかの例外がありますが、期限切れライセンスまたは削除済みライセンスに関連付けられている機能は使用できません。

次の表に、Firepower システムにおける従来のライセンスの概要を示します。

表 *6 : Firepower* システムの従来のライセンス

Firepowerシステムで割り当てるライセンス	購入するサービスサブスクリプション	プラットフォーム	付与される機能	併せて必要なライセンス	有効期限設定可/不可
任意	TA、TAC、TAM、またはTAMC	7000 および 8000 シリーズ ASA FirePOWER NGIPSv	ホスト、アプリケーション、ユーザ検出 SSL 暗号化トラフィックと TLS 暗号化トラフィックの復号および検査	なし	ライセンスによって異なる
プロテクション	TA（デバイスに付属）	7000 および 8000 シリーズ ASA FirePOWER NGIPSv	侵入検知と防御 ファイル制御 Security Intelligence フィルタリング	なし	不可
制御	なし（デバイスに付属）	7000 および 8000 シリーズ	ユーザおよびアプリケーション制御 スイッチングとルーティング 7000 および 8000 シリーズ デバイスの高可用性 7000 および 8000 シリーズネットワーク アドレス変換（NAT）	プロテクション	不可
制御	なし（デバイスに付属）	ASA FirePOWER NGIPSv	ユーザおよびアプリケーション制御	プロテクション	不可
マルウェア	TAM、TAMC、または AMP	7000 および 8000 シリーズ ASA FirePOWER NGIPSv	ネットワーク向け AMP（ネットワークベースの高度なマルウェア防御） ファイル ストレージ	プロテクション	可
URL フィルタリング	TAC、TAMC、または URL	7000 および 8000 シリーズ ASA FirePOWER NGIPSv	カテゴリとレピュテーションに基づく URL フィルタリング	プロテクション	可

Firepower システムで割り当てるライセンス	購入するサービス サブスクリプション	プラットフォーム	付与される機能	併せて必要なライセンス	有効期限設定可/不可
VPN	なし（詳細は販売担当者までお問い合わせください）	7000 および 8000 シリーズ	仮想プライベート ネットワークの導入	制御	可

プロテクション ライセンス

プロテクション ライセンスでは、侵入検知および防御、ファイル制御、およびセキュリティ インテリジェンス フィルタリングを実行できます。

- 侵入検知および防御により、侵入とエクスプロイトを検出するためネットワーク トラフィックを分析できます。またオプションで違反パケットをドロップできます。
- ファイル制御により、特定のアプリケーションプロトコルを介した特定タイプのファイルを検出し、オプションでこれらのファイルのアップロード（送信）またはダウンロード（受信）をユーザからブロックできます。マルウェア ライセンスが必要な ネットワーク向け *AMP* では、マルウェアの性質に基づいて限られたファイル タイプを検査およびブロックすることもできます。
- セキュリティインテリジェンス フィルタリングにより、トラフィックをアクセス制御ルールによる分析対象にする前に、特定の IP アドレス、URL、および DNS ドメイン名をブラックリストに追加（その IP アドレスとの間のトラフィックを拒否）できます。ダイナミック フィードにより、最新の情報に基づいて接続を直ちにブラックリストに追加できます。オプションで、Security Intelligence フィルタリングに「監視のみ」設定を使用できます。

プロテクションライセンス（制御ライセンスと共に）は、クラシック管理対象デバイスの購入時に自動的に組み込まれます。このライセンスは無期限ですが、システムの更新を有効にするには、TA サブスクリプションも購入する必要があります。

ライセンスがない状態でプロテクション関連の検査を実行するようにアクセス制御ポリシーを設定できますが、プロテクション ライセンスを Firepower Management Center に追加し、ポリシー展開対象デバイス上でこのライセンスを有効にするまではポリシーを展開できません。

プロテクション ライセンスを Firepower Management Center から削除するか、または管理対象デバイスでプロテクションを無効にすると、Firepower Management Center は対象デバイスからの侵入イベントとファイルイベントを認識しなくなります。結果として、トリガー条件としてこれらのイベントを使用する相関ルールがトリガーしなくなります。また、Firepower Management Center はシスコ提供またはサード パーティのセキュリティ インテリジェンス情報を取得するためにインターネットに接続しなくなります。プロテクションを再度有効にするまでは、既存のポリシーを再度展開することはできません。

プロテクション ライセンスは URL フィルタリング、マルウェア、および制御ライセンスに必要であるため、プロテクションライセンスを削除または無効にすると、URL フィルタリング、マルウェア、または制御ライセンスを削除または無効にすることと同じ効果があります。

制御ライセンス

制御ライセンスでは、アクセス コントロール ルールにユーザとアプリケーションの条件を追加することで、ユーザとアプリケーションの制御を実装できます。7000 および 8000 シリーズ デバイスでは、このライセンスを使用して、スイッチングとルーティング（DHCP リレーおよび NAT を含む）、およびデバイスのハイ アベイラビリティ ペアも構成できます。管理対象デバイスの制御ライセンスを有効にするには、保護ライセンスも有効にする必要があります。制御ライセンスは（保護ライセンスとともに）、従来の管理対象デバイスの購入時に自動的に付属します。このライセンスは無期限ですが、システムの更新を有効にするには、TA サブスクリプションも購入する必要があります。

従来の管理対象デバイスの制御ライセンスを有効にしない場合は、アクセス コントロール ポリシーのルールにユーザおよびアプリケーションの条件を追加できますが、デバイスにポリシーを展開することはできません。7000 または 8000 シリーズ デバイスの制御ライセンスを明確に有効にしないと、次の操作も行えません。

- スイッチド、ルーテッド、またはハイブリッド インターフェイスの作成
- NAT エントリの作成
- 仮想ルータの DHCP リレーの設定
- デバイスへのスイッチまたはルーティングが含まれているデバイス設定の展開
- デバイス間のハイ アベイラビリティの確立

（注） 制御ライセンスがなくても仮想スイッチおよびルータを作成できますが、データを取り込むスイッチドインターフェイスおよびルーテッドインターフェイスがない状態ではこれらのスイッチとルータは有用ではありません。

Firepower Management Center から制御ライセンスを削除するか、個々のデバイスで制御を無効にする場合：

- 対象デバイスでのスイッチングとルーティングの実行が行われなくなったり、デバイスのハイ アベイラビリティ ペアが解除されたりすることはありません。
- 既存の設定の編集や削除を続けることはできますが、影響を受けるデバイスに対する変更を展開することはできません。
- 新しいスイッチド インターフェイス、ルーテッド インターフェイス、またはハイブリッド インターフェイスを追加することも、新しい NAT エントリの追加、DHCP リレーの設定、7000 または 8000 シリーズ デバイスのハイ アベイラビリティの確立もできません。
- 既存のアクセス コントロール ポリシーに、ユーザ条件またはアプリケーション条件を含むルールが含まれている場合は、それらのポリシーを再展開することができません。

従来のデバイスの URL フィルタリング ライセンス

URL フィルタリングにより、モニタ対象ホストにより要求される URL に基づいて、ネットワーク内を移動できるトラフィックを判別するアクセス制御ルールを作成することができます。URL フィルタリング ライセンスを有効にする場合は、保護ライセンスも有効にする必要があります。従来のデバイスの URL フィルタリング ライセンスは、脅威 & アプリ（TAC）または脅威 & アプリおよびマルウェア（TAMC）サブスクリプションと組み合わせてサービス サブスクリプションとして購入できます。また、脅威 & アプリ（TA）が既に有効になっているシステムの場合は、アドオン サブスクリプションとして購入できます。

ヒント URL フィルタリング ライセンスがない状態で、許可またはブロックする個別 URL または URL グループを指定できます。これにより、Web トラフィックをカスタムできめ細かく制御できますが、URL カテゴリおよびレピュテーション データをネットワーク トラフィックのフィルタリングに使用することはできません。

URL フィルタリング ライセンスがない状態でも、アクセス制御ルールにカテゴリ ベースの URL 条件およびレピュテーション ベースの URL 条件を追加できますが、Firepower Management Center は URL 情報をダウンロードしません。最初に URL フィルタリング ライセンスを Firepower Management Center に追加し、ポリシー適用対象デバイスで有効にするまでは、アクセス コントロール ポリシーを適用できません。

Firepower Management Center からライセンスを削除するか、または管理対象デバイスで URL フィルタリングを無効にすると、URL フィルタリングにアクセスできなくなることがあります。また、URL フィルタリング ライセンスの有効期限が切れることもあります。ライセンスが期限切れになるか、ライセンスを削除または無効化すると、URL 条件が含まれているアクセス制御ルールは URL フィルタリングを直ちに停止し、Firepower Management Center は URL データのアップデートをダウンロードできなくなります。既存のアクセス コントロール ポリシーに、カテゴリ ベースまたはレピュテーション ベースの URL 条件を含むルールが含まれている場合は、それらのポリシーを再展開することができません。

従来のデバイスのマルウェア ライセンス

マルウェア ライセンスを使用すると、ネットワーク向け AMP および Cisco Threat Grid を使用して Cisco Advanced Malware Protection（AMP）を実行することができます。管理対象デバイスを使用して、ネットワーク上で伝送されるファイルのマルウェアを検出してブロックできます。マルウェア ライセンスを有効にするには、保護も有効にする必要があります。マルウェア ライセンスは、脅威 & アプリ（TAM）と組み合わせたサブスクリプションまたは脅威 & アプリおよび URL フィルタリング（TAMC）サブスクリプションとして購入できます。また、脅威 & アプリ（TA）が既に有効になっているシステムの場合は、アドオン サブスクリプションとして購入できます。

（注） マルウェア ライセンスが有効になっている 7000 および 8000 シリーズ 管理対象デバイスは、動的分析を設定していない場合でも、定期的に AMP クラウドへの接続を試行します。このため、デバイスの [インターフェイス トラフィック（Interface Traffic）] ダッシュボード ウィジェットには、送信済みトラフィックが表示されます。これは正常な動作です。

ファイル ポリシーの一部として ネットワーク向け AMP を設定し、その後 1 つ以上のアクセス コントロール ルールを関連付けます。ファイル ポリシーでは、特定のアプリケーション プロトコルを介した特定のタイプのユーザによるファイルのアップロードとダウンロードを検出できます。ネットワーク向け AMP では、ローカル マルウェア分析とファイルの事前分類を使用して、それらの限られた一連のファイルタイプを検査できます。特定のファイル タイプをダウンロードして Cisco Threat Grid クラウドにアップロードして、動的 Spero 分析でマルウェアが含まれているかどうかを判別することもできます。これらのファイルでは、ファイルがネットワーク内で経由する詳細なパスを示すネットワーク ファイル トラジェクトリを表示できます。マルウェア ライセンスでは、ファイル リストに特定のファイルを追加し、そのファイル リストをファイル ポリシー内で有効にすることもできます。これにより、検出時にこれらのファイルを自動的に許可またはブロックできます。

ネットワーク向け AMP 構成を含むアクセス コントロール ポリシーを展開する前に、マルウェア ライセンスを追加してから、そのポリシー展開対象デバイスで有効にする**必要があります**。デバイスでライセンスを後で無効にする場合、既存のアクセス コントロール ポリシーをそれらのデバイスに再度展開することはできません。

マルウェア ライセンスをすべて削除するか、それらがすべて期限切れになると、システムは AMP への問い合わせを停止し、AMP クラウドから送信される遡及的イベントの確認応答も停止します。既存のアクセス コントロール ポリシーに ネットワーク向け AMP 構成が含まれている場合は、それらのポリシーを再展開することができません。マルウェア ライセンスが失効したか削除された後、システムが既存のキャッシュ ファイルの性質を使用できるのは極めて短時間のみであることに注意してください。この時間枠の経過後、システムは `Unavailable` という性質をこれらのファイルに割り当てます。

マルウェア ライセンスが必要なのは ネットワーク向け AMP および Cisco Threat Grid を展開する場合のみです。マルウェア ライセンスがなければ、Firepower Management Center は AMP クラウドからエンドポイント向け AMP マルウェア イベントおよび侵害の兆候（IOC）を受信できます。

ファイルおよびマルウェア ポリシーのライセンス要件（1913 ページ）の重要な情報も参照してください。

7000 および 8000 シリーズ デバイス用の VPN ライセンス

VPN を使用すると、インターネットやその他のネットワークなどの公共ソースを経由してエンドポイント間にセキュア トンネルを確立できます。7000 および 8000 シリーズ デバイスの仮想ルータ間で安全な VPN トンネルを構築するよう、Firepower システムを設定することができます。VPN を有効にするには、保護および制御のライセンスも有効にする必要があります。VPN ライセンスを購入するには、販売担当者までお問い合わせください。

VPN ライセンスがないと、7000 および 8000 シリーズ デバイスで VPN 導入環境を設定できません。導入環境の作成はできますが、データを取り込むための 1 つ以上の VPN 対応スイッチド インターフェイスおよびルーテッド インターフェイスがない状態では、導入環境は有用ではありません。

VPN ライセンスを Firepower Management Center から削除するか、または個別のデバイスで VPN を無効にすると、対象デバイスは現在の VPN 導入環境をブレイクしません。既存の導入環境を編集または削除できますが、対象デバイスに変更を適用することはできません。

デバイス スタックおよびハイ アベイラビリティ ペアのクラシック ライセンス

スタックや 7000 または 8000 シリーズ デバイス ハイ アベイラビリティ ペアを構成するデバイスは、それぞれが同等のライセンスを持っている必要があります。デバイスのスタック構成後に、スタック全体のライセンスを変更できます。ただし、7000 または 8000 シリーズ デバイスのハイ アベイラビリティ ペアでは有効なライセンスを変更することはできません。

「デバイス スタックについて （699 ページ）」および「デバイスのハイ アベイラビリティ要件（680 ページ）」も参照してください。

従来型ライセンスの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
該当なし	任意	従来型	グローバルのみ	管理者

必要に応じて、次のいずれかを実行します。

目的	操作手順
Firepower Management Center に追加済みの従来のライセンスおよびそのタイプ、ステータス、使用状況、有効期限、適用されている管理対象デバイスなどの詳細情報	**[System]** > **[Licenses]** > **[Classic Licenses]**を選択します。 概要には、購入したライセンスの数の後に使用中のライセンスの数が括弧内に表示されます。
管理対象デバイスそれぞれに適用されたライセンス	**[Devices]** > **[Device Management]**を選択します。
ヘルスモニタのライセンステータス	正常性ポリシーでクラシックライセンスモニタのヘルスモジュールを使用します。詳細については、ヘルス モニタリング （349 ページ）、ヘルス モジュール （350 ページ）、および正常性ポリシーの作成 （362 ページ）を参照してください。

目的	操作手順
ダッシュボードのライセンスの概要	任意のダッシュボードに製品ライセンスウィジェットを追加します。手順については、[製品ライセンス（Product Licensing）] ウィジェット （336 ページ）、ダッシュボードへのウィジェットの追加 （340 ページ）、およびユーザ ロール別のダッシュボード ウィジェットの可用性 （324 ページ）を参照してください。

ライセンス キーの特定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
該当なし	任意	従来型	グローバルのみ	管理者

ライセンス キーによって、Firepower Management Center はシスコ ライセンス登録ポータルで一意に識別されます。これは、Firepower Management Center の製品コード（66 など）と管理ポート（eth0）の MAC アドレスで構成されます（66:00:00:77:FF:CC:88 など）。

シスコ ライセンス登録ポータルでは、ライセンス キーを使用して、Firepower Management Center にライセンスを追加する際に必要になるライセンス テキストを取得します。

ステップ 1 **[System]** > **[Licenses]** > **[Classic Licenses]**を選択します。

ステップ 2 [新規ライセンスの追加（Add New License）] をクリックします。

ステップ 3 [機能ライセンスの追加（Add Feature License）] ダイアログの上部にある [ライセンス キー（License Key）] フィールドの値をメモします。

次のタスク

- ライセンスを Firepower Management Center に追加します。クラシック ライセンスの生成と Firepower Management Center への追加 （151 ページ）を参照してください。

  この手順には、ライセンス キーを使用して実際のライセンス テキストを生成するプロセスが含まれています。

クラシック ライセンスの生成と Firepower Management Center への追加

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
該当なし	任意	従来型	グローバルのみ	管理者

（注） バックアップが完了した後にライセンスを追加した場合は、このバックアップを復元するときに、それらのライセンスが削除されたり上書きされたりすることはありません。復元の際の競合を防止するためにも、バックアップを復元する前に、これらのライセンスを（それらが使用されている場所をメモした上で）削除し、バックアップを復元した後で、追加して再設定してください。競合が発生した場合は、サポートに連絡してください。

ヒント サポート サイトにログインした後で、[ライセンス（Licenses）] タブでライセンスを要求することもできます。

始める前に

- ライセンス購入時にCiscoが提供したソフトウェア権利証明書にある製品アクティベーション キー（PAK）をお手元にご用意ください。レガシーの、以前のシスコのライセンスの場合は、サポートに問い合わせてください。
- Firepower Management Center のライセンス キーの種類を確認します。ライセンス キーの特定 （150 ページ） を参照してください。

ステップ 1 **[System]** > **[Licenses]** > **[Classic Licenses]**を選択します。

ステップ 2 [新規ライセンスの追加（Add New License）] をクリックします。

ステップ 3 必要に応じ、続いて以下を行います。

- ライセンス テキストをすでに取得している場合は、ステップ 8 にスキップしてください。
- ライセンスのテキストを取得する必要がある場合は、次の手順を実行します。

ステップ 4 [ライセンス取得（Get License）] をクリックして、Cisco ライセンス登録ポータルを開きます。

（注） ご使用のコンピュータからインターネットにアクセスできない場合は、アクセスできるコンピュータから http://cisco.com/go/licenseを探します。

ステップ 5 ライセンス登録ポータルで、PAK からライセンスを生成します。詳細については、https://www.cisco.com/web/fw/tools/swift/xui/html/help.htmlを参照してください。

この手順には、購入時に入手した PAK と、Firepower Management Center のライセンスキーが必要です。

ステップ 6 ライセンス登録ポータルの表示から、ないしはライセンス登録ポータルより送られてくるメールからライセンス テキストをコピーします。

重要 ポータルまたは電子メール メッセージ内のライセンス テキスト ブロックには、複数のライセンスを含めることができます。各ライセンスは、BEGIN LICENSE 行と END LICENSE 行で囲まれます。一度に 1 つのライセンスしかコピーして貼り付けることができません。

ステップ 7 Firepower Management Center の web インターフェイスの [機能ライセンスの追加（Add Feature License）] ページに戻ります。

ステップ 8 [ライセンス（License）] フィールドにライセンス テキストを貼り付けます。

ステップ 9 [ライセンスの検証（Verify License）] をクリックします。

ライセンスが無効となる場合は、ライセンス テキストが正しくコピーされているか確認します。

ステップ 10 [ライセンスの提出（Submit License）] をクリックします。

次のタスク

- 管理対象デバイスにライセンスを割り当てます。[デバイス管理（Device Management）] ページで管理対象デバイスにライセンスを割り当てる （154 ページ） を参照してください。管理対象デバイスのライセンス取得済み機能を使用するには、これらのデバイスにライセンスを割り当てる**必要があります**。

クラシック ライセンスまたは PAK からスマート ライセンスへの変換

ライセンス登録ポータル (LRP) または、Cisco Smart Software Manager (CSSM) のいずれかを使用してライセンスを変換し、未使用の製品認証キー（PAK）またはデバイスにすでに割り当てられているクラシック ライセンスに変換することができます。

重要 このプロセスは元に戻すことはできません。そのライセンスが元々はクラッシク ライセンスであっても、スマート ライセンスをクラッシク ライセンスに変換することはできません。

Cosco.com のドキュメントでは、クラッシック ライセンスは「従来型の」ライセンスとも呼ばれています。

始める前に

- 製品インスタンスにまだ割り当てられていない未使用の PAK がある場合、従来のライセンスからスマート ライセンスへの変換は最も簡単です。

- ハードウェアで Firepower Threat Defense を実行できる必要があります。詳細については、https://www.cisco.com/c/en/us/support/security/defense-center/products-device-support-tables-list.html で『*Cisco Firepower Compatibility Guide*』を参照してください。
- スマートアカウントが必要です。ない場合は作成します。ライセンスを保持するためのスマート アカウントの作成 （110 ページ）を参照してください。
- 変換する PAK またはライセンスは、スマート アカウントに表示されている必要があります。
- Cisco Smart Software Manager ではなくライセンス登録ポータルを使用して変換する場合に変換プロセスを開始するには、スマート アカウント クレデンシャルを保有している必要があります。

ステップ 1 実行する変換プロセスは、そのライセンスが使用されたことがあるかどうかによって異なります。

- 変換する PAK が使用されたことがない場合は、PAK の変換の手順を実行します。
- 変換する PAK がデバイスにすでに割り当てられている場合は、クラッシク ライセンスの変換の手順を実行します。

既存の従来のライセンスがまだデバイスに登録されていることを確認します。

ステップ 2 次のドキュメントで変換のタイプ（PAK またはインストール済みのクラシック ライセンス）の手順を参照してください。

- LRP を使用して PAK またはライセンスを変換するには、次の手順を実行します。
  - 変換プロセスのライセンス登録ポータル部分の手順がわかるビデオを表示する場合は、https://salesconnect.cisco.com/#/content-detail/7da52358-0fc1-4d85-8920-14a1b7721780 をクリックします。
  - https://cisco.app.box.com/s/mds3ab3fctk6pzonq5meukvcpjizt7wu のドキュメントで「変換（Convert）」を検索します。

    変換手順は 3 つあります。状況に該当する変換手順を選択します。
  - https://tools.cisco.com/SWIFT/LicensingUI/Home でライセンス登録ポータル（LRP）にサインインし、上記のドキュメントの手順を実行します。
- CSSM を使用して PAK またはライセンスを変換するには、次の手順を実行します。
  - ハイブリッド ライセンスをスマート ソフトウェア ライセンス *QRG* に変換するには、次の手順を実行します。

    https://community.cisco.com/t5/licensing-enterprise-agreements/converting-hybrid-licenses-to-smart-software-licenses-qrg/ta-p/3628609?attachment-id=134907
  - https://software.cisco.com/#SmartLicensing-LicenseConversion で CSSM にサインインし、上記のドキュメントの変換タイプ（PAK またはインストール済みのクラッシック ライセンス）の手順を実行します。

ステップ 3 ハードウェアに Firepower Threat Defense を新たにインストールします。

https://www.cisco.com/c/en/us/support/security/firepower-ngfw/products-installation-guides-list.html のハードウェアに関する手順を参照してください。

ステップ 4 Firepower Device Manager を使用してこのデバイスをスタンドアロン デバイスとして管理するには、次の手順を実行します。

https://www.cisco.com/c/en/us/support/security/firepower-ngfw/products-installation-and-configuration-guides-list.html の『*Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager*』のデバイスへのライセンス付与に関する情報を参照してください。

この手順の残りは省略してください。

ステップ 5 Firepower Management Center でスマート ライセンスをすでに展開している場合は、次の手順を実行します。

a) 新しい Firepower Threat Defense デバイスでスマート ライセンスを設定します。

複数の管理対象デバイスへのライセンスの割り当て （135 ページ）を参照してください。

b) 新しいスマート ライセンスがデバイスに正常に適用されていることを確認します。

スマート ライセンスおよびスマート ライセンス ステータスの表示 （136 ページ）を参照してください。

ステップ 6 Firepower Management Center でスマート ライセンスをまだ展開していない場合は、次の手順を実行します。

Firepower Threat Defense デバイスのライセンス （96 ページ）を参照してください。（該当しないか、またはすでに完了しているステップはスキップします。）

[デバイス管理（Device Management）] ページで管理対象デバイスにライセンスを割り当てる

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	任意	任意	リーフのみ	管理者/ネットワーク管理者

一部の例外はありますが、管理対象デバイスでライセンスを無効にすると、そのライセンスに関連づけられている機能は使用できなくなります。

（注） 同じ セキュリティ モジュール/エンジン のコンテナ インスタンスの場合は、ライセンスを各インスタンスに適用します。ただし、セキュリティ モジュール/エンジン のすべてのインスタンスについては、セキュリティ モジュール/エンジン は機能ごとに 1 つのライセンスのみを使用します。

（注） FTD クラスタの場合は、クラスタ全体にライセンスを適用します。ただし、クラスタ内の各ユニットが機能ごとに個別のライセンスを使用します。

始める前に

- デバイスを Firepower Management Center に追加します。Firepower Management Center へのデバイスの追加 （293 ページ）を参照してください。
- スマート ライセンスを割り当てる場合、次の手順に従います。
  - スマートライセンスを同時に多くのデバイスに適用する必要がある場合、次の手順ではなく、[スマート ライセンス（Smart Licenses）] ページを使用します。複数の管理対象デバイスへのライセンスの割り当て （135 ページ）を参照してください
  - 管理対象デバイスに配布するためのスマートライセンスを準備するには、次を参照してください。スマート ライセンスの登録 （113 ページ）

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 ライセンスを割り当てまたは無効にするデバイスの横にある編集アイコン（）をクリックします。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [デバイス（Device）] タブをクリックします。

ステップ 4 [ライセンス（License）] セクションの横にある編集アイコン（）をクリックします。

ステップ 5 適切なチェックボックスをオンまたはオフにして、デバイスのライセンスを割り当て、または無効にします。

ステップ 6 [保存（Save）] をクリックします。

次のタスク

- スマートライセンスを割り当てられている場合、ライセンスのステータスを確認します。

  [System] > **[Licenses]** > **[Smart Licenses]** に移動し、[スマート ライセンス（Smart Licenses）] テーブル上部のフィルタにホスト名またはデバイスの IP アドレスを入力し、各デバイス

および各ライセンス に、チェックマーク（）のある緑色の円のみが表示されることを確認します。その他のアイコンが表示される場合は、アイコンにマウスオーバーすると詳細を確認できます。

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。
- Firepower Threat Defense デバイスのライセンスを供与し、エクスポート制御機能が有効になっている基本ライセンスを適用した場合は、各デバイスを再起動します。高可用性ペアに設定されているデバイスの場合、両方のデバイスを同時に再起動してアクティブ/アクティブの状態を回避します。

FirePOWER のライセンスとサービス サブスクリプションの期限切れ

ライセンスの期限切れとサービス サブスクリプションの期限切れ

Q. FirePOWER の機能ライセンスは期限切れになりますか。

A. 厳密に言えば、FirePOWER の機能ライセンスは期限切れになりません。代わりに、このライセンスをサポートするサービス サブスクリプションが期限切れになります。サービスのサブスクリプションに関する詳細については、https://www.cisco.com/c/en/us/support/security/defense-center/products-installation-and-configuration-guides-list.html から入手できる『*Firepower Management Center Configuration Guide*』の「Service Subscriptions for Firepower Features」を参照してください。

スマート ライセンス

Q. 製品インスタンス登録トークンが期限切れになることはありますか。

A. 特定の有効期間内に製品を登録するために使用されないと、トークンは期限切れになります。Cisco Smart Software Manager でトークンを作成するときに、トークンが有効な日数を設定します。トークンを使用して Firepower Management Center を登録する前にトークンが期限切れになった場合は、新しいトークンを作成する必要があります。

トークンを使用して Firepower Management Center を登録した後は、トークン有効期限は関係がなくなります。トークンの有効期限が経過しても、トークンを使用して登録した Firepower Management Center に影響はありません。

トークンの有効期限の日付は、サブスクリプションの有効期限には影響しません。

詳細については、『*Cisco Smart Software Manager User Guide*』を参照してください。

Q. スマート ライセンス/サービス サブスクリプションが期限切れになっているかどうかや、期限切れが近づいていることを確認するにはどうすればよいですか。

A. サービス サブスクリプションがいつ期限切れになるか（またはいつ期限切れになったか）を判断するには、Cisco Smart Software Manager でエンタイトルメントを確認します。

Firepower Management Center では、**[System]** > **[Licenses]** > **[Smart Licenses]** を選択することで、機能ライセンスのサービス サブスクリプションが現在履行されているかどうかを判断できます。このページでは、製品登録トークンを使用してこの Firepower Management Center に関連付けられているスマート ライセンスのエンタイトルメントが表にまとめられています。[ライセンス ステータス（License Status）] フィールドに基づいて、ライセンスのサービス サブスクリプションが現在履行されているかどうかを判断できます。

Firepower Device Manager で、[スマートライセンス（Smart License）] ページを使用して、システムの現在のライセンス ステータスを表示します。[デバイス（Device）] をクリックしてから、スマート ライセンス サマリーの [設定の表示（View Configuration）] をクリックします。

さらに、Cisco Smart Software Manager はライセンスが期限切れとなる 3 ヵ月前に通知を送信します。

Q. スマート ライセンス/サブスクリプションが期限切れになるとどうなりますか。

A. 購入したサービス サブスクリプションの期限が切れた場合、Firepower Management Center、およびご自分のスマート アカウントに、アカウントが不適合であることが表示されます。Cisco はサブスクリプションの更新が必要なことを通知します。サブスクリプションの更新を参照してください。他の影響はありません。

特定のライセンスの予約

Q. 特定のライセンスの予約の期限が切れた場合はどうなりますか。

A. SLR ライセンスは期間ベースです。

必要なライセンスが使用できないか、または期限が切れている場合、次のアクションは制限されています。

- デバイス登録に使用
- ポリシーの展開

従来のライセンス

Q. クラシック ライセンス/サービス サブスクリプションが期限切れになっているかどうかや、期限切れが近づいていることを確認するにはどうすればよいですか。

A. Firepower Management Center で、**[System]** > **[Licenses]** > **[Classic Licenses]** を選択します。

このページでは、この Firepower Management Center に追加したクラシック ライセンスが表にまとめられています。

[ステータス（Status）] フィールドに基づいて、ライセンスのサービス サブスクリプションが現在履行されているかどうかを判断できます。

[有効期限（Expires）] フィールドの日付により、サービス サブスクリプションがいつ期限切れになるか（またはいつ期限切れになったか）を判断できます。

この情報は、シスコ製品ライセンス登録ポータルでライセンス情報を確認することで得ることもできます。

Q. 「IPSにはIPSの期間サブスクリプションも必要です（IPS Term Subscription is still required for IPS）」とは、どのような意味ですか。

A. このメッセージは、保護および制御の機能には、（期限切れにならない）使用権ライセンスだけでなく、定期的に更新する必要がある 1 つ以上の関連付けられたサービス サブスクリプションも必要であることを伝えているだけです。使用するサービス サブスクリプションが現在のもので、すぐに期限切れにならない場合は、何もする必要はありません。サービス サブスクリプションのステータスを判断するには、クラシック ライセンス/サービス サブスクリプションが期限切れになっているかどうかや、期限切れが近づいていることを確認するにはどうすればよいですか。 （? ページ）を参照してください。

Q. クラシック ライセンス/サブスクリプションが期限切れになるとどうなりますか。

A. クラシック ライセンスをサポートするサービス サブスクリプションの期限が切れると、シスコによってサブスクリプションの更新が必要であることが通知されます。「サブスクリプションの更新」を参照してください。

機能のタイプによっては、関連機能を使用できなくなることがあります。

表 7: クラシック ライセンス/サブスクリプションの期限切れによる影響

従来のライセンス	利用可能なサポート サブスクリプション	期限切れによる影響
Control	TA、TAC、TAM、TAMC	既存の FirePOWER の機能を引き続き使用できますが、アプリケーション署名の更新を含む、VDB 更新はダウンロードできません。
Protection	TA、TAC、TAM、TAMC	侵入インスペクションを引き続き実行できますが、侵入ルールの更新をダウンロードすることはできません。

従来のライセンス	利用可能なサポート サブスクリプション	期限切れによる影響
URL フィルタリング	URL、TAC、TAMC	• URL 条件によるアクセス コントロール ルールが、URL のフィルタリングをただちに停止します。 • URL カテゴリとレピュテーションに基づいてトラフィックをフィルタリングするその他のポリシー（SSL ポリシーなど）が、ただちにその処理を停止します。 • Firepower Management Center は、URL データの更新をダウンロードできなくなります。 • URL カテゴリとレピュテーションのフィルタリングを実行する既存のポリシーを再展開することはできません。

従来のライセンス	利用可能なサポート サブスクリプション	期限切れによる影響
Malware	AMP、TAM、TAMC	• 非常に短い時間の間、システムは既存のキャッシュされたファイル性質を使用できます。この時間枠の経過後、システムは `Unavailable` という性質をこれらのファイルに割り当てます。 • システムは AMP クラウドへの問い合わせを停止し、AMP クラウドから送信されたレトロスペクティブイベントの認証を停止します。 • 既存のアクセス コントロール ポリシーに AMP for Firepower 構成が含まれている場合は、それらのポリシーを再展開することができません。

サブスクリプションの更新

Q. 期限切れ間近のクラシック ライセンスを更新する方法を教えてください。

A. 期限切れ間近のクラシック ライセンスを更新するには、新しい PAK キーを購入し、新しいサブスクリプションを実装する場合と同じプロセスを実行するだけです。

Q. Firepower Management Center から FirePOWER サービス サブスクリプションを更新できますか。

A. いいえ。Firepower サービス サブスクリプション（従来またはスマート）を更新するには、Cisco Commerce Workspace または Cisco Service Contract Center を使用して、新しいサブスクリプションを購入してください。

このガイドのその他のライセンス情報

対象	参照先
スマート ライセンス認証局との FMC 通信用のインターフェイスに関する情報	管理インターフェイスについて（1266ページ）およびサブトピック
ライセンスに関するファイアウォールの要件	インターネット アクセス要件（3281 ページ）
このドキュメントの各手順の最初にある表内のライセンス情報の説明。	ドキュメンテーションのライセンス ステートメント（19 ページ）
バックアップからの復元時のライセンスに関する重要な考慮事項	バックアップからの復元：FMC および 7000/8000 シリーズ（213 ページ）

対象	参照先
ルールとポリシーの適用時のライセンスの効果とそれらのトリガー方法。	ポリシーとルールに関する情報等： • アクセス コントロール ルールの管理 （1693 ページ） • アクセス コントロール ルールのコンポーネント（1694ページ）、状態に関する情報 • TLS/SSL ルールのガイドラインと制限事項 （1848 ページ） • TLS/SSL ルールのコンポーネント （1817 ページ） • QoS ポリシーによるレートの制限 （865 ページ）
展開とライセンスに関連する展開とポリシーまたはルールの管理エラー	このガイド全体のポリシーとルールに関する情報等： • ルールとその他のポリシーの警告 （501 ページ） • QoS ポリシーによるレートの制限 （865 ページ）
SSL のライセンス要件	Firepower Threat Defense に関する SSL 設定 （1371 ページ） での前提条件
SSL プリプロセッサ機能のライセンス要件	SSL プリプロセッサ （2379 ページ）
AMP for Endpoints 統合のライセンス	マルウェア防御の比較：Firepower と AMP for Endpoints （1954 ページ）
クライアントまたはサーバ サービスでのライセンスとストリーム リアセンブル	TCP ストリームのプリプロセス オプション （2425 ページ）
ライセンスと Cisco Threat Intelligence Director（TID）	プラットフォーム、要素、およびライセンスに関する要件 （1971 ページ）
接続イベントへのライセンスの影響	接続イベント フィールドの入力の要件 （3042 ページ）
ライセンスとその他のダッシュボード ウィジェットに関する情報	ユーザ ロール別のダッシュボード ウィジェットの可用性 （324 ページ） [カスタム分析（Custom Analysis）] ウィジェット （327 ページ）

対象	参照先
ライセンスのヘルス モニタに関する情報	スマート ライセンス モニタとクラッシク ライセンスモニタに関する情報 ヘルス モジュール（350 ページ）

Firepower ライセンスに関するその他の情報

ライセンスに関するよくある質問の解決に役立つその他の情報については、次のドキュメントを参照してください。

- 次の『*Frequently Asked Questions (FAQ) about Firepower Licensing*』のドキュメント
  https://www.cisco.com/c/en/us/td/docs/security/firepower/licensing/faq/firepower-licence-FAQ.html
- 次の『*Cisco Firepower System Feature Licenses* 』のドキュメント
  https://www.cisco.com/c/en/us/td/docs/security/firepower/roadmap/firepower-licenseroadmap.html

Cisco Success Network

Cisco Success Network はユーザ対応のクラウド サービスです。Cisco Success Network を有効にすると、Firepower Management Center と Cisco Cloud 間にセキュアな接続が確立され、使用状況に関する情報と統計情報がストリーミングされます。テレメトリをストリーミングすることによって、Firepower システムからの対象のデータを選択してそれを構造化形式でリモートの管理ステーションに送信するメカニズムが提供されるため、次のメリットが得られます。

- ネットワーク内の製品の有効性を向上させるために、利用可能な未使用の機能について通知します。
- 製品に利用可能な、追加のテクニカル サポート サービスとモニタリングについて通知します。
- シスコ製品の改善に役立ちます。

Firepower Management Center は常にセキュアな接続を確立および維持し、Cisco Success Network に登録できるようにします。Cisco Success Network を無効にすることで、いつでもこの接続をオフにできます。これにより、デバイスが Cisco Success Network クラウドから接続解除されます。

Cisco Success Network の有効化

Cisco Smart Software Manager に Firepower Management Center を登録するときは、Cisco Success Network を有効にします。スマート ライセンスの登録 （113 ページ）を参照してください。

[ライセンス（Licenses）] > **[スマートライセンス（Smart Licenses）]** ページで、現在の Cisco Success Network の登録ステータスを表示できます。また、登録ステータスを変更することもできます。Cisco Success Network の登録の変更 （176 ページ）を参照してください。

（注） Firepower Management Center に有効な Smart Software Satellite Server 設定がある場合、Cisco Success Network 機能は無効になるか、または特定のライセンスの予約を使用します。

Cisco Success Network テレメトリ データ

Cisco Success Network では、登録済みの Firepower Management Center はリアルタイムの設定と動作状態に関する情報を Cisco Success Network Cloud に継続的にストリーミングすることができます。収集およびモニタ対象のデータには、次の情報が含まれます。

- [登録済みデバイス情報（Enrolled device information）]：これには、Firepower Management Center のデバイス名、モデル、シリアル番号、UUID、システム稼働時間、およびスマートライセンス情報が含まれます。登録済みデバイス データ （164 ページ）を参照してください。
- [ソフトウェア情報（Software information）]：これには、バージョン番号、ルールの更新バージョン、地理的位置情報データベースのバージョン、脆弱性データベース（VDB）のバージョン情報など、登録済みの Firepower Management Center に関するソフトウェア情報が含まれます。ソフトウェア バージョン データ （164 ページ）を参照してください。
- [管理対象デバイス情報（Managed device information）]：これには、デバイス名、デバイスのモデル、シリアル番号、ソフトウェアのバージョン、およびデバイスごとに使用されているライセンスなど、登録済みの Firepower Management Center に関連付けられているすべての管理対象デバイスに関する情報が含まれます。管理対象デバイス データ （165 ページ）を参照してください。
- [展開情報（Deployment information）]: これには、ポリシーの展開に関する情報が含まれます。展開を設定した後、およびその設定を変更したときは、影響を受けるデバイスにその変更を展開する必要があります。導入情報 （166 ページ）を参照してください。
- [機能の使用状況（Feature usage）]：これには、機能に固有のポリシーおよびライセンスに関する情報が含まれます。
  - [URL フィルタリング（URL filtering）]：これには、デバイスに対して設定され展開されている URL フィルタリング ライセンスの数と、URL フィルタリング機能を使用するポリシーを展開しているデバイスの数が含まれます。
  - [侵入防御（Intrusion prevention）]：これには、侵入防御を設定されている管理対象デバイスの数と、Threat Intelligence Director（TID）に対してデバイスが有効になっているかどうかが含まれます。
  - [マルウェアの検出（Malware detection）]：これには、デバイスに対して設定および展開されているマルウェア ライセンスの数と、マルウェア検出機能を使用するポリシーを展開しているデバイスの数が含まれます

登録済みデバイス データ

Cisco Success Network で Firepower Management Center を登録したら、登録済みの Firepower Management Center のデバイスに関するテレメトリ データがシスコ クラウドにストリーミングされることを選択します。次の表に、登録済みのデバイスに関して収集し、監視しているデータを示します。これには、侵入ポリシー（システムが提供するポリシーとカスタム ポリシーの両方）および登録済みの Firepower Management Center のマルウェア検出に関する機能に固有の情報が含まれます。

表 *8:* 登録済みデバイスのテレメトリ データ

データ ポイント	値の例
デバイス名	Management Center East
デバイス UUID	24fd0ccf-1464- 491f-a503- d241317bb327
HA ピア UUID	24fe0ccd-1564- 491h-b802- d321317cc827
デバイスモデル	Cisco Firepower Management Center 4000 Cisco Firepower Management Center for VMWare
シリアル番号	9AMDESQP6UN
システム稼動時間	99700000
製品 ID	FMC4000-K9 FS-VMW-SW-K9
スマートライセンス PIID	24fd0ccf-1464- 491f-a503- d241317bb327
仮想アカウント識別子	CiscoSVStemp

ソフトウェア バージョン データ

Cisco Success Network は、ソフトウェアのバージョン、ルールの更新バージョン、地理的位置情報データベースのバージョン、脆弱性データベースのバージョン情報など、登録済みの Firepower Management Center デバイスに関連するソフトウェアの情報を収集します。次の表に、登録済みのデバイスに関して収集し、監視しているソフトウェア情報を示します。

表 *9:* ソフトウェア バージョンのテレメトリ データ

データ ポイント	値の例
Firepower Management Center のソフトウェア バージョン	{ type: "SOFTWARE", version: "6.2.3-10517" }
ルールの更新バージョン	{ type: "SNORT_RULES_DB", version: "2016-11-29-001-vrt", lastUpdated: 1468606837000 }

データ ポイント	値の例
脆弱性データベース（VDB）のバージョン	{ type: "VULNERABILITY_DB", version: "271", lastUpdated: 1468606837000 }
地理的位置情報データベースのバージョン	{ type: "GEOLOCATION_DB", version: "850" }

管理対象デバイス データ

Cisco Success Network は、登録済みの Firepower Management Center に関連付けられているすべての管理対象デバイスに関する情報を収集します。次の表に、管理対象デバイスに関して収集し、監視している情報を示します。これには、管理対象デバイスの URL フィルタリング、侵略防御、およびマルウェア検出など、機能に固有のポリシーおよびライセンス情報が含まれます。

表 *10 :* 管理対象デバイスのテレメトリ データ

データ ポイント	値の例
管理対象デバイス名	firepower
管理対象デバイスのバージョン	6.2.3-10616
管理対象デバイス マネージャ	FMC
管理対象デバイス モデル	Cisco Firepower 2130 NGFW アプライアンス Cisco Firepower Threat Defense VMware
管理対象デバイスのシリアル番号	9AMDESQP6UN
管理対象デバイスの PID	FPR2130-NGFW-K9 NGFWv
デバイスにURLフィルタリング ライセンスを使用しているか	True
URLデバイスごとにURL フィルタリングを使用した AC ルール	10
URL フィルタリングライセンスを使用する URL フィルタリングでの AC ルールの数	3
脅威ライセンスを使用するURL フィルタリングでの AC ルールの数	3
デバイスに脅威ライセンスを使用しているか	True
AC ポリシーに侵略ルールを追加しているか	True
侵略ポリシーを使用する AC ルールの数	10

データ ポイント	値の例
デバイスにマルウェア ライセンスを使用しているか	True
マルウェア ポリシーを使用する AC ルールの数	10
マルウェアライセンスを使用するマルウェアポリシーでの AC ルールの数	5
デバイスに Threat Intelligence Director（TID）を使用しているか	True

導入情報

展開を設定した後、およびその設定を変更したときは、影響を受けるデバイスにその変更を展開する必要があります。次の表に、影響を受けるデバイスの数と成功か失敗かの情報を含む展開のステータスなど、設定の展開に関して収集し、モニタするデータを示します。

表 *11* : 導入情報

データ ポイント	値の例
ジョブ ID	8589936079
展開用に選択したデバイスの数	3
展開に失敗したデバイスの数	1
展開に成功したデバイスの数	2
終了時間	1523993913001
Start Time	1523993840445
Status	SUCCEEDED
ターゲットデバイスの UUID	4f14f644-41e0 -11e8-9354- cf32315d7095
展開したポリシータイプ	NetworkDiscovery NGFWPolicy DeviceConfiguration
現在の実行で収集した最後の展開ジョブの ID	8589936079
コンテナタイプ（スタンドアロンまたは HA ペア）	STANDALONE HAPAIR
コンテナの UUID	5e006633-30fe-11e9-8a70-cd88086eeac0

データ ポイント	値の例
デバイスモデル	Cisco Firepower Threat Defense for VMWare
デバイスバージョン	6.4.0
ポリシーバンドルのサイズ	3588153

TLS/SSL インスペクション イベント データ

Firepower システムは、デフォルトではセキュア ソケット レイヤ（SSL）プロトコルまたはその後継である Transport Layer Security（TLS）プロトコルで暗号化されたトラフィックを検査できません。TLS/SSL インスペクションを使用すると、暗号化トラフィックをインスペクションを実行せずにブロックしたり、暗号化または復号されたトラフィックをアクセス コントロールを使用して検査したりできます。次の各表では、暗号化されたトラフィックについて Cisco Success Network と共有する統計情報について説明します。

ハンドシェイク プロセス

システムで TCP 接続での TLS/SSL ハンドシェイクが検出された場合、その検出されたトラフィックを復号できるかどうかが判定されます。システムは、暗号化されたセッションを処理する際にトラフィックに関する詳細をログに記録します。

表 *12 : TLS/SSL* インスペクション : ハンドシェイクのテレメトリ データ

データ ポイント	値の例
システムは、トラフィックが**復号できず**次の状態となった場合、適用されたアクションを報告します。 • ブロック • TCP リセットによるブロック • 復号されない	0 以上の整数値
システムは、トラフィックが次の方法で**復号できた**場合、適用されたアクションを報告します。 • 既知の秘密キーを使用 • 置換キーのみを使用 • 自己署名証明書への再署名 • サーバ証明書の再署名	0 以上の整数値

キャッシュ データ

TLS/SSL ハンドシェイクが完了すると、管理対象デバイスは暗号化セッション データをキャッシュに保存し、それによりフル ハンドシェイクを必要とせずにセッションを再開できます。管理対象デバイスもサーバ証明書データをキャッシュに保存し、それにより後続のセッションでのより速いハンドシェイクの処理が可能になります。

表 *13 : TLS/SSL* インスペクション : キャッシュのテレメトリ データ

データ ポイント	値の例
システムは暗号化されたセッション データおよびサーバ証明書データをキャッシュし、**キャッシュ**について SSL 接続ごとにレポートします。具体的な内容は次のとおりです。 • SSL セッション情報がキャッシュされた回数 • SSL 証明書検証キャッシュがヒットした回数 • SSL 証明書検証キャッシュのルックアップが失敗した回数 • SSL 元証明書キャッシュがヒットした回数 • SSL 元証明書キャッシュのルックアップが失敗した回数 • SSL 再署名証明書キャッシュがヒットした回数 • SSL再署名証明書キャッシュのルックアップが失敗した回数	0 以上の整数値

証明書のステータス

システムは暗号化されたトラフィックを評価し、暗号化サーバの証明書のステータスを報告します。

表 *14 : TLS/SSL* インスペクション：証明書ステータスのテレメトリ データ

データ ポイント	値の例
システムは、暗号化サーバの**証明書のステータス**に基づいて暗号化されたトラフィックを評価し、SSL 証明書が次の状態である接続の数を報告します。 • 有効 • 有効期限切れ • 発行元が無効 • 署名が無効 • チェックされていない • まだ有効でない • 取り消されている • 自己署名されている • 不明	0 以上の整数値

失敗の理由

システムは暗号化されたトラフィックを評価し、システムがトラフィックの復号化に失敗している場合は失敗の理由を報告します。

表 *15 : TLS/SSL* インスペクション：失敗のテレメトリデータ

データ ポイント	値の例
システムは暗号化されたトラフィックを評価し、システムが次の理由のためにトラフィックの復号化に失敗している場合は**失敗の理由**を報告します。 • 復号エラー • ハンドシェイク中のポリシー判定の実行 • ハンドシェイク前のポリシー判定の実行 • 圧縮がネゴシエートされている • キャッシュされていないセッション • インターフェイスがパッシブ モードである • 不明な暗号スイート • サポートされていない暗号スイート	0 以上の整数値

バージョン

システムは暗号化されたトラフィックを評価し、ネゴシエートされた TLS/SSL バージョンを接続ごとに報告します。

表 *16 : TLS/SSL* インスペクション：バージョンのテレメトリ データ

データ ポイント	値の例
システムは暗号化されたトラフィックを評価し、次のようなネゴシエートされた**バージョン**を SSL 接続ごとに報告します。 • SSLv2 のネゴシエート • SSLv3 のネゴシエート • 不明なバージョンのネゴシエート • TLSv1.0 のネゴシエート • TLSv1.1 のネゴシエート • TLSv1.2 のネゴシエート • TLSv1.3 のネゴシエート	0 以上の整数値

Snort 再起動データ

管理対象デバイス上の Snort プロセスと呼ばれるトラフィック インスペクション エンジンが再起動すると、プロセスが再開されるまでインスペクションが中断されます。ユーザ定義のアプリケーションの作成/削除を行うか、システムまたはカスタム アプリケーション ディテクタを有効化/無効化すると、展開プロセスを経由することなく、ただちに Snort プロセスが再起動します。Snort プロセスの再起動が続行されていることが警告され、キャンセルが可能になります。再起動は、現在のドメインまたはそのいずれかの子ドメイン内の任意の管理対象デバイスで発生します。

表 *17 : Snort* 再起動のテレメトリ データ

データ ポイント	値の例
カスタムアプリケーションディテクタを有効または無効にした場合の Snort 再起動の数	0 以上の整数値
カスタムアプリケーションディテクタを作成または変更した場合の Snort 再起動の数	0 以上の整数値

Cisco Security Packet Analyzer データ

組織が Cisco Security Packet Analyzer（Firepower システムとは別個の製品）を展開している場合、Cisco Security Packet Analyzer を使用して Firepower システムが検出するインシデントや不審なイベントのコンテキスト情報を、フル パケット キャプチャの形式で収集できます。

Cisco Security Packet Analyzer と Firepower Management Center は互いに独立して展開され、Cisco Security Packet Analyzer の展開は Firepower システムを認識しません。キャプチャされたデータはパケット アナライザと管理センター間を移動しません。

表 *18 : CSPA* のテレメトリ データ

データ ポイント	値の例
FMC に登録されている Cisco Security Packet Analyzer インスタンスの合計数	0 以上の整数値
FMC 上の Cisco Security Packet Analyzer クエリの数	0 以上の整数値
FMC 上の Cisco Security Packet Analyzer クエリグループの数	0 以上の整数値

コンテキスト クロス起動データ

コンテキスト クロス起動機能を使用すると、Firepower Management Center の外部の Web ベースのリソースにおける潜在的な脅威に関するさらなる情報をすばやく検索できます。FMC のイベント ビューアまたはダッシュボードのイベントから、外部リソースの関連情報を直接ク

リックできます。これにより、そのIPアドレス、ポート、プロトコル、ドメイン、またはSHA 256 ハッシュに基づいて、特定のイベントに関連するコンテキストを迅速に収集できます。

表 *19:* コンテキスト クロス起動のテレメトリ データ

データ ポイント	値の例
FMC 上に設定されているコンテキスト クロス起動リソースの数	0 以上の整数値
FMC 上で有効になっているコンテキスト クロス起動リソースの数	0 以上の整数値
ドメイン変数を含むコンテキスト クロス起動インスタンスの数	0 以上の整数値
IP 変数を含むコンテキスト クロス起動インスタンスの数	0 以上の整数値
SHA 256 変数を含むコンテキスト クロス起動インスタンスの数	0 以上の整数値

テレメトリ ファイルの例

次に、Firepower Management Center とその管理対象デバイスに関してポリシーと展開情報をストリーミングするための Cisco Success Network テレメトリ ファイルの例を示します。


```
{
    "recordType" : "CST_FMC",
    "recordVersion" : "6.4.0",
    "recordedAt" : 1550467152050,
    "fmc" : {
      "deviceInfo" : {
        "deviceModel" : "Cisco Firepower Management Center for VMWare",
        "deviceName" : "firepower",
        "deviceUuid" : "18842483-30cf-11e9-a090-503c97636361",
        "serialNumber" : "None",
       "smartLicenseProductInstanceIdentifier" : "cbs246a5-6d51-4eb7-9gc2-118b177dc4de",

        "smartLicenseVirtualAccountName" : "FTD-ENG-BLR",
        "systemUptime" : 262007000,
        "udiProductIdentifier" : "FS-VMW-SW-K9"
      },
      "versions" : {
        "items" : [ {
          "lastUpdated" : 0,
          "type" : "SOFTWARE",
          "version" : "6.4.0-1335"
        }, {
          "lastUpdated" : 0,
          "type" : "SNORT_RULES_DB",
          "version" : "2018-10-10-001-vrt"
        }, {
          "lastUpdated" : 1550200610000,
          "type" : "VULNERABILITY_DB",
```

```
      "version" : "309"
    }, {
      "lastUpdated" : 0,
      "type" : "GEOLOCATION_DB",
      "version" : "None"
    } ]
  }
},
"managedDevices" : {
  "items" : [ {
    "deviceInfo" : {
      "deviceManager" : "FMC",
      "deviceModel" : "Cisco Firepower Threat Defense for VMWare",
      "deviceName" : "10.10.17.220",
      "deviceVersion" : "6.4.0-1335",
      "serialNumber" : "9AUVT5GTRPA"
    },
    "malware" : {
      "malwareLicenseUsed" : false,
      "numberOfACRulesNeedMalwareLicense" : 10,
      "numberOfACRulesWithMalware" : 20
    },
    "sslUsage" : {
      "isSSLEnabled" : false
    },
    "threat" : {
      "acPolicyHasIntrusion" : true,
      "acRulesWithIntrusion" : 20,
      "isTIDEnabled" : true,
      "threatLicenseUsed" : true
    },
    "urlFiltering" : {
      "acRulesWithURLFiltering" : 10,
      "numberOfACRulesNeedThreatLicense" : 3,
      "numberOfACRulesNeedURLLicense" : 3,
      "urlFilteringLicenseUsed" : true
    }
  }, {
    "deviceInfo" : {
      "deviceManager" : "FMC",
      "deviceModel" : "Cisco Firepower Threat Defense for VMWare",
      "deviceName" : "10.10.17.221",
      "deviceVersion" : "6.4.0-1335",
      "serialNumber" : "9A0NMB3VAL7"
    },
    "malware" : {
      "malwareLicenseUsed" : false,
      "numberOfACRulesNeedMalwareLicense" : 0,
      "numberOfACRulesWithMalware" : 0
    },
    "sslUsage" : {
      "isSSLEnabled" : false
    },
    "threat" : {
      "acPolicyHasIntrusion" : false,
      "acRulesWithIntrusion" : 0,
      "isTIDEnabled" : false,
      "threatLicenseUsed" : false
    },
    "urlFiltering" : {
      "acRulesWithURLFiltering" : 0,
      "urlFilteringLicenseUsed" : false
    }
  }, {
```

```
    "deviceInfo" : {
      "deviceManager" : "FMC",
      "deviceModel" : "Cisco Firepower Threat Defense for VMWare",
      "deviceName" : "10.10.17.222",
      "deviceVersion" : "6.4.0-1335",
      "serialNumber" : "9ATSKTCFNXA"
    },
    "malware" : {
      "malwareLicenseUsed" : true,
      "numberOfACRulesNeedMalwareLicense" : 0,
      "numberOfACRulesWithMalware" : 0
    },
    "sslUsage" : {
      "isSSLEnabled" : false
    },
    "threat" : {
      "acPolicyHasIntrusion" : false,
      "acRulesWithIntrusion" : 0,
      "isTIDEnabled" : false,
      "threatLicenseUsed" : true
    },
    "urlFiltering" : {
      "acRulesWithURLFiltering" : 0,
      "urlFilteringLicenseUsed" : true
    }
  }, {
    "deviceInfo" : {
      "deviceManager" : "FMC",
      "deviceModel" : "Cisco Firepower Threat Defense for VMWare",
      "deviceName" : "10.10.17.223",
      "deviceVersion" : "6.4.0-1335",
      "serialNumber" : "9AP4B2J9BC1"
    },
    "malware" : {
      "malwareLicenseUsed" : true,
      "numberOfACRulesNeedMalwareLicense" : 0,
      "numberOfACRulesWithMalware" : 0
    },
    "sslUsage" : {
      "isSSLEnabled" : false
    },
    "threat" : {
      "acPolicyHasIntrusion" : false,
      "acRulesWithIntrusion" : 0,
      "isTIDEnabled" : false,
      "threatLicenseUsed" : true
    },
    "urlFiltering" : {
      "acRulesWithURLFiltering" : 0,
      "urlFilteringLicenseUsed" : true
    }
  } ]
},
"deploymentData" : {
  "deployJobInfoList" : [ {
    "jobDeviceList" : [ {
      "containerType" : "STANDALONE",
      "deployEndTime" : "1550466953538",
      "deployStartTime" : "1550466890057",
      "deployStatus" : "SUCCEEDED",
      "deviceModel" : "Cisco Firepower Threat Defense for VMWare",
      "deviceOSVersion" : "6.4.0",
      "deviceUuid" : "8918db92-30de-11e9-a576-92cc6a3b249d",
      "pgTypes" : "[PG.FIREWALL.NGFWAccessControlPolicy]",
```

```
      "policyBundleSize" : 3588153
    }, {
      "containerType" : "STANDALONE",
      "deployEndTime" : "1550466953634",
      "deployStartTime" : "1550466890057",
      "deployStatus" : "SUCCEEDED",
      "deviceModel" : "Cisco Firepower Threat Defense for VMWare",
      "deviceOSVersion" : "6.4.0",
      "deviceUuid" : "87cf54e6-30de-11e9-8fdb-ce9d0fc91a42",
      "pgTypes" : "[PG.FIREWALL.NGFWAccessControlPolicy]",
      "policyBundleSize" : 3588172
    }, {
      "containerID" : "5f009744-30fe-11e9-8a70-cd88086eeac0",
      "containerType" : "HAPAIR",
      "deployEndTime" : "1550467052791",
      "deployStartTime" : "1550466890057",
      "deployStatus" : "SUCCEEDED",
      "deviceModel" : "Cisco Firepower Threat Defense for VMWare",
      "deviceOSVersion" : "6.4.0",
      "deviceUuid" : "c8df3b96-30ce-11e9-b5e5-d6beeb6498f5",
      "pgTypes" : "[PG.FIREWALL.NGFWAccessControlPolicy]",
      "policyBundleSize" : 3588212
    } ],
    "jobId" : "12884903350",
    "numberOfDevices" : 3,
    "numberOfFailedDevices" : 0,
    "numberOfSuccessDevices" : 3
  } ],
  "lastJobId" : "12884903350"
},
"cspa" : {
  "cspaCount" : 0,
  "queryCount" : 0,
  "queryGroupCount" : 0
},
"analysis" : {
  "crossLaunchInfo" : {
    "count" : 28,
    "enabledCount" : 28,
    "iocInfo" : [ {
      "domain" : 10,
      "ip" : 9,
      "sha256" : 9
    } ]
  }
},
"SSLStats" : {
  "action" : {
    "block" : 10,
    "block_with_reset" : 4,
    "decrypt_resign_self_signed" : 0,
    "decrypt_resign_self_signed_replace_key_only" : 0,
    "decrypt_resign_signed_cert" : 227,
    "decrypt_with_known_key" : 0,
    "do_not_decrypt" : 9094
  },
  "cache_status" : {
    "cached_session" : 18693,
    "cert_validation_cache_hit" : 0,
    "cert_validation_cache_miss" : 10883,
    "orig_cert_cache_hit" : 15720,
    "orig_cert_cache_miss" : 0,
    "resigned_cert_cache_hit" : 14,
    "resigned_cert_cache_miss" : 4,
```

```
      "session_cache_hit" : 4398,
      "session_cache_miss" : 1922
    },
    "cert_status" : {
      "cert_expired" : 155,
      "cert_invalid_issuer" : 866,
      "cert_invalid_signature" : 0,
      "cert_not_checked" : 1594,
      "cert_not_yet_valid" : 0,
      "cert_revoked" : 0,
      "cert_self_signed" : 362,
      "cert_unknown" : 0,
      "cert_valid" : 9659
    },
    "failure_reason" : {
      "decryption_error" : 0,
      "handshake_error_before_verdict" : 254,
      "handshake_error_during_verdict" : 17,
      "ssl_compression" : 0,
      "uncached_session" : 984,
      "undecryptable_in_passive_mode" : 0,
      "unknown_cipher_suite" : 56,
      "unsupported_cipher_suite" : 125
    },
    "version" : {
      "ssl_v20" : 0,
      "ssl_v30" : 0,
      "ssl_version_unknown" : 10,
      "tls_v10" : 32,
      "tls_v11" : 8,
      "tls_v12" : 11355,
      "tls_v13" : 922
    }
  },
  "snortRestart" : {
    "appDetectorSnortRestartCnt" : 3,
    "appSnortRestartCnt" : 1
  }
}
```


Cisco Success Network の登録の変更

Cisco Smart Software Manager に Firepower Management Center を登録するときは、Cisco Success Network を有効にします。その後、次の手順を使用して、登録ステータスを表示または変更します。

（注） Cisco Success Network は評価モードでは機能しません。

ステップ 1 [システム（System）] をクリックしてから、**[ライセンス（Licenses）]** > **[スマートライセンス（Smart Licenses）]** をクリックします。

ステップ 2 スマート ライセンスのステータスの下で、Cisco Success Network の横にある、Cisco Success Network 機能の [有効/無効（Enabled/Disabled）] コントロールをクリックして、必要に応じて設定を変更します。

ステップ 3 シスコから提供された情報を読み、[Cisco Success Networkの有効化（Enable Cisco Success Network）] を行うかどうかを選択して、[変更内容を適用（Apply Changes）] をクリックします。

次のタスク

（オプション）（オプション）Web分析トラッキングのオプトアウト（1326ページ）を参照してください。

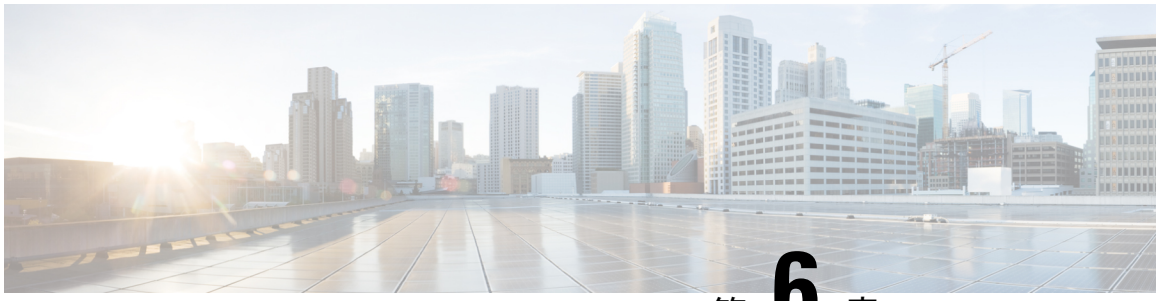
エンドユーザ ライセンス契約書

本製品の使用について規定するシスコ エンドユーザ ライセンス契約書（EULA）および適用される補足契約書（SEULA）は、http://www.cisco.com/go/softwareterms から入手できます。

ライセンスの履歴

機能	バージョン	詳細
Firepower 4100/9300 の FTD に対する複数インスタンス機能のライセンス	6.3	Firepower 4100/9300 に複数の FTD コンテナインスタンスを展開できるようになりました。セキュリティ モジュール/エンジンの機能ごとに必要なライセンスは 1 つのみです。基本ライセンスは、各インスタンスに自動的に割り当てられます。 新規/変更された画面：**[システム（System）] > [ライセンス（Licenses）] > [スマートライセンス（Smart Licenses）]** サポート対象プラットフォーム：Firepower 4100/9300 の FTD

機能	バージョン	詳細
エアギャップ展開に対する特定のライセンスの予約	6.3	展開でインターネットに接続してシスコのライセンス認証局と通信できない顧客は特定のライセンスの予約を使用できます。詳細については、特定のライセンスの予約の概要 （119 ページ）を参照してください。 新規/変更された画面：**[システム（System）] > [ライセンス（Licenses）] > [特定のライセンス（Specific Licenses）]**（このオプションはデフォルトでは使用できません。） サポートされるプラットフォーム：FMC、FTD
制限付きの顧客の輸出規制対象機能	6.3	スマートアカウントで制限付き機能を使用する資格を持たない特定の顧客は、期間ベースのライセンスを承認を受けて購入することができます。詳細については、輸出規制機能の有効化（グローバル権限のないアカウントの場合） （115 ページ）を参照してください。 サポートされるプラットフォーム：FMC、FTD
Firepower Threat Defense デバイスのスマートライセンスを展開するための拡張手順	6.3	新しいトピックFirepower Threat Defense デバイスのライセンス （96 ページ）で、エンドツーエンドのガイダンスを提供しています。また、このトピックからリンクされているトピックでも、新しいよりよい情報を提供しています。



第 6 章

システム ソフトウェアの更新

次のトピックでは、Firepower の展開を更新する方法について説明します。

FirePOWER の更新について

シスコでは、Firepower の展開に対していくつかの種類のアップグレードと更新を配信しています。リリース ノートまたはアドバイザリ テキストに特に記載されていない限り、更新しても設定は変更されません。メジャー アップグレードはアンインストールできません。また、VDB、GeoDB、SRU を前のバージョンに戻すこともできません。

表 *20 : Firepower* のアップグレードと更新

更新のタイプ	説明	ドメイン
メジャー アップグレード	新機能が含まれており、製品の大規模な変更を伴うことがあります。 新規インストールまたは復元はできますが、アンインストールはできません。 オペレーティング システムを個別にアップグレードするデバイスの場合、付随するオペレーティング システムのアップグレードを伴うことがあります。 シスコ エンドユーザ ライセンス契約（EULA）の再承認が必要な場合があります。	グローバルのみ

更新のタイプ	説明	ドメイン
マイナー アップグレード（パッチ）	限られた範囲の修正が含まれています。 アンインストールできますが、新規インストールまたは復元はできません。メジャー バージョンに復元してからマイナー バージョンにアップグレードする必要があります。	グローバルのみ
脆弱性データベース（VDB）	動的分析の対象となる脆弱性、オペレーティング システム、アプリケーション、クライアント、およびファイル タイプの検出を更新します。	グローバルのみ
侵入ルールの更新（SRU）	新規および更新された侵入ルールおよびプリプロセッサ ルール、既存のルールの変更後のステータス、デフォルト侵入ポリシーの変更後の設定が提供されます。 ルールが削除されたり、新しいルール カテゴリとデフォルトの変数が提供されたり、デフォルトの変数値が変更されたりすることもあります。	シスコ提供：グローバルのみ ローカル インポート：任意
位置情報データベース（GeoDB）	物理的な場所や接続タイプなど、検出されたルート可能な IP アドレスに関連付けることができるものに関する情報を更新します。GeoDB をインストールして地理的位置情報の詳細を表示するか、または地理的位置情報ベースのアクセス制御を実行します。	グローバルのみ

Firepower 更新のガイドラインおよび制限事項

更新する前に

Firepower 展開のいずれかのコンポーネント（VDB、GeoDB、SRU など）を更新する前に、更新に付属しているリリース ノートまたはアドバイザリ テキストを読んでおく必要があります。これらは、互換性、前提条件、新機能、動作の変更、警告など、重要かつリリースに固有の情報を提供します。

Firepower Management Center 展開のシステム ソフトウェア アップグレードを準備して正常に完了する方法の詳細については、『Cisco Firepower Management Center Upgrade Guide』を参照してください。

帯域幅のガイドライン

更新には、Firepower Management Center から管理対象デバイスへの大量のデータ転送が必要になる場合があります。開始する前に、管理ネットワークに、転送を正常に実行するために十分な帯域幅があることを確認してください。https://www.cisco.com/c/en/us/support/docs/security/firepower-management-center/212043-Guidelines-for-Downloading-Data-from-the.html で、トラブルシューティングのテクニカル ノートを参照してください。

Firepower システム ソフトウェアのアップグレード

Firepower Management Center 展開のアップグレードは、複雑なプロセスになることがあります。慎重に計画および準備することで、失敗を回避することができます。アップグレードプロセスの一部として、アップグレードスクリプトを呼び出す機械的な手順を実際に実行することと同じくらい、計画と準備を検討する必要があります。

このプロセスの最初の手順は、展開を評価し、アップグレードパス、すなわちアップグレードするアプライアンス、アップグレードするコンポーネント、およびその順序の詳細な計画を作成することです。アップグレード パスは、次の条件を満たす必要があります。

- マネージャとデバイスの互換性を維持します。
- 必要に応じて、オペレーティング システムとホスティング環境のアップグレードを含めます。
- バックアップ、パッケージのダウンロードとプッシュ、準備状況チェック、帯域幅とディスク容量のチェック、アップグレード前後の設定変更などの、その他のタスクを含めます。
- トラフィック フローおよびインスペクションでの潜在的な中断を特定します。

Firepower Management Center 展開のアップグレードを準備して正常に完了する方法の詳細については、『Cisco Firepower Management Center Upgrade Guide』を参照してください。

脆弱性データベース（VDB）の手動による更新

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	任意	任意	グローバルのみ	管理者

Cisco Vulnerability Database（VDB）は、オペレーティングシステム、クライアント、およびアプリケーションのフィンガープリントだけでなく、ホストが影響を受ける可能性がある既知の脆弱性のデータベースです。システムでは、VDB を使用して、特定のホストで感染のリスクが高まるかどうかを判断します。

Cisco Talos Intelligence Group（Talos）では、VDB の定期的な更新を配布しています。Firepower Management Center で VDB と関連付けられたマッピングの更新にかかる時間は、ネットワークマップ内のホストの数によって異なります。一般的に、更新の実行にかかるおおよその時間（分）を判断するには、ホストの数を 1000 で割ります。

Firepower Management Center でインターネット アクセスができない、または VDB 更新を手動で Firepower Management Center へアップロードする場合は、この手順を使用します。VDB 更新を自動化するには、タスクのスケジューリング（**[システム（System）]**>**[ツール（Tools）]**>**[スケジューリング（Scheduling）]**）を使用します。詳細は、脆弱性データベースの更新の自動化 （252 ページ）を参照してください。

重要 自動 VDB 更新をスケジュールしない場合は、これらの更新を定期的にチェックする必要があります。更新は毎日 1 回だけ実行され、https://www.cisco.com/go/firepower-software の適切な子ページに掲載されます。

注意 脆弱性データベース（VDB）の更新のインストールを開始するために Firepower Management Center を選択すると警告が表示される場合は、VDB のインストール後に設定を展開し、Snort プロセスの展開を再開する必要があります。Firepower Threat Defense デバイスへの展開の保留に関する追加の警告が展開ダイアログに表示されます。展開の中断中にインスペクションを続行せずにトラフィックをドロップするか、パスするかは、対象デバイスによるトラフィックの処理方法によって異なります。詳細については、Snort® の再起動によるトラフィックの動作（451 ページ）を参照してください。Firepower Management Center にのみ適用される VDB の更新では再起動が行われないため、更新を展開できません。

始める前に

- https://www.cisco.com/go/firepower-software から更新プログラムをダウンロードします。
- Snort の再起動が発生するため、トラフィック フローとインスペクションに更新による影響があることを考慮します。メンテナンス ウィンドウ期間に更新を実行することをお勧めします。

ステップ 1 **[System]** > **[Updates]** を選択し、[製品の更新（Product Updates）] タブをクリックします。

ステップ 2 VDB 更新の Firepower Management Center へのアップロード方法を選択します。

- Cisco.com から直接ダウンロード：[アップデートのダウンロード（Download Updates）] をクリックします。シスコ サポートおよびダウンロード サイトにアクセスできる場合、Firepower Management Center は最新の VDB をダウンロードします。Firepower Management Center は、アプライアンスが現在実行しているバージョンに関連付けられている各パッチとホットフィックスのパッケージもダウンロードする点に注意してください（ただし、メジャー リリースは含まれない）。
- 手動でアップロード：[更新のアップロード（Upload Update）] をクリックして、[ファイルの選択（Choose File）] をクリックします。ダウンロードした更新を参照して、[アップロード（Upload）] をクリックします。

VDB 更新は、Firepower ソフトウェアのアップグレードおよびアンインストーラ パッケージと同じページに表示されます。

ステップ 3 更新をインストールします。

a) [脆弱性およびフィンガープリント データベースの更新（Vulnerability and Fingerprint Database update）] の横にある [Install（インストール）] アイコンをクリックします。
b) Firepower Management Center を選択します。
c) [Install（インストール）] をクリックします。

ステップ 4 （オプション）メッセージ センターで更新の進行状況をモニタします。

更新が完了するまで、マッピングされた脆弱性に関連するタスクを実行しないでください。メッセージセンターに進行状況が数分間表示されない、または更新が失敗したことが示されている場合でも、更新を再開しないでください。代わりに、Cisco TAC にお問い合わせください。

更新の完了後に、システムで新しい脆弱性情報が使用されます。ただし、更新されたアプリケーションディテクタとオペレーティング システム フィンガープリントを有効にするために、展開する必要があります。

ステップ 5 更新が成功したことを確認します。

現在の VDB バージョンを表示するには、**[ヘルプ（Help）]** > **[バージョン情報（About）]** を選択します。

次のタスク

設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

設定を展開

地理位置情報データベース（GeoDB）の更新

シスコ地理位置情報データベース（GeoDB）は、ルーティング可能な IP アドレスと関連付けられた地理的データ（国、都市、座標など）および接続関連のデータ（インターネット サービス プロバイダー、ドメイン名、接続タイプなど）のデータベースです。検出された IP アドレスと一致する GeoDB 情報が検出された場合は、その IP アドレスに関連付けられている位置情報を表示できます。国や大陸以外の位置情報の詳細を表示するには、システムに GeoDB をインストールする必要があります。シスコでは、GeoDB の定期的な更新を提供しています。

GeoDB を更新するには、Firepower Management Center で [位置情報の更新（Geolocation Updates）] ページ（**[システム（System）]** > **[更新（Updates）]** > **[位置情報の更新（Geolocation Updates）]**）を使用します。サポートまたは自身のアプライアンスから取得した GeoDB の更新をアップロードすると、それらがこのページに表示されます。

（注） [位置情報の更新（Geolocation Updates）] ページで [位置情報の更新をサポート サイトからダウンロードおよびインストールする（Download and install geolocation update from the Support Site）] をクリックするか、または手動でサポート サイトから更新を直接ダウンロードします。電子メールで更新ファイルを転送すると、ファイルが破損することがあります。

GeoDB の更新にかかる時間はアプライアンスによって異なります。インストールには通常、30 ～ 40 分かかります。GeoDB の更新は他のシステムの機能（実行中の地理情報の収集など）を中断することはありませんが、更新が完了するまでシステムのリソースを消費します。更新を計画する場合には、この点について考慮してください。

GeoDB を更新すると、GeoDB の以前のバージョンが上書きされ、すぐに有効になります。GeoDB を更新すると、Firepower Management Center により、管理対象デバイス上の関連データが自動的に更新されます。GeoDB の更新が展開全体で有効になるまでに数分かかることがあります。更新後に再度展開する必要はありません。

手動による GeoDB の更新（インターネット接続）

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	任意	任意	グローバルのみ	管理者

新しい GeoDB 更新プログラムは、アプライアンスがインターネットにアクセスできる場合にのみ、サポート サイトに接続することで自動的にインポートできます。

ステップ 1 **[System]** > **[Updates]**を選択します。

ステップ 2 [位置情報の更新（Geolocation Updates）] タブをクリックします。

ステップ 3 [サポート サイトから地理位置情報の更新をダウンロードしてインストールする（Download and install geolocation update from the Support Site）] を選択します。

ステップ 4 [インポート（Import）] をクリックします。
システムは [地理位置情報の更新（Geolocation Update）] タスクをキューに入れます。このタスクは、最新の更新について、シスコ サポート サイト（http://www.cisco.com/cisco/web/support/index.html）で確認します。

ステップ 5 必要に応じて、タスクのステータスをモニタします。タスク メッセージの表示 （417 ページ）を参照してください。

ステップ 6 更新が終了したら、[地理位置情報の更新（Geolocation Updates）] ページに戻るか、**[ヘルプ（Help）]** > **[バージョン情報（About）]** を選択して、GeoDB のビルド番号がインストールした更新と一致していることを確認します。

地理位置情報データベース（GeoDB）の手動更新：インターネット接続なし

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	任意	任意	グローバルのみ	管理者

Firepower Management Center がインターネットにアクセスできない場合は、シスコ サポート サイトからネットワーク上のローカル マシンに GeoDB の更新をダウンロードして、その更新を手動で Firepower Management Center にアップロードできます。

ステップ 1 シスコのサポート サイト（http://www.cisco.com/cisco/web/support/index.html）から更新を手動でダウンロードします。

ステップ 2 **[System]** > **[Updates]**を選択します。

ステップ 3 [位置情報の更新（Geolocation Updates）] タブをクリックします。

ステップ 4 [地理位置情報の更新のアップロードとインストール（Upload and install geolocation update）] を選択します。

ステップ 5 ダウンロードした更新を参照して、[アップロード（Upload）] をクリックします。

ステップ 6 [インポート（Import）] をクリックします。

ステップ 7 必要に応じて、タスクのステータスをモニタします。タスク メッセージの表示 （417 ページ）を参照してください。

ステップ 8 更新が終了したら、[地理位置情報の更新（Geolocation Updates）] ページに戻るか、**[ヘルプ（Help）]** > **[バージョン情報（About）]** を選択して、GeoDB のビルド番号がインストールした更新と一致していることを確認します。

GeoDB 更新のスケジューリング

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	グローバルだけ。	Admin

Firepower Management Center でインターネット アクセスができる場合、週ごとの GeoDB 更新をお勧めします。

始める前に

Firepower Management Center でインターネットにアクセスできることを確認します。

ステップ 1 **[System]** > **[Updates]** を選択し、[ジオロケーションの更新（Geolocation Updates）] タブをクリックします。

ステップ 2 [位置情報の定期更新（Recurring Geolocation Updates）] で、[週ごとの定期更新を有効にする（Enable Recurring Weekly Updates）] をオンにします。

ステップ 3 [開始時刻の更新（Update Start Time）] を指定します。

ステップ 4 **[保存（Save）]** をクリックします。

侵入ルールの更新

新しい脆弱性が明らかになるのに伴い、Cisco Talos Intelligence Group（Talos）は侵入ルールの更新をリリースします。これらの更新を Firepower Management Center にインポートして、変更後の設定を管理対象デバイスに導入することで、侵入ルールの更新を実装できます。それらの

更新は、侵入ルール、プリプロセッサルール、およびルールを使用するポリシーに影響を及ぼします。

侵入ルール更新は更新を累積されていくものなので、常に最新の更新をインポートすることをお勧めします。現在インストールされているルールのバージョン以前の侵入ルールの更新をインポートすることはできません。

侵入ルールの更新では、次のものを提供します。

- **新規または変更されたルールおよびルール状態**：ルール更新は、新規および更新された侵入ルールとプリプロセッサルールを提供します。新しいルールについては、ルールの状態がそれぞれのシステム提供の侵入ポリシーで異なる場合があります。たとえば、Security over Connectivity の侵入ポリシーでは新しいルールが有効になっており、Connectivity over Security の侵入ポリシーでは無効になっていることがあります。ルールの更新では、既存のルールのデフォルト状態が変更されたり、既存のルールそのものが削除されることもあります。
- **新しいルール カテゴリ**：ルール更新には、常に追加される新しいルール カテゴリが含まれている場合があります。
- **変更されたプリプロセッサおよび詳細設定**：ルール更新によって、システム提供の侵入ポリシーの詳細設定、およびシステム提供のネットワーク分析ポリシーのプリプロセッサ設定が変更されることがあります。また、アクセス コントロール ポリシーの高度な前処理およびパフォーマンスのオプションのデフォルト値も変更される場合があります。
- **新規および変更された変数**：ルール更新によって、既存のデフォルト変数のデフォルト値が変更されることがありますが、ユーザによる変更は上書きされません。新しい変数が常に追加されます。

マルチドメイン展開では、ローカル侵入ルールを任意のドメインにインポートできますが、グローバル ドメイン内の Talos からでなければ、侵入ルールの更新をインポートすることはできません。

侵入ルールの更新によってポリシーが変更されるタイミングについて

侵入ルールの更新は、システムが提供するネットワーク分析ポリシーとカスタム ネットワーク分析ポリシーの両方だけでなく、すべてのアクセス コントロール ポリシーにも影響する場合があります。

- **システム提供**：システムが提供するネットワーク解析および侵入ポリシーへの変更は、その他のアクセス コントロールの詳細設定と同様に、更新後にポリシーを再適用すると自動的に有効になります。
- **カスタム**：カスタムのネットワーク解析および侵入ポリシーは、いずれもシステム提供のポリシーをベースとして使用するか、ポリシー チェーン中でのイベント ベースとして使用しているので、ルール更新がカスタムのネットワーク解析および侵入ポリシーにも影響を与えることがあります。ただし、ルール更新によるこれらの自動的な変更が行われないようにすることができます。これにより、ルール更新のインポートとは関係ないスケジュールで、システムによって提供される基本ポリシーを手動で更新できます。ユーザによる選

択とは関係なく（カスタムポリシーごとに実装）システム提供のポリシーに対する更新では、ユーザがカスタマイズした設定は上書き**されません**。

ルール更新をインポートすると、ネットワーク分析ポリシーと侵入ポリシーのキャッシュされていた変更がすべて廃棄されるので注意してください。便宜のために、[ルールの更新（Rule Updates）]ページには、キャッシュされている変更があるポリシー、および変更を行ったユーザが表示されます。

侵入ルールの更新の展開

侵入ルールの更新によって行われた変更を有効にするには、設定を再導入する必要があります。侵入ルールの更新をインポートする際に、影響を受けるデバイスに自動的に再導入するようシステムを設定できます。この手法が特に役立つのは、侵入ルールの更新によるシステム提供の基本侵入ポリシーの変更を許可する場合です。

侵入ルールの更新の繰り返し

[ルールの更新（Rule Updates）]ページを使用して、ルール更新を日次、週次、または月次ベースでインポートすることができます。

展開に高可用性ペアの Firepower Management Center が含まれる場合は、プライマリ側だけに更新をインポートします。セカンダリ Firepower Management Center は、通常の同期プロセスの一環としてルールの更新を受け取ります。

侵入ルールの更新のインポートに適用されるサブタスクは、ダウンロード、インストール、ベースポリシーの更新、設定の展開の順で実行されます。1 つのサブタスクが完了すると、次のサブタスクが開始されます。

スケジュールされた時間になると、システムはルールの更新をインストールして、前のステップで指定したように変更後の設定を展開します。インポートの前、またはインポート中にログオフすることも、Web インターフェイスを使用して他のタスクを実行することもできます。インポート中にアクセスした場合は、[Rule Update Log] に赤いステータスのアイコン（  ）が表示され、[Rule Update Log] 詳細ビューでは表示されたメッセージを確認できます。ルール更新のサイズと内容によっては、ステータスメッセージが表示されるまでに数分かかることがあります。

ローカル侵入ルールのインポート

ローカル侵入ルールは、ASCII または UTF-8 エンコーディングによるプレーン テキスト ファイルとしてローカル マシンからインポートするカスタム標準テキスト ルールです。Snort ユーザ マニュアル（http://www.snort.org で入手可能）の指示に従って、ローカル ルールを作成することができます。

マルチドメイン展開では、任意のドメインにローカル侵入ルールをインポートできます。現在のドメインと親ドメインにインポートされたローカル侵入ルールを表示できます。

侵入ルールのワンタイム手動更新

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	任意	任意	グローバルだけ。	管理者

Firepower Management Center にインターネット アクセスがない場合、新しい侵入ルールの更新を手動でインポートします。

ステップ 1 シスコのサポート サイト（http://www.cisco.com/cisco/web/support/index.html）から更新を手動でダウンロードします。

ステップ 2 **[System]** > **[Updates]** を選択し、[ルールの更新（Rule Updates）] タブをクリックします。

ステップ 3 削除されるフォルダに作成またはインポートしたすべてのユーザ定義ルールを移動する場合、ツールバーで [すべてのローカル ルールの削除（Delete All Local Rules）] をクリックして [OK] をクリックする必要があります。

ステップ 4 [アップロードおよびインストールするルールの更新またはテキスト ルール ファイル（Rule Update or text rule file to upload and install）] を選択し、[参照（Browse）] をクリックして、ルール アップデート ファイルを選択します。

ステップ 5 更新が完了した後に、ポリシーを管理対象デバイスに自動的に再展開する場合、[ルールの更新のインポートが完了した後にすべてのポリシーを再適用する（Reapply all policies after the rule update import completes）] をオンにします。

ステップ 6 [インポート（Import）] をクリックします。ルールの更新がインストールされ、[ルール アップデート ログ（Rule Update Log）] 詳細ビューが表示されます。

（注） ルール更新のインストール中にエラー メッセージが表示された場合は、サポートに連絡してください。

侵入ルールのワンタイム自動更新

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	任意	任意	グローバルのみ	管理者

新しい侵入ルールの更新を自動的にインポートするには、サポート サイトに接続するためのインターネット アクセスがアプライアンスで必要になります。

始める前に

- Firepower Management Center にインターネット アクセス権があることを確認してください（セキュリティ、インターネットアクセス、および通信ポート（3281 ページ） を参照）。

ステップ 1 **[System]** > **[Updates]**を選択します。

ステップ 2 [ルールの更新（Rule Updates）] タブをクリックします。

ステップ 3 作成した、または削除されたフォルダにインポートしたすべてのユーザ定義ルールを移動するには、ツールバーで [すべてのローカル ルールの削除（Delete All Local Rules）] をクリックし、[OK] をクリックします。

ステップ 4 [サポート サイトから新しいルールの更新をダウンロードする（Download new Rule Update from the Support Site）] を選択します。

ステップ 5 更新が完了した後に、変更した設定を管理対象デバイスに自動的に再展開する場合、[ルールの更新のインポートが完了した後にすべてのポリシーを再適用する（Reapply all policies after the rule update import completes）] チェックボックスをオンにします。

ステップ 6 [インポート（Import）] をクリックします。
ルールの更新がインストールされ、[ルール アップデート ログ（Rule Update Log）] 詳細ビューが表示されます。

注意 ルール更新のインストール中にエラー メッセージが表示された場合は、サポートに連絡してください。

定期的な侵入ルール更新の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	任意	任意	グローバルのみ	管理者

ステップ 1 **[System]** > **[Updates]**を選択します。

ステップ 2 [ルールの更新（Rule Updates）] タブをクリックします。

ステップ 3 作成した、または削除されたフォルダにインポートしたすべてのユーザ定義ルールを移動するには、ツールバーで [すべてのローカル ルールの削除（Delete All Local Rules）] をクリックし、[OK] をクリックします。

ステップ 4 [ルール アップデートの再帰的なインポートを有効にする（Enable Recurring Rule Update Imports）] チェックボックスをオンにします。

[ルール アップデートの再帰的なインポート（Recurring Rule Update Imports）] セクションの見出しの下に、インポート ステータスに関するメッセージが表示されます。

ステップ 5 [インポート頻度（Import Frequency）] フィールドで、次を指定します。

- 更新の頻度（[日次（Daily）]、[週次（Weekly）]、または [月次（Monthly）]）。
- 更新が必要な曜日または日付。
- 更新を開始する時刻。

ステップ 6 更新の完了後、変更された設定を管理対象デバイスに自動的に再展開するには、[ルール更新の完了後、更新されたポリシーを管理対象デバイスに展開する（Deploy updated policies to targeted devices after rule update completes）] チェックボックスをオンにします。

ステップ 7 [保存（Save）] をクリックします。

注意 侵入ルール更新のインストール中にエラー メッセージが表示された場合は、サポートに連絡してください。

[ルール アップデートの再帰的なインポート（Recurring Rule Update Imports）] セクションの見出しの下のステータス メッセージが変わり、ルールの更新がまだ実行されていないことが示されます。

ローカル侵入ルールのインポートのガイドライン

ローカル ルール ファイルをインポートする際には次のガイドラインに従います。

- ルールのインポータには、すべてのカスタム ルールが ASCII または UTF-8 でエンコードされるプレーン テキスト ファイルにインポートされることが必要です。
- テキストファイル名には英数字とスペースを使用できますが、下線（_）、ピリオド（.）、ダッシュ（-）以外の特殊記号は使用できません。
- システムは、単一のポンド文字（#）で始まるローカル ルールをインポートしますが、これらには削除のフラグが立てられます。
- 単一のポンド文字（#）で始まるローカル ルールはインポートされますが、2 つのポンド文字（##）で始まるローカル ルールはインポートされません。
- ルールにはエスケープ文字を含めることはできません。
- マルチドメイン展開では、グローバル ドメインにインポートまたは作成されたルールに 1 の GID が割り当てられ、他のすべてのドメインには 1000 ～ 2000 の間のドメイン固有 GID が割り当てられます。
- ローカル ルールをインポートするときにはジェネレータ ID（GID）を指定する必要はありません。指定する場合は、標準テキスト ルールに GID 1 のみを指定します。
- ルールを初めてインポートするときには、[Snort ID]（SID）またはリビジョン番号を指定しないでください。これにより、削除されたルールを含むその他のルールの SID の競合を回避できます。システムはルールに対して、1000000 以上の次に使用できるカスタム ルール SID 、およびリビジョン番号 の 1 を自動的に割り当てます。

  SID を持つルールをインポートする必要がある場合、SID には 1,000,000 以上の一意の番号を指定できます。

  マルチドメイン展開で、複数の管理者がローカル ルールを同時にインポートする場合、個々のドメイン内の SID が連続していないように見える場合があります。これは、シーケンス内の途中の数字が別のドメインに割り込んで指定されたためです。

- 以前にインポートしたローカル ルールの更新バージョンをインポートするとき、または削除したローカル ルールを元に戻すときは、システムによって指定された SID および現在のリビジョン番号より大きいリビジョン番号を含める必要があります。ルールを編集して、現在のルールまたは削除されたルールのリビジョン番号を判別できます。

（注） ローカル ルールを削除すると、システムは自動的にリビジョン番号を増やします。これは、ローカル ルールを元に戻すための方法です。削除されたすべてのローカル ルールは、ローカル ルール カテゴリから、削除されたルール カテゴリへ移動されます。

- SID 番号の問題を回避するには、ハイ アベイラビリティ ペアのプライマリ Firepower Management Center でローカル ルールをインポートします。
- ルールに次のいずれかが含まれていると、インポートに失敗します。
  - 2147483647 より大きい SID。
  - 64 文字よりも長い送信元ポートまたは宛先ポートのリスト。
  - マルチドメイン展開でグローバル ドメインにインポートする場合、GID:SID の組み合わせでは、別のドメインに既に存在する GID 1 と SID を使用します。これは、バージョン 6.2.1 より前に組み合わせが存在していたことを示します。GID 1 と固有の SID を使用してルールを再インポートできます。
- 非推奨の `threshold` キーワードと侵入イベントしきい値機能を組み合わせて使用しているローカル ルールをインポートして、侵入ポリシーで有効にすると、ポリシーの検証に失敗します。
- インポートされたすべてのローカル ルールは、ローカル ルール カテゴリに自動的に保存されます。
- システムによって、インポートしたローカル ルールは常に無効なルール状態に設定されます。ローカル ルールを侵入ポリシーで使用できるようにするには、ローカル ルールの状態を手動で設定する必要があります。

ローカル侵入ルールのインポート

- ローカル ルール ファイルが、ローカル侵入ルールのインポートのガイドライン（190 ページ）に記載されているガイドラインに従っていることを確認します。
- ローカル侵入ルールのインポート プロセスが、自身のセキュリティ ポリシーに適合していることを確認します。
- 帯域幅の制約や Snort の再起動が発生するため、トラフィック フローとインスペクションにインポートによる影響があることを考慮します。メンテナンス ウィンドウ期間にルール更新をスケジュールすることをお勧めします。

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	任意	任意	任意	管理者

ローカル侵入ルールをインポートするには、次の手順を使用します。インポートされた侵入ルールは、無効状態でローカル ルール カテゴリに表示されます。

ステップ 1 **[System]** > **[Updates]** を選択し、[ルールの更新（Rule Updates）] タブをクリックします。

ステップ 2 （オプション）既存のローカル ルールを削除します。

[すべてのローカルルールの削除（Delete All Local Rules）] をクリックして、すべての作成およびインポートされた侵入ルールを削除フォルダに移動することを確認します。

ステップ 3 [ワンタイムルール更新/ルールインポート（One-Time Rule Update/Rules Import）] で、[ルールの更新またはテキストルールファイル...（Rule update or text rule file...）] を選択して、[ファイルの選択（Choose File）] をクリックしたら、ローカル ルール ファイルを参照します。

ステップ 4 [インポート（Import）] をクリックします。

ステップ 5 メッセージ センターでインポートの進行状況をモニタします。

メッセージ センターを表示するには、メニュー バーの [システムステータス（System Status）] アイコンをクリックします。メッセージセンターに進行状況が数分間表示されない、またはインポートが失敗したことが示されている場合でも、インポートを再起動しません。代わりに、Cisco TAC に連絡してください。

次のタスク

- 侵入ポリシーを編集し、インポートしたルールを有効にします。
- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

ルールの更新ログ

Firepower Management Center は、ユーザがインポートする各ルール更新およびローカル ルール ファイルごとに 1 つのレコードを生成します。

各レコードにはタイム スタンプ、ファイルをインポートしたユーザ名、およびインポートが正常に終了したか失敗したかを示すステータス アイコンが含まれています。ユーザは、インポートしたすべてのルール更新とローカル ルール ファイルのリストを管理したり、リストからレコードを削除したり、インポートしたすべてのルールとルール更新コンポーネントに関する詳細レコードにアクセスすることができます。

[Rule Update Import Log] 詳細ビューには、ルール更新またはローカル ルール ファイルにインポートされた各オブジェクトの詳細レコードが表示されます。表示されるレコードのうち、自分のニーズに合う情報のみを含むカスタム ワークフローまたはレポートを作成することもできます。

侵入ルール更新のログ テーブル

表 *21 :* 侵入ルール更新のログ フィールド

フィールド	説明
Summary	インポート ファイルの名前。インポートが失敗した場合は、ファイル名の下に、失敗した理由の簡単な説明が表示されます。
Time	インポートが開始された日時。
User ID	インポートをトリガーとして使用したユーザ名。
Status	インポートの状態を表します • 正常終了（） • 失敗、または実行中（） インポート中には [ルールアップデートログ（Rule Update Log）] ページで、正常終了しなかった、または完了していないことを示す赤いステータス アイコンが表示され、インポートが正常終了した場合のみこれが緑色のアイコンに変わります。

ヒント　侵入ルール更新のインポートの進行中に示される、インポートの詳細を表示することができます。

侵入ルールの更新ログの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

ステップ 1　**[System]** > **[Updates]** を選択します。

ヒント　侵入ルール エディタ ページ（**[Objects]** > **[Intrusion Rules]**）の [インポート ページ（Import Rules）] をクリックすることもできます。

ステップ 2 [ルールの更新（Rule Updates）] タブをクリックします。

ステップ 3 [ルールアップデートログ（Rule Update Log）] をクリックします。

ステップ 4 次の 2 つの対処法があります。

- 詳細の表示：ルールの更新またはローカル ルール ファイルにインポートされる各オブジェクトの詳細を表示するには、表示するファイルの横にある表示アイコン（  ）をクリックします（侵入ルールの更新インポート ログの詳細の表示 （196 ページ）を参照）。
- 削除：インポート ログからインポート ファイル レコード（ファイルに含まれるすべてのオブジェクトに関する詳細レコードを含む）を削除するには、インポート ファイル名の横にある削除アイコン（  ）をクリックします。

（注） ログからファイルを削除しても、インポート ファイルにインポートされているオブジェクトはいずれも削除されませんが、インポート ログ レコードのみは削除されます。

侵入ルール更新ログのフィールド

ヒント 1 つのインポート ファイルのレコードのみが表示されている [ルール アップデートのインポート ログ（Rule Update Import Log）] 詳細ビューからツールバーの [検索（Search）] をクリックして検索を開始した場合でも、[ルール アップデートのインポート ログ（Rule Update Import Log）]データベースの全体が検索されます。検索の対象とするすべてのオブジェクトが含まれるように、時間制限が設定されていることを確認します。

表 *22 : [*ルール アップデートのインポート ログ（***Rule Update Import Log***）*]* 詳細ビューのフィールド

フィールド	説明
Action	オブジェクト タイプについて、次のいずれかが発生していることを示します。 • [new]（ルールで、このアプライアンスにルールが最初に格納された場合） • [changed]（ルール更新コンポーネントまたはルールで、ルール更新コンポーネントが変更された場合、ルールのリビジョン番号が大きく、GID と SID が同じだった場合） • [collision]（ルール更新コンポーネントまたはルールで、アプライアンス上の既存のコンポーネントまたはルールとリビジョンの競合によりインポートがスキップされた場合） • [deleted]（ルール用。ルール更新からルールが削除された場合） • [enabled]（ルール更新の編集で、プリプロセッサ、ルール、または他の機能が、システムで提供されるデフォルトポリシーで有効になっていた場合） • [disabled]（ルールで、システム提供のデフォルトポリシーでルールが無効になっていた場合） • [drop]（ルールで、システムで提供されるデフォルトポリシーで、ルールが [Drop and Generate Events] に設定されていた場合） • [error]（ルール更新またはローカルルールファイル用。インポートに失敗した場合） • [apply]（インポートに対して [Reapply all policies after the rule update import completes] オプションが有効だった場合）
Default Action	ルールの更新によって定義されているデフォルトのアクション。インポートされたオブジェクトのタイプが [rule] の場合、デフォルトのアクションは [Pass]、[Alert]、または [Drop] になります。インポートされた他のすべてのオブジェクト タイプには、デフォルトのアクションはありません。
Details	コンポーネントまたはルールに対する一意の文字列。ルール、GID、SID、および変更されたルールの以前のリビジョン番号については、`previously (GID:SID:Rev)` のように表示されます。変更されていないルールについては、このフィールドは空白です。
Domain	侵入ポリシーで更新されたルールを使用できるドメイン。子孫ドメインの侵入ポリシーもルールを使用できます。このフィールドは、マルチドメイン展開の場合にのみ存在します。
GID	ルールのジェネレータ ID。たとえば、`1`（標準テキスト ルール、グローバル ドメインまたは従来の GID）または `3`（共有オブジェクト ルール）。
Name	インポートされたオブジェクトの名前。ルールの場合はルールの [Message] フィールドに対応した名前で、ルール更新コンポーネントの場合はコンポーネント名です。
Policy	インポートされたルールの場合、このフィールドには [すべて（All）] が表示されます。つまり、ルールが正常にインポートされ、適切なデフォルト侵入ポリシーすべてで有効にすることができます。インポートされた他のタイプのオブジェクトについては、このフィールドは空白です。
Rev	ルールのリビジョン番号。

フィールド	説明
Rule Update	ルール更新のファイル名。
SID	ルールの SID。
Time	インポートが開始された日時。
Type	インポートされたオブジェクトのタイプで、有効な値は次のいずれかです。 • [rule update component]（ルール パックまたはポリシー パックなどの、インポートされたコンポーネント） • [ルール（rule）]（ルール用。新しいルールまたは更新されたルール。バージョン 5.0.1 では、廃止された `update` 値の代わりにこの値が使用されます）。 • [ポリシー適用（policy apply）]（インポートに対して [ルール更新のインポート完了後にすべてのポリシーを再適用する（Reapply all policies after the rule update import completes）] オプションが有効だった場合）
Count	各レコードのカウント（1）。テーブルが制限されており、[ルールアップデート ログ（Rule Update Log）] 詳細ビューがデフォルトでルール更新レコードに制限されている場合は、テーブル ビューに [メンバー数（Count）] フィールドが表示されます。このフィールドは検索できません。

侵入ルールの更新インポート ログの詳細の表示

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

ステップ 1 **[System]** > **[Updates]**を選択します。

ステップ 2 [ルールの更新（Rule Updates）] タブをクリックします。

ステップ 3 [ルールアップデートログ（Rule Update Log）] をクリックします。

ステップ 4 表示する詳細レコードが含まれているファイルの隣にある表示アイコン（  ）をクリックします。

ステップ 5 次のいずれかの処理を実行できます。

- ブックマーク：現在のページをブックマークするには、[このページをブックマーク（Bookmark This Page）] をクリックします。
- 検索の編集：現在の単一制約が事前入力されている検索ページを開くには、検索制約の横にある [検索の編集（Edit Search）] または [検索の保存（Save Search）] を選択します。

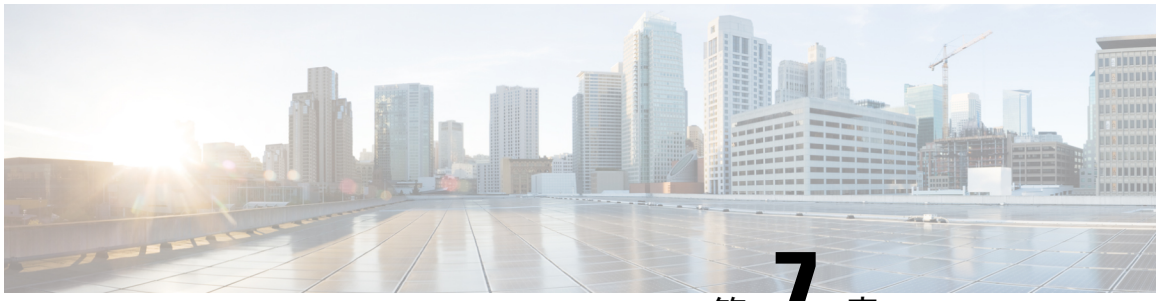
- ブックマークの管理：ブックマークの管理ページに移動するには、[レポート デザイナ（Report Designer）] をクリックします。
- レポート：現在のビューのデータに基づいてレポートを生成するには、[レポート デザイナ（Report Designer）] をクリックします。
- 検索：ルールの更新インポート ログ データベース全体でルールの更新インポート レコードを検索するには、[検索（Search）] をクリックします。
- ソート：現在のワークフロー ページでレコードをソートしたり制約したりするには、詳細についてドリルダウン ページの使用 （2940 ページ）を参照してください。
- ワークフローの切り替え：別のワークフローを一時的に使用するには、[(ワークフローの切り替え)（(switch workflows)）] をクリックします。

エアギャップ展開の維持

Firepower システムがインターネットに接続されていない場合、必要な更新は自動的に実行されません。

それらの更新を手動で取得してインストールする必要があります。次の情報を参照してください。

- 脆弱性データベース（VDB）の手動による更新 （181 ページ）
- 侵入ルールのワンタイム手動更新 （188 ページ）
- 地理位置情報データベース（GeoDB）の手動更新：インターネット接続なし （184ページ）
- *Firepower Management Center Software Upgrade Guide*
  https://www.cisco.com/c/en/us/td/docs/security/firepower/upgrade/fpmc-upgrade-guide.html



第 7 章

バックアップと復元

バックアップと復元について

災害から回復する能力は、システム保守計画の重要な部分を占めます。災害復旧計画の一環として、定期的なバックアップを実行することをお勧めします。このプロセスを自動化するには、スケジュール バックアップ （239 ページ）を参照してください。

（注） Firepower 展開のアップグレード前およびアップグレード後に、リモートロケーションにバックアップして、転送の成功を確認することを強くお勧めします。アプライアンスをアップグレードする際に、ローカルに保存されているバックアップは消去されます。アップグレード後、デバイスがアップグレードされたことを「識別」する新しい FMC バックアップファイルを作成する必要があります。リモートストレージの詳細については、リモートストレージ管理（1283 ページ）を参照してください。

Firepower のバックアップ機能

FMC を使用して、FMC 自体と FMC が管理するデバイスの多くをバックアップすることができます。 また、7000/8000 シリーズのローカル GUI を使用して、個々のデバイスをバックアッ

プすることもできます。FMC から Firepower Threat Defense デバイスをバックアップすることはできますが、復元は FTD CLI から行う必要があることに注意してください。

表 *23 : Firepower* のバックアップ機能

プラットフォーム	バックアップされるデータ	バックアップの保存先	スケジューリング
FMC	次のいずれかです。 • コンフィギュレーション • イベント（キャプチャされたファイルデータは含まれません） • Cisco Threat Intelligence Director（TID） データ：次を参照してください。 TID データのバックアップおよび復元について （1982 ページ） マルチドメイン展開では、イベント/TIDデータのみをバックアップすることはできません。設定もバックアップする必要があります。	FMC または リモート ストレージ	可
FTD：物理デバイス FTDv：VMware	コンフィギュレーション	デバイス、および必要に応じて FMC または リモート ストレージ	可（FMC GUI から）。
7000/8000 シリーズ	コンフィギュレーションD	FMC GUI にバックアップされている場合は、デバイス（および必要に応じて FMC）に保存するか、リモート ストレージに保存します。 デバイスの GUI にバックアップされている場合は、デバイスにのみ保存します。	可（FMC またはデバイス GUI から）。

プラットフォーム	バックアップされるデータ	バックアップの保存先	スケジューリング
FTDv：KVM、AWS、Azure FTD：クラスタ化されたデバイスとコンテナ インスタンス NGIPSv ASA FirePOWER	未サポート これらのデバイスのいずれかを交換する必要がある場合は、デバイス固有の設定を手動で再作成する必要があります。 ただし、FMC をバックアップすると、管理対象デバイスに展開するポリシーやその他の設定のほか、デバイスから FMC にすでに送信されているイベントはバックアップされます。		

バックアップと復元の注意事項と制限事項

以降の項では、デバイスおよび機能領域ごとにバックアップと復元のガイドラインについて詳しく説明します。

- バックアップと復元の注意事項と制限事項：FMC および 7000/8000 シリーズ （202 ページ）
- バックアップと復元の注意事項と制限事項：FTD （203 ページ）
- バックアップと復元の注意事項と制限事項：VPN 証明書を使用している FTD （204 ページ）
- Firepower 4100/9300 のコンフィギュレーションのインポート/エクスポート ガイドライン （204 ページ）

警告 Firepowerのバックアップへの不正アクセスがないことを確認する必要があります。バックアップファイルが何らかの方法で変更されている場合、そのファイルを使用してアプライアンスを復元することはできません。

（注） バックアップデータの収集中に、データの相関付けが一時的に停止してバックアップ関連の設定を変更できなくなることがあります。

関連トピック

侵入イベントを確認済みとしてマーク （3074 ページ）
インターフェイス オブジェクト：インターフェイスグループとセキュリティ ゾーン （535 ページ）

バックアップと復元の注意事項と制限事項：FMC および 7000/8000 シリーズ

Firepower Management Center および 7000/8000 シリーズデバイスのバックアップと復元に関する次の注意事項と制限事項に注意してください。

- 代替アプライアンスにバックアップを復元できるのは、2台が同じモデルであり、同じバージョンの Firepower ソフトウェアを実行している場合のみです。
- 管理対象デバイスをアップグレードした後、Firepower Management Center の新規バックアップを作成します。これは、復元後に、Firepower Management Center の管理対象デバイスの現在のバージョンがバックアップ ファイルのバージョンと同じであるようにするためです。
- Firepower Management Center では、バックアップ機能と復元機能はグローバル ドメインのみで使用できます。サブドメインの範囲内では、バックアップと復元の代わりにエクスポート機能とインポート機能を使用することができます。
- 証明書を含むバックアップ ファイルは、復元後に失敗としてマークされます。そのため、ユーザは Firepower Management Center に証明書を再インストールする必要があります。
- 代替アプライアンスでバックアップを復元すると、既存の設定がすべて削除され、復元された設定に完全に置き換えられます。
- シスコでは、特定のライセンスの予約または永続的なライセンスの予約に変更を加える場合は、Firepower Management Center をバックアップすることをお勧めします。
- アプライアンス間で設定をコピーするためにバックアップおよび復元プロセスを使用しないでください。バックアップ ファイルは、アプライアンスを一意に識別する情報を含んでおり、共有することはできません。
- Firepower Management Center を復元した後、最新の侵入ルールの更新を適用することを推奨します。
- PKI オブジェクトに関連付けられている秘密キーは、アプライアンスに保存されるときに、ランダムに生成されたキーで暗号化されます。PKI オブジェクトに関連付けられた秘密キーを含むバックアップを実行する場合、秘密キーは、暗号化されないバックアップ ファイルに組み込まれる前に復号化されます。バックアップ ファイルは安全な場所に保存してください。
- PKI オブジェクトに関連付けられている秘密キーを含むバックアップを復元すると、その秘密キーはランダムに生成されたキーで暗号化されてからアプライアンスに保存されます。
- クリーン リストとカスタム検出リストのいずれかを有効にしてファイル ポリシーを含むバックアップを復元すると、復元されるファイルのリストとあらゆる既存のファイル リストがマージされます。
- バックアップを実行してから、確認済みの侵入イベントを削除し、そのバックアップを使用して復元すると、削除された侵入イベントは復元されますが、それらの確認済みステー

タスは復元されません。それらの復元された侵入イベントは、[確認済みイベント（Reviewed Events）] ではなく [侵入イベント（Intrusion Events）] に表示されます。

- 侵入イベントのデータを含むバックアップを、そのデータがすでに含まれているアプライアンスに復元すると、重複したイベントが作成されることになります。そのようなことが起こらないようにするため、侵入イベントのバックアップは、以前の侵入イベントデータが含まれていないアプライアンスにのみ復元してください。
- 登録された Firepower デバイスの管理 IP アドレスをデバイスの CLI および Firepower Management Center から変更した場合、HA 同期後も、セカンダリ Firepower Management Center には変更が反映されません。セカンダリ Firepower Management Center も更新されるようにするには、2 つの Firepower Management Center の間でロールを切り替えて、セカンダリ Firepower Management Center をアクティブ ユニットにします。現在アクティブな Firepower Management Center のデバイス管理のページで、登録されている Firepower デバイスの管理 IP アドレスを変更します。

バックアップと復元の注意事項と制限事項：FTD

Firepower Threat Defense でのバックアップと復元については、次の注意事項と制限事項に注意してください。

- 代替 Firepower Threat Defense デバイスにバックアップを復元できるのは、2 台のデバイスが同じモデルであり、同じ Firepower バージョンを実行している場合のみです。
- 高可用性ペアの Firepower Threat Defense デバイスのバックアップ ファイルを Firepower Management Center から作成および復元できます。高可用性展開の場合、代替 Firepower Threat Defense デバイスは、交換されるデバイスと同数のネットワーク モジュールと、同タイプおよび同数の物理インターフェイスを備えている必要があります。
- FTD CLI を使用して、代替 Firepower Threat Defense デバイスにバックアップを復元する必要があります。Web インターフェイスから復元操作を実行することはできません。
- Firepower Threat Defense デバイスを Firepower Management Center から登録解除するか管理対象外にすると、復元操作は一部しか実行されません。

  Firepower Threat Defense デバイスを再登録すると、Firepower Management Center のマッピングとインターフェイスを取る以前のセキュリティーゾーンが失われる食べ、機能を予想どおりに再割当てする必要があります。
- Firepower 4100 シリーズや Firepower 9300 デバイスの場合、バックアップおよび復元操作を実行する前に、設定のエクスポート機能を使用して、Firepower 4100/9300 シャーシの論理デバイスおよびプラットフォーム構成時の設定が含まれている XML ファイルをリモート サーバまたはローカル コンピュータにエクスポートします。詳細については、『*Cisco FXOS Firepower Chassis Manager* コンフィギュレーション ガイド』の「コンフィギュレーションのインポート/エクスポート」にあるガイドラインと制約事項を参照してください。
- 代替 Firepower Threat Defense デバイスにバックアップを復元すると、デバイスが実行中の構成に関する既存の設定は削除され、復元された設定に置き換えられます。

- 復元操作の一環として、代替 Firepower Threat Defense デバイスの管理 IP は、置き換えられる Firepower Threat Defense デバイスと同じものになります。IP の競合を避けるため、古い Firepower Threat Defense デバイスがネットワークに接続されていないことを確認してください。

関連トピック

侵入イベントを確認済みとしてマーク （3074 ページ）
インターフェイス オブジェクト：インターフェイスグループとセキュリティ ゾーン （535 ページ）

バックアップと復元の注意事項と制限事項：VPN 証明書を使用している FTD

VPN 証明書を使用している Firepower Threat Defense デバイスのバックアップと復元を実行する場合、次のガイドラインに注意してください。

ヒント Firepower Threat Defense デバイスで VPN 証明書を登録または削除する手順については、FTD 証明書の管理 （642 ページ） を参照してください。

- Firepower Threat Defense デバイスがバックアップされた後、新しい VPN 証明書が Firepower Management Center に追加されると、Firepower Management Center には新しい証明書がありますが、Firepower Threat Defense デバイスにはありません。Firepower Threat Defense デバイスに新しい証明書を再登録する必要があります。詳細については、FTD 証明書の管理 （642 ページ）を参照してください。
- 復元操作時にすべての VPN 設定と証明書が Firepower Threat Defense デバイスから削除されます。復元操作後は、すべての証明書の登録が失敗したと Firepower Management Center に表示されます。そのため、Firepower Management Center から設定を展開する前に各証明書を再登録する必要があります。

関連トピック

侵入イベントを確認済みとしてマーク （3074 ページ）
インターフェイス オブジェクト：インターフェイスグループとセキュリティ ゾーン （535 ページ）

Firepower 4100/9300 のコンフィギュレーションのインポート/エクスポート ガイドライン

Firepower 4100/9300 シャーシの論理デバイスとプラットフォームのコンフィギュレーション設定を含む XML ファイルをリモート サーバまたはローカル コンピュータにエクスポートするコンフィギュレーションのエクスポート機能を使用できます。そのコンフィギュレーション ファイルを後でインポートして Firepower 4100/9300 シャーシに迅速にコンフィギュレーション設定

を適用し、よくわかっている構成に戻したり、システム障害から回復させたりすることができます。

注意事項および制約事項

- コンフィギュレーション ファイルの内容は、修正しないでください。コンフィギュレーション ファイルが変更されると、そのファイルを使用するコンフィギュレーション インポートが失敗する可能性があります。
- 用途別のコンフィギュレーション設定は、コンフィギュレーションファイルに含まれていません。用途別の設定やコンフィギュレーションを管理するには、アプリケーションが提供するコンフィギュレーション バックアップ ツールを使用する必要があります。
- Firepower 4100/9300 シャーシへのコンフィギュレーションのインポート時、Firepower 4100/9300 シャーシのすべての既存のコンフィギュレーション（論理デバイスを含む）は削除され、インポート ファイルに含まれるコンフィギュレーションに完全に置き換えられます。
- コンフィギュレーション ファイルのエクスポート元と同じ Firepower 4100/9300 シャーシだけにコンフィギュレーション ファイルをインポートすることをお勧めします。
- インポート先の Firepower 4100/9300 シャーシのプラットフォーム ソフトウェア バージョンは、エクスポートしたときと同じバージョンになるはずです。異なる場合は、インポート操作の成功は保証されません。シスコは、Firepower 4100/9300 シャーシをアップグレードしたりダウングレードしたりするたびにバックアップ設定をエクスポートすることを推奨します。
- インポート先の Firepower 4100/9300 シャーシでは、エクスポートしたときと同じスロットに同じネットワーク モジュールがインストールされている必要があります。
- インポート先の Firepower 4100/9300 シャーシでは、インポートするエクスポート ファイルに定義されているすべての論理デバイスに、正しいソフトウェア アプリケーション イメージがインストールされている必要があります。
- 既存のバックアップ ファイルが上書きされるのを回避するには、バックアップ操作時にファイル名を変更するか、既存のファイルを別の場所にコピーしてください。

関連トピック

侵入イベントを確認済みとしてマーク （3074 ページ）
インターフェイス オブジェクト：インターフェイスグループとセキュリティ ゾーン （535 ページ）

のバックアップ Firepower Management Center

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	任意	FMC	グローバルのみ	管理者/メンテナンス

Firepower Management Center をバックアップするには、次の手順を使用します。

始める前に

FMC に十分なディスク領域があることを確認してください。バックアップの処理で使用可能なディスク領域の 90% 超を使用すると、バックアップは失敗することがあります。必要に応じて、古いバックアップ ファイルを削除するか、古いバックアップ ファイルをアプライアンスの外部に転送するか、リモート ストレージを使用してください。リモート ストレージ管理（1283 ページ） を参照してください。

ステップ 1 **[システム（System）] > [ツール（Tools）] > [バックアップ/復元（Backup/Restore）]** を選択します。

ステップ 2 [Firepower 管理バックアップ（Firepower Management Backup）] をクリックします。

ステップ 3 [名前（Name）] を入力します。

ステップ 4 バックアップするものを選択します。

- 設定をアーカイブするには、[設定をバックアップ（Back Up Configuration）] を選択します。マルチドメイン展開では、このオプションを無効にできません。
- イベント データベース全体をアーカイブするには、[イベントをバックアップ（Back Up Events）] を選択します。
- TID 設定と TID データベース全体をアーカイブするには、[TID をバックアップ（Back Up Threat Intelligence Director）] を選択します。

ステップ 5 バックアップの完了時に通知を受けるためには、[電子メール（Email）]チェックボックスを選択して、用意されているテキスト ボックスに電子メール アドレスを入力します。

電子メール通知を受信するには、メール リレー ホストおよび通知アドレスの設定（1303 ページ） で説明されているように、リレー ホストを設定する必要があります。

ステップ 6 セキュアなコピー（SCP）を使用してバックアップ アーカイブを異なるマシンにコピーするには、[完了時にコピー（Copy when complete）] チェックボックスを選択してから、用意されているテキストボックスに以下の情報を入力します。

- [Host] フィールド：バックアップのコピー先となるマシンのホスト名または IP アドレス
- [Path] フィールド：バックアップのコピー先となるディレクトリへのパス
- User] フィールド：リモート マシンへのログインに使用するユーザ名

- [パスワード（Password）] フィールドに、そのユーザ名のパスワード。パスワードの代わりに SSH 公開キーを使用してリモートマシンにアクセスする場合は、そのマシンの指定ユーザの `authorized_keys` ファイルに、[SSH 公開キー（SSH Public Key）] フィールドの内容をコピーします。

このオプションをオフにする場合、バックアップ中に使用された一時ファイルがシステムによってリモートサーバに保存されます。このオプションをオンにする場合は、一時ファイルはリモートサーバに保存され**ません**。Cisco は、システム障害が発生した場合にアプライアンスを復元できるように、バックアップをリモート ロケーションに定期的に保存することを推奨します。

ステップ 7 次の選択肢があります。

- バックアップ ファイルをアプライアンスに保存するには、[Start Backup] をクリックします。バックアップ ファイルは `/var/sf/backup` ディレクトリに保存されます。
- この設定を後で使用できるバックアップ プロファイルとして保存するには、[新規として保存（Save As New）] をクリックします。

次のタスク

バックアップファイルに PKI オブジェクトデータが含まれる場合は、バックアップ内に暗号化されていない秘密キーが含まれています。このため、バックアップはセキュアな場所に保存してください。

デバイスのリモートバックアップ

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	任意	FTD：物理プラットフォーム FTDv VMware 上 7000 & 8000 シリーズ	グローバルのみ	管理者/メンテナンス

Firepower Management Center でリモート デバイスのバックアップを実行するには、次の手順を使用します。

デバイスのバックアップファイルは、デバイスの `/var/sf/backup` ディレクトリに保存されます。Firepower Management Center にバックアップのコピーを保存することを選択した場合、コピーは FMC の `/var/sf/remote-backup` ディレクトリに格納されます。

FTD デバイについては、バックアップファイルは、スタンドアロンデバイスの場合は `<Displayname/IP>-<Timestamp>.tar` の形式に従い、ハイアベイラビリティペアのデバイスの場合は `<Displayname/IP>-<Role>-<Timestamp>.tar` の形式に従います。

始める前に

十分なディスク領域があることを確認してください。バックアップの処理で使用可能なディスク領域の 90% 超を使用すると、バックアップは失敗することがあります。必要に応じて、古いバックアップ ファイルを削除または転送するか、リモート ストレージを使用してください。リモート ストレージ管理 （1283 ページ）を参照してください。

ステップ 1 **[システム（System）] > [ツール（Tools）] > [バックアップ/復元（Backup/Restore）]** を選択します。

ステップ 2 [管理対象デバイスのバックアップ（Managed Device Backup）] をクリックします。

ステップ 3 1 つまたは複数の管理対象デバイスを選択します。

ステップ 4 [管理センターで取得する（Retrieve to Management Center）] を有効または無効にすることによって、バックアップ ファイルを保存する場所を指定します。

- 有効（デフォルト）：デバイスのバックアップをデバイスに保存し、そのファイルを FMC にもコピーします。
- 無効：デバイスのバックアップをデバイスのみに保存します。

リモート バックアップ ストレージを設定している場合、バックアップ ファイルはリモートに保存され、このオプションは無効になります。

ステップ 5 [バックアップ開始（Start Backup）] をクリックします。

次のタスク

バックアップに PKI オブジェクトのデータが含まれている場合、バックアップ内に暗号化されていない秘密キーが保存されるため、安全な場所にバックアップを保存します。

7000/8000 シリーズデバイスのローカルバックアップ

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
該当なし	任意	7000 & 8000 シリーズ	該当なし	管理者/メンテナンス

7000 または 8000 シリーズ デバイスのローカル Web インターフェイスを使用して、次の手順を実行する必要があります。

始める前に

アプライアンスに十分なディスク領域があることを確認してください。バックアップの処理で使用可能なディスク領域の 90%以上を使用すると、バックアップは失敗することがあります。

必要に応じて、古いバックアップ ファイルを削除するか、古いバックアップ ファイルをアプライアンスの外部に転送してください。

ステップ 1 **[システム（System）] > [ツール（Tools）] > [バックアップ/復元（Backup/Restore）]** を選択します。

ステップ 2 [デバイス バックアップ（Device Backup）] をクリックします。

ステップ 3 [名前（Name）] フィールドに、バックアップ ファイルの名前を入力します。

ステップ 4 バックアップの完了時に通知を受けるためには、[電子メール（Email）]チェックボックスを選択して、用意されているテキスト ボックスに電子メール アドレスを入力します。

電子メール通知を受信するには、メール リレー ホストおよび通知アドレスの設定（1303 ページ） で説明されているように、リレー ホストを設定する必要があります。

ステップ 5 セキュアなコピー（SCP）を使用してバックアップ アーカイブを異なるマシンにコピーするには、[完了時にコピー（Copy when complete）] チェックボックスを選択してから、用意されているテキストボックスに以下の情報を入力します。

- [ホスト（Host）] フィールドに、バックアップのコピー先となるマシンのホスト名または IP アドレス。
- [パス（Path）] フィールドに、バックアップのコピー先となるディレクトリへのパス。
- [ユーザ（User）] フィールドに、リモート マシンへのログインに使用するユーザ名。
- [パスワード（Password）] フィールドに、そのユーザ名のパスワード。パスワードの代わりに SSH 公開キーを使用してリモート マシンにアクセスする場合は、そのマシンの指定ユーザの `authorized_keys` ファイルに、[SSH 公開キー（SSH Public Key）] フィールドの内容をコピーします。

このオプションをオフにする場合、バックアップ中に使用された一時ファイルがシステムによってリモート サーバに保存されます。このオプションをオンにする場合は、一時ファイルはリモート サーバに保存されません。Cisco は、システム障害が発生した場合にアプライアンスを復元できるように、バックアップをリモート ロケーションに定期的に保存することを推奨します。

ステップ 6 次の選択肢があります。

- バックアップ ファイルをアプライアンスに保存するには、[Start Backup] をクリックします。バックアップ ファイルは `/var/sf/backup` ディレクトリに保存されます。
- この設定を後で使用できるバックアップ プロファイルとして保存するには、[新規として保存（Save As New）] をクリックします。

次のタスク

バックアップファイルに PKI オブジェクトデータが含まれる場合は、バックアップ内に暗号化されていない秘密キーが含まれています。このため、バックアップはセキュアな場所に保存してください。

バックアップ プロファイルの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	任意	FMC 7000 & 8000 シリーズ	グローバルのみ	管理者/メンテナンス

次の手順は、デバイスの Web ユーザ インターフェイス、または Firepower Management Center Web インターフェイス（該当する場合）を使用して実行する必要があります。

さまざまな種類のバックアップに使用する設定値を含むバックアップ プロファイルを作成できます。バックアップを実行またはスケジュールするときに、これらのプロファイルのいずれかを選択できます。

ヒント　新規ファイル名を使用してバックアップ ファイルを作成する場合、システムにより自動的に、その名前でバックアップ プロファイルが作成されます。

ステップ 1 **[システム（System）] > [ツール（Tools）] > [バックアップ/復元（Backup/Restore）]** を選択し、[バックアッププロファイル（Backup Profiles）] をクリックします。

ステップ 2 [プロファイルの作成（Create Profile）] をクリックします。

ステップ 3 バックアップ ファイルの名前を入力します。

ステップ 4 バックアップ プロファイルを設定します。

オプションの詳細は、のバックアップ Firepower Management Center （206 ページ）を参照してください。

ステップ 5 [新規として保存（Save As New）] をクリックします。

バックアップ ファイルのアップロード

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	FMC 7000 & 8000 シリーズ	グローバルだけ	Admin/Maint

デバイスに応じて、Firepower Management Center Web インターフェイスまたはデバイスのローカル Web インターフェイスを使用して、ローカル ホストから Firepower Management Center、7000 シリーズデバイス、または 8000 シリーズデバイスにバックアップ ファイルをアップロードできます。

バックアップ ファイルに PKI オブジェクトが含まれている場合、アップロード時に、システムはランダム生成されたキーを使用して、内部 CA および内部証明書オブジェクトに関連付けられた秘密キーを再暗号化します。

始める前に

- [バックアップ管理（Backup Management）] ページ（211 ページ）の説明に従って、ダウンロード機能を使用し、バックアップ ファイルをローカル ホストにダウンロードします。
- SCP を介してローカル ホストからリモート ホストに 4GB より大きいバックアップをコピーし、そこから Firepower Management Center に取り出します（Web ブラウザではその大きさのファイルのアップロードがサポートされていないため）。詳細については、リモート ストレージ管理（1283 ページ）を参照してください。

ステップ 1 **[システム（System）] > [ツール（Tools）] > [バックアップ/復元（Backup/Restore）]** を選択します。
ステップ 2 [バックアップのアップロード（Upload Backup）] をクリックします。
ステップ 3 [参照（Browse）] をクリックし、アップロードするバックアップ ファイルまで移動して選択します。
ステップ 4 [バックアップのアップロード（Upload Backup）] をクリックします。
ステップ 5 [バックアップ管理（Backup Management）] をクリックして、[バックアップ管理（Backup Management）] ページに戻ります。

次のタスク

アプライアンスによってファイルの整合性が確認された後、[バックアップ管理（Backup Management）] ページを更新し、詳細なファイル システム情報を表示します。

[バックアップ管理（Backup Management）] ページ

[システム（System）] > [ツール（Tools）] > [バックアップ/復元（Backup/Restore）] > [バックアップ管理（Backup Management）] で、Firepower Management Center Web インターフェイスの [バックアップ管理（Backup Management）] ページにアクセスできます。

バックアップ ファイルに PKI オブジェクトが含まれている場合、アップロード時に、システムはランダム生成されたキーを使用して、内部 CA および内部証明書オブジェクトに関連付けられた秘密キーを再暗号化します。

ローカル ストレージを使用する場合、バックアップ ファイルは `/var/sf/backup` に保存されて、`/var` パーティションで使用されているディスク領域量と共に [バックアップ管理（Backup Management）] ページの下部にリストされます。Firepower Management Center で、[バックアッ

プ管理（Backup Management）] ページの上部にある [リモート ストレージ（Remote Storage）] を選択して、リモート ストレージ オプションを設定します。その後、リモート ストレージを有効にするには[バックアップ管理（Backup Management）]ページの [バックアップ用にリモート ストレージを有効にする（Enable Remote Storage for Backups）] チェック ボックスをオンにします。 リモート ストレージを使用している場合は、プロトコル、バックアップ システム、およびバックアップ ディレクトリがページの下部に表示されます。

次の表では、[バックアップ管理（Backup Management）] ページの各列およびボタンについて説明します。

表 *24 :* バックアップ管理（*Backup Management*）

機能	説明
System Information	元のアプライアンスの名前、タイプ、バージョン （注） バックアップを復元できるのは、同一のアプライアンス タイプとバージョンに対してのみです。
Date Created	バックアップ ファイルが作成された日時
File Name	バックアップ ファイルのフルネーム
VDB Version	バックアップ時にアプライアンスで実行されている脆弱性データベース（VDB）のビルド。
Location	バックアップ ファイルの場所
Size (MB)	バックアップ ファイルのサイズ（メガバイト）
Events?	[Yes] は、バックアップにイベント データが含まれていることを示します
View	バックアップ ファイルの名前をクリックすると、圧縮されたバックアップ ファイルに含まれるファイルのリストが表示されます。
Restore	バックアップファイルが選択された状態でクリックすると、そのバックアップ ファイルがアプライアンスに復元されます。VDB バージョンがバックアップ ファイルの VDB のバージョンと一致しない場合、このオプションは無効になります。詳細については、バックアップからの復元：FMC および 7000/8000 シリーズ （213 ページ）を参照してください。
Download	バックアップファイルが選択された状態でクリックすると、そのバックアップ ファイルがローカル コンピュータに保存されます。
Delete	バックアップファイルが選択された状態でクリックすると、そのバックアップ ファイルが削除されます。

機能	説明
Move	Firepower Management Center で、以前に作成したローカル バックアップが選択された状態でクリックすると、そのバックアップが指定のリモート バックアップ ロケーションに送信されます。

バックアップからの復元：FMC および 7000/8000 シリーズ

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	FMC 7000 & 8000 シリーズ	グローバルだけ	Admin/Maint

Firepower Management Center Web インターフェイスまたはデバイスの Web インターフェイスの [バックアップ管理（Backup Management）] ページを使用して、バックアップ ファイルから Firepower Management Center、7000 シリーズ デバイス、または 8000 シリーズ デバイスを復元できます。

注意 この操作により、すべてのコンフィギュレーション ファイルが上書きされ、管理対象デバイスでは、すべてのイベント データが上書きされます。

（注） バックアップが完了した後にライセンスを追加した場合は、このバックアップを復元するときに、それらのライセンスが削除されたり上書きされたりすることはありません。復元の際の競合を防止するためにも、バックアップを復元する前に、これらのライセンスを（それらが使用されている場所をメモした上で）削除し、バックアップを復元した後で、追加して再設定してください。競合が発生した場合は、サポートに連絡してください。バックアップの完了後に Cisco Smart Software Manager から Firepower Management Center を登録解除し、このバックアップを復元する場合、Firepower Management Center を登録解除し Firepower Management Center を再度登録する必要があります。

（注） Firepower Management Center の登録解除の詳細については、Cisco Smart Software Manager から Firepower Management Center の登録解除 （140 ページ）を参照してください。Firepower Management Center を登録するには、スマート ライセンスの登録 （113 ページ）を参照してください。

始める前に

- バックアップ ファイル内の VDB のバージョンが、アプライアンスの現在の VDB のバージョンと一致していることを確認します。詳細については、ダッシュボードの表示 （346 ページ）を参照してください。
- バックアップの完了後にアプライアンスに追加したライセンスは、リストア時の競合を避けるために、バックアップの復元前に削除します。詳細については、Firepower ライセンスについて （93 ページ）を参照してください。
- バックアップに保管されているものと同じ侵入イベントデータがアプライアンスに存在しないことを確認します。これは、そのような状況下でバックアップを復元すると、重複するイベントが作成されるためです。詳細については、侵入イベントについて （3057ページ）を参照してください。

ステップ 1 **[システム（System）] > [ツール（Tools）] > [バックアップ/復元（Backup/Restore）]** を選択します。

ステップ 2 バックアップ ファイルをクリックして、そのコンテンツを表示します。詳細には、ファイルの所有者、ファイルの権限、ファイル サイズ、および日付が含まれています。

ステップ 3 **[システム（System）] > [ツール（Tools）] > [バックアップ/復元（Backup/Restore）]** を選択して、[バックアップ管理（Backup Management）] ページに戻ります。

ステップ 4 復元するバックアップ ファイルを選択します。

ステップ 5 [復元（Restore）] をクリックします。

（注） バックアップの VDB バージョンがアプライアンスに現在インストールされている VDB のバージョンと一致しない場合、[復元（Restore）] ボタンはグレー表示されます。

ステップ 6 ファイルを復元するには、次のいずれかまたは両方のオプションを選択します。

- **設定データの復元（Restore Configuration Data）**

  （注） 管理対象デバイスの設定をバックアップ ファイルから復元すると、デバイスの管理用の Firepower Management Center から行われたデバイス設定の変更も復元されます。バックアップ ファイルを復元することで、バックアップ ファイルの作成後に行った変更は上書きされます。

- イベント データの復元（Restore Event Data）（FMC のみ）
- Threat Intelligence Director データの復元（Restore Threat Intelligence Director Data）（FMC のみ）

ステップ 7 [復元（Restore）] をクリックします。

ステップ 8 （オプション）システムが自動的に再起動するまで待ちます。

バックアップに設定データが含まれている場合にのみ、システムは自動的に再起動します。

次のタスク

- 最新のシスコ ルール アップデートをインポートします。侵入ルールのワンタイム手動更新（188 ページ）を参照してください。インポートの一環としてポリシーを再展開する場合、設定の変更を展開する必要はありません（後述）。
- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。
- バックアップの復元前に、アプライアンスから削除したライセンスを追加して再設定します。
- 復元時にアプライアンスがライセンスの競合を示した場合は、サポートまでお問い合わせください。

バックアップからの復元： Firepower Threat Defense

問題または障害のある Firepower Threat Defense デバイスを交換する必要がある場合、次に示すバックアップおよび復元手順のいずれかを実行します。

- バックアップからの FTD の復元：Firepower 1000/2100 シリーズ （215 ページ）
- バックアップからの FTD の復元：Firepower 4100/9300 シャーシ （217 ページ）
- バックアップからの FTD の復元： ASA 5500-X シリーズ （220 ページ）
- バックアップからの FTD の復元： FTDv （222 ページ）
- バックアップからの FTD の復元：高可用性 （223 ページ）

バックアップからの FTD の復元：Firepower 1000/2100 シリーズ

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	Firepower 1000 シリーズ Firepower 2100 シリーズ	グローバルだけ	Admin/Maint

問題または障害のある Firepower 1000 シリーズ または Firepower 2100 シリーズ デバイスを交換するには、次の手順を実行します。

警告 Firepower Management Center とのすべての通信が停止するため、障害のある Firepower Threat Defense デバイスを登録解除したり、または管理対象外にしないでください。

始める前に

- バックアップと復元の注意事項と制限事項 （201 ページ）を確認してください。
- 環境内に展開された Firepower 1000 シリーズ または Firepower 2100 シリーズ デバイスのバックアップがあることを確認します。詳細については、デバイスのリモートバックアップ （207 ページ）を参照してください。

  バックアップ ファイルは、Firepower 1000 シリーズ または Firepower 2100 シリーズ デバイスの `/var/sf/backup` でローカルに保持されます。Firepower Management Center 上にバックアップを保持することを選択した場合、バックアップは `/var/sf/remote-backup` ディレクトリに格納されます。
- Cisco Technical Assistance Center（TAC） に連絡して交換を依頼してください。

ステップ 1 障害のあるデバイスをネットワークから取り外します。

ステップ 2 交換用デバイスをネットワーク上に展開し、管理インターフェイスだけを接続して、デバイスの電源を投入します。詳細については、『*Cisco Firepower 1000 Series Using Firepower Management Center Quick Start Guide*』または『*Cisco Firepower 2100 Series Using Firepower Management Center Quick Start Guide*』を参照してください。

ステップ 3 交換用デバイスで実行している Firepower のバージョンが、交換されるデバイスで実行しているバージョンと同じであることを確認します。必要に応じて、交換用デバイスを再イメージ化します。詳細については、*Cisco ASA* および *Firepower Threat Defense* デバイスの再イメージ化ガイドを参照してください。

ステップ 4 `restore` コマンドを使用して、デバイス上のバックアップを復元します。

- ローカルの Firepower Threat Defense からバックアップを復元するには、`restore remote-manager-backup <backup tar-file>` コマンドを使用します。
- SCP 対応リモート ネットワークからバックアップを復元するには、`restore remote-manager-backup location <scp-hostname> <username> <filepath> <backup tar-file>` コマンドを使用します。

復元操作の進捗状況は、Firepower Threat Defense デバイスの `/var/log/restore.log` ログを表示することでモニタできます。

次のタスク

- 復元に成功すると、Firepower Threat Defense デバイスは Firepower Management Center に接続して使用可能になります。復元された Firepower Threat Defense デバイス上のポリシーは期限切れになります。設定の変更を Firepower Management Center から展開して、ポリシーを更新します。詳細については、設定変更の展開 （447 ページ）を参照してください。

（注） Firepower Threat Defense デバイスで VPN 構成を使用している場合は、バックアップと復元の注意事項と制限事項 （201 ページ）の VPN 証明書管理のセクションを参照してください。

- デバイスのデータ インターフェイスをネットワークに接続します。手順については、『*Cisco Firepower 1000 Series Using Firepower Management Center Quick Start Guide*』または『*Cisco Firepower Threat Defense for the Firepower 2100 Series Using Firepower Management Center Quick Start Guide*』を参照してください。

バックアップからの FTD の復元：Firepower 4100/9300 シャーシ

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	Firepower 4100/9300	グローバルだけ	Admin/Maint

Firepower 4100/9300 シャーシで実行中の Firepower Threat Defense でハードウェア障害が発生した場合は、次の手順を実行して交換してください。

警告 Firepower Management Center とのすべての通信が停止するため、障害のある Firepower Threat Defense デバイスを登録解除したり、または管理対象外にしないでください。

始める前に

- バックアップと復元の注意事項と制限事項 （201 ページ）を確認してください。
- Firepower Chassis Manager から FXOS の設定をエクスポートします。詳細については、FXOS コンフィギュレーション ファイルのエクスポート （218 ページ）を参照してください。
- 環境内に展開された Firepower 4100/9300 シャーシで実行中の論理 Firepower Threat Defense デバイスのバックアップがあることを確認します。詳細については、デバイスのリモート バックアップ （207 ページ）を参照してください。

  バックアップ ファイルは、Firepower 4100/9300 シャーシの `/var/sf/backup` でローカルに保持されます。Firepower Management Center 上にバックアップを保持することを選択した場合、バックアップは `/var/sf/remote-backup` ディレクトリに格納されます。
- Firepower 4100/9300 で実行中の Firepower Threat Defense デバイスに障害が発生した場合は、Cisco Technical Assistance Center（TAC） に連絡して交換を依頼してください。

ステップ 1 障害のある Firepower 4100/9300 シャーシをネットワークから取り外します。

ステップ 2 交換用 Firepower 4100/9300 シャーシをネットワーク上に設置し、管理インターフェイスだけを接続して、デバイスの電源を投入します。詳細については、*Cisco Firepower Threat Defense for Firepower 4100* クイック スタート ガイド [英語] または *Cisco Firepower Threat Defense for Firepower 9300* クイック スタート ガイド [英語] を参照してください（該当する場合）。

ステップ 3 Firepower Threat Defense が、交換用デバイスで実行されている FXOS バージョンと互換性があることを確認します。必要に応じて、交換用デバイスを再イメージ化します。詳細については、『*Cisco FXOS Firepower Chassis Manager* コンフィギュレーション ガイド』を参照してください。

ステップ 4 Firepower Chassis Manager から以前エクスポートした FXOS の構成時の設定をインポートします。詳細については、コンフィギュレーション ファイルのインポート （219 ページ）を参照してください。

ステップ 5 `restore` コマンドを使用して、交換用 Firepower Threat Defense デバイスのバックアップを復元します。

- ローカルの Firepower Threat Defense からバックアップを復元するには、`restore remote-manager-backup <backup tar-file>` コマンドを使用します。
- SCP 対応リモート ネットワークからバックアップを復元するには、`restore remote-manager-backup location <scp-hostname> <username> <filepath> <backup tar-file>` コマンドを使用します。

復元操作の進捗状況は、Firepower Threat Defense の `/var/log/restore.log` ログを表示することでモニタできます。

次のタスク

- 復元に成功すると、Firepower Threat Defense デバイスは Firepower Management Center に接続して使用可能になります。復元された Firepower Threat Defense デバイス上のポリシーは期限切れになります。設定の変更を Firepower Management Center から展開して、ポリシーを更新します。詳細については、設定変更の展開 （447 ページ）を参照してください。

（注） 論理 Firepower Threat Defense デバイスで VPN 構成を使用している場合は、バックアップと復元の注意事項と制限事項 （201 ページ）の VPN 証明書管理のセクションを参照してください。

- Firepower 4100/9300 シャーシ デバイスのデータ インターフェイスをネットワークに接続します。手順については、*Cisco Firepower Threat Defense for Firepower 4100* クイック スタート ガイド [英語] または *Cisco Firepower Threat Defense for Firepower 9300* クイック スタート ガイド [英語] を参照してください。

FXOS コンフィギュレーション ファイルのエクスポート

エクスポート設定機能を使用して、Firepower 4100/9300 シャーシの論理デバイスとプラットフォーム構成設定を含むXMLファイルをリモート サーバまたはローカル コンピュータにエクスポートします。

エクスポート機能の使用に関する重要な情報については、「Firepower 4100/9300 のコンフィギュレーションのインポート/エクスポート ガイドライン」を参照してください。

ステップ 1 **[System]** > **[Configuration]** > **[Export]** の順に選択します。

ステップ 2 コンフィギュレーション ファイルをローカル コンピュータにエクスポートするには、次の操作を行います。

a) [Local] オプション ボタンをクリックします。
b) [Export] をクリックします。
コンフィギュレーションファイルが作成され、ブラウザによって、ファイルがデフォルトのダウンロード場所に自動的にダウンロードされるか、またはファイルを保存するようプロンプトが表示されます。

ステップ 3 コンフィギュレーション ファイルをリモート サーバにエクスポートするには、次の操作を行います。

a) [Remote] オプション ボタンをクリックします。
b) リモートサーバとの通信で使用するプロトコルを選択します。選択できるプロトコルは、FTP、TFTP、SCP、または SFTP のいずれかです。
c) バックアップ ファイルを格納する場所のホスト名または IP アドレスを入力します。サーバ、ストレージアレイ、ローカル ドライブ、または Firepower 4100/9300 シャーシがネットワーク経由でアクセス可能な任意の読み取り/書き込みメディアなどを指定できます。

IP アドレスではなくホスト名を使用する場合、DNS サーバを設定する必要があります。

d) デフォルト以外のポートを使用する場合は、[Port] フィールドにポート番号を入力します。
e) リモートサーバにログインするためのユーザ名を入力します。プロトコルが TFTP の場合、このフィールドは適用されません。
f) リモート サーバのユーザ名のパスワードを入力します。プロトコルが TFTP の場合、このフィールドは適用されません。
g) [Location] フィールドに、ファイル名を含むコンフィギュレーション ファイルをエクスポートする場所のフル パスを入力します。ファイル名を省略すると、エクスポート手順によって、ファイルに名前が割り当てられます。
h) [Export] をクリックします。
コンフィギュレーション ファイルが作成され、指定の場所にエクスポートされます。

コンフィギュレーション ファイルのインポート

設定のインポート機能を使用して、Firepower 4100/9300 シャーシからエクスポートした構成設定を適用できます。この機能を使用して、既知の良好な構成に戻したり、システム障害を解決したりできます。インポート機能の使用に関する重要な情報については、「Firepower 4100/9300 のコンフィギュレーションのインポート/エクスポート ガイドライン」を参照してください。

ステップ 1 **[System]** > **[Configuration]** > **[Import]** の順に選択します。

ステップ 2 ローカルのコンフィギュレーション ファイルからインポートする場合は、次の操作を行います。

a) [Local] オプション ボタンをクリックします。
b) [Choose File] をクリックし、インポートするコンフィギュレーション ファイルを選択します。
c) [Import] をクリックします。
操作の続行を確認するダイアログボックスが開き、シャーシの再起動についての警告が表示されます。
d) [Yes] をクリックして、指定したコンフィギュレーション ファイルをインポートします。
既存の設定が削除され、インポートしたファイルの設定が Firepower 4100/9300 シャーシに適用されます。インポート中にブレークアウト ポートの設定が変更された場合は、Firepower 4100/9300 シャーシの再起動が必要になります。

ステップ 3 リモート サーバからコンフィギュレーション ファイルをインポートする場合は、次の操作を行います。

a) [Remote] オプション ボタンをクリックします。
b) リモートサーバとの通信で使用するプロトコルを選択します。選択できるプロトコルは、FTP、TFTP、SCP、または SFTP のいずれかです。
c) デフォルト以外のポートを使用する場合は、[Port] フィールドにポート番号を入力します。
d) バックアップ ファイルが格納されている場所のホスト名または IP アドレスを入力します。サーバ、ストレージ アレイ、ローカル ドライブ、または Firepower 4100/9300 シャーシがネットワーク経由でアクセス可能な任意の読み取り/書き込みメディアなどを指定できます。

   IP アドレスではなくホスト名を使用する場合、DNS サーバを設定する必要があります。

e) リモートサーバにログインするためのユーザ名を入力します。プロトコルが TFTP の場合、このフィールドは適用されません。
f) リモート サーバのユーザ名のパスワードを入力します。プロトコルが TFTP の場合、このフィールドは適用されません。
g) [File Path] フィールドに、コンフィギュレーション ファイルのフル パスをファイル名を含めて入力します。
h) [Import] をクリックします。
   操作の続行を確認するダイアログボックスが開き、シャーシの再起動についての警告が表示されます。
i) [Yes] をクリックして、指定したコンフィギュレーション ファイルをインポートします。
   既存の設定が削除され、インポートしたファイルの設定が Firepower 4100/9300 シャーシに適用されます。インポート中にブレークアウト ポートの設定が変更された場合は、Firepower 4100/9300 シャーシの再起動が必要になります。

バックアップからの FTD の復元： ASA 5500-X シリーズ

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	ASA 5500-X シリーズ with FTD	グローバルだけ	Admin/Maint

問題または障害のある ASA 5500-X シリーズ デバイスを交換するには、次の手順を実行します。

警告 Firepower Management Center とのすべての通信が停止するため、障害のある Firepower Threat Defense デバイスを登録解除したり、または管理対象外にしないでください。

始める前に

- バックアップと復元の注意事項と制限事項 （201 ページ）を確認してください。

- 環境内に展開された ASA 5500-X シリーズ デバイスのバックアップがあることを確認します。詳細については、デバイスのリモートバックアップ （207 ページ）を参照してください。

  バックアップ ファイルは、ASA 5500-X シリーズ デバイスの `/var/sf/backup` でローカルに保持されます。Firepower Management Center 上にバックアップを保持することを選択した場合、バックアップは `/var/sf/remote-backup` ディレクトリに格納されます。

- Cisco Technical Assistance Center（TAC） に連絡して交換を依頼してください。

ステップ 1 障害のあるデバイスをネットワークから取り外します。

ステップ 2 交換用デバイスをネットワーク上に展開し、管理インターフェイスだけを接続して、デバイスの電源を投入します。詳細については、該当する *Firepower Management Center* を使用した *Cisco Firepower Threat Defense*（*ASA 5500-X* シリーズ用）クイック スタート ガイド [英語] を参照してください。

ステップ 3 交換用デバイスで実行している Firepower システム ソフトウェアのバージョンが、交換対象デバイスで実行しているバージョンと同じであることを確認します。必要に応じて、交換用デバイスを再イメージ化します。詳細については、*Cisco ASA* および *Firepower Threat Defense* デバイスの再イメージ化ガイドを参照してください。

ステップ 4 `restore` コマンドを使用して、ASA 5500-X シリーズ デバイス上のバックアップを復元します。

- ローカルの Firepower Threat Defense からバックアップを復元するには、`restore remote-manager-backup <backup tar-file>` コマンドを使用します。
- SCP 対応リモート ネットワークからバックアップを復元するには、`restore remote-manager-backup location <scp-hostname> <username> <filepath> <backup tar-file>` コマンドを使用します。

復元操作の進捗状況は、Firepower Threat Defense デバイスの `/var/log/restore.log` ログを表示することでモニタできます。

次のタスク

- 復元に成功すると、Firepower Threat Defense デバイスは Firepower Management Center に接続して使用可能になります。復元された Firepower Threat Defense デバイス上のポリシーは期限切れになります。設定の変更を Firepower Management Center から展開して、ポリシーを更新します。詳細については、設定変更の展開 （447 ページ）を参照してください。

  （注） Firepower Threat Defense デバイスで VPN 構成を使用している場合は、バックアップと復元の注意事項と制限事項 （201 ページ）の VPN 証明書管理のセクションを参照してください。

- ASA 5500-X シリーズ デバイスのデータ インターフェイスをネットワークに接続します。手順については、*Firepower Management Center* を使用した *Cisco Firepower Threat Defense*（*ASA 5500-X* シリーズ用）クイック スタート ガイド [英語] を参照してください。

バックアップからの FTD の復元： FTDv

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTDv VMware の場合	グローバルだけ	Admin/Maint

VMware で実行中の問題または障害のある Firepower Threat Defense Virtual デバイスを交換するには、次の手順を実行します。

警告 Firepower Management Center とのすべての通信が停止するため、障害のある Firepower Threat Defense デバイスを登録解除したり、または管理対象外にしないでください。

始める前に

- バックアップと復元の注意事項と制限事項 （201 ページ）を確認してください。
- 環境内に展開された Firepower Threat Defense Virtual デバイスのバックアップがあることを確認します。デバイスのリモートバックアップ （207 ページ）を参照してください。

  バックアップ ファイルは、Firepower Threat Defense Virtual デバイスの `/var/sf/backup` でローカルに保持されます。Firepower Management Center 上にバックアップを保持することを選択した場合、バックアップは `/var/sf/remote-backup` ディレクトリに格納されます。
- Cisco Technical Assistance Center（TAC） に連絡して壊れた Firepower Threat Defense Virtual の交換を依頼してください。

ステップ 1 VMware vSphere Web クライアントまたは vSphere Hypervisor を使用して Firepower Threat Defense Virtual を展開します。詳細については、*VMware* 展開向け *Cisco Firepower Threat Defense Virtual* クイック スタート ガイドを参照してください。

ステップ 2 CLI を使用して Firepower Threat Defense Virtual デバイスを設定します。詳細については、*VMware* 展開向け *Cisco Firepower Threat Defense Virtual* クイック スタート ガイドを参照してください。

ステップ 3 （オプション）交換用デバイスを再イメージ化して、実行している Firepower システム ソフトウェアのバージョンを、交換対象デバイスのバージョンと同じにします。詳細については、*VMware* 展開向け *Cisco Firepower Threat Defense Virtual* クイック スタート ガイドを参照してください。

警告 `/var/sf/backup` から SCP 対応のリモート ロケーションまたは Firepower Management Center にバックアップ ファイルをコピーしてから、バックアップを作成した Firepower Threat Defense Virtual デバイスを再イメージ化します。

ステップ 4 `restore` コマンドを使用して、Firepower Threat Defense Virtual のバックアップを復元します。

- ローカルの Firepower Threat Defense からバックアップを復元するには、`restore remote-manager-backup <backup tar-file>` コマンドを使用します。

- SCP 対応リモート ネットワークからバックアップを復元するには、`restore remote-manager-backup location <scp-hostname> <username> <filepath> <backup tar-file>` コマンドを使用します。

復元操作の進捗状況は、`/var/log/restore.log` ログを表示することでモニタできます。

次のタスク

- 復元に成功すると、Firepower Threat Defense デバイスは Firepower Management Center に接続して使用可能になります。復元された Firepower Threat Defense デバイス上のポリシーは期限切れになります。設定の変更を Firepower Management Center から展開して、ポリシーを更新します。詳細については、設定変更の展開 （447 ページ）を参照してください。

（注） Firepower Threat Defense Virtual デバイスで VPN 構成を使用している場合は、バックアップと復元の注意事項と制限事項 （201 ページ）の VPN 証明書管理のセクションを参照してください。

- VMware インターフェイスを追加して設定します。詳細については、*VMware* 展開向け *Cisco Firepower Threat Defense Virtual* クイック スタート ガイドを参照してください。

バックアップからの FTD の復元：高可用性

高可用性ペアの 1 つ以上の障害または問題が発生した Firepower Threat Defense デバイスを交換する必要がある場合は、次に示すいずれかの手順に従う必要があります。

- バックアップからの FTD の復元：HA ペア（1 つのピアの交換） （223 ページ）
- バックアップからの FTD の復元：HA ペア（両方のピアの交換） （225 ページ）

バックアップからの FTD の復元：HA ペア（1 つのピアの交換）

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD：物理プラットフォーム	グローバルだけ	Admin/Maint

高可用性構成の Firepower Threat Defense デバイスでハードウェア障害が発生した場合は、次の手順を実行して交換してください。

警告 Firepower Management Center とのすべての通信が停止するため、障害のある Firepower Threat Defense デバイスを登録解除したり、または管理対象外にしないでください。

始める前に

- バックアップと復元の注意事項と制限事項 （201 ページ）を確認してください。

（注） Firepower Threat Defense で稼働している Firepower 4100/9300 シャーシ デバイスを交換する場合、FXOS の設定を Firepower Chassis Manager からエクスポートしてから Firepower Threat Defense のバックアップと復元操作を進めてください。詳細については、『*Cisco FXOS Firepower Chassis Manager* コンフィギュレーション ガイド』の「コンフィギュレーションのインポート/エクスポート」を参照してください。

- Firepower Threat Defense 高可用性ペアのバックアップがあることを確認します。詳細については、デバイスのリモートバックアップ （207 ページ）を参照してください。

  バックアップ ファイルは、Firepower Threat Defense デバイスの `/var/sf/backup` でローカルに保持されます。Firepower Management Center 上にバックアップを保持することを選択した場合、バックアップは `/var/sf/remote-backup` ディレクトリに格納されます。Firepower Management Center は、プライマリとセカンダリの Firepower Threat Defense デバイスに対してバックアップ ファイルを個別に作成します。高可用性ペアの Firepower Threat Defense デバイスの場合、バックアップ tar ファイルの形式は `<Hostname/IP>-<Role>-<Timestamp>.tar` です。

- 高可用性ペアの Firepower Threat Defense デバイスに障害が発生した場合は、Cisco Technical Assistance Center（TAC） に連絡して交換を依頼してください。

ステップ 1 障害のあるデバイスをネットワークから取り外します。

ステップ 2 交換用デバイスをネットワーク上に展開し、管理インターフェイスと高可用性リンクを接続して、デバイスの電源を投入します。詳細については、該当する *Firepower* クイック スタート ガイドを参照してください。

（注） トラフィックの中断を回避するため、交換用デバイスにデータ インターフェイスが接続されていないことを確認します。

ステップ 3 交換用デバイスで実行している Firepower システム ソフトウェアのバージョンが、交換対象デバイスで実行しているバージョンと同じであることを確認します。必要に応じて、交換用デバイスを再イメージ化します。詳細については、*Cisco ASA* および *Firepower Threat Defense* デバイスの再イメージ化ガイドを参照してください。

ステップ 4 コマンド ライン インターフェイスで `restore` コマンドを使用して Firepower Threat Defense デバイスにバックアップを復元します。

- ローカルの Firepower Threat Defense からバックアップを復元するには、`restore remote-manager-backup <backup tar-file>` コマンドを使用します。
- SCP 対応リモート ネットワークからバックアップを復元するには、`restore remote-manager-backup location <scp-hostname> <username> <filepath> <backup tar-file>` コマンドを使用します。

交換している Firepower Threat Defense デバイスがプライマリか、セカンダリかに応じて、適切なバックアップ ファイルを選択します。復元操作の進捗状況は、Firepower Threat Defense デバイスの `/var/log/restore.log` ログを表示することでモニタできます。

復元が正常に完了すると、デバイスが再起動します。

次のタスク

- コマンド ライン インターフェイスで `configure high-availability resume` コマンドを使用して高可用性ピア間で高可用性設定を再開します。
- 復元に成功すると、Firepower Threat Defense デバイスは Firepower Management Center に接続して使用可能になります。復元された Firepower Threat Defense デバイス上のポリシーは期限切れになります。設定の変更を Firepower Management Center から展開して、ポリシーを更新します。詳細については、設定変更の展開 （447 ページ）を参照してください。
- Firepower Threat Defense デバイスのデータ インターフェイスをネットワークに接続します。手順については、該当する *Cisco Firepower Threat Defense* の *Firepower Management Center* の使用に関するクイック スタート ガイド を参照してください。

バックアップからの FTD の復元：HA ペア（両方のピアの交換）

高可用性構成の両方の Firepower Threat Defense デバイスでハードウェア障害が発生した場合は、次の手順を実行して交換してください。

警告 Firepower Management Center とのすべての通信が停止するため、障害のある Firepower Threat Defense デバイスを登録解除したり、または管理対象外にしないでください。

始める前に

- バックアップと復元の注意事項と制限事項 （201 ページ）を確認してください。

（注） Firepower Threat Defense で稼働している Firepower 4100/9300 シャーシ デバイスを交換する場合、FXOS の設定を Firepower Chassis Manager からエクスポートしてから Firepower Threat Defense のバックアップと復元操作を進めてください。詳細については、『*Cisco FXOS Firepower Chassis Manager* コンフィギュレーション ガイド』の「コンフィギュレーションのインポート/エクスポート」を参照してください。

- Firepower Threat Defense 高可用性ペアのバックアップがあることを確認します。詳細については、デバイスのリモートバックアップ （207 ページ）を参照してください。

バックアップ ファイルは、Firepower Threat Defense デバイスの `/var/sf/backup` でローカルに保持されます。Firepower Management Center 上にバックアップを保持することを選択した場合、バックアップは `/var/sf/remote-backup` ディレクトリに格納されます。Firepower Management Center は、プライマリとセカンダリの Firepower Threat Defense デバイスに対してバックアップ ファイルを個別に作成します。高可用性ペアの Firepower Threat Defense デバイスの場合、バックアップ tar ファイルの形式は `<Hostname/IP>-<Role>-<Timestamp>.tar` です。

- 高可用性ペアの Firepower Threat Defense デバイスに障害が発生した場合は、Cisco Technical Assistance Center（TAC） に連絡して交換を依頼してください。

ステップ 1 障害のあるデバイスをネットワークから取り外します。

ステップ 2 交換用デバイスをネットワーク上に展開し、管理インターフェイスと高可用性リンクを接続して、デバイスの電源を投入します。詳細については、該当する *Firepower* クイック スタート ガイドを参照してください。

（注） トラフィックの中断を回避するため、交換用デバイスにデータ インターフェイスが接続されていないことを確認します。

ステップ 3 交換用デバイスで実行している Firepower システム ソフトウェアのバージョンが、交換対象デバイスで実行しているバージョンと同じであることを確認します。必要に応じて、交換用デバイスを再イメージ化します。詳細については、*Cisco ASA* および *Firepower Threat Defense* デバイスの再イメージ化ガイドを参照してください。

ステップ 4 `restore` コマンドを使用して、両方の Firepower Threat Defense デバイス上のバックアップを連続して復元します。

- ローカルの Firepower Threat Defense デバイスからバックアップを復元するには、`restore remote-manager-backup <backup tar-file>` コマンドを使用します。
- SCP 対応リモート ネットワークからバックアップを復元するには、`restore remote-manager-backup location <scp-hostname> <username> <filepath> <backup tar-file>` コマンドを使用します。

復元されている該当 Firepower Threat Defense デバイスに対応するバックアップ ファイルを選択します。復元操作の進捗状況は、Firepower Threat Defense デバイスの `/var/log/restore.log` ログを表示することでモニタできます。

復元が正常に完了すると、デバイスが再起動します。

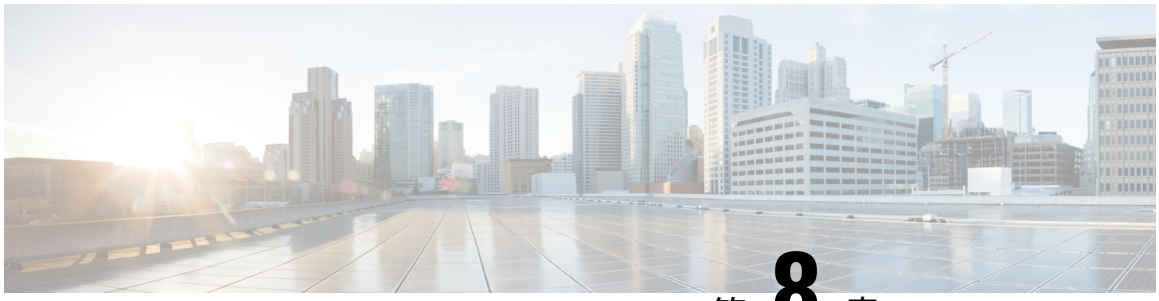
次のタスク

- コマンド ライン インターフェイスで `configure high-availability resume` コマンドを使用して高可用性ピア間で高可用性設定を再開します。
- 復元に成功すると、Firepower Threat Defense デバイスは Firepower Management Center に接続して使用可能になります。復元された Firepower Threat Defense デバイス上のポリシーは期限切れになります。設定の変更を Firepower Management Center から展開して、ポリシーを更新します。詳細については、設定変更の展開 （447 ページ）を参照してください。

- Firepower Threat Defense デバイスのデータ インターフェイスをネットワークに接続します。手順については、該当する *Cisco Firepower Threat Defense* の *Firepower Management Center* の使用に関するクイック スタート ガイド を参照してください。

バックアップと復元の履歴

機能	バージョン	詳細
管理対象デバイスのオンデマンドでのリモート バックアップ	6.3	FMC を使用して、特定の管理対象デバイスのリモートバックアップをオンデマンドで実行できるようになりました。 以前、バックアップをサポートしていたのは 7000 および 8000 シリーズのデバイスのみで、デバイスのローカル GUI を使用する必要がありました。 新規/変更された画面：[システム（System）] > [ツール（Tools）] > [バックアップ/復元（Backup/Restore）] > [管理対象デバイスのバックアップ（Managed Device Backup）] 新規/変更された FTD CLI コマンド： **restore** サポートされるプラットフォーム：FTD の物理プラットフォーム、FTDv for VMware、7000/8000 シリーズ 例外：FTD のクラスタ化されたデバイスまたはコンテナ インスタンスはサポートされていません。



第 8 章

コンフィギュレーションのインポートとエクスポート

次のトピックでは、インポート/エクスポート機能を使用する方法について説明します。

コンフィギュレーションのインポート/エクスポートについて

インポート/エクスポート機能を使用して、アプライアンス間で構成をコピーできます。インポート/エクスポートはバックアップ ツールではありませんが、展開に新しいアプライアンスを追加するプロセスを簡素化できます。

単一の設定をエクスポートすることや、（同じタイプまたは異なるタイプの）一連の設定を単一操作でエクスポートすることができます。後に別のアプライアンスにパッケージをインポートするとき、パッケージ内のどの設定をインポートするかを選択できます。

エクスポートされたパッケージには、その構成のリビジョン情報が含まれ、これにより、別のアプライアンスにその構成をインポートできるかどうかが決まります。アプライアンスに互換性があるものの、パッケージに重複構成が含まれていると、解決オプションが示されます。

（注） インポート側とエクスポート側のアプライアンスは、同じバージョンの Firepower システムを実行している必要があります。アクセスコントロールとそのサブポリシー（侵入ポリシーを含む）の場合、侵入ルールの更新バージョンも一致している必要があります。バージョンが一致しない場合、インポートは失敗します。インポート/エクスポート機能を使用して侵入ルールを更新することはできません。代わりに、最新バージョンのルール更新をダウンロードして適用します。

インポート/エクスポートをサポートする構成

インポート/エクスポートは、次の構成でサポートされます。

- アクセス コントロール ポリシーとそれが呼び出すポリシー：プレフィルタ、ネットワーク分析、侵入、SSL、ファイル、Threat Defense サービス ポリシー
- 侵入ポリシー（アクセス コントロールとは無関係に）
- NAT ポリシー（Firepower Threat Defense のみ）
- FlexConfig ポリシー。ただし、すべての秘密鍵の変数の内容は、ポリシーをエクスポートする際にクリアされます。秘密鍵を使用するFlexConfigポリシーをインポートした後に手動ですべての秘密鍵の値を編集する必要があります。
- プラットフォーム設定
- 正常性ポリシー
- アラート応答
- アプリケーションディテクタ（ユーザ定義およびCisco Professionalサービスによって提供されるディテクタ）
- ダッシュボード
- カスタム テーブル
- カスタム ワークフロー
- 保存済み検索
- カスタム ユーザ ロール
- レポート テンプレート
- サードパーティ製品および脆弱性マッピング

設定のインポート/エクスポートに関する特別な考慮事項

構成をエクスポートすると、他の必要な構成もエクスポートされます。たとえば、アクセスコントロールポリシーをエクスポートすると、そのポリシーが呼び出すサブポリシー、使用しているオブジェクトとオブジェクトグループ、先祖ポリシー（マルチドメイン展開の場合）などもエクスポートされます。別の例として、外部認証が有効になっているプラットフォーム設定ポリシーをエクスポートした場合は、認証オブジェクトもエクスポートされます。ただし、いくつかの例外があります。

- システム提供のデータベースとフィード：URLフィルタリングカテゴリとレピュテーション データ、シスコ インテリジェンス フィードデータ、または地理位置情報データベース（GeoDB）はエクスポートされません。展開内のすべてのアプライアンスがシスコから最新情報を取得していることを確認してください。

- グローバルなセキュリティインテリジェンスのリスト：エクスポートされた構成に関連するグローバルなセキュリティインテリジェンスのブラックリストとホワイトリストがエクスポートされます（マルチドメイン展開では、これは現在のドメインに関係なく実行されます。子孫ドメインのリストはエクスポートされ**ません**）。インポートプロセスはこれらのブラックリストとホワイトリストをユーザ作成リストに変換してから、インポートされた構成でそれらの新しいリストを使用します。これにより、インポートされたリストが既存のグローバルなブラックリストおよびホワイトリストと競合することはありません。インポートされた構成でインポート側の Firepower Management Center のグローバル リストを使用するには、これらを手動で追加します。
- 侵入ポリシー共有層：エクスポートプロセスにより、侵入ポリシー共有レイヤが切断されます。以前の共有レイヤはパッケージに含まれ、インポートされた侵入ポリシーには共有レイヤは含まれません。
- 侵入ポリシーのデフォルト変数セット：エクスポートパッケージには、カスタム変数とシステム提供の変数を含むデフォルト変数セットがユーザ定義値とともに含まれています。インポート プロセスでは、インポートされた値でインポート側の Firepower Management Center のデフォルト変数セットを更新します。ただし、インポートプロセスはエクスポート パッケージに存在しないカスタム変数を削除**しません**。また、エクスポート パッケージに設定されていない値については、インポート側の Firepower Management Center のユーザ定義値を元に戻しません。したがって、インポート側の Firepower Management Center で設定されているデフォルト変数が異なる場合は、インポートされた侵入ポリシーの動作が予想とは異なる可能性があります。
- カスタム ユーザ オブジェクト：Firepower Management Center でカスタム ユーザ グループまたはオブジェクトを作成済みで、そのようなカスタム ユーザ オブジェクトがアクセス コントロール ポリシーのいずれかのルールに含まれている場合、エクスポート ファイル（.sfo）にはそのユーザ オブジェクト情報が格納されません。このため、そうしたポリシーをインポートする際、これらのカスタム ユーザ オブジェクトへの参照が削除され、宛先 Firepower Management Center にはインポートされません。不明なユーザ グループが原因で検出の問題が発生するのを避けるには、カスタマイズされたユーザ オブジェクトを新しい Firepower Management Center に手動で追加し、インポート後にアクセス コントロール ポリシーを再設定します。

オブジェクトおよびオブジェクト グループをインポートする場合：

- 通常、インポートプロセスはオブジェクトとグループを新規としてインポートしますが、既存のオブジェクトとグループを置き換えることはできません。ただし、インポートされた設定のネットワークやポートのオブジェクトまたはグループが既存のオブジェクトまたはグループと一致する場合、インポートした設定は、新しいオブジェクト/グループを作成せずに、既存のオブジェクト/グループを再利用します。システムは、名前（自動生成される番号は除外します）および各ネットワークとポートのオブジェクト/グループの内容を比較して、一致するかどうかを判別します。
- インポートしたオブジェクトの名前がインポートする Firepower Management Center 上の既存のオブジェクトと一致する場合、システムはそれらの名前を一意にするため、インポートされたオブジェクトとグループの名前に自動生成した番号を付加します。

- インポートした設定で使用されているセキュリティ ゾーンとインターフェイス グループを、インポート側の Firepower Management Center で管理されているタイプが一致するゾーンとグループにマッピングする必要があります。
- 秘密キーを含むPKIオブジェクトを使用する構成をエクスポートすると、エクスポートの前に秘密キーが復号されます。インポート時に、キーはランダムに生成されたキーで暗号化されます。

設定のエクスポート

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin

エクスポートされる設定の数や、それらのオブジェクトが参照する設定の数によっては、エクスポート プロセスに数分かかる場合があります。

ヒント

Firepowerシステムの多くのリストページには、リスト項目の横にエクスポートアイコン（）があります。このアイコンがある場合は、それを使用することにより、その後のエクスポート操作を簡単に代行させることができます。

始める前に

- インポートおよびエクスポートするアプライアンスが同じバージョンの Firepower システムを実行していることを確認します。アクセス制御とそのサブポリシー（侵入ポリシーを含む）の場合は、侵入ルールの更新バージョンも一致する必要があります。

ステップ 1 **[System]** > **[Tools]** > **[Import/Export]**を選択します。

折りたたむ（）アイコンか、展開する（）アイコンをクリックし、使用可能な設定のリストを折りたたんだり、展開したりします。

ステップ 2 エクスポートする構成をチェックして [エクスポート（Export）] をクリックします。

ステップ 3 Web ブラウザのプロンプトに従って、エクスポートされたパッケージをコンピュータに保存します。

設定のインポート

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin

インポートされる設定の数や、それらのオブジェクトが参照する設定の数によっては、インポート プロセスに数分かかる場合があります。

（注） システムからログアウトした場合、別のドメインに変更した場合、または[インポート（Import）] をクリックした後にユーザ セッションがタイムアウトした場合、インポート プロセスは完了するまでバックグラウンドで続行されます。

始める前に

- インポートおよびエクスポートするアプライアンスが同じバージョンの Firepower システムを実行していることを確認します。アクセス制御とそのサブポリシー（侵入ポリシーを含む）の場合は、侵入ルールの更新バージョンも一致する必要があります。

ステップ 1 インポートするアプライアンスで、**[System]** > **[Tools]** > **[Import/Export]** を選択します。

ステップ 2 [パッケージのアップロード（Upload Package）] をクリックします。

ステップ 3 エクスポートしたパッケージへのパスを入力するか、そのパッケージの場所を参照して [アップロード（Upload）] をクリックします。

ステップ 4 バージョンが一致していないなどの問題がない場合は、インポートする設定を選択して、[インポート（Import）] をクリックします。
競合の解決やインターフェイス オブジェクトのマッピングを実行する必要がない場合は、インポートが完了して、成功メッセージが表示されます。この手順の残りは省略してください。

ステップ 5 プロンプトが表示されたら、[インポートの競合解決（Import Conflict Resolution）] ページで、インポートする Firepower Management Center で管理されているインターフェイス タイプと一致するゾーンおよびグループに、インポートした設定で使用されている インターフェイス オブジェクトをマップします。

インターフェイス オブジェクト タイプ（セキュリティ ゾーンまたはインターフェイス グループ）およびインターフェイス タイプ（パッシブ、インライン、ルーテッドなど）が送信元と宛先で一致している必要があります。詳細については、インターフェイス オブジェクト：インターフェイスグループとセキュリティ ゾーン （535 ページ）を参照してください。

インポートする設定が存在していないセキュリティ ゾーンまたはインターフェイス グループを参照する場合は、その設定を既存のインターフェイ オブジェクトにマップするか、新しいインターフェイ オブジェクトを作成します。

ステップ 6 [インポート（Import）] をクリックします。

ステップ 7 プロンプトが表示されたら、[インポートの解決（Import Resolution）] ページで、各設定を展開して適切なオプションを選択します。詳細については、インポート競合の解決 （234 ページ）を参照してください。

ステップ 8 [インポート（Import）] をクリックします。

次のタスク

- 必要に応じて、インポートした設定の概要を示すレポートを表示します。タスク メッセージの表示 （417 ページ）を参照してください。

インポート競合の解決

構成をインポートしようすると、同じ名前とタイプの構成がアプライアンスにすでに存在するかどうかがシステムによって確認されます。マルチドメイン展開では、構成が現在のドメイン、またはその先祖あるいは子孫ドメインのいずれかで定義されている構成の複製であるかどうかが確認されます。（子孫ドメインの構成は表示できませんが、重複する名前の構成が子孫ドメインに存在する場合は、システムにより競合が通知されます）。インポートに重複構成が含まれている場合、次の中から展開に適切な解決オプションが表示されます。

- **既存のものを維持する（Keep existing）**

  その構成はインポートされません。

- **既存のものを置換する（Replace existing）**

  インポート用に選択した構成で現在の構成が上書きされます。

- **最新バージョンを残す（Keep newest）**

  選択した構成は、タイムスタンプがアプライアンスの現在の構成のタイムスタンプより新しい場合にのみインポートされます。

- **新たにインポート（Import as new）**

  選択した重複する構成はインポートされ、システム生成の番号が適用されて一意の構成になります。（インポートプロセスが完了する前にこの名前を変更できます）。アプライアンスの元の構成は変更されません。

表示される解決オプションは、展開でドメインを使用するかどうか、およびインポートされた構成が現在のドメインで定義されている構成の複製であるか、または現在のドメインの先祖あるいは子孫で定義された構成であるかどうかによって異なります。次の表に、どの場合に解決オプションが表示されるか表示されないかを示します。

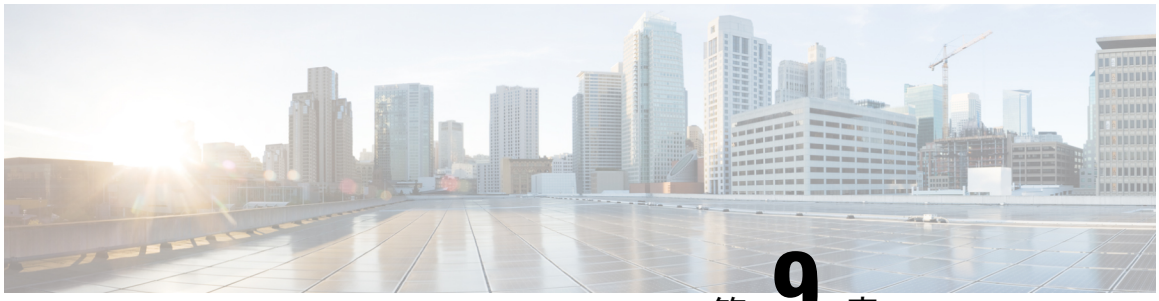
解決オプション	Firepower Management Center		管理対象デバイス
	現在のドメインの複製	子孫または先祖ドメインの複製	
既存のものを維持する（Keep existing）	あり	あり	あり

解決オプション	Firepower Management Center		管理対象デバイス
	現在のドメインの複製	子孫または先祖ドメインの複製	
既存のものを置換する（Replace existing）	あり	なし	あり
最新バージョンを残す（Keep newest）	あり	なし	あり
新たにインポート（Import as new）	あり	あり	あり

クリーンまたはカスタム定義ファイル リストを使用するファイル ポリシーとともにアクセス コントロール ポリシーをインポートし、ファイル リストに重複する名前競合が示されている場合、上記の表に示すように競合解決オプションが表示されますが、ポリシーおよびファイル リストに対して実行されるアクションは、次に表に示すように異なります。

解決オプション	システム アクション	
	アクセス コントロール ポリシーと関連ファイル ポリシーが新たにインポートされ、ファイル リストは統合される	既存のアクセス コントロール ポリシーと関連ファイル ポリシーおよびファイル リストは変更されない
既存のものを維持する（Keep existing）	なし	あり
既存のものを置換する（Replace existing）	あり	なし
新たにインポート（Import as new）	あり	なし
最新バージョンを残す（Keep newest）。インポートされるアクセス コントロール ポリシーが最新	あり	なし
最新バージョンを残す（Keep newest）。既存のアクセス コントロール ポリシーが最新	なし	あり

アプライアンスにインポートされた構成を修正し、後で同じアプライアンスにその構成を再インポートする場合は、保持する構成のバージョンを選択する必要があります。



第 9 章

タスクのスケジューリング

ここでは、タスクをスケジュールする方法について説明します。

タスクのスケジューリングについて

さまざまな種類の管理タスクを、指定した回数（1 度または繰り返し）実行するようにスケジュールを設定できます。

（注） タスクによっては低帯域幅のネットワークに非常に負荷をかけることがあります（ソフトウェアの自動更新が含まれるタスクや、管理対象デバイスに更新をプッシュする必要があるタスクなど）。ネットワーク使用率が低い時間帯にこのようなタスクを実行するよう、スケジュールしてください。

定期タスクの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	タスクに応じて異なる	タスクに応じて異なる	Admin/Maint

定期タスクの頻度を設定する際には、すべてのタイプのタスクで同じ手順に従います。

Webインターフェイスのほとんどのページに表示される時間はローカル時刻であり、ローカル設定で指定したタイム ゾーンに従ってそれが決定されます。さらに、Firepower Management Centerは、該当する場合にはローカル時刻の表示を夏時間（DST）に合わせて自動的に調整し

ます。ただし、DSTから標準時への移行日および元に戻る移行日をまたがる定期タスクは、移行を考慮して調整されません。つまり、標準時の午前 2:00 にタスク スケジュールを作成すると、DST 期間中は午前 3:00 に実行されます。同様に、DST の午前 2:00 にタスク スケジュールを作成すると、標準時には午前 1:00 に実行されます。

ステップ 1 **[システム（System）] > [ツール（Tools）] > [スケジューリング（Scheduling）]** を選択します。

ステップ 2 [タスクの追加（Add Task）] をクリックします。

ステップ 3 [ジョブ タイプ（Job Type）] ドロップダウン リストから、スケジュールするタスクのタイプを選択します。

ステップ 4 [実行するタスクのスケジュール（Schedule task to run）] オプションの横にある [定期（Recurring）] オプション ボタンをクリックします。

ステップ 5 [開始日付（Start On）] フィールドに、定期タスクを開始する日付を指定します。

ステップ 6 [繰り返し設定（Repeat Every）] フィールドに、タスクを繰り返す頻度を指定します。

数値を入力するか、上矢印（▲）および下矢印（▼）アイコンをクリックして、間隔を指定できます。たとえば、2 日おきにタスクを実行するには、2 を入力して [日（Days）] オプション ボタンをクリックします。

ステップ 7 [実行時刻（Run At）] フィールドで、定期タスクを開始する時刻を指定します。

ステップ 8 週または月単位で実行するタスクの場合は、[繰り返す（オン）（Repeat On）] フィールドでタスクを実行する日付を選択します。

ステップ 9 作成するタスクのタイプについて残りのオプションを選択します。

- [バックアップ（Backup）]：FMC およびリモート デバイスのバックアップのスケジューリング （239 ページ）の説明に従って、バックアップ ジョブをスケジュールします。
- [CRL のダウンロード（Download CRL）]：証明書失効リストのダウンロードの設定 （241 ページ）の説明に従って、証明書失効リストのダウンロードをスケジュールします。
- [ポリシーの展開（Deploy Policies）]：ポリシー展開の自動化 （242 ページ）の説明に従って、ポリシーの展開をスケジュールします。
- [Nmap スキャン（Nmap Scan）]：Nmap スキャンのスケジュール （244 ページ）の説明に従って、Nmap スキャンをスケジュールします。
- [レポート（Report）]：次の説明に従って、レポート生成をスケジュールします。 レポートの生成の自動化 （245 ページ）
- [Firepower 推奨ルール（Firepower Recommended Rules）]：次の説明に従って、Firepower 推奨ルールの自動更新をスケジュールします。 Firepower 推奨の自動化 （247 ページ）
- [最新の更新のダウンロード（Download Latest Update）]：ソフトウェア ダウンロードの自動化 （250 ページ）またはVDB 更新のダウンロードの自動化 （253 ページ）の説明に従って、ソフトウェアまたは VDB の更新のダウンロードをスケジュールします。
- [最新の更新のインストール（Install Latest Update）]：ソフトウェア インストールの自動化 （251 ページ）またはVDB 更新のインストールの自動化 （254 ページ）の説明に従って、Firepower Management Center または管理対象デバイスでのソフトウェアまたはVDB の更新のインストールをスケジュールします。

- [最新の更新のプッシュ（Push Latest Update）]：ソフトウェア プッシュの自動化（250ページ）の説明に従って、管理対象デバイスへのソフトウェア更新のプッシュをスケジュールします。
- [URL フィルタリングデータベースの更新（Update URL Filtering Database）]：次の説明に従って、URL フィルタリング データの自動更新をスケジュールします。スケジュール設定されたタスクを使用した URL フィルタリング更新の自動化（255 ページ）

スケジュール バックアップ

Firepower Management Center でスケジューラを使用して、FMC とリモート デバイスの両方のバックアップを自動化することができます。また、7000/8000 シリーズのローカル GUI を使用して、個々のデバイスのバックアップをスケジュールすることもできます。

すべてのデバイスがリモート バックアップをサポートしているわけではないことに注意してください。詳細については、バックアップと復元について（199ページ）を参照してください。

FMC およびリモート デバイスのバックアップのスケジューリング

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	FMC バックアップをサポートしているデバイス	グローバルだけ	Admin/Maint

Firepower Management Center でスケジューラを使用して、FMC とデバイスの両方のバックアップを自動化することができます。すべてのデバイスがリモート バックアップをサポートしているわけではないことに注意してください。詳細については、バックアップと復元について（199 ページ）を参照してください。

始める前に

バックアップ設定を指定するバックアップ プロファイルを作成します。リモート デバイス バックアップの場合、どのデバイスをバックアップするかは、バックアップ プロファイルによって指定されます。詳細については、バックアップ プロファイルの作成（210ページ）を参照してください。

ステップ 1 **[システム（System）] > [ツール（Tools）] > [スケジューリング（Scheduling）]** を選択します。

ステップ 2 [ジョブ タイプ（Job Type）] リストから、[バックアップ（Backup）] を選択します。

ステップ 3 [1回（Once）] または [定期（Recurring）] のどちらでバックアップするかを指定します。

- ワンタイム タスクの場合、ドロップダウンリストを使用して開始日時を指定します。

- 定期タスクの場合、定期タスクの設定 （237 ページ）を参照してください。

ステップ 4 [ジョブ名（Job Name）] を入力します。

ステップ 5 [バックアップのタイプ（Backup Type）]（[管理センター（Management Center）] または [デバイス（Device）] のいずれか）を選択します。

ステップ 6 [バックアッププロファイル（Backup Profile）] を選択します。

ステップ 7 （オプション）[コメント（Comment）] を入力します。

コメントは手短にします。それらはスケジュール予定表ページの [タスクの詳細（Task Details）] セクションに表示されます。

ステップ 8 （オプション）[ステータスの送信先（Email Status To:）] フィールドに、メール アドレスまたはメール アドレスのカンマ区切りのリストを入力します。

タスクのステータス メッセージを送信するように電子メール リレー サーバを設定する方法については、メール リレー ホストおよび通知アドレスの設定 （1303 ページ）を参照してください。

ステップ 9 **[保存（Save）]** をクリックします。

ローカル 7000 & 8000 シリーズ デバイスのバックアップのスケジューリング

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
該当なし	いずれか（Any）	7000 & 8000 シリーズ	該当なし	Admin/Maint

7000 または 8000 シリーズ デバイスでスケジューラを使用して、それ自体のバックアップを自動化することができます。FMC を使用してバックアップをスケジュールするには、FMC およびリモート デバイスのバックアップのスケジューリング （239 ページ）を参照してください。

始める前に

バックアップ設定を指定するバックアップ プロファイルを作成します。詳細については、バックアップ プロファイルの作成 （210 ページ）を参照してください。

ステップ 1 デバイスの Web インターフェイスで、**[システム（System）] > [ツール（Tools）] > [スケジューリング（Scheduling）]** を選択します。

ステップ 2 [ジョブ タイプ（Job Type）] リストから、[バックアップ（Backup）] を選択します。

ステップ 3 [1回（Once）] または [定期（Recurring）] のどちらでバックアップするかを指定します。

- ワンタイム タスクの場合、ドロップダウンリストを使用して開始日時を指定します。
- 定期タスクの場合、定期タスクの設定 （237 ページ）を参照してください。

ステップ 4 [ジョブ名（Job Name）] を入力します。

ステップ 5 [バックアッププロファイル（Backup Profile）] を選択します。

ステップ 6 （オプション）[コメント（Comment）] を入力します。

コメントは手短にします。それらはスケジュール予定表ページの [タスクの詳細（Task Details）] セクションに表示されます。

ステップ 7 （オプション）[ステータスの送信先（Email Status To:）] フィールドに、メール アドレスまたはメール アドレスのカンマ区切りのリストを入力します。

タスクのステータス メッセージを送信するように電子メール リレー サーバを設定する方法については、メール リレー ホストおよび通知アドレスの設定 （1303 ページ）を参照してください。

ステップ 8 **[保存（Save）]** をクリックします。

証明書失効リストのダウンロードの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	デバイスに応じて異なる	Admin/Maint

Firepower Management Center または 7000 または 8000 シリーズ デバイスのローカル Web インターフェイスを使用して、この手順を実行する必要があります。マルチドメイン展開では、このタスクは Firepower Management Center のグローバル ドメインでのみサポートされます。

アプライアンスのユーザ証明書または監査ログ証明書を有効にするアプライアンスのローカル設定で証明書失効リスト（CRL）のダウンロードを有効にすると、CRL のダウンロード タスクが自動的に作成されます。スケジューラを使用してタスクを編集し、更新の頻度を設定できます。

始める前に

- ユーザ証明書または監査ログ証明書を有効にして設定し、1つ以上の CRL のダウンロード URL を設定します。詳細については、有効な HTTPS クライアント証明書の強制 （1260 ページ）と 有効な監査ログ サーバ証明書の要求 （1299 ページ）を参照してください。

ステップ 1 **[システム（System）]** > **[ツール（Tools）]** > **[スケジューリング（Scheduling）]** を選択します。

ステップ 2 [タスクの追加（Add Task）] をクリックします。

ステップ 3 [ジョブ タイプ（Job Type）] リストから、[CRL のダウンロード（Download CRL）] を選択します。

ステップ 4 CRL ダウンロードをスケジュールする頻度として、ワンタイム タスクを示す [1 回（Once）] または定期タスクを示す [定期（Recurring）] を指定します。

- ワンタイム タスクの場合、ドロップダウンリストを使用して開始日時を指定します。

- 定期タスクの場合、詳細については、定期タスクの設定 （237 ページ）を参照してください。

ステップ 5 [ジョブ名（Job Name）] フィールドに名前を入力します。

ステップ 6 タスクについてコメントを付加するには、[コメント（Comment）] フィールドにコメントを入力します。

[コメント（Comment）] フィールドはスケジュール予定表ページの [タスクの詳細（Task Details）] セクションに表示されます。コメントは手短にします。

ステップ 7 タスクのステータス メッセージをメールで送信するには、[ステータスの送信先（Email Status To:）] フィールドにメールアドレス（またはカンマで区切った複数のメールアドレス）を入力します。ステータス メッセージを送信するには、Firepower Management Centerで有効な電子メール中継サーバが設定されている必要があります。

ステップ 8 **[保存（Save）]** をクリックします。

関連トピック

メール リレー ホストおよび通知アドレスの設定 （1303 ページ）

ポリシー展開の自動化

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Maint

FMC の設定を変更した後は、影響を受けるデバイスへ変更を展開する必要があります。

マルチドメイン展開では、現在のドメインに限ってポリシーの展開をスケジュールできます。

⚠

注意 展開する際にリソースを要求すると、いくつかのパケットがインスペクションなしでドロップされることがあります。また、一部のコンフィギュレーションを展開すると、トラフィックのインスペクションを中断するSnortプロセスが再開します。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、ターゲットデバイスがトラフィックを処理する方法に応じて異なります。Snort® の再起動によるトラフィックの動作 （451 ページ）および展開またはアクティブ化された際に Snort プロセスを再起動する設定 （454 ページ）を参照してください。

ステップ 1 **[システム（System）] > [ツール（Tools）] > [スケジューリング（Scheduling）]** を選択します。

ステップ 2 [タスクの追加（Add Task）] をクリックします。

ステップ 3 [ジョブ タイプ（Job Type）] リストから、[ポリシーの展開（Deploy Policies）] を選択します。

ステップ 4 タスクをスケジュールする頻度として、ワンタイム タスクを示す [Once] または定期タスクを示す [Recurring] を指定します。

- ワンタイム タスクの場合、ドロップダウン リストを使用して開始日時を指定します。

- 定期タスクの場合、詳細については、定期タスクの設定 （237 ページ）を参照してください。

ステップ 5 [ジョブ名（Job Name）] フィールドに名前を入力します。

ステップ 6 [デバイス（Device）] フィールドで、ポリシーを展開するデバイスを選択します。

ステップ 7 [最新のデバイスへの展開をスキップする（Skip deployment for up-to-date devices）] チェックボックスを、必要に応じてオンまたはオフにします。

デフォルトでは、ポリシーの展開プロセス中のパフォーマンスを向上させるため、[最新のデバイスへの展開をスキップする（Skip deployment for up-to-date devices）] オプションが有効になっています。

（注） システムは、Firepower Management Center の Web インターフェイスから開始されたポリシーの展開が進行中の場合、スケジュール設定されたポリシーの展開タスクを実行しません。同様に、システムは、スケジュール設定されたポリシーの展開タスクが進行中の場合、Webインターフェイスからポリシーの展開を開始することを許可しません。

ステップ 8 タスクについてコメントを付加するには、[コメント（Comment）] フィールドにコメントを入力します。

[コメント（Comment）] フィールドはスケジュール予定表ページの [タスクの詳細（Task Details）] セクションに表示されます。コメントは手短にします。

ステップ 9 タスクのステータス メッセージをメールで送信するには、[ステータスの送信先（Email Status To:）] フィールドにメールアドレス（またはカンマで区切った複数のメールアドレス）を入力します。ステータス メッセージを送信するには、有効な電子メール中継サーバが設定されている必要があります。

ステップ 10 **[保存（Save）]** をクリックします。

関連トピック

メール リレー ホストおよび通知アドレスの設定 （1303 ページ）
失効ポリシー （459 ページ）

Nmap スキャンの自動化

ネットワーク上のターゲットに対する定期的な Nmap スキャンをスケジュールできます。スキャンを自動化すると、Nmapスキャンによって以前に提供された情報を更新できます。Firepowerシステムは Nmap から提供されるデータを更新できないため、このデータを最新に保つには定期的に再スキャンする必要があります。また、ネットワーク上のホストに識別不能なアプリケーションやサーバがあるかどうか自動的に検査するよう、スキャンをスケジュールすることもできます。

さらに、Discovery Administrator が修正用に Nmap スキャンを使用する場合があることにも注意してください。たとえば、ホストでオペレーティング システム競合が発生したために、Nmap スキャンがトリガーされることがあります。スキャンが実行されると、そのホストでのオペレーティング システムの更新済み情報が取得され、こうして競合が解決されます。

以前にNmapスキャン機能を使用したことがない場合は、スケジュール スキャンを定義する前に、Nmap スキャンを設定します。

関連トピック

Nmap スキャン （2517 ページ）

Nmap スキャンのスケジュール

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Maint

システムで検出されたホストのオペレーティング システム、アプリケーション、またはサーバが Nmap スキャンの結果で置き換えられると、システムは、Nmap によって置換されたホストに関する情報を更新しなくなります。Nmap によって提供されるサービスやオペレーティング システムのデータは、もう 1 度 Nmap スキャンを実行するまで静的な状態のままになります。Nmap を使用したホストのスキャンを計画している場合は、Nmap 提供のオペレーティング システム、アプリケーション、またはサーバを最新の状態に保つために、定期的なスキャン スケジュールをセットアップしてください。ネットワーク マップからホストが削除されて再び追加されると、Nmap スキャン結果はすべて破棄され、システムはホストに関するすべてのオペレーティング システムとサービスのデータのモニタリングを再開します。

マルチドメイン展開では、次のようになります。

- スキャンのスケジュールは、現在のドメインに対してのみ可能です。
- 選択する修正および Nmap ターゲットは、現在のドメインまたは先祖ドメインに存在している必要があります。
- 非リーフ ドメインでの Nmap スキャンの実行を選択すると、そのドメインの各子孫に含まれる同じターゲットをスキャンすることになります。

ステップ 1 **[システム（System）] > [ツール（Tools）] > [スケジューリング（Scheduling）]** を選択します。

ステップ 2 [タスクの追加（Add Task）] をクリックします。

ステップ 3 [ジョブタイプ（Job Type）] リストから、[Nmap スキャン（Nmap Scan）] を選択します。

ステップ 4 タスクをスケジュールする頻度として、ワンタイム タスクを示す [Once] または定期タスクを示す [Recurring] を指定します。

- ワンタイム タスクの場合、ドロップダウン リストを使用して開始日時を指定します。
- 定期タスクの場合、詳細については、定期タスクの設定 （237 ページ） を参照してください。

ステップ 5 [ジョブ名（Job Name）] フィールドに名前を入力します。

ステップ 6 [Nmap 修復（Nmap Remediation）] フィールドで、Nmap 修復を選択します。

ステップ 7 [Nmap ターゲット（Nmap Target）] フィールドで、スキャン ターゲットを選択します。

ステップ 8 [ドメイン（Domain）] フィールドで、増補するネットワーク マップを持つドメインを選択します。

ステップ 9 タスクについてコメントを付加するには、[コメント（Comment）] フィールドにコメントを入力します。

ヒント [コメント（Comment）]フィールドはスケジュール予定表ページの[タスクの詳細（Task Details）]セクションに表示されます。コメントは手短にします。

ステップ 10 タスクのステータス メッセージをメールで送信するには、[ステータスの送信先（Email Status To:）]フィールドにメールアドレス（またはカンマで区切った複数のメールアドレス）を入力します。ステータス メッセージを送信するには、有効な電子メール中継サーバが設定されている必要があります。

ステップ 11 **[保存（Save）]** をクリックします。

関連トピック

メール リレー ホストおよび通知アドレスの設定 （1303 ページ）

レポートの生成の自動化

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Maint

一定期間ごとにレポートを実行するよう自動化できます。

マルチドメイン展開では、現在のドメインに限ってレポートをスケジュールできます。

始める前に

- リスク レポート以外のレポートの場合：レポート テンプレートを作成します。詳細については、レポート テンプレート （2775 ページ）を参照してください。
- スケジューラを使用してメール レポートを配布するには、メール リレーのホストを設定し、レポートの受信者およびメッセージ情報を指定します。メール リレー ホストおよび通知アドレスの設定（1303 ページ） と、（リスク レポート以外のレポートの場合）レポートの生成時の電子メール配布 （2801 ページ）または（リスク レポートの場合）リスク レポートの生成、表示および印刷 （2774 ページ）を参照してください。
- （オプション）スケジュール設定されたレポートのファイル名、出力フォーマット、時間枠、またはメール配布の設定を設定または変更します。スケジュールされたレポート生成設定の指定 （246 ページ）を参照してください。
- レポートの出力形式として PDF を選択する場合は、テンプレートの各セクションの結果数が PDF の制限を超えないことを、レポート テンプレートで確認してください。詳細については、レポート テンプレート フィールド （2776 ページ）を参照してください。

ステップ 1 **[システム（System）]** > **[ツール（Tools）]** > **[スケジューリング（Scheduling）]** を選択します。

ステップ 2 [タスクの追加（Add Task）] をクリックします。

ステップ 3 [ジョブタイプ（Job Type）] リストから、[レポート（Report）] を選択します。

ステップ 4 タスクをスケジュールする頻度として、ワンタイム タスクを示す [Once] または定期タスクを示す [Recurring] を指定します。

- ワンタイム タスクの場合、ドロップダウン リストを使用して開始日時を指定します。
- 定期タスクの場合、詳細については、定期タスクの設定 （237 ページ）を参照してください。

ステップ 5 [ジョブ名（Job Name）] フィールドに名前を入力します。

ステップ 6 [レポートテンプレート（Report Template）] フィールドで、リスクレポート、またはレポートテンプレートを選択します。

ステップ 7 タスクについてコメントを付加するには、[コメント（Comment）] フィールドにコメントを入力します。

[コメント（Comment）] フィールドはスケジュール予定表ページの [タスクの詳細（Task Details）] セクションに表示されます。コメントは手短にします。

ステップ 8 タスクのステータス メッセージをメールで送信するには、[ステータスの送信先（Email Status To:）] フィールドにメールアドレス（またはカンマで区切った複数のメールアドレス）を入力します。ステータス メッセージを送信するには、有効な電子メール中継サーバが設定されている必要があります。

（注） このオプションを設定しても、レポートは配布されません。

ステップ 9 レポートのデータがない場合（たとえばレポート期間中に特定のタイプのイベントが発生しなかった場合）にレポート電子メール添付ファイルを受信しないようにするには、[空のレポートも添付（If report is empty, still attach to email）] チェックボックスを選択します。

ステップ 10 **[保存（Save）]** をクリックします。

スケジュールされたレポート生成設定の指定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Any Security Analyst

スケジュールされたレポートのファイル名、出力形式、時間枠、電子メール配布の設定を指定または変更するには、次の手順に従います。

ステップ 1 [概要（Overview）] > [レポート（Reporting）] > [レポート テンプレート（Report Templates）] の順に選択します。

ステップ 2 変更するレポート テンプレートの [編集（Edit）] をクリックします。

ステップ 3 PDF 出力を選択する場合は、次のようにします。

a) レポートのいずれかのセクションで、結果数の横に黄色い三角形が示されているかどうかを調べます。

b) 黄色の三角形が示されている場合、三角形の上にマウス カーソルを重ねると、PDF 出力のそのセクションに対して許容される結果の最大数が表示されます。

c) 黄色い三角形が示されているセクションごとに、結果数を最大数未満の数に削減します。
d) 黄色い三角形が示されなくなったら、[保存（Save）] をクリックします。

ステップ 4 [生成（Generate）] をクリックします。

（注） 今すぐレポートを生成せずにレポート生成の設定を変更する場合は、テンプレート設定ページで [生成（Generate）] をクリックする必要があります。レポートを生成しない限り、テンプレート リスト ビューで [生成（Generate）] をクリックしても変更は保存されません。

ステップ 5 設定を変更します。

ステップ 6 レポートを生成せずに新しい設定を保存するには、[キャンセル（Cancel）] をクリックします。

新しい設定を保存してレポートを生成するには、[生成（Generate）] をクリックし、この手順の残りのステップをスキップします。

ステップ 7 [保存（Save）] をクリックします。

ステップ 8 保存を求めるプロンプトが出されたら、まだ変更していない場合でも [OK] をクリックします。

Firepower 推奨の自動化

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Maint

カスタム侵入ポリシーで保存済みの最新の設定を使用し、ネットワークのディスカバリ データに基づいてルール状態の推奨を自動的に生成することができます。

（注） 変更が未保存のまま、侵入ポリシーに関するスケジュール済み推奨がシステムによって自動生成される場合、自動生成された推奨をポリシーに反映させるには、そのポリシー内の変更を破棄してポリシーをコミットする必要があります。

タスクを実行すると、推奨ルール状態が自動的に生成され、ポリシーの設定に基づいて侵入ルールの状態が変更されます。変更されたルール状態は、侵入ポリシーを次回に展開するときに有効になります。

マルチドメイン展開では、現在のドメインレベルの侵入ポリシーに関する推奨を自動化できます。 システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、先祖ドメインの侵入ポリシーでこの機能を有効にすると、システムはすべての子孫のリーフ ドメインからのデータを使用して、推奨事項を生成します。これにより、侵入ルールをすべてのリーフ ドメインに存在しない可能性があるアセットに調整することができ、パフォーマンスに影響を与えることができます。

始める前に

- 以下で説明されている、侵入ポリシーでの Firepower 推奨ルールを設定します。 Firepower の推奨事項の生成と適用 （2111 ページ）
- タスクのステータス メッセージをメールで送るには、有効なメール リレー サーバを設定します。

ステップ 1 **[システム（System）] > [ツール（Tools）] > [スケジューリング（Scheduling）]**を選択します。

ステップ 2 [タスクの追加（Add Task）] をクリックします。

ステップ 3 [ジョブ タイプ（Job Type）] リストから、[Firepower 推奨ルール（Firepower Recommended Rules）] を選択します。

ステップ 4 タスクをスケジュールする頻度として、ワンタイム タスクを示す [Once] または定期タスクを示す [Recurring] を指定します。

- ワンタイム タスクの場合、ドロップダウン リストを使用して開始日時を指定します。
- 定期タスクの場合、詳細については、定期タスクの設定 （237 ページ）を参照してください。

ステップ 5 [ジョブ名（Job Name）] フィールドに名前を入力します。

ステップ 6 [ポリシー（Policies）] の横で、推奨を生成する 1 つ以上の侵入ポリシーを選択します。[すべてのポリシー（All Policies）] チェックボックスをオンにして、すべての侵入ポリシーを選択します。

ステップ 7 （オプション）[コメント（Comments）] フィールドにコメントを入力します。

コメントは手短にします。コメントはスケジュール予定表ページの [タスクの詳細（Task Details）] セクションに表示されます。

ステップ 8 （オプション）タスクのステータス メッセージをメールで送信するには、[ステータスの送信先（Email Status To:）] フィールドにメールアドレス（またはカンマで区切った複数のメールアドレス）を入力します。

ステップ 9 **[保存（Save）]** をクリックします。

関連トピック

競合と変更：ネットワーク分析および侵入ポリシー （2041 ページ）
Firepower 推奨ルールについて （2107 ページ）
メール リレー ホストおよび通知アドレスの設定 （1303 ページ）

ソフトウェア更新の自動化

ほとんどのパッチや機能リリースは、自動的にダウンロードして Firepower システムに適用することができます。

ソフトウェア更新をインストールするためにどんなタスクをスケジュールする必要があるかは、FMC を更新する場合と、FMC を使用して管理対象デバイスを更新する場合とで異なります。

（注） シスコでは、FMC を使用して管理対象デバイスを更新することを**強く**お勧めしています。

- FMC を更新するには、Install Latest Update タスクを使用してソフトウェア インストールをスケジュールします。
- FMCを使用して管理対象デバイスのソフトウェア更新を自動化するには、次の2つのタスクをスケジュールする必要があります。
  - Push Latest Update タスクを使用して、管理対象デバイスに更新をプッシュ（コピー）します。
  - Install Latest Update タスクを使用して、管理対象デバイスに更新をインストールします。

  管理対象デバイスに更新をスケジュールする場合、push and install タスクが連続して発生するようにスケジュールします。更新をインストールする前に、最初にデバイスに更新をプッシュする必要があります。デバイス グループでのソフトウェア更新を自動化するには、グループ内のすべてのデバイスを選択する必要があります。タスク間に、プロセスが完了するのに十分な時間があるようにします。タスクとタスクの間に 30 分以上の間隔をあけてスケジュールしてください。更新をインストールするようにタスクをスケジュールしても、FMC からデバイスへの更新のコピーが終了していないと、インストール タスクは正しく実行されません。ただし、スケジュール済みインストール タスクが毎日繰り返される場合は、翌日の実行時に、すでにプッシュされた更新がインストールされます。

（注） 手動で更新をアップロードしてインストールする必要が生じる状況が 2 つあります。まず、Firepower システムへのメジャー アップデート（主要な更新）をスケジュールすることはできません。次に、サポート サイトにアクセスできない FMC の更新や、そのアプライアンスからのプッシュをスケジュールすることはできません。FMC がインターネットに直接接続しない場合、管理インターフェイスの設定を使用して、サポート サイトから更新をダウンロードできるようプロキシをセットアップする必要があります。

デバイス グループに更新プログラムをインストールするようにスケジュールされたタスクによって、デバイス グループ内の各デバイスにプッシュされた更新プログラムが同時にインストールされることに注意してください。デバイス グループ内の各デバイスについてスケジュールされたタスクが完了するだけの十分な時間を確保してください。

このプロセスをより確実に制御するには、更新がリリースされたことがわかった後、[1 回（Once）] オプションを使用してオフピーク時間帯に更新をダウンロードしインストールできます。

関連トピック

管理インターフェイス （1266 ページ）
FirePOWER の更新について （179 ページ）

ソフトウェア ダウンロードの自動化

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	グローバルだけ	Admin/Maint

Cisco から最新のソフトウェア更新を自動的にダウンロードするスケジュール済みタスクを作成することができます。このタスクを使用すると、手動でインストールする予定の更新のダウンロードをスケジュールできます。

ステップ 1 **[システム（System）] > [ツール（Tools）] > [スケジューリング（Scheduling）]** を選択します。

ステップ 2 [タスクの追加（Add Task）] をクリックします。

ステップ 3 [ジョブ タイプ（Job Type）] リストから、[最新の更新のダウンロード（Download Latest Update）] を選択します。

ステップ 4 タスクをスケジュールする頻度として、ワンタイム タスクを示す [Once] または定期タスクを示す [Recurring] を指定します。

- ワンタイム タスクの場合、ドロップダウン リストを使用して開始日時を指定します。
- 定期タスクの場合、詳細については、定期タスクの設定 （237 ページ）を参照してください。

ステップ 5 [ジョブ名（Job Name）] フィールドに名前を入力します。

ステップ 6 [アップデート項目（Update Items）] の横の [ソフトウェア（Software）] チェックボックスをオンにします。

ステップ 7 タスクについてコメントを付加するには、[コメント（Comment）] フィールドにコメントを入力します。

[コメント（Comment）] フィールドはスケジュール予定表ページの [タスクの詳細（Task Details）] セクションに表示されます。コメントは手短にします。

ステップ 8 タスクのステータス メッセージをメールで送信するには、[ステータスの送信先（Email Status To:）] フィールドにメールアドレス（またはカンマで区切った複数のメールアドレス）を入力します。ステータス メッセージを送信するには、有効な電子メール中継サーバが設定されている必要があります。

ステップ 9 **[保存（Save）]** をクリックします。

関連トピック

メール リレー ホストおよび通知アドレスの設定 （1303 ページ）

ソフトウェア プッシュの自動化

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	グローバルだけ	Admin/Maint

管理対象デバイスでのソフトウェア更新のインストールを自動化するには、インストールの前に、更新をデバイスにプッシュする必要があります。

ソフトウェア更新を管理対象デバイスにプッシュするタスクを作成する際には、更新がデバイスに確実にコピーされるよう、プッシュ タスクとスケジュール済みインストール タスクの間に十分な時間を確保してください。

ステップ 1 **[システム（System）] > [ツール（Tools）] > [スケジューリング（Scheduling）]** を選択します。

ステップ 2 [タスクの追加（Add Task）] をクリックします。

ステップ 3 [ジョブタイプ（Job Type）] リストから、[最新の更新をプッシュ（Push Latest Update）] を選択します。

ステップ 4 タスクをスケジュールする頻度として、ワンタイム タスクを示す [Once] または定期タスクを示す [Recurring] を指定します。

- ワンタイム タスクの場合、ドロップダウン リストを使用して開始日時を指定します。
- 定期タスクの場合、詳細については、定期タスクの設定 （237 ページ）を参照してください。

ステップ 5 [ジョブ名（Job Name）] フィールドに名前を入力します。

ステップ 6 [デバイス（Device）] ドロップダウン リストから、更新するデバイスを選択します。

ステップ 7 タスクについてコメントを付加するには、[コメント（Comment）] フィールドにコメントを入力します。

[コメント（Comment）] フィールドはスケジュール予定表ページの [タスクの詳細（Task Details）] セクションに表示されます。コメントは手短にします。

ステップ 8 タスクのステータス メッセージをメールで送信するには、[ステータスの送信先（Email Status To:）] フィールドにメールアドレス（またはカンマで区切った複数のメールアドレス）を入力します。ステータス メッセージを送信するには、有効な電子メール中継サーバが設定されている必要があります。

ステップ 9 **[保存（Save）]** をクリックします。

関連トピック

メール リレー ホストおよび通知アドレスの設定 （1303 ページ）

ソフトウェア インストールの自動化

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	グローバルだけ	Admin/Maint

管理対象デバイスへ更新をプッシュするタスクと、その更新をインストールするタスクの間に十分な時間を確保する必要があります。

⚠

注意 インストールする更新によっては、ソフトウェアのインストール後にアプライアンスがリブートする場合があります。

ステップ 1 **[システム（System）] > [ツール（Tools）] > [スケジューリング（Scheduling）]** を選択します。

ステップ 2 [タスクの追加（Add Task）] をクリックします。

ステップ 3 [ジョブ タイプ（Job Type）] リストから、[最新の更新のインストール（Install Latest Update）] を選択します。

ステップ 4 タスクをスケジュールする頻度として、ワンタイム タスクを示す[Once]または定期タスクを示す[Recurring]を指定します。

- ワンタイム タスクの場合、ドロップダウン リストを使用して開始日時を指定します。
- 定期タスクの場合、詳細については、定期タスクの設定 （237 ページ）を参照してください。

ステップ 5 [ジョブ名（Job Name）] フィールドに名前を入力します。

ステップ 6 [デバイス（Device）] ドロップダウン リストから、更新をインストールするアプライアンス（Firepower Management Centerを含む）を選択します。

ステップ 7 [アップデート項目（Update Items）] の横の [ソフトウェア（Software）] チェックボックスをオンにします。

ステップ 8 タスクについてコメントを付加するには、[コメント（Comment）]フィールドにコメントを入力します。

[コメント（Comment）] フィールドはスケジュール予定表ページの [タスクの詳細（Task Details）] セクションに表示されます。コメントは手短にします。

ステップ 9 タスクのステータス メッセージをメールで送信するには、[ステータスの送信先（Email Status To:）] フィールドにメールアドレス（またはカンマで区切った複数のメールアドレス）を入力します。ステータス メッセージを送信するには、有効な電子メール中継サーバが設定されている必要があります。

ステップ 10 **[保存（Save）]** をクリックします。

関連トピック

メール リレー ホストおよび通知アドレスの設定 （1303 ページ）

脆弱性データベースの更新の自動化

Cisco では脆弱性データベース（VDB）更新を使用して、Firepower システムで認識されるネットワーク アセット、トラフィック、および脆弱性のリストを拡張しています。スケジュール機能を使用して VDB を更新できるため、常に最新の情報を使ってネットワーク上のホストを評価することができます。

VDB 更新を自動化する場合、次に示す 2 つの別個の手順を自動化する必要があります。

- VDB 更新をダウンロードします。
- VDB 更新をインストールします。

注意 VDB の更新に管理対象デバイスに適用される変更が含まれている場合、VDB のインストール後の最初の手動による展開またはスケジュール済みの展開により Snort プロセスが再起動してトラフィックのインスペクションが中断します。展開ダイアログ メッセージで、Firepower Threat Defence デバイスへの展開が保留されている状態での再起動が警告されます。この中断中にインスペクションを続行せずにトラフィックがドロップされるかパスするどうかは、対象デバイスによるトラフィックの処理方法によって異なります。Firepower Management Center にのみ適用される VDB の更新を展開することはできません。またこの更新により再起動は発生しません。詳細については、Snort® の再起動によるトラフィックの動作（451 ページ）を参照してください。

プロセスを完了させるには、タスクとタスクの間に十分な時間を確保してください。たとえば、更新のインストール タスクをスケジュールした場合、更新がまだ完全にダウンロードされていないと、インストール タスクは正しく実行されません。ただし、スケジュール済みインストール タスクが毎日繰り返される場合は、翌日のタスク実行時に、ダウンロード済みの VDB 更新がインストールされます。

（注）

- サポート サイトにアクセスできないアプライアンスの更新をスケジュールすることはできません。FMC がインターネットに直接接続されていない場合、管理インターフェイスの設定を使用して、プロキシが更新をサポート サイトからダウンロードできるようにプロキシをセットアップする必要があります。
- このプロセスをより確実に制御するには、更新がリリースされたことがわかった後、[1 回（Once）] オプションを使用してオフピーク時間帯に VDB 更新をダウンロードしてインストールできます。
- マルチドメイン展開では、VDB 更新をスケジュールできるのはグローバル ドメインについてのみです。変更は、ポリシーを再度展開したときに有効になります。

関連トピック

管理インターフェイス （1266 ページ）

VDB 更新のダウンロードの自動化

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	グローバルだけ	Admin/Maint

ステップ 1 **[システム（System）] > [ツール（Tools）] > [スケジューリング（Scheduling）]** を選択します。

ステップ 2 [タスクの追加（Add Task）] をクリックします。

ステップ 3 [ジョブ タイプ（Job Type）] リストから、[最新の更新のダウンロード（Download Latest Update）] を選択します。

ステップ 4 タスクをスケジュールする頻度として、ワンタイム タスクを示す [Once] または定期タスクを示す [Recurring] を指定します。

- ワンタイム タスクの場合、ドロップダウン リストを使用して開始日時を指定します。
- 定期タスクの場合、詳細については、定期タスクの設定 （237 ページ）を参照してください。

ステップ 5 [ジョブ名（Job Name）] フィールドに名前を入力します。

ステップ 6 [アップデート項目（Update Items）] の横の [脆弱性データベース（Vulnerability Database）] チェックボックスをオンにします。

ステップ 7 タスクについてコメントを付加するには、[コメント（Comment）] フィールドにコメントを入力します。

[コメント（Comment）] フィールドはスケジュール予定表ページの [タスクの詳細（Task Details）] セクションに表示されます。コメントは手短にします。

ステップ 8 タスクのステータス メッセージをメールで送信するには、[ステータスの送信先（Email Status To:）] フィールドにメールアドレス（またはカンマで区切った複数のメールアドレス）を入力します。ステータス メッセージを送信するには、有効な電子メール中継サーバが設定されている必要があります。

ステップ 9 **[保存（Save）]** をクリックします。

関連トピック

メール リレー ホストおよび通知アドレスの設定 （1303 ページ）

VDB 更新のインストールの自動化

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	グローバルだけ	Admin/Maint

VDB 更新をダウンロードするタスクと、その更新をインストールするタスクの間に十分な時間を確保してください。

注意 VDB の更新に管理対象デバイスに適用される変更が含まれている場合、VDB のインストール後の最初の手動による展開またはスケジュール済みの展開により Snort プロセスが再起動してトラフィックのインスペクションが中断します。展開ダイアログ メッセージで、Firepower Threat Defence デバイスへの展開が保留されている状態での再起動が警告されます。この中断中にインスペクションを続行せずにトラフィックがドロップされるかパスするどうかは、対象デバイスによるトラフィックの処理方法によって異なります。Firepower Management Center にのみ適用される VDB の更新を展開することはできません。またこの更新により再起動は発生しません。詳細については、Snort® の再起動によるトラフィックの動作 （451 ページ）を参照してください。

ステップ 1 **[システム（System）] > [ツール（Tools）] > [スケジューリング（Scheduling）]** を選択します。

ステップ 2 [タスクの追加（Add Task）] をクリックします。

ステップ 3 [ジョブ タイプ（Job Type）] リストから、[最新の更新のインストール（Install Latest Update）] を選択します。

ステップ 4 タスクをスケジュールする頻度として、ワンタイム タスクを示す [Once] または定期タスクを示す [Recurring] を指定します。

- ワンタイム タスクの場合、ドロップダウン リストを使用して開始日時を指定します。
- 定期タスクの場合、詳細については、定期タスクの設定 （237 ページ）を参照してください。

ステップ 5 [ジョブ名（Job Name）] フィールドに名前を入力します。

ステップ 6 [デバイス（Device）] ドロップダウン リストから FMC を選択します。

ステップ 7 [アップデート項目（Update Items）] の横の [脆弱性データベース（Vulnerability Database）] チェックボックスをオンにします。

ステップ 8 タスクについてコメントを付加するには、[コメント（Comment）] フィールドにコメントを入力します。

ヒント コメント フィールドはページの [タスクの表示（View Tasks）] セクションに表示されるので、ある程度短くしてください。

ステップ 9 タスクのステータス メッセージをメールで送信するには、[ステータスの送信先（Email Status To:）] フィールドにメールアドレス（またはカンマで区切った複数のメールアドレス）を入力します。ステータス メッセージを送信するには、有効な電子メール中継サーバが設定されている必要があります。

ステップ 10 **[保存（Save）]** をクリックします。

関連トピック

メール リレー ホストおよび通知アドレスの設定 （1303 ページ）

スケジュール設定されたタスクを使用した URL フィルタリング更新の自動化

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス（Access）
URL フィルタリング	URL フィルタリング	いずれか（Any）	グローバルだけ	Admin/Maint

URL フィルタリングの脅威データが最新であることを確認するため、システムは、Cisco（Collective Security IntelligenceCSI）クラウドからデータ更新を取得する必要があります。

デフォルトでは、URL フィルタリングを有効にすると、自動更新が有効になります。ただし、これらの更新が発生する時間を制御する必要がある場合には、デフォルトの更新メカニズムではなく、このトピックで説明されている手順を使用します。

通常、毎日の更新は小規模ですが、最終更新日から5日を超えると、帯域幅によっては新しいURL フィルタリング データのダウンロードに最長 20 分かかる場合があります。その場合、アップデート自体の実行にも最大 30 分かかることがあります。

始める前に

- Firepower Management Center にインターネット アクセス権があることを確認してください（セキュリティ、インターネットアクセス、および通信ポート（3281 ページ）を参照）。
- URL フィルタリングが有効にされていることを確認します。詳細については、カテゴリとレピュテーションを使用した URL フィルタリングの有効化（1724 ページ）を参照してください。
- **[System]** > **[Integration]** メニューの **[Cloud Services]** タブで [自動更新を有効にする（Enable Automatic Updates）] が選択されていないことを確認します。

ステップ 1 **[システム（System）]** > **[ツール（Tools）]** > **[スケジューリング（Scheduling）]** を選択します。

ステップ 2 [タスクの追加（Add Task）] をクリックします。

ステップ 3 [ジョブ タイプ（Job Type）] リストから、[URL フィルタリング データベースの更新（Update URL Filtering Database）] を選択します。

ステップ 4 更新をスケジュールする頻度として、ワンタイム更新を示す [Once] または定期更新を示す [Recurring] を指定します。

- ワンタイム タスクの場合、ドロップダウン リストを使用して開始日時を指定します。
- 定期タスクの場合、詳細については、定期タスクの設定 （237 ページ）を参照してください。

ステップ 5 [ジョブ名（Job Name）] フィールドに名前を入力します。

ステップ 6 タスクについてコメントを付加するには、[コメント（Comment）] フィールドにコメントを入力します。

[コメント（Comment）] フィールドはスケジュール予定表ページの [タスクの詳細（Task Details）] セクションに表示されます。コメントは手短にします。

ステップ 7 タスクのステータス メッセージをメールで送信するには、[ステータスの送信先（Email Status To:）] フィールドにメールアドレス（またはカンマで区切った複数のメールアドレス）を入力します。ステータス メッセージを送信するには、有効な電子メール中継サーバが設定されている必要があります。

ステップ 8 **[保存（Save）]** をクリックします。

関連トピック

メール リレー ホストおよび通知アドレスの設定 （1303 ページ）

スケジュール済みタスクの確認

スケジュール済みタスクを追加した後、それらのタスクを表示したり、状態を評価したりできます。ページの [View Options] セクションで、カレンダーやスケジュール済みタスク リストを使用してスケジュール済みタスクを表示できます。

カレンダー表示オプションを使用すると、どの日にどのスケジュール済みタスクが行われるかを表示できます。

タスク リストには、タスクのリストとその状態が表示されます。タスクリストき、カレンダーを開いたときにカレンダーの下にが表示されます。また、カレンダーで1つの日付またはタスクを選択して表示することもできます。

以前に作成したスケジュール済みタスクを編集できます。この機能は、パラメータが正しいことを確認するために、スケジュール済みタスクを1度テストする場合に特に役立ちます。タスクが正常に完了したら、あとで定期タスクに変更できます。

[Schedule View] ページから 2 種類の削除操作を実行できます。まだ実行されていない特定のワンタイム タスク、または定期タスクのすべてのインスタンスを削除できます。定期タスクの1つのインスタンスを削除すると、そのタスクのすべてのインスタンスが削除されます。1 度だけ実行するようスケジュールされているタスクを削除すると、そのタスクだけが削除されます。

タスク一覧の詳細

表 *25*: タスク一覧のカラム

カラム	説明
Name	スケジュール済みタスクの名前と、関連付けられているコメントを表示します。
Type	スケジュール済みタスクのタイプを表示します。
Start Time	スケジュールされている開始日時を表示します。
Frequency	タスクの実行頻度を表示します。
前回の実行時間（Last Run Time）	実際の開始日時を表示します。 定期タスクの場合、これは最新の実行に適用されます。

カラム	説明
最終実行ステータス（Last Run Status）	スケジュール済みタスクの現在の状態を次のように示します。 • チェック マーク アイコン（  ）は、タスクが正常に実行されたことを示します。 • 疑問符アイコン（  ）は、タスクの状態が不明であることを示します。 • 感嘆符アイコン（  ）は、タスクが失敗したことを示します。 定期タスクの場合、これは最新の実行に適用されます。
次回の実行時間（Next Run Time）	定期タスクの次の実行時間を表示します。 ワンタイム タスクの場合に「該当なし（N/A）」と表示します。
Creator	スケジュール済みタスクを作成したユーザの名前を表示します。
Edit	スケジュール済みタスクを編集します。
Delete	スケジュール済みタスクを削除します。

カレンダーのスケジュール済みタスクの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Maint

マルチドメイン展開では、現在のドメインのスケジュール済みタスクのみを表示できます。

ステップ 1 **[システム（System）] > [ツール（Tools）] > [スケジューリング（Scheduling）]** を選択します。

ステップ 2 カレンダー ビューを使用して、次のタスクを実行できます。

- 二重左矢印アイコン（  ）をクリックすると、1 年戻ります。
- 単一の左矢印アイコン（）をクリックすると、1 ヵ月戻ります。
- 単一の右矢印アイコン（  ）をクリックすると、1 ヵ月進みます。

- 二重右矢印アイコン（»）をクリックすると、1 年進みます。
- [Today] をクリックすると、現在の年月に戻ります。
- [Add Task] をクリックすると、新しいタスクをスケジュールできます。
- 1 つの日付をクリックすると、カレンダーの下にあるタスク リスト表に、特定の日付のスケジュール済みタスクがすべて表示されます。
- ある日付の特定のタスクをクリックすると、カレンダーの下にあるタスク リスト表にそのタスクが表示されます。

スケジュール済みタスクの編集

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Maint

マルチドメイン展開では、現在のドメインのスケジュール済みタスクのみを編集できます。

ステップ 1 **[システム（System）] > [ツール（Tools）] > [スケジューリング（Scheduling）]** を選択します。

ステップ 2 カレンダーで、編集するタスク、またはタスクが表示されている日付をクリックします。

ステップ 3 [タスクの詳細（Task Details）] テーブルで、編集するタスクの横にある編集アイコン（）をクリックします。

ステップ 4 タスクを編集します。

ステップ 5 **[保存（Save）]** をクリックします。

スケジュール済みタスクの削除

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Maint

マルチドメイン導入では、現在のドメインのスケジュール済みタスクのみを削除できます。

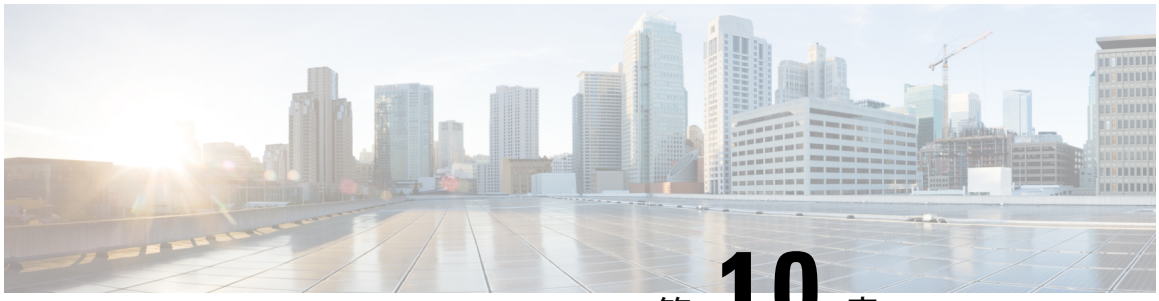
ステップ 1 **[システム（System）] > [ツール（Tools）] > [スケジューリング（Scheduling）]** を選択します。

ステップ 2 カレンダーで、削除するタスクをクリックします。繰り返しタスクの場合は、タスクのインスタンスをクリックします。

ステップ 3 [タスク詳細（Task Details）] テーブルで、削除アイコン（）をクリックし、選択内容を確認します。

スケジュール済みタスクの履歴

機能	バージョン	詳細
管理対象デバイスのスケジュールされたリモート バックアップ	6.4	FMC を使用して、特定の管理対象デバイスのリモートバックアップをスケジュールできるようになりました。 以前、スケジュールされたバックアップをサポートしていたのは 7000 および 8000 シリーズのデバイスのみで、デバイスのローカル GUI を使用する必要がありました。 新規/変更された画面：[システム（System）] > [ツール（Tools）] > [スケジューリング（Scheduling）] > [タスクの追加/編集（add/edit task）] > [ジョブタイプ：バックアップ（Job Type: Backup）] を選択 > [バックアップのタイプ（Backup Type）] を選択 サポートされるプラットフォーム：FTD の物理プラットフォーム、FTDv for VMware、7000/8000 シリーズ 例外：FTD のクラスタ化されたデバイスまたはコンテナ インスタンスはサポートされていません。



第 10 章

FMC データベースの消去

以下のトピックでは、FMC から検出データを消去する方法を示します。

FMC データベースからのデータの消去

スマート ライセンス	従来のライセンス	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	グローバルだけ	Admin/Security Analyst

データベース消去ページを使用すると、検出、アイデンティティ、接続、およびセキュリティインテリジェンスのデータ ファイルを FMC データベースから消去できます。データベースを消去すると、該当するプロセスが再起動される点に注意してください。

⚠

注意 データベースを消去すると、Firepower Management Center から指定したデータが削除されます。削除されたデータは復元できません。

ステップ 1 **[System]** > **[Tools]** > **[Data Purge]**を選択します。

ステップ 2 [Discovery and Identity] の下で、次のいずれかまたはすべてを実行します。

- [ネットワーク検出イベント（Network Discovery Events）] チェックボックスをオンにして、データベースからすべてのネットワーク検出イベントを削除します。
- [ホスト（Hosts）] チェックボックスをオンにして、データベースからすべてのホストとホストの侵害の兆候フラグを削除します。
- [ユーザ アクティビティ（User Activity）] チェックボックスをオンにして、データベースからすべてのユーザ アクティビティ イベントを削除します。
- [ユーザ アイデンティティ（User Identities）] チェックボックスをオンにして、データベースからすべてのユーザ ログインとユーザ履歴データ、およびユーザの侵害の兆候フラグを削除します。

ステップ 3 [接続（Connections）] で、次のいずれかまたはすべてを実行します。

- [接続イベント（Connection Events）] チェックボックスをオンにして、データベースからすべての接続データを削除します。
- [接続の概要イベント（Connection Summary Events）] チェックボックスをオンにして、データベースからすべての接続の概要データを削除します。
- [セキュリティ インテリジェンス イベント（Security Intelligence Events）] チェックボックスをオンにして、データベースからすべてのセキュリティ インテリジェンス データを削除します。

（注） [接続イベント（Connection Events）] チェックボックスをオンにしても、セキュリティ インテリジェンスイベントは削除されません。セキュリティインテリジェンスデータとの接続は、[セキュリティ インテリジェンス イベント（Security Intelligence Events）] ページに引き続き表示されます（[分析（Analysis）] > [接続（Connections）] メニューの下に表示）。同様に、[セキュリティ インテリジェンスイベント（Security Intelligence Events）] チェックボックスをオンにしても、セキュリティ インテリジェンス データに関連する接続イベントは削除されません。

ステップ 4 [選択したイベントの消去（Purge Selected Events）] をクリックします。
項目が消去され、該当するプロセスが再起動されます。

第 11 章

Firepower Management Center のハイ アベイラビリティ

以下のトピックでは、Cisco Firepower Management Center のアクティブ/スタンバイ ハイ アベイラビリティを設定する方法を示します。

Firepower Management Center のハイ アベイラビリティについて

運用の継続性を確保するために、ハイ アベイラビリティ機能を使用して、冗長 Firepower Management Center でデバイスを管理するように指定することができます。Firepower Management Center はアクティブ/スタンバイ ハイ アベイラビリティをサポートしています。つまり 1 台のアプライアンスがアクティブなユニットとなってデバイスを管理します。スタンバイユニットは、アクティブにデバイスを管理しません。アクティブユニットは、データ ストアに設定データを書き込み、両方のユニットのデータを複製し、必要な場合は同期を使用してスタンバイユニットと一部の情報を共有します。

アクティブ/スタンバイ ハイ アベイラビリティでは、プライマリ Firepower Management Center に障害が発生した場合、セカンダリ Firepower Management Center を設定して、プライマリの機能を引き継ぐことができます。プライマリ Firepower Management Center に障害が発生した場合は、セカンダリ Firepower Management Center をプロモートしてアクティブ ユニットにする必要があります。

イベント データは、管理対象デバイスからハイ アベイラビリティ ペアの両方の Firepower Management Center に配信されます。一方の Firepower Management Center で障害が発生した場合、他方の Firepower Management Center の使用を中断せずにネットワークをモニタすることができます。

ハイ アベイラビリティ ペアとして設定する 2 つの Firepower Management Center は、信頼された同じ管理ネットワーク上に存在する必要も、同じ地理的ロケーションに存在する必要もありません。

⚠

注意 システムでは一部の機能をアクティブ Firepower Management Center に制限しているため、そのアプライアンスで障害が発生した場合は、スタンバイ Firepower Management Center をアクティブにプロモートする必要があります。

リモート アクセス VPN のハイ アベイラビリティについて

プライマリ デバイスに、CertEnrollment オブジェクトを使用して登録された ID 証明書を使用したリモート アクセス VPN 設定がある場合、セカンダリ デバイスには、同じ CertEnrollment オブジェクトを使用して登録された ID 証明書が必要です。CertEnrollment オブジェクトは、デバイス固有のオーバーライドにより、プライマリ デバイスとセカンダリ デバイスに異なる値を持つことができます。この制限は、ハイ アベイラビリティの形成前に 2 つのデバイスに同じ CertEnrollment オブジェクトを登録することだけです。

Firepower Management Center 高可用性のシステム要件

この項では、ハイ アベイラビリティ設定にある Firepower Management Center のハードウェア要件、ソフトウェア要件、およびライセンス要件について説明します。

ハードウェア要件

- ハイ アベイラビリティ設定の 2 台の Firepower Management Center は、モデルが同じである必要があります。
- プライマリ Firepower Management Center バックアップをセカンダリ Firepower Management Center に復元することはできません。
- 帯域幅要件：2 つの Firepower Management Center の間にハイ アベイラビリティ構成を設定するには、それらの間に少なくとも 5 Mbps のネットワーク帯域幅が必要です。

ソフトウェア要件

[アプライアンス情報（Appliance Information）] ウィジェットにアクセスして、ソフトウェアバージョン、侵入ルールの更新バージョン、および脆弱性データベースの更新バージョンを確認します。デフォルトでは、[詳細ダッシュボード（Detailed Dashboard）] と [サマリーダッシュボード（Summary Dashboard）] の [ステータス（Status）] タブにウィジェットが表示されます。詳細については、[アプライアンス情報（Appliance Information）] ウィジェット （325 ページ）を参照してください。

- ハイ アベイラビリティ設定の 2 台の Firepower Management Center には、同じメジャー（最初の番号）、マイナー（2 番めの番号）、メンテナンス（3 番めの番号）バージョンのソフトウェアがインストールされている必要があります。
- ハイ アベイラビリティ構成内の 2 つの Firepower Management Center には、同じバージョンの侵入ルールの更新をインストールする必要があります。
- ハイ アベイラビリティ構成内の 2 つの Firepower Management Center には、同じバージョンの脆弱性データベースの更新をインストールする必要があります。

警告 両方の Firepower Management Center でソフトウェア バージョン、侵入ルールの更新バージョン、および脆弱性データベースの更新バージョンが同一でない場合は、ハイ アベイラビリティを確立できません。

ライセンス要件

すべてのライセンスタイプ

高可用性ペア内の Firepower Management Center アプライアンスに特別なライセンスは必要ありません。

高可用性設定の Firepower Management Center アプライアンスで管理されているデバイスには、1 つの Firepower Management Center で管理されているデバイスと同じ数の機能ライセンスとサブスクリプションが必要です。

特定ライセンス予約の展開では、プライマリ FMC のみが特定ライセンス予約を必要とします。

システムは、高可用性ペアが形成された時点でアクティブからスタンバイ Firepower Management Center にすべての機能ライセンスを複製し、実行中のデータ同期の間にライセンスの変更を更新します。そのため、ライセンスはフェールオーバー時に使用できます。

スマート ライセンス

例：Firepower Management Center ペアで管理されている 2 つの Firepower Threat Defense デバイスに対して高度なマルウェア防御を有効にしたい場合は、2 つのマルウェア ライセンスと 2 つの TM サブスクリプションを購入し、アクティブ Firepower Management Center を Cisco Smart Software Manager に登録してから、ライセンスをアクティブ Firepower Management Center 上の 2 つの Firepower Threat Defense デバイスに割り当てます。

アクティブな Firepower Management Center のみが Cisco Smart Software Manager に登録されます。フェールオーバーが実行されると、システムは Cisco Smart Software Manager と通信して、スマート ライセンスの付与資格を最初にアクティブだった Firepower Management Center から解放し、新たにアクティブになる Firepower Management Center に割り当てます。

従来のライセンス

例：Firepower Management Center ペアで管理されている 2 つの デバイスに対して高度なマルウェア防御を有効にしたい場合は、2 つのマルウェア ライセンスと 2 つの TAM サブスクリプションを購入し、それらのライセンスを Firepower Management Center に追加してから、ライセンスをアクティブ Firepower Management Center 上の 2 つの デバイスに割り当てます。

高可用性 Firepower Management Center での役割とステータス

プライマリ/セカンダリの役割

Firepower Management Center を高可用性ペアの形でセットアップする際は、一方の Firepower Management Center をプライマリとして設定し、もう一方をセカンダリとして設定します。設定中に、プライマリ ユニットのポリシーは、セカンダリ ユニットに同期されます。この同期が完了すると、プライマリ Firepower Management Center がアクティブ ピアになり、セカンダリ Firepower Management Center がスタンバイ ピアになって、2 つのユニットが管理対象デバイスおよびポリシー設定に対して単一のアプライアンスとして機能します。

アクティブ/スタンバイ ステータス

高可用性ペアを構成する 2 つの Firepower Management Center の間の主な違いは、どちらがアクティブ ピアで、どちらがスタンバイ ピアであるかという点です。アクティブ Firepower Management Center は、完全に機能する状態に維持され、デバイスとポリシーを管理するために使用できます。スタンバイ Firepower Management Center では機能が非表示になるため、設定の変更を行うことはできません。

Firepower Management Center のハイ アベイラビリティを確立するための前提条件

Firepower Management Center ハイ アベイラビリティ ペアを確立する前に、次の操作を行います。

- 必要なポリシーを、対象のセカンダリ Firepower Management Center から対象のプライマリ Firepower Management Center にエクスポートします。詳細については、設定のエクスポート （232 ページ）を参照してください。
- 対象のセカンダリ Firepower Management Center にデバイスが追加されていないことを確認します。対象のセカンダリ Firepower Management Center からデバイスを削除し、そのデバイスを対象のプライマリ Firepower Management Center に登録します。詳細については、Firepower Management Center からのデバイスの削除 （295 ページ） と Firepower Management Center へのデバイスの追加 （293 ページ） を参照してください。

- 対象のプライマリ Firepower Management Center にポリシーをインポートします。詳細については、設定のインポート （233 ページ）を参照してください。
- 対象のプライマリ Firepower Management Center で、インポートされたポリシーを確認して、必要に応じて編集し、適切なデバイスに展開します。詳細については、設定変更の展開 （447 ページ）を参照してください。
- 対象のプライマリ Firepower Management Center で、適切なライセンスを新しく追加したデバイスに関連付けます。詳細については、[デバイス管理（Device Management）]ページで管理対象デバイスにライセンスを割り当てる （154 ページ）を参照してください。
- なお、Cisco Security Packet Analyzer と統合のための対象のセカンダリ Firepower Management Center の既存設定は、同期が発生した場合は上書きされます。必要に応じて、対象のプライマリ Firepower Management Center でこのような設定を再作成します。

これで、ハイ アベイラビリティの確立に進むことができます。詳細については、「Firepower Management Center ハイ アベイラビリティの確立 （272 ページ）」を参照してください。

Firepower Management Center のハイ アベイラビリティ ペアでのイベント処理

ハイ アベイラビリティ ペアの両方の Firepower Management Center が管理対象デバイスからイベントを受信するため、アプライアンスの管理 IP アドレスは共有されません。これは Firepower Management Center で障害が発生した場合に、継続的な処理を確保するために介入する必要がないことを意味します。

AMP クラウド接続とマルウェア情報

ハイ アベイラビリティ ペアを構成する Firepower Management Center は、ファイル ポリシーおよび関連する設定は共有しますが、シスコ AMP クラウド接続およびマルウェア処理は共有しません。運用の継続性を確保し、検出されたファイルのマルウェア処理が両方の Firepower Management Center で同じであるようにするためには、プライマリとセカンダリ両方の Firepower Management Center が AMP クラウドにアクセスできる必要があります。

URL フィルタリングとセキュリティ インテリジェンス

URL フィルタリングとセキュリティ インテリジェンスの設定および情報は、ハイ アベイラビリティ展開の Firepower Management Center の間で同期されます。ただし、プライマリ Firepower Management Center だけが、セキュリティ インテリジェンス フィードの更新用の URL カテゴリおよびレピュテーション データをダウンロードします。

プライマリ Firepower Management Center に障害が発生した場合は、セカンダリ Firepower Management Center がインターネットにアクセスして脅威インテリジェンスを更新できることを確認する必要があるだけでなく、セカンダリ Firepower Management Center の Web インターフェイスを使用してセカンダリをアクティブにプロモートする必要もあります。

Firepower Management Center のフェールオーバー中のユーザ データの処理

プライマリ Firepower Management Center で障害が発生した場合、ユーザ エージェント、ISE/ISE-PIC、TS エージェント、またはキャプティブ ポータル デバイスから報告されるすべてのログインは、それらのユーザが前に確認されて Firepower Management Center にダウンロードされていた場合でも、フェールオーバーのダウンタイム中に識別することはできません。識別されていないユーザは、Firepower Management Center で [不明（Unknown）] のユーザとして記録されます。

ダウンタイム後、不明のユーザはアイデンティティ ポリシーのルールに従って再確認され、処理されます。

Firepower Management Center ハイ アベイラビリティ ペアの構成管理

ハイ アベイラビリティ展開では、アクティブな Firepower Management Center のみがデバイスを管理し、ポリシーを適用できます。両方の Firepower Management Center は継続的な同期状態を保ちます。

アクティブ状態の Firepower Management Center に障害が発生すると、ハイ アベイラビリティ ペアは縮退状態となります。縮退状態は、スタンバイ状態のアプライアンスを手動でアクティブ状態に上げるまで続きます。スタンバイ状態のアプライアンスをアクティブ状態に上げると、両アプライアンスのメンテナンス モードが終了します。

Cisco Threat Intelligence Director（TID） およびハイ アベイラビリティ構成

ハイ アベイラビリティ構成のアクティブな Firepower Management Center で TID をホスティングする場合、システムは TID 構成と TID データをスタンバイ Firepower Management Center に同期しません。フェールオーバー後にデータを復元できるように、アクティブ Firepower Management Center で TID データの定期的なバックアップを実行することを推奨します。

詳細については、「TID データのバックアップおよび復元について（1982 ページ）」を参照してください。

バックアップ中の Firepower Management Center の高可用性動作

Firepower Management Center 高可用性ペアでバックアップを実行する場合、バックアップ動作によってピア間の同期が一時停止します。この動作中は、引き続きアクティブな Firepower Management Center を使用できますが、スタンバイ ピアを使用することはできません。

バックアップが完了すると、同期が再開され、少しの間、アクティブ ピアでのプロセスが無効になります。この一時停止中、[高可用性（High Availability）] ページには、すべてのプロセスが再開されるまでは一時的に保留ページが表示されます。

Firepower Management Center ハイ アベイラビリティのスプリットブレイン

高可用性ペアのアクティブな Firepower Management Center が（電源の問題、ネットワークや接続の問題で）ダウンした場合は、スタンバイ Firepower Management Center をアクティブ状態に昇格させることができます。元のアクティブなピアが起動すると、両方のピアがアクティブであるとみなされる場合があります。この状態は「スプリットブレイン」と定義されます。このような状況が発生すると、システムによってアクティブなアプライアンスを選択するように要求されます。それによって、もう一方のアプライアンスはスタンバイ状態に降格します。

アクティブな Firepower Management Center がダウンした（またはネットワーク障害により切断された）場合は、高可用性を中断するか、またはロールを切り替えることができます。スタンバイ Firepower Management Center は縮退状態になります。

（注） セカンダリとして使用するアプライアンスがどれであっても、スプリットブレインの解決時にデバイス登録とポリシー設定のすべてが失われます。たとえば、セカンダリに存在し、プライマリには存在しなかったポリシーへの変更は失われます。Firepower Management Center が両方のアプライアンスがアクティブな高可用スプリットブレイン シナリオである場合に、スプリットブレインを解決する前に管理対象デバイスを登録してポリシーを展開する場合は、ハイ アベイラビリティを再確立する前に、ポリシーをエクスポートして、管理対象デバイスを対象のスタンバイ Firepower Management Center から登録解除する必要があります。その後、管理対象デバイスを登録し、目的のアクティブ Firepower Management Center にポリシーをインポートすることができます。

ハイ アベイラビリティ ペアでの Firepower Management Center のアップグレード

Cisco は、各種の更新プログラムを電子形式で定期的に配信します。更新プログラムには、システム ソフトウェアのメジャーおよびマイナー アップグレードが含まれます。ハイ アベイラビリティ セットアップでは、これらの更新を両方の Firepower Management Center にインストールする必要が生じることがあります。

警告 アップグレード中には、少なくとも 1 つの Firepower Management Center を動作状態に維持してください。

始める前に

アップグレードに付属しているリリース ノートまたはアドバイザリ テキストを読んでください。リリース ノートでは、サポートされるプラットフォーム、互換性、前提条件、警告、特定のインストールおよびアンインストールの手順など重要なデータが提供されます。

ステップ 1 アクティブ Firepower Management Center の Web インターフェイスにアクセスし、データ同期を一時停止します（Firepower Management Center ペア間の通信の一時停止 （278 ページ）を参照）。

ステップ 2 スタンバイ Firepower Management Center をアップグレードします（Firepower Management Center でのソフトウェアの更新を参照）。
アップグレードが完了すると、スタンバイ ユニットがアクティブになります。両方のピアがアクティブになると、ハイ アベイラビリティ ペアが劣化状態 (スプリットブレイン) になります。

ステップ 3 もう一方の Firepower Management Center をアップグレードします。

ステップ 4 どちらの Firepower Management Center をスタンバイとして使用するかを決定します。同期を一時停止した後にスタンバイに追加された追加のデバイスまたはポリシーは、アクティブ Firepower Management Center に同期されません。その追加のデバイスのみを登録解除し、維持する必要がある設定をエクスポートします。

新しいアクティブ Firepower Management Center を選択すると、セカンダリとして指定した Firepower Management Center は、同期されていないデバイス登録と展開されたポリシー設定を失います。

ステップ 5 最新のポリシーとデバイスに必要なすべての設定を含む新しいアクティブ Firepower Management Center を選択して、スプリットブレインを解決します。

Firepower Management Center のハイアベイラビリティのトラブルシューティング

この項では、Firepower Management Center のハイ アベイラビリティ操作のいくつかの一般的なエラーに関するトラブルシューティング情報を示します。

エラー（Error）	説明	ソリューション
500 内部（500 Internal）	ピア ロールの切り替えや同期の一時停止と再開などのクリティカルな Firepower Management Center のハイアベイラビリティ操作を実行しているときに Web インターフェイスにアクセスしようとすると表示されることがあります。	Web インターフェイスを使用する前に、操作が完了するまでお待ちください。

エラー（Error）	説明	ソリューション
システム プロセスが起動しています、お待ちください（System processes are starting, please wait） また、Web インターフェイスは応答しません。（Also, the web interface does not respond.）	ハイ アベイラビリティまたはデータ同期操作中に Firepower Management Center が再起動（手動でまたは電源切断からの回復中に）する場合に表示されることがあります。	1. Firepower Management Center シェルにアクセスし、`manage_hadc.pl` コマンドを使用して Firepower Management Center のハイ アベイラビリティ構成ユーティリティにアクセスします。 （注） `sudo` を使用して、ルート ユーザとしてユーティリティを実行します。 2. オプション 5 を使用してミラーリング操作を一時停止します。 Firepower Management Center Web インターフェイスをリロードします。 3. Web インターフェイスを使用して同期を再開します。[システム（System）] > [統合（Integration）] の順に選択し、[ハイ アベイラビリティ（High Availability）] タブをクリックして、[同期の再開（Resume Synchronization）] を選択します。

Firepower Management Center ハイ アベイラビリティの確立

スマート ライセンス	従来のライセンス	サポートされている Management Center	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	MC1000、MC1500、MC1600、MC2000、MC2500、MC2600、MC3500、MC4000、MC4500、MC4600	グローバル	Admin

高可用性を確立するには、ピア間の帯域幅とポリシーの数に応じてかなりの時間がかかり、数時間かかることもあります。また、スタンバイ状態の Firepower Management Center と同期される必要のある、アクティブ Firepower Management Center に登録されたデバイスの数によっても異なります。[ハイ アベイラビリティ（High Availability）] ページを表示すると、ハイ アベイラビリティ ピアのステータスを確認できます。

始める前に

- 両方の Firepower Management Center がハイ アベイラビリティ システム要件を満足していることを確認します。詳細については、Firepower Management Center 高可用性のシステム要件 （264 ページ）を参照してください。
- ハイ アベイラビリティを確立するための前提条件を満足していることを確認します。詳細については、Firepower Management Center のハイ アベイラビリティを確立するための前提条件 （266 ページ）を参照してください。

ステップ 1 セカンダリとして指定する Firepower Management Center にログインします。

ステップ 2 **[System]** > **[Integration]**を選択します。

ステップ 3 [ハイ アベイラビリティ（High Availability）] を選択します。

ステップ 4 この Firepower Management Center の権限で、[セカンダリ（Secondary）] を選択します。

ステップ 5 [プライマリ Firepower Management Center ホスト（Primary Firepower Management Center Host）] テキストボックスに、プライマリ Firepower Management Center のホスト名または IP アドレスを入力します。

ルーティング可能なアドレスがプライマリ Firepower Management Center に設定されていない場合は、空白のままにしても構いません。この場合は、[登録キー（Registration Key）] と [一意の NAT ID（Unique

NAT ID）] の両方のフィールドを使用します。プライマリ ユニットでセカンダリ IP アドレスを指定する必要もあります。少なくとも 1 つのユニットの IP アドレスを指定する必要があります。

ステップ 6 [登録キー（Registration Key）] テキストボックスに、1 回限り使用する登録キーを入力します。

登録キーは、ユーザ定義の最大 37 文字の英数字値です。この登録キーはセカンダリおよびプライマリ Firepower Management Center の登録に使用されます。

ステップ 7 プライマリ IP アドレスを指定しなかった場合、またはプライマリ Firepower Management Center でセカンダリ IP アドレスを指定しない場合は、[一意の NAT ID（Unique NAT ID）] フィールドに一意の英数字 ID を入力します。詳細については、NAT 環境 （289 ページ）を参照してください。

ステップ 8 [Register] をクリックします。

ステップ 9 管理者アクセス権限を持つアカウントを使用して、プライマリとして指定する Firepower Management Center にログインします。

ステップ 10 **[System]** > **[Integration]**を選択します。

ステップ 11 [ハイ アベイラビリティ（High Availability）] を選択します。

ステップ 12 この Firepower Management Center の権限で、[プライマリ（Primary）] を選択します。

ステップ 13 [セカンダリ Firepower Management Center ホスト（Secondary Firepower Management Center Host）] テキストボックスに、セカンダリ Firepower Management Center のホスト名または IP アドレスを入力します。

ルーティング可能なアドレスがセカンダリ Firepower Management Center に設定されていない場合は、空白のままにしても構いません。この場合は、[登録キー（Registration Key）] と [一意の NAT ID（Unique NAT ID）] の両方のフィールドを使用します。セカンダリ ユニットでプライマリ IP アドレスを指定する必要もあります。少なくとも 1 つのユニットの IP アドレスを指定する必要があります。

ステップ 14 [登録キー（Registration Key）] テキストボックスに、ステップ 6 で入力した 1 回限り使用する登録キーと同じものを入力します。

ステップ 15 必要に応じて、[一意の NAT ID（Unique NAT ID）] テキスト ボックスに手順 7 で使用したのと同じ NAT ID を入力します。

ステップ 16 [登録（Register）] をクリックします。

次のタスク

Firepower Management Center ハイ アベイラビリティ ペアを確立すると、アクティブ Firepower Management Center に登録されたデバイスが自動的にスタンバイ Firepower Management Center に登録されます。

（注） 登録済みのデバイスに NAT IP アドレスが割り当てられている場合、デバイスの自動登録は失敗し、セカンダリ Firepower Management Center の [ハイ アベイラビリティ（High Availability）] ページには、そのデバイスがローカルで保留中であると表示されます。次に、スタンバイ Firepower Management Center の [ハイ アベイラビリティ（High Availability）] ページで、異なる NAT IP アドレスをデバイスに割り当てることができます。自動登録がスタンバイ Firepower Management Center で失敗しても、デバイスがアクティブな Firepower Management Center に登録されているように見える場合は、Firepower Management Center のハイ アベイラビリティにおけるデバイス登録を解決するための CLI の使用 （276 ページ） を参照してください。

Firepower Management Center ハイ アベイラビリティ ステータスの表示

スマート ライセンス	従来のライセンス	サポートされている Management Center	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	MC1000、MC1500、MC1600、MC2000、MC2500、MC2600、MC3500、MC4000、MC4500、MC4600	グローバル	Admin

アクティブおよびスタンバイ Firepower Management Center を識別した後、ローカル Firepower Management Center とそのピアに関する情報を表示できます。

（注） このコンテキストでは、ローカル ピアは、システム ステータスを表示するアプライアンスを参照します。リモート ピアは、アクティブ ステータスかスタンバイ ステータスかに関係なく、その他のアプライアンスを参照します。

ステップ 1 高可用性を使用してペアにした Firepower Management Center のいずれかにログインします。

ステップ 2 **[System]** > **[Integration]** を選択します。

ステップ 3 [ハイ アベイラビリティ（High Availability）] を選択します。

次の情報を表示できます。

サマリー情報

- ハイ アベイラビリティ ペアのヘルス ステータス
- ハイ アベイラビリティ ペアの現在の同期ステータス
- アクティブ ピアの IP アドレスと最後に同期された時間
- スタンバイ ピアの IP アドレスと最後に同期された時間

システム ステータス

- 両方のピアの IP アドレス
- 両方のピアのオペレーティング システム
- 両方のピアのソフトウェア バージョン
- 両方のピアのアプライアンス モデル

Firepower Management Center ハイ アベイラビリティ ペアで同期される設定

2 つの Firepower Management Center の間でハイ アベイラビリティを確立すると、次の設定データが同期されます。

- ライセンスの付与資格
- アクセス コントロール ポリシー
- 侵入ルール
- マルウェアおよびファイル ポリシー
- DNS ポリシー
- アイデンティティ ポリシー
- SSL ポリシー
- プレフィルタ ポリシー
- ネットワーク検出ルール
- アプリケーション ディテクタ
- 相関ポリシー ルール
- アラート（Alerts）
- スキャナ（Scanners）

- 応答グループ
- イベントを調査するための外部リソースのコンテキスト クロス起動
- Cisco Security Packet Analyzer との統合
- 修復設定。ただし、両方の Firepower Management Center にカスタム モジュールをインストールする必要があります。修復設定の詳細については、修復モジュールの管理（2768ページ） を参照してください。

Firepower Management Center のハイ アベイラビリティにおけるデバイス登録を解決するための CLI の使用

スマート ライセンス	従来のライセンス	サポートされている Management Center	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	MC1000、MC1500、MC1600、MC2000、MC2500、MC2600、MC3500、MC4000、MC4500、MC4600	グローバル	Admin

自動デバイス登録がスタンバイ Firepower Management Center で失敗したものの、アクティブ Firepower Management Center に登録されたと表示される場合、次の手順を実行します。

ステップ 1 アクティブ Firepower Management Center からデバイスの登録を解除します。

ステップ 2 影響受けるデバイスの CLI にログインします。

ステップ 3 CLI コマンド `configure manager delete` を実行します。
このコマンドは、現在の Firepower Management Center を無効にして削除します。

ステップ 4 CLI コマンド `configure manager add` を実行します。
このコマンドは、デバイスを設定して Firepower Management Center への接続を開始します。

ヒント デバイスのリモート管理を、アクティブな Firepower Management Center の場合のみ設定します。ハイ アベイラビリティを確立すると、デバイスは自動的に追加され、スタンバイ Firepower Management Center によって管理されます。

ステップ 5 アクティブ Firepower Management Center にログインし、デバイスを登録します。

Firepower Management Center ハイ アベイラビリティ ペアにおけるピアの切り替え

スマート ライセンス	従来のライセンス	サポートされている Management Center	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	MC1000、MC1500、MC1600、MC2000、MC2500、MC2600、MC3500、MC4000、MC4500、MC4600	グローバル	Admin

システムでは一部の機能をアクティブ Firepower Management Center に制限しているため、そのアプライアンスで障害が発生した場合は、スタンバイ Firepower Management Center をアクティブ ステータスにプロモートする必要があります。

ステップ 1 高可用性を使用してペアにした Firepower Management Center のいずれかにログインします。

ステップ 2 **[System]** > **[Integration]**を選択します。

ステップ 3 [ハイ アベイラビリティ（High Availability）] を選択します。

ステップ 4 [ピア ロールの切り替え（Switch Peer Roles）] を選択して、ローカル ロールをアクティブからスタンバイ、またはスタンバイからアクティブに変更します。プライマリまたはセカンダリの指定は変更されずに、2 つのピア間でロールが切り替わります。

Firepower Management Center ペア間の通信の一時停止

スマート ライセンス	従来のライセンス	サポートされている **Management Center**	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	MC1000、MC1500、MC1600、MC2000、MC2500、MC2600、MC3500、MC4000、MC4500、MC4600	グローバル	Admin

一時的に高可用性を無効にする場合は、Firepower Management Center 間の通信チャネルを無効にすることができます。アクティブ ピアの同期を一時停止した場合は、スタンバイ ピアまたはアクティブ ピアのいずれでも同期を再開できます。ただし、スタンバイ ピアで同期を一時停止した場合、同期の再開はスタンバイ ピアでのみ可能になります。

ステップ 1 高可用性を使用してペアにした Firepower Management Center のいずれかにログインします。

ステップ 2 **[System]** > **[Integration]**を選択します。

ステップ 3 [ハイ アベイラビリティ（High Availability）] を選択します。

ステップ 4 [同期の一時停止（Pause Synchronization）] を選択します。

Firepower Management Center ペア間の通信の再開

スマート ライセンス	従来のライセンス	サポートされている Management Center	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	MC1000、MC1500、MC1600、MC2000、MC2500、MC2600、MC3500、MC4000、MC4500、MC4600	グローバル	Admin

一時的に高可用性を無効にしている場合は、Firepower Management Center 間の通信チャネルを有効にすることで、高可用性を再開することができます。アクティブ ユニットで同期を一時停止した場合、スタンバイ ユニットまたはアクティブ ユニットのいずれでも同期を再開できます。ただし、スタンバイ ユニットで同期を一時停止した場合、同期の再開はスタンバイ ユニットでのみ可能になります。

ステップ 1 高可用性を使用してペアにした Firepower Management Center のいずれかにログインします。

ステップ 2 **[System]** > **[Integration]**を選択します。

ステップ 3 [ハイ アベイラビリティ（High Availability）] を選択します。

ステップ 4 [同期の再開（Resume Synchronization）] を選択します。

高可用性ペアの Firepower Management Center の IP アドレスの変更

スマート ライセンス	従来のライセンス	サポートされている Management Center	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	MC1000、MC1500、MC1600、MC2000、MC2500、MC2600、MC3500、MC4000、MC4500、MC4600	グローバル	Admin

（注） 7000 および 8000 シリーズ 管理対象デバイスのリモート管理を編集しているときに、このトピックにたどり着いた場合は、管理対象デバイスでのリモート管理の編集（653 ページ）を参照してください。

高可用性ピアのいずれかの IP アドレスを変更すると、高可用性が低下した状態になります。高可用性を回復するには、手動で IP アドレスを変更する必要があります。

ステップ 1 高可用性を使用してペアにした Firepower Management Center のいずれかにログインします。

ステップ 2 **[System]** > **[Integration]**を選択します。

ステップ 3 [ハイ アベイラビリティ（High Availability）] を選択します。

ステップ 4 [ピア マネージャ（Peer Manager）] を選択します。

ステップ 5 編集アイコン（ ）を選択します。

ステップ 6 アプライアンスの表示名を入力します。この表示名は、Firepower システムのコンテキストでのみ使用されます。

別の表示名を入力しても、アプライアンスのホスト名は変更されません。

ステップ 7 完全修飾ドメイン名を入力するか、ローカル DNS で有効な IP アドレス（ホスト名）に解決される名前、またはホストの IP アドレスを入力します。

ステップ 8 **[保存（Save）]** を選択します。

Firepower Management Center ハイ アベイラビリティの無効化

スマート ライセンス	従来のライセンス	サポートされている Management Center	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	MC1000、MC1500、MC1600、MC2000、MC2500、MC2600、MC3500、MC4000、MC4500、MC4600	グローバル	Admin

ステップ 1 ハイ アベイラビリティ ペアのいずれか一方の Firepower Management Center にログインします。

ステップ 2 **[System]** > **[Integration]**を選択します。

ステップ 3 [ハイ アベイラビリティ（High Availability）] を選択します。

ステップ 4 [ハイ アベイラビリティの解消（Break High Availability）] を選択します。

ステップ 5 管理対象デバイスを処理するための以下のいずれかのオプションを選択します。

- この Firepower Management Center を使用してすべての管理対象デバイスを制御する場合には、[このコンソールから登録済みデバイスを管理（Manage registered devices from this console）] を選択します。すべてのデバイスがピアから登録解除されます。
- 他の Firepower Management Center を使用してすべての管理対象デバイスを制御する場合には、[ピアコンソールから登録済みデバイスを管理（Manage registered devices from peer console）] を選択します。すべてのデバイスがこの Firepower Management Center から登録解除されます。
- デバイスの管理をまとめて停止する場合には、[両方のコンソールからの登録済みデバイスの管理を停止（Stop managing registered devices from both consoles）] を選択します。すべてのデバイスが両方の Firepower Management Center から登録解除されます。

（注） セカンダリ Firepower Management Center から登録済みデバイスを管理する場合、そのデバイスはプライマリ Firepower Management Center から登録解除されます。そのデバイスは、セカンダリ Firepower Management Center によって管理されるように登録されます。ただし、そのデバイスに適用されていたライセンスは、ハイ アベイラビリティの中断操作のために登録解除されます。次に、セカンダリ Firepower Management Center からデバイス上でライセンスを再登録（有効化）する必要があります。詳細については、管理対象デバイスからのスマート ライセンスの移動または削除 （138 ページ）を参照してください。

ステップ 6 [OK] をクリックします。

ハイアベイラビリティペアでの FMC の交換

Firepower Management Center ハイ アベイラビリティ ペアで障害が発生したユニットを交換する必要がある場合は、次に示すいずれかの手順に従う必要があります。次の表に、4 つの障害シナリオとそれに対応する交換手順を示します。

障害ステータス	データ バックアップ ステータス	交換手順
プライマリ FMC の障害	データ バックアップが成功	障害が発生したプライマリ FMC の交換（バックアップが成功） （282 ページ）
	データ バックアップが失敗	障害が発生したプライマリ FMC の交換（バックアップが失敗） （283 ページ）
セカンダリ FMC の障害	データ バックアップが成功	障害が発生したセカンダリ FMC の交換（バックアップが成功） （285 ページ）
	データ バックアップが失敗	障害が発生したセカンダリ FMC の交換（バックアップが失敗） （285 ページ）

障害が発生したプライマリ FMC の交換（バックアップが成功）

2 つの Firepower Management Center（FMC1 と FMC2）がハイ アベイラビリティ ペアを構成しています。FMC1 がプライマリ、FMC2 がセカンダリです。このタスクでは、プライマリからのデータ バックアップが成功した場合に、障害が発生したプライマリ Firepower Management Center（FMC1）を交換する手順を説明します。

始める前に

障害が発生したプライマリ Firepower Management Center からのデータ バックアップが成功したことを確認します。

ステップ 1 サポートに連絡して、障害が発生した Firepower Management Center（FMC1）の交換を要請します。

ステップ 2 プライマリ Firepower Management Center（FMC1）で障害が発生した場合は、セカンダリ Firepower Management Center（FMC2）の Web インターフェイスにアクセスしてピアを切り替えます。詳細については、Firepower Management Center ハイ アベイラビリティ ペアにおけるピアの切り替え （277 ページ）を参照してください。

これにより、セカンダリ Firepower Management Center（FMC2）がアクティブに昇格します。

プライマリ Firepower Management Center（FMC1）の交換が完了するまで、FMC2 をアクティブ Firepower Management Center として使用できます。

警告　Firepower Management Center ハイアベイラビリティを FMC2 から分断しないでください。分断すると、（障害前に）FMC1 から FMC2 に同期されていたライセンスが FMC2 から削除されるため、FMC2 から展開アクションを実行できなくなります。

ステップ 3 FMC1 と同じソフトウェア バージョンを使用して交換用 Firepower Management Center を再イメージ化します。

ステップ 4 FMC1 から取得したデータ バックアップを新しい Firepower Management Center に復元します。

ステップ 5 FMC2 と適合するのに必要な Firepower Management Center パッチ、地理位置情報データベース（GeoDB）更新、脆弱性データベース（VDB）更新、システム ソフトウェア更新をインストールします。

これで、新しい Firepower Management Center と FMC2 の両方がアクティブ ピアとなるため、ハイ アベイラビリティがスプリットブレイン状態になります。

ステップ 6 Firepower Management Center Web インターフェイスからアクティブ アプライアンスを選択するよう求めるプロンプトが出されたら、FMC2 をアクティブとして選択します。

これにより、FMC2 の最新の設定が新しい Firepower Management Center（FMC1）に同期されます。

ステップ 7 設定が正常に同期されたら、セカンダリ Firepower Management Center（FMC2）の Web インターフェイスにアクセスし、役割を切り替えてプライマリ Firepower Management Center（FMC1）をアクティブにします。詳細については、Firepower Management Center ハイ アベイラビリティ ペアにおけるピアの切り替え （277 ページ）を参照してください。

ステップ 8 新しい Firepower Management Center（FMC1）で受け取った従来のライセンスを適用し、古いライセンスを削除します。詳細については、クラシック ライセンスの生成と Firepower Management Center への追加 （151 ページ）を参照してください。

スマート ライセンスはシームレスに機能します。

次のタスク

これで、ハイ アベイラビリティが再確立されたため、プライマリおよびセカンダリ Firepower Management Center が正常に動作するようになります。

障害が発生したプライマリ FMC の交換（バックアップが失敗）

2 つの Firepower Management Center（FMC1 と FMC2）がハイ アベイラビリティ ペアを構成しています。FMC1 がプライマリ、FMC2 がセカンダリです。このタスクでは、プライマリからのデータ バックアップが失敗した場合に、障害が発生したプライマリ Firepower Management Center（FMC1）を交換する手順を説明します。

ステップ 1 サポートに連絡して、障害が発生した Firepower Management Center（FMC1）の交換を要請します。

ステップ 2 プライマリ Firepower Management Center（FMC1）で障害が発生した場合は、セカンダリ Firepower Management Center（FMC2）の Web インターフェイスにアクセスしてピアを切り替えます。詳細については、Firepower Management Center ハイ アベイラビリティ ペアにおけるピアの切り替え （277 ページ）を参照してください。

これにより、セカンダリ Firepower Management Center（FMC2）がアクティブに昇格します。

プライマリ Firepower Management Center（FMC1）の交換が完了するまで、FMC2 をアクティブ Firepower Management Center として使用できます。

警告 Firepower Management Center ハイ アベイラビリティを FMC2 から分断しないでください。分断すると、（障害前に）FMC1 から FMC2 に同期されていた従来のライセンスとスマート ライセンスが FMC2 から削除されるため、FMC2 から展開アクションを実行できなくなります。

ステップ 3 FMC1 と同じソフトウェア バージョンを使用して交換用 Firepower Management Center を再イメージ化します。

ステップ 4 FMC2 と適合するのに必要な Firepower Management Center パッチ、地理位置情報データベース（GeoDB）更新、脆弱性データベース（VDB）更新、システム ソフトウェア更新をインストールします。

ステップ 5 Firepower Management Center（FMC2）を Cisco Smart Software Manager から登録解除します。詳細については、Cisco Smart Software Manager から Firepower Management Center の登録解除 （140 ページ）を参照してください。

Cisco Smart Software Manager から Firepower Management Center の登録を解除すると、バーチャル アカウントから Management Center が削除されます。Firepower Management Center リリースに関連付けられているライセンス権限はすべて、ご使用のバーチャル アカウントに戻ります。登録解除後、Firepower Management Center は適用モードになり、ライセンスが適用される機能に対する更新および変更が許可されなくなります。

ステップ 6 セカンダリ Firepower Management Center（FMC2）の Web インターフェイスにアクセスして、Firepower Management Center ハイ アベイラビリティを分断します。詳細については、Firepower Management Center ハイ アベイラビリティの無効化 （281 ページ）を参照してください。管理対象デバイスを処理する方法を選択するよう求められたら、[このコンソールから登録済みデバイスを管理（Manage registered devices from this console）] を選択します。

これにより、セカンダリ Firepower Management Center（FMC2）に同期されていた従来のライセンスとスマート ライセンスが削除されるため、FMC2 から展開アクティビティを実行できなくなります。

ステップ 7 Firepower Management Center ハイ アベイラビリティを再確立するために、Firepower Management Center（FMC2）をプライマリ、Firepower Management Center（FMC1）をセカンダリとして設定します。詳細については、Firepower Management Center ハイ アベイラビリティの確立 （272 ページ）を参照してください。

ステップ 8 新しい Firepower Management Center（FMC1）で受け取った従来のライセンスを適用し、古いライセンスを削除します。詳細については、クラシック ライセンスの生成と Firepower Management Center への追加 （151 ページ）を参照してください。

ステップ 9 スマート ライセンスをプライマリ Firepower Management Center（FMC2）に登録します。詳細については、スマート ライセンスの登録 （113 ページ）を参照してください。

次のタスク

これで、ハイ アベイラビリティが再確立されたため、プライマリおよびセカンダリ Firepower Management Center が正常に動作するようになります。

障害が発生したセカンダリ FMC の交換（バックアップが成功）

2 つの Firepower Management Center（FMC1 と FMC2）がハイ アベイラビリティ ペアを構成しています。FMC1 がプライマリ、FMC2 がセカンダリです。このタスクでは、セカンダリからのデータ バックアップが成功した場合に、障害が発生したセカンダリ Firepower Management Center（FMC2）を交換する手順を説明します。

始める前に

障害が発生したセカンダリ Firepower Management Center からのデータ バックアップが成功したことを確認します。

ステップ 1 サポートに連絡して、障害が発生した Firepower Management Center（FMC2）の交換を要請します。

ステップ 2 引き続きプライマリ Firepower Management Center（FMC1）をアクティブ Firepower Management Center として使用します。

ステップ 3 FMC2 と同じソフトウェア バージョンを使用して交換用 Firepower Management Center を再イメージ化します。

ステップ 4 FMC2 から取得したデータ バックアップを新しい Firepower Management Center に復元します。

ステップ 5 FMC1 と適合するのに必要な Firepower Management Center パッチ、地理位置情報データベース（GeoDB）更新、脆弱性データベース（VDB）更新、システム ソフトウェア更新をインストールします。

ステップ 6 新しい Firepower Management Center（FMC2）の Web インターフェイスからデータ同期を再開して（停止されていた場合）、プライマリ Firepower Management Center（FMC1）の最新の設定を同期させます。詳細については、Firepower Management Center ペア間の通信の再開 （279 ページ）を参照してください。

従来のライセンスとスマート ライセンスはシームレスに機能します。

次のタスク

これで、ハイ アベイラビリティが再確立されたため、プライマリおよびセカンダリ Firepower Management Center が正常に動作するようになります。

障害が発生したセカンダリ FMC の交換（バックアップが失敗）

2 つの Firepower Management Center（FMC1 と FMC2）がハイ アベイラビリティ ペアを構成しています。FMC1 がプライマリ、FMC2 がセカンダリです。このタスクでは、セカンダリからのデータ バックアップが失敗した場合に、障害が発生したセカンダリ Firepower Management Center（FMC2）を交換する手順を説明します。

ステップ 1 サポートに連絡して、障害が発生した Firepower Management Center（FMC2）の交換を要請します。

ステップ 2 引き続きプライマリ Firepower Management Center（FMC1）をアクティブ Firepower Management Center として使用します。

ステップ 3 FMC2 と同じソフトウェア バージョンを使用して交換用 Firepower Management Center を再イメージ化します。

ステップ 4 FMC1 と適合するのに必要な Firepower Management Center パッチ、地理位置情報データベース（GeoDB）更新、脆弱性データベース（VDB）更新、システム ソフトウェア更新をインストールします。

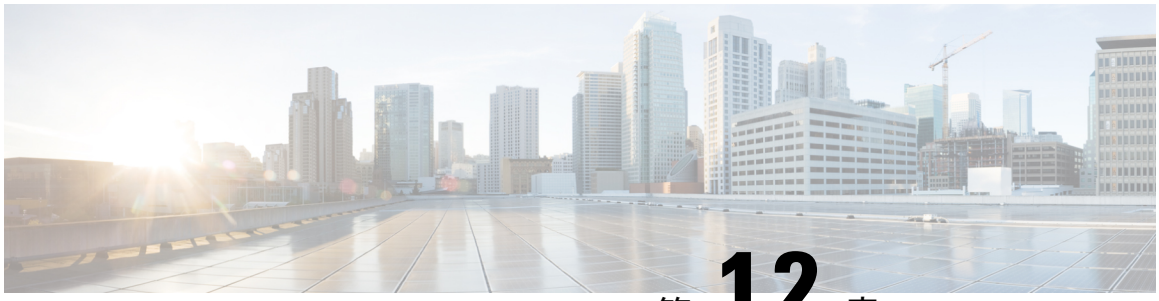
ステップ 5 プライマリ Firepower Management Center（FMC1）の Web インターフェイスにアクセスして、Firepower Management Center ハイ アベイラビリティを分断します。詳細については、Firepower Management Center ハイ アベイラビリティの無効化 （281 ページ）を参照してください。管理対象デバイスを処理する方法を選択するよう求められたら、[このコンソールから登録済みデバイスを管理（Manage registered devices from this console）] を選択します。

ステップ 6 Firepower Management Center ハイ アベイラビリティを再確立するために、Firepower Management Center（FMC1）をプライマリ、Firepower Management Center（FMC2）をセカンダリとして設定します。詳細については、Firepower Management Center ハイ アベイラビリティの確立 （272 ページ）を参照してください。

- ハイ アベイラビリティが正常に確立されると、プライマリ Firepower Management Center（FMC1）の最新の設定がセカンダリ Firepower Management Center（FMC2）に同期されます。
- 従来のライセンスとスマート ライセンスはシームレスに機能します。

次のタスク

これで、ハイ アベイラビリティが再確立されたため、プライマリおよびセカンダリ Firepower Management Center が正常に動作するようになります。



第 12 章

デバイス管理の基本

次のトピックでは、Firepower システムでデバイスを管理する方法について説明します。

デバイス管理について

Firepower Management Center を使用してデバイスを管理します。

Firepower Management Center について

Firepower Management Center を使用して、Firepower システムを構成するすべてのデバイスを管理できます。デバイスを管理するには、Firepower Management Center とデバイスの間に、双方向の SSL 暗号化通信チャネルをセットアップします。Firepower Management Center はこのチャネルを使用して、そのデバイスへのネットワーク トラフィックの分析および管理の方法に関する情報をそのデバイスに送信します。そのデバイスはトラフィックを評価すると、イベントを生成し、同じチャネルを使用してそれらのイベントを Firepower Management Center に送信します。

Firepower Management Center を使用してデバイスを管理すると、以下の利点があります。

- すべてのデバイスのポリシーを一箇所から設定できるため、設定の変更が容易になります。
- さまざまなタイプのソフトウェア アップデートをデバイスにインストールできます。

- ヘルス ポリシーを管理対象デバイスに適用して、Firepower Management Centerからデバイスのヘルス ステータスを監視できます。

Firepower Management Center は、侵入イベント、ネットワーク検出情報、およびデバイスのパフォーマンスデータを集約して相互に関連付けます。そのため、ユーザはデバイスが相互の関連でレポートする情報をモニタして、ネットワーク上で行われている全体的なアクティビティを評価することができます。

Firepower Management Center を使用することで、デバイス動作のほぼすべての側面を管理できます。

（注） Firepower Management Center は、http://www.cisco.com/c/en/us/support/security/defense-center/products-device-support-tables-list.html で使用可能な互換性マトリックスで指定されている特定の以前のリリースを実行しているデバイスを管理できますが、これらの以前のリリースのデバイスでは新しい機能は利用できません。

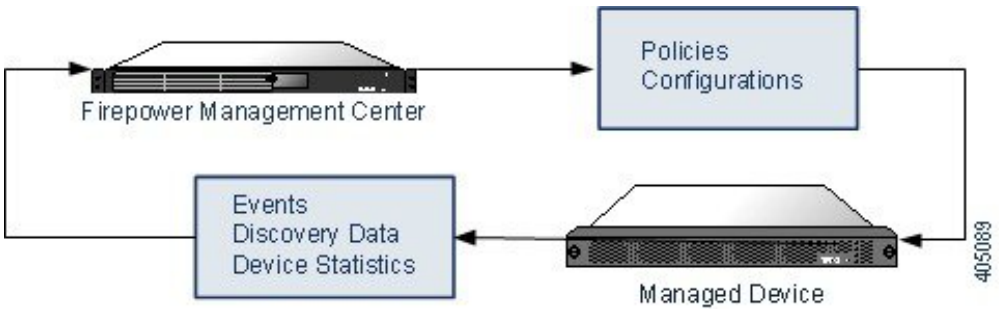
Firepower Management Center で管理できるデバイス

Firepower Management Center を Firepower システムの展開環境における中央の管理ポイントとして使用して、次の各デバイスを管理することができます。

- 7000 および 8000 シリーズ デバイス
- ASA FirePOWER モジュール
- NGIPSv デバイス
- Firepower Threat Defense（物理ハードウェアと仮想）

デバイスを管理する際の情報は、SSL で暗号化されたセキュアな TCP トンネルを介して、Firepower Management Center とデバイスの間で送信されます。

以下の図に、Firepower Management Centerと管理対象デバイスの間で送信される情報をリストします。アプライアンス間で送信されるイベントとポリシーのタイプは、デバイス タイプに基づくことに注意してください。



ポリシーとイベント以外の機能

Firepower Management Center では、ポリシーをデバイスに展開したり、デバイスからイベントを受信するだけでなく、以下のデバイス関連のタスクも実行できます。

デバイスのバックアップ

NGIPSv デバイスや ASA FirePOWER モジュールのバックアップ ファイルを作成、復元することは**できません**。

物理的な管理対象デバイス自体からそのバックアップを実行する場合は、デバイス設定**のみ**をバックアップできます。設定データと統合ファイル（任意）をバックアップするには、管理用のFirepower Management Centerを使用してデバイスのバックアップを実行します。

イベントデータをバックアップするには、管理 Firepower Management Center のバックアップを実行します。

デバイスの更新

シスコは適宜、Firepower システムの更新プログラムをリリースしています。これらのアップデートには以下が含まれます。

- 侵入ルールの更新（新しいルールや更新された侵入ルールが含まれる場合があります）
- 脆弱性データベース（VDB）の更新
- 地理位置情報の更新
- ソフトウェア パッチおよびアップデート

Firepower Management Center を使用して、管理対象デバイスに更新プログラムをインストールできます。

NAT 環境

ネットワーク アドレス変換（NAT）とは、ルータを介したネットワーク トラフィックの送受信方式であり、送信元または宛先 IP アドレスの再割り当てが行われます。NAT の最も一般的な用途は、プライベート ネットワークがインターネットと通信できるようにすることです。スタティック NAT は 1:1 変換を実行し、デバイスとの FMC 通信に支障はありませんが、ポートアドレス変換（PAT）がより一般的です。PAT では、単一のパブリック IP アドレスと一意のポートを使用してパブリック ネットワークにアクセスできます。これらのポートは必要に応じて動的に割り当てられるため、PAT ルータの背後にあるデバイスへの接続は開始できません。

通常は、ルーティングと認証の両方の目的で両方の IP アドレス（登録キー付き）が必要です。デバイスを追加する際には、FMC がデバイスの IP アドレスを指定し（Firepower Management Center へのデバイスの追加 （293 ページ）を参照してください）、デバイスが FMC の IP アドレスを指定します（お使いのモデルのスタートアップ ガイドを参照してください。または、初期セットアップ後に設定を変更するには、管理インターフェイス （1266 ページ）を参照してください）。ただし、IP アドレスの 1 つのみがわかっている場合（ルーティング目的の最小要

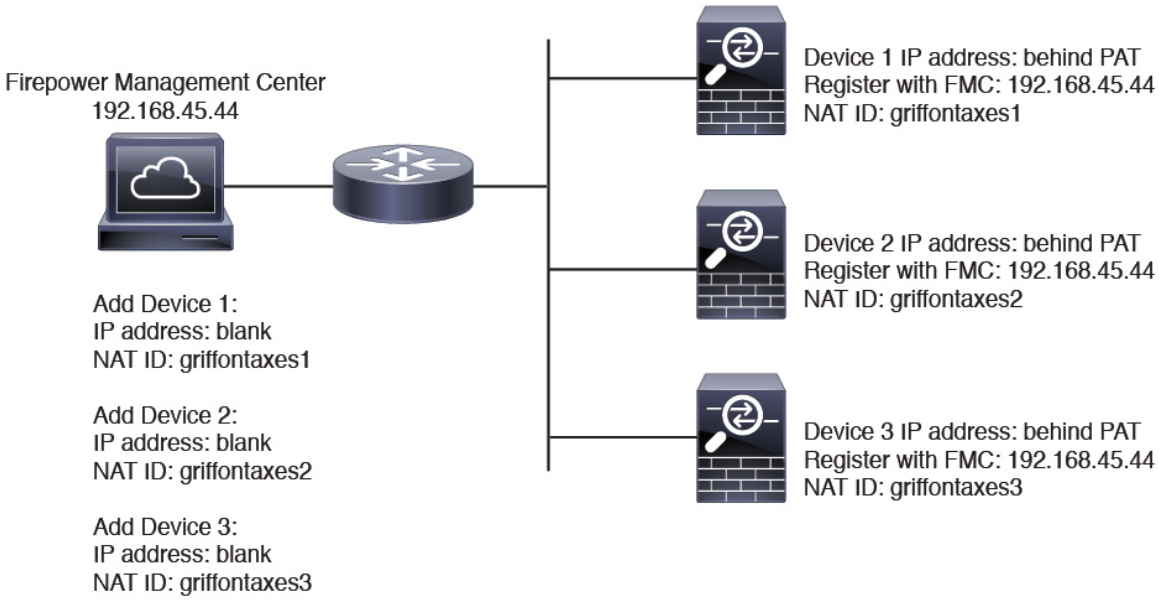
件）は、最初の通信用に信頼を確立して正しい登録キーを検索するために、接続の両側に一意の NAT ID を指定する必要もあります。FMC およびデバイスでは、初期登録の認証と承認を行うために、登録キーおよび NAT ID（IP アドレスではなく）を使用します。

たとえば、デバイスを FMC に追加したときにデバイスの IP アドレスがわからない場合（たとえばデバイスが PAT ルータの背後にある場合）は、NAT ID と登録キーのみを FMC に指定します。IP アドレスは空白のままにします。デバイス上で、FMC の IP アドレス、同じ NAT ID、および同じ登録キーを指定します。デバイスが FMC の IP アドレスに登録されます。この時点で、FMC は IP アドレスの代わりに NAT ID を使用してデバイスを認証します。

NAT 環境では NAT ID を使用するのが最も一般的ですが、NAT ID を使用することで、多数のデバイスを簡単に FMC に追加することができます。FMC で、追加するデバイスごとに IP アドレスは空白のままにして一意の NAT ID を指定し、次に各デバイスで、FMC の IP アドレスと NAT ID の両方を指定します。注：NAT ID はデバイスごとに一意でなければなりません。

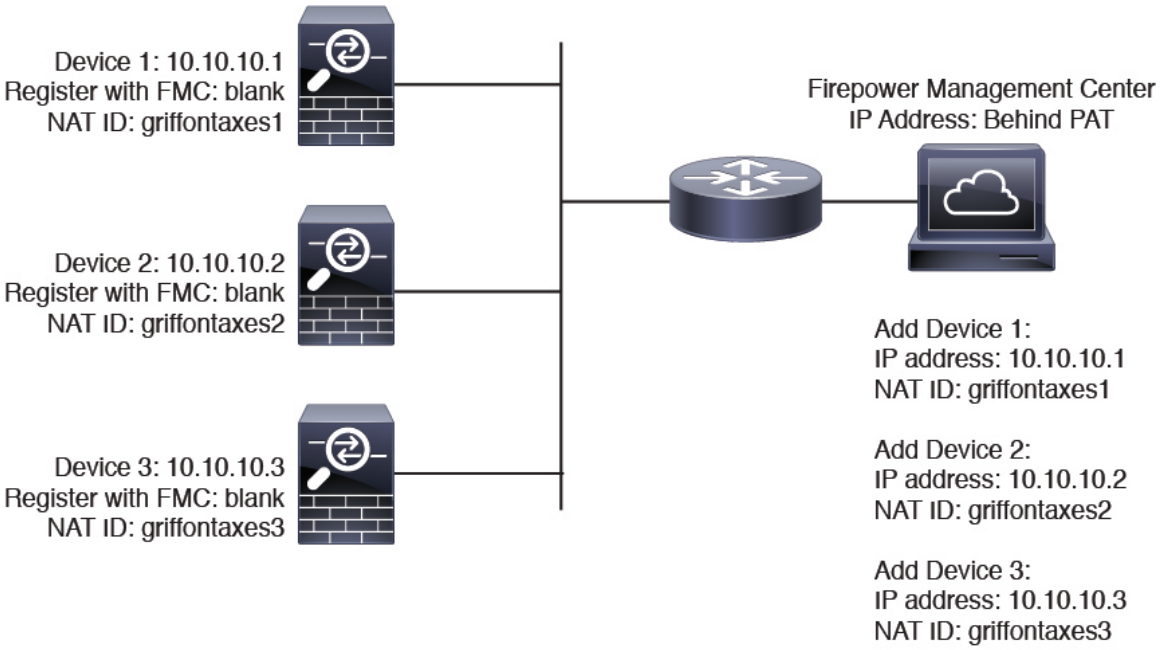
次の例に、PAT IP アドレスの背後にある 3 台のデバイスを示します。この場合、FMC とデバイスの両方でデバイスごとに一意の NAT ID を指定し、デバイス上の FMC の IP アドレスを指定します。

図 *1 : PAT* の背後にある管理対象デバイスの *NAT ID*



次の例に、PAT IP アドレスの背後にある FMC を示します。この場合、FMC とデバイスの両方でデバイスごとに一意の NAT ID を指定し、FMC 上のデバイスの IP アドレスを指定します。

図 *2 : PAT* の背後にある *FMC* の *NAT ID*



[デバイス管理（Device Management）] ページ

[デバイス管理（Device Management）] ページには、登録されたデバイス、7000 および 8000 シリーズ デバイスのハイ アベイラビリティ ペア、およびデバイス グループを管理するために使用できる、一連の情報とオプションが表示されます。このページには、現在 Firepower Management Center に登録されているすべてのデバイスの一覧が表示されます。

このページには、Firepower Management Center によって管理されている破損したデバイスの数も表示されます。ドリル ダウンして、破損したデバイスの名前や IP アドレスを特定することができます。

[表示方法（View by）] ドロップダウン リストを使用すると、グループ、ライセンス、モデル、またはアクセス コントロール ポリシーのいずれかのカテゴリでデバイス一覧をソートして表示できます。マルチドメイン導入では、ドメイン（その導入のデフォルトの表示カテゴリ）を基準にソートして表示することもできます。デバイスはリーフ ドメインに属している必要があります。

ヘルス モニタリング ステータスごとや、展開ステータスごとにデバイスを表示することもできます。

デバイス カテゴリに属するデバイスの一覧は、展開または縮小表示できます。デフォルトでは、デバイス一覧が展開されます。

デバイス一覧の詳細については、以下の表を参照してください。

表 *26 : [*デバイス一覧（***Device List***）*]* のフィールド

フィールド	説明
Name	Firepower Management Center でデバイスに使用されている表示名。名前の左側にあるステータス アイコンは、その名前の現在のヘルス ステータスを示します。
グループ	管理対象デバイスを割り当てたグループ。
モデル	管理対象デバイスのモデル。
バージョン	管理対象デバイスに現在インストールされているソフトウェアのバージョン。
シャーシ	管理対象デバイスのシャーシ マネージャの URL。URL を使用して、Firepower Management Center から Firepower Chassis Manager をクロス起動できます。
ライセンス	管理対象デバイスで有効なライセンス。
アクセス コントロール ポリシー（Access Control Policy）	現在導入されているアクセス コントロール ポリシーへのリンク。システムがアクセス コントロール ポリシーを古いものとして識別すると、そのリンクの横に警告アイコン（）が表示されます。

関連トピック

Firepower ライセンスについて （93 ページ）
ヘルス モニタリングについて （349 ページ）
アクセス コントロール ポリシーの管理 （1671 ページ）

管理対象デバイスのフィルタリング

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	リーフのみ	Admin/Network Admin

Firepower Management Center が大量のデバイスを管理する場合、[デバイス管理（Device Management）] ページの結果を絞り込むことで特定のデバイスを見つけやすくなります。

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 デバイスのリストを絞り込むには、**[デバイス検索（Search Device）]** フィールドにデバイス名、ホスト名または IP アドレスの全体または一部を入力します。

ステップ 3 フィルタをクリアするには、**[デバイス検索（Search Device）]** フィールドをクリアします。

リモート管理の設定

7000 および 8000シリーズを除くすべてのデバイス

リモート管理設定の詳細については、デバイスのクイック スタート ガイドを参照してください。

7000 および 8000 シリーズ デバイス

リモート管理の設定（従来型デバイス） （651 ページ）を参照してください。

Firepower Management Center へのデバイスの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Network Admin

Firepower Management Center に 1 つのデバイスを追加するには、ここに示す手順を実行します。冗長性やパフォーマンスのためにデバイスをリンクする場合、次の点を念頭に置いて、この手順を実行する必要があります。

- 8000 シリーズ スタック：この手順を使用して各デバイスを Firepower Management Center に追加した後、スタックを確立します（デバイス スタックの確立（702 ページ）を参照）。
- 7000 および 8000 シリーズ ハイ アベイラビリティ：この手順を使用して各デバイスを Firepower Management Center に追加した後、高可用性を確立します（Firepower 7000/8000 シリーズ ハイ アベイラビリティの確立 （685 ページ）を参照）。ハイ アベイラビリティ スタックの場合、デバイスをスタックしてから、スタック間のハイ アベイラビリティを確立します。
- FTD ハイ アベイラビリティ：この手順を使用して各デバイスを Firepower Management Center に追加した後、高可用性を確立します（Firepower Threat Defense ハイ アベイラビリティ ペアの追加 （891 ページ）を参照）。
- FTD クラスタ：クラスタ ユニットが FXOS に正常に形成されたクラスタであることを確認し、次の手順を使用して、クラスタ ユニットのいずれかを Firepower Management Center に追加します。FMC は、他のすべてのクラスタ メンバーを自動検出します。詳細については、FMC：クラスタの追加 （931 ページ）を参照してください。

（注） Firepower Management Center ハイ アベイラビリティを確立したか、または確立する予定がある場合、デバイスをアクティブな（またはアクティブにする予定の）Firepower Management Center にのみ追加します。ハイ アベイラビリティを確立すると、アクティブ Firepower Management Center に登録されたデバイスが自動的にスタンバイに登録されます。

始める前に

- デバイスを Firepower Management Center の管理対象として設定します。7000 および 8000 シリーズデバイスについては、管理対象デバイス上のリモート管理の設定 （652 ページ）を参照してください。他のモデルのリモート管理設定の詳細については、該当するクイック スタート ガイドを参照してください。
- IPv4 を使用して登録した Firepower Management Center とデバイスを IPv6 に変換する場合は、デバイスをいったん削除してから再登録する必要があります。

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 [追加（Add）] ドロップダウン メニューから、[デバイスの追加（Add Device）] を選択します。

ステップ 3 [ホスト（Host）] フィールドに、追加するデバイスの IP アドレスまたはホスト名を入力します。

デバイスのホスト名は、完全修飾ドメイン名またはローカル DNS で有効な IP アドレスに解決される名前です。ネットワークで IP アドレスの割り当てに DHCP を使用している場合は、IP アドレスではなく、ホスト名を使用します。

NAT 環境では、Firepower Management Center の管理対象としてデバイスを設定するときに Firepower Management Center の IP アドレスまたはホスト名をすでに指定した場合、デバイスの IP アドレスまたはホスト名を指定する必要がない場合があります。詳細については、NAT 環境 （289 ページ）を参照してください。

ステップ 4 [表示名（Display Name）] フィールドに、Firepower Management Center でのデバイスの表示名を入力します。

ステップ 5 [登録キー（Registration Key）] フィールドに、Firepower Management Center の管理対象としてデバイスを設定したときに使用したのと同じ登録キーを入力します。登録キーは、1 回限り使用可能な共有シークレットです。

ステップ 6 マルチドメイン展開では、現在のドメインに関係なく、デバイスをリーフ ドメインに割り当てます。

現在のドメインがリーフ ドメインである場合、デバイスは自動的に現在のドメインに追加されます。現在のドメインがリーフ ドメインでない場合、登録後、デバイスを設定するために、リーフ ドメインに切り替える必要があります。

ステップ 7 必要に応じて、デバイスをデバイス グループに追加します。

ステップ 8 登録後すぐに、デバイスに展開する最初の [アクセス コントロール ポリシー（Access Control Policy）] を選択するか、新しいポリシーを作成します。

デバイスが選択したポリシーに適合しない場合、展開は失敗します。この不適合には、複数の要因が考えられます。たとえば、ライセンスの不一致、モデルの制限、パッシブとインラインの問題、その他の構成ミスなどです。この障害の原因を解決した後、デバイスに手作業で設定を行います。

ステップ 9 デバイスに適用するライセンスを選択します。

従来型のデバイスでは、次の点に注意してください。

- コントロール、マルウェア、URL フィルタリングライセンスには、保護ライセンスが必要です。
- VPN ライセンスでは、7000 または 8000 シリーズ デバイスを必要とします。
- コントロール ライセンスは、NGIPSv と ASA FirePOWER デバイスでサポートされていますが、8000 シリーズ Fastpath ルール、スイッチング、ルーティング、スタック、デバイスのハイ アベイラビリティを設定することはできません。

ステップ 10 デバイスの設定時に、NAT ID を使用した場合、[詳細（Advanced）] セクションを展開し、[一意の NAT ID（Unique NAT ID）] フィールドに同じ NAT ID を入力します。

ステップ 11 [パケットの転送（Transfer Packets）] チェックボックスをオンにし、デバイスで Firepower Management Center にパケットを転送することを許可します。

このオプションは、デフォルトで有効です。このオプションを有効にして IPS や Snort などのイベントがトリガーされた場合は、デバイスが検査用としてイベント メタデータ情報とパケット データを Firepower Management Center に送信します。このオプションを無効にした場合は、イベント情報だけが Firepower Management Center に送信され、パケット データは送信されません。

ステップ 12 [登録（Register）] をクリックします。

Firepower Management Center がデバイスのハートビートを確認して通信を確立するまでに、最大 2 分かかる場合があります。

関連トピック

基本的なアクセス コントロール ポリシーの作成 （1673 ページ）

Firepower Management Center からのデバイスの削除

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Network Admin

デバイスを管理する必要がなくなった場合、Firepower Management Center からそのデバイスを削除できます。デバイスを削除すると、以下のようになります。

- Firepower Management Center とそのデバイスとの間のすべての通信が切断されます。
- [デバイス管理（Device Management）] ページからデバイスが削除されます。

- プラットフォーム設定ポリシーで、NTP を介して Firepower Management Center から時間を受信するようにデバイスが設定されている場合は、デバイスがローカル時間管理に戻されます。

デバイスを後者で管理するには、デバイスを Firepower Management Center に再度追加します。

（注） デバイスを削除し、再び追加すると、Firepower Management Center Web インターフェイスによって、アクセス コントロール ポリシーを再適用するよう求められます。ただし、登録時に NAT と VPN ポリシーを再適用するオプションはありません。以前に適用された NAT または VPN 設定はすべて登録時に削除されるため、登録が完了した後に再適用する必要があります。

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 削除するデバイスの横にある削除アイコン（）をクリックします。

ステップ 3 デバイスを削除することを確認します。

デバイス コンフィギュレーションの設定

アプライアンス エディタの [デバイス（Device）] ページには、詳細なデバイス設定および情報が表示されます。また、デバイス設定の一部（ライセンスの有効化と無効化、デバイスのシャットダウンと再起動、管理の変更、詳細オプションの設定など）を変更することもできます。

一般的なデバイスの設定

[デバイス（Device）] タブの [全般（General）] セクションには、以下の表に記載された設定を表示します。

表 *27 : [*全般（*General***）*] セクション テーブルのフィールド**

フィールド	説明
Name	Firepower Management Center でのデバイスの表示名。
パケット転送（Transfer Packets）	管理対象デバイスがイベントを含むパケット データを Firepower Management Center に送信するかどうかを表示します。

フィールド	説明
[モード（Mode）]	デバイスの管理インターフェイスのモード（[ルーテッド（routed）] または [トランスペアレント（transparent）]）を表示します。 （注） Firepower Threat Defense デバイスのみに [モード（Mode）] フィールドが表示されます。
コンプライアンス モード	デバイスのセキュリティ認定準拠が表示されます。有効な値は、CC、UCAPL および None です。

デバイス ライセンスの設定

[デバイス（Device）] タブの [ライセンス（License）] セクションでは、そのデバイスに対して有効になっているライセンスが表示されます。

関連トピック

Firepower ライセンスについて （93 ページ）

デバイス システムの設定

[デバイス（Device）] タブの [システム（System）] セクションには、次の表に示すように、システム情報の読み取り専用テーブルが表示されます。

表 *28 : [システム（System）] セクション テーブルのフィールド*

フィールド	説明
Model	管理対象デバイスのモデル名と番号。
Serial	管理対象デバイスのシャーシのシリアル番号。
Time	デバイスの現在のシステム時刻。
Version	管理対象デバイスに現在インストールされているソフトウェアのバージョン。
ポリシー	管理対象デバイスに現在展開されているプラットフォーム設定ポリシーへのリンク。

フィールド	説明
インベントリ	関連付けられているデバイスのインベントリ詳細情報へのリンク。このフィールドは、たとえば Firepower 2100 または Firepower 4100/9300 のコンテナインターフェイスなど、一部のプラットフォームの場合にのみ表示されます。コンテナ インターフェイスの情報を更新するには、[更新（Update）] をクリックします。たとえば、リソース プロファイルを変更した場合は、インベントリの更新を適用することで高可用性ペアの不一致の問題を回避します。それ以外の場合、この情報はポリシーの変更を展開すると更新されます。

デバイスをシャットダウンまたは再起動することもできます。

デバイス ヘルスの設定

[デバイス（Device）] タブの [ヘルス（Health）] セクションには、以下の表に記載された情報を表示します。

表 *29 : [*ヘルス（*Health***）*]* セクション テーブルのフィールド**

フィールド	説明
Status	デバイスの現在のヘルス ステータスを表すアイコン。アイコンをクリックすると、アプライアンスのヘルス モニタが表示されます。
ポリシー	現在デバイスで展開されている、読み取り専用バージョンの正常性ポリシーへのリンク。
ブラックリスト	[ヘルス ブラックリスト（Health Blacklist）] ページへのリンク。このページでは、ヘルス ブラックリスト モジュールを有効または無効に設定できます。

関連トピック

アプライアンス ヘルス モニタの表示 （373 ページ）
正常性ポリシーの編集 （364 ページ）
正常性ポリシー モジュールのブラックリスト登録 （368 ページ）

デバイス管理設定

[デバイス（Device）] タブの [管理（Management）] セクションには、以下の表に記載されたフィールドを表示します。

表 *30 : [*管理（*Management***）*]* セクション テーブルのフィールド**

フィールド	説明
ホスト	デバイスの IP アドレスまたはホスト名。ホスト名は、完全修飾ドメイン名またはローカル DNS で有効な IP アドレスに解決される名前（つまり、ホスト名）です。
ステータス	Firepower Management Center と管理対象デバイス間の通信チャネルのステータスを示すアイコン。ステータス アイコンにポインタを置くと、Firepower Management Center が最後にデバイスにアクセスした時間を表示することができます。

デバイスの詳細設定

[デバイス（Device）] タブの [詳細設定（Advanced）] セクションには、以下で説明する詳細設定のテーブルが表示されます。上記の設定は、いずれも [詳細設定（Advanced）] セクションを使用して編集できます。

表 *31 : [*詳細設定（*Advanced***）*]* セクションのテーブルのフィールド**

フィールド	説明	サポートされるデバイス
Application Bypass	デバイスでの自動アプリケーション バイパスの状態。	7000 & 8000 シリーズ NGIPSv ASA FirePOWER Firepower Threat Defense
Bypass Threshold	自動アプリケーション バイパスのしきい値（ミリ秒）。	
ローカル ルータ トラフィックを検査する（Inspect Local Router Traffic）	デバイスで、ルーテッド インターフェイスで受信した自己を宛先とするトラフィック（ICMP、DHCP、およびOSPF トラフィックなど）を検査するかどうかを示します。	7000 & 8000 シリーズ
高速パス ルール（Fast-Path Rules）	デバイスで作成されている 8000 シリーズ 高速パス ルールの数。	8000 シリーズ

デバイス情報の表示

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Network Admin

マルチドメイン展開では、先祖ドメインは、子孫ドメイン内のすべてのデバイスに関する情報を表示できます。デバイスを編集するリーフ ドメインに位置している必要があります。

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 表示するデバイスの横にある編集アイコン（）をクリックします。

マルチドメイン展開では、先祖ドメインに位置している場合、表示アイコン（）をクリックすると、読み取り専用モードで子孫ドメインのデバイスを表示できます。

ステップ 3 [デバイス（Device）] タブをクリックします。

ステップ 4 次の情報が表示されます。

- [全般（General）]：デバイスの一般設定を表示します（一般的なデバイスの設定 （296 ページ）を参照）。
- [ライセンス（License）]：デバイスのライセンス情報を表示します（デバイス ライセンスの設定 （297 ページ）を参照）。
- [システム（System）]：デバイスのシステム情報を表示します（デバイス システムの設定 （297 ページ）を参照）。
- [ヘルス（Health）]：デバイスの現在のヘルス ステータスに関する情報を表示します（デバイス ヘルスの設定 （298 ページ）を参照）。
- [管理（Management）]：Firepower Management Center とデバイスの間の通信チャネルに関する情報を表示します（デバイス管理設定 （299 ページ）を参照）。
- [詳細（Advanced）]：高度な機能設定に関する情報を表示します（デバイスの詳細設定 （299ページ）を参照）。

デバイス管理設定の編集

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	リーフのみ	Admin/Network Admin

（デバイスの CLI を使用するなどして）デバイスを FMC に追加した後にそのデバイスのホスト名または IP アドレスを編集する場合は、次の手順を使用して管理側の FMC のホスト名または IP アドレスを手動で更新する必要があります。

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

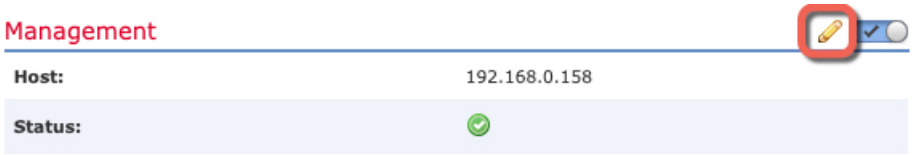
ステップ 2 管理オプションを変更するデバイスの横にある [Edit] アイコン（）をクリックします。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [デバイス（Device）] タブをクリックし、[管理（Management）] 領域を表示します。

ヒント スタック構成のデバイスの場合、アプライアンス エディタの [デバイス（Devices）] ページで、個々のデバイスの管理オプションを変更します。

ステップ 4 [Edit] アイコン（） をクリックして [ホスト（Host）] の IP アドレスまたはホスト名を編集します。



[管理（Management）] ダイアログボックスで、[ホスト（Host）] フィールドの名前または IP アドレスを変更し、[保存（Save）] をクリックします。

ステップ 5 （任意） リモート管理を無効にします。

スライダ（） をクリックしてデバイスの管理を有効または無効にします。管理を無効化すると、Firepower Management Center とデバイス間の接続がブロックされますが、Firepower Management Center からデバイスは削除**されません**。デバイスを管理する必要がなくなった場合は、Firepower Management Center からのデバイスの削除 （295 ページ）を参照してください。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

一般的なデバイス設定の編集

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	リーフのみ	Admin/Network Admin

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 変更するデバイスの横にある編集アイコン（）をクリックします。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [デバイス（Device）] をクリックします。

ステップ 4 [一般（General）] セクションで、編集アイコン（）をクリックします。

ステップ 5 [名前（Name）] に、管理対象デバイスの名前を入力します。

ヒント スタック構成のデバイスの場合、アプライアンス エディタの [スタック（Stack）] ページで、スタックでデバイスに割り当てられている名前を編集します。アプライアンス エディタの [デバイス（Devices）] ページでは、個々のデバイスに割り当てられているデバイス名を編集できます。

ステップ 6 [パケットの転送（Transfer Packets）] 設定を変更します。

- パケット データをイベントと一緒に Firepower Management Center に保存できるようにするには、[パケットの転送（Transfer Packets）] チェックボックスをオンにします。
- 管理対象デバイスがイベントと一緒にパケット データを送信できないようにするには、このチェックボックスをオフにします。

ステップ 7 [強制展開（Force Deploy）] をクリックし、デバイスに現在のポリシーとデバイス設定の展開を強制します。

ステップ 8 **[保存（Save）]** をクリックします。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

デバイス設定のコピー

新しいデバイスをネットワークに展開する場合、新しいデバイスを手動で再設定する代わりに、事前設定されているデバイスの設定とポリシーを簡単にコピーすることができます。

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	Firepower Threat Defense	リーフのみ	Admin/Network Admin

始める前に

次の項目を確認します。

- 送信元と宛先の Firepower Threat Defense デバイスが同じモデルであり、同じバージョンの Firepower ソフトウェアを実行している。
- 送信元がスタンドアロン Firepower Threat Defense デバイスまたは Firepower Threat Defense 高可用性ペアである。
- 宛先のデバイスがスタンドアロン Firepower Threat Defense デバイスである。
- 送信元と宛先の Firepower Threat Defense デバイスに同じ数の物理インターフェイスがある。
- 送信元と宛先の Firepower Threat Defense デバイスが同じファイアウォール モード（ルーテッドまたはトランスペアレント）になっている。
- 送信元と宛先の Firepower Threat Defense デバイスが同じセキュリティ認定コンプライアンス モードになっている。
- 送信元と宛先の Firepower Threat Defense デバイスが同じドメインにある。
- 送信元または宛先 Firepower Threat Defense デバイスのいずれでも設定の展開が進行中ではない。

手順の概要

1. **[Devices]** > **[Device Management]**を選択します。
2. 変更するデバイスの横にある編集アイコン（）をクリックします。
3. [デバイス（Device）] をクリックします。
4. [全般（General）] セクションで、次のいずれかの操作を実行します。
   - [デバイス設定の取得（Get Device Configuration）] アイコン（  ）をクリックして、別のデバイスのデバイス設定を新しいデバイスにコピーします。[デバイス設定の取得（Get Device Configuration）] ページの [デバイスの選択（Select Device）] ドロップダウン リストで、送信元デバイスを選択します。
   - [デバイス設定のプッシュ（Push Device Configuration）] アイコン（  ）をクリックして、現在のデバイスのデバイス設定を新しいデバイスにコピーします。[デバイス設定のプッシュ（Push Device Configuration）] ページの [ターゲット デバイス（Target Device）] ドロップダウン リストで、設定をコピーする宛先を選択します。
5. （オプション）[共有ポリシーの設定を含める（Include shared policies configuration）] チェックボックスを選択して、ポリシーをコピーします。
6. [OK] をクリックします。

手順の詳細

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 変更するデバイスの横にある編集アイコン（）をクリックします。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [デバイス（Device）] をクリックします。

ステップ 4 [全般（General）] セクションで、次のいずれかの操作を実行します。

- [デバイス設定の取得（Get Device Configuration）] アイコン（）をクリックして、別のデバイスのデバイス設定を新しいデバイスにコピーします。[デバイス設定の取得（Get Device Configuration）] ページの [デバイスの選択（Select Device）] ドロップダウン リストで、送信元デバイスを選択します。
- [デバイス設定のプッシュ（Push Device Configuration）] アイコン（）をクリックして、現在のデバイスのデバイス設定を新しいデバイスにコピーします。[デバイス設定のプッシュ（Push Device Configuration）] ページの [ターゲット デバイス（Target Device）] ドロップダウン リストで、設定をコピーする宛先を選択します。

ステップ 5 （オプション）[共有ポリシーの設定を含める（Include shared policies configuration）] チェックボックスを選択して、ポリシーをコピーします。

AC ポリシー、NAT、プラットフォーム設定、および FlexConfig ポリシーなどの共有ポリシーは、複数のデバイス間で共有できます。

ステップ 6 [OK] をクリックします。

デバイス設定のコピー タスクのステータスは、メッセージ センターの [タスク（Tasks）] タブでモニタできます。

デバイス設定のコピー タスクが開始されると、ターゲット デバイスの設定が削除され、送信元デバイスの設定が宛先のデバイスにコピーされます。

警告 デバイス設定のコピー タスクの完了後に、ターゲット デバイスを元の設定に戻すことはできません。

デバイス ライセンスの有効化と無効化

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	リーフのみ	Admin/Network Admin

Firepower Management Center で使用可能なライセンスがある場合、デバイスでそのライセンスを有効にすることができます。

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 ライセンスを有効または無効にするデバイスの横にある編集アイコン（  ）をクリックします。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [デバイス（Device）] タブをクリックします。

ヒント スタック構成のデバイスの場合、アプライアンス エディタの [スタック（Stack）] ページで、スタックに対してラインセンスを有効または無効にします。

ステップ 4 [ライセンス（License）] セクションで、編集アイコン（  ）をクリックします。

ステップ 5 管理対象デバイスに対して有効または無効にするライセンスの横にあるチェックボックスをオンまたはオフにします。

ステップ 6 **[保存（Save）]** をクリックします。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

関連トピック

Firepower ライセンスについて （93 ページ）

詳細なデバイス設定の編集

アプリケーション バイパス、ローカル ルータ トラフィックのインスペクション、および高速パスのルールを設定できます。

自動アプリケーション バイパスの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	リーフのみ	Admin Network Admin

Automatic Application Bypass（AAB）機能は、インターフェイスでのパケット処理時間に制限を設け、この時間を超過した場合、パケットに検出のバイパスを許可します。この機能は任意の展開で使用できますが、インライン展開ではとりわけ価値があります。

パケット処理の遅延は、ネットワークで許容できるパケット レイテンシとバランスを取って調整します。Snort 内での不具合やデバイスの誤った設定が原因で、トラフィックの処理時間が指定のしきい値を超えると、AAB により、その障害発生から 10 分以内に Snort が再起動され、

トラブルシューティングデータが生成されます。このデータを分析することで、過剰な処理時間の原因を調査できます。

一般に、遅延しきい値を超えた後は、高速パス パケットに対して侵入ポリシーの [ルール遅延しきい値（Rule Latency Thresholding）] を使用します。[ルール遅延しきい値（Rule Latency Thresholding）] により、エンジンがシャットダウンされたり、しきい値データが生成されることはありません。

検出がバイパスされると、デバイスがヘルス モニタリング アラートを生成します。

AAB はデフォルトで無効になっています。AAB を有効にするには、次の手順を実行します。

注意 単一パケットに過剰な処理時間がかかっている場合、AAB がアクティブになります。AAB のアクティブ化は、いくつかのパケットのインスペクションを一時的に中断する Snort プロセスを部分的に再起動します。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、ターゲットデバイスがトラフィックを処理する方法に応じて異なります。詳細はSnort® の再起動によるトラフィックの動作 （451 ページ）を参照してください。

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 高度なデバイス設定を編集するデバイスの横にある編集アイコン（）をクリックします。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [デバイス（Device）] タブ（またはスタック構成のデバイスの場合は [スタック（Stack）] タブ）をクリックし、[詳細（Advanced）] セクションの編集アイコン（）をクリックします。

ステップ 4 [自動アプリケーション バイパス（Automatic Application Bypass）] をオンにします。

ステップ 5 [バイパスしきい値（Bypass Threshold）] に 250 ～ 60,000 ミリ秒を入力します。デフォルト設定は 3000 ミリ秒（ms）です。

ステップ 6 **[保存（Save）]** をクリックします。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

ローカル ルータ トラフィックの検査

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	7000 & 8000 シリーズ	リーフのみ	Admin/Network Admin

ローカル内トラフィックがレイヤ3展開のモニタ ルールと一致する場合、そのトラフィックは検査をバイパスすることがあります。トラフィックの検査を確認するには、[ローカル ルータ トラフィックの検査（Inspect Local Router Traffic）] を有効にします。

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 高度なデバイス設定を編集するデバイスの横にある編集アイコン（）をクリックします。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [デバイス（Devices）] タブ（スタック構成のデバイスの場合は [スタック（Stack）] タブ）をクリックして、[詳細（Advanced）] セクションの編集アイコン（）をクリックします。

ステップ 4 7000 または 8000 シリーズ デバイスがルータとして展開されている場合は、[ローカル ルータ トラフィックの検査] をオンにして、例外トラフィックを検査します。

ステップ 5 **[保存（Save）]** をクリックします。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

高速パス ルールの設定（8000 シリーズ）

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
該当なし	いずれか（Any）	8000 シリーズ	リーフのみ	Admin/Network Admin

トラフィック処理の初期形式として、8000 シリーズ高速パス ルールでは、それ以上のインスペクションやロギングを行わずに 8000 シリーズ デバイスを介してトラフィックを直接送信できます。（パッシブ展開では、8000 シリーズ高速パス ルールは単に分析を停止します）。各 8000 シリーズ高速パス ルールは、特定のセキュリティ ゾーンまたはインライン インターフェイス セットに適用されます。8000 シリーズ高速パス ルールはハードウェア レベルで機能するため、高速パス トラフィックには、次の単純な外部ヘッダーの基準のみを使用できます。

- イニシエータおよびレスポンダ IP アドレスまたはアドレス ブロック
- プロトコル、および TCP と UDP の場合は、発信側および応答側のポート
- VLAN ID（Admin. VLAN ID）

デフォルトでは、8000 シリーズ高速パス ルールは指定した発信側から指定した応答側への接続に影響します。ルールの基準を満たすすべての接続を高速パス処理するには、どちらのホストが発信側か応答側かに関係なく、ルールを双方向にすることができます。

（注） 同様の機能を実行しますが、8000 シリーズ高速パス ルールはプレフィルタ ポリシーで設定する高速パス トンネルやプレフィルタ ルールに関連しません。

（注） [任意（Any）] 以外のポートを TCP または UDP のトラフィックに指定すると、一致するフラグメント化トラフィックの最初のフラグメントのみに高速パスの処理が実行されます。その他のすべてのフラグメントは転送され、さらに詳しい検査が行われます。これは、高速パス ルールに一致する必要があるすべての IP ヘッダー情報が各フラグメントの IP ヘッダーに含まれており、後続のフラグメントにはポートを識別するフィールドが含まれていない場合、8000 シリーズ はフラグメント化されたトラフィックのみに高速パス処理を実行するためです。

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 ルールを設定する 8000 シリーズ デバイスの横にある編集アイコン（）をクリックします。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [デバイス（Device）] タブ（またはスタック構成のデバイスの場合は [スタック（Stack）] タブ）をクリックし、[詳細（Advanced）] セクションの編集アイコン（）をクリックします。

ステップ 4 [新しい IPv4 ルール（New IPv4 Rule）] または [新しい IPv6 ルール（New IPv6 Rule）] をクリックします。

ステップ 5 [ドメイン（Domain）] ドロップダウン リストから、インライン セットまたはパッシブ セキュリティ ゾーンを選択します。

ステップ 6 高速パス処理するトラフィックを設定します。トラフィックは高速パス処理のためのすべての条件を満たしている必要があります。

- [イニシエータ（Initiator）] および [レスポンダ（Responder）]（必須）：発信側および応答側の IP アドレスまたはアドレス ブロックを入力します。
- [プロトコル（Protocol）]：プロトコルを選択するか、[すべて（All）] を選択します。
- [イニシエータポート（Initiator Port）] および [レスポンダポート（Responder Port）]：TCP および UDP トラフィックの場合は、イニシエータ ポートとレスポンダ ポートを入力します。フィールドを空白のままにするか、**Any** と入力して、すべての TCP または UDP トラフィックに一致するようにします。ポートのカンマ区切りリストを入力できますが、ポート範囲を入力することはできません。
- [VLAN ID]：VLAN ID を入力します。フィールドを空白のままにするか、**Any** と入力して、VLAN タグに関係なくすべてのトラフィックに一致するようにします。

ステップ 7 （オプション）ルールを [双方向（Bidirectional）] にします。

ステップ 8 [保存（Save）] をクリックしてから、もう一度 [保存（Save）] をクリックします。

次のタスク

設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

システム シャットダウンの管理

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	すべて（ASA FirePOWER を除く）	リーフのみ	Admin/Network Admin

（注） Firepowerシステムのユーザインターフェイスでは、ASA FirePOWERのシャットダウンまたは再起動はできません。それぞれのデバイスをシャットダウンする方法の詳細については、ASAの資料を参照してください。

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 再起動するデバイスの横にある編集アイコン（）をクリックします。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [デバイス（Device）] タブをクリックします。

ヒント スタックに含まれるデバイスの場合、アプライアンス エディタの [デバイス（Devices）] ページで、個々のデバイスをシャット ダウンまたは再起動します。

ステップ 4 デバイスをシャットダウンするには、[システム（System）]セクションでデバイスのシャットダウン アイコン（）をクリックします。

ステップ 5 プロンプトが表示されたら、デバイスのシャットダウンを確認します。

ステップ 6 デバイスを再起動するには、デバイスの再起動アイコン（）をクリックします。

ステップ 7 プロンプトが表示されたら、デバイスを再起動することを確認します。

インターフェイス テーブル ビュー

ハードウェア ビューの下にあるインターフェイス テーブル ビューには、デバイスで使用可能なすべてのインターフェイスが一覧表示されます。テーブル内のナビゲーション ツリーを展開すると、設定されているすべてのインターフェイスを表示できます。インターフェイスの横に

ある矢印アイコンをクリックして、インターフェイスを縮小または展開することで、サブコンポーネントの非表示/表示を切り替えることができます。このインターフェイステーブルビューには、各インターフェイスに関する要約情報も表示されます。

表 *32*：従来のデバイスのインターフェイス

フィールド	説明
Name	各インターフェイスタイプは、タイプとリンク ステート（該当する場合）を示す固有のアイコンによって表されます。名前またはアイコンの上にポインタを置くと、追加情報を含むツールチップが表示されます。インターフェイスアイコンについては、インターフェイスアイコン（655 ページ）を参照してください。 アイコンでは、インターフェイスの現在のリンク状態を示す表示方法が使用されています。次の 3 つの状態のいずれかが表示されます。 • エラー（  ） • 障害（  ） • 使用不可（  ） 論理インターフェイスのリンク状態は、親物理インターフェイスのリンク状態と同じです。 ASA FirePOWER モジュールはリンク状態を表示しません。無効化されたインターフェイスは、半透明のアイコンで表されます。 アイコンの右側に表示されるインターフェイス名は自動生成されます。ただし、ハイブリッド インターフェイスと ASA FirePOWERインターフェイスの名前はユーザが定義します。ASA FirePOWER インターフェイスについては、名前が付けられており、リンクを持つ有効なインターフェイスのみが表示されることに注意してください。 物理インターフェイスでは、物理インターフェイスの名前が表示されます。論理インターフェイスでは、物理インターフェイスの名前と、割り当てられている VLAN タグが表示されます。 ASA FirePOWER インターフェイスでは、複数のセキュリティ コンテキストがある場合は、セキュリティ コンテキストの名前とインターフェイスの名前が表示されます。セキュリティ コンテキストが 1 つしかない場合は、インターフェイスの名前のみが表示されます。
セキュリティ ゾーン（Security Zone）	インターフェイスが割り当てられているセキュリティ ゾーン。セキュリティ ゾーンを追加または編集するには、編集アイコン（  ）をクリックします。
[Used by]	インターフェイスが割り当てられているインラインセット、仮想スイッチ、または仮想ルータ。

フィールド	説明
MAC アドレス（MAC Address）	スイッチド機能およびルーテッド機能で有効にされているインターフェイスに対して表示される MAC アドレス。 NGIPSv デバイスの場合、表示された MAC アドレスにより、デバイス上に設定されたネットワーク アダプタと、[インターフェイス（Interfaces）] ページに表示されるインターフェイスを対応させることができます。
IP アドレス（7000/8000 シリーズのみ）	インターフェイスに割り当てられた IP アドレス。マウスのポインタを IP アドレスの上に重ねると、その IP アドレスがアクティブであるかを確認できます。非アクティブな IP アドレスはグレー表示されます。

表 *33 : FTD* インターフェイス

フィールド	説明
インターフェイス	インターフェイス ID。フェールオーバー リンクまたはクラスタ制御リンクのインターフェイスの場合、インターフェイス設定は表示専用です。
論理名（Logical Name）	インターフェイスの構成名。
タイプ（Type）	インターフェイスのタイプ：[物理（Physical）]、[サブインターフェイス（SubInterface）]、[EtherChannel]、[冗長（Redundant）]、または [ブリッジグループ（BridgeGroup）]（トランスペアレント ファイアウォール モードのみ）。
インターフェイス オブジェクト（Interface Object）	インターフェイスが割り当てられているセキュリティ ゾーンまたはインターフェイス グループ。
MAC アドレス（MAC Address）（アクティブ/スタンバイ）	インターフェイスの MAC アドレス。高可用性の場合、アクティブな MAC アドレスとスタンバイ状態の MAC アドレスの両方が表示されます。
[IPアドレス（IP Address）]	インターフェイスに割り当てられている IP アドレス。括弧で示されるアドレス割り当てのタイプ：[静的（Static）]、[DHCP]、または [PPPoE]。

デバイス グループ管理

Firepower Management Center でデバイスをグループ化すると、複数のデバイスへのポリシーの展開やアップデートのインストールを簡単に行えます。グループに属するデバイスのリストは、展開または縮小表示できます。デフォルトでは、このリストは縮小表示されます。

マルチドメイン展開では、リーフ ドメイン内でのみデバイス グループを作成できます。Firepower Management Center をマルチテナンシー向けに設定すると既存のデバイス グループは削除されます。デバイス グループはリーフ ドメイン レベルで再度追加できます。

デバイス グループの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	リーフのみ	Admin/Network Admin

デバイス グループにより、複数デバイスへのポリシーの割り当てとインストール更新が簡単にできます。

スタック内またはハイ アベイラビリティ ペア内のプライマリ デバイスをグループに追加すると、両方のデバイスがグループに追加されます。デバイスのスタック構成を解除またはハイ アベイラビリティ ペアを分解しても、これらのデバイスは両方ともグループに属したままになります。

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 [追加（Add）] ドロップダウン メニューから、[グループの追加（Add Group）] を選択します。

ステップ 3 名前を入力します。

ステップ 4 [使用可能なデバイス（Available Devices）] から、デバイス グループに追加するデバイスを 1 つ以上選択します。複数のデバイスを選択する場合は、Ctrl または Shift キーを押しながらクリックします。

ステップ 5 [追加（Add）] をクリックして、選択したデバイスをデバイス グループに追加します。

ステップ 6 [OK] をクリックして、デバイス グループを追加します。

デバイス グループの編集

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	リーフのみ	Admin/Network Admin

任意のデバイス グループに含まれる一連のデバイスを変更できます。アプライアンスは、現行のグループから削除してからでないと、新しいグループに追加できません。

アプライアンスを新しいグループに移動しても、そのアプライアンスのポリシーが、新しいグループにすでに割り当てられているポリシーに変更される訳ではありません。グループのポリシーを新しいデバイスに割り当てる必要があります。

スタック内またはデバイスのハイ アベイラビリティ ペア内のプライマリ デバイスをグループに追加すると、両方のデバイスがグループに追加されます。デバイスのスタック構成を解除またはハイ アベイラビリティ ペアを分解しても、これらのデバイスは両方ともグループに属したままになります。

マルチドメイン展開では、デバイス グループは、それらが作成されたドメイン内でのみ編集できます。

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 編集するデバイス グループの横にある編集アイコン（  ）をクリックします。

ステップ 3 必要に応じて、[名前（Name）] フィールドに、グループの新しい名前を入力します。

ステップ 4 [使用可能なデバイス（Available Devices）] から、デバイス グループに追加するデバイスを 1 つ以上選択します。複数のデバイスを選択する場合は、Ctrl または Shift キーを押しながらクリックします。

ステップ 5 [追加（Add）] をクリックして、選択したデバイスをデバイス グループに追加します。

ステップ 6 必要に応じて、デバイス グループからデバイスを削除するには、削除するデバイスの横にある削除アイコン（  ）をクリックします。

ステップ 7 [OK] をクリックして、デバイス グループに加えた変更を保存します。

Firepower 1000/2100 シリーズの SNMP の設定

簡易ネットワーク管理プロトコル（SNMP）は、SNMP マネージャとエージェント間の通信用メッセージフォーマットを提供する、アプリケーションレイヤプロトコルです。SNMP では、ネットワーク内のデバイスのモニタリングと管理に使用する標準フレームワークと共通言語が提供されます。

SNMP フレームワークは 3 つの部分で構成されます。

- SNMP マネージャ：SNMP を使用してネットワーク デバイスのアクティビティを制御し、モニタリングするシステム。
- SNMP エージェント：Firepower シャーシのデータを維持し、必要に応じてそのデータを SNMP マネージャに報告する Firepower 1000/2100 シャーシ内のソフトウェア コンポーネント。Firepower シャーシには、エージェントと一連の MIB が含まれています。SNMP エージェントを有効にし、マネージャとエージェント間のリレーションシップを作成するには、Firepower Management Center で SNMP を有効にし、設定します。
- 管理情報ベース（MIB）：SNMP エージェント上の管理対象オブジェクトのコレクション。

Firepower 1000/2100 シャーシは、SNMPv1、SNMPv2c、および SNMPv3 をサポートします。SNMPv1 および SNMPv2c はどちらも、コミュニティベース形式のセキュリティを使用します。

Firepower 1000/2100 の SNMP の有効化と SNMP プロパティの設定

（注） この手順は、Firepower 2100 と Firepower 1000 シリーズのデバイスのみに適用されます。

ステップ 1 **[デバイス（Devices）] > [デバイス管理（Device Management）]** を選択します。

ステップ 2 [SNMP] タブをクリックします。

ステップ 3 次のフィールドに入力します。

名前	説明
[Admin State] チェックボックス	SNMP が有効化かディセーブルか。システムに SNMP サーバとの統合が含まれる場合にだけこのサービスをイネーブルにします。
[Port] フィールド	Firepower シャーシが SNMP ホストと通信するためのポート。デフォルト ポートは変更できません。
[コミュニティ（Community）] フィールド	Firepower シャーシが SNMP ホストに送信するトラップ メッセージに含まれるデフォルトの SNMP v1 または v2 コミュニティの名前、あるいは SNMP v3 のユーザ名。 1 ～ 32 文字の英数字文字列を入力します。@（アット マーク）、\（バックスラッシュ）、"（二重引用符）、?（疑問符）または空欄スペースは使用しないでください。デフォルトは **public** です。 [コミュニティ（Community）] フィールドがすでに設定されている場合、空白フィールドの右側のテキストは [設定：はい（Set: Yes）] となることに注意してください。[コミュニティ（Community）] フィールドに値が入力されていない場合、空白フィールドの右側のテキストは [設定：いいえ（Set: No）] となります。
[システム管理者名（System Admin Name）] フィールド	SNMP 実装の担当者の連絡先。 電子メール アドレス、名前、電話番号など、255 文字までの文字列を入力します。
[Location]フィールド	SNMP エージェント（サーバ）が実行するホストの場所。 最大 510 文字の英数字を入力します。

ステップ 4 **[Save]** をクリックします。

次のタスク

SNMP トラップおよびユーザを作成します。

Firepower 1000/2100 の SNMP トラップの作成

（注） この手順は、Firepower 2100 と Firepower 1000 シリーズのデバイスのみに適用されます。

ステップ 1 **[デバイス（Devices）] > [デバイス管理（Device Management）]** を選択します。

ステップ 2 [SNMP] タブをクリックします。

ステップ 3 [SNMP トラップ設定（SNMP Traps Configuration）] 領域で、[追加（Add）] をクリックします。

ステップ 4 [SNMP トラップ設定（SNMP Trap Configuration）] ダイアログボックスで、次のフィールドに値を入力します。

名前	説明
[Host Name] フィールド	Firepower シャーシからのトラップを受信する SNMP ホストのホスト名または IP アドレス。
[コミュニティ（Community）] フィールド	Firepower シャーシが SNMP ホストに送信するトラップに含める SNMP v1 または v2 コミュニティ名あるいは SNMP v3 ユーザ名。これは、SNMP サービスに設定されたコミュニティまたはユーザ名と同じである必要があります。 1 ～ 32 文字の英数字文字列を入力します。@（アット マーク）、\（バックスラッシュ）、"（二重引用符）、?（疑問符）または空欄スペースは使用しないでください。
[Port] フィールド	Firepower シャーシが SNMP ホストとのトラップの通信に使用するポート。 1 ～ 65535 の整数を入力します。
[Version] フィールド	トラップに使用される SNMP バージョンおよびモデル。次のいずれかになります。 • **V1** • **[V2]** • **[V3]**
[Type] フィールド	バージョンとして [V2] または [V3] を選択した場合に、送信するトラップのタイプ。次のいずれかになります。 • **[Traps]** • **nforms**

名前	説明
[特権（Privilege）] フィールド	バージョンとして [V3] を選択した場合に、トラップに関連付ける権限。次のいずれかになります。 • [Auth]：認証あり、暗号化なし • [Noauth]：認証なし、暗号化なし • [Priv]：認証あり、暗号化あり

ステップ 5 [OK] をクリックして、[SNMP トラップ設定（SNMP Trap Configuration）] ダイアログボックスを閉じます。

ステップ 6 **[保存（Save）]** をクリックします。

Firepower 1000/2100 の SNMP ユーザの作成

（注） この手順は、Firepower 2100 と Firepower 1000 シリーズのデバイスのみに適用されます。

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択します。

ステップ 2 [SNMP] タブをクリックします。

ステップ 3 [SNMP ユーザ設定（SNMP Users Configuration）] 領域で、[追加（Add）] をクリックします。

ステップ 4 [SNMP ユーザ設定（SNMP User Configuration）] ダイアログボックスで、次のフィールドに値を入力します。

名前	説明
[Username] フィールド	SNMP ユーザに割り当てられるユーザ名。 32 文字までの文字または数字を入力します。名前は文字で始まる必要があり、_（アンダースコア）、.（ピリオド）、@（アットマーク）、-（ハイフン）も指定できます。
[認証アルゴリズム タイプ（Auth Algorithm Type）] フィールド	許可タイプ：**SHA**。
[AES-128 を使用（Use AES-128）] チェックボックス	オンにすると、このユーザに AES-128 暗号化が使用されます。
[認証パスワード（Authentication Password）] フィールド	ユーザのパスワード。
[確認（Confirm）] フィールド	確認のためのパスワードの再入力。

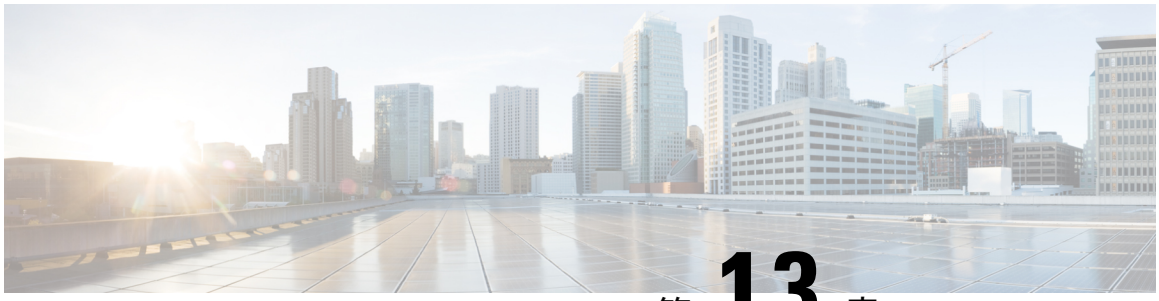
名前	説明
[暗号化パスワード（Encryption Password）] フィールド	ユーザのプライバシー パスワード。
[確認（Confirm）] フィールド	確認のためのプライバシー パスワードの再入力。

ステップ 5 [OK] をクリックして、[SNMP ユーザ設定（SNMP User Configuration）] ダイアログボックスを閉じます。

ステップ 6 **[保存（Save）]** をクリックします。

第 III 部

システム モニタリングとトラブルシューティング



第 13 章

ダッシュボード

次のトピックでは、Firepowerシステムでダッシュボードを使用する方法について説明します。

ダッシュボードについて

Firepower システム ダッシュボードは、システムによって収集および生成されたイベントに関するデータを含む、現在のシステムのステータスを概要的なビューとして提供します。またダッシュボードを使用して、展開のアプライアンスのステータスと全体の正常性に関する情報を表示することもできます。ダッシュボードが提供する情報はシステムのライセンス方法、設定方法、展開方法によって異なる点に注意してください。

ヒント

ダッシュボードは網羅的なデータを提供する複雑で高度にカスタマイズ可能なモニタリング機能です。モニタ対象のネットワークについての広範、簡潔でカラフルな画像を得るには、Context Explorer を使ってください。

ダッシュボードは、Firepower Management Center および 7000 & 8000 シリーズ デバイスで使用できます。

ダッシュボードはウィジェットの表示にタブを使用します。ウィジェットは小さな自己完結型のコンポーネントで、システムのさまざまな側面を理解するうえで役に立ちます。たとえば、定義済みの [アプライアンス情報（Appliance Information）] ウィジェットは、アプライアンスの名前、モデル、およびFirepower システム ソフトウェアの現在実行中のバージョンを通知します。システムはダッシュボードの時間範囲によってウィジェットを制約します。この時間範囲は、最短で 1 時間前から、最長では 1 年前からの期間を反映するように変更できます。

システムには、いくつかの事前定義されたダッシュボードウィジェットが付属していて、使用および変更できます。ユーザ ロールにダッシュボードへのアクセス権が付与されている（管理者、メンテナンス ユーザ、セキュリティ アナリスト（読み取り専用）、およびダッシュボードの権限付きのカスタム ロール）場合、デフォルトでホームページは事前定義されたサマリ

ダッシュボードになっています。ただし、ダッシュボード以外を含む別のデフォルト ホームページを設定できます。デフォルトのダッシュボードを変更することもできます。ダッシュボードへのアクセス権がないユーザ ロールの場合、デフォルトのホームページはロールに関連するページです。たとえば、Discovery Admin ロールの場合はネットワーク検出ページが表示されます。

また、事前定義済みのダッシュボードをカスタム ダッシュボードのベースとして使用することもできます。これは共有することもプライベートとして制限することもできます。管理者アクセス権がない場合、他のユーザが作成したプライベート ダッシュボードは表示も変更もできません。

（注） イベントのドリルダウン ページとテーブル ビューには、[ダッシュボード（Dashboard）] ツールバーのリンクが含まれているものがあります。このリンクをクリックして、関連する事前定義されたダッシュボードを表示することができます。事前定義されたダッシュボードまたはタブを削除すると、関連付けられているツールバーのリンクが機能しなくなります。

マルチドメイン展開では、先祖ドメインのダッシュボードを表示することはできません。ただし、高位レベルのダッシュボードをコピーした新規のダッシュボードを作成することはできます。

Firepower システムのダッシュボード ウィジェット

ダッシュボードには 1 つ以上のタブがあり、それぞれのタブには、3 列のレイアウトで 1 つ以上のウィジェットを表示できます。Firepower システムには、事前定義された多数のダッシュボード ウィジェットが付属しています。それぞれのウィジェットは、Firepower システムのさまざまな側面を理解するうえで役に立ちます。ウィジェットは、次の 3 つのカテゴリに分類されます。

- [分析およびレポート（Analysis & Reporting）] ウィジェットは、Firepower システムで収集および生成されたイベントに関するデータを表示します。
- *[*その他（*Miscellaneous*）*]* ウィジェットは、イベント データもオペレーション データも表示しません。現時点では、このカテゴリのウィジェットのみが RSS フィードを表示します。
- [オペレーション（Operations）] ウィジェットは、Firepower システムのステータスおよび全体の正常性に関する情報を表示します。

表示されるダッシュボード ウィジェットは、次の項目に応じて異なります。

- 使用しているアプライアンスのタイプ
- ユーザ ロール
- 現在のドメイン（マルチドメイン展開内）

また、各ダッシュボードには、動作を決定する一連のプリファレンスがあります。

ユーザは、ウィジェットを最小化および最大化する、タブに対してウィジェットを追加および削除する、タブ上でウィジェットを再配置する、といったことができます。

（注） 所定の時間範囲でのイベント カウントを表示するウィジェットでは、[分析（Analysis）] メニューのページの表で利用できる詳細なデータのイベント数が、イベントの総数に反映されないことがあります。これは、ディスク領域の使用率を管理するために、古いイベントの詳細がシステムによってプルーニングされることがあるために発生します。イベント詳細のプルーニングを最小限にするために、対象の展開にとって最も重要なイベントだけを記録するようにイベント ロギングを調整できます。

ウィジェットの使用可能性

表示できるダッシュボード ウィジェットは、使用中のアプライアンスのタイプ、使用するユーザ ロール、および（マルチドメイン展開での）現在のドメインによって異なります。

マルチドメイン展開で、予期したウィジェットが表示されない場合、グローバル ドメインに切り替えます。Firepower Management Center のドメインの切り替え （12 ページ）を参照してください。

次の点に注意してください。

- 無効なウィジェットとは、ユーザが誤ったタイプのアプライアンスを使用しているために表示できないウィジェットのことです。
- 不正なウィジェットとは、ユーザ アカウントに必要な権限がないために表示できないウィジェットのことです。

たとえば、[アプライアンスの状態（Appliance Status）] ウィジェットを使用できるのは、FMC で、管理者（Administrator）、メンテナンス ユーザ（Maintenance User）、セキュリティ アナリスト（Security Analyst）、またはセキュリティ アナリスト（読み取り専用）（Security Analyst（Read Only））のアカウント権限を持つユーザだけです。

不正なウィジェットまたは無効なウィジェットはダッシュボードに追加できませんが、インポートしたダッシュボードに不正なウィジェットまたは無効なウィジェットが含まれていることがあります。たとえば、インポートしたダッシュボードが次の場合に、このようなウィジェットが含まれている可能性があります。

- 各種アクセス権限を持つユーザによって作成された場合、または
- 先祖ドメインに属している場合。

使用できないウィジェットは無効になり、それらのウィジェットを表示できない理由を示すエラー メッセージが表示されます。

これらのウィジェットがタイムアウトした場合、またはそれ以外で問題が発生した場合には、個々のウィジェットでもエラー メッセージが表示されます。

（注） 不正なウィジェットと無効なウィジェット、および表示するデータがないウィジェットは、削除または最小化できます。共有されているダッシュボード上でウィジェットを変更すると、アプライアンスのすべてのユーザのウィジェットも変更されることに注意してください。

ユーザ ロール別のダッシュボード ウィジェットの可用性

次の表に、各ウィジェットを表示するために必要なユーザ アカウントの権限を示します。Administrator、Maintenance User、Security Analyst、または Security Analyst（読み取り専用）のアクセス権を持つユーザ アカウントのみがダッシュボードを使用できます。

カスタム ロールを持つユーザは、自身のユーザ ロールの許可によって、ウィジェットのいずれかの組み合わせにアクセスできる場合もあれば、どのウィジェットにもアクセスできない場合もあります。

表 *34* : ユーザ ロールとダッシュボード ウィジェットの可用性

ウィジェット	Administrator	Maintenance User	Security Analyst	Security Analyst（RO）
Appliance Information	はい	はい	はい	はい
Appliance Status	はい	はい	はい	いいえ（No）
Correlation Events	はい	いいえ	はい	はい
Current Interface Status	はい	はい	はい	はい
Current Sessions	はい	いいえ	いいえ	いいえ
Custom Analysis	はい	いいえ	はい	はい
Disk Usage	はい	はい	はい	はい
Interface Traffic	はい	はい	はい	はい
Intrusion Events	はい	いいえ	はい	はい
Network Compliance	はい	いいえ	はい	はい
Product Licensing	はい	はい	いいえ	いいえ
Product Updates	はい	はい	いいえ	いいえ
RSS Feed	はい	はい	はい	はい

ウィジェット	Administrator	Maintenance User	Security Analyst	Security Analyst（RO）
System Load	はい	はい	はい	はい
System Time	はい	はい	はい	はい
White List Events	はい	いいえ	はい	はい

定義済みダッシュボード ウィジェット

Firepower システムには、いくつかの定義済みウィジェットが付属しています。これらのウィジェットをダッシュボード上で使用することで、現在のシステム ステータスを一目で確認できます。ウィジェットのビューには、以下の情報が表示されます。

- システムが収集および生成したイベントに関するデータ
- 使用している導入のアプライアンスのステータスと全体的なヘルスに関する情報

（注） 表示できるダッシュボード ウィジェットは、使用しているアプライアンスのタイプとユーザロール、およびマルチドメイン展開の場合は現在のドメインによって異なります。

[アプライアンス情報（Appliance Information）] ウィジェット

[アプライアンス情報（Appliance Information）] ウィジェットは、アプライアンスのスナップショットを提供します。このウィジェットは、Detailed Dashboard および Summary Dashboard の [Status] タブにデフォルトで表示されます。このウィジェットは以下の情報を提供します。

- アプライアンスの名前、IPv4 アドレス、IPv6 アドレス、およびモデル
- ダッシュボードでアプライアンスにインストールされている、Firepower システム ソフトウェア、オペレーティング システム、Snort、ルール アップデート、ルール パック、モジュール パック、脆弱性データベース（VDB）、および地理情報のアップデートのバージョン（仮想 Firepower Management Center は除く）
- 管理対象アプライアンスの場合は、管理アプライアンスとの通信リンクの名前とステータス

単純なビューまたは高度なビューを表示するようにウィジェットのプリファレンスを変更することで、ウィジェットで表示する情報量を調整できます。プリファレンスでは、ウィジェットをアップデートする頻度を調整することもできます。

[アプライアンス ステータス（Appliance Status）] ウィジェット

[アプライアンス ステータス（Appliance Status）] ウィジェットは、アプライアンスの正常性、およびそのアプライアンスが管理しているアプライアンスの正常性を示します。Firepower

Management Centerは、管理対象のデバイスに対して自動的に正常性ポリシーを適用しないため、ユーザは正常性ポリシーをデバイスへ手動で適用する必要があります。このようにしないと、デバイスのステータスは `Disabled` として示されます。このウィジェットは、Detailed Dashboard および Summary Dashboard の [Status] タブにデフォルトで表示されます。

ウィジェットのプリファレンスを変更して、アプライアンスのステータスを円グラフまたは表で表示するように設定できます。

プリファレンスでは、ウィジェットをアップデートする頻度も調整されます。

円グラフの一部、またはアプライアンス ステータス表のいずれかの数字をクリックすると、[ヘルス モニタ（Health Monitor）] ページが表示され、対象のアプライアンス、およびそのアプライアンスが管理しているすべてのアプライアンスのコンパイル済みの正常性ステータスを参照することができます。

[相関イベント（Correlation Events）] ウィジェット

[相関イベント（Correlation Events）] ウィジェットは、ダッシュボードの時間範囲における 1 秒あたりの相関イベントの平均数を、優先度ごとに示します。このウィジェットは、詳細ダッシュボードの [相関（Correlation）] タブにデフォルトで表示されます。

ウィジェットを設定して、線形（増分）や対数（10 の倍数）のスケールを選択するだけでなく、ウィジェットの設定を変更してさまざまな優先度の相関イベントを表示することができます。

優先度を持たないイベントも含めて、特定の優先度のイベントに対して別のグラフを表示するには、1 つ以上の [優先順位（Priorities）] チェックボックスをオンにします。優先度に関係なくすべての相関イベントに対して追加のグラフを表示するには、[すべて表示（Show All）] を選択します。プリファレンスでは、ウィジェットをアップデートする頻度も調整されます。

グラフをクリックして特定の優先度の相関イベントを表示することも、[すべて（All）] グラフをクリックしてすべての相関イベントを表示することもできます。いずれの場合も、イベントはダッシュボードの時間範囲に制限されます。ダッシュボードを介して相関イベントにアクセスすると、そのアプライアンスに対するイベント（またはグローバル）の期間が変わります。

[現在のインターフェイス ステータス（Current Interface Status）] ウィジェット

[現在のインターフェイス ステータス（Current Interface Status）] ウィジェットは、有効になっているか未使用のアプライアンスのすべてのインターフェイスのステータスを示します。Firepower Management Center では、管理（`eth0`、`eth1` など）インターフェイスを表示できます。管理対象デバイスでは、センシング（`s1p1` など）インターフェイスのみを表示するか、または管理インターフェイスとセンシング インターフェイスの両方を表示するかを選択できます。インターフェイスは、タイプ（管理、インライン、パッシブ、スイッチド、ルーテッド、スタック、未使用）別にグループ化されます。

ウィジェットは、各インターフェイスに対して次の情報を提供します。

- インターフェイスの名前
- インターフェイスのリンク状態

- インターフェイスのリンク モード（100Mb 全二重、または 10Mb 半二重など）
- インターフェイスのタイプ（銅線または光ファイバ）
- インターフェイスで受け取ったデータ量（Rx）および送信したデータ量（Tx）

リンクの状態を表すボールの色は、次のように現在のステータスを示します。

- 緑色：リンクはフルスピードでアップ状態です
- 黄色：リンクはアップ状態ですがフルスピードではありません
- 赤色：リンクはアップ状態ではありません
- 灰色：リンクは管理上無効になっています
- 青色：リンク ステート情報は使用可能ではありません（たとえば、ASA）

ウィジェットのプリファレンスでは、ウィジェットをアップデートする頻度を調整します。

[現在のセッション（Current Sessions）] ウィジェット

[現在のセッション（Current Sessions）] ウィジェットは、アプライアンスに現在ログインしているユーザ、セッションが生じたマシンに関連付けられている IP アドレス、各ユーザがアプライアンス上のページにアクセスした最後の（アプライアンスのローカル時間に基づいた）時間を示します。自分を表すユーザ（現在ウィジェットを表示しているユーザ）には、ユーザアイコン（  ）のマークが付けられ、太字で示されます。ログオフするか非アクティブになってから 1 時間以内に、セッションはこのウィジェットのデータからプルーニングされます。このウィジェットは、Detailed Dashboard および Summary Dashboard の [Status] タブにデフォルトで表示されます。

[現在のセッション（Current Sessions）] ウィジェットでは、次のことができます。

- いずれかのユーザ名をクリックして、[ユーザ管理（User Management）] ページでユーザアカウントを管理します。
- ホスト アイコン（  ）、または IP アドレスの隣の侵害されたホスト アイコン（  ）をクリックして、関連付けられているマシンのホスト プロファイルを表示します。
- いずれかの IP アドレスまたはアクセス時間をクリックして、その IP アドレスおよびその IP アドレスに関連付けられているユーザが Web インターフェイスにログオンした時間によって制約される監査ログを表示します。

ウィジェットのプリファレンスでは、ウィジェットをアップデートする頻度を調整します。

[カスタム分析（Custom Analysis）] ウィジェット

[カスタム分析（Custom Analysis）] ウィジェットは高度にカスタマイズ可能なウィジェットで、これを使用すると、Firepower システムで収集および生成されたイベントの詳細情報を表示できます。

このウィジェットには複数のプリセットが用意されており、導入に関する情報にすばやくアクセスできます。事前定義済みのダッシュボードから、これらのプリセットを幅広く使用できます。これらのプリセットを使用することも、カスタム設定を作成することもできます。カスタム構成では少なくとも、関心のあるデータ（表とフィールド）とそのデータの集計方法を指定します。イベントの相対的な発生数を表示するのか（棒グラフ）、一定期間のイベント数を表示するのか（折れ線グラフ）など、その他の表示関連の設定を適用することもできます。

このウィジェットは、ローカル時間に基づいて、最後にアップデートされた時間を表示します。ウィジェットのアップデートは、ダッシュボードの時間範囲に基づいた頻度で実行されます。たとえば、ダッシュボードの時間範囲を 1 時間に設定すると、ウィジェットは 5 分ごとにアップデートされます。また、ダッシュボードの時間範囲を 1 年に設定すると、ウィジェットは 1 週間ごとにアップデートされます。ダッシュボードが次にアップデートされるタイミングを設定するには、ウィジェットの左下にある [最終更新日（Last updated）] の通知にポインタを移動します。

（注） [カスタム分析（Custom Analysis）] ウィジェットに赤い影が付いている場合は、そのウィジェットの使用がシステムのパフォーマンスに悪影響を及ぼしています。ウィジェットが長時間赤い状態のままになっている場合は、そのウィジェットを削除してください。また、システム構成（**[システム（System）] > [設定（Configuration）] > [ダッシュボード（Dashboard）]**）のダッシュボード設定で、すべての [カスタム分析（Custom Analysis）] ウィジェットを無効にすることもできます。

イベントの相対的な発生数の表示（棒グラフ）

[カスタム分析（Custom Analysis）] ウィジェットの棒グラフでは、ウィジェットの背景の色付きバーが、各イベントの相対的な発生数を示します。バーは右から順にお読みください。

矢印のアイコン（▼）は、表示のソート順を示して、制御しています。下向きのアイコンは降順を表し、上向きのアイコンは昇順を表します。ソート順を変更するには、アイコンをクリックします。

最新の結果以降何らかの変更点があることを示すために、ウィジェットでは、各イベントの横に次の 3 つのアイコンのうちの 1 つを表示します。

- 新しいイベント アイコン（  ）は、イベントが、最新の結果以降のものであることを示します。
- 上向き矢印のアイコン（  ）は、ウィジェットが最後にアップデートされた後で、イベントがこの場所に上がってきたことを示します。イベントが何段階上がってきたかを表す数字が、アイコンの横に示されます。
- 下向き矢印のアイコン（  ）は、ウィジェットが最後にアップデートされた後で、イベントがこの場所に下がってきたことを示します。イベントが何段階下がってきたかを表す数字が、アイコンの横に示されます。

一定期間のイベントの表示（折れ線グラフ）

一定期間のイベントまたは収集されたその他のデータに関する情報が必要な場合は、対象の展開で、一定期間に発生した侵入イベントの合計数を表示するような線グラフを表示するように [カスタム分析（Custom Analysis）] ウィジェットを設定することができます。

[カスタム分析（Custom Analysis）] ウィジェットの制限

[カスタム分析（Custom Analysis）] ウィジェットは、表示するように設定されたデータを表示する権限がないことを示すことがあります。たとえば、メンテナンスユーザには検出イベントを表示する権限がありません。また、このウィジェットは、ライセンスされていない機能に関連する情報を表示しません。ただし、そのユーザ（およびダッシュボードを共有している他のユーザ）は、ウィジェットの設定を変更して、自分が表示できるデータを表示することも、ウィジェットを削除することもできます。これを防ぐには、ダッシュボードをプライベート（非公開）で保存します。

ユーザ データを表示した場合は、権限のあるユーザのみが表示されます。

URL カテゴリ情報を表示した場合、分類されていない URL は表示されません。

[カウント（Count）] で集約された侵入イベントを表示すると、カウントには侵入イベントに関して確認済みのイベントが含められます。[分析（Analysis）] のページのテーブルにカウントを表示すると、カウントに確認済みイベントは含められません。

（注） マルチドメイン展開では、システムは、各リーフ ドメインに個別のネットワーク マップを作成します。その結果、リーフ ドメインには、ネットワーク内で一意である IP アドレスを含めることができますが、別のリーフ ドメイン内の IP アドレスと同じにすることができます。先祖ドメインで [カスタム分析（Custom Analysis）] ウィジェットを表示すると、繰り返し使用される IP アドレスの複数のインスタンスを表示できます。一見すると、エントリが重複しているように見えることがあります。ただし、各 IP アドレスのホスト プロファイル情報までドリル ダウンすると、それらが異なるリーフ ドメインに属していることがわかります。

例：カスタム構成

最近の侵入イベントのリストを表示するように [カスタム分析（Custom Analysis）] ウィジェットを設定するには、[侵入イベント（Intrusion Events）] テーブルのデータを表示するようにウィジェットを設定します。[分類（Classification）] フィールドを選択し、このデータを [カウント（Count）] で集約すると、各タイプのイベントがいくつ生成されたかが通知されます。

一方、[一意のイベント（Unique Events）] で集約すると、各タイプで一意の侵入イベントがいくつ発生したかが通知されます（たとえばネットワークの Trojan、企業ポリシーの潜在的な違反、行われたサービス妨害攻撃の検出個数など）。

ウィジェットをさらに制約するには、保存されている検索（アプライアンスに付属している事前定義の検索、またはユーザが作成したカスタム検索のいずれか）を使用します。たとえば、最初の例（[分類（Classification）] フィールドを使用して [カウント

（Count）] で集約する）を、[ドロップされたイベント（Dropped Events）] の検索を使用して制約すると、各タイプの侵入イベントがいくつドロップされたかが通知されます。

関連トピック

ダッシュボードの時刻設定の変更 （345 ページ）

[カスタム分析（Custom Analysis）]ウィジェットのプリファレンス

次の表に、[カスタム分析（Custom Analysis）]ウィジェットで設定できるプリファレンスについて示します。

さまざまなプリファレンスは、ウィジェットを設定する方法に応じて表示されます。たとえば、イベントの相対頻度（棒グラフ）を表示する場合と、時系列のグラフ（線グラフ）を表示する場合とでは、ウィジェットの設定時に異なるプリファレンスセットが表示されます。フィルタなど、一部のプリファレンスは、表示するデータが存在する特定のテーブルを選択する場合にのみ表示されます。

表 *35 : [*カスタム分析（*Custom Analysis***）*]*ウィジェットのプリファレンス**

設定	詳細
タイトル（Title）	ウィジェットのタイトルを指定しない場合、システムは、設定済みのイベントタイプをタイトルとして使用します。
プリセット（Preset）	[カスタム分析（Custom Analysis）]のプリセットによって、展開に関する情報に簡単にアクセスできます。事前定義済みのダッシュボードから、これらのプリセットを幅広く使用できます。これらのプリセットを使用することも、カスタム設定を作成することもできます。
テーブル（Table）（必須）	ウィジェットが表示するデータを含むイベントまたはアセットのテーブル。
フィールド（Field）（必須）	表示するイベント タイプの特定のフィールド。時系列でデータ（線グラフ）を表示するには、[時間（Time）] を選択します。イベントの相対頻度（棒グラフ）を表示するには、もう一方のオプションを選択します。
集約（Aggregate）（必須）	集約方法は、表示するデータをウィジェットがどのようにグループ化するかを設定します。ほとんどのイベント タイプのデフォルト オプションは [カウント（Count）] です。
フィルタ（Filter）	[アプリケーション統計（Application Statistics）] および [アプリケーション別の侵入イベント統計（Intrusion Event Statistics by Application）] テーブルのデータを制約するには、アプリケーション フィルタを使用できます。

設定	詳細
検索（Search）	保存した検索を使用して、ウィジェットが表示するデータを制約することができます。検索を指定する必要はありませんが、プリセットの中には事前定義された検索が使用されるものがあります。 ユーザがアクセスできる検索は、プライベートで保存した検索だけです。共有ダッシュボード上にウィジェットを設定し、プライベートの検索を使用してイベントを制約すると、ウィジェットは、他のユーザがログインしたときにその検索を使用しないようにリセットされます。ウィジェットのビューにも影響します。これを防ぐには、ダッシュボードをプライベート（非公開）で保存します。 接続イベントに基づいて[カスタム分析（Custom Analysis）] ダッシュボード ウィジェットを制約できるのは、接続サマリーを制限しているフィールドだけです。保存した無効な検索はグレー表示されます。 保存されている検索を使用して [カスタム分析（Custom Analysis）] ウィジェットを制約し、その後で検索を編集すると、次にアップデートされるまでウィジェットには変更が反映されません。
表示（Show）	最も高い（[最上位（Top）]）または最も低い（[最下位（Bottom）]）頻度で発生するイベントを表示するかどうかを選択します。
結果（Results）	表示する結果の行数を選択します。
Mover の表示（Show Movers）	最新の結果以降の変更を示すアイコンを表示するかどうかを選択します。
タイム ゾーン	結果の表示に使用するタイム ゾーンを選択します。
カラー（Color）	ウィジェットの棒グラフのバーの色を変更できます。

関連トピック

ウィジェットの設定 （341 ページ）

Custom Analysis ウィジェットから関連付けられているイベントを表示する

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Any Security Analyst/Maint

Custom Analysis ウィジェットから、ウィジェットに表示されるイベントに関する詳細情報を提供するイベント ビュー（ワークフロー）を起動することができます。イベントは、ダッシュボードの時間範囲によって制限されて、そのイベントタイプのデフォルトのワークフローで表示されます。設定した時間枠の数やイベント タイプに応じて、Firepower Management Center の時間枠が適宜変更されます。

次に例を示します。

- 複数の期間が設定されている場合に、Custom Analysis ウィジェットからヘルス イベントにアクセスすると、デフォルトのヘルス イベント ワークフローにイベントが表示され、ヘルス モニタリング期間はダッシュボードの時間範囲に変更されます。
- 1 つの時間枠を設定していて Custom Analysis ウィジェットから任意のタイプのイベントにアクセスすると、イベントはそのイベントタイプのデフォルト ワークフローに表示され、グローバル期間がダッシュボードの時間範囲に変更されます。

次の選択肢があります。

- Custom Analysis ウィジェットの右下にあるすべて表示のアイコン（  ）をクリックして、ウィジェットの設定で制約して、すべての関連イベントを表示することができます。
- 関連するイベントの発生数（棒グラフ）を表示するように設定された Custom Analysis ウィジェットで、任意のイベントをクリックして、ウィジェットの設定、およびそのイベントで制約して、関連イベントを表示します。

[ディスク使用量（Disk Usage）] ウィジェット

[ディスク使用量（Disk Usage）] ウィジェットは、ディスク使用率のカテゴリに基づいて、ハードドライブで使用される領域のパーセンテージを表示します。また、アプライアンスのハードドライブの各パーティションで使用される領域のパーセンテージおよび容量も示します。[ディスク使用量（Disk Usage）] ウィジェットがデバイスにインストールされている場合、または Firepower Management Center が、マルウェア ストレージ パックが含まれているデバイスを管理している場合、[ディスク使用量（Disk Usage）] ウィジェットはマルウェア ストレージ パックについて同じ情報を表示します。このウィジェットは、デフォルト ダッシュボードおよびサマリ ダッシュボードの [ステータス（Status）] タブにデフォルトで表示されます。

[カテゴリ別（By Category）] スタック バーは、各ディスク使用率のカテゴリを、使用可能な合計ディスク領域に対する使用量の割合として表示します。次の表で、使用可能なカテゴリについて説明します。

表 *36* : ディスク使用率のカテゴリ

Disk Usage のカテゴリ	説明
Events	システムで記録されたすべてのイベント
Files	システムに格納されたすべてのファイル

Disk Usage のカテゴリ	説明
Backups	すべてのバックアップ ファイル
Updates	ルールのアップデートやシステムのアップデートなど、アップデートに関連するすべてのファイル
Other	システムのトラブルシューティング ファイルおよびその他のファイル
Free	アプライアンス上の残りの空き領域

By Category スタック バーのディスク使用率カテゴリにポインタを合わせると、使用可能なディスク領域のうち、そのカテゴリで使用された領域の割合、ディスク上の実際のストレージ領域、およびそのカテゴリで使用可能なディスク領域の合計を表示することができます。マルウェア ストレージ パックがインストールされている場合、[ファイル（Files）] カテゴリで使用できるディスク領域の合計は、マルウェア ストレージ パックで使用できるディスク領域になることに注意してください。

ウィジェットのプリファレンスを変更して、[カテゴリ別（By Category）] スタック バーのみを表示したり、スタック バーと admin（/）、/Volume、および /boot パーティションの使用率や、マルウェア ストレージ パックがインストールされている場合は /var/storage パーティションを表示したりするようにウィジェットを設定できます。

ウィジェットのプリファレンスは、ウィジェットのアップデート頻度、およびダッシュボードの時間範囲で現在のディスク使用率または収集したディスク使用率の統計のいずれかを表示するかも制御します。

[インターフェイス トラフィック（Interface Traffic）] ウィジェット

[インターフェイス トラフィック（Interface Traffic）] ウィジェットには、アプライアンスのインターフェイスで送受信された受信（Rx）トラフィックと送信（Tx）トラフィックの割合が示されます。7000 & 8000 シリーズ デバイスの場合、ウィジェットにはセンシング インターフェイスに関する情報も表示されます。このウィジェットは、事前定義されたダッシュボードにデフォルトでは表示されません。

マルウェア ライセンスが有効になっているデバイスは、動的分析を設定していない場合でも、定期的に AMP クラウドへの接続を試行します。そのため、これらのデバイスには送信トラフィックが表示されます。これは想定されている動作です。アウトバウンド（送信）トラフィックには、フロー制御パケットが含まれます。そのため、7000 & 8000 シリーズ デバイス上のパッシブ センシング インターフェイスには、送信トラフィックが表示されることがあり、これもまた想定されている動作です。

ウィジェットのプリファレンスでは、ウィジェットをアップデートする頻度を調整します。7000 & 8000 シリーズ デバイスでは、設定によって、使用されていないインターフェイスのトラフィック レートをウィジェットに表示するかどうかも制御します（デフォルトでは、ウィジェットにはアクティブなインターフェイスのトラフィック レートのみが表示されます）。

[侵入イベント（Intrusion Events）] ウィジェット

[侵入イベント（Intrusion Events）] ウィジェットは、ダッシュボードの時間範囲で発生した侵入イベントを、優先度ごとに表示します。これには、ドロップされたパケットおよびさまざまな影響を含む、侵入イベントの統計が含まれています。このウィジェットは、サマリ ダッシュボードの [侵入イベント（Intrusion Events）] タブにデフォルトで表示されます。

ウィジェットの設定では、次のことができます。

- [イベント フラグ（Event Flags）] には、パケットが欠落したイベント、パケットが欠落した可能性のあるイベント、または特定の影響を示すグラフが個別に表示されます。影響やルールの状態に関係なくすべての侵入イベントに対して追加のグラフを表示するには、[すべて（All）] を選択します。

  アイコンの説明については、侵入イベントの操作（3057ページ）を参照してください。影響レベルの数字の上に表示される矢印（ある場合）はインライン結果を表すもので、次のように定義されています。

  表 *37* : ワークフロー ビューテーブル ビューの *[インライン結果（Inline Result）]* フィールドの内容

アイコン	意味
黒の下矢印	ルールをトリガーとして使用したパケットをシステムがドロップしました
グレーの下矢印	[インライン時にドロップ（Drop when Inline）] 侵入ポリシー オプション（インライン展開環境）を有効にした場合、またはシステムがプルーニングしている間に [ドロップしてイベントを生成する（Drop and Generate）] ルールがイベントを生成した場合、IPS がパケットをドロップしたことを示します
アイコンなし（空白）	トリガーされたルールは [ドロップしてイベントを生成する（Drop and Generate Events）] に設定されていませんでした

  パッシブ展開では、侵入ポリシーのルールの状態やインライン ドロップ動作に関係なく、インライン インターフェイスがタップ モードの場合を含めて、システムはパケットをドロップしません。

- [表示（Show）] では、[1秒あたりの平均イベント数（Average Events Per Second）]（EPS）または [イベントの合計数（Total Events）] を選択できます。
- [縦方向スケール（Vertical Scale）] では、[線形（Linear）]（増分）または [対数（Logarithmic）]（10 の倍数）のスケールを選択できます。
- ウィジェットの更新頻度。

ウィジェットでは次のことができます。

- ドロップされたパケット、ドロップされた可能性のあるパケット、または特定の影響に対応するグラフをクリックして、そのタイプの侵入イベントを表示します。

- ドロップされたイベントに対応するグラフをクリックして、ドロップされたイベントを表示します。
- ドロップされたと考えられるイベントに対応するグラフをクリックして、ドロップされたと考えられるイベントを表示します。
- [すべて（All）] グラフをクリックして、すべての侵入イベントを表示します。

結果のイベント ビューは、ダッシュボードの時間範囲に制約されます。ダッシュボードを介して侵入イベントにアクセスすると、そのアプライアンスに対するイベント（またはグローバル）の期間が変わります。侵入ルールの状態または侵入ポリシーのインライン ドロップ動作に関係なく、パッシブな配置のパケットはドロップされないことに注意してください。

[ネットワーク コンプライアンス（Network Compliance）] ウィジェット

[ネットワーク コンプライアンス（Network Compliance）] ウィジェットは、ユーザが設定したホワイト リストに対するホストのコンプライアンスを要約します。デフォルトではこのウィジェットに、アクティブな相関ポリシーにおけるすべてのコンプライアンス ホワイト リストに対して準拠しているホスト、準拠していないホスト、および評価されなかったホストの数を示す円グラフが表示されます。このウィジェットは、Detailed Dashboard の [Correlation] タブにデフォルトで表示されます。

ウィジェットのプリファレンスを変更して、すべてのホワイトリスト、または特定のホワイトリストのいずれかについてネットワーク コンプライアンスを表示するようにウィジェットを設定できます。

すべてのホワイトリストに対してネットワーク コンプライアンスを表示するよう選択すると、あるホストが、アクティブな相関ポリシーのいずれのホワイト リストにも準拠していない場合、ウィジェットはそのホストが非準拠であるとみなします。

また、このウィジェットのプリファレンスを使用すると、ネットワーク コンプライアンスの表示で次の 3 つのスタイルのうちどれを使用するかを指定することができます。

[Network Compliance] スタイル（デフォルト）は、準拠しているホスト、準拠していないホスト、および評価されなかったホストの数を示す円グラフを表示します。ホストの違反の件数を表示するには、円グラフをクリックします。このようにすると、少なくとも 1 つのホワイトリストに違反しているホストが表示されます。

[一定期間のネットワーク コンプライアンス（%）（Network Compliance over Time (%)）] スタイルは、ダッシュボードの時間範囲において準拠しているホスト、準拠していないホスト、およびまだ評価されていないホストの相対的な割合を示す積み重ね面積グラフを表示します。

[Network Compliance over Time] スタイルは、ダッシュボードの時間範囲において準拠しているホスト、準拠していないホスト、およびまだ評価されていないホストの数を示す線グラフを表示します。

プリファレンスは、ウィジェットをアップデートする頻度を調整します。まだ評価されていないイベントを非表示にするには、[未評価を表示（Show Not Evaluated）] ボックスをオンにします。

[製品ライセンス（Product Licensing）] ウィジェット

[製品ライセンス（Product Licensing）] ウィジェットは、Firepower Management Center に現在インストールされているデバイスおよび機能のライセンスを示します。また、ライセンス契約されているアイテムの数、許可される残りのライセンス契約アイテム数も示します。これは、事前定義されたどのダッシュボードにおいてもデフォルトでは表示されません。

このウィジェットの上部のセクションには、一時的なライセンスも含めて、Firepower Management Center にインストールされているすべてのデバイスおよび機能のライセンスが表示されますが、[期限の切れたライセンス（Expiring Licenses）] セクションには、一時的なライセンスおよび期限の切れたライセンスのみが表示されます。

ウィジェットの背景のバーは、使用中のライセンスのそれぞれのタイプの割合を示しています。このバーは右から左へ読みます。期限の切れたライセンスには、取り消し線が付けられています。

ウィジェットのプリファレンスを変更して、現在ライセンス契約されている機能を表示するか、またはライセンス契約が可能なすべての機能を表示するようにウィジェットを設定することができます。プリファレンスでは、ウィジェットをアップデートする頻度も調整されます。

任意のライセンス タイプをクリックすると、ローカル設定の [ライセンス（License）] ページに移動して、機能ライセンスを追加または削除することができます。

[製品更新（Product Updates）] ウィジェット

[製品更新（Product Updates）] ウィジェットは、アプライアンスに現在インストールされているソフトウェアの概要、およびダウンロード済みだがまだインストールしていない更新プログラムの情報を提供します。このウィジェットは、詳細ダッシュボードおよびサマリ ダッシュボードの [ステータス（Status）] タブにデフォルトで表示されます。

このウィジェットは、スケジュールされたタスクを使用して最新バージョンを判別するため、更新プログラムをダウンロード、プッシュ、またはインストールするようにスケジュールされたタスクを構成するまで、`Unknown` と表示されます。

ウィジェットのプリファレンスを変更して、最新のバージョンを非表示にするようウィジェットを設定できます。プリファレンスでは、ウィジェットをアップデートする頻度も調整されます。

このウィジェットには、ソフトウェアを更新できるページへのリンクもあります。次の操作を実行できます。

- 現在のバージョンをクリックして、アプライアンスを手動で更新します。
- 最新バージョンをクリックして、更新プログラムをダウンロードするタスクをスケジュールします。

[RSS フィード（RSS Feed）] ウィジェット

[RSS フィード（RSS Feed）] ウィジェットは、ダッシュボードに RSS フィードを追加します。デフォルトでは、ウィジェットはシスコのセキュリティ ニュースのフィードを示します。この

ウィジェットは、詳細ダッシュボードおよびサマリ ダッシュボードの [ステータス（Status）] タブにデフォルトで表示されます。

また、企業ニュース、Snort.org ブログ、または Cisco 脅威調査ブログの事前設定済みのフィードを表示するようウィジェットを設定することができます。ウィジェットの設定で URL を指定して、他の RSS フィードに対するカスタム接続を作成することもできます。

フィードは 24 時間ごとに更新されます（ただしユーザはフィードを手動で更新できます）。また、ウィジェットはアプライアンスのローカル時間に基づいて、フィードが最後に更新された時間を表示します。アプライアンスは、（事前設定された 2 つのフィードについて）Web サイトに対するアクセス権を持っている、または設定したいずれかのカスタム フィードに対するアクセス権を持っている必要があります。

ウィジェットを設定する場合には、フィードからいくつのストーリーをウィジェットに表示するか、およびヘッドラインとともにストーリーの説明を表示するかどうかを選択することができます。ただしすべての RSS フィードで説明が使用できるわけではないことに注意してください。

RSS Feed ウィジェットでは、次のことができます。

- フィード内のストーリーのいずれかをクリックして、ストーリーを表示します
- [more] リンクをクリックして、フィードの Web サイトへ移動します
- 更新アイコン（）をクリックして、フィードを手動で更新します

[システム負荷（System Load）] ウィジェット

[システム負荷（System Load）] ウィジェットは、アプライアンス上の（各 CPU についての）CPU の使用率、メモリ（RAM）の使用率、およびシステムの負荷（実行を待機しているプロセスの数によって測定され、負荷平均とも呼ばれる）を現在、およびダッシュボードの時間範囲について表示します。このウィジェットは、Detailed Dashboard および Summary Dashboard の [Status] タブにデフォルトで表示されます。

ウィジェットのプリファレンスを変更して、負荷平均を表示または非表示にするようウィジェットを設定できます。プリファレンスでは、ウィジェットをアップデートする頻度も調整されます。

[システム時刻（System Time）] ウィジェット

[システム時刻（System Time）] ウィジェットは、アプライアンスのローカル システム時間、稼動時間、およびブート時間を表示します。このウィジェットは、Detailed Dashboard および Summary Dashboard の [Status] タブにデフォルトで表示されます。

ウィジェットのプリファレンスを変更して、ブート時間を非表示にするようウィジェットを設定できます。プリファレンスは、ウィジェットがアプライアンスの時計と同期する頻度も調整します。

[ホワイト リスト イベント（White List Events）] ウィジェット

[ホワイト リスト イベント（White List Events）] ウィジェットは、ダッシュボードの時間範囲における1秒あたりの平均イベント数を、優先度別に表示します。このウィジェットは、Default Dashboard の [Correlation] タブにデフォルトで表示されます。

ウィジェットのプリファレンスを変更して、さまざまな優先度のホワイト リスト イベントを表示するようウィジェットを設定できます。

ウィジェットの設定では、次のことができます。

- 優先度を持たないイベントも含めて、特定の優先度のイベントに対して別のグラフを表示するには、1 つ以上の [優先順位（Priorities）] チェックボックスをオンにします。
- 優先度に関係なくすべてのホワイト リスト イベントに対して追加のグラフを表示するには、[すべて表示（Show All）] を選択します。
- [縦方向スケール（Vertical Scale）] を選択して、[線形（Linear）]（増分）または [対数（Logarithmic）]（10 の倍数）のスケールを選択します。

プリファレンスでは、ウィジェットをアップデートする頻度も調整されます。

グラフをクリックして特定の優先度のホワイト リスト イベントを表示することも、[すべて（All）] グラフをクリックしてすべてのホワイトリストイベントを表示することもできます。いずれの場合も、イベントは、ダッシュボードの時間範囲によって制約されます。ダッシュボードを介してホワイト リストイベントにアクセスすると、Firepower Management Center に対するイベント（またはグローバル）の期間が変わります。

ダッシュボードの管理

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Any Security Analyst/Maint

ステップ 1 **[Overview]** > **[Dashboards]** を選択して、変更するダッシュボードをメニューから選択します。

ステップ 2 ダッシュボードを管理します。

- ダッシュボードの作成：カスタム ダッシュボードを作成します。カスタム ダッシュボードの作成 （341 ページ）を参照してください。
- ダッシュボードの削除：ダッシュボードを削除するには、削除するダッシュボードの横にある削除アイコン（）をクリックします。デフォルトのダッシュボードを削除する場合は、新しいデフォルトを定義する必要があります。そうしない場合、ダッシュボードを表示しようとするたびに、アプライアンスからダッシュボードを選択するように要求されます。

- オプションの編集：カスタムのダッシュボードオプションを編集します。ダッシュボードオプションの編集 （344 ページ）を参照してください。
- 時間の制約の変更：ダッシュボードの表示時間または一時停止/一時停止解除の時間を変更します。詳細は、ダッシュボードの時刻設定の変更 （345 ページ）を参照してください。

ステップ 3 ダッシュボードのタブを管理します。

- タブの追加：ダッシュボードにタブを追加します。ダッシュボード タブの追加 （339 ページ）を参照してください。
- タブの削除：ダッシュボードのタブを削除するには、タブの右上隅にある閉じるアイコン（ ）をクリックし、[OK] をクリックして確認します。ダッシュボードから最後のタブを削除することはできません。各ダッシュボードには少なくとも 1 つのタブが必要です。
- タブの名前変更：ダッシュボードのタブの名前を変更します。ダッシュボード タブの名前の変更 （346 ページ）を参照してください。

（注） ダッシュボードのタブの順序は変更できません。

ステップ 4 ダッシュボード ウィジェットを管理します。

- ウィジェットの追加：ダッシュボードにウィジェットを追加します。ダッシュボードへのウィジェットの追加 （340 ページ）を参照してください。
- プリファレンスの設定：ウィジェットのプリファレンスを設定します。ウィジェットの設定 （341 ページ）を参照してください。
- 表示のカスタマイズ：ウィジェットの表示をカスタマイズします。ウィジェット表示のカスタマイズ （344 ページ）を参照してください。
- イベントの表示：カスタム分析ウィジェットから関連するイベントを表示します。Custom Analysis ウィジェットから関連付けられているイベントを表示する （331 ページ）を参照してください。

ヒント シスコの事前定義のダッシュボード内のカスタム分析ウィジェットのすべての設定が、ウィジェットのシステム プリセットに対応しています。これらのウィジェットの 1 つを変更または削除した場合は、適切なプリセットをベースにして新しいカスタム分析ウィジェットを作成して復元することができます。

ダッシュボード タブの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Any Security Analyst/Maint

ステップ 1 変更するダッシュボードを表示します（ダッシュボードの表示 （346 ページ）を参照）。

ステップ 2 最後の既存のタブの横にある追加アイコン（ ）をクリックします。

ステップ 3 タブの名前を入力します。

ステップ 4 [OK] をクリックします。

ダッシュボードへのウィジェットの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Any Security Analyst/Maint

各タブには、3 列のレイアウトで 1 つ以上のウィジェットを表示できます。ダッシュボードにウィジェットを追加するには、ウィジェットを追加するタブを選択します。ウィジェットは、自動的にウィジェットが最も少ない列に追加されます。すべてのカラムに同じ数のウィジェットがある場合、新しいウィジェットは最も左のカラムに追加されます。ダッシュボードタブには最大 15 個のウィジェットを追加できます。

ヒント 追加したウィジェットは、タブの任意の場所に移動できます。ただし、別のタブにはウィジェットを移動できません。

表示されるダッシュボードウィジェットは、使用しているアプライアンスのタイプ、ユーザロールと（マルチドメイン環境では）現在のドメインにより異なります。すべてのユーザロールがすべてのダッシュボード ウィジェットに対してアクセス権を持っているわけではないため、多くの権限を持つユーザが作成したダッシュボードを、それよりも少ない権限を持つユーザが参照する場合、ダッシュボードのすべてのウィジェットを使用できないことがあることに注意してください。ダッシュボード上に、許可されていないウィジェットが表示されることがありますが、これらのウィジェットは無効です。

ステップ 1 ウィジェットを追加するダッシュボードを表示します。ダッシュボードの表示 （346 ページ） を参照してください。

ステップ 2 ウィジェットを追加するタブをクリックします。

ステップ 3 [ウィジェットの追加（Add Widgets）] をクリックします。カテゴリ名をクリックして各カテゴリのウィジェットを表示することも、[すべてのカテゴリ（All Categories）] をクリックしてすべてのウィジェットを表示することもできます。

ステップ 4 追加するウィジェットの横にある [追加（Add）] をクリックします。[ウィジェットの追加（Add Widgets）] ページには、追加するものも含め、各タブにあるウィジェットの数がタイプごとに表示されます。

ヒント （複数の RSS Feed ウィジェット、または複数の Custom Analysis ウィジェットを追加する場合など）同じタイプの複数のウィジェットを追加するには、[追加（Add）] をもう一度クリックします。

ステップ 5 ウィジェットの追加が終了したら、[完了（Done）] をクリックしてダッシュボードに戻ります。

次のタスク

- カスタム分析ウィジェットを追加した場合は、ウィジェットの設定が必要です。ウィジェットの設定 （341 ページ） を参照してください。

関連トピック

ウィジェットの使用可能性 （323 ページ）

ウィジェットの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Any Security Analyst/Maint

各ウィジェットには、動作を決定する一連のプリファレンスがあります。

ステップ 1 プリファレンスを変更するウィジェットのタイトル バーで、プリファレンスの表示アイコン（ ）をクリックします。

ステップ 2 必要に応じて変更を加えます。

ステップ 3 プリファレンスのセクションを非表示にするには、ウィジェットのタイトル バーで、プリファレンスの非表示アイコン（ ）をクリックします。

カスタム ダッシュボードの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Any Security Analyst/Maint

ヒント　新しいダッシュボードを作成する代わりに、別のアプライアンスからダッシュボードをエクスポートし、それを自分のアプライアンスへインポートすることができます。その後でニーズに合わせて、インポートしたダッシュボードを編集することができます。

ステップ 1　**[Overview]** > **[Dashboards]** > **[Management]**を選択します。

ステップ 2　[ダッシュボードの作成（Create Dashboard）] をクリックします。

ステップ 3　カスタム ダッシュボード オプション （342 ページ）の説明に従って、カスタム ダッシュボード オプションを変更します。

ステップ 4　**[保存（Save）]** をクリックします。

カスタム ダッシュボード オプション

次の表に、カスタム ダッシュボードを作成または編集するときに使用できるオプションを示します。

表 *38*：カスタム ダッシュボード オプション

オプション	説明
ダッシュボードのコピー（Copy Dashboard）	カスタム ダッシュボードを作成する場合は、ユーザが作成した、またはシステムで事前定義されている既存のダッシュボードをベースとして使用するよう選択できます。このオプションは、ニーズに合わせて変更できる、既存のダッシュボードのコピーを取ります。必要に応じて、[なし（None）] を選択することで、空白の新規ダッシュボードを作成できます。このオプションは、新しいダッシュボードを作成する場合のみ使用可能になります。 マルチドメイン展開では、先祖ドメインのプライベート以外のダッシュボードはコピーできます。
[名前（Name）]	カスタム ダッシュボードの固有名。
説明	カスタム ダッシュボードの簡単な説明。
タブを変更する間隔（Change Tabs Every）	ダッシュボードがそれぞれのタブを自動変更する頻度（分単位）を指定します。ダッシュボードを一時停止した場合や、ダッシュボードのタブが 1 つのみの場合を除き、この設定により、指定した間隔で次のタブが表示されます。タブの自動変更を無効にするには、[タブを変更する間隔（Change Tabs Every）] フィールドに 0 を入力します。

オプション	説明
ページを更新する間隔（Refresh Page Every）	現在のダッシュボードのタブを新しいデータで更新する頻度（分単位）を指定します。この値は、[タブを変更する間隔（Change Tabs Every）] の設定より大きい値にする必要があります。ダッシュボードを一時停止しない限り、この設定より、指定した間隔でダッシュボード全体が更新されます。定期的なページ更新を無効にするには、[ページを更新する間隔（Refresh Page Every）] フィールドに 0 を入力します。ダッシュボードのページ全体を自動的に更新する頻度を決定します。 ダッシュボード全体を更新すると、共有のダッシュボードに対して他のユーザが行ったプリファレンスまたはレイアウトの変更や、他のコンピュータ上のプライベート ダッシュボードに対して、ダッシュボードが最後に更新された後で自分が行った変更を確認できます。ダッシュボードが常に表示されているネットワーク オペレーション センター（NOC）などでは、頻繁な更新が有効です。ローカル コンピュータでダッシュボードの変更を行なえば、ユーザが指定する間隔で NOC のダッシュボードが自動的に更新されるため、手動による更新は必要ありません。データのアップデートを確認するためにダッシュボード全体を更新する必要はありません。個々のウィジェットはプリファレンスに従ってアップデートされます。 （注） この設定は、個々のウィジェットの多くで使用可能なアップデート間隔とは異なります。ダッシュボードのページを更新すると個々のウィジェットのアップデート間隔はリセットされますが、[ページを更新する間隔（Refresh Page Every）] 設定を無効にしていても、ウィジェットはそれ自身のプリファレンスに従ってアップデートされます。
プライベートとして保存（Save As Private）	カスタム ダッシュボードは、アプライアンスのすべてのユーザが表示および変更可能か、またはユーザ アカウントに関連付けて、独自の使用に限り予約可能かを決定します。ロールに関係なく、ダッシュボードへアクセスできるすべてのユーザは、共有ダッシュボードを変更できることに注意してください。特定のダッシュボードを自分のみが変更できるようにするには、そのダッシュボードをプライベートとして保存します。

ウィジェット表示のカスタマイズ

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Any Security Analyst/Maint

ウィジェットは、タブ上で最小化、最大化、および再配置することができます。

ステップ 1 ダッシュボードを表示します（ダッシュボードの表示 （346 ページ）を参照）。

ステップ 2 次のように、ウィジェット表示をカスタマイズします。

- タブ上でウィジェットを再配置するには、移動するウィジェットのタイトル バーをクリックし、新しい場所へドラッグします。

  （注） 別のタブにウィジェットを移動することはできません。ウィジェットを別のタブに表示する場合は、現在のタブからいったん削除してから新しいタブに追加する必要があります。

- ダッシュボードでウィジェットを最小化または最大化するには、ウィジェットのタイトル バーにある最小化（−）アイコンまたは最大化（□）アイコンをクリックします。
- ウィジェットをタブ上に表示する必要がなくなった場合にそのウィジェットを削除するには、ウィジェットのタイトル バーにある閉じるアイコン（✖）をクリックします。

ダッシュボード オプションの編集

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Any Security Analyst/Maint

ステップ 1 編集するダッシュボードを表示します（ダッシュボードの表示 （346 ページ）を参照）。

ステップ 2 変更するダッシュボードの横にある編集アイコン（  ）をクリックします。

ステップ 3 カスタム ダッシュボード オプション （342 ページ）の説明に従ってオプションを変更します。

ステップ 4 **[保存（Save）]** をクリックします。

ダッシュボードの時刻設定の変更

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Any Security Analyst/Maint

最短で 1 時間前（デフォルト）から、最長では 1 年前からの期間を反映するように時間範囲を変更できます。時間範囲を変更する場合は、時間によって制約される可能性のあるウィジェットが自動でアップデートされ、新しい時間範囲が反映されます。

すべてのウィジェットを時間で制約できるわけではないことに注意してください。たとえば、ダッシュボードの時間範囲は [アプライアンス情報（Appliance Information）] ウィジェットには影響を与えません。このウィジェットは、アプライアンスの名前、モデル、および Firepower システム ソフトウェアの現在のバージョンが含まれている情報を提供します。

企業による Firepower システムの展開では、新しいイベントが古いイベントを置き換える頻度によっては、時間範囲を長期に変更しても、[カスタム分析（Custom Analysis）] ウィジェットなどのウィジェットでは役立たない場合があることに注意してください。

また、ダッシュボードを一時停止することもできます。これにより変更を表示したり、分析を中断したりせずに、ウィジェットで提供されたデータを調べることができます。ダッシュボードを一時停止すると、次のような影響があります。

- Update Every ウィジェットのプリファレンスに関係なく、個々のウィジェットでアップデートが停止します。
- ダッシュボードのプロパティの [Cycle Tabs Every] 設定に関係なく、ダッシュボードのタブの自動変更が停止します。
- ダッシュボードのプロパティの [Refresh Page Every] 設定に関係なく、ダッシュボードのページの更新が停止します。
- 時間範囲を変更しても影響はありません。

分析が完了したら、ダッシュボードの一時停止を解除できます。ダッシュボードの一時停止を解除すると、ページ上で該当するすべてのウィジェットがアップデートされ、最新の時間範囲が反映されます。また、ダッシュボードのプロパティで指定した設定に従って、ダッシュボード タブの自動変更が再開され、ダッシュボード ページの更新が再開されます。

ダッシュボードに対するシステム情報のフローを中断するような接続の問題、または他の問題が発生した場合、ダッシュボードは自動的に一時停止し、問題が解決するまでエラー通知を表示します。

（注） ダッシュボードが一時停止しているかどうかに関係なく、セッションは通常、非アクティブな状態が1時間（または設定した他の時間）続いた場合、ユーザをログアウトします。ダッシュボードを長期間パッシブにモニタリングする場合は、一部のユーザをセッションタイムアウトしないよう設定したり、システムのタイムアウト設定を変更することを検討してください。

ステップ1 ウィジェットを追加するダッシュボードを表示します。ダッシュボードの表示 （346 ページ）を参照してください。

ステップ2 必要に応じて、ダッシュボードの時間範囲を変更するには、[表示経過時間（Show the Last）] ドロップダウンリストから時間範囲を選択します。

ステップ3 必要に応じて、一時停止（⏸）または再生アイコン（▶）を使用して、時間範囲コントロールでダッシュボードを一時停止または一時停止解除します。

ダッシュボード タブの名前の変更

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Any Security Analyst/Maint

ステップ1 変更するダッシュボードを表示します（ダッシュボードの表示 （346 ページ）を参照）。

ステップ2 名前を変更するタブのタイトルをクリックします。

ステップ3 タブの名前を入力します。

ステップ4 [OK] をクリックします。

ダッシュボードの表示

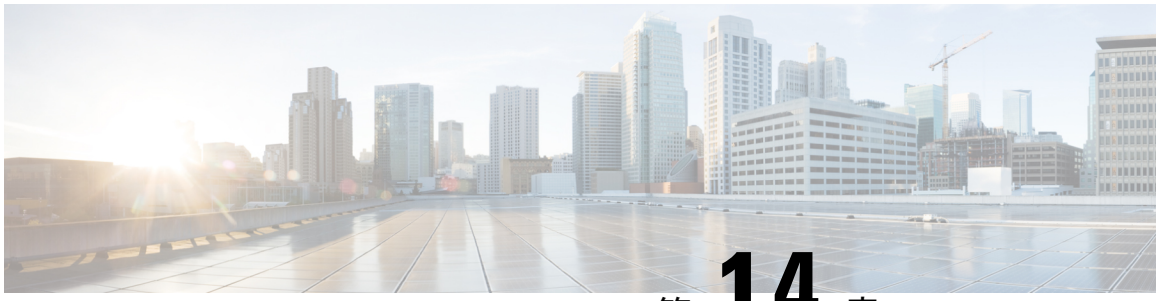
スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Any Security Analyst/Maint

デフォルトでは、アプライアンスのホームページにデフォルトのダッシュボードが表示されます。デフォルトのダッシュボードを定義していない場合は、ホーム ページに [ダッシュボード

の管理（Dashboard Management）] ページが示され、ここで表示するダッシュボードを選択できます。

いつでも次のいずれかの方法で操作できます。

- アプライアンスのデフォルト ダッシュボードを表示するには、**[Overview]** > **[Dashboards]** を選択します。
- 特定のダッシュボードを表示するには、**[Overview]** > **[Dashboards]** を選択し、メニューからダッシュボードを選択します。
- 利用可能なすべてのダッシュボードを表示するには、**[Overview]** > **[Dashboards]** > **[Management]** を選択します。個々のダッシュボードの横にある表示アイコン（  ）を選択すると、そのダッシュボードを表示できます。



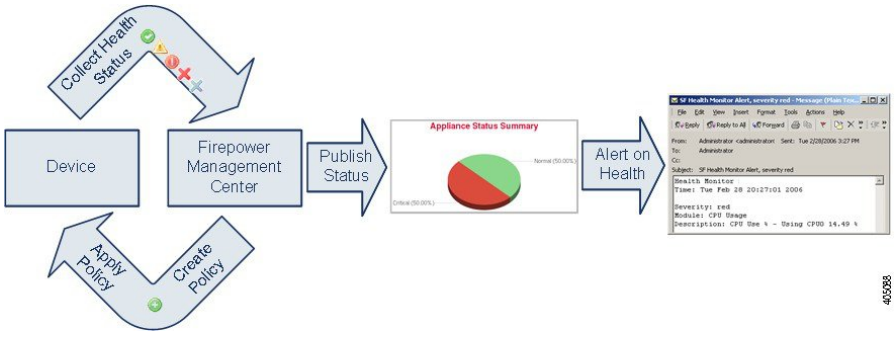
第 14 章

ヘルス モニタリング

次のトピックでは、Firepower システムでヘルス モニタリングを使用する方法について説明します。

ヘルス モニタリングについて

Firepower Management Center のヘルス モニタでは、さまざまなヘルス インジケータを追跡して Firepower システムのハードウェアとソフトウェアが正常に動作することを確認します。ヘルス モニタを使用して、Firepower システム展開全体の重要な機能のステータスを確認できます。



ヘルス モニタを使用すれば、正常性ポリシーとも呼ばれるテストのコレクションを作成し、正常性ポリシーを 1 つ以上のアプライアンスに適用できます。ヘルス モジュールとも呼ばれるテストは、指定された基準に照らしてテストするスクリプトです。テストを有効または無効にするか、テスト設定を変更することによって、正常性ポリシーを変更したり、不要になった正常

性ポリシーを削除したりできます。アプライアンスをブラックリストに登録することによって、選択したアプライアンスからのメッセージを抑制することもできます。

正常性ポリシー内のテストは設定された時間間隔で自動的に実行されます。すべてのテストを実行することも、オンデマンドで特定のテストを実行することもできます。ヘルス モニタは設定されたテスト条件に基づいてヘルス イベントを収集します。

（注） すべてのアプライアンスはハードウェア アラームのヘルス モジュール経由でハードウェアのステータスを自動的に報告します。また、Firepower Management Center はデフォルトの正常性ポリシーで設定されているモジュールを使用して自動的にステータスを報告します。アプライアンス ハートビートなどの一部の正常性モジュールは、Firepower Management Center 上で実行され Firepower Management Center の管理対象デバイスのステータスを報告します。ヘルス モジュールによっては、そのモジュールが設定されている正常性ポリシーをデバイスに適用しない限り管理対象デバイスのステータスを報告しないものもあります。

ヘルス モニタを使用してシステム全体、特定のアプライアンス、または特定のドメイン（マルチドメイン展開の場合）に関するヘルス ステータス情報にアクセスできます。[ヘルス モニタ（Health Monitor）] ページの円グラフとステータス テーブルには、Firepower Management Center を含むネットワーク上のすべてのアプライアンスのステータスの視覚的なサマリが示されます。個々のアプライアンスのヘルス モニタを使用すれば、特定のアプライアンスのヘルス詳細にドリルダウンできます。

完全にカスタマイズ可能なイベント ビューを使用すれば、ヘルス モニタによって収集されたヘルス ステータス イベントを迅速かつ容易に分析できます。このイベント ビューでは、イベントデータを検索して表示したり、調査中のイベントに関係する他の情報にアクセスしたりできます。たとえば、特定のパーセンテージの CPU 使用率の全記録を表示する場合は、CPU 使用率モジュールを検索して、パーセンテージ値を入力できます。

ヘルス イベントに対応した電子メール、SNMP、または syslog アラートを設定することもできます。ヘルス アラートは、標準アラートとヘルス ステータス レベルを関連付けたものです。たとえば、アプライアンスでハードウェアの過負荷が原因で障害が発生することは絶対ないことを確認する必要がある場合は、電子メール アラートをセットアップできます。その後で、CPU、ディスク、またはメモリの使用率がそのアプライアンスに適用される正常性ポリシーで設定された警告レベルに達するたびにその電子メールアラートをトリガーとして使用するヘルスアラートを作成できます。アラートしきい値を、受け取る反復アラートの数が最小になるように設定できます。

サポートから依頼された場合に、アプライアンスのトラブルシューティング ファイルを作成することもできます。

ヘルス モニタリングは管理活動であるため、管理者ユーザ ロール特権を持っているユーザのみがシステム ヘルス データにアクセスできます。

ヘルス モジュール

ヘルス モジュールまたはヘルス テストは、正常性ポリシーに指定した条件でテストします。

表 *39 :* ヘルス モジュール

モジュール	[アプライアンス（**Appliances**）]	説明
AMP for Endpoint のステータス	FMC	このモジュールは、FMC が初期接続の成功後に AMP クラウドまたは Cisco AMP Private Cloud に接続できない場合、またはプライベート クラウドがパブリック AMP クラウドに接続できない場合にアラートを出します。また、AMP for Endpoints 管理コンソールを使用して AMP クラウド接続の登録が解除された場合にもアラートを出します。
AMP for Firepower のステータス （ネットワーク向け AMP ステータス）	FMC	このモジュールは、以下の場合にアラートを出します。 • FMC が AMP クラウド（パブリックまたはプライベート）、Cisco Threat Grid パブリック クラウド、またはオンプレミス アプライアンスに接続できないか、または AMP プライベート クラウドがパブリック AMP クラウドに接続できない。 • 接続に使用する暗号化キーが無効である。 • デバイスが Cisco Threat Grid クラウドまたは Cisco Threat Grid オンプレミス アプライアンスに接続して動的分析用のファイルを送信できない。 • ファイル ポリシー設定に基づいてネットワーク トラフィックで過剰な数のファイルが検出された。 FMC のインターネット接続が切断された場合、ヘルスアラートの生成に最大 30 分かかることがあります。
アプライアンス ハートビート	任意（Any）	このモジュールは、アプライアンス ハートビートがアプライアンスから届いているかどうかを確認し、アプライアンスのハートビート ステータスに基づいてアラートを出します。
自動アプリケーション バイパス ステータス	7000 & 8000 シリーズ	このモジュールは、アプライアンスがバイパスしきい値で設定された秒数以内に応答しなかったためにバイパスされたかどうかを確認し、バイパスが発生した場合にアラートを出します。
バックログのステータス	FMC	このモジュールは、デバイスから FMC に送信されるのを待機しているイベント データのバックログのサイズが、30 分を超えて増大し続けた場合にアラートを表示します。 バックログを減らすには、帯域幅を評価し、ログに記録するイベント数を減らすことを検討してください。
クラシック ライセンス モニタ	FMC	このモジュールは十分なクラシックライセンスが残っているかどうかを確認します。また、スタック内のデバイスに適合しないライセンス セットが含まれている場合にアラートを出します。モジュールに自動的に設定された警告レベルに基づいてアラートを出します。このモジュールの設定は変更できません。

モジュール	[アプライアンス（Appliances）]	説明
CPU 使用率	任意（Any）	このモジュールは、アプライアンス上の CPU が過負荷になっていないことを確認し、CPU使用率がモジュールに設定されたパーセンテージを超えた場合にアラートを出します。
カード リセット	任意（Any）	このモジュールは、リセット時に、ハードウェア障害原因で再起動されたネットワーク カードをチェックし、アラートを出します。
クラスタのステータス	脅威防御	このモジュールは、デバイス クラスタのステータスをモニタします。このモジュールは、以下の場合にアラートを出します。 • クラスタに新しいプライマリ ユニットが選択される。 • 新しいセカンダリ ユニットがクラスタに参加する。 • プライマリまたはセカンダリ ユニットがクラスタから離脱する。
ディスク ステータス	任意（Any）	このモジュールは、ハードディスクと、アプライアンス上のマルウェア ストレージ パック（設置されている場合）のパフォーマンスを調査します。 このモジュールは、ハードディスクと RAID コントローラ（設置されている場合）で障害が発生する恐れがある場合、または、マルウェア ストレージパックではない追加のハードドライブが設置されている場合に、警告（黄色）ヘルスアラートを生成します。また、設置されているマルウェアストレージパックを検出できなかった場合はアラート（赤色）ヘルスアラートを生成します。
ディスク使用量	任意（Any）	このモジュールは、アプライアンスのハードドライブとマルウェア ストレージパック上のディスク使用率をモジュールに設定された制限と比較し、その使用率がモジュールに設定されたパーセンテージを超えた時点でアラートを出します。また、モジュールしきい値に基づいて、システムが監視対象のディスク使用カテゴリ内のファイルを過剰に削除する場合、または、これらのカテゴリを除くディスク使用率が過剰なレベルに達した場合にもアラートを出します。 ディスク使用率ヘルス ステータス モジュールは、アプライアンス上の `/` パーティションと `/volume` パーティションのディスク使用率を監視して、ドレイン頻度を追跡するために使用します。ディスク使用率モジュールは `/boot` パーティションを監視対象パーティションとして列挙しますが、そのパーティションのサイズが固定のため、このモジュールはブート パーティションに基づいてアラートを出すことはしません。

モジュール	[アプライアンス（**Appliances**）]	説明
ホスト制限	FMC	このモジュールは、FMCがモニタできるホスト数が制限に近づいているかどうかを確認し、モジュールに設定された警告レベルに基づいてアラートを出します。詳細については、Firepowerシステムのホスト制限 （2490 ページ）を参照してください。
ハードウェア アラーム	7000 & 8000 シリーズ Threat Defense（物理）	このモジュールは、物理管理対象デバイス上のハードウェアを交換する必要があるかどうかを確認し、ハードウェア ステータスに基づいてアラートを出します。また、ハードウェア関連デーモンのステータスとハイ アベイラビリティ展開の 7000 および 8000 シリーズ デバイスのステータスについてレポートします。
HA ステータス	FMC	このモジュールは、FMCハイ アベイラビリティ ステータスについて、モニタし、アラートを出します。FMC のハイ アベイラビリティを確立していない場合、HAステータスは、「`HA でない（Not in HA）`」になります。 このモジュールは、ペアリングされているかどうかに関わらず、管理対象デバイスのハイ アベイラビリティ ステータスについてはモニタしたり、アラートを出したりしません。管理対象デバイスの HA ステータスは常に「`HA でない（Not in HA）`」になります。**[Devices]** > **[Device Management]** の [デバイス管理（Device Management）] ページを使用して、ハイ アベイラビリティ ペアのデバイスをモニタします。
ヘルス モニタ プロセス	任意（Any）	このモジュールは、ヘルス モニタ自体のステータスを監視し、FMCで受信された最後のステータス イベント以降の分数が警告制限または重大制限を超えた場合にアラートを出します。
ISE 接続ステータスのモニタ	FMC	このモジュールは、Cisco Identity Services Engine（ISE）と FMC 間のサーバ接続のステータスをモニタします。ISE は、追加のユーザデータ、デバイスタイプデータ、デバイスロケーションデータを提供します。。
インライン リンク不一致アラーム	ASA FirePOWER を除くすべての管理対象デバイス	このモジュールは、インライン セットに関連付けられたポートを監視し、インライン ペアの 2 つのインターフェイスが別々の速度をネゴシエートした場合にアラートを出します。

モジュール	[アプライアンス（Appliances）]	説明
侵入およびファイルイベント レート	すべての管理対象デバイス	このモジュールは、1 秒あたりの侵入イベント数をこのモジュールに設定された制限と比較し、制限を超えた場合にアラートを出します。侵入およびファイル イベント レートが 0 の場合は、侵入プロセスがダウンしているか、管理対象デバイスがイベントを送信していない可能性があります。イベントがデバイスから送られているかどうかをチェックするには、**[Analysis]** > **[Intrusions]** > **[Events]** の順に選択します。 一般に、ネットワーク セグメントのイベント レートは平均で 1 秒あたり 20 イベントです。この平均レートのネットワーク セグメントでは、[1 秒あたりのイベント（重大）（Events per second (Critical)）] を 50 に設定し、[1 秒あたりのイベント（警告）（Events per second (Warning)）] を 30 に設定する必要があります。システムの制限を決定するには、デバイスの [統計情報（Statistics）] ページ（**[System]** > **[Monitoring]** > **[Statistics]**）で [イベント/秒（Events/Sec）] 値を探してから、次の式を使用して制限を計算します。 • 1 秒あたりのイベント（重大）= イベント/秒 * 2.5 • Events per second (Warning) = Events/Sec * 1.5 両方の制限に設定可能な最大イベント数は 999 であり、重大制限は警告制限より大きくする必要があります。
インターフェイス ステータス	任意（Any）	このモジュールは、デバイスが現在トラフィックを収集しているかどうかを確認して、物理インターフェイスおよび集約インターフェイスのトラフィック ステータスに基づいてアラートを出します。物理インターフェイスの情報には、インターフェイス名、リンク ステート、および帯域幅が含まれます。集約インターフェイスの情報には、インターフェイス名、アクティブ リンクの数、および総集約帯域幅が含まれます。 ASA FirePOWER の場合、DataPlaneInterfacex というラベルの付いたインターフェイス（ここで、x は数値）は、内部インターフェイス（ユーザ定義ではない）で、システム内部のパケット フローに関与します。

モジュール	[アプライアンス（Appliances）]	説明
リンク ステート伝達	NGIPSv、ASA FirePOWER、Firepower 9300、Firepower 4100 シリーズ、Firepower 2100 シリーズ、Firepower 1000 シリーズ を除き任意	このモジュールは、ペア化されたインラインセット内のリンクで障害が発生した時点を特定して、リンク ステート伝達モードをトリガーとして使用します。 リンク ステートがペアに伝達した場合は、そのモジュールのステータス分類が [重大（Critical）] に変更され、状態が次のように表示されます。 `Module Link State Propagation: ethx_ethy is Triggered` ここで、`x` と `y` はペア化されたインターフェイス番号です。
ローカルマルウェア分析	任意（Any）	このモジュールは、6.3 よりも前のバージョンを実行中のデバイスがローカル マルウェア分析用に設定され、AMP クラウドからローカル マルウェア分析エンジンの署名の更新をダウンロードできなかった場合、アラートを出します。 6.3 以降のバージョンを実行しているデバイスの場合は、[デバイスの脅威データの更新（Threat Data Updates on Devices）] モジュールを確認します。
メモリ使用率	任意（Any）	このモジュールは、アプライアンス上のメモリ使用率をモジュールに設定された制限と比較し、使用率がモジュールに設定されたレベルを超えるとアラートを出します。 メモリが 4 GB を超えるアプライアンスの場合、プリセットされたアラートしきい値は、システム問題を引き起こす可能性のあるメモリ空き容量の割合を求める式に基づいています。4 GB 未満のアプライアンスでは、警告しきい値と重大しきい値の時間間隔が非常に狭いため、[Warning Threshold %] の値を手動で `50` に設定することを推奨します。これにより、時間内にアプライアンスのメモリ アラートを受け取って問題を解決できる可能性がさらに高まります。 複雑なアクセス コントロール ポリシーやルールは、重要なリソースを消費し、パフォーマンスに悪影響を与える可能性があります。FirePOWER サービス ソフトウェア を含む一部のよりローエンドの ASA デバイスでは、デバイスのメモリ割り当てが最大限に使用されているため、断続的なメモリ使用率の警告が生成されることがあります。

モジュール	[アプライアンス（Appliances）]	説明
プラットフォームの障害	Firepower 1000/2100	Firepower 2100 および Firepower 1000 デバイスでは、障害は FMC によって管理される変更可能なオブジェクトです。各障害は、Firepower 1000/2100 インスタンスの障害や、発生したしきい値のアラームを表します。障害のライフサイクルの間に、障害の状態または重大度が変化する場合があります。 各障害には、障害の発生時に影響を受けたオブジェクトの動作状態に関する情報が含まれます。障害の状態が移行して解決すると、そのオブジェクトは機能状態に移行します。 詳細については、『*Cisco Firepower 1000/2100 FXOS Faults and Error Messages Guide*』を参照してください。
電源モジュール	物理 FMC 7000 & 8000 シリーズ	このモジュールは、デバイスの電源が交換が必要かどうかを確認し、電源ステータスに基づいてアラートを出します。 （注） 8000 シリーズ管理対象デバイスで電源障害が発生した場合、アラートを生成するために最大 20 分かかることがあります。
Process Status	任意（Any）	このモジュールは、アプライアンス上のプロセスがプロセス マネージャの外部で停止または終了したかを確認します。 プロセスが故意にプロセス マネージャの外部で停止された場合は、モジュールが再開してプロセスが再起動するまで、モジュール ステータスが Warning に変更され、ヘルス イベント メッセージが停止されたプロセスを示します。プロセスがプロセス マネージャの外部で異常終了またはクラッシュした場合は、モジュールが再開してプロセスが再起動するまで、モジュール ステータスが Critical に変更され、ヘルス イベント メッセージが終了したプロセスを示します。
検出の再設定	すべての管理対象デバイス	このモジュールは、デバイスの再設定が失敗した場合、アラートを出します。
RRD サーバ プロセス	FMC	このモジュールは、時系列データを格納するラウンド ロビン サーバが正常に機能しているかどうかを確認します。このモジュールは、RRD サーバが前回の更新以降に再起動した場合にアラートを出します。また、RRD サーバの再起動を伴う連続更新回数がモジュール設定で指定された数値に達した場合に [重大（Critical）] または [警告（Warning）] ステータスに遷移します。

モジュール	[アプライアンス（Appliances）]	説明
セキュリティインテリジェンス（Security Intelligence）	FMCおよび一部の管理対象デバイス	このモジュールは、セキュリティインテリジェンスが使用中で、次の場合にアラートを出します。 • FMC がフィードを更新できないか、フィード データが破損している、または認識可能な IP アドレスが含まれていない。 • 6.3 よりも前のリリースを実行中の管理対象デバイスで、FMC からの更新済みセキュリティ インテリジェンス データを受信する際に問題が発生しました 。 • 6.3 よりも前のリリースを実行中の管理対象デバイスが、メモリの問題により、FMC から提供されたすべてのセキュリティ インテリジェンスデータをロードできません。メモリ使用のトラブルシューティング （1748 ページ） を参照してください。 • 6.3以降のバージョンを実行している管理対象デバイスの場合は、[デバイスの脅威データの更新（Threat Data Updates on Devices）] モジュールを確認します。
スマート ライセンス モニタ	FMC	このモジュールは、以下の場合にアラートを出します。 • Smart Licensing Agent と Smart Software Manager (SSM) の間の通信にエラーがある。 • 製品インスタンス登録トークンの有効期限が切れている。 • スマートライセンスの使用状況がコンプライアンスに違反している。 • スマートライセンスの権限モードまたは評価モードの有効期限が切れている。

モジュール	[アプライアンス（**Appliances**）]	説明
デバイスでの脅威データの更新	リリース 6.3 以降を実行中の FMC およびデバイス （6.3 よりも前のバージョンを実行中のデバイスの場合、セキュリティ インテリジェンス、URL フィルタリング、およびローカルマルウェア分析ヘルスモジュールに関する次の表を参照してください）。	

モジュール	[アプライアンス（Appliances）]	説明
		デバイスが脅威の検出に使用する特定のインテリジェンスデータと設定は、FMC 上で 30 分ごとにクラウドから更新されます。 このモジュールは、指定した期間内にデバイスでこの情報が更新されない場合にアラートを生成します。 モニタされる更新には次の点が含まれます。 • ローカル URL カテゴリおよびレピュテーション データ • セキュリティインテリジェンス URL リストおよびフィード（Threat Intelligence Director からのグローバル ホワイト リストとブラック リストおよび URLを含む） • セキュリティインテリジェンス ネットワーク リストおよびフィード（IP アドレス）（Threat Intelligence Director からのグローバル ホワイト リストとブラック リストおよび IP アドレスを含む） • セキュリティインテリジェンス DNS リストおよびフィード（Threat Intelligence Director からのグローバル ホワイト リストとブラック リストおよびドメインを含む） • （ClamAV からの）ローカル マルウェア分析の署名 • Threat Intelligence Director からの SHA リスト（[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [セキュリティ インテリジェンス（Security Intelligence）] > [ネットワーク リストおよびフィード（Network Lists and Feeds）] ページにリストされている） • [AMP] > [動的分析接続（Dynamic Analysis Connections）] ページで設定された動的分析の設定 • キャッシュされた URL の期限切れに関連した脅威の構成時の設定（[システム（System）] > [統合（Integration）] **[Cloud Services]** ページでの [キャッシュされたURLの期限切れ（Cached URLs Expire）] 設定を含む）（このモジュールでは、URL キャッシュの更新はモニタされません。） • イベントを送信するためのシスコ クラウドとの通信の問題。[システム（System）] > [統合（Integration）] > [クラウドサービス（Cloud Services）] ページの [シスコクラウド（Cisco Cloud）] ボックスを確認します。 （注） システムに Threat Intelligence Director が設定されており、フィードがある場合にのみ、TID の更新が含まれます。 デフォルトでは、このモジュールは 1 時間後に警告を送信し、24 時間

モジュール	[アプライアンス（Appliances）]	説明
		後に重大なアラートを送信します。 FMC またはいずれかのデバイスで障害が発生していることをこのモジュールが示している場合、FMC がデバイスに到達できることを確認します。 URL カテゴリおよびレピュテーション データ タイプの障害が表示される低メモリ デバイスについては、メモリ使用のトラブルシューティング （1748 ページ） を参照してください。
時系列データ モニタ	FMC	このモジュールは、時系列データ（相関イベント カウントなど）が保存されるディレクトリ内の破損ファイルの存在を追跡して、ファイルが破損としてフラグが付けられ、削除された段階でアラートを出します。
時刻同期ステータス	任意（Any）	このモジュールは、NTP を使用して時刻を取得するデバイス クロックと NTP サーバ上のクロックの同期を追跡して、クロックの差が 10 秒を超えた場合にアラートを出します。
URL フィルタリング モニタ	FMCについて 6.3 以降のバージョンを実行しているデバイスの場合は、[デバイスの脅威データの更新（Threat Data Updates on Devices）] モジュールも確認します。	このモジュールは、FMC が次のことに失敗した場合にアラートを出します。 • シスコ クラウドからの URL 脅威データの更新のダウンロード • （6.3 よりも前のバージョンを実行中のデバイスの場合）URL 脅威データの管理対象デバイスへのプッシュ （6.3 以降のバージョンを実行しているデバイスの場合は、[デバイスの脅威データの更新（Threat Data Updates on Devices）] モジュールで、この問題のためのアラートを設定してください）。 • URL ルックアップの実行 これらのアラートの時間しきい値を設定できます。
ユーザ エージェント ステータス モニタ	FMC	このモジュールは、FMC に接続されたユーザ エージェントでハートビートが検出されない場合にアラートを出します。
VPN ステータス	FMC	このモジュールは、Firepower デバイス間の 1 つ以上の VPN トンネルがダウンしているときにアラートを出します。 このモジュールは、以下を追跡します。 • 7000 & 8000 シリーズ デバイスの VPN） • Firepower Threat Defense のサイト間 VPN • Firepower Threat Defense のリモート アクセス VPN

ヘルス モニタリングの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Maint

ステップ 1 ヘルス モジュール （350 ページ）で説明されているように、モニタするヘルス モジュールを決定します。

Firepower システムで使用しているアプライアンスの種類ごとに固有のポリシーをセットアップして、そのアプライアンスに適切なテストだけを有効にすることができます。

ヒント モニタリング動作をカスタマイズすることなくすぐにヘルス モニタリングを有効にするには、そのために用意されたデフォルト ポリシーを適用できます。

ステップ 2 正常性ポリシーの作成 （362 ページ）で説明されているように、ヘルス ステータスを追跡するアプライアンスごとに正常性ポリシーを適用します。

ステップ 3 （オプション）ヘルス モニタ アラートの作成 （369 ページ）で説明されているように、ヘルス モニタ アラートを設定します。

ヘルス ステータス レベルが特定のヘルス モジュールの特定の重大度レベルに達した段階でトリガーされる電子メール、Syslog、または SNMP アラートをセットアップできます。

正常性ポリシー

正常性ポリシーには、複数のモジュールに対して設定されたヘルステスト基準が含まれます。アプライアンスごとにどのヘルス モジュールを実行するかを制御したり、モジュールごとに実行するテストで使用される特定の制限を設定したりできます。

正常性ポリシーを設定するときに、そのポリシーに対して各ヘルス モジュールを有効にするかどうかを決定します。また、有効にした各モジュールが、プロセスの正常性を評価するたびに報告するヘルス ステータスを制御するための基準を選択することもできます。

システム内のすべてのアプライアンスに適用可能な 1 つの正常性ポリシーを作成することも、適用を計画している特定のアプライアンス用に正常性ポリシーをカスタマイズすることも、付属のデフォルト正常性ポリシーを使用することもできます。マルチドメイン展開では、先祖ドメインの管理者が子孫ドメインのデバイスに正常性ポリシーを適用できます。子孫ドメインではそのポリシーを使用するか、またはカスタマイズされたローカル ポリシーと置き換えることができます。

デフォルトの正常性ポリシー

Firepower Management Center のヘルス モニタでは、アプライアンスのヘルス モニタリングを迅速に実行できるように、デフォルトの正常性ポリシーが提供されます。デフォルト正常性ポリシーでは、実行中のプラットフォーム上で使用可能なヘルス モジュールのほとんどが自動的に有効になります。デフォルト正常性ポリシーは、自動的にFirepower Management Centerに適用されます。また、Firepower Management Center にデバイスを追加すると、デフォルトの正常性ポリシーが管理対象デバイスに適用されます。デフォルト正常性ポリシーを編集することはできませんが、コピーしてその設定に基づくカスタム ポリシーを作成することができます。

正常性ポリシーの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Maint

アプライアンスで使用する正常性ポリシーをカスタマイズすることによって、新しいポリシーを作成できます。ポリシー内の設定は、最初に、新しいポリシーの基準として選択した正常性ポリシー内の設定を使用して生成されます。必要に応じて、ポリシー内のモジュールを有効または無効にし、各モジュールのアラート基準を変更できます。

マルチドメイン展開では、編集できる現在のドメインで作成されたポリシーが表示されます。また、編集できない先祖ドメインで作成されたポリシーも表示されます。下位のドメインで作成されたポリシーを表示および編集するには、そのドメインに切り替えます。 先祖ドメインの管理者は、子孫ドメインのデバイスに正常性ポリシーを適用でき、子孫ドメインはこれを使用するか、またはカスタマイズしたローカル ポリシーに置き換えることができます。

ステップ 1 **[System]** > **[Health]** > **[Policy]** を選択します。

ステップ 2 [ポリシーの作成（Create Policy）] をクリックします。

ステップ 3 [コピー ポリシー（Copy Policy）] ドロップダウン リストから、新しいポリシーの基準として使用する既存のポリシーを選択します。

ステップ 4 ポリシーの名前を入力します。

ステップ 5 ポリシーの説明を入力します。

ステップ 6 [保存（Save）] を選択して、ポリシー情報を保存します。

ステップ 7 使用するモジュールを選択します。

ステップ 8 [有効（Enabled）] オプションに対して [オン（On）] を選択して、ヘルス ステータス テストのモジュールの使用を有効化します。

ステップ 9 該当する場合は、[重大（Critical）] および [警告（Warning）] 基準を設定します。

ステップ 10 モジュールの追加設定を行います。各モジュールで手順 7 ～ 10 を繰り返します。

ステップ 11 次の 3 つのオプションがあります。

- このモジュールに対する変更を保存して、[正常性ポリシー（Health Policy）]ページに戻るには、[ポリシーを保存して終了（Save Policy and Exit）] をクリックします。
- このモジュールの設定を保存せずに、[正常性ポリシー（Health Policy）]ページに戻るには、[キャンセル（Cancel）] をクリックします。
- このモジュールに対する変更を一時的に保存して、変更する他のモジュールの設定に切り替えるには、ページの左側にあるリストから他のモジュールを選択します。設定が終わって[ポリシーを保存して終了（Save Policy and Exit）] をクリックすると、加えたすべての変更が保存されます。[キャンセル（Cancel）] をクリックすると、すべての変更が破棄されます。

次のタスク

- 正常性ポリシーの適用（363ページ）の説明に従って、各アプライアンスに正常性ポリシーを適用します。これにより変更が適用され、影響を受けるすべてのポリシーのポリシー ステータスが更新されます。

正常性ポリシーの適用

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Maint

正常性ポリシーをアプライアンスに適用すると、ポリシー内で有効にしたすべてのモジュールのヘルステストが、アプライアンス上のプロセスとハードウェアの正常性を自動的に監視します。その後、ヘルステストは、ポリシー内で設定された時間間隔で実行を続け、アプライアンスのヘルス データを収集し、そのデータをFirepower Management Centerに転送します。

正常性ポリシーでモジュールを有効にしてから、ヘルステストが必要ないアプライアンスにポリシーを適用した場合、ヘルス モニタはそのヘルス モジュールのステータスを無効として報告します。

すべてのモジュールが無効になっているポリシーをアプライアンスに適用すると、適用されたすべての正常性ポリシーがアプライアンスから削除されるため、どの正常性ポリシーも適用されません。

すでにポリシーが適用されているアプライアンスに別のポリシーを適用した場合は、新しく適用されたテストに基づく新しいデータの表示が少し遅れる可能性があります。

マルチドメイン展開では、編集できる現在のドメインで作成されたポリシーが表示されます。また、編集できない先祖ドメインで作成されたポリシーも表示されます。下位のドメインで作成されたポリシーを表示および編集するには、そのドメインに切り替えます。 先祖ドメインの管理者は、子孫ドメインのデバイスに正常性ポリシーを適用でき、子孫ドメインはこれを使用するか、またはカスタマイズしたローカル ポリシーに置き換えることができます。

ステップ 1 **[System]** > **[Health]** > **[Policy]** を選択します。

ステップ 2 適用するポリシーの横にある適用アイコン（  ）をクリックします。

ヒント [正常性ポリシー（Health Policy）] 列の横にあるステータス アイコン（  ）は、アプライアンスの現在のヘルス ステータスを示します。

ステップ 3 正常性ポリシーを適用するアプライアンスを選択します。

ステップ 4 [適用（Apply）] をクリックして、選択したアプライアンスにポリシーを適用します。

次のタスク

- 必要に応じて、タスクのステータスをモニタします（タスク メッセージの表示（417 ページ） を参照）。

  アプライアンスのモニタリングは、ポリシーが正常に適用された直後に開始されます。

正常性ポリシーの編集

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Maint

マルチドメイン展開では、編集できる現在のドメインで作成されたポリシーが表示されます。また、編集できない先祖ドメインで作成されたポリシーも表示されます。下位のドメインで作成されたポリシーを表示および編集するには、そのドメインに切り替えます。先祖ドメインの管理者は、子孫ドメインのデバイスに正常性ポリシーを適用でき、子孫ドメインはこれを使用するか、またはカスタマイズしたローカル ポリシーに置き換えることができます。

ステップ 1 **[System]** > **[Health]** > **[Policy]** を選択します。

ステップ 2 変更するポリシーの横にある編集アイコン（  ）をクリックします。

ステップ 3 [ポリシー名（Policy Name）] フィールドまたは [ポリシーの説明（Policy Description）] フィールドを必要に応じて編集します。

ステップ 4 変更するヘルス モジュールをクリックします。

ステップ 5 ヘルス モジュール （350 ページ）の説明に従って、設定を変更します。

ステップ 6 次の 3 つのオプションがあります。

- このモジュールに対する変更を保存して、[Health Policy] ページに戻るには、[Save Policy and Exit] をクリックします。
- このモジュールの設定を保存せずに、[正常性ポリシー（Health Policy）] ページに戻るには、[キャンセル（Cancel）] をクリックします。

- このモジュールに対する変更を一時的に保存して、変更する他のモジュールの設定に切り替えるには、ページの左側にあるリストから他のモジュールを選択します。設定が終わって[ポリシーを保存して終了（Save Policy and Exit）] をクリックすると、加えたすべての変更が保存されます。[キャンセル（Cancel）] をクリックすると、すべての変更が破棄されます。

次のタスク

- 正常性ポリシーの適用 （363 ページ）の説明に従って、正常性ポリシーを再適用します。これにより変更が適用され、影響を受けるすべてのポリシーのポリシー ステータスが更新されます。

正常性ポリシーの削除

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Maint

不要になった正常性ポリシーを削除できます。アプライアンスに適用されているポリシーを削除した場合は、別のポリシーを適用するまでそのポリシー設定が有効のままになります。加えて、デバイスに適用されている正常性ポリシーを削除した場合、元となる関連アラート応答を無効にするまでは、そのデバイスに対して有効になっているヘルス モニタリング アラートがアクティブなままになります。

マルチドメイン導入では、現在のドメインで作成された正常性ポリシーのみを削除できます。

ヒント　アプライアンスのヘルス モニタリングを停止するには、すべてのモジュールが無効になっている正常性ポリシーを作成し、それをアプライアンスに適用します。

ステップ 1　**[System]** > **[Health]** > **[Policy]** を選択します。

ステップ 2　削除するポリシーの横にある削除アイコン（）をクリックします。
削除が成功したかどうかを示すメッセージが表示されます。

ヘルス モニタ ブラックリスト

通常のネットワーク メンテナンスの一環として、アプライアンスを無効にしたり、一時的に使用不能にしたりすることがあります。このような機能停止は意図したものであり、アプライア

ンスからのヘルス ステータスに Firepower Management Center 上のサマリー ヘルス ステータスを反映させる必要はありません。

ヘルス モニタ ブラックリスト機能を使用して、アプライアンスまたはモジュールに関するヘルス モニタリング ステータス レポートを無効にすることができます。たとえば、ネットワークのあるセグメントが使用できなくなることがわかっている場合は、そのセグメント上の管理対象デバイスのヘルス モニタリングを一時的に無効にして、Firepower Management Center上のヘルス ステータスにデバイスへの接続がダウンしたことによる警告状態または重大状態が表示されないようにできます。

ヘルス モニタリング ステータスを無効にしても、ヘルス イベントは生成されますが、そのステータスが無効になっているため、ヘルス モニタのヘルス ステータスには影響しません。ブラックリストからアプライアンスまたはモジュールを削除しても、ブラックリストに登録中に生成されたイベントのステータスは Disabled のままです。

アプライアンスからのヘルスイベントを一時的に無効にするには、ブラックリスト設定ページに移動して、アプライアンスをブラックリストに追加します。設定が有効になると、システムは全体のヘルス ステータスを計算するときにブラックリストに登録されているアプライアンスを含めません。[Health Monitor Appliance Status Summary] にはこのアプライアンスが Disabled としてリストされます。

アプライアンス上の個別のヘルス モニタリング モジュールをブラックリストに登録する方が実用的な場合があります。たとえば、Firepower Management Center 上でホスト制限に達した場合、ホスト制限ステータス メッセージをブラックリストに登録できます。

メインの [ヘルス モニタ（Health Monitor）] ページで、ステータス行内の矢印をクリックして特定のステータスを持つアプライアンスのリストを展開表示すれば、ブラックリストに登録されたアプライアンスを区別できることに注意してください。

ブラックリストに登録されたアプライアンスまたは部分的にブラックリストに登録されたアプライアンスのビューを展開すると、ブラックリスト アイコン（）と注記が表示されます。

（注） Firepower Management Centerでは、ヘルス モニタのブラックリスト設定はローカル コンフィギュレーション設定です。そのため、Firepower Management Center上でデバイスをブラックリストに登録してから削除しても、後で再登録すれば、ブラックリスト設定は元どおりになります。新たに再登録したデバイスはブラックリストに登録されたままです。

マルチドメイン導入では、先祖ドメインの管理者が子孫ドメインのアプライアンスやヘルスモジュールをブラックリストに登録できます。ただし、子孫ドメインの管理者は、先祖のコンフィギュレーションをオーバーライドして、自身のドメインのデバイスのブラックリストをクリアすることができます。

アプライアンスのブラックリスト登録

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Maint

アプライアンスは個別に、またはグループ、モデル、関連付けられている正常性ポリシーにより、ブラックリストに登録できます。

ブラックリスト設定が有効になると、[正常性モニタアプライアンスモジュールの概要（Health Monitor Appliance Module Summary）] と [デバイス管理（Device Management）] ページでアプライアンスが [無効（Disabled）] として表示されます。アプライアンスのヘルス イベントのステータスは [無効（Disabled）] です。

個別のアプライアンスのイベントとヘルス ステータスを [無効（Disabled）] に設定する必要がある場合、アプライアンスをブラックリストに登録できます。ブラックリスト設定が有効になると、アプライアンスが [正常性モニタアプライアンスモジュールの概要（Health Monitor Appliance Module Summary）] に [無効（Disabled）] として表示され、アプライアンスのヘルス イベントのステータスが [無効（Disabled）] になります。

マルチドメイン展開では、アプライアンスを先祖ドメインのブラックリストに登録すると、子孫ドメインもすべてブラックリストに登録されたことになります。子孫ドメインは、この設定の継承をオーバーライドし、ブラックリスト指定を解除できます。Firepower Management Center はグローバル レベルでのみブラックリスト指定できます。

ステップ 1 **[System]** > **[Health]** > **[Blacklist]**を選択します。

ステップ 2 アプライアンス グループ、モデル、またはポリシーでリストをソートするには、右側にあるドロップダウンリストを使用します。

ヒント [正常性ポリシー（Health Policy）] 列の横にあるステータス アイコン（）は、アプライアンスの現在のヘルス ステータスを示します。[システムポリシー（System Policy）] 列の横にあるステータス アイコン（  ）は、Firepower Management Center とデバイス間の通信ステータスを示します。

ステップ 3 次の 2 つの選択肢があります。

- グループ、モデル、またはポリシー カテゴリ内のすべてのアプライアンスをブラックリストに登録するには、カテゴリのチェックボックスをオンにしてから、[選択したデバイスをブラックリストに登録（Blacklist Selected Devices）] をクリックします。
- グループ、モデル、またはポリシー カテゴリ内のすべてのアプライアンスをブラックリストから除外するには、カテゴリのチェックボックスをオンにしてから、[選択したデバイスのブラックリスト指定を解除（Clear Blacklist on Selected Devices）] をクリックします。

正常性ポリシー モジュールのブラックリスト登録

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Maint

アプライアンス上の個別の正常性ポリシーモジュールをブラックリストに登録できます。この操作により、モジュールからのイベントによってアプライアンスのステータスが Warning または Critical に変更されないようにすることができます。

ブラックリスト設定が有効になると、アプライアンスが [ブラックリスト（Blacklist）] ページと [アプライアンス正常性モニタモジュールステータスの概要（Appliance Health Monitor Module Status Summary）] で [部分的なブラックリスト指定（Partially Blacklisted）] または [すべてのモジュールがブラックリスト指定（All Modules Blacklisted）] として表示されますが、メインの [アプライアンスのステータスの概要（Appliance Status Summary）] ページでは展開されたビューにだけ表示されます。

ヒント　個別にブラックリストに登録したモジュールを追跡して、必要に応じてそれらを再アクティブ化できるようにしてください。誤ってモジュールを無効にすると、必要な警告または重大メッセージを見逃す可能性があります。

マルチドメイン展開では、先祖ドメインの管理者は子孫ドメインの正常性モジュールをブラックリストに登録できます。しかし、子孫ドメインの管理者は、この先祖の設定をオーバーライドし、ドメインに適用されるポリシーのブラックリスト指定を解除できます。Firepower Management Center 正常性モジュールはグローバル レベルでのみブラックリスト指定できます。

ステップ 1　**[System]** > **[Health]** > **[Blacklist]**を選択します。

ステップ 2　変更するアプライアンスの横にある編集アイコン（）をクリックします。

ステップ 3　ブラックリスト指定する正常性ポリシーモジュールの横にあるチェックボックスをオンにします。一部のモジュールは特定のデバイスにのみ適用できます。詳細はヘルス モジュール （350 ページ）を参照してください。

ステップ 4　**[保存（Save）]** をクリックします。

ヘルス モニタ アラート

正常性ポリシー内のモジュールのステータスが変更された場合に電子メール、SNMP、またはシステム ログ経由で通知するアラートをセットアップできます。特定のレベルのヘルス イベントが発生したときにトリガーとして使用して警告するヘルスイベント レベルと既存のアラート応答を関連付けることができます。

たとえば、アプライアンスがハード ディスク スペースを使い果たす可能性を懸念している場合は、残りのディスク スペースが警告レベルに達したときに自動的に電子メールをシステム管理者に送信できます。ハード ドライブがさらにいっぱいになる場合、ハード ドライブが重大レベルに達したときに 2 つ目の電子メールを送信できます。

マルチドメイン展開では、現在のドメインで作成されたヘルス モニタのアラートのみを表示、および変更できます。

ヘルス モニタ アラート情報

ヘルス モニタによって生成されるアラートには次の情報が含まれます。

- アラートの重大度レベルを示す Severity。
- テスト結果がアラートをトリガーとして使用したヘルス モジュールを示す Module。
- アラートをトリガーとして使用したヘルス テスト結果を含む [説明（Description）]。

次の表で、これらの重大度レベルについて説明します。

表 *40 :* アラートの重大度

重大度	説明
Critical	ヘルス テスト結果が Critical アラート ステータスをトリガーとして使用する基準を満たしました。
Warning	ヘルス テスト結果が Warning アラート ステータスをトリガーとして使用する基準を満たしました。
Normal	ヘルス テスト結果が Normal アラート ステータスをトリガーとして使用する基準を満たしました。
Error	ヘルス テストが実行されませんでした。
Recovered	ヘルス テスト結果がクリティカルまたは警告のアラート ステータスから通常のアラート ステータスに戻るための基準を満たしました。

ヘルス モニタ アラートの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin

ヘルス モニタ アラートを作成するときに、重大度レベル、ヘルス モジュール、およびアラート応答の関連付けを作成します。既存のアラートを使用することも、新しいアラートをシステ

ムヘルスの報告専用に設定することもできます。選択したモジュールが重大度レベルに達すると、アラートがトリガーされます。

既存のしきい値と重複するようにしきい値を作成または更新すると、競合が通知されます。重複したしきい値が存在する場合、ヘルス モニタは最も少ないアラートを生成するしきい値を使用し、その他のしきい値を無視します。しきい値のタイムアウト値は、5 ～ 4,294,967,295 分の間にする必要があります。

マルチドメイン導入では、現在のドメインで作成されたヘルス モニタ アラートのみを表示および変更できます。

始める前に

- ヘルス アラートを送信する SNMP、syslog、電子メール サーバと Firepower Management Center との通信を制御するアラート応答を設定します。Firepower Management Center アラート応答 （2807 ページ）を参照してください。

ステップ 1 **[System]** > **[Health]** > **[Monitor Alerts]**を選択します。

ステップ 2 [ヘルス アラート名（Health Alert Name）] フィールドに、ヘルス アラートの名前を入力します。

ステップ 3 [重大度（Severity）] リストから、アラートをトリガーするために使用する重大度レベルを選択します。

ステップ 4 [モジュール（Module）] リストから、アラートを適用する正常性ポリシー モジュールを選択します。

ステップ 5 [アラート（Alert）] リストから、指定した重大度レベルに達したときにトリガーするアラート応答を選択します。

ステップ 6 オプションで、[しきい値タイムアウト（Threshold Timeout）] フィールドに、それぞれのしきい値期間が終了してしきい値がリセットされるまでの分数を入力します。

ポリシーの実行時間間隔の値がしきい値タイムアウトの値より小さい場合でも、特定のモジュールから報告される 2 つのヘルス イベント間の間隔のほうが常に大きくなります。たとえば、しきい値タイムアウトを 8 分に変更し、ポリシーの実行時間間隔が 5 分である場合、報告されるイベント間の間隔は 10 分（5 × 2）になります。

ステップ 7 [保存（Save）] をクリックして、ヘルス アラートを保存します。

ヘルス モニタ アラートの編集

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin

既存のヘルス モニタ アラートを編集して、ヘルス モニタ アラートに関連付けられた重大度レベル、ヘルス モジュール、またはアラート応答を変更できます。

マルチドメイン導入では、現在のドメインで作成されたヘルス モニタ アラートのみを表示および変更できます。

ステップ 1 **[System]** > **[Health]** > **[Monitor Alerts]**を選択します。
ステップ 2 [アクティブ ヘルス アラート（Active Health Alerts）] リストから、変更するアラートを選択します。
ステップ 3 [ロード（Load）] をクリックして、選択したアラートの構成済みの設定をロードします。
ステップ 4 必要に応じて設定を変更します。
ステップ 5 [保存（Save）] をクリックして、変更したヘルス アラートを保存します。
アラート設定が正常に保存されたかどうかを示すメッセージが表示されます。

ヘルス モニタ アラートの削除

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin

マルチドメイン導入では、現在のドメインで作成されたヘルス モニタ アラートのみを表示および変更できます。

ステップ 1 **[System]** > **[Health]** > **[Monitor Alerts]**を選択します。
ステップ 2 削除するアクティブなヘルス アラートを選択してから、[削除（Delete）] をクリックします。

次のタスク

- アラートが継続しないようにするには、元になるアラート応答を無効にするか、または削除します。Firepower Management Center アラート応答 （2807 ページ）を参照してください。

ヘルス モニタの使用

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Maint/Any Security Analyst

ヘルス モニタには、Firepower Management Center によって管理されているすべてのデバイスに加えて、Firepower Management Center に関して収集されたヘルス ステータスが表示されます。ヘルス モニタは以下で構成されています。

- ステータス テーブル：この Firepower Management Center の管理対象アプライアンスの台数が全体のヘルス ステータス別に表示されます。
- 円グラフ：それぞれのヘルス ステータス カテゴリにおけるアプライアンスの現在のパーセンテージを示します。
- アプライアンス リスト：管理対象デバイスのヘルス状態の詳細が表示されます。

マルチドメイン展開では、先祖ドメインのヘルス モニタに、すべての子孫ドメインからのデータが表示されます。子孫ドメインには、現在のドメインからのデータのみが表示されます。

ステップ 1 **[System]** > **[Health]** > **[Monitor]**を選択します。

ステップ 2 テーブルの[ステータス（Status）]カラム内の該当するステータスまたは円グラフの該当する部分を選択して、そのステータスを持つアプライアンスをリストします。

ヒント ステータス レベルに関する行内の矢印が下向きの場合は、そのステータスのアプライアンス リストが下側のテーブルに表示されます。矢印が右向きの場合、アプライアンス リストは非表示です。

ステップ 3 次の選択肢があります。

- アプライアンスのヘルス モニタを表示します（アプライアンス ヘルス モニタの表示 （373 ページ）を参照）。
- ヘルス ポリシーを作成します（正常性ポリシーの作成 （362 ページ）を参照）。
- ヘルス モニタ アラートを作成します（ヘルス モニタ アラートの作成 （369 ページ）を参照）。

ヘルス モニタ ステータスのカテゴリ

使用可能なステータス カテゴリを、重大度別に次の表に示します。

表 *41* : ヘルス ステータス インジケータ

ステータス レベル	ステータス アイコン	円グラフのステータスの色	説明
エラー（Error）		黒色	アプライアンス上の 1 つ以上のヘルス モニタリング モジュールで障害が発生し、それ以降、正常に再実行していないことを示します。テクニカル サポート担当者に連絡して、ヘルス モニタリング モジュールの更新プログラムを入手してください。

ステータス レベル	ステータス アイコン	円グラフのステータスの色	説明
Critical		赤	アプライアンス上の1つ以上のヘルス モジュールが重大制限を超え、問題が解決されていないことを示します。
Warning		黄色	アプライアンス上の1つ以上のヘルス モジュールが警告制限を超え、問題が解決されていないことを示します。
Normal		グリーン	アプライアンス上のすべてのヘルス モジュールがアプライアンスに適用された正常性ポリシーで設定された制限内で動作していることを示します。
Recovered		グリーン	アプライアンス上のすべてのヘルス モジュールがアプライアンスに適用された正常性ポリシーで設定された制限内で動作していることを示します。これには、前に Critical または Warning 状態だったモジュールも含まれます。
Disabled		青色	アプライアンスが無効またはブラックリストに登録されている、アプライアンスに正常性ポリシーが適用されていない、またはアプライアンスが現在到達不能になっていることを示します。

アプライアンス ヘルス モニタの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Maint/Any Security Analyst

アプライアンス ヘルス モニタは、アプライアンスのヘルス ステータスの詳細ビューを提供します。

マルチドメイン展開では、子孫ドメインのアプライアンスのヘルス ステータスを表示できます。

ヒント　通常は、非活動状態が1時間（または設定された他の時間間隔）続くと、ユーザはセッションからログアウトされます。ヘルス ステータスを長期間受動的に監視する予定の場合は、一部のユーザのセッション タイムアウトの免除、またはシステム タイムアウト設定の変更を検討してください。詳細については、Web インターフェイスでの内部ユーザの追加 （57 ページ）およびセッション タイムアウトの設定 （1315 ページ）を参照してください。

ステップ 1　**[System]** > **[Health]** > **[Monitor]**を選択します。

ステップ 2　アプライアンス リストを展開します。特定のステータスを持つアプライアンスを表示するには、そのステータス行内の矢印をクリックします。または、[アプライアンス ステータスの概要（Appliance Status Summary）] グラフで、表示するアプライアンス ステータス カテゴリの色をクリックします。

ヒント　ステータス レベルに関する行内の矢印が下向きの場合は、そのステータスのアプライアンス リストが下側のテーブルに表示されます。矢印が右を向いている場合、アプライアンス リストは非表示です。

ステップ 3　アプライアンス リストの[アプライアンス（Appliance）]列で、詳細を表示するアプライアンスの名前をクリックします。

ヒント　[モジュール ステータスの概要（Module Status Summary）] グラフで、そのステータス カテゴリの[アラート詳細（Alert Details）]の表示を切り替えるには、イベント ステータス カテゴリの色をクリックします。

次のタスク

- アプライアンスのすべてのヘルス モジュールを実行する場合、次を参照してください。アプライアンスのすべてのモジュールの実行 （375 ページ）
- アプライアンスの特定のヘルス モジュールを実行する場合、次を参照してください。特定のヘルス モジュールの実行 （375 ページ）
- アプライアンスのヘルス モジュール アラート グラフを生成する場合、次を参照してください。ヘルス モジュール アラート グラフの生成 （376 ページ）
- アプライアンスのトラブルシューティング ファイルを生成する場合、次を参照してください。高度なトラブルシューティング ファイルのダウンロード （421 ページ）
- アプライアンスの高度なトラブルシューティング ファイルを生成する場合、次を参照してください。高度なトラブルシューティング ファイルのダウンロード （421 ページ）

- Firepower Management Center Web インターフェイスから Firepower Threat Defense CLI コマンドを実行する場合はWeb インターフェイスからの FTD CLI の使用 （423 ページ）を参照してください。

アプライアンスのすべてのモジュールの実行

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Maint/Any Security Analyst

ヘルス モジュール テストは、正常性ポリシーの作成時に設定されたポリシー実行時間間隔で自動的に実行されます。ただし、アプライアンスの最新の正常性情報を収集するためにすべてのヘルス モジュール テストをオンデマンドで実行することもできます。

マルチドメイン展開では、現在のドメイン内のアプライアンスと、子孫ドメイン内のアプライアンスに対してヘルス モジュール テストを実行できます。

ステップ 1 アプライアンスのヘルス モニタを表示します。アプライアンス ヘルス モニタの表示 （373 ページ）を参照してください。

ステップ 2 [すべてのモジュールの実行（Run All Modules）] をクリックします。ステータス バーにテストの進捗状況が表示されてから、[Health Monitor Appliance] ページが更新されます。

（注） ヘルス モジュールを手動で実行した場合は、自動的に発生する最初の更新に、手動で実行されたテストの結果が反映されない可能性があります。手動で実行したばかりのモジュールの値が変更されていない場合は、数秒待ってから、デバイス名をクリックしてページを更新します。ページが自動的に再び更新されるまで待機していてもかまいません。

特定のヘルス モジュールの実行

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Maint/Any Security Analyst

ヘルス モジュール テストは、正常性ポリシーの作成時に設定されたポリシー実行時間間隔で自動的に実行されます。ただし、そのモジュールの最新のヘルス情報を収集するためにヘルス モジュール テストをオンデマンドで実行することもできます。

マルチドメイン展開では、現在のドメイン内のアプライアンスと、子孫ドメイン内のアプライアンスに対してヘルス モジュール テストを実行できます。

ステップ 1 アプライアンスのヘルス モニタを表示します。アプライアンス ヘルス モニタの表示 （373 ページ）を参照してください。

ステップ 2 [モジュール ステータスの概要] グラフで、表示するヘルス アラート ステータス カテゴリの色をクリックします。

ステップ 3 イベントのリストを表示するアラートの [アラート詳細（Alert Detail）] 行で、[実行（Run）] をクリックします。

ステータス バーにテストの進捗状況が表示されてから、[Health Monitor Appliance] ページが更新されます。

（注） ヘルス モジュールを手動で実行した場合は、自動的に発生する最初の更新に、手動で実行されたテストの結果が反映されない可能性があります。手動で実行したばかりのモジュールの値が変更されていない場合は、数秒待ってから、デバイス名をクリックしてページを更新します。ページが再び自動的に更新されるまで待機していてもかまいません。

ヘルス モジュール アラート グラフの生成

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Maint/Any Security Analyst

特定のアプライアンスの特定のヘルス テストの一定期間にわたる結果をグラフ化できます。

ステップ 1 アプライアンスのヘルス モニタを表示します（アプライアンス ヘルス モニタの表示 （373 ページ）を参照）。

ステップ 2 [ヘルス モニタ アプライアンス（Health Monitor Appliance）] ページの [モジュール ステータスの概要（Module Status Summary）] グラフで、表示するヘルス アラート ステータス カテゴリの色をクリックします。

ステップ 3 イベントのリストを表示するアラートの [アラート詳細（Alert Detail）] 行で、[グラフ（Graph）] をクリックします。

ヒント イベントが 1 つも表示されない場合は、時間範囲を調整することを考慮してください。

ヘルス イベント ビュー

[ヘルス イベント ビュー（Health Event View）] ページでは、ヘルス モニタがログに記録したヘルス イベントを、Firepower Management Center ログ ヘルス イベントで表示できます。完全にカスタマイズ可能なイベント ビューを使用すれば、ヘルス モニタによって収集されたヘル

ス ステータス イベントを迅速かつ容易に分析できます。イベント データを検索して、調査中のイベントに関係する可能性のある他の情報に簡単にアクセスしたりできます。ヘルスモジュールごとにテストされる条件を理解していれば、ヘルスイベントに対するアラートをより効率的に設定できます。

ヘルス イベント ビュー ページで多くの標準イベント ビュー機能を実行できます。

ヘルス イベントの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Maint/Any Security Analyst

[ヘルス イベントのテーブル ビュー（Table View of Health Events）] ページには、指定したアプライアンス上のすべてのヘルス イベントのリストが表示されます。

Firepower Management Center 上の [ヘルス モニタ（Health Monitor）] ページからヘルス イベントにアクセスした場合は、すべての管理対象アプライアンスのすべてのヘルスイベントが表示されます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

ヒント　このビューをブックマークすれば、イベントの [ヘルス イベント（Health Events）] テーブルを含むヘルスイベント ワークフロー内のページに戻ることができます。ブックマークしたビューには、現在見ている時間範囲内のイベントが表示されますが、必要に応じて時間範囲を変更してテーブルを最新情報で更新することができます。

[System] > **[Health]** > **[Events]**を選択します。

ヒント　ヘルス イベントのテーブル ビューが含まれていないカスタム ワークフローを使用している場合は、[(ワークフローの切り替え)（(switch workflow)）] をクリックします。[ワークフローの選択（Select Workflow）] ページで、[ヘルス イベント（Health Events）] をクリックします。

（注）　イベントが 1 つも表示されない場合は、時間範囲を調整することを考慮してください。

モジュールとアプライアンス別のヘルス イベントの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Maint/Any Security Analyst

ステップ 1 アプライアンスのヘルス モニタを表示します（アプライアンス ヘルス モニタの表示 （373 ページ）を参照）。

ステップ 2 [モジュール ステータスの概要（Appliance Status Summary）] グラフで、表示するイベント ステータス カテゴリの色をクリックします。

[アラート詳細（Alert Detail）] リストで、表示を切り替えてイベントを表示または非表示にします。

ステップ 3 イベントのリストを表示するアラートの [アラート詳細（Alert Detail）] 行で、[イベント（Events）] をクリックします。
[ヘルス イベント（Health Events）] ページが開いて、制限としてアプライアンスの名前と指定したヘルス アラート モジュールの名前を含むクエリーの結果が表示されます。イベントが 1 つも表示されない場合は、時間範囲を調整することを考慮してください。

ステップ 4 指定したアプライアンスのすべてのステータス イベントを表示する場合は、[検索制約（Search Constraints）] を展開し、[モジュール名（Module Name）] 制限をクリックして削除します。

ヘルス イベント テーブルの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Maint/Any Security Analyst

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

ステップ 1 **[System]** > **[Health]** > **[Events]**を選択します。

ステップ 2 次の選択肢があります。

- ブックマーク：すぐに現在のページに戻れるように、現在のページをブックマークするには、[このページのブックマーク（Bookmark This Page）] をクリックしてブックマークの名前を指定し、[保存（Save）] をクリックします。
- ワークフローの変更：別のヘルス イベント ワークフローを選択するには、[(ワークフローの切り替え)（(switch workflow)）] をクリックします。

- イベントの削除：ヘルス イベントを削除するには、削除するイベントの横にあるチェックボックスをオンにして、[削除（Delete）] をクリックします。現在の制約されているビューですべてのイベントを削除するには、[すべて削除（Delete All）] をクリックしてから、すべてのイベントを削除することを確認します。
- レポートの生成：テーブル ビューのデータに基づいてレポートを生成するには、[レポート デザイナ（Report Designer）] をクリックします。
- 変更：ヘルステーブル ビューに表示されるイベントの時刻と日付範囲を変更します。イベント ビューを時間で制約している場合は、（グローバルであるかイベントに特有であるかに関係なく）アプライアンスに設定されている時間枠の範囲外に生成されたイベントがイベント ビューに表示されることがあることに注意してください。アプライアンスに対してスライドする時間枠を設定した場合でも、この状況が発生することがあります。
- 移動：イベント ビュー ページを使用して移動します。
- ブックマークの移動：ブックマーク管理ページに移動するには、任意のイベント ビューから [ブックマークの表示（View Bookmarks）] をクリックします。
- その他に移動：他のイベント テーブルに移動して関連イベントを表示します。
- ソート：表示されたイベントをソートする、イベント テーブルに表示するカラムを変更する、または表示するイベントを制約します。
- すべて表示：すべてのイベントのイベントの詳細をビューに表示するには、[すべて表示（View All）] をクリックします。
- 詳細の表示：単一のヘルス イベントに関連付けられる詳細を表示するには、イベントの左側にある下矢印のリンクをクリックします。
- 複数表示：複数のヘルス イベントのイベント詳細を表示するには、詳細を表示するイベントに対応する行の横にあるチェックボックスをオンにして、[表示（View）] をクリックします。
- ステータスの表示：特定のステータスのすべてのイベントを表示するには、そのステータスのイベントの [ステータス（Status）] カラムのステータス アイコンをクリックします。

7000 および 8000 シリーズ デバイスのハードウェア アラートの詳細

（注） 8350 ハードウェア プラットフォームには 6 つのファンがあり、FAN2 ～ FAN7 と表示されています。これは想定されている動作です。8350 プラットフォームで FAN1 またはファンの番号付けに関するハードウェア アラートを受け取った場合は、アラートを無視できます。

表 *42 : 7000* および *8000* シリーズ デバイスの監視対象条件

監視対象条件	黄色または赤色エラー状態の原因
デバイスの高可用性ステータス	高可用性ペアの 7000 または 8000 シリーズ デバイスが相互に通信していない（ケーブル配線の問題などで）場合は、ハードウェア アラーム モジュールが赤色に変化します。

監視対象条件	黄色または赤色エラー状態の原因
ftwo デーモン ステータス	ftwo デーモンがダウンすると、ハードウェア アラーム モジュールのヘルス ステータスが赤色に変化し、メッセージ詳細にデーモンへの参照が追加されます。
検出された NFE カード	システム上で検出された NFE カードの枚数を示します。この値がアプライアンスの予想NFE カウントと一致しない場合は、ハードウェア アラーム モジュールが赤色に変化します。
NFE ハードウェア ステータス	1 つ以上の NFE カードが通信していない場合は、ハードウェア アラーム モジュールが赤色に変化し、該当するカードがメッセージ詳細に表示されます。
NFE ハートビート	システムが NFE ハートビートを検出しなかった場合は、ハードウェア アラーム モジュールが赤色に変化し、メッセージ詳細に関連カードへの参照が追加されます。
NFE 内部リンク ステータス	NMSB カードと NFE カード間のリンクがダウンした場合は、ハードウェア アラーム モジュールが赤色に変化し、メッセージ詳細に関連ポートへの参照が追加されます。
NFE メッセージ デーモン	NFE メッセージ デーモンがダウンすると、ハードウェア アラーム モジュールのヘルス ステータスが赤色に変化し、メッセージ詳細にデーモンへの参照（および該当する場合はNFE カード番号）が追加されます。
NFE 温度	NFE 温度が 97 ℃を超えると、ハードウェア アラーム モジュールのヘルス ステータスが黄色に変化し、メッセージ詳細に NFE 温度への参照（および該当する場合は NFE カード番号）が追加されます。 NFE 温度が 102 ℃を超えると、ハードウェア アラーム モジュールのヘルス ステータスが赤色に変化し、メッセージ詳細に NFE 温度への参照（および該当する場合は NFE カード番号）が追加されます。

監視対象条件	黄色または赤色エラー状態の原因
NFE 温度ステータス	特定の NFE カードの現在の温度ステータスを示します。OK の場合ハードウェア アラーム モジュールは緑色を、Warning の場合は黄色を、Critical の場合は赤色（および該当する場合は NFE カード番号）を示します。
NFE TCAM デーモン	NFE TCAM デーモンがダウンすると、ハードウェア アラーム モジュールのヘルス ステータスが赤色に変化し、メッセージ詳細にデーモンへの参照（および該当する場合は NFE カード番号）が追加されます。
nfm_ipfragd（ホスト フラグ）デーモン	nfm_ipfragd デーモンがダウンすると、ハードウェア アラーム モジュールのヘルス ステータスが赤色に変化し、メッセージ詳細にデーモンへの参照（および該当する場合は NFE カード番号）が追加されます。
NFE プラットフォーム デーモン	NFE プラットフォーム デーモンがダウンすると、ハードウェア アラーム モジュールのヘルス ステータスが赤色に変化し、メッセージ詳細にデーモンへの参照（および該当する場合は NFE カード番号）が追加されます。
NMSB コミュニケーション	メディア アセンブリが存在しないか、通信していない場合は、ハードウェア アラーム モジュールのヘルス ステータスが赤色に変化し、メッセージ詳細に NFE 温度への参照（および該当する場合は NFE カード番号）が追加されます。
psls デーモン ステータス	psls デーモンがダウンすると、ハードウェア アラーム モジュールのヘルス ステータスが赤色に変化し、メッセージ詳細にデーモンへの参照が追加されます。
Rulesd（ホスト ルール）デーモン	Rulesd デーモンがダウンすると、ハードウェア アラーム モジュールのヘルス ステータスが黄色に変化し、メッセージ詳細にデーモンへの参照（および該当する場合は NFE カード番号）が追加されます。

監視対象条件	黄色または赤色エラー状態の原因
scmd デーモン ステータス	scmd デーモンがダウンすると、ハードウェア アラーム モジュールのヘルス ステータスが赤色に変化し、メッセージ詳細にデーモンへの参照が追加されます。

[ヘルス イベント（Health Events）] テーブル

正常性ポリシー内で有効にされたヘルス モニタ モジュールが、さまざまなテストを実行してアプライアンスのヘルス ステータスを特定します。ヘルス ステータスが指定された基準を満たしている場合は、ヘルス イベントが生成されます。

次の表で、ヘルスイベントテーブルで表示および検索できるフィールドについて説明します。

表 *43 :* ヘルス イベント フィールド

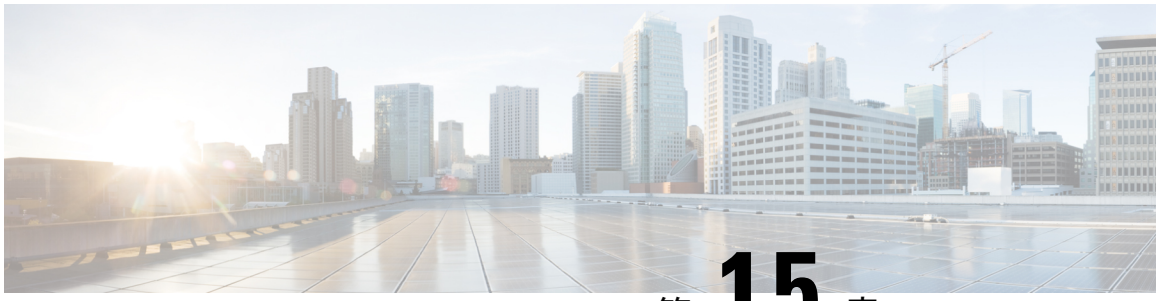
フィールド	説明
Module Name	表示するヘルス イベントを生成したモジュールの名前を指定します。たとえば、CPU パフォーマンスを測定するイベントを表示するには、「CPU」と入力します。検索によって、該当する CPU 使用率イベントと CPU 温度イベントが取得されます。
テスト名（Test Name） （検索専用）	イベントを生成したヘルスモジュールの名前。
時刻（Time） （検索専用）	ヘルス イベントのタイムスタンプ。
Description	イベントを生成したヘルスモジュールの説明。たとえば、プロセスが実行できない場合に生成されるヘルス イベントには [Unable to Execute] というラベルが付けられます。
Value	イベントが生成されたヘルス テストから得られた結果の値（単位数）。 たとえば、監視対象デバイスが 80% 以上の CPU リソースを使用しているときに生成されるヘルス イベントをFirepower Management Centerが生成した場合の値は 80 ～ 100 です。

フィールド	説明
単位	結果の単位記述子。アスタリスク（*）を使用してワイルドカード検索を作成できます。 たとえば、監視対象デバイスが 80% 以上の CPU リソースを使用しているときに生成されるヘルス イベントをFirepower Management Centerが生成した場合の単位記述子はパーセント記号（%）です。
Status	アプライアンスに報告されるステータス（[クリティカル（Critical）]、[黄色（Yellow）]、[緑色（Green）]、または [無効（Disabled）]）。
ドメイン（Domain）	管理対象デバイスによって報告されたヘルス イベントの場合は、ヘルス イベントを報告したデバイスのドメイン。Firepower Management Center によって報告されたヘルス イベントの場合は、`Global`。このフィールドは、マルチドメイン展開の場合にのみ存在します。
Device	ヘルスイベントが報告されたアプライアンス。

ヘルス モニタリングの履歴

機能	バージョン	詳細
URL フィルタリング モニタの改善	6.4	URL フィルタリング モニタ アラートの時間しきい値を設定できるようになりました。 画面の変更：**[システム（System）]** > **[ヘルス（Health）]** > **[ポリシー（Policy）]** > **[URL フィルタリング モニタ（URL Filtering Monitor）]** ページの新しいオプション。 サポートされているプラットフォーム： Firepower Management Center

機能	バージョン	詳細
新規ヘルス モジュール：デバイス上での脅威データの更新	6.3	新しいモジュールの [デバイス上での脅威データの更新（Threat Data Updates on Devices）] を追加しました。 このモジュールは、デバイスが脅威の検出に使用する特定のインテリジェンス データと設定が指定した時間内にデバイス上で更新されなかった場合にアラートを発行します。 新しい画面：**[システム（System）]** > **[正常性（Health）]** > **[ポリシー（Policy）]** に新しい正常性ポリシーを表示 変更後の画面：**[システム（System）]** > **[正常性（Health）]** > **[モニタ（Monitor）]** に新しいモニタ結果を表示 サポートされるプラットフォーム：6.3 以降のバージョンを実行している Firepower Management Center および管理対象デバイス
ヘルス モニタリング	—	バージョン 6.0 よりも前に導入された機能です。 新しい画面：**[システム（System）]** > **[正常性（Health）]** にメニュー オプションを表示 サポートされるプラットフォーム：Firepower Management Center および管理対象デバイス



第 15 章

システムのモニタリング

以下のトピックでは、Firepower システムをモニタする方法を示します。

システム統計について

Firepower Management Center および 7000 & 8000 シリーズ デバイスに関するシステム統計情報を確認できます。

[統計情報（Statistics）] ページには、アプライアンスの現在の一般的ステータスに関する統計情報（ディスク使用量とシステム プロセス）、データ コリレータ統計情報（FMC のみ）、侵入イベント情報（FMC のみ）が表示されます。

[ホスト統計情報（Host Statistics）] セクション

次の表に、[統計情報（Statistics）] ページにリストされるホスト統計情報を示します。

表 *44 :* ホスト統計情報（*Host Statistics*）

カテゴリ	説明
Time	システムの現在の時刻。
Uptime	システムが前回起動されてから経過した日数（該当する場合）、時間数、および分数。

カテゴリ	説明
Memory Usage	使用中のシステム メモリの割合。
Load Average	直前の 1 分間、5 分間、15 分間の CPU キュー内の平均プロセス数。
Disk Usage	使用中のディスクの割合。詳細なホスト統計情報を表示するには、矢印をクリックします。
Processes	システムで実行されているプロセスの概要。

[ディスク使用量（Disk Usage）] セクション

[統計情報（Statistics）] ページの [ディスク使用率（Disk Usage）] セクションは、カテゴリ別およびパーティション ステータス別に、ディスク使用量のクイック概要を示します。マルウェア ストレージ パックがデバイスにインストールされている場合、そのパーティション ステータスも確認できます。このページを定期的に監視して、システム プロセスおよびデータベースで十分なディスク領域が使用可能であることを確認できます。

ヒント　Firepower Management Center で、ヘルス モニタを使用して、ディスク使用状況を監視し、ディスク容量不足の状態をアラートすることもできます。

[プロセス（Processes）] セクション

[統計情報（Statistics）] ページの [プロセス（Processes）] セクションでは、アプライアンスで現在実行中のプロセスを表示できます。これは、一般的なプロセス情報と、実行中の各プロセスに固有の情報を提供します。Firepower Management Center の Web インターフェイスを使用すると、管理対象デバイスのプロセスのステータスを表示できます。

アプライアンスで実行されるプロセスには、デーモンと実行可能ファイルの 2 種類があることに注意してください。デーモンは常に実行され、実行可能ファイルは必要に応じて実行されます。

プロセス使用状況フィールド

統計情報ページのプロセス セクションを展開すると、以下を表示できます。

[CPU（Cpu(s)）]

次の CPU 使用状況情報がリストされます：

- ユーザ プロセスの使用状況の割合

- システム プロセスの使用状況の割合
- nice使用状況の割合（高い優先度を示す、負のnice値を持つプロセスのCPU使用状況）。nice 値は、システム プロセスのスケジュールされた優先度を示しており、-20（最も高い優先度）から 19（最も低い優先度）の範囲の値になります。
- アイドル状態の使用状況の割合

[メモリ（Mem）]

以下のメモリ使用状況情報がリストされます。

- メモリ内の合計キロバイト数
- メモリ内の使用キロバイト数の合計
- メモリ内の空きキロバイト数の合計
- メモリ内のバッファに書き出されたキロバイト数の合計

[切替（Swap）]

以下のスワップ使用状況情報がリストされます。

- スワップ内の合計キロバイト数
- スワップ内の使用キロバイト数の合計
- スワップ内の空きキロバイト数の合計
- スワップ内のキャッシュされたキロバイト数の合計

次の表に、プロセス セクションに表示される各列を示します。

表 *45*：プロセス リスト カラム

カラム	説明
Pid	プロセス ID 番号
Username	プロセスを実行しているユーザまたはグループの名前
Pri	プロセスの優先度
Nice	*nice* 値。プロセスのスケジューリング優先度を示す値です。値は-20（最も高い優先度）から 19（最も低い優先度）までの範囲になります。

カラム	説明
Size	プロセスで使用されるメモリ サイズ（値の後ろにメガバイトを表す m がない場合はキロバイト単位）
Res	メモリ内の常駐ページング ファイルの量（値の後ろにメガバイトを表す m がない場合はキロバイト単位）
State	プロセスの状態： • D - プロセスが中断不能スリープ状態（通常は入出力）にある • N - プロセスの nice 値が正の値 • R - プロセスが実行可能である（実行するキュー上で） • S - プロセスがスリープ モードにある • T - プロセスがトレースまたは停止されている • W - プロセスがページングしている • X - プロセスがデッド状態である • Z - プロセスが機能していない • < - プロセスの nice 値が負の値
Time	プロセスが実行されている時間（時間 : 分 : 秒）
Cpu	プロセスが使用している CPU の割合
Command	プロセスの実行可能ファイル名

関連トピック

システム デーモン （388 ページ）
実行可能ファイルおよびシステム ユーティリティ （391 ページ）

システム デーモン

デーモンは、アプライアンスで継続的に実行されます。これにより、サービスが使用可能になり、必要に応じてプロセスが生成されるようになります。次の表では、[Process Status] ページに表示されるデーモンをリストし、その機能について簡単に説明します。

（注） 次の表は、アプライアンスで実行される可能性があるすべてのプロセスの包括的なリストではありません。

表 *46 :* システム デーモン

デーモン	説明
crond	スケジュールされたコマンド（cron ジョブ）の実行を管理します
dhclient	ダイナミック ホスト IP アドレッシングを管理します
fpcollect	クライアントとサーバのフィンガープリントの収集を管理します
httpd	HTTP（Apache Web サーバ）プロセスを管理します
httpsd	HTTPS（SSL を使用した Apache Web サーバ）サービスを管理し、SSL および有効な証明書の認証が機能しているかチェックし、アプライアンスへの安全な Web アクセスを提供するためにバックグラウンドで実行します。
keventd	Linux カーネルのイベント通知メッセージを管理します
klogd	Linux カーネル メッセージのインターセプションおよびロギングを管理します
kswapd	Linux カーネルのスワップ メモリを管理します
kupdated	ディスクの同期を実行する、Linux カーネルの更新プロセスを管理します
mysqld	データベース プロセスを管理します
ntpd	Network Time Protocol（NTP）プロセスを管理します
pm	すべての Firepower システム プロセスを管理し、必要なプロセスを始動し、予期せずに失敗したプロセスをすべて再始動します
reportd	レポートを管理します

デーモン	説明
safe_mysqld	データベースのセーフ モード運用を管理し、エラーが発生した場合にはデータベース デーモンを再始動し、ランタイム情報をファイルに記録します
SFDataCorrelator	データ転送を管理します
sfestreamer （FMC のみ）	Event Streamer を使用するサードパーティ製クライアント アプリケーションへの接続を管理します
sfmgr	アプライアンスへの sftunnel 接続を使用して、リモートでアプライアンスを管理および設定するための RPC サービスを提供します
SFRemediateD （FMC のみ）	修復応答を管理します
sftimeserviced （FMC のみ）	時間同期メッセージを管理対象デバイスに転送します
sfmbservice	アプライアンスへの sftunnel 接続を使用して、リモート アプライアンスで実行されている sfmb メッセージブローカ プロセスへのアクセスを提供します。現在、ヘルス モニタリングでのみ使用されており、管理対象デバイスから Firepower Management Center へ正常なイベントやアラートを送信します。
sftroughd	着信ソケットで接続をリッスンしてから、正しい実行可能ファイル（通常は、Cisco メッセージブローカ sfmb）を呼び出して要求を処理します
sftunnel	リモート アプライアンスとの通信を必要とするすべてのプロセスに対し、安全な通信チャネルを提供します。
sshd	Secure Shell (SSH) プロセスを管理し、アプライアンスへの SSH アクセスを提供するためにバックグラウンドで実行します
syslogd	システム ロギング（syslog）プロセスを管理します

実行可能ファイルおよびシステム ユーティリティ

システム上には、他のプロセスまたはユーザ操作によって実行される実行可能ファイルが数多く存在します。次の表に、[プロセス ステータス（Process Status）] ページで表示される実行可能ファイルについて説明します。

表 *47 :* システムの実行可能ファイルおよびユーティリティ

実行可能	説明
awk	awkプログラミング言語で作成されたプログラムを実行するユーティリティ
bash	GNU Bourne-Again シェル
cat	ファイルを読み取り、コンテンツを標準出力に書き込むユーティリティ
chown	ユーザおよびグループのファイル権限を変更するユーティリティ
chsh	デフォルトのログイン シェルを変更するユーティリティ
SFDataCorrelator （FMC のみ）	システムで作成されるバイナリ ファイルを分析し、イベント、接続データ、およびネットワーク マップを生成します。
cp	ファイルをコピーするユーティリティ
df	アプライアンスの空き領域の量をリストするユーティリティ
echo	コンテンツを標準出力に書き込むユーティリティ
egrep	指定された入力を、ファイルおよびフォルダで検索するユーティリティ。標準grepでサポートされていない正規表現の拡張セットをサポートします
find	指定された入力のディレクトリを再帰的に検索するユーティリティ
grep	指定された入力をファイルとディレクトリで検索するユーティリティ
halt	サーバを停止するユーティリティ
httpsdctl	セキュアな Apache Web プロセスを処理する

実行可能	説明
hwclock	ハードウェア クロックへのアクセスを許可するユーティリティ
ifconfig	ネットワーク構成実行可能ファイルを示します。MACアドレスが常に一定になるようにします
iptables	[アクセス権の設定（Access Configuration）] ページに加えられた変更に基づいてアクセス制限を処理します。
iptables-restore	iptables ファイルの復元を処理します
iptables-save	iptables に対する保存済みの変更を処理します
kill	セッションおよびプロセスを終了するために使用できるユーティリティ
killall	すべてのセッションおよびプロセスを終了するために使用できるユーティリティ
ksh	Korn シェルのパブリック ドメイン バージョン
logger	コマンドラインから syslog デーモンにアクセスする方法を提供するユーティリティ
md5sum	指定したファイルのチェックサムとブロック数を印刷するユーティリティ
mv	ファイルを移動（名前変更）するユーティリティ
myisamchk	データベース テーブルの検査および修復を示します
mysql	データベース プロセスを示します。複数のインスタンスが表示されることがあります
openssl	認証証明書の作成を示します。
perl	perl プロセスを示します。
ps	標準出力にプロセス情報を書き込むユーティリティ
sed	1 つ以上のテキスト ファイルの編集に使用されるユーティリティ

実行可能	説明
sfheartbeat	アプライアンスがアクティブであることを示す、ハートビート ブロードキャストを識別します。ハートビートはデバイスとFirepower Management Centerの間の接続を維持するのに使用されます
sfmb	メッセージ ブローカ プロセスを示します。Firepower Management Centerとデバイスとの間の通信を処理します。
sh	Korn シェルのパブリック ドメイン バージョン
shutdown	アプライアンスをシャットダウンするユーティリティ
sleep	指定された秒数のあいだプロセスを中断するユーティリティ
smtpclient	電子メールイベント通知機能が有効な場合に、電子メール送信を処理するメール クライアント
snmptrap	SNMP 通知機能が有効な場合に、指定されたSNMP トラップ サーバにSNMP トラップ データを転送します
snort	Snort が動作していることを示します
ssh	アプライアンスへの Secure Shell (SSH) 接続を示します
sudo	sudoプロセスを示します。これにより、admin以外のユーザが実行可能ファイルを実行できるようになります
top	上位の CPU プロセスに関する情報を表示するユーティリティ
touch	指定したファイルへのアクセス時刻や変更時刻を変更するために使用できるユーティリティ
vim	テキストファイルの編集に使用されるユーティリティ
wc	指定したファイルの行、ワード、バイトのカウントを実行するユーティリティ

関連トピック

アクセス リストの設定 （1291 ページ）

[SFDataCorrelator プロセス統計情報（SFDataCorrelator Process Statistics）] セクション

Firepower Management Center では、現在の日付のデータ コリレータとネットワーク検出プロセスに関する統計情報を表示できます。管理対象デバイスがデータの取得、復号化、および分析を実行する際に、ネットワーク検出プロセスはデータをフィンガープリントおよび脆弱性データベースと関連付けてから、Firepower Management Center で実行中のデータ コリレータで処理されるバイナリ ファイルを生成します。データ コリレータはバイナリ ファイルの情報を分析し、イベントを生成し、ネットワーク マップを作成します。

ネットワーク検出とデータ コリレータに表示される統計情報は、デバイスごとに 0:00 から 23:59 までの間に収集された統計情報を使用した、当日の平均です。

次の表に、データ コリレータ プロセスに表示される統計情報を示します。

表 *48 :* データ コリレータ プロセスの統計情報

カテゴリ	説明
Events/Sec	Data Correlator が受信し処理する検出イベントの 1 秒当たりの数
Connections/Sec	Data Correlator が受信し処理する接続の 1 秒当たりの数
CPU Usage — User (%)	当日のユーザプロセスで使用される CPU 時間の平均割合
CPU Usage — System (%)	当日のシステムプロセスで使用される CPU 時間の平均割合
VmSize（KB）	当日の Data Correlator に割り当てられたメモリの平均サイズ（キロバイト単位）
VmRSS（KB）	当日のデータ コリレータで使用されるメモリの平均量（キロバイト単位）

[侵入イベント情報（IntrusionEventInformation）]セクション

Firepower Management Centerデバイスと管理対象デバイスのどちらでも、[統計情報（Statistics）] ページで、侵入イベントに関するサマリ情報を確認できます。表示される情報には、前回の侵入イベントの日時、過去1時間および過去1日に発生したイベントの合計数、データベース内のイベントの合計数などがあります。

（注） [統計情報（Statistics）] ページの [侵入イベント情報（Intrusion Event Information）] セクションにある情報は、Firepower Management Center に送信された侵入イベントではなく、管理対象デバイスに保存されている侵入イベントに基づいています。管理対象デバイスが侵入イベントをローカルに格納できない（または格納しないように設定されている）場合、侵入イベント情報はこのページに表示されません。

次の表に、[統計情報（Statistics）] ページの [侵入イベント情報（Intrusion Event Information）] セクションに表示される統計情報を示します。

表 *49 :* 侵入イベント情報（*Intrusion Event Information*）

統計	説明
Last Alert Was	前回のイベントが発生した日時
Total Events Last Hour	過去 1 時間に発生したイベントの合計数
Total Events Last Day	過去 24 時間に発生したイベントの合計数
Total Events in Database	イベント データベース内のイベントの合計数

システム統計情報の表示

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	グローバルだけ	Admin/Maint

Firepower Management Center では、Web インターフェイスは FMC とその管理対象となるすべてのデバイスの統計情報を表示します。7000 および 8000 シリーズ デバイスでは、システムはそのデバイスの統計情報のみを表示します。

ステップ 1 **[System]** > **[Monitoring]** > **[Statistics]**を選択します。

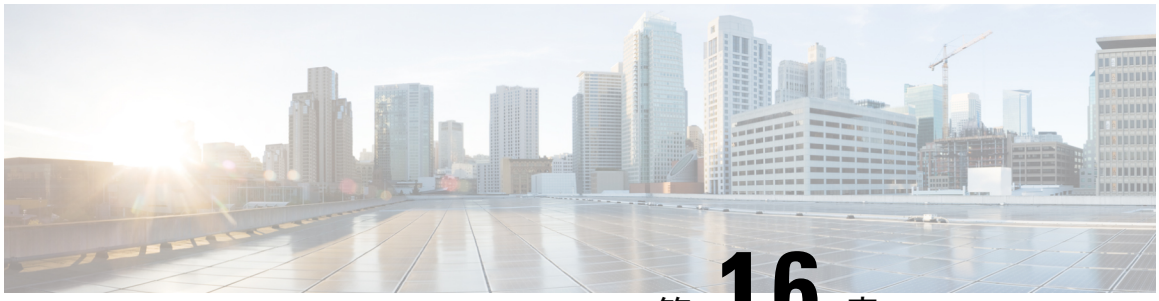
ステップ 2 （FMC のみ）[デバイスの選択（Select Device(s)）] リストからデバイスを選択し、[デバイスの選択（Select Devices）] をクリックします。

ステップ 3 使用可能な統計を表示します。

ステップ 4 [ディスク使用状況（Disk Usage）] セクションでは、次の操作を実行できます。

- [カテゴリ別（By Category）] 積み上げ横棒で、ディスク使用量カテゴリの上にポインタを移動すると、以下が（順番に）表示されます。
  - そのカテゴリが使用する使用可能なディスク領域の割合
  - ディスク上の実際のストレージ領域
  - そのカテゴリで使用可能なディスク領域の合計
- [パーティション別（By Partition）] の横にある下矢印をクリックして展開します。マルウェア ストレージ パックがインストールされている場合は、`/var/storage` パーティションの使用状況が表示されます。

ステップ 5 （オプション）[プロセス（Processes）] の横にある矢印をクリックすると、プロセス使用状況フィールド（386 ページ）で説明されている情報が表示されます。



第 16 章

システムの監査

次のトピックでは、システム上のアクティビティを監査する方法について説明します。

- システム監査について （397 ページ）
- 外部ロケーションへの監査ログの送信について （397 ページ）
- 監査レコード （398 ページ）
- システム ログ （406 ページ）

システム監査について

システム上のアクティビティを 2 つの方法で監査できます。Firepower システムの一部であるアプライアンスによって、Webインターフェイスとユーザとの対話のそれぞれに対して監査レコードが生成され、システム ステータス メッセージがシステム ログに記録されます。

関連トピック

標準レポートの概要 （2775 ページ）

外部ロケーションへの監査ログの送信について

FMC から監査ログを外部の場所に送信する場合は、以下を参照してください。

- 監査ログ （1292 ページ）
- 監査ログ証明書 （1295 ページ）

従来型デバイスの場合は、以下を参照してください。

- 従来型デバイスからの監査ログのストリーミング （1338 ページ）
- 従来型デバイス用の有効な監査ログ サーバ証明書の要求 （1340 ページ）
- 7000/8000 シリーズ デバイスでのセキュアな監査ログ ストリーミング用の署名付きクライアント証明書の取得 （1348 ページ）

監査レコード

Firepower Management Center および 7000 および 8000 シリーズ デバイスは、ユーザ アクティビティに関する読み取り専用の監査情報をログに記録します。監査ログは標準イベント ビューに表示され、監査ビュー内の任意の項目に基づいて監査ログ メッセージを表示、ソート、およびフィルタリングできます。監査情報を簡単に削除したり、それに関するレポートを作成したりすることができ、ユーザが行った変更に関する詳細なレポートを表示することもできます。

監査ログには最大 100,000 個のエントリが保存されます。監査ログ エントリの数が 100,000 を超えると、アプライアンスは最も古いレコードをデータベースからプルーニングして、100,000 エントリまで数を削減します。

（注） 7000 または 8000 シリーズ デバイスをリブートした直後にすばやく補助 CLI にログインした場合、そこで実行するコマンドは、ローカル Web インターフェイスが使用可能になるまでは監査ログに記録されません。

監査レコードの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin

Firepower Management Center または 7000 および 8000 シリーズ デバイスで、監査レコードのテーブルを表示できます。事前定義された監査ワークフローには、イベントを示す単一のテーブル ビューが含まれます。ユーザは検索する情報に応じてテーブル ビューを操作することができます。また、特定のニーズを満たす情報だけを表示するカスタム ワークフローを作成することもできます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

ステップ 1 **[System]** > **[Monitoring]** > **[Audit]** を使用して監査ログのワークフローにアクセスします。

ステップ 2 イベントが 1 つも表示されない場合は、時間範囲を調整することを考慮してください。詳細については、イベント時間の制約 （2952 ページ）を参照してください。

（注） イベント ビューを時間によって制約している場合は、（グローバルかイベント固有かに関係なく）アプライアンスに設定されている時間枠の外で生成されたイベントが、イベント ビューに表示されます。アプライアンスに対してスライドする時間枠を設定した場合でも、この状況が発生することがあります。

ステップ 3 次の選択肢があります。

- テーブルのカラムの内容について詳しく調べるには、システム ログ （406 ページ）を参照してください。
- 現在のワークフロー ページでイベントをソートしたり、制限したりするには、テーブル ビュー ページの使用 （2941 ページ）を参照してください。
- 現在の制約を維持しながら現在のワークフローのページ間で移動するには、ワークフロー ページの左上にある該当するページ リンクをクリックします。詳細については、ワークフローの使用 （2931 ページ）を参照してください。
- ワークフローの次のページにドリルダウンするには、ドリルダウン ページの使用 （2940 ページ）を参照してください。
- 特定の値で制約するには、行内の値をクリックします。ドリルダウン ページで値をクリックすると、次のページに移動し、その値だけに制約されます。テーブル ビューの行内の値をクリックすると、テーブル ビューが制限され、次のページに**ドリルダウンされない**ことに注意してください。詳細については、イベント ビューの制約 （2960 ページ）を参照してください。

  ヒント　テーブル ビューでは、必ずページ名に「Table View」が含まれます。

- 監査レコードを削除するには、削除するイベントの横にあるチェックボックスをオンにして [削除（Delete）] をクリックするか、[すべて削除（Delete All）] をクリックして現在の制約されているビューにあるすべてのイベントを削除します。
- 現在のページにすぐに戻れるようにページをブックマークするには、[このページをブックマーク（Bookmark This Page）] をクリックします。詳細については、ブックマーク （2964 ページ）を参照してください。
- ブックマークの管理ページに移動するには、[ブックマークの表示（View Bookmarks）] をクリックします。詳細については、ブックマーク （2964 ページ）を参照してください。
- 現在のビューのデータに基づいてレポートを生成するには、[レポート デザイナ（Report Designer）] をクリックします。詳細については、イベント ビューからのレポート テンプレートの作成 （2780 ページ）を参照してください。
- 監査ログに記録された変更の概要を表示するには、[メッセージ（Message）] カラムの該当するイベントの横にある比較アイコン（）をクリックします。詳細については、「監査ログを使って変更を調査する （401 ページ）」を参照してください。

関連トピック

イベント ビューの制約 （2960 ページ）

監査ログのワークフロー フィールド

次の表で、表示および検索できる監査ログ フィールドについて説明します。

表 *50* : 監査ログのフィールド

フィールド	説明
Time	アプライアンスが監査レコードを生成した日時。

フィールド	説明
User	監査イベントをトリガーとして使用したユーザのユーザ名。
サブシステム	監査レコードが生成されたときにユーザがたどったフル メニュー パス。たとえば、**[System]** > **[Monitoring]** > **[Audit]** は、監査ログを表示するためのメニュー パスです。 メニュー パスが該当しない数少ないケースでは、[サブシステム（Subsystem）] フィールドにイベント タイプのみが表示されます。たとえば、**Login** はユーザのログイン試行を分類します。
メッセージ（Message）	ユーザが実行したアクション、またはユーザがページでクリックしたボタン。 たとえば、`Page View` は、[サブシステム（Subsystem）] に示されているページをユーザが単に表示したことを意味します。`Save` は、ユーザがページの [保存（Save）] ボタンをクリックしたことを意味します。 Firepower システムに対する変更は比較アイコン（）付きで表示され、アイコンをクリックすると変更の概要を確認することができます。
ソース IP	ユーザが使用したホストに関連付けられている IP アドレス。 注：このフィールドを検索する場合は、特定の IP アドレスを入力する必要があります。監査ログの検索で IP 範囲を使用することはできません。
ドメイン（Domain）	監査イベントがトリガーされたときのユーザの現行ドメイン。 This field is only present if you have ever configured the Firepower Management Center for multitenancy.
設定の変更（Configuration Change） （検索専用）	設定の変更の監査レコードを検索結果に表示するかどうかを指定します。(`yes` または `no`)

フィールド	説明
メンバー数（Count）	各行に表示された情報と一致するイベントの数。[カウント（Count）] フィールドは、複数の同一行が生成される制限を適用した後でのみ表示されることに注意してください。このフィールドは検索できません。

関連トピック

イベントの検索 （2967 ページ）

[監査イベント（Audit Events）] テーブル ビュー

イベント ビューのレイアウトを変更したり、ビュー内のイベントをフィールド値で制限したりできます。カラムを無効にする場合は、非表示にするカラム見出しの [閉じる] アイコン（ ）をクリックした後、表示されるポップアップ ウィンドウで [Apply] をクリックします。カラムを無効にすると、あとで再び追加した場合を除き、そのカラムはセッション有効期間にわたって無効になります。最初のカラムを無効にした場合、[Count] カラムが追加されることに注意してください。

他のカラムを表示/非表示にしたり、無効になったカラムをビューに再び追加したりするには、該当するチェックボックスを選択またはクリアしてから [適用（Apply）] をクリックします。

テーブル ビューの行内の値をクリックすると、テーブル ビューが制約されます（ワークフロー内の次のページにはドリルダウンされません）。

ヒント テーブル ビューでは、必ずページ名に「テーブル ビュー（Table View）」が含まれます。

関連トピック

ワークフローの使用 （2931 ページ）

監査ログを使って変更を調査する

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin

監査ログを使用して、システムの変更に関する詳細レポートを表示できます。これらのレポートは、現在のシステム設定を、特定の変更が行われる直前の設定と比較します。

[設定の比較（Compare Configurations）] ページには、変更前のシステム設定と、現在実行中の設定との違いが横並び形式で表示されます。監査イベント タイプ、最終変更時間、および変更を行ったユーザ名が、各設定の上のタイトル バーに表示されます。

2 つの設定の違いは次のように強調表示されます。

- 青は、強調表示されている設定項目が2つの設定間で異なっていることを示し、異なっている部分は赤のテキストで表示されます。
- 緑は、強調表示されている設定項目が一方の設定に含まれ、もう一方の設定には含まれないことを示します。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

ステップ1 **[System]** > **[Monitoring]** > **[Audit]**を選択します。

ステップ2 [メッセージ（Message）]カラムの該当する監査ログイベントの横にある比較アイコン（）をクリックします。

ヒント タイトル バーの上の [前へ（Previous）] または [次へ（Next）] をクリックすると、個々の変更の間を移動できます。また、変更の概要が複数のページにまたがる場合は、右側のスクロール バーを使って追加の変更を表示できます。

監査レコードの抑制

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin

監査ポリシーで、Firepower System/ユーザ間の特定のタイプのインタラクションを監査する必要がない場合は、それらのインタラクションによって、Firepower Management Center または 7000 および 8000 シリーズ デバイス上で監査レコードが生成されないように設定できます。たとえば、デフォルトでは、ユーザがオンライン ヘルプを表示するたびに、Firepower System は監査レコードを生成します。このようなインタラクションのレコードを保持する必要がない場合は、これらを自動的に抑制できます。

監査イベントの抑制を設定するには、アプライアンスの`admin`ユーザアカウントにアクセスできる必要があり、アプライアンスのコンソールにアクセスできる（またはセキュア シェルを開くことができる）必要があります。

⚠

注意 許可された担当者だけが、アプライアンスとその`admin`アカウントにアクセスできることを確認してください。

`/etc/sf`ディレクトリに、次の形式で1つ以上の`AuditBlock`ファイルを作成します。タイプは、監査ブロック タイプ （403 ページ）で説明されているいずれかのタイプになります。

`AuditBlock.`*`type`*

（注） 特定のタイプの監査メッセージに関する AuditBlock.*type* ファイルを作成した後で、それらの抑制を解除することにした場合、AuditBlock.*type* ファイルの内容を削除する必要がありますが、ファイル自体は Firepower System に残してください。

監査ブロック タイプ

それぞれの監査ブロック タイプの内容は、以下の表に記載されているように、特定の形式でなければなりません。ファイル名の大文字/小文字を必ず正しく表記してください。また、ファイルの内容でも大文字と小文字が区別されることに注意してください。

AuditBlock ファイルを追加した場合、サブシステム Audit およびメッセージ Audit Filter*type*Changed を含む監査レコードが監査イベントに追加されることに注意してください。セキュリティ上の理由から、この監査レコードを抑制することは**できません**。

表 *51* : 監査ブロック タイプ

タイプ	説明
アドレス（Address）	AuditBlock.address という名前のファイルを作成し、監査ログから抑制する IP アドレスを 1 行に 1 つずつ含めます。部分的な IP アドレスを使用できます（ただしアドレスの先頭から照合されます）。たとえば、部分的なアドレス 10.1.1 は、10.1.1.0 から 10.1.1.255 までのアドレスと一致します。
メッセージ	AuditBlock.message という名前のファイルを作成し、抑制するメッセージ部分文字列を 1 行に 1 つずつ含めます。 たとえば backup をこのファイルに含めた場合、部分文字列の照合により backup という語を含むすべてのメッセージが抑制されることに注意してください。
サブシステム	AuditBlock.subsystem という名前のファイルを作成し、抑制するサブシステムを 1 行に 1 つずつ含めます。 部分文字列は照合**されない**ことに注意してください。正確な文字列を使用する必要があります。監査対象のサブシステムのリストについては、監査対象のサブシステム （404 ページ）を参照してください。

タイプ	説明
ユーザ（User）	`AuditBlock.user` という名前のファイルを作成し、抑制するユーザ アカウントを 1 行に 1 つずつ含めます。部分的な文字列の照合を使用できます（ただしユーザ名の先頭から照合されます）。たとえば、部分的なユーザ名 `IPSAnalyst` はユーザ名 `IPSAnalyst1` および `IPSAnalyst2` と一致します。

監査対象のサブシステム

次の表に、監査対象のサブシステムを示します。

表 *52*：サブシステム名

名前	どの機能のユーザ インタラクションを含んでいるか
Admin	管理機能：システムとアクセス権の設定、時刻の同期、バックアップと復元、デバイス管理、ユーザ アカウントの管理、スケジュール設定など
Alerting	アラート機能（電子メール アラート、SNMP アラート、Syslog アラートなど）
監査ログ（Audit Log）	監査イベントの表示
Audit Log Search	監査イベントの検索
Cisco Security Packet Analyzer の統合	Cisco Security Packet Analyzer 統合
コマンド ライン	コマンドライン インターフェイス
Configuration	電子メール アラート機能
contextual cross-launch	システムに追加された外部リソース、またはダッシュボードとイベント ビューからアクセスされた外部リソース
COOP	継続的な運用機能
Date	イベント ビューの日時範囲
Default Subsystem	サブシステムが割り当てられていないオプション
Detection & Prevention Policy	侵入ポリシーのメニュー オプション

名前	どの機能のユーザ インタラクションを含んでいるか
Error	システム レベルのエラー
eStreamer	eStreamer 構成
EULA	エンド ユーザ ライセンス契約書の確認
Event	侵入およびディスカバリ イベント ビュー
Events Clipboard	侵入イベント クリップボード
Events Reviewed	レビューされた侵入イベント
Events Search	あらゆるイベント検索
ルール更新のインストールの失敗（Failed to install rule update）`rule_update_id`	ルール更新のインストール
ヘッダー	ユーザ ログイン後のユーザ インターフェイスの最初の表示
Health	ヘルス モニタリング
Health Events	ヘルス モニタリング イベントの表示
Help	オンライン ヘルプ
高可用性	高可用性ペアでの Firepower Management Center の確立と管理
IDS インパクト フラグ（IDS Impact Flag）	侵入イベントの影響フラグの設定
IDS ポリシー（IDS Policy）	侵入ポリシー
IDS ルール SID：`sig_id` リビジョン：`rev_num`	SID 別の侵入ルール
Incidents	侵入インシデント
インストール（Install）	更新のインストール
Intrusion Events	侵入イベント
Login	Web インターフェイスのログイン/ログアウト機能
ログアウト	Web インターフェイス ログアウト機能
メニュー	あらゆるメニュー オプション

名前	どの機能のユーザ インタラクションを含んでいるか
[設定のエクスポート（Configuration export）] > [config_type] > [config_name]	特定のタイプ/名前の設定のインポート
Permission Escalation	ユーザ ロールのエスカレーション
Preferences	ユーザ アカウントのタイム ゾーンや個々のイベント設定などのユーザ設定
Policy	侵入ポリシーを含むポリシー
Register	FMC でのデバイスの登録
リモート ストレージ デバイス（RemoteStorageDevice）	リモート ストレージ デバイスの設定
Reports	レポート リスト機能およびレポート デザイナ機能
ルール（Rules）	侵入ルール（侵入ルール エディタとルールのインポート プロセスを含む）
ルール更新インポート ログ（Rule Update Import Log）	ルール更新のインポート ログの表示
Rule Update Install	ルール更新のインストール
セッションの時間切れ	Web インターフェイスのセッション タイムアウト
ステータス（Status）	syslog およびホストやパフォーマンスの統計情報
System	システム全体のさまざまな設定
タスク キュー（Task Queue）	バックグラウンド プロセス ステータスの表示
Users	ユーザ アカウントとロールの作成および変更

システム ログ

[システム ログ（System Log）]（syslog）ページには、アプライアンスのシステム ログ情報が表示されます。システム ログには、システムによって生成された各メッセージが表示されます。次の項目が順にリストされます。

- メッセージが生成された日付

- メッセージが生成された時刻
- メッセージを生成したホスト
- メッセージ自体

システム ログの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	グローバルだけ	Admin/Maint

システム ログ情報はローカルな情報です。たとえば、Firepower Management Center を使用して、管理対象デバイスのシステム ログ内のシステム ステータス メッセージを見ることは**できません**。

UNIX ファイル検索ユーティリティ Grep で処理可能なほとんどの構文を使用してメッセージをフィルタ処理できます。つまり、パターン マッチング用に Grep 互換の正規表現を使用できます。

ステップ 1 **[System]** > **[Monitoring]** > **[Syslog]**を選択します。

ステップ 2 システム ログ内で特定のメッセージ内容を検索するには、次のようにします。

a) システム ログ フィルタの構文 （407 ページ）に記載されているように、フィルタのフィールドに単語またはクエリを入力します。

Grep 互換の検索構文のみがサポートされています。

例：

ユーザ名 ”Admin” を含むすべてのログ エントリを検索するには `Admin` を使用します。

11 月 27 日に生成されたすべてのログ エントリを検索するには、（`Nov 27` や `Nov*27` ではなく）`Nov[[:space:]]*27` または `Nov.*27` を使用します。

11 月 5 日のデバッグ情報の認証を含むすべてのログ エントリを検索するには、`Nov[[:space:]]*5.*AUTH.*DEBUG` を使用します。

b) 検索で大文字と小文字を区別するには、[大文字と小文字を区別する（Case-sensitive）] を選択します。（デフォルトでは、フィルタで大文字/小文字は区別されません。）

c) 入力した基準を満たしていないすべてのシステム ログ メッセージを検索するには、[除外（Exclusion）] を選択します。

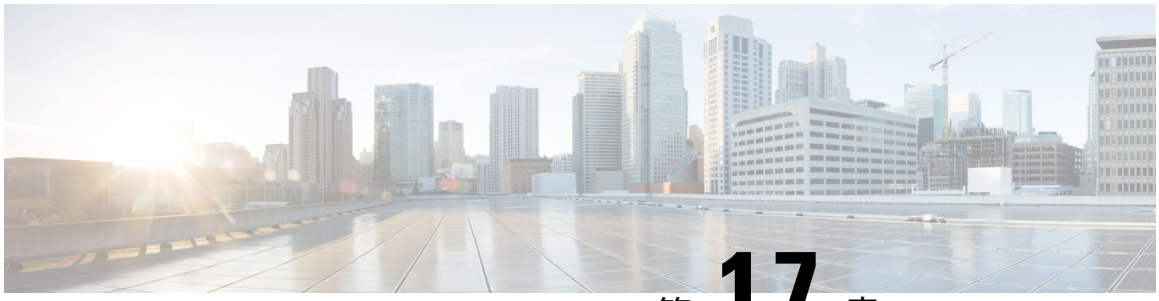
d) [移動（Go）] をクリックします。

システム ログ フィルタの構文

次の表に、システム ログ フィルタで使用できる正規表現構文を示します。

表 *53:* システム ログ フィルタ構文

構文のコンポーネント	説明	例
。	任意の文字またはスペースと一致します	Admi. は、Admin、AdmiN、Admi1、および Admi と一致します。
[[:alpha:]]	任意の英文字と一致します	[[:alpha:]]dmin は、Admin、bdmin、および Cdmin と一致します
[[:upper:]]	任意の大文字の英文字と一致します	[[:upper:]]dmin は、Admin、Bdmin、および Cdmin と一致します
[[:lower:]]	任意の小文字の英文字と一致します	[[:lower:]]dmin は、admin、bdmin、および cdmin と一致します
[[:digit:]]	任意の数字と一致します	[[:digit:]]dmin は、0dmin、1dmin、および 2dmin と一致します
[[:alnum:]]	任意の英数字と一致します	[[:alnum:]]dmin は、1dmin、admin、2dmin、および bdmin と一致します
[[:space:]]	タブを含む、任意のスペースと一致します	Feb[[:space:]]29 は 2 月 29 日のログと一致します
*。	その前にある文字または式のゼロ個以上のインスタンスと一致します	ab* は、a、ab、abb、ca、cab、および cabb と一致します [ab]* はすべてのものと一致します
?	ゼロ個または 1 つのインスタンスと一致します	ab? は、a または ab と一致します
\	これを使用すると、通常は正規表現構文と解釈される文字を検索できます	alert\? は、alert? と一致します



第 17 章

システムのトラブルシューティング

以下のトピックは、Firepower システムで発生する可能性のある問題を診断する方法について説明します。

トラブルシューティングの最初の手順

- 問題の修正を試みるために変更を加える前に、トラブルシューティング ファイルを生成して元の問題をキャプチャします。トラブルシューティング用のヘルス モニタ レポート （419 ページ）およびサブセクションを参照してください。

  サポートのために Cisco TAC に連絡する必要が生じた場合に、このトラブルシューティング ファイルが必要になることがあります。

- メッセージセンターのエラー メッセージと警告メッセージを調べて、調査を開始します。システム メッセージ （410 ページ）を参照してください

- お使いの製品の製品ドキュメント ページの「Troubleshoot and Alerts」という見出しの下にある、該当するテクニカル ノートとその他のトラブルシューティング リソースを探します。FMC 展開に関するトップレベルのドキュメントのリスト ページ （17 ページ）を参照してください。

システム メッセージ

Firepowerシステムで発生した問題を突き止める必要がある場合、調査の出発点となるのはメッセージ センターです。メッセージ センターでは、Firepower システムがシステムのアクティビティとステータスに関して継続的に生成するメッセージを表示できます。

メッセージセンターを開くには、メイン メニューの [展開（Deploy）] ボタンの右隣にある [システム ステータス（System Status）] アイコンをクリックします。このアイコンは、システムのステータスによって以下のように表示されます。

- ：1 つ以上のエラーと任意の数の警告がシステム上に存在することを示します。
- ：1つ以上の警告がシステム上に存在することを示します。エラーは発生していません。
- ：警告とエラーはいずれもシステム上に存在していないことを示します。

アイコンに数字が表示されている場合、その数字は現在のエラー メッセージまたは警告メッセージの数を示します。

メッセージ センターを閉じるには、Firepower システム Web インターフェイス内でメッセージ センターの外側をクリックします。

メッセージ センターに加え、Web インターフェイスには、ユーザのアクティビティおよび進行中のシステム アクティビティに応じて即時にポップアップ通知が表示されます。ポップアップ通知のなかには 5 秒経過すると自動的に非表示になるものや、非表示アイコン（×）をクリックして明示的に表示を消さなければならない「スティッキー」通知もあります。通知リストの最上部にある [表示を消す（Dismiss）] リンクをクリックすると、すべての通知をまとめて非表示にすることができます。

ヒント　スティッキー以外のポップアップ通知の上にマウスのカーソルを合わせると、その通知はスティッキーになります。

システムはユーザのライセンス、ドメイン、アクセス ロールに基づいて、どのメッセージをポップアップ通知やメッセージ センターに表示するか決定します。

メッセージ タイプ

Message Center では、システムのアクティビティとステータスをレポートするメッセージが 3 つのタブに編成されて表示されます。

展開（Deployments）

このタブには、システムの各アプライアンスの設定展開に関連する現在のステータスがドメイン別にグループ化されて表示されます。Firepower システムでは、次の展開ステータス値がこのタブでレポートされます。[履歴の表示（Show History）] をクリックして、展開ジョブに関する追加情報を取得できます。

- [実行中（Running）]（ の表示が回転中）：設定は展開の処理中です。
- [成功（Success）]（）：設定は正常に展開されました。
- [警告（Warning）]（）：警告展開ステータスは、警告システム ステータス アイコン（）とともに表示されるメッセージ数に含まれます。
- [失敗（Failure）]（）：設定は展開に失敗しました。失効ポリシー（459ページ）を参照してください。失敗した展開は、エラー システム ステータス アイコン（）とともに表示されるメッセージ数に含まれます。

ヘルス（Health）

このタブには、システムの各アプライアンスの現在のヘルス ステータス情報がドメイン別にグループ化されて表示されます。ヘルス ステータスは、ヘルス モニタリングについて（349 ページ）に記載されているように、ヘルス モジュールによって生成されます。Firepower システムでは、次のヘルス ステータス値がこのタブでレポートされます。

- [警告（Warning）]（）：アプライアンス上のヘルス モジュールが警告制限を超え、問題が解決されていないことを示します。[ヘルス モニタリング（Health Monitoring）] ページには、これらの状態が黄色い三角形のアイコン（）で示されます。警告ステータスは、警告システム ステータス アイコン（）とともに表示されるメッセージ数に含まれます。
- [重大（Critical）]（）：アプライアンス上のヘルス モジュールが重大制限を超え、問題が解決されていないことを示します。[ヘルス モニタリング（Health Monitoring）] ページには、これらの状態が アイコンで示されます。重大ステータスは、エラー システム ステータス アイコン（）とともに表示されるメッセージ数に含まれます。
- [エラー（Error）]（）：アプライアンス上のヘルス モニタリング モジュールに障害が発生し、それ以降、正常に再実行されていないことを示します。[ヘルス モニタリング（Health Monitoring）] ページには、これらの状態が アイコンで示されます。エラー ステータスは、エラー システム ステータス アイコン（）とともに表示されるメッセージ数に含まれます。

[ヘルス（Health）] タブのリンクをクリックして、[ヘルス モニタリング（Health Monitoring）] ページで関連の詳細情報を表示できます。現在のヘルス ステータス状態がない場合、[ヘルス（Health）] タブにメッセージは表示されません。

タスク

Firepower システムでは、完了するまで時間がかかる可能性がある特定のタスク（構成のバックアップやインストールの更新など）を実行できます。このタブには、これらの長時間実行タスクのステータスが表示され、自分が開始したタスクや、適切なアクセス権がある場合は、システムの他のユーザが開始したタスクが含まれることがあります。このタブには、各メッセージの最新の更新時間に基づいて時系列の逆順にメッセージが表示されます。一部のタスク ステータス メッセージには、問題となっているタスクについての詳細

情報へのリンクが含まれています。Firepower システムでは、次のタスク ステータス値がこのタブでレポートされます。

- [待機中（Waiting）]（）：別の進行中のタスクが完了するまで実行を待機しているタスクを示します。このメッセージ タイプでは、更新の経過表示バーが表示されます。
- [実行中（Running）]（ の表示が回転中）：進行中のタスクを示します。このメッセージ タイプでは、更新の経過表示バーが表示されます。
- [再試行中（Retrying）]（）：自動的に再試行しているタスクを示します。なお、すべてのタスクの再試行が許可されるわけではありません。このメッセージ タイプでは、更新の経過表示バーが表示されます。
- [成功（Success）]（）：正常に完了したタスクを示します。
- [失敗（Failure）]（）：正常に完了しなかったタスクを示します。失敗したタスクは、エラー システム ステータス アイコン（）とともに表示されるメッセージ数に含まれます。
- [停止（Stopped）] または [中断（Suspended）]（）：システム アップデートのために中断されたタスクを示します。停止したタスクを再開することはできません。通常の動作が復元されたら、もう一度タスクを開始してください。
- [スキップ（Skipped）]：進行中のプロセスによって、タスクの開始が妨げられました。タスクの開始をもう一度試行してください。

新しいタスクが開始されると、新しいメッセージがこのタブに表示されます。タスクが完了すると（成功、失敗、または停止のステータス）、タスクを削除するまで、このタブには最終ステータスを示すメッセージが引き続き表示されます。[タスク（Tasks）]タブおよびメッセージデータベースがいっぱいにならないように、メッセージを削除することをお勧めします。

メッセージ管理

メッセージ センターから、以下を実行できます。

- ポップアップ通知の動作を設定します（これらを表示するかどうかを選択します）。
- システム データベースの追加のタスクのステータス メッセージを表示します（削除されていないもので利用可能なものがある場合）。
- 個々のタスクのステータス メッセージを削除します。（これは、削除されたメッセージを確認できるすべてのユーザに影響します）。
- タスクのステータス メッセージを一括で削除します。（これは、削除されたメッセージを確認できるすべてのユーザに影響します）。

ヒント シスコは、表示に加えてデータベースの不要なデータを削除するために、累積されたタスクのステータス メッセージを [タスク（Task）] タブから定期的に削除することを推奨します。データベースのメッセージ数が 100,000 に到達すると、削除したタスクのステータス メッセージが自動的に削除されます。

基本的なシステム情報の表示

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
該当なし	いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）

[バージョン情報（About）] ページには、Firepower システムのさまざまなコンポーネントのモデル、シリアル番号、バージョン情報など、アプライアンスに関する情報が示されます。また、シスコの著作権情報も示されます。

ステップ 1 ページ上部のツールバーから [ヘルプ（Help）] をクリックします。

ステップ 2 [バージョン情報（About）] を選択します。

アプライアンス情報の表示

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	FMC 7000 & 8000 シリーズ	グローバルだけ。	Admin

[System] > **[Configuration]**を選択します。

システム メッセージの管理

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	[展開（Deployment）]：管理者/[設定をデバイスに展開する（Deploy Configuration to Devices）] 権限を持つカスタム ユーザ ロール [ヘルス（Health）]：管理者/[ヘルス（Health）] 権限を持つカスタム ユーザ ロール 他人によって開始されたタスク：管理者/[他のユーザのタスクを確認する（View Other Users' Tasks）] 権限があるカスタム ユーザ ロール 自分が開始したタスク：任意

ステップ 1 [システム ステータス（System Status）] アイコンをクリックして、メッセージ センターを表示します。

ステップ 2 次の選択肢があります。

- [展開（Deployments）] タブをクリックして、設定の展開に関連するメッセージを表示します。展開メッセージの表示 （415 ページ）を参照してください。
- [ヘルス（Health）] タブをクリックして、Firepower Management Center とそれに登録したデバイスの状況に関連するメッセージを表示します。ヘルス メッセージの表示（416 ページ）を参照してください。
- [タスク（Tasks）] タブをクリックして、長時間実行タスクに関連するメッセージを表示または管理します。タスク メッセージの表示 （417 ページ）またはタスク メッセージの管理 （418 ページ）を参照してください。

- Message Centerの右上隅にある歯車アイコン（⚙）をクリックして、ポップアップ通知の動作を設定します。通知動作の設定 （418 ページ）を参照してください。

展開メッセージの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	[設定をデバイスに展開する（Deploy Configuration to Devices）] 権限を持つ管理者/ユーザ ロール

ステップ 1 [システム ステータス（System Status）] アイコンをクリックして、メッセージ センターを表示します。

ステップ 2 [展開（Deployments）] タブをクリックします。

ステップ 3 次の選択肢があります。

- 現在のすべての展開ステータスを表示するには、[合計（total）] をクリックします。
- 任意の展開ステータスに関するメッセージのみを表示するには、そのステータスの値をクリックします。
- 展開の経過時間、開始時刻および停止時刻を表示するには、メッセージの時間経過インジケータ（たとえば、[1分5秒（1m 5s）]）の上にカーソルを置きます。

ステップ 4 展開ジョブの詳細情報を表示するには、[履歴を表示（Show History）] をクリックします。

[展開の履歴（Deployment History）] テーブルには、左側の列に展開ジョブが新しい順にリストされています。

a) 展開ジョブを選択します。

右側の列のテーブルには、ジョブに含まれていた各デバイスと、デバイスごとの展開ステータスが表示されます。

b) デバイスからの応答、および展開中にデバイスに送信されたコマンドを表示するには、デバイスの [トランスクリプト（Transcript）] カラムにあるダウンロード アイコンをクリックします。

トランスクリプトには、次のセクションが含まれています。

- [Snort を適用（Snort Apply）]：Snort 関連ポリシーから障害または応答が発生すると、メッセージがこのセクションに表示されます。通常、このセクションは空です。
- [CLI を適用（CLI Apply）]：このセクションは、Lina プロセスに送信されたコマンドを使用して設定される機能を対象にしています。

- [インフラストラクチャ メッセージ（Infrastructure Messages）]：このセクションには、さまざまな導入モジュールのステータスが表示されます。

[CLI を適用（CLI Apply）] セクションでは、展開トランスクリプトには、デバイスに送信されたコマンド、およびデバイスから返された応答が含まれます。これらの応答は、通知メッセージやエラーメッセージの場合があります。失敗した展開では、コマンドを含むエラーを示すメッセージを探します。これらのエラーを調べることは、FlexConfig ポリシーを使用してカスタマイズされた機能を設定している場合に特に有用になる場合があります。これらのエラーは、コマンドを設定しようとしている FlexConfig オブジェクトのスクリプトを修正するのに役立つ場合があります。

（注） 管理対象機能に送信されるコマンドと、FlexConfig ポリシーから生成されるコマンドとの間のトランスクリプトには違いはありません。

たとえば、次のシーケンスは、論理名が outside の GigabitEthernet0/0 を設定するコマンドを Firepower Management Center（FMC）が送信したことを示しています。デバイスは、自動的にセキュリティ レベルを 0 に設定したことを応答しました。FTD がセキュリティ レベルを使用することはありません。

```
========= CLI APPLY =========

FMC >> interface GigabitEthernet0/0
FMC >>  nameif outside
FTDv 192.168.0.152 >> [info] : INFO: Security level for "outside" set to 0 by default.
```

関連トピック

設定変更の展開 （447 ページ）

ヘルス メッセージの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	[ヘルス（Health）] の権限を持つ管理者/ユーザ ロール

ステップ 1 [システム ステータス（System Status）] アイコンをクリックして、メッセージ センターを表示します。

ステップ 2 [ヘルス（Health）] タブをクリックします。

ステップ 3 次の選択肢があります。

- 現在のすべてのヘルス ステータスを表示するには、[合計（total）] をクリックします。
- 任意のステータスに関するメッセージのみを表示するには、そのステータスの値をクリックします。
- メッセージが最も最近更新された時刻を表示するには、そのメッセージの相対時間インジケータ（たとえば [3 日前（3 day(s) ago）]）の上にカーソルを置きます。

- 特定のメッセージの詳細なヘルス ステータス情報を表示するには、メッセージをクリックします。
- [ヘルス モニタリング（Health Monitoring）] ページの完全なヘルス ステータスを表示するには、タブの下部にある [ヘルス モニタ（Health Monitor）] をクリックします。

関連トピック

ヘルス モニタリングについて （349 ページ）

タスク メッセージの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	他人によって開始されたタスク：管理者/[他のユーザのタスクを確認する（View Other Users' Tasks）] 権限があるカスタム ユーザ ロール 自分が開始したタスク：任意

ステップ 1 [システム ステータス（System Status）] アイコンをクリックして、メッセージ センターを表示します。

ステップ 2 [タスク（Tasks）] タブをクリックします。

ステップ 3 次の選択肢があります。

- 現在のすべてのタスクのステータスを表示するには、[合計（total）] をクリックします。
- 任意のステータスのタスクに関するメッセージのみを表示するには、そのステータスの値をクリックします。

  （注） 停止したタスクのメッセージは、タスクのステータス メッセージの合計リストにのみ表示されます。停止したタスクではフィルタリングできません。

- メッセージが最も最近更新された時刻を表示するには、そのメッセージの相対時間インジケータ（たとえば [3 日前（3 day(s) ago）]）の上にカーソルを置きます。
- タスクに関する詳細を表示するには、メッセージ内のリンクをクリックします。
- さらにタスクのステータス メッセージが表示可能な場合は、メッセージ リストの下部にある [さらにメッセージを取得する（Fetch more messages）] をクリックして取得します。

タスク メッセージの管理

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	他人によって開始されたタスク：管理者/[他のユーザのタスクを確認する（View Other Users' Tasks）] 権限があるカスタム ユーザ ロール 自分が開始したタスク：任意

ステップ 1 [システム ステータス（System Status）] アイコンをクリックして、メッセージ センターを表示します。

ステップ 2 [タスク（Tasks）] タブをクリックします。

ステップ 3 次の選択肢があります。

- さらにタスクのステータス メッセージが表示可能な場合は、メッセージ リストの下部にある [さらにメッセージを取得する（Fetch more messages）] をクリックして取得します。
- 完了したタスク（ステータスが停止、成功、または失敗のタスク）に関する 1 つのメッセージを削除するには、メッセージの横にある削除アイコン（✖）をクリックします。
- すべての完了しているタスク（ステータスが停止、成功、または失敗のタスク）に関するメッセージをすべて削除するには、[総数（total）] でメッセージをフィルタリングして、[すべての完了タスクの削除（Remove all completed tasks）] をクリックします。
- すべての正常に完了したタスクに関するメッセージをすべて削除するには、[成功（success）] でメッセージをフィルタリングして、[すべての成功タスクの削除（Remove all successful tasks）] をクリックします。
- すべての失敗したタスクに関するメッセージをすべて削除するには、[失敗（failure）] でメッセージをフィルタリングして、[すべての失敗タスクの削除（Remove all failed tasks）] をクリックします。

通知動作の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）

（注） この設定は、すべてのポップアップ通知に影響を及ぼし、ログインセッション間で保持されます。

ステップ 1 [システム ステータス（System Status）] アイコンをクリックして、メッセージ センターを表示します。

ステップ 2 メッセージ センターの右上にある歯車アイコン（⚙）をクリックします。

ステップ 3 ポップアップ通知の表示を有効または無効にするには、[通知を表示（Show notifications）] スライダをクリックします。

ステップ 4 スライダを非表示にするには、歯車アイコン（⚙）を再度クリックします。

ステップ 5 [システム ステータス（System Status）] アイコンを再度クリックして、メッセージ センターを閉じます。

トラブルシューティング用のヘルス モニタ レポート

アプライアンスで問題が発生したときに、問題の診断に役立つように、サポートからトラブルシューティング ファイルを提供するように依頼されることがあります。システムは、特定の機能分野を対象とした情報を含むトラブルシューティング ファイルと、高度なトラブルシューティング ファイル（このファイルはサポートと連携して取得します）を生成することができます。次の表に示すオプションのいずれかを選択して、特定の機能のトラブルシューティング ファイルの内容をカスタマイズできます。

一部のオプションは報告対象のデータの点で重複していますが、トラブルシューティング ファイルには、オプションの選択に関係なく冗長コピーは含まれません。

表 *54*：選択可能なトラブルシュート オプション

オプション	報告内容
Snort Performance and Configuration	アプライアンス上の Snort に関連するデータとコンフィギュレーション設定
Hardware Performance and Logs	アプライアンス ハードウェアのパフォーマンスに関連するデータとログ
System Configuration, Policy, and Logs	アプライアンスの現在のシステム設定に関連するコンフィギュレーション設定、データ、およびログ
Detection Configuration, Policy, and Logs	アプライアンス上の検出に関連するコンフィギュレーション設定、データ、およびログ
Interface and Network Related Data	アプライアンスのインライン セットとネットワーク設定に関連するコンフィギュレーション設定、データ、およびログ

オプション	報告内容
Discovery, Awareness, VDB Data, and Logs	アプライアンス上の現在の検出設定と認識設定に関連するコンフィギュレーション設定、データ、およびログ
Upgrade Data and Logs	アプライアンスの以前のアップグレードに関連するデータとログ
All Database Data	トラブルシュート レポートに含まれるすべてのデータベース関連データ
All Log Data	アプライアンス データベースによって収集されたすべてのログ
Network Map Information	現在のネットワーク トポロジ データ

特定のシステム機能のトラブルシューティング ファイルの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Maint/Any Security Analyst

カスタマイズしたトラブルシューティング ファイルを生成およびダウンロードして、そのファイルをサポートに送信できます。

マルチドメイン展開では、子孫ドメイン内のデバイスに対するトラブルシューティング ファイルの生成およびダウンロードが可能です。

⚠

注意 低メモリ デバイス用のトラブルシューティング ファイルを生成すると、自動アプリケーション バイパス（AAB）が有効になっている場合はAABをトリガーすることができます。少なくとも、AABをトリガーするとSnortプロセスを再開すると、一時的にトラフィック検査が中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、ターゲットデバイスがトラフィックを処理する方法に応じて異なります。詳細はSnort® の再起動によるトラフィックの動作（451 ページ）を参照してください。。そのような場合、AAB のトリガーによって、デバイスが一時的に動作不能な状態になることがあります。動作不能な状態が続く場合は Cisco Technical Assistance Center（TAC）に連絡してください。展開に適したソリューションをご提案します。影響を受けやすいデバイスは、Firepower 7010、7020、および 7030、ASA5508-X、5516-X、5515-X、および 5525-X、NGIPSv などです。

ステップ 1 アプライアンス ヘルス モニタの表示（373 ページ）の手順を実行します。

ステップ 2 [トラブルシューティング ファイルの生成（Generate Troubleshooting Files）] をクリックします。

ステップ 3 [全データ（All Data）] を選択して生成可能なすべてのトラブルシューティング データを生成することも、個別のボックスをオンにすることもできます。詳細については、タスク メッセージの表示 （417 ページ）を参照してください。

ステップ 4 [OK] をクリックします。

ステップ 5 Message Center でタスクのメッセージを表示します。タスク メッセージの表示 （417 ページ）を参照してください。

ステップ 6 生成されたトラブルシューティング ファイルに対応するタスクを探します。

ステップ 7 アプライアンスがトラブルシューティング ファイルを生成して、タスク ステータスが [完了（Completed）] に変わったら、[クリックして生成されたファイルを取得（Click to retrieve generated files）] をクリックします。

ステップ 8 ブラウザのプロンプトに従ってファイルをダウンロードします。(トラブルシューティング ファイルは、1 つの `.tar.gz` ファイルでダウンロードされます)。

ステップ 9 サポートの指示に従って、トラブルシューティング ファイルを Cisco に送信してください。

高度なトラブルシューティング ファイルのダウンロード

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Maint/Any Security Analyst

マルチドメイン展開では、子孫ドメイン内のデバイスに対するトラブルシューティング ファイルの生成およびダウンロードが可能です。グローバル ドメインの場合のみ、Firepower Management Center からファイルをダウンロードできます。

ステップ 1 アプライアンスのヘルス モニタを表示します（アプライアンス ヘルス モニタの表示 （373 ページ）を参照）。

ステップ 2 [高度なトラブルシューティング（Advanced Troubleshooting）] をクリックします。

ステップ 3 [ファイルのダウンロード（File Download）] タブで、サポートから提供されたファイル名を入力します。

ステップ 4 [ダウンロード（Download）] をクリックします。

ステップ 5 ブラウザのプロンプトに従ってファイルをダウンロードします。

（注） 管理対象デバイスでは、システムはファイル名の前にデバイス名を付加してファイル名を変更します。

ステップ 6 サポートの指示に従って、トラブルシューティング ファイルを Cisco に送信してください。

一般的なトラブルシューティング

システムでのディスグレイフル以外のシャットダウンまたは再起動は、内部電源障害（ハードウェア障害、電源サージなど）や外部電源の障害（コードが外れている）によって発生します。これらによって最終的にデータが破損することがあります。

接続ベースのトラブルシューティング

接続ベースのトラブルシューティングまたはデバッグにおいて、モジュール間で一貫したデバッグが提供され、特定の接続について適切なログを収集します。また、レベルベースのデバッグを最大 7 レベルまでサポートし、LINA ログと Snort ログで一貫したログ収集メカニズムを使用できます。接続ベースのデバッグでは、次の機能がサポートされています。

- Firepower Threat Defense の問題をトラブルシューティングする一般的な接続ベースのデバッグ サブシステム。
- モジュール間のデバッグ メッセージで均一的な形式。
- リブート後の永続的なデバッグ メッセージ。
- 接続に基づくモジュール間のエンドツーエンドのデバッグ。

（注） 接続ベースのデバッグは、Firepower 2100 シリーズ デバイスではサポートされていません。

接続のトラブルシューティングの詳細については、接続のトラブルシューティング （422 ページ）を参照してください。

接続のトラブルシューティング

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）

ステップ 1 **debug packet condition** コマンドを使用して接続を識別するためのフィルタを設定します。

例：

```
Debug packet condition match tcp 192.168.100.177 255.255.255.255 192.168.102.177
255.255.255.255
```

ステップ 2 対象モジュールおよび対応するレベルのデバッグを有効にします。**debug packet** コマンドを使用します。

例：

```
Debug packet acl 5
```

ステップ 3 次のコマンドを使用してデバッグを開始します。

```
debug packet start
```

ステップ 4 データベースからデバッグ メッセージを取得し、次のコマンドを使用してデバッグ メッセージを分析します。

```
show packet debugs
```

ステップ 5 パケットのデバッグを停止します。

```
debug packet stop
```

FirepowerThreatDefenseデバイスの高度なトラブルシューティング

Firepower Threat Defense デバイスでは、パケット トレーサ機能とパケット キャプチャ機能を使って詳細なトラブルシューティング分析が可能です。パケット トレーサを使うと、ファイアウォール管理者はセキュリティ アプライアンスに仮想パケットを注入し、入力から出力までのフローを追跡できます。このとき、パケットはフローおよびルーティング ルックアップ、ACL、プロトコル インスペクション、NAT、侵入検知に照らして評価されます。このユーティリティの有用性は、プロトコルおよびポート情報を含め、送信元と宛先アドレスを指定することで、実際のトラフィックをシミュレートできるところにあります。パケット キャプチャにはトレース オプションがあり、このオプションを使用すれば、パケットがドロップされたか成功したかの判断を知ることができます。

トラブルシューティング ファイルの詳細については、次を参照してください。高度なトラブルシューティング ファイルのダウンロード （421 ページ）

Web インターフェイスからの FTD CLI の使用

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	FTD	いずれか（Any）	Admin/Maint/Any Security Analyst

Firepower Management Center Web インターフェイスから、選択した FTD コマンドライン インターフェイス（CLI）コマンドを実行できます。これらのコマンドは、`ping`、`traceroute`、`show`（`show` サブコマンドの `history` と `banner` を除く）です。

マルチドメイン環境では、子孫ドメインの管理対象デバイスの Firepower Management Center Web インターフェイスを使用して、FTD CLI コマンドを入力できます。

（注） Firepower Management Center ハイ アベイラビリティを使用した展開では、この機能はアクティブ Firepower Management Center でのみ使用できます。

FTD CLI の詳細については、*Firepower Threat Defense* のコマンド リファレンス [英語] を参照してください。

ステップ 1 アプライアンスのヘルス モニタを表示します（アプライアンス ヘルス モニタの表示 （373 ページ）を参照）。

ステップ 2 [高度なトラブルシューティング（Advanced Troubleshooting）] をクリックします。

ステップ 3 [脅威防御 CLI（Threat Defense CLI）] タブをクリックします。

ステップ 4 [コマンド（Command）] ドロップダウン リストで、コマンドを選択します。

ステップ 5 オプションで、[パラメータ（Parameters）] テキスト ボックスにコマンド パラメータを入力します。

ステップ 6 [実行（Execute）] をクリックして、コマンド出力を表示します。

パケット トレーサの概要

パケット トレーサを使用して、送信元と宛先のアドレスおよびプロトコルの特性に基づいてパケットをモデル化することによってポリシー設定をテストできます。トレースでは、ポリシー ルックアップを実行してアクセス ルール、NAT、ルーティング、アクセス ポリシー、レート制限ポリシーをテストし、パケットを許可するか拒否するかを確認します。パケット フローは、インターフェイス、送信元アドレス、宛先アドレス、ポート、プロトコルに基づいてシミュレートされます。このようにパケットをテストすることによって、ポリシーの結果を確認し、必要に応じて、許可または拒否するトラフィックのタイプが処理されるかどうかをテストできます。設定の確認に加えて、トレーサを使用して許可すべきパケットが拒否されるなどの予期せぬ動作をデバッグできます。パケットを完全にシミュレートするために、パケット トレーサはデータ パス（低速パス モジュールと高速パス モジュール）をトレースします。処理は、セッション単位またはパケット単位に基づいてトランザクションとして行われます。次世代ファイアウォール（NGFW）がセッション単位またはパケット単位でパケットを処理する際は、パケットのトレースとトレースによるキャプチャにより、パケット単位でトレース データがログに記録されます。

パケット トレーサの使用

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	適用対象外	Firepower Threat Defense	任意（Any）	Admin/Maint

ステップ 1 Firepower Management Center で、**[Devices]** > **[Device Management]** を選択します。

ステップ 2 デバイスを選択します。

ステップ 3 トラブルシューティング アイコンをクリックします。
[ヘルス モニタ（Health Monitor）] ページが表示されます。

ステップ 4 [高度なトラブルシューティング（Advanced Troubleshooting）] をクリックします。

ステップ 5 [パケット トレーサ（Packet Tracer）] タブをクリックします。

ステップ 6 トレースの [パケット タイプ（Packet type）] を選択し、以下のプロトコル特性を指定します。

- [ICMP]：ICMP タイプ、ICMP コード（0 ～ 255）、およびオプションで ICMP 識別子を入力します。
- [TCP/UDP/SCTP]：送信元および宛先のポート番号を入力します。
- [IP]：プロトコル番号（0 ～ 255）を入力します。

ステップ 7 パケット トレースの入力 [インターフェイス（Interface）] を選択します。

ステップ 8 パケット トレースの [送信元（Source）] タイプを選択し、送信元 IP アドレスを入力します。

送信元と宛先のタイプとして、IPv4、IPv6、完全修飾ドメイン名（FQDN）を選択できます。Cisco TrustSec を使用する場合、IPv4 または IPv6 アドレスと FQDN を指定できます。

ステップ 9 パケット トレースの [送信元ポート（Source Port）] を選択します。

ステップ 10 パケット トレースの [宛先（Destination）] タイプを選択し、宛先 IP アドレスを入力します。

ステップ 11 パケット トレースの [宛先ポート（Destination Port）] を選択します。

ステップ 12 オプションで、セキュリティ グループ タグ（SGT）値がレイヤ 2 CMD ヘッダー（TrustSec）に組み込まれているパケットをトレースする場合、有効な [SGT 番号（SGT number）] を入力します。

ステップ 13 パケットトレーサで親インターフェイスに入力する（後でサブインターフェイスにリダイレクトされる）場合は、[VLAN ID] を入力します。

インターフェイス タイプはすべてサブインターフェイスで設定するため、これはサブインターフェイスを使用しない場合だけのオプションです。

ステップ 14 パケット トレースの [宛先 MAC アドレス（Destination MAC Address）] を指定します。

Firepower Threat Defense デバイスをトランスペアレント ファイアウォール モードで実行していて、入力インターフェイスが VTEP であるとき、[VLAN ID] に値を入力する場合は、[宛先 MAC アドレス（Destination MAC Address）] は必須になります。一方、インターフェイスがブリッジ グループのメンバーであるとき、[VLAN ID] に値を入力する場合は [宛先 MAC アドレス（Destination MAC Address）] はオプションですが、[VLAN ID] に値を入力しない場合は必須になります。

Firepower Threat Defense をルーテッド ファイアウォール モードで実行しているときに、入力インターフェイスがブリッジ グループのメンバーである場合、[VLAN ID] と [宛先 MAC アドレス（Destination MAC Address）] はオプションになります。

ステップ 15 パケット ログの [出力形式（Output Format）] を選択します。

ステップ 16 [Start] をクリックします。

パケット キャプチャの概要

トレース オプションを有効にしたパケット キャプチャ機能では、入力インターフェイスでキャプチャされた実際のパケットをシステム内でトレースできます。トレース情報は後で表示されます。キャプチャしたパケットは、実際のデータ パス トラフィックであるため、出力インターフェイスでドロップされません。Firepower Threat Defense デバイスのパケット キャプチャは、データ パケットのトラブルシューティングおよび分析をサポートします。

パケットをキャプチャすると、Snort がパケットで有効になっているトレース フラグを検出します。Snort は、パケットが通過するトレーサ エレメントを書き込みます。パケット キャプチャの結果、Snort は [ドロップ（DROP）]/[許可（ALLOW）]/[条件付きドロップ（Would DROP）] のいずれかの判定結果を出します。

パケット キャプチャ機能を使用すると、システム メモリに保存されているパケットをキャプチャしてダウンロードできます。ただし、メモリの制約により、バッファ サイズは 32 MB に制限されます。大量のパケット キャプチャを処理できるシステムはすぐに最大バッファ サイズを超過するため、パケット キャプチャの制限を増やす必要があります。これを行うには、セカンダリ メモリを使用します（ファイルを作成してキャプチャ データを書き込む）。サポートされている最大ファイル サイズは 10 GB です。

ファイル サイズを設定すると、キャプチャされたデータがファイルに保存され、キャプチャ名 **capture_name.pcap** に基づいてファイル名が割り当てられます。

ファイル サイズ オプションは、32 MB 以上のサイズ制限のパケットをキャプチャする必要がある場合に使用されます。

詳細については、Firepower Threat Defense のコマンド リファレンス [英語] を参照してください。

キャプチャ トレースの使用

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	適用対象外	Firepower Threat Defense	任意（Any）	Admin/Maint

パケット キャプチャ データには、パケットの処理中にシステムが行う決定とアクションに関する Snort とプリプロセッサからの情報が含まれています。一度に複数のパケット キャプチャを実行できます。キャプチャの変更、削除、クリア、保存を実行するようにシステムを設定できます。

（注） パケット データのキャプチャには、パケットのコピーが必要です。この操作によって、パケットの処理中に遅延が生じる可能性があります。また、パケットのスループットが低下する可能性もあります。シスコでは、特定のデータ トラフィックをキャプチャするためにパケット フィルタを使用することをお勧めします。

pcap または *ASCII* ファイル形式で保存されたトラフィック データをダウンロードできます。

ステップ 1 Firepower Management Center で、**[Devices]** > **[Device Management]** を選択します。

ステップ 2 デバイスを選択します。

ステップ 3 トラブルシューティング アイコンをクリックします。
[ヘルス モニタ（Health Monitor）] ページが表示されます。

ステップ 4 [高度なトラブルシューティング（Advanced Troubleshooting）] をクリックします。

ステップ 5 [w/トレースのキャプチャ（Capture w/Trace）] タブを選択します。

ステップ 6 **[キャプチャの追加（Add Capture）]** をクリックします。

ステップ 7 トレースのキャプチャの [名前（Name）] を入力します。

ステップ 8 トレースのキャプチャの [インターフェイス（Interface）] を選択します。

ステップ 9 以下の [一致基準（Match Criteria）] の詳細を指定します。

a) [プロトコル（Protocol）] を選択します。
b) [送信元ホスト（Source Host）] の IP アドレスを入力します。
c) [宛先ホスト（Destination Host）] の IP アドレスを入力します。
d) （オプション）[SGT 番号（SGT number）] チェックボックスをオンにし、セキュリティ グループ タグ（SGT）を入力します。

ステップ 10 以下の [バッファ（Buffer）] の詳細を指定します。

a) （オプション）最大 [パケット サイズ（Packet Size）] を入力します。
b) （オプション）最小 [バッファ サイズ（Buffer Size）] を入力します。
c) 中断せずにトラフィックをキャプチャしたい場合は、[連続キャプチャ（Continuous Capture）] を選択し、最大バッファ サイズに到達したらキャプチャを停止したい場合は、[いっぱいになったら停止（Stop when full）] を選択します。
d) 各パケットの詳細をキャプチャする場合は、[トレース（Trace）] を選択します。
e) （オプション）[トレース カウント（Trace Count）] チェックボックスをオンにします。デフォルト値は 50 です。1 ～ 1000 の範囲で値を入力できます。

ステップ 11 **[保存（Save）]** をクリックします。

機能固有のトラブルシューティング

機能固有のトラブルシューティングのヒントやテクニックについては、次の表を参照してください。

表 *55*：機能固有のトラブルシューティング トピック

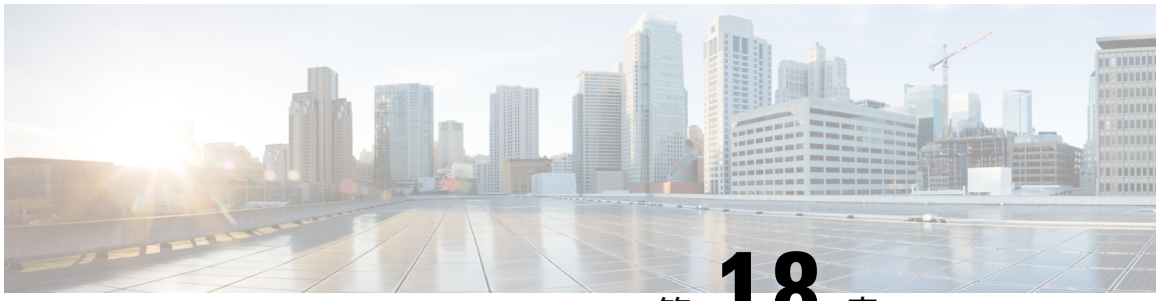
機能	関連するトラブルシューティング情報
LDAP 外部認証	LDAP 認証接続のトラブルシューティング （88 ページ）

機能	関連するトラブルシューティング情報
7000 および 8000 シリーズ デバイスのハイ アベイラビリティ状態共有	トラブルシューティングのためのデバイスのハイ アベイラビリティの状態共有統計情報 （694 ページ）
ユーザ ルール条件	ユーザ制御のトラブルシューティング （494 ページ）
ユーザ アイデンティティ ソース	ユーザ エージェント アイデンティティ ソースのトラブルシューティング （2634 ページ） ISE/ISE-PIC アイデンティティ ソースのトラブルシューティング （2604 ページ） TS エージェント アイデンティティ ソースのトラブルシューティング （2631 ページ） キャプティブ ポータルのアイデンティティ ソースのトラブルシューティング （2620 ページ） リモート アクセス VPN アイデンティティ ソースのトラブルシューティング （2626 ページ）
URL フィルタリング	URL フィルタリングのトラブルシューティング （1730 ページ）
レルムとユーザ データのダウンロード	レルムとユーザのダウンロードのトラブルシュート （2586 ページ）
ネットワーク検出	ネットワーク検出戦略のトラブルシューティング （2673 ページ）
カスタム セキュリティ グループ タグ（SGT）のルール条件	カスタム SGT 条件のトラブルシューティング （498 ページ）
SSL ルール	TLS/SSL ルールのトラブルシューティング （1897 ページ）
Cisco Threat Intelligence Director（TID）	Cisco Threat Intelligence Director（TID） のトラブルシューティング （2019 ページ）
Firepower Threat Defense syslog	Syslog の設定概要 （1385 ページ）
侵入パフォーマンス統計	侵入パフォーマンス統計情報のロギング設定 （2283 ページ）
7000 および 8000 シリーズ NGIPSv 次を搭載した ASA FirePOWER Services	generate-troubleshoot （3351 ページ） （コマンドライン インターフェイス（CLI）のコマンド）
Cisco Security Packet Analyzer との統合	Packet Analyzer クエリのトラブルシューティング （2889 ページ）

機能	関連するトラブルシューティング情報
接続ベースのトラブルシューティング	接続ベースのトラブルシューティング （422 ページ）

第 IV 部

導入管理



第 18 章

ドメイン管理

次のトピックでは、ドメインを使用してマルチテナンシーを管理する方法について説明します。

ドメインを使用したマルチテナンシーの概要

Firepowerシステムでは、ドメインを使用したマルチテナンシーを実装できます。ドメインは、管理対象デバイス、構成、およびイベントへのユーザアクセスをセグメント化します。最上位のグローバルドメインの下に、2つまたは3つのレベルで最大50のサブドメインを作成できます。

Firepower Management Centerにログインすると、現在のドメインと呼ばれる単一ドメインにログインします。ユーザアカウントによっては、他のドメインに切り替えることができる場合があります。

ユーザ ロールによる制限に加えて、現在のドメイン レベルによってさまざまなFirepowerシステム設定の変更が制限される場合もあります。システム ソフトウェア アップデートなどのほとんどの管理タスクは、グローバル ドメインに制限されます。

その他のタスクは、サブドメインがないドメインであるリーフ ドメインに制限されます。たとえば、各管理対象デバイスをリーフ ドメインと関連付け、そのリーフ ドメインのコンテキストからデバイス管理タスクを実行する必要があります。

ヒント このガイドの各タスク トピックには、タスクを実行できるドメイン レベルを示す**サポートされるドメイン数**という値があります。

各リーフ ドメインは、そのリーフ ドメインのデバイスで集められた検出データに基づいて独自のネットワーク マップを作成します。管理対象デバイスによって報告されたイベント（接続、侵入、マルウェアなど）もデバイスのリーフ ドメインに関連付けられます。

1 ドメイン レベル：グローバル

マルチテナンシーを設定しない場合、すべてのデバイス、構成、およびイベントはグローバル ドメインに属します。グローバル ドメインは、このシナリオの場合はリーフ ドメインでもあります。ドメイン管理を除き、サブドメインを追加するまでは、ドメイン固有の構成および分析オプションは非表示になります。

2 ドメイン レベル：グローバル、セカンドレベル

2 レベルのマルチドメイン展開では、グローバル ドメインには直接の子孫ドメインのみがあります。たとえば、マネージドセキュリティ サービスプロバイダー（MSSP）は、1 つの Firepower Management Center を使用して複数の顧客のネットワーク セキュリティを管理できます。

- MSSP の管理者は、グローバル ドメインにログインして、すべての顧客の展開を管理できます。
- 各顧客の管理者は、サブドメインと呼ばれるセカンドレベルにログインして、その組織に適用されるデバイス、構成、およびイベントのみを管理できます。これらのローカル管理者は、MSSP の他の顧客の展開を表示したり、その環境に影響を与えることはできません。

3 ドメイン レベル：グローバル、セカンドレベル、サードレベル

3 レベルのマルチドメイン展開では、グローバル ドメインにはサブドメインがあり、そのうち少なくとも 1 つに独自のサブドメインがあります。前の例を拡張するには、MSSP 顧客（すでにサブドメインに制限されている）がその展開をさらにセグメント化しようとしているシナリオを考えてみます。この顧客は、2 つのクラスのデバイス（ネットワーク エッジに配置されているデバイスと内部に配置されているデバイス）を個別に管理しようとしています。

- 顧客の管理者はセカンドレベルのサブドメインにログインして、顧客の展開全体を管理できます。
- 顧客のエッジ ネットワークの管理者は、サードレベル（リーフ）ドメインにログインして、ネットワーク エッジに展開されているデバイスに適用されるデバイス、構成、およびイベントのみを管理できます。同様に、顧客の内部ネットワークの管理者は、別のサードレベル ドメインにログインして、内部のデバイス、構成、およびイベントを管理できます。エッジと内部の管理者は、互いの展開を表示できません。

ドメインの用語

このマニュアルでは、ドメインおよびマルチドメイン展開を説明する際に次の用語を使用します。

グローバル ドメイン

マルチドメイン展開でのトップレベル ドメイン。マルチテナンシーを設定しない場合、すべてのデバイス、設定、およびイベントはグローバル ドメインに属します。グローバル ドメインの Administrators は、Firepower システム全体の導入を管理できます。

サブドメイン

第 2 または第 3 レベルのドメイン。

第 2 レベル ドメイン

グローバル ドメインの子。第 2 レベル ドメインは、リーフ ドメインにするか、サブドメインを持つことができます。

第 3 レベル ドメイン

第 2 レベル ドメインの子。第 3 レベル ドメインは常にリーフ ドメインです。

リーフ ドメイン

サブドメインを持たないドメイン。各デバイスはリーフ ドメインに属している必要があります。

子孫ドメイン

階層の現在のドメインから下のドメイン。

子ドメイン

ドメインの直接子孫。

先祖ドメイン

現在のドメインより上にある同じ系統のドメイン。

親ドメイン

ドメインの直接先祖。

兄弟ドメイン

同じ親を持つドメイン。

現在のドメイン

現在ログインしているドメイン。システムでは、Webインターフェイスの右上のユーザ名の前に現在のドメイン名が表示されます。ユーザ ロールが制限されている場合を除き、現在のドメインの設定を編集できます。

ドメインのプロパティ

ドメインのプロパティを変更するには、そのドメインの親ドメインの Administrator アクセス権が必要です。

名前と説明

各ドメインには、階層内で一意の名前が必要です。説明は任意です。

[Parent Domain]

第2および第3レベルのドメインには親ドメインがあります。ドメインを作成した後にドメインの親を変更することはできません。

デバイス

リーフ ドメインにのみデバイスを含めることができます。つまり、1つのドメインにはサブドメインまたはデバイスを含めることができますが、両方を含めることはできません。非リーフ ドメインが直接デバイスを制御している展開を保存することはできません。

ドメイン エディタで、ドメイン階層の現在の場所に応じて、Web インターフェイスに使用可能な選択されたデバイスが表示されます。

ホスト制限（Host Limit）

Firepower Management Center がモニタでき、ネットワーク マップに保存できるホストの数。モデルによって異なります。マルチドメイン展開では、リーフ ドメインは使用可能なモニタされたホストのプールを共有しますが、個別のネットワーク マップを持っています。

各リーフ ドメインがネットワーク マップに値を入力できるように、ホスト制限を各サブドメイン レベルで設定できます。ドメインのホスト制限を **0** に設定すると、ドメインは一般的なプールで共有します。

ホスト制限を設定すると、各ドメイン レベルで異なる効果があります。

- リーフ：リーフ ドメインの場合、ホスト制限は単に、リーフ ドメインがモニタできるホスト数の制限です。
- 第2レベル：第3レベルのリーフ ドメインを管理する第2レベルのドメインの場合、ホスト制限は、リーフ ドメインがモニタできるホストの総数を表します。リーフ ドメインは、使用可能なホストのプールを共有します。
- グローバル：グローバル ドメインの場合、ホスト制限は、Firepower Management Center がモニタできるホストの総数に等しくなります。変更することはできません。

サブドメインのホスト制限の合計を、親ドメインのホスト制限より多くすることができます。たとえば、グローバル ドメインのホスト制限が 150,000 の場合、複数のサブドメインを設定して、それぞれのホスト制限を 100,000 にすることができます。これらのドメインのいずれか（すべてではない）が 100,000 のホストをモニタできます。

ホスト制限に到達した後に新しいホストを検出すると、ネットワーク検出ポリシーが制御を行います。新しいホストをドロップするか、または長期間非アクティブになっているホストを置換することができます。各リーフ ドメインには独自のネットワーク検出ポリシーがあるため、各リーフ ドメインは、システムが新しいホストを検出すると、独自の動作を制御します。

ドメインのホスト制限を軽減した場合に、そのネットワークマップに新しい制限より多くのホストが含まれている場合、システムは最も長い間非アクティブになっているホストを削除します。

関連トピック

Firepower システムのホスト制限 （2490 ページ）
ネットワーク検出のデータ ストレージ設定 （2669 ページ）

ドメインの管理

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin

ドメインのプロパティを変更するには、そのドメインの親ドメインへの管理者アクセス権が必要です。

ステップ 1 **[System]** > **[Domains]**を選択します。

ステップ 2 次のようにドメインを管理します。

- 追加：[ドメインの追加（Add Domain）] をクリックするか、または親ドメインの横にある [サブドメインの追加（Add Subdomain）] アイコンをクリックします（新しいドメインの作成 （438 ページ） を参照）。
- 編集：変更するドメインの横にある編集アイコン（  ）をクリックします（ドメインのプロパティ （435 ページ） を参照）。
- 削除：削除する空のドメインの横にある削除アイコン（  ）をクリックして、選択内容を確認します。宛先ドメインを編集することによって、削除するドメインからデバイスを移動します。

ステップ 3 ドメイン構造への変更を行い、すべてのデバイスをリーフ ドメインに関連付けたら、[保存（Save）] をクリックして変更を実行します。

ステップ 4 プロンプトが表示されたら、追加の変更を行います。

- リーフ ドメインを親ドメインに変更した場合は、古いネットワーク マップを移動または削除します（ドメイン間のデータの移動 （439 ページ） を参照）。
- ドメイン間でデバイスを移動し、新しいポリシーおよびセキュリティ ゾーンまたはインターフェイス グループを割り当てる必要がある場合は、ドメイン間のデバイスの移動 （440 ページ） を参照してください。

次のタスク

- 新しいドメインのユーザロールとポリシー（アクセス制御、ネットワーク検出など）を設定します。必要に応じてデバイスのプロパティを更新します。
- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

新しいドメインの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	グローバルおよびセカンドレベル	Admin

最上位のグローバルドメインの下に、2つまたは3つのレベルで最大50のサブドメインを作成できます。

ドメイン設定を実装する前に、リーフ ドメインにすべてのデバイスを割り当てる必要があります。リーフ ドメインにサブドメインを追加すると、ドメインはリーフ ドメインではなくなるので、デバイスを再度割り当てる必要があります。

ステップ 1 グローバルまたはセカンドレベル ドメインで、**[System]** > **[Domains]** を選択します。

ステップ 2 [ドメインの追加（Add Domain）] をクリックするか、または親ドメインの横にある [サブドメインの追加（Add Subdomain）] アイコンをクリックします。

ステップ 3 [Name] と [Description] を入力します。

ステップ 4 [親ドメイン（Parent Domain）] を選択します。

ステップ 5 [デバイス（Devices）] タブで、ドメインに追加する [使用可能なデバイス（Available Devices）] を選択し、[ドメインに追加（Add to Domain）] をクリックするか、または [選択されたデバイス（Selected Devices）] のリストにドラッグ アンド ドロップします。

ステップ 6 必要に応じて、[詳細設定（Advanced）] タブをクリックして、新しいドメインがモニタできるホスト数を制限します（ドメインのプロパティ （435 ページ） を参照）。

ステップ 7 [保存（Save）] をクリックして、ドメイン管理ページに戻ります。
デバイスが非リーフ ドメインに割り当てられている場合は、システムによって警告が表示されます。これらのデバイスに新しいドメインを作成するには、[新しいドメインの作成（Create New Domain）] をクリックします。デバイスを既存のドメインに移動する予定がある場合は、[未割り当てのままにする（Keep Unassigned）] をクリックします。

ステップ 8 ドメイン構造への変更を行い、すべてのデバイスをリーフ ドメインに関連付けたら、[保存（Save）] をクリックして変更を実行します。

ステップ 9 プロンプトが表示されたら、追加の変更を行います。

- リーフ ドメインを親ドメインに変更した場合は、古いネットワーク マップを移動または削除します（ドメイン間のデータの移動 （439 ページ） を参照）。
- ドメイン間でデバイスを移動し、新しいポリシーおよびセキュリティ ゾーンまたはインターフェイス グループを割り当てる必要がある場合は、ドメイン間のデバイスの移動 （440 ページ） を参照してください。

次のタスク

- 新しいドメインのユーザ ロールとポリシー（アクセス制御、ネットワーク検出など）を設定します。必要に応じてデバイスのプロパティを更新します。
- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

ドメイン間のデータの移動

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin

イベントおよびネットワーク マップがリーフ ドメインに関連付けられているため、リーフ ドメインを親ドメインに変更する場合は、2 つの選択肢があります。

- ネットワーク マップおよび関連付けられているイベントを新しいリーフ ドメインに移動します。
- ネットワーク マップは削除しますが、イベントは保持します。この場合、システムが必要に応じてまたは設定されているようにイベントをプルーニングするまで、イベントは親ドメインに関連付けられたままとなります。または、古いイベントを手動で削除できます。

始める前に

以前のリーフ ドメインが現在の親ドメインになるドメイン設定を実行します（ドメインの管理 （437 ページ） を参照）。

ステップ 1 現在は親ドメインである以前の各リーフ ドメインに対して、次の手順を実行します。

- **親ドメイン**のイベントおよびネットワーク マップを継承するには、新しい**リーフ ドメイン**を選択します。
- 親ドメインのネットワーク マップを削除するが、古いイベントは保持する場合は、[なし（None）] を選択します。

ステップ 2 **[保存（Save）]** をクリックします。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

ドメイン間のデバイスの移動

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	グローバルおよびセカンドレベル	Admin

ドメイン間でデバイスを移動すると、デバイスに適用された設定とポリシーに影響する可能性があります。システムは実行できる内容を自動的に保持および更新し、実行できない内容を削除します。

リモート アクセス VPN のポリシーをデバイスに割り当てるときには、ターゲット ドメインがリモート アクセス VPN を設定しているドメインの子である場合にのみ、デバイスをあるドメインから別のドメインに移動できます。

デバイスは、デバイス上の登録済み証明書を削除することなく子ドメインに移動できます。

具体的には次のとおりです。

- 移動したデバイスに割り当てられた正常性ポリシーが新しいドメインでアクセス不能の場合、新しい正常性ポリシーを選択できます。
- 移動したデバイスに割り当てられたアクセス コントロール ポリシーが有効でない場合、または新しいドメインでアクセスできない場合は、新しいポリシーを選択します。すべてのデバイスに、割り当てられたアクセス コントロール ポリシーが必要です。
- 移動したデバイス上のインターフェイスが、新しいドメインでアクセスできないセキュリティ ゾーンに属している場合は、新しいゾーンを選択できます。
- インターフェイスは、以下から削除されます。
  - 新しいドメインでアクセス不能で、アクセス コントロール ポリシーで使用されていないセキュリティ ゾーン。
  - すべてのインターフェイス グループ。

デバイスでポリシーの更新が必要だが、ゾーン間でインターフェイスを移動する必要がない場合は、ゾーン設定が最新であることを示すメッセージが表示されます。たとえば、デバイスのインターフェイスが共通の先祖ドメインに設定されているセキュリティ ゾーンに属している場

合は、サブドメインからサブドメインにデバイスを移動する場合はゾーン設定を更新する必要はありません。

始める前に

- デバイスをドメインからドメインに移動し、次に新しいポリシーとセキュリティゾーンを割り当てる必要があるドメイン構成を実装します（ドメインの管理 （437 ページ） を参照）。

ステップ 1 [デバイスの移動（Move Devices）] ダイアログボックスの [設定するデバイスの選択（Select Device(s) to Configure）] の下で、設定するデバイスをオンにします。

同じ正常性ポリシーとアクセス コントロール ポリシーを割り当てるには、複数のデバイスをオンにします。

ステップ 2 デバイスに適用する [アクセス コントロール ポリシー（Access Control Policy）] を選択するか、または新しいポリシーを作成するには [新しいポリシー（New Policy）] を選択します。

ステップ 3 デバイスに適用する [正常性ポリシー（Health Policy）] を選択するか、またはデバイスに正常性ポリシーを適用しないままにするには [なし（None）] を選択します。

ステップ 4 インターフェイスを新しいゾーンに割り当てるようにプロンプトが表示された場合は、リストされている各インターフェイスに [新しいセキュリティ ゾーン（New Security Zone）] を選択するか、または後で割り当てるには [なし（None）] を選択します。

ステップ 5 すべての影響を受けるデバイスを設定した後、[保存（Save）] をクリックしてポリシーとゾーンの割り当てを保存します。

ステップ 6 [保存（Save）] をクリックして、ドメイン構成を実装します。

次のタスク

- 移動の影響を受けた移動済みデバイスでその他の設定を更新します。
- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

第 19 章

ポリシー管理

ここでは、Firepower Management Center でさまざまなポリシーを管理する方法について説明します。

ポリシーの導入

導入を設定した後、およびその設定を変更したときは、影響を受けるデバイスにその変更を導入する必要があります。導入のステータスは、メッセージ センターで確認できます。

導入を行うと、以下のコンポーネントが更新されます。

- デバイスとインターフェイスの設定
- デバイス関連ポリシー：NAT、VPN、QoS、プラットフォーム設定
- アクセス コントロールおよび関連するポリシー：DNS、ファイル、アイデンティティ、侵入、ネットワーク分析、プレフィルタ、SSL
- ネットワーク検出ポリシー
- 侵入ルールの更新
- これらの要素のいずれかに関連付けられている設定とオブジェクト

システムにポリシーを自動的に導入させるには、導入タスクをスケジュールするか、あるいは侵入ルールの更新をインポートする際に導入するようにシステムを設定します。特に、侵入ポリシーの更新によって侵入およびネットワーク分析に関するシステム定義の基本ポリシーを変更できるようにしている場合は、ポリシーの導入を自動化すると役立ちます。侵入ルール更新によって、アクセス コントロール ポリシーの前処理およびパフォーマンスの詳細設定オプションのデフォルト値が変更されることもあります。

マルチドメイン展開では、ユーザアカウントが属するいずれのドメインにも変更を導入できます。

- 導入先を先祖ドメインに切り替えると、変更がすべてのサブドメインに同時に導入されます。
- 導入先をリーフ ドメインに切り替えると、変更はそのドメインだけに導入されます。

設定変更の展開に関する注意事項

インラインとパッシブの展開

インライン設定をパッシブに展開されたデバイスに適用しないでください。またその逆も同様です。

展開までの時間とメモリの制限

展開までの所要時間は、次の複数の要因（これらに限定されません）によって変わります。

- デバイスに送信する設定。たとえば、ブロックするセキュリティ インテリジェンス エントリの数を大幅に増加する場合、展開時間が長くなります。
- デバイス モデルとメモリ。メモリが少ないデバイスの場合、展開時間が長くなります。たとえば、Firepower 7010、7020、7030 デバイスに展開するには、最大 5 分かかります。

デバイスの機能を超えないように注意してください。ターゲット デバイスでサポートされるルールまたはポリシーの最大数を超えると、システムが警告を表示します。最大数はいくつかの要因によって変わります。デバイスのメモリ量やプロセッサの数だけではなく、ポリシーやルールの複雑さも影響します。ポリシーとルールの最適化については、ルールのパフォーマンスに関するガイドライン （502 ページ）を参照してください。

展開時のトラフィック フローおよび検査の中断

展開する際にリソースを要求すると、いくつかのパケットがインスペクションなしでドロップされることがあります。また、一部のコンフィギュレーションを展開すると、トラフィックのインスペクションを中断するSnortプロセスが再開します。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、ターゲットデバイスがトラフィックを処理する方法に応じて異なります。Snort® の再起動によるトラフィックの動作 （451 ページ）および展開またはアクティブ化された際に Snort プロセスを再起動する設定（454 ページ）を参照してください。

Firepower Threat Defense デバイスの場合、[Deploy] ダイアログの [Inspect Interruption] 列に、展開するとトラフィック フローまたは検査が中断する可能性があることについての警告が表示されます。展開を続行するか、キャンセルまたは遅延できます。詳細は、「Firepower Threat Defense デバイスの再起動の警告 （445 ページ）」を参照してください。

注意 展開は、保守期間中に行うか、中断の影響が最も小さい時点で行うことを強く推奨します。

アプリケーション ディテクタの自動的な有効化

アプリケーション制御の実行時に必要なディテクタが無効になっている場合、システムは、ポリシーの展開時にシステムによって提供される適切なディテクタを自動的に有効にします。存在しない場合、システムはそのアプリケーション対応で最近変更されたユーザ定義のディテクタを有効にします。

ネットワーク検出ポリシーの変更によるアセットの再検出

ネットワーク検出ポリシーに変更を展開する場合、システムは、監視対象ネットワーク内のホストのネットワーク マップから MAC アドレス、TTL、およびホップ情報を削除してから、再検出を行います。また、影響を受ける管理対象デバイスは、まだ Firepower Management Center に送信されていない検出データを破棄します。

関連トピック

Snort® の再起動シナリオ （450 ページ）

Firepower Threat Defense デバイスの再起動の警告

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Network Admin/Security Approver

展開時、展開ダイアログの [Inspect Interruption] 列に、設定を展開したときに Firepower Threat Defense デバイスで Snort プロセスが再起動するかどうかが示されます。*Snort* プロセスと呼ばれるトラフィック インスペクション エンジンが再起動すると、プロセスが再開されるまでインスペクションが中断されます。トラフィックが中断されるか中断中にインスペクションなしで受け渡されるかどうかは、デバイスがトラフィックを処理する方法によって変わります。展開の続行、展開のキャンセル、および設定の変更を実行できます。または、展開によるネットワークへの影響が最小となる時間まで展開を遅らせることができます。

[Inspect Interruption] 列に [Yes] と表示されているときにデバイス構成のリストを展開すると、Snort プロセスを再起動する特定の設定タイプは赤色で強調表示され再起動アイコン（⛔）が付けられます。これらの設定にマウスポインタを合わせると、設定を展開したときにトラフィックが中断される可能性があるというメッセージが表示されます。

次の表に、展開ダイアログでインスペクション中断の警告が表示される方法を示します。

表 *56 :* 展開ダイアログにおけるインスペクション中断のインジケータ

タイプ	インスペクションの中断	説明
FTD	Yes	少なくとも 1 つの設定は、展開するとデバイスでインスペクションが中断します。また、デバイスがトラフィックを処理する方法によって、トラフィックが中断されることがあります。デバイス設定リストを展開して、詳細を確認できます。
	なし	展開されている設定は、デバイスのトラフィックを中断しません。
	不明	システムでは、展開された設定によってデバイスのトラフィックが中断する可能性があるかどうか判断できず、デバイスの横にデバイスの警告アイコン（  ）が表示されます。 不明の状態は、ソフトウェアアップグレード後、最初に展開するまでに表示されるか、サポート コール中に表示されます。
	エラー	内部エラーにより、システムはステータスを特定できません。 操作をキャンセルして再度 [展開（Deploy）] をクリックすると、システムは [インスペクションの中断（Inspect Interruption）] ステータスを特定しなおすことができます。それでも問題が解決しない場合は、サポートにお問い合わせください。
センサー	--	センサーとして識別されるデバイスは Firepower Threat Defense デバイスではありません。設定を展開するとこのデバイスのトラフィックが中断されるかどうかの判断は行われません。

すべてのデバイス タイプの Snort プロセスを再起動する全設定の詳細については、展開またはアクティブ化された際に Snort プロセスを再起動する設定 （454 ページ） を参照してください。

設定変更の展開

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Network Admin/Security Approver

設定を変更した後に、影響を受けるデバイスに展開します。展開は、保守期間中に行うか、トラフィック フローやインスペクションへの中断の影響が最も小さい時点で行うことを強く推奨します。

注意 展開する際にリソースを要求すると、いくつかのパケットがインスペクションなしでドロップされることがあります。また、一部のコンフィギュレーションを展開すると、トラフィックのインスペクションを中断するSnortプロセスが再開します。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、ターゲットデバイスがトラフィックを処理する方法に応じて異なります。Snort® の再起動によるトラフィックの動作 （451 ページ）および展開またはアクティブ化された際に Snort プロセスを再起動する設定（454 ページ）を参照してください。

始める前に

- 「設定変更の展開に関する注意事項（444 ページ）」で説明されているガイドラインを確認してください。
- すべての管理対象デバイスが同じバージョンのセキュリティ ゾーン オブジェクトを使用していることを確認してください。セキュリティ ゾーン オブジェクトを編集している場合：Do not deploy configuration changes to any device until you edit the zone setting for interfaces on *all* devices you want to sync. すべての管理対象デバイスに同時に展開する必要があります。（セキュリティ ゾーン オブジェクトのリビジョンの同期（661 ページ）を参照してください。）

ステップ 1 Firepower Management Center メニュー バーで、[展開（Deploy）] をクリックします。

[ポリシーの展開（Deploy Policies）] ダイアログに、設定の期限が切れているデバイスがリストされます。ダイアログの上部の [バージョン（Version）] は、最後に設定変更を行った時期を示します。

ステップ 2 設定変更を展開するデバイスを特定して選択します。

- [ソート（Sort）]：列ヘッダーをクリックすることで、デバイス リストをソートします。

Firepower Threat Defense デバイスへの展開時にトラフィック検査を中断させたりトラフィック自体を中断させる可能性のある設定を識別するために役立つ列については、Firepower Threat Defense デバイスの再起動の警告 （445 ページ）を参照してください。

すべてのデバイスへの展開時にトラフィック検査を中断させたりトラフィック自体を中断させる可能性のある設定については、展開またはアクティブ化された際に Snort プロセスを再起動する設定 （454 ページ）を参照してください。

- [展開（Expand）]：デバイス リストを展開して展開される設定変更を表示するには、プラス アイコン（⊕）をクリックします。システムは、期限切れのポリシーをインデックス（🕘）アイコンでマーキングします。

  [Inspect Interruption] 列の状態が [Yes] の場合、その展開によって Firepower Threat Defense デバイスのインスペクションとおそらくはトラフィックが中断されることを示しています。展開された一覧では、中断を発生させる構成が赤色で強調表示されます。

- [フィルタ（Filter）]：デバイス リストをフィルタリングします。列ヘッダーの右隅にある矢印をクリックします。

  - [検査中断（Inspect Interruption）] 列：[フィルタ（Filters）] ドロップダウン メニューで、目的のフィルタ オプションを確認します。複数のオプションを選択できます。

    再起動に関する警告の詳細については、Firepower Threat Defense デバイスの再起動の警告 （445 ページ）を参照してください。

  - その他のすべての列：[フィルタ（Filters）] テキスト ボックスにテキストを入力し、Enter を押します。

  [Filters] をオンまたはオフにして、フィルタをアクティブまたは非アクティブにします。

- 変更：右上隅にある歯車のアイコン（⚙）をクリックし、[Columns] ドロップダウン リストで表示する列のチェック ボックスをオンまたはオフにします。
- 調整：マウス カーソルを列ヘッダーの上に移動し、列をドラッグ アンド ドロップして希望の順序にします。

ステップ 3 [Deploy] をクリックします。

ステップ 4 展開する変更に関するエラーや警告がシステムによって識別された場合は、[Errors and Warnings for Requested Deployment] ウィンドウにその内容が表示されます。

次の選択肢があります。

- [続行（Proceed）]：警告状態を解決せずに展開を続行します。システムがエラーを確認した場合は続行できません。
- [キャンセル（Cancel）]：展開せずに終了します。エラーおよび警告状態を解決し、設定の再展開を試行します。

次のタスク

- （オプション）展開の状態をモニタします（展開メッセージの表示 （415 ページ） を参照）。
- 展開に失敗した場合には、「設定変更の展開に関する注意事項 （444 ページ）」を参照してください。

関連トピック

Snort® の再起動シナリオ （450 ページ）

デバイスへの既存の設定の再展開

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	リーフのみ	Admin/Network Admin/Security Approver

既存（変更なし）の設定を単一の管理対象デバイスに強制展開できます。メンテナンス ウィンドウで、またはトラフィック フローとインスペクションに対する中断の影響が最小限になる時間に、展開することを強くお勧めします。

注意 展開する際にリソースを要求すると、いくつかのパケットがインスペクションなしでドロップされることがあります。また、一部のコンフィギュレーションを展開すると、トラフィックのインスペクションを中断する Snort プロセスが再開します。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、ターゲットデバイスがトラフィックを処理する方法に応じて異なります。Snort® の再起動によるトラフィックの動作 （451 ページ）および展開またはアクティブ化された際に Snort プロセスを再起動する設定（454 ページ）を参照してください。

始める前に

設定変更の展開に関する注意事項（444 ページ）で説明されているガイドラインを確認してください。

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 強制導入するデバイスの横にある編集アイコン（）をクリックします。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [デバイス（Device）] タブをクリックします。

ステップ 4 [全般（General）] セクション見出しの横にある編集アイコン（）をクリックします。

ステップ 5 [強制導入（Force Deploy）] 矢印（）をクリックします。

ステップ 6 [展開（Deploy）] をクリックします。

システムでは、展開中の設定で発生したエラーや警告が識別されます。[続行（Proceed）] をクリックすると、警告状態を解決せずに続行できます。ただし、システムがエラーを示している場合は、続行できません。

次のタスク

- （オプション）展開の状態をモニタします（展開メッセージの表示 （415 ページ） を参照）。
- 展開に失敗した場合には、「設定変更の展開に関する注意事項 （444 ページ）」を参照してください。

関連トピック

Snort® の再起動シナリオ （450 ページ）

Snort® の再起動シナリオ

管理対象デバイス上の *Snort* プロセスと呼ばれるトラフィック インスペクション エンジンが再起動すると、プロセスが再開されるまでインスペクションが中断されます。 この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、ターゲット デバイスがトラフィックを処理する方法に応じて異なります。詳細はSnort® の再起動によるトラフィックの動作 （451 ページ） を参照してください。 また、Snort プロセスが再起動するかどうかに関係なく、展開時にリソース需要が高まった結果、いくつかのパケットがインスペクションを実行せずにドロップされることがあります。

次の表に示すいずれかのシナリオでは、Snort プロセスが再起動されます。

表 *57 : Snort* 再起動のシナリオ

再起動のシナリオ	詳細情報
Snort プロセスの再起動が必要な特定の設定を展開した場合。	展開またはアクティブ化された際に Snort プロセスを再起動する設定 （454 ページ）
Snort プロセスを直ちに再起動するように設定を変更した場合。	変更により Snort プロセスがただちに再起動する場合 （456 ページ）
現在展開されている自動アプリケーション バイパス（AAB）設定のトラフィックをアクティブにした場合。	自動アプリケーション バイパスの設定 （305 ページ）

関連トピック

アクセス コントロール ポリシーの詳細設定 （1681 ページ）
展開またはアクティブ化された際に Snort プロセスを再起動する設定 （454 ページ）

ポリシー適用中のトラフィックの検査

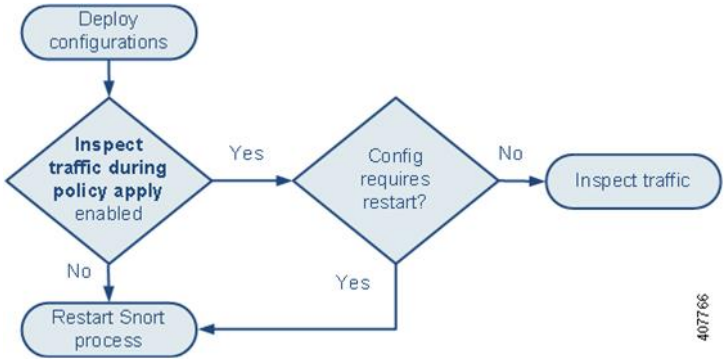
[ポリシー適用時にトラフィックを検査（Inspect traffic during policy apply）] は、管理対象デバイスが設定変更の展開時にトラフィックを検査できるようにするための詳細アクセス コントロール ポリシーの一般設定です。これは、展開する設定で Snort プロセスの再起動が不要な場合に限ります。このオプションは、次のように設定できます。

- [有効（Enabled）]：特定の設定で Snort 処理を再起動する必要な場合を除き、トラフィックは展開時に検査されます。

  展開する設定に Snort の再起動が必要でなければ、システムは現在展開されているアクセス コントロール ポリシーを使用してトラフィックを検査し、導入中に、展開しているアクセス コントロール ポリシーに切り替えます。

- [無効（Disabled）]：展開時にトラフィックは検査されません。Snort プロセスは展開時に必ず再起動されます。

次の図に、[ポリシー適用時にトラフィックを検査（Inspect traffic during policy apply）] を有効にした場合と無効にした場合の Snort の再起動の仕組みを示します。



注意 展開する際にリソースを要求すると、いくつかのパケットがインスペクションなしでドロップされることがあります。また、一部のコンフィギュレーションを展開すると、トラフィックのインスペクションを中断する Snort プロセスが再開します。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、ターゲット デバイスがトラフィックを処理する方法に応じて異なります。Snort® の再起動によるトラフィックの動作 （451 ページ）および展開またはアクティブ化された際に Snort プロセスを再起動する設定（454 ページ）を参照してください。

Snort® の再起動によるトラフィックの動作

次の表に、Snort プロセスが再起動した場合のさまざまなデバイスのトラフィックの処理方法を示します。

表 *58 : FTD* および *FTD* の仮想再起動トラフィックの影響

インターフェイス コンフィギュレーション	再起動によるトラフィックの動作
inline: **Snort Fail Open: Down**: disabled	dropped
inline：**Snort Fail Open**：**Down**：enabled	検査なしで受け渡される
preserve-connection が有効になっている場合（**configure snort preserve-connection enable**、デフォルト）はルーテッド、トランスペアレント（EtherChannel、冗長、サブインターフェイスを含む） 6.4.x FMC で管理対象となる FTD はバージョン 6.4.x、6.3.x、6.2.3、6.2.0.2、または後続の 6.2.0.x パッチを実行している必要があります。 詳細については、Cisco Firepower Threat Defense コマンド リファレンスを参照してください。	既存の TCP/UDP フロー：インスペクションなしで受け渡される 新規 TCP/UDP フローとすべての非 TCP/UDP フロー：ドロップされる **preserve-connection** が有効になっている場合でも、次のトラフィックはドロップされることに注意してください。 • システムが **Do not decrypt** SSL ルールまたはデフォルトポリシー アクションに一致するトラフィックにタグを付ける前に Snort がダウンした （いくつかのハンドシェイク パケット交換の後にタグ付けが行われます） • プレーンテキスト、パススルー プレフィルタ トンネル トラフィック（**Analyze** ルール アクションまたは**Analyze all tunnel traffic** デフォルト ポリシー アクションと一致） • 復号化された TLS/SSL トラフィック • セーフ サーチ フロー • キャプティブ ポータル フロー
次のいずれかの状況の場合はルーテッド、トランスペアレント（EtherChannel、冗長、サブインターフェイスを含む） • **preserve-connection** CLI コマンドが無効になっている（**configure snort preserve-connection disable**） • FTD バージョン（6.2.1、6.2.2、6.2.2.x、または 6.2.0.2 よりも前のバージョン）はこのコマンドをサポートしていません。	dropped

インターフェイス コンフィギュレーション	再起動によるトラフィックの動作
inline: tap mode	すぐにパケットを出力し、バイパス Snort をコピーする
passive	中断なし、インスペクションなし

表 *59 : 7000* および *8000* シリーズ、*NGIPSv* 再起動トラフィックの影響

インターフェイス コンフィギュレーション	再起動によるトラフィックの動作
inline: **Failsafe** enabled または disabled	検査なしで受け渡される [フェールセーフ（Failsafe）] が無効で、Snort がビジーでもダウンしていない場合、いくつかのパケットがドロップすることがあります。
inline: tap mode	すぐにパケットを出力し、バイパス Snort をコピーする
passive	中断なし、インスペクションなし
ルーテッド、スイッチド （7000 および 8000 シリーズのみ）	dropped

表 *60 : ASA FirePOWER Restart* トラフィックの影響

インターフェイス コンフィギュレーション	再起動によるトラフィックの動作
フェールオープン状態のルーテッドまたは透過	検査なしで受け渡される
フェールクローズ状態のルーテッドまたは透過	dropped

（注） 再起動中に Snort プロセスがダウンした場合のトラフィック処理に加え、フェールセーフ オプション（Firepower システムのインライン セット（669 ページ） を参照）または Snort フェールオープンの [ビジー（Busy）] オプション（インライン セットを設定します。（847 ページ） を参照）の設定に応じて、トラフィックをインスペクションなしで通過させたり、または Snort プロセスがビジーのときにトラフィックをドロップしたりすることもできます。デバイスは、フェールセーフ オプションまたは Snort フェールオープン オプションの両方ではなくいずれかをサポートします。

（注） 設定の導入時に Snort プロセスがビジーになったが、ダウンしなかった場合、CPU の合計負荷が 60 % を超えると一部のパケットがルーテッド、スイッチド、またはトランスペアレント インターフェイスでドロップする場合があります。

展開またはアクティブ化された際に Snort プロセスを再起動する設定

AAB以外の構成を展開すると、Snortプロセスが再起動されます。AABの展開自体には再起動が伴いませんが、パケットの遅延が大きすぎると、現在展開されている AAB 設定がアクティブになり、Snort プロセスが部分的に再起動されます。

アクセス コントロール ポリシーの詳細設定

- [ポリシー適用時にトラフィックのインスペクションを実行する（Inspect traffic during policy apply）] が無効な場合に展開します。
- SSL ポリシーを追加または削除します。

ファイル ポリシー（File Policy）

次のいずれかの構成の最初または最後を展開します。これらのファイルポリシー構成を展開しても再起動は発生しませんが、非ファイルポリシー構成を展開すると再起動が発生する可能性があることに注意してください。

- 次のいずれかの操作を行います。
  - 展開されたアクセス コントロール ポリシーに 1 つ以上のファイル ポリシーが含まれている場合は、[アーカイブを検査する（Inspect Archives）] を有効または無効にします。
  - [アーカイブを検査する（Inspect Archives）] が有効になっている場合は、最初のファイル ポリシー ルールを追加するか、または最後のファイル ポリシー ルールを削除します（[アーカイブを検査する（Inspect Archives）] が有意味であるためには 1 つ以上のルールが必要であることに注意してください）。
- [ファイルを検出（Detect Files）] または [ファイルをブロック（Block Files）] ルールで、[ストア ファイル（Store files）] を有効または無効にします。
- [マルウェア クラウドのルックアップ（Malware Cloud Lookup）] または [マルウェアをブロック（Block Malware）] ルール アクションと、分析オプション（[Spero 分析または MSEXE（Spero Analysis or MSEXE）]、[ダイナミック分析（Dynamic Analysis）] または [ローカル マルウェア分析（Local Malware Analysis）]）またはストア ファイル オプション（[マルウェア（Malware）]、[不明（Unknown）]、[クリーン（Clean）] または [カスタム（Custom）]）を組み合わせた最初のアクティブ ファイル ルールを追加するか、または最後のアクティブ ファイル ルールを削除します。

これらのファイル ポリシー構成をセキュリティ ゾーンまたはトンネル ゾーンに展開するアクセス コントロール ルールによって再起動が発生するのは、構成が次の条件を満たす場合だけであることに注意してください。

- アクセス コントロール ルールに含まれる送信元または宛先セキュリティ ゾーンは、ターゲット デバイス上のインターフェイスに関連付けられたセキュリティ ゾーンと一致する必要があります。
- アクセス コントロール ルールに含まれる宛先ゾーンが [任意（any）] でないかぎり、ルールに含まれる送信元トンネル ゾーンは、プレフィルタ ポリシーに含まれるトンネル ルールに割り当てられているトンネル ゾーンと一致する必要があります。

ID ポリシー

- SSL 復号化が無効になっている場合（つまり、アクセス コントロール ポリシーに SSL ポリシーが含まれていない場合）は、最初のアクティブ認証ルールを追加するか、または最後のルールを削除します。

  アクティブな認証ルールに [アクティブ認証（Active Authentication）] ルール アクションが含まれるか、[パッシブ/VPN アイデンティティを確立できない場合にアクティブ認証を使用（Use active authentication if passive or VPN identity cannot be established）] が選択された [パッシブ認証（Passive Authentication）] ルール アクションが含まれます。

ネットワーク ディスカバリ（Network Discovery）

- ネットワーク検出ポリシーを使用して、HTTP、FTP、または MDNS プロトコル経由で権限のないトラフィックベースのユーザ検出を有効または無効にします。

Device Management

- ルーティング：7000 または 8000 シリーズ デバイスにルーテッド インターフェイス ペアまたは仮想ルータを追加します。
- VPN：7000 または 8000 シリーズ デバイスで VPN を追加または削除します。

  ⚠

  注意 システムは、7000 または 8000 シリーズ デバイスの VPN を追加または削除したときに Snort プロセスが再起動することを警告しません。

- MTU：デバイス上のすべての非管理インターフェイスの中で最大の MTU 値を変更します。
- 7000/8000 シリーズのハイアベイラビリティ：ハイアベイラビリティ状態共有オプションを変更します。 システムは、Snort プロセスがプライマリ デバイスとセカンダリ デバイスで再起動することを警告しません。

- Automatic Application Bypass（AAB）： The currently deployed AAB configuration activates when a malfunction of the Snort process or a device misconfiguration causes a single packet to use an excessive amount of processing time. その結果、Snort プロセスが部分的に再起動され、非常に大きい遅延が緩和されるか、または完全なトラフィックの停止が防止されます。この部分的な再起動により、デバイスがトラフィックをどのように処理するかに応じて、いくつかのパケットがインスペクションなしで通過するか、またはドロップされます。

Updates

- System update: Deploy configurations the first time after a software update that includes a new version of the Snort binary or data acquisition library（DAQ).
- VDB: Deploy configurations the first time after installing a vulnerability database（VDB）update that includes changes applicable to managed devices. そのため、インストールを開始するために Firepower Management Center を選択すると、警告メッセージが表示されます。展開ダイアログは、VDB 変更が保留中の場合、Firepower Threat Defense デバイスに関する付加的な警告を提供します。Firepower Management Center にのみ適用される VDB の更新では再起動が行われないため、更新を展開できません。

関連トピック

設定変更の展開 （447 ページ）
Snort® の再起動シナリオ （450 ページ）

変更により Snort プロセスがただちに再起動する場合

以下の変更を行うと、展開プロセスを経ることなく Snort プロセスが直ちに再起動されます。再起動がトラフィックにどのような影響を与えるかは、ターゲットデバイスがトラフィックを処理する方法によって異なります。詳細はSnort® の再起動によるトラフィックの動作 （451 ページ）を参照してください。

- アプリケーションまたはアプリケーションディテクタに関する次の操作のいずれかを実行します。
  - システムまたはカスタム アプリケーション ディテクタを有効または無効にします。
  - アクティブ化されたカスタム ディテクタを削除します。
  - アクティブ化されたカスタム ディテクタを**保存して再アクティブ化**します。
  - ユーザ定義のアプリケーションを作成します。

  この操作を続けると管理対象のすべてのデバイスで Snort プロセスが再起動するという警告メッセージが表示され、キャンセルが可能になります。再起動は、現在のドメインまたはその子ドメインのいずれかの管理対象デバイスで発生します。
- Firepower Threat Defense ハイ アベイラビリティ ペアの作成または解除：ハイ アベイラビリティ ペアの作成を続行すると、プライマリ デバイスとセカンダリ デバイスで Snort プロセスが再起動するという警告メッセージが表示され、キャンセルが可能になります。

- 7000 または 8000 シリーズ ユーザ インターフェイスで Snort プロセスを再起動します（[システム（System）] > [設定（Configuration）] > [プロセス（Process）]）。確認メッセージが表示され、キャンセルすることができます。

ポリシーの比較

変更後のポリシーが組織の標準に準拠することを確かめたり、システム パフォーマンスを最適化したりする目的で、2つのファイル ポリシーの間の違いや、保存済みポリシーと実行中のポリシーの間の違いを調べることができます。

比較できるポリシーのタイプは次のとおりです。

- DNS
- ファイル
- ヘルス
- アイデンティティ
- 侵入
- ネットワーク分析
- SSL

比較ビューには、両方のポリシーが並べて表示されます。2 つのポリシー間の違いは次のように強調表示されます。

- 青色は強調表示された設定が 2 つのポリシーで異なることを示し、差異は赤色で示されます。
- グリーンは、強調表示されている設定項目が一方のポリシーに含まれ、もう一方のポリシーには含まれないことを示します。

ポリシーの比較

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
機能に応じて異なる	機能に応じて異なる	いずれか（Any）	機能に応じて異なる	機能に応じて異なる

ステップ 1 比較するポリシーの管理ページにアクセスします。

- [DNS]：**[Policies]** > **[Access Control]** > **[DNS]**
- [ファイル（File）]：**[Policies]** > **[Access Control]** > **[Malware & File]**

- [状況（Health）]：**[System]** > **[Health]** > **[Policy]**
- [ID（Identity）]：**[Policies]** > **[Access Control]** > **[Identity]**
- [侵入（Intrusion）]：**[Policies]** > **[Access Control]** > **[Intrusion]**
- [ネットワーク分析（Network Analysis）]：**[Policies]** > **[Access Control]**、次に **[Network Analysis Policy]** または **[Policies]** > **[Access Control]** > **[Intrusion]**、次に **[Network Analysis Policy]**

  （注） カスタムユーザロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

- [SSL]：**[Policies]** > **[Access Control]** > **[SSL]**

ステップ 2 [Compare Policies] をクリックします。

ステップ 3 [比較対象（Compare Against）] ドロップダウン リストから、比較するタイプを次のように選択します。

- 異なる 2 つのポリシーを比較するには、[他のポリシー（Other Policy）] を選択します。
- 同じポリシーの 2 つのリビジョンを比較するには、[その他のリビジョン（Other Revision）] を選択します。
- 現在のアクティブ ポリシーを他のポリシーに対して比較するには、[実行中の設定（Running Configuration）] を選択します。

ステップ 4 選択した比較タイプに応じて、次のような選択肢があります。

- 2 つの異なるポリシーを比較する場合、[ポリシー A（Policy A）] ドロップダウン リストと [ポリシー B（Policy B）] ドロップダウン リストから比較するポリシーを選択します。
- 実行中の設定を別のポリシーと比較する場合、[ポリシー B（Policy B）] ドロップダウン リストから 2 番目のポリシーを選択します。

ステップ 5 [OK] をクリックします。

ステップ 6 比較の結果を確認します。

- [比較ビューア（Comparison Viewer）]：比較ビューアを使用して、ポリシーの違いを個別に検索するには、タイトル バーの上にある [前へ（Previous）] または [次へ（Next）] をクリックします。
- [比較レポート（Comparison Report）]：2 つのポリシーの違いを示す PDF レポートを生成するには、[比較レポート（Comparison Report）] をクリックします。

ポリシー レポート

ほとんどのポリシーには、2 種類のレポートを生成することができます。単一のポリシーに関するレポートには、現在保存されているポリシー設定の詳細が記載されます。一方、比較レポートには、2 つのポリシー間の違いだけがリストされます。単一ポリシー レポートは、ヘルス ポリシーを除くすべてのポリシー タイプについて生成できます。

（注） 侵入ポリシー レポートには基本ポリシーの設定とポリシー階層の設定が結合され、どちらが基本ポリシーまたはポリシー レイヤのどちらに基づく設定であるかは区別されません。

現在のポリシー レポートの生成

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
機能に応じて異なる	機能に応じて異なる	いずれか（Any）	機能に応じて異なる	機能に応じて異なる

ステップ 1 レポートを生成するポリシーの管理ページにアクセスします。

- アクセス制御—**[Policies]** > **[Access Control]**
- [DNS]：**[Policies]** > **[Access Control]** > **[DNS]**
- [ファイル（File）]：**[Policies]** > **[Access Control]** > **[Malware & File]**
- [状況（Health）]：**[System]** > **[Health]** > **[Policy]**
- [ID（Identity）]：**[Policies]** > **[Access Control]** > **[Identity]**
- [侵入（Intrusion）]：**[Policies]** > **[Access Control]** > **[Intrusion]**
- 7000 & 8000 シリーズ デバイスの NAT：**[Devices]** > **[NAT]**
- [ネットワーク分析（Network Analysis）]：**[Policies]** > **[Access Control]**、次に **[Network Analysis Policy]** または **[Policies]** > **[Access Control]** > **[Intrusion]**、次に **[Network Analysis Policy]**

  （注） カスタム ユーザ ロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

- [SSL]：**[Policies]** > **[Access Control]** > **[SSL]**

ステップ 2 レポートの生成対象とするポリシーの横にあるレポート アイコン（  ）をクリックします。

失効ポリシー

Firepower システムは、失効したポリシーに赤色のステータス テキストでマークを付けます。このテキストには、ポリシーの更新を必要とするターゲット デバイスの数が示されます。失効ステータスをクリアするには、ポリシーをデバイスに再展開する必要があります。

ポリシーの再展開が必要な設定変更には次のものがあります。

- アクセス コントロール ポリシー自体の変更：アクセス コントロール ルール、デフォルト アクション、ポリシー ターゲット、セキュリティ インテリジェンス フィルタリング、前処理などの詳細オプションの変更。

- アクセス コントロール ポリシーが呼び出すポリシーの変更：SSL ポリシー、ネットワーク分析ポリシー、侵入ポリシー、ファイル ポリシー、アイデンティティ ポリシー、または DNS ポリシー。
- 呼び出されるアクセス コントロール ポリシーで使用される再利用可能オブジェクトまたは設定の変更：
  - ネットワーク、ポート、VLAN タグ、URL、地理位置情報オブジェクト
  - セキュリティ インテリジェンス リストおよびフィード
  - アプリケーション フィルタまたはディテクタ
  - 侵入ポリシーの変数セット
  - ファイル リスト
  - 復号関連のオブジェクトとセキュリティ ゾーン
- システム ソフトウェア、侵入ルール、または脆弱性データベース（VDB）の更新。

Webインターフェイスの複数の場所からこれらの設定の一部を変更できることに留意してください。たとえば、オブジェクト マネージャ（**[Objects]** > **[Object Management]**）を使用してセキュリティ ゾーンを変更できますが、デバイスの設定（**[Devices]** > **[Device Management]**）でインターフェイスのタイプを変更すると、ゾーンも変更され、ポリシーの再展開が必要になります。

次の更新では、ポリシーの再展開は**必要ありません**。

- セキュリティ インテリジェンス フィードへの自動更新およびコンテキスト メニューを使用したセキュリティ インテリジェンスのグローバル ブラックリストおよびホワイトリストへの追加
- URL フィルタリング データへの自動更新
- スケジュールされた位置情報データベース（GeoDB）の更新

限定的な導入のパフォーマンスに関する考慮事項

システムはホスト、アプリケーション、ユーザ検出データを使用することで、ネットワークの完全な最新プロファイルを作成できます。また、システムが侵入検知および防御システム（IPS）として機能して、ネットワーク トラフィックを分析して侵入およびエクスプロイトを検出し、オプションで問題のあるパケットをドロップすることもできます。

検出とIPSを組み合わせることで、ネットワーク アクティビティにコンテンツが提供され、次のような多くの機能を利用することができます。

- 侵害の影響フラグと表示。これによって、どのホストが特定のエクスプロイト、攻撃、またはマルウェアに対して脆弱であるかが示されます。

- アダプティブ プロファイルの更新と Firepower の推奨事項。これによって、宛先ホストに応じてトラフィックを個別に検査できます。
- 相関。これによって、影響を受けるホストに応じて別々に侵入（およびその他のイベント）に応答できます。

ただし、組織が IPS または検出のみを実行することを目的としている場合は、システムのパフォーマンスを最適化できる設定がいくつかあります。

侵入防御のない検出

検出機能では、ネットワーク トラフィックをモニタして、ネットワーク上のホストの数とタイプ（ネットワーク デバイスを含む）だけでなく、それらのホスト上のオペレーティング システム、アクティブなアプリケーション、およびオープン ポートを判断できます。管理対象デバイスをネットワークのユーザアクティビティをモニタするように設定することもできます。検出データを使用して、トラフィック プロファイリングを実行し、ネットワーク コンプライアンスを評価し、ポリシー違反に応答できます。

基本的な展開（検出と単純なネットワークベースのアクセス制御のみ）では、アクセス コントロール ポリシーの設定時にいくつかの重要なガイドラインに従うことで、デバイスのパフォーマンスを向上させることができます。

（注） それが単にすべてのトラフィックを許可する場合であっても、アクセス コントロール ポリシーを使用する必要があります。ネットワーク検出ポリシーが実行できるのは、アクセス コントロール ポリシーが通過を許可したトラフィックを検査することのみです。

最初に、アクセス コントロール ポリシーは複雑な処理を必要とせず、単純なネットワークベースの基準のみを使用してネットワーク トラフィックを処理することを確認します。次のすべてのガイドラインを実装する必要があります。これらのオプションのいずれかを誤って設定すると、パフォーマンス上の利点がなくなります。

- セキュリティ インテリジェンス機能を使用しないでください。入力されたグローバル ホワイトリストまたはブラックリストをポリシーのセキュリティ インテリジェンスの設定から削除します。
- モニタ アクションまたはインタラクティブ ブロック アクションにアクセス コントロール ルールを含めないでください。許可、信頼、およびブロック ルールのみを使用します。許可されたトラフィックは検出によって検査できますが、信頼されたトラフィックとブロックされたトラフィックは検査できないことに留意してください。
- アプリケーション、ユーザ、URL、ISE 属性、または位置情報ベースのネットワーク条件にアクセス コントロール ルールを含めないでください。単純なネットワークベースの条件（ゾーン、IP アドレス、VLAN タグ、およびポート）のみを使用します。

- ファイル、マルウェア、または侵入インスペクションを実行するアクセス コントロール ルールを含めないでください。つまり、ファイルポリシーまたは侵入ポリシーをアクセス コントロール ルールに関連付けないでください。
- アクセス コントロール ポリシーのデフォルトの侵入ポリシーが [アクティブなルールなし（No Rules Active）] に設定されていることを確認します。
- ポリシーのデフォルト アクションとして [ネットワーク検出のみ（Network Discovery Only）] を選択します。侵入インスペクションを実行するポリシーのデフォルト アクションを選択しないでください。

アクセス コントロール ポリシーと組み合わせて、ネットワーク検出ポリシーを設定して適用できます。このポリシーは、システムが検出データについて検査をするネットワーク セグメント、ポート、およびゾーンを指定し、ホスト、アプリケーション、およびユーザがセグメント、ポート、およびゾーンで検出されるかどうかを指定します。

関連トピック

デフォルトの侵入ポリシー （2287 ページ）

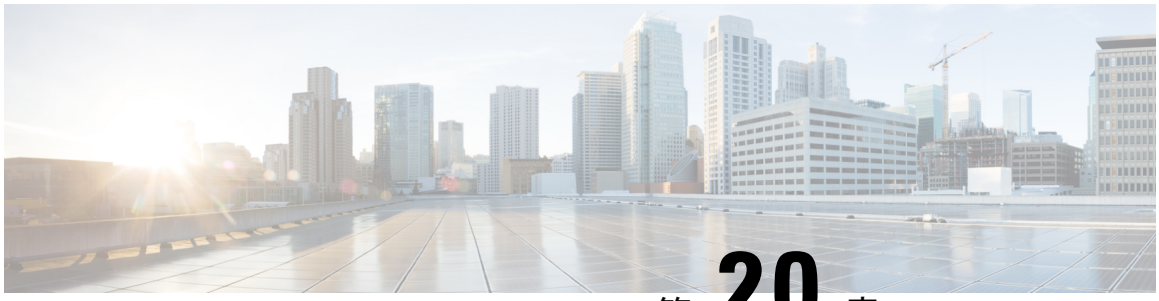
ディスカバリのない侵入防御

必要がない場合（たとえば、IPS のみの展開など）に検出を無効にするとパフォーマンスが向上する可能性があります。検出を無効にするには、次のすべての変更を実装する必要があります。

- ネットワーク検出ポリシーからすべてのルールを削除します。
- 単純なネットワークベースの条件（ゾーン、IP アドレス、VLAN タグ、およびポート）のみを使用してアクセス制御を実行します。

  どんな種類のセキュリティ インテリジェンス、アプリケーション、ユーザ、URL、または地理位置情報の制御も行わないでください。検出データの保存を無効にできても、システムではそれらの機能を実装するためにデータを収集して検査する必要があります。
- デフォルトのグローバル リストなど、アクセス コントロール ポリシーのセキュリティ インテリジェンス設定からすべてのホワイトリストとブラックリストを削除することで、ネットワークと URL ベースのセキュリティ インテリジェンスを無効にします。
- DNS のデフォルトのグローバル ホワイトリストや DNS ルールのグローバル ブラックリストなど、関連付けられている DNS ポリシー内のすべてのルールを削除または無効にすることで、DNS ベースのセキュリティ インテリジェンスを無効にします。

展開後、新たな検出はターゲット デバイス上で停止します。タイムアウトの設定に応じて、システムはネットワーク マップ内の情報を段階的に削除していきます。または、すべての検出データを即座に消去できます。



第 20 章

ルール管理：共通の特性

以下のトピックでは、Firepower Management Center でさまざまなポリシーのルールの共通特性を管理する方法について説明します。

ルールの概要

さまざまなポリシー内のルールで、ネットワーク トラフィックをきめ細かく制御できます。システムは最初の一致のアルゴリズムを使用して、指定した順番でルールに照らし合わせてトラフィックを評価します。

これらのルールはポリシー全体で一貫していない他の設定を含んでいる場合もありますが、次のような多くの基本的な特性や設定メカニズムは共通です。

- 条件：ルールの条件は各ルールが処理するトラフィックを指定します。複数の条件により各ルールを設定できます。トラフィックは、ルールに一致するすべての条件に適合する必要があります。
- アクション：ルールのアクションによって、一致するトラフィックの処理方法が決まります。選択できる [アクション（Action）] リストがルールにない場合でも、ルールには関連付けられたアクションが 1 つある点に注意してください。たとえば、カスタム ネットワーク分析ルールはそのルールの「アクション」としてネットワーク分析ポリシーを使用します。 別の例としては、QoS ルールの場合、どの QoS ルールでもトラフィックのレート制限という同じ動作をするため、明示的なアクションはありません。
- 位置：ルールの位置は評価の順番を決定します。ポリシーを使ってトラフィックを評価すると、システムは指定した順序でトラフィックとルールを照合します。通常は、システム

によるトラフィックの処理は、すべてのルールの条件がトラフィックに一致する最初のルールに従って行われます（追跡とログ記録を行うように設計されたモニタルールは例外です）。適切なルールの順序を指定することで、ネットワークトラフィックの処理に必要なリソースが削減され、ルールのプリエンプションを回避できます。

- カテゴリ：いくつかのルールタイプを整理するために、各親ポリシーでカスタムのルールカテゴリを作成できます。
- ロギング：多くのルールでは、ルールが処理する接続をシステムがロギングするかどうか、およびロギングの処理方法は、ロギングの設定によって制御されます。一部のルール（IDルールやネットワーク分析ルールなど）にはロギング設定は含まれません。これは、ルールが接続の最終的な性質を決定するわけではなく、またそのルールが接続をロギングするために特別に設計されているわけではないためです。 別の例としては、QoS ルールにはロギングの設定は含まれていません。これは、レート制限されているというだけの理由で接続をロギングすることはできないためです。
- コメント：一部のルールタイプでは、変更を保存するたびにコメントを追加できます。たとえば、他のユーザのために設定全体を要約したり、ルールの変更時期と変更理由を記載することができます。

ヒント 多くのポリシーエディタでは、右クリック メニューで編集、削除、移動、有効化、無効化など、数多くのルール管理オプションへのショートカットを提供しています。

共通の特性を持つルール

この章では、以下のルールや設定に見られる多くの共通の側面について説明しています。共通していない設定の情報については、以下を参照してください。

- アクセス コントロール ルール： アクセス コントロール ルール （1689 ページ）
- トンネルとプレフィルタ ルール： トンネルとプレフィルタ ルールのコンポーネント （1775 ページ）
- SSL ルール： TLS/SSL ルールの作成と変更 （1855 ページ）
- DNS ルール： DNS ルールの作成および編集 （1756 ページ）
- ID ルール： アイデンティティ ルールの作成 （2638 ページ）
- ネットワーク分析ルール： ネットワーク分析ルールの設定 （2292 ページ）
- QoS ルール： QoS ルールの設定 （867 ページ）
- インテリジェントアプリケーションバイパス（IAB）： インテリジェントアプリケーション バイパス （1783 ページ）
- アプリケーション フィルタ： アプリケーション フィルタ （530 ページ）

共通の特性のないルール

次のルールの設定は、この章では説明していません。

- 侵入ルール： ルールを使用した侵入ポリシーの調整 （2073 ページ）
- ファイルおよびマルウェア ルール： ファイル ルール （1939 ページ）
- 相関ルール： 相関ルールの設定 （2701 ページ）
- NAT ルール（クラシック）： 7000 および 8000 シリーズ デバイス用の NAT （1427 ページ）
- NAT ルール（Firepower Threat Defense）：Firepower Threat Defense 用のネットワーク アドレス変換（NAT） （1449 ページ）
- 8000 シリーズ 高速パス ルール： 高速パス ルールの設定（8000 シリーズ） （307 ページ）

ルール条件タイプ

次の表は、この章に記述している一般的なルールの条件について説明し、使用設定を列挙します。

条件	トラフィック制御方法	対応しているルール/設定
インターフェイス条件 （468 ページ）	送信元インターフェイスと宛先インターフェイス、対応している場合にはトンネル ゾーン	アクセス コントロール ルール トンネル ルール プレフィルタ ルール SSL ルール DNS ルール アイデンティティ ルール ネットワーク分析ルール QoS ルール
ネットワーク条件 （471 ページ）	送信元 IP アドレスと宛先 IP アドレス、対応している場合には地理的な場所や発信側のクライアント	アクセス コントロール ルール プレフィルタ ルール SSL ルール DNS ルール アイデンティティ ルール ネットワーク分析ルール QoS ルール

条件	トラフィック制御方法	対応しているルール/設定
トンネル エンドポイント条件（474 ページ）	プレーン テキスト用、送信元のトンネル エンドポイントと宛先のトンネル エンドポイント、パススルー トンネル	トンネル ルール
VLAN 条件 （476 ページ）	VLAN タグ	アクセス コントロール ルール トンネル ルール プレフィルタ ルール SSL ルール DNS ルール アイデンティティ ルール ネットワーク分析ルール
ポートおよび ICMP コードの条件 （477 ページ）	送信元ポート、宛先ポート、プロトコル、ICMP コード	アクセス コントロール ルール プレフィルタ ルール SSL ルール アイデンティティ ルール QoS ルール
カプセル化の条件 （479 ページ）	カプセル化プロトコル（非暗号化）	トンネル ルール
アプリケーション条件（アプリケーション制御） （479ページ）	アプリケーションまたはアプリケーション特性（タイプ、リスク、ビジネスの関連性、カテゴリ、タグ）	アクセス コントロール ルール SSL ルール アイデンティティ ルール QoS ルール アプリケーション フィルタ インテリジェント アプリケーション バイパス（IAB）
URL 条件（URL フィルタリング） （489 ページ）	URL、対応している場合には、URL の特性（カテゴリおよびレピュテーション）	アクセス コントロール ルール SSL ルール QoS ルール

条件	トラフィック制御方法	対応しているルール/設定
ユーザ条件、レルム条件、および ISE 属性条件（ユーザ制御） （490 ページ）	ホストのログイン権限のあるユーザまたはそのユーザのレルム、グループ、または ISE 属性	アクセス コントロール ルール SSL ルール（ISE 属性なし） QoS ルール
カスタム SGT 条件 （495 ページ）	カスタム セキュリティ グループ タグ（SGT）	アクセス コントロール ルール QoS ルール

ルール条件の仕組み

ルール条件では、各ルールで処理するトラフィックを指定します。各ルールに複数の条件を設定し、トラフィックがルールに一致するにはすべての条件を満たす必要があります。使用可能な条件タイプは、ルール タイプによって異なります。

ルール エディタには、条件タイプごとに独自のタブ ページがあります。一致させるトラフィック特性を選択して条件を作成します。一般に、左側の使用可能な項目のリスト（1 つまたは 2 つ）から基準を選択し、それらの基準を右側の選択済み項目のリスト（1 つまたは 2 つ）に追加します。たとえば、アクセス コントロール ルールの URL 条件では、URL カテゴリとレピュテーション基準を組み合わせて、ブロックする Web サイトのグループを 1 つ作成できます。

条件を作成しやすくするために、レルム、ISE 属性、さまざまなタイプのオブジェクトやオブジェクト グループなど、さまざまなシステム提供の構成やカスタム構成を使用して、トラフィックを照合できます。多くの場合、ルール基準は手動で指定できます。

可能な場合は常に、一致基準を空のままにします（特にセキュリティ ゾーン、ネットワーク オブジェクト、およびポート オブジェクトの場合）。基準を複数指定すると、指定した条件の内容についてすべての組み合わせと照合する必要があります。

注意 アクセス コントロール ルールを適切に設定しないと、ブロックされるべきトラフィックが許可されるなど、予期しない結果が発生する可能性があります。一般的に、アプリケーション制御ルールは、たとえば IP アドレスに基づくルールよりも照合に時間がかかるため、アクセス コントロール リスト内の順位を低くする必要があります。

特定の条件（ネットワークや IP アドレスなど）を使用するアクセス コントロール ルールは、一般的な条件（アプリケーションなど）を使用するルールの前に順位付けする必要があります。オープン システム相互接続（OSI）モデルに精通している場合は、考え方として同様の順位付けを使用してください。レイヤ 1、2、および 3（物理、データリンク、およびネットワーク）の条件を持つルールは、アクセス コントロール ルールの最初に順位付けする必要があります。レイヤ 5、6、および 7（セッション、プレゼンテーション、およびアプリケーション）の条件は、アクセス コントロール ルールの後ろのほうに順序付けする必要があります。OSI モデルの詳細については、こちらの Wikipedia の記事を参照してください。

送信元と宛先の基準

ルールに送信元と宛先の基準（ゾーン、ネットワーク、ポート）が含まれる場合、通常は一方または両方の基準を制約として使用できます。両方を使用する場合、一致するトラフィックの発信元は、指定した送信元のゾーン、ネットワーク、またはポートのいずれかであり、宛先のゾーン、ネットワーク、またはポートのいずれかから送出される必要があります。

条件ごとの項目

最大 50 個の項目を各条件に追加できます。送信元と宛先の基準を含むルールでは、それぞれ最大 50 個使用できます。選択した項目のいずれかに一致するトラフィックが条件に一致します。

単純なルールの仕組み

ルールエディタには、次の一般的な選択肢があります。条件の作成の詳細な手順については、各条件タイプのトピックを参照してください。

- 項目の選択（Choose Item）：項目をクリックするか、そのチェックボックスにマークを付けます。多くの場合、Ctrl または Shift キーを使用して複数の項目を選択するか、右クリックして [すべて選択（Select All）] を選択できます。
- 検索（Search）：検索フィールドに基準を入力します。入力するとリストが更新されます。項目名が検索され、オブジェクトとオブジェクトグループについては、その値が検索されます。リロード（）またはクリア（）をクリックして検索をクリアします。
- 事前定義された項目の追加（Add Predefined Item）：1 つ以上の使用可能な項目を選択し、[追加（Add）] ボタンをクリックするか、ドラッグアンドドロップします。無効な項目（重複、無効な組み合わせなど）は追加できません。
- 手動項目の追加（Add Manual Item）：[選択済み（Selected）] 項目リストの下のフィールドをクリックし、有効な値を入力して [追加（Add）] をクリックします。ポートを追加すると、ドロップダウン リストからプロトコルも選択できます。
- オブジェクトの作成（Create Object）：追加アイコン（）をクリックし、作成する条件ですぐに使用できる新しい再利用可能オブジェクトを作成し、オブジェクトマネージャで管理できます。この方法を使用してアプリケーションフィルタをその場で追加した場合、別のユーザ作成フィルタが含まれるフィルタを保存することはできません。
- 削除（Delete）：項目の削除アイコン（）をクリックするか、1 つ以上の項目を選択し、右クリックして [選択項目の削除（Delete Selected）] を選択します。

インターフェイス条件

インターフェイスルールの条件は送信元インターフェイスと宛先インターフェイスによってトラフィックを制御します。

ルールタイプと導入環境でのデバイスにより、セキュリティゾーンやインターフェイスグループと呼ばれる定義済みのインターフェイスオブジェクトを使用してインターフェイス条件を構築できます。インターフェイスオブジェクトはネットワークをセグメント化して複数のデバイス間でインターフェイスをグループ化することによってトラフィックフローを制御し、分類しやすくします。インターフェイス オブジェクト：インターフェイスグループとセキュリティゾーン （535 ページ）を参照してください。

ヒント インターフェイスによってルールを制約するのは、システムパフォーマンスを改善するための最適な方法の1つです。ルールがデバイスのすべてのインターフェイスを除外する場合、そのルールはそのデバイスのパフォーマンスに影響しません。

インターフェイスオブジェクト内のすべてのインターフェイスが同じタイプ（すべてインライン、パッシブ、スイッチド、ルーテッド、または ASA FirePOWER）である必要があるのと同様に、インターフェイス条件で使用されているすべてのインターフェイスオブジェクトは同じタイプである必要があります。パッシブに展開されたデバイスはトラフィックを送信しないため、パッシブ展開では宛先インターフェイスでルールを制約することはできません。

トンネルゾーンとセキュリティ ゾーン

一部の設定では、セキュリティゾーンの代わりにトンネルゾーンを使用してインターフェイス条件を制約できます。トンネルゾーンではプレフィルタを使用して、カプセル化された接続の特定のタイプに合わせて後続のトラフィック処理を調整できます。

（注） トンネルゾーンの制約がサポートされる設定の場合、再区分された接続、つまり割り当てられたトンネルゾーンを持つ接続はセキュリティゾーンの制約と一致**しません**。詳細については、トンネル ゾーンおよびプレフィルタリング （1777 ページ）を参照してください。

インターフェイス条件を持つルール

ルール タイプ	セキュリティ ゾーンのサポート	トンネルゾーンのサポート	インターフェイス グループのサポート
アクセス コントロール	はい	はい	いいえ（No）
トンネルとプレフィルタ	Yes	該当なし。プレフィルタポリシー内でトンネルゾーンを割り当てます	可
SSL	はい	いいえ	いいえ
DNS（送信元のみ）	はい	いいえ	いいえ
ID（Identity）	はい	いいえ	いいえ

ルール タイプ	セキュリティ ゾーンのサポート	トンネルゾーンのサポート	インターフェイス グループのサポート
ネットワーク分析	はい	いいえ	いいえ
QoS（ルーテッドのみ、必須）	はい	いいえ	はい

例：セキュリティ ゾーンを使用したアクセス制御

たとえば、ホストがインターネットに無制限でアクセスできるような導入にする一方、着信トラフィックで侵入およびマルウェアの有無を検査することでホストを保護したいとします。

それにはまず、内部ゾーンと外部ゾーンという 2 つのセキュリティ ゾーンを作成します。次に、これらのゾーンに 1 つ以上のデバイス上のインターフェイス ペアを割り当て、各ペアの一方のインターフェイスを内部ゾーンに割り当て、もう一方のインターフェイスを外部ゾーンに割り当てます。内部側のネットワークに接続されたホストは、保護されている資産を表します。

（注） 内部（または外部）のすべてのインターフェイスを 1 つのゾーンにグループ化する必要はありません。導入ポリシーおよびセキュリティ ポリシーが意味をなすグループ化を選択します。

次に、宛先ゾーン条件を内部に設定したアクセス コントロール ルールを構成します。この単純なルールでは、内部ゾーンのいずれかのインターフェイスでデバイスから出力されるトラフィックが照合されます。一致するトラフィックを侵入やマルウェアについて検査するには、ルール アクションとして [許可（Allow）] を選択し、そのルールを侵入ポリシーとファイル ポリシーに関連付けます。

インターフェイス条件の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Access Admin/Network Admin

始める前に

- （アクセス コントロールのみ）セキュリティ ゾーンではなくトンネル ゾーンによってトラフィックを制約する場合は、関連付けられたプレフィルタ ポリシーがそれらのゾーンを割り当てるようにします。アクセス制御への他のポリシーの関連付け（1684 ページ）を参照してください。

ステップ 1 ルール エディタで、インターフェイス条件のタブをクリックします。

- インターフェイス グループおよびセキュリティ ゾーン（トンネル、プレフィルタ、QoS）：[インターフェイス オブジェクト（Interface Objects）] タブをクリックします。
- セキュリティ ゾーン（アクセス コントロール、SSL、DNS、アイデンティティ、ネットワーク分析）：[ゾーン（Zones）] タブをクリックします。
- トンネルゾーン（アクセス コントロール）：[ゾーン（Zones）] タブをクリックします。

ステップ 2 [使用可能なインターフェイス オブジェクト（Available Interface Objects）] または [利用可能なゾーン（Available Zones）] リストから追加するインターフェイスを見つけて選択します。

（アクセス コントロールのみ）再ゾーン分割されたトンネルでの接続を一致させるには、セキュリティ ゾーンではなくトンネル ゾーンを選択します。同じルールでトンネル ゾーンとセキュリティ ゾーンを使用することはできません。詳細については、トンネル ゾーンおよびプレフィルタリング （1777 ページ）を参照してください。

ステップ 3 [送信元に追加（Add to Source）] または [宛先に追加（Add to Destination）] をクリックするか、またはドラッグ アンド ドロップします。

ステップ 4 ルールを保存するか、編集を続けます。

次のタスク

- （アクセス コントロールのみ）プレフィルタ中にトンネルを再ゾーン分割した場合、完全なカバレッジを確保する必要がある場合は追加のルールを設定します。再ゾーン分割されたトンネルでの接続は、セキュリティ ゾーン制約があるルールに一致**しません**。詳細については、「トンネル ゾーンの使用 （1778 ページ）」を参照してください。
- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

ネットワーク条件

ネットワーク ルールの条件では、内部ヘッダーを使用して、送信元と宛先の IP アドレスを基準にトラフィックを制御します。外部ヘッダーを使用するトンネル ルールでは、ネットワーク条件の代わりにトンネル エンドポイント条件を使用します。

事前定義されたオブジェクトを使用してネットワーク条件を作成することも、個々の IP アドレスまたはアドレス ブロックを手動で指定することもできます。

（注） システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。 上書き対応オブジェクトを使用すると、子孫ドメインの管理者は、グローバル コンフィギュレーションを自分のローカル環境に調整できます。

可能な場合は常に、一致基準を空のままにします（特にセキュリティ ゾーン、ネットワーク オブジェクト、およびポート オブジェクトの場合）。基準を複数指定すると、指定した条件の内容についてすべての組み合わせと照合する必要があります。

ネットワーク条件での地理位置情報

ルールによっては、送信元または宛先の地理的位置を使用してトラフィックを照合することもできます。ルールのタイプが地理位置情報をサポートするものであれば、ネットワーク条件と地理位置情報条件を混在させることができます。トラフィックのフィルタリングに最新の地理位置情報データが使用されるよう、地理位置情報データベース（GeoDB）を定期的に更新することを強くお勧めします。

ネットワーク条件での元のクライアント（プロキシ トラフィックのフィルタリング）

一部のルールでは、発信元クライアントに基づいてプロキシ トラフィックを処理できます。送信元ネットワーク条件を使用してプロキシ サーバを指定し、次に元のクライアント制約を追加して元のクライアント IP アドレスを指定します。システムはパケットの X-Forwarded-For（XFF）、True-Client-IP、またはカスタム定義 HTTP ヘッダー フィールドを使用して、元のクライアント IP を判別します。

プロキシの IP アドレスがルールの送信元ネットワークの制約と一致する場合、トラフィックはルールに一致し、さらに元のクライアントの IP アドレスは、ルールの元のクライアント制約に一致します。たとえば、特定の元のクライアント アドレスからのトラフィックを許可するものの、それが特定のプロキシを使用している場合のみに限定するには、以下の 3 つのアクセス コントロール ルールを作成します。

アクセス コントロール ルール 1：特定の IP アドレス（209.165.201.1）からの非プロキシ トラフィックをブロックします。

送信元ネットワーク：209.165.201.1
元のネットワーク クライアント：none または any
アクション：ブロック

アクセス コントロール ルール 2：同じ IP アドレスからのプロキシ トラフィックを許可します。ただし、そのトラフィックのプロキシ サーバが、選択したもの（209.165.200.225 または 209.165.200.238）である場合に限ります。

送信元ネットワーク：209.165.200.225 および 209.165.200.238
元のクライアント ネットワーク：209.165.201.1
アクション：許可

アクセス コントロール ルール 3：同じ IP アドレスからのプロキシ トラフィックを、それが他のプロキシ サーバを使用する場合はブロックします。

[Source Networks]：any
元のクライアント ネットワーク：209.165.201.1
アクション：ブロック

ネットワーク条件を使用したルール

ルール タイプ	地理位置情報による制約のサポート	元のクライアントによる制約のサポート
アクセス コントロール	はい	はい
プレフィルタ	いいえ	いいえ
SSL	はい	いいえ（No）
DNS（送信元ネットワークのみ）	いいえ	いいえ
ID（Identity）	はい	いいえ（No）
ネットワーク分析	いいえ	いいえ
QoS	はい	はい

ネットワーク条件の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Access Admin/Network Admin

ステップ 1 ルール エディタで、[ネットワーク（Networks）] タブをクリックします。

ステップ 2 [利用可能なネットワーク（Available Networks）] リストから追加する定義済みネットワークを見つけて選択します。

ルールが地理位置情報をサポートしている場合は、ネットワークと地理位置情報の基準を同じルールに混在させることができます。

- [ネットワーク（Networks）] : [ネットワーク（Networks）] サブタブをクリックして、ネットワークを選択します。
- [地理位置情報（Geolocation）] : [地理位置情報（Geolocation）] サブタブをクリックして、地理位置情報オブジェクトを選択します。

ステップ 3 （オプション）ルールが元のクライアント制約をサポートしている場合は、[送信元ネットワーク（Source Networks）] で、プロキシされたトラフィックを元のクライアントに基づいて処理するようにルールを設定します。

- [送信元/プロキシ（Source/Proxy）] : [送信元（Source）] サブタブをクリックして、プロキシ サーバを指定します。

- [元のクライアント（Original Client）]：[元のクライアント（Original Client）] サブタブをクリックして、ネットワークを元のクライアント制約として追加します。プロキシ接続では、元のクライアントの IP アドレスは、ルールに一致するネットワークの 1 つと一致する必要があります。

ステップ 4 [送信元に追加（Add to Source）]、[元のクライアントに追加（Add to Original Client）]、または [宛先に追加（Add to Destination）] をクリックするか、またはドラッグ アンド ドロップします。

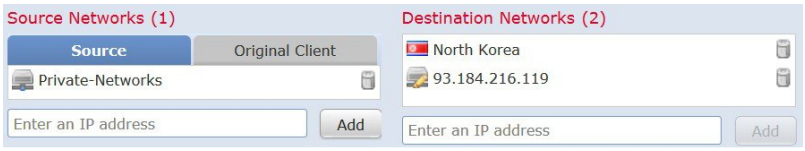
ステップ 5 手動で指定するネットワークを追加します。送信元、元のクライアント、または宛先 IP アドレスかアドレス ブロックを入力し、[追加（Add）] をクリックします。

（注） システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。 上書き対応オブジェクトを使用すると、子孫ドメインの管理者は、グローバル コンフィギュレーションを自分のローカル環境に調整できます。

ステップ 6 ルールを保存するか、編集を続けます。

例：アクセス コントロール ルールのネットワーク条件

次の図は、内部ネットワークから発生し、北朝鮮または 93.184.216.119（example.com）のリソースにアクセスしようとする接続をブロックするアクセス コントロール ルールのネットワーク条件を示しています。



この例で、「Private Networks」と呼ばれるネットワーク オブジェクト グループ（図に示されていない IPv4 および IPv6 プライベート ネットワークのネットワーク オブジェクトから構成されます）は、内部ネットワークを表します。また、example.com の IP アドレスを手動で指定し、システムが提供する北朝鮮の位置情報オブジェクトを使用して北朝鮮の IP アドレスを表しています。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

トンネル エンドポイント条件

トンネル エンドポイント条件は、トンネル ルールに固有のものです。この条件は、他のルール タイプのネットワーク条件と似ています。

トンネルエンドポイント条件は、特定のタイプのプレーンテキスト、パススルートンネル（カプセル化の条件 （479ページ）を参照）を制御します。この制御は、それらの送信元と宛先の IP アドレスによって、外側のカプセル化ヘッダーを使用して行います。これらは、トンネル

エンドポイントの IP アドレス、つまり、トンネルのいずれかの側のネットワーク デバイスのルーテッド インターフェイスです。

トンネル ルールはデフォルトでは双方向で、送信元エンドポイントのいずれかと宛先エンドポイントのいずれかとの間の一致するすべてのトンネルを処理します。ただし、送信元から宛先へのトラフィックのみに一致する単方向トンネル ルールを設定できます。トンネルとプレフィルタ ルールのコンポーネント （1775 ページ）を参照してください。

事前定義済みのネットワーク オブジェクトを使用してトンネル エンドポイント条件を作成したり、個々の IP アドレスまたはアドレス ブロックを手動で指定したりできます。

（注） システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。 上書き対応オブジェクトを使用すると、子孫ドメインの管理者は、グローバル コンフィギュレーションを自分のローカル環境に調整できます。

トンネル エンドポイント条件の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	Firepower Threat Defense	いずれか（Any）	Admin/Access Admin/Network Admin

ステップ 1 ルール エディタで、[トンネル エンドポイント（Tunnel Endpoints）] タブをクリックします。

ステップ 2 [利用可能なトンネル エンドポイント（Available Tunnel Endpoints）] リストから追加する定義済みネットワークを見つけて選択します。

トンネル エンドポイントは、トンネルの両側にあるネットワーク デバイスのルーテッド インターフェイスの IP アドレスであるため、ネットワーク オブジェクトを使用してトンネル エンドポイント条件を作成できます。

ステップ 3 [送信元に追加（Add to Source）] または [宛先に追加（Add to Destination）] をクリックするか、またはドラッグ アンド ドロップします。

トンネル ルールはデフォルトでは双方向であるため、2 つのエンドポイント間のすべてのトラフィックを処理できます。ただし、送信元からのトンネルのみを照合するよう選択した場合、トンネル ルールは、送信元から宛先へのトラフィックのみに一致します。

ステップ 4 手動で指定するエンドポイントを追加します。送信元か宛先の IP アドレス、またはアドレス ブロックを入力し、[追加（Add）] をクリックします。

（注） システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、実際のIPアドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。 上書き対応オブジェクトを使用すると、子孫ドメインの管理者は、グローバル コンフィギュレーションを自分のローカル環境に調整できます。

ステップ 5 ルールを保存するか、編集を続けます。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

VLAN 条件

VLAN ルール条件によって、QinQ（スタック VLAN）など、VLAN タグ付きトラフィックが制御されます。システムでは、プレフィルタ ポリシー（そのルールで最も外側の VLAN タグを使用する）を除き、最も内側の VLAN タグを使用して VLAN トラフィックをフィルタ処理します。

事前定義のオブジェクトを使用して VLAN 条件を作成でき、また **1** ～ **4094** の VLAN タグを手動で入力することもできます。VLANタグの範囲を指定するには、ハイフンを使用します。

最大 50 個の VLAN 条件を指定できます。

（注） システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、実際の VLAN タグを使用してこの設定を抑制すると、予期しない結果になる可能性があります。 上書き対応オブジェクトを使用すると、子孫ドメインの管理者は、グローバル コンフィギュレーションを自分のローカル環境に調整できます。

VLAN 条件が含まれたルール

次のルール タイプでは、VLAN 条件がサポートされます。

- アクセス コントロール
- トンネルとプレフィルタ（最も外側の VLAN タグを使用）
- SSL
- DNS
- ID（Identity）
- ネットワーク分析

ポートおよび ICMP コードの条件

ポート条件を使用することで、トラフィックの送信元および宛先のポートに応じてそのトラフィックを制御できます。ルールのタイプによって、「ポート」は次のいずれかを表します。

- TCP と UDP：TCP および UDP トラフィックは、トランスポート層プロトコルに基づいて制御できます。システムは、カッコ内に記載されたプロトコル番号 + オプションの関連ポートまたはポート範囲を使用してこの設定を表します。例：TCP(6)/22。
- ICMP：ICMP および ICMPv6（IPv6 ICMP）トラフィックは、そのインターネット層プロトコルと、オプションでタイプおよびコードに基づいて制御できます。例：ICMP(1):3:3
- ポートなし：ポートを使用しない他のプロトコルを使用してトラフィックを制御できます。

可能な場合は常に、一致基準を空のままにします（特にセキュリティ ゾーン、ネットワーク オブジェクト、およびポート オブジェクトの場合）。基準を複数指定すると、指定した条件の内容についてすべての組み合わせと照合する必要があります。

送信元と宛先ポートの制約の使用

送信元ポートと宛先ポートの両方を制約に追加する場合、単一のトランスポート プロトコル（TCP または UDP）を共有するポートのみを追加できます。たとえば、送信元ポートとして DNS over TCP を追加する場合は、宛先ポートとして Yahoo Messenger Voice Chat（TCP）を追加できますが、Yahoo Messenger Voice Chat（UDP）は追加できません。

送信元ポートのみ、あるいは宛先ポートのみを追加する場合は、異なるトランスポート プロトコルを使用するポートを追加できます。たとえば、DNS over TCP および DNS over UDP の両方を 1 つのアクセス コントロール ルールの送信元ポート条件として追加できます。

ポート条件を使用した非 TCP トラフィックの照合

非 TCP トラフィックを照合するためのポート条件を設定することはできますが、いくつかの制約事項があります。

- アクセス コントロール ルール：クラシック デバイスの場合、GRE でカプセル化されたトラフィックをアクセス コントロール ルールに照合するには、宛先ポート条件として GRE（47）プロトコルを使用します。GRE 制約ルールには、ネットワーク ベースの条件（ゾーン、IP アドレス、ポート、VLAN タグ）のみを追加できます。また、GRE 制約ルールが設定されたアクセス コントロール ポリシーでは、システムが外側のヘッダーを使用して**すべての**トラフィックを照合します。Firepower Threat Defense デバイスの場合、GRE でカプセル化されたトラフィックを制御するには、プレフィルタ ポリシーでトンネル ルールを使用します。
- SSL ルール：SSL ルールは TCP ポート条件のみをサポートします。

- ⚠

注意 SSL復号が無効の場合（つまりアクセスコントロールポリシーにSSLポリシーが含まれない場合）に、アクティブな最初の認証ルールを追加するか、アクティブな最後の認証ルールを削除すると設定の変更を展開する際にSnortプロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、ターゲットデバイスがトラフィックを処理する方法に応じて異なります。詳細はSnort® の再起動によるトラフィックの動作 （451 ページ）を参照してください。

アクティブ認証ルールには [アクティブ認証（Active Authentication）] ルール アクションが含まれているか、または **[パッシブまたはVPN IDを確立できない場合はアクティブ認証を使用する（Use active authentication if passive or VPN identity cannot be established）]** が選択された [パッシブ認証（Passive Authentication）] ルール アクションが含まれています。

- IMCP エコー：タイプ 0 が設定された宛先 ICMP ポート、またはタイプ 129 が設定された宛先 ICMPv6 ポートは、要求されていないエコー応答だけと照合されます。ICMP エコー要求への応答として送信されるICMPエコー応答は無視されます。ルールですべてのICMPエコーに一致させるには、ICMPタイプ8またはICMPv6タイプ128を使用してください。

ポート条件を使用したルール

次のルールは、ポート条件をサポートします。

- アクセス コントロール
- プレフィルタ
- SSL（TCP トラフィックのみをサポート）
- アイデンティティ（アクティブ認証は TCP トラフィックのみをサポート）
- QoS

ポート条件の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Access Admin/Network Admin

ステップ 1 ルール エディタで、[ポート（Ports）] タブをクリックします。

ステップ 2 [利用可能なポート（Available Ports）] リストから追加する定義済みポートを見つけて選択します。

ステップ 3 [送信元に追加（Add to Source）] または [宛先に追加（Add to Destination）] をクリックするか、またはドラッグ アンド ドロップします。

ステップ 4 手動で指定する送信元ポートまたは宛先ポートを追加します。

- [送信元（Source）]：プロトコルを選択し、0 から 65535 までのポートを 1 つ入力して [追加（Add）] をクリックします。
- [宛先（ICMP 以外）（Destination (non-ICMP)）]：プロトコルを選択または入力します。プロトコルを指定しない場合、または [TCP] か [UDP] を選択した場合は、0 から 65535 までのポートを 1 つ入力します。[追加（Add）] をクリックします。
- [宛先（ICMP）（Destination (ICMP)）]：[プロトコル（Protocol）] ドロップダウン リストから [ICMP] または [IPv6-ICMP] を選択し、表示されるポップアップ ウィンドウでタイプおよび関連するコードを選択します。ICMP タイプとコードの詳細については、Internet Assigned Numbers Authority（IANA）の Web サイトを参照してください。

ステップ 5 ルールを保存するか、編集を続けます。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

カプセル化の条件

カプセル化の条件は、トンネル ルールに固有です。

この条件では、カプセル化プロトコルによって特定のタイプのプレーンテキスト、パススルートンネルを制御します。ルールを保存する前に、一致するプロトコルを 1 つ以上選択する必要があります。次のオプションを選択できます。

- GRE（47）
- IP-in-IP（4）
- IPv6-in-IP（41）
- Teredo（UDP（17）/3455）

アプリケーション条件（アプリケーション制御）

システムは IP トラフィックを分析する際、ネットワークで一般的に使用されているアプリケーションを識別および分類できます。このディスカバリベースのアプリケーション認識は、アプリケーション制御、つまりアプリケーション トラフィック制御機能の基本です。

システム提供のアプリケーション フィルタは、アプリケーションの基本特性（タイプ、リスク、ビジネスとの関連性、カテゴリ、およびタグ）にしたがってアプリケーションを整理する

ことで、アプリケーション制御に役立ちます。システム提供のフィルタの組み合わせやアプリケーションの任意の組み合わせをもとに、ユーザ定義の再利用可能フィルタを作成できます。

ポリシーのアプリケーション ルール条件ごとに、少なくとも1つのディテクタが有効にされている必要があります。有効になっているディテクタがないアプリケーションについては、システム提供のすべてのディテクタが自動的に有効になります。ディテクタが存在しない場合は、そのアプリケーションについて最後に変更されたユーザ定義ディテクタが有効になります。アプリケーションディテクタの詳細については、アプリケーションディテクタの基本（2548ページ）を参照してください。

アプリケーション フィルタと個別に指定されたアプリケーションの両方を使用することで、完全なカバレッジを確保できます。ただし、アクセス コントロール ルールの順序を指定する前に、次の注意事項を確認してください。

アプリケーション制御の一部として、コンテンツ規制を適用するアクセス コントロール ルール（セーフ サーチや YouTube EDU など）を使用することもできます。

注意 アクセス コントロール ルールを適切に設定しないと、ブロックされるべきトラフィックが許可されるなど、予期しない結果が発生する可能性があります。一般的に、アプリケーション制御ルールは、たとえば IP アドレスに基づくルールよりも照合に時間がかかるため、アクセス コントロール リスト内の順位を低くする必要があります。

特定の条件（ネットワークや IP アドレスなど）を使用するアクセス コントロール ルールは、一般的な条件（アプリケーションなど）を使用するルールの前に順位付けする必要があります。オープン システム相互接続（OSI）モデルに精通している場合は、考え方として同様の順位付けを使用してください。レイヤ1、2、および3（物理、データリンク、およびネットワーク）の条件を持つルールは、アクセス コントロール ルールの最初に順位付けする必要があります。レイヤ5、6、および7（セッション、プレゼンテーション、およびアプリケーション）の条件は、アクセス コントロール ルールの後ろのほうに順序付けする必要があります。OSI モデルの詳細については、こちらの Wikipedia の記事を参照してください。

アプリケーション フィルタの利点

アプリケーション フィルタにより、迅速にアプリケーション制御を設定できます。たとえば、システム提供のフィルタを使って、リスクが高く、ビジネスとの関連性が低いアプリケーションをすべて認識してブロックするアクセス コントロール ルールを簡単に作成できます。ユーザがそれらのアプリケーションの1つを使用しようとすると、システムがセッションをブロックします。

アプリケーション フィルタを使用することで、ポリシーの作成と管理は簡単になります。この方法によりアプリケーション トラフィックが期待どおりに制御されます。シスコは、システムと脆弱性データベース（VDB）の更新を通して、頻繁にアプリケーション ディテクタを更新しています。このため、アプリケーション トラフィックは常に最新のディテクタによってモニタされます。また、独自のディテクタを作成し、どのような特性のアプリケーションを検出するかを割り当て、既存のフィルタを自動的に追加することもできます。

アプリケーション条件の設定

次の表に示す設定を行い、アプリケーション制御を実行します。この表には、設定する内容により、アプリケーション制御にどのような制約を設けることができるかも示します。

設定（Configuration）	タイプ、リスク、関連性、カテゴリ	タグ	ユーザ定義のフィルタ	コンテンツ規制
アクセス コントロール ルール	はい	はい	はい	はい
SSL ルール	Yes	No：SSL プロトコル タグによって、自動的に暗号化アプリケーション トラフィックに制約される	いいえ	いいえ
ID ルール（アクティブ認証からアプリケーションを免除）	Yes	No：ユーザ エージェント除外タグによって、自動的に制約される	いいえ	いいえ
QoS ルール	はい	はい	はい	いいえ（No）
オブジェクト マネージャ内のユーザ定義のアプリケーション フィルタ	はい	はい	No：ユーザ定義のフィルタのネストは不可	No
インテリジェント アプリケーション バイパス（IAB）	はい	はい	はい	いいえ（No）

関連トピック

概要：アプリケーション検出 （2547 ページ）

アプリケーション条件とフィルタの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	Control	いずれか（Any）	いずれか（Any）	Admin/Access Admin/Network Admin

アプリケーションの条件またはフィルタを作成するには、使用可能なアプリケーションのリストから、トラフィックを制御するアプリケーションを選択します。オプションとして（推奨）、フィルタを使用して使用可能なアプリケーションを抑制します。フィルタと個別に指定されたアプリケーションを同じ条件で使用できます。

始める前に

- アクセス コントロール ルールでアプリケーション制御を実行するためには、適応型プロファイルの設定（2466ページ）で説明されているように、アダプティブ プロファイルを有効（デフォルト状態）にする**必要があります**。

ステップ 1 ルール エディタまたは設定エディタを起動します。

- アクセス コントロール、SSL、QoS ルール条件：ルール エディタで [アプリケーション（Applications）] タブをクリックします。
- アイデンティティ ルール条件：ルール エディタで [レルムおよび設定（Realms & Settings）] タブをクリックし、アクティブ認証を有効にします。アイデンティティ ルールの作成（2638ページ）を参照してください。
- アプリケーション フィルタ：オブジェクト マネージャの [アプリケーション フィルタ（Application Filters）] ページで、アプリケーション フィルタを追加または編集します。フィルタの一意の**名前**を指定します。
- インテリジェント アプリケーション バイパス（IAB）：アクセス コントロール ポリシー エディタで [詳細（Advanced）] タブをクリックし、IAB の設定を編集して、[バイパス可能なアプリケーションおよびフィルタ（Bypassable Applications and Filters）] をクリックします。

ステップ 2 （オプション）セーフ サーチ（）または YouTube EDU（）のグレー表示のアイコンおよび設定関連のオプションをクリックして、アクセス コントロール ルールのコンテンツ制限機能を有効にします。

その他の設定要件については、アクセス コントロール ルールを使用したコンテンツ制限の実施（1795ページ）を参照してください。

たいていの場合、コンテンツ制限を有効にすると、条件の [Selected Applications and Filters] リストに適切な値が入力されます。コンテンツ制限を有効にするときに、コンテンツ制限に関係するアプリケーションまたはフィルタがすでにリスト内に存在している場合には、システムはリストに自動的に値を入力することはしません。

アプリケーションを絞り込んで選択内容をフィルタする手順を続行するか、またはスキップしてルールの保存に進みます。

ステップ 3 [使用可能なアプリケーション（Available Applications）] リストから追加するアプリケーションを見つけて選択します。

[使用可能なアプリケーション（Available Applications）] に表示されるアプリケーションを抑制するには、1 つ以上の**アプリケーション フィルタ**を選択するか、個別のアプリケーションを検索します。

ヒント サマリー情報とインターネットの検索リンクを表示するには、アプリケーションの横の情報アイコン（）をクリックします。ロック解除アイコン（）は、システムが復号されたトラフィックでのみ識別できるアプリケーションを示します。

フィルタを単独または組み合わせて選択すると、[使用可能なアプリケーション（Available Applications）] リストが更新され、条件を満たすアプリケーションのみが表示されます。システムによって提供されるフィルタは組み合わせて選択できますが、ユーザ定義フィルタはできません。

- 同じ特性（リスク、ビジネス関連性など）の複数のフィルタ：アプリケーション トラフィックは 1 つのフィルタのみに一致する必要があります。たとえば、中リスク フィルタと高リスク フィルタの両方を選択すると、[使用可能なアプリケーション（Available Applications）] リストにすべての中リスク アプリケーションと高リスク アプリケーションが表示されます。
- 異なるアプリケーション特性のフィルタ：アプリケーショントラフィックは、両方のフィルタ タイプに一致する必要があります。たとえば、高リスク フィルタとビジネスとの関連性が低いフィルタの両方を選択すると、[使用可能なアプリケーション（Available Applications）] リストに両方の条件を満たすアプリケーションのみが表示されます。

ステップ 4 [ルールに追加（Add to Rule）] をクリックするか、ドラッグ アンド ドロップします。

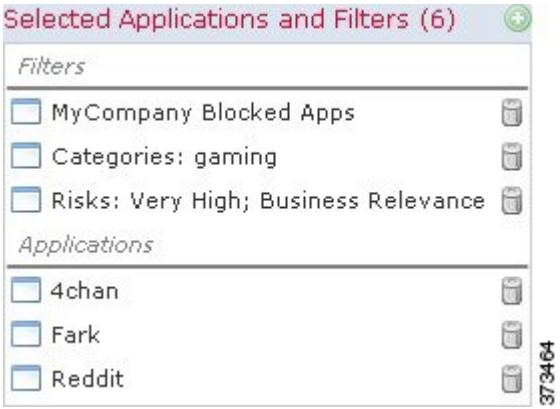
ヒント フィルタとアプリケーションをさらに追加する前に、[フィルタのクリア（Clear Filters）] をクリックして現在の選択をクリアします。

Webインターフェイスでは、条件に追加されたフィルタは上部にリストされ、個別に追加されたアプリケーションとは分けられます。

ステップ 5 ルールまたは設定を保存するか、編集を続けます。

例：アクセス コントロール ルールのアプリケーション条件

次の図は、MyCompany のユーザ定義アプリケーション フィルタ、リスクが高くビジネスとの関連性が低いすべてのアプリケーション、ゲーム アプリケーション、および個々に選択されたいくつかのアプリケーションをブロックするアクセス コントロール ルールのアプリケーション条件を示しています。



次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

アプリケーションの特性

システムは、次の表に示す基準を使用して、検出された各アプリケーションの特性を判別します。これらの特性をアプリケーション フィルタとして使用します。

表 *61* : アプリケーションの特性

特性	説明	例
タイプ（Type）	アプリケーションプロトコルは、ホスト間の通信を意味します。 クライアントは、ホスト上で動作しているソフトウェアを意味します。 Web アプリケーションは、HTTP トラフィックの内容または要求されたURLを意味します。	HTTP と SSH はアプリケーションプロトコルです。 Web ブラウザと電子メール クライアントはクライアントです。 MPEG ビデオと Facebook は Web アプリケーションです。
リスク（Risk）	アプリケーションが組織のセキュリティ ポリシーに違反することがある目的で使用される可能性。	ピアツーピア アプリケーションはリスクが極めて高いと見なされます。
ビジネスとの関連性（Business Relevance）	アプリケーションが、娯楽目的ではなく、組織のビジネス活動の範囲内で使用される可能性。	ゲーム アプリケーションはビジネスとの関連性が極めて低いと見なされます。
カテゴリ	アプリケーションの最も不可欠な機能を表す一般的な分類。各アプリケーションは、少なくとも 1 つのカテゴリに属します。	Facebook はソーシャル ネットワーキングのカテゴリに含まれます。
タグ	アプリケーションに関する追加情報。アプリケーションには任意の数（0 を含む）のタグを付けることができます。	ビデオ ストリーミング Web アプリケーションには、ほとんどの場合、`high bandwidth` と `displays ads` というタグが付けられます。

アプリケーション制御のガイドラインと制限事項

アダプティブ プロファイルが有効になっていることの確認

アダプティブ プロファイルが無効な場合（デフォルト状態）、アクセス制御ルールは、アプリケーション制御を実行できません。

アプリケーション ディテクタの自動有効化

ディテクタが検出対象のアプリケーションに対して有効でない場合、システムは、そのアプリケーションに対応するシステム提供のすべてのディテクタを自動的に有効にします。存在しな

い場合、システムはそのアプリケーション対応で最近変更されたユーザ定義のディテクタを有効にします。

アプリケーション識別の速度

システムは、次の両方の条件が満たされるまで、インテリジェント アプリケーション バイパス（IAB）およびレート制限を含むアプリケーション制御を実行できません。

- モニタ対象の接続がクライアントとサーバの間で確立される。
- システムがセッションでアプリケーションを識別する

この識別は 3 ～ 5 パケット以内で、またはトラフィックが暗号化されている場合は、SSL ハンドシェイクのサーバ証明書交換の後に行われる必要があります。

早期のトラフィックがその他のすべての基準に一致するが、アプリケーション識別が不完全な場合、システムは、パケットの受け渡しと接続の確立（または、SSL ハンドシェイクの完了）を許可します。システムは識別を完了した後、残りのセッション トラフィックに適切なアクションを適用します。

アクセス コントロールの場合、これらの受け渡されたパケットは、アクセス コントロール ポリシーのデフォルトの侵入ポリシー（デフォルト アクション侵入ポリシーでもほぼ一致するルールの侵入ポリシーでもない）によりインスペクションが実行されます。

アプリケーション コントロール ルールの順位付けに関するガイドラインについては、アプリケーション制御に関する推奨事項 （1691 ページ）を参照してください。

アプリケーションや他のルールより前に配置される URL ルール

URL マッチングを最も効果的に行うには、URL 条件を含むルールを他のルールより前に配置します。特に、URL ルールがブロック ルールで、他のルールが次の条件を両方とも満たす場合には、URL 条件を含むルールを前に配置します。

- その他のルールがアプリケーション条件を含んでいる。
- 検査対象のトラフィックが暗号化されている。

暗号化および復号トラフィックのアプリケーション制御

システムは暗号化トラフィックと復号トラフィックを識別し、フィルタ処理することができます。

- 暗号化トラフィック：システムは、SMTPS、POPS、FTPS、TelnetS、IMAPS を含む StartTLS で暗号化されたアプリケーション トラフィックを検出できます。さらに、TLS ClientHello メッセージの Server Name Indication、またはサーバ証明書のサブジェクト識別名の値に基づいて、特定の暗号化されたアプリケーションを識別できます。これらのアプリケーションに `SSL Protocol` タグが付けられます。SSL ルールでは、これらのアプリケーションのみを選択できます。このタグがないアプリケーションは、暗号化されていないまたは復号されたトラフィックでのみ検出できます。

- 復号トラフィック：システムは、復号されたトラフィック（暗号化されたまたは暗号化されていないトラフィックではなく）のみで検出を行うことができるアプリケーションに `decrypted traffic` タグを割り当てます。

アプリケーションのアクティブ認証の免除

アイデンティティ ポリシーでは、特定のアプリケーションのアクティブ認証を免除し、トラフィックにアクセス コントロールの続行を許可できます。これらのアプリケーションには、`User-Agent Exclusion` タグが付けられます。アイデンティティ ルールでは、これらのアプリケーションのみを選択できます。

ペイロードのないアプリケーション トラフィック パケットの処理

アクセス コントロールを実行している場合、システムは、アプリケーションが識別された接続内にペイロードがないパケットに対してデフォルト ポリシー アクションを適用します。

参照されるアプリケーション トラフィックの処理

アドバタイズメント トラフィックなどの Web サーバによって参照されるトラフィックを処理するには、参照しているアプリケーションではなく、参照されるアプリケーションを照合します。

複数のプロトコルを使用するアプリケーション トラフィックの制御（Skype、Zoho）

一部のアプリケーションは、複数のプロトコルを使用します。このようなアプリケーションのトラフィックを制御するには、関連するすべてのオプションがアクセス コントロール ポリシーの対象となっていることを確認します。次に例を示します。

- Skype：Skype のトラフィックを制御するには、個々のアプリケーションを選択するのではなく、[アプリケーション フィルタ（Application Filters）] リストから [Skype] タグを選択します。これにより、システムは同じ方法で Skype のすべてのトラフィックを検出して制御できるようになります。
- Zoho：Zoho メールを制御するには、[使用可能なアプリケーション（Available Application）] リストから [Zoho] と [Zohoメール（Zoho mail）] の両方を選択します。

コンテンツ制限機能用にサポートされる検索エンジン

システムは、特定の検索エンジンの場合のみ、セーフ サーチ フィルタリングをサポートします。システムは、これらの検索エンジンからのアプリケーション トラフィックに `safesearch supported` タグを割り当てます。

回避的アプリケーション トラフィックの制御

用途別の注意事項と制限事項 （487 ページ）を参照してください。

関連トピック

デフォルトの侵入ポリシー （2287 ページ）

アプリケーション検出に関する特別な考慮事項 （2552 ページ）

用途別の注意事項と制限事項

- Office 365 管理者用ポータル：

  制限：アクセスポリシーのロギングが最初と最後で有効になっている場合、最初のパケットは Office 365 として検出され、接続の終了は Office 365 管理者用ポータルとして検出されます。これがブロッキングに影響を与えないようにする必要があります。

- Skype:

  アプリケーション制御のガイドラインと制限事項 （484 ページ）を参照してください

- GoToMeeting

  GoToMeeting を完全に検出するには、ルールに次のすべてのアプリケーションが含まれている必要があります。

  - GoToMeeting
  - Citrix Online
  - Citrix GoToMeeting プラットフォーム
  - LogMeIn
  - STUN

- Zoho:

  アプリケーション制御のガイドラインと制限事項 （484 ページ）を参照してください

- Bittorrent、Tor、Psiphon、および Ultrasurf などの回避的なアプリケーションの場合：

  回避的なアプリケーションの場合、デフォルトでは、信頼性の高いシナリオのみが検出されます。このトラフィックに対するアクション（ブロックや QoS の実装など）を実行する必要がある場合、より効果の高い、さらに積極的な検出の設定が必要なことがあります。これを実行する場合、設定の変更によって誤検出が発生する可能性がありますので、TAC に問い合わせて設定を確認してください。

アプリケーション制御ルールのトラブルシューティング

アプリケーション コントロール ルールが予想どおりに機能しない場合は、このセクションで説明されているガイドラインを確認してください。

アプリケーションによるネットワークへのアクセスを次のように制御することをお勧めします。

- 安全性の低いネットワークからより安全なネットワークへのアプリケーションアクセスを許可またはブロックするには、アクセス コントロール ルールで [ポート（Port）]（[選択した宛先ポート（Selected Destination Port）]）条件を使用します。

たとえば、インターネット（安全性が低い）から内部ネットワーク（安全性が高い）への ICMP トラフィックを許可します。

- ユーザ グループによるアプリケーションへのアクセスを許可またはブロックするには、アクセス コントロール ルールで [アプリケーション（Application）] 条件を使用します。

  たとえば、契約業者グループのメンバーによる Facebook へのアクセスをブロックします。

注意 アクセス コントロール ルールを適切に設定しないと、ブロックされるべきトラフィックが許可されるなど、予期しない結果が発生する可能性があります。一般的に、アプリケーション制御ルールは、たとえば IP アドレスに基づくルールよりも照合に時間がかかるため、アクセス コントロール リスト内の順位を低くする必要があります。

特定の条件（ネットワークや IP アドレスなど）を使用するアクセス コントロール ルールは、一般的な条件（アプリケーションなど）を使用するルールの前に順位付けする必要があります。オープン システム相互接続（OSI）モデルに精通している場合は、考え方として同様の順位付けを使用してください。レイヤ 1、2、および 3（物理、データリンク、およびネットワーク）の条件を持つルールは、アクセス コントロール ルールの最初に順位付けする必要があります。レイヤ 5、6、および 7（セッション、プレゼンテーション、およびアプリケーション）の条件は、アクセス コントロール ルールの後ろのほうに順序付けする必要があります。OSI モデルの詳細については、こちらの Wikipedia の記事を参照してください。

次の表に、アクセス コントロール ルールを設定する方法の例を示します。

コントロールの種類	操作	ゾーン、ネットワーク、VLAN タグ	Users	アプリケーション	ポート	URL	SGT/ISE 属性	インスペクション、ロギング、コメント
アプリケーションがポート（SSH など）を使用する場合の、安全性の高いネットワークから安全性の低いネットワークへのアプリケーション	お客様の選択（この例では [許可（Allow）]）	外部インターフェイスを使用する宛先ゾーンまたはネットワーク	任意（Any）	設定しない	使用可能なポート：**SSH** [選択した宛先ポート（Selected Destination Port）] に追加	任意（Any）	ISE/ISE-PIC でのみ使用。	任意（Any）

コントロールの種類	操作	ゾーン、ネットワーク、VLAN タグ	Users	アプリケーション	ポート	URL	SGT/ISE 属性	インスペクション、ロギング、コメント
アプリケーションがポートを使用していない場合の（ICMP など）、安全性の高いネットワークから安全性の低いネットワークへのアプリケーション	お客様の選択（この例では [許可（Allow）]）	外部インターフェイスを使用する宛先ゾーンまたはネットワーク	任意（Any）	設定しない	選択された宛先ポート プロトコル：**ICMP** タイプ：**Any**	設定しない	ISE/ISE-PIC でのみ使用。	任意（Any）
ユーザ グループによるアプリケーション アクセス	お客様の選択（この例では [ブロック（Block）]）	お客様の選択	ユーザグループ（この例では契約業者グループ）を選択。	アプリケーションの名前（この例では [Facebook]）を選択。	設定しない	設定しない	ISE/ISE-PIC でのみ使用。	お客様の選択

関連トピック

ルールの順序指定のガイドライン （503 ページ）

URL 条件（URL フィルタリング）

URL 条件を使用してネットワークのユーザがアクセスできる Web サイトを制御します。

詳細については、URL Filtering （1717 ページ）を参照してください。

ユーザ条件、レルム条件、および ISE 属性条件（ユーザ制御）

Firepower システムによって収集された権限のあるユーザ アイデンティティ データを使用してユーザ制御を実行することができます。

アイデンティティ ソースはユーザがログインまたはログアウトする際、または Microsoft Active Directory（AD）または LDAP のクレデンシャルを使用して認証する際にユーザをモニタします。次に、この収集されたアイデンティティ データを使用して、モニタ対象ホストに関連付けられているログインしている権限のあるユーザに基づいてトラフィックを処理するルールを設定できます。ユーザは、そのユーザがログオフする（アイデンティティ ソースによって報告される）か、レルムがセッションをタイムアウトするか、システムのデータベースからそのユーザ データが削除されるまで、ホストに関連付けられたままになります。

Firepower システムのご使用のバージョンでサポートされる権限のあるユーザ アイデンティティ ソースについては、ユーザ アイデンティティ ソースについて（2482 ページ）を参照してください。

ユーザ制御を実行するために、次のルール条件を使用できます。

- ユーザ条件およびレルム条件：ホストのログインしている権限のあるユーザに基づいてトラフィックを照合します。トラフィックは、レルム、個々のユーザ、またはそれらのユーザが属しているグループに基づいて制御できます。
- ISE 属性条件：ユーザの、ISE が割り当てたセキュリティ グループ タグ（SGT）、デバイス タイプ（エンドポイント プロファイルとも呼ばれる）、またはロケーション IP（エンドポイント ロケーションとも呼ばれる）に基づいてトラフィックを照合します。ISE をアイデンティティ ソースとして設定する必要があります。

（注） ISE-PIC アイデンティティ ソースでは、ISE 属性データを提供しません。

（注） 一部のルールでは、カスタム SGT 条件が ISE によって割り当てられ**なかった** SGT 属性にタグ付けされたトラフィックを照合できます。これはユーザ制御とはみなされず、ISE をアイデンティティ ソースとして使用していない場合にのみ機能します。カスタム SGT 条件 （495 ページ）を参照してください。

ユーザ条件を持つルール

ルール タイプ	ユーザ条件およびレルム条件のサポート	ISE 属性条件のサポート
アクセス コントロール	はい	はい

ルール タイプ	ユーザ条件およびレルム条件のサポート	ISE 属性条件のサポート
SSL	はい	いいえ（No）
QoS	はい	はい

関連トピック

ユーザ エージェントのアイデンティティ ソース （2633 ページ）
ISE/ISE-PIC アイデンティティ ソース （2593 ページ）
ターミナル サービス（TS）エージェントのアイデンティティ ソース （2629 ページ）
キャプティブ ポータルのアイデンティティ ソース （2607 ページ）

ユーザ制御の前提条件

アイデンティティ ソース/認証方式の設定

実行する認証タイプのアイデンティティ ソースを設定します。詳細については、ユーザ アイデンティティ ソースについて （2482 ページ）を参照してください。

ユーザ エージェント、TS エージェント、または ISE/ISE-PIC デバイスのモニタ対象に多くのユーザ グループを設定した場合、またはネットワークでホストにマップされるユーザ数が非常に多い場合、Firepower Management Center のユーザ制限が原因で、システムがグループに基づいてユーザ マッピングをドロップすることがあります。その結果、レルム、ユーザ、またはユーザ グループの条件のルールが、一致することが想定されているトラフィックと一致しなくなる可能性があります。

レルムの設定

監視対象の各 AD または LDAP サーバ（ISE/ISE-PIC、ユーザ エージェント、および TS エージェント サーバを含む）のレルムを設定し、ユーザのダウンロードを実行します。詳細については、レルムの作成 （2576 ページ）を参照してください。

（注） ISE SGT 属性ルール条件を設定する場合、レルムの設定は任意です。ISE SGT 属性ルール条件は、アイデンティティ ポリシー（レルムの呼び出し元）が関連付けられているかどうかにかかわらず、ポリシー内で設定できます。

レルムを設定するときには、アクティビティを監視するユーザおよびユーザ グループを指定します。ユーザ グループを含めると、自動的に、すべてのセカンダリ グループのメンバーを含む、そのグループのすべてのメンバーが含まれます。ただし、セカンダリ グループをルール条件として使用する場合は、セカンダリ グループをレルム構成に明示的に含める必要があります。

レルムごとに、ユーザデータの自動ダウンロードを有効にすると、ユーザおよびユーザ グループの信頼できるデータを更新することができます。

アイデンティティ ポリシーの作成

レルムを認証方式に関連付けるアイデンティティポリシーを作成し、そのポリシーをアクセス制御に関連付けます。詳細については、アイデンティティポリシーの作成（2643ページ）を参照してください。

デバイスのユーザ制御（アクセス制御、SSL、QoS）を実行するポリシーは、アイデンティティポリシーを共有します。そのアイデンティティポリシーによって、それらのデバイス上のトラフィックに影響するルールで使用できるレルム、ユーザ、およびグループが決まります。

QoSルールでユーザ条件を設定する前に、QoSポリシーの対象となるデバイスが、デバイスに適用されたアクセス制御ポリシーで定義されている正しいアイデンティティポリシーを使用していることを確認する**必要があります**。同じデバイスに適用されたQoSポリシーとアクセス制御ポリシーは明示的にリンクされていないため、QoSルールエディタで無効なレルム、ユーザ、およびグループを選択することが可能です。これらの無効な要素は、Firepower Management Centerに存在するが、QoS対象のデバイスには適用されないアイデンティティポリシーから取得された要素です。これらの要素を使用すると、実際に適用されるまで、無効な選択をしたことが判別されません。

ユーザおよびレルム条件の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	Control	いずれか（Any）	いずれか（Any）	Admin/Access Admin/Network Admin

レルム、またはそのレルム内のユーザとユーザ グループでルールを制約できます。

始める前に

- ユーザ条件、レルム条件、およびISE属性条件（ユーザ制御）（490ページ）で説明されているユーザ制御の前提条件を満たしてください。

ステップ1 ルール エディタで、[ユーザ（Users）] タブをクリックします。

ステップ2 （オプション）[利用可能なレルム（Available Realms）] リストから使用するレルムを見つけて選択します。

ステップ3 （オプション）[有効なユーザ（Available Users）] リストからユーザとグループを選択して、ルールをさらに制約します。

ステップ4 [Add to Rule] をクリックするか、ドラッグ アンド ドロップします。

ステップ5 ルールを保存するか、編集を続けます。

次のタスク

- 設定変更を展開します。設定変更の展開（447ページ）を参照してください。

ISE 属性条件の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	Control	いずれか（Any）	いずれか（Any）	Admin/Access Admin/Network Admin

始める前に

- ユーザ条件、レルム条件、および ISE 属性条件（ユーザ制御） （490 ページ）に記載されているユーザ制御の前提条件を満たします。

ステップ 1 ルール エディタで、ISE 属性条件のタブをクリックします。

- アクセス コントロール：[SGT/ISE 属性（SGT/ISE Attributes）] タブをクリックします。
- QoS：[ISE 属性（ISE Attributes）] タブをクリックします。

ISE 属性条件を制約するために、ISE 割り当てセキュリティ グループ タグ（SGT）を使用できます。アクセス コントロール ルールでカスタム SGT を使用するには、カスタム SGT 条件 （495 ページ）を参照してください。

ステップ 2 [使用可能な属性（Available Attributes）] リストから、使用する ISE 属性を見つけて選択します。

- [セキュリティ グループ タグ（SGT）（Security Group Tag (SGT)）]
- [デバイス タイプ（Device Type）]（エンドポイント プロファイルとも呼ばれます）
- [ロケーション IP（Location IP）]（エンドポイント ロケーションとも呼ばれます）

ステップ 3 [使用可能な ISE メタデータ（AvailableISE Metadata）] [使用可能なメタデータ（Available Metadata）] リストから属性メタデータを選択して、さらにルールを制約します。または、デフォルトの [すべて（any）] のままにします。

ステップ 4 [ルールに追加（Add to Rule）] をクリックするか、ドラッグ アンド ドロップします。

ステップ 5 （オプション）[ロケーション IP アドレスの追加（Add a Location IP Address）] フィールドで、IP アドレスによりルールを制約し、[追加（Add）] をクリックします。

システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。

ステップ 6 ルールを保存するか、編集を続けます。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

ユーザ制御のトラブルシューティング

ユーザ ルールの予期しない動作に気付いたら、ルール、アイデンティティ ソース、またはレルムの設定を調整することを検討してください。その他の関連するトラブルシューティング情報については、以下を参照してください。

- ユーザ エージェント アイデンティティ ソースのトラブルシューティング （2634 ページ）
- ISE/ISE-PIC アイデンティティ ソースのトラブルシューティング （2604 ページ）
- TS エージェント アイデンティティ ソースのトラブルシューティング （2631 ページ）
- キャプティブ ポータルのアイデンティティ ソースのトラブルシューティング （2620 ページ）
- レルムとユーザのダウンロードのトラブルシュート （2586 ページ）

レルム、ユーザ、またはユーザ グループを対象とするルールがトラフィックと一致しない

ユーザ エージェント、TS エージェント、または ISE/ISE-PIC デバイスのモニタ対象に多くのユーザ グループを設定した場合、またはネットワークでホストにマップされるユーザ数が非常に多い場合、Firepower Management Center のユーザ制限が原因で、システムがユーザ レコードをドロップすることがあります。その結果、ユーザ条件のルールが、一致することが想定されているトラフィックと一致しない可能性があります。

ユーザ グループまたはユーザ グループ内のユーザを対象とするルールが、一致することが想定されているトラフィックと一致しない

ユーザ グループ条件を含むルールを設定する場合は、LDAP または Active Directory サーバでユーザ グループを設定している必要があります。サーバが基本的なオブジェクト階層でユーザを整理している場合、システムはユーザ グループ制御を実行できません。

セカンダリ グループ内のユーザを対象とするルールが、一致することが想定されているトラフィックと一致しない

Active Directory サーバのセカンダリ グループのメンバーであるユーザを含めるか除外するユーザ グループ条件を含むルールを設定する場合、サーバは報告するユーザの数を制限していることがあります。

デフォルトでは、Active Directory サーバはセカンダリ グループから報告するユーザの数を制限します。この制限は、セカンダリ グループ内のすべてのユーザが Firepower Management Center に報告され、ユーザ条件を含むルールでの使用に適するようにカスタマイズする必要があります。

ルールが、初めて表示されたユーザと一致しない

システムは、以前に表示されていないユーザからのアクティビティを検出すると、サーバからそれらのユーザに関する情報を取得します。システムがこの情報を正常に取得するまで、このユーザに表示されるアクティビティは、一致するルールによって処理されません。代わりに、

ユーザ セッションが、一致する次のルール（または該当する場合はポリシーのデフォルト アクション）によって処理されます。

たとえば、次のような状況が考えられます。

- ユーザ グループのメンバーであるユーザが、ユーザ グループ条件を含むルールに一致しない。
- ユーザ データの取得に使用されたサーバが Active Directory サーバである場合、ユーザ エージェント、TS エージェント、または ISE/ISE-PIC デバイスによって報告されたユーザがルールと一致しない。

これにより、システムがユーザ データをイベント ビューおよび分析ツールに表示するのが遅れる可能性があることに注意してください。

ルールがすべての ISE ユーザと一致しない

これは想定されている動作です。Active Directory ドメイン コントローラで認証された ISE ユーザに対してユーザ制御を実行することができます。LDAP、RADIUS、または RSA ドメイン コントローラで認証された ISE ユーザに対するユーザ制御は実行できません。

ルールがすべての ISE/ISE-PIC ユーザと一致しない

これは想定されている動作です。Active Directory ドメイン コントローラで認証された ISE/ISE-PIC ユーザに対してユーザ制御を実行することができます。LDAP、RADIUS、または RSA ドメイン コントローラで認証された ISE/ISE-PIC ユーザに対するユーザ制御は実行できません。

ユーザとグループによる大量のメモリの使用

ユーザとグループの処理によって大量のメモリが使用されている場合、**/var/log/messages** に次のようなメッセージが表示されます。

```
UserGroup [WARN] User/Group mem usage is above 80 percent
```

別のメッセージには、ユーザとグループによって使用されているメモリのパーセンテージが表示されます。

こうしたメッセージの表示が続く場合には、次のオプションのいずれかを実行できます。

- アクセス コントロール ポリシーによって処理されるユーザを制限します。
- 管理対象デバイスをメモリが大きなモデルにアップグレードします。

カスタム SGT 条件

ID ソースとして ISE/ISE-PIC を設定しない場合、ISE によって指定**されていない**セキュリティ グループ タグ（SGT）使用してトラフィックを制御できます。SGT は、信頼ネットワーク内での、トラフィックの送信元の権限を指定します。

カスタム SGT ルールの条件では、システムが ISE サーバとの接続によって取得した ISE SGT ではなく、手動で作成された SGT オブジェクトを使ってトラフィックをフィルタ処理します。

この手動で作成された SGT オブジェクトは、制御するトラフィックの SGT 属性に対応します。カスタム SGT を使用したトラフィック制御は、ユーザ制御とは見なされません。

カスタム SGT 条件を持つルール

次のルールがカスタム SGT 条件をサポートしています。

- アクセス コントロール
- QoS

ISE SGT とカスタム SGT ルール条件との比較

ルールの中には、割り当てられた SGT に基づいてトラフィックを制御するために使用できるものがあります。ルールのタイプ、およびアイデンティティ ソースの設定によって、ISE 割り当ての SGT またはカスタム SGT のいずれかを使用して、トラフィックを割り当て済み SGT 属性と照合することができます。

（注） ISE SGT を使用してトラフィックを照合する場合、パケットに SGT 属性が割り当てられていないとしても、パケットの送信元 IP アドレスが ISE 内で既知であれば、そのパケットは ISE SGT ルールと照合されます。

条件タイプ	要件	ルール エディタにリストされている SGT
ISE SGT	ISE アイデンティティ ソース	ISE サーバをクエリして取得され、メタデータが自動的に更新される SGT
カスタム SGT	ISE/ISE-PIC アイデンティティ ソースなし	ユーザが作成するスタティック SGT オブジェクト

関連トピック

ユーザ条件、レルム条件、および ISE 属性条件（ユーザ制御） （490 ページ）

カスタムセキュリティグループタグ（SGT）からISEセキュリティグループタグ（SGT）への自動遷移

カスタム SGT に一致するルールを作成し、ISE/ISE-PIC を ID ソースに設定すると、システムは次の動作をします。

- オブジェクト マネージャの [セキュリティ グループ タグ（Security Group Tag）] オプションを無効にします。システムは既存の SGT オブジェクトをそのまま保持しますが、それらの変更や、新しいオブジェクトの追加はできません。
- カスタム SGT 条件の既存のルールを保持します。ただし、これらのルールはトラフィックの照合を行いません。また、既存のルールにカスタム SGT 基準を追加することや、カスタム SGT 条件を含む新しいルールを作成することはできません。

ISE を設定する場合は、カスタム SGT 条件を含む既存のルールは削除するか、無効にすることを推奨します。SGT 属性を持つトラフィックを照合するには、代わりに ISE 属性条件を使用します。

関連トピック

ユーザ制御用 ISE/ISE-PIC の設定 （2601 ページ）

カスタム SGT 条件の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	Control	いずれか（Any）	いずれか（Any）	Admin/Access Admin/Network Admin

次の手順では、ISE によって割り当てられて**いない** SGT 属性がタグ付けされたトラフィックをフィルタ処理する方法を説明します。これはユーザ制御とみなされず、アイデンティティ ソースとして ISE/ISE-PIC を使用しない場合にのみ機能します。ISE SGT とカスタム SGT ルール条件との比較 （496 ページ）を参照してください。

始める前に

- ISE/ISE-PIC 接続を無効にします。カスタム SGT の照合は、アイデンティティ ソースとして ISE/ISE-PIC を使用する場合、機能しません。
- 一致させる SGT に対応するセキュリティ グループ タグ オブジェクトを設定します。セキュリティ グループ タグ オブジェクトの作成 （532 ページ）を参照してください。

ステップ 1 ルール エディタで、[SGT/ISE 属性（SGT/ISE Attributes）] タブをクリックします。

ステップ 2 [Available Attributes] リストから [Security Group Tag] を選択します。

ステップ 3 [Available Metadata] リストで、カスタム SGT オブジェクトを見つけて選択します。

[すべて（Any）] を選択すると、ルールは SGT 属性があるすべてのトラフィックと一致します。たとえば、この値は、TrustSec 向けに構成されていないホストからのトラフィックをブロックするアクセス コントロール ルールが必要な場合に選択できます。

ステップ 4 [Add to Rule] をクリックするか、ドラッグ アンド ドロップします。

ステップ 5 ルールを保存するか、編集を続けます。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

カスタム SGT 条件のトラブルシューティング

予期しないルールの動作に気付いたら、カスタム SGT オブジェクトの設定を調整することを検討してください。

使用不可のセキュリティ グループ タグ オブジェクト

カスタム SGT オブジェクトは、ISE/ISE-PIC をアイデンティティ ソースとして設定していない場合にのみ使用できます。詳細については、「カスタム セキュリティ グループ タグ（SGT）から ISE セキュリティ グループ タグ（SGT）への自動遷移（496 ページ）」を参照してください。

ルールの検索

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Access Admin/Network Admin

多くのポリシーでは、ルールとルール内の検索が可能です。システムは、入力内容をルールの名前および条件値と照合します。これには、オブジェクトとオブジェクト グループが含まれます。

セキュリティ インテリジェンスまたは URL のリストまたはフィードに含まれる値は検索できません。

ステップ 1 ポリシー エディタで、[ルール（Rules）] タブをクリックします。

ステップ 2 [ルールの検索（Search Rules）] プロンプトをクリックし、検索文字列のすべてまたは一部を入力してから Enter キーを押します。
照合ルールごとに、一致する値のカラムが強調表示されます。ステータス メッセージには、現行の一致および合計一致数が表示されます。

ステップ 3 目的のルールを見つけます。

照合ルールの間を移動する場合は、次の一致アイコン（▼）または前の一致アイコン（▲）をクリックします。

次のタスク

- 新しい検索を開始する前に、クリア アイコン（✖）をクリックして、検索と強調表示をクリアします。

デバイス別のフィルタリング ルール

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	機能に応じて異なる	いずれか（Any）	Admin/Access Admin/Network Admin

一部のポリシーエディタでは、該当デバイスによってルールの表示をフィルタ処理することができます。

システムは、ルールがそのデバイスに影響するかどうかを判断するために、ルールのインターフェイス制約を使用します。インターフェイス（セキュリティゾーンまたはインターフェイスグループの条件）でルールを制約すると、インターフェイスが置かれている場所のデバイスがそのルールの影響を受けます。インターフェイス制約のないルールは、すべてのインターフェイスに適用されるので、すべてのデバイスに適用されることになります。

QoS ルールは、常にインターフェイスで制約されます。

ステップ 1 ポリシーエディタで、[ルール（Rules）] タブをクリックし、[デバイスでフィルタ処理（Filter by Device）] をクリックします。
ターゲット デバイスとデバイス グループのリストが表示されます。

ステップ 2 1 つまたは複数のチェック ボックスをオンにして、これらのデバイスまたはグループに適用されるルールだけを表示します。または、[すべて（All）] をオンにしてリセットし、すべてのルールを表示します。

ヒント ポインタをルール基準に合わせると、その値が表示されます。基準がデバイス特有のオーバーライドを持つオブジェクトを表し、そのデバイスだけでルール リストをフィルタ処理する場合、システムはオーバーライド値を表示します。基準がドメイン特有のオーバーライドを持つオブジェクトを表し、そのドメインのデバイスでルール リストをフィルタ処理する場合、システムはオーバーライド値を表示します。

ステップ 3 [OK] をクリックします。

関連トピック

アクセス コントロール ルールの作成および編集 （1698 ページ）
プレフィルタリングの設定 （1772 ページ）
QoS ルールの設定 （867 ページ）
脅威に対する防御のための NAT の設定 （1466 ページ）

Identify Rules with Issues

展開を防ぐルール（赤色のアイコンでマーく）か、または別のルールがルールの順序で上にあるためにトラフィックが一致することがないルール（黄色のアイコンでマーク）のそれぞれに、システムはフラグを設定します。

重要 他のルールに部分的に一致するルールにはフラグが付けられないため、後続の一部のルールが一致しない場合もあります。

ステップ 1 [ポリシー（Policies）] > [アクセス制御（Access Control）] > [アクセス制御（Access Control）] を選択します。

ステップ 2 ポリシー名をクリックします。

ステップ 3 次のいずれかまたは両方を実行します。

- ウィンドウの上部近くで [警告の表示（Show Warnings）] を探します。

  システムで問題が特定されていない場合、このボタンは表示されません。

  問題がある場合は、このボタンをクリックして問題があるすべてのルールのリストを開きます。

  すべての問題を表示するには、両方のタブ ([ルール エラー（Rule Errors）] と [ルールの警告（Rule Warnings）]) をクリックします。

  下にあるルールのテーブル内からルールを見つけるには、[エラー（Error）] または [警告（Warning）] リストでルール名をクリックします。

- [ルール競合の表示（Show Rule Conflicts）] チェックボックスをオンにします。

  これにより、リスト内で問題があるルールがエラー（赤色）または警告（黄色）のアイコンで示されます。

  必要に応じて、ポリシー内のすべてのルールを確認するまで下にスクロールします。

ステップ 4 問題の詳細を表示するには、アイコンの上にポインタを置きます。

ステップ 5 部分一致のみであるためフラグが付けられていない重複を検索して対処します。

ステップ 6 変更した場合は、[保存（Save）] をクリックするか、または [ルール競合の表示（Show Rule Conflicts）] をいったんオフにしてからもう一度オンにし、変更したルールに競合がないかを評価します。

次のタスク

- 問題があるルールを削除または変更し、問題に対処します。
- SSL ポリシーおよび QoS ポリシーで同様のエラーや警告を調べ、問題に対処しあす。

ルールとその他のポリシーの警告

ポリシーおよびルールエディタでは、トラフィックの分析やフローに悪影響を与える可能性のある設定をアイコンで示します。問題に応じて、システムはユーザがそのようなポリシーを展開しようとするときに警告するか、導入を完全に阻止します。

ヒント　警告、エラー、または情報のテキストを確認するには、マウスのポインタをアイコンの上に置きます。

表 *62 :* ポリシーのエラー アイコン

アイコン	説明	例
error	ルールまたは設定にエラーがある場合、影響を受けるルールを無効にしても、問題を修正するまではポリシーを展開できません。	カテゴリおよびレピュテーション ベースのURLフィルタリングを実行するルールは、URLフィルタリング ライセンスのないデバイスをターゲットにする時点まで有効です。その時点で、ルールの横にエラー アイコンが表示され、ポリシーを展開できなくなります。ポリシーを展開するには、このルールを編集または削除するか、ポリシーのターゲットを変更するか、URLフィルタリング ライセンスを有効にする必要があります。
警告	ルールに関する警告またはその他の警告が表示されていても、ポリシーを展開することはできます。しかし、警告でマークされている誤った設定は有効になりません。 警告が出されているルールを無効にすると、警告アイコンが消えます。潜在する問題を修正せずにルールを有効にすると、警告アイコンが再表示されます。	プリエンプトされるルール、または誤った設定によりトラフィックを照合できないルールは有効になりません。誤った設定には、空のオブジェクト グループ、一致するアプリケーションがないアプリケーション フィルタ、除外されたLDAPユーザ、無効なポートなどを使用した条件が含まれます。 一方、警告アイコンがライセンス エラーまたはモデルの不一致を示している場合は、問題を修正するまでそのポリシーを展開することはできません。

アイコン	説明	例
情報	情報アイコンは、トラフィックのフローに影響する可能性がある設定に関する有用な情報を伝送します。これらの問題によってポリシーの展開が阻止されることはありません。	アプリケーション制御が適用されている場合、システムは接続でアプリケーショントラフィックまたは Web トラフィックを識別するまで、その接続の最初の数パケットと一部のルールとの照合をスキップすることがあります。これにより、アプリケーションと HTTP 要求が識別されるように接続が確立されます。

関連トピック

アプリケーション制御のガイドラインと制限事項 （484 ページ）
URL フィルタリングのガイドラインと制限事項 （1719 ページ）

ルールのパフォーマンスに関するガイドライン

Firepower システムでは、さまざまなポリシーに含まれるルールが、ネットワーク トラフィックをきめ細かく制御します。ルールを適切に設定して順序付けることは、効果的な導入を確立する上で不可欠な要素です。それぞれの組織と導入に固有のポリシーとルールセットがありますが、ニーズに対処しながらもパフォーマンスを最適化するために従うべき一般的なガイドラインがいくつかあります。

パフォーマンスの最適化は、リソースを大量に消費する分析を実行する場合は特に重要です。複雑なポリシーやルールは、重要なリソースを消費し、パフォーマンスに悪影響を与える可能性があります。設定の変更を展開すると、システムはすべてのルールをまとめて評価し、ターゲット デバイスでネットワーク トラフィックを評価するために使用する拡張基準セットを作成します。それらの基準がターゲットデバイスのリソース（物理メモリ、プロセッサなど）を上回っている場合、そのデバイスに展開することはできません。

（注） 常に、ルールを組織のニーズに適した順序に配置する必要があります。すべてのトラフィックに適用する必要がある最優先順位のルールをポリシーの先頭近くに配置します。ただし、ルールに優先順位を付けなければ、アプリケーション条件または URL 条件を設定したルールが一致する可能性が高くなります。これは、システムは接続においてアプリケーショントラフィックまたは Web トラフィックを識別するまで、その接続の最初の数パケットと一部のルールとの照合をスキップすることがあるためです。これにより、アプリケーションと HTTP 要求が識別されるように接続が確立されます。

関連トピック

アプリケーション制御のガイドラインと制限事項 （484 ページ）
URL フィルタリングのガイドラインと制限事項 （1719 ページ）

ルールの簡素化および絞り込みのガイドライン

簡素化：設定しすぎない

処理するトラフィックの照合が 1 つの条件で十分な場合には、2 つの条件を使用しないでください。

個々のルール条件を最小化します。できる限り少ない個々の要素をルールの条件に使用します。たとえば、ネットワーク条件では、個々の IP アドレスではなく IP アドレス ブロックを使用します。

要素をオブジェクトに組み合わせても、パフォーマンスは向上**しません**。たとえば、50 個の IP アドレスを 1 つのネットワーク オブジェクトに含めて使用することにパフォーマンス的なメリットはなく、条件にこれらの IP アドレスを個別に含めるよりも単に構成上のメリットがあるだけです。

アプリケーション検出の推奨事項については、アプリケーション制御に関する推奨事項（1691 ページ）を参照してください。

絞り込み：特にインターフェイスによってリソース消費ルールを絞り込んで制約する

できる限り、ルールの条件を使用してリソース消費ルールが処理するトラフィックを絞り込んで定義します。絞り込まれたルールは、広範な条件を持つルールが多様なタイプのトラフィックを照合し、後でより多くの特定のルールをプリエンプション処理できるという理由からも重要です。以下は、リソース消費ルールの例です。

- トラフィックを復号する SSL ルール：復号だけでなく、復号されたトラフィックの更なる分析にもリソースが必要です。絞り込みを細かくし、また可能な場合は、暗号化トラフィックをブロックするか、復号しないようにします。

  Certain Firepower Management Center モデルはハードウェアで SSL 暗号化と復号化を実行します。これによりパフォーマンスが大きく向上します。詳細については、TLS 暗号化アクセラレーション（1809 ページ）を参照してください。

- ディープ インスペクションを呼び出すアクセス コントロール ルール：特に複数のカスタム侵入ポリシーと変数セットを使用している場合、侵入ファイルやマルウェアのインスペクションにはリソースが必要です。ディープインスペクションは必要な場所でのみ呼び出されることを確認してください。

最大のパフォーマンスによるメリットを得るため、インターフェイスによってルールを制約します。ルールがデバイスのすべてのインターフェイスを除外する場合、そのルールはそのデバイスのパフォーマンスに影響しません。

ルールの順序指定のガイドライン

常に、ルールを組織のニーズに適した順序に配置する必要があります。通常、すべてのトラフィックに適用する必要がある最優先順位のルールをポリシーの先頭近くに配置する必要があります。

例外については、次の項で説明します。

ルールのプリエンプション

ルールのプリエンプションが発生するのは、評価する順番が前のルールがトラフィックと一致するために、その後のルールが全くトラフィックと一致しない場合です。ルールの条件により、そのルールが他のルールをプリエンプション処理するかどうかが決まります。次の例では、最初のルールが管理トラフィックを許可するため、2 番目のルールがそのトラフィックをブロックできません。

アクセス コントロール ルール 1：管理ユーザを許可
アクセス コントロール ルール 2：管理ユーザをブロック

どのようなタイプのルール条件でも、後続のルールを回避する可能性があります。次の例では、最初の SSL ルールでの VLAN 範囲に 2 番目のルールでの VLAN が含まれるため、最初のルールが 2 番目のルールをプリエンプション処理します。

SSL ルール 1：VLAN 22 ～ 33 を復号しない
SSL ルール 2：VLAN 27 をブロック

次の例では、VLAN が設定されていないルール 1 はあらゆる VLAN と一致します。そのため、ルール 1 がルール 2 をプリエンプション処理し、ルール 2 での VLAN 2 の照合は行われません。

アクセス コントロール ルール 1：送信元ネットワーク 10.4.0.0/16 を許可
アクセス コントロール ルール 2：送信元ネットワーク 10.4.0.0/16、VLAN 2 を許可

あるルールとその後続のルールがまったく同じで、いずれもすべて同じ条件が設定されている場合、後続のルールがプリエンプション処理されます。

QoS ルール 1: VLAN 1 URL www.netflix.com をレート制限
QoS ルール 2: VLAN 1 URL www.netflix.com をレート制限

条件が 1 つでも異なる場合は、後続のルールがプリエンプション処理されることはありません。

QoS ルール 1: VLAN 1 URL www.netflix.com をレート制限
QoS ルール 2: VLAN 2 URL www.netflix.com をレート制限

例：プリエンプションを避けるための SSL ルールの順序付け

ここで 1 つのシナリオとして、信頼できる CA（Good CA）が悪意のあるエンティティ（Bad CA）に間違って CA 証明書を発行してしまい、その証明書を取り消していない状況を考えてみましょう。信頼できない CA によって発行された証明書で暗号化されたトラフィックは SSL ポリシーを使用してブロックしたいものの、信頼できる CA の信頼チェーン内にあるそれ以外のトラフィックは許可したいとします。CA 証明書とすべての中間 CA 証明書をアップロードした後、ルールを以下の順序で設定した SSL ポリシーを構成します。

SSL ルール 1：発行元 CN=www.badca.com をブロック

SSL ルール 2：発行元 CN=www.goodca.com を復号しない

上記のルールを逆の順序にすると、不正な CA で信頼されたトラフィックを含め、正当な CA で信頼されたすべてのトラフィックが最初に一致することになります。どのトラフィックも後続の不正な CA ルールに一致しないため、悪意のあるトラフィックはブロックされずに許可される可能性があります。

ルールのアクションとルールの順序

ルールのアクションによって、一致したトラフィックの処理方法が決まります。パフォーマンスを向上させるには、リソースを集約的に使用するルールを実行する前に、トラフィックの追加処理を実行または保証しないルールを配置してください。これにより、システムはさらに検査する必要のあるトラフィックだけを転送できます。

以下の例は、一連のルールがすべて同等に重要であり、プリエンプションが問題にならない場合に、さまざまなポリシーでルールを順序付ける方法を示しています。

ルールにアプリケーション条件が含まれている場合は、アプリケーション制御に関する推奨事項 （1691 ページ）も参照してください。

最適な順序：SSL ルール

復号にはリソースが必要になるだけでなく、復号後のトラフィックの分析も必要になります。したがって、トラフィックを復号する SSL ルールを最後に配置します。

（注） 特定の管理対象デバイスはハードウェアの TLS/SSL トラフィックの暗号化と復号化をサポートしているため、パフォーマンスが大幅に向上します。詳細については、TLS 暗号化アクセラレーション （1809 ページ）を参照してください。

1. [モニタ（Monitor）]：一致する接続をログに記録するだけで、トラフィックに対して他のアクションは実行しないルール。
2. [ブロック（Block）]、[リセットしてブロック（Block with reset）]：それ以上のインスペクションを行わずにトラフィックをブロックするルール。
3. [復号しない（Do not decrypt）]：暗号化トラフィックを復号しないまま、暗号化セッションをアクセス コントロール ルールに渡すルール。これらのセッションのペイロードにディープ インスペクションは適用されません。
4. [復号 - 既知のキー（Decrypt - Known Key）]：既知の秘密キーを使用して着信トラフィックを復号するルール。
5. [復号 - 再署名（Decrypt - Resign）]：サーバ証明書に再署名することによって発信トラフィックを復号するルール。

最適な順序：アクセス コントロール ルール

複数のカスタム侵入ポリシーと変数セットを使用している場合は特に、侵入、ファイル、マルウェアのインスペクションにリソースが必要です。したがって、ディープインスペクションを呼び出すアクセス コントロール ルールを最後に配置します。

1. [モニタ（Monitor）]：一致する接続をログに記録するだけで、トラフィックに対して他のアクションは実行しないルール。ただし、重要な例外と注意事項をアクセス コントロール ルールのモニタ アクション （1701 ページ）で確認してください。
2. [信頼（Trust）]、[ブロック（Block）]、[リセットしてブロック（Block with reset）]：それ以上のインスペクションを行わずにトラフィックを処理するルール。信頼できるトラフィックは、アイデンティティ ポリシーが課す認証要件、およびレート制限の対象となることに注意してください。
3. [許可（Allow）]、[インタラクティブ ブロック（ディープ インスペクションなし）（Interactive Block (no deep inspection)）]：それ以上のインスペクションを行わずにトラフィックのディスカバリを許可するルール。許可されるトラフィックは、アイデンティティ ポリシーが課す認証要件、およびレート制限の対象となることに注意してください。
4. [許可（Allow）]、[インタラクティブ ブロック（ディープ インスペクションあり）（Interactive Block (deep inspection)）]：禁止されているファイル、マルウェア、エクスプロイトのディープ インスペクションを実行するファイル ポリシーまたは侵入ポリシーに関連付けられているルール。

コンテンツ規制ルールの順序

SSL とアクセス コントロール ポリシーの両方でルールのプリエンプションを避けるため、YouTube の制限を制御するルールは、セーフサーチ制限を制御するルールの上に配置します。

アクセス コントロール ルールに対してセーフサーチを有効にする場合、システムは検索エンジンのカテゴリを [選択したアプリケーションとフィルタ（Selected Applications and Filters）] リストに追加します。このアプリケーション カテゴリには YouTube が含まれます。結果として、YouTube EDU がさらに上位の評価優先順位を持つルールで有効にされていない限り、YouTube トラフィックはセーフサーチ ルールに一致します。

同様のルールのプリエンプションは、セーフサーチ サポート フィルタを持つ SSL ルールを、評価順序内で特定の YouTube アプリケーション条件を持つ SSL ルールよりも高い順序に配置した場合に生じます。

関連トピック

コンテンツ制限について （1793 ページ）

アプリケーション ルールの順序

アプリケーション条件を使用するルールは、ルールのリストでより低い順序に移動すると、トラフィックに一致する可能性が高くなります。

特定の条件（ネットワークや IP アドレスなど）を使用するアクセス コントロール ルールは、一般的な条件（アプリケーションなど）を使用するルールの前に順位付けする必要がありま

す。オープン システム相互接続（OSI）モデルに精通している場合は、考え方として同様の順位付けを使用してください。レイヤ1、2、および3（物理、データリンク、およびネットワーク）の条件を持つルールは、アクセス コントロール ルールの最初に順位付けする必要があります。レイヤ5、6、および7（セッション、プレゼンテーション、およびアプリケーション）の条件は、アクセス コントロール ルールの後ろのほうに順序付けする必要があります。OSI モデルの詳細については、こちらの Wikipedia の記事を参照してください。

詳細および例については、アプリケーション制御に関する推奨事項（1691 ページ）を参照してください。

SSL ルールの順序

通常、特定の条件（IPアドレスとネットワークなど）を使用するルールは、一般的な条件（アプリケーションなど）を使用するルールの前に順位付けします。

証明書がピニングされたサイトからのトラフィックの許可

一部のアプリケーションでは、アプリケーション自体に元のサーバ証明書のフィンガープリントを埋め込む、ピニングまたは証明書ピニングと呼ばれる技術が使用されます。*TLS/SSL* そのため、[復号 - 再署名（Decrypt - Resign）] アクションで TLS/SSL ルールを設定した場合は、アプリケーションが管理対象デバイスから再署名された証明書を受信すると、検証が失敗し、接続が中断されます。

TLS/SSL ピニングが行われていることを確認するには、Facebook などのモバイル アプリケーションへのログインを試みます。ネットワーク接続エラーが表示された場合は、Webブラウザを使用してログインします。（たとえば、Facebook のモバイル アプリケーションにログインすることはできませんが、Safari または Chrome を使用して Facebook にログインすることはできます）。Firepower Management Center の接続イベントは、TLS/SSL ピニングのさらなる証明として使用できます

（注） TLS/SSL ピニングはモバイル アプリケーションに限定されません。

このトラフィックを許可するには、サーバ証明書の共通名または識別名と一致させるために、[復号しない（Do Not Decrypt）] アクションを使用して SSL ルールを設定します。SSL ポリシーでは、このルールを、トラフィックと一致するすべての [復号 - 再署名（Decrypt - Resign）] ルールの前に配置してください。Web サイトに正常に接続された後で、クライアント ブラウザから、ピニングされた証明書を取得できます。また、接続が成功したか失敗したかに関わらず、ログに記録された接続イベントから証明書を表示できます。

ClientHello の変更の優先順位付け

ClientHello の変更を優先順位付けするには、ServerHello またはサーバ証明書条件に一致するルールの前に、ClientHello メッセージで使用可能な条件に一致するルールを配置します。

管理対象デバイスが SSL ハンドシェイクを処理するときに、ClientHello メッセージを変更して、復号化の可能性を高めることができます。たとえば、FirePOWER システムは圧縮されたセッションを復号化できないので、圧縮メソッドを削除できます。

システムは [復号 - 再署名（Decrypt - Resign）] アクションを含む SSL ルールに最終的に一致させることができる場合、ClientHello メッセージを変更するのみです。システムが新しいサーバへの暗号化セッションを最初に検出したときは、サーバ証明書データを ClientHello の処理には使用できません。これは復号化されていない最初のセッションとなる可能性があります。同じクライアントからの後続の接続で、システムはサーバ証明書条件を含むルールに ClientHello メッセージを最終的に一致させ、メッセージを処理して、復号化の可能性を最大化できます。

ServerHello またはサーバ証明書条件（証明書、識別名、証明書のステータス、暗号スイート、バージョン）と一致するルールを、ClientHello 条件（ゾーン、ネットワーク、VLAN タグ、ポート、ユーザ、アプリケーション、URL カテゴリ）と一致するルールの前に配置する場合、ClientHello の変更をプリエンプション処理し、復号されないセッションの数を増やすことができます。

SSL ポリシーがバイパスされる状況

SSL ポリシーは、[信頼（Trust）]、[ブロック（Block）]、または [リセットしてブロック（Block With Reset）] のアクションを持つアクセス コントロール ルールが次に当てはまる場合、それらのルールに一致する接続に関してバイパスされます。

- セキュリティ ゾーン、ネットワーク、地理位置情報、およびポートだけをトラフィック照合基準として使用する。
- 検査を必要とする他のルール（アプリケーションまたは URL に基づいて接続を照合するルールなど）に先立つか、侵入またはファイル検査を適用するルールを許可する。

URL ルールの順序

URL マッチングを最も効果的に行うには、URL 条件を含むルールを他のルールより前に配置します。特に、URL ルールがブロック ルールで、他のルールが次の条件を両方とも満たす場合には、URL 条件を含むルールを前に配置します。

- その他のルールがアプリケーション条件を含んでいる。
- 検査対象のトラフィックが暗号化されている。

侵入ポリシーの急増を回避するためのガイドライン

アクセス コントロール ポリシーでは、1 つの侵入ポリシーを各許可ルール、インタラクティブ ブロック ルール、およびデフォルト アクションと関連付けることができます。侵入ポリシーと変数セットの固有の**ペア**はすべて、1 つのポリシーと見なされます。

ただし、ターゲット デバイスでサポートされるアクセス コントロール ルールや侵入ポリシーには最大数があります。この最大数は、ポリシーの複雑性、物理メモリ、デバイスのプロセッサ数などの、さまざまな要因によって異なります。

デバイスでサポートされる最大を超えるとアクセス コントロール ポリシーは展開できず、再評価する必要があります。いくつかの侵入ポリシーまたは変数セットを統合すると、複数のアクセス コントロール ルールに 1 つの侵入ポリシーと変数セットのペアを関連付けることがで

きます。一部のデバイスでは、すべての侵入ポリシーに関して1つの変数セットだけを使用できる場合や、デバイス全体でただ1つの侵入ポリシー/変数セット ペアだけを使用できる場合があります。

大規模接続（フロー）のオフロード

データセンターの Firepower 4100/9300 シャーシ で Firepower Threat Defense を展開する場合、ハードウェアにオフロードされるトラフィックの選択を有効にできます。これは、Firepower Threat Defense デバイスのソフトウェアや CPU で処理されないことを意味します。

トラフィックがNIC自体で切り替えられる超高速パスにオフロードされるトラフィックを識別して選択できます。これは、静的フローオフロードと呼ばれます。オフロードによって、大容量ファイルの転送など、データ集約型アプリケーションのパフォーマンスを向上させることができます。

- ハイパフォーマンス コンピューティング（HPC）調査サイト。ここでは、Firepower Threat Defense デバイスがストレージと高コンピューティング ステーション間で展開されます。1 つの調査サイトが NFS 経由の FTP ファイル転送またはファイル同期を使用してバックアップを行うと、大量のデータ トラフィックがすべての接続に影響を与えます。NFS を介するFTPファイル転送およびファイル同期のオフロードによって、他のトラフィックへの影響が軽減されます。
- 主にコンプライアンス目的で使用される High Frequency Trading（HFT）。ここでは、Firepower Threat Defenseデバイスがワークステーションと Exchange 間で展開されます。セキュリティは通常は問題にはなりませんが、遅延は大きな問題です。

フローのオフロードを信頼を含む複数の条件に基づいて Firepower Threat Defense に許可することもできます。これは、動的フロー オフロードと呼ばれます。

Firepower 4100/9300 シャーシでは、以下の基準を満たす接続をオフロードできます。

- （静的フロー オフロードのみ）プレフィルタ ポリシーにより FastPath される。
- （動的フロー オフロードのみ）。インスペクション エンジンが検査の必要がなくなったと判断した検査済みのフロー。これらのフローには次が含まれます。
  - アクセス コントロール ポリシーの [信頼（Trust）] ルール アクションに一致するフロー。
  - インテリジェントアプリケーションバイパス（IAB）ポリシーで、明示的か、またはフロー バイパスのしきい値を超えているために信頼されているフロー。
  - ファイルポリシーまたは信頼ポリシーに一致し、そのフローが信頼できると判断されたフロー。
- IPv4 アドレスのみ。
- TCP、UDP、GRE のみ。

（注） PPTP GRE 接続はオフロードされません。

- 標準または 802.1Q タグ付きイーサネット フレームのみ。
- スイッチドまたはルーテッドインターフェイスのみ。パッシブ、インライン、インライン タップ インターフェイスではサポートされません。

さらに、動的フロー オフロードは以下をサポートします。

- FTP データ転送などのセカンダリ接続（可能な限り）。
- 次の IPS プリプロセッサが検査したフロー：
  - SSL、SSH、および SMTP。
  - FTP プリプロセッサのセカンダリ接続。
  - Session Initiation Protocol（SIP）プリプロセッサのセカンダリ接続。
- キーワードを使用する侵入ルール（オプションとも呼ばれる）。
- インテリジェントアプリケーション バイパス（IAB）。特定の条件を満たす場合に、追加検査なしでネットワークの通過を信頼するアプリケーションを特定します。

静的フロー オフロードの使い方

オフロードに適格なフローを識別するには、**FastPath** アクションを適用するプレフィルタ ポリシー ルールを作成します。TCP/UDP にはプレフィルタ ルールを使用し、GRE にはトンネル ルールを使用します。ちなみに、セキュリティ ゾーン、送信元と宛先のネットワーク、およびポートのマッチングのみに基づいて [信頼（Trust）] アクションを適用するようにアクセス コントロール ルールを設定し、[セキュリティ インテリジェンス（Security Intelligence）] を無効にする場合、これらのルールをマッチングするフローも、オフロードに適格なフローになります。

接続が確立されると、オフロードに適格な接続であれば、さらなる処理が Firepower Threat Defense ソフトウェアではなく NIC で行われます。 オフロードされたフローは、引き続き制限付きステートフルインスペクション（基本的なTCPフラグおよびオプションのチェックなど）を受信します。システムは必要に応じてさらなる処理のためにファイアウォール システムへのパケットを選択的に増やすことができます。

オフロードされたフローのリバース フローもオフロードされます。

動的フロー オフロードの使い方

動的フロー オフロードはデフォルトで有効です。

（注） 動的フローオフロード条件に一致する2つ以上のフローが、同時にオフロードにキューイングされた場合、衝突が発生します。衝突が発生した場合は、最初のフローのみがオフロードします。他のフローは通常どおりに処理されます。**show flow-offload flow** コマンドはコリジョンの統計情報を表示します。

次に、動的オフロードの無効化の例を示します。

```
> configure flow-offload dynamic whitelist disable
```

次に、動的オフロードの有効化の例を示します。

```
> configure flow-offload dynamic whitelist enable
```

フロー オフロードの制限事項

すべてのフローをオフロードできるわけではありません。オフロードの後でも、フローを特定の条件下でのオフロードから除外することができます。次に、制限事項の一部を示します。

オフロードできないフロー

次のタイプのフローはオフロードできません。

- IPv6 アドレッシングを使用するフロー。
- TCP、UDP、GRE 以外のプロトコルに対するフロー。

（注） PPTP GRE 接続はオフロードできません。

- パッシブ、インラインまたはインライン タップ モードで設定されたインターフェイス上のフロー。ルーテッド インターフェイスおよびスイッチ インターフェイスがサポートされている唯一のタイプです。
- Snort またはその他のインスペクション エンジンによるインスペクションが必要なフロー。FTP など場合によっては、コントロール チャネルはオフロードできませんがセカンダリ データ チャネルはオフロードできます。
- IPsec および VPN 接続。
- 存続可能時間（TTL）値を減少させるフロー。
- 暗号化または復号化を必要とするフロー。
- マルチキャスト フロー。
- TCP インターセプト フロー。
- AAA 関連のフロー。
- Vpath、VXLAN 関連のフロー。

- URL フィルタリング。
- Tracer フロー。
- セキュリティ グループでタグ付けされたフロー。
- クラスタで非対称フローが発生した場合に備えて、別のクラスタ ノードから転送されるリバース フロー。
- クラスタ内の一元化されたフロー（フローのオーナーがマスターでない場合）。

動的にオフロードできない追加のフロー

IP オプションを含むフローは動的にオフロードできません。

ダイナミック フローのオフロードによってすべての TCP ノーマライザのチェックが無効になります。

オフロードを無効にする条件

フローがオフロードされた後、フロー内のパケットは次の条件を満たす場合に Firepower Threat Defense デバイス に返され、さらに処理されます。

- タイムスタンプ以外の TCP オプションが含まれている。
- フラグメント化されている。
- これらは等コストマルチパス（ECMP）ルーティングの対象であり、入力パケットは 1 つのインターフェイスから別のインターフェイスに移動する。

ルール管理の履歴：共通の特性

機能	バージョン	詳細
URL の条件に関する情報を新しい「URL フィルタリング」の章に移動	6.3	URL フィルタリングに関する情報を、URL の条件に関する専用トピックを含めてURL Filtering （1717 ページ）に移動。

第 21 章

再利用可能なオブジェクト

以下のトピックでは、Firepower システムで再利用可能オブジェクトを管理する方法について説明します。

再利用可能オブジェクトの概要

柔軟性と Web インターフェイスの使いやすさを向上させるために、Firepower システムでは、名前を値に関連付ける再利用可能な構成である名前付きオブジェクトを使用します。その値を使用する場合は、代わりに名前付きオブジェクトを使用します。多くのポリシーとルール、イベント検索、レポート、ダッシュボードなど、Webインターフェイスのさまざまな場所でのオブジェクトの使用がサポートされています。よく使用される構成を表す多くの事前定義されたオブジェクトが提供されています。

オブジェクトを作成および管理するには、オブジェクトマネージャを使用します。オブジェクトを使用する多くの構成では、必要に応じて、その場でオブジェクトを作成することもできます。オブジェクト マネージャを使用して、次の操作も実行できます。

- ネットワーク、ポート、VLAN、またはURL オブジェクトが使用されているポリシー、設定、およびその他のオブジェクトを表示します。オブジェクトとその使用状況の表示 （518 ページ）を参照してください。
- 単一の構成で複数のオブジェクトを参照するための、オブジェクトのグループ化。オブジェクト グループ （520 ページ）を参照してください。
- 選択したデバイス、またはマルチドメイン展開の場合は選択したドメインのオブジェクト値のオーバーライド。オブジェクトのオーバーライド（522ページ）を参照してください。

アクティブなポリシーで使用されるオブジェクトを編集した後に、変更を有効にするには、変更した構成を再展開する必要があります。アクティブなポリシーで使用されているオブジェクトは削除できません。

（注） オブジェクトは、そのデバイスに割り当てられているポリシーでオブジェクトが使用される場合のみ、管理対象デバイスで設定されます。特定のデバイスに割り当てられているすべてのポリシーからオブジェクトを削除する場合、オブジェクトは、次の導入時にデバイス設定からも削除され、オブジェクトに対する後続の変更はデバイス設定に反映されません。

オブジェクト タイプ

次の表に、Firepower システムで作成できるオブジェクト、各オブジェクト タイプがグループ化可能かどうか、およびオーバーライドを許可するように構成できるかどうかを示します。

オブジェクト タイプ（Object Type）	グループ化可能	オーバーライドを許可
ネットワーク	はい	はい
[ポート（Port）]	はい	はい
インターフェイス： • セキュリティ ゾーン • インターフェイス グループ	いいえ	いいえ
トンネル ゾーン	いいえ	いいえ
アプリケーション フィルタ	いいえ	いいえ
VLAN タグ	はい	はい
セキュリティ グループ タグ（SGT）	いいえ	いいえ
URL	はい	はい
位置情報（GeoLocation）	いいえ	いいえ
時間範囲	いいえ	いいえ
変数セット	いいえ	いいえ
セキュリティ インテリジェンス：ネットワーク、DNS、URL のリストとフィード	いいえ	いいえ
シンクホール	いいえ	いいえ
ファイル リスト	いいえ	いいえ
暗号スイート リスト	いいえ	いいえ
識別名（Distinguished Name）	はい	いいえ（No）
公開キー インフラストラクチャ（PKI）： • 内部および信頼できる CA • 内部および外部証明書	はい	いいえ（No）
Key Chain	いいえ	はい
DNS サーバ グループ	いいえ	いいえ
SLA モニタ	いいえ	いいえ
プレフィックス リスト：IPv4 および IPv6	いいえ	はい

オブジェクト タイプ（Object Type）	グループ化可能	オーバーライドを許可
ルート マップ	いいえ	はい
アクセス リスト：標準および拡張	いいえ	はい
AS パス	いいえ	はい
コミュニティ リスト（Community List）	いいえ	はい
ポリシー リスト	いいえ	はい
FlexConfig：テキストおよびFlexConfig オブジェクト	いいえ	はい

オブジェクトおよびマルチテナンシー

マルチドメイン展開では、グローバルおよび子孫ドメインでオブジェクトを作成できます。ただし、グローバル ドメインでのみ作成できるセキュリティ グループ タグ（SGT）オブジェクトを除きます。現在のドメインで作成されたオブジェクトが表示されます。このオブジェクトは編集できます。また、編集できない先祖ドメインで作成されたオブジェクトも表示されますが、セキュリティ ゾーンとインターフェイス グループを除きます。

（注） セキュリティ ゾーンとインターフェイス グループは、リーフ レベルで設定したデバイス インターフェイスに関連するため、子孫ドメイン内の管理者は、先祖ドメインで作成されたゾーンとグループを表示および編集できます。サブドメインのユーザは、先祖ゾーンとグループからインターフェイスを追加および削除できますが、ゾーン/グループを削除または名前変更することはできません。

オブジェクト名は、ドメイン階層内で一意である必要があります。システムは、現在のドメインでは表示できないオブジェクトの名前との競合を特定することができます。

グループ化をサポートするオブジェクトの場合、現在のドメインのオブジェクトを先祖ドメインから継承されたオブジェクトとグループ化できます。

オブジェクトのオーバーライドにより、ネットワーク、ポート、VLAN タグ、URL などの特定のオブジェクト タイプのデバイス固有またはドメイン固有の値を定義できます。マルチドメイン展開では、先祖ドメイン内のオブジェクトのデフォルト値を定義できますが、子孫ドメイン内の管理者は、そのオブジェクトのオーバーライドの値を追加できます。

オブジェクト マネージャ

オブジェクト マネージャを使用すると、オブジェクトおよびオブジェクト グループを作成、管理することができます。

オブジェクト マネージャには、ページあたり 20 のオブジェクトまたはグループが表示されます。オブジェクトまたはグループのタイプが 20 を超える場合は、ページ下部のナビゲーション リンクを使用して追加ページを表示します。特定のページにアクセスしたり、更新アイコン（  ）にアクセスしてビューを更新したりすることもできます。

デフォルトでは、オブジェクトとグループはページで、アルファベット順に名前でリストされます。ただし、表示されている任意の列でオブジェクトまたはグループの各タイプをソートできます。ページのオブジェクトは、名前または値でフィルタすることもできます。

オブジェクトの編集

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Access Admin/Network Admin

マルチドメインの展開では、現在のドメインで作成されたオブジェクトが表示されます。このオブジェクトは編集できます。先祖ドメインで作成されたオブジェクトも表示されますが、ほとんどの場合これは編集できません。子孫ドメインにあるオブジェクトを表示および編集するには、そのドメインに切り替えます。

ステップ 1 **[Objects]** > **[Object Management]**を選択します。

ステップ 2 リストからオブジェクト タイプを選択します（再利用可能オブジェクトの概要 （514 ページ）を参照）。

ステップ 3 編集するオブジェクトの横にある編集アイコン（）をクリックします。

代わりに表示アイコン（  ）が表示される場合、オブジェクトは先祖ドメインに属しており、上書きを許可しないように設定されており、オブジェクトを変更する権限がありません。

ステップ 4 必要に応じてオブジェクト設定を変更します。

ステップ 5 変数セットを編集する場合は、セット内の変数を管理します（変数の管理 （554 ページ）を参照）。

ステップ 6 オーバーライドを許可するように設定できるオブジェクトの場合、次の操作をします。

- このオブジェクトのオーバーライドを許可する場合は、[Allow Overrides] チェックボックスをオンにします（オブジェクトのオーバーライドの許可 （524 ページ）を参照）。 現在のドメインに属しているオブジェクトに対してのみ、この設定を変更できます。
- このオブジェクトにオーバーライド値を追加する場合は、[Override] セクションを展開し、[Add] をクリックします（オブジェクトのオーバーライドの追加 （524 ページ）を参照）。

ステップ 7 **[保存（Save）]** をクリックします。

ステップ 8 変数セットを編集するときにそのセットがアクセス コントロール ポリシーで使用されている場合、[はい（Yes）] をクリックして変更の保存を確認します。

次のタスク

- アクティブ ポリシーがオブジェクトを参照する場合は、設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

オブジェクトとその使用状況の表示

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Access Admin/Network Admin

[オブジェクト管理（Object Management）] ページでは、ネットワーク、ポート、VLAN、および URL オブジェクトに追加のオプションがあり、これらのオブジェクトが使用されている場所を確認できます。

（注） マルチドメイン展開では、他のドメインのオブジェクトを表示できます。ただし、子孫ドメインにあるオブジェクトの使用状況を検索するには、そのドメインに切り替えます。

ステップ 1 **[Objects]** > **[Object Management]**を選択します。

ステップ 2 次のオブジェクト タイプのいずれかを選択します。

- ネットワーク
- [ポート（Port）]
- グループ化
- URL

ステップ 3 任意のオブジェクトの横にある [Find Usage] アイコン（  ）をクリックします。

[Object Usage] ウィンドウには、選択したオブジェクトが使用されているすべてのポリシー、オブジェクト、およびその他の設定のリストが表示されます。オブジェクトの使用率の詳細を確認するには、リスト内のいずれかの項目をクリックします。オブジェクトが使用されるポリシーおよびその他の設定については、対応するリンクをクリックすると、それぞれの UI ページにアクセスすることができます。

ステップ 4 [閉じる（Close）] をクリックします。

オブジェクトまたはオブジェクト グループのフィルタ処理

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Access Admin/Network Admin

マルチドメインの導入環境では、現在ドメインと親ドメインで作成されたオブジェクトが表示され、それらをフィルタ処理できます。

ステップ 1 **[Objects]** > **[Object Management]**を選択します。

ステップ 2 [Filter] フィールドのフィルタ条件を入力します。

ページは入力に従って更新され、一致する項目が表示されます。

次のメタ文字を使用できます。

- アスタリスク（*）文字は、ある文字の 0 回以上のオカレンスに一致します。
- キャレット記号（^）は文字列の先頭のコンテンツと一致します。
- ドル記号（$）は文字列の末尾と一致します。

オブジェクトのソート

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Access Admin/Network Admin

マルチドメインの展開では、現在のドメインで作成されたオブジェクトが表示されます。このオブジェクトは編集できます。先祖ドメインで作成されたオブジェクトも表示されますが、ほとんどの場合これは編集できません。子孫ドメインにあるオブジェクトを表示および編集するには、そのドメインに切り替えます。

ステップ 1 **[Objects]** > **[Object Management]**を選択します。

ステップ 2 カラムの見出しをクリックします。反対方向でソートするには、見出しを再度クリックします。

オブジェクト グループ

オブジェクトをグループ化すると、複数のオブジェクトを1つの設定で参照できます。システムでは、Web インターフェイスでオブジェクトおよびオブジェクト グループを交互に使用することができます。たとえば、ポート オブジェクトを使用する場合はいつでも、ポート オブジェクト グループも使用できます。

ネットワーク、ポート、VLANタグ、URL、およびPKIオブジェクトをグループ化できます。ネットワーク オブジェクト グループはネストすることができます。つまり、ネットワーク オブジェクト グループを別のネットワーク オブジェクト グループに追加できます。許容されるネスト レベルは最大 10 です。

同じタイプのオブジェクトおよびオブジェクトグループには、同じ名前を付けることはできません。マルチドメイン展開では、オブジェクトグループの名前をドメイン階層内で一意にする必要があります。システムは、現在のドメインでは表示できないオブジェクトの名前との競合を特定することができます。

ポリシーで使用されるオブジェクト グループ（たとえば、アクセス コントロール ポリシーで使用されるネットワーク オブジェクトグループ）を編集する場合、変更を適用するためには、変更後の設定を再展開する必要があります。

グループを削除しても、グループ内のオブジェクトは削除されず、相互の関連性だけが削除されます。さらに、アクティブポリシーで使用中のグループは削除できません。たとえば、保存されたアクセス コントロール ポリシーの VLAN 条件で使用している VLAN タグのグループは削除できません。

再利用可能オブジェクトのグループ化

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Access Admin/Network Admin

マルチドメインの展開では、現在のドメインで作成されたオブジェクトが表示されます。このオブジェクトは編集できます。先祖ドメインで作成されたオブジェクトも表示されますが、ほとんどの場合これは編集できません。子孫ドメインにあるオブジェクトを表示および編集するには、そのドメインに切り替えます。

先祖ドメインから継承したオブジェクトを持つ現在のドメイン内のオブジェクトをグループ化できます。

ステップ 1 **[Objects]** > **[Object Management]**を選択します。

ステップ 2 グループ化するオブジェクト タイプが、[ネットワーク（Network）]、[ポート（Port）]、[URL]、[VLAN タグ（VLAN Tag）] の場合は、次のように操作します。

a) オブジェクト タイプのリストからオブジェクト タイプを選択します。

b) [追加 [オブジェクト タイプ]（Add [Object Type]）] ドロップダウンリストから [グループの追加（Add Group）] を選択します。

ステップ 3 グループ化するオブジェクト タイプが [識別名（Distinguished Name）] の場合は、次のように操作します。

a) [識別名（Distinguished Name）] ノードを展開します。
b) [オブジェクト グループ（Object Groups）] を選択します。
c) [識別名グループの追加（Add Distinguished Name Group）] をクリックします。

ステップ 4 グループ化するオブジェクト タイプが [PKI] の場合は、次のように操作します。

a) [PKI] ノードを展開します。
b) 次のいずれかを実行します。

- **内部 CA グループ（Internal CA Groups）**
- **信頼できる CA グループ（Trusted CA Groups）**
- **内部証明書グループ（Internal Cert Groups）**
- **外部証明書グループ（External Cert Groups）**

c) [オブジェクト タイプ] グループの追加（Add [Object Type] Group）] ボタンをクリックします。

ステップ 5 一意の [名前（Name）] を入力します。

ステップ 6 リストから 1 つ以上のオブジェクトを選択して、[追加（Add）] をクリックします。

次のことも実行できます。

- 含める既存のオブジェクトを検索するには、フィルタ フィールド（）を使用します。これは入力に従って更新され、一致する項目を表示します。検索文字列をクリアするには、検索フィールドの上にある再ロードアイコン（）をクリックするか、検索フィールド内のクリアアイコン（）をクリックします。
- 既存のオブジェクトがニーズを満たさない場合、すぐにオブジェクトを作成するには、追加アイコン（）をクリックします。

ステップ 7 必要に応じて、[ネットワーク（Network）]、[ポート（Port）]、[URL]、および [VLAN タグ（VLAN Tag）] グループに対し、次の操作を実行します。

- [説明（Description）] を入力します。
- [オーバーライドを許可する（Allow Overrides）] チェックボックスをオンにして、このオブジェクト グループのオーバーライドを許可します。オブジェクトのオーバーライドの許可 （524 ページ）を参照してください。

ステップ 8 [保存（Save）] をクリックします。

次のタスク

- アクティブなポリシーがオブジェクト グループを参照する場合は、設定の変更を展開します。設定変更の展開 （447 ページ）を参照してください。

オブジェクトのオーバーライド

オブジェクトをオーバーライドすることにより、オブジェクトの代替値を定義できます。指定したデバイスに対して、システムはこの代替値を使用します。

ほとんどのデバイスに有効な定義を設定したオブジェクトを作成した後、異なる定義を必要とする少数のデバイスについて、オーバーライドを使用してオブジェクトに対する変更内容を指定できます。また、すべてのデバイスに対してオーバーライドする必要があるオブジェクトを作成し、そのオブジェクトを使用してすべてのデバイスに適用する単一のポリシーを作成することもできます。オブジェクト オーバーライドでは、デバイス全体で使用する共有ポリシーの小さなセットを作成し、個々のデバイスの必要に応じてポリシーを変更できます。

たとえば、社内のさまざまな部門へのICMPトラフィックを拒否する場合があります。それぞれの部門は、異なるネットワークに接続されています。これを実行するには、Departmental Networkという名前のネットワーク オブジェクトを含むルールを使用して、アクセス コントロール ポリシーを定義します。このオブジェクトのオーバーライドを許可することによって、関連する各デバイスで、デバイスが接続されている実際のネットワークを指定するオーバーライドを作成できます。

マルチドメイン展開では、先祖ドメインのオブジェクトのデフォルト値を定義して、子孫ドメインの管理者がそのオブジェクトのオーバーライド値を追加できるようにすることができます。たとえば、マネージドセキュリティサービスプロバイダー（MSSP）では、単一のFirepower Management Centerを使用して複数の顧客のネットワーク セキュリティを管理する場合があります。この場合、MSSPの管理者は、すべての顧客の導入で使用するオブジェクトをグローバル ドメインに定義できます。各顧客の管理者は子孫ドメインにログインして、それぞれの組織に応じてそのオブジェクトをオーバーライドできます。これらのローカル管理者がMSSPの他の顧客のオーバーライド値を表示したり、影響を与えたりすることはできません。

オブジェクト オーバーライドのターゲットを特定のドメインに絞ることもできます。その場合、ユーザがデバイス レベルで値をオーバーライドしない限り、システムはターゲット ドメインのすべてのデバイスにオブジェクト オーバーライド値を使用します。

オブジェクト マネージャで、オーバーライド可能なオブジェクトを選択し、そのオブジェクトに対するデバイス レベルまたはドメイン レベルのオーバーライドのリストを定義できます。

オブジェクト オーバーライドを使用できるオブジェクト タイプは以下に限られます。

- ネットワーク
- [ポート（Port）]
- VLAN タグ
- URL
- SLA モニタ
- プレフィックス リスト
- ルート マップ
- アクセス リスト

- AS パス
- コミュニティ リスト（Community List）
- ポリシー リスト
- PKI 登録
- Key Chain

オブジェクト マネージャでは、オーバーライド可能なオブジェクトのオブジェクト タイプには [オーバーライド（Override）] 列が表示されます。この列の有効な値は以下のとおりです。

- 緑のチェックマーク：このオブジェクトにはオーバーライドを作成できます。オーバーライドはまだ追加されていません。
- 赤の X：このオブジェクトにはオーバーライドを作成できません。
- 数値：このオブジェクトに追加されているオーバーライドの数を表します（たとえば、「2」は 2 つのオーバーライドが追加されていることを意味します）。

オブジェクト オーバーライドの管理

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Access Admin/Network Admin

ステップ 1 **[Objects]** > **[Object Management]**を選択します。

ステップ 2 オブジェクト タイプのリストから選択します（再利用可能オブジェクトの概要 （514 ページ）を参照）。

ステップ 3 編集するオブジェクトの横にある編集アイコン（  ）をクリックします。

代わりに表示アイコン（  ）が表示される場合、オブジェクトは先祖ドメインに属しており、上書きを許可しないように設定されており、オブジェクトを変更する権限がありません。

ステップ 4 オブジェクト オーバーライドを管理します。

- 追加：オブジェクト オーバーライドを追加します（オブジェクトのオーバーライドの追加 （524 ページ）を参照）。
- 許可：オブジェクト オーバーライドを許可します（オブジェクトのオーバーライドの許可 （524 ページ） を参照）。
- 削除：オブジェクト エディタで、削除するオーバーライドの横にある削除アイコン（  ）をクリックします。

- 編集：オブジェクト オーバーライドを編集します（オブジェクト オーバーライドの編集 （525 ページ）を参照）。

オブジェクトのオーバーライドの許可

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Access Admin/Network Admin

ステップ 1 オブジェクト エディタで、[オーバーライドを許可（Allow Overrides）]チェックボックスをオンにします。

ステップ 2 **[Save（保存）]** をクリックします。

次のタスク

オブジェクトのオーバーライド値を追加します（オブジェクトのオーバーライドの追加 （524 ページ）を参照）。

オブジェクトのオーバーライドの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Access Admin/Network Admin

始める前に

オブジェクトのオーバーライドを許可します（オブジェクトのオーバーライドの許可 （524ページ）を参照）。

ステップ 1 オブジェクト エディタで、[オーバーライド（Override）] セクションを展開します。

ステップ 2 [Add] をクリックします。

ステップ 3 [ターゲット（Targets）] タブで、[使用可能なデバイスとドメイン（Available Devices and Domains）] リストからドメインまたはデバイスを選択し、[追加（Add）] をクリックします。

ステップ 4 [オーバーライド（Override）] タブで、[名前（Name）] を入力します。

ステップ 5 （任意）[Description] に説明を入力します。

ステップ 6 オーバーライド値を入力します。

例：

ネットワーク オブジェクトについては、ネットワーク値を入力します。

ステップ 7 [Add] をクリックします。

ステップ 8 **[保存（Save）]** をクリックします。

次のタスク

- アクティブ ポリシーがオブジェクトを参照する場合は、設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

オブジェクト オーバーライドの編集

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Access Admin/Network Admin

既存のオーバーライドの説明と値を変更できます。ただし、既存のターゲット リストは変更できません。代わりに、既存のオーバーライドを置き換える、新しいターゲットに対する新しいオーバーライドを追加する必要があります。

ステップ 1 オブジェクト エディタで、[オーバーライド（Override）] セクションを展開します。

ステップ 2 変更するオーバーライドの横にある編集アイコン（  ）をクリックします。

ステップ 3 必要に応じて、[説明（Description）] を変更します。

ステップ 4 オーバーライド値を変更します。

ステップ 5 [保存（Save）] をクリックして、オーバーライドを保存します。

ステップ 6 [保存（Save）] をクリックして、オブジェクトを保存します。

次のタスク

- アクティブ ポリシーがオブジェクトを参照する場合は、設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

ネットワーク オブジェクト

ネットワーク オブジェクトは 1 つ以上の IP アドレスを表します。ネットワーク オブジェクトおよびグループを、アクセス コントロール ポリシー、ネットワーク変数、アイデンティティ

ルール、ネットワーク検出ルール、イベント検索、レポートなど、システムの Web インターフェイスのさまざまな場所で使用できます。

ネットワーク オブジェクトを必要とするオプションを設定する際は、リストが自動的にフィルタリングされて、そのオプションに有効なネットワーク オブジェクトだけが表示されます。たとえば、オプションのなかにはホスト オブジェクトが必要なものと、サブネットが必要なものがあります。

ネットワーク オブジェクトには、以下のいずれかのタイプを指定できます。

ホスト

単一の IP アドレス。

IPv4 の例：

```
209.165.200.225
```

IPv6 の例：

```
2001:DB8::0DB8:800:200C:417A または 2001:DB8:0:0:0DB8:800:200C:417A
```

範囲

IP アドレスの範囲。

IPv4 の例：

```
209.165.200.225-209.165.200.250
```

IPv6 の例：

```
2001:db8:0:cd30::1-2001:db8:0:cd30::1000
```

ネットワーク（Network）

アドレス ブロック（別名サブネット）。

IPv4 の例：

```
209.165.200.224/27
```

IPv6 の例：

```
2001:DB8:0:CD30::/60
```

[FQDN]

単独の完全修飾ドメイン名（FQDN）Ipv4アドレスのみ、IPv6アドレスのみ、およびIPv4とIPv6アドレス両方でのFQDN解決がサポートされています。

次に例を示します。

```
www.example.com
```

（注）

- FQDN は、数字または文字で始まって終わる必要があります。FQDN で内部文字として使用できるのは、文字、数字、およびハイフンだけです。
- FQDN オブジェクトは、アクセス コントロール ルールとプレフィルタ ルールのみで使用できます。ルールは、DNS ルックアップを介して FQDN で取得された IP アドレスを一致させます。FQDN 解決の最初のインスタンスは、FQDN オブジェクトがアクセス コントロール ポリシーに展開された場合に発生します。FQDN ネットワーク オブジェクトを使用するには、DNS サーバ設定を DNS サーバ グループ オブジェクト（601 ページ） で設定し、DNS プラットフォーム設定を DNS の設定 （1360 ページ） で設定していることを確認します。

グループ

ネットワーク オブジェクトまたは他のネットワーク グループからなるグループ。

次に例を示します。

```
209.165.200.225
209.165.201.1
209.165.202.129
```

あるネットワーク オブジェクト グループを別のネットワーク オブジェクト グループに追加することで、ネストされたグループを作成できます。グループをネストできるレベルは、最大で 10 レベルです。

ネットワーク オブジェクトの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Access Admin/Network Admin

ステップ 1 **[Objects]** > **[Object Management]**を選択します。

ステップ 2 オブジェクト タイプのリストから [ネットワーク（Network）] を選択します。

ステップ 3 [ネットワークを追加（Add Network）] ドロップダウン メニューで、[オブジェクトの追加（Add Object）] を選択します。

ステップ 4 [Name] を入力します。

マルチドメイン展開では、オブジェクト名をドメイン階層内で一意にする必要があります。システムは、現在のドメインでは表示できないオブジェクトの名前との競合を特定することができます。

ステップ 5 （任意）[Description] に説明を入力します。

ステップ 6 [ネットワーク（Network）] フィールドで、必要なオプションを選択して適切な値を入力します（ネットワーク オブジェクト （525 ページ）を参照）。

ステップ 7 （FQDN オブジェクトのみ）[ルックアップ（Lookup）] ドロップダウン メニューから DNS 解決を選択して、IPv4、IPv6、または IPv4 と IPv6 の両方のアドレスを FQDN に関連付けるかを決定します。

ステップ 8 オブジェクトのオーバーライドを管理します。

- このオブジェクトのオーバーライドを許可する場合は、[Allow Overrides] チェックボックスをオンにします（オブジェクトのオーバーライドの許可 （524 ページ）を参照）。
- このオブジェクトにオーバーライド値を追加する場合は、[Override] セクションを展開し、[Add] をクリックします（オブジェクトのオーバーライドの追加 （524 ページ）を参照）。

ステップ 9 **[保存（Save）]** をクリックします。

次のタスク

- アクティブ ポリシーがオブジェクトを参照する場合は、設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

ポート オブジェクト

ポート オブジェクトは、異なるプロトコルをそれぞれ少し異なる方法で表します。

TCP および UDP

ポート オブジェクトは、カッコ内にプロトコル番号が記載されたトランスポート層プロトコルと、オプションの関連ポートまたはポート範囲を表します。例：`TCP(6)/22`。

ICMP および ICMPv6（IPv6-ICMP）

ポート オブジェクトはインターネット層プロトコルと、オプションでタイプおよびコードを表します。例：`ICMP(1):3:3`

ICMP または IPV6-ICMP ポート オブジェクトは、タイプ、および該当する場合はコードを基準に制限できます。ICMP のタイプとコードの詳細については、次の URL を参照してください。

- http://www.iana.org/assignments/icmp-parameters/icmp-parameters.xml
- http://www.iana.org/assignments/icmpv6-parameters/icmpv6-parameters.xml

その他

ポート オブジェクトは、ポートを使用しない他のプロトコルを表します。

Firepower システムには、ウェルノウン ポート用にデフォルトのポート オブジェクトが用意されています。これらのデフォルト オブジェクトを変更または削除することはできません。デフォルト オブジェクトに加え、カスタム ポート オブジェクトを作成できます。

ポート オブジェクトおよびグループは、アクセス コントロール ポリシー、アイデンティティ ルール、ネットワーク検出ルール、ポート変数、イベント検索など、システムの Web インターフェイスのさまざまな場所で使用できます。たとえば、組織が特定のポート範囲を使用するカスタム クライアントを使用していて、システムで過剰なイベントや誤解を与えるイベントが発生した場合、それらのポートをモニタ対象から除外するようネットワーク検出ポリシーを設定できます。

ポート オブジェクトを使用する際は、次のガイドラインに従ってください。

- アクセス コントロール ルールの送信元ポート条件には TCP/UDP 以外のプロトコルを追加できません。さらに、送信元ポートと宛先ポートの両方のポート条件をルールで設定する場合、トランスポート プロトコルを混在させることはできません。
- 送信元ポート条件で使用されるポート オブジェクト グループにサポート対象外のプロトコルを追加した場合、設定を展開しても、その条件が使用されているルールは管理対象デバイスで適用されません。
- TCP と UDP の両方のポートを含むポート オブジェクトを作成してから、ルールの送信元ポート条件としてそのポート オブジェクトを追加した場合、宛先ポートを追加することはできません。その逆もまた同様です。

ポート オブジェクトの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Access Admin/Network Admin

ステップ 1 **[Objects]** > **[Object Management]**を選択します。

ステップ 2 オブジェクト タイプのリストから [ポート（Port）] を選択します。

ステップ 3 [ポートの追加（Add Port）] ドロップダウン リストで、[オブジェクトの追加（Add Object）] を選択します。

ステップ 4 名前を入力します。

ステップ 5 [プロトコル（Protocol）] を選択します。

ステップ 6 選択したプロトコルに応じて、[ポート（Port）] で制限するか、または ICMP の [タイプ（Type）] および [コード（Code）] を選択します。

1 から **65535** のポートを入力できます。ポート範囲を指定するには、ハイフンを使用します。[すべて（All）] のプロトコルと一致させることを選択した場合は、[その他（Other）] ドロップダウン リストを使用して、ポートでオブジェクトを制限する必要があります。

ステップ 7 オブジェクトのオーバーライドを管理します。

- このオブジェクトのオーバーライドを許可する場合は、[Allow Overrides] チェックボックスをオンにします（オブジェクトのオーバーライドの許可 （524 ページ）を参照）。
- このオブジェクトにオーバーライド値を追加する場合は、[Override] セクションを展開し、[Add] をクリックします（オブジェクトのオーバーライドの追加 （524 ページ）を参照）。

ステップ 8 **[保存（Save）]** をクリックします。

次のタスク

- アクティブ ポリシーがオブジェクトを参照する場合は、設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

トンネル ゾーン

トンネル ゾーンとは、特別な分析のために明示的にタグ付けする特定のタイプのプレーン テキスト、パススルー トンネルを表します。トンネル ゾーンは、一部の設定でインターフェイスの制約として使用できますが、インターフェイス オブジェクトではありません。

詳細については、トンネル ゾーンおよびプレフィルタリング （1777 ページ）を参照してください。

アプリケーション フィルタ

システム提供のアプリケーション フィルタは、アプリケーションの基本特性（タイプ、リスク、ビジネスとの関連性、カテゴリ、およびタグ）にしたがってアプリケーションを整理することで、アプリケーション制御に役立ちます。オブジェクト マネージャで、システム提供のフィルタの組み合わせやアプリケーションの任意の組み合わせをもとに、ユーザ定義の再利用可能アプリケーション フィルタを作成、管理できます。詳細については、アプリケーション条件（アプリケーション制御） （479 ページ）を参照してください。

VLAN タグ オブジェクト

設定した個々の VLAN タグ オブジェクトは、1 つの VLAN タグまたはタグの範囲を表します。

複数の VLAN タグ オブジェクトをグループ化できます。グループは複数のオブジェクトを表します。つまり、1 つのオブジェクトで VLAN タグの範囲を使用することは、この意味ではグループとはみなされません。

VLAN タグ オブジェクトとグループは、ルールやイベント検索など、システムの Web インターフェイスのさまざまな場所で使用できます。たとえば、特定の VLAN だけに適用されるアクセス コントロール ルールを作成することができます。

VLAN タグ オブジェクトの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin Access Admin Network Admin

ステップ 1 **[Objects]** > **[Object Management]** を選択します。

ステップ 2 オブジェクト タイプのリストから [VLAN タグ（VLAN Tag）] を選択します。

ステップ 3 [VLAN タグの追加（Add VLAN Tag）] ドロップダウン リストで、[オブジェクトの追加（Add Object）] を選択します。

ステップ 4 名前を入力します。

ステップ 5 [説明（Description）] を入力します。

ステップ 6 [VLAN タグ（VLAN Tag）] フィールドに値を入力します。VLAN タグの範囲を指定するには、ハイフンを使用します。

ステップ 7 オブジェクトのオーバーライドを管理します。

- このオブジェクトのオーバーライドを許可する場合は、[Allow Overrides] チェックボックスをオンにします（オブジェクトのオーバーライドの許可 （524 ページ）を参照）。
- このオブジェクトにオーバーライド値を追加する場合は、[Override] セクションを展開し、[Add] をクリックします（オブジェクトのオーバーライドの追加 （524 ページ）を参照）。

ステップ 8 **[保存（Save）]** をクリックします。

次のタスク

- アクティブ ポリシーがオブジェクトを参照する場合は、設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

セキュリティ グループ タグ オブジェクト

セキュリティ グループ タグ（SGT）オブジェクトは、単一の SGT 値を指定します。ルールで SGT オブジェクトを使用して、Cisco ISE で割り当てられたものでは**ない** SGT 属性を持つトラフィックを制御できます。SGT オブジェクトをグループ化またはオーバーライドすることはできません。

関連トピック

カスタム セキュリティ グループ タグ（SGT）から ISE セキュリティ グループ タグ（SGT）への自動遷移 （496 ページ）

カスタム SGT 条件 （495 ページ）
ISE SGT とカスタム SGT ルール条件との比較 （496 ページ）

セキュリティ グループ タグ オブジェクトの作成

スマートライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	Control	いずれか（Any）	グローバルだけ	Admin/Access Admin/Network Admin

始める前に

- ISE/ISE-PIC 接続を無効にします。アイデンティティ ソースとして ISE/ISE-PIC を使用している場合は、カスタム SGT オブジェクトを作成することはできません。

ステップ 1 **[Objects]** > **[Object Management]**を選択します。
ステップ 2 オブジェクト タイプのリストから [セキュリティ グループ タグ（Security Group Tag）] を選択します。
ステップ 3 [Add Security Group Tag] をクリックします。
ステップ 4 [Name] を入力します。
ステップ 5 （任意）[Description] に説明を入力します。
ステップ 6 [タグ（Tag）] フィールドに、単一の SGT を入力します。
ステップ 7 **[保存（Save）]** をクリックします。

次のタスク

- アクティブ ポリシーがオブジェクトを参照する場合は、設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

関連トピック

カスタム セキュリティ グループ タグ（SGT）から ISE セキュリティ グループ タグ（SGT）への自動遷移 （496 ページ）
カスタム SGT 条件 （495 ページ）
ISE SGT とカスタム SGT ルール条件との比較 （496 ページ）

URL オブジェクト

設定した各 URL オブジェクトは、単一の URL または IP アドレスを表します。URL オブジェクトとグループは、アクセス コントロール ポリシーやイベント検索など、システムの Web イ

ンターフェイスのさまざまな場所で使用できます。たとえば、特定の Web サイトをブロックするアクセス コントロール ルールを作成することができます。

URL オブジェクトを作成する際に、特に暗号化トラフィックを復号化またはブロックする SSL インスペクションを設定しない場合は、次の事項に留意してください。

- アクセス コントロール ルールで URL オブジェクトを使用して HTTPS トラフィックを照合することを計画している場合は、トラフィックの暗号化に使用される公開キー証明書内でサブジェクトの共通名を使用するオブジェクトを作成します。なお、システムはサブジェクトの共通名に含まれるドメインを無視するため、サブドメイン情報は含めないでください。たとえば、www.example.com ではなく、example.com を使用します。
- URL 条件を含むアクセス コントロール ルールを使用して Web トラフィックを照合する場合、システムは暗号化プロトコル（HTTP 対 HTTPS）を無視します。つまり、アプリケーション条件を使用してルールを調整しない限り、Web サイトをブロックすると、その Web サイトへの HTTP と HTTPS の両方のトラフィックがブロックされます。URL オブジェクトを作成する場合は、オブジェクトの作成時にプロトコルを指定する必要はありません。たとえば、`http://example.com/` ではなく、`example.com` を使用します。

URL オブジェクトの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Access Admin/Network Admin

ステップ 1 **[Objects]** > **[Object Management]**を選択します。

ステップ 2 オブジェクト タイプのリストから [URL] を選択します。

ステップ 3 [URL の追加（Add URL）] ドロップダウン リストで、[オブジェクトの追加（Add Object）] を選択します。

ステップ 4 [Name] を入力します。

マルチドメイン展開では、オブジェクト名をドメイン階層内で一意にする必要があります。システムは、現在のドメインでは表示できないオブジェクトの名前との競合を特定することができます。

ステップ 5 （任意）[Description] に説明を入力します。

ステップ 6 [URL] に、URL または IP アドレスを入力します。

ステップ 7 オブジェクトのオーバーライドを管理します。

- このオブジェクトのオーバーライドを許可する場合は、[Allow Overrides] チェックボックスをオンにします（オブジェクトのオーバーライドの許可 （524 ページ）を参照）。
- このオブジェクトにオーバーライド値を追加する場合は、[Override] セクションを展開し、[Add] をクリックします（オブジェクトのオーバーライドの追加 （524 ページ）を参照）。

ステップ 8 **[保存（Save）]** をクリックします。

次のタスク

- アクティブ ポリシーがオブジェクトを参照する場合は、設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

地理位置情報オブジェクト

設定済みの位置情報（ジオロケーション）オブジェクトは、モニタ対象ネットワーク上のトラフィックの送信元または宛先としてシステムで識別された 1 つ以上の国または大陸を表します。アクセス コントロール ポリシー、SSL ポリシー、イベント検索など、システムの Web インターフェイスのさまざまな場所で位置情報オブジェクトを使用できます。たとえば、特定の国が送信元/宛先であるトラフィックをブロックするアクセス コントロール ルールを作成できます。

常に最新の情報を使用してネットワーク トラフィックをフィルタ処理できるように、地理位置情報データベース（GeoDB）を定期的に更新することを強くお勧めします。

地理位置情報オブジェクトの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Access Admin/Network Admin

ステップ 1 **[Objects]** > **[Object Management]**を選択します。

ステップ 2 オブジェクト タイプのリストから [地理位置情報（Geolocation）] を選択します。

ステップ 3 [位置情報の追加（Add Geolocation）] をクリックします。

ステップ 4 名前を入力します。

マルチドメイン展開では、オブジェクト名をドメイン階層内で一意にする必要があります。システムは、現在のドメインでは表示できないオブジェクトの名前との競合を特定することができます。

ステップ 5 地理位置情報オブジェクトに含める国および大陸のチェック ボックスを選択します。大陸を選択すると、その大陸内のすべての国、およびGeoDB 更新によってその大陸に今後追加されるすべての国が選択されます。大陸の下でいずれかの国を選択解除すると、その大陸が選択解除されます。国と大陸を任意に組み合わせて選択できます。

ステップ 6 **[保存（Save）]** をクリックします。

次のタスク

- アクティブ ポリシーがオブジェクトを参照する場合は、設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

インターフェイス オブジェクト：インターフェイスグループとセキュリティ ゾーン

インターフェイス オブジェクトは、ネットワークをセグメント化してトラフィック フローを制御し、分類しやすくします。インターフェイス オブジェクトは単にインターフェイスをグループ化します。これらのグループは複数のデバイスにまたがることがあります。また、単一のデバイスに複数のインターフェイス オブジェクトを設定することもできます。

インターフェイス オブジェクトには次の 2 つのタイプがあります。

- セキュリティ ゾーン：インターフェイスは、1 つのセキュリティ ゾーンにのみ属することができます。
- インターフェイス グループ：インターフェイスは複数のインターフェイスグループ（および 1 つのセキュリティ ゾーン）に属することができます。

  Firepower Threat Defense NAT ポリシー、プレフィルタ ポリシー、および QoS ポリシーでインターフェイス グループを使用できます。

トンネルゾーンはインターフェイス オブジェクトではありませんが、特定の設定ではセキュリティ ゾーンの代わりにトンネルゾーンを使用できます。トンネル ゾーンおよびプレフィルタリング （1777 ページ）を参照してください。

インターフェイス オブジェクト内のすべてのインターフェイスが同じタイプ（すべてインライン、パッシブ、スイッチド、ルーテッド、または ASA FirePOWER）である必要があります。インターフェイス オブジェクトを作成した後、それに含まれるインターフェイスのタイプを変更することはできません。

オブジェクト マネージャのインターフェイス オブジェクトのページでは、管理対象デバイスで設定されているセキュリティ ゾーンとインターフェイス グループの一覧が表示されます。また、このページには、各インターフェイス オブジェクトのタイプも表示され、各インターフェイス オブジェクトを展開すると、どのデバイスのどのインターフェイスが各オブジェクトに属するかを表示できます。

（注） インラインセットでインターフェイスのセキュリティ ゾーンを追加する前に、インラインセットを作成します。作成しない場合、セキュリティ ゾーンが削除されるため再度追加する必要があります。

モデル固有の注意事項および警告

7000 または 8000 シリーズ デバイスの初期設定時に、システムはデバイス用に選択した検出モードに基づいてセキュリティ ゾーンを作成します。たとえば、パッシブ展開ではシステムはパッシブ ゾーンを作成し、インライン展開では外部ゾーンと内部ゾーンを作成します。Firepower Management Center にデバイスを登録すると、これらのセキュリティ ゾーンが FMC に追加されます。

ASA FirePOWER セキュリティ コンテキストの変更（シングル コンテキスト モードからマルチ コンテキスト モードへの変更、またはその逆の変更）をすると、割り当てられているセキュリティ ゾーンからデバイスのすべてのインターフェイスがシステムによって削除されます。

インターフェイス オブジェクトとマルチテナンシー

マルチドメイン展開では、どのレベルでもインターフェイス オブジェクトを作成できます。先祖ドメインで作成されたインターフェイス オブジェクトには別のドメインのデバイスに存在するインターフェイスが含まれる場合があります。この状況において、オブジェクト マネージャ内の先祖のインターフェイス オブジェクトの設定を表示するサブドメイン ユーザには、当該ドメインのインターフェイスのみが確認できます。

ロールによって制限されない限り、サブドメインのユーザは先祖ドメインで作成されたインターフェイス オブジェクトを表示**および**編集できます。サブドメインのユーザは、これらのインターフェイス オブジェクトにインターフェイスの追加や削除を行えます。ただし、インターフェイス オブジェクトの削除や名称変更はできません。子孫ドメインで作成されたインターフェイス オブジェクトの表示や編集はできません。

セキュリティ ゾーンおよびインターフェイス グループ オブジェクトの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	セキュリティ ゾーン：任意 インターフェイス グループ：Firepower Threat Defense	いずれか（Any）	Admin/Access Admin/Network Admin

ヒント　空のインターフェイス オブジェクトを作成し、後からインターフェイスを追加できます。インターフェイスを追加するには、インターフェイスに名前が付いている必要があります。**[Devices]**> **[Device Management]** でインターフェイスを設定しているときに、セキュリティ ゾーンを作成することもできます（インターフェイス グループは作成できません）。

始める前に

- 各種インターフェイス オブジェクトの使用要件および制限を理解します。インターフェイス オブジェクト：インターフェイスグループとセキュリティ ゾーン （535 ページ）を参照してください。
- 必要なインターフェイス オブジェクトを慎重に決定します。既存のセキュリティ ゾーンをインターフェイス グループに、またはその逆に変更することはできません。代わりに、新しいインターフェイス オブジェクトを作成する必要があります。

ステップ 1 **[Objects]** > **[Object Management]**を選択します。

ステップ 2 オブジェクト タイプのリストから、**[インターフェイス（Interface）]** を選択します。

ステップ 3 **[追加（Add）]**>**[セキュリティ ゾーン（Security Zone）]** または **[追加（Add）]**>**[インターフェイス グループ（Interface Group）]** をクリックします。

ステップ 4 名前を入力します。

ステップ 5 [インターフェイス タイプ（Interface Type）] を選択します。

ステップ 6 **[デバイス（Device）]** > **[インターフェイス（Interfaces）]** ドロップダウン リストから、追加するインターフェイスを含むデバイスを選択します。

セキュリティ ゾーンを作成または編集すると、[デバイス（Device）] > [インターフェイス（Interfaces）] ドロップダウン リストに、ハイ アベイラビリティ デバイスのクラスタ名が表示されます。追加するインターフェイスを含むクラスタを選択します。

ステップ 7 1 つ以上のインターフェイスを選択します。

ステップ 8 [追加（Add）] をクリックして、デバイス別にグループ化された、選択したインターフェイスを追加します。

ステップ 9 **[保存（Save）]** をクリックします。

次のタスク

- アクティブ ポリシーがオブジェクトを参照する場合は、設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

時間範囲オブジェクト

指定した時間にのみポリシーを適用するには、時間範囲オブジェクトを使用します。

時間範囲オブジェクトの作成

指定した時間範囲の間にのみポリシーを適用する場合は、時間範囲オブジェクトを作成してから、そのオブジェクトをポリシーで指定します。

時間範囲オブジェクトは、VPN グループ ポリシー オブジェクトでのみ指定できます。

ステップ 1 [オブジェクト（Objects）] > [オブジェクト管理（Object Management）] を選択します。

ステップ 2 オブジェクト タイプのリストから [時間範囲（Time Range）] を選択します。

ステップ 3 [時間範囲の追加（Add Time Range）] をクリックします。

ステップ 4 値を入力します。

次のガイドラインに従ってください。

- 入力したオブジェクト名の周りに赤色のエラーボックスが表示された場合は、[名前（Name）] フィールドの上にマウスを置くと名前付けの制限が表示されます。
- 時間はすべて UTC です。
- 24 時間制で時間を入力します。たとえば、1:30 PM は 13:30 と入力します。
- 通常の週末の時間（夕方および夜を含む、金曜日の 5pm から月曜日の 8am まで）など、1 つの連続する範囲を指定するには、[範囲タイプ（Range Type）] に [範囲（Range）] を選択します。
- 月曜日から金曜日の 8am から 5pm まで（各日の夕方、夜、早朝を除く）など、複数の日の一部分を指定する場合は、[範囲タイプ（Range Type）] に [日次間隔（Daily Interval）] を選択します。
- 同じ曜日の複数の非連続時間、または異なる曜日の異なる時間を指定する場合は、繰り返し間隔を複数作成します。たとえば、標準の営業時間を除くすべての時間にポリシーを適用する場合は、次の 2 つの繰り返し間隔を持つ 1 つの時間範囲オブジェクトを作成します。
  - 月曜日から金曜日の 5pm から 8am の [日次間隔（Daily Interval）]、および
  - 金曜日の 5pm から月曜日の 8am までの [範囲（Range）] の繰り返し間隔。

ステップ 5 [保存（Save）] をクリックします。

次のタスク

[アクセス時間（Access Hours）] フィールドを使用して、VPN グループ ポリシー オブジェクトに時間範囲オブジェクトを指定します。

詳細については、グループ ポリシー オブジェクトの設定 （624 ページ） および グループ ポリシーの詳細オプション （630 ページ） を参照してください。

変数セット

変数は、侵入ルールで一般的に使用される値を表し、送信元および宛先の IP アドレスおよびポートを識別します。侵入ポリシーで変数を使用して、ルール抑制、アダプティブ プロファイルの更新、および動的（ダイナミック）ルール状態で IP アドレスを表すこともできます。

ヒント プリプロセッサルールは、侵入ルールで使用されるネットワーク変数で定義されたホストにかかわらず、イベントをトリガーできます。

変数セットを使用して、変数を管理、カスタマイズ、およびグループ化します。システム提供のデフォルトの変数セットを使用することも、独自のカスタムセットを作成することもできます。いずれのセット内でも、定義済みのデフォルト変数を変更したり、ユーザ定義変数を追加および変更したりできます。

Firepowerシステムで提供する共有オブジェクトルールと標準テキストルールのほとんどで、定義済みのデフォルト変数を使用してネットワークとポート番号を定義します。たとえば、ルールの大半は、保護されたネットワークを指定するために変数 `$HOME_NET` を使用して、保護されていない（つまり外部の）ネットワークを指定するために変数 `$EXTERNAL_NET` を使用します。さらに、特殊なルールでは、他の定義済みの変数がしばしば使用されます。たとえば、Webサーバに対するエクスプロイトを検出するルールは、`$HTTP_SERVERS` 変数および `$HTTP_PORTS` 変数を使用します。

ルールがより効率的なのは、変数がユーザのネットワーク環境をより正確に反映する場合です。少なくとも、デフォルトセットにあるデフォルト変数は変更する必要があります。`$HOME_NET` などの変数がネットワークを正しく定義し、`$HTTP_SERVERS` にネットワーク上のすべてのWebサーバが含まれていれば、処理は最適化され、疑わしいアクティビティがないかどうかすべての関連システムがモニタされます。

変数を使用するには、変数セットをアクセス コントロール ルールまたはアクセス コントロール ポリシーのデフォルト アクションに関連付けられている侵入ポリシーにリンクします。デフォルトでは、デフォルトの変数セットは、アクセス コントロール ポリシーによって使用されるすべての侵入ポリシーにリンクされています。

変数を任意のセットに追加すると、それはすべてのセットに追加されます。つまり、各変数セットは、システムで現在設定されているすべての変数のコレクションになります。どの変数セット内でも、ユーザ定義変数を追加し、任意の変数の値をカスタマイズすることができます。

Firepowerシステムでは、初めに定義済みのデフォルト値で構成された単一のデフォルトの変数セットを提供します。デフォルトセット内の各変数は、最初はそのデフォルト値に設定されています。定義済みの変数の場合、このデフォルト値はCisco Talos Intelligence Group（Talos）によって設定され、ルール更新で提供される値です。

定義済みのデフォルト変数は、そのデフォルト値に設定されたままにすることもできますが、定義済みの変数のサブセットを変更することを推奨します。

変数はデフォルトセットでのみ使用できますが、多くの場合、1つ以上のカスタム設定を追加し、異なるセットで異なる変数の値を設定し、場合によっては新しい変数を追加することによって、最大限に活用できます。

複数のセットを使用する場合は、デフォルトのセットにある任意の変数の現在値によって、他のすべてのセットの変数のデフォルト値が決まることに注意してください。

[オブジェクト マネージャ（Object Manager）] ページで [変数セット（Variable Sets）] を選択した場合、オブジェクトマネージャには、デフォルトの変数セットと、作成したすべてのカスタム セットがリストされます。

新しくインストールされたシステムでは、デフォルトの変数セットは、Cisco で定義済みのデフォルト変数だけで構成されています。

各変数セットには、システムによって提供されるデフォルト変数と、任意の変数セットから追加したすべてのカスタム変数が含まれます。デフォルト設定は編集できますが、デフォルト セットの名前を変更したり、削除したりすることはできないことに注意してください。

マルチドメイン展開では、システムはサブドメインごとにデフォルトの変数セットを生成します。

注意 アクセス コントロールまたは侵入ポリシーをインポートすると、デフォルトの変数セットにある既存のデフォルト変数が、インポートされたデフォルト変数でオーバーライドされます。既存のデフォルト変数セットに、インポートされたカスタム変数セットに存在しないカスタム変数が含まれる場合、一意的な変数が保持されます。

関連トピック

変数の管理 （554 ページ）
変数セットの管理 （552 ページ）

侵入ポリシー内の変数セット

Firepower システムは、デフォルトではアクセス コントロール ポリシーで使用されるすべての侵入ポリシーにデフォルトの変数セットをリンクします。侵入ポリシーを使用するアクセス コントロールポリシーを展開すると、その侵入ポリシー内で有効にした侵入ルールでは、リンクされた変数セットの変数値が使用されます。

アクセス コントロール ポリシー内の侵入ポリシーで使用されるカスタム変数セットを変更すると、システムの [アクセス コントロール ポリシー（Access Control Policy）] ページで、そのポリシーのステータスが「失効（out-of-date）」と表示されます。変数セットの変更内容を実装するには、アクセス コントロール ポリシーを再度展開する必要があります。デフォルト セットを変更すると、侵入ポリシーを使用するすべてのアクセス コントロール ポリシーのステータスが「失効（out-of-date）」と表示され、変更内容を実装するにはすべてのアクセス コントロール ポリシーを再度展開する必要があります。

変数

変数は、次のカテゴリのいずれかに属します。

デフォルト変数

Firepower システムから提供される変数。デフォルト変数の名前変更または削除はできません。また、デフォルト値を変更することもできません。ただし、デフォルト変数のカスタマイズしたバージョンを作成できます。

カスタマイズされた変数

作成した変数。この変数には、次の変数があります。

- カスタマイズされたデフォルト変数

  デフォルト変数の値を編集すると、システムはその変数を[デフォルトの変数（Default Variables）] 領域から [カスタマイズされた変数（Customized Variables）] 領域に移動します。デフォルト セットの変数値によってカスタム セットの変数のデフォルト値が決まるため、デフォルトセットのデフォルト変数をカスタマイズすると、他のすべてのセットの変数のデフォルト値が変更されます。

- ユーザ定義変数

  独自の変数を追加および削除したり、異なる変数セット内の値をカスタマイズしたり、カスタマイズされた変数をそのデフォルト値にリセットしたりできます。ユーザ定義変数をリセットすると、それは[カスタマイズされた変数（Customized Variables）] 領域に残ります。

  ユーザ定義変数は、次のいずれかのタイプにできます。

  - ネットワーク変数は、ネットワーク トラフィックのホストの IP アドレスを指定します。
  - ポート 変数は、ネットワーク トラフィックの TCP または UDP ポートを指定するもので、いずれかのタイプを意味する値 `any` を指定することもできます。

たとえば、カスタム標準テキストルールを作成する場合、独自のユーザ定義変数を追加して、トラフィックをより正確に反映したり、ショートカットとしてルール作成プロセスを単純化したりすることもできます。また、「緩衝地帯」（つまり DMZ）でのみトラフィックを検査するルールを作成する場合、公開されているサーバの IP アドレスが値にリストされる `$DMZ` という変数を作成することもできます。こうして、この地帯で作成された任意のルールで `$DMZ` 変数を使用できます。

拡張変数

特定の条件下で Firepower システムから提供される変数。この変数が含まれる展開は非常に限定的です。

定義済みデフォルト変数

デフォルトでは、Firepower System は、1 つのデフォルト変数セットを提供します。このセットは、定義済みのデフォルト変数から構成されています。Cisco Talos Intelligence Group（Talos）では、ルール更新を使用し、新しい侵入ルールや更新された侵入ルール、他の侵入ポリシーエレメント（デフォルト変数など）を提供します。

システムが提供する侵入ルールの多くが定義済みのデフォルト変数を使用していることから、これらの変数に関する適切な値を設定します。変数セットを使用してネットワーク上のトラフィックを特定する方法によっては、任意またはすべての変数セットにあるこれらのデフォルト変数の値を変更できます。

注意 アクセス コントロールまたは侵入ポリシーをインポートすると、デフォルトの変数セットにある既存のデフォルト変数が、インポートされたデフォルト変数でオーバーライドされます。既存のデフォルト変数セットに、インポートされたカスタム変数セットに存在しないカスタム変数が含まれる場合、一意的な変数が保持されます。

次の表では、システムによって提供される変数について説明し、通常、いずれの変数が変更されるかを示します。変数をご使用のネットワークに合わせて調整する方法を決定するには、プロフェッショナル サービスまたはサポートに問い合わせてください。

表 *63*: システム提供変数

変数名	説明	変更しますか
$AIM_SERVERS	既知の AOL Instant Messenger（AIM）サーバを定義し、チャット ベースのルールおよび AIM エクスプロイトを検索するルールで使用されます。	不要。
$DNS_SERVERS	ドメイン ネーム サービス（DNS）サーバを定義します。DNS サーバに特に影響するルールを作成する場合、$DNS_SERVERS 変数を宛先または送信元 IP アドレスとして使用できます。	現在のルール セットでは不要です。
$EXTERNAL_NET	Firepower System が非保護ネットワークとして表示されるネットワークを定義し、外部ネットワークを定義する多くのルールで使用されます。	はい。$HOME_NET を適切に定義してから、$EXTERNAL_NET の値として $HOME_NET を除外する必要があります。
$FILE_DATA_PORTS	ネットワーク ストリームでファイルを検出する侵入ルールで使用される、暗号化されていないポートを定義します。	不要。
$FTP_PORTS	ネットワーク上の FTP サーバのポートを定義し、FTP サーバのエクスプロイト ルールに使用されます。	はい。FTP サーバがデフォルト ポート以外のポートを使用する場合（web インターフェイスのデフォルト ポートを表示できます）。

変数名	説明	変更しますか
$GTP_PORTS	パケット デコーダが GTP（General Packet Radio Service（GPRS）トンネリング プロトコル）PDU内部でペイロードを取得するデータ チャネル ポートを定義します。	不要。
$HOME_NET	関連した侵入ポリシーが監視するネットワークを定義し、内部ネットワークを定義するために多くのルールで使用されます。	内部ネットワークのIPアドレスを指定する場合は変更します。
$HTTP_PORTS	ネットワーク上のWebサーバのポートを定義し、Webサーバのエクスプロイト ルールに使用されます。	はい。webサーバがデフォルト ポート以外のポートを使用する場合（webインターフェイスのデフォルト ポートを表示できます）。
$HTTP_SERVERS	ネットワーク上のWebサーバを定義します。Web サーバのエクスプロイト ルールで使用されます。	HTTP サーバを実行する場合は変更します。
$ORACLE_PORTS	ネットワーク上でOracleデータベース サーバのポートを定義し、Oracle データベースでの攻撃をスキャンするルールで使用されます。	Oracle サーバを実行する場合は変更します。
$SHELLCODE_PORTS	システムにシェルコードのエクスプロイトをスキャンさせるポートを定義し、シェルコードを使用するエクスプロイトを検出するルールで使用されます。	不要。
$SIP_PORTS	ネットワーク上の SIP サーバのポートを定義し、SIP のエクスプロイト ルールに使用されます。	不要。
$SIP_SERVERS	ネットワーク上で SIP サーバを定義し、SIP をターゲットとしたエクスプロイトを解決するルールで使用されます。	はい。SIP サーバを実行している場合は、$HOME_NET を適切に定義してから、$SIP_SERVERS の値として $HOME_NET を含める必要があります。
$SMTP_SERVERS	ネットワーク上でSMTPサーバを定義し、メールサーバをターゲットとするエクスプロイトを解決するルールで使用されます。	SMTP サーバを実行する場合は変更します。

変数名	説明	変更しますか
$SNMP_SERVERS	ネットワーク上でSNMPサーバを定義し、SNMPサーバでの攻撃をスキャンするルールで使用されます。	SNMPサーバを実行する場合は変更します。
$SNORT_BPF	その後バージョン5.3.0以降にアップグレードされるバージョン5.3.0以前のFirepower Systemソフトウェア リリースのシステム上に存在する場合のみに表示されるレガシー拡張変数を特定します。	変更しません。この変数は表示または削除のみが可能です。削除後に、編集または復元することはできません。
$SQL_SERVERS	ネットワーク上でデータベース サーバを定義し、データベースをターゲットとしたエクスプロイトを解決するルールで使用されます。	SQLサーバを実行する場合は変更します。
$SSH_PORTS	ネットワーク上のSSHサーバのポートを定義し、SSHサーバのエクスプロイト ルールに使用されます。	はい。デフォルト ポート以外のSSHサーバのポートを使用する場合（webインターフェイスでのデフォルトポートを表示できます）。
$SSH_SERVERS	ネットワーク上でSSHサーバを定義し、SSHをターゲットとしたエクスプロイトを解決するルールで使用されます。	はい。SSHサーバを実行している場合は、$HOME_NETを適切に定義してから、$SSH_SERVERSの値として$HOME_NETを含める必要があります。
$TELNET_SERVERS	ネットワーク上で既知のTelnetサーバを定義し、Telnetサーバをターゲットとしたエクスプロイトを解決するルールで使用されます。	Telnetサーバを実行する場合は変更します。
$USER_CONF	Webインターフェイスを介して利用可能できる場合を除き、1つ以上の特徴を設定できる一般的なツールを提供します。 $USER_CONFの設定が競合または重複していると、システムは停止します。	機能の説明で指示されている場合や、サポートによる指示があった場合を除き、変更しません。

ネットワーク変数

ネットワーク変数で表されるIPアドレスを、侵入ポリシーで有効にした侵入ルール、侵入ポリシー ルール抑制、動的ルール状態、およびアダプティブ プロファイルの更新で使用することができます。ネットワーク変数とネットワーク オブジェクトおよびネットワーク オブジェクト グループとの相違点として、ネットワーク変数は侵入ポリシーおよび侵入ルールに固有の

ものです。一方、ネットワーク オブジェクトおよびグループを使用すると、アクセス コントロールポリシー、ネットワーク変数、侵入ルール、ネットワーク検出ルール、イベント検索、レポートなど、システムの Web インターフェイスのさまざまな場所で IP アドレスを表すことができます。

次の設定でネットワーク変数を使用して、ネットワーク上のホストの IP アドレスを指定できます。

- 侵入ルール：侵入ルールの [送信元 IP（Source IPs）] および [宛先 IP（Destination IPs）] 見出しフィールドを使用すると、パケット インスペクションを、特定の送信元または宛先 IP アドレスを持つパケットに制限することができます。
- 抑制：送信元または宛先の侵入ルール抑制の [ネットワーク（Network）] フィールドを使用すると、特定の 1 つの IP アドレスまたは IP アドレス範囲が侵入ルールやプリプロセッサをトリガーした場合の侵入イベント通知を抑制できます。
- 動的ルール状態：送信元または宛先の動的ルール状態の [ネットワーク（Network）] フィールドを使用すると、指定時間内に発生した侵入ルールやプリプロセッサ ルールの一致数が多すぎる場合に、それを検出できます。
- アダプティブ プロファイルの更新：アダプティブ プロファイルの更新が有効にされている場合、アダプティブ プロファイルの [ネットワーク（Networks）] フィールドに、パッシブ展開でパケット フラグメントおよび TCP ストリームのリアセンブルを改善する必要があるホストが示されます。

このセクションで示されるフィールドで変数を使用する場合、侵入ポリシーにリンクされた変数セットは、侵入ポリシーを使用するアクセス コントロールポリシーで処理されるネットワーク トラフィックでの変数値を決定します。

次のネットワーク設定を任意に組み合わせて変数に追加できます。

- 使用可能なネットワーク リストから選択したネットワーク変数、ネットワーク オブジェクト、およびネットワーク オブジェクト グループの任意の組み合わせ
- [新規変数（New Variable）] または [変数の編集（Edit Variable）] ページから追加した個々のネットワーク オブジェクト（独自の変数や、他の既存の変数、さらに今後の変数にこれらを追加できます）
- リテラルの単一 IP アドレスまたはアドレス ブロック

  それぞれを個別に追加することにより、複数のリテラル IP アドレスとアドレス ブロックをリストできます。IPv4 および IPv6 アドレスとアドレス ブロックを単独で、または任意に組み合わせてリストできます。IPv6 アドレスを指定するときには、RFC 4291 で定義された任意のアドレス指定規則を使用できます。

追加する変数での包含ネットワークのデフォルト値は `any` で、これは任意の IPv4 または IPv6 アドレスを示します。除外ネットワークのデフォルト値は `none` で、ネットワークがないことを示しています。また、リテラル値の中でアドレス `::` を指定すると、包含ネットワーク リストで任意の IPv6 アドレスを指定でき、除外リストでは IPv6 アドレスなしを指定できます。

除外リストにネットワークを追加すると、指定されたアドレスおよびアドレスブロックが拒否されます。つまり、除外された IP アドレスやアドレス ブロックを除き、任意の IP アドレスに一致させることができます。

たとえば、リテラル アドレス `192.168.1.1` を除外すると 192.168.1.1 以外の任意の IP アドレスが指定され、`2001:db8:ca2e::fa4c` を除外すると 2001:db8:ca2e::fa4c 以外の任意の IP アドレスが指定されます。

リテラル ネットワークまたは使用可能なネットワークを任意に組み合わせて、除外で使用できます。たとえば、リテラル値 `192.168.1.1` および `192.168.1.5` を除外すると、192.168.1.1 と 192.168.1.5 以外の任意の IP アドレスが含まれます。つまり、システムはこの構文を「192.168.1.1 **でなく、しかも** 192.168.1.5 **でない**」と解釈し、大カッコ内に列挙されたものを除くすべての IP アドレスに一致させます。

ネットワーク変数を追加または編集するときには、次の点に注意してください。

- 論理的に言って、値 `any` を除外することはできません。any を除外すると「アドレスなし」を意味することになります。たとえば、除外ネットワーク リストに、値 `any` を持つ変数を追加することはできません。
- ネットワーク変数は、指定された侵入ルールおよび侵入ポリシー機能に関するトラフィックを識別します。プリプロセッサ ルールは、侵入ルールで使われているネットワーク変数で定義されたホストとは無関係に、イベントをトリガーできることに注意してください。
- 除外される値は、包含される値のサブセットに解決される必要があります。たとえば、アドレス ブロック 192.168.5.0/24 を包含し、192.168.6.0/24 を除外することはできません。

ポート変数

ポート変数は、侵入ポリシーで有効になった侵入ルールの [送信元ポート（Source Port）] および [宛先ポート（Destination Port）] ヘッダー フィールドで使用できる TCP ポートと UDP ポートを表します。ポート変数とポート オブジェクトおよびポート オブジェクト グループとの相違点は、ポート変数が侵入ルール固有のものであることです。TCP や UDP 以外のプロトコル用にポート オブジェクトを作成して、ポート変数、アクセス コントロール ポリシー、ネットワーク検出ルール、イベント検索など、システムの Web インターフェイスのさまざまな場所で使用できます。

侵入ルールの [送信元ポート（Source Port）] および [宛先ポート（Destination Port）] ヘッダー フィールドでポート変数を使用すると、パケット インスペクションを特定の送信元または宛先 TCP/UDP ポートを持つパケットに制限することができます。

これらのフィールドで変数を使用した場合、アクセス コントロール ルールまたはポリシーに関連付けられた侵入ポリシーにリンクされる変数セットは、アクセス コントロール ポリシーが展開されるネットワーク トラフィックでのこれらの変数の値を決定します。

次のポート設定を任意に組み合わせて変数に追加できます。

- 使用可能なポート リストから選択したポート変数およびポート オブジェクトの任意の組み合わせ

使用可能なポート リストには、ポート オブジェクト グループが表示されず、したがってこれらを変数に追加できないことに注意してください。

- [新規変数（New Variable）] または [変数の編集（Edit Variable）] ページから追加した個々のポート オブジェクト（独自の変数や、他の既存の変数、さらに今後の変数にこれらを追加できます）

  有効な変数値は TCP および UDP ポートのみです（どちらのタイプでも値 `any` を含む）。新しい変数のページまたは変数の編集ページを使用して、有効な変数値ではない有効なポート オブジェクトを追加した場合、オブジェクトはシステムに追加されますが、使用可能なオブジェクト リストには表示されません。オブジェクト マネージャを使用して、変数で使われるポート オブジェクトを編集する場合、有効な変数値にのみ値を変更できます。

- 単一のリテラル ポート値とポート範囲

  ポート範囲はダッシュ（-）を使って区切る必要があります。下位互換性のために、コロンで指定されるポート範囲もサポートされていますが、作成するポート変数ではコロンを使用できません。

  複数のリテラル ポートの値および範囲をリストするには、それぞれを個別に追加して任意に組み合わることができます。

ポート変数を追加または編集するときには、次の点に注意してください。

- 追加する変数での包含ポートのデフォルト値は `any` で、これは任意のポートまたはポート範囲を示します。除外ポートのデフォルト値は `none` で、ポートがないことを示しています。

  ヒント 値 `any` を持つ変数を作成するには、特定の値を追加せずに変数に名前を付けて保存します。

- 論理的に言って、値 `any` を除外することはできません。any を除外すると「ポートなし」を意味することになります。たとえば、値 `any` を持つ変数を除外ポート リストに追加した場合、変数セットを保存することはできません。
- 除外リストにポートを追加すると、指定されたポートおよびポート範囲が拒否されます。つまり、除外されたポートまたはポート範囲を除き、任意のポートに一致させることができます。
- 除外される値は、包含される値のサブセットに解決される必要があります。たとえば、ポート範囲 10 から 50 を包含し、ポート 60 を除外することはできません。

拡張変数

拡張変数を使用すると、他の方法では Web インターフェイスで設定できない機能を設定することができます。現在、Firepower システムで提供されている拡張変数は、USER_CONF 変数のみです。

USER_CONF

USER_CONF は、Web インターフェイスで通常設定できない 1 つ以上の機能を設定するための汎用ツールです。

注意 機能の説明またはサポート担当の指示に従う場合を除き、拡張変数USER_CONF を使用して侵入ポリシー機能を設定**しないで**ください。競合または重複する設定が存在すると、システムが停止します。

USER_CONF を編集するときには、1 行に合計 4096 文字まで入力できます。行は自動的に折り返します。変数の最大長 8192 文字、またはディスク スペースなどの物理制限に達するまで、任意の数の有効な指示または行数を含めることができます。コマンドディレクティブでは、完全な引数の後にバックスラッシュ（\）行連結文字を使用します。

USER_CONF をリセットすると、空になります。

変数のリセット

変数セットの新しい変数ページまたは変数の編集ページで、変数をデフォルト値にリセットできます。次の表に、変数をリセットするときの基本原則を要約します。

表 *64 :* 変数のリセット値

リセットする変数のタイプ	それが含まれるセット タイプ	リセット後の値
デフォルト	デフォルト	ルール更新値
ユーザ定義	デフォルト	任意
デフォルトまたはユーザ定義	カスタム	現在のデフォルト セット値（変更/未変更にかかわらず）

カスタム セットの変数をリセットすると、単にデフォルト セット内のその変数の現在値にリセットされます。

逆に、デフォルト セットの変数の値をリセットまたは変更すると、すべてのカスタム セット内のその変数のデフォルト値が常に更新されます。リセットアイコンがグレー表示され、その変数をリセットできないことを示している場合、そのセットでは変数のカスタマイズ値が存在しないことを意味します。カスタム セット内の変数の値をすでにカスタマイズした場合を除き、デフォルトセットの変数を変更すると、変数セットがリンクされた侵入ポリシーで使われている値が更新されます。

（注） デフォルト セット内の変数を変更する際は、リンクされたカスタム セットの変数を使用している侵入ポリシーが、その変更によってどのような影響を受けるかを評価することをお勧めします（特に、カスタム セット内の変数値をまだカスタマイズしていない場合）。

変数セット内のリセット アイコン（）の上にポインタを置くと、リセット値を確認できます。カスタマイズされた値とリセット値が同じである場合は、次のいずれかを示しています。

- カスタム セットまたはデフォルト セットの中で、値 any を持つ変数を追加した
- カスタムセットの中で、明示的な値を持つ変数を追加し、設定した値をデフォルト値として使用することを選択した

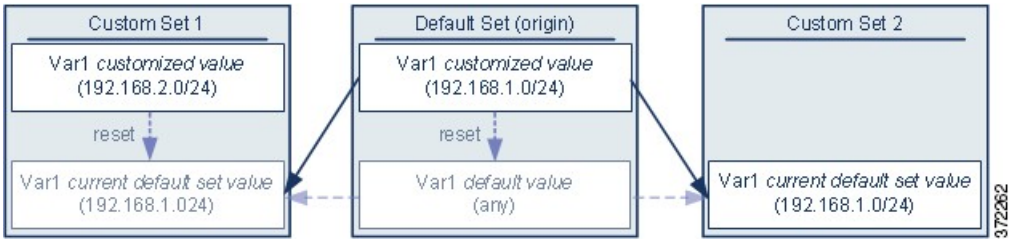
セットに変数を追加する

変数セットに変数を追加すると、他のすべてのセットにもその変数が追加されます。カスタムセットから変数を追加する場合は、設定値をデフォルトセットのカスタマイズ値として使用するかどうかを選択する必要があります。

- 設定値（たとえば、192.168.0.0/16）を**使用する**場合、変数は、デフォルト値 any を持つカスタマイズ値として設定値を使用するデフォルトセットに追加されます。デフォルトセットの現在の値によって他のセットのデフォルト値が決まるため、他のカスタムセットの初期のデフォルト値は設定値（この例では 192.168.0.0/16）になります。
- 設定値を**使用しない**場合、変数はデフォルト値 any のみを使用してデフォルトセットに追加され、こうして、他のカスタム セットの初期のデフォルト値は any になります。

例：デフォルト セットへのユーザ定義変数の追加

次の図は、値が 192.168.1.0/24 のデフォルト セットにユーザ定義の変数 Var1 を追加した場合のセットのインタラクションを示しています。



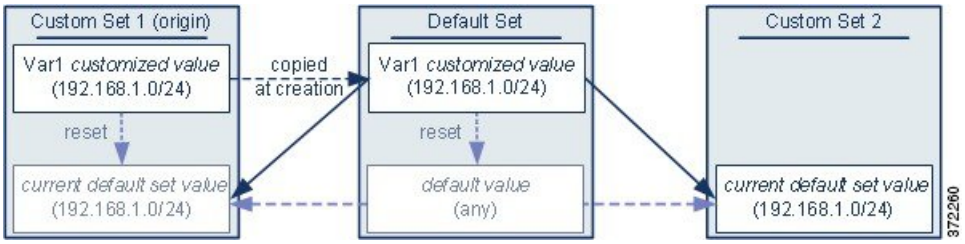
任意のセットで Var1 の値をカスタマイズできます。Var1 がカスタマイズされていない Custom Set 2 では、この値は 192.168.1.0/24 です。Custom Set 1 では、Var1 のカスタマイズ値 192.168.2.0/24 はデフォルト値をオーバーライドします。デフォルトセットのユーザ定義変数をリセットすると、すべてのセットのそのデフォルト値が any にリセットされます。

この例では、Custom Set 2 で Var1 を更新しなかった場合、デフォルト セットで Var1 をカスタマイズまたはリセットすると、Custom Set 2 の現在のデフォルト値 Var1 が更新され、変数セットにリンクされているすべての侵入ポリシーに影響を与えることに注意してください。

この例では示されていませんが、セット間のインタラクションは、デフォルトセットのデフォルト変数をリセットすると現在のルール更新で Cisco によって設定された値に、そのデフォルト変数がリセットされること以外は、ユーザ定義変数およびデフォルト変数で同じであることに注意してください。

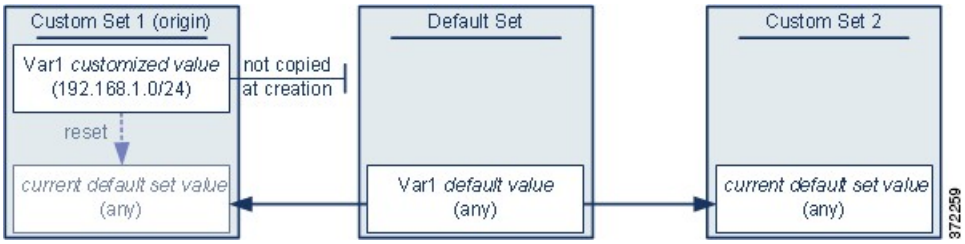
例：カスタム セットへのユーザ定義変数の追加

次の2つの例は、カスタムセットにユーザ定義変数を追加した場合の変数セットのインタラクションについて示しています。新しい変数を保存すると、設定値を他のセットのデフォルト値として使用するかどうかを尋ねるプロンプトが出されます。次の例では、設定値を**使用する**という選択がなされています。



Custom Set 1 からの `Var1` の発信元を除き、この例は `Var1` をデフォルト セットに追加した上述の例と同じであることに注意してください。`Var1` のカスタマイズ値 `192.168.1.0/24` を Custom Set 1 に追加すると、値はデフォルト値 `any` を持つカスタマイズ値としてデフォルト セットにコピーされます。その後、`Var1` の値とインタラクションは、`Var1` をデフォルト セットに追加した場合と同じになります。前述の例と同様、デフォルト セットで `Var1` をカスタマイズまたはリセットすると、Custom Set 2 の現在のデフォルト値 `Var1` が更新され、変数セットにリンクされているすべての侵入ポリシーに影響を与えることに注意してください。

次の例では、前述の例にあるように値が 192.168.1.0/24 の `Var1` を Custom Set 1 に追加しますが、`Var1` の設定値を他のセットのデフォルト値として**使用しない**ことを選択します。



このアプローチでは、`Var1` をデフォルト値 `any` を持つすべてのセットに追加します。`Var1` を追加したら、任意のセットでその値をカスタマイズできます。このアプローチの利点は、デフォルト セットで `Var1` を最初にカスタマイズしないことによって、デフォルト セットの値をカスタマイズし、`Var1` をカスタマイズしていない Custom Set 2 などのセット内の現在の値を意図せずに変更してしまうリスクが軽減されます。

変数のネスト

循環したネストにならない限り、変数をネストすることができます。否定形の変数をネストすることはできません。

有効なネストされた変数

以下の例では、SMTP_SERVERS、HTTP_SERVERS、OTHER_SERVERS がネストしても有効な変数です。

変数	タイプ（Type）	含まれるネットワーク	除外されるネットワーク
SMTP_SERVERS	カスタマイズされたデフォルト	10.1.1.1	—
HTTP_SERVERS	カスタマイズされたデフォルト	10.1.1.2	—
OTHER_SERVERS	ユーザ定義	10.2.2.0/24	—
HOME_NET	カスタマイズされたデフォルト	10.1.1.0/24 OTHER_SERVERS	SMTP_SERVERS HTTP_SERVERS

無効なネストされた変数

以下の例では、HOME_NET はネストすると無効な変数です。HOME_NET をネストすると、変数の循環になるためです。つまり、OTHER_SERVERS の定義には HOME_NET が含まれるため、HOME_NET はそれ自体でネストすることになります。

変数	タイプ（Type）	含まれるネットワーク	除外されるネットワーク
SMTP_SERVERS	カスタマイズされたデフォルト	10.1.1.1	—
HTTP_SERVERS	カスタマイズされたデフォルト	10.1.1.2	—
OTHER_SERVERS	ユーザ定義	10.2.2.0/24 HOME_NET	—
HOME_NET	カスタマイズされたデフォルト	10.1.1.0/24 OTHER_SERVERS	SMTP_SERVERS HTTP_SERVERS

ネストでサポートされない否定形の変数

否定形の変数のネストはサポートされないため、以下の例に示されているように、保護ネットワークの外部にある IP アドレスを表す変数 NONCORE_NET を使用することはできません。

変数	タイプ（Type）	含まれるネットワーク	除外されるネットワーク
HOME_NET	カスタマイズされたデフォルト	10.1.0.0/16 10.2.0.0/16 10.3.0.0/16	—
EXTERNAL_NET	カスタマイズされたデフォルト	—	HOME_NET
DMZ_NET	ユーザ定義	10.4.0.0/16	—
NOT_DMZ_NET	ユーザ定義	—	DMZ_NET
NONCORE_NET	ユーザ定義	EXTERNAL_NET NOT_DMZ_NET	—

ネストでサポートされない否定形の変数の代替手段

上記の例の代替手段として、以下に示す変数 NONCORE_NET を作成することで、保護ネットワークの外部にある IP アドレスを表すことができます。

変数	タイプ（Type）	含まれるネットワーク	除外されるネットワーク
HOME_NET	カスタマイズされたデフォルト	10.1.0.0/16 10.2.0.0/16 10.3.0.0/16	—
DMZ_NET	ユーザ定義	10.4.0.0/16	—
NONCORE_NET	ユーザ定義	—	HOME_NET DMZ_NET

変数セットの管理

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Access Admin/Network Admin

マルチドメインの展開では、現在のドメインで作成されたオブジェクトが表示されます。このオブジェクトは編集できます。先祖ドメインで作成されたオブジェクトも表示されますが、ほとんどの場合これは編集できません。子孫ドメインにあるオブジェクトを表示および編集するには、そのドメインに切り替えます。

ステップ 1 **[Objects]** > **[Object Management]**を選択します。

ステップ 2 オブジェクト タイプのリストから [変数セット（Variable Set）] を選択します。

ステップ 3 変数セットを管理します。

- 追加：カスタムの変数セットを追加するには、[変数セットの追加（Add Variable Set）] をクリックします。変数セットの作成 （553 ページ）を参照してください。
- 削除：カスタムの変数セットを削除するには、変数セットの横にある削除アイコン（）をクリックして、[はい（Yes）]をクリックします。デフォルトの変数セットまたは先祖ドメインに属している変数セットは削除できません。

  （注） 削除する変数セットで作成された変数は、別のセットで削除されたり他の方法で影響を受けることはありません。

- 編集：変数セットを編集するには、変更する変数セットの横にある編集アイコン（）をクリックします。オブジェクトの編集 （517 ページ）を参照してください。
- フィルタ処理：変数セットを名前でフィルタリングするには、名前の入力を開始します。入力中にページが更新され、一致する名前が表示されます。名前のフィルタリングをクリアするには、フィルタ フィールドにあるクリア アイコン（）をクリックします。
- 変数の管理：変数セットに含まれる変数を管理するには、変数の管理 （554 ページ）を参照してください。

変数セットの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Access Admin/Network Admin

ステップ 1 **[Objects]** > **[Object Management]**を選択します。

ステップ 2 オブジェクト タイプのリストから [変数セット（Variable Set）] を選択します。

ステップ 3 [変数セットの追加（Add Variable Set）] をクリックします。

ステップ 4 [Name] を入力します。

マルチドメイン展開では、オブジェクト名をドメイン階層内で一意にする必要があります。システムは、現在のドメインでは表示できないオブジェクトの名前との競合を特定することができます。

ステップ 5 （任意）[Description] に説明を入力します。

ステップ 6 セット内の変数を管理します（変数の管理 （554 ページ）を参照）。

ステップ 7 **[保存（Save）]** をクリックします。

次のタスク

- アクティブポリシーがオブジェクトを参照する場合は、設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

変数の管理

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Access Admin/Network Admin

マルチドメインの展開では、現在のドメインで作成されたオブジェクトが表示されます。このオブジェクトは編集できます。先祖ドメインで作成されたオブジェクトも表示されますが、ほとんどの場合これは編集できません。子孫ドメインにあるオブジェクトを表示および編集するには、そのドメインに切り替えます。

ステップ 1 **[Objects]** > **[Object Management]**を選択します。

ステップ 2 オブジェクト タイプのリストから [変数セット（Variable Set）] を選択します。

ステップ 3 編集する変数セットの横にある編集アイコン（）をクリックします。

代わりに表示アイコン（  ）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 4 変数を管理します。

- 表示：変数の完全な値を表示するには、変数の横の [値（Value）] 列内の値にポインタを重ねます。
- 追加：変数を追加するには、[追加（Add）] をクリックします。変数の追加 （555 ページ）を参照してください。
- 削除：変数の横にある削除アイコン（  ）をクリックします。変数の追加後に変数セットを保存した場合は、[はい（Yes）] をクリックして、変数の削除を確認します。

  次の変数は削除できません。

  - デフォルトの変数
  - 侵入ルールや別の変数で使用されているユーザ定義変数
  - 先祖ドメインに属している変数

- 編集：編集する変数の横にある編集アイコン（）をクリックします。変数の編集 （556 ページ）を参照してください。
- リセット：変更した変数をデフォルト値にリセットするには、変更した変数の横にあるリセット アイコン（）をクリックします。リセットアイコンがグレー表示の場合は、次のいずれかが当てはまります。
  - 現在の値がすでにデフォルト値になっている。
  - 設定が先祖ドメインに属している。

ヒント　アクティブなリセット アイコンの上にポインタを移動して、デフォルト値を表示します。

ステップ 5 [保存（Save）] をクリックして変数セットを保存します。変数セットがアクセス コントロール ポリシーで使用されている場合、[はい（Yes）] をクリックして変更の保存を確認します。

デフォルトセットの現在の値によって他のすべてのセットのデフォルト値が決まるため、デフォルトセットの変数を変更またはリセットすると、デフォルト値がカスタマイズされていない他のセットの現在の値が変更されます。

次のタスク

- アクティブ ポリシーがオブジェクトを参照する場合は、設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

変数の追加

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Access Admin/Network Admin

ステップ 1 変数セット エディタで、[追加（Add）] をクリックします。

ステップ 2 [名前（Name）] に一意の変数名を入力します。

ステップ 3 [タイプ（Type）] ドロップダウン リストから、[ネットワーク（Network）] または [ポート（Port）] を選択します。

ステップ 4 変数の値を指定します。

- 使用可能ネットワークまたはポートのリストの項目を包含リストまたは除外リストに移動する場合は、1 つまたは複数の項目を選択してドラッグアンドドロップするか、[包含（Include）] または [除外（Exclude）] をクリックします。

ヒント ネットワーク変数またはポート変数の包含リストと除外リストにあるアドレスやポートが重複している場合、除外されているアドレスまたはポートが優先されます。

- 1 つのリテラル値を入力し、[追加（Add）] をクリックします。ネットワーク変数の場合、単一の IP アドレスまたはアドレス ブロックを入力できます。ポート変数の場合、単一ポートまたはポート範囲を追加できます。ポート範囲は上限値と下限値をハイフン（-）で区切ります。複数のリテラル値を入力する場合は、必要に応じてこの手順を繰り返します。
- 包含リストまたは除外リストから項目を削除するには、項目の横にある削除アイコン（）をクリックします。

（注） ネットワーク変数の場合、包含または除外する項目のリストは、リテラル文字列や既存の変数、オブジェクト、およびネットワーク オブジェクト グループの任意の組み合わせで構成できます。

ステップ 5 [保存（Save）] をクリックして変数を保存します。カスタム セットから新しい変数を追加する場合、次のオプションがあります。

- [Yes] をクリックすると、設定値を使用する変数がデフォルト セットのカスタマイズ値として追加され、結果として他のカスタム セットのデフォルト値として追加されます。
- [いいえ（No）] をクリックすると、変数はデフォルト セットのデフォルト値 `any` として追加され、結果として他のカスタム セットのデフォルト値として追加されます。

ステップ 6 [保存（Save）] をクリックして変数セットを保存します。変更内容が保存され、変数セットにリンクされているアクセス コントロール ポリシーに失効ステータスが表示されます。

次のタスク

- アクティブ ポリシーがオブジェクトを参照する場合は、設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

変数の編集

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Access Admin/Network Admin

マルチドメインの展開では、現在のドメインで作成されたオブジェクトが表示されます。このオブジェクトは編集できます。先祖ドメインで作成されたオブジェクトも表示されますが、ほとんどの場合これは編集できません。子孫ドメインにあるオブジェクトを表示および編集するには、そのドメインに切り替えます。

カスタム変数とデフォルト変数の両方を編集できます。

既存の変数の [名前（Name）] と [タイプ（Type）] の値は変更できません。

ステップ 1 変数セット エディタで変更する変数の横にある編集アイコン（  ）をクリックします。

代わりに表示アイコン（  ）が表示される場合、設定は先祖ドメインに属しており、オブジェクトを変更する権限がありません。

ステップ 2 変数を変更します。

- 利用可能なネットワークまたはポートのリストから、含める項目のリストまたは除外する項目のリストに項目を移動するには、1つ以上の項目を選択してからドラッグアンドドロップするか、または[含める（Include）] か [除外（Exclude）] をクリックします。

  ヒント ネットワーク変数またはポート変数の包含リストと除外リストにあるアドレスやポートが重複している場合、除外されているアドレスまたはポートが優先されます。

- 1 つのリテラル値を入力し、[追加（Add）] をクリックします。ネットワーク変数の場合、単一の IP アドレスまたはアドレス ブロックを入力できます。ポート変数の場合、単一ポートまたはポート範囲を追加できます。ポート範囲は上限値と下限値をハイフン（-）で区切ります。複数のリテラル値を入力する場合は、必要に応じてこの手順を繰り返します。
- 含めるリストまたは除外リストから項目を削除するには、項目の横にある削除アイコン（  ）をクリックします。

（注） ネットワーク変数の場合、包含または除外する項目のリストは、リテラル文字列や既存の変数、オブジェクト、およびネットワーク オブジェクト グループの任意の組み合わせで構成できます。

ステップ 3 [保存（Save）] をクリックして変数を保存します。

ステップ 4 [保存（Save）] をクリックして変数セットを保存します。変数セットがアクセス コントロール ポリシーで使用されている場合、[はい（Yes）] をクリックして変更の保存を確認します。変更内容が保存され、変数セットにリンクされているアクセス コントロール ポリシーに失効ステータスが表示されます。

次のタスク

- アクティブ ポリシーがオブジェクトを参照する場合は、設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

セキュリティ インテリジェンスのリストとフィード

セキュリティ インテリジェンスのリストとフィードは、以下を収集することでトラフィックをすばやくフィルタリングするのに役立ちます。

- IP アドレスとアドレス ブロック：アクセス コントロール ポリシーでセキュリティ インテリジェンスの一部としてブラックリスト化およびホワイトリスト化するのに使用します。
- ドメイン名：DNS ポリシーでセキュリティ インテリジェンスの一部としてブラックリスト化およびホワイトリスト化するのに使用します。

- URL：アクセス コントロール ポリシーでセキュリティ インテリジェンスの一部としてブラックリスト化およびホワイトリスト化するのに使用します。また、セキュリティインテリジェンス後に分析およびトラフィック処理フェーズが実行されるアクセス コントロール ルールおよび QoS ルールで、URL リストを使用することもできます。

一覧

リストは、手動で管理される静的コレクションです。

デフォルトで、アクセス コントロール ポリシーと DNS ポリシーは、セキュリティ インテリジェンスの一部としてグローバル ブラックリストおよびホワイトリストを使用します。[今すぐホワイトリストに登録（Whitelist Now）] および [今すぐブラックリストに登録（Blacklist Now）] アクションを使用することで、再展開することなくセキュリティ インテリジェンス リストを作成して実装できます。[今すぐブラックリストに登録（Blacklist Now）]、[今すぐホワイトリストに登録（Whitelist Now）]、およびグローバル リスト （560 ページ） を参照してください。

カスタム リストを強化し、フィードとグローバル リストを微調整できます。

フィード

フィードは、HTTP または HTTPS で一定期間更新する動的コレクションです。

定期的に更新される Cisco Intelligence Feed を使用すると、Talos からの最新の脅威インテリジェンスに基づいてネットワーク トラフィックをフィルタリングできます。また、サードパーティのフィードを使用することもできます。あるいは、カスタム内部フィードを使用すると、複数の Firepower Management Center アプライアンスからなる大規模な導入で企業全体のブラックリストを簡単に保守できます。

システムがフィードをインターネットから更新するタイミングを厳密に制御したい場合は、そのフィードの自動更新を無効にできます。ただし、自動更新を行えば、最新の関連するデータであることが確実になります。

（注） システムはカスタム フィードのダウンロード時にピア SSL 証明書の検証を実行**しません**。また、システムは、証明書のバンドルまたは自己署名証明書を使用したリモート ピアの検証もサポートしていません。

リストとフィードの書式設定

各リストまたはフィードは、500MB 未満の単純なテキスト ファイルでなければなりません。リスト ファイルの拡張子は .txt でなければなりません。1 行につきエントリまたはコメントを 1 つ（IP アドレス 1 つ、URL 1 つ、ドメイン名 1 つ）含めます。

ヒント 含めることができるエントリの数は、ファイルの最大サイズによって制限されます。たとえば、コメントがなくURLの長さの平均が100文字（PunycodeまたはUnicode表現と改行のパーセントを含む）のURLリストには、524万を超えるエントリを含めることができます。

DNSリストエントリ内では、ドメインラベルとしてアスタリスク（*）ワイルドカード文字を指定できます。その場合、すべてのラベルがワイルドカードと一致します。たとえば、`www.example.*` のエントリは `www.example.com` と `www.example.co` の両方に一致します。

ソース ファイル内にコメント行を含める場合は、シャープ（#）文字で開始する必要があります。コメントが含まれるソースファイルをアップロードすると、システムによってアップロード中にコメントが削除されます。ダウンロードするソースファイルには、コメントを除くすべてのエントリが含まれます。

リストとフィードの更新

リストとフィードの更新は、既存のリストまたはフィードファイルを新しいファイルの内容に置き換えます。既存ファイルと新しいファイルの内容は結合されていません。

システムが破損したフィードまたは認識不能なエントリがあるフィードをダウンロードした場合、システムは古いフィードデータを引き続き使用します（これが初回のダウンロードである場合を除く）。ただし、システムがフィード内のエントリを1つでも認識できる場合、システムは認識できるエントリを使用します。

セキュリティ インテリジェンス オブジェクトのクイック リファレンス

オブジェクト タイプ（Object Type）	機能の編集	編集後に再度展開しますか?
デフォルト（カスタム入力）ホワイトリストとブラックリスト：グローバル、子孫、ドメイン固有	コンテキスト メニューを使用してエントリを追加。 オブジェクト マネージャを使用してエントリを削除。	エントリを追加後、いいえ。 エントリを削除後、はい。
カスタム ホワイトリストとブラックリスト	オブジェクト マネージャを使用して新しいリストと交換リストをアップロード。	○
システム提供インテリジェンス フィード	オブジェクト マネージャを使用して更新頻度を無効または変更。	×
カスタム フィード	オブジェクト マネージャを使用して完全に変更。	×

オブジェクト タイプ（Object Type）	機能の編集	編集後に再度展開しますか?
シンクホール	オブジェクト マネージャを使用して完全に変更。	対応

[今すぐブラックリストに登録（Blacklist Now）]、[今すぐホワイトリストに登録（Whitelist Now）]、およびグローバル リスト

Firepower Management Center のコンテキスト メニュー（コンテキスト メニュー （13 ページ）を参照）では、セキュリティ インテリジェンスを使って、すばやくブラックリストやホワイトリストに登録することができます。たとえば、エクスプロイトの試行に関連した侵入イベントでルーティング可能な IP アドレスのセットに気付いた場合、それらの IP アドレスを即座にブラックリストに入れることができます。変更内容が伝達されるまでに数分かかる場合がありますが、再度展開する必要はありません。

[今すぐブラックリストに登録（Blacklist Now）] と [今すぐホワイトリストに登録（Whitelist Now）] のコンテキスト メニュー オプションは、IP アドレス、URL、DNS 要求ホットスポットに使用可能です。コンテキスト メニューでブラックリストまたはホワイトリストに登録すると、選択した項目が該当するデフォルト グローバル リストに追加されます。デフォルトでは、アクセス コントロール ポリシーと DNS ポリシーがすべてのセキュリティ ゾーンに適用されるグローバル リストを使用します。ポリシーごとに、これらのリストを使用しないように選択することができます。

（注） これらのオプションは、セキュリティ インテリジェンスにのみ適用されます。セキュリティ インテリジェンスは、すでにファーストパスされたトラフィックをブラックリストに登録することはできません。同様に、セキュリティ インテリジェンスでホワイトリストに登録しても、それに一致するトラフィックが自動的に信頼されることもファーストパスされることもありません。詳細については、セキュリティ インテリジェンスについて （1741 ページ）を参照してください。

コンテキスト メニュー オプション	対象項目	対象グローバル リスト
[今すぐブラックリストに追加（Blacklist Now）] [今すぐホワイトリストに追加（Whitelist Now）]	IP アドレス	[グローバル ブラックリスト（Global Blacklist）] [グローバル ホワイトリスト（Global Whitelist）]

コンテキスト メニュー オプション	対象項目	対象グローバル リスト
[今すぐ URL に HTTP/S 接続をブラックリストする（Blacklist HTTP/S Connections to URL Now）] [今すぐ URL に HTTP/S 接続をホワイトリストする（Whitelist HTTP/S Connections to URL Now）]	URL	[URL グローバル ブラックリスト（Global Blacklist for URL）] [URL グローバル ホワイトリスト（Global Whitelist for URL）]
[今すぐドメインに HTTP/S 接続をブラックリストする（Blacklist HTTP/S Connections to Domain Now）] [今すぐドメインに HTTP/S 接続をホワイトリストする（Whitelist HTTP/S Connections to Domain Now）]	ドメイン全体	[URL グローバル ブラックリスト（Global Blacklist for URL）] [URL グローバル ホワイトリスト（Global Whitelist for URL）]
[今すぐドメインに DNS 要求をブラックリストする（Blacklist DNS Requests to Domain Now）] [今すぐドメインに DNS 要求をホワイトリストする（Whitelist DNS Requests to Domain Now）]	ドメイン全体の DNS 要求	[DNS グローバル ブラックリスト（Global Blacklist for DNS）] [DNS グローバル ホワイトリスト（Global Whitelist for DNS）]

マルチドメイン展開では、グローバル リストだけでなくドメイン リストにも項目を登録することで、ブラックリストやホワイトリストを適用する Firepower システム ドメインを選択することができます。セキュリティ インテリジェンス リストとマルチテナンシー（561 ページ）を参照してください。

セキュリティ インテリジェンス リストにエントリを追加すると、アクセス制御に影響が出るため、次のうちいずれか 1 つが必須です。

- 管理者（Administrator）アクセス
- デフォルト ロールの組み合わせ：ネットワーク管理者（Network Admin）またはアクセス管理者（Access Admin）に加えてセキュリティ アナリスト（Security Analyst）およびセキュリティ承認者（Security Approver）
- アクセス コントロール ポリシーの変更（Modify Access Control Policy）と設定をデバイスに展開（Deploy Configuration to Devices）の両方のアクセス許可を持つカスタム ロール。

セキュリティ インテリジェンス リストとマルチテナンシー

マルチドメイン展開では、グローバル ドメインは、グローバルなブラックリストとホワイトリストを所有しています。グローバル リストに対して項目を追加または削除できるのは、グローバル管理者のみです。サブドメイン ユーザがネットワーク、ドメイン名、および URL をホワ

イトリストとブラックリストに追加できるように、マルチテナンシーでは次のものが追加されます。

- ドメイン リスト：コンテンツが特定のサブドメインにのみ適用されるホワイトリストまたはブラックリスト。グローバル リストは、グローバル ドメインのドメイン リストです。
- 子孫ドメイン リスト：現在のドメインの子孫のドメイン リストを集約するホワイトリストまたはブラックリスト。

ドメイン リスト

グローバルリストに（編集ではなく）アクセスできることに加えて、各サブドメインには独自の名前付きリストがあり、そのコンテンツはそのサブドメインにのみ適用されます。たとえば、Company A という名前のサブドメインは、次のリストを所有するとします。

- ドメイン ブラックリスト - Company A およびドメイン ホワイトリスト - Company A
- DNS のドメイン ブラックリスト - Company A、および DNS のドメイン ホワイトリスト - Company A
- URL のドメイン ブラックリスト - Company A、および URL のドメイン ホワイトリスト - Company A

現在のドメインより上位の管理者は、これらのリストに入力できます。コンテキストメニューを使用して、現在のドメインとすべての子孫ドメインの項目をブラックリストまたはホワイトリストに追加できます。ただし、ドメインリストから項目を削除できるのは、関連付けられたドメインの管理者のみです。

たとえば、グローバル管理者はグローバル ドメインと Company A のドメインの同じ IP アドレスをブラックリストに追加できますが、それを Company B のドメインのブラックリストには追加できません。このアクションにより、同じ IP アドレスが次のリストに追加されます。

- （グローバル管理者のみが削除できる）グローバル ブラックリスト
- （Company A の管理者のみが削除できる）ドメインブラックリスト- Company A

システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。

子孫ドメイン リスト

子孫ドメイン リストは、現在のドメインの子孫のドメイン リストを集約するホワイトリストまたはブラックリストです。リーフ ドメインには、子孫ドメイン リストはありません。

子孫ドメイン リストが便利なのは、上位レベルのドメインの管理者が一般的なセキュリティ インテリジェンス設定を適用できる一方で、サブドメインユーザは独自の展開で項目をブラックリストやホワイトリストに追加できるためです。

たとえば、グローバル ドメインには、次の子孫ドメイン リストがあります。

- 子孫ブラックリスト - グローバルおよび子孫のホワイトリスト - グローバル

- URL の子孫ブラックリスト - グローバル、および子孫の URL のホワイトリスト - グローバル
- URL の子孫ブラックリスト - グローバル、および子孫の URL のホワイトリスト - グローバル

（注） 子孫ドメイン リストは、手動で入力されたリストではなく象徴的な集約であるため、オブジェクト マネージャには表示されません。それを使用できる場所、つまり、アクセス コントロール ポリシーと DNS ポリシーに表示されます。

セキュリティ インテリジェンス フィードの更新頻度の変更

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Access Admin/Network Admin

デフォルトでは、各フィードは 2 時間ごとに Management Center を更新します。システムが提供するフィードは削除できませんが、更新頻度を変更（または無効に設定）できます。

マルチドメイン展開では、システムが提供するフィードはグローバルドメインに属し、このドメインの管理者のみが変更できます。ユーザは、各自が使用するドメインに属するカスタム フィードの更新頻度を更新できます。

（注） Management Center は、セキュリティ インテリジェンスの更新を 30 分ごとに管理対象デバイスにプッシュします。この周波数を変更することはできません。

ステップ 1 **[Objects]** > **[Object Management]** を選択します。

ステップ 2 [セキュリティ インテリジェンス（Security Intelligence）] ノードを展開し、更新頻度を変更するフィードのタイプを選択します。

ステップ 3 更新するフィードの横にある編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、オブジェクトを変更する権限がありません。

ステップ 4 [更新頻度（Update Frequency）] を編集します。

ステップ 5 **[保存（Save）]** をクリックします。

カスタム セキュリティ インテリジェンス フィード

カスタムまたはサードパーティのセキュリティ インテリジェンス フィードを使用すると、インターネット上で定期的に更新される他の信頼できるホワイトリストおよびブラックリストによって、システムが提供するインテリジェンスフィードを拡張することができます。内部フィードをセットアップすることもできます。これは、1つのソースリストを使用して導入環境で複数の Firepower Management Center を更新する場合に役立ちます。

（注） セキュリティ インテリジェンス フィードでは、/0 ネットマスクを使ってアドレス ブロックをホワイトリスト登録またはブラックリスト登録することはできません。ポリシーですべてのトラフィックをモニタまたはブロックする場合は、[モニタ（Monitor）] または [ブロック（Block）] ルール アクションを含むアクセス コントロール ルールを使用し、デフォルト値 any を [送信元ネットワーク（Source Networks）] および [宛先ネットワーク（Destination Networks）] それぞれに設定します。

フィードを設定する場合は、URL を使用して場所を指定します。この URL は Punycode によりエンコードできません。デフォルトで、システムは設定した間隔でフィード ソース全体をダウンロードし、管理対象デバイスを自動更新します。

md5 チェックサムを使用して、更新フィードをダウンロードするかどうか判断するようにシステムを設定することもできます。システムが最後にフィードをダウンロードした後にチェックサムが変更されていない場合、再ダウンロードする必要はありません。特に内部フィードが大きい場合には、md5 チェックサムを使用することができます。md5 チェックサムは、チェックサムのみを含む単純なテキスト ファイルに保存する必要があります。コメントはサポートされていません。

手動でセキュリティ インテリジェンス フィードを更新すると、インテリジェンス フィードを含め、すべてのフィードが更新されます。

セキュリティ インテリジェンス フィードの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Access Admin/Network Admin

ステップ 1 **[Objects]** > **[Object Management]**を選択します。

ステップ 2 [セキュリティ インテリジェンス（Security Intelligence）] ノードを展開し、追加するフィード タイプを選択します。

ステップ 3 上記で選択したフィード タイプに適したオプションをクリックします。

- [ネットワークのリストとフィードの追加（Add Network Lists and Feeds）]（IP アドレス用）

- **[DNS リストとフィードの追加（Add DNS Lists and Feeds）]**
- **[URL リストとフィードの追加（Add URL Lists and Feeds）]**

ステップ 4 フィードの名前を [名前（Name）] に入力します。

マルチドメイン展開では、オブジェクト名をドメイン階層内で一意にする必要があります。システムは、現在のドメインでは表示できないオブジェクトの名前との競合を特定することができます。

ステップ 5 [タイプ（Type）] ドロップダウンリストから [フィード（Feed）] を選択します。

ステップ 6 [フィード URL（Feed URL）] を入力します。

ステップ 7 オプションで、[MD5 URL] を入力します。

ステップ 8 [更新頻度（Update Frequency）] を選択します。

ステップ 9 [保存（Save）] をクリックします。
フィードの更新を無効にした場合を除き、システムはフィードをダウンロードして検証しようとします。

手動によるセキュリティ インテリジェンス フィードの更新

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス（Access）
脅威（セキュリティ インテリジェンス）	保護（セキュリティ インテリジェンス）	いずれか（Any）	いずれか（Any）	Admin/Access Admin/Network Admin

始める前に

少なくとも 1 つのデバイスが管理センターに追加されている必要があります。

ステップ 1 **[Objects]** > **[Object Management]**を選択します。

ステップ 2 [セキュリティ インテリジェンス（Security Intelligence）] ノードを展開し、フィード タイプを選択します。

ステップ 3 [フィードの更新（Update Feeds）] をクリックして、確認します。

ステップ 4 [OK] をクリックします。

フィードの更新をダウンロードして検証した後、Firepower Management Centerはすべての変更内容を管理対象デバイスに通知します。導入環境では、更新されたフィードを使用してトラフィックのフィルタリングが開始されます。

カスタム セキュリティ インテリジェンス リスト

セキュリティ インテリジェンス リストは、IP アドレス、アドレス ブロック、URL、またはドメイン名の単純なスタティック リストで、ユーザがシステムに手動でアップロードします。カ

スタム リストは、単一の Firepower Management Center の管理対象デバイスで、フィードやグローバル リストの 1 つを増やしたり、微調整したりする場合に役立ちます。

たとえば、信頼できるフィードが重要なリソースへのアクセスを誤ってブロックしているものの、このフィードが全体的に部門にとって有用である場合、IP アドレス フィード オブジェクトをアクセス コントロール ポリシーのブラックリストから削除する代わりに、誤って分類された IP アドレスだけが含まれるカスタム ホワイトリストを作成できます。

（注） セキュリティ インテリジェンス リストでは、/0 ネットマスクを使ってアドレス ブロックをホワイトリスト登録またはブラックリスト登録することはできません。ポリシーですべてのトラフィックをモニタまたはブロックする場合は、[モニタ（Monitor）] または [ブロック（Block）] ルール アクションを含むアクセス コントロール ルールを使用し、デフォルト値 any を [送信元ネットワーク（Source Networks）] および [宛先ネットワーク（Destination Networks）] それぞれに設定します。

リスト エントリのフォーマットについて、次の点に注意してください。

- アドレス ブロックのネットマスクは、IPv4 および IPv6 の場合、それぞれ 0 から 32、または 0 から 128 までの整数になります。
- ドメイン名に含まれる Unicode は Punycode 形式でエンコードされる必要があります。大文字と小文字は区別されません。
- ドメイン名の文字の大文字と小文字は区別されません。
- URL に含まれる Unicode はパーセントエンコーディング形式でエンコードする必要があります。
- URL サブディレクトリの文字の大文字と小文字は区別されます。
- シャープ記号（#）で始まるリスト エントリは、コメントと見なされます。

リスト エントリの照合について、次の点に注意してください。

- URL または DNS リストにより高位レベルのドメインが存在する場合、システムはそれより低いレベルのドメインを一致とします。たとえば、DNS リストに example.com を追加すると、システムは www.example.com と test.example.com の両方を一致とします。
- システムは DNS または URL リスト エントリに対して DNS ルックアップを（フォワード ルックアップ、リバース ルックアップともに）行いません。たとえば、URL リストに http://192.168.0.2 を追加し、これがルックアップすれば http://www.example.com であったとします。この場合、システムは http://192.168.0.2 のみ一致とし、http://www.example.com は一致となりません。
- URL リストに末尾がスラッシュ（/）記号で終わる URL を追加した場合、そのエントリに一致するのは完全に一致する URL のみとなります。
- URL または DNS リストに末尾にスラッシュ記号のない URL を追加した場合、そのエントリと同じプレフィックスを持つ URL は一致となります。たとえば、URL リストに

`www.example.com` を追加すると、システムは `www.example.com` と `www.example.com/example` の両方を一致とします。

新しいセキュリティ インテリジェンス リストの Firepower Management Center へのアップロード

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Access Admin/Network Admin

セキュリティ インテリジェンス リストを変更するには、ソース ファイルを変更して、新しいコピーをアップロードする必要があります。Web インターフェイスを使用してファイルの内容を変更することはできません。ソース ファイルへのアクセス権がない場合は、システムからコピーをダウンロードします。

ステップ 1 **[Objects]** > **[Object Management]** を選択します。

ステップ 2 [セキュリティ インテリジェンス（Security Intelligence）] ノードを展開し、リストのタイプを選択します。

ステップ 3 上記の手順で選択したリストに該当するオプションをクリックします。

- [ネットワークのリストとフィードの追加（Add Network Lists and Feeds）]（IP アドレス用）
- **[DNS リストとフィードの追加（Add DNS Lists and Feeds）]**
- **[URL リストとフィードの追加（Add URL Lists and Feeds）]**

ステップ 4 名前を入力します。

マルチドメイン展開では、オブジェクト名をドメイン階層内で一意にする必要があります。システムは、現在のドメインでは表示できないオブジェクトの名前との競合を特定することができます。

ステップ 5 [タイプ（Type）] ドロップダウン リストから、[リスト（List）] を選択します。

ステップ 6 [参照（Browse）] をクリックしてリストの `.txt` ファイルを位置指定し、[アップロード（Upload）] をクリックします。

ステップ 7 **[保存（Save）]** をクリックします。

次のタスク

- アクティブ ポリシーがオブジェクトを参照する場合は、設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

セキュリティ インテリジェンス リストの更新

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Access Admin/Network Admin

マルチドメインの展開では、現在のドメインで作成されたオブジェクトが表示されます。このオブジェクトは編集できます。先祖ドメインで作成されたオブジェクトも表示されますが、ほとんどの場合これは編集できません。子孫ドメインにあるオブジェクトを表示および編集するには、そのドメインに切り替えます。

ステップ 1 **[Objects]** > **[Object Management]**を選択します。

ステップ 2 [セキュリティ インテリジェンス（Security Intelligence）] ノードを展開し、リストのタイプを選択します。

ステップ 3 更新するリストの横にある編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 4 編集するリストのコピーが必要な場合、[ダウンロード（Download）] をクリックし、ブラウザのプロンプトに従ってリストをテキスト ファイルとして保存します。

ステップ 5 必要に応じてリストを変更します。

ステップ 6 [セキュリティ インテリジェンス（Security Intelligence）] ポップアップ ウィンドウで、[参照（Browse）] をクリックして、変更されたリストを参照し、[アップロード（Upload）] をクリックします。

ステップ 7 **[保存（Save）]** をクリックします。

次のタスク

- アクティブ ポリシーがオブジェクトを参照する場合は、設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

シンクホール オブジェクト

シンクホール オブジェクトは、シンクホール内のすべてのドメイン名にルーティング不可アドレスを付与する DNS サーバ、またはサーバに解決しない IP アドレスのいずれかを表します。DNS ポリシー ルール内のシンクホール オブジェクトを参照して、一致するトラフィックをシンクホールにリダイレクトできます。このオブジェクトには IPv4 アドレスと IPv6 アドレスの両方を割り当てる必要があります。

シンクホール オブジェクトの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Access Admin/Network Admin

ステップ 1 **[Objects]** > **[Object Management]**を選択します。

ステップ 2 オブジェクト タイプのリストから [Sinkhole] を選択します。

ステップ 3 [Add Sinkhole] をクリックします。

ステップ 4 [Name] を入力します。

マルチドメイン展開では、オブジェクト名をドメイン階層内で一意にする必要があります。システムは、現在のドメインでは表示できないオブジェクトの名前との競合を特定することができます。

ステップ 5 シンクホールの [IPv4 アドレス（IPv4 Address）] と [IPv6 アドレス（IPv6 Address）] を入力します。

ステップ 6 次の選択肢があります。

- シンクホール サーバへのトラフィックをリダイレクトする場合は、[Log Connections to Sinkhole] を選択します。
- トラフィックを非解決 IP アドレスにリダイレクトするには、[Block and Log Connections to Sinkhole] を選択します。

ステップ 7 侵入の痕跡（IoC）のタイプをシンクホールに割り当てるには、[タイプ（Type）] ドロップダウンからいずれかのタイプを選択します。

ステップ 8 **[保存（Save）]** をクリックします。

ファイル リスト

ネットワーク向け AMP を使用しており、AMP クラウドがファイルの性質を誤って特定した場合は、このファイルをファイル リストに追加して、今後さらに検出できます。このファイルは、SHA-256 ハッシュ値を使用して指定されます。各ファイル リストには、一意の SHA-256 値を最大 10000 個まで含めることができます。

ファイル リストには 2 種類の事前定義済みカテゴリがあります。

クリーン リスト

このリストにファイルを追加すると、システムは AMP クラウドがクリーンな性質を割り当てた場合と同様にファイルを扱います。

カスタム検出リスト

このリストにファイルを追加すると、システムは AMP クラウドがマルウェアの性質を割り当てた場合と同様にファイルを扱います。

マルチドメイン展開では、各ドメインにクリーン リストとカスタム検出リストが存在します。下位レベルのドメインでは、先祖のリストを表示できますが、変更できません。

これらのリストに含まれているファイルに手動でブロッキング動作を指定するため、システムはこれらのファイルの性質について AMP クラウドに照会しません。ファイルの SHA 値を計算するには、[マルウェア クラウド ルックアップ（Malware Cloud Lookup）] アクションと [マルウェア ブロック（Block Malware）] アクションのどちらか、および一致するファイル タイプを使用して、ファイル ポリシー内のルールを設定する必要があります。

⚠

注意 クリーン リストにマルウェアを**含めない**でください。クリーン リストによって、AMP クラウドおよびカスタム検出リストの両方がオーバーライドされます。

ファイル リストのソース ファイル

SHA-256 値のリストと説明を含むカンマ区切り値（CSV）ソース ファイルをアップロードすることによって、複数の SHA-256 値をファイル リストに追加できます。Firepower Management Centerはその内容を検証し、有効な SHA-256 値をファイル リストに入れます。

ソース ファイルは、ファイル名拡張子 .csv の単純なテキスト ファイルである必要があります。見出しはポンド記号（#）で始まる必要があります。これはコメントとして処理され、アップロードされません。各エントリには、1 つの SHA-256 値の後に説明が含まれる必要があり、LF または CR+LF 改行文字で終わる必要があります。システムはエントリ内のこれ以外の情報をすべて無視します。

次の点に注意してください。

- ファイル リストからソース ファイルを削除すると、それに関連付けられているすべての SHA-256 ハッシュもファイル リストから削除されます。
- ソース ファイルのアップロードに成功した結果、10000 個を超える個別の SHA-256 値がファイル リストに含まれる場合は、複数のファイルをファイル リストにアップロードすることはできません。
- システムは、アップロード時に 256 文字を超える説明を最初の 256 文字で切り捨てます。説明にコンマを含める場合は、エスケープ文字（\）を使用する必要があります。説明が含まれていない場合、代わりにソース ファイル名が使用されます。
- 重複しないすべての SHA-256 値がこのファイル リストに追加されます。すでにファイル リストに存在する SHA-256 値を含むソース ファイルをアップロードした場合、新しくアップロードされた値によって既存の SHA--256 値が変更されることはありません。SHA-256 値に関連するキャプチャ済みファイル、ファイル イベント、またはマルウェア イベントを表示するとき、個々の SHA-256 値から脅威名または説明が得られます。

- システムはソース ファイル内の無効な SHA-256 値をアップロードしません。
- アップロードされた複数のソース ファイル内に同じ SHA-256 値に関するエントリが含まれる場合、システムは最も新しい値を使用します。
- 1 つのソース ファイル内に同じ SHA-256 値のエントリが複数含まれる場合、システムは最後のものを使用します。
- オブジェクト マネージャ内でソース ファイルを直接編集することはできません。変更を行うには、最初にソースファイルを直接変更し、システム上のコピーを削除した後、変更済みソース ファイルをアップロードする必要があります。
- ソース ファイルに関連付けられたエントリ数とは、個別の SHA-256 値の数です。ファイル リストからソース ファイルを削除すると、ファイル リストに含まれる SHA-256 エントリの合計数は、ソース ファイル内の有効なエントリ数だけ減少します。

ファイル リスト別の SHA-256 値の追加

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス（Access）
マルウェア	マルウェア	Firepower	任意（Any）	Admin/Network Admin/Access Admin

ファイルのSHA-256値を送信して、それをファイル リストに追加できます。重複するSHA-256値は追加できません。

マルチドメインの展開では、現在のドメインで作成されたオブジェクトが表示されます。このオブジェクトは編集できます。先祖ドメインで作成されたオブジェクトも表示されますが、ほとんどの場合これは編集できません。子孫ドメインにあるオブジェクトを表示および編集するには、そのドメインに切り替えます。

始める前に

- イベント ビューからファイルまたはマルウェア イベントを右クリックし、コンテキスト メニューで [フル テキストの表示（Show Full Text）] を選択し、ファイルの SHA-256 値全体をコピーし、ファイルリストに貼り付けます。

ステップ 1 **[Objects]** > **[Object Management]**を選択します。

ステップ 2 オブジェクト タイプのリストから [ファイル リスト（File List）] を選択します。

ステップ 3 ファイルの追加場所となるクリーン リストまたはカスタム検出リストの横の編集アイコン（  ）をクリックします。

代わりに表示アイコン（  ）が表示される場合、設定は先祖ドメインに属しており、オブジェクトを変更する権限がありません。

ステップ 4 [追加元（Add by）] ドロップダウンリストから [SHA 値の入力（Enter SHA Value）] を選択します。

ステップ 5 [説明（Description）] フィールドにソース ファイルの説明を入力します。

ステップ 6 [SHA-256] フィールドにファイル全体の値を入力し、または貼り付けます。システムでは値の部分的な一致はサポートされません。

ステップ 7 [Add] をクリックします。

ステップ 8 **[保存（Save）]** をクリックします。

次のタスク

- アクティブ ポリシーがオブジェクトを参照する場合は、設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

（注） 設定の変更が展開されたら、システムはそのリストのファイルについて AMP クラウドに問い合わせなくなります。

ファイル リストへの個々のファイルのアップロード

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス（Access）
マルウェア	マルウェア	いずれか（Any）	いずれか（Any）	Admin/Access Admin/Network Admin

ファイル リストに追加するファイルのコピーがある場合、分析用にファイルを Firepower Management Center にアップロードできます。システムはファイルの SHA-256 値を計算し、ファイルをリストに追加します。SHA-256 を計算するとき、システムはファイル サイズを制限しません。

マルチドメインの展開では、現在のドメインで作成されたオブジェクトが表示されます。このオブジェクトは編集できます。先祖ドメインで作成されたオブジェクトも表示されますが、ほとんどの場合これは編集できません。子孫ドメインにあるオブジェクトを表示および編集するには、そのドメインに切り替えます。

ステップ 1 **[Objects]** > **[Object Management]**を選択します。

ステップ 2 オブジェクト タイプのリストから [ファイル リスト（File List）] を選択します。

ステップ 3 ファイルの追加場所となるクリーン リストまたはカスタム検出リストの横の編集アイコン（ ）をクリックします。

代わりに表示アイコン（ ）が表示される場合、設定は先祖ドメインに属しており、オブジェクトを変更する権限がありません。

ステップ 4 [追加（Add by）] ドロップダウン リストから、[SHA の計算（Calculate SHA）] を選択します。

ステップ 5 オプションで、[Description] フィールドにファイルの説明を入力します。説明を入力しない場合、アップロード時にファイル名が説明として使用されます。

ステップ 6 [参照（Browse）] をクリックし、アップロードするファイルを選択します。

ステップ 7 [SHA の計算と追加（Calculate and Add SHA）] をクリックします。

ステップ 8 [保存（Save）] をクリックします。

次のタスク

- アクティブ ポリシーがオブジェクトを参照する場合は、設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

（注） 設定の変更を導入すると、その後システムはそのリストのファイルを AMP クラウドでクエリしなくなります。

ファイル リストへのソース ファイルのアップロード

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス（Access）
マルウェア	マルウェア	いずれか（Any）	いずれか（Any）	Admin/Access Admin/Network Admin

マルチドメインの展開では、現在のドメインで作成されたオブジェクトが表示されます。このオブジェクトは編集できます。先祖ドメインで作成されたオブジェクトも表示されますが、ほとんどの場合これは編集できません。子孫ドメインにあるオブジェクトを表示および編集するには、そのドメインに切り替えます。

ステップ 1 **[Objects]** > **[Object Management]**を選択します。

ステップ 2 [ファイル リスト（File List）] をクリックします。

ステップ 3 ソース ファイルからの値の追加先となるファイル リストの横にある編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、オブジェクトを変更する権限がありません。

ステップ 4 [追加方法（**Add by**）] ドロップダウン リストで [SHA のリスト（List of SHAs）] を選択します。

ステップ 5 オプションで、[Description] フィールドにソース ファイルの説明を入力します。説明を入力しない場合、システムはファイル名を使用します。

ステップ 6 [参照（Browse）] をクリックしてソース ファイルを参照してから、[リストのアップロードと追加（Upload and Add List）] をクリックします。

ステップ 7 [保存（Save）] をクリックします。

次のタスク

- アクティブ ポリシーがオブジェクトを参照する場合は、設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

（注） ポリシーを展開したら、システムはそのリストのファイルについて AMP クラウドに問い合わせなくなります。

ファイル リストの SHA-256 値の編集

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス（Access）
マルウェア	マルウェア	いずれか（Any）	いずれか（Any）	Admin/Access Admin/Network Admin

ファイル リストの個々の SHA-256 値を編集または削除することができます。オブジェクト マネージャ内でソース ファイルを直接編集できないことに注意してください。変更を行うには、最初にソース ファイルを直接変更し、システム上のコピーを削除した後、変更済みソース ファイルをアップロードする必要があります。

マルチドメインの展開では、現在のドメインで作成されたオブジェクトが表示されます。このオブジェクトは編集できます。先祖ドメインで作成されたオブジェクトも表示されますが、ほとんどの場合これは編集できません。子孫ドメインにあるオブジェクトを表示および編集するには、そのドメインに切り替えます。

ステップ 1 **[Objects]** > **[Object Management]** を選択します。

ステップ 2 [ファイル リスト（File List）] をクリックします。

ステップ 3 ファイルの変更対象となるクリーン リストまたはカスタム検出リストの横の編集アイコン（ ）をクリックします。

代わりに表示アイコン（ ）が表示される場合、設定は先祖ドメインに属しており、オブジェクトを変更する権限がありません。

ステップ 4 次の操作を実行できます。

- 変更する SHA-256 値の横にある編集アイコン（）をクリックし、必要に応じて [SHA-256] または [説明（Description）] の値を変更します。
- 削除する SHA-256 値の横にある削除アイコン（）をクリックします。

ステップ 5 [保存（Save）] をクリックし、リストのファイル エントリを更新します。

ステップ 6 [保存（Save）] をクリックして、ファイル リストを保存します。

次のタスク

- アクティブ ポリシーがオブジェクトを参照する場合は、設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

（注） 設定の変更が展開されたら、システムはそのリストのファイルについて AMP クラウドに問い合わせなくなります。

ファイル リストからのソース ファイルのダウンロード

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス（Access）
マルウェア	マルウェア	いずれか（Any）	いずれか（Any）	Admin/Access Admin/Network Admin

マルチドメインの展開では、現在のドメインで作成されたオブジェクトが表示されます。このオブジェクトは編集できます。先祖ドメインで作成されたオブジェクトも表示されますが、ほとんどの場合これは編集できません。子孫ドメインにあるオブジェクトを表示および編集するには、そのドメインに切り替えます。

ステップ 1 **[Objects]** > **[Object Management]**を選択します。

ステップ 2 オブジェクト タイプのリストから [ファイル リスト（File List）] を選択します。

ステップ 3 ソース ファイルのダウンロード対象となるクリーン リストまたはカスタム検出リストの横の編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、オブジェクトを変更する権限がありません。

ステップ 4 ダウンロードするソース ファイルの横にある表示アイコン（）をクリックします。

ステップ 5 [Download SHA List] をクリックし、プロンプトに従ってソース ファイルを保存します。

ステップ 6 [閉じる（Close）] をクリックします。

暗号スイート リスト

暗号スイートリストは複数の暗号スイートからなるオブジェクトです。定義済み暗号スイートの値は、SSL またはTLS暗号化セッションのネゴシエートに使われる暗号スイートを表しています。暗号スイートおよび暗号スイート リストを SSL ルールで使用すると、クライアントとサーバが暗号スイートを使ってSSLセッションをネゴシエートしたかどうかに基づいて暗号化トラフィックを制御できます。SSLルールに暗号スイートリストを追加すると、リスト内のいずれかの暗号スイートでネゴシエートされた SSL セッションがルールに一致します。

（注） Webインターフェイスでは暗号スイートリストと同じ場所で暗号スイートを使用できますが、暗号スイートを追加、変更、削除することはできません。

暗号スイート リストの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	すべて（NGIPSvを除く）	いずれか（Any）	Admin/Access Admin/Network Admin

ステップ 1 **[Objects]** > **[Object Management]**を選択します。

ステップ 2 オブジェクト タイプのリストから [暗号スイート リスト（Cipher Suite List）] を選択します。

ステップ 3 [暗号スイートの追加（Add Cipher Suites）] をクリックします。

ステップ 4 名前を入力します。

マルチドメイン展開では、オブジェクト名をドメイン階層内で一意にする必要があります。システムは、現在のドメインでは表示できないオブジェクトの名前との競合を特定することができます。

ステップ 5 [使用可能な暗号（Available Ciphers）] リストから、1 つ以上の暗号スイートを選択します。

ステップ 6 [追加（Add）] をクリックします。

ステップ 7 オプションで、[選択された暗号（Selected Ciphers）] リストで、削除する暗号スイートの隣にある削除アイコン（）をクリックします。

ステップ 8 **[保存（Save）]** をクリックします。

次のタスク

- アクティブポリシーがオブジェクトを参照する場合は、設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

識別名オブジェクト

それぞれの識別名オブジェクトは、公開鍵証明書のサブジェクトまたは発行元にリストされた識別名を表します。SSL ルールで識別名オブジェクトとグループを使用すると、サブジェクトまたは発行元として識別名を含むサーバ証明書を使ってクライアントとサーバが SSL セッションをネゴシエートしたかどうかに基づき、暗号化トラフィックを制御できます。

識別名オブジェクトには、共通名属性（**CN**）を含めることができます。「CN=」なしで共通名を追加すると、システムはオブジェクトを保存する前に「CN=」を追加します。

さらに、次の表にリストされている、コンマで区切られた属性を含む識別名を追加することもできます。

表 *65 :* 識別名の属性

属性	説明	使用可能な値
C	国番号	2 つの英字
CN	共通名	最大 64 文字の英数字、バックスラッシュ（\）、ハイフン（-）、引用符（"）、アスタリスク（*）、スペース文字
O	組織	最大 64 文字の英数字、バックスラッシュ（\）、ハイフン（-）、引用符（"）、アスタリスク（*）、スペース文字
OU	組織単位	最大 64 文字の英数字、バックスラッシュ（\）、ハイフン（-）、引用符（"）、アスタリスク（*）、スペース文字

ワイルドカードとして 1 つ以上のアスタリスク（*）を属性に定義できます。共通名属性では、ドメイン名ラベルごとに 1 つ以上のアスタリスクを定義できます。ワイルドカードはそのラベル内でのみ照合されますが、ワイルドカードを使用して複数のラベルを定義できます。例については、以下の表を参照してください。

表 *66 :* 共通名属性のワイルドカードの例

属性	一致する	一致しない
CN=”*ample.com”	example.com	mail.example.com example.text.com ampleexam.com
CN=”exam*.com”	example.com	mail.example.com example.text.com ampleexam.com
CN=”*xamp*.com”	example.com	mail.example.com example.text.com ampleexam.com
CN=”*.example.com”	mail.example.com	example.com example.text.com ampleexam.com
CN=”*.com”	example.com ampleexam.com	mail.example.com example.text.com
CN=”*.*.com”	mail.example.com example.text.com	example.com ampleexam.com

識別名オブジェクトの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	すべて（NGIPSvを除く）	いずれか（Any）	Admin/Access Admin/Network Admin

ステップ 1 **[Objects]** > **[Object Management]**を選択します。

ステップ 2 [識別名（Distinguished Name）] ノードを展開し、[個別オブジェクト（Individual Objects）] を選択します。

ステップ 3 [識別名の追加（Add Distinguished Name）] をクリックします。

ステップ 4 名前を入力します。

マルチドメイン展開では、オブジェクト名をドメイン階層内で一意にする必要があります。システムは、現在のドメインでは表示できないオブジェクトの名前との競合を特定することができます。

ステップ 5 [DN] フィールドに、識別名または共通名の値を入力します。次の選択肢があります。

- 識別名を追加する場合は、識別名オブジェクト （577 ページ）に示されている属性をカンマで区切って含めることができます。
- 共通名を追加する場合は、複数のラベルとワイルドカードを含めることができます。

ステップ 6 **[保存（Save）]** をクリックします。

次のタスク

- アクティブポリシーがオブジェクトを参照する場合は、設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

PKI オブジェクト

SSL アプリケーションの PKI オブジェクト

PKI オブジェクトは、導入をサポートするために必要な公開鍵証明書、およびペアになった秘密鍵を表します。内部 CA オブジェクトおよび信頼できる CA オブジェクトは、認証局（CA）証明書で構成されます。また、内部 CA オブジェクトには、証明書とペアになった秘密鍵も含まれます。内部証明書オブジェクトおよび外部証明書オブジェクトは、サーバ証明書で構成されます。また、内部証明書オブジェクトには、証明書とペアになった秘密鍵も含まれます。

信頼できる認証局オブジェクトと内部証明書オブジェクトを使用して ISE/ISE-PIC への接続を設定する場合、ISE/ISE-PIC をアイデンティティ ソースとして使用できます。

内部証明書オブジェクトを使用してキャプティブ ポータルを設定する場合、システムはキャプティブ ポータル デバイスがユーザの Web ブラウザに接続する際に、デバイスのアイデンティティを検証できます。

信頼できる認証局オブジェクトを使用してレルムを設定する場合、LDAP または AD サーバへのセキュア接続を設定できます。

SSL ルールで PKI オブジェクトを使用する場合、以下のものを使用して暗号化されたトラフィックを照合することができます。

- 外部証明書オブジェクト内の証明書
- 信頼できる CA オブジェクトの CA によって署名された証明書、または信頼できる CA チェーン内で署名された証明書

SSL ルールで PKI オブジェクトを使用する場合、以下のものを復号できます。

- 発信トラフィック：内部 CA オブジェクトを使ってサーバ証明書を再署名することによって復号します
- 受信トラフィック：内部証明書オブジェクトにある既知の秘密鍵を使用して復号します

証明書とキーの情報を手動で入力し、その情報を含むファイルをアップロードします。場合によっては、新しい CA 証明書や秘密キーを生成することができます。

オブジェクト マネージャで PKI オブジェクトのリストを表示すると、システムは証明書のサブジェクト識別名をオブジェクト値として表示します。証明書の完全なサブジェクト識別名を表示するには、値の上にポインタを移動してください。証明書に関する他の詳細を表示するには、PKI オブジェクトを編集します。

（注） Firepower Management Centerおよび管理対象デバイスは、内部 CA オブジェクトと内部証明書オブジェクトに保存されるすべての秘密鍵を、保存前にランダムに生成された鍵を使って暗号化します。パスワード保護されている秘密キーをアップロードすると、アプライアンスはユーザ提供のパスワードを使って秘密キーを復号し、ランダムに生成されたキーを使ってそれを再暗号化してから保存します。

証明書の登録の PKI オブジェクト

証明書の登録オブジェクトには、証明書署名要求（CSR）を作成したり、指定された CA からアイデンティティ証明書を取得したりするために必要な証明機関（CA）サーバ情報や登録パラメータが含まれています。これらのアクティビティは、秘密キー インフラストラクチャ（PKI）で発生します。

証明書の登録オブジェクトには、証明書失効情報も含まれている場合があります。PKI、デジタル証明書、および証明書の登録の詳細については、PKIインフラストラクチャとデジタル証明書 （1062 ページ） を参照してください。

内部認証局オブジェクト

設定されたそれぞれの内部認証局（CA）オブジェクトは、組織で制御される CA の CA 公開鍵証明書を表します。このオブジェクトは、オブジェクト名、CA 証明書、およびペアになった秘密鍵からなります。SSL ルールで内部 CA オブジェクトとグループを使用すると、内部 CA によってサーバ証明書に再署名することにより、発信する暗号化トラフィックを復号できます。

（注） [復号 - 再署名（Decrypt - Resign）] SSL ルールで内部 CA オブジェクトを参照する場合、ルールが暗号化セッションに一致すると、SSL ハンドシェイクのネゴシエート中は証明書を信頼できないという警告がユーザのブラウザに表示されることがあります。これを回避するには、信頼できるルート証明書のクライアントまたはドメイン リストに内部CAオブジェクト証明書を追加します。

次の方法で内部 CA オブジェクトを作成できます。

- RSA ベースまたは楕円曲線ベースの既存の CA 証明書と秘密キーをインポートする
- 新しい RSA ベースの自己署名 CA 証明書と秘密キーを生成する

- RSA ベースの未署名の CA 証明書と秘密キーを生成する内部 CA オブジェクトを使用する前に、証明書に署名するために証明書署名要求（CSR）を別の CA に送信する必要があります。

署名付き証明書を含む内部CAオブジェクトを作成した後で、CA証明書と秘密鍵をダウンロードできるようになります。システムは、ダウンロードされた証明書と秘密キーをユーザ提供のパスワードで暗号化します。

システムで生成された場合でも、ユーザによって作成された場合でも、内部CAオブジェクトの名前は変更できますが、他のオブジェクト プロパティは変更できません。

使用中の内部 CA オブジェクトは削除できません。さらに、SSL ポリシーで使用される内部CAオブジェクトを編集すると、関連するアクセス コントロール ポリシーが失効します。変更を反映させるには、アクセス コントロール ポリシーを再度展開する必要があります。

CA 証明書と秘密キーのインポート

X.509 v3 CA 証明書と秘密キーをインポートすることによって、内部 CA オブジェクトを設定できます。サポートされる次のいずれかの形式でエンコードされたファイルをアップロードできます。

- 識別符号化規則（DER）
- プライバシー強化電子メール（PEM）

秘密キーファイルがパスワード保護されている場合は、復号パスワードを提供できます。証明書とキーが PEM 形式でエンコードされている場合は、情報をコピーして貼り付けることもできます。

適切な証明書またはキーの情報を含んでいる、相互にペアになっているファイルのみをアップロードできます。システムはオブジェクトを保存する前にペアを検証します。

（注） ルールに [復号 - 再署名（Decrypt - Resign）] アクションを設定すると、そのルールでは、設定されているルール条件に加えて、参照される内部CA証明書の暗号化アルゴリズムのタイプに基づいてトラフィックが照合されます。たとえば、楕円曲線ベースのアルゴリズムで暗号化された発信トラフィックを復号するには、楕円曲線ベースのCA証明書をアップロードする必要があります。

CA 証明書と秘密キーのインポート

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	すべて（NGIPSvを除く）	いずれか（Any）	Admin/Access Admin/Network Admin

マルチドメインの展開では、現在のドメインで作成されたオブジェクトが表示されます。このオブジェクトは編集できます。先祖ドメインで作成されたオブジェクトも表示されますが、ほとんどの場合これは編集できません。子孫ドメインにあるオブジェクトを表示および編集するには、そのドメインに切り替えます。

ステップ 1 **[Objects]** > **[Object Management]**を選択します。

ステップ 2 [PKI] ノードを展開し、[内部 CA（Internal CAs）] を選択します。

ステップ 3 [CA のインポート（Import CA）] をクリックします。

ステップ 4 名前を入力します。

マルチドメイン展開では、オブジェクト名をドメイン階層内で一意にする必要があります。システムは、現在のドメインでは表示できないオブジェクトの名前との競合を特定することができます。

ステップ 5 [証明書データ（Certificate Data）] フィールドの上部にある [参照（Browse）] をクリックして、DER または PEM でエンコードされた X.509 v3 CA 証明書ファイルをアップロードします。

ステップ 6 [キー（Key）] フィールドの上部にある [参照（Browse）] をクリックして、DER または PEM でエンコードされたペアの秘密キー ファイルをアップロードします。

ステップ 7 アップロード ファイルがパスワード保護されている場合は、[暗号化および次のパスワード:（Encrypted, and the password is:）] チェックボックスをオンにして、パスワードを入力します。

ステップ 8 **[保存（Save）]** をクリックします。

次のタスク

- アクティブ ポリシーがオブジェクトを参照する場合は、設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

CA 証明書および秘密キーの生成

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	すべて（NGIPSv を除く）	いずれか（Any）	Admin/Access Admin/Network Admin

識別情報を提供することで、RSA ベースの自己署名 CA 証明書と秘密キーを生成するように内部 CA オブジェクトを設定できます。

生成される CA 証明書の有効期間は 10 年です。[有効期間の開始（Valid From）] の日付は、生成の一週間前です。

マルチドメインの展開では、現在のドメインで作成されたオブジェクトが表示されます。このオブジェクトは編集できます。先祖ドメインで作成されたオブジェクトも表示されますが、ほとんどの場合これは編集できません。子孫ドメインにあるオブジェクトを表示および編集するには、そのドメインに切り替えます。

ステップ 1 **[Objects]** > **[Object Management]**を選択します。

ステップ 2 [PKI] ノードを展開し、[内部 CA（Internal CAs）] を選択します。

ステップ 3 [CA の生成（Generate CA）] をクリックします。

ステップ 4 名前を入力します。

マルチドメイン展開では、オブジェクト名をドメイン階層内で一意にする必要があります。システムは、現在のドメインでは表示できないオブジェクトの名前との競合を特定することができます。

ステップ 5 ID 属性を入力します。

ステップ 6 [自己署名 CA の生成（Generate self-signed CA）] をクリックします。

新しい署名付き証明書

署名付き証明書を CA から取得することによって、内部 CA オブジェクトを設定できます。これは、次の 2 段階からなります。

- 内部 CA オブジェクトを設定するための識別情報を指定します。これにより、未署名の証明書およびペアになった秘密鍵が生成され、指定した CA に対する証明書署名要求（CSR）が作成されます。
- CA により署名付き証明書が発行されたら、それを内部 CA オブジェクトにアップロードして、未署名の証明書と置き換えます。

署名付き証明書が含まれている場合にのみ、SSL ルールで内部 CA オブジェクトを参照できます。

未署名の CA 証明書と CSR の作成

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	すべて（NGIPSv を除く）	いずれか（Any）	Admin/Access Admin/Network Admin

ステップ 1 **[Objects]** > **[Object Management]**を選択します。

ステップ 2 [PKI] ノードを展開し、[内部 CA（Internal CAs）] を選択します。

ステップ 3 [CA の生成（Generate CA）] をクリックします。

ステップ 4 名前を入力します。

マルチドメイン展開では、オブジェクト名をドメイン階層内で一意にする必要があります。システムは、現在のドメインでは表示できないオブジェクトの名前との競合を特定することができます。

ステップ 5 ID 属性を入力します。

ステップ 6 [Generate CSR] をクリックします。

ステップ 7 CA に送信するために CSR をコピーします。

ステップ 8 [OK] をクリックします。

次のタスク

- CA によって発行される署名済み証明書をアップロードする必要があります。次のページを参照してください。 CSR への応答として発行された署名付き証明書のアップロード （584 ページ）

CSR への応答として発行された署名付き証明書のアップロード

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	すべて（NGIPSv を除く）	いずれか（Any）	Admin/Access Admin/Network Admin

マルチドメインの展開では、現在のドメインで作成されたオブジェクトが表示されます。このオブジェクトは編集できます。先祖ドメインで作成されたオブジェクトも表示されますが、ほとんどの場合これは編集できません。子孫ドメインにあるオブジェクトを表示および編集するには、そのドメインに切り替えます。

一度アップロードすると、署名付き証明書は SSL ルールで参照できます。

ステップ 1 **[Objects]** > **[Object Management]**を選択します。

ステップ 2 [PKI] ノードを展開し、[内部 CA（Internal CAs）] を選択します。

ステップ 3 CSR を待機している未署名の証明書を含む CA オブジェクトの横の編集アイコン（  ）をクリックします。

ステップ 4 [Install Certificate] をクリックします。

ステップ 5 [参照（Browse）] をクリックして、DER または PEM でエンコードされた X.509 v3 CA 証明書ファイルをアップロードします。

ステップ 6 アップロード ファイルがパスワード保護されている場合は、[暗号化済み、パスワード：（Encrypted, and the password is:）] チェック ボックスをオンにして、パスワードを入力します。

ステップ 7 [保存（Save）] をクリックして、CA オブジェクトに署名付き証明書をアップロードします。

次のタスク

- アクティブ ポリシーがオブジェクトを参照する場合は、設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

CA 証明書および秘密キーのダウンロード

証明書および鍵の情報を含むファイルを内部 CA オブジェクトからダウンロードすることにより、CA 証明書およびペアになった秘密鍵をバックアップまたは転送できます。

注意 ダウンロードされた鍵情報は必ず安全な場所に保存してください。

システムは、内部 CA オブジェクトに保存されている秘密鍵をディスクに保存する前に、ランダムに生成された鍵を使って暗号化します。証明書および秘密鍵を内部 CA オブジェクトからダウンロードすると、システムはまず情報を復号化してから、証明書および秘密鍵の情報を含むファイルを作成します。その後、ダウンロードファイルを暗号化するためにシステムで使われるパスワードを提供する必要があります。

注意 システムバックアップの一部としてダウンロードされる秘密鍵は、復号化されてから、非暗号化バックアップ ファイルに保存されます。

CA 証明書と秘密キーのダウンロード

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	すべて（NGIPSv を除く）	いずれか（Any）	Admin/Access Admin/Network Admin

マルチドメインの展開では、現在のドメインで作成されたオブジェクトが表示されます。このオブジェクトは編集できます。先祖ドメインで作成されたオブジェクトも表示されますが、ほとんどの場合これは編集できません。子孫ドメインにあるオブジェクトを表示および編集するには、そのドメインに切り替えます。

現在のドメインおよび先祖ドメインの両方の CA 証明書をダウンロードできます。

ステップ 1 **[Objects]** > **[Object Management]**を選択します。

ステップ 2 [PKI] ノードを展開し、[内部 CA（Internal CAs）] を選択します。

ステップ 3 証明書および秘密キーをダウンロードする対象となる内部 CA オブジェクトの横の編集アイコン（）をクリックします。

マルチドメイン導入では、表示アイコン（）をクリックして、先祖ドメインのオブジェクトの証明書および秘密キーをダウンロードします。

ステップ 4 [Download] をクリックします。

ステップ 5 [パスワード（Password）] および [パスワードの確認（Confirm Password）] フィールドに、暗号化パスワードを入力します。

ステップ 6 [OK] をクリックします。

信頼できる認証局オブジェクト

設定した信頼できる認証局（CA）オブジェクトは、それぞれ信頼できるCAに属するCA公開鍵証明書を表します。このオブジェクトは、オブジェクト名とCA公開鍵証明書からなります。次のものに設定された外部CAオブジェクトとグループを使用できます。

- 信頼できるCA、または信頼チェーン内のいずれかのCAによって署名された証明書で暗号化されたトラフィックを制御するためのSSLポリシー。
- LDAPまたはADサーバへのセキュアな接続を確立するためのレルムの設定。
- ISE/ISE-PIC接続。[pxGridサーバCA（pxGrid Server CA）]フィールドと[MNTサーバCA（MNT Server CA）]フィールドで信頼できる認証局オブジェクトを選択します。

信頼できるCAオブジェクトを作成した後で、その名前を変更したり、証明書失効リスト（CRL）を追加したりすることはできますが、他のオブジェクトプロパティを変更することはできません。オブジェクトに追加できるCRLの数には制限がありません。オブジェクトにアップロード済みのCRLを変更するには、オブジェクトをいったん削除して再作成する必要があります。

（注） オブジェクトがISE/ISE-PIC統合設定で使用されている場合は、オブジェクトにCRLを追加しても影響はありません。

使用中の信頼できるCAオブジェクトを削除することはできません。また、使用中の信頼できるCAオブジェクトを編集すると、関連付けられているアクセス コントロール ポリシーが最新ではなくなります。変更を有効にするには、アクセス コントロール ポリシーを再度展開する必要があります。

信頼できる CA オブジェクト

外部CAオブジェクトは、X.509 v3 CA証明書をアップロードすることによって設定できます。次のサポートされている形式のいずれかでエンコードしたファイルをアップロードできます。

- 識別符号化規則（DER）
- プライバシー強化電子メール（PEM）

ファイルがパスワード保護されている場合は、復号パスワードを提供する必要があります。証明書がPEM形式でエンコードされている場合は、情報をコピーして貼り付けることもできます。

ファイルに適切な証明書情報が含まれる場合にのみ、CA証明書をアップロードできます。システムはオブジェクトを保存する前に証明書を検証します。

信頼できる CA オブジェクトの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	すべて（NGIPSv を除く）	いずれか（Any）	Admin/Access Admin/Network Admin

ステップ 1 **[Objects]** > **[Object Management]**を選択します。

ステップ 2 [PKI] ノードを展開し、[信頼できる CA（Trusted CAs）] を選択します。

ステップ 3 [信頼できる CA の追加（Add Trusted CAs）] をクリックします。

ステップ 4 名前を入力します。

マルチドメイン展開では、オブジェクト名をドメイン階層内で一意にする必要があります。システムは、現在のドメインでは表示できないオブジェクトの名前との競合を特定することができます。

ステップ 5 [参照（Browse）] をクリックして、DER または PEM でエンコードされた X.509 v3 CA 証明書ファイルをアップロードします。

ステップ 6 ファイルがパスワード保護されている場合は、[暗号化、パスワード：（Encrypted, and the password is:）] チェックボックスをオンにして、パスワードを入力します。

ステップ 7 **[保存（Save）]** をクリックします。

次のタスク

- アクティブポリシーがオブジェクトを参照する場合は、設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

信頼できる CA オブジェクトの証明書失効リスト

信頼できる CA オブジェクトに CRL をアップロードできます。信頼できる CA オブジェクトを SSL ポリシーの中で参照すると、セッションの暗号化証明書を発行した CA がその後で証明書を取り消したかどうかに基づいて、暗号化されたトラフィックを制御できます。サポートされる次のいずれかの形式でエンコードされたファイルをアップロードできます。

- 識別符号化規則（DER）
- プライバシー強化電子メール（PEM）

CRL を追加した後、失効した証明書のリストを表示することができます。オブジェクトにアップロード済みの CRL を変更するには、オブジェクトをいったん削除して再作成する必要があります。

適切な CRL を含んでいるファイルのみをアップロードできます。信頼できる CA オブジェクトに追加できる CRL の数には制限がありません。ただし、CRL をアップロードした場合、別の CRL を追加する前に、オブジェクトをその都度保存する必要があります。

（注） オブジェクトが ISE/ISE-PIC 統合設定で使用されている場合は、オブジェクトに CRL を追加しても影響はありません。

信頼できる CA オブジェクトへの証明書失効リストの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	すべて（NGIPSv を除く）	いずれか（Any）	Admin/Access Admin/Network Admin

マルチドメインの展開では、現在のドメインで作成されたオブジェクトが表示されます。このオブジェクトは編集できます。先祖ドメインで作成されたオブジェクトも表示されますが、ほとんどの場合これは編集できません。子孫ドメインにあるオブジェクトを表示および編集するには、そのドメインに切り替えます。

（注） オブジェクトが ISE/ISE-PIC 統合設定で使用されている場合は、オブジェクトに CRL を追加しても影響はありません。

ステップ 1 **[Objects]** > **[Object Management]**を選択します。

ステップ 2 [PKI] ノードを展開し、[信頼できる CA（Trusted CAs）] を選択します。

ステップ 3 信頼できる CA オブジェクトの横にある編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 4 [CRL の追加（Add CRL）] をクリックして、DER または PEM でエンコードされた CRL ファイルをアップロードします。

ステップ 5 [OK] をクリックします。

次のタスク

- アクティブ ポリシーがオブジェクトを参照する場合は、設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

外部証明書オブジェクト

設定済みのそれぞれの外部証明書オブジェクトは、組織に属さないサーバ公開鍵証明書を表します。このオブジェクトは、オブジェクト名と証明書からなります。SSLルールで外部証明書オブジェクトとグループを使用すると、サーバ証明書で暗号化されたトラフィックを制御できます。たとえば、信頼できる自己署名サーバ証明書をアップロードできますが、信頼できるCA 証明書を使って検証することはできません。

X.509 v3 サーバ証明書をアップロードすることによって、外部証明書オブジェクトを設定できます。サポートされている次のいずれかの形式のファイルをアップロードできます。

- 識別符号化規則（DER）
- プライバシー強化電子メール（PEM）

適切なサーバ証明書情報を含んでいるファイルだけをアップロードできます。システムはオブジェクトを保存する前にファイルを検証します。証明書が PEM 形式でエンコードされている場合は、情報をコピーして貼り付けることもできます。

外部証明書オブジェクトの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	すべて（NGIPSvを除く）	いずれか（Any）	Admin/Access Admin/Network Admin

ステップ 1 **[Objects]** > **[Object Management]**を選択します。

ステップ 2 [PKI] ノードを展開し、[外部証明書（External Certs）] を選択します。

ステップ 3 [外部証明書の追加（Add External Cert）] をクリックします。

ステップ 4 名前を入力します。

マルチドメイン展開では、オブジェクト名をドメイン階層内で一意にする必要があります。システムは、現在のドメインでは表示できないオブジェクトの名前との競合を特定することができます。

ステップ 5 [証明書データ（Certificate Data）] フィールドの上部にある [参照（Browse）] をクリックして、DER または PEM でエンコードされた X.509 v3 サーバ証明書ファイルをアップロードします。

ステップ 6 **[保存（Save）]** をクリックします。

次のタスク

- アクティブポリシーがオブジェクトを参照する場合は、設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

内部証明書オブジェクト

設定済みのそれぞれの内部証明書オブジェクトは、組織に属するサーバ公開鍵証明書を表します。このオブジェクトは、オブジェクト名、公開鍵証明書、およびペアになった秘密鍵からなります。内部証明書オブジェクトとグループは、以下で使用することができます。

- SSL ルール。既知の秘密キーを使用する組織のサーバの 1 つに着信するトラフィックを復号します。
- ISE/ISE-PIC 接続。[MC サーバ証明書（MC Server Certificate）] フィールド用の内部証明書オブジェクトを選択します。
- キャプティブ ポータル設定。ユーザの Web ブラウザに接続する際にキャプティブ ポータル デバイスのアイデンティティを認証するように設定します。[サーバ証明書（Server Certificate）] フィールド用の内部証明書オブジェクトを選択します。

X.509 v3 RSA ベースまたは楕円曲線ベースのサーバ証明書およびペアの秘密キーをアップロードすることにより、内部証明書オブジェクトを設定できます。サポートされている次のいずれかの形式のファイルをアップロードできます。

- 識別符号化規則（DER）
- プライバシー強化電子メール（PEM）

ファイルがパスワード保護されている場合は、復号パスワードを提供する必要があります。証明書とキーが PEM 形式でエンコードされている場合は、情報をコピーして貼り付けることもできます。

適切な証明書またはキーの情報を含んでいる、相互にペアになっているファイルのみをアップロードできます。システムはオブジェクトを保存する前にペアを検証します。

内部証明書オブジェクトを作成した後、その名前を変更することはできますが、他のオブジェクト プロパティを変更することはできません。

使用中の内部証明書オブジェクトは削除できません。さらに、使用中の内部証明書オブジェクトを編集すると、関連するアクセス コントロール ポリシーが失効します。変更を反映させるには、アクセス コントロール ポリシーを再度展開する必要があります。

内部証明書オブジェクトの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	すべて（NGIPSv を除く）	いずれか（Any）	Admin/Access Admin/Network Admin

ステップ 1 **[Objects]** > **[Object Management]**を選択します。

ステップ 2 [PKI] ノードを展開し、[内部証明書（Internal Certs）] を選択します。

ステップ 3 [内部証明書の追加（Add Internal Cert）] をクリックします。

ステップ 4 名前を入力します。

マルチドメイン展開では、オブジェクト名をドメイン階層内で一意にする必要があります。システムは、現在のドメインでは表示できないオブジェクトの名前との競合を特定することができます。

ステップ 5 [証明書データ（Certificate Data）] フィールドの上部にある [参照（Browse）] をクリックして、DER または PEM でエンコードされた X.509 v3 サーバ証明書ファイルをアップロードします。

ステップ 6 [キー（Key）] フィールドの上部にある [参照（Browse）] をクリックして、DER または PEM でエンコードされたペアの秘密キー ファイルをアップロードします。

ステップ 7 アップロードする秘密キー ファイルがパスワード保護されている場合は、[暗号化済み、パスワード：（Encrypted, and the password is:）] チェックボックスをオンにして、パスワードを入力します。

ステップ 8 **[保存（Save）]** をクリックします。

証明書の登録オブジェクト

トラストポイントを使用すると、CA と証明書の管理とトレースができます。トラストポイントとは、CA または ID ペアを表現したものです。トラストポイントには、CA の ID、CA 固有のコンフィギュレーション パラメータ、登録されている ID 証明書とのアソシエーションが含まれています。

証明書の登録オブジェクトには、証明書署名要求（CSR）を作成したり、指定された CA からアイデンティティ証明書を取得したりするために必要な証明機関（CA）サーバ情報や登録パラメータが含まれています。これらのアクティビティは、秘密キー インフラストラクチャ（PKI）で発生します。

証明書の登録オブジェクトには、証明書失効情報も含まれている場合があります。PKI、デジタル証明書、および証明書の登録の詳細については、PKI インフラストラクチャとデジタル証明書 （1062 ページ） を参照してください。

証明書の登録オブジェクト の使用方法

証明書の登録オブジェクト は、管理対象デバイスを PKI インフラストラクチャに登録し、以下を実行することで VPN 接続をサポートするデバイス上にトラストポイント（CA オブジェクト）を作成するために使用されます。

1. 証明書の登録オブジェクトの CA 認証と登録のパラメータを定義します。共有パラメータを指定し、オーバーライド機能を使用して、異なるデバイスに固有のオブジェクト設定を指定します。
2. アイデンティティ証明書を必要とする各管理対象デバイスにこのオブジェクトを関連付けてインストールします。デバイス上で、そのオブジェクトはトラストポイントになります。

   証明書の登録オブジェクトがデバイスに関連付けられ、デバイスにインストールされるとすぐに証明書の登録プロセスが開始されます。プロセスは、自己署名、SCEP、および PKCS12 ファイル登録タイプの場合は自動的に行われます。つまり、管理者による追加の

アクションは必要ありません。手動証明書登録では、さらに管理者の操作が必要になります。

3. 作成されたトラストポイントを VPN の設定で指定します。

証明書の登録オブジェクト の管理

証明書の登録オブジェクト を管理するには、[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] に移動し、ナビゲーション ウィンドウから [PKI] > [証明書の登録（Certificate Enrollment）] を選択します。次の情報が表示されます。

- 既存の証明書の登録オブジェクトが [名前（Name）] 列に表示されます。

  リストをフィルタリングするには検索フィールド（虫めがね）を使用します。

- 各オブジェクトの登録タイプが [タイプ（Type）] 列に表示されます。次の登録方式を使用できます。

  - [自署（Self Signed）]：管理対象デバイスが独自の自己署名ルート証明書を生成します。
  - [SCEP]：（デフォルト）Simple Certificate Enrollment Protocol は、CA からアイデンティティ証明書を取得するためにデバイスで使用されます。
  - [手動（Manual）]：登録のプロセスは、管理者によって手動で実行されます。
  - PKCS12 ファイル（PKCS12 File）：VPN の接続をサポートする Firepower Threat Defense の管理対象デバイスで PKCS12 ファイルをインポートします。PKCS#12（PFX または P12）ファイルとは、サーバ証明書、中間証明書、秘密キーのすべてを暗号化して保持するファイルです。復号のための [パスフレーズ（Passphrase）] 値を入力します。

- [オーバーライド（Override）] 列は、オブジェクトがオーバーライド（緑のチェック マーク）を許可するかしないか（赤の X）を示します。数が表示される場合、これはオーバーライドの数です。

  [オーバーライド（Override）] オプションを使用して、VPN 設定の一部である各デバイスのオブジェクト設定をカスタマイズします。オーバーライドすると、各デバイスのトラストポイントの詳細が一意になります。通常、共通名またはサブジェクトは、VPN の設定内の各デバイスに対して上書きされます。

  任意のタイプのオブジェクトのオーバーライドに関する詳細および手順については、オブジェクトのオーバーライド （522 ページ）を参照してください。

- 編集アイコン（鉛筆）をクリックして、前に作成した 証明書の登録オブジェクト を**編集**します。編集は、登録オブジェクトがどの管理対象デバイスにも関連付けられていない場合にのみ実行できます。証明書の登録オブジェクトの編集については、追加の手順を参照してください。失敗した登録オブジェクトを編集できます。

- 削除アイコン（ごみ箱）をクリックして、前に作成した 証明書の登録オブジェクト を**削除**します。管理対象デバイスに関連付けられている証明書の登録オブジェクトは削除できません。

[（+）証明書登録の追加（(+) Add Cert Enrollment）] を押して、[証明書登録の追加（Add Cert Enrollment）] ダイアログを開き、証明書の登録オブジェクト を設定します。証明書の登録オブジェクトの追加（593ページ）を参照してください。次に、管理対象のヘッドエンドデバイスごとに証明書をインストールします。

関連トピック

自己署名登録を使用した証明書のインストール （643 ページ）
SCEP の登録を使用した証明書のインストール （644 ページ）
手動登録を使用した証明書のインストール （645 ページ）
PKCS12 ファイルを使用した証明書のインストール （646 ページ）

証明書の登録オブジェクトの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin/Network Admin

ステップ 1 以下の方法のいずれかにより、[証明書登録の追加（Add Cert Enrollment）] ダイアログを開きます。

- オブジェクト管理から直接開く：[オブジェクト（Objects）]>[オブジェクト管理（Object Management）] 画面で、[ナビゲーション（Navigation）] ペインの [PKI] > [証明書の登録（Cert Enrollment）] を選択し、[証明書の登録の追加（Add Cert Enrollment）] を押します。
- 管理対象デバイスの設定中に開く：**[デバイス（Devices）] > [証明書（Certificates）]** 画面で、**[追加（Add）] > [新しい証明書の追加（Add New Certificate）]** を選択し、**[証明書の登録（Certificate Enrollment）]** フィールドの **(+)** をクリックします。

ステップ 2 [名前（Name）] を入力し、任意で登録するオブジェクトの [説明（Description）] を入力します。

登録が完了すると、この名前が関連付けられた管理対象デバイスのトラストポイントの名前になります。

ステップ 3 [CA 情報（CA Information）] タブを開いてから、[登録タイプ（Enrollment Type）] を選択します。

- [自己署名証明書（Self-Signed Certificate）]：管理対象デバイスが CA として機能し、自己の署名付きルート証明書を生成します。このペインでは、さらに必要となる情報はありません。

  （注） 自己署名証明書を登録するときには、証明書パラメータで共通名（CN）を指定する必要があります。

- [SCEP]：（デフォルト）Simple Certificate Enrollment Protocol。SCEP 情報を指定します。証明書の登録オブジェクト SCEP オプション （594 ページ）を参照してください。
- [手動（Manual）]：取得した CA 証明書を [CA 証明書（CA Certificate）] フィールドに貼り付けます。CA 証明書は別のデバイスからコピーして取得できます。
- [PKCS12 ファイル（PKCS12 File）]：VPN 接続をサポートしている FTD 管理対象デバイスの PKCS 12 ファイルをインポートします。PKCS#12 ファイル、または PFX ファイルは、サーバ証明書、中間証明

書、秘密キーが含まれる単一の暗号化ファイルです。復号のための[パスフレーズ（Passphrase）]値を入力します。

ステップ 4 （任意）[証明書のパラメータ（Certificate Parameters）]タブを開き、証明書の内容を指定します。証明書の登録オブジェクト 証明書のパラメータ （595 ページ）を参照してください。

この情報は、証明書に格納され、このルータから証明書を受信するすべての第三者が表示できます。

ステップ 5 （任意）[キー（Key）]タブを開き、キーの内容を指定します。証明書の登録オブジェクト の主要なオプション （597 ページ）を参照してください。

ステップ 6 （任意）[失効（Revocation）]タブをクリックし、失効のオプションを指定します。証明書の登録オブジェクト 失効オプション （597 ページ）を参照してください。

ステップ 7 必要に応じ、このオブジェクトについて[オーバーライドを許可（Allow Overrides）]しておきます。オブジェクトのオーバーライドの詳細はオブジェクトのオーバーライド （522 ページ）を参照してください。

次のタスク

デバイスのトラストポイントを作成するため、デバイスの登録オブジェクトの関連付けとインストールを行います。

関連トピック

自己署名登録を使用した証明書のインストール （643 ページ）
SCEP の登録を使用した証明書のインストール （644 ページ）
手動登録を使用した証明書のインストール （645 ページ）
PKCS12 ファイルを使用した証明書のインストール （646 ページ）

証明書の登録オブジェクト SCEP オプション

Firepower Management Center ナビゲーション パス

[オブジェクト（Objects）]>[オブジェクト管理（Object Management）]の次に、ナビゲーション ウィンドウから **[PKI] > [PKI 登録（PKI Enrollment）]** を選択します。[（+）PKI 登録の追加（(+) Add PKI Enrollment）]を押して、[PKI 登録の追加（Add PKI Enrollment）]ダイアログを開き、[CA 情報（CA Information）]タブを選択します。

フィールド

[登録タイプ（Enrollment Type）]：[SCEP] に設定します。

[登録 URL（Enrollment URL）]：デバイスが登録を試行する先の CA サーバの URL。

`http://CA_name:port` の形式の HTTP URL を使用します。ここで、CA_name は CA サーバのホスト DNS 名または IP アドレスです。ポート番号は必須です。

（注） SCEP サーバがホスト名/FQDN で参照されている場合は、FlexConfig オブジェクトを使用して DNS サーバを設定します。

CA での CA cgi-bin スクリプト位置がデフォルト（/cgi-bin/pkiclient.exe）でない場合は、その標準以外のスクリプト位置を http://CA_name:port/script_location の形式で URL に含める必要があります。ここで、script_location は CA スクリプトへのフル パスです。

[チャレンジ パスワード/パスワードの確認（Challenge Password/Confirm Password）]：CA サーバがデバイスの ID を検証するために使用するパスワード。CA サーバに直接アクセスして、または Web ブラウザにアドレス（**http://URLHostName/certsrv/mscep/mscep.dll**）を入力して、パスワードを取得できます。このパスワードは、CA サーバから取得した時間から 60 分間有効です。したがって、パスワードは、作成後、できるだけ迅速に配布する必要があります。

[再試行期間（Retry Period）]：証明書要求の試行間隔（分数）。値には 1 ～ 60 分を指定できます。デフォルトは 1 分です。

[再試行回数（Retry Count）]：最初の要求時に証明書が発行されていない場合、実行する再試行回数。1 ～ 100 の値を指定できます。デフォルトは 10 です。

[CA 証明書の取得元（CA Certificate Source）]：CA 証明書の取得方法を指定します。

- [SCEP を使用した取得（Retrieve Using SCEP）]（デフォルトであり、唯一サポートされているオプション）：Simple Certificate Enrollment Process（SCEP）を使用して CA サーバから証明書を取得します。SCEP を使用するにはデバイスと CA サーバとの間の接続が必要です。登録プロセスを開始する前に、デバイスから CA サーバへのルートがあることを確認します。

[フィンガープリント（Fingerprint）]：SCEP を使用して CA 証明書を取得する場合、CA サーバのフィンガープリントを入力する必要があります。フィンガープリントを使用して CA サーバの証明書の真正性を確認すると、不正な第三者が、本物の証明書を偽の証明書に置き換えることを阻止できます。CA サーバの [フィンガープリント（Fingerprint）] には 16 進数形式で入力します。入力した値が証明書のフィンガープリントと一致しない場合、証明書は拒否されます。サーバに直接アクセスして、または Web ブラウザにアドレス（**http://<URLHostName>/certsrv/mscep/mscep.dll**）を入力して、CA のフィンガープリントを取得します。

証明書の登録オブジェクト 証明書のパラメータ

CA サーバに送信される証明書要求に、その他の情報を指定します。この情報は、証明書に格納され、このルータから証明書を受信するすべての第三者が表示できます。

Firepower Management Center ナビゲーション パス

[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] の次に、ナビゲーション ウィンドウから **[PKI] > [PKI 登録（PKI Enrollment）]** を選択します。[（+）PKI 登録の追

加（(+) Add PKI Enrollment）] を押して、[PKI 登録の追加（Add PKI Enrollment）] ダイアログを開き、[証明書のパラメータ（Certificate Parameters）] タブを選択します。

フィールド

標準の LDAP X.500 形式を使用して、すべての情報を入力します。

- [FQDN を含む（Include FQDN）]：デバイスの Fully Qualified Domain Name（FQDN; 完全修飾ドメイン名）を証明書要求に含めるかどうかを指定します。選択肢は次のとおりです。
  - **[デバイスのホスト名を FQDN として使用（Use Device Hostname as FQDN）]**
  - **[証明書には FQDN を使用しない（Don't use FQDN in certificate）]**
  - [カスタム FQDN（Custom FQDN）]：これを選択し、表示された [カスタム FQDN（Custom FQDN）] フィールドに指定します。
- [デバイスの IP アドレスを含める（Include Device's IP Address）]：IP アドレスが証明書要求に含まれているインターフェイス。
- [共通名（CN）（Common Name (CN)）]：証明書に含める X.500 共通名。

（注） 自己署名証明書を登録するときには、証明書パラメータで共通名（CN）を指定する必要があります。

- [組織単位（OU）（Organizational Unit (OU)）]：証明書に含める組織単位の名前（部門名など）。
- [組織（O）（Organization (O)）]：証明書に含める組織または会社の名前。
- [地域（L）（Locality (L)）]：証明書に含める地域。
- [都道府県（ST）（State (ST)）]：証明書に含める州または都道府県。
- [国コード（C）（County Code (C)）]：証明書に含める国。これらのコードは、ISO 3166 の国の省略形に準拠しています（たとえばアメリカ合衆国は「US」）。
- [電子メール（E）（Email (E)）]：証明書に含める電子メール アドレス。
- [デバイスのシリアル番号を含める（Include Device's Serial Number）]：デバイスのシリアル番号を証明書に含めるかどうかを指定します。CA は、このシリアル番号を使用して、証明書を認証するか、またはあとで証明書を特定のデバイスに関連付けます。シリアル番号を含めるかどうか判断できない場合は、デバッグに役立つため、含めてください。

証明書の登録オブジェクト の主要なオプション

Firepower Management Center ナビゲーション パス

[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] の次に、ナビゲーション ウィンドウから **[PKI] > [PKI 登録（PKI Enrollment）]** を選択します。[（+）PKI 登録の追加（(+) Add PKI Enrollment）] を押して、[PKI 登録の追加（Add PKI Enrollment）] ダイアログを開き、[キー（Key）] タブを選択します。

フィールド

- [キー タイプ（Key Type）]：RSA（デフォルト、およびサポートされるオプションのみ）または ECDSA。
- [キー名（Key Name）]：証明書と関連付けるキー ペアが既に存在する場合、このフィールドではそのキー ペアの名前を指定します。キー ペアが存在しない場合、このフィールドには登録中に生成されるキー ペアに指定する名前を指定します。RSA キー ペアを指定しない場合、Fully Qualified Domain Name（FQDN; 完全修飾ドメイン名）が代わりに使用されます。
- [キー サイズ（Key Size）]：キー ペアが存在しない場合は、必要なキー サイズ（係数）をビットで定義します。推奨サイズは 1024 です。係数のサイズが大きくなるほど、キーがよりセキュアになります。ただし、係数のサイズが大きいキーほど、生成に時間がかかり（512 ビットより大きい場合は 1 分以上）、交換するときの処理にも時間がかかります。
- [詳細設定（Advanced Settings）]：IPsec リモート クライアント証明書の、キーの使用状況エクステンションおよび拡張キーの使用状況エクステンションの値を検証しない場合は、[IPsecキーの使用状況を無視（Ignore IPsec Key Usage）] を選択します。IPsec クライアント証明書のキーの使用状況チェックを行わないようにできます。デフォルトでは、このオプションは無効になっています。

（注） サイト間VPN接続では、Windows認証局（CA）を使用する場合、デフォルトのアプリケーション ポリシー拡張は **IP セキュリティ IKE 中間**です。このデフォルト設定を使用している場合は、選択したオブジェクトで [IPsecキーの使用状況を無視（Ignore IPsec Key Usage）] オプションを選択する必要があります。それ以外の場合、エンドポイントはサイト間 VPN 接続を完了できません。

証明書の登録オブジェクト 失効オプション

証明書の失効ステータスを確認するかどうかを、方法を選択して設定することで指定します。失効の確認はデフォルトでオフになっており、どちらの方法（CRL または OCSP）もオンになっていません。

Firepower Management Center ナビゲーション パス

[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] の次に、ナビゲーション ウィンドウから **[PKI] > [PKI 登録（PKI Enrollment）]** を選択します。[（+）PKI 登録の追加（(+) Add PKI Enrollment）] を押して、[PKI 登録の追加（Add PKI Enrollment）] ダイアログを開き、[失効（Revocation）] タブを選択します。

フィールド

- [証明書失効リストの有効化（Enable Certificate Revocation Lists）]：CRL の確認を有効にするにはオンにします。
  - [証明書からの CRL 分散ポイント（Use CRL distribution point from the certificate）]：証明書からの失効リスト配布 URL を取得するにはオンにします。
  - [設定された静的 URL を使用（Use static URL configured）]：失効リストのスタティックな事前定義された配布 URL を追加するには、これをオンにします。次に URL を追加します。

    [CRL サーバの URL（CRL Server URLs）]：CRL をダウンロード可能な LDAP サーバの URL。この URL は **ldap://** から始まり、URL にはポート番号が含まれる必要があります。

- [Online Certificate Status Protocol（OCSP）の有効化（Enable Online Certificate Status Protocol）]：OCSP チェックを有効にするにはオンにします。

  [OCSP サーバ URL（OCSP Server URL）]：OCSP チェックを必須としている場合に、失効をチェックする OCSP サーバの URL。この URL は、**http://** で始まる必要があります。

- [失効情報にアクセスできない場合、証明書は有効と見なされます（Consider the certificate valid if revocation information can not be reached）]：デフォルトでオンになっています。これを許可しない場合は、チェックボックスをオフにします。

キー チェーンのオブジェクト

デバイスのデータ セキュリティと保護を向上させるため、IGP ピアを認証するために 180 日以下の期間の循環キーが展開されています。循環キーは、悪意のあるユーザがルーティング プロトコル認証に使用されているキーを推測できないようにし、ネットワークによる誤ったルートのアドバタイズやトラフィックのリダイレクトを防ぎます。頻繁にキーを変更することで、推測されるリスクを最終的に軽減します。キー チェーンを提供するルーティング プロトコルの認証を設定する場合は、キーチェーン内でキーを設定してライフタイムを重複させます。こうすることによって、キーで保護された通信がアクティブなキーがないことよって損失することを防ぐために役立ちます。循環キーは OSPFv2 プロトコルにのみ適用されます。キーのライフタイムが切れ、アクティブなキーがなくなると、OSPF は最後に有効だったキーを使用してピアとの隣接関係を維持します。

（注） 認証に使用されるのは MD5 暗号化アルゴリズムのみです。

キーのライフタイム

安定した通信を維持するためには、各デバイスがキー チェーンの認証キーを保存し、複数のキーを同時に機能に使用します。キーの送信と受け入れのライフタイムに基づき、キーのロールオーバーを処理するセキュアなメカニズムがキーチェーン管理によって提供されます。デバイスは、キーのライフタイムを使用してキーチェーン内でアクティブになっているキーを判断します。

キー チェーン内の各キーには 2 つのライフタイムがあります。

- 受け入れライフタイム：別のデバイスとのキー交換時にデバイスがそのキーを受け入れる期間。
- 送信ライフタイム：別のデバイスとのキー交換時にデバイスがそのキーを送信する期間。

キーの送信ライフタイム中、デバイスはルーティング アップデート パケットをキーとともに送信します。送信されたキーがデバイス上のキーの受け入れライフタイム期間内でない場合、そのデバイスはキーを送信したデバイスからの通信を受け入れません。

ライフタイムが設定されていない場合は、タイムラインなしで MD5 認証を設定するのと同じことになります。

キーの選択

- キー チェンに複数の有効なキーがある場合、OSPF はライフタイムが最大のキーを選択します。
- ライフタイムが無限のキーが優先されます。
- ライフタイムが同じキーが複数ある場合は、もっとも大きなキー ID を持つキーが優先されます。

キー チェーンのオブジェクトの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Access Admin/Network Admin

ステップ 1 **[Objects]** > **[Object Management]**を選択します。

ステップ 2 オブジェクト タイプのリストから [キー チェーン（Key Chain）] を選択します。

ステップ 3 [キー チェーンの追加（Add Key Chain）] をクリックします。

ステップ 4 [キー チェーン オブジェクトの追加（Add Key Chain Object）] ダイアログボックスで、キー チェーンの名前を [名前（Name）] フィールドに入力します。

名前はアンダースコアまたはアルファベットから開始し、英数字文字または特殊文字（-、 _、+、 .）を続けます。

ステップ 5 キーをキー チェーンに追加するには、[追加（Add）] をクリックします。

ステップ 6 [キー ID（Key ID）] フィールドにキー識別子を指定します。

キー ID の値には 0 ～ 255 を使用できます。無効なキーを通知する場合にのみ、値 0 を使用します。

ステップ 7 [アルゴリズム（Algorithm）] フィールドと [暗号化タイプ（Crypto Encryption Type）] フィールドにサポート対象のアルゴリズムと暗号化タイプ、つまり [MD5] と [プレーン テキスト（Plain Text）] がそれぞれ表示されます。

ステップ 8 [暗号キー文字列（Crypto Key String）] フィールドにパスワードを入力し、[暗号キー文字列の確認（Confirm Crypto Key String）] フィールドにパスワードを再入力します。

- パスワードの最大長は 80 文字です。
- パスワードは 10 文字以上必要です。また、数字の後に空白を含む文字列は使用できません。たとえば、「0 pass」や「1」は無効です。

ステップ 9 デバイスが他のデバイスとキー交換をしている間にキーを受領/送信する時間間隔をデバイスに設定するには、[受け入れライフタイム（Accept Lifetime）] フィールドと [送信ライフタイム（Send Lifetime）] フィールドにライフタイムの値を指定します。

（注） デフォルトでは、日時の値は UTC タイムゾーンになります。

終了時刻は、期間、受け入れ/送信ライフタイムが終了する絶対時間、または無期限です。デフォルトの終了時刻は、DateTime です。

次に、開始と終了の値についての検証ルールを示します。

- 終了ライフタイムを指定した場合、開始ライフタイムを null にできません。
- 受け入れまたは送信のライフタイムの開始ライフタイムは、それぞれの終了時刻よりも前である必要があります。

ステップ 10 [追加（Add）] をクリックします。

ステップ 5 ～ 10 を繰り返してキーを作成します。キー チェーンにはライフタイムが重複するキーを 2 つ以上作成します。こうすることによって、キーで保護された通信がアクティブなキーがないことよって損失することを防ぐために役立ちます。

ステップ 11 オブジェクトのオーバーライドを管理します。

- このオブジェクトのオーバーライドを許可する場合は、[Allow Overrides] チェックボックスをオンにします（オブジェクトのオーバーライドの許可 （524 ページ）を参照）。
- このオブジェクトにオーバーライド値を追加する場合は、[Override] セクションを展開し、[Add] をクリックします（オブジェクトのオーバーライドの追加 （524 ページ）を参照）。

ステップ 12 **[保存（Save）]** をクリックします。

次のタスク

- アクティブ ポリシーがオブジェクトを参照する場合は、設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

DNS サーバ グループ オブジェクト

ドメイン ネーム システム（DNS）サーバは、www.example.com などの完全修飾ドメイン名（FQDN）を IP アドレスに解決します。

DNS サーバ グループ オブジェクトの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	NGIPS を除くすべて	任意（Any）	Access Admin/Admin/Network Admin

ステップ 1 **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** を選択します。

ステップ 2 ネットワーク オブジェクト リストから [DNSサーバ グループ（DNS Server Group）] をクリックします。

ステップ 3 [DNS サーバ グループの追加（Add DNS Server Group）] をクリックします。

ステップ 4 [名前（Name）]を入力します。

マルチドメイン展開では、オブジェクト名をドメイン階層内で一意にする必要があります。システムは、現在のドメインでは表示できないオブジェクトの名前との競合を特定することができます。

ステップ 5 状況に応じて、完全修飾されていないホスト名に追加するために使用される [デフォルト ドメイン（Default Domain）] を入力します。

ステップ 6 デフォルトの [タイムアウト（Timeout）] と [再試行（Retries）] の値は事前入力されています。必要に応じて、これらの値を変更します。

- [再試行（Retries）]：システムが応答を受信しない場合に DNS サーバのリストを再試行する回数（0 ～ 10）。デフォルトは 2 です。
- [タイムアウト（Timeout）]：次の DNS サーバを試行する前に待機する秒数（1 ～ 30）。デフォルト値は 2 秒です。システムがサーバのリストを再試行するたびに、このタイムアウトは 2 倍になります。

ステップ 7 このグループの一部になる [DNS サーバ（DNS Servers）] を、IPv4 または IPv6 の形式のカンマ区切りのエントリとして入力します。

1 つのグループには、最大で 6 DNS サーバを含めることができます。

ステップ 8 [保存（Save）] をクリックします。

次のタスク

DNS サーバ グループに設定されている DNS サーバは、DNS プラットフォーム設定でインターフェイス オブジェクトに割り当てる必要があります。詳細については、「DNS の設定 （1360 ページ）」を参照してください。

SLA モニタ オブジェクト

各インターネット プロトコル サービス レベル契約（SLA）モニタでは、モニタリング対象のアドレスへの接続ポリシーを定義し、そのアドレスへのルートの可用性をトラッキングします。ルートの可用性は、ICMP エコー要求を送信し、応答を待機することによって、定期的にチェックされます。要求がタイムアウトすると、そのルートはルーティング テーブルから削除され、バックアップ ルートに置き換えられます。SLA モニタリング ジョブは、デバイス設定から SLA モニタを削除していない限り、展開後すぐに開始して実行し続けます（つまり、ジョブはエージング アウトしません）。インターネット プロトコル サービス レベル契約（SLA）モニタ オブジェクトは、IPv4 スタティック ルート ポリシーの [ルートトラッキング（Route Tracking）] フィールドで使用されます。IPv6 ルートでは、ルート トラッキングによって SLA モニタを使用することはできません.

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin Access Admin Network Admin

ステップ 1 **[オブジェクト（Objects）] > [オブジェクト管理（Object Management）]** を選択し、コンテンツ テーブルから [SLA モニタ（SLA Monitor）] を選択します。

ステップ 2 [SLA モニタの追加（Add SLA Monitor）] をクリックします。

ステップ 3 [名前（Name）] フィールドにオブジェクトの名前を入力します。

ステップ 4 （オプション）[説明（Description）] フィールドにオブジェクトの説明を入力します。

ステップ 5 [頻度（Frequency）] フィールドに、ICMP エコー要求送信の頻度（秒単位）を入力します。有効な値の範囲は、1 ～ 604800 秒（7 日）です。デフォルトは 60 秒です。

（注） 頻度はタイムアウト値未満にできません。これらの値を比較するには、頻度をミリ秒に換算する必要があります。

ステップ 6 [SLA モニタ ID（SLA Monitor ID）] フィールドに SLA 操作の ID 番号を入力します。値の範囲は 1 ～ 2147483647 です。1 つのデバイスには最大で 2000 個の SLA 操作を作成できます。各 ID 番号はポリシーとデバイス設定に対して一意である必要があります。

ステップ 7 [しきい値（Threshold）] フィールドに、上昇しきい値が宣言されるまでに、ICMP エコー要求の後に経過する必要のある時間（ミリ秒単位）を入力します。有効な値の範囲は、0 ～ 2147483647 ミリ秒です。デフォルトは 5000 ミリ秒です。しきい値は、定義された値を超過したイベントを示すためだけに使用されます。これらのイベントは、タイムアウト値が適切であるかどうかを評価するために使用できます。このイベントは、モニタリング対象のアドレスへの到達可能性を直接的に示すものではありません。

（注） しきい値はタイムアウト値を超過しないようにします。

ステップ 8 [タイムアウト（Timeout）] フィールドに、SLA 操作が ICMP エコー要求への応答を待機する時間（ミリ秒単位）を入力します。値の範囲は 0 ～ 604800000 ミリ秒（7 日）です。デフォルトは 5000 ミリ秒です。モニタリング対象のアドレスからの応答がこのフィールドに定義された時間内に受信されない場合、スタティック ルートがルーティング テーブルから削除され、バックアップ ルートに置き換えられます。

（注） タイムアウト値は頻度値を超過できません。2 つの数値を比較するには、頻度値をミリ秒に換算してください。

ステップ 9 [データ サイズ（Data Size）] フィールドに、ICMP 要求パケット ペイロードのサイズ（バイト単位）を入力します。値の範囲は 0 ～ 16384 バイトです。デフォルトは 28 バイトです。この場合、全体の ICMP パケットは 64 バイトとなります。この値には、プロトコルまたは Path Maximum Transmission Unit（PMTU）で許可される最大値を超える値を設定しないでください。場合によっては、到達可能性を確保するために、デフォルトのデータ サイズを大きくして、ソースとターゲットの間での PMTU の違いを検出できるようにすることが必要となります。PMTU が小さいと、セッションのパフォーマンスに影響を及ぼすことがあります。セッションのパフォーマンスへの影響が検出されると、セカンダリ パスが使用されます。

ステップ 10 [ToS] フィールドに、ICMP 要求パケットの IP ヘッダーで定義されたタイプ オブ サービス（ToS）の値を入力します。値の範囲は 0 ～ 255 です。デフォルトは 0 です。このフィールドには、遅延、優先順位、信頼性などの情報が含まれます。この情報は、ポリシー ルーティングのためにネットワーク上の他のデバイスが使用する場合もあれば、専用アクセス レートなどの機能によって使用される場合もあります。

ステップ 11 [パケット数（Number of Packets）] フィールドに、送信されるパケットの数を入力します。値の範囲は 1 ～ 100 です。デフォルトは 1 パケットです。

（注） パケット損失によって、Firepower Threat Defense デバイスがモニタリング対象のアドレスに到達できないと誤って認識することが懸念される場合は、デフォルトのパケット数を大きくしてください。

ステップ 12 [モニタリング対象アドレス（Monitored Address）] フィールドに、SLA 操作によって可用性がモニタされている IP アドレスを入力します。

ステップ 13 [使用可能なゾーン（Available Zones）] リストには、ゾーンとインターフェイス グループの両方が表示されます。[ゾーン/インターフェイス（Zones/Interfaces）] リストで、デバイスが管理ステーションと通信するインターフェイスを含むゾーンまたはインターフェイス グループを追加します。1 つのインターフェイスを指定するには、インターフェイスにゾーンまたはインターフェイスのグループを作成する必要があります。セキュリティ ゾーンおよびインターフェイス グループ オブジェクトの作成（536 ページ）を参照してください。デバイスに選択したインターフェイスまたはゾーンが含まれている場合にのみ、デバイスでホストが設定されます。

ステップ 14 **[保存（Save）]** をクリックします。

プレフィックス リスト

ルート マップ、ポリシー マップ、OSPF フィルタリング、BGP ネイバー フィルタリングを設定する際に使用する、IPv4 および IPv6 用のプレフィックス リスト オブジェクトを作成できます。

IPv6 プレフィックス リストの設定

IPv6 プレフィックス リストの設定ページを使用して、プレフィックス リスト オブジェクトを作成、コピー、編集します。ルート マップ、ポリシー マップ、OSPF フィルタリングまたは BGP ネイバー フィルタリングを設定するときに使用する、プレフィックス リスト オブジェクトを作成できます。

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin Access Admin Network Admin

ステップ 1 **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** を選択し、目次で **[プレフィックス リスト（Prefix Lists）]** > **[IPv6 プレフィックス リスト（IPv6 Prefix List）]** を選択します。

ステップ 2 [プレフィックス リストの追加（Add Prefix List）] をクリックします。

ステップ 3 [新しいプレフィックス リスト オブジェクト（New Prefix List Object）] ウィンドウの [名前（Name）] フィールドで、プレフィックス リスト オブジェクトの名前を入力します。

ステップ 4 [新しいプレフィックス リスト オブジェクト（New Prefix List Object）] ウィンドウで、[追加（Add）] をクリックします。

ステップ 5 [アクション（Action）] ドロップダウンリストから適切なアクション、[許可（Allow）] または [ブロック（Block）] を選択して、再配布アクセスを指定します。

ステップ 6 このオブジェクトですでに設定されているプレフィックス リスト エントリのリストにおける、新しいプレフィックス リスト エントリの位置を示す固有の数字を、[シーケンス番号（Sequence No.）] フィールドに入力します。空白にしておくと、現在使用されている最大シーケンス番号より 5 大きいシーケンス番号がデフォルトになります。

ステップ 7 [IP アドレス（IP address）] フィールドの IP アドレス/マスク長形式で、IPv6 アドレスを指定します。マスク長は 1 ～ 128 の有効な値でなければなりません。

ステップ 8 [最小プレフィックス長（Minimum Prefix Length）] フィールドで最小プレフィックス長を入力します。値は、最大プレフィックス長の値が指定されている場合に、マスク長以上、最大プレフィックス長以下でなければなりません。

ステップ 9 [最大プレフィックス長（Maximum Prefix Length）] フィールドで最大プレフィックス長を入力します。値は、最小プレフィックス長の値が指定されている場合に、最小プレフィックス長以上、最小プレフィックス長の値が指定されていない場合に、マスク長以上でなければなりません。

ステップ 10 [Add] をクリックします。

ステップ 11 このオブジェクトのオーバーライドを許可する場合は、[Allow Overrides] チェックボックスをオンにします（オブジェクトのオーバーライドの許可 （524 ページ）を参照）。

ステップ 12 **[保存（Save）]** をクリックします。

IPv4 プレフィックス リストの設定

IPv4 プレフィックス リストの設定ページを使用して、プレフィックス リスト オブジェクトを作成、コピー、編集します。ルート マップ、ポリシー マップ、OSPF フィルタリングまたは BGP ネイバー フィルタリングを設定するときに使用する、プレフィックス リスト オブジェクトを作成できます。

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin Access Admin Network Admin

ステップ 1 [オブジェクト（Objects）] > [オブジェクト管理（Object Management）] を選択し、目次で [プレフィックス リスト（Prefix Lists）] > [IPv4 プレフィックス リスト（IPv4 Prefix List）] を選択します。 > >

ステップ 2 [プレフィックス リストの追加（Add Prefix List）] をクリックします。

ステップ 3 [新しいプレフィックス リスト オブジェクト（New Prefix List Object）] ウィンドウの [名前（Name）] フィールドで、プレフィックス リスト オブジェクトの名前を入力します。

ステップ 4 [追加（Add）] をクリックします。

ステップ 5 [アクション（Action）] ドロップダウンリストから適切なアクション、[許可（Allow）] または [ブロック（Block）] を選択して、再配布アクセスを指定します。

ステップ 6 このオブジェクトですでに設定されているプレフィックス リスト エントリのリストにおける、新しいプレフィックス リスト エントリの位置を示す固有の数字を、[シーケンス番号（Sequence No.）] フィールドに入力します。空白にしておくと、現在使用されている最大シーケンス番号より 5 大きいシーケンス番号がデフォルトになります。

ステップ 7 [IP アドレス（IP address）] フィールドの IP アドレス/マスク長形式で、IPv4 アドレスを指定します。マスク長は 1 ～ 32 の有効な値でなければなりません。

ステップ 8 [最小プレフィックス長（Minimum Prefix Length）] フィールドで最小プレフィックス長を入力します。値は、最大プレフィックス長の値が指定されている場合に、マスク長以上、最大プレフィックス長以下でなければなりません。

ステップ 9 [最大プレフィックス長（Maximum Prefix Length）] フィールドで最大プレフィックス長を入力します。値は、最小プレフィックス長の値が指定されている場合に、最小プレフィックス長以上、最小プレフィックス長の値が指定されていない場合に、マスク長以上でなければなりません。

ステップ 10 [Add] をクリックします。

ステップ 11 このオブジェクトのオーバーライドを許可する場合は、[Allow Overrides] チェックボックスをオンにします（オブジェクトのオーバーライドの許可 （524 ページ）を参照）。

ステップ 12 **[保存（Save）]** をクリックします。

ルート マップ

ルート マップは、ルートをルーティング プロセスに再配布するときに使用できます。また、デフォルト ルートをルーティング プロセスに生成するときにも使用します。ルート マップは、指定されたルーティング プロトコルのどのルートを対象ルーティング プロセスに再配布できるのかを定義します。ルート マップを設定して、ルート マップ オブジェクトの新しいルート マップ エントリを作成したり、既存のルート マップ エントリを編集したりします。

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin Access Admin Network Admin

始める前に

ルート マップは、これらのオブジェクトの 1 つまたは複数を使用することができます。これらのオブジェクトをすべて追加する必要はありません。これらのオブジェクトを必要に応じて作成および使用して、ルート マップを設定します。

- ACL の追加
- プレフィックス リストの追加
- AS パスの追加
- コミュニティ リストの追加
- ポリシー リストの追加

ステップ 1 **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** を選択し、コンテンツ テーブルから **[ルート マップ（Route Map）]** を選択します。

ステップ 2 [ルート マップの追加（Add Route Map）] をクリックします。

ステップ 3 [新しいルート マップ オブジェクト（New Route Map Object）] ウィンドウで [追加（Add）] をクリックします。

ステップ 4 [シーケンス番号（Sequence No.）] フィールドで、このルート マップ オブジェクトにすでに設定されているルート マップ エントリのリストでの新しいルート マップ エントリの位置を示す、0 ～ 65535 の番号を入力します。

（注） 将来的に句を挿入する必要性が生じたときの番号の間隔を確保するために、少なくとも 10 単位で句に番号を指定することをお勧めします。

ステップ 5 [再配布（Redistribution）] ドロップダウン リストから、再配布アクセスを示す適切なアクション（[許可（Allow）] または [ブロック（Block）]）を選択します。

ステップ 6 [句の照合（Match Clauses）] タブをクリックして、コンテンツ テーブルで選択する次の条件に基づいて照合します（ルート/トラフィック）。

- [セキュリティ ゾーン（Security Zones）]：（I/O）インターフェイスに基づいてトラフィックを照合します。ゾーンを選択して追加するか、インターフェイス名を入力して追加します。
- [IPv4]：次の条件に基づいて IPv4（ルート/トラフィック）を照合します。条件を定義するタブを選択します。
  1. ルート アドレスに基づいてルートを照合するには、[アドレス（Address）] タブをクリックします。IPv4 アドレスに対して、照合にアクセス リストまたはプレフィックス リストを使用するかどうかをドロップダウン リストから選択し、照合に使用する ACL オブジェクトまたはプレフィックス リストを入力または選択します。
  2. ルートのネクスト ホップ アドレスに基づいてルートを照合するには、[ネクスト ホップ（Next Hop）] タブをクリックします。IPv4 アドレスに対して、照合にアクセス リストまたはプレフィックス リストを使用するかどうかをドロップダウン リストから選択し、照合に使用する ACL オブジェクトまたはプレフィックス リストを入力または選択します。
  3. ルートのアドバタイズ送信元アドレスに基づいてルートを照合するには、[ルート送信元（Route Source）] タブをクリックします。IPv4 アドレスに対して、照合にアクセス リストまたはプレフィックス リストを使用するかどうかをドロップダウン リストから選択し、照合に使用する ACL オブジェクトまたはプレフィックス リストを入力または選択します。
- [IPv6]：ルート：ルートのルート アドレス、ネクストホップ アドレス、またはアドバタイズ送信元アドレスに基づいて IPv6（ルート/トラフィック）を照合します。
- [BGP]：次の条件に基づいて BGP（ルート/トラフィック）を照合します。条件を定義するタブを選択します。
  1. BGP 自律システム パス アクセス リストと指定されたパス アクセス リストの照合を有効にするには、[AS パス（AS Path）] タブをクリックします。複数のパス アクセス リストを指定した場合、ルートはいずれかのパス アクセス リストと一致します。
  2. BGP コミュニティと指定されたコミュニティの照合を有効にするには、[コミュニティ リスト（Community List）] タブをクリックします。複数のコミュニティを指定した場合、ルートはいずれかのコミュニティと一致します。少なくとも 1 つの Match コミュニティと一致しないルートは、アウトバウンド ルート マップにアドバタイズされません。

3. BGP ポリシーを評価および処理するためのルート マップを設定するには、[ポリシー リスト（Policy List）] タブをクリックします。1 つのルート マップ エントリ内で複数のポリシー リストが照合を行う場合、ポリシー リストすべては受信属性だけで照合を行います。

- [その他（Others）]：次の条件に基づいてルートまたはトラフィックを照合します。

1. ルートのメトリックの照合を有効にするには、[メトリック ルート値（Metric Route Value）] フィールドに、照合に使用するメトリック値を入力します。複数の値をカンマで区切って入力することもできます。設定したメトリックを持つ任意のルートを照合できます。メトリック値は、0 ～ 4294967295 の範囲で指定します。
2. [タグ値（Tag Values）] フィールドに、照合に使用するタグ値を入力します。複数の値をカンマで区切って入力することもできます。指定したセキュリティ グループ タグを持つ任意のルートを照合できます。タグ値は、0 ～ 4294967295 の範囲で指定します。
3. ルート タイプの照合を有効にするには、適切な**ルート タイプ**オプションをオンにします。有効なルート タイプは、External1、External2、Internal、Local、NSSA-External1、NSSA-External2 です。複数のルート タイプをリストから選択することができます。

ステップ 7 [句の設定（Set Clauses）] タブをクリックして、コンテンツ テーブルで選択する次の条件に基づいてルート/トラフィックを設定します。

- [メトリック値（Metric Values）]：[帯域幅（Bandwidth）]、すべての値、または値なしを設定します。

1. [帯域幅（Bandwidth）] フィールドに、メトリック値または帯域幅（キロビット/秒）を入力します。有効な値は、0 ～ 4294967295 の範囲の整数値です。
2. [メトリック タイプ（Metric Type）] ドロップダウン リストから、宛先ルーティング プロトコルのメトリックのタイプを選択して指定します。有効な値は、internal、type-1、または type-2 です。
3. [遅延（Delay）] フィールドに、EIGRP ルートの遅延を 10 マイクロ秒単位で入力します。有効な値の範囲は、1 ～ 4294967295 です。
4. [信頼性（Reliability）] フィールドに、EIGRP のパケット伝送の成功率を入力します。有効な値の範囲は 0 ～ 255 です。値 255 は 100 % の信頼性を意味し、0 は信頼性がないことを意味します。
5. [有効（Effective）] フィールドに、EIGRP の有効な帯域幅を入力します。有効な値の範囲は 1 ～ 255 です。値 255 は、100% のロードを意味します。
6. [MTU] フィールドに、EIGRP のルートの最小 MTU サイズをバイト単位で入力します。有効な値の範囲は 1 ～ 4294967295 です。

- [BGP 句（BGP Clauses）]：次の条件に基づいて BGP ルートを設定します。条件を定義するタブを選択します。

1. BGP ルートの自律システム パスを変更するには、[AS パス（AS Path）] タブをクリックします。

1. 任意の自律システム パス文字列を BGP ルートの前に付加するには、[AS パスを前に付加（Prepend AS Path）] タブをクリックします。通常、ローカルな AS 番号が複数回追加され、自律システム パス長が増します。複数の AS パス番号を指定した場合、ルートはいずれかの AS 番号を付加できます。
2. 最後の AS 番号を AS パスの前に付加するには、[最後の AS を AS パスの前に付加（Prepend Last AS to AS Path）] フィールドに AS パス番号を入力します。AS 番号の値を 1 ～ 10 の範囲で入力します。
3. ルートのタグを自律システム パスに変換するには、[ルート タグを AS パスに変換する（Convert route tag into AS path）] チェックボックスをオンにします。

2. コミュニティ属性を設定するには、[コミュニティ リスト（Community List）] タブをクリックします。
   1. ルート マップをパスするプレフィックスからコミュニティ属性を除去するには、[なし（None）] ラジオ ボタンをクリックします。
   2. コミュニティ番号を入力するには、[コミュニティの指定（Specify Community）] ラジオ ボタンをクリックします（必要な場合）。有効な値は 1 ～ 4294967295 です。
   3. 既存のコミュニティにコミュニティを追加するには、[既存のコミュニティに追加する（Add to existing communities）] チェックボックスをオンにします。
   4. 既知のコミュニティのいずれかを使用するには、[インターネット（Internet）]、[アドバタイズなし（No-Advertise）]、または [エクスポートなし（No-Export）] チェックボックスをオンにします。

3. 追加属性を設定するには、[その他（Others）] タブをクリックします。
   1. タグ値を自動的に計算するには、[自動タグを設定する（Set Automatic Tag）] チェックボックスをオンにします。
   2. [ローカル優先度の設定（Set Local Preference）] フィールドに自律システム パスの優先度値を入力します。0 から 4294967295 までの値を入力してください。
   3. [重み付けの設定（Set Weight）] フィールドにルーティング テーブルの BGP ウェイトを入力します。0 から 65535 までの値を入力してください。
   4. BGP の発信元コードを選択して指定します。有効な値は [ローカル IGP（Local IGP）] および [未完了（Incomplete）] です。
   5. [IPv4 設定（IPv4 Settings）] セクションで、パケットが出力されるネクスト ホップのネクスト ホップ IPv4 アドレスを指定します。隣接ルータである必要はありません。複数の IPv4 アドレスを指定した場合、いずれかの IP アドレスでパケットを出力できます。

      [プレフィックス リスト（Prefix List）] ドロップダウン リストから IPv4 プレフィックス リストを選択して指定します。

6. [IPv6 設定（IPv4 Settings）] セクションで、パケットが出力されるネクスト ホップのネクスト ホップ IPv6 アドレスを指定します。隣接ルータである必要はありません。複数の IPv6 アドレスを指定した場合、いずれかの IP アドレスでパケットを出力できます。

   [プレフィックス リスト（Prefix List）] ドロップダウン リストから IPv6 プレフィックスを選択して指定します。

ステップ 8 [Add] をクリックします。

ステップ 9 このオブジェクトのオーバーライドを許可する場合は、[Allow Overrides] チェックボックスをオンにします（オブジェクトのオーバーライドの許可 （524 ページ）を参照）。

ステップ 10 **[保存（Save）]** をクリックします。

アクセス リスト

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin Access Admin Network Admin

アクセス リスト オブジェクトは、アクセス コントロール リスト（ACL）とも呼ばれ、トラフィックに適用されるサービスを選択します。アクセス リスト オブジェクトを使って、ルート マップなどの機能を設定します。ACL で許可されたトラフィックはサービスを利用できますが、「ブロックされた」トラフィックはサービスから除外されます。サービスから除外されたトラフィックが必ずしも完全にドロップされるわけではありません。

次のタイプの ACL を設定できます。

- 拡張：送信元と宛先アドレスおよびポートに基づいてトラフィックを識別します。IPv4 および IPv6 アドレスをサポートしており、任意のルールで混在させることができます。
- 標準：宛先アドレスのみに基づいてトラフィックを識別します。IPv4 のみサポートしています。

ACL は 1 つまたは複数のアクセス コントロール エントリ（ACE）またはルールで構成されます。ACE の順番は重要です。パケットを「許可」 ACE と照合して ACL を評価する際、ACL に登録されている ACE の順番どおりに照合します。一致が見つかると、それ以降の ACE とは照合しません。たとえば、10.100.10.1 を「許可」して、10.100.10.0/24 の残りはすべて「ブロック」する場合、許可エントリがブロック エントリより前に登録されている必要があります。通常、具体性の高いルールを ACL の上部に置きます。

「許可」エントリに一致しないパケットはブロックされたと見なします。

次に、ACL オブジェクトの設定方法について説明します。

拡張 ACL オブジェクトの設定

送信元および宛先アドレス、プロトコル、およびポートに基づいて、あるいはトラフィックが IPv6 の場合にトラフィックを照合するには、拡張 ACL オブジェクトを使用します。

ステップ 1 **[オブジェクト（Objects）] > [オブジェクト管理（Object Management）]** を選択し、コンテンツ テーブルから **[アクセス コントロール リスト（Access Control Lists）] > [拡張（Extended）]** を選択します。

ステップ 2 次のいずれかを実行します。

- [拡張 ACL の追加（Add Extended ACL）] をクリックして、新しいオブジェクトを作成します。
- 編集アイコン（）をクリックして、既存のオブジェクトを編集します。

ステップ 3 [拡張 ACL オブジェクト（Extended ACL Object）] ダイアログボックスで、オブジェクトの名前を入力し（スペースは使用不可）、アクセス コントロール エントリを設定します。

a) 次のいずれかを実行します。

- 新しいエントリを作成するには、[Add] をクリックします。
- 編集アイコン（）をクリックして、既存のエントリを編集します。

右クリック メニューからも、エントリの切り取り、コピー、貼り付け、または削除を行うことができます。

b) トラフィック基準を許可（一致）するか、またはブロック（一致しない）するかの**アクション**を選択します。

（注） [ログ（Logging）]、[ログ レベル（Log Level）]、および [ログ インターバル（Log Interval）] オプションはアクセス ルールに対してのみ使用されます（インターフェイスに接続されているか、グローバルで適用される ACL）。ACL オブジェクトがアクセス ルールで使用されていないため、これらの値にはデフォルトを使用します。

c) 次のテクニックのいずれかを使用して、[ネットワーク（Network）] タブで送信元および宛先アドレスを設定します。

- [利用可能（Available）] リストから目的のネットワーク オブジェクトまたはグループを選択し、[送信元に追加（Add to Source）] または [宛先に追加（Add to Destination）] をクリックします。リストの上の [+] ボタンをクリックすると、新しいオブジェクトを作成できます。IPv4 アドレスと IPv6 アドレスを組み合わせることができます。
- 送信元または宛先リストの下の編集ボックスにアドレスを入力し、[追加（Add）] をクリックします。1 つのホスト アドレス（10.100.10.5、2001:DB8::0DB8:800:200C:417A など）またはサブネット（10.100.10.0/24 または 10.100.10.0 255.255.255.0 の形式。IPv6 の場合は 2001:DB8:0:CD30::/60）を指定できます。

d) [ポート（Port）] タブをクリックし、次のテクニックのいずれかを使用してサービスを設定します。

- [利用可能（Available）] リストから目的のポート オブジェクトまたはグループを選択し、[送信元に追加（Add to Source）] または [宛先に追加（Add to Destination）] をクリックします。リストの上の [+] ボタンをクリックすると、新しいオブジェクトを作成できます。オブジェクトによって TCP/UDP ポート、ICMP/ICMPv6 メッセージ タイプ、その他のプロトコルを指定できます（「任意」を含む）。ただし、通常は空にしておく送信元ポートは TCP/UDP のみを受け入れます。
- 送信元または宛先リストの下の編集ボックスでポートまたはプロトコルを入力または選択し、[追加（Add）] をクリックします。

（注） すべての IP トラフィックに適用するエントリを取得するには、「すべて」のプロトコルを指定する宛先ポート オブジェクトを選択します。

e) [追加（Add）] をクリックして、エントリをオブジェクトに追加します。

f) 必要に応じて、エントリをクリックおよびドラッグして、ルール順序で目的の場所まで上下に移動します。

このプロセスを繰り返して、オブジェクトに追加エントリを作成または編集します。

ステップ 4 このオブジェクトのオーバーライドを許可する場合は、[Allow Overrides] チェックボックスをオンにします（オブジェクトのオーバーライドの許可 （524 ページ）を参照）。

ステップ 5 **[保存（Save）]** をクリックします。

標準 ACL オブジェクトの設定

宛先 IPv4 アドレスのみに基づいてトラフィックを照合する場合は、標準 ACL オブジェクトを使用します。それ以外の場合は、拡張 ACL を使用します。

ステップ 1 **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** を選択し、コンテンツ テーブルから **[アクセス コントロール リスト（Access Control Lists）]** > **[標準（Standard）]** を選択します。

ステップ 2 次のいずれかを実行します。

- [標準 ACL の追加（Add Standard ACL）] をクリックして、新しいオブジェクトを作成します。
- 編集アイコン（）をクリックして、既存のオブジェクトを編集します。

ステップ 3 [標準 ACL オブジェクト（Standard ACL Object）] ダイアログボックスで、オブジェクトの名前を入力し（スペースは使用できません）、アクセス コントロール エントリを設定します。

a) 次のいずれかを実行します。

- 新しいエントリを作成するには、[Add] をクリックします。
- 編集アイコン（  ）をクリックして、既存のエントリを編集します。

右クリック メニューからも、エントリの切り取り、コピー、貼り付け、または削除を行うことができます。

b) アクセス コントロール エントリごとに、次のプロパティを設定します。

- [アクション（Action）]：トラフィック基準を許可（一致）またはブロック（不一致）するかどうか。
- [ネットワーク（Network）]：IPv4 ネットワーク オブジェクトまたはトラフィックの宛先を特定するグループを追加します。

c) [追加（Add）] をクリックして、エントリをオブジェクトに追加します。
d) 必要に応じて、エントリをクリックおよびドラッグして、ルール順序で目的の場所まで上下に移動します。

このプロセスを繰り返して、オブジェクトに追加エントリを作成または編集します。

ステップ 4 このオブジェクトのオーバーライドを許可する場合は、[Allow Overrides] チェックボックスをオンにします（オブジェクトのオーバーライドの許可 （524 ページ）を参照）。

ステップ 5 **[保存（Save）]** をクリックします。

AS パスのオブジェクト

AS パスは BGP のセットアップの必須属性です。これは、ネットワークのアクセスを可能にする AS 番号のシーケンスです。AS パスは、移動パケットの最短ルートになる送信元と宛先のルータ間の中間 AS 番号のシーケンスです。異なる AS プレフィックスにリーチする方法に関するメッセージを交換、更新するのに、ネイバー自律システム（ASes）で BGP が使用されます。各ルータで宛先までの最適ルートに関する新たなローカル判断が行われた後、用意されている距離メトリックおよびパス属性とともに、ルートまたはパスの情報がそれぞれのピアに送信されます。この情報がネットワークを移動すると、パスに沿った各ルータは、固有の AS 番号を BGP メッセージの ASes リストの前に付加します。このリストは、ルートの AS パスです。AS パスは AS プレフィックスとともに、ネットワークを介した一方向の中継ルートの特定のハンドルになります。AS パス ページの設定を使用して、自律システム（AS）のパスのポリシー オブジェクトを作成、コピー、編集します。ルート マップ、ポリシー マップ、または BGP ネイバー フィルタリングを設定するときに使用する、AS パス オブジェクトを作成できます。AS パスのフィルタにより、正規表現でルーティング アップデート メッセージをフィルタ処理できます。

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin Access Admin Network Admin

ステップ 1 [オブジェクト（Objects）] > [オブジェクト管理（Object Management）] を選択して、目次で [AS パス（AS Path）] を選択します。 >

ステップ 2 [AS パスの追加（Add AS Path）] をクリックします。

ステップ 3 [名前（Name）] フィールドに AS パス オブジェクトの名前を入力します。有効な値は、1 ～ 500 です。

ステップ 4 [新しい AS パス オブジェクト（New AS Path Object）] ウィンドウで、[追加（Add）] をクリックします。

a) [アクション（Action）] ドロップダウンリストから [許可（Allow）] または [ブロック（Block）] オプションを選択して、再配布アクセスを指定します。

b) [正規表現（Regular Expression）] フィールドで AS パスのフィルタ処理を定義する正規表現を指定します。

c) [Add] をクリックします。

ステップ 5 このオブジェクトのオーバーライドを許可する場合は、[Allow Overrides] チェックボックスをオンにします（オブジェクトのオーバーライドの許可 （524 ページ）を参照）。

ステップ 6 **[保存（Save）]** をクリックします。

コミュニティ リスト

コミュニティは、遷移的 BGP 属性のオプションです。コミュニティは、共通するいくつかの属性を共有する宛先のグループです。これはルート タギングに使用されます。BGP のコミュニティ属性は、特定のプレフィックスに割り当てられ、他のネイバーにアドバタイズされる数値です。コミュニティは、一般的な属性を共有する一連のプレフィックスのマーキングに使用できます。アップストリームプロバイダーは、これらのマーカーを使用して、特定のローカル設定のフィルタリングまたは割り当て、あるいは他の属性の変更などの一般的なルーティング ポリシーを適用します。コミュニティ リストの設定ページを使用して、コミュニティ リスト ポリシー オブジェクトを作成、コピー、編集します。ルート マップまたはポリシー マップを設定するときに使用する、コミュニティ リスト ポリシー オブジェクトを作成できます。コミュニティ リストを使用すると、ルート マップの match 句で使用されるコミュニティ グループを作成できます。コミュニティ リストは、一致ステートメントの番号付きリストです。接続先は、一致が見つかるまでルールと照合します。

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin Access Admin Network Admin

ステップ 1 [オブジェクト（Objects）] > [オブジェクト管理（Object Management）] を選択して、目次で [コミュニティ リスト（Community List）] を選択します。 >

ステップ 2 [コミュニティ リストの追加（Add Community List）] をクリックします。

ステップ 3 [名前（Name）] フィールドに、コミュニティ リスト オブジェクトの名前を指定します。

ステップ 4 [新しいコミュニティ リスト オブジェクト（New Community List Object）] ウィンドウで、[追加（Add）] をクリックします。

ステップ 5 [標準（Standard）] オプション ボタンを選択して、コミュニティ ルールの種類を表示します。

標準コミュニティ リストは、ウェルノウン コミュニティやコミュニティ番号の指定に使用されます。

（注） 標準を使用したエントリ、コミュニティ ルールの拡張種類を使用したエントリを、同じコミュニティ リスト オブジェクトに含めることはできません。

a) [アクション（Action）] ドロップダウンリストから [許可（Allow）] または [ブロック（Block）] オプションを選択して、再配布アクセスを指定します。

b) [コミュニティ（Communities）] フィールドで、コミュニティ番号を指定します。有効な値は 1 ～ 4294967295 または 0:1 ～ 65534:65535 です。

c) 適切な [ルート タイプ（Route Type）] を選択します。

- [インターネット（Internet）]：インターネットのウェルノウン コミュニティを指定するために選択します。このコミュニティのルートは、すべてのピア（内部および外部）にアドバタイズされます。
- [非アドバタイズ（No Advertise）]：非アドバタイズのウェルノウン コミュニティを指定するために選択します。このコミュニティのあるルートはピア（内部または外部）にはアドバタイズされません。
- [非エクスポート（No Export）]：非エクスポートのウェルノウン コミュニティを指定するために選択します。このコミュニティのあるルートは、同じ自律システム内のピアへのみ、または連合内の他のサブ自律システムへのみアドバタイズされます。これらのルートは外部ピアにはアドバタイズされません。

ステップ 6 [拡張（Expanded）] オプション ボタンを選択して、コミュニティ ルールの種類を表示します。

拡張コミュニティ リストは正規表現によるフィルタ コミュニティに使用されます。正規表現は、コミュニティ属性の照合パターンの指定に使用されます。

a) [アクション（Action）] ドロップダウンリストから [許可（Allow）] または [ブロック（Block）] オプションを選択して、再配布アクセスを指定します。

b) [表現（Expressions）] フィールドで、正規表現を指定します。

ステップ 7 [Add] をクリックします。

ステップ 8 このオブジェクトのオーバーライドを許可する場合は、[Allow Overrides] チェックボックスをオンにします（オブジェクトのオーバーライドの許可 （524 ページ）を参照）。

ステップ 9 **[保存（Save）]** をクリックします。

ポリシー リスト

ポリシー リストのポリシー オブジェクトを作成、コピー、編集するには、[ポリシー リストの設定（Configure Policy List）] ページを使用します。ルート マップを設定するときに使用するポリシー リスト オブジェクトを作成できます。ルート マップ内でポリシー リストが参照されると、ポリシー リスト内の match 文すべてが評価され、処理されます。1 つのルート マップに 2 つ以上のポリシー リストを設定できる。ポリシー リストは、同じルート マップ内にあるがポリシー リストの外で設定されている他の既存の match および set 文とも共存できます。1 つ

のルート マップ エントリ内で複数のポリシー リストがマッチングを行う場合、ポリシー リストすべては受信属性だけでマッチング。

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin Access Admin Network Admin

ステップ 1 **[オブジェクト（Objects）] > [オブジェクト管理（Object Management）]** を選択し、コンテンツ テーブルから [ポリシー リスト（Policy List）] を選択します。

ステップ 2 [ポリシー リストの追加（Add Policy List）] をクリックします。

ステップ 3 [名前（Name）] フィールドにポリシー リスト オブジェクトの名前を入力します。オブジェクト名では、大文字と小文字が区別されません。

ステップ 4 [アクション（Action）] ドロップダウン リストから、一致する条件へのアクセスを許可するかブロックするかを選択します。

ステップ 5 [インターフェイス（Interface）] タブをクリックして、指定したいずれかのインターフェイスの外部にネクスト ホップを持つルートを配布します。

[ゾーン/インターフェイス（Zones/Interfaces）] リストに、デバイスが管理ステーションとの通信を行うインターフェイスが含まれたゾーンを追加します。ゾーン内にないインターフェイスの場合は、[選択したゾーン/インターフェイス（Selected Zone/Interface）] リストの下のフィールドにインターフェイス名を入力し、[追加（Add）] をクリックします。デバイスに選択したインターフェイスまたはゾーンが含まれている場合にのみ、デバイスでホストが設定されます。

ステップ 6 [アドレス（Address）] タブをクリックして、標準アクセス リストまたはプレフィックス リストで許可された宛先アドレスを持つルートを再配布します。

照合に [アクセス リスト（Access List）] または [プレフィックス リスト（Prefix List）] のどちらを使用するかを選択し、照合に使用する標準アクセス リスト オブジェクトまたはプレフィックス リスト オブジェクトを入力するか選択します。

ステップ 7 [ネクスト ホップ（Next Hop）] タブをクリックして、指定したアクセス リストまたはプレフィックス リストの 1 つから渡されたネクスト ホップ ルータ アドレスを持つルートを再配布します。

照合に [アクセス リスト（Access List）] または [プレフィックス リスト（Prefix List）] のどちらを使用するかを選択し、照合に使用する標準アクセス リスト オブジェクトまたはプレフィックス リスト オブジェクトを入力するか選択します。

ステップ 8 [ルート送信元（Route Source）] タブをクリックして、アクセス リストまたはプレフィックス リストで指定されたアドレスのルータおよびアクセス サーバによってアドバタイズされたルートを再配布します。

照合に [アクセス リスト（Access List）] または [プレフィックス リスト（Prefix List）] のどちらを使用するかを選択し、照合に使用する標準アクセス リスト オブジェクトまたはプレフィックス リスト オブジェクトを入力するか選択します。

ステップ 9 [AS パス（AS Path）] タブをクリックして、BGP 自律システム パスを一致させます。複数の AS パスを指定した場合、ルートはいずれかの AS パスと一致します。

ステップ 10 [コミュニティ ルール（Community Rule）] タブをクリックすると、BGP コミュニティと指定されたコミュニティの照合が有効になります。複数のコミュニティを指定した場合、ルートはいずれかのコミュニティと一致します。BGP コミュニティと指定したコミュニティの完全一致を有効にするには、[指定したコミュニティと完全に一致（Match the specified community exactly）] チェックボックスをオンにします。

ステップ 11 [メトリックとタグ（Metric & tag）] タブをクリックして、メトリックとルートのセキュリティ グループ タグを照合します。

a) [Metric（メトリック）]フィールドに、照合に使用するメトリック値を入力します。複数の値をカンマで区切って入力することもできます。設定したメトリックを持つ任意のルートを照合できます。メトリック値は、0 ～ 4294967295 の範囲で指定します。

b) [タグ（Tag）] フィールドに照合に使用するタグ値を入力します。複数の値をカンマで区切って入力することもできます。指定したセキュリティ グループ タグを持つ任意のルートを照合できます。タグ値は、0 ～ 4294967295 の範囲で指定します。

ステップ 12 このオブジェクトのオーバーライドを許可する場合は、[Allow Overrides] チェックボックスをオンにします（オブジェクトのオーバーライドの許可 （524 ページ）を参照）。

ステップ 13 **[保存（Save）]** をクリックします。

VPN オブジェクト

FTD IKE ポリシー

Internet Key Exchange（IKE、インターネット キー エクスチェンジ）は、IPsec ピアの認証、IPsec 暗号キーのネゴシエーションと配布、および IPsec Security Association（SA、セキュリティ アソシエーション）の自動的な確立に使用されるキー管理プロトコルです。IKE ネゴシエーションは 2 つのフェーズで構成されています。フェーズ 1 では、2 つの IKE ピア間のセキュリティ アソシエーションをネゴシエートします。これにより、ピアはフェーズ 2 で安全に通信できるようになります。フェーズ 2 のネゴシエーションでは、IKE によって IPsec などの他のアプリケーション用の SA が確立されます。両方のフェーズで接続のネゴシエーション時にプロポーザルが使用されます。IKE プロポーザルは、2 つのピア間のネゴシエーションを保護するためにこれらのピアで使用されるアルゴリズムのセットです。IKE ネゴシエーションは、共通（共有）IKE ポリシーに合意している各ピアによって開始されます。このポリシーは、後続の IKE ネゴシエーションを保護するために使用されるセキュリティ パラメータを示します。

IKEv1 では、IKE プロポーザルには、単一のアルゴリズム セットと係数グループが含まれています。複数のポリシーをプライオリティ付きで作成して、少なくとも 1 つのポリシーがリモート ピアのポリシーに一致するようにできます。IKEv1 とは異なり、IKEv2 プロポーザルでは、1 つのポリシーで複数のアルゴリズムおよびモジュラス グループを選択できます。フェーズ 1 のネゴシエーションでピアを選択するため、作成する IKE プロポーザルの数を 1 つにすることは可能ですが、複数の異なる IKE プロポーザルを作成して、最も望ましいオプションを高い優

先順位に設定することも検討してください。IKEv2 では、ポリシー オブジェクトが認証方式を指定しないため、その他のポリシーで認証要件を定義する必要があります。

サイト間 IPsec VPN を設定する際は、IKE ポリシーが必要です。詳細については、「Firepower Threat Defense の VPN （1051 ページ）」を参照してください。

IKEv1 ポリシー オブジェクトの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス（Access）
エクスポート コンプライアンス	該当なし	FTD	リーフのみ	Admin

IKEv1 ポリシー ページを使用して、IKEv1 ポリシー オブジェクトを作成、削除、または編集します。これらのポリシー オブジェクトには、IKEv1 ポリシーに必要なパラメータが含まれています。

ステップ 1 **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** を選択し、目次で **[VPN]** > **[IKEv1 ポリシー（IKEv1 Policy）]** を選択します。

前に設定したポリシーは、システムによって定義されるデフォルトにリストされています。アクセス レベルによっては、プロポーザルを編集（）、表示（）、または削除（）することもできます。

ステップ 2 （任意） [IKEv1 ポリシーの追加（Add IKEv1 Policy）] を選択して、新しいポリシー オブジェクトを作成します。

ステップ 3 このポリシーの [名前（Name）] を入力します。最大 128 文字を使用できます。

ステップ 4 （任意） このプロポーザルの [説明（Description）] を入力します。最大 1,024 文字を使用できます。

ステップ 5 IKE ポリシーの [プライオリティ（Priority）] 値を入力します。

このプライオリティ値によって、共通のセキュリティ アソシエーション（SA）の検出試行時に、ネゴシエーションする 2 つのピアを比較することで、IKE ポリシーの順序が決定します。リモート IPsec ピアが、最初のプライオリティ ポリシーで選択されているパラメータをサポートしていない場合、次に低いプライオリティで定義されているパラメータの使用を試行します。有効な値の範囲は 1 ～ 65,535 です。値が小さいほど、プライオリティが高くなります。このフィールドをブランクのままにすると、管理センターによって、まだ割り当てられていない最も小さい値が割り当てられます。値は 1 から始まり、次は 5 となり、その後は 5 ずつ増加します。

ステップ 6 [暗号化（Encryption）] 方法を選択します。

IKEv1 ポリシーで使用する暗号化およびハッシュ アルゴリズムを決定する場合、ピア デバイスによってサポートされているアルゴリズムだけを選択できます。VPN トポロジのエクストラネットのデバイスでは、両方のピアに一致するアルゴリズムを選択する必要があります。IKEv1 では、いずれかのオプションを選択します。オプションの詳しい説明については、使用する暗号化アルゴリズムの決定 （1058 ページ）を参照してください。

ステップ 7 [ハッシュ（Hash）] アルゴリズムを選択して、メッセージの整合性の確保に使用されるメッセージ ダイジェストを作成します。

IKEv1 プロポーザルで使用する暗号化およびハッシュ アルゴリズムを決定する場合、管理対象デバイスによってサポートされているアルゴリズムだけを選択できます。VPN トポロジのエクストラネットのデバイスでは、両方のピアに一致するアルゴリズムを選択する必要があります。 オプションの詳しい説明については、使用するハッシュ アルゴリズムの決定 （1059 ページ）を参照してください。

ステップ 8 **[Diffie-hellman グループ（Diffie-Hellman Group）]** を設定します。

暗号化に使用する Diffie-Hellman グループ。係数が大きいほどセキュリティが強化されますが、処理時間が長くなります。2 つのピアに、一致する係数グループが設定されている必要があります。VPN で許可するグループを選択します。オプションの詳しい説明については、使用する Diffie-Hellman 係数グループの決定 （1060 ページ）を参照してください。

ステップ 9 セキュリティ アソシエーション（SA）の [ライフタイム（Lifetime）]（秒数）を設定します。120 ～ 2,147,483,647 秒の値を指定できます。デフォルトは 86400 です。

このライフタイムを超えると、SA の期限が切れ、2 つのピア間で再ネゴシエーションを行う必要があります。一般的に、一定の限度に達するまで、ライフタイムが短いほど、IKE ネゴシエーションがセキュアになります。ただし、ライフタイムが長いと、今後の IPsec セキュリティ アソシエーションのセットアップが、短いライフタイムの場合よりも迅速に行われます。

ステップ 10 2 つのピア間で使用する [認証方法（Authentication Method）] を設定します。

- [事前共有キー（Preshared Key）]：事前共有キーを使用すると、秘密キーを 2 つのピア間で共有したり、認証フェーズ中に IKE で使用したりできます。参加ピアの 1 つに同じ事前共有キーが設定されていない場合は、IKE SA を確立できません。
- [証明書（Certificate）]：VPN 接続に認証方式として証明書を使用すると、ピアは PKI インフラストラクチャの CA サーバからデジタル証明書を取得して、互いの認証で交換します。

（注） IKEv1 をサポートする VPN トポロジでは、選択した IKEv1 ポリシー オブジェクトで指定した [認証方式（Authentication Method）] が、IKEv1 の [認証タイプ（Authentication Type）] 設定のデフォルトになります。これらの値は一致する必要があります。一致しないと設定がエラーになります。

ステップ 11 [Save] をクリックします。
新しい IKEv1 ポリシーがリストに追加されます。

IKEv2 ポリシー オブジェクトの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス（Access）
エクスポート コンプライアンス	該当なし	FTD	リーフのみ	Admin

IKEv2 ポリシー ダイアログボックスを使用して、IKEv2 ポリシーオブジェクトを作成、削除、編集します。これらのポリシーオブジェクトには、IKEv2 ポリシーに必要なパラメータが含まれています。

ステップ 1 **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** を選択し、目次で **[VPN]** > **[IKEv2 ポリシー（IKEv2 Policy）]** を選択します。

前に設定したポリシーは、システムによって定義されるデフォルトにリストされています。アクセス レベルによっては、ポリシーを編集（）、表示（）、または削除（）することもできます。

ステップ 2 [IKEv2 ポリシーの追加（Add IKEv2 Policy）] を選択して、新しいポリシーを作成します。

ステップ 3 このポリシーの [名前（Name）] を入力します。

ポリシー オブジェクトの名前。最大 128 文字を使用できます。

ステップ 4 このポリシーの [説明（Description）] を入力します。

ポリシー オブジェクトの説明。最大 1024 文字を使用できます。

ステップ 5 [プライオリティ（Priority）] を入力します。

IKE プロポーザルのプライオリティ値。このプライオリティ値によって、共通のセキュリティ アソシエーション（SA）の検出試行時に、ネゴシエーションする 2 つのピアを比較することで、IKE プロポーザルの順序が決定します。リモート IPsec ピアが、最初のプライオリティ ポリシーで選択されているパラメータをサポートしていない場合、次に低いプライオリティ ポリシーで定義されているパラメータの使用を試行します。有効な値の範囲は 1 ～ 65535 です。値が小さいほど、プライオリティが高くなります。このフィールドをブランクのままにすると、管理センターによって、まだ割り当てられていない最も小さい値が割り当てられます。値は 1 から始まり、次は 5 となり、その後は 5 ずつ増加します。

ステップ 6 セキュリティ アソシエーション（SA）の [ライフタイム（Lifetime）]（秒数）を設定します。120 ～ 2,147,483,647 秒の値を指定できます。デフォルトは 86400 です。

このライフタイムを超えると、SA の期限が切れ、2 つのピア間で再ネゴシエーションを行う必要があります。一般的に、一定の限度に達するまで、ライフタイムが短いほど、IKE ネゴシエーションがセキュアになります。ただし、ライフタイムが長いと、今後の IPsec セキュリティ アソシエーションのセットアップが、短いライフタイムの場合よりも迅速に行われます。

ステップ 7 IKE ポリシーで使用するハッシュ アルゴリズムの [整合性アルゴリズム（Integrity Algorithms）] 部分を選択します。このハッシュ アルゴリズムによって、メッセージの整合性の確保に使用されるメッセージ ダイジェストが作成されます。

IKEv2 プロポーザルで使用する暗号化およびハッシュ アルゴリズムを決定する場合、管理対象デバイスによってサポートされているアルゴリズムだけを選択できます。VPN トポロジのエクストラネットのデバイスでは、両方のピアに一致するアルゴリズムを選択する必要があります。VPN で許可するアルゴリズムすべてを選択します。オプションの詳しい説明については、使用するハッシュ アルゴリズムの決定（1059 ページ）を参照してください。

ステップ 8 フェーズ 2 ネゴシエーションを保護するためのフェーズ 1 SA の確立に使用される [暗号化アルゴリズム（Encryption Algorithm）] を選択します。

IKEv2 プロポーザルで使用する暗号化およびハッシュ アルゴリズムを決定する場合、管理対象デバイスによってサポートされているアルゴリズムだけを選択できます。VPN トポロジのエクストラネットのデバイスでは、両方のピアに一致するアルゴリズムを選択する必要があります。VPN で許可するアルゴリズムすべてを選択します。 オプションの詳しい説明については、使用する暗号化アルゴリズムの決定 （1058 ページ）を参照してください。

ステップ 9 [PRF アルゴリズム（PRF Algorithm）] を選択します。

IKE ポリシーに使用されるハッシュ アルゴリズムの疑似乱数関数（PRF）部分です。IKEv1 では、整合性アルゴリズムと PRF アルゴリズムを分けることができません。ただし、IKEv2 では、これらのエレメントに対して異なるアルゴリズムを指定できます。VPN で許可するアルゴリズムすべてを選択します。オプションの詳しい説明については、使用するハッシュ アルゴリズムの決定 （1059ページ）を参照してください。

ステップ 10 [DH グループ（DH Group）] を選択し、[追加（Add）] します。

暗号化に使用される Diffie-Hellman グループ。係数が大きいほどセキュリティが強化されますが、処理時間が長くなります。2 つのピアに、一致する係数グループが設定されている必要があります。VPN で許可するグループを選択します。 オプションの詳しい説明については、使用する Diffie-Hellman 係数グループの決定 （1060 ページ）を参照してください。

ステップ 11 [Save] をクリックします。
任意の有効な組み合わせが選択された場合、新しい IKEv2 ポリシーがリストに追加されます。選択されなかった場合、エラーが表示され、このポリシーを正常に保存するために、変更する必要があります。

FTD IPsec プロポーザル

IPsec プロポーザル（またはトランスフォーム セット）は VPN トポロジを設定するときに使用されます。ピアは、ISAKMP との IPsec セキュリティ アソシエーションのネゴシエート中に、特定のデータ フローを保護する特定のプロポーザルの使用に同意します。プロポーザルは、両方のピアで同じである必要があります。

IKE バージョン（IKEv1 または IKEv2）に基づいて、別個の IPsec プロポーザル オブジェクトがあります。

- IKEv1 IPsec プロポーザル（またはトランスフォーム セット）オブジェクトを作成する場合、IPsec が動作するモードを選択し、必要な暗号化タイプおよび認証タイプを定義します。アルゴリズムには単一のオプションを選択できます。VPN で複数の組み合わせをサポートするには、複数の IKEv1 IPsec プロポーザル オブジェクトを作成します。
- IKEv2 IPsec プロポーザル オブジェクトを作成する際に、VPN で許可するすべての暗号化アルゴリズムとハッシュ アルゴリズムを選択できます。IKEv2 ネゴシエーション中に、ピアは、それぞれでサポートされる最適なオプションを選択します。

カプセル化セキュリティ プロトコル（ESP）は、IKEv1 と IKEv2 の両方の IPsec プロポーザルに使用されます。これは認証、暗号化、およびアンチリプレイ サービスを提供します。ESP は、IP プロトコル タイプ 50 です。

（注） IPsec トンネルで暗号化と認証の両方を使用することを推奨します。

IKEv1 IPsec プロポーザル オブジェクトの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス（Access）
エクスポート コンプライアンス	該当なし	FTD	リーフのみ	Admin

ステップ 1 **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** を選択し、目次で **[VPN]** > **[IPsec IKev1 プロポーザル（IPsec IKev1 Proposal）]** を選択します。

前に設定したプロポーザルは、システムによって定義されるデフォルトにリストされています。アクセスレベルによっては、プロポーザルを編集（）、表示（）、または削除（）することもできます。

ステップ 2 [IPsec IKEv1 プロポーザルの追加（Add IPsec IKEv1 Proposal）] を選択して、新しいプロポーザルを作成します。

ステップ 3 このプロポーザルの [名前（Name）] を入力します。

ポリシー オブジェクトの名前。最大 128 文字を使用できます。

ステップ 4 このプロポーザルの [説明（Description）] を入力します。

ポリシー オブジェクトの説明。最大 1024 文字を使用できます。

ステップ 5 [ESP 暗号化（ESP Encryption）] 方法を選択します。このプロポーザルのカプセル化セキュリティ プロトコル（ESP）暗号化アルゴリズム。

IKEv1 では、いずれかのオプションを選択します。IPsec プロポーザルで使用する暗号化およびハッシュ アルゴリズムを決定する場合、VPN 内のデバイスによってサポートされているアルゴリズムだけを選択できます。 オプションの詳しい説明については、使用する暗号化アルゴリズムの決定（1058 ページ）を参照してください。

ステップ 6 [ESP ハッシュ（ESP Hash）] のオプションを選択します。

オプションの詳しい説明については、使用するハッシュ アルゴリズムの決定（1059 ページ）を参照してください。

ステップ 7 [Save] をクリックします。
新しいプロポーザルがリストに追加されます。

IKEv2 IPsec プロポーザル オブジェクトの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス（Access）
エクスポート コンプライアンス	該当なし	FTD	リーフのみ	Admin

ステップ 1 **[オブジェクト（Objects）] > [オブジェクト管理（Object Management）]** を選択し、目次で **[VPN] > [IKEv2 IPsec プロポーザル（IKEv2 IPsec Proposal）]** を選択します。

前に設定したプロポーザルは、システムによって定義されるデフォルトにリストされています。アクセスレベルによっては、プロポーザルを編集（）、表示（）、または削除（）することもできます。

ステップ 2 [IKEv2 IPsec プロポーザルの追加（Add IKEv2 IPsec Proposal）] を選択して、新しいプロポーザルを作成します。

ステップ 3 このプロポーザルの [名前（Name）] を入力します。

ポリシー オブジェクトの名前。最大 128 文字を使用できます。

ステップ 4 このプロポーザルの [説明（Description）] を入力します。

ポリシー オブジェクトの説明。最大 1024 文字を使用できます。

ステップ 5 [ESP ハッシュ（ESP Hash）] 方法を選択して、ハッシュまたは整合性アルゴリズムを認証用プロポーザルに使用します。

IKEv2 では、[ESP ハッシュ（ESP Hash）] をサポートするオプションすべてを選択します。 オプションの詳しい説明については、使用するハッシュ アルゴリズムの決定 （1059 ページ）を参照してください。

ステップ 6 [ESP 暗号化（ESP Encryption）] 方法を選択します。このプロポーザルのカプセル化セキュリティ プロトコル（ESP）暗号化アルゴリズム。

IKEv2 では、[選択（Select）] をクリックして、サポートするすべてのオプションを選択できるダイアログボックスを開きます。IPsec プロポーザルで使用する暗号化およびハッシュ アルゴリズムを決定する場合、VPN 内のデバイスによってサポートされているアルゴリズムだけを選択できます。 オプションの詳しい説明については、使用する暗号化アルゴリズムの決定 （1058 ページ）を参照してください。

ステップ 7 [Save] をクリックします。
新しいプロポーザルがリストに追加されます。

FTD グループ ポリシー オブジェクト

グループ ポリシーはグループ ポリシー オブジェクト内に保存される属性と値の一連のペアで、リモート アクセス VPN のエクスペリエンスを定義します。たとえば、グループ ポリシー オブジェクトで、アドレス、プロトコル、接続設定などの一般的な属性を設定します。

ユーザに適用されるグループポリシーはVPNトンネルが確立される際に決定されます。RADIUS承認サーバがグループポリシーを割り当てるか、または現在の接続プロファイルから取得されます。

（注） FTD ではグループ ポリシー属性の継承はありません。ユーザについては、グループ ポリシー オブジェクトが全体として使用されます。ログイン時に AAA サーバで特定されたグループ ポリシー オブジェクトが使用されるか、またはこれが指定されていない場合は、VPN 接続に対して設定されたデフォルトのグループ ポリシーが使用されます。指定されたデフォルトのグループ ポリシーはデフォルト値に設定できますが、これは、接続プロファイルに割り当てられ、他のグループ ポリシーがユーザに対して特定されていない場合にのみ使用されます。

関連トピック

グループ ポリシー オブジェクトの設定 （624 ページ）

グループ ポリシー オブジェクトの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス（Access）
エクスポート制御機能が有効なスマート ライセンス アカウントに関連付けられている次の AnyConnect ライセンスのいずれか。 • AnyConnect VPN Only • AnyConnect Plus • AnyConnect Apex	該当なし	FTD	いずれか（Any）	Admin

FTD グループ ポリシー オブジェクト （623 ページ）を参照してください。

ステップ 1 **[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [VPN] > [グループ ポリシー（Group Policy）]** を選択します。

以前に設定したポリシーがシステム デフォルトと共にリストされます。ユーザのアクセス レベルに応じて、グループ ポリシーの編集、表示、または削除ができます。

ステップ 2 [グループ ポリシーの追加（Add Group Policy）] をクリックするか、現在のポリシーを選択して編集します。

ステップ 3 このポリシーの [名前（Name）] とオプションで [説明（Description）] を入力します。

名前には最大 64 文字の長さを使用でき、スペースも使用できます。説明には、最大 1,024 文字を使用できます。

ステップ 4 グループ ポリシー一般オプション （625 ページ）の説明に従って、このグループ ポリシーの [General] パラメータを指定します。

ステップ 5 グループ ポリシー AnyConnect オプション （628 ページ）の説明に従って、このグループ ポリシーの [AnyConnect] パラメータを指定します。

ステップ 6 グループ ポリシーの詳細オプション （630 ページ）の説明に従って、このグループ ポリシーの [詳細（Advanced）] パラメータを指定します。

ステップ 7 [保存（Save）] をクリックします。
新しいグループ ポリシーがリストに追加されます。

次のタスク

グループ ポリシー オブジェクトをリモート アクセス VPN 接続プロファイルに追加します。

グループ ポリシー一般オプション

ナビゲーション パス

[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [VPN] > [グループ ポリシー（Group Policy）]、[グループ ポリシーの追加（Add Group Policy）] をクリックするか、現在のポリシーを選択して編集します。 をクリックして、[一般（General）] タブを選択します。

VPN プロトコル フィールド

このグループ ポリシーを適用するときに使用できるリモート アクセス VPN トンネルのタイプを指定します。[SSL] または [IPsec IKEv2]

IP アドレス プール

リモート アクセス VPN のユーザ グループに固有のアドレス プールに基づいて適用される IPv4 アドレス割り当てを指定します。リモート アクセス VPN では、認証に RADIUS/ISE を使用して、識別されたユーザ グループの特定のアドレス プールから IP アドレスを割り当てることができます。特定のユーザ グループに対して、特定のグループ ポリシーを RADIUS 認証属性（GroupPolicy/Class）として設定することにより、非アイデンティティ ウェア システム内のユーザまたはユーザ グループにポリシーの適用をシームレスに実行できます。たとえば、請負業者用に特定のアドレス プールを選択して、これらのアドレスを使用してポリシーの適用を行い、内部ネットワークへの制限付きのアクセスを許可する必要があります。

Firepower Threat Defense デバイスがクライアントに IPv4 アドレス プールを割り当てる優先順位：

1. IPv4 アドレス プールの RADIUS 属性
2. グループ ポリシーの RADIUS 属性
3. 接続プロファイルにマップされたグループ ポリシー内のアドレス プール
4. 接続プロファイル内の IPv4 アドレス プール

グループ ポリシーで IP アドレス プールを使用する際の制限事項の一部を以下に示します。

- IPv6 アドレス プールはサポートされていません。
- グループ ポリシーでは、最大で 6 つの IPv4 アドレス プールを設定できます。
- 使用中のアドレス プールが変更されると、展開が失敗します。アドレス プールを変更する前に、すべてのユーザをログオフする必要があります。
- アドレス プールの名前が変更されたり、重複するアドレス プールが設定されると、展開が失敗する可能性があります。変更を展開するには、古いアドレス プールを削除してから、変更されたアドレス プールを展開する必要があります。

  トラブルシューティング コマンドの一部を以下に示します。

  - `show ip local pool <address-pool-name>`
  - `show vpn-sessiondb detail anyconnect`
  - `vpn-sessiondb loggoff all noconfirm`

バナー フィールド

ログイン時にユーザに対して表示するバナー テキストを指定します。長さは最大 491 文字です。デフォルト値はありません。IPsec VPN クライアントではバナーに対してすべての HTML がサポートされますが、AnyConnect クライアントでは一部の HTML のみがサポートされます。バナーがリモート ユーザに正しく表示されるようにするには、IPsec クライアントに /n タグ、SSL クライアントに
 タグを使用します。

DNS/WINS フィールド

Domain Naming System（DNS）サーバおよび Windows Internet Naming System（WINS）サーバ。AnyConnect クライアントの名前解決に使用されます。

- [プライマリ DNS サーバ（Primary DNS Server）] および [セカンダリ DNS サーバ（Secondary DNS Server）]：このグループで使用する DNS サーバの IPv4 または IPv6 アドレスを定義するネットワーク オブジェクトを選択または作成します。
- [プライマリ WINS サーバ（Primary WINS Server）] および [セカンダリ WINS サーバ（Secondary WINS Server）]：このグループで使用する WINS サーバの IP アドレスを含むネットワーク オブジェクトを選択または作成します。

- [DHCP ネットワーク範囲（DHCP Network Scope）]：このグループの DHCP ネットワークの IPv4 アドレスを含むネットワーク オブジェクトを選択または作成します。この設定では、IPv6、アドレス範囲、またはサブネット仕様はサポートされていません。適切に設定されていない場合、VPN ポリシーの展開は失敗します。
- [デフォルト ドメイン（Default Domain）]：デフォルト ドメインの名前。最上位ドメイン（たとえば、**example.com**）を指定します。

スプリット トンネリング フィールド

スプリット トンネリングは、一部のネットワーク トラフィックを VPN トンネルに誘導して通過させ（暗号化）、残りのネットワーク トラフィックを VPN トンネルの外に誘導します（非暗号化、つまり「クリア テキストの状態」）。

- [IPv4 スプリット トンネリング/IPv6 スプリット トンネリング（IPv4 Split Tunneling/IPv6 Split Tunneling）]：デフォルトでは、スプリット トンネリングは無効です。IPv4 と IPv6 両方とも、[トンネル上ですべてのトラフィックを許可する（Allow all traffic over tunnel）] に設定されています。このままにした場合、エンドポイントからのすべてのトラフィックは VPN 接続経由で送信されます。

  スプリット トンネリングを設定するには、[次に指定されたトンネル ネットワーク（Tunnel networks specified below）] または [次に指定されたネットワークを除外（Exclude networks specified below）] を選択します。その後、そのポリシーのアクセス コントロール リストを設定します。

- [スプリット トンネル ネットワーク リスト タイプ（Split Tunnel Network List Type）]：使用するアクセス リストのタイプを選択します。[標準アクセス リスト（Standard Access List）] または [拡張アクセス リスト（Extended Access List）] を選択するか、作成します。詳細については、アクセス リスト （610 ページ）を参照してください。

- [DNS 要求スプリット トンネリング（DNS Request Split Tunneling）]：スプリット DNS とも呼ばれます。ご使用の環境で期待される DNS 動作を設定します。

  デフォルトでは、スプリット DNS は無効で、[スプリット トンネル ポリシーに従って DNS 要求を送信する（Send DNS request as per split tunnel policy）] に設定されています。[DNS 要求を常にトンネル経由で送信する（Always send DNS request over tunnel）] を選択すると、すべての DNS 要求は強制的にトンネル経由でプライベート ネットワークに送信されます。

  スプリット DNS を設定するには、[指定したドメインのみをトンネル経由で送信（Send only specified domains over tunnel）] を選択し、ドメイン名のリストを [ドメイン リスト（Domain List）] フィールドに入力します。これらの要求が、プライベート ネットワークにスプリット トンネルを介して解決されます。他のすべての名前は、パブリック DNS サーバを使用して解決されます。ドメインのリストに最大 10 のエントリをカンマで区切って入力します。文字列全体は、255 文字以下である必要があります。

関連トピック

グループ ポリシー オブジェクトの設定 （624 ページ）

グループ ポリシー AnyConnect オプション

これらの仕様は、AnyConnect VPN クライアントの動作に適用されます。

ナビゲーション

[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [VPN] > [グループ ポリシー（Group Policy）]。[グループ ポリシーの追加（Add Group Policy）] をクリックするか、現在のポリシーを選択して編集します。次に、[AnyConnect（AnyConnect）] タブを選択します。

プロファイル フィールド

[プロファイル（Profile）]：AnyConnect クライアント プロファイル を含むファイル オブジェクトを選択または作成します。オブジェクト作成の詳細については、FTD ファイル オブジェクト （631 ページ）を参照してください。

AnyConnect クライアント プロファイルは XML ファイルに格納された設定パラメータのグループです。AnyConnect ソフトウェア クライアントは、クライアントのユーザ インターフェイスに表示される接続エントリを設定するためにこれを使用します。これらのパラメータ（XML タグ）では、追加の AnyConnect 機能を有効にする設定も行われます。

AnyConnect クライアント プロファイル を作成するには、独立した構成ツールである GUI ベースの AnyConnect プロファイル エディタ を使用します。詳細については、『Cisco AnyConnect Secure Mobility Client Administrator Guide』の該当するリリースの *AnyConnect* プロファイル エディタ の章を参照してください。

SSL 設定フィールド

- [SSL 圧縮（SSL Compression）]：データ圧縮を有効にするかどうか。有効にする場合は、使用するデータ圧縮の方法（[圧縮（Deflate）] または [LZS（LZS）]）。[SSL 圧縮（SSL Compression）] はデフォルトで無効になっています。

  データ圧縮は、伝送速度を上げますが、各ユーザ セッションのメモリ要件と CPU 使用率も高めます。そのため、セキュリティ アプライアンスの全体的なスループットが低下します。

- [DTLS 圧縮（DTLS Compression）]：LZS を使用してこのグループの Datagram Transport Layer Security（DTLS）の接続を圧縮するかどうか。[DTLS 圧縮（DTLS Compression）] はデフォルトで無効になっています。

- [MTU サイズ（MTU Size）]：Cisco AnyConnect VPN クライアントによって確立された SSL VPN 接続の最大伝送単位（MTU）サイズ。デフォルトは 1406 バイト、有効な範囲は 576 ～ 1462 バイトです。

  - [DF ビットを無視（Ignore DF Bit）]：フラグメント化が必要なパケットの Don't Fragment（DF）ビットを無視するかどうか。DF ビットが設定されているパケットを強制的にフラグメント化して、トンネルを通過させることができます。

接続設定フィールド

- [AnyConnect クライアントと VPN ゲートウェイ間のキープアライブ メッセージの有効化（Enable Keepalive Messages between AnyConnect Client and VPN gateway）] およびその [間隔（Interval）] 設定：トンネルでのデータ送受信にピアを使用できることを示すために、ピア間でキープアライブ メッセージを交換するかどうかを指定します。デフォルトでは有効です。キープアライブ メッセージは、設定された間隔で送信されます。有効にする場合は、リモート クライアントが IKE キープアライブ パケットの各送信間の待機時間の間隔を入力します（秒単位）。デフォルトの間隔は 20 秒、有効な範囲は 15 ～ 600 秒です。

- **[デッド ピア検出の有効化（Enable Dead Peer Detection on ...）]** . およびその [間隔（Interval）] 設定：デッド ピア検出（DPD）により、VPN セキュア ゲートウェイまたは VPN クライアントは、ピアが応答しなくなったこと、および接続に失敗したことを迅速に検出できます。デフォルトでは、ゲートウェイとクライアントの両方で有効です。DPD メッセージは、設定された間隔で送信されます。有効にする場合は、リモート クライアントが DPD メッセージの各送信間の待機時間の間隔を入力します（秒単位）。デフォルトの間隔は 30 秒、有効な範囲は 5 ～ 3600 秒です。

- [クライアント バイパス プロトコルを有効にする（Enable Client Bypass Protocol）]：セキュア ゲートウェイが IPv6 トラフィックだけを想定しているときの IPv4 トラフィックの管理方法や、IPv4 トラフィックだけを想定しているときの IPv6 トラフィックの管理方法を設定することができます。

  AnyConnect クライアントがヘッドエンドに VPN 接続するときに、ヘッドエンドは IPv4 と IPv6 の一方または両方のアドレスを割り当てます。ヘッドエンドが AnyConnect 接続に IPv4 アドレスのみ、または IPv6 アドレスのみを割り当てた場合に、ヘッドエンドが IP アドレスを割り当てなかったネットワーク トラフィックについて、クライアント プロトコル バイパスによってそのトラフィックをドロップさせるか（デフォルト、無効、オフ）、またはヘッドエンドをバイパスしてクライアントからの暗号化なし、つまり「クリアテキスト」としての送信を許可するか（有効、オン）を設定できるようになりました。

  たとえば、セキュア ゲートウェイが AnyConnect 接続に IPv4 アドレスだけを割り当て、エンドポイントがデュアルスタックされていると想定してください。このエンドポイントが IPv6 アドレスへの到達を試みたときに、クライアント バイパス プロトコルが無効の場合は、IPv6 トラフィックがドロップされますが、クライアント バイパス プロトコルが有効の場合は、IPv6 トラフィックはクライアントからクリア テキストとして送信されます。

- [SSL キー再生成（SSL rekey）]：クライアントが接続のキーを再生成できるようにして、暗号キーと初期化ベクターを再ネゴシエートし、接続のセキュリティを向上させます。これは、デフォルトでは無効になっています。有効にすると、再ネゴシエーションが指定された間隔で実行され、既存のトンネルのキーが再生成されるか、次のフィールドを設定して新しいトンネルが作成されます。

  - [方法（Method）]：SSL キー再生成が有効な場合に使用可能です。[新しいトンネル（New Tunnel）] を作成する（デフォルト）か、[既存のトンネル（Existing Tunnel）] の仕様を再ネゴシエーションします。

  - [間隔（Interval）]：SSL キー再生成が有効な場合に使用可能です。4 ～ 10080 分（1 週間）の範囲で 4 分のデフォルトに設定します。

- [クライアント ファイアウォール ルール（Client Firewall Rules）]：クライアント ファイアウォール ルールを使用して VPN クライアントのプラットフォームのファイアウォール設定を設定します。ルールは、送信元アドレス、宛先アドレス、プロトコルなどの基準に基づいています。拡張アクセス コントロール リストの構成要素オブジェクトは、トラフィック フィルタ基準を定義するために使用されます。このグループ ポリシーの拡張 ACL を選択するか、作成します。プライベート ネットワークに流れるデータを制御する [プライベート ネットワーク ルール（Private Network Rule）]、確立された VPN トンネルの外部に「クリア テキストで」流れるデータを制御する [パブリック ネットワーク ルール（Public Network Rule）]、または両方を定義します。

（注） ACL に TCP/UDP/ICMP/IP ポートのみが含まれていて、送信元ネットワークが any、any-IPv4、または any-IPv6 であることを確認します。

Microsoft Windows を実行している VPN クライアントだけが、これらのファイアウォール設定を使用できます。

関連トピック

グループ ポリシー オブジェクトの設定 （624 ページ）

グループ ポリシーの詳細オプション

ナビゲーション パス

[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [VPN] > [グループ ポリシー（Group Policy）]、[グループ ポリシーの追加（Add Group Policy）] をクリックするか、現在のポリシーを選択して編集します。 をクリックし、[詳細設定（Advanced）] タブを選択します。

トラフィック フィルタ フィールド

- [アクセス リスト フィルタ（Access List Filter）]：フィルタは、VPN 接続を経由するトンネリングされたデータ パケットを許可するかブロックするかを決定するルールで構成されています。ルールは、送信元アドレス、宛先アドレス、プロトコルなどの基準に基づいています。拡張アクセス コントロール リストの構成要素オブジェクトは、トラフィック フィルタ基準を定義するために使用されます。このグループ ポリシーの新しい拡張 ACL を選択または作成します。

- [VPN を VLAN に規制する（Restrict VPN to VLAN）]：「VLAN マッピング」とも呼ばれ、このパラメータにより、このグループ ポリシーが適用されるセッションの出力 VLAN インターフェイスが指定されます。ASA は、このグループからのすべてのトラフィックを指定された VLAN に転送します。

  この属性を使用して VLAN をグループ ポリシーに割り当て、アクセス コントロールを簡素化します。この属性に値を割り当てる方法は、ACL を使用してセッションのトラフィッ

クをフィルタリングする方法の代替方法です。ドロップダウン リストには、デフォルト値（Unrestricted）の他に、この ASA で設定されている VLAN だけが表示されます。可能な値の範囲は 1 ～ 4094 です。

セッション設定フィールド

- [アクセス時間（Access Hours）]：時間範囲オブジェクトを選択または作成します。このオブジェクトは、このグループ ポリシーがリモート アクセス ユーザに適用可能な時間範囲を指定します。詳細については、時間範囲オブジェクト（537 ページ）を参照してください。
- [ユーザあたり同時ログイン（Simultaneous Logins Per User）]：ユーザに許可する同時ログインの最大数を指定します。デフォルト値は 3 です。最小値は 0 で、この場合ログインが無効になり、ユーザ アクセスを禁止します。複数の同時接続を許可した場合、セキュリティの重大な問題が発生し、パフォーマンスに影響する可能性があります。
- [最大接続時間（Maximum Connection Time）]/[アラート間隔（Alert Interval）]：最大ユーザ接続時間（分単位）を指定します。ここで指定した時間が経過すると、システムは接続を停止します。最小値は 1 分です。[アラート間隔（Alert Interval）] では、最大接続時間に達してユーザにメッセージを表示するまでの時間間隔を指定します。
- [アイドル タイムアウト（Idle Timeout）]/[アラート間隔（Alert Interval）]：このユーザのアイドル タイムアウト期間（分単位）を指定します。この期間、ユーザ接続に通信アクティビティがなかった場合、システムは接続を停止します。最小値は 1 分です。デフォルトは 30 分です。[アラート間隔（Alert Interval）] では、アイドル時間に達してユーザにメッセージを表示するまでの時間間隔を指定します。

関連トピック

グループ ポリシー オブジェクトの設定 （624 ページ）

FTD ファイル オブジェクト

[ファイル オブジェクトの追加（Add File Object）] や [ファイル オブジェクトの編集（Edit File Object）] ダイアログボックスを使用して、ファイル オブジェクトを作成および編集します。ファイル オブジェクトは、通常はリモート アクセス VPN ポリシーの設定で使用するファイルを表します。これには、AnyConnect クライアント プロファイル ファイルや AnyConnect クライアントイメージ ファイルが含まれます。

ファイル オブジェクトを作成すると、Firepower Management Center によってそのファイルのコピーがリポジトリに作成されます。これらのファイルは、データベースのバックアップを作成するたびにバックアップされ、データベースを復元すると復元されます。ファイル オブジェクトでの使用のためにファイルを Firepower Management Center プラットフォームにコピーするときは、ファイルをファイル リポジトリに直接コピーしないでください。

ファイル オブジェクトを削除しても、関連付けられているファイルはファイル リポジトリから削除されず、オブジェクトのみが削除されます。

ファイル オブジェクトを指定する設定を展開すると、関連付けられているファイルが、該当するディレクトリのデバイスにダウンロードされます。

ナビゲーション パス

[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [VPN] > [AnyConnect ファイル（AnyConnect File）]。

フィールド

- [名前（Name）] と [説明（Description）]：最大 128 文字の名前を入力し、オプションでこのファイル オブジェクトを識別するための説明を入力します。
- [ファイル名（File Name）] と [ファイル タイプ（File Type）]：ファイルの名前とフルパス、およびタイプ。[参照（Browse）] をクリックしてファイルを選択し、該当するタイプをクリックします。

  ファイル オブジェクトに含めるためには **AnyConnect クライアントイメージ** および **AnyConnect クライアント プロファイル** タイプのみが有効で、Firepower Management Center プラットフォームに存在する必要があります。

関連トピック

Cisco AnyConnect セキュア モビリティ クライアント イメージ （1118 ページ）
グループ ポリシー AnyConnect オプション （628 ページ）

FTD 証明書のマップ オブジェクトについて

証明書のマップ オブジェクトは、証明書一致ルールの名前付きセットです。これらのオブジェクトは、受信した証明書とリモート アクセス VPN 接続プロファイルとの関連付けを提供するために使用されます。接続プロファイルと証明書のマップ オブジェクトは両方とも、リモート アクセス VPN ポリシーの一部です。受信した証明書が証明書マップに含まれているルールと一致すると、接続は指定の接続プロファイルに「マッピングされている」か、関連付けられています。ルールは優先順位で整理され、UI に表示される順序で照合されます。照合は、証明書マップ オブジェクト内の最初のルールが一致したときに終了します。

ナビゲーション

[オブジェクト（Objects）] > [オブジェクトの管理（Object Management）] > [VPN] > [証明書のマップ（Certificate Map）]

フィールド

- [名前（Name）]：このオブジェクトを特定します。これにより、リモート アクセス VPN などの他の設定で参照できます。
- [マッピング条件（Mapping Criteria）]：評価する証明書の内容を指定します。証明書がこれらのルールの条件を満たしている場合、ユーザはこのオブジェクトを含む接続プロファイルにマッピングされます。

- [コンポーネント（Component）]：一致ルールに対して使用するクライアント証明書のコンポーネントを選択します。
- [フィールド（Field）]：クライアント証明書の [件名（Subject）] または [発行元（Issuer）] に従って、一致ルールのフィールドを選択します。

  [フィールド（Field）] が [代替サブジェクト（Alternative Subject）] または [拡張キーの使用状況（Extended Key Usage）] に設定されている場合、コンポーネントは [フィールド全体（Whole Field）] として凍結されます。
- [演算子（Operator）]：一致ルールの演算子を次のうちから選択します。
  - [等しい（Equals）]：証明書コンポーネントは、入力された値と一致する必要があります。完全に一致しない場合、接続は拒否されます。
  - [含む（Contains）]：証明書コンポーネントには、入力された値が含まれている必要があります。コンポーネントにその値が含まれていない場合、接続は拒否されます。
  - [等しくない（Does Not Equal）]：証明書コンポーネントは、入力された値と等しくない必要があります。たとえば、選択された証明書コンポーネントが Country であり、入力された値が US である場合、クライアントの国の値が US と等しければ、接続が拒否されます。
  - [次を含まない（Does Not Contain）]：証明書コンポーネントには、入力された値が含まれていない必要があります。たとえば、選択された証明書コンポーネントが Country であり、入力された値が US である場合、クライアントの国の値に US が含まれていると、接続が拒否されます。

- [値（Value）]：一致ルールの値。入力された値は、選択されたコンポーネントおよび演算子と関連付けられています。

関連トピック

証明書マップの設定 （1122 ページ）

アドレス プール

クラスタリングの Diagnostic インターフェイス、または VPN リモート アクセス プロファイルに使用できる IPv4 および IPv6 の両方で、IP アドレス プールを設定できます。

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin Access Admin Network Admin

ステップ 1 **[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [アドレス プール（Address Pools）] > [IPv4 プール（IPv4 Pools）]** を選択します。

ステップ 2 [IPv4 プールを追加（Add IPv4 Pools）] をクリックし、次のフィールドを設定します。

- [名前（Name）]：アドレス プールの名前を入力します。最大 64 文字を指定できます。
- [説明（Description）]：このプールのオプションの説明を追加します。
- [IP アドレス（IP Address）]：プールで使用できるアドレスの範囲を入力します。ドット付き 10 進表記および最初と最後のアドレスの間でハイフンを使用します。例：10.10.147.100-10.10.147.177。
- [マスク（Mask）]：この IP アドレスプールが常駐するサブネットを指定します。
- [オーバーライドを許可（Allow Overrides）]：このチェックボックスをオンにして、オブジェクトのオーバーライドを有効にします。展開矢印をクリックして、[オーバーライド（Overrides）] テーブルを表示します。[追加（Add）] をクリックして、新たなオーバーライドを追加することができます。詳細については、オブジェクトのオーバーライド （522 ページ）を参照してください。

ステップ 3 [保存（Save）] をクリックします。

ステップ 4 [IPv6 プールの追加（Add IPv6 Pools）] をクリックし、次のフィールドを設定します。

- [名前（Name）]：アドレス プールの名前を入力します。最大 64 文字を指定できます。
- [説明（Description）]：このプールのオプションの説明を追加します。
- [IPv6 アドレス（IPv6 Address）]：設定されたプールで使用できる最初の IP アドレスとビットのプレフィックス長を入力します。たとえば、2001:DB8::1/64 となります。
- [アドレスの数（Number of Addresses）]：開始 IP アドレスから始まる、プールにある IPv6 アドレスの数を指定します。
- [オーバーライドを許可（Allow Overrides）]：このチェックボックスをオンにして、オーバーライドを有効にします。展開矢印をクリックして、[オーバーライド（Overrides）] テーブルを表示します。[追加（Add）] をクリックして、新たなオーバーライドを追加することができます。詳細については、オブジェクトのオーバーライド （522 ページ）を参照してください。

ステップ 5 **[保存（Save）]** をクリックします。

FlexConfig オブジェクト

FlexConfig ポリシーで FlexConfig ポリシー オブジェクトを使用して、他の方法では Firepower Management Center を使用して設定できない FTD デバイスの機能のカスタマイズされた設定を指定します。FlexConfig ポリシーの詳細については、FlexConfig ポリシーの概要 （1201 ページ）を参照してください。

FlexConfig の次のタイプのオブジェクトを設定できます。

テキスト オブジェクト

テキスト オブジェクトは、FlexConfig オブジェクトで変数として使用する自由形式のテキスト文字列を定義します。このオブジェクトに単一の値を設定したり、このオブジェクトを複数の値のリストにしたりすることができます。

事前定義済みの FlexConfig オブジェクトで使用される複数の事前定義済みテキスト オブジェクトがあります。関連付けられている FlexConfig オブジェクトを使用する場合は、単に、テキスト オブジェクトの内容を編集して、FlexConfig オブジェクトによる特定のデバイスの設定方法をカスタマイズすることだけが必要です。事前定義済みのオブジェクトを編集するには、一般に、これらのオブジェクトのデフォルト値を直接変更するのではなく、設定しているデバイスごとにデバイスの上書きを作成することをお勧めします。これは、他のユーザが別の一連のデバイスに同じ FlexConfig オブジェクトを使用する場合に、意図しない結果が発生しないようにするのに役立ちます。

テキスト オブジェクトの設定については、FlexConfig テキスト オブジェクトの設定 （1234 ページ）を参照してください。

FlexConfig オブジェクト

FlexConfig オブジェクトには、デバイス設定コマンド、変数、およびスクリプト言語の手順が含まれています。導入展開時に、これらの手順が処理されて、一連の設定コマンドが、ターゲット デバイスで特定の機能を設定するカスタマイズされたパラメータとともに作成されます。

これらの手順は、通常の Firepower Management Center ポリシーで定義されている機能が設定される前（先頭に付加）または後（付加）に設定されます。Firepower Management Center で設定されたオブジェクト（ネットワーク オブジェクトなど）に依存する FlexConfig は、設定展開に付加される必要があります。付加されない場合、必要なオブジェクトが、FlexConfig がこのオブジェクトを参照する必要がある前に設定されません。

FlexConfig オブジェクトの設定の詳細については、FlexConfig オブジェクトの設定 （1229 ページ）を参照してください。

RADIUS サーバ グループ

RADIUS サーバ グループ オブジェクトには、RADIUS サーバへの参照が 1 つ以上含まれています。これらのサーバは、リモート アクセス VPN 接続を通じてユーザのログインを認証するために使用されます。

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス（Access）
エクスポート制御機能が有効なスマート ライセンス アカウントに関連付けられている次の AnyConnect ライセンスのいずれか。 • AnyConnect VPN Only • AnyConnect Plus • AnyConnect Apex	該当なし	FTD	いずれか（Any）	Admin

始める前に

（注） RADIUS サーバ グループ オブジェクトは、オーバーライドできません。

ステップ 1 **[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [RADIUS サーバ グループ（RADIUS Server Group）]** を選択します。

現在設定されているすべての RADIUS サーバ グループ オブジェクトがリスト表示されます。フィルタを使用して、リストを絞り込んでください。

ステップ 2 リストされた [RADIUS サーバ グループ（RADIUS Server Group）] オブジェクトを選択し、編集するか、新しいオブジェクトを追加します。

このオブジェクトを設定する場合は、RADIUS サーバ オプション （638 ページ）およびRADIUS サーバ グループのオプション （637 ページ）を参照してください。

ステップ 3 [Save（保存）] をクリックします。

RADIUS サーバ グループのオプション

ナビゲーション パス

[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [RADIUS サーバ グループ（RADIUS Server Group）]。設定済みの RADIUS サーバ グループ オブジェクトを選択して編集するか、または新しく追加します。

フィールド

- [名前（Name）] と [説明（Description）]：この RADIUS サーバ グループ オブジェクトを識別するための名前と、任意で説明を入力します。
- [グループ アカウンティング モード（Group Accounting Mode）]：グループ内の RADIUS サーバにアカウンティング メッセージを送信するための方法です。[1 つ（Single）] を選択します。アカウンティング メッセージがグループ内の 1 つのサーバに送信されます。これはデフォルトです。または、[同時（Simultaneous）] を選択します。アカウンティング メッセージがグループ内のすべてのサーバに同時に送信されます。
- [間隔のリトライ（Retry Interval）]：RADIUS サーバへの接続を試みる間隔です。間隔の範囲は、1 ～ 10 秒です。
- [レルム（Realms）]（オプション）：この RADIUS サーバ グループに関連付ける AD または LDAP レルムを指定または選択します。その後、トラフィック フローの VPN 認証アイデンティティ ソースの判別時に、関連する RADIUS サーバ グループにアクセスするためにこのレルムがアイデンティティ ポリシーで選択されます。このレルムは実質的に、アイデンティティ ポリシーからこの Radius サーバ グループへのブリッジを提供します。この RADIUS サーバ グループにレルムを関連付けない場合、アイデンティティ ポリシーでトラフィック フローの VPN 認証アイデンティティ ソースを判別するために RADIUS サーバ グループに到達することができません。
- [許可のみを有効にする（Enable authorize only）]：この RADIUS サーバ グループが認証に使用されないが、許可またはアカウンティングに使用される場合は、このフィールドをオンにすると RADIUS サーバ グループの許可限定モードが有効になります。

  許可限定モードでは、アクセス要求に RADIUS サーバ パスワードを含める必要がありません。したがって、個別の RADIUS サーバに設定されたパスワードが無視されます。
- [アカウントの暫定更新（Enable interim account update）を有効にする] および [間隔（Interval）]：新たに割り当てられた IP アドレスを RADIUS サーバに通知するために、RADIUS interim-accounting-update メッセージの生成を有効にします。[間隔（Interval）] フィールドの定期アカウンティング更新の間隔時間長を設定します。有効数は 1 ～ 120 であり、デフォルト値は 24 です。
- [ダイナミック認証の有効化（Enable Dynamic Authorization）] と [ポート（Port）]：この RADIUS サーバ グループの RADIUS ダイナミック認証または認可変更（CoA）サービスを有効にします。[ポート（Port）] フィールドで、RADIUS CoA 要求のリスニング ポートを指定します。有効数は 1024 ～ 65535 であり、デフォルト値は 1700 です。一旦定義され

ると、対応する RADIUS サーバ グループが CoA 通知用に登録され、Cisco Identity Services Engine（ISE）から CoA ポリシーの更新を行うポートにリッスンします。

- [RADIUSサーバ（RADIUS Servers）]：RADIUS サーバ オプション （638 ページ） を参照してください。

関連トピック

RADIUS サーバ グループ （635 ページ）

RADIUS サーバ オプション

ナビゲーション パス

[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [RADIUS サーバ グループ（RADIUS Server Group）]。リストされた [RADIUS サーバ グループ（RADIUS Server Group）] オブジェクトを選択し、編集するか、新しいオブジェクトを追加します。次に、[RADIUS サーバ グループ（RADIUS Server Group）] ダイアログで、リストされた RADIUS サーバを選択して、編集するか、新しい RADIUS サーバを追加します。

フィールド

- [IPアドレス/ホスト名（IP Address/Hostname）]：認証要求が送信される RADIUS サーバのホスト名または IP アドレスを特定するネットワーク オブジェクトです。ホスト名または IP アドレスを 1 つのみ選択し、追加のサーバに追加し、更なる RADIUS サーバを RADIUS サーバ グループ リストに追加します。

（注） Firepower Threat Defense は、RADIUS 認証の IPv6 IP アドレスをサポートするようになりました。

- [認証ポート（Authentication Port）]：RADIUS 認証および承認が行われるポートです。デフォルトは 1812 です。
- [キー（Key）] および [キーの確認（Confirm Key）]：管理対象デバイス（クライアント）と RADIUS サーバ間でデータを暗号化するために使用される共有秘密です。

  キーでは、127 文字以下の英数字で、大文字と小文字を区別します。特殊文字も使用可能です。

  このフィールドで定義したキーは、RADIUS サーバのキーと一致している必要があります。確認フィールドでもう一度キーを入力します。
- [アカウンティング ポート（Accounting Port）]：RADIUS アカウンティングが実行されるポートです。デフォルトは 1813 です。
- [タイムアウト（Timeout）]：認証のセッション タイムアウト。

（注） RADIUS 二要素認証の場合、タイムアウト値は 60 秒以上必要です。デフォルトのタイムアウト値は 10 秒です。

- [使用して接続（Connect Using）]：ルーティングまたは特定のインターフェイスを使用して、Firepower Threat Defense から RADIUS サーバへの接続を確立します。RADIUS サーバに [ルーティング（Routing）] を選択すると、ルーティング テーブルによって解決済みのパスで接続が確立されます。または [特定のインターフェイス（Specific Interface）] を選択し、リストからインターフェイスを選択するか、新しいインターフェイス/セキュリティゾーンを追加します。

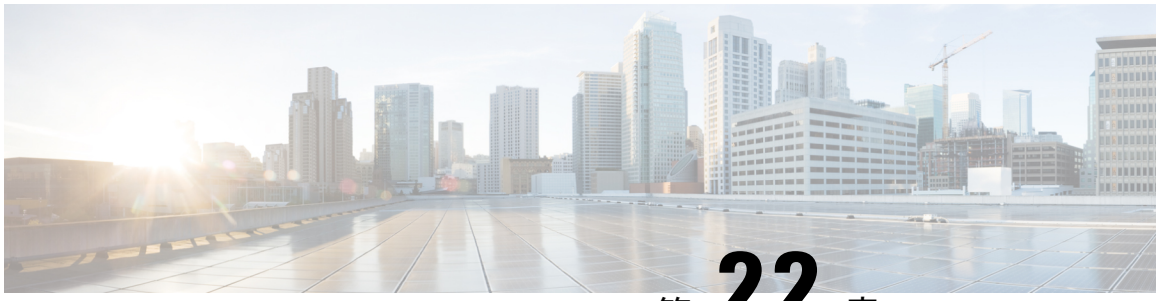
  Firepower Threat Defense から RADIUS サーバへの接続は、セキュリティ ゾーンまたはインターフェイス グループの一部である特定のインターフェイスを介して確立されます。リストからインターフェイスが選択されていない場合、診断インターフェイスがデフォルトのインターフェイスとして使用されます。

  インターフェイス オブジェクト：インターフェイス グループとセキュリティ ゾーン（535 ページ）を参照してください。
- [リダイレクトACL（Redirect ACL）]：リストからリダイレクト ACL を選択するか、新しいリダイレクト ACL を追加します。

（注） これは、リダイレクトされるトラフィックを決定するために Firepower Threat Defense で定義されている ACL の名前です。ここでのリダイレクト ACL の名前は、ISE サーバの *redirect-acl* の名前と同じである必要があります。ACL オブジェクトを設定する場合は、ISE サーバと DNS サーバに [Block（ブロック）] アクションを、残りのサーバに [許可（Allow）] アクションを必ず選択してください。

関連トピック

RADIUS サーバ グループ （635 ページ）
RADIUS サーバ グループのオプション （637 ページ）



第 22 章

Firepower Threat Defense Certificate ベースの認証

Firepower Threat Defense VPN 証明書の注意事項と制約事項

- 証明書登録オブジェクトがデバイスに関連付けられ、デバイスにインストールされるとすぐに、証明書登録プロセスが開始されます。プロセスは、自己署名および SCEP 登録タイプの場合は自動的に行われます。つまり、管理者による追加のアクションは必要ありません。手動証明書登録では、さらに管理者の操作が必要になります。
- 登録が完了すると、証明書の登録オブジェクトと同じ名前のトラストポイントがデバイス上に生成されます。VPN 認証方式の設定でこのトラストポイントを使用します。
- FTD デバイスは、Microsoft CA サービスと、Cisco 適応型セキュリティ アプライアンス（ASA）および Cisco IOS ルータで提供される CA サービスを使用した証明書の登録をサポートしており、検証済みです。
- FTD デバイスは、CA として設定することはできません。

ドメインとデバイス間での証明書の管理のガイドライン

- 証明書の登録は、子ドメインまたは親ドメインで行うことができます。

- 親ドメインからの登録が完了したら、証明書の登録オブジェクトもそのドメイン内に存在する必要があります。デバイスのトラストポイントが子ドメインで上書きされた場合、上書きされた値がデバイスに展開されます。
- リーフ ドメインのデバイスで証明書の登録が行われる場合、その登録は親ドメインまたは他の子ドメインに表示されます。また、証明書を追加することもできます。
- リーフ ドメインが削除されると、含まれているデバイス上の証明書の登録が自動的に削除されます。
- あるドメインに登録されている証明書を持つデバイスは、他のドメインに登録できます。他のドメインに証明書を追加できます。
- あるドメインから別のドメインにデバイスを移動すると、証明書もそれに応じて移動します。これらのデバイスの登録を削除するための警告が表示されます。

FTD 証明書の管理

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin/Network Admin/Security Approver

デジタル証明書の概要については、PKI インフラストラクチャとデジタル証明書 （1062 ページ）を参照してください。

管理対象デバイスの証明書を登録および取得するために使用するオブジェクトの説明については、証明書の登録オブジェクト （591 ページ）を参照してください。

ステップ 1 **[Devices]** > **[Certificates]** に進みます。

この画面で、次の操作を実行します。

- すでにトラストポイントが関連付けられているデバイスは、[名前（Name）] 列にリスト表示されます。デバイスを展開して、関連付けられたトラストポイントのリストを確認します。

  このトラストポイントに使用する登録タイプは、[登録タイプ（Enrollment Type）] 列に表示されます。

  特定のドメインに登録された証明書が [ドメイン] 列に表示されます。

- [ステータス（Status）] 列には、[CA 証明書（CA Certificate）] と [アイデンティティ証明書（Identity Certificate）] のステータスが表示されます。虫めがねをクリックすることで、証明書の内容を表示できます（`Available` の場合）。

  登録に失敗した場合は、アイコンをクリックして失敗メッセージを表示します。

- 管理対象デバイスの証明書を更新します（環状の矢印）。証明書を更新すると、Firepower Threat Defense デバイスの証明書ステータスが Firepower Management Center に同期されます。
- 再登録アイコンを使用して、アイデンティティ証明書を登録します。

  ポリシーの展開中に、証明書の登録プロセスが失敗した場合は、再登録オプションを使用してアイデンティティ証明書を再度登録します。
- 設定済みの証明書を削除（ゴミ箱に移動）します。

ステップ 2 [（+）追加（(+) Add）] を選択して、登録オブジェクトをデバイスに関連付けてインストールします。

証明書登録オブジェクトがデバイスに関連付けられ、デバイスにインストールされるとすぐに、証明書登録プロセスが開始されます。プロセスは、自己署名および SCEP 登録タイプの場合は自動的に行われます。つまり、管理者による追加のアクションは必要ありません。手動証明書登録では、さらに管理者の操作が必要になります。

（注） デバイス上の証明書の登録ではユーザ インターフェイスがブロックされず、登録プロセスはバックグラウンドで実行され、ユーザは他のデバイスで証明書の登録を並行して実行できます。これらの並列操作の進行状況は、同じユーザ インターフェイスでモニタできます。それぞれのアイコンには、証明書の登録ステータスが表示されます。

関連トピック

自己署名登録を使用した証明書のインストール （643 ページ）
SCEP の登録を使用した証明書のインストール （644 ページ）
手動登録を使用した証明書のインストール （645 ページ）
PKCS12 ファイルを使用した証明書のインストール （646 ページ）

自己署名登録を使用した証明書のインストール

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin/Network Admin

ステップ 1 [デバイス（Devices）]>[証明書（Certificates）] 画面で [追加（Add）] を選択して、[新規証明書の追加（Add New Certificate）] ダイアログを開きます。

ステップ 2 [デバイス（Device）] ドロップダウン リストからデバイスを選択します。

ステップ 3 次のいずれかの方法で、証明書の登録オブジェクトとこのデバイスを関連付けます。

- ドロップダウンリストからタイプが [自己署名（Self-Signed）] の証明書登録オブジェクトを選択します。

- [(+)] をクリックして、新しい証明書登録オブジェクトを追加します。証明書の登録オブジェクトの追加 （593 ページ） を参照してください。

ステップ 4 [追加（Add）] をクリックして、自己署名の自動登録プロセスを開始します。

自己署名登録タイプのトラストポイントの場合、[CA 証明書（CA Certificate）] ステータスは、常にアイコンで表示されます。これは、管理対象デバイス自体が独自の CA として機能し、独自のアイデンティティ証明書を生成するために CA 証明書を必要としないためです。

[ID 証明書（Identity Certificate）] は、デバイスが独自の自己署名アイデンティティ証明書を作成すると、InProgress から Available に変化します。

ステップ 5 虫めがねをクリックして、このデバイスの自己署名アイデンティティ証明書を表示します。

次のタスク

登録が完了すると、証明書登録オブジェクトと同じ名前のトラストポイントがデバイス上に生成されます。サイト間およびリモート アクセス VPN 認証方式の設定でこのトラストポイントを使用します。

SCEP の登録を使用した証明書のインストール

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin/Network Admin

始める前に

（注） SCEP 登録を使用すると、管理対象デバイスと CA サーバとの間に直接接続が確立されます。したがって、登録プロセスを開始する前に、デバイスが CA サーバに接続されていることを確認してください。

ステップ 1 [デバイス（Devices）] > [証明書（Certificates）] 画面で [追加（Add）] を選択して、[新規証明書の追加（Add New Certificate）] ダイアログを開きます。

ステップ 2 [デバイス（Device）] ドロップダウン リストからデバイスを選択します。

ステップ 3 次のいずれかの方法で、証明書の登録オブジェクトとこのデバイスを関連付けます。

- ドロップダウンリストからタイプが [SCEP] の証明書登録オブジェクトを選択します。
- [(+)] アイコンをクリックして、新しい証明書登録オブジェクトを追加します。証明書の登録オブジェクトの追加 （593 ページ）を参照してください。

ステップ 4 [追加（Add）] をクリックして、自動登録プロセスを開始します。

SCEP 登録タイプのトラストポイントの場合、[CA 証明書（CA Certificate）] ステータスは、CA サーバから CA 証明書が取得され、デバイスにインストールされると、InProgress から Available に遷移します。

[アイデンティティ証明書（Identity Certificate）] は、デバイスが SCEP を使用したアイデンティティ証明書を指定の CA から取得すると、`InProgress` から `Available` に変化します。場合によっては、アイデンティティ証明書の取得には手動更新が必要になります。

ステップ 5 虫めがねをクリックして、このデバイスに作成してインストールしたアイデンティティ証明書を表示します。

次のタスク

登録が完了すると、証明書登録オブジェクトと同じ名前のトラストポイントがデバイス上に生成されます。サイト間およびリモート アクセス VPN 認証方式の設定でこのトラストポイントを使用します。

手動登録を使用した証明書のインストール

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin/Network Admin

ステップ 1 [デバイス（Devices）]>[証明書（Certificates）] 画面で [追加（Add）] を選択して、[新規証明書の追加（Add New Certificate）] ダイアログを開きます。

ステップ 2 [デバイス（Device）] ドロップダウン リストからデバイスを選択します。

ステップ 3 次のいずれかの方法で、証明書の登録オブジェクトとこのデバイスを関連付けます。

- ドロップダウンリストからタイプが [マニュアル（Manual）] の証明書登録オブジェクトを選択します。
- [(+)] アイコンをクリックして、新しい証明書登録オブジェクトを追加します。証明書の登録オブジェクトの追加 （593 ページ）を参照してください。

ステップ 4 [追加（Add）] をクリックして、登録プロセスを開始します。

ステップ 5

ステップ 6 アイデンティティ証明書を取得するための PKI CA サーバに対する適切なアクティビティを実行します。

a) [アイデンティティ証明書（Identity Certificate）] の警告アイコンをクリックして、CSR を表示してコピーします。

b) この CSR を使用してアイデンティティ証明書を取得するための PKI CA サーバに対する適切なアクティビティを実行します。

このアクティビティは、Firepower Management Center または管理対象デバイスとは完全に無関係です。完了すると、管理対象デバイスのアイデンティティ証明書が生成されます。ファイルに配置できます。

c) 手動プロセスを終了するには、取得したアイデンティティ証明書を管理対象デバイスにインストールします。

Firepower Management Center ダイアログに戻って、[アイデンティティ証明書の参照（Browse Identity Certificate）] を選択して、アイデンティティ証明書ファイルを選択します。

ステップ 7 [インポート（Import）] を選択して、アイデンティティ証明書をインポートします。

[アイデンティティ証明書（Identity Certificate）] のステータスは、インポートが完了すると `Available` になります。

ステップ 8 虫めがねをクリックして、このデバイスの [アイデンティティ証明書（Identity Certificate）] を表示します。

次のタスク

登録が完了すると、証明書登録オブジェクトと同じ名前のトラストポイントがデバイス上に生成されます。サイト間およびリモート アクセス VPN 認証方式の設定でこのトラストポイントを使用します。

PKCS12 ファイルを使用した証明書のインストール

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin/Network Admin

ステップ 1 [デバイス（Devices）]>[証明書（Certificates）] 画面の順に移動し、[追加（Add）] を選択して、[新規証明書の追加（Add New Certificate）] ダイアログを開きます。

ステップ 2 [デバイス（Device）] ドロップダウンリストから、事前設定された管理対象デバイスを選択します。

ステップ 3 次のいずれかの方法で、証明書の登録オブジェクトとこのデバイスを関連付けます。

- ドロップダウン リストから PKCS タイプの 証明書の登録オブジェクト を選択します。
- [(+)] アイコンをクリックして新しい証明書の登録オブジェクトを追加します。証明書の登録オブジェクトの追加 （593 ページ）を参照してください。

ステップ 4 [ツイカ（Add）] を押します。

[CA証明書（CA Certificate）] および [アイデンティティ証明書（Identity Certificate）] のステータスは、デバイスに PKCS12 ファイルがインストールされるときに `In Progress` から `Available` に変化します。

（注） 初めて PKCS12 ファイルをアップロードすると、ファイルが CertEnrollment オブジェクトの一部として Firepower Management Center に格納されます。不正なパスフレーズや展開の失敗が原因で登録できなかった場合は、ファイルをアップロードせずに PKCS12 証明書の登録を再試行します。PKCS12 ファイル サイズは 24 K を超えてはなりません。

ステップ 5 `Available` になったら、虫めがねをクリックして、このデバイスのアイデンティティ証明書を表示します。

次のタスク

管理対象デバイスの証明書（トラストポイント）には、PKCS#12 ファイルと同じ名前が付けられます。この証明書は、VPN 認証設定で使用します。

FTD 証明書のトラブルシューティング

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin/Network Admin/Security Approver

Firepower Threat Defense VPN 証明書の注意事項と制約事項（641 ページ）を参照して、証明書の登録環境のバリエーションが原因で問題が発生しているかどうかを判断してください。その後、次の点を確認します。

- デバイスから CA サーバへのルートがあることを確認します。

  CA サーバのホスト名が登録オブジェクトで指定されている場合、Flex コンフィギュレーションを使用して、サーバに到達できるように DNS を適切に設定します。あるいは、CA サーバの IP アドレスを使用することもできます。

- Microsoft 2012 CA サーバを使用している場合、デフォルトの IPsec テンプレートは管理対象デバイスで受け入れられないため、これを変更する必要があります。

  作業テンプレートを設定するには、MS CA のドキュメントを参照しながら次の手順に従います。

  1. IPsec（オフライン要求）テンプレートを複製します。
  2. [拡張子（Extensions）] タブで、[アプリケーション ポリシー（Application policies）] として [*IP* セキュリティ *IKE* 中間（*IP security IKE intermediate*）]ではなく、[*IP* セキュリティ末端システム（*IP security end system*）] を選択します。
  3. アクセス許可とテンプレート名を設定します。
  4. 新しいテンプレートを追加し、レジストリ設定を変更して新しいテンプレート名を反映させます。

第 V 部

クラシック デバイス設定の基本

第 23 章

クラシック デバイス管理の基本

次のトピックでは、Firepower システムで従来型デバイス（7000 および 8000 シリーズ、ASA with Firepower Services、NGIPSv）を管理する方法について説明します。

リモート管理の設定（従来型デバイス）

7000 および 8000シリーズを除くすべてのデバイス

従来のライセンスを使用するデバイスのリモート管理設定の詳細については、デバイスのクイック スタート ガイドを参照してください。

7000 および 8000 シリーズ デバイス

FMC にデバイスを登録する前にローカル Web インターフェイスを使用して、7000 または 8000 シリーズ デバイスのリモート管理を設定します。

Firepower デバイスを管理できるようにするには、事前にデバイスと Firepower Management Center との間に双方向の SSL 暗号化通信チャネルをセットアップする必要があります。このチャネルを使用して、両方のアプライアンスが設定とイベント情報を共有します。ハイ アベイラビリティ ピアも、このチャネルを使用します。このチャネルは、デフォルトではポート 8305/tcp に位置します。

2 つのアプライアンス間の通信を可能にするためには、次のように、アプライアンスが互いを認識する手段を提供しなければなりません。

- 通信を確立する対象のアプライアンスのホスト名または IP アドレス。

  NAT 環境では、ルーティング可能なアドレスがもう一方のアプライアンスにないとしても、リモート管理を設定する際、または管理対象アプライアンスを追加する際には、ホスト名または IP アドレスのいずれかを指定する必要があります。

- 接続を識別するために自己生成される、最大 37 文字の英数字による登録キー。

- NAT 環境で通信を確立するために利用できるオプションの一意の英数字による NAT ID。

NAT ID は、管理対象アプライアンスを登録するために使用されているすべての NAT ID の間で一意でなければなりません。

管理対象デバイス上のリモート管理の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	7000 & 8000 シリーズ	該当なし	Admin/Network Admin

ステップ 1 管理するデバイスの Web インターフェイスで、**[System]** > **[Integration]** > **[Remote Management]** を選択します。

ステップ 2 [リモート管理（Remote Management）] タブが表示されていない場合は、クリックします。

ステップ 3 [マネージャの追加（Add Manager）] をクリックします。

ステップ 4 [管理ホスト（Management Host）] フィールドに、このアプライアンスを管理するために使用する Firepower Management Center について、次のいずれかを入力します。

- IP アドレス
- 完全修飾ドメイン名またはローカル DNS で有効な IP アドレスに解決される名前（つまり、ホスト名）

注意 ネットワークで IP アドレスの割り当てに DHCP を使用している場合は、IP アドレスではなく、ホスト名を使用します。

NAT 環境では、管理対象アプライアンスを追加する際に IP アドレスまたはホスト名を指定する予定の場合、ここで IP アドレスまたはホスト名を指定する必要はありません。その場合、Firepower システムは後で指定される NAT ID を使用して、管理対象アプライアンスの Web インターフェイス上のリモート マネージャを識別します。

ステップ 5 [登録キー（Registration Key）] フィールドに、アプライアンス間の通信をセットアップするために使用する登録キーを入力します。

ステップ 6 NAT 環境の場合は、[固有 NAT ID（Unique NAT ID）] フィールドに、アプライアンス間の通信をセットアップするために使用する、英数字による一意の NAT ID を入力します。

ステップ 7 [保存（Save）] をクリックします。

次のタスク

- アプライアンスが相互に通信できることを確認し、ステータスとして [登録保留（Pending Registration）] が表示されるまで待ちます。
- このデバイスを Firepower Management Center に追加します。Firepower Management Center へのデバイスの追加 （293 ページ）を参照してください。

管理対象デバイスでのリモート管理の編集

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	7000 & 8000 シリーズ	該当なし	Admin/Network Admin

リモート マネージャを編集するには、次の点に注意してください。

- [ホスト（Host）] フィールドでは、完全修飾ドメイン名またはローカル DNS で有効な IP アドレスに解決される名前（つまり、ホスト名）を指定します。
- [名前（Name）] フィールドには、Firepower システムのコンテキストでのみ使用される、管理アプライアンスの表示名を指定します。別の表示名を入力しても、管理デバイスのホスト名は変更されません。

ステップ 1 デバイスの Web インターフェイスで、**[System]** > **[Integration]** を選択します。

ステップ 2 まだ表示されていない場合は、[リモート管理（Remote Management）] タブをクリックします。

ステップ 3 次の操作を実行できます。

- リモート管理の無効化：マネージャの横にあるスライダをクリックして、これを有効または無効にします。管理を無効化すると、Firepower Management Center とデバイス間の接続がブロックされますが、Firepower Management Center からデバイスは削除**されません**。デバイスを管理する必要がなくなった場合は、Firepower Management Center からのデバイスの削除 （295 ページ）を参照してください。
- マネージャ情報の編集：変更するマネージャの横にある編集アイコン（  ）をクリックして、[名前（Name）] および [ホスト（Host）] フィールドをクリックし、[保存（Save）] をクリックします。

管理ポートの変更

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	7000 & 8000 シリーズ FMC	グローバルだけ	Admin/Network Admin

アプライアンスは、双方向の SSL 暗号化通信チャネルを使用して通信します。このチャネルは、デフォルトではポート 8305 に位置します。

設定をデフォルトのままにすることを強く奨励します。管理ポートがネットワークでの他の通信と競合する場合には、他のポートを選択できます。通常、管理ポートの変更はインストール時に行います。

⚠

注意 管理ポートを変更する場合は、導入内の相互に通信する必要があるすべてのアプライアンスの管理ポートを変更する必要があります。

ステップ 1 **[System]** > **[Configuration]**を選択します。

ステップ 2 [管理インターフェイス（Management Interfaces）] をクリックします。

ステップ 3 [共有設定（Shared Settings）] セクションで、[リモート管理ポート（Remote Management Port）] フィールドに使用するポート番号を入力します。

ステップ 4 [保存（Save）] をクリックします。

次のタスク

このアプライアンスと通信する必要がある、展開環境内のすべてのアプライアンスについて、この手順を繰り返します。

インターフェイス構成時の設定

アプライアンス エディタの [インターフェイス（Interfaces）] ページには、詳細なインターフェイス設定情報が表示されます。このページは、物理ハードウェア ビューとインターフェイス テーブル ビューで構成されており、構成の詳細情報にドリルダウンできます。このページからインターフェイスを追加したり編集したりできます。

物理的なハードウェア ビュー

[インターフェイス（Interfaces）] ページの一番上には、7000 または 8000 シリーズ デバイスの物理的なハードウェア ビューがグラフィカル表示されます。

物理的なハードウェア ビューは、次の目的で使用します。

- ネットワーク モジュールのタイプ、部品番号、およびシリアル番号を確認する
- インターフェイス テーブル ビューでインターフェイスを選択する
- インターフェイス エディタを開く
- インターフェイスの名前、タイプ、リンクの有無、速度設定、およびインターフェイスがバイパス モードになっているかを確認する
- エラーまたは警告の詳細を参照する

インターフェイス アイコン

表 *67*：インターフェイス アイコンのタイプと説明

アイコン	インターフェイス タイプ	詳細情報の参照先
	物理的：未設定の物理インターフェイス。	物理スイッチド インターフェイスの設定（1571 ページ）または物理ルーテッド インターフェイスの設定 （1583 ページ）
	パッシブ：パッシブ展開でトラフィックを分析するように設定されているセンシング インターフェイス。	パッシブ インターフェイスの設定 （664 ページ）
	インライン：インライン展開でトラフィックを処理するように設定されているセンシング インターフェイス。	インライン インターフェイスの設定 （668 ページ）
	スイッチド：レイヤ 2 展開でトラフィックを切り替えるように設定されているインターフェイス。	スイッチドインターフェイスの設定 （1570 ページ）
	ルーテッド：レイヤ 3 展開でトラフィックをルーティングするように設定されているインターフェイス。	ルーテッド インターフェイス （1582 ページ）
	集約：1 つの論理リンクとして設定されている複数の物理インターフェイス。	集約インターフェイスについて （1619 ページ）
	集約スイッチド：レイヤ 2 展開で 1 つの論理リンクとして設定されている複数の物理インターフェイス。	集約スイッチド インターフェイスの追加 （1626 ページ）
	集約ルーテッド：レイヤ 3 展開で 1 つの論理リンクとして設定されている複数の物理インターフェイス。	集約ルーテッド インターフェイスの追加 （1629 ページ）
	ハイブリッド：仮想ルータと仮想スイッチ間でトラフィックをブリッジするように設定されている論理インターフェイス。	論理ハイブリッドインターフェイス （1637 ページ）
	HA：デバイス間で冗長通信チャネルとして機能するように設定されている、デバイスのペア メンバー上のインターフェイス（別名「ハイ アベイラビリティ リンク インターフェイス」）。	HA リンク インターフェイスの設定 （658 ページ）

アイコン	インターフェイス タイプ	詳細情報の参照先
	ASA FirePOWER：ASA FirePOWER モジュールがインストールされた ASA デバイスに設定されているインターフェイス。	Cisco ASA FirePOWER インターフェイスの管理 （660 ページ）

物理ハードウェア ビューの使用

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	7000 & 8000 シリーズ	いずれか（Any）	Admin/Network Admin

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 管理するデバイスの横にある編集アイコン（  ）をクリックします。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 グラフィカル インターフェイスを使用して、以下を実行できます。

- 選択：インターフェイスを選択する場合、インターフェイス アイコンをクリックします。システムは、インターフェイス テーブルの関連項目を強調表示します。
- 編集：インターフェイスエディタを開く場合、インターフェイスアイコンをダブルクリックします。
- エラーまたは警告情報の表示：エラーまたは警告に関する詳細を表示するには、ネットワーク モジュール上の影響を受けるポートの上にカーソルを置きます。
- インターフェイス情報の表示：インターフェイスの名前、インターフェイスのタイプ、インターフェイスにリンク画が存在するかどうか、インターフェイスの速度設定、インターフェイスが現在バイパス モードであるかどうかについて表示するには、インターフェイス上にカーソルを置きます。
- ネットワーク モジュール情報の表示：ネットワーク モジュールのタイプ、製品番号、シリアル番号を表示するには、ネットワーク モジュールの左下隅にある黒い円の上にカーソルを置きます。

センシング インターフェイスの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
該当なし	いずれか（Any）	従来型	リーフのみ	Admin/Network Admin

アプライアンス エディタの [インターフェイス（Interfaces）] ページで、Firepower の展開に応じて、管理対象デバイスのセンシング インターフェイスを設定できます。管理対象デバイスには、合計 1024 個のインターフェイスを設定できることに注意してください。

（注） Firepower Management Center では、ASA FirePOWER が SPAN ポート モードで展開されている場合、ASA インターフェイスを表示しません。

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 インターフェイスを設定するデバイスの横にある編集アイコン（）をクリックします。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 設定するインターフェイスの横にある編集アイコン（）をクリックします。

ステップ 4 インターフェイス エディタを使用して、センシング インターフェイスを設定します。

- [HAリンク（HA Link）] : 7000/8000 シリーズ デバイスのハイ アベイラビリティ ペアの各メンバーに設定されたインターフェイスを、（ハイ アベイラビリティ リンク インターフェイスとも呼ばれる）デバイス間の冗長通信チャネルとして機能させるには、[HAリンク（HA Link）] をクリックし、HA リンク インターフェイスの設定 （658 ページ）の説明に従って続行します。
- [インライン（Inline）] : 設定されたインターフェイスでインライン展開のトラフィックを処理するように設定するには、[インライン（Inline）] をクリックし、インライン インターフェイスの設定 （668 ページ）の説明に従って続行します。
- [パッシブ（Passive）] : 設定されたインターフェイスでパッシブ展開のトラフィックを分析するように設定するには、[パッシブ（Passive）] をクリックし、パッシブ インターフェイスの設定 （664 ページ）の説明に従って続行します。
- [ルーテッド（Routed）] : 設定されたインターフェイスで 7000/8000 シリーズ レイヤ 3 展開のトラフィックをルーティングするように設定するには、[ルーテッド（Routed）] をクリックし、ルーテッド インターフェイス （1582 ページ）の説明に従って続行します。
- [スイッチド（Switched）] : 設定されたインターフェイスで 7000/8000 シリーズ レイヤ 2 展開のトラフィックをスイッチングするように設定するには、[スイッチド（Switched）] をクリックし、スイッチド インターフェイスの設定 （1570 ページ）の説明に従って続行します。

ステップ 5 **[保存（Save）]** をクリックします。

次のタスク

設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

HA リンク インターフェイスの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
該当なし	いずれか（Any）	7000 & 8000 シリーズ	リーフのみ	Admin/Network Admin

7000 または 8000 シリーズ デバイスの高可用性ペアを確立した後、物理インターフェイスをハイ アベイラビリティ（HA）リンク インターフェイスとして設定する必要があります。このリンクは、ペアリングされたデバイス間でヘルス情報を共有するために使用する、冗長通信チャネルとして機能します。1 つのデバイスに HA リンク インターフェイスを設定すると、自動的に 2 番目のデバイスにインターフェイスが設定されます。同じブロードキャスト ドメインに、両方の HA リンクを設定する必要があります。

ダイナミック NAT は、他の IP アドレスとポートにマップする IP アドレスとポートの動的割り当てに依存します。HA リンクがなければ、これらのマッピングはフェールオーバーで失われます。その場合、変換されたすべての接続は高可用性ペアで新しくアクティブになったデバイスを介してルーティングされることになるため、それらの接続は失敗します。

同様に、高可用性状態共有、ダイナミック NAT、または VPN が設定された 7000 または 8000 シリーズ デバイスには、HA リンク インターフェイスが必要です。

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 HA リンク インターフェイスを設定するピアの横にある編集アイコン（）をクリックします。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 HA リンク インターフェイスとして設定するインターフェイスの横にある編集アイコン（）をクリックします。

ステップ 4 [HA リンク（HA Link）] をクリックします。

ステップ 5 [有効（Enabled）] チェックボックスをオンにします。

チェックボックスをオフにした場合、システムはインターフェイスを管理上停止し、無効にします。

ステップ 6 [モード（Mode）] ドロップダウン リストからリンク モードを指定するオプションを選択するか、[自動ネゴシエーション（Autonegotiation）] を選択して、速度とデュプレックスの設定を自動ネゴシエートするようにインターフェイスを設定します。

ステップ 7 [MDI/MDIX] ドロップダウン リストから、インターフェイスの設定対象として MDI（メディア依存型インターフェイス）、MDIX（メディア依存型インターフェイス クロスオーバー）、または自動 MDIX のいずれかを指定するオプションを選択します。

通常、[MDI/MDIX] は [自動 MDIX（Auto-MDIX）] に設定します。これにより、MDI と MDIX の間の切り替えが自動的に処理され、リンクが確立されます。

ステップ 8 [MTU] フィールドに最大伝送ユニット（MTU）を入力します。

MTU 値の範囲は管理対象デバイスのモデルとインターフェイス タイプによって異なる場合があります。詳細については、7000 および 8000 シリーズ デバイスおよび NGIPSv の MTU 範囲 （661 ページ）を参照してください。

注意 デバイス上のすべての非管理インターフェイスの中で最大 MTU 値を変更し、設定変更を展開すると、Snort プロセスが再起動され、トラフィック インスペクションが一時的に中断されます。インスペクションは、変更したインターフェイスだけでなく、すべての非管理インターフェイスで中断されます。この中断によってトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびインターフェイスのタイプに応じて異なります。詳細については、「Snort® の再起動によるトラフィックの動作 （451 ページ）」を参照してください。

ステップ 9 **[保存（Save）]** をクリックします。

次のタスク

設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

関連トピック

Snort® の再起動シナリオ （450 ページ）
7000 および 8000 シリーズ デバイスおよび NGIPSv の MTU 範囲 （661 ページ）

インターフェイスの無効化

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	7000 & 8000 シリーズ NGIPSv	リーフのみ	Admin/Network Admin

インターフェイス タイプを [なし（None）] に設定することで、インターフェイスを無効にすることができます。無効にされたインターフェイスは、インターフェイス リストでグレー表示されます。

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 インターフェイスを無効にするデバイスの横にある編集アイコン（  ）をクリックします。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 無効にするインターフェイスの横にある編集アイコン（  ）をクリックします。

ステップ 4 [なし（None）] をクリックします。

ステップ 5 **[保存（Save）]** をクリックします。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

Cisco ASA FirePOWER インターフェイスの管理

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	ASA FirePOWER	リーフのみ	Admin/Network Admin

ASA FirePOWER インターフェイスを編集する際に、Firepower Management Center から設定できるのは、インターフェイスのセキュリティ ゾーンのみです。

ASA FirePOWER インターフェイスを完全に設定するには、ASA 専用ソフトウェアおよび CLI を使用します。ASA FirePOWER およびスイッチを編集して、マルチ コンテキスト モードからシングル コンテキスト モード（またはその逆）に切り替えると、ASA FirePOWER はそのインターフェイスの名前をすべて変更します。ASA FirePOWER の更新されたインターフェイス名を使用するように、すべての Firepower System セキュリティ ゾーン、相関ルール、関連する設定を再設定する必要があります。ASA FirePOWER インターフェイスの設定の詳細については、ASA のマニュアルを参照してください。

（注） ASA FirePOWER インターフェイスのタイプは変更できません。また、Firepower Management Center からインターフェイスを無効にすることもできません。

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 インターフェイスを編集するデバイスの横にある編集アイコン（  ）をクリックします。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [インターフェイス（Interfaces）] タブが表示されていない場合は、そのタブをクリックします。

ステップ 4 編集するインターフェイスの横にある編集アイコン（  ）をクリックします。

ステップ 5 [セキュリティ ゾーン（Security Zone）] ドロップダウンリストから既存のセキュリティ ゾーンを選択するか、[新規（New）] を選択して新しいセキュリティ ゾーンを追加します。

ステップ 6 [保存（Save）] をクリックして、セキュリティ ゾーンを設定します。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

7000 および 8000 シリーズ デバイスおよび NGIPSv の MTU 範囲

デバイス上のすべての非管理インターフェイスの中で最大 MTU 値を変更し、設定変更を展開すると、Snort プロセスが再起動され、トラフィック インスペクションが一時的に中断されます。インスペクションは、変更したインターフェイスだけでなく、すべての非管理インターフェイスで中断されます。この中断によってトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびインターフェイスのタイプに応じて異なります。詳細については、「Snort® の再起動によるトラフィックの動作 （451 ページ）」を参照してください。

（注） システムは、設定された MTU 値から 18 バイトを切り捨てます。594 より小さい IPv4 MTU または 1298 より小さい IPv6 MTU を設定しないでください。

プラットフォーム	MTU 範囲
7000 & 8000 シリーズ	576 ～ 9234（管理インターフェイス） 576 ～ 10172（インライン セット、パッシブ インターフェイス） 576 ～ 9922（その他）
NGIPSv	576 ～ 9018（すべてのインターフェイス、インライン セット）

関連トピック

MTU について （827 ページ）

セキュリティ ゾーン オブジェクトのリビジョンの同期

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	7000 & 8000 シリーズ NGIPSv	リーフのみ	Admin/Network Admin

セキュリティ ゾーン オブジェクトを更新すると、システムはそのオブジェクトの新しいリビジョンを保存します。その結果、同じセキュリティ ゾーン内の管理対象デバイスに、インター

フェイスで設定されたセキュリティ オブジェクトの異なるリビジョンがある場合、接続が重複しているようなログが記録される可能性があります。

接続の重複が報告されていることに気づいた場合、同じリビジョンのオブジェクトを使用するよう、すべての管理対象デバイスを更新できます。

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 セキュリティ ゾーンの選択を更新するデバイスの横にある編集アイコン（  ）をクリックします。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

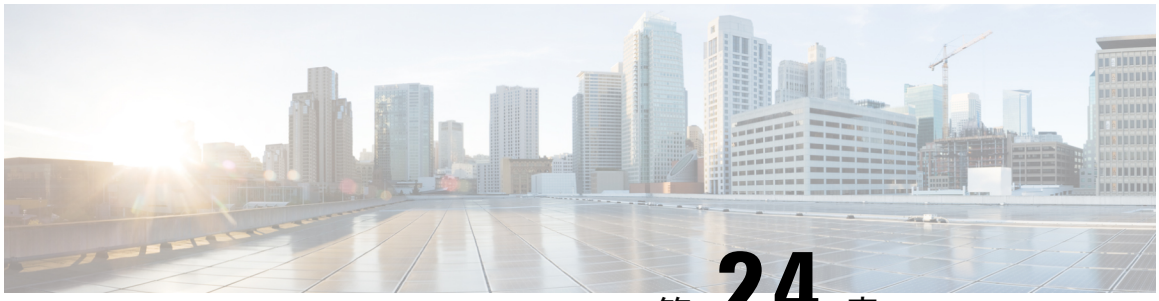
ステップ 3 重複する接続のイベントを記録しているインターフェイスのそれぞれについて、[セキュリティ ゾーン（Security Zone）] を別のゾーンに変更して [保存（Save）] をクリックした後、目的のゾーンに再び設定し、もう一度 [保存（Save）] をクリックします。

ステップ 4 重複イベントを記録しているデバイスごとに、ステップ 2 から 3 を繰り返します。続行する前に、すべてのデバイスを編集する必要があります。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

注意 Do not deploy configuration changes to any device until you edit the zone setting for interfaces on *all* devices you want to sync. すべての管理対象デバイスに同時に展開する必要があります。



第 24 章

IPS デバイスの展開と設定

以下のトピックでは、IPS 展開でデバイスを設定する方法について説明します。

IPS デバイスの展開と設定の概要

パッシブまたはインラインのいずれかの IPS 展開でデバイスを設定できます。パッシブ展開では、ネットワーク トラフィックのフローからアウトオブバンドでシステムを展開します。インライン展開では、2つのポートを一緒にバインドすることで、ネットワーク セグメント上でシステムを透過的に設定します。

パッシブ IPS 展開

パッシブ（受動）IPS 展開では、Firepower システムはスイッチ SPAN またはミラー ポートを使用してネットワークを流れるトラフィックをモニタします。SPAN またはミラー ポートでは、スイッチ上の他のポートからトラフィックをコピーできます。これにより、ネットワーク トラフィックのフローに含まれなくても、ネットワークでのシステムの可視性が備わります。パッシブ展開で構成されたシステムでは、特定のアクション（トラフィックのブロッキングやシェーピングなど）を実行することができません。パッシブ インターフェイスはすべてのトラフィックを無条件で受信します。このインターフェイスで受信されたトラフィックは再送されません。

（注） アウトバウンド トラフィックにはフロー制御パケットが含まれています。そのため、アプライアンスのパッシブ インターフェイスにアウトバウンド トラフィックが表示されることがあり、設定によっては、イベントが生成されることもあります。これは正常な動作です。

Firepower システムのパッシブ インターフェイス

管理対象デバイス上の 1 つ以上の物理ポートをパッシブ インターフェイスとして設定できます。

パッシブインターフェイスがトラフィックをモニタすることを可能にする場合、銅線インターフェイスでのみ使用可能なモードおよび MDI/MDIX 設定を指定します。8000 シリーズ アプライアンスのインターフェイスは、半二重オプションをサポートしません。

パッシブインターフェイスを無効にする場合、ユーザはセキュリティのためにアクセスできなくなります。

MTU 値の範囲は管理対象デバイスのモデルとインターフェイス タイプによって異なる場合があります。

⚠

注意 デバイス上のすべての非管理インターフェイスの中で最大 MTU 値を変更し、設定変更を展開すると、Snort プロセスが再起動され、トラフィック インスペクションが一時的に中断されます。インスペクションは、変更したインターフェイスだけでなく、すべての非管理インターフェイスで中断されます。この中断によってトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびインターフェイスのタイプに応じて異なります。詳細については、「Snort® の再起動によるトラフィックの動作 （451 ページ）」を参照してください。

関連トピック

7000 および 8000 シリーズ デバイスおよび NGIPSv の MTU 範囲 （661 ページ）
Snort® の再起動シナリオ （450 ページ）

パッシブ インターフェイスの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	機能に応じて異なる	リーフのみ	Admin/Network Admin

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 パッシブ インターフェイスを設定するデバイスの横にある編集アイコン（✎）をクリックします。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 パッシブインターフェイスとして設定するインターフェイスの横にある編集アイコン（✎）をクリックします。

ステップ 4 [パッシブ（Passive）] をクリックします。

ステップ 5 セキュリティ ゾーンにパッシブ インターフェイスを関連付けるには、次のいずれかを実行します。

- [セキュリティ ゾーン（Security Zone）] ドロップダウン リストから既存のセキュリティ ゾーンを選択します。
- [新規（New）] を選択して新しいセキュリティ ゾーンを追加します。セキュリティ ゾーンおよびインターフェイス グループ オブジェクトの作成 （536 ページ） を参照してください。

ステップ 6 [有効（Enabled）] チェックボックスをオンにします。

このチェックボックスをオフにすると、インターフェイスは無効になり、ユーザはセキュリティ上の理由によりアクセスできなくなります。

ステップ 7 7000 & 8000 シリーズのみ：[モード（Mode）] ドロップダウン リストからリンク モードを指定するか、または [自動ネゴシエーション（Auto Negotiation）] を選択して、速度とデュプレックス設定を自動的にネゴシエートするようにインターフェイスを設定します。

モード設定は銅線インターフェイスにのみ使用できます。

8000 シリーズ アプライアンスのインターフェイスは、半二重オプションをサポートしません。

ステップ 8 7000 & 8000 シリーズのみ：[MDI/MDIX] ドロップダウン リストから、インターフェイスの設定対象として MDI（メディア依存型インターフェイス）、MDIX（メディア依存型インターフェイス クロスオーバー）、または自動 MDIX のいずれかを指定します。

[MDI/MDIX] 設定は銅線インターフェイスでのみ使用できます。

デフォルトでは、[MDI/MDIX] は [自動 MDIX（Auto-MDIX）] に設定され、MDI と MDIX の間の切り替えを自動的に処理してリンクを確立します。

ステップ 9 [MTU] フィールドに最大伝送ユニット（MTU）を入力します。

MTU 値の範囲は管理対象デバイスのモデルとインターフェイス タイプによって異なる場合があります。

注意 デバイス上のすべての非管理インターフェイスの中で最大MTU値を変更し、設定変更を展開すると、Snortプロセスが再起動され、トラフィック インスペクションが一時的に中断されます。インスペクションは、変更したインターフェイスだけでなく、すべての非管理インターフェイスで中断されます。この中断によってトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびインターフェイスのタイプに応じて異なります。詳細については、「Snort® の再起動によるトラフィックの動作 （451 ページ）」を参照してください。

ステップ 10 **[保存（Save）]** をクリックします。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

インライン IPS 展開

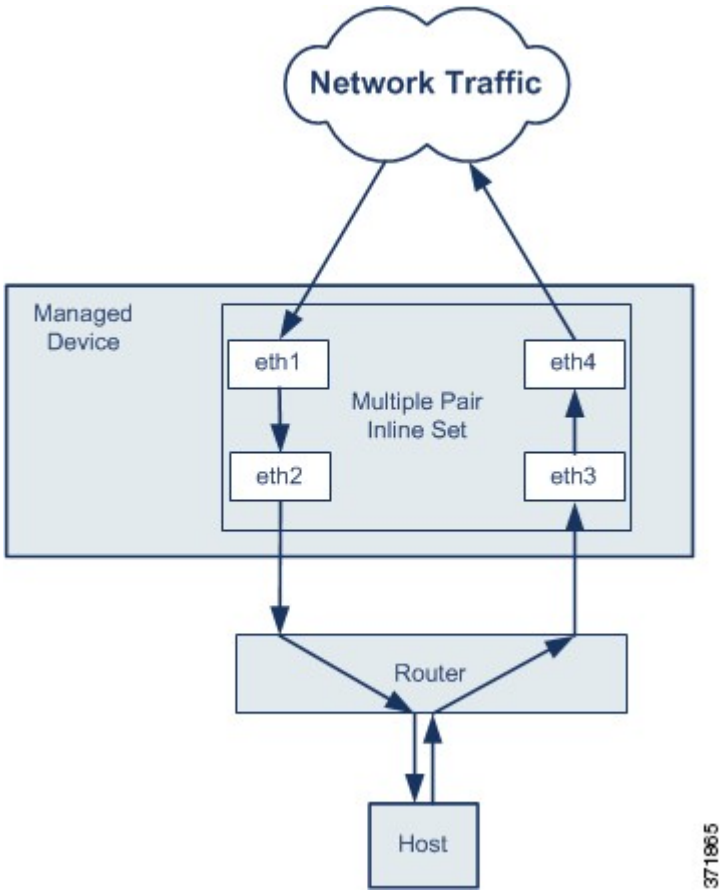
インライン IPS 展開では、2 つのポートを一緒にバインドすることで、ネットワーク セグメント上で Firepower システムを透過的に設定します。これによって、隣接するネットワーク デバイスの設定がなくても、任意のネットワーク環境にシステムをインストールできます。インライン インターフェイスはすべてのトラフィックを無条件に受信しますが、これらのインターフェイスで受信されたすべてのトラフィックは、明示的にドロップされない限り、インラインセットの外部に再送信されます。

（注） システムがトラフィックに影響を与えるためには、ルーテッド、スイッチド、トランスペアレント インターフェイスまたはインライン インターフェイスのペアを使用して関連する設定を管理対象デバイスに展開する必要があります。

デバイス トラフィックがインバウンドであるかアウトバウンドであるかに応じて、異なるインライン インターフェイス ペアを介してネットワーク上のホストと外部ホスト間のトラフィックをルーティングするように、管理対象デバイスのインターフェイスを設定できます。これは非同期ルーティング設定です。非同期ルーティングを展開し、インラインセットに 1 つのインターフェイス ペアしか含めないと、デバイスがトラフィックの半分しか認識しないため、ネットワーク トラフィックが適切に分析されない可能性があります。

同じインライン インターフェイス セットに複数のインライン インターフェイス ペアを追加すると、システムが着信トラフィックと発信トラフィックを同じトラフィック フローの一部として識別できるようになります。パッシブ インターフェイスでのみ、同じセキュリティ ゾーンにインターフェイス ペアを含めることによっても実現できます。

非同期ルーティング構成を通過するトラフィックから接続イベントが生成された場合、そのイベントは同じインライン インターフェイス ペアの入力インターフェイスと出力インターフェイスを識別できます。たとえば、次の図の構成では、**eth3** を入力インターフェイス、**eth2** を出力インターフェイスとして識別する接続イベントが生成されます。これは、この構成の予期される動作です。



（注） 単一のインライン インターフェイス セットに複数のインターフェイス ペアを割り当てたときに、重複トラフィックの問題が発生した場合は、システムがパケットを一意に識別できるように再設定します。たとえば、別のインライン セットにインターフェイス ペアを再度割り当てるか、セキュリティ ゾーンを変更できます。

インラインセットを使用するデバイスでは、デバイス再起動後にパケットを転送するようソフトウェアブリッジが自動的にセットアップされます。デバイスが再起動しているときには、実行中のソフトウェア ブリッジがありません。インライン セットでパイパス モードを有効にすると、デバイスの再起動中にハードウェアバイパスになります。その場合、システムが停止して再起動する際に、デバイスとのリンクの再ネゴシエーションが原因で数秒間のパケットが失われる可能性があります。ただし、Snort の再起動中にシステムはトラフィックを通過させます。

関連トピック

7000 および 8000 シリーズ デバイスおよび NGIPSv の MTU 範囲 （661 ページ）
Snort® の再起動シナリオ （450 ページ）

Firepower システムのインライン インターフェイス

管理対象デバイス上の1つ以上の物理ポートをインラインインターフェイスとして設定できます。インラインインターフェイスがインライン展開環境のトラフィックを処理するには、その前に、インラインインターフェイスのペアをインラインセットに割り当てる必要があります。

（注）

- インライン ペアのインターフェイスをそれぞれ異なる速度に設定した場合、またはインターフェイスが異なる速度にネゴシエートされる場合は、システムによって警告が出されます。
- インターフェイスをインラインインターフェイスとして設定すると、そのインターフェイスの NetMod 上の隣接ポートも自動的にインラインインターフェイスとなり、インラインインターフェイスのペアが完成します。
- NGIPSv デバイスでインライン インターフェイスを設定するには、隣接するインターフェイスを使用してインライン ペアを作成する必要があります。

インライン インターフェイスの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	機能に応じて異なる	リーフのみ	Admin/Network Admin

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 インターフェイスを設定するデバイスの横にある編集アイコン（  ）をクリックします。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 設定するインターフェイスの横にある編集アイコン（  ）をクリックします。

ステップ 4 [インライン（Inline）] をクリックします。

ステップ 5 インラインインターフェイスをセキュリティ ゾーンと関連付ける場合は、次のいずれかを実行します。

- [セキュリティ ゾーン（Security Zone）] ドロップダウン リストから既存のセキュリティ ゾーンを選択します。
- [新規（New）] を選択して新しいセキュリティ ゾーンを追加します。セキュリティ ゾーンおよびインターフェイス グループ オブジェクトの作成 （536 ページ） を参照してください。

ステップ 6 [インラインセット（Inline Set）] ドロップダウン リストから既存のインラインセットを選択するか、[新規（New）] を選択して新しいインライン セットを追加します。

（注） 新しいインラインセットを追加する場合は、インラインインターフェイスを設定した後、設定する必要があります。インライン セットの追加 （672 ページ）を参照してください。

ステップ 7 [有効（Enabled）] チェックボックスをオンにします。

このチェックボックスをオフにすると、インターフェイスは無効になり、ユーザはセキュリティ上の理由によりアクセスできなくなります。

ステップ 8 7000 & 8000 シリーズのみ：[モード（Mode）] ドロップダウン リストからリンク モードを指定するか、または [自動ネゴシエーション（Auto Negotiation）] を選択して、速度とデュプレックス設定を自動的にネゴシエートするようにインターフェイスを設定します。

モード設定は銅線インターフェイスにのみ使用できます。

8000 シリーズ アプライアンスのインターフェイスは、半二重オプションをサポートしません。

ステップ 9 7000 & 8000 シリーズのみ：[MDI/MDIX] ドロップダウン リストから、インターフェイスの設定対象として MDI（メディア依存型インターフェイス）、MDIX（メディア依存型インターフェイス クロスオーバー）、または自動 MDIX のいずれかを指定します。

[MDI/MDIX] 設定は銅線インターフェイスでのみ使用できます。

デフォルトでは、[MDI/MDIX] は [自動 MDIX（Auto-MDIX）] に設定され、MDI と MDIX の間の切り替えを自動的に処理してリンクを確立します。

ステップ 10 **[保存（Save）]** をクリックします。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

Firepower システムのインライン セット

インライン展開でインライン インターフェイスを使用するには、事前に、インライン セットを設定してインライン インターフェイス ペアをそれらに割り当てる必要があります。インライン セットは、デバイス上の 1 つ以上のインライン インターフェイス ペアからなるグループです。インライン インターフェイス ペアは、一度に 1 つのインライン セットにのみ属することができます。

[Device Management] ページの [Inline Sets] タブには、デバイスに設定されているすべてのインライン セットのリストが表示されます。

[デバイスの管理（Device Management）] ページの [インライン セット（Inline Sets）] タブからインライン セットを追加できます。または、インライン インターフェイスを設定するときにインライン セットを追加できます。

インライン セットにはインライン インターフェイス ペア**のみ**を割り当てることができます。管理対象デバイスでインライン インターフェイスを設定する前にインライン セットを作成す

る必要がある場合は、空のインラインセットを作成し、後からそれにインターフェイスを追加できます。インライン セットの名前を入力する場合は、英数字とスペースを使用できます。

（注） インラインセットでインターフェイスのセキュリティゾーンを追加する前に、インラインセットを作成します。作成しない場合、セキュリティゾーンが削除されるため再度追加する必要があります。

名前

インライン セットの名前。

インターフェイス

インライン セットに割り当てられているすべてのインライン ペアのリスト。[Interfaces] タブでペアのいずれかのインターフェイスを無効にした場合、そのペアは含まれません。

MTU

インライン セットの最大伝送ユニット。 MTU 値の範囲は管理対象デバイスのモデルとインターフェイス タイプによって異なる場合があります。

注意 デバイス上のすべての非管理インターフェイスの中で最大 MTU 値を変更し、設定変更を展開すると、Snort プロセスが再起動され、トラフィック インスペクションが一時的に中断されます。インスペクションは、変更したインターフェイスだけでなく、すべての非管理インターフェイスで中断されます。この中断によってトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびインターフェイスのタイプに応じて異なります。詳細については、「Snort® の再起動によるトラフィックの動作 （451 ページ）」を参照してください。

[フェールセーフ（Failsafe）]

Snort プロセスがビジー状態またはダウンしている場合の、7000 または 8000 シリーズ または NGIPSv デバイス上のインターフェイスの動作。

- [有効（Enabled）]：Snort プロセスがビジー状態またはダウンしている場合、新規または既存のフローをインスペクションなしで受け渡します。
- [無効（Disabled）]：Snort プロセスがビジー状態の場合は、新規および既存のフローをドロップし、Snort プロセスがダウンしている場合はフローをインスペクションなしで受け渡します。

トラフィック バッファが満杯の場合、Snortプロセスがビジー状態のことがあります。つまり、管理対象デバイスが処理可能な量を超えたトラフィックが存在するか、またはその他のソフトウェアに問題があることを示しています。

Snort プロセスを再起動する必要がある設定を展開すると、Snort プロセスはダウンします。詳細については、「展開またはアクティブ化された際に Snort プロセスを再起動する設定 （454 ページ）」を参照してください。

（注） インスペクションを実行せずにトラフィックを受け渡す場合は、Snort プロセスに依存している機能は動作しません。そのような機能には、アプリケーション制御とディープ インスペクションが含まれます。システムでは、シンプルかつ容易に判断できるトランスポート層とネットワークの特性を使用して、基本的なアクセス コントロールのみ実行されます。

Bypass Mode

Firepower 7000 または 8000 シリーズ のみ：インライン セットの設定済みバイパス モード。この設定により、インターフェイスに障害が発生した場合のインライン インターフェイスのリレーの応答方法が決まります。バイパスモードは、トラフィックがインターフェイスを通過し続けることを許可します。非バイパス モードでは、トラフィックがブロックされます。

注意 バイパス モードでは、アプライアンスのリブート時に少数のパケットが失われることがあります。ハイ アベイラビリティ ペアの 7000 または 8000 シリーズ デバイスのインライン セット、8000 シリーズ デバイスの非バイパス NetMod、Firepower 7115 または 7125 デバイスの SFP モジュールには、バイパス モードを設定できません。

関連トピック

7000 および 8000 シリーズ デバイスおよび NGIPSv の MTU 範囲 （661 ページ）
Snort® の再起動シナリオ （450 ページ）

インライン セットの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Network Admin

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 インライン セットを表示するデバイスの横にある編集アイコン（）をクリックします。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [インライン セット（Inline Sets）] タブをクリックします。

インライン セットの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	機能に応じて異なる	リーフのみ	Admin/Network Admin

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 インライン セットを追加するデバイスの横にある編集アイコン（）をクリックします。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [インライン セット（Inline Sets）] タブをクリックします。

ステップ 4 [Add Inline Set] をクリックします。

ステップ 5 [名前（Name）] を入力します。

ステップ 6 [インターフェイス（Interfaces）] の横で、1 つ以上のインライン インターフェイス ペアを選択し、選択項目の追加アイコン（）をクリックします。すべてのインターフェイス ペアをインライン セットに追加するには、「すべてを追加」アイコン（）をクリックします。

ヒント インライン セットからインライン インターフェイスを削除するには、1 つ以上のインライン インターフェイス ペアを選択して、選択項目の削除アイコン（）をクリックします。インライン セットからすべてのインターフェイス ペアを削除するには、「すべてを削除」アイコン（）をクリックします。また、[インターフェイス（Interfaces）] タブでペアのいずれかのインターフェイスを無効にすると、ペアが削除されます。

ステップ 7 [MTU] フィールドに最大伝送ユニット（MTU）を入力します。

MTU 値の範囲は管理対象デバイスのモデルとインターフェイス タイプによって異なる場合があります。

注意 デバイス上のすべての非管理インターフェイスの中で最大MTU値を変更し、設定変更を展開すると、Snortプロセスが再起動され、トラフィック インスペクションが一時的に中断されます。インスペクションは、変更したインターフェイスだけでなく、すべての非管理インターフェイスで中断されます。この中断によってトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびインターフェイスのタイプに応じて異なります。詳細については、「Snort® の再起動によるトラフィックの動作 （451 ページ）」を参照してください。

ステップ 8 Snortプロセスが取り込み中またはダウンしているときに検出をバイパスさせ、デバイスにトラフィックを通すには、[フェールセーフ（Failsafe）] を選択します。 詳細については、Firepower システムのインライン セット （669 ページ）を参照してください。

内部トラフィック バッファがいっぱいになったが、特定の状況下でデバイスがまだパケットをドロップする可能性がある場合は、インライン セットでデバイスの [フェールセーフ（Failsafe）] を有効にする

と、ドロップされたパケットのリスクが大幅に軽減されます。最悪の場合は、デバイスで一時的にネットワークが停止することがあります。

ステップ 9 （7000/8000 シリーズのみ）バイパスモードを指定します。

- トラフィックがインターフェイスを通過し続けることを許可するには、[バイパス（Bypass）] をクリックします。
- トラフィックをブロックするには、[バイパスしない（Non-Bypass）] をクリックします。

（注） 高可用性ペアの 7000 または 8000 シリーズ デバイスのインライン セット、NGIPSv デバイスのインライン セット、8000 シリーズ デバイスの非バイパス ネットワーク モジュール、Firepower 7115 または 7125 デバイスの SFP モジュールには、バイパス モードを設定できません。

ステップ 10 必要に応じて、詳細な設定を行います。インライン セットの詳細オプション （673 ページ） を参照してください。

ステップ 11 [OK] をクリックします。

次のタスク

設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

関連トピック

7000 および 8000 シリーズ デバイスおよび NGIPSv の MTU 範囲 （661 ページ）
Snort® の再起動シナリオ （450 ページ）

インライン セットの詳細オプション

インライン セットを設定する際に考慮できる詳細オプションがいくつかあります。

タップ モード

7000および8000シリーズデバイスでは、インライン（またはフェール オープン可能なインライン）インターフェイス セットを作成するときにタップ モードを使用できます。

タップモードの場合、デバイスはインラインで展開されますが、パケットがデバイスを通過する代わりに各パケットのコピーがデバイスに送信され、ネットワーク トラフィック フローは影響を受けません。パケット自体ではなくパケットのコピーを処理するため、ドロップするように設定したルール、および置換キーワードを使用するルールはパケット ストリームに影響を与えません。ただし、これらのタイプのルールでは、トリガーされた侵入イベントが生成され、侵入イベントのテーブル ビューには、トリガーの原因となったパケットがインライン展開でドロップされたことが示されます。

インライン展開されたデバイスでタップモードを使用することには、利点があります。たとえば、デバイスがインラインであるかのようにデバイスとネットワークの間の配線をセットアップし、デバイスが生成するタイプの侵入イベントを分析することができます。その結果に基づいて、効率性に影響を与えることなく最適なネットワーク保護を提供するように、侵入ポリシーを変更して廃棄ルールを追加できます。デバイスをインラインで展開する準備ができた

ら、タップ モードを無効にして、デバイスとネットワークの間の配線を再びセットアップすることなく、不審なトラフィックをドロップし始めることができます。

ただし、同じインライン セットに対してこのオプションと厳格な TCP 強制を有効にすることはできません。

リンク ステートの伝達（Propagate Link State）

（注） リンク ステートの伝達は、バーチャル デバイスではサポートされていません。リンク ステートの伝達は 7000 および 8000 シリーズ デバイスのみでサポートされています。

リンク ステートの伝達は、インライン セットのペアの両方で状態を追跡できるよう、バイパス モードと非バイパス モードで設定されるインライン セットの機能です。リンク ステートの伝達は、銅線と光ファイバの両方の設定可能なバイパス インターフェイスで使用できます。

リンク ステートの伝達によって、インライン セットのインターフェイスの 1 つが停止した場合、インライン インターフェイス ペアの 2 番目のインターフェイスも自動的に停止します。停止したインターフェイスが再び起動すると、2 番目のインターフェイスも自動的に起動します。つまり、1 つのインターフェイスのリンク ステートが変化すると、アプライアンスはその変化を検知し、それに合わせて他のインターフェイスのリンク ステートを更新します。ただし、アプライアンスがリンク ステートの変更を伝達するのに最大 4 秒かかります。

リンク ステートの伝達は、ルータが障害状態のネットワーク デバイスを避け、トラフィックを自動的に再ルーティングするよう設定された、復元力の高いネットワーク環境では特に有効です。

高可用性ペアの 7000 および 8000 シリーズ デバイスで設定されたインライン セットのリンク ステートの伝達を無効にすることはできません。

トランスペアレント インライン モード（Transparent Inline Mode）

[トランスペアレント インライン モード（Transparent Inline Mode）] オプションを使用すると、デバイスを「Bump In The Wire」として機能させることができます。つまり、デバイスは、送信元と宛先に関係なく、認識するすべてのネットワーク トラフィックを転送するということです。7000 および 8000 シリーズ デバイスではこのオプションを無効にできません。

厳密な TCP の適用

（注） 厳密な TCP 適用は、バーチャル デバイスではサポートされていません。7000 および 8000 シリーズ デバイスでのみ、このオプションを使用できます。また、同じインライン セットで、このオプションとタップ モードを有効にすることはできません。

最大限の TCP セキュリティを実現するため、厳格な強制を有効にすることができます。この機能は、3 ウェイ ハンドシェイクが完了していない接続をブロックします。厳密な適用では次のパケットもブロックされます。

- 3 ウェイ ハンドシェイクが完了していない接続の非 SYN TCP パケット
- 応答側が SYN-ACK を送信する前に TCP 接続の発信側から送信された非 SYN/RST パケット
- SYN の後ではあるがセッションの確立前に TCP 接続の応答側から送信された非 SYN-ACK/RST パケット
- 発信側または応答側のどちらかから送信された、確立された TCP 接続の SYN パケット

高度なインライン セット オプションの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	機能に応じて異なる	リーフのみ	Admin/Network Admin

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 インライン セットを編集するデバイスの横にある編集アイコン（  ）をクリックします。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [インライン セット（Inline Sets）] タブをクリックします。

ステップ 4 編集するインライン セットの横にある編集アイコン（）をクリックします。

ステップ 5 [Advanced] タブをクリックします。

ステップ 6 インライン セットの詳細オプション （673 ページ）の説明に従ってオプションを設定します。

（注） リンク ステートの伝達と厳密な TCP 適用は、仮想デバイスではサポートされていません。

ステップ 7 [OK] をクリックします。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

インライン セットの削除

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	リーフのみ	Admin/Network Admin

インライン セットを削除すると、そのセットに割り当てられたインライン インターフェイスを別のセットに含めることができるようになります。それらのインターフェイスは削除されません。

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 インライン セットを削除するデバイスの横にある編集アイコン（  ）をクリックします。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [インライン セット（Inline Sets）] タブをクリックします。

ステップ 4 削除するインライン セットの横にある削除アイコン（  ）をクリックします。

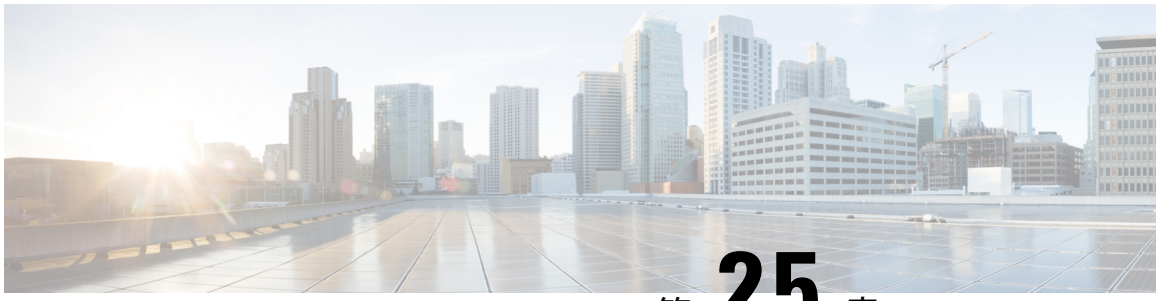
ステップ 5 プロンプトが表示されたら、インライン セットを削除することを確認します。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

第 VI 部

クラシック デバイスのハイ アベイラビリティと拡張性



第 25 章

7000 および 8000 シリーズ デバイスのハイ アベイラビリティ

次の各トピックでは、Firepower システムにおける Firepower 7000 シリーズおよび 8000 シリーズ デバイスのハイ アベイラビリティの設定方法について説明します。

7000 および 8000 シリーズ デバイスのハイ アベイラビリティについて

7000 および 8000 シリーズ デバイス ハイ アベイラビリティを利用することで、2 つのピア デバイス間または 2 つのピア デバイス スタック間のネットワーキング機能と設定データの冗長性を確保できます。

2 つのピア デバイスまたは 2 つのピア デバイス スタックを、ポリシーの展開、システムの更新、登録を行う単一の論理システムとして機能するハイ アベイラビリティ ペアとして構成することにより、構成の冗長性を実現できます。その他の設定データは、システムによって自動的に同期されます。

（注） スタティック ルート、非 SFRP IP アドレス、およびルーティングの優先順位は、ピア デバイスまたはピア デバイス スタック間で同期されません。各ピア デバイスまたはピア デバイス スタックは、独自のルーティング インテリジェンスを維持します。

関連トピック

SFRP
仮想スイッチの詳細設定 （1577 ページ）

デバイスのハイ アベイラビリティ要件

7000 および 8000 シリーズ デバイスのハイ アベイラビリティ ペアを構成するには、以下に従う必要があります。

- 単一デバイスと単一デバイスのペア、またはデバイス スタックとデバイス スタックのペアのみを構成できます。
- 両方のデバイスまたはデバイス スタックが正常なヘルス ステータスであり、同じソフトウェアを実行し、同じライセンスが有効になっている必要があります。詳細については、ヘルス モニタの使用 （371 ページ）を参照してください。特に、デバイスでのハードウェア障害は許容されません。ハードウェア障害が発生すると、デバイスがメンテナンス モードに入り、フェールオーバーがトリガーされます。

  （注） デバイスのペアを構成した後は、ペアを構成する個々のデバイスのライセンス オプションを変更することはできませんが、ハイ アベイラビリティ ペア全体のライセンスは変更できます。

- 各デバイスまたはスタック内の各プライマリ デバイスにインターフェイスを設定する必要があります。
- 両方のデバイスまたはデバイス スタックのプライマリ メンバーが同じモデルである必要があり、銅ケーブルまたは光ファイバの同じインターフェイスが必要です。
- デバイス スタックのハードウェア構成は同一でなければなりませんが、インストール済みのマルウェア ストレージ パックについてはその限りではありません。たとえば、Firepower 8290 と別の 8290 のペアを構成することができます。どちらかのスタック内でマルウェア ストレージ パックが、どのデバイスに存在しなくても、1 つのデバイスにのみ、またはすべてのデバイスに存在しても構いません。

注意 Cisco から供給されたハード ドライブ以外はデバイスに取り付けないでください。サポートされていないハード ドライブを取り付けると、デバイスが破損する可能性があります。マルウェア ストレージ パック キットは、シスコから**のみ**購入でき、8000 シリーズ デバイスで**のみ**使用できます。マルウェア ストレージ パックのサポートが必要な場合は、サポートにお問い合わせください。詳細については、*Firepower System Malware Storage Pack Guide*を参照してください。

- デバイスが NAT ポリシーのターゲットとなっている場合、両方のピアに同じ NAT ポリシーを適用する必要があります。
- マルチドメイン展開では、7000 または 8000 シリーズ デバイスのハイ アベイラビリティまたはリーフ ドメイン内のデバイス スタックのみを確立できます。

（注） フェールオーバーとリカバリの後に、SFRP はマスター ノードにプリエンプション処理します。

デバイスハイアベイラビリティフェールオーバーとメンテナンスモード

7000 および 8000 シリーズ デバイス ハイ アベイラビリティのフェールオーバーは、手動または自動で行われます。手動でフェールオーバーをトリガーするには、ペアを構成するデバイスまたはスタックのいずれかでメンテナンス モードを開始します。

自動フェールオーバーは、アクティブ デバイスまたはアクティブ スタックの正常性が損なわれた場合、システム更新時、または管理者権限によりデバイスがシャットダウンされた場合に発生します。また、自動フェールオーバーは、アクティブ デバイスまたはデバイス スタックで NMSB 障害、NFE 障害、ハードウェア障害、ファームウェア障害、重大なプロセス障害、ディスク フル エラー、または 2 つのスタック構成のデバイス間のリンク障害が起きた場合にも発生します。スタンバイのデバイスまたはスタックの正常性がアクティブデバイス同様に損なわれている場合は、フェールオーバーは行われず、クラスタは縮退状態になります。また、いずれかのデバイスまたはデバイス スタックがメンテナンス モードになっている場合も、フェールオーバーは行われません。アクティブ スタックからスタック ケーブルを切断すると、そのスタックはメンテナンス モードに入ることに注意してください。アクティブ スタックのセカンダリ デバイスをシャットダウンした場合も、スタックはメンテナンス モードに入ります。

（注） ハイ アベイラビリティ ペアのアクティブなメンバーがメンテナンス モードになり、アクティブ ロールが他のペア メンバーにフェールオーバーされた場合、元のアクティブ ペアのメンバーは、通常動作に復帰したときに自動的にアクティブ ロールを再要求しません。

ハイ アベイラビリティ ペアの設定展開とアップグレードの動作

このトピックでは、ハイ アベイラビリティ ペアでの 7000 および 8000 シリーズ デバイス（およびスタック）のアップグレードと展開の動作について説明します。

展開時の動作

ハイ アベイラビリティ ペアのメンバーに同時に設定の変更を展開します。展開は、両方のピアについて成功するか失敗するかのいずれかです。Firepower Management Center は、アクティブ デバイスに展開します。この展開に成功すると、次に変更がスタンバイに展開されます。

注意 展開する際にリソースを要求すると、いくつかのパケットがインスペクションなしでドロップされることがあります。また、一部のコンフィギュレーションを展開すると、トラフィックのインスペクションを中断する Snort プロセスが再開します。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、ターゲット デバイスがトラフィックを処理する方法に応じて異なります。Snort® の再起動によるトラフィックの動作（451 ページ）および展開またはアクティブ化された際に Snort プロセスを再起動する設定（454 ページ）を参照してください。

アップグレード時の動作

ハイ アベイラビリティ ペアのデバイス（またはデバイス スタック）をアップグレードする間に、トラフィック フローまたはインスペクションが中断されることはありません。継続稼働できるように、一度に 1 つずつアップグレードされます。アップグレード中、デバイスはメンテナンス モードで稼働します。

最初にアップグレードするピアは、展開によって異なります。

- ルーテッドまたはスイッチド：最初にスタンバイをアップグレードします。デバイスの役割が切り替わり、新しくスタンバイになったデバイスがアップグレードされます。アップグレードの完了時には、デバイスの役割は切り替わったままです。アクティブ/スタンバイの役割を維持する場合、アップグレード前に役割を手動で切り替えます。それにより、アップグレード プロセスによって元の役割に切り替わります。
- アクセス制御のみ：最初にアクティブをアップグレードします。アップグレードの完了時に、アクティブとスタンバイの以前の役割がデバイスで維持されます。

展開タイプとデバイス ハイ アベイラビリティ

7000 または 8000 シリーズ デバイスのハイ アベイラビリティ構成は、Firepower システム展開（パッシブ、インライン、ルーテッド、またはスイッチド）に応じて決定します。同時に複数のロールを持たせてシステムを展開することもできます。4つの展開タイプのうち、ハイ アベイラビリティを用いた冗長性をもたらすためにデバイスまたはスタックの構成が必要になるのは、パッシブ展開のみです。他の展開タイプでは、デバイス ハイ アベイラビリティを使用しても使用しなくてもネットワークの冗長性を確立できます。各展開タイプにおけるハイ アベイラビリティの概要については、以降の各項を参照してください。

（注） レイヤ 3 の冗長性については、デバイス ハイ アベイラビリティを使わずに、Cisco Redundancy Protocol（SFRP）により実現できます。SFRP では、指定した IP アドレスに対する冗長なゲートウェイとしてデバイスを機能させることができます。ネットワークの冗長性では、2 つのデバイスまたは 2 つのスタックが同一のネットワーク接続を提供するように設定することで、ネットワーク上の他のホストに対する接続を維持できます。

パッシブ展開での冗長性

一般に、パッシブ インターフェイスは中央スイッチのタップ ポートに接続されます。この場合、スイッチを通過するトラフィックのすべてを、パッシブ インターフェイスで分析することが可能になります。複数のデバイスが同じタップ フィードに接続されている場合、システムはそれぞれのデバイスからイベントを生成します。ハイ アベイラビリティ ペアとして構成されているデバイスは、アクティブまたはスタンバイのいずれかとして機能するため、システムはシステム障害が発生したとしてもトラフィックを分析できると同時に、重複するイベントを防止できます。

インライン展開での冗長性

インライン セットは、自身を通過するパケットのルーティングを制御できないため、展開環境で常にアクティブになっていなければなりません。したがって、冗長性を確立できるかどうかは、外部システムがトラフィックを適切にルーティングするかどうかに依存します。冗長インライン セットは、7000 または 8000 シリーズ デバイスのハイ アベイラビリティを使用しても使用しなくても設定できます。

冗長インライン セットを展開するには、循環ルーティングを防止する一方で、トラフィックがインライン セットのいずれか1つだけを通過できるようにネットワーク トポロジーを設定します。インライン セットのいずれかで障害が発生すると、周辺ネットワーク インフラストラクチャがゲートウェイ アドレスへの接続が切断されたことを検出し、ルートを調整して冗長セット経由でトラフィックを送信します。

ルーテッド展開での冗長性

IP ネットワーク内のホストは、既知のゲートウェイ アドレスを使用して、トラフィックをさまざまなネットワークに送信する必要があります。ルーテッド展開で冗長性を確立するには、ルーテッド インターフェイスがゲートウェイ アドレスを共有し、そのアドレスに対するトラ

フィックを常に1つのインターフェイスだけが処理するようにしなければなりません。そのためには、仮想ルータで同じ数のIPアドレスを維持する必要があります。1つのインターフェイスがアドレスをアドバタイズします。そのインターフェイスがダウンすると、スタンバイインターフェイスがアドレスのアドバタイズを開始します。

ハイ アベイラビリティ ペアのメンバーではないデバイスでは、複数のルーティングされたインターフェイス間で共有するゲートウェイ IP アドレスの設定し、SFRP によって冗長性を確保します。SFRP は、7000 または 8000 シリーズ デバイスのハイ アベイラビリティを使用しても使用しなくても設定できます。また、OSPF や RIP などのダイナミック ルーティングを使用して冗長性を確保することもできます。

スイッチド展開での冗長性

スイッチド展開では、高度な仮想スイッチ設定の 1 つであるスパニング ツリー プロトコル（STP）を使用して冗長性を確保します。STP はブリッジ型ネットワーク トポロジを管理するプロトコルです。このプロトコルは、スタンバイ リンクを設定することなく、冗長リンクでスイッチドインターフェイスの自動スタンバイを行えるように設計されています。スイッチド展開でのデバイスは、STP に依存して、冗長インターフェイス間のトラフィックを管理します。同じブロードキャスト ネットワークに接続されている 2 つのデバイスは、STP によって計算されたトポロジに基づいてトラフィックを受信します。

（注） 7000 または 8000 シリーズ デバイスのハイ アベイラビリティ ペアに展開する予定の仮想スイッチを設定する際には、STP を有効にするよう強く推奨します。

デバイスのハイ アベイラビリティ設定

7000 または 8000 シリーズ デバイスのハイ アベイラビリティを確立する際には、デバイスまたはスタックのうちの一方をアクティブとして指定し、もう一方をスタンバイとして指定します。システムは、マージした設定を、ペア内のデバイスに適用します。競合が存在する場合、システムはアクティブとして指定されたデバイスまたはスタックの設定を適用します。

デバイスのペアを構成した後は、ペアを構成する個々のデバイスのライセンス オプションを変更することはできませんが、ハイ アベイラビリティ ペア全体のライセンスは変更できます。スイッチド インターフェイスまたはルーテッド インターフェイスで設定しなければならないインターフェイス属性がある場合、システムはハイ アベイラビリティ ペアを確立しますが、そのステータスを保留中に設定します。ユーザが必要な属性を設定した後、システムはハイ アベイラビリティ ペアを完成させて、正常なステータスに設定します。

ハイ アベイラビリティ ペアを確立した後、[デバイス管理（Device Management）]ページでは、ピア デバイスまたはスタックが単一のデバイスとして扱われます。デバイスのハイ アベイラビリティ ペアは、アプライアンス リストではハイ アベイラビリティ アイコン（  ）が表示されます。ユーザが行った設定変更は、いずれもペアを構成するデバイスの間で同期されます。[デバイス管理（Device Management）] ページには、ハイ アベイラビリティ ペアのどのデ

バイスまたはスタックがアクティブであるかが表示されます。アクティブなデバイスまたはスタックは、手動または自動フェールオーバーが発生すると変更されます。

デバイスのハイ アベイラビリティ ペアの登録を Firepower Management Center から削除すると、その登録は両方のデバイスまたはスタックから削除されます。デバイスのハイ アベイラビリティ ペアを Firepower Management Center から削除する方法は、個々の管理対象デバイスを削除する場合の方法と同じです。

登録が削除されたハイ アベイラビリティ ペアは、別の Firepower Management Center に登録できます。ハイ アベイラビリティ ペアを構成する一方のデバイスを登録するには、ペアのうちアクティブ デバイスにリモート管理を追加してから、そのデバイスを Firepower Management Center に追加します。これにより、ペア全体が追加されます。ハイ アベイラビリティ ペアのうちスタック構成のデバイスを登録するには、どちらか一方のスタックのプライマリ デバイスにリモート管理を追加してから、そのデバイスを Firepower Management Center に追加します。これにより、ペア全体が追加されます。

デバイスのハイ アベイラビリティ ペアを確立したら、ハイ アベイラビリティ リンク インターフェイスを設定する必要があります。

（注） ハイ アベイラビリティ ペアのデバイスを使用してダイナミック NAT、HA 状態共有、または VPN を設定する場合は、ハイ アベイラビリティ リンク インターフェイスを構成する必要があります。詳細については、「HA リンク インターフェイスの設定 （658 ページ）」を参照してください。

Firepower 7000/8000 シリーズ ハイ アベイラビリティの確立

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
該当なし	Control	7000 & 8000 シリーズ	任意（Any）	Admin/Network Admin

（注） この手順では、7000 & 8000 シリーズ デバイスのハイ アベイラビリティ ペアの確立について説明します。Firepower Threat Defense のハイ アベイラビリティの確立については、Firepower Threat Defense ハイ アベイラビリティ ペアの追加 （891 ページ）を参照してください。

7000 & 8000 シリーズ デバイスのハイ アベイラビリティ ペアを確立する際には、デバイスまたはスタックのうちの一方をアクティブとして指定し、もう一方をスタンバイとして指定します。システムは、マージした設定を、ペア内のデバイスに適用します。競合が存在する場合、システムはアクティブとして指定されたデバイスまたはスタックの設定を適用します。

マルチドメイン展開では、ハイ アベイラビリティ ペアのデバイスは同じドメインに属している必要があります。

始める前に

すべての要件が満たされていることを確認します。デバイスのハイ アベイラビリティ要件 （680 ページ）を参照してください。

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 [追加（Add）] ドロップダウン メニューから、[高可用性の追加（Add High Availability）] を選択します。

ステップ 3 名前を入力します。

ステップ 4 [デバイス タイプ（Device Type）] で [Firepower] を選択します。

ステップ 5 デバイスまたはスタックにロールを割り当てます。

a) [アクティブ ピア（Active Peer）] のデバイスまたはスタックをハイ アベイラビリティ ペア用に選択します。

b) [スタンバイ ピア（Standby Peer）] のデバイスまたはスタックをハイ アベイラビリティ ペア用に選択します。

ステップ 6 [追加（Add）]をクリックします。このプロセスではデータの同期が行われるため、プロセスが完了するまでに数分かかります。

次のタスク

HA 状態共有、ダイナミック NAT、または VPN をデバイスに設定する予定の場合は、高可用性ペアの各デバイスで HA リンク インターフェイスを作成します。HA リンク インターフェイスの詳細については、HA リンク インターフェイスの設定（658ページ）を参照してください。

デバイスのハイ アベイラビリティの編集

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
該当なし	Control	7000 & 8000 シリーズ	リーフのみ	Admin/Network Admin

7000 または 8000 シリーズ デバイスのハイ アベイラビリティ ペアを確立した後は、デバイス設定を変更すると、通常はハイ アベイラビリティ ペア全体の設定も変更されます。

[一般（General）] セクションのステータス アイコンにマウスのポインタを合わせると、ハイ アベイラビリティ ペアのステータスが表示されます。また、ペア内のデバイスまたはスタックのどれがアクティブ ピアで、どれがスタンバイ ピアであるかも確認できます。

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 設定を編集するデバイスのハイ アベイラビリティ ペアの横にある編集アイコン（  ）をクリックします。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [ハイ アベイラビリティ（High Availability）] ページのセクションを使用して、単一のデバイス設定を変更する場合と同じように、ハイ アベイラビリティ ペアの設定を変更します。

高可用性ペアの個々のデバイスの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
該当なし	Control	7000 & 8000 シリーズ	リーフのみ	Admin/Network Admin

7000 または 8000 シリーズ デバイスの高可用性ペアを確立した後でも、ペア内の個々のデバイスに対して設定できる属性がいくつかあります。ペアリングされたデバイスに変更を加える方法は、単一のデバイスに変更を加える場合の方法と同じです。

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 設定を編集するデバイスの高可用性ペアの横にある編集アイコン（）をクリックします。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [デバイス] タブをクリックします。

ステップ 4 [選択されたデバイス（Selected Device）] ドロップダウン リストから、変更するデバイスを選択します。

ステップ 5 [デバイス（Devices）] ページのセクションを使用して、単一のデバイスに対して変更を加える場合と同じように、ペアリングされた個々のデバイスに変更を加えます。

高可用性ペアの個々のデバイス スタックの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
該当なし	Control	Firepower 8140、Firepower 8200 ファミリ、Firepower 8300 ファミリ	リーフのみ	Admin/Network Admin

高可用性ペアにスタック構成の 8000 シリーズ デバイスを設定すると、編集可能なスタック属性が制限されます。ペアリングされたスタックの名前は編集できます。また、高可用性ペアのデバイスでのインターフェイスの設定（688 ページ）で説明している手順に従って、スタックのネットワーク設定を編集できます。

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 設定を編集するデバイスの高可用性ペアの横にある編集アイコン（  ）をクリックします。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [スタック（Stacks）] タブをクリックします。

ステップ 4 [選択されたデバイス（Selected Device）] ドロップダウン リストから、変更するスタックを選択します。

ステップ 5 [一般（General）] セクションの横にある編集アイコン（  ）をクリックします。

ステップ 6 [名前（Name）] を入力します。

ステップ 7 **[保存（Save）]** をクリックします。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

高可用性ペアのデバイスでのインターフェイスの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
該当なし	Control	7000 & 8000 シリーズ	リーフのみ	Admin/Network Admin

7000 または 8000 シリーズ デバイスの高可用性ペアの個々のデバイスに、インターフェイスを設定できます。ただし、その場合には、ペアのピア デバイスにも同等のインターフェイスを設定する必要があります。ペアリングされたスタックの場合は、スタックのプライマリ デバイスのそれぞれに、同じインターフェイスを設定する必要があります。仮想ルータを設定するときに、その仮想ルータを設定するスタックを選択します。

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 インターフェイスを設定するデバイスの高可用性ペアの横にある編集アイコン（  ）をクリックします。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [インターフェイス（Interfaces）] タブをクリックします。

ステップ 4 [選択されたデバイス（Selected Device）] ドロップダウン リストから、変更するデバイスを選択します。

ステップ 5 個々のデバイスに設定する場合と同じようにインターフェイスを設定します。

関連トピック

仮想ルータ設定 （1591 ページ）

デバイスのハイアベイラビリティペアにおけるアクティブ ピアの切り替え

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
該当なし	Control	7000 & 8000 シリーズ	任意（Any）	Admin/Network Admin

7000 または 8000 シリーズ デバイスのハイ アベイラビリティ ペアを確立した後、アクティブなピア デバイスまたはスタックをスタンバイに手動で切り替えることができます。

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 アクティブ ピアを変更するデバイスのハイ アベイラビリティ ペアの横にあるアクティブ ピア切り替えアイコン（  ）をクリックします。

ステップ 3 次の操作を実行できます。

- ハイ アベイラビリティ ペアでスタンバイ ピアをアクティブ ピアにすぐに切り替える場合は、[はい（Yes）] をクリックします。

- キャンセルして [デバイス管理（Device Management）] ページに戻る場合は、[いいえ（No）] をクリックします。

高可用性ピアのメンテナンス モードへの切り替え

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
該当なし	Control	7000 & 8000 シリーズ	任意（Any）	Admin/Network Admin

7000 または 8000 シリーズ デバイス高可用性ペアを設定した後で、デバイスのメンテナンスを実行するために、いずれかのピアをメンテナンス モードに切り替えることで、手動でフェールオーバーをトリガーできます。メンテナンス モードでは、システムが管理目的で管理インターフェイスを除くすべてのインターフェイスをダウンさせます。メンテナンスの完了後、ピアを再度有効にして、通常の動作を再開できます。

（注） 高可用性ペアの両方のピアを同時にメンテナンス モードにしないでください。これを行うと、そのペアではトラフィックを検査できなくなります。

ステップ 1 **[Devices]** > **[Device Management]** を選択します。

ステップ 2 メンテナンス モードを開始するピアの横にあるメンテナンス モード切り替えアイコン（）をクリックします。

ステップ 3 [はい（Yes）] をクリックして、メンテナンス モードを確定します。

次のタスク

- メンテナンスが完了したら、メンテナンス モード切り替えアイコン（）を再度クリックして、ピアのメンテナンス モードを終了します。

高可用性ペアのスタック内のデバイスの交換

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
該当なし	Control	Firepower 8140、8200 ファミリ、8300 ファミリ	任意（Any）	Admin/Network Admin

高可用性ペアのメンバーになっているスタックをメンテナンス モードに切り替えた後で、スタック内のセカンダリ デバイスを別のデバイスと交換できます。選択できるデバイスは、現在スタックのメンバーにも、ペアにもなっていないデバイスのみです。新しいデバイスは、デバイス スタックを確立する場合と同じガイドラインに従っている必要があります。

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 メンテナンス モードを開始するスタック メンバーの横にあるメンテナンス モード切り替えアイコン（）をクリックします。

ステップ 3 [はい（Yes）] をクリックして、メンテナンス モードを確定します。

ステップ 4 デバイス交換アイコン（）をクリックします。

ステップ 5 ドロップダウンリストから [交換デバイス（Replacement Device）] を選択します。

ステップ 6 [交換（Replace）] をクリックして、デバイスを交換します。

ステップ 7 メンテナンス モード切り替えアイコン（）を再度クリックすると、スタックのメンテナンス モードが即時に終了します。

（注） デバイス設定を再展開する必要はありません。

デバイスのハイ アベイラビリティ状態共有

デバイスのハイ アベイラビリティ状態共有を使用すると、ハイ アベイラビリティ ペアのデバイスまたはスタックで、可能な限り状態を同期できます。したがって、いずれか一方のデバイスまたはスタックで障害が発生しても、もう一方のピアがトラフィック フローを中断せずに引き継ぐことができます。状態共有を使用しない場合、以下の機能が適切にフェールオーバーしない可能性があります。

- 厳密な TCP 適用
- 単方向アクセス コントロール ルール
- ブロッキングの永続性

ただし、状態共有を有効にすると、システムパフォーマンスが低下することに注意してください。

ハイ アベイラビリティ状態共有を設定するには、あらかじめハイ アベイラビリティ ペアの両方のデバイスまたはスタック構成のプライマリ デバイスで HA リンク インターフェイスを設定し、有効にする必要があります。Firepower 82xx ファミリおよび 83xx ファミリには 10 G の HA リンクが必要ですが、他のモデルのデバイスには 1 G の HA リンクで十分です。

HA リンク インターフェイスを変更する前に、状態共有を無効にする必要があります。

（注） ペアを構成するデバイスでフェールオーバーが発生した場合は、アクティブデバイス上の既存の SSL 暗号化セッションがすべて終了されます。ハイ アベイラビリティ状態共有を設定しているとしても、これらのセッションをスタンバイデバイスで再ネゴシエートする必要があります。SSL セッションを確立しているサーバがセッションの再利用をサポートしている場合でも、スタンバイ デバイスに SSL セッション ID がないと、セッションを再ネゴシエートできません。

厳密な TCP の適用

ドメインに対して厳密な TCP 適用を有効にすると、システムは TCP セッションで正常ではないパケットをすべてドロップします。たとえば、未確立の接続で受信した SYN 以外のパケットはドロップされます。状態共有が有効な場合、厳密な TCP 適用が有効にされているとしても、ハイ アベイラビリティ ペアのデバイスは、フェールオーバー後に接続を再び確立することなく TCP セッションを続行できます。厳密な TCP 適用は、インライン セット、仮想ルータ、および仮想スイッチで有効にすることができます。

単方向アクセス コントロール ルール

単方向アクセス コントロール ルールを設定している場合、システムがフェールオーバーの後に接続ミッドストリームを再評価する際に、ネットワーク トラフィックが意図されたものとは異なるアクセス コントロール ルールに一致する可能性があります。たとえば、ポリシーに以下の 2 つのアクセス コントロール ルールが含まれているとします。

```
Rule 1: Allow from 192.168.1.0/24 to 192.168.2.0/24
Rule 2: Block all
```

状態共有が有効でない場合、フェールオーバーの後に 192.168.1.1 ～ 192.168.2.1 からの許可される接続がまだアクティブになっているために、次のパケットが応答パケットとしてみなされると、システムは接続を拒否します。状態共有が有効であれば、ミッドストリーム ピックアップが既存の接続に一致することになり、接続が引き続き許可されます。

ブロッキングの永続性

アクセス コントロール ルールやその他の要素に基づいて、最初のパケットで多数の接続がブロックされるとしても、システムが接続のブロッキングを決定する前に、いくつかのパケットを許可する場合があります。状態共有が有効な場合、システムはピアデバイスまたはスタックでも即時に接続をブロックします。

ハイ アベイラビリティ ペアの状態共有を確立するときに、次のオプションを設定できます。

[有効（Enabled）]

状態共有を有効にするには、このチェック ボックスをクリックします。チェック ボックスをクリアすると、状態共有が無効になります。

Minimum Flow Lifetime

最小セッション時間（ミリ秒）を指定します。この時間を経過すると、システムがセッションの同期メッセージを送信します。0 ～ 65535 の整数を使用できます。この最小フロー有効期間に達しないセッションは、いずれも同期されず、接続のパケットを受信した時点でのみ、同期が行われます。

Minimum Sync. Interval

セッションの更新メッセージ間隔（ミリ秒）を指定します。0～65535の整数を使用できます。最小同期間隔を設定することで、特定の接続が最小有効期間に達した後、その接続に対して、設定された値より頻繁に同期メッセージが送信されないようにします。

HTTP URL の最大文字数（Maximum HTTP URL Length）

ペアを構成するデバイス間で同期する、URL の最大文字数を指定します。0 ～ 225 の整数を使用できます。

関連トピック

HA リンク インターフェイスの設定 （658 ページ）

デバイスのハイ アベイラビリティ状態共有の確立

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
該当なし	Control	7000 & 8000 シリーズ	リーフのみ	Admin/Network Admin

デバイスのハイ アベイラビリティ状態共有を使用すると、ハイ アベイラビリティ ペア内の 7000 または 8000 シリーズ デバイスまたはスタック間で、可能な限り状態を同期できます。したがって、いずれか一方のデバイスまたはスタックで障害が発生しても、もう一方のピアがトラフィック フローを中断せずに引き継ぐことができます。

注意 7000 または 8000 シリーズ デバイスのハイ アベイラビリティ状態共有オプションを変更すると、プライマリ デバイスとセカンダリ デバイスの Snort プロセスが再起動され、両方のデバイスのトラフィック インスペクションが一時的に中断されます。 この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、ターゲット デバイスがトラフィックを処理する方法に応じて異なります。詳細はSnort® の再起動によるトラフィックの動作 （451 ページ）を参照してください。

ステップ 1 デバイスのハイ アベイラビリティ ペアのデバイスごとに HA リンク インターフェイスを設定します。HA リンク インターフェイスの設定 （658 ページ）を参照してください。

ステップ 2 **[Devices]** > **[Device Management]**を選択します。

ステップ 3 編集するデバイス ハイ アベイラビリティ ペアの横にある編集アイコン（）をクリックします。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 4 [状態共有（State Sharing）] セクションの横にある編集アイコン（）をクリックします。

ステップ 5 状態共有の値を下げてペア内のピアの準備状況を改善するか、値を上げてパフォーマンスを向上できるようにします。

展開で値を変更する正当な理由がない限り、デフォルト値を使用することを推奨します。

ステップ 6 [OK] をクリックします。

次のタスク

設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

関連トピック

HA リンク インターフェイスの設定 （658 ページ）
Snort® の再起動シナリオ （450 ページ）

トラブルシューティングのためのデバイスのハイアベイラビリティの状態共有統計情報

以下の項では、デバイスごとに表示可能な統計情報と、7000 および 8000 シリーズ デバイスのハイ アベイラビリティ ペアの状態共有設定をトラブルシューティングするためにどのように利用できるかを説明します。

受信メッセージ（ユニキャスト）（Messages Received (Unicast)）

ペアを構成するピアから受信した、ハイ アベイラビリティ同期メッセージの数です。

値は、ピアが送信したメッセージ数と同等になっているはずです。アクティブに使用されている間は、値が一致しない場合もありますが、その差は小さいはずです。トラフィックが停止すると、値は安定し、受信したメッセージ数が送信されたメッセージ数と一致します。

トラブルシューティングを行う場合は、受信したメッセージ数と送信されたメッセージ数の両方を確認して増加率を比較し、両方の値が同等であることを確認します。各ピアでの送信数の値は、対応するピアでの受信数の値とほぼ同じ率で増えていなければなりません。

受信したメッセージの数が増加しなくなった場合、または増加率がピアから送信されたメッセージ数に追いついていない場合は、サポートに連絡してください。

受信パケット数（Packets received）

システムはオーバーヘッドを低減させるために、複数のメッセージを単一のパケットにまとめます。[Packets Received] カウンタは、デバイスが受信したこれらのデータ パケットとその他の制御パケットの数を表示します。

値は、ピアデバイスが送信したパケット数と同等になっているはずです。アクティブに使用されている間は、値が一致しない場合もありますが、その差は小さいはずです。受信メッセージの数は、ピアが送信したメッセージ数と同等で、同じ率で増加していなければなりません。したがって、受信したパケットの数も同じ動作となるはずです。

トラブルシューティングを行う場合は、受信したパケットと送信されたメッセージの両方を確認して増加率を比較し、値が同じ率で増加していることを確認します。ペアを構成するピアでの送信の値が増えている場合、デバイスでの受信の値も同じ率で増えているはずです。

受信したパケットの数が増加しなくなった場合、または増加率がピアから送信されたメッセージ数に追いついていない場合は、サポートに連絡してください。

Total Bytes Received

ピアで受信されたパケットの合計バイト数です。

値は、もう一方のピアが送信したバイト数と同等になっているはずです。アクティブに使用されている間は、値が一致しない場合もありますが、その差は小さいはずです。

トラブルシューティングを行う場合は、受信した合計バイト数と送信されたメッセージ数の両方を確認して増加率を比較し、両方の値が同じ率で増えていることを確認します。ペアを構成するピアでの送信の値が増えている場合、デバイスでの受信の値も同じ率で増えているはずです。

受信バイト数が増加しなくなった場合、または増加率がピアから送信されたメッセージ数に追いついていない場合は、サポートに連絡してください。

Protocol Bytes Received

受信したプロトコル オーバーヘッドのバイト数です。この数には、セッション状態同期メッセージのペイロードを除くすべてが含まれます。

値は、ピアが送信したバイト数と同等になっているはずです。アクティブに使用されている間は、値が一致しない場合もありますが、その差は小さいはずです。

トラブルシューティングを行う場合は、受信した合計バイト数を確認してプロトコルデータと比較し、実際の状態データがどれだけ共有されているのかを調べます。プロトコルデータが送信されるデータの大部分を占めている場合は、最小同期間隔を調整できます。

受信したプロトコルバイト数が、受信した合計バイト数と同等の割合で増えている場合は、サポートに連絡してください。受信したプロトコルバイト数が受信した合計バイト数に占める割合は、最小限でなければなりません。

送信メッセージ（Messages Sent）

ペアを構成するピアに送信した、ハイ アベイラビリティ同期メッセージの数です。

このデータは、受信メッセージ数との比較で役立ちます。アクティブに使用されている間は、値が一致しない場合もありますが、その差は小さいはずです。

トラブルシューティングを行う場合は、受信したメッセージ数と送信されたメッセージ数の両方を確認して増加率を比較し、両方の値が同等であることを確認します。

送信したメッセージ数が、受信した合計バイト数と同等の割合で増えている場合は、サポートに連絡してください。

送信バイト数（Bytes Sent）

ピアに送信したハイ アベイラビリティ同期メッセージの合計送信バイト数です。

このデータは、受信メッセージ数との比較で役立ちます。アクティブに使用されている間は、値が一致しない場合もありますが、その差は小さいはずです。ピアで受信されたバイト数は、この値と同等であり、それより大きい値にはなっていないはずです。

受信した合計バイト数が、送信されたバイト数と同じような比率で増えていない場合は、サポートに連絡してください。

Tx Errors

システムがペアを構成するピアに送信するメッセージ用にスペースを割り当てるときに、メモリ割り当てに失敗した回数です。

この値は両方のピアで常にゼロでなければなりません。この数がゼロでない場合、あるいは着実に増加している場合（これは、システムにメモリ割り当てが不可能なエラーが発生していることを示します）は、サポートに連絡してください。

Tx Overruns

システムがメッセージをトランジット キューに入れようとして失敗した回数です。

この値は両方のピアで常にゼロでなければなりません。値がゼロでない場合、あるいは着実に増加している場合、これは、システムがHAリンクの間で過剰なデータを共有していて、データの送信に時間がかかりすぎていることを示します。

HA リンク MTU がデフォルト値（9918 または 9922）未満に設定されている場合は、値を増やす必要があります。最小フロー有効期間と最小同期間隔の設定を変更することで、HA リンク間で共有されるデータ量を減らし、この数の増加を防ぐことができます。

この値がゼロにならない場合、または増加し続けている場合は、サポートに連絡してください。

最近のログ（Recent Logs）

システム ログには、最新のハイ アベイラビリティ同期メッセージが表示されます。ログには、ERROR または WARN メッセージが示されていてはなりません。ログの内容は、常にピア間で同等でなければなりません（接続ソケットの数が同じであるなど）。

ただし、場合によっては、対照的なデータが表示されることもあります。たとえば、一方のピアがもう一方のピアから接続を受信したことをレポートしている場合、それぞれのログで参照される IP アドレスは異なります。このログから、ハイ アベイラビリティ状態共有接続を包括的に理解し、接続で発生したすべてのエラーを確認できます。

ログに、ERROR または WARN メッセージ、あるいは単なる通知目的ではないようなメッセージが示されている場合は、サポートに連絡してください。

デバイス ハイ アベイラビリティの状態共有統計情報の表示

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
該当なし	Control	7000 & 8000 シリーズ	リーフのみ	Admin/Network Admin

状態共有を確立した後は、[ハイ アベイラビリティ（High Availability）] ページの [状態共有（State Sharing）] セクションで、設定に関する以下の情報を確認できます。

- 使用されている HA リンク インターフェイスおよび現在のリンク状態
- 問題のトラブルシューティングに使用できる、同期に関する詳細な統計情報

状態共有の統計情報は、主に、送受信されたハイ アベイラビリティ同期トラフィックのさまざまな側面に関するカウンタで、その他のエラー カウンタも含まれます。さらに、ハイ アベイラビリティ ペアのデバイスごとの最新システム ログも表示できます。

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 編集するデバイス ハイ アベイラビリティ ペアの横にある編集アイコン（  ）をクリックします。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [状態共有（State Sharing）] セクションで、統計情報表示アイコン（  ）をクリックします。

ステップ 4 ハイ アベイラビリティ ペアがデバイス スタックで構成されている場合、表示する [デバイス（Device）] を選択します。

ステップ 5 次の操作を実行できます。

- [更新（Refresh）] をクリックして統計情報を更新します。
- [表示（View）] をクリックして、ハイ アベイラビリティ ペアのデバイスごとの最新システム ログを表示します。

デバイス高可用性ペアの分離

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
該当なし	Control	7000 & 8000 シリーズ	任意（Any）	Admin/Network Admin

7000 または 8000 シリーズ デバイス高可用性ペアを分離（分断）すると、次のようになります。

- アクティブなピア（デバイスまたはスタック）は、完全な展開機能を維持します
- スタンバイ ピア（デバイスまたはスタック）はインターフェイス設定を失って、アクティブ ピアにフェールオーバーします。ただし、インターフェイス設定をアクティブのままにすることを選択すると、スタンバイ ピアは通常の動作を再開します。
- スタンバイ ピアは、常にパッシブ インターフェイスの設定を失います。
- メンテナンス モードのピアは、通常の動作を再開します。

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 分断する高可用性ペアの横にある HA の分断アイコン（）をクリックします。

ステップ 3 必要に応じて、スタンバイ ピアのインターフェイス設定を削除するためのチェックボックスをオンにします。

この手順により、管理インターフェイス以外のすべてのインターフェイスを管理のためにダウンさせます。

ステップ 4 [Yes] をクリックします。

第 26 章

8000 シリーズ デバイスのスタック構成

次のトピックでは、Firepower システムにおける Firepower 8000 シリーズ デバイス スタックの使用方法について説明します。

デバイス スタックについて

スタック構成に含まれるデバイスを使用して、ネットワークセグメントで検査されるトラフィックの量を増やすことができます。それぞれのスタック構成では、スタックに含まれるすべてのデバイスが同じハードウェアを使用していなければなりません。ただし、マルウェア ストレージパックが一部またはすべてのデバイスにインストールされていたり、どのデバイスにもインストールされていなかったりする場合があります。また、以下のスタック構成に従って、同じデバイス ファミリのデバイスを使用する必要があります。

スタック構成は Firepower 8140、Firepower 8200 ファミリ、Firepower 8300 ファミリのデバイスでサポートされます。

81xx ファミリの場合：

- 2 台の Firepower 8140

82xx ファミリの場合：

- 最大 4 台の Firepower 8250
- 1 台の Firepower 8260（プライマリ デバイスおよびセカンダリ デバイス）
- 1 台の Firepower 8270（容量 40 G のプライマリ デバイスと 2 つのセカンダリ デバイス）
- 1 台の Firepower 8290（容量 40 G のプライマリ デバイスと 3 つのセカンダリ デバイス）

83xx ファミリの場合：

- 最大 4 台の Firepower 8350
- 最大 4 つの AMP8350
- 1 台の Firepower 8360（容量 40 G のプライマリ デバイスと 1 つのセカンダリ デバイス）
- 1 つの AMP8360（容量 40 G のプライマリ デバイスとセカンダリ デバイス）
- 1 台の Firepower 8370（容量 40 G のプライマリ デバイスと 2 つのセカンダリ デバイス）
- 1 つの AMP8370（容量 40 G のプライマリ デバイスと 2 つのセカンダリ デバイス）
- 1 台の Firepower 8390（容量 40 G のプライマリ デバイスと 3 つのセカンダリ デバイス）
- 1 つの AMP8390（容量 40 G のプライマリ デバイスと 3 つのセカンダリ デバイス）

スタック構成の詳細については、Cisco Firepower 8000 シリーズ スタートアップ ガイドを参照してください。マルウェア ストレージ パックの詳細については、*Firepower System Malware Storage Pack Guide*を参照してください。*Firepower System Malware Storage Pack Guide*。

⚠

注意 Cisco から供給されたハード ドライブ以外はデバイスに取り付けないでください。サポートされていないハードドライブを取り付けると、デバイスが破損する可能性があります。マルウェア ストレージパック キットは、シスコから**のみ**購入でき、8000 シリーズデバイスで**のみ**使用できます。マルウェア ストレージ パックのサポートが必要な場合は、サポートにお問い合わせください。詳細については、*Firepower System Malware Storage Pack Guide*を参照してください。

スタック構成を確立するときに、各スタック構成デバイスのリソースを 1 つの共有構成に統合します。

1 つのデバイスをプライマリ デバイスとして指定し、そのデバイスにスタック全体のインターフェイスを設定します。その他のデバイスはセカンダリ デバイスとして指定します。セカンダリ デバイスは、現在トラフィックを検知していないデバイスで、かつインターフェイス上にリンクがないデバイスでなければなりません。

単一のデバイスを設定する場合と同じように、プライマリ デバイスを分析対象のネットワーク セグメントに接続します。Cisco Firepower 8000 シリーズ スタートアップ ガイドで説明されて

いるスタック構成のデバイスの配線手順に従って、セカンダリ デバイスをプライマリ デバイスに接続します。

スタック構成に含まれるすべてのデバイスは、同じハードウェアを使用し、同じソフトウェアバージョンを実行し、同じライセンスが適用されている必要があります。デバイスが NAT ポリシーのターゲットとなっている場合は、プライマリ デバイスとセカンダリ デバイスの両方に同じ NAT ポリシーを適用する必要があります。更新は、Firepower Management Center からスタック全体に対して展開する必要があります。スタック構成の 1 つ以上のデバイスで更新に失敗した場合、スタックはバージョンが混在した状態になります。バージョンが混在するスタックには、ポリシーを展開することも、更新を展開することもできません。この状態を修正するには、スタックを解除するか、バージョンが異なる個々のデバイスを削除し、それらのデバイスを個別に更新してからスタック構成を再確立します。デバイスをスタックに入れた後は、ライセンスの変更は、スタック全体に対してのみ行うことができます。

スタック構成を確立した後は、スタック構成に含まれるすべてのデバイスが単一の共有構成のように機能します。プライマリ デバイスで障害が発生した場合、トラフィックはセカンダリ デバイスに渡されません。この場合、セカンダリ デバイスでスタック ハートビートが失敗したことを通知する、ヘルス アラートが生成されます。

スタック内のセカンダリ デバイスで障害が発生すると、設定可能なバイパスが有効になっているインライン セットがプライマリ デバイス上でバイパス モードになります。それ以外のすべての設定では、システムは、失敗したセカンダリ デバイスへ継続してトラフィックをロードバランシングします。いずれの場合も、リンクが失われたことを示すためのヘルス アラートが生成されます。

デバイス スタックは展開内で単一のデバイスと同じように使用できますが、いくつかの例外があります。ハイ アベイラビリティ ペアに 7000 または 8000 シリーズ デバイスがある場合は、デバイスのハイ アベイラビリティ ペアまたはハイ アベイラビリティ ペアのデバイスをスタックできません。また、デバイス スタックに NAT を設定することもできません。

（注） スタック構成のデバイスからのイベント データを、eStreamer を使用して外部クライアント アプリケーションに配信する場合は、各デバイスからデータを収集して、各デバイスが同じように設定されていることを確認します。eStreamer 設定は、スタック構成のデバイス間で自動的に同期されません。

マルチドメイン展開では、同じドメインに属しているデバイスのみをスタックできます。

関連トピック

ヘルス モニタリングについて （349 ページ）

デバイス スタック設定

2 台の Firepower 8140 デバイス、最大 4 台の Firepower 8250、1 台の Firepower 8260、1 台の Firepower 8270、1 台の Firepower 8290、最大 4 台の Firepower 8350、1 台の Firepower 8360、1 台の Firepower 8370、または 1 台の Firepower 8390 をスタック構成し、それらを組み合わせた

リソースを単一の共有設定で使用することによって、ネットワーク セグメントで検査されるトラフィック量を増やすことができます。ハイ アベイラビリティ ペアに7000または8000シリーズ デバイスがある場合、デバイスのハイ アベイラビリティ ペア、またはハイ アベイラビリティ ペアの一方のデバイスのスタックは構成できません。ただし、2つのデバイス スタックのハイ アベイラビリティ ペアを構成できます。

デバイス スタックを確立すると、これらのデバイスは、[デバイス管理（Device Management）]ページで単一のデバイスとして扱われます。デバイス スタックには、アプライアンスのリストでスタック アイコン（  ）が表示されます。

デバイス スタックの登録をFirepower Management Centerから削除すると、その登録は両方のデバイスから削除されます。スタックに含まれるデバイスをFirepower Management Centerから削除する方法は、単一の管理対象デバイスを削除する場合と同じです。削除したスタックは、別のFirepower Management Centerに登録できます。新しいFirepower Management Centerに、スタックに含まれるデバイスのいずれか1つを登録するだけで、スタック全体が表示されるようになります。

デバイス スタックを確立した後は、スタックを解除して再確立しない限り、デバイスのプライマリまたはセカンダリとしての役割を変更することはできません。ただし、次の作業を実行できます。

- 最大 4 台の Firepower 8250 を 1 つのスタックの限度として、2 台または 3 台の Firepower 8250、1 台の Firepower 8260、または 1 台の Firepower 8270 からなる既存のスタックにセカンダリ デバイスを追加できます。
- 最大 4 台の Firepower 8350 を 1 つのスタックの限度として、2 台または 3 台の Firepower 8350、1 台の Firepower 8360、または 1 台の Firepower 8370 からなる既存のスタックにセカンダリ デバイスを追加できます。

デバイスを追加する場合、スタックのプライマリ デバイスに、追加のデバイスを配線するために必要なスタック NetMods がなければなりません。たとえば、プライマリに単一のスタック NetMod しかない Firepower 8260 を使用している場合、このスタックに別のセカンダリ デバイスを追加することはできません。セカンダリ デバイスを既存のスタックに追加する方法は、最初にスタックに含まれるデバイスの設定を確立したときの方法と同じです。

デバイス スタックの確立

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
該当なし	いずれか（Any）	Firepower 8140、8200 ファミリ、8300 ファミリ	任意（Any）	Admin/Network Admin

スタック内のすべてのデバイスが同じハードウェア モデル（たとえば、Firepower 8140 と別の 8140）である必要があります。8200 ファミリおよび 8300 ファミリでは、合計 4 つのデバイス（1 つのプライマリ デバイスと最大 3 つのセカンダリ デバイス）でスタックを構成できます。

マルチドメイン展開では、スタック内のすべてのデバイスが同じドメインに属している必要があります。

始める前に

- プライマリ デバイスとして指定するユニットを決定します。
- プライマリとセカンダリの関係を指定する前に、ユニット間の配線が適切に行われていることを確認します。ケーブルについては、Cisco Firepower 8000 シリーズ スタートアップ ガイドを参照してください。

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 [追加（Add）] ドロップダウン メニューから、[スタックの追加（Add Stack）] を選択します。

ステップ 3 [プライマリ（Primary）] ドロップダウン リストから、プライマリ デバイスとして運用するために配線したデバイスを選択します。

（注） プライマリ デバイスとして配線されていないデバイスを選択すると、以降の手順を実行できなくなります。

ステップ 4 名前を入力します。

ステップ 5 [追加（Add）] をクリックし、スタックに含めるデバイスを選択します。

ステップ 6 [プライマリ デバイスのスロット（Slot on Primary Device）] ドロップダウン リストから、プライマリ デバイスをセカンダリ デバイスに接続するスタック構成ネットワーク モジュールを選択します。

ステップ 7 [セカンダリ デバイス（Secondary Device）] ドロップダウン リストから、セカンダリ デバイスとして運用するために配線したデバイスを選択します。

ステップ 8 [セカンダリ デバイスのスロット（Slot on Secondary Device）] ドロップダウン リストから、セカンダリ デバイスをプライマリ デバイスに接続するスタック構成ネットワーク モジュールを選択します。

ステップ 9 [追加（Add）] をクリックします。

ステップ 10 複数の Firepower 8250、1 つの Firepower 8260、1 つの Firepower 8270 の既存のスタック、複数の Firepower 8350、1 つの Firepower 8360 または 1 つの Firepower 8370 の既存のスタックにセカンダリ デバイスを追加する場合は、手順 5 ～ 9 を繰り返します。

ステップ 11 [スタック（Stack）] をクリックし、デバイス スタックを確立するか、セカンダリ デバイスを追加します。このプロセスではシステム データの同期が行われるため、プロセスが完了するまでに数分かかることに注意してください。

関連トピック

7000 および 8000 シリーズ デバイスのハイ アベイラビリティについて （679 ページ）
Firepower Management Center からのデバイスの削除 （295 ページ）
Firepower Management Center へのデバイスの追加 （293 ページ）

デバイス スタックの編集

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
該当なし	いずれか（Any）	Firepower 8140、Firepower 8200 ファミリ、Firepower 8300 ファミリ	リーフのみ	Admin/Network Admin

デバイス スタックを確立した後は、デバイス設定を変更すると、通常はスタック全体の設定も変更されます。単一のデバイスの [デバイス（Device）] ページで設定を変更する場合と同じように、アプライアンス エディタの [スタック（Stack）] ページで、スタック設定に変更を加えることができます。

スタックの表示名を変更したり、ライセンスを有効または無効にしたり、システム ポリシーや正常性ポリシーを表示したり、詳細設定を構成したりすることができます。

ステップ 1 **[Devices]** > **[Device Management]** を選択します。

ステップ 2 設定を編集する、スタックに含まれるデバイスの横にある編集アイコン（  ）をクリックします。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [スタック（Stack）] ページのセクションを使用して、単一のデバイス設定を変更する場合と同じように、スタック構成の設定を変更します。

スタック内のデバイスの交換

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
該当なし	いずれか（Any）	FirePOWER 8140、8200 ファミリ、8300 ファミリ	任意（Any）	Admin/Network Admin

Firepower Management Center がデバイスと通信できない場合に、スタックを分離してデバイスの登録を解除するには、デバイスに接続して CLI コマンドを使用する必要があります。詳細については、関連する章「クラシック デバイス CLI 設定コマンド （3325 ページ）」の **stacking disable** CLI コマンドおよび **delete** CLI コマンドを参照してください。

スタック内のデバイスを交換するには、以下を行います。

ステップ 1 デバイスを含むスタックを選択し、そのスタックを交換して解除します。詳細については、スタック構成のデバイスの分離 （707 ページ）を参照してください。

ステップ 2 Firepower Management Center からデバイスを登録解除します。詳細については、Firepower Management Center からのデバイスの削除 （295 ページ）を参照してください。

ステップ 3 交換デバイスを Firepower Management Center に登録します。詳細については、Firepower Management Center へのデバイスの追加 （293 ページ）を参照してください。

ステップ 4 交換デバイスを含むデバイス スタックを作成します。詳細については、デバイス スタックの確立 （702 ページ）を参照してください。

高可用性ペアのスタック内のデバイスの交換

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
該当なし	Control	Firepower 8140、8200 ファミリ、8300 ファミリ	任意（Any）	Admin/Network Admin

高可用性ペアのメンバーになっているスタックをメンテナンス モードに切り替えた後で、スタック内のセカンダリ デバイスを別のデバイスと交換できます。選択できるデバイスは、現在スタックのメンバーにも、ペアにもなっていないデバイスのみです。新しいデバイスは、デバイス スタックを確立する場合と同じガイドラインに従っている必要があります。

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 メンテナンス モードを開始するスタック メンバーの横にあるメンテナンス モード切り替えアイコン（）をクリックします。

ステップ 3 [はい（Yes）] をクリックして、メンテナンス モードを確定します。

ステップ 4 デバイス交換アイコン（  ）をクリックします。

ステップ 5 ドロップダウンリストから [交換デバイス（Replacement Device）] を選択します。

ステップ 6 [交換（Replace）] をクリックして、デバイスを交換します。

ステップ 7 メンテナンス モード切り替えアイコン（  ）を再度クリックすると、スタックのメンテナンス モードが即時に終了します。

（注） デバイス設定を再展開する必要はありません。

スタックに含まれる個々のデバイスの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
該当なし	いずれか（Any）	Firepower 8140、Firepower 8200 ファミリ、Firepower 8300 ファミリ	リーフのみ	Admin/Network Admin

デバイス スタックを確立した後でも、スタック内の個々のデバイスに対して設定できる属性がいくつかあります。スタックに設定されたデバイスに変更を加える方法は、単一のデバイスに変更を加える場合の方法と同じです。このページでは、デバイスの表示名の変更、システム設定の表示、デバイスのシャットダウンまたは再起動、ヘルス情報の表示、およびデバイス管理設定の編集を行うことができます。

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 設定を編集する、スタックに含まれるデバイスの横にある編集アイコン（  ）をクリックします。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [デバイス（Device）] タブをクリックします。

ステップ 4 [選択されたデバイス（Selected Device）] ドロップダウン リストから、変更するデバイスを選択します。

ステップ 5 [デバイス（Devices）] ページのセクションを使用して、単一のデバイスに対して変更を加える場合と同じように、スタックに含まれる個々のデバイスに変更を加えます。

スタック構成のデバイスでのインターフェイスの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
該当なし	いずれか（Any）	Firepower 8140、Firepower 8200 ファミリ、Firepower 8300 ファミリ	リーフのみ	Admin/Network Admin

管理インターフェイスを除き、スタック構成のデバイスにインターフェイスを設定するには、スタックのプライマリ デバイスの [インターフェイス（Interfaces）] ページを使用します。管理インターフェイスを設定する場合は、スタックに含まれる任意のデバイスを選択できます。

Firepower スタック構成デバイスの [インターフェイス（Interfaces）] ページに、個々のデバイスのハードウェアおよびインターフェイスのビューがあります。

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 プライマリ スタック構成デバイスの横で、編集アイコン（  ）をクリックします。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [インターフェイス（Interfaces）] タブをクリックします。

ステップ 4 [選択されたデバイス（Selected Device）] ドロップダウン リストから、変更するデバイスを選択します。

ステップ 5 個々のデバイスに設定する場合と同じようにインターフェイスを設定します。センシング インターフェイスの設定 （656 ページ）を参照してください。

関連トピック

管理インターフェイス （1266 ページ）

スタック構成のデバイスの分離

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
該当なし	いずれか（Any）	FirePOWER 8140、8200 ファミリ、8300 ファミリ	任意（Any）	Admin/Network Admin

デバイスのスタック構成を使用する必要がなくなった場合、スタックを解除してデバイスを分離できます。

（注） スタック構成のデバイスに障害が発生した場合や、スタックのメンバーデバイス間の通信に障害が発生した場合は、Firepower Management Center Web インターフェイスを使用してスタック構成のデバイスを分離することはできません。この場合は、補助 CLI コマンド `configure stacking disable` を使用して、それぞれのデバイスから個別にスタック設定を削除します。

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 分断するデバイス スタックの横にあるスタックの分断アイコン（）をクリックします。

ヒント スタックを分断することなく、3 台以上の Firepower 8250 デバイスのスタックからセカンダリ デバイスを削除するには、スタックからの削除アイコン（）をクリックします。セカンダリ デバイスを削除すると、システムがそのデバイス抜きで動作するスタックを再設定する間、トラフィック検査、トラフィック フロー、またはリンク状態が短時間中断されます。

ステップ 3 [はい（Yes）] をクリックして、デバイス スタックを分離します。

スタック内のデバイスの交換

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
該当なし	いずれか（Any）	FirePOWER 8140、8200 ファミリ、8300 ファミリ	任意（Any）	Admin/Network Admin

Firepower Management Center がデバイスと通信できない場合に、スタックを分離してデバイスの登録を解除するには、デバイスに接続して CLI コマンドを使用する必要があります。詳細については、関連する章「クラシック デバイス CLI 設定コマンド （3325 ページ）」の **stacking disable** CLI コマンドおよび **delete** CLI コマンドを参照してください。

スタック内のデバイスを交換するには、以下を行います。

ステップ 1 デバイスを含むスタックを選択し、そのスタックを交換して解除します。詳細については、スタック構成のデバイスの分離 （707 ページ）を参照してください。

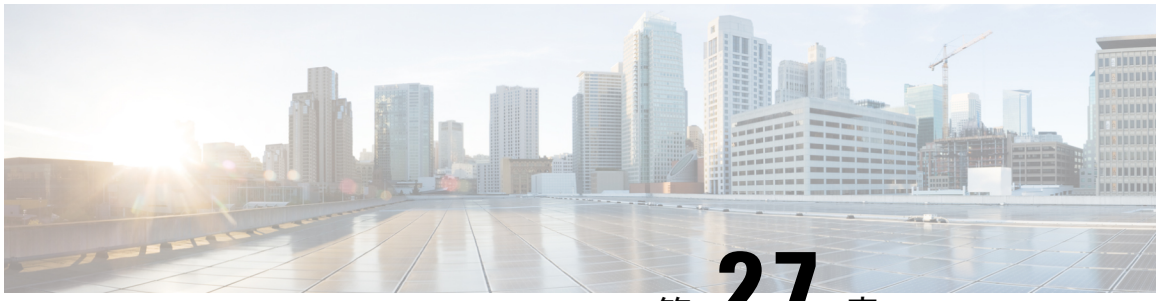
ステップ 2 Firepower Management Center からデバイスを登録解除します。詳細については、Firepower Management Center からのデバイスの削除 （295 ページ）を参照してください。

ステップ 3 交換デバイスを Firepower Management Center に登録します。詳細については、Firepower Management Center へのデバイスの追加 （293 ページ）を参照してください。

ステップ 4 交換デバイスを含むデバイス スタックを作成します。詳細については、デバイス スタックの確立 （702 ページ）を参照してください。

第 VII 部

Firepower Threat Defense を使用する前に



第 27 章

Firepower Threat Defense 用のトランスペアレントまたはルーテッド ファイアウォール モード

この章では、ファイアウォール モードをルーテッドまたはトランスペアレントに設定する方法と、ファイアウォールが各ファイアウォール モードでどのように機能するかについて説明します。

（注） ファイアウォール モードは通常のファイアウォール インターフェイスのみに影響し、インライン セットやパッシブ インターフェイスなどの IPS 専用インターフェイスには影響しません。IPS 専用インターフェイスはどちらのファイアウォール モードでも使用できます。IPS 専用インターフェイスの詳細については、Firepower Threat Defense のインライン セットとパッシブ インターフェイス （841 ページ） を参照してください。インライン セットは「トランスペアレント インライン セット」と呼ばれることもありますが、インライン インターフェイス タイプはこの章で説明するトランスペアレント ファイアウォール モードおよびファイアウォール タイプのインターフェイスとは無関係です。

ファイアウォール モードについて

Firepower Threat Defense デバイスは、通常のファイアウォール インターフェイスでルーテッド ファイアウォール モードとトランスペアレント ファイアウォール モードの 2 つのファイアウォール モードをサポートします。

ルーテッド ファイアウォール モードについて

ルーテッドモードでは、Firepower Threat Defenseデバイスはネットワーク内のルータ ホップと見なされます。ルーティングを行う各インターフェイスは異なるサブネット上にあります。

統合ルーティングおよびブリッジングにより、ネットワーク上の複数のインターフェイスをまとめた「ブリッジ グループ」を使用できます。そして、Firepower Threat Defenseデバイス はブリッジング技術を使用してインターフェイス間のトラフィックを通すことができます。各ブリッジ グループには、ネットワーク上で IP アドレスが割り当てられるブリッジ仮想インターフェイス（BVI）が含まれます。Firepower Threat Defense デバイス は BVI と通常のルーテッド インターフェイス間でルーティングを行います。、クラスタリング、EtherChannel、冗長またはメンバーインターフェイスが必要ない場合は、トランスペアレントモードではなくルーテッド モードの使用を検討すべきです。ルーテッド モードでは、トランスペアレント モードと同様に1つ以上の分離されたブリッジ グループを含めることができます。また、モードが混在する導入に関しては、通常のルーテッド インターフェイスも含めることができます。

トランスペアレント ファイアウォール モードについて

従来、ファイアウォールはルーテッドホップであり、保護されたサブネットのいずれかに接続するホストのデフォルト ゲートウェイとして機能します。これに対し、トランスペアレント ファイアウォールは、「Bump In The Wire」または「ステルス ファイアウォール」のように動作するレイヤ2ファイアウォールであり、接続されたデバイスへのルータ ホップとしては認識されません。ただし、他のファイアウォールのように、インターフェイス間のアクセス制御は管理され、ファイアウォールによる通常のすべてのチェックが実施されます。

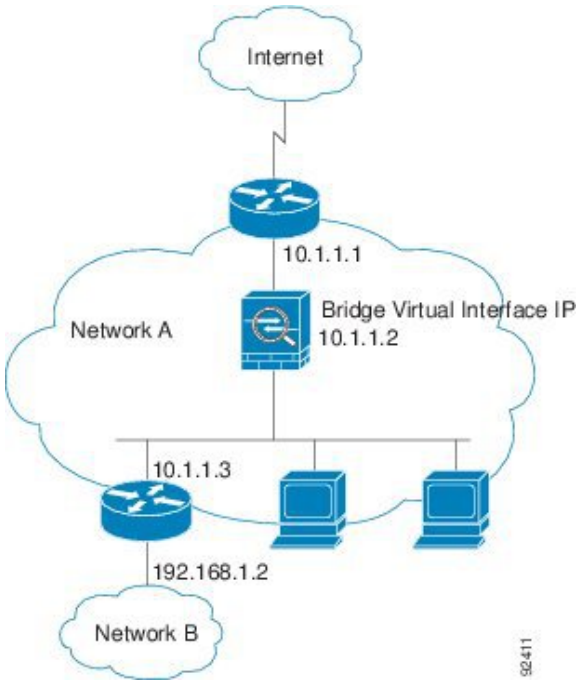
レイヤ 2 の接続は、ネットワークの内部と外部のインターフェイスをまとめた「ブリッジ グループ」を使用して実現されます。また、Firepower Threat Defense デバイス はブリッジング技術を使用してインターフェイス間のトラフィックを通すことができます。各ブリッジ グループには、ネットワーク上でIPアドレスが割り当てられるブリッジ仮想インターフェイス（BVI）が含まれます。複数のネットワークに複数のブリッジ グループを設定できます。トランスペアレント モードでは、これらのブリッジ グループは相互通信できません。

ネットワーク内でトランスペアレント ファイアウォールの使用

Firepower Threat Defense デバイス は、自身のインターフェイス間を同じネットワークで接続します。トランスペアレントファイアウォールはルーティングされたホップではないため、既存のネットワークに簡単に導入できます。

次の図に、外部デバイスが内部デバイスと同じサブネット上にある一般的なトランスペアレント ファイアウォール ネットワークを示します。内部ルータとホストは、外部ルータに直接接続されているように見えます。

図 *3:* トランスペアレント ファイアウォール ネットワーク



診断 [インターフェイス（Interface）]

各ブリッジ仮想インターフェイス（BVI）IP アドレスのほかに、別の診断 スロット/ポート インターフェイスを追加できます。このインターフェイスはどのブリッジグループにも属さず、Firepower Threat Defense デバイス への管理トラフィックのみを許可します。

ルーテッド モード機能のためのトラフィックの通過

トランスペアレント ファイアウォールで直接サポートされていない機能の場合は、アップストリーム ルータとダウンストリーム ルータが機能をサポートできるようにトラフィックの通過を許可することができます。たとえば、アクセス ルールを使用することによって、（サポートされていない DHCP リレー機能の代わりに）DHCP トラフィックを許可したり、IP/TV で作成されるようなマルチキャスト トラフィックを許可したりできます。また、トランスペアレント ファイアウォールを通過するルーティング プロトコル隣接関係を確立することもできます。つまり、OSPF、RIP、EIGRP、または BGP トラフィックをアクセス ルールに基づいて許可できます。同様に、HSRP や VRRP などのプロトコルは Firepower Threat Defense デバイス を通過できます。

ブリッジグループについて

ブリッジ グループは、Firepower Threat Defense デバイス がルーティングではなくブリッジするインターフェイスのグループです。 ブリッジグループはトランスペアレント ファイアウォール モード、ルーテッド ファイアウォール モードの両方でサポートされています。他のファイ

アウォールインターフェイスのように、インターフェイス間のアクセス制御は管理され、ファイアウォールによる通常のすべてのチェックが実施されます。

ブリッジ仮想インターフェイス（BVI）

各ブリッジ グループには、ブリッジ仮想インターフェイス（BVI）が含まれます。Firepower Threat Defense デバイス は、ブリッジ グループから発信されるパケットの送信元アドレスとしてこの BVI IP アドレスを使用します。BVI IP アドレスは□ブリッジ グループ メンバー インターフェイスと同じサブネット上になければなりません。BVI では、セカンダリ ネットワーク上のトラフィックはサポートされていません。BVI IP アドレスと同じネットワーク上のトラフィックだけがサポートされています。

トランスペアレント モード：インターフェイス ベースの各機能はブリッジ グループのメンバー インターフェイスだけを指定でき、これらについてのみ使用できます。

ルーテッド モード：BVI はブリッジ グループと他のルーテッド インターフェイス間のゲートウェイとして機能します。ブリッジ グループ/ルーテッド インターフェイス間でルーティングするには、BVI を指定する必要があります。一部のインターフェイス ベース機能に代わり、BVI 自体が利用できます。

- DHCPv4 サーバ：BVI のみが DHCPv4 サーバの構成をサポートします。
- スタティック ルート：BVI のスタティック ルートを設定できます。メンバー インターフェイスのスタティック ルートは設定できません。
- Syslog サーバと Firepower Threat Defense デバイス 由来の他のトラフィック：syslog サーバ（または SNMP サーバ、Firepower Threat Defense デバイス からトラフィックが送信される他のサービス）を指定する際、BVI またはメンバー インターフェイスのいずれかも指定できます。

ルーテッド モードで BVI を指定しない場合、Firepower Threat Defense デバイス はブリッジ グループのトラフィックをルーティングしません。この設定は、ブリッジ グループのトランスペアレント ファイアウォール モードを複製します。、クラスタリング、EtherChannel、冗長または メンバーインターフェイスが不要であれば、ルーテッド モードの使用を検討すべきです。ルーテッド モードでは、トランスペアレント モードと同様に 1 つ以上の分離されたブリッジ グループを含めることができます。また、モードが混在する導入に関しては、通常のルーテッド インターフェイスも含めることができます。

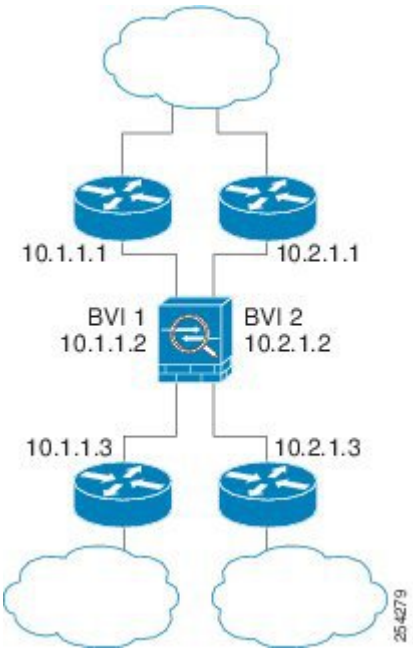
トランスペアレント ファイアウォール モードのブリッジ グループ

ブリッジ グループのトラフィックは他のブリッジ グループから隔離され、トラフィックは Firepower Threat Defense デバイス 内の他のブリッジ グループにはルーティングされません。また、トラフィックは外部ルータから Firepower Threat Defense デバイス 内の他のブリッジ グループにルーティングされる前に、Firepower Threat Defense デバイス から出る必要があります。ブリッジング機能はブリッジ グループごとに分かれていますが、その他の多くの機能はすべてのブリッジ グループ間で共有されます。たとえば、syslog サーバまたは AAA サーバの設定は、すべてのブリッジ グループで共有されます。

1 つのブリッジグループにつき複数のインターフェイスを入れることができます。サポートされるブリッジ グループとインターフェイスの正確な数については、ファイアウォール モードのガイドライン（721 ページ）を参照してください。ブリッジグループごとに 2 つ以上のインターフェイスを使用する場合は、内部、外部への通信だけでなく、同一ネットワーク上の複数のセグメント間の通信を制御できます。たとえば、相互通信を希望しない内部セグメントが 3 つある場合、インターフェイスを別々のセグメントに置き、外部インターフェイスとのみ通信させることができます。または、インターフェイス間のアクセスルールをカスタマイズし、希望通りのアクセスを設定できます。

次の図に、2 つのブリッジ グループを持つ、Firepower Threat Defense デバイス に接続されている 2 つのネットワークを示します。

図 *4：2* つのブリッジ グループを持つトランスペアレント ファイアウォール ネットワーク

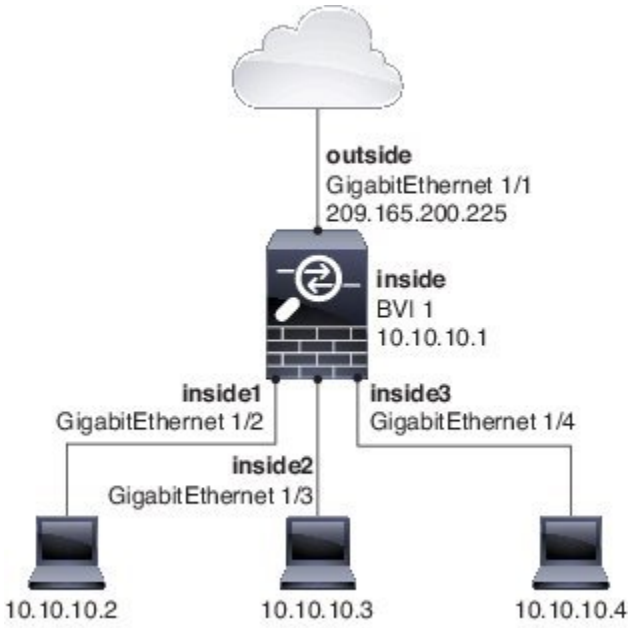


ルーテッド ファイアウォール モードのブリッジグループ

ブリッジグループ トラフィックは、他のブリッジグループまたはルーテッド インターフェイスにルーティングできます。ブリッジグループの BVI インターフェイスに名前を割り当てないでおくことで、ブリッジグループ トラフィックを分離できます。BVI の名前を指定すると、この BVI は他の通常のインターフェイスと同様にルーティングに参加します。

ルーテッド モードでブリッジ グループを使用する方法として、外部スイッチの代わりに Firepower Threat Defense デバイス 追加のインターフェイスを使用する方法があります。たとえば、一部のデバイスのデフォルト設定では、外部インターフェイスが通常のインターフェイスとして含まれており、その他のすべてのインターフェイスが内部ブリッジグループに割り当てられています。このブリッジグループは、外部スイッチを置き換えることを目的としているため、すべてのブリッジグループインターフェイスが自由に通信できるようにアクセスポリシーを設定する必要があります。

図 *5:* 内部ブリッジグループと外部ルーテッド インターフェイスからなるルーテッド ファイアウオール ネットワーク



レイヤ 3 トラフィックの許可

- ユニキャストの IPv4 および IPv6 トラフィックがブリッジグループを通過するにはアクセル ルールが必要です。
- ARP は、アクセス ルールなしで両方向にブリッジグループを通過できます。ARP トラフィックは、ARP インスペクションによって制御できます。
- IPv6 ネイバー探索およびルータ送信要求パケットは、アクセス ルールを使用して通過させることができます。
- ブロードキャストおよびマルチキャスト トラフィックは、アクセス ルールを使用して通過させることができます。

許可される MAC アドレス

アクセス ポリシーで許可されている場合、以下の宛先 MAC アドレスをブリッジグループで使用できます（レイヤ 3 トラフィックの許可 （716 ページ）を参照）。このリストにない MAC アドレスはドロップされます。

- FFFF.FFFF.FFFF の TRUE ブロードキャスト宛先 MAC アドレス
- 0100.5E00.0000 ～ 0100.5EFE.FFFF までの IPv4 マルチキャスト MAC アドレス
- 3333.0000.0000 ～ 3333.FFFF.FFFF までの IPv6 マルチキャスト MAC アドレス
- 0100.0CCC.CCCD の BPDU マルチキャスト アドレス

BPDU の処理

スパニングツリープロトコルを使用するときのループを防止するために、デフォルトでBPDUが渡されます。

デフォルトでは、BPDUは高度なインスペクションにも転送されます。このインスペクションは、このタイプのパケットには必要なく、インスペクションの再起動によってブロックされた場合など、問題を引き起こす可能性があります。BPDUは高度なインスペクションから常に除外することをお勧めします。これを行うには、FlexConfigを使用してBPDUを信頼するEtherType ACLを設定し、各メンバーインターフェイス上の高度な検査からBPDUを除外します。Firepower Threat Defense の FlexConfig ポリシー （1201 ページ）を参照してください。

FlexConfig オブジェクトは次のコマンドを展開する必要があります。ここで、<if-name> はインターフェイス名に置き換えます。必要な数の access-group コマンドを追加して、デバイス上の各ブリッジ グループのメンバー インターフェイスをカバーします。また、ACL に別の名前を選択することもできます。

```
access-list permit-bpdu ethertype trust bpdu
access-group permit-bpdu in interface <if-name>
```

MAC アドレスとルート ルックアップ

ブリッジ グループ内のトラフィックでは、パケットの発信インターフェイスは、ルート ルックアップではなく宛先 MAC アドレス ルックアップを実行することによって決定されます。

ただし、次の場合にはルート ルックアップが必要です。

- トラフィックの発信元が Firepower Threat Defense デバイス：syslog サーバなどがあるリモート ネットワーク宛てのトラフィック用に、Firepower Threat Defense デバイス にデフォルト/スタティック ルートを追加します。
- Voice over IP（VoIP）および TFTP トラフィック、エンドポイントが 1 ホップ以上離れている：セカンダリ接続が成功するように、リモートエンドポイント宛てのトラフィック用に、Firepower Threat Defense デバイス にスタティック ルートを追加します。Firepower Threat Defense デバイス は、セカンダリ接続を許可するためにアクセス コントロール ポリシーに一時的な「ピンホール」を作成します。セカンダリ接続ではプライマリ接続とは異なる IP アドレスのセットが使用される可能性があるため、Firepower Threat Defense デバイスは正しいインターフェイスにピンホールをインストールするために、ルート ルックアップを実行する必要があります。

  影響を受けるアプリケーションは次のとおりです。

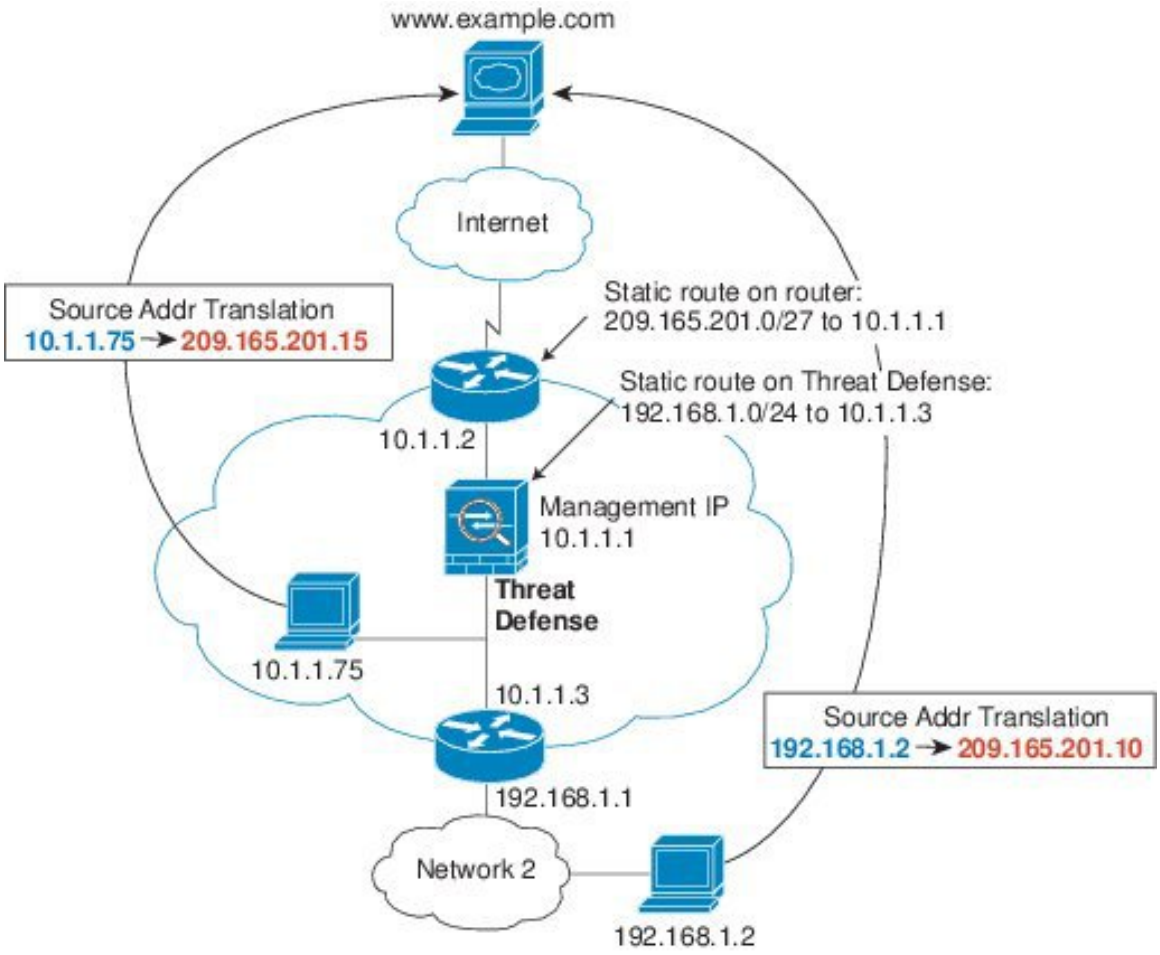
  - H.323
  - RTSP
  - SIP
  - Skinny（SCCP）
  - SQL*Net

- SunRPC
- TFTP

- Firepower Threat Defense デバイス が NAT を実行する 1 ホップ以上離れたトラフィック：リモート ネットワーク宛てのトラフィック用に、Firepower Threat Defense デバイス にスタティック ルートを設定します。また、Firepower Threat Defense デバイス に送信されるマッピング アドレス宛てのトラフィック用に、上流に位置するルータにもスタティック ルートが必要です。

  このルーティング要件は、NAT が有効になっている VoIP と DNS の、1 ホップ以上離れている組み込み IP アドレスにも適用されます。Firepower Threat Defense デバイス は、変換を実行できるように正しい出力インターフェイスを識別する必要があります。

図 *6 : NAT* の例：ブリッジ グループ内の *NAT*



トランスペアレント モードのブリッジ グループのサポートされていない機能

次の表に、トランスペアレント モードのブリッジ グループでサポートされない機能を示します。

表 *68 :* トランスペアレント モードでサポートされない機能

機能	説明
ダイナミック DNS	-
DHCP リレー	トランスペアレント ファイアウォールは DHCPv4 サーバとして機能することができますが、DHCP リレー コマンドはサポートしません。2 つのアクセス ルールを使用して DHCP トラフィックを通過させることができるので、DHCP リレーは必要ありません。1 つは内部インターフェイスから外部インターフェイスへの DHCP 要求を許可し、もう 1 つはサーバからの応答を逆方向に許可します。
ダイナミック ルーティング プロトコル	ただし、ブリッジグループ メンバー インターフェイスの場合、Firepower Threat Defense デバイス で発信されたトラフィックにスタティック ルートを追加できます。アクセス ルールを使用して、ダイナミック ルーティング プロトコルが Firepower Threat Defense デバイス を通過できるようにすることもできます。
マルチキャスト IP ルーティング	アクセス ルールで許可することによって、マルチキャスト トラフィックが Firepower Threat Defense デバイス を通過できるようにすることができます。
QoS	—
通過トラフィック用の VPN ターミネーション	トランスペアレント ファイアウォールは、ブリッジグループ メンバー インターフェイスでのみ、管理接続用のサイト間 VPN トンネルをサポートします。これは、Firepower Threat Defense デバイスを通過するトラフィックに対して VPN 接続を終端しません。アクセス ルールを使用して VPN トラフィックに ASA を通過させることはできますが、非管理接続は終端されません。

ルーテッド モードのブリッジ グループのサポートされていない機能

次の表に、ルーテッド モードのブリッジ グループでサポートされていない機能を示します。

表 *69 :* ルーテッド モードでサポートされていない機能

機能	説明
EtherChannel メンバー インターフェイス	物理インターフェイス、冗長インターフェイス、およびサブインターフェイスのみがブリッジ グループ メンバー インターフェイスとしてサポートされます。 診断 インターフェイスもサポートされていません。
クラスタ	クラスタリングではブリッジ グループはサポートされません。
ダイナミック DNS	-
DHCP リレー	ルーテッド ファイアウォールは DHCPv4 サーバとして機能しますが、BVI またはブリッジ グループ メンバー インターフェイス上での DHCP リレーはサポートしません。
ダイナミック ルーティング プロトコル	ただし、BVI のスタティック ルートを追加することはできます。アクセス ルールを使用して、ダイナミック ルーティング プロトコルが Firepower Threat Defense デバイス を通過できるようにすることもできます。非ブリッジ グループ インターフェイスはダイナミック ルーティングをサポートします。
マルチキャスト IP ルーティング	アクセス ルールで許可することによって、マルチキャスト トラフィックが Firepower Threat Defense デバイス を通過できるようにすることができます。非ブリッジ グループ インターフェイスはマルチキャスト ルーティングをサポートします。
QoS	非ブリッジ グループ インターフェイスは QoS をサポートします。

機能	説明
通過トラフィック用のVPNターミネーション	BVI で VPN 接続を終端することはできません。非ブリッジグループ インターフェイスは VPN をサポートします。 ブリッジグループ メンバーインターフェイスは、管理接続についてのみ、サイト間VPNトンネルをサポートします。これは、Firepower Threat Defense デバイスを通過するトラフィックに対してVPN接続を終端しません。アクセス ルールを使用して VPN トラフィックにブリッジ グループを通過させることはできますが、非管理接続は終端されません。

デフォルト設定

ブリッジグループのデフォルト

デフォルトでは、すべての ARP パケットはブリッジ グループ内で渡されます。

ファイアウォール モードのガイドライン

モデルのガイドライン

- ブリッジされた ixgbevf インターフェイスを持つ VMware 上の Firepower Threat Defense Virtual では、 のブリッジグループはサポートされません。
- Firepower 2100 シリーズでは、ルーテッド モードのブリッジ グループはサポートされません。
- Firepower Threat Defense Virtual では、ルーテッド モードのブリッジ グループはサポートされません。

ブリッジグループのガイドライン（トランスペアレントおよびルーテッドモード）

- 64のインターフェイスをもつブリッジ グループを 250 まで作成できます。
- 直接接続された各ネットワークは同一のサブネット上にある必要があります。
- Firepower Threat Defense デバイス では、セカンダリ ネットワーク上のトラフィックはサポートされていません。BVI IP アドレスと同じネットワーク上のトラフィックだけがサポートされています。

- IPv4 の場合は、管理トラフィックと、Firepower Threat Defense デバイス を通過するトラフィックの両方の各ブリッジ グループに対し、BVI の IP アドレスが必要です。IPv6 アドレスは BVI でサポートされますが必須ではありません。
- IPv6 アドレスは手動でのみ設定できます。
- BVI IP アドレスは、接続されたネットワークと同じサブネット内にある必要があります。サブネットにホスト サブネット（255.255.255.255）を設定することはできません。
- 管理インターフェイスはブリッジ グループのメンバーとしてサポートされません。
- Firepower 4100/9300 では、データ共有インターフェイスはブリッジ グループのメンバーとしてサポートされません。
- トランスペアレント モードでは、少なくとも 1 つのブリッジ グループを使用し、データ インターフェイスがブリッジ グループに属している必要があります。
- トランスペアレント モードでは、接続されたデバイス用のデフォルト ゲートウェイとして BVI IP アドレスを指定しないでください。デバイスは Firepower Threat Defense デバイス の他方側のルータをデフォルト ゲートウェイとして指定する必要があります。
- トランスペアレント モードでは、管理トラフィックの戻りパスを指定するために必要な *default* ルートは、1 つのブリッジ グループ ネットワークからの管理トラフィックにだけ適用されます。これは、デフォルト ルートはブリッジ グループのインターフェイスとブリッジ グループ ネットワークのルータ IP アドレスを指定しますが、ユーザは 1 つのデフォルト ルートしか定義できないためです。複数のブリッジ グループ ネットワークからの管理トラフィックが存在する場合は、管理トラフィックの発信元ネットワークを識別する標準のスタティック ルートを指定する必要があります。
- トランスペアレント モードでは、PPPoE は 診断 インターフェイスでサポートされません。
- ルーテッドモードでは、ブリッジグループと他のルーテッドインターフェイスの間をルーティングするために、BVI を指定する必要があります。
- ルーテッド モードでは、FTD 定義の EtherChannel インターフェイスがブリッジ グループのメンバーとしてサポートされません。Firepower 4100/9300 上の Etherchannel は、ブリッジ グループ メンバーにすることができます。
- Bidirectional Forwarding Detection（BFD）エコー パケットは、ブリッジ グループ メンバを使用するときに、FTD を介して許可されません。BFD を実行している FTD の両側に 2 つのネイバーがある場合、FTD は BFD エコー パケットをドロップします。両方が同じ送信元および宛先 IP アドレスを持ち、LAND 攻撃の一部であるように見えるからです。

ファイアウォール モードの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin Access Admin Network Admin

ファイアウォール モードは、最初のシステム セットアップの実行時に CLI で設定できます。セットアップ時にファイアウォールモードを設定することをお勧めします。これは、ファイアウォールモードを変更すると、非適合の設定が発生しないように設定が消去されるためです。ファイアウォール モードの変更が後で必要になった場合は、CLI から変更する必要があります。

ステップ 1 FMC から FTD デバイスの登録を解除します。

モードの変更は、デバイスの登録を解除するまで実行できません。

a) **[デバイス（Devices）] > [デバイス管理（Device Management）]** を選択します。
b) 管理対象デバイスのリストから、デバイスを選択します。
c) デバイスを削除（ゴミ箱アイコンをクリック）して、確認してから、システムがデバイスを削除するまで待機します。

ステップ 2 FTD デバイスの CLI にアクセスします。可能ならばコンソール ポートからアクセスします。

診断インターフェイスへの SSH を使用している場合、モードを変更すると、インターフェイスの設定が消去され、切断されます。代わりに、管理インターフェイスに接続する必要があります。

ステップ 3 ファイアウォール モードを変更します。

configure firewall [**routed** | **transparent**]

例：

```
> configure firewall transparent
This will destroy the current interface configurations, are you sure that you want to proceed? [y/N]
 y
The firewall mode was changed successfully.
```

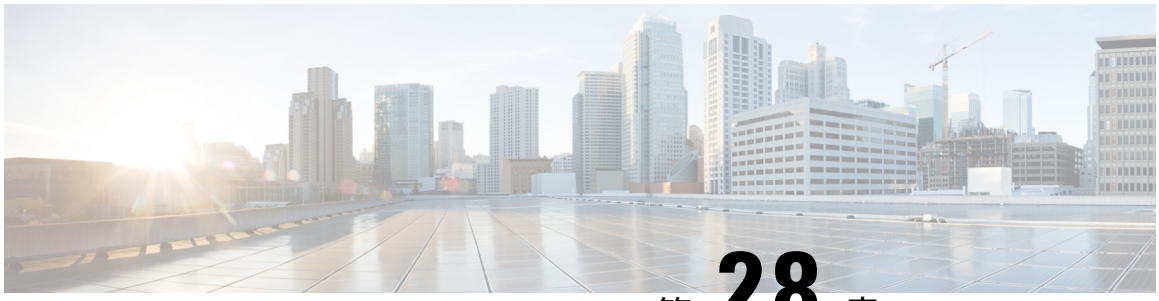
ステップ 4 FMC に再登録します。

configure manager add {*hostname* | *ip_address* | **DONTRESOLVE**} *reg_key* [*nat_id*]

引数の説明

- {*hostname* | *ip_address* | **DONTRESOLVE** } は、FMC の完全修飾ホスト名または IP アドレスのいずれかを指定します。FMC を直接アドレス指定できない場合は、**DONTRESOLVE** を使用します。
- *reg_key* はデバイスを FMC へ登録するのに必要な英数字の一意の登録キーです。

- *nat_id* は、FMC とデバイス間の登録プロセス中に使用されるオプションの英数字文字列です。これは、ホスト名が **DONTRESOLVE** に設定されている場合に必要です。



第 28 章

の Firepower Threat Defense の論理デバイス Firepower 4100/9300

Firepower 4100/9300 は柔軟なセキュリティ プラットフォームが 1 つまたは複数の論理デバイスをインストールすることができます。FTD を FMC に追加する前に、シャーシ インターフェイスを設定し、論理デバイスを追加し、Firepower Chassis Manager または FXOS の CLI を使用して Firepower 4100/9300 シャーシ上のデバイスにインターフェイスを割り当てる必要があります。この章では、基本的なインターフェイスの設定、および Firepower Chassis Manager を使用したスタンドアロンまたはハイ アベイラビリティ論理デバイスの追加方法について説明します。クラスタ化された論理デバイスを追加する場合は、Firepower Threat Defense 用のクラスタリング （907 ページ）を参照してください。FXOS CLI を使用する場合は、FXOS CLI コンフィギュレーション ガイドを参照してください。高度な FXOS の手順とトラブルシューティングについては、FXOS コンフィギュレーション ガイドを参照してください。

Firepower インターフェイスについて

Firepower 4100/9300 シャーシは、物理インターフェイス、コンテナ インスタンスの LAN サブインターフェイス、および EtherChannel（ポートチャネル）インターフェイスをサポートします。EtherChannel のインターフェイスには、同じタイプのメンバインターフェイスを最大で 16 個含めることができます。

シャーシ管理インターフェイス

シャーシ管理インターフェイスは、SSH または Firepower Chassis Manager で、FXOS シャーシの管理に使用されます。このインターフェイスはMGMTとして、[Interfaces] タブの上部に表示されます。[Interfaces] タブでは、このインターフェイスの有効化または無効化のみを実行できます。このインターフェイスは、アプリケーション管理の論理デバイスに割り当てる管理タイプのインターフェイスから分離されています。

このインターフェイスのパラメータを設定するには、CLIから設定にする必要があります。このインターフェイスについての情報を FXOS CLI で表示するには、ローカル管理に接続し、管理ポートを表示します。

FirePOWER **connect local-mgmt**

firepower(local-mgmt) # **show mgmt-port**

物理ケーブルまたは SFP モジュールが取り外されている場合や **mgmt-port shut** コマンドが実行されている場合でも、シャーシ管理インターフェイスは稼働状態のままである点に注意してください。

インターフェイス タイプ

各インターフェイスは、次のいずれかのタイプになります。

- Data：通常のデータに使用します。データ インターフェイスは論理デバイス間で共有できません。データ インターフェイスを論理デバイス間で共有することはできません。また、論理デバイスからバックプレーンを介して他の論理デバイスに通信することはできません。データ インターフェイスのトラフィックの場合、すべてのトラフィックは別の論理デバイスに到達するために、あるインターフェイスでシャーシを抜け出し、別のインターフェイスで戻る必要があります。

- Data-sharing：通常のデータに使用します。コンテナ インスタンスでのみサポートされ、これらのデータ インターフェイスは 1 つまたは複数の論理デバイス/コンテナ インスタンス（FTD 専用）で共有できます。各コンテナ インスタンスは、このインターフェイスを共有する他のすべてのインスタンスと、バック プレーン経由で通信できます。共有インターフェイスは、展開可能なコンテナインスタンスの数に影響を及ぼすことがあります。を参照してください。共有インターフェイスの拡張性 （727ページ）共有インターフェイスは、ブリッジ グループ メンバー インターフェイス（トランスペアレント モードまたはルーテッド モード）、インライン セット、パッシブ インターフェイス、またはフェールオーバー リンクではサポートされません。

- Mgmt：アプリケーション インスタンスの管理に使用します。これらのインターフェイスは、外部ホストにアクセスするために1つまたは複数の論理デバイスで共有できます。論理デバイスが、このインターフェイスを介して、インターフェイスを共有する他の論理デバイスと通信することはできません。各論理デバイスには、管理インターフェイスを1つだけ割り当てることができます。個別のシャーシ管理インターフェイスについては、シャーシ管理インターフェイス （726 ページ）を参照してください。

- Firepower-eventing：FTD デバイスのセカンダリ管理インターフェイスとして使用します。このインターフェイスを使用するには、FTD CLI で IP アドレスなどのパラメータを設定する必要があります。たとえば、イベント（Web イベントなど）から管理トラフィックを分類できます。 管理インターフェイス （1266 ページ）を参照してください。
  Firepower-eventing インターフェイスは、外部ホストにアクセスするために 1 つまたは複数の論理デバイスで共有できます。論理デバイスはこのインターフェイスを介してインターフェイスを共有する他の倫理デバイスと通信することはできません。
- Cluster：クラスタ化された論理デバイスのクラスタ制御リンクとして使用します。デフォルトでは、クラスタ制御リンクは 48 番のポートチャネル上に自動的に作成されます。このタイプは、EtherChannel インターフェイスのみでサポートされます。

シャーシとアプリケーションの独立したインターフェイスの状態

管理上、シャーシとアプリケーションの両方で、インターフェイスを有効および無効にできます。インターフェイスを動作させるには、両方のオペレーティング システムで、インターフェイスを有効にする必要があります。インターフェイスの状態は個別に制御されるので、シャーシとアプリケーションの間に不一致が生じることがあります。

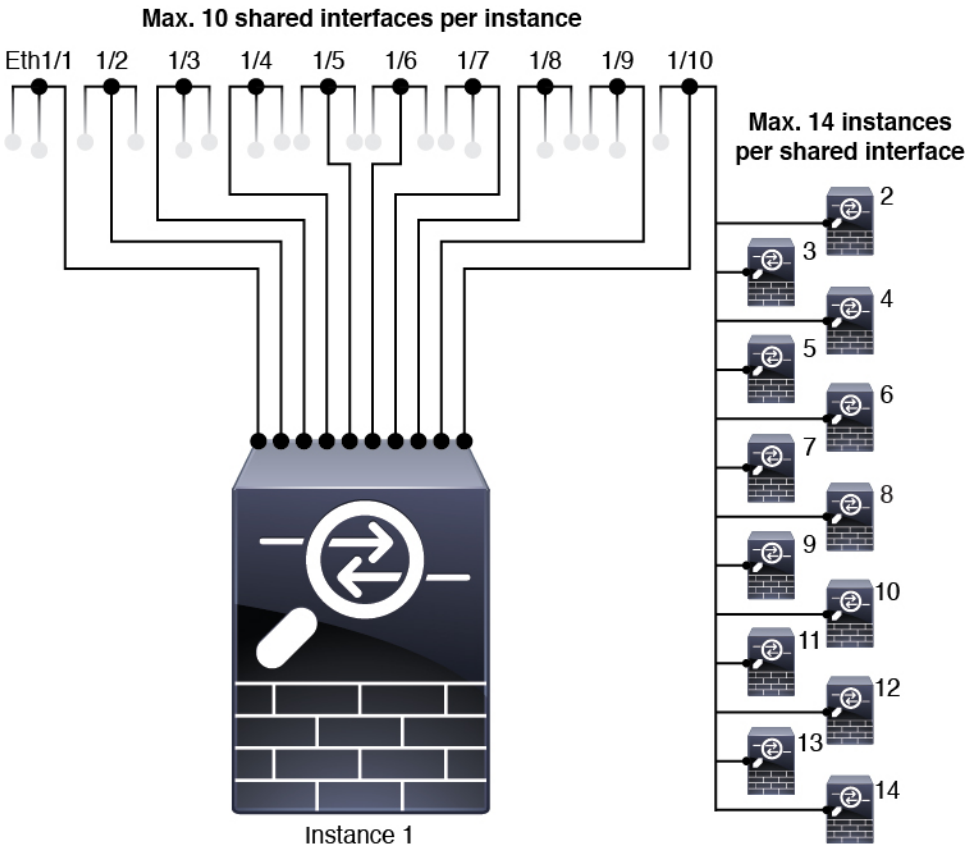
アプリケーションにおけるインターフェイスのデフォルトの状態は、インターフェイスのタイプによって異なります。たとえば、物理インターフェイスまたは EtherChannel は、アプリケーション内ではデフォルトで無効になっていますが、サブインターフェイスはデフォルトで有効になっています。

共有インターフェイスの拡張性

コンテナ インスタンスは、data-sharing タイプのインターフェイスを共有できます。この機能を使用して、物理インターフェイスの使用率を節約し、柔軟なネットワークの導入をサポートできます。インターフェイスを共有する場合、シャーシは一意の MAC アドレスを使用して適切なインスタンスにトラフィックを転送します。ただし、共有インターフェイスを使用すると、シャーシ内にフルメッシュトポロジが必要になるため、転送テーブルのサイズが大きくなることがあります（すべてのインスタンスが同じインターフェイスを共有している他のすべてのインスタンスと通信できる必要があります）。そのため、共有できるインターフェイスの数には制限があります。

転送テーブルに加えて、シャーシは VLAN サブインターフェイスの転送用に VLAN グループテーブルも保持します。親インターフェイスの数とその他の導入決定に応じて、最大 500 個の VLAN サブインターフェイスを作成できます。

共有インターフェイスの割り当てについては、次の制限事項を参照してください。



共有インターフェイスのベスト プラクティス

転送テーブルの拡張性を最適にするには、共有するインターフェイスの数をできる限り少なくします。代わりに、1 つまたは複数の物理インターフェイスに最大 500 個の VLAN サブインターフェイスを作成し、コンテナ インスタンスで VLAN を分割できます。

インターフェイスを共有する場合は、拡張性が高いものから低いものへの順序で次の手順に従います。

1. 最適：単一の親の下のサブインターフェイスを共有し、論理デバイス グループと同じサブインターフェイスのセットを使用します。

   たとえば、同じ種類のインターフェイスをすべてバンドルするための大規模な EtherChannel を作成し、Port-Channel1、Port-Channel2、Port-Channel3 の代わりに、その EtherChannel のサブインターフェイス（Port-Channel1.100、200、300）を共有します。単一の親のサブインターフェイスを共有する場合、物理/EtherChannel インターフェイスまたは複数の親にわたるサブインターフェイスを共有するときの VLAN グループ テーブルの拡張性は転送テーブルよりも優れています。

   論理デバイスのグループと同じサブインターフェイスのセットを共有しない場合は、（VLAN グループよりも）より多くのリソースを設定で使用することになる可能性があります。たとえば、Port-Channel1.100 を論理デバイス 1 および 2 と共有するとともに、Port-Channel1.200

を論理デバイス 2 および 3 と共有するのではなく、Port-Channel1.100 および 200 を論理デバイス 1、2、3（1 つの VLAN グループ）と共有します。

2. 普通：親の間でサブインターフェイスを共有します。

   たとえば、Port-Channel1、Port-Channel2、Port-Channel3 の代わりに Port-Channel1.100、Port-Channel2.200、Port-Channel3.300 を共有します。この使用方法は同じ親のサブインターフェイスのみを共有するよりも効率は劣りますが、VLAN グループを利用しています。

3. 最悪：個々の親インターフェイス（物理または EtherChannel）を共有します。

   この方法は、最も多くの転送テーブル エントリを使用します。

共有インターフェイスの使用例

インターフェイスの共有と拡張性の例について、以下の表を参照してください。以下のシナリオは、すべてのインスタンス間で共有されている管理用の 1 つの物理/EtherChannel インターフェイスと、ハイ アベイラビリティで使用する専用のサブインターフェイスを含むもう 1 つの物理/EtherChannel インターフェイスを使用していることを前提としています。

- 表 70 : 3 つの SM-44 を備えた Firepower 9300 の物理/EtherChannel インターフェイスとインスタンス （730 ページ）
- 表 71 : 3 つの SM-44 を備えた Firepower 9300 上の 1 つの親のサブインターフェイスとインスタンス （732 ページ）
- 表 72 : 1 つの SM-44 を備えた Firepower 9300 の物理/EtherChannel インターフェイスとインスタンス （734 ページ）
- 表 73 : 1 つの SM-44 を備えた Firepower 9300 上の 1 つの親のサブインターフェイスとインスタンス （736 ページ）

3 つの SM-44 と firepower 9300

次の表は、物理インターフェイスまたはEtherchannelのみを使用している9300のSM-44セキュリティモジュールに適用されます。サブインターフェイスがなければ、インターフェイスの最大数が制限されます。さらに、複数の物理インターフェイスを共有するには、複数のサブインターフェイスを使用するよりも多くの転送テーブル リソースを使用します。

各 SM-44 モジュールは、最大 14 のインスタンスをサポートできます。インスタンスは、制限内に収める必要に応じてモジュール間で分割されます。

表 *70 : 3* つの *SM-44* を備えた *Firepower 9300* の物理*/EtherChannel* インターフェイスとインスタンス

専用インターフェイス	共有インターフェイス	インスタンス数	転送テーブルの使用率（%）
32： • 8 • 8 • 8 • 8	**0**	**4**： • インスタンス 1 • インスタンス 2 • インスタンス 3 • インスタンス 4	16 %
30： • 15 • 15	**0**	**2:** • インスタンス 1 • インスタンス 2	14%
14： • 14（1 ea.）	**1**	**14**： • インスタンス 1 - インスタンス 14	46 %
33： • 11（1 ea.） • 11（1 ea.） • 11（1 ea.）	**3**： • 1 • 1 • 1	**33**： • インスタンス 1 - インスタンス 11 • インスタンス 12 - インスタンス 22 • インスタンス 23 - インスタンス 33	98%
33： • *11*（*1 ea.*） • *11*（*1 ea.*） • *12*（*1 ea.*）	*3*： • *1* • *1* • *1*	*34*： • インスタンス *1* - インスタンス *11* • インスタンス *12* - インスタンス *22* • インスタンス *23* - インスタンス *34*	*102 %* 許可しない
30： • 30（1 ea.）	**1**	**6**： • インスタンス 1 - インスタンス 6	25 %

専用インターフェイス	共有インターフェイス	インスタンス数	転送テーブルの使用率（%）
30： • 10（5 ea.） • 10（5 ea.） • 10（5 ea.）	**3**： • 1 • 1 • 1	**6**： • インスタンス 1 - インスタンス 2 • インスタンス 2 - インスタンス 4 • インスタンス 5 - インスタンス 6	23 %
30： • 30（6 ea.）	**2**	**5**： • インスタンス 1 - インスタンス 5	28%
30： • 12（6 ea.） • 18（6 ea.）	**4**： • 2 • 2	**5**： • インスタンス 1 - インスタンス 2 • インスタンス 2 - インスタンス 5	26 %
24： • 6 • 6 • 6 • 6	**7**	**4**： • インスタンス 1 • インスタンス 2 • インスタンス 3 • インスタンス 4	44 %
24： • 12（6 ea.） • 12（6 ea.）	**14**： • 7 • 7	**4**： • インスタンス 1 - インスタンス 2 • インスタンス 2 - インスタンス 4	41%

次の表は、単一の親物理インターフェイス上でサブインターフェイスを使用している 9300 上の 3 つの SM-44 セキュリティ モジュールに適用されます。たとえば、同じ種類のインターフェイスをすべてバンドルするための大規模な EtherChannel を作成し、EtherChannel のサブインターフェイスを共有します。複数の物理インターフェイスを共有するには、複数のサブインターフェイスを使用するよりも多くの転送テーブル リソースを使用します。

各 SM-44 モジュールは、最大 14 のインスタンスをサポートできます。インスタンスは、制限内に収める必要に応じてモジュール間で分割されます。

表 *71 : 3* つの *SM-44* を備えた *Firepower 9300* 上の *1* つの親のサブインターフェイスとインスタンス

専用サブインターフェイス	共有サブインターフェイス	インスタンス数	転送テーブルの使用率（%）
168： • 168（4 ea.）	**0**	**42**： • インスタンス 1 - インスタンス 42	33%
224： • 224（16 ea.）	**0**	**14**： • インスタンス 1 - インスタンス 14	27 %
14： • 14（1 ea.）	**1**	**14**： • インスタンス 1 - インスタンス 14	46 %
33： • 11（1 ea.） • 11（1 ea.） • 11（1 ea.）	**3**： • 1 • 1 • 1	**33**： • インスタンス 1 - インスタンス 11 • インスタンス 12 - インスタンス 22 • インスタンス 23 - インスタンス 33	98%
70： • 70（5 ea.）	**1**	**14**： • インスタンス 1 - インスタンス 14	46 %
165： • 55（5 ea.） • 55（5 ea.） • 55（5 ea.）	**3**： • 1 • 1 • 1	**33**： • インスタンス 1 - インスタンス 11 • インスタンス 12 - インスタンス 22 • インスタンス 23 - インスタンス 33	98%

専用サブインターフェイス	共有サブインターフェイス	インスタンス数	転送テーブルの使用率（%）
70： • 70（5 ea.）	**2**	**14**： • インスタンス 1 - インスタンス 14	46 %
165： • 55（5 ea.） • 55（5 ea.） • 55（5 ea.）	**6**： • 2 • 2 • 2	**33**： • インスタンス 1 - インスタンス 11 • インスタンス 12 - インスタンス 22 • インスタンス 23 - インスタンス 33	98%
70： • 70（5 ea.）	**10**	**14**： • インスタンス 1 - インスタンス 14	46 %
165： • *55（5 ea.）* • *55（5 ea.）* • *55（5 ea.）*	***30***： • *10* • *10* • *10*	***33***： • インスタンス *1* - インスタンス *11* • インスタンス *12* - インスタンス *22* • インスタンス *23* - インスタンス *33*	*102 %* 許可しない

1 つの SM 44 を備えた Firepower 9300

次の表は、物理インターフェイスまたは Etherchannel のみを使用している 1 つの SM-44 を備えた Firepower 9300 に適用されます。サブインターフェイスがなければ、インターフェイスの最大数が制限されます。さらに、複数の物理インターフェイスを共有するには、複数のサブインターフェイスを使用するよりも多くの転送テーブル リソースを使用します。

1 つの SM-44 を備えた Firepower Firepower 9300 は、最大 14 のインスタンスをサポートできます。

表 *72 : 1* つの *SM-44* を備えた *Firepower 9300* の物理*/EtherChannel* インターフェイスとインスタンス

専用インターフェイス	共有インターフェイス	インスタンス数	転送テーブルの使用率（%）
32： • 8 • 8 • 8 • 8	**0**	**4**： • インスタンス 1 • インスタンス 2 • インスタンス 3 • インスタンス 4	16 %
30： • 15 • 15	**0**	**2:** • インスタンス 1 • インスタンス 2	14%
14： • 14（1 ea.）	**1**	**14**： • インスタンス 1 - インスタンス 14	46 %
14： • 7（1 ea.） • 7（1 ea.）	**2:** • **1** • **1**	**14**： • インスタンス 1 - インスタンス 7 • インスタンス 8 - インスタンス 14	37 %
32： • 8 • 8 • 8 • 8	**1**	**4**： • インスタンス 1 • インスタンス 2 • インスタンス 3 • インスタンス 4	21 %
32： • 16（8 ea.） • 16（8 ea.）	**2**	**4**： • インスタンス 1 - インスタンス 2 • インスタンス 3 - インスタンス 4	20 %

専用インターフェイス	共有インターフェイス	インスタンス数	転送テーブルの使用率（%）
32： • 8 • 8 • 8 • 8	**2**	**4**： • インスタンス 1 • インスタンス 2 • インスタンス 3 • インスタンス 4	25 %
32： • 16（8 ea.） • 16（8 ea.）	**4**： • 2 • 2	**4**： • インスタンス 1 - インスタンス 2 • インスタンス 3 - インスタンス 4	24 %
24： • 8 • 8 • 8	**8**	**3**： • インスタンス 1 • インスタンス 2 • インスタンス 3	37 %
10： • 10（2 ea.）	**10**	**5**： • インスタンス 1 - インスタンス 5	69%
10： • 6（2 ea.） • 4（2 ea.）	**20**： • 10 • 10	**5**： • インスタンス 1 - インスタンス 3 • インスタンス 4 - インスタンス 5	59%
14： • *12*（*2 ea.*）	***10***	*7*： • インスタンス *1* - インスタンス *7*	*109%* 許可しない

次の表は、単一の親物理インターフェイス上でサブインターフェイスを使用している 1 つの SM-44 を備えた Firepower 4150 に適用されます。たとえば、同じ種類のインターフェイスをすべてバンドルするための大規模な EtherChannel を作成し、EtherChannel のサブインターフェイ

スを共有します。複数の物理インターフェイスを共有するには、複数のサブインターフェイスを使用するよりも多くの転送テーブル リソースを使用します。

1 つの SM-44 を備えた Firepower 9300 は、最大 14 のインスタンスをサポートできます。

表 *73 : 1* つの *SM-44* を備えた *Firepower 9300* 上の *1* つの親のサブインターフェイスとインスタンス

専用サブインターフェイス	共有サブインターフェイス	インスタンス数	転送テーブルの使用率（%）
112： • 112（8 ea.）	**0**	**14**： • インスタンス 1 - インスタンス 14	17%
224： • 224（16 ea.）	**0**	**14**： • インスタンス 1 - インスタンス 14	17%
14： • 14（1 ea.）	**1**	**14**： • インスタンス 1 - インスタンス 14	46 %
14： • 7（1 ea.） • 7（1 ea.）	**2:** • 1 • 1	**14**： • インスタンス 1 - インスタンス 7 • インスタンス 8 - インスタンス 14	37 %
112： • 112（8 ea.）	**1**	**14**： • インスタンス 1 - インスタンス 14	46 %
112： • 56（8 ea.） • 56（8 ea.）	**2:** • 1 • 1	**14**： • インスタンス 1 - インスタンス 7 • インスタンス 8 - インスタンス 14	37 %
112： • 112（8 ea.）	**2**	**14**： • インスタンス 1 - インスタンス 14	46 %

専用サブインターフェイス	共有サブインターフェイス	インスタンス数	転送テーブルの使用率（%）
112： • 56（8 ea.） • 56（8 ea.）	**4**： • 2 • 2	**14**： • インスタンス 1 - インスタンス 7 • インスタンス 8 - インスタンス 14	37 %
140： • 140（10 ea.）	**10**	**14**： • インスタンス 1 - インスタンス 14	46 %
140： • 70（10 ea.） • 70（10 ea.）	**20**： • 10 • 10	**14**： • インスタンス 1 - インスタンス 7 • インスタンス 8 - インスタンス 14	37 %

共有インターフェイス リソースの表示

転送テーブルと VLAN グループの使用状況を表示するには、**scope fabric-interconnect** で **show detail** コマンドを入力します。次に例を示します。

```
Firepower# scope fabric-interconnect
DFirepower /fabric-interconnect # show detail

Fabric Interconnect:
    ID: A
    Product Name: Cisco FPR9K-SUP
    PID: FPR9K-SUP
    VID: V02
    Vendor: Cisco Systems, Inc.
    Serial (SN): JAD104807YN
    HW Revision: 0
    Total Memory (MB): 16185
    OOB IP Addr: 10.10.5.14
    OOB Gateway: 10.10.5.1
    OOB Netmask: 255.255.255.0
    OOB IPv6 Address: ::
    OOB IPv6 Gateway: ::
    Prefix: 64
    Operability: Operable
    Thermal Status: Ok
    Ingress VLAN Group Entry Count (Current/Max): 0/500
    Switch Forwarding Path Entry Count (Current/Max): 16/1021
    Current Task 1:
    Current Task 2:
```

```
Current Task 3:
```

Firepower Threat Defense のインライン セット リンク ステートの伝達

インラインセットはワイヤ上のバンプのように動作し、2つのインターフェイスを一緒にバインドし、既存のネットワークに組み込みます。この機能によって、隣接するネットワーク デバイスの設定がなくても、任意のネットワーク環境にシステムをインストールすることができます。インラインインターフェイスはすべてのトラフィックを無条件に受信しますが、これらのインターフェイスで受信されたすべてのトラフィックは、明示的にドロップされない限り、インライン セットの外部に再送信されます。

FTD アプリケーションでインライン セットを設定し、リンク ステート伝達を有効にすると、FTD はインライン セット メンバーシップを FXOS シャーシに送信します。リンク ステート伝達により、インラインセットのインターフェイスの1つが停止した場合、シャーシは、インライン インターフェイス ペアの 2 番目のインターフェイスも自動的に停止します。停止したインターフェイスが再び起動すると、2番目のインターフェイスも自動的に起動します。つまり、1つのインターフェイスのリンク ステートが変化すると、シャーシはその変化を検知し、その変化に合わせて他のインターフェイスのリンク ステートを更新します。ただし、シャーシからリンク ステートの変更が伝達されるまで最大 4 秒かかります。障害状態のネットワーク デバイスを避けてトラフィックを自動的に再ルーティングするようルータが設定された復元力の高いネットワーク環境では、リンク ステート伝播が特に有効です。

論理デバイスについて

論理デバイスでは、1 つのアプリケーション インスタンス（ASA または Firepower Threat Defense のいずれか）および 1 つのオプション デコレータ アプリケーション（Radware DefensePro）を実行し、サービス チェーンを形成できます。

論理デバイスを追加するときに、アプリケーション インスタンスのタイプおよびバージョンの定義、インターフェイスの割り当て、アプリケーション構成にプッシュされるブートストラップ設定の構成も行います。

（注） Firepower 9300 の場合、異なるアプリケーションタイプ（ASA および FTD）をシャーシ内の個々のモジュールにインストールできます。別個のモジュールでは、異なるバージョンのアプリケーション インスタンス タイプも実行できます。

スタンドアロン論理デバイスとクラスタ化論理デバイス

次の論理デバイス タイプを追加できます。

- スタンドアロン：スタンドアロン論理デバイスは、スタンドアロン ユニットまたはハイアベイラビリティ ペアのユニットとして動作します。

- クラスタ：クラスタ化論理デバイスを使用すると複数の装置をグループ化することで、単一デバイスのすべての利便性（管理、ネットワークへの統合）を提供し、同時に複数デバイスによる高いスループットと冗長性を実現できます。Firepower 9300 などの複数のモジュール デバイスが、シャーシ内クラスタリングをサポートします。Firepower 9300 のすべての 3 つのモジュール アプリケーション インスタンスは、1 つの論理デバイスに属しています。

（注） Firepower 9300 の場合、すべてのモジュールがクラスタに属している必要があります。1 つのセキュリティ モジュールにスタンドアロン論理デバイスを作成し、残り 2 つのセキュリティ モジュールを使用してクラスタを作成することはできません。

論理デバイスのアプリケーションインスタンス：コンテナとネイティブ

アプリケーション インスタンスは次の展開タイプで実行します。

- ネイティブ インスタンス：ネイティブ インスタンスはセキュリティモジュール/エンジンのすべてのリソース（CPU、RAM、およびディスク容量）を使用するため、ネイティブ インスタンスを 1 つだけインストールできます。
- コンテナ インスタンス：コンテナ インスタンスでは、セキュリティモジュール/エンジンのリソースのサブセットを使用するため、複数のコンテナインスタンスをインストールできます。マルチインスタンス機能は、FMC を使用する Firepower Threat Defense でのみサポートされています。ASA ではサポートされていません。

（注） マルチインスタンス機能は、実装は異なりますが、ASA マルチ コンテキスト モードに似ています。マルチ コンテキスト モードでは、単一のアプリケーション インスタンスがパーティション化されますが、マルチインスタンス機能では、独立したコンテナインスタンスを使用できます。コンテナインスタンスでは、ハードリソースの分離、個別の構成管理、個別のリロード、個別のソフトウェア アップデート、および Firepower Threat Defense のフル機能のサポートが可能です。マルチ コンテキスト モードでは、共有リソースのおかげで、特定のプラットフォームでより多くのコンテキストをサポートできます。マルチ コンテキスト モードは Firepower Threat Defense では利用できません。

Firepower 9300 の場合、一部のモジュールでネイティブ インスタンスを使用し、他のモジュールではコンテナ インスタンスを使用することができます。

コンテナ インスタンス インターフェイス

コンテナ インターフェイスでの柔軟な物理インターフェイスの使用を可能にするため、FXOSでVLANサブインターフェイスを作成し、複数のインスタンス間でインターフェイス（VLANまたは物理）を共有することができます。ネイティブのインスタンスは、VLANサブインターフェイスまたは共有インターフェイスを使用できません。共有インターフェイスの拡張性（727ページ）およびコンテナ インスタンスへのVLANサブインターフェイスの追加（759ページ）を参照してください。

シャーシがパケットを分類する方法

シャーシに入ってくるパケットはいずれも分類する必要があります。その結果、シャーシは、どのインスタンスにパケットを送信するかを決定できます。

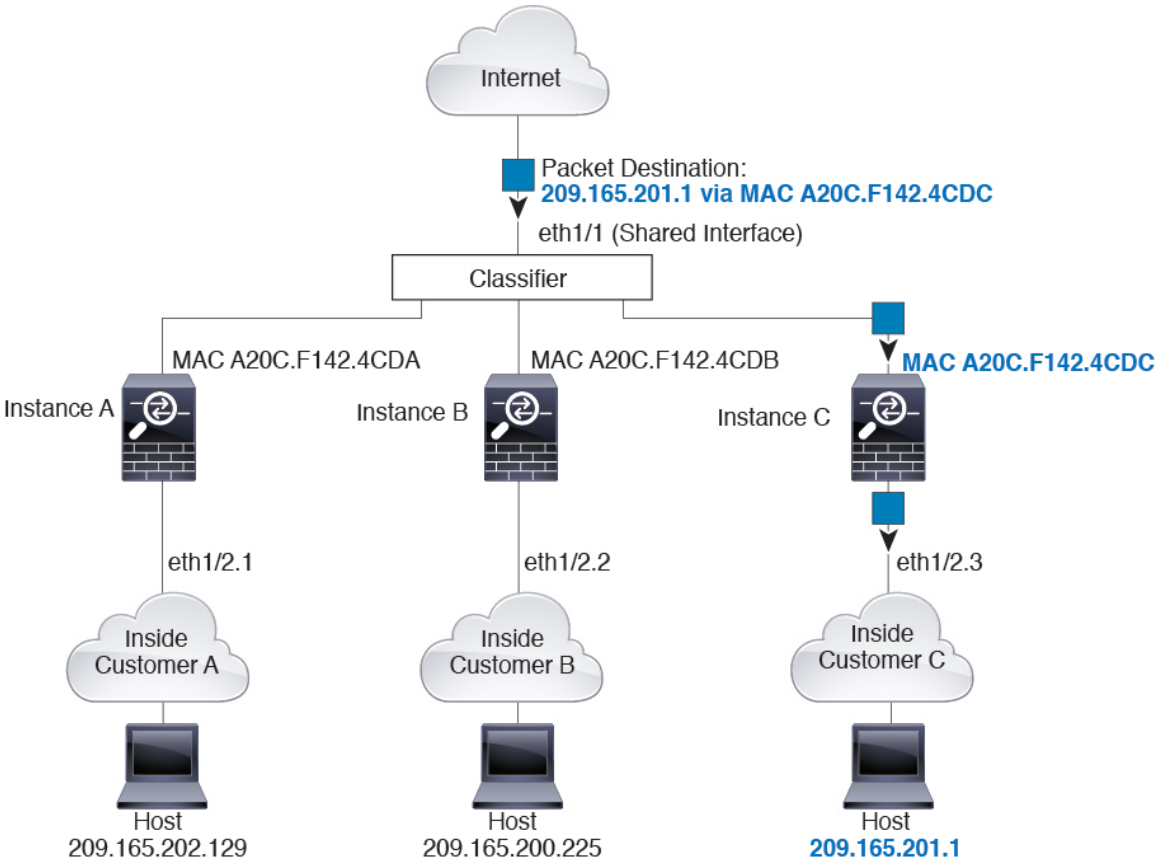
- 一意のインターフェイス：1つのインスタンスしか入力インターフェイスに関連付けられていない場合、シャーシはそのインスタンスにパケットを分類します。ブリッジグループメンバー インターフェイス（トランスペアレント モードまたはルーテッド モード）、インライン セット、またはパッシブ インターフェイスの場合は、この方法を常にパケットの分類に使用します。
- 一意のMACアドレス：シャーシは、共有インターフェイスを含むすべてのインターフェイスに一意のMACアドレスを自動的に生成します。複数のインスタンスが同じインターフェイスを共有している場合、分類子には各インスタンスでそのインターフェイスに割り当てられた固有のMACアドレスが使用されます。固有のMACアドレスがないと、アップストリームルータはインスタンスに直接ルーティングできません。アプリケーション内で各インターフェイスを設定するときに、手動でMACアドレスを設定することもできます。ただし、MACアドレスを手動で設定すると、サブインターフェイスを共有していない場合でも、分類が正しく行われるように同じ親インターフェイス上のすべてのサブインターフェイスで固有のMACアドレスを使用します。

（注） 宛先MACアドレスがマルチキャストまたはブロードキャストMACアドレスの場合、パケットが複製されて各インスタンスに送信されます。

分類例

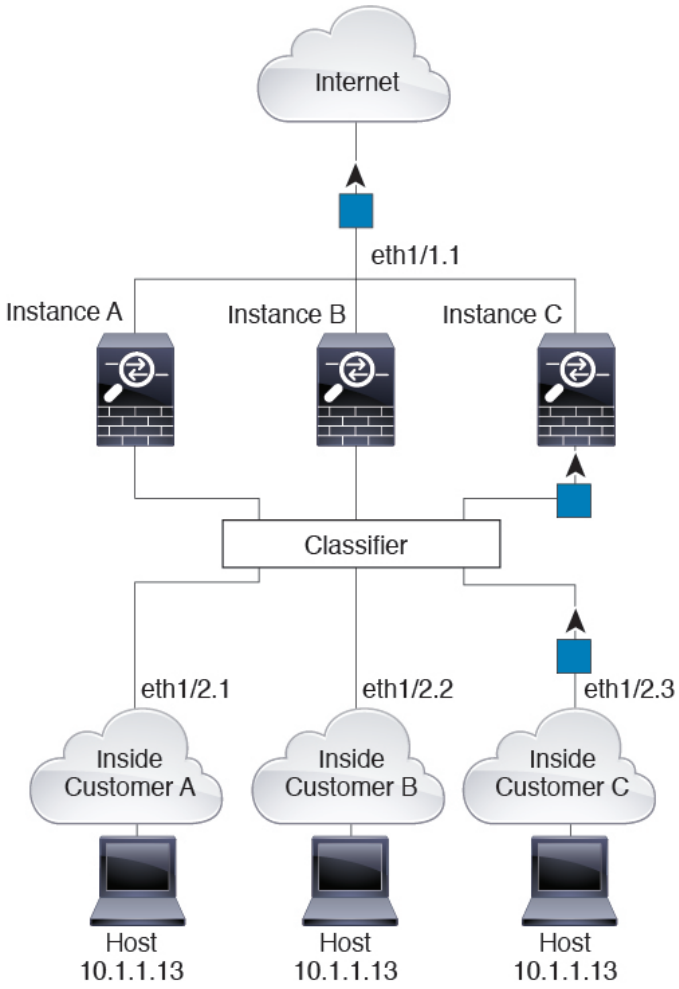
次の図に、外部インターフェイスを共有する複数のインスタンスを示します。インスタンスCにはルータがパケットを送信するMACアドレスが含まれているため、分類子はパケットをインスタンスCに割り当てます。

図 *7*: ***MAC*** アドレスを使用した共有インターフェイスのパケット分類



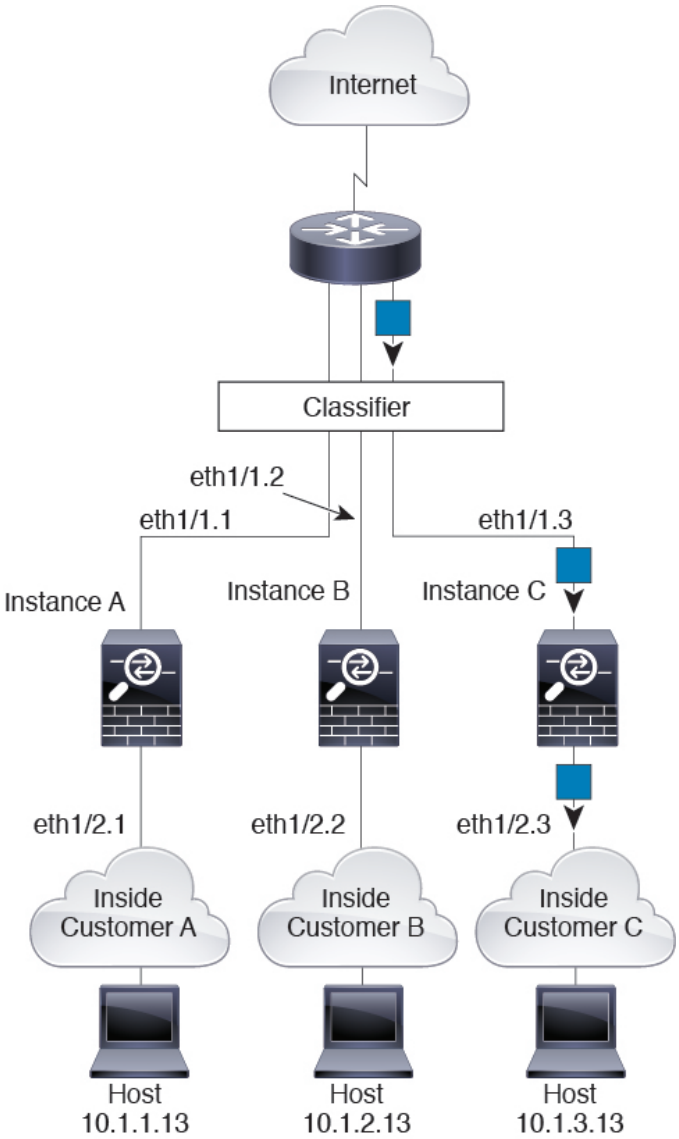
内部ネットワークからのものを含め、新たに着信するトラフィックすべてが分類される点に注意してください。次の図に、インターネットにアクセスするネットワーク内のインスタンスCのホストを示します。分類子は、パケットをインスタンスCに割り当てます。これは、入力インターフェイスがイーサネット 1/2.3 で、このイーサネットがインスタンス C に割り当てられているためです。

図 *8*: 内部ネットワークからの着信トラフィック



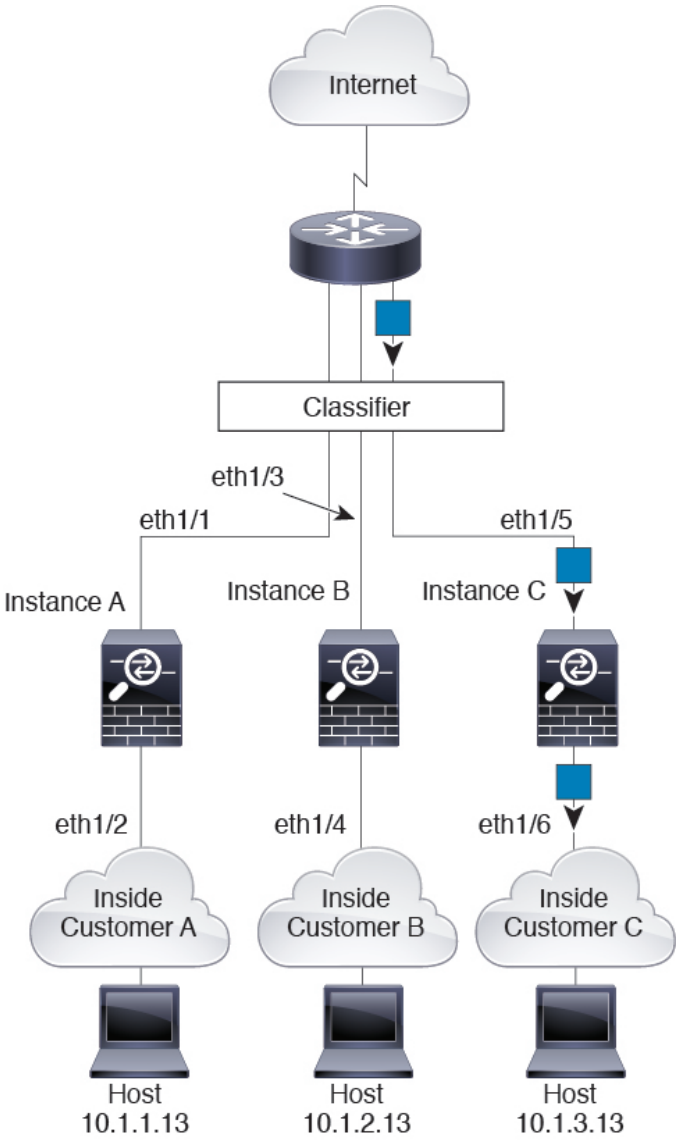
トランスペアレントファイアウォールでは、固有のインターフェイスを使用する必要があります。次の図に、ネットワーク内のインスタンスCのホストに向けられたインターネットからのパケットを示します。分類子は、パケットをインスタンスCに割り当てます。これは、入力インターフェイスがイーサネット 1/2.3 で、このイーサネットがインスタンス C に割り当てられているためです。

図 *9:* トランスペアレント ファイアウォール インスタンス



インラインセットの場合、一意のインターフェイスを使用する必要があり、そのインターフェイスは物理インターフェイスまたは Etherchannel である必要があります。次の図に、ネットワーク内のインスタンス C のホストに向けられたインターネットからのパケットを示します。分類子は、パケットをインスタンス C に割り当てます。これは、入力インターフェイスがイーサネット 1/5 で、このイーサネットがインスタンス C に割り当てられているためです。

図 *10 : FTD* のインライン セット

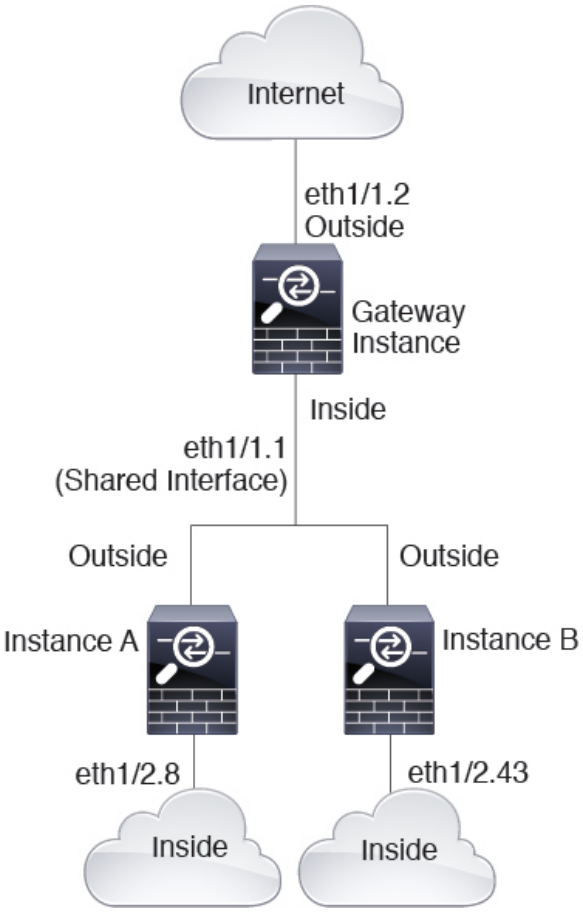


コンテナ インスタンスのカスケード

別のインスタンスの前にコンテナ インスタンスを直接配置することをカスケード コンテナ インスタンスと呼びます。1 つのインスタンスの外部インターフェイスは、別のインスタンスの内部インターフェイスと同じインターフェイスです。いくつかのインスタンスのコンフィギュレーションを単純化する場合、最上位インスタンスの共有パラメータを設定することで、インスタンスをカスケード接続できます。

次の図に、ゲートウェイの背後に2つのインスタンスがあるゲートウェイ インスタンスを示します。

図 *11* : コンテナ インスタンスのカスケード

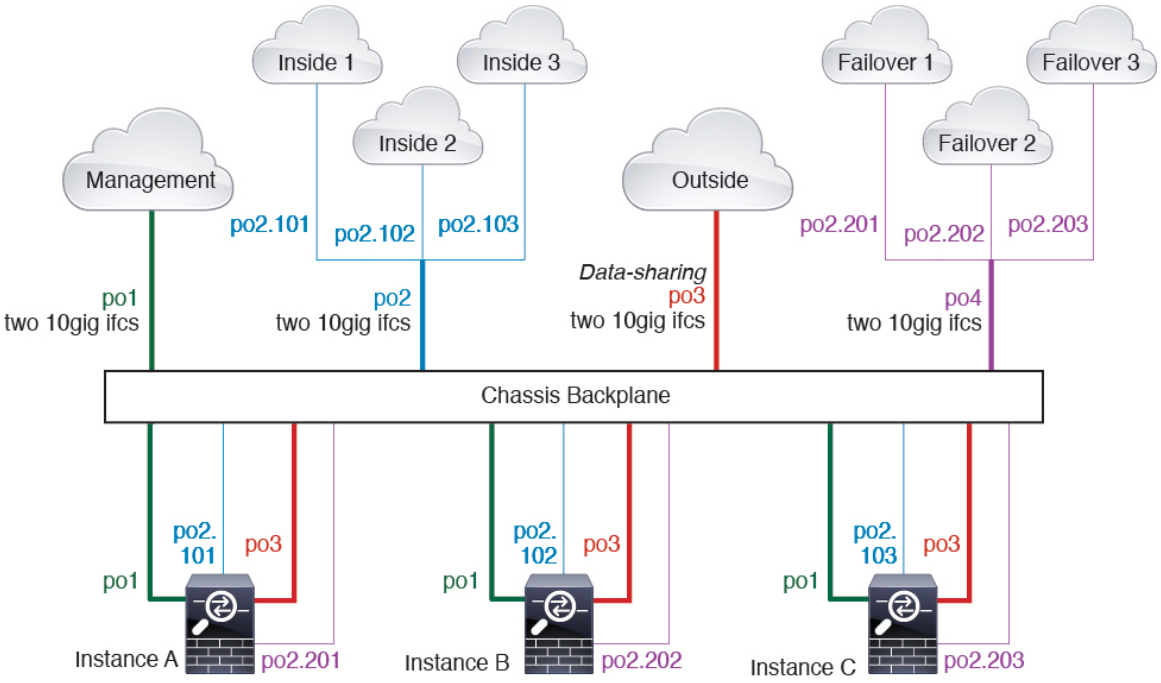


一般的な複数インスタンス展開

次の例には、ルーテッドファイアウォールモードのコンテナインスタンスが3つ含まれます。これらには次のインターフェイスが含まれます。

- 管理：すべてのインスタンスがポートチャネル1インターフェイス（管理タイプ）を使用します。この EtherChannel には 2 つの 10 ギガビット イーサネット インターフェイスが含まれます。各アプリケーション内で、インターフェイスは同じ管理ネットワークで一意の IP アドレスを使用します。
- 内部：各インスタンスがポートチャネル2（データ タイプ）のサブインターフェイスを使用します。この EtherChannel には 2 つの 10 ギガビット イーサネット インターフェイスが含まれます。各サブインターフェイスは別々のネットワーク上に存在します。
- 外部：すべてのインスタンスがポートチャネル3インターフェイス（データ共有タイプ）を使用します。この EtherChannel には 2 つの 10 ギガビット イーサネット インターフェイスが含まれます。各アプリケーション内で、インターフェイスは同じ管理ネットワークで一意の IP アドレスを使用します。

- フェールオーバー：各インスタンスがポートチャネル4（データタイプ）のサブインターフェイスを使用します。この EtherChannel には 2 つの 10 ギガビット イーサネット インターフェイスが含まれます。各サブインターフェイスは別々のネットワーク上に存在します。



コンテナ インスタンス インターフェイスの自動 MAC アドレス

FXOS シャーシは、各インスタンスの共有インターフェイスが一意の MAC アドレスを使用するように、コンテナインスタンスインターフェイスの MAC アドレスを自動的に生成します。

アプリケーション内の共有インターフェイスに MAC アドレスを手動で割り当てると、手動で割り当てられた MAC アドレスが使用されます。後で手動 MAC アドレスを削除すると、自動生成されたアドレスが使用されます。生成した MAC アドレスがネットワーク内の別のプライベート MAC アドレスと競合することがまれにあります。この場合は、アプリケーション内のインターフェイスの MAC アドレスを手動で設定してください。

自動生成されたアドレスは A2 で始まるため、アドレスが重複するリスクがあることから手動 MAC アドレスを A2 で始めることはできません。

（注） MAC アドレスを手動で設定すると、サブインターフェイスを共有していない場合でも、分類が正しく行われるように、同じ親インターフェイス上のすべてのサブインターフェイスで一意の MAC アドレスを使用します。

FXOS シャーシは、次の形式を使用して MAC アドレスを生成します。

A2*xx.yyzz.zzzz*

xx.yy はユーザ定義のプレフィックスまたはシステム定義のプレフィックスであり、*zz.zzzz* はシャーシが生成した内部カウンタです。システム定義のプレフィックスは、IDPROMにプログラムされている Burned-in MAC アドレス プール内の最初の MAC アドレスの下部 2 バイトと一致します。**connect fxos** を使用し、次に **show module** を使用して、MAC アドレス プールを表示します。たとえば、モジュール1について示されているMACアドレスの範囲がb0aa.772f.f0b0 ～ b0aa.772f.f0bf の場合、システム プレフィックスは f0b0 になります。

ユーザ定義のプレフィックスは、16進数に変換される整数です。ユーザ定義のプレフィックスの使用方法を示す例の場合、プレフィックス 77 を設定すると、シャーシは 77 を 16 進数値 004D（*yyxx*）に変換します。MAC アドレスで使用すると、プレフィックスはシャーシ ネイティブ形式に一致するように逆にされます（*xxyy*）。

A24**D.00***zz.zzzz*

プレフィックス 1009（03F1）の場合、MAC アドレスは次のようになります。

A2**F1.03***zz.zzzz*

コンテナ インスタンスのリソース管理

コンテナ インスタンスごとのリソース使用率を指定するには、FXOS で 1 つまたは複数のリソース プロファイルを作成します。論理デバイス/アプリケーション インスタンスを展開する場合は、使用するリソース プロファイルを指定します。リソース プロファイルは CPU コアの数を設定します。RAM はコアの数に従って動的に割り当てられ、ディスク容量はインスタンスごとに 40 GB に設定されます。モデルごとの使用可能なリソースを表示するには、コンテナ インスタンスの要件と前提条件（750 ページ）を参照してください。リソース プロファイルを追加するには、コンテナ インスタンスのリソース プロファイルの追加（761 ページ）を参照してください。

マルチインスタンス機能のパフォーマンス スケーリング係数

プラットフォームの最大接続数は、ネイティブ インスタンスがメモリと CPU を使用するために計算されます（この値は **show resource usage** に示されます）。ただし、マルチインスタンス機能を使用する場合、使用可能な最大接続数は、1 つのネイティブ インスタンス用の接続数未満（約 70 ～ 80 %）になり、ネットワークによってはスケーリングが改善または悪化する可能性があります。たとえば、次の比較を参照してください。

- Firepower 9300 SM-24
- ネイティブ インスタンスの最大同時接続数：30,000,000
- マルチインスタンスの最大同時接続数：約 21,000,000 ～ 24,000,000

コンテナ インスタンスおよびハイ アベイラビリティ

2 つの個別のシャーシでコンテナ インスタンスを使用してハイ アベイラビリティを使用できます。たとえば、それぞれ 10 個のインスタンスを使用する 2 つのシャーシがある場合、10 個のハイ アベイラビリティ ペアを作成できます。ハイ アベイラビリティは FXOS で構成されません。各ハイ アベイラビリティ ペアはアプリケーション マネージャで構成します。

各装置で同じリソース プロファイル属性を使用する必要があります。

各ハイ アベイラビリティ ペアには専用のフェールオーバー リンクが必要です。データ共有インターフェイスを使用することはできません。親インターフェイスでサブインターフェイスを作成し、各インスタンスのサブインターフェイスを割り当てて、フェールオーバー リンクとして使用することをお勧めします。

（注） クラスタリングはサポートされません。

コンテナ インスタンスのライセンス

すべてのライセンスがコンテナ インスタンスごとではなく、セキュリティ エンジン/シャーシ（Firepower 4100 の場合）またはセキュリティ モジュール（Firepower 9300 の場合）ごとに使用されます。次の詳細情報を参照してください。

- 基本ライセンスが セキュリティ モジュール/エンジン ごとに 1 つ自動的に割り当てられます。
- 機能ライセンスは各インスタンスに手動で割り当てますが、セキュリティ モジュール/エンジン につき機能ごとに 1 つのライセンスのみを使用します。たとえば、3 台のセキュリティ モジュールを搭載した Firepower 9300 の場合、使用中のインスタンスの数に関係なく、モジュールごとに 1 つの URL フィルタリング ライセンスが必要で、合計 3 つのライセンスが必要になります。
- ハイ アベイラビリティについては、高可用性ペアでの FTD デバイスのライセンス要件 （875 ページ）を参照してください。

次に例を示します。

表 *74 : Firepower 9300* のコンテナ インスタンスのライセンスの使用状況

Firepower 9300	インスタンス	ライセンス
セキュリティ モジュール 1	インスタンス 1	基本、URL フィルタリング、マルウェア
	インスタンス 2	基本、URL フィルタ リング
	インスタンス 3	基本、URL フィルタ リング
セキュリティ モジュール 2	インスタンス 4	基本、脅威
	インスタンス 5	、URL フィルタ リング、マルウェア、脅威の基本します。

Firepower 9300	インスタンス	ライセンス
セキュリティ モジュール 3	インスタンス 6	基本、マルウェア、脅威
	インスタンス 7	基本、脅威

表 *75:* ライセンスの総数

基本	URL フィルタリング	マルウェア	脅威
3	2	3	2

論理デバイスの要件と前提条件

要件と前提条件については、次のセクションを参照してください。

ハードウェアとソフトウェアの組み合わせの要件と前提条件

Firepower 4100/9300では、複数のモデル、セキュリティモジュール、アプリケーションタイプ、および高可用性と拡張性の機能がサポートされています。許可された組み合わせについては、次の要件を参照してください。

Firepower 9300 の要件

Firepower 9300 には、3 つのセキュリティモジュール スロットと複数タイプのセキュリティモジュールが実装されています。次の要件を参照してください。

- セキュリティモジュール タイプ：Firepower 9300 に異なるタイプのモジュールをインストールできます。たとえば、SM-36 をモジュール 1、SM-40 をモジュール 2 、SM-44 をモジュール 3 としてインストールできます。
- クラスタリング：クラスタ内またはシャーシ間であるかどうかにかかわらず、クラスタ内のすべてのセキュリティモジュールは同じタイプである必要があります。各シャーシに異なる数のセキュリティモジュールをインストールできますが、すべての空のスロットを含め、シャーシのすべてのモジュールをクラスタに含める必要があります。たとえば、シャーシ 1 に 2 つの SM-36 を、シャーシ 2 に 3 つの SM-36 をインストールできます。 同じシャーシに 1 つの SM-24 および 2 つの SM-36 をインストールする場合、クラスタリングは使用できません。
- 高可用性：高可用性は Firepower 9300 の同じタイプのモジュール間でのみサポートされています。 ただし、2つのシャーシに混在モジュールを含めることができます。たとえば、各シャーシに SM-36、SM-40、および SM-44 を配置できます。SM-36 モジュール間、SM-40 モジュール間、および SM-44 モジュール間に高可用性ペアを作成できます。
- ASA および FTD のアプリケーションタイプ：異なるアプリケーション タイプをシャーシ内の別個のモジュールにインストールすることができます。たとえば、モジュール 1 とモ

ジュール 2 に ASA をインストールし、モジュール 3 に FTD をインストールすることができます。

- ASA または FTD のバージョン：個別のモジュールで異なるバージョンのアプリケーション インスタンス タイプを実行することも、同じモジュール上の個別のコンテナインスタンスとして実行することもできます。たとえば、モジュール 1 に FTD 6.3 を、モジュール 2 に FTD 6.4 を、モジュール 3 に FTD 6.5 をインストールできます。

Firepower 4100 の要件

Firepower 4100 は複数のモデルに搭載されています。次の要件を参照してください。

- ネイティブインスタンスとコンテナインスタンス：Firepower 4100 にコンテナインスタンスをインストールする場合、そのデバイスは他のコンテナインスタンスのみをサポートできます。ネイティブインスタンスはデバイスのすべてのリソースを使用するため、デバイスにはネイティブインスタンスを 1 つのみインストールできます。
- クラスタリング：クラスタ内のすべてのシャーシが同じモデルである必要があります。
- 高可用性：高可用性は同じタイプのモデル間でのみサポートされています。
- ASA および FTD のアプリケーションタイプ：Firepower 4100 は、1 つのアプリケーションタイプのみを実行できます。
- FTD コンテナインスタンスのバージョン：同じモジュール上で異なるバージョンの FTD を個別のコンテナインスタンスとして実行できます。

コンテナ インスタンスの要件と前提条件

サポートされるアプリケーション タイプ

- Firepower Threat Defense

FTD：モデルごとの最大コンテナインスタンス数とリソース

各コンテナインスタンスに対して、インスタンスに割り当てる CPU コアの数を指定できます。RAM はコアの数に従って動的に割り当てられ、ディスク容量はインスタンスごとに 40 GB に設定されます。

表 *76*：モデルごとの最大コンテナ インスタンス数とリソース

モデル	最大コンテナインスタンス数	使用可能な CPU コア数	使用可能な RAM	使用可能なディスク容量
Firepower 4110	3	22	53 GB	125.6 GB
Firepower 4115	7	46	162 GB	308 GB

モデル	最大コンテナインスタンス数	使用可能な CPU コア数	使用可能な RAM	使用可能なディスク容量
Firepower 4120	3	46	101 GB	125.6 GB
Firepower 4125	10	62	162 GB	644 GB
Firepower 4140	7	70	222 GB	311.8 GB
Firepower 4145	14	86	344 GB	608 GB
Firepower 4150	7	86	222 GB	311.8 GB
Firepower 9300 SM-24 セキュリティモジュール	7	46	226 GB	656.4 GB
Firepower 9300 SM-36 セキュリティモジュール	11	70	222 GB	640.4 GB
Firepower 9300 SM-40 セキュリティ モジュール	13	78	334 GB	1359 GB
Firepower 9300 SM-44 セキュリティ モジュール	14	86	218 GB	628.4 GB
Firepower 9300 SM-48 セキュリティモジュール	15	94	334 GB	1341 GB
Firepower 9300 SM-56 セキュリティ モジュール	18	110	334 GB	1314 GB

Firepower Management Center の要件

Firepower 4100 シャーシまたは Firepower 9300 モジュール上のすべてのインスタンスに対して、ライセンスの実装のために同じ Firepower Management Center（FMC）を使用する必要があります。

論理デバイスに関する注意事項と制約事項

ガイドラインと制限事項については、以下のセクションを参照してください。

Firepower インターフェイスに関する注意事項と制約事項

VLAN サブインターフェイス

- ネットワーク展開に応じて、最大 500 の VLAN ID を使用してシャーシあたり 250 ～ 500 のサブインターフェイスを作成できます。
- サブインターフェイスは、データまたはデータ共有タイプのインターフェイスでのみサポートされます。
- サブインターフェイス（および親インターフェイス）はコンテナインスタンスにのみ割り当てることができます。

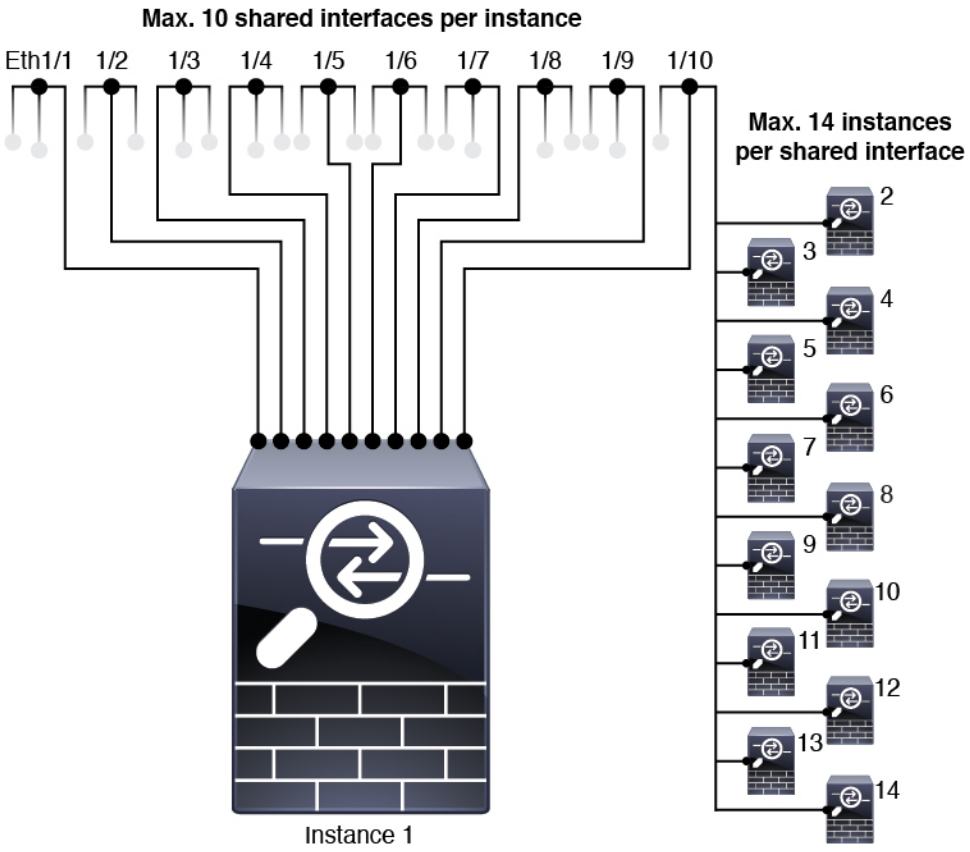
（注） コンテナインスタンスに親インターフェイスを割り当てる場合、タグなし（非 VLAN）トラフィックのみを渡します。タグなしトラフィックを渡す必要がない限り、親インターフェイスを割り当てないでください。

- 論理デバイスアプリケーション内での次の制限事項を確認し、インターフェイスの割り当てを計画する際には留意してください。
  - FTD インラインセットのサブインターフェイスを使用することはできません。また、パッシブ インターフェイスとして使用することはできません。
  - フェールオーバー リンクに対してサブインターフェイスを使用する場合、その親にあるすべてのサブインターフェイスと親自体のフェールオーバー リンクとしての使用が制限されます。一部のサブインターフェイスをフェールオーバーリンクとして使用し、一部を通常のデータインターフェイスとして使用することはできません。

データ共有インターフェイス

- 共有インターフェイスごとの最大インスタンス数：14。たとえば、Instance1 から Instance14 に Ethernet1/1 を割り当てることができます。

  インスタンスごとの最大共有インターフェイス数：10。たとえば、Ethernet1/1.10 を介して Instance1 に Ethernet1/1.1 を割り当てることができます。



- ネイティブ インスタンスでデータ共有インターフェイスを使用することはできません。
- 論理デバイスアプリケーション内での次の制限事項を確認し、インターフェイスの割り当てを計画する際には留意してください。
  - トランスペアレント ファイアウォール モード デバイスでデータ共有インターフェイスを使用することはできません。
  - FTDインラインセットでまたはパッシブインターフェイスとしてデータ共有インターフェイスを使用することはできません。
  - フェールオーバー リンクに対してデータ共有インターフェイスを使用することはできません。

次のインライン セット FTD

- 物理インターフェイス（通常かつブレイクアウト ポート）とEtherchannelのサポート。 サブインターフェイスはサポートされません。
- リンク ステートの伝達はサポートされます。

ハードウェア バイパス

- FTD をサポート。ASA の通常のインターフェイスとして使用できます。
- FTD はインライン セットでのみ ハードウェア バイパス をサポートします。
- ハードウェア バイパス 対応のインターフェイスをブレークアウト ポート用に設定することはできません。
- ハードウェア バイパス インターフェイスを EtherChannel に含めたり、ハードウェア バイパス 用に使用することはできません。EtherChannel で通常のインターフェイスとして使用できます。
- ハードウェア バイパス ハイ アベイラビリティではサポートされていません。

デフォルトの MAC アドレス

ネイティブインスタンス向け：

デフォルトの MAC アドレスの割り当ては、インターフェイスのタイプによって異なります。

- 物理インターフェイス：物理インターフェイスは、Burned-in MAC Address を使用します。
- EtherChannel：EtherChannel の場合は、そのチャネル グループに含まれるすべてのインターフェイスが同じ MAC アドレスを共有します。この機能によって、EtherChannel はネットワーク アプリケーションとユーザに対してトランスペアレントになります。ネットワーク アプリケーションやユーザから見えるのは 1 つの論理接続のみであり、個々のリンクのことは認識しないためです。ポート チャネル インターフェイスは、プールからの一意の MAC アドレスを使用します。インターフェイスのメンバーシップは、MAC アドレスには影響しません。

コンテナインスタンス向け：

- すべてのインターフェイスの MAC アドレスは MAC アドレス プールから取得されます。サブインターフェイスでは、MAC アドレスを手動で設定する場合、分類が正しく行われるように、同じ親インターフェイス上のすべてのサブインターフェイスで一意の MAC アドレスを使用します。コンテナ インスタンス インターフェイスの自動 MAC アドレス （746 ページ）を参照してください。

一般的なガイドラインと制限事項

ファイアウォール モード

FTD のブートストラップ設定でファイアウォール モードをルーテッドまたはトランスペアレントに設定できます。

ハイ アベイラビリティ

- アプリケーション設定内でハイアベイラビリティを設定します。

- 任意のデータ インターフェイスをフェールオーバー リンクおよびステート リンクとして使用できます。 データ共有インターフェイスはサポートされていません。
- ハイ アベイラビリティ フェールオーバーを設定される 2 つのユニットは、次の条件を満たしている必要があります。
  - 同じモデルであること。
  - ハイアベイラビリティ論理デバイスに同じインターフェイスが割り当てられていること。
  - インターフェイスの数とタイプが同じであること。ハイ アベイラビリティを有効にする前に、すべてのインターフェイスを FXOS で事前に同じ設定にすること。
- 詳細については、高可用性 のシステム要件 （874 ページ）を参照してください。

マルチインスタンスとコンテキスト モード

- ASA ではマルチ コンテキスト モードはサポートされていません。
- コンテナ インスタンスによる複数インスタンス機能は FMC を使用する FTD に対してのみ使用できます。
- コンテナ インスタンスの場合、各共有インターフェイスを最大 14 個のコンテナ インスタンスに割り当てることができます。
- 特定のコンテナ インスタンスの場合、最大 10 個の共有インターフェイスを割り当てることができます。
- FTD コンテナ インスタンスの場合、1 つの Firepower Management Center で セキュリティ モジュール/エンジン のすべてのインスタンスを管理する必要があります。
- の で TLS 暗号化アクセラレーション を有効にできます。
- FTD コンテナ インスタンスの場合、次の機能はサポートされていません。
  - クラスタ
  - Radware DefensePro リンク デコレータ
  - FMC バックアップおよび復元
  - FMC UCAPL/CC モード

インターフェイスの設定

デフォルトでは、物理インターフェイスはディセーブルになっています。インターフェイスを有効にし、EtherChannels を追加して、VLAN サブインターフェイスを追加し、、インターフェイス プロパティを編集して。

インターフェイスの有効化または無効化

各インターフェイスの **[Admin State]** を有効または無効に切り替えることができます。デフォルトでは、物理インターフェイスはディセーブルになっています。 VLAN サブインターフェイスの場合、管理状態は親インターフェイスから継承されます。

ステップ 1 [Interfaces] を選択して [Interfaces] ページを開きます。

[Interfaces] ページには、ページの上部に現在インストールされているインターフェイスが視覚的に表示され、下の表にはインストールされているインターフェイスのリストが示されています。

ステップ 2 インターフェイスを有効にするには、[disabled スライダ（  ）] をクリックします。これで、[enabled スライダ（  ）] に変わります。

[Yes] をクリックして、変更を確認します。視覚的に表示された対応するインターフェイスがグレーからグリーンに変わります。

ステップ 3 インターフェイスを無効にするには、[enabled スライダ（  ）] をクリックします。これで、[disabled スライダ（  ）] に変わります。

[Yes] をクリックして、変更を確認します。視覚的に表示された対応するインターフェイスがグリーンからグレーに変わります。

物理インターフェイスの設定

インターフェイスを物理的に有効および無効にすること、およびインターフェイスの速度とデュプレックスを設定することができます。インターフェイスを使用するには、インターフェイスを FXOS で物理的に有効にし、アプリケーションで論理的に有効にする必要があります。

始める前に

- すでに EtherChannel のメンバーであるインターフェイスは個別に変更できません。EtherChannel に追加する前に、設定を行ってください。

ステップ 1 [Interfaces] を選択して [Interfaces] ページを開きます。

[**すべてのインターフェイス（All Interfaces）**] ページでは、上部に現在インストールされているインターフェイスが視覚的に表示され、下部の表にそれらのリストが表示されます。

ステップ 2 編集するインターフェイスの行の [Edit] をクリックし、[Edit Interface] ダイアログボックスを開きます。

ステップ 3 インターフェイスをイネーブルにするには、[Enable] チェックボックスをオンにします。インターフェイスをディセーブルにするには、[Enable] チェックボックスをオフにします。

ステップ 4 インターフェイスの [タイプ（Type）] を次から選択します。**Data**、**Data-sharing**、**Mgmt**、**Firepower-eventing**、または **Cluster**。

Cluster タイプは選択しないでください。デフォルトでは、Cluster Control Link はポートチャネル 48 に自動的に作成されます。

ステップ 5 （任意） [Speed] ドロップダウン リストからインターフェイスの速度を選択します。

ステップ 6 （任意） インターフェイスで [Auto Negotiation] がサポートされている場合は、[Yes] または [No] オプション ボタンをクリックします。

ステップ 7 （任意） [Duplex] ドロップダウン リストからインターフェイスのデュプレックスを選択します。

ステップ 8 [OK] をクリックします。

EtherChannel（ポート チャネル）の追加

EtherChannel（別名ポート チャネル）には、同じタイプのメンバー インターフェイスを最大 16 個含めることができます。リンク集約制御プロトコル（LACP）では、2 つのネットワーク デバイス間でリンク集約制御プロトコル データ ユニット（LACPDU）を交換することによって、インターフェイスが集約されます。

EtherChannel 内の各物理データまたはデータ共有インターフェイスを次のように設定できます。

- アクティブ：LACP アップデートを送信および受信します。アクティブ EtherChannel は、アクティブまたはパッシブ EtherChannel と接続を確立できます。LACP トラフィックを最小にする必要がある場合以外は、アクティブ モードを使用する必要があります。
- オン：EtherChannel は常にオンであり、LACP は使用されません。「オン」の EtherChannel は、別の「オン」の EtherChannel のみと接続を確立できます。

（注） モードを [On] から [Active] に変更するか、[Active] から [On] に変更すると、EtherChannel が動作状態になるまで最大 3 分かかることがあります。

非データ インターフェイスはアクティブ モードのみをサポートします。

LACP では、ユーザが介入しなくても、EtherChannel へのリンクの自動追加および削除が調整されます。また、コンフィギュレーションの誤りが処理され、メンバインターフェイスの両端が正しいチャネル グループに接続されていることがチェックされます。「オン」モードではインターフェイスがダウンしたときにチャネル グループ内のスタンバイ インターフェイスを使用できず、接続とコンフィギュレーションはチェックされません。

Firepower 4100/9300 シャーシが EtherChannel を作成すると、EtherChannel は [一時停止（Suspended）] 状態（Active LACP モードの場合）または [ダウン（Down）] 状態（On LACP モードの場合）になり、物理リンクがアップしても論理デバイスに割り当てるまでそのままになります。EtherChannel は次のような状況でこの [Suspended] 状態になります。

- EtherChannel がスタンドアロン論理デバイスのデータまたは管理インターフェイスとして追加された

- EtherChannel がクラスタの一部である論理デバイスの管理インターフェイスまたは Cluster Control Link として追加された
- EtherChannel がクラスタの一部である論理デバイスのデータ インターフェイスとして追加され、少なくとも 1 つのユニットがクラスタに参加している

EtherChannel は論理デバイスに割り当てるまで動作しないことに注意してください。EtherChannel が論理デバイスから削除された場合や論理デバイスが削除された場合は、EtherChannel が [一時停止（Suspended）] または [ダウン（Down）] 状態に戻ります。

ステップ 1 [Interfaces] を選択して [Interfaces] ページを開きます。

[**すべてのインターフェイス（All Interfaces**）]ページでは、上部に現在インストールされているインターフェイスが視覚的に表示され、下部の表にそれらのリストが表示されます。

ステップ 2 インターフェイス テーブルの上にある **[Add Port Channel]**をクリックして、**[Add Port Channel]**ダイアログボックスを開きます。

ステップ 3 **[Port Channel ID]**フィールドに、ポート チャネルの ID を入力します。有効な値は、1 ～ 47 です。

クラスタ化した論理デバイスを導入すると、ポートチャネル 48 はクラスタ制御リンク用に予約されます。クラスタ制御リンクにポートチャネル 48 を使用しない場合は、別の ID で EtherChannel を設定し、インターフェイスにクラスタ タイプを選択できます。シャーシ内クラスタリングでは、クラスタ EtherChannel にインターフェイスを割り当てないでください。

ステップ 4 ポート チャネルを有効化するには、**[Enable]**チェックボックスをオンにします。ポート チャネルをディセーブルにするには、**[Enable]**チェックボックスをオフにします。

ステップ 5 インターフェイスの [Type] を次から選択します。**Data**、**Data-sharing**、**Mgmt**、**Firepower-eventing**、または **Cluster**。

デフォルトの代わりに、このポートチャネルを Cluster Control Link として使用する場合以外は、**Cluster** タイプを選択しないでください。

ステップ 6 ドロップダウン リストでメンバー インターフェイスの [Admin Speed] を設定します。

ステップ 7 データまたはデータ共有インターフェイスに対して、LACP ポート チャネル [Mode]、[Active] または [On] を選択します。

非データまたは非データ共有インターフェイスの場合、モードは常にアクティブです。

ステップ 8 [Admin Duplex]、[Full Duplex] または [Half Duplex] を設定します。

ステップ 9 ポート チャネルにインターフェイスを追加するには、**[Available Interface]**リストでインターフェイスを選択し、**[Add Interface]**をクリックしてそのインターフェイスを [Member ID] リストに移動します。同じタイプと速度の最大 16 のインターフェイスを追加できます。

ヒント 複数のインターフェイスを一度に追加できます。複数の個別インターフェイスを選択するには、**Ctrl**キーを押しながら目的のインターフェイスをクリックします。一連のインターフェイスを選択するには、その範囲の最初のインターフェイスを選択し、**Shift**キーを押しながら最後のインターフェイスをクリックして選択します。

ステップ 10 ポートチャネルからインターフェイスを削除するには、[Member ID]リストでそのインターフェイスの右側にある**[Delete]**ボタンをクリックします。

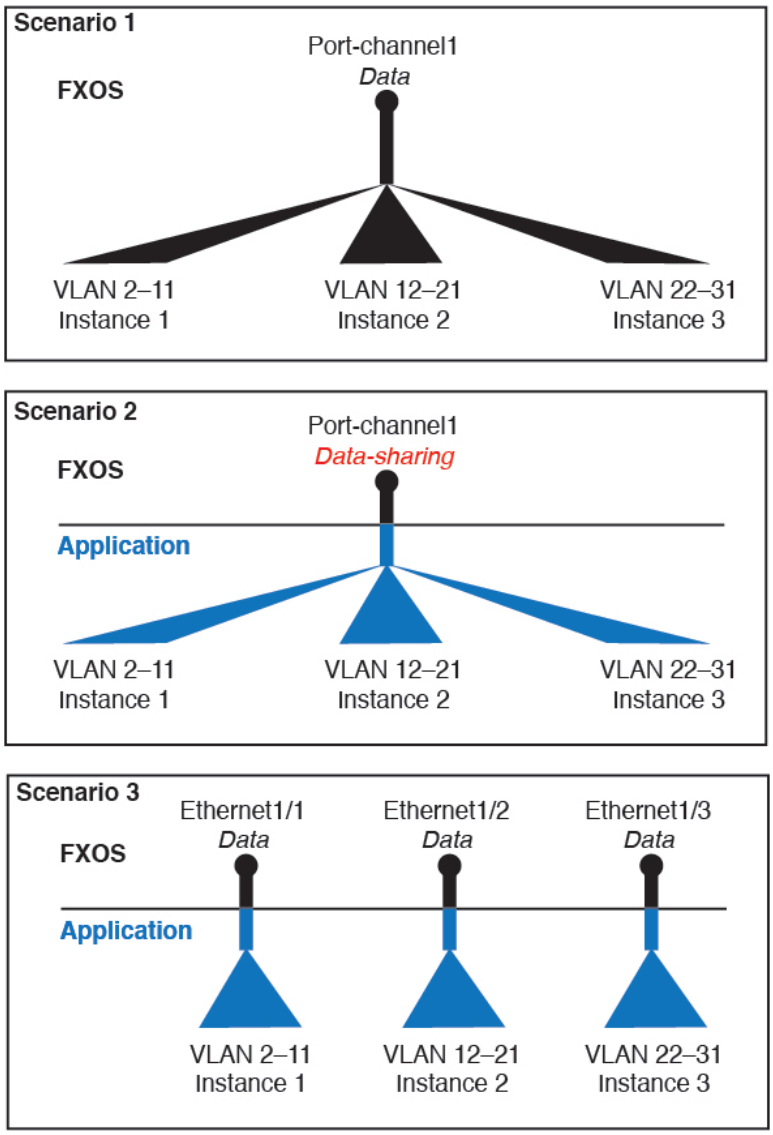
ステップ 11 **[OK]**をクリックします。

コンテナ インスタンスへの VLAN サブインターフェイスの追加

ネットワーク配置に応じて、250 ～ 500 の VLAN サブインターフェイスをシャーシに追加できます。

インターフェイスごとの VLAN ID は一意であることが必要です。またコンテナ インスタンス内では、すべての割り当てられたインターフェイスでVLAN IDが一意であることが必要です。異なるコンテナ インスタンスに割り当てられている限り、VLAN ID を別のインターフェイス上で再利用できます。ただし、同じ ID を使用していても、各サブインターフェイスが制限のカウント対象になります。

ネイティブ インスタンスの場合、アプリケーション内でのみ VLAN サブインターフェイスを作成できます。コンテナインスタンスの場合、FXOS VLAN サブインターフェイスが定義されていないインターフェイスのアプリケーション内でも VLAN サブインターフェイスを作成できます。これらのサブインターフェイスにはFXOS制限が適用されません。サブインターフェイスを作成するオペレーティング システムの選択は、ネットワーク導入および個人設定によって異なります。たとえば、サブインターフェイスを共有するには、FXOS でサブインターフェイスを作成する必要があります。FXOS サブインターフェイスを優先するもう 1 つのシナリオでは、1つのインターフェイス上の別のサブインターフェイス グループを複数のインスタンスに割り当てます。たとえば、インスタンス A で VLAN 2-11 を、インスタンス B で VLAN 12-21 を、インスタンス C で VLAN 22-31 を使用して Port-Channel1 を使うとします。アプリケーション内でこれらのサブインターフェイスを作成する場合、FXOS 内で親インターフェイスを共有しますが、これはお勧めしません。このシナリオを実現する 3 つの方法については、次の図を参照してください。



ステップ 1 **[Interfaces]** を選択して **[All Interfaces]** タブを開きます。

[All Interfaces] タブには、ページの上部に現在インストールされているインターフェイスが視覚的に表示され、下の表にはインストールされているインターフェイスのリストが示されています。

ステップ 2 **[Add New** > **Subinterface]** をクリックして [Add Subinterface] ダイアログボックスを開きます。

ステップ 3 インターフェイス **[Type]**：**[Data]** または **[Data-sharing]** を選択します。

サブインターフェイスはデータまたはデータ共有タイプのインターフェイスでのみサポートされます。タイプは親インターフェイスのタイプに依存しません。たとえば、データ共有タイプの親インターフェイスとデータ タイプのサブインターフェイスを持つことができます。

ステップ 4 ドロップダウンリストから親 [Interface] を選択します。

現在論理デバイスに割り当てられている物理インターフェイスにサブインターフェイスを追加することはできません。親の他のサブインターフェイスが割り当てられている場合は、親インターフェイス自体が割り当てられていない限り、新しいサブインターフェイスを追加できます。

ステップ 5 [Subinterface ID]（1 ～ 4294967295）を入力します。

この ID は *interface_id.subinterface_id* として親インターフェイスの ID に付加されます。たとえば、サブインターフェイスを ID 100 で Ethernet1/1 に追加する場合、そのサブインターフェイス ID は Ethernet1/1.100 になります。利便性を考慮して一致するように設定することができますが、この ID は VLAN ID と同じではありません。

ステップ 6 [VLAN ID]（1 ～ 4095）を設定します。

ステップ 7 [OK] をクリックします。

親インターフェイスを展開して、その下にあるすべてのサブインターフェイスを表示します。

論理デバイスの設定

Firepower 4100/9300 シャーシに、スタンドアロン論理デバイスまたはハイ アベイラビリティ ペアを追加します。

クラスタ リングについては、Firepower Threat Defense 用のクラスタリング （907 ページ）を参照してください。

コンテナ インスタンスのリソース プロファイルの追加

コンテナインスタンスごとにリソース使用率を指定するには、1つまたは複数のリソース プロファイルを作成します。論理デバイス/アプリケーション インスタンスを展開するときに、使用するリソース プロファイルを指定します。リソース プロファイルは CPU コアの数を設定します。RAM はコアの数に従って動的に割り当てられ、ディスク容量はインスタンスごとに 40 GB に設定されます。

- コアの最小数は 6 です。
- 内部アーキテクチャにより 8 コアを指定することはできません。
- コアを偶数（6、10、12、14 など）で最大値まで割り当てることができます。
- 利用可能な最大コア数は、セキュリティ モジュール/シャーシ モデルによって異なります。コンテナ インスタンスの要件と前提条件 （750 ページ）を参照してください。

シャーシには、「Default-Small」と呼ばれるデフォルト リソース プロファイルが含まれています。このコア数は最小です。このプロファイルの定義を変更したり、使用されていない場合には削除することもできます。シャーシをリロードし、システムに他のプロファイルが存在しない場合は、このプロファイルが作成されます。

使用中のリソースプロファイルの設定を変更することはできません。リソースプロファイルを使用しているすべてのインスタンスを無効にしてから、リソースプロファイルを変更し、最後にインスタンスを再度有効にする必要があります。確立されたハイ アベイラビリティ ペア内のインスタンスのサイズを変更する場合、できるだけ早くすべてのメンバを同じサイズにする必要があります。

FTD インスタンスを FMC に追加した後にリソースプロファイルの設定を変更する場合は、**[Devices]** > **[Device Management]** > **[Device]** > **[System]** > **[Inventory]** ダイアログボックスで各ユニットのインベントリを更新します。

ステップ 1 **[Platform Settings]** > **[Resource Profiles]** を選択し、[Add] をクリックします。

[Add Resource Profile] ダイアログボックスが表示されます。

ステップ 2 次のパラメータを設定します。

- [Name]：プロファイルの名前を 1 ～ 64 文字で設定します。追加後にこのプロファイルの名前を変更することはできません。
- [Description]：プロファイルの説明を最大 510 文字で設定します。
- [Number of Cores]：プロファイルのコア数を 6 ～ 最大数（偶数）で設定します。最大数はシャーシによって異なります。8 コアを指定することはできません。

ステップ 3 [OK] をクリックします。

スタンドアロン Firepower Threat Defense の追加

スタンドアロンの論理デバイスは、単独またはハイ アベイラビリティ ペアで動作します。複数のセキュリティモジュールを搭載する Firepower 9300 では、クラスタまたはスタンドアロンデバイスのいずれかを展開できます。クラスタはすべてのモジュールを使用する必要があるため、たとえば、2 モジュール クラスタと単一のスタンドアロンデバイスをうまく組み合わせることはできません。

一部のモジュールでネイティブインスタンスを使用し、その他のモジュールでコンテナインスタンスを使用することができます。

始める前に

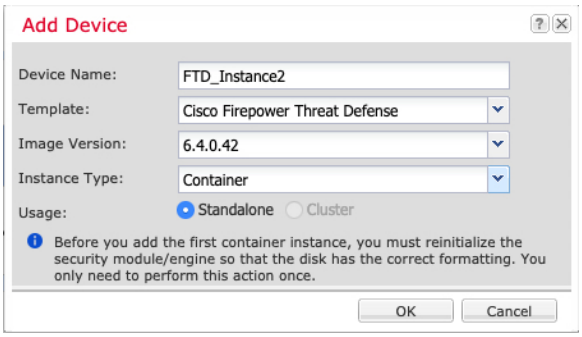
- 論理デバイスに使用するアプリケーション イメージを Cisco.com からダウンロードして、そのイメージを Firepower 4100/9300 シャーシ にアップロードします。

（注） Firepower 9300 の場合、異なるアプリケーションタイプ（ASA およびFTD）をシャーシ内の個々のモジュールにインストールできます。別個のモジュールでは、異なるバージョンのアプリケーション インスタンス タイプも実行できます。

- 論理デバイスで使用する管理インターフェイスを設定します。管理インターフェイスが必要です。この管理インターフェイスは、シャーシの管理のみに使用されるシャーシ管理ポートと同じではありません（また、[Interfaces] タブの上部に [MGMT] として表示されます）。
- また、少なくとも 1 つのデータ タイプのインターフェイスを設定する必要があります。必要に応じて、すべてのイベントのトラフィック（Web イベントなど）を運ぶ firepower-eventing インターフェイスも作成できます。詳細については、「インターフェイス タイプ （726 ページ）」を参照してください。
- コンテナインスタンスに対して、デフォルトのプロファイルを使用しない場合は、コンテナインスタンスのリソース プロファイルの追加 （761 ページ）に従ってリソース プロファイルを追加します。
- コンテナ インスタンスの場合、最初にコンテナ インスタンスをインストールする前に、ディスクが正しいフォーマットになるようにセキュリティ モジュール/エンジン を再度初期化する必要があります。[Security Modules] または [Security Engine] を選択して、[Reinitialize] アイコン（ ） をクリックします。既存の論理デバイスは削除されて新しいデバイスとして再インストールされるため、ローカルのアプリケーション設定はすべて失われます。ネイティブインスタンスをコンテナインスタンスで置き換えるときには、常にネイティブインスタンスを削除する必要があります。ネイティブインスタンスをコンテナインスタンスに自動的に移行することはできません。
- 次の情報を用意します。
  - このデバイスのインターフェイス ID
  - 管理インターフェイス IP アドレスとネットワーク マスク
  - ゲートウェイ IP アドレス
  - FMC 選択した IP アドレスや NAT ID
  - DNS サーバの IP アドレス。
  - FTD ホスト名とドメイン名

ステップ 1 [論理デバイス（Logical Devices）] を選択します。

ステップ 2 **[デバイスの追加（Add Device）]** をクリックし、次のパラメータを設定します。



a) **デバイス名**を入力します。

この名前は、シャーシ スーパーバイザが管理設定を行ってインターフェイスを割り当てるために使用します。これはアプリケーション設定で使用されるデバイス名ではありません。

b) [Template] では、[Cisco Firepower Threat Defense] を選択します。

c) [Image Version] を選択します。

d) [Instance Type] として [Container] または [Native] を選択します。

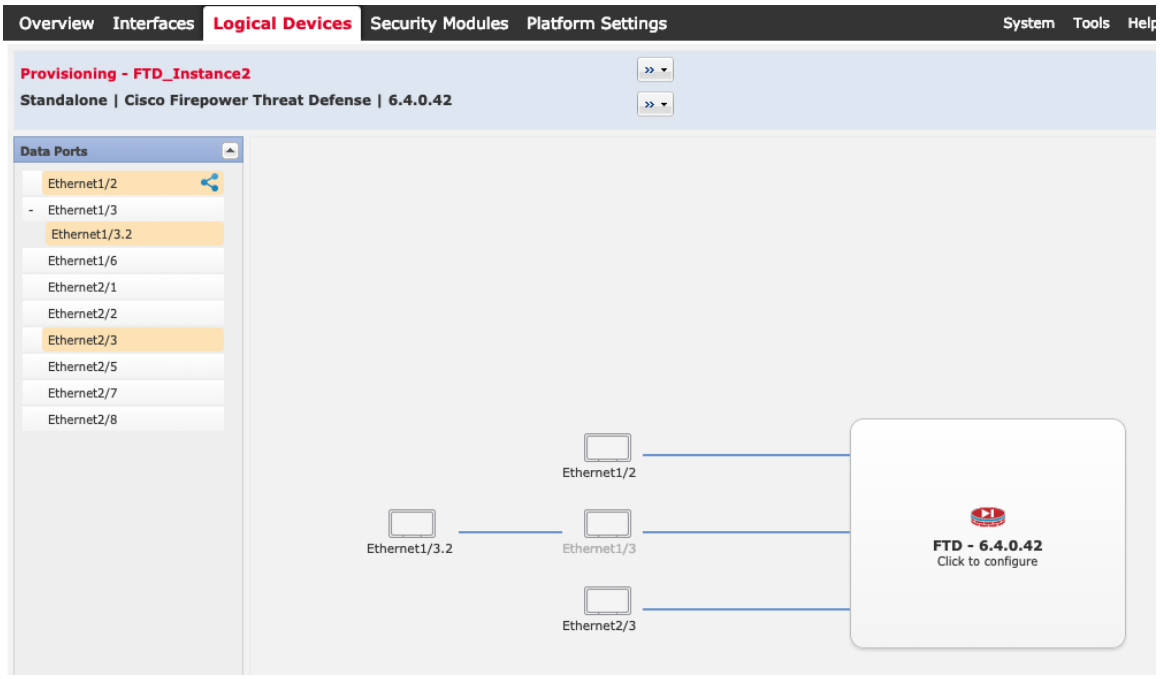
ネイティブ インスタンスはセキュリティ モジュール/エンジンのすべてのリソース（CPU、RAM、およびディスク容量）を使用するため、ネイティブ インスタンスを 1 つのみインストールできます。コンテナインスタンスでは、セキュリティ モジュール/エンジンのリソースのサブセットを使用するため、複数のコンテナ インスタンスをインストールできます。

e) [使用方法（Usage）] で、[スタンドアロン（Standalone）] オプション ボタンをクリックします。

f) [OK] をクリックします。

[Provisioning - *device name*] ウィンドウが表示されます。

ステップ 3 [Data Ports] 領域を展開し、デバイスに割り当てるインターフェイスをそれぞれクリックします。



[Interfaces] ページでは、以前に有効にしたデータとデータ共有インターフェイスのみを割り当てることができます。後でFMCのこれらのインターフェイスを有効にして設定します。これには、IPアドレスの設定も含まれます。

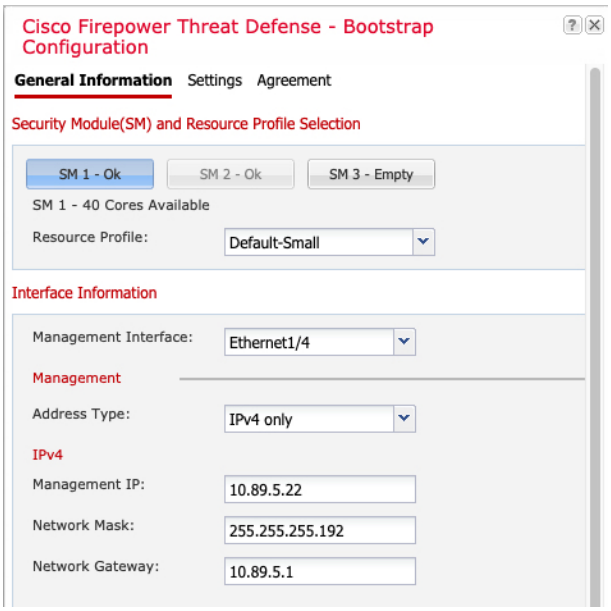
コンテナ インスタンスごとに最大 10 のデータ共有インターフェイスを割り当てることができます。また、各データ共有インターフェイスは、最大 14 個のコンテナインスタンスに割り当てることができます。データ共有インターフェイスは [Sharing] アイコン（ ） で示されます。

ハードウェア バイパス 対応のポートは次のアイコンで表示されます：。特定のインターフェイス モジュールでは、インラインセットインターフェイスに対してのみハードウェアバイパス機能を有効にできます（FMC設定ガイドを参照）。ハードウェアバイパスは、停電時にトラフィックがインラインインターフェイス ペア間で流れ続けることを確認します。この機能は、ソフトウェアまたはハードウェア障害の発生時にネットワーク接続を維持するために使用できます。ハードウェアバイパスペアの両方のインターフェイスとも割り当てられていない場合、割り当てが意図的であることを確認する警告メッセージが表示されます。ハードウェアバイパス機能を使用する必要はないため、単一のインターフェイスを割り当てることができます。

ステップ 4 画面中央のデバイス アイコンをクリックします。

初期ブートストラップ設定を設定できるダイアログボックスが表示されます。これらの設定は、初期導入専用、またはディザスタ リカバリ用です。通常の運用では、後でアプリケーション CCLI 設定のほとんどの値を変更できます。

ステップ 5 [General Information] ページで、次の手順を実行します。



a) （Firepower 9300 の場合）[Security Module Selection] の下で、この論理デバイスに使用するセキュリティモジュールをクリックします。

b) コンテナのインスタンスでは、**リソースのプロファイル**を指定します。

後で異なるリソースプロファイルを割り当てると、インスタンスがリロードされ、約 5 分かかることがあります。確立されたハイ アベイラビリティ ペアの場合に、異なるサイズのリソース プロファイルを割り当てるときは、すべてのメンバのサイズが同じであることをできるだけ早く確認してください。

c) [Management Interface] を選択します。

このインターフェイスは、論理デバイスを管理するために使用されます。このインターフェイスは、シャーシ管理ポートとは別のものです。

d) 管理インターフェイスの [Address Type] として、[IPv4 only]、[IPv6 only]、または [IPv4 and IPv6] を選択します。

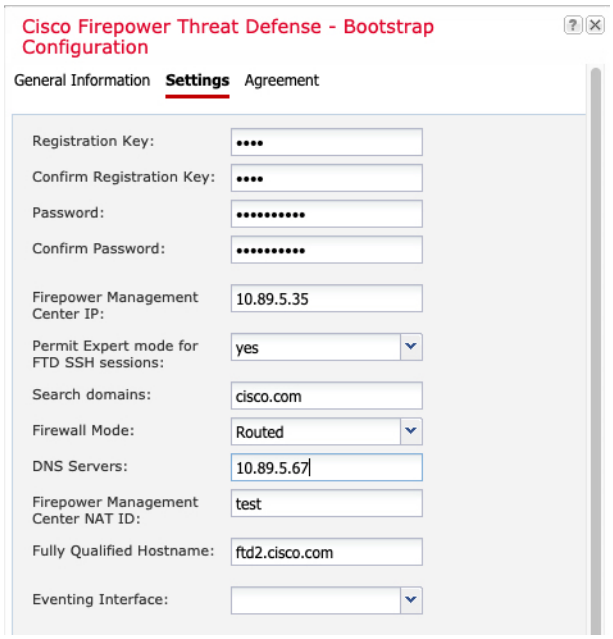
e) [Management IP] アドレスを設定します。

このインターフェイスの一意の IP アドレスを設定します。

f) **ネットワーク マスク**または**プレフィックス長**を入力します。

g) **ネットワーク ゲートウェイ** アドレスを入力します。

ステップ 6 [Settings] タブで、次の手順を実行します。



a) 管理 FMC の [Firepower Management Center IP] を入力します。FMC の IP アドレスがわからない場合は、このフィールドを空白のままにして、[Firepower Management Center NAT ID] フィールドにパスフレーズを入力します。

b) **FTD SSH セッションからエキスパート モード**、[**Yes**]、または [**No**] を許可します。エキスパートモードでは、高度なトラブルシューティングに FTD シェルからアクセスできます。

このオプションで [Yes] を選択すると、SSH セッションからコンテナインスタンスに直接アクセスするユーザがエキスパートモードを開始できます。[No] を選択すると、FXOS CLI からコンテナインスタンスにアクセスするユーザのみがエキスパートモードを開始できます。インスタンス間の分離を増やすには、[No] を選択することをお勧めします。

マニュアルの手順で求められた場合、または Cisco Technical Assistance Center から求められた場合のみ、エキスパート モードを使用します。このモードを開始するには、FTD CLI で **expert** コマンドを使用します。

c) カンマ区切りリストとして [Search Domains] を入力します。

d) [**Firewall Mode**]で[**Transparent**]、または [**Routed**] を選択します。

ルーテッド モードでは、FTDはネットワーク内のルータ ホップと見なされます。ルーティングを行う各インターフェイスは異なるサブネット上にあります。これに対し、トランスペアレント ファイアウォールは、「Bump In The Wire」または「ステルス ファイアウォール」のように動作するレイヤ 2 ファイアウォールであり、接続されたデバイスへのルータ ホップとしては認識されません。

ファイアウォール モードは初期展開時にのみ設定します。ブートストラップの設定を再適用する場合、この設定は使用されません。

e) [DNS Servers] をカンマ区切りのリストとして入力します。

たとえば、FMCのホスト名を指定する場合、FTDは DNS を使用します。

f) FTD の [Fully Qualified Hostname] を入力します。

g) 登録時に FMC とデバイス間で共有する [Registration Key] を入力します。

このキーには、1 ～ 37 文字の任意のテキスト文字列を選択できます。FTD を追加するときに、 FMC に同じキーを入力します。

h) CLI アクセス用の FTD 管理ユーザの [Password] を入力します。

i) Firepower イベントの送信に使用する [Eventing Interface] を選択します。指定しない場合は、管理インターフェイスが使用されます。

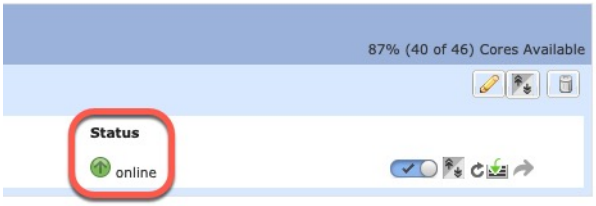
このインターフェイスは、Firepower-eventing インターフェイスとして定義する必要があります。

ステップ 7 [利用規約（Agreement）] タブで、エンド ユーザ ライセンス（EULA）を読んで、同意します。

ステップ 8 [OK] をクリックして、設定ダイアログボックスを閉じます。

ステップ 9 **[Save]** をクリックします。

シャーシは、指定したソフトウェアバージョンをダウンロードし、アプリケーションインスタンスにブートストラップ設定と管理インターフェイス設定をプッシュすることで、論理デバイスを導入します。[**論理デバイス（Logical Devices）**] ページで、新しい論理デバイスのステータスを確認します。論理デバイスの [Status] が [online] と表示されたら、アプリケーションでセキュリティ ポリシーの設定を開始できます。



ステップ 10 FTD を管理対象デバイスとして追加し、セキュリティ ポリシーの設定を開始するには、FMC コンフィギュレーション ガイドを参照してください。

ハイ アベイラビリティ ペアの追加

FTDハイ アベイラビリティ（フェールオーバーとも呼ばれます）は、FXOS ではなくアプリケーション内で設定されます。ただし、ハイ アベイラビリティのシャーシを準備するには、次の手順を参照してください。

始める前に

- ハイ アベイラビリティ フェールオーバーを設定される 2 つのユニットは、次の条件を満たしている必要があります。

- 同じモデルであること。
- ハイアベイラビリティ論理デバイスに同じインターフェイスが割り当てられていること。
- インターフェイスの数とタイプが同じであること。ハイアベイラビリティを有効にする前に、すべてのインターフェイスを FXOS で事前に同じ設定にすること。

- 高可用性は Firepower 9300 の同じタイプのモジュール間でのみサポートされていますが、2 台のシャーシにモジュールを混在させることができます。たとえば、各シャーシに SM-36、SM-40、および SM-44 を配置できます。SM-36 モジュール間、SM-40 モジュール間、および SM-44 モジュール間に高可用性ペアを作成できます。
- 他のハイ アベイラビリティ システム要件については、高可用性のシステム要件（874 ページ）を参照してください。

ステップ 1 各論理デバイスは個別のシャーシ上にある必要があります。Firepower 9300 のシャーシ内のハイ アベイラビリティは推奨されず、サポートされない可能性があります。

ステップ 2 各論理デバイスに同一のインターフェイスを割り当てます。

ステップ 3 フェールオーバー リンクとステート リンクに 1 つまたは 2 つのデータ インターフェイスを割り当てます。

これらのインターフェイスは、2 つのシャーシ間でハイ アベイラビリティ トラフィックを交換します。統合されたフェールオーバー リンクとステート リンクには、10 GB のデータ インターフェイスを使用することを推奨します。別のフェールオーバーおよび状態のリンクを使用できます使用可能なインターフェイスがあれば、状態のリンクには、ほとんどの帯域幅が必要です。フェールオーバー リンクまたはステート リンクに管理タイプのインターフェイスを使用することはできません。同じネットワーク セグメント上で他のデバイスをフェールオーバー インターフェイスとして使用せずに、シャーシ間でスイッチを使用することをお勧めします。

コンテナインスタンスの場合、データ共有インターフェイスは、フェールオーバーリンクではサポートされていません。親インターフェイスまたは EtherChannel でサブインターフェイスを作成し、各インスタンスのサブインターフェイスを割り当てて、フェールオーバーリンクとして使用することをお勧めします。同じ親のすべてのサブインターフェイスをフェールオーバーリンクとして使用する必要があることに注意してください。あるサブインターフェイスをフェールオーバーリンクとして使用して、他のサブインターフェイス（または親インターフェイス）を通常のデータインターフェイスとして使用することはできません。

ステップ 4 論理デバイスでハイ アベイラビリテを有効にします。Firepower Threat Defense のハイ アベイラビリティ（873 ページ）を参照してください。

ステップ 5 ハイ アベイラビリティを有効にした後でインターフェイスを変更する必要がある場合は、最初にスタンバイ装置で変更を実行してから、アクティブ装置で変更を実行します。

Firepower Threat Defense 論理デバイスのインターフェイスの変更

FTD 論理デバイスでは、インターフェイスの割り当てや割り当て解除、または管理インターフェイスの置き換えを行うことができます。その後、FMC でインターフェイス設定を同期できます。

新しいインターフェイスを追加したり、未使用のインターフェイスを削除したりしても、FTD の設定に与える影響は最小限です。ただし、セキュリティ ポリシーで使用されているインターフェイスを削除すると、設定に影響を与えます。インターフェイスは、アクセス ルール、NAT、SSL、アイデンティティ ルール、VPN、DHCP サーバなど、FTD の設定における多くの場所で直接参照されている可能性があります。セキュリティ ゾーンを参照するポリシーは影響を受けません。また、論理デバイスに影響を与えず、かつ FMC での同期を必要とせずに、割り当てられた EtherChannel のメンバーシップを編集できます。

インターフェイスを削除すると、そのインターフェイスに関連付けられている設定がすべて削除されます。

始める前に

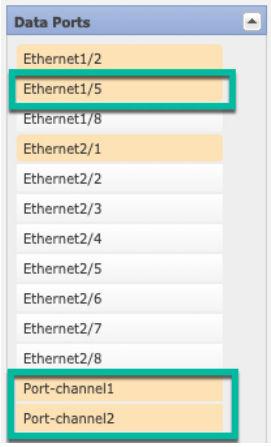
- 物理インターフェイスの設定 （756 ページ）およびEtherChannel（ポート チャネル）の追加 （757 ページ）に従って、インターフェイスを設定し、EtherChannel を追加します。
- すでに割り当てられているインターフェイスを EtherChannel に追加するには（たとえば、デフォルトではすべてのインターフェイスがクラスタに割り当てられます）、まず論理デバイスからインターフェイスの割り当てを解除し、次に EtherChannel にインターフェイスを追加する必要があります。新しい EtherChannel の場合、デバイスに EtherChannel を割り当てることができます。
- 管理インターフェイスまたは Firepower イベント インターフェイスを管理 EtherChannel に置き換えるには、未割り当てのデータ メンバー インターフェイスが少なくとも 1 つある EtherChannel を作成し、現在の管理インターフェイスをその EtherChannel に置き換える必要があります。FTDがリブートし（管理インターフェイスを変更するとリブートします）、FMC で設定を同期すると、（現在未割り当ての）管理インターフェイスも EtherChannel に追加できます。
- クラスタリングまたは高可用性のため、FMC で設定を同期する前に、すべてのユニットでインターフェイスを追加または削除していることを確認してください。最初にスレーブ/スタンバイ ユニットでインターフェイスを変更してから、マスター/アクティブ ユニットで変更することをお勧めします。新しいインターフェイスは管理上ダウンした状態で追加されるため、インターフェイス モニタリングに影響を及ぼさないことに注意してください。

ステップ 1 Firepower Chassis Manager で、[Logical Devices] を選択します。

ステップ 2 右上にある [Edit] アイコンをクリックして、その論理デバイスを編集します。

ステップ 3 [Data Ports] 領域で新しいデータ インターフェイスを選択して、そのインターフェイスを割り当てます。

まだインターフェイスを削除しないでください。



ステップ 4 次のように、管理インターフェイスまたはイベント インターフェイスを置き換えます。

これらのタイプのインターフェイスでは、変更を保存するとデバイスがリブートします。

a) ページ中央のデバイス アイコンをクリックします。

b) [一般（General）] または [クラスタ情報（Cluster Information）] タブで、ドロップダウン リストから新しい [管理インターフェイス（Management Interface）] を選択します。

c) [Settings] タブで、ドロップダウン リストから新しい [Eventing Interface] を選択します。

d) [OK] をクリックします。

管理インターフェイスの IP アドレスを変更した場合は、Firepower Management Center でデバイスの IP アドレスも変更する必要があります。**[Devices]** > **[Device Management]** > **[Device/Cluster]** と移動します。[Management] 領域で、ブートストラップ設定アドレスと一致するように IP アドレスを設定します。

ステップ 5 [保存（Save）] をクリックします。

ステップ 6 FMC でインターフェイスを同期します。

a) FMC にログインします。

b) **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** の順に選択し、FTD デバイスの編集アイコン（ ）をクリックします。[インターフェイス（Interfaces）] タブがデフォルトで選択されます。

c) [インターフェイス（Interfaces）] タブの左上にある [デバイスの同期（Sync Device）] ボタンをクリックします。

d) 変更が検出されると、インターフェイス設定が変更されたことを示す赤色のバナーが [インターフェイス（Interfaces）] ページに表示されます。[クリックして詳細を表示（Click to know more）] リンクをクリックしてインターフェイスの変更内容を表示します。

e) インターフェイスを削除する予定の場合は、古いインターフェイスから新しいインターフェイスに任意のインターフェイス設定を手動で転送します。

まだインターフェイスを削除していないので、既存の設定を参照できます。古いインターフェイスを削除して検証を再実行した後も、さらに設定を修正する機会があります。検証では、古いインターフェイスでまだ使用されているすべての場所が表示されます。

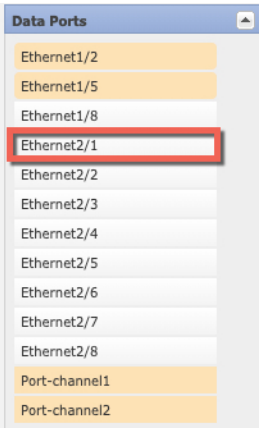
f) [変更の検証（Validate Changes）] をクリックし、インターフェイスが変更されてもポリシーが機能していることを確認します。

エラーがある場合は、ポリシーを変更して検証に戻る必要があります。

g) [Save] をクリックします。

h) [展開（Deploy）]をクリックし、割り当てたデバイスにポリシーを展開します。変更はポリシーを導入するまで有効になりません。

ステップ 7 Firepower Chassis Manager で、[データポート（Data Ports）] 領域でデータ インターフェイスの選択を解除し、そのインターフェイスの割り当てを解除します。



ステップ 8 [Save] をクリックします。

ステップ 9 FMC でインターフェイスを再度同期します。

アプリケーションのコンソールへの接続

次の手順を使用して、アプリケーションのコンソールに接続します。

ステップ 1 コンソール接続または Telnet 接続を使用して、モジュール CLI に接続します。

connect module *slot_number* {**console** | **telnet**}

複数のセキュリティ モジュールをサポートしないデバイスのセキュリティ エンジンに接続するには、*slot_number* として **1** を使用します。

Telnet 接続を使用する利点は、モジュールに同時に複数のセッションを設定でき、接続速度が速くなることです。

例：

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.

CISCO Serial Over LAN:
Close Network Connection to Exit
```

```
Firepower-module1>
```

ステップ 2 アプリケーションのコンソールに接続します。

connect ftd *name*

インスタンス名を表示するには、名前を付けずにコマンドを入力します。

例：

```
Firepower-module1> connect ftd ftd1
Connecting to ftd(ftd-native) console... enter exit to return to bootCLI
[...]
>
```

ステップ 3 アプリケーション コンソールを終了して FXOS モジュール CLI に移動します。

- FTD：**exit** と入力

ステップ 4 FXOS CLI のスーパバイザ レベルに戻ります。

コンソールを終了します。

a) ~ と入力

Telnet アプリケーションに切り替わります。

b) Telnet アプリケーションを終了するには、次を入力します。

telnet>**quit**

Telnet セッションを終了します。

a) **Ctrl-], .** と入力

Firepower Threat Defense の論理デバイスの履歴

機能	バージョン	詳細
FTD Firepower 4115、4125、および 4145	6.4.0	Firepower 4115、4125、および 4145 が導入されました。 （注） FXOS 2.6.1.157 が必要です。
Firepower 9300 SM-40、SM-48、および SM-56 のサポート	6.4.0	3 つのセキュリティ モジュール、SM-40、SM-48、および SM-56 が導入されました。 （注） FXOS 2.6.1.157 が必要です。

機能	バージョン	詳細
ASA および FTD を同じ Firepower 9300 の別のモジュールでサポート	6.4.0	ASA および FTD 論理デバイスを同じ Firepower 9300 上で展開できるようになりました。 （注） FXOS 2.6.1.157 が必要です。
モジュール/セキュリティ エンジンのいずれかの FTD コンテナ インスタンスでの SSL ハードウェア アクセラレーションのサポート	6.4.0	これで、モジュール/セキュリティ エンジンのいずれかのコンテナインスタンスに対して SSL ハードウェア アクセラレーションを有効にすることができるようになりました。他のコンテナインスタンスに対して SSL ハードウェア アクセラレーションは無効になっていますが、ネイティブインスタンスには有効になっています。 新規/変更された FXOS コマンド：**config hwCrypto enable** 変更された画面はありません。 （注） FXOS 2.6.1.157 が必要です。

機能	バージョン	詳細
Firepower 4100/9300 上の Firepower Threat Defense のマルチインスタンス機能	6.3.0	

機能	バージョン	詳細
		単一のセキュリティエンジンまたはモジュールに、それぞれ Firepower Threat Defense コンテナ インスタンスがある複数の論理デバイスを展開できるようになりました。以前は、単一のネイティブ アプリケーション インスタンスのみ展開できました。 柔軟な物理インターフェイスの使用を可能にするため、FXOS で VLAN サブインターフェイスを作成し、複数のインスタンス間でインターフェイスを共有することができます。リソース管理では、各インスタンスのパフォーマンス機能をカスタマイズできます。 2 台の個別のシャーシ上でコンテナ インスタンスを使用して高可用性を使用できます。クラスタリングはサポートされません。 （注） マルチインスタンス機能は、実装は異なりますが、ASA マルチ コンテキスト モードに似ています。マルチ コンテキスト モードは Firepower Threat Defense では利用できません。 新規/変更された [Firepower Management Center] 画面： • **[デバイス（Devices）] > [デバイス管理（Device Management）] > [編集（Edit）]** アイコン **> [インターフェイス（Interfaces）]** タブ 新規/変更された [Firepower Chassis Manager] 画面： • **[Overview] > [Devices]** • **[Interfaces] > [All Interfaces] > [Add New]** ドロップダウン メニュー **> [Subinterface]** • **[Interfaces] > [All Interfaces] > [Type]**

機能	バージョン	詳細
		• **[Logical Devices] > [Add Device]** • **[Platform Settings] > [Mac Pool]** • **[Platform Settings] > [Resource Profiles]** 新規/変更された FXOS コマンド：**connect ftd** *name*、**connect module telnet**、**create bootstrap-key PERMIT_EXPERT_MODE**、**createresource-profile**、**create subinterface**、**scope auto-macpool**、**set cpu-core-count**、**set deploy-type**、**set port-type data-sharing**、**set prefix**、**set resource-profile-name**、**set vlan**、**scope app-instance ftd** *name*、**show cgroups container**、**show interface**、**show mac-address**、**show subinterface**、**show tech-support module app-instance**、**show version** サポートされるプラットフォーム：Firepower 4100/9300

機能	バージョン	詳細
Firepower 4100/9300 のクラスタ制御リンクのカスタマイズ可能な IP アドレス	6.3.0	クラスタ制御リンクのデフォルトでは 127.2.0.0/16 ネットワークが使用されます。FXOS にクラスタを展開する際にネットワークを設定できるようになりました。シャーシは、シャーシ ID およびスロット ID（127.2.*chassis_id*.*slot_id*）に基づいて、各ユニットのクラスタ制御リンクインターフェイス IP アドレスを自動生成します。ただし、一部のネットワーク展開では、127.2.0.0/16 トラフィックはパスできません。そのため、ループバック（127.0.0.0/8）およびマルチキャスト（224.0.0.0/4）アドレスを除き、FXOS にクラスタ制御リンクのカスタム /16 サブネットを作成できるようになりました。 新規/変更された [Firepower Chassis Manager] 画面： • **[論理デバイス（Logical Devices）] > [デバイスの追加（Add Device）] > [クラスタ情報（Cluster Information）]** > [CCL Subnet IP] フィールド 新規/変更された FXOS コマンド：**set cluster-control-link network** サポートされるプラットフォーム：Firepower 4100/9300

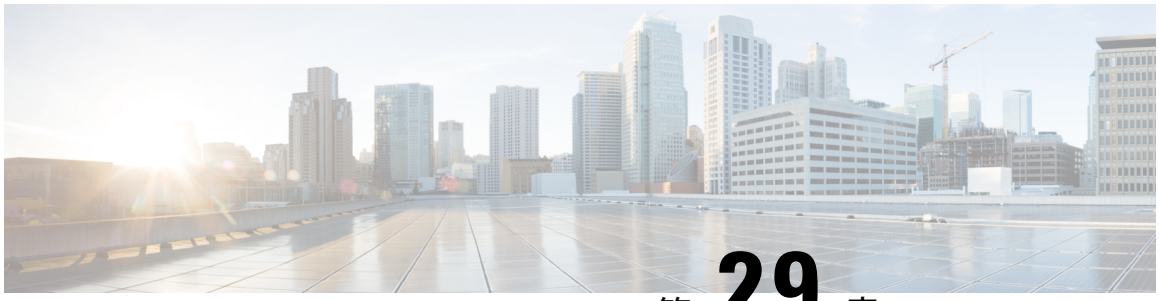
機能	バージョン	詳細
オン モードでのデータ EtherChannel のサポート	6.3.0	データおよびデータ共有 EtherChannel をアクティブ LACP モードまたはオンモードに設定できるようになりました。他の種類の EtherChannel は、アクティブ モードのみサポートしています。 新規/変更された [Firepower Chassis Manager] 画面： • **[インターフェイス（Interfaces）] > [すべてのインターフェイス（All Interfaces）] > [ポート チャネルの編集（Edit Port Channel）] > [モード（Mode）]** 新規/変更された FXOS コマンド：**set port-channel-mode** サポートされるプラットフォーム：Firepower 4100/9300
FTD インライン セットでの EtherChannel のサポート	6.2.0	FTD インライン セットで Etherchannel を使用できるようになりました。 サポートされるプラットフォーム：Firepower 4100/9300
6 つの FTD モジュールのシャーシ間クラスタリング	6.2.0	FTD のシャーシ間クラスタリングを有効化できます。最大 6 つのシャーシに最大 6 つのモジュールを含めることができます。 新規/変更された [Firepower Chassis Manager] 画面： • **[論理デバイス（Logical Devices）] > [構成（Configuration）]** サポートされるプラットフォーム：Firepower 4100/9300

機能	バージョン	詳細
サポート対象ネットワーク モジュールに対する Firepower 4100/9300 でのハードウェア バイパス サポート	6.1.0	ハードウェア バイパスは、停電時にトラフィックがインライン インターフェイス ペア間で流れ続けることを確認します。この機能は、ソフトウェアまたはハードウェア障害の発生時にネットワーク接続を維持するために使用できます。 新しい/変更された画面： • **[Devices] > [Device Management] > [Interfaces] > [Edit Physical Interface]** サポートされるプラットフォーム：Firepower 4100/9300
FTD のインライン セット リンク ステート伝達サポート	6.1.0	FTD アプリケーションでインライン セットを設定し、リンク ステート伝達を有効にすると、FTD はインライン セット メンバーシップを FXOS シャーシに送信します。リンク ステート伝達により、インライン セットのインターフェイスの 1 つが停止した場合、シャーシは、インライン インターフェイス ペアの 2 番目のインターフェイスも自動的に停止します。 新規/変更された FXOS コマンド：**show fault |grep link-down**、**show interface detail** サポートされるプラットフォーム：Firepower 4100/9300

機能	バージョン	詳細
Firepower 9300 の FTD でのシャーシ内クラスタリング サポート	6.0.1	Firepower 9300 が FTD アプリケーションでシャーシ内クラスタリングをサポートするようになりました。 新規/変更された [Firepower Chassis Manager] 画面： • **[論理デバイス（Logical Devices）] > [構成（Configuration）]** 新規/変更されたFXOSコマンド：**enter mgmt-bootstrap ftd, enter bootstrap-key FIREPOWER_MANAGER_IP, enter bootstrap-key FIREWALL_MODE, enter bootstrap-key-secret REGISTRATION_KEY, enter bootstrap-key-secret PASSWORD, enter bootstrap-key FQDN, enter bootstrap-key DNS_SERVERS, enter bootstrap-key SEARCH_DOMAINS, enter ipv4 firepower, enter ipv6 firepower, set value, set gateway, set ip, accept-license-agreement** サポートされるプラットフォーム：Firepower 4100/9300

第 VIII 部

Firepower Threat Defense インターフェイスとデバイスの設定



第 29 章

Firepower Threat Defense のインターフェイスの概要

FTD デバイスには、種々のモードで設定できるデータ インターフェイス、および管理/診断インターフェイスが組み込まれています。

管理/診断インターフェイス

物理的な管理インターフェイスは、診断論理インターフェイスと管理論理インターフェイスの間で共有できます。

管理インターフェイス

管理論理インターフェイスはデバイスの他のインターフェイスから切り離されています。これは、Firepower Management Center にデバイスを設定し、登録するために使用されます。また、固有の IP アドレスとスタティック ルーティングを使用します。管理インターフェイスを設定するには、CLI で **configure network** コマンドを使用します。管理インターフェイスを Firepower Management Center に追加した後にその IP アドレスを CLI で変更した場合、Firepower Management Center での IP アドレスを **[デバイス（Devices）] > [デバイス管理（Device Management）] > [デバイス（Devices）] > [管理（Management）]** 領域で一致させることができます。

診断インターフェイス

診断論理インターフェイスは残りのデータ インターフェイスとともに、**[デバイス（Devices）]**> **[デバイス管理（Device Management）]** > **[インターフェイス（Interfaces）]** 画面で設定できます。診断インターフェイスの使用はオプションです（シナリオについては、ルーテッドモードおよびトランスペアレントモードの展開を参照）。診断インターフェイスは管理トラフィックのみを許可し、トラフィックのスルーは許可しません。これはSSHをサポートしません。データ インターフェイスまたは管理インターフェイスのみに SSH を使用できます。診断インターフェイスは、SNMP や syslog のモニタリングに役立ちます。

インターフェイス モードとタイプ

通常のファイアウォール モードと IPS 専用モードの 2 つのモードで FTD インターフェイスを展開できます。同じデバイスにファイアウォールインターフェイスとIPS専用インターフェイスの両方を含めることができます。

通常のファイアウォール モード

ファイアウォール モードのインターフェイスでは、トラフィックが、フローの維持、IP レイヤおよび TCP レイヤの両方でのフロー状態の追跡、IP 最適化、TCP の正規化などのファイアウォール機能の対象となります。オプションで、セキュリティポリシーに従ってこのトラフィックに IPS 機能を設定することもできます。

設定できるファイアウォール インターフェイスのタイプは、ルーテッド モードとトランスペアレントモードのどちらのファイアウォールモードがそのデバイスに設定されているかによって異なります。詳細については、Firepower Threat Defense 用のトランスペアレントまたはルーテッド ファイアウォール モード （711 ページ）を参照してください。

- ルーテッドモードインターフェイス（ルーテッドファイアウォール モードのみ）：ルーティングを行う各インターフェイスは異なるサブネット上にあります。
- ブリッジグループ インターフェイス（ルーテッドおよびトランスペアレント ファイアウォールモード）：複数のインターフェイスをネットワーク上でグループ化することができ、Firepower Threat Defense デバイスはブリッジング技術を使用してインターフェイス間のトラフィックを通過させることができます。各ブリッジグループには、ネットワーク上で IP アドレスが割り当てられるブリッジ仮想インターフェイス（BVI）が含まれます。ルーテッド モードでは、Firepower Threat Defense デバイスは BVI と通常のルーテッド インターフェイス間をルーティングします。トランスペアレントモードでは、各ブリッジグループは分離されていて、相互通信できません。

IPS 専用モード

IPS専用モードのインターフェイスは、多数のファイアウォールのチェックをバイパスし、IPS セキュリティポリシーのみをサポートします。別のファイアウォールがこれらのインターフェイスを保護していて、ファイアウォール機能のオーバーヘッドを避けたい場合、IPS 専用のインターフェイスを実装することがあります。

（注） ファイアウォール モードは通常のファイアウォール インターフェイスのみに影響し、インライン セットやパッシブ インターフェイスなどのIPS専用インターフェイスには影響しません。IPS 専用インターフェイスはどちらのファイアウォール モードでも使用できます。

IPS 専用インターフェイスは以下のタイプとして展開できます。

- インライン セット、タップ モードのオプションあり：インライン セットは「Bump In The Wire」のように動作し、2 つのインターフェイスを一緒にバインドし、既存のネットワークに組み込みます。この機能によって、隣接するネットワーク デバイスの設定がなくても、任意のネットワーク環境にシステムをインストールすることができます。インライン インターフェイスはすべてのトラフィックを無条件に受信しますが、これらのインターフェイスで受信されたすべてのトラフィックは、明示的にドロップされない限り、インライン セットの外部に再送信されます。

  タップ モードの場合、デバイスはインラインで展開されますが、パケットがデバイスを通過する代わりに各パケットのコピーがデバイスに送信され、ネットワーク トラフィック フローは影響を受けません。ただし、これらのタイプのルールでは、トリガーされた侵入イベントが生成され、侵入イベントのテーブル ビューには、トリガーの原因となったパケットがインライン展開でドロップされたことが示されます。インライン展開されたデバイスでタップ モードを使用することには、利点があります。たとえば、デバイスがインラインであるかのようにデバイスとネットワークの間の配線をセットアップし、デバイスが生成するタイプの侵入イベントを分析することができます。その結果に基づいて、効率性に影響を与えることなく最適なネットワーク保護を提供するように、侵入ポリシーを変更して廃棄ルールを追加できます。デバイスをインラインで展開する準備ができたら、タップ モードを無効にして、デバイスとネットワークの間の配線を再びセットアップすることなく、不審なトラフィックをドロップし始めることができます。

  （注） 「透過インライン セット」としてインライン セットに馴染みがある人もいますが、インライン インターフェイスのタイプはトランスペアレント ファイアウォール モードやファイアウォール タイプのインターフェイスとは無関係です。

- パッシブまたはERSPAN パッシブ：パッシブ インターフェイスは、スイッチ SPAN またはミラー ポートを使用してネットワークを流れるトラフィックをモニタします。SPAN またはミラー ポートでは、スイッチ上の他のポートからトラフィックをコピーできます。この機能により、ネットワーク トラフィックのフローに含まれなくても、ネットワークでのシステムの可視性が備わります。パッシブ展開で構成されたシステムでは、特定のアクション（トラフィックのブロッキングやシェーピングなど）を実行することができません。パッシブ インターフェイスはすべてのトラフィックを無条件で受信します。このインターフェイスで受信されたトラフィックは再送されません。Encapsulated Remote Switched Port Analyzer（ERSPAN）インターフェイスは、複数のスイッチに分散された送信元ポートからのトラフィックをモニタし、GRE を使用してトラフィックをカプセル化します。

ERSPAN インターフェイスは、デバイスがルーテッド ファイアウォール モードになっている場合にのみ許可されます。

セキュリティ ゾーンとインターフェイス グループ

各インターフェイスは、セキュリティ ゾーンおよび/またはインターフェイス グループに割り当てる必要があります。その上で、ゾーンまたはグループに基づいてセキュリティ ポリシーを適用します。たとえば、内部インターフェイスを内部ゾーンに割り当て、外部インターフェイスを外部ゾーンに割り当てることができます。また、たとえば、トラフィックが内部から外部に移動できるようにアクセス コントロール ポリシーを設定することはできますが、外部から内部に向けては設定できません。 ポリシーによっては、セキュリティ ゾーンだけをサポートする場合も、ゾーンとグループの両方をサポートする場合もあります。詳細については、インターフェイス オブジェクト：インターフェイス グループとセキュリティ ゾーン（535 ページ）を参照してください。セキュリティ ゾーンおよびインターフェイス グループは、[オブジェクト（Objects）] ページで作成できます。また、インターフェイスを設定する際にゾーンを追加することもできます。インターフェイスは、そのインターフェイスに適切なタイプのゾーン（パッシブ、インライン、ルーテッド、スイッチド ゾーン タイプ）にのみ追加できます。

診断/管理インターフェイスは、ゾーンまたはインターフェイス グループには属しません。

Auto-MDI/MDIX 機能

RJ-45 インターフェイスでは、デフォルトの自動ネゴシエーション設定に Auto-MDI/MDIX 機能も含まれています。Auto-MDI/MDIX は、オートネゴシエーション フェーズでストレート ケーブルを検出すると、内部クロスオーバーを実行することでクロス ケーブルによる接続を不要にします。インターフェイスの Auto-MDI/MDIX をイネーブルにするには、速度とデュプレックスのいずれかをオートネゴシエーションに設定する必要があります。速度とデュプレックスの両方に明示的に固定値を指定すると、両方の設定でオートネゴシエーションがディセーブルにされ、Auto-MDI/MDIX もディセーブルになります。ギガビット イーサネットの速度と二重通信をそれぞれ 1000 と全二重に設定すると、インターフェイスでは常にオートネゴシエーションが実行されるため、Auto-MDI/MDIX は常にイネーブルになり、ディセーブルにできません。

インターフェイスのデフォルト設定

この項では、インターフェイスのデフォルト設定を示します。

インターフェイスのデフォルトの状態

インターフェイスの状態は、タイプによって異なります。

- 物理インターフェイス：ディセーブル。初期セットアップで有効になる診断インターフェイスは例外です。

- 冗長インターフェイス：イネーブル。ただし、トラフィックが冗長インターフェイスを通過するためには、メンバ物理インターフェイスもイネーブルになっている必要があります。
- VLANサブインターフェイス：イネーブル。ただし、トラフィックがサブインターフェイスを通過するためには、物理インターフェイスもイネーブルになっている必要があります。
- EtherChannelポートチャネルインターフェイス（ASAモデル）：有効。ただし、トラフィックがEtherChannelを通過するためには、チャネルグループ物理インターフェイスもイネーブルになっている必要があります。
- EtherChannel ポートチャネル インターフェイス（Firepower モデル）：ディセーブル。

（注） Firepower 4100/9300 の場合、管理上、シャーシおよび FMC の両方で、インターフェイスを有効および無効にできます。インターフェイスを動作させるには、両方のオペレーティング システムで、インターフェイスを有効にする必要があります。インターフェイスの状態は個別に制御されるので、シャーシと FMC の間の不一致が生じることがあります。

デフォルトの速度および二重通信

デフォルトでは、銅線（RJ-45）インターフェイスの速度とデュプレックスは、オートネゴシエーションに設定されます。

物理インターフェイスの有効化およびイーサネット設定の構成

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin Access Admin Network Admin

ここでは、次の方法について説明します。

- 物理インターフェイスを有効にします。デフォルトでは、物理インターフェイスは無効になっています（診断 インターフェイスを除く）。
- 特定の速度と二重通信を設定します。デフォルトでは、速度とデュプレックスは [自動（Auto）] に設定されます。

この手順は、インターフェイス設定のごく一部にすぎません。この時点では、他のパラメータを設定しないようにします。たとえば、EtherChannel または冗長インターフェイスの一部として使用するインターフェイスには名前を付けることはできません。

（注） Firepower 4100/9300 の場合、FXOS の基本インターフェイスの設定を行います。詳細については、物理インターフェイスの設定 （756 ページ）を参照してください。

始める前に

FMC に追加した後、デバイスの物理インターフェイスを変更した場合、[インターフェイス（Interfaces）] タブの左上にある [デバイスからのインターフェイスの同期（Sync Interfaces from device）] ボタンをクリックしてそのインターフェイス リストを更新する必要があります。

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** の順に選択し、FTD デバイスの編集アイコン（）をクリックします。デフォルトで [インターフェイス（Interfaces）] タブが選択されています。

ステップ 2 編集するインターフェイスの編集アイコン（）をクリックします。

ステップ 3 [有効（Enabled）] チェック ボックスをオンにして、インターフェイスを有効化します。

ステップ 4 （任意） [説明（Description）] フィールドに説明を追加します。

説明は 200 文字以内で入力できます。改行を入れずに 1 行で入力します。

ステップ 5 （任意） [ハードウェア構成（Hardware Configuration）] タブをクリックして、デュプレックスと速度を設定します。

- [デュプレックス（Duplex）] : [全（Full）]、[半（Half）]、または [自動（Auto）] を選択します。[自動（Auto）] は、インターフェイスによってサポートされる場合のみデフォルトとなります。たとえば、Firepower 2100 シリーズの SFP インターフェイスでは [自動（Auto）] を選択できません。
- [速度（Speed）] : [10]、[100]、[1000]、または [自動（Auto）] を選択します。デフォルトは [自動（Auto）] です。インターフェイスのタイプによって、選択可能なオプションが制限されます。たとえば、Firepower 2100 シリーズ デバイスでは、GigabitEthernet ポートでは 10、100、1000（1Gbps）、SFP ポートでは 1000 または 10000（10 Gbps）を選択できます。Firepower 2100 シリーズ デバイスの SFP インターフェイスは、[自動（Auto）] をサポートしていないことに注意してください。

ステップ 6 [モード（Mode）] ドロップダウン リストで、次のいずれかを選択します。

- [なし（None）]: この設定を通常のファイアウォール インターフェイスおよびインライン セットに選択します。他の設定に基づいて [ルーテッド（Routed）]、[スイッチド（Switched）]、または [インライン（Inline）] にモードが自動的に変更されます。
- [パッシブ（Passive）] : この設定を IPS 専用インターフェイスに選択します。
- [Erspan] : この設定を Erspan パッシブ IPS 専用インターフェイスに選択します。

ステップ 7 [OK] をクリックします。

ステップ 8 **[Save（保存）]** をクリックします。

これで、[Deploy]をクリックして割り当てられているデバイスにポリシーを展開できます。変更はポリシーを導入するまで有効になりません。

インターフェイスの変更と Firepower Management Center の同期

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin Access Admin Network Admin

デバイスのインターフェイスの設定を変更することによって FMC とデバイスが同期しなくなる可能性があります。FMC は次の方法のいずれかでインターフェイスの変更を検出できます。

- デバイスから送信されたイベント
- からの展開の同期 FMC

  展開を試行したときに FMC がインターフェイスを検出すると、その展開は失敗します。最初にインターフェイスの変更を承認する必要があります。
- 手動同期

FMC が変更を検出すると、[インターフェイス（Interface）] タブの各インターフェイス アイコンの左側にステータス アイコン（[削除済み（removed）]、[変更済み（changed）]、または [追加済み（added）]）が表示されます。

新しいインターフェイスを追加したり、未使用のインターフェイスを削除したりしても、FTD の設定に与える影響は最小限です。ただし、セキュリティ ポリシーで使用されているインターフェイスを削除すると、設定に影響を与えます。インターフェイスは、アクセス ルール、NAT、SSL、アイデンティティ ルール、VPN、DHCP サーバなど、FTD の設定における多くの場所で直接参照されている可能性があります。インターフェイスを削除すると、そのインターフェイスに関連付けられている設定がすべて削除されます。セキュリティ ゾーンを参照するポリシーは影響を受けません。また、論理デバイスに影響を与えず、かつ FMC での同期を必要とせずに、割り当てられた EtherChannel のメンバーシップを編集できます。

この手順では、必要に応じてデバイスの変更を手動で同期する方法と、検出された変更を保存する方法について説明します。デバイスの変更が一時的なものである場合は、その変更を FMC に保存する必要はありません。デバイスが安定するまで待機してから再同期します。

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** の順に選択し、FTD デバイスの編集アイコン（  ）をクリックします。デフォルトで [インターフェイス（Interfaces）] タブが選択されています。

ステップ 2 必要に応じて、[インターフェイス（Interfaces）] タブの左上にある [デバイスの同期（Sync Device）] ボタンをクリックします。

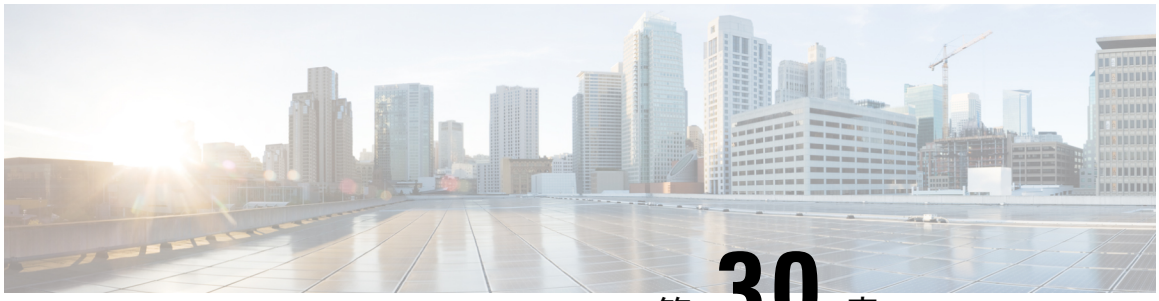
ステップ 3 変更が検出されると、インターフェイス設定が変更されたことを示す赤色のバナーが [インターフェイス（Interfaces）] タブに表示されます。[クリックして詳細を表示（Click to know more）] リンクをクリックしてインターフェイスの変更内容を表示します。

ステップ 4 [変更の検証（Validate Changes）] をクリックし、インターフェイスが変更されてもポリシーが機能していることを確認します。

エラーがある場合は、ポリシーを変更して検証に戻る必要があります。

ステップ 5 **[Save（保存）]** をクリックします。

これで、[Deploy] をクリックして割り当てられているデバイスにポリシーを展開できます。変更はポリシーを導入するまで有効になりません。



第 30 章

Firepower Threat Defense の通常のファイアウォール インターフェイス

この章では、 EtherChannel、VLAN サブインターフェイス、IP アドレスなどを含む通常のファイアウォール FTD インターフェイスの設定について説明します。

（注） Firepower 4100/9300 の最初のインターフェイスの設定については、インターフェイスの設定（755 ページ）を参照してください。

EtherChannel と冗長インターフェイスの設定

このセクションでは、EtherChannel インターフェイスと冗長インターフェイスを設定する方法について説明します。

（注） Firepower 4100/9300 の場合は、FXOS の EtherChannel を設定します。詳細については、EtherChannel（ポートチャネル）の追加 （757 ページ）を参照してください。冗長インターフェイスはサポートされません。

EtherChannel インターフェイスと冗長インターフェイスについて

この項では、EtherChannel インターフェイスと冗長インターフェイスについて説明します。

冗長インターフェイスについて

論理冗長インターフェイスは、物理インターフェイスのペア（アクティブ インターフェイスとスタンバイ インターフェイス）で構成されます。アクティブ インターフェイスで障害が発生すると、スタンバイ インターフェイスがアクティブになって、トラフィックを通過させ始めます。冗長インターフェイスを設定してFirepower Threat Defense デバイスの信頼性を高めることができます。

最大 8 個の冗長インターフェイス ペアを設定できます。

冗長インターフェイスの MAC アドレス

冗長インターフェイスでは、追加した最初の物理インターフェイスの MAC アドレスを使用します。コンフィギュレーションでメンバー インターフェイスの順序を変更すると、MAC アドレスは、リストの最初になったインターフェイスの MAC アドレスと一致するように変更されます。または、冗長インターフェイスに手動で MAC アドレスを割り当てることができます。これはメンバー インターフェイスの MAC アドレスに関係なく使用されます。アクティブ インターフェイスがスタンバイ インターフェイスにフェールオーバーすると、トラフィックが中断しないように同じ MAC アドレスが維持されます。

EtherChannel について

802.3ad EtherChannel は、単一のネットワークの帯域幅を増やすことができるように、個別のイーサネット リンク（チャネル グループ）のバンドルで構成される論理インターフェイスです（ポートチャネル インターフェイスと呼びます）。ポートチャネル インターフェイスは、インターフェイス関連の機能を設定するときに、物理インターフェイスと同じように使用します。

モデルでサポートされているインターフェイスの数に応じて、最大 48 個の Etherchannel を設定できます。

チャネル グループのインターフェイス

各チャネルグループには、最大16個のアクティブインターフェイスを設定できます。ただし、Firepower 1000 または 2100 は、8 個のアクティブインターフェイスをサポートしています。8 個のアクティブ インターフェイスだけをサポートするスイッチの場合、1つのチャネル グループに最大 16 個のインターフェイスを割り当てることができます。インターフェイスは 8 個のみアクティブにできるため、残りのインターフェイスは、インターフェイスの障害が発生した場合のスタンバイ リンクとして動作できます。16 個のアクティブインターフェイスの場合、スイッチがこの機能をサポートしている必要があります（たとえば、Cisco Nexus 7000 と F2 シリーズ 10 ギガビット イーサネット モジュール）。

チャネル グループのすべてのインターフェイスは、同じタイプと速度である必要があります。チャネル グループに追加された最初のインターフェイスによって、正しいタイプと速度が決まります。

EtherChannelによって、チャネル内の使用可能なすべてのアクティブ インターフェイスのトラフィックが集約されます。インターフェイスは、送信元または宛先 MAC アドレス、IP アドレ

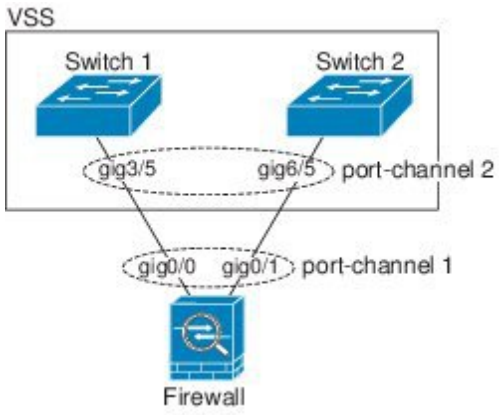
ス、TCP および UDP ポート番号、および VLAN 番号に基づいて、独自のハッシュ アルゴリズムを使用して選択されます。

別のデバイスの EtherChannel への接続

FTD EtherChannel の接続先のデバイスも 802.3ad EtherChannel をサポートしている必要があります。たとえば、Catalyst 6500 スイッチまたは Cisco Nexus 7000 に接続できます。

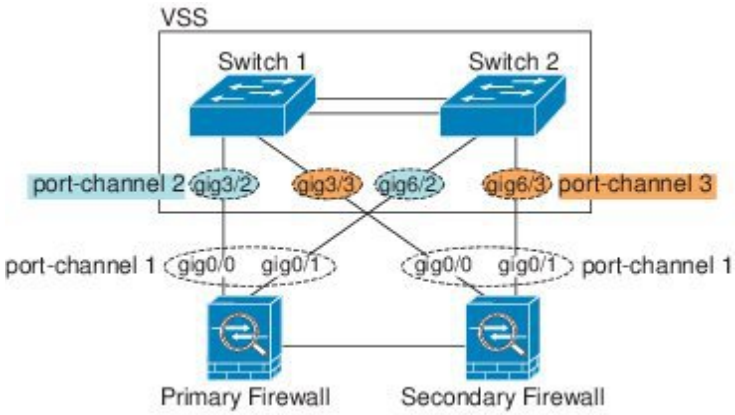
スイッチが仮想スイッチング システム（VSS）または 仮想ポート チャネル（vPC）の一部である場合、同じ EtherChannel 内の FTD インターフェイスを VSS/vPC 内の個別のスイッチに接続できます。スイッチ インターフェイスは同じ EtherChannel ポートチャネル インターフェイスのメンバです。複数の個別のスイッチが単一のスイッチのように動作するからです。

図 *12 : VSS/vPC* への接続



FTD をアクティブ/スタンバイ フェールオーバー配置で使用する場合、FTD ごとに 1 つ、VSS/vPC 内のスイッチで個別の EtherChannel を作成する必要があります。各 FTD で、1 つの EtherChannel が両方のスイッチに接続します。すべてのスイッチインターフェイスを両方の FTD に接続する単一の EtherChannel にグループ化できる場合でも（この場合、個別の FTD システム ID のため、EtherChannel は確立されません）、単一の EtherChannel は望ましくありません。これは、トラフィックをスタンバイ FTD に送信しないようにするためです。

図 *13 :* アクティブ/スタンバイ フェールオーバーと *VSS/vPC*



Link Aggregation Control Protocol

リンク集約制御プロトコル（LACP）では、2 つのネットワーク デバイス間でリンク集約制御プロトコル データ ユニット（LACPDU）を交換することによって、インターフェイスが集約されます。

EtherChannel 内の各物理インターフェイスを次のように設定できます。

- アクティブ：LACP アップデートを送信および受信します。アクティブ EtherChannel は、アクティブまたはパッシブ EtherChannel と接続を確立できます。LACP トラフィックを最小にする必要がある場合以外は、アクティブ モードを使用する必要があります。
- パッシブ：LACP アップデートを受信します。パッシブ EtherChannel は、アクティブ EtherChannel のみと接続を確立できます。Firepower ハードウェア モデルではサポートされていません。
- オン：EtherChannel は常にオンであり、LACP は使用されません。「オン」の EtherChannel は、別の「オン」の EtherChannel のみと接続を確立できます。

LACP では、ユーザが介入しなくても、EtherChannel へのリンクの自動追加および削除が調整されます。また、コンフィギュレーションの誤りが処理され、メンバインターフェイスの両端が正しいチャネル グループに接続されていることがチェックされます。「オン」モードではインターフェイスがダウンしたときにチャネル グループ内のスタンバイ インターフェイスを使用できず、接続とコンフィギュレーションはチェックされません。

ロード バランシング

FTD は、パケットの送信元および宛先 IP アドレスをハッシュすることによって、パケットを EtherChannel 内のインターフェイスに分散します（この基準は設定可能です）。生成されたハッシュ値をアクティブなリンクの数で割り、そのモジュロ演算で求められた余りの値によってフローの割り当て先のインターフェイスが決まります。*hash_value* **mod** *active_links* の結果が 0 となるすべてのパケットは、EtherChannel 内の最初のインターフェイスへ送信され、以降は結果が 1 となるものは 2 番目のインターフェイスへ、結果が 2 となるものは 3 番目のインターフェイスへ、というように送信されます。たとえば、15 個のアクティブ リンクがある場合、モジュロ演算では 0 ～ 14 の値が得られます。6 個のアクティブ リンクの場合、値は 0 ～ 5 となり、以降も同様になります。

アクティブ インターフェイスがダウンし、スタンバイ インターフェイスに置き換えられない場合、トラフィックは残りのリンク間で再バランスされます。失敗はレイヤ 2 のスパニングツリーとレイヤ 3 のルーティング テーブルの両方からマスクされるため、他のネットワーク デバイスへのスイッチオーバーはトランスペアレントです。

EtherChannel MAC アドレス

1 つのチャネル グループに含まれるすべてのインターフェイスは、同じ MAC アドレスを共有します。この機能によって、EtherChannel はネットワーク アプリケーションとユーザに対してトランスペアレントになります。ネットワーク アプリケーションやユーザから見えるのは 1 つの論理接続のみであり、個々のリンクのことは認識しないからです。

ポートチャネルインターフェイスは、最も小さいチャネル グループ インターフェイスの MAC アドレスをポート チャネル MAC アドレスとして使用します。または、ポートチャネル インターフェイスの MAC アドレスを手動で設定することもできます。グループ チャネルインターフェイスのメンバーシップを変更する場合は、固有の MAC アドレスを設定することを推奨します。ポートチャネル MAC アドレスを提供していたインターフェイスを削除すると、そのポートチャネルの MAC アドレスは次に番号が小さいインターフェイスに変わるため、トラフィックが分断されます。

EtherChannel インターフェイスと冗長インターフェイスのガイドライン

Bridge Group

ルーテッド モードでは、FMC で定義された EtherChannel はブリッジ グループ メンバーとしてサポートされません。Firepower 4100/9300 上の Etherchannel は、ブリッジ グループ メンバーにすることができます。

高可用性

- 冗長インターフェイスまたは EtherChannel インターフェイスを 高可用性 リンクとして使用する場合、高可用性ペアの両方のユニットでその事前設定を行う必要があります。プライマリ ユニットで設定し、セカンダリ装置に複製されることは想定できません。これは、複製には 高可用性 リンク自体が必要であるためです。
- 冗長インターフェイスまたは EtherChannel インターフェイスをステート リンクに対して使用する場合、特別なコンフィギュレーションは必要ありません。コンフィギュレーションは通常どおりプライマリ装置から複製されます。Firepower 4100/9300 シャーシ では、Etherchannel を含むすべてのインターフェイスを両方のユニットで事前に設定する必要があります。
- **monitor-interface** コマンドを使用して、高可用性。アクティブなメンバインターフェイスがスタンバイインターフェイスにフェールオーバーすると、デバイスレベルの 高可用性 をモニタしているときには、冗長インターフェイスまたは EtherChannel インターフェイスで障害が発生しているようには見えません。すべての物理インターフェイスで障害が発生した場合にのみ、冗長インターフェイスまたは EtherChannel インターフェイスで障害が発生しているように見えます（EtherChannel インターフェイスでは、障害の発生が許容されるメンバ インターフェイスの数を設定できます）。
- EtherChannel インターフェイスを 高可用性 またはステートリンクに対して使用する場合、順序が不正なパケットを防止するために、EtherChannel 内の 1 つのインターフェイスのみが使用されます。そのインターフェイスで障害が発生した場合は、EtherChannel 内の次のリンクが使用されます。高可用性 リンクとして使用中の EtherChannel の設定は変更できません。設定を変更するには、高可用性 を一時的に無効にする必要があります。これにより、高可用性 がその期間に発生することはありません。

サポート モデル

- Firepower 4100/9300 または FTDv では FMC に Etherchannel を追加することはできません。Firepower 4100/9300 は Etherchannel をサポートしていますが、シャーシ上の FXOS で Etherchannel のすべてのハードウェア設定を実行する必要があります。
- Firepower 2100、 Firepower 2100、Firepower 4100/9300 シャーシでは、冗長インターフェイスはサポートされていません。
- Etherchannel で Firepower 1010 のスイッチ ポートまたは VLAN インターフェイスを使用することはできません。

冗長インターフェイスの一般的なガイドライン

- 最大 8 個の冗長インターフェイス ペアを設定できます。
- すべてのFTD コンフィギュレーションは、メンバ物理インターフェイスではなく論理冗長インターフェイスを参照します。
- EtherChannel の一部として冗長インターフェイスを使用することはできません。また、冗長インターフェイスの一部として EtherChannel を使用することはできません。冗長インターフェイスと EtherChannel インターフェイスでは同じ物理インターフェイスを使用できません。ただし、同じ物理インターフェイスを使用するのでなければ、両方のタイプを FTD 上で設定することができます。
- アクティブ インターフェイスをシャットダウンすると、スタンバイ インターフェイスがアクティブになります。
- 冗長インターフェイスは、診断 *slot*/*port*インターフェイスをメンバーとしてサポートしません。ただし、診断インターフェイス以外の複数インターフェイスからなる冗長インターフェイスを、管理専用として設定できます。

EtherChannel の一般的なガイドライン

- モデルで使用可能なインターフェイスの数に応じて、最大48 個の Etherchannel を設定できます。
- 各チャネルグループには、最大 16 個のアクティブインターフェイスを設定できます。ただし、Firepower 1000 または 2100 は、8 個のアクティブインターフェイスをサポートしています。8 個のアクティブ インターフェイスだけをサポートするスイッチの場合、1 つのチャネル グループに最大16個のインターフェイスを割り当てることができます。インターフェイスは8個のみアクティブにできるため、残りのインターフェイスは、インターフェイスの障害が発生した場合のスタンバイ リンクとして動作できます。16 個のアクティブ インターフェイスの場合、スイッチがこの機能をサポートしている必要があります（たとえば、Cisco Nexus 7000 と F2 シリーズ 10 ギガビット イーサネット モジュール）。
- チャネル グループのすべてのインターフェイスは、同じタイプと速度である必要があります。チャネル グループに追加された最初のインターフェイスによって、正しいタイプと速度が決まります。

- FTD の EtherChannel の接続先デバイスも 802.3ad EtherChannel をサポートしている必要があります。
- FTD は、VLAN タグ付きの LACPDU をサポートしていません。Cisco IOS **vlan dot1Q tag native** コマンドを使用して、隣接スイッチのネイティブ VLAN タギングをイネーブルにすると FTD はタグ付きの LACPDU をドロップします。隣接スイッチのネイティブ VLAN タギングは、必ずディセーブルにしてください。
- 15.1(1)S2 以前の Cisco IOS ソフトウェアバージョンを実行する FTD では、スイッチスタックへの EtherChannel の接続がサポートされていませんでした。デフォルトのスイッチ設定では、FTD EtherChannel がクロススタックに接続されている場合、マスタースイッチの電源がオフになると、残りのスイッチに接続されている EtherChannel は起動しません。互換性を高めるため、**stack-mac persistent timer** コマンドを設定して、十分なリロード時間を確保できる大きな値、たとえば 8 分、0 （無制限）などを設定します。または、15.1(1)S2 など、より安定したスイッチ ソフトウェア バージョンにアップグレードできます。
- すべての FTD コンフィギュレーションは、メンバ物理インターフェイスではなく論理 EtherChannel インターフェイスを参照します。
- EtherChannel の一部として冗長インターフェイスを使用することはできません。また、冗長インターフェイスの一部として EtherChannel を使用することはできません。冗長インターフェイスと EtherChannel インターフェイスでは同じ物理インターフェイスを使用できません。ただし、同じ物理インターフェイスを使用するのでなければ、両方のタイプを FTD 上で設定することができます。

冗長インターフェイスの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin Access Admin Network Admin

論理冗長インターフェイスは、物理インターフェイスのペア（アクティブインターフェイスとスタンバイ インターフェイス）で構成されます。アクティブ インターフェイスで障害が発生すると、スタンバイインターフェイスがアクティブになって、トラフィックを通過させ始めます。冗長インターフェイスを設定してFTDの信頼性を高めることができます。デフォルトでは、冗長インターフェイスは有効になっています。

- 最大 8 個の冗長インターフェイス ペアを設定できます。
- 両方のメンバインターフェイスが同じ物理タイプである必要があります。たとえば、両方ともギガビット イーサネットにする必要があります。

（注） 冗長インターフェイスは Firepower 4100/9300 ではサポートされていません。

始める前に

- 名前が設定されている場合は、物理インターフェイスを冗長インターフェイスに追加できません。最初に名前を削除する必要があります。

注意 コンフィギュレーション内で物理インターフェイスをすでに使用している場合、名前を削除すると、このインターフェイスを参照しているすべてのコンフィギュレーションが消去されます。

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** の順に選択し、FTD デバイスの編集アイコン（）をクリックします。デフォルトで [インターフェイス（Interfaces）] タブが選択されています。

ステップ 2 物理インターフェイスの有効化およびイーサネット設定の構成（789ページ）に従って、メンバーインターフェイスを有効にします。

ステップ 3 **[インターフェイスの追加（Add Interfaces）]** > **[冗長インターフェイス（Redundant Interface）]** をクリックします。

ステップ 4 [一般（General）] タブで、次のパラメータを設定します。

a) [冗長 ID（Redundant ID）]：1 ～ 8 の整数を設定します。

b) [プライマリ インターフェイス（Primary Interface）]：ドロップダウン リストからインターフェイスを選択します。インターフェイスを追加すると、インターフェイスのコンフィギュレーション（IP アドレスなど）はすべて削除されます。

c) [セカンダリ インターフェイス（Secondary Interface）]：2 番目のインターフェイスは、最初のインターフェイスと同じ物理的なタイプである必要があります。

ステップ 5 [OK] をクリックします。

ステップ 6 **[Save（保存）]** をクリックします。

これで、[Deploy] をクリックして割り当てられているデバイスにポリシーを展開できます。変更はポリシーを導入するまで有効になりません。

ステップ 7 （任意） VLAN サブインターフェイスを追加します。サブインターフェイスの追加（805 ページ）を参照してください。

ステップ 8 ルーテッドまたはトランスペアレント モード インターフェイスのパラメータを設定します。ルーテッドモードのインターフェイスの設定（810 ページ）またはの□ブリッジ グループ インターフェイスの設定（813 ページ）を参照してください。

EtherChannel の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin Access Admin Network Admin

ここでは、EtherChannel ポートチャネル インターフェイスの作成、インターフェイスの EtherChannel への割り当て、EtherChannel のカスタマイズ方法について説明します。

ガイドライン

- モデルのインターフェイスの数に応じて、最大 48 個の Etherchannel を設定できます。
- 各チャネル グループには、最大 16 個のアクティブ インターフェイスを持たせることができます。ただし、Firepower 1000 または 2100 は、8 個のアクティブ インターフェイスをサポートしています。8 個のアクティブ インターフェイスだけをサポートするスイッチの場合、1 つのチャネル グループに最大 16 個のインターフェイスを割り当てることができます。インターフェイスは 8 個のみアクティブにできるため、残りのインターフェイスは、インターフェイスの障害が発生した場合のスタンバイ リンクとして動作できます。
- チャネル グループのすべてのインターフェイスは、同じタイプ、速度、および二重通信である必要があります。半二重はサポートされません。

（注） Firepower 4100/9300 の場合は、FXOS の EtherChannel を設定します。詳細については、EtherChannel（ポート チャネル）の追加 （757 ページ）を参照してください。

始める前に

- 名前が設定されている場合は、物理インターフェイスをチャネル グループに追加できません。最初に名前を削除する必要があります。

（注） コンフィギュレーション内で物理インターフェイスをすでに使用している場合、名前を削除すると、このインターフェイスを参照しているすべてのコンフィギュレーションが消去されます。

ステップ 1 **[デバイス（Devices）] > [デバイス管理（Device Management）]** の順に選択し、FTD デバイスの編集アイコン（）をクリックします。デフォルトで [インターフェイス（Interfaces）] タブが選択されています。

ステップ 2 物理インターフェイスの有効化およびイーサネット設定の構成 （789 ページ）に従って、メンバー インターフェイスを有効にします。

ステップ 3 **[インターフェイスの追加（Add Interfaces）] > [Ether Channel インターフェイス（Ether Channel Interface）]** をクリックします。

ステップ 4 [一般（General）] タブで、[イーサネットチャネルID（Ether Channel ID）] を 1 ～ 48（Firepower 1010 の場合は 1 および 8）の数値に設定します。

ステップ 5 [使用可能なインターフェイス（Available Interfaces）] 領域でインターフェイスをクリックし、[追加（Add）] をクリックして [選択したインターフェイス（Selected Interface）] 領域にそのインターフェイスを移動します。メンバーを作成するすべてのインターフェイスに対して繰り返します。

すべてのインターフェイスが同じタイプと速度であるようにします。最初に追加するインターフェイスによって、EtherChannel のタイプと速度が決まります。一致しないインターフェイスを追加すると、そのインターフェイスは停止状態になります。FMC では、一致しないインターフェイスの追加は防止されません。

ステップ 6 （任意） [詳細（Advanced）] タブをクリックして EtherChannel をカスタマイズします。[情報（Information）] サブタブで次のパラメータを設定します。

- （ASA 5500-X モデルのみ）[ロードバランシング（Load Balance）] : パケットをグループ チャネル インターフェイス間でロードバランスするために使用する基準を選択します。デフォルトでは、FTD デバイスはパケットの送信元および宛先 IP アドレスに従って、インターフェイスでのパケットのロードをバランスします。パケットが分類される基準になるプロパティを変更する場合は、別の基準のセットを選択します。たとえば、トラフィックが同じ送信元および宛先 IP アドレスに大きく偏っている場合、EtherChannel 内のインターフェイスに対するトラフィックの割り当てがアンバランスになります。別のアルゴリズムに変更すると、トラフィックはより均等に分散される場合があります。ロードバランシングの詳細については、ロードバランシング （796 ページ）を参照してください。
- [LACP モード（LACP Mode）] : [アクティブ（Active）]、[パッシブ（Passive）]、または [オン（On）] を選択します。[アクティブ（Active）] モード（デフォルト）を使用することを推奨します。
- （ASA 5500-X モデルのみ）[アクティブな物理インターフェイス：範囲（Active Physical Interface: Range）] : 左側のドロップダウン リストから、EtherChannel をアクティブにするために必要なアクティブ インターフェイスの最小数を 1 ～ 16 の範囲で選択します。デフォルトは 1 です。右側のドロップダウン リストから、EtherChannel で許可されるアクティブ インターフェイスの最大数を 1 ～ 16 の範囲で選択します。デフォルトは 16 です。スイッチが 16 個のアクティブ インターフェイスをサポートしていない場合、このコマンドは必ず 8 以下に設定する必要があります。
- [アクティブな MAC アドレス（Active Mac Address）] : 必要に応じて手動 MAC アドレスを設定します。mac_address は、H.H.H 形式で指定します。H は 16 ビットの 16 進数です。たとえば、MAC アドレス 00-0C-F1-42-4C-DE は、000C.F142.4CDE と入力します。

ステップ 7 （任意） [ハードウェア構成（Hardware Configuration）] タブをクリックしてデュプレックスと速度を設定し、すべてのメンバー インターフェイスでこれらの設定を上書きします。これらのパラメータはチャネル グループのすべてのインターフェイスで一致している必要があるため、この方法はこれらのパラメータを設定するショートカットになります。

ステップ 8 [OK] をクリックします。

ステップ 9 **[Save（保存）]** をクリックします。

これで、[Deploy] をクリックして割り当てられているデバイスにポリシーを展開できます。変更はポリシーを導入するまで有効になりません。

ステップ 10 （任意） VLAN サブインターフェイスを追加します。サブインターフェイスの追加 （805 ページ）を参照してください。

ステップ 11 ルーテッドまたはトランスペアレントモードインターフェイスのパラメータを設定します。ルーテッドモードのインターフェイスの設定 （810 ページ）またはの□ブリッジ グループ インターフェイスの設定（813 ページ）を参照してください。

VLAN サブインターフェイスと 802.1Q トランキングの設定

VLAN サブインターフェイスを使用すると、1 つの物理インターフェイス、冗長インターフェイス、または EtherChannel インターフェイスを、異なる VLAN ID でタグ付けされた複数の論理インターフェイスに分割できます。VLAN サブインターフェイスが 1 つ以上あるインターフェイスは、自動的に 802.1Q トランクとして設定されます。VLAN では、所定の物理インターフェイス上でトラフィックを分離しておくことができるため、物理インターフェイスまたはデバイスを追加しなくても、ネットワーク上で使用できるインターフェイスの数を増やすことができます。

VLAN サブインターフェイスのガイドラインと制限事項

高可用性

フェールオーバーリンクまたは状態リンクにサブインターフェイスを使用することはできません。ただし、コンテナ インターフェイスの場合は Firepower 4100/9300 シャーシに定義されているサブインターフェイスを使用できます。

その他のガイドライン

- 物理インターフェイス上のタグなしパケットの禁止：サブインターフェイスを使用する場合、物理インターフェイスでトラフィックを通過させないようにすることもよくあります。物理インターフェイスはタグのないパケットを通過させることができるためです。この特性は、冗長インターフェイスペアのアクティブな物理インターフェイスと EtherChannel リンクにも当てはまります。サブインターフェイスでトラフィックを通過させるには物理、冗長、または EtherChannel インターフェイスを有効にする必要があるため、インターフェイスに名前を設定しないことでトラフィックを通過させないようにします。物理インターフェイス、冗長インターフェイス、または EtherChannel インターフェイスでタグのないパケットを通過させる場合は、通常通り名前を設定できます。
- 診断インターフェイスではサブインターフェイスを設定できません。

- 同じ親インターフェイスのすべてのサブインターフェイスは、ブリッジグループ メンバーかルーテッドインターフェイスのいずれかである必要があります。混在および一致はできません。
- FTD はダイナミック トランキング プロトコル（DTP）をサポートしないため、接続されているスイッチ ポートを無条件にトランキングするように設定する必要があります。
- 親インターフェイスの同じ Burned-In MAC Address を使用するため、FTD で定義されたサブインターフェイスに一意の MAC アドレスを割り当てる必要のある場合があります。たとえば、サービス プロバイダーによっては、MAC アドレスに基づいてアクセス コントロールを実行する場合があります。また、IPv6 リンクローカル アドレスは MAC アドレスに基づいて生成されるため、サブインターフェイスに一意の MAC アドレスを割り当てることで、一意の IPv6 リンクローカル アドレスが可能になり、FTD で特定のインスタンスでのトラフィックの中断を避けることができます。

デバイス モデルによる VLAN サブインターフェイスの最大数

デバイスモデルにより、設定できる VLAN サブインターフェイスの最大数が制限されます。データインターフェイスでのみサブインターフェイスを設定することができ、管理インターフェイスでは設定できないことに注意してください。

次の表で、各デバイスモデルの制限について説明します。

モデル	VLAN サブインターフェイスの最大数
Firepower 1010	60
Firepower 1120	512
Firepower 1140	1024
Firepower 2100	1024
Firepower 4100	1024
Firepower 9300	1024
Firepower Threat Defense Virtual	50
ASA 5508-X	50
ASA 5515-X	100
ASA 5516-X	100
ASA 5525-X	200
ASA 5545-X	300
ASA 5555-X	500
ISA 3000	25

サブインターフェイスの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin Access Admin Network Admin

1 つ以上のサブインターフェイスを物理インターフェイス、冗長インターフェイス、または PortChannel インターフェイスに追加します。

Firepower 4100/9300 の場合、コンテナインターフェイスで使用するためのサブインターフェイスを FXOS で作成します。コンテナ インスタンスへの VLAN サブインターフェイスの追加 （759 ページ）を参照してください。これらのサブインターフェイスは FMC のインターフェイスリストに表示されます。FMC にサブインターフェイスを追加することもできますが、FXOS にサブインターフェイスが定義されていない親インターフェイス上に限ります。

（注） 親の物理インターフェイスがタグなしのパケットを渡します。タグなしのパケットを渡さない場合は、セキュリティ ポリシーの親インターフェイスが含まれていないことを確認します。

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** の順に選択し、FTD デバイスの編集アイコン（）をクリックします。デフォルトで [インターフェイス（Interfaces）] タブが選択されています。

ステップ 2 物理インターフェイスの有効化およびイーサネット設定の構成 （789 ページ）に従って、親インターフェイスを有効にします。

ステップ 3 **[インターフェイスの追加（Add Interfaces）]** > **[インターフェイス（Sub Interface）]** をクリックします。

ステップ 4 [一般（General）] タブで、次のパラメータを設定します。

a) [インターフェイス（Interface）]：サブインターフェイスを追加する物理、冗長、またはポートチャネル インターフェイスを選択します。

b) [サブインターフェイス ID（Sub-Interface ID）]：サブインターフェイス ID を 1 ～ 4294967295 の範囲の整数で入力します。許可されるサブインターフェイスの番号は、プラットフォームによって異なります。設定後は ID を変更できません。

c) [VLAN ID]：VLAN ID を 1 ～ 4094 の範囲で入力します。これは、このサブインターフェイス上のパケットにタグを付けるために使用されます。

この VLAN ID は一意である必要があります。

ステップ 5 [OK] をクリックします。

ステップ 6 **[Save（保存）]** をクリックします。

これで、[Deploy] をクリックして割り当てられているデバイスにポリシーを展開できます。変更はポリシーを導入するまで有効になりません。

ステップ 7 ルーテッドまたはトランスペアレント モード インターフェイスのパラメータを設定します。ルーテッド モードのインターフェイスの設定（810 ページ）またはの□ブリッジ グループ インターフェイスの設定（813 ページ）を参照してください。

ルーテッド モードとトランス ペアレント モードのインターフェイスの設定

この項では、ルーテッド ファイアウォール モードおよびトランスペアレント ファイアウォール モードで、すべてのモデルに対応する標準のインターフェイス設定を完了するためのタスクについて説明します。

ルーテッド モード インターフェイスとトランスペアレント モード インターフェイスについて

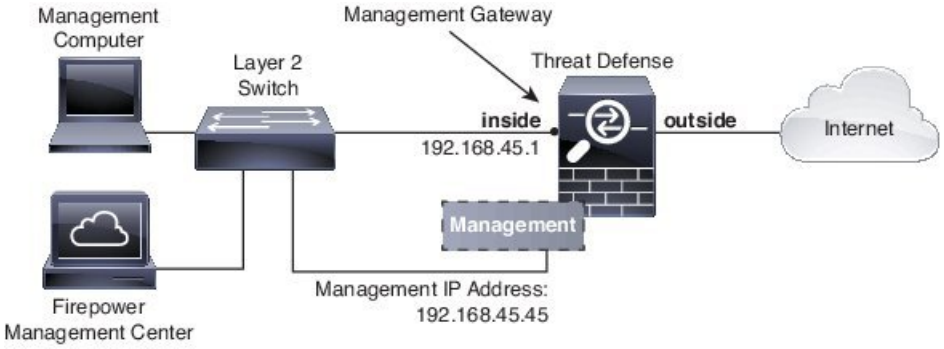
Firepower Threat Defense デバイス は、ルーテッドおよびブリッジという 2 つのタイプのインターフェイスをサポートします。

各レイヤ 3 ルーテッドインターフェイスは一意のサブネット上に IP アドレスを必要とします。

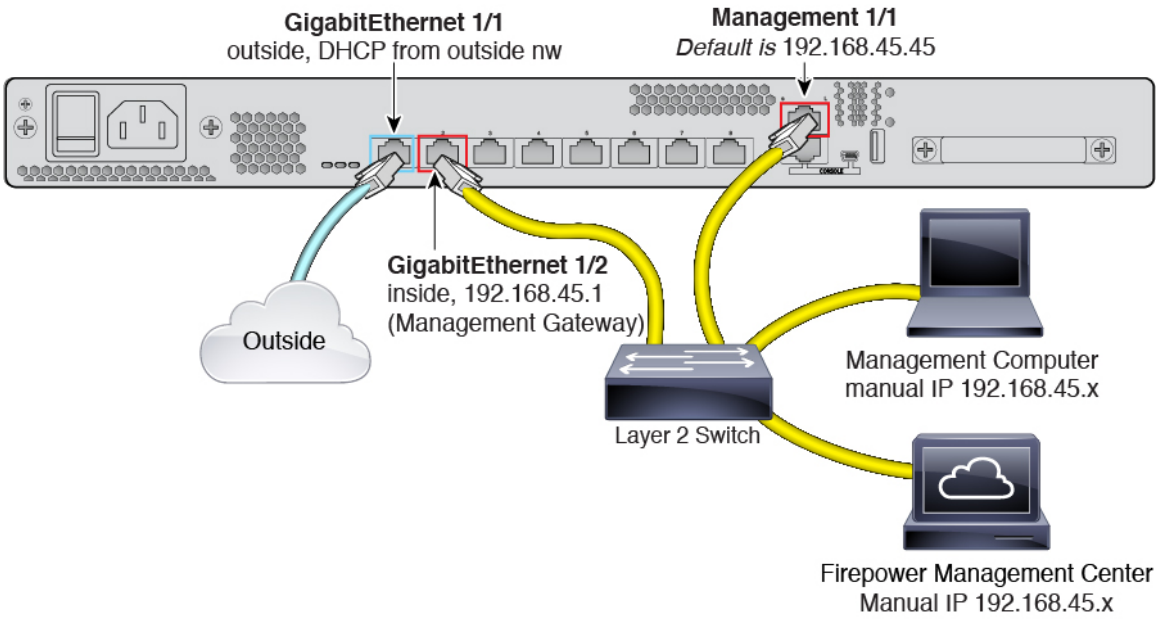
ブリッジインターフェイスはブリッジ グループに属し、すべてのインターフェイスは同じネットワーク内にあります。ブリッジ グループはブリッジ ネットワーク上に IP アドレスを持つブリッジ仮想インターフェイス（BVI）で表されます。ルーテッド モードは、ルーテッド インターフェイスとブリッジ インターフェイスの両方をサポートし、ルーテッド インターフェイスと BVI との間のルーティングが可能です。トランスペアレント ファイアウォール モードでは、ブリッジ グループと BVI インターフェイスのみがサポートされます。

ルーテッド モードの導入

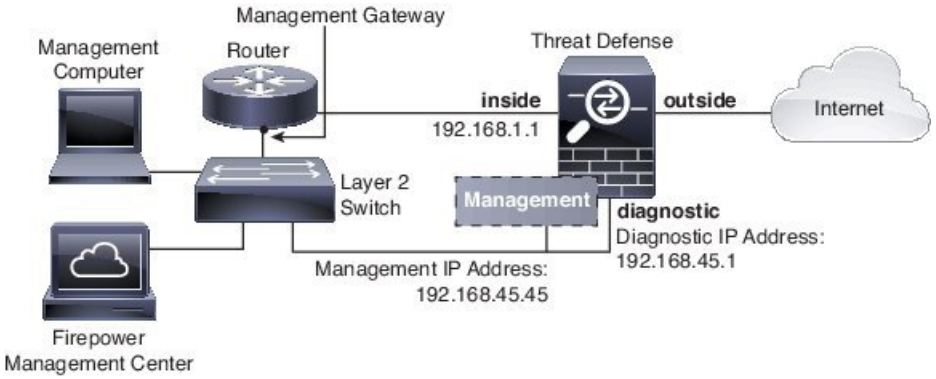
内部ルータがない場合は診断インターフェイスの IP アドレスを設定しないことをお勧めします。診断インターフェイスの IP アドレスを設定しなければ、他のデータ インターフェイスと同じネットワーク上に管理インターフェイスを配置できます。診断インターフェイスを設定すると、一般的にその IP アドレスは管理 IP アドレスと同じネットワークになり、他のデータ インターフェイスと同じネットワーク上に存在できない標準インターフェイスと見なされます。管理インターフェイスは更新のためにインターネットにアクセスする必要があるため、管理インターフェイスを内部インターフェイスと同じネットワーク上に置くと、内部にスイッチのみを持つ FTD デバイスを導入して、そのゲートウェイとして内部インターフェイスを指定できます。内部スイッチを使用する次の導入を参照してください。



ASA 5508-X、またはASA 5516-Xで上記のシナリオをケーブル接続するには、次を参照してください。

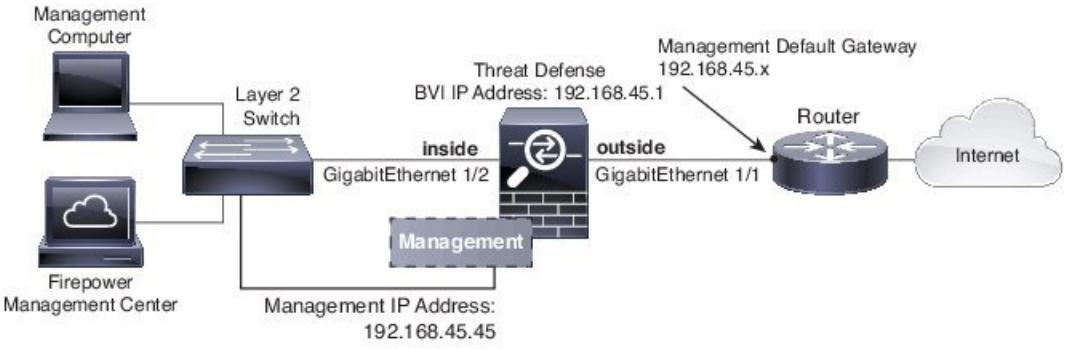


診断IPアドレスを設定する場合は、内部ルータが必要です。

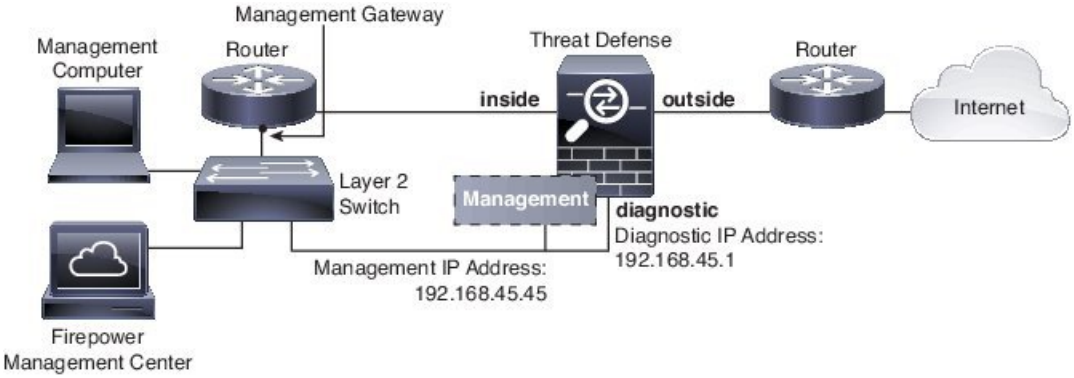


トランスペアレント モードの展開

ルーテッドモードの展開と同様、内部スイッチを使用したデバイスの展開を選択できます。この場合、診断インターフェイスを IP アドレスなしで維持する必要があります。



また、内部ルータを使用して展開することもできます。この場合、追加の管理アクセスのために、IP アドレスを持つ診断インターフェイスを使用できます。



デュアル IP スタック（IPv4 および IPv6）

Firepower Threat Defense デバイス は、インターフェイスで IPv6 アドレスと IPv4 アドレスの両方をサポートしています。IPv4 と IPv6 の両方で、デフォルト ルートを設定してください。

ルーテッド モードおよびトランスペアレント モードのインターフェイスのガイドラインおよび要件

高可用性

- フェールオーバー リンクは、この章の手順で設定しないでください。詳細については、高可用性の章も参照してください。
- 高可用性を使用する場合、データ インターフェイスの IP アドレスとスタンバイ アドレスを手動で設定する必要があります。DHCP および PPPoE はサポートされません。**[Monitored**

Interfaces] 領域の **[Devices]** > **[Device Management]** > **[High Availability]** タブで、スタンバイ IP アドレスを設定します。詳細については、高可用性の章も参照してください。

IPv6

- IPv6 はすべてのインターフェイスでサポートされます。
- トランスペアレント モードでは、IPv6 アドレスは手動でのみ設定できます。
- Firepower Threat Defense デバイスは、IPv6 エニーキャスト アドレスはサポートしません。

サポート モデル

- Firepower 2100 シリーズでは、ルーテッド モードのブリッジ グループはサポートされません。
- Firepower Threat Defense Virtual では、ルーテッド モードのブリッジ グループはサポートされません。

トランスペアレント モードとブリッジ グループのガイドライン

- 64のインターフェイスをもつブリッジ グループを 250 まで作成できます。
- 直接接続された各ネットワークは同一のサブネット上にある必要があります。
- Firepower Threat Defense デバイス では、セカンダリ ネットワーク上のトラフィックはサポートされていません。BVI IP アドレスと同じネットワーク上のトラフィックだけがサポートされています。
- IPv4 の場合は、管理トラフィックと、Firepower Threat Defense デバイス を通過するトラフィックの両方の各ブリッジ グループに対し、BVI の IP アドレスが必要です。IPv6 アドレスは BVI でサポートされますが必須ではありません。
- IPv6 アドレスは手動でのみ設定できます。
- BVI IP アドレスは、接続されたネットワークと同じサブネット内にある必要があります。サブネットにホスト サブネット（255.255.255.255）を設定することはできません。
- 管理インターフェイスはブリッジ グループのメンバーとしてサポートされません。
- Firepower 4100/9300 では、データ共有インターフェイスはブリッジ グループのメンバーとしてサポートされません。
- トランスペアレント モードでは、少なくとも 1 つのブリッジ グループを使用し、データ インターフェイスがブリッジ グループに属している必要があります。
- トランスペアレント モードでは、接続されたデバイス用のデフォルト ゲートウェイとして BVI IP アドレスを指定しないでください。デバイスは Firepower Threat Defense デバイス の他方側のルータをデフォルト ゲートウェイとして指定する必要があります。

- トランスペアレント モードでは、管理トラフィックの戻りパスを指定するために必要な *default* ルートは、1 つのブリッジ グループ ネットワークからの管理トラフィックにだけ適用されます。これは、デフォルト ルートはブリッジ グループのインターフェイスとブリッジ グループ ネットワークのルータ IP アドレスを指定しますが、ユーザは 1 つのデフォルト ルートしか定義できないためです。複数のブリッジ グループ ネットワークからの管理トラフィックが存在する場合は、管理トラフィックの発信元ネットワークを識別する標準のスタティック ルートを指定する必要があります。
- トランスペアレント モードでは、PPPoE は 診断 インターフェイスでサポートされません。
- ルーテッドモードでは、ブリッジグループと他のルーテッドインターフェイスの間をルーティングするために、BVI を指定する必要があります。
- ルーテッド モードでは、FTD 定義の EtherChannel インターフェイスがブリッジ グループのメンバーとしてサポートされません。Firepower 4100/9300 上の Etherchannel は、ブリッジ グループ メンバーにすることができます。
- Bidirectional Forwarding Detection（BFD）エコー パケットは、ブリッジ グループ メンバを使用するときに、FTD を介して許可されません。BFD を実行している FTD の両側に 2 つのネイバーがある場合、FTD は BFD エコー パケットをドロップします。両方が同じ送信元および宛先 IP アドレスを持ち、LAND 攻撃の一部であるように見えるからです。

ルーテッド モードのインターフェイスの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin Access Admin Network Admin

この手順では、名前、セキュリティ ゾーン、および IPv4 アドレスを設定する方法について説明します。

始める前に

- **Firepower 4100/9300**
  1. 物理インターフェイスの設定 （756 ページ）
  2. （オプション）特別なインターフェイスを設定します。
     - EtherChannel（ポート チャネル）の追加 （757 ページ）
     - コンテナ インスタンスへの VLAN サブインターフェイスの追加 （759 ページ）
       FXOS で次を実行します。
     - FMC でのサブインターフェイスの追加 （805 ページ）

- （オプション）**他のすべてのモデル**：
  - 冗長インターフェイスの設定 （799 ページ）
  - EtherChannel の設定 （801 ページ）
  - サブインターフェイスの追加 （805 ページ）

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** の順に選択し、FTD デバイスの編集アイコン（）をクリックします。デフォルトで [インターフェイス（Interfaces）] タブが選択されています。

ステップ 2 編集するインターフェイスの編集アイコン（）をクリックします。

ステップ 3 [名前（Name）] フィールドに、48 文字以内で名前を入力します。

ステップ 4 [有効（Enabled）] チェック ボックスをオンにして、インターフェイスを有効化します。

ステップ 5 （任意） このインターフェイスを [管理専用（Management Only）] に設定してトラフィックを管理トラフィックに制限します。through-the-box トラフィックは許可されていません。

ステップ 6 （任意） [説明（Description）] フィールドに説明を追加します。

説明は 200 文字以内で入力できます。改行を入れずに 1 行で入力します。

ステップ 7 [モード（Mode）] ドロップダウン リストで、[なし（None）] を選択します。

通常のファイアウォール インターフェイスのモードは [なし（None）] に設定されています。他のモードは IPS 専用インターフェイス タイプ向けです。

ステップ 8 [セキュリティ ゾーン（Security Zone）] ドロップダウン リストからセキュリティ ゾーンを選択するか、[新規（New）] をクリックして、新しいセキュリティ ゾーンを追加します。

ルーテッド インターフェイスは、ルーテッド タイプ インターフェイスであり、ルーテッド タイプのゾーンにのみ属することができます。

ステップ 9 **MTU** についてはMTU の設定 （831 ページ）を参照してください。

ステップ 10 [IPv4] タブをクリックします。IP アドレスを設定するには、[IP タイプ（IP Type）] ドロップダウン リストにある次のオプションのいずれかを使用します。

- [静的 IP を使用する（Use Static IP）]：IP アドレスおよびサブネット マスクを入力します。ハイ アベイラビリティの場合は、静的 IP アドレスのみを使用できます。[モニタ対象インターフェイス（Monitored Interfaces）] エリアの **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > **[ハイアベイラビリティ（High Availability）]** タブで、スタンバイ IP アドレスを設定します。スタンバイ IP アドレスを設定しない場合、アクティブ ユニットはネットワーク テストを使用してスタンバイ インターフェイスをモニタできず、リンク ステートをトラックすることしかできません。
- [DHCP の使用（Use DHCP）]：次のオプションのパラメータを設定します。
  - [DHCP を使用してデフォルト ルートを取得（Obtain default route using DHCP）]：DHCP サーバからデフォルト ルートを取得します。

- [DHCP ルートメトリック（DHCP route metric）]：アドミニストレーティブ ディスタンスを学習したルートに割り当てます（1 ～ 255）。学習したルートのデフォルトのアドミニストレーティブ ディスタンスは 1 です。

- [PPPoE を使用（Use PPPoE）]：インターフェイスが DSL、ケーブル モデム、またはその他の手段で ISP に接続されていて、ISP が PPPoE を使用して IP アドレスを割り当てる場合は、次のパラメータを設定します。
  - [VPDN グループ名（VPDN Group Name）]：この接続を表すために選択するグループ名を指定します。
  - [PPPoE ユーザ名（PPPoE User Name）]：ISP によって提供されたユーザ名を指定します。
  - [PPPoE パスワード/パスワードの確認（PPPoE Password/Confirm Password）]：ISP によって提供されたパスワードを指定し、確認します。
  - [PPP 認証（PPP Authentication）]：[PAP]、[CHAP]、または [MSCHAP] を選択します。

    PAP は認証時にクリアテキストのユーザ名とパスワードを渡すため、セキュアではありません。CHAP では、サーバのチャレンジに対して、クライアントは暗号化された「チャレンジとパスワード」およびクリアテキストのユーザ名を返します。CHAP は PAP よりセキュアですが、データを暗号化しません。MSCHAP は CHAP に似ていますが、サーバが CHAP のようにクリア テキスト パスワードを扱わず、暗号化されたパスワードだけを保存、比較するため、CHAP よりセキュアです。また、MSCHAP では MPPE によるデータの暗号化のためのキーを生成します。
  - [PPPoE ルート メトリック（PPPoE route metric）]：アドミニストレーティブ ディスタンスを学習したルートに割り当てます。有効な値は 1 ～ 255 です。デフォルトでは、学習したルートのアドミニストレーティブ ディスタンスは 1 です。
  - [ルート設定の有効化（Enable Route Settings）]：手動で PPPoE の IP アドレスを設定するには、このチェックボックスをオンにして、[IP アドレス（IP Address）] を入力します。

    [ルート設定を有効化（Enable Route Settings）]チェックボックスをオンにして、[IPアドレス（IP Address）] を空欄にした場合、**ip address pppoe setroute** コマンドが次のように適用されます。

    ```
    interface GigabitEthernet0/2
    nameif inside2_pppoe
    cts manual
      propagate sgt preserve-untag
      policy static sgt disabled trusted
    security-level 0
    pppoe client vpdn group test
    pppoe client route distance 10
    ip address pppoe setroute
    ```
  - [フラッシュにユーザ名とパスワードを保存（Store Username and Password in Flash）]：フラッシュ メモリにユーザ名とパスワードを保存します。

    FTD デバイスは、NVRAM の特定の場所にユーザ名とパスワードを保存します。

ステップ 11 （任意） IPv6 アドレスの設定 （819 ページ）を参照して [IPv6] タブでの IPv6 アドレスを設定します。

ステップ 12 （任意） MAC アドレスの設定 （833 ページ）を参照して [詳細設定（Advanced）] タブで MAC アドレスを手動で設定します。

ステップ 13 （任意） [ハードウェア構成（Hardware Configuration）] タブをクリックして、デュプレックスと速度を設定します。

- [デュプレックス（Duplex）] : [全（Full）]、[半（Half）]、または [自動（Auto）] を選択します。[自動（Auto）] は、インターフェイスによってサポートされる場合のみデフォルトとなります。たとえば、Firepower 2100 シリーズの SFP インターフェイスでは [自動（Auto）] を選択できません。
- [速度（Speed）] : [10]、[100]、[1000]、または [自動（Auto）] を選択します。デフォルトは [自動（Auto）] です。インターフェイスのタイプによって、選択可能なオプションが制限されます。たとえば、Firepower 2100 シリーズ デバイスでは、GigabitEthernet ポートでは 10、100、1000（1Gbps）、SFP ポートでは 1000 または 10000（10 Gbps）を選択できます。Firepower 2100 シリーズ デバイスの SFP インターフェイスは、[自動（Auto）] をサポートしていないことに注意してください。

ステップ 14 [OK] をクリックします。

ステップ 15 **[Save（保存）]** をクリックします。

これで、[Deploy] をクリックして割り当てられているデバイスにポリシーを展開できます。変更はポリシーを導入するまで有効になりません。

の ブリッジ グループ インターフェイスの設定

ブリッジ グループは、Firepower Threat Defense デバイス がルーティングではなくブリッジするインターフェイスのグループです。 ブリッジグループはトランスペアレント ファイアウォール モード、ルーテッド ファイアウォール モードの両方でサポートされています。ブリッジグループの詳細については、ブリッジグループについて （713 ページ）を参照してください。

ブリッジ グループと関連インターフェイスを設定するには、次の手順を実行します。

ブリッジ グループ メンバーの一般的なインターフェイス パラメータの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin Access Admin Network Admin

この手順は、ブリッジ グループ メンバー インターフェイスの名前とセキュリティ ゾーンを設定する方法について説明します。同じブリッジグループで、さまざまな種類のインターフェイス（物理インターフェイス、VLAN サブインターフェイス、VNI インターフェイス、EtherChannel、冗長インターフェイス）を含めることができます。診断インターフェイスはサポートされていません。 ルーテッドモードでは、EtherChannel はサポートされません。Firepower 4100/9300 では、データ共有タイプのインターフェイスはサポートされていません。

始める前に

- **Firepower 4100/9300**
  1. 物理インターフェイスの設定 （756 ページ）
  2. （オプション）特別なインターフェイスを設定します。
     - EtherChannel（ポート チャネル）の追加 （757 ページ）
     - コンテナ インスタンスへの VLAN サブインターフェイスの追加 （759 ページ）
       FXOS で次を実行します。
     - FMC でのサブインターフェイスの追加 （805 ページ）

- （オプション）**他のすべてのモデル**：
  - 冗長インターフェイスの設定 （799 ページ）
  - EtherChannel の設定 （801 ページ）
  - サブインターフェイスの追加 （805 ページ）

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** の順に選択し、FTD デバイスの編集アイコン（  ）をクリックします。デフォルトで [インターフェイス（Interfaces）] タブが選択されています。

ステップ 2 編集するインターフェイスの編集アイコン（  ）をクリックします。

ステップ 3 [名前（Name）] フィールドに、48 文字以内で名前を入力します。

ステップ 4 [有効（Enabled）] チェック ボックスをオンにして、インターフェイスを有効化します。

ステップ 5 （任意） このインターフェイスを [管理専用（Management Only）] に設定してトラフィックを管理トラフィックに制限します。through-the-box トラフィックは許可されていません。

ステップ 6 （任意） [説明（Description）] フィールドに説明を追加します。

説明は 200 文字以内で入力できます。改行を入れずに 1 行で入力します。

ステップ 7 [モード（Mode）] ドロップダウン リストで、[なし（None）] を選択します。

通常のファイアウォール インターフェイスのモードは [なし（None）] に設定されています。他のモードは IPS 専用インターフェイス タイプ向けです。このインターフェイスをブリッジ グループに割り当てると、[スイッチド（Switched）] がモードに表示されます。

ステップ 8 [セキュリティ ゾーン（Security Zone）] ドロップダウン リストからセキュリティ ゾーンを選択するか、[新規（New）] をクリックして、新しいセキュリティ ゾーンを追加します。

ブリッジ グループ メンバー インターフェイスは、スイッチドタイプ インターフェイスであり、スイッチドタイプのゾーンにのみ属することができます。このインターフェイスに対して IP アドレス設定は行わないでください。ブリッジ仮想インターフェイス（BVI）に対してのみ IP アドレスを設定します。BVI

はゾーンに属しておらず、BVI にはアクセス コントロール ポリシーを適用できないことに注意してください。

ステップ 9 **MTU** についてはMTU の設定 （831 ページ）を参照してください。

ステップ 10 （任意） [ハードウェア構成（Hardware Configuration）] タブをクリックして、デュプレックスと速度を設定します。

- [デュプレックス（Duplex）] : [全（Full）]、[半（Half）]、または [自動（Auto）] を選択します。[自動（Auto）] は、インターフェイスによってサポートされる場合のみデフォルトとなります。たとえば、Firepower 2100 シリーズの SFP インターフェイスでは [自動（Auto）] を選択できません。
- [速度（Speed）] : [10]、[100]、[1000]、または [自動（Auto）] を選択します。デフォルトは [自動（Auto）] です。インターフェイスのタイプによって、選択可能なオプションが制限されます。たとえば、Firepower 2100 シリーズ デバイスでは、GigabitEthernet ポートでは 10、100、1000（1Gbps）、SFP ポートでは 1000 または 10000（10 Gbps）を選択できます。Firepower 2100 シリーズ デバイスの SFP インターフェイスは、[自動（Auto）] をサポートしていないことに注意してください。

ステップ 11 （任意） IPv6 アドレスの設定 （819 ページ）を参照して [IPv6] タブでの IPv6 アドレスを設定します。

ステップ 12 （任意） MAC アドレスの設定 （833 ページ）を参照して [詳細設定（Advanced）] タブで MAC アドレスを手動で設定します。

ステップ 13 [OK] をクリックします。

ステップ 14 **[Save（保存）]** をクリックします。

これで、[Deploy] をクリックして割り当てられているデバイスにポリシーを展開できます。変更はポリシーを導入するまで有効になりません。

ブリッジ仮想インターフェイス（BVI）の設定

ブリッジ グループごとに、IP アドレスを設定する BVI が必要です。FTD はブリッジ グループが発信元になるパケットの送信元アドレスとして、この IP アドレスを使用します。BVI IP アドレスは、接続されているネットワークと同じサブネット上になければなりません。IPv4 トラフィックの場合、すべてのトラフィックを通過させるには、BVI IP アドレスが必要です。IPv6 トラフィックの場合は、少なくとも、トラフィックを通過させるリンクローカルアドレスを設定する必要があります。リモート管理などの管理操作を含めたフル機能を実現するために、グローバル管理アドレスを設定することを推奨します。

ルーテッドモードの場合、BVI に名前を指定すると、BVI がルーティングに参加します。名前を指定しなければ、ブリッジ グループはトランスペアレント ファイアウォール モードの場合と同じように隔離されたままになります。

（注） 個別の 診断 インターフェイスでは、設定できないブリッジ グループ（ID 301）は、設定に自動的に追加されます。このブリッジ グループはブリッジ グループの制限に含まれません。

始める前に

セキュリティ ゾーンに BVI を追加することはできません。そのため、BVI にアクセス コントロール ポリシーを適用することはできません。ゾーンに基づいてブリッジ グループのメンバー インターフェイスにポリシーを適用する必要があります。

ステップ 1 **[デバイス（Devices）] > [デバイス管理（Device Management）]** の順に選択し、FTD デバイスの編集アイコン（✎）をクリックします。デフォルトで [インターフェイス（Interfaces）] タブが選択されています。

ステップ 2 **[インターフェイスの追加（Add Interfaces）] > [ブリッジ グループ インターフェイス（Bridge Group Interface）]** を選択します。

ステップ 3 （ルーテッド モード）[名前（Name）] フィールドに、名前を 48 文字以内で入力します。

トラフィックをブリッジ グループ メンバーの外部（たとえば、外部インターフェイスや他のブリッジ グループのメンバー）にルーティングする必要がある場合は、BVI に名前を付ける必要があります。名前は大文字と小文字が区別されません。

ステップ 4 [ブリッジ グループ ID（Bridge Group ID）] フィールドに、1 ～ 250 の間のブリッジ グループ ID を入力します。

ステップ 5 （オプション）[説明（Description）] フィールドに、このブリッジ グループの説明を入力します。

ステップ 6 [インターフェイス（Interfaces）] タブでインターフェイスをクリックし、[追加（Add）] をクリックして [選択したインターフェイス（Selected Interfaces）] 領域にそのインターフェイスを移動します。ブリッジ グループのメンバーにするすべてのインターフェイスに対して繰り返します。

ステップ 7 （トランスペアレント モード）[IPv4] タブをクリックします。[IP アドレス（IP Address）] フィールドに IPv4 アドレスおよびサブネット マスクを入力します。

BVI にはホスト アドレス（/32 または 255.255.255.255）を割り当てないでください。また、/30 サブネットなど（255.255.255.252）、ホスト アドレスが 3 つ未満（アップストリーム ルータ、ダウンストリーム ルータ、トランスペアレント ファイアウォールにそれぞれ 1 つずつ）の他のサブネットを使用しないでください。FTD デバイスは、サブネットの先頭アドレスと最終アドレスで送受信されるすべての ARP パケットをドロップします。たとえば、/30 サブネットを使用し、そのサブネットからアップストリーム ルータへの予約済みアドレスを割り当てた場合、FTD デバイスはダウンストリーム ルータからアップストリーム ルータへの ARP 要求をドロップします。

ハイ アベイラビリティの場合は、[モニタ対象インターフェイス（Monitored Interfaces）] エリアの **[デバイス（Devices）] > [デバイス管理（Device Management）] > [ハイアベイラビリティ（High Availability）]** タブで、スタンバイ IP アドレスを設定します。スタンバイ IP アドレスを設定しない場合、アクティブ ユニットはネットワーク テストを使用してスタンバイ インターフェイスをモニタできず、リンク ステートをトラックすることしかできません。

ステップ 8 （ルーテッドモード）[IPv4] タブをクリックします。IP アドレスを設定するには、[IP タイプ（IP Type）] ドロップダウン リストにある次のオプションのいずれかを使用します。

- [静的 IP を使用する（Use Static IP）]：IP アドレスおよびサブネット マスクを入力します。ハイ アベイラビリティの場合は、静的 IP アドレスのみを使用できます。[モニタ対象インターフェイス（Monitored Interfaces）] エリアの **[デバイス（Devices）] > [デバイス管理（Device Management）] > [ハイアベイラビリティ（High Availability）]** タブで、スタンバイ IP アドレスを設定します。スタン

バイ IP アドレスを設定しない場合、アクティブ ユニットはネットワーク テストを使用してスタンバイ インターフェイスをモニタできず、リンク ステートをトラックすることしかできません。

- [DHCP の使用（Use DHCP）]：次のオプションのパラメータを設定します。
  - [DHCP を使用してデフォルト ルートを取得（Obtain default route using DHCP）]：DHCP サーバからデフォルト ルートを取得します。
  - [DHCP ルートメトリック（DHCP route metric）]：アドミニストレーティブ ディスタンスを学習したルートに割り当てます（1 ～ 255）。学習したルートのデフォルトのアドミニストレーティブ ディスタンスは 1 です。

ステップ 9 （任意） IPv6 アドレッシングの設定については、IPv6 アドレスの設定 （819 ページ）を参照してください。

ステップ 10 （任意） スタティック ARP エントリの追加 （834 ページ）および静的 MAC アドレスの追加とのブリッジ グループの MAC 学習の無効化 （835 ページ）（トランスペアレント モードの場合のみ）を参照して **ARP** と **MAC** を設定します。

ステップ 11 [OK] をクリックします。

ステップ 12 **[Save（保存）]** をクリックします。

これで、[Deploy] をクリックして割り当てられているデバイスにポリシーを展開できます。変更はポリシーを導入するまで有効になりません。

トランスペアレント モードの診断（管理）インターフェイスの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin Access Admin Network Admin

トランスペアレント ファイアウォール モードでは、すべてのインターフェイスがブリッジ グループに属している必要があります。唯一の例外は診断 *slot*/*port* インターフェイスです。Firepower 4100/9300 シャーシ では、診断インターフェイス ID は FTD 論理デバイスに割り当てた mgmt-type インターフェイスによって異なります。他のインターフェイス タイプは診断インターフェイスとして使用できません。設定できる診断インターフェイスは 1 つです。

始める前に

このインターフェイスをブリッジ グループに割り当てないでください。設定できないブリッジ グループ（ID 301）は、コンフィギュレーションに自動的に追加されます。このブリッジ グループはブリッジ グループの制限に含まれません。

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** の順に選択し、FTD デバイスの編集アイコン（）をクリックします。デフォルトで [インターフェイス（Interfaces）] タブが選択されています。

ステップ 2 診断 インターフェイスの編集アイコン（）をクリックします。

ステップ 3 [名前（Name）] フィールドに、48 文字以内で名前を入力します。

ステップ 4 [IPv4] タブをクリックします。IP アドレスを設定するには、[IP タイプ（IP Type）] ドロップダウン リストにある次のオプションのいずれかを使用します。

- [静的 IP を使用する（Use Static IP）]：IP アドレスおよびサブネット マスクを入力します。
- [DHCP の使用（Use DHCP）]：次のオプションのパラメータを設定します。
  - [DHCP を使用してデフォルト ルートを取得（Obtain default route using DHCP）]：DHCP サーバからデフォルト ルートを取得します。
  - [DHCP ルートメトリック（DHCP route metric）]：アドミニストレーティブ ディスタンスを学習したルートに割り当てます（1 ～ 255）。学習したルートのデフォルトのアドミニストレーティブ ディスタンスは 1 です。
- [PPPoE の使用（Use PPPoE）]：次のパラメータを設定します。
  - [VPDN グループ名（VPDN Group Name）]：グループ名を指定します。
  - [PPPoE ユーザ名（PPPoE User Name）]：ISP によって提供されたユーザ名を指定します。
  - [PPPoE パスワード/パスワードの確認（PPPoE Password/Confirm Password）]：ISP によって提供されたパスワードを指定し、確認します。
  - [PPP 認証（PPP Authentication）]：[PAP]、[CHAP]、または [MSCHAP] を選択します。

    PAP は認証時にクリアテキストのユーザ名とパスワードを渡すため、セキュアではありません。CHAP では、サーバのチャレンジに対して、クライアントは暗号化された「チャレンジとパスワード」およびクリアテキストのユーザ名を返します。CHAP は PAP よりセキュアですが、データを暗号化しません。MSCHAP は CHAP に似ていますが、サーバが CHAP のようにクリア テキスト パスワードを扱わず、暗号化されたパスワードだけを保存、比較するため、CHAP よりセキュアです。また、MSCHAP では MPPE によるデータの暗号化のためのキーを生成します。
  - [PPPoE ルート メトリック（PPPoE route metric）]：アドミニストレーティブ ディスタンスを学習したルートに割り当てます。有効な値は 1 ～ 255 です。デフォルトでは、学習したルートのアドミニストレーティブ ディスタンスは 1 です。
  - [ルート設定の有効化（Enable Route Settings）]：手動で PPPoE の IP アドレスを設定するには、このチェックボックスをオンにして、[IP アドレス（IP Address）] を入力します。
  - [フラッシュにユーザ名とパスワードを保存（Store Username and Password in Flash）]：フラッシュ メモリにユーザ名とパスワードを保存します。

    FTD デバイスは、NVRAM の特定の場所にユーザ名とパスワードを保存します。

ステップ 5 （任意） **IPv6** アドレッシングの設定については、IPv6 アドレスの設定 （819 ページ）を参照してください。

ステップ 6 （任意） [詳細設定（Advanced）] タブで、オプションの設定を実行します。

- MAC アドレスの設定 （833 ページ）を参照してください。
- スタティック ARP エントリの追加 （834 ページ）を参照してください。
- セキュリティの設定パラメータの設定 （836 ページ）を参照してください。

ステップ 7 [OK] をクリックします。

ステップ 8 **[Save（保存）]** をクリックします。

これで、[Deploy] をクリックして割り当てられているデバイスにポリシーを展開できます。変更はポリシーを導入するまで有効になりません。

IPv6 アドレスの設定

ここでは、ルーテッド モードおよびトランスペアレント モードで IPv6 アドレッシングを設定する方法について説明します。

IPv6 について

このセクションには、IPv6 に関する情報が含まれています。

IPv6 アドレス指定

次の 2 種類の IPv6 のユニキャスト アドレスを設定できます。

- グローバル：グローバル アドレスは、パブリック ネットワークで使用可能なパブリック アドレスです。ブリッジ グループの場合、このアドレスは各メンバー インターフェイスごとに設定するのではなく、BVI 用に設定する必要があります。また、トランスペアレント モードで管理インターフェイスのグローバルな IPv6 アドレスを設定することもできます。
- リンクローカル：リンクローカルアドレスは、直接接続されたネットワークだけで使用できるプライベート アドレスです。ルータは、リンクローカル アドレスを使用してパケットを転送するのではなく、特定の物理ネットワーク セグメント上で通信だけを行います。ルータは、アドレス設定またはアドレス解決などの Neighbor Discovery 機能に使用できます。ブリッジ グループでは、メンバー インターフェイスのみがリンクローカル アドレスを所有しています。BVI にはリンクローカル アドレスはありません。

最低限、IPv6 が動作するようにリンクローカル アドレスを設定する必要があります。グローバル アドレスを設定すると、リンクローカル アドレスがインターフェイスに自動的に設定されるため、リンクローカル アドレスを個別に設定する必要はありません。ブリッジ グループ インターフェイスでは、BVI でグローバル アドレスを設定した場合、Firepower Threat Defense デバイス が自動的にメンバー インターフェイスのリンクローカル アドレスを生成します。グ

ローバル アドレスを設定しない場合は、リンクローカル アドレスを自動的にするか、手動で設定する必要があります。

Modified EUI-64 インターフェイス ID

RFC 3513「Internet Protocol Version 6 (IPv6) Addressing Architecture」（インターネット プロトコル バージョン 6 アドレッシング アーキテクチャ）では、バイナリ値 000 で始まるものを除き、すべてのユニキャスト IPv6 アドレスのインターフェイス識別子部分は長さが 64 ビットで、Modified EUI-64 形式で組み立てることが要求されています。Firepower Threat Defense デバイスでは、ローカル リンクに接続されたホストにこの要件を適用できます。

この機能がインターフェイスでイネーブルになっていると、そのインターフェイス ID が Modified EUI-64 形式を採用していることを確認するために、インターフェイスで受信した IPv6 パケットの送信元アドレスが送信元 MAC アドレスに照らして確認されます。IPv6 パケットがインターフェイス ID に Modified EUI-64 形式を採用していない場合、パケットはドロップされ、次のシステム ログ メッセージが生成されます。

```
325003: EUI-64 source address check failed.
```

アドレス形式の確認は、フローが作成される場合にのみ実行されます。既存のフローからのパケットは確認されません。また、アドレスの 確認はローカル リンク上のホストに対してのみ実行できます。

グローバル IPv6 アドレスの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin Access Admin Network Admin

ルーテッド モードの任意のインターフェイスとトランスペアレント モードまたはルーテッド モードの BVI に対してグローバル IPv6 アドレスを設定するには、次の手順を実行します。

（注） グローバルアドレスを設定すると、リンクローカルアドレスは自動的に設定されるため、別々に設定する必要はありません。ブリッジ グループについて、BVI でグローバル アドレスを設定すると、すべてのメンバー インターフェイスのリンクローカル アドレスが自動的に設定されます。

FTD で定義されているサブインターフェイスの場合、親インターフェイスの同じ Burned-In MAC Address を使用するので、MAC アドレスも手動で設定することをお勧めします。IPv6 リンクローカル アドレスは MAC アドレスに基づいて生成されるため、サブインターフェイスに一意の MAC アドレスを割り当てることで、一意の IPv6 リンクローカル アドレスが可能になり、FTD で特定のインスタンスでのトラフィックの中断を避けることができます。MAC アドレスの設定 （833 ページ）を参照してください。

ステップ 1 **[デバイス（Devices）] > [デバイス管理（Device Management）]** の順に選択し、FTD デバイスの編集アイコン（  ）をクリックします。デフォルトで [インターフェイス（Interfaces）] タブが選択されています。

ステップ 2 編集するインターフェイスの編集アイコン（  ）をクリックします。

ステップ 3 [IPv6] タブをクリックします。

ルーテッドモードでは、[基本（Basic）] タブがデフォルトで選択されています。トランスペアレントモードでは、[アドレス（Address）] タブがデフォルトで選択されています。

ステップ 4 グローバル IPv6 アドレスを次のいずれかの方法で設定します。

- （ルーテッド インターフェイス）ステートレス自動設定：[自動設定（Autoconfiguration）] チェックボックスをオンにします。

  インターフェイス上でステートレス自動設定をイネーブルにすると、受信したルータ アドバタイズメント メッセージのプレフィックスに基づいて IPv6 アドレスを設定します。ステートレスな自動設定がイネーブルになっている場合、インターフェイスのリンクローカル アドレスは、Modified EUI-64 インターフェイス ID に基づいて自動的に生成されます。

  RFC 4862 では、ステートレス自動設定用に設定されたホストはルータ アドバタイズメント メッセージを送信しないと規定されていますが、この場合は、FTD デバイスがルータ アドバタイズメント メッセージを送信します。**[IPv6] > [設定（Settings）] > [RA の有効化（Enable RA）]** チェックボックスをオフにして、メッセージを抑制します。

- 手動設定：グローバル IPv6 アドレスを手動で設定するには、次の手順を実行します。

  1. [アドレス（Address）] タブをクリックして、[アドレスの追加（Add Address）] をクリックします。

     [アドレスの追加（Add Address）] ダイアログボックスが表示されます。

  2. [アドレス（Address）] フィールドに、インターフェイス ID を含む完全なグローバル IPv6 アドレス、または IPv6 プレフィックス長と IPv6 プレフィックスのいずれかを入力します。（ルーテッド モード）プレフィックスだけを入力した場合は、必ず [EUI-64 を適用（Enforce EUI 64）] チェックボックスをオンにして、Modified EUI-64 形式を使用してインターフェイス ID を生成するようにしてください。たとえば、2001:0DB8::BA98:0:3210/48（完全なアドレス）または 2001:0DB8::/48（プレフィックス、[EUI 64] はオン）。

     （[EUI 64の適用（Enforce EUI 64）] を設定しなかった場合は）ハイ アベイラビリティのために、[モニタ対象インターフェイス（Monitored Interfaces）] エリアの **[デバイス（Devices）] > [デバイス管理（Device Management）] > [ハイアベイラビリティ（High Availability）]** タブで、スタンバイ IP アドレスを設定します。スタンバイ IP アドレスを設定しない場合、アクティブ ユニットはネットワーク テストを使用してスタンバイ インターフェイスをモニタできず、リンク ステートをトラックすることしかできません。

ステップ 5 ルーテッド インターフェイスの場合は、オプションで [基本（Basic）] タブで次の値を設定できます。

- グローバル アドレスを設定しない場合に自動的にリンクローカル アドレスを設定するには、[IPv6 の有効化（Enable IPv6）] チェックボックスをオンにします。

グローバルアドレスを設定する必要がなく、リンクローカルアドレスだけを設定する必要がある場合は、リンクローカル アドレスをインターフェイスの MAC アドレス（Modified EUI-64 形式。MAC アドレスで使用するビット数は 48 ビットであるため、インターフェイス ID に必要な 64 ビットを埋めるために追加ビットを挿入する必要があります。）

- ローカル リンクの IPv6 アドレスに Modified EUI-64 形式のインターフェイス識別子の使用を適用するには、[EUI-64 を適用（Enforce EUI-64）] チェックボックスをオンにします。
- リンクローカル アドレスを手動で設定するには、[リンクローカル アドレス（Link-Local address）] フィールドにアドレスを入力します。

  リンクローカル アドレスは、FE8、FE9、FEA、または FEB で始まっている必要があります。例、fe80::20d:88ff:feee:6a82。グローバルアドレスを設定する必要がなく、リンクローカルアドレスだけを設定する必要がある場合は、リンクローカルアドレスを手動で定義できます。Modified EUI-64 形式に基づくリンクローカルアドレスを自動的に割り当てることを推奨します。たとえば、他のデバイスが Modified EUI-64 形式の使用を必要とする場合、手動で割り当てたリンクローカルアドレスのパケットはドロップされる可能性があります。

- [アドレス設定の DHCP を有効化（Enable DHCP for address config）] チェックボックスをオンにして、IPv6 ルータ アドバタイズメント パケットの Managed Address Config フラグを設定します。

  IPv6 ルータ アドバタイズメント内のこのフラグは、取得されるステートレス自動設定のアドレス以外のアドレスの取得に DHCPv6 を使用する必要があることを、IPv6 自動設定クライアントに通知します。

- [アドレス設定の DHCP を有効化（Enable DHCP for address config）] チェックボックスをオンにして、IPv6 ルータ アドバタイズメント パケットの Other Address Config フラグを設定します。

  IPv6 ルータ アドバタイズメント内のこのフラグは、DHCPv6 から DNS サーバ アドレスなどの追加情報の取得に DHCPv6 を使用する必要があることを、IPv6 自動設定クライアントに通知します。

ステップ 6 ルーテッド インターフェイスの場合は、[プレフィックス（Prefixes）] タブと [設定（Settings）] タブでの設定についてIPv6 ネイバー探索の設定 （823 ページ）を参照してください。BVI インターフェイスの場合は、[設定（Settings）] タブの以下のパラメータを参照してください。

- [DAD 試行（DAD attempts）]：DAD 試行の最大数（1 ～ 600）。重複アドレス検出（DAD）プロセスをディセーブルにするには、この値を 0 に設定します。この設定では、DAD が IPv6 アドレスで実行されている間に、インターフェイスに連続して送信されるネイバー送信要求メッセージの数を設定します。デフォルトでは 1 になっています。
- [NS 間隔（NS Interval）]：インターフェイスでの IPv6 ネイバー要請再送信の間隔（1000 ～ 3600000 ms）。デフォルト値は 1000 ミリ秒です。
- [到達可能時間（Reachable Time）]：到達可能性確認イベントが発生した後でリモートの IPv6 ノードを到達可能とみなす時間（0 ～ 3600000 ms）。デフォルト値は 0 ミリ秒です。value に 0 を使用すると、到達可能時間が判定不能として送信されます。到達可能時間の値を設定し、追跡するのは、受信デバイスの役割です。ネイバー到達可能時間を設定すると、使用できないネイバーを検出できます。時間を短く設定すると、使用できないネイバーをより早く検出できます。ただし、時間を短くするほど、IPv6 ネットワーク帯域幅とすべての IPv6 ネットワーク デバイスの処理リソースの消費量が増えます。通常の IPv6 の運用では、あまり短い時間設定は推奨できません。

ステップ 7 [OK] をクリックします。

ステップ 8 **[Save（保存）]** をクリックします。

これで、[Deploy]をクリックして割り当てられているデバイスにポリシーを展開できます。変更はポリシーを導入するまで有効になりません。

IPv6 ネイバー探索の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin Access Admin Network Admin

IPv6 ネイバー探索プロセスは、ICMPv6 メッセージおよび送信要求ノード マルチキャスト アドレスを使用して、同じネットワーク（ローカル リンク）上のネイバーのリンク層アドレスを決定し、ネイバーの読み出し可能性を確認し、隣接ルータを追跡します。

ノード（ホスト）はネイバー探索を使用して、接続リンク上に存在することがわかっているネイバーのリンク層アドレスの特定や、無効になったキャッシュ値の迅速なパージを行います。また、ホストはネイバー探索を使用して、ホストに代わってパケットを転送しようとしている隣接ルータを検出します。さらに、ノードはこのプロトコルを使用して、どのネイバーが到達可能でどのネイバーがそうでないかをアクティブに追跡するとともに、変更されたリンク層アドレスを検出します。ルータまたはルータへのパスが失敗すると、ホストは機能している代替ルータまたは代替パスをアクティブに検索します。

始める前に

ルーテッド モードのみでサポートされます。

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** の順に選択し、FTD デバイスの編集アイコン（）をクリックします。デフォルトで [インターフェイス（Interfaces）] タブが選択されています。

ステップ 2 編集するインターフェイスの編集アイコン（  ）をクリックします。

ステップ 3 [IPv6] タブをクリックして、[プレフィックス（Prefixes）] タブをクリックします。

ステップ 4 （任意） IPv6 ルータ アドバタイズメントに含める IPv6 プレフィックスを設定するには、次の手順を実行します。

a) [プレフィックスの追加（Add Prefix）] をクリックします。

b) [アドレス（Address）] フィールドに、プレフィックス長の IPv6 アドレスを入力するか、または [デフォルト（Default）] チェックボックスをオンにして、デフォルトのプレフィックスを使用します。

c) （任意） IPv6 プレフィックスをアドバタイズしない場合は、[アドバタイズメント（Advertisement）] チェックボックスをオフにします。

d) [オフ リンク（Off Link）] チェックボックスをオンにして、指定したプレフィックスがリンクに割り当てられたことを示します。指定したプレフィックスを含むアドレスにトラフィックを送信するノードは、宛先がリンク上でローカルに到達可能であると見なします。このプレフィックスは、オンリンクの判別には使用しないでください。

e) 指定されているプレフィックスを自動設定に使用する場合、[自動設定（Autoconfiguration）] チェックボックスをオンにします。

f) [プレフィックス ライフタイム（Prefix Lifetime）] で、[期間（Duration）] または [失効日（Expiration Date）] をクリックします。

- [期間（Duration）]：プレフィックスの [優先ライフタイム（Preferred Lifetime）] を秒単位で入力します。この設定は、指定の IPv6 プレフィックスが有効なものとしてアドバタイズする時間です。最大値は無限大です。有効な値は、0 ～ 4294967295 です。デフォルトは 2592000（30 日間）です。プレフィックスの [有効ライフタイム（Valid Lifetime）] を秒単位で入力します。この設定は、指定の IPv6 プレフィックスが優先であるとしてアドバタイズする時間です。最大値は無限大です。有効な値は、0 ～ 4294967295 です。デフォルト設定は、604800（7 日）です。または、[無限大（Infinite）] チェックボックスをオンにして、時間無制限を設定します。
- [失効日（Expiration Date）]：[有効（Valid）]、[優先（Preferred）] 日時を選択します。

g) [OK] をクリックします。

ステップ 5 [設定（Settings）] タブをクリックします。

ステップ 6 （任意） [DAD 試行（DAD attempts）] の最大数、1 ～ 600 を設定します。デフォルトでは 1 になっています。重複アドレス検出（DAD）プロセスをディセーブルにするには、この値を 0 に設定します。

この設定では、DAD が IPv6 アドレスで実行されている間に、インターフェイスに連続して送信されるネイバー送信要求メッセージの数を設定します。

ステートレス自動設定プロセス中に、重複アドレス検出は、アドレスがインターフェイスに割り当てられる前に、新しいユニキャスト IPv6 アドレスの一意性を確認します。

重複アドレスが検出されると、そのアドレスの状態は DUPLICATE に設定され、アドレスは使用対象外となり、次のエラー メッセージが生成されます。

```
325002: Duplicate address ipv6_address/MAC_address on interface
```

重複アドレスがインターフェイスのリンクローカル アドレスであれば、インターフェイス上で IPv6 パケットの処理はディセーブルになります。重複アドレスがグローバル アドレスであれば、そのアドレスは使用されません。

ステップ 7 （任意） [NS インターバル（NS Interval）] フィールドで、IPv6 ネイバー勧誘再送信の時間の間隔を、1000 ～ 3600000ms で設定します。

デフォルト値は 1000 ミリ秒です。

ローカル リンク上にある他のノードのリンクレイヤアドレスを検出するため、ノードからネイバー送信要求メッセージ（ICMPv6 Type 135）がローカル リンクに送信されます。ネイバー送信要求メッセージを受信すると、宛先ノードは、ネイバー アドバタイズメント メッセージ（ICPMv6 Type 136）をローカル リンク上に送信して応答します。

送信元ノードがネイバー アドバタイズメントを受信すると、送信元ノードと宛先ノードが通信できるようになります。ネイバー送信要求メッセージは、ネイバーのリンク層アドレスが識別された後に、ネイバーの到達可能性の確認にも使用されます。ノードがネイバーの到達可能性を確認するときに、ネイバー送信要求メッセージの宛先アドレスは、ネイバーのユニキャスト アドレスです。

ネイバーアドバタイズメントメッセージは、ローカル リンク上のノードのリンク層アドレスが変更されたときにも送信されます。

ステップ 8 （任意） 到達可能性確認イベントが発生した後でリモートIPv6ノードが到達可能であると見なされる時間を、[到達可能時間（Reachable Time）] フィールドにて、0 ～ 3600000ms で設定します。

デフォルト値は 0 ミリ秒です。value に 0 を使用すると、到達可能時間が判定不能として送信されます。到達可能時間の値を設定し、追跡するのは、受信デバイスの役割です。

ネイバー到達可能時間を設定すると、使用できないネイバーを検出できます。時間を短く設定すると、使用できないネイバーをより早く検出できます。ただし、時間を短くするほど、IPv6 ネットワーク帯域幅とすべてのIPv6ネットワーク デバイスの処理リソースの消費量が増えます。通常のIPv6の運用では、あまり短い時間設定は推奨できません。

ステップ 9 （任意） ルータ アドバタイズメントの伝送を抑制にするには、[RA を有効にする（Enable RA）] チェックボックスをオフにします。ルータ アドバタイズメントの伝送を有効にすると、RA ライフタイムと時間間隔を設定できます。

ルータ要請メッセージ（ICMPv6 Type 133）に応答して、ルータアドバタイズメントメッセージ（ICMPv6 Type 134）が自動的に送信されます。ルータ送信要求メッセージは、ホストからシステムの起動時に送信されるため、ホストは、次にスケジュールされているルータアドバタイズメントメッセージを待つことなくただちに自動設定を行うことができます。

Firepower Threat Defense デバイスで IPv6 プレフィックスを提供する必要がないインターフェイス（外部インターフェイスなど）では、これらのメッセージをディセーブルにできます。

- [RA ライフタイム（RA Lifetime）] : IPv6ルータ アドバタイズメントのルータのライフタイム値を、0 ～ 9000 秒で設定します。

  デフォルトは 1800 秒です。

- [RA インターバル（RA Interval）] : IPv6 ルータ アドバタイズメントの伝送の間の時間間隔を、3 ～ 1800 秒で設定します。

  デフォルトは 200 秒です。

ステップ 10 [OK] をクリックします。

ステップ 11 **[Save（保存）]** をクリックします。

これで、[Deploy] をクリックして割り当てられているデバイスにポリシーを展開できます。変更はポリシーを導入するまで有効になりません。

高度なインターフェイスの設定

この項では、通常のファイアウォール モードのインターフェイスの MAC アドレスの設定方法、最大伝送ユニット（MTU）の設定方法、およびその他の詳細パラメータの設定方法について説明します。

高度なインターフェイス設定について

この項では、インターフェイスの高度な設定について説明します。

MAC アドレスについて

手動で MAC アドレスを割り当ててデフォルトをオーバーライドできます。 コンテナ インスタンスでは、FXOS シャーシがすべてのインターフェイスに一意の MAC アドレスを自動的に生成します。

（注） 親インターフェイスの同じ Burned-In MAC Address を使用するため、FTD で定義されたサブインターフェイスに一意の MAC アドレスを割り当てる必要のある場合があります。たとえば、サービス プロバイダーによっては、MAC アドレスに基づいてアクセス コントロールを実行する場合があります。また、IPv6 リンクローカル アドレスは MAC アドレスに基づいて生成されるため、サブインターフェイスに一意の MAC アドレスを割り当てることで、一意の IPv6 リンクローカル アドレスが可能になり、FTD で特定のインスタンスでのトラフィックの中断を避けることができます。

（注） コンテナ インスタンスでは、MAC アドレスを手動で設定すると、サブインターフェイスを共有していない場合でも、分類が正しく行われるように、同じ親インターフェイス上のすべてのサブインターフェイスで一意の MAC アドレスを使用します。

デフォルトの MAC アドレス

ネイティブインスタンス向け：

デフォルトの MAC アドレスの割り当ては、インターフェイスのタイプによって異なります。

- 物理インターフェイス：物理インターフェイスは、Burned-in MAC Address を使用します。
- 冗長インターフェイス：冗長インターフェイスでは、最初に追加された物理インターフェイスの MAC アドレスが使用されます。構成でメンバー インターフェイスの順序を変更すると、MAC アドレスがリストの先頭にあるインターフェイスの MAC アドレスと一致するように変更されます。冗長インターフェイスに MAC アドレスを割り当てると、メンバー インターフェイスの MAC アドレスに関係なく、割り当てた MAC アドレスが使用されます。

- EtherChannel（Firepower Models）：EtherChannel の場合は、そのチャネル グループに含まれるすべてのインターフェイスが同じ MAC アドレスを共有します。この機能によって、EtherChannel はネットワーク アプリケーションとユーザに対してトランスペアレントになります。ネットワーク アプリケーションやユーザから見えるのは 1 つの論理接続のみであり、個々のリンクのことは認識しないからです。ポート チャネル インターフェイスは、プールからの一意の MAC アドレスを使用します。インターフェイスのメンバーシップは、MAC アドレスには影響しません。
- EtherChannel（ASA モデル）：ポート チャネル インターフェイスは、最も小さいチャネル グループ インターフェイスの MAC アドレスをポート チャネル MAC アドレスとして使用します。または、ポート チャネル インターフェイスの MAC アドレスを設定することもできます。グループ チャネル インターフェイスのメンバーシップが変更された場合に備えて、一意の MAC アドレスを設定することを推奨します。ポートチャネル MAC アドレスを提供していたインターフェイスを削除すると、そのポートチャネルの MAC アドレスは次に番号が小さいインターフェイスに変わるため、トラフィックが分断されます。
- サブインターフェイス（FTD 定義済）：物理インターフェイスのすべてのサブインターフェイスは同じ Burned-In MAC Address を使用します。サブインターフェイスに一意の MAC アドレスを割り当てることが必要になる場合があります。たとえば、サービス プロバイダーによっては、MAC アドレスに基づいてアクセス コントロールを実行する場合があります。また、IPv6 リンクローカルアドレスは MAC アドレスに基づいて生成されるため、サブインターフェイスに一意の MAC アドレスを割り当てることで、一意の IPv6 リンクローカル アドレスが可能になり、FTD で特定のインスタンスでのトラフィックの中断を避けることができます。

コンテナインスタンス向け：

- すべてのインターフェイスの MAC アドレスは MAC アドレス プールから取得されます。サブインターフェイスでは、MAC アドレスを手動で設定する場合、分類が正しく行われるように、同じ親インターフェイス上のすべてのサブインターフェイスで一意の MAC アドレスを使用します。コンテナ インスタンス インターフェイスの自動 MAC アドレス （746 ページ）を参照してください。

MTU について

MTU は、Firepower Threat Defense デバイス が特定のイーサネット インターフェイスで送信する最大フレームペイロードサイズを指定します。MTU の値は、イーサネットヘッダー、VLAN タギング、他のオーバーヘッドを含まないフレーム サイズです。たとえば、MTU を 1500 に設定すると、予想されるフレーム サイズは、ヘッダーを含めて 1518 バイトです。または、VLAN を使用している場合は、1522 バイトです。これらのヘッダーに対応するために MTU 値を高く設定しないでください。

『Path MTU Discovery』

Firepower Threat Defense デバイス は、Path MTU Discovery（RFC 1191 の定義に従う）をサポートします。つまり、2 台のホスト間のネットワーク パス内のすべてのデバイスで MTU を調整できます。したがってパスの最小 MTU の標準化が可能です。

デフォルト MTU

Firepower Threat Defense デバイス のデフォルト MTU は、1500 バイトです。この値には、イーサネット ヘッダー、VLAN タギングや他のオーバーヘッドのための 18～22 バイト以上は含まれません。

MTU とフラグメンテーション

IPv4 では、出力 IP パケットが指定された MTU より大きい場合、2 つ以上のフレームにフラグメント化されます。フラグメントは送信先（場合によっては中継先）で組立て直されますが、フラグメント化はパフォーマンス低下の原因となります。IPv6 では、通常、パケットはフラグメント化を許可されていません。したがってフラグメント化を避けるために、IP パケットを MTU サイズ以内に収める必要があります。

TCP パケットでは、通常、エンドポイントは MTU を使用して TCP の最大セグメント サイズ（たとえば、MTU - 40）を判別します。途中で追加の TCP ヘッダーが追加された場合（たとえば、サイト間 VPN トンネル）、TCP MSS はトンネリング エンティティで下方調整しないといけない場合があります。TCP MSS について （828 ページ）を参照してください。

UDP または ICMP では、フラグメンテーションを回避するために、アプリケーションは MTU を考慮する必要があります。

（注） Firepower Threat Defense デバイス はメモリに空きがある限り、設定された MTU よりも大きいフレームを受信します。

MTU とジャンボ フレーム

より大きな MTU は、より大きなパケットの送信が可能です。より大きなパケットは、ネットワークにとってより効率的な場合があります。次のガイドラインを参照してください。

- トラフィック パスの MTU の一致：すべての FTD インターフェイスとトラフィック パス内のその他のデバイスのインターフェイスでは、MTU が同じになるように設定することを推奨します。MTU の一致により、中間デバイスでのパケットのフラグメント化が回避できます。
- ジャンボ フレームへの対応：MTU を最大 9198 バイトに設定できます。Firepower Threat Defense Virtual の最大値は 9000 です。Firepower 4100/9300 の最大値は 9184 です。

TCP MSS について

最大セグメント サイズ（TCP MSS）とは、あらゆる TCP および IP ヘッダーが追加される前の TCP ペイロードのサイズです。UDP パケットは影響を受けません。接続を確立するときのスリーウェイ ハンドシェイク中に、クライアントとサーバは TCP MSS 値を交換します。

FlexConfig の Sysopt_Basic オブジェクトを使用して（Firepower Threat Defense の FlexConfig ポリシー （1201 ページ）を参照）Firepower Threat Defense デバイス で TCP MSS を通過トラフィック用に設定できます。デフォルトでは、最大 TCP MSS は 1380 バイトに設定されます。この設定は、Firepower Threat Defense デバイス が IPsec VPN カプセル化のパケットサイズを追加する

必要がある場合に役立ちます。ただし、非IPsecエンドポイントでは、Firepower Threat Defense デバイス の最大 TCP MSS を無効にする必要があります。

最大TCP MSSを設定している場合、接続のいずれかのエンドポイントがFirepower Threat Defense デバイス に設定された値を超える TCP MSS を要求すると、Firepower Threat Defense デバイス は要求パケット内の TCP MSS を Firepower Threat Defense デバイス の最大サイズで上書きします。ホストまたはサーバが TCP MSS を要求しない場合、Firepower Threat Defense デバイス は RFC 793 のデフォルト値 536 バイト（IPv4）または 1220 バイト（IPv6）を想定しますが、パケットは変更しません。たとえば、MTUをデフォルトの1500バイトのままにします。ホストは、1500 バイトの MSS から TCP および IP のヘッダー長を減算して、MSS を 1460 バイトに設定するように要求します。Firepower Threat Defense デバイス の最大 TCP MSS が 1380（デフォルト）の場合、Firepower Threat Defense デバイス は TCP 要求パケットの MSS 値を 1380 に変更します。その後、サーバは、1380バイトのペイロードを含むパケットを送信します。Firepower Threat Defense デバイス は、最大 120 バイトのヘッダーをパケットに追加しても、1500 バイトの MTU サイズに適応することができます。

TCP の最小 MSS も設定できます。ホストまたはサーバが非常に小さい TCP MSS を要求した場合、Firepower Threat Defense デバイスは値を調整します。デフォルトでは、最小 TCP MSS は有効ではありません。

SSL VPN接続用を含め、to-the-boxトラフィックの場合、この設定は適用されません。Firepower Threat Defense デバイス は MTU を使用して、TCP MSS を導き出します。MTU - 40（IPv4）または MTU - 60（IPv6）となります。

デフォルト TCP MSS

デフォルトでは、Firepower Threat Defense デバイス の最大 TCP MSS は 1380 バイトです。このデフォルトは、ヘッダーが最大 120 バイトの IPv4 IPsec VPN 接続に対応しています。この値は、MTU の デフォルトの 1500 バイト内にも収まっています。

TCP MSS の推奨最大設定

デフォルトでは TCP MSS は、Firepower Threat Defense デバイス が IPv4 IPsec VPN エンドポイントとして機能し、MTU が 1500 バイトであることを前提としています。Firepower Threat Defense デバイス が IPv4 IPsec VPN エンドポイントとして機能している場合は、最大 120 バイトの TCP および IP ヘッダーに対応する必要があります。

MTU 値を変更して、IPv6 を使用するか、または IPsec VPN エンドポイントとして Firepower Threat Defense デバイス を使用しない場合は、FlexConfig の Sysopt_Basic オブジェクトを使用して TCP MSS 設定を変更する必要があります。Firepower Threat Defense の FlexConfig ポリシー（1201 ページ）を参照してください。次のガイドラインを参照してください。

- 通常のトラフィック：TCP MSS の制限を無効にし、接続のエンドポイント間で確立された値を受け入れます。通常、接続エンドポイントはMTUからTCP MSSを取得するため、非 IPsec パケットは通常この TCP MSS を満たしています。
- IPv4 IPsec エンドポイント トラフィック：最大 TCP MSS を MTU - 120 に設定します。たとえば、ジャンボ フレームを使用しており、MTU を 9000 に設定すると、新しい MTU を使用するために、TCP MSS を 8880 に設定する必要があります。

• IPv6 IPsec エンドポイント トラフィック：最大 TCP MSS を MTU - 140 に設定します。

ブリッジグループのトラフィックの ARP インスペクション

デフォルトでは、ブリッジグループのメンバーの間ですべてのARPパケットが許可されます。ARP パケットのフローを制御するには、ARP インスペクションをイネーブルにします。

ARPインスペクションによって、悪意のあるユーザが他のホストやルータになりすます（ARPスプーフィングと呼ばれる）のを防止できます。ARP スプーフィングが許可されていると、「中間者」攻撃を受けることがあります。たとえば、ホストが ARP 要求をゲートウェイ ルータに送信すると、ゲートウェイルータはゲートウェイ ルータのMACアドレスで応答します。ただし、攻撃者は、ルータの MAC アドレスではなく攻撃者の MAC アドレスで別の ARP 応答をホストに送信します。これで、攻撃者は、すべてのホストトラフィックを代行受信してルータに転送できるようになります。

ARP インスペクションを使用すると、正しい MAC アドレスとそれに関連付けられた IP アドレスがスタティック ARP テーブル内にある限り、攻撃者は攻撃者の MAC アドレスで ARP 応答を送信できなくなります。

ARP インスペクションをイネーブルにすると、Firepower Threat Defense デバイスは、すべての ARP パケット内の MAC アドレス、IP アドレス、および送信元インターフェイスを ARP テーブル内のスタティック エントリと比較し、次のアクションを実行します。

- IP アドレス、MAC アドレス、および送信元インターフェイスが ARP エントリと一致する場合、パケットを通過させます。
- MAC アドレス、IP アドレス、またはインターフェイス間で不一致がある場合、Firepower Threat Defense デバイスはパケットをドロップします。
- ARP パケットがスタティック ARP テーブル内のどのエントリとも一致しない場合、パケットをすべてのインターフェイスに転送（フラッディング）するか、またはドロップするようにFirepower Threat Defense デバイスを設定できます。

（注） 専用の 診断 インターフェイスは、このパラメータが flood に設定されている場合でもパケットをフラッディングしません。

MAC アドレス テーブル

ブリッジ グループを使用する場合、FTD は、通常のブリッジまたはスイッチと同様に、MAC アドレスを学習して MAC アドレス テーブルを作成します。デバイスがブリッジ グループ経由でパケットを送信すると、FTD が MAC アドレスをアドレス テーブルに追加します。テーブルで MAC アドレスと発信元インターフェイスが関連付けられているため、FTDは、パケットが正しいインターフェイスからデバイスにアドレス指定されていることがわかります。ブリッジ グループ メンバー間のトラフィックには FTD セキュリティ ポリシーが適用されるため、パケットの宛先 MAC アドレスがテーブルに含まれていなくても、通常のブリッジのように、すべてのインターフェイスに元のパケットを FTD がフラッディングすることはありません。代

わりに、直接接続されたデバイスまたはリモート デバイスに対して次のパケットを生成します。

- 直接接続されたデバイスへのパケット：FTD は宛先 IP アドレスに対して ARP 要求を生成し、ARP 応答を受信したインターフェイスを学習します。
- リモート デバイスへのパケット：FTD は宛先 IP アドレスへの ping を生成し、ping 応答を受信したインターフェイスを学習します。

元のパケットはドロップされます。

デフォルト設定

- ARP インスペクションをイネーブルにした場合、デフォルト設定では、一致しないパケットはフラッドします。
- ダイナミック MAC アドレス テーブルのデフォルトのタイムアウト値は 5 分です。
- デフォルトでは、各インターフェイスはトラフィックに入る MAC アドレスを自動的に学習し、Firepower Threat Defense デバイスは対応するエントリを MAC アドレス テーブルに追加します。

ARP インスペクションと MAC アドレス テーブルのガイドライン

- ARP インスペクションは、ブリッジグループでのみサポートされます。
- MAC アドレス テーブル構成は、ブリッジグループでのみサポートされます。

MTU の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin Access Admin Network Admin

たとえば、ジャンボ フレームを許可するようにインターフェイスの MTU をカスタマイズします。

⚠

注意 デバイス上で非管理/診断インターフェイスの最大 MTU 値を変更し、設定の変更を展開すると、Snortプロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。インスペクションは、変更したインターフェイスだけでなく、すべての非管理/診断インターフェイスで中断されます。この中断によってトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびインターフェイスのタイプに応じて異なります。詳細については、「Snort® の再起動によるトラフィックの動作 （451 ページ）」を参照してください。

始める前に

- MTU を 1500 バイトより大きい値に変更すると、自動的にジャンボ フレームが有効になります。ASA モデルの場合、ジャンボ フレームを使用するには、システムをリロードする必要があります。
- インライン セットでインターフェイスを使用する場合、MTU 設定は使用されません。ただし、ジャンボ フレームの設定はインライン セットに関連します。ジャンボ フレームによりインライン インターフェイスは最大 9000 バイトのパケットを受信できます。ジャンボ フレームを有効にするには、すべてのインターフェイスの MTU を 1500 バイトより大きい値に設定する必要があります。

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** の順に選択し、FTD デバイスの編集アイコン（✎）をクリックします。デフォルトで [インターフェイス（Interfaces）] タブが選択されています。

ステップ 2 編集するインターフェイスの編集アイコン（✎）をクリックします。

ステップ 3 [一般（General）] タブで、[MTU] を 64 ～ 9198 バイトに設定します。最大値は Firepower Threat Defense Virtual では 9000、Firepower 4100/9300 シャーシ上の FTD では 9184 です。

デフォルト値は 1500 バイトです。

ステップ 4 **[OK]** をクリックします。

ステップ 5 **[Save（保存）]** をクリックします。

これで、[Deploy] をクリックして割り当てられているデバイスにポリシーを展開できます。変更はポリシーを導入するまで有効になりません。

ステップ 6 ASA モデルでは、MTU を 1500 バイトを超える値に設定する場合はシステムをリロードしてジャンボ フレームを有効にします。

MAC アドレスの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin Access Admin Network Admin

MAC アドレスを手動で割り当てることが必要となる場合があります。また、**[デバイス（Devices）] > [デバイス管理（Device Management）] > [ハイアベイラビリティ（High Availability）]** タブで、アクティブ MAC アドレスとスタンバイ MAC アドレスを設定することもできます。両方の画面でインターフェイスの MAC アドレスを設定した場合は、**[インターフェイス（Interfaces）] > [詳細（Advanced）]** タブのアドレスが優先されます。

（注） コンテナ インスタンスでは、MAC アドレスを手動で設定すると、サブインターフェイスを共有していない場合でも、分類が正しく行われるように、同じ親インターフェイス上のすべてのサブインターフェイスで一意の MAC アドレスを使用します。

ステップ 1 **[デバイス（Devices）] > [デバイス管理（Device Management）]** の順に選択し、FTD デバイスの編集アイコン（）をクリックします。デフォルトで [インターフェイス（Interfaces）] タブが選択されています。

ステップ 2 編集するインターフェイスの編集アイコン（）をクリックします。

ステップ 3 [詳細（Advanced）] タブをクリックします。
[情報（Information）] タブが選択されています。

ステップ 4 [アクティブな MAC アドレス（Active MAC Address）] フィールドに、MAC アドレスを H.H.H 形式で設定します。H は 16 ビットの 16 進数です。

たとえば、MAC アドレスが 00-0C-F1-42-4C-DE の場合、000C.F142.4CDE と入力します。MAC アドレスはマルチキャスト ビット セットを持つことはできません。つまり、左から 2 番目の 16 進数字を奇数にすることはできません。

ステップ 5 [スタンバイMACアドレス（Standby MAC Address）] フィールドに、ハイ アベイラビリティで使用する MAC アドレスを入力します。

アクティブ装置がフェールオーバーし、スタンバイ装置がアクティブになると、新しいアクティブ装置はアクティブな MAC アドレスの使用を開始して、ネットワークの切断を最小限に抑えます。一方、古いアクティブ装置はスタンバイ アドレスを使用します。

ステップ 6 [OK] をクリックします。

ステップ 7 **[Save（保存）]** をクリックします。

これで、[Deploy] をクリックして割り当てられているデバイスにポリシーを展開できます。変更はポリシーを導入するまで有効になりません。

スタティック ARP エントリの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin Access Admin Network Admin

デフォルトでは、ブリッジグループのメンバーの間ですべての ARP パケットが許可されます。ARP パケットのフローを制御するには、ARP インスペクションを有効にします（ARP インスペクションの設定 （1357 ページ） 参照）。ARP インスペクションは、ARP パケットを ARP テーブルのスタティック ARP エントリと比較します。

ルーテッド インターフェイスの場合、スタティック ARP エントリを入力できますが、通常はダイナミック エントリで十分です。ルーテッド インターフェイスの場合、直接接続されたホストにパケットを配送するために ARP テーブルが使用されます。送信者は IP アドレスでパケットの宛先を識別しますが、イーサネットにおける実際のパケット配信は、イーサネット MAC アドレスに依存します。ルータまたはホストは、直接接続されたネットワークでパケットを配信する必要がある場合、IP アドレスに関連付けられた MAC アドレスを要求する ARP 要求を送信し、ARP 応答に従ってパケットを MAC アドレスに配信します。ホストまたはルータには ARP テーブルが保管されるため、配信が必要なパケットごとに ARP 要求を送信する必要はありません。ARP テーブルは、ARP 応答がネットワーク上で送信されるたびにダイナミックに更新されます。一定期間使用されなかったエントリは、タイムアウトします。エントリが正しくない場合（たとえば、所定の IP アドレスの MAC アドレスが変更された場合など）、新しい情報で更新される前にこのエントリがタイムアウトする必要があります。

トランスペアレント モードの場合、管理トラフィックなどの FTD デバイスとの間のトラフィックに、FTD は ARP テーブルのダイナミック ARP エントリのみを使用します。

始める前に

この画面は、名前付きインターフェイスについてのみ使用できます。

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** の順に選択し、FTD デバイスの編集アイコン（  ）をクリックします。デフォルトで [インターフェイス（Interfaces）] タブが選択されています。

ステップ 2 編集するインターフェイスの編集アイコン（  ）をクリックします。

ステップ 3 [詳細（Advanced）] タブをクリックして、[ARP] タブをクリックします（トランスペアレント モードでは、[ARP と MAC（ARP and MAC）]）。

ステップ 4 [ARP 設定を追加（Add ARP Config）] をクリックします。

[ARP 設定を追加（Add ARP Config）] ダイアログボックスが表示されます。

ステップ 5 [IP アドレス（IP Address）] フィールドに、ホストの IP アドレスを入力します。

ステップ 6 [MAC アドレス（MAC Address）] フィールドに、ホストの MAC アドレスを入力します。たとえば、「00e0.1e4e.3d8b」のように入力します。

ステップ 7 このアドレスでプロキシ ARP を実行するには、[エイリアスを有効にする（Enable Alias）] チェックボックスをオンにします。

FTD デバイスは、指定された IP アドレスの ARP 要求を受信すると、指定された MAC アドレスで応答します。

ステップ 8 [OK] をクリックし、次にもう一度 [OK] をクリックして、[詳細設定（Advanced settings）] を閉じます。

ステップ 9 **[Save（保存）]** をクリックします。

これで、[Deploy] をクリックして割り当てられているデバイスにポリシーを展開できます。変更はポリシーを導入するまで有効になりません。

静的 MAC アドレスの追加とのブリッジ グループの MAC 学習の無効化

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin Access Admin Network Admin

通常、MAC アドレスは、特定の MAC アドレスからのトラフィックがインターフェイスに入ったときに、MAC アドレス テーブルに動的に追加されます。MAC アドレス ラーニングを無効にすることができます。ただし、MAC アドレスをスタティックにテーブルに追加しないかぎり、トラフィックは FTD デバイスを通過できません。スタティック MAC アドレスは、MAC アドレス テーブルに追加することもできます。スタティック エントリを追加する利点の 1 つに、MAC スプーフィングに対処できることがあります。スタティック エントリと同じ MAC アドレスを持つクライアントが、そのスタティック エントリに一致しないインターフェイスにトラフィックを送信しようとした場合、FTD デバイスはトラフィックをドロップし、システム メッセージを生成します。スタティック ARP エントリを追加するときに（スタティック ARP エントリの追加 （834 ページ） を参照）、スタティック MAC アドレス エントリは MAC アドレス テーブルに自動的に追加されます。

始める前に

この画面は、名前付きインターフェイスについてのみ使用できます。

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** の順に選択し、FTD デバイスの編集アイコン（  ）をクリックします。デフォルトで [インターフェイス（Interfaces）] タブが選択されています。

ステップ 2 編集するインターフェイスの編集アイコン（  ）をクリックします。

ステップ 3 [詳細（Advanced）] タブをクリックして、[ARP と MAC（ARP and MAC）] タブをクリックします。

ステップ 4 （任意） [MAC ラーニングを有効にする（Enable MAC Learning）] チェックボックスをオフにして MAC ラーニングを無効にします。

ステップ 5 スタティック MAC アドレスを追加するには、[MAC 設定を追加（Add MAC Config）] をクリックします。[MAC 設定を追加（Add MAC Config）] ダイアログボックスが表示されます。

ステップ 6 [MAC アドレス（MAC Address）] フィールドに、ホストの MAC アドレスを入力します。たとえば、「00e0.1e4e.3d8b」のように入力します。[OK] をクリックします。

ステップ 7 [OK] をクリックして詳細設定を終了します。

ステップ 8 **[Save（保存）]** をクリックします。

これで、[Deploy] をクリックして割り当てられているデバイスにポリシーを展開できます。変更はポリシーを導入するまで有効になりません。

セキュリティの設定パラメータの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin Access Admin Network Admin

この項では、IP スプーフィングの防止方法、完全フラグメント リアセンブルの許可方法、および [プラットフォーム設定（Platform Settings）] でデバイス レベルで設定されるデフォルトのフラグメント設定のオーバーライド方法について説明します。

アンチ スプーフィング

この項では、インターフェイスでユニキャスト リバース パス フォワーディング（ユニキャスト RPF）を有効にします。ユニキャスト RPF は、ルーティング テーブルに従って、すべてのパケットが正しい送信元インターフェイスと一致する送信元 IP アドレスを持っていることを確認して、IP スプーフィング（パケットが不正な送信元 IP アドレスを使用し、実際の送信元を隠蔽すること）から保護します。

通常、FTDデバイスは、パケットの転送先を判定するときに宛先アドレスだけを調べます。ユニキャストRPFは、送信元アドレスも調べるようにデバイスに指示します。そのため、リバース パス フォワーディング（Reverse Path Forwarding）と呼ばれます。FTD デバイスの通過を許可するすべてのトラフィックについて、送信元アドレスに戻るルートをデバイスのルーティング テーブルに含める必要があります。詳細については、RFC 2267 を参照してください。

たとえば、外部トラフィックの場合、FTD デバイスはデフォルト ルートを使用してユニキャスト RPF 保護の条件を満たすことができます。トラフィックが外部インターフェイスから入り、送信元アドレスがルーティング テーブルにない場合、デバイスはデフォルト ルートを使用して、外部インターフェイスを送信元インターフェイスとして正しく識別します。

ルーティングテーブルにあるアドレスから外部インターフェイスにトラフィックが入り、このアドレスが内部インターフェイスに関連付けられている場合、FTD デバイスはパケットをドロップします。同様に、未知の送信元アドレスから内部インターフェイスにトラフィックが入った場合は、一致するルート（デフォルトルート）が外部インターフェイスを示しているため、デバイスはパケットをドロップします。

Unicast RPF は、次のように実装されます。

- ICMP パケットにはセッションがないため、個々のパケットはチェックされません。
- UDP と TCP にはセッションがあるため、最初のパケットは逆ルート ルックアップが必要です。セッション中に到着する後続のパケットは、セッションの一部として保持されている既存の状態を使用してチェックされます。最初のパケット以外のパケットは、最初のパケットと同じインターフェイスに到着したことを保証するためにチェックされます。

パケットあたりのフラグメント

デフォルトでは、FTD デバイスは 1 つの IP パケットにつき最大 24 のフラグメントを許可し、最大 200 のフラグメントのリアセンブリ待ちを許可します。NFS over UDP など、アプリケーションが日常的にパケットをフラグメント化する場合は、ネットワークでフラグメント化を許可する必要があります。ただし、トラフィックをフラグメント化するアプリケーションがない場合は、フラグメントが FTD デバイスを通過できないようにすることをお勧めします。フラグメント化されたパケットは、DoS 攻撃によく使われます。

フラグメントのリアセンブル

FTD デバイスは、次に示すフラグメント リアセンブル プロセスを実行します。

- IP フラグメントは、フラグメント セットが作成されるまで、またはタイムアウト間隔が経過するまで収集されます。
- フラグメントセットが作成されると、セットに対して整合性チェックが実行されます。これらのチェックには、重複、テール オーバーフロー、チェーン オーバーフローはいずれも含まれません。
- FTD デバイスで終端する IP フラグメントは、常に完全にリアセンブルされます。
- [完全フラグメント リアセンブル（Full Fragment Reassembly）] が無効化されている場合（デフォルト）、フラグメントセットは、さらに処理するためにトランスポート層に転送されます。
- [完全フラグメント リアセンブル（Full Fragment Reassembly）] が有効化されている場合、フラグメント セットは、最初に単一の IP パケットに結合されます。この単一の IP パケットは、さらに処理するためにトランスポート層に転送されます。

始める前に

この画面は、名前付きインターフェイスでのみ使用できます。

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** の順に選択し、FTD デバイスの編集アイコン（  ）をクリックします。デフォルトで [インターフェイス（Interfaces）] タブが選択されています。

ステップ 2 編集するインターフェイスの編集アイコン（  ）をクリックします。

ステップ 3 [詳細（Advanced）] タブをクリックして、[セキュリティ設定（Security Configuration）] タブをクリックします。

ステップ 4 ユニキャストリバースパスフォワーディングを有効にするには、[アンチスプーフィング（Anti-Spoofing）] チェックボックスをオンにします。

ステップ 5 完全フラグメントリアセンブルを有効化するには、[完全フラグメント リアセンブル（Full Fragment Reassembly）] チェックボックスをオンにします。

ステップ 6 パケットごとに許容するフラグメント数を変更するには、[デフォルトフラグメント設定のオーバーライド（Override Default Fragment Setting）] チェックボックスをオンにして、次に示す値を設定します。

- サイズ（Size）：リアセンブルを待機する IP リアセンブル データベースに格納可能なパケットの最大数を設定します。デフォルトは 200 です。この値を 1 に設定すると、フラグメントが無効化されます。
- チェーン（Chain）：1 つの完全な IP パケットにフラグメント化できる最大パケット数を指定します。デフォルトは 24 パケットです。
- タイムアウト（Timeout）：フラグメント化されたパケット全体が到着するまで待機する最大秒数を指定します。タイマーは、パケットの最初のフラグメントが到着したあとに開始します。指定した秒数までに到着しなかったパケットフラグメントがある場合、到着済みのすべてのパケットフラグメントが廃棄されます。デフォルトは 5 秒です。

ステップ 7 [OK] をクリックします。

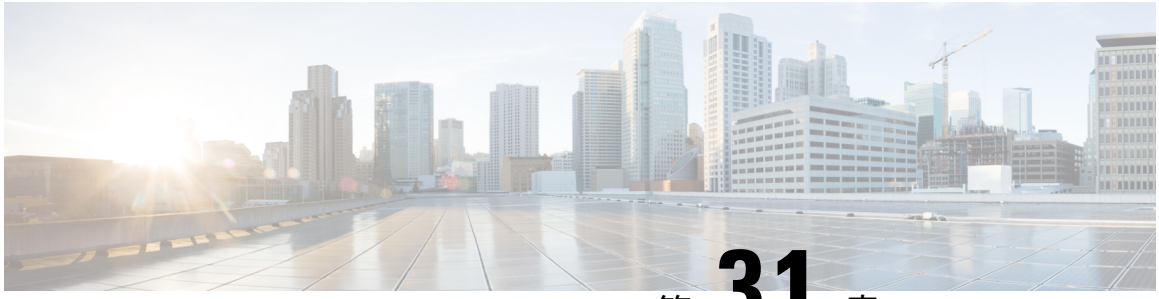
ステップ 8 **[Save（保存）]** をクリックします。

これで、[Deploy] をクリックして割り当てられているデバイスにポリシーを展開できます。変更はポリシーを導入するまで有効になりません。

Firepower Threat Defense の通常のファイアウォール インターフェイスの履歴

機能	バージョン	詳細
コンテナ インスタンスで使用される VLAN サブインターフェイス	6.3.0	柔軟な物理インターフェイスの使用を可能にするため、FXOS で VLAN サブインターフェイスを作成し、複数のインスタンス間でインターフェイスを共有することができます。 新規/変更された Firepower Management Center 画面： **[デバイス（Devices）] > [デバイス管理（Device Management）] > [編集（Edit）]** アイコン **> [インターフェイス（Interfaces）]** タブ 新規/変更された Firepower Chassis Manager 画面： **[Interfaces] > [All Interfaces] > [Add New]** ドロップダウン メニュー **> [Subinterface]** 新規/変更された FXOS コマンド：**create subinterface、set vlan、show interface、show subinterface** サポートされるプラットフォーム：Firepower 4100/9300
コンテナ インスタンスのデータ共有インターフェイス	6.3.0	柔軟な物理インターフェイスの使用を可能にするため、複数のインスタンス間でインターフェイスを共有することができます。 新規/変更された Firepower Chassis Manager 画面： **[Interfaces] > [All Interfaces] > [Type]** 新規/変更された FXOS コマンド：**set port-type data-sharing、show interface** サポートされるプラットフォーム：Firepower 4100/9300

機能	バージョン	詳細
統合ルーティングおよびブリッジング	6.2.0	統合ルーティングおよびブリッジングによって、ブリッジ グループとルーテッド インターフェイスの間でルーティングする機能が提供されます。ブリッジ グループは、FTD がルーティングではなくブリッジするインターフェイスのグループです。FTD は、FTD がファイアウォールとして機能し続ける点で本来のブリッジとは異なります。つまり、インターフェイス間のアクセス制御が実行され、通常のファイアウォール検査もすべて実行されます。以前は、トランスペアレント ファイアウォール モードでのみブリッジグループの設定が可能だったため、ブリッジグループ間でのルーティングはできませんでした。この機能を使用すると、ルーテッド ファイアウォール モードのブリッジ グループの設定と、ブリッジグループ間およびブリッジグループとルーテッドインターフェイス間のルーティングを実行できます。ブリッジグループは、ブリッジ仮想インターフェイス（BVI）を使用してそのブリッジグループのゲートウェイとして機能することにより、ルーティングに参加します。FTDにブリッジ グループを割り当てるための追加インターフェイスがある場合、統合ルーティングおよびブリッジングによって、外部のレイヤ2スイッチを使用するのではない別の方法が提供されます。ルーテッド モードでは、BVI は名前付きインターフェイスとなり、アクセス ルールや DHCP サーバなどの一部の機能に、メンバー インターフェイスとは個別に参加できます。 トランスペアレント モードでサポートされるクラスタリングの機能は、ルーテッド モードではサポートされません。マルチキャスト ルーティングとダイナミック ルーティングの機能も、BVI ではサポートされません。 新しい/変更された画面： • **[Devices] > [Device Management] > [Interfaces] > [Edit Physical Interface]** • **[デバイス（Devices）] > [デバイス管理（Device Management）] > [インターフェイス（Interfaces）] > -[インターフェイスを追加（Add Interfaces）] > [ブリッジ グループ インターフェイス（Bridge Group Interface）]** サポートされるプラットフォーム：すべて（Firepower 2100 と Firepower Threat Defense Virtual を除く）



第 31 章

Firepower Threat Defense のインライン セットとパッシブ インターフェイス

IPS 専用のパッシブ インターフェイス、パッシブ ERSPAN インターフェイス、インライン セットを設定できます。IPS 専用モードのインターフェイスは、多数のファイアウォールのチェックをバイパスし、IPS セキュリティ ポリシーのみをサポートします。別のファイアウォールがこれらのインターフェイスを保護していて、ファイアウォール機能のオーバーヘッドを避けたい場合、IPS 専用のインターフェイスを実装することがあります。

インライン セットのハードウェア バイパスについて

Firepower 9300、4100、および 2100 シリーズの特定のインターフェイス モジュールでは（インライン セットの前提条件 （843 ページ）を参照）、ハードウェア バイパス 機能を有効にできます。ハードウェア バイパスにより、停電中のインライン インターフェイス ペア間でトラフィックが引き続きフローできるようにします。この機能は、ソフトウェアまたはハードウェア障害の発生時にネットワーク接続を維持するために使用できます。

ハードウェア バイパス トリガー

ハードウェア バイパス は次のシナリオでトリガーされることがあります。

- FTD アプリケーションのクラッシュ
- FTD アプリケーションの再起動
- セキュリティ モジュールの再起動

- Firepower のシャーシのクラッシュ
- Firepower のシャーシの再起動またはアップグレード
- 手動トリガー
- Firepower のシャーシの電力損失
- セキュリティ モジュールの電力損失

ハードウェア バイパスのスイッチオーバー

通常の運用からハードウェア バイパスに切り替えたとき、またはハードウェア バイパスから通常の運用に戻したときに、トラフィックが数秒間中断する可能性があります。中断時間の長さに影響を与える可能性があるいくつかの要因があります。たとえば、銅線ポートの自動ネゴシエーション、リンク エラーやデバウンスのタイミングをどのように処理するかなどのオプティカル リンク パートナーの動作、スパニング ツリー プロトコルのコンバージェンス、ダイナミック ルーティング プロトコルのコンバージェンスなどです。この間は、接続が落ちることがあります。

また、通常の操作に戻った後で接続のミッドストリームを分析するときに、アプリケーションの識別エラーが原因で接続が切断されることがあります。

Snort フェール オープンと ハードウェア バイパス

タップ モード以外のインライン セットでは、[Snort フェール オープン（Snort Fail Open）] オプションを使用して、トラフィックをドロップするか、Snort プロセスがビジーまたはダウンしている場合に検査なしでトラフィックの通過を許可します。Snort フェール オープンは、ハードウェア バイパスをサポートするインターフェイス上のみでなく、タップ モードのものを除くすべてのインライン セットでサポートされます。

ハードウェア バイパス機能を使用すると、停電時や特定の限定されたソフトウェア障害などのハードウェア障害時にトラフィックが流れます。Snort フェール オープンをトリガーするソフトウェアの障害は、ハードウェア バイパスをトリガーしません。

ハードウェア バイパス Status

システムの電源が入っている場合、バイパス LED はハードウェア バイパスのステータスを表示します。LED の説明については、Firepower シャーシ ハードウェア インストレーションガイドを参照してください。

インライン セットの前提条件

ハードウェア バイパス のサポート

FTD は、以下のモデルの特定のネットワーク モジュールのインターフェイス ペアで ハードウェア バイパス をサポートします。

- Firepower 9300
- Firepower 4100 シリーズ
- Firepower 2100 シリーズ

これらのモデルでサポートされている ハードウェア バイパス ネットワーク モジュールは以下のとおりです。

- FirePOWER 6 ポート 1G SX FTW ネットワーク モジュール シングルワイド（FPR-NM-6X1SX-F）
- FirePOWER 6 ポート 10G SR FTW ネットワーク モジュール シングルワイド（FPR-NM-6X10SR-F）
- FirePOWER 6 ポート 10G LR FTW ネットワーク モジュール シングルワイド（FPR-NM-6X10LR-F）
- FirePOWER 2 ポート 40G SR FTW ネットワーク モジュール シングルワイド（FPR-NM-2X40G-F）
- Firepower 8 ポート 1G Copper FTW ネットワーク モジュール シングルワイド（FPR-NM-8X1G-F）

ハードウェア バイパス では以下のポート ペアのみ使用できます。

- 1 と 2
- 3 と 4
- 5 と 6
- 7 および 8

インラインセットとパッシブインターフェイスのガイドライン

ファイアウォール モード

- ERSPAN インターフェイスは、デバイスがルーテッド ファイアウォール モードになっている場合にのみ許可されます。

一般的なガイドライン

- インラインセットとパッシブインターフェイスは物理インターフェイスおよびEtherChannelのみをサポートし、、冗長インターフェイス、VLAN などを使用するとはできません。IPS 専用インターフェイスでは、Firepower 4100/9300 サブインターフェイスもサポートされていません。
- インレット セットとパッシブ インターフェイスは、シャーシ内およびシャーシ間のクラスタリングでサポートされます。
- Bidirectional Forwarding Detection（BFD）エコー パケットは、インライン セットを使用するときに、FTD を介して許可されません。BFD を実行している FTD の両側に 2 つのネイバーがある場合、FTD は BFD エコー パケットをドロップします。両方が同じ送信元および宛先 IP アドレスを持ち、LAND 攻撃の一部であるように見えるからです。

ハードウェア バイパス ガイドライン

- ハードウェア バイパス ポートはインライン セットでのみサポートされます。
- ハードウェア バイパス ポートを EtherChannel の一部にはできません。
- シャーシ内クラスタリングでサポートされます。シャーシ内の最後のユニットに障害が発生すると、ポートはハードウェア バイパス モードになります。 シャーシ間クラスタリングはサポートされていません。
- クラスタ内のすべてのユニットに障害が発生すると、最終ユニットでハードウェアバイパスがトリガーされ、トラフィックは引き続き通過します。ユニットが復帰すると、ハードウェア バイパスはスタンバイ モードに戻ります。ただし、アプリケーション トラフィックと一致するルールを使用すると、それらの接続が切断され、再確立する必要がある場合があります。状態情報がクラスタユニットに保持されず、ユニットがトラフィックを許可されたアプリケーションに属するものとして識別できないため、接続は切断されます。トラフィックのドロップを回避するには、アプリケーションベースのルールの代わりにポートベースのルールを使用します（展開に適している場合）。
- ハードウェア バイパス 高可用性モードではサポートされていません。

IPS インターフェイスでサポートされていないファイアウォール機能

- [DHCP サーバ（DHCP server）]
- DHCP リレー
- DHCP クライアント
- TCP Intercept
- ルーティング
- NAT
- VPN
- アプリケーション インスペクション
- QoS
- NetFlow
- VXLAN

パッシブ インターフェイスの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin Access Admin Network Admin

ここでは、次の方法について説明します。

- インターフェイスを有効にします。デフォルトでは、インターフェイスは無効です。
- インターフェイス モードをパッシブまたはERSPANに設定します。ERSPANインターフェイスの場合は、ERSPAN パラメータと IP アドレスを設定します。
- MTU を交換してください。デフォルトでは、MTU は 1500 バイトに設定されます。MTU の詳細については、MTU について （827 ページ）を参照してください。
- 特定の速度と二重通信（使用できる場合）を設定する。デフォルトでは、速度とデュプレックスは [自動（Auto）] に設定されます。

（注） FXOS シャーシ上の Firepower Threat Defense の場合、Firepower 4100/9300 シャーシ の基本インターフェイスの設定を行います。詳細については、「物理インターフェイスの設定 （756 ページ）」を参照してください。

ステップ 1 **[デバイス（Devices）] > [デバイス管理（Device Management）]** の順に選択し、FTD デバイスの編集アイコン（  ）をクリックします。デフォルトで [インターフェイス（Interfaces）] タブが選択されています。

ステップ 2 編集するインターフェイスの編集アイコン（  ）をクリックします。

ステップ 3 [モード（Mode）] ドロップダウン リストで、[パッシブ（Passive）] または [Erspan] を選択します。

ステップ 4 [有効（Enabled）] チェック ボックスをオンにして、インターフェイスを有効化します。

ステップ 5 [名前（Name）] フィールドに、48 文字以内で名前を入力します。

ステップ 6 [セキュリティ ゾーン（Security Zone）] ドロップダウン リストからセキュリティ ゾーンを選択するか、[新規（New）] をクリックして、新しいセキュリティ ゾーンを追加します。

ステップ 7 （任意） [説明（Description）] フィールドに説明を追加します。

説明は 200 文字以内で入力できます。改行を入れずに 1 行で入力します。

ステップ 8 （任意） [一般（General）] タブで、[MTU] を 64 ～ 9198 バイトの間で設定します。Firepower Threat Defense Virtual および FXOS シャーシ上の Firepower Threat Defense の場合、最大値は 9000 バイトです。

デフォルト値は 1500 バイトです。

ステップ 9 ERSPAN インターフェイスの場合は、次のパラメータを設定します:

- [フロー ID（Flow Id）] : ERSPAN トラフィックを特定するために送信元と宛先セッションによって使用される ID を、1 ～ 1023 の間で設定します。この ID は、ERSPAN 宛先セッション設定でも入力する必要があります。
- [ソース IP（Source IP）] : ERSPAN トラフィックの送信元として使用される IP アドレスを設定します。

ステップ 10 ERSPAN インターフェイスの場合は、[IPv4] タブで IPv4 アドレスとマスクを設定します。

ステップ 11 （任意） [ハードウェア構成（Hardware Configuration）] タブをクリックして、デュプレックスと速度を設定します。

正確な速度とデュプレックス オプションはハードウェアによって異なります。

- [デュプレックス（Duplex）] : [全（Full）]、[半（Half）]、または [自動（Auto）] を選択します。デフォルトは [自動（Auto）] です。
- [速度（Speed）] : [10]、[100]、[1000]、または [自動（Auto）] を選択します。デフォルトは [自動（Auto）] です。

ステップ 12 [OK] をクリックします。

ステップ 13 **[Save（保存）]** をクリックします。

これで、[Deploy] をクリックして割り当てられているデバイスにポリシーを展開できます。変更はポリシーを導入するまで有効になりません。

インライン セットを設定します。

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin Access Admin Network Admin

ここでは、インラインセットに追加できる2つの物理インターフェイスを有効にして名前を付けます。また、状況に応じて、サポートされるインターフェイス ペアに対して ハードウェア バイパス を有効にすることができます。

（注） FXOS シャーシ上の Firepower Threat Defense の場合、Firepower 4100/9300 シャーシ の基本インターフェイスの設定を行います。詳細については、「物理インターフェイスの設定（756 ページ）」を参照してください。

始める前に

- Firepower Threat Defense インライン ペア インターフェイスに接続する STP 対応スイッチに対して STP PortFast を設定することをお勧めします。 この設定は、ハードウェア バイパス の設定に特に有効でバイパス時間を短縮できます。

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** の順に選択し、FTD デバイスの編集アイコン（）をクリックします。デフォルトで [インターフェイス（Interfaces）] タブが選択されています。

ステップ 2 編集するインターフェイスの編集アイコン（）をクリックします。

ステップ 3 [モード（Mode）] ドロップダウン リストで、[なし（None）] を選択します。

このインターフェイスをインライン セットに追加すると、このフィールドにモードのインラインが表示されます。

ステップ 4 [有効（Enabled）] チェック ボックスをオンにして、インターフェイスを有効化します。

ステップ 5 [名前（Name）] フィールドに、48 文字以内で名前を入力します。

セキュリティ ゾーンはまだ設定しないでください。後でこの手順でインライン セットを作成してから設定する必要があります。

ステップ 6 （任意） [説明（Description）] フィールドに説明を追加します。

説明は 200 文字以内で入力できます。改行を入れずに 1 行で入力します。

ステップ 7 （任意）[ハードウェア構成（Hardware Configuration）] タブをクリックして、デュプレックスと速度を設定します。

正確な速度とデュプレックス オプションはハードウェアによって異なります。

- [デュプレックス（Duplex）] : [全（Full）]、[半（Half）]、または [自動（Auto）] を選択します。デフォルトは [自動（Auto）] です。
- [速度（Speed）] : [10]、[100]、[1000]、または [自動（Auto）] を選択します。デフォルトは [自動（Auto）] です。

ステップ 8 [OK] をクリックします。

このインターフェイスに対して他の設定は行わないでください。

ステップ 9 インライン セットに追加する 2 番目のインターフェイスに対し、編集アイコン（  ）をクリックします。

ステップ 10 最初のインターフェイスに関する設定を行います。

ステップ 11 [インライン セット（Inline Sets）] タブをクリックします。

ステップ 12 [Add Inline Set] をクリックします。
[インライン セットの追加（Add Inline Set）] ダイアログボックスが、[一般（General）] タブが選択された状態で表示されます。

ステップ 13 [名前（Name）] フィールドに、セットの名前を入力します。

ステップ 14 （任意） ジャンボ フレームを有効にするには、**MTU** を変更します。

インライン セットの MTU の設定は使用されません。ただし、ジャンボ フレームの設定はインライン セットに関連します。ジャンボ フレームによりインライン インターフェイスは最大 9000 バイトのパケットを受信できます。ジャンボ フレームを有効にするには、デバイスのすべてのインターフェイスの MTU を 1500 バイトより大きい値に設定する必要があります。

ステップ 15 （任意） [バイパス（Bypass）] モードの場合、次のいずれかのオプションを選択します。

- [Disabled] : ハードウェア バイパス がサポートされているインターフェイスの場合は ハードウェア バイパス を無効にするか、または ハードウェア バイパス がサポートされていないインターフェイスを使用します。
- [Standby] : サポートされているインターフェイスのハードウェア バイパスをスタンバイ状態に設定します。ハードウェア バイパス インターフェイスのペアのみ表示されます。スタンバイ状態の場合、トリガー イベントが発生するまで、インターフェイスは通常動作を保ちます。
- [バイパス強制（Bypass-Force）] : インターフェイス ペアを手動で強制的にバイパス状態にします。[インライン セット（Inline Sets）] タブでは、[バイパス強制（Bypass-Force）] モードになっているインターフェイス ペアに対して [はい（Yes）] が表示されます。

ステップ 16 [使用可能なインターフェイス ペア（Available Interfaces Pairs）] 領域でペアをクリックし、[追加（Add）] をクリックして [選択済みインターフェイス ペア（Selected Interface Pair）] 領域にそのペアを移動します。

この領域には、モードが [なし（None）] に設定されている名前付きインターフェイスと有効なインターフェイス間で可能なすべてのペアが表示されます。

ステップ 17 （任意） [詳細（Advanced）] タブをクリックして、次のオプション パラメータを設定します。

- [タップ モード（Tap Mode）]：インライン タップ モードに設定します。

  同じインラインセットでこのオプションと厳密な TCP 強制を有効にすることはできないことに注意してください。

- [リンク ステートの伝達（Propagate Link State）]：リンク ステートの伝達を設定します。

  リンク ステートの伝達によって、インライン セットのインターフェイスの 1 つが停止した場合、インライン インターフェイス ペアの 2 番目のインターフェイスも自動的に停止します。停止したインターフェイスが再び起動すると、2 番目のインターフェイスも自動的に起動します。つまり、1 つのインターフェイスのリンク ステートが変化すると、デバイスはその変化を検知し、その変化に合わせて他のインターフェイスのリンク ステートを更新します。ただし、デバイスからリンク ステートの変更が伝達されるまで最大 4 秒かかります。障害状態のネットワーク デバイスを自動的に避けてトラフィックを再ルーティングするようにルータが設定されている復元力の高いネットワーク環境では、リンク ステートの伝達が特に有効です。

- [厳密な TCP 強制（Strict TCP Enforcement）]：TCP のセキュリティを最大限に生かすために、厳密な強制を有効にできます。この機能は 3 ウェイ ハンドシェイクが完了していない接続をブロックします。

  厳密な適用では次のパケットもブロックされます。

  - 3 ウェイ ハンドシェイクが完了していない接続の非 SYN TCP パケット
  - レスポンダが SYN-ACK を送信する前に TCP 接続のイニシエータから送信された非 SYN/RST パケット
  - SYN の後、セッションの確立前に TCP 接続のレスポンダから送信された非 SYN-ACK/RST パケット
  - 発信側または応答側のどちらかから送信された、確立された TCP 接続の SYN パケット

- [Snort フェール オープン（Snort Fail Open）]：Snort プロセスがビジーであるか、ダウンしている場合に、インスペクション（有効）またはドロップ（無効）されることなく、新規および既存のトラフィックを通過させる場合は、[ビジー（Busy）] オプションおよび [ダウン（Down）] オプションのいずれかまたは両方を有効または無効にします。

  デフォルトでは、Snort プロセスがダウンしている場合、トラフィックはインスペクションなしで通過し、Snort プロセスがビジーの場合、トラフィックはドロップされます。

  Snort プロセスが次の場合。

  - [ビジー（Busy）]：トラフィック バッファが満杯なため、トラフィックを高速処理できません。デバイスの処理量を超えるトラフィックが存在していること、またはその他のソフトウェア リソースの問題があることを示しています。

- [ダウン（Down）]：再起動が必要な設定が展開されたため、プロセスが再起動しています。展開またはアクティブ化された際に Snort プロセスを再起動する設定（454 ページ）を参照してください。

  Snort プロセスは、ダウンしてから再起動すると、新しい接続のインスペクションを実行します。Snort プロセスでは、誤検出と検出漏れを防ぐために、インライン インターフェイス、ルーテッド インターフェイス、またはトランスペアレント インターフェイスの既存の接続のインスペクションは実行されません。これは、プロセスがダウンしていた間に初期のセッション情報が失われている可能性があるためです。

（注） Snort フェール オープン時には、Snort プロセスに依存する機能は働きません。そのような機能には、アプリケーション制御とディープ インスペクションが含まれます。システムでは、シンプルかつ容易に判断できるトランスポート層とネットワークの特性を使用して、基本的なアクセス コントロールのみ実行されます。

ステップ 18 [Interfaces] タブをクリックします。

ステップ 19 いずれかのメンバー インターフェイスの編集（  ）アイコンをクリックします。

ステップ 20 [セキュリティ ゾーン（Security Zone）] ドロップダウン リストからセキュリティ ゾーンを選択するか、[新規（New）] をクリックして、新しいセキュリティ ゾーンを追加します。

ゾーンは、インラインセットにインターフェイスを追加した後にのみ設定できます。インラインセットにインターフェイスを追加することで、インラインのモードが設定され、インラインタイプのセキュリティ ゾーンを選択できます。

ステップ 21 [OK] をクリックします。

ステップ 22 2 番目のインターフェイスのセキュリティ ゾーンを設定します。

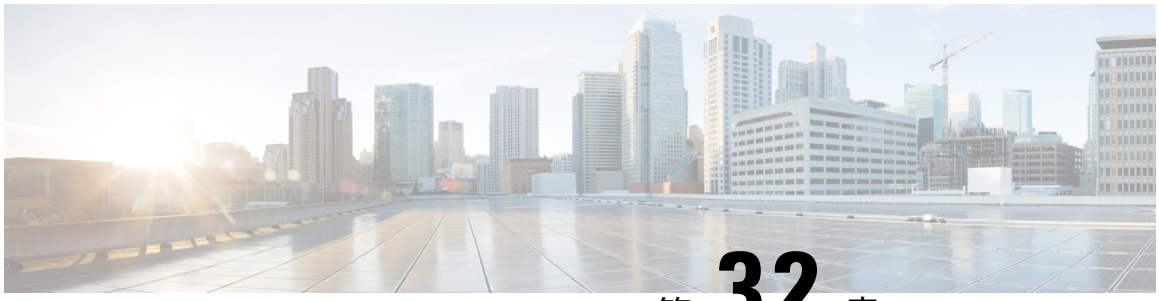
ステップ 23 **[Save（保存）]** をクリックします。

これで、[Deploy] をクリックして割り当てられているデバイスにポリシーを展開できます。変更はポリシーを導入するまで有効になりません。

Firepower Threat Defense のインライン セットとパッシブ インターフェイスの履歴

機能	バージョン	詳細
サポート対象ネットワーク モジュールに対する Firepower 2100 でのハードウェア バイパス サポート	6.3.0	Firepower 2100 は、ハードウェア バイパス ネットワーク モジュールの使用時に、ハードウェア バイパス機能をサポートするようになりました。 新しい/変更された画面： **[Devices] > [Device Management] > [Interfaces] > [Edit Physical Interface]** サポートされるプラットフォーム：Firepower 2100
FTD インライン セットでの EtherChannel のサポート	6.2.0	FTD インライン セットで Etherchannel を使用できるようになりました。 サポートされるプラットフォーム：Firepower 4100/9300
サポート対象ネットワーク モジュールに対する Firepower 4100/9300 でのハードウェア バイパス サポート	6.1.0	ハードウェア バイパスは、停電時にトラフィックがインライン インターフェイス ペア間で流れ続けることを確認します。この機能は、ソフトウェアまたはハードウェア障害の発生時にネットワーク接続を維持するために使用できます。 新しい/変更された画面： **[Devices] > [Device Management] > [Interfaces] > [Edit Physical Interface]** サポートされるプラットフォーム：Firepower 4100/9300

機能	バージョン	詳細
FTD のインライン セット リンク ステート伝達サポート	6.1.0	FTD アプリケーションでインライン セットを設定し、リンク ステート伝達を有効にすると、FTD はインライン セット メンバーシップを FXOS シャーシに送信します。リンク ステート伝達により、インラインセットのインターフェイスの 1 つが停止した場合、シャーシは、インラインインターフェイス ペアの 2 番目のインターフェイスも自動的に停止します。 新規/変更された FXOS コマンド：**show fault |grep link-down**、**show interface detail** サポートされるプラットフォーム：Firepower 4100/9300



第 32 章

Threat Defense 用の DHCP および DDNS サービス

次のトピックでは、DHCP サービスと DDNS サービスについて、および Threat Defense デバイスでこれらを設定する方法について説明します。

DHCP サービスと DDNS サービスについて

次の項では、DHCP サーバ、DHCP リレー エージェント、および DDNS 更新について説明します。

DHCPv4 サーバについて

DHCP は、IP アドレスなどのネットワーク コンフィギュレーション パラメータを DHCP クライアントに提供します。Firepower Threat Defense デバイスはFirepower Threat Defense デバイス インターフェイスに接続されている DHCP クライアントに、DHCP サーバを提供します。DHCP サーバは、ネットワーク コンフィギュレーション パラメータを DHCP クライアントに直接提供します。

IPv4 DHCP クライアントは、サーバに到達するために、マルチキャストアドレスよりもブロードキャストを使用します。DHCP クライアントは UDP ポート 68 でメッセージを待ちます。DHCP サーバは UDP ポート 67 でメッセージを待ちます。

IPv6 の DHCP サーバはサポートされていません。ただし、IPv6 トラフィックの DHCP リレーを有効にできます。

DHCP オプション

DHCP は、TCP/IP ネットワーク上のホストに設定情報を渡すフレームワークを提供します。設定パラメータは DHCP メッセージの Options フィールドにストアされているタグ付けされたアイテムにより送信され、このデータはオプションとも呼ばれます。ベンダー情報も Options に保存され、ベンダー拡張情報はすべて DHCP オプションとして使用できます。

たとえば、Cisco IP Phone が TFTP サーバから設定をダウンロードする場合を考えます。Cisco IP Phone の起動時に、IP アドレスと TFTP サーバの IP アドレスの両方が事前に設定されていない場合、Cisco IP Phone ではオプション 150 または 66 を伴う要求を DHCP サーバに送信して、この情報を取得します。

- DHCP オプション 150 では、TFTP サーバのリストの IP アドレスが提供されます。
- DHCP オプション 66 では、1 つの TFTP サーバの IP アドレスまたはホスト名が与えられます。
- DHCP オプション 3 はデフォルト ルートを設定します。

1 つの要求にオプション 150 と 66 の両方が含まれている場合があります。この場合、両者が ASA ですでに設定されていると、ASA の DHCP サーバは、その応答で両方のオプションに対する値を提供します。

高度な DHCP オプションにより、DNS、WINS、ドメインネームパラメータを DHCP クライアントに提供できます。DNS ドメインサフィックスは DHCP オプション 15 を使用します。これらの値は DHCP 自動設定により、または手動で設定できます。この情報の定義に 2 つ以上の方法を使用すると、次の優先順位で情報が DHCP クライアントに渡されます。

1. 手動で行われた設定
2. 高度な DHCP オプションの設定
3. DHCP 自動コンフィギュレーションの設定

たとえば、DHCP クライアントが受け取るドメイン名を手動で定義し、次に DHCP 自動コンフィギュレーションをイネーブルにできます。DHCP 自動構成によって、DNS サーバおよび WINS サーバとともにドメインが検出されても、手動で定義したドメイン名が、検出された DNS サーバ名および WINS サーバ名とともに DHCP クライアントに渡されます。これは、DHCP 自動構成プロセスで検出されたドメイン名よりも、手動で定義されたドメイン名の方が優先されるためです。

DHCP リレー エージェントについて

インターフェイスで受信した DHCP 要求を 1 つまたは複数の DHCP サーバに転送するように DHCP リレー エージェントを設定できます。DHCP クライアントは、最初の DHCPDISCOVER メッセージを送信するために UDP ブロードキャストを使用します。接続されたネットワークについての情報がクライアントにはないためです。サーバを含まないネットワーク セグメントにクライアントがある場合、Firepower Threat Defense デバイスはブロードキャスト トラフィックを転送しないため、UDP ブロードキャストは通常転送されません。DHCP リレー エージェ

ントを使用して、ブロードキャストを受信している Firepower Threat Defense デバイス のインターフェイスが DHCP 要求を別のインターフェイスの DHCP サーバに転送するように設定できます。

DDNS の概要

DDNS アップデートでは、DNS を DHCP に組み込みます。これら 2 つのプロトコルは相互補完します。DHCP は、IP アドレス割り当てを集中化および自動化します。DDNS アップデートは、割り当てられたアドレスとホスト名の間のアソシエーションを事前定義された間隔で自動的に記録します。DDNS は、頻繁に変わるアドレスとホスト名のアソシエーションを頻繁にアップデートできるようにします。これにより、たとえばモバイルホストは、ユーザまたは管理者が操作することなく、ネットワーク内を自由に移動できます。DDNS は、DNS サーバ上で、名前からアドレスへのマッピングと、アドレスから名前へのマッピングをダイナミックにアップデートして、同期化します。

DDNS の名前とアドレスのマッピングは、DHCP サーバ上で 2 つのリソース レコード（RR）で行われます。A RR では、名前から IP アドレスへのマッピングが保持され、PTR RR では、アドレスから名前へのマッピングが行われます。DDNS 更新を実行するための 2 つの方式（RFC 2136 で規定されている IETF 標準規格、および一般的な HTTP 方式）のうち、Firepower Threat Defense デバイス では、IETF 方式をサポートしています。

（注） DDNS は BVI またはブリッジ グループのメンバー インターフェイスではサポートされません。

DDNS アップデート コンフィギュレーション

2 つの最も一般的な DDNS アップデート コンフィギュレーションは次のとおりです。

- DHCP クライアントは A RR をアップデートし、DHCP サーバは PTR RR をアップデートします。
- DHCP サーバは、A RR と PTR RR の両方をアップデートします。

通常、DHCP サーバはクライアントの代わりに DNS PTR RR を保持します。クライアントは、必要なすべての DNS アップデートを実行するように設定できます。サーバは、これらのアップデートを実行するかどうかを設定できます。DHCP サーバは、PTR RR をアップデートするクライアントの完全修飾ドメイン名（FQDN）を認識している必要があります。クライアントは Client FQDN と呼ばれる DHCP オプションを使用して、サーバに FQDN を提供します。

UDP パケット サイズ

DDNS は、DNS 要求者が UDP パケットのサイズをアドバタイズできるようにし、512 オクテットより大きいパケットの転送を容易にします。DNS サーバは UDP 上で要求を受信すると、OPT RR から UDP パケット サイズを識別し、要求者により指定された最大 UDP パケット サイズにできるだけ多くのリソース レコードを含めることができるよう、応答のサイズを調整します。

DNS パケットのサイズは、BIND の場合は最大 4096 バイト、Windows 2003 DNS サーバの場合は 1280 バイトです。

DHCP サービスと DDNS サービスのガイドライン

この項では、DHCP および DDNS サービスを設定する前に確認する必要のあるガイドラインおよび制限事項について説明します。

ファイアウォール モード

- DHCP リレーは、トランスペアレント ファイアウォール モード、BVI 上のルーテッド モードまたはブリッジグループ メンバー インターフェイスではサポートされません。
- DHCP サーバは、ブリッジグループ メンバー インターフェイス上のトランスペアレント ファイアウォール モードでサポートされます。 ルーテッド モードでは、DHCP サーバは BVI インターフェイスでサポートされますが、ブリッジ グループ メンバー インターフェイスではサポートされません。DHCP サーバを動作させるために、BVI には名前が必要です。
- DDNS は、トランスペアレント ファイアウォール モード、BVI 上のルーテッド モードまたはブリッジグループ メンバー インターフェイスではサポートされません。

IPv6

DHCP サーバでサポートされます。 DHCP リレーの IPv6 はサポートされます。

DHCPv4 サーバ

- 使用可能な DHCP の最大プールは 256 アドレスです。
- インターフェイスごとに 1 つの DHCP サーバのみを設定できます。各インターフェイスは、専用のアドレス プールのアドレスを使用できます。しかし、DNS サーバ、ドメイン名、オプション、ping のタイムアウト、WINS サーバなど他の DHCP 設定はグローバルに設定され、すべてのインターフェイス上の DHCP サーバによって使用されます。
- DHCP クライアントや DHCP リレー サービスは、サーバがイネーブルになっているインターフェイス上では設定できません。また、DHCP クライアントは、サーバがイネーブルになっているインターフェイスに直接接続する必要があります。
- Firepower Threat Defense デバイス は、QIP DHCP サーバと DHCP プロキシ サービスとの併用をサポートしません。
- DHCP サーバもイネーブルになっている場合、リレーエージェントをイネーブルにすることはできません。
- DHCP サーバは、BOOTP 要求をサポートしません。

DHCP リレー

- グローバルおよびインターフェイス固有のサーバを合わせて 10 台までの DHCPv4 リレー サーバを設定できます。インターフェイスごとには、4 台まで設定できます。
- 10 台までの DHCPv6 リレー サーバを設定できます。IPv6 のインターフェイス固有のサーバはサポートされません。
- DHCP サーバもイネーブルになっている場合、リレーエージェントをイネーブルにできません。
- DHCP リレー サービスは、トランスペアレント ファイアウォール モード。ただし、アクセス ルールを使用して DHCP トラフィックを通過させることはできます。DHCP 要求と応答がFirepower Threat Defenseデバイスを通過できるようにするには、2 つのアクセス ルールを設定する必要があります。1 つは内部インターフェイスから外部（UDP 宛先ポート 67）への DCHP 要求を許可するもので、もう 1 つは逆方向（UDP 宛先ポート 68）に向かうサーバからの応答を許可するためのものです。
- IPv4 の場合、クライアントは直接 Firepower Threat Defense デバイス に接続する必要があり、他のリレー エージェントやルータを介して要求を送信できません。IPv6 の場合、Firepower Threat Defense デバイス は別のリレー サーバからのパケットをサポートします。
- DHCP クライアントは、Firepower Threat Defense デバイス が要求をリレーする DHCP サーバとは別のインターフェイスに存在する必要があります。
- トラフィック ゾーン内のインターフェイスで DHCP リレーを有効にできません。

DHCP サーバの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin Access Admin Network Admin

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** の順に選択し、FTD デバイスを編集します。

ステップ 2 [DHCP] > [DHCP サーバ（DHCP Server）] を選択します。

ステップ 3 次の DHCP サーバのオプションを設定します。

- [Ping タイムアウト（Ping Timeout）]：Firepower Threat Defense デバイスが DHCP ping 試行のタイムアウトを待つ時間をミリ秒単位で入力します。有効値の範囲は 10 ～ 10000 ミリ秒です。デフォルト値は 50 ミリ秒です。

  アドレスの衝突を避けるために、Firepower Threat Defense デバイスは、1 つのアドレスに ICMP ping パケットを 2 回送信してから、そのアドレスを DHCP クライアントに割り当てます。

- [リース長（Lease Length）]：リースの期間が終了する前に、割り当てIPアドレスをクライアントが使用できる秒単位の時間。有効値の範囲は 300 ～ 1048575 秒です。デフォルト値は 3600 秒（1 時間）です。
- （ルーテッド モード）[自動設定（Auto-configuration）]：Firepower Threat Defense デバイスで DHCP 自動設定を有効にします。自動設定では、指定したインターフェイスで動作している DHCP クライアントから取得した DNS サーバ、ドメイン名、および WINS サーバの情報が、DHCP サーバから DHCP クライアントに提供されます。自動設定にしない場合は、自動設定を無効にして、手順 4 で値を追加することもできます。
- （ルーテッドモード）[インターフェイス（Interface）]：自動設定に使用されるインターフェイスを指定します。

ステップ 4 自動設定をオーバーライドするには、以下を実行します。

- インターフェイスのドメイン名を入力します。たとえば、デバイスは Your_Company ドメインにあるかもしれません。
- ドロップダウン リストから、インターフェイスに設定された DNS サーバ（プライマリおよびセカンダリ）を選択します。DNS サーバを新たに追加する手順については、ネットワーク オブジェクトの作成 （527 ページ）を参照してください。
- ドロップダウン リストから、インターフェイスに設定された WINS サーバ（プライマリおよびセカンダリ）を選択します。WINS サーバを新たに追加する手順については、ネットワーク オブジェクトの作成 （527 ページ）を参照してください。

ステップ 5 [サーバ（Server）] タブを選択して [追加（Add）] をクリックし、次のオプションを設定します。

- [インターフェイス（Interface）]：ドロップダウン リストからインターフェイスを選択します。トランスペアレント モードでは、名前付きブリッジ グループ メンバー インターフェイスを指定します。ルーテッド モードでは、名前付きルーテッド インターフェイスまたは名前付き BVI を指定します。ブリッジ グループ メンバー インターフェイスは指定しないでください。DHCP サーバが動作するためには、BVI の各ブリッジ グループ メンバー インターフェイスにも名前を付ける必要があることに注意してください。
- [アドレス プール（Address Pool）]：DHCP サーバが使用する IP アドレスの最下位から最上位の間の範囲です。IPアドレスの範囲は、選択したインターフェイスと同じサブネット上に存在する必要があり、インターフェイス自身の IP アドレスを含めることはできません。
- [DHCP サーバを有効にする（Enable DHCP Server）]：選択したインターフェイスの DHCP サーバを有効にします。

ステップ 6 [OK] をクリックして、DHCP サーバの設定を保存します。

ステップ 7 （オプション）[詳細（Advanced）] タブを選択して、[追加（Add）] をクリックし、DHCP クライアントに戻すオプションの情報のタイプを指定します。

- [オプション コード（Option Code）]：Firepower Threat Defense デバイスは、RFC 2132、RFC 2562、および RFC 5510 に記載されている情報を送信する DHCP オプションをサポートしています。オプション 1、12、50 ～ 54、58 ～ 59、61、67、82 を除き、すべての DHCP オプション（1 ～ 255）がサポート

されています。DHCP オプション コードの詳細については、DHCPv4 サーバについて （853 ページ）を参照してください。

（注） Firepower Threat Defense デバイスは、指定されたオプションのタイプおよび値が、RFC 2132 に定義されているオプション コードに対して期待されているタイプおよび値と一致するかどうかは確認しません。オプション コードと、コードに関連付けられたタイプおよび期待値の詳細については、RFC 2132 を参照してください。

- [タイプ（Type）]：DHCP のオプションのタイプ。使用できるオプションには、IP、ASCII、および HEX が含まれます。IP を選択する場合、[IP アドレス（IP Address）] フィールドに IP アドレスを追加する必要があります。ASCII を選択する場合、[ASCII] フィールドに [ASCII] 値を追加する必要があります。HEX を選択する場合、[HEX] フィールドに [HEX] 値を追加する必要があります。
- [IP アドレス 1（IP Address 1）] および [IP アドレス 2（IP Address 2）]：このオプションコードで戻る IP アドレス。IP アドレスを新たに追加する手順については、ネットワーク オブジェクトの作成 （527 ページ）を参照してください。
- [ASCII]：DHCP クライアントに戻る ASCII 値。文字列にスペースを含めることはできません。
- [HEX]：DHCP クライアントに戻る HEX 値。文字列はスペースなしの偶数でなければなりません。0x プレフィックスを使用する必要はありません。

ステップ 8 [OK] をクリックして、オプション コードの設定を保存します。

ステップ 9 DHCP ページで [保存（Save）] をクリックして変更を保存します。

DHCP リレー エージェントの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin Access Admin Network Admin

インターフェイスで受信した DHCP 要求を 1 つまたは複数の DHCP サーバに転送するように DHCP リレー エージェントを設定できます。DHCP クライアントは、最初の DHCPDISCOVER メッセージを送信するために UDP ブロードキャストを使用します。接続されたネットワークについての情報がクライアントにはないためです。サーバを含まないネットワーク セグメントにクライアントがある場合、Firepower Threat Defense デバイスはブロードキャスト トラフィックを転送しないため、UDP ブロードキャストは通常転送されません。

ブロードキャストを受信している Firepower Threat Defense デバイスのインターフェイスが DHCP 要求を別のインターフェイスの DHCP サーバに転送するように設定すると、この状況を改善できます。

（注） DHCP リレーは、トランスペアレント ファイアウォール モードまたは では、サポートされません。

ステップ 1 **[デバイス（Devices）] > [デバイス管理（Device Management）]** の順に選択し、FTD デバイスを編集します。

ステップ 2 [DHCP] > [DHCP リレー（DHCP Relay）] を選択します。

ステップ 3 [タイムアウト（Timeout）] フィールドでは、Firepower Threat Defense デバイスが DHCP リレー エージェントのタイムアウトを待つ時間を秒単位で入力します。有効な値の範囲は 1 ～ 3600 秒です。デフォルト値は 60 秒です。

タイムアウトは、ローカル DHCP リレー エージェントを介すアドレス ネゴシエーション用です。

ステップ 4 [DHCP リレー エージェント（DHCP Relay Agent）] タブで、[追加（Add）] をクリックして、以下のオプションを設定します。

- [インターフェイス（Interface）]：DHCP クライアントに接続されているインターフェイス。
- [DHCP リレーを有効にする（Enable DHCP Relay）]：このインターフェイスで IPv4 DHCP リレーを有効にします。
- [ルート設定（Set Route）]：（IPv4 用）サーバからの DHCP メッセージのデフォルト ゲートウェイ アドレスを、元の DHCP 要求をリレーした DHCP クライアントに最も近い Firepower Threat Defense デバイスのインターフェイスのアドレスに変更します。このアクションを行うと、クライアントは、自分のデフォルト ルートを設定して、DHCP サーバで異なるルータが指定されている場合でも、Firepower Threat Defense デバイスをポイントすることができます。パケット内にデフォルトのルータ オプションがなければ、Firepower Threat Defense デバイスは、そのインターフェイスのアドレスを含んでいるデフォルト ルータを追加します。
- [IPv6 リレーを有効にする（Enable IPv6 Relay）]：このインターフェイスで IPv6 DHCP リレーを有効にします。

ステップ 5 [OK] をクリックして、DHCP リレー エージェントの変更を保存します。

ステップ 6 [DHCP サーバ（DHCP Servers）] タブで、[追加（Add）] をクリックして、以下のオプションを設定します。

IPv4 サーバ アドレスおよび IPv6 サーバ アドレスが同じサーバに属していても、個別のエントリとして追加します。

- [サーバ（Server）]：DHCP サーバの IP アドレス。ドロップダウン リストから IP アドレスを選択します。新たに加えるには、次を参照してください。 ネットワーク オブジェクトの作成 （527 ページ）
- [インターフェイス（Interface）]：指定の DHCP サーバが接続されるインターフェイス。DHCP リレー エージェントと DHCP サーバを、同じインターフェイスに設定することはできません。

ステップ 7 [OK] をクリックして、DHCP サーバの変更を保存します。

ステップ 8 DHCP ページで [保存（Save）] をクリックして変更を保存します。

DDNS の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin Access Admin Network Admin

ダイナミック DNS（DDNS）アップデートにより、DNS を DHCP に組み込みます。DDNS 更新プログラムは割り当て済みアドレスとホスト名の間のアソシエーションを自動的に記録し、頻繁に変更されるアドレスとホスト名間のアソシエーションを効果的に更新できるようにします。

始める前に

- 概要については、DDNS の概要 （855 ページ）を参照してください。
- DDNS は、トランスペアレント ファイアウォール モードでサポートされていません。

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** の順に選択し、FTD デバイスを編集します。

ステップ 2 **[DHCP]** > **[DDNS]**を選択して、次の DDNS オプションを設定します。

- [DHCP クライアントが記録更新を DHCP サーバに要求（DHCP Client Requests DHCP Server to update Records）]：DHCP サーバによる指定の記録の更新を DHCP クライアントが要求するよう設定します。使用可能なオプションは、[選択なし（Not Selected）]、[更新なし（No Update）]、[PTR のみ（Only PTR）]、[A と PTR 記録（Both A and PTR Records）] です。A および PTR 記録の説明については、DDNS の概要 （855 ページ）を参照してください。
- [DHCP クライアント ブロードキャストを有効にする（Enable DHCP Client Broadcast）]：DHCP クライアントが DHCP サーバに到達するためにブロードキャスト アドレスを使用することを有効にします。
- [ダイナミック DNS 更新（Dynamic DNS Update）]：DHCP サーバの DDNS 更新に使用する記録を選択します。使用可能なオプションは、[選択なし（Not Selected）]、[PTR のみ（Only PTR）]、[A と PTR 記録（Both A and PTR Records）] です。
- [DHCP クライアント要求のオーバーライド（Override DHCP Client Requests）]：DHCP サーバのアクションが、DHCP クライアントによって要求された更新アクションをオーバーライドするよう指定します。

ステップ 3 [DHCP クライアント ID インターフェイス（DHCP Client ID Interface）] タブで、[使用可能なインターフェイス（Available Interfaces）] リストからインターフェイスを選択し、[追加（Add）] をクリックして、インターフェイスを [選択されたインターフェイス（Selected Interfaces）] リストに移動します。

ステップ 4 [DDNS インターフェイス設定（DDNS Interface Settings）] タブで、[追加（Add）] をクリックし、以下のオプションを設定します。

- [インターフェイス（Interface）]：設定済みのそれぞれのインターフェイスに DDNS 設定を追加するには、ドロップダウン リストからインターフェイスを選択します。
- [方法名（Method Name）]：インターフェイスに割り当てられた DDNS 更新方法。
- [ホスト名（Host Name）]：DDNS クライアントのホスト名。
- [DHCP クライアントが更新要求を DHCP サーバに要求（DHCP Client requests DHCP server to update requests）]：DHCP サーバによる指定の記録の更新を DHCP クライアントが要求するよう設定します。使用可能なオプションは、[選択なし（Not Selected）]、[更新なし（No Update）]、[PTR のみ（Only PTR）]、[A と PTR 記録（Both A and PTR Records）] です。A および PTR 記録の説明については、DDNS の概要 （855 ページ）を参照してください。
- [ダイナミック DNS 更新（Dynamic DNS Update）]：DHCP サーバの DDNS 更新に使用する記録を選択します。使用可能なオプションは、[選択なし（Not Selected）]、[PTR のみ（Only PTR）]、[A と PTR 記録（Both A and PTR Records）] です。
- [DHCP クライアント要求のオーバーライド（Override DHCP Client Requests）]：DHCP サーバのアクションが、DHCP クライアントによって要求された更新アクションをオーバーライドするよう指定します。

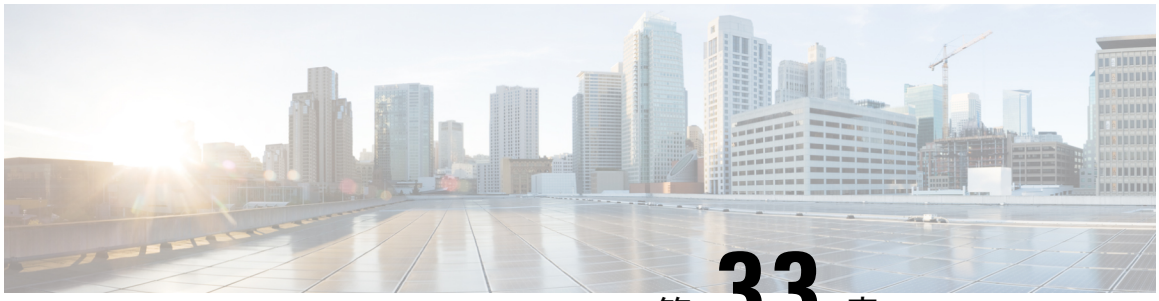
ステップ 5 [OK] をクリックして、DDNS のインターフェイスの変更を保存します。

ステップ 6 [DDNS 更新方法（DDNS Update Methods）] タブで、[追加（Add）] をクリックし、以下のオプションを設定します。

- [方法名（Method Name）]：インターフェイスに割り当てられた DDNS 更新方法。
- [更新間隔（Update Interval）]：日（0 ～ 364）、時（0 ～ 23）、分（0 ～ 59）、秒（0 ～ 59）で設定される DNS の更新試行の整数の更新間隔。これらの単位は、追加式です。つまり、日数に 0、時間数に 0、分数に 5、秒数に 15 を入力した場合、このアップデート方式がアクティブである限り、5 分 15 秒ごとに更新が試行されます。
- [更新記録（Update Records）]：DNS クライアントによるサーバ リソース記録の更新を保存します。使用可能なオプションは、[定義なし（Not Defined]、[A と PTR 記録（Both A and PTR Records）]、[A 記録（A Records）] です。

ステップ 7 [OK] をクリックして、DDNS の更新方法の変更を保存します。

ステップ 8 DHCP ページで [保存（Save）] をクリックして変更を保存します。



第 33 章

Firepower Threat Defense 用の Quality of Service（QoS）

以下のトピックでは、Firepower Threat Defense デバイスを使ってネットワーク トラフィックを管理するために Quality of Service（QoS）機能を使用する方法について説明します。

QoS の概要

Quality of Service（QoS）は、アクセス制御によって許可または信頼されている（ポリシーの）ネットワーク トラフィックをレート制限します。システムはファストパスされたトラフィックにレート制限は行いません。

QoS は、Firepower Threat Defense デバイスのルーテッド インターフェイスのみでサポートされています。

レート制限された接続のロギング

QoS 用のロギング設定はありません。接続はロギングなしでレート制限することができ、またレート制限されているという理由だけで接続をロギングすることはできません。接続イベントで QoS 情報を表示するには、適切な接続の終了を Firepower Management Center データベースに個別にロギングする必要があります。ログ可能なその他の接続（3003 ページ）を参照してください。

レート制限された接続の接続イベントには、どの程度のトラフィックがドロップされ、どの QoS の設定がトラフィックを制限したかについての情報が含まれています。この情報はイベント ビューア（ワークフロー）、ダッシュボード、レポートで確認できます。

QoS ポリシーについて

管理対象デバイスに展開する QoS ポリシーによりレート制限が決まります。各 QoS ポリシーは、複数のデバイスを対象にすることができます。各デバイスで同時に展開可能な QoS ポリシーは 1 つです。

QoS ポリシーでは、最大 32 の QoS ルールがネットワーク トラフィックを処理します。システムは指定した順序で QoS ルールをトラフィックと照合します。システムは、すべての条件がトラフィックに一致する最初のルールに従ってトラフィックをレート制限します。どのルールにも一致しないトラフィックは、レート制限を受けません。

QoS ルールは、送信元または接続先（ルーティング先）インターフェイスによって制約を設ける必要があります。システムは、これらの個別のインターフェイスでそれぞれ独立したレート制限を行います。複数のインターフェイスにまとめてレート制限を指定することはできません。

QoS ルールでは、その他のネットワーク特性や、アプリケーション、URL、ユーザ ID、およびカスタム セキュリティ グループ タグ（SGT）などのコンテキスト情報によってトラフィックのレート制限を行うこともできます。

トラフィックのアップロードやダウンロードのレート制限を個別に行うことが可能です。システムは、接続イニシエータに基づいてダウンロード方向とアップロード方向を決定します。

（注） QoS はマスターアクセス制御設定に従属するものではありません。QoS は個別に設定します。ただし、同じデバイスに展開されたアクセス コントロール ポリシーおよび QoS ポリシーはアイデンティティ設定を共有します。アクセス制御への他のポリシーの関連付け （1684 ページ）を参照してください。

QoS ポリシーとマルチテナンシー

マルチドメイン展開では、編集できる現在のドメインで作成されたポリシーが表示されます。また、編集できない先祖ドメインで作成されたポリシーも表示されます。下位のドメインで作成されたポリシーを表示および編集するには、そのドメインに切り替えます。

先祖ドメインの管理者は、異なる子孫ドメインのデバイスに、同じ QoS ポリシーを展開できます。子孫ドメインの管理者は、この先祖ドメインから展開された読み取り専用 QoS ポリシーを使用するか、またはローカル ポリシーに置き換えることができます。

QoS ポリシーによるレートの制限

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin/Access Admin/Network Admin

ポリシー ベースのレート制限を実行するために、管理対象デバイスに QoS ポリシーを設定して展開します。各 QoS ポリシーは複数のデバイスをターゲットにすることができます。各デバイスに同時に展開できる QoS ポリシーは 1 つです。

ポリシーの編集は、1 つのブラウザ ウィンドウを使用して、一度に 1 人のみで行う必要があります。複数のユーザが同じポリシーを保存した場合は、最後に保存された変更が保持されます。ユーザにとっての便宜性を考慮して、各ポリシーを現在編集している人（いる場合）の情報が表示されます。セッションのプライバシーを保護するために、ポリシーエディタが非アクティブになってから 30 分後に警告が表示されます。60 分後には、システムにより変更が破棄されます。

ステップ 1 **[Devices]** > **[QoS]**を選択します。

ステップ 2 [新規ポリシー（New Policy）] をクリックして、新しい QoS ポリシーを作成して、必要に応じてターゲット デバイスを割り当てます。詳細については、QoS ポリシーの作成 （866 ページ）を参照してください。

また、既存のポリシーをコピー（  ）または編集（  ）することもできます。

ステップ 3 QoS ルールを設定します。QoS ルールの設定 （867 ページ）またはルール管理：共通の特性 （463 ページ）を参照してください。

QoS ポリシーエディタの [ルール（Rules）] タブには、各ルールが評価順にリストされ、ルール条件とレート制限の設定の概要が表示されます。右クリックのメニューには、ルールの管理オプション（移動、有効化、無効化など）があります。

大規模な展開では、特定のデバイスまたはデバイスのグループに影響するルールのみを表示する、[デバイス基準のフィルタ（Filter by Device）] が役に立ちます。また、ルールの検索とルール内の検索も可能です。システムは、[ルールの検索（Search Rules）] フィールドに入力されたテキストをルールの名前および条件値と照合します。これには、オブジェクトとオブジェクト グループが含まれます。

（注） ルールを適切に作成して順序付けることは複雑なタスクですが、効果的な展開を構築する上で不可欠なタスクです。慎重に計画していないと、ルールが別のルールをプリエンプション処理したり、追加のライセンスが必要になったり、ルールに無効な設定が含まれる場合があります。アイコンにより、コメント、警告、およびエラーが表されます。問題があれば、[警告の表示（Show Warnings）] をクリックしてリストを表示します。詳細については、ルールのパフォーマンスに関するガイドライン （502 ページ）を参照してください。

ステップ 4 [ポリシーの割り当て（Policy Assignments）] をクリックして、ポリシーがターゲットにしている管理対象デバイスを特定します。詳細については、QoS ポリシーのターゲット デバイスの設定 （867 ページ）を参照してください。

ポリシーの作成中にデバイス ターゲットを特定した場合は、選択内容を確認します。

ステップ 5 QoS ポリシーを保存します。

ステップ 6 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

QoS ポリシーの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin Access Admin Network Admin

ルールのない新規 QoS ポリシーは、レート制限を実行しません。

ステップ 1 **[Devices]** > **[QoS]**を選択します。

ステップ 2 [新しいポリシー（New Policy）] をクリックします。

ステップ 3 [名前（Name）] を入力し、必要に応じて [説明（Description）] を入力します。

ステップ 4 （オプション）ポリシーを展開する [使用可能なデバイス（Available Devices）] を選択し、[ポリシーに追加（Add to Policy）] をクリックするか、[選択されたデバイス（Selected Devices）] にドラッグ アンド ドロップします。表示されるデバイスを絞り込むには、[検索（Search）] フィールドに検索文字列を入力します。

ポリシーを展開する前に、デバイスを割り当てる必要があります。

ステップ 5 [保存（Save）] をクリックします。

次のタスク

- QoS ポリシーを設定および展開します。QoS ポリシーによるレートの制限 （865 ページ）を参照してください。

QoS ポリシーのターゲット デバイスの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin Access Admin Network Admin

各 QoS ポリシーは複数のデバイスをターゲットにすることができます。各デバイスに同時に展開できる QoS ポリシーは 1 つです。

ステップ 1 QoS ポリシー エディタで、[ポリシーの割り当て（Policy Assignments）] をクリックします。

ステップ 2 ターゲット リストを作成します。

- 追加：1 つ以上の [使用可能なデバイス（Available Devices）] を選択して、[ポリシーに追加（Add to Policy）] をクリックするか、[選択したデバイス（Selected Devices）] のリストにドラッグ アンド ドロップします。
- 削除：1 つのデバイスの横にある削除アイコン（）をクリックするか、複数のデバイスを選択して、右クリックしてから [選択済み項目の削除（Delete Selected）] を選択します。
- 検索：検索フィールドに検索文字列を入力します。検索をクリアするには、クリア（）をクリックします。

ステップ 3 [OK] をクリックしてポリシーの割り当てを保存します。

ステップ 4 [保存（Save）] をクリックして、ポリシーを保存します。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

QoS ルールの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin/Access Admin/Network Admin

ルールを作成または編集するときに、一般的なルール プロパティを設定するには、ルール エディタの上部を使用します。ルール条件とコメントを設定するには、下部のタブを使用します。

ステップ 1 QoS ポリシー エディタの [ルール（Rules）] タブで、次の操作を実行します。

- ルールの追加：[ルールの追加（Add Rule）] をクリックします。
- ルールの編集：編集アイコン（  ）をクリックします。

ステップ 2 [名前（Name）]を入力します。

ステップ 3 ルール コンポーネントを設定します。

- [有効化（Enabled）]：ルールを有効にするかどうかを指定します。
- [QoS の適用（Apply QoS On）]：レート制限するインターフェイス（[宛先インターフェイス オブジェクトのインターフェイス（Interfaces in Destination Interface Objects）] または [送信元インターフェイス オブジェクトのインターフェイス（Interfaces in Source Interface Objects）]）を選択します。選択するインターフェイスは、入力されたインターフェイス制約（任意ではなく）と一致する必要があります。
- [インターフェイスごとのトラフィック制限（Traffic Limit Per Interface）]：ダウンロード制限とアップロード制限を Mbits/sec 単位で入力します。[無制限（Unlimited）] のデフォルト値にすると、一致するトラフィックはその方向でレート制限されません。
- [条件（Conditions）]：追加する条件に対応するタブをクリックします。[QoS の適用（Apply QoS On）] の選択内容に対応する、送信元インターフェイスまたは宛先インターフェイスの条件を設定する必要があります。
- [コメント（Comments）]：[コメント（Comments）] タブをクリックします。コメントを追加するには、[新規コメント（New Comment）] をクリックしてコメントを入力し、[OK] をクリックします。ルールを保存するまでこのコメントを編集または削除できます。

ルール コンポーネントの詳細については、QoS ルール コンポーネント （869 ページ）を参照してください。

ステップ 4 ルールを保存します。

ステップ 5 ポリシー エディタで、ルールの位置を設定します。クリックしてドラッグするか、または右クリック メニューを使用してカット アンド ペーストを実行します。

ルールには1から番号が付けられます。システムは、ルール番号の昇順で上から順に、ルールをトラフィックと照合します。トラフィックが一致する最初のルールは、そのトラフィックを処理するルールです。適切なルールの順序を指定することで、ネットワーク トラフィックの処理に必要なリソースが削減され、ルールのプリエンプションを回避できます。

ステップ 6 [保存（Save）] をクリックして、ポリシーを保存します。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

関連トピック

ルールのパフォーマンスに関するガイドライン （502 ページ）

QoS ルール コンポーネント

状態（有効/無効）

デフォルトでは、ルールは有効になっています。ルールを無効にすると、システムはそのルールを使用せず、そのルールに対する警告とエラーの生成を停止します。

インターフェイス（QoS の適用対象）

すべてのトラフィックがレート制限されている QoS のルールは保存できません。QoS のルールごとに、次のいずれかに QoS を適用する必要があります：

- 送信元インターフェイスオブジェクトのインターフェイス：レートは、ルールの送信元インターフェイスを介するトラフィックに制限されます。このオプションを選択すると、少なくとも 1 つの送信元インターフェイスの制約を追加する必要があります（**どんな**制約であってもよいわけではありません）。
- 宛先インターフェイスオブジェクト：レートは、ルールの宛先インターフェイスを介するトラフィックに制限されます。このオプションを選択すると、少なくとも 1 つの宛先インターフェイスの制約を追加する必要があります（**どんな**制約であってもよいわけではありません）。

インターフェイスごとのトラフィック制限

QoS ルールでは、[QoS の適用対象（Apply QoS On）] オプションで指定するインターフェイスごとに個別にレートを制限します。インターフェイスのセットに対して集約レート制限を指定することはできません。

トラフィックのレート制限を M ビット/秒とします。[無制限（Unlimited）] のデフォルト値では、一致したトラフィックのレートは制限されません。

トラフィックのアップロードやダウンロードのレート制限を個別に行うことが可能です。システムは、接続イニシエータに基づいてダウンロード方向とアップロード方向を決定します。

インターフェイスの最大スループットを超える制限を指定すると、システムは一致しているトラフィックのレート制限は行いません。最大スループットはインターフェイスのハードウェア構成による影響を受ける可能性があり、各デバイス（**[Devices]** > **[Device Management]**）のプロパティに指定します。

条件

条件は、ルールで処理する特定のトラフィックを指定します。複数の条件により各ルールを設定できます。トラフィックは、ルールに一致するすべての条件に適合する必要があります。各条件の種類には、ルールエディタ内に独自のタブがあります。以下を使用して、トラフィックをレート制限できます：

- インターフェイス条件 （468 ページ） （ルート設定済みの場合のみ、必須）
- ネットワーク条件 （471 ページ）

- ポートおよび ICMP コードの条件 （477 ページ）
- アプリケーション条件（アプリケーション制御） （479 ページ）
- URL Filtering （1717 ページ）
- ユーザ条件、レルム条件、および ISE 属性条件（ユーザ制御） （490 ページ）
- カスタム SGT 条件 （495 ページ）

説明

ルールで変更を保存するたびに、コメントを追加することができます。たとえば、他のユーザのために設定全体を要約したり、ルールの変更時期と変更理由を記載することができます。

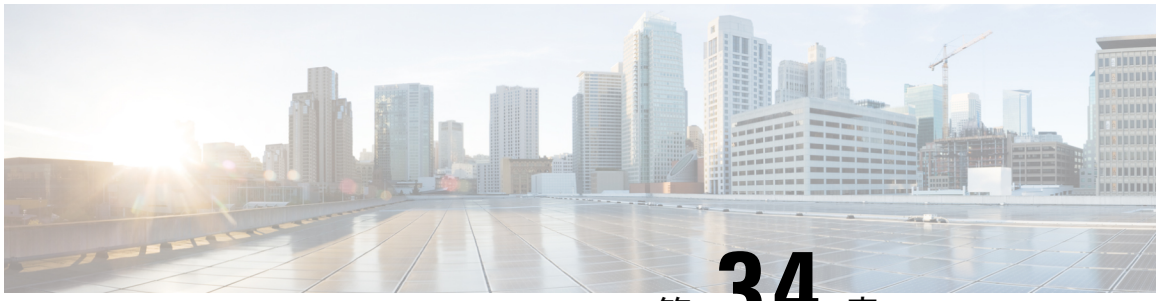
ポリシー エディタでは、システムがそのルールのコメント数を表示します。ルール エディタでは、[コメント（Comments）]タブを使用して、既存のコメントを表示し、新しいコメントを追加します。

QOS の履歴

機能	バージョン	詳細
レート制限の増大	6.2.1	最大レート制限が 1,000 Mbps から 100,000 Mbps に増やされました。 変更された画面：QoS ルール エディタ サポートされているプラットフォーム：Firepower Threat Defense
カスタム SGT および元のクライアント ネットワーク フィルタリング	6.2.1	QoS では、カスタム セキュリティ グループ タグ（SGT）および元のクライアント ネットワーク情報（XFF、True-Client-IP、またはカスタム定義の HTTP ヘッダー）を使用して、トラフィックのレート制限を行えるようになりました。 変更された画面：QoS ルール エディタ サポートされているプラットフォーム：Firepower Threat Defense
QoS（レート制限）	6.1	導入された機能。 QoS は、アクセス制御によって許可または信頼されている（ポリシーの）ネットワーク トラフィックをレート制限します。 新しい画面：**[デバイス（Devices）] > [QoS]** サポートされているプラットフォーム：Firepower Threat Defense

第 IX 部

Firepower Threat Defense のハイ アベイラビリティと拡張性



第 34 章

Firepower Threat Defense のハイ アベイラビリティ

次のトピックでは、Cisco Firepower Threat Defense のハイ アベイラビリティを達成するためにアクティブ/スタンドバイ フェールオーバーを設定する方法について説明します。

ハイ アベイラビリティ Firepower Threat Defense について

フェールオーバーとも呼ばれるハイアベイラビリティを設定するには、専用フェールオーバーリンク（および任意でステートリンク）を介して相互に接続された 2 台の同じ Firepower Threat Defense デバイスが必要です。Firepower Threat Defense はアクティブ/スタンバイ フェールオーバーをサポートしています。つまり 1 台のユニットがアクティブなユニットとなりトラフィックを渡します。スタンバイ装置は、アクティブにトラフィックを通過させることはありませんが、アクティブ装置の設定やその他の状態情報を同期しています。フェールオーバーが発生すると、アクティブ装置がスタンバイ装置にフェールオーバーし、そのスタンバイ装置がアクティブになります。

アクティブ装置（ハードウェア、インターフェイス、ソフトウェアおよび環境ステータス）の状態は、特定のフェールオーバー条件に一致しているかどうかを確認するためにモニタされます。所定の条件に一致すると、フェールオーバーが行われます。

（注） ハイ アベイラビリティは、パブリック クラウドで実行される Firepower Threat Defense Virtual ではサポートされていません。

高可用性 のシステム要件

この項では、高可用性 コンフィギュレーションにあるFirepower Threat Defense デバイスのハードウェア要件、ソフトウェア要件、およびライセンス要件について説明します。

ハードウェア要件

高可用性コンフィギュレーションの2台の装置は、次の条件を満たしている必要があります。

- 同じモデルであること。 さらに、コンテナ インスタンスでは、同じリソース プロファイル属性を使用する必要があります。

  Firepower 9300 の場合、高可用性は同じタイプのモジュール間でのみサポートされていますが、2 台のシャーシにモジュールを混在させることができます。たとえば、各シャーシにSM-36、、およびSM-44を配置できます。SM-36モジュール間、およびSM-44モジュール間に高可用性ペアを作成できます。

  ハイ アベイラビリティ ペアを FMC に追加した後にリソース プロファイルを変更する場合は、**[Devices]** > **[Device Management]** > **[Device]** > **[System]** > **[Inventory]** ダイアログ ボックスで各装置のインベントリを更新します。

- インターフェイスの数とタイプが同じであること。

  Firepower 4100/9300 シャーシ では、高可用性 を有効にする前に、すべてのインターフェイスがFXOSで同一に事前構成されている必要があります。高可用性を有効にした後でインターフェイスを変更する場合は、スタンバイ ユニットの FXOS でインターフェイスを変更し、アクティブ ユニットで同じ変更を行います。

高可用性 コンフィギュレーションで装置に異なるサイズのフラッシュ メモリを使用している場合、小さい方のフラッシュ メモリを取り付けた装置に、ソフトウェア イメージ ファイルおよびコンフィギュレーション ファイルを格納できる十分な容量があることを確認してください。十分な容量がない場合、フラッシュ メモリの大きい装置からフラッシュ メモリの小さい装置にコンフィギュレーションの同期が行われると、失敗します。

ソフトウェア要件

高可用性コンフィギュレーションの2台の装置は、次の条件を満たしている必要があります。

- 同じファイアウォール モードにあること（ルーテッドまたはトランスペアレント）。
- ソフトウェア バージョンが同じであること。
- Firepower Management Center 上で、同じドメインまたはグループに入っていること。
- 同じ NTP コンフィギュレーションであること。脅威に対する防御のための NTP 時刻同期の設定 （1406 ページ）を参照してください。
- 非コミットの変更で、Firepower Management Center 上で完全に展開していること。
- どのインターフェイスでも、DHCP または PPPoE は変更していないこと。

- （Firepower 4100/{3}9300{3}）同じフロー オフロード モードを使用し、両方とも有効または無効になっている。

高可用性ペアでの FTD デバイスのライセンス要件

ハイ アベイラビリティ構成での Firepower Threat Defense デバイスは、すべて同じライセンスである必要があります。ハイ アベイラビリティを確立する前に、どのライセンスがセカンダリ/スタンバイ デバイスに割り当てられているかどうかは問題にはなりません。ハイ アベイラビリティの設定中に、Firepower Management Center はスタンバイに割り当てられている不要なライセンスをすべて削除し、プライマリ/アクティブ デバイスに割り当てられているのと同じライセンスで置き換えます。たとえば、アクティブ デバイスは基本ライセンスと Threat ライセンスであり、スタンバイ デバイスは基本ライセンスだけの場合、Firepower Management Center は Cisco Smart Software Manager と通信して、アカウントからスタンバイ デバイス用に使用可能な Threat ラインセンスを取得します。スマート ライセンス アカウントで十分な数の資格が購入されていなければ、正しい数のライセンスを購入するまで、アカウントは非準拠の状態になります。ハイ アベイラビリティ構成には、2 つのスマート ライセンス資格（ペアを構成するデバイスごとに 1 つ）が必要です。

フェールオーバー リンクとステートフル フェールオーバー リンク

フェールオーバー リンクとオプションのステートフル フェールオーバー リンクは、2 つの装置間の専用接続です。シスコでは、フェールオーバー リンクまたはステートフル フェールオーバー リンク内の 2 つのデバイス間で同じインターフェイスを使用することを推奨しています。たとえば、フェールオーバー リンクで、デバイス 1 で eth0 を使用していた場合は、デバイス 2 でも同じインターフェイス（eth0）を使用します。

フェールオーバー リンク

フェールオーバー ペアの 2 台の装置は、フェールオーバー リンク経由で常に通信して、各装置の動作ステータスを確認しています。

フェールオーバー リンク データ

次の情報がフェールオーバー リンク経由で伝達されています。

- 装置の状態（アクティブまたはスタンバイ）
- hello メッセージ（キープアライブ）
- ネットワーク リンクの状態
- MAC アドレス交換
- コンフィギュレーションの複製および同期

フェールオーバー リンクのインターフェイス

使用されていないデータ インターフェイス（物理、冗長、または EtherChannel）はいずれもフェールオーバー リンクとして使用できます。ただし、現在名前が設定されているインターフェイスは指定できません。サブインターフェイスを使用することもできません。コンテナインスタンスの Firepower 4100/9300 シャーシで定義されたサブインターフェイスを除きます。フェールオーバー リンク インターフェイスは、通常のネットワーク インターフェイスとしては設定されません。フェールオーバー通信のためにだけ存在します。このインターフェイスは、フェールオーバー リンク用にのみ使用できます（ステート リンク用としても使用できます）。

FTD は、ユーザ データとフェールオーバー リンク間でのインターフェイスの共有をサポートしていません。同じ親の別のサブインターフェイスをフェールオーバー リンクやデータのために使用することもできません（Firepower 4100/9300 シャーシのサブインターフェイスのみ）。フェールオーバー リンクに対して Firepower 4100/9300 サブインターフェイスを使用する場合、その親にあるすべてのサブインターフェイスと親自体のフェールオーバー リンクとしての使用が制限されます。

（注） フェールオーバーまたはステート リンクとして EtherChannel または冗長インターフェイスを使用している場合、ハイ アベイラビリティを確立する前に、両方のデバイスで同じメンバー インターフェイスを備えた同じ EtherChannel または冗長インターフェイスが存在していることを確認する必要があります。

フェールオーバー リンクとして使用される冗長インターフェイスについては、冗長性の増強による次の利点を参照してください:

- フェールオーバー ユニットが起動すると、メンバー インターフェイスを交互に実行し、アクティブ ユニットを検出します。
- メンバー インターフェイスの 1 つにあるピアからのキープアライブ メッセージの受信をフェールオーバー ユニットが停止した場合、別のメンバー インターフェイスに切り替えます。

フェールオーバー リンクとして使用される EtherChannel の場合は、順序が不正なパケットを防止するために、EtherChannel 内の 1 つのインターフェイスのみが使用されます。そのインターフェイスで障害が発生した場合は、EtherChannel 内の次のリンクが使用されます。フェールオーバー リンクとして使用中の EtherChannel の設定は変更できません。

フェールオーバー リンクの接続

フェールオーバー リンクを次の 2 つの方法のいずれかで接続します。

- Firepower Threat Defense デバイスのフェールオーバー インターフェイスと同じネットワーク セグメント（ブロードキャスト ドメインまたは VLAN）に他の装置のないスイッチを使用する。
- イーサネット ケーブルを使用して装置を直接接続します。外部スイッチは必要ありません。

装置間でスイッチを使用しない場合、インターフェイスに障害が発生すると、リンクは両方のピアでダウンします。このような状況では、障害が発生してリンクがダウンする原因になったインターフェイスがどちらの装置のものかを簡単に特定できないため、トラブルシューティング作業が困難になる場合があります。

ステートフル フェールオーバー リンク

ステートフル フェールオーバーを使用するには、接続ステート情報を渡すためのステートフル フェールオーバー リンク（ステート リンクとも呼ばれる）を設定する必要があります。

（注） ステートフル フェールオーバー リンクの帯域幅は、少なくともデータ インターフェイスの帯域幅と同等にすることを推奨します。

フェールオーバー リンクの共有

インターフェイスを節約するための最適な方法はフェールオーバー リンクの共有です。ただし、設定が大規模でトラフィックが膨大なネットワークを使用している場合は、ステート リンクとフェールオーバー リンク専用のインターフェイスを検討する必要があります。

ステートフル フェールオーバー リンク専用のインターフェイス

ステート リンク専用のデータ インターフェイス（物理、冗長、またはEtherChannel）を使用できます。ステート リンクとして使用されるEtherChannelの場合は、順序が不正なパケットを防止するために、EtherChannel 内の 1 つのインターフェイスのみが使用されます。そのインターフェイスで障害が発生した場合は、EtherChannel 内の次のリンクが使用されます。

次の 2 つの方法のいずれかで、専用のステート リンクを接続します。

- Firepower Threat Defense デバイスのフェールオーバー インターフェイスと同じネットワーク セグメント（ブロードキャスト ドメインまたは VLAN）に他の装置のないスイッチを使用する。
- イーサネット ケーブルを使用してアプライアンスを直接接続します。外部スイッチは必要ありません。

  装置間でスイッチを使用しない場合、インターフェイスに障害が発生すると、リンクは両方のピアでダウンします。このような状況では、障害が発生してリンクがダウンする原因になったインターフェイスがどちらの装置のものかを簡単に特定できないため、トラブルシューティング作業が困難になる場合があります。

  Firepower Threat Defenseデバイスは、銅線イーサネット ポートでAuto-MDI/MDIXをサポートしているため、クロスオーバー ケーブルまたはストレート ケーブルのいずれかを使用できます。ストレート ケーブルを使用した場合は、インターフェイスが自動的にケーブルを検出して、送信/受信ペアの 1 つを MDIX にスワップします。

長距離のフェールオーバーを使用する場合のステート リンクの遅延は、パフォーマンスを最善にするには 10 ミリ秒未満でなければならず、250 ミリ秒を超えないようにする必要がありま

す。遅延が10ミリ秒を上回る場合、フェールオーバー メッセージの再送信によって、パフォーマンスが低下する可能性があります。

フェールオーバーの中断の回避とデータ リンク

すべてのインターフェイスで同時に障害が発生する可能性を減らすために、フェールオーバー リンクとデータ インターフェイスは異なるパスを通すことを推奨します。フェールオーバー リンクがダウンした場合、フェールオーバーが必要かどうかの決定に、Firepower Threat Defense デバイスはデータインターフェイスを使用できます。その後、フェールオーバー動作は、フェールオーバー リンクのヘルスが復元されるまで停止されます。

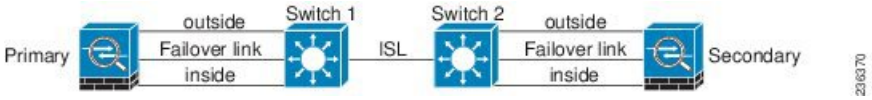
耐障害性のあるフェールオーバー ネットワークの設計については、次の接続シナリオを参照してください。

シナリオ 1：非推奨

2 つの Firepower Threat Defense デバイス間のフェールオーバーとデータ インターフェイスの両方を接続するために1つのスイッチまたは一連のスイッチを使用している場合、スイッチまたはスイッチ間リンクがダウンしていると、両方の Firepower Threat Defense デバイスがアクティブになります。したがって、次の図で示されている 2 つの接続方式は推奨**しません**。

図 *14 :* 単一のスイッチを使用した接続：非推奨

図 *15 : 2* つのスイッチを使用した接続：非推奨



シナリオ 2：推奨

フェールオーバー リンクには、データ インターフェイスと同じスイッチを使用しないことを推奨します。代わりに、次の図に示すように、別のスイッチを使用するか直接ケーブルを使用して、フェールオーバー リンクを接続します。

図 *16 :* 異なるスイッチを使用した接続

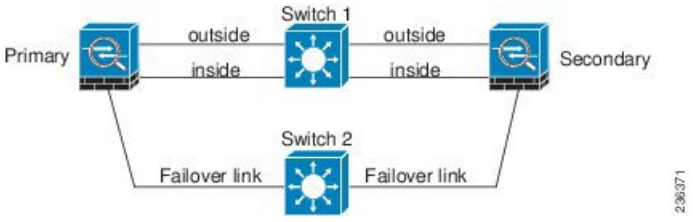
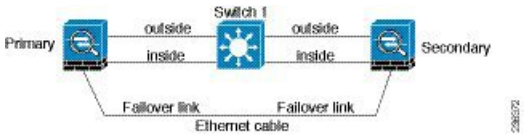


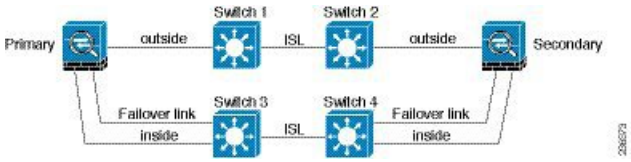
図 *17* : ケーブルを使用した接続



シナリオ 3：推奨

Firepower Threat Defense データ インターフェイスが複数セットのスイッチに接続されている場合、フェールオーバー リンクはいずれかのスイッチに接続できます。できれば、次の図に示すように、ネットワークのセキュアな側（内側）のスイッチに接続します。

図 *18* : セキュア スイッチを使用した接続



シナリオ 4：推奨

最も信頼性の高いフェールオーバー構成では、次の図に示すように、フェールオーバー リンクに冗長インターフェイスを使用します。

図 *19* : 冗長インターフェイスを使用した接続

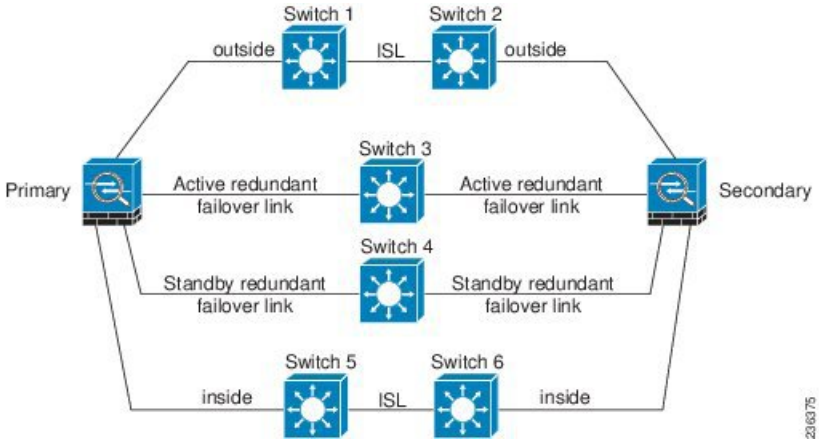
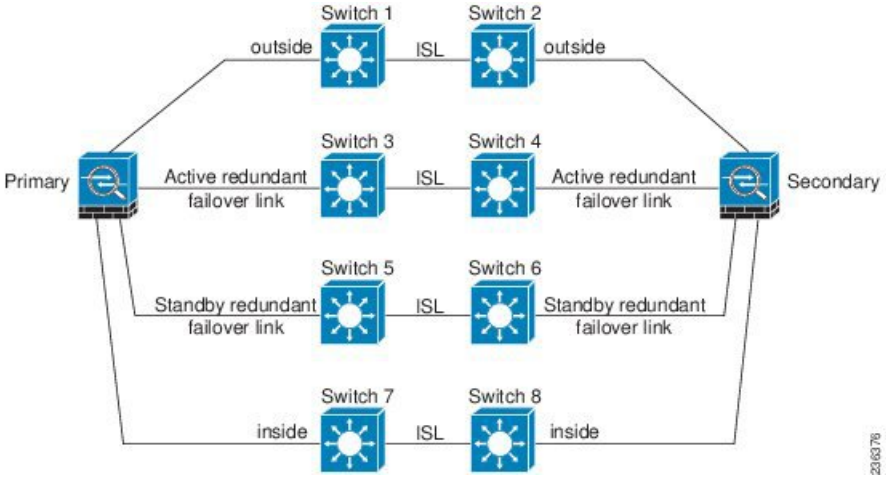


図 *20 : Inter-Switch Link*（*ISL*）を使用した接続



高可用性 の MAC アドレスと IP アドレス

インターフェイスを設定する場合、同じネットワーク上のアクティブ IP アドレスとスタンバイ IP アドレスを指定できます。一般的に、フェールオーバーが発生した場合、新しいアクティブ装置がアクティブな IP アドレスと MAC アドレスを引き継ぎます。ネットワーク デバイスは、MAC と IP アドレスの組み合わせについて変更を認識しないため、ネットワーク上のどのような場所でも ARP エントリが変更されたり、タイムアウトが生じたりすることはありません。

（注） スタンバイ アドレスを設定することが推奨されていますが、必須ではありません。スタンバイ IP アドレスがないと、アクティブ装置はスタンバイ インターフェイスの状態を確認するためのネットワーク テストを実行できません。リンク ステートのみ追跡できます。また、管理目的でそのインターフェイスのスタンバイ装置に接続することもできません。

ステート リンク用の IP アドレスおよび MAC アドレスは、フェールオーバー実行後も変更されません。

アクティブ/スタンバイ IP アドレスと MAC アドレス

アクティブ/スタンバイ 高可用性 の場合、フェールオーバー イベント中の IP アドレスと MAC アドレスの使用については、次を参照してください。

1. アクティブ装置は常にプライマリ装置の IP アドレスと MAC アドレスを使用します。
2. アクティブ装置が故障すると、スタンバイ装置は故障した装置の IP アドレスと MAC アドレスを引き継ぎ、トラフィックを通過させます。
3. 故障した装置がオンラインに復帰すると、スタンバイ状態となり、スタンバイ IP アドレスと MAC アドレスを引き継ぎます。

ただし、セカンダリ装置がプライマリ装置を検出せずにブートした場合、セカンダリ装置がアクティブ装置になります。プライマリ装置の MAC アドレスを認識していないため、自分の MACアドレスを使用します。プライマリ装置が使用可能になると、セカンダリ（アクティブ）装置は MAC アドレスをプライマリ装置の MAC アドレスに変更します。これによって、ネットワーク トラフィックが中断されることがあります。同様に、プライマリ装置を新しいハードウェアと交換すると、新しい MAC アドレスが使用されます。

仮想 MAC アドレスがこの中断を防ぎます。なぜなら、アクティブ MAC アドレスは起動時にセカンダリ装置によって認識され、プライマリ装置のハードウェアが新しくなっても変わらないからです。仮想MACアドレスを設定しなかった場合、トラフィック フローを復元するために、接続されたルータの ARP テーブルをクリアする必要がある場合があります。Firepower Threat Defense デバイス は MAC アドレスを変更するときに、スタティック NAT アドレスに対して Gratuitous ARP を送信しません。そのため、接続されたルータはこれらのアドレスの MAC アドレスの変更を認識できません。

仮想 MAC アドレス

Firepower Threat Defense デバイス には、仮想 MAC アドレスを設定する複数の方法があります。1 つの方法のみ使用することをお勧めします。複数の方法を使用して MAC アドレスを設定した場合は、どの MAC アドレスが使用されるかは多くの可変要素によって決まるため、予測できないことがあります。

マルチインスタンス機能では、FXOS シャーシがすべてのインターフェイスのプライマリ MAC アドレスのみを自動生成します。プライマリおよびセカンダリ MAC アドレスの両方で、生成された MAC アドレスを仮想 MAC アドレスで上書きすることができますが、セカンダリ MAC アドレスを事前に定義することは必須ではありません。セカンダリ MAC アドレスを設定すると、セカンダリ装置のハードウェアが新しい場合に、to-the-box 管理トラフィックが中断されないようになります。

Stateful Failover

、ステートフェールオーバー中にアクティブ装置は接続ごとのステート情報をスタンバイ装置に継続的に渡します。。フェールオーバーの発生後も、新しいアクティブ装置で同じ接続情報が利用できます。サポートされているエンドユーザのアプリケーションでは、同じ通信セッションを保持するために再接続する必要はありません。

サポートされる機能

ステートフル フェールオーバーでは、次のステート情報がスタンバイ Firepower Threat Defense デバイスに渡されます。

- NAT 変換テーブル
- TCP 接続と UDP 接続、および HTTP 接続状態を含む状態。他のタイプの IP プロトコルおよびICMP は、新しいパケットが到着したときに新しいアクティブユニットで確立されるため、アクティブ装置によって解析されません。

- 厳密な TCP 強制を含む、Snort の接続状態、インスペクション結果、およびピンホール情報。
- ARP テーブル
- レイヤ 2 ブリッジ テーブル（ブリッジ グループ用）
- ISAKMP および IPSec SA テーブル
- GTP PDP 接続データベース
- SIP シグナリング セッションとピンホール。
- スタティックおよびダイナミック ルーティング テーブル：ステートフル フェールオーバーはダイナミック ルーティング プロトコル（OSPF や EIGRP など）に参加するため、アクティブ装置上のダイナミック ルーティング プロトコルによる学習ルートが、スタンバイ装置のルーティング情報ベース（RIB）テーブルに維持されます。フェールオーバーイベントで、アクティブなセカンダリ ユニットには最初にプライマリ ユニットをミラーリングするルールがあるため、パケットは通常は最小限の中断でトラフィックに移動します。フェールオーバーの直後に、新しくアクティブになった装置で再コンバージェンス タイマーが開始されます。次に、RIB テーブルのエポック番号が増加します。再コンバージェンス中に、OSPF および EIGRP ルートは新しいエポック番号で更新されます。タイマーが期限切れになると、失効したルート エントリ（エポック番号によって決定される）はテーブルから削除されます。これで、RIB には新しくアクティブになった装置での最新のルーティング プロトコル転送情報が含まれています。

  （注） ルートは、アクティブ装置上のリンクアップまたはリンクダウン イベントの場合のみ同期されます。スタンバイ装置上でリンクがアップまたはダウンすると、アクティブ装置から送信されたダイナミック ルートが失われることがあります。これは正常な予期された動作です。

- DHCP サーバ：DHCP アドレス リースは複製されません。ただし、インターフェイスで設定された DHCP サーバは、DHCP クライアントにアドレスを付与する前にアドレスが使用されていないことを確認するために ping を送信するため、サービスに影響はありません。ステート情報は、DHCP リレーまたは DDNS とは関連性がありません。
- アクセス コントロール ポリシーの判断：フェールオーバー時には、トラフィックの照合（URL、URL カテゴリ、地理位置情報など）、侵入検知、マルウェア、ファイル タイプに関する判断が保持されます。ただし、フェールオーバーの時点で評価される接続には、次のような注意事項があります。
  - AVC：App-ID 判定は複製されますが、検出状態は複製されません。フェールオーバーが発生する前に、App-ID 判定が完了および同期されていれば、正常に同期は行われます。
  - 侵入検知状態：フェールオーバーの際、フロー中にピックアップが発生すると、新しいインスペクションは完了しますが、古い状態は失われます。

- ファイル マルウェア ブロッキング：ファイルの処分は、フェールオーバー前にできるようになる必要があります。
- ファイル タイプ検出とブロッキング：ファイル タイプは、フェールオーバー前に特定される必要があります。元のアクティブ デバイスでファイルを特定している間にフェールオーバーが発生すると、ファイル タイプの同期は失われます。ファイル ポリシーでそのファイル タイプがブロックされている場合でも、新しいアクティブ デバイスはファイルをダウンロードします。

- ユーザ エージェントと ISE セッション ディレクトリを介してパッシブに収集されたユーザと IP アドレスのマッピングを含むアイデンティティ ポリシーや、キャプティブ ポータルを介したアクティブ認証の、ユーザ識別の判断。フェールオーバーの時点でアクティブ認証していたユーザには、再度認証を求めるプロンプトが表示されることがあります。
- ネットワーク AMP：クラウド ルックアップは各デバイスから独立しているため、一般的に、フェールオーバーはこの機能には影響しません。具体的には次のとおりです。
  - 署名ルックアップ：ファイルの送信中にフェールオーバーが発生した場合、ファイル イベントは生成されず、検出も発生しません。
  - ファイル ストレージ：ファイルの保存中にフェールオーバーが発生した場合、元のアクティブ デバイスに保存されます。ファイルの保存中に元のアクティブなデバイスがダウンした場合、ファイルは保存されません。
  - ファイルの事前分類（ローカル分析）：事前分類中にフェールオーバーが発生した場合、検出は失敗します。
  - ファイル ダイナミック分析（クラウドとの接続性）：フェールオーバーが発生しても、システムはクラウドにファイルを提出できます。
  - アーカイブ ファイル サポート：分析中にフェールオーバーが発生した場合、システムはファイル/アーカイブ内の可視性を失います。
  - カスタム ブラックリスト：フェールオーバーが発生した場合、イベントは生成されません。
- セキュリティ インテリジェンス判断。ただし、フェールオーバーの時点で処理されていた DNS ベースの判断は完了しません。
- RA VPN：リモート アクセス VPN エンド ユーザは、フェールオーバー後に VPN セッションを再認証または再接続する必要はありません。ただし、VPN 接続上で動作するアプリケーションは、フェールオーバー プロセス中にパケットを失って、パケット損失から回復できない可能性があります。

サポートされない機能

ステートフル フェールオーバーでは、次のステート情報はスタンバイ Firepower Threat Defense デバイスに渡されません。

- GREやIP-in-IPなどのプレーンテキストトンネル内のセッション。トンネル内のセッションは複製されず、新しいアクティブノードは、既存のインスペクションの判定を再利用して、正しいポリシー ルールを照合することができません。
- SSL復号ポリシーにより復号された接続：復号状態は同期されず、現在の復号された接続はリセットされ、ブロックされます。新しい接続が適切に機能します。（復号しないルールと一致する）復号されない接続は影響を受けず、他の TCP 接続と同様に正しく複製されます。
- TCP ステート バイパス接続
- マルチキャスト ルーティング。

ハイ アベイラビリティのためのブリッジ グループの要件

ブリッジ グループを使用する場合は、ハイ アベイラビリティに関して特別な考慮事項があります。

アクティブ装置がスタンバイ装置にフェールオーバーするときに、スパニング ツリー プロトコル（STP）を実行しているスイッチ ポートは、トポロジ変更を検出すると 30 ～ 50 秒間ブロッキング状態に移行できます。ポートがブロッキング状態の間のブリッジ グループ メンバーインターフェイスでのトラフィックの損失を回避するために、次の回避策のいずれかを設定できます。

- アクセス モードのスイッチ ポート：スイッチで STP PortFast 機能を有効にします。

```
interface interface_id
  spanning-tree portfast
```

PortFast機能を設定すると、リンクアップと同時にポートがSTPフォワーディング モードに遷移します。ポートは引き続きSTPに参加しています。したがって、ポートがループの一部になる場合、最終的にはSTP ブロッキング モードに遷移します。

- スイッチ ポートがトランク モードになっている場合、またはSTP PortFast を有効にできない場合は、フェールオーバー機能またはSTPの安定性に影響を与える、次のあまり望ましくない回避策のいずれかを使用できます。
  - ブリッジ グループおよびメンバー インターフェイスでインターフェイス モニタリングを無効にします。
  - フェールオーバー基準のインターフェイス保留時間を、ユニットがフェールオーバーする前に STP が収束できる大きな値に増やします。
  - スイッチのSTPタイマーを短くして、STPがインターフェイス保留時間よりも早く収束できるようにします。

フェールオーバーのヘルス モニタ

Firepower Threat Defense デバイスは、各装置について全体的なヘルスおよびインターフェイス ヘルスをモニタします。この項では、各装置の状態を判断するために、Firepower Threat Defense デバイスがテストを実行する方法について説明します。

ユニットのヘルス モニタリング

Firepower Threat Defenseデバイスは、helloメッセージでフェールオーバー リンクをモニタして相手装置のヘルスを判断します。フェールオーバー リンクで 3 回連続して hello メッセージを受信しなかったときは、フェールオーバー リンクを含む各データインターフェイスでLANTEST メッセージを送信し、ピアが応答するかどうかを確認します。Firepower Threat Defense デバイスが行うアクションは、相手装置からの応答によって決まります。次の可能なアクションを参照してください。

- Firepower Threat Defenseデバイスがフェールオーバー リンクで応答を受信した場合、フェールオーバーは行われません。
- Firepower Threat Defenseデバイスがフェールオーバー リンクで応答を受信せず、データ インターフェイスで応答を受信した場合、装置のフェールオーバーは行われません。フェールオーバー リンクが故障とマークされます。フェールオーバー リンクがダウンしている間、装置はスタンバイ装置にフェールオーバーできないため、できるだけ早くフェールオーバー リンクを復元する必要があります。
- Firepower Threat Defenseデバイスがどのインターフェイスでも応答を受信しなかった場合、スタンバイ装置がアクティブ モードに切り替わり、相手装置を故障に分類します。

インターフェイス モニタリング

ユニットは、モニタ対象のインターフェイス上で 15 秒間 hello メッセージを受信しなかった場合に、インターフェイステストを実行します。1 つのインターフェイスに対するインターフェイステストのいずれかが失敗したものの、他のユニット上のこの同じインターフェイスが正常にトラフィックを渡し続けている場合は、そのインターフェイスに障害があるものと見なされ、デバイスはテストの実行を停止します。

障害が発生したインターフェイスの数に対して定義したしきい値が満たされ（**[デバイス（Devices）] > [デバイス管理（Device Management）] > [ハイアベイラビリティ（High Availability）] > [フェールオーバートリガー条件（Failover Trigger Criteria）]** を参照）、さらに、アクティブユニットでスタンバイ装置よりも多くの障害が発生した場合は、フェールオーバーが発生します。両方のユニット上のインターフェイスに障害が発生した場合は、両方のインターフェイスが「未知」状態になり、フェールオーバー インターフェイス ポリシーで定義されているフェールオーバー限界値に向けてのカウントは行われません。

インターフェイスは、何らかのトラフィックを受信すると、再度動作状態になります。故障した デバイスは、インターフェイス障害しきい値が満たされなくなった場合、スタンバイ モードに戻ります。

インターフェイスに IPv4 および IPv6 アドレスが設定されている場合、デバイスは IPv4 を使用してヘルス モニタリングを実行します。インターフェイスに IPv6 アドレスだけが設定されている場合、デバイスは ARP ではなく IPv6 ネイバー探索を使用してヘルス モニタリング テストを実行します。ブロードキャスト ping テストの場合、デバイスは IPv6 全ノード アドレス（FE02::1）を使用します。

インターフェイス テスト

Firepower Threat Defense デバイスでは、次のインターフェイス テストが使用されます。各テストの時間は。

1. リンク アップ/ダウン テスト：インターフェイス ステータスのテストです。リンク アップ/ダウン テストでインターフェイスがダウンしていることが示された場合、デバイスは障害が発生し、テストが停止したと見なします。ステータスがアップの場合、デバイスはネットワーク アクティビティを実行します。

2. ネットワーク動作のテスト：ネットワークの受信動作のテストです。テストの開始時に、各装置はインターフェイスの受信パケット カウントをリセットします。テスト中にユニットが適切なパケットを受信すると、すぐにインターフェイスは正常に動作していると見なされます。両方の装置がトラフィックを受信した場合、テストは停止します。どちらか一方のユニットだけがトラフィックを受信している場合は、トラフィックを受信していないユニットのインターフェイスで障害が発生していると見なされ、テストは停止します。どちらのユニットもトラフィックを受信していない場合は、デバイスは ARP テストを開始します。

3. ARP テスト：ARP が正しく応答するかどうかをテストします。各ユニットは、ARP テーブル内の最新のエントリの IP アドレスに対して単一の ARP 要求を送信します。ユニットがテスト中に ARP 応答またはその他のネットワーク トラフィックを受信する場合、インターフェイスは動作していると見なされます。ユニットが ARP 応答を受信しない場合、デバイスは、ARP テーブル内の「次の」エントリの IP アドレスに対して単一の ARP 要求を送信します。ユニットがテスト中に ARP 応答またはその他のネットワーク トラフィックを受信する場合、インターフェイスは動作していると見なされます。両方のユニットがトラフィックを受信した場合、テストは停止します。どちらか一方のユニットだけがトラフィックを受信している場合は、トラフィックを受信していないユニットのインターフェイスで障害が発生していると見なされ、テストは停止します。どちらのユニットもトラフィックを受信していない場合は、デバイスはブートストラップ ping テストを開始します。

4. ブロードキャスト Ping テスト：ping 応答が正しいかどうかをテストします。各ユニットがブロードキャスト ping を送信し、受信したすべてのパケットをカウントします。パケットはテスト中にパケットを受信すると、インターフェイスは正常に動作していると見なされます。両方のユニットがトラフィックを受信した場合、テストは停止します。どちらか一方のユニットだけがトラフィックを受信している場合は、トラフィックを受信していないユニットのインターフェイスで障害が発生していると見なされ、テストは停止します。どちらのユニットもトラフィックを受信しない場合、ARP テストを使用してテストが再開されます。両方の装置が ARP およびブロードキャスト ping テストからトラフィックを受信し続けない場合、これらのテストは永久に実行し続けます。

Interface Status

モニタ対象のインターフェイスには、次のステータスがあります。

- Unknown：初期ステータスです。このステータスは、ステータスを特定できないことを意味する場合もあります。
- Normal：インターフェイスはトラフィックを受信しています。
- Normal (Waiting)：インターフェイスは起動していますが、ピア ユニットの対応するインターフェイスからまだ hello パケットを受信していません。
- Normal (Not-Monitored)：インターフェイスは動作中ですが、フェールオーバー プロセスによってモニタされていません。
- Testing：ポーリング 5 回の間、インターフェイスで hello メッセージが検出されていません。
- Link Down：インターフェイスまたは VLAN は管理のためにダウンしています。
- Link Down (Waiting)：インターフェイスまたは VLAN は管理上ダウンしており、ピア ユニットの対応するインターフェイスからまだ hello パケットを受信していません。
- Link Down (Not-Monitored)：インターフェイスまたは VLAN は管理上ダウンしていますが、フェールオーバー プロセスによってモニタされていません。
- No Link：インターフェイスの物理リンクがダウンしています。
- No Link (Waiting)：インターフェイスの物理リンクがダウンしており、ピア ユニットの対応するインターフェイスから hello パケットをまだ受信していません。
- No Link (Not-Monitored)：インターフェイスの物理リンクがダウンしていますが、フェールオーバー プロセスによってモニタされていません。
- Failed：インターフェイスではトラフィックを受信していませんが、ピア インターフェイスではトラフィックを検出しています。

フェールオーバー トリガーおよび検出タイミング

次の表に、フェールオーバー トリガー イベントと、関連する障害検出のタイミングを示します。フェールオーバーが発生した場合、フェールオーバーの理由およびその他のハイ アベイラビリティ ペアに関するさまざまな作業をメッセージ センターで表示できます。

表 *77 : Firepower Threat Defense* フェールオーバー時間

フェールオーバートリガーイベント	最小ハードウェア	デフォルト	最大
アクティブ装置で電源断が生じる、または通常の動作が停止する。	800 ミリ秒	15 秒	45 秒

フェールオーバートリガーイベント	最小ハードウェア	デフォルト	最大
アクティブ ユニット インターフェイス物理リンクがダウンする。	500 ミリ秒	5 秒	15 秒
アクティブ装置のインターフェイスは実行されているが、接続の問題によりインターフェイス テストを行っている。	5 秒	25 秒	75 秒

アクティブ/スタンバイ フェールオーバーについて

アクティブ/スタンバイ フェールオーバーでは、障害が発生した装置の機能を、スタンバイ Firepower Threat Defense デバイスに引き継ぐことができます。アクティブ装置に障害が発生した場合、スタンバイ装置がアクティブ装置になります。

プライマリ/セカンダリ ロールとアクティブ/スタンバイ ステータス

アクティブ/スタンバイ フェールオーバーを設定する場合、1 つのユニットをプライマリとして設定し、もう1つのユニットをセカンダリとして設定します。設定中に、プライマリ ユニットのポリシーは、セカンダリ ユニットに同期化されます。この時点で、2つのユニットは、デバイスおよびポリシー設定に関して単一のデバイスとして機能します。ただし、イベント、ダッシュボード、レポートおよびヘルス モニタリングに関しては、別々のデバイスとして引き続き表示されます。

フェールオーバー ペアの2つのユニットの主な相違点は、どちらのユニットがアクティブでどちらのユニットがスタンバイであるか、つまりどちらの IP アドレスを使用するか、およびどちらのユニットがアクティブにトラフィックを渡すかということに関連します。

しかし、プライマリである装置（コンフィギュレーションで指定）とセカンダリである装置との間で、いくつかの相違点があります。

- 両方の装置が同時にスタートアップした場合（さらに動作ヘルスが等しい場合）、プライマリ装置が常にアクティブ装置になります。
- プライマリ ユニットの MAC アドレスは常に、アクティブ IP アドレスと結び付けられています。このルールの例外は、セカンダリ ユニットがアクティブであり、フェールオーバー リンク経由でプライマリ ユニットの MAC アドレスを取得できない場合に発生します。この場合、セカンダリ装置の MAC アドレスが使用されます。

起動時のアクティブ装置の判別

アクティブ装置は、次の条件で判別されます。

- 装置がブートされ、ピアがすでにアクティブとして動作中であることを検出すると、その装置はスタンバイ装置になります。
- 装置がブートされてピアを検出できないと、その装置はアクティブ装置になります。
- 両方の装置が同時にブートされた場合は、プライマリ装置がアクティブ装置になり、セカンダリ装置がスタンバイ装置になります。

フェールオーバー イベント

アクティブ/スタンバイ フェールオーバーでは、フェールオーバーはユニットごとに行われます。

次の表に、各障害イベントに対するフェールオーバーアクションを示します。この表には、各フェールオーバー イベントに対して、フェールオーバー ポリシー（フェールオーバーまたはフェールオーバーなし）、アクティブ装置が行うアクション、スタンバイ装置が行うアクション、およびフェールオーバー条件とアクションに関する特別な注意事項を示します。

表 *78 :* フェールオーバー イベント

障害の状況	ポリシー（**Policy**）	アクティブグループのアクション	スタンバイグループのアクション	注記
アクティブ装置が故障（電源またはハードウェア）	フェールオーバー	n/a	アクティブになる アクティブに故障とマークする	モニタ対象インターフェイスまたはフェールオーバー リンクで hello メッセージは受信されません。
以前にアクティブであった装置の復旧	フェールオーバーなし	スタンバイになる	動作なし	なし。
スタンバイ装置が故障（電源またはハードウェア）	フェールオーバーなし	スタンバイに故障とマークする	n/a	スタンバイ装置が故障とマークされている場合、インターフェイス障害しきい値を超えても、アクティブ装置はフェールオーバーを行いません。
動作中にフェールオーバー リンクに障害が発生した	フェールオーバーなし	フェールオーバー リンクに故障とマークする	フェールオーバー リンクに故障とマークする	フェールオーバー リンクがダウンしている間、装置はスタンバイ装置にフェールオーバーできないため、できるだけ早くフェールオーバー リンクを復元する必要があります。

障害の状況	ポリシー（Policy）	アクティブグループのアクション	スタンバイグループのアクション	注記
スタートアップ時にフェールオーバーリンクに障害が発生した	フェールオーバーなし	フェールオーバーリンクに故障とマークする	アクティブになる	スタートアップ時にフェールオーバーリンクがダウンしていると、両方の装置がアクティブになります。
ステートリンクの障害	フェールオーバーなし	動作なし	動作なし	ステート情報が古くなり、フェールオーバーが発生するとセッションが終了します。
アクティブ装置におけるしきい値を超えたインターフェイス障害	フェールオーバー	アクティブに故障とマークする	アクティブになる	なし。
スタンバイ装置におけるしきい値を超えたインターフェイス障害	フェールオーバーなし	動作なし	スタンバイに故障とマークする	スタンバイ装置が故障とマークされている場合、インターフェイス障害しきい値を超えても、アクティブ装置はフェールオーバーを行いません。

高可用性のガイドライン

サポート モデル

- Firepower 9300：シャーシ内ハイ アベイラビリティはサポートされません。
- Microsoft Azure や Amazon Web Services などのパブリック クラウド ネットワーク上の Firepower Threat Defense Virtual では、レイヤ 2 接続が必要なため、高可用性はサポートされません。

その他のガイドライン

- アクティブ装置がスタンバイ装置にフェールオーバーするときに、スパニングツリープロトコル（STP）を実行している接続済みスイッチ ポートは、トポロジ変更を検出すると 30 ～ 50 秒間ブロッキング ステートに移行できます。ポートがブロッキング ステートである間のトラフィック損失を防ぐには、スイッチで STP PortFast 機能を有効にします。

  interface *interface_id* **spanning-tree portfast**

この回避策は、ルーテッド モードおよびブリッジ グループ インターフェイスの両方に接続されているスイッチに適用されます。PortFast 機能を設定すると、リンクアップと同時にポートが STP フォワーディング モードに遷移します。ポートは引き続き STP に参加しています。したがって、ポートがループの一部になる場合、最終的にはSTPブロッキングモードに遷移します。

- ローカル CA サーバが設定されている場合、フェールオーバーを有効にできません。CA コンフィギュレーションを削除するには、**no crypto ca server** コマンドを使用します。
- Firepower Threat Defense フェールオーバー ペアに接続されたスイッチ上でポート セキュリティを設定すると、フェールオーバーイベントが発生したときに通信の問題が起きることがあります。この問題は、あるセキュア ポートで設定または学習されたセキュア MAC アドレスが別のセキュア ポートに移動し、スイッチのポート セキュリティ機能によって違反フラグが付けられた場合に発生します。
- アクティブ/スタンバイ 高可用性と VPN IPsec トンネルの場合、SNMP を使用して VPN トンネル上でアクティブ ユニットとスタンバイ ユニットの両方をモニタすることはできません。スタンバイ ユニットにはアクティブ VPN トンネルがないため、NMS に向けられたトラフィックはドロップされます。代わりに暗号化付き SNMPv3 を使用すれば、IPsec トンネルが不要になります。

Firepower Threat Defense ハイ アベイラビリティ ペアの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	Firepower Threat Defense Firepower Threat Defense Virtual	いずれか（Any）	Admin/Network Admin

アクティブ/スタンバイの高可用性ペアを確立するには、一方のデバイスをプライマリ、他方をセカンダリとして指定します。システムは、マージした設定を、ペア内のデバイスに適用します。競合する場合、システムはプライマリとして指定されたデバイスの構成を適用します。

マルチドメインの導入環境では、高可用性ペアのデバイスが同じドメインに属している必要があります。

（注） ステートフル フェールオーバー リンクがピア間のアプリケーション コンテンツの同期に使用されている場合には、システムはフェールオーバーリンクを使用して構成を同期します。フェールオーバー リンクとステートフル フェールオーバー リンクはプライベート IP スペースにあり、ハイ アベイラビリティ ペアのピア間の通信にのみ使用されます。ハイ アベイラビリティが確立された後は、ハイ アベイラビリティ ペアを解除して再構成することなく、選択したインターフェイス リンクと暗号化設定を変更することはできません。

注意 Firepower Threat Defense のハイ アベイラビリティ ペアを作成または破棄すると、プライマリおよびセカンダリ デバイスの Snort プロセスが直ちに再起動され、両方のデバイスのトラフィック インスペクションが一時的に中断されます。 この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、ターゲット デバイスがトラフィックを処理する方法に応じて異なります。詳細はSnort® の再起動によるトラフィックの動作（451 ページ）を参照してください。ハイ アベイラビリティ ペアの作成を続けると、プライマリ デバイスとセカンダリ デバイスで Snort プロセスが再起動され、キャンセルすることができるという警告が表示されます。

始める前に

以下の点について両方のデバイスを確認してください。

- 同じモデルであること。
- インターフェイスの数とタイプが同じであること。
- ドメインおよびグループが同じであること。
- 通常のヘルス ステータスであり、同じソフトウェアを実行していること。
- ルーティングされているか、またはトランスペアレント モードであること。
- NTP 設定が同じであること。脅威に対する防御のための NTP 時刻同期の設定（1406 ページ）を参照してください。
- 未確定の変更がない状態で、完全に展開されていること。
- すべてのインターフェイスで DHCP または PPPoE が設定されていないこと。

（注） プライマリ デバイスで利用可能な証明書がセカンダリ デバイスに存在しない場合は、2 台の Firepower Threat Defense デバイス間でハイ アベイラビリティを構成することができます。ハイ アベイラビリティが構成されると、証明書がセカンダリ デバイス上で同期されます。

ステップ 1 Firepower Management Center へのデバイスの追加 （293 ページ） に従って、両方のデバイスを Firepower Management Center に追加します。

ステップ 2 **[Devices]** > **[Device Management]**を選択します。

ステップ 3 [追加（Add）] ドロップダウン メニューから、[高可用性の追加（Add High Availability）] を選択します。

ステップ 4 高可用性ペアの表示用の [名前（Name）] を入力してください。

ステップ 5 [デバイス タイプ（Device Type）] では、[Firepower Threat Defense] を選択します。

ステップ 6 高可用性ペアの [プライマリ ピア（Primary Peer）] デバイスを選択します。

ステップ 7 高可用性ペアの [セカンダリ ピア（Secondary Peer）] デバイスを選択します。

ステップ 8 [続行（Continue）] をクリックします。

ステップ 9 LAN フェールオーバー リンクでは、フェールオーバーの通信のための十分な帯域幅の [インターフェイス（Interface）] を選択します。

（注） 論理名がなくセキュリティ ゾーンに属さないインターフェイスのみが、[ハイ アベイラビリティ ペアの追加（Add High Availability Pair）] ダイアログの [インターフェイス（Interface）] ドロップダウンに一覧表示されます。

ステップ 10 識別するための任意の [論理名（Logical Name）] を入力します。

ステップ 11 アクティブなユニットの、フェールオーバー リンクの [プライマリ IP（Primary IP）] アドレスを指定します。このアドレスは、未使用のサブネット上になければなりません。

（注） 169.254.0.0/16 および fd00:0:0:*::/64 は内部で使用されるサブネットです。フェイルオーバーやステート リンクにはこれらを使用できません。

ステップ 12 必要に応じて、[IPv6 アドレスを使用（Use IPv6 Address）] を選択します。

ステップ 13 スタンバイ ユニットのフェールオーバー リンクの [セカンダリ IP（Secondary IP）] アドレスを指定します。この IP アドレスはプライマリ IP アドレスのように、同じサブネット内になければなりません。

ステップ 14 IPv4 アドレスを使用する場合、プライマリとセカンダリの IP アドレス両方に適用されるサブネットマスクを入力します。

ステップ 15 必要に応じて、ステートフル フェールオーバー リンクでは、同じインターフェイスを選択するか、または別のインターフェイスを選択し、高可用性の設定情報を入力します。

（注） 169.254.0.0/16 および fd00:0:0:*::/64 は内部で使用されるサブネットです。フェイルオーバーやステート リンクにはこれらを使用できません。

ステップ 16 必要に応じて、フェールオーバー リンク間の IPsec 暗号化について、[有効（Enabled）] を選択し、さらに [キー生成（key generate）] メソッドを選択します。

ステップ 17 [OK] をクリックします。システム データの同期が行われるため、このプロセスが完了するまでに数分かかります。

次のタスク

デバイスがバックアップされていることを確認します。バックアップは、障害が発生したデバイスを迅速に交換するため、Firepower Management Center からリンク解除せずにハイ アベイラ

ビリティ サービスを回復するために使用できます。デバイスのバックアップ手順については、デバイスのリモートバックアップ （207 ページ）を参照してください。

オプションの高可用性パラメータの設定

最初の高可用性構成を Firepower Management Center で確認できます。高可用性ペアを解除して再設定しないと、これらの設定を編集することはできません。

フェールオーバーの結果を改善するために、フェールオーバー トリガー条件を編集できます。インターフェイス モニタリングでは、どのインタフェースがフェイルオーバーに適しているかを判断できます。

スタンバイ IP アドレスとインターフェイス モニタリングの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	Firepower Threat Defense Firepower Threat Defense Virtual	いずれか（Any）	Admin/Network Admin

各インターフェイスにスタンバイ IP アドレスを設定します。スタンバイ アドレスを設定することが推奨されていますが、必須ではありません。スタンバイ IP アドレスがないと、アクティブ装置はスタンバイ インターフェイスの状態を確認するためのネットワーク テストを実行できません。リンク ステートのみ追跡できます。

デフォルトでは、論理名が設定されているすべての物理インターフェイスでモニタリングが有効になっています。重要度の低いネットワークに接続されているインターフェイスがフェールオーバー ポリシーに影響を与えないようにできます。

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 編集するデバイス ハイ アベイラビリティ ペアの横にある [Edit] アイコン（✎） をクリックします。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [High Availability] タブをクリックします

ステップ 4 [モニタ対象インターフェイス（Monitored Interfaces）] エリアで、編集するインターフェイスの横にある [Edit] アイコン（✎） をクリックします。

ステップ 5 [このインターフェイスの障害をモニタする（Monitor this interface for failures）] チェック ボックスをオンにします。

ステップ 6 [IPv4] タブで、[スタンバイ IP アドレス（Standby IP Address）] を入力します。

このアドレスは、アクティブ IP アドレスと同じネットワーク上のフリーアドレスである必要があります。

ステップ 7 IPv6 アドレスを手動で設定した場合、[IPv6] タブでアクティブ IP アドレスの横にある [Edit] アイコン（✎）をクリックして、[スタンバイ IP アドレス（Standby IP Address）] を入力し、[OK] をクリックします。

このアドレスは、アクティブ IP アドレスと同じネットワーク上のフリーアドレスである必要があります。自動生成 [EUI 64 の適用（Enforce EUI 64）] アドレスの場合、スタンバイ アドレスは自動的に生成されます。

ステップ 8 [OK] をクリックします。

ハイ アベイラビリティ フェールオーバー条件の編集

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	Firepower Threat Defense Firepower Threat Defense Virtual	いずれか（Any）	Admin/Network Admin

ネットワーク配置に基づいてフェールオーバー条件をカスタマイズできます。

ステップ 1 **[Devices]** > **[Device Management]** を選択します。

ステップ 2 編集するデバイス ハイ アベイラビリティ ペアの横にある [Edit] アイコン（✎） をクリックします。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [ハイアベイラビリティ（High Availability）] を選択します。

ステップ 4 [フェールオーバートリガー条件（Failover Trigger Criteria）] の横にある [Edit] アイコン（✎） をクリックします。

ステップ 5 [インターフェイス障害しきい値（Interface Failure Threshold）] で、デバイスがフェールオーバーする条件となるインターフェイスの失敗の数または割合を選択します。

ステップ 6 [hello パケット間隔（Hello packet Intervals）] で、フェールオーバー リンクを介して送信される hello パケットの頻度を選択します。

（注） Firepower 2100 でリモートアクセス VPN を使用する場合は、デフォルトの hello パケット間隔を使用します。使用しない場合は、CPU 使用率が高くなる場合があり、フェールオーバーを発生させる可能性があります。

ステップ 7 [OK] をクリックします。

仮想 MAC アドレスの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	Firepower Threat Defense Firepower Threat Defense Virtual	いずれか（Any）	Admin/Network Admin

フェールオーバーのため、以下の Firepower Management Centerの 2 か所にアクティブ MAC アドレスとスタンバイ MAC アドレスを設定できます。

- [インターフェイスの編集（Edit Interface）] ページの [詳細（Advanced）] タブ。MAC アドレスの設定 （833 ページ） を参照してください。
- [高可用性（High Availability）] ページからアクセスする [インターフェイス MAC アドレスの追加（Add Interface MAC Address）] ページ。次を参照してください。

アクティブ MAC アドレスとスタンバイ MAC アドレスが両方の場所で設定されている場合、フェールオーバーではインターフェイスの設定で定義されたアドレスが優先されます。

物理インターフェイスにアクティブ MAC アドレスとスタンバイ MAC アドレスを指定することでフェールオーバー中のトラフィック喪失を最低に抑えることができます。この機能は、フェールオーバーのための IP アドレスのマッピングに冗長性を提供します。

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 編集するデバイス ハイ アベイラビリティ ペアの横にある編集アイコン（  ）をクリックします。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [ハイ アベイラビリティ（High Availability）] を選択します。

ステップ 4 インターフェイス MAC アドレスの横にある追加アイコン（）を選択します。

ステップ 5 [物理インターフェイス（Physical Interface）] を選択します。

ステップ 6 [アクティブインターフェイス MAC アドレス（Active Interface Mac Address）] を入力します。

ステップ 7 [スタンバイインターフェイス MAC アドレス（Standby Interface Mac Address）] を入力します。

ステップ 8 [OK] をクリックします。

高可用性 の管理

この項では、高可用性の設定を変更する方法、ある装置から別の装置にフェールオーバーを強制実行する方法など、高可用性をイネーブルにした後に高可用性装置を管理する方法について説明します。

Firepower Threat Defense ハイ アベイラビリティ ペアにおけるアクティブ ピアの切り替え

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	Firepower Threat Defense Firepower Threat Defense Virtual	いずれか（Any）	Admin/Network Admin

Firepower Threat Defense ハイ アベイラビリティ ペアを確立した後、アクティブ ユニットとスタンバイ ユニットを手動で切り替えることができます。そうすることで、現在のアクティブ ユニットにおける持続的な障害やヘルス イベントなどに起因するフェールオーバーを効果的に実施できます。この手順を実行する前に、両方のユニットを完全に展開しておく必要があります。

始める前に

Firepower Threat Defense ハイ アベイラビリティ ペアにおけるノード ステータスの更新 （898 ページ）

（注） これにより、Firepower Threat Defense ハイ アベイラビリティ デバイス ペアのステータスと Firepower Management Center のステータスが同期されます。

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 アクティブピアを変更するハイ アベイラビリティ ペアの横にあるアクティブ ピア切り替えアイコン（  ）をクリックします。

ステップ 3 次の操作を実行できます。

- ハイ アベイラビリティ ペアでスタンバイ デバイスをアクティブ デバイスにすぐに切り替える場合は、[はい（Yes）] をクリックします。

- キャンセルして [デバイス管理（Device Management）] ページに戻る場合は、[いいえ（No）] をクリックします。

Firepower Threat Defense ハイ アベイラビリティ ペアにおけるノード ステータスの更新

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	Firepower Threat Defense Firepower Threat Defense Virtual	いずれか（Any）	Admin/Network Admin

ハイ アベイラビリティ ペアのアクティブ デバイスまたはスタンバイ デバイスが再起動されると、Firepower Management Center はどちらのデバイスでも正確なハイ アベイラビリティ ステータスを表示しない場合があります。これは、Firepower Threat Defense が再起動すると、高可用性ステータスが Firepower Threat Defense 上で直ちに更新され、対応するイベントが Firepower Management Center に送信されるためです。ただし、Firepower Threat Defense と Firepower Management Center 間の通信がまだ確立されていないため、ステータスが Firepower Management Center で更新されないことがあります。

Firepower Management Center と Firepower Threat Defense のデバイスとの間で通信障害が発生したり、通信チャネルが不安定になったりすると、データの同期が失われる可能性があります。ハイ アベイラビリティ ペアのアクティブ デバイスとスタンバイ デバイスを切り替えると、かなりの時間が経過しても変更が Firepower Management Center に反映されないことがあります。

これらのシナリオでは、ハイ アベイラビリティ ノードのステータスを更新して、ハイ アベイラビリティ ペアのアクティブ デバイスとスタンバイ デバイスに関する正確な情報を取得できます。

（注） ノードの更新操作は、Firepower Management Center バージョン 6.2.3 以降で管理されている Firepower Threat Defense の高可用性デバイスでのみ可能です。

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 ノード ステータスを更新するハイ アベイラビリティ ペアの横にある [HA ノードのステータス更新（Refresh HA Node Status）] アイコン（）をクリックします。

ステップ 3 次の操作を実行できます。

- ハイ アベイラビリティ ペアのノード ステータスを更新する場合は、[はい（Yes）] をクリックします。

- キャンセルして[デバイス管理（Device Management）]ページに戻る場合は、[いいえ（No）]をクリックします。

ハイ アベイラビリティの中断と再開

ハイ アベイラビリティ ペアの 1 つのユニットを中断できます。これは、次の場合に役立ちます。

- 両方のユニットがアクティブ-アクティブの状況で、フェールオーバー リンクでの通信を修復しても、問題が解決されない場合。
- アクティブユニットまたはスタンバイユニットをトラブルシューティングする間、ユニットのフェールオーバーを発生させたくない場合。

ハイ アベイラビリティを中断すると、デバイスのペアがフェールオーバー ユニットとして動作しなくなります。現在アクティブなデバイスはアクティブなままで、すべてのユーザ接続を処理します。ただし、フェールオーバー基準はモニタされなくなり、システムにより現在の擬似-スタンバイ デバイスにフェールオーバーされることはなくなります。スタンバイ デバイスの設定は保持されますが、非アクティブのままです。

HA の中断と HA の破棄の主な違いは、中断された HA デバイスではハイ アベイラビリティ設定が保持されることです。HA を破棄すると、この設定は消去されます。そのため、中断されたシステムで HA を再開するためのオプションがあります。これにより、既存の設定が有効になり、2 台のデバイスがフェールオーバー ペアとして再び機能します。

HA を一時停止するには、 **configure high-availability suspend** コマンドを使用します。

```
> configure high-availability suspend
Please ensure that no deployment operation is in progress before suspending
high-availability.
Please enter 'YES' to continue if there is no deployment operation in
progress and 'NO' if you wish to abort: YES
Successfully suspended high-availability.
```

アクティブ装置からハイ アベイラビリティを中断すると、アクティブ装置とスタンバイ装置の両方で設定が中断されます。スタンバイ装置から中断すると、スタンバイ装置でのみ中断されますが、アクティブ装置は中断されたユニットへのフェールオーバーを試みなくなります。

フェールオーバーを再開するには、**configure high-availability resume** コマンドを使用します。

```
> configure high-availability resume
Successfully resumed high-availablity.
```

ユニットが中断状態の場合にのみ、ユニットを再開できます。ユニットは、ピア ユニットとアクティブ/スタンバイ ステータスをネゴシエートします。

（注） ハイ アベイラビリティの中断は一時的な状態です。ユニットをリロードすると、ハイ アベイラビリティ設定が自動的に再開され、ピアとアクティブ/スタンバイ ステータスがネゴシエートされます。

ハイ アベイラビリティ ペアでのユニット交換

次のいずれかの手順を使用すると、ハイ アベイラビリティ ペアで障害が発生したまたは修復済みの Firepower Threat Defense デバイスを交換できます。

- 障害が発生したデバイスのバックアップが利用可能な場合は、バックアップからの FTD の復元：高可用性 （223 ページ）の手順を実行するとデバイスを正常に交換できます。

  （注） 障害が発生した Firepower Threat Defense デバイスを Firepower Management Center から登録解除しないでください。復元手順では、トラフィックを損失せずに Firepower Management Center の設定と接続の復元を行います。

- デバイスのバックアップが利用不可の場合は、Firepower Management Center でデバイスを管理不能にし、デバイスを交換してから、ハイ アベイラビリティ ペアを再確立する必要があります。そのため、Firepower Threat Defense のハイ アベイラビリティを中断して再作成する必要があります。その結果、トラフィックが失われることがあります。詳細な手順については、バックアップなしでのユニット交換 （900 ページ）を参照してください。

バックアップなしでのユニット交換

バックアップをしていない Firepower Threat Defense のハイ アベイラビリティ ペアにおいて故障したユニットを交換する必要がある場合、[ブレークを強制（Force Break）] オプション選択して、このペアを分離する必要があります。ユニットを交換するか、修理した後、Firepower Management Center のデバイスを登録し、高可用性を再度確立する必要があります。このプロセスは、デバイスがプライマリ、セカンダリであるかによって異なります。

プライマリ ユニットの交換

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	Firepower Threat Defense Firepower Threat Defense Virtual	いずれか（Any）	Admin/Network Admin

次に示す手順に従って、Firepower Threat Defense の高可用性ペアで障害が発生したプライマリ ユニットを交換します。ここに示した手順に従わないと、既存の高可用性設定を上書きする可能性があります。

注意 Firepower Threat Defense のハイ アベイラビリティ ペアを作成または破棄すると、プライマリおよびセカンダリ デバイスの Snort プロセスが直ちに再起動され、両方のデバイスのトラフィック インスペクションが一時的に中断されます。 この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、ターゲット デバイスがトラフィックを処理する方法に応じて異なります。詳細はSnort® の再起動によるトラフィックの動作 （451 ページ）を参照してください。ハイ アベイラビリティ ペアの作成を続けると、プライマリ デバイスとセカンダリ デバイスで Snort プロセスが再起動され、キャンセルすることができるという警告が表示されます。

ステップ 1 [強制切断（Force Break）] を選択して、高可用性ペアを分離します。ハイ アベイラビリティ ペアにおけるユニットの分離 （902 ページ）を参照してください。

（注） 切断操作により、Firepower Threat Defense と Firepower Management Center から HA に関連するすべての設定を削除し、後で手動で再作成する必要があります。同じ HA ペアを正常に設定するには、HA 切断操作を実行する前に、すべてのインターフェイス/サブインターフェイスの IP、MAC アドレス、およびモニタリング設定を保存してください。

ステップ 2 障害が発生したプライマリ Firepower Threat Defense デバイスの登録を Firepower Management Center から解除します。Firepower Management Center からのデバイスの削除 （295 ページ）を参照してください。

ステップ 3 交換した Firepower Threat Defense を Firepower Management Center に登録します。Firepower Management Center へのデバイスの追加 （293 ページ）を参照してください。

ステップ 4 登録時には、既存のセカンダリ/アクティブ ユニットをプライマリ デバイスとして使用し、交換したデバイスをセカンダリ/スタンバイ デバイスとして使用して、高可用性を設定します。Firepower Threat Defense ハイ アベイラビリティ ペアの追加 （891 ページ）を参照してください。

セカンダリ ユニットの交換

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	Firepower Threat Defense Firepower Threat Defense Virtual	いずれか（Any）	Admin/Network Admin

次に示す手順に従って、Firepower Threat Defense の高可用性ペアで障害が発生したセカンダリ ユニットを交換します。

⚠

注意 Firepower Threat Defense のハイ アベイラビリティ ペアを作成または破棄すると、プライマリおよびセカンダリ デバイスの Snort プロセスが直ちに再起動され、両方のデバイスのトラフィック インスペクションが一時的に中断されます。 この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、ターゲット デバイスがトラフィックを処理する方法に応じて異なります。詳細はSnort® の再起動によるトラフィックの動作（451 ページ）を参照してください。ハイ アベイラビリティ ペアの作成を続けると、プライマリ デバイスとセカンダリ デバイスで Snort プロセスが再起動され、キャンセルすることができるという警告が表示されます。

ステップ 1 [強制切断（Force Break）] を選択して、高可用性ペアを分離します。ハイ アベイラビリティ ペアにおけるユニットの分離 （902 ページ）を参照してください。

（注） 切断操作により、Firepower Threat Defense と Firepower Management Center から HA に関連するすべての設定を削除し、後で手動で再作成する必要があります。同じ HA ペアを正常に設定するには、HA 切断操作を実行する前に、すべてのインターフェイス/サブインターフェイスの IP、MAC アドレス、およびモニタリング設定を保存してください。

ステップ 2 セカンダリ Firepower Threat Defense デバイスの登録を Firepower Management Center から解除します。Firepower Management Center からのデバイスの削除 （295 ページ）を参照してください。

ステップ 3 交換した Firepower Threat Defense を Firepower Management Center に登録します。Firepower Management Center へのデバイスの追加 （293 ページ）を参照してください。

ステップ 4 登録時には、既存のプライマリ/アクティブ ユニットをプライマリ デバイスとして使用し、交換したデバイスをセカンダリ/スタンバイ デバイスとして使用して、高可用性を設定します。Firepower Threat Defense ハイ アベイラビリティ ペアの追加 （891 ページ）を参照してください。

ハイ アベイラビリティ ペアにおけるユニットの分離

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	Firepower Threat Defense Firepower Threat Defense Virtual	いずれか（Any）	Admin/Network Admin

ハイ アベイラビリティ ペアを分断しても、アクティブ デバイスは完全な展開の機能を維持します。スタンバイ デバイスは、フェールオーバー設定とインターフェイス設定を失って、スタンドアロンのデバイスになります。

分断操作前のアクティブデバイスに展開されていなかったポリシーは、分断操作完了後も展開されません。分断操作完了後、スタンドアロン デバイスにポリシーを展開します。

ヒント　この例外は、flex-config ポリシーです。アクティブなデバイスに展開されている flex-config ポリシーでは、HA の中断操作後に展開の失敗を表示する場合があります。flex-config ポリシーを変更してアクティブなデバイス上に再展開する必要があります。

（注）　Firepower Management Center を使用して高可用性ペアにアクセスできない場合は、CLI コマンド **configure high-availability disable** を使用して、両方のデバイスからフェールオーバー設定を削除します。

始める前に

Firepower Threat Defense ハイ アベイラビリティ ペアにおけるノード ステータスの更新 （898 ページ）

（注）　これにより、Firepower Threat Defense ハイ アベイラビリティ デバイス ペアのステータスと Firepower Management Center のステータスが同期されます。

ステップ 1　**[Devices]** > **[Device Management]**を選択します。

ステップ 2　分断する高可用性ペアの横にある HA の分断アイコン（）をクリックします。

ステップ 3　必要に応じて、スタンバイ ピアが応答しなかった場合に、強制的に分断するためのチェックボックスをオンにします。

ステップ 4　[Yes] をクリックします。デバイスの高可用性ペアが分離されます。

分断操作によって、アクティブおよびスタンバイ デバイスからフェールオーバー設定が削除されます。

次のタスク

（オプション）アクティブなデバイス上で flex-config ポリシーを使用している場合は、flex-config ポリシーを変更して再展開し、展開エラーを解消します。

ハイ アベイラビリティ ペアの登録解除

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	Firepower Threat Defense Firepower Threat Defense Virtual	いずれか（Any）	Admin/Network Admin

各ユニットで CLI を使用することによって、Firepower Management Center からペアを削除し、ハイ アベイラビリティを無効にすることができます。

始める前に

この手順では、CLI アクセスが必要です。

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 登録解除するハイ アベイラビリティ ペアの横にある削除アイコン（）をクリックします。

ステップ 3 [Yes] をクリックします。デバイス ハイ アベイラビリティ ペアが削除されます。

ステップ 4 各ユニットで、Firepower Threat Defense CLI にアクセスし、次のコマンドを入力します。

configure high-availability disable

このコマンドを入力しない場合、ユニットを再登録して、新しい HA ペアを形成することはできません。

（注） ファイアウォール モードを変更する前に、このコマンドを入力します。モードを変更すると、ユニットでは **configure high-availability disable** コマンドを入力できなくなります。Firepower Management Center では、このコマンドを使用せずに HA ペアを再形成することはできません。

モニタリング 高可用性

このセクションでは、高可用性 ステータスをモニタできます。

フェールオーバー履歴の表示

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	Firepower Threat Defense Firepower Threat Defense Virtual	いずれか（Any）	Admin/Network Admin

ハイ アベイラビリティの両方のデバイスに関するフェールオーバーの履歴を1つのビューに表示できます。履歴は古いものから順番に表示され、すべてのフェールオーバーの理由が示されます。

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 編集するデバイス ハイ アベイラビリティ ペアの横にある編集アイコン（  ）をクリックします。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [サマリー（Summary）] を選択します。

ステップ 4 [全般（General）] の下で、表示アイコン（）をクリックします。

ステートフル フェールオーバーの統計情報の表示

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	Firepower Threat Defense Firepower Threat Defense Virtual	いずれか（Any）	Admin/Network Admin

ハイ アベイラビリティ ペアのプライマリとセカンダリ デバイス両方のステートフル フェールオーバー リンク統計情報を表示できます。

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

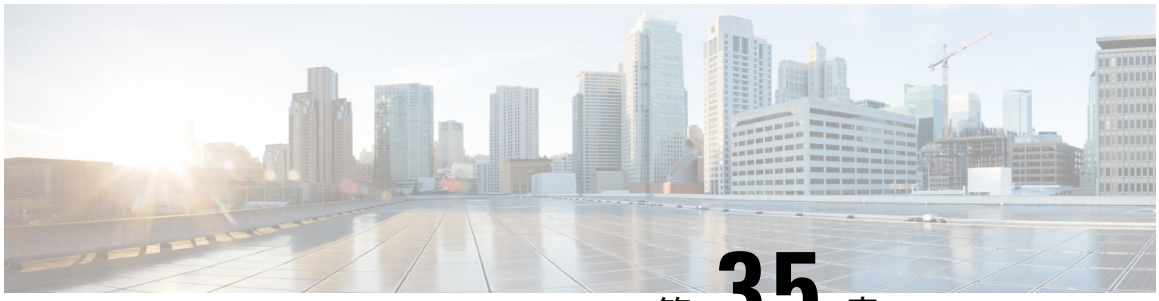
ステップ 2 編集するデバイス ハイ アベイラビリティ ペアの横にある編集アイコン（  ）をクリックします。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [ハイ アベイラビリティ（High Availability）] を選択します。

ステップ 4 ステートフル フェールオーバー リンクの下にある表示アイコン（🔍）をクリックします。

ステップ 5 統計情報を表示するデバイスを選択します。



第 35 章

Firepower Threat Defense 用のクラスタリング

クラスタリングを利用すると、複数の FTD ユニットを 1 つの論理デバイスにグループ化できます。クラスタリングは、Firepower 9300 および Firepower 4100 シリーズ 上の FTD デバイスでのみサポートされます。クラスタは、単一デバイスのすべての利便性（管理、ネットワークへの統合）を備える一方で、複数デバイスによって高いスループットおよび冗長性を達成します。

（注） 一部の機能は、クラスタリングを使用する場合、サポートされません。クラスタリングでサポートされない機能 （913 ページ）を参照してください。

Firepower4100/9300シャーシでのクラスタリングについて

クラスタは、単一の論理ユニットとして機能する複数のデバイスから構成されます。Firepower 4100/9300 シャーシ にクラスタを展開すると、以下の処理が実行されます。

- ユニット間通信用のクラスタ制御リンク（デフォルトのポート チャネル 48）を作成します。シャーシ内クラスタリングでは（Firepower 9300のみ）、このリンクは、クラスタ通

信にFirepower 9300バックプレーンを使用します。シャーシ間クラスタリングでは、シャーシ間通信のために、このEtherChannelに物理インターフェイスを手動で割り当てる必要があります。

- アプリケーション内のクラスタブートストラップコンフィギュレーションを作成します。

  クラスタを展開すると、クラスタ名、クラスタ制御リンクインターフェイス、およびその他のクラスタ設定を含む各ユニットに対して、最小限のブートストラップ構成がFirepower 4100/9300 シャーシ スーパーバイザからプッシュされます。

- スパンドインターフェイスとして、クラスタにデータインターフェイスを割り当てます。

  シャーシ内クラスタリングでは、スパンドインターフェイスは、シャーシ間クラスタリングのようにEtherChannelに制限されません。Firepower 9300スーパーバイザは共有インターフェイスの複数のモジュールにトラフィックをロードバランシングするために内部でEtherChannelテクノロジーを使用するため、スパンドモードではあらゆるタイプのデータインターフェイスが機能します。 シャーシ間クラスタリングでは、すべてのデータ インターフェイスでスパンド EtherChannel を使用します。

（注） 管理インターフェイス以外の個々のインターフェイスはサポートされていません。

- 管理インターフェイスをクラスタ内のすべてのユニットに指定します。

ここでは、クラスタリングの概念と実装について詳しく説明します。クラスタリングの参考資料 （942 ページ）も参照してください。

Bootstrap Configuration

クラスタを展開すると、クラスタ名、クラスタ制御リンクインターフェイス、およびその他のクラスタ設定を含む各ユニットに対して、最小限のブートストラップ構成がFirepower 4100/9300 シャーシ スーパーバイザからプッシュされます。

クラスタ メンバー

クラスタ メンバーは連携して動作し、セキュリティ ポリシーおよびトラフィック フローの共有を達成します。

クラスタ内のメンバの 1 つが**マスター** ユニットです。マスター ユニットは自動的に決定されます。他のすべてのメンバは**スレーブ** ユニットです。

すべてのコンフィギュレーション作業はマスターユニット上でのみ実行する必要があります。コンフィギュレーションはその後、スレーブ ユニットに複製されます。

機能によっては、クラスタ内でスケーリングしないものがあり、そのような機能についてはマスター ユニットがすべてのトラフィックを処理します。。クラスタリングの中央集中型機能（913 ページ）を参照してください。

クラスタ制御リンク

クラスタ制御リンクは、ポートチャネル 48 インターフェイスを使用して自動的に作成されます。シャーシ間クラスタリングでは、このインターフェイスにメンバーインターフェイスはありません。このクラスタ タイプの EtherChannel は、シャーシ内クラスタリング用のクラスタ通信に Firepower 9300 バックプレーンを使用します。

クラスタ制御リンク トラフィックには、制御とデータの両方のトラフィックが含まれます。

シャーシ間クラスタリングのクラスタ制御リンクのサイズ

可能であれば、各シャーシの予想されるスループットに合わせてクラスタ制御リンクをサイジングする必要があります。そうすれば、クラスタ制御リンクが最悪のシナリオを処理できます。

クラスタ制御リンク トラフィックの内容は主に、状態アップデートや転送されたパケットです。クラスタ制御リンクでのトラフィックの量は常に変化します。転送されるトラフィックの量は、ロードバランシングの有効性、または中央集中型機能のための十分なトラフィックがあるかどうかによって決まります。次に例を示します。

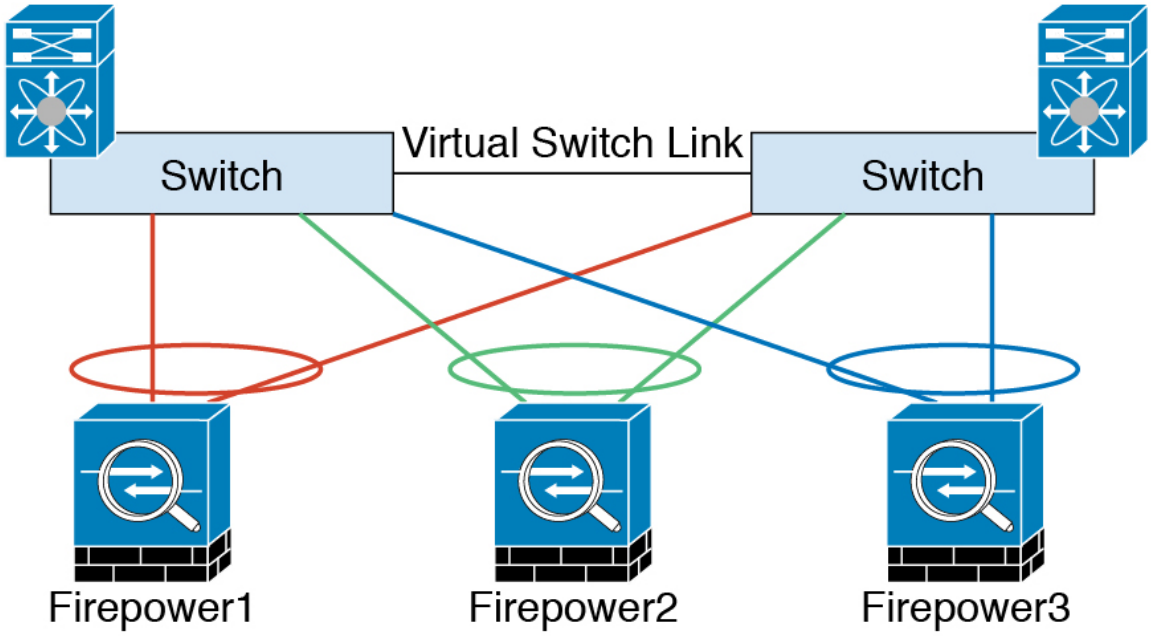
- NAT では接続のロード バランシングが低下するので、すべてのリターン トラフィックを正しいユニットに再分散する必要があります。
- メンバーシップが変更されると、クラスタは大量の接続の再分散を必要とするため、一時的にクラスタ制御リンクの帯域幅を大量に使用します。

クラスタ制御リンクの帯域幅を大きくすると、メンバーシップが変更されたときの収束が高速になり、スループットのボトルネックを回避できます。

（注） クラスタに大量の非対称（再分散された）トラフィックがある場合は、クラスタ制御リンクのサイズを大きくする必要があります。

シャーシ間クラスタリングのクラスタ制御リンク冗長性

次の図は、仮想スイッチングシステム（VSS）または仮想ポートチャネル（vPC）環境でクラスタ制御リンクとして EtherChannel を使用する方法を示します。EtherChannel のすべてのリンクがアクティブです。スイッチが VSS または vPC の一部である場合は、同じ EtherChannel 内の Firepower 9300 シャーシ インターフェイスをそれぞれ、VSS または vPC 内の異なるスイッチに接続できます。スイッチ インターフェイスは同じ EtherChannel ポートチャネル インターフェイスのメンバです。複数の個別のスイッチが単一のスイッチのように動作するからです。この EtherChannel は、スパンド EtherChannel ではなく、デバイス ローカルであることに注意してください。



シャーシ間クラスタリングのクラスタ制御リンクの信頼性

クラスタ制御リンクの機能を保証するには、ユニット間のラウンドトリップ時間（RTT）が20 ms 未満になるようにします。この最大遅延により、異なる地理的サイトにインストールされたクラスタ メンバとの互換性が向上します。遅延を調べるには、ユニット間のクラスタ制御リンクで ping を実行します。

クラスタ制御リンクは、順序の異常やパケットのドロップがない信頼性の高いものである必要があります。たとえば、サイト間の導入の場合、専用リンクを使用する必要があります。

クラスタ制御リンク ネットワーク

Firepower 4100/9300 シャーシは、シャーシ ID およびスロット ID（127.2.*chassis_id.slot_id*）に基づいて、各ユニットのクラスタ制御リンク インターフェイス IP アドレスを自動生成します。クラスタを展開する場合にこの IP アドレスをカスタマイズできます。クラスタ制御リンク ネットワークには、ユニット間のルータを含めることはできません。レイヤ 2 スイッチングのみが許可されます。

管理ネットワーク

すべてのユニットを単一の管理ネットワークに接続することを推奨します。このネットワークは、クラスタ制御リンクとは別のものです。

管理インターフェイス

管理タイプのインターフェイスをクラスタに割り当てる必要があります。このインターフェイスはスパンド インターフェイスではなく、特別な個別インターフェイスです。管理インター

フェイスによって各単位に直接接続できます。この管理論理インターフェイスはデバイスの他のインターフェイスから切り離されています。これは、Firepower Management Center にデバイスを設定し、登録するために使用されます。管理インターフェイスは、独自のローカル認証、IP アドレス、およびスタティック ルーティングを使用します。クラスタの各メンバーは、管理ネットワーク上で、それぞれに異なる IP アドレスを使用します。これらの IP アドレスは、ブートストラップ構成の一部としてユーザが設定します。

管理インターフェイスは、管理論理インターフェイスと診断論理インターフェイスの間で共有されます。診断論理インターフェイスはオプションであり、ブートストラップ構成の一部としては設定されません。診断インターフェイスは、他のデータ インターフェイスと併せて設定できます。診断インターフェイスを設定する場合、メイン クラスタ IP アドレスを、そのクラスタの固定アドレス（常に現在のマスターユニットに属するアドレス）として設定します。アドレス範囲も設定して、現在のマスターを含む各ユニットがその範囲内のローカルアドレスを使用できるようにします。このメイン クラスタ IP アドレスによって、診断アクセスのアドレスが一本化されます。マスター ユニットが変更されると、メイン クラスタ IP アドレスは新しいマスターユニットに移動するので、クラスタへのアクセスをシームレスに続行できます。TFTP や syslog などの発信管理トラフィックの場合、マスター ユニットを含む各ユニットは、ローカル IP アドレスを使用してサーバに接続します。

クラスタ インターフェイス

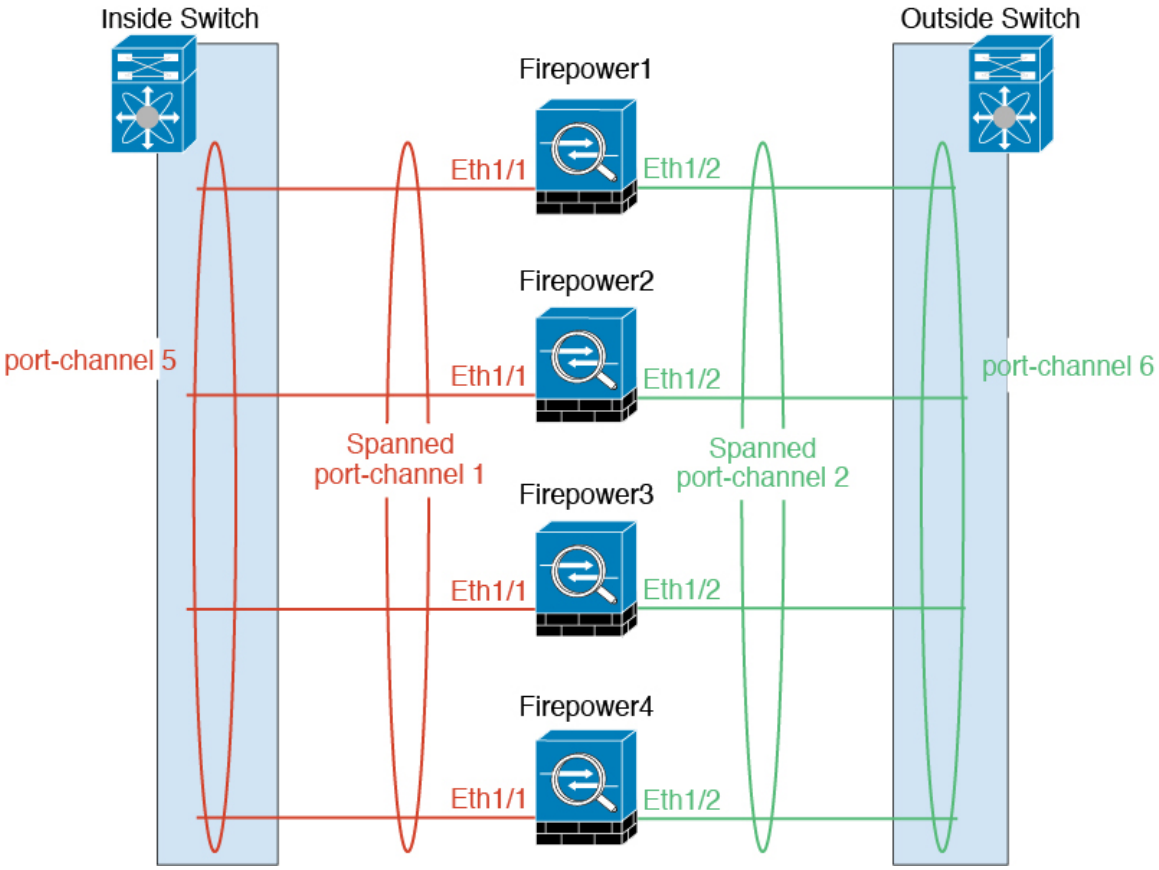
シャーシ内クラスタリングでは、物理インターフェイス、EtherChannel （ポートチャネルとも呼ばれる）の両方を割り当てることができます。クラスタに割り当てられたインターフェイスはクラスタ内のすべてのメンバーのトラフィックのロード バランシングを行うスパンド インターフェイスです。

シャーシ間クラスタリングでは、データ EtherChannel のみをクラスタに割り当てできます。これらのスパンド EtherChannel は、各シャーシの同じメンバー インターフェイスを含みます。アップストリーム スイッチでは、これらのインターフェイスはすべて単一の EtherChannel に含まれ、スイッチは複数のデバイスに接続されていることを察知しません。

管理インターフェイス以外の個々のインターフェイスはサポートされていません。

スパンド EtherChannel

シャーシあたり 1 つ以上のインターフェイスをグループ化して、クラスタのすべてのシャーシに広がる EtherChannel とすることができます。EtherChannel によって、チャネル内の使用可能なすべてのアクティブ インターフェイスのトラフィックが集約されます。スパンド EtherChannel は、ルーテッドとトランスペアレントのどちらのファイアウォール モードでも設定できます。ルーテッド モードでは、EtherChannel は単一の IP アドレスを持つルーテッド インターフェイスとして設定されます。トランスペアレント モードでは、IP アドレスはブリッジグループ メンバーではなく BVI に割り当てられます。EtherChannel は初めから、ロードバランシング機能を基本的動作の一部として備えています。



VSS または vPC への接続

インターフェイスに冗長性を確保するため、EtherChannel を VSS または vPC に接続することを推奨します。

設定の複製

クラスタ内のすべてのユニットは、単一のコンフィギュレーションを共有します。コンフィギュレーション変更を加えることができるのはマスターユニット上だけであり、変更は自動的にクラスタ内の他のすべてのユニットに同期されます。

Firepower Threat Defense の機能とクラスタリング

FTD の一部の機能はクラスタリングではサポートされず、一部はマスター ユニットのみでサポートされます。その他の機能については適切な使用に関する警告がある場合があります。

クラスタリングでサポートされない機能

これらの機能は、クラスタリングがイネーブルのときは設定できず、コマンドは拒否されます。

- リモート アクセス VPN（SSL VPN および IPsec VPN）
- DHCP クライアント、サーバ、およびプロキシDHCP リレーがサポートされている。
- 高可用性
- Integrated Routing and Bridging（IRB）
- デッド接続検出（DCD）

クラスタリングの中央集中型機能

次の機能は、マスターユニット上だけでサポートされます。クラスタの場合もスケーリングされません。

（注） 中央集中型機能のトラフィックは、クラスタ制御リンク経由でメンバ ユニットからマスター ユニットに転送されます。

再分散機能を使用する場合は、中央集中型機能のトラフィックが中央集中型機能として分類される前に再分散が行われて、マスター以外のユニットに転送されることがあります。この場合は、トラフィックがマスター ユニットに送り返されます。

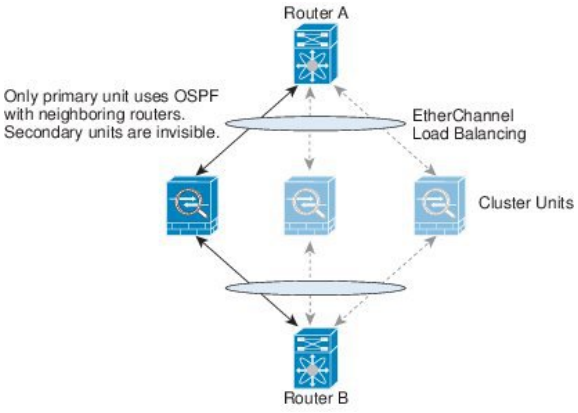
中央集中型機能については、マスターユニットで障害が発生するとすべての接続がドロップされるので、新しいマスター ユニット上で接続を再確立する必要があります。

- 次のアプリケーション インスペクション：
  - DCERPC
  - NetBIOS
  - RSH
  - SUNRPC
  - TFTP
  - XDMCP
- ダイナミック ルーティング
- スタティック ルート モニタリング

ダイナミック ルーティングおよびクラスタリング

ルーティング プロセスはマスター ユニット上だけで実行されます。ルートはマスター ユニットを介して学習され、セカンダリに複製されます。ルーティング パケットがスレーブに到着した場合は、マスター ユニットにリダイレクトされます。

図 *21* : ダイナミック ルーティング



スレーブ メンバがマスター ユニットからルートを学習した後は、各ユニットが個別に転送に関する判断を行います。

OSPF LSA データベースは、マスター ユニットからスレーブ ユニットに同期されません。マスターユニットのスイッチオーバーが発生した場合は、隣接ルータが再起動を検出します。スイッチオーバーは透過的ではありません。OSPF プロセスが IP アドレスの 1 つをルータ ID として選択します必須ではありませんが、スタティック ルータ ID を割り当てることができます。これで、同じルータ ID がクラスタ全体で使用されるようになります。割り込みを解決するには、OSPF ノンストップ フォワーディング機能を参照してください。

NAT とクラスタリング

NAT は、クラスタの全体的なスループットに影響を与えることがあります。着信および発信の NAT パケットが、クラスタ内のそれぞれ別の Firepower Threat Defense デバイス に送信されることがあります。これは、ロード バランシング アルゴリズムは IP アドレスとポートに依存していますが、NAT が使用される場合、着信と発信でパケットの IP アドレスやポートが異なるためです。NAT オーナーではない Firepower Threat Defense デバイス に到着したパケットは、クラスタ制御リンクを介してオーナーに転送されるので、大量のトラフィックがクラスタ制御リンク上で発生します。NAT オーナーはセキュリティおよびポリシー チェックの結果に応じてパケットの接続を作成するため、受信側ユニットは転送フローをオーナーに作成しません。

それでもクラスタリングで NAT を使用する場合は、次のガイドラインを考慮してください。

- ダイナミック PAT 用 NAT プール アドレス分散：マスター ユニットは、アドレスをクラスタ全体に均等に分配します。メンバーが接続を受信したときに、そのメンバーのアドレスが 1 つも残っていない場合は、接続はドロップされます（他のメンバーにはまだ使用可能なアドレスがある場合でも）。最低でも、クラスタ内のユニットと同数の NAT アドレ

スが含まれていることを確認してください。各ユニットが確実に1つのアドレスを受け取るようにするためです。

- ラウンドロビンなし：PATプールのラウンドロビンは、クラスタリングではサポートされません。
- マスターユニットによって管理されるダイナミックNAT xlate：マスターユニットがxlateテーブルを維持し、スレーブ ユニットに複製します。ダイナミック NAT を必要とする接続をスレーブ ユニットが受信したときに、その xlate がテーブル内にない場合は、スレーブはマスター ユニットに xlate を要求します。スレーブ ユニットが接続を所有します。
- 次のインスペクション用のスタティック PAT はありません。
  - FTP
  - RSH
  - SQLNET
  - TFTP
  - XDMCP
  - SIP

SIP インスペクションとクラスタリング

制御フローは、任意のユニットで作成できます（ロードバランシングのため）。その子データフローは同じユニットに存在する必要があります。

syslog とクラスタリング

- クラスタの各ユニットは自身のsyslogメッセージを生成します。各ユニットのsyslogメッセージ ヘッダー フィールドで使用されるデバイス ID を同一にするか、別にするかを設定できます。たとえば、ホスト名コンフィギュレーションはクラスタ内のすべてのユニットに複製されて共有されます。ホスト名をデバイス ID として使用するようにロギングを設定した場合は、どのユニットで生成されたsyslogメッセージも1つのユニットからのように見えます。クラスタ ブートストラップ コンフィギュレーションで割り当てられたローカル ユニット名をデバイス ID として使用するようにロギングを設定した場合は、syslogメッセージはそれぞれ別のユニットからのように見えます。

SNMP とクラスタリング

SNMP エージェントは、個々の Firepower Threat Defense デバイス を、その診断インターフェイス ローカル IP アドレスによってポーリングします。クラスタの統合データをポーリングすることはできません。

SNMP ポーリングには、メイン クラスタ IP アドレスではなく、常にローカル アドレスを使用してください。SNMP エージェントがメイン クラスタ IP アドレスをポーリングする場合は、新しいマスターが選定されたときに、新しいマスター ユニットのポーリングに失敗します。

FTP とクラスタリング

- FTP データ チャネルとコントロール チャネルのフローがそれぞれ別のクラスタ メンバよって所有されている場合は、データ チャネルのオーナーは定期的にアイドル タイムアウト アップデートをコントロール チャネルのオーナーに送信し、アイドル タイムアウト値を更新します。ただし、コントロール フローのオーナーがリロードされて、コントロール フローが再ホスティングされた場合は、親子フロー関係は維持されなくなります。したがって、コントロール フローのアイドル タイムアウトは更新されません。

Cisco TrustSec とクラスタリング

マスター ユニットだけがセキュリティ グループ タグ（SGT）情報を学習します。マスター ユニットからこの SGT がスレーブに渡されるので、スレーブは、セキュリティ ポリシーに基づいて SGT の一致決定を下せます。

VPN とクラスタリング

サイトツーサイト VPN は、中央集中型機能です。マスター ユニットだけが VPN 接続をサポートします。

（注） リモート アクセス VPN は、クラスタリングではサポートされません。

VPN 機能を使用できるのはマスター ユニットだけであり、クラスタのハイ アベイラビリティ能力は活用されません。マスター ユニットで障害が発生した場合は、すべての既存の VPN 接続が失われ、VPN ユーザにとってはサービスの中断となります。新しいマスターが選定されたときに、VPN 接続を再確立する必要があります。

VPN トンネルをスパンドインターフェイスのアドレスに接続すると、接続が自動的にマスター ユニットに転送されます。

VPN 関連のキーと証明書は、すべてのユニットに複製されます。

クラスタリングのライセンス

FTD はスマート ライセンスを使用します。個別のユニットではなく、クラスタ全体にライセンスを割り当てます。ただし、クラスタの各ユニットは機能ごとに個別のライセンスを使用します。

クラスタ メンバーを FMC に追加する際に、そのクラスタに使用する機能ライセンスを指定できます。クラスタのライセンスは、**[デバイス（Devices）] > [デバイス管理（Device Management）] > [クラスタ（Cluster）] > [ライセンス（License）]** 領域で変更できます。

（注） FMCにライセンスを取得する（および評価モードで実行する）前にクラスタを追加した場合、FMC にライセンスを取得する際にポリシーの変更をクラスタに展開するとトラフィックの中断が発生することがあります。ライセンスモードを変更したことによって、すべてのスレーブユニットがクラスタをいったん離れてから再参加することになります。

クラスタリングの要件と前提条件

クラスタ モデルのサポート

- Firepower 9300：クラスタには最大 6 ユニットを含めることができます。たとえば、6 つのシャーシで 1 つのモジュールを使用したり、3 つのシャーシで 2 つのモジュールを使用したり、最大 6 つのモジュールを組み合わせたりできます。シャーシ内クラスタリングとシャーシ間クラスタリングをサポートします。
- Firepower 4100 シリーズ：シャーシ間クラスタリングを使用して最大 6 ユニットをサポートします。

シャーシ間のクラスタリング ハードウェアおよびソフトウェアの要件

クラスタ内のすべてのシャーシ：

- Firepower4100シリーズ：すべてのシャーシが同一モデルである必要があります。Firepower 9300：すべてのセキュリティ モジュールは同じタイプである必要があります。たとえば、クラスタリングを使用する場合は、Firepower 9300 のすべてのモジュールは SM-40 である必要があります。各シャーシに異なる数のセキュリティ モジュールをインストールできますが、すべての空のスロットを含め、シャーシのすべてのモジュールをクラスタに含める必要があります。
- イメージアップグレード時を除き、同じFXOS ソフトウェアを実行する必要があります。
- クラスタに割り当てるインターフェイスは、管理インターフェイス、EtherChannel、アクティブインターフェイス、スピード、デュプレックスなど、同じインターフェイス構成を含める必要があります。同じインターフェイス ID の容量が一致し、インターフェイスが同じスパンドEtherChannelに内に問題なくバンドルできる限り、シャーシに異なるタイプのネットワーク モジュールを使用できます。シャーシ間クラスタリングでは、すべてのデータ インターフェイスを EtherChannel とする必要があります。（インターフェイス モジュールの追加または削除、あるいはEtherChannelの設定などにより）クラスタリングを有効にした後にFXOSでインターフェイスを変更した場合は、各シャーシで同じ変更を行います（スレーブ ユニットから始めて、マスターで終わります）。

- 同じ NTP サーバを使用する必要があります。 Firepower Threat Defense のため、Firepower Management Center は同じ NTP サーバを使用する必要があります。手動で時間を設定しないでください。

シャーシ間クラスタリングのスイッチ要件

- Firepower 4100/9300 シャーシのクラスタリングを設定する前に、スイッチの設定を完了し、シャーシからスイッチまですべての EtherChannel を良好に接続してください。
- サポートされているスイッチのリストについては、「Cisco FXOS Compatibility」を参照してください。

クラスタリング ガイドラインと制限事項

シャーシ間クラスタリングのスイッチ

- ASR 9006 では、非デフォルト MTU を設定する場合は、ASR インターフェイス MTU をクラスタ デバイス MTU より 14 バイト大きく設定します。そうしないと、**mtu-ignore** オプションを使用しない限り、OSPF 隣接関係（アジャセンシー）ピアリングの試行が失敗する可能性があります。クラスタ デバイス MTU は、ASR *IPv4* MTU と一致する必要があります。
- クラスタ制御リンク インターフェイスのスイッチでは、クラスタ ユニットに接続されるスイッチ ポートに対してスパニングツリー PortFast をイネーブルにすることもできます。このようにすると、新規ユニットの参加プロセスを高速化できます。
- スイッチ上のスパンド EtherChannel のバンドリングが遅いときは、スイッチの個別インターフェイスに対して LACP 高速レートをイネーブルにできます。Nexus シリーズなど一部のスイッチでは、インサービス ソフトウェア アップグレード（ISSU）を実行する際に LACP 高速レートがサポートされないことに注意してください。そのため、クラスタリングで ISSU を使用することは推奨されません。
- スイッチでは、EtherChannel ロードバランシング アルゴリズム **source-dest-ip** または **source-dest-ip-port**（Cisco Nexus OS および Cisco IOS の **port-channel load-balance** コマンドを参照）を使用することをお勧めします。クラスタのデバイスにトラフィックを不均一に配分する場合があるので、ロード バランス アルゴリズムでは **vlan** キーワードを使用しないでください。
- スイッチの EtherChannel ロードバランシング アルゴリズムを変更すると、スイッチの EtherChannel インターフェイスは一時的にトラフィックの転送を停止し、スパニングツリー プロトコルが再始動します。トラフィックが再び流れ出すまでに、少し時間がかかります。
- 一部のスイッチは、LACP でのダイナミック ポート プライオリティをサポートしていません（アクティブおよびスタンバイ リンク）。ダイナミック ポート プライオリティを無効化することで、スパンド EtherChannel との互換性を高めることができます。

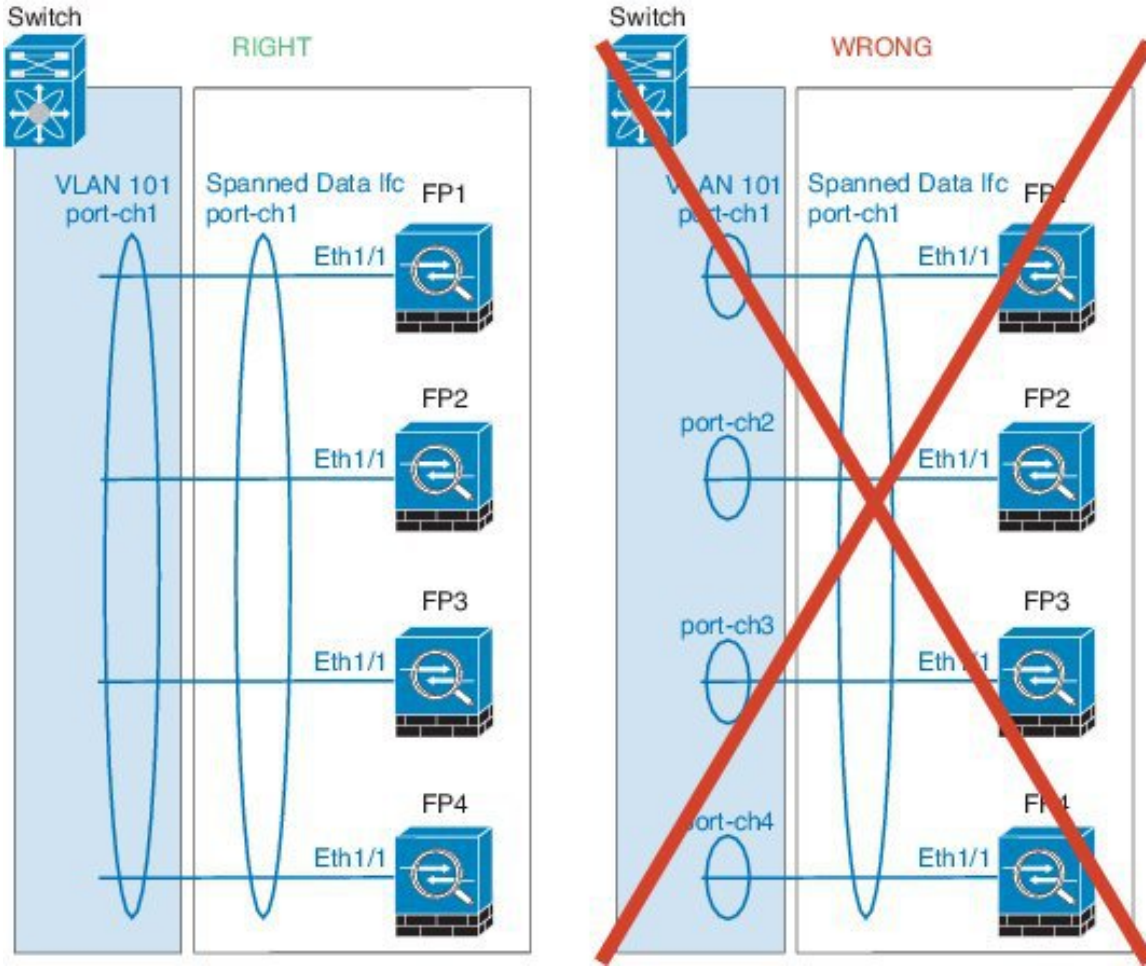
- クラスタ制御リンク パスのスイッチでは、L4 チェックサムを検証しないようにする必要があります。クラスタ制御リンク経由でリダイレクトされたトラフィックには、正しい L4 チェックサムが設定されていません。L4 チェックサムを検証するスイッチにより、トラフィックがドロップされる可能性があります。
- ポートチャネル バンドルのダウンタイムは、設定されているキープアライブ インターバルを超えてはなりません。
- Supervisor 2T EtherChannel では、デフォルトのハッシュ配信アルゴリズムは適応型です。VSS設計での非対称トラフィックを避けるには、クラスタ デバイスに接続されているポートチャネルでのハッシュ アルゴリズムを固定に変更します。

  router(config)# **port-channel** *id* **hash-distribution fixed**

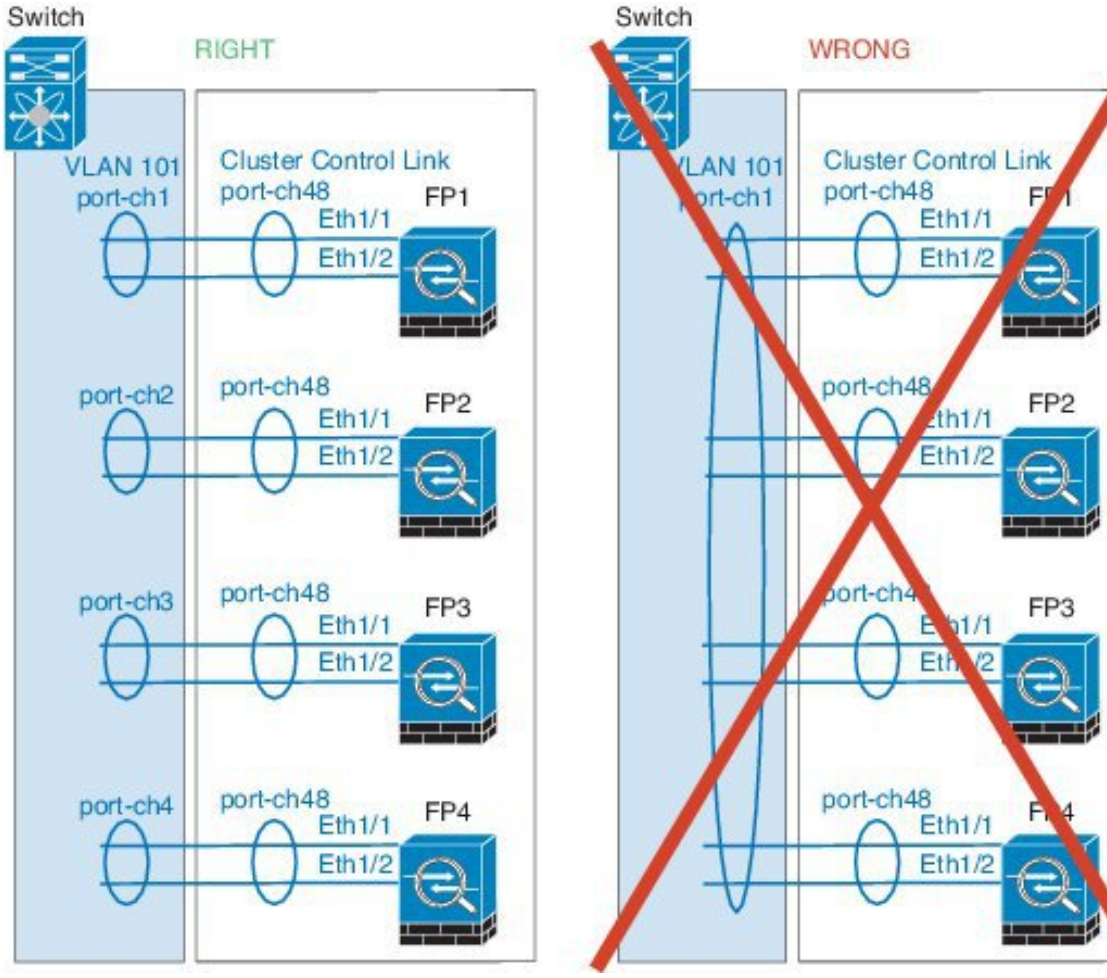
  アルゴリズムをグローバルに変更しないでください。VSS ピア リンクに対しては適応型アルゴリズムを使用できます。

シャーシ間クラスタリングの EtherChannel

- スイッチ接続用に、EtherChannel モードをアクティブに設定します。クラスタ制御リンクであっても、Firepower 4100/9300 シャーシではオン モードはサポートされません。
- FXOS EtherChannel にはデフォルトで [fast] に設定されている LACP レートがあります。Nexus シリーズなど一部のスイッチでは、インサービス ソフトウェア アップグレード（ISSU）を実行する際に LACP 高速レートがサポートされないため、クラスタリングで ISSU を使用することは推奨されません。
- 15.1(1)S2 より前の Catalyst 3750-X Cisco IOS ソフトウェア バージョンでは、クラスタ ユニットはスイッチ スタックに EtherChannel を接続することをサポートしていませんでした。デフォルトのスイッチ設定では、クラスタ ユニット EtherChannel がクロス スタックに接続されている場合、マスター スイッチの電源がオフになると、残りのスイッチに接続されている EtherChannel は起動しません。互換性を高めるため、**stack-mac persistent timer** コマンドを設定して、十分なリロード時間を確保できる大きな値、たとえば 8 分、0（無制限）などを設定します。または、15.1(1)S2 など、より安定したスイッチ ソフトウェア バージョンにアップグレードできます。
- スパンド EtherChannel とデバイス ローカル EtherChannel のコンフィギュレーション：スパンド EtherChannel と デバイス ローカル EtherChannel に対してスイッチを適切に設定します。
  - スパンド EtherChannel：クラスタ ユニット スパンド EtherChannel（クラスタのすべてのメンバに広がる）の場合は、複数のインターフェイスが結合されてスイッチ上の単一の EtherChannel となります。各インターフェイスがスイッチ上の同じチャネル グループ内にあることを確認してください。



- デバイス ローカル EtherChannel：クラスタ ユニット デバイス ローカル EtherChannel（クラスタ制御リンク用に設定された EtherChannel もこれに含まれます）は、それぞれ独立した EtherChannel としてスイッチ上で設定してください。スイッチ上で複数のクラスタ ユニット EtherChannel を結合して 1 つの EtherChannel としないでください。



その他のガイドライン

- ユニットを既存のクラスタに追加したときや、ユニットをリロードしたときは、一時的に、限定的なパケット/接続ドロップが発生します。これは予定どおりの動作です。場合によっては、ドロップされたパケットが原因で接続がハングすることがあります。たとえば、FTP 接続の FIN/ACK パケットがドロップされると、FTP クライアントがハングします。この場合は、FTP 接続を再確立する必要があります。
- スパンド EtherChannel インターフェイスに接続された Windows 2003 Server を使用している場合、syslog サーバポートがダウンしたときにサーバが ICMP エラーメッセージをスロットリングしないと、多数の ICMP メッセージがクラスタに送信されることになります。このようなメッセージにより、クラスタの一部のユニットで CPU 使用率が高くなり、パフォーマンスに影響する可能性があります。ICMP エラー メッセージを調節することを推奨します。
- 冗長性を持たせるため、VSS または vPC に EtherChannel を接続することを推奨します。

- シャーシ内では、スタンドアロン モードで一部のシャーシ セキュリティ モジュールをクラスタ化し、他のセキュリティ モジュールを実行することはできません。クラスタ内にすべてのセキュリティ モジュールを含める必要があります。

デフォルト

- クラスタのヘルス チェック機能は、デフォルトでイネーブルになり、ホールド時間は3秒です。デフォルトでは、すべてのインターフェイスでインターネット ヘルス モニタリングがイネーブルになっています。
- 失敗したクラスタ制御リンクのクラスタ自動再結合機能は、5 分おきに無制限に試行されるように設定されています。
- 失敗したデータ インターフェイスのクラスタ自動再結合機能は、5 分後と、2 に設定された増加間隔で合計で 3 回試行されるように設定されています。
- HTTP トラフィックは、5 秒間の接続レプリケーション遅延がデフォルトで有効になっています。

クラスタリングの設定

クラスタは、Firepower 4100/9300 シャーシ スーパバイザから簡単に展開できます。すべての初期設定が各ユニットに自動的に生成されます。その後、ユニットを FMC に追加し、1 つのクラスタにグループ化できます。

FXOS：Firepower Threat Defense クラスタの追加

単独の Firepower 9300 シャーシをシャーシ内クラスタとして追加することも、複数のシャーシをシャーシ間クラスタリングに追加することもできます。シャーシ間クラスタリングでは、各シャーシを別々に設定します。1 つのシャーシにクラスタを追加したら、導入を簡単にするため、ブートストラップ設定を最初のシャーシから次のシャーシにコピーし、

Firepower Threat Defense クラスタの作成

クラスタは、Firepower 4100/9300 シャーシ スーパバイザから簡単に展開できます。すべての初期設定が各ユニットに自動的に生成されます。

シャーシ間クラスタリングでは、各シャーシを別々に設定します。導入を容易にするために、1 つのシャーシにクラスタを導入し、その後、最初のシャーシから次のシャーシにブートストラップ コンフィギュレーションをコピーできます。

モジュールがインストールされていない場合でも、Firepower 9300 シャーシの 3 つすべてのモジュール スロットでクラスタリングを有効にする必要があります。3つすべてのモジュールを設定していないと、クラスタは機能しません。

始める前に

- 論理デバイスに使用するアプリケーションイメージを Cisco.com からダウンロードして、そのイメージを Firepower 4100/9300 シャーシ にアップロードします。
- 次の情報を用意します。
  - 管理インターフェイス ID、IP アドレス、およびネットワークマスク
  - ゲートウェイ IP アドレス
  - FMC 選択した IP アドレスや NAT ID
  - DNS サーバの IP アドレス。
  - FTD ホスト名とドメイン名

ステップ 1 インターフェイスを設定します。

a) クラスタを展開する前に、1 つ以上のデータ タイプのインターフェイスまたは EtherChannel（ポート チャネルとも呼ばれる）を追加します。EtherChannel（ポート チャネル）の追加 （757 ページ） または 物理インターフェイスの設定 （756 ページ） を参照してください。

シャーシ間クラスタリングでは、すべてのデータインターフェイスが 1 つ以上のメンバーインターフェイスを持つスパンド EtherChannel である必要があります。各シャーシに同じ EtherChannel を追加します。スイッチ上で、すべてのクラスタユニットからメンバーインターフェイスを 1 つの EtherChannel へと結合します。シャーシ間クラスタリングの EtherChannel についての詳細は、クラスタリング ガイドラインと制限事項 （918 ページ） を参照してください。

デフォルトでは、すべてのインターフェイスがクラスタに割り当てられます。 シャーシ間クラスタリングでは、EtherChannel のみが割り当てられます。他のインターフェイスタイプを割り当てることはできません。導入後にもクラスタにデータ インターフェイスを追加できます。

b) 管理タイプのインターフェイスまたは EtherChannel を追加します。EtherChannel（ポート チャネル）の追加 （757 ページ） または 物理インターフェイスの設定 （756 ページ） を参照してください。

管理インターフェイスが必要です。この管理インターフェイスは、シャーシの管理のみに使用されるシャーシ管理インターフェイスと同じではありません（FXOS では、シャーシ管理インターフェイスは MGMT、management0 のような名前で表示されます）。

シャーシ間クラスタリングの場合、各シャーシに同じ管理インターフェイスを追加します。

c) シャーシ間クラスタリングでは、ポート チャネル 48 にメンバー インターフェイスを追加し、クラスタ制御リンクとして使用します。

シャーシ内クラスタリングのメンバー インターフェイスを追加しないでください。メンバーを追加すると、シャーシはこのクラスタがシャーシ間であると見なし、例えばスパンド Etherchannel のみを使用できるようになります。

[Interfaces] タブで、ポート チャネル 48 クラスタ タイプのインターフェイスは、メンバインターフェイスが含まれていない場合は、[Operation State] を [failed] と表示します。シャーシ内クラスタリング

の場合、この EtherChannel はメンバ インターフェイスを必要としないため、この動作状態は無視して構いません。

各シャーシに同じメンバ インターフェイスを追加します。クラスタ制御リンクは、各シャーシのデバイスローカル EtherChannel です。デバイスごとにスイッチで個別の EtherChannel を使用します。シャーシ間クラスタリングの EtherChannel についての詳細は、クラスタリング ガイドラインと制限事項 （918 ページ） を参照してください。

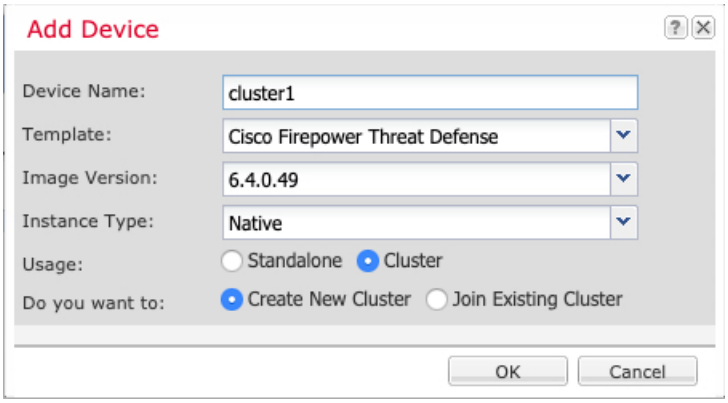
d) （任意） Firepower-eventing インターフェイスを追加します。

このインターフェイスは、FTD デバイスのセカンダリ管理インターフェイスです。このインターフェイスを使用するには、FTD CLI で IP アドレスなどのパラメータを設定する必要があります。たとえば、イベント（Web イベントなど）から管理トラフィックを分類できます。Firepower Threat Defense コマンドリファレンスの **configure network** コマンドを参照してください。

シャーシ間クラスタリングの場合、各シャーシに同じイベンティング インターフェイスを追加します。

ステップ 2 [論理デバイス（Logical Devices）] を選択します。

ステップ 3 **[追加（Add）] > [クラスタ（Cluster）][デバイスの追加（Add Device）]** をクリックし、次のパラメータを設定します。



a) **デバイス名**を入力します。

この名前は、シャーシスーパバイザが管理設定を行ってインターフェイスを割り当てるために使用します。これはアプリケーション設定で使用されるデバイス名ではありません。

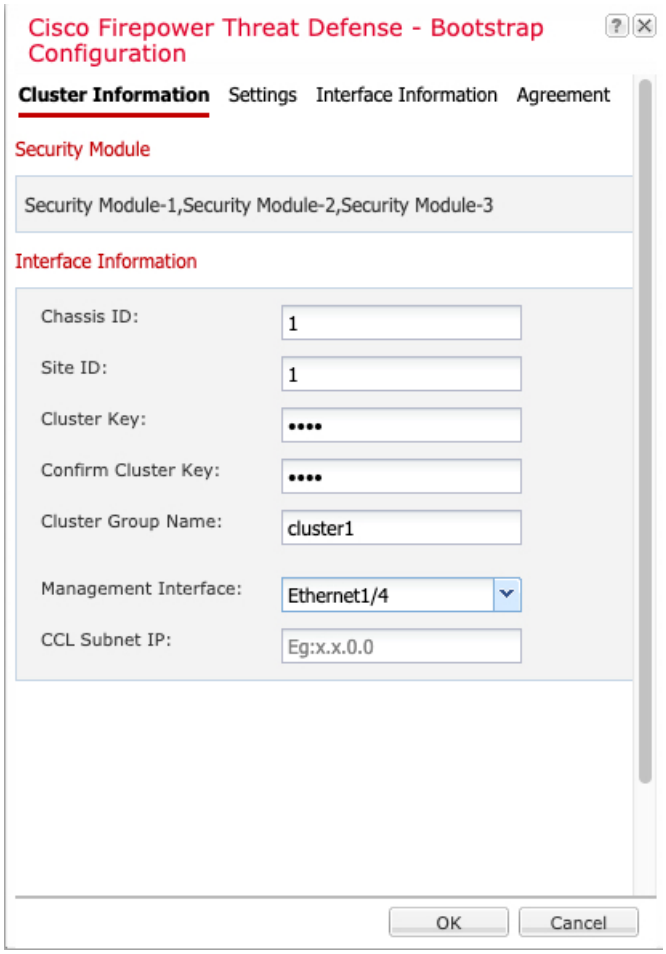
b) [Template] では、[Cisco Firepower Threat Defense] を選択します。
c) [Image Version] を選択します。
d) [Instance Type] では、[Native] タイプのみがサポートされます。
e) [Usage] では、[Cluster] オプションボタンをクリックします。
f) [OK] をクリックします。

[Provisioning - *device name*] ウィンドウが表示されます。デフォルトでは、すべてのインターフェイスがクラスタに割り当てられます。

ステップ 4 画面中央のデバイス アイコンをクリックします。

初期ブートストラップ設定を設定できるダイアログボックスが表示されます。これらの設定は、初期導入専用、またはディザスタ リカバリ用です。通常の運用では、後でアプリケーション CCLI 設定のほとんどの値を変更できます。

ステップ 5 [Cluster Information] ページで、次の手順を実行します。



a) シャーシ間クラスタリングでは、**シャーシ ID** フィールドに、シャーシ ID を入力します。クラスタの各シャーシに固有の ID を使用する必要があります。

このフィールドは、クラスタ制御リンク Port-Channel 48 にメンバー インターフェイスを追加した場合にのみ表示されます。

b) サイト間クラスタリングの場合、[Site ID] フィールドに、このシャーシのサイト ID を 1 ～ 8 の範囲で入力します。この機能は、Firepower Management Center FlexConfig 機能を使用した場合にのみ構成可能です。

c) [Cluster Key] フィールドで、クラスタ制御リンクの制御トラフィックの認証キーを設定します。

共有秘密は、1 ～ 63 文字の ASCII 文字列です。共有秘密は、キーを生成するために使用されます。このオプションは、データパス トラフィック（接続状態アップデートや転送されるパケットなど）には影響しません。データパス トラフィックは、常にクリア テキストとして送信されます。

d) [Cluster Group Name] を設定します。これは、論理デバイス設定のクラスタ グループ名です。

名前は 1 ～ 38 文字の ASCII 文字列であることが必要です。

e) [Management Interface] を選択します。

このインターフェイスは、論理デバイスを管理するために使用されます。このインターフェイスは、シャーシ管理ポートとは別のものです。

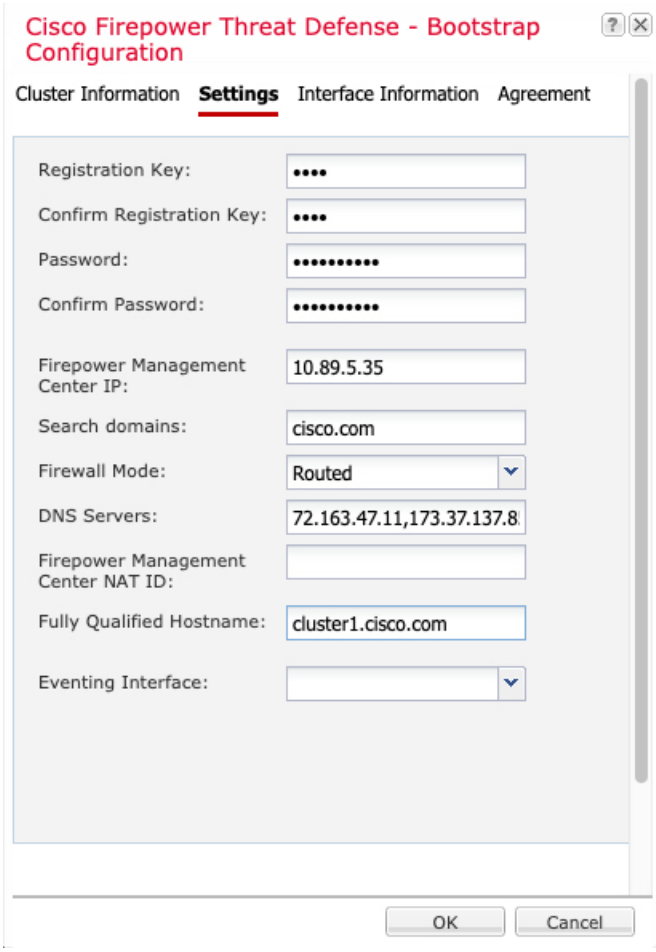
ハードウェア バイパス 対応のインターフェイスをマネジメント インターフェイスとして割り当てると、割り当てが意図的であることを確認する警告メッセージが表示されます。

f) **CCL サブネット IP** を *a.b*.**0.0** に設定します。

クラスタ制御リンクのデフォルトでは 127.2.0.0/16 ネットワークが使用されます。ただし、一部のネットワーク展開では、127.2.0.0/16 トラフィックはパスできません。この場合、クラスタの固有ネットワークに任意の /16 ネットワーク アドレスを指定します（ループバック（127.0.0.0/8）およびマルチキャスト（224.0.0.0/4）のアドレスを除く）。値を 0.0.0.0 に設定すると、デフォルトのネットワークが使用されます。

シャーシは、シャーシ ID とスロット ID（*a.b.chassis_id.slot_id*）に基づいて、各ユニットのクラスタ制御リンク インターフェイスの IP アドレスを自動生成します。

ステップ 6 [設定（**Settings**）] ページで、以下を実行します。



a) [Registration Key] フィールドに、登録時に Firepower Management Center とクラスタ メンバー間で共有するキーを入力します。

このキーには、1 ～ 37 文字の任意のテキスト文字列を選択できます。FTD を追加するときに、 FMC に同じキーを入力します。

b) CLI アクセス用の FTD 管理ユーザの [Password] を入力します。

c) [Firepower Management Center IP] フィールドに、管理 Firepower Management Center の IP アドレスを入力します。FMC の IP アドレスがわからない場合は、このフィールドを空白のままにして、[Firepower Management Center NAT ID] フィールドにパスフレーズを入力します。

d) [Search Domains] フィールドに、管理ネットワークの検索ドメインのカンマ区切りのリストを入力します。

e) [Firewall Mode] ドロップダウン リストから、[Transparent] または [Routed] を選択します。

ルーテッド モードでは、FTDはネットワーク内のルータ ホップと見なされます。ルーティングを行う各インターフェイスは異なるサブネット上にあります。これに対し、トランスペアレント ファイアウォールは、「Bump In The Wire」または「ステルス ファイアウォール」のように動作するレイヤ 2 ファイアウォールであり、接続されたデバイスへのルータ ホップとしては認識されません。

ファイアウォール モードは初期展開時にのみ設定します。ブートストラップの設定を再適用する場合、この設定は使用されません。

f) [**DNSサーバ（DNS Servers**）] フィールドに、DNS サーバのカンマ区切りのリストを入力します。

たとえば、FMCのホスト名を指定する場合、FTDは DNS を使用します。

g) （任意） [Firepower Management Center NAT ID] フィールドにパスフレーズを入力します。このパスフレーズは、新しいデバイスとしてクラスタを追加するときに FMC でも入力します。

通常は、ルーティングと認証の両方の目的で両方の IP アドレス（登録キー付き）が必要です。FMC がデバイスの IP アドレスを指定し、デバイスが FMC の IP アドレスを指定します。ただし、IP アドレスの 1 つのみがわかっている場合（ルーティング目的の最小要件）は、最初の通信用に信頼を確立して正しい登録キーを検索するために、接続の両側に一意の NAT ID を指定する必要もあります。NAT ID として、1 ～ 37 文字の任意のテキスト文字列を指定できます。FMC およびデバイスでは、初期登録の認証と承認を行うために、登録キーおよび NAT ID（IP アドレスではなく）を使用します。

h) [Fully Qualified Hostname] フィールドに、FTD デバイスの完全修飾名を入力します。

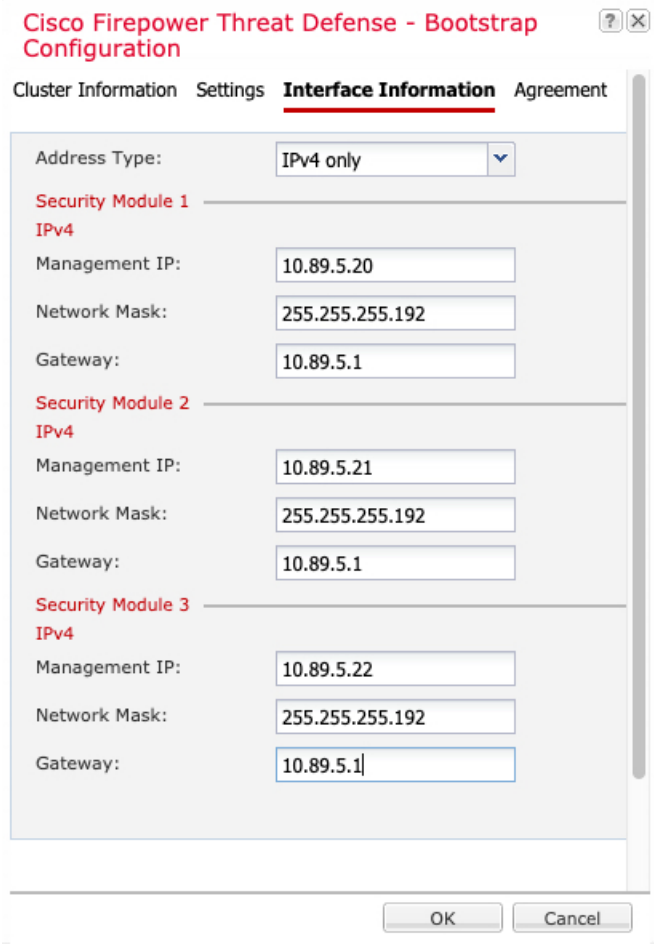
有効な文字は、a ～ z の文字、0 ～ 9 の数字、ドット（.）、およびハイフン（-）です。最大文字数は 253 です。

i) [Eventing Interface] ドロップダウン リストから、Firepowerイベントを送信するインターフェイスを選択します。指定しない場合は、管理インターフェイスが使用されます。

Firepowerイベントに使用する別のインターフェイスを指定するには、*firepower-eventing*インターフェイスとしてインターフェイスを設定する必要があります。ハードウェア バイパス 対応のインターフェイスを Eventing インターフェイスとして割り当てると、割り当てが意図的であることを確認する警告メッセージが表示されます。

ステップ 7 [Interface Information] ページで、クラスタ内の各セキュリティモジュールの管理 IP アドレスを設定します。[Address Type] ドロップダウン リストからアドレスのタイプを選択し、セキュリティ モジュールごとに次の手順を実行します。

（注） モジュールがインストールされていない場合でも、シャーシの 3 つすべてのモジュール スロットで IP アドレスを設定する必要があります。3 つすべてのモジュールを設定していないと、クラスタは機能しません。



a) [Management IP] フィールドで、IP アドレスを設定します。

モジュールごとに同じネットワークの一意の IP アドレスを指定します。

b) **ネットワーク マスク**または**プレフィックス長**を入力します。

c) **ネットワーク ゲートウェイ** アドレスを入力します。

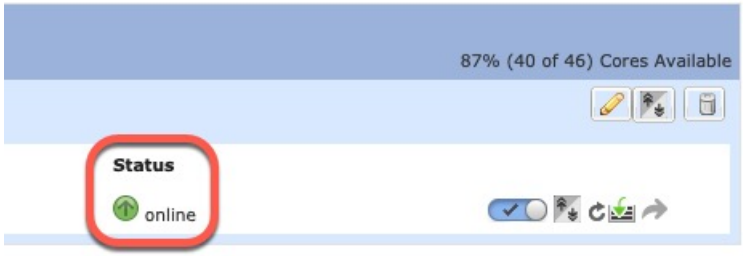
ステップ 8 [Agreement] タブで、エンド ユーザ ライセンス契約（EULA）を読み、これに同意します。

ステップ 9 [OK] をクリックして、設定ダイアログボックスを閉じます。

ステップ 10 **[Save]** をクリックします。

シャーシは、指定したソフトウェアバージョンをダウンロードし、アプリケーションインスタンスにブートストラップ設定と管理インターフェイス設定をプッシュすることで、論理デバイスを導入します。[論

理デバイス（**Logical Devices**）] ページで、新しい論理デバイスのステータスを確認します。論理デバイスの [Status] が [online] と表示されたら、アプリケーションでセキュリティ ポリシーの設定を開始できます。



ステップ 11 シャーシ間クラスタリングでは、クラスタに次のシャーシを追加します。

a) 最初のシャーシの Firepower Chassis Manager で、右上にある [Show Configuration] アイコン（ ） をクリックして、表示されるクラスタの設定をコピーします。

b) 次のシャーシの Firepower Chassis Manager に接続し、この手順に従って論理デバイスを追加します。

c) [必要な操作（I want to:）]> [既存のクラスタへの参加（Join an Existing Cluster）] を選択します。

d) **[構成のコピー（Copy config）]** チェックボックスをオンにし、**[OK]** をクリックします。このチェックボックスをオフにする場合は、手動で最初のシャーシの設定に一致するように設定を入力する必要があります。

e) [Copy Cluster Details] ボックスに、最初のシャーシのクラスタ設定を貼り付け、[OK] をクリックします。

f) 画面中央のデバイス アイコンをクリックします。クラスタ情報は大半は事前に入力済みですが、次の設定は変更する必要があります。

- **Chassis ID**：一意のシャーシ ID を入力します。
- **Site ID**：サイト間クラスタリングの場合、このシャーシのサイト ID（1 ～ 8）を入力します。この機能は、Firepower Management Center FlexConfig 機能を使用した場合にのみ構成可能です。
- **Cluster Key**：（事前に入力されていない）同じクラスタ キーを入力します。
- **Management IP**：各モジュールの管理アドレスを、他のクラスタ メンバーと同じネットワーク上に存在する一意の IP アドレスとなるように変更します。

[OK] をクリックします。

g) **[保存（Save）]** をクリックします。

ステップ 12 管理 IP アドレスを使用してマスターユニットを Firepower Management Center に追加します。

すべてのクラスタ ユニットは、Firepower Management Center に追加する前に、FXOS で正常な形式のクラスタ内に存在している必要があります。

Firepower Management Center がスレーブ ユニットを自動的に検出します。

クラスタ メンバの追加

既存のクラスタ内の FTD クラスタ メンバを追加または置き換えます。

（注） このプロシージャにおけるFXOSの手順は、新しいシャーシの追加のみに適用されます。クラスタリングがすでに有効になっている Firepower 9300 に新しいモジュールを追加する場合、モジュールは自動的に追加されます。ただし、Firepower Management Center に新しいモジュールを追加する必要があります。Firepower Management Center の手順までスキップします。

始める前に

- 置き換える場合は、Firepower Management Center から古いクラスタ メンバを削除する必要があります。新しいユニットに置き換えると、Firepower Management Center 上の新しいデバイスとみなされます。
- インターフェイスの設定は、新しいシャーシでの設定と同じである必要があります。FXOS シャーシ設定をエクスポートおよびインポートし、このプロセスを容易にすることができます。

ステップ 1 既存のクラスタ シャーシ Firepower Chassis Manager で、[Logical Devices] を選択して [Logical Devices] ページを開きます。

ステップ 2 右上の [Show Configuration] アイコン（  ） をクリックして、表示されるクラスタの設定をコピーします。

ステップ 3 新しいシャーシの Firepower Chassis Manager に接続して、**[追加（Add）]** > **[クラスタ（Cluster）]|[デバイスの追加（Add Device）]** をクリックします。

ステップ 4 [Device Name] に論理デバイスの名前を入力します。

ステップ 5 [Template] では、[Cisco Firepower Threat Defense] を選択します。

ステップ 6 [Image Version] では、FTD ソフトウェア バージョンを選択します。

ステップ 7 [デバイス モード（Device Mode）] では、[クラスタ（Cluster）] オプション ボタンをクリックします。

ステップ 8 [Join an Existing Cluster] を選択します。

ステップ 9 **[構成のコピー（Copy config）]** チェックボックスをオンにし、**[OK]** をクリックします。このチェックボックスをオフにする場合は、手動で最初のシャーシの設定に一致するように設定を入力する必要があります。

ステップ 10 [Copy Cluster Details] ボックスに、最初のシャーシのクラスタ設定を貼り付け、[OK] をクリックします。

ステップ 11 画面中央のデバイス アイコンをクリックします。クラスタ情報は大半は事前に入力済みですが、次の設定は変更する必要があります。

- **Chassis ID**：一意のシャーシ ID を入力します。
- **Site ID**：サイト間クラスタリングの場合、このシャーシのサイト ID（1～8）を入力します。この機能は、Firepower Management Center FlexConfig 機能を使用した場合にのみ構成可能です。
- **Cluster Key**：（事前に入力されていない）同じクラスタ キーを入力します。
- **Management IP**：各モジュールの管理アドレスを、他のクラスタ メンバーと同じネットワーク上に存在する一意の IP アドレスとなるように変更します。

[OK] をクリックします。

ステップ 12 [保存（Save）] をクリックします。

ステップ 13 Firepower Management Center で、**[デバイス（Devices）] > [デバイス管理（Device Management）]** を選択してから **[追加（Add）] > [デバイスの追加（Add Device）]** を選択して、新しい論理デバイスを追加します。

ステップ 14 [追加（Add）] > [クラスタの追加（Add Cluster）] を選択します。 >

ステップ 15 ドロップダウン リストから現在の [マスター（Master）] デバイスを選択します。

クラスタにすでに含まれているマスター デバイスを選択した場合、既存のクラスタの名前が自動入力され、[Slave Devices] ボックスに選択可能なすべてのスレーブ デバイスが表示されます。これには、FMC に追加したばかりの新しいユニットが含まれます。

ステップ 16 [追加（Add）] をクリックし、次に [導入（Deploy）] をクリックします。

クラスタは新しいメンバを追加して更新されます。

FMC：クラスタの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	Firepower 4100 および 9300 上の FTD	任意	Access Admin Administrator Network Admin

クラスタ ユニットのいずれかを新しいデバイスとして Firepower Management Center に追加します。FMC は、他のすべてのクラスタ メンバーを自動検出します。

始める前に

- クラスタを追加するためのこの方法には、Firepower Threat Defense バージョン 6.2 以降が必要です。以前のバージョンのデバイスを管理する必要がある場合には、そのバージョンの Firepower Management Center コンフィギュレーション ガイドを参照してください。

- クラスタを Management Center に追加する前に、すべてのクラスタ ユニットが FXOS 上の正常に形成されたクラスタ内に存在している必要があります。また、どのユニットがマスター ユニットかを確認することも必要です。Firepower Chassis Manager の [論理デバイス（Logical Devices）] 画面を参照するか、または Firepower Threat Defense の **show cluster info** コマンドを使用します。

ステップ 1 FMC で、**[デバイス（Devices）] > [デバイス管理（Device Management）]** の順に選択してから、**[追加（Add）] > [デバイスの追加（Add Device）]** の順に選択して、クラスタを展開したときに割り当てた管理 IP アドレスを使用して、クラスタ ユニットのいずれかを追加します。

最適なパフォーマンスを得るため、マスターユニットの追加を推奨しますが、任意のユニットを追加できます。

FMC は、マスター ユニットを識別して登録した後、すべてのスレーブ ユニットを登録します。マスターユニットが正常に登録されていない場合、クラスタは追加されません。クラスタがシャーシで稼働状態になかったか、その他の接続問題が原因で、登録エラーが発生する場合があります。こうした状況では、クラスタ ユニットを再度追加することをお勧めします。

[デバイス（Devices）] > [デバイス管理（Device Management）] ページにクラスタ名が表示されます。クラスタを展開して、クラスタ ユニットを表示します。現在登録されているユニットには、ロードアイコンが表示されます。クラスタ ユニットの登録をモニタするには、システム ステータス アイコンをクリックし、[タスク（Tasks）] タブを選択します。FMC は、ユニットの登録ごとにクラスタ登録タスクを更新します。いずれかのユニットの登録に失敗した場合には、クラスタ メンバーの照合 （939 ページ） を参照してください。

ステップ 2 デバイス固有の設定を行うには、クラスタの編集アイコン（  ）をクリックします。クラスタを全体として設定することはできますが、クラスタのメンバー ユニットは設定できません。

ステップ 3 **[デバイス（Devices）] > [デバイス管理（Device Management）] > [クラスタ（Cluster）]** タブに、[全般（General）]、[ライセンス（License）]、[システム（System）]、および [ヘルス（Health）] の設定が表示されます。

- [全般（General）] 領域で、[現在のクラスタの概要（Current Cluster Summary）] リンクをクリックして、[クラスタ ステータス（Cluster Status）] ダイアログ ボックスを開きます。[クラスタ ステータス（Cluster Status）] ダイアログ ボックスで、[照合（Reconcile）] をクリックしてスレーブの登録を再試行することもできます。
- ライセンス付与資格を設定するには、[ライセンス（License）] 領域で [Edit] アイコン（  ） をクリックします。

ステップ 4 **[デバイス（Devices）] > [デバイス管理（Device Management）] > [デバイス（Devices）]** タブの右上のドロップダウン メニューで、クラスタ内の各メンバーを選択できます。

デバイス設定で管理 IP アドレスを変更する場合、FMC で新しいアドレスを一致させてネットワーク上のデバイスに到達できるようにし、[管理（Management）] 領域で [ホスト（Host）] アドレスを編集します。

FMC：データ インターフェイスと診断インターフェイスの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	Firepower 4100 および 9300 上の Firepower Threat Defense	任意	Access Admin Administrator Network Admin

この手順では、FXOS にクラスタを展開したときにクラスタに割り当てられた各データ インターフェイスの基本的なパラメータを設定します。シャーシ間クラスタリングの場合、データ インターフェイスは常にスパンド EtherChannel インターフェイスです。個別インターフェイスとして実行できる唯一のインターフェイスである診断インターフェイスを設定することもできます。

（注） シャーシ間クラスタリングにスパンド EtherChannel を使用している場合、クラスタリングが完全に有効になるまで、ポートチャネルインターフェイスは起動しません。この要件により、クラスタのアクティブではないユニットにトラフィックが転送されるのが防がれます。

ステップ 1 **[デバイス（Devices）] > [デバイス管理（Device Management）]** を選択し、クラスタの横にある [Edit] アイコン（✎） をクリックします。

ステップ 2 [インターフェイス（Interfaces）] タブをクリックします。

ステップ 3 （任意）インターフェイスに VLAN サブインターフェイスを設定します。この手順の残りの部分は、サブインターフェイスに適用されます。サブインターフェイスの追加 （805 ページ）を参照してください。

ステップ 4 データ インターフェイスの [Edit] アイコン（✎） をクリックします。

ステップ 5 シャーシ間クラスタの場合は、EtherChannel の手動グローバル MAC アドレスを設定します。

潜在的なネットワークの接続問題を回避するために、スパンド EtherChannel にはグローバル MAC アドレスを設定する必要があります。MAC アドレスが手動設定されている場合、その MAC アドレスは現在のマスター ユニットに留まります。MAC アドレスを設定していない場合に、マスター ユニットが変更された場合、新しいマスター ユニットはインターフェイスに新しい MAC アドレスを使用します。これにより、一時的なネットワークの停止が発生する可能性があります。

a) [詳細（Advanced）] タブをクリックします。
[情報（Information）] タブが選択されています。

b) [アクティブな MAC アドレス（Active MAC Address）] フィールドに、MAC アドレスを H.H.H 形式で設定します。H は 16 ビットの 16 進数です。

たとえば、MAC アドレスが 00-0C-F1-42-4C-DE の場合、000C.F142.4CDE と入力します。MAC アドレスはマルチキャスト ビット セットを持つことはできません。つまり、左から 2 番目の 16 進数字を奇数にすることはできません。

[スタンバイ MAC アドレス（Standby MAC Address）] は設定しないでください。無視されます。

ステップ 6 ルーテッド モードのインターフェイスの設定（810 ページ）またはの□ブリッジ グループ インターフェイスの設定（813 ページ）に従い、名前、IP アドレス、およびその他のパラメータを設定します。

ステップ 7 [OK] をクリックします。他のデータ インターフェイスについても前述の手順を繰り返します。

ステップ 8 （任意） 診断インターフェイスを設定します。

診断インターフェイスは、個別インターフェイス モードで実行できる唯一のインターフェイスです。syslog メッセージや SNMP などに、このインターフェイスを使用できます。

a) **[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [アドレス プール（Address Pools）]** を選択して、IPv4 または IPv6 アドレス プールを追加します。アドレス プール（633 ページ）を参照してください。

最低でも、クラスタ内のユニット数と同じ数のアドレスが含まれるようにしてください。仮想 IP アドレスはこのプールには含まれませんが、同一ネットワーク上に存在している必要があります。各ユニットに割り当てられる正確なローカル アドレスを事前に決定することはできません。

b) **[デバイス（Devices）] > [デバイス管理（Device Management）] > [インターフェイス（Interfaces）]** で、診断インターフェイスの [Edit] アイコン（✎） をクリックします。

c) [IPv4] タブで、[仮想 IP アドレス（Virtual IP Address）] とマスクを入力します。この IP アドレスは、そのクラスタの固定アドレスで、常に現在のマスター ユニットに属します。

d) 作成したアドレス プールを [IPv4 アドレス プール（IPv4 Address Pool）] ドロップダウン リストから選択します。

e) [IPv6] > [基本（Basic）] タブで、作成したアドレス プールを [IPv6 アドレス プール（IPv6 Address Pool）] ドロップダウンリストから選択します。

f) 通常どおり、他のインターフェイス設定を行います。

ステップ 9 **[Save（保存）]** をクリックします。

これで、[Deploy] をクリックして割り当てられているデバイスにポリシーを展開できます。変更はポリシーを導入するまで有効になりません。

FXOS：クラスタ メンバの削除

ここでは、メンバを一時的に、またはクラスタから永続的に削除する方法について説明します。

一時的な削除

たとえば、ハードウェアまたはネットワークの障害が原因で、クラスタ メンバはクラスタから自動的に削除されます。この削除は、条件が修正されるまでの一時的なものであるため、クラスタに再参加できます。また、手動でクラスタリングを無効にすることもできます。

デバイスが現在クラスタ内にあるかどうかを確認するには、Firepower Chassis Manager の [Logical Devices] ページで、のクラスタ ステータスを確認します。

FMC を使用した FTD では、FMC デバイス リストにデバイスを残し、クラスタリングを再度有効にした後にすべての機能を再開できるようにする必要があります。

- アプリケーションでのクラスタリングの無効化：アプリケーション CLI を使用してクラスタリングを無効にすることができます。**cluster remove unit** *name* コマンドを入力して、ログインしているユニット以外のすべてのユニットを削除します。ブートストラップ コンフィギュレーションは変更されず、マスターユニットから最後に同期されたコンフィギュレーションもそのままであるので、コンフィギュレーションを失わずに後でそのユニットを再度追加できます。マスター ユニットを削除するためにスレーブ ユニットでこのコマンドを入力した場合は、新しいマスター ユニットが選定されます。

  デバイスが非アクティブになると、すべてのデータ インターフェイスがシャットダウンされます。管理専用インターフェイスのみがトラフィックを送受信できます。トラフィック フローを再開するには、クラスタリングを再度有効にします。管理インターフェイスは、そのユニットがブートストラップ設定から受け取った IP アドレスを使用して引き続き稼働状態となります。ただし、リロードしてもユニットがクラスタ内でまだアクティブではない場合、管理インターフェイスは無効になります。

  クラスタリングを再度有効にするには、FTD で **cluster enable** を入力します。

- アプリケーション インスタンスの無効化：Firepower Chassis Manager の [Logical Devices] ページで [Disable] スライダ（ ） をクリックします。[Enable] スライダ（ ） を使用して後で再度有効にすることができます。

- セキュリティ モジュール/エンジン のシャットダウン：Firepower Chassis Manager の [Module/Engine] ページで、[Power Off] アイコン（ ） をクリックします。

- シャーシのシャットダウン：Firepower Chassis Manager の [Overview] ページで、 [Shut Down] アイコン（ ） をクリックします。

完全な削除

次の方法を使用して、クラスタ メンバを完全に削除できます。

FMC を使用した FTD の場合、シャーシでクラスタリングを無効にした後でユニットを FMC デバイス リストから削除してください。

- 論理デバイスの削除：Firepower Chassis Manager の [Logical Devices] ページで、[Delete] アイコン（）をクリックします。その後、スタンドアロンの論理デバイスや新しいクラスタを展開したり、同じクラスタに新しい論理デバイスを追加したりすることもできます。
- サービスからのシャーシまたはセキュリティ モジュールの削除：サービスからデバイスを削除する場合は、交換用ハードウェアをクラスタの新しいメンバーとして追加できます。

FMC：クラスタ メンバーの管理

クラスタを導入した後は、コンフィギュレーションを変更し、クラスタ メンバを管理できます。

新規クラスタ メンバーの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	Firepower 4100 および 9300 上の Firepower Threat Defense	任意	Access Admin Administrator Network Admin

FXOS に新しいクラスタ メンバーを追加すると、Firepower Management Center によりメンバーが自動的に追加されます。

始める前に

- インターフェイスの設定が他のシャーシと交換用ユニットで同じ設定になっていることを確認します。

ステップ 1 FXOS のクラスタに新しいユニットを追加します。『FXOS コンフィギュレーション ガイド』を参照してください。

新しいユニットがクラスタに追加されるまで待機します。Firepower Chassis Manager の [論理デバイス（Logical Devices）] 画面を参照するか、または Firepower Threat Defense の **show cluster info** コマンドを使用してクラスタ ステータスを表示します。

ステップ 2 新しいクラスタ メンバーは自動的に追加されます。交換用ユニットの登録状況をモニタするには、次のように表示します。

- [クラスタ ステータス（Cluster Status）] ダイアログボックス（**[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > **[クラスタ（Cluster）]** タブ > [全般（General）] 領域 > [現在のクラスタの概要（Current Cluster Summary）] リンク）で、シャーシ上でクラスタに追加中のユニットに「クラスタに追加中...（Joining cluster...）」と示されます。クラスタに追加された後に、FMC はこれの登録を試み、ステータスが「登録可能（Available for Registration）」に変わります。登録が完了すると、ス

テータスが「同期状態（In Sync）」に変わります。登録に失敗すると、ユニットは「登録可能（Available for Registration）」の状態に留まります。この場合、[照合（Reconcile）] をクリックして再登録を強制します。

- システム ステータス アイコン > [タスク（Tasks）] タブ：FMC にすべての登録イベントとエラーが表示されます。
- **[デバイス（Devices）] > [デバイス管理（Device Management）]**：デバイスの一覧表示ページでクラスタを展開して、左側にロードアイコンがある場合は、ユニットが登録中であることを示しています。

クラスタ メンバーの置換

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	Firepower 4100 および 9300 上の FTD	任意	Access Admin Administrator Network Admin

既存クラスタ内のクラスタ メンバーを置き換えることができます。Firepower Management Center は交換ユニットを自動検出します。ただし、Firepower Management Center 内の古いクラスタ メンバーは手動で削除する必要があります。また、この手順は再初期化したユニットにも適用されます。その場合は、ハードウェアが同じでも新しいメンバーとして表示されます。

始める前に

- インターフェイス設定が他のシャーシに関する交換ユニットと同じであることを確認します。

ステップ 1 新しいシャーシの場合、可能であれば、FXOS 内の古い シャーシの設定をバックアップして復元します。

Firepower 9300 のモジュールを交換する場合は、次の手順を実行する必要はありません。

古いシャーシのバックアップ FXOS 設定がない場合は、最初に新規クラスタ メンバーの追加（936 ページ）の手順を実行します。

以下のすべての手順については、FXOS コンフィギュレーション ガイド [英語] を参照してください。

a) 設定のエクスポート機能を使用して、Firepower 4100/9300 シャーシの論理デバイスとプラットフォームの構成時の設定を含んでいる XML ファイルをエクスポートします。
b) 交換用シャーシに設定ファイルをインポートします。
c) ライセンス契約に同意します。
d) 必要に応じて、論理デバイスのアプリケーション インスタンス バージョンをアップグレードして、残りのクラスタと一致させます。

ステップ 2 Firepower Management Center で、**[デバイス（Devices）] > [デバイス管理（Device Management）]** を選択し、古いユニットの横にある [Delete] アイコン（） をクリックします。

ステップ 3 ユニットを削除することを確認します。

ユニットがクラスタから削除され、FMC デバイス リストからも削除されます。

ステップ 4 新しいクラスタ メンバーまたは再初期化したクラスタ メンバーは自動的に追加されます。交換用ユニットの登録状況をモニタするには、次のように表示します。

- [クラスタ ステータス（Cluster Status）] ダイアログボックス（**[デバイス（Devices）] > [デバイス管理（Device Management）] > [クラスタ（Cluster）]** タブ > [全般（General）] 領域 > [現在のクラスタの概要（Current Cluster Summary）] リンク）で、シャーシ上でクラスタに追加中のユニットに「クラスタに追加中...（Joining cluster...）」と示されます。クラスタに追加された後に、FMC はこれの登録を試み、ステータスが「登録可能（Available for Registration）」に変わります。登録が完了すると、ステータスが「同期状態（In Sync）」に変わります。登録に失敗すると、ユニットは「登録可能（Available for Registration）」の状態に留まります。この場合、[照合（Reconcile）] をクリックして再登録を強制します。
- システム ステータス アイコン > [タスク（Tasks）] タブ：FMC にすべての登録イベントとエラーが表示されます。
- **[デバイス（Devices）] > [デバイス管理（Device Management）]**：デバイスの一覧表示ページでクラスタを展開して、左側にロードアイコンがある場合は、ユニットが登録中であることを示しています。

スレーブ メンバーの削除

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	Firepower 4100 および 9300 上の FTD	任意	Access Admin Administrator Network Admin

クラスタ メンバーを完全に削除する必要がある場合（たとえば、Firepower 9300 でモジュールを削除する場合、またはシャーシを削除する場合）は、FMC からメンバーを削除する必要があります。

始める前に

メンバーが正常なクラスタの一部である場合、またはメンバーを一時的に無効にするだけの場合は、メンバーを削除しないでください。FXOS のクラスタから完全に削除するには、FXOS：クラスタ メンバの削除 （934 ページ）を参照してください。FMC から削除した後もメンバーがクラスタの一部である場合、トラフィックは引き続き通過し、FMC で管理不能なマスター ユニットになることもあります。

ステップ 1 ユニットが FMC から削除できる状態であることを確認します。

a) **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択して、クラスタの編集アイコン（）をクリックします。

b) **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > **[クラスタ（Cluster）]** タブ > [全般（General）] 領域で、[現在のクラスタの概要（Current Cluster Summary）] リンクをクリックして [クラスタ ステータス（Cluster Status）] ダイアログボックスを開きます。

c) 削除するデバイスが「削除可能」状態であることを確認します。

ステータスが古い場合は、[照合（Reconcile）] をクリックして強制的に更新します。

ステップ 2 FMC で、**[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択し、スレーブ ユニットの横にある [Delete] アイコン（） をクリックします。

ステップ 3 ユニットを削除することを確認します。

ユニットがクラスタから削除され、FMC デバイス リストからも削除されます。

クラスタ メンバーの照合

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	Firepower 4100 および 9300 上の Firepower Threat Defense	任意	Access Admin Administrator Network Admin

クラスタ メンバーの登録に失敗した場合、シャーシから Firepower Management Center に対してクラスタ メンバーシップを照合することができます。たとえば、FMC が特定のプロセスで占領されているか、またはネットワークに問題がある場合、スレーブ ユニットの登録に失敗することがあります。

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択し、クラスタの [Edit] アイコン（）をクリックします。

ステップ 2 [クラスタ（Cluster）] タブ > [全般（General）] 領域で、[現在のクラスタの概要（Current Cluster Summary）] リンクをクリックして [クラスタ ステータス（Cluster Status）] ダイアログボックスを開きます。

ステップ 3 [照合（Reconcile）] をクリックします。

クラスタ ステータスの詳細については、FMC：クラスタのモニタリング （941 ページ）を参照してください。

メンバーの非アクティブ化

ログインしているユニット以外のメンバーを非アクティブにするには、FTD CLI で次のステップを実行します。この手順の目的は、メンバーを一時的に非アクティブにし、FMC のデバイス リスト内にユニットを保持する必要があります。

（注） ユニットが非アクティブになると、すべてのデータインターフェイスがシャットダウンされます。管理インターフェイスのみがトラフィックを送受信できます。トラフィック フローを再開するには、クラスタリングを再度有効にします。管理インターフェイスは、そのユニットがブートストラップ設定から受け取った IP アドレスを使用して引き続き稼働状態となります。ただし、リロードする場合、クラスタでユニットがまだ非アクティブになっていると、管理インターフェイスは無効になります。それ以降のコンフィギュレーション作業には、コンソールを使用する必要があります。

ステップ 1 FTD CLI にアクセスします。

ステップ 2 ユニットをクラスタから削除します。

cluster remove unit *unit_name*

ブートストラップ コンフィギュレーションは変更されず、マスター ユニットから最後に同期されたコンフィギュレーションもそのままになるので、コンフィギュレーションを失わずに後でそのユニットを再度追加できます。マスターユニットを削除するためにスレーブユニットでこのコマンドを入力した場合は、新しいマスター ユニットが選定されます。

メンバ名を一覧表示するには、**cluster remove unit ?** と入力するか、**show cluster info** コマンドを入力します。

例：

```
> cluster remove unit ?

Current active units in the cluster:
ftd1
ftd2
ftd3

> cluster remove unit ftd2
WARNING: Clustering will be disabled on unit ftd2. To bring it back
to the cluster please logon to that unit and re-enable clustering
```

ステップ 3 クラスタリングを再び有効にするには、クラスタへの再参加 （941 ページ）を参照してください。

クラスタへの再参加

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	Firepower 4100 および 9300 上の Firepower Threat Defense	任意	Access Admin Administrator Network Admin

ユニット（障害が発生したインターフェイスなど）がクラスタから削除された場合は、そのユニットのCLIにアクセスして、手動でクラスタに再参加させる必要があります。クラスタへの再参加を試行する前に、障害が解決されていることを確認します。クラスタからユニットが削除される理由の詳細については、クラスタへの再参加 （944 ページ）を参照してください。

ステップ 1 クラスタに再参加させる必要のあるユニットの CLI に、コンソール ポートからアクセスするか、管理インターフェイスへの SSH を使用してアクセスします。ユーザ名 **admin** と、初期セットアップ時に設定したパスワードを使用してログインします。

ステップ 2 クラスタリングを有効にします。

cluster enable

FMC：クラスタのモニタリング

クラスタのモニタリングは、Firepower Management Center および FTD CLI で実行できます。

- **[デバイス（Devices）] > [デバイス管理（Device Management）] > [クラスタ（Cluster）]** タブ > [一般（General）] エリア > [現在のクラスタの概要（Current Cluster Summary）] リンク > [クラスタのステータス（Cluster Status）] ダイアログボックス。

  クラスタ メンバ状態には、以下が含まれます。

  - 同期中（In Sync）：装置は FMC に登録されています。
  - 登録可能（Available for Registration）：装置はクラスタの一部ですが、まだ FMC に登録されていません。装置が登録に失敗した場合、[照合（Reconcile）] クリックして登録を再試行することができます。
  - 削除可能（Available for Deletion）：装置は FMC に登録されていますが、クラスタの一部ではなく、削除する必要があります。
  - クラスタに参加中（Joining cluster）：装置がシャーシ上でクラスタに参加していますが、参加は完了していません。参加後に FMC に登録されます。

  このダイアログボックスを更新するには、閉じてから再度開きます。

- システム ステータス アイコン > [タスク（Tasks）] タブ。

  [タスク（Tasks）] タブには、装置の登録ごとに、クラスタ登録タスクの更新が表示されます。

- **[デバイス（Devices）] > [デバイス管理（Device Management）] >** *cluster_name*。

  デバイスの一覧表示ページでクラスタを展開すると、IP アドレスの隣の「（master）」と表示されるマスター装置を含めて、すべてのメンバ装置を表示できます。登録中の装置には、ロード中のアイコンが表示されます。

- **show cluster** {**access-list** [*acl_name*] | **conn** [**count**] | **cpu** [**usage**] | **history** | **interface-mode** | **memory** | **resource usage** | **service-policy** | **traffic** | **xlate count**}

  クラスタ全体の集約データまたはその他の情報を表示するには、**show cluster** コマンドを使用します。

- **show cluster info** [**auto-join** | **clients** | **conn-distribution** | **flow-mobility counters** | **goid** [*options*] | **health** | **incompatible-config** | **loadbalance** | **old-members** | **packet-distribution** | **trace** [*options*] | **transport** { **asp** | **cp**}]

  クラスタ情報を表示するには、**show cluster info** コマンドを使用します。

クラスタリングの参考資料

このセクションには、クラスタリングの動作に関する詳細情報が含まれます。

パフォーマンス スケーリング係数

複数のユニットをクラスタに結合した場合、期待できる合計クラスタ パフォーマンスの概算値は次のようになります。

- TCP または CPS の合計スループットの 80 %
- UDP の合計スループットの 90 %
- トラフィックの混在に応じて、イーサネット MIX（EMIX）の合計スループットの 60 %。

たとえば、TCP スループットについては、3 つのモジュールを備えた Firepower 9300 は、単独で動作している場合、約 135 Gbps の実際のファイアウォール トラフィックを処理できます。2 シャーシの場合、最大スループットの合計は 270 Gbps（2 シャーシ X 135 Gbps）の約 80 %、つまり 216 Gbps です。

マスター ユニット選定

クラスタのメンバは、クラスタ制御リンクを介して通信してマスターユニットを選定します。方法は次のとおりです。

1. クラスタを展開すると、各ユニットは選定要求を 3 秒ごとにブロードキャストします。

2. プライオリティの高い他のユニットがこの選定要求に応答します。プライオリティはクラスタの展開時に設定され、設定の変更はできません。
3. 45 秒経過しても、プライオリティの高い他のユニットからの応答を受信していない場合は、そのユニットがマスターになります。
4. 後からクラスタに参加したユニットのプライオリティの方が高い場合でも、そのユニットが自動的にマスター ユニットになることはありません。既存のマスター ユニットは常にマスターのままです。ただし、マスターユニットが応答を停止すると、その時点で新しいマスター ユニットが選定されます。

（注） 特定のユニットを手動で強制的にマスターにすることができます。中央集中型機能については、マスターユニット変更を強制するとすべての接続がドロップされるので、新しいマスターユニット上で接続を再確立する必要があります。

クラスタ内のハイ アベイラビリティ

クラスタリングは、シャーシ、ユニットとインターフェイスの正常性を監視し、ユニット間で接続状態を複製することにより、ハイ アベイラビリティを提供します。

シャーシアプリケーションのモニタリング

シャーシアプリケーションのヘルス モニタリングは常に有効になっています。Firepower 4100/9300 シャーシスーパーバイザはFirepower Threat Defenseアプリケーションを定期的に確認します（毎秒）。Firepower Threat Defense デバイスが作動中で、Firepower 4100/9300 シャーシスーパーバイザと 3 秒間通信できなければFirepower Threat Defense デバイスは syslog メッセージを生成して、クラスタを離れます。

Firepower 4100/9300 シャーシスーパーバイザが 45 秒後にアプリケーションと通信できなければ、Firepower Threat Defense デバイスをリロードします。Firepower Threat Defense デバイスがスーパーバイザと通信できなければ、自身をクラスタから削除します。

ユニットのヘルス モニタリング

マスター ユニットは、各スレーブ ユニットをモニタするために、クラスタ制御リンクを介してキープアライブ メッセージを定期的に送信します。各スレーブ ユニットは、同じメカニズムを使用してマスターユニットをモニタします。ユニットの健全性チェックが失敗すると、ユニットはクラスタから削除されます。

インターフェイス モニタリング

各ユニットは、使用中のすべてのハードウェア インターフェイスのリンク ステータスをモニタし、ステータス変更をマスターユニットに報告します。シャーシ間クラスタリングでは、スパンド EtherChannel はクラスタ Link Aggregation Control Protocol（cLACP）を使用します。各シャーシはリンク ステータスと cLACP プロトコル メッセージをモニタして EtherChannel で

ポートがアクティブであるかどうかを判別し、インターフェイスがダウンしている場合には Firepower Threat Defense アプリケーションに通知します。ヘルス モニタリングを有効にすると、デフォルトではすべての物理インターフェイスがモニタされます（EtherChannel インターフェイスのメイン EtherChannel を含む）。アップ状態の指名されたインターフェイスのみモニタできます。たとえば、名前付き EtherChannel がクラスタから削除される前に、EtherChannel のすべてのメンバー ポートがエラーとなる必要があります。

あるモニタ対象のインターフェイスが、特定のユニット上では障害が発生したが、別のユニットではアクティブの場合は、そのユニットはクラスタから削除されます。Firepower Threat Defense デバイス がメンバーをクラスタから削除するまでの時間は、そのユニットが確立済みメンバーであるか、またはクラスタに参加しようとしているかによって異なります。Firepower Threat Defense デバイス は、ユニットがクラスタに参加する最初の 90 秒間はインターフェイスを監視ししません。この間にインターフェイスのステータスが変化しても、Firepower Threat Defense デバイス はクラスタから削除されません。設定済みのメンバーの場合は、500 ミリ秒後にユニットが削除されます

シャーシ間クラスタリングでは、クラスタから EtherChannel を追加または削除した場合、各シャーシに変更を加えられるように、インターフェイス ヘルス モニタリングは 95 秒間中断されます。

障害後のステータス

クラスタ内のユニットで障害が発生したときに、そのユニットでホスティングされている接続は他のユニットにシームレスに移管されます。トラフィック フローのステート情報は、クラスタ制御リンクを介して共有されます。

マスターユニットで障害が発生した場合は、そのクラスタの他のメンバーのうち、プライオリティが最高（番号が最小）のものがマスター ユニットになります。

障害イベントに応じて、Firepower Threat Defense デバイス は自動的にクラスタへの再参加を試みます。

（注） Firepower Threat Defense デバイス が非アクティブになり、クラスタへの自動再参加に失敗すると、すべてのデータ インターフェイスがシャットダウンされます。管理/診断インターフェイスのみがトラフィックを送受信できます。

クラスタへの再参加

クラスタ メンバがクラスタから削除された後、クラスタに再参加できる方法は、削除された理由によって異なります。

- クラスタ制御リンクの障害：クラスタ制御リンクの問題を解決した後、クラスタリングを再び有効にして、手動でクラスタに再参加する必要があります。
- データ インターフェイスの障害：FTD アプリケーションは自動的に最初は 5 分後、次に 10 分後、最終的に 20 分後に再参加を試みます。20 分後に参加できない場合、FTD アプリ

ケーションはクラスタリングを無効にします。データインターフェイスの問題を解決した後、手動でクラスタリングを有効にする必要があります。

- ユニットの障害：ユニットがヘルスチェック失敗のためクラスタから削除された場合、クラスタへの再参加は失敗の原因によって異なります。たとえば、一時的な電源障害の場合は、クラスタ制御リンクが稼働している限り、ユニットは再起動するとクラスタに再参加します。FTD アプリケーションは 5 秒ごとにクラスタへの再参加を試みます。
- シャーシアプリケーション通信の障害：FTDアプリケーションはシャーシアプリケーションの状態が回復したことを検出すると、自動的にクラスタへの再参加を試みます。
- 内部エラー：内部エラーには、アプリケーション同期のタイムアウト、一貫性のないアプリケーション ステータスなどがあります。

データ パス接続状態の複製

どの接続にも、1 つのオーナーおよび少なくとも 1 つのバックアップ オーナーがクラスタ内にあります。バックアップ オーナーは、障害が発生しても接続を引き継ぎません。代わりに、TCP/UDP のステート情報を保存します。これは、障害発生時に接続が新しいオーナーにシームレスに移管されるようにするためです。バックアップオーナーは通常ディレクタでもあります。

トラフィックの中には、TCP または UDP レイヤよりも上のステート情報を必要とするものがあります。この種類のトラフィックに対するクラスタリングのサポートの可否については、次の表を参照してください。

表 *79*：クラスタ全体で複製される機能

Traffic	状態のサポート	注意
Up time	Yes	システム アップ タイムをトラッキングします。
ARP Table	Yes	—
MAC アドレス テーブル	Yes	—
ユーザ アイデンティティ	Yes	—
IPv6 ネイバー データベース	Yes	—
ダイナミック ルーティング	Yes	—
SNMP エンジン ID	なし	—
集中型 VPN（サイト間）	なし	VPN セッションは、マスターユニットで障害が発生すると切断されます。

クラスタが接続を管理する方法

接続をクラスタの複数のメンバにロードバランスできます。接続のロールにより、通常動作時とハイ アベイラビリティ状況時の接続の処理方法が決まります。

接続のロール

接続ごとに定義された次のロールを参照してください。

- オーナー：通常、最初に接続を受信するユニット。オーナーは、TCP 状態を保持し、パケットを処理します。1 つの接続に対してオーナーは 1 つだけです。元のオーナーに障害が発生すると、新しいユニットが接続からパケットを受信したときにディレクタがこれらのユニットの新しいオーナーを選択します。
- バックアップ オーナー：オーナーから受信した TCP/UDP ステート情報を格納するユニット。これにより、障害が発生した場合に新しいオーナーにシームレスに接続を転送できます。バックアップ オーナーは、障害発生時に接続を引き継ぎません。オーナーが使用不可能になった場合は、その接続からパケットを受け取る最初のユニット（ロードバランシングに基づく）がバックアップ オーナーに問い合わせて、関連するステート情報を取得し、これでそのユニットが新しいオーナーになることができます。

  ディレクタ（下記参照）がオーナーと同じユニットでない限り、ディレクタはバックアップ オーナーでもあります。オーナーがディレクタとして自分自身を選択すると、別のバックアップ オーナーが選択されます。

  1 台のシャーシに最大 3 つのクラスタ ユニットを搭載できる Firepower 9300 のシャーシ間クラスタリングでは、バックアップ オーナーがオーナーと同じシャーシにある場合、シャーシ障害からフローを保護するために、別のシャーシから追加のバックアップ オーナーが選択されます。
- ディレクタ：フォワーダからのオーナールックアップ要求を処理するユニット。オーナーが新しい接続を受信すると、オーナーは、送信元/宛先 IP アドレスおよび ポートのハッシュに基づいてディレクタを選択し、新しい接続を登録するためにメッセージをそのディレクタに送信します。パケットがオーナー以外のユニットに到着した場合は、そのユニットはどのユニットがオーナーかをディレクタに問い合わせます。これで、パケットを転送できるようになります。1 つの接続に対してディレクタは 1 つだけです。ディレクタが失敗すると、オーナーは新しいディレクタを選択します。

  ディレクタがオーナーと同じユニットでない限り、ディレクタはバックアップ オーナーでもあります（上記参照）。オーナーがディレクタとして自分自身を選択すると、別のバックアップ オーナーが選択されます。
- フォワーダ：パケットをオーナーに転送するユニット。フォワーダが接続のパケットを受信したときに、その接続のオーナーが自分ではない場合は、フォワーダはディレクタにオーナーを問い合わせてから、そのオーナーへのフローを確立します。これは、この接続に関してフォワーダが受信するその他のパケット用です。ディレクタは、フォワーダにもなることができます。フォワーダが SYN-ACK パケットを受信した場合、フォワーダはパケットの SYN クッキーからオーナーを直接取得できるので、ディレクタに問い合わせる必要がないことに注意してください（TCP シーケンスのランダム化をディセーブ ルにし

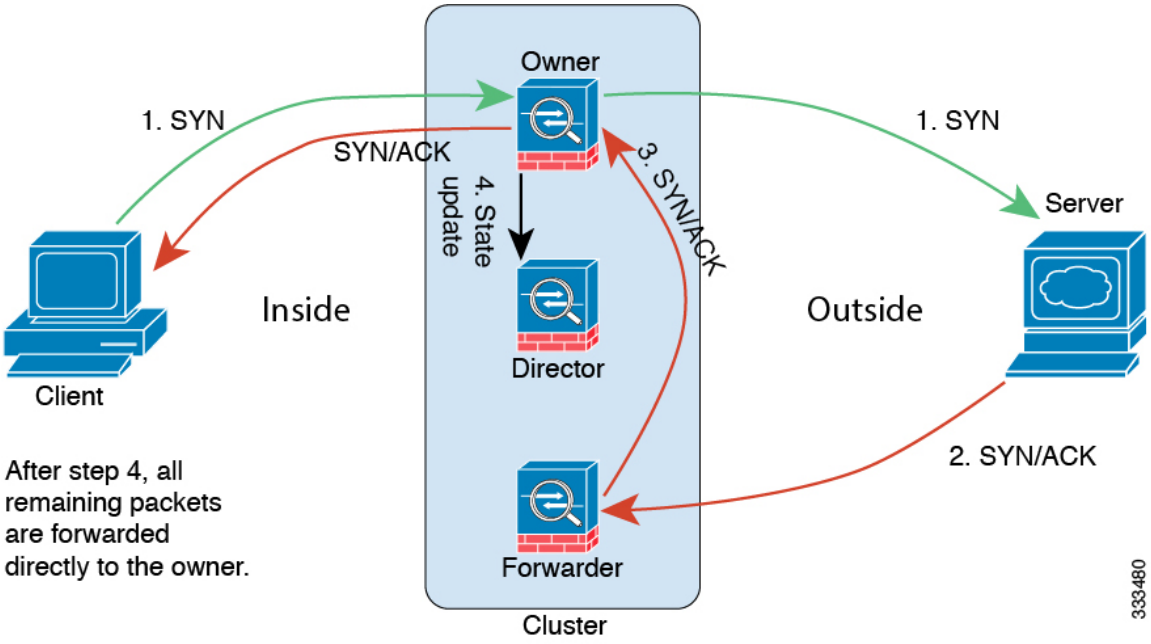
た場合は、SYN Cookie は使用されないので、ディレクタへの問い合わせが必要です）。存続期間が短いフロー（たとえばDNSやICMP）の場合は、フォワーダは問い合わせの代わりにパケットを即座にディレクタに送信し、ディレクタがそのパケットをオーナーに送信します。1 つの接続に対して、複数のフォワーダが存在できます。最も効率的なスループットを実現できるのは、フォワーダが 1 つもなく、接続のすべてのパケットをオーナーが受信するという、優れたロードバランシング方法が使用されている場合です。

新しい接続の所有権

新しい接続がロードバランシング経由でクラスタのメンバに送信される場合は、そのユニットがその接続の両方向のオーナーとなります。接続のパケットが別のユニットに到着した場合は、そのパケットはクラスタ制御リンクを介してオーナーユニットに転送されます。逆方向のフローが別のユニットに到着した場合は、元のユニットにリダイレクトされます。

サンプル データ フロー

次の例は、新しい接続の確立を示します。



1. SYN パケットがクライアントから発信され、Firepower Threat Defense デバイスの 1 つ（ロードバランシング方法に基づく）に配信されます。これがオーナーとなります。オーナーはフローを作成し、オーナー情報をエンコードして SYN Cookie を生成し、パケットをサーバに転送します。
2. SYN-ACK パケットがサーバから発信され、別の Firepower Threat Defense デバイス（ロードバランシング方法に基づく）に配信されます。この Firepower Threat Defense デバイスはフォワーダです。

3. フォワーダはこの接続を所有してはいないので、オーナー情報を SYN Cookie からデコードし、オーナーへの転送フローを作成し、SYN-ACK をオーナーに転送します。
4. オーナーはディレクタに状態アップデートを送信し、SYN-ACK をクライアントに転送します。
5. ディレクタは状態アップデートをオーナーから受信し、オーナーへのフローを作成し、オーナーと同様に TCP ステート情報を記録します。ディレクタは、この接続のバックアップ オーナーとしての役割を持ちます。
6. これ以降、フォワーダに配信されたパケットはすべて、オーナーに転送されます。
7. パケットがその他のユニットに配信された場合は、そのユニットはディレクタに問い合わせてオーナーを特定し、フローを確立します。
8. フローの状態が変化した場合は、状態アップデートがオーナーからディレクタに送信されます。

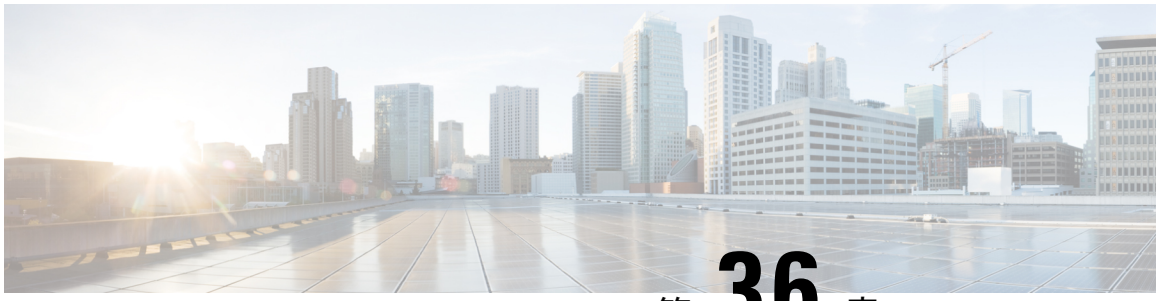
クラスタリングの履歴

機能	バージョン	詳細
強化された Firepower Threat Defense クラスタの Firepower Management Center への追加	6.3.0	Firepower Management Center にクラスタの任意のユニットを追加できるようになりました。他のクラスタ ユニットは自動的に検出されます。以前は、各クラスタ ユニットを個別のデバイスとして追加し、Management Center でグループ化してクラスタにする必要がありました。クラスタ ユニットの追加も自動で実行されるようになりました。ユニットは手動で削除する必要があることに注意してください。 新しい/変更された画面： **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > [追加（Add）] ドロップダウン メニュー > [デバイス（Devices）] > [デバイスの追加（Add Device）] ダイアログボックス **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > [クラスタ（Cluster）] タブ > [全般（General）] 領域 > [クラスタの登録ステータス（Cluster Registration Status）] リンク > [クラスタ ステータス（Cluster Status）] ダイアログ ボックス サポートされるプラットフォーム：Firepower 4100/9300
中央集中型機能としてのクラスタリングによるサイト間 VPN のサポート	6.2.3.3	クラスタリングを使用してサイト間 VPN を設定できるようになりました。サイトツーサイト VPN は、中央集中型機能です。マスター ユニットだけが VPN 接続をサポートします。 サポートされるプラットフォーム：Firepower 4100/9300

機能	バージョン	詳細
内部エラーの発生後に自動的にクラスタに再参加します。	6.2.3	以前は、多くの内部エラー状態によって、クラスタ ユニットがクラスタから削除され、ユーザが問題を解決した後で、手動でクラスタに再参加する必要がありました。現在は、ユニットが自動的に、5 分、10 分、20 分の間隔でクラスタに再参加しようとします。内部エラーには、アプリケーション同期のタイムアウト、一貫性のないアプリケーション ステータスなどがあります。 新しい/変更されたコマンド：**show cluster info auto-join** 変更された画面はありません。 サポートされているプラットフォーム：Firepower 4100/9300 の Firepower Threat Defense
6 モジュールのシャーシ間クラスタリング、Firepower 4100 サポート	6.2.0	FXOS 2.1.1 では、Firepower 9300 および 4100 でシャーシ間クラスタリングを有効化できるようになりました。Firepower 9300 の場合、最大 6 つのモジュールを含めることができます。たとえば、6 つのシャーシで 1 つのモジュールを使用したり、3 つのシャーシで 2 つのモジュールを使用したり、最大 6 つのモジュールを組み合わせたりできます。Firepower 4100 の場合、最大 6 つのシャーシを含めることができます。 （注） サイト間クラスタリングが、FlexConfig のみを使用してサポートされるようになりました。 変更された画面はありません。 サポートされているプラットフォーム：Firepower 4100/9300 の Firepower Threat Defense
Firepower 9300 用シャーシ内クラスタリング	6.0.1	FirePOWER 9300 シャーシ内では、最大 3 つセキュリティ モジュールをクラスタ化できます。シャーシ内のすべてのモジュールは、クラスタに属している必要があります。 新しい/変更された画面： **[デバイス（Devices）] > [デバイス管理（Device Management）] > [追加（Add）] > -[クラスタの追加（Add Cluster）]** **[デバイス（Devices）] > [デバイス管理（Device Management）] > [クラスタ（Cluster）]** サポートされているプラットフォーム：Firepower 9300 の Firepower Threat Defense

第 X 部

Firepower Threat Defense のルーティング



第 36 章

Firepower Threat Defense のルーティングの概要

この章では、Firepower Threat Defense 内でのルーティング動作の基本概念について説明します。

パス判別

ルーティング プロトコルでは、メトリックを使用して、パケットの移動に最適なパスを評価します。メトリックは、宛先への最適なパスを決定するためにルーティング アルゴリズムが使用する、パスの帯域幅などの測定基準です。パスの決定プロセスを支援するために、ルーティング アルゴリズムは、ルート情報が格納されるルーティング テーブルを初期化して保持します。ルート情報は、使用するルーティング アルゴリズムによって異なります。

ルーティング アルゴリズムにより、さまざまな情報がルーティング テーブルに入力されます。宛先またはネクスト ホップの関連付けにより、最終的な宛先に達するまで、「ネクスト ホップ」を表す特定のルータにパケットを送信することによって特定の宛先に最適に到達できることがルータに示されます。ルータは、着信パケットを受信すると宛先アドレスを確認し、このアドレスとネクスト ホップとを関連付けようとします。

ルーティング テーブルには、パスの妥当性に関するデータなど、他の情報を格納することもできます。ルータは、メトリックを比較して最適なルートを決定します。これらのメトリックは、使用しているルーティング アルゴリズムの設計によって異なります。

ルータは互いに通信し、さまざまなメッセージの送信によりそのルーティング テーブルを保持しています。ルーティング アップデート メッセージはそのようなメッセージの 1 つで、通常はルーティング テーブル全体か、その一部で構成されています。ルーティング アップデート

を他のすべてのルータから分析することで、ルータはネットワークトポロジの詳細な全体像を構築できます。ルータ間で送信されるメッセージのもう1つの例であるリンクステートアドバタイズメントは、他のルータに送信元のリンクのステートを通知します。リンク情報も、ネットワークの宛先に対する最適なルートをルータが決定できるように、ネットワークトポロジの全体像の構築に使用できます。

サポートされるルート タイプ

ルータが使用できるルート タイプには、さまざまなものがあります。Firepower Threat Defense デバイスでは、次のルート タイプが使用されます。

- スタティックとダイナミックの比較
- シングルパスとマルチパスの比較
- フラットと階層型の比較
- リンクステートと距離ベクトル型の比較

スタティックとダイナミックの比較

スタティック ルーティング アルゴリズムは、実はネットワーク管理者が確立したテーブル マップです。このようなマッピングは、ネットワーク管理者が変更するまでは変化しません。スタティック ルートを使用するアルゴリズムは設計が容易であり、ネットワーク トラフィックが比較的予想可能で、ネットワーク設計が比較的単純な環境で正しく動作します。

スタティック ルーティング システムはネットワークの変更に対応できないため、一般に、変化を続ける大規模なネットワークには不向きであると考えられています。主なルーティング アルゴリズムのほとんどはダイナミック ルーティング アルゴリズムであり、受信したルーティング アップデート メッセージを分析することで、変化するネットワーク環境に適合します。メッセージがネットワークが変化したことを示している場合は、ルーティング ソフトウェアはルートを再計算し、新しいルーティング アップデート メッセージを送信します。これらのメッセージはネットワーク全体に送信されるため、ルータはそのアルゴリズムを再度実行し、それに従ってルーティング テーブルを変更します。

ダイナミック ルーティング アルゴリズムは、必要に応じてスタティック ルートで補足できます。たとえば、ラスト リゾート ルータ（ルーティングできないすべてのパケットが送信されるルータのデフォルトルート）を、ルーティングできないすべてのパケットのリポジトリとして機能するように指定し、すべてのメッセージを少なくとも何らかの方法で確実に処理することができます。

シングルパスとマルチパスの比較

一部の高度なルーティング プロトコルは、同じ宛先に対する複数のパスをサポートしています。シングルパス アルゴリズムとは異なり、これらのマルチパス アルゴリズムでは、複数の

回線でトラフィックを多重化できます。マルチパスアルゴリズムの利点は、スループットと信頼性が大きく向上することであり、これは一般に「ロードシェアリング」と呼ばれています。

フラットと階層型の比較

ルーティングアルゴリズムには、フラットなスペースで動作するものと、ルーティング階層を使用するものがあります。フラット ルーティング システムでは、ルータは他のすべてのルータのピアになります。階層型ルーティング システムでは、一部のルータが実質的なルーティング バックボーンを形成します。バックボーン以外のルータからのパケットはバックボーン ルータに移動し、宛先の一般エリアに達するまでバックボーンを通じて送信されます。この時点で、パケットは、最後のバックボーン ルータから、1 つ以上のバックボーン以外のルータを通じて最終的な宛先に移動します。

多くの場合、ルーティング システムは、ドメイン、自律システム、またはエリアと呼ばれるノードの論理グループを指定します。階層型のシステムでは、ドメイン内の一部のルータは他のドメインのルータと通信できますが、他のルータはそのドメイン内のルータ以外とは通信できません。非常に大規模なネットワークでは、他の階層レベルが存在することがあり、最も高い階層レベルのルータがルーティング バックボーンを形成します。

階層型ルーティングの第一の利点は、ほとんどの企業の組織に類似しているため、そのトラフィック パターンもサポートするという点です。ほとんどのネットワーク通信は、小さい企業グループ（ドメイン）内で発生します。ドメイン内ルータは、そのドメイン内の他のルータだけを認識していれば済むため、そのルーティングアルゴリズムを簡素化できます。また、使用しているルーティング アルゴリズムに応じて、ルーティング アップデート トラフィックを減少させることができます。

リンクステートと距離ベクトル型の比較

リンクステートアルゴリズム（最短パス優先アルゴリズムとも呼ばれる）は、インターネットワークのすべてのノードにルーティング情報をフラッドします。ただし、各ルータは、それ自体のリンクのステートを記述するルーティング テーブルの一部だけを送信します。リンクステート アルゴリズムでは、各ルータはネットワークの全体像をそのルーティング テーブルに構築します。距離ベクトル型アルゴリズム（Bellman-Ford アルゴリズムとも呼ばれる）では、各ルータが、そのネイバーだけに対してそのルーティングテーブル全体または一部を送信するように要求されます。つまり、リンクステートアルゴリズムは小規模なアップデートを全体に送信しますが、距離ベクトル型アルゴリズムは、大規模なアップデートを隣接ルータだけに送信します。距離ベクトル型アルゴリズムは、そのネイバーだけを認識します。通常、リンクステート アルゴリズムは OSPF ルーティング プロトコルとともに使用されます。

ルーティングにサポートされているインターネットプロトコル

Firepower Threat Defense デバイスは、ルーティングに対してさまざまなインターネット プロトコルをサポートしています。この項では、各プロトコルについて簡単に説明します。

- Enhanced Interior Gateway Routing Protocol（EIGRP）

  EIGRP は、IGRP ルータとの互換性とシームレスな相互運用性を提供するシスコ独自のプロトコルです。自動再配布メカニズムにより、IGRP ルートを Enhanced IGRP に、または Enhanced IGRP からインポートできるため、Enhanced IGRP を既存の IGRP ネットワークに徐々に追加できます。

- Open Shortest Path First（OSPF）

  OSPF は、インターネット プロトコル（IP）ネットワーク向けに、インターネット技術特別調査委員会（IETF）の Interior Gateway Protocol（IGP）作業部会によって開発されたルーティング プロトコルです。OSPF は、リンクステートアルゴリズムを使用して、すべての既知の宛先までの最短パスを構築および計算します。OSPF エリア内の各ルータには、ルータが使用可能なインターフェイスと到達可能なネイバーそれぞれのリストである同一のリンクステート データベースが置かれています。

- ルーティング情報プロトコル（RIP）

  RIP は、ホップ カウントをメトリックとして使用するディスタンスベクトル プロトコルです。RIP は、グローバルなインターネットでトラフィックのルーティングに広く使用されている Interior Gateway Protocol（IGP）です。つまり、1 つの自律システム内部でルーティングを実行します。

- Border Gateway Protocol（BGP）

  BGP は自律システム間のルーティング プロトコルです。BGP は、インターネットのルーティング情報を交換するために、インターネット サービス プロバイダー（ISP）間で使用されるプロトコルです。カスタマーは ISP に接続し、ISP は BGP を使用してカスタマーおよび ISP ルートを交換します。自律システム（AS）間で BGP を使用する場合、このプロトコルは外部 BGP（EBGP）と呼ばれます。サービス プロバイダーが BGP を使用して AS 内でルートを交換する場合、このプロトコルは内部 BGP（IBGP）と呼ばれます。

Routing Table

FTD はデータ トラフィック（デバイスを介して）および管理トラフィック（デバイスから）に別々のルーティング テーブルを使用します。ここでは、ルーティング テーブルの仕組みについて説明します。管理ルーティング テーブルの詳細については、管理トラフィック用ルーティングテーブル （961 ページ）も参照してください。

ルーティング テーブルへの入力方法

FTDのルーティング テーブルには、スタティックに定義されたルート、直接接続されているルート、およびダイナミック ルーティング プロトコルで検出されたルートを入力できます。FTDは、ルーティング テーブルに含まれるスタティック ルートと接続されているルートに加えて、複数のルーティング プロトコルを実行できるため、同じルートが複数の方法で検出または入力される可能性があります。同じ宛先への2つのルートがルーティング テーブルに追加されると、ルーティング テーブルに残るルートは次のように決定されます。

- 2つのルートのネットワーク プレフィックス長（ネットワーク マスク）が異なる場合は、どちらのルートも固有と見なされ、ルーティングテーブルに入力されます。入力された後は、パケット転送ロジックが 2 つのうちどちらを使用するかを決定します。

  たとえば、RIP プロセスと OSPF プロセスが次のルートを検出したとします。

  - RIP：192.168.32.0/24
  - OSPF：192.168.32.0/19

  OSPF ルートのアドミニストレーティブ ディスタンスの方が適切であるにもかかわらず、これらのルートのプレフィックス長（サブネットマスク）はそれぞれ異なるため、両方のルートがルーティング テーブルにインストールされます。これらは異なる宛先と見なされ、パケット転送ロジックが使用するルートを決定します。

- FTDが、1 つのルーティング プロトコル（RIP など）から同じ宛先に複数のパスがあることを検知すると、（ルーティングプロトコルが判定した）メトリックがよい方のルートがルーティング テーブルに入力されます。

  メトリックは特定のルートに関連付けられた値で、ルートを最も優先されるものから順にランク付けします。メトリックスの判定に使用されるパラメータは、ルーティングプロトコルによって異なります。メトリックが最も小さいパスは最適パスとして選択され、ルーティングテーブルにインストールされます。同じ宛先への複数のパスのメトリックが等しい場合は、これらの等コスト パスに対してロード バランシングが行われます。

- FTD が、ある宛先へのルーティング プロトコルが複数あることを検知すると、ルートのアドミニストレーティブ ディスタンスが比較され、アドミニストレーティブ ディスタンスが最も小さいルートがルーティング テーブルに入力されます。

ルートのアドミニストレーティブ ディスタンス

ルーティング プロトコルによって検出されるルート、またはルーティング プロトコルに再配布されるルートのアドミニストレーティブ ディスタンスは変更できます。2 つの異なるルーティングプロトコルからの2つのルートのアドミニストレーティブディスタンスが同じ場合、デフォルトのアドミニストレーティブ ディスタンスが小さい方のルートがルーティング テーブルに入力されます。EIGRP ルートと OSPF ルートの場合、EIGRP ルートと OSPF ルートのアドミニストレーティブ ディスタンスが同じであれば、デフォルトで EIGRP ルートが選択されます。

アドミニストレーティブディスタンスは、2つの異なるルーティングプロトコルから同じ宛先に複数の異なるルートがある場合に、Firepower Threat Defense デバイスが最適なパスの選択に使用するルート パラメータです。ルーティング プロトコルには、他のプロトコルとは異なるアルゴリズムに基づくメトリックがあるため、異なるルーティングプロトコルによって生成された、同じ宛先への 2 つのルートについて常に最適パスを判定できるわけではありません。

各ルーティング プロトコルには、アドミニストレーティブ ディスタンス値を使用して優先順位が付けられています。次の表に、Firepower Threat Defense デバイスがサポートするルーティングプロトコルのデフォルトのアドミニストレーティブ ディスタンス値を示します。

表 *80 :* サポートされるルーティング プロトコルのデフォルトのアドミニストレーティブ ディスタンス

ルートの送信元	デフォルトのアドミニストレーティブ ディスタンス
接続されているインターフェイス	0
スタティック ルート	1
EIGRP サマリー ルート	5
外部 BGP	20
内部 EIGRP	90
OSPF	110
IS-IS	115
RIP	120
EIGRP 外部ルート	170
内部およびローカル BGP	200
不明（Unknown）	255

アドミニストレーティブ ディスタンス値が小さいほど、プロトコルの優先順位が高くなります。たとえば、Firepower Threat Defense デバイスが OSPF ルーティング プロセス（デフォルトのアドミニストレーティブ ディスタンスが 110）と RIP ルーティング プロセス（デフォルトのアドミニストレーティブディスタンスが 120）の両方から特定のネットワークへのルートを受信すると、OSPF ルーティング プロセスの方が優先度が高いため、Firepower Threat Defense デバイスは OSPF ルートを選択します。この場合、ルータは OSPF バージョンのルートをルーティング テーブルに追加します。

この例では、OSPF 導出ルートの送信元が（電源遮断などで）失われると、Firepower Threat Defense デバイスは、OSPF 導出ルートが再度現れるまで、RIP 導出ルートを使用します。

アドミニストレーティブ ディスタンスはローカルの設定値です。たとえば、OSPF を通じて取得したルートのアドミニストレーティブディスタンスを変更する場合、その変更は、コマンドが入力された Firepower Threat Defense デバイス のルーティング テーブルにだけ影響します。アドミニストレーティブ ディスタンスがルーティング アップデートでアドバタイズされることはありません。

アドミニストレーティブ ディスタンスは、ルーティング プロセスに影響を与えません。ルーティング プロセスは、ルーティング プロセスで検出されたか、またはルーティング プロセスに再配布されたルートだけをアドバタイズします。たとえば、RIP ルーティング プロセスは、のルーティング テーブルで OSPF ルーティング プロセスによって検出されたルートが使用されていても、RIP ルートをアドバタイズします。

ダイナミック ルートとフローティング スタティック ルートのバックアップ

ルートを最初にルーティングテーブルにインストールしようとしたとき、他のルートがインストールされてしまい、インストールできなかった場合に、そのルートはバックアップルートとして登録されます。ルーティングテーブルにインストールされたルートに障害が発生すると、ルーティング テーブル メンテナンス プロセスが、登録されたバックアップ ルートを持つ各ルーティングプロトコルプロセスを呼び出し、ルーティングテーブルにルートを再インストールするように要求します。障害が発生したルートに対して、登録されたバックアップルートを持つプロトコルが複数ある場合、アドミニストレーティブディスタンスに基づいて優先順位の高いルートが選択されます。

このプロセスのため、ダイナミック ルーティング プロトコルによって検出されたルートに障害が発生したときにルーティング テーブルにインストールされるフローティング スタティック ルートを作成できます。フローティング スタティック ルートとは、単に、Firepower Threat Defense デバイスで動作しているダイナミック ルーティング プロトコルよりも大きなアドミニストレーティブ ディスタンスが設定されているスタティック ルートです。ダイナミック ルーティング プロセスで検出された対応するルートに障害が発生すると、このスタティック ルートがルーティング テーブルにインストールされます。

転送の決定方法

転送は次のように決定されます。

- 宛先が、ルーティング テーブル内のエントリと一致しない場合、パケットはデフォルトルートに指定されているインターフェイスを通して転送されます。デフォルトルートが設定されていない場合、パケットは破棄されます。
- 宛先が、ルーティングテーブル内の1つのエントリと一致した場合、パケットはそのルートに関連付けられているインターフェイスを通して転送されます。
- 宛先が、ルーティング テーブル内の複数のエントリと一致する場合、パケットはネットワーク プレフィックス長がより長いルートに関連付けられているインターフェイスから転送されます。

たとえば、192.168.32.1 宛てのパケットが、ルーティング テーブルの次のルートを使用してインターフェイスに到着したとします。

- 192.168.32.0/24 のゲートウェイ 10.1.1.2
- 192.168.32.0/19 のゲートウェイ 10.1.1.3

この場合、192.168.32.1 は 192.168.32.0/24 ネットワークに含まれるため、192.168.32.1 宛てのパケットは 10.1.1.2 宛てに送信されます。このアドレスはまた、ルーティング テーブルの他のルートにも含まれますが、ルーティングテーブル内では 192.168.32.0/24 の方が長いプレフィックスを持ちます（24 ビットと 19 ビット）。パケットを転送する場合、プレフィックスが長い方が常に短いものより優先されます。

（注） ルートの変更が原因で新しい同様の接続が異なる動作を引き起こしたとしても、既存の接続は設定済みのインターフェイスを使用し続けます。

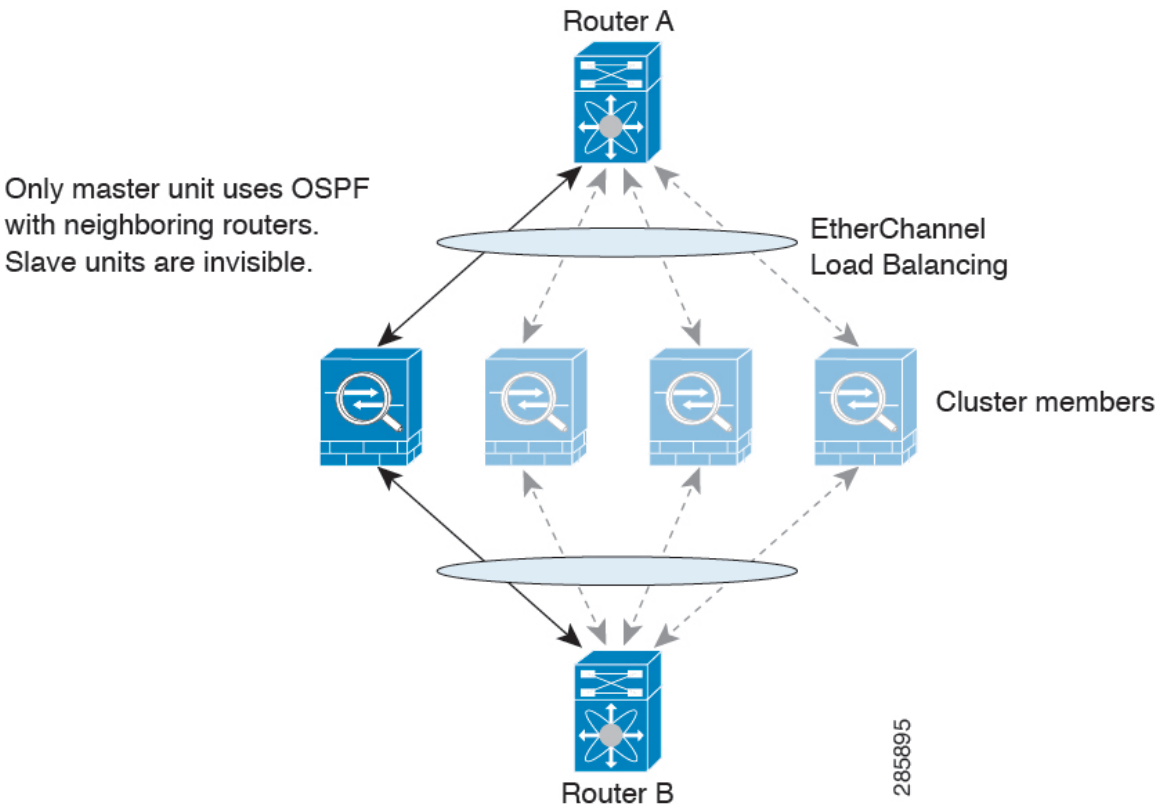
ダイナミック ルーティングと 高可用性

アクティブなユニットでルーティング テーブルが変更されると、スタンバイ ユニットでダイナミック ルートが同期されます。これは、アクティブ ユニットのすべての追加、削除、または変更がただちにスタンバイ ユニットに伝播されることを意味します。スタンバイ ユニットがアクティブ/スタンバイの待受中 高可用性 ペアでアクティブになると、ルートは 高可用性 バルク同期および連続複製プロセスの一部として同期されるため、そのユニットには以前のアクティブ ユニットと同じルーティング テーブルがすでに作成されています。

クラスタリングでのダイナミック ルーティング

ルーティング プロセスはマスター ユニット上だけで実行されます。ルートはマスター ユニットを介して学習され、スレーブに複製されます。ルーティング パケットがスレーブに到着した場合は、マスター ユニットにリダイレクトされます。

図 *22*: クラスタリングでのダイナミック ルーティング



スレーブ メンバがマスター ユニットからルートを学習した後は、各ユニットが個別に転送に関する判断を行います。

OSPF LSA データベースは、マスター ユニットからスレーブ ユニットに同期されません。マスターユニットのスイッチオーバーが発生した場合は、隣接ルータが再起動を検出します。スイッチオーバーは透過的ではありません。OSPF プロセスが IP アドレスの 1 つをルータ ID として選択します必須ではありませんが、スタティック ルータ ID を割り当てることができます。これで、同じルータ ID がクラスタ全体で使用されるようになります。割り込みを解決するには、OSPF ノンストップ フォワーディング機能を参照してください。

管理トラフィック用ルーティングテーブル

標準的なセキュリティ実践として、データ トラフィックを管理トラフィックから分離しなければならない場合があります。この分離を実現するために、FTDは管理専用トラフィックとデータ トラフィックに個別のルーティング テーブルを使用します。個別のルーティング テーブルは、データと管理用に別のデフォルト ルートを作成できることを意味します。

デバイス間トラフィックでは、常にデータ ルーティング テーブルが使用されます。

デバイス間トラフィックでは、そのタイプに応じて、デフォルトで管理ルーティングテーブルまたはデータ ルーティング テーブルのいずれかが使用されます。デフォルトのルーティングテーブルで一致が見つからなかった場合は、他のルーティングテーブルがチェックされます。

デバイス間トラフィックの管理テーブルには、HTTP、SCP、TFTP、などを使用してリモートファイルを開く機能が含まれています。

データ テーブルのデバイス間トラフィックには、ping、DNS、DHCP などの他のすべての機能が含まれています。

デフォルトのルーティングテーブルにないインターフェイスに移動するために、ボックス内のトラフィックを必要とするとき、場合によっては、他のテーブルへのフォールバックに頼るのではなく、インターフェイスを設定するときにそのインターフェイスを指定する必要があります。FTD は、正しいルーティング テーブルをチェックし、そのインターフェイスのルートがないか調べます。たとえば、管理専用インターフェイスにpingを送信する必要がある場合は、ping 機能でそのインターフェイスを指定します。そうではなく、データ ルーティング テーブルにデフォルト ルートがある場合は、デフォルト ルートに一致し、管理ルーティング テーブルにフォールバックすることは決してありません。

管理ルーティング テーブルは、データ インターフェイス ルーティング テーブルとは分離したダイナミック ルーティングをサポートします。ダイナミック ルーティング プロセスは管理専用インターフェイスまたはデータ インターフェイスで実行されなければなりません。両方のタイプを混在させることはできません。

管理専用インターフェイスには、すべての診断 x/x インターフェイス、および管理専用として設定したすべてのインターフェイスが含まれています。

（注） このルーティングテーブルは、FMC との通信に使用する特別な FTD 管理論理インターフェイスには影響しません。そのインターフェイスには独自のルーティングテーブルが備わっています。一方、診断論理インターフェイスは、この項で説明している管理専用ルーティングテーブルを使用します。

等コスト マルチパス（ECMP）ルーティング

Firepower Threat Defense デバイス は、等コスト マルチパス（ECMP）ルーティングをサポートしています。

インターフェイスごとに最大 3 の等コストのスタティック ルートタまたはダイナミック ルートを設定できます。たとえば、次のように異なるゲートウェイを指定する外部インターフェイスで複数のデフォルト ルートを設定できます。

```
route for 0.0.0.0 0.0.0.0 through outside to 10.1.1.2
route for 0.0.0.0 0.0.0.0 through outside to 10.1.1.3
route for 0.0.0.0 0.0.0.0 through outside to 10.1.1.4
```

この場合、トラフィックは、10.1.1.2、10.1.1.3 と 10.1.1.4 間の外部インターフェイスでロードバランスされます。トラフィックは、送信元 IP アドレスと宛先 IP アドレス、着信インターフェイス、プロトコル、送信元ポートと宛先ポートをハッシュするアルゴリズムに基づいて、指定したゲートウェイ間に分配されます。

ECMP は複数のインターフェイス間ではサポートされないため、異なるインターフェイスで同じ宛先へのルートを定義することはできません。上記のルートのいずれかを設定すると、次のルートは拒否されます。

```
route for 0.0.0.0 0.0.0.0 through outside2 to 10.2.1.1
```

ルート マップについて

ルート マップは、ルートを OSPF、RIP、EIGRP、または BGP ルーティング プロセスに再配布するときに使用します。また、デフォルト ルートを OSPF ルーティング プロセスに生成するときにも使用します。ルート マップは、指定されたルーティング プロトコルのどのルートを対象ルーティング プロセスに再配布できるのかを定義します。

ルート マップは、広く知られた ACL と共通の機能を数多く持っています。両方に共通する主な特性は次のとおりです。

- いずれも、それぞれが許可または拒否の結果を持つ個々の文を一定の順序で並べたものです。ACL またはルートマップの評価は、事前に定義された順序でのリストのスキャンと、一致する各文の基準の評価で構成されています。リストのスキャンは、文の一致が初めて見つかり、その文に関連付けられたアクションが実行されると中断します。

- これらは一般的なメカニズムです。基準一致と一致解釈は、適用方法とこれらを使用する機能によって決定します。異なる機能に適用される同じルートマップの解釈が異なることがあります。

次のように、ルート マップと ACL には違いがいくつかあります。

- ルート マップは ACL よりも柔軟性が高く、ACL が確認できない基準に基づいてルートを確認できます。たとえば、ルートマップはルートのタイプが内部であるかどうかを確認できます。
- 設計規則により、各 ACL は暗黙の deny 文で終了します。一致試行の間にルート マップの終わりに達した場合は、そのルートマップの特定のアプリケーションによって結果が異なります。再配布に適用されるルートマップの動作はACLと同じです。ルートがルートマップのどの句とも一致しない場合は、ルートマップの最後に deny 文が含まれている場合と同様に、ルートの再配布が拒否されます。

permit 句と deny 句

ルート マップでは permit 句と deny 句を使用できます。deny 句は、ルートの照合の再配布を拒否します。ルートマップでは、一致基準として ACL を使用できます。ACL には permit 句と deny 句もあるため、パケットが ACL と一致した場合に次のルールが適用されます。

- ACL permit + route map permit：ルートは再配布されます。
- ACL permit + route map deny：ルートは再配布されません。
- ACL deny + route map permit or deny：ルート マップの句は一致せず、次のルート マップ句が評価されます。

match 句と set 句の値

各ルート マップ句には、次の 2 種類の値があります。

- match 値は、この句が適用されるルートを選択します。
- set 値は、ターゲット プロトコルに再配布される情報を変更します。

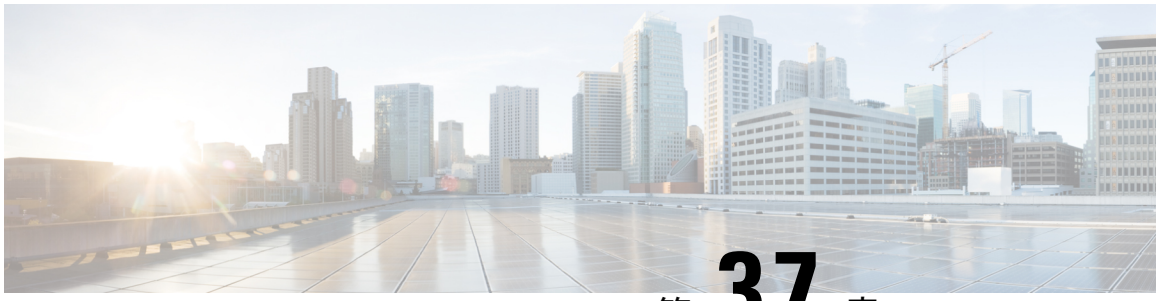
再配布される各ルートについて、ルータは最初にルートマップの句の一致基準を評価します。一致基準が満たされると、そのルートは、permit 句または deny 句に従って再配布または拒否され、そのルートの一部の属性が、set コマンドによって設定された値で変更されます。一致基準が満たされないと、この句はルートに適用されず、ソフトウェアはルートマップの次の句でルートを評価します。ルートマップのスキャンは、ルートと一致する句が見つかるまで、もしくはルートマップの最後に到達するまで続行します。

次のいずれかの条件が満たされる場合は、各句の match 値または set 値を省略したり、何回か繰り返したりできます。

- 複数の match エントリが句に含まれる場合に、特定のルートが句に一致するためには、そのルートですべての照合に成功しなければなりません（つまり、複数の match コマンドでは論理 AND アルゴリズムが適用される）。
- match エントリが 1 つのエントリの複数のオブジェクトを指している場合は、そのいずれかが一致していなければなりません（論理 OR アルゴリズムが適用される）。
- match エントリがない場合は、すべてのルートが句に一致します。
- ルート マップの permit 句に set エントリが存在しない場合、ルートは、その現在の属性を変更されずに再配布されます。

（注） ルート マップの deny 句では set エントリを設定しないでください。deny 句を指定するとルートの再配布が禁止され、情報が何も変更されないからです。

match エントリまたは set エントリがないルート マップ句はアクションを実行します。空の permit 句を使用すると、変更を加えずに残りのルートの再配布が可能になります。空の deny 句では、他のルートの再配布はできません。これは、ルートマップがすべてスキャンされたときに、明示的な一致が見つからなかったときのデフォルト アクションです。



第 37 章

Firepower Threat Defense のスタティック ルートとデフォルト ルート

この章では、FTD でスタティック ルートとデフォルト ルートを設定する方法について説明します。

スタティック ルートとデフォルト ルートについて

接続されていないホストやネットワークにトラフィックをルーティングするには、スタティック ルーティングまたはダイナミック ルーティングを使用して、ホストやネットワークへのルートを定義する必要があります。通常は、少なくとも 1 つのスタティック ルート、つまり、他の方法でデフォルトのネットワーク ゲートウェイにルーティングされていない、すべてのトラフィック用のデフォルト ルート（通常、ネクスト ホップ ルータ）を設定する必要があります。

Default Route

最も単純なオプションは、すべてのトラフィックをアップストリーム ルータに送信するようにデフォルト スタティック ルートを設定して、トラフィックのルーティングをルータに任せることです。デフォルト ルートは、既知のルートもスタティック ルートも指定されていない IP パケットすべてを、FTD デバイスが送信するゲートウェイの IP アドレスを特定するルートです。デフォルト スタティック ルートとは、つまり宛先の IP アドレスとして 0.0.0.0/0（IPv4）または ::/0（IPv6）が指定されたスタティック ルートのことです。

デフォルト ルートを常に定義する必要があります。

FTD はデータ トラフィックと管理トラフィックに別々のルーティング テーブルを使用するため、必要に応じて、データ トラフィック用のデフォルト ルートと管理トラフィック用の別のデフォルト ルートを設定できます。デバイス間トラフィックでは、タイプに応じてデフォルトで管理またはデータ ルーティング テーブルが使用されます（管理トラフィック用ルーティング テーブル （961 ページ）を参照）。ただし、ルートが見つからない場合は、他のルーティン

グテーブルにフォールバックします。デフォルトルートは常にトラフィックに一致するため、他のルーティングテーブルへのフォールバックが妨げられます。この場合、インターフェイスがデフォルトのルーティングテーブルになければ、出力トラフィックに使用するインターフェイスを指定する必要があります。

スタティック ルート

次の場合は、スタティック ルートを使用します。

- ネットワークがサポート対象外のルータ ディスカバリ プロトコルを使用している。
- ネットワークが小規模でスタティック ルートを容易に管理できる。
- ルーティング プロトコルが関係するトラフィックまたは CPU のオーバーヘッドをなくす必要がある。
- 場合によっては、デフォルトルートだけでは不十分である。デフォルトのゲートウェイでは宛先ネットワークに到達できない場合があるため、スタティックルートをさらに詳しく設定する必要があります。たとえば、デフォルトのゲートウェイが外部の場合、デフォルト ルートは、FTD デバイス に直接接続されていない内部ネットワークにはまったくトラフィックを転送できません。
- ダイナミック ルーティング プロトコルをサポートしていない機能を使用している。

不要なトラフィックを「ブラックホール化」するためのnull0インターフェイスへのルート

アクセスルールを使用すると、ヘッダーに含まれている情報に基づいてパケットをフィルタ処理することができます。null0 インターフェイスへのスタティック ルートは、アクセス ルールを補完するソリューションです。null0 ルートを使用して、不要なトラフィックや望ましくないトラフィックを「ブラック ホール」に転送できるため、トラフィックがドロップされます。

スタティック null0 ルートには、望ましいパフォーマンス プロファイルがあります。また、スタティック null0 ルートを使用して、ルーティング ループ回避することもできます。BGP では、リモート トリガ型ブラック ホール ルーティングのためにスタティック null0 ルートを活用できます。

ルートのプライオリティ

- 特定の宛先が特定されたルートはデフォルト ルートより優先されます。
- 宛先が同じルートが複数存在する場合（スタティックまたはダイナミック）、ルートのアドミニストレーティブディスタンスによってプライオリティが決まります。スタティックルートは 1 に設定されるため、通常、それらが最もプライオリティの高いルートです。

- 宛先かつアドミニストレーティブ ディスタンスが同じスタティック ルートが複数存在する場合は、等コスト マルチパス（ECMP）ルーティング （962 ページ）を参照してください。
- [トンネル化（Tunneled）] オプションを使用してトンネルから出力されるトラフィックの場合、このルートが他の設定済みルートまたは学習されたデフォルト ルートをすべてオーバーライドします。

トランスペアレントファイアウォールモードとブリッジグループルート

ブリッジ グループ メンバー インターフェイスを通じて直接には接続されていないネットワークに向かう Firepower Threat Defense デバイス で発信されるトラフィックの場合、Firepower Threat Defense デバイス がどのブリッジ グループ メンバー インターフェイスからトラフィックを送信するかを認識するように、デフォルト ルートまたはスタティック ルートを設定する必要があります。Firepower Threat Defense デバイス で発信されるトラフィックは、syslog サーバまたはSNMP サーバへの通信も含むことがあります。1 つのデフォルト ルートで到達できないサーバがある場合、スタティック ルートを設定する必要があります。トランスペアレント モードの場合、ゲートウェイ インターフェイスに BVI を指定できません。メンバー インターフェイスのみが使用できます。ルーテッド モードのブリッジ グループの場合、スタティック ルートに BVI を指定する必要があります。メンバー インターフェイスを指定することはできません。詳細については、「MAC アドレスとルート ルックアップ （717 ページ）」を参照してください。

スタティック ルート トラッキング

スタティック ルートの問題の 1 つは、ルートがアップ状態なのかダウン状態なのかを判定する固有のメカニズムがないことです。スタティック ルートは、ネクスト ホップ ゲートウェイが使用できなくなった場合でも、ルーティング テーブルに保持されています。スタティック ルートは、Firepower Threat Defense デバイス 上の関連付けられたインターフェイスがダウンした場合に限りルーティング テーブルから削除されます。

スタティック ルート トラッキング機能には、スタティック ルートの使用可能状況を追跡し、プライマリ ルートがダウンした場合のバックアップ ルートをインストールするための方式が用意されています。たとえば、ISP ゲートウェイへのデフォルト ルートを定義し、かつ、プライマリ ISP が使用できなくなった場合に備えて、セカンダリ ISP へのバックアップ デフォルト ルートを定義できます。

Firepower Threat Defense デバイス では、Firepower Threat Defense デバイス が ICMP エコー要求を使用してモニタする宛先ネットワーク上でモニタリング対象スタティック ルートを関連付けることでスタティック ルート トラッキングを実装します。指定された時間内にエコー応答がない場合は、そのホストはダウンしていると見なされ、関連付けられたルートはルーティング テーブルから削除されます。削除されたルートに代わって、メトリックが高い追跡対象外のバックアップ ルートが使用されます。

モニタリング対象の選択時には、その対象がICMPエコー要求に応答できることを確認してください。対象には任意のネットワーク オブジェクトを選択できますが、次のものを使用することを検討する必要があります。

- ISP ゲートウェイ アドレス（デュアル ISP サポート用）
- ネクストホップ ゲートウェイ アドレス（ゲートウェイの使用可能状況に懸念がある場合）
- Firepower Threat Defense デバイス が通信を行う必要のある対象ネットワーク上のサーバ（syslog サーバなど）
- 宛先ネットワーク上の永続的なネットワーク オブジェクト

（注） 夜間にシャットダウンする PC は適しません。

スタティック ルート トラッキングは、スタティックに定義されたルートや、DHCP または PPPoE を通じて取得したデフォルト ルートに対して設定することができます。設定済みのルート トラッキングでは、複数のインターフェイス上の PPPoE クライアントだけをイネーブルにすることができます。

スタティックルートとデフォルトルートのガイドライン

ファイアウォール モードとブリッジグループ

- トランスペアレント モードでは、スタティック ルートをブリッジグループ メンバー インターフェイスをゲートウェイとして使用する必要があります。BVI を指定することはできません。
- ルーテッド モードでは、BVI をゲートウェイとして指定する必要があります。メンバー インターフェイスを指定することはできません。
- スタティック ルート トラッキングは、ブリッジグループ メンバー インターフェイスまたは BVI ではサポートされません。

IPv6

- IPv6 では、スタティック ルート トラッキングはサポートされません。

クラスタ

クラスタリングでは、スタティック ルート モニタリングはプライマリ ユニットでのみサポートされます。

スタティック ルートの追加

スタティック ルートは、特定の宛先ネットワークのトラフィックの送信先を定義します。少なくともデフォルト ルートを定義する必要があります。デフォルト ルートは、宛先 IP アドレスが 0.0.0.0/0 のスタティック ルートです。

ステップ 1 **[デバイス（Devices）] > [デバイス管理（Device Management）]** の順に選択し、FTD デバイスを編集します。

ステップ 2 [ルーティング（Routing）] タブをクリックします。

ステップ 3 コンテンツのテーブルから [スタティック ルート（Static Route）] を選択します。

ステップ 4 [ルートを追加（Add Routes）] をクリックします。

ステップ 5 追加するスタティック ルートのタイプに応じて、[IPv4] または [IPv6] オプション ボタンをクリックします。

ステップ 6 このスタティック ルートを適用する [インターフェイス（Interface）] を選択します。

トランスペアレント モードの場合は、ブリッジ グループのメンバー インターフェイスの名前を選択します。 ブリッジ グループによるルーティング モードの場合、BVI 名として、いずれかのブリッジ グループ メンバー インターフェイスを選択できます。不要なトラフィックを「ブラック ホール化」するには、**Null0** インターフェイスを選択します。

ステップ 7 [利用可能なネットワーク（Available Network）] リストで、宛先ネットワークを選択します。

デフォルト ルートを定義するには、アドレス 0.0.0.0/0 のオブジェクトを作成し、ここでそれを選択します。

ステップ 8 [ゲートウェイ（Gateway）] または [IPv6 ゲートウェイ（IPv6 Gateway）] フィールドで、このルートのネクスト ホップであるゲートウェイ ルータを入力または選択します。IP アドレスまたはネットワーク/ホスト オブジェクトを指定できます。

ステップ 9 [メトリック（Metric）] フィールドに、宛先ネットワークへのホップの数を入力します。有効値の範囲は 1 ～ 255 で、デフォルト値は 1 です。メトリックは、特定のホストが存在するネットワークへのホップ数（ホップ カウント）に基づくルートの「コスト」を示す測定値です。ホップ カウントは、ネットワーク パケットが最終的な宛先に到達するまでに通過する必要があるネットワークの数であり、宛先ネットワークも含まれます。メトリックは、複数のルーティング プロトコル間でルートを比較するために使用されます。スタティック ルートのデフォルトのアドミニストレーティブ ディスタンスは 1 で、ダイナミック ルーティング プロトコルで検出されるルートより優先されますが、直接には接続されていないルートです。OSPF で検出されるルートのデフォルトのアドミニストレーティブ ディスタンスは 110 です。スタティック ルートとダイナミック ルートのアドミニストレーティブ ディスタンスが同じ場合、スタティック ルートが優先されます。接続されているルートは常に、スタティック ルートおよびダイナミックに検出されたルートのどちらよりも優先されます。

ステップ 10 （任意） デフォルト ルートの場合は、[トンネル型（Tunneled）] チェックボックスをオンにして、VPN トラフィック用に別個のデフォルト ルートを定義します。

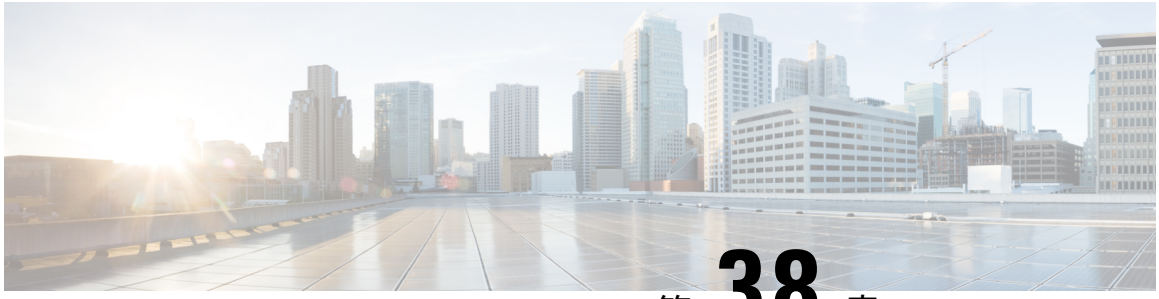
VPN トラフィックに非 VPN トラフィックとは別のデフォルト ルートを使用する必要がある場合は、VPN トラフィック用の別個のデフォルト ルートを定義できます。その場合、たとえば VPN 接続からの着信ト

ラフィックは内部ネットワークに転送する一方、内部ネットワークからのトラフィックは外部に転送するといった設定を簡単に行うことができます。[トンネル型（tunneled）]オプションを使用してデフォルト ルートを作成すると、デバイスに着信するトンネルからのすべてのトラフィックは、学習したルートまたはスタティック ルートを使用してルーティングできない場合、このルートに送信されます。設定できるデフォルトのトンネル ゲートウェイは、デバイスごとに 1 つのみです。トンネル トラフィックの ECMP はサポートされません。

ステップ 11 （IPv4 スタティック ルートのみ）ルートの可用性をモニタするには、モニタリング ポリシーを定義する SLA（サービス レベル契約）モニタ オブジェクトの名前を [ルート トラッキング（Route Tracking）] フィールドで入力または選択します。

SLA モニタ オブジェクト （602 ページ）を参照してください。

ステップ 12 [OK] をクリックします。



第 38 章

Firepower Threat Defense の OSPF

この章では、Open Shortest Path First（OSPF）ルーティング プロトコルを使用してデータをルーティングし、認証を実行し、ルーティング情報を再配布するように FTD を設定する方法について説明します。

Firepower Threat Defense の OSPF

この章では、Open Shortest Path First（OSPF）ルーティング プロトコルを使用してデータをルーティングし、認証を実行し、ルーティング情報を再配布するように FTD を設定する方法について説明します。

OSPF の概要

OSPF は、パスの選択に距離ベクトル型ではなくリンク ステートを使用する Interior Gateway Routing Protocol（IGRP）です。OSPF は、ルーティング テーブル アップデートではなく、リンクステート アドバタイズメントを伝搬します。ルーティング テーブル全体ではなく LSA だけが交換されるため、OSPF ネットワークは RIP ネットワークよりも迅速に収束します。

OSPF は、リンクステート アルゴリズムを使用して、すべての既知の宛先までの最短パスを構築および計算します。OSPF エリア内の各ルータには、ルータが使用可能なインターフェイスと到達可能なネイバーそれぞれのリストである同一のリンクステート データベースが置かれています。

RIP に比べると OSPF は次の点で有利です。

- OSPF のリンクステート データベースのアップデート送信は RIP ほど頻繁ではありません。また、古くなった情報がタイムアウトしたときに、リンクステート データベースは徐々にアップデートされるのではなく、瞬時にアップデートされます。

- ルーティング決定はコストに基づいて行われます。これは、特定のインターフェイスを介してパケットを送信するためにオーバーヘッドが必要であることを示しています。Firepower Threat Defense デバイスは、インターフェイスのコストをリンク帯域幅に基づいて計算し、宛先までのホップ数は使用しません。コストは優先パスを指定するために設定できます。

最短パス優先アルゴリズムの欠点は、CPU サイクルとメモリが大量に必要になることです。

Firepower Threat Defense デバイス は、OSPF プロトコルの 2 つのプロセスを異なるセットのインターフェイス上で同時に実行できます。同じ IP アドレスを使用する複数のインターフェイス（NAT ではこのようなインターフェイスは共存可能ですが、OSPF ではアドレスの重複は許しません）があるときに、2 つのプロセスを実行する場合があります。あるいは、一方のプロセスを内部で実行しながら別のプロセスを外部で実行し、ルートのサブセットをこの 2 つのプロセス間で再配布する場合もあります。同様に、プライベート アドレスをパブリック アドレスから分離する必要がある場合もあります。

OSPF ルーティング プロセスには、別の OSPF ルーティング プロセスや RIP ルーティング プロセスから、または OSPF 対応インターフェイスに設定されているスタティック ルートおよび接続されているルートから、ルートを再配布できます。

Firepower Threat Defense デバイスでは、次の OSPF の機能がサポートされています。

- エリア内ルート、エリア間ルート、および外部ルート（タイプ I とタイプ II）。
- 仮想リンク。
- LSA フラッディング。
- OSPF パケットの認証（パスワード認証と MD5 認証の両方）
- Firepower Threat Defense デバイス の指定ルータまたは指定バックアップ ルータとしての設定。Firepower Threat Defense デバイスは、ABR として設定することもできます。
- スタブ エリアと not so stubby エリア。
- エリア境界ルータのタイプ 3 LSA フィルタリング

OSPF は、MD5 とクリア テキスト ネイバー認証をサポートしています。OSPF と他のプロトコル（RIP など）の間のルート再配布は、攻撃者によるルーティング情報の悪用に使用される可能性があるため、できる限りすべてのルーティング プロトコルで認証を使用する必要があります。

NAT が使用されている場合、OSPF がパブリック エリアおよびプライベート エリアで動作している場合、またアドレス フィルタリングが必要な場合は、2 つの OSPF プロセス（1 つはパブリック エリア用、1 つはプライベート エリア用）を実行する必要があります。

複数のエリアにインターフェイスを持つルータは、エリア境界ルータ（ABR）と呼ばれます。ゲートウェイとして動作し、OSPF を使用しているルータと他のルーティング プロトコルを使用しているルータの間でトラフィックを再配布するルータは、自律システム境界ルータ（ASBR）と呼ばれます。

ABR は LSA を使用して、使用可能なルータに関する情報を他の OSPF ルータに送信します。ABR タイプ 3 LSA フィルタリングを使用して、ABR として機能する ASA で、プライベート

エリアとパブリック エリアを分けることができます。タイプ 3 LSA（エリア間ルート）は、プライベート ネットワークをアドバタイズしなくても NAT と OSPF を一緒に使用できるように、1 つのエリアから他のエリアにフィルタリングできます。

（注） フィルタリングできるのはタイプ 3 LSA だけです。プライベート ネットワーク内の ASBR として設定されている Firepower Threat Defense デバイス は、プライベート ネットワークを記述するタイプ 5 LSA を送信しますが、これは AS 全体（パブリック エリアも含む）にフラッディングされます。

NAT が採用されているが、OSPF がパブリック エリアだけで実行されている場合は、パブリック ネットワークへのルートを、デフォルトまたはタイプ 5 AS 外部 LSA としてプライベート ネットワーク内で再配布できます。ただし、Firepower Threat Defense デバイスにより保護されているプライベート ネットワークにはスタティック ルートを設定する必要があります。また、同一のFirepower Threat Defense デバイス インターフェイス上で、パブリック ネットワークとプライベート ネットワークを混在させることはできません。

Firepower Threat Defense デバイスでは、2 つの OSPF ルーティング プロセス（1 つの RIP ルーティング プロセスと 1 つの EIGRP ルーティング プロセス）を同時に実行できます。

fast hello パケットに対する OSPF のサポート

fast hello パケットに対する OSPF のサポートには、1 秒未満のインターバルで hello パケットの送信を設定する方法が用意されています。このような設定により、Open Shortest Path First（OSPF）ネットワークでの統合がより迅速になります。

fast hello パケットに対する OSPF のサポートの前提条件

OSPF がネットワークですでに設定されているか、fast hello パケットに対する OSPF のサポートと同時に設定される必要があります。

OSPF Hello インターバルおよび dead 間隔

OSPF hello パケットとは、OSPF プロセスがネイバーとの接続を維持するために OSPF ネイバーに送信するパケットです。hello パケットは、設定可能なインターバル（秒単位）で送信されます。デフォルトのインターバルは、イーサネット リンクの場合 10 秒、ブロードキャスト以外のリンクの場合 30 秒です。hello パケットには、デッド インターバル中に受信したすべてのネイバーのリストが含まれます。デッドインターバルも設定可能なインターバル（秒単位）で送信されます。デフォルトは hello インターバルの値の 4 倍です。hello インターバルの値は、ネットワーク内ですべて同一にする必要があります。デッドインターバルの値も、ネットワーク内ですべて同一にする必要があります。

この 2 つのインターバルは、リンクが動作していることを示すことにより、接続を維持するために連携して機能します。ルータがデッド インターバル内にネイバーから hello パケットを受信しない場合、ルータはこのネイバーがダウンしていると判定します。

OSPF fast hello パケット

OSPF fast hello パケットとは、1 秒よりも短いインターバルで送信される hello パケットのことです。fast hello パケットを理解するには、OSPF hello パケット インターバルとデッド インターバルとの関係についてあらかじめ理解しておく必要があります。OSPF Hello インターバルおよび dead 間隔 （973 ページ）を参照してください。

OSPF fast hello パケットは、ospf dead-interval コマンドで設定されます。デッド インターバルは 1 秒に設定され、hello-multiplier の値は、その 1 秒間に送信する hello パケット数に設定されるため、1 秒未満の「fast」hello パケットになります。

インターフェイスで fast hello パケットが設定されている場合、このインターフェイスから送出される hello パケットでアドバタイズされる hello 間隔は 0 に設定されます。このインターフェイス経由で受信した hello パケットの hello 間隔は無視されます。

デッド インターバルは、1 つのセグメント上で一貫している必要があり、1 秒に設定するか（fast hello パケットの場合）、他の任意の値を設定します。デッド インターバル内に少なくとも 1 つの hello パケットが送信される限り、hello multiplier がセグメント全体で同じである必要はありません。

OSPF fast hello パケットの利点

OSPF fast hello パケット機能を利用すると、ネットワークがこの機能を使用しない場合よりも、短い時間で統合されます。この機能によって、失われたネイバーを 1 秒以内に検出できるようになります。この機能は、ネイバーの損失が Open System Interconnection（OSI）物理層またはデータ リンク層で検出されないことがあっても、特に LAN セグメントで有効です。

OSPFv2 および OSPFv3 間の実装の差異

OSPFv3 には、OSPFv2 との下位互換性はありません。OSPF を使用して、IPv4 および IPv6 トラフィックの両方をルーティングするには、OSPFv2 および OSPFv3 の両方を同時に実行する必要があります。これらは互いに共存しますが、相互に連携していません。

OSPFv3 では、次の追加機能が提供されます。

- リンクごとのプロトコル処理。
- アドレッシング セマンティックの削除。
- フラッディング スコープの追加。
- リンクごとの複数インスタンスのサポート。
- ネイバー探索およびその他の機能に対する IPv6 リンクローカル アドレスの使用。
- プレフィックスおよびプレフィックス長として表される LSA。
- 2 つの LSA タイプの追加。
- 未知の LSA タイプの処理。

• RFC-4552 で指定されている OSPFv3 ルーティング プロトコル トラフィックの IPsec ESP 標準を使用する認証サポート。

OSPF のガイドライン

ファイアウォール モードのガイドライン

OSPF は、ルーテッド ファイアウォール モードのみをサポートしています。OSPF は、トランスペアレント ファイアウォール モードをサポートしません。

高可用性 ガイドライン

OSPFv2 および OSPFv3 は、ステートフル 高可用性 をサポートしています。

IPv6 のガイドライン

- OSPFv2 は IPv6 をサポートしません。
- OSPFv3 は IPv6 をサポートしています。
- OSPFv3 は、IPv6 を使用して認証を行います。
- Firepower Threat Defense デバイス は、OSPFv3 ルートが最適なルートの場合、IPv6 RIB にこのルートをインストールします。

クラスタリングのガイドライン

- OSPFv3 暗号化はサポートされていません。クラスタリング環境で OSPFv3 暗号化を設定しようとすると、エラー メッセージが表示されます。
- スパンド インターフェイス モードでは、ダイナミック ルーティングは管理専用インターフェイスではサポートされません。
- クラスタでマスター ロールの変更が発生した場合、次の挙動が発生します。
  - スパンド インターフェイス モードでは、ルータ プロセスはマスター ユニットでのみアクティブになり、スレーブ ユニットでは停止状態になります。コンフィギュレーションがマスターユニットと同期されているため、各クラスタ ユニットには同じルータ ID があります。その結果、隣接ルータはロール変更時のクラスタのルータ ID の変更を認識しません。

マルチプロトコル ラベル スイッチング（MPLS）と OSPF のガイドライン

MPLS 設定ルータから送信されるリンク ステート（LS）アップデート パケットに、Opaque Type-10 リンクステート アドバタイズメント（LSA）が含まれており、この LSA に MPLS ヘッダーが含まれている場合、認証は失敗し、アプライアンスはアップデート パケットを確認せず

にサイレントにドロップします。ピアルータは確認応答を受信していないため、最終的にネイバー関係を終了します。

ネイバー関係の安定を維持するため、アプライアンスでノンストップフォワーディング（NSF）が無効であることを確認します。

- Firepower Management Center の [Non Stop Forwarding] タブに移動します（[Devices] > [Device Management] > [Routing] > [OSPF] > [Advanced] > [Non Stop Forwarding]）。

  [Non Stop Forwarding Capability] のボックスがオンになっていないことを確認します。

その他のガイドライン

- OSPFv2 および OSPFv3 は 1 つのインターフェイス上での複数インスタンスをサポートしています。
- OSPFv3 は、非クラスタ環境での ESP ヘッダーを介した暗号化をサポートしています。
- OSPFv3 は非ペイロード暗号化をサポートします。
- OSPFv2 は RFC 4811、4812 および 3623 でそれぞれ定義されている、Cisco NSF グレースフル リスタートおよびIETF NSF グレースフル リスタート メカニズムをサポートします。
- OSPFv3 は RFC 5187 で定義されているグレースフル リスタート メカニズムをサポートします。
- 配布可能なエリア内（タイプ 1）ルートの数は限られています。これらのルートでは、1 つのタイプ 1 LSA にすべてのプレフィックスが含まれています。システムではパケットサイズが 35 KB に制限されているため、3000 ルートの場合、パケットがこの制限を超過します。2900 本のタイプ 1 ルートが、サポートされる最大数であると考えてください。

OSPFv2 の設定

ここでは、OSPFv2 ルーティング プロセスの設定に関連するタスクについて説明します。

OSPF エリア、範囲、仮想リンクの設定

認証の設定、スタブエリアの定義、デフォルトの集約ルートへの特定コストの割り当てが含まれる複数の OSPF エリア パラメータを設定できます。最大 2 つの OSPF プロセス インスタンスを有効にできます。各 OSPF プロセスには、独自のエリアとネットワークが関連付けられます。認証では、エリアへの不正アクセスに対してパスワードベースで保護します。

スタブ エリアは、外部ルートの情報が送信されないエリアです。その代わりに、ABR で生成されるデフォルトの外部ルートがあり、このルートは自律システムの外部の宛先としてスタブ エリアに送信されます。OSPF スタブ エリアのサポートを活用するには、デフォルトのルーティングをスタブ エリアで使用する必要があります。

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** の順に選択し、FTD デバイスを編集します。

ステップ 2 [ルーティング（Routing）] タブをクリックします。

ステップ 3 [OSPF] をクリックします。

ステップ 4 [プロセス 1（Process 1）] を選択します。それぞれのコンテキストで最大 2 つの OSPF プロセス インスタンスを有効にできます。エリアパラメータを設定するには、OSPF プロセスを選択する必要があります。

ステップ 5 OSPF のロールをドロップダウンリストから選択し、次のフィールドにそれぞれの説明を入力します。オプションは、[内部（Internal）]、[ABR]、[ASBR]、[ABR および ASBR（ABR and ASBR）] です。OSPF の権限の説明については、OSPF の概要 （971 ページ）を参照してください。

ステップ 6 [エリア（Area）] タブを選択し、[追加（Add）] をクリックします。

編集アイコン（  ）をクリックするか、右クリック メニューを使用して、エリアの切り取り、コピー、貼り付け、挿入、および削除を行うことができます。

ステップ 7 以下のエリアのオプションを、それぞれの OSPF プロセスで設定します。

- [OSPF Process]：1 または 2 を選択します。
- [エリア ID（Area ID）]：：ルートをサマライズするエリアの接続先。
- [エリア タイプ（Area Type）]：次のいずれかを選択します。
  - [Normal]：（デフォルト）標準 OSPF エリア。
  - [スタブ（Stub）]：スタブエリアには、その向こう側にルータまたはエリアはありません。スタブ エリアは、自律システム（AS）External LSA（タイプ 5 LSA）がスタブ エリアにフラッディングされないようにします。スタブ エリアを作成すると、[サマリー スタブ（Summary Stub）] チェックボックスをオフにすることによって、集約 LSA（タイプ 3 および 4）がそのエリアにフラッディングされるのを防ぐことができます。
  - [NSSA]：エリアを Not-So-Stubby Area にします。NSSA は、タイプ 7 LSA を受け入れます。[再配布（Redistribute）] チェックボックスをオフにし、[デフォルト情報起点（Default Information Originate）] チェックボックスをオンにすることで、ルートの再配布をディセーブルにすることができます。[集約 NSSA（Summary NSSA）] チェックボックスをオフにすることによって、集約 LSA でエリアへのフラッディングを防止できます。
- [メトリック値（Metric Value）]：デフォルト ルートの生成に使用するメトリックを指定します。デフォルト値は 10 です。有効なメトリック値の範囲は、0 ～ 16777214 です。
- [メトリック タイプ（Metric Type）]：メトリック タイプは、OSPF ルーティング ドメインにアドバタイズされるデフォルト ルートに関連付けられた外部リンク タイプです。使用可能なオプションは、タイプ 1 外部ルートの場合は 1、タイプ 2 外部ルートの場合は 2 です。
- [使用可能なネットワーク（Available Network）]：使用可能なネットワークのいずれかを選択して [追加（Add）] をクリックするか、追加アイコン（  ）をクリックして新しいネットワーク オブジェクトを追加します。ネットワークの追加手順については、ネットワーク オブジェクト （525 ページ）を参照してください。

- [認証（Authentication）]：OSPF 認証を選択します。
  - [なし（None）]：（デフォルト）OSPF エリアの認証を無効にします。
  - [パスワード（Password）]：クリアテキストパスワードがエリア認証に使用されますが、セキュリティが懸念となっている場合は推奨しません。
  - [MD5]：MD5 認証を許可します。
- [デフォルト コスト（Default Cost）]：接続先までの最短パスを割り出す OSPF エリアのデフォルトのコスト。有効値の範囲は、0 ～ 65535 です。デフォルト値は 1 です。

ステップ 8 [OK] をクリックして、エリア設定を保存します。

ステップ 9 [範囲（Range）] タブを選択し、[追加（Add）] をクリックします。

- 使用可能なネットワークのいずれかを選択して、アドバタイズするかを決めます。
- または、追加アイコン（  ）をクリックして、新しいネットワーク オブジェクトを加えます。ネットワークの追加手順については、ネットワーク オブジェクト （525 ページ）を参照してください。

ステップ 10 [OK] をクリックして、範囲設定を保存します。

ステップ 11 [仮想リンク（Virtual Link）] タブを選択して、[追加（Add）] をクリックし、それぞれの OSPF プロセスに以下のオプションを設定します。

- [ピア ルータ（Peer Router）]：ピア ルータの IP アドレスを選択します。新しいピア ルータを追加するには、追加アイコン（  ）をクリックします。ネットワークの追加手順については、ネットワーク オブジェクト （525 ページ）を参照してください。
- [Hello 間隔（Hello Interval）]：hello パケットがインターフェイスで送信される秒単位の間隔です。hello 間隔は、hello パケットでアドバタイズされる符号なし整数です。この値は、特定のネットワーク上のすべてのルータおよびアクセス サーバで同じである必要があります。有効値の範囲は 1 ～ 65535 です。デフォルトは 10 です。

  hello 間隔を小さくすると、トポロジ変更が検出されるまでの時間が短くなりますが、インターフェイス上で送信されるトラフィックは多くなります。
- [転送遅延（Transmit Delay）]：インターフェイス上で LSA パケットを送信するために必要と推定される時間（秒単位）。ゼロよりも大きい整数値を指定します。有効値の範囲は 1 ～ 8192 です。デフォルトは 1 です。

  アップデート パケット内の LSA 自体の経過時間は、転送前にこの値の分だけ増分されます。リンクでの送信前に遅延が加算されていない場合、LSA がリンクを介して伝播する時間は考慮されません。値は、インターフェイスの送信および伝播遅延を考慮して割り当てる必要があります。この設定は、非常に低速のリンクでより重要な意味を持ちます。
- [再転送間隔（Retransmit Interval）]：インターフェイスに属する隣接関係の LSA 再送信間の時間（秒単位）。再送信間隔は、接続されているネットワーク上の任意の 2 台のルータ間の予想されるラウンドトリップ遅延です。この値は、予想されるラウンドトリップ遅延より大きくなり、1 ～ 65535 の範囲で指定できます。デフォルトは 5 です。

ルータが自身のネイバーに LSA を送信する場合、ルータは確認応答メッセージを受信するまでその LSA を保持します。確認応答を受信しなかった場合、ルータでは LSA を再送します。この値は控えめに設定する必要があります。そうしないと、不要な再送信が発生する可能性があります。シリアル回線および仮想リンクの場合は、値を大きくする必要があります。

- [デッド間隔（Dead Interval）]：ルータがダウンしていることをネイバーが示す前に hello パケットを非表示にする秒単位の時間。デッド間隔は符号なし整数です。デフォルトは hello 間隔の 4 倍または 40 秒です。この値は、共通のネットワークに接続されているすべてのルータおよびアクセス サーバで同じであることが必要です。有効値の範囲は 1 ～ 65535 です。
- [認証（Authentication）]：以下から OSPF 仮想リンクの認証を選択します。
  - [なし（None）]：（デフォルト）仮想リンク エリアの認証を無効にします。
  - [エリア認証（Area Authentication）]：MD5 を使用して、エリア認証を有効にします。[追加（Add）] ボタンをクリックして、キー ID とキーを入力し、キーを確認し、[OK] をクリックします。
  - [パスワード（Password）]：クリアテキストパスワードが仮想リンクの認証に使用されますが、セキュリティが懸念となっている場合は推奨しません。
  - [MD5]：MD5 認証を許可します。[追加（Add）] ボタンをクリックして、キー ID とキーを入力し、キーを確認し、[OK] をクリックします。

    （注） MD5 キー ID として数字のみを入力してください。
  - [キー チェーン（Key Chain）]：キー チェーン認証を許可します。[追加（Add）] ボタンをクリックしてキー チェーンを作成した後、[保存（Save）] をクリックします。詳細な手順については、キー チェーンのオブジェクトの作成 （599 ページ）を参照してください。隣接関係を正常に確立するには、ピアに対して同じ認証タイプ（MD5 またはキー チェーン）とキー ID を使用します。

ステップ 12 [OK] をクリックして、仮想リンクの設定を保存します。

ステップ 13 ルーティング ページで [保存（Save）] をクリックして変更を保存します。

次のタスク

OSPF 再配布の設定 を続けます。

OSPF 再配布の設定

Firepower Threat Defense デバイスは、OSPF ルーティング プロセス間のルート再配布を制御できます。1 つのルーティング プロセスから OSPF ルーティング プロセスへの再配布ルートのルールが表示されます。RIP および BGP で検出されたルートを、OSPF ルーティング プロセスに再配布することができます。スタティック ルートおよび接続されているルートも、OSPF ルーティング プロセスに再配布できます。

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** の順に選択し、FTD デバイスを編集します。

ステップ 2 [ルーティング（Routing）] タブをクリックします。

ステップ 3 [OSPF] をクリックします。

ステップ 4 [Redistribution] タブを選択し、[Add] をクリックします。

編集アイコン（  ）をクリックするか、右クリック メニューを使用して、エリアの切り取り、コピー、貼り付け、挿入、および削除を行うことができます。

ステップ 5 OSPF プロセスごとに、次の再配布オプションを設定します。

- [OSPF Process]：1 または 2 を選択します。
- [ルート タイプ（Route Type）]：次のいずれかのタイプを選択します。
  - [スタティック（Static）]：スタティック ルートを OSPF ルーティング プロセスに再配布します。
  - [接続済み（Connected）]：接続されたルート（インターフェイス上で IP アドレスを有効にすることによって自動的に確立されるルート）を OSPF ルーティング プロセスに再配布します。接続済みルートは、デバイスの外部として再配布されます。[オプション（Optional）] リストのサブネットを使用するかどうかを選択できます。
  - [OSPF]：別の OSPF ルーティング プロセスからルートを再配布します（内部、外部 1 と 2、NSSA 外部 1 と 2、またはサブネットを使用するかどうか）。[オプション（Optional）] リストでこれらのオプションを選択できます。
  - [BGP]：BGP ルーティング プロセスからルートを再配布します。AS 番号およびサブネットを使用するかどうかを追加します。
  - [RIP]：RIP ルーティング プロセスからルートを再配布します。[オプション（Optional）] リストのサブネットを使用するかどうかを選択できます。
- [メトリック値（Metric Value）]：再配布するルートのメトリック値。デフォルト値は 10 です。有効な値の範囲は 0 ～ 16777214 です。

  同じデバイス上で 1 つの OSPF プロセスから別の OSPF プロセスに再配布する場合、メトリック値を指定しないと、メトリックは 1 つのプロセスから他のプロセスへ存続します。他のプロセスを OSPF プロセスに再配布するときに、メトリック値を指定しない場合、デフォルトのメトリックは 20 です。
- [メトリック タイプ（Metric Type）]：メトリック タイプは、OSPF ルーティング ドメインにアドバタイズされるデフォルト ルートに関連付けられた外部リンク タイプです。使用可能なオプションは、タイプ 1 外部ルートの場合は 1、タイプ 2 外部ルートの場合は 2 です。
- [タグ値（Tag Value）]：タグは 32 ビット 10 進数値を指定します。この値は、OSPF 自身では使用されないが ASBR 間の情報伝達に使用できる外部ルートのそれぞれに関連付けられます。何も指定しない場合、BGP および EGP からのルートにはリモート自律システムの番号が使用されます。その他のプロトコルについては、ゼロが使用されます。有効な値は、0 ～ 4294967295 です。

- [RouteMap]：送信元ルーティング プロトコルから現在のルーティング プロトコルへのルートのインポートのフィルタリングをチェックします。このパラメータを指定しない場合、すべてのルートが再配布されます。このパラメータを指定し、ルートマップ タグが表示されていない場合、ルートはインポートされません。または、追加アイコン（  ）をクリックして新しいルート マップを追加できます。新しいルート マップの追加については、「ルート マップ」を参照してください。

ステップ 6 [OK] をクリックして、再配布設定を保存します。

ステップ 7 [ルーティング（Routing）] ページで [保存（Save）] をクリックして変更を保存します。

次のタスク

OSPF エリア間フィルタリングの設定 （981 ページ）に進みます。

OSPF エリア間フィルタリングの設定

ABR のタイプ 3 LSA フィルタリングは、OSPF を実行している ABR の機能を拡張して、異なる OSPF エリア間のタイプ 3 LSA をフィルタリングします。プレフィックス リストが設定されているときは、指定されたプレフィックスのみが OSPF エリア間で送信されます。その他のすべてのプレフィックスは、それぞれの OSPF エリアに制限されます。このタイプのエリア フィルタリングは、OSPF エリアを出入りするトラフィックに対して、またはそのエリアの着信と発信の両方のトラフィックに対して適用できます。

プレフィックス リストの複数のエントリが指定されたプレフィックスと一致する場合、シーケンス番号が最も小さいエントリが使用されます。効率性を高めるため、頻繁に一致するエントリまたは一致しないエントリに、小さいシーケンス番号を手動で割り当てることで、それらをリストの上部に配置することもできます。デフォルトでは、シーケンス番号は自動的に生成され、開始値は 5 で 5 ずつ増えていきます。

ステップ 1 **[デバイス（Devices）] > [デバイス管理（Device Management）]** の順に選択し、FTD デバイスを編集します。

ステップ 2 [ルーティング（Routing）] タブをクリックします。

ステップ 3 [OSPF] をクリックします。

ステップ 4 [エリア間（InterArea）] タブを選択し、[追加（Add）] をクリックします。

編集アイコン（  ）をクリックするか、右クリック メニューを使用して、エリア間の切り取り、コピー、貼り付け、挿入、および削除を行うことができます。

ステップ 5 OSPF プロセスごとに、次のエリア間フィルタリング オプションを設定します。

- [OSPF Process]：1 または 2 を選択します。
- [エリア ID（Area ID）]：ルートを要約するエリア。
- [PrefixList]：プレフィックスの名前。新しいプレフィックス リスト オブジェクトを追加するには、ステップ 5 を参照してください。

- [トラフィックの方向（Traffic Direction）]：着信または発信。OSPF エリアへの LSA をフィルタリングするには [Inbound] を選択し、OSPF エリアからの LSA をフィルタリングするには [Outbound] を選択します。既存のフィルタ エントリを編集している場合、この設定は変更できません。

ステップ 6 追加アイコン（）をクリックして、新しいプレフィックスリストの名前と、オーバーライドを許可するかどうかを入力します。

プレフィックス ルールを設定する前に、プレフィックス リストを設定する必要があります。

ステップ 7 [追加（Add）] をクリックしてプレフィックス ルールを設定し、次のパラメータを設定します。

- [アクション（Action）]：再配布アクセスに対して [ブロック（Block）] または [許可（Allow）] を選択します。
- [シーケンス番号（Sequence No）]：ルーティング シーケンス番号。デフォルトでは、シーケンス番号は自動的に生成され、開始値は 5 で 5 ずつ増えていきます。
- [IP アドレス（IP Address）]：プレフィックス番号を IP アドレス/マスク長の形式で指定します。
- [最小プレフィックス長（Min Prefix Length）]：（オプション）最小のプレフィックス長。
- [最大プレフィックス長（Max Prefix Length）]：（オプション）最大のプレフィックス長。

ステップ 8 [OK] をクリックして、エリア間フィルタリング設定を保存します。

ステップ 9 [ルーティング（Routing）] ページで [保存（Save）] をクリックして変更を保存します。

次のタスク

OSPF のフィルタ ルールの設定 （982 ページ）に進みます。

OSPF のフィルタ ルールの設定

OSPF プロセスごとに ABR タイプ 3 LSA フィルタを設定できます。ABR タイプ 3 LSA フィルタを設定すると、指定したプレフィックスだけが 1 つのエリアから別のエリアに送信され、その他のプレフィックスはすべて制限されます。このタイプのエリア フィルタリングは、特定の OSPF エリアから、特定の OSPF エリアへ、または同じ OSPF エリアへ同時に適用できます。OSPF ABR タイプ 3 LSA フィルタリングによって、OSPF エリア間のルート再配布の制御が向上します。

ステップ 1 **[デバイス（Devices）] > [デバイス管理（Device Management）]** の順に選択し、FTD デバイスを編集します。

ステップ 2 [ルーティング（Routing）] タブをクリックします。

ステップ 3 [OSPF] をクリックします。

ステップ 4 [フィルタ ルール（Filter Rule）] タブを選択し、[追加（Add）] をクリックします。

編集アイコン（  ）をクリックするか、右クリック メニューを使用して、フィルタ ルールの切り取り、コピー、貼り付け、挿入、および削除を行うことができます。

ステップ 5 OSPF プロセスごとに、次のフィルタ ルール オプションを設定します。

- [OSPF Process]：1 または 2 を選択します。
- [アクセス リスト（Access List）]：この OSPF プロセスのアクセス リスト。新しい標準アクセス リスト オブジェクトを追加するには、追加アイコン（  ）をクリックし、標準 ACL オブジェクトの設定（612 ページ）を参照してください。
- [トラフィックの方向（Traffic Direction）]：フィルタリングするトラフィックの方向として [イン（In）] または [アウト（Out）] を選択します。OSPF エリアへの LSA をフィルタリングするには [イン（In）] を選択し、OSPF エリアからの LSA をフィルタリングするには [アウト（Out）] を選択します。既存のフィルタ エントリを編集している場合、この設定は変更できません。
- [インターフェイス（Interface）]：このフィルタ ルールのインターフェイス。

ステップ 6 [OK] をクリックしてルール設定を保存します。

ステップ 7 [ルーティング（Routing）] ページで [保存（Save）] をクリックして変更を保存します。

次のタスク

OSPF サマリー アドレスの設定 （983 ページ）に進みます。

OSPF サマリー アドレスの設定

他のプロトコルからのルートを OSPF に再配布する場合、各ルートは外部 LSA で個別にアドバタイズされます。ただし、再配布されるルートのうち、指定のネットワーク アドレスとマスクに含まれるすべてのものを 1 つのルートで表し、そのルートだけをアドバタイズするように Firepower Threat Defense デバイスを設定することができます。この設定によって OSPF リンク ステート データベースのサイズが小さくなります。指定した IP アドレス マスク ペアと一致するルートは廃止できます。ルート マップで再配布を制御するために、タグ値を一致値として使用できます。

他のルーティング プロトコルから学習したルートをサマライズできます。サマリーのアドバタイズに使用されるメトリックは、具体的なルートすべての中で最小のメトリックです。サマリー ルートは、ルーティング テーブルのサイズを削減するのに役立ちます。

OSPF のサマリー ルートを使用すると、OSPF ASBR は、そのアドレスでカバーされるすべての再配布ルートの集約として、1 つの外部ルートをアドバタイズします。OSPF に再配布されている、他のルーティング プロトコルからのルートだけをサマライズできます。

ステップ 1 **[デバイス（Devices）] > [デバイス管理（Device Management）]** の順に選択し、FTD デバイスを編集します。

ステップ 2 [ルーティング（Routing）] タブをクリックします。

ステップ 3 [OSPF] をクリックします。

ステップ 4 [サマリー アドレス（Summary Address）] タブを選択し、[追加（Add）] をクリックします。

編集アイコン（）をクリックして編集するか、右クリック メニューを使用して、サマリー アドレスの切り取り、コピー、貼り付け、挿入、および削除を行うことができます。

ステップ 5 OSPF プロセスごとに、次のサマリー アドレス オプションを設定します。

- [OSPF Process]：1 または 2 を選択します。
- [利用可能なネットワーク（Available Networks）]：サマリーの IP アドレス。利用可能なネットワークリストから 1 つを選択して [追加（Add）] をクリックするか、追加アイコン（）をクリックして新しいネットワークを追加します。ネットワークを追加する手順については、ネットワーク オブジェクト （525 ページ）を参照してください。
- [タグ（Tag）]：各外部ルートに付加される 32 ビットの 10 進数値。この値は OSPF 自身には使用されませんが、ASBR 間の情報伝達に使用できます。
- [アドバタイズ（Advertise）]：集約ルートをアドバタイズします。サマリー アドレスになるルートを抑止するには、このチェックボックスをオフにします。デフォルトでは、このチェックボックスはオンになっています。

ステップ 6 [OK] をクリックしてサマリー アドレス設定を保存します。

ステップ 7 [ルーティング（Routing）] ページで [保存（Save）] をクリックして変更を保存します。

次のタスク

OSPF インターフェイスとネイバーの設定 （984 ページ）に進みます。

OSPF インターフェイスとネイバーの設定

必要に応じて一部のインターフェイス固有の OSPFv2 パラメータを変更できます。これらのパラメータを変更することは必須ではありませんが、hello インターバル、Dead 間隔、認証キーというインターフェイスパラメータは、接続されているネットワーク内のすべてのルータで一致している必要があります。これらのパラメータを設定する場合は、ネットワーク上のすべてのルータで、コンフィギュレーションの値が矛盾していないことを確認してください。

ポイントツーポイントの非ブロードキャスト ネットワークを介して OSPFv2 ルートをアドバタイズするには、スタティック OSPFv2 ネイバーを定義する必要があります。この機能により、OSPFv2 アドバタイズメントを GRE トンネルにカプセル化しなくても、既存の VPN 接続でブロードキャストすることができます。

ステップ 1 **[デバイス（Devices）] > [デバイス管理（Device Management）]** の順に選択し、FTD デバイスを編集します。

ステップ 2 [ルーティング（Routing）] タブをクリックします。

ステップ 3 [OSPF] をクリックします。

ステップ 4 [インターフェイス（Interface）] タブを選択し、[追加（Add）] をクリックします。

編集アイコン（  ）をクリックするか、右クリック メニューを使用して、エリアの切り取り、コピー、貼り付け、挿入、および削除を行うことができます。

ステップ 5 OSPF プロセスごとに、次のインターフェイス オプションを設定します。

- [インターフェイス（Interface）] : 設定するインターフェイス。
- [デフォルト コスト（Default Cost）] : インターフェイスを介したパケット送信のコスト。デフォルト値は 10 です。
- [優先順位（Priority）] : ネットワークの代表ルータを指定します。有効な値の範囲は 0 ～ 255 です。デフォルト値は 1 です。この設定に 0 を入力すると、適切でないルータが指定ルータになったり、指定ルータのバックアップが行われたりします。

  2 つのルータがネットワークに接続している場合、両方が指定ルータになろうとします。ルータ優先順位の高いデバイスが指定ルータになります。ルータ優先順位が同じ場合は、ルータ ID が高い方が指定ルータになります。この設定は、ポイントツーポイントのインターフェイスとして設定されているインターフェイスには適用されません。
- [MTU 無視（MTU Ignore）] : OSPF は、共通のインターフェイス上でネイバーが同一の MTU を使用しているかどうかをチェックします。このチェックは、ネイバーによる DBD パケットの交換時に行われます。DBD パケット内の受信した MTU が、受信インターフェイスに設定されている IP MTU より大きい場合は、OSPF 隣接関係は確立されません。
- [データベース フィルタ（Database Filter）] : この設定は、同期とフラッディングのときに発信 LSA インターフェイスをフィルタリングするのに使用します。デフォルトでは、OSPF は、LSA が到着したインターフェイスを除き、同じエリア内のすべてのインターフェイスで新しい LSA をフラッドします。完全メッシュ化トポロジでは、このフラッディングによって帯域幅が浪費されて、リンクおよび CPU の過剰使用につながることがあります。このチェックボックスをオンにすると、選択されているインターフェイスでは OSPF の LSA フラッディングが行われなくなります。
- [Hello 間隔（Hello Interval）] : インターフェイス上で送信される hello パケットの間隔を秒単位で指定します。有効な値の範囲は、1 ～ 8192 秒です。デフォルト値は 10 秒です。

  hello 間隔を小さくすると、トポロジ変更が検出されるまでの時間が短くなりますが、インターフェイス上で送信されるトラフィックは多くなります。この値は、特定のインターフェイス上のすべてのルータおよびアクセス サーバで同じである必要があります。
- [伝送遅延（Transmit Delay）] : インターフェイス上で LSA パケットを送信するのに必要な予想時間（秒単位）。有効値の範囲は、1 ～ 65535 秒です。デフォルト値は 1 秒です。

  更新パケット内の LSA には、送信前に、このフィールドで指定した値によって増分された経過時間が格納されます。リンクでの送信前に遅延が加算されていない場合、LSA がリンクを介して伝播する時間は考慮されません。値は、インターフェイスの送信および伝播遅延を考慮して割り当てる必要があります。この設定は、非常に低速のリンクでより重要な意味を持ちます。

- [再送信間隔（Retransmit Interval）]：インターフェイスに属する隣接関係の LSA 再送信間の時間（秒単位）。接続ネットワーク上の任意の 2 台のルータ間で想定される往復遅延より大きな値にする必要があります。有効値の範囲は、1 ～ 65535 秒です。デフォルトは 5 秒です。

  ルータが自身のネイバーに LSA を送信する場合、ルータは確認応答メッセージを受信するまでその LSA を保持します。確認応答を受信しなかった場合、ルータでは LSA を再送します。この値は控えめに設定する必要があります。そうしないと、不要な再送信が発生する可能性があります。シリアル回線および仮想リンクの場合は、値を大きくする必要があります。

- [Dead 間隔（Dead Interval）]：hello パケットが確認されない場合に、ルータがダウンしたとネイバーが判断するまでの待ち時間（秒単位）。この値はネットワーク上のすべてのノードで同じにする必要があります。値の範囲は、1 ～ 65535 です。

- [Hello 乗数（Hello Multiplier）]：1 秒ごとに送信される hello パケットの数を指定します。有効な値は、3 ～ 20 です。

- [ポイント ツー ポイント（Point-to-Point）]：VPN トンネルで OSPF ルートを送信できます。

- [認証（Authentication）]： OSPF のインターフェイス認証を次から選択します。

  - [なし（None）]：（デフォルト）インターフェイス認証を無効にします。

  - [エリア認証（Area Authentication）]：MD5 を使用したインターフェイス認証を有効にします。[追加（Add）] ボタンをクリックして、キー ID とキーを入力し、キーを確認し、[OK] をクリックします。

  - [パスワード（Password）]：クリア テキスト パスワードが仮想リンクの認証に使用されますが、セキュリティが懸念となっている場合は推奨しません。

  - [MD5]：MD5 認証を許可します。[追加（Add）] ボタンをクリックして、キー ID とキーを入力し、キーを確認し、[OK] をクリックします。

    （注） MD5 キー ID として数字のみを入力してください。

  - [キー チェーン（Key Chain）]：キー チェーン認証を許可します。[追加（Add）] ボタンをクリックしてキー チェーンを作成した後、[保存（Save）] をクリックします。詳細な手順については、キー チェーンのオブジェクトの作成 （599 ページ）を参照してください。隣接関係を正常に確立するには、ピアに対して同じ認証タイプ（MD5 またはキー チェーン）とキー ID を使用します。

- [パスワードの入力（Enter Password）]：認証のタイプとして [パスワード（Password）] を選択した場合に、設定するパスワード。

- [パスワードの確認（Confirm Password）]：選択したパスワードを確認します。

ステップ 6 [ネイバー（Neighbor）] タブを選択し、[追加（Add）] をクリックします。

編集アイコン（  ）をクリックするか、右クリック メニューを使用して、エリアの切り取り、コピー、貼り付け、挿入、および削除を行うことができます。

ステップ 7 OSPF プロセスごとに、次のパラメータを設定します。

- [OSPF プロセス（OSPF Process）]：1 または 2 を選択します。

- [ネイバー（Neighbor）]：ドロップダウンリストでネイバーの1人を選択するか、追加アイコン（）をクリックして新しいネイバーを追加します。名前、説明、ネットワーク、およびオーバーライドを許可するかどうかを入力し、[保存（Save）] をクリックします。
- [インターフェイス（Interface）]：ネイバーに関連付けられたインターフェイスを選択します。

ステップ 8 [OK] をクリックして、ネイバー設定を保存します。

ステップ 9 [ルーティング（Routing）] ページで [保存（Save）] をクリックして変更を保存します。

OSPF 詳細プロパティの設定

[高度なプロパティ（Advanced Properties）] タブを使用すると、syslog メッセージ生成、アドミニストレーティブ ルート ディスタンス、LSA タイマー、グレースフル リスタートなどのオプションを設定できます。

グレースフル リスタート

Firepower Threat Defense デバイスでは、既知の障害状況が発生することがあります。これにより、スイッチング プラットフォーム全体でパケット転送に影響を与えることがあってはなりません。Non-Stop Forwarding（NSF）機能では、ルーティング プロトコル情報を復元している間に、既知のルートへのデータ転送が続行されます。この機能は、スケジュール済みヒットレス ソフトウェア アップグレードがあるときに便利です。NSF Cisco（RFC 4811 および RFC 4812）または NSF IETF（RFC 3623）のいずれかを使用して、OSPFv2 上でグレースフル リスタートを設定できます。

（注） NSF 機能は HA モードとクラスタリングでも役立ちます。

NSF グレースフル リスタート機能の設定には、機能の設定と NSF 対応または NSF 認識としてのデバイスの設定という 2 つのステップが伴います。NSF 対応デバイスは、ネイバーに対して独自のリスタート アクティビティを示すことができ、NSF 認識デバイスはネイバーのリスタートをサポートすることができます。

デバイスは、いくつかの条件に応じて、NSF 対応または NSF 認識として設定できます。

- デバイスは、現在のデバイスのモードに関係なく、NSF 認識デバイスとして設定できます。
- デバイスを NSF 対応として設定するには、デバイスはフェールオーバーまたはスパンド EtherChannel（L2）クラスタ モードのいずれかである必要があります。
- デバイスを NSF 認識または NSF 対応にするには、必要に応じて opaque リンク ステート アドバタイズメント（LSA）/リンク ローカル シグナリング（LLS）ブロックの機能を使って設定する必要があります。

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** の順に選択し、FTD デバイスを編集します。

ステップ 2 [Routing] をクリックします。

ステップ 3 [OSPF] をクリックし、次に [Advanced] をクリックします。

ステップ 4 [一般（General）] タブを選択し、次のように設定します。

- [ルータ ID（Router Id）]：ルータ ID に [自動（Automatic）] または [IP アドレス（IP address）] を選択します。[IP アドレス（IP address）] を選択する場合は、[IP アドレス（IP Address）] フィールドに IP アドレスを入力します。
- [LSA MOSPF を無視（Ignore LSA MOSPF）]：ルートがサポートされていない LSA タイプ 6 マルチキャスト OSPF（MOSPF）パケットを受信した場合、syslog メッセージを抑制します。
- [RFC 1583 互換（RFC 1583 Compatible）]：集約ルートのコストを計算するための手段として RFC 1583 の互換性を設定します。RFC 1583 の互換性が有効な場合、ルーティング ループが発生することがあります。ルーティング ループを防止するには、これを無効にします。OSPF ルーティング ドメイン内のすべての OSPF ルータの RFC 互換設定が同じである必要があります。
- [隣接関係の変更（Adjacency Changes）]：syslog メッセージが送信される隣接関係の変更内容を定義します。

  デフォルトでは、OSPF ネイバーがアップ状態またはダウン状態になったときに、syslog メッセージが生成されます。OSPF ネイバーがダウンしたときに syslog メッセージを送信するようルータを設定することも、状態ごとに syslog を送信するように設定することもできます。

  - [隣接関係の変更のログ記録（Log Adjacency Changes）]：OSPF ネイバーが起動または停止したときに、Firepower Threat Defense デバイスによって syslog メッセージが送信されるようになります。この設定は、デフォルトでオンになっています。
  - [隣接関係の変更の詳細のログ記録（Log Adjacency Change Details）]：ネイバーがアップ状態またはダウン状態になったときだけでなく、状態の変更が発生したときにも Firepower Threat Defense デバイスによって syslog メッセージが送信されるようになります。デフォルトでは、この設定はオフになっています。

- [アドミニストレーティブ ルート ディスタンス（Administrative Route Distances）]：エリア間、エリア内、および外部 IPv6 ルートのアドミニストレーティブ ルート ディスタンスの設定に使用された設定を変更できます。アドミニストレーティブ ルート ディスタンスは 1 ～ 254 の整数です。デフォルトは 110 です。
- [LSA グループ ペーシング（LSA Group Pacing）]：LSA をグループにまとめてリフレッシュ、チェックサム計算、エージングする間隔を秒単位で指定します。有効値の範囲は 10 ～ 1800 です。デフォルト値は 240 です。
- [デフォルト情報の発信を有効にする（Enable Default Information Originate）]：デフォルトの外部ルートを OSPF ルーティング ドメインに生成するには、[有効化（Enable）] チェックボックスをオンにして、次のオプションを設定します。

- [デフォルト ルートを常にアドバタイズする（Always advertise the default route）]：デフォルト ルートが常にアドバタイズされるようにします。
- [メトリック（Metric）]：デフォルト ルートを生成するために使用するメトリック。有効なメトリック値の範囲は、0 ～ 16777214 です。デフォルト値は 10 です。
- [メトリック タイプ（Metric Type）]：OSPFv3 ルーティング ドメインにアドバタイズされるデフォルト ルートに関連付けられた外部リンク タイプ。有効な値は 1（タイプ 1 の外部ルート）および 2（タイプ 2 の外部ルート）です。デフォルトはタイプ 2 外部ルートです。
- [ルート マップ（Route Map）]：ルート マップが満たされている場合にデフォルト ルートを生成するルーティング プロセスを選択するか、追加アイコン（）をクリックして、新しいルーティング プロセスを追加します。新しいルート マップの追加については、「ルート マップ」を参照してください。

ステップ 5 [OK] をクリックして、一般設定を保存します。

ステップ 6 [Non Stop Forwarding] タブを選択し、NSF 対応または NSF 認識デバイスに対して、OSPFv2 の Cisco NSF グレースフル リスタートを設定します。

（注） OSPFv2 には、Cisco NSF と IETF NSF の 2 つのグレースフル リスタート メカニズムがあります。OSPF インスタンスに対しては、これらのグレースフル リスタート メカニズムのうち一度に設定できるのは 1 つだけです。NSF 認識デバイスは、Cisco NSF ヘルパーと IETF NSF ヘルパーの両方として設定できますが、NSF 対応デバイスは OSPF インスタンスに対して、Cisco NSF または IETF NSF モードのいずれかとして設定できます。

a) [Cisco Non Stop Forwarding 機能を有効にする（Enable Cisco Non Stop Forwarding Capability）] チェックボックスをオンにします。

b) （オプション）必要に応じて、[非 NSF 認識隣接ネットワーキング デバイスが検出されたときに NSF リスタートをキャンセルする（Cancel NSF restart when non-NSF-aware neighboring networking devices are detected）] チェックボックスをオンにします。

c) （オプション）[Cisco Non Stop Forwarding ヘルパー モードを有効にする（Enable Cisco Non Stop Forwarding Helper mode）] チェックボックスをオフにして、NSF 認識デバイスでのヘルパー モードを無効にします。

ステップ 7 NSF 対応または NSF 認識デバイスに対して、OSPFv2 の IETF NSF グレースフル リスタートを設定します。

a) [IETF Non Stop Forwarding 機能を有効にする（Enable IETF Non Stop Forwarding Capability）] チェックボックスをオンにします。

b) [グレースフル リスタート間隔（秒）（Length of graceful restart interval (seconds)）] フィールドにリスタート間隔を秒単位で入力します。デフォルト値は 120 秒です。30 秒以下のリスタート間隔の場合、グレースフル リスタートは終了します。

c) （オプション）[ヘルパー モードの IETF Nonstop Forwarding（NSF）を有効にする（Enable IETF nonstop forwarding (NSF) for helper mode）] チェックボックスをオフにして、NSF 認識デバイスでの IETF NSF ヘルパー モードを無効にします。

d) [厳密なリンク ステートのアドバタイズメント チェックを有効にする（Enable Strict Link State advertisement checking）]：有効にすると、再起動ルータにフラッディングされる可能性がある LSA への変更があることが検出された場合、またはグレースフル リスタート プロセスが開始されたときに再起動ルータの

再送リスト内に変更された LSA があると検出された場合、ヘルパー ルータはルータの再起動プロセスを終了させます。

e) [IETF Non Stop Forwarding を有効にする（Enable IETF Non Stop Forwarding）]：スイッチオーバー後にルーティング プロトコル情報が復元される間、データのパケットの転送が既知のルートで続行される Non Stop Forwarding を有効にします。OSPF は OSPF プロトコルの拡張を使用して、隣接する OSPF デバイスからステートを回復します。リカバリが機能するためには、ネイバーが NSF プロトコル拡張をサポートし、再起動するデバイスの「ヘルパー」として積極的に動作する必要があります。ネイバーはまた、プロトコル ステートのリカバリが行われる間、再起動するデバイスにデータ トラフィックを転送し続ける必要もあります。

OSPFv3 の設定

ここでは、OSPFv3 ルーティング プロセスの設定に関連するタスクについて説明します。

OSPFv3 エリア、ルート集約、および仮想リンクの設定

OSPFv3 を有効にするには、OSPFv3 ルーティング プロセスを作成し、OSPFv3 用のエリアを作成して、OSPFv3 のインターフェイスを有効にする必要があります。その後、ターゲットの OSPFv3 ルーティング プロセスにルートを再配布する必要があります。

ステップ 1 **[デバイス（Devices）] > [デバイス管理（Device Management）]** の順に選択し、FTD デバイスを編集します。

ステップ 2 [ルーティング（Routing）] > [OSPFv3] を選択します。

ステップ 3 デフォルトでは、[プロセス 1 を有効にする（Enable Process 1）] が選択されています。最大 2 つの OSPF プロセス インスタンスを有効にできます。

ステップ 4 OSPFv3 ロールをドロップダウン リストから選択し、それに対応する説明を入力します。オプションは、[内部（Internal）]、[ABR]、[ASBR]、[ABR および ASBR（ABR and ASBR）] です。OSPFv3 ロールの説明については、OSPF の概要 （971 ページ）を参照してください。

ステップ 5 [エリア（Area）] タブを選択し、[追加（Add）] をクリックします。

編集アイコン（  ）をクリックするか、右クリック メニューを使用して、エリアの切り取り、コピー、貼り付け、挿入、および削除を行うことができます。

ステップ 6 [一般（General）] タブを選択し、各 OSPF プロセスについて次のオプションを設定します。

- [エリア ID（Area ID）]：ルートを要約するエリア。
- [コスト（Cost）]：この集約ルートのメトリックまたはコスト。宛先への最短パスを決定するための OSPF SPF 計算で使用します。有効な値の範囲は 0 ～ 16777215 です。
- [タイプ（Type）]：[標準（Normal）]、[NSSA]、[スタブ（Stub）] を指定します。[標準（Normal）] を選択した場合、設定するその他のパラメータはありません。[スタブ（Stub）] を選択した場合、エ

リアでサマリー LSA を送信することができます。[NSSA] を選択した場合、次の 3 つのオプションを設定できます。

- [このエリアへのサマリー LSA の送信を許可する（Allow Sending summary LSA into this area）]：エリアにサマリー LSA を送信することを許可します。
- [標準および NSSA エリアにインポート ルートを再配布する（Redistribute imports routes to normal and NSSA area）]：再配布でルートをスタブ エリアでなく標準エリアにインポートできるようになります。
- [デフォルト情報生成（Defaults information originate）]：OSPFv3 ルーティング ドメインへのデフォルト外部ルートを生成します。

- [メトリック（Metric）]：デフォルト ルートを生成するために使用するメトリック。デフォルト値は 10 です。有効なメトリック値の範囲は、0 ～ 16777214 です。
- [メトリック タイプ（Metric Type）]：メトリック タイプは、OSPFv3 ルーティング ドメインにアドバタイズされるデフォルト ルートに関連付けられた外部リンク タイプです。使用可能なオプションは、タイプ 1 外部ルートの場合は 1、タイプ 2 外部ルートの場合は 2 です。

ステップ 7 [OK] をクリックして、一般設定を保存します。

ステップ 8 [ルート集約（Route Summary）] タブを選択し、[ルート集約の追加（Add Route Summary）] をクリックします。

編集アイコン（）をクリックするか、右クリック メニューを使用して、ルート集約の切り取り、コピー、貼り付け、挿入、および削除を行うことができます。

ステップ 9 OSPF プロセスごとに、次のルート集約オプションを設定します。

- [IPv6 プレフィックス/長さ（IPv6 Prefix/Length）]：IPv6 プレフィックス。新しいネットワーク オブジェクトを追加するには、追加アイコン（）をクリックします。ネットワークを追加する手順については、ネットワーク オブジェクト （525 ページ）を参照してください。
- [コスト（Cost）]：この集約ルートのメトリックまたはコスト。宛先への最短パスを決定するための OSPF SPF 計算で使用します。有効な値の範囲は 0 ～ 16777215 です。
- [アドバタイズ（Advertise）]：集約ルートをアドバタイズします。サマリー アドレスになるルートを抑止するには、このチェックボックスをオフにします。デフォルトでは、このチェックボックスはオンになっています。

ステップ 10 [OK] をクリックして、ルート集約設定を保存します。

ステップ 11 [仮想リンク（Virtual Link）] タブを選択し、[仮想リンクの追加（Add Virtual Link）] をクリックして、各 OSPF プロセスについて次のオプションを設定します。

- [ピア ルータ ID（Peer RouterID）]：ピア ルータの IP アドレスを選択します。新しいネットワーク オブジェクトを追加するには、追加アイコン（）をクリックします。ネットワークを追加する手順については、ネットワーク オブジェクト （525 ページ）を参照してください。

- [TTL セキュリティ（TTL Security）]：TTL セキュリティ チェックを有効にします。このホップカウントの値は、1 ～ 254 の数値です。デフォルトは 1 です。

  OSPF は、IP ヘッダー存続可能時間（TTL）の値が 255 の発信パケットを送信し、設定可能なしきい値よりも低い TTL 値の入力パケットを廃棄します。IP パケットを転送する各デバイスは TTL が低下するため、直接（1 ホップ）接続により受信されたパケットの TTL 値は 255 になります。2 つのホップを通過するパケットの値は 254 というようになります。受信しきい値は、パケットが移動する可能性がある最大ホップ数で設定されます。

- [Dead 間隔（Dead Interval）]：hello パケットが届かなかった場合にネイバーがルータのダウンを示すまでの時間（秒単位）。デフォルトは hello 間隔の 4 倍または 40 秒です。有効な値の範囲は 1 ～ 65535 です。

  Dead 間隔は符号なし整数です。この値は、共通のネットワークに接続されているすべてのルータおよびアクセス サーバで同じであることが必要です。

- [Hello 間隔（Hello Interval）]：hello パケットがインターフェイスで送信される間隔（秒単位）。有効な値の範囲は 1 ～ 65535 です。デフォルトは 10 です。

  hello 間隔は、hello パケットでアドバタイズされる符号なし整数です。この値は、特定のネットワーク上のすべてのルータおよびアクセス サーバで同じである必要があります。hello 間隔を小さくすると、トポロジ変更が検出されるまでの時間が短くなりますが、インターフェイス上で送信されるトラフィックは多くなります。

- [再転送間隔（Retransmit Interval）]：インターフェイスに属する隣接関係の LSA 再送信間の時間（秒単位）。再送信間隔は、接続されているネットワーク上の任意の 2 台のルータ間の予想されるラウンドトリップ遅延です。この値は、予想されるラウンドトリップ遅延より大きくなり、1 ～ 65535 の範囲で指定できます。デフォルトは 5 です。

  ルータが自身のネイバーに LSA を送信する場合、ルータは確認応答メッセージを受信するまでその LSA を保持します。確認応答を受信しなかった場合、ルータでは LSA を再送します。この値は控えめに設定する必要があります。そうしないと、不要な再送信が発生する可能性があります。シリアル回線および仮想リンクの場合は、値を大きくする必要があります。

- [転送遅延（Transmit Delay）]：インターフェイス上で LSA パケットを送信するために必要と推定される時間（秒単位）。ゼロよりも大きい整数値を指定します。有効な値の範囲は 1 ～ 8192 です。デフォルトは 1 です。

  アップデート パケット内の LSA 自体の経過時間は、転送前にこの値の分だけ増分されます。リンクでの送信前に遅延が加算されていない場合、LSA がリンクを介して伝播する時間は考慮されません。値は、インターフェイスの送信および伝播遅延を考慮して割り当てる必要があります。この設定は、非常に低速のリンクでより重要な意味を持ちます。

ステップ 12 [OK] をクリックして、仮想リンク設定を保存します。

ステップ 13 [ルータ（Router）] ページで [保存（Save）] をクリックして変更を保存します。

次のタスク

OSPFv3 再配布の設定を続けます。

OSPFv3 再配布の設定

Firepower Threat Defense デバイスは、OSPF ルーティング プロセス間のルート再配布を制御できます。1 つのルーティング プロセスから OSPF ルーティング プロセスへの再配布ルートのルールが表示されます。RIP および BGP で検出されたルートを、OSPF ルーティング プロセスに再配布することができます。スタティック ルートおよび接続されているルートも、OSPF ルーティング プロセスに再配布できます。

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** の順に選択し、FTD デバイスを編集します。

ステップ 2 [ルーティング（Routing）] > [OSPF] を選択します。

ステップ 3 [再配布（Redistribution）] タブを選択し、[追加（Add）] をクリックします。

編集アイコン（）をクリックするか、右クリック メニューを使用して、エリアの切り取り、コピー、貼り付け、挿入、および削除を行うことができます。

ステップ 4 OSPF プロセスごとに、次の再配布オプションを設定します。

- [ソース プロトコル（Source Protocol）]：ルートの再配布元となるソース プロトコル。サポートされるプロトコルは、接続済み、OSPF、スタティック、BGP です。OSPF を選択した場合は、[プロセス ID（Process ID）] フィールドにプロセス ID を入力する必要があります。BCP を選択した場合は、[AS 番号（AS Number）] フィールドに AS 番号を追加する必要があります。
- [メトリック（Metric）]：配布されるルートのメトリック値。 デフォルト値は 10 です。有効な値の範囲は 0 ～ 16777214 です。

  同じデバイス上で 1 つの OSPF プロセスから別の OSPF プロセスに再配布する場合、メトリック値を指定しないと、メトリックは 1 つのプロセスから他のプロセスへ存続します。他のプロセスを OSPF プロセスに再配布するときに、メトリック値を指定しない場合、デフォルトのメトリックは 20 です。
- [メトリック タイプ（Metric Type）]：メトリック タイプは、OSPF ルーティング ドメインにアドバタイズされるデフォルト ルートに関連付けられた外部リンク タイプです。使用可能なオプションは、タイプ 1 外部ルートの場合は 1、タイプ 2 外部ルートの場合は 2 です。
- [タグ（Tag）]：タグは 32 ビット 10 進数値を指定します。この値は、OSPF 自身では使用されないが ASBR 間の情報伝達に使用できる外部ルートのそれぞれに関連付けられます。何も指定しない場合、BGP および EGP からのルートにはリモート自律システムの番号が使用されます。その他のプロトコルについては、ゼロが使用されます。有効な値は、0 ～ 4294967295 です。
- [ルート マップ（Route Map）]：送信元ルーティング プロトコルから現在のルーティング プロトコルへのルートのインポートのフィルタリングをチェックします。このパラメータを指定しない場合、すべてのルートが再配布されます。このパラメータを指定し、ルート マップ タグが表示されていない場合、ルートはインポートされません。または、追加アイコン（）をクリックして新しいルート マッ

プを追加できます。新しいルートマップを追加する手順については、ルートマップ （606 ページ）を参照してください。

- [プロセス ID（Process ID）]：OSPF プロセス ID。1 または 2。

  （注） プロセス ID が有効であると、OSPFv3 プロセスは別の OSPFv3 プロセスから認識したルートを再配布します。

- [一致（Match）]：OSPF ルートを他のルーティング ドメインに再配布できるようにします。
  - [内部（Internal）] は、特定の自律システムの内部にあるルートです。
  - [外部 1（External 1）] は、自律システムの外部であるが、OSPFv3 にタイプ 1 外部ルートとしてインポートされるルートです。
  - [外部 2（External 2）] は、自律システムの外部であるが、OSPFv3 にタイプ 2 外部ルートとしてインポートされるルートです。
  - [NSSA 外部 1（NSSA External 1）] は、自律システムの外部であるが、IPv6 用の NSSA の OSPFv3 にタイプ 1 の外部ルートとしてインポートされるルートです。
  - [NSSA 外部 2（NSSA External 2）] は、自律システムの外部であるが、IPv6 用の NSSA の OSPFv3 にタイプ 2 の外部ルートとしてインポートされるルートです。

ステップ 5 [OK] をクリックして、再配布設定を保存します。

ステップ 6 [ルーティング（Routing）] ページで [保存（Save）] をクリックして変更を保存します。

次のタスク

OSPFv3 サマリー プレフィックスの設定 （994 ページ）に進みます。

OSPFv3 サマリー プレフィックスの設定

指定された IPv6 プレフィックスとマスクのペアに一致するルートをアドバタイズするように Firepower Threat Defense デバイスを設定できます。

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** の順に選択し、FTD デバイスを編集します。

ステップ 2 [ルーティング（Routing）] > [OSPFv3] を選択します。

ステップ 3 [サマリー プレフィックス（Summary Prefix）] タブを選択し、[追加（Add）] をクリックします。

編集アイコン（）をクリックするか、右クリック メニューを使用して、サマリー プレフィックスの切り取り、コピー、貼り付け、挿入、および削除を行うことができます。

ステップ 4 OSPF プロセスごとに、次のサマリー プレフィックス オプションを設定します。

- [IPv6 プレフィックス/長さ（IPv6 Prefix/Length）]：IPv6 プレフィックスとプレフィックス長のラベル。

  リストから 1 つを選択するか、追加（）アイコンをクリックして新しいネットワーク オブジェクトを追加します。ネットワークを追加する手順については、ネットワーク オブジェクト （525 ページ）を参照してください。
- [アドバタイズ（Advertise）]：指定されたプレフィックスとマスクのペアに一致するルートをアドバタイズします。このチェックボックスをオフにすると、指定されたプレフィックスとマスク ペアと一致するルートが抑制されます。
- （オプション）[タグ（Tag）]：ルート マップで再配布を制御するための「match」値として使用できるタグ値。

ステップ 5 [OK] をクリックして、サマリー プレフィックス設定を保存します。

ステップ 6 [ルーティング（Routing）] ページで [保存（Save）] をクリックして変更を保存します。

次のタスク

OSPFv3 インターフェイス、認証、およびネイバーの設定 （995 ページ）に進みます。

OSPFv3 インターフェイス、認証、およびネイバーの設定

必要に応じて特定のインターフェイス固有の OSPFv3 パラメータを変更できます。これらのパラメータを必ずしも変更する必要はありませんが、hello interval と dead interval というインターフェイスパラメータは、接続されているネットワーク内のすべてのルータで一致している必要があります。これらのパラメータを設定する場合は、ネットワーク上のすべてのルータで、コンフィギュレーションの値が矛盾していないことを確認してください。

ステップ 1 **[デバイス（Devices）] > [デバイス管理（Device Management）]** の順に選択し、FTD デバイスを編集します。

ステップ 2 [ルーティング（Routing）] > [OSPFv3] を選択します。

ステップ 3 [インターフェイス（Interface）] タブを選択し、[追加（Add）] をクリックします。

[鉛筆（Pencil）]アイコンをクリックして編集するか、右クリック メニューを使用して、エリアの切り取り、コピー、貼り付け、挿入、および削除を行うことができます。

ステップ 4 各 OSPFv3 プロセスについて、次のインターフェイス オプションを設定します。

- [インターフェイス（Interface）]：設定するインターフェイス。
- [OSPFv3 を有効にする（Enable OSPFv3）]：OSPFv3 を有効にします。
- [OSPF プロセス（OSPF Process）]：1 または 2 を選択します。
- [エリア（Area）]：このプロセスのエリア ID。

- [インスタンス（Instance）]：インターフェイスに割り当てるエリア インスタンス ID を指定します。インターフェイスは、OSPFv3 エリアを 1 つだけ保有できます。複数のインターフェイスで同じエリアを使用でき、各インターフェイスは異なるエリア インスタンス ID を使用できます。

ステップ 5 [プロパティ（Properties）] タブを選択し、各 OSPFv3 プロセスについて次のオプションを設定します。

- [発信リンク ステート アドバタイズメントをフィルタ（Filter Outgoing Link Status Advertisements）]：OSPFv3 インターフェイスへの発信 LSA をフィルタ処理します。デフォルトでは、すべての発信 LSA がインターフェイスにフラッディングされます。
- [MTU 不一致検出を無効にする（Disable MTU mismatch detection）]：DBD パケットが受信された場合、OSPF MTU 不一致検出を無効にします。OSPF MTU 不一致検出は、デフォルトで有効になっています。
- [フラッドの削減（Flood Reduction）]：エリア全体で 3600 秒ごとにフラッディングしないように、標準の LSA を [LSA をエージングしない（Do Not Age LSAs）] に変更します。

  OSPF LSA は 3600 秒ごとに更新されます。大規模な OSPF ネットワークでは、これにより大量の不要な LSA フラッディングがエリアからエリアに発生する可能性があります。
- [ポイントツーポイント ネットワーク（Point-to-Point Network）]：OSPF ルートを VPN トンネル経由で送信できます。インターフェイスをポイントツーポイント、非ブロードキャストとして設定すると、次の制限が適用されます。
  - インターフェイスにはネイバーを 1 つだけ定義できます。
  - ネイバーは手動で設定する必要があります
  - クリプト エンドポイントを指すスタティック ルートを定義する必要があります。
  - トンネル経由の OSPF がインターフェイスで実行中である場合は、アップストリーム ルータを使用する通常の OSPF を同じインターフェイス上で実行することはできません。
  - OSPF ネイバーを指定する前に、クリプト マップをインターフェイスにバインドする必要があります。これは、OSPF アップデートが VPN トンネルを通過できるようにするためです。OSPF ネイバーを指定した後でクリプト マップをインターフェイスにバインドした場合は、**clear local-host all** コマンドを使用して OSPF 接続をクリアします。これで、OSPF 隣接関係を VPN トンネル経由で確立できるようになります。
- [ブロードキャスト（Broadcast）]：インターフェイスがブロードキャスト インターフェイスであることを指定します。デフォルトでは、イーサネット インターフェイスの場合はこのチェックボックスがオンになっています。このチェックボックスをオフにすると、インターフェイスをポイントツーポイントの非ブロードキャスト インターフェイスとして指定したことになります。インターフェイスをポイントツーポイントの非ブロードキャストとして指定すると、OSPF ルートを VPN トンネル経由で送信できます。
- [コスト（Cost）]：インターフェイスでパケットを送信するコストを指定します。この設定の有効値の範囲は 0 ～ 255 です。デフォルト値は 1 です。この設定に 0 を入力すると、適切でないルータが指定ルータになったり、指定ルータのバックアップが行われたりします。この設定は、ポイントツー

ポイントの非ブロードキャスト インターフェイスとして設定されているインターフェイスには適用されません。

2つのルータがネットワークに接続している場合、両方が指定ルータになろうとします。ルータ優先順位の高いデバイスが指定ルータになります。ルータ優先順位が同じ場合は、ルータ ID が高い方が指定ルータになります。

- [優先順位（Priority）]：ネットワークの代表ルータを指定します。有効な値の範囲は 0 ～ 255 です。
- [Dead 間隔（Dead Interval）]：hello パケットが確認されない場合に、ルータがダウンしたとネイバーが判断するまでの待ち時間（秒単位）。この値はネットワーク上のすべてのノードで同じにする必要があります。値の範囲は、1 ～ 65535 です。
- [ポーリング間隔（Poll Interval）]：ネイバーとの隣接関係が確立される前にルータが送信する OSPF パケット間の期間（秒単位）。ルーティング デバイスがアクティブなネイバーを検出すると、hello パケット間隔はポーリング間隔で指定された時間から Hello 間隔で指定された時間に変更されます。有効な値の範囲は、1 ～ 65535 秒です。
- [再送信間隔（Retransmit Interval）]：インターフェイスに属する隣接関係の LSA 再送信間の時間（秒単位）。接続ネットワーク上の任意の 2 台のルータ間で想定される往復遅延より大きな値にする必要があります。有効値の範囲は、1 ～ 65535 秒です。デフォルトは 5 秒です。
- [転送遅延（Transmit Delay）]：インターフェイス上でリンクステート更新パケットを送信する予想時間（秒単位）。有効値の範囲は、1 ～ 65535 秒です。デフォルト値は 1 秒です。

ステップ 6 [OK] をクリックして、プロパティ設定を保存します。

ステップ 7 [認証（Authentication）] タブを選択し、各 OSPFv3 プロセスについて次のオプションを設定します。

- [タイプ（Type）]：認証のタイプ。使用可能なオプションは、[Area]、[Interface]、[None] です。[None] オプションを選択すると、認証が行われません。
- [セキュリティ パラメータ インデックス（Security Parameters Index）]：256 ～ 4294967295 の数値。タイプとして [インターフェイス（Interface）] を選択した場合、このオプションを設定します。
- [認証（Authentication）]：認証アルゴリズムのタイプ。サポートされる値は、[SHA-1] および [MD5] です。タイプとして [インターフェイス（Interface）] を選択した場合、このオプションを設定します。
- [認証キー（Authentication Key）]：MD5 認証を使用する場合、キーの長さは 32 桁の 16 進数（16 バイト）である必要があります。SHA-1 認証を使用する場合、キーの長さは 40 桁の 16 進数（20 バイト）である必要があります。
- [認証キーを暗号化する（Encrypt Authentication Key）]：認証キーの暗号化を有効にします。
- [暗号化を含める（Include Encryption）]：暗号化を有効にします。
- [暗号化アルゴリズム（Encryption Algorithm）]：暗号化アルゴリズムのタイプ。サポートされる値は DES です。ヌルのエントリは暗号化されません。[暗号化を含める（Include Encryption）] を選択した場合、このオプションを設定します。

- [暗号化キー（Encryption Key）]：暗号キーを入力します。[暗号化を含める（Include Encryption）] を選択した場合、このオプションを設定します。
- [キーを暗号化する（Encrypt Key）]：キーを暗号化できるようにします。

ステップ 8 [OK] をクリックして、認証設定を保存します。

ステップ 9 [ネイバー（Neighbor）] タブを選択し、[追加（Add）] をクリックして、各 OSPFv3 プロセスについて次のオプションを設定します。

- [リンク ローカル アドレス（Link Local Address）]：スタティック ネイバーの IPv6 アドレス。
- [コスト（Cost）]：コストを有効にします。アドバタイズする場合は、[コスト（Cost）] フィールドにコストを入力し、[発信リンク ステート アドバタイズメントをフィルタ（Filter Outgoing Link State Advertisements）] をオンにします。
- （オプション）[ポーリング間隔（Poll Interval）]：ポーリング間隔を有効にします。[優先順位（Priority）] レベルと [ポーリング間隔（Poll Interval）]（秒単位）を入力します。

ステップ 10 [追加（Add）] をクリックして、ネイバーを追加します。

ステップ 11 [OK] をクリックして、インターフェイス設定を保存します。

OSPFv3 詳細プロパティの設定

[高度なプロパティ（Advanced Properties）] タブを使用すると、syslog メッセージ生成、アドミニストレーティブ ルート ディスタンス、パッシブ OSPFv3 ルーティング、LSA タイマー、グレースフル リスタートなどのオプションを設定できます。

グレースフル リスタート

Firepower Threat Defense デバイスでは、既知の障害状況が発生することがあります。これにより、スイッチング プラットフォーム全体でパケット転送に影響を与えることがあってはなりません。Non-Stop Forwarding（NSF）機能では、ルーティング プロトコル情報を復元している間に、既知のルートへのデータ転送が続行されます。この機能は、スケジュール済みヒットレス ソフトウェア アップグレードがあるときに便利です。グレースフル リスタート（RFC 5187）を使用して、OSPFv3 上でグレースフル リスタートを設定できます。

（注） NSF 機能は HA モードとクラスタリングでも役立ちます。

NSF グレースフル リスタート機能の設定には、機能の設定と NSF 対応または NSF 認識としてのデバイスの設定という 2 つのステップが伴います。NSF 対応デバイスは、ネイバーに対して独自のリスタート アクティビティを示すことができ、NSF 認識デバイスはネイバーのリスタートをサポートすることができます。

デバイスは、いくつかの条件に応じて、NSF 対応または NSF 認識として設定できます。

- デバイスは、現在のデバイスのモードに関係なく、NSF 認識デバイスとして設定できます。
- デバイスを NSF 対応として設定するには、デバイスはフェールオーバーまたはスパンド EtherChannel（L2）クラスタ モードのいずれかである必要があります。
- デバイスを NSF 認識または NSF 対応にするには、必要に応じて opaque リンク ステート アドバタイズメント（LSA）/リンク ローカル シグナリング（LLS）ブロックの機能を使って設定する必要があります。

ステップ 1 **[デバイス（Devices）] > [デバイス管理（Device Management）]** の順に選択し、FTD デバイスを編集します。

ステップ 2 [ルーティング（Routing）] > [OSPFv3] を選択し、[詳細（Advanced）] をクリックします。

ステップ 3 [ルータ ID（Router ID）] には、[自動（Automatic）] または [IP アドレス（IP address）] を選択します。[IP アドレス（IP address）] を選択する場合は、[IP アドレス（IP Address）] フィールドに IP アドレスを入力します。

ステップ 4 ルートがサポートされていない LSA タイプ 6 Multicast OSPF（MOSPF）パケットを受信する場合に syslog メッセージを抑制するには、[LSA MOSPF を無視（Ignore LSA MOSPF）] チェックボックスをオンにします。

ステップ 5 [一般（General）] タブを選択し、次のように設定します。

- [隣接関係の変更（Adjacency Changes）]：syslog メッセージが送信される隣接関係の変更内容を定義します。

  デフォルトでは、OSPF ネイバーがアップ状態またはダウン状態になったときに、syslog メッセージが生成されます。OSPF ネイバーがダウンしたときに syslog メッセージを送信するようルータを設定することも、状態ごとに syslog を送信するように設定することもできます。

  - [隣接関係の変更（Adjacency Changes）]：OSPF ネイバーが起動または停止したときに、Firepower Threat Defense デバイスによって syslog メッセージが送信されるようになります。この設定は、デフォルトでオンになっています。
  - [詳細を含める（Include Details）]：ネイバーがアップ状態またはダウン状態になったときだけでなく、状態の変更が発生したときにも Firepower Threat Defense デバイスによって syslog メッセージが送信されるようになります。デフォルトでは、この設定はオフになっています。

- [アドミニストレーティブ ルート ディスタンス（Administrative Route Distances）]：エリア間、エリア内、および外部 IPv6 ルートのアドミニストレーティブ ルート ディスタンスの設定に使用された設定を変更できます。アドミニストレーティブ ルート ディスタンスは 1 ～ 254 の整数です。デフォルトは 110 です。
- [デフォルト情報の発信（Default Information Originate）]：デフォルトの外部ルートを OSPFv3 ルーティング ドメインに生成するには、[有効化（Enable）] チェックボックスをオンにして、次のオプションを設定します。
  - [常にアドバタイズする（Always Advertise）]：デフォルト ルートが存在するかどうかにかかわらず、常にアドバタイズします。

- [メトリック（Metric）]：デフォルト ルートを生成するために使用するメトリック。有効なメトリック値の範囲は、0 ～ 16777214 です。デフォルト値は 10 です。
- [メトリック タイプ（Metric Type）]：OSPFv3 ルーティング ドメインにアドバタイズされるデフォルト ルートに関連付けられた外部リンク タイプ。有効な値は 1（タイプ 1 の外部ルート）および 2（タイプ 2 の外部ルート）です。デフォルトはタイプ 2 外部ルートです。
- [ルート マップ（Route Map）]：ルート マップが満たされている場合にデフォルト ルートを生成するルーティング プロセスを選択するか、追加アイコン（  ）をクリックして、新しいルーティング プロセスを追加します。新しいルート マップを追加するには、ルート マップ （606 ページ）を参照してください。

ステップ 6 [OK] をクリックして、一般設定を保存します。

ステップ 7 [パッシブ インターフェイス（Passive Interfaces）] タブを選択して、[使用可能なインターフェイス（Available Interfaces）] リストからパッシブ OSPFv3 ルーティングを有効にするインターフェイスを選択し、[追加（Add）] をクリックして [選択したインターフェイス（Selected Interfaces）] リストにこれらを移動します。

パッシブ ルーティングは、OSPFv3 ルーティング情報のアドバタイズメントの制御に有効であり、インターフェイスでの OSPFv3 ルーティング更新の送受信を無効にします。

ステップ 8 [OK] をクリックしてパッシブ インターフェイス設定を保存します。

ステップ 9 [タイマー（Timer）] タブを選択し、次の LSA ペーシングと SPF 計算タイマーを設定します。

- [到着（Arrival）]：ネイバーから到着する同一 LSA の最短受信間隔をミリ秒単位で指定します。有効な範囲は 0 ～ 6000,000 ミリ秒です。デフォルトは 1000 ミリ秒です。
- [フラッド ペーシング（Flood Pacing）]：フラッディング キュー内の LSA が更新間にペーシング処理される時間を指定します（ミリ秒単位）。設定できる範囲は 5 ～ 100 ミリ秒です。デフォルト値は 33 ミリ秒です。
- [グループ ペーシング（Group Pacing）]：LSA をグループにまとめてリフレッシュ、チェックサム計算、エージングする間隔を秒単位で指定します。有効値の範囲は 10 ～ 1800 です。デフォルト値は 240 です。
- [再送信ペーシング（Retransmission Pacing）]：再送信キュー内の LSA がペースされる時間をミリ秒単位で指定します。設定できる範囲は 5 ～ 200 ミリ秒です。デフォルト値は 66 ミリ秒です。
- [LSA スロットル（LSA Throttle）]：LSA の最初のオカレンスを生成する遅延を指定します（ミリ秒単位）。デフォルト値は、0 ミリ秒です。最小値は、同じ LSA を送信する最小遅延をミリ秒単位で指定します。デフォルト値は、5000 ミリ秒です。最大値は、同じ LSA を送信する最大遅延をミリ秒単位で指定します。デフォルト値は 5000 ミリ秒です。

  （注） LSA スロットリングでは、最小時間または最大時間が最初のオカレンスの値よりも小さい場合、OSPFv3 が自動的に最初のオカレンス値に修正します。同様に、指定された最遅延が最小遅延よりも小さい場合、OSPFv3 が自動的に最小遅延値に修正します。

- [SPF スロットル（SPF Throttle）]：SPF 計算の変更を受信する遅延をミリ秒単位で指定します。デフォルト値は、5000 ミリ秒です。最小値は、最初と 2 番目の SPF 計算の間の遅延をミリ秒単位で指

定します。デフォルト値は、10000 ミリ秒です。最大値は、SPF 計算の最大待機時間をミリ秒単位で指定します。デフォルト値は 10000 ミリ秒です。

（注） SPF スロットリングでは、最短時間または最長時間が最初のオカレンスの値よりも小さい場合、OSPFv3 が自動的に最初のオカレンス値に修正します。同様に、指定された最遅延が最小遅延よりも小さい場合、OSPFv3 が自動的に最小遅延値に修正します。

ステップ 10 [OK] をクリックして LSA タイマー設定を保存します。

ステップ 11 [Non Stop Forwarding] タブを選択し、[グレースフル リスタート ヘルパーを有効にする（Enable graceful-restart helper）] チェックボックスをオンにします。このチェックボックスは、デフォルトではオンになっています。NSF 認識デバイスでグレースフル リスタート ヘルパー モードを無効にするには、このチェックボックスをオフにします。

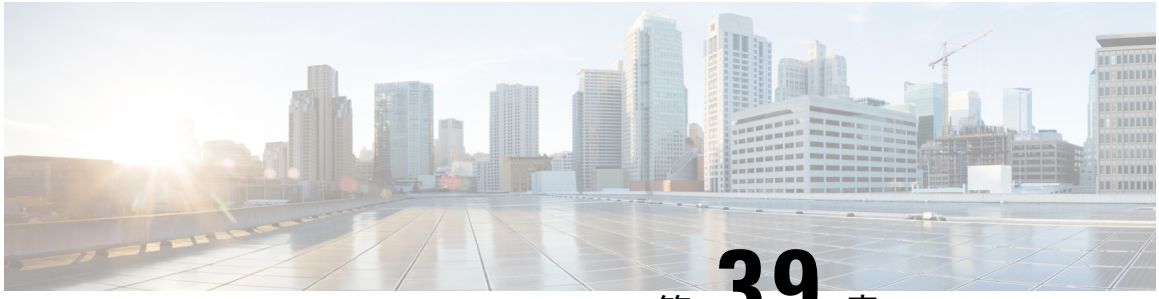
ステップ 12 [リンク ステート アドバタイズメントを有効にする（Enable link state advertisement）] チェックボックスをオンにして、厳密なリンク ステート アドバタイズメント チェックを有効にします。

有効にすると、再起動ルータにフラッディングされる可能性がある LSA への変更があることが検出された場合、またはグレースフル リスタート プロセスが開始されたときに再起動ルータの再送リスト内に変更された LSA があると検出された場合、ヘルパー ルータはルータの再起動プロセスを終了させることを示します。

ステップ 13 [グレースフル リスタートを有効にする（スパンド クラスタまたはフェールオーバーが設定されている場合に使用）（Enable graceful-restart (Use when Spanned Cluster or Failover Configured)）] をオンにして、グレースフル リスタート間隔を秒単位で入力します。範囲は 1 ～ 1800 です。デフォルト値は 120 秒です。30 秒以下のリスタート間隔の場合、グレースフル リスタートは終了します。

ステップ 14 [OK] をクリックしてグレースフル リスタート設定を保存します。

ステップ 15 [ルーティング（Routing）] ページで [保存（Save）] をクリックして変更を保存します。



第 39 章

Firepower Threat Defense の BGP

この項では、Border Gateway Protocol（BGP）を使用してデータのルーティング、認証の実行、ルーティング情報の再配布を行うように FTD を設定する方法について説明します。

BGPについて

BGP は相互および内部の自律システムのルーティング プロトコルです。自律システムとは、共通の管理下にあり、共通のルーティング ポリシーを使用するネットワークまたはネットワーク グループです。BGP は、インターネットのルーティング情報を交換するために、インターネット サービス プロバイダー（ISP）間で使用されるプロトコルです。

ルーティング テーブルの変更

BGP ネイバーは、ネイバー間で最初に TCP 接続を確立する際に、完全なルーティング情報を交換します。ルーティングテーブルで変更が検出された場合、BGPルータはネイバーに対し、変更されたルートのみを送信します。BGP ルータは、定期的にルーティング アップデートを送信しません。また BGP ルーティング アップデートは、宛先ネットワークに対する最適パスのアドバタイズのみを行います。

BGPにより学習されたルートには、特定の宛先に対して複数のパスが存在する場合、宛先に対する最適なルートを決定するために使用されるプロパティが設定されています。これらのプロパティは BGP 属性と呼ばれ、ルート選択プロセスで使用されます。

- Weight：これは、シスコ定義の属性で、ルータに対してローカルです。Weight 属性は、隣接ルータにアドバタイズされません。ルータが同じ宛先への複数のルートがあることを学習すると、Weight が最も大きいルートが優先されます。
- Local preference：Local preference 属性は、ローカル AS からの出力点を選択するために使用されます。Weight 属性とは異なり、Local preference 属性は、ローカル AS 全体に伝搬さ

れます。AS からの出力点が複数ある場合は、Local preference 属性が最も高い出力点が特定のルートの出力点として使用されます。

- Multi-exit discriminator：メトリック属性である Multi-exit discriminator（MED）は、メトリックをアドバタイズしている AS への優先ルートに関して、外部 AS への提案として使用されます。これが提案と呼ばれるのは、MED を受信している外部 AS がルート選択の際に他の BGP 属性も使用している可能性があるためです。MED メトリックが小さい方のルートが優先されます。
- Origin：Origin 属性は、BGP が特定のルートについてどのように学習したかを示します。Origin 属性は、次の 3 つの値のいずれかに設定することができ、ルート選択に使用されます。
  - IGP：ルートは発信側 AS の内部にあります。この値は、ネットワーク ルータ コンフィギュレーション コマンドを使用して BGP にルートを挿入する場合に設定されます。
  - EGP：ルートは Exterior Border Gateway Protocol（EBGP）を使用して学習されます。
  - Incomplete：ルートの送信元が不明であるか、他の方法で学習されています。Incomplete の Origin は、ルートが BGP に再配布されるときに発生します。
- AS_path：ルートアドバタイズメントが自律システムを通過すると、ルートアドバタイズメントが通過した AS 番号が AS 番号の順序付きリストに追加されます。AS_path リストが最も短いルートのみ、IP ルーティング テーブルにインストールされます。
- Next hop：EBGP の Next-hop 属性は、アドバタイズしているルータに到達するために使用される IP アドレスです。EBGP ピアの場合、ネクスト ホップ アドレスは、ピア間の接続の IP アドレスです。IBGP の場合、EBGP のネクスト ホップ アドレスがローカル AS に伝送されます。
- Community：Community 属性は、ルーティングの決定（承認、優先度、再配布など）を適用できる宛先をグループ化する方法、つまりコミュニティを提供します。ルート マップは、Community 属性を設定するために使用されます。事前定義済みの Community 属性は次のとおりです。
  - no-export：EBGP ピアにこのルートをアドバタイズしません。
  - no-advertise：このルートをどのピアにもアドバタイズしない。
  - internet：インターネット コミュニティにこのルートをアドバタイズします。ネットワーク内のすべてのルートがこのコミュニティに属します。

BGP を使用する状況

大学や企業などの顧客ネットワークでは、そのネットワーク内でルーティング情報を交換するために OSPF などの内部ゲートウェイ プロトコル（IGP）を通常使用しています。カスタマーは ISP に接続し、ISP は BGP を使用してカスタマーおよび ISP ルートを交換します。自律システム（AS）間で BGP を使用する場合、このプロトコルは外部 BGP（EBGP）と呼ばれます。

サービス プロバイダーが BGP を使用して AS 内でルートを交換する場合、このプロトコルは内部 BGP（IBGP）と呼ばれます。

BGP は、IPv6 ネットワーク上で IPv6 プレフィックスのルーティング情報を伝送するために使用することができます。

BGP パスの選択

BGP は、異なる送信元から同じルートの複数のアドバタイズメントを受信する場合があります。BGP は最適なパスとして 1 つのパスだけを選択します。このパスを選択すると、BGP は IP ルーティング テーブルに選択したパスを格納し、そのネイバーにパスを伝搬します。BGP は次の基準を使用して（示されている順序で）、宛先へのパスを選択します。

- パスで指定されているネクストホップが到達不能な場合、このアップデートは削除されます。
- Weight が最大のパスが優先されます。
- Weight が同じである場合、Local preference が最大のパスが優先されます。
- Local preference が同じである場合、このルータで動作している BGP により発信されたパスが優先されます。
- ルートが発信されていない場合、AS_path が最短のルートが優先されます。
- すべてのパスの AS_path の長さが同じである場合、Origin タイプが最下位のパス（IGP は EGP よりも低く、EGP は Incomplete よりも低い）が優先されます。
- Origin コードが同じである場合、最も小さい MED 属性を持つパスが優先されます。
- パスの MED が同じである場合、内部パスより外部パスが優先されます。
- それでもパスが同じである場合、最も近い IGP ネイバーを経由するパスが優先されます。
- BGP マルチパス （1005 ページ） のルーティング テーブルで、複数のパスのインストールが必要かどうかを判断します。
- 両方のパスが外部の場合、最初に受信したパス（最も古いパス）が優先されます。
- BGP ルータ ID で指定された、IP アドレスが最も小さいパスが優先されます。
- 送信元またはルータ ID が複数のパスで同じである場合、クラスタ リストの長さが最小のパスが優先されます。
- 最も小さいネイバー アドレスから発信されたパスが優先されます。

BGP マルチパス

BGP マルチパスでは、同一の宛先プレフィックスへの複数の等コスト BGP パスを IP ルーティング テーブルに組み込むことができます。その場合、宛先プレフィックスへのトラフィックは、組み込まれたすべてのパス間で共有されます。

これらのパスは、負荷共有のためのベスト パスと共にテーブルに組み込まれます。BGP マルチパスは、ベストパスの選択には影響しません。たとえば、ルータは引き続き、アルゴリズムに従っていずれかのパスをベスト パスとして指定し、このベスト パスをルータの BGP ピアにアドバタイズします。

同一宛先へのパスをマルチパスの候補にするには、これらのパスの次の特性がベストパスと同等である必要があります。

- 重量
- ローカル プリファレンス
- AS-PATH の長さ
- オリジン コード
- Multi Exit Discriminator（MED）
- 次のいずれかです。
  - ネイバー AS またはサブ AS（BGP マルチパスの追加前）
  - AS-PATH（BGP マルチパスの追加後）

一部の BGP マルチパス機能では、マルチパス候補に要件が追加されます。

- パスは外部ネイバーまたは連合外部ネイバー（eBGP）から学習される必要があります。
- BGP ネクスト ホップへの IGP メトリックは、ベストパス IGP メトリックと同等である必要があります。

内部 BGP（iBGP）マルチパス候補の追加要件を次に示します。

- 内部ネイバー（iBGP）からパスが学習される必要があります。
- ルータが不等コスト iBGP マルチ パス用に設定されていない限り、BGP ネクストホップへの IGP メトリックは、ベスト パス IGP メトリックと同等です。

BGP はマルチパス候補から最近受信したパスのうち、最大 *n* 本のパスを IP ルーティング テーブルに挿入します。この *n* は、BGP マルチパスの設定時に指定した、ルーティング テーブルに組み込まれるルートの数です。マルチパスが無効な場合のデフォルト値は 1 です。

不等コスト ロード バランシングの場合、BGP リンク帯域幅も使用できます。

（注） 内部ピアへの転送前に、eBGP マルチパスで選択されたベストパスに対し、同等の next-hop-self が実行されます。

BGP のガイドライン

ファイアウォール モードのガイドライン

トランスペアレント ファイアウォール モードはサポートされません。BGP は、ルーテッド モードでのみサポートされています。

IPv6 のガイドライン

IPv6 をサポートします。グレースフル リスタートは、IPv6 アドレス ファミリではサポートされません。

BGP を設定する。

BGP を設定するには、以下のトピックを参照してください。

ステップ 1 BGP 基本設定 （1007 ページ）
ステップ 2 BGP 一般設定 （1010 ページ）
ステップ 3 BGP ネイバーの設定 （1012 ページ）
ステップ 4 BGP 集約アドレス設定 （1016 ページ）
ステップ 5 BGPv4 フィルタリング設定 （1017 ページ）

（注） フィルタリング セクションは、IPv4 設定にのみ適用されます。

ステップ 6 BGP ネットワーク設定 （1018 ページ）
ステップ 7 BGP 再配布設定 （1018 ページ）
ステップ 8 BGP ルート注入の設定 （1019 ページ）

BGP 基本設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin Access Admin Network Admin

BGP の多くの基本設定が可能です。

ステップ 1 **[デバイス（Devices）] > [デバイス管理（Device Management）]** の順に選択し、FTD デバイスを編集します。

ステップ 2 [ルーティング（Routing）] タブを選択します。

ステップ 3 [BGP] を選択します。

ステップ 4 [Enable BGP] チェックボックスをオンにして、BGP ルーティングプロセスを有効にします。

ステップ 5 [AS 番号（AS Number）] フィールドに、BGP プロセスの自律システム（AS）番号を入力します。AS 番号内部には、複数の自律番号が含まれます。AS 番号には、1 ～ 4294967295 または 1.0 ～ 65535.65535 を指定できます。AS 番号は固有に割り当てられた値であるため、インターネットの各ネットワークが識別されます。

ステップ 6 （オプション）[General] でさまざまな BGP 設定を編集します。これらの設定のデフォルトはほとんどの場合で適切ですが、ネットワークのニーズに合わせて調整できます。[編集（Edit）]（鉛筆）ボタンをクリックして、グループの設定を編集します。

a) [ルータ ID（Router ID）] ドロップダウンリストで、[自動（Automatic）] または [手動（Manual）] を選択します。自動を選択すると、Firepower Threat Defense デバイス上で最上位の IP アドレスがルータ ID として使用されます。固定ルータ ID を使用するには、[手動（Manual）] を選択して、[IP アドレス（IP Address）] フィールドに IPv4 アドレスを入力します。デフォルト値は [自動（Automatic）] です。

b) [AS_パス属性の AS 番号の数（number of AS numbers in AS_PATH attribute）] を入力します。AS パス属性は、移動パケットの最短ルートになる送信元と宛先のルータ間の中間 AS 番号のシーケンスです。有効な値は、1 ～ 254 です。デフォルト値は None です。

c) [ログ ネイバー変更（Log Neighbor Changes）] チェックボックスをオンにして、BGP ネイバーの変更（アップ状態またはダウン状態）およびリセットのロギングをイネーブルにします。これは、ネットワーク接続の問題をトラブルシューティングしたり、ネットワークの安定性を評価する際に役に立ちます。この設定はデフォルトで有効になっています。

d) [TCP パス MTU ディスカバリ使用（Use TCP path MTU discovery）] チェックボックスをオンにし、パス MTU 手法を使用して 2 つの IP ホスト間のネットワーク パスにおける最大伝送単位（MTU）のサイズを決定します。これにより、IP フラグメンテーションが回避されます。この設定はデフォルトで有効になっています。

e) [フェールオーバー後すぐにセッションをリセット（Reset session upon Failover）] チェックボックスをオンにして、リンク障害の発生時に外部 BGP セッションをただちにリセットします。この設定はデフォルトで有効になっています。

f) [最初の AS を EBGP ルートのピアの AS として実行（Enforce that first AS is peer's AS for EBGP routes）] チェックボックスをオンにして、その AS 番号を AS_path 属性の 1 つ目のセグメントとしてリストしていない外部 BGP ピアから受信した着信アップデートを破棄します。これにより、誤って設定されたピアや許可されていないピアが、別の自律システムから送信されたかのようにルートをアドバイタイズしてトラフィックを誤った宛先に送信することがなくなります。この設定はデフォルトで有効になっています。

g) [AS 番号のドット表記を使用（Use dot notation for AS numbers）] チェックボックスをオンにして、完全なバイナリ 4 バイトの AS 番号を、ドットで区切られた 16 ビットの 2 文字ずつに分割します。0 ～ 65553 の AS 番号は 10 進数で表され、65535 を超える AS 番号はドット付き表記を使用して表されます。これは、デフォルトでは無効になっています。

h) [OK] をクリックします。

ステップ 7 （オプション）[ベスト パス選択（Best Path Selection）] セクションを編集します。

a) [デフォルト ローカル優先度（Default Local Preference）] で 0 ～ 4294967295 の値を入力します。デフォルト値は 100 です。値が大きいほど、優先度が高いことを示します。この優先度は、ローカル自律システム内のすべてのルータおよびアクセス サーバに送信されます。

b) [異なるネイバーからの MED 比較を許可（Allow comparing MED from different neighbors）] チェックボックスをオンにして、さまざまな自律システムのネイバーからのパスにおいて Multi-exit discriminator（MED）の比較ができるようにします。これは、デフォルトでは無効になっています。

c) [同一 EBGP パスのルータ ID を比較（Compare Router ID for identical EBGP paths）] チェックボックスをオンにして、最適なパスの選択プロセス中に、外部 BGP ピアから受信した類似のパスを比較し、最適なパスをルータ ID が最も小さいルートに切り替えます。これは、デフォルトでは無効になっています。

d) [隣接する AS がアドバタイズしたパス間の最適 MED を選別（Pick the best MED path among paths advertised from the neighboring AS）] チェックボックスをオンにして、連合ピアから学習したパス間における MED 比較を有効にします。MED 間の比較は、外部の自律システムがパスに存在しない場合にのみ行われます。これは、デフォルトでは無効になっています。

e) [欠落 MED を最低優先度として処理（Treat missing MED as the least preferred one）] チェックボックスをオンにして、欠落している MED 属性は無限大の値を持つものとみなし、このパスを最も推奨度の低いパスにします。したがって、MED が欠落しているパスが最も優先度が低くなります。これは、デフォルトでは無効になっています。

f) [OK] をクリックします。

ステップ 8 （オプション）[ネイバー タイマー（Neighbor Timers）] セクションを編集します。

a) [キープアライブ インターバル（Keepalive interval）] フィールドでキープアライブ メッセージを送信しなかった場合に、その後 BGP ネイバーがアクティブな状態を維持する時間間隔を入力します。このキープアライブ インターバルが終わると、メッセージが送信されない場合、BGP ピアはデッドとして宣言されます。デフォルト値は 60 秒です。

b) [維持時間（Hold Time）] フィールドで、BGP 接続が開始、設定されている間、BGP ネイバーがアクティブな状態を維持する時間間隔を入力します。デフォルト値は 180 秒です。

c) （オプション）[最小維持時間（Min Hold time）] フィールドで、BGP 接続が開始、設定されている間、BGP ネイバーがアクティブな状態を維持する最小時間間隔を入力します。0 ～ 65535 の値を指定します。

d) [OK] をクリックします。

ステップ 9 （オプション）[グレースフル リスタート（Graceful Restart）] セクションを編集します。

（注） このセクションは、Firepower Threat Defenseデバイスがフェールオーバーまたはスパンド クラスタ モードになっているときにのみ使用できます。フェールオーバー設定のデバイスの 1 つが失敗した場合に、トラフィック フローのパケットでドロップがないように行われるものです。

a) [グレースフル リスタートを有効にする（Enable Graceful Restart）] チェックボックスをオンにして、FTD ピアがスイッチオーバー後のルート フラップを回避できるようにします。

b) [リスタート時間（Restart Time）] フィールドで BGP オープン メッセージが受信される前に、FTD ピアが古いルートを削除するまでの待機時間を入力します。デフォルト値は 120 秒です。有効な値は 1 ～ 3600 秒です。

c) [Stalepath 時間（Stalepath Time）] フィールドで、リスタートする FTDから End Of Record（EOR）メッセージを受信した後、FTDが古いルートを削除するまでの待機時間を入力します。デフォルト値は 360 秒です。有効な値は 1 ～ 3600 秒です。

d) [OK] をクリックします。

ステップ 10 [保存（Save）] をクリックします。

BGP 一般設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin Access Admin Network Admin

ルートマップ、アドミニストレーティブルートディスタンス、同期、ネクストホップ、パケット転送を設定します。これらの設定のデフォルトはほとんどの場合で適切ですが、ネットワークのニーズに合わせて調整できます。

ステップ 1 **[ルーティング（Routing）]** > **[BGP]** > **[IPv4]** または **[Ipv6]** に進み、**[一般（General）]** タブを選択します。

ステップ 2 [一般（General）] タブで、次のセクションを更新します。

a) [設定（Settings）] セクションで、[ルートマップ（Route Map）] オブジェクトを入力または選択して、ネクストホップ検証用の BGP ルータの [スキャン インターバル（Scanning Interval）] を入力します。有効な値は 5 ～ 60 秒です。デフォルト値は 60 です。[OK] をクリックします。

（注） [ルート マップ（Route Map）] フィールドは、IPv4 設定にのみ適用されます。

b) [ルートと同期化（Routes and Synchronization）] セクションで、必要に応じて以下を更新し、[OK] をクリックします。

- （オプション）[デフォルト ルートの生成（Generate Default Routes）]：これを選択して、デフォルト ルート（ネットワーク 0.0.0.0）を配布するように BGP ルーティング プロセスを設定します。
- （オプション）[サブネット ルートのネットワーク レベル ルートへの集約（Summarize subnet routes into network-level routes）]：これを選択して、ネットワーク レベルのルートへのサブネット ルートの自動集約を設定します。このチェックボックスを適用できるのは、IPv4 設定だけです。
- （オプション）[非アクティブなルートのアドバタイズ（Advertise inactive routes）]：これを選択して、ルーティング情報ベース（RIB）にインストールされていないルートをアドバタイズします。
- （オプション）[BGP と IGP システム間の同期化（Synchronise between BGP and IGP system）]：これを選択して、BGP と内部ゲートウェイ プロトコル（IGP）システムの間の同期を有効にします。通常、ルートがローカルであるか IGP に存在する場合を除き、BGP スピーカーは外部ネイバーにルートをアドバタイズしません。この機能により、自律システム内のルータおよびアクセス サー

バは、BGP が他の自律システムでルートを使用可能にする前にルートを確保できるようになります。

- （オプション）[IBGP の IGP への再配布（Redistribute IBGP into IGP）]：これを選択して、OSPF などの内部ゲートウェイ プロトコル（IGP）への iBGP の再配布を設定します。

c) [アドミニストレーティブ ルート ディスタンス（Administrative Route Distances）] セクションで、必要に応じて以下を更新し、[OK] をクリックします。

- [外部（External）]：外部 BGP ルートのアドミニストレーティブ ディスタンスを入力します。ルートは、外部自律システムから学習された場合は外部になります。この引数の値の範囲は 1 ～ 255 です。デフォルト値は 20 です。
- [内部（Internal）]：内部 BGP ルートのアドミニストレーティブ ディスタンスを入力します。ルートは、ローカル自律システムのピアから学習された場合は内部です。この引数の値の範囲は 1 ～ 255 です。デフォルト値は 200 です。
- [ローカル（Local）]：ローカル BGP ルートのアドミニストレーティブ ディスタンスを入力します。ローカル ルートは、別のプロセスから再配布されているルータまたはネットワークの、多くの場合バック ドアとして、ネットワーク ルータ表示コマンドによりリストされるネットワークです。この引数の値の範囲は 1 ～ 255 です。デフォルト値は 200 です。

d) [ネクスト ホップ（Next Hop）] セクションで、必要に応じて BGP ネクストホップ アドレスを有効にする [アドレス追跡を有効にする（Enable address tracking）] チェックボックスを選択し、ルーティング テーブルにインストールされた更新ネクストホップルートのチェックの間で [遅延インターバル（Delay Interval）] を入力します。[OK] をクリックします。

（注） [ネクスト ホップ（Next Hop）] セクションは、IPv4 設定にのみ適用されます。

e) [多重パスでパケットを転送（Forward Packets over Multiple Paths）] セクションで、必要に応じて以下を更新し、[OK] をクリックします。

- （オプション）[パスの数（Number of Paths）]：ルーティング テーブルにインストール可能な Border Gateway Protocol ルートの最大数を指定します。値の範囲は 1 ～ 8 です。デフォルト値は 1 です。
- （オプション）[IBGP パスの数（IBGP Number of Paths）]：ルーティング テーブルにインストール可能な並行内部ボーダー ゲートウェイ プロトコル（IBGP）ルートの最大数を指定します。値の範囲は 1 ～ 8 です。デフォルト値は 1 です。

ステップ 3 **[保存（Save）]** をクリックします。

BGP ネイバーの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin Access Admin Network Admin

BGPルータは更新を交換する前に、各ピアとの接続を確立する必要があります。これらのピアはBGP ネイバーと呼ばれます。[ネイバー（Neighbor）] タブを使用して、BGP IPv4 または IPv6 ネイバーとネイバーの設定を定義します。

ステップ 1 **[ルーティング（Routing）] > [BGP] > [IPv4]** または [IPv6] を選択し、[ネイバー（Neighbor）] タブをクリックします。

ステップ 2 [追加（Add）] をクリックして、BGP ネイバーとネイバーの設定を定義します。

ステップ 3 BGP ネイバーの **IP アドレス**を入力します。この IP アドレスは、BGP ネイバー テーブルに追加されます。

ステップ 4 BGP ネイバーの**インターフェイス**を入力します。

（注） [インターフェイス（Interface）] フィールドは、IPv6 の設定にのみ適用されます。

ステップ 5 [リモート AS（Remote AS）] フィールドに、BGP ネイバーが属する自律システムを入力します。

ステップ 6 [有効アドレス（Enabled address）] チェックボックスをオンにして、BGP ネイバーとの通信を有効にします。[有効アドレス（Enabled address）] チェックボックスがオンの場合にのみ、追加のネイバー設定が行われます。

ステップ 7 （オプション）[管理シャットダウン（Shutdown administratively）] チェックボックスをオンにして、ネイバーまたはピア グループを無効化します。

ステップ 8 （オプション）[グレースフル リスタートの設定（Configure graceful restart）] チェックボックスをオンにして、このネイバーのBGP グレースフル リスタート機能の設定を有効にします。このオプションを選択した後、[グレースフル リスタート（フェールオーバー/スパンドモード）（Graceful Restart (failover/spanned mode)）] オプションを使用して、このネイバーに対してグレースフル リスタートを有効にするか、または無効にするかを指定する必要があります。

（注） [グレースフル リスタート（graceful restart）] フィールドは、IPv4 の設定にのみ適用されます。

ステップ 9 （オプション）[BFDフォールオーバー（BFD Fallover）] チェックボックスを選択し、BGP の BFD サポートの設定を有効にします。この選択により、BFD から転送パス検出失敗メッセージを受信するように BGP ネイバーが登録されます。

ステップ 10 （オプション）BGP ネイバーの**説明**を入力します。

ステップ 11 （オプション）[ルートのフィルタリング（Filtering Routes）] タブで、必要に応じてアクセス リスト、ルート マップ、プレフィックス リスト、および AS パスのフィルタを使用して、BGP ネイバー情報を配布します。次の各セクションを更新します。

a) 適切な着信または発信**アクセス リスト**を入力または選択して、BGP ネイバー情報を配布します。

（注） アクセス リストは、IPv4 の設定にのみ適用されます。

b) 適切な着信または発信**ルート マップ**を入力または選択して、着信または発信ルートにルート マップを適用します。
c) 適切な着信または発信**プレフィックス リスト**を入力または選択して、BGP ネイバー情報を配布します。
d) 適切な着信または発信 **AS パス フィルタ**を入力または選択して、BGP ネイバー情報を配布します。
e) [ネイバーから許可されるプレフィックスの数を制限する（Limit the number of prefixes allowed from the neighbor）] チェックボックスをオンにして、ネイバーから受信できるプレフィックスの数を制御します。
   - [最大プレフィックス数（Maximum Prefixes）] フィールドに、特定のネイバーからの許可される最大プレフィックス数を入力します。
   - [しきい値レベル（Threshold Level）] フィールドに、ルータが警告メッセージの生成を開始するパーセンテージ（最大数に対する割合）を入力します。有効な値は 1 ～ 100 の整数です。デフォルト値は 75 です。

f) [ピアから受信したプレフィックスを制御する（Control prefixes received from the peer）] チェックボックスをオンにし、ピアから受信したプレフィックスに対する追加の制御を指定します。次のいずれかを実行します。
   - プレフィックス数の制限値に到達したときに BGP ネイバーを停止するには、[プレフィックス数の制限値を超えたときにピアリングを停止する（Terminate peering when prefix limit is exceeded）] ラジオ ボタンを選択します。[再起動間隔（Restart interval）] フィールドで、BGP ネイバーが再起動するまでの時間を指定します。
   - 最大プレフィックス数の制限値を超えたときにログ メッセージを生成するには、[プレフィックス数の制限値を超えたときに警告メッセージのみを表示する（Give only warning message when prefix limit is exceeded）] ラジオ ボタンを選択します。この場合、BGP ネイバーは終了しません。

g) [OK] をクリックします。

ステップ 12 （オプション）[ルート（Routes）] タブで、その他のネイバー ルート パラメータを指定します。次を更新します。

a) [アドバタイズメントの間隔（Advertisement Interval）] フィールドに、BGP ルーティング アップデートが送信される最小間隔（秒）を入力します。有効な値は、1 ～ 600 です。
b) [発信ルーティング更新からプライベート AS 番号を削除する（Remove private AS numbers from outbound routing updates）] を選択して、プライベート AS 番号を発信ルートにおけるアドバタイズ対象から除外します。
c) [デフォルト ルートの生成（Generate default routes）] チェックボックスをオンにして、ローカル ルータにネイバーへのデフォルト ルート 0.0.0.0 の送信を許可して、このルートがデフォルト ルートとして使用されるようにします。[ルート マップ（Route map）] フィールドで、ルート 0.0.0.0 が条件に応じて注入されるように許可するルート マップを入力または選択します。
d) 条件に応じてアドバタイズされるルートを追加するには、[行を追加（Add Row）]（+）ボタンをクリックします。[アドバタイズ対象ルートの追加（Add Advertised Route）] ダイアログボックスで、次の手順を実行します。

1. [アドバタイズ マップ（Advertise Map）] フィールドで、exist-map または非存在マップの条件が満たされた場合にアドバタイズされるルート マップを追加または選択します。
2. [exist-map（Exist Map）] ラジオ ボタンを選択し、[ルート マップ オブジェクト セレクタ（Route Map Object Selector）] からルート マップを選択します。このルート マップは、advertise-map のルートがアドバタイズされるかどうかを判断するために BGP テーブル内のルートと比較されます。
3. [非存在マップ（Non-Exist Map）] ラジオ ボタンを選択し、[ルート マップ オブジェクト セレクタ（Route Map Object Selector）] からルート マップを選択します。このルート マップは、advertise-map のルートがアドバタイズされるかどうかを判断するために BGP テーブル内のルートと比較されます。
4. [OK] をクリックします。

ステップ 13 [タイマー（Timers）] タブで [BGP ピアの時間を設定する（Set Timers for the BGP Peer）] チェックボックスをオンにし、キープアライブ頻度、保留時間、最小保留時間を設定します。

- [キープアライブ インターバル（Keepalive Interval）]：FTD デバイスがキープアライブ メッセージをネイバーに送信する頻度（秒）を入力します。有効な値は、0 ～ 65535 です。デフォルト値は 60 秒です。
- [保留時間（Hold time）]：キープアライブ メッセージを受信できない状態が継続して、ピアがデッドであると FTD デバイスが宣言するまでの時間（秒）を入力します。有効な値は、0 ～ 65535 です。デフォルト値は 180 秒です。
- [最小保留時間（Min hold time）]：（オプション）キープアライブ メッセージを受信できない状態が継続して、ピアがデッドであると FTD デバイスが宣言するまでの最小時間（秒）を入力します。有効な値は、0 ～ 65535 です。デフォルト値は 0 秒です。

ステップ 14 [詳細（Advanced）] タブで、次を更新します。

a) （オプション）[認証を有効にする（Enable Authentication）] を選択して、2 つの BGP ピア間の TCP 接続で MD5 認証を有効にします。

1. [暗号化を有効にする（Enable Encryption）] ドロップダウン リストから暗号化タイプを選択します。
2. パスワードを [パスワード（Password）] フィールドに入力します。[確認（Confirm）] フィールドにパスワードを再入力します。パスワードは大文字と小文字を区別し、service password-encryption コマンドが有効な場合は最大 25 文字、service password-encryption コマンドが有効でない場合は最大 81 文字を指定できます。最初の文字を数値にはできません。この文字列には、スペースも含め、あらゆる英数字を使用できます。

   （注） 数字-スペース-任意の文字の形式でパスワードを指定することはできません。数字の後にスペースを使用すると、認証に失敗する原因となることがあります。

b) （オプション）[このネイバーにコミュニティ属性を送信する（Send Communty attribute to this neighbor）] チェックボックスをオンにして、コミュニティ属性を BGP ネイバーに送信することを指定します。

c) （オプション）[このネイバーのネクスト ホップとして FTD を使用する（Use FTD as next hop for this neighbor）] チェックボックスをオンにし、ルータを BGP スピーキング ネイバーまたはピア グループのネクスト ホップとして設定します。

d) [接続の検証を無効にする（Disable Connection Verification）] チェックボックスをオンにして、シングルホップで到達可能な eBGP ピアリング セッションについての接続の検証プロセスを無効にします。これにより、ループバック インターフェイスで設定されたピアや直接接続されない IP アドレスが設定されたピアとの間でセッションを確立することができます。オフ（デフォルト）にすると、シングルホップ eBGP ピアリング セッション（TTL=254）について、BGP ルーティング プロセスで接続が検証され、eBGP ピアが同じネットワーク セグメントに直接接続されているかどうか確認されます。ピアが同じネットワーク セグメントに直接接続されていない場合、ピアリング セッションは確立されません。

e) [直接接続されていないネイバーとの接続を許可する（Allow connections with neighbor that is not directly connected）] ラジオボタンを選択して、直接接続されていないネットワーク上で外部ピアからの BGP 接続を受け入れ、またそのピアへの BGP 接続を試みます。（オプション）[TTL hops] フィールドに存続可能時間を入力します。有効な値は、1 ～ 255 です。または、[ネイバーへの TTL ホップの制限数（Limited number of TTL hops to neighbor）] ラジオ ボタンを選択して、BGP ピアリング セッションを保護します。[TTL hops] フィールドに、eBGP ピアを区切るホップの最大数を入力します。有効な値は、1 ～ 254 です。

f) （オプション）[TCP MTU パス検出の使用（Use TCP MTU path discovery）] チェックボックスをオンにして、BGP セッションの TCP トランスポート セッションを有効にします。

g) [TCP トランスポート モード（TCP Transport Mode）] ドロップダウン リストから TCP 接続モードを選択します。オプションは [デフォルト（Default）]、[アクティブ（Active）]、または [パッシブ（Passive）] です。

h) （オプション）BGP ネイバー接続の**ウェイト**を入力します。

i) ドロップダウン リストから FTD デバイスが受け入れる **BGP バージョン**を選択します。[4 のみ（4-Only）] に設定すると、指定されたネイバーとの間でバージョン 4 だけが使用されます。デフォルトでは、バージョン 4 が使用され、要求された場合は動的にネゴシエートしてバージョン 2 に下がります。

ステップ 15 AS 移行を考慮する場合にのみ [移行（Migration）] タブを更新します。

（注） AS 移行カスタマイズは、遷移の完了後に削除される必要があります。

a) （オプション）[ネイバーから受信したルートの AS 番号をカスタマイズする（Customize the AS number for routes received from the neighbor）] チェックボックスをオンにして、eBGP ネイバーから受信したルートの AS_path 属性をカスタマイズします。

b) [ローカル AS 番号（Local AS number）] フィールドにローカル自律システム番号を入力します。有効な値は、1 ～ 4294967295 または 1.0 ～ 65535.65535 の有効な自律システム番号です。

c) （オプション）[ローカル AS 番号をネイバーから受信したルートの前に付加しない（Do not prepend local AS number to routes received from neighbor）] チェックボックスをオンにして、ローカル AS 番号が eBGP ピアから受信したルートの前に付加されないようにします。

d) （オプション）[実 AS 番号をネイバーから受信したルートのローカル AS 番号に置き換える（Replace real AS number with local AS number in routes received from neighbor）] チェックボックスをオンにして、実自律システム番号を eBGP 更新のローカル自律システム番号に置き換えます。ローカル BGP ルーティング プロセスからの自律システム番号は、追加されません。

e) （オプション）[実 AS 番号またはネイバーから受信したルートのローカル AS 番号を受け入れる（Accept either real AS number or local AS number in routesreceived from neighbor）] チェックボックスをオンにして、実自律システム番号（ローカル BGP ルーティング プロセスより）またはローカル自律システム番号を使用するピアリング セッションを確立するように eBGP ネイバーを設定します。

ステップ 16 [OK] をクリックします。

ステップ 17 [保存（Save）] をクリックします。

BGP 集約アドレス設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin Access Admin Network Admin

BGP ネイバーはルーティング情報を格納し、交換しますが、設定される BGP スピーカーの数が増えるに従って、ルーティング情報の量が増えます。ルート集約は、複数の異なるルートの属性を合成し、1 つのルートだけがアドバタイズされるようにするプロセスです。集約プレフィックスは、クラスレス ドメイン間ルーティング（CIDR）の原則を使用して、複数の隣接するネットワークを、ルーティング テーブルに要約できる IP アドレスのクラスレス セット 1 つに合成します。結果として、アドバタイズの必要なルートは少なくなります。[集約アドレスの追加/編集（Add/Edit Aggregate Address）] ダイアログボックスで、特定のルートの 1 つのルートへの集約を定義します。

ステップ 1 Firepower Threat Defense デバイスを編集する際、**[ルーティング（Routing）] > [BGP] > [IPv4]** または **[IPv6]** を選択して、**[集約アドレス（Aggregate Address）]** タブを選択します。

ステップ 2 [集約アドレス（Aggregate Addresses）] タブをクリックします。

ステップ 3 [集約タイマー（Aggregate Timer）] フィールドで、集約タイマーの値（秒）を入力します。有効な値は、0 または 6 ～ 60 の値です。デフォルト値は 30 です。

ステップ 4 [追加（Add）] をクリックして、[集約アドレスの追加（Add Aggregate Address）] ダイアログを更新します。

a) [ネットワーク（Network）]：IPv4 アドレスを入力するか、任意のネットワーク/ホスト オブジェクトを選択します。

b) [集約マップ（Attribute Map）]：（オプション）集約ルートの属性の設定に使用されるルート マップを入力または選択します。

c) [アドバタイズ マップ（Advertise Map）]：（オプション）AS 設定の元のコミュニティを作成するルートの選択に使用されるルート マップを入力または選択します。

d) [抑制マップ（Suppress Map）]：（オプション）抑制するルートの選択に使用されるルート マップを入力または選択します。

e) [AS 設定パス情報の生成（Generate AS set path Information）]：（オプション）自律システム設定パス情報の生成を有効にするには、チェックボックスを選択します。
f) [更新から全ルートをフィルタ処理（Filter all routes from updates）]：（オプション）更新からのすべての特定のルートをフィルタ処理するには、チェックボックスを選択します。
g) [OK] をクリックします。

次のタスク

- BGPv4 設定については、次に進みます。 BGPv4 フィルタリング設定 （1017 ページ）
- BGPv6 設定については、次に進みます。 BGP ネットワーク設定 （1018 ページ）

BGPv4 フィルタリング設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin Access Admin Network Admin

フィルタリング設定は、受信される BGP 更新プログラムのフィルタ処理ルートまたはネットワークに使用されます。フィルタリングは、ルータが学習またはアドバタイズするルーティング情報を制限するために使用されます。

始める前に

フィルタリングは、BGP の IPv4 ルーティング ポリシーでのみ適用されます。

ステップ 1 **[ルーティング（Routing）]** > **[BGP]** > **[IPv4]** を選択し、**[フィルタリング（Filtering）]** タブを選択します。
ステップ 2 [追加（Add）] をクリックして、[フィルタの追加（Add Filter）] ダイアログを更新します。
a) [アクセス リスト（Access List）]：受信されるネットワークとルーティング アップデートで抑制されるネットワークを定義するアクセスコントロールリストを選択します。
b) [指示（Direction）]：（オプション）インバウンド更新、アウトバウンド更新のどちらにフィルタを適用するかを指定する指示を選択します。
c) [プロトコル（Protocol）]：（オプション）なし、BGP、接続中、OSPF、RIP または静的のルーティング プロセスのうち、フィルタ処理するものを選択します。
d) [プロセス ID（Process ID）]：（オプション）OSPF ルーティング プロトコルのプロセス ID を入力します。
e) [OK] をクリックします。
ステップ 3 [保存（Save）] をクリックします。

BGP ネットワーク設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin Access Admin Network Admin

ネットワーク設定は、BGPルーティングプロセスによってアドバタイズされるネットワーク、アドバタイズされるネットワークのフィルタ処理で確認されるルートマップを追加するために使用されます。

ステップ 1 **[ルーティング（Routing）]** > **[BGP]** > **[IPv4]** または **[IPv6]** に進み、[ネットワーク（Networks）] タブを選択します。

ステップ 2 [追加（Add）] をクリックして、[ネットワークの追加（Add Networks）] ダイアログを更新します。

a) [ネットワーク（Network）]：BGPルーティングプロセスによってアドバタイズされるネットワークを入力します。

b) （オプション）[ルート マップ（Route Map）]：アドバタイズされるネットワークをフィルタ処理するために調べる必要のあるルート マップを入力または選択します。この値を指定しない場合、すべてのネットワークが再配布されます。

c) [OK] をクリックします。

ステップ 3 [保存（Save）] をクリックします。

BGP 再配布設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin Access Admin Network Admin

再配布設定により、別のルーティング ドメインから BGP にルートを再配布する条件を定義できます。

ステップ 1 **[ルーティング（Routing）]** > **[BGP** > **IPv4]** または **[IPv6]** に進み、[再配布（Redistribution）] タブを選択します。

ステップ 2 [追加（Add）] をクリックして、[再配布の追加（Add Redistribution）] ダイアログを更新します。

a) [送信元プロトコル（Source Protocol）]：送信元プロトコル ドロップダウンリストから、どのプロトコルからルートを BGP ドメインに再配布するかを選択します。

b) [プロセス ID（Process ID）]：選択されている送信元プロトコルの識別子を入力します。OSPF プロトコルに適用されます。
c) [メトリック（Metric）]：（オプション）再配布されているルートのメトリックを入力します。
d) [ルート マップ（Route Map）]：再配布されるネットワークをフィルタ処理するために調べる必要のあるルート マップを入力または選択します。この値を指定しない場合、すべてのネットワークが再配布されます。
e) [一致（Match）]：1 つのルーティング プロトコルから別のルーティング プロトコルへのルート再配布に使用される条件。ルートが再配布されるには、選択した条件と一致している必要があります。次の一致条件から 1 つ以上を選択できます。これらのオプションは、OSPF が送信元プロトコルとして選択されているときにのみ有効になります。
   - 内線
   - 外部 1
   - 外部 2
   - NSSA 外部 1
   - NSSA 外部 2

f) [OK] をクリックします。

BGP ルート注入の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin Access Admin Network Admin

ルート注入設定により、条件に応じて BGP ルーティング テーブルに注入されるルートを定義できます。

ステップ 1 **[ルーティング（Routing）]** > **[BGP]** > **[IPv4]** または **[IPv6]** を選択し、[ルート注入（Route Injection）] タブを選択します。

ステップ 2 [追加（Add）] をクリックして、[ルート注入の追加（Add Route Injection）] ダイアログを更新します。

a) [マップ注入（Inject Map）]：ローカル BGP ルーティング テーブルに注入するプレフィックスを指定するルート マップを入力または選択します。
b) [マップ存在（Exist Map）]：BGP スピーカーが追跡するプレフィックスを含むルート マップを入力または選択します。
c) [注入されたルートが集約ルートの属性を継承（Injected routes will inherit the attributes of the aggregate route）]：これを選択し、集約ルートの属性を継承するよう注入されたルートを設定します。

d) [OK] をクリックします。

ステップ 3 [保存（Save）] をクリックします。

第 40 章

Firepower Threat Defense の RIP

この章では、ルーティング情報プロトコル（RIP）を使用してデータをルーティングし、認証を実行し、ルーティング情報を再配布するように FTD を設定する方法について説明します。

RIP について

RIP と呼ばれることが多い Routing Information Protocol は、すべてのルーティング プロトコルの中で最も堅牢なものの 1 つです。RIP には、ルーティング アップデート プロセス、RIP ルーティング メトリック、ルーティング安定性、ルーティング タイマーの 4 つの基本的なコンポーネントがあります。RIP をサポートしているデバイスは、ルーティング アップデート メッセージを定期的に、またネットワーク トポロジが変更されたときに送信します。これらの RIP パケットには、デバイスが到達可能なネットワークに関する情報、さらに宛先アドレスに到達するためにパケットが通過しなければならないルータやゲートウェイの数が含まれています。RIP では、生成されるトラフィックは OSPF より多くなりますが、設定は OSPF より容易です。

RIP は、ホップ カウントをパス選択のメトリックとして使用するディスタンス ベクター ルーティング プロトコルです。インターフェイス上で RIP が有効になっている場合、インターフェイスは、ネイバー デバイスと RIP ブロードキャストを交換して、ルートの動的な学習およびアドバタイズを行います。

Firepower Threat Defense デバイス は、RIP バージョン 1 と RIP バージョン 2 の両方をサポートしています。RIP バージョン 1 では、ルーティング アップデートでサブネットマスクは送信されません。RIP バージョン 2 では、ルーティング アップデートでサブネットマスクが送信され、可変長サブネット マスクがサポートされています。さらに、RIP バージョン 2 では、ルーティング アップデートを交換するときのネイバー認証がサポートされています。この認証により、信頼性の高い送信元から信頼できるルーティング情報が Firepower Threat Defense デバイスで受信できるようになります。

RIP は、初期設定が簡単で、トポロジが変更されても設定を更新する必要がないため、スタティック ルーティングより有利です。RIP の欠点は、スタティック ルーティングよりネットワークや処理オーバーヘッドが大きいことです。

ルーティング アップデート プロセス

RIPは、ルーティングアップデートメッセージを定期的に送信するだけでなく、ネットワークトポロジが変更された場合にも送信します。ルータは、エントリの変更が含まれるルーティング アップデートを受け取ると、新しいルートを反映するようにそのルーティング テーブルを更新します。パスのメトリック値は1ずつ大きくなり、送信者はネクストホップとして示されます。RIP ルータは、宛先に対する最適なルート（メトリック値が最も小さいルート）だけを保持します。ルータは、そのルーティング テーブルを更新した後、他のネットワーク ルータに変更を通知するために、ルーティングアップデートの送信をただちに開始します。これらのアップデートは、RIP ルータが送信する定期的にスケジュールされたアップデートとは独立して送信されます。

RIP のルーティング メトリック

RIP は、1 つのルーティング メトリック（ホップ カウント）を使用して発信元と宛先ネットワークとの距離を測定します。発信元から宛先までのパスの各ホップにはホップ カウント値（通常は1）が割り当てられます。ルータが、新しいまたは変更された宛先ネットワーク エントリが含まれるルーティングアップデートを受け取ると、アップデートで示されたメトリック値に 1 を加算し、そのネットワークをルーティング テーブルに入れます。送信者の IP アドレスがネクスト ホップとして使用されます。

RIP 安定性機能

RIP は、送信元から宛先へのパスで許可されるホップ数に制限を導入することにより、ルーティング ループが無限に続くことを防止しています。パス内のホップの最大数は 15 です。新しいまたは変更されたエントリが含まれるルーティングアップデートをルータが受信し、メトリック値に1を加えた結果、メトリックが無限（つまり16）になる場合は、ネットワークの宛先は到達不能と見なされます。この安定性機能の欠点は、この機能によってRIPネットワークの直径の最大値が 16 ホップ未満に制限されることです。

RIPには、その他にも、多くのルーティングプロトコルに共通の安定性機能がいくつか含まれます。ネットワークトポロジは急激に変化する可能性がありますが、これらの機能は、安定性を提供するように設計されています。たとえば、RIPでは、スプリットホライズンとホールドダウン メカニズムを実装して、間違ったルーティング情報が伝搬されることを防止しています。

RIP タイマー

RIP では、多数のタイマーを使用してそのパフォーマンスを調整しています。これらのタイマーには、ルーティングアップデートタイマー、ルートタイムアウトタイマー、ルートフラッシュ タイマーがあります。ルーティングアップデートタイマーは、定期的なルーティングアップデートの間隔を測ります。通常は 30 秒に設定されており、タイマーがリセットされたときにはランダムな時間がわずかに追加されます。これは、すべてのルータがそのネイバーを同時にアップデートしようとした結果発生する輻輳を防ぐためです。ルーティングテーブルの各エ

ントリには、ルートタイムアウト タイマーが関連付けられています。ルートタイムアウト タイマーが期限切れになると、ルートには無効のマークが付きますが、ルートフラッシュ タイマーが期限切れになるまではテーブル内に保持されます。

RIP のガイドライン

IPv6 のガイドライン

IPv6 はサポートされません。

その他のガイドライン

次の情報は、RIP バージョン 2 だけに適用されます。

- ネイバー認証を使用する場合、認証キーとキー ID は、RIP バージョン 2 アップデートをそのインターフェイスに提供するすべてのネイバーデバイス上で同じにする必要があります。
- RIP バージョン 2 の場合、Firepower Threat Defense デバイス は、マルチキャスト アドレス 224.0.0.9 を使用してデフォルト ルート アップデートを送受信します。パッシブ モードでは、そのアドレスでルート アップデートが受信されます。
- RIP バージョン 2 がインターフェイス上で設定されると、マルチキャスト アドレス 224.0.0.9 がそのインターフェイス上で登録されます。RIP バージョン 2 設定がインターフェイスから削除されると、そのマルチキャスト アドレスの登録は解除されます。

制限事項

- RIP アップデートは、Firepower Threat Defense デバイス のインターフェイス間を通過できません。
- RIP バージョン 1 では、可変長サブネット マスクがサポートされていません。
- RIP の最大ホップ カウントは 15 です。ホップ カウントが 15 を超えるルートは、到達不能と見なされます。
- RIP の収束は、他のルーティング プロトコルと比べて時間がかかります。
- Firepower Threat Defense デバイス では、RIP プロセスを 1 つだけイネーブルにできます。

RIP の設定

RIP は、ホップ カウントをメトリックとして使用するディスタンスベクトル ルーティング プロトコルです。

ステップ 1 **[デバイス（Devices）] > [デバイス管理（Device Management）]** の順に選択し、FTD デバイスを編集します。

ステップ 2 [ルーティング（Routing）] タブを選択します。

ステップ 3 コンテンツ テーブルから [RIP] を選択します。

ステップ 4 [RIP を有効にする（Enable RIP）] チェックボックスをオンにして、RIP を設定します。

ステップ 5 [RIP バージョン（RIP Version）] ドロップダウン リストから、RIP の更新を送受信するための RIP バージョンを選択します。

ステップ 6 （オプション）[デフォルト ルートの生成（Generate Default Route）] チェックボックスをオンにして、指定したルート マップに基づく配布用のデフォルト ルートを生成します。

a) [ルート マップ（Route map）] フィールドで、デフォルト ルートの生成に使用するルート マップ名を指定します。
[ルート マップ（Route map）] フィールドで指定したルート マップが存在する場合、特定のインターフェイスで配布されるデフォルト ルート 0.0.0.0/0 が生成されます。

ステップ 7 [RIP バージョン（RIP Version）] として [バージョン 2 の送受信（Send and Receive Version 2）] を選択した場合、[自動集約の有効化（Enable Auto Summary）] オプションが使用可能になります。[自動集約の有効化（Enable Auto Summary）] チェックボックスをオンにすると、自動ルート集約が有効になります。切断されているサブネット間のルーティングを実行する必要がある場合は、自動サマライズをディセーブルにします。自動サマライズをディセーブルにすると、サブネットがアドバタイズされます。

（注） RIP バージョン 1 では、常に自動サマライズが使用されます。無効にすることはできません。

ステップ 8 [ネットワーク（Networks）] タブをクリックします。RIP ルーティングに対して 1 つ以上のネットワークを定義します。IP アドレスを入力するか、目的のネットワーク/ホスト オブジェクトを入力または選択します。セキュリティ アプライアンスの設定に追加できるネットワーク数に制限はありません。このコマンドで定義されるネットワークに属しているインターフェイスは、RIP ルーティング プロセスに参加します。RIP ルーティング更新は、指定したネットワークのインターフェイスだけを介して送受信されます。また、インターフェイスのネットワークを指定しない場合、インターフェイスは RIP 更新でアドバタイズされません。

（注） RIP では、IPv4 オブジェクトのみがサポートされます。

ステップ 9 （オプション）[パッシブ インターフェイス（Passive Interfaces）] タブをクリックします。このオプションを使用して、アプライアンスでパッシブ インターフェイスを指定してから、アクティブ インターフェイスを指定します。デバイスは、そのルーティング テーブルを入力するための情報を使用して、パッシブ インターフェイスでの RIP ルートのブロードキャストをリッスンしますが、パッシブ インターフェイスでのルーティング更新はブロードキャストしません。パッシブとして指定されていないインターフェイスは、更新を送受信します。

ステップ 10 [再配布（Redistribution）] タブをクリックして、再配布ルートを管理します。これらは、他のルーティング プロセスから RIP ルーティング プロセスに再配布されているルートです。

a) [追加（Add）] をクリックして、再配布ルートを指定します。

b) [プロトコル（Protocol）] ドロップダウン リストから、RIP ルーティング プロセスに再配布するルーティング プロトコルを選択します。

（注） OSPF プロトコルの場合は、プロセス ID を指定します。同様に、BGP の場合は AS パスとして指定します。[プロトコル（Protocol）] ドロップダウン リストで [接続済み（Connected）] オプションを選択すると、直接接続されたネットワークを RIP ルーティング プロセスに再配布できます。

c) （オプション）OSPF ルートを RIP ルーティング プロセスに再配布する場合、[一致（Match）] ドロップダウン リストで、再配布する特定のタイプの OSPF ルートを選択できます。複数のタイプを選択するには、Ctrl を押しながらクリックします。

- [内部（Internal）]：自律システム（AS）の内部のルートが再配布されます。
- [外部 1（External 1）]：AS に対して外部のタイプ 1 ルートが再配布されます。
- [外部 2（External 2）]：AS に対して外部のタイプ 2 ルートが再配布されます。
- [NSSA 外部 1（NSSA External 1）]：Not-So-Stubby Area（NSSA）の外部のタイプ 1 ルートが再配布されます。
- [NSSA 外部 2（NSSA External 2）]：NSSA に対して外部のタイプ 2 ルートが再配布されます。

（注） デフォルトの一致は、[内部（Internal）]、[外部 1（External 1）]、および [外部 2（External 2）] です。

d) [メトリック（Metric）] ドロップダウン リストから、再配布されたルートに適用する RIP メトリック タイプを選択します。選択肢は次の 2 つです。

- [トランスペアレント（Transparent）]：現在のルート メトリックを使用します。
- [指定値（Specified Value）]：特定のメトリック値を割り当てます。[メトリック値（Metric Value）] フィールドに 0 ～ 16 の特定の値を入力します。
- [なし（None）]：メトリックが指定されません。再配布されたルートに適用するメトリック値を使用しないでください。

e) （オプション）[ルート マップ（Route Map）] フィールドに、ルートが RIP ルーティング プロセスに再配布される前に満たす必要のあるルート マップの名前を指定します。ルートは、IP アドレスがルート マップ アドレス リストの許可文と一致する場合にのみ再配布されます。

f) [OK] をクリックします。

ステップ 11 （オプション）[フィルタリング（Filtering）] タブをクリックして、RIP ポリシーのフィルタを管理します。このセクションでは、インターフェイスでのルーティング更新の回避、ルーティング更新でのルートのアドバタイズ制御、ルーティング更新の処理制御、およびルーティング更新の送信元フィルタリングに、フィルタを使用します。

a) [追加（Add）] をクリックして、RIP フィルタを追加します。

b) [トラフィックの方向（Traffic Direction）] フィールドでフィルタリングされるトラフィックのタイプ（[着信（Inbound）] または [発信（Outbound）]）を選択します。

（注） トラフィックの方向が着信の場合、インターフェイス フィルタだけを定義できます。

c) [フィルタ オン（Filter On）] フィールドで適切なラジオ ボタンを選択して、フィルタがインターフェイスまたはルートのいずれに基づくかを指定します。[インターフェイス（Interface）] を選択した場合、ルーティング更新がフィルタリングされるインターフェイスの名前を入力または選択します。[ルート（Route）] を選択した場合、ルート タイプを選択します。

- [スタティック（Static）]：スタティック ルートだけがフィルタリングされます。
- [接続済み（Connected）]：接続されたルートだけがフィルタリングされます。
- [OSPF]：指定した OSPF プロセスによって検出された OSPFv2 ルートだけがフィルタリングされます。フィルタリングされる OSPF プロセスの [プロセス ID（Process ID）] を入力します。
- [BGP]：指定した BGP プロセスによって検出された BGPv4 ルートだけがフィルタリングされます。フィルタリングされる BGP プロセスの AS パスを入力します。

d) [アクセス リスト（Access List）] フィールドで、許可されるネットワークまたは RIP ルート アドバタイズメントから削除されるネットワークを定義する 1 つ以上のアクセス コントロール リスト（ACL）の名前を入力または選択します。

e) [OK] をクリックします。

ステップ 12 （オプション）[ブロードキャスト（Broadcast）] タブをクリックして、インターフェイス設定を追加または編集します。[ブロードキャスト（Broadcast）] タブを使用して、インターフェイスごとに送受信するグローバル RIP バージョンをオーバーライドできます。また、有効な RIP アップデートを確認するための認証を実装する場合は、インターフェイスごとの認証パラメータを定義できます。

a) [追加（Add）] をクリックして、インターフェイス設定を追加します。

b) [インターフェイス（Interface）] フィールドで、このアプライアンスで定義されるインターフェイスを入力または選択します。

c) [送信（Send）] オプションで、該当するボックスを選択して、RIP バージョン 1、バージョン 2、または両方を使用して更新を送信するように指定します。これらのオプションを使用して、指定されたインターフェイスについて、指定したグローバルな送信バージョンをオーバーライドできます。

d) [受信（Receive）] オプションで、該当するボックスを選択して、RIP バージョン 1、バージョン 2、または両方を使用して更新を受け入れるように指定します。これらのオプションを使用して、指定されたインターフェイスについて、指定したグローバルな受信バージョンをオーバーライドできます。

e) RIP ブロードキャストに対してこのインターフェイスで使用される**認証**を選択します。

- [なし（None）]：認証はありません。
- [MD5]：MD5 を使用します。
- [クリア テキスト（Clear Text）]：クリア テキスト認証を使用します。

[MD5] または [クリア テキスト（Clear Text）] を選択した場合、次の認証パラメータも指定する必要があります。

- [キー ID（Key ID）]：認証キーの ID。有効な値は 0 ～ 255 です。
- [キー（Key）]：選択した認証方式で使用されるキー。最大 16 文字まで使用できます
- [確認（Confirm）]：確認のために、認証キーを再度入力します。

f) [OK] をクリックします。

第 41 章

Firepower Threat Defense のマルチキャスト ルーティング

この章では、マルチキャスト ルーティング プロトコルを使用するように Firepower Threat Defense デバイス を設定する方法について説明します。

マルチキャスト ルーティングの概要

マルチキャスト ルーティングは、単一の情報ストリームを数千もの企業や家庭に同時に配信することでトラフィックを軽減する帯域幅節約型のテクノロジーです。マルチキャスト ルーティングを活用するアプリケーションには、ビデオ会議、企業通信、遠隔学習に加えて、ソフトウェア、株価、およびニュースの配信などがあります。

マルチキャスト ルーティング プロトコルでは、競合テクノロジーのネットワーク帯域幅の使用量を最小限に抑えながら、発信元や受信者の負荷を増加させずに発信元のトラフィックを複数の受信者に配信します。マルチキャスト パケットは、Protocol Independent Multicast（PIM）やサポートする他のマルチキャスト プロトコルを使用したFirepower Threat Defense デバイスによりネットワークで複製されるため、複数の受信者にできる限り高い効率でデータを配信できます。

Firepower Threat Defense デバイスは、スタブ マルチキャスト ルーティングと PIM マルチキャスト ルーティングの両方をサポートしています。ただし、1 つのFirepower Threat Defense デバイスに両方を同時に設定できません。

（注） UDP と非 UDP の両方のトランスポートがマルチキャスト ルーティングに対してサポートされます。ただし、非 UDP トランスポートでは FastPath 最適化は行われません。

IGMP プロトコル

IP ホストは、Internet Group Management Protocol（IGMP）を使用して、そのグループ メンバーシップを、直接接続されているマルチキャスト ルータに報告します。IGMP は、マルチキャスト グループの個々のホストを特定の LAN にダイナミックに登録するために使用します。ホストは、そのローカル マルチキャスト ルータに IGMP メッセージを送信することで、グループ メンバーシップを識別します。IGMP では、ルータは IGMP メッセージを受信し、定期的にクエリーを送信して、特定のサブネットでアクティブなグループと非アクティブなグループを検出します。

IGMP は、グループ アドレス（Class D IP アドレス）をグループ識別子として使用します。ホスト グループ アドレスとして使用できるのは、224.0.0.0 ～ 239.255.255.255 の範囲内のアドレスです。アドレス 224.0.0.0 がグループに割り当てられることはありません。アドレス 224.0.0.1 は、サブネットのシステムすべてに割り当てられます。アドレス 224.0.0.2 は、サブネットのルータすべてに割り当てられます。

（注） Firepower Threat Defense デバイスでマルチキャスト ルーティングを有効にすると、IGMP バージョン 2 がすべてのインターフェイスで自動的に有効になります。

マルチキャスト グループへのクエリ メッセージ

Firepower Threat Defense デバイスは、クエリ メッセージを送信して、インターフェイスに接続されているネットワークにメンバーを持つマルチキャスト グループを検出します。メンバは、IGMP 報告メッセージで応答して、特定のグループに対するマルチキャスト パケットの受信を希望していることを示します。クエリー メッセージは、アドレスが 224.0.0.1 で存続可能時間値が 1 の全システム マルチキャスト グループ宛に送信されます。

これらのメッセージが定期的に送信されることにより、Firepower Threat Defense デバイスに保存されているメンバーシップ情報が更新されます。Firepower Threat Defense デバイスで、ローカル メンバーがいなくなったマルチキャスト グループがまだインターフェイスに接続されていることがわかると、そのグループへのマルチキャスト パケットを接続されているネットワークに転送するのを停止し、そのパケットの送信元にプルーニング メッセージを戻します。

デフォルトでは、サブネット上の PIM 指定ルータがクエリー メッセージの送信を担当します。このメッセージは、デフォルトでは 125 秒間に 1 回送信されます。

クエリー応答時間を変更する場合は、IGMP クエリーでアドバタイズする最大クエリー応答時間はデフォルトで 10 秒になります。Firepower Threat Defense デバイスがこの時間内にホスト クエリの応答を受信しなかった場合、グループを削除します。

スタブ マルチキャスト ルーティング

スタブ マルチキャスト ルーティングは、ダイナミック ホスト登録の機能を提供して、マルチキャスト ルーティングを容易にします。スタブ マルチキャスト ルーティングを設定すると、Firepower Threat Defense デバイスは IGMP のプロキシ エージェントとして動作します。Firepower Threat Defense デバイスは、マルチキャスト ルーティングに全面的に参加するのではなく、IGMP メッセージをアップストリームのマルチキャスト ルータに転送し、そのルータがマルチキャスト データの送信をセットアップします。スタブ マルチキャスト ルーティングを設定する場合は、Firepower Threat Defense デバイス を PIM スパース モードまたは双方向モードに設定できません。IGMP スタブ マルチキャスト ルーティングに参加しているインターフェイス上で PIM を有効にする必要があります。

Firepower Threat Defense デバイス は、PIM-SM および双方向 PIM の両方をサポートしています。PIM-SMは、基盤となるユニキャスト ルーティング情報ベースまたは別のマルチキャスト対応ルーティング情報ベースを使用するマルチキャスト ルーティング プロトコルです。このプロトコルは、マルチキャスト グループあたり 1 つのランデブー ポイント（RP）をルートにした単方向の共有ツリーを構築し、オプションでマルチキャストの発信元ごとに最短パス ツリーを作成します。

PIM マルチキャスト ルーティング

双方向 PIM は PIM-SM の変形で、マルチキャストの発信元と受信者を接続する双方向の共有ツリーを構築します。双方向ツリーは、マルチキャスト トポロジの各リンクで動作する指定フォワーダ（DF）選択プロセスを使用して構築されます。DF に支援されたマルチキャスト データは発信元からランデブー ポイント（RP）に転送されます。この結果、マルチキャスト データは発信元固有の状態を必要とせず、共有ツリーをたどって受信者に送信されます。DF の選択は RP の検出中に行われ、これによってデフォルト ルートが RP に提供されます。

（注） Firepower Threat Defense デバイスが PIM RP の場合は、Firepower Threat Defense デバイスの変換されていない外部アドレスを RP アドレスとして使用してください。

PIM Source Specific Multicast のサポート

Firepower Threat Defense デバイス は PIM Source Specific Multicast（SSM）の機能や関連設定をサポートしていません。ただし、Firepower Threat Defense デバイス は SSM 関連のパケットが最終ホップ ルータとして配置されていない限り、通過を許可します。

SSMは、IPTVなどの1対多のアプリケーションのデータ送信メカニズムとして分類されます。SSM モデルは、（S、G）ペアで示される「チャネル」の概念を使用します。S は発信元アドレス、GはSSM宛先アドレスです。チャネルに登録するには、IGMPv3 などのグループ管理プロトコルを使用して行います。SSMは、特定のマルチキャスト送信元について学習した後、受信側のクライアントを有効にします。これにより、共有ランデブー ポイント（RP）からではなく、直接送信元からマルチキャスト ストリームを受信できるようになります。アクセス制御

メカニズムは SSM 内に導入され、現在のスパースまたはスパース - デンス モード導入では使用できないセキュリティ強化を提供します。

PIM-SSM は、RP または共有ツリーを使用しない点で PIM-SM とは異なります。代わりに、マルチキャスト グループの発信元アドレスの情報は、ローカル受信プロトコル（IGMPv3）経由で受信者から提供され、送信元固有ツリーを直接作成するために使用されます。

マルチキャスト双方向 PIM

マルチキャスト双方向 PIM は、ビデオ会議、Webex ミーティング、およびグループチャットなどのように、同時に通信を行う送信元と受信者が多く存在し、各参加者がマルチキャスト トラフィックの送信元、受信者のどちらにもなりうるネットワークで有効です。PIM 双方向モードを使用すると、RP は共有ツリーの（*,G）エントリのみを作成します。（S,G）エントリはありません。各（S,G）エントリの状態テーブルを維持しないので、RP のリソースの節約になります。

PIM スパース モードでは、トラフィックは共有ツリーを下りにのみ流れます。PIM 双方向モードでは、トラフィックは共有ツリーの上りと下りの双方向に流れます。

PIM 双方向モードでは、PIM 登録/登録停止メカニズムを使って RP に送信元の登録をしません。送信元はそれぞれ、いつでもソースへの送信を開始できます。マルチキャスト パケットが RP に到達すると、共有ツリーで下りに転送されるか（受信者がいる場合）、ドロップされます（受信者がいない場合）。ただし、RP から送信元に対してマルチキャスト トラフィックの送信停止を命令する方法はありません。

設計の観点から、ネットワークのどこに RP を配置するかを考える必要があります。ネットワーク内の送信元と受信者の中間のどこかに配置する必要があるからです。

PIM 双方向モードには、リバース パス フォワーディング（RPF）のチェックがありません。ループを回避するため、代わりに代表フォワーダ（DF）の概念を使用します。この DF は、セグメント内で唯一、RP にマルチキャスト トラフィックの送信を許可されたルータです。マルチキャスト トラフィックを転送するルータがセグメントあたり 1 台だけであれば、ループは発生しません。DF は次のメカニズムを使って選択されます。

- RP へのメトリックが最も小さいルータが DF になる。
- メトリックが等しい場合は、IP アドレスが最も大きいルータが DF になる。

PIM ブートストラップ ルータ（BSR）

PIM ブートストラップ ルータ（BSR）は、RP 機能およびグループの RP 情報をリレーするために候補のルータを使用する動的ランデブーポイント（RP）セレクション モデルです。RP 機能には RP の検出が含まれており、RP にデフォルト ルートを提供します。これは、一連のデバイスを BSR の選択プロセスに参加する候補の BSR（C-BSR）として設定し、その中から BSR を選択することで実現します。BSR が選択されると、候補のランデブー ポイント（C-RP）として設定されたデバイスは、選定された BSR にグループ マッピングの送信を開始します。次に、BSR はホップ単位で PIM ルータ間を移動する BSR メッセージ経由で、マルチキャスト ツリーに至る他のすべてのデバイスにグループ/RP マッピング情報を配布します。

この機能は、RPを動的に学習する方法を提供し、これはRPが定期的に上下移動する複雑な大型ネットワークに非常に重要です。

PIM ブートストラップ ルータ（BSR）の用語

PIM BSR の設定では、次の用語がよく使用されます。

- ブートストラップ ルータ（BSR）：BSR はホップバイホップ ベースの PIM が設定された他のルータに、ランデブー ポイント（RP）情報をアドバタイズします。選択プロセスの後に、複数の候補 BSR の中から 1 つの BSR が選択されます。このブートストラップ ルータの主な目的は、すべての候補 RP（C-RP）通知を RP-set というデータベースに収集し、これをネットワーク内の他のすべてのルータに定期的に BSR メッセージとして送信することです（60 秒ごと）。
- ブートストラップ ルータ（BSR）メッセージ：BSR メッセージは、TTL が 1 に設定された All-PIM-Routers グループへのマルチキャストです。これらのメッセージを受信するすべてのPIMネイバーは、メッセージを受信したインターフェイスを除くすべてのインターフェイスからそのメッセージを再送信します（TTLは1に設定）。BSRメッセージには、現在アクティブな BSR の RP-set と IP アドレスが含まれています。この方法で、C-RP は C-RP メッセージのユニキャスト先を認識します。
- 候補ブートストラップ ルータ（C-BSR）：候補 BSR として設定されるデバイスは、BSR 選択メカニズムに参加します。最も優先順位の高い C-BSR が BSR として選択されます。C-BSR の最上位の IP アドレスはタイブレイカーとして使用されます。BSR の選択プロセスはプリエンプティブです。たとえば、より優先順位の高いC-BSRが新たに見つかると、新しい選択プロセスがトリガーされます。
- 候補ランデブーポイント（C-RP）：RPはマルチキャストデータの送信元と受信者が対面する場所として機能します。C-RP として設定されているデバイスは、マルチキャスト グループ マッピング情報を、ユニキャスト経由で直接、選択された BSR に定期的にアドバタイズします。これらのメッセージには、グループ範囲、C-RP アドレス、および保留時間が含まれています。現在の BSR の IP アドレスは、ネットワーク内のすべてのルータが受信した定期的な BSR メッセージから学習されます。このようにして、BSR は現在動作中で到達可能な RP 候補について学習します。

（注） C-RP は BSR トラフィックの必須要件ですが、Firepower Threat Defense デバイス は C-RP としては機能しません。ルータのみが C-RP として機能できます。したがって、BSRのテスト機能では、トポロジにルータを追加する必要があります。

- BSR 選択メカニズム：各 C-BSR は、BSR 優先順位フィールドを含むブートストラップ メッセージ（BSM）を生成します。ドメイン内のルータは、ドメイン全体にBSMをフラッディングします。自身より優先順位の高い C-BSR に関する情報を受け取った BSR は、一定期間、BSM の送信を抑止します。残った単一の C-BSR が選択された BSR となり、その BSM により、選択された BSR に関する通知がドメイン内の他のすべてのルータに対して送信されます。

マルチキャスト グループの概念

マルチキャストはグループの概念に基づくものです。受信者の任意のグループは、特定のデータ ストリームを受信することに関心があります。このグループには物理的または地理的な境界がなく、インターネット上のどの場所にホストを置くこともできます。特定のグループに流れるデータの受信に関心があるホストは、IGMP を使用してグループに加入する必要があります。ホストがデータ ストリームを受信するには、グループのメンバでなければなりません。

マルチキャスト アドレス

マルチキャストアドレスは、グループに加入し、このグループに送信されるトラフィックの受信を希望する IP ホストの任意のグループを指定します。

クラスタ

マルチキャスト ルーティングは、クラスタリングをサポートします。スパンド EtherChannel クラスタリングでは、ファースト パス転送が確立されるまでの間、プライマリ ユニットがすべてのマルチキャスト ルーティング パケットとデータ パケットを送信します。ファースト パス転送が確立されると、従属ユニットがマルチキャスト データ パケットを転送できます。すべてのデータ フローは、フル フローです。スタブ転送フローもサポートされます。スパンド EtherChannel クラスタリングでは 1 つのユニットだけがマルチキャスト パケットを受信するため、プライマリ ユニットへのリダイレクションは共通です。

マルチキャスト ルーティングのガイドライン

コンテキスト モード

シングル コンテキスト モードでサポートされています。

ファイアウォール モード

ルーテッド ファイアウォール モードでだけサポートされています。トランスペアレント ファイアウォール モードはサポートされません。

IPv6

IPv6 はサポートされません。

クラスタ

IGMP および PIM のクラスタリングでは、この機能はプライマリ ユニットでのみサポートされます。

その他のガイドライン

224.1.2.3 などのマルチキャスト ホストへのトラフィックを許可するには、インバウンド セキュリティ ゾーン上のアクセス制御またはプレフィルタ ルールを設定する必要があります。ただし、ルールの宛先セキュリティ ゾーンを指定したり、初期接続確認の間にマルチキャストの接続に適用したりすることはできません。

IGMP 機能の設定

IP ホストは、自身のグループ メンバーシップを直接接続されているマルチキャスト ルータに報告するために IGMP を使用します。IGMP は、マルチキャスト グループの個々のホストを特定の LAN にダイナミックに登録するために使用します。ホストは、そのローカル マルチキャスト ルータに IGMP メッセージを送信することで、グループ メンバーシップを識別します。IGMP では、ルータは IGMP メッセージを受信し、定期的にクエリーを送信して、特定のサブネットでアクティブなグループと非アクティブなグループを検出します。

ここでは、インターフェイス単位で任意の IGMP 設定を行う方法について説明します。

ステップ 1 マルチキャスト ルーティングの有効化 （1035 ページ）
ステップ 2 IGMP プロトコルの設定 （1036 ページ）。
ステップ 3 IGMP アクセスグループの設定 （1038 ページ）。
ステップ 4 IGMP スタティック グループの設定 （1039 ページ）。
ステップ 5 IGMP 参加グループの設定 （1039 ページ）。

マルチキャスト ルーティングの有効化

Firepower Threat Defense デバイスでマルチキャスト ルーティングを有効にすると、デフォルトですべてのインターフェイス上の IGMP と PIM が有効になります。IGMP は、直接接続されているサブネット上にグループのメンバが存在するかどうか学習するために使用されます。ホストは、IGMP 報告メッセージを送信することにより、マルチキャスト グループに参加します。PIM は、マルチキャスト データグラムを転送するための転送テーブルを維持するために使用されます。

（注） マルチキャスト ルーティングでは、UDP トランスポート層だけがサポートされています。

以下の表に、Firepower Threat Defense デバイスの RAM の量に基づいた特定のマルチキャスト テーブルのエントリの最大数を示します。この上限に達すると、新しいエントリは廃棄されます。

表 *81 :* マルチキャスト テーブルのエントリ数の上限

Table	16 MB	128 MB	128 + MB
MFIB	1000	3000	30000
IGMP グループ	1000	3000	30000
PIM ルート	3000	7000	72000

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** の順に選択し、FTD デバイスを編集します。

ステップ 2 Choose **[ルーティング（Routing）]** > **[マルチキャスト ルーティング（Multicast Routing）]** > **[IGMP]** を選択します。

ステップ 3 [マルチキャスト ルーティングの有効化（Enable Multicast Routing）] チェックボックスをオンにします。

このチェックボックスをオンにすると、Firepower Threat Defense デバイス上で IP マルチキャスト ルーティングが有効になります。このチェックボックスをオフにすると、IP マルチキャスト ルーティングがディセーブルになります。デフォルトでは、マルチキャストはディセーブルになっています。マルチキャスト ルーティングをイネーブルにすると、すべてのインターフェイス上でマルチキャストがイネーブルになります。

マルチキャストはインターフェイスごとにディセーブルにできます。この情報が役に立つのは、あるインターフェイス上にマルチキャスト ホストがないことがわかっている場合に、そのインターフェイス上で Firepower Threat Defense デバイスからホスト クエリ メッセージが送信されないように設定するときです。

IGMP プロトコルの設定

転送インターフェイス、クエリ メッセージ、時間間隔などのインターフェイスごとに、IGMP パラメータを設定できます。

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** の順に選択し、FTD デバイスを編集します。

ステップ 2 **[ルーティング（Routing）]** > **[マルチキャスト ルーティング（Multicast Routing）]** > **[IGMP]** を選択します。

ステップ 3 [プロトコル（Protocol）] タブで、[追加（Add）] または [編集（Edit）] をクリックします。

[IGMP パラメータの追加（Add IGMP parameters）] ダイアログボックスで、Firepower Threat Defense デバイスに新しい IGMP パラメータを追加します。既存のパラメータを変更する場合は、[IGMP パラメータの編集（Edit IGMP parameters）] ダイアログボックスを使用します。

ステップ 4 次のオプションを設定します。

- [インターフェイス（Interface）]：ドロップダウン リストから、IGMP プロトコルを設定するインターフェイスを選択します。
- [IGMP を有効にする（Enable IGMP）]：IGMP を有効にするには、このチェックボックスをオンにします。

  （注） 特定のインターフェイスでの IGMP 無効が役に立つのは、あるインターフェイス上にマルチキャスト ホストがないことがわかっている場合に、そのインターフェイス上で Firepower Threat Defense デバイスからホスト クエリー メッセージが送信されないように設定するときです。

- [インターフェイスの転送（Forward Interface）]：ドロップダウン リストから、どのインターフェイスから IGMP メッセージを送信するかを選択します。

  これは Firepower Threat Defense デバイスを、IGMP プロキシ エージェントとして設定し、あるインターフェイスに接続されているホストから、別のインターフェイスのアップストリーム マルチキャスト ルータに IGMP メッセージを転送します。

- [バージョン（Version）]：IGMP バージョン 1 または 2 を選択します。

  デフォルトでは、Firepower Threat Defense デバイスで IGMP バージョン 2 が実行されるため、多数の追加機能が使用できるようになります。

  （注） サブネットのマルチキャスト ルータはすべて、同じ IGMP バージョンをサポートしている必要があります。Firepower Threat Defense デバイスが自動的にバージョン 1 ルータを検出してバージョン 1 に切り替えることはありません。ただ、サブネットに IGMP のバージョン 1 のホストとバージョン 2 のホストを混在させることも可能です。IGMP バージョン 2 を実行している Firepower Threat Defense デバイスは、IGMP バージョン 1 のホストが存在しても正常に動作します。

- [クエリー インターバル（Query Interval）]：指定したルータから IGMP ホストクエリー メッセージが送信される秒単位の時間間隔。指定できる範囲は 1 ～ 3600 です。デフォルトは 125 です。

  （注） 指定されたタイムアウト値の時間が経過しても、Firepower Threat Defense デバイスがインターフェイス上でクエリー メッセージを検出できなかった場合は、その Firepower Threat Defense デバイスが指定ルータになり、クエリー メッセージの送信を開始します。

- [応答時間（Response Time）]：Firepower Threat Defense デバイスでグループが削除される前の秒単位の時間間隔。指定できる範囲は 1 ～ 25 です。デフォルトは 10 です。

  Firepower Threat Defense デバイスがこの時間内にホスト クエリーの応答を受信しなかった場合、グループを削除します。

- [グループ制限（Group Limit）]：インターフェイス上で加入する最大ホスト数。指定できる範囲は 1 ～ 500 です。デフォルトは 500 です。

  IGMP メンバーシップ報告の結果の IGMP 状態の数は、インターフェイスごとに制限することができます。設定された上限を超過したメンバーシップ報告は IGMP キャッシュに入力されず、超過した分のメンバーシップ報告のトラフィックは転送されません。

- [クエリー タイムアウト（Query Timeout）]：秒単位の時間で、前のリクエスタがリクエスタとしての動作を停止してからこの時間が経過すると、この Firepower Threat Defense デバイスがそのインターフェイスのリクエスタの役割を引き継ぎます。指定できる範囲は 60 ～ 300 です。デフォルトは 255 です。

ステップ 5 [OK] をクリックして、IGMP プロトコル構成を保存します。

IGMP アクセスグループの設定

アクセス コントロール リストを使用して、マルチキャスト グループへのアクセスを制御できます。

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** の順に選択し、FTD デバイスを編集します。

ステップ 2 **[ルーティング（Routing）]** > **[マルチキャスト ルーティング（Multicast Routing）]** > **[アクセス グループ（Access Group）]** を選択します。

ステップ 3 [アクセス グループ（Access Group）] タブで、[追加（Add）] または [編集（Edit）] をクリックします。

[IGMP アクセス グループ パラメータを追加（Add IGMP Access Group parameters）] ダイアログボックスを使用して、新しい IGMP アクセスグループをアクセスグループ テーブルに追加します。既存のパラメータを変更する場合は、[IGMP アクセス グループ パラメータを編集（Edit IGMP Access Group parameters）] ダイアログボックスを使用します。

ステップ 4 次のオプションを設定します。

a) [インターフェイス（Interface）] ドロップダウンリストから、アクセス グループが関連付けられるインターフェイスを選択します。既存のアクセス グループを編集しているときは、関連インターフェイスは変更できません。

b) 次のいずれかのオプション ボタンをクリックします。

- [標準アクセス リスト（Standard Access List）]：[標準アクセス リスト（Standard Access List）] ドロップダウンリストから、標準 ACL を選択するか、または追加アイコン（  ）をクリックして新しい標準 ACL を作成します。手順については、標準 ACL オブジェクトの設定（612 ページ）を参照してください。
- [拡張アクセス リスト（Extended Access List）]：[拡張アクセス リスト（Extended Access List）] ドロップダウンリストから、拡張 ACL を選択するか、または追加アイコン（）をクリックして新しい拡張 ACL を作成します。手順については、拡張 ACL オブジェクトの設定（611 ページ）を参照してください。

ステップ 5 [OK] をクリックして、アクセスグループ構成を保存します。

IGMP スタティック グループの設定

グループ メンバーがグループのメンバーシップをレポートできなかったり、ネットワーク セグメントにグループのメンバーが存在しない場合でも、そのグループのマルチキャスト トラフィックをそのネットワーク セグメントに送信しなければならないことがあります。そのようなグループのマルチキャスト トラフィックをそのセグメントに送信するには、スタティック加入した IGMP グループを設定します。この方法の場合、Firepower Threat Defense デバイスはパケットそのものを受信せず、転送だけを実行します。そのため、スイッチングが高速に実施されます。発信インターフェイスはIGMP キャッシュ内に存在しますが、このインターフェイスはマルチキャスト グループのメンバーではありません。

ステップ 1 **[デバイス（Devices）] > [デバイス管理（Device Management）]** の順に選択し、FTD デバイスを編集します。

ステップ 2 **[ルーティング（Routing）] > [マルチキャスト ルーティング（Multicast Routing）] > [IGMP]** を選択します。

ステップ 3 [スタティック グループ（Static Group）] タブで、[追加（Add）] または [編集（Edit）] をクリックします。

インターフェイスに対してマルチキャスト グループをスタティックに割り当てる場合は、[IGMP スタティック グループ パラメータの追加（Add IGMP Static Group parameters）] ダイアログボックスを使用します。既存のスタティック グループの割り当てを変更する場合は、[IGMP スタティック グループ パラメータの編集（Edit IGMP Static Group parameters）] ダイアログボックスを使用します。

ステップ 4 次のオプションを設定します。

- [インターフェイス（Interface）] ドロップダウン リストから、マルチキャスト グループをスタティックに割り当てるインターフェイスを選択します。既存のエントリを編集しているときは、値は変更できません。
- [マルチキャスト グループ（Multicast Groups）] ドロップダウンリストから、インターフェイスを割り当てるマルチキャスト グループを選択するか、追加アイコン（  ）をクリックして、新しいマルチキャスト グループを作成します。手順については、ネットワーク オブジェクトの作成を参照してください。

ステップ 5 [OK] をクリックして、スタティック グループ設定を保存します。

IGMP 参加グループの設定

インターフェイスをマルチキャスト グループのメンバーとして設定できます。マルチキャスト グループに加入するように Firepower Threat Defense デバイスを設定すると、アップストリーム ルータはそのグループのマルチキャスト ルーティング テーブル情報を維持して、このグループをアクティブにするパスを保持します。

（注） IGMP スタティック グループの設定 （1039ページ）を参照して、特定のグループのマルチキャストパケットを特定のインターフェイスに転送する必要がある場合に、Firepower Threat Defense デバイスがそのパケットをそのグループの一部として受け付けることがないようにする方法を確認してください。

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** の順に選択し、FTD デバイスを編集します。

ステップ 2 **[ルーティング（Routing）]** > **[マルチキャスト ルーティング（Multicast Routing）]** > **[IGMP]** を選択します。

ステップ 3 [参加グループ（Join Group）] タブで、[追加（Add）] または [編集（Edit）] をクリックします。

Firepower Threat Defense デバイスをマルチキャスト グループのメンバーに設定する場合は、[IGMP 参加グループ パラメータの追加（Add IGMP Join Group parameters）] ダイアログボックスを使用します。既存のパラメータを変更する場合は、[IGMP 参加グループ パラメータの編集（Edit IGMP Join Group parameters）] ダイアログボックスを使用します。

ステップ 4 次のオプションを設定します。

- [インターフェイス（Interface）] ドロップダウンリストから、マルチキャスト グループのメンバーにするインターフェイスを選択します。既存のエントリを編集しているときは、値は変更できません。
- [参加グループ（Join Group）] ドロップダウンリストから、インターフェイスを割り当てるマルチキャスト グループを選択するか、[プラス（Plus）] アイコンをクリックして、新しいマルチキャスト グループを作成します。手順については、ネットワーク オブジェクトの作成 を参照してください。

PIM 機能の設定

ルータは PIM を使用して、マルチキャスト ダイアグラムを転送するために使われる転送テーブルを維持します。Firepower Threat Defense デバイスでマルチキャスト ルーティングをイネーブルにすると、PIM および IGMP がすべてのインターフェイスで自動的にイネーブルになります。

（注） PIM は、PAT ではサポートされません。PIM プロトコルはポートを使用せず、PAT はポートを使用するプロトコルに対してのみ動作します。

ここでは、任意の PIM 設定を行う方法について説明します。

ステップ 1 PIM プロトコルの設定 （1041 ページ）

ステップ 2 PIM ネイバー フィルタの設定 （1042 ページ）
ステップ 3 PIM 双方向ネイバー フィルタの設定 （1043 ページ）
ステップ 4 PIM ランデブー ポイントの設定 （1044 ページ）
ステップ 5 PIM ルート ツリーの設定 （1045 ページ）
ステップ 6 PIM リクエスト フィルタの設定 （1046 ページ）
ステップ 7 マルチキャスト境界フィルタの設定 （1049 ページ）

PIM プロトコルの設定

PIM は、特定のインターフェイスで有効または無効にすることができます。

代表ルータ（DR）のプライオリティを設定することもできます。DR は、PIM 登録メッセージ、PIM 加入メッセージ、およびプルーニング メッセージの RP への送信を担当します。1 つのネットワーク セグメントに複数のマルチキャスト ルータがある場合は、DR プライオリティに基づいて DR が選択されます。複数のデバイスの DR プライオリティが等しい場合、最上位の IP アドレスを持つデバイスが DR になります。デフォルトでは、Firepower Threat Defense デバイスの DR プライオリティは 1 です。

ルータ クエリ メッセージは、PIM DR の選択に使用されます。PIM DR は、ルータ クエリー メッセージを送信します。デフォルトでは、ルータ クエリー メッセージは 30 秒間隔で送信されます。さらに、60 秒ごとに、Firepower Threat Defense デバイスは PIM 加入メッセージおよびプルーニング メッセージを送信します。

ステップ 1 **[デバイス（Devices）] > [デバイス管理（Device Management）]** の順に選択し、FTD デバイスを編集します。
ステップ 2 **[ルーティング（Routing）] > [マルチキャスト ルーティング（Multicast Routing）] > [PIM]** を選択します。
ステップ 3 [プロトコル（Protocol）] タブで、[追加（Add）] または [編集（Edit）] をクリックします。

インターフェイスに新しい PIM パラメータを追加する場合は、[PIM パラメータの追加（Add PIM parameters）] ダイアログボックスを使用します。既存のパラメータを変更する場合は、[PIM パラメータの編集（Edit PIM parameters）] ダイアログボックスを使用します。

ステップ 4 次のオプションを設定します。

- [インターフェイス（Interface）]：ドロップダウン リストから、PIM プロトコルを設定するインターフェイスを選択します。
- [PIM を有効にする（Enable PIM）]：PIM を有効にするには、このチェックボックスをオンにします。
- [DR プライオリティ（DR Priority）]：選択したインターフェイスの DR の値。サブネット上のルータのうち、DR プライオリティが最いものが指定ルータになります。有効な値の範囲は 0 ～ 4294967294 です。デフォルトの DR プライオリティは 1 です。この値を 0 に設定した場合は、その Firepower Threat Defense デバイス インターフェイスがデフォルトのルータになることはありません。

- [Hello 間隔（Hello Interval）]：インターフェイスから PIM hello メッセージが送信される時間間隔（秒単位）。指定できる範囲は 1 ～ 3600 です。デフォルトは 30 です。
- [参加プルーニング間隔（Join Prune Interval）]：インターフェイスから PIM の加入アドバタイズメントおよびプルーニング アドバタイズメントが送信される時間間隔（秒単位）。指定できる範囲は 10 ～ 600 です。デフォルトは 60 です。

ステップ 5 [OK] をクリックして、PIM プロトコル設定を保存します。

PIM ネイバー フィルタの設定

PIM ネイバーにできるルータの定義が可能です。PIM ネイバーにできるルータをフィルタリングすると、次の制御を行うことができます。

- 許可されていないルータが PIM ネイバーにならないようにする。
- 添付されたスタブ ルータが PIM に参加できないようにする。

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** の順に選択し、FTD デバイスを編集します。

ステップ 2 **[ルーティング（Routing）]** > **[マルチキャスト ルーティング（Multicast Routing）]** > **[PIM]** を選択します。

ステップ 3 [ネイバー フィルタ（Neighbor Filter）] タブで、[追加（Add）] または [編集（Edit）] をクリックします。

インターフェイスに新しいPIMネイバーフィルタを追加する場合は、[PIMネイバーフィルタの追加（Add PIM Neighbor Filter）] ダイアログボックスを使用します。既存のパラメータを変更する場合は、[PIM ネイバー フィルタの編集（Edit PIM Neighbor Filter）] ダイアログボックスを使用します。

ステップ 4 次のオプションを設定します。

- [インターフェイス（Interface）] ドロップダウン リストから、PIM ネイバー フィルタを追加するインターフェイスを選択します。
- [標準アクセス リスト（Standard Access List）]：[標準アクセス リスト（Standard Access List）] ドロップダウン リストから標準 ACL を選択するか、追加アイコン（）をクリックして新しい標準 ACL を作成します。手順については、標準 ACL オブジェクトの設定 （612 ページ）を参照してください。

  （注） [標準アクセス リスト エントリの追加（Add Standard Access List Entry）] ダイアログボックスで [許可（Allow）] を選択すると、マルチキャスト グループ アドバタイズメントはこのインターフェイスを通過できるようになります。[ブロック（Block）]を選択すると、指定したマルチキャスト グループ アドバタイズメントはこのインターフェイスを通過できなくなります。インターフェイスに対してマルチキャスト境界を設定すると、ネイバーフィルタエントリで許可されていない限り、すべてのマルチキャスト トラフィックが、インターフェイスの通過を拒否されます。

ステップ 5 [OK] をクリックして、PIM ネイバー フィルタ設定を保存します。

PIM 双方向ネイバー フィルタの設定

PIM 双方向ネイバー フィルタは、Designated Forwarder（DF）選定に参加できるネイバー デバイスを定義する ACL です。PIM 双方向ネイバー フィルタがインターフェイスに設定されていなければ、制限はありません。PIM 双方向ネイバー フィルタが設定されている場合は、ACL で許可されるネイバーだけが DF 選択プロセスに参加できます。

双方向 PIM では、マルチキャスト ルータで保持するステート情報を減らすことができます。DF を選択するために、セグメント内のすべてのマルチキャスト ルータが双方向で有効になっている必要があります。

PIM 双方向ネイバー フィルタがイネーブルの場合、その ACL によって許可されるルータは、双方向に対応していると見なされます。したがって、次のことが当てはまります。

- 許可されたネイバーが双方向モードをサポートしていない場合、DF 選択は実施されません。
- 拒否されたネイバーが双方向モードをサポートしている場合、DF 選択は実施されません。
- 拒否されたネイバーが双方向モードをサポートしていない場合、DF 選択が実行される可能性があります。

ステップ 1 **[デバイス（Devices）] > [デバイス管理（Device Management）]** の順に選択し、FTD デバイスを編集します。

ステップ 2 [マルチキャスト ルーティング（Multicast Routing）] > [PIM] を選択します。

ステップ 3 [双方向ネイバー フィルタ（Bidirectional Neighbor Filter）] タブで、[追加（Add）] または [編集（Edit）] をクリックします。

PIM 双方向ネイバー フィルタ ACL の ACL エントリを作成する場合は、[PIM 双方向ネイバー フィルタの追加（Add PIM Bidirectional Neighbor Filter）] ダイアログボックスを使用します。既存のパラメータを変更する場合は、[PIM 双方向ネイバー フィルタの編集（Edit PIM Bidirectional Neighbor Filter）] ダイアログボックスを使用します。

ステップ 4 次のオプションを設定します。

- [インターフェイス（Interface）] ドロップダウン リストから、PIM 双方向ネイバー フィルタの ACL エントリを設定するインターフェイスを選択します。
- [標準アクセス リスト（Standard Access List）]：[標準アクセス リスト（Standard Access List）] ドロップダウン リストから標準 ACL を選択するか、追加アイコン（  ）をクリックして新しい標準 ACL を作成します。手順については、標準 ACL オブジェクトの設定 （612 ページ）を参照してください。

（注） [標準アクセス リスト エントリの追加（Add Standard Access List Entry）] ダイアログボックスで [許可（Allow）] を選択すると、指定したデバイスが DR 選択プロセスに参加できます。[ブロック（Block）] を選択すると、指定したデバイスは DR 選択プロセスに参加できなくなります。

ステップ 5 [OK] をクリックして、PIM 双方向ネイバー フィルタ設定を保存します。

PIM ランデブー ポイントの設定

Firepower Threat Defense デバイスを複数のグループの RP として機能するように設定することができます。ACL に指定されているグループ範囲によって、PIM RP のグループ マッピングが決まります。ACL が指定されていない場合は、マルチキャスト グループ全体の範囲（224.0.0.0/4）にグループの RP が適用されます。双方向 PIM の詳細については、マルチキャスト双方向 PIM （1032 ページ）を参照してください。

RP には、次の制約事項が適用されます。

- 同じ RP アドレスは、2 度使用できません。
- 複数の RP に対しては、[All Groups] を指定できません。

ステップ 1 **[デバイス（Devices）] > [デバイス管理（Device Management）]** の順に選択し、FTD デバイスを編集します。

ステップ 2 **[ルーティング（Routing）] > [マルチキャスト ルーティング（Multicast Routing）] > [PIM]** を選択します。

ステップ 3 [ランデブー ポイント（Rendezvous Points）] タブで、[追加（Add）] または [編集（Edit）] をクリックします。

[ランデブー ポイント（Rendezvous Points）] テーブルに新しいエントリを作成する場合は、[ランデブー ポイントの追加（Add Rendezvous Point）] ダイアログボックスを使用します。既存のパラメータを変更する場合は、[ランデブー ポイントの編集（Edit Rendezvous Point）] ダイアログボックスを使用します。

ステップ 4 次のオプションを設定します。

- [ランデブー ポイントの IP アドレス（Rendezvous Point IP address）] ドロップダウン リストから、RP として追加する IP アドレスを選択するか、追加アイコン（  ）をクリックして新しいネットワーク オブジェクトを作成します。手順については、ネットワーク オブジェクトの作成を参照してください。
- [双方向転送の使用（Use bi-directional forwarding）] チェックボックスをオンにすると、指定されているマルチキャスト グループは双方向モードで動作します。双方向モードでは、Firepower Threat Defense デバイスがマルチキャスト パケットを受信したときに、直接接続されたメンバーも PIM ネイバーも存在しない場合は、送信元にプルーニング メッセージが返されます。

- 指定した RP をインターフェイス上のすべてのマルチキャスト グループに対して使用する場合は、[すべてのマルチキャスト グループに対してこの RP を使用する（Use this RP for All Multicast Groups）] オプション ボタンを選択します。
- [次に指定するようにすべてのマルチキャスト グループに対してこの RP を使用する（Use this RP for all Multicast Groups as specified below）] を選択して、指定の RP とともに使用するマルチキャスト グループを指定します。次に [標準アクセス リスト（Standard Access List）] ドロップダウン リストから標準 ACL を選択するか、追加アイコン（  ）をクリックして、新しい標準 ACL を作成します。手順については、標準 ACL オブジェクトの設定 （612 ページ）を参照してください。

ステップ 5 [OK] をクリックして、ランデブー ポイント設定を保存します。

PIM ルート ツリーの設定

デフォルトでは、PIM リーフ ルータは、新しい送信元から最初のパケットが到着した直後に、最短パス ツリーに加入します。この方法では、遅延が短縮されますが、共有ツリーに比べて多くのメモリが必要になります。すべてのマルチキャスト グループまたは特定のマルチキャスト アドレスに対して、Firepower Threat Defense デバイスを最短パス ツリーに加入させるか、共有ツリーを使用するかを設定できます。

[Multicast Groups] テーブルで指定されていないグループには最短パス ツリーが使用されます。[Multicast Groups] テーブルには、共有ツリーを使用するマルチキャスト グループが表示されます。テーブル エントリは、上から下の順で処理されます。ある範囲のマルチキャスト グループが含まれるエントリを作成し、その範囲の中から特定のグループを除外するには、その除外するグループに対する拒否ルールをテーブルの先頭に配置し、その範囲内のマルチキャスト グループ全体に対する許可ルールを deny 文の下に配置します。

（注） この動作は Shortest Path Switchover（SPT）と呼ばれます。[共有ツリー（Shared Tree）] オプションを常に使用することをお勧めします。

ステップ 1 **[デバイス（Devices）] > [デバイス管理（Device Management）]** の順に選択し、FTD デバイスを編集します。

ステップ 2 **[ルーティング（Routing）] > [マルチキャスト ルーティング（Multicast Routing）] > [PIM]** を選択します。

ステップ 3 [ルート ツリー（Route Tree）] タブで、ルート ツリーのパスを選択します。

- すべてのマルチキャスト グループに最短パス ツリーを使用する場合は、[最短パス（Shortest Path）] オプション ボタンをクリックします。
- すべてのマルチキャスト グループに共有ツリーを使用する場合は、[共有ツリー（Shared Tree）] オプション ボタンをクリックします。

- [次に示すグループの共有ツリー（Shared tree for below mentioned group）] オプション ボタンをクリックして、[マルチキャスト グループ（Multicast Groups）] テーブルで指定されたグループを指定します。次に [標準アクセス リスト（Standard Access List）] ドロップダウン リストから標準 ACL を選択するか、追加アイコン（  ）をクリックして、新しい標準ACLを作成します。手順については、標準ACL オブジェクトの設定 （612 ページ）を参照してください。

ステップ 4 [OK] をクリックして、ルート ツリー設定を保存します。

PIM リクエスト フィルタの設定

Firepower Threat Defense デバイスが RP として動作しているときは、特定のマルチキャスト送信元を登録できないように制限することができます。このようにすると、未許可の送信元が RP に登録されるのを回避できます。Firepower Threat Defense デバイスが PIM 登録メッセージを受け入れるマルチキャスト送信元を定義できます。

ステップ 1 **[デバイス（Devices）] > [デバイス管理（Device Management）]** の順に選択し、FTD デバイスを編集します。

ステップ 2 **[ルーティング（Routing）] > [マルチキャスト ルーティング（Multicast Routing）] > [PIM]** を選択します。

ステップ 3 [リクエスト フィルタ（Request Filter）] タブで、RP として動作する Firepower Threat Defense デバイスに登録できるマルチキャスト送信元を定義します。

- [PIM 登録メッセージのフィルタ方法：（Filter PIM register messages using:）] ドロップダウン リストから [なし（None）]、[アクセス リスト（Access List）]、または [ルート マップ（Route Map）] を選択します。
- ドロップダウン リストから [アクセス リスト（Access List）] を選択した場合は、拡張 ACL を選択するか、追加アイコン（  ）をクリックして新しい拡張ACLを作成します。手順については、拡張ACL オブジェクトの設定 （611 ページ）を参照してください。

  （注） [拡張アクセス リスト エントリの追加（Add Extended Access List Entry）] ダイアログボックスで、ドロップダウン リストから [許可（Allow）] を選択して、指定したマルチキャスト トラフィックの指定した送信元を Firepower Threat Defense デバイスに登録することを許可するルールを作成します。または、[ブロック（Block）] を選択して、指定したマルチキャスト トラフィックの指定した送信元が Firepower Threat Defense デバイスに登録されることを防ぐルールを作成します。

- [ルート マップ（Route Map）] を選択した場合は、[ルート マップ（Route Map）] ドロップダウン リストからルート マップを選択するか、追加アイコン（  ）をクリックして新しいルート マップを作成します。手順については、ネットワーク オブジェクトの作成を参照してください。

ステップ 4 [OK] をクリックして、リクエスト フィルタ設定を保存します。

Firepower Threat Defense デバイスのブートストラップ ルータ設定

Firepower Threat Defense デバイスを BSR 候補として設定できます。

ステップ 1 **[デバイス（Devices）] > [デバイス管理（Device Management）]** の順に選択し、FTD デバイスを編集します。

ステップ 2 **[ルーティング（Routing）] > [マルチキャスト ルーティング（Multicast Routing）] > [PIM]** を選択します。

ステップ 3 [ブートストラップ ルータ（Bootstrap Router）] タブで、[この FTD をブートストラップ ルータ候補として設定（Configure this FTD as a Candidate Bootstrap Router (C-BSR)）] チェックボックスをオンにして、C-BSR の設定をします。

a) [インターフェイス（Interface）] ドロップダウンリストから、BSR アドレスが派生する Firepower Threat Defense デバイスのインターフェイスを選択して、候補にします。

このインターフェイスは PIM を使用して有効化する必要があります。

b) [ハッシュ マスク長（Hash mask length）] フィールドに、ハッシュ関数が呼び出される前にグループ アドレスと論理積をとるマスク長（最大 32 ビット）を入力します。ハッシュ元が同じであるすべてのグループは、同じ RP に対応します。たとえば、マスク長が 24 の場合、グループ アドレスの最初の 24 ビットだけが使用されます。これにより、複数のグループについて 1 つの RP を取得できます。指定できる範囲は 0 ～ 32 です。

c) [優先度（Priority）] フィールドに、BSR 候補の優先度を入力します。プライオリティが大きな BSR が優先されます。プライオリティ値が同じ場合は、IP アドレスがより高位であるルータが BSR となります。指定できる範囲は 0 ～ 255 です。デフォルト値は 0 です。

ステップ 4 （オプション）[この FTD をボーダー ブートストラップ ルータとして設定（Configure this FTD as a Border Bootstrap Router (BSR)）] セクションで、追加アイコン（  ）をクリックして、PIM BSR メッセージを送受信しないインターフェイスを選択します。

- [インターフェイス（Interface）] ドロップダウンリストから、PIM BSR メッセージを送受信しないインターフェイスを選択します。

  RP または BSR アドバタイズメントは、フィルタリングされている効果的に隔てられた 2 つの RP 情報交換ドメインです。

- BSR を有効化するには、[ボーダー BSR を有効にする（Enable Border BSR）] チェックボックスをオンにします。

ステップ 5 [OK] をクリックして、ブートストラップ ルータ設定を保存します。

マルチキャスト ルートの設定

スタティック マルチキャスト ルートを設定すると、マルチキャスト トラフィックをユニキャスト トラフィックから分離できます。たとえば、送信元と宛先の間のパスでマルチキャスト ルーティングがサポートされていない場合は、その解決策として、2 つのマルチキャスト デバ

イスの間に GRE トンネルを設定し、マルチキャスト パケットをそのトンネル経由で送信します。

PIM を使用する場合、Firepower Threat Defense デバイスは、ユニキャスト パケットを発信元に返送するときと同じインターフェイスでパケットを受信することを想定しています。マルチキャスト ルーティングをサポートしていないルートをバイパスする場合などは、ユニキャスト パケットで 1 つのパスを使用し、マルチキャスト パケットで別の 1 つのパスを使用することもあります。

スタティック マルチキャスト ルートはアドバタイズも再配布もされません。

ステップ 1 **[デバイス（Devices）] > [デバイス管理（Device Management）]** の順に選択し、FTD デバイスを編集します。

ステップ 2 **[ルーティング（Routing）] > [マルチキャスト ルーティング（Multicast Routing）] > [マルチキャスト ルート（Multicast Routes）]** を選択し、[追加（Add）] または [編集（Edit）] をクリックします。

Firepower Threat Defense デバイスに新しいマルチキャスト ルートを追加する場合は、[マルチキャスト ルート設定の追加（Add Multicast Route Configuration）] ダイアログボックスを使用します。既存のマルチキャスト ルートを変更する場合は、[マルチキャスト ルート設定の編集（Edit Multicast Route Configuration）] ダイアログボックスを使用します。

ステップ 3 [送信元ネットワーク（Source Network）] ドロップダウンボックスから、既存のネットワークを選択するか、追加アイコン（  ）をクリックして新しいネットワークを追加します。手順については、ネットワーク オブジェクトの作成 を参照してください。

ステップ 4 ルートを転送するようインターフェイスを設定するには、[インターフェイス（Interface）] オプション ボタンをクリックして、以下のオプションを設定します。

- [送信元インターフェイス（Source Interface）] ドロップダウンリストから、マルチキャスト ルートの着信インターフェイスを選択します。
- [発信インターフェイス/デンス（Output Interface/Dense）] ドロップダウンリストから、ルートが転送される宛先インターフェイスを選択します。
- [距離（Distance）] フィールドに、マルチキャスト ルートの距離を入力します。指定できる範囲は 0 ～ 255 です。

ステップ 5 ルートを転送するよう RPF アドレスを設定するには、[アドレス（Address）] オプションボタンをクリックして、以下のオプションを設定します。

- [RPF アドレス（RPF Address）] フィールドに、マルチキャスト ルートの IP アドレスを入力します。
- [距離（Distance）] フィールドに、マルチキャスト ルートの距離を 0 ～ 255 で入力します。

ステップ 6 [OK] をクリックして、マルチキャスト ルータの設定を保存します。

マルチキャスト境界フィルタの設定

アドレス スコーピングは、同じ IP アドレスを持つ RP が含まれるドメインが相互にデータを漏出させることのないように、ドメイン境界フィルタを定義します。スコーピングは、大きなドメイン内のサブネット境界や、ドメインとインターネットの間の境界で実行されます。

インターフェイスでマルチキャスト グループ アドレスの管理スコープ境界フィルタを設定できます。IANA では、239.0.0.0 ～ 239.255.255.255 のマルチキャスト アドレス範囲が管理スコープアドレスとして指定されています。この範囲のアドレスは、さまざまな組織で管理されるドメイン内で再使用されます。このアドレスはグローバルではなく、ローカルで一意であると見なされます。

影響を受けるアドレスの範囲は、標準 ACL で定義します。境界フィルタが設定されると、マルチキャスト データ パケットは境界を越えて出入りできなくなります。境界フィルタを定めることで、同じマルチキャスト グループ アドレスをさまざまな管理ドメイン内で使用できます。

管理スコープ境界での Auto-RP 検出および通知のメッセージの設定、検査、フィルタリングを行うことができます。境界の ACL で拒否された Auto-RP パケットからの Auto-RP グループ範囲通知は削除されます。Auto-RP グループ範囲通知は、Auto-RP グループ範囲のすべてのアドレスが境界 ACL によって許可される場合に限り境界フィルタを通過できます。許可されないアドレスがある場合は、グループ範囲全体がフィルタリングされ、Auto-RP メッセージが転送される前に Auto-RP メッセージから削除されます。

ステップ 1 **[デバイス（Devices）] > [デバイス管理（Device Management）]** の順に選択し、FTD デバイスを編集します。

ステップ 2 **[ルーティング（Routing）] > [マルチキャスト ルーティング（Multicast Routing）] > [マルチキャスト境界フィルタ（Multicast Boundary Filter）]** を選択し、[追加（Add）] または [編集（Edit）] をクリックします。

[マルチキャスト境界フィルタの追加（Add Multicast Boundary Filter）] ダイアログボックスを使用して、新しいマルチキャスト境界フィルタを Firepower Threat Defense デバイスに追加します。既存のパラメータを変更するには、[マルチキャスト境界フィルタの編集（Edit Multicast Boundary Filter）] ダイアログボックスを使用します。

管理スコープ マルチキャスト アドレスのマルチキャスト境界を設定できます。マルチキャスト境界により、マルチキャスト データ パケット フローが制限され、同じマルチキャスト グループ アドレスを複数の管理ドメインで再利用できるようになります。インターフェイスに対してマルチキャスト境界が定義されている場合、フィルタ ACL により許可されたマルチキャスト トラフィックだけが、そのインターフェイスを通過します。

ステップ 3 [インターフェイス（Interface）] ドロップダウン リストから、マルチキャスト境界フィルタ ACL を設定するインターフェイスを選択します。

ステップ 4 [標準アクセス リスト（Standard Access List）] ドロップダウン リストから、使用する標準 ACL を選択するか、追加アイコン（  ）をクリックして新しい標準 ACL を作成します。手順については、標準 ACL オブジェクトの設定 （612 ページ）を参照してください。

ステップ 5 境界 ACL によって拒否されたソースからの Auto-RP メッセージをフィルタするには、[境界によって拒否された Auto-RP パケットからの Auto-RP グループ範囲通知の削除（Remove any Auto-RP group range announcement from the Auto-RP packets that are denied by the boundary）] チェックボックスをオンにします。このチェックボックスをオンにしていない場合、すべての Auto-RP メッセージが通過します。

ステップ 6 [OK] をクリックして、マルチキャスト境界フィルタの設定を保存します。

第 XI 部

Firepower Threat Defense の VPN

第 42 章

Firepower Threat Defense の VPN の概要

バーチャルプライベートネットワーク（VPN）接続は、インターネットなどのパブリック ネットワークを介してエンドポイント間の安全なトンネルを確立します。

この章は、Firepower Threat Defense デバイス上のリモート アクセスおよびサイト間 VPN に適用されます。サイト間およびリモートアクセス VPN の構築に使用される Internet Protocol Security（IPsec）、Internet Security Association and Key Management Protocol（ISAKMP、または IKE）および SSL 規格について説明します。

Firepower Management Center でゲートウェイ VPN または Firepower VPN と呼ばれる、7000 および 8000 シリーズ デバイス上のサイト間 VPN については ゲートウェイ VPN （1643 ページ）で説明しています。

VPN タイプ

Firepower Management Center は次のタイプの VPN 接続をサポートします。

- Firepower Threat Defense デバイス上のリモート アクセス VPN。

  リモート アクセス VPN は、リモート ユーザと会社のプライベート ネットワーク間のセキュアな暗号化接続、またはトンネルです。接続は、社内のプライベートネットワークのエッジにある、VPN クライアント機能を備えたワークステーションやモバイル デバイスである VPN エンドポイントデバイス、VPN ヘッドエンドデバイス、またはセキュア ゲートウェイで構成されます。

  Firepower Threat Defense デバイスは SSL 経由のリモート アクセス VPN または Firepower Management Center による IPsec IKEv2 をサポートするように設定できます。このデバイスは、この容量でセキュアなゲートウェイとして機能して、リモートユーザを認証し、アクセスを許可し、データを暗号化してネットワークへのセキュアな接続を提供します。

Firepower Management Center によって管理されるその他のタイプのアプライアンスは、リモート アクセス VPN 接続をサポートしていません。

Firepower Threat Defense セキュア ゲートウェイは、AnyConnect Secure Mobility Client[AnyConnectSecureMobilityClient] の完全なトンネル クライアントをサポートしています。このクライアントは、リモート ユーザにセキュアな SSL IPsec IKEv2 接続を提供するために必要です。接続時にクライアントプラットフォームに展開できるため、このクライアントにより、ネットワーク管理者がリモート コンピュータにクライアントをインストールして設定しなくても、リモートユーザはクライアントを活用できます。これは、エンドポイント デバイスでサポートされている唯一のクライアントです。

- Firepower Threat Defense デバイス上のサイト間 VPN。

  サイト間 VPN は、地理的に異なる場所にあるネットワークを接続します。管理対象デバイス間、および管理対象デバイスと関連するすべての規格に準拠するその他のシスコまたはサードパーティのピアとの間で、サイト間IPsec接続を作成できます。これらのピアは、IPv4 アドレスと IPv6 アドレスの内部と外部の任意の組み合わせを持つことができます。サイト間トンネルは、Internet Protocol Security（IPsec）プロトコル スイートと IKEv1 または IKEv2 を使用して構築されます。VPN 接続が確立されると、ローカル ゲートウェイの背後にあるホストはセキュアな VPN トンネルを介して、リモート ゲートウェイの背後にあるホストに接続することができます。

- 7000 および 8000 シリーズ デバイス上のサイト間 VPN。

  これらのサイト間 VPN は、Firepower Management Center 内でゲートウェイ VPN または Firepower VPN と呼ばれます。このタイプの VPN 接続については、ゲートウェイ VPN （1643 ページ） を参照してください。

VPN の基本

トンネリングによって、インターネットなどのパブリック TCP/IP ネットワークの使用が可能となり、リモートユーザとプライベート企業ネットワークとの間でセキュアな接続を作成できます。各セキュアな接続がトンネルと呼ばれます。

IPsec ベースの VPN テクノロジーでは、Internet Security Association and Key Management Protocol（ISAKMP または IKE）と IPsec トンネリングを使用して、トンネルを構築し管理します。ISAKMP と IPsec は、次を実現します。

- トンネル パラメータのネゴシエート。
- トンネルの確立。
- ユーザとデータの認証。
- セキュリティ キーの管理。
- データの暗号化と復号。
- トンネルを経由するデータ転送の管理。

- トンネルエンドポイントまたはルータとしてのインバウンドおよびアウトバウンドのデータ転送の管理。

VPN 内のデバイスは、双方向トンネル エンドポイントとして機能します。プライベート ネットワークからプレーンパケットを受信してカプセル化し、トンネルを作成して、カプセル化したパケットをトンネルのもう一方の終端に送信します。トンネルの終端では、パケットのカプセル化が解除されて最終的な宛先に送信されます。また、カプセル化されたパケットをパブリック ネットワークから受信してカプセル化を解除し、プライベート ネットワーク上の最終的な宛先に送信します。

サイト間 VPN 接続が確立された後、ローカル ゲートウェイの背後にあるホストは、セキュアなVPNトンネルを介してリモートゲートウェイの背後にあるホストと接続できます。接続は、2つのゲートウェイのIPアドレスとホスト名、それらの背後にあるサブネット、および2つのゲートウェイが互いを認証するために使用する方式で構成されます。

インターネット キー エクスチェンジ（IKE）

インターネットキーエクスチェンジ（IKE）は、IPsecピアを認証し、IPsec暗号化キーをネゴシエートして配信し、IPsecセキュリティアソシエーション（SA）を自動的に確立するために使用されるキー管理プロトコルです。

IKEネゴシエーションは2つのフェーズで構成されています。フェーズ1では、2つのIKEピア間のセキュリティアソシエーションをネゴシエートします。これにより、ピアはフェーズ2で安全に通信できるようになります。フェーズ2のネゴシエーションでは、IKEによってIPsecなどの他のアプリケーション用のSAが確立されます。両方のフェーズで接続のネゴシエーション時にプロポーザルが使用されます。

IKEポリシーは、2つのピアが、ピア間のIKEネゴシエーションの安全性を確保するために使用する一連のアルゴリズムです。IKEネゴシエーションは、共通（共有）IKEポリシーに合意している各ピアによって開始されます。このポリシーは、どのセキュリティパラメータが後続のIKEネゴシエーションを保護するかを規定します。IKEバージョン1（IKEv1）の場合、IKEポリシーには単一セットのアルゴリズムとモジュラスグループが含まれます。IKEv1とは異なり、IKEv2ポリシーでは、フェーズ1ネゴシエーション中にピアがその中から選択できるように、複数のアルゴリズムとモジュラス グループを選択できます。単一のIKEポリシーを作成できますが、最も必要なオプションにより高い優先順位をつけるために異なるポリシーが必要となる場合もあります。サイト間VPNの場合は、単一のIKEポリシーを作成できます。

IKEポリシーを定義するには、次を指定します。

- 固有の優先順位（1 ～ 65,543、1 が最高の優先順位）。
- データを保護し、プライバシーを確保するための IKE ネゴシエーションの暗号化方式。
- 送信者のIDを保証し、メッセージが伝送中に変更されないように確保するためのハッシュメッセージ認証コード（HMAC）方式（IKEv2 では整合性アルゴリズムと呼ばれる）。
- IKEv2 の場合、IKEv2 トンネル暗号化に必要なキーの材料とハッシュ操作を派生させるためのアルゴリズムとして使用される個別の擬似乱関数（PRF）。オプションは、ハッシュアルゴリズムで使用されているものと同じです。

- 暗号化キー判別アルゴリズムの強度を決定する Diffie-Hellman グループ。デバイスは、このアルゴリズムを使用して、暗号化キーとハッシュ キーを派生させます。
- ピアの ID を保証するための認証方式。
- デバイスが暗号化キーを交換するまでに使用できる時間制限。

IKE ネゴシエーションが開始すると、ネゴシエーションを開始するピアはリモート ピアにすべてのポリシーを送信し、リモート ピアは優先順位順に自身のポリシーとの一致を検索します。ピアが、暗号化、ハッシュ（IKEv2 の場合は整合性と PRF）、認証、Diffie-Hellman 値を保持し、さらに、送信されたポリシーのライフタイム以下である SA ライフタイムを保持している場合に、IKE ポリシー間に一致が存在します。ライフタイムが同じでない場合は、リモート ピア ポリシーの短い方のライフタイムが適用されます。デフォルトでは、Firepower Management Center は、正常なネゴシエーションを確保するために、すべての VPN エンドポイントに対して IKEv1 ポリシーを最低優先順位で展開します。

IPsec

IPsec は、VPN を設定する場合の最も安全な方法の 1 つです。IPsec では、IP パケット レベルでのデータ暗号化が提供され、標準規格に準拠した堅牢なセキュリティ ソリューションが提供されます。IPsec では、データはトンネルを介してパブリック ネットワーク経由で送信されます。トンネルとは、2 つのピア間のセキュアで論理的な通信パスです。IPSec トンネルを通過するトラフィックは、セキュリティ プロトコルとアルゴリズムの組み合わせによって保護されます。

IPsec プロポーザル ポリシーは、IPsec トンネルに必要な設定を定義します。IPsec プロポーザルとは、デバイスの VPN インターフェイスに適用される 1 つ以上の暗号マップの集合です。暗号マップには、IPsec セキュリティ アソシエーションを設定するために必要なすべてのコンポーネントが組み合わされています。これらのコンポーネントには以下のものがあります。

- プロポーザル（またはトランスフォーム セット）とは、IPsec トンネル内のトラフィックを保護するためのセキュリティ プロトコルおよびアルゴリズムの組み合わせです。IPsec セキュリティ アソシエーション（SA）ネゴシエーション中に、ピアでは、両方のピアに共通するプロポーザルが検索されます。そのようなプロポーザルが検出されると、そのプロポーザルを適用して、その暗号マップのアクセス リストでデータ フローを保護する SA が作成され、VPN でトラフィックが保護されます。IKEv1 と IKEv2 には別個の IPsec プロポーザルがあります。IKEv1 プロポーザル（トランスフォーム セット）では、パラメータごとに 1 つの値を設定します。IKEv2 プロポーザルでは、単一のプロポーザルに複数の暗号化アルゴリズムと統合アルゴリズムを設定できます。
- 暗号マップには、IPsec ルール、プロポーザル、リモート ピア、IPsec SA を定義するために必要なその他のパラメータを含む、IPsec セキュリティ アソシエーション（SA）を設定するために必要なすべてのコンポーネントが組み合わされています。2 つのピアが SA を確立しようとする場合は、それぞれに少なくとも 1 つの互換暗号マップ エントリが必要です。

  不明なリモート ピアがローカル ハブとの間の IPsec セキュリティ アソシエーションの開始を試みた場合、ダイナミック暗号マップ ポリシーがサイト間 VPN で使用されます。ハ

ブは、セキュリティ アソシエーション ネゴシエーションを開始できません。ダイナミック暗号ポリシーを使用することによって、ハブがリモート ピアのアイデンティティを把握していない場合でも、リモート ピアはローカル ハブとの間で IPsec トラフィックを交換できます。実質的には、ダイナミック暗号マップ ポリシーによって、すべてのパラメータが設定されていない暗号マップ エントリが作成されます。設定されていないパラメータは、IPsec ネゴシエーションの結果として、リモート ピアの要件に合うようにあとで動的に設定されます。

ダイナミック暗号マップ ポリシーは、ハブアンドスポークとポイントツーポイント VPN トポロジの両方に適用されます。ダイナミック暗号マップ ポリシーを適用するには、トポロジ内のピアの 1 つにダイナミック IP アドレスを指定し、このトポロジでダイナミック暗号マップが有効になっていることを確認します。フル メッシュ VPN トポロジでは、スタティック クリプト マップ ポリシーのみを適用できます。

VPN パケット フロー

FTD デバイスでは、デフォルトでは、明示的な許可なしにいずれのトラフィックもアクセス コントロールを通過できません。VPN トンネル トラフィックも、Snort を通過するまでは、エンドポイントにリレーされません。着信トンネル パケットは復号されてから、Snort プロセスへ送信されます。Snort は、暗号化の前に発信パケットを処理します。

VPN トンネルのエンドポイント ノードごとに保護されたネットワークを識別するアクセス制御は、どのトラフィックが FTD デバイスをパス スルーしてエンドポイントに到達できるかを決定します。リモート アクセス VPN トラフィックでは、グループ ポリシー フィルタまたはアクセス制御ルールを、VPN トラフィック フローを許可するように設定する必要があります。

さらに、システムは、トンネルがダウンしている場合は、トンネル トラフィックをパブリックなソースに送信しません。

VPN ライセンス

Firepower Threat Defense VPN を有効にするための特別なライセンスはありません。デフォルトで利用可能です。

Firepower Management Center は、スマート ライセンス サーバから提供される属性に基づいて、Firepower Threat Defense デバイスで強力な暗号の使用を許可するかブロックするかを決定します。

これは、Cisco Smart License Manager に登録するときにデバイス上で輸出管理機能を許可するオプションを選択しているかどうかによって制御されます。評価ライセンスを使用している場合、または輸出管理機能を有効にしていない場合は、強力な暗号化を使用できません。

VPN 接続の安全性を確保する方法

VPN トンネルは通常、インターネットなどのパブリック ネットワークを経由するため、トラフィックを保護するために接続を暗号化する必要があります。IKE ポリシーと IPsec プロポーサルを使用して、暗号化とその他のセキュリティ技術を定義し、適用します。

デバイス ライセンスによって強力な暗号化を適用できる場合は、広範な暗号化とハッシュ アルゴリズム、および Diffie-Hellman グループがあり、その中から選択できます。ただし、一般に、トンネルに適用する暗号化が強力なほど、システム パフォーマンスは低下します。効率を損なうことなく十分な保護を提供するセキュリティとパフォーマンスのバランスを見出します。

シスコでは、どのオプションを選択するかについての特定のガイダンスは提供できません。比較的大規模な企業またはその他の組織内で運用している場合は、すでに、満たす必要がある標準が定義されている可能性があります。定義されていない場合は、時間を割いてオプションを調べてください。

以降のトピックでは、使用可能なオプションについて説明します。

セキュリティ証明書要件の遵守

多数の VPN 設定には、さまざまなセキュリティ認証規格に準拠するためのオプションがあります。認定要件と使用可能なオプションを確認して、VPN構成を計画します。コンプライアンスに関連する追加のシステム情報については、セキュリティ認定準拠（1411ページ）を参照してください。

使用する暗号化アルゴリズムの決定

IKE ポリシーまたは IPsec プロポーザルに使用する暗号化アルゴリズムを決定する際、選択肢は VPN のデバイスでサポートされるアルゴリズムに限られます。

IKEv2 では、複数の暗号化アルゴリズムを設定できます。システムは、設定をセキュア度が最も高いものから最も低いものに並べ替え、その順序を使用してピアとのネゴシエーションを行います。IKEv1 では、単一のオプションのみ選択できます。

IPsec プロポーザルでは、認証、暗号化、およびアンチリプレイ サービスを提供するカプセル化セキュリティ プロトコル（ESP）によってアルゴリズムが使用されます。ESP は、IP プロトコル タイプ 50 です。IKEv1 IPsec プロポーザルでは、アルゴリズム名の前に ESP というプレフィックスが付けられます。

デバイス ライセンスが強力な暗号化を適用できる場合、次の暗号化アルゴリズムを選択できます。強力な暗号化の対象ではない場合、DES のみ選択できます。

- AES-GCM—（IKEv2 のみ）Galois/カウンタ モードの Advanced Encryption Standard は、機密性、データの発信元の認証を提供する操作のブロック暗号モードであり、AES よりも優れたセキュリティを提供します。AES-GCM には、128 ビット、192 ビット、256 ビットの 3 種類のキー強度が用意されています。キーが長いほど安全になりますが、パフォーマン

スは低下します。GCM は NSA Suite B をサポートするために必要となる AES モードです。NSA Suite B は、暗号化強度に関する連邦標準規格を満たすためにデバイスがサポートすべき一連の暗号化アルゴリズムです。.

- AES-GMAC—（IKEv2 IPsec プロポーザルのみ）。Advanced Encryption Standard のガロアメッセージ認証コード（GMAC）は、データ発信元認証だけを行う操作のブロック暗号モードです。これは AES-GCM の一種であり、データを暗号化せずにデータ認証が行えます。AES-GMAC には、128 ビット、192 ビット、256 ビットの 3 種類のキー強度が用意されています。
- AES（Advanced Encryption Standard）は DES よりも高度なセキュリティを提供する対称暗号化アルゴリズムであり、計算的には 3DES よりも効率的です。AES には、128 ビット、192 ビット、256 ビットの 3 種類のキー強度が用意されています。キーが長いほど安全になりますが、パフォーマンスは低下します。
- 3DES（トリプル DES）：56 ビット キーを使用して暗号化を 3 回行います。異なるキーを使用してデータの各ブロックを 3 回処理するため、DES よりも安全です。ただし、使用するシステム リソースが多くなり、DES よりも速度が遅くなります。
- DES（データ暗号化標準）：56 ビット キーを使用して暗号化する対称秘密鍵ブロック アルゴリズムです。ライセンスアカウントが輸出規制の要件を満たしていない場合、これは唯一のオプションです。3DES よりも高速であり、使用するシステム リソースも少ないですが、安全性も劣ります。堅牢なデータ機密保持が必要ない場合、およびシステム リソースや速度が重要である場合には、DES を選択します。
- Null：ヌル暗号化アルゴリズムは暗号化なしで認証します。通常はテスト目的にのみ使用されます。

使用するハッシュ アルゴリズムの決定

IKE ポリシーでは、ハッシュ アルゴリズムがメッセージ ダイジェストを作成します。これは、メッセージの整合性を保証するために使用されます。IKEv2 では、ハッシュ アルゴリズムは 2 つのオプションに分かれています。1 つは整合性アルゴリズムに使用され、もう 1 つは擬似乱数関数（PRF）に使用されます。

IPsec プロポーザルでは、ハッシュ アルゴリズムはカプセル化セキュリティ プロトコル（ESP）による認証のために使用されます。IKEv2 IPsec プロポーザルでは、これは整合性のハッシュと呼ばれます。IKEv1 IPsec プロポーザルでは、アルゴリズム名に ESP というプレフィックスだけでなく HMAC というサフィックスも付けられます（ハッシュ方式認証コードを意味する）。

IKEv2 では、複数のハッシュ アルゴリズムを設定できます。システムは、設定をセキュア度が最も高いものから最も低いものに並べ替え、その順序を使用してピアとのネゴシエーションを行います。IKEv1 では、単一のオプションのみ選択できます。

選択可能なハッシュ アルゴリズムは、次のとおりです。

- [SHA（Secure Hash Algorithm）]：標準 SHA（SHAI）が 160 ビットのダイジェストを生成します。SHA には、総当たり攻撃に対して、MD5 よりも高い耐性が備えられています。

ただし、SHA は MD5 よりもリソース消費量が大きくなります。最大レベルのセキュリティを必要とする実装には、SHA ハッシュ アルゴリズムを使用してください。

IKEv2 の設定では、以下の SHA-2 オプションを指定して、より高度なセキュリティを実現できます。NSA Suite B 暗号化仕様を実装するには、次のいずれかを選択します。

- SHA256：256 ビットのダイジェストを生成するセキュア ハッシュ アルゴリズム SHA 2 を指定します。
- SHA384：384 ビットのダイジェストを生成するセキュア ハッシュ アルゴリズム SHA 2 を指定します。
- SHA512：512 ビットのダイジェストを生成するセキュア ハッシュ アルゴリズム SHA 2 を指定します。

- MD5 (Message Digest 5)：128 ビットのダイジェストを生成します。MD5 は処理時間が短いため、全体的なパフォーマンスが SHA より高速ですが、SHA より強度は低いと考えられています。
- NULL またはなし（NULL、ESP-NONE）：（IPsec プロポーザルのみ）NULL ハッシュ アルゴリズム。通常はテスト目的のみに使用されます。ただし、暗号化アルゴリズムとして AES-GCM/GMAC オプションのいずれかを選択した場合は、ヌル整合性アルゴリズムを選択する必要があります。NULL 以外のオプションを選択した場合、これらの暗号化標準に対しては、整合性ハッシュは無視されます。

使用する Diffie-Hellman 係数グループの決定

次の Diffie-Hellman キー導出アルゴリズムを使用して、IPsec Security Association（SA：セキュリティ アソシエーション）キーを生成することができます。各グループでは、異なるサイズの係数が使用されます。係数が大きいほどセキュリティが強化されますが、処理時間が長くなります。両方のピアに、一致する係数グループが存在する必要があります。

AES 暗号化を選択する場合は、AES で必要な大きいキー サイズをサポートするために、Diffie-Hellman（DH：デフィーヘルマン）グループ 5 以降を使用する必要があります。IKEv1 ポリシーは、以下にリストされているすべてのグループをサポートしていません。

NSA Suite-B の暗号化の仕様を実装するには、IKEv2 を使用して楕円曲線 Diffie-Hellman（ECDH）オプション：19、20、21 のいずれか 1 つを選択します。楕円曲線オプションと、2048 ビット係数を使用するグループは、Logjam のような攻撃にさらされる可能性が低くなります。

IKEv2 では、複数のグループを設定できます。システムは、設定をセキュア度が最も高いものから最も低いものに並べ替え、その順序を使用してピアとのネゴシエーションを行います。IKEv1 では、単一のオプションのみ選択できます。

- 2：Diffie-Hellman グループ 2（1024 ビット Modular Exponential（MODP）グループ）。このオプションは優れた保護とは見なされなくなりました。

- 5：Diffie-Hellman グループ 5（1536 ビット MODP グループ）。以前は 128 ビット キーに対する優れた保護と見なされていましたが、このオプションは優れた保護と見なされなくなりました。
- 14：Diffie-Hellman グループ 14（2048 ビット Modular Exponential（MODP）グループ）。192 ビットのキーでは十分な保護レベルです。
- 19：Diffie-Hellman グループ 19（国立標準技術研究所（NIST）256 ビット楕円曲線モジュロ プライム（ECP）グループ）。
- 20：Diffie-Hellman グループ 20（NIST 384 ビット ECP グループ）。
- 21：Diffie-Hellman グループ 21（NIST 521 ビット ECP グループ）。
- 24：Diffie-Hellman グループ 24（2048 ビット MODP グループおよび 256 素数位数サブグループ）。このオプションは推奨されなくなりました。

使用する認証方式の決定

事前共有キーとデジタル証明書は、VPN で使用可能な認証方法です。

サイト間、IKEv1 および IKEv2 VPN 接続では、両方のオプションを使用できます。

SSL および IPsec IKEv2 のみを使用するリモート アクセスでは、デジタル証明書認証だけがサポートされます。

事前共有キーを使用すると、秘密鍵を2つのピア間で共有したり、認証フェーズ中にIKEで使用したりできます。各ピアに同じ共有キーを設定する必要があります。同じキーが設定されていない場合は、IKE SA を確立できません。

デジタル証明書は IKE キー管理メッセージの署名や暗号化に RSA キー ペアを使用します。証明書によって、2 つのピア間の通信の否認防止を実施します。つまり、実際に通信が行われたことを証明できます。この認証方式を使用する場合、ピアが証明機関（CA）からデジタル証明書を取得できるように Public Key Infrastructure（PKI）を定義する必要があります。CA は参加するネットワーク デバイスの証明書要求を管理し、証明書の発行を行うことで、すべての参加デバイスの Centralized Key Management を行っています。

事前共有キーの拡張性は高くありませんが、CA を使用することによって IPsec ネットワークの管理性や拡張性が高まります。CA を使用する場合は、すべての暗号化デバイス間でキーを設定する必要がありません。代わりに、参加する各デバイスは CA に登録され、CA に対して証明書を要求します。自身の証明書と CA の公開キーを持つ各デバイスは、その CA のドメイン内にある他のすべてのデバイスを認証できます。

事前共有キー

事前共有キーにより、秘密キーを2つのピアの間で共有できます。このキーは、認証フェーズでIKEが使用します。各ピアに同じ共有キーを設定する必要があります。同じキーが設定されていなければ、IKE SA を確立できません。

事前共有キーを設定するには、手動または自動生成されたキーを使用するかどうかを選択し、IKEv1/IKEv2 オプションでキーを指定します。これにより、設定の展開時に、トポロジ内のすべてのデバイス上に共有キーが設定されます。

PKI インフラストラクチャとデジタル証明書

公開キー インフラストラクチャ

PKI では、参加ネットワーク デバイスのキーを一元管理できます。PKI は、一般にデジタル証明書 と呼ばれる公開キー証明書 を生成、検証、失効することで公開キー暗号化 をサポートするポリシー、プロシージャ、権限の定義済みセットです。

公開キー暗号化では、接続の各エンドポイントが公開キーと秘密キーの両方からなるキー ペアを保持します。キー ペアは、VPN エンドポイントがメッセージに署名して暗号化するために使用します。これらのキーは相互に補完し合い、一方のキーで暗号化されたものはもう一方のキーでしか復号できません。この仕組みにより、接続で送受信されるデータを保護します。

署名と暗号化の両方に使用される汎用 RSA または ECDSA キー ペアを生成するか、署名用と暗号化用に別々のキーペアを生成します。署名用と暗号化用にキーを分けると、キーが公開される頻度を少なくすることができます。SSL は署名用ではなく暗号化用にキーを使用しますが、IKEは暗号化ではなく署名にキーを使用します。キーを用途別に分けることで、キーの公開頻度が最小化されます。

デジタル証明書

デジタル証明書を VPN 接続の認方式として使用する場合、ピアはデジタル証明書を認証局（CA）から取得するように設定されます。CAは、証明書に「署名」してその認証を確認することで、デバイスまたはユーザのアイデンティティを保証する、信頼できる機関です。

CA サーバは公開 CA 証明書要求を管理し、参加ネットワーク デバイスに公開キー インフラストラクチャ（PKI）の一部として証明書を発行します。このアクティビティは、証明書の登録と呼ばれます。これらのデジタル証明書は、アイデンティティ証明書とも呼ばれています。デジタル証明書の内容は以下のとおりです。

- 認証のための所有者のデジタル識別（名前、シリアル番号、会社、部署、IP アドレスなど）。
- 証明書所有者に対して暗号化データを送受信するために必要な公開キー。
- CA のセキュアなデジタル署名。

また、証明書によって、2 つのピア間の通信の否認が防止されます。つまり、実際に通信が行われたことを証明できます。

証明書の登録

PKI を使用すると、すべての暗号化デバイス間で事前に共有するキーを設定する必要がなくなるため、VPNをもっと容易に管理できるようになり、スケーラビリティが高まります。代わりに、参加する各デバイスを CA サーバに個別に登録します。CA サーバは、アイデンティティを検証し、デバイスのアイデンティティ証明書を作成することを明示的に信任されています。

登録が完了すると、参加する各ピアは、もう一方の参加するピアにアイデンティティ証明書を送信し、証明書に含まれる公開キーでそのアイデンティティを検証して、暗号化セッションを確立できるようにします。FTDデバイスの登録の詳細については、証明書の登録オブジェクト（591 ページ）を参照してください。

認証局証明書

ピアの証明書を検証するには、参加デバイスのそれぞれが CA の証明書をサーバから取得する必要があります。CA 証明書は、他の証明書に署名するために使用されます。これは自己署名され、ルート証明書と呼ばれます。この証明書に含まれる CA の公開キーを使用して、CA のデジタル署名および受信したピアの証明書の内容を復号して検証します。CA 証明書は次の方法で取得可能です。

- Simple Certificate Enrollment Protocol（SCEP）を使用して、CA サーバから CA の証明書を取得します。
- 別の参加デバイスから CA の証明書を手動でコピーします。

トラストポイント

登録が完了すると、管理対象デバイス上にトラストポイントが作成されます。トラストポイントは、CAおよび関連する証明書を表すオブジェクトです。トラストポイントには、CAのID、CA 固有のパラメータ、単一の登録済みアイデンティティ証明書とのアソシエーションが含まれています。

PKCS#12 ファイル

PKCS#12（PFX）ファイルとは、サーバ証明書、中間証明書、秘密キーのすべてを暗号化して保持するファイルです。このタイプのファイルをデバイスに直接インポートして、トラストポイントを作成できます。

失効チェック

さらにCAは、ネットワークに参加しなくなったピアの証明書を無効にすることもできます。失効した証明書は、オンライン証明書ステータス プロトコル（OCSP）サーバによって管理されるか、LDAP サーバに格納されている証明書失効リスト（CRL）に含まれます。ピアは、別のピアからの証明書を受け入れる前に、これらを検査できます。

VPN トポロジ オプション

新しいVPNトポロジを作成するには、最低でも、固有の名前をつけ、トポロジの型を特定し、IKE バージョンを選択する必要があります。それぞれが VPN トンネル グループを含む 3 つの型のトポロジから選択できます。

- ポイントツーポイント（PTP）トポロジでは、2 つのエンドポイント間に VPN トンネルを確立します。

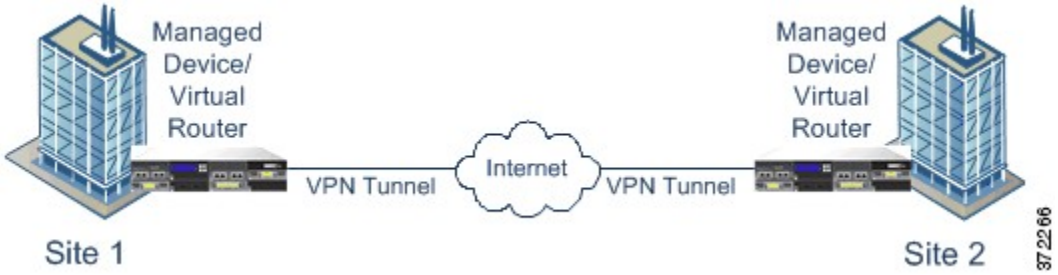
- ハブおよびスポーク トポロジは、ハブ エンドポイントをスポーク エンドポイントのグループに接続する VPN トンネル グループを確立します。
- フル メッシュのトポロジは、エンドポイントのセットの間で VPN トンネルのグループを確立します。

VPN認証の事前共有キーを手動または自動で定義します。デフォルトのキーはありません。自動を選択すると、Firepower Management Center は事前共有キーを生成して、そのキーをトポロジ内のすべてのノードに割り当てます。

ポイントツーポイントの VPN トポロジ

ポイントツーポイントのVPNトポロジでは、2つのエンドポイントが相互に直接通信します。2つのエンドポイントをピア デバイスとして設定し、いずれかのデバイスでセキュアな接続を開始することができます。

次の図は、一般的なポイントツーポイントの VPN トポロジを示しています。

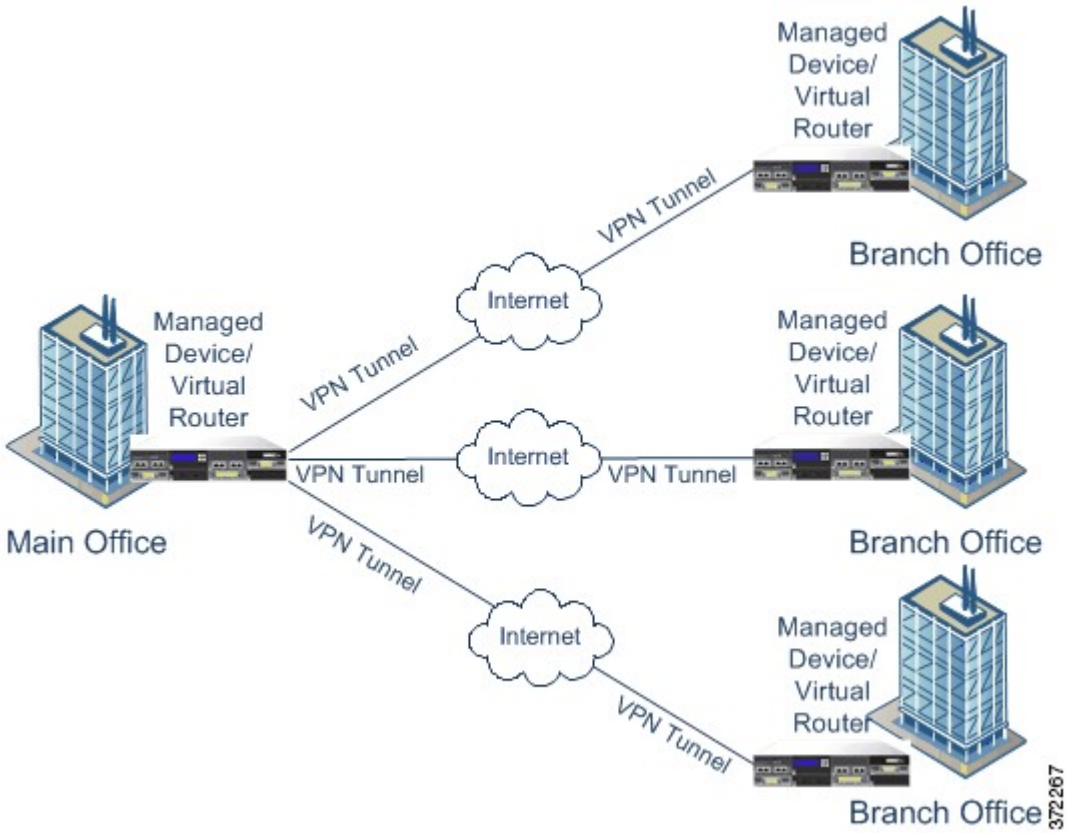


ハブ アンド スポーク VPN トポロジ

ハブ アンド スポーク VPN トポロジでは、中央のエンドポイント（ハブ ノード）が複数のエンドポイント（スポーク ノード）と接続します。ハブ ノードと個々のスポーク エンドポイント間のそれぞれの接続は、別の VPN トンネルです。いずれかのスポーク ノードの背後にあるホストは、ハブ ノードを介して互いに通信できます。

ハブ アンド スポーク トポロジは一般的に、インターネットや他のサードパーティのネットワークを介してセキュアな接続を使用している組織の本社とブランチ オフィスを接続する VPN を表します。これらの展開は、すべての従業員に対して、組織のネットワークへのコントロールされたアクセスを提供します。一般的に、ハブ ノードは本社に配置します。スポーク ノードはブランチ オフィスに配置し、大半のトラフィックはここから開始されます。

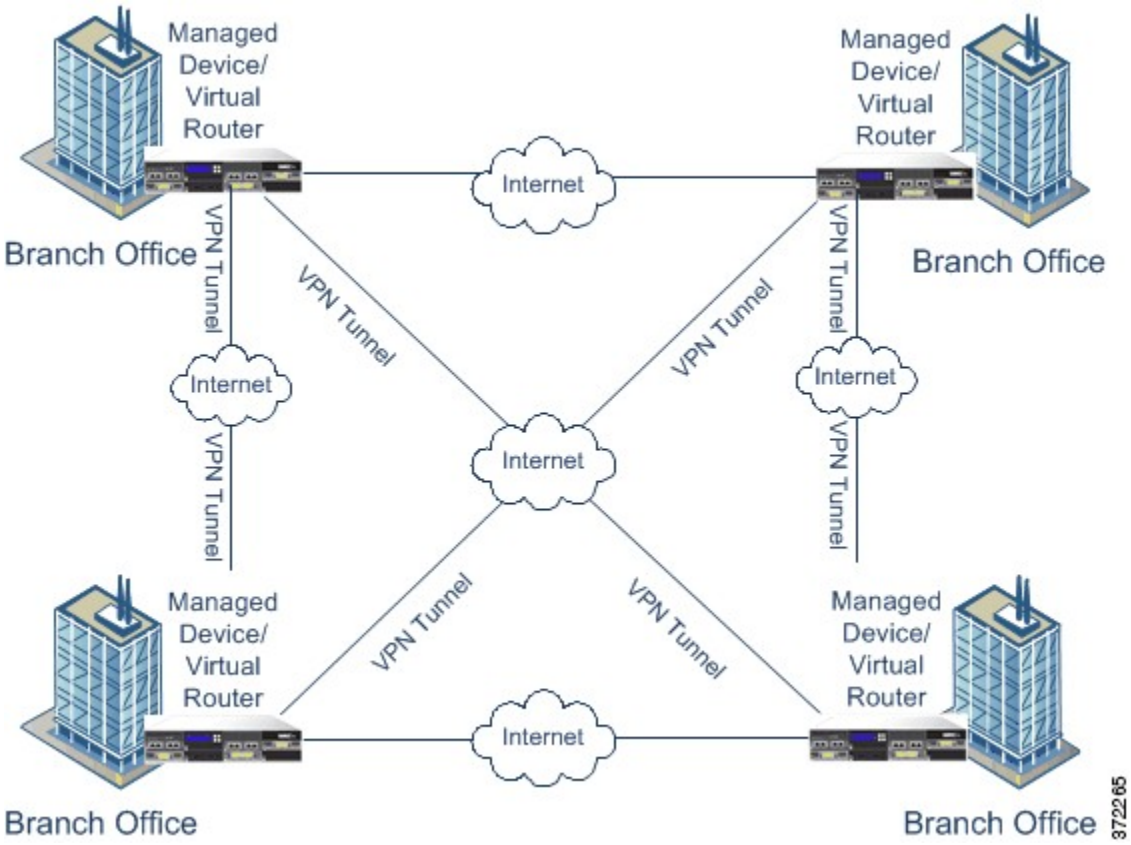
次の図は、一般的なハブ アンド スポーク VPN トポロジを示しています。



フル メッシュ VPN トポロジ

フル メッシュ VPN トポロジでは、すべてのエンドポイントが個々の VPN トンネルによって他のエンドポイントと通信できます。このトポロジにより、あるエンドポイントで障害が発生しても、残りのエンドポイントの相互通信は維持されるように冗長性が提供されます。これは、一般的に分散したブランチ オフィスが配置されたグループを接続する VPN を表します。この設定で展開する VPN 対応の管理対象デバイスの数は、必要な冗長性のレベルによって異なります。

次の図は、一般的なフル メッシュ VPN トポロジを示しています。



暗黙的トポロジ

3つの主要なVPNトポロジに加えて、これらのトポロジを組み合わせた他のより複雑なトポロジを作成することもできます。具体的には以下のとおりです。

- 部分メッシュ：このネットワークでは、一部のデバイスはフル メッシュ トポロジに編成され、その他のデバイスは、フル メッシュ構成のデバイスのうちのいくつかとのハブアンドスポーク接続またはポイントツーポイント接続を形成します。部分メッシュには、フル メッシュ トポロジほどの冗長性はありませんが、導入コストがより低くなります。部分メッシュ トポロジは、フル メッシュ構成のバックボーンに接続するペリフェラル ネットワークで使用されます。
- 階層型ハブアンドスポーク：このネットワークでは、あるデバイスが、1 つ以上のトポロジでハブとして動作し、他のトポロジではスパイクとして動作できます。スポーク グループからそれらの直近のハブへのトラフィックが許可されます。
- 結合ハブアンドスポーク：接続して 1 つのポイントツーポイント トンネルを形成する、2 つのトポロジ（ハブアンドスポーク、ポイントツーポイント、またはフル メッシュ）の組み合わせです。たとえば、2 つのハブアンドスポーク トポロジから構成され、それぞれのハブがポイントツーポイント トポロジのピア デバイスとして動作する結合ハブアンドスポーク トポロジを作成できます。

第 43 章

のサイト間 VPN Firepower Threat Defense

Firepower Threat Defense サイト間 VPN について

Firepower Threat Defense サイト間 VPN では、次の機能がサポートされています。

- IPsec IKEv1 および IKEv2 プロトコルの両方をサポート。
- 証明書および自動または手動の事前共有認証キー。
- IPv4 および IPv6。内部、外部のすべての組み合わせをサポート。
- IPsec IKEv2 サイト間 VPN トポロジは、セキュリティ認証に準拠するための構成時の設定を提供します。
- スタティック インターフェイスおよびダイナミック インターフェイス。
- Firepower Management Center および FTD 両方の HA 環境をサポート。
- トンネルがダウンした際の VPN アラート。
- FTD 統合 CLI により利用可能なトンネル統計。
- ポイントツーポイント エクストラネット VPN の IKEv1 バックアップ ピア設定をサポート。
- 「ハブ アンド スポーク」展開でのハブとしてエクストラネット デバイスをサポート。
- 「ポイントツーポイント」展開でのエクストラネットデバイスを使用した管理対象エンドポイント ペアリングのダイナミック IP アドレスをサポート。
- エクストラネットデバイスのダイナミック IP アドレスをエンドポイントとしてサポート。
- 「ハブ アンド スポーク」展開でのエクストラネットとしてハブをサポート。

VPN トポロジ

新しいサイト間 VPN トポロジを作成するには、少なくとも、一意の名前を付け、トポロジ タイプを指定し、IPsec IKEv1 または IKEv2 あるいはその両方に使用される IKE バージョンを選択する必要があります。また、認証方法を決定します。設定したら、Firepower Threat Defense デバイスにトポロジを展開します。Firepower Management Center は、FTD デバイスのサイト間 VPN のみ設定します。

次の 3 つのタイプのトポロジから選択することができます。トポロジには、VPN トンネルが 1 つ以上含まれています。

- ポイントツーポイント（PTP）型の展開は、2 つのエンドポイント間で VPN トンネルを確立します。
- ハブ アンド スポーク型の展開は、VPN トンネルのグループを確立し、ハブ エンドポイントをスポーク ノードのグループに接続します。
- フル メッシュ型の展開は、エンドポイントのセット内で VPN トンネルのグループを確立します。

IPsec と IKE

Firepower Management Center では、サイト間 VPN は、VPN トポロジに割り当てられた IKE ポリシーおよびIPsecプロポーザルに基づいて設定されます。ポリシーとプロポーザルはパラメータのセットであり、これらのパラメータによって、IPsec トンネル内のトラフィックでセキュリティを確保するために使用されるセキュリティ プロトコルやアルゴリズムなど、サイト間 VPN の特性が定義されます。VPN トポロジに割り当て可能な完全な設定イメージを定義するために、複数のポリシー タイプが必要となる場合があります。

認証

VPN接続の認証には、トポロジ内で事前共有キー、または各デバイスでトラストポイントを設定します。事前共有キーにより、IKE 認証フェーズで使用する秘密鍵を 2 つのピア間で共有できます。トラストポイントには、CA の ID、CA 固有のパラメータ、登録されている単一の ID 証明書とのアソシエーションが含まれています。

エクストラネット デバイス

各トポロジ タイプには、Firepower Management Center で管理しないデバイスである、エクストラネット デバイスが含まれる可能性があります。これには次が含まれます。

- Firepower Management Center ではサポートされているが、ユーザの部門が担当していないシスコ デバイス。たとえば、社内の他の部門が管理するネットワーク内のスポークや、サービス プロバイダーやパートナー ネットワークへの接続などです。
- シスコ製以外のデバイス。Firepower Management Center を使用して、シスコ製以外のデバイスに対する設定を作成したり、展開したりすることはできません。

シスコ以外のデバイス、またはFirepower Management Centerで管理されていないシスコ デバイスを VPN トポロジに「エクストラネット」デバイスとして追加します。また、各リモート デバイスの IP アドレスも指定します。

Firepower Threat Defense サイト間 VPN ガイドラインと制約事項

- 現在のドメイン内ではないエンドポイント用のエクストラネット ピアを使用してのみ、ドメイン間の VPN 接続が可能です。
- VPN トポロジをドメイン間で移動させることはできません。
- 「範囲」オプションのあるネットワーク オブジェクトは、VPN では対応していません。
- Firepower Threat Defense VPN のバックアップは、Firepower Management バックアップを使用した場合のみ行われます。
- Firepower Threat Defense VPN では、現在、PDF のエクスポートおよびポリシーの比較には対応していません。
- Firepower Threat Defense VPN ではトンネル単位またはデバイス単位の編集オプションはありません。トポロジ全体のみ編集できます。
- 暗号 ACL が選択されている場合、トランスポート モードのデバイス インターフェイス アドレス検証は実行されません。
- 暗号 ACL または保護されたネットワークのいずれかを使用して、トポロジ内のすべてのノードを設定する必要があります。あるノードでは暗号 ACL を使用し、別のノードでは保護されたネットワークを使用して、トポロジを設定することはできません。
- 自動ミラー ACE 生成はサポートされません。ピアのミラー ACE 生成は、どちらの側でも手動プロセスです。
- 暗号 ACL を使用している間はハブ、スポーク、フル メッシュのトポロジはサポートされません。ポイントツーポイント VPN のみがサポートされます。さらに、暗号 ACL では、VPN トポロジのトンネル ヘルス イベントがサポートされません。
- IKE ポート 500/4500 が使用されている場合、またはアクティブな PAT 変換がある場合は、これらのポートでサービスを開始できないため、サイト間 VPN を同じポートに設定することはできません。
- Firepower Management Center では、トンネルの状態はリアルタイムではなく、5 分間隔でアップロードされます。
- 文字"（二重引用符）は事前共有キーの一部としてサポートされていません。事前共有キーで " を使用した場合は、Firepower Threat Defense 6.30 にアップグレードした後に必ず文字を変更してください。

Firepower Threat Defense のサイト間 VPN の管理

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス（Access）
エクスポート コンプライアンス	該当なし	FTD	リーフのみ	Admin

ステップ 1 VPN の証明書認証の場合は、トラストポイントを割り当てることでデバイスを準備する必要があります。詳細については、Firepower Threat Defense Certificate ベースの認証 （641 ページ） を参照してください。

ステップ 2 **[デバイス（Devices）] > [VPN] > [サイト間（Site To Site）]** を選択して、Firepower Threat Defense のサイト間 VPN の設定と展開を管理します。次のオプションから選択します。

- 追加：新しい VPN トポロジを作成するには、**[VPN の追加（Add VPN）] > [Firepower Threat Defense デバイス（Firepower Threat Defense Device）]** をクリックして、Firepower Threat Defense サイト間 VPN の設定 （1071 ページ） の手順を実行します。

  （注） VPN トポロジは、リーフ ドメインでのみ作成できます。

- 編集：既存の VPN トポロジの設定を変更するには、編集アイコン（）をクリックします。変更は設定とほとんど同じです。前述の手順を実行してください。

  （注） トポロジタイプは、最初の保存後に編集することはできません。トポロジタイプを変更するには、トポロジを削除してから新しいものを作成します。

  2 人のユーザが同じトポロジを同時に編集**してはいけません**。ただし、Web インターフェイスでは同時編集を防止していません。

- 削除：VPN の展開を削除するには、削除アイコン（）をクリックします。
- VPN ステータスの表示：このステータスは Firepower の VPN にのみ適用されます。現時点では、FTD VPN についてはステータスが表示されません。FTD VPN のステータスを確認するには、Firepower Threat Defense の VPN モニタリング （1161 ページ） を参照してください。
- 展開：[展開（Deploy）] をクリックします（設定変更の展開 （447 ページ） を参照）。

  （注） 一部の VPN 設定は、展開時にのみ検証されます。展開が成功したことを確認してください。

Firepower Threat Defense サイト間 VPN の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス（Access）
エクスポート コンプライアンス	該当なし	FTD	リーフのみ	Admin

ステップ 1 [デバイス（Devices）] > [VPN] > [サイト間（Site To Site）]。次に、[VPN の追加（Add VPN）] > [Firepower Threat Defense デバイス（Firepower Threat Defense Device）]、または、リストされている VPN トポロジを編集します。を選択します。

ステップ 2 一意のトポロジ名を入力します。トポロジには、FTD VPN であることとトポロジタイプを示す名前を付けることをお勧めします。

ステップ 3 この VPN のネットワーク トポロジを選択します。

ステップ 4 IKE ネゴシエーション中に使用する IKE バージョンとして、[IKEv1] または [IKEv2] のいずれかを選択します。

デフォルトは [IKEv2] です。必要に応じて、いずれかまたは両方のオプションを選択します。トポロジ内のデバイスが IKEv2 をサポートしない場合は、[IKEv1] を選択します。

Ikev1 の場合は、ポイントツー ポイント エクストラネット VPN のバックアップ ピアを設定できます。詳細については、FTD VPN エンドポイント オプション （1072 ページ）を参照してください。

ステップ 5 必須: トポロジの各ノードの追加アイコン（  ）をクリックして、この VPN 展開のためのエンドポイントを追加します。

FTD VPN エンドポイント オプション （1072 ページ）の説明に従って各エンドポイント フィールドを設定します。

- ポイントツーポイントの場合は、ノード A とノード B を設定します。
- ハブ アンド スポークの場合は、ハブ ノードとスポーク ノードを設定します。
- フル メッシュの場合は、複数のノードを設定します

ステップ 6 （任意） 次の説明に従って、この展開のデフォルト以外の IKE オプションを指定します FTD VPN IKE オプション （1075 ページ）

ステップ 7 （任意） 次の説明に従って、この展開のデフォルト以外の IPsec オプションを指定します FTD VPN IPsec オプション （1077 ページ）

ステップ 8 （任意） FTD のサイト間 VPN 展開の詳細オプション （1080 ページ）の説明に従って、この展開のデフォルト以外の詳細オプションを指定します。

ステップ 9 [保存（Save）] をクリックします。
エンドポイントが構成に追加されます。

次のタスク

設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

（注） 一部の VPN 設定は、展開時にのみ検証されます。展開が成功したことを確認してください。

FTD VPN エンドポイント オプション

ナビゲーション パス

> [サイト間（Site To Site）]。その後、[VPN の追加（Add VPN）] > [Firepower Threat Defense デバイス（Firepower Threat Defense Device）]、またはリストされている VPN トポロジを編集します。[エンドポイント（Endpoint）] タブを開きます。

フィールド

Device

展開するエンドポイント ノードを選択します。

- この FTD で管理する Firepower Management Center デバイス。
- この FTD で管理する Firepower Management Center ハイ アベイラビリティ コンテナ。
- [エクストラネット（Extranet）] デバイス。この Firepower Management Center の管理対象ではない任意のデバイス（シスコまたはサードパーティ）。

デバイス名（Device Name）

エクストラネットデバイスの場合のみ、このデバイスの名前を入力します。シスコでは、管理対象ではないデバイスとして識別できるような名前を付けることを推奨します。

インターフェイス（Interface）

エンドポイントとして管理対象デバイスを選択した場合は、その管理対象デバイスのインターフェイスを選択します。

「ポイントツーポイント」展開の場合、ダイナミック インターフェイスを使用してエンドポイントを設定することもできます。ダイナミック インターフェイスを使用したエンドポイントはエクストラネットデバイスとのみペアリングできます。管理対象デバイスを持つエンドポイントとはペアリングできません。

[デバイス（Devices）] > [デバイス管理（Device Management）] > [デバイスの追加/編集（Add/Edit device）] > [インターフェイス（Interfaces）] でデバイスのインターフェイスを設定できます。

IP Address

- Firepower Management Center の管理対象デバイス**ではない**エクストラネット デバイスを選択した場合は、エンドポイントの IP アドレスを指定します。

エクストラネット デバイスの場合は、[スタティック（Static）] を選択して IP アドレスを指定するか、または[ダイナミック（Dynamic）] を選択してダイナミック エクストラネット デバイスを許可します。

ポイントツーポイント トポロジーと IKEv1 のみを選択した場合は、プライマリ IP アドレスとバックアップ ピアの IP アドレスをカンマで区切って入力することでバックアップ ピアを設定できます。

- エンドポイントとして管理対象デバイスを選択した場合は、ドロップダウン リストから 1 つの IPv4 アドレスまたは複数の IPv6 アドレスを選択します（これらはすでにこの管理対象デバイスのこのインターフェイスに割り当てられているアドレスです）。
- トポロジ内のすべてのエンドポイントは、同じ IP アドレッシング方式でなければなりません。IPv4 トンネルは IPv6 トラフィックを伝送でき、逆もまた同様です。保護ネットワークでは、トンネルするトラフィックで使用するアドレッシング方式が定義されます。
- 管理対象デバイスがハイ アベイラビリティ コンテナである場合は、インターフェイスのリストから選択します。

この IP はプライベートです（This IP is Private）

エンドポイントが、ネットワーク アドレス変換（NAT）を備えたファイアウォールの背後に配置されている場合は、このチェックボックスをオンにします。

パブリック IP アドレス（Public IP address）

[この IP はプライベートです（This IP is Private）] チェックボックスがオンの場合は、ファイアウォールのパブリック IP アドレスを指定します。エンドポイントがレスポンダの場合は、この値を指定します。

接続タイプ（Connection Type）

許可されるネゴシエーションを、bidirectional、answer-only、または originate-only として指定します。接続タイプのサポートされる組み合わせは次のとおりです。

表 *82 :* 接続タイプのサポートされる組み合わせ

リモート ノード	中央ノード
Originate-Only	Answer-Only
Bi-Directional	Answer-Only
Bi-Directional	Bi-Directional

証明書マップ

事前構成された証明書マップ オブジェクトを選択するか、受信したクライアント証明書に必要な情報が VPN 接続に有効であることを定義する証明書マップ オブジェクトを追加アイコン（  ）をクリックして追加します。詳細については、「FTD 証明書のマップ オブジェクトについて （632 ページ）」を参照してください。

保護されたネットワーク（Protected Networks）

この VPN エンドポイントによって保護されるネットワークを定義します。このエンドポイントによって保護されるネットワークを定義するサブネット/IP アドレスのリストを選択することで、ネットワークにマークを付けることができます。追加アイコン（  ）をクリックして、使用可能なネットワーク オブジェクトから選択するか、新しいネットワーク オブジェクトを追加します。ネットワーク オブジェクトの作成（527 ページ）を参照してください。アクセス コントロール リストがここで選択されたものから生成されます。

- [サブネット/IP アドレス（ネットワーク）（Subnet/IP Address (Network)）]：VPN エンドポイントは同じ IP アドレスを持つことはできません。また、VPN エンドポイント ペアの保護されたネットワークは重複することはできません。エンドポイントについて保護されたネットワークのリストに 1 つ以上の IPv4 または IPv6 エントリが含まれている場合、他のエンドポイントの保護されたネットワークは、同じタイプ（つまり、IPv4 または IPv6）のエントリを少なくとも 1 つ持っていることが必要です。このようなエントリを持っていない場合、他のエンドポイントの IP アドレスが同じタイプであること、および保護されたネットワーク内でエントリが重複しないことが必要です。（IPv4 については/32 CIDR アドレスを使用し、IPv6 については/128 CIDR アドレス ブロックを使用します）。これらの両方のチェックに失敗すると、エンドポイントのペアは機能しません。

（注） [サブネット/IPアドレス（ネットワーク）（Subnet/IP Address (Network)）] はデフォルトの選択のままにします。

[保護されたネットワーク（Protected Networks）] を [任意（Any）] として選択し、デフォルトのルート トラフィックがドロップされることを確認した場合は、[VPN] > [サイト間（Site to Site）] > [VPN の編集（edit a VPN）] > [IPsec] > [リバース ルート インジェクションを有効にする（Enable Reverse Route Injection）] でリバース ルート インジェクションを無効にします。設定変更を展開します。これによって暗号マップから set reverse-route（リバース ルート インジェクション）が削除され、リバース トンネル トラフィックをドロップするようにする NVP でアドバタイズされたリバース ルートが削除されます。

- [アクセス リスト（拡張）（Access List (Extended)）]：拡張アクセス リストは、GRE トラフィックや OSPF トラフィックなどの、このエンドポイントによって受け入れられるトラフィックのタイプを制御する機能を提供します。トラフィックは、アドレスまたはポートにより制限できます。[追加（Add）] アイコン（  ）をクリックして、アクセス コントロール リスト オブジェクトを追加します。

（注） アクセス コントロール リストは、ポイントツーポイント トポロジでのみサポートされています。

FTD VPN IKE オプション

このトポロジに選択した IKE のバージョンの場合は、[IKEv1/IKEv2 設定（IKEv1/IKEv2 Settings）] を指定します。

（注） このダイアログの設定は、トポロジ全体、すべてのトンネル、すべての管理対象デバイスに適用されます。

ナビゲーション パス

> [サイト間（Site To Site）]。その後、[VPN の追加（Add VPN）] > [Firepower Threat Defense デバイス（Firepower Threat Defense Device）]、またはリストされている VPN トポロジを編集します。[IKE] タブを開きます。

フィールド

ポリシー

事前定義済みの IKEv1 または IKEv2 ポリシー オブジェクトを選択するか、または使用する新しいポリシー オブジェクトを作成します。詳細については、FTD IKE ポリシー（617 ページ）を参照してください。

認証タイプ（Authentication Type）

サイト間 VPN では、事前共有キーと証明書の 2 つの認証方式がサポートされています。2 つの方式の説明については、使用する認証方式の決定（1061 ページ）を参照してください。

（注） IKEv1 をサポートする VPN トポロジでは、選択した IKEv1 ポリシー オブジェクトで指定した [認証方式（Authentication Method）] が、IKEv1 の [認証タイプ（Authentication Type）] 設定のデフォルトになります。これらの値は一致する必要があります。一致しないと設定がエラーになります。

- [事前共有自動キー（Pre-shared Automatic Key）]：管理センターが、この VPN に使用される事前共有キーを自動的に定義します。[事前共有キー長（Pre-shared Key Length）] を指定します。キーの文字数は 1 ～ 27 文字です。

  文字 "（二重引用符）は事前共有キーの一部としてサポートされていません。事前共有キーで " を使用した場合は、Firepower Threat Defense 6.30 以降にアップグレードした後に必ず文字を変更してください。

- [事前共有手動キー（Pre-shared Manual Key）]：この VPN に使用される事前共有キーを手動で割り当てます。[キー（Key）] を指定して、[キーの確認（Confirm Key）] に再入力して確認します。

  IKEv2 に対してこのオプションを選択すると、[16 進数ベースの事前共有キーのみを適用する（Enforce hex-based pre-shared key only）] チェックボックスが表示されるの

で、必要に応じてオンにします。適用する場合は、キーの有効な 16 数値を、数字 0 ～ 9 または A ～ F を使用して、2 ～ 256 文字の偶数で入力する必要があります。

- [証明書（Certificate）]：VPN 接続の認証方法として証明書を使用する場合、ピアは PKI インフラストラクチャ内の CA サーバからデジタル証明書を取得し、相互に認証するためにトレードします。

  [証明書（Certificate）]フィールドで、事前設定された証明書登録オブジェクトを選択します。この登録オブジェクトは、管理対象デバイス上で同じ名前のトラストポイントを生成するために使用されます。証明書登録オブジェクトが関連付けられ、デバイスにインストールされ、登録プロセスが完了してから、トラストポイントが作成されます。

  トラストポイントとは、CA またはIDペアを表現したものです。トラストポイントには、CA の ID、CA 固有のコンフィギュレーション パラメータ、登録されている ID 証明書とのアソシエーションが含まれています。

  このオプションを選択する前に、次の点に注意してください。

  - トポロジ内のすべてのエンドポイントに証明書登録オブジェクトが登録されることを確認します。証明書登録オブジェクトには、証明書署名要求（CSR）を作成し、指定された認証局（CA）から ID 証明書を取得するために必要な CA サーバ情報と登録パラメータが含まれています。証明書登録オブジェクトは、管理対象デバイスを PKI インフラストラクチャに登録し、VPN 接続をサポートするデバイス上にトラストポイント（CA オブジェクト）を作成するために使用されます。証明書登録オブジェクトの作成手順については、証明書の登録オブジェクトの追加 （593 ページ）を参照してください。エンドポイントにオブジェクトを登録する手順については、次のいずれかを参照してください。
    - 自己署名登録を使用した証明書のインストール （643 ページ）
    - SCEP の登録を使用した証明書のインストール （644 ページ）
    - 手動登録を使用した証明書のインストール （645 ページ）
    - PKCS12 ファイルを使用した証明書のインストール （646 ページ）

  （注） サイト間 VPN トポロジの場合、同じ証明書登録オブジェクトがトポロジ内のすべてのエンドポイントに登録されていることを確認します。詳細については、次の表を参照してください。

  - さまざまなシナリオの登録要件については、次の表を参照してください。一部のシナリオでは、特定のデバイスの証明書登録オブジェクトを上書きする必要があります。オブジェクトの上書き方法については、オブジェクト オーバーライドの管理 （523 ページ）を参照してください。

証明書の登録タイプ	すべてのエンドポイントのデバイス ID 証明書の CA が同じ		すべてのエンドポイントのデバイス ID 証明書の CA が異なる
	デバイス固有のパラメータが証明書登録オブジェクトで指定されていない	デバイス固有のパラメータが証明書登録オブジェクトで指定されている	
[手動（Manual）]	上書きは不要	上書きが必要	上書きが必要
SCEP	上書きは不要	上書きが必要	上書きが必要
PKCS	上書きが必要	上書きが必要	上書きが必要
自己署名（Self-signed）	N/A	N/A	N/A

- Firepower Threat Defense VPN 証明書の注意事項と制約事項 （641 ページ）記載されている VPN 証明書の制限事項を確認。

（注） Windows 認証局（CA）を使用する場合、デフォルトのアプリケーション ポリシー拡張は **IP セキュリティ IKE 中間**です。このデフォルト設定を使用している場合は、選択したオブジェクトの [PKI証明書登録（PKI Certificate Enrollment）] ダイアログボックスの [キー（Key）] タブの [詳細設定（Advanced Settings）] セクションで [IPsecキーの使用状況を無視（Ignore IPsec Key Usage）] オプションを選択する必要があります。それ以外の場合、エンドポイントはサイト間 VPN 接続を完了できません。

FTD VPN IPsec オプション

（注） このダイアログの設定は、トポロジ全体、すべてのトンネル、すべての管理対象デバイスに適用されます。

クリプト マップ タイプ（Crypto-Map Type）

クリプト マップには、IPsec Security Association（SA; セキュリティ アソシエーション）を設定するために必要なすべてのコンポーネントが組み合わされています。2 つのピアが SA を確立しようとする場合は、それぞれに少なくとも 1 つの互換クリプト マップ エントリが必要です。クリプト マップ エントリに定義されたプロポーザルは、そのクリプト マップの IPsec ルールによって指定されたデータ フローを保護するための IPsec セキュリティ

ネゴシエーションで使用されます。この展開のクリプトマップにスタティックまたはダイナミックを選択します。

- [スタティック（Static）]：スタティック クリプト マップは、ポイントツーポイントまたは完全メッシュ VPN トポロジで使用します。
- [ダイナミック（Dynamic）]：実質的に、ダイナミック暗号マップによって、すべてのパラメータが設定されていない暗号マップエントリが作成されます。設定されていないパラメータは、IPsec ネゴシエーションの結果として、リモート ピアの要件に合うようにあとで動的に設定されます。

  ダイナミック暗号マップ ポリシーは、ハブアンドスポークとポイントツーポイント VPN トポロジの両方に適用されます。ダイナミック暗号マップ ポリシーを適用するには、トポロジ内のピアの 1 つにダイナミック IP アドレスを指定し、このトポロジでダイナミック暗号マップが有効になっていることを確認します。フルメッシュ VPN トポロジでは、スタティック クリプト マップ ポリシーのみを適用できます。

IKEv2 モード（IKEv2 Mode）

IPsec IKEv2 の場合のみ、カプセル化モードはトンネルに ESP 暗号化と認証を適用するために指定します。これにより、ESP が適用されるオリジナルの IP パケットの部分が決定されます。

- [トンネル モード（Tunnel mode）]：（デフォルト）カプセル化モードがトンネル モードに設定されます。トンネル モードでは、ESP 暗号化と認証が元の IP パケット全体（IP ヘッダーとデータ）に適用されるため、最終的な送信元アドレスと宛先アドレスが非表示になり、新しい IP パケットでペイロードになります。

  トンネル モードの大きな利点は、エンド システムを変更しなくても IPsec を利用できるということです。このモードでは、ルータなどのネットワーク デバイスが IPsec のプロキシとして動作できます。つまり、ルータがホストに代わって暗号化を行います。送信元ルータがパケットを暗号化し、IPsec トンネルを使用して転送します。宛先ルータは元の IP データグラムを復号化し、宛先システムに転送します。また、トラフィック分析から保護することもできます。トンネル モードを使用すると、攻撃者にはトンネルのエンドポイントしかわからず、トンネリングされたパケットの本来の送信元と宛先はわかりません（これらがトンネルのエンドポイントと同じ場合でも同様）。

- [転送優先（Transport preferred）]：ピアがサポートしていない場合、カプセル化モードは、トンネル モードにフォールバックするオプション付きの転送モードに設定されます。転送モードでは IP ペイロードだけが暗号化され、元の IP ヘッダーはそのまま使用されます。したがって、管理者は、VPN インターフェイスの IP アドレスと一致する保護されたネットワークを選択する必要があります。

  このモードには、各パケットに数バイトしか追加されず、パブリック ネットワーク上のデバイスに、パケットの最終的な送信元と宛先を認識できるという利点があります。transport モードでは、中間ネットワークでの特別な処理（たとえば QoS）を、IP ヘッダーの情報に基づいて実行できるようになります。ただし、レイヤ 4 ヘッダーが暗号化されるため、パケットの検査が制限されます。

- [転送必須（Transport required）]：カプセル化モードは転送モードのみに設定され、トンネルモードにフォールバックすることはできません。転送モードをサポートしていない1つのエンドポイントがあるせいで、エンドポイントが転送モードを正常にネゴシエートできない場合、VPN 接続は行われません。

プロポーザル（Proposals）

選択した IKEv1 または IKEv2 メソッドのプロポーザルを指定するには、（  ）をクリックします。利用可能な [IKEv1 IPsec プロポーザル（IKEv1 IPsec Proposals）] または [IKEv2 IPsec プロポーザル（IKEv2 IPsec Proposals）] オブジェクトから選択するか、または新しいプロポーザルを作成して選択します。詳細については、「IKEv1 IPsec プロポーザル オブジェクトの設定 （622 ページ）」および「IKEv2 IPsec プロポーザル オブジェクトの設定（623 ページ）」を参照してください。

セキュリティ アソシエーション（SA）の強度適用の有効化（Enable Security Association (SA) Strength Enforcement）

このオプションを有効にすると、子 IPsec SA で使用される暗号化アルゴリズムが、親 IKE SA よりも強くなることはありません（キー内のビット数の観点から）。

リバース ルート インジェクションを有効にする（Enable Reverse Route Injection）

リバース ルート インジェクション（RRI）により、スタティック ルートは、リモート トンネル エンドポイントで保護されているネットワークとホストのルーティング プロセスに自動的に挿入されます。

Perfect Forward Secrecy の有効化（Enable Perfect Forward Secrecy）

暗号化された交換ごとに一意のセッション キーを生成および使用するために、Perfect Forward Secrecy（PFS）を使用するかどうかを指定します。固有のセッション キーを使用することで、後続の復号から交換が保護されます。また、交換全体が記録されていて、攻撃者がエンドポイントデバイスで使用されている事前共有キーや秘密キーを入手している場合であっても保護されます。このオプションを選択する場合は、[係数グループ（Modulus Group）] リストで、PFS セッション キーの生成時に使用する Diffie-Hellman キー導出アルゴリズムも選択します。

係数グループ（Modulus Group）

2 つの IPsec ピア間の共有秘密キーを互いに送信することなく取得するために使用する Diffie-Hellman グループ。係数が大きいほどセキュリティが強化されますが、処理時間が長くなります。2 つのピアに、一致する係数グループが設定されている必要があります。 オプションの詳しい説明については、使用する Diffie-Hellman 係数グループの決定 （1060 ページ）を参照してください。

ライフタイム期間

セキュリティ アソシエーションが期限切れになる前に存続できる秒数。デフォルトは 28,800 秒です。

ライフタイム サイズ

特定のセキュリティ アソシエーションが期限切れになる前にそのセキュリティ アソシエーションを使用して IPsec ピア間を通過できるトラフィック量（KB 単位）。デフォルトは 4,608,000 KB です。無制限のデータは許可されていません。

ESPv3 設定（ESPv3 Settings）

着信 ICMP のエラーメッセージを検証（Validate incoming ICMP error messages）
IPsec トンネルを介して受信され、プライベート ネットワーク上の内部ホストが宛先の ICMP エラー メッセージを検証するかどうかを選択します。

「フラグメント禁止」ポリシーを有効にする（Enable 'Do Not Fragment' Policy）
IP ヘッダーに Do-Not-Fragment（DF）ビット セットを持つ大きなパケットを IPsec サブシステムがどのように処理するかを定義します。

ポリシー

- [DF ビッドのコピー（Copy DF bit）]：DF ビットを維持します。
- [DF ビッドのクリア（Clear DF bit）]：DF ビットを無視します。
- [DF ビットの設定（Set DF bit）]：DF ビットを設定して使用します。

トラフィック フロー機密保持（TFC）パケットを有効にする（Enable Traffic Flow Confidentiality (TFC) Packets）
トンネルを通過するトラフィック プロファイルをマスクするダミーの TFC パケットを有効にします。[バースト（Burst）]、[ペイロードサイズ（Payload Size）]、および [タイムアウト（Timeout）]パラメータを使用して、指定した SA で不定期にランダムな長さのパケットを生成します。

FTD のサイト間 VPN 展開の詳細オプション

ここでは、S2S VPN の展開で指定できる詳細オプションについて説明します。それらの設定は、トポロジ全体、すべてのトンネル、およびすべての管理対象デバイスに適用されます。

FTD VPN の IKE 詳細オプション

[詳細設定（Advanced）] > [IKE] > [ISAKAMP 設定（ISAKAMP Settings）]

IKE キープアライブ（IKE Keepalive）

IKE キープアライブを有効または無効にします。または、[永続的に有効にする（EnableInfinite）] に設定して、デバイスがキープアライブ モニタリングを開始することがないように指定します。

しきい値（Threshold）
IKE キープアライブの信頼間隔を指定します。これは、キープアライブ モニタリングを開始するまでにピアに許可されるアイドル時間（秒）です。最小値およびデフォルトは 10 秒で、最大値は 3600 秒です。

再試行間隔（Retry Interval）
IKE キープアライブの再試行から再試行までの待機秒数を指定します。デフォルトは 2 秒で、最大値は 10 秒です。

ピアに送信される ID:（Identity Sent to Peers:）
IKE ネゴシエーションでピアが自身の識別に使用する ID を選択します。

- autoOrDN（デフォルト）：接続タイプによってIKEネゴシエーションを判別します。事前共有キーのIPアドレスまたは証明書認証の証明書DN（未サポート）を使用します。
- ipAddress：ISAKMP 識別情報を交換するホストの IP アドレスを使用します。
- ホスト名（Hostname）：ISAKMP識別情報を交換するホストの完全修飾ドメイン名を使用します。この名前は、ホスト名とドメイン名で構成されます。

アグレッシブ モードの有効化（Enable Aggressive Mode）

ハブアンドスポーク VPN トポロジでのみ使用できます。IP アドレスが不明であり、デバイスで DNS 解決を使用できない可能性がある場合は、このネゴシエーション方式を選択してキー情報を交換します。ホスト名およびドメイン名に基づいてネゴシエーションが行われます。

[詳細設定（Advanced）]>[IKE]>[IVEv2セキュリティ アソシエーション（SA）設定（IVEv2 Security Association (SA) Settings）]

IKE v2 について、オープン SA の数を制限するさらに詳細なセッション制御を使用することができます。デフォルトでは、SA の数は制限されません。

クッキー チャレンジ（Cookie Challenge）

SA 開始パケットの応答としてピア デバイスにクッキー チャレンジを送信するかどうかを指定します。これは、サービス妨害（DoS）攻撃の防止に役立つことがあります。デフォルトでは、使用可能な SA の 50% がネゴシエーション中である場合にクッキー チャレンジを使用します。次のオプションのいずれか 1 つを選択します。

- カスタム：（Custom：）
- しない（Never）（デフォルト）
- 常に（Always）

着信クッキー チャレンジのしきい値（Threshold to Challenge Incoming Cookies）

許可されるネゴシエーション中の SA の総数の割合。この設定を指定すると、以降の SA ネゴシエーションに対してクッキー チャレンジがトリガーされます。範囲は 0 ～ 100% です。

許可されるネゴシエーション中の SA の数（Number of SAs Allowed in Negotiation）

一時点でネゴシエーション中にできるSAの最大数を制限します。クッキーチャレンジと共に使用する場合は、有効なクロスチェックが実行されるようにするため、クッキーチャレンジのしきい値をこの制限値よりも低くしてください。

許可される SA の最大数（Maximum number of SAs Allowed）

許可される IKEv2 接続の数を制限します。デフォルトでは無制限です。

トンネルの切断時の通知を有効にする（Enable Notification on Tunnel Disconnect）

管理者は、SA で受信された着信パケットがその SA のトラフィック セレクタと一致しない場合のピアへのIKE通知の送信を有効または無効にすることができます。デフォルトでは、[この通知を送信する（Sending this notification）] は無効になっています。

FTD VPN の IPsec 詳細オプション

[詳細設定（Advanced）] > [IPsec] > [IPsec 設定（IPsec Settings）]

暗号化の前にフラグメンテーションを有効にする（Enable Fragmentation Before Encryption）
このオプションは、IP フラグメンテーションをサポートしていない NAT デバイス間をトラフィックが通過できるようにします。このオプションを使用しても、IP フラグメンテーションをサポートしていない NAT デバイスの動作を妨げることはありません。

パスの最大伝送ユニットのエージング（Path Maximum Transmission Unit Aging）
オンにすると、PMTU（パス最大伝送ユニット）のエージング、つまり、SA（セキュリティ アソシエーション）の PMTU リセットまでの時間が有効になります。

値のリセット間隔（Value Reset Interval）
SA（セキュリティ アソシエーション）の PMTU 値が元の値にリセットされるまでの時間（分）を入力します。有効範囲は 10 ～ 30 分です。デフォルトは無制限です。

FTD のサイト間 VPN トンネルの詳細オプション

ナビゲーション パス

[サイト間（Site To Site）]、その後 [VPN の追加（Add VPN）] > [Firepower Threat Defense デバイス（Firepower Threat Defense Device）] を選択するか、またはリストされている VPN トポロジを編集します。[詳細設定（Advanced）] タブを開き、ナビゲーション ウィンドウで [トンネル（Tunnel）] を選択します。

トンネル オプション

ハブ アンド スポークおよびフル メッシュ トポロジでのみ使用できます。このセクションはポイントツーポイント構成では表示されません。

- [ハブを介したスポークツースポーク接続を有効にする（Enable Spoke to Spoke Connectivity through Hub）]：デフォルトでは無効になっています。このフィールドを選択すると、スポークの両端にあるデバイスは、ハブ ノードを介して他のデバイスへの接続を拡張できます。

NAT 設定

- [キープアライブ メッセージ トラバーサル（Keepalive Messages Traversal）]：NAT キープアライブ メッセージ トラバーサルを有効にするかどうかを指定します。VPN 接続ハブとスポークとの間にデバイス（中間デバイス）が配置されている場合、キープアライブ メッセージを転送するために NAT トラバーサル キープアライブを使用します。このデバイスでは、IPsec フローで NAT を実行します。

  このオプションを選択する場合は、セッションがアクティブであることを示すためにスポークと中間デバイス間でキープアライブ信号が送信される**間隔**（秒）を設定します。値は、5 ～ 3600 秒の範囲で指定します。デフォルトは 20 秒です。

VPN トラフィックのアクセス制御

- [復号されたトラフィック（sysopt permit-vpn）に対するバイパス アクセス コントロール ポリシー（Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)）]：デフォルトでは、復号されたトラフィックは、アクセス コントロール ポリシーのインスペクションの対象になります。復号されたトラフィック オプションに対してバイパス アクセス コントロールポリシーを有効にすると、ACLインスペクションがバイパスされますが、AAA サーバからダウンロードされた VPN フィルタ ACL と認証 ACL は、VPN トラフィックに引き続き適用されます。

証明書マップの設定

- [エンドポイントで設定された証明書マップを使用してトンネルを判別する（Use the certificate map configured in the Endpoints to determine the tunnel）]：このオプションを有効にする（オンにする）と、受信した証明書の内容をエンドポイント ノードに設定されている証明書マップ オブジェクトと照合することによってトンネルが判別されます。
- [証明書の OU フィールドを使用してトンネルを判別する（Use the certificate OU field to determine the tunnel）]：選択した場合、設定されたマッピング（上記のオプション）に基づいてノードが判別されない場合は、受信した証明書のサブジェクト識別名（DN）の組織単位（OU）の値を使用してトンネルを判別することを示します。
- [IKE ID を使用してトンネルを判別する（Use the IKE identity to determine the tunnel）]：選択した場合、OU（上記のオプション）と一致するルールまたは OU から取得されたルールに基づいてノードが判別されない場合は、証明書ベースの IKE セッションが、フェーズ 1 IKE ID の内容に基づいてトンネルにマッピングされることを示します。
- [ピア IP アドレスを使用してトンネルを判別する（Use the peer IP address to determine the tunnel）]：選択した場合、トンネルが OU または IKE ID 方式と一致するルールまたはその方式から取得されたルールに基づいて判別されない場合は、確立されたピア IP アドレスを使用することを示します。

第 44 章

のリモート アクセス VPN Firepower Threat Defense

Firepower Threat Defense リモート アクセス VPN の概要

Firepower Threat Defense は、リモート アクセス SSL と IPsec-IKEv2 VPN をサポートするセキュアなゲートウェイ機能を提供します。完全なトンネル クライアントである AnyConnect Secure Mobility Client[AnyConnectSecureMobilityClient] は、セキュリティ ゲートウェイへのセキュアな SSL および IPsec-IKEv2 接続をリモート ユーザに提供します。AnyConnect はエンドポイント デバイスでサポートされている唯一のクライアントで、Firepower Threat Defense デバイスへのリモート VPN 接続が可能です。このクライアントにより、ネットワーク管理者がリモート コンピュータにクライアントをインストールして設定しなくても、リモート ユーザは SSL または IPsec-IKEv2 VPN クライアントを活用できます。Windows、Mac、および Linux 用の AnyConnect モバイル クライアントは、接続時にセキュア ゲートウェイから展開されます。Apple iOS デバイスおよび Android デバイス用の AnyConnect アプリは、当該プラットフォームのアプリ ストアからインストールされます。

Firepower Management Center の [リモートアクセスVPNポリシー（Remote Access VPN Policy）] ウィザードを使用して、SSL と IPsec-IKEv2 リモート アクセス VPN を基本機能とともに迅速かつ容易にセットアップします。次に、必要に応じてポリシー設定を強化し、Firepower Threat Defense セキュア ゲートウェイ デバイスに展開します。

リモート アクセス VPN ポリシーを使用して、次の設定を構成できます。

- Two-Factor Authentication （1133 ページ）
- Secondary Authentication （1139 ページ）
- 承認を得るための LDAP または Active Directory の設定 （1147 ページ）
- VPN セッションでのパスワード変更の管理 （1146 ページ）
- RADIUS サーバへのアカウンティング レコードの送信 （1148 ページ）
- 許可サーバによるグループ ポリシーまたはその他の属性の選択のオーバーライド （1150 ページ）
  - ユーザ グループへの VPN アクセスの拒否 （1151 ページ）
  - ユーザ グループに対する接続プロファイルの選択の制限 （1152 ページ）

次の例を使用して、VPN ユーザに限定帯域幅を割り当てたり、ユーザ ID ベースのアクセス コントロール ルールに VPN ID を使用したりできます。

- ユーザあたりの AnyConnect 帯域幅を制限する方法 （1154 ページ）
- ユーザ ID ベースのアクセス コントロール ルールに VPN アイデンティティを使用する方法 （1157 ページ）

リモート アクセス VPN の機能

次の項では、Firepower Threat Defense のリモート アクセス VPN の機能について説明します。

- Cisco AnyConnect セキュア モビリティ クライアントを使用した SSL および IPsec-IKEv2 リモート アクセス。
- Firepower Management Center IPv4 トンネル上の IPv6 など、すべての組み合わせがサポートされています。
- FMC と FDM の両方での設定サポート。デバイス固有のオーバーライド。
- Firepower Management Center および FTD 両方の HA 環境をサポート。
- 複数のインターフェイスと複数の AAA サーバのサポート。
- Rapid Threat Containment では、RADIUS CoA または RADIUS ダイナミック認証の使用がサポートされています。

AAA

- 自己署名または CA 署名のアイデンティティ証明書を使用したサーバ認証。
- RADIUS サーバ、LDAP、または AD を使用する AAA ユーザ名とパスワードベースのリモート認証。

- RADIUS グループとユーザ承認属性、および RADIUS アカウンティング。
- 二重認証では、セカンダリ認証での他の AAA サーバの使用がサポートされています。
- VPN ID を使用した NGFW アクセス制御の統合。

VPN トンネリング

- アドレス割り当て
- スプリット トンネリング
- スプリット DNS
- クライアント ファイアウォール ACL
- 最大接続およびアイドル時間のセッション タイムアウト

モニタリング（Monitoring）

- 期間、クライアント アプリケーションなどのさまざまな特性によって VPN ユーザを表示する新しい VPN ダッシュボード ウィジェット。
- ユーザ名やOSプラットフォームなどの認証情報を含むリモートアクセスVPNイベント。
- FTD 統合 CLI により利用可能なトンネル統計。

AnyConnect のコンポーネント

AnyConnect Secure Mobility Client[AnyConnectSecureMobilityClient]導入

リモート アクセス VPN ポリシーに、接続エンドポイントに配布するための AnyConnect クライアントイメージおよび AnyConnect クライアント プロファイルを含めることができます。または、クライアント ソフトウェアを他の方法で配布できます。『Cisco AnyConnect Secure Mobility Client Administrator Guide』の該当するバージョンで、「*Deploy AnyConnect*」の章を参照してください。

事前にクライアントがインストールされていない場合、リモート ユーザは、SSL または IPsec-IKEv2 VPN 接続を受け入れるように設定されているインターフェイスの IP アドレスをブラウザに入力します。セキュリティ アプライアンスが http:// 要求を https:// にリダイレクトするように設定されている場合を除いて、リモート ユーザは https://*address* の形式で URL を入力する必要があります。URL を入力すると、ブラウザがそのインターフェイスに接続して、ログイン画面が表示されます。

ユーザ ログイン後、セキュア ゲートウェイは VPN クライアントを必要としているとユーザを識別すると、リモート コンピュータのオペレーティング システムに一致するクライアントをダウンロードします。ダウンロード後、クライアントは自動的にインストールと設定を行い、セキュアな接続を確立します。接続の終了時には、（セキュリティ アプライアンスの設定に応じて）そのまま残るか、または自動的にアンインストールを実行します。以前にインストール

されたクライアントの場合、ログイン後、Firepower Threat Defense セキュリティ ゲートウェイはクライアントのバージョンを検査し、必要に応じてアップグレードします。

AnyConnect Secure Mobility Client[AnyConnectSecureMobilityClient] 操作

クライアントがセキュリティアプライアンスとの接続をネゴシエートする場合、クライアントは、Transport Layer Security（TLS）、および任意で Datagram Transport Layer Security（DTLS）を使用して接続します。DTLS により、一部の SSL 接続で発生する遅延および帯域幅の問題が回避され、パケット遅延の影響を受けやすいリアルタイム アプリケーションのパフォーマンスが向上します。

IPsec-IKEv2 VPN クライアントがセキュア ゲートウェイへの接続を開始すると、インターネットキーエクスチェンジ（IKE）によるデバイスの認証と、続く IKE 拡張認証（Xauth）によるユーザ認証からなるネゴシエーションが行われます。グループ プロファイルが VPN クライアントにプッシュされ、IPsec セキュリティ アソシエーション（SA）が作成されて VPN が完了します。

AnyConnect クライアント プロファイル およびエディタ

AnyConnect クライアント プロファイルは、設定パラメータのグループで、動作や表示の設定に VPN クライアントが使用する XML ファイル内に保存されます。これらのパラメータ（XML タグ）には、ホストコンピュータの名前とアドレス、および追加のクライアント機能を有効にする設定が含まれています。

AnyConnectプロファイルエディタを使用してプロファイルを設定できます。このエディタは、AnyConnect ソフトウェア パッケージの一部として利用できる便利な GUI ベースの設定ツールです。これは、Firepower Management Center の外部から実行する独立したプログラムです。

リモート アクセス VPN 認証

リモート アクセス VPN サーバ認証

Firepower Threat Defense セキュア ゲートウェイは、VPN クライアントのエンドポイントに対して自身を特定し、認証するために必ず証明書を使用します。

ウィザードを使用してリモート アクセス VPN 構成を設定するときに、選択した証明書を対象の Firepower Threat Defense デバイスに登録できます。ウィザードの [アクセスおよび証明書（Access & Certificate）] フェーズで、[選択した証明書オブジェクトをターゲットデバイスに登録する（Enroll the selected certificate object on the target devices）] オプションを選択します。証明書の登録は、指定したデバイス上で自動的に開始されます。リモート アクセス VPN の構成が完了すると、デバイス証明書のホームページで登録した証明書のステータスを確認できます。ステータスは、証明書の登録が成功したかどうかを明確に示します。これで、リモートアクセス VPN の設定が完了し、導入の準備ができました。

PKI の登録とも呼ばれる、セキュア ゲートウェイの証明書の取得については、Firepower Threat Defense Certificate ベースの認証 （641 ページ）で説明しています。この章には、ゲートウェイ証明書の設定、登録、および管理の詳細な説明が含まれています。

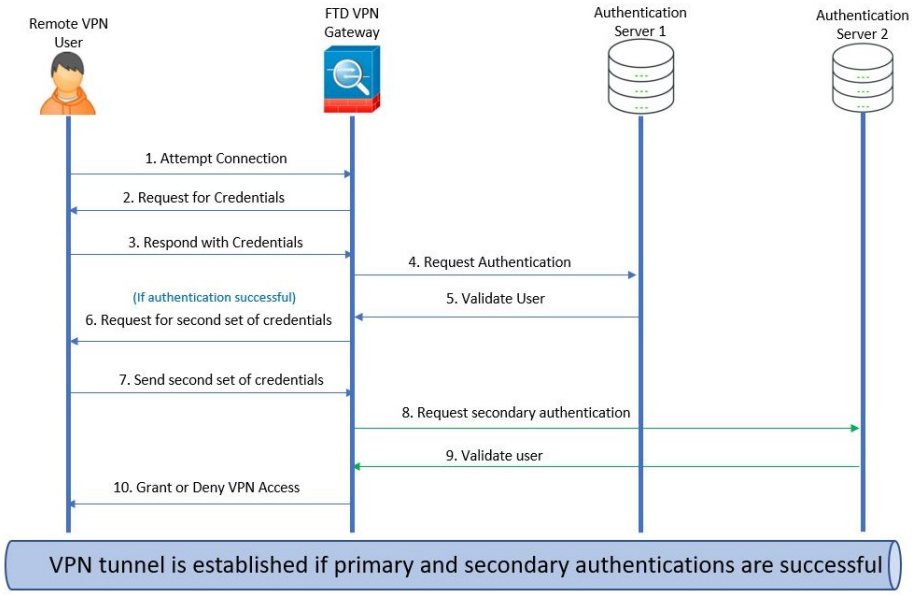
リモート アクセス VPN のクライアント AAA

SSL と IPsec-IKEv2 の両方について、リモート ユーザ認証はユーザ名とパスワードのみ、証明書のみ、あるいはこの両方を使用して実行されます。

（注） 展開でクライアント証明書を使用している場合は、Firepower Threat Defense または Firepower Management Center に関係なく、クライアントのプラットフォームにこれらの証明書を追加する必要があります。クライアントに証明書を入力するために、SCEP や CA サービスなどの機能は提供されません。

AAA サーバでは、セキュア ゲートウェイとして機能する管理対象デバイスが、ユーザの身元（認証）、ユーザが許可されていること（認可）、およびユーザが行ったこと（アカウンティング）を確認できます。AAA サーバの例としては、RADIUS、LDAP/AD、TACACS+、Kerberos などがあります。Firepower Threat Defense デバイス上のリモート アクセス VPN では、AD、LDAP、および RADIUS AAA サーバが認証のためにサポートされています。認証サーバとアカウンティング サーバには、RADIUS サーバのみを構成して使用できます。リモート アクセス VPN の認可の詳細については、「権限および属性のポリシー実施の概要」の項を参照してください。

図 *23 :* リモート アクセス *VPN AAA* 認証



（注） リモート アクセス VPN ポリシーを追加または編集する前に、指定するレルムおよび RADIUS サーバ グループを設定する必要があります。詳細については、レルムの作成 （2576ページ）およびRADIUS サーバ グループ （635 ページ）を参照してください。

DNS が設定されていないと、デバイスは AAA サーバ名、名前付き URL、および FQDN またはホスト名を持つ CA サーバを解決できません。解決できるのは IP アドレスのみです。

リモート ユーザから提供されるログイン情報は、LDAP または AD レルムまたは RADIUS サーバ グループによって検証されます。これらのエンティティは、Firepower Threat Defense セキュア ゲートウェイと統合されます。

（注） ユーザが認証ソースとして Active Directory を使用して RA VPN で認証を受ける場合、ユーザは自分のユーザ名を使用してログインする必要があります。`domain\username` または `username@domain` 形式は失敗します。（Active Directory はこのユーザ名をログオン名、または場合によっては `sAMAccountName` と呼んでいます）。詳細については、MSDN でユーザの命名属性 [英語] を参照してください。

認証に RADIUS を使用する場合、ユーザは前述のどの形式でもログインできます。

VPN 接続経由で認証されると、リモート ユーザには *VPN ID* が適用されます。この VPN ID は、そのリモート ユーザに属しているネットワーク トラフィックを認識し、フィルタリングするために Firepower Threat Defense のセキュア ゲートウェイ上のアイデンティティ ポリシーで使用されます。

アイデンティティ ポリシーはアクセス コントロール ポリシーと関連付けられ、これにより、誰がネットワーク リソースにアクセスできるかが決まります。リモート ユーザがブロックされるか、またはネットワーク リソースにアクセスできるかはこのようにして決まります。

詳細については、アイデンティティ ポリシーについて （2637ページ）およびアクセス コントロール ポリシーの開始 （1665 ページ）のセクションを参照してください。

権限および属性のポリシー実施の概要

Firepower Threat Defense デバイスは、外部認証サーバおよび/または承認 AAA サーバ（RADIUS）から、あるいは Firepower Threat Defense デバイス上のグループ ポリシーから、ユーザ承認属性（ユーザの権利または権限とも呼ばれる）を VPN 接続に適用することをサポートしています。Firepower Threat Defense デバイスがグループ ポリシーに設定されている属性と競合する外部 AAA サーバから属性を受信した場合は、AAA サーバからの属性が常に優先されます。

Firepower Threat Defense デバイスは次の順序で属性を適用します。

1. **外部 AAA サーバ上のユーザ属性**：ユーザ認証や認可が成功すると、サーバからこの属性が返されます。
2. **Firepower Threat Defense デバイス上で設定されているグループ ポリシー**：RADIUS サーバからユーザの RADIUS CLASS 属性 IETF-Class-25（OU=group-policy）の値が返された場

合は、Firepower Threat Defense デバイスはそのユーザを同じ名前のグループ ポリシーに入れて、そのグループ ポリシーの属性のうち、サーバから返されないものを適用します。

3. **接続プロファイル（トンネル グループと呼ばれる）で割り当てられたグループ ポリシー**：接続プロファイルには、接続の事前設定と、認証前にユーザに適用されるデフォルトのグループ ポリシーが含まれています。

（注） Firepower Threat Defense デバイスは、デフォルトのグループ ポリシー *DfltGrpPolicy* から継承したシステム デフォルト属性をサポートしていません。前述のとおり、ユーザ属性または AAA サーバのグループ ポリシーによって上書きされない場合、接続プロファイルに割り当てられたグループ ポリシーの属性がユーザ セッションに使用されます。

AAA サーバ接続の概要

LDAP、AD、および RADIUS AAA サーバは、ユーザ識別処理のみの場合、VPN 認証のみの場合、またはそれら両方の場合に、Firepower Threat Defense デバイスから到達できる必要があります。AAA サーバは、次のアクティビティのためにリモートアクセス VPN で使用されます。

- **ユーザ識別処理**：サーバは管理インターフェイスを介して到達できる必要があります。

  Firepower Threat Defense デバイスの管理インターフェイスには、VPN で使用される通常のインターフェイスとは別のルーティング プロセスと設定があります。

- **VPN 認証**：サーバは通常のインターフェイス（診断インターフェイスまたはデータ インターフェイス）のいずれかを介して到達できる必要があります。

  通常のインターフェイスでは、2 つのルーティング テーブルが使用されます。診断インターフェイス用および管理専用に設定されたその他のインターフェイス用の管理専用ルーティング テーブルと、データ インターフェイスに使用されるデータ ルーティング テーブルです。ルート ルックアップが完了すると、管理専用ルーティング テーブルが最初にチェックされ、次にデータ ルーティング テーブルがチェックされます。最初の照合は、AAA サーバに到達するように選択されます。

  （注） データ インターフェイスに AAA サーバを配置する場合は、管理専用ルーティング ポリシーがデータ インターフェイス宛てのトラフィックと一致しないようにしてください。たとえば、診断インターフェイスを介するデフォルトルートがある場合、トラフィックが決してデータ ルーティング テーブルにフォールバックしないように注意してください。**show route management-only** コマンドと **show route** コマンドを使用してルーティングの決定を確認します。

同じ AAA サーバ上の両方のアクティビティについて、ユーザ識別処理用の管理インターフェイスを介してサーバに到達可能にすることに加え、次のいずれかを実行して、同じ AAA サーバへの VPN 認証アクセスを確保します。

- 管理インターフェイスと同じサブネット上の IP アドレスを使用して診断インターフェイスを有効にして設定し、インターフェイスを介した AAA サーバへのルートを設定します。診断インターフェイスのアクセスは、VPN アクティビティ、識別処理のための管理インターフェイスのアクセスに使用されます。

（注） このように構成すると、診断インターフェイスおよび管理インターフェイスと同じサブネット上にデータインターフェイスを設定することもできません。管理インターフェイスとデータ インターフェイスが同じネットワーク上に必要な場合（たとえば、デバイス自体をゲートウェイとして使用する場合）でも、診断インターフェイスは無効のままでなければならないため、このソリューションを使用できません。

- AAA サーバへのデータ インターフェイスを介してルートを設定します。データ インターフェイスのアクセスは、VPN アクティビティ、ユーザ識別処理のための管理インターフェイスのアクセスに使用されます。

さまざまなインターフェイスの詳細については、Firepower Threat Defense の通常のファイアウォール インターフェイス （793 ページ）を参照してください。

展開後、次の CLI コマンドを使用して、Firepower Threat Defense デバイスからの AAA サーバ接続をモニタおよびトラブルシューティングします。

- **show aaa-server** AAA サーバの統計情報を表示します。
- **show route management-only** 管理専用ルーティング テーブル エントリを表示します。
- **show route** データ トラフィックのルーティング テーブル エントリを表示します。
- **ping** *system* と **traceroute** *system* は管理インターフェイスを介して AAA サーバへのパスを確認します。
- **ping interface** *ifname* と **traceroute** *destination* は診断インターフェイスとデータインターフェイスを介して AAA サーバへのパスを確認します。
- **test aaa-server authentication** と **test aaa-server authorization** は AAA サーバでの認証と許可をテストします。
- **clear aaa-server statistics** *groupname* または **clear aaa-server statistics protocol** *protocol* はグループ別またはプロトコル別に AAA サーバの統計情報をクリアします。
- **aaa-server** *groupname* **active host** *hostname* は障害が発生した AAA サーバをアクティブ化します。または、 **aaa-server** *groupname* **fail host** *hostname* で AAA サーバを不合格にします。

- **debug ldap level**、**debug aaa authentication**、 **debug aaa authorization**、**debug aaa accounting**。

リモート アクセス VPN のガイドラインと制限事項

リモート アクセス VPN ポリシーの設定

- 新しいリモートアクセスVPNポリシーは、ウィザードを使用してのみ追加できます。ウィザードのすべての手順を実行して新しいポリシーを作成する必要があります。ウィザードを完了する前にキャンセルすると、ポリシーは保存されません。
- 2 人のユーザが同時にリモート アクセス VPN ポリシーを編集することは**できません**。ただし、Webインターフェイスでは同時編集が防止されません。これが発生した場合、最後に保存された設定が保持されます。
- リモート アクセス VPN ポリシーがそのデバイスに割り当てられている場合、あるドメインから別のドメインに Firepower Threat Defense デバイスを移動することはできません。
- クラスタ モードの Firepower 9300 および 4100 シリーズは、リモート アクセス VPN の設定をサポートしていません。
- 誤って設定された FTD NAT ルールがあると、リモート アクセス VPN 接続が失敗する可能性があります。
- IKE ポート 500/4500 または SSL ポート 443 が使用されている場合、またはアクティブな PAT 変換がある場合は、これらのポートでサービスを開始できないため、AnyConnect IPSec-IKEv2 または SSL リモート アクセス VPN を同じポートに設定することはできません。これらのポートは、リモート アクセス VPN を設定する前に Firepower Threat Defense デバイスで使用しないようにする必要があります。
- ウィザードを使用してリモート アクセス VPN を設定しているときは、インライン証明書登録オブジェクトを作成できますが、それらを使用してアイデンティティ証明書をインストールすることはできません。証明書登録オブジェクトは、リモート アクセス VPN ゲートウェイとして設定されている Firepower Threat Defense デバイスでアイデンティティ証明書を生成するために使用されます。デバイスにリモート アクセス VPN 設定を展開する前に、デバイスにアイデンティティ証明書をインストールします。証明書登録オブジェクトに基づいてアイデンティティ証明書をインストールする方法の詳細については、オブジェクト マネージャ （516 ページ）を参照してください。
- リモート アクセス VPN ポリシーの設定を変更した後は、Firepower Threat Defense デバイスに変更を再展開します。設定変更の展開にかかる時間は、ポリシーとルールの複雑さ、デバイスに送信する設定のタイプと量、メモリとデバイスモデルなど、複数の要因によって異なります。リモート アクセス VPN ポリシーの変更を展開する前に、設定変更の展開に関する注意事項 （444 ページ）を確認してください。

同時 VPN セッションのキャパシティ プランニング

同時 VPN セッションの最大数は、プラットフォーム固有の制限に準拠し、ライセンスには依存しません。デバイス モデルに基づいて、1 台のデバイスで許可される同時リモート アクセス VPN セッション数に上限が設けられます。この制限は、システム パフォーマンスが許容できないレベルに低下しないように設計されています。これらの制限は、キャパシティ プランニングに使用します。

デバイス モデル	最大同時リモート アクセス VPN セッション数
Firepower 2110	1500
Firepower 2120	3500
Firepower 2130	7500
Firepower 2140	10000

他のハードウェア モデルの容量については、セールス担当者にお問い合わせください。

（注） プラットフォームごとのセッション数の上限に達すると、FTD デバイスが VPN 接続を拒否します。Syslog メッセージが示され、接続が拒否されます。Syslog メッセージ ガイドで Syslog メッセージ「%ASA-4-113029」と「and %ASA-4-113038」を参照してください。詳細については、http://www.cisco.com/c/en/us/td/docs/security/asa/syslog-guide/syslogs.htmlを参照してください。

VPN の暗号使用方法の制御

DES よりも高度な暗号方式を使用しないようにするため、Firepower Management Center の次の場所で、展開前チェックを使用することもできます。

[デバイス（Devices）] > [プラットフォーム設定（Platform Settings）] > [SSL 設定（SSL Settings）]

[デバイス（Devices）] > [VPN] > [リモート アクセス（Remote Access）] > [詳細（Advanced）] > [IPsec]

SSL 設定と IPsec の詳細については、SSL 設定 （1371 ページ）およびリモート アクセス VPN の [IPsec/IKEv2パラメータ （IPsec/IKEv2 Parameters）] の設定 （1129 ページ）を参照してください。

認証、認可、アカウンティング

- Firepower Threat Defense デバイスは、システム統合認証サーバのみを使用するリモート アクセス VPN ユーザの認証をサポートしており、ローカル ユーザ データベースはサポートされていません。

- LDAP または AD の認可とアカウンティングは、リモート アクセス VPN ではサポートされていません。リモート アクセス VPN ポリシーでは、RADIUS サーバ グループのみを承認サーバまたはアカウンティング サーバとして構成できます。
- リモート アクセス VPN を使用するには、トポロジ内の各デバイスで DNS を設定します。DNS がないと、デバイスは AAA サーバ名、名前付き URL、および FQDN またはホスト名を持つ CA サーバを解決できません。解決できるのは IP アドレスのみです。

  プラットフォームの設定を使用して DNS を設定できます。詳細については、DNS の設定（1360 ページ）およびDNS サーバ グループ オブジェクト（601 ページ）を参照してください。

クライアント証明書

- 展開でクライアント証明書を使用している場合は、Firepower Threat Defense または Firepower Management Center に関係なく、クライアントのプラットフォームにこれらの証明書を追加する必要があります。クライアントに証明書を入力するために、SCEP や CA サービスなどの機能は提供されません。

AnyConnect のサポート対象外の機能

サポートされている VPN クライアントは、Cisco AnyConnect セキュア モビリティ クライアントのみです。それ以外のクライアントまたはネイティブ VPN はサポートされていません。クライアントレス VPN は、Web ブラウザを使用して AnyConnect クライアントの展開に使用されるだけで、VPN 接続としてはサポートされていません。

FTD セキュア ゲートウェイに接続する場合、次の AnyConnect 機能はサポートされていません。

- セキュア モビリティ、ネットワーク アクセス管理、およびコア VPN 機能と VPN クライアント プロファイルを超えたその他のすべての AnyConnect モジュールとそのプロファイル。
- Hostscan およびエンドポイント ポスチャ アセスメント と、クライアント ポスチャに基づくダイナミック アクセス ポリシーなどのポスチャ派生機能。
- AnyConnect のカスタマイズとローカリゼーションのサポート。FTD デバイスは、これらの機能のために AnyConnect を設定するために必要なファイルを設定または展開しません。
- AnyConnect クライアントのカスタム属性は、FTD ではサポートされません。したがって、デスクトップ クライアントでの遅延アップグレード、モバイル クライアントでのアプリケーションごとの VPN といった、カスタム属性を使用するすべての機能はサポートされません。
- ローカル認証では、VPN ユーザを FTD セキュア ゲートウェイで設定することはできません。

  ローカル CA では、セキュア ゲートウェイは認証局として動作できません。
- SAML 2.0 を使用したシングル サインオン

- TACACS、Kerberos（KCD 認証および RSA SDI）
- LDAP 認証（LDAP 属性マップ）
- ブラウザ プロキシ
- VPN ロード バランシング。

新しいリモート アクセス VPN 接続の設定

ここでは、VPN ゲートウェイとして Firepower Threat Defense デバイスを使用したり、VPN クライアントとして Cisco AnyConnect を使用したりして、新しいリモート アクセスを設定する手順について説明します。

	操作内容	詳細
ステップ 1	ガイドラインと前提条件を確認します。	リモート アクセス VPN のガイドラインと制限事項 （1093 ページ） リモート アクセス VPN を設定するための前提条件 （1097 ページ）
ステップ 2	ウィザードを使用して新しいリモート アクセス VPN ポリシーを作成します。	新しいリモート アクセス VPN ポリシーの作成 （1098 ページ）
ステップ 3	デバイスに展開されているアクセス コントロール ポリシーを更新します。	Firepower Threat Defense デバイスのアクセス コントロール ポリシーの更新 （1100 ページ）
ステップ 4	（オプション）NAT がデバイスで設定されている場合は、NAT 免除ルールを設定します。	（オプション）NAT 免除の設定 （1101 ページ）
ステップ 5	DNS を設定します。	DNS の設定 （1102 ページ）
ステップ 6	AnyConnect クライアント プロファイルを追加します。	AnyConnect クライアント プロファイル XML ファイルの追加 （1102 ページ）
ステップ 7	リモート アクセス VPN ポリシーを展開します。	設定変更の展開 （447 ページ）

	操作内容	詳細
ステップ 8	（オプション）リモート アクセス VPN ポリシー設定を確認します。	設定の確認 （1104 ページ）

リモート アクセス VPN を設定するための前提条件

- Firepower Threat Defense デバイスを展開し、Firepower Management Center を設定して、輸出規制対象の機能を有効にした必要なライセンスを持つデバイスを管理します。詳細については、VPN ライセンス （1057 ページ）を参照してください。
- リモート アクセス VPN ゲートウェイとして機能する各 Firepower Threat Defense デバイスにアイデンティティ証明書を取得するために使用する証明書登録オブジェクトを設定します。
- RADIUS サーバ グループ オブジェクトと、リモート アクセス VPN ポリシーで使用されている AD または LDAP レルムを設定します。
- リモート アクセス VPN 設定が機能するように AAA サーバに Firepower Threat Defense デバイスからアクセスできることを確認します。AAA サーバへの接続を確実にするために、ルーティングを設定します（[デバイス（Devices）]>[デバイス管理（Device Management）]>[デバイスの編集（Edit Device）]>[ルーティング（Routing）]）。

  リモート アクセス VPN の二重認証の場合は、二重認証設定が機能するようにプライマリとセカンダリの両方の認証サーバに Firepower Threat Defense デバイスからアクセスできることを確認します。
- Firepower Threat Defense のリモート アクセス VPN を有効にするため、AnyConnect Plus、AnyConnect Apex、または AnyConnect VPN Only のうちいずれかの Cisco AnyConnect ライセンスを購入します。
- シスコのソフトウェア ダウンロード センターから最新の AnyConnect イメージ ファイルをダウンロードします。

  Firepower Management Center の Web インターフェイスで、[オブジェクト（Objects）]>[オブジェクト管理（Object Management）]>[VPN]>[AnyConnect ファイル（AnyConnect File）]に移動し、新しいAnyConnect クライアント イメージ ファイルを追加します。
- ユーザが VPN 接続のためにアクセスするネットワーク インターフェイスを含む、セキュリティ ゾーンまたはインターフェイス グループを作成します。インターフェイス オブジェクト：インターフェイス グループとセキュリティ ゾーン （535 ページ）を参照してください
- AnyConnect プロファイル エディタをシスコのソフトウェア ダウンロード センターからダウンロードし、AnyConnect クライアント プロファイルを作成します。スタンドアロン プロファイル エディタを使用して、新しい AnyConnect プロファイルを作成したり、既存の AnyConnect プロファイルを変更したりできます。

新しいリモート アクセス VPN ポリシーの作成

新しいリモートアクセスVPNポリシーを追加できるのはリモートアクセスVPNポリシー ウィザードを使用する場合のみです。このウィザードは、基本的な機能を持つリモート アクセス VPNをすばやく、簡単にセットアップできるようにします。さらに、必要に応じて追加の属性を指定することでポリシー設定を強化して Firepower Threat Defense のセキュア ゲートウェイ デバイスに展開できます。

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス（Access）
エクスポート制御機能が有効なスマート ライセンス アカウントに関連付けられている次の AnyConnect ライセンスのいずれか。 • AnyConnect VPN Only • AnyConnect Plus • AnyConnect Apex	該当なし	FTD	いずれか（Any）	Admin

始める前に

- リモート アクセス VPN を設定するための前提条件（1097 ページ） に示されているすべての前提条件を満たしていることを確認します。

ステップ 1 **[Devices]** > **[VPN]** > **[Remote Access]**を選択します。

ステップ 2 [追加（Add）]（  ）をクリックし、基本的なポリシー設定を行うウィザードを使用して新しいリモート アクセス VPN ポリシーを作成します。

ウィザードのすべての手順を実行して新しいポリシーを作成する必要があります。ウィザードを完了する前にキャンセルすると、ポリシーは保存されません。

ステップ 3 [ターゲット デバイス（Target Devices）] と [プロトコル（Protocols）] を選択します。

選択した Firepower Threat Defense デバイスは、VPN クライアント ユーザのリモート アクセス VPN ゲートウェイとして機能します。リストからデバイスを選択するか、または新しいデバイスを追加します。

SSL または IPSec-IKEv2、あるいはその両方の VPN プロトコルを選択できます。Firepower Threat Defense は、VPN トンネルを経由するパブリック ネットワークを介してセキュアな接続を確立するために両方のプロトコルをサポートしています。SSL 設定については、SSL 設定 （1371 ページ）を参照してください。

ステップ 4 [接続プロファイル（Connection Profile）] および [グループポリシー（Group Policy）] 設定を設定します。

接続プロファイルでは、リモート ユーザが VPN デバイスに接続する方法を定義するパラメータ セットを指定します。パラメータには、認証、VPN クライアントへのアドレスの割り当てとグループ ポリシーの設定および属性が含まれています。Firepower Threat Defense デバイスは、リモート アクセス VPN ポリシーを設定する際の *DefaultWEBVPNGroup* というデフォルトの接続プロファイルを提供します。

詳細については、接続プロファイルの設定 （1105 ページ）を参照してください。

グループ ポリシーはグループ ポリシー オブジェクト内に保存される属性と値の一連のペアで、VPN ユーザに対してリモート アクセス VPN のエクスペリエンスを定義します。グループ ポリシーを使用して、ユーザ認証プロファイル、IP アドレス、AnyConnect 設定、VLAN マッピング、およびユーザ セッション設定などの属性を設定します。RADIUS 承認サーバがグループ ポリシーを割り当てるか、または現在の接続プロファイルから取得されます。

詳細については、グループ ポリシーの設定 （1123 ページ）を参照してください。

ステップ 5 VPN ユーザがリモート アクセス VPN への接続に使用する [AnyConnect クライアント イメージ（AnyConnect Client Image）] を選択します。

Cisco AnyConnect セキュア モビリティ クライアントは Firepower Threat Defense デバイスへのセキュアな SSL 接続または IPSec（IKEv2）接続を提供し、これにより、リモート ユーザによる企業リソースへのフル VPN プロファイリングが可能となります。Firepower Threat Defense デバイスにリモート アクセス VPN ポリシーを展開したら、VPN ユーザは設定したデバイス インターフェイスの IP アドレスをブラウザに入力し、AnyConnect クライアントをダウンロードしてインストールできるようになります。

ステップ 6 [ネットワーク インターフェイスとアイデンティティ証明書（Network Interface and Identity Certificate）] を選択します。

インターフェイス オブジェクトは、ネットワークをセグメント化してトラフィック フローを管理し、分類しやすくします。セキュリティ ゾーン オブジェクトは単にインターフェイスをグループ化します。これらのグループは複数のデバイスにまたがることがあります。また、単一のデバイスに複数のゾーンインターフェイス オブジェクトを設定することもできます。インターフェイス オブジェクトには次の 2 つのタイプがあります。

- セキュリティ ゾーン：インターフェイスは、1 つのセキュリティ ゾーンにのみ属することができます。
- インターフェイス グループ：インターフェイスは複数のインターフェイスグループ（および 1 つのセキュリティ ゾーン）に属することができます。

ステップ 7 リモート アクセス VPN ポリシー設定の [概要（Summary）] を表示します。

[概要（Summary）] ページには、これまでに設定したすべてのリモート アクセス VPN 設定が表示され、選択したデバイスにリモート アクセス VPN ポリシーを展開する前に実行する必要がある追加設定へのリンクが示されます。

必要に応じて、[戻る（Back）] をクリックして設定に変更を加えます。

ステップ 8 リモート アクセス VPN ポリシーの基本設定を完了するには、[終了（Finish）] をクリックします。

ウィザードを使用してリモート アクセス VPN ポリシーを完了すると、ポリシー リスト ページに戻ります。DNS 設定をセットアップし、VPN ユーザのアクセス制御を設定し、NAT の免除を有効にして（必要な場合）、基本的な RA VPN のポリシー設定を完了します。次に、設定を展開し、VPN 接続を確立します。

Firepower Threat Defense デバイスのアクセス コントロール ポリシーの更新

リモート アクセス VPN ポリシーを展開する前に、VPN トラフィックを許可するルールを使用してターゲットの Firepower Threat Defense デバイス上でアクセス コントロール ポリシーを更新する必要があります。ルールは、定義済み VPN プール ネットワークの送信元と社内ネットワークの宛先を持つ外部インターフェイスを通過するすべてのトラフィックを許可する必要があります。

（注） [復号されたトラフィックのアクセス コントロール ポリシーをバイパスする（sysopt permit-vpn）（Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)）] オプションを選択した場合は、リモート アクセス VPN のアクセス コントロール ポリシーを更新する必要はありません。詳細については、リモートアクセス VPN のアクセス インターフェイスの設定（1115 ページ）を参照してください。

始める前に

リモート アクセス VPN ポリシー ウィザードを使用してリモート アクセス VPN ポリシーの設定を実行します。

ステップ 1 Firepower Management Center の Web インターフェイスで、[ポリシー（Policies）] > [アクセス制御（Access Control）] を選択します。

ステップ 2 リモート アクセス VPN ポリシーが展開されるターゲット デバイスに割り当てられているアクセス コントロール ポリシーを選択し、[編集（Edit）] をクリックします。

ステップ 3 新しいルールを追加するには、[ルールの追加（Add Rule）] をクリックします。

ステップ 4 ルールの [名前（Name）] を指定し、[有効（Enabled）] を選択します。

ステップ 5 [アクション（Action）]、[許可（Allow）]、または [信頼（Allow）] を選択します。

ステップ 6 [ゾーン（Zones）] タブで次の項目を選択します。

a) [使用可能なゾーン（Available Zones）] から外部ゾーンを選択し、[送信元に追加（Add to Source）] をクリックします。

b) [使用可能なゾーン（Available Zones）] から内部ゾーンを選択し、[宛先に追加（Add to Destination）] をクリックします。

ステップ 7 [ネットワーク（Networks）] タブで次の項目を選択します。

a) 使用可能なネットワークから内部ネットワーク（内部インターフェイスまたは社内ネットワーク）を選択し、[宛先に追加（Add to Destination）] をクリックします。

b) **使用可能なネットワーク**から VPN アドレス プール ネットワークを選択し、[送信元ネットワークに追加（Add to Source Networks）] をクリックします。

ステップ 8 その他の必要なアクセス制御ルールを設定して [追加（Add）] をクリックします。

ステップ 9 ルールとアクセス コントロール ポリシーを保存します。

（オプション）NAT 免除の設定

NAT 免除を使用すると、アドレスは変換から除外され、変換済みのホストとリモート ホストの両方が保護されたホストとの接続を開始できるようになります。アイデンティティ NAT と同様に、特定のインターフェイスでホストの変換を制限するのではなく、すべてのインターフェイスを経由する接続に NAT 免除を使用する必要があります。ただし、NAT 免除では変換対象の実際のアドレスを決定するときに実際のアドレスおよび宛先アドレスを指定できます（ポリシー NAT と類似）。アクセス リストのポートを考慮するには、スタティック アイデンティティ NAT を使用します。

始める前に

リモート アクセス VPN ポリシーが展開されているターゲット デバイスに NAT が設定されているかどうかを確認します。NAT がターゲット デバイスで有効になっている場合、NAT ポリシーを定義して VPN トラフィックを対象外にする必要があります。

ステップ 1 Firepower Management Center の Web インターフェイスで、[デバイス（Devices）] > [NAT] をクリックします。

ステップ 2 更新する NAT ポリシーを選択するか、または [新しいポリシー（New Policy）] > [脅威対策NAT（Threat Defense NAT）] をクリックし、すべてのインターフェイスへの接続を許可する NAT ルールを含む NAT ポリシーを作成します。

ステップ 3 [ルールの追加（Add Rule）] をクリックして NAT ルールを追加します。

ステップ 4 [NAT ルールの追加（Add NAT Rule）] ウィンドウで、次を選択します。

a) [NAT ルール（NAT Rule）] に [手動 NAT ルール（Manual NAT Rule）] を選択します。

b) [タイプ（Type）] に [スタティック（Static）] を選択します。

c) [インターフェイスオブジェクト（Interface Objects）] タブで、送信元と宛先のインターフェイス オブジェクトを選択します。

（注） このインターフェイス オブジェクトは、リモート アクセス VPN ポリシーで選択したインターフェイスと同じである必要があります。

詳細については、リモートアクセス VPN のアクセス インターフェイスの設定（1115 ページ）を参照してください。

a) [変換（Translation）] タブで送信元と宛先のネットワークを選択します。

- [元の送信元（Original Source）] および [変換済み送信元（Translated Source）]
- [元の宛先（Original Destination）] および [変換済み宛先（Translated Destination）]

ステップ 5 [詳細（Advanced）] タブで [宛先インターフェイスでプロキシ ARP を使用しない（Do not proxy ARP on Destination interface）] を選択します。

[宛先インターフェイスでプロキシ ARP を使用しない（Do not proxy ARP on Destination Interface）]：マッピング IP アドレスへの着信パケットのプロキシ ARP を無効にします。マッピング インターフェイスと同じネットワーク上のアドレスを使用した場合、システムはプロキシ ARP を使用してマッピング アドレスのすべての ARP 要求に応答することで、マッピング アドレスを宛先とするトラフィックを代行受信します。この方法では、デバイスがその他のネットワークのゲートウェイである必要がないため、ルーティングが簡略化されます。必要に応じてプロキシ ARP をディセーブルにできます。その場合は、アップストリーム ルータの適切なルートがあることを確認する必要があります。

ステップ 6 [OK] をクリックします。

DNS の設定

リモート アクセス VPN を使用するには、Firepower Threat Defense の各デバイスで DNS を設定します。DNS がないと、デバイスは AAA サーバ名、名前付き URL、FQDN またはホスト名を持つ CA サーバを解決できません。IP アドレスのみを解決できます。

ステップ 1 DNS サーバの詳細とドメイン ルックアップ インターフェイスを [プラットフォーム設定（Platform Settings）] を使用して設定します。詳細については、DNS の設定（1360 ページ）および DNS サーバ グループ オブジェクト（601 ページ）を参照してください。

ステップ 2 VNP ネットワーク経由で DNS サーバに到達可能な場合は、リモート アクセス VPN トンネルを介して DNS トラフィックを許可するためのスプリット トンネルをグループ ポリシーに設定します。詳細については、「グループ ポリシー オブジェクトの設定（624 ページ）」を参照してください。

AnyConnect クライアント プロファイル XML ファイルの追加

AnyConnect クライアント プロファイルは、設定パラメータのグループで、動作や表示の設定にクライアントが使用する XML ファイル内に保存されます。これらのパラメータ（XML タ

グ）には、ホストコンピュータの名前とアドレス、および追加のクライアント機能を有効にする設定が含まれています。

AnyConnect プロファイル エディタを使用すると、AnyConnect クライアント プロファイルを作成できます。このエディタは、AnyConnect ソフトウェア パッケージの一部として利用できる GUI ベースの設定ツールです。これは、Firepower Management Center の外部で実行する独立したプログラムです。AnyConnect プロファイル エディタの使用の詳細については、『*Cisco AnyConnect Secure Mobility Client Administrator Guide*』を参照してください。

始める前に

Firepower Threat Defense リモート アクセス VPN ポリシーには VPN クライアントに割り当てる AnyConnect クライアント プロファイルが必要です。クライアント プロファイルはグループ ポリシーに関連付けられます。

AnyConnect プロファイル エディタはシスコのソフトウェア ダウンロード センターからダウンロードします。

ステップ 1 [デバイス（Devices）] > [VPN] > [リモート アクセス（Remote Access）]。

ステップ 2 リストから既存のリモート アクセス VPN ポリシーを選択し、対応する [編集（Edit）] アイコンをクリックします。
リモート アクセス VPN のポリシーに設定されている接続プロファイルのリストが表示されます。

ステップ 3 AnyConnect クライアント プロファイルを更新する接続プロファイルを選択し、[編集（Edit）] アイコンをクリックします。

ステップ 4 [追加（Add）] アイコンをクリックしてグループ ポリシーを追加するか、または [グループ ポリシーの編集（Edit Group Policy）] > [全般（General）] > [AnyConnect] をクリックします。

ステップ 5 リストからクライアント プロファイルを選択するか、または [追加（Add）] アイコンをクリックして新しいプロファイルを追加します。

a) AnyConnect プロファイルの [名前（Name）] を指定します。

b) [参照（Browse）] をクリックし、AnyConnect プロファイルの XML ファイルを選択します。

（注） 二要素認証の場合、AnyConnect クライアント プロファイル XML ファイルでタイムアウトが 60 秒以上に更新されていることを確認してください。

c) **[保存（Save）]** をクリックします。

（オプション）スプリット トンネリングの設定

スプリット トンネルではセキュア トンネル経由のリモート ネットワークへの VPN 接続が可能ですが、VPN トンネル外のネットワークにも接続できます。VPN ユーザがリモートアクセス VPN に接続されている間、外部ネットワークにアクセスできるようにするには、スプリット トンネルを設定します。スプリットトンネル リストを設定するには、標準アクセス リストまたは拡張アクセス リストを作成する必要があります。

詳細については、グループ ポリシーの設定 （1123 ページ）を参照してください。

ステップ 1 [デバイス（Devices）] > [VP] > [リモート アクセス（Remote Access）] を選択します。

ステップ 2 リストから既存のリモート アクセス ポリシーを選択し、対応する編集アイコンをクリックします。

ステップ 3 接続プロファイルを選択して [編集（Edit）] アイコンをクリックします。

ステップ 4 [追加（Add）] アイコンをクリックしてグループ ポリシーを追加します。または、[グループポリシーの編集（Edit Group Policy）] > [全般（General）] > [スプリットトンネリング（Split Tunneling）] をクリックします。

ステップ 5 [IPv4スプリットトンネリング（IPv4 Split Tunneling）] または [IPv6スプリットトンネリング（IPv6 Split Tunneling）] リストから、[以下に指定したネットワークを除外する（Exclude networks specified below）] を選択し、VPN トラフィックから除外するネットワークを選択します。
スプリット トンネリング オプションをこのままにした場合、エンドポイントからのすべてのトラフィックは VPN 接続経由で送信されます。

ステップ 6 [標準アクセスリスト（Standard Access List）] または [拡張アクセスリスト（Extended Access List）] をクリックし、ドロップダウンからアクセス リストを選択するか、新しいアクセス リストを追加します。

ステップ 7 新しい標準アクセス リストまたは拡張アクセス リストを追加する場合は、次の手順を実行します。

a) 新しいアクセス リストの [名前（Name）] を指定し、[追加（Add）] をクリックします。

b) [アクション（Action）] から [許可（Allow）] を選択します。

c) VPN トンネル上で許可するネットワーク トラフィックを選択し、[追加（Add）] をクリックします。

ステップ 8 **[保存（Save）]** をクリックします。

関連トピック

アクセス リスト （610 ページ）

設定の確認

ステップ 1 外部ネットワークのマシンで Web ブラウザを開きます。

ステップ 2 リモート アクセス VPN ゲートウェイとして設定されている FTD デバイスの URL を入力します。

ステップ 3 プロンプトが表示されたらユーザ名とパスワードを入力し、[ログオン（Logon）] をクリックします。

（注） システムに AnyConnect がインストールされている場合は、VPN に自動的に接続されます。

AnyConnect がインストールされていない場合は、AnyConnect クライアントをダウンロードするように求められます。

ステップ 4 まだインストールされていない場合は AnyConnect をダウンロードし、VPN に接続します。
AnyConnect クライアントは自身をインストールします。認証が成功すると、Firepower Threat Defense リモート アクセス VPN ゲートウェイに接続されます。該当するアイデンティティ ポリシーまたは QoS ポリシーは、リモート アクセス VPN ポリシーの設定に従って適用されます。

オプションのリモート アクセス VPN 設定

接続プロファイルの設定

リモート アクセス VPN ポリシーには、特定のデバイスを対象とする接続プロファイルが含まれています。これらのポリシーはトンネル自体の作成に関連しています。たとえば AAA を行う方法、アドレス（DHCP やアドレス プール）を VPN クライアントに割り当てる方法などです。また、Firepower Threat Defense デバイスで設定された（または AAA サーバから得られる）グループ ポリシーで識別されるユーザ属性も、これらに含まれます。また、デバイスには *DefaultWEBVPNGroup* という名前のデフォルト接続プロファイルもあります。ウィザードを使って設定された接続プロファイルがリストに表示されます。

ステップ 1 **[Devices]** > **[VPN]** > **[Remote Access]**を選択します。

ステップ 2 リストから既存のリモート アクセス VPN ポリシーを選択し、対応する [編集（Edit）] アイコンをクリックします。

ステップ 3 接続プロファイルを選択し、対応する編集アイコンをクリックします。
[接続プロファイルの編集（edit connection profile）] ページが表示されます。

ステップ 4 （オプション）複数の接続プロファイルを追加します。
複数の接続プロファイルの設定 （1105 ページ）

ステップ 5 VPN クライアントの IP アドレスを設定します。
VPN クライアントの IP アドレスの設定 （1106 ページ）

ステップ 6 （オプション）リモート アクセス VPN の AAA 設定を更新します。
リモート アクセス VPN 認証 （1088 ページ）

ステップ 7 （オプション）エイリアスを作成または更新します。
接続プロファイルのエイリアスの作成または更新 （1114 ページ）

ステップ 8 接続プロファイルを保存します。

複数の接続プロファイルの設定

別のグループの VPN ユーザに異なる権限を付与する場合は、各ユーザ グループの特定の接続プロファイルまたはグループ ポリシーを設定することができます。たとえば、経理グループ、カスタマー サポート グループ、および MIS（経営情報システム）グループが、プライベート ネットワークのそれぞれ異なる部分にアクセスできるようにする場合が考えられます。また、MIS に所属する特定のユーザには、他の MIS ユーザにはアクセスできないシステムにアクセスを許可する場合があります。接続プロファイルとグループ ポリシーにより、このような柔軟な設定を安全に実行することができます。

リモート アクセス ポリシー ウィザードを使用して VPN ポリシーを作成する場合に設定できる接続プロファイルは 1 つのみです。接続プロファイルは後で追加できます。また、デバイスには *DfaultWEBVPNGroup* というデフォルトの接続プロファイルもあります。

始める前に

リモートアクセス ポリシー ウィザードを使用し、接続プロファイルでリモートアクセス VPN が設定されていることを確認します。

ステップ 1 Firepower Management Center の Web インターフェイスで、[デバイス（Devices）] > [VPN] > [リモート アクセス（Remote Access）] を選択します。
既存のリモート アクセス ポリシーがリストされます。

ステップ 2 リストから既存のリモートアクセス VPN ポリシーを選択し、対応する [編集（Edit）] アイコンをクリックします。

ステップ 3 [追加（Add）] アイコンをクリックし、[接続プロファイルの追加（Add Connection Profile）] ウィンドウで次の項目を指定します。

a) [接続プロファイル（Connection Profile）]：リモート ユーザが VPN 接続のために使用する名前を指定します。接続プロファイルにはリモートユーザによる VPN デバイスへの接続方法を定義する一連のパラメータが含まれます。

b) [クライアントアドレスの割り当て（Client Address Assignment）]：リモート クライアントの IP アドレスは、ローカルの IP アドレス プール、DHCP サーバ、および AAA サーバから割り当てられます。

c) [AAA]：セキュア VPN ゲートウェイとして機能する管理対象デバイスが、どのユーザに（認証）、何を許可し（承認）、そのユーザが何を実行したか（アカウンティング）を判断できるようにAAAサーバを設定します。

d) [エイリアス（Aliases）]：接続プロファイルの代替名または URL を指定します。リモート アクセス VPN 管理者は、エイリアス名とエイリアス URL を有効または無効にできます。VPN ユーザは、AnyConnect VPN クライアントを使用して Firepower Threat Defense デバイスのリモート アクセス VPN に接続する場合にエイリアス名を使用できます。

ステップ 4 **[保存（Save）]** をクリックします。

関連トピック

接続プロファイルの設定 （1105 ページ）

VPN クライアントの IP アドレスの設定

クライアント アドレスの割り当ては、リモート アクセス VPN ユーザ用の IP アドレスを割り当てる手段です。

リモート VPN クライアントの IP アドレスは、ローカルの IP アドレス プール、DHCP サーバ、および AAA サーバから割り当てように設定できます。最初に AAA サーバが割り当てられ、その後で他のものが割り当てられます。[詳細（Advanced）] タブで [クライアント アドレスの割り当て（Client Address Assignment）] ポリシーを設定して、割り当て基準を定義します。この接続プロファイルに関連付けられているグループ ポリシーやシステムのデフォルト グループ ポリシーである [DfltGrpPolicy] で定義された IP プールが存在しない場合、この接続プロファイルで定義されている IP プールのみが使用されます。

[IPv4 アドレス プール（IPv4 Address Pools）]：SSL VPN クライアントは、Firepower Threat Defense デバイスに接続したときに新しい IP アドレスを受け取ります。アドレス プールでは、

リモート クライアントが受け取ることのできるアドレス範囲が定義されます。既存の IP アドレス プールを選択します。IPv4 および IPv6 アドレスそれぞれに最大 6 つのプールを追加できます。

（注） Firepower Management Center の既存の IP プールから IP アドレスを使用するか、または [追加（Add）] オプションを使用して新しいプールを作成できます。また、[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [アドレスプール（Address Pools）] パスを使用して、Firepower Management Center に IP プールを作成することもできます。詳細については、アドレス プール （633 ページ）を参照してください。

ステップ 1 Firepower Management Center の Web インターフェイスで、[デバイス（Devices）] > [VPN] > [リモート アクセス（Remote Access）] を選択します。
既存のリモート アクセス ポリシーがリストされます。

ステップ 2 リストから既存のリモート アクセス VPN ポリシーを選択し、対応する [編集（Edit）] アイコンをクリックします。

ステップ 3 更新する接続プロファイルを選択し、対応する [編集（Edit）] アイコンをクリックして、[クライアントアドレスの割り当て（Client Address Assignment）] タブを選択します。

ステップ 4 [アドレスプール（Address Pools）] で次の項目を選択します。

a) [追加（Add）] アイコンをクリックして IP アドレスを追加し、[IPv4] または [IPv6] を選択して対応するアドレス プールを追加します。利用可能なプールから IP アドレス プールを選択し、[追加（Add）] をクリックします。

（注） 複数の Firepower Threat Defense デバイス間でリモート アクセス VPN ポリシーを共有する場合は、すべてのデバイスが同じアドレス プールを共有することに留意してください。ただし、デバイスレベルのオブジェクト オーバーライドを使用して、グローバル定義をデバイスごとの一意なアドレス プールに置き換える場合を除きます。NAT を使用していないデバイスでアドレスが重複しないようにするには、一意なアドレス プールが必要です。

b) 新しい IPv4 または IPv6 アドレス プールを追加するには、[アドレスプール（Address Pools）] ウィンドウで [追加（Add）] アイコンを選択します。IPv4 プールを選択する場合は、開始と終了の IP アドレスを提供します。新しい IPv6 アドレス プールを含めることを選択する場合は、1 ～ 16384 の範囲の [アドレス数（Number of Addresses）] を入力します。オブジェクトが多数のデバイス間で共有される場合は、IP アドレスの競合を回避するために、[オーバーライドを許可（Allow Overrides）] オプションを選択します。詳細については、アドレス プール （633 ページ）を参照してください。

c) [OK] をクリックします。

ステップ 5 [DHCPサーバ（DHCP Servers）] で次の項目を選択します。

（注） DHCP サーバ アドレスは、IPv4 アドレスでのみ設定可能です。

a) 名前と DHCP（Dynamic Host Configuration Protocol）のサーバ アドレスをネットワーク オブジェクトとして指定します。オブジェクト リストからサーバを選択するには、[追加（Add）] アイコンを選択します。DHCP サーバを削除するには、その行で [削除（Delete）] アイコンを選択します。

b) [新しいネットワーク オブジェクト（New Network Objects）] ウィンドウで [追加（Add）] アイコンを選択し、新しいネットワーク オブジェクトを追加します。新しいオブジェクト名、説明、ネットワークを入力し、必要に応じて [オーバーライドを許可（Allow Overrides）] オプションを選択します。詳細については、ネットワーク オブジェクトの作成 （527 ページ）およびオブジェクトのオーバーライドの許可 （524 ページ）を参照してください。

c) [OK] をクリックします。

ステップ 6 [保存（Save）] をクリックします。

関連トピック

接続プロファイルの設定 （1105 ページ）

リモートアクセス VPN の AAA 設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス（Access）
エクスポート制御機能が有効なスマート ライセンス アカウントに関連付けられている次の AnyConnect ライセンスのいずれか。 • AnyConnect VPN Only • AnyConnect Plus • AnyConnect Apex	該当なし	FTD	いずれか（Any）	Admin

ステップ 1 **[Devices]** > **[VPN]** > **[Remote Access]**を選択します。

ステップ 2 リストから既存のリモート アクセス VPN ポリシーを選択し、対応する [編集（Edit）] アイコンをクリックします。

ステップ 3 AAA 設定が更新されるように接続プロファイルを選択し、対応する [編集（Edit）] アイコンをクリックしてから、[AAA] タブをクリックします。

ステップ 4 [認証（Authentication）] で次の項目を選択します。

- [認証方式（Authentication Method）]：ユーザに対してネットワークとネットワーク サービスへのアクセスを許可する前に、ユーザの識別方法を決定します。有効なユーザ クレデンシャル（通常は、ユーザ名とパスワード）を要求することで、アクセスが制御されます。また、クライアントからの証明書

も含まれます。サポートされている認証方式は、[AAA のみ（AAA only）]、[クライアント証明書のみ（Client Certificate only）]、および [AAA とクライアント証明書（AAA + Client Certificate）] です。

[認証方式（Authentication Method）] の選択に応じて、次のようになります。

- [AAA のみ（AAA only）] : [認証サーバ（Authentication Server）] に [RADIUS] を選択した場合、デフォルトで許可サーバは同じ値になります。ドロップダウン リストから [アカウンティング サーバ（Accounting Server）] を選択します。認証サーバ ドロップダウン リストから [AD] と [LDAP] を選択した場合は常に、[認証サーバ（Authorization Server）] と [アカウンティング サーバ（Accounting Server）] をそれぞれ手動で選択する必要があります。
- [クライアント証明書のみ（Client Certificate Only）] : 各ユーザはクライアント証明書を使用して認証されます。クライアント証明書は、VPN クライアント エンドポイントで設定する必要があります。デフォルトでは、ユーザ名はクライアント証明書フィールド CN および OU から派生します。クライアント証明書の他のフィールドにユーザ名が指定されている場合は、[プライマリ（Primary）] と [セカンダリ（Secondary）] フィールドを使用して適切なフィールドをマップします。

  クライアント証明書のユーザ名が含まれる [マップ固有フィールド（Map Specific Field）] オプションを選択すると、[プライマリ（Primary）] および [セカンダリ（Secondary）] フィールドに [CN（一般名）（CN (Common Name)）] と [OU（組織ユニット）（OU (Organisational Unit)）] のデフォルト値がそれぞれ表示されます。[DN全体をユーザ名として使用（Use entire DN as username）] オプションを選択した場合、ユーザ ID が自動的に取得されます。識別名（DN）は、個々のフィールドから構成される一意の識別子であり、ユーザを接続プロファイルと照合するときに識別子として使用できます。DN ルールは、拡張証明書認証に使用されます。

  [固有のフィールドをマップ（Map specific field）] オプションに関連する [プライマリ（Primary）] フィールドと [セカンダリ（Secondary）] フィールドには、次の共通の値が含まれています。

  - C（国）
  - CN（一般名）
  - DNQ（DN 修飾子）
  - EA（電子メール アドレス）
  - GENQ（世代識別子）
  - GN（姓名の名）
  - I（イニシャル）
  - L（地名）
  - N（名前）
  - O（組織）
  - OU（組織ユニット）
  - SER（シリアル番号）
  - SN（姓名の姓）

- SP（都道府県）
- T（タイトル）
- UID（ユーザ ID）
- UPN（ユーザ プリンシパル名）

- [クライアント証明書とAAA（Client Certificate & AAA）]：各ユーザはクライアント証明書とAAAサーバの両方を使用して認証されます。

  どの認証方式を選択する場合にも、[ユーザが承認データベースに存在するときにのみ接続を許可（Allow connection only if user exists in authorization database）] を選択または選択解除します。

- [認証サーバ（Authentication Server）]：認証とは、ユーザに対してネットワークとネットワーク サービスへのアクセスを許可する前に、ユーザの識別を行う方法です。認証には、有効なユーザ クレデンシャル、証明書、またはその両方が必要です。認証は、単独で使用することも、認可およびアカウンティングとともに使用することもできます。

  以前にリモート アクセス VPN ユーザを認証するように設定した LDAP または AD レルムか RADIUS サーバ グループを指定します。

- [セカンダリ認証を使用（Use secondary authentication）]：VPN セッションのセキュリティを強化するため、プライマリ認証の他にセカンダリ認証を設定します。セカンダリ認証は、[AAA のみ（AAA only）] と [クライアント証明書と AAA（Client Certificate & AAA）] の認証方式にのみ適用されます。

  セカンダリ認証はオプションの機能であり、2 つのセットのユーザ名とパスワードを AnyConnect ログイン画面に入力するにはVPNユーザが必要です。認証サーバまたはクライアント証明書からセカンダリ ユーザ名を事前入力するように設定することもできます。リモート アクセス VPN 認証は、プライマリとセカンダリの両方の認証が成功した場合にのみ許可されます。いずれの認証サーバに到達できない場合、1 つの認証が失敗すると、VPN 認証が拒否されます。

  セカンダリ認証の設定前に、2つ目のユーザ名とパスワードのセカンダリ認証のサーバグループ（AAA サーバ）を設定する必要があります。たとえば、プライマリ認証サーバをLDAPまたはActive Directoryレルムに、セカンダリ認証を RADIUS サーバに設定できます。

  （注）　デフォルトでは、セカンダリ認証は必要ありません。

  [認証サーバ（Authentication Server）]：VPN ユーザのセカンダリ ユーザ名とパスワードを提供するセカンダリ認証サーバ。

  [セカンダリ認証のユーザ名（Username for secondary authentication）] で次の項目を選択します。

  - [プロンプト（Prompt）]：VPN ゲートウェイへのログイン中にユーザ名とパスワードを入力するようユーザに要求します。
  - [プライマリ認証ユーザ名を使用（Use primary authentication username）]：プライマリとセカンダリの両方の認証にプライマリ認証サーバからユーザ名が取得されます。パスワードは 2 つ入力する必要があります。

- [クライアント証明書からのユーザ名をマップ（Map username from client certificate）]：クライアント証明書からセカンダリ ユーザ名が事前に入力されます。
  - クライアント証明書のユーザ名を含む [固有のフィールドをマップ（Map specific field）] オプションを選択する場合。[プライマリ（Primary）] フィールドと [セカンダリ（Secondary）] フィールドには、デフォルト値の [CN（共通名）（CN (Common Name)）] と [組織ユニット（OU）（OU (Organisational Unit)）] がそれぞれ表示されます。[DN（識別名）全体をユーザ名として使用（Use entire DN (Distinguished Name) as username）] オプションを選択した場合はユーザ ID が自動的に取得されます。

    プライマリとセカンダリのフィールドのマッピングの詳細については、「**認証方式**」の説明を参照してください。
  - [ユーザ ログイン ウィンドウに証明書からユーザ名を事前に入力（Prefill username from certificate on user login window）]：ユーザが AnyConnect VPN クライアント経由で接続したときにクライアント証明書からセカンダリ ユーザ名を事前に入力します。
    - [ログイン ウィンドウでユーザ名を非表示にする（Hide username in login window）]：セカンダリ ユーザ名はクライアント証明書から事前に入力されますがユーザには表示されず、ユーザが事前に入力されたユーザ名を変更しないようにします。

- [VPN セッションのセカンダリ ユーザ名を使用（Use secondary username for VPN session）]：VPN セッション中のユーザ アクティビティのレポートにセカンダリ ユーザ名を使用します。

ステップ 5 [認可（Authorization）] で次の項目を選択します。

- [認可（Authorization Server）]：認証の完了後、認可によって、認証済みの各ユーザが使用できるサービスおよびコマンドが制御されます。認可は、ユーザが実行を認可されていることを示す属性のセット、実際の機能、および制限事項をアセンブルすることによって機能します。認可を使用しない場合は、認証が単独で、認証済みのすべてのユーザに対して同じアクセス権を提供します。認可には、認証が必要です。RADIUS サーバのみが承認サービスでサポートされます。リモート アクセス VPN 認可の仕組みについては、権限および属性のポリシー実施の概要（1090 ページ）を参照してください。

  リモート アクセス VPN ユーザを承認するように事前設定された RADIUS サーバ グループ オブジェクトを入力または選択します。

  RADIUS サーバが接続プロファイルのユーザ承認用に構成されている場合、リモート アクセス VPN システムの管理者は、ユーザまたはユーザ グループに複数の承認属性を構成できます。RADIUS サーバに構成される承認属性は、ユーザまたはユーザ グループに固有にできます。ユーザが認証されると、これらの特定の承認属性が Firepower Threat Defense デバイスにプッシュされます。

  （注） 許可サーバから所得した AAA サーバ属性は、グループ ポリシーまたは接続プロファイルで事前に設定されていた可能性がある属性値を上書きします。

- 必要な場合は、[ユーザが承認データベースに存在するときにのみ接続を許可（Allow connection only if user exists in authorization database）] をオンにします。

  有効にすると、システムは正常に接続するために、クライアントのユーザ名が承認データベース内に存在することを確認します。ユーザ名が承認データベース内に存在しない場合、接続が拒否されます。

ステップ 6 [アカウンティング（Accounting）] で次の項目を選択します。

- [アカウンティングサーバ（Accounting Server）]：アカウンティングは、ユーザがアクセスしているサービス、およびユーザが消費しているネットワーク リソース量を追跡するために使用されます。AAAアカウンティングがアクティブになると、ネットワーク アクセス サーバはユーザ アクティビティを RADIUS サーバに報告します。アカウンティング情報には、セッションの開始時刻と停止時刻、ユーザ名、セッションごとのデバイスを通過したバイト数、使用されたサービス、および各セッションの時間が含まれています。このデータを、ネットワーク管理、クライアント請求、または監査のために分析できます。アカウンティングは、単独で使用するか、認証および認可とともに使用することができます。

  リモート アクセス VPN セッションを構成するために使用される RADIUS サーバ グループ オブジェクトを指定します。

ステップ 7 [詳細設定（Advanced Settings）] で次の項目を選択します。

- [ユーザ名からレルムを削除（Strip Realm from username）]：ユーザ名を AAA サーバに渡す前に、ユーザ名からレルムを削除するには選択します。たとえば、このオプションを選択して、*domain\username* を指定した場合、ユーザ名からドメインが削除され、認証用の AAA サーバに送信されます。デフォルトでは、このオプションはオフになっています。
- [ユーザ名からグループを削除（Strip Group from username）]：ユーザ名を AAA サーバに渡す前に、ユーザ名からグループを削除するには選択します。デフォルトでは、このオプションはオフになっています。

  （注） レルムとは管理ドメインのことです。これらのオプションを有効にすると、ユーザ名だけに基づいて認証できます。これらのオプションを任意に組み合わせて有効にできます。ただし、サーバが区切り文字を解析できない場合は、両方のチェックボックスをオンにする必要があります。

- [パスワード管理（Password Management）]：リモート アクセス VPN ユーザのパスワードを管理できるようにします。パスワードが期限切れになる前に通知するか、パスワードが期限切れになる日に通知するかを選択します。

ステップ 8 **[保存（Save）]** をクリックします。

の RADIUS サーバ属性 Firepower Threat Defense

Firepower Threat Defense デバイスは、リモート アクセス VPN ポリシーで認証および/または承認のために設定された外部 RADIUS サーバから、VPN 接続にユーザ承認属性（ユーザの権利または権限とも呼ばれる）を適用することをサポートしています。

（注） Firepower Threat Defense デバイスはベンダー ID 3076 の属性をサポートしています。

次のユーザ認可属性が Firepower Threat Defense デバイスから RADIUS サーバに送信されます。

- RADIUS 属性 146 および 150 は、認証および認可の要求の場合に Firepower Threat Defense デバイスから RADIUS サーバに送信されます。
- 3 つの属性（146、150、151）はすべて、アカウンティングの開始、暫定更新、および停止要求のために、Firepower Threat Defense デバイスから RADIUS サーバに送信されます。

表 *83 : Firepower Threat Defense* から *RADIU* サーバに送信される *RADIUS* 属性

属性	Attribute Number	構文、タイプ	シングルまたはマルチ値	説明または値
接続プロファイル名またはトンネル グループ名。	146	文字列	シングル	1 ～ 253 文字
クライアント タイプ（Client Type）	150	整数	シングル	2 = AnyConnect クライアント SSL VPN、6 = AnyConnect クライアント IPsec VPN（IKEv2）
セッション タイプ	151	整数	シングル	1 = AnyConnect クライアント SSL VPN、2 = AnyConnect クライアント IPsec VPN（IKEv2）

表 *84 :* 送信される *RADIUS* 属性 *Firepower Threat Defense*

属性	Attribute Number	構文、タイプ	シングルまたはマルチ値	説明または値
Access-List-Inbound	86	文字列	シングル	アクセス リスト属性の両方が、FTDデバイスで設定されている ACL の名前を使用します。スマート CLI 拡張アクセス リストのオブジェクト タイプを使用して、これらの ACL を作成します（**[デバイス（Device）] > [詳細設定（Advanced Configuration）] > [スマートCLI（Smart CLI）] > [オブジェクト（Object）]** を選択します）。 これらの ACL は、着信（FTD デバイスに入るトラフィック）または発信（FTDデバイスから出るトラフィック）方向のトラフィックフローを制御します。
Access-List-Outbound	87	文字列	シングル	
Address-Pools	217	文字列	シングル	FTDデバイスで定義されたネットワークオブジェクトの名前。RA VPN へのクライアント接続のアドレスプールとして使用されるサブネットを識別します。[Objects] ページでネットワークオブジェクトを定義します。
Banner1	15	文字列	シングル	ユーザがログインするときに表示されるバナー。

属性	Attribute Number	構文、タイプ	シングルまたはマルチ値	説明または値
Banner2	36	文字列	シングル	ユーザがログインするときに表示されるバナーの 2 番目の部分。Banner2 は Banner1 に付加されます。
ダウンロード可能 ACL（Downloadable ACLs）	Cisco-AV-Pair	merge-dacl {before-avpair | after-avpair}		Cisco-AV-Pair 構成でサポートされます。
Filter ACLs	86、87	文字列	シングル	フィルタ ACL は、RADIUS サーバで ACL 名で参照されます。ACL 設定が Firepower Threat Defense デバイス上にすでに存在していて、RADIUS 承認時に使用できるようにする必要があります。 86 = アクセスリスト-インバウンド 87 = アクセスリスト-アウトバウンド
Group-Policy	25	文字列	シングル	接続に使用されるグループポリシー。RA VPN の [Group Policy] ページでグループポリシーを作成する必要があります。次の形式のいずれかを使用できます。 • グループ ポリシー名 • OU=グループ ポリシー名 • OU=グループ ポリシー名;
Simultaneous-Logins	2	整数	シングル	ユーザが確立を許可されている個別の同時接続の数（0 ～ 2147483647）。
VLAN	140	整数	シングル	ユーザの接続を制限する VLAN（0 ～ 4094）。FTD デバイスのサブインターフェイスでも、この VLAN を設定する必要があります。

接続プロファイルのエイリアスの作成または更新

エイリアスには、特定の接続プロファイルの代替名または URL が含まれます。リモート アクセス VPN 管理者は、エイリアス名とエイリアス URL を有効または無効にできます。VPN ユーザは、Firepower Threat Defense デバイスに接続するときにエイリアス名を選択できます。このデバイスに設定されているすべての接続のエイリアス名の表示をオンまたはオフにできます。また、リモート アクセス VPN 接続の開始時にエンドポイントが選択できるエイリアス URL のリストを設定することもできます。ユーザがエイリアス URL を使用して接続すると、システムはエイリアス URL と一致する接続プロファイルを使用して自動的にそのユーザをログに記録します。

ステップ 1 **[Devices]** > **[VPN]** > **[Remote Access]**を選択します。

ステップ 2 使用可能な VPN ポリシーのリストから、設定を変更するポリシーを選択します。

ステップ 3 接続プロファイルを選択し、対応する編集アイコンをクリックします。

ステップ 4 [エイリアス（Aliases）] タブをクリックします。

ステップ 5 エイリアス名を追加するには、次の手順を実行します。

a) [エイリアス名（Alias Names）] の [追加（Add）] をクリックします。
b) [エイリアス名（Alias Name）] を指定します。
c) エイリアスを有効にするには、各ウィンドウで [有効（Enabled）] チェックボックスをオンにします。
d) [OK] をクリックします。

ステップ 6 エイリアス URL を追加するには、次の手順を実行します。

a) [エイリアスURL（Alias URL）] の [追加（Add）] をクリックします。
b) リストから [エイリアスURL（Alias URL）] を選択するか、新しい URL オブジェクトを作成します。詳細については、URL オブジェクトの作成 （533 ページ）を参照してください。
c) エイリアスを有効にするには、各ウィンドウで [有効（Enabled）] チェックボックスをオンにします。
d) [OK] をクリックします。

- エイリアス名またはエイリアス URL を編集するには、[編集（Edit）] アイコンをクリックします。
- エイリアス名またはエイリアス URL を削除するには、その行で [削除（Delete）] アイコンをクリックします。

ステップ 7 **[保存（Save）]** をクリックします。

関連トピック

接続プロファイルの設定 （1105 ページ）

リモートアクセス VPN のアクセス インターフェイスの設定

[アクセス インターフェイス（Access Interface）] テーブルには、デバイス インターフェイスを含むインターフェイス グループとセキュリティ ゾーンが示されています。これらは、リモート アクセス SSL または IPsec IKEv2 VPN 接続用に設定されています。このテーブルには、各インターフェイス グループまたはセキュリティ ゾーン、インターフェイスで使用されるインターフェイス トラストポイント、および Datagram Transport Layer Security（DTLS）が有効かどうかが表示されます。

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス（Access）
エクスポート制御機能が有効なスマート ライセンス アカウントに関連付けられている次の AnyConnect ライセンスのいずれか。 • AnyConnect VPN Only • AnyConnect Plus • AnyConnect Apex	該当なし	FTD	いずれか（Any）	Admin

ステップ 1 **[Devices]** > **[VPN]** > **[Remote Access]**を選択します。

ステップ 2 リストから既存のリモート アクセス VPN ポリシーを選択し、対応する [編集（Edit）] アイコンをクリックします。

ステップ 3 [アクセスインターフェイス（Access Interface）] タブをクリックします。

ステップ 4 アクセスインターフェイスを追加するには、[追加（Add）] アイコンを選択し、[アクセスインターフェイスの追加（Add Access Interface）] ウィンドウで以下に対する値を指定します。

a) [アクセスインターフェイス（Access Interface）]：インターフェイスが属するインターフェイス グループまたはセキュリティ ゾーンを選択します。

インターフェイス グループまたはセキュリティ ゾーンは、ルーテッド タイプでなければなりません。他のインターフェイス タイプは、リモート アクセス VPN 接続ではサポートされていません。

b) 次のオプションを選択して、アクセスインターフェイスに [プロトコル（Protocol）] オブジェクトを関連付けます。

- [IPSet-IKEv2の有効化（Enable IPSet-IKEv2）]：**IKEv2** 設定を有効にするには、このオプションを選択します。
- [SSL の有効化（Enable SSL）]：**SSL** 設定を有効にするには、このオプションを選択します。
  - [Datagram Transport Layer Security の有効化（Enable Datagram Transport Layer Security）] を選択します。

    選択すると、インターフェイスで Datagram Transport Layer Security（DTLS）がイネーブルになり、AnyConnect VPN Client は 2 つの同時トンネル（SSL トンネルと DTLS トンネル）を使用して SSL VPN 接続を確立できます。

DTLS を有効にすると、一部の SSL 接続で発生する遅延および帯域幅の問題が回避され、パケット遅延の影響を受けやすいリアルタイム アプリケーションのパフォーマンスが向上します。

- [インターフェイス固有のアイデンティティ証明書を設定する（Configure Interface Specific Identity Certificate）] チェックボックスをオンにして、ドロップダウン リストから [インターフェイスアイデンティティ証明書（Interface Identity Certificate）] を選択します。

  [インターフェイスアイデンティティ証明書（Interface Identity Certificate）] を選択しないと、[トラストポイント（Trustpoint）] がデフォルトで使用されます。

  [インターフェイスアイデンティティ証明書（Interface Identity Certificate）] または [トラストポイント（Trustpoint）] を選択しないと、[SSLグローバルアイデンティティ証明書（SSL Global Identity Certificate）] がデフォルトで使用されます。

c) [OK] をクリックして変更を保存します。

ステップ 5 [アクセス設定（Access Settings）] で次の項目を選択します。

- [ユーザがログイン中に接続プロファイルを選択することを許可する（Allow Users to select connection profile while logging in）]：複数の接続プロファイルがある場合、このオプションを選択すると、ユーザはログイン時に正しい接続プロファイルを選択できます。このオプションを **IPsec-IKEv2** VPN に選択する必要があります。

ステップ 6 [SSL設定（SSL Settings）] で次のオプションを使用します。

- [Web アクセス ポート番号（Web Access Port Number）]：VPN セッションで使用するポート。デフォルト ポートは 443 です。
- [DTLS ポート番号（DTLS Port Number）]：DTLS 接続に使用する UDP ポート。デフォルト ポートは 443 です。
- [SSLグローバルアイデンティティ証明書（SSL Global Identity Certificate）]：[インターフェイス固有のアイデンティティ証明書（Interface Specific Identity Certificate）] が提供されていない場合、選択した [SSLグローバルアイデンティティ証明書（SSL Global Identity Certificate）] がすべての関連インターフェイスに使用されます。

ステップ 7 [IPsec-IKEv2設定（IPsec-IKEv2 Settings）] の場合、リストから [IKEv2アイデンティティ証明書（IKEv2 Identity Certificate）] を選択するか、アイデンティティ証明書を追加します。

ステップ 8 [VPNトラフィックのアクセスコントロール（Access Control for VPN Traffic）] セクションで、アクセス コントロール ポリシーをバイパスする場合に次のオプションを選択します。

- [復号されたトラフィック（sysopt permit-vpn）に対するバイパス アクセス コントロール ポリシー（Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)）]：デフォルトでは、復号されたトラフィックは、アクセス コントロール ポリシーのインスペクションの対象になります。復号されたトラフィック オプションに対してバイパス アクセス コントロール ポリシーを有効にすると、ACL インスペクションがバイパスされますが、AAA サーバからダウンロードされた VPN フィルタ ACL と認証 ACL は、VPN トラフィックに引き続き適用されます。

（注） このオプションを選択した場合は、Firepower Threat Defense デバイスのアクセス コントロール ポリシーの更新 （1100 ページ） で指定したリモート アクセス VPN のアクセス コントロール ポリシーを更新する必要はありません。

ステップ 9 [保存（Save）] をクリックしてアクセス インターフェイスの変更を保存します。

関連トピック

インターフェイス オブジェクト：インターフェイス グループとセキュリティ ゾーン （535 ページ）

リモート アクセス VPN の高度なオプションの設定

Cisco AnyConnect セキュア モビリティ クライアント イメージ

Cisco AnyConnect セキュア モビリティ クライアント イメージ

Cisco AnyConnect セキュア モビリティ クライアントは Firepower Threat Defense デバイスへのセキュアな SSL 接続または IPsec（IKEv2）接続を提供し、これにより、リモート ユーザによる企業リソースへのフル VPN プロファイリングが可能となります。インストール済みのクライアントがない場合、リモート ユーザは、クライアントレス VPN 接続を受け入れるように設定されたインターフェイスの IP アドレスをブラウザに入力し、AnyConnect クライアントをダウンロードしてインストールすることができます。Firepower Threat Defense デバイスは、リモート コンピュータのオペレーティング システムに適合するクライアントをダウンロードします。ダウンロード後に、クライアントがインストールされてセキュアな接続が確立されます。すでにクライアントがインストールされている場合は、ユーザの認証時に Firepower Threat Defense デバイスがクライアントのバージョンを検査し、必要に応じてクライアントをアップグレードします。

リモート アクセス VPN 管理者は、新規または追加の AnyConnect クライアント イメージを VPN ポリシーに関連付けます。管理者は、サポート対象外または期限切れで不要になったクライアント パッケージの関連付けを解除できます。

Firepower Management Center は、ファイル パッケージ名を使用してオペレーティング システムの種類を判別します。ユーザがオペレーティング システム情報を示さずにファイルの名前を変更した場合は、有効なオペレーティング システム タイプをリスト ボックスから選択する必要があります。

シスコのソフトウェア ダウンロード センターを参照して AnyConnect クライアント イメージ ファイルをダウンロードします。

関連トピック

への Cisco AnyConnect Mobility クライアント イメージの追加 Firepower Management Center （1119 ページ）

への Cisco AnyConnect Mobility クライアント イメージの追加 Firepower Management Center

[AnyConnectファイル（AnyConnect File）] オブジェクトを使用して、Cisco AnyConnect Mobility クライアント イメージを Firepower Management Center にアップロードすることもできます。詳細については、FTD ファイル オブジェクト（631 ページ）を参照してください。クライアント イメージの詳細については、Cisco AnyConnect セキュア モビリティ クライアント イメージ（1118 ページ）を参照してください。

特定のクライアント イメージを表示するには、[再注文ボタンの表示（Show re-order buttons）] リンクをクリックします。

（注） すでにインストールされている Cisco AnyConnect クライアント イメージを削除するには、その行の [削除（Delete）] アイコンをクリックします。

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス（Access）
エクスポート制御機能が有効なスマート ライセンス アカウントに関連付けられている次の AnyConnect ライセンスのいずれか。 • AnyConnect VPN Only • AnyConnect Plus • AnyConnect Apex	該当なし	FTD	いずれか（Any）	Admin

ステップ 1 Firepower Management Center Web インターフェイスで、[デバイス（Devices）] > [VPN] > [リモート アクセス（Remote Access）]、リストされている RA VPN ポリシーを選択および編集し、[詳細設定（Advanced）] タブを選択します。 を選択します

ステップ 2 [AnyConnect イメージ（AnyConnect Images）] ダイアログの [使用可能な AnyConnect イメージ（Available AnyConnect Images）] 部分で [追加（Add）] アイコンをクリックします。

ステップ 3 使用可能な AnyConnect イメージの [名前（Name）]、[ファイル名（File Name）]、および [説明（Description）] を入力します。

ステップ 4 [参照（Browse）] をクリックして、アップロードするクライアント イメージを選択する場所に移動します。

ステップ 5 [保存（Save）] をクリックしてイメージを Firepower Management Center にアップロードします。
クライアント イメージを Firepower Management Center にアップロードすると、オペレーティング システムに Firepower Management Center にアップロードされたイメージのプラットフォーム情報が表示されます。

関連トピック

Cisco AnyConnect セキュア モビリティ クライアント イメージ （1118 ページ）

リモート アクセス VPN クライアントに対する AnyConnect イメージの更新

シスコのソフトウェア ダウンロード センターで新しい AnyConnect クライアント更新を入手できる場合は、そのパッケージを手動でダウンロードしてリモート アクセス VPN ポリシーに追加します。それにより、オペレーティング システムに応じて VPN クライアント システム上で新しい AnyConnect パッケージがアップグレードされます。

始める前に

この項の手順は、Firepower Threat Defense VPN ゲートウェイに接続しているリモート アクセス VPN クライアントに新しい AnyConnect クライアント イメージを更新するのに役立ちます。AnyConnect のイメージを更新する前に、次の設定が完了していることを確認します。

- シスコのソフトウェア ダウンロード センターから最新の AnyConnect イメージ ファイルをダウンロードします。
- Firepower Management Center の Web インターフェイスで、[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [VPN] > [AnyConnect ファイル（AnyConnect File）] に移動し、新しいAnyConnect クライアント イメージ ファイルを追加します。

ステップ 1 Firepower Management Center の Web インターフェイスで、[デバイス（Devices）] > [VPN] > [リモート アクセス（Remote Access）] を選択します。

ステップ 2 リストから既存のリモート アクセス ポリシーを選択し、対応する [編集（Edit）] アイコンをクリックします。

ステップ 3 [詳細（Advanced）] > [AnyConnect クライアント イメージ（AnyConnect Client Image）] >[追加（Add）] をクリックします。

ステップ 4 [利用可能なAnyConnectイメージ（Available AnyConnect Images）] からクライアント イメージ ファイルを選択し、[追加（Add）] をクリックします。

必要な AnyConnect クライアント イメージが表示されていない場合は、[追加（Add）] アイコンをクリックして参照し、イメージをアップロードします。

ステップ 5 リモート アクセス VPN ポリシーを保存します。
リモート アクセス VPN ポリシーの変更が展開されると、リモート アクセス VPN ゲートウェイとして設定されている Firepower Threat Defense デバイスで新しい AnyConnect クライアント イメージが更新されます。新しい VPN ユーザが VPN ゲートウェイに接続すると、クライアント イメージのオペレーティング システムに応じて、新しい AnyConnect クライアント イメージがダウンロードされます。既存の VPN ユーザの場合、AnyConnect クライアント イメージは次の VPN セッションで更新されます。

関連トピック

リモート アクセス VPN 接続プロファイル オプション

リモート アクセス VPN のアドレス割り当てポリシー

Firepower Threat Defense デバイスは、IPv4 または IPv6 ポリシーを使用して、リモート アクセス VPN クライアントに IP アドレスを割り当てることができます。複数のアドレス割り当て方式を設定すると、Firepower Threat Defense デバイスは IP アドレスが見つかるまで各オプションを試行します。

IPv4 または IPv6 ポリシー

IPv4 または IPv6 ポリシーを使用すると、リモート アクセス VPN クライアントへの IP アドレスに対応できます。まず、IPv4 ポリシーを試してから、次に IPv6 ポリシーを試す必要があります。

- [承認サーバを使用（Use Authorization Server）]：ユーザごとに外部承認サーバからアドレスを取得します。IP アドレスが設定された承認サーバを使用している場合は、この方式を使用することをお勧めします。アドレス割り当ては、RADIUS ベースの承認サーバでのみサポートされています。AD/LDAP ではサポートされていません。この方法は、IPv4 と IPv6 の両方の割り当てポリシーで使用できます。
- [DHCP を使用（Use DHCP）]：接続プロファイルに設定された DHCP サーバから IP アドレスを取得します。グループ ポリシーで DHCP ネットワーク範囲を設定することによって、DHCP サーバが使用できる IP アドレスの範囲を定義することもできます。DHCP を使用する場合は、[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [ネットワーク（Network）] ペインでサーバを設定します。この方法は IPv4 の割り当てポリシーに使用できます。
- [内部アドレス プールを使用（Use an internal address pool）]：内部的に設定されたアドレス プールは、最も設定が簡単なアドレス プール割り当て方式です。この方式を使用する場合は、[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [アドレス プール（Address Pools）] ペインで IP アドレス プールを作成し、接続プロファイルで同じものを選択します。この方法は、IPv4 と IPv6 の両方の割り当てポリシーで使用できます。
- [IP アドレスが解放された後時間が経ってから IP アドレスを再利用する（Reuse an IP address so many minutes after it is released）]：IP アドレスがアドレス プールに戻った後、IP アドレスの再使用を遅らせます。遅延時間を設けることにより、IP アドレスがすぐに再割り当てされることによって発生する問題がファイアウォールで生じないようにできます。デフォルトでは、遅延はゼロに設定されています。つまり、Firepower Threat Defense デバイスは IP アドレスの再使用の際に遅延を課しません。遅延時間を延長する場合は、IP アドレスを再割り当てするまでの時間を 0 ～ 480 の範囲で指定します。この設定要素は、IPv4 割り当てポリシーで使用できます。

関連トピック

接続プロファイルの設定 （1105 ページ）
リモート アクセス VPN 認証 （1088 ページ）

証明書マップの設定

証明書マップを使用して、証明書フィールドの内容に基づいて接続プロファイルとユーザ証明書をマッチングするルールを定義できます。証明書マップは、セキュア ゲートウェイでの証明書認証に使用されます。

ルール、または証明書マップは、FTD 証明書のマップ オブジェクトについて（632 ページ）で定義されます。

ステップ 1 **[Devices]** > **[VPN]** > **[Remote Access]**を選択します。

ステップ 2 リストから既存のリモート アクセス VPN ポリシーを選択し、対応する [編集（Edit）] アイコンをクリックします。

ステップ 3 **[詳細（Advanced）]** > **[証明書マップ（Certificate Maps）]** をクリックします。

ステップ 4 [証明書グループ照合の全般設定（General Settings for Certificate Group Matching）] ペインで次のオプションを選択します。

優先順位に基づいて選択されます。つまり、最初の選択候補で一致するものが見つからなかった場合、オプション リストの次の候補がマッチングされます。ルールが満たされると、マッピングが実行されます。ルールが満たされない場合、デフォルトの接続プロファイル（下に表示されている）がこの接続に使用されます。次のいずれか、またはすべてのオプションを選択して、認証を確立し、クライアントにマッピングする必要のある接続プロファイル（トンネル グループ）を決定します。

- **グループ URL と証明書マップが異なる接続プロファイルと一致する場合、グループ URL を使用します**
- [設定されているルールを使用して証明書を接続プロファイルと照合（Use the configured rules to match a certificate to a Connection Profile）]：接続プロファイル マップで定義されているルールを使用するには、これを有効にします。

（注） 証明書マッピングを設定することは、証明書に基づく認証を意味します。設定されている認証方法に関係なく、リモート ユーザはクライアント証明書を提供するよう求められます。

ステップ 5 [証明書から接続プロファイルへのマップ（Certificate to Connection Profile Map）] セクションで、[マッピングの追加（Add Mapping）] をクリックし、このポリシーの証明書から接続プロファイルへのマッピングを作成します。

a) [証明書マップ（Certificate Map）] オブジェクトを選択するか、作成します。
b) 証明書マップ オブジェクトのルールが満たされた場合に使用する必要のある [接続プロファイル（Connection Profile）] を選択します。
c) [OK] をクリックして、マッピングを作成します。

ステップ 6 **[保存（Save）]** をクリックします。

グループ ポリシーの設定

グループ ポリシーはグループ ポリシー オブジェクト内に保存される属性と値の一連のペアで、リモート アクセス VPN のエクスペリエンスを定義します。たとえば、グループ ポリシー オブジェクトで、アドレス、プロトコル、接続設定などの一般的な属性を設定します。

ユーザに適用されるグループ ポリシーはVPN トンネルが確立される際に決定されます。RADIUS 承認サーバがグループ ポリシーを割り当てるか、または現在の接続プロファイルから取得されます。

（注） FTD ではグループ ポリシー属性の継承はありません。ユーザについては、グループ ポリシー オブジェクトが全体として使用されます。ログイン時に AAA サーバで特定されたグループ ポリシー オブジェクトが使用されるか、またはこれが指定されていない場合は、VPN 接続に対して設定されたデフォルトのグループ ポリシーが使用されます。指定されたデフォルトのグループ ポリシーはデフォルト値に設定できますが、これは、接続プロファイルに割り当てられ、他のグループ ポリシーがユーザに対して特定されていない場合にのみ使用されます。

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin

ステップ 1 **[Devices]** > **[VPN]** > **[Remote Access]**を選択します。

ステップ 2 リストから既存のリモート アクセス VPN ポリシーを選択し、対応する [編集（Edit）] アイコンをクリックします。

ステップ 3 **[詳細（Advanced）]** > **[グループ ポリシー（Group Policies）]** をクリックします。

ステップ 4 このリモート アクセス VPN ポリシーに関連付けるグループ ポリシーをさらに選択します。これらは、リモート アクセス VPN ポリシー作成中に割り当てられたデフォルトのグループ ポリシーを凌駕するものです。[追加（Add）] をクリックします。

[更新（Refresh）] と [検索（Search）] ユーティリティを使用して、グループ ポリシーを検索します。必要に応じて、新しいグループ ポリシー オブジェクトを追加します。

ステップ 5 利用可能なグループ ポリシーから [グループポリシー（group policies）] を選択し、[追加（Add）] をクリックして選択します。

ステップ 6 [OK] をクリックして、グループ ポリシーの選択を完了します。

関連トピック

グループ ポリシー オブジェクトの設定 （624 ページ）

リモート アクセス VPN の IPsec の設定

IPsec 設定は、リモート アクセス VPN ポリシーを設定する際に、VPN プロトコルとして IPsec を選択した場合にのみ適用可能です。そうでない場合は、[アクセス インターフェイスの編集（Edit Access Interface）] ダイアログボックスを使用して、IKEv2 を有効にすることができます。詳細については、リモートアクセス VPN のアクセス インターフェイスの設定（1115 ページ）を参照してください。

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス（Access）
エクスポート制御機能が有効なスマート ライセンス アカウントに関連付けられている次の AnyConnect ライセンスのいずれか。 • AnyConnect VPN Only • AnyConnect Plus • AnyConnect Apex	該当なし	FTD	いずれか（Any）	Admin

ステップ 1 **[Devices]** > **[VPN]** > **[Remote Access]**を選択します。

ステップ 2 使用可能な VPN ポリシーのリストから、設定を変更するポリシーを選択します。

ステップ 3 [Advanced] タブをクリックします。
IPsec 設定のリストは、画面左側のナビゲーション ウィンドウに表示されます。

ステップ 4 ナビゲーション ウィンドウを使用して、次の IPsec オプションを編集します。

a) 暗号マップ（Crypto Maps）：[暗号マップ（Crypto Maps）] ページには、IKEv2 プロトコルが有効になっているインターフェイス グループがリストされます。暗号マップは、IKEv2 プロトコルが有効になっているインターフェイス用に自動生成されます。暗号マップを編集するには、リモート アクセス VPN 暗号マップの設定（1125 ページ）を参照してください。[アクセス インターフェイス（Access Interface）] タブで、選択した VPN ポリシーにインターフェイス グループを追加または削除できます。詳細については、リモートアクセス VPN のアクセス インターフェイスの設定（1115 ページ）を参照してください。

b) IKE ポリシー（IKE Policy）：[IKE ポリシー（IKE Policy）] ページには、AnyConnect エンドポイントが IPsec プロトコルを使用して接続している場合、選択した VPN ポリシーに適用可能なすべての IKE ポリシー オブジェクトがリストされます。詳細については、リモート アクセス VPN での IKE ポリシー

（1128 ページ）を参照してください。新しい IKE ポリシーを追加するには、IKEv2 ポリシー オブジェクトの設定 （619 ページ）を参照してください。FTD がサポートしているのは AnyConnect IKEv2 のみです。サードパーティ標準の IKEv2 クライアントはサポートされていません。

c) [IPsec/IKEv2 パラメータ（IPsec/IKEv2 Parameters）]：[IPsec/IKEv2 パラメータ（IPsec/IKEv2 Parameters）] ページでは、IKEv2 セッション設定、IKEv2 セキュリティ アソシエーション設定、IPsec 設定、および NAT 透過設定を変更できます。詳細については、リモート アクセス VPN の [IPsec/IKEv2パラメータ（IPsec/IKEv2 Parameters）] の設定 （1129 ページ）を参照してください。

ステップ 5 **[保存（Save）]** をクリックします。

リモート アクセス VPN 暗号マップの設定

暗号マップは、IPsec-IKEv2 プロトコルが有効になっているインターフェイス用に自動生成されます。[アクセス インターフェイス（Access Interface）] タブで、選択した VPN ポリシーにインターフェイス グループを追加または削除できます。詳細については、リモートアクセス VPN のアクセス インターフェイスの設定 （1115 ページ）を参照してください。

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス（Access）
エクスポート制御機能が有効なスマート ライセンス アカウントに関連付けられている次の AnyConnect ライセンスのいずれか。 • AnyConnect VPN Only • AnyConnect Plus • AnyConnect Apex	該当なし	FTD	いずれか（Any）	Admin

ステップ 1 **[Devices]** > **[VPN]** > **[Remote Access]**を選択します。

ステップ 2 使用可能な VPN ポリシーのリストから、設定を変更するポリシーを選択します。

ステップ 3 [詳細設定（Advanced）] > [暗号マップ（Crypto Maps）] をクリックし、テーブルの行を選択して、[編集（Edit）] アイコンをクリックし、暗号マップ オプションを編集します。

ステップ 4 [IKEv2 IPsecプロポーザル（IKEv2 IPsec Proposals）] を選択し、トランスフォーム セットを選択して、トンネル内のトラフィックの保護に使用される認証アルゴリズムおよび暗号化アルゴリズムを指定します。

ステップ 5 [リバースルートインジェクションを有効にする（Enable Reverse Route Injection）] を選択し、スタティック ルートは、リモート トンネル エンドポイントで保護されているネットワークとホストのルーティング プロセスに自動的に挿入されます。

ステップ 6 [クライアントサービスの有効化（Enable Client Services）] を選択し、ポート番号を指定します。

クライアント サービス サーバは、HTTPS（SSL）アクセスを提供します。これにより、AnyConnect ダウンロードは、ソフトウェア アップグレード、プロファイル、ローカリゼーションおよびカスタマイゼーション ファイル、CSD、SCEP、および AnyConnect クライアントが必要とするその他のファイル ダウンロードを受信できます。このオプションを選択した場合は、クライアント サービスのポート番号を指定します。クライアント サービス サーバを有効にしない場合、ユーザは、AnyConnect クライアントが必要する可能性があるこれらのファイルをダウンロードできません。

（注） 同じデバイスで実行する SSL VPN に対して同じポートを使用できます。SSL VPN を設定した場合でも、IPsec-IKEv2 クライアントで SSL を介してファイルをダウンロードするには、このオプションを選択する必要があります。

ステップ 7 [Perfect Forward Secrecyの有効化（Enable Perfect Forward Secrecy）] を選択し、[係数グループ（Modulus Group）] を選択します。

暗号化された交換ごとに一意のセッション キーを生成および使用するために、Perfect Forward Secrecy（PFS）を使用します。固有のセッション キーを使用することで、後続の復号から交換が保護されます。また、交換全体が記録されていて、攻撃者がエンドポイント デバイスで使用されている事前共有キーや秘密キーを入手している場合であっても保護されます。このオプションを選択する場合は、[係数グループ（Modulus Group）] リストで、PFS セッション キーの生成時に使用する Diffie-Hellman キー導出アルゴリズムも選択します。

係数グループは、2 つの IPsec ピア間の共有秘密キーを互いに送信することなく取得するために使用する Diffie-Hellman グループです。係数が大きいほどセキュリティが強化されますが、処理時間が長くなります。2 つのピアに、一致する係数グループが設定されている必要があります。リモート アクセス VPN 設定を許可する係数グループを選択します。

- [1]：Diffie-Hellman グループ 1（768 ビット係数）。
- [2]：Diffie-Hellman グループ 2（1024 ビット係数）。
- [5]：Diffie-Hellman グループ 5（1536 ビット係数。128 ビット キーの保護に推奨されるが、グループ 14 の方がより強力）。AES 暗号化を使用する場合は、このグループ（またはそれ以上）を使用します。
- [14]：Diffie-Hellman グループ 14（2048 ビット係数。128 ビット キーの保護に推奨される）。
- [19]：Diffie-Hellman グループ 19（256 ビットの楕円曲線フィールド サイズ）。
- [20]：Diffie-Hellman グループ 20（384 ビットの楕円曲線フィールド サイズ）。
- [21]：Diffie-Hellman グループ 21（521 ビットの楕円曲線フィールド サイズ）。
- [24]：Diffie-Hellman グループ 24（2048 ビット係数および 256 ビット素数位数サブグループ）。

ステップ 8 [ライフタイム継続時間（秒数）（Lifetime Duration (seconds)）] を指定します。

セキュリティ アソシエーション（SA）のライフタイム（秒数）。このライフタイムを超えると、SA の期限が切れ、2つのピア間で再ネゴシエーションを行う必要があります。一般的に、一定の限度に達するまで、ライフタイムが短いほど、IKE ネゴシエーションがセキュアになります。ただし、ライフタイムが長いと、今後の IPsec セキュリティ アソシエーションのセットアップが、短いライフタイムの場合よりも迅速に行われます。

120 ～ 2147483647 秒の値を指定できます。デフォルトは 28800 秒です。

ステップ 9 [ライフタイムのサイズ（KB）（Lifetime Size (kbytes)）] を指定します。

特定のセキュリティ アソシエーションが期限切れになる前にそのセキュリティ アソシエーションを使用して IPsec ピア間を通過できるトラフィック量（KB 単位）。

10 ～ 2147483647 KB の値を指定できます。デフォルトは 4,608,000 KB です。無限のデータを指定することはできません。

ステップ 10 次の [ESPv3設定（ESPv3 Settings）] を選択します。

- [着信ICMPのエラーメッセージを検証（Validate incoming ICMP error messages）]：IPsec トンネルを介して受信され、プライベート ネットワーク上の内部ホストが宛先の ICMP エラー メッセージを検証するかどうかを選択します。
- [「フラグメント禁止」ポリシーを有効にする（Enable 'Do Not Fragment' Policy）]：IP ヘッダーに Do-Not-Fragment（DF）ビット セットを使用する大量のパケットを IPsec サブシステムがどのように処理するかを定義し、[ポリシー（Policy）] リストからいずれかの項目を選択します。
  - コピー（Copy）：DF ビットを保持します。
  - クリア（Clear）：DF ビットを無視します。
  - 設定（Set）：DF ビットを設定して使用します。
- [トラフィックフロー機密保持（TFC）パケットを有効にする（Enable Traffic Flow Confidentiality (TFC) Packets）]：トンネルを通過するトラフィック プロファイルをマスクするダミーの TFC パケットを有効にします。[バースト（Burst）]、[ペイロード サイズ（Payload Size）]、および [タイムアウト（Timeout）] パラメータを使用して、指定した SA で不定期にランダムな長さのパケットを生成します。
  - バースト（Burst）：1 ～ 16 バイトの値を指定します。
  - ペイロード サイズ（Payload Size）：64 ～ 1024 バイトの値を指定します。
  - タイムアウト（Timeout）：10 ～ 60 秒の値を指定します。

ステップ 11 [OK] をクリックします。

関連トピック

インターフェイス オブジェクト：インターフェイス グループとセキュリティ ゾーン（535 ページ）

リモート アクセス VPN での IKE ポリシー

Internet Key Exchange（IKE、インターネット キー エクスチェンジ）は、IPsec ピアの認証、IPsec 暗号キーのネゴシエーションと配布、および IPsec Security Association（SA、セキュリティ アソシエーション）の自動的な確立に使用されるキー管理プロトコルです。IKE ネゴシエーションは 2 つのフェーズで構成されています。フェーズ 1 では、2 つの IKE ピア間のセキュリティ アソシエーションをネゴシエートします。これにより、ピアはフェーズ 2 で安全に通信できるようになります。フェーズ 2 のネゴシエーションでは、IKE によって IPsec などの他のアプリケーション用の SA が確立されます。両方のフェーズで接続のネゴシエーション時にプロポーザルが使用されます。IKE プロポーザルは、2 つのピア間のネゴシエーションを保護するためにこれらのピアで使用されるアルゴリズムのセットです。IKE ネゴシエーションは、共通（共有）IKE ポリシーに合意している各ピアによって開始されます。このポリシーは、後続の IKE ネゴシエーションを保護するために使用されるセキュリティ パラメータを示します。

（注） FTD は、リモート アクセス VPN では IKEv2 のみサポートします。

IKEv1 とは異なり、IKEv2 プロポーザルでは、1 つのポリシーで複数のアルゴリズムおよびモジュラス グループを選択できます。フェーズ 1 のネゴシエーションでピアを選択するため、作成する IKE プロポーザルの数を 1 つにすることは可能ですが、複数の異なる IKE プロポーザルを作成して、最も望ましいオプションを高い優先順位に設定することも検討してください。IKEv2 では、ポリシー オブジェクトが認証方式を指定しないため、その他のポリシーで認証要件を定義する必要があります。

リモート アクセス IPsec VPN を設定する際には IKE ポリシーが必要です。

リモート アクセス *VPN IKE* ポリシーの設定

IKE ポリシー テーブルには、IPsec プロトコルを使用して AnyConnect のエンドポイントを接続するとき、選択した VPN 設定に利用可能なすべての IKE ポリシー オブジェクトを記述します。詳細については、リモート アクセス VPN での IKE ポリシー（1128 ページ）を参照してください。

（注） FTD では、リモート アクセス VPN の IKEv2 のみに対応しています。

ステップ 1 **[Devices]** > **[VPN]** > **[Remote Access]**を選択します。

ステップ 2 使用可能な VPN ポリシーのリストから、設定を変更するポリシーを選択します。

ステップ 3 [詳細設定（Advanced）] > [IKEポリシー（IKE Policy）] をクリックします。

ステップ 4 [追加（Add）] ボタンをクリックして、利用可能な IKEv2 ポリシーから選択するか、新しい IKEv2 ポリシーを追加して、次の項目を指定します。

- [Name（名前）]：IKEv2 ポリシーの名前。
- [説明（Description）]：IKEv2 ポリシーの任意の説明

- [優先度（Priority）]：このプライオリティ値によって、共通のセキュリティ アソシエーション（SA）の検出試行時に、ネゴシエーションする 2 つのピアを比較することで、IKE ポリシーの順序が決定します。
- [ライフタイム（Lifetime）]：セキュリティ アソシエーション（SA）のライフタイム（秒数）。
- [整合性（Integrity）]：IKEv2 ポリシーで使用されるハッシュ アルゴリズムの整合性アルゴリズム部分です。
- [暗号化（Encryption）]：フェーズ 2 ネゴシエーションを保護するためのフェーズ 1 SA の確立に使用される暗号化アルゴリズムです。
- [PRFハッシュ（PRF Hash）]：IKE ポリシーに使用されるハッシュ アルゴリズムの疑似乱数関数（PRF）部分です。IKEv2 では、これらの要素に異なるアルゴリズムを指定できます。
- [DHグループ（DH Group）]：暗号化に使用する Diffie-Hellman グループです。

ステップ 5 **[保存（Save）]** をクリックします。

関連トピック

リモート アクセス VPN のアクセス インターフェイス オプション

リモート アクセス VPN の [IPsec/IKEv2パラメータ（IPsec/IKEv2 Parameters）] の設定

ステップ 1 **[Devices]** > **[VPN]** > **[Remote Access]**を選択します。

ステップ 2 使用可能な VPN ポリシーのリストから、設定を変更するポリシーを選択します。

ステップ 3 [詳細設定（Advanced）] > [IPsec] > [IPsec/IKEv2パラメータ（IPsec/IKEv2 Parameters）] をクリックします。

ステップ 4 [IKEv2セッション設定（IKEv2 Session Settings）] で次の項目を選択します。

- [ピアに送信されるID（Identity Sent to Peers）]：IKE ネゴシエーションでピアが自身の識別に使用する ID を選択します。
  - [自動（Auto）]：接続タイプごとの IKE ネゴシエーションを決定します。事前共有キー用の IP アドレス、証明書認証のための Cert DN（非対応）。
  - [IPアドレス（IP address）]：ISAKMP 識別情報を交換するホストの IP アドレスを使用します。
  - ホスト名（Hostname）：ISAKMP 識別情報を交換するホストの完全修飾ドメイン名（FQDN）を使用します。この名前は、ホスト名とドメイン名で構成されます。
- [トンネルの切断時の通知を有効にする（Enable Notification on Tunnel Disconnect）]：管理者は、SA で受信された着信パケットがその SA のトラフィック セレクタと一致しない場合のピアへの IKE 通知の送信を有効または無効にすることができます。デフォルトでは、[この通知を送信する（Sending this notification）] は無効になっています。
- [すべてのセッションが終了するまでデバイスの再起動を許可しない（Do not allow device reboot until all sessions are terminated）]：オンにすると、すべてのアクティブなセッションが自主的に終了してからシステムが再起動されます。デフォルトでは、無効になっています。

ステップ 5 [IKEv2セキュリティアソシエーションIKEv（SA）の設定（IKEv2 Security Association (SA) Settings）] で次の項目を選択します。

- [クッキーチャレンジ（Cookie Challenge）]：SA 開始パケットに応答してピア デバイスにクッキー チャレンジを送信するかどうかを選択します。阻止サービス妨害（DoS）攻撃に役立つことがあります。デフォルトでは、使用可能な SA の 50% がネゴシエーション中である場合にクッキー チャレンジを使用します。次のオプションのいずれか 1 つを選択します。
  - [カスタム（Custom）]：[着信クッキーチャレンジのしきい値（Threshold to Challenge Incoming Cookies）] を指定します。これは許可されるネゴシエーション中の SA の総数の割合です。この設定を指定すると、以降の SA ネゴシエーションに対してクッキーチャレンジがトリガーされます。範囲は 0 ～ 100 % です。デフォルト値は 50 % です。
  - [常時（Always）]：ピア デバイスにクッキー チャレンジを常に送信します。
  - [不可（Never）]：ピア デバイスにクッキー チャレンジを送信しません。
-
- [許可されるネゴシエーション中のSAの数（Number of SAs Allowed in Negotiation）]：一時点でのネゴシエーション中 SA の総数を制限します。クッキー チャレンジと共に使用する場合は、有効なクロス チェックが実行されるようにするため、クッキー チャレンジのしきい値をこの制限値よりも低くしてください。デフォルトは 100 % です。
- [許可されるSAの最大数（Maximum number of SAs Allowed）]：許可される IKEv2 接続の数を制限します。

ステップ 6 [IPsec設定（IPsec Settings）] で次の項目を選択します。

- [暗号化の前にフラグメンテーションを有効にする（Enable Fragmentation Before Encryption）]：このオプションは、IP フラグメンテーションをサポートしていない NAT デバイス間をトラフィックが通過できるようにします。このオプションを使用しても、IP フラグメンテーションをサポートしていない NAT デバイスの動作が妨げられることはありません。
- [パスの最大伝送ユニットのエージング（Path Maximum Transmission Unit Aging）]：PMTU（パスの最大伝送ユニット）のエージング（SA（セキュリティ アソシエーション）のリセット PMTU までのインターバル）が可能であるかを確認します。
- [値のリセット間隔（Value Reset Interval）]：SA（セキュリティ アソシエーション）の PMTU 値が元の値にリセットされるまでの時間（分）を入力します。有効範囲は 10 ～ 30 分です。デフォルトは無制限です。

ステップ 7 [NAT設定（NAT Settings）] で次の項目を選択します。

- [キープアライブメッセージトラバーサル（Keepalive Messages Traversal）]：NAT キープアライブ メッセージ トラバーサルを有効にするかどうかを設定します。VPN 接続ハブとスポークとの間にデバイス（中間デバイス）が配置されている場合、キープアライブ メッセージを転送するために NAT トラバーサル キープアライブを使用します。このデバイスでは、IPsec フローで NAT を実行します。このオプションを選択する場合は、セッションがアクティブであることを示すためにスポークと中間デバイス

間でキープアライブ信号が送信される間隔（秒）を設定します。値は10～3600秒となります。デフォルトは20秒です。

- [間隔（Interval）]：NATキープアライブ間隔を10～3600秒に設定します。デフォルトは20秒です。

ステップ8 **[保存（Save）]** をクリックします。

RADIUS ダイナミック認証

Firepower Threat Defenseは、RADIUSサーバを使用して、ダイナミックアクセスコントロールリスト（ACL）またはユーザごとのACL名を使用するVPNリモートアクセスおよびファイアウォールカットスループロキシセッションのユーザ許可を実行できます。ダイナミック認証またはRADIUS認可変更（RADIUS CoA）のダイナミックACLを実装するには、RADIUSサーバをサポートするように設定する必要があります。ユーザが認証を試みる場合、RADIUSサーバによってダウンロード可能ACL、またはACL名がFirepower Threat Defenseに送信されます。特定のサービスへのアクセスはACLによって許可されるか拒否されるかのいずれかです。Firepower Threat Defenseは認証セッションの期限が切れるとACLを削除します。

関連トピック

RADIUS サーバ グループ （635 ページ）
インターフェイス オブジェクト：インターフェイスグループとセキュリティ ゾーン （535 ページ）
RADIUS ダイナミック認証の設定 （1132 ページ）
の RADIUS サーバ属性 Firepower Threat Defense （1112 ページ）

RADIUS ダイナミック認証の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス（Access）
エクスポート制御機能が有効なスマート ライセンス アカウントに関連付けられている次の AnyConnect ライセンスのいずれか。 • AnyConnect VPN Only • AnyConnect Plus • AnyConnect Apex	該当なし	FTD	いずれか（Any）	Admin

始める前に：

- RADIUS サーバで参照されている場合、セキュリティ ゾーンやインターフェイス グループには 1 つのインターフェイスのみ設定できます。
- ダイナミック認証が有効になっている RADIUS サーバでダイナミック認証を機能させるためには、Firepower Threat Defense 6.3 以降が必要です。
- Firepower Threat Defense 6.2.3 以前のバージョンでは、RADIUS サーバでのインターフェイスの選択はサポートされていません。展開中、インターフェイス オプションは無視されます。

表 *85*：手順

	操作内容	詳細
ステップ 1	Firepower Management Center Web インターフェイスにログインします。	
ステップ 2	ダイナミック認証を使用して、RADIUS サーバ オブジェクトを設定します。	RADIUS サーバ グループのオプション （637 ページ）

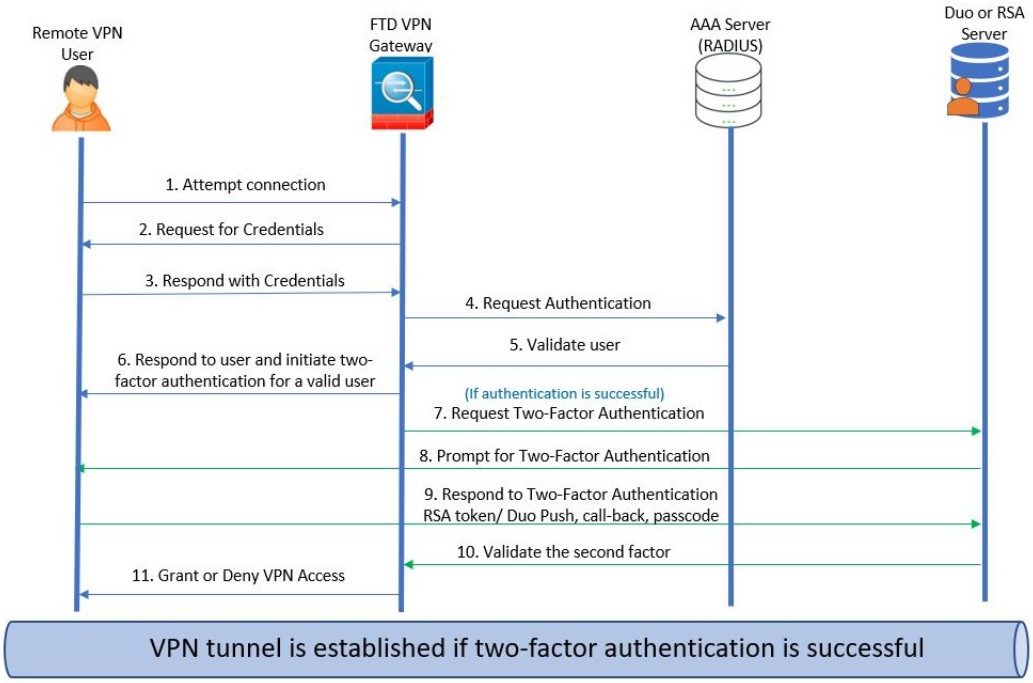
	操作内容	詳細
ステップ 3	認可変更（CoA）が有効になっているインターフェイスを介してISEサーバへのルートを設定し、ルーティングまたは特定のインターフェイスを介して Firepower Threat Defense から RADIUS サーバへの接続を確立します。	RADIUS サーバ グループのオプション （637 ページ） ユーザ制御用 ISE/ISE-PIC の設定 （2601 ページ）
ステップ 4	リモートアクセス VPN ポリシーを設定し、ダイナミック認証を使用して作成した RADIUS サーバ グループ オブジェクトを選択します。	新しいリモート アクセス VPN ポリシーの作成 （1098 ページ）
ステップ 5	DNS サーバの詳細とドメインルックアップ インターフェイスを [プラットフォーム設定（Platform Settings）] を使用して設定します。	DNS の設定 （1102 ページ） DNS サーバ グループ オブジェクト （601 ページ）
ステップ 6	VNP ネットワーク経由で DNS サーバに到達可能な場合は、リモート アクセス VPN トンネルを介して DNS トラフィックを許可するためのスプリット トンネルをグループ ポリシーに設定します。	グループ ポリシー オブジェクトの設定 （624 ページ）
ステップ 7	設定変更を展開します。	設定変更の展開 （447 ページ）

Two-Factor Authentication

リモート アクセス VPN に対して二要素認証を設定することができます。二要素認証を使用する場合、ユーザはユーザ名とスタティック パスワードに加えて、RSA トークンやパスコードなどの追加項目を指定する必要があります。二要素認証が 2 番目の認証ソースを使用することと異なるのは、1 つの認証ソースで 2 つの要素が設定され、RSA サーバとの関係がプライマリ認証ソースに関連付けられている点です。

Firepower Threat Defense 2 番目の要素のためにモバイルにプッシュされる RSA トークンと Duo パスコードを、二要素認証プロセスの最初の要素としての RADIUS サーバまたは AD サーバとの組み合わせをサポートします。

図 *24 :* 二要素認証



RSA 二要素認証の設定

このタスクの概要：

RADIUS サーバまたは AD サーバを RSA サーバの認証エージェントとして設定し、サーバをリモートアクセス VPN のプライマリ認証ソースとして Firepower Management Center で使用することができます。

この方法を使用する場合、ユーザは RADIUS または AD サーバで設定されているユーザ名を使用して認証し、パスワードと 1 回限りの一時的な RSA トークンを連結し、パスワードとトークンをカンマで区切る必要があります（*password,token*）。

この設定では、認証サービスを提供するために（Cisco ISE で供給されるような）個別の RADIUS サーバを使用することが一般的です。2 番目の RADIUS サーバを認証サーバとして設定し、必要に応じてアカウンティング サーバとしても設定します。

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス（Access）
エクスポート制御機能が有効なスマート ライセンス アカウントに関連付けられている次の AnyConnect ライセンスのいずれか。 • AnyConnect VPN Only • AnyConnect Plus • AnyConnect Apex	該当なし	FTD	いずれか（Any）	Admin

始める前に：

Firepower Threat Defense に RADIUS 二要素認証を設定する前に、次の設定が完了していることを確認します。

RSA サーバ上で以下の操作を実行します。

- RADIUS または Active Directory サーバを認証エージェントとして設定します。
- 設定（*sdconf.rec*）ファイルを生成してダウンロードします。
- トークン プロファイルを作成してトークンをユーザに割り当て、トークンをユーザに配布します。トークンをダウンロードして、リモート アクセス VPN クライアント システムにインストールします。

詳細については、RSA SecureID スイートのドキュメントを参照してください。

ISE サーバ上で以下の操作を実行します。

- RSA サーバで生成した設定（*sdconf.rec*）ファイルをインポートします。
- 外部アイデンティティ ソースとして RSA サーバを追加して、共有秘密を指定します。

表 *86 :* 手順

	操作内容	詳細
ステップ 1	Firepower Management Center Web インターフェイスにログインします。	
ステップ 2	RADIUS サーバ グループを作成します。	RADIUS サーバ グループのオプション （637 ページ）
ステップ 3	RADIUS または AD サーバをホストとして指定して、新しい RADIUS サーバ グループ内に RADIUS サーバ オブジェクトを作成します。タイムアウトの時間は 60 秒以上に設定します。	RADIUS サーバ オプション （638 ページ） （注） RADIUS または AD サーバは、RSA サーバで認証エージェントとして設定されているサーバと同じである必要があります。 二要素認証の場合は、AnyConnect クライアントプロファイル XML ファイルでもタイムアウトが 60 秒以上に更新されていることを確認してください。
ステップ 4	ウィザードを使用して新しいリモートアクセス VPN ポリシーを設定するか、既存のリモートアクセス VPN ポリシーを編集します。	新しいリモートアクセス VPN ポリシーの作成 （1098 ページ）
ステップ 5	認証サーバとして RADIUS を選択し、新しく作成した RADIUS サーバ グループを認証サーバとして選択します。	リモートアクセス VPN の AAA 設定 （1108 ページ）
ステップ 7	設定変更を展開します。	設定変更の展開 （447 ページ）

Duo 二要素認証の設定

このタスクの概要：

Duo RADIUS サーバはプライマリ認証ソースとして設定できます。この方法では、Duo RADIUS 認証プロキシを使用します。（LDAPS 経由での Duo クラウド サービスとの直接接続は使用できません）。

Duo の設定に関する詳細手順については、https://duo.com/docs/cisco-firepower を参照してください。

その後、最初の認証要素として別の RADIUS サーバ（または AD サーバ）を使用し、2 番目の要素として Duo クラウド サービスを使用するため、プロキシ サーバ宛の認証要求を転送するように Duo を設定します。

このアプローチを使用する場合、Duo クラウドまたは web サーバと、関連付けられている RADIUS サーバの両方で設定されたユーザ名を使用してユーザを認証する必要があります。ユーザは、RADIUS サーバに設定されたパスワードと、その後に次のいずれかの Duo コードを入力する必要があります。

- **Duo-passcode**。*my-password*12345 など。
- **push**。たとえば、*my-password*,**push** など。push は、ユーザによるインストールと登録が完了している Duo モバイル アプリに認証をプッシュ送信するように Duo に指示する場合に使用します。
- **sms**。たとえば、*my-password*,**sms** など。**sms** は、ユーザのモバイルデバイスにパスコードの新しいバッチと SMS メッセージを送信するように Duo に指示する場合に使用します。**sms** を使用すると、ユーザの認証試行が失敗します。ユーザは再認証し、2 番目の要素として新しいパスコードを入力する必要があります。

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス（**Access**）
エクスポート制御機能が有効なスマート ライセンス アカウントに関連付けられている次の AnyConnect ライセンスのいずれか。 • AnyConnect VPN Only • AnyConnect Plus • AnyConnect Apex	該当なし	FTD	いずれか（Any）	Admin

始める前に：

Firepower Threat Defense で Duo 認証プロキシを使用する RADIUS 二要素認証を設定する前に、次の設定が完了していることを確認します。

- リモート アクセス VPN ユーザに対して実行中のプライマリ認証（RADIUS または AD）を設定してから、Duo の展開を開始します。
- ネットワーク内の Windows または Linux マシンに Duo プロキシ サービスをインストールして、Duo と Firepower Threat Defense リモート アクセス VPN を統合します。また、この Duo プロキシ サーバは RADIUS サーバとしても機能します。

  次の場所から最新の Duo 認証プロキシをダウンロードしてインストールします。

  - **Windows**：https://dl.duosecurity.com/duoauthproxy-latest.exe
  - **Linux**：https://dl.duosecurity.com/duoauthproxy-latest-src.tgz
  - https://duo.com/docs/checksums#duo-authentication-proxy でチェックサムを確認します。

- Duo 認証ファイル `authproxy.cfg` を設定します。https://duo.com/docs/authproxy_reference ページの指示に従って、認証設定を構成します。

  `authproxy.cfg` 設定ファイルには、RADIUS または ISE サーバの詳細、Firepower Threat Defense デバイス、Duo プロキシ サーバの詳細、統合鍵、秘密鍵、API ホストの詳細を含める必要があります。

- `authproxy.cfg` ファイルに正しい API ホスト情報が含まれていることを確認します。
- [Duoセキュリティ設定（Duo Security Server）] > [Duo管理者パネル（Duo Admin Panel）] > [アプリケーション（Applications）] > [CISCO RADIUS VPN] で、新しくインストールされた Duo プロキシ サーバのセカンダリ認証ファクタなど、その他の必要な設定を指定します。

表 *87* : 手順

	操作内容	詳細
ステップ 1	Firepower Management Center Web インターフェイスにログインします。	
ステップ 2	RADIUS サーバ グループを作成します。	RADIUS サーバ グループのオプション （637 ページ）
ステップ 3	RADIUS サーバをホストとして指定して、新しい RADIUS サーバ グループ内に RADIUS サーバ オブジェクトを作成します。タイムアウトの時間は 60 秒以上に設定します。	RADIUS サーバ オプション （638 ページ） （注） RADIUS サーバは、RSA サーバで認証エージェントとして設定されているサーバと同じである必要があります。 二要素認証の場合は、AnyConnect クライアントプロファイル XML ファイルでもタイムアウトが 60 秒以上に更新されていることを確認してください。

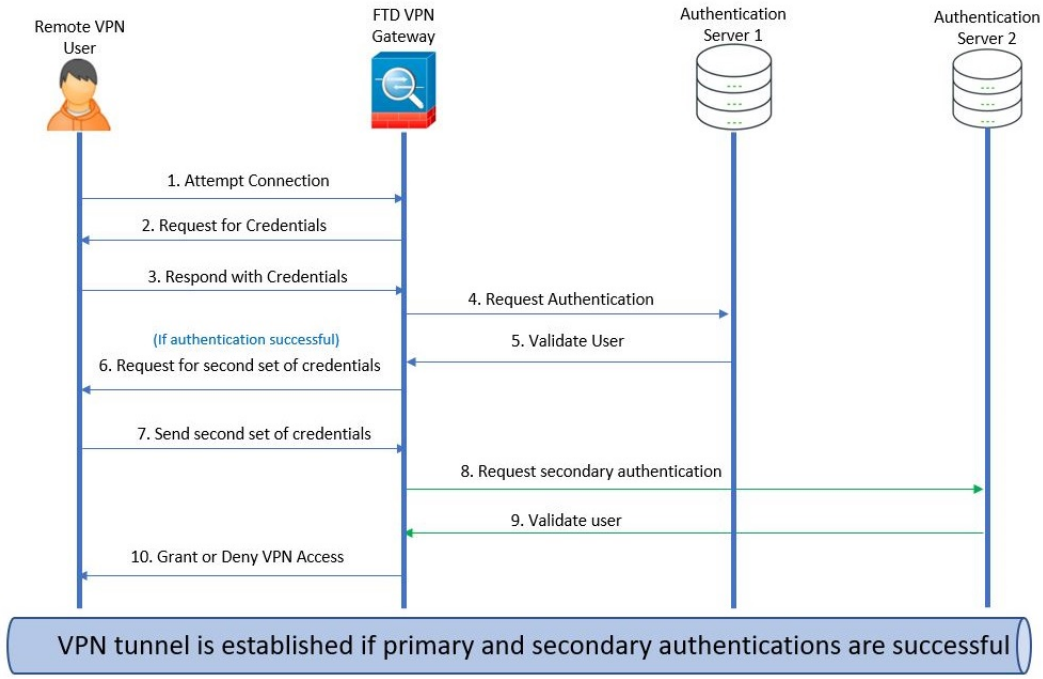
	操作内容	詳細
ステップ 4	ウィザードを使用して新しいリモートアクセス VPN ポリシーを設定するか、既存のリモートアクセス VPN ポリシーを編集します。	新しいリモートアクセス VPN ポリシーの作成 （1098 ページ）
ステップ 5	認証サーバとして RADIUS を選択し、Duo プロキシ サーバを指定して作成した RADIUS サーバ グループを認証サーバとして選択します。	リモートアクセス VPN の AAA 設定 （1108 ページ）
ステップ 7	設定変更を展開します。	設定変更の展開 （447 ページ）

Secondary Authentication

Firepower Threat Defense のセカンダリ認証または二重認証は、2 つの異なる認証サーバを使用して、リモート アクセス VPN 接続にさらにもう 1 つのセキュリティのレイヤを追加します。セカンダリ認証が有効になっている場合、AnyConnect VPN のユーザは VPN ゲートウェイにログインするために 2 組のクレデンシャルを提供する必要があります。

Firepower Threat Defense リモート アクセス VPN は、AAA のみのセカンダリ認証と、クライアント証明書認証方式および AAA 認証方式をサポートします。

図 *25 :* リモート アクセス *VPN* セカンダリ認証または二重認証



関連トピック

リモートアクセス VPN のセカンダリ認証の設定 （1140 ページ）

リモートアクセス VPN のセカンダリ認証の設定

クライアント証明書と認証サーバの両方を使用するようにリモート アクセス VPN 認証が設定されている場合、VPN クライアント認証はクライアント証明書の検証と AAA サーバの両方を使用して実行されます。

始める前に

- 2 つの認証（AAA）サーバの設定：プライマリおよびセカンダリ認証サーバ、必要な ID 証明書。認証サーバには、RADIUS サーバ、AD または LDAP レルムを使用できます。
- リモート アクセス VPN 設定が機能するように AAA サーバに Firepower Threat Defense デバイスからアクセスできることを確認します。AAA サーバへの接続を確実にするために、ルーティングを設定します（[デバイス（Devices）] > [デバイス管理（Device Management）] > [デバイスの編集（Edit Device）] > [ルーティング（Routing）]）。

ステップ 1 Firepower Management Center の Web インターフェイスで、[デバイス（Devices）] > [VPN] > [リモート アクセス（Remote Access）] を選択します。

ステップ 2 リスト内の既存のリモート アクセス ポリシーを選択し、対応する [編集（Edit）] アイコンをクリックします。または、[追加（Add）] をクリックして新しいリモート アクセス VPN ポリシーを作成します。

ステップ 3 新しいリモート アクセス VPN ポリシーには、接続プロファイルの設定時に認証を設定します。既存の設定の場合は、クライアント プロファイルが含まれている接続プロファイルを選択し、[編集（Edit）] をクリックします。

ステップ 4 [AAA] タブで、[認証方式（Authentication Method）]、[AAA]、[クライアント証明書とAAA（Client Certificate & AAA）] を選択します。

- [認証方式（Authentication Method）] の選択に応じて、次のようになります。

  [クライアント証明書とAAA（Client Certificate & AAA）]：クライアント証明書と AAA サーバの両方を使用して認証されます。

  - [AAA]：[認証サーバ（Authentication Server）] に [RADIUS] を選択した場合、デフォルトで許可サーバは同じ値になります。ドロップダウン リストから [アカウンティング サーバ（Accounting Server）] を選択します。認証サーバ ドロップダウン リストから [AD] と [LDAP] を選択した場合は常に、[認証サーバ（Authorization Server）] と [アカウンティング サーバ（Accounting Server）] をそれぞれ手動で選択する必要があります。
  - どの認証方式を選択する場合にも、[ユーザが承認データベースに存在するときにのみ接続を許可（Allow connection only if user exists in authorization database）] を選択または選択解除します。

- [セカンダリ認証を使用（Use secondary authentication）]：VPN セッションのセキュリティを強化するため、プライマリ認証の他にセカンダリ認証を設定します。セカンダリ認証は、[AAA のみ（AAA only）] と [クライアント証明書と AAA（Client Certificate & AAA）] の認証方式にのみ適用されます。

  セカンダリ認証はオプションの機能であり、2 つのセットのユーザ名とパスワードを AnyConnect ログイン画面に入力するには VPN ユーザが必要です。認証サーバまたはクライアント証明書からセカンダリ ユーザ名を事前入力するように設定することもできます。リモート アクセス VPN 認証は、プライマリとセカンダリの両方の認証が成功した場合にのみ許可されます。いずれの認証サーバに到達できない場合、1 つの認証が失敗すると、VPN 認証が拒否されます。

  セカンダリ認証の設定前に、2つ目のユーザ名とパスワードのセカンダリ認証のサーバ グループ（AAA サーバ）を設定する必要があります。たとえば、プライマリ認証サーバを LDAP または Active Directory レルムに、セカンダリ認証を RADIUS サーバに設定できます。

  （注） デフォルトでは、セカンダリ認証は必要ありません。

  [認証サーバ（Authentication Server）]：VPN ユーザのセカンダリ ユーザ名とパスワードを提供するセカンダリ認証サーバ。

  [セカンダリ認証のユーザ名（Username for secondary authentication）] で次の項目を選択します。

  - [プロンプト（Prompt）]：VPN ゲートウェイへのログイン中にユーザ名とパスワードを入力するようユーザに要求します。
  - [プライマリ認証ユーザ名を使用（Use primary authentication username）]：プライマリとセカンダリの両方の認証にプライマリ認証サーバからユーザ名が取得されます。パスワードは 2 つ入力する必要があります。
  - [クライアント証明書からのユーザ名をマップ（Map username from client certificate）]：クライアント証明書からセカンダリ ユーザ名が事前に入力されます。

- クライアント証明書のユーザ名を含む [固有のフィールドをマップ（Map specific field）] オプションを選択する場合。[プライマリ（Primary）] フィールドと [セカンダリ（Secondary）] フィールドには、デフォルト値の [CN（共通名）（CN (Common Name)）] と [組織ユニット（OU）（OU (Organisational Unit)）] がそれぞれ表示されます。[DN（識別名）全体をユーザ名として使用（Use entire DN (Distinguished Name) as username）] オプションを選択した場合はユーザ ID が自動的に取得されます。

  プライマリとセカンダリのフィールドのマッピングの詳細については、「**認証方式**」の説明を参照してください。

- [ユーザ ログイン ウィンドウに証明書からユーザ名を事前に入力（Prefill username from certificate on user login window）]：ユーザが AnyConnect VPN クライアント経由で接続したときにクライアント証明書からセカンダリ ユーザ名を事前に入力します。

  - [ログイン ウィンドウでユーザ名を非表示にする（Hide username in login window）]：セカンダリ ユーザ名はクライアント証明書から事前に入力されますがユーザには表示されず、ユーザが事前に入力されたユーザ名を変更しないようにします。

- [VPN セッションのセカンダリ ユーザ名を使用（Use secondary username for VPN session）]：VPN セッション中のユーザ アクティビティのレポートにセカンダリ ユーザ名を使用します。

詳細については、「リモートアクセス VPN の AAA 設定 （1108 ページ）」を参照してください。

関連トピック

接続プロファイルの設定 （1105 ページ）

リモート アクセス VPN の AAA の設定のカスタマイズ

ここでは、リモート アクセス VPN の AAA プリファレンスのカスタマイズについて説明します。詳細については、「リモートアクセス VPN の AAA 設定 （1108 ページ）」を参照してください。

クライアント証明書を使用した VPN ユーザの認証

ウィザードを使用するか、またはポリシーを後で編集することによって新しいリモートアクセス VPN ポリシーを作成するときに、クライアント証明書を使用してリモート アクセス VPN 認証を設定できます。

始める前に

VPN ゲートウェイとして機能する各 Firepower Threat Defense デバイスにアイデンティティ証明書を取得するために使用する証明書登録オブジェクトを設定します。

ステップ 1 Firepower Management Center の Web インターフェイスで、[デバイス（Devices）] > [VPN] > [リモート アクセス（Remote Access）] を選択します。

ステップ 2 リスト内の既存のリモート アクセス ポリシーを選択し、対応する [編集（Edit）] アイコンをクリックします。または、[追加（Add）] をクリックして新しいリモート アクセス VPN ポリシーを作成します。

ステップ 3 新しいリモート アクセス VPN ポリシーには、接続プロファイルの設定時に認証を設定します。既存の設定の場合は、クライアント プロファイルが含まれている接続プロファイルを選択し、[編集（Edit）] をクリックします。

ステップ 4 [AAA] タブで、[認証方式（Authentication Method）]、[クライアント証明書のみ（Client Certificate Only）] を選択します。

この認証方式では、ユーザはクライアント証明書を使用して認証されます。VPN クライアント エンドポイントで設定する必要があります。デフォルトでは、ユーザ名はクライアント証明書フィールド CN および OU からそれぞれ派生します。クライアント証明書の他のフィールドにユーザ名が指定されている場合は、[プライマリ（Primary）] と [セカンダリ（Secondary）] フィールドを使用して適切なフィールドをマップします。

クライアント証明書のユーザ名を含む [固有のフィールドをマップ（Map specific field）] オプションを選択する場合。[プライマリ（Primary）] フィールドと [セカンダリ（Secondary）] フィールドには、デフォルト値の [CN（共通名）（CN (Common Name)）] と [組織ユニット（OU）（OU (Organisational Unit)）] がそれぞれ表示されます。[DN全体をユーザ名として使用（Use entire DN as username）] オプションを選択した場合、ユーザ ID が自動的に取得されます。識別名（DN）は、個々のフィールドから構成される一意の識別子であり、ユーザを接続プロファイルと照合するときに識別子として使用できます。DN ルールは、拡張証明書認証に使用されます。

- [固有のフィールドをマップ（Map specific field）] オプションに関連する [プライマリ（Primary）] フィールドと [セカンダリ（Secondary）] フィールドには、次の共通の値が含まれています。
  - C（国）
  - CN（一般名）
  - DNQ（DN 修飾子
  - EA（電子メール アドレス）
  - GENQ（世代識別子）
  - GN（姓名の名）
  - I（イニシャル）
  - L（地名）
  - N（名前）
  - O（組織）
  - OU（組織ユニット）
  - SER（シリアル番号）

- SN（姓名の姓）
- SP（都道府県）
- T（タイトル）
- UID（ユーザ ID）
- UPN（ユーザ プリンシパル名）

- どの認証方式を選択する場合にも、[ユーザが承認データベースに存在するときにのみ接続を許可（Allow connection only if user exists in authorization database）] を選択または選択解除します。

詳細については、「リモートアクセス VPN の AAA 設定 （1108 ページ）」を参照してください。

関連トピック

接続プロファイルの設定 （1105 ページ）
証明書の登録オブジェクトの追加 （593 ページ）

クライアント証明書と AAA サーバ経由でのリモート アクセス VPN のログインの設定

クライアント証明書と認証サーバの両方を使用するようにリモート アクセス VPN 認証が設定されている場合、VPN クライアント認証はクライアント証明書の検証と AAA サーバの両方を使用して実行されます。

始める前に

- VPN ゲートウェイとして機能する各 Firepower Threat Defense デバイスのアイデンティティ証明書を取得するために使用される証明書登録オブジェクトを設定します。
- RADIUS サーバ グループ オブジェクトと、このリモート アクセス VPN ポリシーで使用されている AD または LDAP レルムを設定します。
- リモート アクセス VPN 設定が機能するように AAA サーバに Firepower Threat Defense デバイスからアクセスできることを確認します。

ステップ 1 Firepower Management Center の Web インターフェイスで、[デバイス（Devices）] > [VPN] > [リモート アクセス（Remote Access）] を選択します。

ステップ 2 リスト内の既存のリモート アクセス ポリシーを選択し、対応する [編集（Edit）] アイコンをクリックします。または、[追加（Add）] をクリックして新しいリモート アクセス VPN ポリシーを作成します。

ステップ 3 新しいリモート アクセス VPN ポリシーには、接続プロファイルの設定時に認証を設定します。既存の設定の場合は、クライアント プロファイルが含まれている接続プロファイルを選択し、[編集（Edit）] をクリックします。

ステップ 4 [AAA] タブで、[認証方式（Authentication Method）]、[クライアント証明書と AAA（Client Certificate & AAA）] を選択します。

- [認証方式（Authentication Method）] の選択に応じて、次のようになります。

  [クライアント認証と AAA（Client Certificate & AAA）]：両方のタイプの認証が実行されます。

  - [AAA]：[認証サーバ（Authentication Server）] に [RADIUS] を選択した場合、デフォルトで許可サーバは同じ値になります。ドロップダウン リストから [アカウンティング サーバ（Accounting Server）] を選択します。認証サーバ ドロップダウン リストから [AD] と [LDAP] を選択した場合は常に、[認証サーバ（Authorization Server）] と [アカウンティング サーバ（Accounting Server）] をそれぞれ手動で選択する必要があります。

  - [クライアント証明書（Client Certificate）]：ユーザはクライアント証明書を使用して認証されます。クライアント証明書は、VPN クライアント エンドポイントで設定する必要があります。デフォルトでは、ユーザ名はクライアント証明書フィールド CN および OU からそれぞれ派生します。クライアント証明書の他のフィールドにユーザ名が指定されている場合は、[プライマリ（Primary）] と [セカンダリ（Secondary）] フィールドを使用して適切なフィールドをマップします。

    クライアント証明書のユーザ名を含む [固有のフィールドをマップ（Map specific field）] オプションを選択する場合。[プライマリ（Primary）] フィールドと [セカンダリ（Secondary）] フィールドには、デフォルト値の [CN（共通名）（CN (Common Name)）] と [組織ユニット（OU）（OU (Organisational Unit)）] がそれぞれ表示されます。[DN全体をユーザ名として使用（Use entire DN as username）] オプションを選択した場合、ユーザ ID が自動的に取得されます。識別名（DN）は、個々のフィールドから構成される一意の識別子であり、ユーザを接続プロファイルと照合するときに識別子として使用できます。DN ルールは、拡張証明書認証に使用されます。

    [固有のフィールドをマップ（Map specific field）] オプションに関連する [プライマリ（Primary）] フィールドと [セカンダリ（Secondary）] フィールドには、次の共通の値が含まれています。

    - C（国）
    - CN（一般名）
    - DNQ（DN 修飾子
    - EA（電子メール アドレス）
    - GENQ（世代識別子）
    - GN（姓名の名）
    - I（イニシャル）
    - L（地名）
    - N（名前）
    - O（組織）
    - OU（組織ユニット）
    - SER（シリアル番号）

- SN（姓名の姓）
- SP（都道府県）
- T（タイトル）
- UID（ユーザ ID）
- UPN（ユーザ プリンシパル名）

- どの認証方式を選択する場合にも、[ユーザが承認データベースに存在するときにのみ接続を許可（Allow connection only if user exists in authorization database）] を選択または選択解除します。

詳細については、「リモートアクセス VPN の AAA 設定 （1108 ページ）」を参照してください。

関連トピック

接続プロファイルの設定 （1105 ページ）
証明書の登録オブジェクトの追加 （593 ページ）

VPN セッションでのパスワード変更の管理

パスワードの管理では、リモート アクセス VPN 管理者がリモート アクセス VPN ユーザのパスワード期限切れの通知を設定できます。パスワード管理は、 AAA のみとクライアント証明書と AAA の認証設定の AAA 設定で使用できます。詳細については、リモートアクセス VPN の AAA 設定 （1108 ページ）を参照してください。

ステップ 1 Firepower Management Center の Web インターフェイスで、[デバイス（Devices）] > [VPN] > [リモート アクセス（Remote Access）] を選択します。

ステップ 2 リストから既存のリモート アクセス ポリシーを選択し、対応する [編集（Edit）] アイコンをクリックします。

ステップ 3 AAA の設定が含まれている接続プロファイルを選択し、[編集（Edit）] をクリックします。

ステップ 4 [AAA] > [詳細設定（Advanced Settings）] > [パスワード管理（Password Management）] を選択します。

ステップ 5 [パスワード管理の有効化（Enable Password Management）] を選択し、次のいずれかを選択します。

- [Notify User（ユーザ通知）]：パスワードの有効期限が切れる前にユーザに通知します。ボックスに日数を指定します。
- [パスワードの有効期限の日にユーザに通知（Notify user on the day password expires）]：パスワードが期限切れになる当日にユーザに通知します。

ステップ 6 **[保存（Save）]** をクリックします。

関連トピック

接続プロファイルの設定 （1105 ページ）

承認を得るための LDAP または Active Directory の設定

認証に LDAP サーバまたは Active Directory（AD）サーバを使用してリモート アクセス VPN を設定する場合は、FlexConfig オブジェクトを使用して属性マップを設定する必要があります。これは、Firepower Management Center の Web インターフェイス上では属性マップが直接サポートされていないためです。

始める前に

LDAP または AD のレルム オブジェクトが作成されていることを確認します。

ステップ 1 Firepower Management Center の Web インターフェイスで、[デバイス（Devices）] > [VPN] > [リモート アクセス（Remote Access）] を選択します。

ステップ 2 認証サーバとして、LDAP または AD レルム オブジェクトを含むリモート アクセス VPN ポリシーを作成します。または、既存のリモート アクセス VPN の設定を編集し、LDAP または AD レルムを認証サーバとして選択します。

ステップ 3 [オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [FlexConfig] > [FlexConfig オブジェクト（FlexConfig Object）] を選択します。

ステップ 4 FlexConfig ポリシーを作成し、次の 2 つの FlexConfig オブジェクトを作成して追加セクションに割り当てます。

FlexConfig ポリシーの設定 （1236 ページ）を参照してください。

a) [展開タイプ（Deployment type）] を [1 回（Once）]、[タイプ（Type）] を [後ろに付加（Append）] にして、LDAP 属性マップの FlexConfig オブジェクトを作成します。

オブジェクトの本文には、次を入力します。

```
lda attribute-map <LDAP_Map_for_VPN_Access>
          map-name  memberOf Group-Policy
          map-value memberOf CN=APP-SSL-VPN Managers,CN=Users,OU=stbu,DC=cisco,DC=com
LabAdminAccessGroupPolicy
         map-value memberOf CN=cisco-Eng,CN=Users,OU=stbu,DC=cisco,DC=com VPNAccessGroupPolicy
```

b) [展開タイプ（Deployment type）] を [毎回（Everytime）]、[タイプ（Type）] を [後ろに付加（Append）] にして、LDAP 属性マップを LDAP AAA サーバに関連付ける FlexConfig オブジェクト属性を作成します。

（注） このマッピングは、LDAP 属性マップの割り当てが Firepower Management Center によって拒否されるため、その割り当てを元に戻すために必要です。

オブジェクトの本文領域に次を入力します。

```
aaa-server <LDAP/AD_Realm_name> host <AD Server IP>
          ldap-attribute-map <LDAP_Map_for_VPN_Access>
          exit
```

リモート アクセス VPN ポリシーの設定に追加した接続プロファイルの AAA サーバの設定に使用した LDAP レルム名と同じ *AAA* サーバを使用します。

詳細については、FlexConfig テキスト オブジェクトの設定 （1234 ページ）を参照してください。

a) **[保存（Save）]** をクリックします。

FlexConfig ポリシー内での FlexConfig オブジェクトの順序が、LDAP 属性マップの FlexConfig オブジェクトの後に AAA サーバ オブジェクトが続いていることを確認します。

これは、LDAP 属性マップを設定し、それを Firepower Threat Defense デバイス上の LDAP サーバ設定と関連付けます。

関連トピック

FlexConfig オブジェクトの設定 （1229 ページ）

RADIUS サーバへのアカウンティング レコードの送信

リモート アクセス VPN のアカウンティング レコードは、ユーザがアクセスしたサービスやユーザが使用したネットワーク リソースの量を VPN 管理者が追跡するのに役立ちます。アカウンティング情報には、ユーザセッションの開始時刻と停止時刻、ユーザ名、セッションごとのデバイスを通過したバイト数、使用されたサービス、および各セッションの時間が含まれています。このデータを、ネットワーク管理、クライアント請求、または監査のために分析できます。

アカウンティングは、単独で使用するか、認証および認可とともに使用することができます。AAA アカウンティングをアクティブ化すると、ネットワーク アクセス サーバは設定されたアカウンティング サーバにユーザ アクティビティをレポートします。RADIUS サーバはアカウンティング サーバとして設定できます。そのため、ユーザ アクティビティ情報のすべてが Firepower Management Center から RADIUS サーバに送信されます。

（注） リモート アクセス VPN AAA の設定では、認証、許可、およびアカウンティング用に同じ RADIUS サーバまたは個別の RADIUS サーバを使用できます。

始める前に

認証要求またはアカウンティング レコードが送信される RADIUS サーバで RADIUS グループ オブジェクトを設定します。RADIUS サーバ グループのオプション （637 ページ）を参照してください。

RADIUS サーバが Firepower Threat Defense デバイスから到達可能であることを確認します。[デバイス（Devices）] > [デバイス管理（Device Management）] > [デバイスの編集（Edit Device）] > [ルーティング（Routing）] で Firepower Management Center のルーティングを設定し、RADIUS へのサーバへの接続を確保します。

ステップ 1 Firepower Management Center の Web インターフェイスで、[デバイス（Devices）] > [VPN] > [リモート アクセス（Remote Access）] を選択します。

ステップ 2 リスト内の既存のリモート アクセス ポリシーを選択し、対応する [編集（Edit）] アイコンをクリックします。または、新しいリモート アクセス VPN ポリシーを作成します。

ステップ 3 AAA の設定が含まれている接続プロファイルを選択し、[編集（Edit）] > [AAA] をクリックします。
ステップ 4 **アカウンティング サーバ**として RADIUS サーバを選択します。
ステップ 5 **[保存（Save）]** をクリックします。

関連トピック

接続プロファイルの設定 （1105 ページ）
リモートアクセス VPN の AAA 設定 （1108 ページ）

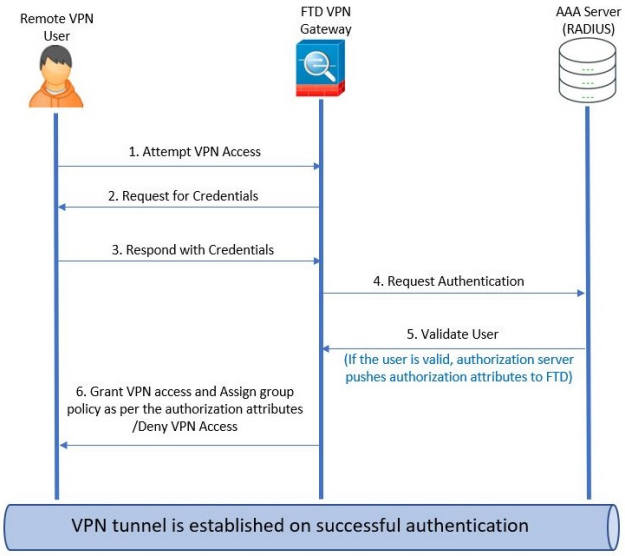
認証サーバへのグループ ポリシーの選択の委任

ユーザに適用されるグループ ポリシーは VPN トンネルが確立される際に決定されます。ウィザードを使用してリモートアクセス VPN ポリシーを作成するときに接続プロファイルのグループポリシーを選択するか、または後で接続プロファイルの接続ポリシーを更新することができます。ただし、グループポリシーを割り当てるように AAA（RADIUS）サーバを設定するか、または現在の接続プロファイルから取得されます。Firepower Threat Defense デバイスが設定プロファイルに設定されている属性と競合する外部 AAA サーバから属性を受信した場合は、AAA サーバからの属性が常に優先されます。

IETF RADIUS サーバ属性 25 を送信してユーザ/ユーザ グループの許可プロファイルを設定し、対応するグループ ポリシー名にマップするように、ISE または RADIUS サーバを構成します。ユーザまたはユーザ グループに特定のグループ ポリシーを設定すると、ダウンロード可能な ACL をプッシュし、バナーを設定し、VLAN を制限し、セッションに SGT を適用する高度なオプションを設定できます。これらの属性は、VPN 接続が確立した時点でそのグループに含まれているすべてのユーザに適用されます。

詳細については、『Cisco Identity Services Engine Administrator Guide』の「Configure Standard Authorization Policies」」の項およびの RADIUS サーバ属性 Firepower Threat Defense （1112 ページ）を参照してください。

図 *26 : AAA* サーバによるリモート アクセス *VPN* グループ ポリシーの選択



関連トピック

グループ ポリシー オブジェクトの設定 （624 ページ）
接続プロファイルの設定 （1105 ページ）

許可サーバによるグループポリシーまたはその他の属性の選択のオーバーライド

リモートアクセス VPN ユーザが VPN に接続すると、接続プロファイル内に設定されているグループ ポリシーとその他の属性がそのユーザに割り当てられます。ただし、リモート アクセス VPN システムの管理者は、ユーザまたはユーザ グループの許可プロファイルを設定するように ISE または RADIUS サーバを設定することによって、グループ ポリシーとその他の属性の選択を認証サーバに委任できます。ユーザが認証されると、これらの特定の承認属性が Firepower Threat Defense デバイスにプッシュされます。

始める前に

許可サーバとして RADIUS を使用したリモート アクセス VPN ポリシーが設定されていることを確認します。

ステップ 1 Firepower Management Center の Web インターフェイスで、[デバイス（Devices）] > [VPN] > [リモート アクセス（Remote Access）] を選択します。

ステップ 2 リストから既存のリモート アクセス ポリシーを選択し、対応する [編集（Edit）] アイコンをクリックします。

ステップ 3 まだ設定されていない場合は、許可サーバとして RADIUS または ISE を選択します。

ステップ 4 [詳細（Advanced）] > [グループ ポリシー（Group Policies）] を選択し、必要なグループ ポリシーを追加します。グループ ポリシー オブジェクトの詳細については、グループ ポリシー オブジェクトの設定 （624 ページ）を参照してください。

1 つのグループ ポリシーのみを 1 つの接続プロファイルにマップすることができますが、1 つのリモート アクセス VPN ポリシーには複数のグループ ポリシーを作成できます。これらのグループ ポリシーは、ISE または RADIUS サーバで参照でき、許可サーバの許可属性を割り当てることによって接続プロファイル内に設定されているグループ ポリシーをオーバーライドするように設定できます。

ステップ 5 ターゲットの Firepower Threat Defense デバイス上に設定を展開します。

ステップ 6 許可サーバで、IP アドレスとダウンロード可能な ACL の RADIUS 属性を持つ許可プロファイルを作成します。

リモート アクセスで選択した許可サーバにグループ ポリシーを設定すると、そのグループ ポリシーは、ユーザが認証された後にリモート アクセス VPN ユーザの接続プロファイルに設定されているグループ ポリシーをオーバーライドします。

関連トピック

グループ ポリシー オブジェクトの設定 （624 ページ）

ユーザ グループへの VPN アクセスの拒否

VPN を使用可能な認証済みのユーザまたはユーザ グループが不要な場合は、VPN アクセスを拒否するグループ ポリシーを設定できます。リモート アクセス VPN ポリシー内にグループ ポリシーを作成し、許可を行うため、ISE または RADIUS サーバの設定でそれを参照します。

始める前に

リモート アクセス ポリシー ウィザードを使用してリモート アクセス VPN が設定されており、リモート アクセス VPN ポリシーに認証の設定が行われていることを確認します。

ステップ 1 Firepower Management Center の Web インターフェイスで、[デバイス（Devices）] > [VPN] > [リモート アクセス（Remote Access）] を選択します。

ステップ 2 リストから既存のリモート アクセス ポリシーを選択し、対応する [編集（Edit）] アイコンをクリックします。

ステップ 3 [詳細（Advanced）] > [グループ ポリシー（Group Policies）] をクリックします。

ステップ 4 グループ ポリシーを選択して [編集（Edit）] アイコンをクリックするか、または新しいグループ ポリシーを追加します。

ステップ 5 [詳細（Advanced）] > [セッション設定（Session Settings）] を選択し、[ユーザごとの同時ログイン（Simultaneous Login Per User）] を 0（ゼロ）に設定します。
これにより、ユーザまたはユーザ グループは VPN への接続を完全に停止します。

ステップ 6 [保存（Save）] をクリックしてグループ ポリシーを保存した後、リモート アクセス VPN 設定を保存します。

ステップ 7 IETF RADIUS サーバ 属性 25 を送信し、対応するグループ ポリシー名にマップするようにユーザ/ユーザ グループの許可プロファイルを設定して、ISE または RADIUS サーバ サーバを設定します。

ステップ 8 リモート アクセス VPN ポリシーでは、ISE または RADIUS サーバを承認サーバとして構成できます。

ステップ 9 リモート アクセス VPN ポリシーを保存および展開します。

関連トピック

接続プロファイルの設定 （1105 ページ）

ユーザ グループに対する接続プロファイルの選択の制限

1 つの接続プロファイルをユーザまたはユーザ グループに適用する場合、接続プロファイルを無効にすることで、AnyConnect VPN クライアントを使用して接続するときに選択するユーザのグループ エイリアスまたは URL のリストが表示されないようにすることができます。

たとえば、モバイルユーザ、会社支給のラップトップのユーザ、個人のラップトップのユーザなど、異なる VPN ユーザ グループに組織が特定の設定を使用する場合は、それらの各ユーザ グループに固有の接続プロファイルを設定し、ユーザが VPN に接続したときに適切に接続プロファイルを適用することができます。

デフォルトでは、AnyConnect クライアントは Firepower Management Center に設定されており、Firepower Threat Defense に展開されている接続プロファイル（接続プロファイル名別、エイリアス別、またはエイリアス URL 別）のリストを表示します。カスタム接続プロファイルが設定されていない場合、AnyConnect は *DefaultWEBVPNGroup* 接続プロファイルを表示します。次の手順を使用して、1 つの接続プロファイルをユーザ グループに適用します。

始める前に

- Firepower Management Center の Web インターフェイスで、リモート アクセス VPN ポリシー ウィザードを使用し、[認証方式（Authentication Method）] を [クライアント証明書のみ（Client Certificate Only）] または [クライアント証明書と AAA（Client Certificate + AAA）] に設定してリモート アクセス VPN を設定します。証明書からユーザ名のフィールドを選択します。
- 認証のための ISE または RADIUSの サーバを設定し、グループ ポリシーを認証サーバに関連付けます。

ステップ 1 Firepower Management Center の Web インターフェイスで、[デバイス（Devices）] > [VPN] > [リモート アクセス（Remote Access）] を選択します。

ステップ 2 リストから既存のリモート アクセス ポリシーを選択し、対応する [編集（Edit）] アイコンをクリックします。

ステップ 3 [アクセス インターフェイス（Access Interfaces）] タブを選択し、[ログイン時にユーザによる接続プロファイルの選択を許可（Allow users to select the connection profile while logging in）] を無効にします。

ステップ 4 [詳細（Advanced）]> [証明書マップ（Certificate Maps）] をクリックします。

ステップ 5 [設定したルールを使用して証明書を接続プロファイルと照合する（Use the configured rules to match a certificate to a Connection Profile）] をオンにします。

ステップ 6 [証明書マップ名（Certificate Map Name）] を選択するか、または [追加（Add）] アイコンをクリックして証明書ルールを追加します。

ステップ 7 [接続プロファイル（Connection Profile）] を選択し、[OK] をクリックします。
この設定では、ユーザが AnyConnect クライアントから接続すると、そのユーザにはマップされた接続プロファイルが提供され、VPN を使用するように認証されます。

関連トピック

グループ ポリシー オブジェクトの設定 （624 ページ）
接続プロファイルの設定 （1105 ページ）

リモート アクセス VPN クライアントでの AnyConnect クライアント プロファイルの更新

AnyConnect クライアント プロファイルは、AnyConnect の一部として VPN クライアント システムに展開される管理者定義のエンドユーザ要件および認証ポリシーを含む XML ファイルです。これでエンドユーザが事前設定されたネットワーク プロファイルを使用できるようになります。

独立した設定ツールである GUI ベースの AnyConnect プロファイル エディタを使用して AnyConnect クライアント プロファイルを作成します。スタンドアロン プロファイル エディタを使用して、新しい AnyConnect プロファイルを作成したり、既存の AnyConnect プロファイルを変更したりできます。プロファイル エディタはシスコのソフトウェア ダウンロード センターからダウンロードできます。

詳細については、『Cisco AnyConnect Secure Mobility Client Administrator Guide』の該当するリリースの「AnyConnect プロファイル エディタ」の章を参照してください。

始める前に

- リモート アクセス ポリシー ウィザードを使用してリモート アクセス VPN が設定されており、設定が Firepower Threat Defense デバイスに展開されていることを確認します。新しいリモート アクセス VPN ポリシーの作成 （1098 ページ）を参照してください。
- Firepower Management Center の Web インターフェイスで、[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [VPN] > [AnyConnect ファイル（AnyConnect File）] に移動し、新しいAnyConnect クライアント イメージ を追加します。

ステップ 1 Firepower Management Center の Web インターフェイスで、[デバイス（Devices）] > [VPN] > [リモート アクセス（Remote Access）] を選択します。

ステップ 2 リストから既存のリモート アクセス VPN ポリシーを選択し、対応する [編集（Edit）] アイコンをクリックします。

ステップ 3 クライアントプロファイルに含まれている編集すべき接続プロファイルを選択して[編集（Edit）]をクリックします。

ステップ 4 [グループ ポリシーの編集（Edit Group Policy）] > [AnyConnect] > [プロファイル（Profiles）] をクリックします。

ステップ 5 リストからクライアント プロファイルの XML ファイルを選択するか、または [追加（Add）] アイコンをクリックして新しいクライアント プロファイルを追加します。

ステップ 6 グループポリシーと接続プロファイルを保存し、その後にリモートアクセスVPNポリシーを保存します。

ステップ 7 変更を展開します。
クライアント プロファイルに加えた変更は、リモート アクセス VPN ゲートウェイに接続したときに VPN クライアント上で更新されます。

関連トピック

グループ ポリシー オブジェクトの設定 （624 ページ）

リモート アクセス VPN の例

ユーザあたりの AnyConnect 帯域幅を制限する方法

ここでは、ユーザが Cisco AnyConnect VPN クライアントを使用して Firepower Threat Defense リモートアクセス VPN ゲートウェイに接続する場合に VPN ユーザに消費される最大帯域幅を制限する手順について説明します。Firepower Threat Defense で Quality of Service（QoS）ポリシーを使用して最大帯域幅を制限し、単一のユーザやグループまたは複数のユーザがリソース全体を引き継ぐことがないようにすることができます。この設定では、重要なトラフィックに優先順位を付け、帯域幅の占有を防止し、ネットワークを管理できます。トラフィックが最大レートを超えると、Firepower Threat Defenseは超過した分のトラフィックをドロップします。

	操作内容	詳細
ステップ 1	レルムを作成および設定します。	Active Directory レルムの作成および設定 （1155 ページ）。
ステップ 2	新しく作成したレルムで利用可能なユーザまたはグループの QoS ポリシーおよび QoS ルールを作成します。	QoS ポリシーとルールの作成 （1155 ページ）
ステップ 3	リモートアクセスVPNポリシーを設定し、ユーザ認証用に新しく作成したレルムを選択します。	リモート アクセス VPN ポリシーの作成または更新 （1157 ページ）

	操作内容	詳細
ステップ 4	リモートアクセス VPN ポリシーを展開します。	設定変更の展開 （447 ページ）

Active Directory レルムの作成および設定

ここでは、レルムを作成し、アクティビティをモニタする VPN ユーザおよびユーザ グループを指定する手順について説明します。

ステップ 1 Firepower Management Center web インターフェイスで、[システム（System）] > [統合（Integration）] > [レルム（Realms）] を選択します。

ステップ 2 [新規レルム（New Realm）] をクリックして、レルムの詳細を指定し、[OK] をクリックします。

ステップ 3 次のタブに必要な詳細を入力し、[保存（Save）] をクリックします。

- [ディレクトリ（Directory）]：1 つのレルムに複数のディレクトリを指定できます。この場合、ユーザ制御用のユーザ クレデンシャルとグループ クレデンシャルを照合するために、そのレルムの [ディレクトリ（Directory）] タブ ページにリストされている順序で、各ドメイン コントローラがクエリされます。

  レルム ディレクトリの設定 （2582 ページ）を参照してください。

- [レルム設定（Realm Configuration）]：レルムの作成中に入力されたレルム設定を更新できます。
- [ユーザダッシュボード（User Download）]：ユーザとグループは、Firepower Management Center のダウンロードに含めることも、ダウンロードから除外することもできます。

レルムが作成され、[レルム（Realms）] タブに追加されます。

ステップ 4 [ステート（State）] を右にスライドし、レルムをユーザ コントロールで使用できるように有効にします。レルムの管理 （2584 ページ）を参照してください

ステップ 5 ダウンロードアイコンをクリックし、ユーザおよびユーザ グループを Firepower Management Center にダウンロードします。ユーザとグループのダウンロード （2583 ページ）を参照してください

ステップ 6 **[保存（Save）]** をクリックします。

関連トピック

レルムの作成 （2576 ページ）

QoS ポリシーとルールの作成

管理対象デバイスに展開する QoS ポリシーにより レート制限が決まります。ユーザまたはユーザ グループが消費できる VPN 帯域幅を制限するようにレルムを選択すると、QoS ポリシーを作成できます。各 QoS ポリシーは、複数のデバイスを対象にすることができます。各デバイスで同時に展開可能な QoS ポリシーは 1 つです。

。

ステップ 1 Firepower Management Center web インターフェイスで、[デバイス（Devices）] > [QoS] > [新しいポリシー（New Policy）] を選択します。

ステップ 2 [名前（Name）] を入力し、必要に応じて [説明（Description）] を入力します。

ステップ 3 （オプション）QoS ポリシーを展開する [使用可能なデバイス（Available Devices）] を選択し、[ポリシーに追加（Add to Policy）] をクリックするか、[選択されたデバイス（Selected Devices）] にドラッグ アンド ドロップします。

（注） リモート アクセス VPN ポリシーを展開する同じデバイスを選択します。ポリシーを展開する前に、デバイスを割り当てる必要があります。

ステップ 4 QoS ポリシーの [ルール（Rules）] タブで、[ルールの追加（Add Rule）] をクリックします。

ステップ 5 [名前（Name）]を入力します。

ステップ 6 ルール コンポーネントを設定します。

- [有効（Enabled）]：ルールを有効にするかどうかを指定します。
- [QoSの適用（Apply QoS On）]：レート制限するインターフェイス（[宛先インターフェイスオブジェクトのインターフェイス（Interfaces in Destination Interface Objects）] または [送信元インターフェイスオブジェクトのインターフェイス（Interfaces in Source Interface Objects）]）を選択します。選択するインターフェイスは、入力されたインターフェイス制約（任意ではなく）と一致する必要があります。
- [インターフェイスごとのトラフィック制限（Traffic Limit Per Interface）]：ダウンロード制限とアップロード制限を Mbits/sec 単位で入力します。[無制限（Unlimited）] のデフォルト値にすると、一致するトラフィックはその方向でレート制限されません。
- [ユーザ（Users）]：[ユーザ（Users）] で、新しい作成したレルムおよびユーザを選択し、VPN トラフィックを制限します。追加する条件に対応する他のタブをクリックします。[QoSの適用（Apply QoS On）] の選択内容に対応する、送信元インターフェイスまたは宛先インターフェイスの条件を設定する必要があります。
- [コメント（Comments）]：[コメント（Comments）] をクリックし、コメントを追加し、[OK] をクリックします。

ステップ 7 ルールを保存します。

ポリシー エディタで、ルールの位置を設定します。クリックしてドラッグするか、または右クリック メニューを使用してカットアンドペーストを実行します。ルールには 1 から番号が付けられます。システムは、ルール番号の昇順で上から順に、ルールをトラフィックと照合します。トラフィックが一致する最初のルールは、そのトラフィックを処理するルールです。適切なルールの順序を指定することで、ネットワーク トラフィックの処理に必要なリソースが削減され、ルールのプリエンプションを回避できます。

ステップ 8 [保存（Save）] をクリックして、ポリシーを保存します。

関連トピック

QoS ポリシーの作成 （866 ページ）
QoS ポリシーによるレートの制限 （865 ページ）

リモート アクセス VPN ポリシーの作成または更新

ステップ 1 Firepower Management Center の Web インターフェイスで、[デバイス（Devices）] > [VPN] > [リモート アクセス（Remote Access）] を選択します。

ステップ 2 ウィザードを使用して新しいリモート アクセス VPN ポリシーを作成します。[認証サーバ（Authentication Server）] で新しく作成したレルムをするか、既存の VPN ポリシーを編集して、次の手順を実行します。

a) VPN ユーザに割り当てる接続プロファイルを選択し、[編集（Edit）] ボタンをクリックします。

b) [AAA] タブで、[認証方式（Authentication Method）] : [AAA] または [証明書と AAA（Certificate & AAA）] を選択します。

c) [認証サーバ（Authentication Server）] として必要なレルムを選択します。

d) 必要に応じて他の接続プロファイル オプションを更新し、接続プロファイルを保存します。

ステップ 3 リモート アクセス VPN ポリシーに必要な設定を完了し、[保存（Save）] をクリックします。

関連トピック

新しいリモート アクセス VPN 接続の設定 （1096 ページ）
接続プロファイルの設定 （1105 ページ）

ユーザ ID ベースのアクセス コントロール ルールに VPN アイデンティティを使用する方法

	操作内容	詳細
ステップ 1	レルムを作成および設定します。	Active Directory レルムの作成および設定 （1155 ページ）。
ステップ 2	アイデンティティ ポリシーを作成し、アイデンティティ ルールを追加します。	アイデンティティ ポリシーおよびアイデンティティ ルールの作成 （1158 ページ）。
ステップ 3：	アクセス コントロール ポリシーとアイデンティティ ポリシーを関連付けます。	アイデンティティポリシーとアクセスコントロール ポリシーの関連付け （1159 ページ）
ステップ 4	リモートアクセス VPN ポリシーを設定し、ユーザ認証用に新しく作成したレルムを選択します。	リモート アクセス VPN ポリシーの作成または更新 （1157 ページ）
ステップ 5	リモートアクセス VPN ポリシーを展開します。	設定変更の展開 （447 ページ）

Active Directory レルムの作成および設定

ここでは、レルムを作成し、アクティビティをモニタする VPN ユーザおよびユーザ グループを指定する手順について説明します。

ステップ 1 Firepower Management Center web インターフェイスで、[システム（System）] > [統合（Integration）] > [レルム（Realms）] を選択します。

ステップ 2 [新規レルム（New Realm）] をクリックして、レルムの詳細を指定し、[OK] をクリックします。

ステップ 3 次のタブに必要な詳細を入力し、[保存（Save）] をクリックします。

- [ディレクトリ（Directory）]：1 つのレルムに複数のディレクトリを指定できます。この場合、ユーザ制御用のユーザ クレデンシャルとグループ クレデンシャルを照合するために、そのレルムの [ディレクトリ（Directory）] タブ ページにリストされている順序で、各ドメイン コントローラがクエリされます。

  レルム ディレクトリの設定 （2582 ページ）を参照してください。

- [レルム設定（Realm Configuration）]：レルムの作成中に入力されたレルム設定を更新できます。
- [ユーザダッシュボード（User Download）]：ユーザとグループは、Firepower Management Center のダウンロードに含めることも、ダウンロードから除外することもできます。

レルムが作成され、[レルム（Realms）] タブに追加されます。

ステップ 4 [ステート（State）] を右にスライドし、レルムをユーザ コントロールで使用できるように有効にします。レルムの管理 （2584 ページ）を参照してください

ステップ 5 ダウンロードアイコンをクリックし、ユーザおよびユーザ グループを Firepower Management Center にダウンロードします。ユーザとグループのダウンロード （2583 ページ）を参照してください

ステップ 6 **[保存（Save）]** をクリックします。

関連トピック

レルムの作成 （2576 ページ）

アイデンティティ ポリシーおよびアイデンティティ ルールの作成

アイデンティティ ポリシーには、トラフィックに関連付けられているレルムと認証方式に基づいて、ユーザ認証を実行するアイデンティティ ルールが含まれます。アイデンティティ ルールでは、トラフィックのセットを、レルムおよび認証方式（パッシブ認証、アクティブ認証、または認証なし）と関連付けます。アイデンティティ ルールで呼び出す前に、使用するレルムおよび認証方式を完全に設定しておく必要があります。

ステップ 1 Firepower Management Center web インターフェイスで、[ポリシー（Policies）] > [アクセスコントロール（Access Control）] > [アイデンティティ（Identity）] を選択し、[新しいポリシー（New Policy）] をクリックします。

ステップ 2 [名前（Name）] および [説明（Description）] を入力し、[保存（Save）] をクリックします。

ステップ 3 ポリシーにルールを追加するには、[ルールの追加（Add Rule）] をクリックし、[名前（Name）] を入力します。

ステップ 4 ルールを**有効**にするかどうかを指定します。

ステップ 5 既存のカテゴリにルールを追加するには、ルールを[挿入（Insert）]する場所を指定します。新しいカテゴリを追加するには、[カテゴリの追加（Add Category）] をクリックします。

ステップ 6 リストからルール [アクション（Action）] を選択し、リモート アクセス VPN で設定されているインターフェイスを送信元インターフェイスとして選択します。

ステップ 7 [レルムと設定（Realms & Settings）] タブをクリックし、[レルム（Realms）] リストからアイデンティティ ルール用に作成された新しいレルムを選択します。リモート アクセス VPN ポリシーでユーザ認証用に選択したものと同じレルムを選択していることを確認してください。

ステップ 8 選択したレルムでユーザの優先設定を構成し、その他の必要なルール オプションを選択します。

ステップ 9 [追加（Add）] をクリックして、アイデンティティ ポリシーを保存します。

関連トピック

アイデンティティ ポリシーの作成および管理 （2637 ページ）

アイデンティティ ポリシーとアクセス コントロール ポリシーの関連付け

アイデンティティ ポリシーを、リモート アクセス VPN ポリシーが展開される Firepower Threat Defense デバイスに展開されているアクセス コントロール ポリシーに関連付ける必要があります。

ステップ 1 Firepower Management Center web インターフェイスで、[ポリシー（Policies）] > [アクセスコントロール（Access Control）] を選択し、[アクセスコントロール（Access Control）] をクリックします。

ステップ 2 必要なアクセス コントロール ポリシーを選択し、[編集（Edit）] アイコンをクリックします。

ステップ 3 アクセス コントロール ポリシー エディタで、[詳細（Advanced）] タブをクリックします。

ステップ 4 [アイデンティティポリシー設定（Identity Policy Settings）] 領域で編集アイコン（  ）をクリックします。

代わりに表示アイコン（  ）が表示される場合、設定は先祖ポリシーから継承され、設定を変更する権限がありません。 設定がロック解除されている場合は、[Inherit from base policy] をオフにして、編集を有効にします。

ステップ 5 ドロップダウン リストからアイデンティティ ポリシーを選択します。

編集アイコンをクリックすると、アイデンティティ ポリシーを編集できます。

ステップ 6 [OK] をクリックします。

ステップ 7 [保存（Save）] をクリックして、アクセス コントロール ポリシーを保存します。

関連トピック

アイデンティティ ポリシーの作成および管理 （2637 ページ）

リモート アクセス VPN ポリシーの作成または更新

ステップ 1 Firepower Management Center の Web インターフェイスで、[デバイス（Devices）] > [VPN] > [リモート アクセス（Remote Access）] を選択します。

ステップ 2 ウィザードを使用して新しいリモート アクセス VPN ポリシーを作成します。[認証サーバ（Authentication Server）] で新しく作成したレルムをするか、既存の VPN ポリシーを編集して、次の手順を実行します。

a) VPN ユーザに割り当てる接続プロファイルを選択し、[編集（Edit）] ボタンをクリックします。

b) [AAA] タブで、[認証方式（Authentication Method）] : [AAA] または [証明書と AAA（Certificate & AAA）] を選択します。

c) [認証サーバ（Authentication Server）] として必要なレルムを選択します。

d) 必要に応じて他の接続プロファイル オプションを更新し、接続プロファイルを保存します。

ステップ 3 リモート アクセス VPN ポリシーに必要な設定を完了し、[保存（Save）] をクリックします。

関連トピック

新しいリモート アクセス VPN 接続の設定 （1096 ページ）
接続プロファイルの設定 （1105 ページ）

第 45 章

Firepower Threat Defense の VPN モニタリング

この章では、Firepower Threat Defense VPN のモニタリング ツール、パラメータ、および統計情報について説明します。

VPN サマリ ダッシュボード

Firepower システム ダッシュボードは、システムによって収集および生成されたイベントに関するデータを含む、現在のシステムのステータスを概要的なビューとして提供します。VPN ダッシュボードを使用して、ユーザの現在のステータス、デバイス タイプ、クライアント アプリケーション、ユーザの位置情報、接続時間などの VPN ユーザに関する統合情報を表示できます。

VPN サマリ ダッシュボードの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス（Access）
エクスポート コンプライアンス	該当なし	FTD	リーフのみ	Admin

リモート アクセス VPN は、モバイル ユーザや在宅勤務者などのリモート ユーザにセキュアな接続を提供します。これらの接続をモニタリングすることで、接続とユーザ セッションのパフォーマンスの重要なインジケータを一目で把握できます。

ステップ 1 **[概要（Overview）] > [ダッシュボード（Dashboards）] > [アクセス制御されたユーザの統計情報（Access Controlled User Statistics）]** を選択し、[VPN] ダッシュボードを選択します。

ステップ 2 次のリモート アクセス VPN 情報ウィジェットを表示します。

- 現在の VPN ユーザ数（時間別）
- 現在の VPN ユーザ数（クライアント アプリケーション別）
- 現在の VPN ユーザ数（デバイス別）
- VPN ユーザ数（転送されたデータ別）
- VPN ユーザ数（時間別）
- VPN ユーザ数（クライアント アプリケーション別）
- VPN ユーザ数（クライアントの国別）

次のタスク

[VPN] ダッシュボードは網羅的なデータを提供する複雑で高度にカスタマイズ可能なモニタリング機能です。

- Firepower システムでダッシュボードを使用する方法の詳細については、ダッシュボード（321 ページ） を参照してください。
- VPN ダッシュボード ウィジェットを変更する方法については、ウィジェットの設定（341 ページ） を参照してください。

VPN セッションとユーザ情報

Firepower システムでは、VPN 関連アクティビティを含む、ネットワーク上のユーザ アクティビティの詳細を伝達するイベントを生成します。Firepower システムのモニタリング機能を使用すると、リモート アクセス VPN の問題が存在するかどうか、および存在する場所を迅速に特定できます。この情報を利用し、ネットワーク管理ツールを使用して、ネットワークおよびユーザの問題を軽減したり、なくしたりすることが可能です。オプションで、必要に応じてリモート アクセス VPN ユーザをログアウトすることができます。

リモート アクセス VPN アクティブ セッションの表示

[分析（Analysis）] > [ユーザ（Users）] > [アクティブなセッション（Active Sessions）]

ユーザ名、ログイン時間、認証タイプ、割り当て済み/パブリック IP アドレス、デバイスの詳細、クライアントのバージョン、エンドポイント情報、スループット、帯域幅消費グループ ポリシー、トンネル グループなどのサポート情報を使用して、現在ログインしている VPN ユーザを任意の時点で表示できます。また、現在のユーザ情報をフィルタリングし、ユーザをログアウトし、要約リストからユーザを削除する機能も提供されます。

- アクティブ セッションの詳細については、アクティブ セッション データの表示（3255 ページ） を参照してください。

- アクティブ セッション テーブルのカラムの内容について詳しく調べるには、アクティブ セッション、ユーザ、およびユーザ アクティビティ データ （3245 ページ） を参照してください。

リモート アクセス VPN ユーザ アクティビティの表示

[Analysis] > [Users] > [User Activity]

ネットワーク上のユーザアクティビティの詳細を表示できます。システムは履歴イベントを記録し、接続プロファイル情報、IPアドレス、位置情報、接続時間、スループット、デバイス情報などの VPN 関連情報が含まれています。

- ユーザアクティビティについての詳細は、ユーザアクティビティデータの表示 （3262 ページ） を参照してください。
- ユーザ アクティビティ テーブルのカラムの内容について詳しく調べるには、アクティブ セッション、ユーザ、およびユーザ アクティビティ データ （3245 ページ） を参照してください。

VPN ヘルス イベント

[ヘルス イベント（Health Events）] ページでは、Firepower Management Center のヘルス モニタで記録された VPN ヘルス イベントを表示できます。Firepower システム デバイス間で 1 つ以上の VPN トンネルがダウンすると、次のイベントが追跡されます。

- 次を対象とした VPN 7000 & 8000 シリーズ
- Firepower Threat Defense のサイト間 VPN
- Firepower Threat Defense のリモート アクセス VPN

ヘルス モニタを使用して、Firepower システム展開全体の重要な機能のステータスを確認する方法の詳細については、ヘルス モニタリング （349 ページ） を参照してください。

VPN ヘルス イベントの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Maint/Any Security Analyst

Firepower Management Center 上の [ヘルス イベント（Health Events）] ページからヘルス イベントにアクセスした場合は、すべての管理対象アプライアンスのすべてのヘルスイベントが取得されます。表示したいヘルスイベントを生成したモジュールを指定することによって、イベントを絞り込むことができます。

ステップ 1 **[システム（System）] > [ヘルス（Health）] > [イベント（Events）]** を選択します。

ステップ 2 [モジュール名（Module Name）] 列で [VPN ステータス（VPN Status）] を選択します。

システムのヘルス イベントの詳細については、ヘルス イベント ビュー （376 ページ） を参照してください。

第 46 章

Firepower Threat Defense の VPN のトラブルシューティング

この章では、Firepower Threat Defense VPN のトラブルシューティング ツールとデバッグ情報について説明します。

システム メッセージ

メッセージ センターは、トラブルシューティングを開始する場所です。この機能を使用すると、システムの使用状況およびステータスについて継続的に生成されるメッセージを確認できます。メッセージ センターを開くには、メイン メニューの [展開（Deploy）] ボタンのすぐ右側にある [システム ステータス（System Status）] アイコンをクリックします。メッセージ センターの使用方法については、システム メッセージ （410 ページ）を参照してください。

VPN システム ログ

FTD デバイスのシステム ロギング（syslog）を有効にすることができます。情報をロギングすることで、ネットワークの問題またはデバイス設定の問題を特定して分離できます。VPN ロギングを有効にすると、これらの syslog は FTD デバイスから Firepower Management Center に送信され、解析とアーカイブが行われます。

表示される VPN syslog には、デフォルトの重大度レベル「ERROR」以上があります（変更されない限り）。VPN ロギングは、FTD プラットフォーム設定によって管理されます。対象となるデバイスの FTD プラットフォーム設定ポリシーで [VPN ロギング設定（VPN Logging Settings）] を編集して、メッセージの重大度を調整できます（**[プラットフォーム設定（Platform Settings）]** > **[Syslog]** > **[ロギングの設定（Logging Setup）]**）。VPN ロギングの有効化、syslog サーバの設定、およびシステム ログの表示の詳細については、Syslog の設定概要 （1385 ページ） を参照してください。

（注） デバイスがサイト間 VPN またはリモート アクセス VPN で設定されると、VPN syslog はデフォルトで自動的に Firepower Management Center に送信されます。

VPN システム ログの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス（Access）
エクスポート コンプライアンス	該当なし	FTD	リーフのみ	Admin

Firepower システムは、VPN の問題の原因に関する追加情報を収集するのに役立つイベント情報をキャプチャします。表示される VPN syslog には、デフォルトの重大度レベル「ERROR」以上があります（変更されない限り）。デフォルトでは、行は [時間（Time）] 列でソートされています。

始める前に

FTD プラットフォーム設定の [FMC へのロギングを有効化（Enable Logging to FMC）] チェックボックスをオンにして、VPN ロギングを有効にします（**[デバイス（Devices）]** > **[プラットフォーム設定（Platform Settings）]** > **[Syslog]** > **[ロギングの設定（Logging Setup）]**）。VPN ロギングの有効化、syslog サーバの設定、およびシステム ログの表示の詳細については、Syslog の設定概要 （1385 ページ） を参照してください。

ステップ 1 **[デバイス（Devices）]** > **[VPN]** > **[トラブルシューティング（Troubleshooting）]** を選択します。

ステップ 2 次の選択肢があります。

- 検索：現在のメッセージ情報をフィルタリングするには、[検索の編集（Edit Search）] をクリックします。
- 表示：選択したメッセージに関連付けられた VPN の詳細をビューに表示するには、[表示（View）] をクリックします。
- すべて表示：すべてのメッセージの VPN の詳細をビューに表示するには、[すべて表示（View All）] をクリックします。
- 削除：選択したメッセージをデータベースから削除するには [削除（Delete）] をクリックするか、またはすべてのメッセージを削除するには [すべて削除（Delete All）] をクリックします。

debug コマンド

ここでは、debug コマンドを使用して、VPN 関連の問題を診断および解決する方法について説明します。すべての使用可能なデバッグ コマンドがこのセクションで説明されているわけではありません。ここに含まれているコマンドは、VPN 関連の問題の診断における有用性に基づいています。

使用上のガイドライン

デバッグ出力は CPU プロセスで高プライオリティが割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。したがって、**debug** コマンドを使用するのは、特定の問題のトラブルシューティング時か、または Cisco Technical Assistance Center（TAC）とのトラブルシューティング セッション時に限定してください。さらに、**debug** コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

CLI セッションでのみデバッグ出力を確認できます。出力は、コンソール ポートに接続したとき、または診断 CLI（**system support diagnostic-cli** と入力）で直接入手できます。また、**show console-output** コマンドを使用して、通常の Firepower Threat Defense CLI からの出力を確認することもできます。

特定の機能のデバッグ メッセージを表示するには、**debug** コマンドを使用します。デバッグ メッセージの表示を無効にするには、このコマンドの **no** 形式を使用します。すべてのデバッグ コマンドをオフにするには、**no debug all** を使用します。

debug *feature* ［*subfeature*］［*level*］
no debug *feature* ［*subfeature*］

構文の説明

feature	デバッグをイネーブルにする機能を指定します。使用可能な機能を表示するには、**debug ?** コマンドを使用して CLI ヘルプを表示します。
subfeature	（オプション）機能によっては、1 つ以上のサブ機能のデバッグ メッセージをイネーブルにできます。使用可能なサブ機能を表示するには ? を使用します。
level	（オプション）デバッグ レベルを指定します。このレベルは、一部の機能で使用できない場合があります。使用可能なレベルを表示するには ? を使用します。

コマンド デフォルト

デフォルトのデバッグ レベルは 1 です。

例

リモート アクセス VPN 上で複数のセッションを実行すると、ログのサイズを考慮するとトラブルシューティングが困難になることがあります。**debug webvpn condition**

コマンドを使用して、デバッグ プロセスをより正確に絞り込むためのフィルタを設定できます。

debug webvpn condition { **group** *name* | **p-ipaddress** *ip_address* [{ **subnet** *subnet_mask*| **prefix** *length*}] | **reset** | **user** *name*}

それぞれの説明は次のとおりです。

- **group** *name* は、グループ ポリシー（トンネル グループまたは接続プロファイルではない）でフィルタ処理を行います。
- **p-ipaddress** *ip_address* [{**subnet** *subnet_mask* | **prefix** *length*}] は、クライアントのパブリック IP アドレスでフィルタ処理を行います。サブネットマスク（IPv4）またはプレフィックス（IPv6）はオプションです。
- **reset** はすべてのフィルタをリセットします。**no debug webvpn condition** コマンドを使用して、特定のフィルタをオフにできます。
- **user** *name* は、ユーザ名でフィルタ処理を行います。

複数の条件を設定すると、条件が結合（AND で連結）され、すべての条件が満たされた場合にのみデバッグが表示されます。

条件フィルタを設定したら、基本の **debug webvpn** コマンドを使用してデバッグをオンにします。条件を設定するだけではデバッグは有効になりません。デバッグの現在の状態を表示するには、**show debug** および **show webvpn debug-condition** コマンドを使用します。

次に、ユーザ jdoe で条件付きデバッグを有効にする例を示します。

```
firepower# debug webvpn condition user jdoe

firepower# show webvpn debug-condition
INFO: Webvpn conditional debug is turned ON
INFO: User name filters:
INFO: jdoe

firepower# debug webvpn
INFO: debug webvpn  enabled at level 1.

firepower# show debug
debug webvpn  enabled at level 1
INFO: Webvpn conditional debug is turned ON
INFO: User name filters:
INFO: jdoe
```

関連コマンド

コマンド	説明
show debug	現在アクティブなデバッグ設定を示します。
undebug	ある機能のデバッグを無効にします。このコマンドは **no debug** の同意語です。

debug aaa

認証、認可、アカウンティング（AAA、「トリプルA」と発音）に関連するデバッグの構成または設定については、次のコマンドを参照してください。

debug *aaa* ［*accounting* | *authentication* | *authorization* | *common* | *internal* | *shim* | *url-redirect*］

構文の説明

aaa	AAA のデバッグをイネーブルにします。使用可能なサブ機能を表示するには ? を使用します。
accounting	（オプション）AAA アカウンティング デバッグを有効にします。
認証	（オプション）AAA 認証デバッグを有効にします。
authorization	（オプション）AAA 認可デバッグを有効にします。
common	（オプション）AAA 共通デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
internal	（オプション）AAA 内部デバッグを有効にします。
shim	（オプション）AAA shim デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
url-redirect	（オプション）AAA URL リダイレクト デバッグを有効にします。

コマンド デフォルト

デフォルトのデバッグ レベルは 1 です。

関連コマンド

コマンド	説明
show debug aaa	AAA の現在アクティブなデバッグ設定を示します。
undebug aaa	AAA のデバッグを無効にします。このコマンドは **no debug aaa** の同意語です。

debug crypto

暗号に関連するデバッグの構成または設定については、次のコマンドを参照してください。

debug *crypto* ［*ca* | *condition* | *engine* | *ike-common* | *ikev1* | *ikev2* | *ipsec* | *ss-apic*］

構文の説明

crypto	*crypto* のデバッグをイネーブルにします。使用可能なサブ機能を表示するには ? を使用します。
ca	（オプション）PKIデバッグ レベルを指定します。使用可能なサブ機能を表示するには ? を使用します。

condition	（オプション）IPsec/ISAKMP デバッグ フィルタを指定します。使用可能なフィルタを表示するには ? を使用します。
engine	（オプション）暗号エンジン デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
ike-common	（オプション）IKE 共通デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
ikev1	（オプション）IKE バージョン 1 デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
ikev2	（オプション）IKE バージョン 2 デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
ipsec	（オプション）IPsec デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
condition	(オプション）暗号化セキュア ソケット API デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
vpnclient	（オプション）EasyVPN クライアント デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。

コマンド デフォルト

デフォルトのデバッグ レベルは 1 です。

関連コマンド

コマンド	説明
show debug crypto	暗号化の現在アクティブなデバッグ設定を示します。
undebug crypto	暗号化のデバッグを無効にします。このコマンドは **no debug crypto** の同意語です。

debug crypto ca

crypto ca に関連付けられたデバッグの構成または設定については、次のコマンドを参照してください。

debug *crypto ca* ［*cluster* | *messages* | *periodic-authentication* | *scep-proxy* | *transactions* | *trustpool*］［*1-255*］

構文の説明

crypto ca	*crypto ca* のデバッグをイネーブルにします。使用可能なサブ機能を表示するには ? を使用します。
cluster	（オプション）PKI クラスタ デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。

cmp	（オプション）CMP トランザクション デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
messages	（オプション）PKI の入力/出力メッセージのデバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
periodic-authentication	（オプション）PKI 定期認証デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
scep-proxy	（オプション）SCEP プロキシデバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
server	（オプション）ローカル CA サーバのデバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
transactions	（オプション）PKI トランザクションデバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
trustpool	（オプション）トラストプール デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
1-255	（オプション）デバッグ レベルを指定します。

コマンド デフォルト

デフォルトのデバッグ レベルは 1 です。

関連コマンド

コマンド	説明
show debug crypto ca	crypto ca の現在アクティブなデバッグ設定を示します。
undebug	crypto ca のデバッグを無効にします。このコマンドは **no debug crypto ca** の同意語です。

debug crypto ikev1

インターネット キー エクスチェンジ バージョン 1（IKEv1）に関連するデバッグの構成または設定については、次のコマンドを参照してください。

debug *crypto ikev1* ［*timers*］［*1-255*］

構文の説明

ikev1	*ikev1* のデバッグをイネーブルにします。使用可能なサブ機能を表示するには ? を使用します。
timers	（オプション）IKEv1 タイマーのデバッグを有効にします。
1-255	（オプション）デバッグ レベルを指定します。

コマンド デフォルト

デフォルトのデバッグ レベルは 1 です。

関連コマンド

コマンド	説明
show debug crypto ikev1	IKEv1 の現在アクティブなデバッグ設定を示します。
undebug crypto ikev1	IKEv1 のデバッグを無効にします。このコマンドは **no debug crypto ikev1** の同意語です。

debug crypto ikev2

インターネット キー エクスチェンジ バージョン 2（IKEv2）に関連するデバッグの構成または設定については、次のコマンドを参照してください。

debug *crypto ikev2* ［*ha* | *platform* | *protocol* | *timers*］

構文の説明

ikev2	デバッグ *ikev2* を有効にします。使用可能なサブ機能を表示するには ? を使用します。
ha	（オプション）IKEv2 HA デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
platform	（オプション）IKEv2 プラットフォーム デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
protocol	（オプション）IKEv2 プロトコル デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
timers	（オプション）IKEv2 タイマーのデバッグを有効にします。

コマンド デフォルト

デフォルトのデバッグ レベルは 1 です。

関連コマンド

コマンド	説明
show debug crypto ikev2	IKEv2 の現在アクティブなデバッグ設定を示します。
undebugcrypto ikev2	IKEv2 のデバッグを無効にします。このコマンドは **no debug crypto ikev2** の同意語です。

debug crypto ipsec

IPsec に関連するデバッグの構成または設定については、次のコマンドを参照してください。

debug *crypto ipsec* ［*1-255*］

構文の説明

ipsec	*ipsec* のデバッグをイネーブルにします。使用可能なサブ機能を表示するには ? を使用します。

1-255	（オプション）デバッグ レベルを指定します。

コマンド デフォルト

デフォルトのデバッグ レベルは 1 です。

関連コマンド

コマンド	説明
show debug crypto ipsec	IPsec の現在アクティブなデバッグ設定を示します。
undebugcrypto ipsec	IPsec のデバッグを無効にします。このコマンドは **no debug crypto ipsec** の同意語です。

debug ldap

LDAP（Lightweight Directory Access Protocol）に関連するデバッグの構成または設定については、次のコマンドを参照してください。

debug *ldap* ［*1-255*］

構文の説明

ldap	LDAP のデバッグをイネーブルにします。使用可能なサブ機能を表示するには ? を使用します。
1-255	（オプション）デバッグ レベルを指定します。

コマンド デフォルト

デフォルトのデバッグ レベルは 1 です。

関連コマンド

コマンド	説明
show debug ldap	LDAP の現在アクティブなデバッグ設定を示します。
undebugldap	LDAP のデバッグを無効にします。このコマンドは **no debug ldap** の同意語です。

debug ssl

SSL セッションに関連するデバッグの構成または設定については、次のコマンドを参照してください。

debug *ssl* ［*cipher* | *device*］［*1-255*］

構文の説明

ssl	SSL のデバッグをイネーブルにします。使用可能なサブ機能を表示するには ? を使用します。
cipher	（オプション）SSL 暗号デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。

device	（オプション）SSL デバイス デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
1-255	（オプション）デバッグ レベルを指定します。

コマンド デフォルト

デフォルトのデバッグ レベルは 1 です。

関連コマンド

コマンド	説明
show debug ssl	SSL の現在アクティブなデバッグ設定を示します。
undebug ssl	SSL のデバッグを無効にします。このコマンドは **no debug ssl** の同意語です。

debug webvpn

WebVPN に関連するデバッグの構成または設定については、次のコマンドを参照してください。

debug *webvpn* [*anyconnect* | *chunk* | *cifs* | *citrix* | *compression* | *condition* | *cstp-auth* | *customization* | *failover* | *html* | *javascript* | *kcd* | *listener* | *mus* | *nfs* | *request* | *response* | *saml* | *session* | *task* | *transformation* | *url* | *util* | *xml*]

構文の説明

webvpn	WebVPN のデバッグをイネーブルにします。使用可能なサブ機能を表示するには ? を使用します。
anyconnect	（オプション）WebVPN AnyConnect デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
chunk	（オプション）WebVPN チャンク デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
cifs	（オプション）WebVPN CIFS デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
citrix	（オプション）WebVPN Citrix デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
compression	（オプション）WebVPN 圧縮デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
condition	（オプション）WebVPN フィルタ条件デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
cstp-auth	（オプション）WebVPN CSTP 認証デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。

customization	（オプション）WebVPNカスタマイズデバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
failover	（オプション）WebVPN フェールオーバー デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
html	（オプション）WebVPN HTML デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
javascript	（オプション）WebVPN Javascript デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
kcd	（オプション）WebVPN KCD デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
listener	（オプション）WebVPN リスナー デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
mus	（オプション）WebVPN MUS デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
nfs	（オプション）WebVPN NFS デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
request	（オプション）WebVPN 要求デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
response	（オプション）WebVPN 応答デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
saml	（オプション）WebVPN SAML デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
session	（オプション）WebVPN セッション デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
task	（オプション）WebVPN タスク デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
transformation	（オプション）WebVPN 変換デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
url	（オプション）WebVPN URL デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
util	（オプション）WebVPN ユーティリティ デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
xml	（オプション）WebVPN XML デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。

コマンド デフォルト

デフォルトのデバッグ レベルは 1 です。

関連コマンド

コマンド	説明
show debug webvpn	WebVPN の現在アクティブなデバッグ設定を示します。
undebug webvpn	WebVPN のデバッグを無効にします。このコマンドは **no debug webvpn** の同意語です。

第 XII 部

Firepower Threat Defense の詳細設定

第 47 章

Threat Defense サービス ポリシー

Firepower Threat Defense サービス ポリシーを使用して、特定のトラフィック クラスにサービスを適用することができます。たとえば、サービス ポリシーを使用すると、すべての TCP アプリケーションに適用されるタイムアウト コンフィギュレーションではなく、特定の TCP アプリケーションに固有のタイムアウト コンフィギュレーションを作成できます。サービス ポリシーは、1 つのインターフェイスに適用されるか、またはグローバルに適用される複数のアクションまたはルールで構成されます。

Firepower Threat Defense のサービス ポリシーについて

Firepower Threat Defense サービス ポリシーを使用して、特定のトラフィック クラスにサービスを適用することができます。サービスポリシーを使用すると、デバイスまたは特定のインターフェイスに着信するすべての接続に同じサービス以外を適用することができます。

トラフィック クラスはインターフェイスと拡張アクセス コントロール リスト（ACL）の組み合わせです。ACL の「許可」ルールによってクラスに含まれる接続が決定されます。ACL の「拒否」トラフィックには、そのトラフィックに適用されているサービスがないというだけで、これらの接続は実際にはドロップされません。IP アドレスと TCP/UCP ポートを使用し、必要な精度で対応する接続を特定できます。

トラフィック クラスには 2 つのタイプがあります。

- インターフェイスベースのルール：サービス ポリシー ルールでセキュリティ ゾーンまたはインターフェイス グループを指定すると、インターフェイス オブジェクトに含まれているすべてのインターフェイスを通過する ACL の「許可」トラフィックにルールが適用されます。

特定の機能では、入力インターフェイスに適用されたインターフェイスベースのルールがグローバル ルールよりも常に優先されます。入力インターフェイスベースのルールを接続に適用すると、対応するグローバル ルールは無視されます。入力インターフェイスまたはグローバル ルールが適用されていない場合は、出力インターフェイスのインターフェイス サービス ルールが適用されます。

- グローバル ルール：すべてのインターフェイスにこれらのルールが適用されます。インターフェイスベースのルールを接続に適用しない場合は、グローバル ルールが確認され、ACL で「許可」されているすべての接続に適用されます。何も適用しない場合は、どのサービスも適用されずに接続が続行されます。

特定の接続が一致するのは、特定の機能のインターフェイス ベースまたはグローバルのいずれか 1 つのトラフィック クラスのみです。特定のインターフェイス オブジェクト/トラフィック フローの組み合わせには設定できるルールは 1 つのみです。

サービス ポリシーのルールは、アクセス制御ルールの後に適用されます。これらのサービスは、許可している接続にのみ設定されます。

FlexConfig とその他の機能にサービス ポリシーを関連付ける方法

バージョン 6.3(0) よりも前では、接続関連のサービス ルールは TCP_Embryonic_Conn_Limit と TCP_Embryonic_Conn_Timeout の事前定義の FlexConfig オブジェクトを使用して設定できました。これらのオブジェクトを削除し、Firepower Threat Defense Service サービス ポリシーを使用してルールを作り直す必要があります。これらの接続関連コマンドの実装にカスタム FlexConfig オブジェクトを作成した場合（**set connection** コマンド）は、それらのオブジェクトも削除し、サービス ポリシー経由で機能を実装する必要があります。

接続関連のサービス ポリシーの機能は、その他のサービスルールで実装された機能とは異なる機能グループとして処理されます。そのため、トラフィック クラスが重複する問題に直面することはありません。ただし、次を設定する際には十分注意してください。

- QoS ポリシー ルールはサービス ポリシー CLI を使用して実装されます。これらのルールは接続ベースのサービス ポリシー ルールよりも前に適用されます。ただし、QoS と接続の両方の設定を同じトラフィック クラスか、または重複するトラフィック クラスに適用できます。

- FlexConfig ポリシーを使用してカスタマイズされたアプリケーションのインスペクションと NetFlow を実装できます。**show running-config** コマンドを使用して、サービス ルールをすでに設定している **policy-map** コマンド、**class-map** コマンド、**service-policy** コマンドなど、CLI を調査できます。NetFlow とアプリケーション インスペクションは QoS および接続の設定との互換性はありますが、FlexConfig を実装する前に既存の設定を把握しておく必要があります。接続の設定は、アプリケーション インスペクションと NetFlow よりも前に適用されます。

（注） Firepower Threat Defense サービス ポリシーから作成されたトラフィック クラスは **class_map**_*ACLname* という名前になります。*ACLname* はサービス ポリシー ルールで使用された拡張 ACL オブジェクトの名前。

接続設定に関する情報

接続の設定は、Firepower Threat Defense デバイス を経由する TCP フローなどのトラフィック接続の管理に関連するさまざまな機能で構成されます。一部の機能は、特定のサービスを提供するために設定する名前付きコンポーネントです。

接続の設定には、次が含まれています。

- **さまざまなプロトコルのグローバル タイムアウト**：すべてのグローバル タイムアウトにデフォルト値があるため、早期の接続の切断が発生した場合にのみグローバル タイムアウトを変更する必要があります。Firepower Threat Defense のプラットフォーム ポリシーにグローバル タイムアウトを設定します。**[Devices]** > **[Platform Settings]** を選択します。
- **トラフィック クラスごとの接続タイムアウト**：サービス ポリシーを使用して、特定のタイプのトラフィックのグローバル タイムアウトを上書きできます。すべてのトラフィック クラスのタイムアウトにデフォルト値があるため、それらの値を設定する必要はありません。
- **接続制限と TCP 代行受信**：デフォルトでは、Firepower Threat Defense デバイス を経由する（または宛先とする）接続の数に制限はありません。サービス ポリシー ルールを使用して特定のトラフィック クラスに制限を設定することで、サービス妨害（DoS）攻撃からサーバを保護できます。特に、初期接続（TCP ハンドシェイクを完了していない初期接続）に制限を設定できます。これにより、SYN フラッディング攻撃から保護されます。初期接続の制限を超えると、TCP 代行受信コンポーネントは、プロキシ接続に関与してその攻撃が抑制されていることを確認します。
- **Dead Connection Detection（DCD; デッド接続検出）**：アイドル タイムアウトの設定を超えたために接続が閉じられるように、頻繁にアイドル状態になっても有効な接続を維持する場合、Dead Connection Detection をイネーブルにして、アイドル状態でも有効な接続を識別してそれを維持することができます（接続のアイドル タイマーをリセットすることによって）。アイドル時間を超えるたびに、DCD は接続の両側にプローブを送信して、接続が有効であることを両側で合意しているかどうかを確認します。**show service-policy** コマンド出力には、DCD からのアクティビティ量を示すためのカウンタが含まれています。
- **TCP シーケンスのランダム化**：それぞれの TCP 接続には 2 つの ISN（初期シーケンス番号）が割り当てられており、そのうちの 1 つはクライアントで生成され、もう 1 つはサーバで生成されます。デフォルトでは、Firepower Threat Defense デバイス は、着信と発信の両方向で通過する TCP SNY の ISN をランダム化します。ランダム化により、攻撃者が新しい接続に使用される次の ISN を予測して新しいセッションをハイジャックするのを阻止します。必要に応じて、トラフィック クラスごとにランダム化をディセーブルにすることができます。

- **TCP 正規化**：TCP ノーマライザは、異常なパケットから保護します。一部のタイプのパケット異常をトラフィック クラスで処理する方法を設定できます。FlexConfig ポリシーを使用して TCP 正規化を設定できます。
- **TCPステートバイパス**：ネットワークで非対称ルーティングを使用するかどうかをチェックする TCP ステートをバイパスできます。

サービス ポリシーのガイドラインと制限事項

- サービス ポリシーは、ルーテッド モードまたはトランスペアレント モードのいずれかのルーテッド インターフェイスまたはスイッチ インターフェイスのみに適用されます。インライン セットまたはパッシブ インターフェイスには適用されません。
- 特定のインターフェイスまたはグローバル ポリシーに最大 25 のトラフィック クラスを設定できます。つまり、25 を超えるサービス ポリシー ルールを特定のセキュリティ ゾーンまたはインターフェイス グループのグローバル ポリシーに設定することはできません。ただし、インターフェイスの場合、同じインターフェイスをセキュリティ ゾーンとインターフェイス グループに表示できるため、実際の制限はゾーンやグループではなく、インターフェイスに基づきます。したがって、ゾーン/グループのメンバーシップに基づき、ゾーン/グループごとに 25 のルールを設定できない場合があります。
- 特定のインターフェイス オブジェクト/トラフィック フローの組み合わせに設定できるルールは 1 つのみです。
- コンフィギュレーションに対してサービス ポリシーの変更を加えた場合は、すべての新しい接続で新しいサービス ポリシーが使用されます。既存の接続では、その接続が確立された時点で設定されていたポリシーの使用が続行されます。すべての接続に新しいポリシーをすぐに使用するには、現在の接続を切断し、新しいポリシーを使用して再度接続できるようにする必要があります。SSH またはコンソール CLI セッションから **clear conn** コマンドまたは **clear local-host** コマンドを入力します。

Firepower Threat Defense のサービス ポリシーの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin Access Admin Network Admin

Firepower Threat Defense サービス ポリシーを使用して、特定のトラフィック クラスにサービスを適用することができます。たとえば、サービス ポリシーを使用すると、すべての TCP アプリケーションに適用されるタイムアウト コンフィギュレーションではなく、特定の TCP アプリケーションに固有のタイムアウト コンフィギュレーションを作成できます。サービス ポリ

シーは、1 つのインターフェイスに適用されるか、またはグローバルに適用される複数のアクションまたはルールで構成されます。

ステップ 1 **[ポリシー（Policies）] > [アクセス制御（Access Control）] > [アクセス制御（Access Control）]** を選択し、編集する Firepower Threat Defense のサービス ポリシーのアクセス コントロール ポリシーで [Edit] アイコン（✎） をクリックします。

ステップ 2 [詳細（Advanced）] タブをクリックします。

ステップ 3 **Threat Defense サービス ポリシー** グループで [Edit] アイコン（✎） をクリックします。

既存のポリシーが表示されたダイアログボックスが開きます。ポリシーは番号付きのルールのリストから構成されており、グローバル ルール（すべてのインターフェイスに適用）とインターフェイスベースのルールに分かれています。テーブルには、インターフェイス オブジェクトおよび拡張アクセス コントロール リスト名（これらの組み合わせでルールのトラフィック クラスを定義）と適用されたサービスが表示されます。

ステップ 4 次のいずれかを実行します。

- [ルールの追加（Add Rule）] をクリックして、新しいルールを作成します。サービス ポリシー ルールの設定 （1183 ページ）を参照してください。
- [Edit] アイコン（✎） をクリックして、既存のルールを編集します。サービス ポリシー ルールの設定（1183 ページ）を参照してください。
- [Delete] アイコン（🗑） をクリックしてルールを削除します。
- ルールをクリックし、移動先の新しい場所までドラッグします。インターフェイスとグローバル リスト間ではルールはドラッグできません。その代りに、ルールを編集してインターフェイス/グローバル設定を変更する必要があります。接続と一致するリスト内の最初のルールが接続に適用されます。

ステップ 5 ポリシーの編集が終了したら、[OK] をクリックします。

ステップ 6 [詳細（Advanced）] タブ ウィンドウで [保存（Save）] をクリックします。このボタンをクリックするまでは変更は保存されません。

サービス ポリシー ルールの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin Access Admin Network Admin

特定のトラフィック クラスにサービスを適用するサービス ポリシー ルールを設定します。

始める前に

[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [アクセス リスト（Access List）] > [拡張（Extended）] に移動し、ルールが適用されるトラフィックを定義する拡張アクセス リストを作成します。ルールは、拡張アクセス リスト内の許可ルールに一致するすべての接続に適用されます。ACL ルールは正確に定義し、サービスが必要なトラフィックにのみサービス ポリシー ルールが適用されるようにします。

インターフェイスベースのルールを作成している場合は、割り当てられたデバイスにインターフェイスを設定し、それらのインターフェイスをセキュリティ ゾーンまたはインターフェイス グループに追加する必要もあります。

ステップ 1 [Firepower Threat Defense サービス ポリシー（Firepower Threat Defense Service Policy）] ダイアログボックスがまだ表示されていない場合は、**[ポリシー（Policies）] > [アクセス制御（Access Control）] > [アクセス制御（Access Control）]** を選択してアクセス コントロール ポリシーを編集し、[詳細（Advanced）] タブをクリックして [脅威に対する防御サービス ポリシー（Threat Defense Service Policy）] を編集します。

ステップ 2 次のいずれかを実行します。

- [ルールの追加（Add Rule）] をクリックして、新しいルールを作成します。
- [Edit] アイコン（✎） をクリックして、既存のルールを編集します。

サービス ポリシー ルール ウィザードが開き、ルールの設定プロセスの手順が表示されます。

ステップ 3 [インターフェイス オブジェクト（Interface Object）] 手順で、ポリシーを使用するインターフェイスを定義するオプションを選択します。

- [グローバルに適用（Apply Globally）]：すべてのインターフェイスに適用されるグローバル ルールを作成するには、このオプションを選択します。
- [インターフェイス オブジェクトを選択（Select Interface Objects）]：インターフェイスベースのルールを作成するには、このオプションを選択します。次に、目的のインターフェイスを含むセキュリティ ゾーンまたはインターフェイス オブジェクトを選択し、[>] をクリックして、それらを選択済みリストに移動します。サービス ポリシー ルールは、選択したオブジェクトに含まれる各インターフェイスで設定されますが、ゾーンやグループ自体には設定されません。

インターフェイスの基準が完成したら、[次へ（Next）] をクリックします。

ステップ 4 [トラフィック フロー（Traffic Flow）] 手順で、ルールが適用される接続を定義する拡張 ACL オブジェクトを選択して [次へ（Next）] をクリックします。

ステップ 5 [接続の設定（Connection Setting）] 手順で、このトラフィック クラスに適用するサービスを設定します。

- [TCP 状態バイパスの有効化（Enable TCP State Bypass）]（TCP 接続のみ）：TCP 状態バイパスを実装します。TCP 状態バイパスの対象である接続は、インスペクション エンジンによる検査はされず、すべての TCP 状態のチェックと TCP 正規化をバイパスします。詳細については、非同期ルーティングの TCP ステート チェックのバイパス（TCP ステート バイパス） （1187 ページ）を参照してください。

（注） TCP 状態バイパスは、トラブルシューティングのために、または非対称ルーティングを解決できない場合に使用します。この機能は複数のセキュリティ機能を無効化するため、定義が狭いトラフィック クラスを指定して適切に実装しないと、多数の接続が発生することがあります。

- [TCP シーケンス番号のランダム化（Randomize TCP Sequence Number）]（TCP 接続のみ）：TCP シーケンス番号のランダム化を有効にするか、無効にするかを示します。デフォルトでは、ランダム化が有効になっています。詳細については、TCP シーケンスのランダム化のディセーブル（1191 ページ）を参照してください。
- [デクリメント TTL の有効化（Enable Decrement TTL）]（TCP 接続のみ）：クラスに一致するパケットの存続可能時間（TTL）をデクリメントします。パケット存続時間（TTL）をデクリメントすると、TTL が 1 のパケットはドロップされますが、接続に TTL がより大きいパケットを含むと想定されるセッションでは、接続が開かれます。OSPF hello パケットなどの一部のパケットは TTL = 1 で送信されるため、パケット存続時間（TTL）をデクリメントすると、予期しない結果が発生する可能性があります。

  （注） Firepower Threat Defense デバイスをトレースルートに表示する場合は、デクリメント TTL オプションを設定し、プラットフォームの設定のポリシーに ICMP 到達不能レート制限も設定する必要があります。Firepower Threat Defense デバイスをトレースルートに表示する （1197 ページ）を参照してください。

- [接続（Connections）]：クラス全体で許可される接続の数を制限します。次のオプションを設定可能です。
  - [TCP と UDP の最大数（Maximum TCP and UDP）]（TCP または UDP 接続のみ）：クラス全体で許可される同時接続の最大数（0 ～ 2000000）。TCP の場合、この数は確立された接続にのみ適用されます。デフォルトは 0 で、この場合は接続数が制限されません。制限がクラスに適用されるため、1 つの攻撃ホストがすべての接続を使い果たし、クラスに一致する他のホストが使用できる接続がなくなる可能性があります。この問題を改善するには、クライアントごとの制限を設定します。
  - [最大初期接続数（Maximum Embryonic）]（TCP 接続のみ）：許可される TCP の同時初期接続（TCP ハンドシェイクで完了しない接続）の最大数（0 ~ 2000000）。デフォルトは 0 で、この場合は接続数が制限されません。0 以外の制限を設定することで、TCP 代行受信をイネーブルにします。代行受信によって、TCP SYN パケットを使用してインターフェイスをフラッディングする DoS 攻撃から内部システムを保護します。また、クライアントごとのオプションを設定して、SYN フラッディングから保護します。詳細については、SYN フラッド DoS 攻撃からのサーバの保護（TCP 代行受信） （1193 ページ）を参照してください。
- [クライアントあたりの接続数（Connections Per Client）]：特定のクライアント（送信元 IP アドレス）で許可される接続数の制限。次のオプションを設定可能です。
  - [TCP と UDP の最大数（Maximum TCP and UDP）]（TCP または UDP 接続のみ）：クライアントごとに許可される同時接続の最大数（0 ～ 2000000）。TCP の場合は、確立済み接続、ハーフオープン（初期）接続、ハーフクローズ接続が含まれます。デフォルトは 0 で、この場合は接続数が制限されません。このオプションでは、クラスに一致する各ホストに許可される同時接続の最大数が制限されます。

- [最大初期接続数（Maximum Embryonic）]（TCP 接続のみ）：クライアントごとに許可される TCP の同時初期接続の最大数（0 ～ 2000000）。デフォルトは 0 で、この場合は接続数が制限されません。詳細については、SYN フラッド DoS 攻撃からのサーバの保護（TCP 代行受信）（1193 ページ）を参照してください。

- [接続タイムアウト（Connections Timeout）]：トラフィック クラスに適用されるタイムアウトの設定。これらのタイムアウトで、プラットフォーム設定ポリシーに定義されているグローバル タイムアウトがオーバーライドされます。次の設定を行えます。
  - [初期接続（Embryonic）]（TCP 接続のみ）：TCP 初期（ハーフオープン）接続が閉じられるまでのタイムアウト期間（0:0:5 ～ 1193:00:00）。デフォルト値は 0:0:30 です。
  - [ハーフクローズ（Half Closed）]（TCP 接続のみ）：ハーフクローズ接続が閉じられるまでのアイドル タイムアウト期間（0:0:30 ～ 1193:0:0）。デフォルト値は 0:10:0 です。ハーフクローズ接続は、Dead Connection Detection（DCD; デッド接続検出）の影響を受けません。また、システムは、ハーフクローズ接続の切断時にリセットを送信しません。
  - [アイドル（Idle）]（TCP、UDP、ICMP、IP 接続）：プロトコルの確立された接続が閉じた後のアイドル タイムアウト期間（0:0:1 ～ 1193:0:0）。デフォルトは 1:0:0 です。ただし、デフォルトが 0:2:0 である [TCP 状態バイパス（TCP State Bypass）] オプションを選択している場合を除く。
  - [タイムアウト時に接続をリセット（Reset Connection Upon Timeout）]（TCP 接続のみ）：アイドル接続が削除された後に、両方のエンド システムに TCP RST パケットを送信するかどうかを示します。

- [デッド接続の検出（Detect Dead Connections）]（TCP 接続のみ）：Dead Connection Detection（DCD; デッド接続検出）を有効にするかどうかを示します。アイドル接続の期限が切れる前に、システムはエンド ホストにプローブを送信して接続が有効であるかどうかを判断します。両方のホストが応答した場合は、接続が維持されます。それ以外の場合は、接続が解放されます。トランスペアレント ファイアウォール モードで動作している場合、エンドポイントにスタティック ルートを設定する必要があります。クラスタ内では DCD を使用できません。

  次のオプションを設定します。
  - [検出のタイムアウト（Detection Timeout）]：DCD プローブに応答がない場合に別のプローブを送信するまで待機する時間（hh:mm:ss 形式で、0:0:1 ～ 24:0:0 の範囲で指定）。デフォルト値は 0:0:15 です。

    または高可用性構成で動作しているシステムでは、間隔を 1 分（0:1:0）未満に設定しないことを推奨します。接続をシステム間で移動する必要がある場合、必要な変更には 30 秒以上かかり、変更が行われる前に接続が削除される場合があります。
  - [検出の再試行（Detection Retries）]：接続がデッドであると宣言する前に行われる DCD の再試行の連続失敗回数（1 ～ 255）。デフォルトは 5 です。

ステップ 6 [終了（Finish）] をクリックして変更を保存します。

ルールは適切なリスト（インターフェイスまたはグローバル）の下部に追加されます。グローバル ルールは上から下の順に照合されます。インターフェイス リスト内のルールは、各インターフェイス オブジェク

トで上から下の順に照合されます。定義が狭いトラフィック クラスのルールは、定義が広いルールの上に配置し、適切なサービスが適用されるようにします。各リスト内のルールはドラッグアンドドロップで移動できます。リスト間でルールを移動することはできません。

非同期ルーティングの TCP ステート チェックのバイパス（TCP ステート バイパス）

ネットワークで非同期ルーティング環境を設定し、特定の接続の発信フローと着信フローが 2 つの異なる Firepower Threat Defense デバイスを通過できる場合は、影響を受けるトラフィックに TCP ステート バイパスを実装する必要があります。

ただし、TCPステートバイパスによってネットワークのセキュリティが弱体化するため、非常に詳細に限定されたトラフィック クラスでバイパスを適用する必要があります。

ここでは、問題と解決策についてより詳細に説明します。

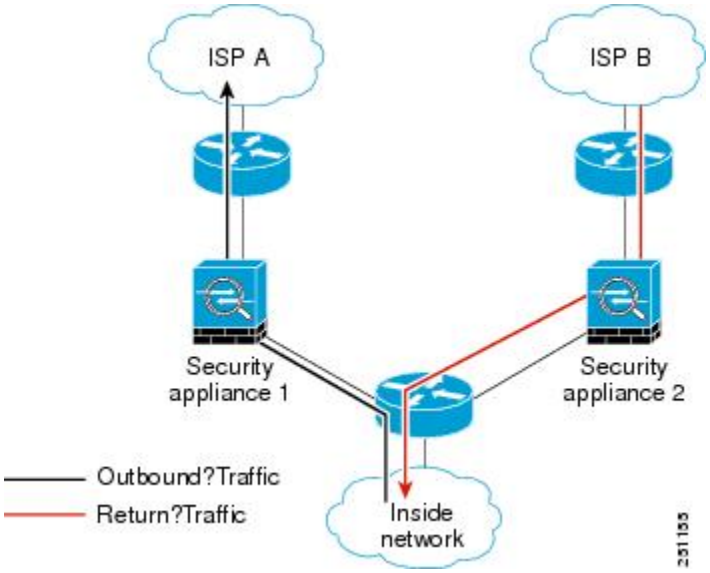
非同期ルーティングの問題

デフォルトで、Firepower Threat Defense デバイスを通過するすべてのトラフィックは、適応型セキュリティ アルゴリズムを使用して検査され、セキュリティ ポリシーに基づいて許可またはドロップされます。Firepower Threat Defense デバイス では、各パケットの状態（新規接続であるか、または確立済み接続であるか）がチェックされ、そのパケットをセッション管理パス（新規接続の SYN パケット）、高速パス（確立済みの接続）、またはコントロール プレーン パス（高度なインスペクション）に割り当てることによって、ファイアウォールのパフォーマンスが最大化されます。

高速パスの既存の接続に一致する TCP パケットは、セキュリティ ポリシーのあらゆる面の再検査を受けることなくFirepower Threat Defense デバイスを通過できます。この機能によってパフォーマンスは最大になります。ただし、SYN パケットを使用してファスト パスにセッションを確立する方法、およびファストパスで行われるチェック（TCP シーケンス番号など）が、非対称ルーティング ソリューションの障害となる場合があります。これは、接続の発信フローと着信フローの両方が同じFirepower Threat Defense デバイスを通過する必要があるためです。

たとえば、ある新しい接続がセキュリティアプライアンス 1 に到達するとします。SYN パケットはセッション管理パスを通過し、接続のエントリが高速パステーブルに追加されます。この接続の後続パケットがセキュリティアプライアンス 1 を通過した場合、高速パス内のエントリに一致するのでこのパケットは送信されます。しかし、後続のパケットがセキュリティアプライアンス 2 に到着すると、SYN パケットがセッション管理パスを通過していないために、高速パスにはその接続のエントリがなく、パケットはドロップされます。次の図は、非対称ルーティングの例を示したもので、アウトバウンド トラフィックはインバウンド トラフィックとは異なる Firepower Threat Defense デバイス を通過しています。

図 *27 :* 非対称ルーティング



アップストリーム ルータに非対称ルーティングが設定されており、トラフィックが 2 つの Firepower Threat Defense デバイスを通過することがある場合は、特定のトラフィックに対して TCP ステート バイパスを設定できます。TCP ステート バイパスは、高速パスでのセッションの確立方法を変更し、高速パスのインスペクションをディセーブルにします。この機能では、UDP 接続の処理と同様の方法で TCP トラフィックが処理されます。指定されたネットワークと一致した非 SYN パケットがFirepower Threat Defense デバイスに入った時点で高速パス エントリが存在しない場合、高速パスで接続を確立するために、そのパケットはセッション管理パスを通過します。いったん高速パスに入ると、トラフィックは高速パスのインスペクションをバイパスします。

TCP ステート バイパスのガイドラインと制限事項

TCP ステート バイパスでサポートされない機能

TCP ステート バイパスを使用するときは、次の機能はサポートされません。

- アプリケーション インスペクション：インスペクションでは、着信トラフィックと発信トラフィックの両方が同じ Firepower Threat Defense デバイス を通過する必要があるため、インスペクションは TCP ステート バイパス トラフィックに適用されません。
- Snort インスペクション：インスペクションでは着信トラフィックと発信トラフィックが同じデバイスを通過する必要があります。ただし、Snort インスペクションは、TCP ステート バイパストラフィックでは自動的にバイパスされません。また、TCP ステート バイパスを設定する同じトラフィック クラスにプレフィルタ fastpath ルールを設定する必要もあります。
- TCP 代行受信、最大初期接続制限、TCP シーケンス番号ランダム化：Firepower Threat Defense デバイスでは接続の状態が追跡されないため、これらの機能は適用されません。

- TCP 正規化：TCP ノーマライザはディセーブルです。
- ステートフル フェールオーバー。

TCP ステート バイパスのガイドライン

変換セッションはFirepower Threat Defenseデバイス ごとに個別に確立されるため、TCP ステート バイパス トラフィック用に両方のデバイスでスタティック NAT を設定する必要があります。ダイナミック NAT を使用すると、デバイス 1 でのセッションに選択されるアドレスは、デバイス 2 でのセッションに選択されるアドレスとは異なります。

TCP ステート バイパスの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin Access Admin Network Admin

非同期ルーティング環境で TCP ステート チェックをバイパスするには、影響を受けるホストまたはネットワークにのみに適用するトラフィック クラスを注意深く定義してから、サービス ポリシーを使用してトラフィック クラスで TCP ステート バイパスをイネーブルにします。また、同じトラフィックに対応するプレフィルタ fastpath ポリシーを設定してトラフィックもインスペクションをバイパスさせる必要もあります。

バイパスによってネットワークのセキュリティが低下するため、そのアプリケーションをできるだけ制限します。

ステップ 1 トラフィック クラスを定義する拡張 ACL を作成します。

たとえば、10.1.1.1 to 10.2.2.2 からの TCP トラフィックのトラフィック クラスを定義するには、次の手順を実行します。

a) **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** を選択します。
b) 目次から **[アクセス リスト（Access List）]** > **[拡張（Extended）]** を選択します。
c) [拡張アクセス リストを追加（Add Extended Access List）] ボタンをクリックします。
d) オブジェクトの [名前（Name）]（bypass など）を入力します。
e) [追加（Add）] をクリックしてルールを追加します。
f) アクションは [許可（Allow）] のままにします。
g) [送信元（Source）] リストの下に 10.1.1.1 と入力して [追加（Add）] をクリックし、[宛先（Destination）] リストの下に 10.2.2.2 と入力して [追加（Add）] をクリックします。
h) [ポート（Port）] タブをクリックし、[選択済みの送信元ポート（Selected Source Ports）] リストの下で [TCP (6)] を選択して [追加（Add）] をクリックします。ポート番号は入力せず、すべてのポートをカバーするプロトコルとして TCP を単純に追加します。
i) [拡張アクセス リスト エントリ（Extended Access List Entry）] ダイアログボックスで [追加（Add）] をクリックして、ルールを ACL に追加します。

j) [拡張アクセス リスト オブジェクト（Extended Access List Object）] ダイアログボックスで [保存（Save）] をクリックして、ACL オブジェクトを保存します。

ステップ 2 TCP ステート バイパスのサービス ポリシー ルールを設定します。

たとえば、このトラフィック クラスの TCP ステート バイパスをグローバルに設定するには、次の手順を実行します。

a) **[ポリシー（Policies）] > [アクセス制御（Access Control）] > [アクセス制御（Access Control）]** を選択して、このサービスを必要とするデバイスに割り当てられているポリシーを編集します。
b) [詳細（Advanced）] タブをクリックして、[脅威に対する防御サービス ポリシー（Threat Defense Service Policy）] の [Edit] アイコン（） をクリックします。
c) [ルールの追加（Add Rule）] をクリックします。
d) [グローバルに適用（Apply Globally）] を選択して、[次へ（Next）] をクリックします。
e) このルールに対して作成した拡張 ACL オブジェクトを選択して、[次へ（Next）] をクリックします。
f) [TCP ステート バイパスの有効化（Enable TCP State Bypass）] を選択します。
g) （オプション）バイパスされる接続の [アイドル（Idle）] タイムアウトを調整します。デフォルトは 2 分です。
h) [終了（Finish）] をクリックしてルールを追加します。必要に応じて、ルールをサービス ポリシー内の必要な位置にドラッグアンドドロップします。
i) [OK] をクリックして、サービス ポリシーに加えた変更を保存します。
j) [詳細（Advanced）] タブで [保存（Save）] をクリックして、アクセス コントロール ポリシーに加えた変更を保存します。

ステップ 3 トラフィック クラスのプレフィルタ fastpath のルールを設定します。

プレフィルタ ルール内に ACL オブジェクトを使用できません。そのため、プレフィルタ ルールに直接か、またはクラスを定義するネットワーク オブジェクトを最初に作成するかのいずれかでトラフィック クラスを再度作成する必要があります。

次の手順では、アクセス コントロール ポリシーに接続されているプレフィルタ ポリシーがすでにあることを前提としています。プレフィルタ ポリシーをまだ作成していない場合は、**[ポリシー（Policies）] > [アクセス制御（Access Control）] > [プレフィルタ（Prefilter）]** に移動し、最初にポリシーを作成します。アクセス コントロール ポリシーに接続し、ルールを作成するには、この手順を使用できます。

この手順は 10.1.1.1 から 10.2.2.2 への TCP トラフィックの fastpath ルールを作成する例に沿っています。

a) **[ポリシー（Policies）] > [アクセス制御（Access Control）] > [アクセス制御（Access Control）]** を選択して、TCP バイパス サービス ポリシー ルールを持つポリシーを編集します。
b) ポリシーの説明のすぐ下の左側にある [プレフィルタ ポリシー（Prefilter Policy）] のリンクをクリックします。
c) [プレフィルタ ポリシー（Prefilter Policy）] ダイアログボックスで、適切なポリシーがまだ選択されていないデバイスに割り当てるポリシーを選択します。この時点ではまだ [OK] をクリックしないでください。

デフォルトのプレフィルタ ポリシーにはルールを追加できないため、カスタム ポリシーを選択する必要があります。

d) [プレフィルタ ポリシー（Prefilter Policy）] ダイアログボックスで、[Edit] アイコン（） をクリックします。このアクションによって、ポリシーの編集が可能な新しいブラウザ ウィンドウまたはタブが開きます。

e) [プレフィルタ ルールの追加（Add Prefilter Rule）] をクリックし、次のプロパティを使用してルールを設定します。

- [名前（Name）]：自分にとってわかりやすい名前（TCPBypass など）。
- [アクション（Action）]：[Fastpath] を選択します。
- [インターフェイス オブジェクト（Interface Objects）] タブ：TCP ステート バイパスをグローバル ルールとして設定した場合は送信元も宛先もデフォルトの [任意（any）] のままにします。インターフェイスベースのルールを作成した場合は、[送信元インターフェイス オブジェクト（Source Interface Objects）] リストのルールに使用したものと同じインターフェイス オブジェクトを選択し、宛先は [任意（any）] のままにします。
- [ネットワーク（Networks）] タブ：[送信元ネットワーク（Source Networks）] リストに 10.1.1.1 を、[宛先ネットワーク（Destination Networks）] リストに 10.2.2.2 を追加します。ネットワーク オブジェクトを使用するか、またはアドレスを手動で追加することができます。
- [ポート（Ports）] タブ： [選択済み送信元ポート（Selected Source Ports）] で、TCP(6) を選択し、**ポートを入力せずに** [追加（Add）] をクリックします。こうすることで、TCP ポート番号に関係なく、すべての（および唯一の）TCP トラフィックにルールが適用されます。

f) [追加（Add）] をクリックしてプレフィルタ ポリシーにルールを追加します。

g) [保存（Save）] をクリックしてプレフィルタ ポリシーに変更を保存します。

これで、プレフィルタ編集ウィンドウを閉じてアクセス コントロール ポリシーの編集ウィンドウに戻ることができます。

h) アクセス コントロール ポリシーの編集ウィンドウには [プレフィルタ ポリシー（Prefilter Policy）] ダイアログボックスが開かれたままになっています。[OK] をクリックしてプレフィルタ ポリシーの割り当てに変更を保存します。

i) プレフィルタ ポリシーの割り当てを変更した場合は、アクセス コントロール ポリシーで [保存（Save）] をクリックしてその変更を保存します。

これで、影響を受けるデバイスに変更を展開できます。

TCP シーケンスのランダム化のディセーブル

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin Access Admin Network Admin

各 TCP 接続には 2 つの初期シーケンス番号（ISN）が割り当てられており、1 つはクライアントで生成され、もう 1 つはサーバで生成されます。Firepower Threat Defense デバイスは、着信と発信の両方向で通過する TCP SYN の ISN をランダム化します。

保護対象のホストの ISN をランダム化することにより、攻撃者が新しい接続に使用される次の ISN を予測して新しいセッションをハイジャックするのを阻止します。

たとえば、データがスクランブルされるため、必要に応じて TCP 初期シーケンス番号ランダム化をディセーブルにすることができます。次に、ランダム化を無効にする状況をいくつか示します。

- 別の直列接続されたファイアウォールでも初期シーケンス番号がランダム化され、トラフィックに影響することはないものの、両方のファイアウォールでこの動作を実行する必要がない場合。
- デバイスで eBGP マルチホップを使用していて、eBGP ピアで MD5 を使用している場合。ランダム化により、MD5 チェックサムは分解されます。
- Firepower Threat Defense デバイスによる接続のシーケンス番号のランダム化が不要な WAAS デバイスを使用する場合。
- ISA 3000 のハードウェア バイパスを有効にしている場合、ISA 3000 がデータ パスの一部でなくなると、TCP 接続はドロップされます。

ステップ 1 トラフィック クラスを定義する拡張 ACL を作成します。

たとえば、任意のホストから 10.2.2.2 に送信される TCP トラフィックのトラフィック クラスを定義するには、次の手順を実行します。

a) **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** を選択します。
b) 目次から **[アクセス リスト（Access List）]** > **[拡張（Extended）]** を選択します。
c) [拡張アクセス リストを追加（Add Extended Access List）] ボタンをクリックします。
d) オブジェクトの [名前（Name）]（preserve-sq-no など）を入力します。
e) [追加（Add）] をクリックしてルールを追加します。
f) アクションは [許可（Allow）] のままにします。
g) [送信元（Source）] リストを空白のままにして、[宛先（Destination）] リストの下に 10.2.2.2 と入力して、[追加（Add）] をクリックします。
h) [ポート（Port）] タブをクリックし、[選択済みの送信元ポート（Selected Source Ports）] リストの下で [TCP (6)] を選択して [追加（Add）] をクリックします。ポート番号は入力せず、すべてのポートをカバーするプロトコルとして TCP を単純に追加します。
i) [拡張アクセス リスト エントリ（Extended Access List Entry）] ダイアログボックスで [追加（Add）] をクリックして、ルールを ACL に追加します。
j) [拡張アクセス リスト オブジェクト（Extended Access List Object）] ダイアログボックスで [保存（Save）] をクリックして、ACL オブジェクトを保存します。

ステップ 2 TCP シーケンス番号のランダム化を無効にするサービス ポリシー ルールを設定します。

たとえば、このトラフィック クラスのランダム化をグローバルに無効にするには、次の手順を実行します。

a) **[ポリシー（Policies）] > [アクセス制御（Access Control）] > [アクセス制御（Access Control）]** を選択して、このサービスを必要とするデバイスに割り当てられているポリシーを編集します。
b) [詳細（Advanced）] タブをクリックして、[脅威に対する防御サービス ポリシー（Threat Defense Service Policy）] の [Edit] アイコン（✎） をクリックします。
c) [ルールの追加（Add Rule）] をクリックします。
d) [グローバルに適用（Apply Globally）] を選択して、[次へ（Next）] をクリックします。
e) このルールに対して作成した拡張 ACL オブジェクトを選択して、[次へ（Next）] をクリックします。
f) [TCP シーケンス番号のランダム化（Randomize TCP Sequence Number）] の選択を解除します。
g) （オプション）その他の接続オプションを必要に応じて調節します。
h) [終了（Finish）] をクリックしてルールを追加します。必要に応じて、ルールをサービス ポリシー内の必要な位置にドラッグアンドドロップします。
i) [OK] をクリックして、サービス ポリシーに加えた変更を保存します。
j) [詳細（Advanced）] タブで [保存（Save）] をクリックして、アクセス コントロール ポリシーに加えた変更を保存します。

これで、影響を受けるデバイスに変更を展開できます。

サービス ポリシーのルールの例

次のトピックにサービス ポリシー ルールの例を示します。

SYN フラッド DoS 攻撃からのサーバの保護（TCP 代行受信）

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin Access Admin Network Admin

攻撃者が一連の SYN パケットをホストに送信すると、SYN フラッディング サービス妨害（DoS）攻撃が発生します。これらのパケットは通常、スプーフィングされた IP アドレスから発信されます。SYN パケットのフラッディングが定常的に生じると、SYN キューが一杯になる状況が続き、正規ユーザからの接続要求に対してサービスを提供できなくなります。

SYN フラッディング攻撃を防ぐために初期接続数を制限できます。初期接続とは、送信元と宛先の間で必要になるハンドシェイクを完了していない接続要求のことです。

接続の初期接続しきい値を超えると、Firepower Threat Defense デバイスはサーバのプロキシとして動作し、SYN Cookie 方式を使用してクライアント SYN 要求に対する SYN-ACK 応答を生成します（SYN Cookie の詳細については、Wikipedia を参照してください）。Firepower Threat

Defenseデバイスはクライアントから ACK を受信すると、クライアントが本物であることを認証し、サーバへの接続を許可できます。プロキシを実行するコンポーネントは、TCP代行受信と呼ばれます。

接続制限を設定すると、サーバを SYN フラッド攻撃から保護できます。必要に応じて、TCP代行受信の統計情報を有効にして、ポリシーの結果をモニタできます。次の手順では、エンドツーエンドのプロセスについて説明します。

始める前に

- 保護するサーバの TCP SYN バックログ キューより低い初期接続制限を設定していることを確認します。これより高い初期接続制限を設定すると、有効なクライアントが、SYN攻撃中にサーバにアクセスできなくなります。初期接続制限に適切な値を決定するには、サーバの容量、ネットワーク、サーバの使用状況を入念に分析してください。
- Firepower Threat Defense デバイス上の CPU コア数によっては、各コアによる接続の管理方法が原因で、同時接続および初期接続の最大数が設定されている数を超える場合があります。最悪の場合、デバイスは最大 n-1 の追加接続および初期接続を許可します。ここで、n はコアの数です。たとえば、モデルに 4 つのコアがあり、6 つの同時接続および 4 つの初期接続を設定した場合は、各タイプで 3 つの追加接続を使用できます。モデルのコア数を確認するには、デバイスの CLI で **show cpu core** コマンドを入力します。

ステップ 1 保護するサーバのリストであるトラフィック クラスを定義する拡張 ACL を作成します。

たとえば、IP アドレスが 10.1.1.5 と 10.1.1.6 の Web サーバを保護するためのトラフィック クラスを定義します。

a) **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** を選択します。
b) 目次から **[アクセス リスト（Access List）]** > **[拡張（Extended）]** を選択します。
c) [拡張アクセス リストを追加（Add Extended Access List）] ボタンをクリックします。
d) オブジェクトの [名前（Name）]（protected-servers など）を入力します。
e) [追加（Add）] をクリックしてルールを追加します。
f) アクションは [許可（Allow）] のままにします。
g) [送信元（Source）] リストを空白のままにして、[宛先（Destination）] リストの下に 10.1.1.5 と入力して、[追加（Add）] をクリックします。
h) また、[宛先（Destination）] リストの下に 10.1.1.6 と入力して、[追加（Add）] をクリックします。
i) [ポート（Port）] タブをクリックし、利用可能なポートのリストで [HTTP] を選択して、[宛先に追加（Add to Destination）] をクリックします。サーバで HTTPS 接続もサポートされている場合は、HTTPS ポートも追加します。
j) [拡張アクセス リスト エントリ（Extended Access List Entry）] ダイアログボックスで [追加（Add）] をクリックして、ルールを ACL に追加します。
k) [拡張アクセス リスト オブジェクト（Extended Access List Object）] ダイアログボックスで [保存（Save）] をクリックして、ACL オブジェクトを保存します。

ステップ 2 初期接続制限を設定するサービス ポリシールールを設定します。

たとえば、同時初期接続の合計を 1000 接続に設定し、クライアントごとの制限を 50 接続に設定する場合は、次の手順を実行します。

a) **[ポリシー（Policies）] > [アクセス制御（Access Control）] > [アクセス制御（Access Control）]** を選択して、このサービスを必要とするデバイスに割り当てられているポリシーを編集します。
b) [詳細（Advanced）] タブをクリックして、[脅威に対する防御サービス ポリシー（Threat Defense Service Policy）] の [Edit] アイコン（✎） をクリックします。
c) [ルールの追加（Add Rule）] をクリックします。
d) [グローバルに適用（Apply Globally）] を選択して、[次へ（Next）] をクリックします。
e) このルールに対して作成した拡張 ACL オブジェクトを選択して、[次へ（Next）] をクリックします。
f) **[接続（Connections）] > [最大初期接続数（Maximum Embryonic）]** に 1000 を入力します。
g) **[クライアントあたりの接続数（Connections Per Client）] > [最大初期接続数（Maximum Embryonic）]** に 50 を入力します。
h) （オプション）その他の接続オプションを必要に応じて調節します。
i) [終了（Finish）] をクリックしてルールを追加します。必要に応じて、ルールをサービス ポリシー内の必要な位置にドラッグアンドドロップします。
j) [OK] をクリックして、サービス ポリシーに加えた変更を保存します。
k) [詳細（Advanced）] タブで [保存（Save）] をクリックして、アクセス コントロール ポリシーに加えた変更を保存します。

ステップ 3 （オプション）TCP 代行受信の統計情報のレートを設定します。

TCP 代行受信では次のオプションを使用して、統計情報の収集レートが決定されます。すべてのオプションにはデフォルト値があります。それらのレートがニーズに合っている場合は、この手順を省略できます。

- [レート間隔（Rate Interval）]：履歴監視ウィンドウのサイズ（1 ～ 1440 分）。デフォルトは 30 分です。この間隔の間に、システムは攻撃の数を 30 回サンプリングします。
- [バースト レート（Burst Rate）]：Syslog メッセージ生成のしきい値（25 ～ 2147483647）。デフォルトは 1 秒間に 400 です。バースト レートを超えると、デバイスは Syslog メッセージ 733104 を生成します。
- [平均レート（Average Rate）]：Syslog メッセージ生成の平均レートのしきい値（25 ～ 2147483647）。デフォルトは 1 秒間に 200 回です。平均レートを超えると、デバイスは Syslog メッセージ 733105 を生成します。

これらのオプションを調整する場合は、次の手順を実行します。

a) **[オブジェクト（Objects）] > [オブジェクト管理（Object Management）]** を選択します。
b) **[FlexConfig] > [テキスト オブジェクト（Text Object）]** を選択します。
c) システム定義オブジェクト threat_defense_statistics の [Edit] アイコン（✎） をクリックします。
d) 値は直接変更できますが、[オーバーライド（Override）] セクションを開き、[追加（Add）] をクリックして、デバイス オーバーライドを作成することを推奨します。
e) （アクセス コントロール ポリシーの割り当てを介して）サービス ポリシーを割り当てるデバイスを選択し、[追加（Add）] をクリックして、選択済みリストにデバイスを移動します。
f) [オーバーライド（Override）] タブをクリックします。

g) オブジェクトには 3 つのエントリが必要なため、3 になるまで必要に応じて [カウント（Count）] ボタンをクリックします。
h) レート間隔、バースト レート、および平均レートとして 1 ～ 3 の順序で必要な値を入力します。オブジェクトの説明を参照し、正しい順序で値を入力していることを確認してください。
i) [オブジェクトのオーバーライド（Object Override）] ダイアログボックスで [追加（Add）] をクリックします。
j) [テキスト オブジェクトの編集（Edit Text Object）] ダイアログボックスで [保存（Save）] をクリックします。

ステップ 4 TCP 代行受信の統計情報を有効にします。

TCP 代行受信の統計情報を有効にするには FlexConfig ポリシーを設定する必要があります。

a) **[デバイス（Devices）] > [FlexConfig]** を選択します。
b) ポリシーをすでにデバイスに割り当てている場合は、そのポリシーを編集します。割り当てていない場合は、新しいポリシーを作成して、影響を受けるデバイスに割り当てます。
c) [利用可能な FlexConfig（Available FlexConfig）] リストで [Threat_Detection_Configure] を選択して [>>] をクリックします。オブジェクトが [選択済み追加 FlexConfig（Selected Append FlexConfigs）] リストに追加されます。
d) [保存（Save）] をクリックします。
e) （オプション）[プレビュー設定（Preview Config）] をクリックし、いずれかのデバイスを選択することで、設定が正しいことを確認できます。

次の展開時にデバイスに書き込まれる CLI コマンドが生成されます。それらのコマンドには、サービス ポリシーおよび脅威検出の統計情報に必要なコマンドが含まれます。プレビューの下にスクロールして、追加された CLI を確認します。デフォルト値を使用している場合、TCP 代行受信の統計情報のコマンドは、次のようになります（わかりやすくするために改行されています）。

```
###Flex-config Appended CLI ###

threat-detection statistics tcp-intercept rate-interval 30
       burst-rate 400 average-rate 200
```

ステップ 5 これで、影響を受けるデバイスに変更を展開できます。

ステップ 6 次のコマンドを使用して、デバイスの CLI から TCP 代行受信の統計情報をモニタします。

- **show threat-detection statistics top tcp-intercept** [**all** | **detail**]：攻撃を受けて保護された上位 10 のサーバを表示します。**all** キーワードは、トレースされているすべてのサーバの履歴データを表示します。**detail** キーワードは、履歴サンプリング データを表示します。システムはレート間隔の間に攻撃の数を 30 回サンプリングするため、デフォルトの 30 分間隔の場合、60 秒ごとに統計情報が収集されます。

  （注） **shun** コマンドを使用して、ホスト IP アドレスへの攻撃をブロックできます。ブロックを削除するには、**no shun** コマンドを使用します。

- **clear threat-detection statistics tcp-intercept**TCP 代行受信の統計情報を削除します。

例：

```
hostname(config)# show threat-detection statistics top tcp-intercept
Top 10 protected servers under attack (sorted by average rate)
Monitoring window size: 30 mins    Sampling interval: 30 secs
<Rank> <Server IP:Port> <Interface> <Ave Rate> <Cur Rate> <Total> <Source IP (Last Attack Time)>
------------------------------------------------------------------------------
1    10.1.1.5:80 inside 1249 9503 2249245 <various> Last: 10.0.0.3 (0 secs ago)
2    10.1.1.6:80 inside 10 10 6080 10.0.0.200 (0 secs ago)
```

Firepower Threat Defense デバイスをトレースルートに表示する

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin Access Admin Network Admin

デフォルトでは、Firepower Threat Defense デバイスは、トレースルートにホップとして表示されません。表示されるようにするには、デバイスを通過するパケットの存続可能時間を減らし、ICMP 到達不能メッセージのレート制限を増やす必要があります。これを行うには、サービスポリシールールを設定し、ICMPプラットフォーム設定ポリシーを調整する必要があります。

（注） パケット存続時間（TTL）をデクリメントすると、TTL が 1 のパケットはドロップされますが、接続に TTL がより大きいパケットを含むと想定されるセッションでは、接続が開かれます。OSPF hello パケットなどの一部のパケットは TTL = 1 で送信されるため、パケット存続時間（TTL）をデクリメントすると、予期しない結果が発生する可能性があります。トラフィック クラスを定義する際には、これらの考慮事項に注意してください。

ステップ 1 Traceroute レポートを有効にするトラフィック クラスを定義する拡張 ACL を作成します。

たとえば、OSPF トラフィックを除く、すべてのアドレスのトラフィック クラスを定義するには、次の手順を実行します。

a) **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** を選択します。
b) 目次から **[アクセス リスト（Access List）]** > **[拡張（Extended）]** を選択します。
c) [拡張アクセス リストを追加（Add Extended Access List）] ボタンをクリックします。
d) オブジェクトの [名前（Name）]（traceroute-enabled など）を入力します。
e) [追加（Add）] をクリックして、OSPF を除外するルールを追加します。
f) アクションを [ブロック（Block）] に変更し、[ポート（Port）] タブをクリックします。[宛先ポート（Destination Ports）] リストの下でプロトコルとして [OSPFIGP (89)] を選択し、[追加（Add）] をクリックして、プロトコルを選択済みリストに追加します。

g) [拡張アクセス リスト エントリ（Extended Access List Entry）] ダイアログボックスで [追加（Add）] をクリックして、OSPF ルールを ACL に追加します。
h) [追加（Add）] をクリックして、その他すべての接続を含めるルールを追加します。
i) アクションは [許可（Allow）] のままにして、[送信元（Source）] と [宛先（Destination）] リストの両方を空にします。
j) [拡張アクセス リスト エントリ（Extended Access List Entry）] ダイアログボックスで [追加（Add）] をクリックして、ルールを ACL に追加します。

OSPF 拒否ルールが [すべて許可（Allow Any）] ルールの上にあることを確認します。必要に応じて、ルールをドラッグアンドドロップして移動します。

k) [拡張アクセス リスト オブジェクト（Extended Access List Object）] ダイアログボックスで [保存（Save）] をクリックして、ACL オブジェクトを保存します。

ステップ 2 存続可能時間の値をデクリメントするサービス ポリシールールを設定します。

たとえば、存続可能時間をグローバルにデクリメントするには、次の手順を実行します。

a) **[ポリシー（Policies）] > [アクセス制御（Access Control）] > [アクセス制御（Access Control）]** を選択して、このサービスを必要とするデバイスに割り当てられているポリシーを編集します。
b) [詳細（Advanced）] タブをクリックして、[脅威に対する防御サービス ポリシー（Threat Defense Service Policy）] の [Edit] アイコン（✎） をクリックします。
c) [ルールの追加（Add Rule）] をクリックします。
d) [グローバルに適用（Apply Globally）] を選択して、[次へ（Next）] をクリックします。
e) このルールに対して作成した拡張 ACL オブジェクトを選択して、[次へ（Next）] をクリックします。
f) [デクリメント TTL の有効化（Enable Decrement TTL）] を選択します。
g) （オプション）その他の接続オプションを必要に応じて調節します。
h) [終了（Finish）] をクリックしてルールを追加します。必要に応じて、ルールをサービス ポリシー内の必要な位置にドラッグアンドドロップします。
i) [OK] をクリックして、サービス ポリシーに加えた変更を保存します。
j) [詳細（Advanced）] タブで [保存（Save）] をクリックして、アクセス コントロール ポリシーに加えた変更を保存します。

これで、影響を受けるデバイスに変更を展開できます。

ステップ 3 ICMP 到達不能メッセージのレート制限を増やします。

a) **[デバイス（Devices）] > [プラットフォーム設定（Platform Settings）]** を選択します。
b) ポリシーをすでにデバイスに割り当てている場合は、そのポリシーを編集します。割り当てていない場合は、新しい Firepower Threat Defense プラットフォーム設定ポリシーを作成して、影響を受けるデバイスに割り当てます。
c) 目次から [ICMP] を選択します。
d) [レート制限（Rate Limit）] を（50 などに）増やします。[バースト サイズ（Burst Size）] は使用されないため、無視できます。

ICMP ルール テーブルは、このタスクには無関係なので、空のままにすることができます。

e) [保存（Save）] をクリックします。

ステップ 4 これで、影響を受けるデバイスに変更を展開できます。

サービス ポリシーのモニタリング

デバイスのCLIを使用してサービスポリシー関連の情報をモニタできます。次に、便利なコマンドをいくつか示します。

- **show conn** [**detail**]

  接続情報を表示します。詳細情報は、フラグを使用して特別な接続の特性を示します。たとえば、「b」フラグは、TCPステート バイパスの対象であるトラフィックを示します。

- **show service-policy**

  Dead Connection Detection（DCD; デッド接続検出）の統計情報を含むサービス ポリシーの統計情報を表示します。

- **show threat-detection statistics top tcp-intercept** [**all** | **detail**]

  攻撃を受けて保護された上位 10 サーバを表示します。**all** キーワードは、トレースされているすべてのサーバの履歴データを表示します。**detail** キーワードは、履歴サンプリングデータを表示します。システムはレート間隔の間に攻撃の数を 30 回サンプリングするため、デフォルトの 30 分間隔の場合、60 秒ごとに統計情報が収集されます。

Firepower Threat Defense のサービス ポリシーの履歴

機能	バージョン	説明
Firepower Threat Defense のサービス ポリシー。	6.3	Firepower Threat Defense をアクセス コントロール ポリシーの高度なオプションの一部として設定できるようになりました。Firepower Threat Defense サービス ポリシーを使用して、特定のトラフィック クラスにサービスを適用することができます。サポートされている機能には、TCP ステート バイパス、TCP シーケンス番号のランダム化、パケットでの存続可能時間（TTL）の値の減分、デッド接続検出、トラフィック クラスごとおよびクライアントごとの接続および初期接続の最大数の制限の設定、初期接続、ハーフクローズ接続、およびアイドル接続のタイムアウトなどがあります。 新規画面：**[ポリシー（Policies）] > [アクセス制御（Access Control）] > [アクセス制御（Access Control）]**、[詳細（Advanced）] タブ、[Threat Defense サービス ポリシー（Threat Defense Service Policy）]。 サポートされているプラットフォーム：Firepower Threat Defense

第 48 章

Firepower Threat Defense の FlexConfig ポリシー

次のトピックでは、FlexConfig ポリシーを設定して導入する方法について説明します。

FlexConfig ポリシーの概要

FlexConfig ポリシーは FlexConfig オブジェクトの番号付きリストのコンテナです。各オブジェクトは、定義する一連の Apache Velocity のスクリプト言語コマンド、ASA ソフトウェアの設定コマンド、および変数に影響を与えます。各 FlexConfig オブジェクトの内容は、基本的に、割り当てられたデバイスに展開する一連の ASA コマンドを生成するプログラムです。このコマンド シーケンスは、その後、FTD デバイスで関連機能を設定します。

FTD では、ASA 設定コマンドを使用して、すべての機能ではなく一部の機能を実装します。FTD 設定コマンドの一意のセットはありません。代わりに、FlexConfig のポイントは、Firepower Management Center ポリシーおよび設定を介して直接まだサポートされていない機能を設定できることです。

注意 シスコでは、ASA に精通している上級ユーザが自身の責任で行う場合にのみ FlexConfig ポリシーを使用することを**強く**お勧めします。ブラックリストに登録されていない任意のコマンドを設定できます。FlexConfig ポリシーによって機能を有効にすると、他の設定された機能により意図しない結果を引き起こす可能性があります。

設定した FlexConfig ポリシーに関するサポートについては、Cisco Technical Assistance Center にお問い合わせください。Cisco Technical Assistance Center は、顧客に代わってカスタム設定を設計したり、作成したりしません。シスコは、その他の Firepower システムの機能との正しい動作または相互運用性を保証しません。FlexConfig 機能は廃止になる可能性があります。完全に保証された機能のサポートについては、Firepower Management Center サポートを待つ必要があります。判別できない場合は、FlexConfig ポリシーを使用しないでください。

FlexConfig ポリシーの推奨される使用法

FlexConfig ポリシーには、推奨される使用法が主に 2 つあります。

- ASA から FTD に変換し、Firepower Management Center で直接サポートされない互換機能を使用している（および引き続き使用する必要がある）場合。この場合、ASA で **show running-config** コマンドを使用してその互換機能の設定を確認し、その機能を実装する FlexConfig オブジェクトを作成します。オブジェクトの導入設定（1 回/毎回、前に付加/後ろに付加）をいろいろと試して、正しい設定になるようにします。2 台のデバイスでの **show running-config** の出力を比較して確認します。
- FTD を使用しているものの、構成が必要な設定または機能がある場合（たとえば、Cisco Technical Assistance Center から、発生している特定の問題を解決するための具体的な設定を指示された場合）。複雑な機能については、ラボ デバイスを使用して FlexConfig をテストし、期待する動作を得られることを確認します。

システムには、テスト対象の設定を表す一連の定義済み FlexConfig オブジェクトが含まれています。これらのオブジェクトのなかに必要な機能を表すものがない場合は、まず、標準ポリシーで同等の機能を設定できるかどうかを判断します。たとえば、アクセス コントロール ポリシーには侵入検知および防御、HTTP およびその他のタイプのプロトコル インスペクション、URL フィルタリング、アプリケーション フィルタリング、アクセス制御が含まれており、ASA はこれらの要素を別個の機能を使用して実装します。多くの機能は CLI コマンドを使用して設定されていないため、**show running-config** の出力内にすべてのポリシーが表示されるわけではありません。

（注） 常に、ASA と FTD との間の重複は 1 対 1 であるわけではないことに注意してください。FTD デバイスで ASA 設定を完全に作成し直そうとしないでください。設定する機能は、FlexConfig を使用して慎重にテストする必要があります。

FlexConfig オブジェクトの CLI コマンド

FTD では一部の機能の設定に ASA コンフィギュレーション コマンドを使用します。ASA のすべての機能に FTD との互換性があるわけではありませんが、FTD で使用はできるが Firepower Management Center ポリシーでは設定できない機能があります。こうした機能を設定するには、FlexConfig オブジェクトを使って必要な CLI を指定します。

FlexConfig を使って手動で機能を設定する場合、ユーザは自身の責任において正しいコマンド シンタックスを理解し、実装してください。FlexConfig ポリシーは CLI コマンド シンタックスの検証は行いません。正しいシンタックスと CLI コマンドの設定に関する詳細については、ASA ドキュメンテーションを参照してください。

- 『ASA CLI configuration guides』では機能を設定する方法について説明しています。ガイドは http://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/products-installation-and-configuration-guides-list.html にあります。
- 『ASA コマンド リファレンス』ではコマンド名ごとにその他の情報が記載されています。参考資料は http://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/products-command-reference-list.html にあります。

ここでは、コンフィギュレーション コマンドについて詳しく説明します。

ASA ソフトウェアのバージョンおよび現在の CLI 設定の特定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	Firepower Threat Defense Firepower Threat Defense Virtual	いずれか（Any）	Admin

システムが ASA ソフトウェア コマンドを使用して一部の機能を設定するため、FTD デバイスで実行するソフトウェアで使用されている現在の ASA バージョンを特定する必要があります。このバージョン番号に従って、機能設定時の手順に使用する ASA CLI 設定ガイドを選択します。また、現在の CLI ベースの設定を確認し、実装する ASA 設定と比較する必要があります。

FTD 設定とどの ASA 設定も大きく異なることに注意してください。FTD ポリシーの多くは CLI の外部で設定されるため、コマンドを調べても設定を確認することができません。ASA と FTD 設定が 1 対 1 で対応するように作成しようとしないでください。

この情報を表示するには、デバイスの管理インターフェイスへの SSH 接続を確立し、次のコマンドを発行します。

- **show version system** また、Cisco 適応型セキュリティ アプライアンス ソフトウェアのバージョン番号を検索します。（Firepower Management Center CLI ツールを使用してコマンドを発行する場合は、**system** キーワードを省略します。）

- **show running-config** 現在の CLI 設定を表示します。
- **show running-config all** 現在の CLI 設定にすべてのデフォルト コマンドを含めます。

また、次の手順を使用して、Firepower Management Center 内からこれらのコマンドを発行することもできます。

ステップ 1 **[システム（System）] > [ヘルス（Health）] > [モニタ（Monitor）]** を選択します。

ステップ 2 FlexConfig ポリシーの対象となるデバイスの名前をクリックします。

目的のデバイスを表示するために、[ステータス（Status）] テーブルの [カウント（Count）] カラムにある開く/閉じるの矢印をクリックする必要がある場合があります。

ステップ 3 [高度なトラブルシューティング（Advanced Troubleshooting）] を選択します。

ステップ 4 [脅威に対する防御 CLI（Threat Defense CLI）] を選択します。

ステップ 5 コマンドとして **show** を選択し、パラメータとして **version** を入力するか、他のコマンドの 1 つを入力します。

ステップ 6 [実行（Execute）] をクリックします。

version を入力した場合、Cisco 適応型セキュリティ アプライアンス ソフトウェアのバージョン番号の出力を検索します。

後で実行する分析のために、出力を選択して Ctrl + C を押し、テキスト ファイルに貼り付けることができます。

禁止された CLI コマンド

FlexConfig の目的は、Firepower Management Center を使用している FTD デバイスで設定できない ASA デバイスで使用可能な機能を設定することです。

したがって、Firepower Management Center に同等の機能がある ASA 機能は設定することができません。次の表に、これらの禁止されたコマンド領域のいくつかを示します。

また、一部の **clear** コマンドは管理対象ポリシーと重複しており、管理対象ポリシーの設定の一部を削除する可能性があるため禁止されています。

FlexConfig オブジェクト エディタでは、禁止されたコマンドをオブジェクトに含めることはできません。

禁止された CLI コマンド	説明
AAA	設定がブロックされます。
AAA-Server	設定がブロックされます。

禁止された CLI コマンド	説明
Access-list	高度 ACL、拡張 ACL、および標準 ACL がブロックされます。Ethertype ACL は許可されます。 テンプレート内のオブジェクト マネージャで定義されている標準および拡張 ACL オブジェクトを変数として使用することができます。
ARP Inspection	設定がブロックされます。
As-path Object	設定がブロックされます。
Banner	設定がブロックされます。
BGP	設定がブロックされます。
Clock	設定がブロックされます。
Community-list Object	設定がブロックされます。
コピー（Copy）	設定がブロックされます。
削除（Delete）	設定がブロックされます。
DHCP	設定がブロックされます。
パスワードを有効にする（Enable Password）	設定がブロックされます。
削除（Erase）	設定がブロックされます。
Fragment Setting	**fragment reassembly** を除きブロックされます。
Fsck	設定がブロックされます。
HTTP	設定がブロックされます。
ICMP	設定がブロックされます。
インターフェイス（Interface）	**nameif**、**mode**、**shutdown**、**ip address**、および **mac-address** コマンドのみがブロックされます。
Multicast Routing	設定がブロックされます。
NAT	設定がブロックされます。
Network Object/Object-group	FlexConfig オブジェクトでの Network オブジェクトの作成がブロックされますが、テンプレート内のオブジェクト マネージャで定義されているネットワーク オブジェクトとグループを変数として使用することができます。

禁止された CLI コマンド	説明
NTP	設定がブロックされます。
OSPF/OSPFv3	設定がブロックされます。
ポケットベル	設定がブロックされます。
パスワードの暗号化	設定がブロックされます。
Policy-list Object	設定がブロックされます。
Prefix-list Object	設定がブロックされます。
リロード（Reload）	リロードはスケジュールできません。システムは、システムを再起動するために **reload** コマンドを使用せず、**reboot** コマンドを使用します。
RIP	設定がブロックされます。
Route-Map Object	FlexConfig オブジェクトでの Route-map オブジェクトの作成がブロックされますが、テンプレート内のオブジェクト マネージャで定義されているルートマップ オブジェクトを変数として使用することができます。
Service Object/Object-group	FlexConfig オブジェクトでの Service オブジェクトの作成がブロックされますが、テンプレート内のオブジェクト マネージャで定義されているポート オブジェクトを変数として使用することができます。
SNMP	設定がブロックされます。
SSH	設定がブロックされます。
Static Route	設定がブロックされます。
Syslog	設定がブロックされます。
Time Synchronization	設定がブロックされます。
Timeout	設定がブロックされます。
VPN	設定がブロックされます。

テンプレート スクリプト

スクリプト言語を使用して、FlexConfig オブジェクト内部での処理を制御できます。スクリプト言語命令は、Apache Velocity 1.3.1 テンプレート エンジンでサポートされているコマンドの

サブセットです。Velocity テンプレート エンジンは、ループ、if/else ステートメント、および変数をサポートする Java ベースのスクリプト言語です。

スクリプト言語の使用方法についての詳細は、『*Velocity Developer Guide*』（http://velocity.apache.org/engine/devel/developer-guide.html）を参照してください。

FlexConfig 変数

コマンドまたは処理手順の一部がスタティック情報ではなくランタイム情報に依存する場合は、FlexConfig オブジェクトに変数を使用できます。展開時に、変数は変数のタイプに基づいてデバイスのその他の設定から取得された文字列に置き換えられます。

- ポリシー オブジェクト変数は、Firepower Management Center で定義されているオブジェクトから取得された文字列に置き換えられます。
- システム変数は、デバイス自体やデバイスに設定されたポリシーから取得した情報に置き換えられます。
- プロセス変数は、スクリプト コマンドの処理時に、ポリシー オブジェクトまたはシステム変数の内容とともにロードされます。たとえば、ループで、ポリシーオブジェクトまたはシステム変数から 1 つの値をプロセス変数に反復してロードし、プロセス変数を使用して、コマンド文字列を形成するか、その他のアクションを実行します。これらのプロセス変数は、FlexConfig オブジェクト内の [変数（Variables）] リストに表示されません。また、FlexConfig オブジェクト エディタの [挿入（Insert）] メニューを使用してこれらを追加しません。
- 秘密キー変数は、FlexConfig オブジェクト内の変数に定義された単一の文字列に置き換えられます。

変数は、$ 文字で始まりますが、@ で始まる秘密キーを除きます。たとえば、$ifname は次のコマンドのポリシー オブジェクト変数で、@keyname は秘密キーです。

```
interface $ifname
key @keyname
```

（注） ポリシー オブジェクトまたはシステム変数を初めて挿入する場合は、FlexConfig オブジェクト エディタの [挿入（Insert）] メニューを使用して挿入する必要があります。このアクションによって、FlexConfig オブジェクト エディタの下部にある [変数（Variables）] リストに変数が追加されます。ただし、システム変数を使用する場合でも、後続の使用では変数文字列を入力する必要があります。オブジェクトまたはシステム変数の割り当てがないプロセス変数を追加する場合は、[挿入（Insert）] メニューを使用しないでください。秘密キーを追加する場合は、常に [挿入（Insert）] メニューを使用します。秘密キーの変数は [変数（Variables）] リストに表示されません。

変数が単一の文字列、文字列のリスト、または値のテーブルのいずれとして解決されるかは、変数に割り当てるポリシー オブジェクトまたはシステム変数のタイプによって決まります（秘

密キーは、常に、単一の文字列として解決されます）。変数を適切に処理するには、何が返されるかを理解する必要があります。

次の各トピックでは、変数のさまざまなタイプとその処理方法について説明します。

変数の処理方法

ランタイムで、変数は単一の文字列、同じタイプの文字列のリスト、異なるタイプの文字列のリスト、あるいは名前付き値の表として解決することができます。また、複数の値に解決される変数の長さは一定、不定のどちらにすることもできます。変数を正しく処理するためには、何が返されるかを理解する必要があります。

返される値には、主に次の可能性があります。

単一値変数

変数が常に単一の文字列に解決される場合、FlexConfig スクリプトを変更せずに、その変数をそのまま使用できます。

たとえば、定義済みのテキスト変数 tcpMssBytes は常に単一の値（数値でなければなりません）に解決されます。**Sysopt_basic** FlexConfig は if/then/else 構造を使用して、別の単一値テキスト変数 tcpMssMinimum に基づきセグメントの最大サイズを設定します。

```
#if($tcpMssMinimum == "true")
  sysopt connection tcpmss minimum $tcpMssBytes
#else
  sysopt connection tcpmss $tcpMssBytes
#end
```

この例では、FlexConfig オブジェクト エディタで [挿入（Insert）] メニューを使用して最初の $tcpMssBytes の使用を追加しますが、#else 行には直接この変数を入力します。

秘密鍵の変数は、特殊なタイプの単一値変数です。秘密鍵では、変数を繰り返し使用する場合でも常に [挿入（Insert）] メニューを使用して変数を追加します。これらの変数は、FlexConfig オブジェクト内の [変数（Variables）] リストに表示されません。たとえば、EIGRP 設定のキーを非表示にするには、**Eigrp_Interface_Configure FlexConfig** をコピーして、$eigrpAuthKey 変数と $eigrpAuthKeyId 変数をそれぞれ秘密鍵 @SecretEigrpAuthKey および @SecretEigrpAuthKeyId で置き換えます。

```
authentication key eirgp $eigrpAS @SecretEigrpAuthKey key-id @SecretEigrpAuthKeyId
```

（注） ネットワーク オブジェクトのポリシー オブジェクト変数も、IP アドレスの単一の指定（ホスト アドレス、ネットワーク アドレス、アドレス範囲のいずれか）になります。ただしこの場合、ASA コマンドには特定のアドレス タイプが必要であるため、期待されるアドレスのタイプを把握している必要があります。たとえば、コマンドにホストアドレスが必要な場合、ネットワーク アドレスを含むオブジェクトを指すネットワーク オブジェクト変数を使用すると、導入時にエラーが発生します。

同じタイプの複数の値を持つ変数

ポリシーオブジェクトおよびシステム変数のなかには、同じタイプの複数の値に解決されるものがあります。たとえば、ネットワーク オブジェクト グループを指すオブジェクト変数は、そのグループ内の IP アドレスのリストに解決されます。同様に、システム変数 $SYS_FW_INTERFACE_NAME_LIST は、インターフェイス名のリストに解決されます。

同じタイプの複数の値に対応するテキスト オブジェクトを作成することもできます。たとえば、定義済みのテキストオブジェクト enableInspectProtocolList には複数のプロトコル名を含めることができます。

同じタイプの項目のリストに解決される複数の値を持つ変数は、長さが不定であることはよくあります。たとえば、ユーザは随時インターフェイスを設定または設定解除できるので、デバイス上にある名前付きインターフェイスの数を前もって知ることはできません。

そのため、同じタイプの複数の値を持つ変数を処理するには、通常はループを使用します。たとえば、定義済みの FlexConfig **Default_Inspection_Protocol_Enable** では、#foreach ループを使用して enableInspectProtocolList オブジェクトの各値を処理します。

```
policy-map global_policy
    class inspection_default
    #foreach ( $protocol in $enableInspectProtocolList)
    inspect $protocol
    #end
```

この例では、スクリプトが各値を順に $protocol 変数に代入し、その結果を ASA の **inspect** コマンドで使用して、そのプロトコルに対してインスペクションエンジンを有効にします。この場合、変数名として単純に $protocol と入力します。オブジェクトやシステム値を変数に代入するわけではないので、[挿入（Insert）] メニューを使用して変数を追加することはしません。ただし、$enableInspectProtocolList を追加する場合は、[挿入（Insert）] メニューを使用する必要があります。

システムは $enableInspectProtocolList 内の値がなくなるまで、#foreach と #end の間にあるコードをループ処理します。

タイプが異なる複数の値を持つ変数

それぞれの値が異なる目的を果たす、複数の値を持つテキストオブジェクトを作成できます。たとえば、定義済みの **netflow_Destination** テキスト オブジェクトに、インターフェイス名、宛先 IP アドレス、UDP ポート番号という 3 つの値がこの順で設定されているとします。

このように定義するオブジェクトは、既定の数の値を持たなければなりません。そうでないと、処理するのが難しくなります。

このようなオブジェクトを処理するには、get メソッドを使用します。オブジェクト名の末尾に **.get(*n*)** と入力し、*n* をそのオブジェクトのインデックスで置き換えます。テキスト オブジェクトは値を 1 からリストしますが、インデックスは 0 からカウントします。

たとえば、Netflow_Add_Destination オブジェクトは次の行を使用して、netflow_Destination に含まれる 3 つの値を ASA の **flow-export** コマンドに追加します。

```
flow-export destination $netflow_Destination.get(0) $netflow_Destination.get(1)
```

```
$netflow_Destination.get(2)
```

この例では、FlexConfig オブジェクト エディタの [挿入（Insert）] メニューを使用して $netflow_Destination の最初の使用を追加してから、**.get(0)** を追加します。ただし、**$netflow_Destination.get(1)** および **$netflow_Destination.get(2)** の変数は直接入力して指定する必要があります。

値のテーブルに解決される、複数の値を持つ変数

システム変数のなかには、値のテーブルを返すものがあります。そのような変数に該当するのは、たとえば $SYS_FTD_ROUTED_INTF_MAP_LIST のように、MAP が名前に含まれる変数です。ルーテッド インターフェイス マップは、以下のようなデータを返します（わかりやすくするために改行が追加されています）。

```
[{intf_hardwarare_id=GigabitEthernet0/0, intf_ipv6_eui64_addresses=[],
intf_ipv6_prefix_addresses=[], intf_subnet_mask_v4=255.255.255.0,
intf_ip_addr_v4=10.100.10.1, intf_ipv6_link_local_address=,
intf_logical_name=outside},

{intf_hardwarare_id=GigabitEthernet0/1, intf_ipv6_eui64_addresses=[],
intf_ipv6_prefix_addresses=[], intf_subnet_mask_v4=255.255.255.0,
intf_ip_addr_v4=10.100.11.1, intf_ipv6_link_local_address=,
intf_logical_name=inside},

{intf_hardwarare_id=GigabitEthernet0/2, intf_ipv6_eui64_addresses=[],
intf_ipv6_prefix_addresses=[], intf_subnet_mask_v4=, intf_ip_addr_v4=,
intf_ipv6_link_local_address=, intf_logical_name=},

{intf_hardwarare_id=Management0/0, intf_ipv6_eui64_addresses=[],
intf_ipv6_prefix_addresses=[], intf_subnet_mask_v4=, intf_ip_addr_v4=,
intf_ipv6_link_local_address=, intf_logical_name=diagnostic}]
```

上記の例では、4 つのインターフェイスに関する情報が返されています。インターフェイスごとに、名前付き値のテーブルが含まれています。たとえば、intf_hardwarare_id はインターフェイス ハードウェアの名前プロパティであり、GigabitEthernet0/0 などの文字列として返されます。

このような変数は、通常は長さが不定であるため、値を処理するにはループ処理を使用する必要があります。また、取得対象の値を示すために、変数名にプロパティ名も追加する必要があります。

たとえば、IS-IS 構成では、インターフェイス コンフィギュレーション モードで、論理名を持つインターフェイスに ASA の **isis** コマンドを追加する必要があります。ただし、このモードを開始する際は、インターフェイスのハードウェア名を使用します。したがって、論理名を持つインターフェイスを識別してから、それらのインターフェイスだけをそれぞれのハードウェア名を使用して設定する必要があります。ISIS_Interface_Configuration の定義済み FlexConfig は、そのために、ループ内にネストされた if/then 構造を使用します。以下のコードを見るとわかるように、#foreach スクリプト コマンドで各インターフェイス マップを $intf 変数に読み込んだ後、#if ステートメントでマップ（$intf.intf_logical_name）から intf_logical_name の値を取得し、その値が isisIntfList 定義済みテキスト変数で定義されているリストに含まれている場合は、intf_hardwarare_id の値（$intf.intf_hardwarare_id）を使用してインターフェイス コマンドを

入力します。IS-IS を設定するインターフェイスの名前を追加する場合は、isisIntfList 変数を編集する必要があります。

```
#foreach ($intf in $SYS_FTD_ROUTED_INTF_MAP_LIST)
 #if ($isIsIntfList.contains($intf.intf_logical_name))
  interface $intf.intf_hardwarare_id
   isis
   #if ($isIsAddressFamily.contains("ipv6"))
   ipv6 router isis
   #end
 #end
#end
```

変数がデバイスに関して返す内容を表示する方法

変数が何を返すかを評価する簡単な方法は、変数の注釈付きリストを処理するだけの簡単な FlexConfig オブジェクトを作成することです。次に、作成したオブジェクトを FlexConfig ポリシーに割り当て、ポリシーをデバイスに割り当てます。ポリシーを保存してから、そのデバイスの設定のプレビューをプレビューします。解決された値がプレビューに表示されます。プレビューのテキストを選択し、Ctrl キーを押した状態で C キーを押し、出力を分析用にテキストファイルに貼り付けることができます。

（注） ただし、FlexConfig には有効な設定コマンドが一切含まれていないため、FlexConfig をデバイスに展開しないでください。展開すると展開エラーが生じます。プレビューの取得後、FlexConfig ポリシーから FlexConfig オブジェクトを削除し、ポリシーを保存します。

たとえば、次の FlexConfig オブジェクトを作成することができます。

```
Following is a network object group variable for the
IPv4-Private-All-RFC1918 object:

$IPv4_Private_addresses

Following is the system variable SYS_FW_MANAGEMENT_IP:

$SYS_FW_MANAGEMENT_IP

Following is the system variable SYS_FW_ENABLED_INSPECT_PROTOCOL_LIST:

$SYS_FW_ENABLED_INSPECT_PROTOCOL_LIST

Following is the system variable SYS_FTD_ROUTED_INTF_MAP_LIST:

$SYS_FTD_ROUTED_INTF_MAP_LIST

Following is the system variable SYS_FW_INTERFACE_NAME_LIST:

$SYS_FW_INTERFACE_NAME_LIST
```

このオブジェクトのプレビューは以下のように表示されます（明確にするために改行が追加されています）。

```
###Flex-config Prepended CLI ###

###CLI generated from managed features ###

###Flex-config Appended CLI ###
Following is an network object group variable for the
IPv4-Private-All-RFC1918 object:

[10.0.0.0, 172.16.0.0, 192.168.0.0]

Following is the system variable SYS_FW_MANAGEMENT_IP:

192.168.0.171

Following is the system variable SYS_FW_ENABLED_INSPECT_PROTOCOL_LIST:

[dns, ftp, h323 h225, h323 ras, rsh, rtsp, sqlnet, skinny, sunrpc,
xdmcp, sip, netbios, tftp, icmp, icmp error, ip-options]

Following is the system variable SYS_FTD_ROUTED_INTF_MAP_LIST:

[{intf_hardwarare_id=GigabitEthernet0/0, intf_ipv6_eui64_addresses=[],
intf_ipv6_prefix_addresses=[], intf_subnet_mask_v4=255.255.255.0,
intf_ip_addr_v4=10.100.10.1, intf_ipv6_link_local_address=,
intf_logical_name=outside},

{intf_hardwarare_id=GigabitEthernet0/1, intf_ipv6_eui64_addresses=[],
intf_ipv6_prefix_addresses=[], intf_subnet_mask_v4=255.255.255.0,
intf_ip_addr_v4=10.100.11.1, intf_ipv6_link_local_address=,
intf_logical_name=inside},

{intf_hardwarare_id=GigabitEthernet0/2, intf_ipv6_eui64_addresses=[],
intf_ipv6_prefix_addresses=[], intf_subnet_mask_v4=, intf_ip_addr_v4=,
intf_ipv6_link_local_address=, intf_logical_name=},

{intf_hardwarare_id=Management0/0, intf_ipv6_eui64_addresses=[],
intf_ipv6_prefix_addresses=[], intf_subnet_mask_v4=, intf_ip_addr_v4=,
intf_ipv6_link_local_address=, intf_logical_name=diagnostic}]

Following is the system variable SYS_FW_INTERFACE_NAME_LIST:

[outside, inside, diagnostic]
```

FlexConfig ポリシー オブジェクト変数

ポリシー オブジェクト変数は、オブジェクト マネージャで設定されている特定のポリシー オブジェクトに関連付けられます。FlexConfig オブジェクトにポリシー オブジェクト変数を挿入する場合、変数に名前を付け、これに関連付けられているオブジェクトを選択します。

関連付けられているオブジェクトと完全に同じ名前を変数に付けても、変数自体は、関連付けられたオブジェクトと同じではありません。FlexConfig で初めてスクリプトに変数を追加し、オブジェクトとの関連付けを確立するには、FlexConfig オブジェクト エディタの **[挿入（Insert）] > [ポリシー オブジェクトの挿入（Insert Policy Object）] > *[オブジェクト タイプ（Object Type）]*** メニューを使用する必要があります。単に $ 記号に続けてオブジェクト名を入力しても、ポリシー オブジェクト変数は作成されません。

以下のタイプのオブジェクトを指す変数を作成できます。各変数に適切なタイプのオブジェクトを作成するようにしてください。オブジェクトを作成するには、**[オブジェクト（Objects）]**> **[オブジェクト管理（Object Management）]** に移動します。

- テキスト オブジェクト（Text Objects）：テキスト文字列の場合。これには、IP アドレス、番号や、インターフェイス、ゾーン名などの自由形式のテキストが含まれます。コンテンツ テーブルから **[FlexConfig]** > **[テキスト オブジェクト（Text Object）]** を選択し、[テキスト オブジェクトの追加（Add Text Object）] をクリックします。単一の値または複数の値を含むようにこれらのオブジェクトを設定できます。これらのオブジェクトは柔軟性が高く、FlexConfig オブジェクト内で使用するよう特別に構築されています。詳細については、FlexConfig テキスト オブジェクトの設定 （1234 ページ）を参照してください。
- ネットワーク（Network）：IP アドレスの場合。ネットワーク オブジェクトまたはグループを使用できます。コンテンツ テーブルから [ネットワーク（Network）] を選択し、**[ネットワークを追加（Add Network）]** > **[オブジェクトの追加（Add Object）]** または [グループの追加（Add Group）] を選択します。グループ オブジェクトを使用すると、変数によりグループ内の各 IP アドレス指定のリストが返されます。アドレスは、オブジェクトの内容に応じて、ホスト、ネットワーク、またはアドレス範囲にできます。ネットワーク オブジェクト （525 ページ）を参照してください。
- セキュリティ ゾーン（Security Zones）：セキュリティ ゾーンまたはインターフェイス グループ内のインターフェイスの場合。コンテンツ テーブルから [インターフェイス（Interface）] を選択し、**[追加（Add）]** > **[セキュリティ ゾーン（Security Zones）]** または [インターフェイス グループ（Interface Group）] を選択します。セキュリティ ゾーン変数では、設定中のデバイスのゾーンまたはグループ内のインターフェイスのリストが返されます。インターフェイス オブジェクト：インターフェイスグループとセキュリティ ゾーン （535 ページ）を参照してください。
- 標準 ACL オブジェクト（Standard ACL Object）：標準アクセス コントロール リストの場合。標準 ACL 変数では、標準 ACL オブジェクトの名前が返されます。コンテンツ テーブルから **[アクセス リスト（Access List）]** > **[標準（Standard）]** を選択し、[標準アクセス リスト オブジェクトの追加（Add Standard Access List Object）] をクリックします。アクセス リスト （610 ページ）を参照してください。
- 拡張 ACL オブジェクト（Extended ACL Object）：拡張アクセス コントロール リストの場合。拡張 ACL 変数では、拡張 ACL オブジェクトの名前が返されます。コンテンツ テーブルから **[アクセス リスト（Access List）]** > **[拡張（Extended）]** を選択し、[拡張アクセス リスト オブジェクトの追加（Add Extended Access List Object）] をクリックします。アクセス リスト （610 ページ）を参照してください。
- ルート マップ（Route Map）：ルート マップ オブジェクトの場合。ルート マップ変数では、ルート マップ オブジェクトの名前が返されます。コンテンツ テーブルから [ルート マップ（Route Map）] を選択し、[ルート マップの追加（Add Route Map）] をクリックします。ルート マップ （606 ページ）を参照してください。

FlexConfig システム変数

システム変数は、デバイス自体やデバイスに設定されたポリシーから取得した情報に置き換えられます。

FlexConfig オブジェクト エディタの **[挿入（Insert）] > [システム変数の挿入（Insert System Variable）] > /変数名/** メニューを使用して、最初の変数を FlexConfig のスクリプトに追加し、システム変数とのアソシエーションを確立します。単に $ 記号に続けてシステム変数名を入力しても、FlexConfig オブジェクトのコンテキストでのシステム変数は作成されません。

次の表に、使用可能なシステム変数の説明を示します。変数を使用する前に、通常、その変数に何が返されるかを確認します。変数がデバイスに関して返す内容を表示する方法（1211 ページ）を参照してください。

名前	説明
SYS_FW_OS_MODE	デバイスのオペレーティング システム モード。値は ROUTED または TRANSPARENT です。
SYS_FW_OS_MULTIPLICITY	デバイスがシングル コンテキスト モードまたはマルチ コンテキスト モードのいずれで動作するか。値は、SINGLE、MULTI、または NOT_APPLICABLE です。
SYS_FW_MANAGEMENT_IP	デバイスの管理 IP アドレス。
SYS_FW_HOST_NAME	デバイスのホスト名。
SYS_FTD_INTF_POLICY_MAP	キーがインターフェイス名で、値がポリシーマップのマップ。この変数は、デバイスにインターフェイスベースのサービス ポリシーが定義されていない場合、値を返しません。
SYS_FW_ENABLED_INSPECT_PROTOCOL_LIST	インスペクションが有効になっているプロトコルのリスト。
SYS_FTD_ROUTED_INTF_MAP_LIST	デバイスのルーテッド インターフェイス マップのリスト。各マップには、ルーテッド インターフェイス構成に関連する一連の名前付き値が含まれます。
SYS_FTD_SWITCHED_INTF_MAP_LIST	デバイスのスイッチド インターフェイス マップのリスト。各マップには、スイッチド インターフェイス構成に関連する一連の名前付き値が含まれます。
SYS_FTD_INLINE_INTF_MAP_LIST	デバイスのインライン インターフェイス マップのリスト。各マップには、インライン セット インターフェイス構成に関連する一連の名前付き値が含まれます。
SYS_FTD_PASSIVE_INTF_MAP_LIST	デバイスのパッシブ インターフェイス マップのリスト。各マップには、パッシブ インターフェイス構成に関連する一連の名前付き値が含まれます。

名前	説明
SYS_FTD_INTF_BVI_MAP_LIST	デバイスのブリッジ仮想インターフェイスマップのリスト。各マップには、BVI 構成に関連する一連の名前付き値が含まれます。
SYS_FW_INTERFACE_HARDWARE_ID_LIST	GigabitEthernet0/0 など、デバイスのインターフェイスのハードウェア名のリスト。
SYS_FW_INTERFACE_NAME_LIST	内部など、デバイスのインターフェイスの論理名のリスト。
SYS_FW_INLINE_INTERFACE_NAME_LIST	パッシブまたは ERSPAN パッシブとして設定されたインターフェイスの論理名のリスト。
SYS_FW_NON_INLINE_INTERFACE_NAME_LIST	すべてのルーテッド インターフェイスなど、インライン セットの一部ではないインターフェイスの論理名のリスト。

定義済みの FlexConfig オブジェクト

定義済みの FlexConfig オブジェクトは、選択機能に検証済みの設定を提供します。Firepower Management Center で別の方法では設定できないこれらの機能を設定する必要がある場合は、これらのオブジェクトを使用します。

次の表に、使用可能なオブジェクトを示します。関連するテキスト オブジェクトをメモしてください。定義済みの FlexConfig オブジェクトの動作をカスタマイズするには、これらのテキスト オブジェクトを編集する必要があります。テキスト オブジェクトにより、ネットワークおよびデバイスで必要な IP アドレスとその他の属性を使用して、設定をカスタマイズできます。

定義済みの FlexConfig オブジェクトを変更する必要がある場合は、オブジェクトをコピーしてそれを変更し、新しい名前で保存します。定義済みの FlexConfig オブジェクトを直接編集することはできません。

FlexConfig を使用して、他の ASA ベースの機能を設定できますが、これらの機能の設定は検証されていません。ASA 機能が Firepower Management Center ポリシーで設定できる機能と重複している場合は、FlexConfig を使用して設定しないでください。

たとえば、Snort 検査には HTTP プロトコルが含まれるため、ASA スタイルの HTTP 検査を有効にしないでください。（実際に、enableInspectProtocolList オブジェクトに **http** を追加することはできません。この場合、デバイスを誤って設定することが回避されます）。代わりに、必要に応じて、アプリケーションまたは URL フィルタリングを実行するアクセス コントロール ポリシーを設定し、HTTP 検査要件を実装します。

FlexConfig オブジェクト名	説明	関連するテキスト オブジェクト
Default_DNS_Configure (非推奨メソッド.)	デフォルト DNS グループを設定します。デフォルト DNS グループでは、データインターフェイスの完全修飾ドメイン名を解決する際に使用できる DNS サーバを定義します。これにより、IP アドレスではなくホスト名を使用して、CLI で **ping** などのコマンドを使用することができます。 バージョン 6.3 以降では、Firepower Threat Defense プラットフォーム設定ポリシーでデータ インターフェイスの DNS を設定します。	defaultDNSNameServerList、defaultDNSParameters
Default_Inspection_Protocol_Disable	global_policy デフォルト ポリシー マップのプロトコルを無効にします。	disableInspectProtocolList
Default_Inspection_Protocol_Enable	global_policy デフォルト ポリシー マップのプロトコルを有効にします。	enableInspectProtocolList
DHCPv6_Prefix_Delegation_Configure	IPv6 プレフィックス委任の 1 つの外部インターフェイス（プレフィックス委任クライアント）と 1 つの内部インターフェイス（委任されたプレフィックスの受信者）を設定します。このテンプレートを使用するには、テンプレートをコピーして変数を変更します。	pdoutside、pdinside また、システム変数 SYS_FTD_ROUTED_INTF_MAP_LIST を使用します
DHCPv6_Prefix_Delegation_UnConfigure	DHCPv6 プレフィックス委任設定を削除します。	pdoutside、pdinside また、システム変数 SYS_FTD_ROUTED_INTF_MAP_LIST を使用します
DNS_Configure	デフォルト以外の DNS サーバ グループの DNS サーバを設定します。グループの名前を変更するには、オブジェクトをコピーします。	dnsNameServerList、dnsParameters。
DNS_UnConfigure	Default_DNS_Configure と DNS_Configure で実行される DNS サーバの構成を削除します。DNS_Configure を変更した場合に DNS サーバ グループ名を変更するには、オブジェクトをコピーします。	—

FlexConfig オブジェクト名	説明	関連するテキスト オブジェクト
Eigrp_Configure	EIGRP ルーティングのネクストホップ、自動集約、ルータ ID、eigrp スタブを設定します。	eigrpAS、eigrpNetworks、eigrpDisableAutoSummary、eigrpRouterId、eigrpStubReceiveOnly、eigrpStubRedistributed、eigrpStubConnected、eigrpStubStatic、eigrpStubSummary
Eigrp_Interface_Configure	EIGRPインターフェイス認証モード、認証キー、Hello インターバル、ホールド時間、スプリットホライズンを設定します。	eigrpIntfList、eigrpAS、eigrpAuthKey、eigrpAuthKeyId、eigrpHelloInterval、eigrpHoldTime、eigrpDisableSplitHorizon また、システム変数 SYS_FTD_ROUTED_INTF_MAP_LIST を使用します
Eigrp_Unconfigure	デバイスから自律システムのEIGRP設定をクリアします。	—
Eigrp_Unconfigure_all	すべてのEIGRP設定をクリアします。	—
Inspect_IPv6_Configure	global_policy ポリシーマップで IPv6 検査を設定し、IPv6ヘッダーコンテンツに基づいてトラフィックを記録およびドロップします。	IPv6RoutingHeaderDropLogList、IPv6RoutingHeaderLogList、IPv6RoutingHeaderDropList。
Inspect_IPv6_UnConfigure	IPv6 検査をクリアおよび無効にします。	—
ISIS_Configure	IS-IS ルーティングのグローバル パラメータを設定します。	isIsNet、isIsAddressFamily、isISType
ISIS_Interface_Configuration	インターフェイス レベルの IS-IS 設定。	isIsAddressFamily、IsIsIntfList また、システム変数 SYS_FTD_ROUTED_INTF_MAP_LIST を使用します
ISIS_Unconfigure	デバイスの IS-IS ルータ設定をクリアします。	—
ISIS_Unconfigure_All	デバイスから IS-IS ルータ設定をクリアします（デバイスインターフェイスの IS-IS ルータ割り当てなど）。	—
Netflow_Add_Destination	NetFlow エクスポートの宛先を作成し、設定します。	Netflow_Destinations、netflow_Event_Types

FlexConfig オブジェクト名	説明	関連するテキスト オブジェクト
Netflow_Clear_Parameters	NetFlow エクスポートのグローバル デフォルト設定を復元します。	—
Netflow_Delete_Destination	NetFlow エクスポートの宛先を削除します。	Netflow_Destinations、netflow_Event_Types
Netflow_Set_Parameters	NetFlow エクスポートのグローバル パラメータを設定します。	netflow_Parameters
NGFW_TCP_NORMALIZATION	デフォルト TCP 正規化設定を変更します。	—
Policy_Based_Routing	この設定例を使用するには、コピーしてインターフェイス名を変更し、r-map-object テキストオブジェクトを使用してオブジェクト マネージャでルート マップ オブジェクトを特定します。	—
Policy_Based_Routing_Clear	デバイスからポリシーベース ルーティング設定をクリアします。	—
Sysopt_AAA_radius	RADIUS アカウンティング応答内の認証キーを無視します。	—
Sysopt_AAA_radius_negate	Sysopt_AAA_radius 設定を拒否します。	—
Sysopt_basic	sysopt 待機時間、TCP パケットの最大セグメントサイズ、詳細トラフィック統計情報を設定します。	tcpMssMinimum、tcpMssBytes
Sysopt_basic_negate	sysopt_basic 詳細トラフィック統計情報、待機時間、TCP 最大セグメント サイズをクリアします。	—
Sysopt_clear_all	デバイスからすべての sysopt 設定をクリアします。	—
Sysopt_noproxyarp	noproxy arp CLI を設定します。	システム変数 SYS_FW_NON_INLINE_INTF_NAME_LIST を使用します
Sysopt_noproxyarp_negate	Sysopt_noproxyarp 設定をクリアします。	システム変数 SYS_FW_NON_INLINE_INTF_NAME_LIST を使用します
Sysopt_Preserve_Vpn_Flow	syopt 保存 VPN フローを設定します。	—

FlexConfig オブジェクト名	説明	関連するテキスト オブジェクト
Sysopt_Preserve_Vpn_Flow_negate	Sysopt_Preserve_Vpn_Flow 設定をクリアします。	—
Sysopt_Reclassify_Vpn	sysopt 再分類 vpn を設定します。	—
Sysopt_Reclassify_Vpn_Negate	sysopt 再分類 vpn を拒否します。	—
TCP_Embryonic_Conn_Limit (非推奨メソッド.)	初期接続制限を設定して SYN フラッドサービス妨害（DoS）攻撃から保護します。 バージョン 6.3 以降では、これらの機能を Firepower Threat Defense サービスポリシーで設定します。このポリシーは、デバイスに割り当てられているアクセス コントロール ポリシーの [詳細（Advanced）] タブで確認できます。	tcp_conn_misc、tcp_conn_limit
TCP_Embryonic_Conn_Timeout (非推奨メソッド.)	初期接続タイムアウトを設定してSYN フラッドサービス妨害（DoS）攻撃から保護します。 バージョン 6.3 以降では、これらの機能を Firepower Threat Defense サービスポリシーで設定します。このポリシーは、デバイスに割り当てられているアクセス コントロール ポリシーの [詳細（Advanced）] タブで確認できます。	tcp_conn_misc、tcp_conn_timeout
Threat_Detection_Clear	脅威検出TCP代行受信設定をクリアします。	—
Threat_Detection_Configure	TCP代行受信によって代行受信される攻撃の脅威検出統計情報を設定します。	threat_detection_statistics
VxLAN_Clear_Nve	デバイスから VxLAN_Configure_Port_And_Nve が使用される場合、NVE 1 設定を削除します。	—
VxLAN_Clear_Nve_Only	展開時にインターフェイスで設定された NVE 設定をクリアします。	—
VxLAN_Configure_Port_And_Nve	VLAN ポートと NVE 1 を設定します。	vxlan_Port_And_Nve

FlexConfig オブジェクト名	説明	関連するテキスト オブジェクト
VxLAN_Make_Nve_Only	NVE のみのインターフェイスを設定します。	vxlan_Nve_Only また、システム変数 SYS_FTD_ROUTED_MAP_LIST と SYS_FTD_SWITCHED_INTF_MAP_LIST を使用します
VxLAN_Make_Vni	VNI インターフェイスを作成します。これを展開した後、VNI インターフェイスを正しく検出するには、デバイスの登録を解除して、再登録する必要があります。	vxlan_Vni
Wccp_Configure	このテンプレートは WCCP を設定する例を提供します。	isServiceIdentifier、serviceIdentifier、wccpPassword
Wccp_Configure_Clear	WCCP 設定をクリアします。	—

定義済みのテキスト オブジェクト

複数の定義済みのテキスト オブジェクトがあります。これらのオブジェクトは、定義済みの FlexConfig オブジェクトで使用される変数に関連付けられています。ほとんどの場合、関連付けられた FlexConfig オブジェクトを使用するにはこれらのオブジェクトを編集して値を追加する必要があります。そうしない場合、展開中にエラーが表示されます。これらのオブジェクトの一部にはデフォルト値が含まれていますが、その他は空となっています。

テキスト オブジェクトの編集の詳細については、FlexConfig テキスト オブジェクトの設定 （1234 ページ）を参照してください。

名前	説明	関連する FlexConfig オブジェクト
defaultDNSNameServerList (非推奨メソッド.)	デフォルト DNS グループで設定する DNS サーバの IP アドレス。 バージョン 6.3 以降では、Firepower Threat Defense プラットフォーム設定ポリシーでデータ インターフェイスの DNS を設定します。	Default_DNS_Configure

名前	説明	関連する FlexConfig オブジェクト
defaultDNSParameters (非推奨メソッド.)	デフォルト DNS サーバ グループの DNS 動作を制御するパラメータ。オブジェクトには、再試行、タイムアウト、有効期限エントリ タイマー、ポール タイマー、ドメイン名の個別のエントリが順番に含まれています。 バージョン 6.3 以降では、Firepower Threat Defense プラットフォーム設定ポリシーでデータ インターフェイスの DNS を設定します。	Default_DNS_Configure
disableInspectProtocolList	デフォルト ポリシー マップ（global_policy）のプロトコルを無効にします。	Disable_Default_Inspection_Protocol
dnsNameServerList	ユーザ定義の DNS グループで設定する DNS サーバの IP アドレス。	DNS_Configure
dnsParameters	デフォルト以外の DNS サーバ グループの DNS 動作を制御するパラメータ。オブジェクトには、再試行、タイムアウト、ドメイン名、ドメイン名、ネーム サーバ インターフェイスの個別のエントリが順番に含まれています。	DNS_Configure
eigrpAS	自律システム番号。	Eigrp_Configure、 Eigrp_Interface_Configure、 Eigrp_Unconfigure
eigrpAuthKey	EIGRP 認証キー。	Eigrp_Interface_Configure
eigrpAuthKeyId	認証キーと一致する共有キー ID。	Eigrp_Interface_Configure
eigrpDisableAutoSummary	true の場合に自動集約を無効にするフラグ。	Eigrp_Configure
eigrpDisableSplitHorizon	true の場合にスプリット ホライズンを無効にするフラグ。	Eigrp_Interface_Configure
eigrpHelloInterval	hello 伝送間の秒数。	Eigrp_Interface_Configure
eigrpHoldTime	ネイバーが停止しているとみなされるまで秒数。	Eigrp_Interface_Configure
eigrpIntfList	EIGRP が適用される論理インターフェイス名のリスト。	Eigrp_Interface_Configure

名前	説明	関連する FlexConfig オブジェクト
eigrpRouterId	IP アドレス形式でのルータ ID。	Eigrp_Configure
eigrpStubConnected	true の場合、**eigrp stub** の設定で **connected** を使用できるようにするフラグ。	Eigrp_Configure
eigrpStubReceiveOnly	true の場合、**eigrp stub** の設定で **receive-only** を使用できるようにするフラグ。	Eigrp_Configure
eigrpStubRedistributed	true の場合、**eigrp stub** の設定で **redistributed** を使用できるようにするフラグ。	Eigrp_Configure
eigrpStubSummary	true の場合、**eigrp stub** の設定で **summary** を使用できるようにするフラグ。	Eigrp_Configure
enableInspectProtocolList	デフォルト ポリシー マップ（global_policy）のプロトコルを有効にします。検査が Snort 検査と競合するプロトコルを追加することはできません。	Enable_Default_Inspection_Protocol
IPv6RoutingHeaderDropList	ユーザが拒否する IPv6 ルーティング ヘッダー タイプのリスト。これらのヘッダーを含むパケットは IPv6 検査でドロップをログに記録せずにドロップされます。	Inspect_IPv6_Configure
IPv6RoutingHeaderDropLogList	ユーザが拒否し、ログに記録する IPv6 ルーティング ヘッダー タイプのリスト。これらのヘッダーを含むパケットは IPv6 検査でドロップされ、ドロップに関する syslog メッセージが送信されます。	Inspect_IPv6_Configure
IPv6RoutingHeaderLogList	許可するが、ログに記録する IPv6 ルーティング ヘッダー タイプのリスト。これらのヘッダーを含むパケットは IPv6 検査で許可されますが、ヘッダーの存在に関する syslog メッセージが送信されます。	Inspect_IPv6_Configure
isIsAddressFamily	IPv4 または IPv6 アドレス ファミリ。	ISIS_Configure ISIS_Interface_Configuration

名前	説明	関連する FlexConfig オブジェクト
IsIsIntfList	論理インターフェイス名のリスト。	ISIS_Interface_Configuration
isIsISType	IS タイプ（level-1、level-2-only、または level-1-2）。	ISIS_Configure
isIsNet	ネットワーク エンティティ。	ISIS_Configure
isServiceIdentifier	false の場合は、標準 **web-cache** サービス識別子を使用します。	Wccp_Configure
netflow_Destination	1 つの NetFlow エクスポート宛先のインターフェイス、接続先、およびUDPポート番号を定義します。	Netflow_Add_Destination
netflow_Event_Types	エクスポートされる宛先のイベントのタイプを **all**、**flow-create**、**flow-defined**、**flow-teardown**、**flow-update** のいずれかのサブセットとして定義します。	Netflow_Add_Destination
netflow_Parameters	NetFlow エクスポートのグローバル設定を指定します。アクティブ更新間隔（フロー更新イベント間の分数）、遅延（フロー作成遅延（秒単位）。デフォルトの 0 ではコマンドは表示されません）、およびテンプレートタイムアウト レート（分単位）。	Netflow_Set_Parameters
PrefixDelegationInside	DHCPv6 プレフィックス委任の内部インターフェイスを設定します。オブジェクトには、インターフェイス名、IPv6 サフィックスとプレフィックス長、およびプレフィックスプール名の複数のエントリが順番に含まれています。	なし、ただし DHCPv6_Prefix_Delegation_Configure のコピーとともに使用できます。
PrefixDelegationOutside	外部 DHCPv6 プレフィックス委任クライアントを設定します。オブジェクトには、インターフェイス名と IPv6 プレフィックス長の複数のエントリが順番に含まれています。	なし、ただし DHCPv6_Prefix_Delegation_Configure のコピーとともに使用できます。
serviceIdentifier	ダイナミック WCCP サービス ID 番号。	Wccp_Configure

名前	説明	関連する FlexConfig オブジェクト
tcp_conn_limit (非推奨メソッド.)	TCP 初期接続制限を設定するために使用されるパラメータ。 バージョン 6.3 以降では、これらの機能を Firepower Threat Defense サービス ポリシーで設定します。このポリシーは、デバイスに割り当てられているアクセス コントロール ポリシーの [詳細（Advanced）] タブで確認できます。	TCP_Embryonic_Conn_Limit
tcp_conn_misc (非推奨メソッド.)	TCP 初期接続設定を設定するために使用されるパラメータ。 バージョン 6.3 以降では、これらの機能を Firepower Threat Defense サービス ポリシーで設定します。このポリシーは、デバイスに割り当てられているアクセス コントロール ポリシーの [詳細（Advanced）] タブで確認できます。	TCP_Embryonic_Conn_Limit、 TCP_Embryonic_Conn_Timeout
tcp_conn_timeout (非推奨メソッド.)	TCP 初期接続タイムアウトを設定するために使用されるパラメータ。 バージョン 6.3 以降では、これらの機能を Firepower Threat Defense サービス ポリシーで設定します。このポリシーは、デバイスに割り当てられているアクセス コントロール ポリシーの [詳細（Advanced）] タブで確認できます。	TCP_Embryonic_Conn_Timeout
tcpMssBytes	最大セグメント サイズ（バイト単位）。	Sysopt_basic
tcpMssMinimum	このフラグが true の場合にのみ設定される最大セグメント サイズ（MSS）を設定するかどうかをチェックします。	Sysopt_basic
threat_detection_statistics	TCP 代行受信の脅威検出統計情報に使用されるパラメータ。	Threat_Detection_Configure

名前	説明	関連する FlexConfig オブジェクト
vxlan_Nve_Only	インターフェイスで NVE-only を設定するためのパラメータ： • インターフェイスの論理名 • IPv4 アドレス（ルーテッド インターフェイスではオプション） • IPv4 ネットマスク（ルーテッドインターフェイスではオプション）	VxLAN_Make_Nve_Only
vxlan_Port_And_Nve	VXLAN のポートおよび NVE を設定するために使用されるパラメータ： • vxlan ポート • 送信元インターフェイス（論理名） • タイプ（ピアまたは mcast） • ピアとなる IP アドレスまたは default-mcast-grooup	VxLAN_Configure_Port_And_Nve
vxlan_Vni	VNI を作成するために使用されるパラメータ： • インターフェイス番号（1 ～ 10000） • segment-id（1 ～ 16777215） • nameif（インターフェイスの論理名） • タイプ（ルーテッドまたはトランスペアレント） • IP アドレス（ルーテッドモードのデバイスの場合に使用）またはブリッジグループ番号（トランスペアレントモードのデバイスの場合に使用） • ネットマスク（デバイスがルーテッドモードの場合）または未使用	VxLAN_Make_Vni
wccpPassword	WCCP パスワード。	Wccp_Configure

FlexConfig の注意事項と制約事項

- FlexConfig ポリシーに誤りがあると、システムは失敗した FlexConfig を含む展開の試行に含まれるすべての変更をロールバックします。展開の失敗が原因でロールバックに設定のクリアが含まれるため、ネットワークに悪影響を及ぼす可能性があります。営業時間外の FlexConfig の変更を含む、展開のタイミングを検討します。また、FlexConfig の変更だけが含まれるように展開を分離し、その他のポリシーの更新が行われないようにします。
- VxLAN_Make_VNI オブジェクトを使用する場合は、クラスタまたはハイ アベイラビリティ ペアを形成する前に、同じ FlexConfig をクラスタまたはハイ アベイラビリティ ペアのすべてのユニットに展開する必要があります。管理センターでは、クラスタまたはハイアベイラビリティ ペアを形成する前に、すべてのデバイスで VXLAN インターフェイスを照合する必要があります。
- トラフィック ゾーンを使用して Equal-Cost-Multi-Path（ECMP）ルーティングを構成する場合、**zone** コマンドは、ASA で使用されるものと FTD デバイスとで異なります。ただし、ASA の一般的な構成ガイドの指示を引き続き利用できます。ASA バージョンのコマンドの代わりに **zone** *name* **ecmp** を使用します。それ以外の場合は、ASA と FTD のトラフィック ゾーン機能の動作は同じです。

（注） また、一部のインターフェイスをパッシブとして定義する場合は、**zone** *name* **passive** コマンドを設定してパッシブ ゾーンを設定します。これは、ご使用のインターフェイス構成に基づいて自動的に処理されます。パッシブ トラフィック ゾーンを作成するために FlexConfig を使用しないでください。

FlexConfig ポリシーによるデバイス設定のカスタマイズ

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	Firepower Threat Defense Firepower Threat Defense Virtual	いずれか（Any）	Admin

FlexConfig ポリシーを使用して、FTD デバイスの設定をカスタマイズします。

FlexConfig を使用する前に、Firepower Management Center のその他の機能を使用して、必要なすべてのポリシーと設定を設定してみます。FlexConfig は、FTD との互換性があるが、他の方法では Firepower Management Center で設定できない ASA ベースの機能を設定するための最終手段です。

次に、FlexConfig ポリシーを設定し、導入するためのエンドツーエンドの手順を示します。

ステップ 1 設定する CLI コマンド シーケンスを特定します。

ASA デバイスに機能する設定がある場合は、**show running-config** を使用して必要なコマンドのシーケンスを取得します。必要に応じてインターフェイス名、IP アドレスなどの項目を調整します。

新しい機能の場合は、ラボの設定でASAデバイスに実装して、コマンドシーケンスが適切であることを確認することをお勧めします。

詳細は、次のトピックを参照してください。

- FlexConfig ポリシーの推奨される使用法 （1202 ページ）
- FlexConfig オブジェクトの CLI コマンド （1203 ページ）

ステップ 2 **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** を選択し、コンテンツ テーブルから **[FlexConfig]** > **[FlexConfig オブジェクト（FlexConfig Object）]** を選択します。

事前定義済みFlexConfigオブジェクトを確認して、必要なコマンドを生成できるかどうかを判断します。

表示アイコン（  ）をクリックして、オブジェクトの内容を表示します。既存のオブジェクトが必要なオブジェクトに近い場合は、最初にオブジェクトをコピーして、そのコピーを編集します。定義済みの FlexConfig オブジェクト （1215 ページ）を参照してください。

また、オブジェクトの確認によって、FlexConfig オブジェクトの構造、コマンド構文、および予測されるシーケンシングを把握できます。

（注） 使用するオブジェクトを見つけた場合は、オブジェクトの下の [変数（Variables）] リストを直接またはコピーして確認します。SYS で始まるすべて大文字の変数名（システム変数）を除くすべての変数名を記録します。これらの変数は、特にデフォルト値のカラムでオブジェクトに値がないことが示されている場合に、編集またはオーバーライドの定義が必要になる可能性があるテキスト オブジェクトです。

ステップ 3 独自の FlexConfig オブジェクトを作成する必要がある場合は、必要な変数を特定し、関連オブジェクトを作成します。

導入する必要がある CLI には、時間の経過とともに調整する必要がある IP アドレス、インターフェイス名、ポート番号、およびその他のパラメータが含まれている場合があります。これらは、必要な値が含まれているオブジェクトを指す変数に隔離することをお勧めします。また、設定の一部であるが、時間の経過とともに変化する可能性がある文字列の変数が必要な場合があります。

さらに、ポリシーを割り当てる各デバイスに異なる値が必要かどうかを特定します。たとえば、3つのデバイスの機能を設定し、これらのデバイスそれぞれに指定されたコマンドで異なるインターフェイス名またはIP アドレスの指定が必要になる場合があります。各デバイスのオブジェクトをカスタマイズする必要がある場合は、オブジェクトを作成するときにオーバーライドを有効にして、デバイスごとのオーバーライド値を定義します。

変数のさまざまなタイプおよび必要に応じた関連オブジェクトの設定方法については、次のトピックを参照してください。

- FlexConfig 変数 （1207 ページ）
- FlexConfig ポリシー オブジェクト変数 （1212 ページ）
- FlexConfig システム変数 （1214 ページ）
- FlexConfig テキスト オブジェクトの設定 （1234 ページ）

ステップ 4 事前定義済み FlexConfig オブジェクトを使用する場合は、変数として使用されるテキスト オブジェクトを編集します。

FlexConfig テキスト オブジェクトの設定 （1234 ページ）を参照してください。

ステップ 5 （必要な場合）FlexConfig オブジェクトの設定 （1229 ページ）。

事前定義済みオブジェクトが機能しない場合にのみ、オブジェクトを作成する必要があります。

ステップ 6 FlexConfig ポリシーの設定 （1236 ページ）。

ステップ 7 FlexConfig ポリシーのターゲット デバイスの設定 （1237 ページ）。

ポリシーを作成するときに、デバイスにポリシーを割り当てることもできます。ポリシーをプレビューするには、そのポリシーに 1 つ以上のデバイスが割り当てられている必要があります。

ステップ 8 FlexConfig ポリシーのプレビュー （1238 ページ）。

ポリシーをプレビューする前に変更を保存する必要があります。

生成されたコマンドが目的のものであること、およびすべての変数が正しく解決されていることを確認します。

ステップ 9 メニュー バーで [展開（Deploy）] をクリックし、ポリシーに割り当てられているデバイスを選択して、[展開（Deploy）] ボタンをクリックします。

展開が完了するまで待機します。

ステップ 10 展開された構成の確認 （1239 ページ）。

ステップ 11 （必要な場合）FlexConfig を使用した設定済み機能の削除 （1241 ページ）。

他のタイプのポリシーとは異なり、単にデバイスから FlexConfig を割り当て解除しても関連設定は削除されません。FlexConfig で生成された設定を削除するには、指示された手順に従う必要があります。

FlexConfig オブジェクトの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	Firepower Threat Defense Firepower Threat Defense Virtual	いずれか（Any）	Admin

FlexConfig オブジェクトを使用して、デバイスに展開する設定を定義します。各 FlexConfig ポリシーは、FlexConfigオブジェクトのリストで構成されるため、オブジェクトは基本的にApache Velocity スクリプト コマンド、ASA ソフトウェア コンフィギュレーション コマンド、および変数で構成されるコード モジュールです。

直接使用できる事前定義済みのFlexConfigオブジェクトがいくつかあります。これらを編集する必要がある場合は、コピーすることができます。また、独自のオブジェクトをはじめから作成することもできます。FlexConfig オブジェクトの内容の範囲は、単一の簡単なコマンド文字列から、変数およびスクリプトコマンドを使用してデバイスまたは展開ごとに内容が異なるコマンドを展開する複雑な CLI コマンド構造におよびます。

また、FlexConfig ポリシーを定義するときに、FlexConfig ポリシー オブジェクトを作成できます。

始める前に

次の点を考慮してください。

- FlexConfig オブジェクトはデバイスに展開されるコマンドに変換されます。これらのコマンドは、グローバル コンフィギュレーション モードですでに発行されています。したがって **enable** コマンドと **configure terminal** コマンドを FlexConfig オブジェクトの一部として含めないでください。
- 必要な変数のタイプを特定し、必要なポリシー オブジェクトを作成します。FlexConfigオブジェクトの編集時に変数のオブジェクトを作成することはできません。
- コマンドがデバイスの VPN またはアクセス コントロール設定とまったく競合していないことを確認します。
- インターフェイスのコマンド セットが複数ある場合は、最後のコマンド セットだけが展開されます。したがって、開始コマンドと終了コマンドを使用してインターフェイスを設定しないことを推奨します。インターフェイスを設定する例として、事前定義済み FlexConfig オブジェクトの ISIS_Interface_Configuration を参照してください。

ステップ 1 **[Objects]** > **[Object Management]**を選択します。

ステップ 2 オブジェクト タイプのリストから **[FlexConfig]** > **[FlexConfig オブジェクト（FlexConfig Object）]** を選択します。

ステップ 3 次のいずれかを実行します。

- [FlexConfig オブジェクトの追加（Add FlexConfig Object）] をクリックして、新しいオブジェクトを作成します。
- 編集アイコン（）をクリックして、既存のオブジェクトを編集します。
- 表示アイコン（）をクリックして、事前定義済みオブジェクトの内容を表示します。
- 事前定義済みオブジェクトを編集するには、コピーアイコン（）をクリックして、同じ内容の新しいオブジェクトを作成します。

ステップ 4 **名前**を入力し、オプションでオブジェクトの説明を入力します。

ステップ 5 オブジェクト本体領域に、必要な設定を生成するためのコマンドと命令を入力します。

オブジェクトの内容は、有効な ASA ソフトウェアのコマンド シーケンスを生成する一連のスクリプト コマンドおよびコンフィギュレーション コマンドです。FTD デバイスでは、ASA ソフトウェア コマンドを使用して一部の機能を設定します。スクリプトコマンドおよびコンフィギュレーションコマンドの詳細については、次を参照してください。

- テンプレート スクリプト （1206 ページ）
- FlexConfig オブジェクトの CLI コマンド （1203 ページ）

変数を使用して、ランタイムにのみ通知される情報やデバイスごとに異なる情報を指定できます。プロセス変数に入力しますが、[挿入（Insert）] メニューを使用して、ポリシーオブジェクトまたはシステム変数に関連付けられているか、秘密キーである変数を追加する必要があります。変数の詳細については、FlexConfig 変数 （1207 ページ）を参照してください。

- システム変数を挿入するには、**[挿入（Insert）] > [システム変数の挿入（Insert System Variable）] > [変数名]** を選択します。これらの変数の詳細については、FlexConfig システム変数（1214 ページ）を参照してください。
- ポリシーオブジェクトの変数を挿入するには、**[挿入（Insert）] > [ポリシーオブジェクトの挿入（Insert Policy Object）] > [オブジェクト タイプ]** を選択し、適切なオブジェクトのタイプを選択します。次に、変数に名前を付け（関連付けられたポリシー オブジェクトと同じ名前にすることができます）、変数に関連付けるオブジェクトを選択し、[保存（Save）] をクリックします。これらのタイプの詳細については、FlexConfig ポリシー オブジェクト変数 （1212 ページ）を参照してください。手順の詳細については、FlexConfig オブジェクトへのポリシーオブジェクト変数の追加 （1232 ページ）を参照してください。
- 秘密キーの変数を挿入するには、**[挿入（Insert）] > [秘密キー（Secret Key）]** を選択し、変数名と値を定義します。手順の詳細については、秘密キーの設定 （1233 ページ）を参照してください。

（注） [挿入（Insert）]メニューを使用して、新しいポリシーオブジェクトまたはシステム変数を作成する必要があります。ただし、その変数を後で使用するために、$ を含めて入力する必要があります。これは、システム変数にも当てはまります。システム変数を初めて使用する場合は、[挿入（Insert）]メニューから追加します。次に、後で使用するために入力します。1 つのシステム変数に [挿入（Insert）] メニューを複数回使用すると、システム変数が [変数（Variables）] リストに複数回追加され、FlexConfig が有効ではなくなるため、変更を保存できなくなります。プロセス変数（ポリシーオブジェクトやシステム変数に関連付けられていない）の場合は、変数を入力します。秘密キーを追加する場合は、常に[挿入（Insert）]メニューを使用します。秘密キーの変数は [変数（Variables）] リストに表示されません。

ステップ 6 展開の頻度およびタイプを選択します。

- [展開（Deployment）]：オブジェクトにコマンドを [1 回（Once）] または [毎回（Everytime）] 展開することを指定します。適切なオプションを選択する唯一の方法は、展開の結果をテストする方法です。

  最初に [毎回（Everytime）] を選択します。次に、FlexConfig ポリシーにオブジェクトをアタッチして、設定を展開します。展開に成功したら、FlexConfig ポリシーに戻り、FlexConfig ポリシーのプレビュー（1238 ページ）の説明に従って、割り当てられたいずれかのデバイスの設定をプレビューします。`###CLI generated from managed features ###` のラベルが付いたセクションに、オブジェクト内のコマンドの clear または negate コマンドが含まれていて、`###Flex-config Appended CLI ###` セクションに機能を再設定するためのコマンドが含まれている場合、[毎回（Everytime）] が適切なオプションであることがわかります。

  negate コマンドが表示されていない場合でも、デバイス設定に少し変更を加えて、別の展開を実行します。展開が正常に完了したら、展開トランスクリプトを確認できます（展開された構成の確認（1239 ページ）を参照）。（コマンドがすでに設定されている場合でも）コマンドがエラーなく再発行されているのを確認できたら、[毎回（Everytime）] のままにします。

  システムがオブジェクト内のコマンドを最初に取り消してから再発行しない場合、または展開の結果に、コマンドに固有のエラーがある場合にのみ [1 回（Once）] に変更します。場合によっては、設定済みのコマンドの発行を許可されないことがありますが、それは例外的です。

  追加のヒント：

  - FlexConfig オブジェクトが、ネットワーク オブジェクトや ACL オブジェクトなどのシステム管理対象オブジェクトを指している場合は、[毎回（Everytime）] を選択します。そうしないと、オブジェクトに対する更新が展開されない可能性があります。
  - オブジェクトで行う操作が設定のクリアだけの場合は、[1 回（Once）] を使用します。そして、次の展開後に FlexConfig ポリシーからオブジェクトを削除します。

- [タイプ（Type）]：次のいずれかを選択します。
  - [後に付加（Append）]：（デフォルト）。オブジェクトのコマンドは、Firepower Management Center ポリシーから生成された設定の最後に配置されます。管理対象オブジェクトから生成されたオブジェクトを指すポリシー オブジェクトの変数を使用する場合は、[後に付加（Append）] を使用する必要があります。その他のポリシー向けに生成されたコマンドがオブジェクトで指定されているものと重複する場合は、このオプションを選択してコマンドが上書きされないようにする必要があります。これは最も安全なオプションです。

- [前に付加（Prepend）]：オブジェクトのコマンドは、Firepower Management Center ポリシーから生成された設定の最初に配置されます。通常、設定をクリアまたは除外するコマンドに [前に付加（Prepend）] を使用します。

ステップ 7 （オプション）オブジェクト本体の上にある [検証（Validate）] アイコンをクリックして、スクリプトの整合性を確認します。

[保存（Save）] をクリックするたびに、オブジェクトが検証されます。無効なオブジェクトを保存することはできません。

ステップ 8 **[保存（Save）]** をクリックします。

次のタスク

- アクティブ ポリシーがオブジェクトを参照する場合は、設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

FlexConfig オブジェクトへのポリシーオブジェクト変数の追加

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	Firepower Threat Defense Firepower Threat Defense Virtual	いずれか（Any）	Admin

FlexConfig ポリシー オブジェクトに、ポリシー オブジェクトの他のタイプと関連付けられた変数を挿入できます。FlexConfig をデバイスに展開すると、これらの変数は関連づけられたオブジェクトの名前やコンテンツに合わせて変換されます。

FlexConfig オブジェクトで初めてポリシー オブジェクト変数を使うときは、次の手順に従ってください。オブジェクトを再度参照する必要が生じたら、（$マークを含めて）変数を入力します。変数の使用方法を理解するには、変数の処理方法（1208 ページ）を参照してください。

ステップ 1 **[挿入（Insert）] > [ポリシー オブジェクトの挿入（Insert Policy Object）] > [オブジェクトのタイプ（*Object Type*）]** から、適切なタイプのオブジェクトを選択します。

ステップ 2 変数の名前を入力し、任意で説明を入力します。

名前は、FlexConfig オブジェクトのコンテキストの中で一意なものである必要があります。スペースを含めることはできません。変数に関連付けるオブジェクトと同一の名前を使用できます。

ステップ 3 変数と関連付けるオブジェクトを選択し、[追加（Add）] をクリックしてこれを [選択済みオブジェクト（Selected Object）] リストに移動します。

変数には、1 つのみのオブジェクトを関連付けることができます。

（注） テキストオブジェクトには、必要に応じて前もって定義されたオブジェクトを選択できます。しかし、これらオブジェクトの多くにはデフォルト値はありません。オブジェクトの更新では、必須の値を直接与えるか、ないしは FlexConfig オブジェクトを展開するデバイスのオーバーライドとして与える必要があります。これらのオブジェクトを更新せずに FlexConfig の展開を試行しても、多くの場合展開のエラーにつながります。

ステップ 4 [保存（Save）] をクリックします。

変数は、FlexConfig オブジェクトエディタの下の変数リストに表示されます。

秘密キーの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	Firepower Threat Defense Firepower Threat Defense Virtual	いずれか（Any）	Admin

秘密キーは、パスワードなどの、内容をマスクする単一文字列の変数です。機密情報の拡散を防ぐため、これらの変数にはシステムによって特別な処理が行われます。

秘密キー変数は FlexConfig オブジェクトの変数リストに表示されません。

FlexConfig オブジェクトで秘密キー変数を作成、挿入、および管理するには、次の手順を使用します。他のタイプ変数とは異なり、所定の秘密キー変数を挿入する必要があるたびに **Insert** コマンドを使用できます。処理については、これらの変数は単一値のテキストオブジェクト変数と同様に機能します。単一値変数 （1208 ページ）を参照してください。

（注） 秘密キー変数で定義されたデータは、FlexConfig ポリシーのプレビュー時を除き、ユーザからマスクされます。また、FlexConfig ポリシーをエクスポートする場合、すべての秘密キー変数の内容が消去されます。ポリシーをインポートする場合、各秘密キー変数を手動で編集してデータを入力する必要があります。

ステップ 1 FlexConfig ポリシー オブジェクトを編集する際には、**[挿入（Insert）]** > **[秘密キー（Secret Key）]** を選択します。

ステップ 2 [秘密キーの挿入（Insert Secret Key）] ダイアログボックスで、次のいずれかの手順を実行します。

- 新しいキーを作成するには、[秘密キーの追加（Add Secret Key）] をクリックし、次の情報を入力して [追加（Add）] をクリックします。
  - [秘密キー名（Secret Key Name）]：変数の名前。この名前は、前に @ が付けられて FlexConfig オブジェクトに表示されます。

- [パスワード（Password）]、[パスワードの確認（Confirm Password）]：入力と同時に、アスタリスクでマスクされる秘密の文字列です。

- FlexConfig オブジェクトに秘密キー変数を挿入するには、変数のチェックボックスをオンにします。
- 秘密キー変数の値を編集するには、変数の編集アイコン（  ）をクリックします。変更を加えて、[追加（Add）] をクリックします。
- 秘密キー変数を削除するには、変数の削除アイコン（  ）をクリックします。

ステップ 3 **[保存（Save）]** をクリックします。

FlexConfig テキスト オブジェクトの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	Firepower Threat Defense Firepower Threat Defense Virtual	いずれか（Any）	Admin

ポリシー オブジェクト変数の対象として FlexConfig オブジェクトでテキスト オブジェクトを使用します。変数を使用して、ランタイムにのみ通知される情報やデバイスごとに異なる情報を指定できます。展開中に、テキスト オブジェクトを指す変数はテキスト オブジェクトの内容に置き換えられます。

テキスト オブジェクトには自由形式の文字列が含まれます。キーワード、インターフェイス名、番号、IP アドレスなどにすることも可能です。内容は、FlexConfig スクリプト内の情報の使用方法によって異なります。

テキスト オブジェクトを作成または編集する前に、必要な内容を特定します。これにはオブジェクトの処理方法が含まれます。これを決めることで、1 つの文字列オブジェクトまたは複数の文字列オブジェクトのいずれを作成するかを決定するのに役立ちます。次のトピックを参照してください。

- FlexConfig 変数 （1207 ページ）
- 変数の処理方法 （1208 ページ）

ステップ 1 **[Objects]** > **[Object Management]** を選択します。
ステップ 2 オブジェクト タイプのリストから **[FlexConfig]** > **[テキスト オブジェクト（Text Object）]** を選択します。
ステップ 3 次のいずれかを実行します。

- [テキスト オブジェクトの追加（Add Text Object）] をクリックして、新しいオブジェクトを作成します。
- 編集アイコン（  ）をクリックして、既存のオブジェクトを編集します。事前定義済み FlexConfig オブジェクトを使用する場合に必要となる、事前定義済みテキスト オブジェクトを編集できます。

ステップ 4 **名前**を入力し、オプションでオブジェクトの説明を入力します。

ステップ 5 （新しいオブジェクトのみ）ドロップダウン リストから**変数タイプ**を選択します。

- [単一（Single）]：オブジェクトに単一のテキスト文字列を含める必要がある場合。
- [複数（Multiple）]：オブジェクトにテキスト文字列のリストを含める必要がある場合。

オブジェクトの保存後は変数タイプを変更できません。

ステップ 6 変数タイプが [複数（Multiple）] の場合は、上下矢印を使用して [カウント（Count）] を指定します。

数を変更すると、オブジェクトの行が追加されたり、削除されたりします。

ステップ 7 オブジェクトに内容を追加します。

変数番号の横のテキスト ボックスをクリックして値を入力するか、テキスト オブジェクトを使用する FlexConfig オブジェクトを割り当てられる各デバイスに対してデバイスの上書きを設定できます。両方行うこともできますが、この場合、ベース オブジェクトで設定した値は、指定したデバイスの上書きが存在しない場合にデフォルト値として機能します。

事前定義済みオブジェクトの編集時には、デバイスの上書きを使用することをお勧めします。これは、別の FlexConfig ポリシーでオブジェクトを使用する必要がある他のユーザ用に、デフォルトが残るようにするためです。実行するアプローチは、組織の要件に応じて異なります。

ヒント 一部の事前定義済みオブジェクトには、各値が特定の目的を提供する複数の値が必要です。オブジェクトの予測される値を特定するために、説明テキストを注意深く読みます。手順では、base 値を変更する代わりに上書きを使用する必要があることが指定される場合があります。enableInspectProtocolList の場合は、インスペクションに Snort インスペクションとの互換性がないプロトコルを入力できません。

デバイスの上書きを使用する場合は、次の手順を実行します。

a) [オーバーライドを許可（Allow Overrides）] を選択します。
b) [オーバーライド（Overrides）] を展開し（必要な場合）、[追加（Add）] をクリックします。

上書きがデバイスにすでにある場合は、上書きの編集アイコンをクリックして変更します。

c) [オブジェクトのオーバーライドの追加（Add Object Override）] ダイアログボックスの [ターゲット（Targets）] タブで、値を定義するデバイスを選択し、[追加（Add）] をクリックして [選択されたデバイス（Selected Devices）] リストに移動します。
d) [オーバーライド（Overrides）] タブをクリックし、必要に応じて [カウント（Count）] を調整し、変数フィールドをクリックして、デバイスの値を入力します。
e) [Add] をクリックします。

ステップ 8 **[保存（Save）]** をクリックします。

次のタスク

- アクティブ ポリシーがオブジェクトを参照する場合は、設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

FlexConfig ポリシーの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	Firepower Threat Defense Firepower Threat Defense Virtual	いずれか（Any）	Admin

FlexConfig ポリシーには、FlexConfig オブジェクトの 2 つの順序のリストが含まれています。1 つは先頭に追加されたリスト、もう 1 つは末尾に追加されたリストです。先頭に追加/末尾に追加の説明については、FlexConfig オブジェクトの設定 （1229 ページ）を参照してください。

FlexConfig ポリシーは、複数のデバイスに割り当てることができる共有ポリシーです。

ステップ 1 **[Devices]** > **[FlexConfig]** を選択します。

ステップ 2 次のいずれかを実行します。

- [新しいポリシー（New Policy）] をクリックして、新しい FlexConfig ポリシーを作成します。名前を入力するプロンプトが表示されます。必要に応じて、[使用可能なデバイス（Available Devices）] リストでデバイスを選択し、[ポリシーに追加（Add to Policy）] をクリックしてデバイスを割り当てます。[保存（Save）] をクリックします。
- 編集アイコン（  ）をクリックして、既存のポリシーを編集します。名前や説明を編集モードでクリックして変更できます。
- コピーアイコン（  ）をクリックして、同じ内容の新しいポリシーを作成します。名前を入力するプロンプトが表示されます。デバイス割り当てはコピーに保持されません。
- 削除アイコンをクリックして、不要になったポリシーを削除します。

ステップ 3 ポリシーに必要な FlexConfig オブジェクトを [使用可能な FlexConfig（Available FlexConfig）] リストから選択し、[>] をクリックしてポリシーに追加します。

オブジェクトは FlexConfig オブジェクトで指定した展開タイプに基づいて、先頭に追加されたリストまたは末尾に追加されたリストに自動的に追加されます。

選択したオブジェクトを削除するには、オブジェクトの横にある削除アイコン（）をクリックします。

ステップ 4 選択したオブジェクトごとに、オブジェクトの横にある表示アイコン（）をクリックして、オブジェクトで使用されている変数を特定します。

SYS で始まるシステム変数を除き、変数に関連付けられているオブジェクトが空でないことを確認する必要があります。空白または間に何もない角カッコは、空のオブジェクトを示します。ポリシーを展開する前に、これらのオブジェクトを編集する必要があります。

（注） オブジェクトのオーバーライドを使用する場合、これらの値はこのビューに表示されません。したがって、空のデフォルト値は、必ずしもオブジェクトが必要な値で更新されていないことを意味するわけではありません。設定をプレビューすると、変数が所定のデバイスに対して正しく解決されるかどうかが示されます。FlexConfig ポリシーのプレビュー （1238 ページ）を参照してください。

ステップ 5 [保存（Save）] をクリックします。

次のタスク

- ポリシーのターゲット デバイスを設定します。FlexConfig ポリシーのターゲット デバイスの設定 （1237 ページ）を参照してください。
- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

FlexConfig ポリシーのターゲット デバイスの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	Firepower Threat Defense Firepower Threat Defense Virtual	いずれか（Any）	Admin

FlexConfig ポリシーを作成するときに、ポリシーを使用するデバイスを選択できます。その後、次の説明に従って、ポリシーに対するデバイスの割り当てを変更できます。

（注） 通常、デバイスからポリシーの割り当てを解除すると、次回の展開時に、システムは関連付けられた設定を自動的に削除します。ただし、FlexConfig オブジェクトはカスタマイズされたコマンドを展開するためのスクリプトであるため、単にデバイスから FlexConfig ポリシーの割り当てを解除しても、FlexConfig オブジェクトによって設定されたコマンドは削除されません。FlexConfig によって生成されたコマンドをデバイスの構成から削除することが目的の場合は、FlexConfig を使用した設定済み機能の削除 （1241 ページ）を参照してください。

ステップ 1 **[デバイス（Devices）]** > **[FlexConfig]** を選択して、FlexConfig ポリシーを編集します。

ステップ 2 [ポリシーの割り当て（Policy Assignments）] をクリックします。

ステップ 3 [ターゲット デバイス（Targeted Devices）] タブで、ターゲット リストを作成します。

- 追加：1 つ以上の [使用可能なデバイス（Available Devices）] を選択して、[ポリシーに追加（Add to Policy）] をクリックするか、[選択したデバイス（Selected Devices）] のリストにドラッグ アンド ドロップします。ポリシーは、デバイス、高可用性ペア、およびクラスタを構成するデバイスに割り当てることができます。
- 削除：1つのデバイスの横にある削除アイコン（）をクリックするか、複数のデバイスを選択して、右クリックしてから [選択項目の削除（Delete Selection）] を選択します。

ステップ 4 [OK] をクリックして選択内容を保存します。

ステップ 5 [保存（Save）] をクリックして、FlexConfig ポリシーを保存します。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

FlexConfig ポリシーのプレビュー

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	Firepower Threat Defense Firepower Threat Defense Virtual	いずれか（Any）	Admin

FlexConfig ポリシーをプレビューして、FlexConfig オブジェクトが、どのように CLI コマンドに変換されるかを確認します。プレビューには、FlexConfig オブジェクトで使用されるスクリプトおよび変数から、選択したデバイスに応じて生成されるコマンドが示されます。変数はデバイスの設定に基づいて解決されるため、展開される内容を明確に理解できます。

プレビューを使用すると、FlexConfig オブジェクトの潜在的な問題が見つかります。期待される結果がプレビューに示されるまで、オブジェクトを修正します。

設定は、デバイスごとに個別にプレビューする必要があります。これは、変数がデバイス設定に基づいてさまざまに解決される可能性があるためです。

ステップ 1 **[デバイス（Devices）]** > **[FlexConfig]** を選択して、FlexConfig ポリシーを編集します。

ステップ 2 未確定の変更がある場合は、[保存（Save）] をクリックします。

プレビューには、最後に保存したバージョンのポリシーに含まれる FlexConfig オブジェクトの結果のみが示されます。新しく追加したオブジェクトのプレビューを確認するには、ポリシーを保存する必要があります。

ステップ 3 [設定のプレビュー（Preview Config）] をクリックします。

ステップ 4 [デバイスの選択（Select Device）] ドロップダウンリストからデバイスを選択します。

システムは、デバイスからの情報と設定済みのポリシーを取得して、次回のデバイスへの展開時に生成する CLI コマンドを決定します。出力を選択してから Ctrl + C を押すことで、その出力をクリップボードにコピーできます。この出力は、詳細な分析のためにテキスト ファイルに貼り付けることができます。

プレビューには、次のセクションが含まれています。

- Flex-config により前に付加される CLI（Flex-config Prepended CLI）：FlexConfig によって生成されるコマンドであり、設定の前に付加されます。
- 管理対象の機能から生成された CLI（CLI generated from managed features）：Firepower Management Center で設定されたポリシーに応じて生成されるコマンドです。コマンドは、デバイスへの最後の正常な展開後の新規ポリシーまたは変更されたポリシーに対して生成されます。これらのコマンドは、割り当て済みのポリシーを実装するために必要なすべてのコマンドを表しているわけではありません。このセクション内のコマンドは、FlexConfig オブジェクトから生成されたものではありません。
- Flex-config により後に付加される CLI（Flex-config Appended CLI）：FlexConfig によって生成されるコマンドであり、設定の後に付加されます。

ステップ 5 [閉じる（Close）] ボタンをクリックして、プレビュー ダイアログを閉じます。

展開された構成の確認

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	Firepower Threat Defense Firepower Threat Defense Virtual	いずれか（Any）	Admin

デバイスにFlexConfigポリシーを展開した後、展開が成功したこと、およびこの構成が期待どおりのものであることを確認します。また、デバイスが期待どおりに機能していることを確認します。

ステップ 1 展開が成功したことを確認するには、次の手順を実行します。

a) メニュー バーのシステム ステータス アイコンをクリックします。このアイコンは、[展開（Deploy）] と [システム（System）] の間にある、名前のないアイコンです。

アイコンは、次のいずれかで、エラーがあると番号が付くことがあります。

- ：警告またはエラーがシステムにないことを示します。
- ：1 つ以上の警告またはエラーがシステムにあることを示します。
- ：1 つ以上のエラーと任意の数の警告がシステムにあることを示します。

b) [展開（Deployment）] タブで、展開が成功したことを確認します。
c) 詳細な情報、特に失敗した展開の詳細を表示するには、[履歴の表示（Show History）] をクリックします。
d) 左側の列にあるジョブのリストで展開ジョブを選択します。

ジョブは新しい順に表示され、リストの一番上に最新のジョブが表示されます。

e) 右側の列にあるデバイスの [トランスクリプト（Transcript）] 列でダウンロードアイコンをクリックします。

展開トランスクリプトには、デバイスに送信されたコマンドおよびデバイスから返された応答が含まれます。これらの応答は、通知メッセージやエラーメッセージの場合があります。失敗した展開では、FlexConfig から送信したコマンドを含む、エラーを示すメッセージを探します。これらのエラーは、コマンドを設定しようとしている FlexConfig オブジェクトのスクリプトを修正するのに役立つ場合があります。

（注） 管理対象機能に送信されるコマンドと、FlexConfig ポリシーから生成されるコマンドとの間のトランスクリプトには違いはありません。

たとえば、次のシーケンスは、論理名が outside の GigabitEthernet0/0 を設定するコマンドを Firepower Management Center（FMC）が送信したことを示しています。デバイスは、自動的にセキュリティ レベルを 0 に設定したことを応答しました。FTD がセキュリティ レベルを使用することはありません。FlexConfig に関連したメッセージは、トランスクリプトの [CLI 適用（CLI Apply）] セクションにあります。

```
========== CLI APPLY ==========

FMC >> interface GigabitEthernet0/0
FMC >>  nameif outside
FTDv 192.168.0.152 >> [info] : INFO: Security level for "outside" set to 0 by default.
```

ステップ 2 展開された構成に必要なコマンドが含まれていることを確認します。

これは、デバイスの管理 IP アドレスへの SSH 接続を確立することで行うことができます。**show running-config** コマンドを使用して、設定を表示します。

または、Firepower Management Center 内で CLI ツールを使用します。

a) **[システム（System）]** > **[ヘルス（Health）]** > **[モニタ（Monitor）]** を選択し、デバイスの名前をクリックします。

ステータス テーブルの [カウント（Count）] 列で開く/閉じる矢印をクリックしてデバイスを表示することが必要になる場合があります。

b) [詳細なトラブルシューティング（Advanced Troubleshooting）] をクリックします。

c) [脅威防御 CLI（Threat Defense CLI）] タブをクリックします。
d) コマンドとして [show] を選択し、パラメータとして「**running-config**」と入力します。
e) [実行（Execute）] をクリックします。

実行中の構成がテキスト ボックスに表示されます。構成を選択し、Ctrl キーを押した状態で C キーを押して、後で分析できるようにテキスト ファイルに貼り付けることができます。

ステップ 3 デバイスが期待どおりに機能していることを確認します。

機能に関連する **show** コマンドを使用して、詳細情報と統計情報を表示します。たとえば、追加のプロトコル インスペクションを有効にした場合、**show service-policy** コマンドを使用すると、この情報が提供されます。使用する正確なコマンドは機能に依存し、機能の設定方法を学習するときに使用した ASA 構成ガイドおよびコマンド リファレンスに記載されています。

統計情報を表示するコマンドで数（ヒット数、接続数など）が変更されていないことが示された場合、構成は有効であっても意味がないことがあります。トラフィックが、統計情報に表示されるはずのデバイスを通過していることがわかっている場合は、構成に欠如しているものを確認します。たとえば、トラフィックは、機能が適用される前に NAT またはアクセス ルールによってドロップまたは変更される場合があります。

SSH セッションまたは Firepower Management Center CLI ツールから **show** コマンドを使用できます。

ただし、使用する必要がある **show** コマンドを FTD CLI 内で直接使用できない場合は、デバイスへの SSH 接続を確立してコマンドを使用する必要があります。CLI から、次のコマンド シーケンスを入力して、診断 CLI 内で特権 EXEC モードに切り替えます。ここから、これらのサポートされない **show** コマンドを入力できます。

```
> system support diagnostic-cli
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
firepower> enable
Password: <press enter, do not enter a password>
firepower#
```

FlexConfig を使用した設定済み機能の削除

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	Firepower Threat Defense Firepower Threat Defense Virtual	いずれか（Any）	Admin

FlexConfig を使用して設定した一連の設定コマンドの削除が必要な場合は、その設定を手動で削除する必要があります。デバイスから FlexConfig ポリシーの割り当てを解除しても、すべての設定が削除されないことがあります。

手動で設定を削除するには、新しいFlexConfigオブジェクトを作成して、設定コマンドを消去または無効化します。

始める前に

オブジェクトによって生成された設定の一部またはすべてを手動で削除する必要があるかどうかを確認するには、次の手順を実行します。

1. FlexConfigポリシーのプレビュー（1238ページ）の説明に従い、設定のプレビューを調べます。FlexConfigオブジェクト内のすべてのコマンドを削除するためのclearまたはnegateコマンドが`###CLI generated from managed features ###`セクションに含まれている場合は、FlexConfigポリシーから単純にオブジェクトを削除し、保存して再展開できます。
2. FlexConfigポリシーからオブジェクトを削除し、変更を保存して、もう一度設定をプレビューします。`###CLI generated from managed features ###`セクションにまだ必要なclearまたはnegateコマンドが含まれていない場合は、次の手順を実行して、手動で設定を削除する必要があります。

ステップ1 **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** を選択して、FlexConfigオブジェクトを作成することで、設定コマンドを消去または取り消します。

機能に構成時の設定をすべて削除できる**clear**コマンドがある場合は、そのコマンドを使用します。たとえば、事前定義されているEigrp_Unconfigure_Allオブジェクトには、次に示すように、すべてのEIGRP関連の設定コマンドを削除する1つのコマンドが含まれています。

```
clear configure router eigrp
```

その機能に**clear**コマンドが存在しない場合は、削除する各コマンドの**no**形式を使用する必要があります。たとえば、事前定義されているSysopt_basic_negateオブジェクトは、事前定義されているSysopt_basicオブジェクトで設定したコマンドを削除します。

```
no sysopt traffic detailed-statistics
no sysopt connection timewait
```

通常、設定を削除するFlexConfigオブジェクトを前に追加された、1回のみ展開されるオブジェクトとして設定します。

ステップ2 **[デバイス（Devices）]** > **[FlexConfig]** を選択して、新しいFlexConfigポリシーを作成するか、既存のポリシーを編集します。

設定コマンドを展開するFlexConfigポリシーを保持する場合は、コマンドの取り消し専用の新しいポリシーを作成して、そのポリシーにデバイスを割り当てます。その後で、新しいFlexConfigオブジェクトをポリシーに追加します。

すべてのデバイスから完全にFlexConfig設定オブジェクトを削除する場合は、既存のFlexConfigポリシーから該当するコマンドを削除して、それらのコマンドを設定を取り消すオブジェクトで置き換えます。

ステップ 3 [保存（Save）] をクリックして、FlexConfig ポリシーを保存します。

ステップ 4 [設定のプレビュー（Preview Config）] をクリックして、消去および取り消しコマンドが適切に生成されていることを確認します。

ステップ 5 メニュー バーの [展開（Deploy）] をクリックし、デバイスを選択して [展開（Deploy）] ボタンをクリックします。

展開が完了するまで待機します。

ステップ 6 コマンドが削除されたことを確認します。

デバイスの実行コンフィギュレーションを表示して、コマンドが削除されていることを確認します。詳細については、展開された構成の確認 （1239 ページ）を参照してください。

ステップ 7 FlexConfig ポリシーの編集中に、[ポリシーの割り当て（Policy Assignments）] をクリックして、デバイスを削除します。必要に応じて、ポリシーから FlexConfig オブジェクトを削除します。

FlexConfig ポリシーは単に不要な設定コマンドを削除するものであるため、削除の完了後にデバイスに割り当てたポリシーを保持する必要はありません。

ただし、FlexConfig ポリシーにデバイスで設定する必要のあるオプションが残っている場合は、そのポリシーから取り消しオブジェクトを削除します。これらは不要です。

FlexConfig の履歴

機能	バージョン	説明
FlexConfig。	6.2	FlexConfig 機能では、Firepower Management Center を使用して ASA CLI テンプレートベースの機能を Firepower Threat Defense デバイスに展開できます。この機能を使用すると、Firepower Threat Defense で現在使用できない最も重要な ASA 機能の一部を有効にすることができます。この機能は、ポリシー内で連携するテンプレートとオブジェクトとして構造化されています。デフォルトのテンプレートは Cisco TAC で公式にサポートされています。 新規画面：**[デバイス（Devices）]** > **[FlexConfig]**。また、**[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** の下の **[FlexConfig]** > **[FlexConfigオブジェクト（FlexConfig Objects）]** および **[FlexConfig]** > **[テストオブジェクト（Text Object）]**。 サポートされているプラットフォーム： Firepower Threat Defense

機能	バージョン	説明
FlexConfig の更新	6.2(1) 6.2(2)	政府による認定要件に従って、パスワード、システム提供またはユーザ定義の FlexConfig オブジェクトの共有キーなどの機密情報はすべて、秘密キー変数を使用してマスクする必要があります。Firepower Management Center をこれらのリリースに更新すると、Flexconfig オブジェクト内のすべての機密情報が秘密キーの変数形式に変換されます。 さらに、次の新しい FlexConfig テンプレートが追加されます。 • **Default_DNS_Configure** テンプレートでは、デフォルトの DNS グループを使用できます。これはデータインターフェイスを介して名前を解決するコマンドまたは機能のホスト名を解決するために使用されます。 • **TCP 初期接続制限およびタイムアウト設定**テンプレートでは、SYN フラッド DoS 攻撃から保護するように初期接続制限/タイムアウト CLI を設定できます。 • **脅威検出の設定およびクリア**テンプレートでは、TCP 代行受信によって傍受された攻撃の脅威検出統計情報を設定できます。 • **IPV6 ルータ ヘッダーの検査**テンプレートでは、さまざまなタイプの特定のヘッダーを選択的に許可またはブロックするように IPV6 検査ヘッダーを設定できます（RH タイプ 2、モバイルの許可など）。 • **DHCPv6 プレフィックス委任**テンプレートでは、IPv6 プレフィックス委任に対して 1 つの外部インターフェイス（プレフィックス委任クライアント）と 1 つの内部インターフェイス（委任されたプレフィックスの受信者）を設定します。 サポートされているプラットフォーム： Firepower Threat Defense

機能	バージョン	説明
委任された FlexConfig オブジェクト。	6.3	FlexConfig を使用して設定した以前のリリースの一部の機能が、Firepower Management Center で直接サポートされるようになりました。この FlexConfig オブジェクトを使用している場合は削除し、新しいオブジェクトを使用するように設定を変換する必要があります。次に、非推奨の FlexConfig オブジェクトおよびテキスト オブジェクトを示します。 • defaultDNSNameServerList および defaultDNSParameters テキスト オブジェクトを含む **Default_DNS_Configure**。プラットフォーム設定ポリシーで、データ インターフェイスの DNS を設定してください。 • **TCP_Embryonic_Conn_Limit**、tcp_conn_misc and tcp_conn_limit テキスト オブジェクト。これらの機能は、Firepower Threat Defense サービス ポリシーで設定します。ポリシーは、デバイスに割り当てられているアクセス制御ポリシーの [詳細設定（Advanced）] タブで確認できます。 • **TCP_Embryonic_Conn_Timeout**、tcp_conn_misc および tcp_conn_timeout テキスト オブジェクト。Firepower Threat Defense サービス ポリシーでこれらの機能を設定します。 サポートされているプラットフォーム： Firepower Threat Defense

第 XIII 部

アプライアンス プラットフォームの設定

第 49 章

システム設定

以下のトピックでは、Firepower Management Center および管理対象デバイスでシステム設定を行う方法について説明します。

• システム設定の履歴 （1327 ページ）

システムの設定について

システム設定の設定値は、Firepower Management Center またはクラシック管理対象デバイス（7000 および 8000 シリーズ、ASA FirePOWER、NGIPSv）のいずれかに適用されます。

- Firepower Management Center では、これらの構成設定は「ローカル」のシステム設定の一部です。Firepower Management Center 上のシステム設定は単一システムに固有のものであり、FMC のシステム設定への変更はそのシステムのみに影響する点に注意してください。
- クラシック管理対象デバイスでは、プラットフォーム設定ポリシーの一部として Firepower Management Center から設定を適用します。共有ポリシーを作成して、展開全体で同様の設定になっている可能性の高い、管理対象デバイスに最適なシステム設定の設定値のサブセットを設定します。

ヒント 7000 および 8000 シリーズ デバイスでは、ローカル Web インターフェイスからコンソール設定やリモート管理などのシステム設定の制限付きタスクを実行できます。これらは、プラットフォーム設定ポリシーを使用して 7000 または 8000 シリーズ デバイスに適用される設定とは異なります。

Firepower Management Center システム設定のナビゲーション

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	FMC	グローバルだけ。	Admin

システム設定により、Firepower Management Center の基本設定を特定します。

ステップ 1 **[System]** > **[Configuration]**を選択します。

ステップ 2 ナビゲーション ウィンドウを使用して、変更する設定を選択します。詳細については、表 88 : システム設定 （1251 ページ）を参照してください。

システム設定

管理対象デバイスの場合、これらの設定の多くは、FMC から適用されるプラットフォーム設定ポリシーによって処理されることに注意してください。プラットフォーム設定ポリシー （1331 ページ）を参照してください。7000/8000 シリーズ デバイスの場合は、ローカル Web イン

ターフェイスにログインして、非ポリシー ベースのシステム設定を行うこともできます。7000/8000 シリーズ デバイスのローカル システム設定 （1347 ページ）を参照してください。

表 *88* : システム設定

設定	説明
アクセス コントロールの設定	ユーザがアクセス コントロール ポリシーを追加または変更する際にユーザにコメントを要求するようにシステムを設定します。ポリシー変更のコメント （1289ページ）を参照してください。
アクセス リスト	どのコンピュータが特定のポートでシステムにアクセスできるかを制御します。アクセス リスト （1291 ページ）を参照してください。
監査ログ	外部ホストに監査ログを送信するようにシステムを設定します。監査ログ （1292ページ）を参照してください。
監査ログ証明書	監査ログを外部ホストにストリーミングする際にチャネルを保護するようにシステムを設定します。監査ログ証明書 （1295 ページ）を参照してください。
リコンサイルの変更	過去 24 時間にわたるシステムへの変更の詳細なレポートを送信するようにシステムを設定します。変更調整 （1288 ページ）を参照してください。
コンソール設定	VGA またはシリアル ポート経由、または Lights-Out Management（LOM）経由のコンソール アクセスを設定します。リモート コンソールのアクセス管理 （1317ページ）を参照してください。 FMC CLI を有効または無効にします。Firepower Management Center のコマンド ライン リファレンス （3363 ページ）を参照してください。
ダッシュボード	ダッシュボードのカスタム分析ウィジェットを有効にします。ダッシュボード設定 （1301ページ）を参照してください。
データベース	Firepower Management Center が保存できる各イベントのタイプの最大数を指定します。データベース イベント数の制限 （1264 ページ）を参照してください。
DNS キャッシュ	イベント表示ページで IP アドレスを自動的に解決するようにシステムを設定します。DNS キャッシュ （1302 ページ）を参照してください。
電子メール通知	メール ホストを設定し、暗号化方式を選択して、電子メールベースの通知とレポートに認証クレデンシャルを提供します。電子メールの通知 （1303 ページ）を参照してください。
外部データベース アクセス	データベースへの外部読み取り専用アクセスを有効にし、ダウンロードするクライアント ドライバを提供します。外部データベース アクセスの設定 （1262ページ）を参照してください。
HTTPS Certificate	必要に応じて、信頼できる認証局の HTTPS サーバ証明書を要求し、システムに証明書をアップロードします。HTTPS 証明書 （1254 ページ）を参照してください。
情報	アプライアンスに関する最新情報を表示し、表示名を編集します。アプライアンス情報（Appliance Information） （1253 ページ）を参照してください。

設定	説明
侵入ポリシーの設定	ユーザが侵入ポリシーを変更する際にユーザにコメントを要求するようにシステムを設定します。ポリシー変更のコメント （1289 ページ）を参照してください。
[言語（Language）]	Webインターフェイスに異なる言語を指定します。言語の選択 （1304ページ）を参照してください。
ログイン バナー	ユーザがログインすると表示されるカスタム ログイン バナーを作成します。ログイン バナー （1305 ページ）を参照してください。
管理インターフェイス	アプライアンスの IP アドレス、ホスト名、プロキシ設定などのオプションを変更します。管理インターフェイス （1266 ページ）を参照してください。
ネットワーク分析ポリシーの設定	ユーザがネットワーク分析ポリシーを変更する際にユーザにコメントを要求するようにシステムを設定します。ポリシー変更のコメント （1289 ページ）を参照してください。
プロセス	Firepower のプロセスをシャットダウン、リブート、または再起動します。シャットダウンまたは再起動 （1282 ページ）を参照してください。
リモート ストレージ デバイス	バックアップとレポート用のリモート ストレージ デバイスを設定します。リモート ストレージ管理 （1283 ページ）を参照してください。
REST API 設定	Firepower REST API 経由の Firepower Management Center へのアクセスを有効または無効にします。REST API 設定 （1324 ページ）を参照してください。
シェル タイムアウト	ユーザのログイン セッションが非アクティブによりタイムアウトするまでのアイドル時間の長さを分単位で設定します。セッション タイムアウト （1315ページ）を参照してください。
SNMP	Simple Network Management Protocol （SNMP）のポーリングを有効にします。SNMP ポーリング （1305 ページ）を参照してください。
時刻（Time）	現在の時刻設定を表示および変更します。時刻および時刻同期 （1307ページ）を参照してください。
時刻の同期	システムの時刻の同期を管理します。時刻および時刻同期 （1307 ページ）を参照してください。
UCAPL/CC コンプライアンス	米国国防総省によって設定される特定の要件の順守を有効にします。セキュリティ認定コンプライアンスの有効化 （1417 ページ）を参照してください。
ユーザの設定	Firepower Management Center を設定し、すべてのユーザの正常なログインの履歴とパスワードの履歴を追跡するか、無効なログイン クレデンシャルを入力したユーザに一時的なロックアウトを適用します。グローバル ユーザ構成時の設定 （1312 ページ）を参照してください。
VMware ツール	VMware ツールを有効にして Firepower Management Center Virtual で使用します。VMware Tools と仮想システム （1325 ページ）を参照してください。
脆弱性マッピング	ホストIPアドレスから送受信されるアプリケーションプロトコルトラフィックの脆弱性をそのホストIPアドレスにマップします。脆弱性マッピング （1315ページ）を参照してください。

設定	説明
Web 分析	システムからの個人を特定できない情報の収集を有効または無効にします。（オプション）Web 分析トラッキングのオプトアウト （1326 ページ）を参照してください。

関連トピック

従来型デバイス用のプラットフォーム設定について （1335 ページ）

アプライアンス情報（Appliance Information）

[システム（System）]>[設定（Configuration）]ページには、次の表に示す情報が含まれています。別途記載のない限り、フィールドはすべて読み取り専用です。

（注） 同様の情報が含まれている [ヘルプ（Help）] >[概要（About）] ページも参照してください。

フィールド	説明
Name	アプライアンスに割り当てられた名前。この名前はFirepowerシステムのコンテキスト内でのみ使用されることに注意してください。ホスト名をアプライアンスの名前として使用できますが、このフィールドに別の名前を入力しても、ホスト名が変更されることはありません。
製品モデル（Product Model）	アプライアンスのモデル名。
シリアル番号（Serial Number）	アプライアンスのシリアル番号。
ソフトウェア バージョン（Software Version）	アプライアンスに現在インストールされているソフトウェアのバージョン。
Firepower Management Center へのパケット転送を禁止(Prohibit Packet Transfer to the Defense Center)	管理対象デバイスがイベントに合わせてパケット データを送信し、Firepower Management Center 上にデータを保存するかを指定します。この設定は、7000 および 8000 シリーズ デバイスのローカル Web インターフェイスで使用できます。
Operating System	アプライアンス上で現在実行されているオペレーティング システム。
Operating System Version	アプライアンス上で現在実行されているオペレーティング システムのバージョン。

フィールド	説明
IPv4 Address	デフォルト管理インターフェイス（eth0）の IPv4 アドレス。IPv4 の管理が無効になっている場合は、このフィールドにそのことが示されます。
IPv6 アドレス（IPv6 Address）	デフォルト管理インターフェイス（eth0）の IPv6 アドレス。IPv6 の管理が無効になっている場合は、このフィールドに表示されます。
現在のポリシー（Current Policies）	現在展開されているシステム レベルのポリシー。ポリシーが最後に適用された後で更新されていると、ポリシー名がイタリック体で表示されます。
モデル番号（Model Number）	内部フラッシュ ドライブに保存されているアプライアンス固有のモデル番号。この番号は、トラブルシューティングで重要になる場合があります。

HTTPS 証明書

Firepower Management Center および 7000 および 8000 シリーズ デバイスは、セキュア ソケット レイヤ（SSL）/TLS 証明書によりシステムと Web ブラウザ間に暗号化チャネルを確立することができます。すべての Firepower デバイスにデフォルト証明書が含まれていますが、これはグローバル レベルで既知の CA から信頼された認証局（CA）によって生成された証明書ではありません。したがって、デフォルト証明書ではなく、グローバル レベルで既知の CA または内部で信頼された CA 署名付きのカスタム証明書の使用を検討してください。

注意 FMC は 4096 ビット HTTPS 証明書をサポートしています。FMC で使用する証明書が 4096 ビットを超える公開サーバ キーを使用して生成されている場合、FMC Web インターフェイスにログインできません。この問題が発生した場合は、Cisco TACにお問い合わせください。

デフォルト HTTPS サーバ証明書

アプライアンスに提供されるデフォルトサーバ証明書を使用する場合、Web インターフェイスのアクセスに有効な HTTPS クライアント証明書が必要になるようにシステムを設定しないでください。これは、デフォルトサーバ証明書が、クライアント証明書に署名する CA によって署名されないためです。

アプライアンスに提供されるデフォルトサーバ証明書は、3 年後に自動的に期限切れとなります。バージョン 6.3 にアップグレードされる前に生成されたデフォルト証明書をアプライアンスが使用している場合、証明書は最初に生成されたときから 20 年後に期限切れとなります。

Firepower Management Center デバイスと 7000 および 8000 シリーズ デバイスで、**[System]** > **[Configuration]** > [HTTPS証明書（HTTPS Certificate）] ページでデフォルトの証明書を更新します。7000 および 8000 シリーズ デバイスで、CLI コマンド `system renew-http-cert` を使用してデフォルトの証明書も更新できます。

カスタム HTTPS サーバ証明書

Firepower Management Center Web インターフェイスを使用して、システム情報と指定した ID 情報に基づいて、サーバ証明書要求を生成できます。ブラウザによって信頼されている内部認証局（CA）がインストールされている場合は、この要求を使用して証明書に署名することができます。生成された要求を認証局に送信して、サーバ証明書を要求することもできます。認証局（CA）から署名付き証明書を取得すると、その証明書をインポートできます。

HTTPS サーバ証明書の要件

HTTPS 証明書を使用して web ブラウザと Firepower アプライアンスの web インターフェイス間の接続を保護する場合は、インターネット X.509 公開キー インフラストラクチャ証明書および証明書失効リスト（CRL）プロファイル（RFC 3280）に準拠する証明書を使用する必要があります。サーバ証明書をアプライアンスにインポートする場合、証明書がその標準のバージョン 3（x.509 v3）に準拠していないと、システムによって証明書は拒否されます。

HTTPS サーバ証明書をインポートする前に、次のフィールドが含まれていることを確認してください。

証明書フィールド	説明
バージョン	エンコードされた証明書のバージョン。バージョン 3 を使用します。RFC 3280 の 4.1.2.1 の項を参照してください。
Serial number	発行元 CA によって証明書に割り当てられた正の整数。発行者とシリアル番号を組み合わせて、証明書を一意に識別します。RFC 3280 の 4.1.2.2 の項を参照してください。
シグネチャ	証明書の署名用に CA で使用されるアルゴリズムの識別子。signatureAlgorithm フィールドと一致している必要があります。RFC 3280 の 4.1.2.3 の項を参照してください。
発行元（Issuer）	証明書を署名および発行したエンティティを識別します。RFC 3280 の 4.1.2.4 の項を参照してください。

証明書フィールド	説明
Validity	CA が証明書のステータスに関する情報を維持することを保証する期間。RFC 3280 の 4.1.2.5 の項を参照してください。
Subject	サブジェクトの公開キーフィールドに保存された公開キーに関連付けられているエンティティを識別します。X.500 識別名（DN）を指定する必要があります。RFC 3280 の 4.1.2.6 の項を参照してください。
Subject Public Key Info	公開キーとそのアルゴリズムの識別子。RFC 3280 の 4.1.2.7 の項を参照してください。
認証局キー識別子の拡張	証明書の署名に使用される秘密キーに対応する公開キーを識別する手段を提供します。RFC 3280 の 4.2.1.1 の項を参照してください。
サブジェクト キー識別子の拡張	特定の公開キーが含まれる証明書を識別する手段を提供します。RFC 3280 の 4.2.1.2 の項を参照してください。
キーの用途拡張	証明書に含まれるキーの目的を定義します。RFC 3280 の 4.2.1.3 の項を参照してください。
基本制約拡張	証明書のサブジェクトが CA で、この証明書を含む検証認証パスの最大深さかどうかを識別します。RFC 3280 の 4.2.1.10 の項を参照してください。Firepower アプライアンスで使用されるサーバ証明書の場合は、`critical CA:FALSE` を使用します。
拡張キーの用途拡張	キーの用途拡張で示されている基本的な目的に加えて、認定公開キーを使用する目的を 1 つ以上示します。RFC 3280 の 4.2.1.13 の項を参照してください。サーバ証明書として使用できる証明書をインポートしてください。
signatureAlgorithm	証明書の署名用に CA で使用されるアルゴリズムの識別子。[署名（Signature）] フィールドと一致する必要があります。RFC 3280 の 4.1.1.2 の項を参照してください。
signatureValue	デジタル署名。RFC 3280 の 4.1.1.3 の項を参照してください。

HTTP クライアント証明書

クライアント ブラウザの証明書チェック機能を使用して、Firepower システムの Web サーバへのアクセスを制限できます。ユーザ証明書を有効にすると、Web サーバはユーザのブラウザ クライアントで有効なユーザ証明書が選択されていることを確認します。そのユーザ証明書は、サーバ証明書で使用されているのと同じ信頼できる認証局によって生成されている必要があります。以下の状況ではいずれの場合もブラウザは Web インターフェイスをロードできません。

- ユーザがブラウザに無効な証明書を選択する。
- ユーザがブラウザにサーバ証明書に署名した認証局が生成していない証明書を選択する。
- ユーザがブラウザにデバイスの証明書チェーンの認証局が生成していない証明書を選択する。

クライアントブラウザ証明書を確認するには、システムを設定してオンライン証明書ステータスプロトコル（OCSP）を使用するか、1つ以上の証明書失効リスト（CRL）ファイルをロードします。OCSP を使用する場合、Web サーバは接続要求を受信すると、接続を確立する前に認証局と通信して、クライアント証明書の有効性を確認します。サーバに1つ以上の CRL をロードするよう設定する場合、Web サーバはクライアント証明書を CRL の一覧に照らして比較します。ユーザが CRL にある失効した証明書の一覧に含まれる証明書を選択した場合、ブラウザは Web インターフェイスをロードできません。

（注） CRL を使用した証明書の確認を選択すると、システムはクライアント ブラウザ証明書、監査ログ サーバ証明書の両方の検証に同じ CRL を使用します。

現在の HTTPS サーバ証明書の表示

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	FMC 7000 および 8000 シリーズ	グローバルだけ。	Admin

ログインしているアプライアンスのサーバ証明書のみを表示できます。

ステップ 1 **[System]** > **[Configuration]**を選択します。

ステップ 2 [HTTPS Certificate] をクリックします。

HTTPS サーバの証明書署名要求の作成

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
該当なし	いずれか（Any）	FMC 7000 および 8000 シリーズ	グローバルだけ。	Admin

広く知られている CA または内部的に信頼できる CA によって署名されていない証明書をインストールすると、Webインターフェイスに接続しようとするとブラウザにセキュリティ警告が表示されます。

証明書署名要求（CSR）は生成元のアプライアンスまたはデバイスに対して一意です。1 つのアプライアンスの複数のデバイスに対して CSR を生成することはできません。

証明書要求用に生成されるキーは、ベース 64 エンコードの PEM 形式です。

ステップ 1 **[System]** > **[Configuration]**を選択します。

ステップ 2 [HTTPS Certificate] をクリックします。

ステップ 3 [新規 CSR の生成（Generate New CSR）] をクリックします。

ステップ 4 [国名（2 文字のコード）（Country Name (two-letter code)）] フィールドに国番号を入力します。

ステップ 5 [都道府県（State or Province）] フィールドに、都道府県名を入力します。

ステップ 6 [市区町村（Locality or City）] を入力します。

ステップ 7 [組織（Organization）] の名前を入力します。

ステップ 8 [組織単位（部署名）（Organizational Unit (Department)）] の名前を入力します。

ステップ 9 [共通名（Common Name）] フィールドに、証明書を要求するサーバの完全修飾ドメイン名を入力します。

（注） [共通名（Common Name）] フィールドには、証明書に表示されるとおりに、サーバの完全修飾ドメイン名を正確に入力する必要があります。共通名と DNS ホスト名が一致していないと、アプライアンスへの接続時に警告が表示されます。

ステップ 10 [生成（Generate）] をクリックします。

ステップ 11 テキスト エディタを開きます。

ステップ 12 証明書要求のテキスト ブロック全体（`BEGIN CERTIFICATE REQUEST` 行と `END CERTIFICATE REQUEST` 行を含む）をコピーして、空のテキスト ファイルに貼り付けます。

ステップ 13 このファイルを *servername*`.csr` として保存します。*servername* は証明書を使用するサーバの名前です。

ステップ 14 [閉じる（Close）] をクリックします。

次のタスク

- 証明機関に証明書要求を送信します。
- 署名された証明書を受け取ったら、Firepower Management Center にインポートします。HTTPS サーバ証明書のインポート （1259 ページ）を参照してください。

HTTPS サーバ証明書のインポート

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	FMC 7000 および 8000 シリーズ	グローバルだけ。	Admin

証明書を生成した署名認証局から中間 CA を信頼するように要求された場合は、証明書チェーン（証明書パス）も提供する必要があります。

クライアント証明書が必要な場合、サーバ証明書が次に示すいずれかの条件を満たしていないときに、Web インターフェイス経由でのアプライアンスへのアクセスに失敗します。

- 証明書が、クライアント証明書に署名したものと同じ CA によって署名されている。
- 証明書が、証明書チェーンの中間証明書に署名したものと同じ CA によって署名されている。

⚠

注意 Firepower Management Center は 4096 ビット HTTPS 証明書をサポートしています。Firepower Management Center で使用する証明書が 4096 ビットを超える公開サーバ キーを使用して生成されている場合、FMC Web インターフェイスにログインできません。HTTPS 証明書のバージョン 6.0.0 への更新に関する詳細は、*FirePOWER* システム リリース ノート、バージョン *6.0* の「Update Management Center HTTPS Certificates to Version 6.0」を参照してください。HTTPS 証明書を生成またはインポートしていて、FMC の Web インターフェイスにログインできない場合は、サポートまでお問い合わせください。

始める前に

- 証明書署名要求を生成します。HTTPS サーバの証明書署名要求の作成 （1258 ページ）を参照してください。
- この CSR ファイルを証明書の要求先となる認証局にアップロードするか、この CSR を使用して自己署名証明書を作成します。
- 証明書がHTTPS サーバ証明書の要件 （1255 ページ）で説明されている要件を満たしていることを確認します。

ステップ 1 **[System]** > **[Configuration]**を選択します。

ステップ 2 [HTTPS Certificate] をクリックします。

ステップ 3 [HTTPSサーバ証明書のインポート（Import HTTPS Server Certificate）] をクリックします。

ステップ 4 テキスト エディタでサーバ証明書を開いて、`BEGIN CERTIFICATE` の行と `END CERTIFICATE` の行を含むテキストのブロック全体をコピーします。このテキストを [サーバ証明書（Server Certificate）] フィールドに貼り付けます。

ステップ 5 **秘密キー**を指定する必要があるかどうかは、証明書署名要求の生成方法によって異なります。

- Firepower Management Center Web インターフェイスを使用して証明書署名要求を生成した場合（HTTPS サーバの証明書署名要求の作成（1258 ページ）に記載）、システムにはすでに秘密キーがあるため、ここで入力する必要はありません。
- 他の方法を使用して証明書署名要求を生成した場合、ここで秘密キーを指定する必要があります。秘密キー ファイルを開いて、`BEGIN RSA PRIVATE KEY` の行と `END RSA PRIVATE KEY` の行を含むテキストのブロック全体をコピーします。このテキストを [秘密キー（Private Key）] フィールドに貼り付けます。

ステップ 6 必要な中間証明書をすべて開いて、それぞれのテキストのブロック全体をコピーして、[証明書チェーン（Certificate Chain）] フィールドに貼り付けます。

ステップ 7 **[保存（Save）]** をクリックします。

有効な HTTPS クライアント証明書の強制

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	FMC 7000 および 8000 シリーズ	グローバルだけ。	Admin

システムは、OCSP または PEM（Privacy-enhanced Electronic Mail）形式でインポートされた CRL を使用した HTTPS クライアント証明書の検証をサポートしています。

CRL を使用する場合は、失効した証明書のリストを最新の状態に保つために、CRL を更新するスケジュール タスクを作成してください。システムは、最後に更新した CRL を表示します。

（注） クライアント認証を有効にした後で Web インターフェイスにアクセスするには、ブラウザに有効なクライアント証明書が存在している（またはリーダーに CAC が挿入されている）**必要があります**。

始める前に

- 接続に使用するクライアント証明書に署名したものと同じ認証局で署名されたサーバ証明書をインポートします。HTTPS サーバ証明書のインポート （1259 ページ）を参照してください。
- サーバ証明書チェーンをインポートします（必要な場合）。HTTPS サーバ証明書のインポート （1259 ページ）を参照してください。

ステップ 1 **[System]** > **[Configuration]**を選択します。

ステップ 2 [HTTPS Certificate] をクリックします。

ステップ 3 [クライアント証明書の有効化（Enable Client Certificates）] を選択します。プロンプトが表示されたら、ドロップダウンリストから該当する証明書を選択します。

ステップ 4 次の 3 つのオプションがあります。

- 1 つ以上の CRL を使用してクライアント証明書を検証する場合は、[CRL のフェッチの有効化（Enable Fetching of CRL）] を選択して、手順 5 に進みます。
- OCSP を使用してクライアント証明書を検証する場合は、[OCSPの有効化（Enable OCSP）] を選択して、手順 7 に進みます。
- 失効の確認なしでクライアント証明書を承認する場合は、手順 8 に進みます。

ステップ 5 既存の CRL ファイルへの有効な URL を入力して、[CRL の追加（Add CRL）] をクリックします。最大 25 個まで CRL の追加を繰り返します。

ステップ 6 [CRL の更新（Refresh CRL）] をクリックして現在の CRL をロードするか、指定した URL から CRL をロードします。

（注） CRL のフェッチを有効にすると、定期的に CRL を更新するスケジュール タスクが作成されます。このタスクを編集して、更新の頻度を設定します。

ステップ 7 クライアント証明書がアプライアンスにロードされた認証局によって署名されていることと、サーバ証明書がブラウザの証明書ストアにロードされている認証局によって署名されていることを確認します。（これらは同じ認証局であることが必要です）。

注意 有効化したクライアント証明書で設定を保存している場合、ブラウザの証明書ストアに有効なクライアント証明書がないと、アプライアンスへの Web サーバアクセスがすべて無効になります。設定を保存する前に、有効なクライアント証明書がインストールされていることを確認してください。

ステップ 8 **[保存（Save）]** をクリックします。

関連トピック

証明書失効リストのダウンロードの設定 （241 ページ）

デフォルトの HTTPS サービス証明書の更新

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	FMC 7000 および 8000 シリーズ	グローバルだけ。	Admin

ログインしているアプライアンスのサーバ証明書のみを表示できます。

ステップ 1 **[System]** > **[Configuration]**を選択します。

ステップ 2 [HTTPS Certificate] をクリックします。

システムがデフォルトのHTTPSサーバ証明書を使用するように設定されている場合にのみ、ボタンが表示されます。

ステップ 3 [HTTPS 証明書の更新（Renew HTTPS Certificate）] ボタンをクリックします。（このボタンは、デフォルトのHTTPSサーバ証明書を使用するようにシステムが設定されている場合にのみ、証明書情報の下のディスプレイに表示されます。）

ステップ 4 （オプション）[HTTPS 証明書の更新（Renew HTTPS Certificate）] ダイアログボックスで、[新しいキーの生成（Generate New Key）] を選択して証明書の新しいキーを生成します。

ステップ 5 [HTTPS 証明書の更新（Renew HTTPS Certificate）] ダイアログボックスで [保存（Save）] をクリックします。

次のタスク

[HTTPS 証明書（HTTPS Certificate）] ページに表示されている証明書の有効日が更新されていることを確認することによって証明書が更新されていることを確認できます。

外部データベース アクセスの設定

サードパーティ製クライアントによるデータベースへの読み取り専用アクセスを許可するように、Firepower Management Center を設定できます。これによって、次のいずれかを使用して SQL でデータベースを照会できるようになります。

- 業界標準のレポート作成ツール（Actuate BIRT、JasperSoft iReport、Crystal Reports など）
- JDBC SSL 接続をサポートするその他のレポート作成アプリケーション（カスタム アプリケーションを含む）
- シスコが提供する RunQuery と呼ばれるコマンドライン型 Java アプリケーション（インタラクティブに実行することも、1 つのクエリの結果をカンマ区切り形式で取得することもできる）

Firepower Management Center のシステム設定を使用して、データベース アクセスを有効にして、選択したホストにデータベースの照会を許可するアクセス リストを作成します。このアクセス リストは、アプライアンスのアクセスは制御しません。

次のツールを含むパッケージをダウンロードすることもできます。

- RunQuery（シスコが提供するデータベース クエリ ツール）
- InstallCert（アクセスしたい Firepower Management Center から SSL 証明書を取得して受け入れるために使用できるツール）
- データベースへの接続時に使用する必要がある JDBC ドライバ

データベース アクセスを構成するためにダウンロードしたパッケージ内のツールの使用方法については、『*Firepower System Database Access Guide*』を参照してください。

データベースへの外部アクセスの有効化

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	FMC	グローバルだけ。	Admin

ステップ 1 **[System]** > **[Configuration]**を選択します。

ステップ 2 [外部データベース アクセス（External Database Access）] をクリックします。

ステップ 3 [外部データベース アクセスの許可（Allow External Database Access）] チェックボックスをオンにします。

ステップ 4 [サーバ ホスト名（Server Hostname）] フィールドに、適切な値を入力します。サードパーティ アプリケーションの要件に応じて、この値は、Firepower Management Center の完全修飾ドメイン名（FQDN）、IPv4 アドレス、または IPv6 アドレスにできます。

ステップ 5 [クライアント JDBC ドライバ（Client JDBC Driver）] の横にある [ダウンロード（Download）] をクリックし、ブラウザのプロンプトに従って `client.zip` パッケージをダウンロードします。

ステップ 6 1 つ以上の IP アドレスからのデータベース アクセスを追加するには、[ホストの追加（Add Hosts）] をクリックします。[アクセス リスト（Access List）] フィールドに [IP アドレス（IP Address）] フィールドが表示されます。

ステップ 7 [IP アドレス（IP Address）] フィールドに、IP アドレスまたはアドレスの範囲を入力するか、`any` を入力します。

ステップ 8 [Add] をクリックします。

ステップ 9 **[保存（Save）]** をクリックします。

ヒント 最後に保存されたデータベース設定に戻すには、[更新（Refresh）] をクリックします。

関連トピック

Firepower システムの IP アドレス表記法 （20 ページ）

データベース イベント数の制限

Firepower Management Center が保存できる各イベント タイプの最大数を指定できます。パフォーマンスを向上させるには、定期的に処理するイベント数に合わせてイベント数の制限を調整する必要があります。一部のイベント タイプでは、ストレージを無効にすることができます。

システムは侵入イベント、ディスカバリ イベント、監査レコード、セキュリティ インテリジェンスデータ、URL フィルタリング データをアプライアンスのデータベースから自動的にプルーニングします。イベントが自動的にプルーニングされると自動で電子メール通知を生成するようにシステムを設定できます。また、手動でディスカバリ データベースやユーザ データベースをプルーニングし、Firepower Management Center データベースからディスカバリ データや接続データを消去することもできます。

データベース イベント数の制限の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	FMC	グローバルだけ。	Admin

始める前に

- Firepower Management Center のデータベースからイベントがプルーニングされた場合に電子メール通知を受信するには、電子メール サーバを設定する必要があります。メール リレー ホストおよび通知アドレスの設定 （1303 ページ）を参照してください。

ステップ 1 **[System]** > **[Configuration]**を選択します。

ステップ 2 [データベース（Database）] を選択します。

ステップ 3 各データベースについて、保存するレコードの数を入力します。

各データベースが保持できるレコード数の詳細については、データベース イベント数の制限（1264 ページ）を参照してください。

ステップ 4 必要に応じて、[データ プルーニング通知のアドレス（Data Pruning Notification Address）] フィールドに、プルーニング通知を受信する電子メール アドレスを入力します。

ステップ 5 **[保存（Save）]** をクリックします。

データベース イベント数の制限

次の表に、Firepower Management Center に保存可能な各イベント タイプのレコードの最小数と最大数を示します。

表 *89 :* データベース イベント数の制限

イベント タイプ	上限	下限
侵入イベント	1,000 万（FMC Virtual） 2,000 万（MC750） 3,000 万（MC1000、MC1500、MC1600） 6,000 万（MC2000、MC2500、MC2600） 1 億 5,000 万（MC3500） 3 億（MC4000、MC4500、MC4600）	10,000
検出イベント	1,000 万 2000 万（MC2000、MC2500、MC2600、MC4000、MC4500、MC4600）	0（ストレージを無効化）
接続イベント セキュリティ インテリジェンス イベント	5,000 万（FMC 仮想） 5,000 万（MC750） 1 億（MC1000、MC1500、MC1600） 3 億（MC2000、MC2500、MC2600） 5 億（MC3500） 10 億（MC4000、MC4500、MC4600） 制限は接続イベントとセキュリティ インテリジェンスイベントの間で共有されます。設定済みの最大数の合計がこの制限を超えることはできません。	0（ストレージを無効化）
接続の要約（集約された接続イベント）	5,000 万（FMC 仮想） 5,000 万（MC750） 1 億（MC1000、MC1500、MC1600） 3 億（MC2000、MC2500、MC2600） 5 億（MC3500） 10 億（MC4000、MC4500、MC4600）	0（ストレージを無効化）
相関イベントおよびコンプライアンスのホワイト リスト イベント	100 万 200 万（MC2000、MC2500、MC2600、MC4000、MC4500、MC4600）	1 つ

イベント タイプ	上限	下限
マルウェア イベント	1,000 万 2000 万（MC2000、MC2500、MC2600、MC4000、MC4500、MC4600）	10,000
ファイル イベント	1,000 万 2000 万（MC2000、MC2500、MC2600、MC4000、MC4500、MC4600）	0（ストレージを無効化）
ヘルス イベント	100 万	0（ストレージを無効化）
監査レコード	100,000	1 つ
修復ステータス イベント	1,000 万	1 つ
ホワイトリスト違反履歴	30 日間の違反履歴	1 日の履歴
ユーザ アクティビティ（ユーザ イベント）	1,000 万	1 つ
ユーザ ログイン（ユーザ履歴）	1,000 万	1 つ
侵入ルール更新のインポート ログ レコード	100 万	1 つ
VPN トラブルシューティング データベース	1,000 万	0（ストレージを無効化）

管理インターフェイス

セットアップの完了後、管理ネットワーク設定を変更することができます。これには、FMC と管理対象デバイスの両方での管理インターフェイス、ホスト名、検索ドメイン、DNS サーバ、HTTP プロキシの追加が含まれます。

管理インターフェイスについて

デフォルトでは、Firepower Management Center はすべてのデバイスを 1 つの管理インターフェイス上で制御します。各デバイスには FMC と通信するための管理インターフェイスが 1 つ含まれています。

また、初期設定（FMC および管理対象デバイスの両方）や、管理者として FMC にログインする際にも管理インターフェイスで行います。

管理インターフェイスは、スマートライセンスサーバとの通信、更新プログラムのダウンロード、その他の管理機能の実行にも使用します。

Firepower Management Center 上の管理インターフェイス

Firepower Management Center では、初期セットアップ、管理者の HTTP アクセス、デバイスの管理、ならびにその他の管理機能（ライセンス管理や更新など）に、eth0 インターフェイスが使用されます。

同じネットワーク上、あるいは別のネットワーク上に、追加の管理インターフェイスを設定することもできます。FMC が管理するデバイスの数が多い場合、管理インターフェイスをさらに追加することで、スループットとパフォーマンスの向上につながります。これらの管理インターフェイスをその他すべての管理機能に使用することもできます。管理インターフェイスごとに、対応する機能を限定することをお勧めします。たとえば、ある特定の管理インターフェイスを HTTP 管理者アクセス用に使用し、別の管理インターフェイスをデバイスの管理に使用するなどです。

デバイス管理用に、管理インターフェイスには 2 つの別個のトラフィック チャネルがあります。管理トラフィック チャネルはすべての内部トラフィック（デバイス管理に固有のデバイス間トラフィックなど）を伝送し、イベント トラフィック チャネルはすべてイベント トラフィック（Web イベントなど）を伝送します。オプションで、FMC 上にイベントを処理するためのイベント専用インターフェイスを別個に設定することもできます。設定できるイベント専用インターフェイスは 1 つだけです。イベント トラフィックは大量の帯域幅を使用する可能性があるので、管理トラフィックからイベント トラフィックを分離することで、FMC のパフォーマンスを向上させることができます。たとえば、10 GigabitEthernet インターフェイスをイベント インターフェイスとして割り当て、可能なら、1 GigabitEthernet インターフェイスを管理用に使用します。たとえば、イベント専用インターフェイスは完全にセキュアなプライベート ネットワーク上に設定し、通常の管理インターフェイスはインターネットにアクセスできるネットワーク上で使用することをお勧めします。目的がスループットの向上だけである場合は、管理インターフェイスとイベント インターフェイスを同じネットワーク上で使用することもできます。FMC にイベント専用インターフェイスを設定する場合は管理用とイベント専用に個別のインターフェイスでデバイスをサポートしますが、個別のインターフェイスを持たないデバイスもサポートできます。管理用とイベント用を組み合わせた単一インターフェイスを持つデバイスの場合は、すべてのトラフィックが FMC 管理インターフェイスに移動します。

（注） すべての管理インターフェイスが、アクセス リスト設定（アクセス リストの設定 （1291 ページ））によって制御される HTTP 管理者アクセスをサポートします。逆に、インターフェイスを HTTP アクセスのみに制限することはできません。管理インターフェイスでは、常にデバイス管理がサポートされます（管理トラフィック、イベント トラフィック、またはその両方）。

（注） eth0 インターフェイスのみが DHCP IP アドレスをサポートします。他の管理インターフェイスはスタティック IP アドレスのみをサポートします。

管理対象デバイス上の管理インターフェイス

一部のモデルでは、イベント トラフィック専用として設定できる追加管理インターフェイスがあり、FMC との通信中に管理トラフィックとイベント トラフィックを分離できます。

デバイスをセットアップするときに、接続先とする FMC の IP アドレスを指定します。初期登録時は、管理トラフィックとイベント トラフィックの両方がこのアドレスに送信されます。注：場合によっては、FMC が別の管理インターフェイスで初期接続を確立することがあります。その場合、以降の接続では指定した IP アドレスの管理インターフェイスを使用する必要があります。

デバイスと FMC の両方に別個のイベント インターフェイスが設定されている場合は、デバイスと Management Center が互いのイベント インターフェイスを管理通信中に学習した後、ネットワークで許可されていれば、後続のイベント トラフィックがそれらのインターフェイス間で送られます。イベント ネットワークがダウンすると、イベント トラフィックは、通常の管理インターフェイスに戻ります。デバイスは、可能な場合に別個のイベント インターフェイスを使用しますが、管理インターフェイスは常にバックアップです。管理対象デバイス上で 1 つの管理インターフェイスだけを使用している場合、管理トラフィックを FMC 管理インターフェイスに送信できませんし、イベント トラフィックを別個の FMC イベント インターフェイスに送信することもできません。FMC と管理対象デバイスの両方で別個のイベント インターフェイスを使用する必要があります。この場合、管理トラフィックとイベント トラフィックの両方が FMC 管理インターフェイスに進み、このデバイスの FMC イベント インターフェイスは使用されません。

管理インターフェイスのサポート

管理インターフェイスの場所については、ご使用のモデルのハードウェア インストレーション ガイドを参照してください。

（注） Firepower 4100/9300 シャーシ の場合、MGMT インターフェイスは FTD の論理デバイスを管理するためではなく、シャーシを管理するために使用します。mgmt タイプ（または firepower-eventing タイプあるいはその両方）の別個の NIC インターフェイスを設定してから、そのインターフェイスを FTD 論理デバイスに割り当てる必要があります。

（注） シャーシ上の FTD の場合、物理管理インターフェイスは、診断論理インターフェイス（SNMP または syslog に利用できて、FMC でデータ インターフェイスと併せて設定されます）と、FMC 通信用の管理論理インターフェイスの間で共有されます。詳細については、管理/診断インターフェイス （785 ページ）を参照してください。

Firepower Management Center および管理対象デバイスの各モデルでサポートされる管理インターフェイスについては、以下の表を参照してください。

表 *90 : Firepower Management Center* でサポートされる管理インターフェイス

モデル	管理インターフェイス
MC750、MC1500、MC3500	eth0（デフォルト） eth1
MC2000、MC4000	eth0（デフォルト） eth1 eth2 eth3
MC1000	eth0（デフォルト） eth1
MC1600、MC2500、MC2600、MC4500、MC4600	eth0（デフォルト） eth1 eth2 eth3
Firepower Management Center Virtual	eth0（デフォルト）

表 *91 :* 管理対象デバイスでサポートされる管理インターフェイス

モデル	管理インターフェイス	オプションのイベント インターフェイス
7000 シリーズ	eth0	サポートなし
8000 シリーズ	eth0	eth1
NGIPSv	eth0	サポートなし
ASA 5585-X 上の ASA FirePOWER サービス モジュール	eth0 （注） eth0 は、管理 1/0 インターフェイスの内部名です。	eth1 （注） eth1 は、管理 1/1 インターフェイスの内部名です。
ASA5508-X、5516-X 上の ASA FirePOWER サービス モジュール	eth0 （注） eth0 は、管理 1/1 インターフェイスの内部名です。	サポートなし

モデル	管理インターフェイス	オプションのイベント インターフェイス
ASA 5525-X から 5555-X 上の ASA FirePOWER サービス モジュール	eth0 （注） eth0 は、管理 0/0 インターフェイスの内部名です。	サポートなし
Firepower Threat Defense Firepower 1000 上	management0 （注） management0 は管理 1/1 インターフェイスの内部名です。	サポートなし
Firepower 2100 上の Firepower Threat Defense	management0 （注） management0 は管理 1/1 インターフェイスの内部名です。	サポートなし
Firepower 4100 および 9300 上の Firepower Threat Defense	management0 （注） management0 は、物理インターフェイス ID に関わらず、このインターフェイスの内部名です。	management1 （注） management1 は、物理インターフェイス ID に関わらず、このインターフェイスの内部名です。
ASA 、5508-X、5516-X 上の Firepower Threat Defense	br1 （注） br1 は、管理 1/1 インターフェイスの内部名です。	サポートなし
5525 ～ 5555-X 上の Firepower Threat Defense	br1 （注） br1 は、管理 0/0 インターフェイスの内部名です。	サポートなし
ISA 3000 上の Firepower Threat Defense	br1 （注） br1 は、管理 1/1 インターフェイスの内部名です。	サポートなし
Firepower Threat Defense Virtual	br1	サポートなし

管理インターフェイス上のネットワーク ルート

管理インターフェイス（イベント専用インターフェイスを含む）は、リモートネットワークに到達するためのスタティック ルートのみをサポートしています。FMC または管理対象デバイスをセットアップすると、セットアップ プロセスにより、指定したゲートウェイ IP アドレスへのデフォルトルートが作成されます。このルートを削除することはできません。また、このルートで変更できるのはゲートウェイ アドレスのみです。

一部のプラットフォームでは、複数の管理インターフェイスを設定できます。デフォルトルートには出力インターフェイスが含まれていないため、選択されるインターフェイスは、指定したゲートウェイアドレスと、ゲートウェイが属するインターフェイスのネットワークによって異なります。デフォルトネットワーク上に複数のインターフェイスがある場合、デバイスは出力インターフェイスとして番号の小さいインターフェイスを使用します。

複数のインターフェイスが同じネットワーク上にある場合を含めて、リモートネットワークにアクセスするには、管理インターフェイスごとに1つ以上のスタティック ルートを使用することをお勧めします。

たとえば、FMC で、eth0 と eth1 が同じネットワーク上にありますが、各インターフェイスで異なるデバイス グループを管理するとします。デフォルト ゲートウェイは192.168.45.1 です。eth1 でリモート 10.6.6.0/24 宛先ネットワーク上のデバイスを管理する場合は、同じ 192.168.45.1 のゲートウェイを使用して eth1 経由で 10.6.6.0/24 用のスタティック ルートを作成できます。10.6.6.0/24 へのトラフィックは、デフォルト ルートの前にこのルートに到達するため、eth1 が想定どおりに使用されます。

2 つの FMC インターフェイスを使用して同じネットワーク上のリモート デバイスを管理する場合は、デバイス IP アドレスごとに別のスタティック ルートが必要なため、FMC のスタティック ルーティングが適切に拡張できないことがあります。

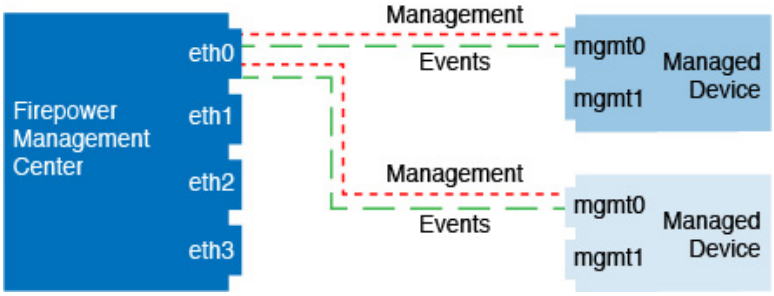
別の例には、FMC と管理対象デバイスの両方に個別の管理インターフェイスとイベント専用インターフェイスが含まれています。イベント専用インターフェイスは、管理インターフェイスとは別のネットワーク上にあります。この場合は、リモートイベント専用ネットワーク宛てのトラフィック用にイベント専用インターフェイスを介してスタティック ルートを追加します。その逆も同様です。

（注） 管理インターフェイスのルーティングは、データ インターフェイスに対して設定するルーティングとは完全に別のものです。

管理およびイベント トラフィック チャネルの例

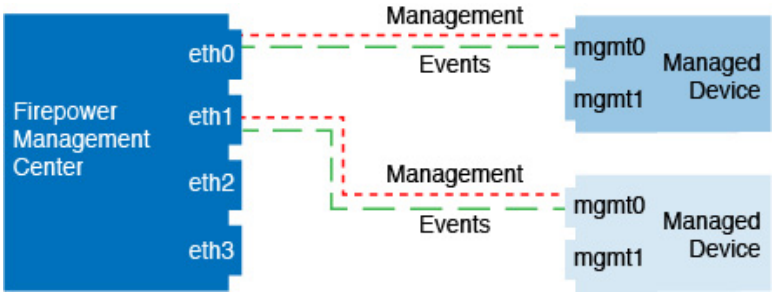
以下に、Firepower Management Center と管理対象デバイスでデフォルト管理インターフェイスのみを使用する例を示します。

図 *28 : Firepower Management Center* 上で単一の管理インターフェイスを使用する場合



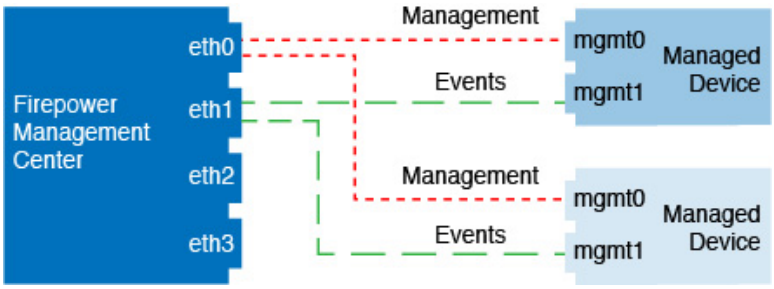
以下に、Firepower Management Center でデバイスごとに別個の管理インターフェイスを使用する例を示します。この場合、各管理対象デバイスが 1 つの管理インターフェイスを使用します。

図 *29 : Firepower Management Center* 上の複数の管理インターフェイスを使用する場合



以下に、個別のイベント インターフェイスを使用する Firepower Management Center と管理対象デバイスの例を示します。

図 *30 : Firepower Management Center*上の個別のイベント インターフェイスと管理対象デバイスを使用する場合



以下に、Firepower Management Center 上で複数の管理インターフェイスと個別のイベント インターフェイスが混在し、個別のイベントインターフェイスを使用する管理対象デバイスと単一の管理インターフェイスを使用する管理対象デバイスが混在する例を示します。

図 *31* : 管理インターフェイスとイベント インターフェイスを混在させて使用する場合

管理インターフェイスの設定

Firepower アプライアンスの管理インターフェイス設定を変更できます。

- Firepower Management Center：Web インターフェイスを使用します。Cisco TAC または FMC マニュアルの明示的な手順による指示がない限り、Firepower Management Center Linux シェルを使用しないことを強くお勧めします。
- FTD デバイス、NGIPSv、ASA FirePOWER：CLI を使用します。
- 7000 & 8000 シリーズ デバイス：制限された Web インターフェイスまたは CLI を使用します。

次の項を参照してください。

関連トピック

通信ポートの要件 （3284 ページ）

Firepower Management Center 管理インターフェイスの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	FMC	グローバルだけ。	Admin

Firepower Management Center で管理インターフェイスの設定を変更します。オプションとして追加の管理インターフェイスを有効にしたり、イベントのみのインターフェイスを設定したりできます。

⚠

注意 接続されている管理インターフェイスを変更する場合は十分にご注意ください。設定エラーのために再接続できない場合は、FMC コンソール ポートにアクセスして、Linux シェルでネットワーク設定を再設定する必要があります。この操作では、Cisco TAC に連絡する必要があります。

始める前に

プロキシを使用する場合：

- NT LAN Manager（NTLM）認証を使用するプロキシはサポートされません。
- スマート ライセンスを使用しているか、または使用する予定がある場合は、プロキシの FQDN は 64 文字以内にする必要があります。

ステップ 1 **[System]** > **[Configuration]** を選択して、[管理インターフェイス（Management Interfaces）] を選択します。

ステップ 2 [インターフェイス（Interfaces）]エリアで、設定するインターフェイスの横にある [編集（Edit）] をクリックします。

このセクションでは、利用可能なすべてのインターフェイスがリストされます。インターフェイスをさらに追加することはできません。

それぞれの管理インターフェイスに対して、以下のオプションを設定できます。

- [有効にする（Enabled）]：管理インターフェイスを有効にします。デフォルト eth0 管理インターフェイスを無効に**しないでください**。eth0 インターフェイスを必要とするプロセスもあります。
- [チャネル（Channels）]：イベントのみのインターフェイスを設定します。FMC では 1 つのイベント インターフェイスしか設定できません。これを設定するには、[管理トラフィック（Management Traffic）] チェックボックスをオフにして、[イベント トラフィック（Event Traffic）]チェックボックスをオンのままにしておきます。必要に応じて、管理インターフェイスの[イベント トラフィック（Event Traffic）] を無効にすることができます。いずれの場合も、デバイスは、イベントのみのインターフェイスにイベントを送信しようとします。そのインターフェイスがダウンしていた場合は、イベント チャネルが無効になっていても、管理インターフェイス上でイベントを送信します。インターフェイス上でイベント チャネルと管理チャンネルの両方を無効にすることはできません。
- [モード（Mode）]：リンク モードを指定します。GigabitEthernet インターフェイスでは、自動ネゴシエーションの値を変更しても反映されないことに注意してください。
- [MDI/MDIX]：[自動-MDIX（Auto-MDIX）] を設定します。
- [MTU]：最大伝送ユニット（MTU）を設定します。デフォルトは 1500 です。設定可能な MTU の範囲は、モデルとインターフェイスのタイプによって異なる場合があります。

  システムは、設定された MTU 値から自動的に 18 バイトを削減するため、IPv6 の場合、1298 未満の値は MTU の最小値である 1280 に準拠しません。IPv4 の場合は、594 未満の値は MTU の最小値 576 に準拠しません。たとえば、構成値 576 は自動的に 558 に削減されます。
- [IPv4 設定（IPv4 Configuration）]：IPv4 IP アドレスを設定します。次のどちらかを選択します。
  - [スタティック（Static）]：**IPv4 の管理 IP アドレス** と**ネットマスク**を手動で入力します。
  - [DHCP]：DHCP を使用するインターフェイスを設定します（eth0 のみ）。
  - [無効（Disabled）]：無効 IPv4。IPv4 と IPv6 の両方を無効に**しないでください**。
- [IPv6 設定（IPv6 Configuration）]：IPv6 IP アドレスを設定します。次のどちらかを選択します。

- [スタティック（Static）]：**IPv6 の管理 IP アドレス**と **IPv6 のプレフィックス長**を手動で入力します。
- [DHCP]：DHCPv6 を使用するインターフェイスを設定します（eth0 のみ）。
- [ルータ割当て（Router Assigned）]：ステートレス自動設定を有効にします。
- [無効（Disabled）]：IPv6 を無効にします。IPv4 と IPv6 の両方を無効に**しないでください**。
- [IPv6 DAD]：IPv6 を有効にするときに [重複アドレス検出（DAD）] を有効または無効にします。DAD を使用することによってサービス拒否攻撃の可能性が拡大するため、DAD は無効にすることができます。この設定を無効にした場合は、すでに割り当てられているアドレスがこのインターフェイスで使用されていないことを手動で確認する必要があります。

ステップ 3 [ルート（Routes）] エリアで、スタティック ルートを編集アイコン（）をクリックして編集するか、またはルートを追加アイコン（）をクリックして追加します。表示アイコン（）をクリックして、ルートの統計を表示します。

追加の各インターフェイスがリモート ネットワークに到達するには、スタティック ルートが必要です。新しいルートが必要になるケースの詳細については、管理インターフェイス上のネットワーク ルート（1271 ページ）を参照してください。

（注） デフォルト ルートでは、ゲートウェイ IP アドレスのみを変更できます。出力インターフェイスは、指定したゲートウェイをインターフェイスのネットワークに照合することで自動的に選択されます。

次の設定をスタティック ルートに対して設定できます。

- [宛先（Destination）]：ルートを作成する宛先ネットワークのアドレスを設定します。
- [ネットマスク（Netmask）] または [プレフィックス長（Prefix Length）]：ネットワークのネットマスク（IPv4）またはプレフィックス長（IPv6）を設定します。
- [インターフェイス（Interface）]：出力管理インターフェイスを設定します。
- [ゲートウェイ（Gateway）]：ゲートウェイ IP アドレスを設定します。

ステップ 4 [共有設定（Shared Settings）] エリアで、すべてのインターフェイスで共有されているネットワーク パラメータを設定します。

（注） eth0 インターフェイスで [DHCP] を選択すると、DHCP サーバから取得する共有設定の一部を手動で指定することができなくなります。

以下の共有設定を行うことができます。

- [ホスト名（Hostname）]：FMC ホスト名を設定します。ホスト名を変更する場合、syslog メッセージに反映される新しいホスト名を使用するには、FMC を再起動します。再起動するまでは、新しいホスト名が Syslog メッセージに反映されません。
- [ドメイン（Domains）]：カンマで区切られた、FMC の検索ドメインを設定します。これらのドメインは、コマンド（**ping system** など）に完全修飾ドメイン名を指定しない場合にホスト名に追加されま

す。ドメインは、管理インターフェイスまたは管理インターフェイスを経由するコマンドでのみ、使用されます。

- [プライマリ DNS サーバ（Primary DNS Server）]、[セカンダリ DNS サーバ（Secondary DNS Server）]、[テリタリ DNS サーバ（Tertiary DNS Server）]：DNS サーバが優先順で使用されるよう設定します。
- [リモート管理ポート（Remote Management Port）]：管理対象デバイスとの通信用のリモート管理ポートを設定します。FMCおよび管理対象デバイスは、双方向のSSL暗号化通信チャネル（デフォルトではポート 8305）を使用して通信します。

（注） シスコは、リモート管理ポートをデフォルト設定のままにしておくことを**強く**推奨していますが、管理ポートがネットワーク上の他の通信と競合する場合は、別のポートを選択できます。管理ポートを変更する場合は、導入内の相互に通信する必要がある**すべての**デバイスの管理ポートを変更する必要があります。

ステップ 5 [ICMPv6] 領域で、ICMPv6 の設定を行います。

- [エコー応答パケットの送信を許可する（Allow Sending Echo Reply Packets）]：エコー応答パケットを有効または無効にします。これらのパケットを無効にすることで、サービス拒否攻撃の可能性から保護します。エコー応答パケットを無効にすると、FMC の管理インターフェイスにテスト目的で IPv6 ping を使用できなくなります。
- [宛先到達不能パケットの送信を許可する（Allow Sending Destination Unreachable Packets）]：宛先到達不能パケットを有効または無効にします。これらのパケットを無効にすることで、サービス拒否攻撃の可能性から保護します。

ステップ 6 [プロキシ（Proxy）] エリアで、HTTP プロキシ設定をします。

FMC は、ポート TCP/443（HTTPS）および TCP/80（HTTP）でインターネットに直接接続するように構成されています。HTTP ダイジェスト経由で認証できるプロキシ サーバを使用できます。

このトピックの前提条件のプロキシの要件を参照してください。

a) [有効（Enabled）] チェックボックスをオンにします。
b) [HTTP プロキシ（HTTP Proxy）] フィールドに、プロキシ サーバの IP アドレスまたは完全修飾ドメイン名を入力します。

このトピックの前提条件の要件を参照してください。

c) [ポート（Port）] フィールドに、ポート番号を入力します。
d) [プロキシ認証の使用（Use Proxy Authentication）] を選択してから [ユーザ名（User Name）] と [パスワード（Password）] を入力して、認証資格情報を設定します。

ステップ 7 [保存（Save）] をクリックします。

ステップ 8 管理 IP アドレスを変更すると、FMC と管理対象デバイスの間の通信に影響を与える可能性があります。

IP アドレスを変更しても、現在の接続には影響を与えません。ただし、デバイスまたは FMC をリロードした場合は、接続を再確立する必要があります。ピアの正しい IP アドレスを持つために、少なくとも 1 つのデバイス（FMC または管理対象デバイス）が必要です。たとえば、FMC でデバイスを追加し、（IP アドレスの代わりに）NAT ID を指定した場合は、設定時にデバイスに定義した FMC IP アドレスが正しくな

くなるため、デバイスは通信を再確立できなくなります。さらに、デバイスの FMC の IP アドレスは更新できません。できることは、IPアドレスを置換して新しいデバイスとして再登録することだけです（**configure manager add**）。一方で、FMC で管理対象デバイスの正しい IP アドレスが認識されている場合は、管理対象デバイスが持つ FMC 用の IP アドレスが正しくない場合でも、FMC は正常に接続を確立できます。

CLI でのデバイス管理インターフェイスの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	グローバルだけ。	Admin

CLI を使用して、管理対象デバイスの管理インターフェイスの設定を変更します。これらの設定の多くは、初期セットアップ時に設定されたものです。この手順に従うことで、それらの設定を変更でき、さらに設定を追加できます（例：モデルでサポートされる場合にイベント インターフェイスを有効化する、スタティック ルートを追加する）。

FTD CLI については、『*Command Reference for Firepower Threat Defense*』を参照してください。

クラシック デバイス CLI の詳細については、このガイドの従来型デバイスのコマンド ライン リファレンス （3289 ページ）を参照してください。

FTDおよびクラシック デバイスは、管理インターフェイス設定に同じコマンドを使用します。その他のコマンドは、プラットフォーム間で異なる可能性があります。

（注） SSH を使用する際は、慎重に管理インターフェイスに変更を加えてください。構成エラーで再接続できなくなると、デバイスのコンソール ポートへのアクセスが必要になります。

始める前に

- Firepower Threat Defense デバイスでは、**configure user add** コマンドを使用して CLI にログイン可能なユーザ アカウントを作成できます。CLI での内部ユーザの追加 （60 ページ）を参照してください。SSH の外部認証の設定 （1361 ページ）に従って AAA ユーザを設定することもできます。
- 7000 & 8000 シリーズ デバイスでは、Web インターフェイスでの内部ユーザの追加 （57 ページ）の説明に従って、Web インターフェイスでユーザ アカウントを作成できます。

ステップ 1 コンソール ポートから、または SSH を使用して、デバイス CLI に接続します。

FTD デバイスのコマンドライン インターフェイスへのログイン （37 ページ）または7000/8000 シリーズ、ASA FirePOWER、および NGIPSv デバイスの CLI へのログイン （37 ページ）を参照してください。

ステップ 2 管理者のユーザ名とパスワードでログインします。

ステップ 3 イベント オンリーのインターフェイスを有効にします（サポート モデルについては、管理インターフェイスのサポート （1268 ページ）参照）。

configure network management-interface enable *management_interface*

configure network management-interface disable-management-channel *management_interface*

例：

これは Firepower 4100 または 9300 デバイスの例です。有効なインターフェイス名はデバイス タイプによって異なります。

```
> configure network management-interface enable management1
Configuration updated successfully

> configure network management-interface disable-management-channel management1
Preserve existing configuration- currently no IP addresses on eth1 to update (bootproto
IPv4:,bootproto IPv6:
at /usr/local/sf/lib/perl/5.10.1/SF/NetworkConf/NetworkSettings.pm line 821.
Configuration updated successfully

>
```

Firepower Management Center イベント専用インターフェイスは管理チャネルのトラフィックを受け入れることができないので、デバイス イベント インターフェイスで管理チャネルを単に無効にしてください。

必要に応じて、**configure network management-interface disable-events-channel** コマンドを使用して管理インターフェイスのイベントを無効にできます。いずれの場合も、デバイスは、イベントのみのインターフェイス上でイベントを送信しようとします。そのインターフェイスがダウンしていた場合は、イベント チャネルが無効になっていても、管理インターフェイス上でイベントを送信します。

インターフェイス上でイベント チャネルと管理チャンネルの両方を無効にすることはできません。

ステップ 4 管理インターフェイスまたはイベント インターフェイスのネットワーク設定をします。

management_interface 引数を指定しない場合は、デフォルトの管理インターフェイスのネットワーク設定を変更します。イベント インターフェイスを設定する際は、必ず *management_interface* 引数を指定してください。イベントインターフェイスは、管理インターフェイスの個別のネットワーク、または同じネットワークに配置できます。自分で設定するインターフェイスに接続すると、切断されます。新しい IP アドレスに再接続できます。

a) IPv4 アドレスを設定します。

- 手動設定

  configure network ipv4 manual *ip_address netmask gateway_ip* [*management_interface*]

  このコマンド内の *gateway_ip* は、プライマリ管理インターフェイスのデフォルト ルートを作成するためにしか使用されないことに注意してください。イベントのみのインターフェイスのゲートウェイを設定する場合、このコマンドは、ゲートウェイを無視して、それ用のデフォルト ルートまたはスタティック ルートを作成しません。**configure network static-routes** コマンドを使用してスタティック ルートを別途作成する必要があります。

  例：

```
> configure network ipv4 manual 10.10.10.45 255.255.255.0 management1
Setting IPv4 network configuration.
Network settings changed.

>
```

- DHCP（デフォルト管理インターフェイスのみでサポート）。

  configure network ipv4 dhcp

b) IPv6 アドレスを設定します。

- ステートレス自動設定

  configure network ipv6 router [*management_interface*]

  例：

```
> configure network ipv6 router management0
Setting IPv6 network configuration.
Network settings changed.

>
```

- 手動設定

  configure network ipv6 manual *ip6_address ip6_prefix_length* [*ip6_gateway_ip*] [*management_interface*]

  このコマンド内の *ipv6_gateway_ip* は、プライマリ管理インターフェイスのデフォルト ルートを作成するためにしか使用されないことに注意してください。イベントのみのインターフェイスのゲートウェイを設定する場合、このコマンドは、ゲートウェイを無視して、それ用のデフォルト ルートまたはスタティック ルートを作成しません。**configure network static-routes** コマンドを使用してスタティック ルートを別途作成する必要があります。

  例：

```
> configure network ipv6 manual 2001:0DB8:BA98::3210 64 management1
Setting IPv6 network configuration.
Network settings changed.

>
```

- DHCPv6（デフォルト管理インターフェイスのみでサポート）。

  configure network ipv6 dhcp

ステップ 5 IPv6 の場合、ICMPv6 エコー応答と宛先到達不能メッセージを有効または無効にします。デフォルトでは、これらのメッセージは有効になっています。

configure network ipv6 destination-unreachable {**enable** | **disable**}

configure network ipv6 echo-reply {**enable** | **disable**}

これらのパケットを無効にすることで、サービス拒否攻撃の可能性から保護します。エコー応答パケットを無効にすると、デバイスの管理インターフェイスにテスト目的で IPv6 ping を使用できなくなります。

例：

```
> configure network ipv6 destination-unreachable disable
> configure network ipv6 echo-reply disable
```

ステップ 6 （FTD のみ）デフォルト管理インターフェイスの DHCP サーバが、接続されているホストに IP アドレスを提供することを可能にします。

configure network ipv4 dhcp-server-enable *start_ip_address end_ip_address*

例：

```
> configure network ipv4 dhcp-server-enable 10.10.10.200 10.10.10.254
DHCP Server Enabled

>
```

管理インターフェイスの IP アドレスを手動で設定するときにのみ、DHCP サーバを設定できます。このコマンドは、Firepower Threat Defense Virtual ではサポートされません。DHCP サーバのステータスを表示するには、**show network-dhcp-server** を入力します。

```
> show network-dhcp-server
DHCP Server Enabled
10.10.10.200-10.10.10.254
```

ステップ 7 Firepower Management Center がリモート ネットワーク上にある場合は、イベント専用インターフェイスのスタティック ルートを追加します。追加しないと、すべてのトラフィックが管理インターフェイスを通じてデフォルト ルートと一致します。

configure network static-routes {**ipv4** | **ipv6**} **add** *management_interface destination_ip netmask_or_prefix gateway_ip*

デフォルト ルートの場合は、このコマンドを使用しないでください。デフォルト管理インターフェイスに対して **configure network ipv4** コマンドまたは **ipv6** コマンドを使用する場合は、デフォルト ルート ゲートウェイの IP アドレスしか変更できません（ステップ 4 を参照）。

ルーティングの詳細については、管理インターフェイス上のネットワーク ルート（1271 ページ）を参照してください。

例：

```
> configure network static-routes ipv4 add management1 192.168.6.0 255.255.255.0 10.10.10.1
Configuration updated successfully

> configure network static-routes ipv6 add management1 2001:0DB8:AA89::5110 64 2001:0DB8:BA98::3211
Configuration updated successfully

>
```

スタティック ルートを表示するには、**show network-static-routes** を入力します（デフォルト ルートは表示されません）。

```
> show network-static-routes
---------------[ IPv4 Static Routes ]---------------
Interface                 : management1
Destination               : 192.168.6.0
Gateway                   : 10.10.10.1
Netmask                   : 255.255.255.0
[…]
```

ステップ 8 ホスト名の設定

configure network hostname *name*

例：

```
> configure network hostname farscape1
```

Syslog メッセージは、再起動するまで新しいホスト名を反映しません。

ステップ 9 検索ドメインを設定します。

configure network dns searchdomains *domain_list*

例：

```
> configure network dns searchdomains example.com,cisco.com
```

カンマで区切ったデバイスの検索ドメインを設定します。これらのドメインは、コマンド（**ping system** など）に完全修飾ドメイン名を指定しない場合にホスト名に追加されます。ドメインは、管理インターフェイスまたは管理インターフェイスを経由するコマンドでのみ、使用されます。

ステップ 10 カンマで区切った 3 つの DNS サーバを設定します。

configure network dns servers *dns_ip_list*

例：

```
> configure network dns servers 10.10.6.5,10.20.89.2,10.80.54.3
```

ステップ 11 FMC で通信のリモート管理ポートを設定します。

configure network management-interface tcpport *number*

例：

```
> configure network management-interface tcpport 8555
```

FMC および管理対象デバイスは、双方向の SSL 暗号化通信チャネル（デフォルトではポート 8305）を使用して通信します。

（注） シスコは、リモート管理ポートをデフォルト設定のままにしておくことを**強く**推奨していますが、管理ポートがネットワーク上の他の通信と競合する場合は、別のポートを選択できます。管理ポートを変更する場合は、導入内の相互に通信する必要がある**すべての**デバイスの管理ポートを変更する必要があります。

ステップ 12 HTTP プロキシを設定します。デバイスは、ポート TCP/443（HTTPS）および TCP/80（HTTP）でインターネットに直接接続するように構成されています。HTTP ダイジェスト経由で認証できるプロキシサーバを使用できます。コマンド発行後に、HTTP プロキシのアドレスとポート、プロキシの認証が必要かどうかをユーザは尋ねられます。認証が必要な場合はプロキシのユーザ名、プロキシのパスワード、およびプロキシのパスワードの確認を入力するよう要求されます。

（注） Cisco Firepower Threat Defense のプロキシ パスワードの場合は、使用できる文字は A ～ Z、a ～ z、および 0 ～ 9 のみです。

configure network http-proxy

例：

```
> configure network http-proxy
Manual proxy configuration
Enter HTTP Proxy address: 10.100.10.10
Enter HTTP Proxy Port: 80
Use Proxy Authentication? (y/n) [n]: Y
Enter Proxy Username: proxyuser
Enter Proxy Password: proxypassword
Confirm Proxy Password: proxypassword
```

ステップ 13 管理 IP アドレスを変更した場合は、デバイス管理設定の編集 （300 ページ） に従って FMC の管理対象デバイスの IP アドレスを変更します。

FMC のデバイスに（IP アドレスではなく）NAT ID を指定した場合は、この手順をスキップできます。

シャットダウンまたは再起動

FMC のプロセスのシャットダウンおよび再起動を制御するには、Web インターフェイスを使用します。次の操作を実行できます。

- シャットダウン：アプライアンスのグレースフル シャットダウンを開始します。

注意 電源ボタンを使用して Firepower アプライアンスを停止しないでください。データが失われる可能性があります。Web インターフェイス（または CLI）を使用すると、設定データを失うことなく、安全にシステムの電源を切って再起動する準備が整います。

- リブート：シャットダウンしてグレースフルに再起動します。

- コンソールの再起動：通信、データベース、HTTP サーバのプロセスを再起動します。これは通常、トラブルシューティングの際に使用されます。

ヒント　Snort プロセスの再起動など、7000/8000 シリーズ デバイスのシャットダウン/再起動の詳細については、7000/8000 シリーズデバイスのシャットダウンまたは再起動（1354 ページ）を参照してください。仮想デバイスの場合は、ご使用の仮想プラットフォームのマニュアルを参照してください。特に VMware の場合、カスタム電源オプションは VMware ツールの一部です。

FMC のシャットダウンまたは再起動

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	
いずれか（Any）	いずれか（Any）	FMC	グローバルだけ。	Admin

ステップ 1　**[System]** > **[Configuration]**を選択します。

ステップ 2　[プロセス（Process）] を選択します。

ステップ 3　次のいずれかを実行します。

シャットダウン	[管理センターのシャットダウン（Shutdown Management Center）] の横にある [コマンドの実行（Run Command）] をクリックします。
再起動	[管理センターの再起動（Reboot Management Center）] の横にある [コマンドの実行（Run Command）] をクリックします。 （注）　再起動するとログアウトします。システムはデータベース チェックを実行しますが、これは完了するのに 1 時間かかります。
コンソールの再起動	[管理センターの再起動（Restart Management Center）] の横にある [コマンドの実行（Run Command）] をクリックします。 （注）　再起動すると、ネットワーク マップ内に削除されたホストが再表示されることがあります。

関連トピック

Snort® の再起動シナリオ （450 ページ）

リモート ストレージ管理

Firepower Management Center では、バックアップおよびレポートのローカル ストレージまたはリモート ストレージとして、以下を使用することができます。

- ネットワーク ファイル システム（NFS）
- サーバ メッセージ ブロック（SMB）/Common Internet File System（CIFS）
- セキュア シェル（SSH）

（注） システムは、バックアップおよびリモート ストレージの SMBv1 のみをサポートします。

1 つのリモート システムにバックアップを送信し、別のリモート システムにレポートを送信することはできませんが、どちらかをリモート システムに送信し、もう一方を Firepower Management Center に格納することは可能です。

ヒント リモート ストレージを構成して選択した後は、接続データベースの制限を**増やさなかった**場合に**のみ**、ローカル ストレージに戻すことができます。

ローカル ストレージの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	FMC	グローバルだけ。	Admin

ステップ 1 **[System]** > **[Configuration]**を選択します。

ステップ 2 [リモート ストレージ デバイス（Remote Storage Device）] を選択します。

ステップ 3 [ストレージ タイプ（Storage Type）] ドロップダウン リストから [ローカル（リモート ストレージなし）（Local (No Remote Storage)）] を選択します。

ステップ 4 **[保存（Save）]** をクリックします。

リモート ストレージの NFS の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	FMC	グローバルだけ。	Admin

始める前に

- 外部リモート ストレージ システムが機能しており、FMC からアクセスできることを確認します。

ステップ 1 **[System]** > **[Configuration]**を選択します。
ステップ 2 [リモート ストレージ デバイス（Remote Storage Device）] をクリックします。
ステップ 3 [ストレージ タイプ（Storage Type）] ドロップダウン リストから [NFS] を選択します。
ステップ 4 接続情報を追加します。

- [Host] フィールドに、ストレージ システムの IPv4 アドレスまたはホスト名を入力します。
- [ディレクトリ（Directory）] フィールドに、ストレージ領域へのパスを入力します。

ステップ 5 必要に応じて、[詳細オプションの使用（Use Advanced Options）] チェックボックスをオンにして、必要なコマンドライン オプションを入力します。リモート ストレージ管理の詳細オプション（1287 ページ）を参照してください。
ステップ 6 [システムの使用方法（System Usage）] で、次の手順を実行します。

- 指定したホストにバックアップを格納するには、[バックアップに使用（Use for Backups）] を選択します。
- 指定したホストにレポートを格納するには、[レポートに使用（Use for Reports）] を選択します。
- リモート ストレージへのバックアップに関する [ディスク容量のしきい値（Disk Space Threshold）] を入力します。デフォルトは 90% です。

ステップ 7 設定をテストするには、[テスト（Test）] をクリックします。
ステップ 8 **[保存（Save）]** をクリックします。

リモート ストレージの SMB の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	FMC	グローバルだけ。	Admin

始める前に

- 外部リモート ストレージ システムが機能しており、FMC からアクセスできることを確認します。

ステップ 1 **[System]** > **[Configuration]**を選択します。
ステップ 2 [リモート ストレージ デバイス（Remote Storage Device）] をクリックします。
ステップ 3 [ストレージ タイプ（Storage Type）] ドロップダウン リストから [SMB] を選択します。
ステップ 4 接続情報を追加します。

- [Host] フィールドに、ストレージ システムの IPv4 アドレスまたはホスト名を入力します。
- [Share] フィールドに、ストレージ領域の共有を入力します。システムに認識されるのはファイルのフル パスではなく最上位の共有だけであることに注意してください。指定した共有ディレクトリをリモート バックアップ先として使用するには、それを Windows システムで共有する必要があります。
- 必要に応じて、[Domain] フィールドにリモート ストレージ システムのドメイン名を入力します。
- [ユーザ名（Username）] フィールドにストレージ システムのユーザ名を入力し、[パスワード（Password）] フィールドにそのユーザのパスワードを入力します。

ステップ 5 必要に応じて、[詳細オプションの使用（Use Advanced Options）] チェックボックスをオンにして、必要なコマンドライン オプションを入力します。リモート ストレージ管理の詳細オプション（1287ページ）を参照してください。

ステップ 6 [システムの使用方法（System Usage）] で、次の手順を実行します。

- 指定したホストにバックアップを格納するには、[バックアップに使用（Use for Backups）] を選択します。
- 指定したホストにレポートを格納するには、[レポートに使用（Use for Reports）] を選択します。

ステップ 7 設定をテストするには、[テスト（Test）] をクリックします。

ステップ 8 **[保存（Save）]** をクリックします。

リモート ストレージの SSH の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	FMC	グローバルだけ。	Admin

始める前に

- 外部リモート ストレージ システムが機能しており、Firepower Management Center からアクセスできることを確認します。

ステップ 1 **[System]** > **[Configuration]** を選択します。

ステップ 2 [リモート ストレージ デバイス（Remote Storage Device）] をクリックします。

ステップ 3 [ストレージ タイプ（Storage Type）] ドロップダウン リストから [SSH] を選択します。

ステップ 4 接続情報を追加します。

- [ホスト（Host）] フィールドに、ストレージ システムの IP アドレスまたはホスト名を入力します。
- [ディレクトリ（Directory）] フィールドに、ストレージ領域へのパスを入力します。

- [ユーザ名（Username）] フィールドにストレージ システムのユーザ名を入力し、[パスワード（Password）] フィールドにそのユーザのパスワードを入力します。接続ユーザ名の一部としてネットワーク ドメインを指定するには、ユーザ名の前にドメインを入力し、スラッシュ（/）で区切ります。
- SSH キーを使用するには、[SSH 公開キー（SSH Public Key）] フィールドの内容をコピーして authorized_keys ファイルに貼り付けます。

ステップ 5 必要に応じて、[詳細オプションの使用（Use Advanced Options）] チェックボックスをオンにして、必要なコマンドライン オプションを入力します。リモート ストレージ管理の詳細オプション（1287 ページ）を参照してください。

ステップ 6 [システムの使用方法（System Usage）] で、次の手順を実行します。

- 指定したホストにバックアップを格納するには、[バックアップに使用（Use for Backups）] を選択します。
- 指定したホストにレポートを格納するには、[レポートに使用（Use for Reports）] を選択します。

ステップ 7 設定をテストする場合は、[テスト（Test）] をクリックする必要があります。

ステップ 8 **[保存（Save）]** をクリックします。

リモート ストレージ管理の詳細オプション

Secure File Transfer Protocol（SFTP）を使用してレポートとバックアップを保存するために、ネットワーク ファイル システム（NFS）プロトコル、サーバ メッセージ ブロック（SMB）プロトコル、または SSH を選択すると、NFS、SMB、SSH マウントのマニュアル ページに記載されているいずれかのマウント バイナリ オプションを使用するために、[詳細設定オプションの使用（Use Advanced Options）] チェック ボックスを選択できます。

SMB を選択すると、次の形式で [コマンド ライン オプション（Command Line Options）] フィールドにセキュリティ モードを入力します。

```
sec=mode
```

`mode` は、リモート ストレージで使用するセキュリティ モードです。

表 *92 : SMB* セキュリティ モードの設定

モード	説明
（なし）	NULL ユーザ（名前なし）として接続します。
`krb5`	Kerberos バージョン 5 認証を使用します。
`krb5i`	Kerberos 認証とパケット署名を使用します。
`ntlm`	NTLM パスワード ハッシュを使用します。（デフォルト）

モード	説明
ntlmi	署名付きのNTLMパスワードハッシュを使用します（/proc/fs/cifs/PacketSigningEnabledがオンになっている場合またはサーバが署名を要求する場合はデフォルト）。
ntlmv2	NTLMv2パスワードハッシュを使用します。
ntlmv2i	パケット署名付きのNTLMv2パスワードハッシュを使用します。

変更調整

ユーザが行う変更をモニタし、変更が部門の推奨する標準に従っていることを確認するため、過去24時間に行われたシステム変更の詳細なレポートを電子メールで送信するようにシステムを構成できます。ユーザが変更をシステム構成に保存するたびに、変更のスナップショットが取得されます。変更調整レポートは、これらのスナップショットを組み合せて、最近のシステム変更の概要を提供します。

次の図は、変更調整レポートの[User]セクションの例を示しています。ここには、各構成の変更前の値と変更後の値の両方が一覧表示されています。ユーザが同じ構成に対して複数の変更を行った場合は、個々の変更の概要が最新のものから順に時系列でレポートに一覧表示されます。

過去24時間に行われた変更を参照できます。

変更調整の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	FMC 7000および8000シリーズ	グローバルだけ。	Admin

始める前に

- 24時間にシステムに行われた変更のメール送信されるレポートを受信する電子メールサーバを設定します。詳細については、メールリレーホストおよび通知アドレスの設定（1303ページ）を参照してください。

ステップ1 **[System]** > **[Configuration]**を選択します。

ステップ 2 [変更調整（Change Reconciliation）] をクリックします。

ステップ 3 **[有効（Enable）]** チェックボックスをオンにします。

ステップ 4 [実行する時間（Time to Run）] ドロップダウン リストから、システムが変更調整レポートを送信する時刻を選択します。

ステップ 5 [メール宛先（Email to）] フィールドにメール アドレスを入力します。

ヒント 電子メール アドレスを追加したら、いつでも [最新のレポートの再送信（Resend Last Report）] をクリックして、最新の変更調整レポートのコピーを受信者に再送信できます。

ステップ 6 ポリシーの変更を追加する場合は、[ポリシー設定を含める（Include Policy Configuration）] チェックボックスをオンにします。

ステップ 7 過去 24 時間のすべての変更を含める場合は、[全変更履歴を表示（Show Full Change History）] チェックボックスをオンにします。

ステップ 8 **[保存（Save）]** をクリックします。

関連トピック

監査ログを使って変更を調査する （401 ページ）

変更調整オプション

[ポリシー設定を含める（Include Policy Configuration）] オプションは、ポリシーの変更のレコードを変更調整レポートに含めるかどうかを制御します。これには、アクセス制御、侵入、システム、ヘルス、およびネットワーク検出の各ポリシーの変更が含まれます。このオプションを選択しなかった場合は、ポリシーの変更はどれもレポートに表示されません。このオプションは Firepower Management Center のみで使用できます。

[すべての変更履歴を表示する（Show Full Change History）] オプションは、過去 24 時間のすべての変更のレコードを変更調整レポートに含めるかどうかを制御します。このオプションを選択しなかった場合は、変更がカテゴリごとに統合された形でレポートに表示されます。

ポリシー変更のコメント

ユーザがアクセス コントロール ポリシー、侵入ポリシー、またはネットワーク分析ポリシーを変更した場合、それらのポリシー関連の変更をコメント機能を使用してトラッキングするように Firepower システムを設定することができます。

ポリシー変更のコメントが有効にされていると、管理者はコメントにアクセスして、導入で重要なポリシーが変更された理由を素早く評価できます。オプションで、侵入ポリシーおよびネットワーク分析ポリシーに対する変更を監査ログに書き込むこともできます。

ポリシーの変更を追跡するコメントの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	FMC	グローバルだけ。	Admin

ユーザがアクセス コントロール ポリシー、侵入ポリシー、またはネットワーク分析ポリシーを変更する場合に、コメントの入力を要求するように Firepower システムを設定できます。コメントを使用して、ユーザのポリシーの変更の理由を追跡できます。ポリシーの変更に関するコメントを有効にした場合、コメントをオプションまたは必須に設定できます。システムは、ポリシーに対する新しい変更が保存されるたびに、ユーザにコメントを入力するようプロンプトを出します。

ステップ 1 **[System]** > **[Configuration]**を選択します。

システム設定オプションは、左側のナビゲーション パネルに表示されます。

ステップ 2 次のいずれかのポリシー コメントの設定を行います。

- アクセス コントロール ポリシーのコメント設定には、[アクセス コントロールの設定（Access Control Preferences）] をクリックします。
- 侵入ポリシーのコメント設定には、[侵入ポリシー設定（Intrusion Policy Preferences）] をクリックします。
- ネットワーク分析ポリシーのコメント設定には、[ネットワーク分析ポリシー設定（Network Analysis Policy Preferences）] をクリックします。

ステップ 3 各ポリシー タイプに次の選択肢があります。

- [無効化（Disabled）]：変更のコメントを無効にします。
- [オプション（Optional）]：コメントの変更について記述するオプションをユーザに提供します。
- [必須（Required）]：保存する前にコメントで変更について説明するようにユーザに要求します。

ステップ 4 侵入ポリシーまたはネットワーク分析ポリシーのコメントには、次のオプションがあります。

- 侵入ポリシーのすべての変更を監査ログに書き込むには、[侵入ポリシーの変更を監査ログに書き込む（Write changes in Intrusion Policy to audit log）] をオンにします。
- ネットワーク分析ポリシーのすべての変更を監査ログに書き込むには、[ネットワーク分析ポリシーの変更を監査ログに書き込む（Write changes in Network Analysis Policy to audit log）] をオンにします。

ステップ 5 **[保存（Save）]** をクリックします。

アクセス リスト

IP アドレスとポートによって FMC へのアクセスを制限できます。デフォルトでは、任意の IP アドレスに対して以下のポートが有効化されています。

- 443（HTTPS）：Web インターフェイス アクセスに使用されます。
- 22（SSH）：CLI アクセスに使用されます。

さらに、ポート 161 で SNMP 情報をポーリングするためのアクセスも追加できます。SNMP はデフォルトで無効になっているため、SNMP アクセスルールを追加する前に、まず SNMP を有効にする必要があります。詳細については、「SNMP ポーリングの設定（1306 ページ）」を参照してください。

注意 デフォルトでは、アクセスは制限されていません。よりセキュアな環境で運用するために、特定の IP アドレスに対するアクセスを追加してから、デフォルトの **any** オプションを削除することを検討してください。

アクセス リストの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	FMC	いずれか（Any）	Admin

このアクセス リストは、外部データベース アクセスを制御しません。データベースへの外部アクセスの有効化（1263 ページ）を参照してください。

注意 FMC への接続に現在使用されている IP アドレスへのアクセスを削除し、「`IP=any port=443`」のエントリが存在しない場合、保存した時点でアクセスは失われます。

従来型デバイスのアクセス リストを設定するには、デバイスのプラットフォーム設定を使用します。従来型デバイス用のアクセスリストの設定（1337 ページ）を参照してください。

始める前に

デフォルトでは、アクセスリストには HTTPS と SSH のルールが含まれています。SNMP ルールをアクセスリストに追加するには、まず SNMP を有効にする必要があります。詳細については、SNMP ポーリングの設定（1306 ページ）を参照してください。

ステップ 1 **[System]** > **[Configuration]** を選択します。

ステップ 2 （オプション）SNMP ルールをアクセスリストに追加する場合は、[SNMP] をクリックして SNMP を設定します。デフォルトでは、SNMP は無効になっています。SNMP ポーリングの設定 （1306 ページ）を参照してください。

ステップ 3 [アクセス リスト（Access List）] をクリックします。

ステップ 4 1 つ以上の IP アドレスへのアクセスを追加するには、[ルールの追加（Add Rules）] をクリックします。

ステップ 5 [IP アドレス（IP Address）] フィールドに、IP アドレスまたはアドレスの範囲を入力するか、`any` を入力します。

ステップ 6 [SSH]、[HTTPS]、[SNMP]、またはこれらのオプションの組み合わせを選択して、これらの IP アドレスで有効にするポートを指定します。

ステップ 7 [Add] をクリックします。

ステップ 8 **[保存（Save）]** をクリックします。

関連トピック

Firepower システムの IP アドレス表記法 （20 ページ）

監査ログ

Firepower Management Center は、ユーザのアクティビティを読み取り専用監査ログに記録します。監査ログのデータは、いくつかの方法で確認できます。

- Web インターフェイスの使用：システムの監査 （397 ページ）。

  監査ログは標準イベント ビューに表示され、監査ビュー内の任意の項目に基づいて監査ログ メッセージを表示、ソート、およびフィルタリングできます。監査情報を簡単に削除したり、それに関するレポートを作成したりすることができ、ユーザが行った変更に関する詳細なレポートを表示することもできます。

- syslog への監査ログ メッセージのストリーミング：syslog への監査ログのストリーミング （1293 ページ）。.

- HTTP サーバへの監査ログ メッセージのストリーミング：HTTP サーバへの監査ログのストリーミング （1294 ページ）。

監査ログ データを外部サーバにストリーミングすると、FMC の容量を節約できますを参照してください。 外部 URL に監査情報を送信すると、システム パフォーマンスに影響を与える場合があるので注意してください。

オプションで監査ログ ストリーミングのチャネルを保護するには、TLS 証明書を使用して TLS および相互認証を有効にします。監査ログ証明書 （1295 ページ）を参照してください。

従来型デバイスも監査ログを保持します。従来型デバイスから監査ログをストリーミングする場合は、従来型デバイスからの監査ログのストリーミング （1338ページ）を参照してください。

syslog への監査ログのストリーミング

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	FMC	いずれか（Any）	Admin

この機能を有効にすると、監査ログ レコードは、syslog に次の形式で表示されます。

```
Date Time Host [Tag] Sender: User_Name@User_IP, Subsystem, Action
```

現地の日付、時刻、および発信元ホスト名の後に、角括弧で囲まれたオプション タグが続き、送信側デバイス名の後に監査ログ メッセージが続きます。

たとえば、FROMMC のタグを指定した場合は、監査ログメッセージ例は次のように表示されます。

```
Mar 01 14:45:24 localhost [FROMMC] Dev-MC7000: admin@10.1.1.2, Operations > Monitoring, Page View
```

メッセージに関連付ける重大度、ファシリティ、およびオプション タグを指定できます。タグは、syslogの監査ログ メッセージと一緒に表示されます。ファシリティはメッセージを作成するサブシステムを示し、重大度はメッセージの重大度を定義します。syslog メッセージにはファシリティおよび重大度は含まれません。これらの値はsyslogメッセージを受信するシステムにメッセージの分類方法を示す値です。

従来型デバイスから監査ログをストリーミングするには、デバイスのプラットフォーム設定を使用します：従来型デバイスからの監査ログのストリーミング （1338 ページ）。

始める前に

FMC が syslog サーバと通信できることを確認します。設定を保存すると、システムはポート 7/UDP を使用して、syslog サーバが到達可能であることを確認します。次に、システムは 514/UDP を使用して監査ログをストリーミングします。チャネルを保護している場合（（オプション）監査ログ証明書 （1295 ページ）を参照）、システムは 6514/TCP を使用します。

ステップ 1 **[System]** > **[Configuration]**を選択します。

ステップ 2 [監査ログ（Audit Log）] をクリックします。

ステップ 3 [監査ログを Syslog に送信（Send Audit Log to Syslog）] ドロップダウン メニューから、[有効（Enabled）] を選択します。

ステップ 4 [ホスト（Host）] フィールドにある syslog サーバの IP アドレスまたは完全修飾名を使用して、監査情報の宛先ホストを指定します。

ステップ 5 Syslog アラート ファシリティ （2812 ページ）で説明されているとおりに、[ファシリティ（Facility）] リストからファシリティを選択します。

ステップ 6 syslog 重大度レベル （2813 ページ）で説明されているとおりに、[重大度（Severity）] リストから重大度を選択します。

ステップ 7 オプションで、[タグ（Tag）] フィールドに、syslog メッセージとともに表示するタグ名を入力します。たとえば、syslog に送信されるすべての監査ログ レコードの先頭に「FROMMC」を付加したい場合に、このフィールドに「FROMMC」と入力します。

ステップ 8 [保存（Save）] をクリックします。
システムは、ポート 7/UDP で syslog サーバにアクセスしようとします。

HTTP サーバへの監査ログのストリーミング

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	FMC	いずれか（Any）	Admin

この機能を有効にすると、アプライアンスは、HTTP サーバに次の形式で監査ログ レコードを送信します。

```
Date Time Host [Tag] Sender: User_Name@User_IP, Subsystem, Action
```

ローカルの日付、時刻、および発信元ホスト名の後に、角括弧で囲まれたオプション タグが続き、送信側アプライアンスまたはデバイス名の後に監査ログ メッセージが続きます。

たとえば、FROMMC のタグを指定した場合は、監査ログメッセージ例は次のように表示されます。

```
Mar 01 14:45:24 localhost [FROMMC] Dev-MC7000: admin@10.1.1.2, Operations > Monitoring, Page View
```

従来型デバイスから監査ログをストリーミングするには、デバイスのプラットフォーム設定を使用します：従来型デバイスからの監査ログのストリーミング （1338 ページ）。

始める前に

デバイスが HTTP サーバと通信できることを確認します。オプションで、チャネルを保護します。監査ログ証明書 （1295 ページ）を参照してください。

ステップ 1 **[System]** > **[Configuration]**を選択します。

ステップ 2 [監査ログ（Audit Log）] をクリックします。

ステップ 3 必要に応じて、[タグ（Tag）] フィールドに、メッセージとともに表示するタグ名を入力します。たとえば、すべての監査ログ レコードの前に FROMMC を付けるには、このフィールドに FROMMC を入力します。

ステップ 4 [HTTP サーバへの監査ログの送信（Send Audit Log to HTTP Server）] ドロップダウン リストから、[有効（Enabled）] を選択します。

ステップ 5 [監査情報を送信する URL（URL to Post Audit）] フィールドに、監査情報の送信先 URL を指定します。次にリストした HTTP POST 変数を要求するリスナー プログラムに対応する URL を入力します。

- `subsystem`
- `actor`

- `event_type`
- `message`
- `action_source_ip`
- `action_destination_ip`
- 結果
- 時刻
- `tag`（定義されている場合。手順 3 を参照）

注意 暗号化されたポストを許可するには、HTTPS URL を使用します。外部 URL に監査情報を送信すると、システム パフォーマンスに影響を与える場合があります。

ステップ 6 **[保存（Save）]** をクリックします。

監査ログ証明書

Transport Layer Security（TLS）証明書を使用して、Firepower アプライアンスと信頼できる監査ログ サーバ間の通信を保護することができます。

クライアント証明書（必須）

各アプライアンス（クライアント証明書は一意）については、証明書署名要求（CSR）を生成して、署名のために認証局（CA）に送信してから、署名付き証明書をアプライアンスにインポートする必要があります。

FMC を使用して、管理対象デバイスに監査ログ証明書をインポートすることはできません。これらの証明書は各アプライアンスに固有のものであり、各アプライアンスにログインして証明書をローカルにインポートする必要があります。

- FMC の場合は、ローカルシステム設定を使用します。FMC の署名付き監査ログ クライアント証明書の取得 （1297 ページ） および FMC への監査ログ クライアント証明書のインポート （1298 ページ）。
- 7000/8000 シリーズ デバイスの場合は、ローカルシステム設定を使用します。7000/8000 シリーズ デバイスでのセキュアな監査ログ ストリーミング用の署名付きクライアント証明書の取得 （1348 ページ） 。
- ASA FirePOWER および NGIPSv の場合は、OpenSSL などのツールを使用して CSR を生成してから、CLI を使用して署名付き証明書をインポートします。**configure audit_cert import**。

サーバ証明書（オプション）

セキュリティを強化するために、Firepower アプライアンスと監査ログ サーバ間の相互認証を要求することを推奨します。相互認証を実現するには、1 つ以上の証明書失効リスト（CRL）

をロードします。これらの CRL にリストされている失効した証明書を使用して、サーバに監査ログをストリーミングすることはできません。

Firepower は、識別符号化規則（DER）形式でエンコードされた CRL をサポートしています。これらの CRL は、システムが FMC Web インターフェイスの HTTPS クライアント証明書を検証するために使用する CRL と同じであることに注意してください。

有効な監査ログ サーバ証明書を要求するには、FMC Web インターフェイスを使用します。

- FMC の場合は、ローカル システム設定を使用します。有効な監査ログ サーバ証明書の要求 （1299 ページ）。
- 従来型デバイス（7000/8000 シリーズを含む）の場合は、デバイスのプラットフォーム設定を使用します。従来型デバイス用の有効な監査ログ サーバ証明書の要求（1340ページ）。

監査ログのセキュアなストリーミング

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	FMC	いずれか（Any）	Admin

信頼できる HTTP サーバまたは syslog サーバに監査ログをストリーミングする場合、Transport Layer Security（TLS）証明書を使用して FMC とサーバ間のチャネルを保護できます。監査するアプライアンスごとに一意のクライアント証明書を生成する必要があります。

従来型デバイスに監査ログをセキュアにストリーミングする場合は、従来型デバイスからの監査ログのストリーミング （1338 ページ）を参照してください。

始める前に

クライアントおよびサーバ証明書を必須とする場合の影響については、監査ログ証明書 （1295 ページ）を参照してください。

ステップ 1 署名付きクライアント証明書を入手し、FMC にインストールします。

a) FMC の署名付き監査ログ クライアント証明書の取得 （1297 ページ）：

システム情報と指定した ID 情報に基づいて、FMC で証明書署名要求（CSR）を生成します。

CSR を認識済みの信頼できる認証局（CA）に送信して、署名付きクライアント証明書を要求します。

FMC と監査ログ サーバ間の相互認証が必要な場合、接続に使用するサーバ証明書に署名したのと同じ CA がクライアント証明書に署名する必要があります。

b) 認証局から署名付き証明書を受信した後は、その証明書を FMC にインポートします。FMC への監査ログ クライアント証明書のインポート （1298 ページ）を参照してください。

ステップ 2 Transport Layer Security（TLS）を使用するサーバとの通信チャネルを設定し、相互認証を有効にします。有効な監査ログ サーバ証明書の要求 （1299 ページ）を参照してください。

ステップ 3 まだ行っていない場合は、監査ログ ストリーミングを設定します。

syslog への監査ログのストリーミング（1293 ページ）または HTTP サーバへの監査ログのストリーミング（1294 ページ）を参照してください。

FMC の署名付き監査ログ クライアント証明書の取得

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
該当なし	いずれか（Any）	FMC	グローバルだけ。	Admin

管理対象の従来型デバイスの証明書を取得するには、7000/8000 シリーズ デバイスでのセキュアな監査ログ ストリーミング用の署名付きクライアント証明書の取得（1348 ページ）を参照してください。

重要 ハイ アベイラビリティ設定のスタンバイ Firepower Management Center では [監査ログ証明書（Audit Log Certificate）] ページを使用できません。スタンバイ Firepower Management Center からこのタスクを実行することはできません。

システムは、ベース 64 エンコードの PEM 形式で証明書要求のキーを生成します。

始める前に

次の点を考慮してください。

- 証明書をインストールするデバイスまたはアプライアンスで、証明書署名要求（CSR）を生成する必要があります。（たとえば、アプライアンス A でデバイス B の証明書署名要求は生成できません。）各デバイスおよびアプライアンスで固有の証明書署名要求を生成する必要があります。
- セキュリティを確保するには、グローバルに認識された信頼できる認証局（CA）を使用して、証明書に署名します。
- アプライアンスと監査ログ サーバ間で相互認証が必要な場合は、同じ認証局によってクライアント証明書とサーバ証明書の両方が署名される必要があります。

ステップ 1 **[System]** > **[Configuration]** を選択します。

ステップ 2 [監査ログ証明書（Audit Log Certificate）] をクリックします。

ステップ 3 [新規 CSR の生成（Generate New CSR）] をクリックします。

ステップ 4 [国名（2 文字のコード）（Country Name (two-letter code)）] フィールドに国番号を入力します。

ステップ 5 [都道府県（State or Province）] フィールドに、都道府県名を入力します。

ステップ 6 [市区町村（Locality or City）] を入力します。

ステップ 7 [組織（Organization）] の名前を入力します。

ステップ 8 [組織単位（部署名）（Organizational Unit (Department)）] の名前を入力します。

ステップ 9 [共通名（Common Name）] フィールドに、証明書を要求するサーバの完全修飾ドメイン名を入力します。

（注） 共通名と DNS ホスト名が一致しないと、監査ログのストリーミングは失敗します。

ステップ 10 [生成（Generate）] をクリックします。

ステップ 11 テキスト エディタで、新しい空のファイルを開きます。

ステップ 12 証明書要求のテキスト ブロック全体（`BEGIN CERTIFICATE REQUEST` 行と `END CERTIFICATE REQUEST` 行を含む）をコピーして、空のテキスト ファイルに貼り付けます。

ステップ 13 このファイルを *clientname*`.csr` として保存します。*clientname* は、証明書を使用する予定のアプライアンスの名前にします。

ステップ 14 [閉じる（Close）] をクリックします。

次のタスク

- この手順の「はじめる前に」セクションのガイドラインを使用して選択した認証局に、証明書署名要求を送信します。
- 署名された証明書を受け取ったら、アプライアンスにインポートします。FMC への監査ログ クライアント証明書のインポート （1298 ページ）を参照してください。

FMC への監査ログ クライアント証明書のインポート

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	FMC	グローバルだけ。	Admin

FMC ハイ アベイラビリティ設定では、アクティブ ピアを使用する必要があります。

ASA FirePOWER および NGIPSv の場合は、CLI を使用して署名付き証明書をインポートします。**configure audit_cert import**。7000/8000 シリーズ デバイスの場合は、デバイスのローカル Web インターフェイスでシステム設定（**[System]** > **[Configuration]**）を使用します。7000/8000 シリーズ デバイスでのセキュアな監査ログ ストリーミング用の署名付きクライアント証明書の取得 （1348 ページ）。

始める前に

- FMC の署名付き監査ログ クライアント証明書の取得 （1297 ページ）。
- 正しいアプライアンスの署名付き証明書をインポートしていることを確認します。各証明書は、アプライアンスやデバイスごとに異なります。

- 証明書を生成した署名認証局から中間 CA を信頼するように要求された場合は、必要な証明書チェーン（証明書パスとも呼ばれる）を提供します。クライアント証明書に署名した CA は、証明書チェーンのいずれの中間証明書に署名した CA と同じである必要があります。

ステップ 1 FMC で、**[System]** > **[Configuration]** を選択します。

ステップ 2 [監査ログ証明書（Audit Log Certificate）] をクリックします。

ステップ 3 [監査クライアント証明書のインポート（Import Audit Client Certificate）] をクリックします。

ステップ 4 テキスト エディタでクライアント証明書を開いて、`BEGIN CERTIFICATE` の行と `END CERTIFICATE` の行を含むテキストのブロック全体をコピーします。このテキストを [クライアント証明書（Client Certificate）] フィールドに貼り付けます。

ステップ 5 秘密キーをアップロードするには、秘密キー ファイルを開いて、`BEGIN RSA PRIVATE KEY` の行と `END RSA PRIVATE KEY` の行を含むテキストのブロック全体をコピーします。このテキストを [秘密キー（Private Key）] フィールドに貼り付けます。

ステップ 6 必要な中間証明書をすべて開いて、それぞれのテキストのブロック全体をコピーして、[証明書チェーン（Certificate Chain）] フィールドに貼り付けます。

ステップ 7 **[保存（Save）]** をクリックします。

有効な監査ログ サーバ証明書の要求

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	FMC	グローバルだけ。	Admin

システムは、識別符号化規則（DER）形式でインポートされている CRL を使用した、監査ログ サーバ証明書の検証をサポートしています。

（注） CRL を使用して証明書を確認する場合、システムは、監査ログ サーバ証明書の検証と、アプライアンスと Web ブラウザの間の HTTP 接続を保護する証明書の検証の両方に、同じ CRL を使用します。

重要 ハイ アベイラビリティ ペアのスタンバイ Firepower Management Center でこの手順を実行することはできません。

始める前に

- 相互認証を必須とし、証明書失効リスト（CRL）を使用して証明書の有効性を保持する場合の影響について説明します。監査ログ証明書 （1295 ページ）を参照してください。
- 監査ログのセキュアなストリーミング（1296ページ）に記載されている手順およびその手順で参照されているトピックに従って、クライアント証明書を取得してインポートします。

ステップ 1 FMC で、**[System]** > **[Configuration]** を選択します。

ステップ 2 [監査ログ証明書（Audit Log Certificate）] をクリックします。

ステップ 3 Transport Layer Security を使用して監査ログを安全に外部サーバへストリーミングするには、[TLSの有効化（Enable TLS）] 選択します。

ステップ 4 検証せずにサーバ証明書を受け入れる場合（非推奨）、次を実行します。

a) [相互認証の有効化（Enable Mutual Authentication）] をオフにします。

b) [保存（Save）] をクリックして、残りの手順をスキップします。

ステップ 5 監査ログ サーバの証明書を検証するには、[相互認証の有効化（Enable Mutual Authentication）] をオンにします。

ステップ 6 （相互認証を有効にした場合）無効な証明書を自動的に認識するには、次を実行します。

a) [CRLの取得の有効化（Enable Fetching of CRL）] をオンにします。

（注） CRL のフェッチを有効にすると、定期的に CRL を更新するスケジュール タスクが作成されます。

b) 既存の CRL ファイルへの有効な URL を入力して、[CRL の追加（Add CRL）] をクリックします。

最大 25 個まで CRL の追加を繰り返します。

c) [CRL の更新（Refresh CRL）] をクリックして現在の CRL をロードするか、指定した URL から CRL をロードします。

ステップ 7 クライアント証明書を作成したものと同じ認証局によって生成された有効なクライアント証明書があることを確認します。

ステップ 8 [保存（Save）] をクリックします。

次のタスク

（オプション）CRL 更新の頻度を設定します。証明書失効リストのダウンロードの設定 （241 ページ）を参照してください。

FMC での監査ログ クライアント証明書の表示

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	FMC	グローバルだけ。	Admin

ログインしているアプライアンスの監査ログ クライアント証明書のみ表示できます。 FMC ハイ アベイラビリティ ペアでは、アクティブ ピアのみで証明書を表示できます。

従来型デバイスで監査ログ証明書を表示するには、7000/8000 シリーズ デバイスの Web インターフェイスでシステム設定を使用するか、CLI で **show audit_cert** を使用します。

ステップ 1 **[System]** > **[Configuration]**を選択します。

ステップ 2 [監査ログ証明書（Audit Log Certificate）] をクリックします。

ダッシュボード設定

ダッシュボードでは、ウィジェットを使用することにより、現在のシステム ステータスが一目でわかります。ウィジェットは小さな自己完結型コンポーネントであり、Firepower システムのさまざまな側面に関するインサイトを提供します。Firepower システムには、事前定義された複数のダッシュボード ウィジェットが付属しています。

[カスタム分析（Custom Analysis）] ウィジェットがダッシュボードで有効になるように、Firepower Management Center を設定できます。

関連トピック

ダッシュボードについて （321 ページ）

ダッシュボードのカスタム分析ウィジェットの有効化

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	FMC	グローバルだけ。	Admin

[カスタム分析（Custom Analysis）] ダッシュボード ウィジェットを使用して、柔軟でユーザによる構成が可能なクエリに基づいてイベントのビジュアル表現を作成します。

ステップ 1 **[System]** > **[Configuration]**を選択します。

ステップ 2 [ダッシュボード（Dashboard）] をクリックします。

ステップ 3 ユーザが [カスタム分析（Custom Analysis）] ウィジェットをダッシュボードに追加できるようにするには、[カスタム分析ウィジェットの有効化（Enable Custom Analysis Widgets）] チェックボックスをオンにします。

ステップ 4 **[保存（Save）]** をクリックします。

DNS キャッシュ

イベント表示ページで、IP アドレスを自動的に解決するようにシステムを設定できます。また、アプライアンスによって実行される DNS キャッシュの基本的なプロパティを設定できます。DNS キャッシングを設定すると、追加のルックアップを実行せずに、以前に解決した IP アドレスを識別できます。これにより、IP アドレスの解決が有効になっている場合に、ネットワーク上のトラフィックの量を減らし、イベントページの表示速度を速めることができます。

DNS キャッシュ プロパティの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	FMC	グローバルだけ。	Admin

DNS 解決のキャッシングは、以前に解決された DNS ルックアップのキャッシングを許可するシステム全体の設定です。

ステップ 1 **[System]** > **[Configuration]** を選択します。

ステップ 2 [DNS キャッシュ（DNS Cache）] を選択します。

ステップ 3 [DNS 解決のキャッシング（DNS Resolution Caching）] ドロップダウン リストから、次のいずれかを選択します。

- [有効化（Enabled）]：キャッシングを有効にします。
- [無効化（Disabled）]：キャッシングを無効にします。

ステップ 4 [DNS キャッシュ タイムアウト（分）（DNS Cache Timeout（in minutes））] フィールドで、非アクティブのために削除されるまで DNS エントリがメモリ内にキャッシュされる時間（分単位）を入力します。

デフォルトは 300 分（5 時間）です。

ステップ 5 [保存（Save）] をクリックします。

関連トピック

イベント ビュー設定の設定 （43 ページ）
管理インターフェイス （1266 ページ）

電子メールの通知

次の処理を行う場合は、メール ホストを設定します。

- イベントベースのレポートの電子メール送信
- スケジュールされたタスクのステータス レポートの電子メール送信
- 変更調整レポートの電子メール送信
- データプルーニング通知の電子メール送信
- 検出イベント、インパクト フラグ、相関イベント アラート、侵入イベント アラート、およびヘルス イベント アラートでの電子メールの使用

電子メール通知を設定する場合、システムとメール リレー ホスト間の通信に使用する暗号化方式を選択し、必要に応じて、メール サーバの認証クレデンシャルを指定できます。設定した後、接続をテストできます。

メール リレー ホストおよび通知アドレスの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	FMC	グローバルだけ。	Admin

ステップ 1 **[System]** > **[Configuration]**を選択します。

ステップ 2 [電子メール通知（Email Notification）] をクリックします。

ステップ 3 [メール リレー ホスト（Mail Relay Host）] フィールドで、使用するメール サーバのホスト名または IP アドレスを入力します。入力したメール ホストはアプライアンスからのアクセスを許可している**必要があります**。

ステップ 4 [ポート番号（Port Number）] フィールドに、電子メール サーバで使用するポート番号を入力します。

一般的なポートには次のものがあります。

- 25。暗号化を使用しない場合
- 465。SSLv3 を使用する場合
- 587。TLS を使用する場合

ステップ 5 [暗号化方式（Encryption Method）] を選択します。

- [TLS]：Transport Layer Security を使用して通信を暗号化します。
- [SSLv3]：セキュア ソケット レイヤを使用して通信を暗号化します。
- [なし（None）]：暗号化されていない通信を許可します。

（注） アプライアンスとメール サーバとの間の暗号化された通信では、証明書の検証は不要です。

ステップ 6 [送信元アドレス（From Address）] フィールドに、アプライアンスから送信されるメッセージの送信元電子メール アドレスとして使用する有効な電子メール アドレスを入力します。

ステップ 7 必要に応じて、メール サーバに接続する際にユーザ名とパスワードを指定するには、[認証を使用（Use Authentication）] を選択します。[Username] フィールドにユーザ名を入力します。パスワードを [Password] フィールドに入力します。

ステップ 8 設定したメール サーバを使用してテスト メールを送信するには、[Test Mail Server Settings] をクリックします。
テストの成功または失敗を示すメッセージがボタンの横に表示されます。

ステップ 9 **[保存（Save）]** をクリックします。

言語の選択

[言語（Language）] ページを使用して、Web インターフェイス用に異なる言語を指定できます。

Web インターフェイスの言語の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	FMC	グローバルだけ。	Admin

ここで指定した言語は、すべてのユーザの Web インターフェイスに使用されます。次の中から選択できます。

- 英語
- 中国語（簡体字）
- 中国語（繁体字）
- 日本語
- 韓国語

7000/8000 シリーズ デバイスの言語を設定するには、デバイスのプラットフォーム設定を使用します。7000/8000 シリーズ Web インターフェイスの言語の設定 （1343 ページ）。

ステップ 1 **[System]** > **[Configuration]** を選択します。

ステップ 2 [言語（Language）] をクリックします。

ステップ 3 使用する言語を選択します。

ステップ 4 **[保存（Save）]** をクリックします。

ログイン バナー

[ログイン バナー（Login Banner）] ページを使用して、セキュリティ アプライアンスまたは共有ポリシーのセッション バナー、ログイン バナー、カスタム メッセージ バナーを指定できます。

バナーのテキストにはスペースを使用できますが、タブは使用できません。バナーには複数行のテキストを指定できます。テキストに空の行が含まれている場合、バナーでは、その行が改行（CR）として表示されます。使用できるのは、改行（Enter キーを押す）を含む ASCII 文字だけです。改行は 2 文字としてカウントされます。

Telnet または SSH を介してセキュリティ アプライアンスにアクセスしたときに、バナー メッセージを処理するのに十分なシステム メモリがなかった場合や、バナー メッセージの表示を試行して TCP 書き込みエラーが発生した場合には、セッションが閉じます。

ログイン バナーのカスタマイズ

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	FMC	いずれか（Any）	Admin

従来型デバイスのログイン バナーをカスタマイズするには、デバイスのプラットフォーム設定を使用します。従来型デバイス用のログイン バナーのカスタマイズ （1344 ページ）を参照してください。

ステップ 1 **[System]** > **[Configuration]** を選択します。

ステップ 2 [ログイン バナー（Login Banner）] を選択します。

ステップ 3 [カスタム ログイン バナー（Custom Login Banner）] フィールドに、使用するログイン バナー テキストを入力します。

ステップ 4 **[保存（Save）]** をクリックします。

SNMP ポーリング

Simple Network Management Protocol （SNMP）のポーリングを有効にできます。SNMP 機能は、SNMP プロトコルのバージョン 1、2、3 をサポートします。この機能を使用すると、標準 Management Information Base（MIB）にアクセスできます。MIB には、連絡先、管理、場所、

サービス情報、IP アドレッシングやルーティングの情報、トランスミッション プロトコルの使用状況の統計などのシステムの詳細が含まれます。

（注） SNMP プロトコルの SNMP バージョンを選択する場合、SNMPv2 では読み取り専用コミュニティのみがサポートされ、SNMPv3 では読取り専用ユーザのみがサポートされることに注意してください。SNMPv3 は、AES128 での暗号化をサポートします。

SNMP ポーリングを有効にすると、システムで SNMP トラップを送信できなくなり、MIB の情報はネットワーク管理システムによるポーリングでのみ使用可能になります。

SNMP ポーリングの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	FMC	いずれか（Any）	Admin

従来型デバイスでSNMPポーリングを設定するには、デバイスのプラットフォーム設定を使用します。従来型デバイスでの SNMP ポーリングの設定 （1346 ページ）を参照してください。

始める前に

使用するコンピュータごとにSNMPアクセスを追加し、システムをポーリングします。アクセス リストの設定 （1291 ページ）を参照してください。

（注） SNMP MIB には展開の攻撃に使用される可能性がある情報が含まれています。SNMP アクセスのアクセス リストを MIB のポーリングに使用される特定のホストに制限することを推奨します。SNMPv3 を使用し、ネットワーク管理アクセスには強力なパスワードを使用することも推奨します。

ステップ 1 **[System]** > **[Configuration]** を選択します。

ステップ 2 [SNMP] をクリックします。

ステップ 3 [SNMPバージョン（SNMP Version）] ドロップダウン リストから、使用する SNMP バージョンを選択します。

- [Version 1] または [Version 2]：[Community String] フィールドに読み取り専用の SNMP コミュニティ名を入力してから、手順の最後までスキップします。

  （注） SNMP コミュニティストリング名には、特殊文字（<>/%#&?', etc.）を使用できません。

- [バージョン3（Version 3）]：[ユーザを追加（Add User）] をクリックすると、ユーザ定義ページが表示されます。SNMPv3 は、読み取り専用ユーザと AES128 による暗号化のみをサポートしています。

ステップ 4 ユーザ名を入力します。

ステップ 5 [認証プロトコル（Authentication Protocol）] ドロップダウン リストから、認証に使用するプロトコルを選択します。

ステップ 6 [認証パスワード（Authentication Password）] フィールドに SNMP サーバの認証に必要なパスワードを入力します。

ステップ 7 [パスワードの確認（Verify Password）] フィールドに、認証パスワードを再度入力します。

ステップ 8 使用するプライバシー プロトコルを [プライバシー プロトコル（Privacy Protocol）] リストから選択するか、プライバシー プロトコルを使用しない場合は [なし（None）] を選択します。

ステップ 9 [プライバシー パスワード（Privacy Password）] フィールドに SNMP サーバで必要な SNMP プライバシー キーを入力します。

ステップ 10 [パスワードの確認（Verify Password）] フィールドに、プライバシー パスワードを再度入力します。

ステップ 11 [Add] をクリックします。

ステップ 12 **[保存（Save）]** をクリックします。

時刻および時刻同期

FirePOWER システムを正常に動作させるには、Firepower Management Center とその管理対象デバイスのシステム時刻を同期させることが不可欠です。FMC 初期設定時に NTP サーバを指定することを推奨しますが、初期設定の完了後に、このセクションの情報を使用して、時刻同期設定を確立または変更することができます。

FMC とすべてのデバイスのシステム時刻を同期させるには、Network Time Protocol（NTP）サーバを使用します。

⚠

注意 Firepower Management Center と管理対象デバイスの時刻が同期していないと、意図しない結果になることがあります。

FMC と管理対象デバイスの時刻を同期するには、次を参照してください。

- 推奨： FMC の時刻を NTP サーバに同期 （1308 ページ）

  このトピックには、FMC と同期するように管理対象デバイスを設定する手順のリンクが含まれています。

- その他の場合： ネットワーク NTP サーバにアクセスせずに時刻を同期 （1309 ページ）

  このトピックには、FMC と同期するように管理対象デバイスを設定する手順のリンクが含まれています。

FMC の時刻を NTP サーバに同期

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	FMC	グローバルだけ。	Admin

Firepower Management Center とすべての管理対象デバイス間で適切な時刻同期を維持する最適な方法は、ネットワークで NTP サーバを使用することです。

始める前に

次の点に注意してください。

- FMC および管理対象デバイスがネットワーク NTP サーバにアクセスできない場合は、この手順を使用しないでください。代わりに、ネットワーク NTP サーバにアクセスせずに時刻を同期 （1309 ページ）を参照してください。
- 信頼できない NTP サーバを指定しないでください。
- NTP サーバへの接続では、構成されたプロキシ設定は使用されません。

注意 Firepower Management Center が再起動され、ここで指定したものとは異なる NTP サーバ レコードを DHCP サーバが設定した場合、DHCP 提供の NTP サーバが代わりに使用されます。この状況を回避するには、同じ NTP サーバを設定するように DHCP サーバを設定します。

ステップ 1 **[System]** > **[Configuration]**を選択します。

ステップ 2 [Time Synchronization] をクリックします。

ステップ 3 [NTPを使用して時間を提供（Serve Time via NTP）] が [有効（Enabled）] の場合、[無効（Disabled）] を選択して、NTP サーバの FMC を無効にします。

ステップ 4 [マイクロックの設定（Set My Clock）] オプションには、[NTPの接続元（Via NTP from）] を選択して、NTP サーバのホスト名または IP アドレスを入力します。

組織内に連携する NTP サーバがある場合は、複数の NTP サーバをカンマ区切りのリストで入力します。

ステップ 5 [保存（Save）] をクリックします。

次のタスク

管理対象デバイスでは同じ NTP サーバを使用して同期するように設定します。

- デバイスのプラットフォーム設定の構成：脅威に対する防御のための NTP 時刻同期の設定 （1406 ページ）および従来型デバイスの時刻を NTP サーバに同期 （1344 ページ）。
- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

ネットワーク NTP サーバにアクセスせずに時刻を同期

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	FMC	グローバルだけ。	Admin

デバイスがネットワーク NTP サーバに直接アクセスできない、または組織内にネットワーク NTP サーバがない場合は、物理ハードウェア Firepower Management Center を NTP サーバとして使用できます。

重要 仮想 Firepower Management Center を NTP サーバとして使用しません。

ステップ 1 Firepower Management Center でシステム時刻を手動で設定するには、次の手順を実行します。

a) **[System]** > **[Configuration]**を選択します。
b) [Time Synchronization] をクリックします。
c) [NTP を使用して時間を提供（Serve Time via NTP）] が [有効（Enabled）] の場合、[無効（Disable）] を選択します。
d) [保存（Save）] をクリックします。
e) [マイクロックの設定（Set My Clock）] で、[ローカル設定で手動（Manually in Local Configuration）] を選択します。
f) **[Save（保存）]** をクリックします。
g) 画面の左側のナビゲーション パネルで [時間（Time）] をクリックします。
h) [時間の設定（Set Time）] ドロップダウン リストを使用して時間を設定します。
i) 表示されるタイムゾーンが UTC ではない場合、クリックして、タイムゾーンを [UTC] に設定します。
j) **[Save（保存）]** をクリックします。
k) [Done] をクリックします。
l) [Apply] をクリックします。

ステップ 2 Firepower Management Center を NTP サーバとして機能するように設定します。

a) 画面の左側のナビゲーション パネルで [時刻同期（Time Synchronization）] をクリックします。
b) [NTPを使用して時間を提供（Serve Time via NTP）] で、[有効（Enabled）] を選択します。
c) **[Save（保存）]** をクリックします。

ステップ 3 管理対象デバイスでは Firepower Management Center NTP サーバを使用して同期するように設定します。

a) 管理対象デバイスに割り当てられたプラットフォーム設定ポリシーの [Time Synchronization] 設定で、[Via NTP from Management Center] に同期するようにクロックを設定します。
b) 管理対象デバイスへの変更を導入します。

手順については、次を参照してください。

- Firepower Threat Defense デバイスの場合は、次を参照してください。 脅威に対する防御のための NTP 時刻同期の設定 （1406 ページ）
- その他すべてのデバイスについては、次を参照してください。 従来型デバイスの時刻を NTP サーバに同期 （1344 ページ）

時刻同期の設定の変更について

- NTP を使用して時刻を提供するように FMC を設定してから、後でそれを無効にした場合、管理対象デバイスの NTP サービスは引き続き FMC と時刻を同期しようとします。新しい時刻ソースを確立するには、すべての該当するプラットフォーム設定ポリシーを更新および再展開する必要があります。
- Firepower Management Center を NTP サーバとして設定した**後に**時刻を手動で変更する必要がある場合、NTP オプションを無効にして時刻を手動で変更してから NTP オプションを再度有効にする必要があります。

現在のシステム時刻、ソース、および**NTP**サーバ接続ステータスの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	FMC	グローバルだけ。	Admin

[ユーザ設定（User Preferences）] の [タイムゾーン（Time Zone）] ページで設定したタイムゾーン（デフォルトでは America/New York）を使用すると、ほとんどのページでローカル時刻で時刻設定が表示されますが、アプライアンスには UTC 時間を使用して格納されます。

さらに、現在の時刻は [時間（Time）] ページの上部に UTC で表示されます（ローカル時刻は手動時計設定オプションで表示されます（有効になっている場合））。

制約事項

タイムゾーン機能（[ユーザ設定（User Preferences）]）は、デフォルトのシステム クロックが UTC 時間に設定されていることを前提としています。システム時刻を変更しようとしないでください。システム時刻の UTC からの変更はサポートされていません。また、システム時刻を変更した場合はデバイスを再イメージ化してサポートされていない状態から回復させる必要があります。

（注） 7000および8000シリーズハードウェアデバイスで時刻および時刻源情報を表示する場合は、7000/8000 シリーズ デバイスのシステム時刻の表示 （1355 ページ）を参照してください。

ステップ 1 **[System]** > **[Configuration]**を選択します。

ステップ 2 [時間（Time）] をクリックします。

アプライアンスで NTP サーバを使用する場合、テーブル エントリについては、NTP サーバのステータス （1311 ページ）を参照してください。

NTP サーバのステータス

NTP サーバから時刻を同期する場合は、[時間（Time）] ページ（[システム（System）] > [設定（Configuration）] を選択）で接続ステータスを確認できます。

表 *93 : NTP* ステータス

カラム	説明
NTP サーバ	設定済みの NTP サーバの IP アドレスまたは名前。
ステータス	NTP サーバの時間同期のステータス。 • [使用中（Being Used）] は、アプライアンスが NTP サーバと同期していることを示します。 • [Available] は、NTP サーバが使用可能であるものの、時間がまだ同期していないことを示します。 • [Not Available] は、NTP サーバが構成に含まれているものの、NTP デーモンがその NTP サーバを使用できないことを示します。 • [Pending] は、NTP サーバが新しいか、または NTP デーモンが最近再起動されたことを示します。この値は、時間の経過とともに [Being Used]、[Available]、または [Not Available] に変わるはずです。 • [不明（Unknown）] は、NTP サーバのステータスが不明であることを示します。
オフセット	アプライアンスと構成済みの NTP サーバ間の時間の差（ミリ秒）。負の値はアプライアンスの時間が NTP サーバより遅れていることを示し、正の値は進んでいることを示します。

カラム	説明
Last Update	NTP サーバと最後に時間を同期してから経過した時間（秒数）。NTP デーモンは、いくつかの条件に基づいて自動的に同期時間を調整します。たとえば、更新時間が大きい（300 秒など）場合、それは時間が比較的安定しており、NTP デーモンが小さい更新増分値を使用する必要がないと判断したことを示します。

グローバル ユーザ構成時の設定

グローバル ユーザの設定は、Firepower Management Center のすべてのユーザに影響します。[User Configuration] ページで次の設定を行います（**[System]** > **[Configuration]** > **[User Configuration]**）。

- [パスワード再使用制限（Password Reuse Limit）]：ユーザの最新の履歴の中で再利用できないパスワードの数。この制限は、すべてのユーザの Web インターフェイスに適用されます。`admin` ユーザの場合、これは CLI/シェル アクセスにも適用されます。システムは各アクセス形式に対して個別のパスワード リストを維持します。制限をゼロに設定すると（デフォルト）パスワードの再利用に制限は課せられません。パスワードの再使用制限の設定 （1313 ページ）を参照してください。
- [成功したログインの追跡（Track Successful Logins）]：Firepower Management Center へのログインの成功をユーザごとにアクセス方式（Web インターフェイスまたは CLI/シェル）別に追跡する日数。ユーザがログインすると、使用しているインターフェイスで成功したログイン回数が表示されます。[成功したログインの追跡（Track Successful Logins）] をゼロに設定すると（デフォルト）、システムは成功したログイン アクティビティを追跡せず、レポートもしません。成功したログインの追跡（1313ページ）を参照してください。
- [ログイン失敗の最大数（Max Number of Login Failures）]：ユーザが誤った Web インターフェイスのログイン クレデンシャルを連続して入力できる回数。この回数を超えると、設定されている時間にわたって一時的にアカウントにアクセスできなくなります。一時的なロックアウトが適用されている間にユーザがログインを試行し続けた場合：
  - 一時的なロックアウトが適用されていることをユーザに通知せず、（有効なパスワードを使用したとしても）システムはそのアカウントへのアクセスを拒否します。
  - ログイン試行のたびにシステムはそのアカウントの失敗ログイン数を増やし続けます。
  - ユーザが個人の [ユーザ設定（User Configuration）] ページでそのアカウントに設定した [ログイン失敗の最大数（Maximum Number of Failed Logins）] を超えた場合、管理者ユーザがそのアカウントを再アクティブ化するまではそのアカウントはロックアウトされます。

- [一時的にユーザをロックアウトする分単位の時間の設定（Set Time in Minutes to Temporarily Lockout Users）]：[ログイン失敗の最大数（Max Number of Failed Logins）] がゼロ以外の場合にユーザが一時的に Web インターフェイスからロックアウトされる分単位の時間。

パスワードの再使用制限の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	FMC	グローバル	Admin

[パスワード再利用の制限（Password Reuse Limit）] を有効にすると、システムに FMC ユーザの暗号化されたパスワード履歴が保持されます。ユーザはパスワード履歴内のパスワードを再利用できません。各ユーザの保存されたパスワードの数をアクセス方式（Webインターフェイスまたは CLI/シェル）ごとに指定できます。ユーザの現在のパスワードはこの番号に対してカウントされます。制限を低くすると、システムは履歴から古い順にパスワードを削除します。制限を高くすると、削除されたパスワードが復元されません。

ステップ 1 **[System]** > **[Configuration]** を選択します。

ステップ 2 [ユーザ設定（User Configuration）] をクリックします。

ステップ 3 [パスワード再利用制限（Password Reuse Limit）] を履歴に維持したいパスワードの数（最大 256）に設定します。

パスワード再利用のチェックを無効にするには、0 を入力します。

ステップ 4 **[保存（Save）]** をクリックします。

成功したログインの追跡

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	FMC	グローバル	Admin

この手順を使用して、各ユーザの成功したログインの追跡を指定した日数の間、有効にします。この追跡が有効になっている場合は、ユーザが Web インターフェイスまたは CLI/シェルにログインしたときにシステムは成功したログイン数を表示します。

（注） 日数を少なくすると、システムはログインのレコードを古いものから削除します。制限値を大きくすると、システムはその日数からカウントを復元しません。その場合、成功したログインの復元された数は、一時的に実際の番号よりも少なくなる場合があります。

ステップ 1 **[System]** > **[Configuration]**を選択します。

ステップ 2 [ユーザ設定（User Configuration）] をクリックします。

ステップ 3 [成功したログイン日数の追跡（Track Successful Login Days）] を成功したログインを追跡する日数（最大365）に設定します。

ログインの追跡を無効にするには、0 を入力します。

ステップ 4 **[保存（Save）]** をクリックします。

一時的なロックアウトの有効化

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	FMC	グローバル	Admin

システムがロックアウトを有効にする前に連続して失敗したログイン試行を許可する回数を指定して、一時的な時限ロックアウト機能を有効にします。

ステップ 1 **[System]** > **[Configuration]** を選択します。

ステップ 2 [ユーザ設定（User Configuration）] をクリックします。

ステップ 3 [ログイン失敗の最大数（Max Number of Login Failures）] をユーザが一時的にロックアウト されるまで連続して失敗できるログイン試行の最大回数に指定します。

一時的なロックアウトを無効にするには、ゼロを入力します。

ステップ 4 [ユーザを一時的にロックアウトする分単位の時間（Time in Minutes to Temporarily Lockout Users）] は一時的なロックアウトをトリガーしたユーザをロックアウトする分数に設定します。

この値がゼロの場合は、[ログイン失敗最大数（Max Number of Login Failures）] がゼロ以外でも、ユーザはログインの再試行を待機する必要はありません。

ステップ 5 **[保存（Save）]** をクリックします。

セッション タイムアウト

無人ログインセッションは、セキュリティ上のリスクを生じさせる場合があります。ユーザのログインセッションが非アクティブになったためにタイムアウトするまでのアイドル時間を設定できます。

システムを長期間にわたってパッシブかつセキュアにモニタする予定のシナリオでは、特定のWebインターフェイスのユーザがタイムアウトしないように設定できることに注意してください。メニューオプションへの完全なアクセス権がある管理者ロールのユーザは、侵害が生じる場合、余分のリスクを生じさせますが、セッションタイムアウトから除外することはできません。

セッション タイムアウトの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	FMC	いずれか（Any）	Admin

従来型デバイスのセッションタイムアウトを設定するには、デバイスのプラットフォーム設定を使用します。従来型デバイスのセッションタイムアウトの設定（1345ページ）を参照してください。

ステップ 1 **[System]** > **[Configuration]**を選択します。

ステップ 2 [シェル タイムアウト（Shell Timeout）] をクリックします。

ステップ 3 セッション タイムアウトの設定

- Web インターフェイス（FMC のみ）：[ブラウザセッションタイムアウト（分）（Browser Session Timeout (Minutes)）] を設定します。デフォルトの値は `60` で、最大値は `1440`（24 時間）です。

  このセッション タイムアウトからユーザを除外する場合は、Web インターフェイスでの内部ユーザの追加（57 ページ）を参照してください。

- CLI：[シェルタイムアウト（分）（Shell Timeout (Minutes)）] フィールドを設定します。デフォルトの値は `0` で、最大値は `1440`（24 時間）です。

ステップ 4 **[保存（Save）]** をクリックします。

脆弱性マッピング

サーバのディスカバリ イベント データベースにアプリケーション ID が含まれており、トラフィックのパケット ヘッダにベンダーおよびバージョンが含まれる場合、Firepower システム

は、そのアドレスから送受信されるすべてのアプリケーション プロトコル トラフィックについて、脆弱性をホスト IP アドレスに自動的にマップします。

パケットにベンダー情報もバージョン情報も含まれないサーバすべてに対して、システムでこれらのベンダーとバージョンレスのサーバのサーバ トラフィックと脆弱性を関連付けるかどうかを設定できます。

たとえば、ホストがヘッダーにベンダーまたはバージョンが含まれていないSMTP トラフィックを提供しているとします。システム設定の [脆弱性マッピング（Vulnerability Mapping）] ページでSMTPサーバを有効にしてから、そのトラフィックを検出するデバイスを管理するFirepower Management Centerにその設定を保存した場合、SMTP サーバと関連付けられているすべての脆弱性がそのホストのホスト プロファイルに追加されます。

ディテクタがサーバ情報を収集して、それをホストプロファイルに追加しますが、アプリケーション プロトコル ディテクタは脆弱性のマッピングに使用されません。これは、カスタム アプリケーション プロトコル ディテクタにベンダーまたはバージョンを指定できず、また脆弱性マッピング用のサーバを選択できないためです。

サーバの脆弱性のマッピング

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	保護	FMC	グローバルだけ	Admin

ステップ 1 **[System]** > **[Configuration]**を選択します。

ステップ 2 [脆弱性マッピング（Vulnerability Mapping）] を選択します。

ステップ 3 次の選択肢があります。

- ベンダーまたはバージョンの情報が含まれていないアプリケーションプロトコル トラフィックを受信するホストに、サーバの脆弱性がマップされないようにするには、そのサーバのチェックボックスをオフにします。
- ベンダーまたはバージョンの情報が含まれていないアプリケーションプロトコル トラフィックを受信するホストに、サーバの脆弱性がマップされるようにするには、そのサーバのチェックボックスをオフにします。

ヒント [有効（Enabled）] の横にあるチェックボックスを使用すると、すべてのチェックボックスを一度にオンまたはオフにできます。

ステップ 4 **[保存（Save）]** をクリックします。

リモート コンソールのアクセス管理

サポート対象システム上でリモート アクセスを行うため、VGA ポート（デフォルト）または物理アプライアンス上のシリアル ポートを介して Linux システムのコンソールを使用できます。[コンソール設定（Console Configuration）] ページを使用して組織の Firepower 展開環境の物理レイアウトに最も適したオプションを選択します。

（注） [コンソール設定（Console Configuration）] ページからは、リモート コンソールのアクセス管理を設定する他に、Firepower Management Center の CLI を有効または無効にすることができます。詳細については、Firepower Management Center のコマンド ライン リファレンス（3363 ページ）を参照してください。

サポートされている物理ハードウェア ベースの Firepower システムでは、Serial Over LAN（SOL）接続のデフォルト管理インターフェイス（`eth0`）で Lights-Out 管理（LOM）を使用すると、システムの管理インターフェイスにログインすることなく、リモートでシステムをモニタまたは管理できます。アウトオブバンド管理接続のコマンドライン インターフェイスを使用すると、シャーシのシリアル番号の表示や状態（ファン速度や温度など）のモニタなどの、限定タスクを実行できます。

LOM は、システムとシステムを管理するユーザの両方で有効にする必要があります。システムとユーザを有効にした後、サードパーティ製の Intelligent Platform Management Interface（IPMI）ユーティリティを使用し、システムにアクセスして管理します。

システム上のリモート コンソール設定の構成

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	FMC 7000 & 8000 シリーズ	グローバルだけ	LOM アクセス権限のある Admin

始める前に

- デバイスの管理インターフェイスに接続されたサードパーティ スイッチング装置で、スパニング ツリー プロトコル（STP）を無効にします。

ステップ 1 **[System]** > **[Configuration]** を選択します。

ステップ 2 [コンソール構成（Console Configuration）] をクリックします。

ステップ 3 リモート コンソール アクセスのオプションを選択します。

- アプライアンスの VGA ポートを使用するには、[VGA] を選択します。
- アプライアンスのシリアル ポートを使用するか、Firepower Management Center、Firepower 7050、または 8000 シリーズ デバイス上で LOM/SOL を使用する場合には、[物理シリアルポート（Physical Serial Port）] を選択します。
- 7000 シリーズデバイス（Firepower 7050 以外）で LOM/SOL を使用する場合は、[Lights-Out Management] を選択します。これらのデバイスでは、SOL と通常のシリアル接続を同時に使用することはできません。

（注） リモート コンソールを [物理シリアル ポート（Physical Serial Port）] から [Lights-Out Management] に変更した場合や、70xx ファミリのデバイス（Firepower 7050 以外）で [Lights-Out Management] から [物理シリアル ポート（Physical Serial Port）] に変更した場合は、アプライアンスを 2 回リブートしないと、期待どおりのブート プロンプトが表示されないことがあります。

ステップ 4 SOL 経由で LOM を設定するには、必要な IPv4 設定を入力します。

- システムのアドレス構成（[DHCP] または [Manual（手動）]）を選択します。
- LOM に使用する IP アドレスを入力します。

（注） LOM IP アドレスは、システムの管理インターフェイスの IP アドレスとは異なる必要があります。

- システムのネットマスクを入力します。
- システムのデフォルト ゲートウェイを入力します。

ステップ 5 [保存（Save）] をクリックします。

次のタスク

- Lights-Out Management を設定した場合は、Lights-Out Management ユーザを有効にします。Lights-Out 管理のユーザ アクセス設定 （1318 ページ）を参照してください。

Lights-Out 管理のユーザ アクセス設定

Lights-Out 管理機能を使用するユーザに対して、この機能の権限を明示的に付与する必要があります。LOM ユーザには、次のような制約もあります。

- ユーザに Administrator ロールを割り当てる必要があります。
- ユーザ名に使用できるのは最大 16 個の英数字です。LOM ユーザに対し、ハイフンやそれより長いユーザ名はサポートされていません。
- 71xx ファミリ デバイスへの設定を除き、パスワードには最大 20 文字の英数字を使用できます。Firepower 7110、7115、7120、または 7125 デバイスで LOM が有効になっている場合、パスワードには最大 16 文字の英数字を使用できます。ユーザの LOM パスワードは、そのユーザのシステム パスワードと同じです。辞書に載っていない複雑な最大長のパス

ワードをアプライアンスに対して使用し、それを 3 か月ごとに変更することを推奨します。

- 物理 Firepower Management Center および 8000 シリーズ デバイスには最大 13 人の LOM ユーザを設定でき、8000 シリーズ デバイスには最大 8 人の LOM ユーザを設定できます。

あるロールを持つユーザのログイン中に LOM でそのロールを非アクティブ化してから再アクティブ化した場合や、ユーザのログインセッション中にそのユーザまたはユーザ ロールをバックアップから復元した場合、そのユーザは IPMItool コマンドへのアクセスを回復するために Web インターフェイスにログインし直す必要があります。

Lights-Out 管理ユーザ アクセスの有効化

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	FMC 7000 & 8000 シリーズ	グローバルだけ	LOM アクセス権限のある Admin

各システムのローカル Web インターフェイスを使用して、システムごとに LOM と LOM ユーザを設定します。つまり、Firepower Management Center を使用して管理対象デバイスで LOM を設定することはできません。同様に、ユーザはアプライアンスごとに個別に管理されるため、Firepower Management Center で LOM 対応ユーザを有効化または作成しても、管理対象デバイスのユーザにはその機能は転送されません。

ステップ 1 **[System]** > **[Configuration]**を選択します。

ステップ 2 [コンソール構成（Console Configuration）] をクリックします。

ステップ 3 [Lights Out 管理（Lights Out Management）] をクリックします。

ステップ 4 次の選択肢があります。

- 既存のユーザに LOM ユーザ アクセスを許可するには、リスト内のユーザ名の横にある編集アイコン（）をクリックします。
- 新しいユーザに LOM ユーザ アクセスを許可するには、[Create User] をクリックします。

ステップ 5 [ユーザの設定（User Configuration）] で、Administrator ロールを有効にします。

ステップ 6 [Lights-Out 管理アクセスの許可（Allow Lights-Out Management Access）] チェックボックスをオンにします。

ステップ 7 **[保存（Save）]** をクリックします。

Serial over LAN 接続の設定

アプライアンスへの Serial over LAN 接続を作成するには、コンピュータ上でサードパーティ製の IPMI ユーティリティを使用します。Linux 系環境または Mac 環境を使用するコンピュータでは IPMItool を使用し、Windows 環境では IPMIutil を使用します。

（注） シスコでは、IPMItool バージョン 1.8.12 以降の使用を推奨しています。

Linux

多くのディストリビューションで IPMItool が標準となっており、使用可能です。

Mac

Mac では、IPMItool をインストールする必要があります。最初に、Mac に Apple の XCode Apple Developer Tools がインストールされていることを確認します。これにより、コマンドライン開発用のオプション コンポーネント（新しいバージョンでは UNIX Development and System Tools、古いバージョンでは Command Line Support）がインストールされていることを確認できます。次に、MacPorts と IPMItool をインストールします。詳細については、好みの検索エンジンを使用するか、次のサイトを参照してください。

```
https://developer.apple.com/technologies/tools/
http://www.macports.org/
```

Windows

Windows では、IPMIutil をコンパイルする必要があります。コンパイラにアクセスできない場合は、IPMIutil 自体を使用してコンパイルできます。詳細については、好みの検索エンジンを使用するか、次のサイトを参照してください。

```
http://ipmiutil.sourceforge.net/
```

IPMI ユーティリティのコマンドについて

IPMI ユーティリティで使用するコマンドは、次の IPMItool の例に示したセグメントで構成されます。

```
ipmitool -I lanplus -H IP_address -U user_name command
```

引数の説明

- `ipmitool` はユーティリティを起動します
- `-I lanplus` はセッションの暗号化を有効にします
- `-H` IP_address はアクセスするアプライアンスの IP アドレスを示します
- `-U` user_name は権限を持つユーザの名前です

- - command は指定するコマンドの名前です

（注） シスコでは、IPMItool バージョン 1.8.12 以降の使用を推奨しています。

Windows 用の同等のコマンドは次のとおりです。

```
ipmiutil command -V 4 -J 3 -N IP_address -Uuser_name
```

このコマンドは、アプライアンスのコマンドラインにユーザを接続します。これによって、ユーザは物理的にそのアプライアンスの近くにいるときと同じようにログインできます。場合によっては、パスワードの入力を求められます。

IPMItool を使用した Serial Over LAN の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	FMC 7000 & 8000 シリーズ	いずれか（Any）	LOM アクセス権限のある Admin

IPMItool を使用して、次のコマンドと、プロンプトが表示されたらパスワードを入力します:

```
ipmitool -I lanplus -H IP_address -U user_name sol activate
```

IPMIutil を使用した Serial Over LAN の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	FMC 7000 & 8000 シリーズ	いずれか（Any）	LOM アクセス権限のある Admin

IPMIutil を使用して、次のコマンドと、プロンプトが表示されたらパスワードを入力します。

```
ipmiutil -J 3 -H IP_address -U username sol -a
```

Lights-Out 管理の概要

Lights-Out管理（LOM）では、システムにログインすることなく、デフォルトの管理インターフェイス（eth0）から SOL 接続を介して一連の限定操作を実行できます。SOL 接続を作成するコマンドに続いて、次のいずれかの LOM コマンドを使用します。コマンドが完了すると、接続は終了します。電源制御コマンドの中には、70xx Family デバイスに対して有効でないものもあります。

（注） Firepower 71xx、Firepower 82xx、またはFirepower 83xx デバイスのベースボード管理コントローラ（BMC）は、ホストの電源がオンのときにのみ 1 Gbps のリンク速度でアクセスできます。デバイスの電源がオフの場合、BMC は 10/100 Mbps でのみイーサネット リンクを確立できます。したがって、デバイスにリモートから電源供給するために LOM を使用している場合は、10/100 Mbps のリンク速度だけを使用してデバイスをネットワークに接続してください。

注意 まれに、コンピュータがシステムの管理インターフェイスとは異なるサブネットにあり、そのシステムに DHCP が構成されている場合は、LOM 機能にアクセスしようとすると失敗することがあります。この場合は、システムの LOM を無効にして再び有効にするか、または同じサブネット上のコンピュータをシステムとして使用して、その管理インターフェイスを ping することができます。その後、LOM を使用できるようになるはずです。

注意 シスコでは、Intelligent Platform Management Interface（IPMI）標準（CVE-2013-4786）に内在する脆弱性を認識しています。システムのLights-Out管理（LOM）を有効にすると、この脆弱性にさらされます。この脆弱性を軽減するために、信頼済みユーザだけがアクセス可能なセキュアな管理ネットワークにシステムを展開し、辞書に載っていない複雑な最大長のパスワードをシステムに対して使用し、それを3か月ごとに変更してください。この脆弱性のリスクを回避するには、LOM を有効にしないでください。

システムへのアクセス試行がすべて失敗した場合は、LOM を使用してリモートでシステムを再起動できます。SOL 接続がアクティブなときにシステムが再起動すると、LOM セッションが切断されるか、またはタイムアウトする可能性があります。

注意 システムが別の再起動の試行に応答している間は、システムを再起動**しないでください**。リモートでシステムを再起動すると、通常の方法でシステムがリブートしないため、データが失われる可能性があります。

表 *94 : Lights-Out* 管理のコマンド

IPMItool	IPMIutil	説明
（非該当）	`-V 4`	IPMI セッションの管理者権限を有効にします
`-I lanplus`	`-J 3`	IPMI セッションの暗号化を有効にします
`-H`	`-N`	リモート アプライアンスの IP アドレスを指定します
`-U`	`-U`	認可された LOM アカウントのユーザ名を指定します
`sol activate`	`sol -a`	SOL セッションを開始します
`sol deactivate`	`sol -d`	SOL セッションを終了します
`chassis power cycle`	`power -c`	アプライアンスを再起動します（70xx Family デバイスでは無効）。
`chassis power on`	`power -u`	アプライアンスの電源を投入します
`chassis power off`	`power -d`	アプライアンスの電源をオフにします（70xx Family デバイスでは無効）。
`sdr`	`sensor`	アプライアンスの情報（ファン速度や温度など）を表示します

たとえば、アプライアンスの情報のリストを表示する IPMItool のコマンドは、次のとおりです。

```
ipmitool -I lanplus -H IP_address -U user_name sdr
```

（注） シスコでは、IPMItool バージョン 1.8.12 以降の使用を推奨しています。

IPMIutil ユーティリティの同等のコマンドは次のとおりです。

```
ipmiutil sensor -V 4 -J 3 -N IP_address -U user_name
```

IPMItool による Lights-Out Management の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	FMC 7000 & 8000 シリーズ	いずれか（Any）	LOM アクセス権限のある Admin

プロンプトが表示されたら、IPMItool の次のコマンドとパスワードを入力します。

```
ipmitool -I lanplus -H IP_address -U user_name command
```

IPMIutil による Lights-Out Management の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	FMC 7000 & 8000 シリーズ	いずれか（Any）	LOM アクセス権限のある Admin

プロンプトが表示されたら、IPMIutil の次のコマンドとパスワードを入力します。

```
ipmiutil -J 3 -H IP_address -U username command
```

REST API 設定

Firepower の REST API は、サードパーティ アプリケーションで REST クライアントおよび標準HTTP メソッドを使用してアプライアンス設定を表示および管理するための軽量のインターフェイスを提供します。Firepower の REST API の詳細については、『*Firepower REST API Quick Start Guide*』を参照してください。

デフォルトでは、Firepower Management Center はアプリケーションからの REST API を使用した要求を許可します。このアクセスをブロックするように Firepower Management Center を設定できます。

REST API アクセスの有効化

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	FMC	いずれか（Any）	Admin

（注） Firepower Management Center ハイ アベイラビリティを使用する展開では、この機能は、アクティブな Firepower Management Center でだけ使用できます。

ステップ 1 **[System]** > **[Configuration]** を選択します。

ステップ 2 [REST API 設定（REST API Preferences）] をクリックします。

ステップ 3 Firepower Management Center への REST API アクセスを有効または無効にするには、[REST API の有効化（Enable REST API）] チェックボックスをオンまたはオフにします。

ステップ 4 **[保存（Save）]** をクリックします。

VMware Tools と仮想システム

VMware Tools は、仮想マシン向けのパフォーマンスを向上させるためのユーティリティ スイートです。これらのユーティリティを使用すると、VMware 製品の便利な機能をフルに活用できます。VMware で実行されている Firepower 仮想アプライアンスは、次のプラグインをサポートします。

- guestInfo
- powerOps
- timeSync
- vmbackup

サポートされるすべてのバージョンの ESXi で VMware Tools を有効にすることもできます。サポートされているバージョンの一覧については、『Cisco Firepower NGIPSv（VMware 向け）クイック スタート』を参照してください。VMware Tools のすべての機能については、VMware の Web サイト（http://www.vmware.com/）を参照してください。

VMware 向け Firepower Management Center での VMware ツールの有効化

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	Firepower Management Center	グローバルだけ。	Admin

NGIPSv には Web インターフェイスがないため、そのプラットフォームで VMware ツールを有効にするには CLI を使用する必要があります（Cisco Firepower NGIPSv（VMware 向け）クイック スタートを参照）。

ステップ 1 **[System]** > **[Configuration]**を選択します。
ステップ 2 [VMware ツール（VMware Tools）] をクリックします。
ステップ 3 [VMware ツールの有効化（Enable VMware Tools）] をクリックします。
ステップ 4 **[保存（Save）]** をクリックします。

（オプション）Web 分析トラッキングのオプトアウト

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	FMC	グローバルだけ。	Admin

デフォルトでは、Firepower 製品の向上のために、ページの閲覧内容、ブラウザのバージョン、製品バージョン、ユーザの場所、Firepower Management Center アプライアンスの管理 IP アドレスまたはホスト名など、個人を特定できない使用データがシスコによって収集されます。

このデータの収集を拒否する場合は、次の手順を実行してオプト アウトできます。

ステップ 1 [システム（System）] > [設定（Configuration）] を選択します。
ステップ 2 [Web 分析（Web Analytics）] をクリックします。
ステップ 3 適切に選択してから、[保存（Save）] をクリックします。

次のタスク

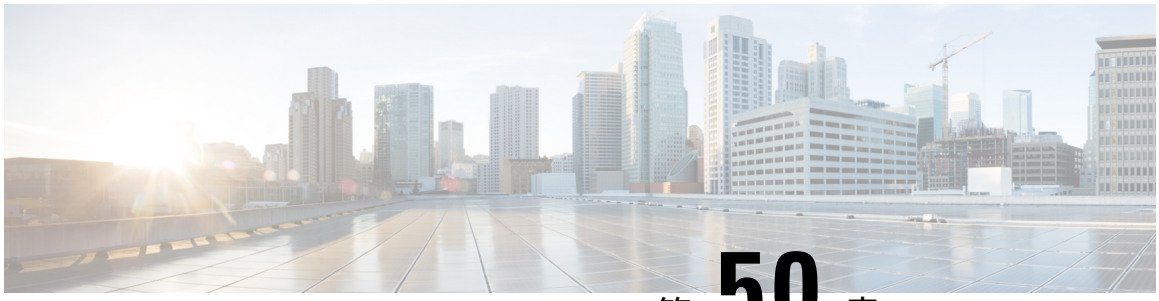
（オプション）Cisco Success Network （162 ページ） 経由でデータを共有するかどうかを決定します。

システム設定の履歴

機能	バージョン	詳細
管理インターフェイスで重複アドレス検出（DAD）を無効にする機能	6.4	IPv6 を有効にすると、DAD を無効にすることができます。DAD を使用することによってサービス拒否攻撃の可能性が拡大するため、DAD は無効にすることができます。この設定を無効にした場合は、すでに割り当てられているアドレスがこのインターフェイスで使用されていないことを手動で確認する必要があります。 新規/変更された画面： **[システム（System）] > [設定（Configuration）] > [管理インターフェイス（Management Interfaces）] > [インターフェイス（Interfaces）] > [インターフェイスの編集（Edit Interface）]** ダイアログボックス > [IPv6 DAD] チェックボックス サポートされるプラットフォーム：FMC、7000 および 8000 シリーズ デバイス
管理インターフェイス上の ICMPv6 エコー応答と宛先到達不能メッセージを無効にする機能	6.4	IPv6 を有効にすると、ICMPv6 エコー応答および宛先到達不能メッセージを無効できるようになりました。これらのパケットを無効にすることで、サービス拒否攻撃の可能性から保護します。エコー応答パケットを無効にすると、デバイスの管理インターフェイスにテスト目的で IPv6 ping を使用できなくなります。 新規/変更された画面： **[システム（System）] > [設定（Configuration）] > [管理インターフェイス（Management Interfaces）] > [ICMPv6]** 新規/変更されたコマンド：**configure network ipv6 destination-unreachable**、**configure network ipv6 echo-reply** サポートされるプラットフォーム：FMC（Web インターフェイスのみ）、 7000 および 8000 シリーズ、 FTD（CLI のみ）、ASA FirePOWER モジュール（CLI のみ）、NGIPSv（CLI のみ）

機能	バージョン	詳細
グローバルユーザ構成時の設定	6.3	[成功したログインの追跡（Track Successful Logins）]の設定を追加しました。システムは、選択した日数までに各 FMC アカウントが実行し、成功したログインの回数を追跡できます。この機能を有効にすると、ログイン中のユーザには、設定した過去の日数内にシステムへのログインが何回成功したかを報告するメッセージが表示されます（Web インターフェイスとシェル/CLI アクセスに適用）。 [パスワード再利用制限（Password Reuse Limit）] の設定を追加しました。設定可能な過去のパスワード数について各アカウントのパスワードの履歴を追跡できます。システムは、すべてのユーザがその履歴に表示されているパスワードを再利用できないようにします（Web インターフェイスとシェル/CLI アクセスに適用）。 [ログイン失敗の最大数（Max Number of Login Failures）] と [ユーザを一時的にロックアウトする分単位の時間の設定（Set Time in Minutes to Temporarily Lockout Users）] の設定を追加しました。これらの機能によって、管理者はシステムが設定可能な時間にわたってアカウントを一時的にブロックするまでに、ユーザが誤った Web インターフェイスのログイン クレデンシャルを連続して入力できる回数を制限できます。 新規画面：**[システム（System）] > [設定（Configuration）] > [ユーザ設定（User Configuration）]** サポート対象プラットフォーム： FMC
HTTPS 証明書	6.3	現在、システムとともに提供されるデフォルトの HTTPS サーバ クレデンシャルは 3 年で期限が切れます。バージョン 6.3 にアップグレードされる前に生成されたデフォルトのサーバ証明書をアプライアンスが使用している場合、サーバ証明書は最初に生成されたときから 20 年後に期限切れとなります。デフォルトの HTTPS サーバ証明書を使用している場合、システムはその証明書を更新する機能を提供しています。 新規/変更された画面： **[システム（System）] > [設定（Configuration）] > [HTTPS 証明書（HTTPS Certificate）]** ページ > [HTTPS 証明書の更新（Renew HTTPS Certificate）] ボタン。 サポートされるプラットフォーム：物理 FMC、7000 および 8000 シリーズ デバイス

機能	バージョン	詳細
のCLIアクセスを有効化および無効化する機能 FMC	6.3	新しい/変更された画面： FMC の Web インターフェイスで管理者が使用可能な新しいチェックボックス：**[System]** > **[Configuration]** の [CLI アクセスの有効化（Enable CLI Access）] > [コンソール設定（Console Configuration）] ページ。 • オン： SSH を使用して FMC にログインすると CLI にアクセスします。 • オフ：SSH を使用して FMC にログインすると Linux シェルにアクセスします。これは、バージョン 6.3 の新規インストールと、以前のリリースからバージョン 6.3 にアップグレードした場合のデフォルトの状態です。 バージョン 6.3 より前では、[コンソール設定（Console Configuration）] ページには 1 つの設定のみしかなく、物理デバイスのみに適用されていました。そのため、[コンソール設定（Console Configuration）] ページは仮想 FMC には使用できませんでした。この新しいオプションを追加することで、[コンソール設定（Console Configuration）] ページに物理とともに 仮想 FMC が表示されるようになりました。ただし、仮想 FMC の場合、このページに表示されるのはこのチェックボックスのみです。 サポートされるプラットフォーム FMC



第 50 章

プラットフォーム設定ポリシー

以下のトピックでは、プラットフォーム設定ポリシーについて、および管理対象デバイスにそれらを導入する方法について説明します。

プラットフォーム設定の概要

プラットフォーム設定ポリシーは、時刻の設定や外部認証など、展開内の他の管理対象デバイスと同様になる可能性の高い、管理対象デバイスの側面を定義する共有の機能またはパラメータのセットです。

共有ポリシーによって同時に複数の管理対象デバイスを設定することができ、これによって展開に一貫性をもたらし、管理の手間を合理化することができます。プラットフォーム設定ポリシーへの変更は、ポリシーを適用したすべての管理対象デバイスに影響します。デバイスごとに異なる設定を使用する場合でも、共有ポリシーを作成して目的のデバイスに適用する必要があります。

たとえば、組織のセキュリティ ポリシーではユーザのログイン時にアプライアンスに「無断使用禁止」のメッセージを表示する必要があるとします。プラットフォーム設定を使えば、プラットフォーム設定ポリシー内で一度ログイン バナーを設定するだけで完了します。

また、Firepower Management Center で複数のプラットフォーム設定ポリシーを活用することもできます。たとえば、さまざまな状況で別々のメール リレー ホストを使用する場合や、さまざまなアクセス リストをテストする場合は、単一のポリシーを編集するのではなく、いくつかのプラットフォーム設定ポリシーを作成し、それらを切り替えることができます。

関連トピック

従来型デバイス用のプラットフォーム設定の構成 （1337 ページ）

システム設定 （1250 ページ）

プラットフォーム設定ポリシーの管理

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Access Admin/Network Admin

[プラットフォームの設定（Platform Settings）]ページ（**[デバイス（Devices）]**>**[プラットフォーム設定（Platform Settings）]**）を使用して、プラットフォーム設定ポリシーを管理します。このページには、各ポリシーのデバイスのタイプが示されます。[ステータス（Status）]列で、ポリシーのデバイス ターゲットが示されます。

ステップ 1 **[デバイス（Devices）]**>**[プラットフォーム設定（Platform Settings）]**を選択します。

ステップ 2 プラットフォーム設定ポリシーを管理します。

- 作成：新しいプラットフォーム設定ポリシーを作成するには、[新規ポリシー（New Policy）]をクリックします。プラットフォーム設定ポリシーの作成 （1333 ページ）を参照してください。
- コピー：プラットフォーム設定ポリシーをコピーするには、コピー アイコン（  ）をクリックします。
- 編集：既存のプラットフォーム設定ポリシーの設定を変更するには、編集アイコン（  ）をクリックします。
- 削除：使用されていないポリシーを削除するには、削除アイコン（  ）をクリックして、選択内容を確認します。

  注意 どのターゲット デバイスでも、最後に展開したポリシーは期限切れであっても削除しないでください。ポリシーを完全に削除する前に、それらのターゲットに別のポリシーを展開するようにしてください。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

プラットフォーム設定ポリシーの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Access Admin/Network Admin

Firepower Threat Defense デバイスのプラットフォーム設定は、従来型デバイスのプラットフォーム設定とは異なります。新しいプラットフォーム設定ポリシーを作成する場合は、*Firepower*（従来型管理対象デバイス用）または *Threat Defense*（FTD デバイス用）のどちらかのタイプを選択する必要があります。

ステップ 1 **[デバイス（Devices）]** > **[プラットフォーム設定（Platform Settings）]**を選択します。

ステップ 2 [新しいポリシー（New Policy）] をクリックします。

ステップ 3 ドロップダウン リストから、デバイス タイプを選択します。

- [Firepower設定（Firepower Settings）]：従来型管理対象デバイス用の共有ポリシーを作成します。
- [脅威に対する防御設定（Threat Defense Settings）]：Firepower Threat Defense の管理対象デバイス用の共有ポリシーを作成します。

ステップ 4 新しいポリシーの [名前（Name）]、および必要に応じて [説明（Description）] を入力します。

ステップ 5 必要に応じて、ポリシーを適用する [使用可能なデバイス（Available Devices）] を選択し、[ポリシーに追加（Add to Policy）] をクリック（またはドラッグ アンド ドロップ）して、選択したデバイスを追加します。[検索（Search）] フィールドに検索文字列を入力して、デバイスのリストを絞り込むことができます。

ステップ 6 [保存（Save）] をクリックします。
システムにより、ポリシーが作成され、編集のために開かれます。

ステップ 7 デバイス プラットフォーム タイプに基づいて、プラットフォーム設定を行います。

- Firepower設定については、従来型デバイス用のプラットフォーム設定 （1335 ページ）を参照してください。
- 脅威に対する防御設定については、Firepower Threat Defense のプラットフォーム設定 （1357 ページ）を参照してください。

ステップ 8 **[保存（Save）]** をクリックします。

次のタスク

設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

プラットフォーム設定ポリシーのターゲットデバイスの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Access Admin/Network Admin

新しいポリシーを作成すると同時にターゲットデバイスを追加したり、後で変更したりできます。

ステップ 1 **[デバイス（Devices）] > [プラットフォーム設定（Platform Settings）]**を選択します。

ステップ 2 編集するプラットフォーム設定ポリシーの横にある編集アイコン（）をクリックします。

ステップ 3 [ポリシーの割り当て（Policy Assignment）] をクリックします。

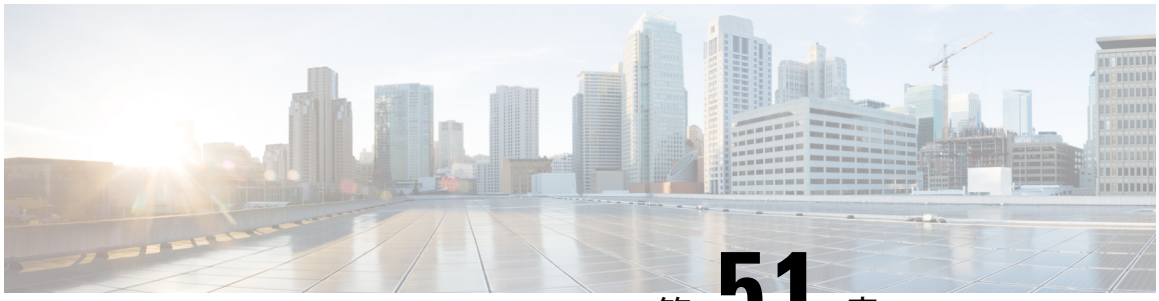
ステップ 4 次のいずれかを実行します。

- デバイス、スタック、ハイ アベイラビリティ ペア、またはデバイス グループをポリシーに割り当てるには、[使用可能なデバイス（Available Devices）] リストで選択し、[ポリシーに追加（Add to Policy）] をクリックします。ドラッグ アンド ドロップを使用することもできます。
- デバイスの割り当てを削除するには、[選択されたデバイス（Selected Device）] リストのデバイス、スタック、ハイ アベイラビリティ ペア、またはデバイス グループの横にある削除アイコン（）をクリックします。

ステップ 5 [OK] をクリックします。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。



第 51 章

従来型デバイス用のプラットフォーム設定

次のトピックでは、Firepower プラットフォーム設定について、および従来型デバイスでそれを設定する方法について説明します。

従来型デバイス用のプラットフォーム設定について

管理対象デバイスのプラットフォーム設定はポリシーベースであるため、複数のデバイスに同じ設定を適用できます。次の従来型デバイスでは *Firepower* プラットフォーム設定ポリシーを使用します。

- 7000/8000 シリーズ デバイス
- ASA FirePOWER モジュール
- NGIPSv

FMC の場合、これらの設定の多くはシステム設定で処理されることに注意してください。システム設定 （1249 ページ）を参照してください。

表 *95*：従来型デバイス用の *Firepower* プラットフォーム設定

プラットフォーム設定	説明	参照先
Access List	どのコンピュータが特定のポートでシステムにアクセスできるかを制御します。	従来型デバイス用のアクセスリストの設定 （1337 ページ）
監査ログ	外部ホストに監査ログを送信するようにシステムを設定します。	従来型デバイスからの監査ログのストリーミング （1338 ページ）

プラットフォーム設定	説明	参照先
監査ログ証明書	監査ログのセキュアなストリーミングの一部として、従来型デバイスと監査ログ サーバ間の相互認証が必要です。	従来型デバイス用の有効な監査ログ サーバ証明書の要求（1340ページ）
外部認証	外部 RADIUS、LDAP、または Microsoft Active Directory のリポジトリによって認証される 7000/8000 シリーズ デバイス ユーザのデフォルト ユーザ ロールを設定します。	7000/8000 シリーズ デバイスへの外部認証の有効化（1341ページ）
言語	7000/8000 シリーズ デバイスの Web インターフェイスに別の言語を指定します。	7000/8000 シリーズ Webインターフェイスの言語の設定 （1343ページ）
ログイン バナー	ユーザがログインすると表示されるカスタム ログイン バナーを作成します。	従来型デバイス用のログインバナーのカスタマイズ （1344ページ）
シェル タイムアウト	ユーザのログイン セッションが非アクティブになったためにタイムアウトするまでのアイドル時間の長さを分単位で設定します。	従来型デバイスのセッションタイムアウトの設定 （1345 ページ）
SNMP	Simple Network Management Protocol （SNMP）のポーリングを有効にします。	従来型デバイスでの SNMP ポーリングの設定 （1346 ページ）
時刻の同期	システムの時刻の同期を管理します。	従来型デバイスの時刻を NTP サーバに同期（1344 ページ）
UCAPL/CC コンプライアンス	米国国防総省によって設定される特定の要件の順守を有効にします。	セキュリティ認定コンプライアンスの有効化（1417 ページ）

従来型デバイス用のプラットフォーム設定の要件

ライセンス要件

なし。

モデルの要件

Firepower プラットフォーム設定ポリシーを従来型デバイスに適用できます。

一部のプラットフォーム設定は、7000/8000 シリーズ デバイスのみに適用されます。これらのデバイスには、外部認証設定、表示言語、セッション タイムアウトなどの Web インターフェイスがあるためです。これらの設定を ASA FirePOWER または NGIPSv に適用しても効果はありません。

7000/8000 シリーズ デバイスのローカル Web インターフェイスにログインして、非ポリシーベースのシステム設定を行うこともできます。7000/8000 シリーズ デバイスのローカル システム設定 （1347 ページ）を参照してください。

ドメインの要件

なし。

Firepower プラットフォーム設定ポリシーは、任意のドメイン レベルで適用できます。

従来型デバイス用のプラットフォーム設定の構成

管理対象デバイスのプラットフォーム設定はポリシーベースであるため、複数のデバイスに同じ設定を適用できます。従来型デバイスでは Firepower プラットフォーム設定ポリシーを使用します。

ステップ 1 **[デバイス（Devices）] > [プラットフォーム設定（Platform Settings）]** を選択し、Firepower ポリシーを作成または編集します。

従来型デバイス用のプラットフォーム設定について （1335ページ） およびプラットフォーム設定ポリシーの作成 （1333 ページ） を参照してください。

ステップ 2 [ポリシー割り当て（Policy Assignment）] をクリックして、ポリシーを展開する [使用可能なデバイス（Available Devices）] を選択します。

ステップ 3 [ポリシーに追加（Add to Policy）] をクリックして（またはドラッグ アンド ドロップして）、選択したデバイスを追加します。

ステップ 4 **[保存（Save）]** をクリックします。

次のタスク

設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

従来型デバイス用のアクセスリストの設定

デフォルトでは、Firepower デバイスへのアクセスは制限されていません。ポート 22（SSH）は、CLI アクセス用に開かれています。 7000/8000 シリーズ デバイスでは、Web インターフェイス アクセス用にポート 443（HTTPS）も開いています。

よりセキュアな環境で運用するために、特定の IP アドレスに対するアクセスを追加することを検討してください。さらに、ポート 161 で SNMP 情報をポーリングするためのアクセスも追加できます。

ステップ 1 **[デバイス（Devices）] > [プラットフォーム設定（Platform Settings）]** を選択し、Firepower ポリシーを作成または編集します。

ステップ 2 [アクセス リスト（Access List）] をクリックします。

ステップ 3 1 つ以上の IP アドレスへのアクセスを追加するには、[ルールの追加（Add Rules）] をクリックします。

ステップ 4 [IP アドレス（IP Address）] フィールドに、IP アドレスまたはアドレスの範囲を入力するか、`any` を入力します。

ステップ 5 [SSH]、[HTTPS]、[SNMP]、またはこれらのオプションの組み合わせを選択して、これらの IP アドレスで有効にするポートを指定します。

ステップ 6 [Add] をクリックします。

ステップ 7 **[保存（Save）]** をクリックします。

次のタスク

設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

従来型デバイスからの監査ログのストリーミング

Firepower アプライアンスは、ユーザ インタラクションのレコード（または監査ログ）を生成します。これらの監査ログは、syslog または HTTP サーバにストリーミングできます。外部 URL に監査情報を送信すると、システム パフォーマンスに影響を与える場合があるので注意してください。

ヒント 7000/8000 シリーズ デバイスでは、デバイスの Web インターフェイスで監査ログを確認することもできます。システムの監査 （397 ページ）

オプションで、Transport Layer Security（TLS）証明書を使用して、Firepower デバイスと信頼できる監査ログ サーバ間の通信を保護することができます。各デバイス（クライアント証明書は一意）については、証明書署名要求（CSR）を生成して、署名のために認証局（CA）に送信してから、署名付き証明書をデバイスにインポートする必要があります。FMC を使用して、管理対象デバイスに監査ログ証明書をインポートすることはできません。これらの証明書は各デバイスに固有のものであり、各デバイスにログインして証明書をインポートする必要があります。

セキュリティを確保するには、グローバルに認識された信頼できる CA を使用します。同じ CA が次の証明書に署名する必要があります。

- クライアント証明書とサーバ証明書の両方（デバイスと監査ログ サーバ間で相互認証が必要になる場合）。

- 証明書チェーンの中間証明書。署名 CA から中間 CA を信頼するように要求された場合は、必要な証明書チェーン（証明書パスとも呼ばれる）を提供する必要があります。

監査ログの形式は次のとおりです。

```
timestamp host [tag] appliance_name: username@ip_address, subsystem, action
```

次に例を示します。

```
Mar 01 14:45:24 localhost [FIREPOWER] MyFirepowerAppliance: admin@10.1.1.2, System >
Configuration, Page View
```

タグはオプションであり、ユーザ設定可能であることに注意してください。syslog イベントには、オプションのファシリティと重大度もあります。。

始める前に

デバイスが、監査ログをストリーミングする予定のサーバと通信できることを確認します。syslog のストリーミングの場合、システムはポート 7/UDP を使用して、設定を保存した際に syslog サーバが到達可能であることを確認します。次に、システムはポート 514/UDP を使用して監査ログをストリーミングします。 チャネルを保護している場合、システムは 6514/TCP を使用します。

手順

	コマンドまたはアクション	目的
ステップ 1	（オプション）監査ログ サーバとのセキュアな通信を設定します。	ASA FirePOWER および NGIPSv の場合は、OpenSSL などのツールを使用して CSR を生成してから、CLI を使用して署名付き証明書をインポートすることができます。**configure audit_cert import**。7000/8000 シリーズデバイスの場合は、デバイスの Web インターフェイスでシステム設定（**[System]** > **[Configuration]**）を使用します。7000/8000 シリーズデバイスでのセキュアな監査ログ ストリーミング用の署名付きクライアント証明書の取得 （1348 ページ）。 証明書が正しくインポートされたことを確認するには、7000/8000 シリーズ デバイスの Web インターフェイスを使用するか、CLI で **show audit_cert** を使用します。
ステップ 2	FMC で、**[デバイス（Devices）]** > **[プラットフォーム設定（Platform Settings）]** を選択し、Firepower ポリシーを作成または編集します。	
ステップ 3	監査ログのストリーミングを設定するには、[監査ログ（Audit Log）] をクリックします。	syslog のストリーミング： HTTP のストリーミング：

	コマンドまたはアクション	目的
ステップ 4	（オプション）各メッセージに含める [タグ（Tag）] を入力します。たとえば、Firepower 監査ログに **Firepower** をタグ付けする必要がある場合があります。	
ステップ 5	[Save] をクリックします。	syslog のストリーミングを設定した場合、システムは syslog サーバが到達可能であることを確認します。

次のタスク

- （オプション）セキュアな通信を設定した場合は、デバイスと監査ログ サーバ間の相互認証を要求することもお勧めします。従来型デバイス用の有効な監査ログ サーバ証明書の要求 （1340 ページ）
- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

従来型デバイス用の有効な監査ログ サーバ証明書の要求

セキュリティを強化するために、Firepower アプライアンスと監査ログ サーバ間の相互認証を要求することを推奨します。相互認証を実現するには、1 つ以上の証明書失効リスト（CRL）をロードします。これらの CRL にリストされている失効した証明書を使用して、サーバに監査ログをストリーミングすることはできません。

Firepower は、識別符号化規則（DER）形式でエンコードされた CRL をサポートしています。これらの CRL は、システムが FMC Web インターフェイスの HTTPS クライアント証明書を検証するために使用する CRL と同じであることに注意してください。

始める前に

署名付きクライアント証明書を入手し、各デバイスにインポートします。

- ASA FirePOWER および NGIPSv の場合は、OpenSSL などのツールを使用して CSR を生成してから、CLI を使用して署名付き証明書をインポートすることができます。**configure audit_cert import**。
- 7000/8000 シリーズ デバイスの場合は、デバイスの Web インターフェイスでシステム設定（**[System]** > **[Configuration]**）を使用します。7000/8000 シリーズ デバイスでのセキュアな監査ログ ストリーミング用の署名付きクライアント証明書の取得 （1348 ページ）。

グローバルに認識された信頼できる CA を使用します。同じ CA が、インポートしたクライアント証明書と、この手順で必要になるサーバ証明書に署名する必要があります。

ステップ 1 **[デバイス（Devices）]** > **[プラットフォーム設定（Platform Settings）]** を選択し、Firepower ポリシーを作成または編集します。

ステップ 2 [監査ログ証明書（Audit Log Certificate）] をクリックします。

ステップ 3 [TLSの有効化（Enable TLS）]、[相互認証の有効化（Enable Mutual Authentication）] の順に選択します。

相互認証を有効にすることをお勧めします。そうしないと、デバイスは検証せずにサーバ証明書を受け入れます。

ステップ 4 [CRLの取得の有効化（Enable Fetching of CRL）] を選択し、CRL ファイルに URL を入力して、[CRLの追加（Add CRL）] をクリックします。

最大 25 個の CRL を追加できます。展開すると、システムは CRL の更新をスケジュールします。更新頻度を設定する場合は、証明書失効リストのダウンロードの設定 （241 ページ）を参照してください。

ステップ 5 **[保存（Save）]** をクリックします。

次のタスク

設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

7000/8000 シリーズ デバイスへの外部認証の有効化

LDAP または RADIUS サーバに対して 7000/8000 シリーズ デバイスのユーザを認証できるようにするには、ローカル データベースを使用するのではなく、デバイス プラットフォーム設定を使用します。

始める前に

外部認証オブジェクトを設定します。外部認証の設定 （62 ページ）を参照してください。

ステップ 1 **[デバイス（Devices）]** > **[プラットフォーム設定（Platform Settings）]** を選択し、Firepower ポリシーを作成または編集します。

ステップ 2 [External Authentication] をクリックします。

ステップ 3 [ステータス（Status）] ドロップダウン リストから [有効（Enabled）] を選択します。

ステップ 4 [デフォルト ユーザ ロール（Default User Role）] ドロップダウン リストから、ユーザ ロールを選択して、外部認証済みユーザに付与するデフォルト権限を定義します。

ステップ 5 外部サーバを使用して CLI またはシェル アクセス アカウントを認証する場合、[シェル認証（Shell Authentication）] ドロップダウン リストから [有効（Enabled）] を選択します。

ステップ 6 CAC 認証および認可を有効にする場合は、[CAC 認証（CAC Authentication）] ドロップダウン リストから使用可能な CAC 認証オブジェクトを選択します。

詳細については、LDAP を使用した共通アクセス カード認証の設定 （80 ページ）を参照してください。

ステップ 7 使用する外部認証オブジェクトそれぞれの横にあるチェック ボックスをクリックします。複数のオブジェクトを有効にすると、ユーザは指定された順序でサーバと照合されます。サーバの順序を変更する場合は、次の手順を参照してください。

シェル認証を有効にする場合は、[シェルアクセスフィルタ（Shell Access Filter）] を含む外部認証オブジェクトを有効にする必要があります。CLI/シェル アクセスのユーザは、認証オブジェクトがリストの順序で最も高いサーバに対してのみ認証できることに注意してください。

CLI と CAC の両方の認証が必要な場合は、各目的のため個別の認証オブジェクトを使用する必要があります。

ステップ 8 （オプション）上矢印および下矢印を使用して、認証要求が行われたときに認証サーバがアクセスされる順序を変更できます。

ステップ 9 **[保存（Save）]** をクリックします。

次のタスク

設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

7000/8000 シリーズ デバイスの外部認証について

外部認証サーバを参照する認証オブジェクトを作成する場合、外部認証を有効にすることにより、ローカルデータベースを使用せずに、管理対象デバイスにログインしているユーザをそのサーバに認証させることができます。

外部認証を有効にすると、システムでは LDAP または RADIUS サーバのユーザのユーザ クレデンシャルが確認されます。さらに、ユーザがローカルの内部認証を有効にしており、ユーザクレデンシャルが内部データベースにない場合、システムは一致するクレデンシャルのセットがないか外部サーバを検査します。ユーザが複数のシステムで同じユーザ名を持っている場合、すべてのサーバですべてのパスワードが動作します。ただし、使用可能な外部認証サーバで認証が失敗した場合、システムはローカルデータベースの検査に戻らないので注意してください。

外部認証を有効にすると、アカウントが外部で認証されている任意のユーザのデフォルトのユーザ ロールを設定できます。これらのロールを組み合わせることができる場合は、複数のロールを選択できます。たとえば、自社の [Network Security] グループのユーザのみを取得する外部認証を有効化した場合、デフォルトのユーザ ロールを設定して [Security Analyst] ロールを組み込み、ユーザが自分で追加のユーザ設定を行わなくても収集されたイベントデータにアクセスできるようにすることが可能です。ただし、外部認証がセキュリティ グループに加えて他のユーザのレコードを取得する場合、デフォルトのロールを未選択のままにしておきたい場合もあります。

アクセス ロールが選択されていない場合、ユーザはログインできますが、どの機能にもアクセスできません。ユーザがログインを試行すると、アカウントがユーザ管理ページ（**[System]** > **[Users]**）に表示されます。ここで、追加の権限を付与するアカウント設定を編集できます。

ヒント 1 つのユーザ ロールを使用するようにシステムを設定してそのポリシーを適用し、後で設定を変更して別のデフォルトのユーザ ロールを使用する場合、アカウントを変更するか、削除して再作成するまで、変更前に作成されたユーザ アカウントはすべて、最初のユーザ ロールを保持します。

CLI/シェル アクセスまたは CAC 認証および承認のために LDAP サーバに対して認証できる一連のユーザを指定する場合は、それぞれに個別の認証オブジェクトを作成し、オブジェクトを個別に有効にする必要があります。

内部認証によってユーザがログインしようとすると、システムは最初にそのユーザがローカル ユーザ データベースに存在するかどうか検査します。ユーザが存在する場合、システムは次にユーザ名とパスワードをローカル データベースに対して検査します。一致が検出されると、ユーザは正常にログインします。ただし、ログインが失敗し、外部認証が有効になっている場合、システムはそれぞれの外部認証サーバに対して、ユーザを設定に表示される認証順序で検査します。ユーザ名およびパスワードが外部サーバからの結果と一致した場合、システムはユーザを、その認証オブジェクトに対してデフォルトの権限を持つ外部ユーザに変更します。

外部ユーザがログインしようとすると、システムは外部認証サーバに対してユーザ名およびパスワードを検査します。一致が検出されると、ユーザは正常にログインします。ログインが失敗した場合、ユーザのログイン試行は拒否されます。外部ユーザは、ローカル データベース内のユーザ リストに対して認証できません。ユーザが新しい外部ユーザの場合、外部認証オブジェクトのデフォルト権限を持つ外部ユーザ アカウントがローカル データベースに作成されます。

7000/8000 シリーズ Web インターフェイスの言語の設定

ここで指定した言語は、ログインしたすべてのユーザの Web インターフェイスに使用されます。次の言語を選択できます。

- 英語
- 中国語（簡体字）
- 中国語（繁体字）
- 日本語
- 韓国語

ステップ 1 **[デバイス（Devices）]** > **[プラットフォーム設定（Platform Settings）]** を選択し、Firepower ポリシーを作成または編集します。

ステップ 2 [言語（Language）] をクリックします。

ステップ 3 使用する言語を選択します。

ステップ 4 **[保存（Save）]** をクリックします。

次のタスク

設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

従来型デバイス用のログイン バナーのカスタマイズ

従来型デバイス用の CLI ログイン バナーをカスタマイズできます。 7000/8000 シリーズ デバイスの場合、ログイン バナーも Web インターフェイスに表示されます。ログイン バナーが大きすぎる場合や、エラーの原因となる場合、システムがバナーを表示しようとすると、CLI セッションが失敗することがあります。

ステップ 1 **[デバイス（Devices）] > [プラットフォーム設定（Platform Settings）]** を選択し、Firepower ポリシーを作成または編集します。

ステップ 2 [ログイン バナー（Login Banner）] を選択します。

ステップ 3 [カスタム ログイン バナー（Custom Login Banner）] フィールドに、使用するログイン バナー テキストを入力します。

タブによるスペース設定は維持されません。

ステップ 4 **[保存（Save）]** をクリックします。

次のタスク

設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

従来型デバイスの時刻を NTP サーバに同期

正常に動作させるには、Firepower Management Center とその管理対象デバイスのシステム時刻を同期させることが不可欠です。展開に FTD デバイスが含まれている場合は、脅威に対する防御のための NTP 時刻同期の設定 （1406 ページ）を参照してください。

注意 FMC と管理対象デバイスの時刻が同期していないと、意図しない結果になることがあります。

展開後、設定された NTP サーバと管理対象デバイスを同期するには、数分かかる場合があります。NTP サーバとして設定されている FMC とデバイスを同期する場合、FMC 自体が NTP サーバを使用するように設定されていると、時刻の同期にさらに時間がかかることがあります。

始める前に

デバイスが、使用予定の NTP サーバと通信できることを確認します。次のいずれかの操作を実行できます。

- FMC と同じ NTP サーバを使用します。FMC の時刻を NTP サーバに同期 （1308 ページ）。
- FMC を NTP サーバとして設定します。ネットワーク NTP サーバにアクセスせずに時刻を同期 （1309 ページ）。

ステップ 1 **[デバイス（Devices）]** > **[プラットフォーム設定（Platform Settings）]** を選択し、Firepower ポリシーを作成または編集します。

ステップ 2 [Time Synchronization] をクリックします。

ステップ 3 時刻の同期方法を指定します。

- [NTPの接続元（Via NTP from）]：ネットワーク上の NTP サーバから時刻を受信します。
- [Management CenterのNTPを使用（Via NTP from Management Center）]：FMC が NTP サーバとして機能するように設定されています。

ステップ 4 **[保存（Save）]** をクリックします。

次のタスク

設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

従来型デバイスのセッション タイムアウトの設定

無人ログインセッションは、セキュリティ上のリスクを生じさせる場合があります。ユーザのログインセッションが非アクティブになったためにタイムアウトするまでのアイドル時間を設定できます。最大値は 24 時間（1440 分）です。

ステップ 1 **[デバイス（Devices）]** > **[プラットフォーム設定（Platform Settings）]** を選択し、Firepower ポリシーを作成または編集します。

ステップ 2 [シェル タイムアウト（Shell Timeout）] をクリックします。

ステップ 3 セッション タイムアウトの設定

- Webインターフェイス（7000/8000シリーズのみ）：[ブラウザセッションタイムアウト（分）（Browser Session Timeout (Minutes)）] を入力します。

  システムを長期間にわたってパッシブかつセキュアにモニタする予定のシナリオでは、特定の Web インターフェイスのユーザがタイムアウトしないように設定できます。詳細については、Web インターフェイスでの内部ユーザの追加 （57 ページ）を参照してください。

- CLI：[シェルタイムアウト（分）（Shell Timeout (Minutes)）] を入力します。

ステップ 4 **[保存（Save）]** をクリックします。

次のタスク

設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

従来型デバイスでの SNMP ポーリングの設定

Simple Network Management Protocol（SNMP）を使用すると、Firepower デバイスの標準 Management Information Base（MIB）にアクセスできます。MIB には、連絡先、管理、場所、サービス情報、IP アドレッシングやルーティングの情報、トランスミッション プロトコルの使用状況の統計などのシステムの詳細が含まれます。 7000/8000 シリーズ デバイスの追加の MIB には、物理インターフェイス、論理インターフェイス、仮想インターフェイス、ARP、NDP、仮想ブリッジ、仮想ルータを通して渡されるトラフィックの統計が含まれます。SNMP ポーリングを有効にすると、システムで SNMP トラップを送信できなくなり、MIB の情報はネットワーク管理システムによるポーリングのみで使用可能になることに注意してください。

システムは、SNMPv1、v2、および v3 をサポートしています。SNMPv2 は読み取り専用コミュニティのみをサポートし、SNMPv3 は読み取り専用ユーザのみをサポートしています。SNMPv3 は、AES128 での暗号化をサポートします。

始める前に

使用するコンピュータごとに SNMP アクセスを追加し、システムをポーリングします。従来型デバイス用のアクセスリストの設定 （1337 ページ）を参照してください。

（注） SNMP MIB には展開の攻撃に使用される可能性がある情報が含まれています。SNMP アクセスのアクセス リストを MIB のポーリングに使用される特定のホストに制限することを推奨します。SNMPv3 を使用し、ネットワーク管理アクセスには強力なパスワードを使用することも推奨します。

ステップ 1 **[デバイス（Devices）] > [プラットフォーム設定（Platform Settings）]** を選択し、Firepower ポリシーを作成または編集します。

ステップ 2 [SNMP] をクリックします。

ステップ 3 [SNMPバージョン（SNMP Version）] ドロップダウン リストから、使用する SNMP バージョンを選択します。

- [Version 1] または [Version 2]：[Community String] フィールドに読み取り専用の SNMP コミュニティ名を入力してから、手順の最後までスキップします。

  （注） SNMP コミュニティストリング名には、特殊文字（<>/%#&?', etc.）を使用できません。

- [バージョン3（Version 3）]：[ユーザを追加（Add User）] をクリックすると、ユーザ定義ページが表示されます。SNMPv3 は、読み取り専用ユーザと AES128 による暗号化のみをサポートしています。

ステップ 4 ユーザ名を入力します。

ステップ 5 [認証プロトコル（Authentication Protocol）] ドロップダウン リストから、認証に使用するプロトコルを選択します。

ステップ 6 [認証パスワード（Authentication Password）] フィールドに SNMP サーバの認証に必要なパスワードを入力します。

ステップ 7 [パスワードの確認（Verify Password）] フィールドに、認証パスワードを再度入力します。

ステップ 8 使用するプライバシー プロトコルを [プライバシー プロトコル（Privacy Protocol）] リストから選択するか、プライバシー プロトコルを使用しない場合は [なし（None）] を選択します。

ステップ 9 [プライバシー パスワード（Privacy Password）] フィールドに SNMP サーバで必要な SNMP プライバシー キーを入力します。

ステップ 10 [パスワードの確認（Verify Password）] フィールドに、プライバシー パスワードを再度入力します。

ステップ 11 [Add] をクリックします。

ステップ 12 **[保存（Save）]** をクリックします。

次のタスク

設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

7000/8000 シリーズ デバイスのローカル システム設定

7000/8000 シリーズ デバイスのローカル Web インターフェイスにログインして、非ポリシーベースのシステム設定を行うことができます。これらの設定の多くは FMC システム設定とパラレルです。詳細は、FMC システム設定の章「システム設定 （1249 ページ）」に記載されています。

表 *96 : 7000/8000* シリーズ デバイスのローカル システム設定

システム設定	説明	参照先
監査ログ証明書	監査ログのセキュアなストリーミングの一部として、7000/8000 シリーズ デバイスの署名付きクライアント証明書を取得およびインポートします。	7000/8000 シリーズ デバイスでのセキュアな監査ログ ストリーミング用の署名付きクライアント証明書の取得 （1348 ページ）
Change Reconciliation	過去 24 時間にわたるシステムへの変更の詳細なレポートを送信します。	変更調整 （1288 ページ）
Console Configuration	VGA またはシリアル ポート経由、または Lights-Out Management（LOM）経由のコンソール アクセスを設定します。	リモート コンソールのアクセス管理 （1317 ページ）
HTTPS Certificate	必要に応じて、信頼できる認証局の HTTPS サーバ証明書を要求し、システムに証明書をアップロードします。	HTTPS 証明書 （1254 ページ）

システム設定	説明	参照先
Information	アプライアンスに関する最新情報を表示し、表示名を編集します。	アプライアンス情報（Appliance Information）（1253 ページ）
管理インターフェイス	アプライアンスの IP アドレス、ホスト名、プロキシ設定などのオプションを変更します。	7000/8000 シリーズ デバイスでの管理インターフェイスの設定（1350 ページ）
プロセス	Firepower のプロセスをシャットダウン、リブート、または再起動します。	7000/8000 シリーズ デバイスのシャットダウンまたは再起動（1354 ページ）
パケット転送の禁止	低帯域幅の展開で、7000/8000 シリーズ デバイスから FMC へのパケット データの送信を無効にします。	FMC へのパケット転送の禁止（1350 ページ）
時刻	現在の時刻設定を表示します。	7000/8000 シリーズ デバイスのシステム時刻の表示（1355ページ）

7000/8000 シリーズ デバイスでのセキュアな監査ログ ストリーミング用の署名付きクライアント証明書の取得

オプションで、Transport Layer Security（TLS）証明書を使用して、Firepower デバイスと信頼できる監査ログ サーバ間の通信を保護することができます。各デバイス（クライアント証明書は一意）については、証明書署名要求（CSR）を生成して、署名のために認証局（CA）に送信してから、署名付き証明書をデバイスにインポートする必要があります。FMC を使用して、管理対象デバイスに監査ログ証明書をインポートすることはできません。これらの証明書は各デバイスに固有のものであり、各デバイスにログインして証明書をインポートする必要があります。

セキュリティを確保するには、グローバルに認識された信頼できる CA を使用します。同じ CA が次の証明書に署名する必要があります。

- クライアント証明書とサーバ証明書の両方（デバイスと監査ログ サーバ間で相互認証が必要になる場合）。
- 証明書チェーンの中間証明書。署名 CA から中間 CA を信頼するように要求された場合は、必要な証明書チェーン（証明書パスとも呼ばれる）を提供する必要があります。

システムは、ベース 64 エンコードの PEM 形式で証明書要求のキーを生成します。

ステップ 1 デバイスの Web インターフェイスにログインし、**[System]** > **[Configuration]** を選択します。

ステップ 2 [監査ログ証明書（Audit Log Certificate）] をクリックします。

ステップ 3 CSR を作成します。

a) [Generate New CSR] をクリックします。

b) 必要な場所と組織の情報を入力します。

c) [共通名（Common Name）] フィールドに、証明書を要求するサーバの完全修飾ドメイン名を入力します。共通名と DNS ホスト名が一致しないと、監査ログのストリーミングは失敗します。

d) [生成（Generate）] をクリックします。

ステップ 4 CSR のテキスト ファイルを作成します。

a) 証明書要求のテキスト ブロック全体（`BEGIN CERTIFICATE REQUEST` 行と `END CERTIFICATE REQUEST` 行を含む）をコピーして貼り付けます。

b) このファイルを *`clientname`*`.csr` として保存します。*`clientname`* は、証明書を使用する予定のデバイスの名前にします。

ステップ 5 CSR を CA に送信して、署名付き証明書の受信を待機します。

ステップ 6 デバイスに署名付き証明書をインポートします。

ページを離れた場合は、**[[System]** > **[Configuration]] > [監査ログ証明書（Audit Log Certificate）]** に戻り、[監査クライアント証明書のインポート（Import Audit Client Certificate）] をクリックします。以下をコピーして貼り付けます。

- [クライアント証明書（Client Certificate）]：署名付き証明書のすべてのテキスト（`BEGIN CERTIFICATE` 行と `END CERTIFICATE` 行を含む）。
- [秘密キー（Private Key）]：秘密キー ファイルのすべてのテキスト（`BEGIN RSA PRIVATE KEY` 行と `END RSA PRIVATE KEY` 行を含む）。
- [証明書チェーン（Certificate Chain）]：必要な各中間証明書のすべてのテキスト。

正しい証明書をインポートしていることを確認します。クライアント証明書は一意です。

ステップ 7 [Save] をクリックします。

次のタスク

まだ設定していない場合は、FMC のデバイス プラットフォーム設定を使用して監査ログのストリーミングを設定します。従来型デバイスからの監査ログのストリーミング（1338ページ）。

FMC へのパケット転送の禁止

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
該当なし	いずれか（Any）	7000 & 8000 シリーズ	該当なし	Admin

侵入ポリシー違反をトリガーしたパケットの具体的な内容について気にする必要がない場合、低帯域幅の展開で 7000 または 8000 シリーズ デバイスから Firepower Management Center デバイスにパケットを送信することを無効にするとができます。

ステップ 1 7000 または 8000 シリーズ デバイスのローカル web インターフェイスで、**[System]** > **[Configuration]** を選択します。

ステップ 2 [情報（Information）] をクリックします。

ステップ 3 [管理センターへのパケット転送を禁止する（Prohibit Packet Transfer to the Management Center）] を選択します。

ステップ 4 **[保存（Save）]** をクリックします。

7000/8000 シリーズ デバイスでの管理インターフェイスの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
該当なし	いずれか（Any）	7000 & 8000 シリーズ	グローバルだけ。	Admin

Webインターフェイスを使用して、管理対象デバイスの管理インターフェイスの設定を変更します。モデルでサポートされている場合に、オプションでイベントインターフェイスを有効にすることができます。管理インターフェイスの詳細については、管理インターフェイス （1266 ページ）を参照してください。

⚠

注意 慎重に管理インターフェイスに変更を加えてください。構成エラーで再接続できなくなると、デバイスのコンソール ポートへのアクセスおよび CLI での再設定が必要になります。

ステップ 1 **[System]** > **[Configuration]** を選択して、[管理インターフェイス（Management Interfaces）] を選択します。

ステップ 2 [インターフェイス（Interfaces）]エリアで、設定するインターフェイスの横にある [編集（Edit）] をクリックします。

このセクションでは、利用可能なすべてのインターフェイスがリストされます。インターフェイスをさらに追加することはできません。

それぞれの管理インターフェイスに対して、以下のオプションを設定できます。

- [有効にする（Enabled）]：管理インターフェイスを有効にします。デフォルト eth0 管理インターフェイスを無効に**しないでください**。eth0 インターフェイスを必要とするプロセスもあります。
- [チャネル（Channels）]：（8000 シリーズのみ）イベント オンリーのインターフェイスを設定します。8000 シリーズのデバイスで eth1 管理インターフェイスを有効にして、イベント インターフェイスとして機能させることができます。これを設定するには、[管理トラフィック（Management Traffic）] チェックボックスをオフにして、[イベント トラフィック（Event Traffic）] チェックボックスをオンのままにしておきます。eth0 管理インターフェイスを入力するには、両方のチェックボックスをオンのままにしておきます。

  Firepower Management Center イベント専用インターフェイスは管理チャネルのトラフィックを受け入れることができないので、デバイス イベント インターフェイスで管理チャネルを単に無効にしてください。

  必要に応じて、管理インターフェイスの [イベント トラフィック（Event Traffic）] を無効にすることができます。いずれの場合も、デバイスは、イベントのみのインターフェイス上でイベントを送信しようとします。そのインターフェイスがダウンしていた場合は、イベント チャネルが無効になっていても、管理インターフェイス上でイベントを送信します。

  インターフェイス上でイベント チャネルと管理チャンネルの両方を無効にすることはできません。
- [モード（Mode）]：リンク モードを指定します。GigabitEthernet インターフェイスでは、自動ネゴシエーションの値を変更しても反映されないことに注意してください。
- [MTU]：最大伝送ユニット（MTU）を設定します。デフォルトは 1500 です。設定可能な MTU の範囲は、モデルとインターフェイスのタイプによって異なる場合があります。

  システムは、設定された MTU 値から自動的に 18 バイトを削減するため、IPv6 の場合、1298 未満の値は MTU の最小値である 1280 に準拠しません。IPv4 の場合は、594 未満の値は MTU の最小値 576 に準拠しません。たとえば、構成値 576 は自動的に 558 に削減されます。
- [MDI/MDIX]：[自動-MDIX（Auto-MDIX）] を設定します。
- [IPv4 設定（IPv4 Configuration）]：IPv4 IP アドレスを設定します。次のどちらかを選択します。
  - [スタティック（Static）]：**IPv4 の管理 IP アドレス** と**ネットマスク**を手動で入力します。
  - [DHCP]：DHCP を使用するインターフェイスを設定します（eth0 のみ）。
  - [無効（Disabled）]：無効 IPv4。IPv4 と IPv6 の両方を無効に**しないでください**。
- [IPv6 設定（IPv6 Configuration）]：IPv6 IP アドレスを設定します。次のどちらかを選択します。
  - [スタティック（Static）]：**IPv6 の管理 IP アドレス**と **IPv6 のプレフィックス長**を手動で入力します。
  - [DHCP]：DHCPv6 を使用するインターフェイスを設定します（eth0 のみ）。
  - [ルータ割当て（Router Assigned）]：ステートレス自動設定を有効にします。

- [無効（Disabled）]：IPv6 を無効にします。IPv4 と IPv6 の両方を無効にしないでください。
- [IPv6 DAD]：IPv6 を有効にするときに [重複アドレス検出（DAD）] を有効または無効にします。DAD を使用することによってサービス拒否攻撃の可能性が拡大するため、DAD は無効にすることができます。この設定を無効にした場合は、すでに割り当てられているアドレスがこのインターフェイスで使用されていないことを手動で確認する必要があります。

ステップ 3 [ルート（Routes）] エリアで、スタティック ルートを編集アイコン（  ）をクリックして編集するか、またはルートを追加アイコン（  ）をクリックして追加します。表示アイコン（  ）をクリックして、ルートの統計を表示します。

（注） Firepower Management Center がリモート ネットワーク上にある場合は、イベント専用インターフェイスのスタティック ルートを追加する必要があります。追加しないと、すべてのトラフィックが管理インターフェイスを通じてデフォルト ルートと一致します。デフォルト ルートでは、ゲートウェイ IP アドレスのみを変更できます。出力インターフェイスは、指定したゲートウェイをインターフェイスのネットワークに照合することで自動的に選択されます。ルーティングの詳細については、管理インターフェイス上のネットワーク ルート （1271 ページ）を参照してください。

次の設定をスタティック ルートに対して設定できます。

- [宛先（Destination）]：ルートを作成する宛先ネットワークのアドレスを設定します。
- [ネットマスク（Netmask）] または [プレフィックス長（Prefix Length）]：ネットワークのネットマスク（IPv4）またはプレフィックス長（IPv6）を設定します。
- [インターフェイス（Interface）]：出力管理インターフェイスを設定します。
- [ゲートウェイ（Gateway）]：ゲートウェイ IP アドレスを設定します。

ステップ 4 [共有設定（Shared Settings）] エリアで、すべてのインターフェイスで共有されているネットワーク パラメータを設定します。

（注） eth0 インターフェイスで [DHCP] を選択すると、DHCP サーバから取得する共有設定の一部を手動で指定することができなくなります。

以下の共有設定を行うことができます。

- [ホスト名（Hostname）]：デバイスのホスト名を設定します。ホスト名を変更する場合、Syslog メッセージに新しいホスト名を反映させるには、デバイスをリブートします。再起動するまでは、新しいホスト名が Syslog メッセージに反映されません。
- [ドメイン（Domains）]：カンマで区切ったデバイスの検索ドメインを設定します。これらのドメインは、コマンド（**ping system** など）に完全修飾ドメイン名を指定しない場合にホスト名に追加されます。ドメインは、管理インターフェイスまたは管理インターフェイスを経由するコマンドでのみ、使用されます。
- [プライマリ DNS サーバ（Primary DNS Server）]、[セカンダリ DNS サーバ（Secondary DNS Server）]、[テリタリ DNS サーバ（Tertiary DNS Server）]：DNS サーバが優先順で使用されるよう設定します。

- [リモート管理ポート（Remote Management Port）]：FMC で通信のリモート管理ポートを設定します。FMC および管理対象デバイスは、双方向の SSL 暗号化通信チャネル（デフォルトではポート 8305）を使用して通信します。

  （注） シスコは、リモート管理ポートをデフォルト設定のままにしておくことを**強く**推奨していますが、管理ポートがネットワーク上の他の通信と競合する場合は、別のポートを選択できます。管理ポートを変更する場合は、導入内の相互に通信する必要がある**すべての**デバイスの管理ポートを変更する必要があります。

ステップ 5 [ICMPv6] 領域で、ICMPv6 の設定を行います。

- [エコー応答パケットの送信を許可する（Allow Sending Echo Reply Packets）]：エコー応答パケットを有効または無効にします。これらのパケットを無効にすることで、サービス拒否攻撃の可能性から保護します。エコー応答パケットを無効にすると、デバイスの管理インターフェイスにテスト目的で IPv6 ping を使用できなくなります。
- [宛先到達不能パケットの送信を許可する（Allow Sending Destination Unreachable Packets）]：宛先到達不能パケットを有効または無効にします。これらのパケットを無効にすることで、サービス拒否攻撃の可能性から保護します。

ステップ 6 [LCD パネル（LCD Panel）] エリアで、[ネットワーク設定の再設定を許可（Allow reconfiguration of network settings）] チェックボックスをオンにして、デバイスの LCD パネルを使用したネットワーク設定の変更を有効にします。

LCD パネルを使用して、デバイスの IP アドレスを編集できます。変更が管理 Firepower Management Center に反映されていることを確認します。状況によっては、Firepower Management Center でデータを手動で更新することが必要になります。

注意 LCD パネルを使用した再構成を許可すると、セキュリティ リスクが発生する可能性があります。LCD パネルを使用してネットワーク設定を構成する場合は、物理的にアクセスするだけでよく、認証は必要ありません。このオプションを有効にするとセキュリティ上の問題が発生する可能性があることを示す警告が Web インターフェイスに表示されます。

ステップ 7 [プロキシ（Proxy）] エリアで、HTTP プロキシ設定をします。

デバイスは、ポート TCP/443（HTTPS）および TCP/80（HTTP）でインターネットに直接接続するように構成されています。HTTP ダイジェスト経由で認証できるプロキシ サーバを使用できます。

（注） NT LAN Manager（NTLM）認証を使用するプロキシはサポートされません。

a) [有効（Enabled）] チェックボックスをオンにします。
b) [HTTP プロキシ（HTTP Proxy）] フィールドに、プロキシ サーバの IP アドレスまたは完全修飾ドメイン名を入力します。
c) [ポート（Port）] フィールドに、ポート番号を入力します。
d) [プロキシ認証の使用（Use Proxy Authentication）] を選択してから [ユーザ名（User Name）] と [パスワード（Password）] を入力して、認証資格情報を設定します。

ステップ 8 [保存（Save）] をクリックします。

ステップ 9 管理 IP アドレスを変更すると、FMC と管理対象デバイスの間の通信に影響を与える可能性があります。

IP アドレスを変更しても、現在の接続には影響を与えません。ただし、デバイスまたは FMC をリロードした場合は、接続を再確立する必要があります。ピアの正しい IP アドレスを持つために、少なくとも 1 つのデバイス（FMC または管理対象デバイス）が必要です。たとえば、デバイス設定中に（IP アドレスの代わりに）FMC の NAT ID を指定した場合は、デバイスを追加したときに FMC で定義したデバイス IP アドレスが正しくなくなるため、FMC は通信を再確立できなくなります。この場合は、FMC でデバイスの管理 IP アドレスを変更する必要があります。デバイス管理設定の編集 （300 ページ）を参照してください。

7000/8000 シリーズ デバイスのシャットダウンまたは再起動

ステップ 1 デバイスの Web インターフェイスで、**[System]** > **[Configuration]** を選択します。

ステップ 2 [プロセス（Process）] を選択します。

ステップ 3 次のいずれかを実行します。

シャットダウン	[アプライアンスのシャットダウン（Shutdown Appliance）] の横にある [コマンドの実行（Run Command）] をクリックします。 **注意** 電源ボタンを使用して Firepower アプライアンスを停止しないでください。データが失われる可能性があります。Web インターフェイス（または CLI）を使用すると、設定データを失うことなく、安全にシステムの電源を切って再起動する準備が整います。
再起動	[アプライアンスの再起動（Reboot Appliance）] の横にある [コマンドの実行（Run Command）] をクリックします。 （注） 再起動するとログアウトします。システムはデータベース チェックを実行しますが、これは完了するのに 1 時間かかります。
コンソールの再起動	[アプライアンスコンソールの再起動（Restart Appliance Console）] の横にある [コマンドの実行（Run Command）] をクリックします。
Snort プロセスの再起動	[Snortの再起動（Restart Snort）] の横にある [コマンドの実行（Run Command）] をクリックします。 **注意** Snort プロセスを再開すると、一時的にトラフィック検査が中断されます。この中断中にトラフィックがドロップするか、検査なしで通過するかどうかは、デバイスの設定方法によって異なります。詳細については、「Snort® の再起動によるトラフィックの動作（451 ページ）」を参照してください。

7000/8000 シリーズ デバイスのシステム時刻の表示

[ユーザ設定（User Preferences）] の [タイムゾーン（Time Zone）] ページで設定したタイムゾーンを使用すると、ほとんどのページでローカル時刻で時刻設定が表示されますが、アプライアンスには UTC 時間を使用して格納されます。さらに、現在の時刻は [時刻の同期（Time Synchronization）] ページの上部に UTC で表示されます（ローカル時刻は手動時計設定オプションで表示されます（有効になっている場合））。

制約事項

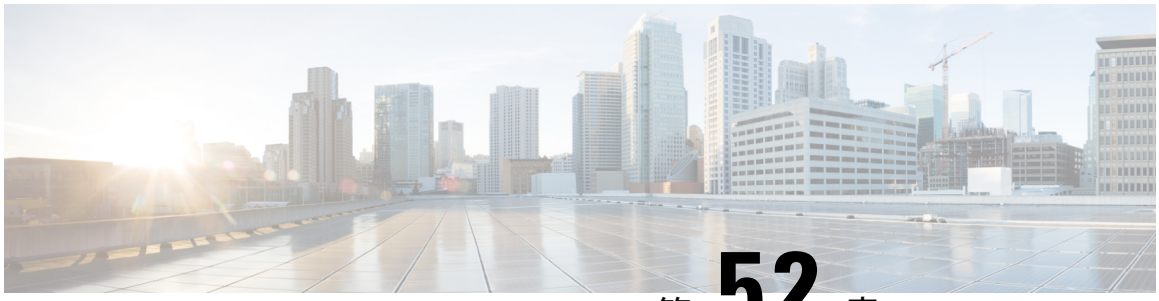
タイムゾーン機能（[ユーザ設定（User Preferences）]）は、デフォルトのシステム クロックが UTC 時間に設定されていることを前提としています。**これは変更しないでください。**システム時刻を UTC から変更することはサポートされていないため、デバイスを再イメージ化する必要があります。

次の手順を使用して、7000 および 8000 シリーズ デバイスでシステム時刻情報を確認します。

ステップ 1 デバイスの Web インターフェイスにログインし、**[System]** > **[Configuration]** を選択します。

ステップ 2 [Time] をクリックします。

NTP を使用している場合は、NTP サーバのステータス （1311 ページ）を参照してください。



第 52 章

Firepower Threat Defense のプラットフォーム設定

FTDデバイス用のプラットフォーム設定では、互いに関連しないさまざまな機能を設定して、いくつかのデバイス間でその値を共有できます。デバイスごとに異なる設定が必要な場合でも、共有ポリシーを作成し、該当するデバイスにそれを適用する必要があります。

ARP インスペクションの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin Access Admin Network Admin

デフォルトでは、ブリッジグループのメンバーの間ですべてのARPパケットが許可されます。ARP パケットのフローを制御するには、ARP インスペクションをイネーブルにします。

ARPインスペクションによって、悪意のあるユーザが他のホストやルータになりすます（ARP スプーフィングと呼ばれる）のを防止できます。ARP スプーフィングが許可されていると、「中間者」攻撃を受けることがあります。たとえば、ホストが ARP 要求をゲートウェイ ルータに送信すると、ゲートウェイルータはゲートウェイルータのMACアドレスで応答します。ただし、攻撃者は、ルータの MAC アドレスではなく攻撃者の MAC アドレスで別の ARP 応答をホストに送信します。これで、攻撃者は、すべてのホストトラフィックを代行受信してルータに転送できるようになります。

ARP インスペクションを使用すると、正しい MAC アドレスとそれに関連付けられた IP アドレスがスタティック ARP テーブル内にある限り、攻撃者は攻撃者の MAC アドレスで ARP 応答を送信できなくなります。

ARP インスペクションをイネーブルにすると、Firepower Threat Defense デバイスは、すべての ARP パケット内の MAC アドレス、IP アドレス、および送信元インターフェイスを ARP テーブル内のスタティック エントリと比較し、次のアクションを実行します。

- IP アドレス、MAC アドレス、および送信元インターフェイスが ARP エントリと一致する場合、パケットを通過させます。
- MAC アドレス、IP アドレス、またはインターフェイス間で不一致がある場合、Firepower Threat Defense デバイスはパケットをドロップします。
- ARP パケットがスタティック ARP テーブル内のどのエントリとも一致しない場合、パケットをすべてのインターフェイスに転送（フラッディング）するか、またはドロップするようにFirepower Threat Defense デバイスを設定できます。

（注） 専用の 診断 インターフェイスは、このパラメータが flood に設定されている場合でもパケットをフラッディングしません。

ステップ 1 **[デバイス（Devices）] > [プラットフォーム設定（Platform Settings）]** を選択し、FTD ポリシーを作成または編集します。

ステップ 2 [ARP インスペクション（ARP Inspection）] を選択します。

ステップ 3 ARP インスペクション テーブルにエントリを追加します。

a) [追加（Add）] をクリックして新しいエントリを作成するか、エントリがすでにある場合は、[編集（Edit）] アイコンをクリックします。

b) 任意のオプションを選択します。

- [インスペクション有効（Inspect Enabled）]：選択されているインターフェイスとゾーンの ARP インスペクションを実行します。

- [フラッディング有効（Flood Enabled）]：静的 ARP エントリに一致しない ARP 要求を元のインターフェイスまたは専門の管理インターフェイス以外のすべてのインターフェイスにフラッディングします。これはデフォルトの動作です。

  ARP 要求のフラッディングを選択しない場合、静的 ARP エントリに一致する要求のみが許可されます。

- [セキュリティ ゾーン（Security Zones）]：選択されているアクションを実行するインターフェイスを含むゾーンを追加します。ゾーンはスイッチド ゾーンにする必要があります。ゾーンに存在しないインターフェイスの場合は、[選択されたセキュリティ ゾーン（Selected Security Zone）] リストの下のフィールドにインターフェイス名を入力し、[追加（Add）] をクリックします。選択されているインターフェイスまたはゾーンがデバイスに含まれているときにのみ、これらのルールがデバイスに適用されます。

c) [OK] をクリックします。

ステップ 4 スタティック ARP エントリの追加 （834 ページ）に従って、静的 ARP エントリを追加します。

ステップ 5 **[Save（保存）]** をクリックします。

これで、[Deploy] をクリックして割り当てられているデバイスにポリシーを展開できます。変更はポリシーを導入するまで有効になりません。

バナー設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin Access Admin Network Admin

デバイスの CLI（コマンドライン インターフェイス）に接続するユーザを表示するよう、メッセージを設定できます。

ステップ 1 **[デバイス（Devices）]** > **[プラットフォーム設定（Platform Settings）]** を選択し、FTD ポリシーを作成または編集します。

ステップ 2 [バナー（Banner）] を選択します。

ステップ 3 バナーを設定します。

以下は、バナーのコツと要件です。

- 使用できる文字は ASCII 文字のみです。回線返品（Enter を押します）を使用できますが、タブを使用できません。

- デバイスのホスト名またはドメイン名は、**$(hostname)** 変数と **$(domain)** 変数を組み込むことによってダイナミックに追加できます。
- バナーに長さの制限はありませんが、バナー メッセージの処理に十分なシステム メモリがない場合、Telnet または SSH セッションは閉じます。
- セキュリティの観点から、バナーで不正アクセスを防止することが重要です。侵入者を招き入れる可能性があるので、「ようこそ」や「お願いします」などの言葉は使用しないでください。次のバナーは、不正アクセスに対する適切な基調を定めます。

```
You have logged in to a secure device.
If you are not authorized to access this device,
log out immediately or risk criminal charges.
```

ステップ 4 **[Save（保存）]** をクリックします。

これで、[Deploy] をクリックして割り当てられているデバイスにポリシーを展開できます。変更はポリシーを導入するまで有効になりません。

DNS の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	Firepower Threat Defense	任意	Access Admin Administrator Network Admin

DNS 解決の設定では、データ インターフェイスおよび診断インターフェイスの DNS を設定できます。また、DNS サーバに接続するための変数も設定できます。

始める前に

DNS サーバ グループを作成していることを確認します。この説明については、DNS サーバ グループ オブジェクトの作成 （601 ページ） を参照してください。

ステップ 1 **[デバイス（Devices）]** > **[プラットフォーム設定（Platform Settings）]** を選択し、Firepower Threat Defense ポリシーを作成または編集します。

ステップ 2 [DNS] をクリックします。

ステップ 3 [デバイスによるDNS名前解決を有効にする（Enable DNS name resolution by device）] チェックボックスを選択します。

ステップ 4 作成済みの [DNS サーバ グループ（DNS Server Group）] を選択します。

ステップ 5 （オプション）[有効期限エントリ タイマー（Expiry Entry Timer）] と [ポール タイマー（Poll Timer）] の値を分単位で入力します。

- 有効期限エントリ タイマーでは、存続可能時間（TTL）経過後に、DNS ルックアップ テーブルから解決済み FQDN の IP アドレスを削除するまでの制限時間を指定します。エントリを削除するとテーブルの再コンパイルが必要になるため、頻繁に削除するとデバイスの処理負荷が増えることがあります。この設定は事実上 TTL を延長します。
- ポール タイマーでは、ネットワーク オブジェクト グループに定義されている FQDN を解決するために、デバイスが DNS サーバにクエリを行うまでの制限時間を指定します。FQDN は、ポール タイマーの期限切れ、または解決された IP エントリの TTL の期限切れのいずれかが発生すると定期的に解決されます。

（注） FQDN 解決の最初のインスタンスは、FQDN オブジェクトがアクセス コントロール ポリシーに展開された場合に発生します。

ステップ 6 （オプション）使用可能リストから必要なインターフェイス オブジェクトを選択し、[追加（Add）] を選択して、[選択済みインターフェイス オブジェクト（Selected Interface Objects）] リストに追加します。

インターフェイスを指定せず、診断インターフェイスで DNS ルックアップを有効にしない場合（次の手順を参照）、FTD はルーティング テーブルを使用してインターフェイスを決定します。一致しない場合は、管理ルーティング テーブルが使用されます。

ステップ 7 （オプション）[診断インターフェイス経由の DNS ルックアップも有効にする（Enable DNS Lookup via diagnostic interface also）] チェックボックスを選択します。

有効になっている場合、Firepower Threat Defense は、選択したデータ インターフェイスと診断インターフェイスの両方を DNS 解決に使用します。**[デバイス（Devices）] > [デバイス管理（Device Management）] > [デバイスの編集（edit device）] > [インターフェイス（Interfaces）]** ページで診断インターフェイスの IP アドレスを設定してください。

ステップ 8 [保存（Save）] をクリックします。

次のタスク

アクセス制御ルールの FQDN オブジェクトを使用するには、アクセス制御ルールに割り当て可能な FQDN ネットワーク オブジェクトを作成します。手順については、ネットワーク オブジェクトの作成 （527 ページ）を参照してください。

SSH の外部認証の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	管理者

管理ユーザの外部認証を有効にすると、FTDにより外部認証オブジェクトで指定されたLDAPまたはRADIUS サーバを使用してユーザ クレデンシャルが検証されます。

外部認証オブジェクトの共有

外部認証オブジェクトは、FMC、7000および8000シリーズ、およびFTDデバイスで使用できます。すべてのアプライアンス/デバイス タイプで同じオブジェクトを共有することも、別々のオブジェクトを作成することもできます。FTDはRADIUSサーバでのユーザの定義をサポートしますが、他のプラットフォームでは外部認証オブジェクトのユーザ リストを事前に認証する必要があります。FTD には事前に定義されているリスト方式を使用できますが、RADIUS サーバでユーザを定義する場合はFTD とその他のプラットフォームに個別のオブジェクトを作成する必要があります。

デバイスへの外部認証オブジェクトの割り当て

FMC では、**[システム（System）]** > **[ユーザ（Users）]** > **[外部認証（External Authentication）]** タブで外部認証オブジェクトを直接有効にします。この設定は、FMC の使用にのみ影響し、管理対象デバイスを使用する場合には、このタブで有効にする必要はありません。7000および8000 シリーズおよびFTD のデバイスでは、デバイスに展開するプラットフォーム設定で外部認証オブジェクトを有効にする必要があります。FTD、では、ポリシーごとにアクティブ化できる外部認証オブジェクトは 1 つのみです。CAC 認証を有効にした LDAP オブジェクトは、CLI アクセスでも使用することはできません。

FTD サポート対象フィールド

FTDSSHアクセスでは、外部認証オブジェクト内のフィールドのサブセットのみが使用されます。その他のフィールドに値を入力しても無視されます。このオブジェクトを他のデバイス タイプにも使用する場合は、それらのフィールドが使用されます。この手順は、FTDでサポートされているフィールドのみを対象とします。その他のフィールドについては、外部認証の設定（62 ページ）を参照してください。

ユーザ名

ユーザ名はLinuxで有効な名前で、かつ、小文字のみである必要があり、英数文字とピリオド（.）およびハイフン（-）を使用できます。アットマーク（@）やスラッシュ（/）など、その他の特殊文字はサポートされていません。外部認証に**admin**ユーザを追加することはできません。外部ユーザは、FMC で（外部認証オブジェクトの一部として）追加することしかできません。CLIでは追加できません。内部ユーザは、FMCではなく、CLIでしか追加できないことに注意してください。

configure user add 内部ユーザとして同じユーザ名がコマンドを使用して設定されていた場合は、FTD は最初にその内部ユーザのパスワードをチェックし、それが失敗した場合はAAAサーバをチェックします。後から外部ユーザと同じ名前の内部ユーザを追加できないことに注意してください。既存の内部ユーザしかサポートされません。RADIUSサーバで定義されているユーザの場合は、内部ユーザの権限レベルと同じに設定してください。そうしないと、外部ユーザ パスワードを使用してログインできません。

Privilege Level

LDAP ユーザには常に Config 権限があります。RADIUS ユーザは、Config ユーザまたは Basic ユーザとして定義できます。

始める前に

- SSHアクセスは管理インターフェイス上でデフォルトで有効になります。データインターフェイス上でSSHアクセスを有効にするには、セキュア シェルの設定（1375 ページ）を参照してください。SSH は診断インターフェイスに対してサポートされていません。
- RADIUS ユーザに次の動作を通知し、適切に動作するようにします。
  - 外部ユーザが初めてログインすると、FTD は必要な構造体を作成しますが、ユーザセッションを同時に作成することはできません。ユーザがセッションを開始するには、再度認証する必要があるだけです。ユーザには次のようなメッセージが表示されます。「New external username identified. Please log in again to start a session.」
  - 同様に、最後のログイン以降に Service-Type で定義したユーザの認証が変更された場合は、ユーザは再認証する必要があります。ユーザには次のようなメッセージが表示されます。「Your authorization privilege has changed. セッションを開始するにはもう一度ログインしてください。（Please log in again to start a session.）」

ステップ 1 **[デバイス（Devices）]** > **[プラットフォーム設定（Platform Settings）]** を選択し、FTD ポリシーを作成または編集します。

ステップ 2 [外部認証（External Authentication）] をクリックします。

ステップ 3 [外部認証サーバの管理（Manage External Authentication Server）] リンクをクリックします。

新しいブラウザタブで、**[システム（System）]** > **[ユーザ（Users）]** > **[外部認証（External Authentication）]** 画面が開きます。

ステップ 4 LDAP 認証オブジェクトを設定します。

a) [外部認証オブジェクトの追加（Add External Authentication Object）] をクリックします。
b) [認証方式（Authentication Method）] を [LDAP] に設定します。
c) [名前（Name）] とオプションの [説明（Description）] を入力します。
d) ドロップダウン リストから [サーバタイプ（Server Type）] を選択します。
e) [プライマリサーバ（Primary Server）] の場合は、[ホスト名/IPアドレス（Host Name/IP Address）] を入力します。

（注） 証明書を使用し、TLS または SSL 経由で接続する場合は、証明書のホスト名が、このフィールドに入力するホスト名と一致している必要がりあります。また、暗号化接続では IPv6 アドレスはサポートされていません。

f) （任意） [ポート（Port）] をデフォルトから変更します。
g) （任意） [バックアップサーバ（Backup Server）] パラメータを入力します。
h) [LDAP固有のパラメータ（LDAP-Specific Parameters）] を入力します。
   - [ベースDN（Base DN）]：アクセスするLDAPディレクトリのベース識別名を入力します。たとえば、Example 社のセキュリティ（Security）部門の名前を認証するには、`ou=security,dc=example,dc=com` と入力します。または、[DNの取得（Fetch DNs）] をクリックし、ドロップダウン リストから適切なベース識別名を選択します。

- （オプション）[基本フィルタ（Base Filter）]：たとえば、ディレクトリ ツリー内のユーザ オブジェクトに `physicalDeliveryOfficeName` 属性が設定されており、New York 支店のユーザに対しこの属性に値 `NewYork` が設定されている場合、New York 支店のユーザだけを取得するには、`(physicalDeliveryOfficeName=NewYork)` と入力します。
- [ユーザ名（User Name）]：LDAP サーバを参照するために十分なクレデンシャルを持つユーザの識別名を入力します。たとえば、ユーザ オブジェクトに `uid` 属性が含まれている OpenLDAP サーバに接続し、Example 社のセキュリティ（Security）部門の管理者のオブジェクトの `uid` に値 `NetworkAdmin` が設定されている場合は、`uid=NetworkAdmin,ou=security,dc=example,dc=com` と入力します。
- [パスワード（Password）] と [パスワードの確認（Confirm Password）]：ユーザのパスワードを入力して確認します。
- （オプション）[詳細オプションを表示（Show Advanced Options）]：次の詳細オプションを設定します。
  - **[暗号化（Encryption）]**：**[なし（None）]**、**[TLS]**、または **[SSL]** をクリックします。

    （注） ポートを指定した後で暗号化方式を変更すると、ポートがその方式のデフォルト値にリセットされます。[なし（None）] または [TLS] の場合、ポートはデフォルト値の 389 にリセットされます。[SSL] 暗号化を選択した場合、ポートは 636 にリセットされます。

  - [SSL証明書アップロードパス（SSL Certificate Upload Path）]：SSL または TLS 暗号化の場合は、[ファイルの選択（Choose File）] をクリックして証明書を選択する必要があります。
  - （未使用）[ユーザ名テンプレート（User Name Template）]：FTD では使用されていません。
  - [タイムアウト（Timeout）]：バックアップ接続にロールオーバーするまでの秒数を入力します。デフォルトは 30 です。

i) （任意） ユーザ識別タイプ以外のシェル アクセス属性を使用する場合は、[シェルアクセス属性（Shell Access Attribute）] を設定します。たとえば、Microsoft Active Directory Server で `sAMAccountName` シェル アクセス属性を使用してシェル アクセス ユーザを取得するには、[シェル アクセス属性（Shell Access Attribute）] フィールドに `sAMAccountName` と入力します。

j) [シェルアクセスフィルタ（Shell Access Filter）] を設定します。

次のいずれかの方法を選択します。

- 認証設定の設定時に指定したものと同じフィルタを使用するには、[基本フィルタと同じ（Same as Base Filter）] を選択します。
- 属性値に基づいて管理ユーザ項目を取得するには、属性名、比較演算子、およびフィルタとして使用する属性値を、カッコで囲んで入力します。たとえば、すべてのネットワーク管理者の `manager` 属性に属性値 `shell` が設定されている場合は、基本フィルタ `(manager=shell)` を設定できます。

LDAP サーバ上の名前は、次のように Linux に対して有効である必要があります。

- 英数字、ハイフン（-）、およびアンダースコア（_）が使用可で、最大 32 文字
- すべて小文字
- 最初の文字にハイフン（-）は使用不可、すべて数字は不可、ピリオド（.）、アットマーク（@）、またはスラッシュ（/）は使用不可

k) [保存（Save）] をクリックします。

ステップ 5 LDAP の場合、LDAP サーバで後からユーザを追加または削除する場合は、ユーザ リストを更新し、プラットフォーム設定を再展開する必要があります。

a) **[システム（System）] > [ユーザ（Users）] > [外部認証（External Authentication）]** を選択します。

b) LDAP サーバの横にある[Refresh] アイコン（）をクリックします。

ユーザ リストが変更された場合は、デバイスの設定変更を展開するように促すメッセージが表示されます。Firepower Threat Defense のプラットフォーム設定には、「*x* 台の対象デバイスで古くなっている」ことも表示されます。

c) 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

ステップ 6 RADIUS 認証オブジェクトを設定します。

a) Service-Type 属性を使用して RADIUS サーバ上のユーザを定義します。

次に、Service-Type 属性でサポートされている値を示します。

- Administrator (6)：CLI への config アクセス認証を提供します。これらのユーザは、CLI ですべてのコマンドを使用できます。
- NAS Prompt (7) または 6 以外のレベル：CLI への基本的なアクセス認証を提供します。これらのユーザは **show** コマンドなど、モニタリングやトラブルシューティングのための読み取り専用コマンドを使用できます。

または、外部認証オブジェクトにユーザを事前定義できます（ステップ 6.j （1366 ページ） を参照）。

名前は、次のように Linux に対して有効である必要があります。

- 英数字、ハイフン（-）、およびアンダースコア（_）が使用可で、最大 32 文字
- すべて小文字
- 最初の文字にハイフン（-）は使用不可、すべて数字は不可、ピリオド（.）、アットマーク（@）、またはスラッシュ（/）は使用不可

b) FMC で [外部認証オブジェクトの追加（Add External Authentication Object）] をクリックします。

c) [認証方式（Authentication Method）] を [RADIUS] に設定します。

d) [名前（Name）] とオプションの [説明（Description）] を入力します。

e) [プライマリサーバ（Primary Server）] の場合は、[ホスト名/IPアドレス（Host Name/IP Address）] を入力します。

（注） 証明書を使用し、TLS または SSL 経由で接続する場合は、証明書のホスト名が、このフィールドに入力するホスト名と一致している必要がりあります。また、暗号化接続では IPv6 アドレスはサポートされていません。

f) （任意）[ポート（Port）] をデフォルトから変更します。

g) [RADIUS秘密キー（RADIUS Secret Key）] を入力します。

h) （任意）[バックアップサーバ（Backup Server）] パラメータを入力します。

i) [RADIUS固有のパラメータ（RADIUS-Specific Parameters）] を入力します。

- [タイムアウト（秒）（Timeout (Seconds)）]：バックアップ接続にロールオーバーするまでの秒数を入力します。デフォルトは 30 です。
- [再試行（Retries）]：バックアップ接続にロールオーバーする前にプライマリ サーバ接続を試行する回数を入力します。デフォルトは 3 です。

j) （オプション）外部認証オブジェクトにユーザ名を事前に定義する場合は、[シェルアクセス フィルタ（Shell Access Filter）] の [管理者シェル アクセス ユーザ リスト（Administrator Shell Access User List）] にカンマ区切りのユーザ名のリストを入力します。たとえば、**`jchrichton, aerynsun, rygel`** と入力します。

これらのユーザ名が RADIUS サーバのユーザ名と一致していることを確認します。名前は、次のように Linux に対して有効である必要があります。

- 英数字、ハイフン（-）、およびアンダースコア（_）が使用可で、最大 32 文字
- すべて小文字
- 最初の文字にハイフン（-）は使用不可、すべて数字は不可、ピリオド（.）、アットマーク（@）、またはスラッシュ（/）は使用不可

（注） RADIUS サーバでユーザのみを定義する場合は、このセクションを空のままにしておく必要があります。

k) [保存（Save）] をクリックします。

ステップ 7 **[デバイス（Devices）]** > > **[プラットフォーム設定（Platform Settings）]** > **[外部認証（External Authentication）]** タブに戻ります。

ステップ 8 [Refresh] アイコン（）をクリックして、新しく追加したオブジェクトを表示します。

LDAP の場合は、SSL 暗号化または TLS 暗号化を指定するときに、その接続用の証明書をアップロードする必要があります。アップロードしない場合は、このタブにサーバがリストされません。

ステップ 9 使用する外部認証オブジェクトの横にあるスライダ（）をクリックします。有効にできるのは、1 つのオブジェクトのみです。

ステップ 10 [保存（Save）] をクリックします。

ステップ 11 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

フラグメントの処理の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin Access Admin Network Admin

デフォルトでは、FTD デバイスは 1 つの IP パケットにつき最大 24 のフラグメントを許可し、最大 200 のフラグメントのリアセンブリ待ちを許可します。NFS over UDP など、アプリケーションが日常的にパケットをフラグメント化する場合は、ネットワークでフラグメント化を許可する必要があります。ただし、トラフィックをフラグメント化するアプリケーションがない場合は、[チェーン（Chain）] を 1 に設定してフラグメントを許可しないようにすることをお勧めします。フラグメント化されたパケットは、サービス妨害（DoS）攻撃によく使われます。

（注） これらの設定は、このポリシーが割り当てられたデバイスのデフォルトになります。インターフェイス構成で [デフォルト フラグメント設定のオーバーライド（Override Default Fragment Setting）] を選択することで、デバイスの特定のインターフェイスでこれらの設定をオーバーライドできます。インターフェイスを編集する際、[詳細（Advanced）] > [セキュリティ設定（Security Configuration）] タブでオプションを確認できます>。[デバイス（Devices）] > [デバイス管理（Device Management）] を選択して、FTD デバイスを編集し、[インターフェイス（Interfaces）] タブを選択して、インターフェイスのプロパティを編集します。 >

ステップ 1 **[デバイス（Devices）] > [プラットフォーム設定（Platform Settings）]** を選択し、FTD ポリシーを作成または編集します。

ステップ 2 [フラグメント（Fragment）] を選択します。

ステップ 3 次のオプションを設定します。デフォルト設定を使用する場合は、[デフォルトにリセット（Reset to Defaults）] をクリックします。

- [サイズ（ブロック（Size (Block)）] : リアセンブルを待機可能な、すべての集合的な接続からのパケット フラグメントの最大数。デフォルトは 200 フラグメントです。
- [チェーン（フラグメント）（Chain (Fragment)）] : 1 つの完全な IP パケットにフラグメント化できる最大パケット数を指定します。デフォルトは 24 パケットです。フラグメントを許可しない場合は、このオプションを 1 に設定します。
- [タイムアウト（秒）（Timeout (Sec)）] : フラグメント化されたパケット全体の到着を待機する最大秒数を設定します。デフォルトは 5 秒です。すべてのフラグメントがこの時間内に受信されなかった場合、すべてのフラグメントが破棄されます。

ステップ 4 **[Save（保存）]** をクリックします。

これで、[Deploy] をクリックして割り当てられているデバイスにポリシーを展開できます。変更はポリシーを導入するまで有効になりません。

HTTP の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin Access Admin Network Admin

HTTPS 接続を FTD デバイスの複数のインターフェイスに対して許可するには、HTTPS 設定を行います。トラブルシューティングでパケット キャプチャをダウンロードするために、HTTPS を使用できます。

始める前に

- Firepower Management Center を使用して FTD を管理する場合は、FTD に対する HTTPS アクセスがパケット キャプチャ ファイルの表示にしか使用されません。FTD は、この管理モードでの設定用の Web インターフェイスを備えていません。
- HTTPS ローカル ユーザは、CLI で **configure user add** コマンドを使用することによってのみ設定できます。デフォルトでは、初期設定時にパスワードを設定した**Admin**ユーザが存在します。AAA 外部認証はサポートされません。
- 物理管理インターフェイスは、診断論理インターフェイスと管理論理インターフェイス間で共有されます。この設定は、使用されている診断論理インターフェイスまたはその他のデータ インターフェイスにのみ適用されます。管理論理インターフェイスはデバイスの他のインターフェイスから切り離されています。これは、Firepower Management Center にデバイスを設定し、登録するために使用されます。これには、個別の IP アドレスとスタティック ルーティングがあります。
- HTTPS の使用で、ホスト IP アドレスを許可するアクセス ルールは必要ありません。このセクションの手順に従って、HTTPS アクセスを設定する必要があるだけです。
- 到達可能なインターフェイスにのみ HTTPS を使用できます。HTTPS ホストが外部インターフェイスにある場合は、外部インターフェイスへの直接的な管理接続のみ開始できます。
- 同じ TCP ポートに関して、同じインターフェイスに HTTPS と AnyConnect リモート アクセス SSL VPN の両方を設定することはできません。たとえば、外部インターフェイスにリモート アクセス SSL VPN を設定する場合、ポート 443 で HTTPS 接続用の外部インターフェイスも開くことはできません。同じインターフェイスに両方の機能を設定する必要がある場合は、別々のポートを使用します。たとえば、ポート 4443 で HTTPS を開きます。

- デバイスでは、最大 5 つの HTTPS 接続を同時にできます。
- デバイスへの HTTPS 接続に許可するホストまたはネットワークを定義するネットワークオブジェクトが必要です。手順の一部としてオブジェクトを追加できますが、IP アドレスのグループを特定するためにオブジェクト グループを使用する場合は、ルールで必要なグループがすでに存在することを確認します。**[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** を選択してオブジェクトを設定します。

（注） システム提供の **any** ネットワーク オブジェクト グループは使用できません。代わりに、**any-ipv4** または **any-ipv6** を使用します。

ステップ 1 **[デバイス（Devices）]** > **[プラットフォーム設定（Platform Settings）]** を選択し、FTD ポリシーを作成または編集します。

ステップ 2 [HTTP] を選択します。

ステップ 3 [HTTP サーバを有効にする（Enable HTTP server）] をクリックして、HTTPS サーバを有効にします。

ステップ 4 （任意） HTTPS ポートを変更します。デフォルトは 443 です。

ステップ 5 HTTPS 接続を許可する IP アドレスとインターフェイスを指定します。

このテーブルを使用して、HTTPS 接続および HTTPS 接続が許可されているクライアントの IP アドレスを承認するインターフェイスを制限します。個々の IP アドレスはなく、ネットワーク アドレスを使用できます。

a) [追加（Add）] をクリックして新しいルールを追加するか、[編集（Edit）] アイコンをクリックして既存のルールを編集します。

b) 次のルール プロパティを設定します。

- [IP アドレス（IP Address）]：HTTPS 接続を許可するホストまたはネットワークを識別するネットワーク オブジェクト。オブジェクトをドロップダウン メニューから選択するか、または + ボタンをクリックして新しいネットワーク オブジェクトを追加します。
- [セキュリティ ゾーン（Security Zones）]：HTTPS 接続を許可するインターフェイスを含むゾーンを追加します。ゾーンに存在しないインターフェイスの場合は、[選択されたセキュリティ ゾーン（Selected Security Zone）] リストの下のフィールドにインターフェイス名を入力し、[追加（Add）] をクリックします。選択されているインターフェイスまたはゾーンがデバイスに含まれているときにのみ、これらのルールがデバイスに適用されます。

c) [OK] をクリックします。

ステップ 6 **[Save（保存）]** をクリックします。

これで、[Deploy] をクリックして割り当てられているデバイスにポリシーを展開できます。変更はポリシーを導入するまで有効になりません。

ICMP アクセス ルールの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin Access Admin Network Admin

デフォルトでは、IPv4 または IPv6 を使用して任意のインターフェイスに ICMP パケットを送信できます。ただし、次の例外があります。

- Firepower Threat Defense デバイス は、ブロードキャスト アドレス宛ての ICMP エコー要求に応答しません。
- Firepower Threat Defense デバイスは、トラフィックが着信するインターフェイス宛ての ICMP トラフィックにのみ応答します。ICMP トラフィックは、インターフェイス経由で離れたインターフェイスに送信できません。

デバイスを攻撃から保護するために、ICMP ルールを使用して、インターフェイスへの ICMP アクセスを特定のホスト、ネットワーク、または ICMP タイプに限定できます。ICMP ルールにはアクセス ルールと同様に順序があり、パケットに最初に一致したルールのアクションが適用されます。

インターフェイスに対して any ICMP ルールを設定すると、ICMP ルールのリストの最後に暗黙の deny ICMP ルールが追加され、デフォルトの動作が変更されます。そのため、一部のメッセージ タイプだけを拒否する場合は、残りのメッセージ タイプを許可するように ICMP ルールのリストの最後に permit any ルールを含める必要があります。

ICMP 到達不能メッセージ タイプ（タイプ 3）の権限を常に付与することを推奨します。ICMP 到達不能メッセージを拒否すると、ICMP パス MTU ディスカバリがディセーブルになり、IPsec および PPTP トラフィックが停止することがあります。また、IPv6 の ICMP パケットは、IPv6 のネイバー探索プロセスに使用されます。

始める前に

ルールに必要なオブジェクトがすでに存在していることを確認します。[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] を選択し、オブジェクトを設定します。 > 任意のホストまたはネットワークを定義するネットワーク オブジェクトまたはグループ、あるいは制御する ICMP メッセージ タイプを定義するポート オブジェクトが必要です。

ステップ 1 **[デバイス（Devices）] > [プラットフォーム設定（Platform Settings）]** を選択し、FTD ポリシーを作成または編集します。

ステップ 2 [ICMP] を選択します。

ステップ 3 ICMP ルールを設定します。

a) [追加（Add）] をクリックして新しいルールを追加するか、[編集（Edit）] アイコンをクリックして既存のルールを編集します。
b) 次のルール プロパティを設定します。
   - [アクション（Action）] : 一致するトラフィックを許可または拒否（ドロップ）するかどうかを指定します。
   - [ICMP サービス（ICMP Service）] : ICMP メッセージ タイプを識別するポート オブジェクト。
   - [ネットワーク（Network）] : アクセスを制御しているホストまたはネットワークを識別するネットワーク オブジェクトまたはグループ。
   - [セキュリティ ゾーン（Security Zones）] : 保護しているインターフェイスを含むゾーンを追加します。ゾーンに存在しないインターフェイスの場合は、[選択されたセキュリティ ゾーン（Selected Security Zone）] リストの下のフィールドにインターフェイス名を入力し、[追加（Add）] をクリックします。選択されているインターフェイスまたはゾーンがデバイスに含まれているときにのみ、これらのルールがデバイスに適用されます。
c) [OK] をクリックします。

ステップ 4 （任意）ICMPv4 到達不能メッセージをレート制限します。

- [レート制限（Rate Limit）] : 到達不能メッセージのレート制限を、1 秒あたり 1 ～ 100 の範囲で設定します。デフォルトは、1 秒あたり 1 メッセージです。
- [バースト サイズ（Burst Size）] : バースト レートを 1 ～ 10 の範囲で設定します。現在、この値はシステムによって使用されていません。

ステップ 5 **[Save（保存）]** をクリックします。

これで、[Deploy] をクリックして割り当てられているデバイスにポリシーを展開できます。変更はポリシーを導入するまで有効になりません。

SSL 設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス（Access）
エクスポート コンプライアンス	該当なし	FTD	リーフのみ	Admin

始める前に

完全にライセンス供与されたバージョンの Firepower Management Center を実行していることを確認する必要があります。評価モードで Firepower Management Center を実行している場合は、[SSL 設定（SSL Settings）] タブは無効になります。また、ライセンス供与された Firepower

Management Center のバージョンがエクスポートのコンプライアンス基準を満たしていない場合、[SSL 設定（SSL Settings）] タブは無効になります。SSL でリモート アクセス VPN を使用している場合、スマートアカウントで強力な暗号化機能が有効になっている必要があります。詳細については、スマート ライセンスのタイプと制約事項 （101 ページ）を参照してください。

ステップ 1 [デバイス（Devices）] > [プラットフォーム設定（Platform Settings）] を選択し、Firepower Threat Defense ポリシーを作成または編集します。

ステップ 2 [SSL] を選択します。

ステップ 3 エントリを、[SSL 設定の追加（Add SSL Configuration）] テーブルに追加します。

a) [追加（Add）] をクリックして新しいエントリを作成するか、エントリがすでにある場合は、[編集（Edit）] アイコンをクリックします。

b) ドロップダウン リストから必要なセキュリティ設定を選択します。

- [**プロトコル バージョン（Protocol Version）**]：リモート アクセス VPN セッションを設定するときに使用する TLS プロトコルを指定します。
- [**セキュリティ レベル（Security Level）**]：SSL で設定するセキュリティ ポジショニングのタイプを指定します。

ステップ 4 選択するプロトコル バージョンに基づく [使用可能なアルゴリズム（Available Algorithms）] を選択し、[追加（Add）] をクリックして選択したプロトコルに含めます。詳細については、次を参照してください。SSL 設定について （1372 ページ）

アルゴリズムは、選択するプロトコルバージョンに基づいてリストされます。それぞれのセキュリティ プロトコルは、セキュリティ レベルの設定の一意のアルゴリズムを識別します。

ステップ 5 [OK] をクリックして変更を保存します。

次のタスク

これで、[展開（Deploy）] をクリックし、割り当てたデバイスにポリシーを展開できます。

SSL 設定について

Firepower Threat Defense デバイスでは、セキュア ソケット レイヤ（SSL）プロトコルと Transport Layer Security（TLS）を使用して、リモート クライアントからのリモート アクセス VPN のセキュア メッセージ伝送をサポートします。[SSL 設定（SSL Settings）] ウィンドウでは、SSL でのリモート VPN アクセス中に、ネゴシエートとメッセージ伝送に使用される SSL バージョンと暗号化アルゴリズムを設定できます。

SSL 設定は、次の場所で構成します。

[デバイス（Devices）] > [プラットフォーム設定（Platform Settings）] > [SSL]

フィールド

[最小 SSL バージョン サーバ（Minimum SSL Version Server）]：Firepower Threat Defense デバイスがサーバとして動作するときに使用する最小バージョンの SSL/TLS プロトコルを指定します。たとえば、リモート アクセス VPN ゲートウェイとして機能する場合です。ドロップダウン リストからプロトコル バージョンを選択します。

TLS V1	SSLv2 クライアントの hello を受け入れ、TLSv1（以降）をネゴシエートします。
TLSV1.1	SSLv2 クライアントの hello を受け入れ、TLSv1.1（以降）をネゴシエートします。
TLSV1.2	SSLv2 クライアントの hello を受け入れ、TLSv1.2（以降）をネゴシエートします。

[Diffie-Hellman グループ（Diffie-Hellmann Group）]：ドロップダウン リストからグループを選択します。使用可能なオプションは、[Group1]（768 ビット絶対値）、[Group2]（1024 ビット絶対値）、[Group5]（1536 ビット絶対値）、[Group14]（2048 ビット絶対値、224 ビット素数位数）、および [Group24]（2048 ビット絶対値、256 ビット素数位数）です。デフォルト値は [Group1] です。

[楕円曲線 Diffie-Hellman グループ（Elliptical Curve Diffie-Hellman Group）]：ドロップダウン リストからグループを選択します。使用可能なオプションは、[Group19]（256 ビット EC）、[Group20]（384 ビット EC）、および [Group21]（521 ビット EC）です。デフォルト値は [Group19] です。

TLSv1.2 では、次の暗号方式のサポートが追加されています。

- ECDHE-ECDSA-AES256-GCM-SHA384
- ECDHE-RSA-AES256-GCM-SHA384
- DHE-RSA-AES256-GCM-SHA384
- AES256-GCM-SHA384
- ECDHE-ECDSA-AES256-SHA384
- ECDHE-RSA-AES256-SHA384
- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-RSA-AES128-GCM-SHA256
- DHE-RSA-AES128-GCM-SHA256
- RSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES128-SHA256
- ECDHE-RSA-AES128-SHA256

（注） 優先度が最も高いのは ECDSA 暗号および DHE 暗号です。

Firepower Threat Defense デバイスでサポートしたいプロトコル バージョン、セキュリティ レベル、および暗号アルゴリズムを指定するために、SSL 設定テーブルを使用できます。

[プロトコル バージョン（Protocol Version）]：Firepower Threat Defense デバイスでサポートされ、SSL 接続に使用されるプロトコル バージョンを一覧表示します。利用可能なプロトコル バージョンは次のとおりです。

- デフォルト
- TLSV1
- TLSV1.1
- TLSV1.2
- DTLSv1

[セキュリティ レベル（Security Level）]：Firepower Threat Defense デバイスでサポートされ、SSL 接続に使用される暗号セキュリティ レベルを一覧表示します。次のいずれかのオプションを選択します。

[All]：NULL-SHA を含むすべての暗号。

[Low]：NULL-SHA を除くすべての暗号。

[Medium]：NULL-SHA、DES-CBC-SHA、RC4-SHA、および RC4-MD5 を除くすべての暗号（これがデフォルトです）。

[Fips]：NULL-SHA、DES-CBC-SHA、RC4-MD5、RC4-SHA、および DES-CBC3-SHA を除く FIPS 準拠のすべての暗号。

[高（High）]：SHA-2 暗号を使用する AES-256 のみを含み、TLS バージョン 1.2 およびデフォルト バージョンに適用される。

[Custom]：[Cipher algorithms/custom string] ボックスで指定する 1 つ以上の暗号。このオプションでは、OpenSSL 暗号定義文字列を使用して暗号スイートを詳細に管理できます。

[暗号アルゴリズム/カスタム文字列（Cipher Algorithms/Custom String）]：Firepower Threat Defense デバイスでサポートされ、SSL 接続に使用される暗号アルゴリズムを一覧表示します。OpenSSL を使用した暗号の詳細については、https://www.openssl.org/docs/apps/ciphers.html を参照してください。 https://www.openssl.org/docs/apps/ciphers.html

Firepower Threat Defense デバイスでは、サポートされる暗号方式の優先度が次のように指定されています。

TLSv1.2 のみでサポートされる暗号方式

ECDHE-ECDSA-AES256-GCM-SHA384
ECDHE-RSA-AES256-GCM-SHA384

DHE-RSA-AES256-GCM-SHA384
AES256-GCM-SHA384
ECDHE-ECDSA-AES256-SHA384
ECDHE-RSA-AES256-SHA384
DHE-RSA-AES256-SHA256
AES256-SHA256
ECDHE-ECDSA-AES128-GCM-SHA256
ECDHE-RSA-AES128-GCM-SHA256
DHE-RSA-AES128-GCM-SHA256
AES128-GCM-SHA256
ECDHE-ECDSA-AES128-SHA256
ECDHE-RSA-AES128-SHA256
DHE-RSA-AES128-SHA256
AES128-SHA256

TLSv1.1 または TLSv1.2 でサポートされない暗号方式

RC4-SHA
RC4-MD5
DES-CBC-SHA
NULL-SHA

セキュア シェルの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin Access Admin Network Admin

FTD デバイス上で 1 つ以上のデータ インターフェイスへの SSH 接続を許可するには、セキュア シェル設定を構成します。 SSH は診断論理インターフェイスに対してサポートされません。物理的な管理インターフェイスは、診断論理インターフェイスと管理論理インターフェイスの

間で共有できます。SSH は管理論理インターフェイス上でデフォルトで有効になっていますが、この画面は管理 SSH アクセスに影響しません。

管理論理インターフェイスはデバイスの他のインターフェイスから切り離されています。これは、Firepower Management Center にデバイスを設定し、登録するために使用されます。データインターフェイスの SSH は、管理インターフェイスの SSH と内部および外部ユーザ リストを共有します。その他の設定は個別に設定されます。データ インターフェイスでは、この画面を使用して SSH とアクセス リストを有効にします。データ インターフェイスの SSH トラフィックは通常のルーティング設定を使用し、設定時に設定されたスタティック ルートや CLI で設定されたスタティック ルートは使用しません。

管理インターフェイスの場合、SSH アクセス リストを設定するには『Firepower Threat Defense Command Reference』の **configure ssh-access-list** コマンドを参照してください。スタティック ルートを設定するには、**configure network static-routes** コマンドを参照してください。デフォルトでは、初期設定時に管理インターフェイスからデフォルト ルートを設定します。

SSH を使用するには、ホスト IP アドレスを許可するアクセス ルールは必要ありません。このセクションの手順に従って、SSH アクセスを設定する必要があるだけです。

SSH は、到達可能なインターフェイスにのみ使用できます。SSH ホストが外部インターフェイスにある場合、外部インターフェイスへの直接管理接続のみ開始できます。

デバイスでは、最大 5 つの同時 SSH 接続を許可できます。

（注） すべてのアプライアンスでは、SSH を介した CLI またはシェルへのログイン試行が 3 回連続して失敗すると、SSH 接続は終了します。

始める前に

- SSH 内部ユーザは、**configure user add** コマンドを使用して CLI でのみ設定できます。CLI での内部ユーザの追加 （60 ページ）を参照してください。デフォルトでは、初期設定時にパスワードを設定した**Admin**ユーザが存在します。LDAP または RADIUS 上の外部ユーザは、プラットフォーム設定で [外部認証（External Authentication）] を設定することによっても設定できます。SSH の外部認証の設定 （1361 ページ）を参照してください。
- デバイスへの SSH 接続を許可するホストまたはネットワークを定義するネットワーク オブジェクトが必要です。手順の一部としてオブジェクトを追加できますが、IP アドレスのグループを特定するためにオブジェクト グループを使用する場合は、ルールで必要なグループがすでに存在することを確認します。**[オブジェクト（Objects）] > [オブジェクト管理（Object Management）]** を選択してオブジェクトを設定します。

（注） システムが提供する **any** ネットワーク オブジェクトは使用できません。代わりに、**any-ipv4** または **any-ipv6** を使用します。

ステップ 1 **[デバイス（Devices）] > [プラットフォーム設定（Platform Settings）]** を選択し、FTD ポリシーを作成または編集します。

ステップ 2 [セキュア シェル（Secure Shell）] を選択します。

ステップ 3 SSH 接続を許可するインターフェイスと IP アドレスを指定します。

この表を使用して、SSH 接続を受け入れるインターフェイス、およびそれらの接続を許可されるクライアントの IP アドレスを制限します。個々の IP アドレスはなく、ネットワーク アドレスを使用できます。

a) [追加（Add）] をクリックして新しいルールを追加するか、[編集（Edit）] アイコンをクリックして既存のルールを編集します。

b) 次のルール プロパティを設定します。

- [IP アドレス（IP Address）]：SSH 接続を許可するホストまたはネットワークを特定するネットワーク オブジェクト。オブジェクトをドロップダウン メニューから選択するか、または + ボタンをクリックして新しいネットワーク オブジェクトを追加します。
- [セキュリティ ゾーン（Security Zones）]：SSH 接続を許可するインターフェイスを含むゾーンを追加します。ゾーンに存在しないインターフェイスの場合は、[選択されたセキュリティ ゾーン（Selected Security Zone）] リストの下のフィールドにインターフェイス名を入力し、[追加（Add）] をクリックします。選択されているインターフェイスまたはゾーンがデバイスに含まれているときにのみ、これらのルールがデバイスに適用されます。

c) [OK] をクリックします。

ステップ 4 **[Save（保存）]** をクリックします。

これで、[Deploy] をクリックして割り当てられているデバイスにポリシーを展開できます。変更はポリシーを導入するまで有効になりません。

SMTP の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin Access Admin Network Admin

Syslog 設定で電子メール アラートを設定する場合は、SMTP サーバを指定する必要があります。Syslog で設定する送信元電子メール アドレスは、SMTP サーバの有効なアカウントである必要があります。

始める前に

プライマリおよびセカンダリ SMTP サーバのホストアドレスを定義するネットワーク オブジェクトが存在することを確認します。**[オブジェクト（Objects）] > [オブジェクト管理（Object Management）]** を選択してオブジェクトを定義します。または、ポリシーの編集時にオブジェクトを作成することもできます。

ステップ 1 **[デバイス（Devices）] > [プラットフォーム設定（Platform Settings）]** を選択し、FTD ポリシーを作成または編集します。

ステップ 2 [SMTP サーバ（SMTP Server）] をクリックします。

ステップ 3 [プライマリ サーバの IP アドレス（Primary Server IP Address）]、およびオプションで、[セカンダリ サーバの IP アドレス（Secondary Server IP Address）] を特定するネットワーク オブジェクトを選択します。

ステップ 4 **[Save（保存）]** をクリックします。

これで、[Deploy] をクリックして割り当てられているデバイスにポリシーを展開できます。変更はポリシーを導入するまで有効になりません。

SNMP の脅威に対する防御の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin Access Admin Network Admin

簡易ネットワーク管理プロトコル（SNMP）は、PC またはワークステーションで実行されているネットワーク管理ステーションが、スイッチ、ルータ、セキュリティアプライアンスなどのさまざまなタイプのデバイスのヘルスとステータスをモニタするための標準的な方法を定義します。[SNMP] ページを使用して、SNMP 管理ステーションによってモニタされるようにファイアウォール デバイスを設定できます。

簡易ネットワーク管理プロトコル（SNMP）は、集中管理する場所からのネットワーク デバイスのモニタリングをイネーブルにします。Cisco セキュリティ アプライアンスでは、SNMP バージョン 1、2c、および 3 を使用したネットワーク モニタリングに加えて、トラップおよび SNMP 読み取りアクセスがサポートされます。SNMP 書き込みアクセスはサポートされません。

SNMPv3 は、読み取り専用ユーザと AES128 による暗号化のみをサポートしています。

（注） 外部 SNMP サーバでアラートを作成するには、[ポリシー（Policies）]>[アクション（Action）] > [アラート（Alerts）] にアクセスします。 > >

ステップ 1 **[デバイス（Devices）] > [プラットフォーム設定（Platform Settings）]** を選択し、FTD ポリシーを作成または編集します。

ステップ 2 [SNMP] を選択します。

ステップ 3 SNMP を有効にし、基本オプションを設定します。

- [SNMP サーバを有効にする（Enable SNMP Servers）]：設定された SNMP ホストに SNMP 情報を提供するかどうかを指定します。このオプションの選択を解除すると、設定情報を保持したまま、SNMP モニタリングをディセーブルにできます。
- [コミュニティ ストリングの表示（Read Community String）]、[確認（Confirm）]：SNMP 管理ステーションが FTD デバイスに要求を送信する際に使用するパスワードを入力します。SNMP コミュニティストリングは、SNMP 管理ステーションと管理対象のネットワーク ノード間の共有秘密キーです。セキュリティ デバイスでは、このパスワードを使用して、着信 SNMP 要求が有効かどうかを判断します。パスワードは大文字小文字が区別される、最大 32 文字の英数字の文字列です。スペースと特殊文字は使用できません。
- [システム管理者名（System Administrator Name）]：デバイス管理者またはその他の担当者の名前を入力します。この文字列は大文字と小文字が区別され、最大 127 文字です。スペースを使用できますが、複数のスペースを入力しても 1 つのスペースになります。
- [場所（Location）]：このセキュリティ デバイスの場所を入力します（Building 42, Sector 54 など）。この文字列は大文字と小文字が区別され、最大 127 文字です。スペースを使用できますが、複数のスペースを入力しても 1 つのスペースになります。
- [ポート（Port）]：着信要求が受け入れられる UDP ポートを入力します。デフォルトは 161 です。

ステップ 4 （SNMPv3 のみ）SNMPv3 ユーザの追加 （1379 ページ）。

ステップ 5 SNMP ホストの追加 （1381 ページ）。

ステップ 6 SNMP トラップの設定 （1383 ページ）。

ステップ 7 **[Save（保存）]** をクリックします。

これで、[Deploy] をクリックして割り当てられているデバイスにポリシーを展開できます。変更はポリシーを導入するまで有効になりません。

SNMPv3 ユーザの追加

（注） SNMPv3 でのみユーザを作成できます。以下の手順は、SNMPv1 または SNMPv2c には適用されません。

SNMPv3 は読み取り専用ユーザのみをサポートすることに注意してください。

SNMP ユーザには、ユーザ名、認証パスワード、暗号化パスワードおよび使用する認証アルゴリズムと暗号化アルゴリズムが指定されています。認証アルゴリズムのオプションは MD5 と SHA です。暗号化アルゴリズムのオプションは DES、3DES と AES128 です。

ステップ 1 **[デバイス（Devices）] > [プラットフォーム設定（Platform Settings）]** を選択し、FTD ポリシーを作成または編集します。

ステップ 2 目次の [SNMP] をクリックして、[ユーザ（User）] タブをクリックします。

ステップ 3 [追加（Add）] をクリックします。

ステップ 4 [セキュリティ レベル（Security Level）] ドロップダウン リストからユーザに適したセキュリティ レベルを選択します。

- **Auth**：認証はありますがプライバシーはありません。メッセージが認証されることを意味します。
- **No Auth**：認証もプライバシーもありません。メッセージにどのようなセキュリティも適用されないことを意味します。
- **Priv**：認証とプライバシーがあります。メッセージが認証および暗号化されることを意味します。

ステップ 5 [ユーザ名（Username）] フィールドに SNMP ユーザの名前を入力します。このユーザ名は 32 文字以下であることが必要です。

ステップ 6 [暗号化パスワード タイプ（Encryption Password Type）] ドロップダウン リストから使用するパスワードのタイプを選択します。

- **Clear text**：FTD デバイスは、デバイスへの導入時を待ってパスワードを暗号化します。
- **Encrypted**：FTD デバイスは、暗号化を済ませたパスワードを直接展開します。

ステップ 7 [認証アルゴリズム タイプ（Auth Algorithm Type）] ドロップダウン リストから MD5 または SHA のうち、使用する認証タイプを選択します。

ステップ 8 認証に使用するパスワードを、[認証パスワード（Authentication Password）] フィールドに入力します。暗号化パスワードタイプに [暗号化（Encrpted）] を選択した場合、パスワードは xx:xx:xx... という形式にフォーマットされます。ここで、xx は 16 進数の値です。

（注） パスワードの長さは、選択した認証アルゴリズムによって異なります。すべてのパスワードの長さを 256 文字以下とする必要があります。

暗号化パスワードタイプに [クリア テキスト（Clear Text）] を選択した場合、[確認（Confirm）] フィールドにパスワードをもう一度入力してください。

ステップ 9 [暗号化タイプ（Encryption Type）] ドロップダウン リストで、AES128、AES192、AES256、3DES、DES の中から使用する暗号化タイプを選択します。

（注） AES または 3DES 暗号化を使用するには、デバイスに適切なライセンスをインストールしておく必要があります。

ステップ 10 [暗号化パスワード（Encryption Password）] フィールドに暗号化で使用するパスワードを入力します。暗号化パスワードタイプに [暗号化（Encrpted）] を選択した場合、パスワードは xx:xx:xx... という形式にフォーマットされます。ここで、xx は 16 進数の値です。暗号化を行う場合のパスワードの長さは選択された暗号化のタイプにより異なります。パスワードの長さは次のとおりです（各 xx は 1 つのオクテットを示します）。

- AES 128 では 16 オクテットとする必要があります

- AES 192 では 24 オクテットとする必要があります
- AES 256 では 32 オクテットとする必要があります
- 3DES では 32 オクテットとする必要があります
- DES の長さはさまざまです。

（注） すべてのパスワードの長さを 256 文字以下とする必要があります。

暗号化パスワードタイプに [クリア テキスト（Clear Text）] を選択した場合、[確認（Confirm）] フィールドにパスワードをもう一度入力してください。

ステップ 11 [OK] をクリックします。

ステップ 12 **[Save（保存）]** をクリックします。

これで、[Deploy] をクリックして割り当てられているデバイスにポリシーを展開できます。変更はポリシーを導入するまで有効になりません。

SNMP ホストの追加

[ホスト（Host）] タブを使用して、[SNMP] ページにある [SNMP ホスト（SNMP Hosts）] テーブルのエントリを追加または編集します。これらのエントリは、FTDデバイスへのアクセスが許可されている SNMP 管理ステーションを示します。

最大 4000 個までホストを追加できます。ただし、トラップの対象として設定できるのはそのうちの 128 個だけです。

始める前に

SNMP管理ステーションを定義するネットワーク オブジェクトが存在することを確認します。[デバイス（Device）] > [オブジェクト管理（Object Management）] を選択し、ネットワークオブジェクトを設定します。 >

（注） サポートされているネットワーク オブジェクトには、IPv6 ホスト、IPv4 ホスト、IPv4 範囲および IPv4 サブネット アドレスが含まれます。

ステップ 1 **[デバイス（Devices）]** > **[プラットフォーム設定（Platform Settings）]** を選択し、FTD ポリシーを作成または編集します。

ステップ 2 目次の [SNMP] をクリックして、[ホスト（Hosts）] タブをクリックします。

ステップ 3 [追加（Add）] をクリックします。

ステップ 4 [IP アドレス（IP Address）] フィールドに、有効な Ipv6 ホストまたは IPv4 ホストを入力するか、SNMP 管理ステーションのホストアドレスを定義するネットワーク オブジェクトを選択します。

IP アドレスには、IPv6 ホスト、IPv4 ホスト、IPv4 範囲または IPv4 サブネットを使用できます。

ステップ 5 [SNMP バージョン（SNMP Version）] ドロップダウン リストから、適切な SNMP バージョンを選択します。

ステップ 6 （SNMPv3 のみ）[ユーザ名（User Name）] ドロップダウン リストから設定した SNMP ユーザのユーザ名を選択します。

（注） SNMP ホストごとに 23 人までの SNMP ユーザを関連付けることができます。

ステップ 7 （SNMPv1、2c のみ）[Read コミュニティ ストリング（Read Community String）] フィールドに、デバイスの読み取りアクセスのためにすでに設定してあるコミュニティ ストリングを入力します。確認のためにこの文字列を再入力します。

（注） この文字列は、この SNMP ステーションで使用されている文字列が [SNMP サーバを有効にする（Enable SNMP Server）] セクションに定義済みのものと異なる場合のみ必須です。

ステップ 8 デバイスと SNMP 管理ステーションの間の通信タイプを選択します。両方のタイプを選択できます。

- **[ポーリング（Poll）]**：管理ステーションは定期的にデバイスに情報を要求します。
- **[トラップ（Trap）]**：デバイスは、イベント発生時にこれをトラップし、管理ステーションに送信します。

（注） SNMP ホストの IP アドレスが IPv4 範囲または IPv4 サブネットのいずれかである場合、[ポーリング（Poll）] と [トラップ（Trap）] の両方ではなく、いずれかを設定できます。

ステップ 9 [ポート（Port）] フィールドに、SNMP ホストの UDP ポート番号を入力します。デフォルト値は 162 です。有効な範囲は 1 ～ 65535 です。

ステップ 10 [追加（Add）] をクリックし、この SNMP 管理ステーションがデバイスにアクセスするインターフェイスを入力または選択します。

ステップ 11 [ゾーン/インターフェイス（Zones/Interfaces）] リストに、デバイスが管理ステーションとの通信を行うインターフェイスが含まれたゾーンを追加します。ゾーン内にないインターフェイスの場合は、[選択したゾーン/インターフェイス（Selected Zone/Interface）] リストの下のフィールドにインターフェイス名を入力し、[追加（Add）] をクリックします。デバイスに選択したインターフェイスまたはゾーンが含まれている場合にのみ、デバイスでホストが設定されます。

（注） インターフェイスの IP アドレスが、ステップ 4（1381 ページ） の SNMP ホストに定義されている IP アドレスの値と競合しないことを確認します。

ステップ 12 [OK] をクリックします。

ステップ 13 **[Save（保存）]** をクリックします。

これで、[Deploy] をクリックして割り当てられているデバイスにポリシーを展開できます。変更はポリシーを導入するまで有効になりません。

SNMP トラップの設定

[SNMP トラップ] タブを使用して、FTD デバイスの SNMP トラップ（イベント通知）を設定します。トラップは参照とは異なります。トラップは、生成されるリンクアップイベント、リンクダウン イベント、Syslog イベントなど、特定のイベントに対する FTD デバイスから管理ステーションへの割り込み「コメント」です。デバイスの SNMP オブジェクト ID（OID）は、デバイスから送信される SNMP イベント トラップに表示されます。

一部のトラップは、特定のハードウェア モデルに適用できません。これらのトラップは、これらのモデルの 1 つのポリシーを適用すると無視されます。たとえば、すべてのモデルに現場交換可能ユニットがあるわけではありません。そのため、[現場交換可能ユニット挿入/削除（Field Replaceable Unit Insert/Delete）] トラップはこれらのモデルで設定されません。

SNMP トラップは、標準またはエンタープライズ固有の MIB のいずれかで定義されます。標準トラップは IETF によって作成され、さまざまな RFC に記載されています。SNMP トラップは、FTD ソフトウェアにコンパイルされています。

必要に応じて、次の場所から RFC、標準 MIB、および標準トラップをダウンロードできます。

http://www.ietf.org/

次の場所から Cisco MIB、トラップ、および OID の完全なリストを参照してください。

ftp://ftp.cisco.com/pub/mibs/

また、Cisco OID を次の場所から FTP でダウンロードしてください。

ftp://ftp.cisco.com/pub/mibs/oid/oid.tar.gz

ステップ 1 **[デバイス（Devices）] > [プラットフォーム設定（Platform Settings）]** を選択し、FTD ポリシーを作成または編集します。

ステップ 2 目次の [SNMP] をクリックし、[SNMP トラップ（SNMP Traps）] タブをクリックして、FTD デバイスの SNMP トラップ（イベント通知）を設定します。

ステップ 3 適切な [Enable Traps] オプションを選択します。いずれかまたは両方のオプションを選択できます。

a) [すべての SNMP トラップを有効にする（Enable All SNMP Traps）] にマークを付けて、連続する 4 セクションですべてのトラップを素早く選択します。

b) [すべての Syslog トラップを有効にする（Enable All Syslog Traps）] にマークを付けて、トラップ関連の Syslog メッセージの伝送を有効にします。

（注） SNMP トラップはリアルタイムに近いことが期待されるため、FTD からの他の通知メッセージよりも優先順位が高いです。すべての SNMP トラップまたは syslog トラップを有効にすると、SNMP プロセスがエージェントとネットワーク内で過剰にリソースを消費し、システムがハングアップする可能性があります。システムの遅延、未完了の要求、またはタイムアウトが発生した場合は、SNMP トラップと syslog トラップを選択して有効にすることができます。また、syslog メッセージの生成レートは、重大度レベルまたはメッセージ ID によって制限できます。たとえば、212 で始まる syslog メッセージ ID はすべて、SNMP クラスに関連しています。syslog メッセージの生成レートの制限 （1399 ページ）を参照してください。

ステップ 4 [標準（Standard）]セクションのイベント通知トラップは、既存のポリシーでは、デフォルトで有効になっています。

- [認証（Authentication）]：未認可の SNMP アクセス。この認証エラーは、間違ったコミュニティ ストリングが付いたパケットによって発生します。
- [リンクアップ（Link Up）]：通知に示されているとおり、デバイスの通信リンクの 1 つが使用可能になりました。
- [リンクダウン（Link Down）]：通知に示されているとおり、デバイスの通信リンクの 1 つにエラーが発生しました。
- [コールドスタート（Cold Start）]：デバイスが自動で再初期化しているときに、その設定またはプロトコル エンティティの実装が変更されることがあります。
- [ウォームスタート（Warm Start）]：デバイスが自動で再初期化しているときに、その設定またはプロトコル エンティティの実装が変更されることはありません。

ステップ 5 [エンティティ MIB（Entity MIB）] セクションで好きなイベント通知トラップを選択します。

- [現場交換可能ユニット挿入（Field Replaceable Unit Insert）]：示されているとおり、現場交換可能ユニット（FRU）が挿入されました（FRU には電源装置、ファン、プロセッサ モジュール、インターフェイス モジュールなどの組み立て部品が含まれます）。
- [現場交換可能ユニット除外（Field Replaceable Unit Remove）]：通知に示されているとおり、現場交換可能ユニット（FRU）が取り外されました。
- [設定変更（Configuration Change）]：通知に示されているとおり、ハードウェアに変更がありました。

ステップ 6 [リソース（Resource）] セクションで好きなイベント通知トラップを選択します。

- [接続制限到達（Connection Limit Reached）]：このトラップは、設定した接続制限に達したため、接続試行が拒否されたことを示します。

ステップ 7 [その他（Other）] セクションで好きなイベント通知トラップを選択します。

- [NAT パケット破棄（NAT Packet Discard）]：IP パケットが NAT 機能により廃棄されると、この通知が生成されます。ネットワーク アドレス変換の使用可能なアドレスまたはポートが、設定したしきい値を下回りました。

ステップ 8 **[Save（保存）]** をクリックします。

これで、[Deploy]をクリックして割り当てられているデバイスにポリシーを展開できます。変更はポリシーを導入するまで有効になりません。

Syslog の設定概要

FTD デバイスのシステム ロギング（syslog）を有効にすることができます。情報をロギングすることで、ネットワークの問題またはデバイス設定の問題を特定して分離できます。また、一部のセキュリティ イベントを syslog サーバに送信することもできます。ここでは、ロギングとその設定方法について説明します。

Syslog について

システム ロギングは、デバイスから syslog デーモンを実行するサーバへのメッセージを収集する方法です。中央の syslog サーバへロギングは、ログおよびアラートの集約に役立ちます。シスコ デバイスでは、これらのログ メッセージを UNIX スタイルの syslog サービスに送信できます。syslog サービスは、シンプル コンフィギュレーション ファイルに従って、メッセージを受信してファイルに保存するか、出力します。この形式のロギングは、保護された長期的な保存場所をログに提供します。ログは、ルーチン トラブルシューティングおよびインシデント処理の両方で役立ちます。

表 *97 :* のシステム ログ *Firepower Threat Defense*

関連ログ	詳細	設定
デバイスとシステム ヘルス、ネットワーク構成	この syslog 設定では、データ プレーン上で実行されている機能、つまり **show running-config** コマンドで表示できる CLI 設定で定義されている機能に関するメッセージが生成されます。これには、ルーティング、VPN、データ インターフェイス、DHCP サーバ、NAT などの機能が含まれます。データ プレーンの syslog メッセージには番号が付けられており、ASA ソフトウェアを実行しているデバイスで生成されるものと同じです。ただし、Firepower Threat Defense は、必ずしも ASA ソフトウェアで使用可能なすべてのメッセージ タイプを生成するとは限りません。これらのメッセージの詳細については、https://www.cisco.com/c/en/us/td/docs/security/firepower/Syslogs/b_fptd_syslog_guide.html の『*Cisco Firepower Threat Defense Syslog Messages*』を参照してください。この構成については、次のトピックで説明します。	**プラットフォームの設定**

関連ログ	詳細	設定
（バージョン 6.3 以降を実行しているデバイス） セキュリティ イベント	この syslog の設定では、ファイルとマルウェア、接続、セキュリティ インテリジェンス、および侵入イベントのアラートが生成されます。詳細については、セキュリティ イベントの syslog メッセージの送信について（2894 ページ）およびサブトピックを参照してください。	アクセス コントロール ポリシーの [プラットフォーム設定（Platform Settings）] と [ロギング（Logging）] タブ
（すべてのデバイス） ポリシー、ルール、およびイベント	この syslog 設定では、アラート応答のサポート設定（2808 ページ） で説明されているように、アクセス制御ルール、侵入ルール、およびその他のアドバンスド サービスに関するアラートが生成されます。これらのメッセージには番号が付けられていません。このタイプの syslog の設定については、Syslog アラート応答の作成（2810 ページ） を参照してください。	アクセス コントロール ポリシーの [アラート応答（Alert Responses）] と [ロギング（Logging）] タブ

複数の syslog サーバを設定し、各サーバに送信されるメッセージとイベントを制御できます。また、コンソール、電子メール、内部バッファなどの異なる宛先を構成することもできます。

重大度

次の表に、syslog メッセージの重大度の一覧を示します。

表 *98 : Syslog* メッセージの重大度

レベル番号	重大度	説明
0	**緊急**	システムが使用不可能な状態。
1	**アラート**	すぐに措置する必要があります。
2	**重大**	深刻な状況です。
3	**エラー**	エラー状態です。
4	**警告**	警告状態。
5	**通知**	正常ですが、注意を必要とする状況です。
6	**情報**	情報メッセージです。
7	**デバッグ**	デバッグ メッセージです。

（注） Firepower Threat Defenseは、重大度 0（emergencies）の syslog メッセージを生成しません。

syslog メッセージ フィルタリング

生成される syslog メッセージは、特定の syslog メッセージだけが特定の出力先に送信されるようにフィルタリングできます。たとえば、Firepower Threat Defense デバイスを設定して、すべての syslog メッセージを 1 つの出力先に送信し、それらの syslog メッセージのサブセットを別の出力先に送信することができます。

具体的には、syslog メッセージが次の基準に従って出力先に転送されるようにできます。

- syslog メッセージの ID 番号

  （これは、接続および侵入イベントなどのセキュリティ イベントの syslog メッセージには適用されません。）

- syslog メッセージの重大度
- syslog メッセージ クラス（機能エリアと同等）

  （これは、接続および侵入イベントなどのセキュリティ イベントの syslog メッセージには適用されません。）

これらの基準は、出力先を設定するときに指定可能なメッセージリストを作成して、カスタマイズできます。あるいは、メッセージ リストとは無関係に、特定のメッセージ クラスを各タイプの出力先に送信するようにFirepower Threat Defense デバイスを設定することもできます。

（メッセージ リストは、接続および侵入イベントなどのセキュリティ イベントの syslog メッセージには適用されません。）

syslog メッセージ クラス

（注） このトピックは、セキュリティ イベント（接続、侵入など）のメッセージには適用されません。

syslog メッセージのクラスは次の 2 つの方法で使用できます。

- syslog メッセージのカテゴリ全体の出力場所を指定します。
- メッセージ クラスを指定するメッセージ リストを作成します。

syslog メッセージ クラスは、デバイスの特徴または機能と同等のタイプによって syslog メッセージを分類する方法を提供します。たとえば、RIP クラスは RIP ルーティングを示します。

特定のクラスに属する syslog メッセージの ID 番号はすべて、最初の 3 桁が同じです。たとえば、611 で始まるすべての syslog メッセージ ID は、vpnc（VPN クライアント）クラスに関連付けられています。VPN クライアント機能に関連付けられている syslog メッセージの範囲は、611101 ～ 611323 です。

また、ほとんどの ISAKMP syslog メッセージには先頭に付加されたオブジェクトの共通セットが含まれているため、トンネルを識別するのに役立ちます。これらのオブジェクトは、使用可能なときに、syslog メッセージの説明テキストの前に付加されます。syslog メッセージ生成時にオブジェクトが不明な場合、特定の heading = value の組み合わせは表示されません。

オブジェクトは次のように先頭に付加されます。

Group = *groupname*, Username = *user*, IP = *IP_address*

Group はトンネル グループ、Username はローカル データベースまたは AAA サーバから取得したユーザ名、IP アドレスはリモート アクセス クライアントまたはレイヤ 2 ピアのパブリック IP アドレスです。

次の表に、メッセージ クラスと各クラスのメッセージ ID の範囲をリストします。

表 *99 : syslog* メッセージ クラスおよび関連付けられているメッセージ *ID* 番号

クラス	定義	Syslog メッセージ ID 番号
auth	User Authentication	109、113
—	アクセス リスト	106
—	アプリケーション ファイアウォール	415
bridge	トランスペアレント ファイアウォール	110、220
ca	PKI 認証局	717
citrix	Citrix Client	723
—	クラスタ	747
—	カード管理	323
config	コマンド インターフェイス	111、112、208、308
csd	Secure Desktop	724
cts	Cisco TrustSec	776
dap	ダイナミック アクセス ポリシー	734
eap、eapoudp	ネットワーク アドミッション コントロールの EAP または EAPoUDP	333、334
eigrp	EIGRP ルーティング	336

クラス	定義	Syslog メッセージ ID 番号
電子メール	電子メール プロキシ	719
—	環境モニタリング	735
ha	フェールオーバー	101、102、103、104、105、210、311、709
—	Identity-Based ファイアウォール	746
ids	侵入検知システム	400、733
—	IKEv2 ツールキット	750、751、752
ip	IP スタック	209、215、313、317、408
ipaa	IP アドレス割り当て	735
ips	侵入防御システム	400、401、420
—	IPv6	325
—	ブラック リスト、ホワイト リスト、およびグレー リスト	338
—	ライセンス	444
mdm-proxy	MDM プロキシ	802
nac	ネットワーク アドミッション コントロール	731、732
nacpolicy	NAC ポリシー	731
nacsettings	NAC ポリシーを適用する NAC 設定	732
—	ネットワーク アクセス ポイント	713
np	ネットワーク プロセッサ	319
—	NP SSL	725
ospf	OSPF ルーティング	318、409、503、613
—	パスワードの暗号化	742
—	電話プロキシ	337
rip	RIP ルーティング	107、312
rm	Resource Manager	321
—	Smart Call Home	120

クラス	定義	Syslog メッセージ ID 番号
session	ユーザ セッション	106、108、201、202、204、302、303、304、305、314、405、406、407、500、502、607、608、609、616、620、703、710
snmp	SNMP	212
—	ScanSafe	775
ssl	SSL スタック	725
svc	SSL VPN クライアント	722
sys	システム	199、211、214、216、306、307、315、414、604、605、606、610、612、614、615、701、711、741
—	脅威の検出	733
tre	トランザクション ルール エンジン	780
—	UC-IME	339
tag-switching	サービス タグ スイッチング	779
vm	VLAN マッピング	730
vpdn	PPTP および L2TP セッション	213、403、603
vpn	IKE および IPsec	316、320、402、404、501、602、702、713、714、715
vpnc	VPN クライアント	611
vpnfo	VPN フェールオーバー	720
vpnlb	VPN ロード バランシング	718
—	VXLAN	778
webfo	WebVPN フェールオーバー	721
webvpn	WebVPN と AnyConnect Client	716
—	NAT および PAT	305

ロギングのガイドライン

この項では、ロギングを設定する前に確認する必要のある制限事項とガイドラインについて説明します。

IPv6 のガイドライン

- IPv6 がサポートされます。Syslog は、TCP または UDP を使用して送信できます。
- syslog 送信用に設定されたインターフェイスが有効であること、IPv6 対応であること、および syslog サーバが指定インターフェイス経由で到達できることを確認します。
- IPv6 上でのセキュア ロギングはサポートされません。

その他のガイドライン

- syslog サーバでは、syslogd というサーバプログラムを実行する必要があります。Windows では、オペレーティング システムの一部として syslog サーバを提供しています。
- Firepower Threat Defense デバイスが生成したログを表示するには、ロギングの出力先を指定する必要があります。ロギングの出力先を指定せずにロギングをイネーブルにすると、Firepower Threat Defense デバイス はメッセージを生成しますが、それらのメッセージは後で表示できる場所に保存されません。各ロギングの出力先は個別に指定する必要があります。
- 2 つの異なるリストまたはクラスを、異なる syslog サーバまたは同じロケーションに割り当てることはできません。
- 最大 16 台の syslog サーバを設定できます。
- syslog サーバは、Firepower Threat Defense デバイス 経由で到達できなければなりません。syslog サーバが到達できるインターフェイス上で、デバイスが ICMP 到達不能メッセージを拒否し、同じサーバに syslog を送信するように設定する必要があります。すべての重大度に対してロギングがイネーブルであることを確認します。syslog サーバがクラッシュしないようにするため、syslog 313001、 313004、および 313005 の生成を抑制します。
- syslog の UDP 接続の数は、ハードウェア プラットフォームの CPU の数と、設定する syslog サーバの数に直接関連しています。可能な UDP syslog 接続の数は常に、CPU の数と設定する syslog サーバの数を乗算した値と同じになります。たとえば各 syslog サーバでは次のようになります。
  - Firepower 4110 では最大 22 の UDP syslog 接続が可能です。
  - Firepower 4120 では最大 46 の UDP syslog 接続が可能です。

  これは予期されている動作です。グローバル UDP 接続アイドル タイムアウトはこれらのセッションに適用され、デフォルトは 2 分であることに注意してください。これらのセッションをこれよりも短い時間で閉じる場合にはこの設定を調整できますが、タイムアウトは syslog だけでなくすべての UDP 接続に適用されます。

- Firepower Threat Defense デバイス が TCP 経由で syslog を送信すると、syslogd サービスの再起動後、接続の開始に約 1 分かかります。

FTD デバイスの syslog ロギングの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin Access Admin Network Admin

ヒント セキュリティ イベント（接続イベントや侵入イベントなど）に関する syslog メッセージを送信するようにデバイスを設定すると、ほとんどの FTD プラットフォーム設定がこれらのメッセージに適用されません。セキュリティ イベントの syslog メッセージに適用する FTD プラットフォームの設定 （1393 ページ）を参照してください。

Syslog の設定を行うには、以下の手順を実行します。

始める前に

ロギングのガイドライン （1391 ページ）で要件を参照してください。

ステップ 1 **[デバイス（Devices）]** > **[プラットフォーム設定（Platform Settings）]** を選択し、FTD ポリシーを作成または編集します。

ステップ 2 目次の [Syslog] をクリックします。

ステップ 3 [ロギング設定（Logging Setup）] タブをクリックしてロギングを有効にし、FTP サーバの設定を指定し、フラッシュの使用を指定します。詳細については、ロギングの有効化および基本設定の構成 （1394ページ）を参照してください。

ステップ 4 [ロギング接続先（Logging Destinations）] タブをクリックして、特定の接続先へのロギングを有効にし、メッセージ重要度、イベント クラスまたはカスタム イベント リストでフィルタリングを指定します。詳細については、ロギング接続先の有効化 （1395 ページ）を参照してください。

ロギング接続先を有効にして、その接続先でメッセージを表示可能にする必要があります。

ステップ 5 [電子メール設定（E-mail Setup）] タブをクリックして、Syslog メッセージを電子メールとして送信する際に、その送信元アドレスとして使用する電子メール アドレスを指定します。詳細については、電子メール アドレスへの syslog メッセージの送信 （1397 ページ）を参照してください。

ステップ 6 [イベント リスト（Events List）] タブをクリックして、イベント クラス、重要度、イベント ID を含むカスタム イベント リストを定義します。詳細については、カスタム イベント リストの作成 （1398 ページ）を参照してください。

ステップ 7 [レート制限（Rate Limit）] タブをクリックして、設定されているすべての宛先に送信されるメッセージの量を指定し、レート制限を割り当てるメッセージの重大度を定義します。詳細については、syslog メッセージの生成レートの制限 （1399 ページ）を参照してください。

ステップ 8 [Syslog 設定（Syslog Settings）] タブをクリックして、サーバを Syslog 接続先として設定するために、ロギング機能を指定し、タイムスタンプの包含を有効にし、他の設定を有効にします。詳細については、Syslog 設定 （1400 ページ）を参照してください。

ステップ 9 [Syslog サーバ（Syslog Servers）] タブをクリックして、ロギング接続先として指定される Syslog サーバの IP アドレス、使用されているプロトコル、形式、およびセキュリティ ゾーンを指定します。詳細については、Syslog サーバの設定 （1402 ページ）を参照してください。

セキュリティ イベントの syslog メッセージに適用する FTD プラットフォームの設定

「セキュリティ イベント」には、接続、セキュリティ インテリジェンス、侵入、ファイルとマルウェアのイベントが含まれます。

[デバイス（Devices）] > [プラットフォーム設定（Platform Settings）] > [Threat Defense設定（Threat Defense Settings）] > [Syslog] ページとそのタブの syslog 設定の一部はセキュリティ イベントの syslog メッセージに適用されますが、多くの場合は、システム ヘルスとネットワークに関連するイベントのメッセージに適用されるだけです。

セキュリティ イベントの syslog メッセージには、次の設定が適用されます。

- [ロギング セットアップ（Logging Setup）] タブ：
  - **EMBLEM 形式で syslog を送信**
- [Syslog 設定（Syslog Settings）] タブ：
  - **syslog メッセージのタイムスタンプを有効化**
  - **タイムスタンプ形式**
  - **Enable Syslog Device ID**
- [Syslog サーバ（Syslog Servers）] タブ：
  - [Syslog サーバを追加（Add Syslog Server）] 形式（および設定済みサーバのリスト）のすべてのオプション

セキュリティ イベント syslog メッセージングを設定するためのベストプラクティス （2895 ページ）も参照してください。

ロギングの有効化および基本設定の構成

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin Access Admin Network Admin

データ プレーン イベントの syslog メッセージを生成するには、システムでロギングを有効にする必要があります。

また、ローカル バッファがいっぱいになると、フラッシュまたは FTP サーバ上のアーカイブを保存場所として設定することもできます。ログデータは保存後に操作できます。たとえば、特定タイプの syslog メッセージがログに記録されたときに特別なアクションが実行されるように指定したり、ログからデータを抽出してレポート用の別のファイルにその記録を保存したり、サイト固有のスクリプトを使用して統計情報を追跡したりできます。

次の手順では、基本的な syslog 設定の一部について説明します。

ヒント セキュリティ イベント（接続イベントや侵入イベントなど）に関する syslog メッセージを送信するようにデバイスを設定すると、ほとんどの FTD プラットフォーム設定がこれらのメッセージに適用されません。セキュリティ イベントの syslog メッセージに適用する FTD プラットフォームの設定 （1393 ページ）を参照してください。

ステップ 1 **[デバイス（Devices）] > [プラットフォーム設定（Platform Settings）]** を選択し、FTD ポリシーを作成または編集します。

ステップ 2 **[syslog] > [ロギングの設定（Logging Setup）]** を選択します。

ステップ 3 ロギングを有効にし、基本のロギング設定を構成します。

- [ロギングの有効化（Enable Logging）]：Firepower Threat Defense デバイスのデータ プレーン システム ロギングをオンにします。
- フェールオーバー スタンバイ ユニットでのロギングの有効化（Enable Logging on the Failover Standby Unit）：Firepower Threat Defense デバイスのスタンバイのロギングをオンにします。
- EMBLEM 形式での syslog の送信（Send syslogs in EMBLEM format）：すべてのロギング宛先に対して、EMBLEM 形式のロギングを有効にします。EMBLEM を有効にする場合は、UDP プロトコルを使用して syslog メッセージをパブリッシュする必要があります。EMBLEM は TCP と互換性がありません。
- デバッグ メッセージを syslog として送信（Send debug messages as syslogs）：すべてのデバッグ トレース出力を syslog にリダイレクトします。このオプションが有効になっている場合、syslog メッセージはコンソールに表示されません。したがって、デバッグ メッセージを表示するには、コンソールでロギングを有効にし、デバッグ syslog メッセージ番号とログ レベルの宛先として設定する必要があります。使用される syslog メッセージ番号は 711011 です。この syslog のデフォルト ログ レベルは [デバッグ（debug）] です。

- 内部バッファのメモリ サイズ（Memory Size of Internal Buffer）：ロギング バッファが有効の場合に syslog メッセージが保存される内部バッファのサイズを指定します。バッファが一杯になった場合は上書きされます。デフォルトは 4096 バイトです。指定できる範囲は 4096 ～ 52428800 です。

ステップ 4 （オプション）[FMC へのロギングを有効化（Enable Logging to FMC）] チェックボックスをオンにして、VPN ロギングを有効にします。[ログ レベル（Logging Level）] ドロップダウン リストから、VPN メッセージの syslog セキュリティ レベルを選択します。

レベルについては、重大度 （1386 ページ） を参照してください。

ステップ 5 （オプション）バッファが上書きされる前に、サーバにログ バッファの内容を保存するには、FTP サーバを設定します。FTP サーバ情報を指定します。

- FTP サーバ バッファ ラップ（FTP Server Buffer Wrap）：バッファの内容が上書きされる前に FTP サーバに保存するには、このボックスをオンにし、次のフィールドに必要な宛先情報を入力します。FTP 設定を削除するには、このオプションを選択解除します。
- IP アドレス（IP Address）：FTP サーバの IP アドレスを含むホスト ネットワーク オブジェクトを選択します。
- ユーザ名（User Name）：FTP サーバに接続するときに使用するユーザ名を入力します。
- パス（Path）：バッファの内容を保存するパスを FTP ルートからの相対で入力します。
- パスワードの確認（Password Confirm）：FTP サーバへのユーザ名の認証に使用されるパスワードを入力および確認します。

ステップ 6 （オプション）バッファが上書きされる前に、サーバにログ バッファの内容を保存するには、フラッシュ サイズを指定します。

- フラッシュ（Flash）：バッファの内容が上書きされる前にフラッシュ メモリに保存するには、このチェックボックスをオンにします。
- ロギングに使用する最大フラッシュ（KB）（Maximum flash to be used by logging (KB)）：フラッシュ メモリ内でロギングに使用される最大領域を指定します（KB）。範囲は、4 ～ 8044176 バイトです。
- 保持する最小空き領域（KB）（Minimum free space to be preserved (KB)）：フラッシュ メモリに保持する最小空き領域を指定します（KB）。範囲は、0 ～ 8044176 バイトです。

ステップ 7 **[Save（保存）]** をクリックします。

これで、[Deploy] をクリックして割り当てられているデバイスにポリシーを展開できます。変更はポリシーを導入するまで有効になりません。

ロギング接続先の有効化

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin Access Admin Network Admin

ロギング接続先を有効にして、その接続先でメッセージを表示可能にする必要があります。接続先を有効にするとき、その接続先に適用するメッセージフィルタも指定する必要があります。

ヒント セキュリティ イベント（接続イベントや侵入イベントなど）に関する syslog メッセージを送信するようにデバイスを設定すると、ほとんどの FTD プラットフォーム設定がこれらのメッセージに適用されません。セキュリティ イベントの syslog メッセージに適用する FTD プラットフォームの設定 （1393 ページ）を参照してください。

ステップ 1 **[デバイス（Devices）] > [プラットフォーム設定（Platform Settings）]** を選択し、FTD ポリシーを作成または編集します。

ステップ 2 [Syslog] > [ロギング接続先（Logging Destinations）] を選択します。 >

ステップ 3 接続先を有効にし、ロギング フィルタを適用するか、または既存の接続先を編集するには、[追加（Add）] をクリックします。

ステップ 4 [ロギング接続先（Logging Destinations）] ダイアログボックスで、接続先を選択し、接続先で使用するフィルタを設定します。

a) [ロギング接続先（Logging Destination）] ドロップダウンリストで、有効にする接続先を選択します。コンソール、メール、内部バッファ、SNMP トラップ、SSH セッション、Syslog サーバのそれぞれの接続先に各自のフィルタを作成できます。

（注） コンソールおよび SSH セッション ロギングは、診断 CLI でのみ機能します。**system support diagnostic-cli** を入力します。

b) [イベントクラス（Event Class）] で、テーブルに表示されていないすべてのクラスに適用するフィルタを選択します。

次のフィルタを設定できます。

- [重大度によるフィルタ（Filter on severity）]：重大度のレベルを選択します。設定したレベル以上のメッセージが接続先に送られます。
- [イベントリスト使用（Use Event List）]：フィルタを定義するイベントリストを選択します。このイベントリストは [イベントリスト（Event Lists）] タブで作成します。
- [ロギング無効（Disable Logging）]：この接続先へのメッセージ送信を停止します。

c) イベントクラスごとのフィルタを作成するには、[追加（Add）] をクリックして新しいフィルタを作成するか、既存のフィルタを編集し、そのクラスでのメッセージを制限するイベントクラスと重大度レベルを選択します。[OK] をクリックして、フィルタを保存します。

イベント クラスの説明については、syslog メッセージ クラス （1387 ページ） を参照してください。

d) [OK] をクリックします。

ステップ 5 **[Save（保存）]** をクリックします。

これで、[Deploy] をクリックして割り当てられているデバイスにポリシーを展開できます。変更はポリシーを導入するまで有効になりません。

電子メール アドレスへの syslog メッセージの送信

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin Access Admin Network Admin

電子メールとして送信される syslog メッセージの受信者リストを設定できます。

ヒント セキュリティ イベント（接続イベントや侵入イベントなど）に関する syslog メッセージを送信するようにデバイスを設定すると、ほとんどの FTD プラットフォーム設定がこれらのメッセージに適用されません。セキュリティ イベントの syslog メッセージに適用する FTD プラットフォームの設定 （1393 ページ）を参照してください。

始める前に

- SMTP サーバのプラットフォーム設定ページで SMTP サーバを設定します
- ロギングの有効化および基本設定の構成 （1394 ページ）
- ロギング接続先の有効化

ステップ 1 **[デバイス（Devices）] > [プラットフォーム設定（Platform Settings）]** を選択し、FTD ポリシーを作成または編集します。

ステップ 2 **[Syslog] > [電子メールの設定（Email Setup）]** を選択します。

ステップ 3 電子メール メッセージとして送信される syslog メッセージの送信元アドレスとして使用する電子メール アドレスを指定します。

ステップ 4 [Add] をクリックして、指定した syslog メッセージの受信者の電子メール アドレスを入力します。

ステップ 5 その受信者に送信する syslog メッセージの重大度レベルを、ドロップダウン リストから選択します。

宛先の電子メール アドレスに対して適用される syslog メッセージの重大度フィルタにより、指定された重大度レベル以上のメッセージが送信されます。レベルについては、重大度 （1386 ページ） を参照してください。

ステップ 6 [OK] をクリックします。

ステップ 7 **[Save（保存）]** をクリックします。

これで、[Deploy] をクリックして割り当てられているデバイスにポリシーを展開できます。変更はポリシーを導入するまで有効になりません。

カスタム イベント リストの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin Access Admin Network Admin

イベント リストは、ロギング接続先に適用して接続先に送信するメッセージを制御できるカスタム フィルタです。通常、重大度のみに基づいて接続先へのメッセージをフィルタリングしますが、イベント リストを使用して、イベント クラス、重大度、およびメッセージ識別子（ID）の組み合わせに基づいて送信されるメッセージを微調整できます。

カスタム イベント リストの作成は、2 段階のプロセスです。[イベント リスト（Event Lists）] タブでカスタム リストを作成し、イベント リストを使用して、[宛先のロギング（Logging Destinations）] タブで各種宛先のロギング フィルタを定義します。

ヒント　セキュリティ イベント（接続イベントや侵入イベントなど）に関する syslog メッセージを送信するようにデバイスを設定すると、ほとんどの FTD プラットフォーム設定がこれらのメッセージに適用されません。セキュリティ イベントの syslog メッセージに適用する FTD プラットフォームの設定 （1393 ページ）を参照してください。

ステップ 1　**[デバイス（Devices）] > [プラットフォーム設定（Platform Settings）]** を選択し、FTD ポリシーを作成または編集します。

ステップ 2　**[Syslog] > [イベント リスト（Events List）]** を選択します。

ステップ 3　イベント リストを設定します。

a) [追加（Add）] をクリックして新規リストを追加したり、既存のリストを編集したりします。

b) [名前（Name）] フィールドにイベント リストの名前を入力します。スペースは使用できません。

c) 重大度またはイベント クラスに基づいてメッセージを識別するには、[重大度/イベント クラス（Severity/Event Class）] タブを選択して、項目を追加または編集します。

使用可能なクラスの詳細については、syslog メッセージ クラス （1387 ページ） を参照してください。

レベルについては、重大度 （1386 ページ） を参照してください。

特定のイベント クラスは、トランスペアレント モードのデバイスには適用されません。そのようなオプションが設定された場合、オプションは無視され、展開されません。

d) メッセージ ID を指定してメッセージを識別するには、[メッセージ ID（Message ID）] タブを選択し、ID を追加または編集します。

ハイフンを使用して ID 範囲を入力できます（たとえば、100000-200000）。ID は 6 桁の数字です。最初の 3 桁が機能にどのようにマップされるかについては、syslog メッセージ クラス （1387 ページ） を参照してください。

特定のメッセージ番号については、『Cisco ASA Series Syslog Messages』を参照してください。

e) [OK] をクリックして、イベント リストを保存します。

ステップ 4 [ロギング接続先（Logging Destinations）] タブをクリックし、フィルタを使用する必要がある接続先を追加または編集します。

ロギング接続先の有効化 （1395 ページ）を参照してください。

ステップ 5 **[Save（保存）]** をクリックします。

これで、[Deploy] をクリックして割り当てられているデバイスにポリシーを展開できます。変更はポリシーを導入するまで有効になりません。

syslog メッセージの生成レートの制限

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin Access Admin Network Admin

syslog メッセージの生成レートは、重大度レベルまたはメッセージ ID によって制限できます。ロギング レベルごと、および Syslog メッセージ ID ごとに個別の制限を指定できます。設定が競合する場合は、Syslog メッセージ ID の制限が優先されます。

ヒント セキュリティ イベント（接続イベントや侵入イベントなど）に関する syslog メッセージを送信するようにデバイスを設定すると、ほとんどの FTD プラットフォーム設定がこれらのメッセージに適用されません。セキュリティ イベントの syslog メッセージに適用する FTD プラットフォームの設定 （1393 ページ）を参照してください。

ステップ 1 **[デバイス（Devices）]** > **[プラットフォーム設定（Platform Settings）]** を選択し、FTD ポリシーを作成または編集します。

ステップ 2 **[Syslog]** > **[レート制限（Rate Limit）]** を選択します。

ステップ 3 重大度レベルによりメッセージの生成を制限するには、[ログ レベル（Logging Level）] タブで [追加（Add）] をクリックして、次のオプションを設定します。

- ログ レベル（Logging Level）：レートを制限する重大度レベル。レベルについては、重大度 （1386 ページ） を参照してください。

- メッセージ数（Number of messages）：指定した時間内に許容される指定したタイプのメッセージの最大数。
- 間隔（Interval）：レート制限カウンタがリセットされるまでの秒数。

ステップ 4 [OK] をクリックします。

ステップ 5 syslog のメッセージ ID によりメッセージの生成を制限するには、[Syslog レベル（Syslog Level）] タブで [追加（Add）] をクリックし、次のオプションを設定します。

- [Syslog ID]：レートを制限する syslog のメッセージ ID。特定のメッセージ番号については、『Cisco ASA Series Syslog Messages』を参照してください。
- メッセージ数（Number of messages）：指定した時間内に許容される指定したタイプのメッセージの最大数。
- 間隔（Interval）：レート制限カウンタがリセットされるまでの秒数。

ステップ 6 [OK] をクリックします。

ステップ 7 **[Save（保存）]** をクリックします。

これで、[Deploy] をクリックして割り当てられているデバイスにポリシーを展開できます。変更はポリシーを導入するまで有効になりません。

Syslog 設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin Access Admin Network Admin

一般的な Syslog 設定を設定して、Syslog サーバに送信される Syslog メッセージに含めるファシリティ コードの設定、各メッセージにタイムスタンプが含まれるかどうかの指定、メッセージに含めるデバイス ID の指定、メッセージの重大度レベルの表示と変更、および特定のメッセージの生成のディセーブル化を行うことができます。

セキュリティ イベント（接続イベントや侵入イベントなど）に関する syslog メッセージを送信するようにデバイスを設定すると、このページの一部の設定がこれらのメッセージに適用されません。セキュリティ イベントの syslog メッセージに適用する FTD プラットフォームの設定 （1393 ページ）を参照してください。

ステップ 1 **[デバイス（Devices）] > [プラットフォーム設定（Platform Settings）]** を選択し、FTD ポリシーを作成または編集します。

ステップ 2 [Syslog] > [Syslog 設定（Syslog Settings）] を選択します。 >

ステップ 3 ファイル メッセージのベースとして使用する Syslog サーバのシステム ログ機能を、[ファシリティ（Facility）] ドロップダウン リストから選択します。

デフォルトは LOCAL4(20) です。これは UNIX システムで最も可能性の高いコードです。ただし、ネットワーク デバイス間では使用可能なファシリティが共用されているため、システム ログではこの値を変更しなければならない場合があります。

通常、ファシリティの値はセキュリティ イベントとは関係ありません。ファシリティの値をメッセージに含める必要がある場合は、セキュリティ イベントの syslog メッセージのファシリティ（2904 ページ）を参照してください。

ステップ 4 [タイムスタンプを各 Syslog メッセージで有効にする（Enable timestamp on each syslog message）] チェックボックスをオンにして、メッセージ生成日時を Syslog メッセージに含めます。

ステップ 5 syslog メッセージの [タイムスタンプの形式（Timestamp Format）] を選択します。

- [レガシー（Legacy）]（MMM dd yyyy HH:mm:ss）形式は、syslog メッセージのデフォルト形式です。

  このタイムスタンプ形式を選択すると、メッセージには常に UTC であるタイム ゾーンが表示されません。

- [RFC 5424]（yyyy-MM-ddTHH:mm:ssZ）は RFC 5425 形式で指定されている ISO 8601 タイムスタンプ形式を使用します。

  RFC 5424 形式を選択すると、「Z」が各スタンプの末尾に追加され、タイムスタンプが UTC タイム ゾーンを使用していることを示します。

ステップ 6 デバイス識別子を Syslog メッセージに追加する場合は（これはメッセージの先頭に配置されます）、[Syslog デバイス ID を有効にする（Enable Syslog Device ID）] チェックボックスをオンにし、ID のタイプを選択します。

- [インターフェイス（Interface）]：アプライアンスがメッセージの送信に使用するインターフェイスに関係なく、選択されたインターフェイスの IP アドレスを使用します。インターフェイスを識別するセキュリティ ゾーンを選択します。ゾーンは、単一のインターフェイスにマッピングされる必要があります。
- [ユーザー定義 ID（User Defined ID）]：選択したテキスト文字列を使用します（最大 16 文字）。
- [ホスト名（Host Name）]：デバイスのホスト名を使用します。

ステップ 7 [Syslog Message] テーブルを使用して、特定の Syslog メッセージのデフォルト設定を変更します。デフォルト設定を変更する場合にだけ、このテーブルでルールを設定する必要があります。メッセージに割り当てられている重大度を変更したり、メッセージの生成を無効にしたりできます。

デフォルトでは、NetFlow が有効になり、エントリはテーブルに表示されます。

a) NetFlow が原因で冗長している Syslog メッセージを抑制にするには、[ネットフロー同等 Syslog（Netflow Equivalent Syslogs）] を選択します。

   これにより、メッセージが抑止されたメッセージとしてテーブルに追加されます。

   （注） これらの同等の Syslog メッセージがすでにテーブルにある場合、既存のルールは上書きされません。

b) ルールを追加するには、[追加（Add）] ボタンをクリックします。

c) 設定変更するメッセージ番号を [Syslog ID] ドロップダウンリストから選択し、新しい重大度を [ロギング レベル（Logging Level）] ドロップダウンリストから選択するか、または [抑制（Suppressed）] を選

択してメッセージの生成を無効にします。通常は、重大度レベルの変更やメッセージのディセーブル化は行いませんが、必要に応じて両方のフィールドを変更できます。

d) [OK] をクリックしてテーブルにルールを追加します。

ステップ 8 **[Save（保存）]** をクリックします。

これで、[Deploy] をクリックして割り当てられているデバイスにポリシーを展開できます。変更はポリシーを導入するまで有効になりません。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

関連トピック

セキュリティ イベントの syslog メッセージに適用する FTD プラットフォームの設定 （1393 ページ）

Syslog サーバの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin Access Admin Network Admin

システムから生成されたメッセージを処理するように syslog サーバを設定するには、次の手順を実行します。

（バージョン 6.3 以降を実行しているデバイスの場合）この syslog サーバが接続イベントや侵入イベントなどのセキュリティ イベントを受信する場合は、セキュリティ イベントの syslog メッセージに適用する FTD プラットフォームの設定 （1393 ページ）も参照してください。

始める前に

- ロギングのガイドライン （1391 ページ）で要件を参照してください。
- デバイスからネットワーク上の syslog コレクタに到達できることを確認します。

ステップ 1 **[デバイス（Devices）] > [プラットフォーム設定（Platform Settings）]** を選択し、FTD ポリシーを作成または編集します。

ステップ 2 [Syslog] > [Syslog サーバ（Syslog Server）] > を選択します。

ステップ 3 [TCP syslog サーバのダウン時ユーザ トラフィックの通過を許可（Allow user traffic to pass when TCP syslog server is down）] チェックボックスをオンにして、TCP プロトコルを使用する Syslog サーバがダウンしている場合にトラフィックを許可するようにします。

ステップ 4 [メッセージ キュー サイズ（メッセージ）（Message queue size (messages)）] フィールドに、Syslog サーバが取り込み中の場合に、Syslog メッセージをセキュリティ アプライアンスに保存するキューのサイズを入力します。最小件数は 1 件です。デフォルトは 512 です。無制限の数のメッセージをキューに入れる場合は、0 を指定します（使用可能なブロック メモリによって制限されます）。

ステップ 5 [追加（Add）] をクリックして、新しい Syslog サーバを追加します。

a) [IP アドレス（IP Address）] ドロップダウン リストで、Syslog サーバの IP アドレスを含むネットワーク ホスト オブジェクトを選択します。

b) プロトコル（TCP または UDP）を選択し、Firepower Threat Defense デバイスと Syslog サーバの間の通信のポート番号を入力します。

UDP は高速で、TCP よりもデバイス上のリソースが減少します。

UDP のデフォルト ポートは 514、TCP のデフォルト ポートは 1470 です。有効な非デフォルトのポート値は、どちらのプロトコルでも 1025 ～ 65535 です。

c) [Cisco EMBLEM 形式でのログ メッセージ（UDP のみ）（Log messages in Cisco EMBLEM format (UDP only)）] チェックボックスをオンにして、Cisco の EMBLEM 形式でメッセージをログに記録するかどうかを指定します（プロトコルとして UDP が選択されている場合に限る）。

d) [セキュア Syslog を有効にする（Enable Secure Syslog）] チェックボックスをオンにして、デバイスとサーバの間の接続を TCP の SSL/TLS を使用して暗号化します。

（注） このオプションを使用するには、TCP をプロトコルとして選択する必要があります。また、[デバイス（Devices）] > [証明書（Certificates）] ページで、Syslog サーバとの通信に必要な証明書をアップロードする必要があります。 > 最後に、Firepower Threat Defense デバイスから syslog サーバに証明書をアップロードして、セキュアな関係を完成させ、トラフィックの復号化を許可します。デバイス管理インターフェイスでは、[セキュア Syslog を有効にする（Enable Secure Syslog）] オプションはサポートされていません。

e) Syslog サーバと通信するための [デバイス管理インターフェイス（Device Management Interface）] または [セキュリティ ゾーンまたは名前付きインターフェイス（Security Zones or Named Interfaces）] を選択します。

- [デバイス管理インターフェイス（Device Management Interface）]：このオプションは、バージョン 6.3 以降の Firepower Threat Defense デバイスにのみ適用されます。

  （注） [デバイス管理インターフェイス（Device Management Interface）] オプションでは、[セキュア Syslog を有効にする（Enable Secure Syslog）] オプションをサポートされていません。

- [セキュリティ ゾーンまたは名前付きインターフェイス（Security Zones or Named Interfaces）]：[使用可能ゾーン（Available Zones）] のリストからインターフェイスを選択して、[追加（Add）] をクリックします。また、診断インターフェイスにこの名前（まだ設定されていない場合）と IP アドレスを設定する必要があります（[デバイス管理（Device Management）] ページでデバイス設定を編集し、[インターフェイス（Interfaces）] タブを選択します）。管理/診断インターフェイスの詳細については、診断インターフェイス （786 ページ） を参照してください。

（注） Syslog サーバが物理管理インターフェイスに接続されたネットワーク上にある場合は、そのインターフェイスの名前を [選択したセキュリティ ゾーン（Selected Security Zones）] リストの下の [インターフェイス名（Interface Name）] フィールドに入力し、[追加（Add）] をクリックします。また、診断インターフェイスにこの名前（まだ設定されていない場合）と IP アドレスを設定する必要があります（[デバイス管理（Device Management）] ページでデバイス設定を編集し、[インターフェイス（Interfaces）] タブを選択します）。管理/診断インターフェイスの詳細については、診断インターフェイス （786 ページ） を参照してください。

f) [OK] をクリックします。

ステップ 6 **[Save（保存）]** をクリックします。

これで、[Deploy] をクリックして割り当てられているデバイスにポリシーを展開できます。変更はポリシーを導入するまで有効になりません。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ） を参照してください。

グローバル タイムアウトの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin Access Admin Network Admin

さまざまなプロトコルの接続スロットと変換スロットのグローバル アイドル タイムアウト期間を設定できます。指定したアイドル時間の間スロットが使用されなかった場合、リソースは空いているプールに戻されます。

また、デバイスのコンソール セッションでタイムアウトを設定できます。

ステップ 1 **[デバイス（Devices）] > [プラットフォーム設定（Platform Settings）]** を選択し、FTD ポリシーを作成または編集します。

ステップ 2 [タイムアウト（Timeouts）] を選択します。

ステップ 3 変更するタイムアウトを設定します。

任意の設定で、[カスタム（Custom）] を選択して自分の値を定義し、[デフォルト（Default）] を選択してシステムのデフォルト値に戻します。ほとんどの場合、最大タイムアウトは 1193 時間です。

[無効（Disable）] を選択して、タイムアウトを無効にできます。

- [コンソール タイムアウト（Console Timeout）]：コンソールへの接続が閉じられるまでのアイドル時間。範囲は 、5 ～ 1440 分です。デフォルトは 0 で、セッションがタイムアウトしないことを示します。値を変更すると、既存のコンソール セッションで古いタイムアウト値が使用されます。新しい値は新しい接続にのみ適用されます。
- [変換スロット（Translation Slot (xlate)）]：NAT 変換スロットが解放されるまでのアイドル時間。この期間は 1 分以上にする必要があります。デフォルトは 3 時間です。
- [接続（Connection (Conn)）]：接続スロットが解放されるまでのアイドル時間。この期間は 5 分以上にする必要があります。デフォルトは 1 時間です。
- [ハーフクローズ（Half-Closed）]：TCP ハーフクローズ接続を閉じるまでのアイドル時間。最小は 30 秒です。デフォルトは 10 分です。
- [UDP]：UDP 接続を閉じるまでのアイドル時間。この期間は 1 分以上にする必要があります。デフォルトは 2 分です。
- [ICMP]：全般的な ICMP 状態が終了するまでのアイドル時間。デフォルト（および最小）は 2 秒です。
- [RPC/Sun RPC]：SunRPC スロットが解放されるまでのアイドル時間。この期間は 1 分以上にする必要があります。デフォルトは 10 分です。
- [H.225]：H.225 シグナリング接続を閉じるまでのアイドル時間。デフォルトは 1 時間です。すべての呼び出しがクリアされた後に接続をすぐにクローズするには、タイムアウト値を 1 秒（0:0:1）にすることを推奨します。
- [H.323]：H.245（TCP）および H.323（UDP）メディア接続が終了するまでのアイドル時間。デフォルト（および最小）は 5 分です。H.245 と H.323 のいずれのメディア接続にも同じ接続フラグが設定されているため、H.245（TCP）接続は H.323（RTP および RTCP）メディア接続とアイドル タイムアウトを共有します。
- [SIP]：SIP シグナリング ポート接続を閉じるまでのアイドル時間。この期間は 5 分以上にする必要があります。デフォルトは 30 分です。
- [SIP メディア（SIP Media）]：SIP メディア ポート接続を閉じるまでのアイドル時間。この期間は 1 分以上にする必要があります。デフォルトは 2 分です。SIP メディア タイマーは、SIP UDP メディア パケットを使用する SIP RTP/RTCP で、UDP 非アクティブ タイムアウトの代わりに使用されます。
- [SIP 接続解除（SIP Disconnect）]：CANCEL メッセージまたは BYE メッセージで 200 OK を受信しなかった場合に、SIP セッションを削除するまでのアイドル時間（0:0:1 ～ 00:10:0）。デフォルトは 2 分（0:2:0）です。
- [SIP インバイト（SIP Invite）]：暫定応答のピンホールとメディア xlate を閉じるまでのアイドル時間（0:1:0 ～ 00:30:0）。デフォルトは、3 分（0:3:0）です。
- [SIP 暫定メディア（SIP Provisional Media）]：SIP 暫定メディア接続のタイムアウト値（1 ～ 30 分）。デフォルトは 2 分です。
- [フローティング接続（Floating Connection）]：1 つのネットワークに複数のルートが存在しており、それぞれメトリックが異なる場合、ASA は接続確立時点でメトリックが最良のルートを使用します。より適切なルートが使用可能になった場合は、このタイムアウトによって接続が閉じられるので、その

適切なルートを使用して接続を再確立できます。デフォルトは 0 です（接続はタイムアウトしません）。より良いルートを使用できるようにするには、タイムアウト値を 0:0:30 ～ 1193:0:0 の間で設定します。

- [Xlate PAT]：PAT 変換スロットが解放されるまでのアイドル時間（0:0:30～ 0:5:0）。デフォルトは 30 秒です。前の接続がアップストリーム デバイスで引き続き開いている可能性があるため、開放された PAT ポートを使用する新しい接続をアップストリーム ルータが拒否する場合、このタイムアウトを増やすことができます。
- [TCP Proxy Reassembly]：再構築のためバッファ内で待機しているパケットをドロップするまでのアイドル タイムアウト（0:0:10 ～ 1193:0:0）。デフォルトは、1 分（0:1:0）です。
- [ARP タイムアウト（ARP Timeout）]：（トランスペアレント モードのみ）。ARP テーブルを再構築する間隔の秒数（60 ～ 4294967）。デフォルトは 14,400 秒（4 時間）です。

ステップ 4 **[Save（保存）]** をクリックします。

これで、[Deploy] をクリックして割り当てられているデバイスにポリシーを展開できます。変更はポリシーを導入するまで有効になりません。

脅威に対する防御のための NTP 時刻同期の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin Access Admin Network Admin

Network Time Protocol（NTP）サーバを使用して、デバイスのクロック設定を同期します。デフォルトでは、デバイスは Firepower Management Center サーバを NTP サーバとして使用しますが、可能な場合は別の NTP サーバを設定する必要があります。

（注） Firepower 4100/9300 シャーシに FTD を導入する場合は、スマート ライセンスが正しく機能し、デバイス登録に適切なタイムスタンプを確保するように、Firepower 4100/9300 シャーシで NTP を設定する必要があります。Firepower 4100/9300 シャーシと Firepower Management Center には、同じ NTP サーバを使用する必要があります。

始める前に

- 組織に FTD からアクセスできる 1 台以上の NTP サーバがある場合は、FMC の [System] > [Configuration] ページで、時刻の同期用に設定したデバイスと同じ NTP サーバを使用します。指定した値をコピーします。

- デバイスが NTP サーバにアクセスできない場合、または組織に NTP サーバがない場合は、Firepower Management Center を NTP サーバとして使用するように設定する必要があります。ネットワーク NTP サーバにアクセスせずに時刻を同期 （1309 ページ）を参照してください。

ステップ 1 **[デバイス（Devices）] > [プラットフォーム設定（Platform Settings）]** を選択し、FTD ポリシーを作成または編集します。

ステップ 2 [Time Synchronization] を選択します。

ステップ 3 次のいずれかのクロック オプションを設定します。

- [Defense CenterのNTPを使用（Via NTP from Defense Center）]：Firepower Management Center サーバを NTP サーバとして使用します（この機能を提供するように設定している場合）。これはデフォルトです。
- [Via NTP from]：Firepower Management Center がネットワーク上の NTP サーバを使用している場合は、このオプションを選択し、FMC の [System] > [Configuration] > [Time Synchronization] で指定した NTP サーバと同じ完全修飾 DNS 名（ntp.example.com など）または IP アドレスを入力します。

ステップ 4 **[Save（保存）]** をクリックします。

次のタスク

- ポリシーがデバイスに割り当てられていることを確認します。プラットフォーム設定ポリシーのターゲット デバイスの設定 （1334 ページ）を参照してください。
- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。
- Firepower システムに従来型デバイスが含まれている場合は、そのデバイスの時刻の同期を設定します。従来型デバイスの時刻を NTP サーバに同期 （1344 ページ）を参照してください。

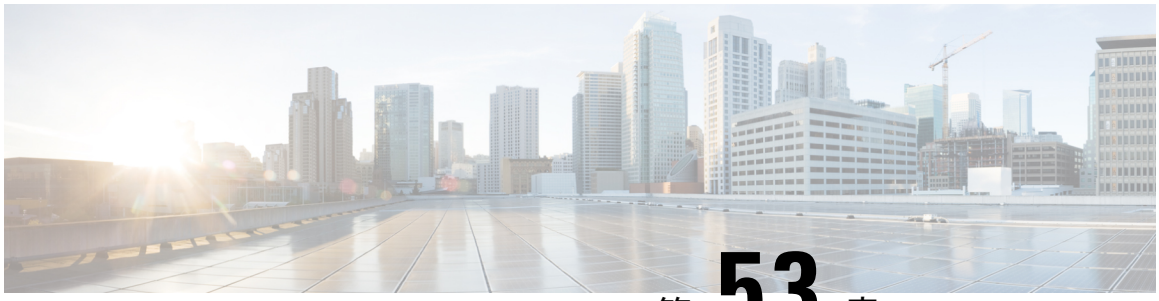
Firepower Threat Defense プラットフォーム設定の履歴

機能	バージョン	詳細
SSH ログイン失敗の制限数	6.3	ユーザが SSH 経由でデバイスにアクセスし、ログイン試行を 3 回続けて失敗すると、デバイスは SSH セッションを終了します。

機能	バージョン	詳細
SSH 用に追加された外部認証	6.2.3	LDAP または RADIUS を使用して、Firepower Threat Defense への SSH アクセス用に外部認証を設定できるようになりました。 新しい/変更された画面： **[デバイス（Devices）] > [プラットフォームの設定（Platform Settings）] > [外部認証（External Authentication）]** サポートされているプラットフォーム：Firepower Threat Defense
UC/APPL 準拠モードのサポート	6.2.1	セキュリティ認定コンプライアンスは、CC モードまたは UCAPL モードで有効にすることができます。セキュリティ認定コンプライアンスを有効にしても、選択したセキュリティモードのすべての要件との厳密なコンプライアンスが保証されるわけではありません。強化手順についての詳細は、認定機関から提供されている本製品に関するガイドラインを参照してください。 新しい/変更された画面： **[デバイス（Devices）] > [プラットフォーム設定（Platform Settings）] > [UC/APPL準拠（UC/APPL Compliance）]** サポートされているプラットフォーム：すべてのデバイス

機能	バージョン	詳細
リモート アクセス VPN の SSL 設定	6.2.1	Firepower Threat Defense デバイスでは、セキュア ソケット レイヤ（SSL）プロトコルと Transport Layer Security（TLS）を使用して、リモート クライアントからのリモート アクセス VPN 接続のセキュア メッセージ伝送をサポートします。SSL でのリモート VPN アクセス中に、ネゴシエートとメッセージ伝送に使用される SSL バージョンと暗号化アルゴリズムを設定できます。 新しい/変更された画面： **[デバイス（Devices）] > [プラットフォーム設定（Platform）] > [SSL]** サポートされているプラットフォーム：Firepower Threat Defense
SSH および HTML 用の外部認証が削除	6.1.0	統合管理アクセスをサポートするための変更により、データ インターフェイスに対する SSH および HTML ではローカル ユーザのみがサポートされます。また、論理診断インターフェイスに対する SSH は使用できなくなりました。代わりに、（同じ物理ポートを共有する）論理管理インターフェイスに対する SSH を使用できます。以前は、診断およびデータ インターフェイスに対する SSH および HTML アクセスでは外部認証のみがサポートされていましたが、管理インターフェイスに対してはローカル ユーザのみがサポートされていました。 新しい/変更された画面： **[デバイス（Devices）] > [プラットフォームの設定（Platform Settings）] > [外部認証（External Authentication）]** サポートされているプラットフォーム：Firepower Threat Defense

機能	バージョン	詳細
Firepower Threat Defense のサポート	6.0.1	この機能が導入されました。 新しい/変更された画面： **[Devices] > [Platform Settings]** サポートされているプラットフォーム：Firepower Threat Defense



第 53 章

セキュリティ認定準拠

次のトピックでは、セキュリティ認定規格に準拠するようにシステムを設定する方法について説明します。

セキュリティ認定準拠のモード

お客様の組織が、米国防総省およびグローバル認定組織によって確立されたセキュリティ基準に従う機器とソフトウェアだけを使用することを求められる場合があります。Firepower では、以下のセキュリティ認定標準規格へのコンプライアンスをサポートします。

- コモン クライテリア（CC）：国際コモン クライテリア承認アレンジメントによって確立された、セキュリティ製品のプロパティを定義するグローバル標準規格
- Unified Capabilities Approved Products List（UCAPL）：米国国防情報システム局（DISA）によって確立された、セキュリティ要件を満たす製品のリスト

（注） 米国政府は、Unified Capabilities Approved Products List（UCAPL）の名称を Defense Information Network Approved Products List（DODIN APL）に変更しました。このドキュメントおよび Firepower Management Center Web インターフェイスでの UCAPL の参照は、DODIN APL への参照として解釈できます。

- 連邦情報処理標準（FIPS）140：暗号化モジュールの要件に関する規定

セキュリティ認定コンプライアンスは、CC モードまたは UCAPL モードで有効にすることができます。セキュリティ認定コンプライアンスを有効にしても、選択したセキュリティ モードのすべての要件との厳密なコンプライアンスが保証されるわけではありません。強化手順につ

いての詳細は、認定機関から提供されている本製品に関するガイドラインを参照してください。

⚠

注意 この設定を有効にした後は、無効にすることはできません。アプライアンスを CC モードまたは UCAPL モードから解除する必要がある場合は、再イメージ化する必要があります。

セキュリティ認定準拠特性

次の表は、CC または UCAPL モードを有効にしたときの動作の変更を示しています。ログインアカウントの制約は、Webインターフェイスアクセスではなく、コマンドラインまたはシェル アクセスを指します。）

システムの変更	Firepower Management Center		従来型管理対象デバイス		Firepower Threat Defense	
	CC モード	UCAPL モード	CC モード	UCAPL モード	CC モード	UCAPL モード
FIPS コンプライアンスは有効です。	あり	あり	あり	あり	あり	あり
バックアップまたはレポートについては、リモート ストレージは利用できません。	あり	あり	—	—	—	—
追加のシステム監査デーモンが開始されます。	なし	あり	なし	あり	なし	なし
システム ブートローダは固定されています。	なし	あり	なし	あり	なし	なし
追加のセキュリティがログイン アカウントに適用されます。	なし	あり	なし	あり	なし	なし
再起動のキー シーケンス Ctrl+Alt+Del を無効にします。	なし	あり	なし	あり	なし	なし
最大 10 の同時ログインセッションを実行します。	なし	あり	なし	あり	なし	なし
パスワード長は少なくとも 15 文字で、大文字/小文字の英数字を組み合わせて 1 つ以上の数字を含む必要があります。	なし	あり	なし	あり	なし	なし
ローカル `admin` ユーザに必要な最小パスワード長を設定するには、ローカル デバイス CLI を使用できます。	—	—	なし	なし	あり	あり

システムの変更	Firepower Management Center		従来型管理対象デバイス		Firepower Threat Defense	
	CC モード	UCAPL モード	CC モード	UCAPL モード	CC モード	UCAPL モード
パスワードは、辞書に出現する単語であったり、連続する繰り返し文字を含んでいたりすることができません。	なし	あり	なし	あり	なし	なし
3 回連続してログインに失敗した場合、admin 以外のユーザはロックアウトされます。この場合は、管理者がパスワードをリセットする必要があります。	なし	あり	なし	あり	なし	なし
デフォルトでは、システムはパスワード履歴を保存します。	なし	あり	なし	あり	なし	なし
admin ユーザは、Web インターフェイスで設定可能な最大許容回数を超えてログイン試行に失敗した後、ロックアウトされます。	あり	あり	あり	あり	—	—
admin ユーザは、ローカル アプライアンス CLI で設定可能な最大許容回数を超えてログイン試行に失敗した後、ロックアウトされます。	—	—	はい（セキュリティ認定準拠の有効/無効にかかわらず）。	はい（セキュリティ認定準拠の有効/無効にかかわらず）。	あり	あり
次の場合、システムは、アプライアンスとの SSH セッションで自動的にキーを再生成します： • セッション アクティビティでキーが 1 時間使用された後 • キーを使用して接続で 1 GB のデータが伝送された後	あり	あり	あり	あり	あり	あり
システムは、ブート時にファイル システム整合性チェック（FSIC）を実行します。FSIC が失敗した場合、Firepower ソフトウェアは起動せず、リモート SSH アクセスが無効になり、ローカル コンソールを介してのみアプライアンスにアクセスできます。これが発生した場合は Cisco TAC に連絡してください。	あり	あり	あり	あり	あり	あり

セキュリティ認定準拠の推奨事項

セキュリティ認定コンプライアンスの使用が有効のときに、次のベストプラクティスを確認することをお勧めします。

- 展開時にセキュリティ認定準拠を有効にするには、最初に Firepower Management Center で有効にし、次に、管理対象のすべてのデバイスの同じモードで有効にします。

  ⚠

  注意 両方が同じセキュリティ認定準拠モードで動作していない限り、Firepower Management Center は管理対象デバイスからイベントデータを受信しません。

- 高可用性設定で Firepower Management Center を使用すると、双方の設定を行い、同じセキュリティ認定準拠モードを使用します。
- Firepower 4100/9300 シャーシで、CC または UCAPL モードで動作するように Firepower Threat Defense を設定した場合は、Firepower 4100/9300 シャーシも CC モードで動作するように設定する必要があります。詳細については、『*Cisco FXOS Firepower Chassis Manager Configuration Guide*』を参照してください。
- 次の機能を使用するようにシステムを設定できません。
  - 電子メールレポート、アラート、データのプルーニング通知。
  - Nmap Scan、Cisco IOS Null Route、Set Attribute Value、ISE EPS の修復。
  - バックアップまたはレポート用のリモート ストレージ。
  - サードパーティ クライアントのシステム データベースへのアクセス。
  - 電子メール（SMTP）、SNMP トラップ、syslog から送信される外部通知、アラート。
  - アプライアンスとサーバの間のチャネルを保護するために、SSL 証明書を使用せずに、HTTP サーバまたは syslog サーバに送信された監査ログ メッセージ。
- CC モードを使用して展開する場合は、LDAP または RADIUS を使用して外部認証を有効にしないでください。
- CC モードを使用して展開中に CAC を有効にできません。
- CC または UCAPL モードを使用した展開では、Firepower REST API 経由で Firepower Management Center および管理対象デバイスへのアクセスを無効にします。
- UCAPL モードを使用して展開中に CAC を有効にします。
- Firepower Threat Defense デバイスが両方とも同じセキュリティ認定準拠モードを使用していない限り、ハイ アベイラビリティ ペアに構成しないでください。

（注） FirePOWER システムは、次の CC または UCAPL モードをサポートしていません：

- スタックまたはハイ アベイラビリティ ペアの従来型デバイス
- クラスタ内の Firepower Threat Defense デバイス
- Firepower Threat Defense のコンテナ インスタンス Firepower 4100/9300

アプライアンスの強化

Firepower システムの強化に使用可能な機能の詳細については、最新バージョンの『*Cisco Firepower Management Center Hardening Guide*』と『*Cisco Firepower Threat Defense Hardening Guide*』、および本書の以降のトピックを参照してください。

- Firepower システムのライセンス （93 ページ）
- ユーザ アカウントについて （51 ページ）
- Firepower システムへのログイン （25 ページ）
- 監査ログ （1292 ページ）
- 監査ログ証明書 （1295 ページ）
- 時刻および時刻同期 （1307 ページ）
- 脅威に対する防御のための NTP 時刻同期の設定 （1406 ページ）
- 電子メール アラート応答の作成 （2813 ページ）
- 侵入イベントに対する電子メール アラートの設定 （2822 ページ）
- SMTP の設定 （1377 ページ）
- Firepower 1000/2100 シリーズの SNMP の設定 （313 ページ）
- SNMP の脅威に対する防御の設定 （1378 ページ）
- SNMP アラート応答の作成 （2809 ページ）
- DDNS の設定 （861 ページ）
- DNS キャッシュ （1302 ページ）
- システムの監査 （397 ページ）
- アクセス リスト （1291 ページ）
- セキュリティ認定準拠 （1411 ページ）
- リモート ストレージの SSH の設定 （1286 ページ）

- 監査ログ証明書 （1295 ページ）
- HTTPS 証明書 （1254 ページ）
- Web インターフェイス用のユーザ ロールのカスタマイズ （81 ページ）
- 社内ユーザ アカウントの追加 （57 ページ）
- セッション タイムアウト （1315 ページ）
- Syslog の設定概要 （1385 ページ）
- スケジュール バックアップ （239 ページ）
- のサイト間 VPN Firepower Threat Defense （1067 ページ）
- のリモート アクセス VPN Firepower Threat Defense （1085 ページ）
- Firepower Threat Defense の FlexConfig ポリシー （1201 ページ）

ネットワークの保護

ネットワークを保護するために構成できる Firepower システムの機能については、次のトピックを参照してください。

- アクセス コントロール ポリシーの開始 （1665 ページ）
- セキュリティ インテリジェンス ブラックリスト （1741 ページ）
- 侵入ポリシーの使用を開始するには （2063 ページ）
- ルールを使用した侵入ポリシーの調整 （2073 ページ）
- 侵入ルール エディタ （2137 ページ）
- 侵入ルールの更新 （185 ページ）
- 侵入イベント ロギングのグローバル制限 （2129 ページ）
- トランスポート層およびネットワーク層プリプロセッサ （2397 ページ）
- 特定の脅威の検出 （2439 ページ）
- アプリケーション層プリプロセッサ （2305 ページ）
- IPS デバイスの展開と設定 （663 ページ）
- システムの監査 （397 ページ）
- 侵入イベントの操作 （3057 ページ）
- イベントの検索 （2967 ページ）
- ワークフロー （2917 ページ）
- デバイス管理の基本 （287 ページ）

• ログイン バナー （1305 ページ）
• システム ソフトウェアの更新 （179 ページ）

セキュリティ認定コンプライアンスの有効化

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	任意（Any）	いずれか（Any）	Admin

この設定は、Firepower Management Center または管理対象デバイスに適用されます。

- Firepower Management Center では、この設定はシステム設定の一部になります。
- 管理対象デバイスでは、この設定をプラットフォーム設定ポリシーの一部として FMC から適用します。

いずれの場合も、システム設定変更を保存するか、共有プラットフォーム設定ポリシーを展開するまで、設定は有効にはなりません。

注意 この設定を有効にした後に無効にすることはできません。アプライアンスを CC モードまたは UCAPL モードから解除する必要がある場合は、再イメージ化する必要があります。

始める前に

- アプライアンスでセキュリティ認定コンプライアンスを有効にする前に、展開に組み込む予定のあるすべてのデバイスを FMC に登録することをお勧めします。
- Firepower Threat Defense デバイスは評価ライセンスを使用できません。輸出管理機能を有効にするには、Cisco Smart Software Manager アカウントを有効にする必要があります。
- Firepower Threat Defense デバイスはルーテッド モードで展開する必要があります。

ステップ 1 FMC を設定するか管理対象デバイスを設定するかに応じて、次の操作を実行します。

- FMC：**[System]** > **[Configuration]** を選択します。
- 従来型デバイス：**[デバイス（Devices）]** > **[プラットフォーム設定（Platform Settings）]** を選択し、Firepower ポリシーを作成または編集します。
- FTD デバイス：**[デバイス（Devices）]** > **[プラットフォーム設定（Platform Settings）]** を選択し、Firepower Threat Defense ポリシーを作成または編集します。

ステップ 2 [UCAPL/CC コンプライアンス（UCAPL/CC Compliance）] をクリックします。

（注） UCAPL または CC コンプライアンスを有効にすると、アプライアンスがリブートします。FMC は、システム設定を保存するとリブートし、管理対象デバイスは、設定の変更を展開するとリブートします。

ステップ 3 アプライアンスのセキュリティ認定コンプライアンスを永続的に有効にするには、2 つの選択肢があります。

- [コモン クライテリア（Common Criteria）] モードでセキュリティ認定コンプライアンスを有効にするには、ドロップダウン リストから [CC] を選択します。
- [Unified 機能承認製品リスト（Unified Capabilities Approved Products List）] モードでセキュリティ認定コンプライアンスを有効にするには、ドロップダウン リストから [UCAPL] を選択します。

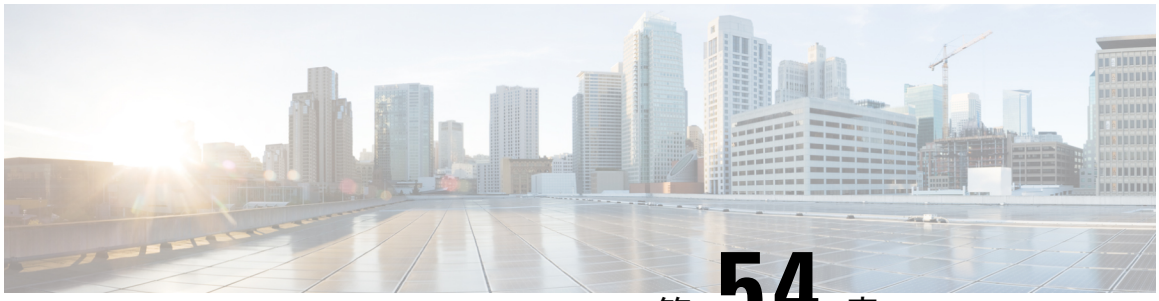
ステップ 4 [保存（Save）] をクリックします。

次のタスク

- まだ適用していない場合は、制御と防御のライセンスを、展開内のすべての従来型デバイスに適用します。
- 認証エンティティによって提供されるこの製品のガイドラインの説明に従い、追加の設定変更を行います。
- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

第 XIV 部

Network Address Translation（NAT）



第 54 章

NAT ポリシー管理

以下のトピックでは、Firepower システム用の NAT ポリシーを管理する方法について説明します。

NAT ポリシーの管理

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	Control	7000 & 8000 シリーズ FTD	任意（Any）	Access Admin Administrator Network Admin

マルチドメイン展開では、編集できる現在のドメインで作成されたポリシーが表示されます。また、編集できない先祖ドメインで作成されたポリシーも表示されます。下位のドメインで作成されたポリシーを表示および編集するには、そのドメインに切り替えます。

先祖ドメインの管理者は、NAT ポリシーの対象を子孫ドメインのデバイスにすることができます。子孫ドメインではこの NAT ポリシーを使用するか、カスタマイズされたローカル ポリシーに置き換えることができます。NAT ポリシーが異なる子孫ドメインのデバイスを対象とする場合、子孫ドメインの管理者は自分のドメインに属する対象デバイスに関する情報のみを表示できます。

ステップ 1 **[Devices]** > **[NAT]** を選択します。

ステップ 2 NAT ポリシーを管理します。

- コピー：コピーするポリシーの横にあるコピー アイコン（）をクリックします。NAT ポリシーのコピー （1426 ページ）を参照してください。
- 作成：[新規ポリシー（New Policy）] をクリックします。NAT ポリシーの作成 （1422 ページ）を参照してください。
- 削除：削除するポリシーの横にある削除アイコン（  ）をクリックして、[OK] をクリックします。続行するかどうかを尋ねるプロンプトで、ポリシー内に別のユーザの未保存の変更が存在するかどうかも通知されます。

  注意 管理対象デバイスに NAT ポリシーを展開した後は、デバイスからそのポリシーを削除できません。その代わりに、ルールを持たない NAT ポリシーを展開して、すでに管理対象デバイスに存在する NAT ルールを削除する必要があります。また、どのターゲット デバイスでも、最後に展開したポリシーは期限切れであっても削除できません。ポリシーを完全に削除する前に、それらのターゲットに異なるポリシーを展開する必要があります。

- 展開：[展開（Deploy）] をクリックします（設定変更の展開 （447 ページ） を参照）。
- 編集：編集アイコン（）をクリックします。NAT ポリシーの設定 （1423 ページ）を参照してください。
- [レポート（Report）]：レポート アイコン（  ）をクリックします（現在のポリシー レポートの生成 （459 ページ） を参照）。

NAT ポリシーの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	Control	7000 & 8000 シリーズ FTD	いずれか（Any）	Access Admin Administrator Network Admin

新しい NAT ポリシーを作成する場合、少なくとも一意の名前を付ける必要があります。ポリシーの作成時にポリシー ターゲットを特定する必要はありませんが、ポリシーを展開する前に、この手順を実行する必要があります。ルールを持たない NAT ポリシーをデバイスに適用すると、そのデバイスからすべての NAT ルールが削除されます。

マルチドメイン展開では、編集できる現在のドメインで作成されたポリシーが表示されます。また、編集できない先祖ドメインで作成されたポリシーも表示されます。下位のドメインで作成されたポリシーを表示および編集するには、そのドメインに切り替えます。

先祖ドメインの管理者は、NAT ポリシーの対象を子孫ドメインのデバイスにすることができます。子孫ドメインではこの NAT ポリシーを使用するか、カスタマイズされたローカル ポリ

シーに置き換えることができます。NAT ポリシーが異なる子孫ドメインのデバイスを対象とする場合、子孫ドメインの管理者は自分のドメインに属する対象デバイスに関する情報のみを表示できます。

ステップ 1 **[Devices]** > **[NAT]** を選択します。

ステップ 2 [新しいポリシー（New Policy）] ドロップダウン リストで、以下のいずれかを選択します。

- 7000 & 8000 シリーズ デバイスの場合は [Firepower NAT]。
- FTD デバイスの場合は [脅威に対する防御 NAT（Threat Defense NAT）]。

ステップ 3 [名前（Name）] に一意の名前を入力します。

マルチドメイン展開では、ポリシー名をドメイン階層内で一意にする必要があります。システムは、現在のドメインでは表示できないポリシーの名前との競合を特定することができます。

ステップ 4 必要に応じて、[説明（Description）] を入力します。

ステップ 5 ポリシーを展開するデバイスを選択します。

- [使用可能なデバイス（Available Devices）] リストでデバイスを選択し、[ポリシーに追加（Add to Policy）] をクリックします。
- [使用可能なデバイス（Available Devices）] リストから [選択されたデバイス（Selected Devices）] リストに、デバイスをクリックしてドラッグします。
- デバイスの横にある削除アイコン（）をクリックして、[選択されたデバイス（Selected Devices）] リストからデバイスを削除します。

ステップ 6 [保存（Save）] をクリックします。

次のタスク

設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

NAT ポリシーの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	Control	7000 & 8000 シリーズ FTD	いずれか（Any）	Access Admin Administrator Network Admin

マルチドメイン展開では、編集できる現在のドメインで作成されたポリシーが表示されます。また、編集できない先祖ドメインで作成されたポリシーも表示されます。下位のドメインで作成されたポリシーを表示および編集するには、そのドメインに切り替えます。

先祖ドメインの管理者は、NAT ポリシーの対象を子孫ドメインのデバイスにすることができます。子孫ドメインではこの NAT ポリシーを使用するか、カスタマイズされたローカル ポリシーに置き換えることができます。NAT ポリシーが異なる子孫ドメインのデバイスを対象とする場合、子孫ドメインの管理者は自分のドメインに属する対象デバイスに関する情報のみを表示できます。

インターフェイスのタイプを、そのインターフェイスがあるデバイスを対象とする NAT ポリシーでの使用が無効なタイプに変更した場合、ポリシーはそのインターフェイスに削除済みのラベルを付けます。NAT ポリシーの [保存（Save）] をクリックすると、インターフェイスはポリシーから自動的に削除されます。

（注） ルール属性は NAT ポリシー タイプによって異なります。ルールを追加または編集する場合、詳細については、ダイアログボックスで [?] をクリックするか、関連する章Firepower Threat Defense 用のネットワーク アドレス変換（NAT） （1449 ページ）または7000 および 8000 シリーズ デバイス用の NAT （1427 ページ）を参照してください。

ステップ 1 **[Devices]** > **[NAT]** を選択します。

ステップ 2 変更する NAT ポリシーの横にある編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 NAT ポリシーを設定します。

- ポリシー名や説明を変更するには、[名前（Name）] または [説明（Description）] フィールドをクリックし、必要に応じて文字を削除し、新しい名前または説明を入力します。 マルチドメイン展開では、ポリシー名をドメイン階層内で一意にする必要があります。システムは、現在のドメインでは表示できないポリシーの名前との競合を特定することができます。
- ポリシーの対象を管理するには、NAT ポリシーの対象の設定 （1425 ページ）を参照してください。
- ポリシーの変更を保存するには、[保存（Save）] をクリックします。
- ポリシーにルールを追加するには、[ルールの追加（Add Rule）] をクリックします。
- 既存のルールを編集するには、ルールの横にある編集アイコン（）をクリックします。
- ルールを削除するには、ルールの横にある削除アイコン（）をクリックし、[OK] をクリックします。
- 既存のルールを有効または無効にするには、ルールを右クリックして [状態（State）] を選択し、[無効化（Disable）] または [有効化（Enable）] を選択します。
- （Firepower NAT のみ）特定のルール属性の設定ページを表示するには、ルールの行にある条件の列で名前、値、またはアイコンをクリックします。たとえば、[Source Network] 列の名前または値をクリックすると、選択したルールの [Source Network] ページが表示されます。

次のタスク

設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

NAT ポリシーの対象の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	Control	7000 & 8000 シリーズ FTD	任意（Any）	Access Admin Administrator Network Admin

ポリシーを適用する管理対象デバイスは、ポリシーを作成または編集する際に特定できます。使用可能なデバイス、7000 または 8000 シリーズ スタック、およびハイ アベイラビリティ ペアのリストを検索して、選択したデバイスのリストに追加できます。

異なるバージョンの Firepower システムを実行中のスタック構成デバイスを対象にすることはできません（たとえば、デバイスのいずれかでアップグレードが失敗した場合）。

マルチドメイン展開では、編集できる現在のドメインで作成されたポリシーが表示されます。また、編集できない先祖ドメインで作成されたポリシーも表示されます。下位のドメインで作成されたポリシーを表示および編集するには、そのドメインに切り替えます。

先祖ドメインの管理者は、NAT ポリシーの対象を子孫ドメインのデバイスにすることができます。子孫ドメインではこの NAT ポリシーを使用するか、カスタマイズされたローカル ポリシーに置き換えることができます。NAT ポリシーが異なる子孫ドメインのデバイスを対象とする場合、子孫ドメインの管理者は自分のドメインに属する対象デバイスに関する情報のみを表示できます。

ステップ 1 **[Devices]** > **[NAT]** を選択します。

ステップ 2 変更する NAT ポリシーの横にある編集アイコン（  ）をクリックします。

代わりに表示アイコン（  ）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 [ポリシー割り当て（Policy Assignments）] をクリックします。

ステップ 4 次のいずれかを実行します。

- デバイス、スタック、ハイ アベイラビリティ ペア、またはデバイス グループをポリシーに割り当てるには、[使用可能なデバイス（Available Devices）] リストで選択し、[ポリシーに追加（Add to Policy）] をクリックします。ドラッグ アンド ドロップを使用することもできます。
- デバイスの割り当てを削除するには、[選択されたデバイス（Selected Device）] リストのデバイス、スタック、ハイ アベイラビリティ ペア、またはデバイス グループの横にある削除アイコン（  ）をクリックします。

ステップ 5 [OK] をクリックします。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

NAT ポリシーのコピー

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	Control	7000 & 8000 シリーズ FTD	任意（Any）	Access Admin Administrator Network Admin

NAT ポリシーのコピーを作成できます。コピーには、ポリシーのすべてのルールと設定が含まれます。

マルチドメイン導入では、現在のドメインおよび先祖ドメインからポリシーをコピーできます。

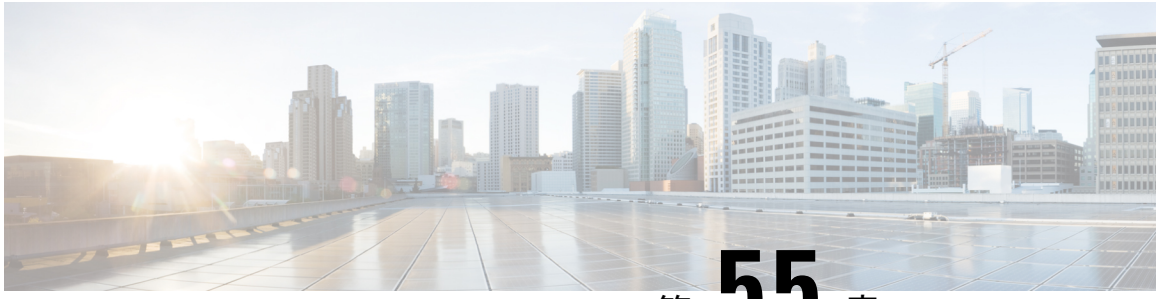
ステップ 1 **[Devices]** > **[NAT]** を選択します。

ステップ 2 コピーする NAT ポリシーの横にあるコピー アイコン（  ）をクリックします。

ステップ 3 [名前（Name）] に、ポリシーの一意の名前を入力します。

マルチドメイン展開では、ポリシー名をドメイン階層内で一意にする必要があります。システムは、現在のドメインでは表示できないポリシーの名前との競合を特定することができます。

ステップ 4 [OK] をクリックします。



第 55 章

7000 および 8000 シリーズ デバイス用の NAT

以下のトピックでは、7000 および 8000 シリーズ デバイス用に NAT を設定する方法を示します。

NAT ポリシーの設定

特定のネットワーク ニーズを管理するためにさまざまな方法で NAT ポリシーを設定できます。次の操作を実行できます。

- 外部ネットワークに内部サーバを公開します。

  この設定では、外部 IP アドレスから内部 IP アドレスへのスタティック変換を定義するため、システムはネットワーク外部から内部サーバにアクセスできます。サーバに送信されるトラフィックは、外部 IP アドレスまたは IP アドレスとポートを対象とし、内部 IP アドレスまたは IP アドレスとポートに変換されます。サーバからのリターン トラフィックは、外部アドレスに再度変換されます。

- 内部ホスト/サーバが外部アプリケーションに接続できるようにします。

  この設定では、内部アドレスから外部アドレスへのスタティック変換を定義します。この定義により、内部ホストまたはサーバは、内部ホストまたはサーバが特定の IP アドレスおよびポートを持っていると予期する外部アプリケーションへの接続を開始できます。したがって、システムは内部ホストまたはサーバのアドレスを動的に割り当てることはできません。

- 外部ネットワークに対してプライベート ネットワーク アドレスを隠します。

  以下のいずれかの設定を使用して、内部ネットワーク アドレスをわかりにくくすることができます。

  - 内部ネットワークの必要に十分対応できるだけの数の外部 IP アドレスがある場合は、IP アドレスのブロックを使用できます。この設定では、すべての発信トラフィックの

送信元 IP アドレスを、外部に面する IP アドレスのうち未使用の IP アドレスに自動的に変換するダイナミック変換を作成します。

- 内部ネットワークの必要に対応できるだけの数の外部 IP アドレスがない場合は、限定した数の IP アドレスのブロックとポート変換を使用できます。この設定では、発信トラフィックの送信元 IP アドレスとポートを、外部に面する IP アドレスのうち未使用の IP アドレスとポートに自動的に変換するダイナミック変換を作成します。

⚠

注意 7000 または 8000 シリーズ デバイスの高可用性ペアでは、NAT 変換により影響を受けるすべてのネットワークがプライベートの場合、ペアを構成するデバイス上でのスタティック NAT ルールに対して個別のピア インターフェイスのみを選択します。パブリック ネットワークとプライベート ネットワーク間のトラフィックに影響するスタティック NAT ルールには、この設定を**使用しないでください**。

NAT ポリシーの設定ガイドライン

NAT ポリシーを設定するには、ポリシーに一意の名前を付け、ポリシーを展開するデバイスつまりターゲットを特定する必要があります。また、NAT ルールを追加、編集、削除、有効化、および無効化することができます。NAT ポリシーを作成または変更した後、ターゲット デバイスのすべてまたは一部にポリシーを展開できます。

スタンドアロン デバイスと同様に、NAT ポリシーをペアリングされたスタックを含む 7000 または 8000 シリーズ デバイス高可用性ペアに展開できます。ただし、個別のペアリングされたデバイスまたは高可用性ペア全体でインターフェイスのスタティック NAT ルールを定義し、送信元ゾーン内でインターフェイスを使用できます。ダイナミック ルールの場合、送信元ゾーンまたは宛先ゾーンで高可用性ペア全体のインターフェイスのみを使用できます。

⚠

注意 7000 または 8000 シリーズ デバイス高可用性ペアで、NAT 変換により影響を受けるすべてのネットワークがプライベートの場合、ペアリングされたデバイスのスタティック NAT ルールに対して、個別のピア インターフェイスのみを選択します。パブリック ネットワークとプライベート ネットワーク間のトラフィックに影響するスタティック NAT ルールに対してこの設定を使用**しない**でください。

HA リンク インターフェイスが確立されていないデバイス高可用性ペアでダイナミック NAT を設定した場合、両方のペアリングされたデバイスは別々にダイナミック NAT エントリを割り当て、システムはデバイス間でエントリを同期できません。

スタンドアロン デバイスと同様に、NAT ポリシーをデバイス スタックに展開できます。NAT ポリシーに含まれ、スタックのメンバーであるセカンダリ デバイスのインターフェイスに関連付けられているルールを持ったデバイスからデバイス スタックを確立した場合、セカンダリ デバイスのインターフェイスは NAT ポリシーに残ります。インターフェイスを持つポリシーを保存および展開できますが、ルールは変換を実現しません。

（注） アクティブ FTP は、NAT が設定された 7000 または 8000 シリーズ デバイスではサポートされていません。代わりにパッシブ FTP を使用してください。

先祖ドメインのマルチドメイン展開では、編集できる現在のドメインで作成されたポリシーが表示されます。また、編集できない先祖ドメインで作成されたポリシーも表示されます。下位のドメインで作成されたポリシーを表示および編集するには、そのドメインに切り替えます。管理者は、NAT ポリシーのターゲットを子孫ドメインのデバイスに設定できます。こうすることで、子孫ドメインではカスタマイズされたローカル ポリシーを使用または置き換えることができます。

NAT ポリシー内のルール編成

NAT ポリシーの編集ページにはスタティックな NAT ルールとダイナミックな NAT ルールが別々に表示されます。スタティック ルールは名前のアルファベット順に並べ替えられ、表示順序を変更できません。同一の照合値を持つスタティック ルールは作成できません。システムの照合では、ダイナミック変換を検査する前に、スタティック変換を検査します。

ダイナミック ルールは番号順に処理されます。各ダイナミック ルールの番号位置は、ページ左側のルールの横に表示されます。ダイナミック ルールは移動または挿入したり、ルールの順序を変更したりすることができます。たとえば、ダイナミック ルール 10 をダイナミック ルール 3 の下に移動した場合、ルール 10 がルール 4 になり、後に続くすべての番号が順次繰り上がります。

システムはポリシーの [Edit] ページ上のルールの番号順にパケットとダイナミック ルールを比較するので、ダイナミック ルールの位置は重要です。パケットがダイナミック ルールのすべての条件を満たすと、システムはパケットにそのルール条件を適用し、そのパケットに対する後続のルールはすべて無視します。

ダイナミック ルールを追加または編集する際、ダイナミック ルールの番号の位置を指定できます。新しいダイナミック ルールを追加する前にダイナミック ルールを強調表示して、強調表示したルールの下に新しいルールを挿入することもできます。

ルールの行内の空白部分をクリックすることにより、1つ以上のダイナミック ルールを選択できます。選択したダイナミック ルールを新しい場所にドラッグ アンド ドロップできます。これにより、移動したルールと後続のすべてのルールの位置が変更されます。

選択したルールを既存のルールの上または下にカット アンド ペーストできます。スタティック ルールは [Static Translations] リストにのみ、ダイナミック ルールは [Dynamic Translations] リストにのみ貼り付けることができます。また、選択したルールを削除したり、既存のルール リスト内の任意の場所に新しいルールを挿入したりすることもできます。

先行ルールが優先して適用されるために決して一致することがないルールを示す、説明的な警告を表示することもできます。

展開にアクセス コントロール ポリシーが存在する場合、このシステムではアクセス制御を通過するまでトラフィックを変換することありません。

NAT ルールの編成

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
該当なし	Control	7000 & 8000 シリーズ	任意（Any）	Admin/Network Admin

ステップ 1 **[Devices]** > **[NAT]** を選択します。

ステップ 2 変更する NAT ポリシーの横にある編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 NAT ルールを編成します。

- ルールを選択するには、ルールの行の空白部分をクリックします。
- ルールの選択をクリアするには、ページの右下にあるリロードアイコン（）をクリックします。個別のルールをクリアするには、Ctrl キーを押しながら各ルールの行内の空白部分をクリックします。
- 選択したルールを切り取りまたはコピーするには、選択したルールの行の空白部分を右クリックして、[切り取り（Cut）] または [コピー（Copy）] を選択します。
- 切り取ったルールまたはコピーしたルールをルール リストに貼り付けるには、選択したルールを貼り付けるルールの行の空白部分を右クリックして、[上に貼り付け（Paste above）] または [下に貼り付け（Paste below）] を選択します。
- 選択したルールを移動するには、選択したルールを新しい位置の下にドラッグ アンド ドロップします。この移動先の位置は、ドラッグ時にポインタの上に表示される青い横線で示されます。
- ルールを削除するには、ルールの横にある削除アイコン（）をクリックして、[OK] をクリックします。
- 警告を表示するには、[警告の表示（Show Warnings）] をクリックします。

NAT ルールの警告とエラー

NAT ルールの条件が後続のルールによるトラフィックの照合をプリエンプション処理する場合があります。どのようなタイプのルール条件でも、後続のルールを回避する可能性があります。

あるルールとその後続のルールがまったく同じで、いずれもすべて同じ条件が設定されている場合、後続のルールは回避されます。いずれかの条件が異なっていた場合、後続のルールはプリエンプション処理されません。

NAT ポリシーの展開失敗の原因となるルールを作成した場合、ルールの横にエラー アイコン（  ）が表示されます。スタティック ルールに矛盾がある場合、または現時点で無効となるポリシーで使用されるネットワーク オブジェクトを編集した場合、エラーが発生します。たとえば、IPv6 アドレスのみを使用するようにネットワーク オブジェクトを変更した結果、少なくとも 1 つのネットワークが必要な状況で、そのオブジェクトを使用するルールに有効なネットワークがなくなると、エラーが発生します。エラー アイコンは自動的に表示されます。[警告を表示（Show Warnings）] をクリックする必要はありません。

NAT ルール警告の表示と非表示

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
該当なし	Control	7000 & 8000 シリーズ	任意（Any）	Admin/Network Admin

ステップ 1 **[Devices]** > **[NAT]** を選択します。

ステップ 2 変更する NAT ポリシーの横にある編集アイコン（  ）をクリックします。

代わりに表示アイコン（  ）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 警告を表示するには、[警告を表示（Show Warnings）] をクリックします。

ページが更新され、プリエンプション処理された各ルールの横に警告アイコン（  ）が表示されます。

ステップ 4 ルールの警告を表示するには、ルールの横にある警告アイコン（  ）の上にポインタを合わせます。

ルールをプリエンプション処理するルールを示すメッセージが表示されます。

ステップ 5 警告をクリアするには、[警告を非表示（Hide Warnings）] をクリックします。

ページが更新され、警告が消えます。

NAT ポリシー規則のオプション

NAT ルールは次の働きを持つ設定および条件のセットです。

- ネットワーク トラフィックを限定する
- 条件に一致するトラフィックの変換方法を指定する

既存の NAT ポリシーから NAT ルールを作成および編集します。各ルールは 1 つのポリシーにのみ属します。

ルールの追加と編集は同様の Web インターフェイスで行います。ページの上部でルールの名前、状態、タイプ、および位置（ダイナミックの場合）を指定します。ページの左側のタブを使用して、条件を構築します。条件タイプごとに独自のタブがあります。

次のリストは、NAT ルールの設定可能なコンポーネントを示しています。

Name

各ルールに一意の名前を付けます。スタティック NAT ルールでは、最大 22 文字を使用します。ダイナミック NAT ルールでは、最大 30 文字を使用します。スペースや特殊文字（「:」は除く）など、印刷可能文字を使用できます。

Rule State

デフォルトでは、ルールが有効状態になります。ルールを無効にすると、変換用のネットワーク トラフィックの評価に使用されません。NAT ポリシーのルール リストを表示すると、無効なルールはグレー表示されますが、変更は可能です。

Type

ルールのタイプによって、ルールの条件に一致するトラフィックの処理方法が決まります。NAT ルールを作成および編集する際、設定可能なコンポーネントはルール タイプによって異なります。

位置（Position）（ダイナミック ルールのみ）

NAT ポリシーのダイナミック ルールには 1 から始まる番号が付いています。システムは、ルール番号の昇順で、NAT ルールを上から順にトラフィックと照合します。

ルールをポリシーに追加する際、参照ポイントとしてルール番号を使用し、特定のルールの**上**または**下**に配置することによって位置を指定します。既存のルールを編集するときには、同様の方法でルールを**移動**できます。

条件（Conditions）

ルール条件は変換する特定のトラフィックを識別します。条件はセキュリティ ゾーン、ネットワーク、および転送プロトコルのポートなど、複数の属性を任意に組み合わせてトラフィックと照合できます。

関連トピック

NAT ルールの作成および編集 （1432 ページ）

NAT ルールの作成および編集

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
該当なし	Control	7000 & 8000 シリーズ	任意（Any）	Admin/Network Admin

マルチドメイン導入では、現在のドメインで作成されたポリシーとルールが表示されます。これは編集できます。先祖ドメインで作成されたポリシーとルールも表示されますが、これは編

集できません。下位のドメインで作成されたルールを表示および編集するには、そのドメインに切り替えます。

ステップ 1 **[Devices]** > **[NAT]** を選択します。

ステップ 2 ルールを追加する NAT ポリシーの横にある編集アイコン（  ）をクリックします。

代わりに表示アイコン（  ）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 新しいルールを追加するか、既存のルールを編集します。

- 新しいルールを追加するには、[ルールの追加（Add Rule）] をクリックします。
- 既存のルールを編集するには、そのルールの横にある編集アイコン（  ）をクリックします。

ステップ 4 [名前（Name）] に一意のルール名を入力します。

ステップ 5 次のルール コンポーネントを設定します。

- ルールを**有効**にするかどうかを指定します。
- [タイプ（Type）] で、ルール タイプを指定します。
- ルールの位置（ダイナミック ルールのみ）を指定します。
- ルールの条件を設定します。

（注） スタティック ルールは元の宛先ネットワークを含む必要があります。ダイナミック ルールは変換された送信元ネットワークを含む必要があります。

ステップ 6 [Add] をクリックします。

ステップ 7 **[保存（Save）]** をクリックします。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

NAT ルールのタイプ

すべての NAT ルールには次の働きを持つタイプが関連付けられています。

- ネットワーク トラフィックを限定する
- 条件に一致するトラフィックの変換方法を指定する

次に、NAT ルール タイプの概要を示します。

スタティック

スタティック ルールは宛先ネットワークと任意選択のポートおよびプロトコルで1対1変換を提供します。スタティック変換を設定する場合、送信元ゾーン、宛先ネットワーク、および宛先ポートを設定できます。宛先ゾーンまたは送信元ネットワークを設定できません。

元の宛先ネットワークを指定する**必要**があります。宛先ネットワークでは、単一の IP アドレスを含むネットワーク オブジェクトおよびグループを選択するか、または単一の IP アドレスを表すリテラル IP アドレスを入力することのみが可能です。元の宛先ネットワークと変換後の宛先ネットワークはそれぞれ 1 つのみ指定できます。

（注） システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。 上書き対応オブジェクトを使用すると、子孫ドメインの管理者は、グローバル コンフィギュレーションを自分のローカル環境に調整できます。

元の宛先ポートと変換後の宛先ポートをそれぞれ1つ指定できます。元の宛先ポートを指定するには、その前に、元の宛先ネットワークを指定する必要があります。さらに、元の宛先ポートを指定しない場合は、変換後の宛先ポートを指定できません。また、変換後の値は、元の値のプロトコルと一致する必要があります。

注意 高可用性ペアとして構成されている 7000 または 8000 シリーズ デバイスのスタティック NAT ルールについては、NAT 変換で影響を受けるすべてのネットワークがプライベートの場合、個別のピアインターフェイスのみを選択します。パブリック ネットワークとプライベート ネットワーク間のトラフィックに影響するスタティック NAT ルールに対してこの設定を使用**しない**でください。

ダイナミック IP 専用

ダイナミック IP 専用ルールは多対多の送信元ネットワークを変換しますが、ポートおよびプロトコルを維持しますダイナミック IP 専用変換を設定する場合、ゾーン、送信元ネットワーク、元の宛先ネットワーク、および元の宛先ポートを設定できます。変換後の宛先ネットワークまたは変換後の宛先ポートは設定できません。

変換後の送信元ネットワークを少なくとも1つ指定する**必要**があります。変換後の送信元ネットワーク値の数が元の送信元ネットワークの数よりも小さい場合、元のアドレスがすべて照合される前に変換後のアドレスが不足する可能性があるという警告がルールに表示されます。

同じパケットに一致する条件を持つルールが複数個ある場合、優先度の低いルールはデッド ルールとなり、トリガーされなくなります。デッド ルールにも警告が表示されます。ツールチップを表示して、デッド ルールに代わるルールを判別できます。

（注） デッドルールを持つポリシーを保存し、展開することは可能ですが、ルールは変換を実現できません。

場合によっては、範囲の広いルールよりも優先される、範囲が限定されたルールを作成することをお勧めします。次に例を示します。

```
Rule 1: Match on address A and port A/Translate to address B
Rule 2: Match on address A/Translate to Address C
```

この例で、ルール 1 はルール 2 にも一致するいくつかのパケットに一致します。したがって、ルール 2 が完全に無効（デッド）ではありません。

元の宛先ポートだけを指定した場合、変換後の宛先ポートを指定することはできません。

ダイナミック IP およびポート

ダイナミック IP およびポート ルールは多対 1 または多対多の送信元ネットワークとポートおよびプロトコルを変換します。ダイナミック IP およびポート変換を設定する場合、ゾーン、送信元ネットワーク、元の宛先ネットワーク、および元の宛先ポートを設定できます。変換後の宛先ネットワークまたは変換後の宛先ポートは設定できません。

変換後の送信元ネットワークを少なくとも 1 つ指定する**必要**があります。同じパケットに一致する条件を持つルールが複数個ある場合、優先度の低いルールはデッド ルールとなり、トリガーされなくなります。デッド ルールにも警告が表示されます。ツールチップを表示して、デッド ルールに代わるルールを判別できます。

（注） デッドルールを持つポリシーを保存し、展開することは可能ですが、ルールは変換を実現できません。

元の宛先ポートだけを指定した場合、変換後の宛先ポートを指定することはできません。

（注） ダイナミック IP およびポート ルールを作成し、システムがポートを使用しないトラフィックを渡す場合、そのトラフィックに対して変換は発生しません。たとえば、送信元ネットワークに一致する IP アドレスからの ping（ICMP）は、ICMP がポートを使用しないため、マッピングされません。

NAT ルールの条件タイプ

次の表に、指定された NAT ルール タイプに基づいて設定可能な NAT ルールの条件タイプをまとめています。

表 *100 : NAT* ルール タイプごとに使用可能な *NAT* ルールの条件タイプ

条件	スタティック	ダイナミック（IP 専用または IP およびポート）
送信元ゾーン	任意	任意
宛先ゾーン	不可	任意
元の送信元ネットワーク	不可	任意
変換後の送信元ネットワーク	不可	**必須**
元の宛先ネットワーク	**必須**	任意
変換後の宛先ネットワーク	任意。単一アドレスのみ	不可
元の宛先ポート	任意。単一ポートでのみ、元の宛先ネットワークを定義する場合のみ可能	任意
変換後の宛先ポート	任意。単一ポートでのみ、元の宛先ポートを定義する場合のみ可能	不可

NAT ルールの条件と条件の仕組み

ルールに一致するトラフィックのタイプを識別するために NAT ルールに条件を追加できます。それぞれの条件タイプごとに、使用可能条件リストから、ルールに追加する条件を選択します。条件フィルタを適用できる場合は、条件フィルタを使って使用可能な条件を限定できます。使用可能な条件リスト、および選択した条件リストは、1 つの条件だけを含む場合も、数ページに及ぶ場合もあります。使用可能な条件は検索することができ、名前や値を入力するとそれに一致する条件だけが表示され、入力していくにつれてそのリストが更新されます。

条件のタイプに応じて、使用可能条件リストには、Cisco から直接提供された条件と、他の Firepower システム機能を使って設定された条件が一緒に含まれることがあります。その中には、オブジェクト マネージャ（**[Objects]** > **[Object Management]**）を使って作成されたオブジェクト、個別の条件ページから直接作成されたオブジェクト、およびリテラル条件が含まれます。

NAT ルールの条件

次の表で説明されている条件のいずれかを満たすトラフィックを照合するための NAT ルールを設定できます。

表 *101 : NAT* ルールの条件タイプ

条件	説明
ゾーン	NAT ポリシーを展開できる 1 つ以上のルーテッド インターフェイスの設定。ゾーンは、送信元インターフェイスと宛先インターフェイスでトラフィックを分類するメカニズムであり、ルールに送信元のゾーン条件と宛先のゾーン条件を追加することができます。
ネットワーク	明示的に指定した、またはネットワーク オブジェクトとグループを使用した、個々の IP アドレス、CIDR ブロック、およびプレフィックス長の組み合わせ。NAT ルールに送信元ネットワーク条件と宛先ネットワーク条件を追加できます。
宛先ポート	トランスポート プロトコルに基づいて作成される、個別のポート オブジェクトとグループポート オブジェクトを含むトランスポート プロトコル ポート。

NAT ルールへの条件の追加

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
該当なし	Control	7000 & 8000 シリーズ	任意（Any）	Admin/Network Admin

NAT ルールへの条件の追加は基本的にどの条件のタイプでも同じです。左側の使用可能な条件のリストから選択して、右側で選択した条件の 1 つまたは 2 つのリストに、選択した条件を追加します。

すべての条件タイプで、使用可能な個々の条件を 1 つまたは複数クリックすると、それが強調表示され、選択状態になります。2 つのタイプのリスト間にあるボタンをクリックして選択した使用可能な条件を選択した条件のリストに追加するか、または選択した使用可能な条件を選択した条件のリストにドラッグ アンド ドロップします。

選択済み条件リストには、タイプごとに最大 50 個までの条件を追加できます。たとえばアプライアンスの上限に達するまで、最大 50 個の送信元ゾーン条件、最大 50 個の宛先ゾーン条件、最大 50 個の送信元ネットワーク条件などを追加できます。

ステップ 1 **[Devices]** > **[NAT]** を選択します。

ステップ 2 変更する NAT ポリシーの横にある編集アイコン（  ）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 [ルールの追加（Add Rule）] をクリックします。

ステップ 4 ルールの [名前（Name）] を入力します。

ステップ 5 ルールの [タイプ（Type）] を指定します。

ステップ 6 ルールに追加する条件タイプに対応したタブをクリックします。

ステップ 7 次のいずれかの操作を行います。

- 表示されている条件を、すでに選択済みの条件のリストに追加するには、表示されている条件をクリックします。
- 表示されている条件をすべて選択するには、条件のいずれかの行を右クリックし、[すべて選択（Select All）] をクリックします。
- 表示されている条件の一部またはフィルタされた条件を選択するには、[検索（Search）] フィールド内をクリックし、検索のための文字列を入力します。入力していくと、リストが更新されて一致する項目が表示されます。

  オブジェクト名およびオブジェクトに設定されている値を検索対象にできます。たとえば `Texas Office` という名前の個別ネットワーク オブジェクトがあり、`192.168.3.0/24` という値が設定されていて、`US Offices` というグループ オブジェクトに含まれる場合、`Tex` などの部分的または完全な検索文字列を入力するか、または `3` などの値を入力することにより、両方のオブジェクトを表示できます。

- 表示されている条件を検索中、またはフィルタ中に検索文字列をクリアするには、検索フィールドの上のリロード アイコン（）または検索フィールド内のクリア アイコン（）をクリックします。
- 表示されている条件リストからゾーンの条件を選択し、選択済みの送信元または宛先の条件リストに追加するには、[送信元に追加（Add to Source）] または [宛先に追加（Add to Destination）] をクリックします。
- 表示されている条件リストからネットワークとポートの条件を選択し、選択済みの元または変換済みの条件リストに追加するには、[元に追加（Add to Original）] または [変換済みに追加（Add to Translated）] をクリックします。
- 表示されている条件を選択済み条件のリストにドラッグアンドドロップするには、選択済み条件をクリックし、選択済み条件のリストにドラッグ アンド ドロップします。
- リテラルフィールドを使用し、選択済み条件のリストにリテラル条件を追加するには、クリックしてリテラルフィールドからのプロンプトを削除し、リテラル条件を入力し、[追加（Add）] をクリックします。ネットワーク条件は、リテラル条件を追加するためのフィールドを提供します。
- ドロップダウン リストを使用し、選択済み条件のリストにリテラル条件を追加するには、ドロップダウン リストから条件を選択し、[追加（Add）] をクリックします。ポート条件には、リテラル条件を追加するためのドロップダウン リストがあります。
- 個々のオブジェクトまたは条件フィルタを追加して、条件リストからそれを選択できるよう表示させるには、追加アイコン（）をクリックします。
- 選択済み条件のリストから条件を 1 つだけ削除するには、条件の横にある削除アイコン（）をクリックします。
- 選択済み条件のリストから条件を削除するには、選択済み条件のリストの行を右クリックして強調表示し、[削除（Delete）] をクリックします。

ステップ 8 設定を保存するには、[追加（Add）] をクリックします。

NAT ルールのリテラル条件

次の条件タイプについて、元のおよび変換後の条件のリストにリテラル値を追加できます。

- ネットワーク
- ポート

ネットワーク条件の場合、元のまたは変換後の条件リストの下にある設定フィールドにリテラル値を入力します。

ポート条件では、ドロップダウン リストからプロトコルを選択します。プロトコルが `All`、または `TCP` または `UDP` である場合、設定フィールドにポート番号を入力します。

該当するそれぞれの条件ページには、リテラル値を追加するために必要なコントロールがあります。設定フィールドに入力した値が無効である場合や、まだ有効と認識されていない場合は、赤いテキストとして表示されます。入力時に有効と認識された値は青色に変わります。有効な値が認識されると、グレー表示の [追加（Add）] ボタンがアクティブになります。追加したリテラル値は、選択済み条件リストにただちに表示されます。

（注） システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。 上書き対応オブジェクトを使用すると、子孫ドメインの管理者は、グローバル コンフィギュレーションを自分のローカル環境に調整できます。

NAT ルールの条件のオブジェクト

オブジェクト マネージャ（**[Objects]** > **[Object Management]**）で作成されたオブジェクトは、使用可能な NAT ルール条件の関連リストからすぐに選択可能になります。

NAT ポリシーから直接オブジェクトを作成することもできます。該当する条件ページ上のコントロールでは、オブジェクトマネージャでの設定コントロールと同じ機能を利用できます。

直接作成された個別のオブジェクトは使用可能なオブジェクトのリストにすぐに表示されます。それらを現在のルールと他の既存および将来のルールに追加できます。該当する条件ページとポリシー編集ページで、ポインタを 1 つの個別オブジェクトの上に置くとそのオブジェクトの内容が表示され、グループ オブジェクトの上に置くと、グループ内の個々のオブジェクトの数が表示されます。

NAT ルール内のゾーン条件

システムのセキュリティゾーンは、管理対象デバイス上のインターフェイスから構成されています。NAT ルールに追加するゾーンは、それらのゾーン内にルーテッドまたはハイブリッドインターフェイスを持つネットワーク上のデバイスへのルールをターゲットにします。NAT ルールの条件として、ルーテッド インターフェイスまたはハイブリッド インターフェイスを持つセキュリティ ゾーンのみを追加できます。

現在仮想ルータに割り当てられているゾーンまたはスタンドアロンインターフェイスのどちらかをNATルールに追加できます。デバイス設定が展開されていないデバイスがある場合、[ゾーン（Zones）] ページの使用可能なゾーン リストの上に警告アイコン（  ）が表示され、展開済みのゾーンとインターフェイスだけが表示されることが示されます。ゾーンの横にある矢印アイコン（）をクリックして、ゾーンを縮小または展開し、そのインターフェイスを非表示または表示することができます。

インターフェイスがハイ アベイラビリティペアの 7000 または 8000 シリーズ デバイス上にある場合、使用可能なゾーンのリストに、そのインターフェイスからの追加のブランチが表示されると共に、そのハイ アベイラビリティ ペアの他のインターフェイスがそのハイ アベイラビリティ ペアのアクティブ デバイスのプライマリ インターフェイスの子として表示されます。矢印アイコン（）をクリックして、ペアになったデバイスインターフェイスを縮小または展開し、そのインターフェイスを非表示または表示することもできます。

（注） 無効にされたインターフェイスを持つポリシーを保存して展開できますが、ルールではそれらのインターフェイスが有効になるまで変換を提供できません。

右側の 2 つのリストは、NAT ルールによって照合目的に使用される送信元ゾーンと宛先ゾーンです。すでにルールに値が設定されている場合、ルールを編集する際、これらのリストには既存の値が表示されます。送信元ゾーンのリストが空の場合、ルールは任意のゾーンまたはインターフェイスからのトラフィックを照合します。宛先ゾーンのリストが空の場合、ルールは任意のゾーンまたはインターフェイス宛てのトラフィックを照合します。

対象のデバイスでトリガーされることがないゾーンの組み合わせを持つルールに対しては警告が表示されます。

（注） これらのゾーンの組み合わせを持つポリシーを保存して展開できますが、ルールでは変換を提供しません。

ゾーン内の項目を選択するか、またはスタンドアロンインターフェイスを選択することによって、個別のインターフェイスを追加できます。割り当てられているゾーンがまだ送信元ゾーンまたは宛先ゾーンのリストに追加されていない場合のみ、ゾーン内のインターフェイスを追加できます。これらの個別に選択されたインターフェイスは、それらのインターフェイスを削除して別のゾーンに追加した場合でも、各ゾーンに対する変更の影響を受けません。インターフェイスがハイ アベイラビリティ ペアのプライマリ メンバーで、ダイナミック ルールを設定す

る場合、そのプライマリインターフェイスだけを送信元ゾーンまたは宛先ゾーンのリストに追加できます。スタティック ルールの場合、個別のハイ アベイラビリティ ペアのメンバー インターフェイスを送信元ゾーンのリストに追加できます。ハイ アベイラビリティ ペアのプライマリ インターフェイスは、その子がまったく追加されていない場合にだけ、リストに追加できます。また、個別のハイ アベイラビリティ ペアのインターフェイスは、プライマリが追加されていない場合にだけ追加できます。

ゾーンを追加すると、ルールではそのゾーンに関連付けられているすべてのインターフェイスを使用します。ゾーンに対してインターフェイスを追加または削除すると、インターフェイスが存在するデバイスにデバイス設定が再度展開されるまで、ルールでは更新されたバージョンのゾーンを使用しません。

（注） スタティック NAT ルールでは、送信元ゾーンのみを追加できます。ダイナミック NAT ルールでは、送信元ゾーンと宛先ゾーンの両方を追加できます。

NAT ルールへのゾーン条件の追加

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
該当なし	Control	7000 & 8000 シリーズ	任意（Any）	Admin/Network Admin

ステップ 1 **[Devices]** > **[NAT]** を選択します。

ステップ 2 変更する NAT ポリシーの横にある編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 [ルールの追加（Add Rule）] をクリックします。

ステップ 4 ルールの [名前（Name）] を入力します。

ステップ 5 ルールの [タイプ（Type）] を指定します。

ステップ 6 [ゾーン（Zones）] タブをクリックします。

ステップ 7 [使用可能なゾーン（Available Zones）] リスト内のゾーンまたはインターフェイスをクリックします。

ステップ 8 次の選択肢があります。

- 送信元ゾーンによりトラフィックを照合するには、[Add to Source] をクリックします。
- 宛先ゾーンによりトラフィックを照合するには、[宛先に追加（Add to Destination）] をクリックします。

（注） スタティック NAT ルールには送信元ゾーンのみを追加できます。さらに、無効になっているインターフェイスを NAT ルールに追加できますが、ルールは変換を実現しません。

ステップ 9 [追加（Add）] をクリックして新しいルールを保存します。

ステップ 10 [保存（Save）] をクリックして、変更したポリシーを保存します。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

ダイナミック NAT ルールの送信元ネットワーク条件

パケットの送信元 IP アドレスの照合値と変換値を設定します。元の送信元ネットワークが設定されていない場合、すべての送信元 IP アドレスがダイナミック NAT ルールに一致します。スタティック NAT ルールの送信元ネットワークは設定できないことに注意してください。パケットがNATルールに一致すると、システムは変換後の送信元ネットワークの値を使用して、送信元 IP アドレスの新しい値を割り当てます。ダイナミック ルール用に少なくとも 1 つの値を持つ変換後の送信元ネットワークを設定する必要があります。

注意 ネットワーク オブジェクトまたはオブジェクト グループが NAT ルールで使用されている場合に、オブジェクトまたはグループを変更または削除すると、ルールが無効になる可能性があります。

ダイナミック NAT ルールに、次の種類の送信元ネットワーク条件を追加できます。

- オブジェクト マネージャを使って作成した個別およびグループのネットワーク オブジェクト
- 送信元ネットワーク条件のページから追加し、ユーザのルールと他の既存および将来のルールに追加可能な個別のネットワーク オブジェクト
- リテラル、単一 IP アドレス、範囲、またはアドレス ブロック

（注） システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。 上書き対応オブジェクトを使用すると、子孫ドメインの管理者は、グローバル コンフィギュレーションを自分のローカル環境に調整できます。

ネットワーク条件のダイナミック NAT ルールへの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
該当なし	Control	7000 & 8000 シリーズ	任意（Any）	Admin/Network Admin

展開されているポリシーで使用中のダイナミック ルールのネットワーク条件を更新すると、既存の変換済みアドレス プールを使用しているネットワーク セッションがドロップされます。

ステップ 1 **[Devices]** > **[NAT]** を選択します。

ステップ 2 変更する NAT ポリシーの横にある編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 [ルールの追加（Add Rule）] をクリックします。

ステップ 4 ルールの [名前（Name）] を入力します。

ステップ 5 ルールのダイナミック [タイプ（Type）] を指定します。

- **ダイナミック IP 専用**
- **ダイナミック IP およびポート**

ステップ 6 [送信元ネットワーク（Source Network）] タブをクリックします。

ステップ 7 必要に応じて、リストの上にある追加アイコン（）をクリックし、[使用可能なネットワーク（Available Networks）] リストへ個々のネットワーク オブジェクトを追加します。

各ネットワーク オブジェクトに複数の IP アドレス、CIDR ブロック、およびプレフィクス長を追加できます。

ステップ 8 [使用可能なネットワーク（Available Networks）] リスト内の条件をクリックします。

ステップ 9 次の選択肢があります。

- 元の送信元ネットワークによりトラフィックを照合するには、[Add to Original] をクリックします。
- 変換後の送信元ネットワークと照合するトラフィックの変換値を指定するには、[変換後に追加（Add to Translated）] をクリックします。

ステップ 10 リテラル IP アドレス、範囲、アドレスブロックを追加するには、

a) [元の送信元ネットワーク（Original Source Network）] または [変換後の送信元ネットワーク（Translated Source Network）] リストの下にある [IP アドレス入力（Enter an IP address）] プロンプトをクリックします。

b) IP アドレス、範囲、アドレスブロックを入力します。

範囲は、下位の IP アドレス - 上位の IP アドレスの形式で追加します。例：`179.13.1.1-179.13.1.10`.

（注） システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。 上書き対応オブジェクトを使用すると、子孫ドメインの管理者は、グローバル コンフィギュレーションを自分のローカル環境に調整できます。

c) 入力した値の横にある [追加（Add）] をクリックします。

ステップ 11 [追加（Add）] をクリックしてルールを保存します。

ステップ 12 [保存（Save）] をクリックして、変更したポリシーを保存します。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

NAT ルールの宛先ネットワーク条件

パケットの宛先 IP アドレスの照合値と変換値を設定します。ダイナミック NAT ルールの変換後の宛先ネットワークを設定できないことに注意してください。

スタティック NAT ルールは 1 対 1 変換であるため、[Available Networks] リストには単一の IP アドレスのみを含むネットワーク オブジェクトおよびグループのみが含まれます。スタティック変換用に、単一のオブジェクトまたはリテラル値のみを [Original Destination Network] リストと [Translated Destination Network] リストの両方に追加できます。

注意 ネットワーク オブジェクトまたはオブジェクト グループが NAT ルールで使用されている場合に、オブジェクトまたはグループを変更または削除すると、ルールが無効になる可能性があります。

NAT ルールに、次の種類の宛先ネットワーク条件を追加できます。

- オブジェクト マネージャを使って作成した個別およびグループのネットワーク オブジェクト
- [宛先ネットワーク（Destination Network）] 条件のページから追加し、ユーザのルールと他の既存および将来のルールに追加可能な個別のネットワーク オブジェクト
- リテラル、単一 IP アドレス、範囲、またはアドレス ブロック

  スタティック NAT ルールでは、リストにまだ値がない場合に限り、CIDR とサブネット マスク /32 のみを追加できます。

（注） システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。 上書き対応オブジェクトを使用すると、子孫ドメインの管理者は、グローバル コンフィギュレーションを自分のローカル環境に調整できます。

NAT ルールへの宛先ネットワーク条件の追加

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
該当なし	Control	7000 & 8000 シリーズ	任意（Any）	Admin/Network Admin

展開されているポリシーで使用中のダイナミック ルールのネットワーク条件を更新すると、既存の変換済みアドレス プールを使用しているネットワーク セッションがドロップされます。

ステップ 1 **[Devices]** > **[NAT]** を選択します。

ステップ 2 変更する NAT ポリシーの横にある編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 [ルールの追加（Add Rule）] をクリックします。

ステップ 4 ルールの [名前（Name）] を入力します。

ステップ 5 ルールの [タイプ（Type）] を指定します。

ステップ 6 [宛先ネットワーク（Destination Network）] タブをクリックします。

ステップ 7 必要に応じて、リストの上にある追加アイコン（）をクリックし、[使用可能なネットワーク（Available Networks）] リストへ個々のネットワーク オブジェクトを追加します。

ダイナミック ルールの場合、各ネットワーク オブジェクトに複数の IP アドレス、CIDR ブロック、およびプレフィクス長を追加できます。スタティック ルールの場合、単一の IP アドレスのみを追加できます。

ステップ 8 [使用可能なネットワーク（Available Networks）] リスト内の条件またはオブジェクトをクリックします。

ステップ 9 次の選択肢があります。

- 元の宛先ネットワークによりトラフィックを照合するには、[Add to Original] をクリックします。
- 変換後の宛先ネットワークと照合するトラフィックの変換値を指定するには、[変換後に追加（Add to Translated）] をクリックします。

ステップ 10 オプションで、[元の宛先ネットワーク（Original Destination Network）] リストまたは [変換後の宛先ネットワーク（Translated Destination Network）] リストの下の [IP アドレス入力（Enter an IP address）] プロンプトをクリックし、次に、IP アドレスまたはアドレス ブロックを入力して、[追加（Add）] をクリックします。

ステップ 11 [追加（Add）] をクリックします。

ステップ 12 [保存（Save）] をクリックし、ポリシーの変更内容を保存します。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

NAT ルールでのポート条件

ルールにポート条件を追加することで、元の宛先ポートと変換後の宛先ポートおよび変換用の転送プロトコルに基づいてネットワークトラフィックを照合できます。元のポートが設定されていない場合、すべての宛先ポートがルールに一致します。パケットがNATルールに一致し、変換後の宛先ポートが設定されている場合、システムはその値にポートを変換します。ダイナミック ルールでは元の宛先ポートのみを指定できることに注意してください。スタティック ルールの場合、変換後の宛先ポートを定義できますが、元の宛先ポート オブジェクトまたはリテラル値と同じプロトコルを持つオブジェクトでのみ可能です。

システムは宛先ポートを、スタティック ルールの元の宛先ポート リスト内のポート オブジェクトまたはリテラル ポートの値、またはダイナミック ルールの複数の値と照合します。

スタティック NAT ルールは 1 対 1 変換であるため、[Available Ports] リストには単一のポートのみを含むポート オブジェクトおよびグループのみが含まれます。スタティック変換用に、単一のオブジェクトまたはリテラル値のみを [Original Port] リストと [Translated Port] リストの両方に追加できます。

ダイナミック ルールの場合は、ポートの範囲を追加できます。たとえば、元の宛先ポートを指定する場合、リテラル値として `1000-1100` を追加できます。

⚠

注意 ポート オブジェクトまたはオブジェクト グループが NAT ルールで使用されている場合に、オブジェクトまたはグループを変更または削除すると、ルールが無効になる可能性があります。

NAT ルールに、次の種類のポート条件を追加できます。

- オブジェクト マネージャを使って作成した個別およびグループのポート オブジェクト
- 宛先ポート条件のページから追加し、ユーザのルールと他の既存および将来のルールに追加可能な個別のポート オブジェクト
- TCP、UDP、またはすべて（TCPおよびUDP）の転送プロトコルとポートから構成されるリテラル ポート値

NAT ルールへのポートの条件の追加

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
該当なし	Control	7000 & 8000 シリーズ	任意（Any）	Admin/Network Admin

ステップ 1 **[Devices]** > **[NAT]** を選択します。

ステップ 2 変更する NAT ポリシーの横にある編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 [ルールの追加（Add Rule）] をクリックします。

ステップ 4 ルールの [名前（Name）] を入力します。

ステップ 5 ルールの [タイプ（Type）] を指定します。

ステップ 6 [宛先ポート（Destination Port）] タブをクリックします。

ステップ 7 必要に応じて、[使用可能なポート（Available Ports）] リストの上にある追加アイコン（）をクリックし、リストに個別のポートオブジェクトを追加します。

追加する各ポート オブジェクトの 1 つのポートまたはポート範囲を指定できます。その後、ルールの条件として追加するオブジェクトを選択できます。スタティック ルールの場合、単一のポートを持つポート オブジェクトのみを使用できます。

ステップ 8 [使用可能なポート（Available Ports）] リスト内の条件をクリックします。

ステップ 9 次の選択肢があります。

- [元に追加（Add to Original）] をクリックします。
- [変換後に追加（Add to Translated）] をクリックします。
- 使用可能なポートをリストにドラッグ アンド ドロップします。

ステップ 10 リテラルポートを追加するには、次の手順を実行します。

a) [元のポート（Original Port）] または [変換後のポート（Translated Port）] リストの下にある [プロトコル（Protocol）] ドロップダウンリストからエントリを選択します。

b) ポートを入力します。

c) [追加（Add）] をクリックします。

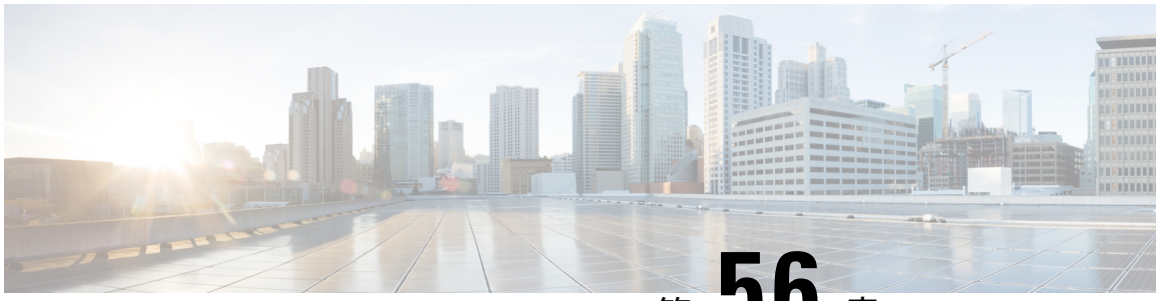
ダイナミック ルールの場合、単一のポートまたは範囲を指定できます。

ステップ 11 [追加（Add）] をクリックします。

ステップ 12 [保存（Save）] をクリックし、ポリシーの変更内容を保存します。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。



第 56 章

Firepower Threat Defense 用のネットワークアドレス変換（NAT）

ここでは、ネットワーク アドレス変換（NAT）について、および Firepower Threat Defense デバイスでそれを設定する方法について説明します。

NAT を使用する理由

IP ネットワーク内の各コンピュータおよびデバイスには、ホストを識別する固有の IP アドレスが割り当てられています。パブリック IPv4 アドレスが不足しているため、これらの IP アドレスの大部分はプライベートであり、プライベートの企業ネットワークの外部にルーティングできません。RFC 1918 では、アドバタイズされない、内部で使用できるプライベート IP アドレスが次のように定義されています。

- 10.0.0.0 ～ 10.255.255.255
- 172.16.0.0 ～ 172.31.255.255
- 192.168.0.0 ～ 192.168.255.255

NAT の主な機能の 1 つは、プライベート IP ネットワークがインターネットに接続できるようにすることです。NAT は、プライベート IP アドレスをパブリック IP に置き換え、内部プライベート ネットワーク内のプライベート アドレスをパブリック インターネットで使用可能な正式の、ルーティング可能なアドレスに変換します。このようにして、NAT はパブリック アド

レスを節約します。これは、ネットワーク全体に対して1つのパブリック アドレスだけを外部に最小限にアドバタイズするように NAT を設定できるからです。

NAT の他の機能には、次のおりです。

- セキュリティ：内部アドレスを隠蔽し、直接攻撃を防止します。
- IP ルーティング ソリューション：NAT を使用する際は、重複 IP アドレスが問題になりません。
- 柔軟性：外部で使用可能なパブリック アドレスに影響を与えずに、内部 IP アドレッシング スキームを変更できます。たとえば、インターネットにアクセス可能なサーバの場合、インターネット用に固定 IP アドレスを維持できますが、内部的にはサーバのアドレスを変更できます。
- IPv4 と IPv6（ルーテッド モードのみ）の間の変換：IPv4 ネットワークに IPv6 ネットワークを接続する場合は、NAT を使用すると、2 つのタイプのアドレス間で変換を行うことができます。

（注） NAT は必須ではありません。特定のトラフィック セットに NAT を設定しない場合、そのトラフィックは変換されませんが、セキュリティ ポリシーはすべて通常どおりに適用されます。

NAT の基本

ここでは、NAT の基本について説明します。

NAT の用語

このマニュアルでは、次の用語を使用しています。

- 実際のアドレス/ホスト/ネットワーク/インターフェイス：実際のアドレスとは、ホストで定義されている、変換前のアドレスです。内部ネットワークが外部にアクセスするときに内部ネットワークを変換するという典型的な NAT のシナリオでは、内部ネットワークが「実際の」ネットワークになります。内部ネットワークだけでなく、デバイスに接続されている任意のネットワークに変換できることに注意してください。したがって、外部アドレスを変換するように NAT を設定した場合、「実際の」は、外部ネットワークが内部ネットワークにアクセスしたときの外部ネットワークを指します。
- マッピング アドレス/ホスト/ネットワーク/インターフェイス：マッピング アドレスとは、実際のアドレスが変換されるアドレスです。内部ネットワークが外部にアクセスするときに内部ネットワークを変換するという典型的な NAT のシナリオでは、外部ネットワークが「マッピング」ネットワークになります。

（注） アドレスの変換中、デバイス インターフェイスに設定された IP アドレスは変換されません。

- 双方向の開始：スタティック NAT では、双方向に接続を開始できます。つまり、ホストへの接続とホストからの接続の両方を開始できます。
- 送信元および宛先の NAT：任意のパケットについて、送信元 IP アドレスと宛先 IP アドレスの両方を NAT ルールと比較し、1 つまたは両方を変換する、または変換しないことができます。スタティック NAT の場合、ルールは双方向であるため、たとえば、特定の接続が「宛先」アドレスから発生する場合でも、このガイドを通じてのコマンドおよび説明では「送信元」および「宛先」が使用されていることに注意してください。

NAT タイプ

NAT は、次の方法を使用して実装できます。

- ダイナミック NAT：実際の IP アドレスのグループが、（通常は、より小さい）マッピング IP アドレスのグループに先着順でマッピングされます。実際のホストだけがトラフィックを開始できます。ダイナミック NAT （1470 ページ）を参照してください。
- ダイナミック ポート アドレス変換（PAT）：実際の IP アドレスのグループが、1 つの IP アドレスにマッピングされます。この IP アドレスのポートが使用されます。ダイナミック PAT （1476 ページ）を参照してください。
- スタティック NAT：実際の IP アドレスとマッピング IP アドレスとの間での一貫したマッピング。双方向にトラフィックを開始できます。スタティック NAT （1485 ページ）を参照してください。
- アイデンティティ NAT：実際のアドレスが同一アドレスにスタティックに変換され、基本的に NAT をバイパスします。大規模なアドレスのグループを変換するものの、小さいアドレスのサブセットは免除する場合は、NAT をこの方法で設定できます。アイデンティティ NAT （1496 ページ）を参照してください。

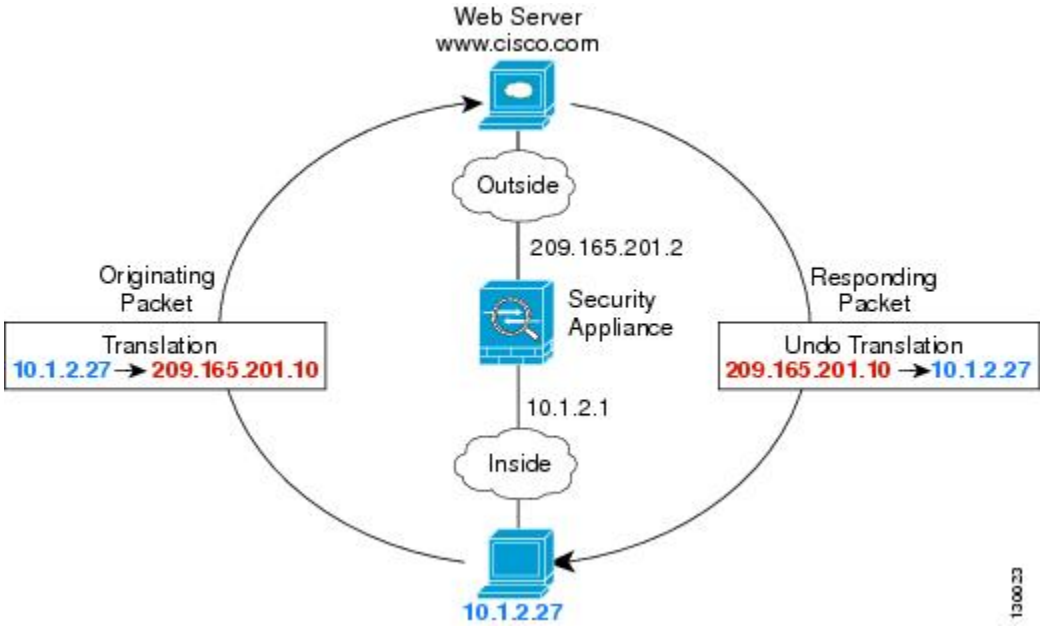
ルーテッド モードとトランスペアレント モードの NAT

NAT は、ルーテッド モードおよびトランスペアレント ファイアウォール モードの両方に設定できます。インライン、インライン タップ、またはパッシブ モードで動作するインターフェイスに対しては NAT を設定できません。次の項では、各ファイアウォール モードの一般的な使用方法について説明します。

ルーテッド モードの NAT

次の図は、内部にプライベート ネットワークを持つ、ルーテッド モードの一般的な NAT の例を示しています。

図 *32 : NAT* の例：ルーテッド モード



1. 内部ホスト 10.1.2.27 が Web サーバにパケットを送信すると、パケットの実際の送信元アドレス 10.1.2.27 はマッピング アドレス 209.165.201.10 に変換されます。
2. 応答時、サーバはマッピング アドレス 209.165.201.10 に応答を送信します。Firepower Threat Defense デバイス はプロキシ ARP を実行してパケットを要求するため、Firepower Threat Defense デバイス がパケットを受信します。
3. Firepower Threat Defense デバイス はその後、パケットをホストに送信する前に、マッピング アドレス 209.165.201.10 を変換し、実際のアドレス 10.1.2.27 に戻します。

トランスペアレント モードまたはブリッジ グループ内の NAT

NAT をトランスペアレント モードで使用すると、ネットワークで NAT を実行するためのアップストリーム ルータまたはダウンストリーム ルータが必要なくなります。これによりルーテッド モードでブリッジ グループ内で同様の機能を実行できます。

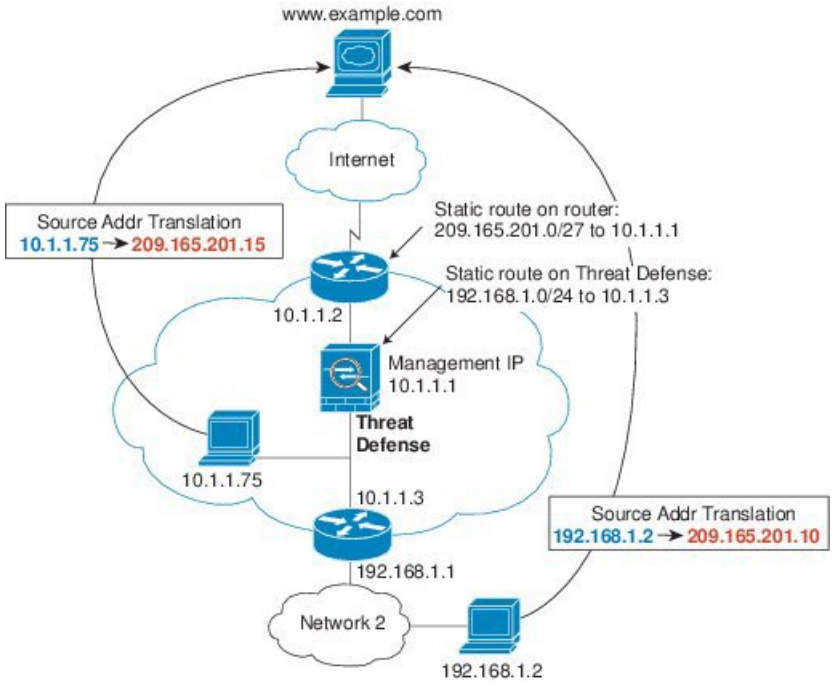
トランスペアレント モードまたは同じブリッジ グループのメンバー間のルーテッド モードの NAT には、以下の要件および制限があります。

- インターフェイスに接続されている IP アドレスがないため、マッピングされたアドレスがブリッジ グループ メンバーのインターフェイスである場合、インターフェイス PAT を設定することはできません。
- ARP インスペクションはサポートされていません。また、何らかの理由で、一方の Firepower Threat Defense デバイスのホストがもう一方の Firepower Threat Defense デバイスのホストに ARP 要求を送信し、開始ホストの実際のアドレスが同じサブネットの別のアドレスにマッピングされる場合、実際のアドレスは ARP 要求で可視のままになります。

- IPv4 および IPv6 ネットワークの間の変換はサポートされていません。2 つの IPv6 ネットワーク間、または 2 つの IPv4 ネットワーク間の変換がサポートされます。

次の図に、インターフェイス内部と外部に同じネットワークを持つ、トランスペアレントモードの一般的なNATのシナリオを示します。このシナリオのトランスペアレントファイアウォールは NAT サービスを実行しているため、アップストリーム ルータは NAT を実行する必要がありません。

図 *33 : NAT* の例：トランスペアレント モード



1. 内部ホスト 10.1.1.75 が Web サーバにパケットを送信すると、パケットの実際の送信元アドレス 10.1.1.75 はマッピング アドレス 209.165.201.15 に変更されます。
2. サーバが応答すると、マッピング アドレス 209.165.201.15 に応答を送信し、Firepower Threat Defense デバイス がそのパケットを受信します。これは、アップストリーム ルータには、Firepower Threat Defense デバイス の管理 IP アドレスに転送されるスタティック ルートのこのマッピング ネットワークが含まれるためです。
3. その後、Firepower Threat Defense デバイスはマッピング アドレス 209.165.201.15 を変換して実際のアドレス 10.1.1.1.75 に戻します。実際のアドレスは直接接続されているため、Firepower Threat Defense デバイスはそのアドレスを直接ホストに送信します。
4. ホスト 192.168.1.2 の場合も、リターン トラフィックを除き、同じプロセスが発生します。Firepower Threat Defense デバイス はルーティング テーブルでルートを検索し、192.168.1.0/24 の Firepower Threat Defense デバイス スタティック ルートに基づいてパケットを 10.1.1.3 にあるダウンストリーム ルータに送信します。

自動 NAT および 手動 NAT

自動 *NAT* および 手動 *NAT* という 2 種類の方法でアドレス変換を実装できます。

手動 NAT の追加機能を必要としない場合は、自動 NAT を使用することをお勧めします。自動 NAT の設定が容易で、Voice over IP（VoIP）などのアプリケーションでは信頼性が高い場合があります（VoIP では、ルールで使用されているオブジェクトのいずれにも属さない間接アドレスの変換が失敗することがあります）。

自動 NAT

ネットワーク オブジェクトのパラメータとして設定されているすべての NAT ルールは、自動 *NAT* ルールと見なされます。これは、ネットワーク オブジェクトに NAT を設定するための迅速かつ簡単な方法です。しかし、グループ オブジェクトに対してこれらのルールを作成することはできません。

これらのルールはオブジェクト自体の一部として設定されますが、オブジェクト マネージャを通してオブジェクト定義内の NAT 設定を確認することはできません。

パケットがインターフェイスに入ると、送信元 IP アドレスと宛先 IP アドレスの両方が 自動 NAT ルールと照合されます。個別の照合が行われる場合、パケット内の送信元 IP アドレスと宛先 IP アドレスは、個別のルールによって変換できます。これらのルールは、相互に結び付けられていません。トラフィックに応じて、異なる組み合わせのルールを使用できます。

ルールがペアになることはないため、sourceA/destinationA で sourceA/destinationB とは別の変換が行われるように指定することはできません。この種の機能には、手動 NAT を使用することで、1 つのルールで送信元アドレスおよび宛先アドレスを識別できます。

手動 NAT

手動 NAT では、1 つのルールで送信元アドレスおよび宛先アドレスの両方を識別できます。送信元アドレスと宛先アドレスの両方を指定すると、sourceA/destinationA で sourceA/destinationB とは別の変換が行われるように指定できます。

（注） スタティック NAT の場合、ルールは双方向であるため、たとえば、特定の接続が「宛先」アドレスから発生する場合でも、このガイドを通じてのコマンドおよび説明では「送信元」および「宛先」が使用されていることに注意してください。たとえば、ポートアドレス変換を使用するスタティック NAT を設定し、送信元アドレスを Telnet サーバとして指定する場合に、Telnet サーバに向かうすべてのトラフィックのポートを 2323 から 23 に変換するには、変換する送信元ポート（実際：23、マッピング：2323）を指定する必要があります。Telnet サーバアドレスを送信元アドレスとして指定しているため、その送信元ポートを指定します。

宛先アドレスはオプションです。宛先アドレスを指定する場合、宛先アドレスを自身にマッピングするか（アイデンティティ NAT）、別のアドレスにマッピングできます。宛先マッピングは、常にスタティック マッピングです。

自動 NAT と 手動 NAT の比較

これら 2 つの NAT タイプの主な違いは、次のとおりです。

- 実際のアドレスの定義方法
  - 自動 NAT：NAT ルールは、ネットワーク オブジェクトのパラメータとなります。ネットワーク オブジェクトの IP アドレスは元の（実際の）アドレスとして機能します。
  - 手動 NAT：実際のアドレスとマッピングアドレスの両方のネットワークオブジェクトまたはネットワーク オブジェクト グループを識別します。この場合、NAT はネットワーク オブジェクトのパラメータではありません。ネットワーク オブジェクトまたはグループが、NAT コンフィギュレーションのパラメータです。実際のアドレスのネットワーク オブジェクト グループを使用できることは、手動 NAT がよりスケーラブルであることを意味します。
- 送信元および宛先 NAT の実装方法
  - 自動 NAT：各ルールは、パケットの送信元または宛先のいずれかに適用できます。このため、送信元 IP アドレス、宛先 IP アドレスにそれぞれ 1 つずつ、計 2 つのルールが使用される場合もあります。このような 2 つのルールを 1 つに結合し、送信元/宛先ペアに対して特定の変換を強制することはできません。
  - 手動 NAT：1 つのルールで送信元と宛先の両方を変換します。パケットは 1 つのルールにのみ一致し、それ以上のルールはチェックされません。オプションの宛先アドレスを設定しない場合でも、マッチングするパケットは 1 つの 手動 NAT ルールだけに一致します。送信元および宛先は相互に結び付けられるため、送信元と宛先の組み合わせに応じて、異なる変換を適用できます。たとえば、sourceA/destinationA には、sourceA/destinationB とは異なる変換を設定できます。
- NAT ルールの順序。
  - 自動 NAT：NAT テーブルで自動的に順序付けされます。
  - 手動 NAT：NAT テーブルで手動で順序付けします（自動 NAT ルールの前または後）。

NAT ルールの順序

自動 NAT および 手動 NAT ルールは、3 つのセクションに分かれた単一のテーブルに保存されます。最初にセクション 1 のルール、次にセクション 2、最後にセクション 3 というように、一致が見つかるまで順番に適用されます。たとえば、セクション 1 で一致が見つかった場合、セクション 2 とセクション 3 は評価されません。次の表に、各セクション内のルールの順序を示します。

表 *102 : NAT* ルール テーブル

テーブルのセクション	ルール タイプ	セクション内のルールの順序
セクション 1	手動 NAT	コンフィギュレーションに登場する順に、最初の一致ベースで適用されます。最初の一致が適用されるため、一般的なルールの前に固有のルールが来るようにする必要があります。そうしない場合、固有のルールを期待どおりに適用できない可能性があります。デフォルトでは、手動 NAT ルールはセクション 1 に追加されます。
セクション 2	自動 NAT	セクション 1 で一致が見つからない場合、セクション 2 のルールが次の順序で適用されます。 **1.** スタティック ルール **2.** ダイナミック ルール **各ルールタイプでは、次の順序ガイドラインが使用されます。** **1.** 実際の IP アドレスの数量：小から大の順。たとえば、アドレスが 1 個のオブジェクトは、アドレスが 10 個のオブジェクトよりも先に評価されます。 **2.** 数量が同じ場合には、アドレス番号（低から高の順）が使用されます。たとえば、10.1.1.0 は、11.1.1.0 よりも先に評価されます。 **3.** 同じ IP アドレスが使用される場合、ネットワーク オブジェクトの名前がアルファベット順で使用されます。たとえば、abracadabra は catwoman よりも先に評価されます。
セクション 3	手動 NAT	まだ一致が見つからない場合、セクション 3 のルールがコンフィギュレーションに登場する順に、最初の一致ベースで適用されます。このセクションには、最も一般的なルールを含める必要があります。このセクションにおいても、一般的なルールの前に固有のルールが来るようにする必要があります。そうしない場合、一般的なルールが適用されます。

たとえばセクション 2 のルールでは、ネットワーク オブジェクト内に定義されている次の IP アドレスがあるとします。

- 192.168.1.0/24（スタティック）
- 192.168.1.0/24（ダイナミック）

- 10.1.1.0/24（スタティック）
- 192.168.1.1/32（ダイナミック）
- 172.16.1.0/24（ダイナミック）（オブジェクト def）
- 172.16.1.0/24（ダイナミック）（オブジェクト abc）

この結果、使用される順序は次のとおりです。

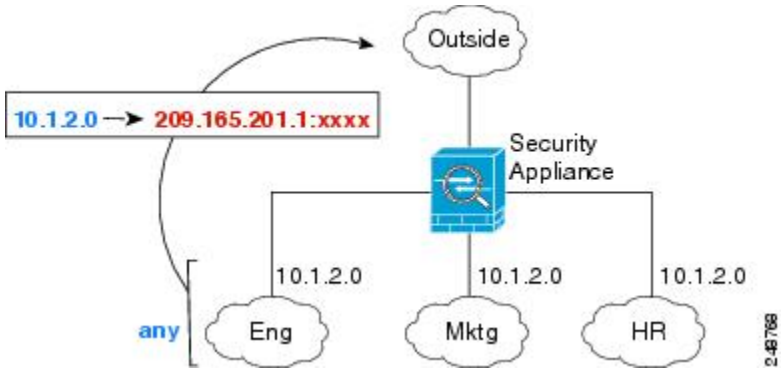
- 192.168.1.1/32（ダイナミック）
- 10.1.1.0/24（スタティック）
- 192.168.1.0/24（スタティック）
- 172.16.1.0/24（ダイナミック）（オブジェクト abc）
- 172.16.1.0/24（ダイナミック）（オブジェクト def）
- 192.168.1.0/24（ダイナミック）

NAT インターフェイス

ブリッジ グループ メンバーのインターフェイスを除き、任意のインターフェイス（つまり、すべてのインターフェイス）に適用できるように NAT ルールを設定することも、特定の実際のインターフェイスおよびマッピングインターフェイスを識別することもできます。実際のアドレスには任意のインターフェイスを指定できます。マッピングインターフェイスには特定のインターフェイスを指定できます。または、その逆も可能です。

たとえば、複数のインターフェイスで同じプライベートアドレスを使用し、外部へのアクセス時にはすべてのインターフェイスを同じグローバルプールに変換する場合、実際のアドレスに任意のインターフェイスを指定し、マッピング アドレスには outside インターフェイスを指定します。

図 *34 :* 任意のインターフェイスの指定



ただし、「任意の」インターフェイスの概念は、ブリッジ グループ メンバーのインターフェイスには適用されません。「任意の」インターフェイスを指定すると、すべてのブリッジ グ

ループ メンバーのインターフェイスは除外されます。したがって、ブリッジグループ メンバーにNATを適用するには、メンバーのインターフェイスを指定する必要があります。これでは、1 つのインターフェイスのみが異なる多くの類似するルールが発生する可能性があります。ブリッジ仮想インターフェイス（BVI）自体に NAT を設定することはできませんが、メンバーのインターフェイスのみに NAT を設定することはできます。

（注） インライン、インライン タップ、またはパッシブ モードで動作するインターフェイスに対しては NAT を設定できません。インターフェイスの指定は、インターフェイスを含むインターフェイス オブジェクトを選択することによって間接的に行います。

NAT のルーティング設定

FTDデバイスは、変換された（マッピング）アドレスに送信されるパケットの宛先である必要があります。

パケットを送信する際の出力インターフェイスの決定に、指定した場合はその宛先インターフェイスが使用され、指定していない場合はルーティング テーブル ルックアップが使用されます。アイデンティティNATの場合は、宛先インターフェイスを指定している場合でも、ルート ルックアップの使用を選択できます。

必要となるルーティング設定のタイプは、マッピングアドレスのタイプによって異なります。以下の各トピックでは、その詳細について説明します。

マッピング インターフェイスと同じネットワーク上のアドレス

宛先（マッピング）インターフェイスと同じネットワーク上のアドレスを使用する場合、Firepower Threat Defense デバイス はプロキシ ARP を使用してマッピング アドレスの ARP 要求に応答し、マッピングアドレス宛てのトラフィックを代行受信します。この方法では、Firepower Threat Defense デバイスがその他のネットワークのゲートウェイである必要がないため、ルーティングが簡略化されます。このソリューションは、外部ネットワークに十分な数のフリーアドレスが含まれている場合に最も適しており、ダイナミック NAT またはスタティック NAT などの 1:1 変換を使用している場合は考慮が必要です。ダイナミック PAT ではアドレス数が少なくても使用できる変換の数が大幅に拡張されるので、外部ネットワークで使用できるアドレスが少ししかない場合でも、この方法を使用できます。PAT では、マッピング インターフェイスの IP アドレスも使用できます。

（注） マッピング インターフェイスを任意のインターフェイスとして設定し、マッピング インターフェイスの1つとして同じネットワーク上のマッピングアドレスを指定すると、そのマッピング アドレスの ARP 要求を別のインターフェイスで受信する場合、入力インターフェイスでそのネットワークのARPエントリを手動で設定し、そのMACアドレスを指定する必要があります。通常、マッピング インターフェイスに任意のインターフェイスを指定して、マッピングアドレスの固有のネットワークを使用すると、この状況は発生しません。入力インターフェイスの [Advanced] 設定で、ARP テーブルを設定します。

固有のネットワーク上のアドレス

宛先（マッピングされた）インターフェイスネットワークで使用可能なアドレスより多くのアドレスが必要な場合は、別のサブネット上のアドレスを識別できます。アップストリームルータには、Firepower Threat Defense デバイスをポイントするマッピングアドレスのスタティックルートが必要です。

また、ルーテッドモードの場合、宛先ネットワーク上の IP アドレスをゲートウェイとして使用して、マッピングアドレスの Firepower Threat Defense デバイスにスタティックルートを設定し、ルーティングプロトコルを使用してルートを再配布することができます。たとえば、内部ネットワーク（10.1.1.0/24）に NAT を使用し、マッピング IP アドレス 209.165.201.5 を使用する場合は、209.165.201.5 255.255.255.255（ホストアドレス）のスタティックルートを再配布可能な 10.1.1.99 ゲートウェイに設定できます。

トランスペアレントモードの場合は、実際のホストが直接接続されてる場合は、Firepower Threat Defense デバイスをポイントするようにアップストリームルータのスタティックルートを設定します。ブリッジグループの IP アドレスを指定します。トランスペアレントモードのリモートホストの場合、アップストリームルータのスタティックルートで代わりにダウンストリームルータの IP アドレスを指定できます。

実際のアドレスと同じアドレス（アイデンティティ NAT）

アイデンティティ NAT のデフォルト動作で、プロキシ ARP はイネーブルにされ、他のスタティック NAT ルールと一致します。必要に応じてプロキシ ARP をディセーブルにできます。必要に応じて標準スタティック NAT のプロキシ ARP をディセーブルにできます。その場合は、アップストリームルータの適切なルートがあることを確認する必要があります。

アイデンティティ NAT の場合、通常はプロキシ ARP が不要で、場合によっては接続性に関する問題を引き起こす可能性があります。たとえば、任意の IP アドレスの広範なアイデンティティ NAT ルールを設定した場合、プロキシ ARP をイネーブルのままにしておくと、マッピングインターフェイスに直接接続されたネットワーク上のホストの問題を引き起こすことがあります。この場合、マッピングネットワークのホストが同じネットワークの他のホストと通信すると、ARP 要求内のアドレスは（任意のアドレスと一致する）NAT ルールと一致します。このとき、実際には Firepower Threat Defense デバイス向けのパケットでない場合でも、Firepower Threat Defense デバイスはこのアドレスの ARP をプロキシします。（この問題は、手動 NAT ルールが設定されている場合にも発生します。NAT ルールは送信元と宛先のアドレス両方に一致する必要がありますが、プロキシ ARP 判定は「送信元」アドレスに対してのみ行われます）。実際のホストの ARP 応答の前に Firepower Threat Defense デバイスの ARP 応答を受信した場合、トラフィックは誤って Firepower Threat Defense デバイスに送信されます。

NAT のガイドライン

ここでは、NAT を実装するためのガイドラインについて詳細に説明します。

NAT のファイアウォール モードのガイドライン

NAT は、ルーテッド モードとトランスペアレント ファイアウォール モードでサポートされています。

ただし、ブリッジ グループ メンバーのインターフェイス（ブリッジ グループ仮想インターフェイスの一部であるインターフェイス、BVI）での NAT 設定には次の制限があります。

- ブリッジ グループのメンバーの NAT を設定するには、メンバー インターフェイスを指定します。ブリッジ グループ インターフェイス（BVI）の NAT 自体を設定することはできません。
- ブリッジ グループ メンバーのインターフェイス間で NAT を実行するときには、実際のおよびマッピングされたアドレスを指定する必要があります。インターフェイスとして「任意」を指定することはできません。
- インターフェイスに接続されている IP アドレスがないため、マッピングされたアドレスがブリッジ グループ メンバーのインターフェイスである場合、インターフェイス PAT を設定することはできません。
- 送信元と宛先インターフェイスが同じブリッジ グループのメンバーである場合、IPv4 と IPv6 ネットワーク間の変換はできません（NAT64/46）。スタティック NAT/PAT 44/66、ダイナミック NAT44/66 およびダイナミック PAT44 だけが許可される方法であり、ダイナミック PAT66 はサポートされません。ただし、さまざまなブリッジ グループのメンバー間、またはブリッジ グループ メンバー（送信元）と標準ルーテッド インターフェイス（宛先）間では NAT64/46 を実行できます。

（注） インライン、インライン タップ、またはパッシブ モードで動作するインターフェイスに対しては NAT を設定できません。

IPv6 NAT のガイドライン

NAT では、IPv6 のサポートに次のガイドラインと制約が伴います。

- ルーテッド モード インターフェイスの場合は、IPv4 と IPv6 との間の変換もできます。
- 同じブリッジ グループのメンバーであるインターフェイスでは IPv4 と IPv6 の間の変換はできません。2 つの IPv6 または 2 つの IPv4 ネットワーク間でのみ変換できます。この制限は、インターフェイスが異なるブリッジ グループのメンバーである場合、またはブリッジ グループのメンバーと標準的なルーテッド インターフェイスの間には該当しません。
- 同じブリッジ グループのインターフェイス間で変換するときは、IPv6 のダイナミック PAT（NAT66）を使用できません。この制限は、インターフェイスが異なるブリッジ グループのメンバーである場合、またはブリッジ グループのメンバーと標準的なルーテッド インターフェイスの間には該当しません。

- スタティック NAT の場合は、/64 までの IPv6 サブネットを指定できます。これよりも大きいサブネットはサポートされません。
- FTP を NAT46 とともに使用する場合は、IPv4 FTP クライアントが IPv6 FTP サーバに接続するときに、クライアントは拡張パッシブ モード（EPSV）または拡張ポート モード（EPRT）を使用する必要があります。PASV コマンドおよび PORT コマンドは IPv6 ではサポートされません。

IPv6 NAT のベスト プラクティス

NAT を使用すると、IPv6 ネットワーク間、さらに IPv4 および IPv6 ネットワークの間で変換できます（ルーテッド モードのみ）。次のベスト プラクティスを推奨します。

- NAT66（IPv6-to-IPv6）：スタティック NAT を使用することを推奨します。ダイナミック NAT または PAT を使用できますが、IPv6 アドレスは大量にあるため、ダイナミック NAT を使用する必要がありません。リターントラフィックを許可しない場合は、スタティック NAT ルールを単一方向にできます（手動 NAT のみ）。
- NAT46（IPv4-to-IPv6）：スタティック NAT を使用することを推奨します。IPv6 アドレス空間は IPv4 アドレス空間よりもかなり大きいので、容易にスタティック変換に対応できます。リターントラフィックを許可しない場合は、スタティック NAT ルールを単一方向にできます（手動 NAT のみ）。IPv6 サブネットに変換する場合（/96 以下）、結果のマッピング アドレスはデフォルトで IPv4 埋め込み IPv6 アドレスとなります。このアドレスでは、IPv4 アドレスの 32 ビットが IPv6 プレフィックスの後に埋め込まれています。たとえば、IPv6 プレフィックスが /96 プレフィックスの場合、IPv4 アドレスは、アドレスの最後の 32 ビットに追加されます。たとえば、201b::0/96 に 192.168.1.0/24 をマッピングする場合、192.168.1.4 は 201b::0.192.168.1.4 にマッピングされます（混合表記で表示）。/64 など、より小さいプレフィックスの場合、IPv4 アドレスがプレフィックスの後に追加され、サフィックスの 0s が IPv4 アドレスの後に追加されます。また、任意で、ネット間のアドレスを変換できます。この場合、最初の IPv6 アドレスに最初の IPv4 アドレス、2 番目 IPv6 アドレスに 2 番目の IPv4 アドレス、のようにマッピングします。
- NAT64（IPv6-to-IPv4）：IPv6 アドレスの数に対応できる十分な数の IPv4 アドレスがない場合があります。大量の IPv4 変換を提供するためにダイナミック PAT プールを使用することを推奨します。

検査対象プロトコルに対する NAT サポート

セカンダリ接続を開くアプリケーション層プロトコルの一部、またはパケットに IP アドレスを埋め込んだアプリケーション層プロトコルの一部は、次のサービスを提供するために検査されます。

- ピンホールの作成：一部のアプリケーション プロトコルは、標準ポートまたはネゴシエートされたポートでセカンダリ TCP または UDP 接続を開きます。インスペクションでは、これらのセカンダリ ポートのピンホールが開くので、ユーザはそれらを許可するアクセス制御ルールを作成する必要はありません。

- NATの書き換え：プロトコルの一部としてのパケットデータ内のセカンダリ接続用のFTP埋め込み型 IP アドレスおよびポートなどのプロトコル。エンドポイントのいずれかに関与する NAT 変換がある場合、インスペクション エンジンは、埋め込まれたアドレスおよびポートの NAT 変換を反映するようにパケット データを書き換えます。セカンダリ接続は NAT の書き換えがないと動作しません。
- プロトコルの強制：一部のインスペクションでは、検査対象プロトコルにある程度のRFCへの準拠が強制されます。

次の表に、NAT の書き換えと NAT の制限事項を適用する検査対象プロトコルを示します。これらのプロトコルを含む NAT ルールの作成時は、これらの制限事項に留意してください。ここに記載されていない検査対象プロトコルは NAT の書き換えを適用しません。これらのインスペクションには、GTP、HTTP、IMAP、POP、SMTP、SSH、および SSL が含まれます。

（注） NAT の書き換えは、リストされているポートでのみサポートされます。これらのプロトコルの一部では、ネットワーク解析ポリシーを使用してインスペクションを他のポートに拡張できますが、NAT の書き換えはこれらのポートに拡張されません。これには、DCERPC、DNS、FTP、および Sun RPC インスペクションが含まれます。非標準ポートでこれらのプロトコルを使用する場合は、接続で NAT を使用しないでください。

表 *103 : NAT* のサポート対象アプリケーション インスペクション

アプリケーション	検査対象プロトコル、ポート	NAT に関する制限事項	作成済みのピンホール
DCERPC	TCP/135	NAT64 なし	Yes
DNS over UDP	UDP/53	NAT サポートは、WINS 経由の名前解決では使用できません。	なし
ESMTP	TCP/25	NAT64 なし	No
FTP	TCP/21	制限なし。 （クラスタリング）スタティック PAT はサポートされません。	○
H.323 H.225（コールシグナリング） H.323 RAS	TCP/1720 UDP/1718 RAS の場合、UDP/1718 ～ 1719	（クラスタリング）スタティック PAT なし。 拡張 PAT はサポートされません。 NAT64 なし。	Yes

アプリケーション	検査対象プロトコル、ポート	NAT に関する制限事項	作成済みのピンホール
ICMP ICMP Error	ICMP （デバイス インターフェイスに送信される ICMP トラフィックは検査されません。）	制限なし。	No
IP オプション	RSVP	NAT64 なし。	No
NetBIOS Name Server over IP	UDP/137、138（送信元ポート）	拡張 PAT はサポートされません。 NAT64 なし	No
RSH	TCP/514	PAT はサポートされません。 NAT64 なし。 （クラスタリング）スタティック PAT なし。	○
RTSP	TCP/554 （HTTP クローキングは処理しません。）	拡張 PAT はサポートされません。 NAT64 なし。 （クラスタリング）スタティック PAT なし。	○
SIP	TCP/5060 UDP/5060	拡張 PAT はサポートされません。 NAT64 または NAT46 はなし。 （クラスタリング）スタティック PAT なし。	○
Skinny（SCCP）	TCP/2000	拡張 PAT はサポートされません。 NAT64、NAT46、または NAT66 はなし。 （クラスタリング）スタティック PAT なし。	○
SQL*Net （バージョン 1、2）	TCP/1521	拡張 PAT はサポートされません。 NAT64 なし。 （クラスタリング）スタティック PAT なし。	○
Sun RPC	TCP/111 UDP/111	拡張 PAT はサポートされません。 NAT64 なし	Yes
TFTP	UDP/69	NAT64 なし。 （クラスタリング）スタティック PAT はサポートされません。 ペイロード IP アドレスは変換されません。	Yes

アプリケーション	検査対象プロトコル、ポート	NAT に関する制限事項	作成済みのピンホール
XDMCP	UDP/177	拡張 PAT はサポートされません。 NAT64 なし。 （クラスタリング）スタティック PAT なし。	対応

NAT のその他のガイドライン

- ブリッジグループのメンバーであるインターフェイスでは、メンバーのインターフェイスに NAT ルールを記述します。ブリッジ仮想インターフェイス（BVI）自体に NAT ルールを記述することはできません。
- （自動 NAT のみ）。特定のオブジェクトに対して 1 つの NAT ルールだけを定義できます。オブジェクトに対して複数の NAT ルールを設定する場合は、同じ IP アドレスを指定する異なる名前の複数のオブジェクトを作成する必要があります。
- VPN がインターフェイスで定義されると、インターフェイスの着信 ESP トラフィックに NAT ルールは適用されません。システムでは確立された VPN トンネルの ESP トラフィックのみ許可され、既存のトンネルに関連付けられていないトラフィックは廃棄されます。この制約は ESP と UDP ポート 500 および 4500 に適用されます。
- ダイナミック PAT を適用するデバイスの背後のデバイス（VPN UDP ポート 500 と 4500 は実際に使用されるポートではない）でサイト間 VPN を定義した場合、PAT デバイスの背後にあるデバイスから接続を開始する必要があります。正しいポート番号がわからないため、レスポンダはセキュリティ アソシエーション（SA）を開始できません。
- NAT コンフィギュレーションを変更したときに、既存の変換がタイムアウトするまで待たずに新しい NAT コンフィギュレーションを使用できるようにするには、デバイス CLI で **clear xlate** コマンドを使用して変換テーブルを消去します。ただし、変換テーブルを消去すると、変換を使用している現在の接続がすべて切断されます。

（注） ダイナミック NAT または PAT ルールを削除し、次に削除したルールに含まれるアドレスと重複するマッピングアドレスを含む新しいルールを追加すると、新しいルールは、削除されたルールに関連付けられたすべての接続がタイムアウトするか **clear xlate** コマンドを使用してクリアされるまで使用されません。この予防手段のおかげで、同じアドレスが複数のホストに割り当てられないようにできます。

- 1 つのオブジェクト グループに IPv4 と IPv6 の両方のアドレスを入れることはできません。オブジェクト グループには、1 つのタイプのアドレスだけが含まれている必要があります。

- （手動 NATのみ）。NAT ルールで送信元アドレスとして **any** を使用する場合、「any」トラフィックの定義（IPv4 と IPv6）はルールによって異なります。Firepower Threat Defense デバイス がパケットに対して NAT を実行する前に、パケットが IPv6-to-IPv6 または IPv4-to-IPv4 である必要があります。この前提条件では、Firepower Threat Defense デバイスは、NAT ルールの **any** の値を決定できます。たとえば、「any」から IPv6 サーバへのルールを設定しており、このサーバが IPv4 アドレスからマップされている場合、**any** は「任意の IPv6 トラフィック」を意味します。「any」から「any」へのルールを設定しており、送信元をインターフェイス IPv4 アドレスにマッピングする場合、マッピングされたインターフェイス アドレスによって宛先も IPv4 であることが示されるため、**any** は「任意の IPv4 トラフィック」を意味します。
- 同じマッピング オブジェクトやグループを複数の NAT ルールで使用できます。
- マッピング IP アドレス プールは、次のアドレスを含むことができません。
  - マッピング インターフェイスの IP アドレス。ルールに「any」インターフェイスを指定すると、すべてのインターフェイスの IP アドレスが拒否されます。インターフェイス PAT（ルーテッド モードのみ）の場合は、インターフェイス アドレスの代わりにインターフェイス名を指定します。
  - フェールオーバー インターフェイスの IP アドレス。
  - （トランスペアレント モード）管理 IP アドレス。
  - （ダイナミック NAT）VPN がイネーブルの場合は、スタンバイ インターフェイスの IP アドレス。
- スタティックおよびダイナミック NAT ポリシーでは重複アドレスを使用しないでください。たとえば、重複アドレスを使用すると、PPTP のセカンダリ接続がダイナミック xlate ではなくスタティックにヒットした場合、PPTP 接続の確立に失敗する可能性があります。
- NAT ルールの送信元アドレスとリモート アクセス VPN アドレス プールの重複アドレスは使用できません。
- ルールで宛先インターフェイスを指定すると、ルーティング テーブルでルートが検索されるのではなく、そのインターフェイスが出力インターフェイスとして使用されます。ただし、アイデンティティ NAT の場合は、代わりにルート ルックアップを使用するオプションがあります。
- NAT はトラフィックを介してのみ適用されます。システムによって生成されたトラフィックは NAT の対象にはなりません。

脅威に対する防御のための NAT の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin Access Admin Network Admin

ネットワーク アドレス変換は非常に複雑な場合があります。変換の問題やトラブルシューティングが困難な状況を避けるため、ルールはできるだけシンプルにすることを推奨します。NAT を実装する前に注意深く計画することが重要です。次の手順では、基本的なアプローチを示します。

NAT ポリシーは、共有ポリシーです。同様の NAT ルールを持つべきデバイスに、ポリシーを割り当てます。

割り当てられたデバイスにポリシーの特定のルールが適用されるかどうかは、ルールで使用されるインターフェイス オブジェクト（セキュリティ ゾーンまたはインターフェイス グループ）によって決定されます。インターフェイス オブジェクトにデバイスのインターフェイスが 1 つ以上含まれている場合、ルールがデバイスに導入されます。したがって、注意深くインターフェイス オブジェクトを設計することで、単一の共有ポリシー内のデバイスのサブセットに適用されるルールを設定できます。「任意」のインターフェイス オブジェクトに適用されるルールは、すべてのデバイスに導入されます。

デバイスのグループにさまざまなルールが必要な場合は、複数の NAT ポリシーを設定できます。

ステップ 1 **[デバイス（Devices）] > [NAT]** を選択します。

- 新しいポリシーを作成するには、**[新しいポリシー（New Policy）] > [脅威防御 NAT（Threat Defense NAT）]** をクリックします。ポリシーに名前を付け、オプションでデバイスを割り当て、[保存（Save）] をクリックします。

  デバイスの割り当てを後で変更するには、ポリシーを編集して、[ポリシー割り当て（Policy Assignments）] リンクをクリックします。

- 既存の脅威防御 NAT ポリシーを編集するには、編集アイコン（  ）をクリックします。このページには、FTD では使用されない Firepower NAT ポリシーも表示されます。

ステップ 2 必要なルールを決定します。

ダイナミック NAT ルール、ダイナミック PAT ルール、スタティック NAT ルール、およびアイデンティティ NAT ルールを作成できます。概要については、「NAT タイプ（1451 ページ）」を参照してください。

ステップ 3 手動 NAT または自動 NAT として実装するルールを決定します。

これらの 2 つの実装オプションの比較については、自動 NAT および 手動 NAT （1454 ページ）を参照してください。

ステップ 4 デバイスごとにカスタマイズするルールを決定します。

複数のデバイスに 1 つの NAT ポリシーを割り当てることができるため、多くのデバイスに 1 つのルールを設定できます。ただし、各デバイスによって異なる解釈が必要なルールや、デバイスのサブセットにのみ適用すべきルールの場合もあります。

インターフェイス オブジェクトを使用して、ルールを設定するデバイスを制御します。次に、ネットワーク オブジェクトでオブジェクトのオーバーライドを使用して、デバイスごとに使用されるアドレスをカスタマイズします。

詳細については、複数のデバイスの NAT ルールのカスタマイズ （1468 ページ）を参照してください。

ステップ 5 次の項で説明するルールを作成します。

- ダイナミック NAT （1470 ページ）
- ダイナミック PAT （1476 ページ）
- スタティック NAT （1485 ページ）
- アイデンティティ NAT （1496 ページ）

ステップ 6 NAT ポリシーとルールを管理します。

ポリシーとそのルールを管理するには、次のことを行います。

- ポリシーの名前または説明を編集するには、これらのフィールドをクリックし、変更を入力して、フィールドの外側をクリックします。
- 特定のデバイスに適用されるルールのみを表示するには、[デバイスによるフィルタ（Filter by Device）] をクリックし、目的のデバイスを選択します。ルールがデバイスのインターフェイスを含むインターフェイス オブジェクトを使用している場合、そのデバイスにルールが適用されます。
- ポリシーが割り当てられているデバイスを変更するには、[ポリシー割り当て（Policy Assignments）] リンクをクリックし、必要に応じて選択したデバイス リストを変更します。
- ルールが有効であるか、または無効であるかを変更するには、ルールを右クリックし、[状態（State）] コマンドから目的のオプションを選択します。これらのコントロールを使用して、ルールを削除しないで一時的に無効にすることができます。
- ルールを編集するには、ルールの編集アイコン（  ）をクリックします。
- ルールを削除するには、ルールの [削除（delete）] アイコン（  ）をクリックします。

ステップ 7 **[Save（保存）]** をクリックします。

これで、[Deploy] をクリックして割り当てられているデバイスにポリシーを展開できます。変更はポリシーを導入するまで有効になりません。

複数のデバイスの NAT ルールのカスタマイズ

NAT ポリシーは共有されるため、複数のデバイスに特定のポリシーを割り当てることができます。ただし、指定したオブジェクトに設定できる自動 NAT ルールは 1 つまでです。そのため、変換を実行する特定のデバイスに基づいてオブジェクトにさまざまな変換を設定する場合は、インターフェイス オブジェクト（セキュリティ ゾーンまたはインターフェイス グループ）を注意深く設定し、変換済みアドレスのネットワーク オブジェクトのオーバーライドを定義する必要があります。

インターフェイス オブジェクトでは、ルールを設定するデバイスを決定します。ネットワーク オブジェクトのオーバーライドでは、そのオブジェクトの特定のデバイスで使用する IP アドレスを決定します。

次のような例が考えられます。

- FTD-A と FTD-B に、「inside」という名前のインターフェイスに接続される内部ネットワーク 192.168.1.0/24 があります。
- FTD-A では、「外部」インターフェイスに移動するときに、すべての 192.168.1.0/24 アドレスを 10.100.10.10 ～ 10.100.10.200 の範囲の NAT プールに変換する必要があります。
- FTD-B では、「外部」インターフェイスに移動するときに、すべての 192.168.1.0/24 アドレスを 10.200.10.10 ～ 10.200.10.200 の範囲の NAT プールに変換する必要があります。

このように変換するには、次の手順を実行します。この例のルールはダイナミック自動 NAT 用ですが、任意のタイプの NAT ルールにこのテクニックを一般化できます。

ステップ 1 内部インターフェイスと外部インターフェイスのセキュリティ ゾーンを作成します。

a) **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** を選択します。

b) コンテンツのテーブルから [インターフェイス オブジェクト（Interface Objects）] を選択し、**[追加（Add）]** > **[セキュリティ ゾーン（Security Zone）]** をクリックします。（ゾーンの代わりにインターフェイス グループを使用できます）。

c) 内部ゾーンのプロパティを設定します。

- [名前（Name）]：**inside-zone** などの名前を入力します。
- [タイプ（Type）]：ルーテッド モードのデバイスの場合は [ルーテッド（Routed）]、トランスペアレント モードの場合は [スイッチド（Switched）] を選択します。
- [選択したインターフェイス（Selected Interfaces）]：選択済みリストに FTD-A/内部および FTD-B/内部インターフェイスを追加します。

d) [保存（Save）] をクリックします。

e) **[追加（Add）]** > **[セキュリティ ゾーン（Security Zone）]** をクリックし、外部ゾーンのプロパティを定義します。

- [名前（Name）]：**outside-zone** などの名前を入力します。

- [タイプ（Type）]：ルーテッドモードのデバイスの場合は[ルーテッド（Routed）]、トランスペアレント モードの場合は [スイッチド（Switched）] を選択します。
- [選択したインターフェイス（Selected Interfaces）]：選択済みリストに FTD-A/外部および FTD-B/外部インターフェイスを追加します。

f) [保存（Save）] をクリックします。

ステップ 2 [オブジェクト管理（Object Management）] ページで、元の内部ネットワーク内のネットワーク オブジェクトを作成します。

a) コンテンツのテーブルから [ネットワーク（Network）] を選択し、**[ネットワークの追加（Add Network）] > [Add Object（オブジェクトの追加）]** をクリックします。
b) 内部ネットワークのプロパティを設定します。
   - [名前（Name）]：**inside-network** などの名前を入力します。
   - [ネットワーク（Network）]：**192.168.1.0/24** などのネットワーク アドレスを入力します。
c) [保存（Save）] をクリックします。

ステップ 3 変換済み NAT プールのネットワーク オブジェクトを作成し、オーバーライドを定義します。

a) **[ネットワークの追加（Add Network）] > [Add Object（オブジェクトの追加）]** をクリックします。
b) FTD-A の NAT プールのプロパティを設定します。
   - [名前（Name）]：**NAT-pool** などの名前を入力します。
   - [ネットワーク（Network）]：**10.100.10.10-10.100.10.200** などの FTD-A のプールに含めるアドレスの範囲を入力します。
c) [オーバーライドを許可（Allow Overrides）] を選択します。
d) [オーバーライド（Override）]の見出しをクリックして、オブジェクト オーバーライドのリストを開きます。
e) [追加（Add）] をクリックして、[オブジェクト オーバーライドの追加（Add Object Override）] ダイアログボックスを開きます。
f) FTD-B を選択し、[選択されたデバイス（Selected Devices）] リストに追加します。
g) [オーバーライド（Override）] タブをクリックし、[ネットワーク（Network）] を [10.200.10.10-10.200.10.200] に変更します。
h) [追加（Add）] をクリックして、オーバーライドをデバイスに追加します。

   FTD-B のオーバーライドを定義すると、FTD-B のこのオブジェクトが設定されるたびに、元のオブジェクトに定義されている値の代わりにオーバーライド値が使用されます。

i) [保存（Save）] をクリックします。

ステップ 4 NAT ルールを設定します。

a) **[デバイス（Devices）] > [NAT]** の順に選択し、FTD NAT ポリシーを作成または編集します。
b) [ルールの追加（Add Rule）] をクリックします。
c) 次のプロパティを設定します。

- [NAT ルール（NAT Rule）] = 自動 NAT ルール。
- [タイプ（Type）] = Dynamic。

d) [インターフェイス オブジェクト（Interface Objects）] タブで、以下の設定を行います。

- [送信元インターフェイス オブジェクト（Source Interface Objects）]：inside-zone。
- [宛先インターフェイス オブジェクト（Destination Interface Objects）]：outside-zone。

（注） インターフェイスオブジェクトはルールが設定されるデバイスを制御します。この例ではゾーンに FTD-A と FTD-B のインターフェイスのみが含まれているため、NAT ポリシーが追加のデバイスに割り当てられた場合でも、ルールはこれらの2つのデバイスにのみ展開されます。

e) [変換（Translation）] タブで、次の項目を設定します。

- [元の送信元（Original Source）]：inside-network オブジェクト。
- **[変換済み送信元（Translated Source）] > [アドレス（Address）]**：NAT-pool オブジェクト。

f) [保存（Save）] をクリックします。

各ファイアウォールによって保護される内部ネットワークに固有の変換を指定して、1 つのルールを FTD-A と FTD-B で異なるように解釈できるようになりました。

ダイナミック NAT

ここでは、ダイナミック NAT とその設定方法について説明します。

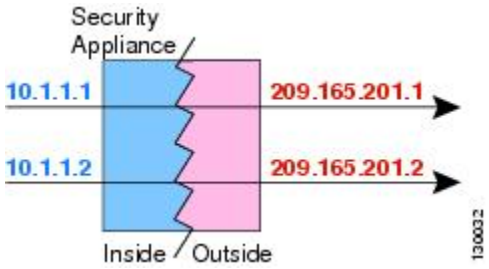
ダイナミック NAT について

ダイナミック NAT では、実際のアドレスのグループは、宛先ネットワーク上でルーティング可能なマッピングアドレスのプールに変換されます。マッピングされたプールにあるアドレスは、通常、実際のグループより少なくなります。変換対象のホストが宛先ネットワークにアクセスすると、NATは、マッピングされたプールからIPアドレスをそのホストに割り当てます。変換は、実際のホストが接続を開始したときにだけ作成されます。変換は接続が継続している間だけ有効であり、変換がタイムアウトすると、そのユーザは同じ IP アドレスを保持しません。したがって、アクセスルールでその接続が許可されている場合でも、宛先ネットワークのユーザは、ダイナミック NAT を使用するホストへの確実な接続を開始できません。

（注） 変換が継続している間、アクセス ルールで許可されていれば、リモート ホストは変換済みホストへの接続を開始できます。アドレスは予測不可能であるため、ホストへの接続は確立されません。ただし、この場合は、アクセス ルールのセキュリティに依存できます。

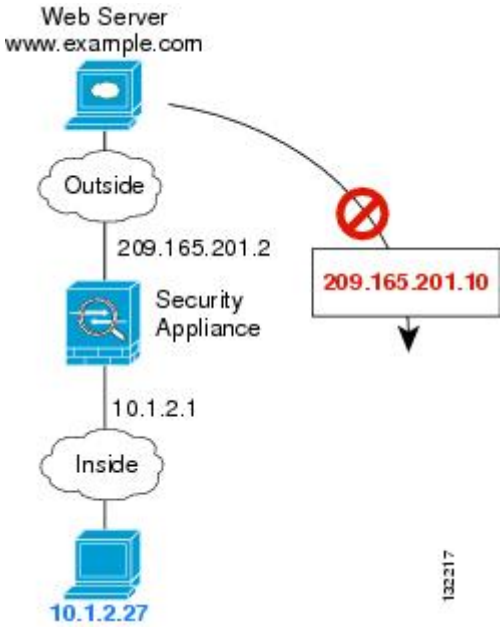
次の図に、一般的なダイナミック NAT のシナリオを示します。実際のホストだけが NAT セッションを作成でき、応答トラフィックが許可されます。

図 *35* : ダイナミック *NAT*



次の図に、マッピング アドレスへの接続開始を試みているリモート ホストを示します。このアドレスは、現時点では変換テーブルにないため、パケットはドロップされます。

図 *36* : マッピング アドレスへの接続開始を試みているリモート ホスト



ダイナミック NAT の欠点と利点

ダイナミック NAT には、次の欠点があります。

- マッピングされたプールにあるアドレスが実際のグループより少ない場合、予想以上にトラフィックが多いと、アドレスが不足する可能性があります。

  PAT では、1 つのアドレスのポートを使用して 64,000 を超える変換を処理できるため、このイベントが頻繁に発生する場合は、PAT または PAT のフォールバック方式を使用します。

- マッピング プールではルーティング可能なアドレスを多数使用する必要があるのに、ルーティング可能なアドレスは多数用意できない場合があります。

ダイナミック NAT の利点は、一部のプロトコルが PAT を使用できないということです。たとえば、PAT は次の場合は機能しません。

- GRE バージョン 0 などのように、オーバーロードするためのポートがない IP プロトコルでは機能しません。
- 一部のマルチメディア アプリケーションなどのように、1 つのポート上にデータ ストリームを持ち、別のポート上に制御パスを持ち、公開規格ではないアプリケーションでも機能しません。

ダイナミック自動 NAT の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin Access Admin Network Admin

ダイナミック自動 NAT ルールを使用して、宛先ネットワーク上でルーティング可能な別の IP アドレスにアドレスを変換します。

始める前に

[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] を選択し、ルールで必要なネットワーク オブジェクトまたはグループを作成します。 > または、NAT ルールを定義しているときにオブジェクトを作成することもできます。オブジェクトは次の要件を満たす必要があります。

- [元の送信元（Original Source）]：これはネットワーク オブジェクト（グループではない）でなければならず、ホスト、範囲またはサブネットも可能です。
- [変換済み送信元（Translated Source）]：ネットワーク オブジェクトまたはグループを指定できますが、サブネットを含めることはできません。グループに IPv4 アドレスと IPv6 アドレスの両方を含めることはできません。1 つのタイプだけ含める必要があります。グループに範囲とホスト IP アドレスの両方が含まれている場合、範囲はダイナミック NAT に使用され、ホスト IP アドレスは PAT のフォールバックとして使用されます。

ステップ 1 **[デバイス（Devices）] > [NAT]** の順に選択し、FTD NAT ポリシーを作成または編集します。

ステップ 2 次のいずれかを実行します。

- [ルールの追加（Add Rule）] ボタンをクリックして、新しいルールを作成します。
- [編集（edit）] アイコン（  ）をクリックして、既存のルールを編集します。

右クリック メニューにも、ルールの切り取り、コピー、貼り付け、挿入、削除オプションがあります。

ステップ 3 基本ルールのオプションを設定します。

- [NAT ルール（NAT Rule）]：[自動 NAT ルール（Auto NAT Rule）] を選択します。
- [タイプ（Type）]：[ダイナミック（Dynamic）] を選択します。

ステップ 4 [インターフェイス オブジェクト（Interface Objects）] タブで、次のフィールドを設定します。

- [送信元インターフェイス オブジェクト（Source Interface Objects）]、[宛先インターフェイス オブジェクト（Destination Interface Objects）]：（ブリッジ グループ メンバー インターフェイスの場合に必要）。この NAT ルールを適用するインターフェイスを特定するインターフェイス オブジェクト（セキュリティ ゾーンまたはインターフェイス グループ）。[Source] は実際のインターフェイスを含むオブジェクトで、このインターフェイスを経由してトラフィックはデバイスに入ります。[宛先（Destination）]は、デバイスから出るトラフィックが通過するマッピング インターフェイスを含んでいるオブジェクトです。デフォルトでは、ルールはブリッジ グループ メンバー インターフェイスを除くすべてのインターフェイス（[Any]）に適用されます。

ステップ 5 [一般（General）] [変換（Translation）] タブで、次のオプションを設定します。

- [元の送信元（Original Source）]：変換するアドレスを含むネットワーク オブジェクト。
- [変換済み送信元（Translated Source）]：マッピング アドレスを含むネットワーク オブジェクトまたはグループ。

ステップ 6 （オプション）[詳細（Advanced）] タブで、必要なオプションを選択します。

- [このルールに一致する DNS 応答を変換（Translate DNS replies that match this rule）]：DNS 応答の IP アドレスを変換するかどうかを指定します。マッピング インターフェイスから実際のインターフェイスに移動する DNS 応答の場合、アドレス（IPv4 A または IPv6 AAAA）レコードはマッピングされた値から実際の値に書き換えられます。反対に、実際のインターフェイスからマッピングされたインターフェイスへの DNS 応答の場合、レコードは実際の値からマッピングされた値に書き換えられます。このオプションは特殊な状況で使用され、書き換えにより A レコードと AAAA レコード間でも変換が行われる NAT64/46 変換のために必要なことがあります。詳細については、NAT を使用した DNS クエリと応答の書き換え （1551 ページ）を参照してください。
- [インターフェイス PAT へのフォールスルー（Fallthrough to Interface PAT）]（宛先インターフェイス）：その他のマッピング アドレスがすでに割り当てられている場合に、宛先インターフェイスの IP アドレスをバックアップ方式として使用するかどうかを指定します（インターフェイス PAT フォールバック）。このオプションは、ブリッジ グループのメンバーではない宛先インターフェイスを選択している場合にのみ使用できます。インターフェイスの IPv6 アドレスを使用するには、[IPv6] オプションも選択します。
- [IPv6]：インターフェイス PAT の宛先インターフェイスの IPv6 アドレスを使用するかどうか。

ステップ 7 [保存（Save）] をクリックしてルールを追加します。

ステップ 8 NAT ページで [保存（Save）] をクリックして変更を保存します。

ダイナミック手動 NAT の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin Access Admin Network Admin

自動 NAT では要件を満たせない場合は、ダイナミック手動 NAT ルールを使用します。たとえば、宛先に応じて異なる変換をしたい場合などです。ダイナミック NAT は、宛先ネットワーク上でルーティング可能な別の IP アドレスにアドレスを変換します。

始める前に

[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] を選択し、ルールで必要なネットワーク オブジェクトまたはグループを作成します。 > IPv4 アドレスと IPv6 アドレスの両方をグループに入れることはできません。1 つのタイプだけが含まれている必要があります。または、NAT ルールを定義しているときにオブジェクトを作成することもできます。またオブジェクトは次の要件も満たす必要があります。

- [元の送信元（Original Source）]：これはネットワーク オブジェクトまたはグループで、ホスト、範囲、またはサブネットを含むことができます。すべての元の送信元トラフィックを変換する場合、この手順をスキップし、ルールで [すべて（Any）] を指定します。
- [変換済み送信元（Translated Source）]：ネットワーク オブジェクトまたはグループを指定できますが、サブネットを含めることはできません。グループに範囲とホスト IP アドレスの両方が含まれている場合、範囲はダイナミック NAT に使用され、ホスト IP アドレスは PAT のフォールバックとして使用されます。

ルールで各アドレスの静的変換を設定すると、[元の宛先（Original Destination）] および [変換済み宛先（Translated Destination）] のネットワーク オブジェクトを作成できます。

ダイナミック NAT の場合、宛先でポート変換を実行することもできます。オブジェクト マネージャで、[元の宛先ポート（Original Destination Port）] と [変換済み宛先ポート（Translated Destination Port）] に使用できるポート オブジェクトがあることを確認します。送信元ポートを指定した場合、無視されます。

ステップ 1 **[デバイス（Devices）] > [NAT]** の順に選択し、FTD NAT ポリシーを作成または編集します。

ステップ 2 次のいずれかを実行します。

- [ルールの追加（Add Rule）] ボタンをクリックして、新しいルールを作成します。
- [編集（edit）] アイコン（  ）をクリックして、既存のルールを編集します。

右クリック メニューにも、ルールの切り取り、コピー、貼り付け、挿入、削除オプションがあります。

ステップ 3 基本ルールのオプションを設定します。

- [NAT ルール（NAT Rule）]：[手動 NAT ルール（Manual NAT Rule）] を選択します。

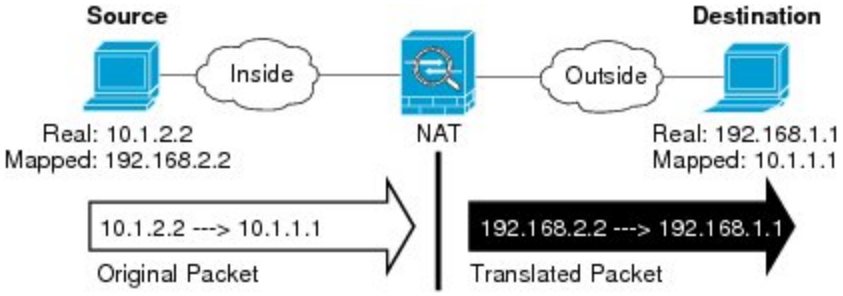
- [タイプ（Type）]：[ダイナミック（Dynamic）] を選択します。この設定は送信元アドレスにのみ適用されます。宛先アドレスの変換を定義している場合、変換は常に静的に行われます。
- [有効化（Enable）]：ルールをアクティブにするかどうかを指定します。ルールページの右クリックメニューを使用して、後でルールをアクティブ化または非アクティブ化することができます。
- [挿入（Insert）]：ルールを追加する場所を指定します。ルールは、カテゴリ（自動 NAT ルールの前か後）、または指定したルール番号の上か下に挿入できます。

ステップ 4 [インターフェイス オブジェクト（Interface Objects）] タブで、次のフィールドを設定します。

- [送信元インターフェイス オブジェクト（Source Interface Objects）]、[宛先インターフェイス オブジェクト（Destination Interface Objects）]：（ブリッジ グループ メンバー インターフェイスの場合に必要）。この NAT ルールを適用するインターフェイスを特定するインターフェイス オブジェクト（セキュリティ ゾーンまたはインターフェイス グループ）。[Source] は実際のインターフェイスを含むオブジェクトで、このインターフェイスを経由してトラフィックはデバイスに入ります。[宛先（Destination）] は、デバイスから出るトラフィックが通過するマッピング インターフェイスを含んでいるオブジェクトです。デフォルトでは、ルールはブリッジ グループ メンバー インターフェイスを除くすべてのインターフェイス（[Any]）に適用されます。

ステップ 5 （[変換（Translation）] タブで次を実行します）。元のパケット アドレス（IPv4 または IPv6）、つまり、元のパケットに表示されるパケット アドレスを特定します。

元のパケットと変換されたパケットの例については、次の図を参照してください。



- [Original Source][Address]：変換するアドレスを含むネットワーク オブジェクト、またはネットワーク グループ。
- [Original Destination][Address]：（オプション）。宛先アドレスを含むネットワーク オブジェクト。空白にしておくと、宛先に関わりなく発信元アドレスの変換が適用されます。宛先アドレスを指定した場合、そのアドレスにスタティック変換を設定するか、単にアイデンティティ NAT を使用できます。

  [Interface][Source Interface IP] が送信元インターフェイス（[Any] は不可）上の元の宛先に基づいて指定されるように選択できます。このオプションを選択する場合、変換済みの宛先オブジェクトも選択する必要があります。スタティック インターフェイス NAT に宛先アドレスのポート変換を実装するには、このオプションを選択し、さらにその宛先ポートの適切なポート オブジェクトを選択します。

ステップ 6 変換済みパケット アドレス（つまり、IPv4 または IPv6）を特定します。パケット アドレスは、宛先インターフェイス ネットワークに表示されます。必要に応じて、IPv4 と IPv6 の間で変換できます。

- [変換済み送信元（Translated Source）]：マッピング アドレスを含むネットワーク オブジェクトまたはグループ。
- [変換済み宛先（Translated Destination）]：（オプション）。変換されたパケットで使用される宛先アドレスを含むネットワーク オブジェクトまたはグループ。[元の宛先（Original Destination）] を選択した場合、同じオブジェクトを選択することによって、アイデンティティ NAT（つまり変換なし）を設定できます。

ステップ 7 （任意）サービス変換の宛先サービス ポートを指定します。[Original Destination Port]、[Translated Destination Port]

ダイナミック NAT はポート変換をサポートしていないため、[Original Source Port] フィールドと [Translated Source Port] フィールドは空白のままにしておきます。しかし、宛先変換は常にスタティックなので、宛先ポートに対してポート変換を実行できます。

NAT では、TCP または UDP だけがサポートされます。ポートを変換する場合、実際のサービス オブジェクトのプロトコルとマッピング サービス オブジェクトのプロトコルの両方が同じにします（両方とも TCP または両方とも UDP）。アイデンティティ NAT では、実際のポートとマッピング ポートの両方に同じサービス オブジェクトを使用できます。

ステップ 8 （オプション）[詳細（Advanced）] タブで、必要なオプションを選択します。

- （送信元変換の場合のみ）[このルールに一致する DNS 応答を変換（Translate DNS replies that match this rule）]：DNS 応答の IP アドレスを変換するかどうかを指定します。マッピング インターフェイスから実際のインターフェイスに移動する DNS 応答の場合、アドレス（IPv4 A または IPv6 AAAA）レコードはマッピングされた値から実際の値に書き換えられます。反対に、実際のインターフェイスからマッピングされたインターフェイスへの DNS 応答の場合、レコードは実際の値からマッピングされた値に書き換えられます。このオプションは特殊な状況で使用され、書き換えにより A レコードと AAAA レコード間でも変換が行われる NAT64/46 変換のために必要なことがあります。詳細については、NAT を使用した DNS クエリと応答の書き換え （1551 ページ）を参照してください。
- [インターフェイス PAT へのフォールスルー（Fallthrough to Interface PAT）]（宛先インターフェイス）：その他のマッピング アドレスがすでに割り当てられている場合に、宛先インターフェイスの IP アドレスをバックアップ方式として使用するかどうかを指定します（インターフェイス PAT フォールバック）。このオプションは、ブリッジ グループのメンバーではない宛先インターフェイスを選択している場合にのみ使用できます。インターフェイスの IPv6 アドレスを使用するには、[IPv6] オプションも選択します。
- [IPv6]：インターフェイス PAT の宛先インターフェイスの IPv6 アドレスを使用するかどうか。

ステップ 9 [保存（Save）] をクリックしてルールを追加します。

ステップ 10 NAT ページで [保存（Save）] をクリックして変更を保存します。

ダイナミック PAT

次のトピックでは、ダイナミック PAT について説明します。

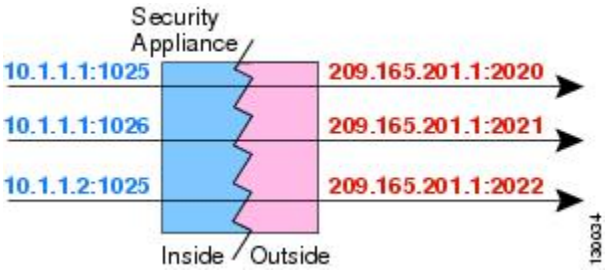
ダイナミック PAT について

ダイナミック PAT では、実際のアドレスおよび送信元ポートが 1 つのマッピング アドレスおよび固有のポートに変換されることによって、複数の実際のアドレスが 1 つのマッピング IP アドレスに変換されます。使用できる場合、実際の送信元ポート番号がマッピング ポートに対して使用されます。ただし、実際のポートが使用できない場合は、デフォルトで、マッピング ポートは実際のポート番号と同じポート範囲（0 ～ 511、512 ～ 1023、および 1024 ～ 65535）から選択されます。そのため、1024 よりも下のポートでは、小さい PAT プールのみを使用できます。下位ポート範囲を使用するトラフィックの量が多い場合は、サイズの異なる 3 つの層ではなく、フラットなポート範囲が使用されるように指定できます。

送信元ポートが接続ごとに異なるため、各接続には別の変換セッションが必要です。たとえば、10.1.1.1:1025 には、10.1.1.1:1026 とは別の変換が必要です。

次の図に、一般的なダイナミック PAT のシナリオを示します。実際のホストだけが NAT セッションを作成でき、応答トラフィックが許可されます。マッピング アドレスはどの変換でも同じですが、ポートがダイナミックに割り当てられます。

図 *37*：ダイナミック *PAT*



変換が継続している間、アクセス ルールで許可されていれば、宛先ネットワーク上のリモート ホストは変換済みホストへの接続を開始できます。実際のポート アドレスおよびマッピング ポート アドレスはどちらも予測不可能であるため、ホストへの接続は確立されません。ただし、この場合は、アクセス ルールのセキュリティに依存できます。

接続の有効期限が切れると、ポート変換も有効期限切れになります。

（注） インターフェイスごとに異なる PAT プールを使用することをお勧めします。複数のインターフェイス、特に「any」インターフェイスに同じプールを使用すると、プールがすぐに枯渇し、新しい変換に使用できるポートがなくなります。

ダイナミック PAT の欠点と利点

ダイナミック PAT では、1 つのマッピング アドレスを使用できるため、ルーティング可能なアドレスが節約されます。さらに、Firepower Threat Defense デバイス インターフェイスの IP アドレスを PAT アドレスとして使用できます。

同じブリッジ グループのインターフェイス間で変換するときは、IPv6 のダイナミック PAT（NAT66）を使用できません。この制限は、インターフェイスが異なるブリッジ グループの

メンバーである場合、またはブリッジ グループのメンバーと標準的なルーテッドインターフェイスの間には該当しません。

ダイナミック PAT は、制御パスとは異なるデータ ストリームを持つ一部のマルチメディア アプリケーションでは機能しません。詳細については、検査対象プロトコルに対するNATサポート （1461 ページ）を参照してください。

ダイナミック PAT によって、単一の IP アドレスから送信されたように見える数多くの接続が作成されることがあります。この場合、このトラフィックはサーバで DoS 攻撃として解釈される可能性があります。 アドレスの PAT プールを設定して、PAT アドレスのラウンドロビン割り当てを使用すると、この状況を緩和できます。

PAT プール オブジェクトの注意事項

PAT プールのネットワーク オブジェクトを作成する場合は、次のガイドラインに従ってください。

PAT プールの場合

- 使用できる場合、実際の送信元ポート番号がマッピング ポートに対して使用されます。ただし、実際のポートが使用できない場合は、デフォルトで、マッピング ポートは実際のポート番号と同じポート範囲（0 ～ 511、512 ～ 1023、および 1024 ～ 65535）から選択されます。そのため、1024 よりも下のポートでは、小さい PAT プールのみを使用できます。下位ポート範囲を使用するトラフィックが数多くある場合は、サイズが異なる 3 つの層の代わりにフラットなポート範囲を使用するように指定できます。1024 ～ 65535 または 1 ～ 65535 です。
- 同じ PAT プール オブジェクトを 2 つの異なるルールの中で使用する場合は、必ず同じオプションを各ルールに指定してください。たとえば、1 つのルールで拡張 PAT およびフラットな範囲が指定される場合は、もう一方のルールでも拡張 PAT およびフラットな範囲が指定される必要があります。

PAT プールの拡張 PAT の場合

- 多くのアプリケーション インスペクションでは、拡張 PAT はサポートされていません。
- ダイナミック PAT ルールに対して拡張 PAT をイネーブルにする場合、PAT プールのアドレスを、ポート トランスレーション ルールを持つ別のスタティック NAT の PAT アドレスとしても使用することはできません。たとえば、PAT プールに 10.1.1.1 が含まれている場合、PAT アドレスとして 10.1.1.1 を使用する、ポート トランスレーション ルールを持つスタティック NAT は作成できません。
- PAT プールを使用し、フォールバックのインターフェイスを指定する場合、拡張 PAT を使用できません。
- ICE または TURN を使用する VoIP 配置では、拡張 PAT を使用しないでください。ICE および TURN は、すべての宛先に対して同じであるために PAT バインディングに依存しています。

PAT プールのラウンド ロビン方式の場合

- ホストに既存の接続がある場合は、そのホストからの以降の接続は同じ PAT IP アドレスを使用します（ポートが使用可能である場合）。ただし、この「粘着性」は、フェールオーバーが発生すると失われます。デバイスがフェールオーバーすると、ホストからの後続の接続では最初の IP アドレスが使用されない場合があります。
- PAT プール ルール/ラウンド ロビン ルールとインターフェイス PAT ルールが同じインターフェイス上で混在していると、IP アドレスの「スティッキ性」も影響を受けます。指定したインターフェイスで PAT プールまたはインターフェイス PAT のいずれかを選択します。競合する PAT ルールは作成しないでください。
- ラウンドロビンでは、特に拡張 PAT と組み合わせた場合に、大量のメモリが消費されます。NAT プールはマッピングされるプロトコル/IP アドレス/ポート範囲ごとに作成されるため、ラウンドロビンでは数多くの同時NATプールが作成され、メモリが使用されます。拡張 PAT では、さらに多くの同時 NAT プールが作成されます。

ダイナミック自動 PAT の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin Access Admin Network Admin

ダイナミック自動 PAT ルールを使用して、複数の IP アドレスのみに変換するのではなく、固有の IP アドレスとポートの組み合わせにアドレスを変換します。1 つのアドレス（宛先インターフェイスまたは他のアドレスのいずれか）に変換するか、またはたくさんの有効な変換を提供するために、アドレスの PAT プールを使用します。

始める前に

[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] を選択し、ルールで必要なネットワーク オブジェクトまたはグループを作成します。 > または、NAT ルールを定義しているときにオブジェクトを作成することもできます。オブジェクトは次の要件を満たす必要があります。

- [元の送信元（Original Source）]：これはネットワーク オブジェクト（グループではない）でなければならず、ホスト、範囲またはサブネットも可能です。
- [変換済み送信元（Translated Source）]：PAT アドレスを指定するオプションは次のとおりです。
  - [宛先インターフェイス（Destination Interface）]：宛先インターフェイスのアドレスを使用するには、ネットワーク オブジェクトは必要ありません。
  - [単一 PAT アドレス（Single PAT address）]：単一のホストを含むネットワーク オブジェクトを作成します。

- [PAT プール（PAT pool）]：範囲を含むネットワーク オブジェクトを作成するか、またはホスト、範囲あるいはその両方を含むネットワーク オブジェクト グループを作成します。サブネットを含めることはできません。グループに IPv4 アドレスと IPv6 アドレスの両方を含めることはできません。1 つのタイプだけ含める必要があります。

ステップ 1 **[デバイス（Devices）]** > **[NAT]** の順に選択し、FTD NAT ポリシーを作成または編集します。

ステップ 2 次のいずれかを実行します。

- [ルールの追加（Add Rule）] ボタンをクリックして、新しいルールを作成します。
- [編集（edit）] アイコン（  ）をクリックして、既存のルールを編集します。

右クリック メニューにも、ルールの切り取り、コピー、貼り付け、挿入、削除オプションがあります。

ステップ 3 基本ルールのオプションを設定します。

- [NAT ルール（NAT Rule）]：[自動 NAT ルール（Auto NAT Rule）] を選択します。
- [タイプ（Type）]：[ダイナミック（Dynamic）] を選択します。

ステップ 4 [インターフェイス オブジェクト（Interface Objects）] タブで、次のフィールドを設定します。

- [送信元インターフェイス オブジェクト（Source Interface Objects）]、[宛先インターフェイス オブジェクト（Destination Interface Objects）]：（ブリッジ グループ メンバー インターフェイスの場合に必要）。この NAT ルールを適用するインターフェイスを特定するインターフェイス オブジェクト（セキュリティ ゾーンまたはインターフェイス グループ）。[Source] は実際のインターフェイスを含むオブジェクトで、このインターフェイスを経由してトラフィックはデバイスに入ります。[宛先（Destination）]は、デバイスから出るトラフィックが通過するマッピング インターフェイスを含んでいるオブジェクトです。デフォルトでは、ルールはブリッジ グループ メンバー インターフェイスを除くすべてのインターフェイス（[Any]）に適用されます。

ステップ 5 [一般（General）] [変換（Translation）] タブで、次のオプションを設定します。

- [元の送信元（Original Source）]：変換するアドレスを含むネットワーク オブジェクト。
- [変換済み送信元（Translated Source）]：次のいずれかになります。
  - （インターフェイス PAT）。宛先インターフェイスのアドレスを使用するには、**[宛先インターフェイス IP（Destination Interface IP）]** を選択します。また特定の宛先インターフェイス オブジェクトを選択する必要もあります。インターフェイスの IPv6 アドレスを使用するには、[詳細（Advanced）] タブで [IPv6] オプションを選択する必要もあります。PAT プールの設定ステップを飛ばします。
  - 宛先インターフェイスのアドレス以外の単一アドレスを使用する場合は、そのために作成したホスト ネットワーク オブジェクトを選択します。PAT プールの設定ステップを飛ばします。
  - PAT プールを使用するには、[変換済み送信元（Translated Source）] を空にしておきます。

ステップ 6 PAT プールを使用している場合は、[PAT Pool] タブを選択し、次の手順を実行します。

a) [PATプールの有効化（Enable PAT pool）] を選択します。

b) **[PAT]** > **[アドレス（Address）]** フィールドで、プールのアドレスを保持するネットワーク オブジェクト グループを選択します。

または、インターフェイス PAT を実装するもう 1 つの方法として、[インターフェイス（Interface）] [宛先インターフェイスIP（Destination Interface IP）] を選択します。

c) （オプション）必要に応じて、次のオプションを選択します。

- [Use Round Robin Allocation]：アドレスとポートをラウンドロビン形式で割り当てる場合。デフォルトではラウンドロビンは使用されず、1 つの PAT アドレスのポートがすべて割り当てられると次の PAT アドレスが使用されます。ラウンドロビン方式では、プール内の各 PAT アドレスから 1 つずつアドレス/ポートが割り当てられると最初のアドレスに戻り、次に 2 番目のアドレスというように順に使用されます。
- [Extended PAT Table]：拡張 PAT を使用する場合。拡張 PAT では、変換情報の宛先アドレスとポートを含め、IPアドレスごとではなく、サービスごとに65535個のポートが使用されます。通常は、PAT変換を作成するときに宛先ポートとアドレスは考慮されないため、PATアドレスごとに65535個のポートに制限されます。たとえば、拡張 PAT を使用して、192.168.1.7:23 に向かう場合の 10.1.1.1:1027 の変換、および 192.168.1.7:80 に向かう場合の 10.1.1.1:1027 の変換を作成できます。このオプションは、インターフェイス PAT またはインターフェイス PAT フォールバックで使用することはできません。
- [Flat Port Range]、[Include Reserved Ports]：TCP/UDP ポートを割り当てる際に、ポート範囲（1024 ～ 65535）を単一のフラットな範囲として使用する場合。変換用のマッピング ポート番号を選択する場合、PATによって、実際の送信元ポート番号が使用されます（使用可能な場合）。ただし、このオプションを設定しないと、実際のポートが使用できない場合は、デフォルトで、マッピング ポートは実際のポート番号と同じポート範囲（1 ～ 511、512 ～ 1023、および 1024 ～ 65535）から選択されます。下位範囲でポートが不足するのを回避するには、この設定を行います。1 ～ 65535 の範囲全体を使用するには、[予約済みポートを含む（Include Reserved Ports）] オプションも選択します。

ステップ 7 （オプション）[詳細（Advanced）] タブで、必要なオプションを選択します。

- [インターフェイス PAT へのフォールスルー（Fallthrough to Interface PAT）]（宛先インターフェイス）：その他のマッピングアドレスがすでに割り当てられている場合に、宛先インターフェイスのIPアドレスをバックアップ方式として使用するかどうかを指定します（インターフェイス PAT フォールバック）。このオプションは、ブリッジ グループのメンバーではない宛先インターフェイスを選択している場合にのみ使用できます。インターフェイスの IPv6 アドレスを使用するには、[IPv6] オプションも選択します。すでにインターフェイス PAT を変換済みアドレスとして設定している場合には、このオプションは使用できません。
- [IPv6]：インターフェイス PAT の宛先インターフェイスの IPv6 アドレスを使用するかどうか。

ステップ 8 [保存（Save）] をクリックしてルールを追加します。

ステップ 9 NAT ページで [保存（Save）] をクリックして変更を保存します。

ダイナミック手動 PAT の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin Access Admin Network Admin

自動 PAT がお客様のニーズを満たしていない場合は、ダイナミック手動 PAT ルールを使用します。たとえば、宛先に応じて異なる変換をしたい場合などです。ダイナミック PAT は、複数の IP アドレスのみに変換するのではなく、固有の IP アドレスとポートの組み合わせにアドレスを変換します。1 つのアドレス（宛先インターフェイスまたは他のアドレスのいずれか）に変換するか、またはたくさんの有効な変換を提供するために、アドレスの PAT プールを使用します。

始める前に

[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] を選択し、ルールで必要なネットワーク オブジェクトまたはグループを作成します。 > IPv4 アドレスと IPv6 アドレスの両方をグループに入れることはできません。1 つのタイプだけが含まれている必要があります。または、NAT ルールを定義しているときにオブジェクトを作成することもできます。またオブジェクトは次の要件も満たす必要があります。

- [元の送信元（Original Source）]：これはネットワーク オブジェクトまたはグループで、ホスト、範囲、またはサブネットを含むことができます。すべての元の送信元トラフィックを変換する場合、この手順をスキップし、ルールで [すべて（Any）] を指定します。
- [変換済み送信元（Translated Source）]：PAT アドレスを指定するオプションは次のとおりです。
  - [宛先インターフェイス（Destination Interface）]：宛先インターフェイスのアドレスを使用するには、ネットワーク オブジェクトは必要ありません。
  - [単一 PAT アドレス（Single PAT address）]：単一のホストを含むネットワーク オブジェクトを作成します。
  - [PAT プール（PAT pool）]：範囲を含むネットワーク オブジェクトを作成するか、またはホスト、範囲あるいはその両方を含むネットワーク オブジェクト グループを作成します。サブネットを含めることはできません。

ルールで各アドレスの静的変換を設定すると、[元の宛先（Original Destination）] および [変換済み宛先（Translated Destination）] のネットワーク オブジェクトを作成できます。

ダイナミック NAT の場合、宛先でポート変換を実行することもできます。オブジェクト マネージャで、[元の宛先ポート（Original Destination Port）] と [変換済み宛先ポート（Translated Destination Port）] に使用できるポート オブジェクトがあることを確認します。送信元ポートを指定した場合、無視されます。

ステップ 1 **[デバイス（Devices）] > [NAT]** の順に選択し、FTD NAT ポリシーを作成または編集します。

ステップ 2 次のいずれかを実行します。

- [ルールの追加（Add Rule）] ボタンをクリックして、新しいルールを作成します。
- [編集（edit）] アイコン（）をクリックして、既存のルールを編集します。

右クリック メニューにも、ルールの切り取り、コピー、貼り付け、挿入、削除オプションがあります。

ステップ 3 基本ルールのオプションを設定します。

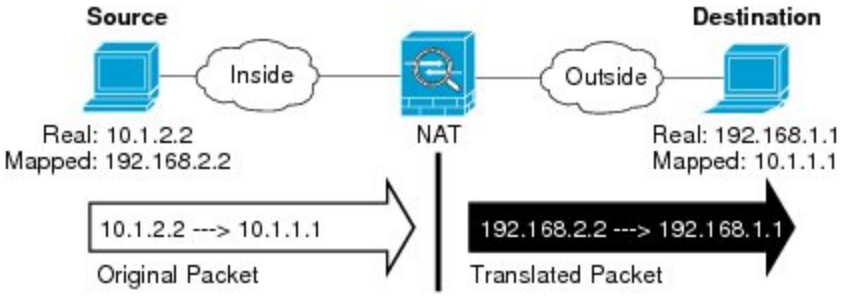
- [NAT ルール（NAT Rule）] : [手動 NAT ルール（Manual NAT Rule）] を選択します。
- [タイプ（Type）] : [ダイナミック（Dynamic）] を選択します。この設定は送信元アドレスにのみ適用されます。宛先アドレスの変換を定義している場合、変換は常に静的に行われます。
- [有効化（Enable）] : ルールをアクティブにするかどうかを指定します。ルールページの右クリック メニューを使用して、後でルールをアクティブ化または非アクティブ化することができます。
- [挿入（Insert）] : ルールを追加する場所を指定します。ルールは、カテゴリ（自動 NAT ルールの前か後）、または指定したルール番号の上か下に挿入できます。

ステップ 4 [インターフェイス オブジェクト（Interface Objects）] タブで、次のフィールドを設定します。

- [送信元インターフェイス オブジェクト（Source Interface Objects）]、[宛先インターフェイス オブジェクト（Destination Interface Objects）] :（ブリッジ グループ メンバー インターフェイスの場合に必要）。この NAT ルールを適用するインターフェイスを特定するインターフェイス オブジェクト（セキュリティ ゾーンまたはインターフェイス グループ）。[Source] は実際のインターフェイスを含むオブジェクトで、このインターフェイスを経由してトラフィックはデバイスに入ります。[宛先（Destination）] は、デバイスから出るトラフィックが通過するマッピング インターフェイスを含んでいるオブジェクトです。デフォルトでは、ルールはブリッジ グループ メンバー インターフェイスを除くすべてのインターフェイス（[Any]）に適用されます。

ステップ 5 （[変換（Translation）] タブで次を実行します）。元のパケット アドレス（IPv4 または IPv6）、つまり、元のパケットに表示されるパケット アドレスを特定します。

元のパケットと変換されたパケットの例については、次の図を参照してください。



- [Original Source][Address]：変換するアドレスを含むネットワーク オブジェクト、またはネットワーク グループ。
- [Original Destination][Address]：（オプション）。宛先アドレスを含むネットワーク オブジェクト。空白にしておくと、宛先に関わりなく発信元アドレスの変換が適用されます。宛先アドレスを指定

した場合、そのアドレスにスタティック変換を設定するか、単にアイデンティティ NAT を使用できます。

[Interface][Source Interface IP] が送信元インターフェイス（[Any] は不可）上の元の宛先に基づいて指定されるように選択できます。このオプションを選択する場合、変換済みの宛先オブジェクトも選択する必要があります。スタティック インターフェイス NAT に宛先アドレスのポート変換を実装するには、このオプションを選択し、さらにその宛先ポートの適切なポート オブジェクトを選択します。

ステップ 6 変換済みパケット アドレス（つまり、IPv4 または IPv6）を特定します。パケット アドレスは、宛先インターフェイス ネットワークに表示されます。必要に応じて、IPv4 と IPv6 の間で変換できます。

- [変換済み送信元（Translated Source）]：次のいずれかになります。
  - （インターフェイス PAT）。宛先インターフェイスのアドレスを使用するには、**[宛先インターフェイス IP（Destination Interface IP）]** を選択します。また特定の宛先インターフェイス オブジェクトを選択する必要もあります。インターフェイスの IPv6 アドレスを使用するには、[詳細（Advanced）] タブで [IPv6] オプションを選択する必要もあります。PAT プールの設定ステップを飛ばします。
  - 宛先インターフェイスのアドレス以外の単一アドレスを使用する場合は、そのために作成したホスト ネットワーク オブジェクトを選択します。PAT プールの設定ステップを飛ばします。
  - PAT プールを使用するには、[変換済み送信元（Translated Source）] を空にしておきます。
- [変換済み宛先（Translated Destination）]：（オプション）。変換されたパケットで使用される宛先アドレスを含むネットワーク オブジェクトまたはグループ。[元の宛先（Original Destination）] を選択した場合、同じオブジェクトを選択することによって、アイデンティティ NAT（つまり変換なし）を設定できます。

ステップ 7 （任意）サービス変換の宛先サービス ポートを指定します。[Original Destination Port]、[Translated Destination Port]

ダイナミック NAT はポート変換をサポートしていないため、[Original Source Port] フィールドと [Translated Source Port] フィールドは空白のままにしておきます。しかし、宛先変換は常にスタティックなので、宛先ポートに対してポート変換を実行できます。

NAT では、TCP または UDP だけがサポートされます。ポートを変換する場合、実際のサービス オブジェクトのプロトコルとマッピング サービス オブジェクトのプロトコルの両方が同じにします（両方とも TCP または両方とも UDP）。アイデンティティ NAT では、実際のポートとマッピング ポートの両方に同じサービス オブジェクトを使用できます。

ステップ 8 PAT プールを使用している場合は、[PAT Pool] タブを選択し、次の手順を実行します。

a) [PATプールの有効化（Enable PAT pool）] を選択します。

b) **[PAT]** > **[アドレス（Address）]** フィールドで、プールのアドレスを保持するネットワーク オブジェクト グループを選択します。

または、インターフェイス PAT を実装するもう 1 つの方法として、[インターフェイス（Interface）] [宛先インターフェイスIP（Destination Interface IP）] を選択します。

c) （オプション）必要に応じて、次のオプションを選択します。

- [Use Round Robin Allocation]：アドレスとポートをラウンドロビン形式で割り当てる場合。デフォルトではラウンドロビンは使用されず、1 つの PAT アドレスのポートがすべて割り当てられると次の PAT アドレスが使用されます。ラウンドロビン方式では、プール内の各 PAT アドレスから 1 つずつアドレス/ポートが割り当てられると最初のアドレスに戻り、次に 2 番目のアドレスというように順に使用されます。
- [Extended PAT Table]：拡張 PAT を使用する場合。拡張 PAT では、変換情報の宛先アドレスとポートを含め、IP アドレスごとではなく、サービスごとに 65535 個のポートが使用されます。通常は、PAT 変換を作成するときに宛先ポートとアドレスは考慮されないため、PAT アドレスごとに 65535 個のポートに制限されます。たとえば、拡張 PAT を使用して、192.168.1.7:23 に向かう場合の 10.1.1.1:1027 の変換、および 192.168.1.7:80 に向かう場合の 10.1.1.1:1027 の変換を作成できます。このオプションは、インターフェイス PAT またはインターフェイス PAT フォールバックで使用することはできません。
- [Flat Port Range]、[Include Reserved Ports]：TCP/UDP ポートを割り当てる際に、ポート範囲（1024 ～ 65535）を単一のフラットな範囲として使用する場合。変換用のマッピング ポート番号を選択する場合、PAT によって、実際の送信元ポート番号が使用されます（使用可能な場合）。ただし、このオプションを設定しないと、実際のポートが使用できない場合は、デフォルトで、マッピング ポートは実際のポート番号と同じポート範囲（1 ～ 511、512 ～ 1023、および 1024 ～ 65535）から選択されます。下位範囲でポートが不足するのを回避するには、この設定を行います。1 ～ 65535 の範囲全体を使用するには、[予約済みポートを含む（Include Reserved Ports）] オプションも選択します。

ステップ 9 （オプション）[詳細（Advanced）] タブで、必要なオプションを選択します。

- [インターフェイス PAT へのフォールスルー（Fallthrough to Interface PAT）]（宛先インターフェイス）：その他のマッピング アドレスがすでに割り当てられている場合に、宛先インターフェイスの IP アドレスをバックアップ方式として使用するかどうかを指定します（インターフェイス PAT フォールバック）。このオプションは、ブリッジ グループのメンバーではない宛先インターフェイスを選択している場合にのみ使用できます。インターフェイスの IPv6 アドレスを使用するには、[IPv6] オプションも選択します。
- [IPv6]：インターフェイス PAT の宛先インターフェイスの IPv6 アドレスを使用するかどうか。

ステップ 10 [保存（Save）] をクリックしてルールを追加します。

ステップ 11 NAT ページで [保存（Save）] をクリックして変更を保存します。

スタティック NAT

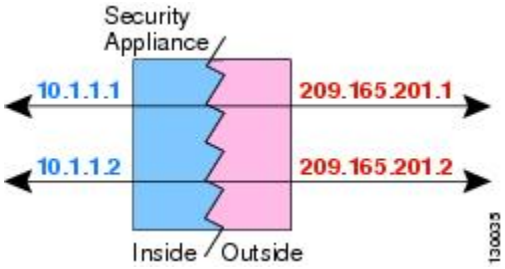
ここでは、スタティック NAT とその実装方法について説明します。

スタティック NAT について

スタティック NAT では、実際のアドレスからマッピング アドレスへの固定変換が作成されます。マッピング アドレスは連続する各接続で同じなので、スタティック NAT では、双方向の接続（ホストへの接続とホストから接続の両方）を開始できます（接続を許可するアクセス ルールが存在する場合）。一方、ダイナミック NAT および PAT では、各ホストが以降の各変換に対して異なるアドレスまたはポートを使用するので、双方向の開始はサポートされません。

次の図に、一般的なスタティック NAT のシナリオを示します。この変換は常にアクティブなので、実際のホストとリモート ホストの両方が接続を開始できます。

図 *38 :* スタティック *NAT*



（注） 必要に応じて、双方向をディセーブルにできます。

ポート変換を設定したスタティック NAT

ポート変換を設定したスタティック NAT では、実際のプロトコルおよびポートとマッピングされたプロトコルおよびポートを指定できます。

スタティック NAT を使用してポートを指定する場合、ポートまたは IP アドレスを同じ値にマッピングするか、別の値にマッピングするかを選択できます。

次の図に、ポート変換が設定された一般的なスタティック NAT のシナリオを示します。自身にマッピングしたポートと、別の値にマッピングしたポートの両方を示しています。いずれのケースでも、IP アドレスは別の値にマッピングされています。この変換は常にアクティブなので、変換されたホストとリモート ホストの両方が接続を開始できます。

図 *39 :* ポート変換を設定したスタティック *NAT* の一般的なシナリオ

ポート変換ルールを設定したスタティック NAT は、指定されたポートの宛先 IP アドレスのみにアクセスを制限します。NAT ルール対象外の別のポートで宛先 IP アドレスにアクセスしようとすると、接続がブロックされます。さらに、手動 NAT の場合、NAT ルールの送信元 IP アドレスと一致しないトラフィックが宛先 IP アドレスと一致する場合、宛先ポートに関係なくドロップされます。したがって、宛先IPアドレスに対して許可される他のすべてのトラフィックに追加ルールを追加する必要があります。たとえば、ポートを指定せずに IP アドレスにスタティック NAT ルールを設定し、ポート変換ルールの後ろにそれを配置できます。

（注） セカンダリ チャネルのアプリケーション インスペクションが必要なアプリケーション（FTP、VoIP など）を使用する場合は、NAT が自動的にセカンダリ ポートを変換します。

次に、ポート変換を設定したスタティック NAT のその他の使用例の一部を示します。

アイデンティティ ポート変換を設定したスタティック NAT

内部リソースへの外部アクセスを簡素化できます。たとえば、異なるポートでサービスを提供する 3 つの個別のサーバ（FTP、HTTP、SMTP など）がある場合は、それらのサービスにアクセスするための単一の IP アドレスを外部ユーザに提供できます。その後、アイデンティティ ポート変換を設定したスタティック NAT を設定し、アクセスしようとしているポートに基づいて、単一の外部 IP アドレスを実サーバの正しい IP アドレスにマッピングすることができます。サーバは標準のポート（それぞれ 21、80、および 25）を使用しているため、ポートを変更する必要はありません。

標準以外のポートのポート変換を設定したスタティック NAT

ポート変換を設定したスタティック NAT を使用すると、予約済みポートから標準以外のポートへの変換や、その逆の変換も実行できます。たとえば、内部 Web サーバがポート 8080 を使用する場合、ポート 80 に接続することを外部ユーザに許可し、その後、変換を元のポート 8080 に戻すことができます。同様に、セキュリティをさらに高めるには、Web ユーザに標準以外のポート 6785 に接続するように指示し、その後、変換をポート 80 に戻すことができます。

ポート変換を設定したスタティック インターフェイス NAT

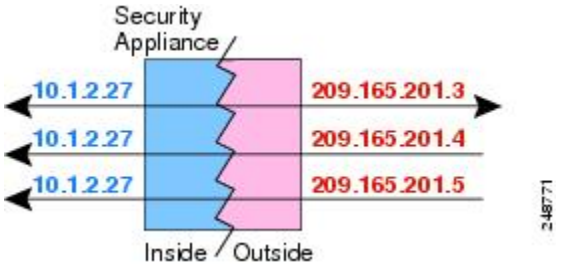
スタティック NAT は、実際のアドレスをインターフェイス アドレスとポートの組み合わせにマッピングするように設定できます。たとえば、デバイスの外部インターフェイスへの Telnet アクセスを内部ホストにリダイレクトする場合、内部ホストの IP アドレス/ポート 23 を外部インターフェイス アドレス/ポート 23 にマッピングできます。

一対多のスタティック NAT

通常、スタティック NAT は 1 対 1 のマッピングで設定します。しかし場合によっては、1 つの実際のアドレスを複数のマッピング アドレスに設定することがあります（1 対多）。1 対多のスタティック NAT を設定する場合、実際のホストがトラフィックを開始すると、常に最初のマッピングアドレスが使用されます。しかし、ホストに向けて開始されたトラフィックの場合、任意のマッピングアドレスへのトラフィックを開始でき、1 つの実際のアドレスには変換されません。

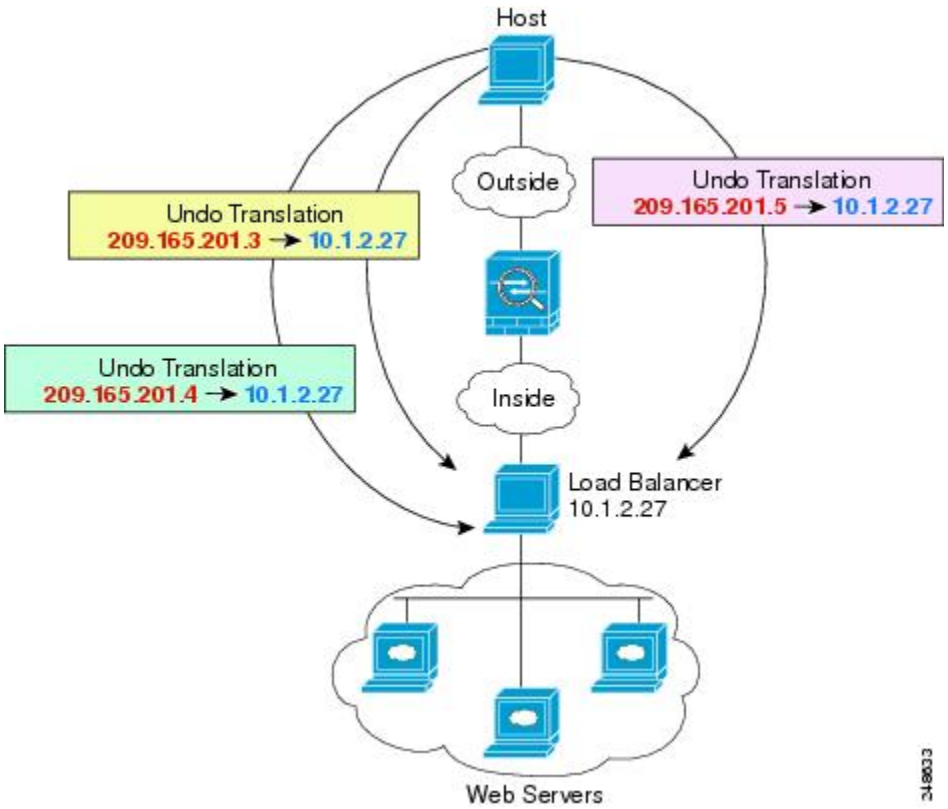
次の図に、一般的な 1 対多のスタティック NAT シナリオを示します。実際のホストが開始すると、常に最初のマッピング アドレスが使用されるため、実際のホスト IP/最初のマッピング IP の変換は、理論的には双方向変換のみが行われます。

図 *40 :* 一対多のスタティック *NAT*



たとえば、10.1.2.27 にロード バランサが存在するとします。要求される URL に応じて、トラフィックを正しい Web サーバにリダイレクトします。

図 *41 :* 一対多のスタティック *NAT* の例



他のマッピング シナリオ（非推奨）

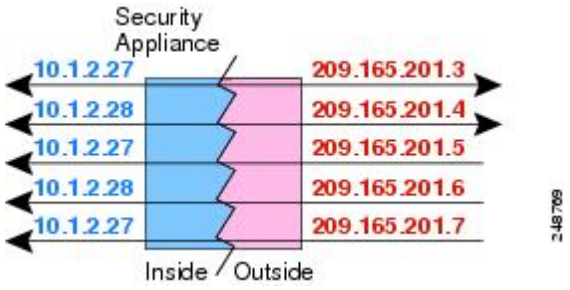
NAT には、1 対 1、1 対多だけではなく、少対多、多対少、多対 1 など任意の種類のスタティック マッピング シナリオを使用できるという柔軟性があります。1 対 1 マッピングまたは 1 対多

マッピングだけを使用することをお勧めします。これらの他のマッピング オプションは、予期しない結果が発生する可能性があります。

機能的には、少対多は、1 対多と同じです。しかし、コンフィギュレーションが複雑化して、実際のマッピングが一目では明らかでない場合があるため、必要とする実際の各アドレスに対して 1 対多のコンフィギュレーションを作成することを推奨します。たとえば、少対多のシナリオでは、少数の実際のアドレスが多数のマッピング アドレスに順番にマッピングされます（A は 1、B は 2、C は 3）。すべての実際のアドレスがマッピングされたら、次にマッピングされるアドレスは、最初の実際のアドレスにマッピングされ、すべてのマッピング アドレスがマッピングされるまで続行されます（A は 4、B は 5、C は 6）。この結果、実際の各アドレスに対して複数のマッピング アドレスが存在することになります。1 対多のコンフィギュレーションのように、最初のマッピングだけが双方向であり、以降のマッピングでは、実際のホストへのトラフィックを開始できますが、実際のホストからのすべてのトラフィックは、送信元の最初のマッピング アドレスだけを使用できます。

次の図に、一般的な少対多のスタティック NAT シナリオを示します。

図 *42*：少対多のスタティック *NAT*

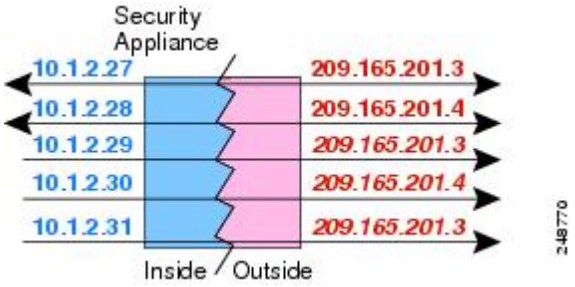


多対少または多対 1 コンフィギュレーションでは、マッピング アドレスよりも多くの実際のアドレスが存在します。実際のアドレスが不足するよりも前に、マッピング アドレスが不足します。双方向の開始を実現できるのは、最下位の実際の IP アドレスとマッピングされたプールの間でマッピングを行ったときだけです。残りの上位の実際のアドレスはトラフィックを開始できますが、これらへのトラフィックを開始できません。接続のリターン トラフィックは、接続の固有の 5 つの要素（送信元 IP、宛先 IP、送信元ポート、宛先ポート、プロトコル）によって適切な実際のアドレスに転送されます。

（注） 多対少または多対 1 の NAT は PAT ではありません。2 つの実際のホストが同じ送信元ポート番号を使用して同じ外部サーバおよび同じ TCP 宛先ポートにアクセスする場合は、両方のホストが同じ IP アドレスに変換されると、アドレスの競合がある（5 つのタプルが一意でない）ため、両方の接続がリセットされます。

次の図に、一般的な多対少のスタティック NAT シナリオを示します。

図 *43 :* 多対少のスタティック *NAT*



このようにスタティック ルールを使用するのではなく、双方向の開始を必要とするトラフィックに 1 対 1 のルールを作成し、残りのアドレスにダイナミック ルールを作成することをお勧めします。

スタティック自動 NAT の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin Access Admin Network Admin

スタティック自動 NAT ルールを使用して、アドレスを宛先ネットワーク上でルーティング可能な別の IP アドレスに変換します。また、スタティック NAT ルールでポートの変換もできます。

始める前に

[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] を選択し、ルールで必要なネットワーク オブジェクトまたはグループを作成します。 > または、NAT ルールを定義しているときにオブジェクトを作成することもできます。オブジェクトは次の要件を満たす必要があります。

- [元の送信元（Original Source）]：これはネットワーク オブジェクト（グループではない）でなければならず、ホスト、範囲またはサブネットも可能です。
- [変換済み送信元（Translated Source）]：変換済みアドレスを指定するには、次のオプションがあります。
  - [宛先インターフェイス（Destination Interface）]：宛先インターフェイス アドレスを使用するには、ネットワーク オブジェクトは必要ありません。これはポート変換と共に、スタティック インターフェイス NAT を設定します。送信元アドレス/ポートは、インターフェイスのアドレス、および同じポート番号に変換されます。
  - [アドレス（Address）]：ホスト、範囲、またはサブネットを含むネットワーク オブジェクトまたはグループを作成します。IPv4 アドレスと IPv6 アドレスの両方をグループに入れることはできません。1 つのタイプだけが含まれている必要があります。通

常、1 対 1 のマッピングでは、実際のアドレスと同じ数のマッピング アドレスを設定します。しかし、アドレスの数が一致しない場合もあります。

ステップ 1 **[デバイス（Devices）]** > **[NAT]** の順に選択し、FTD NAT ポリシーを作成または編集します。

ステップ 2 次のいずれかを実行します。

- [ルールの追加（Add Rule）] ボタンをクリックして、新しいルールを作成します。
- [編集（edit）] アイコン（）をクリックして、既存のルールを編集します。

右クリック メニューにも、ルールの切り取り、コピー、貼り付け、挿入、削除オプションがあります。

ステップ 3 基本ルールのオプションを設定します。

- [NAT ルール（NAT Rule）] : [自動 NAT ルール（Auto NAT Rule）] を選択します。
- [タイプ（Type）] : [スタティック（Static）] を選択します。

ステップ 4 [インターフェイス オブジェクト（Interface Objects）] タブで、次のフィールドを設定します。

- [送信元インターフェイス オブジェクト（Source Interface Objects）]、[宛先インターフェイス オブジェクト（Destination Interface Objects）] :（ブリッジ グループ メンバー インターフェイスの場合に必要）。この NAT ルールを適用するインターフェイスを特定するインターフェイス オブジェクト（セキュリティ ゾーンまたはインターフェイス グループ）。[Source] は実際のインターフェイスを含むオブジェクトで、このインターフェイスを経由してトラフィックはデバイスに入ります。[宛先（Destination）]は、デバイスから出るトラフィックが通過するマッピング インターフェイスを含んでいるオブジェクトです。デフォルトでは、ルールはブリッジ グループ メンバー インターフェイスを除くすべてのインターフェイス（[Any]）に適用されます。

ステップ 5 [一般（General）] [変換（Translation）] タブで、次のオプションを設定します。

- [元の送信元（Original Source）] : 変換するアドレスを含むネットワーク オブジェクト。
- [変換済み送信元（Translated Source）] : 次のいずれかになります。
  - アドレスの設定グループを使用するには、[アドレス（Address）] およびマッピングされたアドレスを含むネットワーク オブジェクトまたはグループを選択します。通常、1 対 1 のマッピングでは、実際のアドレスと同じ数のマッピング アドレスを設定します。しかし、アドレスの数が一致しない場合もあります。
  - （ポート変換を設定したスタティック インターフェイス NAT）宛先インターフェイスのアドレスを使用するには、**[宛先インターフェイス IP（Destination Interface IP）]** を選択します。また特定の宛先インターフェイス オブジェクトを選択する必要もあります。インターフェイスの IPv6 アドレスを使用するには、[詳細（Advanced）] タブで [IPv6] オプションを選択する必要もあります。これはポート変換と共に、スタティック インターフェイス NAT を設定します。送信元アドレス/ポートは、インターフェイスのアドレス、および同じポート番号に変換されます。
- （オプション）[元のポート（Original Port）]、[変換済みポート（Translated Port）] : TCP または UDP ポートを変換する必要がある場合は、[元のポート（Original Port）] でプロトコルを選択し、元のポート番号と変換済みポート番号を入力します。たとえば、必要に応じて TCP/80 を 8080 に変換できます。

ステップ 6 （オプション）[詳細（Advanced）] タブで、必要なオプションを選択します。

- [このルールに一致する DNS 応答を変換（Translate DNS replies that match this rule）]：DNS 応答の IP アドレスを変換するかどうかを指定します。マッピング インターフェイスから実際のインターフェイスに移動する DNS 応答の場合、アドレス（IPv4 A または IPv6 AAAA）レコードはマッピングされた値から実際の値に書き換えられます。反対に、実際のインターフェイスからマッピングされたインターフェイスへの DNS 応答の場合、レコードは実際の値からマッピングされた値に書き換えられます。このオプションは特殊な状況で使用され、書き換えにより A レコードと AAAA レコード間でも変換が行われる NAT64/46 変換のために必要なことがあります。詳細については、NAT を使用した DNS クエリと応答の書き換え（1551 ページ）を参照してください。このオプションはポート変換を行う場合は使用できません。
- [IPv6]：インターフェイス PAT の宛先インターフェイスの IPv6 アドレスを使用するかどうか。
- [ネット間マッピング（Net to Net Mapping）]：NAT 46 の場合、このオプションを選択して、最初の IPv4 アドレスを最初の IPv6 アドレスに変換し、2 番目を 2 番目に変換という順序で変換します。このオプションを選択しない場合、IPv4 埋め込み方式が使用されます。1 対 1 の変換の場合は、このオプションを使用する必要があります。
- [宛先インターフェイスで ARP をプロキシしない（Do not proxy ARP on Destination Interface）]：マッピング IP アドレスへの着信パケットのプロキシ ARP を無効にします。マッピング インターフェイスと同じネットワーク上のアドレスを使用した場合、システムはプロキシ ARP を使用してマッピング アドレスのすべての ARP 要求に応答することで、マッピング アドレスを宛先とするトラフィックを代行受信します。この方法では、デバイスがその他のネットワークのゲートウェイである必要がないため、ルーティングが簡略化されます。必要に応じてプロキシ ARP をディセーブルにできます。その場合は、アップストリーム ルータの適切なルートがあることを確認する必要があります。アイデンティティ NAT の場合、通常はプロキシ ARP は不要です。場合によっては接続の問題が生じることがあります。

ステップ 7 [保存（Save）] をクリックしてルールを追加します。

ステップ 8 NAT ページで [保存（Save）] をクリックして変更を保存します。

スタティック手動 NAT の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin Access Admin Network Admin

自動 NAT がニーズを満たさない場合、スタティック手動 NAT ルールを使用します。たとえば、宛先に応じて異なる変換をしたい場合などです。スタティック NAT は、アドレスを宛先ネットワーク上でルーティング可能な別の IP アドレスに変換します。また、スタティック NAT ルールでポートの変換もできます。

始める前に

[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] を選択し、ルールで必要なネットワーク オブジェクトまたはグループを作成します。 > IPv4 アドレスと IPv6 アドレスの両方をグループに入れることはできません。1 つのタイプだけが含まれている必要があります。または、NAT ルールを定義しているときにオブジェクトを作成することもできます。またオブジェクトは次の要件も満たす必要があります。

- [元の送信元（Original Source）]：これはネットワーク オブジェクトまたはグループで、ホスト、範囲、またはサブネットを含むことができます。すべての元の送信元トラフィックを変換する場合、この手順をスキップし、ルールで [すべて（Any）] を指定します。
- [変換済み送信元（Translated Source）]：変換済みアドレスを指定するには、次のオプションがあります。
  - [宛先インターフェイス（Destination Interface）]：宛先インターフェイス アドレスを使用するには、ネットワーク オブジェクトは必要ありません。これはポート変換と共に、スタティック インターフェイス NAT を設定します。送信元アドレス/ポートは、インターフェイスのアドレス、および同じポート番号に変換されます。
  - [アドレス（Address）]：ホスト、範囲、またはサブネットを含むネットワーク オブジェクトまたはグループを作成します。通常、1 対 1 のマッピングでは、実際のアドレスと同じ数のマッピング アドレスを設定します。しかし、アドレスの数が一致しない場合もあります。

ルールで各アドレスの静的変換を設定すると、[元の宛先（Original Destination）] および [変換済み宛先（Translated Destination）] のネットワーク オブジェクトを作成できます。ポート変換を設定した宛先のスタティック インターフェイス NAT のみを設定する場合は、宛先のマッピング アドレスに対するオブジェクトの追加をスキップでき、ルールでインターフェイスを指定します。

また送信元、宛先、またはその両方のポート変換も実行できます。オブジェクト マネージャでは、元のポートと変換されたポートで使用できるポート オブジェクトがあることを確認します。

ステップ 1 **[デバイス（Devices）] > [NAT]** の順に選択し、FTD NAT ポリシーを作成または編集します。

ステップ 2 次のいずれかを実行します。

- [ルールの追加（Add Rule）] ボタンをクリックして、新しいルールを作成します。
- [編集（edit）] アイコン（）をクリックして、既存のルールを編集します。

右クリック メニューにも、ルールの切り取り、コピー、貼り付け、挿入、削除オプションがあります。

ステップ 3 基本ルールのオプションを設定します。

- [NAT ルール（NAT Rule）]：[手動 NAT ルール（Manual NAT Rule）] を選択します。
- [タイプ（Type）]：[スタティック（Static）] を選択します。この設定は送信元アドレスにのみ適用されます。宛先アドレスの変換を定義している場合、変換は常に静的に行われます。

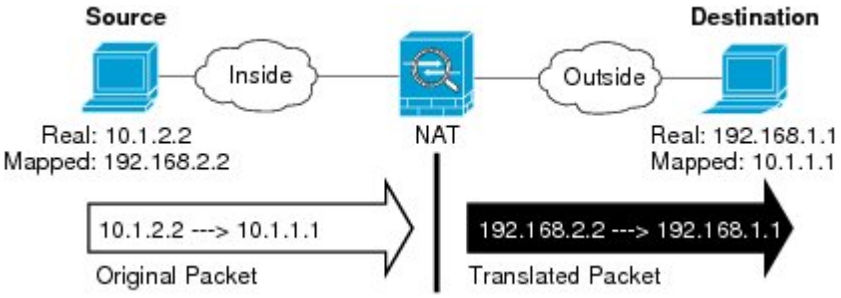
- [有効化（Enable）]：ルールをアクティブにするかどうかを指定します。ルールページの右クリックメニューを使用して、後でルールをアクティブ化または非アクティブ化することができます。
- [挿入（Insert）]：ルールを追加する場所を指定します。ルールは、カテゴリ（自動 NAT ルールの前か後）、または指定したルール番号の上か下に挿入できます。

ステップ 4 [インターフェイス オブジェクト（Interface Objects）] タブで、次のフィールドを設定します。

- [送信元インターフェイス オブジェクト（Source Interface Objects）]、[宛先インターフェイス オブジェクト（Destination Interface Objects）]：（ブリッジ グループ メンバー インターフェイスの場合に必要）。この NAT ルールを適用するインターフェイスを特定するインターフェイス オブジェクト（セキュリティ ゾーンまたはインターフェイス グループ）。[Source] は実際のインターフェイスを含むオブジェクトで、このインターフェイスを経由してトラフィックはデバイスに入ります。[宛先（Destination）] は、デバイスから出るトラフィックが通過するマッピング インターフェイスを含んでいるオブジェクトです。デフォルトでは、ルールはブリッジ グループ メンバー インターフェイスを除くすべてのインターフェイス（[Any]）に適用されます。

ステップ 5 （[変換（Translation）] タブで次を実行します）。元のパケット アドレス（IPv4 または IPv6）、つまり、元のパケットに表示されるパケット アドレスを特定します。

元のパケットと変換されたパケットの例については、次の図を参照してください。



- [Original Source][Address]：変換するアドレスを含むネットワーク オブジェクト、またはネットワーク グループ。
- [Original Destination][Address]：（オプション）。宛先アドレスを含むネットワーク オブジェクト。空白にしておくと、宛先に関わりなく発信元アドレスの変換が適用されます。宛先アドレスを指定した場合、そのアドレスにスタティック変換を設定するか、単にアイデンティティ NAT を使用できます。

  [Interface][Source Interface IP] が送信元インターフェイス（[Any] は不可）上の元の宛先に基づいて指定されるように選択できます。このオプションを選択する場合、変換済みの宛先オブジェクトも選択する必要があります。スタティック インターフェイス NAT に宛先アドレスのポート変換を実装するには、このオプションを選択し、さらにその宛先ポートの適切なポート オブジェクトを選択します。

ステップ 6 変換済みパケット アドレス（つまり、IPv4 または IPv6）を特定します。パケット アドレスは、宛先インターフェイス ネットワークに表示されます。必要に応じて、IPv4 と IPv6 の間で変換できます。

- [変換済み送信元（Translated Source）]：次のいずれかになります。

- アドレスの設定グループを使用するには、[アドレス（Address）] およびマッピングされたアドレスを含むネットワーク オブジェクトまたはグループを選択します。通常、1 対 1 のマッピングでは、実際のアドレスと同じ数のマッピング アドレスを設定します。しかし、アドレスの数が一致しない場合もあります。
- （ポート変換を設定したスタティック インターフェイス NAT）宛先インターフェイスのアドレスを使用するには、**[宛先インターフェイス IP（Destination Interface IP）]** を選択します。また特定の宛先インターフェイス オブジェクトを選択する必要もあります。インターフェイスの IPv6 アドレスを使用するには、[詳細（Advanced）] タブで [IPv6] オプションを選択する必要もあります。これはポート変換と共に、スタティック インターフェイス NAT を設定します。送信元アドレス/ポートは、インターフェイスのアドレス、および同じポート番号に変換されます。

- [変換済み宛先（Translated Destination）]：（オプション）。変換されたパケットで使用される宛先アドレスを含むネットワーク オブジェクトまたはグループ。[元の宛先（Original Destination）] を選択した場合、同じオブジェクトを選択することによって、アイデンティティ NAT（つまり変換なし）を設定できます。

ステップ 7 （任意）サービス変換の送信元サービス ポートまたは宛先サービス ポートを識別します。

ポート変換を設定したスタティック NAT を設定した場合、送信元、宛先、またはその両方のポートを変換できます。たとえば、TCP/80 と TCP/8080 間を変換できます。

NAT では、TCP または UDP だけがサポートされます。ポートを変換する場合、実際のサービス オブジェクトのプロトコルとマッピング サービス オブジェクトのプロトコルの両方が同じにします（両方とも TCP または両方とも UDP）。アイデンティティ NAT では、実際のポートとマッピング ポートの両方に同じサービス オブジェクトを使用できます。

- [元の送信元ポート（Original Source Port）]、[変換済み送信元ポート（Translated Source Port）]：送信元アドレスのポート変換を定義します。
- [元の宛先ポート（Original Destination Port）]、[変換済み宛先ポート（Translated Destination Port）]：宛先アドレスのポート変換を定義します。

ステップ 8 （オプション）[詳細（Advanced）] タブで、必要なオプションを選択します。

- [このルールに一致する DNS 応答を変換（Translate DNS replies that match this rule）]：DNS 応答の IP アドレスを変換するかどうかを指定します。マッピング インターフェイスから実際のインターフェイスに移動する DNS 応答の場合、アドレス（IPv4 A または IPv6 AAAA）レコードはマッピングされた値から実際の値に書き換えられます。反対に、実際のインターフェイスからマッピングされたインターフェイスへの DNS 応答の場合、レコードは実際の値からマッピングされた値に書き換えられます。このオプションは特殊な状況で使用され、書き換えにより A レコードと AAAA レコード間でも変換が行われる NAT64/46 変換のために必要なことがあります。詳細については、NAT を使用した DNS クエリと応答の書き換え（1551 ページ）を参照してください。このオプションはポート変換を行う場合は使用できません。
- [IPv6]：インターフェイス PAT の宛先インターフェイスの IPv6 アドレスを使用するかどうか。
- [ネット間マッピング（Net to Net Mapping）]：NAT 46 の場合、このオプションを選択して、最初の IPv4 アドレスを最初の IPv6 アドレスに変換し、2 番目を 2 番目に変換という順序で変換します。このオプションを選択しない場合、IPv4 埋め込み方式が使用されます。1 対 1 の変換の場合は、このオプションを使用する必要があります。

- [宛先インターフェイスで ARP をプロキシしない（Do not proxy ARP on Destination Interface）]：マッピング IP アドレスへの着信パケットのプロキシ ARP を無効にします。マッピング インターフェイスと同じネットワーク上のアドレスを使用した場合、システムはプロキシ ARP を使用してマッピング アドレスのすべての ARP 要求に応答することで、マッピング アドレスを宛先とするトラフィックを代行受信します。この方法では、デバイスがその他のネットワークのゲートウェイである必要がないため、ルーティングが簡略化されます。必要に応じてプロキシ ARP をディセーブルにできます。その場合は、アップストリーム ルータの適切なルートがあることを確認する必要があります。アイデンティティ NAT の場合、通常はプロキシ ARP は不要です。場合によっては接続の問題が生じることがあります。
- [単一方向（Unidirectional）]：このオプションを選択すると、宛先アドレスが発信元アドレスにトラフィックを開始しないようにできます。

ステップ 9 [保存（Save）] をクリックしてルールを追加します。

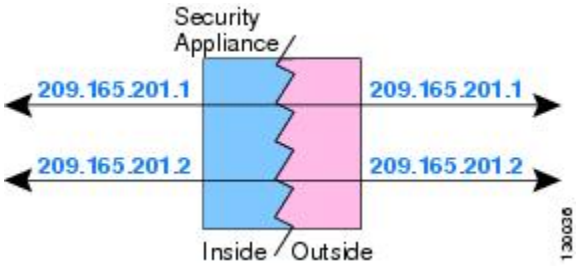
ステップ 10 NAT ページで [保存（Save）] をクリックして変更を保存します。

アイデンティティ NAT

IP アドレスを自身に変換する必要のある NAT コンフィギュレーションを設定できます。たとえば、NAT を各ネットワークに適するものの、1 つのネットワークを NAT から除外するという広範なルールを作成する場合、スタティック NAT ルールを作成して、アドレスを自身に変換することができます。

次の図に、一般的なアイデンティティ NAT のシナリオを示します。

図 *44 :* アイデンティティ *NAT*



ここでは、アイデンティティ NAT の設定方法について説明します。

アイデンティティ自動 NAT の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin Access Admin Network Admin

スタティック アイデンティティ自動 NAT ルールを使用して、アドレスの変換を防止します。つまり、自身のアドレスに変換します。

始める前に

[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] を選択し、ルールで必要なネットワーク オブジェクトまたはグループを作成します。 > または、NAT ルールを定義しているときにオブジェクトを作成することもできます。オブジェクトは次の要件を満たす必要があります。

- [元の送信元（Original Source）]：これはネットワーク オブジェクト（グループではない）でなければならず、ホスト、範囲またはサブネットも可能です。
- [変換済み送信元（Translated Source）]：元の送信元オブジェクトとコンテンツが全く同一のネットワーク オブジェクトまたはグループ。同じオブジェクトを使用できます。

ステップ 1 **[デバイス（Devices）]** > **[NAT]** の順に選択し、FTD NAT ポリシーを作成または編集します。

ステップ 2 次のいずれかを実行します。

- [ルールの追加（Add Rule）] ボタンをクリックして、新しいルールを作成します。
- [編集（edit）] アイコン（  ）をクリックして、既存のルールを編集します。

右クリック メニューにも、ルールの切り取り、コピー、貼り付け、挿入、削除オプションがあります。

ステップ 3 基本ルールのオプションを設定します。

- [NAT ルール（NAT Rule）]：[自動 NAT ルール（Auto NAT Rule）] を選択します。
- [タイプ（Type）]：[スタティック（Static）] を選択します。

ステップ 4 [インターフェイス オブジェクト（Interface Objects）] タブで、次のフィールドを設定します。

- [送信元インターフェイス オブジェクト（Source Interface Objects）]、[宛先インターフェイス オブジェクト（Destination Interface Objects）]：（ブリッジ グループ メンバー インターフェイスの場合に必要）。この NAT ルールを適用するインターフェイスを特定するインターフェイス オブジェクト（セキュリティ ゾーンまたはインターフェイス グループ）。[Source] は実際のインターフェイスを含むオブジェクトで、このインターフェイスを経由してトラフィックはデバイスに入ります。[宛先（Destination）]は、デバイスから出るトラフィックが通過するマッピング インターフェイスを含んでいるオブジェクトです。デフォルトでは、ルールはブリッジ グループ メンバー インターフェイスを除くすべてのインターフェイス（[Any]）に適用されます。

ステップ 5 [一般（General）] [変換（Translation）] タブで、次のオプションを設定します。

- [元の送信元（Original Source）]：変換するアドレスを含むネットワーク オブジェクト。
- [変換済み送信元（Translated Source）]：元の送信元と同じオブジェクト。状況に応じて、コンテンツがまったく同一の別のオブジェクトを選択できます。

アイデンティティ NAT には、[元のポート（Original Port）] オプションと [変換済みポート（Translated Port）] オプションを設定しないでください。

ステップ 6 （オプション）[詳細（Advanced）] タブで、必要なオプションを選択します。

- [このルールと一致する DNS 応答を変換（Translate DNS replies that match this rule）]：アイデンティティ NAT には、このオプションを設定しないでください。
- [IPv6]：アイデンティティ NAT にこのオプションを設定しないでください。
- [ネット マッピングへのネット（Net to Net Mapping）]：アイデンティティ NAT にこのオプションを設定しないでください。
- [宛先インターフェイスで ARP をプロキシしない（Do not proxy ARP on Destination Interface）]：マッピング IP アドレスへの着信パケットのプロキシ ARP を無効にします。マッピング インターフェイスと同じネットワーク上のアドレスを使用した場合、システムはプロキシ ARP を使用してマッピング アドレスのすべての ARP 要求に応答することで、マッピング アドレスを宛先とするトラフィックを代行受信します。この方法では、デバイスがその他のネットワークのゲートウェイである必要がないため、ルーティングが簡略化されます。必要に応じてプロキシ ARP をディセーブルにできます。その場合は、アップストリーム ルータの適切なルートがあることを確認する必要があります。アイデンティティ NAT の場合、通常はプロキシ ARP は不要です。場合によっては接続の問題が生じることがあります。
- [宛先インターフェイスのルート ルックアップの実行（Perform Route Lookup for Destination Interface）]：元の発信元アドレスと変換された発信元アドレスに同一のオブジェクトを選択する際に送信元インターフェイスと宛先インターフェイスを選択する場合、このオプションを選択すると、NAT ルールで設定された宛先インターフェイスではなくルーティング テーブルに基づいてシステムが宛先インターフェイスを決定するようにできます。

ステップ 7 [保存（Save）] をクリックしてルールを追加します。

ステップ 8 NAT ページで [保存（Save）] をクリックして変更を保存します。

アイデンティティ手動 NAT の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin Access Admin Network Admin

自動 NAT がお客様のニーズを満たしていない場合は、スタティック アイデンティティ手動 NAT ルールを使用します。たとえば、宛先に応じて異なる変換をしたい場合などです。スタティック アイデンティティ NAT ルールを使用して、アドレスの変換を防止します。つまり、自身のアドレスに変換します。

始める前に

[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] を選択し、ルールで必要なネットワーク オブジェクトまたはグループを作成します。 > IPv4 アドレスと IPv6 アドレスの両方をグループに入れることはできません。1 つのタイプだけが含まれている必要があり

ます。または、NAT ルールを定義しているときにオブジェクトを作成することもできます。またオブジェクトは次の要件も満たす必要があります。

- [元の送信元（Original Source）]：これはネットワーク オブジェクトまたはグループで、ホスト、範囲、またはサブネットを含むことができます。すべての元の送信元トラフィックを変換する場合、この手順をスキップし、ルールで [すべて（Any）] を指定します。
- [変換済み送信元（Translated Source）]：元の送信元と同じオブジェクト。オプションで、内容がまったく同じ別のオブジェクトを選択できます。

ルールで各アドレスの静的変換を設定すると、[元の宛先（Original Destination）] および [変換済み宛先（Translated Destination）] のネットワーク オブジェクトを作成できます。ポート変換を設定した宛先のスタティック インターフェイス NAT のみを設定する場合は、宛先のマッピング アドレスに対するオブジェクトの追加をスキップでき、ルールでインターフェイスを指定します。

また送信元、宛先、またはその両方のポート変換も実行できます。オブジェクト マネージャでは、元のポートと変換されたポートで使用できるポート オブジェクトがあることを確認します。アイデンティティ NAT には同じオブジェクトを使用できます。

ステップ 1 **[デバイス（Devices）] > [NAT]** の順に選択し、FTD NAT ポリシーを作成または編集します。

ステップ 2 次のいずれかを実行します。

- [ルールの追加（Add Rule）] ボタンをクリックして、新しいルールを作成します。
- [編集（edit）] アイコン（）をクリックして、既存のルールを編集します。

右クリック メニューにも、ルールの切り取り、コピー、貼り付け、挿入、削除オプションがあります。

ステップ 3 基本ルールのオプションを設定します。

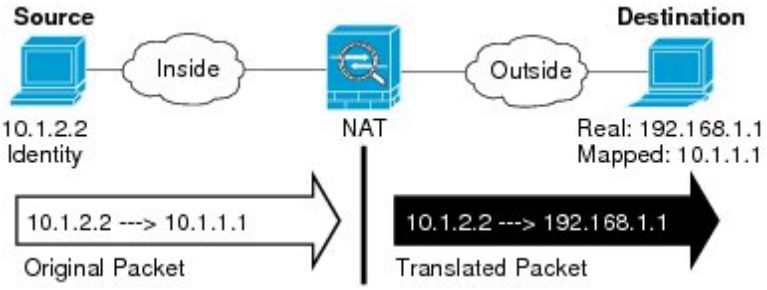
- [NAT ルール（NAT Rule）]：[手動 NAT ルール（Manual NAT Rule）] を選択します。
- [タイプ（Type）]：[スタティック（Static）] を選択します。この設定は送信元アドレスにのみ適用されます。宛先アドレスの変換を定義している場合、変換は常に静的に行われます。
- [有効化（Enable）]：ルールをアクティブにするかどうかを指定します。ルール ページの右クリック メニューを使用して、後でルールをアクティブ化または非アクティブ化することができます。
- [挿入（Insert）]：ルールを追加する場所を指定します。ルールは、カテゴリ（自動 NAT ルールの前か後）、または指定したルール番号の上か下に挿入できます。

ステップ 4 [インターフェイス オブジェクト（Interface Objects）] タブで、次のフィールドを設定します。

- [送信元インターフェイス オブジェクト（Source Interface Objects）]、[宛先インターフェイス オブジェクト（Destination Interface Objects）]：（ブリッジ グループ メンバー インターフェイスの場合に必要）。この NAT ルールを適用するインターフェイスを特定するインターフェイス オブジェクト（セキュリティ ゾーンまたはインターフェイス グループ）。[Source] は実際のインターフェイスを含むオブジェクトで、このインターフェイスを経由してトラフィックはデバイスに入ります。[宛先（Destination）] は、デバイスから出るトラフィックが通過するマッピング インターフェイスを含んでいるオブジェクトです。デフォルトでは、ルールはブリッジ グループ メンバー インターフェイスを除くすべてのインターフェイス（[Any]）に適用されます。

ステップ 5 元のパケット アドレス（IPv4 または IPv6）、つまり、元のパケットに表示されるパケット アドレスを特定します。

元のパケットと変換済みパケットの例については、次の図を参照してください。ここでは、内部ホストでアイデンティティ NAT を実行しますが、外部ホストを変換します。



- [元の送信元（Original Source）]：変換しているアドレスを含むネットワーク オブジェクトまたはグループ。
- [元の宛先（Original Destination）]：（オプション）。宛先アドレスを含むネットワーク オブジェクト。空白にしておくと、宛先に関わりなく発信元アドレスの変換が適用されます。宛先アドレスを指定した場合、そのアドレスにスタティック変換を設定するか、単にアイデンティティ NAT を使用できます。

  [インターフェイス オブジェクト（Interface Object）] を選択し、送信元インターフェイスの元の宛先（[Any] は選択不可）をベースにすることができます。このオプションを選択する場合、変換済みの宛先オブジェクトも選択する必要があります。スタティック インターフェイス NAT に宛先アドレスのポート変換を実装するには、このオプションを選択し、さらにその宛先ポートの適切なポート オブジェクトを選択します。

ステップ 6 変換済みパケット アドレス（つまり、IPv4 または IPv6）を特定します。パケット アドレスは、宛先インターフェイス ネットワークに表示されます。必要に応じて、IPv4 と IPv6 の間で変換できます。

- [変換済み送信元（Translated Source）]：元の送信元と同じオブジェクト。オプションで、内容がまったく同じ別のオブジェクトを選択できます。
- [変換済み宛先（Translated Destination）]：（オプション）。変換されたパケットで使用される宛先アドレスを含むネットワーク オブジェクトまたはグループ。[元の宛先（Original Destination）] を選択した場合、同じオブジェクトを選択することによって、アイデンティティ NAT（つまり変換なし）を設定できます。

ステップ 7 （任意）サービス変換の送信元サービス ポートまたは宛先サービス ポートを識別します。

ポート変換を設定したスタティック NAT を設定した場合、送信元、宛先、またはその両方のポートを変換できます。たとえば、TCP/80 と TCP/8080 間を変換できます。

NAT では、TCP または UDP だけがサポートされます。ポートを変換する場合、実際のサービス オブジェクトのプロトコルとマッピング サービス オブジェクトのプロトコルの両方が同じにします（両方とも TCP または両方とも UDP）。アイデンティティ NAT では、実際のポートとマッピング ポートの両方に同じサービス オブジェクトを使用できます。

- [元の送信元ポート（Original Source Port）]、[変換済み送信元ポート（Translated Source Port）]：送信元アドレスのポート変換を定義します。
- [元の宛先ポート（Original Destination Port）]、[変換済み宛先ポート（Translated Destination Port）]：宛先アドレスのポート変換を定義します。

ステップ 8 （オプション）[詳細（Advanced）] タブで、必要なオプションを選択します。

- [このルールと一致する DNS 応答を変換（Translate DNS replies that match this rule）]：アイデンティティ NAT には、このオプションを設定しないでください。
- [IPv6]：インターフェイス PAT の宛先インターフェイスの IPv6 アドレスを使用するかどうか。
- [宛先インターフェイスで ARP をプロキシしない（Do not proxy ARP on Destination Interface）]：マッピング IP アドレスへの着信パケットのプロキシ ARP を無効にします。マッピング インターフェイスと同じネットワーク上のアドレスを使用した場合、システムはプロキシ ARP を使用してマッピング アドレスのすべての ARP 要求に応答することで、マッピング アドレスを宛先とするトラフィックを代行受信します。この方法では、デバイスがその他のネットワークのゲートウェイである必要がないため、ルーティングが簡略化されます。必要に応じてプロキシ ARP をディセーブルにできます。その場合は、アップストリーム ルータの適切なルートがあることを確認する必要があります。アイデンティティ NAT の場合、通常はプロキシ ARP は不要です。場合によっては接続の問題が生じることがあります。
- [宛先インターフェイスのルートルックアップの実行（Perform Route Lookup for Destination Interface）]：元の発信元アドレスと変換された発信元アドレスに同一のオブジェクトを選択する際に送信元インターフェイスと宛先インターフェイスを選択する場合、このオプションを選択すると、NAT ルールで設定された宛先インターフェイスではなくルーティング テーブルに基づいてシステムが宛先インターフェイスを決定するようにできます。
- [単一方向（Unidirectional）]：このオプションを選択すると、宛先アドレスが発信元アドレスにトラフィックを開始しないようにできます。

ステップ 9 [保存（Save）] をクリックしてルールを追加します。

ステップ 10 NAT ページで [保存（Save）] をクリックして変更を保存します。

Firepower Threat Defense の NAT ルール プロパティ

ネットワークアドレス変換（NAT）ルールを使用して、IP アドレスを他の IP アドレスに変換します。通常は、NAT ルールを使用してプライベート アドレスをパブリックにルーティングできるアドレスに変換します。1 つのアドレスを別のアドレスに変換するか、ポート アドレス変換（PAT）を使用して多数のアドレスを 1 つまたは少数のアドレスに変換し、ポート番号を使用して送信元アドレスを識別することができます。

NAT ルールの基本的なプロパティは、次のとおりです。プロパティは、指示されていることを除き、自動 NAT ルールと手動 NAT ルールで同じです。

NAT タイプ（NAT Type）

[手動 NAT ルール（Manual NAT Rule）] または [自動 NAT ルール（Auto NAT Rule）] のどちらを設定するのかを指定します。自動 NAT は、送信元アドレスのみを変換します。宛

先アドレスに基づいた他の変換方法作成することはできません。自動 NAT のほうが設定するのが簡単なので、手動 NAT の機能を追加する必要がない限り、自動 NAT を使用してください。この 2 つの間の違いについて詳しくは、自動 NAT および 手動 NAT （1454 ページ）を参照してください。

[タイプ（Type）]

変換ルールを [ダイナミック（Dynamic）] にするか、[スタティック（Static）] にするかを指定します。ダイナミック変換では、アドレス プールからマッピング アドレスが自動的に選択されるか、または、PAT の実装時にはアドレス/ポートの組み合わせが自動的に選択されます。マッピングアドレス/ポートを明確に定義する必要がある場合は、スタティック変換を使用します。

有効化（Enable）（手動 NAT のみ）

ルールをアクティブにするかどうかを指定します。ルール ページの右クリック メニューを使用して、後でルールをアクティブ化または非アクティブ化することができます。自動 NAT ルールを無効化することはできません。

挿入（Insert）（手動 NAT のみ）

ルールを追加する場所を指定します。ルールは、カテゴリ（自動NATルールの前か後）、または指定したルール番号の上か下に挿入できます。

説明（任意、手動 NAT のみ）。

ルールの目的の説明。

以降のトピックで、NAT ルール プロパティのタブについて説明します。

インターフェイス オブジェクト：NAT のプロパティ

インターフェイス オブジェクト（セキュリティゾーンまたはインターフェイスグループ）は、NAT ルールが適用されるインターフェイスを定義します。ルーテッド モードでは、送信元と宛先の両方にデフォルトの「任意（Any）」を使用すれば、割り当てられたすべてのデバイスのすべてのインターフェイスに適用できます。ただし、通常は特定の送信元と宛先インターフェイスを選択します。

（注） 「任意」のインターフェイスの概念は、ブリッジグループ メンバー インターフェイスには適用されません。「任意の」インターフェイスを指定すると、すべてのブリッジ グループ メンバーのインターフェイスは除外されます。したがって、ブリッジ グループ メンバーに NAT を適用するには、メンバーのインターフェイスを指定する必要があります。ブリッジ仮想インターフェイス（BVI）自体に NAT を設定することはできず、メンバー インターフェイスにのみ NAT を設定できます。

インターフェイス オブジェクトを選択すると、NAT ルールはデバイスのインターフェイスが選択されたすべてのオブジェクトに含まれているときにのみ設定されます。たとえば、送信元と宛先の両方のセキュリティ ゾーンを選択すると、特定のデバイスに対して 1 つ以上のインターフェイスが両方のゾーンに含まれている必要があります。

送信元インターフェイス オブジェクト、宛先インターフェイス オブジェクト

（ブリッジ グループ メンバー インターフェイスの場合に必要）。この NAT ルールを適用するインターフェイスを特定するインターフェイス オブジェクト（セキュリティ ゾーンまたはインターフェイス グループ）。[Source] は実際のインターフェイスを含むオブジェクトで、このインターフェイスを経由してトラフィックはデバイスに入ります。[宛先（Destination）] は、デバイスから出るトラフィックが通過するマッピング インターフェイスを含んでいるオブジェクトです。デフォルトでは、ルールはブリッジ グループ メンバー インターフェイスを除くすべてのインターフェイス（[Any]）に適用されます。

自動 NAT の [変換（Translation）] プロパティ

[変換（Translation）] タブのオプションを使って発信元アドレスやマッピングされた変換アドレスを定義します。次のプロパティは、自動 NAT にのみ適用されます。

[元の送信元（Original Source）]（常に必須）。

変換しているアドレスを含むネットワーク オブジェクト。グループではなくネットワーク オブジェクトにする必要があり、ホスト、範囲、またはサブネットを含めることができます。

[変換済み送信元（Translated Source）]（通常は必須）。

変換先のマッピング アドレス。ここで選択する内容は、定義している変換ルールのタイプによって異なります。

- [ダイナミックNAT（Dynamic NAT）]：マッピング アドレスを含むネットワーク オブジェクトまたはグループ。ネットワーク オブジェクトまたはグループにできますが、サブネットを含むことはできません。グループに IPv4 アドレスと IPv6 アドレスの両方を含めることはできません。1 つのタイプだけ含める必要があります。グループに範囲とホスト IP アドレスの両方が含まれている場合、範囲はダイナミック NAT に使用され、ホスト IP アドレスは PAT のフォールバックとして使用されます。
- [ダイナミック PAT（Dynamic PAT）]：次のいずれかを実行します。
  - （インターフェイスPAT）。宛先インターフェイスのアドレスを使用するには、**[宛先インターフェイス IP（Destination Interface IP）]** を選択します。また特定の宛先インターフェイス オブジェクトを選択する必要もあります。インターフェイスのIPv6アドレスを使用するには、[詳細（Advanced）] タブで [IPv6] オプションを選択する必要もあります。PAT プールは設定しないでください。
  - 宛先インターフェイスのアドレス以外の単一アドレスを使用する場合は、そのために作成したホスト ネットワーク オブジェクトを選択します。PAT プールは設定しないでください。
  - PAT プールを使用するには、[変換された送信元（Translated Source）] を空のままにしておきます。[PAT プール（PAT Pool）] タブで PAT プール オブジェクトを選択します。
- [スタティック NAT（Static NAT）]：次のいずれかを実行します。

- アドレスの設定グループを使用するには、[アドレス（Address）]およびマッピングされたアドレスを含むネットワーク オブジェクトまたはグループを選択します。オブジェクトまたはグループに、ホスト、範囲、またはサブネットを含めることができます。通常、1対1のマッピングでは、実際のアドレスと同じ数のマッピングアドレスを設定します。しかし、アドレスの数が一致しない場合もあります。
- （ポート変換を設定したスタティック インターフェイスNAT）宛先インターフェイスのアドレスを使用するには、**[宛先インターフェイス IP（Destination Interface IP）]** を選択します。また特定の宛先インターフェイス オブジェクトを選択する必要もあります。インターフェイスの IPv6 アドレスを使用するには、[詳細（Advanced）] タブで [IPv6] オプションを選択する必要もあります。これはポート変換と共に、スタティック インターフェイス NAT を設定します。送信元アドレス/ポートは、インターフェイスのアドレス、および同じポート番号に変換されます。

- [アイデンティティ NAT（Identity NAT）]：元の送信元と同じオブジェクト。状況に応じて、コンテンツがまったく同一の別のオブジェクトを選択できます。

[元のポート（Original Port）]、[変換済みポート（Translated Port）]（スタティック NAT のみ）。

TCP または UDP ポートを変換する必要がある場合、[元のポート（Original Port）] でプロトコルを選択し、元のポートおよび変換済みポートの番号を入力します。たとえば、必要に応じて TCP/80 を 8080 に変換できます。アイデンティティ NAT にこれらのオプションを設定しないでください。

手動 NAT の [変換（Translation）] プロパティ

[変換（Translation）] タブのオプションを使って発信元アドレスやマッピングされた変換アドレスを定義します。次のプロパティは、手動 NAT にのみ適用されます。指示されている場合を除き、すべてオプションです。

[元の送信元（Original Source）]（常に必須）。

変換しているアドレスを含むネットワーク オブジェクトまたはグループ。ネットワーク オブジェクトまたはグループにすることが可能で、ホスト、範囲、またはサブネットを含めることができます。元の送信元トラフィックをすべて変換する場合は、ルールに [すべて（Any）] を指定します。

[変換済み送信元（Translated Source）]（通常は必須）。

変換先のマッピングアドレス。ここで選択する内容は、定義している変換ルールのタイプによって異なります。

- [ダイナミックNAT（Dynamic NAT）]：マッピング アドレスを含むネットワーク オブジェクトまたはグループ。ネットワーク オブジェクトまたはグループにできますが、サブネットを含むことはできません。グループに IPv4 アドレスと IPv6 アドレスの両方を含めることはできません。1 つのタイプだけ含める必要があります。グループに

範囲とホスト IP アドレスの両方が含まれている場合、範囲はダイナミック NAT に使用され、ホスト IP アドレスは PAT のフォールバックとして使用されます。

- [ダイナミック PAT（Dynamic PAT）]：次のいずれかを実行します。
  - （インターフェイス PAT）。宛先インターフェイスのアドレスを使用するには、**[宛先インターフェイス IP（Destination Interface IP）]** を選択します。また特定の宛先インターフェイス オブジェクトを選択する必要もあります。インターフェイスの IPv6 アドレスを使用するには、[詳細（Advanced）] タブで [IPv6] オプションを選択する必要もあります。PAT プールは設定しないでください。
  - 宛先インターフェイスのアドレス以外の単一アドレスを使用する場合は、そのために作成したホスト ネットワーク オブジェクトを選択します。PAT プールは設定しないでください。
  - PAT プールを使用するには、[変換された送信元（Translated Source）] を空のままにしておきます。[PAT プール（PAT Pool）] タブで PAT プール オブジェクトを選択します。
- [スタティック NAT（Static NAT）]：次のいずれかを実行します。
  - アドレスの設定グループを使用するには、[アドレス（Address）]およびマッピングされたアドレスを含むネットワーク オブジェクトまたはグループを選択します。オブジェクトまたはグループに、ホスト、範囲、またはサブネットを含めることができます。通常、1 対 1 のマッピングでは、実際のアドレスと同じ数のマッピング アドレスを設定します。しかし、アドレスの数が一致しない場合もあります。
  - （ポート変換を設定したスタティック インターフェイス NAT）宛先インターフェイスのアドレスを使用するには、**[宛先インターフェイス IP（Destination Interface IP）]** を選択します。また特定の宛先インターフェイス オブジェクトを選択する必要もあります。インターフェイスの IPv6 アドレスを使用するには、[詳細（Advanced）] タブで [IPv6] オプションを選択する必要もあります。これはポート変換と共に、スタティック インターフェイス NAT を設定します。送信元アドレス/ポートは、インターフェイスのアドレス、および同じポート番号に変換されます。
- [アイデンティティ NAT（Identity NAT）]：元の送信元と同じオブジェクト。状況に応じて、コンテンツがまったく同一の別のオブジェクトを選択できます。

[元の宛先（Original Destination）]

宛先アドレスを含むネットワーク オブジェクト。空白にしておくと、宛先に関わりなく発信元アドレスの変換が適用されます。宛先アドレスを指定した場合、そのアドレスにスタティック変換を設定するか、単にアイデンティティ NAT を使用できます。

[Interface][Source Interface IP] が送信元インターフェイス（[Any] は不可）上の元の宛先に基づいて指定されるように選択できます。このオプションを選択する場合、変換済みの宛先オブジェクトも選択する必要があります。スタティック インターフェイス NAT に宛先

アドレスのポート変換を実装するには、このオプションを選択し、さらにその宛先ポートの適切なポート オブジェクトを選択します。

[変換済みの宛先（Translated Destination）]

変換されたパケットで使用される宛先アドレスを含むネットワーク オブジェクトまたはグループ。[元の宛先（Original Destination）] を選択した場合、同じオブジェクトを選択することによって、アイデンティティ NAT（つまり変換なし）を設定できます。

[元の送信元ポート（Original Source Port）]、[変換済み送信ポート（Translated Source Port）]、[元の宛先ポート（Original Destination Port）]、[変換済み宛先ポート（Translated Destination Port）]

元のパケットおよび変換済みパケットの送信元および宛先サービスを定義するポート オブジェクト。ポートを変換したり、ポートを変換せずに同じオブジェクトを選択してサービスに対するルールの感度を向上できます。サービスを設定するときは、次のルールに注意してください。

- （ダイナミック NAT または PAT）[元の送信元ポート（Original Source Port）] および [変換済み送信元ポート（Translated Source Port）] では変換できません。宛先ポートでのみ変換できます。
- NAT では、TCP または UDP だけがサポートされます。ポートを変換する場合、実際のサービス オブジェクトのプロトコルとマッピング サービス オブジェクトのプロトコルの両方が同じにします（両方とも TCP または両方とも UDP）。アイデンティティ NAT では、実際のポートとマッピング ポートの両方に同じサービス オブジェクトを使用できます。

PAT プールの NAT プロパティ

ダイナミック NAT を設定する際に、[PAT プール（PAT Pool）] タブのプロパティを使用して、ポート アドレス変換に使用するアドレスのプールを定義できます。

PAT プールの有効化（Enable PAT Pool）

PAT に使用するアドレスのプールを設定する場合は、このオプションを選択します。

PAT

PAT プールに使用するアドレスとして、以下のいずれかを指定します。

- [アドレス（Address）]：PAT プール アドレスを定義するオブジェクト。アドレスの範囲を含むネットワーク オブジェクト、またはホスト、範囲、あるいはその両方を含むネットワーク オブジェクト グループのいずれかです。サブネットを含めることはできません。グループに IPv4 アドレスと IPv6 アドレスの両方を含めることはできません。1 つのタイプだけ含める必要があります。
- **[宛先インターフェイス IP（Destination Interface IP）]**：PAT アドレスとして使用する宛先インターフェイスを指定します。このオプションを使用する場合、特定の [宛先インターフェイス オブジェクト（Destination Interface Object）] を選択する必要があります。[すべて（Any）] を宛先インターフェイスとして使用することはできません。これは、インターフェイス PAT を実装するもう 1 つの方法です。

ラウンドロビン（Round Robin）

アドレスとポートをラウンドロビン形式で割り当てる場合。デフォルトではラウンドロビンは使用されず、1 つの PAT アドレスのポートがすべて割り当てられると次の PAT アドレスが使用されます。ラウンドロビン方式では、プール内の各 PAT アドレスから 1 つずつアドレス/ポートが割り当てられると最初のアドレスに戻り、次に 2 番目のアドレスというように順に使用されます。

拡張 PAT テーブル（Extended PAT Table）

拡張 PAT を使用する場合。拡張 PAT では、変換情報の宛先アドレスとポートを含め、IP アドレスごとではなく、サービスごとに 65535 個のポートが使用されます。通常は、PAT 変換を作成するときに宛先ポートとアドレスは考慮されないため、PAT アドレスごとに 65535 個のポートに制限されます。たとえば、拡張 PAT を使用して、192.168.1.7:23 に向かう場合の 10.1.1.1:1027 の変換、および 192.168.1.7:80 に向かう場合の 10.1.1.1:1027 の変換を作成できます。このオプションは、インターフェイス PAT またはインターフェイス PAT フォールバックで使用することはできません。

フラット ポート範囲（Flat Port Range）、予約済みポートを含める（Include Reserved Ports）

TCP/UDP ポートを割り当てる際に、ポート範囲（1024 ～ 65535）を単一のフラットな範囲として使用する場合。変換用のマッピング ポート番号を選択する場合、PAT によって、実際の送信元ポート番号が使用されます（使用可能な場合）。ただし、このオプションを設定しないと、実際のポートが使用できない場合は、デフォルトで、マッピング ポートは実際のポート番号と同じポート範囲（1 ～ 511、512 ～ 1023、および 1024 ～ 65535）から選択されます。下位範囲でポートが不足するのを回避するには、この設定を行います。1 ～ 65535 の範囲全体を使用するには、[予約済みポートを含む（Include Reserved Ports）] オプションも選択します。

詳細 NAT プロパティ

NAT を設定するとき、[詳細（Advanced）] オプションで特別なサービスを提供するプロパティを設定できます。これらのプロパティはすべてオプションであり、該当サービスが必要な場合だけに設定します。

このルールに一致する DNS 回答の変換

DNS 応答の IP アドレスを変換するかどうかを指定します。マッピング インターフェイスから実際のインターフェイスに移動する DNS 応答の場合、アドレス（IPv4 A または IPv6 AAAA）レコードはマッピングされた値から実際の値に書き換えられます。反対に、実際のインターフェイスからマッピングされたインターフェイスへの DNS 応答の場合、レコードは実際の値からマッピングされた値に書き換えられます。このオプションは特殊な状況で使用され、書き換えにより A レコードと AAAA レコード間でも変換が行われる NAT64/46 変換のために必要なことがあります。詳細については、NAT を使用した DNS クエリと応答の書き換え（1551 ページ）を参照してください。このオプションは、スタティック NAT ルールでポート変換を行っているときは利用できません。

[インターフェイス PAT（宛先インターフェイス）へのフォールスルー（Fallthrough to Interface PAT (Destination Interface)）]（ダイナミック NAT のみ）

その他のマッピングアドレスがすでに割り当てられている場合に、宛先インターフェイスの IP アドレスをバックアップ方式として使用するかどうかを指定します（インターフェイス PAT フォールバック）。このオプションは、ブリッジ グループのメンバーではない宛先インターフェイスを選択している場合にのみ使用できます。インターフェイスの IPv6 アドレスを使用するには、[IPv6] オプションも選択します。変換されたアドレスとしてすでにインターフェイス PAT を設定している場合、このオプションを選択できません。PAT プールを構成する場合も、このオプションを選択することはできません。

IPv6

インターフェイス PAT の宛先インターフェイスの IPv6 アドレスを使用するかどうか。

[ネット間マッピング（Net to Net Mapping）]（スタティック NAT のみ）

NAT 46 の場合、このオプションを選択して、最初の IPv4 アドレスを最初の IPv6 アドレスに変換し、2 番目を 2 番目に変換という順序で変換します。このオプションを選択しない場合、IPv4 埋め込み方式が使用されます。1 対 1 の変換の場合は、このオプションを使用する必要があります。

宛先インターフェイスでプロキシ ARP なし（スタティック NAT のみ）

マッピング IP アドレスへの着信パケットのプロキシ ARP を無効にします。マッピング インターフェイスと同じネットワーク上のアドレスを使用した場合、システムはプロキシ ARP を使用してマッピング アドレスのすべての ARP 要求に応答することで、マッピング アドレスを宛先とするトラフィックを代行受信します。この方法では、デバイスがその他のネットワークのゲートウェイである必要がないため、ルーティングが簡略化されます。必要に応じてプロキシ ARP をディセーブルにできます。その場合は、アップストリーム ルータの適切なルートがあることを確認する必要があります。アイデンティティ NAT の場合、通常はプロキシ ARP は不要です。場合によっては接続の問題が生じることがあります。

宛先インターフェイスでルート ルックアップを実行します（スタティック ID NAT のみ。ルーテッド モードのみ）

元の発信元アドレスと変換された発信元アドレスに同一のオブジェクトを選択する際に送信元インターフェイスと宛先インターフェイスを選択する場合、このオプションを選択すると、NAT ルールで設定された宛先インターフェイスではなくルーティング テーブルに基づいてシステムが宛先インターフェイスを決定するようにできます。

[単方向（Unidirectional）]（手動 NAT のみ、スタティック NAT のみ）。

このオプションを選択すると、宛先アドレスが発信元アドレスにトラフィックを開始しないようにできます。

IPv6 ネットワークの変換

IPv6 のみと IPv4 のみのネットワーク間でトラフィックを通過させる必要がある場合、アドレス タイプの変換に NAT を使用する必要があります。2 つの IPv6 ネットワークでも、外部ネットワークから内部アドレスを非表示にする必要がある場合もあります。

IPv6 ネットワークで次の変換タイプを使用できます。

- NAT64、NAT46：IPv6 パケットを IPv4 パケットに（またはその逆に）変換します。2 つのポリシー、IPv6 から IPv4 への変換、および IPv4 から IPv6 への変換を定義する必要があります。これは 1 つの 手動 NAT ルールで実現できますが、DNS サーバが外部ネットワークにある場合は、おそらく DNS 応答をリライトする必要があります。宛先を指定するときに 手動 NAT ルールで DNS リライトを有効にすることができないため、2 つの 自動 NAT ルールを作成することがより適切なソリューションです。

  （注） NAT46 はスタティック マッピングのみをサポートします。

- NAT66：IPv6 パケットを別の IPv6 アドレスに変換します。スタティック NAT を使用することを推奨します。ダイナミック NAT または PAT を使用できますが、IPv6 アドレスは大量にあるため、ダイナミック NAT を使用する必要がありません。

（注） NAT64 および NAT 46 は標準ルーテッドインターフェイスでのみ有効です。NAT66 はルーテッドおよびブリッジ グループ メンバーのインターフェイスの両方で有効です。

NAT64/46：IPv6 アドレスの IPv4 への変換

トラフィックが IPv6 ネットワークから IPv4 のみのネットワークにアクセスするときは、IPv6 アドレスを IPv4 アドレスに変換し、IPv4 から IPv6 へトラフィックが返される必要があります。2 つのアドレス プールを定義する必要があります。IPv4 ネットワークでの IPv6 アドレスをバインドする IPv4 アドレス プールと、IPv6 ネットワークの IPv4 アドレスをバインドする IPv6 アドレス プールです。

- NAT64 ルールの IPv4 アドレス プールは通常小さく、IPv6 クライアント アドレスとの 1 対 1 のマッピングを行うのに十分なアドレスがない可能性があります。ダイナミック PAT はダイナミックまたはスタティック NAT と比較して、より簡単に多数の IPv6 クライアント アドレスに対応できます。

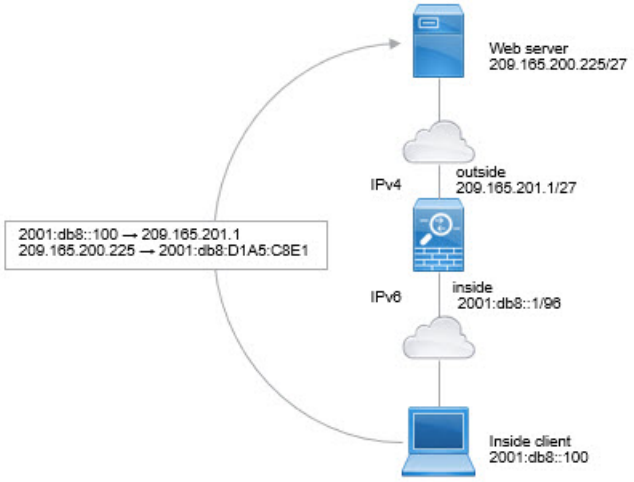
- NAT46 ルールの IPv6 アドレス プールは、マッピングされる IPv4 アドレスの数と等しいか、またはそれを超える数が可能です。これにより、各 IPv4 アドレスを異なる IPv6 アドレスにマッピングできるようになります。NAT46 はスタティック マッピングのみをサポートするため、ダイナミック PAT を使用することはできません。

送信元 IPv6 ネットワーク用と、宛先 IPv4 ネットワーク用の 2 つのポリシーを定義する必要があります。これは 1 つの 手動 NAT ルールで実現できますが、DNS サーバが外部ネットワークにある場合は、おそらく DNS 応答をリライトする必要があります。宛先を指定するときに 手動 NAT ルールで DNS リライトを有効にすることができないため、2 つの 自動 NAT ルールを作成することがより適切なソリューションです。

NAT64/46 の例：内部 IPv6 ネットワークと外部 IPv4 インターネット

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin Access Admin Network Admin

次に示すのは単純な例で、IPv6 のみの内部ネットワークがあり、インターネットに送信するトラフィックについて IPv4 に変換する必要があります。この例では DNS 変換の必要がないことを前提としています。そのため、単一の 手動 NAT ルールで NAT64 と NAT46 の両方の変換を実行できます。



この例では、外部インターフェイスの IP アドレスとダイナミック PAT インターフェイスを使用して、内部 IPv6 ネットワークを IPv4 に変換します。外部 IPv4 トラフィックは 2001:db8::/96 ネットワークのアドレスに静的に変換され、内部ネットワークでの送信が許可されます。

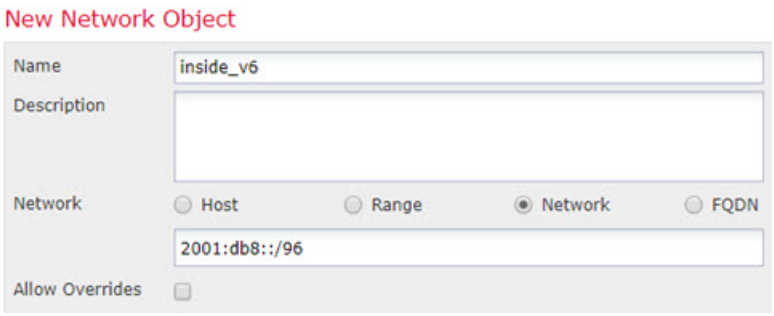
ステップ 1 内部 IPv6 ネットワークを定義するネットワーク オブジェクトを作成します。

a) **[オブジェクト（Objects）] > [オブジェクト管理（Object Management）]** を選択します。

b) コンテンツのテーブルから [ネットワーク（Network）] を選択し、**[ネットワークを追加（Add Network）] > [オブジェクトの追加（Add Object）]** をクリックします。

c) 内部 IPv6 ネットワークを定義します。

ネットワーク オブジェクトに名前（inside_v6 など）を付け、ネットワーク アドレス 2001:DB8::/96 を入力します。



d) [保存（Save）] をクリックします。

ステップ 2 IPv6 ネットワークを IPv4 に変換して再び戻すための手動 NAT ルールを作成します。

a) **[デバイス（Devices）] > [NAT]** の順に選択し、FTD NAT ポリシーを作成または編集します。

b) [ルールの追加（Add Rule）] をクリックします。

c) 次のプロパティを設定します。

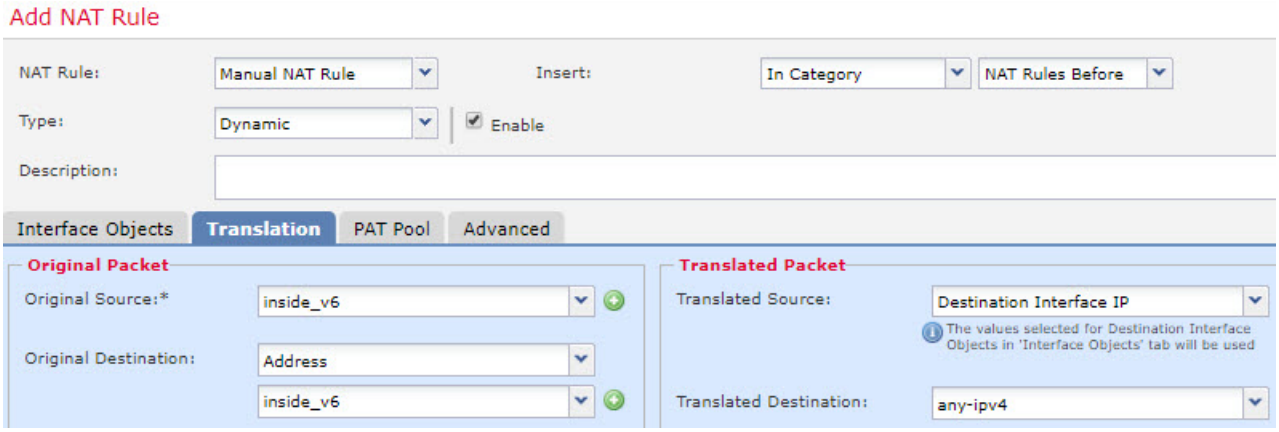
- [NAT ルール（NAT Rule）] = 手動 NAT ルール（Manual NAT Rule）。
- [タイプ（Type）] = Dynamic。

d) [インターフェイス オブジェクト（Interface Objects）] タブで、以下の設定を行います。

- [送信元インターフェイス オブジェクト（Source Interface Objects）] = inside。
- [宛先インターフェイス オブジェクト（Destination Interface Objects）] = outside。

e) [変換（Translation）] タブで、次の項目を設定します。

- [元の送信元（Original Source）] = inside_v6 ネットワーク オブジェクト。
- [変換済みの送信元（Translated Source）] = 宛先インターフェイス IP（Destination Interface IP）。
- [元の宛先（Original Destination）]：inside_v6 ネットワーク オブジェクト。
- [変換済みの宛先（Translated Destination）] = any-ipv4 ネットワーク オブジェクト。



f) [OK] をクリックします。

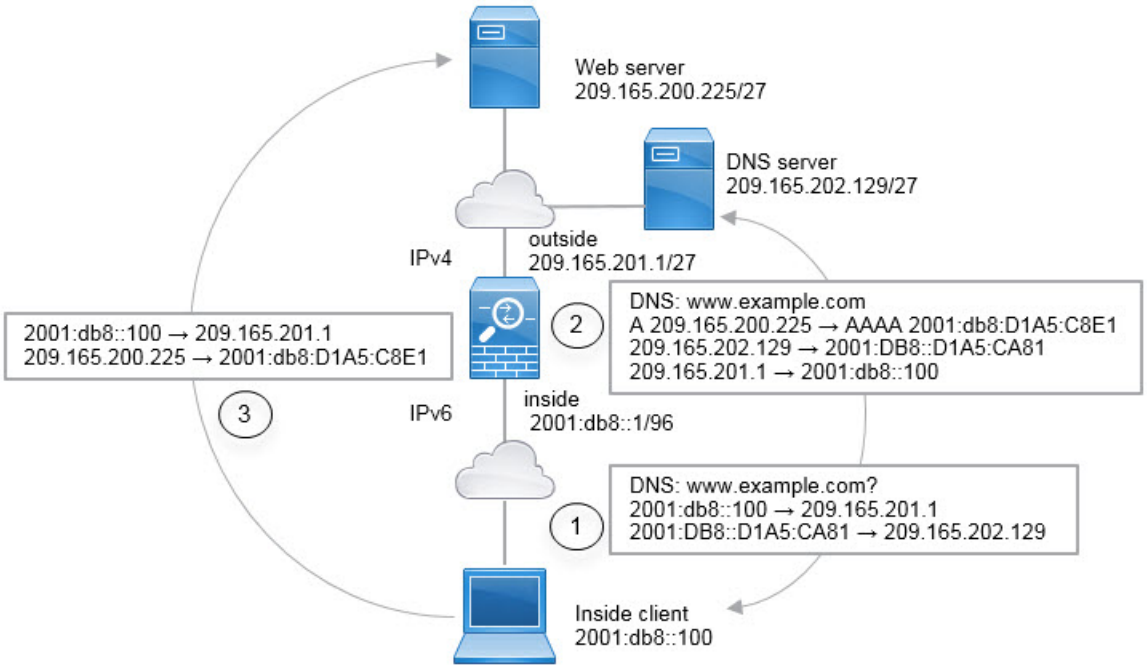
このルールにより、内部インターフェイスの 2001:db8::/96 サブネットから外部インターフェイスに向かうすべてのトラフィックが、外部インターフェイスの IPv4 アドレスを使用して NAT64 PAT 変換されます。逆に、内部インターフェイスに入る外部ネットワークの IPv4 アドレスはすべて、組み込み IPv4 アドレス方式を使用して 2001:db8::/96 ネットワーク上の 1 つのアドレスに変換されます。

g) [NATルール（NAT rule）] ページで [保存（Save）] をクリックします。

NAT64/46 の例：外部 IPv4 インターネットと DNS 変換を使用した内部 IPv6 ネットワーク

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin Access Admin Network Admin

以下は、IPv6 のみの内部ネットワークがあり、外部のインターネットに内部ユーザが必要とする IPv4 のみのサービスがある場合の代表的な例です。



この例では、外部インターフェイスの IP アドレスとダイナミック PAT インターフェイスを使用して、内部 IPv6 ネットワークを IPv4 に変換します。外部 IPv4 トラフィックは 2001:db8::/96 ネットワークのアドレスに静的に変換され、内部ネットワークでの送信が許可されます。外部 DNS サーバからの応答が A（IPv4）から AAAA（IPv6）レコードに変換され、アドレスが IPv4 から IPv6 に変換されるように、NAT46 ルールの DNS リライトを有効にします。

以下は、内部 IPv6 ネットワークの 2001:DB8::100 のクライアントが www.example.com を開こうとしている場合の、Web 要求の一般的なシーケンスです。

1. クライアント コンピュータは 2001:DB8::D1A5:CA81 の DNS サーバに DNS 要求を送信します。NAT ルールが DNS 要求の送信元と宛先に対して次の変換を行います。
   - 2001:DB8::100 から 209.165.201.1 の一意のポートへ（NAT64 インターフェイス PAT ルール）
   - 2001:DB8::D1A5:CA81 から 209.165.202.129 へ（NAT46 ルール。D1A5:CA81 は 209.165.202.129 に相当する IPv6 です）
2. DNS サーバは、www.example.com が 209.165.200.225 であることを示す A レコードを使用して応答します。DNS リライトが有効な NAT46 ルールは、A レコードを IPv6 相当の AAAA レコードに変換し、AAAA レコードで 209.165.200.225 を 2001:db8:D1A5:C8E1 に変換します。また、DNS 応答の送信元と宛先アドレスは、変換されません。
   - 209.165.202.129 から 2001:DB8::D1A5:CA81 へ
   - 209.165.201.1 から 2001:db8::100 へ
3. IPv6 クライアントは、Web サーバの IP アドレスを持つことになり、2001:db8:D1A5:C8E1 の www.example.com への HTTP 要求を作成します。（D1A5:C8E1 は 209.165.200.225 に相当する IPv6 です）HTTP 要求の送信元と宛先が次のように変換されます。
   - 2001:DB8::100 から 209.156.101.54 の一意のポートへ（NAT64 インターフェイス PAT ルール）
   - 2001:db8:D1A5:C8E1 から 209.165.200.225 へ（NAT46 ルール）

次の手順では、この例の指定方法について説明します。

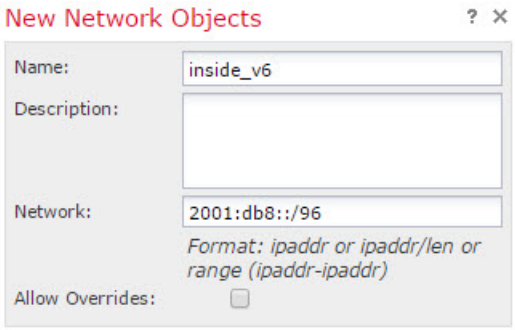
始める前に

デバイスに対応するインターフェイスが含まれているインターフェイス オブジェクト（セキュリティ ゾーンまたはインターフェイス グループ）があることを確認します。この例では、インターフェイス オブジェクトが「**inside**」および「**outside**」という名前のセキュリティ ゾーンであると仮定しています。インターフェイス オブジェクトを設定するには、**[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** を選択してから、[インターフェイス（Interface）] を選択します。

ステップ 1 内部 IPv6 ネットワークと外部 IPv4 ネットワークを定義するネットワーク オブジェクトを作成します。

a) **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** を選択します。
b) コンテンツのテーブルから [ネットワーク（Network）] を選択し、**[ネットワークを追加（Add Network）]** > **[オブジェクトの追加（Add Object）]** をクリックします。
c) 内部 IPv6 ネットワークを定義します。

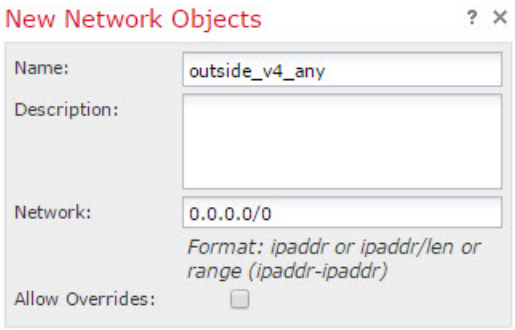
ネットワーク オブジェクトに名前（inside_v6 など）を付け、ネットワーク アドレス 2001:DB8::/96 を入力します。



d) [保存（Save）] をクリックします。

e) **[ネットワークの追加（Add Network）] > [オブジェクトの追加（Add Object）]** をクリックして、外部 IPv4 ネットワークを定義します。

ネットワーク オブジェクトに名前（たとえば、outside_v4_any）を付けて、ネットワーク アドレス 0.0.0.0/0 を入力します。



f) [保存（Save）] をクリックします。

ステップ 2 内部 IPv6 ネットワークの NAT64 ダイナミック PAT ルールを設定します。

a) **[デバイス（Devices）] > [NAT]** の順に選択し、FTD NAT ポリシーを作成または編集します。

b) [ルールの追加（Add Rule）] をクリックします。

c) 次のプロパティを設定します。

- [NAT ルール（NAT Rule）] = 自動 NAT ルール。
- [タイプ（Type）] = Dynamic。

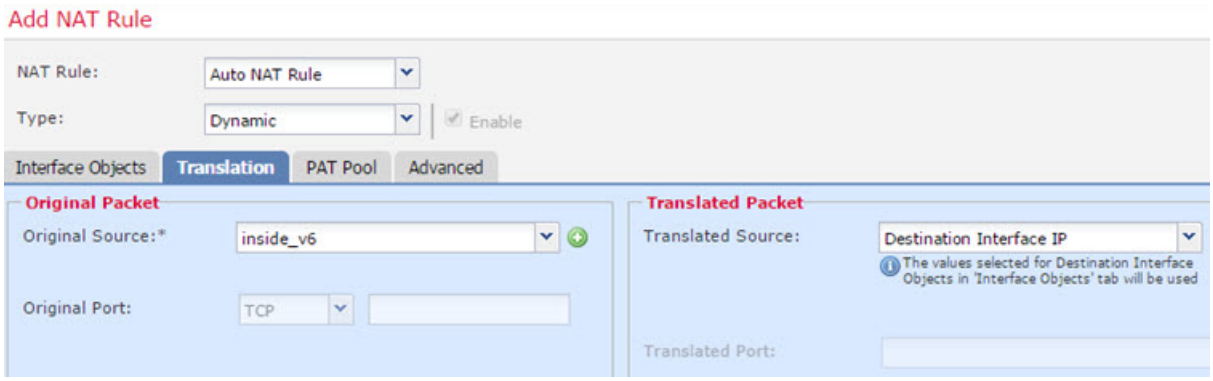
d) [インターフェイス オブジェクト（Interface Objects）] タブで、以下の設定を行います。

- [送信元インターフェイス オブジェクト（Source Interface Objects）] = inside。
- [宛先インターフェイス オブジェクト（Destination Interface Objects）] = outside。

e) [変換（Translation）] タブで、次の項目を設定します。

- [元の送信元（Original Source）] = inside_v6 ネットワーク オブジェクト。

- [変換済みの送信元（Translated Source）] = 宛先インターフェイス IP（Destination Interface IP）。



f) [OK] をクリックします。

このルールにより、内部インターフェイスの 2001:db8::/96 サブネットから外部インターフェイスへのトラフィックは、外部インターフェイスの IPv4 アドレスを使用した NAT64 PAT 変換を取得します。

ステップ 3 外部 IPv4 ネットワークのスタティック NAT46 ルールを設定します。

a) [ルールの追加（Add Rule）] をクリックします。

b) 次のプロパティを設定します。

- [NAT ルール（NAT Rule）] = 自動 NAT ルール。
- [タイプ（Type）] = Static。

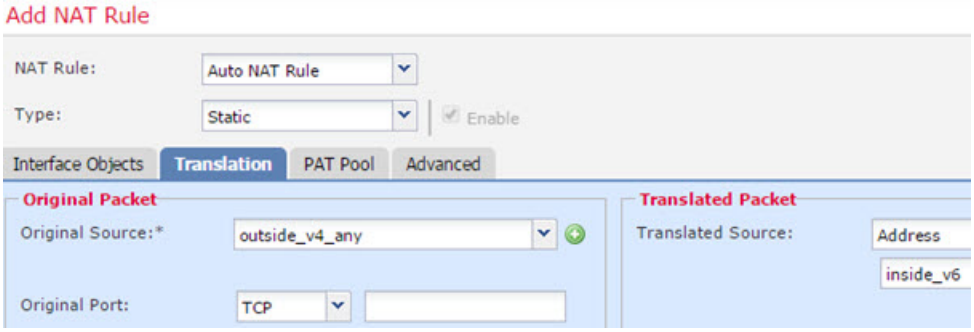
c) [インターフェイス オブジェクト（Interface Objects）] タブで、以下の設定を行います。

- [送信元インターフェイス オブジェクト（Source Interface Objects）] = outside。
- [宛先インターフェイス オブジェクト（Destination Interface Objects）] = inside。

d) [変換（Translation）] タブで、次の項目を設定します。

- [元の送信元（Original Source）] = outside_v4_any ネットワーク オブジェクト。
- **[変換済みの送信元（Translated Source）]** > **[アドレス（Address）]** = inside_v6 ネットワーク オブジェクト。

e) [詳細（Advanced）] タブで、[このルールと一致する DNS 応答を変換（Translate DNS replies that match this rule）] を選択します。



f) [OK] をクリックします。

このルールにより、内部インターフェイスに向かう外部ネットワークのすべての IPv4 アドレスは、組み込み IPv4 アドレス方式を使用して 2001:db8::/96 ネットワークのアドレスに変換されます。また、DNS 応答は A（IPv4）から AAAA（IPv6）レコードに変換され、アドレスは IPv4 から IPv6 に変換されます。

NAT66：IPv6 アドレスから別の IPv6 アドレスへの変換

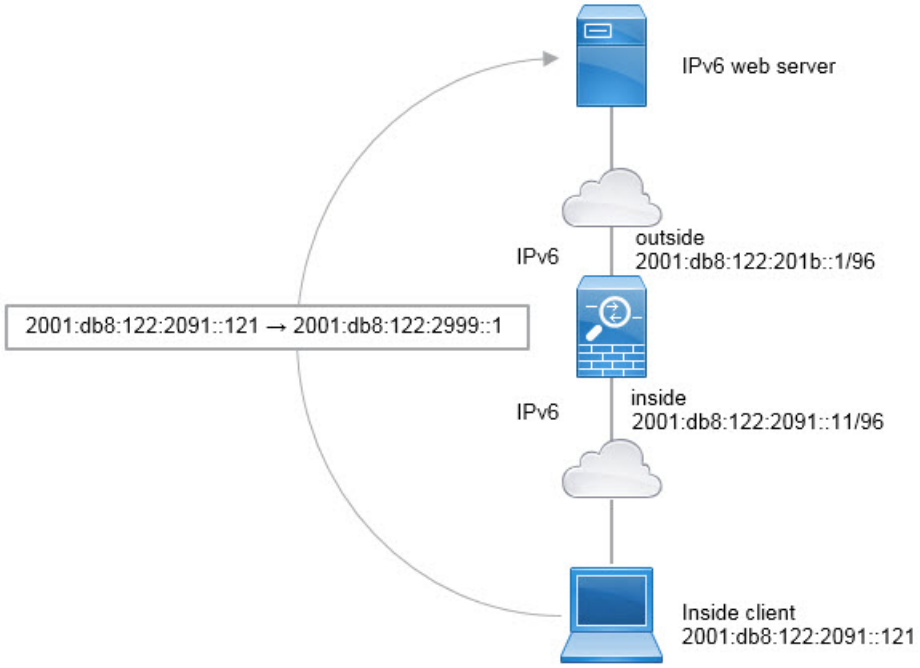
IPv6 ネットワークから別の IPv6 ネットワークへ移動するとき、そのアドレスを外部ネットワークの別の IPv6 アドレスに変換できます。スタティック NAT を使用することを推奨します。ダイナミック NAT または PAT を使用できますが、IPv6 アドレスは大量にあるため、ダイナミック NAT を使用する必要がありません。

異なるアドレス タイプの間で変換されていないため、NAT66 変換用の 1 つのルールが必要です。これらのルールは、自動 NAT を使用して簡単にモデル化することができます。ただし、リターントラフィックを許可しない場合は、手動 NAT のみを使用してスタティック NAT ルールを単方向にできます。

NAT66 の例、ネットワーク間のスタティック変換

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin Access Admin Network Admin

自動NATを使用して、IPv6アドレスプール間のスタティック変換を設定できます。次の例は、2001:db8:122:2091::/96 ネットワークの内部アドレスを、2001:db8:122:2999::/96 ネットワークの外部アドレスへ変換する方法について説明しています。



始める前に

デバイスに対応するインターフェイスが含まれているインターフェイス オブジェクト（セキュリティ ゾーンまたはインターフェイス グループ）があることを確認します。この例では、インターフェイス オブジェクトが「**inside**」および「**outside**」という名前のセキュリティ ゾーンであると仮定しています。インターフェイス オブジェクトを設定するには、**[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** を選択してから、[インターフェイス（Interface）] を選択します。

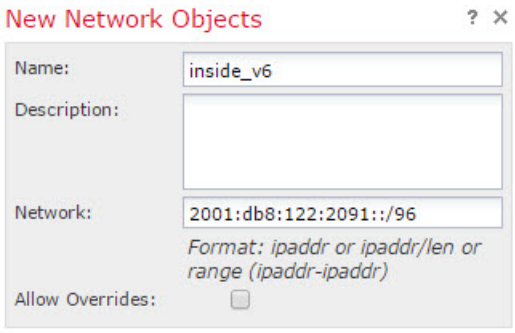
ステップ 1 内部 IPv6 ネットワークと外部 IPv6 NAT ネットワークを定義するネットワーク オブジェクトを作成します。

a) **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** を選択します。

b) コンテンツのテーブルから [ネットワーク（Network）] を選択し、**[ネットワークを追加（Add Network）]** > **[オブジェクトの追加（Add Object）]** をクリックします。

c) 内部 IPv6 ネットワークを定義します。

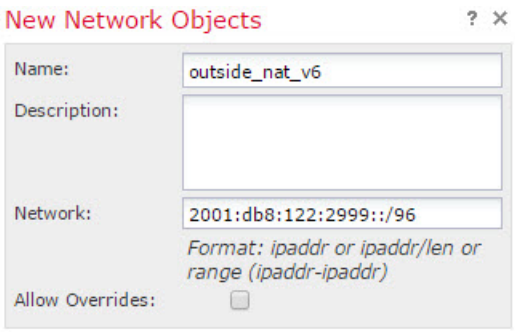
ネットワーク オブジェクトに名前（たとえば、inside_v6）を付けて、ネットワーク アドレス 2001:db8:122:2091::/96 を入力します。



d) [保存（Save）] をクリックします。

e) **[ネットワークの追加（Add Network）]** > **[オブジェクトの追加（Add Object）]** をクリックして、外部 IPv6 NAT ネットワークを定義します。

ネットワーク オブジェクトに名前（たとえば、outside_nat_v6）を付けて、ネットワーク アドレス 2001:db8:122:2999::/96 を入力します。



f) [保存（Save）] をクリックします。

ステップ 2 内部 IPv6 ネットワークのスタティック NAT ルールを設定します。

a) **[デバイス（Devices）]** > **[NAT]** の順に選択し、FTD NAT ポリシーを作成または編集します。

b) [ルールの追加（Add Rule）] をクリックします。

c) 次のプロパティを設定します。

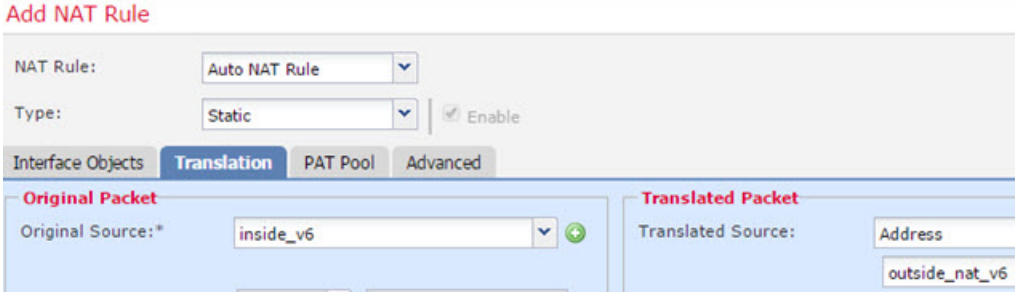
- [NAT ルール（NAT Rule）] = 自動 NAT ルール。
- [タイプ（Type）] = Static。

d) [インターフェイス オブジェクト（Interface Objects）] タブで、以下の設定を行います。

- [送信元インターフェイス オブジェクト（Source Interface Objects）] = inside。
- [宛先インターフェイス オブジェクト（Destination Interface Objects）] = outside。

e) [変換（Translation）] タブで、次の項目を設定します。

- [元の送信元（Original Source）] = inside_v6 ネットワーク オブジェクト。
- **[変換済みの送信元（Translated Source）]** > **[アドレス（Address）]** = outside_nat_v6 ネットワーク オブジェクト。



f) [OK] をクリックします。

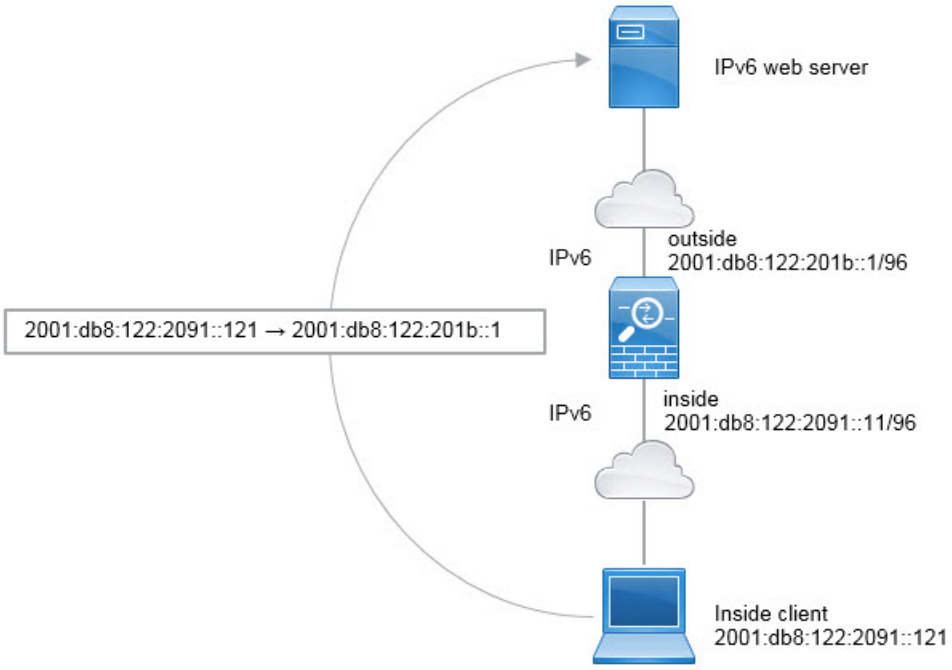
このルールにより、内部インターフェイスの 2001:db8:122:2091::/96 サブネットから外部インターフェイスへのすべてのトラフィックは、2001:db8:122:2999::/96 ネットワークのアドレスへのスタティック NAT66 変換を取得します。

NAT66 の例、シンプルな IPv6 インターフェイス PAT

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin Access Admin Network Admin

NAT66 を実装するための簡単なアプローチは、外部インターフェイス IPv6 アドレスの別のポートに内部アドレスを動的に割り当てることです。

NAT66 のインターフェイス PAT ルールを設定すると、そのインターフェイスに設定されているすべてのグローバル アドレスは、PAT のマッピングに使用されます。インターフェイスのリンクローカルまたはサイトローカル アドレスは、PAT に使用されません。



始める前に

デバイスに対応するインターフェイスが含まれているインターフェイス オブジェクト（セキュリティ ゾーンまたはインターフェイス グループ）があることを確認します。この例では、インターフェイス オブジェクトが「**inside**」および「**outside**」という名前のセキュリティ ゾーンであると仮定しています。インターフェイス オブジェクトを設定するには、**[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** を選択してから、[インターフェイス（Interface）] を選択します。

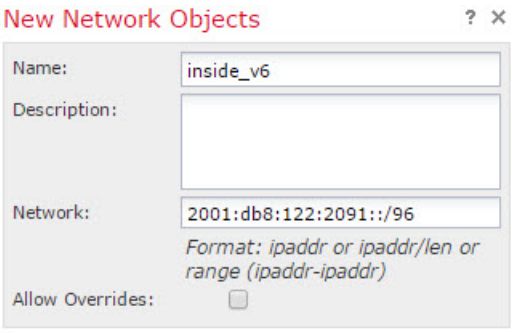
ステップ 1 内部 IPv6 ネットワークを定義するネットワーク オブジェクトを作成します。

a) **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** を選択します。

b) コンテンツのテーブルから [ネットワーク（Network）] を選択し、**[ネットワークを追加（Add Network）]** > **[オブジェクトの追加（Add Object）]** をクリックします。

c) 内部 IPv6 ネットワークを定義します。

ネットワーク オブジェクトに名前（たとえば、inside_v6）を付けて、ネットワーク アドレス 2001:db8:122:2091::/96 を入力します。



d) [保存（Save）] をクリックします。

ステップ 2 内部 IPv6 ネットワークのダイナミック PAT ルールを設定します。

a) **[デバイス（Devices）] > [NAT]** の順に選択し、FTD NAT ポリシーを作成または編集します。

b) [ルールの追加（Add Rule）] をクリックします。

c) 次のプロパティを設定します。

- [NAT ルール（NAT Rule）] = 自動 NAT ルール。
- [タイプ（Type）] = Dynamic。

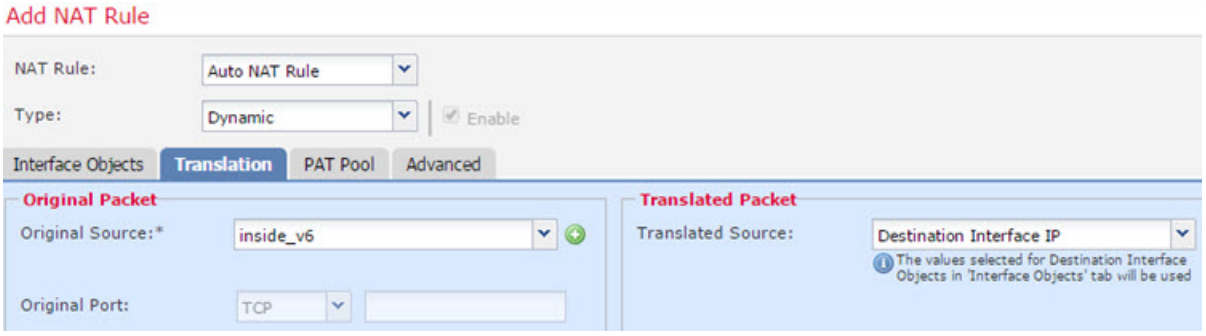
d) [インターフェイス オブジェクト（Interface Objects）] タブで、以下の設定を行います。

- [送信元インターフェイス オブジェクト（Source Interface Objects）] = inside。
- [宛先インターフェイス オブジェクト（Destination Interface Objects）] = outside。

e) [変換（Translation）] タブで、次の項目を設定します。

- [元の送信元（Original Source）] = inside_v6 ネットワーク オブジェクト。
- [変換済みの送信元（Translated Source）] = 宛先インターフェイス IP（Destination Interface IP）。

f) [詳細（Advanced）] タブで、[IPv6] を選択します。これは、宛先インターフェイスの IPv6 が使用されることを意味します。



g) [OK] をクリックします。

このルールでは、内部インターフェイスの 2001:db8:122:2091::/96 サブネットから外部インターフェイスへのトラフィックは、外部インターフェイス用に設定された IPv6 グローバル アドレスのいずれかへの NAT66 PAT 変換を取得します。

NAT のモニタリング

NAT 接続をモニタしてトラブルシューティングを実行するには、デバイス CLI にログインして次のコマンドを使用します。

- **show nat** NAT ルールとルールごとのヒット数を表示します。NAT の他の側面を表示するための追加キーワードがあります。
- **show xlate** 現在アクティブな実際の NAT 変換を表示します。
- **clear xlate** アクティブな NAT 変換を削除できます。既存の接続は接続が終了するまで古い変換スロットを継続して使用するため、NAT ルールを変更する場合はアクティブな変換を削除しなければならないことがあります。変換をクリアすると、システムは、新しいルールに基づいたクライアントの次の接続試行でクライアントの新しい変換を作成できます。

NAT の例

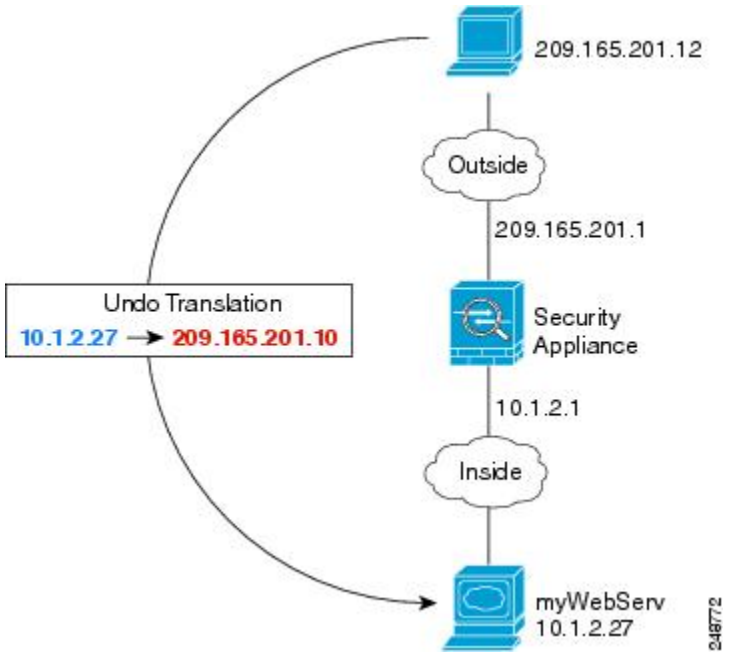
以下の各トピックでは、Threat Defense デバイスでの NAT の設定例を紹介します。

内部 Web サーバへのアクセスの提供（スタティック自動 NAT）

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin Access Admin Network Admin

次の例では、内部 Web サーバに対してスタティック NAT を実行します。実際のアドレスはプライベート ネットワーク上にあるので、パブリック アドレスが必要です。スタティック NAT は、固定アドレスにある Web サーバへのトラフィックをホストが開始できるようにするために必要です

図 *45 :* 内部 *Web* サーバのスタティック *NAT*



始める前に

Web サーバを保護するデバイスのインターフェイスが含まれているインターフェイ オブジェクト（セキュリティ ゾーンまたはインターフェイス グループ）があることを確認します。この例では、インターフェイス オブジェクトが「**inside**」および「**outside**」という名前のセキュリティ ゾーンであると仮定しています。インターフェイス オブジェクトを設定するには、**[オブジェクト（Objects）] > [オブジェクト管理（Object Management）]** を選択してから、[インターフェイス（Interface）] を選択します。

ステップ 1 サーバのプライベート ホスト アドレスとパブリック ホスト アドレスを定義するネットワーク オブジェクトを作成します。

a) **[オブジェクト（Objects）] > [オブジェクト管理（Object Management）]** を選択します。
b) コンテンツのテーブルから [ネットワーク（Network）] を選択し、**[ネットワークを追加（Add Network）] > [オブジェクトの追加（Add Object）]** をクリックします。
c) Web サーバのプライベート アドレスを定義します。

ネットワーク オブジェクトに名前（たとえば、WebServerPrivate）を付けて、実際のホスト IP アドレス 10.1.2.27 を入力します。

d) [保存（Save）] をクリックします。

e) **[ネットワークの追加（Add Network）] > [オブジェクトの追加（Add Object）]** をクリックして、パブリック アドレスを定義します。

ネットワーク オブジェクトに名前（たとえば、WebServerPublic）を付けて、ホスト アドレス 209.165.201.10 を入力します。

f) [保存（Save）] をクリックします。

ステップ 2 オブジェクトのスタティック NAT を設定します。

a) **[デバイス（Devices）] > [NAT]** の順に選択し、FTD NAT ポリシーを作成または編集します。

b) [ルールの追加（Add Rule）] をクリックします。

c) 次のプロパティを設定します。

- [NAT ルール（NAT Rule）] = 自動 NAT ルール。
- [タイプ（Type）] = Static。

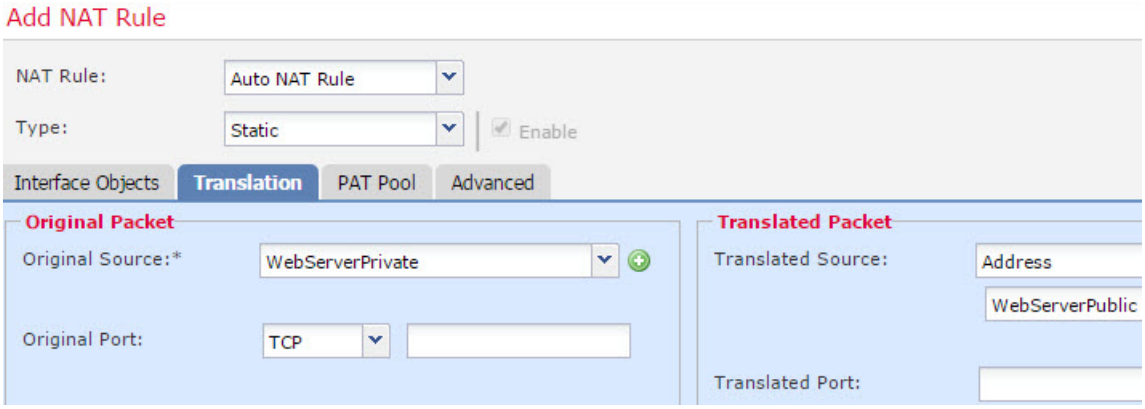
d) [インターフェイス オブジェクト（Interface Objects）] タブで、以下の設定を行います。

- [送信元インターフェイス オブジェクト（Source Interface Objects）] = inside。
- [宛先インターフェイス オブジェクト（Destination Interface Objects）] = outside。

e) [変換（Translation）] タブで、次の項目を設定します。

- [元の送信元（Original Source）] = WebServerPrivate ネットワーク オブジェクト。

- **[変換済みの送信元（Translated Source）]** > **[アドレス（Address）]** = WebServerPublic ネットワーク オブジェクト。



f) [保存（Save）] をクリックします。

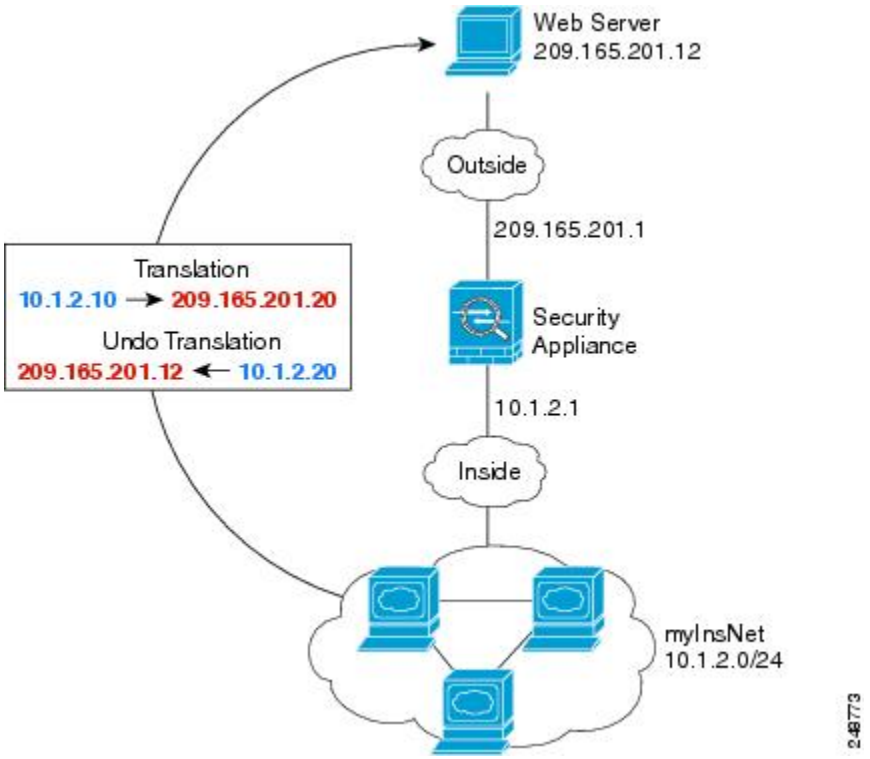
ステップ 3 [NAT ルール（NAT rule）] ページで [保存（Save）] をクリックします。

内部ホストのダイナミック自動 NAT および外部 Web サーバのスタティック NAT

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin Access Admin Network Admin

次の例では、プライベート ネットワーク上の内部ユーザが外部にアクセスする場合、このユーザにダイナミック NAT を設定します。また、内部ユーザが外部 Web サーバに接続する場合、この Web サーバのアドレスが内部ネットワークに存在するように見えるアドレスに変換されます

図 *46 :* 内部のダイナミック *NAT*、外部 *Web* サーバのスタティック *NAT*



始める前に

Web サーバを保護するデバイスのインターフェイスが含まれているインターフェイ オブジェクト（セキュリティ ゾーンまたはインターフェイス グループ）があることを確認します。この例では、インターフェイス オブジェクトが「**inside**」および「**outside**」という名前のセキュリティ ゾーンであると仮定しています。インターフェイス オブジェクトを設定するには、**[オブジェクト（Objects）] > [オブジェクト管理（Object Management）]** を選択してから、[インターフェイス（Interface）] を選択します。

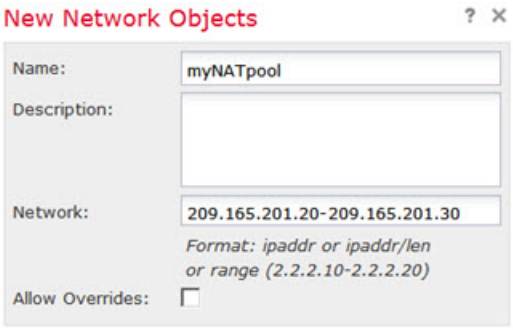
ステップ 1 内部アドレスを変換するダイナミック NAT プールのネットワーク オブジェクトを作成します。

a) **[オブジェクト（Objects）] > [オブジェクト管理（Object Management）]** を選択します。

b) コンテンツのテーブルから [ネットワーク（Network）] を選択し、**[ネットワークを追加（Add Network）] > [オブジェクトの追加（Add Object）]** をクリックします。

c) ダイナミック NAT プールを定義します。

ネットワーク オブジェクトに名前を付け（myNATpool など）、ネットワーク範囲 209.165.201.20 ～ 209.165.201.30 を入力します。

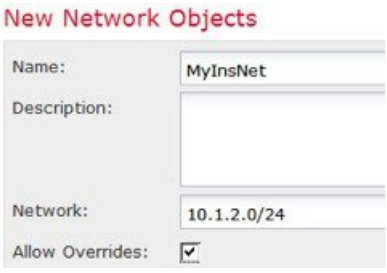


d) [保存（Save）] をクリックします。

ステップ 2 内部ネットワークのネットワーク オブジェクトを作成します。

a) **[ネットワークを追加（Add Network）] > [オブジェクトの追加（Add Object）]** をクリックします。

b) ネットワーク オブジェクトに名前を付け（MyInsNet など）、ネットワーク アドレス 10.1.2.0/24 を入力します。



c) [保存（Save）] をクリックします。

ステップ 3 外部 Web サーバのネットワーク オブジェクトを作成します。

a) **[ネットワークを追加（Add Network）] > [オブジェクトの追加（Add Object）]** をクリックします。

b) ネットワーク オブジェクトに名前を付け（MyWebServer など）、ホスト アドレス 209.165.201.12 を入力します。

c) [保存（Save）] をクリックします。

ステップ 4 変換済み Web サーバ アドレスのネットワーク オブジェクトを作成します。

a) **[ネットワークを追加（Add Network）] > [オブジェクトの追加（Add Object）]** をクリックします。

b) ネットワーク オブジェクトに名前を付け（TransWebServer など）、ホスト アドレス 10.1.2.20 を入力します。

c) [保存（Save）] をクリックします。

ステップ 5 ダイナミック NAT プール オブジェクトを使用して内部ネットワークのダイナミック NAT を設定します。

a) **[デバイス（Devices）] > [NAT]** の順に選択し、FTD NAT ポリシーを作成または編集します。

b) [ルールの追加（Add Rule）] をクリックします。

c) 次のプロパティを設定します。

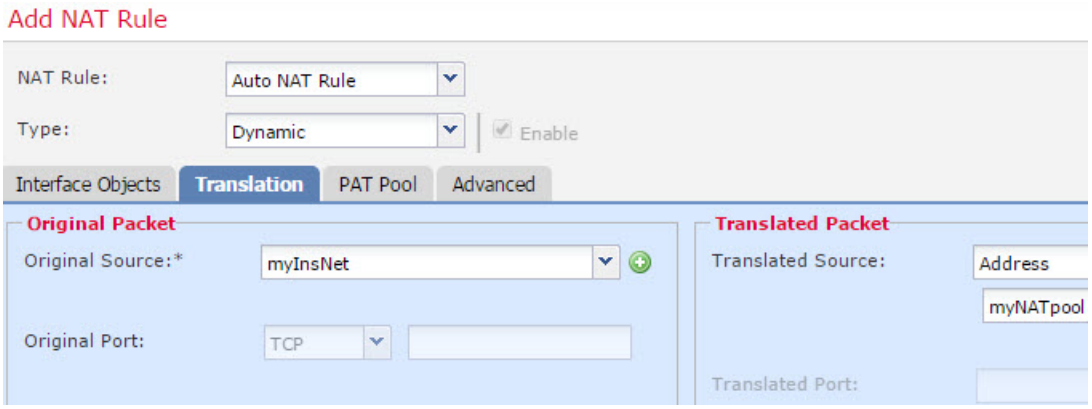
- [NAT ルール（NAT Rule）] = 自動 NAT ルール。
- [タイプ（Type）] = Dynamic。

d) [インターフェイス オブジェクト（Interface Objects）] タブで、以下の設定を行います。

- [送信元インターフェイス オブジェクト（Source Interface Objects）] = inside。
- [宛先インターフェイス オブジェクト（Destination Interface Objects）] = outside。

e) [変換（Translation）] タブで、次の項目を設定します。

- [元の発信元（Original Source）] = myInsNet ネットワーク オブジェクト。
- [変換済みの発信元アドレス（Translated Source Address）] = myNATpool ネットワーク オブジェクト。 >



f) [保存（Save）] をクリックします。

ステップ 6 Web サーバのスタティック NAT を設定します。

a) [ルールの追加（Add Rule）] をクリックします。

b) 次のプロパティを設定します。

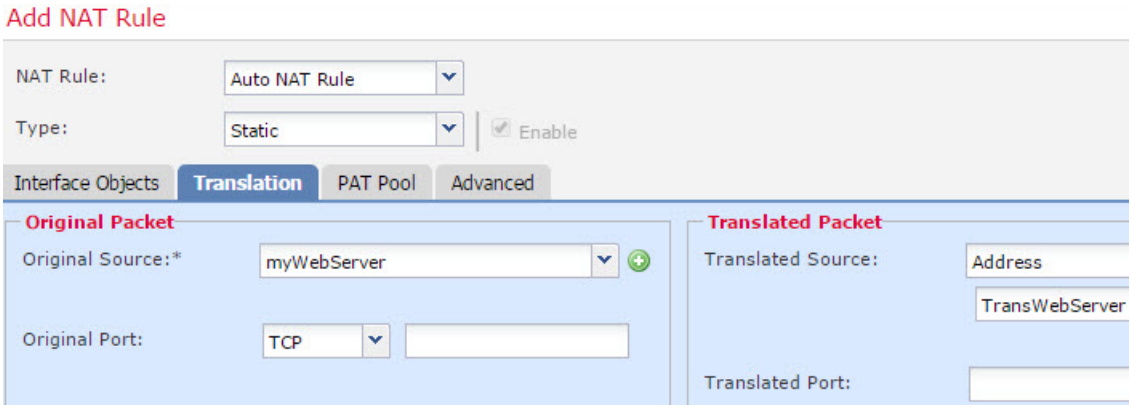
- [NAT ルール（NAT Rule）] = 自動 NAT ルール。
- [タイプ（Type）] = Static。

c) [インターフェイス オブジェクト（Interface Objects）] タブで、以下の設定を行います。

- [送信元インターフェイス オブジェクト（Source Interface Objects）] = outside。
- [宛先インターフェイス オブジェクト（Destination Interface Objects）] = inside。

d) [変換（Translation）] タブで、次の項目を設定します。

- [元の発信元（Original Source）] = myWebServer ネットワーク オブジェクト。
- [変換済みの発信元アドレス（Translated Source Address）] = TransWebServer ネットワーク オブジェクト。 >



e) [保存（Save）] をクリックします。

ステップ 7 [NAT ルール（NAT rule）] ページで [保存（Save）] をクリックします。

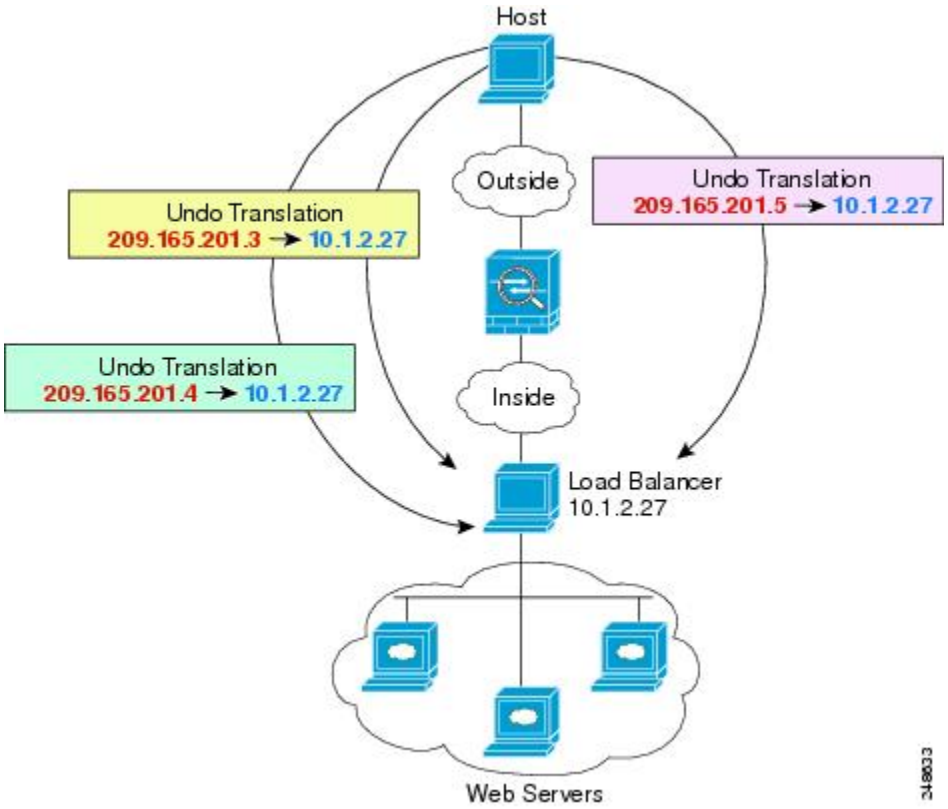
複数のマッピング アドレス（スタティック自動 NAT、1 対多）を持つ内部ロード バランサ

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin Access Admin Network Admin

次の例は、複数の IP アドレスに変換される内部ロードバランサを示します。外部ホストがマッピング IP アドレスの 1 つにアクセスする場合、1 つのロード バランサのアドレスには変換さ

れません。要求される URL に応じて、トラフィックを正しい Web サーバにリダイレクトします。

図 *47*：内部ロード バランサのスタティック *NAT*（一対多）



始める前に

Web サーバを保護するデバイスのインターフェイスが含まれているインターフェイ オブジェクト（セキュリティ ゾーンまたはインターフェイス グループ）があることを確認します。この例では、インターフェイス オブジェクトが「**inside**」および「**outside**」という名前のセキュリティ ゾーンであると仮定しています。インターフェイス オブジェクトを設定するには、**[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** を選択してから、[インターフェイス（Interface）] を選択します。

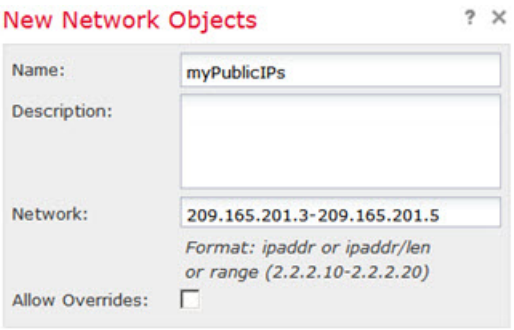
ステップ 1 ロード バランサをマッピングするアドレスに対し、ネットワーク オブジェクトを作成します。

a) **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** を選択します。

b) コンテンツのテーブルから [ネットワーク（Network）] を選択し、**[ネットワークを追加（Add Network）]** > **[オブジェクトの追加（Add Object）]** をクリックします。

c) アドレスを定義します。

ネットワーク オブジェクトに名前（たとえば、myPublicIPs）を付けて、ネットワーク範囲 209.165.201.3-209.165.201.5 を入力します。

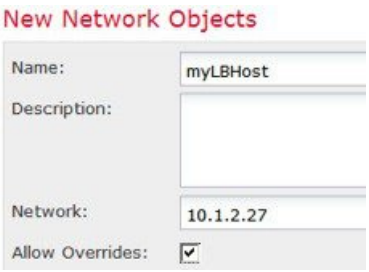


d) [保存（Save）] をクリックします。

ステップ 2 ロード バランサに対するネットワーク オブジェクトを作成します。

a) **[ネットワークの追加（Add Network）]** > **[オブジェクトの追加（Add Object）]** をクリックします。

b) ネットワーク オブジェクトに名前（たとえば、myLBHost）を付けて、ホスト アドレス 10.1.2.27 を入力します。



c) [保存（Save）] をクリックします。

ステップ 3 ロード バランサのスタティック NAT を設定します。

a) **[デバイス（Devices）]** > **[NAT]** の順に選択し、FTD NAT ポリシーを作成または編集します。

b) [ルールの追加（Add Rule）] をクリックします。

c) 次のプロパティを設定します。

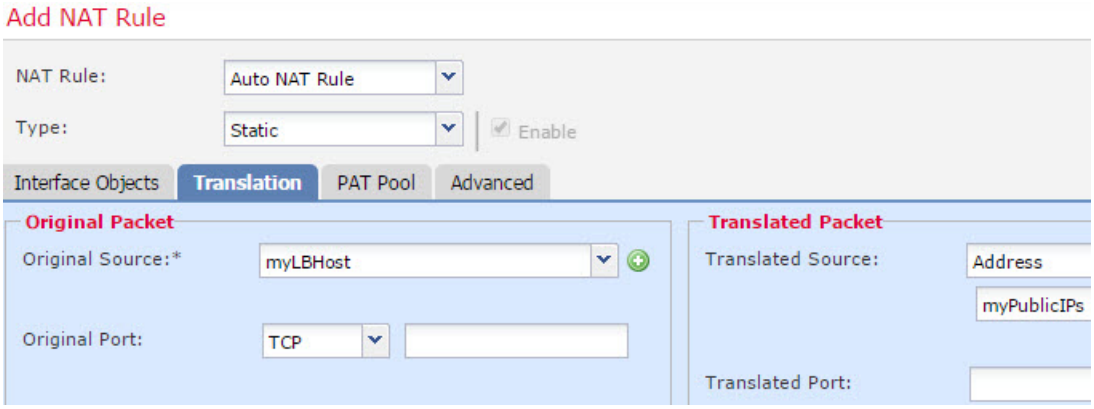
- [NAT ルール（NAT Rule）] = 自動 NAT ルール。
- [タイプ（Type）] = Static。

d) [インターフェイス オブジェクト（Interface Objects）] タブで、以下の設定を行います。

- [送信元インターフェイス オブジェクト（Source Interface Objects）] = inside。
- [宛先インターフェイス オブジェクト（Destination Interface Objects）] = outside。

e) [変換（Translation）] タブで、次の項目を設定します。

- [元の送信元（Original Source）] = myLBHost ネットワーク オブジェクト。
- **[変換済みの送信元（Translated Source）]** > **[アドレス（Address）]**= myPublicIPs ネットワーク グループ。



f) [保存（Save）] をクリックします。

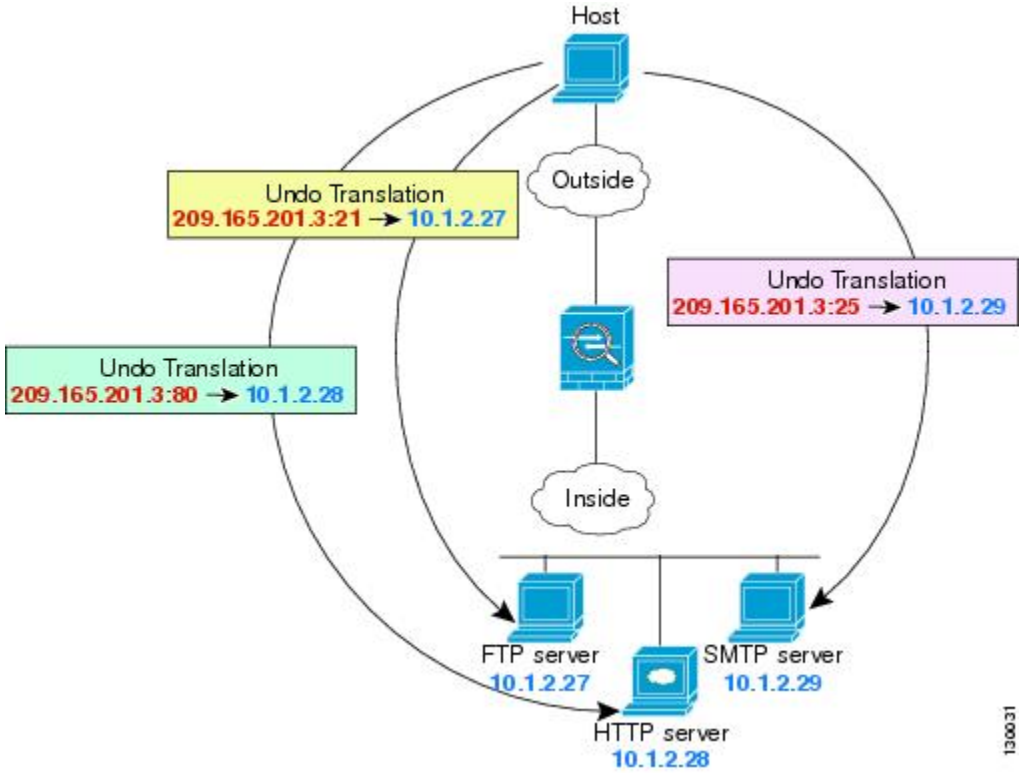
ステップ 4 [NAT ルール（NAT rule）] ページで [保存（Save）] をクリックします。

FTP、HTTP、および SMTP の単一アドレス（ポート変換を設定したスタティック自動 NAT）

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin Access Admin Network Admin

次のポート変換を設定したスタティック NAT の例では、リモート ユーザが FTP、HTTP、および SMTP にアクセスするための単一のアドレスを提供します。これらのサーバは実際には、それぞれ異なるデバイスとして実際のネットワーク上に存在しますが、ポート変換を設定したスタティック NAT ルールを指定すると、使用するマッピング IP アドレスは同じで、それぞれ別のポートを使用することができます。

図 *48 :* ポート変換を設定したスタティック *NAT*



始める前に

サーバを保護するデバイスのインターフェイスが含まれるインターフェイス オブジェクト（セキュリティ ゾーンまたはインターフェイス グループ）があることを確認します。この例では、インターフェイス オブジェクトが「**inside**」および「**outside**」という名前のセキュリティ ゾーンであると仮定しています。インターフェイス オブジェクトを設定するには、**[オブジェクト（Objects）] > [オブジェクト管理（Object Management）]** を選択してから、[インターフェイス（Interface）] を選択します。

ステップ 1 FTP サーバのネットワーク オブジェクトを作成します。

a) **[オブジェクト（Objects）] > [オブジェクト管理（Object Management）]** を選択します。

b) コンテンツのテーブルから [ネットワーク（Network）] を選択し、**[ネットワークを追加（Add Network）] > [オブジェクトの追加（Add Object）]** をクリックします。

c) ネットワーク オブジェクトに名前を付け（たとえば「FTPserver」）、FTP サーバの実際の IP アドレス（10.1.2.27）を入力します。

d) [保存（Save）] をクリックします。

ステップ 2 HTTP サーバのネットワーク オブジェクトを作成します。

a) **[ネットワークの追加（Add Network）] > [オブジェクトの追加（Add Object）]** をクリックします。

b) ネットワーク オブジェクトに名前を付け（たとえば「HTTPserver」）、ホストアドレス（10.1.2.28）を入力します。

c) [保存（Save）] をクリックします。

ステップ 3 SMTP サーバのネットワーク オブジェクトを作成します。

a) **[ネットワークの追加（Add Network）] > [オブジェクトの追加（Add Object）]** をクリックします。

b) ネットワーク オブジェクトに名前を付け（たとえば「SMTPserver」）、ホストアドレス（10.1.2.29）を入力します。

c) [保存（Save）] をクリックします。

ステップ 4 3 つのサーバに使用されるパブリック IP アドレスのネットワーク オブジェクトを作成します。

a) **[ネットワークの追加（Add Network）] > [オブジェクトの追加（Add Object）]** をクリックします。

b) ネットワーク オブジェクトに名前を付け（たとえば「ServerPublicIP」）、ホストアドレス（209.165.201.3）を入力します。

c) [保存（Save）] をクリックします。

ステップ 5 FTP サーバのポート変換を設定したスタティック NAT を設定し、FTP ポートを自身にマッピングします。

a) **[デバイス（Devices）] > [NAT]** の順に選択し、FTD NAT ポリシーを作成または編集します。

b) [ルールの追加（Add Rule）] をクリックします。

c) 次のプロパティを設定します。

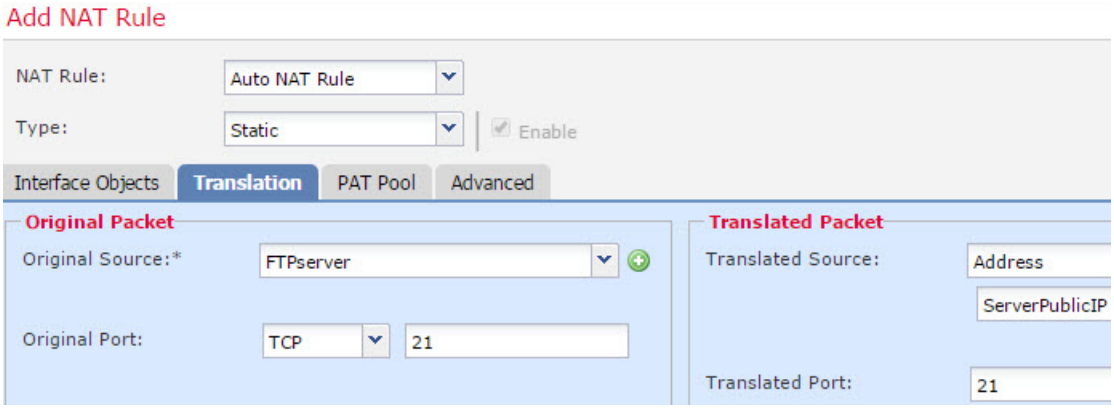
- [NAT ルール（NAT Rule）] = 自動 NAT ルール。
- [タイプ（Type）] = Static。

d) [インターフェイス オブジェクト（Interface Objects）] タブで、以下の設定を行います。

- [送信元インターフェイス オブジェクト（Source Interface Objects）] = inside。
- [宛先インターフェイス オブジェクト（Destination Interface Objects）] = outside。

e) [変換（Translation）] タブで、次の項目を設定します。

- [元の発信元（Original Source）] = FTPserver ネットワーク オブジェクト。
- **[変換済みの発信元（Translated Source）] > [アドレス（Address）]** = ServerPublicIP ネットワーク オブジェクト。
- **[元のポート（Original Port）] > [TCP]** = 21。
- **[変換済みポート（Translated Port）]** = 21。



f) [保存（Save）] をクリックします。

ステップ 6 HTTP サーバのポート変換を設定したスタティック NAT を設定し、HTTP ポートを自身にマッピングします。

a) [ルールの追加（Add Rule）] をクリックします。

b) 次のプロパティを設定します。

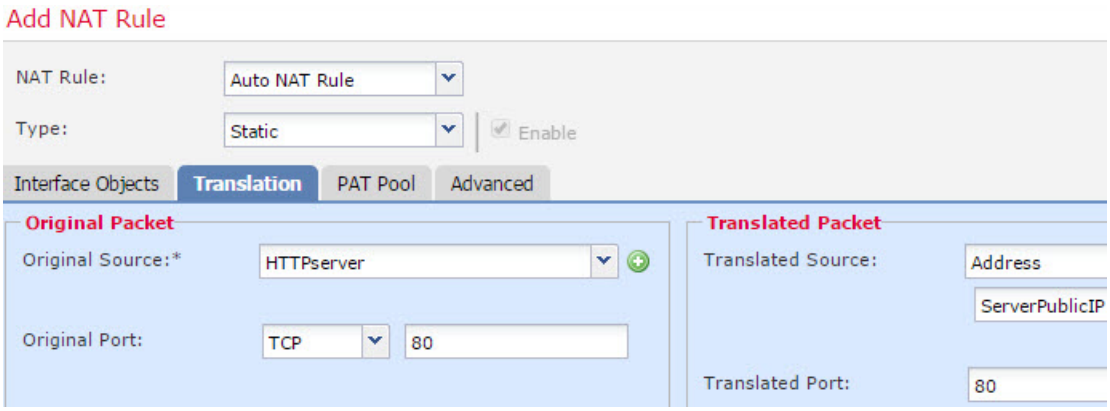
- [NAT ルール（NAT Rule）] = 自動 NAT ルール。
- [タイプ（Type）] = Static。

c) [インターフェイス オブジェクト（Interface Objects）] タブで、以下の設定を行います。

- [送信元インターフェイス オブジェクト（Source Interface Objects）] = inside。
- [宛先インターフェイス オブジェクト（Destination Interface Objects）] = outside。

d) [変換（Translation）] タブで、次の項目を設定します。

- [元の発信元（Original Source）] = HTTPserver ネットワーク オブジェクト。
- **[変換済みの発信元（Translated Source）]** > **[アドレス（Address）]** = ServerPublicIP ネットワーク オブジェクト。
- **[元のポート（Original Port）]** > **[TCP]** = 80。
- **[変換済みポート（Translated Port）]** = 80。



e) [保存（Save）] をクリックします。

ステップ 7 SMTP サーバのポート変換を設定したスタティック NAT を設定し、SMTP ポートを自身にマッピングします。

a) [ルールの追加（Add Rule）] をクリックします。

b) 次のプロパティを設定します。

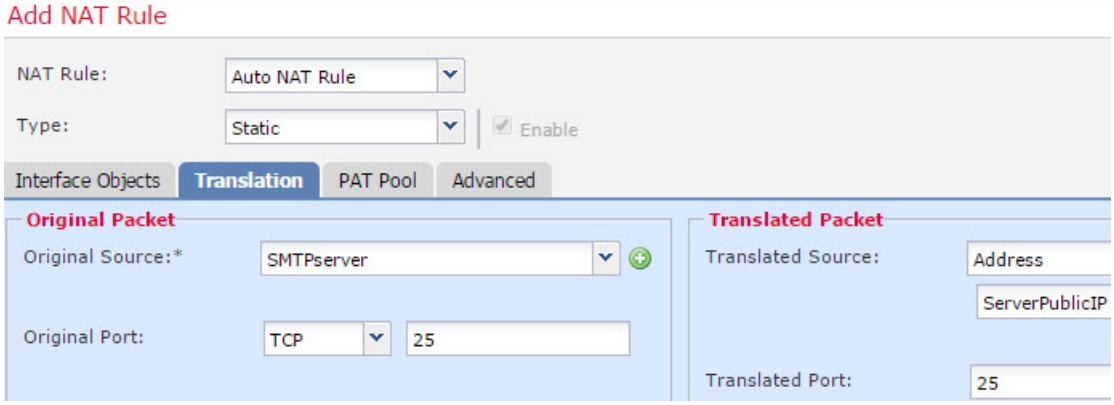
- [NAT ルール（NAT Rule）] = 自動 NAT ルール。
- [タイプ（Type）] = Static。

c) [インターフェイス オブジェクト（Interface Objects）] タブで、以下の設定を行います。

- [送信元インターフェイス オブジェクト（Source Interface Objects）] = inside。
- [宛先インターフェイス オブジェクト（Destination Interface Objects）] = outside。

d) [変換（Translation）] タブで、次の項目を設定します。

- [元の発信元（Original Source）] = SMTPserver ネットワーク オブジェクト。
- **[変換済みの発信元（Translated Source）]** > **[アドレス（Address）]** = ServerPublicIP ネットワーク オブジェクト。
- **[元のポート（Original Port）]** > **[TCP]** = 25。
- **[変換済みポート（Translated Port）]** = 25。



e) [保存（Save）] をクリックします。

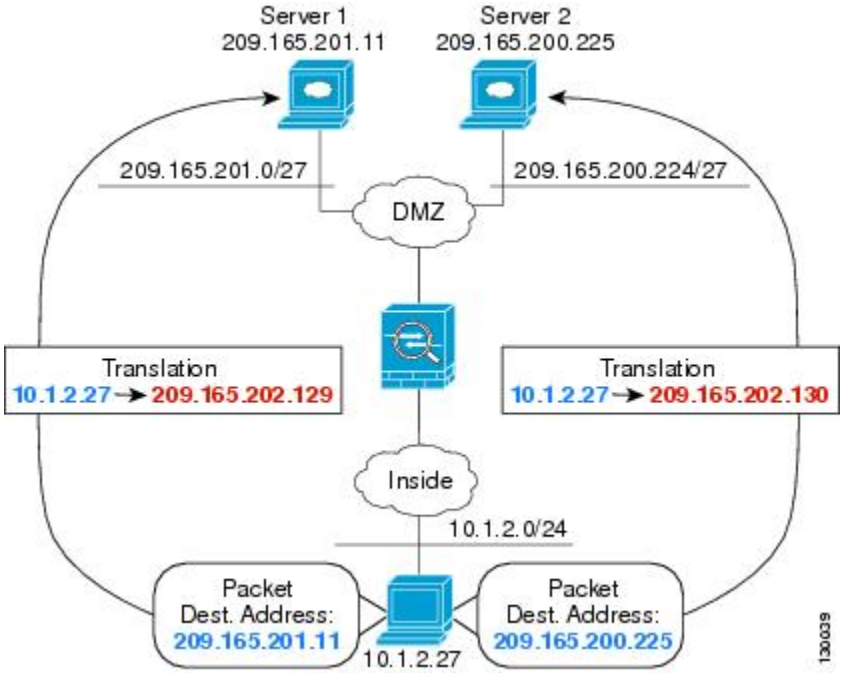
ステップ 8 [NAT ルール（NAT rule）] ページで [保存（Save）] をクリックします。

宛先に応じて異なる変換（ダイナミック手動 PAT）

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin Access Admin Network Admin

次の図に、2 台の異なるサーバにアクセスしている 10.1.2.0/24 ネットワークのホストを示します。ホストがサーバ 209.165.201.11 にアクセスすると、実際のアドレスは 209.165.202.129:ポートに変換されます。ホストがサーバ 209.165.200.225 にアクセスすると、実際のアドレスは 209.165.202.130:ポートに変換されます。

図 *49 :* 異なる宛先アドレスを使用する手動 *NAT*



始める前に

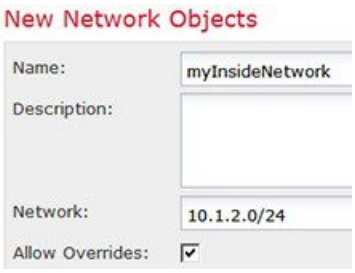
サーバを保護するデバイスのインターフェイスが含まれるインターフェイス オブジェクト（セキュリティ ゾーンまたはインターフェイス グループ）があることを確認します。この例では、インターフェイス オブジェクトは「**inside**」および「**dmz**」という名前のセキュリティ ゾーンであると仮定しています。インターフェイス オブジェクトを設定するには、**[オブジェクト（Objects）] > [オブジェクト管理（Object Management）]** を選択し、[インターフェイス（Interface）] を選択します。

ステップ 1 内部ネットワークのネットワーク オブジェクトを作成します。

a) **[オブジェクト（Objects）] > [オブジェクト管理（Object Management）]** を選択します。

b) コンテンツのテーブルから [ネットワーク（Network）] を選択し、**[ネットワークを追加（Add Network）] > [オブジェクトの追加（Add Object）]** をクリックします。

c) ネットワーク オブジェクトに名前を付け（myInsideNetwork など）、実際のネットワーク アドレス 10.1.2.0/24 を入力します。

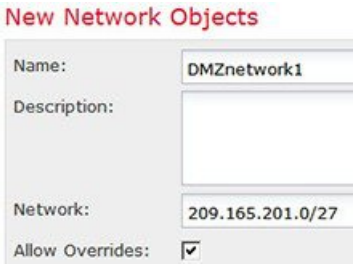


d) [保存（Save）] をクリックします。

ステップ 2 DMZ ネットワーク 1 のネットワーク オブジェクトを作成します。

a) **[ネットワークを追加（Add Network）] > [オブジェクトの追加（Add Object）]** をクリックします。

b) ネットワーク オブジェクトに名前を付け（DMZnetwork1 など）、ネットワーク アドレス 209.165.201.0/27 を入力します（255.255.255.224 のサブネット マスク）。



c) [保存（Save）] をクリックします。

ステップ 3 DMZ ネットワーク 1 の PAT アドレスのネットワーク オブジェクトを作成します。

a) **[ネットワークを追加（Add Network）] > [オブジェクトの追加（Add Object）]** をクリックします。

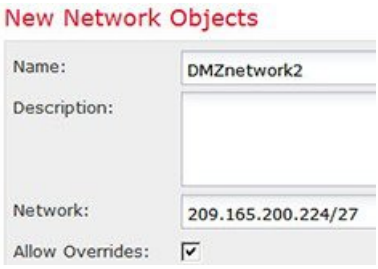
b) ネットワーク オブジェクトに名前を付け（PATaddress1 など）、ホスト アドレス 209.165.202.129 を入力します。

c) [保存（Save）] をクリックします。

ステップ 4 DMZ ネットワーク 2 のネットワーク オブジェクトを作成します。

a) **[ネットワークを追加（Add Network）] > [オブジェクトの追加（Add Object）]** をクリックします。

b) ネットワーク オブジェクトに名前を付け（DMZnetwork2 など）、ネットワーク アドレス 209.165.200.224/27 を入力します（255.255.255.224 のサブネット マスク）。



c) [保存（Save）] をクリックします。

ステップ 5 DMZ ネットワーク 2 の PAT アドレスのネットワーク オブジェクトを作成します。

a) **[ネットワークを追加（Add Network）]** > **[オブジェクトの追加（Add Object）]** をクリックします。
b) ネットワーク オブジェクトに名前を付け（PATaddress2 など）、ホスト アドレス 209.165.202.130 を入力します。

c) [保存（Save）] をクリックします。

ステップ 6 DMZ ネットワーク 1 のダイナミック手動 PAT を設定します。

a) **[デバイス（Devices）]** > **[NAT]** の順に選択し、FTD NAT ポリシーを作成または編集します。
b) [ルールの追加（Add Rule）] をクリックします。
c) 次のプロパティを設定します。

- [NAT ルール（NAT Rule）] = 手動 NAT ルール（Manual NAT Rule）。
- [タイプ（Type）] = Dynamic。

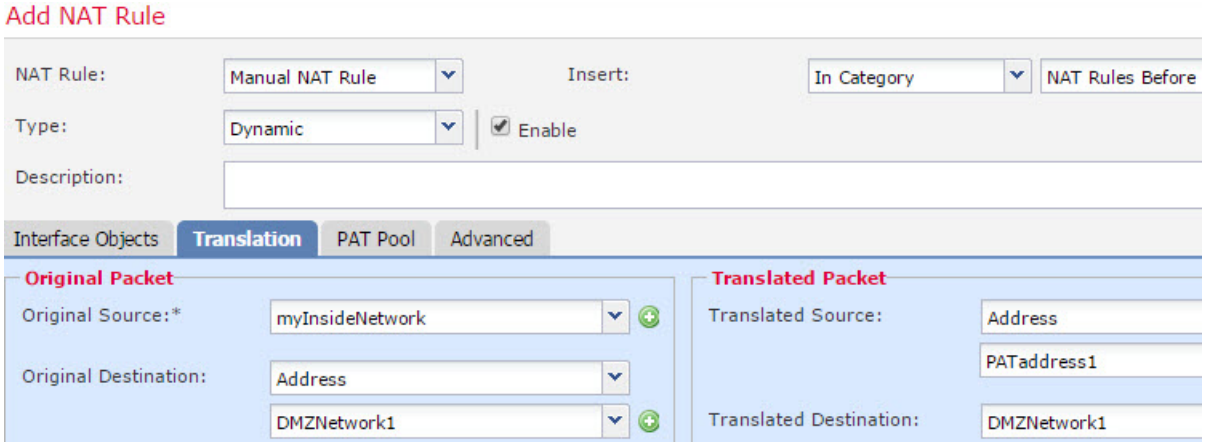
d) [インターフェイス オブジェクト（Interface Objects）] タブで、以下の設定を行います。

- [送信元インターフェイス オブジェクト（Source Interface Objects）] = inside。
- [宛先インターフェイス オブジェクト（Destination Interface Objects）] = dmz。

e) [変換（Translation）] タブで、次の項目を設定します。

- [元の発信元（Original Source）] = myInsideNetwork ネットワーク オブジェクト。
- [変換済みの発信元アドレス（Translated Source Address）] > = PATaddress1 ネットワーク オブジェクト。
- [元の宛先アドレス（Original Destination Address）] = DMZnetwork1 ネットワーク オブジェクト。 >
- [変換済みの宛先（Translated Destination）] = DMZnetwork1 ネットワーク オブジェクト。

（注） 宛先アドレスは変換しないため、元の宛先アドレスと変換された宛先アドレスに同じアドレスを指定することによって、アイデンティティ NAT を設定する必要があります。[ポート（Port）] フィールドはすべて空白のままにします。



f) [保存（Save）] をクリックします。

ステップ 7 DMZ ネットワーク 2 のダイナミック手動 PAT を設定します。

a) [ルールの追加（Add Rule）] をクリックします。

b) 次のプロパティを設定します。

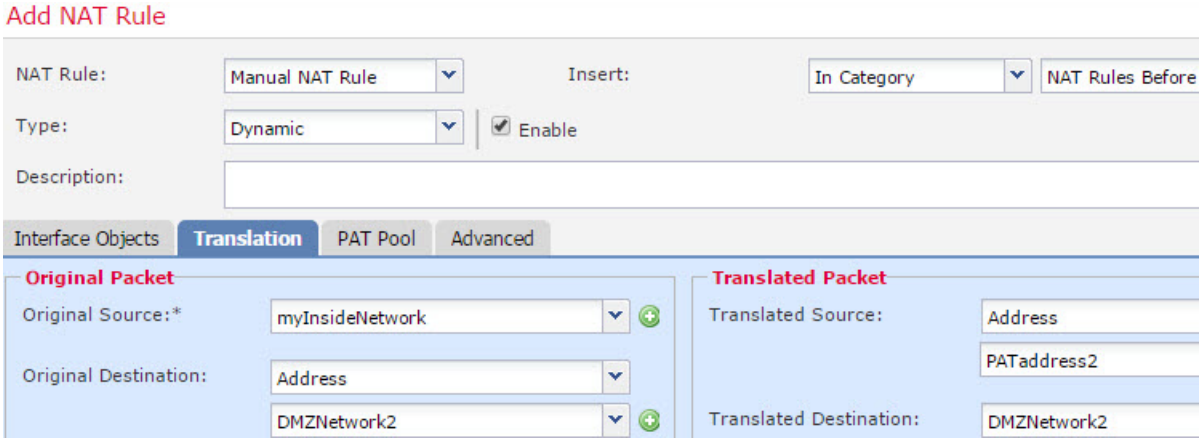
- [NAT ルール（NAT Rule）] = 手動 NAT ルール（Manual NAT Rule）。
- [タイプ（Type）] = Dynamic。

c) [インターフェイス オブジェクト（Interface Objects）] タブで、以下の設定を行います。

- [送信元インターフェイス オブジェクト（Source Interface Objects）] = inside。
- [宛先インターフェイス オブジェクト（Destination Interface Objects）] = dmz。

d) [変換（Translation）] タブで、次の項目を設定します。

- [元の発信元（Original Source）] = myInsideNetwork ネットワーク オブジェクト。
- [変換済みの発信元アドレス（Translated Source Address）] = PATaddress2 ネットワーク オブジェクト。 >
- [元の宛先アドレス（Original Destination Address）] = DMZnetwork2 ネットワーク オブジェクト。 >
- [変換済みの宛先（Translated Destination）] = DMZnetwork2 ネットワーク オブジェクト。



e) [保存（Save）] をクリックします。

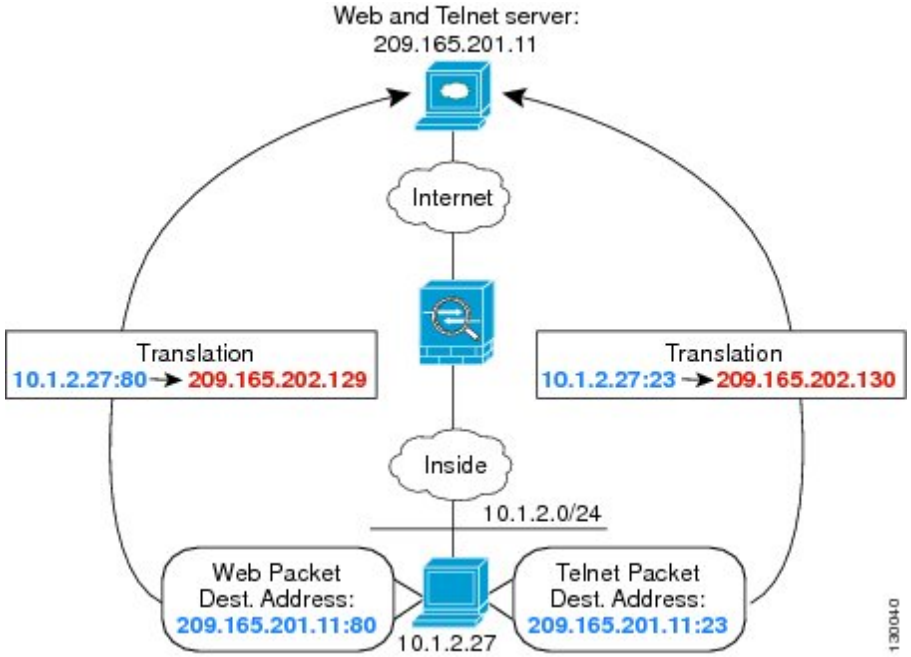
ステップ 8 [NAT ルール（NAT rule）] ページで [保存（Save）] をクリックします。

宛先アドレスおよびポートに応じて異なる変換（ダイナミック手動 PAT）

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin Access Admin Network Admin

次の図に、送信元ポートおよび宛先ポートの使用例を示します。10.1.2.0/24 ネットワークのホストは Web サービスと Telnet サービスの両方を提供する 1 つのホストにアクセスします。ホストが Telnet サービスを求めてサーバにアクセスすると、実際のアドレスは 209.165.202.129:*port* に変換されます。ホストが Web サービスを求めて同じサーバにアクセスすると、実際のアドレスは 209.165.202.130:*port* に変換されます。

図 *50 :* 異なる宛先ポートを使用する手動 *NAT*



始める前に

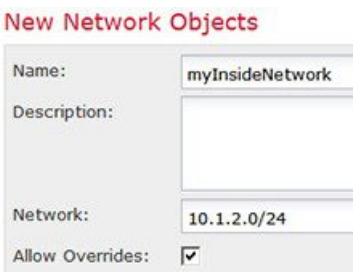
サーバを保護するデバイスのインターフェイスが含まれるインターフェイス オブジェクト（セキュリティ ゾーンまたはインターフェイス グループ）があることを確認します。この例では、インターフェイス オブジェクトは「**inside**」および「**dmz**」という名前のセキュリティ ゾーンであると仮定しています。インターフェイス オブジェクトを設定するには、**[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** を選択し、[インターフェイス（Interface）] を選択します。

ステップ 1 内部ネットワークのネットワーク オブジェクトを作成します。

a) **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** を選択します。

b) コンテンツのテーブルから [ネットワーク（Network）] を選択し、**[ネットワークを追加（Add Network）]** > **[オブジェクトの追加（Add Object）]** をクリックします。

c) ネットワーク オブジェクトに名前を付け（myInsideNetwork など）、実際のネットワーク アドレス 10.1.2.0/24 を入力します。



d) [保存（Save）] をクリックします。

ステップ 2 Telnet/Web サーバのネットワーク オブジェクトを作成します。

a) **[ネットワークを追加（Add Network）] > [オブジェクトの追加（Add Object）]** をクリックします。

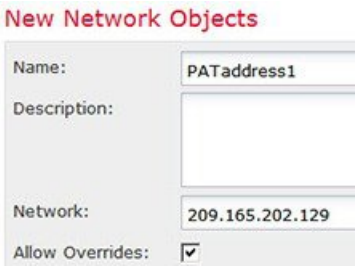
b) ネットワーク オブジェクトに名前を付け（TelnetWebServer など）、ホスト アドレス 209.165.201.11 を入力します。

c) [保存（Save）] をクリックします。

ステップ 3 Telnet を使用するときは、PAT アドレスのネットワーク オブジェクトを作成します。

a) **[ネットワークを追加（Add Network）] > [オブジェクトの追加（Add Object）]** をクリックします。

b) ネットワーク オブジェクトに名前を付け（PATaddress1 など）、ホスト アドレス 209.165.202.129 を入力します。

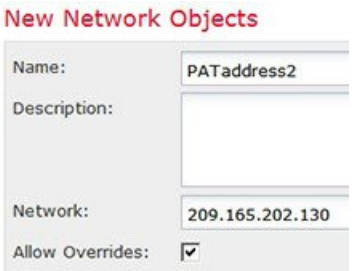


c) [保存（Save）] をクリックします。

ステップ 4 HTTP を使用するときは、PAT アドレスのネットワーク オブジェクトを作成します。

a) **[ネットワークを追加（Add Network）] > [オブジェクトの追加（Add Object）]** をクリックします。

b) ネットワーク オブジェクトに名前を付け（PATaddress2 など）、ホスト アドレス 209.165.202.130 を入力します。

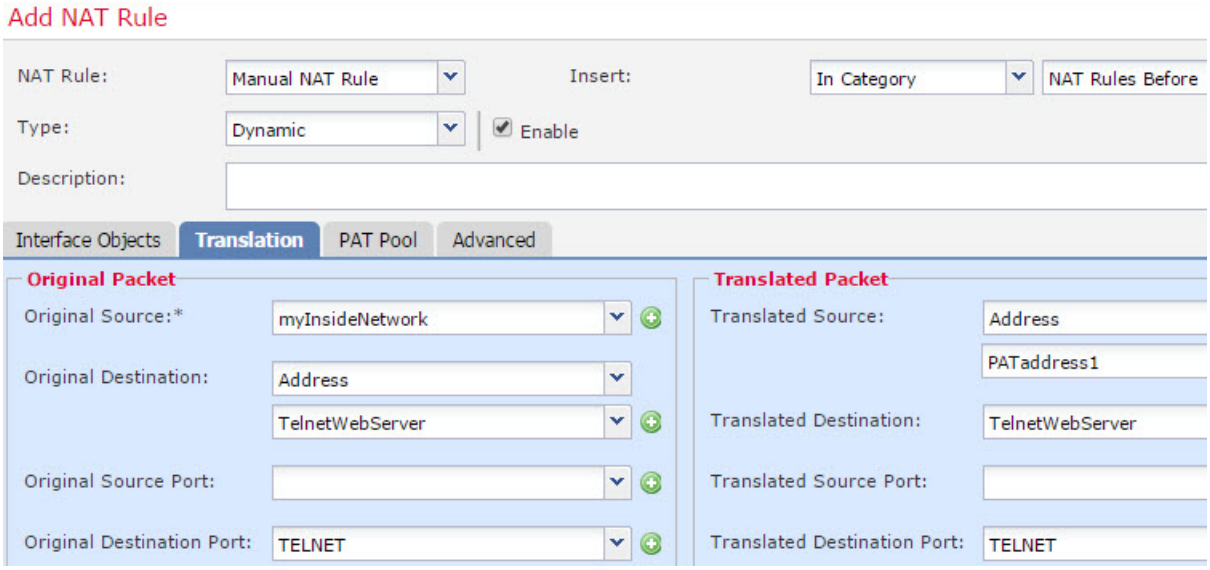


c) [保存（Save）] をクリックします。

ステップ 5 Telnet アクセスのダイナミック手動 PAT を設定します。

a) **[デバイス（Devices）]** > **[NAT]** の順に選択し、FTD NAT ポリシーを作成または編集します。
b) [ルールの追加（Add Rule）] をクリックします。
c) 次のプロパティを設定します。
   - [NAT ルール（NAT Rule）] = 手動 NAT ルール（Manual NAT Rule）。
   - [タイプ（Type）] = Dynamic。
d) [インターフェイス オブジェクト（Interface Objects）] タブで、以下の設定を行います。
   - [送信元インターフェイス オブジェクト（Source Interface Objects）] = inside。
   - [宛先インターフェイス オブジェクト（Destination Interface Objects）] = dmz。
e) [変換（Translation）] タブで、次の項目を設定します。
   - [元の発信元（Original Source）] = myInsideNetwork ネットワーク オブジェクト。
   - [変換済みの発信元アドレス（Translated Source Address）] > = PATaddress1 ネットワーク オブジェクト。
   - [元の宛先アドレス（Original Destination Address）] = TelnetWebServer ネットワーク オブジェクト。 >
   - [変換済みの宛先（Translated Destination）] = TelnetWebServer ネットワーク オブジェクト。
   - [元の宛先ポート（Original Destination Port）] = TELNET ポート オブジェクト（システム定義）。
   - [変換済みの宛先ポート（Translated Destination Port）] = TELNET ポート オブジェクト（システム定義）。

     （注） 宛先アドレスまたはポートを変換しないため、元のアドレスと変換済みの宛先アドレスに同じアドレスを指定し、元のポートと変換済みのポートに同じポートを指定することによって、アイデンティティ NAT を設定する必要があります。



f) [保存（Save）] をクリックします。

ステップ 6 Web アクセスのダイナミック手動 PAT を設定します。

a) [ルールの追加（Add Rule）] をクリックします。

b) 次のプロパティを設定します。

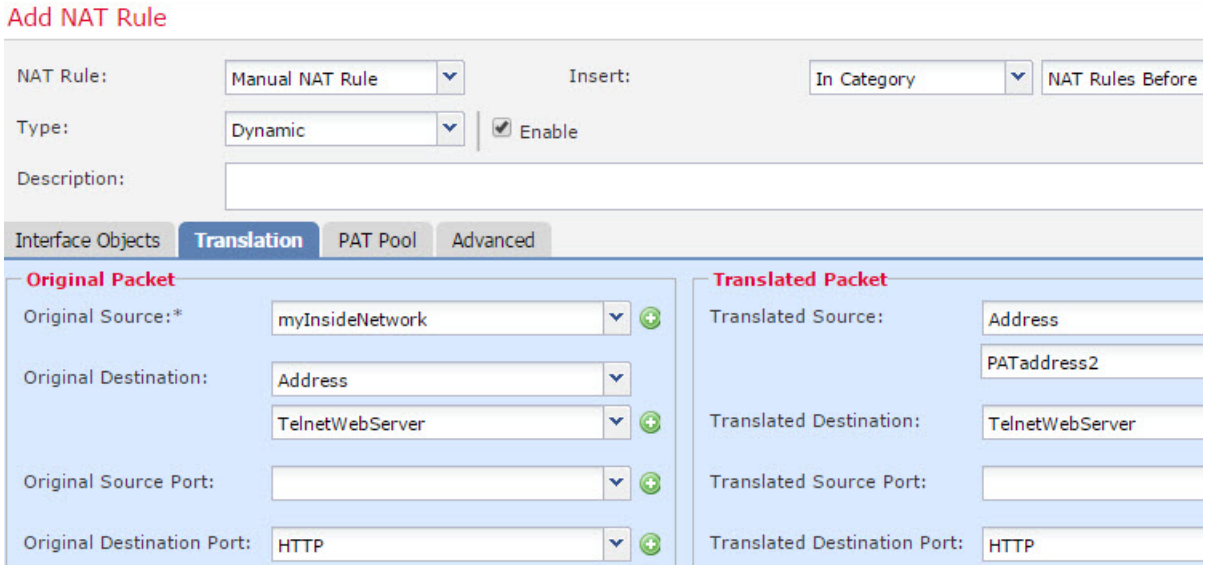
- [NAT ルール（NAT Rule）] = 手動 NAT ルール（Manual NAT Rule）。
- [タイプ（Type）] = Dynamic。

c) [インターフェイス オブジェクト（Interface Objects）] タブで、以下の設定を行います。

- [送信元インターフェイス オブジェクト（Source Interface Objects）] = inside。
- [宛先インターフェイス オブジェクト（Destination Interface Objects）] = dmz。

d) [変換（Translation）] タブで、次の項目を設定します。

- [元の発信元（Original Source）] = myInsideNetwork ネットワーク オブジェクト。
- [変換済みの発信元アドレス（Translated Source Address）] = PATaddress2 ネットワーク オブジェクト。 >
- [元の宛先アドレス（Original Destination Address）] = TelnetWebServer ネットワーク オブジェクト。 >
- [変換済みの宛先（Translated Destination）] = TelnetWebServer ネットワーク オブジェクト。
- [元の宛先ポート（Original Destination Port）] = HTTP ポート オブジェクト（システム定義）。
- [変換済みの宛先ポート（Translated Destination Port）] = HTTP ポート オブジェクト（システム定義）。



e) [保存（Save）] をクリックします。

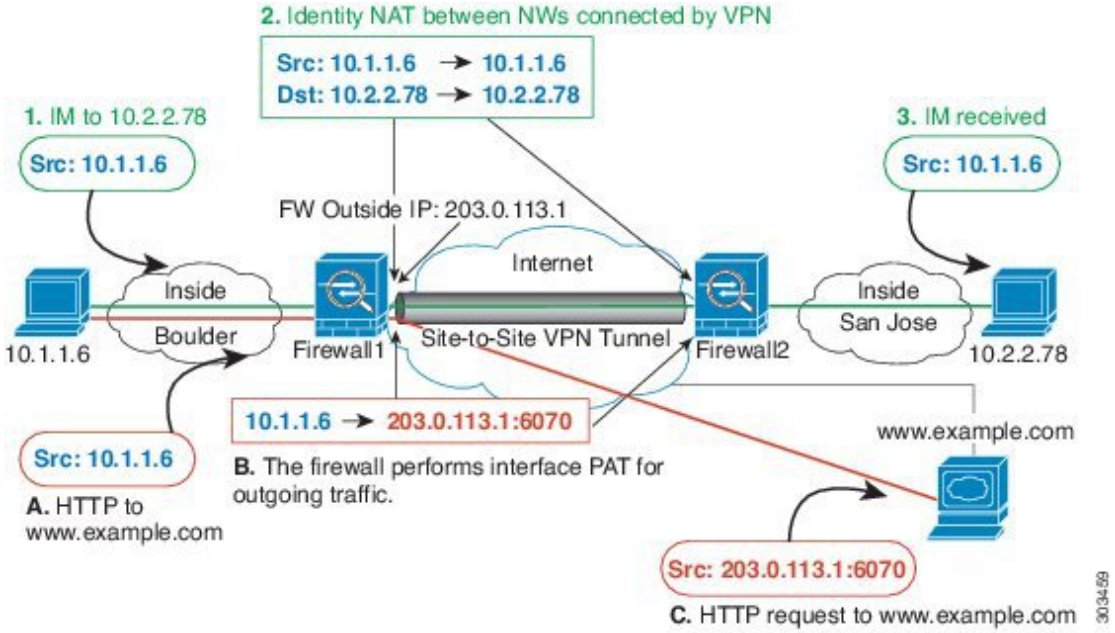
ステップ 7 [NAT ルール（NAT rule）] ページで [保存（Save）] をクリックします。

NAT およびサイトツーサイト VPN

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin Access Admin Network Admin

次の図に、ボールダーとサンノゼのオフィスを接続するサイトツーサイト トンネルを示します。インターネットに渡すトラフィックについて（たとえばボールダーの 10.1.1.6 から www.example.com へ）、インターネットへのアクセスのために NAT によって提供されるパブリック IP アドレスが必要です。次の例では、インターフェイス PAT ルールを使用しています。ただし、VPN トンネルを経由するトラフィックについては（たとえば、ボールダーの 10.1.1.6 からサンノゼの 10.2.2.78 へ）、NAT を実行しません。そのため、アイデンティティ NAT ルールを作成して、そのトラフィックを除外する必要があります。アイデンティティ NAT は同じアドレスにアドレスを変換します。

図 *51 :* サイトツーサイト *VPN* のためのインターフェイス *PAT* およびアイデンティティ *NAT*



次の例は、Firewall1（ボールダー）の設定を示します。

始める前に

VPN 内のデバイスに対応するインターフェイスが含まれているインターフェイス オブジェクト（セキュリティ ゾーンまたはインターフェイス グループ）があることを確認します。この例では、インターフェイス オブジェクトは、Firewall1（ボールダー）インターフェイスに対応する **inside-boulder** および **outside-boulder** という名前のセキュリティ ゾーンであると仮定します。インターフェイス オブジェクトを設定するには、**[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** を選択してから、[インターフェイス（Interfaces）] を選択します。

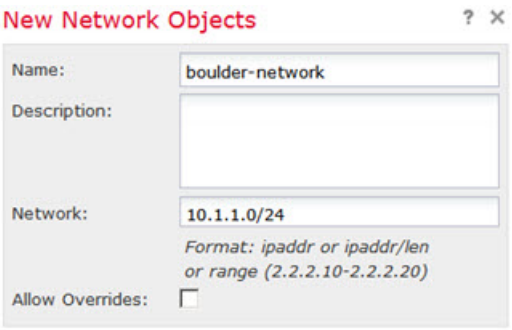
ステップ 1 さまざまなネットワークを定義するには、オブジェクトを作成します。

a) **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** を選択します。

b) コンテンツのテーブルから [ネットワーク（Network）] を選択し、**[ネットワークを追加（Add Network）]** > **[オブジェクトの追加（Add Object）]** をクリックします。

c) ボールダー内部ネットワークを特定します。

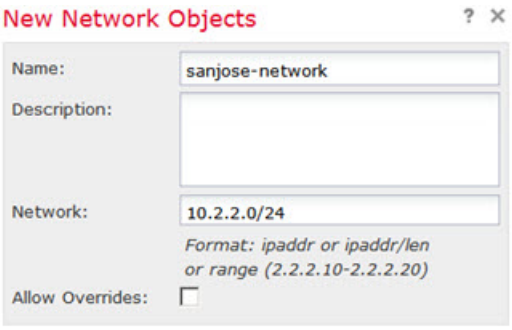
ネットワーク オブジェクトに名前（たとえば、boulder-network）を付けて、ネットワーク アドレス 10.1.1.0/24 を入力します。



d) [保存（Save）] をクリックします。

e) **[ネットワークの追加（Add Network）]** > **[オブジェクトの追加（Add Object）]** をクリックして、内部サンノゼ ネットワークを定義します。

ネットワーク オブジェクトに名前（たとえば、sanjose-network）を付けて、ネットワーク アドレス 10.2.2.0/24 を入力します。



f) [保存（Save）] をクリックします。

ステップ 2 Firewall1（ボールダー）上でVPN経由でサンノゼに向かう場合、ボールダーネットワークの手動アイデンティティ NAT を設定します。

a) **[デバイス（Devices）]** > **[NAT]** の順に選択し、FTD NAT ポリシーを作成または編集します。

b) [ルールの追加（Add Rule）] をクリックします。

c) 次のプロパティを設定します。

- [NAT ルール（NAT Rule）] = 手動 NAT ルール（Manual NAT Rule）。
- [タイプ（Type）] = Static。

d) [インターフェイス オブジェクト（Interface Objects）] タブで、以下の設定を行います。

- [送信元インターフェイス オブジェクト（Source Interface Objects）] = inside-boulder。
- [宛先インターフェイス オブジェクト（Destination Interface Objects）] = outside-boulder。

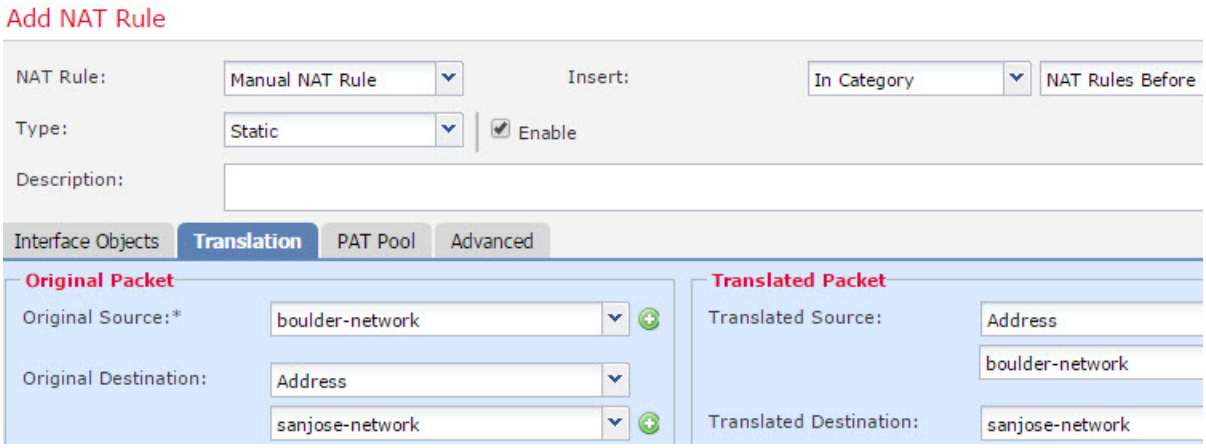
e) [変換（Translation）] タブで、次の項目を設定します。

- [元の送信元（Original Source）] = boulder-network オブジェクト。

- **[変換済みの送信元（Translated Source）]** > **[アドレス（Address）]** = boulder-network オブジェクト。
- **[元の宛先（Original Destination）]** > **[アドレス（Address）]** = sanjose-network オブジェクト。
- [変換済みの宛先] = sanjose-network オブジェクト。

（注） 宛先アドレスは変換しないため、元の宛先アドレスと変換された宛先アドレスに同じアドレスを指定することによって、アイデンティティ NAT を設定する必要があります。[ポート（Port）] フィールドはすべて空白のままにします。このルールは、送信元と宛先の両方のアイデンティティ NAT を設定します。

f) [詳細（Advanced）] タブで [宛先インターフェイスでプロキシ ARP なし（Do not proxy ARP on Destination interface）] を選択します。



g) [保存（Save）] をクリックします。

ステップ 3 Firewall1（ボールダー）上で内部ボールダー ネットワークのインターネットに入る場合、手動ダイナミック インターフェイス PAT を設定します。

a) [ルールの追加（Add Rule）] をクリックします。

b) 次のプロパティを設定します。

- [NAT ルール（NAT Rule）] = 手動 NAT ルール（Manual NAT Rule）。
- [タイプ（Type）] = ダイナミック（Dynamic）。
- [挿入ルール（Insert Rule）] = 最初のルールの後の任意の位置。このルールは任意の宛先アドレスに適用されるため、sanjose-network を宛先として使用するルールはこのルールの前に来る必要があります。そうでなければ、sanjose-network ルールは永遠に一致することがありません。デフォルトでは、新しい手動 NAT ルールは [自動 NAT の前に NAT ルール（NAT Rules Before Auto NAT）] セクションの最後に配置されます。

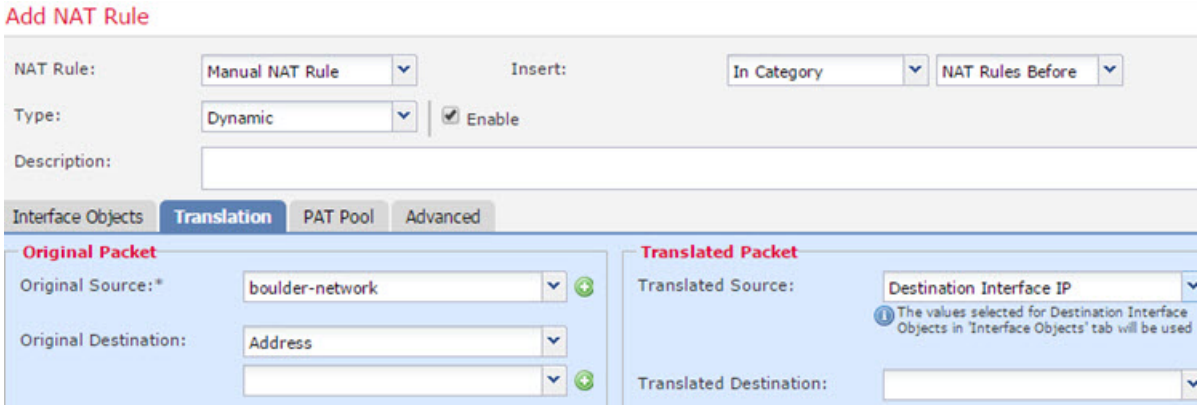
c) [インターフェイス オブジェクト（Interface Objects）] タブで、次の項目を設定します。

- [送信元インターフェイス オブジェクト（Source Interface Objects）] = inside-boulder。

- [宛先インターフェイス オブジェクト（Destination Interface Objects）] = outside-boulder。

d) [変換（Translation）] タブで、次の項目を設定します。

- [元の送信元（Original Source）] = boulder-network オブジェクト。
- [変換済みの送信元（Translated Source）] = 宛先インターフェイス IP（Destination Interface IP）。このオプションでは、宛先インターフェイス オブジェクトに含まれているインターフェイスを使用して、インターフェイス PAT を設定します。
- **[元の宛先（Original Destination）] > [アドレス（Address）]** = 任意（空白のまま）。
- [変換済みの宛先（Translated Destination）] = 任意（空白のまま）。



e) [保存（Save）] をクリックします。

ステップ 4 Firewall2（サンノゼ）の管理を行っている場合、そのデバイスに同様のルールを設定できます。

- 手動アイデンティティ NAT ルールは、宛先が boulder-network の場合は sanjose-network 向けになります。Firewall2 の内部および外部ネットワーク向けに新しいインターフェイス オブジェクトを作成します。
- 手動ダイナミック インターフェイス PAT ルールは、宛先が「任意」の場合は sanjose-network 向けになります。

NAT を使用した DNS クエリと応答の書き換え

応答内のアドレスを NAT コンフィギュレーションと一致するアドレスに置き換えて、DNS 応答を修正するようにFirepower Threat Defense デバイスを設定することが必要になる場合があります。DNS 修正は、各トランスレーション ルールを設定するときに設定できます。DNS 修正は DNS 改ざんとも呼ばれます。

この機能は、NAT ルールに一致する DNS クエリと応答のアドレスを書き換えます（たとえば、IPv4 の A レコード、IPv6 の AAAA レコード、または逆引き DNS クエリの PTR レコード）。マッピング インターフェイスから他のインターフェイスに移動する DNS 応答では、A

レコードはマップされた値から実際の値へリライトされます。逆に、任意のインターフェイスからマッピング インターフェイスに移動する DNS 応答では、A レコードは実際の値からマップされた値へ書き換えられます。

NAT ルールに DNS の書き換えを設定する必要が生じる主な状況を次に示します。

- ルールが NAT64 または NAT46 で、DNS サーバが外部ネットワークにある場合。DNS A レコード（IPv4 向け）と AAAA レコード（IPv6 向け）間の変換のために DNS を書き換える場合。
- DNS サーバが外部に、クライアントが内部にあり、クライアントが使用する完全修飾ドメイン名を解決すると他の内部ホストになる場合。
- DNS サーバが内部にあり、プライベート IP アドレスを使用して応答し、クライアントが外部にあり、クライアントが完全修飾ドメイン名を指定して内部にホストされているサーバをアクセスする場合。

DNS の書き換えの制限

次に DNS リライトの制限事項を示します。

- 個々の A レコードまたは AAAA レコードに複数の PAT ルールを適用できることで、使用する PAT ルールが不明確になるため、DNS リライトは PAT には適用されません。
- 手動 NAT ルールを設定する場合、宛先アドレスおよび送信元アドレスを指定すると、DNS 修正を設定できません。これらの種類のルールでは、A と B に向かった場合に 1 つのアドレスに対して異なる変換が行われる可能性があります。したがって、Firepower Threat Defense デバイス は、DNS 応答内の IP アドレスを適切な Twice NAT ルールに一致させることができません。DNS 応答には、DNS 要求を求めたパケット内の送信元アドレスと宛先アドレスの組み合わせに関する情報が含まれません。
- DNS クエリと応答を書き換えるには、NAT のルールに対して DNS NAT リライトを有効にした DNS アプリケーション インスペクションを有効にする必要があります。DNS NAT のリライトを有効にした DNS アプリケーション インスペクションはデフォルトでグローバルに適用されるため、インスペクションの設定を変更する必要は通常ありません。
- 実際には、DNS の書き換えは NAT ルールではなく xlate エントリで実行されます。したがって、ダイナミック ルールに xlate がない場合、リライトが正しく実行されません。スタティック NAT の場合は、同じような問題が発生しません。
- DNS の書き換えによって、DNS ダイナミック アップデートのメッセージ（オペレーション コード 5）は書き換えられません。

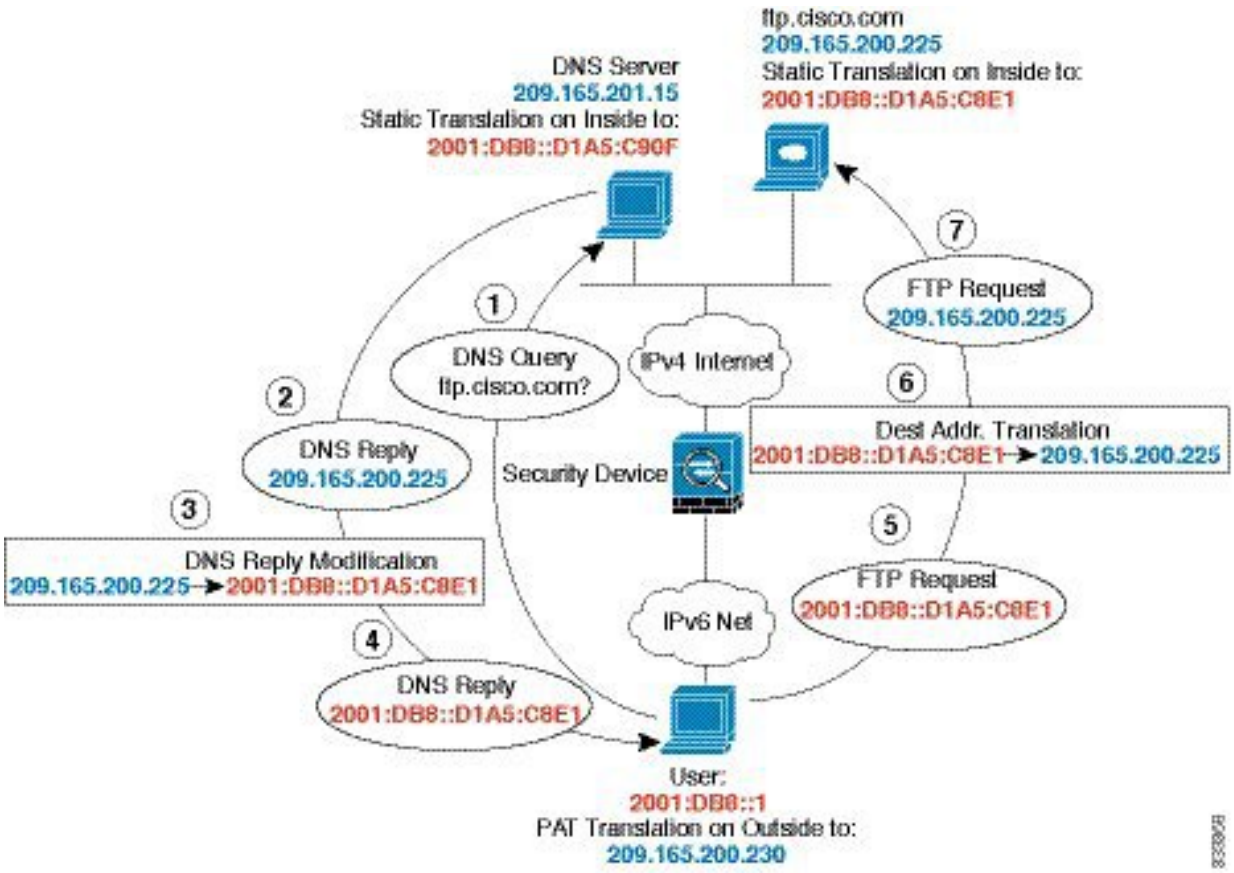
次のトピックで、NAT ルールの DNS リライトの例を示します。

DNS64 応答修正

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin Access Admin Network Admin

次の図に、外部の IPv4 ネットワーク上の FTP サーバと DNS サーバを示します。システムには、外部サーバ用のスタティック変換があります。この場合に、内部 IPv6 ユーザが ftp.cisco.com のアドレスを DNS サーバに要求すると、DNS サーバは応答として実際のアドレス 209.165.200.225 を返します。

ftp.cisco.com のマッピング アドレス（2001:DB8::D1A5:C8E1、ここで D1A5:C8E1 は 209.165.200.225 に相当する IPv6）が内部ユーザによって使用されるようにするには、スタティック変換に対して DNS 応答修正を設定する必要があります。この例には、DNS サーバのスタティック NAT 変換、および内部 IPv6 ホストの PAT ルールも含まれています。



始める前に

デバイスに対応するインターフェイスが含まれているインターフェイス オブジェクト（セキュリティ ゾーンまたはインターフェイス グループ）があることを確認します。この例では、インターフェイス オブジェクトが「**inside**」および「**outside**」という名前のセキュリティ ゾーンであると仮定しています。インターフェイス オブジェクトを設定するには、**[オブジェクト（Objects）] > [オブジェクト管理（Object Management）]** を選択してから、[インターフェイス（Interface）] を選択します。

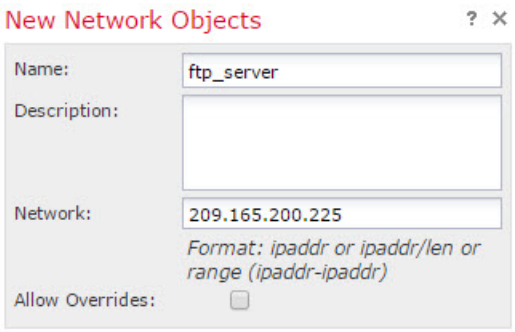
ステップ 1 FTP サーバ、DNS サーバ、内部ネットワーク、および PAT プールのネットワーク オブジェクトを作成します。

a) **[オブジェクト（Objects）] > [オブジェクト管理（Object Management）]** を選択します。

b) コンテンツのテーブルから [ネットワーク（Network）] を選択し、**[ネットワークを追加（Add Network）] > [オブジェクトの追加（Add Object）]** をクリックします。

c) 実際の FTP サーバ アドレスを定義します。

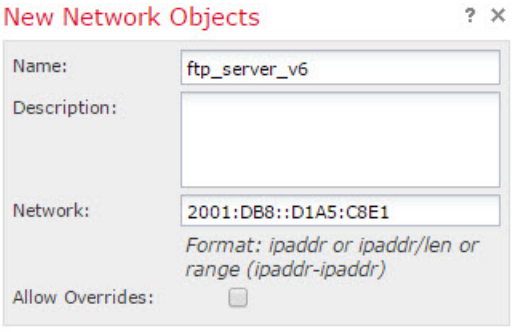
ネットワーク オブジェクトに名前を付け（ftp_server など）、ホスト アドレス 209.165.200.225 を入力します。



d) [保存（Save）] をクリックします。

e) **[ネットワークを追加（Add Network）] > [オブジェクトの追加（Add Object）]** をクリックして、FTP サーバの変換済み IPv6 アドレスを定義します。

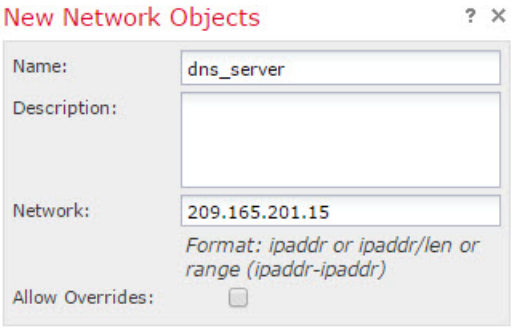
ネットワーク オブジェクトに名前を付け（ftp_server_v6 など）、ホストアドレス 2001:DB8::D1A5:C8E1 を入力します。



f) [保存（Save）] をクリックします。

g) **[ネットワークを追加（Add Network）]** > **[オブジェクトの追加（Add Object）]** をクリックして、DNS サーバの実際のアドレスを定義します。

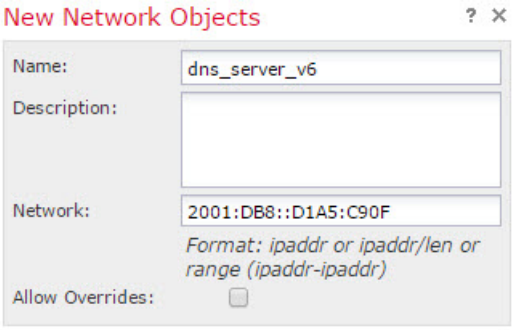
ネットワーク オブジェクトに名前を付け（dns_server など）、ホスト アドレス 209.165.201.15 を入力します。



h) [保存（Save）] をクリックします。

i) **[ネットワークを追加（Add Network）]** > **[オブジェクトの追加（Add Object）]** をクリックして、DNS サーバの変換済み IPv6 アドレスを定義します。

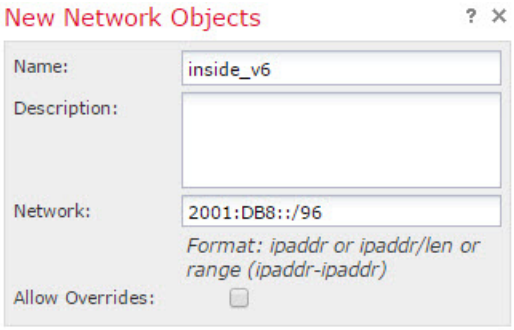
ネットワーク オブジェクトに名前を付け（dns_server_v6 など）、ホスト アドレス 2001:DB8::D1A5:C90F を入力します（ここで、D1A5:C90F は IPv6 の場合の 209.165.201.15 です）。



j) [保存（Save）] をクリックします。

k) **[ネットワークを追加（Add Network）]** > **[オブジェクトの追加（Add Object）]** をクリックして、内部 IPv6 ネットワークを定義します。

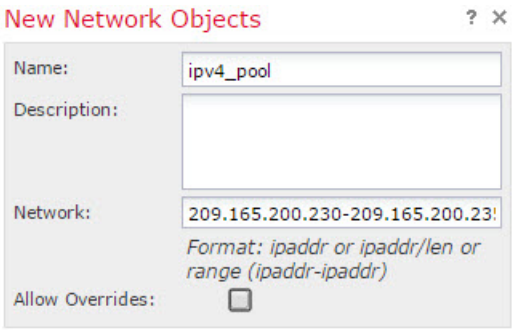
ネットワーク オブジェクトに名前（inside_v6 など）を付け、ネットワーク アドレス 2001:DB8::/96 を入力します。



l) [保存（Save）] をクリックします。

m) **[ネットワークを追加（Add Network）] > [オブジェクトの追加（Add Object）]** をクリックし、内部 IPv6 ネットワークの IPv4 PAT プールを定義します。

ネットワーク オブジェクトに名前を付け（ipv4_pool など）、範囲 209.165.200.230 ～ 209.165.200.235 を入力します。



n) [保存（Save）] をクリックします。

ステップ 2 FTP サーバのための、DNS 修正を設定したスタティック NAT ルールを設定します。

a) **[デバイス（Devices）] > [NAT]** の順に選択し、FTD NAT ポリシーを作成または編集します。

b) [ルールの追加（Add Rule）] をクリックします。

c) 次のプロパティを設定します。

- [NAT ルール（NAT Rule）] = 自動 NAT ルール。
- [タイプ（Type）] = Static。

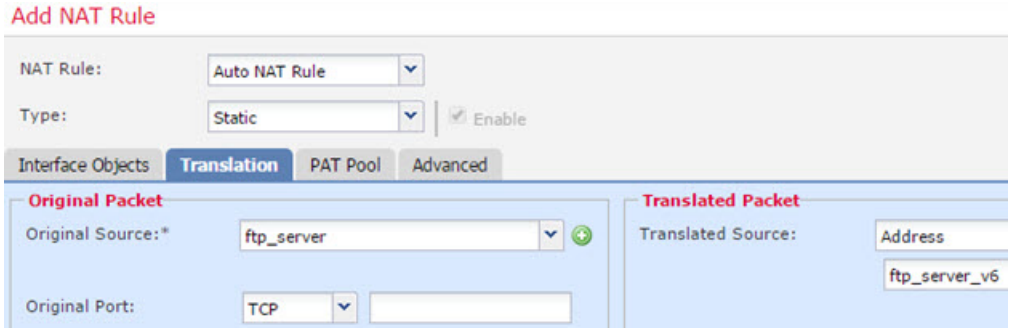
d) [インターフェイス オブジェクト（Interface Objects）] タブで、以下の設定を行います。

- [送信元インターフェイス オブジェクト（Source Interface Objects）] = outside。
- [宛先インターフェイス オブジェクト（Destination Interface Objects）] = inside。

e) [変換（Translation）] タブで、次の項目を設定します。

- [元の発信元（Original Source）] = ftp_server ネットワーク オブジェクト。

- [変換済みの発信元アドレス（Translated Source Address）] = ftp_server_v6 ネットワーク オブジェクト。 >



f) [詳細（Advanced）] タブで、以下のオプションを選択します。

- [このルールに一致する DNS 応答を変換（Translate DNS replies that match this rule）]。
- [ネット間マッピング（Net to Net Mapping）]。1 対 1 の NAT46 変換であるためです。

g) [OK] をクリックします。

ステップ 3 DNS サーバのためのスタティック NAT ルールを設定します。

a) [ルールの追加（Add Rule）] をクリックします。

b) 次のプロパティを設定します。

- [NAT ルール（NAT Rule）] = 自動 NAT ルール。
- [タイプ（Type）] = Static。

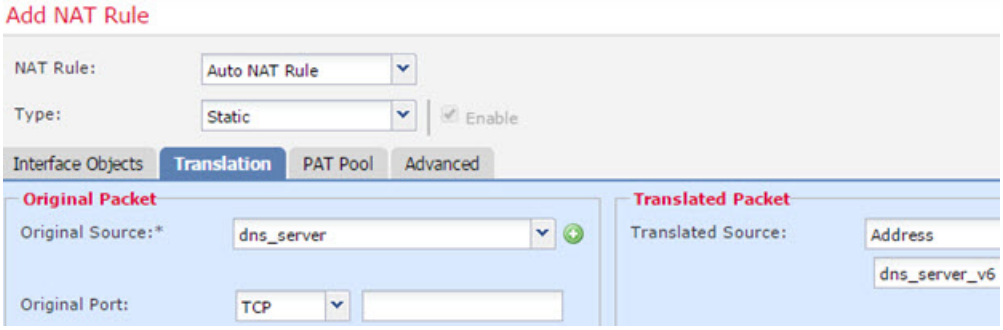
c) [インターフェイス オブジェクト（Interface Objects）] タブで、以下の設定を行います。

- [送信元インターフェイス オブジェクト（Source Interface Objects）] = outside。
- [宛先インターフェイス オブジェクト（Destination Interface Objects）] = inside。

d) [変換（Translation）] タブで、次の項目を設定します。

- [元の発信元（Original Source）] = dns_server ネットワーク オブジェクト。
- [変換済みの発信元アドレス（Translated Source Address）] = dns_server_v6 ネットワーク オブジェクト。 >

e) これは 1 対 1 の NAT46 変換であるため、[詳細（Advanced）] タブで、[ネット間マッピング（Net to Net Mapping）] を選択します。



f) [OK] をクリックします。

ステップ 4 内部 IPv6 ネットワークに対し、PAT プール ルールを持つダイナミック NAT を設定します。

a) [ルールの追加（Add Rule）] をクリックします。

b) 次のプロパティを設定します。

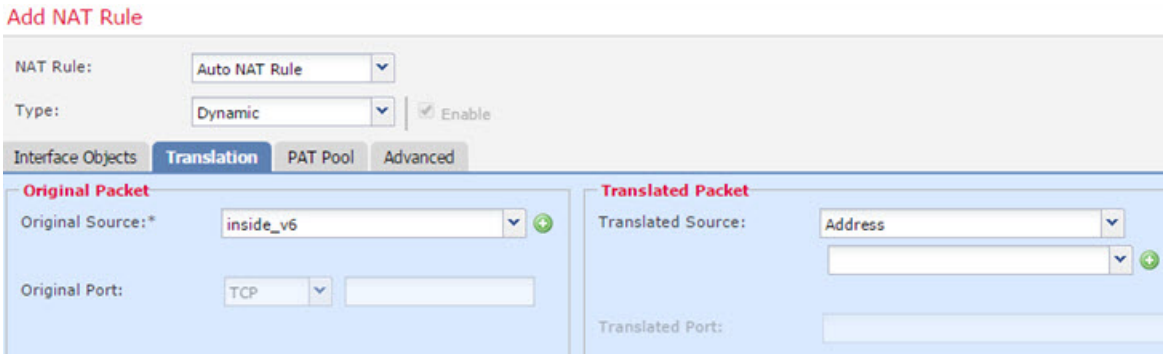
- [NAT ルール（NAT Rule）] = 自動 NAT ルール。
- [タイプ（Type）] = Dynamic。

c) [インターフェイス オブジェクト（Interface Objects）] タブで、以下の設定を行います。

- [送信元インターフェイス オブジェクト（Source Interface Objects）] = inside。
- [宛先インターフェイス オブジェクト（Destination Interface Objects）] = outside。

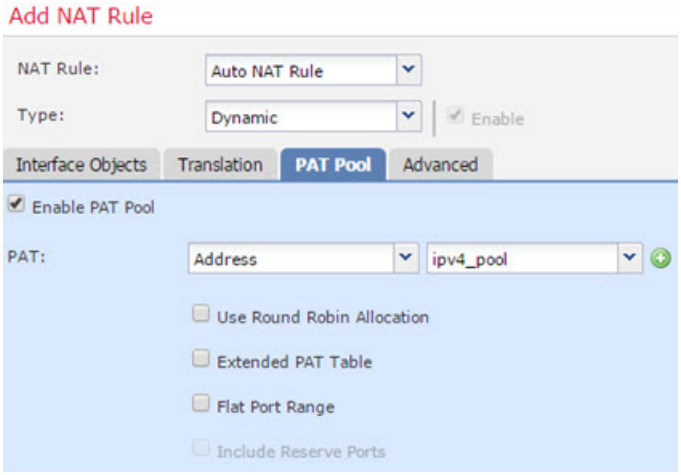
d) [変換（Translation）] タブで、次の項目を設定します。

- [元の送信元（Original Source）] = inside_v6 ネットワーク オブジェクト。
- [変換済みの発信元アドレス（Translated Source Address）] > = このフィールドは空のままにします。



e) [PAT プール（PAT Pool）] タブで、以下の設定を行います。

- [PAT プールの有効化（Enable PAT Pool）] = このオプションを選択します。
- [変換済みの発信元アドレス（Translated Source Address）] = ipv4_pool ネットワーク オブジェクト。 >



f) [OK] をクリックします。

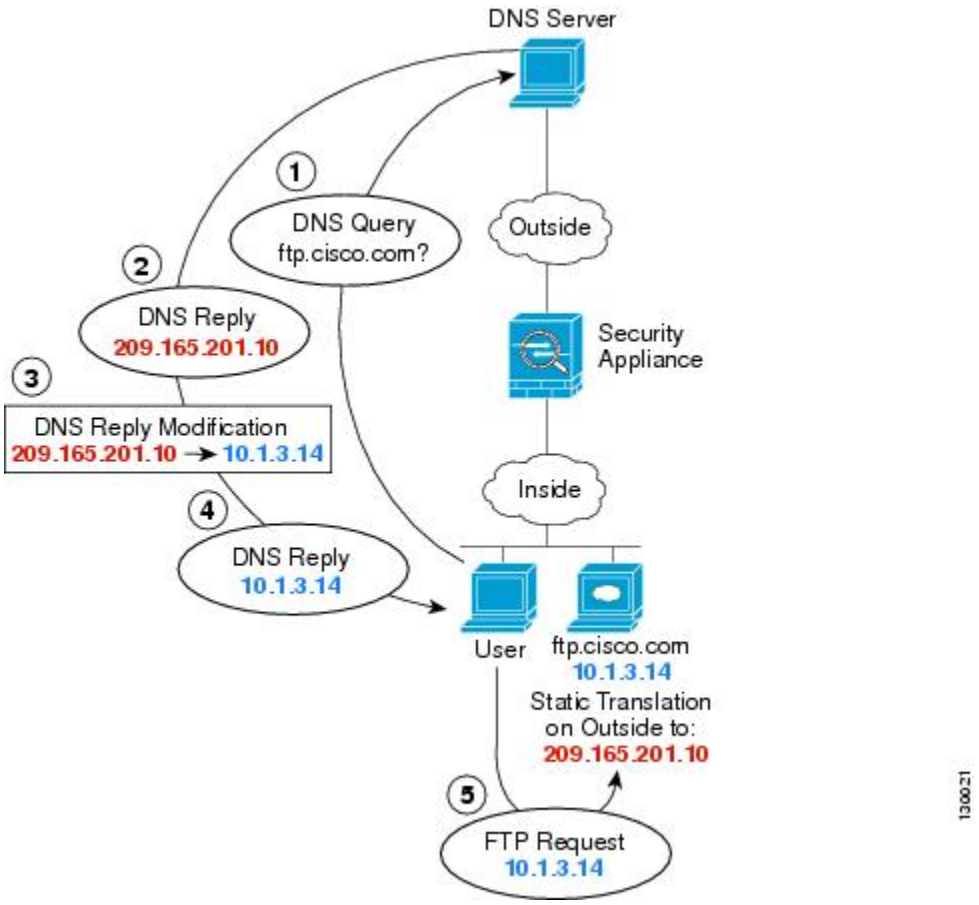
DNS 応答修正：Outside 上の DNS サーバ

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin Access Admin Network Admin

次の図に、外部インターフェイスからアクセス可能な DNS サーバを示します。ftp.cisco.com というサーバが内部インターフェイス上にあります。ftp.cisco.com の実際のアドレス（10.1.3.14）を、外部ネットワーク上で可視のマッピング アドレス（209.165.201.10）にスタティックに変換するように NAT を設定します

この場合、このスタティック ルールで DNS 応答修正をイネーブルにする必要があります。これにより、実際のアドレスを使用して ftp.cisco.com にアクセスすることを許可されている内部ユーザは、マッピング アドレスではなく実際のアドレスを DNS サーバから受信できるようになります。

内部ホストが ftp.cisco.com のアドレスを求める DNS 要求を送信すると、DNS サーバは応答でマッピング アドレス（209.165.201.10）を示します。システムは、内部サーバのスタティック ルールを参照し、DNS 応答内のアドレスを 10.1.3.14 に変換します。DNS 応答修正を有効にしない場合、内部ホストは ftp.cisco.com に直接アクセスする代わりに、209.165.201.10 にトラフィックの送信を試みます。



始める前に

デバイスに対応するインターフェイスが含まれているインターフェイス オブジェクト（セキュリティ ゾーンまたはインターフェイス グループ）があることを確認します。この例では、インターフェイス オブジェクトが「**inside**」および「**outside**」という名前のセキュリティ ゾーンであると仮定しています。インターフェイス オブジェクトを設定するには、**[オブジェクト（Objects）] > [オブジェクト管理（Object Management）]** を選択してから、[インターフェイス（Interface）] を選択します。

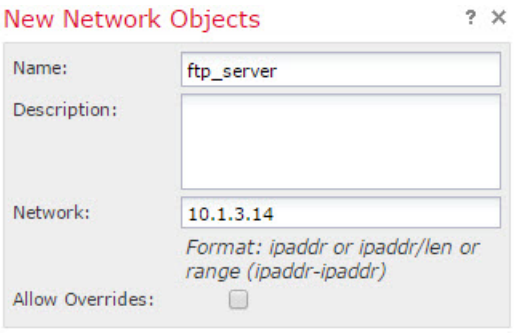
ステップ 1 FTP サーバのネットワーク オブジェクトを作成します。

a) **[オブジェクト（Objects）] > [オブジェクト管理（Object Management）]** を選択します。

b) コンテンツのテーブルから [ネットワーク（Network）] を選択し、**[ネットワークを追加（Add Network）] > [オブジェクトの追加（Add Object）]** をクリックします。

c) 実際の FTP サーバ アドレスを定義します。

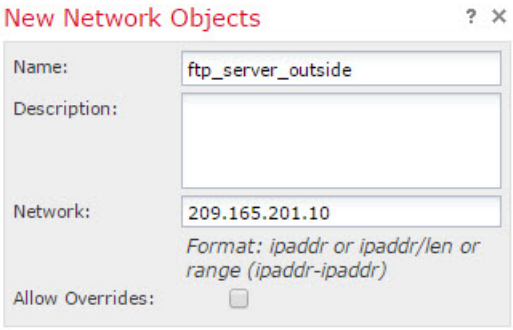
ネットワーク オブジェクトに名前を付け（ftp_server など）、ホスト アドレス 10.1.3.14 を入力します。



d) [保存（Save）] をクリックします。

e) **[ネットワークを追加（Add Network）] > [オブジェクトの追加（Add Object）]** をクリックして、FTP サーバの変換済みアドレスを定義します。

ネットワーク オブジェクトに名前を付け（ftp_server_outside など）、ホスト アドレス 209.165.201.10 を入力します。



f) [保存（Save）] をクリックします。

ステップ 2 FTP サーバのための、DNS 修正を設定したスタティック NAT ルールを設定します。

a) **[デバイス（Devices）] > [NAT]** の順に選択し、FTD NAT ポリシーを作成または編集します。

b) [ルールの追加（Add Rule）] をクリックします。

c) 次のプロパティを設定します。

- [NAT ルール（NAT Rule）] = 自動 NAT ルール。
- [タイプ（Type）] = Static。

d) [インターフェイス オブジェクト（Interface Objects）] タブで、以下の設定を行います。

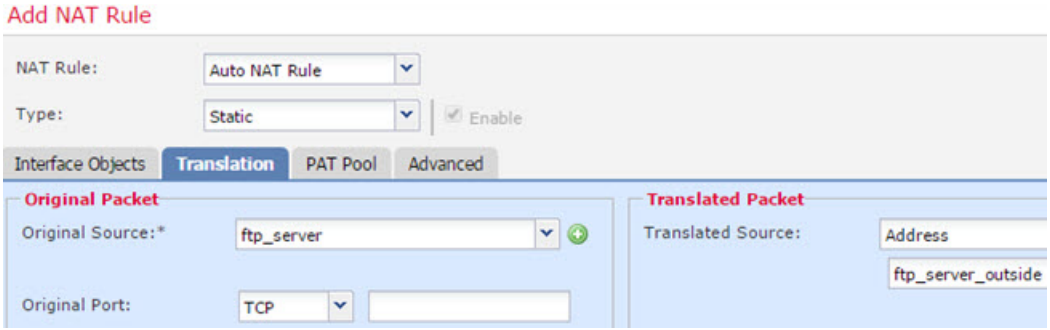
- [送信元インターフェイス オブジェクト（Source Interface Objects）] = inside。
- [宛先インターフェイス オブジェクト（Destination Interface Objects）] = outside。

e) [変換（Translation）] タブで、次の項目を設定します。

- [元の発信元（Original Source）] = ftp_server ネットワーク オブジェクト。

- [変換済みの発信元アドレス（Translated Source Address）] = ftp_server_outside ネットワーク オブジェクト。 >

f) [詳細（Advanced）] タブで、[このルールと一致する DNS 応答を変換（Translate DNS replies that match this rule）] を選択します。

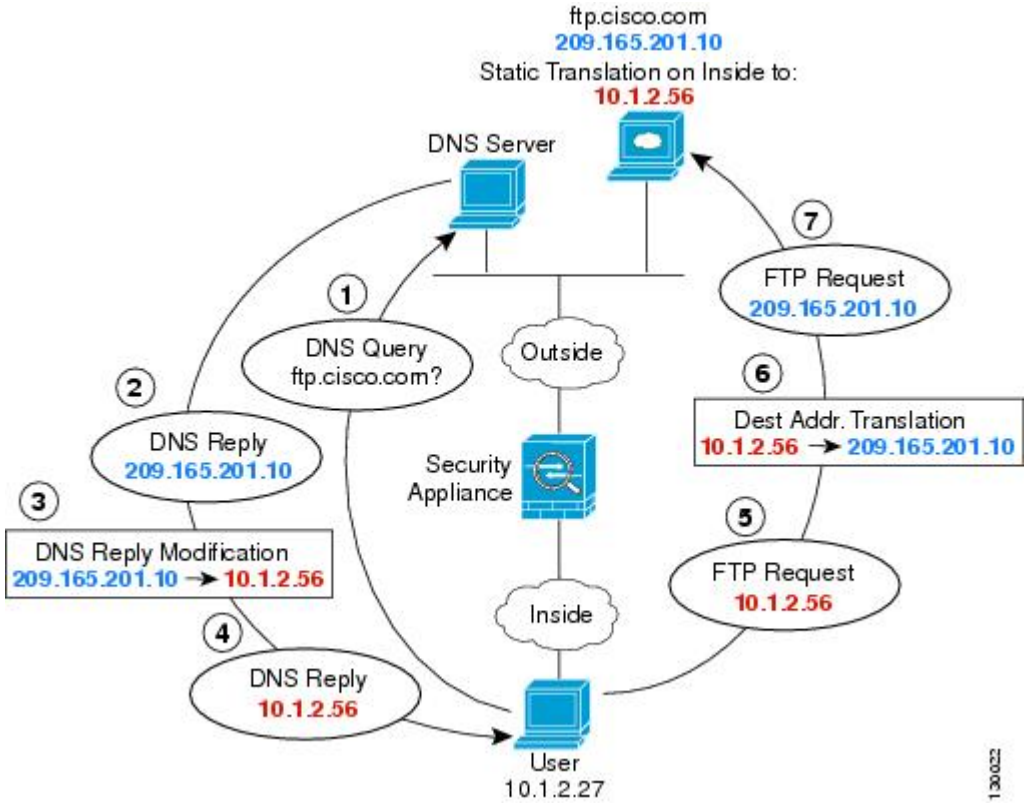


g) [OK] をクリックします。

DNS 応答修正：ホスト ネットワーク上の DNS サーバ

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin Access Admin Network Admin

次の図に、外部の FTP サーバと DNS サーバを示します。システムには、外部サーバ用のスタティック変換があります。この場合、ftp.cisco.com のアドレスを DNS サーバに要求すると、DNS サーバは応答で実際のアドレス 209.165.20.10 を示します。内部ユーザに ftp.cisco.com のマッピング アドレス（10.1.2.56）を使用させるには、スタティック変換用の DNS 応答修正を設定する必要があります。



始める前に

デバイスに対応するインターフェイスが含まれているインターフェイス オブジェクト（セキュリティ ゾーンまたはインターフェイス グループ）があることを確認します。この例では、インターフェイス オブジェクトが「**inside**」および「**outside**」という名前のセキュリティ ゾーンであると仮定しています。インターフェイス オブジェクトを設定するには、**[オブジェクト（Objects）] > [オブジェクト管理（Object Management）]** を選択してから、[インターフェイス（Interface）] を選択します。

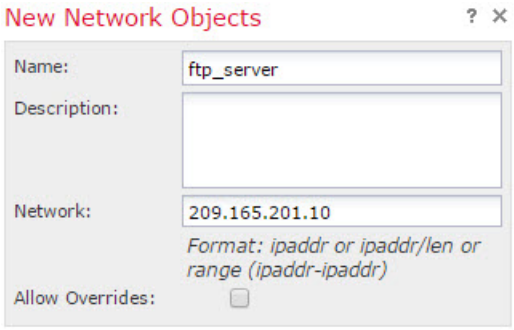
ステップ 1 FTP サーバのネットワーク オブジェクトを作成します。

a) **[オブジェクト（Objects）] > [オブジェクト管理（Object Management）]** を選択します。

b) コンテンツのテーブルから [ネットワーク（Network）] を選択し、**[ネットワークを追加（Add Network）] > [オブジェクトの追加（Add Object）]** をクリックします。

c) 実際の FTP サーバ アドレスを定義します。

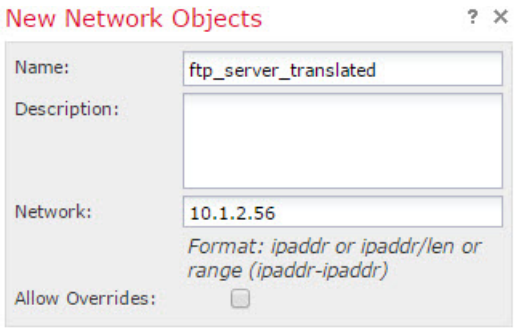
ネットワーク オブジェクトに名前を付け（ftp_server など）、ホスト アドレス 209.165.201.10 を入力します。



d) [保存（Save）] をクリックします。

e) **[ネットワークを追加（Add Network）] > [オブジェクトの追加（Add Object）]** をクリックして、FTP サーバの変換済みアドレスを定義します。

ネットワーク オブジェクトに名前を付け（ftp_server_translated など）、ホスト アドレス 10.1.2.56 を入力します。



f) [保存（Save）] をクリックします。

ステップ 2 FTP サーバのための、DNS 修正を設定したスタティック NAT ルールを設定します。

a) **[デバイス（Devices）] > [NAT]** の順に選択し、FTD NAT ポリシーを作成または編集します。

b) [ルールの追加（Add Rule）] をクリックします。

c) 次のプロパティを設定します。

- [NAT ルール（NAT Rule）] = 自動 NAT ルール。
- [タイプ（Type）] = Static。

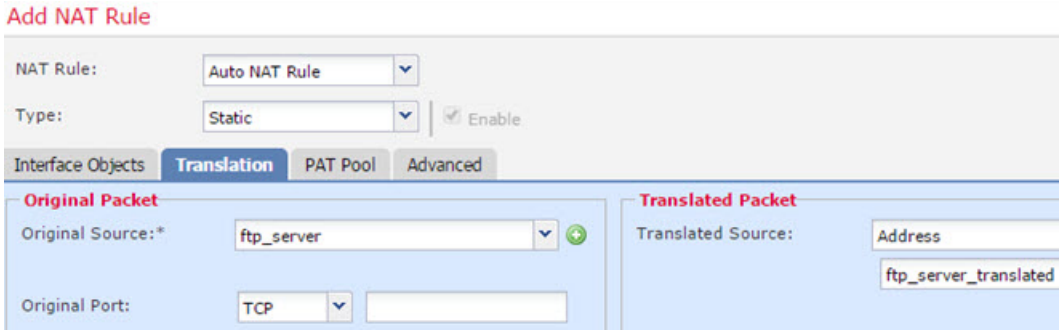
d) [インターフェイス オブジェクト（Interface Objects）] タブで、以下の設定を行います。

- [送信元インターフェイス オブジェクト（Source Interface Objects）] = outside。
- [宛先インターフェイス オブジェクト（Destination Interface Objects）] = inside。

e) [変換（Translation）] タブで、次の項目を設定します。

- [元の発信元（Original Source）] = ftp_server ネットワーク オブジェクト。
- [変換済みの発信元アドレス（Translated Source Address）] = ftp_server_translated ネットワーク オブジェクト。 >

f) [詳細（Advanced）] タブで、[このルールと一致する DNS 応答を変換（Translate DNS replies that match this rule）] を選択します。



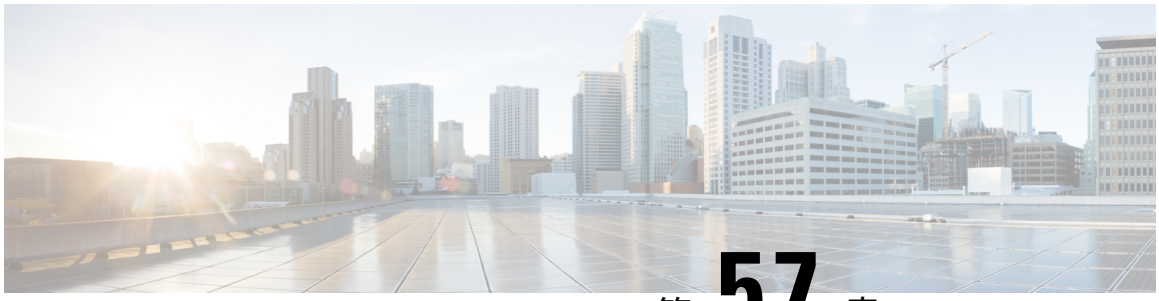
g) [OK] をクリックします。

FTD NAT の履歴

機能	バージョン	詳細
Firepower Threat Defense のネットワーク アドレス変換（NAT）。	6.0.1	Firepower Threat Defense の NAT ポリシーが追加されました。 新規/変更された画面：Threat Defense が NAT ポリシーのタイプとして **[デバイス（Devices）]** > **[NAT]** ページに追加されました。 サポートされるプラットフォーム Firepower Threat Defense
Firepower Threat Defense の NAT のネットワーク範囲のオブジェクトのサポート。	6.1.0	Firepower Threat Defense NAT ルール内のネットワーク範囲のオブジェクトを必要に応じて使用できるようになりました。

第 XV 部

7000 および 8000 シリーズの高度な導入オプション



第 57 章

仮想スイッチのセットアップ

以下のトピックでは、Firepower システムで仮想スイッチをセットアップする方法について説明します。

仮想スイッチ

レイヤ 2 展開の 7000 または 8000 シリーズ デバイスは、2 つ以上のネットワーク間でパケットスイッチングを提供するように設定できます。レイヤ 2 展開では、仮想スイッチをスタンドアロン ブロードキャスト ドメインとして機能させ、ネットワークを論理セグメントに分割するように設定できます。仮想スイッチでは、ホストからの Media Access Control（MAC）アドレスを使用して、パケットの送信先を判断します。

仮想スイッチを設定すると、スイッチはまず、スイッチ上の使用可能なすべてのポートからパケットをブロードキャストします。その後は、タグ付きのリターン トラフィックを使用して、各ポートに接続されたネットワーク上にどのホストが存在するのかを学習していきます。

仮想スイッチがトラフィックを処理するには、仮想スイッチに複数のスイッチドインターフェイスがなければなりません。仮想スイッチごとに、トラフィックは、スイッチ型インターフェイスとして設定されたいくつかのポートに限定されます。たとえば、4 つのスイッチ型インターフェイスのある仮想スイッチを設定した場合、ブロードキャスト用に 1 つのポートを介して送入されるパケットは、そのスイッチ上の残る 3 つのポートからのみ送出可能です。

物理スイッチ型インターフェイスを設定するときには、仮想スイッチにそれを割り当てる必要があります。また、必要に応じて、物理ポート上に追加の論理スイッチドインターフェイスを定義することもできます。複数の物理インターフェイスを Link Aggregation Group（LAG）と呼ばれる単一の論理スイッチドインターフェイスにグループ化できます。この単一の集約論理リンクによって、帯域幅と冗長性の向上と、2 つのエンドポイント間でのロードバランシングが実現されます。

注意 レイヤ2展開に何らかの理由で障害が発生した場合、デバイスはトラフィックを転送しなくなります。

スイッチド インターフェイスの設定

物理設定または論理設定を備えるよう、スイッチ型インターフェイスをセットアップできます。タグなし VLAN トラフィックを処理するよう物理スイッチ型インターフェイスを設定できます。また、VLANタグが指定されたトラフィックを処理するよう論理スイッチ型インターフェイスを作成することもできます。

レイヤ2展開では、外部の物理インターフェイス上でトラフィックを受信した場合、それを待機しているスイッチ型インターフェイスがなければ、システムはそのトラフィックをドロップします。VLANタグのないパケットを受信した場合、そのポート用の物理スイッチ型インターフェイスが未設定であれば、システムはパケットをドロップします。VLANタグ付きパケットを受信した場合、論理スイッチ型インターフェイスが未設定であれば、システムは同様にパケットをドロップします。

スイッチ型インターフェイスで VLAN タグ付きで受信されたトラフィックをシステムが処理するときには、ルールの評価や転送の決定を行う前に、入力における最も外側の VLAN タグを取り除きます。VLANタグ付き論理スイッチ型インターフェイスを介してデバイスから出るパケットは、出力において関連する VLAN タグ付きでカプセル化されます。

親の物理インターフェイスをインラインまたはパッシブに変更すると、システムは関連するすべての論理インターフェイスを削除することに注意してください。

スイッチ型インターフェイスの設定メモ

管理対象デバイス上の1つ以上の物理ポートはスイッチ型インターフェイスとして設定できます。トラフィックを処理できるようにするには、その前に、物理スイッチ型インターフェイスを仮想スイッチに割り当てる必要があります。リンク モード設定および MDI/MDIX 設定は、銅線インターフェイスにのみ設定できます。

（注） 8000シリーズアプライアンスのインターフェイスは、半二重オプションをサポートしません。

物理スイッチ型インターフェイスごとに、複数の論理スイッチ型インターフェイスを追加できます。物理インターフェイスで受信される VLAN タグ付きトラフィックを処理するには、各論理インターフェイスをその特定のタグに関連付ける必要があります。トラフィックを処理するには、論理スイッチ型インターフェイスを仮想スイッチに割り当てる必要があります。

スイッチ型インターフェイスを設定する場合、設定可能なMTUの範囲は、Firepowerシステムのデバイスのモデルとインターフェイスのタイプによって異なる可能性があります。

MTU 値の範囲は管理対象デバイスのモデルとインターフェイス タイプによって異なる場合があります。

注意 デバイス上のすべての非管理インターフェイスの中で最大 MTU 値を変更し、設定変更を展開すると、Snort プロセスが再起動され、トラフィック インスペクションが一時的に中断されます。インスペクションは、変更したインターフェイスだけでなく、すべての非管理インターフェイスで中断されます。この中断によってトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびインターフェイスのタイプに応じて異なります。詳細については、「Snort® の再起動によるトラフィックの動作 （451 ページ）」を参照してください。

既存の論理スイッチ型インターフェイスを編集するには、インターフェイスの横にある編集アイコン（[ ]）をクリックします。

論理スイッチ型インターフェイスを削除すると、それが存在する物理インターフェイスから、および関連付けられている仮想スイッチとセキュリティ ゾーンからそれが削除されます。

関連トピック

7000 および 8000 シリーズ デバイスおよび NGIPSv の MTU 範囲 （661 ページ）
Snort® の再起動シナリオ （450 ページ）

物理スイッチド インターフェイスの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	Control	7000 & 8000 シリーズ	リーフのみ	Admin/Network Admin

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 スイッチド インターフェイスを設定するデバイスの横にある編集アイコン（ ）をクリックします。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 スイッチドインターフェイスとして設定するインターフェイスの横にある編集アイコン（ ）をクリックします。

ステップ 4 [スイッチド（Switched）] タブをクリックします。

ステップ 5 セキュリティ ゾーンをスイッチド インターフェイスに関連付けるには、次のいずれかを実行します。

- [セキュリティ ゾーン（Security Zone）] ドロップダウン リストから既存のセキュリティ ゾーンを選択します。

- [新規（New）] を選択して新しいセキュリティ ゾーンを追加します。セキュリティ ゾーンおよびインターフェイス グループ オブジェクトの作成 （536 ページ） を参照してください。

ステップ 6 仮想スイッチをスイッチド インターフェイスに関連付けるには、次のいずれかを実行します。

- [仮想スイッチ（Virtual Switch）] ドロップダウン リストから既存の仮想スイッチを選択します。
- [新規（New）] を選択して新しい仮想スイッチを追加します。仮想スイッチの追加 （1576 ページ） を参照してください。

ステップ 7 スイッチドインターフェイスにトラフィックを処理させるには、[有効（Enabled）] チェックボックスをオンにします。

（注） このチェックボックスをオフにすると、インターフェイスは無効になり、ユーザはセキュリティ上の理由によりアクセスできなくなります。

ステップ 8 [モード（Mode）] ドロップダウン リストからリンク モードを指定するオプションを選択するか、または [自動ネゴシエーション（Auto Negotiation）] を選択して、速度とデュプレックス設定を自動的にネゴシエートするようインターフェイスを設定します。

モード設定は銅線インターフェイスにのみ使用できます。

8000 シリーズ アプライアンスのインターフェイスは、半二重オプションをサポートしません。

ステップ 9 [MDI/MDIX] ドロップダウン リストから、インターフェイスの設定対象として MDI（メディア依存型インターフェイス）、MDIX（メディア依存型インターフェイス クロスオーバー）、または自動 MDIX のいずれかを指定するオプションを選択します。

デフォルトでは、[MDI/MDIX] は [自動 MDIX（Auto-MDIX）] に設定され、MDI と MDIX の間の切り替えを自動的に処理してリンクを確立します。

ステップ 10 [MTU] フィールドに、最大伝送ユニット（MTU）を入力して、パケットの最大許容サイズを指定します。

MTU 値の範囲は管理対象デバイスのモデルとインターフェイス タイプによって異なる場合があります。

注意 デバイス上のすべての非管理インターフェイスの中で最大MTU値を変更し、設定変更を展開すると、Snortプロセスが再起動され、トラフィック インスペクションが一時的に中断されます。インスペクションは、変更したインターフェイスだけでなく、すべての非管理インターフェイスで中断されます。この中断によってトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびインターフェイスのタイプに応じて異なります。詳細については、「Snort® の再起動によるトラフィックの動作 （451 ページ）」を参照してください。

ステップ 11 **[保存（Save）]** をクリックします。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

関連トピック

7000 および 8000 シリーズ デバイスおよび NGIPSv の MTU 範囲 （661 ページ）
Snort® の再起動シナリオ （450 ページ）

論理スイッチドインターフェイスの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	Control	7000 & 8000 シリーズ	リーフのみ	Admin/Network Admin

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 スイッチドインターフェイスを追加するデバイスの横にある編集アイコン（  ）をクリックします。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [追加（Add）] ドロップダウン メニューから、[論理インターフェイスの追加（Add Logical Interface）] を選択します。

ステップ 4 [スイッチド（Switched）] をクリックします。

ステップ 5 [インターフェイス（Interface）] ドロップダウン リストから、VLAN タグ付きトラフィックを受信する物理インターフェイスを選択します。

ステップ 6 [VLAN タグ（VLAN Tag）] フィールドで、このインターフェイス上のインバウンド/アウトバウンド トラフィックに割り当てるタグ値を入力します。

このタグの値には、1 ～ 4094 の任意の整数を指定できます。

ステップ 7 セキュリティ ゾーンをスイッチド インターフェイスに関連付けるには、次のいずれかを実行します。

- [セキュリティ ゾーン（Security Zone）] ドロップダウン リストから既存のセキュリティ ゾーンを選択します。
- [新規（New）] を選択して新しいセキュリティ ゾーンを追加します。セキュリティ ゾーンおよびインターフェイス グループ オブジェクトの作成 （536 ページ） を参照してください。

ステップ 8 仮想スイッチをスイッチド インターフェイスに関連付けるには、次のいずれかを実行します。

- [仮想スイッチ（Virtual Switch）] ドロップダウン リストから既存の仮想スイッチを選択します。
- [新規（New）]を選択して新しい仮想スイッチを追加します。仮想スイッチの追加 （1576 ページ） を参照してください。

ステップ 9 スイッチドインターフェイスにトラフィックを処理させるには、[有効（Enabled）] チェックボックスをオンにします。

このチェックボックスをオフにすると、インターフェイスは無効になり、管理上はダウンした状態になります。物理インターフェイスを無効にする場合、それに関連付けられているすべての論理インターフェイスも無効にします。

ステップ 10 [MTU] フィールドに、最大伝送ユニット（MTU）を入力して、パケットの最大許容サイズを指定します。

MTU 値の範囲は管理対象デバイスのモデルとインターフェイス タイプによって異なる場合があります。

注意 デバイス上のすべての非管理インターフェイスの中で最大MTU値を変更し、設定変更を展開すると、Snortプロセスが再起動され、トラフィック インスペクションが一時的に中断されます。インスペクションは、変更したインターフェイスだけでなく、すべての非管理インターフェイスで中断されます。この中断によってトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびインターフェイスのタイプに応じて異なります。詳細については、「Snort® の再起動によるトラフィックの動作 （451 ページ）」を参照してください。

ステップ 11 **[保存（Save）]** をクリックします。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

関連トピック

7000 および 8000 シリーズ デバイスおよび NGIPSv の MTU 範囲 （661 ページ）
Snort® の再起動シナリオ （450 ページ）

論理スイッチド インターフェイスの削除

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	Control	7000 & 8000 シリーズ	リーフのみ	Admin/Network Admin

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 削除するスイッチド インターフェイスが含まれる管理対象デバイスの横にある編集アイコン（）をクリックします。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 削除する論理スイッチド インターフェイスの横にある削除アイコン（  ）をクリックします。

ステップ 4 入力を求められた場合、インターフェイスを削除することを確認します。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

仮想スイッチの設定

レイヤ 2 展開でスイッチド インターフェイスを使用できるようにするには、その前に仮想スイッチを設定し、スイッチドインターフェイスをその仮想スイッチに割り当てる必要があります。仮想スイッチとは、ネットワークを通過するインバウンドトラフィックとアウトバウンドトラフィックを処理する複数のスイッチド インターフェイスからなるグループのことです。

仮想スイッチの設定に関する注意事項

仮想スイッチは、[デバイス管理（Device Management）] ページの [仮想スイッチ（Virtual Switches）] タブから追加することができます。[仮想スイッチ（Virtual Switches）] タブには、デバイス上で設定済みのすべての仮想スイッチのリストが表示されます。このページには、各スイッチのサマリ情報が表示されます。

表 *104*: 仮想スイッチ テーブル ビューのフィールド

フィールド	説明
Name	仮想スイッチの名前。
Interfaces	仮想スイッチに割り当てられたすべてのスイッチ型インターフェイス。[Interfaces] タブで無効にしたインターフェイスは表示されません。
Hybrid Interface	仮想スイッチを仮想ルータに結合する、オプション設定のハイブリッドインターフェイス。
Unicast Packets	次の項目を含む、仮想スイッチのユニキャスト パケット統計： • 受信されたユニキャスト パケット • 転送されたユニキャスト パケット（ホストによるドロップを除く） • 誤ってドロップされたユニキャスト パケット

フィールド	説明
Broadcast Packets	次の項目を含む、仮想スイッチのブロードキャスト パケット統計： • 受信されたブロードキャスト パケット • 転送されたブロードキャスト パケット • 誤ってドロップされたブロードキャスト パケット

また、スイッチ型インターフェイスを設定するときにスイッチを追加することもできます。仮想スイッチには、スイッチ型インターフェイスだけ割り当てることができます。管理対象デバイス上でスイッチ型インターフェイスを設定する前に仮想スイッチを作成する必要がある場合は、空の仮想スイッチを作成し、あとでそれにインターフェイスを追加できます。

ヒント　既存の仮想スイッチを編集するには、スイッチの横にある編集アイコン（）をクリックします。

仮想スイッチの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	Control	7000 & 8000 シリーズ	リーフのみ	Admin/Network Admin

ステップ 1　**[Devices]** > **[Device Management]**を選択します。

ステップ 2　仮想スイッチを追加するデバイスの横にある編集アイコン（）をクリックします。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3　[仮想スイッチ（Virtual Switches）] タブをクリックします。

ステップ 4　[仮想スイッチの追加（Add Virtual Switch）] をクリックします。

ステップ 5　[名前（Name）] フィールドに名前を入力します。

ステップ 6　[使用可能（Available）] リストから、仮想スイッチに追加される 1 つ以上のスイッチド インターフェイスを選択します。

ヒント　[インターフェイス（Interfaces）] タブですでに無効にしたインターフェイスは使用できません。インターフェイスを追加した後で無効にすると、設定からそれが削除されます。

ステップ 7 [追加（Add）] をクリックします。

ステップ 8 仮想ルータに仮想スイッチを結びつけるには、[ハイブリッド インターフェイス（Hybrid Interface）] ドロップダウン リストからハイブリッド インターフェイスを選択します。

ステップ 9 必要に応じて、スイッチの詳細設定を行います。以下を参照してください。仮想スイッチの詳細設定（1577 ページ）

ステップ 10 **[保存（Save）]** をクリックします。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

関連トピック

論理ハイブリッド インターフェイス （1637 ページ）

仮想スイッチの詳細設定

スタティック MAC エントリを追加する（Adding Static MAC Entries）

仮想スイッチは、ネットワークからのリターン トラフィックにタグを付けることで、時間の経過と共に MAC アドレスを学習します。手動でスタティック MAC エントリを追加できます。そのようにすることで、MAC アドレスが特定のポート上にあることを指定します。そのポートからトラフィックを受信するかどうかに関わらず、MACアドレスはテーブル内でスタティック アドレスとして保持されます。仮想スイッチごとに 1 つ以上のスタティック MAC アドレスを指定できます。

スパニング ツリー プロトコル（STP）を有効にしてブリッジ プロトコル データ ユニット（BPDU）をドロップする（Enabling Spanning Tree Protocol (STP) and Dropping Bridge Protocol Data Units (BPDU)）

STP は、ネットワーク ループを防止するために使用されるネットワーク プロトコルです。BPDU は、ネットワーク ブリッジに関する情報を伝送し、ネットワークを介して交換されます。ネットワーク内に冗長リンクがある場合、プロトコルはBPDUを使用して最も高速なネットワーク リンクを識別し、選択します。ネットワーク リンクで障害が発生した場合、スパニング ツリーは既存の代替リンクにフェールオーバーします。

（注） Cisco では、高可用性ペアで 7000 または 8000 シリーズ デバイスに展開する予定の仮想スイッチを設定する場合は、STP を有効にすることを強く推奨しています。仮想スイッチが複数のネットワーク インターフェイス間のトラフィックを切り替える場合は、STP のみを有効にします。

仮想スイッチが複数の VLAN 間のトラフィックをルーティングする場合、ルータ オン ア スティックと同様に、BPDUはさまざまな論理スイッチドインターフェイスを介してデバイスを

出入りしますが、物理スイッチドインターフェイスは同じです。その結果、STP はデバイスを冗長ネットワーク ループとして識別します。特定のレイヤ 2 配置ではこれにより問題が生じる場合があります。それを防ぐため、トラフィックのモニタリング時にデバイスが BPDU をドロップするようにドメイン レベルで仮想スイッチを設定することができます。STP を無効にする場合は、BPDU をドロップするしかありません。

（注） 仮想スイッチが 1 つの物理インターフェイス上の VLAN 間でトラフィックをルーティングする場合にのみ、BPDU をドロップしてください。

厳格な TCP 強制を有効にする（Enabling Strict TCP Enforcement）

最大限の TCP セキュリティを実現するため、厳格な強制を有効にすることができます。この機能は、3 ウェイ ハンドシェイクが完了していない接続をブロックします。厳密な適用では次のパケットもブロックされます。

- 3 ウェイ ハンドシェイクが完了していない接続の非 SYN TCP パケット
- 応答側が SYN-ACK を送信する前に TCP 接続の発信側から送信された非 SYN/RST パケット
- SYN の後ではあるがセッションの確立前に TCP 接続の応答側から送信された非 SYN-ACK/RST パケット
- イニシエータまたはレスポンダからの、確立済みの TCP 接続上の SYN パケット

仮想スイッチを論理ハイブリッドインターフェイスに関連付けると、そのスイッチでは、論理ハイブリッド インターフェイスに関連付けられた仮想ルータと同じ厳密な TCP 強制設定が使用されることに注意してください。その場合、スイッチで厳格な TCP 強制を指定することはできません。

仮想スイッチの詳細設定の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	Control	7000 & 8000 シリーズ	リーフのみ	Admin/Network Admin

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 編集する仮想スイッチが含まれるデバイスの横にある編集アイコン（）をクリックします。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [仮想スイッチ（Virtual Switches）] タブをクリックします。

ステップ 4 編集する仮想スイッチの横にある編集アイコン（）をクリックします。

ステップ 5 [Advanced] タブをクリックします。

ステップ 6 スタティック MAC エントリを追加するには、[追加（Add）] をクリックします。

ステップ 7 [MAC アドレス（MAC Address）] フィールドで、2 桁の 16 進数 6 組をコロンで区切った標準形式を使用して、アドレスを入力します（たとえば 01:23:45:67:89:AB）。

（注） ブロードキャスト アドレス（00:00:00:00:00:00 と FF:FF:FF:FF:FF:FF）をスタティック MAC アドレスとして追加することはできません。

ステップ 8 [インターフェイス（Interface）] ドロップダウン リストから、MAC アドレスを割り当てるインターフェイスを選択します。

ステップ 9 [OK] をクリックします。

ステップ 10 スパニング ツリー プロトコルを有効にする場合は、[スパニング ツリー プロトコルを有効にする（Enable Spanning Tree Protocol）] チェックボックスをオンにします。

ステップ 11 厳密な TCP 強制を有効にするには、[厳密な TCP 強制（Strict TCP Enforcement）] チェックボックスをオンにします。

仮想スイッチを論理ハイブリッド インターフェイスに関連付けると、このオプションは表示されず、論理ハイブリッド インターフェイスに関連付けられた仮想ルータと同じ設定がスイッチで使用されます。

ステップ 12 ドメイン レベルで BPDU をドロップするには、[BPDU のドロップ（Drop BPDUs）] チェックボックスをオンにします。

ステップ 13 **[保存（Save）]** をクリックします。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

仮想スイッチの削除

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	Control	7000 & 8000 シリーズ	リーフのみ	Admin/Network Admin

仮想スイッチを削除すると、そのスイッチに割り当てられたスイッチドインターフェイスを別のスイッチに含めることができるようになります。

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 削除する仮想スイッチが含まれる管理対象デバイスの横にある編集アイコン（  ）をクリックします。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

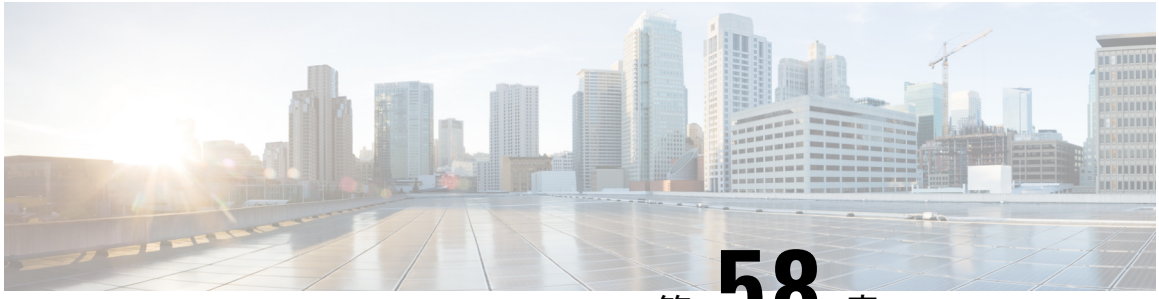
ステップ 3 [仮想スイッチ（Virtual Switches）] タブをクリックします。

ステップ 4 削除する仮想スイッチの横にある削除アイコン（  ）をクリックします。

ステップ 5 プロンプトが表示されたら、仮想スイッチを削除することを確認します。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。



第 58 章

仮想ルータのセットアップ

以下のトピックでは、Firepower システムで仮想ルータをセットアップする方法について説明します。

仮想ルータ

レイヤ3展開の管理対象デバイスは、2つ以上のインターフェイス間のトラフィックをルーティングするように設定できます。トラフィックをルーティングするには、IP アドレスを各インターフェイスに割り当ててから、これらのインターフェイスを仮想ルータに割り当てる必要があります。仮想ルータに割り当てるインターフェイスは、物理インターフェイス、論理インターフェイス、または Link Aggregation Group（LAG）インターフェイスのいずれかにできます。

システムは、宛先アドレスに従ってパケット転送の決定を行うことで、パケットをルーティングするように設定できます。ルーテッドインターフェイスとして設定されるインターフェイスは、レイヤ3トラフィックを受信し、転送します。ルータは転送基準に基づいて発信インター

フェイスから宛先を取得し、アクセス コントロール ルールが、適用するセキュリティ ポリシーを指定します。

レイヤ 3 配置では、スタティック ルートを定義できます。さらに、Routing Information Protocol（RIP）および Open Shortest Path First（OSPF）のダイナミック ルーティング プロトコルを設定できます。さらに、スタティック ルートと RIP、またはスタティック ルートと OSPF の組み合わせを設定することもできます。

7000 または 8000 シリーズ デバイス上には、仮想ルータ、物理ルーテッド インターフェイス、または論理ルーテッド インターフェイスしか設定できないことに注意してください。

注意 レイヤ 3 展開に何らかの理由で障害が発生した場合、デバイスはトラフィックを転送しなくなります。

関連トピック

LAG 設定 （1620 ページ）

ルーテッド インターフェイス

物理的設定または論理的設定のいずれかでルーテッド インターフェイスをセットアップできます。タグのない VLAN トラフィックを処理するために、物理的ルーテッド インターフェイスを設定できます。指定された VLAN タグのあるトラフィックを処理するために、論理的ルーテッド インターフェイスも作成できます。

レイヤ 3 の展開では、システムは待機しているルーテッド インターフェイスのない外部の物理的インターフェイスから受信したトラフィックをドロップします。このシステムでは、以下の場合パケットをドロップします。

- VLAN タブのないパケットを受信した場合、そのポート向けにルーテッド インターフェイスを設定したことがない場合。
- VLAN タグ付きパケットを受信した場合、そのポートの論理的ルーテッド インターフェイスを設定したことがない場合。

このシステムでは、ルールを評価するか、決定を転送する前にイングレスの最も外側の VLAN タグを削除して、スイッチ インターフェイス上で VLAN タグで受信したトラフィックを処理します。VLAN タグ付きの論理ルーテッド インターフェイスを通ってデバイスから離れるパケットは出力で関連付けられた VLAN タグによりカプセル化されます。このシステムでは、削除プロセスの完了後、VLAN タブで受信したトラフィックをドロップします。

スタティック Address Resolution Protocol（ARP）エントリをルーテッド インターフェイスに追加できます。外部ホストがトラフィックを送信する、ローカル ネットワーク上の宛先 IP アドレスの MAC アドレスを知る必要がある場合、ARP 要求を送信します。スタティック ARP エントリを設定する場合、仮想ルータは IP アドレスや関連付けられた MAC アドレスに応答します。

論理ルーテッドLAGインターフェイスの[ICMP有効応答（ICMP Enable Responses）]オプションを無効にしても、すべてのシナリオでICMP応答が抑制されるわけではありません。宛先IPがルーテッド インターフェイスのIPで、プロトコルがICMPであるパケットをドロップするように、アクセス コントロール ポリシーにネットワークベースのルールを追加できます。

管理対象デバイスの[ローカル ルータ トラフィックを検査する（Inspect Local Router Traffic）]オプションを有効にすると、システムは、ホストに到着する前にパケットをドロップし、これによっていかなる応答も阻止できます。

MTU 値の範囲は管理対象デバイスのモデルとインターフェイス タイプによって異なる場合があります。

注意 デバイス上のすべての非管理インターフェイスの中で最大 MTU 値を変更し、設定変更を展開すると、Snort プロセスが再起動され、トラフィック インスペクションが一時的に中断されます。インスペクションは、変更したインターフェイスだけでなく、すべての非管理インターフェイスで中断されます。この中断によってトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびインターフェイスのタイプに応じて異なります。詳細については、「Snort® の再起動によるトラフィックの動作 （451 ページ）」を参照してください。

上位の物理的インターフェイスをインラインまたはパッシブに変更する場合、システムでは、関連付けられた論理的インターフェイをすべて削除します。

関連トピック

デバイスの詳細設定 （299 ページ）
7000 および 8000 シリーズ デバイスおよび NGIPSv の MTU 範囲 （661 ページ）
Snort® の再起動シナリオ （450 ページ）

物理ルーテッド インターフェイスの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
該当なし	Control	7000 & 8000 シリーズ	リーフのみ	Admin/Network Admin

ルーテッド インターフェイスとして管理対象デバイスの 1 つ以上の物理ポートを設定できます。トラフィックをルーティングする前に、物理ルーテッドインターフェイスを仮想ルータに割り当てる必要があります。

⚠

注意 ルーテッド インターフェイス ペアを 7000 または 8000 シリーズ デバイスに追加すると、設定の変更を展開する際に Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、ターゲットデバイスがトラフィックを処理する方法に応じて異なります。詳細はSnort® の再起動によるトラフィックの動作 （451 ページ）を参照してください。

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 変更するデバイスの横にある編集アイコン（）をクリックします。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 変更するインターフェイスの横にある編集アイコン（）をクリックします。

ステップ 4 [ルーテッド（Routed）] をクリックして、ルーテッド インターフェイス オプションを表示します。

ステップ 5 セキュリティ ゾーンを適用するには、次のいずれかを実行します。

- [セキュリティ ゾーン（Security Zone）] ドロップダウン リストから既存のセキュリティ ゾーンを選択します。
- [新規（New）] を選択して新しいセキュリティ ゾーンを追加します。セキュリティ ゾーンおよびインターフェイス グループ オブジェクトの作成 （536 ページ） を参照してください。

ステップ 6 仮想ルータを指定するには、次のいずれかを実行します。

- [仮想ルータ（Virtual Router）] ドロップダウン リストから既存の仮想ルータを選択します。
- [新規（New）] を選択して新しい仮想ルータ 仮想ルータの追加 （1592 ページ）を追加します。

ステップ 7 ルーテッドインターフェイスにトラフィックを処理させるには、[有効（Enabled）] チェックボックスをオンにします。このチェックボックスをオフにすると、インターフェイスは無効になり、ユーザはセキュリティ上の理由によりアクセスできなくなります。

ステップ 8 [モード（Mode）] ドロップダウン リストからリンク モードを指定するオプションを選択するか、または [自動ネゴシエーション（Auto Negotiation）] を選択して、速度とデュプレックス設定を自動的にネゴシエートするようインターフェイスを設定します。

モード設定は銅線インターフェイスにのみ使用できます。

8000 シリーズ アプライアンスのインターフェイスは、半二重オプションをサポートしません。

ステップ 9 [MDI/MDIX] ドロップダウン リストから、インターフェイスの設定対象として MDI（メディア依存型インターフェイス）、MDIX（メディア依存型インターフェイス クロスオーバー）、または自動 MDIX のいずれかを指定するオプションを選択します。

通常、[MDI/MDIX] は [自動 MDIX（Auto-MDIX）] に設定します。これにより、MDI と MDIX の間の切り替えが自動的に処理され、リンクが確立されます。

[MDI/MDIX] 設定は銅線インターフェイスでのみ使用できます。

ステップ 10 [MTU] フィールドに、最大伝送ユニット（MTU）を入力して、パケットの最大許容サイズを指定します。

MTU はレイヤ 2 MTU/MRU であり、レイヤ 3 MTU ではありません。

MTU 値の範囲は管理対象デバイスのモデルとインターフェイス タイプによって異なる場合があります。

注意 デバイス上のすべての非管理インターフェイスの中で最大MTU値を変更し、設定変更を展開すると、Snortプロセスが再起動され、トラフィック インスペクションが一時的に中断されます。インスペクションは、変更したインターフェイスだけでなく、すべての非管理インターフェイスで中断されます。この中断によってトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびインターフェイスのタイプに応じて異なります。詳細については、「Snort® の再起動によるトラフィックの動作 （451 ページ）」を参照してください。

ステップ 11 [ICMP] の横にある [応答を有効にする（Enable Responses）] チェックボックスをオンにして、インターフェイスを ping や traceroute などの ICMP トラフィックに応答可能にします。

ステップ 12 [IPv6 NDP] の横にある [ルータ アドバタイズメントを有効にする（Enable Router Advertisement）] チェックボックスをオンにして、インターフェイスがルータ アドバタイズメントを伝送できるようにします。

ステップ 13 IP アドレスを追加するには、[追加（Add）] をクリックします。

ステップ 14 [アドレス（Address）] フィールドに、ルーテッド インターフェイスの IP アドレスとサブネット マスクを CIDR 表記で入力します。

次の点に注意してください。

- ネットワークおよびブロードキャストアドレス、またはスタティック MAC アドレス 00:00:00:00:00:00 および FF:FF:FF:FF:FF:FF は追加できません。
- サブネット マスクに関係なく、仮想ルータのインターフェイスに同じ IP アドレスを追加できません。

ステップ 15 組織が IPv6 アドレスを使用している場合、インターフェイスの IP アドレスを自動的に設定するには、[IPv6] フィールドの横の [アドレス自動設定（Address Autoconfiguration）] チェックボックスをオンにします。

ステップ 16 [タイプ（Type）] には、[普通（Normal）] または [SFRP] を選択します。

SFRP オプションの詳細についてはSFRP の設定 （1589 ページ）を参照してください。

ステップ 17 [OK] をクリックします。

- IP アドレスを編集するには、編集アイコン（  ）をクリックします。
- IP アドレスを削除するには、削除アイコン（  ）をクリックします。

IP アドレスを 7000 または 8000 シリーズ デバイスのルーテッド インターフェイスに追加する場合、ハイアベイラビリティ ペア ピアのルーテッド インターフェイスに対応する IP アドレスを追加する必要があります。

ステップ 18 スタティック ARP エントリを追加するには、[追加（Add）] をクリックします。

ステップ 19 [IP アドレス（IP Address）] フィールドに、スタティック ARP エントリの IP アドレスを入力します。

ステップ 20 [MAC アドレス（MAC Address）] フィールドに、IP アドレスに関連付ける MAC アドレスを入力します。2 桁の 16 進数の 6 個のグループをコロンで区切る標準アドレス形式を使用します（たとえば、01:23:45:67:89:AB）。

ステップ 21 [OK] をクリックします。

ステップ 22 [保存（Save）] をクリックします。

次のタスク

設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

関連トピック

7000 および 8000 シリーズ デバイスおよび NGIPSv の MTU 範囲 （661 ページ）
Snort® の再起動シナリオ （450 ページ）

論理ルーテッドインターフェイスの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
該当なし	Control	7000 & 8000 シリーズ	リーフのみ	Admin/Network Admin

各物理ルーテッド インターフェイスで、複数の論理ルーテッド インターフェイスを追加できます。物理インターフェイスで受信される VLAN タグ付きトラフィックを処理するには、各論理インターフェイスをその特定のタグに関連付ける必要があります。トラフィックをルーティングするには、論理ルーテッドインターフェイスを仮想ルータに割り当てる必要があります。

⚠

注意 7000 または 8000 シリーズ デバイス 設定の変更を展開する際に Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、ターゲット デバイスがトラフィックを処理する方法に応じて異なります。詳細はSnort® の再起動によるトラフィックの動作 （451 ページ）を参照してください。 でのルーテッド インターフェイス ペアの追加

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 変更するデバイスの横にある編集アイコン（✎）をクリックします。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [インターフェイスの追加（Add Interface）] をクリックします。

ステップ 4 [ルーテッド（Routed）] をクリックして、ルーテッド インターフェイス オプションを表示します。

ステップ 5 [インターフェイス（Interface）] ドロップダウン リストから、論理インターフェイスを追加する物理インターフェイスを選択します。

ステップ 6 [VLAN タグ（VLAN Tag）] フィールドで、このインターフェイス上のインバウンド/アウトバウンド トラフィックに割り当てるタグ値を入力します。この値には、1 ～ 4094 の任意の整数を指定できます。

ステップ 7 セキュリティ ゾーンを適用するには、次のいずれかを実行します。

- [セキュリティ ゾーン（Security Zone）] ドロップダウン リストから既存のセキュリティ ゾーンを選択します。
- [新規（New）] を選択して新しいセキュリティ ゾーンを追加します。セキュリティ ゾーンおよびインターフェイス グループ オブジェクトの作成 （536 ページ） を参照してください。

ステップ 8 仮想ルータを指定するには、次のいずれかを実行します。

- [仮想ルータ（Virtual Router）] ドロップダウン リストから既存の仮想ルータを選択します。
- [新規（New）] を選択して新しい仮想ルータ 仮想ルータの追加 （1592 ページ）を追加します。

ステップ 9 ルーテッドインターフェイスにトラフィックを処理させるには、[有効（Enabled）] チェックボックスをオンにします。

このチェックボックスをオフにすると、インターフェイスは無効になり、管理上はダウンした状態になります。物理インターフェイスを無効にする場合、それに関連付けられているすべての論理インターフェイスも無効にします。

ステップ 10 [MTU] フィールドに、最大伝送ユニット（MTU）を入力して、パケットの最大許容サイズを指定します。

MTU はレイヤ 2 MTU/MRU であり、レイヤ 3 MTU ではありません。

MTU 値の範囲は管理対象デバイスのモデルとインターフェイス タイプによって異なる場合があります。

注意 デバイス上のすべての非管理インターフェイスの中で最大 MTU 値を変更し、設定変更を展開すると、Snort プロセスが再起動され、トラフィック インスペクションが一時的に中断されます。インスペクションは、変更したインターフェイスだけでなく、すべての非管理インターフェイスで中断されます。この中断によってトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびインターフェイスのタイプに応じて異なります。詳細については、「Snort® の再起動によるトラフィックの動作 （451 ページ）」を参照してください。

ステップ 11 [ICMP] の横にある [応答を有効にする（Enable Responses）] チェックボックスをオンにして、他のルータ、中間デバイス、またはホストに更新またはエラー情報を伝送します。

ステップ 12 [IPv6 NDP] の横にある [ルータ アドバタイズメントを有効にする（Enable Router Advertisement）] チェックボックスをオンにして、インターフェイスがルータ アドバタイズメントを伝送できるようにします。

ステップ 13 IP アドレスを追加するには、[追加（Add）] をクリックします。

ステップ 14 [アドレス（Address）] フィールドに、IP アドレスを CIDR 表記で入力します。

次の点に注意してください。

- ネットワークおよびブロードキャストアドレス、またはスタティック MAC アドレス 00:00:00:00:00:00 および FF:FF:FF:FF:FF:FF は追加できません。
- サブネット マスクに関係なく、仮想ルータのインターフェイスに同じ IP アドレスを追加できません。

ステップ 15 IPv6 を使用した環境で、インターフェイスの IP アドレスを自動設定するには、[IPv6] フィールドの横にある [アドレスの自動設定（Address Autoconfiguration）] チェックボックスを選択します。

ステップ 16 [タイプ（Type）] には、[普通（Normal）] または [SFRP] を選択します。

SFRP オプションの詳細についてはSFRP の設定 （1589 ページ）を参照してください。

ステップ 17 [OK] をクリックします。

- IP アドレスを編集するには、編集アイコン（  ）をクリックします。
- IP アドレスを削除するには、削除アイコン（  ）をクリックします。

IP アドレスを 7000 または 8000 シリーズ デバイスの高可用性ペアのルーテッドインターフェイスに追加する場合、高可用性ペアピアのルーテッドインターフェイスに対応する IP アドレスを追加する必要があります。

ステップ 18 スタティック ARP エントリを追加するには、[追加（Add）] をクリックします。

ステップ 19 [IP アドレス（IP Address）] フィールドに、スタティック ARP エントリの IP アドレスを入力します。

ステップ 20 [MAC アドレス（MAC Address）] フィールドに、IP アドレスに関連付ける MAC アドレスを入力します。2 桁の 16 進数の 6 個のグループをコロンで区切る標準アドレス形式を使用します（たとえば、01:23:45:67:89:AB）。

ステップ 21 [OK] をクリックします。スタティック ARP エントリが追加されます。

ステップ 22 **[保存（Save）]** をクリックします。

次のタスク

設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

関連トピック

7000 および 8000 シリーズ デバイスおよび NGIPSv の MTU 範囲 （661 ページ）
Snort® の再起動シナリオ （450 ページ）

論理ルーテッド インターフェイスの削除

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	Control	7000 & 8000 シリーズ	リーフのみ	Admin/Network Admin

論理ルーテッドインターフェイスを削除すると、帰属する物理インターフェイスのほか、割り当てられた仮想ルータおよびセキュリティ ゾーンからも削除されます。

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 変更するデバイスの横にある編集アイコン（）をクリックします。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 削除する論理ルーテッド インターフェイスの横にある削除アイコン（）をクリックします。

ステップ 4 入力を求められた場合、インターフェイスを削除することを確認します。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

SFRP の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	Control	7000 & 8000 シリーズ	リーフのみ	Admin/Network Admin

Cisco 冗長プロトコル（SFRP）を設定して、7000 または 8000 シリーズ デバイスのハイ アベイラビリティ ペアまたは個別のデバイスのハイ アベイラビリティを得るためのネットワーク冗長性を実現できます。SFRP は IPv4 と IPv6 の両方のアドレスのゲートウェイ冗長性を提供します。ルーテッド インターフェイスおよびハイブリッド インターフェイスの SFRP を設定できます。

インターフェイスが個別のデバイスに設定される場合、同じブロードキャスト ドメインに存在する必要があります。インターフェイスのうち少なくとも 1 つをマスターに指定し、同じ数のバックアップを指定する必要があります。システムは IP アドレスごとに 1 つのマスターと 1 つのバックアップのみをサポートします。ネットワーク接続が失われた場合、システムは自動的にバックアップをマスターに昇格し、接続を維持します。

SFRP に設定するオプションは、SFRP インターフェイス グループのすべてのインターフェイスで同じにする必要があります。グループ内の複数の IP アドレスのマスターとバックアップの状態は同じである必要があります。そのため、 IP アドレスを追加または編集する場合、そのアドレスに設定する状態はグループ内のすべてのアドレスに適用されます。セキュリティのために、グループ内のインターフェイス間で共有される [グループ ID（Group ID）] と [共有秘密（Shared Secret）] の値を入力する必要があります。

仮想ルータで SFRP IP アドレスを有効にするには、1 つの非 SFRP IP アドレスを設定する必要もあります。インターフェイスごとに、非 SFRP アドレスを 1 つだけ設定する必要があることにご注意ください。

あるグループに含まれる SFRP はすべて一緒にフェールオーバーするので、同じ仮想ルータ上のすべての SFRP は同じ SFRP グループに属する必要があります。さらに、NAT、HA 状態共有、または VPN を使用している場合は、高可用性ペアの各デバイスに HA リンク インターフェイスを設定する必要もあります。HA リンク インターフェイスの詳細については、HA リンク インターフェイスの設定 （658 ページ）を参照してください。

高可用性ペアの 7000 または 8000 シリーズ デバイスの場合、共有秘密を指定すると、SFRP の IP 設定とともに高可用性ペアのピアにコピーされます。共有秘密は、ピアのデータを認証します。

（注） 7000 または 8000 シリーズ デバイスのハイ アベイラビリティ ペアのルーティングされたインターフェイスまたはハイブリッドインターフェイスで SFRP IP アドレスがすでに 1 つ構成されている場合、複数の非 SFRP IP アドレスを有効にすることは推奨しません。7000 または 8000 シリーズ デバイスのハイ アベイラビリティ ペアがスタンバイ モードでフェールオーバーした場合、NAT は実行されません。

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 変更するデバイスの横にある編集アイコン（）をクリックします。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 SFRP を設定するインターフェイスの横にある編集アイコン（）をクリックします。

ステップ 4 SFRP を設定するインターフェイスのタイプ（[ルーテッド（Routed）] または [ハイブリッド（Hybrid）]）を選択します。

ステップ 5 IP アドレスを追加または編集するときに SFRP を設定できます。[追加（Add）] をクリックして、IP アドレスを追加します。IP アドレスを編集するには、編集アイコン（）をクリックします。

ステップ 6 [タイプ（Type）] に [SFRP] を選択して SFRP オプションを表示します。

ステップ 7 [グループ ID（Group ID）] フィールドに、SFRP 用に設定されたマスターまたはバックアップ インターフェイス グループを指定する値を入力します。

ステップ 8 [優先順位（Priority）] で、[マスター（Master）] または [バックアップ（Backup）] のどちらかを選択して、優先するインターフェイスを指定します。

- 個別のデバイスの場合、1 つのデバイスにマスターへのインターフェイスを 1 個設定し、2 番目のデバイスにバックアップへのインターフェイスを設定する必要があります。
- 7000 または 8000 シリーズ デバイスのハイ アベイラビリティ ペアの場合、マスターとして 1 個のインターフェイスを設定すると、もう 1 個のインターフェイスは自動的にバックアップになります。

ステップ 9 [共有秘密（Shared Secret）] フィールドに、共有秘密を入力します。

[共有秘密（Shared Secret）] フィールドには、7000 または 8000 シリーズ デバイスのハイ アベイラビリティ ペア内のグループに関するデータが自動的に入力されます。

ステップ 10 [**アドバタイズメント間隔（秒単位）（Adv. Interval (seconds)**] フィールドに、レイヤ 3 トラフィックのルート アドバタイズメントの間隔を入力します。

ステップ 11 [OK] をクリックします。

ステップ 12 [保存（Save）] をクリックします。

次のタスク

設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

関連トピック

7000 および 8000 シリーズ デバイスのハイ アベイラビリティについて （679 ページ）

仮想ルータ設定

注意 7000 または 8000 シリーズ デバイスで仮想ルータを追加した場合 設定の変更を展開する際に Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、ターゲットデバイスがトラフィックを処理する方法に応じて異なります。詳細はSnort® の再起動によるトラフィックの動作 （451 ページ）を参照してください。

レイヤ3配置でルーテッドインターフェイスを使用する前に、仮想ルータを設定し、ルーテッド インターフェイスを割り当てる必要があります。仮想ルータは、レイヤ 3 トラフィックをルーティングするルーテッド インターフェイスのグループです。

1 つの仮想ルータに割り当てることができるのは、ルーテッドインターフェイスとハイブリッド インターフェイスのみです。

最大限の TCP セキュリティを実現するため、厳格な強制を有効にすることができます。この機能は、3 ウェイ ハンドシェイクが完了していない接続をブロックします。厳密な適用では次のパケットもブロックされます。

- 3 ウェイ ハンドシェイクが完了していない接続の非 SYN TCP パケット
- 応答側が SYN-ACK を送信する前に TCP 接続の発信側から送信された非 SYN/RST パケット
- SYN の後ではあるがセッションの確立前に TCP 接続の応答側から送信された非 SYN-ACK/RST パケット
- 発信側または応答側のどちらかから送信された、確立された TCP 接続の SYN パケット

レイヤ 3 インターフェイスの設定を非レイヤ 3 インターフェイスに変更したり、仮想ルータからレイヤ3インターフェイスを削除したりすると、ルータは無効な状態になる場合があることに注意してください。たとえば、DHCPv6 で使用されている場合、アップストリームとダウンストリームの不一致が生じることがあります。

仮想ルータの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	Control	7000 & 8000 シリーズ	リーフのみ	Admin/Network Admin

[デバイス管理（Device Management）] ページの [仮想ルータ（Virtual Routers）] タブから仮想ルータを追加できます。ルーテッドインターフェイスを設定するときに、ルータを追加することもできます。

管理対象デバイスのインターフェイスを設定する前に仮想ルータを作成する場合は、空の仮想ルータを作成し、後でインターフェイスを追加できます。

注意 7000 または 8000 シリーズ デバイスで仮想ルータを追加した場合 設定の変更を展開する際に Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、ターゲットデバイスがトラフィックを処理する方法に応じて異なります。詳細は Snort® の再起動によるトラフィックの動作 （451 ページ）を参照してください。

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 変更するデバイスの横にある編集アイコン（  ）をクリックします。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [仮想ルータ（Virtual Routers）] タブをクリックします。

ヒント デバイスが高可用性ペアのスタックにある場合、[選択済みデバイス（Selected Device）] ドロップダウン リストから、変更するスタックを選択します。

ステップ 4 [仮想ルータの追加（Add Virtual Router）] をクリックします。

ステップ 5 [名前（Name）] フィールドに仮想ルータの名前を入力します。英数字とスペースを使用できます。

ステップ 6 [IPv6 サポート（IPv6 Support）] チェックボックスをオンまたはオフにして、仮想ルータで IPv6 スタティック ルーティング、OSPFv3 と RIPng を設定します。

ステップ 7 TCP の厳密な適用をやめるには、[TCP の厳密な適用（Strict TCP Enforcement）] チェックボックスをオフにします。このオプションは、デフォルトで有効です。

ステップ 8 [インターフェイス（Interfaces）] の [使用可能（Available）] リストから 1 つまたは複数のインターフェイスを選択し、[追加（Add）] をクリックします。

[使用可能（Available）] リストには、仮想ルータに割り当てることが可能なデバイス上のすべての有効なレイヤ 3 インターフェイス（ルーテッドおよびハイブリッド）が含まれます。

ヒント 仮想ルータからルーテッドまたはハイブリッドインターフェイスを削除するには、削除アイコン（）をクリックします。[Interfaces] タブで、設定したインターフェイスを無効にすることによっても削除できます。

ステップ 9 **[保存（Save）]** をクリックします。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

DHCP リレー

DHCP はインターネット ホストに設定パラメータを提供します。IP アドレスを未取得の DHCP クライアントは、ブロードキャスト ドメインの外にある DHCP サーバと直接通信できません。DHCP クライアントが DHCP サーバと通信できるようにするには、クライアントがサーバと同じブロードキャスト ドメイン内にない状況に対応できるように DHCP リレー インスタンスを設定します。

ユーザが設定した各仮想ルータの DHCP リレーを設定できます。デフォルトでは、この機能はディセーブルになっています。DHCPv4 リレーまたは DHCPv6 リレーのどちらかを有効にできます。

（注） 同じデバイスで実行中の複数の仮想ルータを介して DHCPv6 リレー チェーンを実行することはできません。

DHCPv4 リレーの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	Control	7000 & 8000 シリーズ	リーフのみ	Admin/Network Admin

次の手順は、仮想ルータで DHCPv4 リレーを設定する方法について説明します。

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 変更するデバイスの横にある編集アイコン（）をクリックします。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [仮想ルータ（Virtual Routers）] タブをクリックします。

ステップ 4 変更する仮想ルータの横にある編集アイコン（）をクリックします。

ステップ 5 [DHCPv4（DHCPv6）] チェックボックスをオンにします。

ステップ 6 [サーバ（Servers）] フィールドに、サーバの IP アドレスを入力します。

ステップ 7 [追加（Add）] をクリックします。

最大 4 台の DHCP サーバを追加できます。

ステップ 8 [最大ホップ（Max Hops）] フィールドに 1 ～ 255 の最大ホップ カウントを入力します。

ステップ 9 **[保存（Save）]** をクリックします。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

DHCPv6 リレーの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	Control	7000 & 8000 シリーズ	リーフのみ	Admin/Network Admin

同じデバイスで実行中の複数の仮想ルータを介して DHCPv6 リレー チェーンを実行することはできません。

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 変更するデバイスの横にある編集アイコン（）をクリックします。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [仮想ルータ（Virtual Routers）] タブをクリックします。

ステップ 4 DHCP リレーを設定する仮想ルータの横にある編集アイコン（）をクリックします。

ステップ 5 [DHCPv6] チェックボックスをオンにします。

ステップ 6 [インターフェイス（Interfaces）] フィールドで、仮想ルータに割り当てられている 1 つ以上のインターフェイスの横にあるチェックボックスをオンにします。

ヒント　DHCPv6 リレー用に設定されているインターフェイスは、[インターフェイス（Interfaces）] タブから無効にできません。最初に [DHCPv6 リレー インターフェイス（DHCPv6 Relay interfaces）] チェックボックスをオフにして、設定を保存する必要があります。

ステップ 7 選択したインターフェイスの横にあるドロップダウン アイコンをクリックし、インターフェイスが DHCP 要求をリレーする方式として、[アップストリーム（Upstream）]、[ダウンストリーム（Downstream）]、または [両方（Both）] を選択します。

（注）　少なくとも 1 つのダウンストリーム インターフェイスと 1 つのアップストリーム インターフェイスを含める必要があります。[両方（Both）] を選択することは、インターフェイスがダウンストリームとアップストリームの両方であることを意味します。

ステップ 8 [最大ホップ（Max Hops）] フィールドに 1 ～ 255 の最大ホップ カウントを入力します。

ステップ 9 **[保存（Save）]** をクリックします。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

スタティック ルート

スタティック ルーティングにより、ルータを通過するトラフィックの IP アドレスに関するルールを作成することができます。これはネットワークの現在のトポロジに関して他のルータとの通信がないため、仮想ルータのパス選択を設定する最も簡単な方法です。

割り当てられた仮想ルータがパケットをルーティングできない DHCPv4 サーバでは、IP インターフェイスへのルーティングを設定しないでください。これを行うと、以前に指定したルーティング可能な DHCP4 サーバがルーティングできなくなります。

スタティック ルート テーブルには次の表に示すように、各ルートに関するサマリー情報が含まれます。

表 *105:* スタティック ルート テーブル ビュー フィールド

フィールド	説明
Enabled	このルートが現在有効であるか、無効であるかを示します。
Name	スタティック ルートの名前。
Destination	トラフィックがルーティングされる宛先ネットワーク。

フィールド	説明
Type	このルートに対して実行するアクションを指定します。次のいずれかです。 • IP：パケットが、隣接ルータのアドレスに転送されることを指定します。 • [インターフェイス（Interface）]：そのインターフェイスを介してトラフィックが直接接続されたネットワーク上のホストにルーティングされるインターフェイスにパケットが転送されることを指定します。 • [破棄（Discard）]：スタティック ルートでパケットをドロップすることを指定します。
ゲートウェイ（Gateway）	スタティック ルートのタイプとして IP を選択した場合はターゲット IP アドレス、またはスタティック ルート タイプとしてインターフェイスを選択した場合はインターフェイス。
Preference	ルート選択を決定します。同じ宛先に対する複数のルートが存在する場合、より高い優先順位のルートが選択されます。

静的ルート テーブルの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	Control	7000 & 8000 シリーズ	任意（Any）	Admin/Network Admin

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 表示するデバイスの横にある編集アイコン（  ）をクリックします。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [仮想ルータ（Virtual Routers）] タブをクリックします。

ステップ 4 静的ルートを表示する仮想ルータの横にある編集アイコン（  ）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は子孫ドメインに属しているか、設定を変更する権限がありません。

ステップ 5 [静的（Static）] タブをクリックします。

スタティック ルートの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	Control	7000 & 8000 シリーズ	リーフのみ	Admin/Network Admin

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 スタティック ルートを追加するデバイスの横にある編集アイコン（）をクリックします。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [仮想ルータ（Virtual Routers）] タブをクリックします。

ステップ 4 スタティック ルートを追加する仮想ルータの横にある編集アイコン（）をクリックします。

ステップ 5 [静的（Static）] をクリックして、スタティック ルートのオプションを表示します。

ステップ 6 [静的ルートの追加（Add Static Route）] をクリックします。

ステップ 7 [ルート名（Route Name）] フィールドに、スタティック ルートの名前を入力します。英数字とスペースを使用できます。

ステップ 8 [有効（Enabled）] チェックボックスをオンにして、ルートが現在有効であることを指定します。

ステップ 9 [優先（Preference）] フィールドに、ルート選択を決定するための 1 ～ 65535 の数値を入力します。

（注） 同じ宛先に対する複数のルートが存在する場合、より高い優先順位のルートが使用されます。

ステップ 10 [タイプ（Type）] ドロップダウン リストから、設定するスタティック ルートのタイプを選択します。

ステップ 11 [宛先（Destination）] フィールドに、トラフィックがルーティングされる宛先ネットワークの IP アドレスを入力します。

ステップ 12 [ゲートウェイ（Gateway）] フィールドでは、次の 2 つの選択肢があります。

- スタティック ルート タイプとして [IP] を選択した場合は、IP アドレスを選択します。
- スタティック ルート タイプとして [インターフェイス（Interface）] を選択した場合は、ドロップダウン リストから有効なインターフェイスを選択します。

ヒント [インターフェイス（Interfaces）] タブから無効にしたインターフェイスは使用できません。追加したインターフェイスを無効にすると、設定から削除されます。

ステップ 13 [OK] をクリックします。

ステップ 14 [保存（Save）] をクリックします。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

ダイナミック ルーティング

ダイナミックつまり適応型のルーティングは、ルーティングプロトコルを使用して、ルートが取るパスをネットワーク条件の変化に応じて変更します。この適応は、できるだけ多くのルートの有効性を維持し、変更に応じて宛先に到達可能とすることを目的としたものです。このため、他のパスを選択できる限り、ネットワークはノードまたはノード間の接続の損失といった障害を「迂回」することができます。ダイナミックルーティングなしでルータを設定することも、Routing Information Protocol（RIP）または Open Shortest Path First（OSPF）のルーティングプロトコルを設定することもできます。

RIP コンフィギュレーション

Routing Information Protocol（RIP）はホップ カウントを使用してルートを決定する、小規模な IP ネットワーク向けのダイナミック ルーティング プロトコルです。最適なルートは最小数のホップを使用します。RIP で許可されるホップの最大数は 15 です。このホップ制限により、RIP がサポートできるネットワークのサイズも制限されます。

RIP 設定のインターフェイスの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	Control	7000 & 8000 シリーズ	リーフのみ	Admin/Network Admin

RIP を設定する際、RIP を設定する仮想ルータにすでに含まれているインターフェイスを選択する必要があります。無効になっているインターフェイスを使用することはできません。

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 変更するデバイスの横にある編集アイコン（  ）をクリックします。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [仮想ルータ（Virtual Routers）] タブをクリックします。

ステップ 4 変更する仮想ルータの横にある編集アイコン（）をクリックします。

ステップ 5 [ダイナミック ルーティング（Dynamic Routing）] をクリックして、ダイナミック ルーティングのオプションを表示します。

ステップ 6 [RIP] をクリックして、RIP オプションを表示します。

ステップ 7 [インターフェイス（Interfaces）] の下で、追加アイコン（）をクリックします。

ステップ 8 [名前（Name）] ドロップダウン リストから、RIP を設定するインターフェイスを選択します。

ヒント [インターフェイス（Interfaces）] タブから無効にしたインターフェイスは使用できません。追加したインターフェイスを無効にすると、設定から削除されます。

ステップ 9 [メトリック（Metric）] フィールドに、インターフェイスのメトリックを入力します。異なる RIP インスタンスからのルートを使用可能で、すべてが同じ設定である場合、メトリックが最小のルートが優先ルートになります。

ステップ 10 [モード（Mode）] ドロップダウン リストから、次のいずれかのオプションを選択します。

- [マルチキャスト（Multicast）]：RIP が指定されたアドレスですべての隣接ルータにルーティング テーブル全体をマルチキャストするデフォルトのモード。
- [Broadcast]：マルチキャスト モードが可能な場合でも、RIP にブロードキャスト（RIPv1 など）の使用を強制します。
- [Quiet]：RIP は、このインターフェイスに定期メッセージを送信しません。
- [No Listen]：RIP は、このインターフェイスに送信しますが、リッスンしません。

ステップ 11 **[保存（Save）]** をクリックします。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

RIP の認証設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	Control	7000 & 8000 シリーズ	リーフのみ	Admin/Network Admin

RIP 認証では、仮想ルータに設定した認証プロファイルの 1 つが使用されます。

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 変更するデバイスの横にある編集アイコン（）をクリックします。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [仮想ルータ（Virtual Routers）] タブをクリックします。

ステップ 4 RIP 認証プロファイルを追加する仮想ルータの横にある編集アイコン（）をクリックします。

ステップ 5 [ダイナミック ルーティング（Dynamic Routing）] をクリックして、ダイナミック ルーティングのオプションを表示します。

ステップ 6 [RIP] をクリックして、RIP オプションを表示します。

ステップ 7 [認証（Authentication）] で、[プロファイル（Profile）] ドロップダウン リストから既存の仮想ルータの認証プロファイルを選択するか、[なし（None）] を選択します。

ステップ 8 **[保存（Save）]** をクリックします。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

高度な RIP の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	Control	7000 & 8000 シリーズ	リーフのみ	Admin/Network Admin

プロトコルの動作に影響するさまざまなタイムアウト値およびその他の機能に関していくつかの高度な RIP 設定を構成できます。

注意 不正な値に対する高度な RIP 設定を変更すると、ルータが他の RIP ルータと正常に通信することを妨げる場合があります。

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 変更するデバイスの横にある編集アイコン（）をクリックします。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [仮想ルータ（Virtual Routers）] タブをクリックします。

ステップ 4 変更する仮想ルータの横にある編集アイコン（）をクリックします。

ステップ 5 [ダイナミック ルーティング（Dynamic Routing）] をクリックして、ダイナミック ルーティングのオプションを表示します。

ステップ 6 [RIP] をクリックして、RIP オプションを表示します。

ステップ 7 [優先順位（Preference）] フィールドに、ルーティング プロトコルの優先度の数値（高いほど優先される）を入力します。システムはスタティック ルートよりも RIP を使用して学習したルートを優先します。

ステップ 8 [期間（Period）] フィールドに、定期的な更新間隔（秒単位）を入力します。低い数値は高速なコンバージェンスを示しますが、ネットワーク負荷が大きくなります。

ステップ 9 [タイムアウト時間（Timeout Time）] フィールドに、到達不能とみなされるまでのルートの存続時間（秒単位）を指定する数値を入力します。

ステップ 10 [ガベージ時間（Garbage Time）] フィールドに、破棄されるまでのルートの存続時間（秒単位）を指定する数値を入力します。

ステップ 11 [無限（Infinity）] フィールドに、コンバージェンスの計算で無限間隔の値を指定する数値を入力します。値が大きいほど、プロトコル コンバージェンスが遅くなります。

ステップ 12 [実行（Honor）] ドロップダウン リストから、ルーティング テーブルをダンプする要求がいつ実行されるかを指定する、次のいずれかのオプションを選択します。

- [常時（Always）]：常に要求を実行する
- [Neighbor]：直接接続されたネットワーク上のホストから送信された要求のみを実行する
- [Never]：要求を実行しない

ステップ 13 **[保存（Save）]** をクリックします。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

RIP 設定へのインポート フィルタの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	Control	7000 & 8000 シリーズ	リーフのみ	Admin/Network Admin

ルート テーブルに対して RIP からの受け入れまたは拒否を行うルートを指定するために、インポート フィルタを追加できます。インポート フィルタはテーブルに表示される順に適用されます。

インポート フィルタを追加するときは、仮想ルータに設定したフィルタの 1 つを使用します。

ヒント

RIP インポート フィルタを編集するには、編集アイコン（）をクリックします。RIP インポート フィルタを削除するには、削除アイコン（）をクリックします。

始める前に

- 仮想ルータの追加 （1592 ページ） の説明に従い、仮想ルータを追加します。
- 仮想ルータのフィルタの設定 （1614 ページ） の説明に従い、仮想ルータにフィルタを設定します。

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 変更するデバイスの横にある編集アイコン（）をクリックします。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [仮想ルータ（Virtual Routers）] タブをクリックします。

ステップ 4 RIP 仮想ルータ フィルタを追加する仮想ルータの横にある編集アイコン（）をクリックします。

ステップ 5 [ダイナミック ルーティング（Dynamic Routing）] をクリックして、ダイナミック ルーティングのオプションを表示します。

ステップ 6 [RIP] をクリックして、RIP オプションを表示します。

ステップ 7 [インポート フィルタ（Import Filters）] の下で、追加アイコン（）をクリックします。

ステップ 8 [名前（Name）] ドロップダウン リストから、インポート フィルタとして追加するフィルタを選択します。

ステップ 9 [アクション（Action）] の横にある [承認（Accept）] または [拒否（Reject）] を選択します。

ステップ 10 [OK] をクリックします。

ヒント インポート フィルタの順序を変更するには、必要に応じて、上へ移動するアイコン（）または下へ移動するアイコン（）をクリックします。リスト内でフィルタを上下にドラッグすることもできます。

ステップ 11 **[保存（Save）]** をクリックします。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

RIP 設定へのエクスポート フィルタの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	Control	7000 & 8000 シリーズ	リーフのみ	Admin/Network Admin

ルート テーブルから RIP に対しての受け入れまたは拒否を行うルートを定義するために、エクスポート フィルタを追加できます。エクスポート フィルタはテーブルに表示される順に適用されます。

エクスポート フィルタを追加するときは、仮想ルータに設定したフィルタの 1 つを使用します。

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 変更するデバイスの横にある編集アイコン（）をクリックします。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [仮想ルータ（Virtual Routers）] タブをクリックします。

ステップ 4 RIP 仮想ルータ フィルタを追加する仮想ルータの横にある編集アイコン（）をクリックします。

ステップ 5 [ダイナミック ルーティング（Dynamic Routing）] をクリックして、ダイナミック ルーティングのオプションを表示します。

ステップ 6 [RIP] をクリックして、RIP オプションを表示します。

ステップ 7 [エクスポート フィルタ（Export Filters）] の下で、追加アイコン（）をクリックします。

ステップ 8 [名前（Name）] ドロップダウン リストから、エクスポート フィルタとして追加するフィルタを選択します。

ステップ 9 [アクション（Action）] の横にある [承認（Accept）] または [拒否（Reject）] を選択します。

ステップ 10 [OK] をクリックします。

ヒント エクスポート フィルタの順序を変更するには、必要に応じて、上へ移動するアイコン（）または下へ移動するアイコン（）をクリックします。リスト内でフィルタを上下にドラッグすることもできます。

ステップ 11 **[保存（Save）]** をクリックします。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

OSPF の設定

Open Shortest Path First（OSPF）は、他のルータから情報を取得し、リンク ステート アドバタイズメントを使用してルートを他のルータにアドバタイズすることで、ルートを動的に定義する適応型ルーティング プロトコルです。ルータは、それ自体と宛先との間のリンクに関する情報を維持し、ルーティングを決定します。OSPF は、各ルーテッド インターフェイスにコストを割り当て、コストが最低のルータを最適であるとみなします。

OSPF ルーティング エリア

OSPF ネットワークは、管理を簡略化し、トラフィックおよびリソースの使用を最適化するために、ルーティング エリアに構造化つまり分割することができます。エリアは、単純な 10 進数またはよく使用されるオクテットベースのドット付き 10 進数表記のいずれかで表現される 32 ビットの数字により識別されます。

慣習により、エリア ゼロつまり 0.0.0.0 は OSPF ネットワークのコアまたはバックボーン エリアを表します。他のエリアも指定できます。多くの場合、管理者はエリアのメイン ルータの IP アドレスをエリア ID として選択します。追加の各エリアはバックボーンの OSPF エリアに直接または仮想接続できる必要があります。そうした接続は、エリア境界ルータ（ABR）と呼ばれる相互接続ルータによって保持されます。ABR は、管轄する各エリアの個々のリンクステートデータベースを管理し、ネットワーク内のすべてのエリアの集約ルートを保守します。

OSPF エリアの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	Control	7000 & 8000 シリーズ	リーフのみ	Admin/Network Admin

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 変更するデバイスの横にある編集アイコン（）をクリックします。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [仮想ルータ（Virtual Routers）] タブをクリックします。

ステップ 4 変更する仮想ルータの横にある編集アイコン（）をクリックします。

ステップ 5 [ダイナミック ルーティング（Dynamic Routing）] をクリックして、ダイナミック ルーティングのオプションを表示します。

ステップ 6 [OSPF（OSPF）] をクリックして、OSPF オプションを表示します。

ステップ 7 [エリア（Areas）] の下で、追加アイコン（）をクリックします。

ステップ 8 [エリア ID（Area Id）] フィールドに、エリアを表す数値を入力します。この値には整数または IPv4 アドレスを指定できます。

ステップ 9 オプションで、[スタブネット（Stubnet）] チェックボックスをオンにし、エリアが自律システムの外部のルータ アドバタイズメントを受信せず、エリア内のルーティングは完全にデフォルト ルートに基づくことを指定します。チェックボックスをオフにすると、このエリアはバックボーン エリアになります。それ以外の場合は、非スタブ エリアになります。

ステップ 10 [デフォルト コスト（Default cost）] フィールドに、エリアのデフォルト ルートに関連付けられたコストを入力します。

ステップ 11 [スタブネット（Stubnets）] の下で、追加アイコン（）をクリックします。

ステップ 12 [IP アドレス（IP Address）] フィールドに、IP アドレスを CIDR 表記で入力します。

ステップ 13 [非表示（Hidden）] チェックボックスを選択して、スタブネットが非表示であることを示します。

非表示のスタブネットは別のエリアに伝播されません。

ステップ 14 [サマリ（Summary）]チェックボックスを選択して、このスタブネットのサブネットワークであるデフォルトのスタブネットが非表示となるように指定します。

ステップ 15 [スタブ コスト（Stub cost）] フィールドに、このスタブ ネットワークへのルーティングに関連付けられたコストを定義する値を入力します。

ステップ 16 [OK] をクリックします。

ステップ 17 ネットワークを追加するには[ネットワーク（Networks）]の下の追加アイコン（  ）をクリックします。

ステップ 18 [IP アドレス（IP Address）] フィールドに、ネットワークの IP アドレスを CIDR 表記で入力します。

ステップ 19 [非表示（Hidden）] チェックボックスをオンにして、ネットワークが非表示であることを示します。非表示のネットワークは別のエリアに伝播されません。

ステップ 20 [OK] をクリックします。

ステップ 21 [保存（Save）] をクリックします。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

OSPF エリア インターフェイス

OSPF 用に仮想ルータに割り当てられたインターフェイスのサブセットを設定できます。次のリストに、各インターフェイスで指定できるオプションを示します。

Interfaces

OSPF を設定するインターフェイスを選択します。[Interfaces] タブから無効にしたインターフェイスは使用できません。

Type

次のオプションから、OSPF インターフェイスのタイプを選択します。

- Broadcast：ブロードキャスト ネットワークでは、フラッディングおよび hello メッセージはマルチキャストを使用し、すべてのネイバーに対して 1 つのパケットで送信されます。このオプションは、ルータがリンク ステート データベースと同期し、ネットワーク リンク ステート アドバタイズメントを発信するように指定します。このネットワーク タイプは、物理的なノンブロードキャスト マルチプル アクセス（NBMP）ネットワークと適切な IP プレフィクスなしのアンナンバード ネットワークには使用できません。
- Point-to-Point (PtP)：ポイントツーポイント ネットワークでは、2 台のルータのみを接続します。選定は実行されず、ネットワーク リンク ステート アドバタイズメントは発生しないので、より単純かつ高速に確立されます。このネットワーク タイプは物理的な PtP イン

ターフェイスだけでなく、PtP リンクとして使用されるブロードキャスト ネットワークにも役立ちます。このネットワーク タイプは物理的な NBMP ネットワークでは使用できません。

- Non-Broadcast：NBMP ネットワークで、パケットはマルチキャスト機能がないために各ネイバーに別々に送信されます。ブロードキャスト ネットワークと同様に、このオプションはリンク ステート アドバタイズメント伝播で中心的な役割を果たすルータを指定します。このネットワーク タイプはアンナンバード ネットワークでは使用できません。
- Autodetect：システムは指定されたインターフェイスに基づいて正しいタイプを判別します。

Cost

インターフェイスの出力コストを指定します。

Stub

インターフェイスが OSPF トラフィックをリッスンし、独自のトラフィックを送信する必要があるかどうかを指定します。

Priority

指定ルータの選定に使用される優先度を示す数値を入力します。多重アクセス ネットワークごとに、システムはルータおよびバックアップ ルータを指定します。これらのルータには、フラッディング プロセスでの特別な機能があります。優先度を高くすると、この選定での優先順位が上がります。優先度 0 でルータを設定することはできません。

Nonbroadcast

hello パケットが任意の未定義のネイバーに送信されるかどうかを指定します。このスイッチは、任意の NBMA ネットワークでは無視されます。

Authentication

仮想ルータに設定した認証プロファイルの 1 つからこのインターフェイスが使用する OSPF 認証プロファイルを選択するか、または [None] を選択します。認証プロファイルの設定に関する詳細については、仮想ルータ認証プロファイルの追加（1615ページ）を参照してください。

Hello Interval

hello メッセージの送信間隔（秒単位）を入力します。

Poll

NBMA ネットワーク上の一部のネイバーに対する hello メッセージの送信間隔（秒単位）を入力します。

Retrans Interval

確認応答されていないアップデートの再送信間隔（秒単位）を入力します。

Retrans Delay

インターフェイス経由でのリンクステート アップデート パケットの送信に要する推定秒数を入力します。

Wait Time

ルータが選定の開始と隣接関係の構築の間で待機する秒数を入力します。

Dead Interval

ルータがネイバーからのメッセージを受信しない場合に、ネイバーの停止を宣言するまで待機する秒数を入力します。この値が定義されている場合、deadカウントから計算された値はオーバーライドされます。

Dead Count

hello間隔と乗算されるときに、ルータがネイバーからのメッセージを受信しない場合に、ネイバーの停止を宣言するまで待機する秒数を指定する、数値を入力します。

OSPFエリアインターフェイスを編集するには、編集アイコン（）をクリックします。OSPF エリア インターフェイスを削除するには、削除アイコン（  ）をクリックします。[インターフェイス（Interfaces）] タブで設定されたインターフェイスを無効にすると削除されます。

OSPF エリア インターフェイスの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	Control	7000 & 8000 シリーズについて	リーフのみ	Admin/Network Admin

OSPF 用に仮想ルータに割り当てられたインターフェイスのサブセットを設定できます。

OSPF エリアで使用するインターフェイスは 1 つのみ選択できます。

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 OSPF インターフェイスを追加するデバイスの横にある編集アイコン（  ）をクリックします。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [仮想ルータ（Virtual Routers）] タブをクリックします。

ステップ 4 OSPF インターフェイスを追加する仮想ルータの横にある編集アイコン（  ）をクリックします。

ステップ 5 [ダイナミック ルーティング（Dynamic Routing）] をクリックして、ダイナミック ルーティングのオプションを表示します。

ステップ 6 [OSPF（OSPF）] をクリックして、OSPF オプションを表示します。

ステップ 7 [エリア（Areas）] の下で、追加アイコン（）をクリックします。

ステップ 8 [インターフェイス（Interfaces）] をクリックします。

ステップ 9 追加アイコン（）をクリックします。

ステップ 10 OSPF エリア インターフェイス （1605 ページ）で説明されているアクションのいずれかを実行します。

ステップ 11 ネットワークを追加するには[ネットワーク（Networks）]の下の追加アイコン（）をクリックします。

ステップ 12 [IP アドレス（IP address）] フィールドに、このインターフェイスから非ブロードキャスト ネットワークの hello メッセージを受信するネイバーの IP アドレスを入力します。

ステップ 13 [資格あり（Eligible）] チェックボックスをオンにして、ネイバーがメッセージを受け取る資格があることを示します。

ステップ 14 [OK] をクリックします。

ヒント ネイバーを編集するには、編集アイコン（）をクリックします。ネイバーを削除するには、削除アイコン（）をクリックします。

ステップ 15 [OK] をクリックします。

ステップ 16 [保存（Save）] をクリックします。

ステップ 17 **[保存（Save）]** をクリックします。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

OSPF エリア vlink の追加

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	Control	7000 & 8000 シリーズ	リーフのみ	Admin/Network Admin

OSPF 自律システムのすべてのエリアは、物理的にバックボーン エリアと接続されている必要があります。この物理接続が不可能である場合は、vlink を使用して、非バックボーン エリアを経由してバックボーンに接続できます。また vlink を使用して、非バックボーン エリアを経由し、分割されたバックボーンの 2 つの部分を接続することもできます。

vlink を追加するには、最低 2 つの OSPF エリアを追加しておく必要があります。

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 変更するデバイスの横にある編集アイコン（）をクリックします。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [仮想ルータ（Virtual Routers）] タブをクリックします。

ステップ 4 変更する仮想ルータの横にある編集アイコン（  ）をクリックします。

ステップ 5 [ダイナミック ルーティング（Dynamic Routing）] をクリックして、ダイナミック ルーティングのオプションを表示します。

ステップ 6 [OSPF（OSPF）] をクリックして、OSPF オプションを表示します。

ステップ 7 [エリア（Areas）] の下で、追加アイコン（  ）をクリックします。

ステップ 8 [Vlinks] をクリックします。

ステップ 9 追加アイコン（  ）をクリックします。

ステップ 10 [ルータ ID（Router ID）] フィールドに、ルータの IP アドレスを入力します。

ステップ 11 [認証（Authentication）] ドロップダウン リストから、vlink が使用する認証プロファイルを選択します。

ステップ 12 [Hello インターバル（Hello Interval）] フィールドに、hello メッセージの送信間隔（秒単位）を入力します。

ステップ 13 [再送信間隔（Retrans Interval）] フィールドに、確認応答されていないアップデートの再送信間隔（秒単位）を入力します。

ステップ 14 [待機時間（Wait Time）] フィールドに、ルータが選定の開始と隣接関係の構築の間で待機する秒数を入力します。

ステップ 15 [Dead 間隔（Dead Interval）] フィールドに、ルータがネイバーからのメッセージを受信しない場合に、ネイバーの停止を宣言するまで待機する秒数を入力します。この値が定義されている場合、dead カウントから計算された値はオーバーライドされます。

ステップ 16 [Dead 回数（Dead Count）] フィールドに、hello 間隔と乗算されるときに、ルータがネイバーからのメッセージを受信しない場合に、ネイバーの停止を宣言するまで待機する秒数を指定する、数値を入力します。

ステップ 17 [OK] をクリックします。

ステップ 18 [保存（Save）] をクリックします。

ステップ 19 **[保存（Save）]** をクリックします。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

OSPF 設定へのインポート フィルタの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	Control	7000 & 8000 シリーズ	リーフのみ	Admin/Network Admin

ルートテーブルに対してOSPFからの受け入れまたは拒否を行うルートを定義するために、インポート フィルタを追加できます。インポート フィルタはテーブルに表示される順に適用されます。

インポートフィルタを追加するときは、仮想ルータに設定したフィルタの1つを使用します。

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 変更するデバイスの横にある編集アイコン（）をクリックします。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [仮想ルータ（Virtual Routers）] をクリックします。

ステップ 4 変更する仮想ルータの横にある編集アイコン（）をクリックします。

ステップ 5 [ダイナミック ルーティング（Dynamic Routing）] をクリックして、ダイナミック ルーティングのオプションを表示します。

ステップ 6 [OSPF（OSPF）] をクリックして、OSPF オプションを表示します。

ステップ 7 [インポート フィルタ（Import Filters）] の下で、追加アイコン（）をクリックします。

ステップ 8 [名前（Name）] ドロップダウン リストから、インポート フィルタとして追加するフィルタを選択します。

ステップ 9 [アクション（Action）] の横にある [承認（Accept）] または [拒否（Reject）] を選択します。

ステップ 10 [OK] をクリックします。

ヒント インポート フィルタの順序を変更するには、必要に応じて、上へ移動するアイコン（）または下へ移動するアイコン（）をクリックします。リスト内でフィルタを上下にドラッグすることもできます。

ステップ 11 **[保存（Save）]** をクリックします。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

OSPF 設定へのエクスポート フィルタの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	Control	7000 & 8000 シリーズ	リーフのみ	Admin/Network Admin

ルート テーブルから OSPF に対しての受け入れまたは拒否を行うルートを定義するために、エクスポート フィルタを追加できます。エクスポート フィルタはテーブルに表示される順に適用されます。

エクスポート フィルタを追加するときは、仮想ルータに設定したフィルタの 1 つを使用します。

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 変更するデバイスの横にある編集アイコン（）をクリックします。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [仮想ルータ（Virtual Routers）] タブをクリックします。

ステップ 4 OSPF 仮想ルータ フィルタを追加する仮想ルータの横にある編集アイコン（）をクリックします。

ステップ 5 [ダイナミック ルーティング（Dynamic Routing）] タブをクリックして、ダイナミック ルーティングのオプションを表示します。

ステップ 6 [OSPF] をクリックして、OSPF オプションを表示します。

ステップ 7 [エクスポート フィルタ（Export Filters）] の下で、追加アイコン（）をクリックします。

ステップ 8 [名前（Name）] ドロップダウン リストから、エクスポート フィルタとして追加するフィルタを選択します。

ステップ 9 [アクション（Action）] の横にある [承認（Accept）] または [拒否（Reject）] を選択します。

ステップ 10 [OK] をクリックします。

ヒント エクスポート フィルタの順序を変更するには、必要に応じて、上へ移動するアイコン（）または下へ移動するアイコン（）をクリックします。リスト内でフィルタを上下にドラッグすることもできます。

ステップ 11 **[保存（Save）]** をクリックします。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

仮想ルータのフィルタ

フィルタは、仮想ルータのルート テーブルへのインポートおよびルートのダイナミック プロトコルへのエクスポートを行うために、ルートを照合する方法を提供します。フィルタのリストを作成および管理できます。各フィルタは特定の基準を定義し、静的に定義されるか、またはダイナミック プロトコルから受信したルートを検索します。

仮想ルータ フィルタ テーブルには、仮想ルータに設定した各フィルタのサマリ情報が表示されます（次の表を参照してください）。

表 *106 :* 仮想ルータ フィルタ テーブル ビューのフィールド

フィールド	説明
Name	フィルタの名前。
Protocol	ルートが発生するプロトコル。 • [Static]：ルートはローカル スタティック ルートとして発生します。 • [RIP]：ルートはダイナミックな RIP 設定から発生します。 • [OSPF]：ルートはダイナミックな OSPF 設定から発生します。
From Router	このフィルタがルートで一致を試みるルータの IP アドレス。スタティック フィルタおよび RIP フィルタに対してこの値を入力する必要があります。
Next Hop	このルートを使用するパケットが転送されるネクストホップ。スタティック フィルタおよび RIP フィルタに対してこの値を入力する必要があります。
Destination Type	パケットが送信される宛先のタイプ。 • ルータ • デバイス • 廃棄
Destination Network	このフィルタがルートで一致を試みるネットワーク。

フィールド	説明
OSPF Path Type	OSPF プロトコルにのみ適用されます。パスタイプは次のいずれかです。 • Ext-1 • Ext-2 • Inter Area • Intra Area
OSPF Router ID	OSPFプロトコルにのみ適用されます。ルート/ネットワークをアドバタイズするルータのルータ ID。

仮想ルータ フィルタの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	Control	7000 & 8000 シリーズ	任意（Any）	Admin/Network Admin

仮想ルータ エディタの [フィルタ（Filter）] タブには、仮想ルータに設定したすべてのフィルタを含むテーブルが表示されます。テーブルには、各フィルタに関するサマリー情報が含まれています。

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 表示するデバイスの横にある編集アイコン（）をクリックします。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [仮想ルータ（Virtual Routers）] タブをクリックします。

ステップ 4 フィルタを表示する仮想ルータの横にある編集アイコン（）をクリックします。

ステップ 5 [フィルタ（Filter）] タブをクリックします。

仮想ルータのフィルタの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	Control	7000 & 8000 シリーズ	リーフのみ	Admin/Network Admin

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 変更するデバイスの横にある編集アイコン（  ）をクリックします。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [仮想ルータ（Virtual Routers）] タブをクリックします。

ステップ 4 変更する仮想ルータの横にある編集アイコン（  ）をクリックします。

ステップ 5 [フィルタ処理（Filter）] タブをクリックします。

ステップ 6 [フィルタの追加（Add Filter）] をクリックします。

ステップ 7 [名前（Name）] フィールドにフィルタの名前を入力します。英数字のみを使用できます。

ステップ 8 [プロトコル（Protocol）] で、[すべて（All）] を選択するか、フィルタに適用するプロトコルを選択します。

ステップ 9 [プロトコル（Protocol）] として [すべて（All）]、[スタティック（Static）]、または [RIP] を選択した場合は、[ルータから（From Router）] で、このフィルタがルートで一致を試みるルータ IP アドレスを入力します。

（注） IPv4 アドレスに対する /32 の CIDR ブロックと IPv6 アドレスに対する /128 のプレフィクス長も入力可能です。他のすべてのアドレス ブロックは、このフィールドでは無効です。

ステップ 10 [追加（Add）] をクリックします。

ステップ 11 [プロトコル（Protocol）] として [すべて（All）]、[スタティック（Static）]、または [RIP（RIP）] を選択した場合は、[ネクスト ホップ（Next Hop）] で、このフィルタがルートで一致を試みるゲートウェイの IP アドレスを入力します。

（注） IPv4 アドレスに対する /32 の CIDR ブロックと IPv6 アドレスに対する /128 のプレフィクス長も入力可能です。他のすべてのアドレス ブロックは、このフィールドでは無効です。

ステップ 12 [追加（Add）] をクリックします。

ステップ 13 [送信先のタイプ（Destination Type）] で、フィルタに適用するオプションを選択します。

ステップ 14 [宛先ネットワーク（Destination Network）] で、このフィルタがルートで一致を試みるネットワークの IP アドレスを入力します。

ステップ 15 [追加（Add）] をクリックします。

ステップ 16 [プロトコル（Protocol）] として [すべて（All）] または [OSPF] を選択した場合は、[パスのタイプ（Path Type）] で、フィルタに適用するオプションを選択します。少なくとも 1 つのパス タイプを選択する必要があります。

ステップ 17 [プロトコル（Protocol）] として [OSPF] を選択した場合は、[ルータ ID（Router ID）] で、ルート/ネットワークをアドバタイズするルータのルータ ID の役割を持つ IP アドレスを入力します。

ステップ 18 [追加（Add）] をクリックします。

ステップ 19 [OK] をクリックします。

ステップ 20 [保存（Save）] をクリックします。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

仮想ルータ認証プロファイルの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	Control	7000 & 8000 シリーズ	リーフのみ	Admin/Network Admin

RIP および OSPF の設定で使用する認証プロファイルをセットアップできます。簡易パスワードを設定するか、共有暗号キーを指定できます。簡易パスワードでは、すべてのパケットが 8 バイトのパスワードを伝送できます。システムはこのパスワードが欠如している受信パケットを無視します。暗号キーでは検証が可能で、パスワードから生成される 16 バイト長のダイジェストがすべてのパケットに付加されます。

OSPF の場合、各エリアは異なる認証方式を使用できることに注意してください。そのため、多くのエリア間で共有できる認証プロファイルを作成します。OSPFv3 の認証は追加できません。

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 変更するデバイスの横にある編集アイコン（）をクリックします。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [仮想ルータ（Virtual Routers）] タブをクリックします。

ステップ 4 変更する仮想ルータの横にある編集アイコン（）をクリックします。

ステップ 5 [認証プロファイル（Authentication Profile）] をクリックします。

ステップ 6 [認証プロファイルの追加（Add Authentication Profile）] をクリックします。

ステップ 7 [認証プロファイル名（Authentication Profile Name）] フィールドに、認証プロファイルの名前を入力します。

ステップ 8 [認証タイプ（Authentication Type）] ドロップダウン リストから、[単純（simple）] または [暗号化（cryptographic）] を選択します。

ステップ 9 [パスワード（Password）] フィールドに、安全なパスワードを入力します。

ステップ 10 確認のために [パスワードの確認（Confirm Password）] フィールドにもう一度パスワードを入力します。

ステップ 11 [OK] をクリックします。

ステップ 12 [保存（Save）] をクリックします。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

仮想ルータ統計情報の表示

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	Control	7000 & 8000 シリーズ	任意（Any）	Admin/Network Admin

各仮想ルータの実行時統計情報を表示できます。統計情報にはユニキャスト パケット、ドロップされたパケット、IPv4 および IPv6 アドレスの個別のルーティング テーブルが表示されます。

ステップ 1 **[Devices]** > **[Device Management]** を選択します。

ステップ 2 統計情報を表示するデバイスの横にある編集アイコン（  ）をクリックします。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [仮想ルータ（Virtual Routers）] タブをクリックします。

ステップ 4 ルータ統計情報を表示する仮想ルータの横にある表示アイコン（  ）をクリックします。

仮想ルータの削除

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	Control	7000 & 8000 シリーズ	リーフのみ	Admin/Network Admin

仮想ルータを削除すると、ルータに割り当てられているすべてのルーテッドインターフェイスを他のルータに含めることができるようになります。

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 変更するデバイスの横にある編集アイコン（  ）をクリックします。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

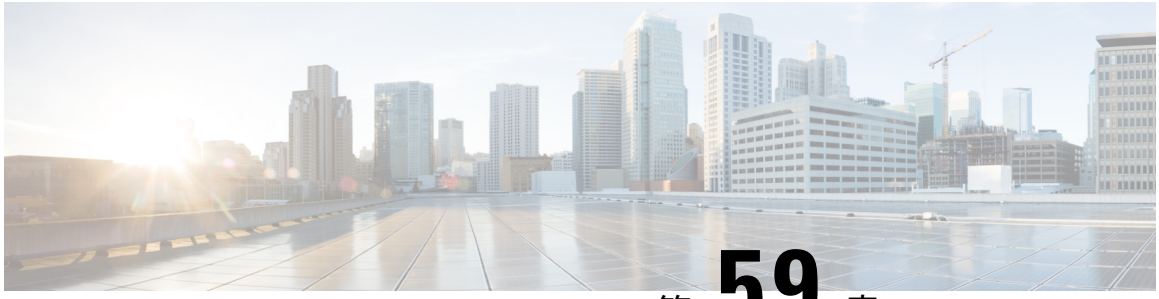
ステップ 3 [仮想ルータ（Virtual Routers）] タブをクリックします。

ステップ 4 削除する仮想ルータの横にある削除アイコン（  ）をクリックします。

ステップ 5 入力を求められた場合、仮想ルータを削除することを確認します。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。



第 59 章

集約インターフェイスと LACP

以下のトピックでは、集約インターフェイスの設定について、および管理対象デバイスでLACPがどのように機能するかについて説明します。

集約インターフェイスについて

Firepower システムでは、管理対象デバイスがレイヤ 2（ネットワーク間でパケット スイッチングを行う）、またはレイヤ 3（インターフェイス間でトラフィックをルーティングする）に展開されている場合、複数の物理イーサネットインターフェイスを管理対象デバイス上で1つの論理リンクにグループ化できます。このように1つに集約された論理リンクは、帯域幅と冗長性の向上および、2 つのエンドポイント間でのロードバランシングを実現します。

集約リンクを作成するには、スイッチドまたはルーテッド リンク集約グループ（LAG）を作成します。集約グループを作成すると、集約インターフェイスと呼ばれる論理インターフェイスが作成されます。上位層エンティティである LAG は単一の論理リンクに似ており、データトラフィックは集約インターフェイスを介して送信されます。集約リンクは、複数のリンクの帯域幅をまとめて追加することによって帯域幅を増加させます。また、使用可能なすべてのリンクのトラフィックをロードバランシングすることで、冗長性を実現します。リンクの1つで障害が発生すると、トラフィックは残りのリンク全体にロードバランシングされます。

LAG のエンドポイントは、7000 または 8000 シリーズ デバイス（上記の図を参照）が 2 つの場合もあれば、一方がサードパーティ アクセス スイッチまたはルータに接続されている 7000

または 8000 シリーズ デバイスの場合もあります。2 つのデバイスは一致している必要はありませんが、同じ物理構成で、IEEE 802.ad リンク アグリゲーション標準規格をサポートしている必要があります。LAG の通常の展開では、2 つの管理対象デバイス間のアクセス リンクを集約するか、管理対象デバイスとアクセス スイッチまたはルータ間にポイントツーポイント接続を確立します。

NGIPSv デバイスや ASA FirePOWER モジュールでは集約インターフェイスを設定することはできません。

LAG 設定

集約インターフェイスには次の 2 種類があります。

- スイッチド：レイヤ 2 集約インターフェイス
- ルーテッド：レイヤ 3 集約インターフェイス

リンク集約は、リンク集約グループ（LAG）を使用して実装します。LAG を設定するには、集約スイッチドまたはルーテッドインターフェイスを作成して、一連の物理インターフェイスをリンクに関連付けます。すべての物理インターフェイスは同じ速度とメディアでなければなりません。

集約リンクは動的または静的に作成します。動的リンク集約では、IEEE 802.ad リンク集約標準のコンポーネットである Link Aggregation Control Protocol（LACP）が使用されますが、静的リンク集約では使用されません。LACP は、LAG の両端の各デバイスでリンクおよびシステムの情報を交換できるようにして、集約でアクティブに使用するリンクを決定します。静的LAG 構成では、手動でリンク集約を維持し、ロード バランシング ポリシーとリンク選択ポリシーを展開する必要があります。

スイッチドまたはルーテッド集約インターフェイスを作成すると、同じタイプのリンク集約グループが自動的に作成され、それに番号が付けられます。たとえば、最初の LAG（スイッチドまたはルーテッド）を作成すると、その集約インターフェイスは、管理対象デバイスの [インターフェイス（Interfaces）] タブの **lag0** ラベルによって識別できます。物理インターフェイスと論理インターフェイスをこの LAG に関連付けると、それらは階層ツリー メニューのプライマリ LAG の下にネスト表示されます。ただし、スイッチド LAG にはスイッチド物理インターフェイスのみを含めることができ、ルーテッド LAG にはルーテッド物理インターフェイスのみを含めることができます。

LAG を設定する際は、以下の要件を考慮してください。

- Firepower システムは、最大 14 の LAG をサポートし、各 LAG インターフェイスに 0 ～ 13 の一意の ID を割り当てます。LAG ID は設定できません。
- リンクの両側に LAG を設定し、どちらの側のインターフェイスも同じ速度に設定する必要があります。
- 各 LAG ごとに少なくとも 2 つの物理インターフェイスを関連付ける必要があります（最大 8 つ）。物理インターフェイスは複数の LAG に属することはできません。

- LAG の物理インターフェイスは、他の動作モードでインラインまたはパッシブとして使用できず、タグ付きトラフィックの別の論理インターフェイスの一部として使用することもできません。
- LAG の物理インターフェイスは複数の NetMods にまたがることが可能ですが、複数のセンサーにまたがることはできません（すべての物理インターフェイスが同じデバイス上に存在する必要があります）。
- LAG にはスタック構成の NetMod を含めることができません。

スイッチド インターフェイスの集約

管理対象デバイスの 2 ～ 8 つの物理ポートを組み合わせて、スイッチド LAG インターフェイスを作成できます。トラフィックを処理できるようにするには、その前に、スイッチド LAG インターフェイスを仮想スイッチに割り当てる必要があります。管理対象デバイスは、最大 14 の LAG インターフェイスをサポートできます。

MTU 値の範囲は管理対象デバイスのモデルとインターフェイス タイプによって異なる場合があります。

注意 デバイス上のすべての非管理インターフェイスの中で最大 MTU 値を変更し、設定変更を展開すると、Snort プロセスが再起動され、トラフィック インスペクションが一時的に中断されます。インスペクションは、変更したインターフェイスだけでなく、すべての非管理インターフェイスで中断されます。この中断によってトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびインターフェイスのタイプに応じて異なります。詳細については、「Snort® の再起動によるトラフィックの動作 （451 ページ）」を参照してください。

関連トピック

7000 および 8000 シリーズ デバイスおよび NGIPSv の MTU 範囲 （661 ページ）
Snort® の再起動シナリオ （450 ページ）

ルーテッド インターフェイスの集約

7000 または 8000 シリーズ デバイスの 2 ～ 8 つの物理ポートを組み合わせて、ルーテッド LAG インターフェイスを作成できます。トラフィックをルーティングする前に、ルーテッド LAG インターフェイスを仮想ルータに割り当てる必要があります。管理対象デバイスは、最大 14 の LAG インターフェイスをサポートできます。

ルーテッド LAG インターフェイスにスタティック Address Resolution Protocol（ARP）エントリを追加できます。外部ホストは、トラフィックの送信先となるローカル ネットワーク上の宛先 IP アドレスの MAC アドレスを知る必要がある場合は、ARP 要求を送信します。スタティック ARP エントリを設定する場合、仮想ルータは IP アドレスや関連付けられた MAC アドレスに応答します。

ルーテッド LAG インターフェイスの [ICMP 対応の応答数（ICMP Enable Responses）] オプションを無効にしても、すべてのシナリオで ICMP 応答が抑制されるわけではありません。引き続き、アクセス コントロール ルールを使用して、宛先 IP がルーテッド インターフェイスの IP であり、プロトコルが ICMP である接続を処理することができます。ポートおよび ICMP コードの条件 （477 ページ）を参照してください。

[ローカル ルータ トラフィックを検査する（Inspect Local Router Traffic）] オプションを有効にすると、パケットはホストに到達する前にドロップされるため、あらゆる応答が抑制されます。ローカル ルータ トラフィックの検査の詳細については、デバイスの詳細設定 （299 ページ）を参照してください。

MTU 値の範囲は管理対象デバイスのモデルとインターフェイス タイプによって異なる場合があります。

注意 デバイス上のすべての非管理インターフェイスの中で最大 MTU 値を変更し、設定変更を展開すると、Snort プロセスが再起動され、トラフィック インスペクションが一時的に中断されます。インスペクションは、変更したインターフェイスだけでなく、すべての非管理インターフェイスで中断されます。この中断によってトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびインターフェイスのタイプに応じて異なります。詳細については、「Snort® の再起動によるトラフィックの動作 （451 ページ）」を参照してください。

関連トピック

7000 および 8000 シリーズ デバイスおよび NGIPSv の MTU 範囲 （661 ページ）
Snort® の再起動シナリオ （450 ページ）

論理集約インターフェイス

各スイッチドまたはルーテッド集約インターフェイスごとに、複数の論理インターフェイスを追加できます。論理 LAG インターフェイスで受信した VLAN タグ付きトラフィックを処理するには、各論理 LAG インターフェイスをその特定のタグに関連付ける必要があります。物理スイッチドまたはルーテッドインターフェイスに追加するのと同じ方法で、論理インターフェイスをスイッチドまたはルーテッド集約インターフェイスに追加します。

（注） LAG インターフェイスを作成すると、デフォルトで「タグなし」論理インターフェイスが作成されます。このインターフェイスは **lag*n.0*** ラベルによって識別されます（***n*** は 0 ～ 13 の整数）。動作させるには、各 LAG にこの論理インターフェイスが少なくとも 1 つ必要です。LAG に追加の論理インターフェイスを関連付けて、VLAN タグ付きトラフィックを処理できます。追加する各論理インターフェイスには固有の VLAN タグが必要です。Firepower System は 1 ～ 4094 の VLAN タグをサポートします。

論理ルーテッド インターフェイスには、シスコ冗長プロトコル（SFRP）を設定することもできます。SFRP では、指定した IP アドレスに対する冗長なゲートウェイとしてデバイスを機能させることができます。

論理ルーテッド LAG インターフェイスの [ICMP 有効応答（ICMP Enable Responses）] オプションを無効にしても、すべてのシナリオで ICMP 応答が抑制されるわけではありません。宛先 IP がルーテッド インターフェイスの IP で、プロトコルが ICMP であるパケットをドロップするように、アクセス コントロール ポリシーにネットワークベースのルールを追加できます。

管理対象デバイスの詳細設定である [ローカル ルータ トラフィックの検閲（Inspect Local Router Traffic）] オプションを有効にした場合、パケットはホストに到達する前にドロップされるため、すべての応答を防ぐことができます。

MTU 値の範囲は管理対象デバイスのモデルとインターフェイス タイプによって異なる場合があります。

⚠

注意 デバイス上のすべての非管理インターフェイスの中で最大 MTU 値を変更し、設定変更を展開すると、Snort プロセスが再起動され、トラフィック インスペクションが一時的に中断されます。インスペクションは、変更したインターフェイスだけでなく、すべての非管理インターフェイスで中断されます。この中断によってトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびインターフェイスのタイプに応じて異なります。詳細については、「Snort® の再起動によるトラフィックの動作 （451 ページ）」を参照してください。

関連トピック

SFRP
デバイスの詳細設定 （299 ページ）
7000 および 8000 シリーズ デバイスおよび NGIPSv の MTU 範囲 （661 ページ）
Snort® の再起動シナリオ （450 ページ）

ロード バランシング アルゴリズム

LAG バンドルのメンバー リンクへのトラフィックの分散方法を決定する出口ロード バランシング アルゴリズムを LAG に割り当てます。ロード バランシング アルゴリズムは、レイヤ 2 MAC アドレス、レイヤ 3 IP アドレス、レイヤ 4 ポート番号（TCP/UDP トラフィック）など、さまざまなパケット フィールドの値に基づいてハッシュを決定します。選択したロード バランシング アルゴリズムは、LAG バンドルのメンバー リンクすべてに適用されます。

LAG を設定する場合は、次のオプションから展開シナリオに対応するロード バランシング アルゴリズムを選択します。

- 宛先 IP（Destination IP）
- Destination MAC
- Destination Port
- Source IP

- Source MAC
- Source Port
- Source and Destination IP
- Source and Destination MAC
- Source and Destination Port

（注） LAG の両端に同じロード バランシング アルゴリズムを設定する必要があります。必要に応じて、上位層のアルゴリズムが下位層のアルゴリズムにバックオフされます（例：ICMP トラフィックに対してレイヤ 3 にバックオフされるレイヤ 4 アルゴリズムなど）。

リンク セレクション ポリシー

リンク アグリゲーションでは、両方のエンドポイントで各リンクの速度とメディアが同じである必要があります。リンク プロパティを動的に変更できるので、リンク選択ポリシーは、システムによるリンク選択プロセスの管理方法を決定する上で役立ちます。最大ポート数を最大化するリンク選択ポリシーはリンク冗長性をサポートし、総帯域幅を最大化するリンク選択ポリシーを全体的なリンク速度をサポートします。安定したリンク選択ポリシーは、リンク状態の過剰な変更を最小限に抑えようとします。

（注） LAG の両端に同じリンク選択ポリシーを設定する必要があります。

次のオプションから展開シナリオに対応するリンク選択ポリシーを選択します。

- [最大ポート数（Highest Port Count）]：冗長性を向上させる最大アクティブ ポート数を割り当てるには、このオプションを選択します。
- [最大合計帯域幅（Highest Total Bandwidth）]：集約リンクに最大合計帯域幅を割り当てるには、このオプションを選択します。
- [安定（Stable）]：最大の課題がリンクの安定性と信頼性である場合は、このオプションを選択します。LAG を設定すると、アクティブ リンクは、ポート数や帯域幅が追加された場合ではなく、どうしても必要な場合（リンク障害などの場合）にのみ変更されます。
- [LACP 優先順位（LACP Priority）]：LAG でアクティブにするリンクを LACP アルゴリズムにより決定するには、このオプションを選択します。この設定は、展開目標が未定義の場合や、LAG の一端のデバイスが Firepower Management Center によって管理されていない場合に適しています。

LACPは、動的リンクアグリゲーションをサポートするリンク選択方式の自動化における主要部分です。LACP を有効にすると、LACP の優先度に基づいたリンク選択ポリシーは LACP の次のプロパティを使用します。

LACP システム プライオリティ

リンクアグリゲーションにおいて優位なデバイスを判断するには、LACPを実行している各パートナー デバイスにこの値を設定します。値が小さいシステムほど、システム プライオリティが高くなります。動的リンク集約では、最初に、LACP システム プライオリティの高いシステム側でメンバー リンクに選択された状態が設定され、次に、プライオリティの低いシステムでメンバー リンクが適宜設定されます。0 ～ 65535 を指定できます。値を指定しない場合、デフォルトの優先順位は 32768 になります。

LACP リンク優先順位。

集約グループに属する各リンクにこの値を設定します。リンク プライオリティによって、LAG におけるアクティブ リンクとスタンバイ リンクが決まります。値が小さいリンクほどプライオリティが高くなります。アクティブ リンクがダウンすると、最もプライオリティの高いスタンバイ リンクが選択され、ダウンしたリンクと交換されます。ただし、複数のリンクの LACP リンク プライオリティが同じである場合は、物理ポート番号が最も小さいリンクがスタンバイ リンクとして選択されます。0 ～ 65535 を指定できます。値を指定しない場合、デフォルトの優先順位は 32768 になります。

リンク集約制御プロトコル（LACP）

IEEE 802.3ad のコンポーネントであるリンク集約制御プロトコル（LACP）は、LAG バンドルを作成して維持するためにシステムおよびポートの情報を交換する 1 つの方式です。LACP を有効にすると、LAG の両端の各デバイスは LACP を使用して、集約においてアクティブに使用されているリンクを特定します。LACP は、リンク間で LACP パケット（または制御メッセージ）を交換することによって、アベイラビリティと冗長性を実現します。このプロトコルは、リンクの能力を動的に学習し、他のポートに通知します。LACP は、適合するリンクを特定すると、それらのリンクを LAG にグループ化します。あるリンクで障害が発生した場合、トラフィックは他のリンクで継続されます。リンクを機能させるには、LAG の両端で LACP を有効にする必要があります。

LACP

LACPを有効にする場合は、LAGの両端で転送モードを指定して、ペアになったデバイス間での LACP パケットの交換方法を指定する必要があります。LACP モードには次の 2 つのオプションがあります。

- [アクティブ（Active）] : デバイスをアクティブ ネゴシエーション ステートにするにはこのモードを選択します。このモードでは、デバイスはLACPパケットを送信することにより、リモート リンクとのネゴシエーションを開始します。

- [パッシブ（Passive）]：デバイスをパッシブ ネゴシエーション ステートにするにはこのモードを選択します。このモードでは、デバイスは受信したLACPパケットには応答しますが、LACP ネゴシエーションを開始しません。

（注） どちらのモードでも、LACP はリンク間でネゴシエートして、それらのリンクがポート速度などの基準に基づいてリンク バンドルを形成可能かどうかを判定できます。ただし、パッシブ対パッシブの構成は避けるようにしてください。そのような構成では、基本的に LAG の両端がリスニング モードになります。

LACPには、デバイス間でのLACPパケットの送信頻度を定義するタイマーがあります。LACPは次のレートでパケットを交換します。

- [Slow]：30 秒
- [Fast]：1 秒

このオプションが適用されたデバイスは、LAG の反対側のパートナー デバイスからこの頻度で LACP パケットを受信することを予期します。

（注） LAG がデバイス スタック内の管理対象デバイスに設定されている場合は、プライマリ デバイスだけがパートナー システムとのLACP通信に参加します。すべてのセカンダリ デバイスは、LACP メッセージをプライマリ デバイスに転送します。プライマリ デバイスは、動的な LAG の変更をセカンダリ デバイスにリレーします。

集約スイッチド インターフェイスの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	Control	7000 & 8000 シリーズ	リーフのみ	Admin/Network Admin

管理対象デバイスの 2 ～ 8 つの物理ポートを組み合わせて、スイッチド LAG インターフェイスを作成できます。トラフィックを処理できるようにするには、その前に、スイッチド LAG インターフェイスを仮想スイッチに割り当てる必要があります。管理対象デバイスは、最大14の LAG インターフェイスをサポートできます。

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 スイッチド LAG インターフェイスを設定するデバイスの横にある編集アイコン（）をクリックします。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [追加（Add）] ドロップダウン メニューから [集約インターフェイスの追加（Add Aggregate Interface）] を選択します。

ステップ 4 [スイッチド（Switched）] をクリックして、スイッチド LAG インターフェイスのオプションを表示します。

ステップ 5 セキュリティ ゾーンを適用するには、次のいずれかを実行します。

- [セキュリティ ゾーン（Security Zone）] ドロップダウン リストから既存のセキュリティ ゾーンを選択します。
- [新規（New）] を選択して新しいセキュリティ ゾーンを追加します。セキュリティ ゾーンおよびインターフェイス グループ オブジェクトの作成 （536 ページ） を参照してください。

ステップ 6 仮想スイッチを指定します。

- [仮想スイッチ（Virtual Switch）] ドロップダウン リストから既存の仮想スイッチを選択します。
- [新規（New）] を選択して新しい仮想スイッチを追加します。仮想スイッチの追加 （1576 ページ） を参照してください。

ステップ 7 [有効（Enabled）] チェックボックスをオンにして、スイッチド LAG インターフェイスがトラフィックを処理できるようにします。

このチェックボックスをオフにすると、インターフェイスは無効になり、ユーザはセキュリティ上の理由によりアクセスできなくなります。

ステップ 8 [モード（Mode）] からリンク モードを指定するオプションを選択するか、または [Autonegotiation] を選択して、速度とデュプレックス設定を自動的にネゴシエートするようインターフェイスを設定します。

モード設定は銅線インターフェイスにのみ使用できます。

8000 シリーズ アプライアンスのインターフェイスは、半二重オプションをサポートしません。リンクが自動的に速度をネゴシエートする場合は、同じ速度設定に基づいて LAG のすべてのアクティブ リンクが選択されます。

ステップ 9 [MDI/MDIX] ドロップダウン リストから、インターフェイスの設定対象として MDI（メディア依存型インターフェイス）、MDIX（メディア依存型インターフェイス クロスオーバー）、または Auto-MDIX のいずれかを指定するオプションを選択します。

[MDI/MDIX] 設定は銅線インターフェイスでのみ使用できます。

デフォルトでは、MDI/MDIX は自動 MDI に設定され、MDI と MDIX の間のスイッチングを自動的に処理してリンクを確立します。

ステップ 10 [MTU] フィールドに最大伝送ユニット（MTU）を入力します。

設定可能な MTU の範囲は、Firepower System のデバイス モデルおよびインターフェイスのタイプによって異なる場合があります。詳細については、7000 および 8000 シリーズ デバイスおよび NGIPSv の MTU 範囲 （661 ページ）を参照してください。

ステップ 11 [リンク アグリゲーション（Link Aggregation）] で、LAG バンドルに追加する物理インターフェイスを [使用できるインターフェイス（Available Interfaces）] から 1 つまたは複数選択します。

ヒント LAG バンドルから物理インターフェイスを削除するには、1 つ以上の物理インターフェイスを選択して、選択項目の削除アイコン（  ）をクリックします。LAG バンドルからすべての物理インターフェイスを削除するには、すべてを削除アイコン（  ）をクリックします。[インターフェイス（Interfaces）] タブから LAG インターフェイスを削除すると、そのインターフェイスも削除されます。

ステップ 12 [ロードバランシング アルゴリズム（Load-Balancing Algorithm）] ドロップダウン リストからオプションを選択します。

ステップ 13 ドロップダウンリストから [リンク選択ポリシー（Link Selection Policy）] を選択します。

ヒント Firepower System デバイスとサードパーティ製ネットワーク デバイスとの間に集約インターフェイスを設定する場合は、[LACP 優先（LACP Priority）] を選択します。

ステップ 14 [リンク選択ポリシー（Link Selection Policy）] に [LACP 優先（LACP Priority）] を選択した場合は、[システム優先度（System Priority）] に値を割り当て、[インターフェイスの優先度の設定（Configure Interface Priority）] リンクをクリックして優先度の値を LAG の各インターフェイスに割り当てます。

ステップ 15 [トンネルレベル（Tunnel Level）] ドロップダウン リストから [内部（Inner）] または [外部（Outer）] を選択します。

（注） レイヤ 3 ロード バランシングが設定されている場合、トンネル レベルは IPv4 トラフィックにのみ適用されます。外部トンネルは常に、レイヤ 2 と IPv6 トラフィックに使用されます。[トンネル レベル（Tunnel Level）] が明示的に設定されていない場合、デフォルトは [外部（Outer）] になります。

ステップ 16 [LACP] で [有効（Enabled）] チェックボックスをオンにして、スイッチド LAG インターフェイスがリンク集約制御プロトコルを使用してトラフィックを処理できるようにします。

このチェックボックスをオフにすると、LAG インターフェイスは静的設定になり、Firepower System は選択されたすべての物理インターフェイスを集約に使用します。

ステップ 17 [レート（Rate）] オプション ボタンをクリックし、パートナー デバイスから LACP 制御メッセージを受信する頻度を設定します。

- パケットを 30 秒ごとに受信するには、[遅い（Slow）] をクリックします。
- パケットを 1 秒ごとに受信するには、[速い（Fast）] をクリックします。

ステップ 18 [モード（Mode）] オプション ボタンをクリックし、デバイスのリスニング モードを設定します。

- パートナー デバイスに LACP パケットを送信してリモート リンクとのネゴシエーションを開始するには、[アクティブ（Active）] をクリックします。
- 受信した LACP パケットに応答するには、[パッシブ（Passive）] をクリックします。

ステップ 19 **[保存（Save）]** をクリックします。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

関連トピック

7000 および 8000 シリーズ デバイスおよび NGIPSv の MTU 範囲 （661 ページ）
Snort® の再起動シナリオ （450 ページ）

集約ルーテッド インターフェイスの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	Control	7000 & 8000 シリーズ	リーフのみ	Admin/Network Admin

管理対象デバイスの 2 ～ 8 つの物理ポートを組み合わせて、ルーテッド LAG インターフェイスを作成できます。トラフィックをルーティングする前に、ルーテッド LAG インターフェイスを仮想ルータに割り当てる必要があります。管理対象デバイスは、最大 14 の LAG インターフェイスをサポートできます。

注意 7000 または 8000 シリーズ デバイス 設定の変更を展開する際に Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、ターゲット デバイスがトラフィックを処理する方法に応じて異なります。詳細はSnort® の再起動によるトラフィックの動作 （451 ページ）を参照してください。 でのルーテッド インターフェイス ペアの追加

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 ルーテッド LAG インターフェイスを設定するデバイスの横にある編集アイコン（  ）をクリックします。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [追加（Add）] ドロップダウン メニューから [集約インターフェイスの追加（Add Aggregate Interface）] を選択します。

ステップ 4 [Routed] をクリックして、ルーテッド LAG インターフェイス オプションを表示します。

ステップ 5 セキュリティ ゾーンを適用するには、次のいずれかを実行します。

- [セキュリティ ゾーン（Security Zone）] ドロップダウン リストから既存のセキュリティ ゾーンを選択します。
- [新規（New）] を選択して新しいセキュリティ ゾーンを追加します。セキュリティ ゾーンおよびインターフェイス グループ オブジェクトの作成 （536 ページ） を参照してください。

ステップ 6 仮想ルータを指定します。

- [仮想ルータ（Virtual Router）] ドロップダウン リストから既存の仮想ルータを選択します。
- [新規（New）] を選択して新しい仮想ルータ 仮想ルータの追加 （1592 ページ）を追加します。

ステップ 7 [有効（Enabled）]チェックボックスをオンにして、ルーテッドLAGインターフェイスがトラフィックを処理できるようにします。

このチェックボックスをオフにすると、インターフェイスは無効になり、ユーザはセキュリティ上の理由によりアクセスできなくなります。

ステップ 8 [モード（Mode）] ドロップダウン リストからリンク モードを指定するオプションを選択するか、または [Autonegotiation] を選択して、速度とデュプレックス設定を自動的にネゴシエートするようLAGインターフェイスを設定します。

モード設定は銅線インターフェイスにのみ使用できます。

8000シリーズアプライアンスのインターフェイスは、半二重オプションをサポートしません。リンクが自動的に速度をネゴシエートする場合は、同じ速度設定に基づいて LAG のすべてのアクティブ リンクが選択されます。

ステップ 9 [MDI/MDIX] ドロップダウン リストから、インターフェイスの設定対象として MDI（メディア依存型インターフェイス）、MDIX（メディア依存型インターフェイス クロスオーバー）、または Auto-MDIX のいずれかを指定するオプションを選択します。

[MDI/MDIX] 設定は銅線インターフェイスでのみ使用できます。

デフォルトでは、MDI/MDIX は自動 MDI に設定され、MDI と MDIX の間のスイッチングを自動的に処理してリンクを確立します。

ステップ 10 [MTU] フィールドに最大伝送ユニット（MTU）を入力します。

MTU 値の範囲は管理対象デバイスのモデルとインターフェイス タイプによって異なる場合があります。

注意 デバイス上のすべての非管理インターフェイスの中で最大MTU値を変更し、設定変更を展開すると、Snortプロセスが再起動され、トラフィック インスペクションが一時的に中断されます。インスペクションは、変更したインターフェイスだけでなく、すべての非管理インターフェイスで中断されます。この中断によってトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびインターフェイスのタイプに応じて異なります。詳細については、「Snort® の再起動によるトラフィックの動作 （451 ページ）」を参照してください。

ステップ 11 LAG インターフェイスが ping や traceroute のような ICMP トラフィックに応答できるようにするには、[ICMP] の横にある [応答を有効にする（Enable Responses）] チェックボックスをオンにします。

ステップ 12 LAG インターフェイスがルータアドバタイズメントをブロードキャストできるようにするには、[IPv6 NDP] の横にある [ルータアドバタイズメントを有効にする（Enable Router Advertisement）] チェックボックスをオンにします。

ステップ 13 [追加（Add）] をクリックして、IP アドレスを追加します。

ステップ 14 [アドレス（Address）] フィールドで、CIDR 表記を使用して、ルーテッド LAG インターフェイスの IP アドレスとサブネット マスクを入力します。

次の点に注意してください。

- ネットワークおよびブロードキャストアドレス、またはスタティック MAC アドレス 00:00:00:00:00:00 および FF:FF:FF:FF:FF:FF は追加できません。
- サブネット マスクに関係なく、仮想ルータのインターフェイスに同じ IP アドレスを追加できません。

ステップ 15 IPv6 を使用した環境で、LAG インターフェイスの IP アドレスを自動設定するには、[IPv6] フィールドの横にある [アドレスの自動設定（Address Autoconfiguration）] チェックボックスをオンにします。

ステップ 16 [タイプ（Type）] には、[普通（Normal）] または [SFRP] を選択します。

ステップ 17 [タイプ（Type）] に SFRP を選択した場合は、SFRPの説明に従いオプションを設定してください。

ステップ 18 [OK] をクリックします。

（注） IP アドレスを 7000 または 8000 シリーズ デバイスの高可用性ペアのルーテッド インターフェイスに追加する場合、高可用性ピアのルーテッドインターフェイスに対応する IP アドレスを追加する必要があります。

ステップ 19 [追加（Add）] をクリックして、スタティック ARP エントリを追加します。

ステップ 20 [IP アドレス（IP Address）] フィールドに IP アドレスを入力します。

ステップ 21 [MAC アドレス（MAC Address）] フィールドに IP アドレスに関連付ける MAC アドレスを入力します。標準形式を使用します（たとえば、01:23:45:67:89:AB）。

ステップ 22 [OK] をクリックします。

ステップ 23 [リンク アグリゲーション（Link Aggregation）] で、LAG バンドルに追加する物理インターフェイスを [使用できるインターフェイス（Available Interfaces）] から 1 つまたは複数選択します。

ヒント LAG バンドルから物理インターフェイスを削除するには、1 つ以上の物理インターフェイスを選択して、選択項目の削除アイコン（  ）をクリックします。LAGバンドルからすべての物理インターフェイスを削除するには、すべてを削除アイコン（  ）をクリックします。[インターフェイス（Interfaces）] タブから LAG インターフェイスを削除すると、そのインターフェイスも削除されます。

ステップ 24 ドロップダウンリストから [ロードバランシング アルゴリズム（Load-Balancing Algorithm）] を選択します。

ステップ 25 ドロップダウンリストから [リンク選択ポリシー（Link Selection Policy）] を選択します。

ヒント Firepower System デバイスとサードパーティ製ネットワーク デバイスとの間に集約インターフェイスを設定する場合は、[LACP 優先（LACP Priority）] を選択します。

ステップ 26 [リンク選択ポリシー（Link Selection Policy）] に [LACP 優先（LACP Priority）] を選択した場合は、[システム優先度（System Priority）] に値を割り当て、[インターフェイスの優先度の設定（Configure Interface Priority）] リンクをクリックして優先度の値を LAG の各インターフェイスに割り当てます。

ステップ 27 [トンネルレベル（Tunnel Level）] ドロップダウン リストから [内部（Inner）] または [外部（Outer）] を選択します。

（注） レイヤ 3 ロード バランシングが設定されている場合、トンネル レベルは IPv4 トラフィックにのみ適用されます。外部トンネルは常に、レイヤ 2 と IPv6 トラフィックに使用されます。[トンネル レベル（Tunnel Level）] が明示的に設定されていない場合、デフォルトは [外部（Outer）] になります。

ステップ 28 [LACP] で [有効（Enabled）] チェックボックスをオンにして、ルーテッド LAG インターフェイスがリンク集約制御プロトコルを使用してトラフィックを処理できるようにします。

このチェックボックスをオフにすると、LAG インターフェイスは静的設定になり、Firepower System はすべての物理インターフェイスを集約に使用します。

ステップ 29 [レート（Rate）] オプション ボタンをクリックし、パートナー デバイスから LACP 制御メッセージを受信する頻度を設定します。

- パケットを 30 秒ごとに受信するには、[遅い（Slow）] をクリックします。
- パケットを 1 秒ごとに受信するには、[速い（Fast）] をクリックします。

ステップ 30 [モード（Mode）] オプション ボタンをクリックし、デバイスのリスニング モードを設定します。

- パートナー デバイスに LACP パケットを送信してリモート リンクとのネゴシエーションを開始するには、[アクティブ（Active）] をクリックします。
- 受信した LACP パケットに応答するには、[パッシブ（Passive）] をクリックします。

ステップ 31 **[保存（Save）]** をクリックします。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

関連トピック

デバイスの詳細設定 （299 ページ）

論理集約インターフェイスの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	Control	7000 & 8000 シリーズ	リーフのみ	Admin/Network Admin

各スイッチドまたはルーテッド集約インターフェイスごとに、複数の論理インターフェイスを追加できます。論理 LAG インターフェイスで受信した VLAN タグ付きトラフィックを処理するには、各論理 LAG インターフェイスをその特定のタグに関連付ける必要があります。物理スイッチドまたはルーテッドインターフェイスに追加するのと同じ方法で、論理インターフェイスをスイッチドまたはルーテッド集約インターフェイスに追加します。

（注） LAG インターフェイスを作成すると、デフォルトで「タグなし」論理インターフェイスが作成されます。このインターフェイスは **lag*n.0*** ラベルによって識別されます（***n*** は 0 ～ 13 の整数）。動作させるには、各 LAG にこの論理インターフェイスが少なくとも 1 つ必要です。LAG に追加の論理インターフェイスを関連付けて、VLAN タグ付きトラフィックを処理できます。追加する各論理インターフェイスには固有の VLAN タグが必要です。Firepower System は 1 ～ 4094 の VLAN タグをサポートします。

注意 7000 または 8000 シリーズ デバイス 設定の変更を展開する際に Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、ターゲットデバイスがトラフィックを処理する方法に応じて異なります。詳細はSnort® の再起動によるトラフィックの動作 （451 ページ）を参照してください。 でのルーテッド インターフェイス ペアの追加

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 論理 LAG インターフェイスを追加するデバイスの横にある、編集アイコン（  ）をクリックします。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [追加（Add）] ドロップダウン メニューから、[論理インターフェイスの追加（Add Logical Interface）] を選択します。

ステップ 4 [スイッチド（Switched）] をクリックしてスイッチド インターフェイス オプションを表示するか、[ルーテッド（Routed）] をクリックしてルーテッド インターフェイス オプションを表示します。

ステップ 5 [インターフェイス（Interface）] ドロップダウン リストから使用可能な LAG を選択します。集約インターフェイスは **lag*n*** ラベルによって識別されます（***n*** は 0 ～ 13 の整数）。

ステップ 6 選択したインターフェイスのタイプに適した残りの設定を行います。

- スイッチド：スイッチドインターフェイスへの論理インターフェイスの追加方法の詳細については、論理スイッチドインターフェイスの追加 （1573 ページ）を参照してください。
- ルーテッド：ルーテッドインターフェイスへの論理インターフェイスの追加方法の詳細については、論理ルーテッドインターフェイスの追加 （1586 ページ）を参照してください。

関連トピック

SFRP
デバイスの詳細設定 （299 ページ）
7000 および 8000 シリーズ デバイスおよび NGIPSv の MTU 範囲 （661 ページ）
Snort® の再起動シナリオ （450 ページ）

集約インターフェイス統計情報の表示

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	Control	7000 & 8000 シリーズ	リーフのみ	Admin/Network Admin

各集約インターフェイスのプロトコルおよびトラフィックの統計情報を表示できます。統計情報には、LACP キーとパートナー情報などの LACP プロトコル情報、受信パケット、転送パケット、ドロップ パケットが表示されます。統計情報は、メンバー インターフェイスごとに詳細化されており、ポート単位でトラフィックとリンクの情報が表示されます。

集約インターフェイス情報は、事前定義されたウィジェットを介してダッシュボードにも表示されます。Current Interface Status ウィジェットは、有効になっているか未使用のアプライアンスのすべてのインターフェイスのステータスを示します。Interface Traffic ウィジェットには、ダッシュボードの時間範囲においてアプライアンスのインターフェイスで送受信された受信（Rx）トラフィックと送信（Tx）トラフィックの割合が示されます。定義済みダッシュボード ウィジェット （325 ページ）を参照してください。

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 論理集約インターフェイス統計情報を表示するデバイスの横にある、編集アイコン（  ）をクリックします。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 インターフェイス統計情報を表示するインターフェイスの横にある、表示アイコン（  ）をクリックします。

集約インターフェイスの削除

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	Control	7000 & 8000 シリーズ	リーフのみ	Admin/Network Admin

集約インターフェイスは **lag*n*** ラベルによって識別できます（***n*** は 0 ～ 13 の整数）。

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 集約インターフェイスを削除するデバイスの横にある、編集アイコン（  ）をクリックします。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 削除する集約インターフェイスの横にある、削除アイコン（  ）をクリックします。

ステップ 4 プロンプトが表示されたら、集約インターフェイスを削除することを確認します。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

第 60 章

ハイブリッド インターフェイス

次のトピックでは、ローカル ハイブリッド インターフェイスの設定方法を示します。

ハイブリッド インターフェイスについて

管理対象デバイス上に論理ハイブリッド インターフェイスを設定することで、Firepower システムが仮想ルータと仮想スイッチの間でトラフィックをブリッジできるようになります。仮想スイッチのインターフェイスで受信した IP トラフィックの宛先が、そのスイッチに関連付けられた論理ハイブリッドインターフェイスの MAC アドレスとなっている場合、システムは、そのトラフィックをレイヤ 3 トラフィックとして処理し、宛先 IP アドレスに応じてトラフィックをルーティングするかトラフィックに応答します。それ以外の宛先が設定されたトラフィックを受信した場合、システムはそのトラフィックをレイヤ 2 トラフィックとして処理し、適切なスイッチングを行います。NGIPSv デバイス上で論理ハイブリッドインターフェイスを設定することはできません。

仮想スイッチと仮想ルータの両方に関連付けられていないハイブリッドインターフェイスは、ルーティングに使用できず、トラフィックを生成することも、トラフィックに応答することもありません。

論理ハイブリッド インターフェイス

レイヤ 2 とレイヤ 3 の間でトラフィックを中継するには、論理ハイブリッドインターフェイスを仮想ルータと仮想スイッチに関連付ける必要があります。仮想スイッチに関連付けることができるハイブリッド インターフェイスは 1 つだけです。一方、仮想ルータには複数のハイブリッド インターフェイスを関連付けることができます。

論理ハイブリッド インターフェイスには、シスコ冗長プロトコル（SFRP）を設定することもできます。SFRP では、指定した IP アドレスに対する冗長なゲートウェイとしてデバイスを機能させることができます。

ハイブリッド インターフェイスの [ICMP 有効応答（ICMP Enable Responses）] オプションを無効にしても、すべてのシナリオで ICMP 応答が抑止されるわけではありません。宛先 IP がハイブリッド インターフェイスの IP で、プロトコルが ICMP であるパケットをドロップするように、アクセス コントロール ポリシーにネットワークベースのルールを追加できます。

管理対象デバイスの [ローカル ルータ トラフィックの検閲（Inspect Local Router Traffic）] オプションを有効にした場合、パケットはホストに到達する前にドロップされるため、すべての応答を防ぐことができます。

MTU 値の範囲は管理対象デバイスのモデルとインターフェイス タイプによって異なる場合があります。

⚠

注意 デバイス上のすべての非管理インターフェイスの中で最大 MTU 値を変更し、設定変更を展開すると、Snort プロセスが再起動され、トラフィック インスペクションが一時的に中断されます。インスペクションは、変更したインターフェイスだけでなく、すべての非管理インターフェイスで中断されます。この中断によってトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびインターフェイスのタイプに応じて異なります。詳細については、「Snort® の再起動によるトラフィックの動作 （451 ページ）」を参照してください。

関連トピック

SFRP の設定 （1589 ページ）
デバイスの詳細設定 （299 ページ）
7000 および 8000 シリーズ デバイスおよび NGIPSv の MTU 範囲 （661 ページ）
Snort® の再起動シナリオ （450 ページ）

論理ハイブリッドインターフェイスの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	Control	7000 & 8000 シリーズ	リーフのみ	Admin/Network Admin

注意 7000 または 8000 シリーズ デバイス 設定の変更を展開する際に Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、ターゲットデバイスがトラフィックを処理する方法に応じて異なります。詳細はSnort® の再起動によるトラフィックの動作 （451 ページ）を参照してください。 でのルーテッド インターフェイス ペアの追加

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 ハイブリッドインターフェイスを追加するデバイスの横にある編集アイコン（  ）をクリックします。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [追加（Add）] ドロップダウン メニューから、[論理インターフェイスの追加（Add Logical Interface）] を選択します。

ステップ 4 [ハイブリッド（Hybrid）] をクリックして、ハイブリッド インターフェイス オプションを表示します。

ステップ 5 [名前（Name）] フィールドに、インターフェイスの名前を入力します。

ステップ 6 [仮想ルータ（Virtual Router）] ドロップダウン リストから既存の仮想ルータを選択し、[なし（None）] を選択するか、または [新規（New）] を選択して新しい仮想ルータを追加します。

（注） 新しい仮想ルータを追加する場合は、ハイブリッド インターフェイスのセットアップが完了した後に、[デバイス管理（Device Management）] ページで、その仮想ルータを設定する必要があります。仮想ルータの追加 （1592 ページ）を参照してください。

ステップ 7 [仮想スイッチ（Virtual Switch）] ドロップダウン リストから既存の仮想スイッチを選択し、[なし（None）] を選択するか、または [新規（New）] を選択して新しい仮想スイッチを追加します。

（注） 新しい仮想スイッチを追加する場合は、ハイブリッド インターフェイスのセットアップが完了した後に、[デバイス管理（Device Management）] ページで、その仮想スイッチを設定する必要があります。仮想スイッチの追加 （1576 ページ）を参照してください。

ステップ 8 ハイブリッドインターフェイスにトラフィックを処理させるには、[有効（Enabled）] チェックボックスをオンにします。

（注） このチェックボックスをオフにすると、インターフェイスは無効になり、管理上はダウンした状態になります。

ステップ 9 [MTU] フィールドに、最大伝送ユニット（MTU）を入力して、パケットの最大許容サイズを指定します。

MTU 値の範囲は管理対象デバイスのモデルとインターフェイス タイプによって異なる場合があります。

注意 デバイス上のすべての非管理インターフェイスの中で最大MTU値を変更し、設定変更を展開すると、Snortプロセスが再起動され、トラフィック インスペクションが一時的に中断されます。インスペクションは、変更したインターフェイスだけでなく、すべての非管理インターフェイスで中断されます。この中断によってトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびインターフェイスのタイプに応じて異なります。詳細については、「Snort® の再起動によるトラフィックの動作 （451 ページ）」を参照してください。

ステップ 10 [ICMP] の横にある [応答を有効にする（Enable Responses）] チェックボックスをオンにして、インターフェイスを ping や traceroute などの ICMP トラフィックに応答可能にします。

ステップ 11 [IPv6 NDP] の横にある [ルータ アドバタイズメントを有効にする（Enable Router Advertisement）] チェックボックスをオンにして、インターフェイスがルータ アドバタイズメントを伝送できるようにします。このオプションを有効にできるのは、IPv6 アドレスを追加した場合のみです。

ステップ 12 IP アドレスを追加するには、[追加（Add）] をクリックします。

ステップ 13 [アドレス（Address）] フィールドに、IP アドレスとサブネットマスクを入力します。次の点に注意してください。

- ネットワークおよびブロードキャストアドレス、またはスタティック MAC アドレス 00:00:00:00:00:00 および FF:FF:FF:FF:FF:FF は追加できません。
- サブネット マスクに関係なく、仮想ルータのインターフェイスに同じ IP アドレスを追加できません。

ステップ 14 IPv6 アドレスがある場合、オプションで、[IPv6] フィールドの横にある [アドレスの自動設定（Address Autoconfiguration）] チェックボックスをオンにして、インターフェイスの IP アドレスを自動的に設定します。

ステップ 15 [タイプ（Type）] には、[普通（Normal）] または [SFRP] を選択します。

ステップ 16 [タイプ（Type）] に SFRP を選択した場合は、SFRPの説明に従いオプションを設定してください。

ステップ 17 [OK] をクリックします。

ステップ 18 [保存（Save）] をクリックします。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

関連トピック

7000 および 8000 シリーズ デバイスおよび NGIPSv の MTU 範囲 （661 ページ）
Snort® の再起動シナリオ （450 ページ）

論理ハイブリッド インターフェイスの削除

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	Control	7000 & 8000 シリーズ	リーフのみ	Admin/Network Admin

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 論理ハイブリッド インターフェイスを削除するデバイスの横にある編集アイコン（  ）をクリックします。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 削除する論理ハイブリッド インターフェイスの横にある削除アイコン（  ）をクリックします。

ステップ 4 入力を求められた場合、インターフェイスを削除することを確認します。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

第 61 章

ゲートウェイ VPN

次のトピックでは、VPN 展開を管理する方法について説明します。

ゲートウェイ VPN の基本

バーチャル プライベート ネットワーク（VPN）は、インターネットや他のネットワークなどのパブリック ソースを介したエンドポイント間でセキュアなトンネルを確立するネットワーク接続です。Firepower 管理対象デバイスの仮想ルータ間にセキュア VPN トンネルを確立するように Firepower システムを設定できます。システムは、インターネット プロトコル セキュリティ（IPsec）プロトコル スイートを使用してトンネルを構築します。

VPN 接続が確立されると、ローカル ゲートウェイの背後にあるホストはセキュアな VPN トンネルを介して、リモート ゲートウェイの背後にあるホストに接続することができます。接続は、2 つのゲートウェイの IP アドレスとホスト名、その背後のサブネット、および相互認証のための 2 つのゲートウェイの共有秘密で構成されます。

VPN エンドポイントは、Internet Key Exchange（IKE）のバージョン 1 またはバージョン 2 のいずれかのプロトコルを使用して相互に認証し、トンネルに対してセキュリティ アソシエーションを作成します。システムは IPsec Authentication Header（AH）プロトコルまたは IPsec Encapsulating Security Payload（ESP）プロトコルのいずれかを使用して、トンネルに入るデータを認証します。ESP プロトコルは、AH と同じ機能を提供する他にデータの暗号化も行います。

展開にアクセス コントロール ポリシーが存在する場合、システムは、VPN トラフィックがアクセス コントロールを通過するまで VPN トラフィックを送信しません。さらに、システムは、トンネルがダウンしている場合は、トンネル トラフィックをパブリックなソースに送信しません。

VPN を Firepower 用に設定して展開するには、展開先の各管理対象デバイスで VPN ライセンスを有効にしておく必要があります。また、VPN 機能は 7000 および 8000 シリーズ デバイスでのみ使用できます。

IPsec

IPsec プロトコル スイートは、VPN トンネルにおいて、IP パケットが ESP または AH セキュリティ プロトコルでどのようにハッシュ、暗号化、およびカプセル化されるかを定義します。Firepower システムはハッシュ アルゴリズムおよび Security Association（SA）の暗号キーを使用しますが、これは、Internet Key Exchange（IKE）プロトコルによって 2 つのゲートウェイ間で確立されています。

セキュリティ アソシエーション（SA）は 2 つのデバイス間で共有のセキュリティ属性を確立し、VPN エンドポイントがセキュアな通信をサポートできるようにします。SA は、2 つの VPN エンドポイントが、VPN トンネルがどのようにセキュアにされているかを表すパラメータを処理することができます。

システムは、IPsec 接続のネゴシエーションの最初の段階で Internet Security Association and Key Management Protoco（ISAKMP）を使用し、エンドポイントと認証キー交換の間で VPN を確立します。IKE プロトコルは ISAKMP 内にあります。

AH セキュリティ プロトコルは、パケット見出しとデータを保護しますが、暗号化はできません。ESP はパケットを暗号化および保護しますが、最も外側の IP 見出しをセキュアにすることはできません。多くの場合、この保護は必要なく、大半の VPN 展開は、（暗号化の機能により）AH よりも頻繁に ESP を使用します。VPN はトンネル モードのみで動作するため、システムはレイヤ 3 からのパケット全体を暗号化および認証し、ESP プロトコル内で稼動します。トンネル モードの ESP は、後者の暗号化機能だけでなく、データを暗号化します。

IKE

Firepower システムは IKE プロトコルを使用して、トンネルに対して SA をネゴシエートする他に、2 つのゲートウェイを相互に認証します。プロセスは、次の 2 つのフェーズで構成されます。

IKE フェーズ 1 では、Diffie-Hellman キー交換によってセキュアに認証された通信チャネルを確立し、より多くの IKE 通信を暗号化するために事前共有キーを生成します。このネゴシエーションにより、双方向の ISAKMP セキュリティ アソシエーションが生じます。ユーザは、事前共有キーを使用して認証を行うことができます。フェーズ 1 はメイン モードで機能します。このフェーズでは、ネゴシエーションの間にすべてのデータを保護しようとしますが、ピアのアイデンティティも保護します。

IKE フェーズ 2 では、IKE ピアが、フェーズ 1 で確立されたセキュアなチャネルを使用して、IPsec の代わりにセキュリティ アソシエーションにネゴシエートします。ネゴシエーションにより、最低 2 つの単方向セキュリティ アソシエーション（一方は着信、他方は発信）が生じます。

VPN 展開

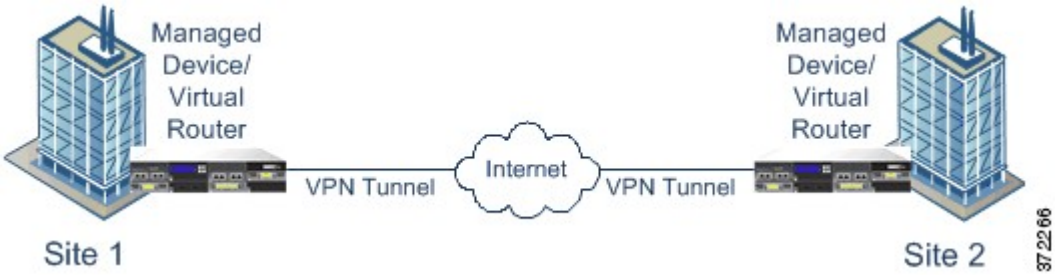
VPN 展開は、VPN に含まれているエンドポイントおよびネットワークを指定し、またそれらが相互にどのように接続しているかを指定します。VPN 展開を Firepower Management Center に設定すると、次に管理対象デバイス、または別の Firepower Management Center によって管理されているデバイスにその VPN 展開を導入できます。

システムでは、ポイントツーポイント、スター、およびメッシュという 3 つのタイプの VPN 展開がサポートされています。

ポイントツーポイントの VPN 展開

ポイントツーポイントの VPN 展開では、2 つのエンドポイントが相互に直接通信します。2 つのエンドポイントをピアデバイスとして設定し、いずれかのデバイスでセキュアな接続を開始できます。この設定の各デバイスは、VPN 対応の管理対象デバイスであることが必要です。

次の図は、一般的なポイントツーポイントの VPN 展開を示しています。



スター VPN 導入

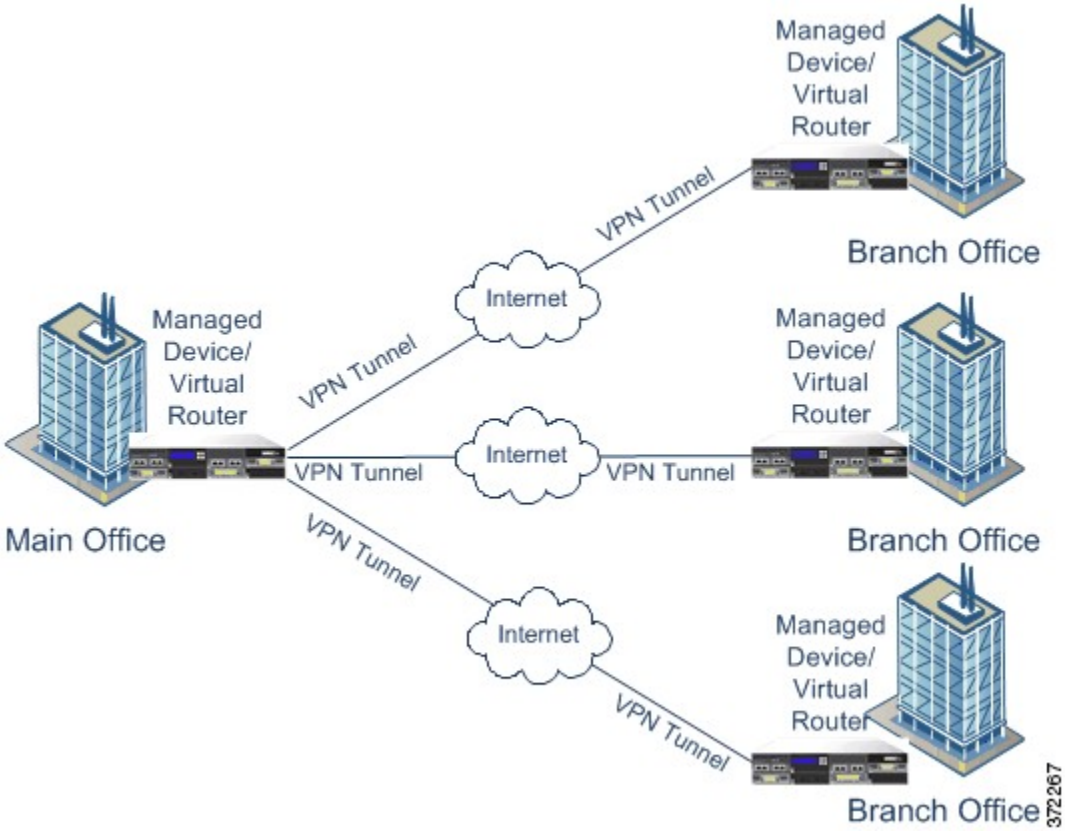
スター VPN 導入では、中央のエンドポイント（ハブ ノード）が、複数のリモート エンドポイント（リーフ ノード）とのセキュアな接続を確立します。ハブ ノードと個々のリーフ ノード間のそれぞれの接続は、別の VPN トンネルです。いずれかのリーフ ノードの背後にあるホストは、ハブ ノードを介して互いに通信できます。

スター型の展開は一般的に、インターネットや他のサードパーティのネットワークを介してセキュアな接続を使用している組織の本店と支店を接続する VPN を表します。スター VPN 展開は、すべての従業員に対して、組織のネットワークへのコントロールされたアクセスを提供します。

一般的なスター型の導入では、ハブ ノードは本社に配置します。リーフ ノードは支社に配置します。トラフィックの大部分は、これらのリーフ ノードから開始されます。各ノードは、VPN 対応の管理対象デバイスであることが必要です。

スター型の導入は、IKE バージョン 2 のみをサポートします。

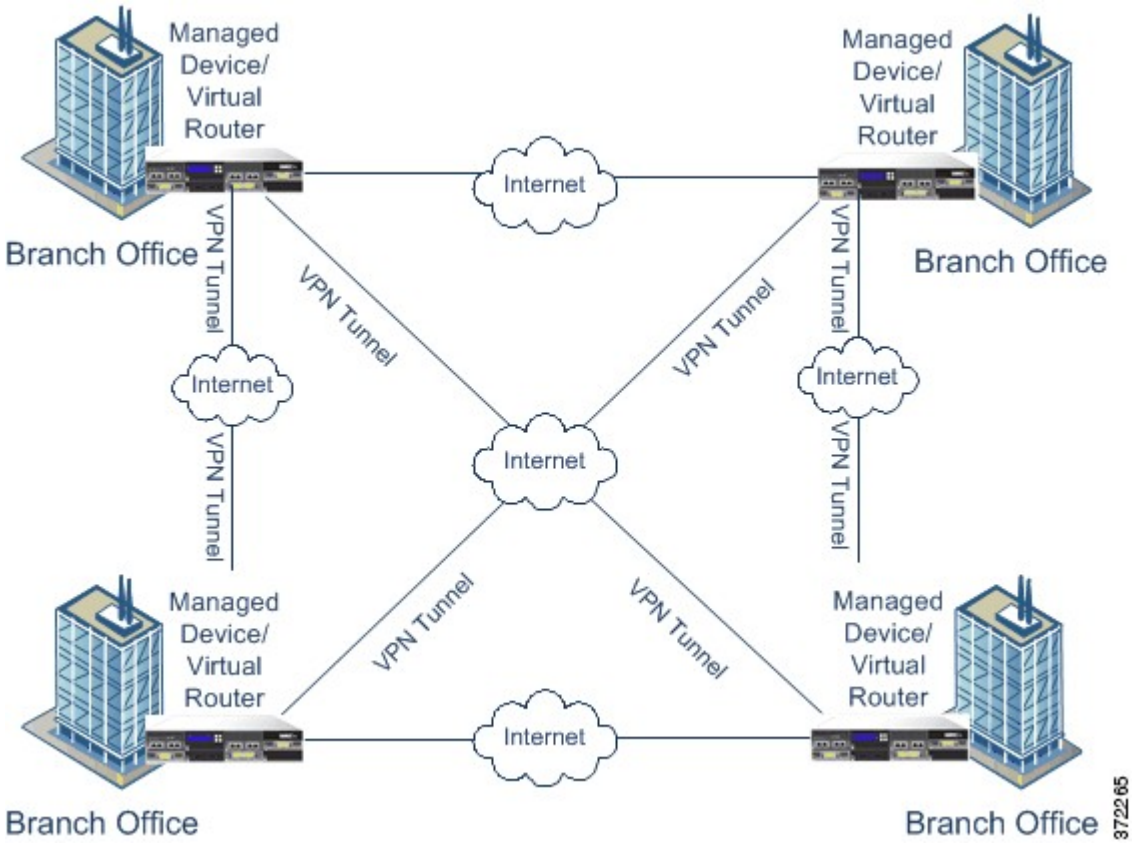
次の図は、一般的なスター VPN 導入を示しています。



メッシュ VPN 展開

メッシュ VPN 展開では、すべてのエンドポイントが個々の VPN トンネルによって他のエンドポイントと通信できます。メッシュ型の展開では 1 つのエンドポイントで障害が発生しても残りのエンドポイントが相互に通信できるように、冗長性を備えています。このタイプの展開は一般的に、分散した支店が配置されたグループを接続する VPN を表します。この設定で展開する VPN 対応の管理対象デバイスの数は、必要な冗長性のレベルによって異なります。各エンドポイントは、VPN 対応の管理対象デバイスであることが必要です。

次の図は、一般的なメッシュ VPN 展開を示しています。



VPN 展開の管理

[VPN] ページ（**[Devices]** > **[VPN]** > **[Site to Site]**）で、現行のすべての VPN 展開を、展開に含まれている名前およびエンドポイントごとに表示することができます。このページ内のオプションを使用して、VPN 展開のステータスを表示する、新しい展開を作成する、管理対象デバイスに展開する、展開を修正または削除する、といった操作を実行することができます。

デバイスを Firepower Management Center に登録すると、登録中に、展開済みの VPN が Firepower Management Center と同期されることに注意してください。

関連トピック

VPN 展開の管理 （1654 ページ）

VPN 展開オプション

新しい VPN 展開を作成する場合には、最小限の処理として、一意の名前と展開のタイプを指定し、事前共有キーを指定する必要があります。次の 3 つのタイプの展開から選択することができ、それぞれの展開には VPN トンネルが含まれています。

- ポイントツーポイント（PTP）型の展開は、2 つのエンドポイント間で VPN トンネルを確立します。

- スター型の展開は VPN トンネルのグループを確立し、ハブ エンドポイントをリーフ エンドポイントのグループに接続します。
- メッシュ型の展開は、エンドポイントのセット内で VPN トンネルのグループを確立します。

VPN 展開でエンドポイントとして使用できるのは、Cisco の管理対象デバイスのみです。サードパーティ製のエンドポイントはサポートされません。

VPN 認証に対して事前共有キーを定義する必要があります。展開内で生成したすべての VPN 接続で使用するデフォルトのキーを指定できます。ポイントツーポイント型の展開では、各エンドポイントのペアに事前共有キーを指定できます。

マルチドメイン展開では、ドメイン間で VPN 展開を構成できます。つまり、異なるドメインに属するデバイスにエンドポイントを割り当てることができます。このような場合は、関連する子孫ドメインで先祖の展開を表示できますが、変更することはできません。ドリルダウンして展開の詳細を表示すると、現在のドメインに属するデバイスの情報のみが表示されます。

ポイントツーポイント VPN 展開オプション

ポイントツーポイント VPN 展開を設定する場合は、エンドポイント ペアのグループを定義し、各ペアの 2 つのノード間に VPN を作成します。

次に、展開で指定できるオプションについて示します。

[名前（Name）]

展開の一意の名前を指定します。

タイプ（Type）

ポイントツーポイント型の展開を設定するには、[PTP] をクリックします。

Pre-shared Key

認証に対して一意の事前共有キーを定義します。各エンドポイント ペアに対して事前共有キーを指定しない場合は、システムで展開内のすべての VPN に対してこのキーが使用されます。

Device

展開のエンドポイントとして、デバイス スタックやデバイス高可用性ペアなどの管理対象デバイスを選択できます。使用している Firepower Management Center で管理されていないシスコの管理対象デバイスの場合は、[その他（Other）] を選択し、エンドポイントの IP アドレスを指定します。

[仮想ルータ（Virtual Router）]

エンドポイントとして管理対象デバイスを選択する場合は、選択したデバイスに現在適用されている仮想ルータを選択します。複数のエンドポイントに同じ仮想ルータを選択することはできません。

インターフェイス（Interface）

エンドポイントとして管理対象デバイスを選択した場合は、指定した仮想ルータに割り当てられているルーテッド インターフェイスを選択します。

[IPアドレス（IP Address）]

- エンドポイントとして管理対象デバイスを選択する場合は、指定されたルーテッドインターフェイスに割り当てられている IP アドレスを選択します。
- 管理対象デバイスがデバイス高可用性ペアの場合は、SFRP IP アドレスのリストからのみ選択できます。
- 選択した管理対象デバイスが Firepower Management Center で管理されて**いない**場合は、エンドポイントに IP アドレスを指定します。

[保護されたネットワーク（Protected Networks）]

暗号化された展開でネットワークを指定します。各ネットワークに対して CIDR ブロックでサブネットを入力します。IKE バージョン 1 は、保護された単一のネットワークのみサポートしています。

VPN エンドポイントは同じ IP アドレスを持つことはできません。また、VPN エンドポイントペアの保護されたネットワークは重複することはできないことに注意してください。エンドポイントについて保護されたネットワークのリストに 1 つ以上の IPv4 または IPv6 エントリが含まれている場合、他のエンドポイントの保護されたネットワークは、同じタイプ（IPv4 または IPv6）のエントリを少なくとも 1 つ持っていることが必要です。このようなエントリを持っていない場合、他のエンドポイントの IP アドレスが同じタイプであること、および保護されたネットワーク内でエントリが重複しないことが必要です（IPv4 については /32 CIDR アドレスを使用し、IPv6 については /128 CIDR アドレス ブロックを使用します）。これらの両方のチェックに失敗すると、エンドポイントのペアは機能しません。

[内部 IP（Internal IP）]

エンドポイントが、ネットワーク アドレス変換を備えたファイアウォールの背後に配置されている場合は、このチェックボックスをオンにします。

[パブリック IP（Public IP）]

[内部 IP（Internal IP）] チェックボックスをオンにした場合は、ファイアウォールに対してパブリック IP アドレスを指定します。エンドポイントが応答側の場合は、この値を指定する必要があります。

[パブリック IKE ポート（Public IKE Port）]

[内部 IP（Internal IP）] チェックボックスをオンにした場合は、内部のエンドポイントにポート転送されているファイアウォール上の UDP ポートに対して、1 ～ 65535 の数値を指定します。エンドポイントが応答側で、転送されているファイアウォール上のポートが 500 または 4500 ではない場合、この値を指定する必要があります。

[実装キーを使用する（Use Deployment Key）]

展開に対して定義されている事前共有キーを使用する場合は、チェックボックスをオンにします。このエンドポイント ペアに対して VPN 認証の事前共有キーを指定するには、チェックボックスをオフにします。

Pre-shared Key

[実装キーを使用する（Use Deployment Key）] チェックボックスをオフにした場合は、このフィールドに事前共有キーを指定します。

関連トピック

ポイントツーポイント VPN 展開の設定 （1655 ページ）

スター VPN の展開オプション

スター VPN 展開を設定する場合は、1 つのハブ ノード エンドポイント、およびリーフ ノード エンドポイントのグループを定義します。展開を設定するには、ハブ ノード エンドポイントと、少なくとも 1 つのリーフ ノード エンドポイントを定義する必要があります。

次に、展開で指定できるオプションについて示します。

[名前（Name）]

展開の一意の名前を指定します。

タイプ（Type）

スター型の展開を設定するには、[Star] をクリックします。

Pre-shared Key

認証に対して一意の事前共有キーを定義します。

Device

展開のエンドポイントとして、デバイス スタックやデバイス高可用性ペアなどの管理対象デバイスを選択できます。使用している Firepower Management Center で管理されていないシスコの管理対象デバイスの場合は、[その他（Other）] を選択し、エンドポイントの IP アドレスを指定します。

[仮想ルータ（Virtual Router）]

エンドポイントとして管理対象デバイスを選択する場合は、選択したデバイスに現在適用されている仮想ルータを選択します。複数のエンドポイントに同じ仮想ルータを選択することはできません。

インターフェイス（Interface）

エンドポイントとして管理対象デバイスを選択する場合は、選択した仮想ルータに割り当てられているルーテッド インターフェイスを選択します。

[IPアドレス（IP Address）]

- エンドポイントとして管理対象デバイスを選択する場合は、指定されたルーテッドインターフェイスに割り当てられている IP アドレスを選択します。

- 管理対象デバイスがデバイス高可用性ペアの場合は、SFRP IP アドレスのリストからのみ選択できます。
- 選択した管理対象デバイスが Firepower Management Center で管理されて**いない**場合は、エンドポイントに IP アドレスを指定します。

[保護されたネットワーク（Protected Networks）]

暗号化された展開でネットワークを指定します。各ネットワークに対して CIDR ブロックでサブネットを入力します。

VPN エンドポイントは同じ IP アドレスを持つことはできません。また、VPN エンドポイントペアの保護されたネットワークは重複することはできないことに注意してください。エンドポイントについて保護されたネットワークのリストに 1 つ以上の IPv4 または IPv6 エントリが含まれている場合、他のエンドポイントの保護されたネットワークは、同じタイプ（IPv4 または IPv6）のエントリを少なくとも 1 つ持っていることが必要です。このようなエントリを持っていない場合、他のエンドポイントの IP アドレスが同じタイプであること、および保護されたネットワーク内でエントリが重複しないことが必要です（IPv4 については /32 CIDR アドレスを使用し、IPv6 については /128 CIDR アドレス ブロックを使用します）。これらの両方のチェックに失敗すると、エンドポイントのペアは機能しません。

[内部 IP（Internal IP）]

エンドポイントが、ネットワーク アドレス変換を備えたファイアウォールの背後に配置されている場合は、このチェックボックスをオンにします。

[パブリック IP（Public IP）]

[内部 IP（Internal IP）] チェックボックスをオンにした場合は、ファイアウォールに対してパブリック IP アドレスを指定します。エンドポイントが応答側の場合は、この値を指定する必要があります。

[パブリック IKE ポート（Public IKE Port）]

[内部 IP（Internal IP）] チェックボックスをオンにした場合は、内部のエンドポイントにポート転送されているファイアウォール上の UDP ポートに対して、1 ～ 65535 の数値を指定します。エンドポイントが応答側で、転送されているファイアウォール上のポートが 500 または 4500 ではない場合、この値を指定する必要があります。

関連トピック

スター VPN 展開の設定 （1656 ページ）

メッシュ VPN 展開オプション

メッシュ VPN 展開を設定する場合は、VPN のグループを定義して、特定のエンドポイントセットに任意の 2 つのポイントをリンクさせます。

次に、展開で指定できるオプションについて示します。

[名前（Name）]

展開の一意の名前を指定します。

タイプ（Type）

メッシュ型の展開を設定するには、[Mesh] をクリックします。

Pre-shared Key

認証に対して一意の事前共有キーを定義します。

Device

展開のエンドポイントとして、デバイス スタックやデバイス高可用性ペアなどの管理対象デバイスを選択できます。使用している Firepower Management Center で管理されていないシスコの管理対象デバイスの場合は、[その他（Other）] を選択し、エンドポイントの IP アドレスを指定します。

[仮想ルータ（Virtual Router）]

エンドポイントとして管理対象デバイスを選択した場合は、指定したデバイスに適用されている仮想ルータを選択します。複数のエンドポイントに同じ仮想ルータを選択することはできません。

インターフェイス（Interface）

エンドポイントとして管理対象デバイスを選択した場合は、指定した仮想ルータに割り当てられているルーテッド インターフェイスを選択します。

[IPアドレス（IP Address）]

- エンドポイントとして管理対象デバイスを選択した場合は、選択したルーテッドインターフェイスに割り当てられている IP アドレスを選択します。
- 管理対象デバイスがデバイス高可用性ペアの場合は、SFRP IP アドレスのリストからのみ選択できます。
- 選択した管理対象デバイスが Firepower Management Center で管理されて**いない**場合は、エンドポイントに IP アドレスを指定します。

[保護されたネットワーク（Protected Networks）]

暗号化された展開でネットワークを指定します。各ネットワークに対して CIDR ブロックでサブネットを入力します。IKE バージョン 1 は、保護された単一のネットワークのみサポートしています。

VPN エンドポイントは同じ IP アドレスを持つことはできません。また、VPN エンドポイントペアの保護されたネットワークは重複することはできないことに注意してください。エンドポイントについて保護されたネットワークのリストに 1 つ以上の IPv4 または IPv6 エントリが含まれている場合、他のエンドポイントの保護されたネットワークは、同じタイプ（IPv4 または IPv6）のエントリを少なくとも 1 つ持っていることが必要です。このようなエントリを持っていない場合、他のエンドポイントの IP アドレスが同じタイプであること、および保護されたネットワーク内でエントリが重複しないことが必要です（IPv4 については /32 CIDR アドレスを使用し、IPv6 については /128 CIDR アドレス ブロックを使用します）。これらの両方のチェックに失敗すると、エンドポイントのペアは機能しません。

[内部 IP（Internal IP）]

エンドポイントが、ネットワークアドレス変換を備えたファイアウォールの背後に配置されている場合は、このチェックボックスをオンにします。

[パブリック IP（Public IP）]

[内部 IP（Internal IP）] チェックボックスをオンにした場合は、ファイアウォールに対してパブリック IP アドレスを指定します。エンドポイントが応答側の場合は、この値を指定する必要があります。

[パブリック IKE ポート（Public IKE Port）]

[内部 IP（Internal IP）] チェックボックスをオンにした場合は、内部のエンドポイントにポート転送されているファイアウォール上の UDP ポートに対して、1 ～ 65535 の数値を指定します。エンドポイントが応答側で、転送されているファイアウォール上のポートが 500 または 4500 ではない場合、この値を指定する必要があります。

関連トピック

メッシュ VPN 展開の設定 （1657 ページ）

VPN 展開の詳細オプション

VPN の展開には、展開の VPN で共有できる共通設定がいくつか含まれています。各 VPN では、デフォルトの設定を使用するか、またはそのデフォルトの設定を上書きすることができます。通常、詳細設定はほとんど、あるいはまったく変更する必要がありません。詳細設定は導入環境ごとに異なります。

次に、展開で指定できる高度なオプションについて示します。

許可されるその他のアルゴリズム（Other Algorithm Allowed）

このチェックボックスをオンにすると、[アルゴリズム（Algorithm）] リストに含まれていないがリモートピアによって提案されるアルゴリズムについて、自動ネゴシエーションが有効になります。

アルゴリズム（SNMP (v3) Auth. Alrorithm）

展開でデータのセキュリティを確保するため、フェーズ 1 とフェーズ 2 のアルゴリズムの提案を指定します。両方のフェーズに対して、**[暗号（Cipher）]**、**[ハッシュ（Hash）]**、および [Diffie-Hellman (**DH**)]グループ認証メッセージを選択します。

IKE ライフタイム（IKE Life Time）

IKE SA の最大ネゴシエーション間隔について、数値を指定し、時間単位を選択します。最小 15 分、最大 30 日を指定できます。

IKE v2

システムで IKE バージョン 2 を使用する場合は、このチェックボックスをオンにします。このバージョンでは、スター型の展開と複数の保護ネットワークがサポートされます。

Life Time

SA の最大の再ネゴシエーション間隔に対して数値を指定し、時間単位を選択します。最低 5 分、最大 24 時間まで指定できます。

Life Packets

有効期間が終了する前に、IPsec SA を介して伝送できるパケット数を指定します。0～18446744073709551615 の整数を使用できます。

Life Bytes

有効期間が終了する前に、IPsec SA を介して伝送できるバイト数を指定します。0～18446744073709551615 の整数を使用できます。

AH

保護対象のデータに対して認証ヘッダー セキュリティ プロトコルを使用するように指定する場合は、このチェックボックスをオンにします。暗号化サービスペイロード（ESP）プロトコルを使用する場合は、このチェックボックスをオフにします。

関連トピック

高度な VPN 展開を設定する方法 （1658 ページ）

VPN 展開の管理

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
該当なし	VPN	7000 & 8000 シリーズ	任意（Any）	Admin/Network Admin

注意 7000 または 8000 シリーズ デバイス上の VPN を追加または削除して、設定の変更を展開する際に Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、ターゲットデバイスがトラフィックを処理する方法に応じて異なります。詳細はSnort® の再起動によるトラフィックの動作 （451 ページ）を参照してください。

ステップ 1 **[Devices]** > **[VPN]** > **[Site to Site]**を選択します。

ステップ 2 VPN の展開を管理します。

- 追加：新しい VPN の展開を作成するには、**[VPN の追加（Add VPN）]** > **[Firepower デバイス（Firepower Device）]** をクリックして、展開タイプに応じて次の手順を実行します。
  - メッシュ VPN 展開の設定 （1657 ページ）
  - ポイントツーポイント VPN 展開の設定 （1655 ページ）
  - スター VPN 展開の設定 （1656 ページ）

- 編集：既存の VPN 展開の設定を変更するには、編集アイコン（  ）をクリックします。VPN 展開の編集 （1659 ページ）を参照してください。
- 削除：VPN 展開を削除するには、削除アイコン（  ）をクリックします。
- 展開：[展開（Deploy）] をクリックします（設定変更の展開 （447 ページ） を参照）。
- VPN ステータスの表示：既存の VPN 展開のステータスを表示するには、ステータスアイコンをクリックします。VPN ステータスの表示 （1660 ページ）を参照してください。

関連トピック

Snort® の再起動シナリオ （450 ページ）

ポイントツーポイント VPN 展開の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
該当なし	VPN	7000 & 8000 シリーズ	任意（Any）	Admin/Network Admin

始める前に

管理対象デバイスをエンドポイントとして使用している場合、仮想ルータを作成し、それを適切なデバイスに適用します。

（注） 複数のエンドポイントに同じ仮想ルータを使用することはできません。詳細については、仮想ルータのセットアップ （1581 ページ）を参照してください。

ステップ 1 **[Devices]** > **[VPN]** > **[Site to Site]**を選択します。

ステップ 2 **[VPN の追加（Add VPN）]** > **[Firepower デバイス（Firepower Device）]** をクリックします。

ステップ 3 一意の名前を入力します。

ステップ 4 [タイプ（Type）] として [PTP] が選択されていることを確認します。

ステップ 5 一意の事前共有キーを入力します。

ステップ 6 [ノード ペア（Node Pairs）] の隣の追加アイコン（  ）をクリックします。

ステップ 7 ポイントツーポイント VPN 展開オプション （1648 ページ）で説明されている VPN 展開オプションを設定します。

ステップ 8 [ノード A（Node A）] の下の [保護されたネットワーク（Protected Networks）] の隣にある追加アイコン（  ）をクリックします。

ステップ 9 保護されたネットワークの CIDR ブロックを入力します。

ステップ 10 [OK] をクリックします。
ステップ 11 [ノード B（Node B）] に対して手順 8 ～ 10 を繰り返します。
ステップ 12 [保存（Save）] をクリックします。
エンドポイント ペアが展開に追加されます。
ステップ 13 [保存（Save）] をクリックして、展開の設定を終了します。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

スター VPN 展開の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
該当なし	VPN	7000 & 8000 シリーズ	任意（Any）	Admin/Network Admin

始める前に

管理対象デバイスをエンドポイントとして使用している場合、仮想ルータを作成し、それを適切なデバイスに適用します。

（注） 複数のエンドポイントに同じ仮想ルータを使用することはできません。詳細については、仮想ルータのセットアップ （1581 ページ）を参照してください。

ステップ 1 **[Devices]** > **[VPN]** > **[Site to Site]**を選択します。
ステップ 2 **[VPN の追加（Add VPN）]** > **[Firepower デバイス（Firepower Device）]** をクリックします。
ステップ 3 一意の名前を入力します。
ステップ 4 [スター（Star）] をクリックしてタイプを指定します。
ステップ 5 一意の事前共有キーを入力します。
ステップ 6 [ハブ ノード（Hub Node）] の隣の編集アイコン（）をクリックします。
ステップ 7 スター VPN の展開オプション （1650 ページ）で説明されている VPN 展開オプションを設定します。
ステップ 8 [保護されたネットワーク（Protected Networks）] の隣の追加アイコン（）をクリックします。
ステップ 9 保護されたネットワークの IP アドレスを入力します。
ステップ 10 [OK] をクリックします。
ステップ 11 [保存（Save）] をクリックします。ハブ ノードが展開に追加されます。
ステップ 12 [リーフ ノード（Leaf Nodes）] の隣の追加アイコン（）をクリックします。

ステップ 13 リーフ ノードを完了するには、手順 7 ～ 10 を繰り返します。これにより、ハブ ノードと同じオプションが設定されます。

ステップ 14 [保存（Save）] をクリックします。
リーフ ノードが展開に追加されます。

ステップ 15 [保存（Save）] をクリックして、展開の設定を終了します。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

メッシュ VPN 展開の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
該当なし	VPN	7000 & 8000 シリーズ	任意（Any）	Admin/Network Admin

始める前に

管理対象デバイスをエンドポイントとして使用している場合、仮想ルータを作成し、それを適切なデバイスに適用します。

（注） 複数のエンドポイントに同じ仮想ルータを使用することはできません。詳細については、仮想ルータのセットアップ （1581 ページ）を参照してください。

ステップ 1 **[Devices]** > **[VPN]** > **[Site to Site]**を選択します。

ステップ 2 **[VPN の追加（Add VPN）]** > **[Firepower デバイス（Firepower Device）]** をクリックします。

ステップ 3 一意の名前を入力します。

ステップ 4 [メッシュ（Mesh）] をクリックして [タイプ（Type）] を指定します。

ステップ 5 一意の事前共有キーを入力します。

ステップ 6 [ノード（Nodes）] の隣の追加アイコン（）をクリックします。

ステップ 7 メッシュ VPN 展開オプション （1651 ページ）で説明されている VPN 展開オプションを設定します。

ステップ 8 [保護されたネットワーク（Protected Networks）] の隣の追加アイコン（）をクリックします。

ステップ 9 保護されたネットワークの CIDR ブロックを入力します。

ステップ 10 [OK] をクリックします。
保護されたネットワークが追加されます。

ステップ 11 [保存（Save）] をクリックします。

展開にエンドポイントが追加されます。

ステップ 12 エンドポイントをさらに追加するには、ステップ 6 ～ 11 を繰り返します。

ステップ 13 [保存（Save）] をクリックして展開を完了します。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

高度な VPN 展開を設定する方法

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
該当なし	VPN	7000 & 8000 シリーズ	任意（Any）	Admin/Network Admin

マルチドメイン展開では、現在のドメインで作成された VPN 展開が表示されます。これは編集できます。また、エンドポイントデバイスの 1 つがドメインに属している場合は、先祖ドメインで作成された VPN 展開も表示されます。先祖ドメインで作成された VPN 展開は編集できません。下位のドメインで作成された VPN 展開を表示および編集するには、そのドメインに切り替えます。

ステップ 1 **[Devices]** > **[VPN]** > **[Site to Site]**を選択します。

ステップ 2 編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 [Advanced] タブをクリックします。

ステップ 4 VPN 展開の詳細オプション （1653 ページ）の説明に従って、詳細設定を行います。

ステップ 5 [アルゴリズム（Algorithms）] の隣の追加アイコン（）をクリックします。

ステップ 6 両方のフェーズに対して、[暗号（Cipher）]、[ハッシュ（Hash）]、および[Diffie-Hellman]（[DH]）グループ認証のメッセージを選択します。

ステップ 7 [OK] をクリックします。

ステップ 8 [保存（Save）] をクリックします。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

VPN 展開の編集

注意 2 人のユーザが同じ展開について同時に編集**してはいけません**。ただし、Web インターフェイスでは同時編集を防止していないことに注意してください。

マルチドメイン展開では、現在のドメインで作成された VPN 展開が表示されます。これは編集できます。また、エンドポイントデバイスの 1 つがドメインに属している場合は、先祖ドメインで作成された VPN 展開も表示されます。先祖ドメインで作成された VPN 展開は編集できません。下位のドメインで作成された VPN 展開を表示および編集するには、そのドメインに切り替えます。

ステップ 1 **[Devices]** > **[VPN]** > **[Site to Site]**を選択します。

ステップ 2 編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 必要な設定を変更します。

- [詳細設定（Advanced）]の設定。高度な VPN 展開を設定する方法（1658 ページ）を参照してください。
- メッシュ展開の設定。メッシュ VPN 展開の設定（1657 ページ）を参照してください。
- ポイントツーポイント型の展開の設定。ポイントツーポイント VPN 展開の設定（1655 ページ）を参照してください。
- スター型の展開の設定。スター VPN 展開の設定（1656 ページ）を参照してください。

ヒント 展開を最初に保存した後で、展開のタイプを編集することはできません。展開のタイプを変更するには、展開を削除してから新しい展開を作成する必要があります。

次のタスク

- 設定変更を展開します。設定変更の展開（447 ページ）を参照してください。

VPN 展開のステータス

VPN 展開を設定した後で、設定した VPN トンネルのステータスを表示できます。VPN ページには、各 VPN 展開の展開後に、その展開のステータス アイコンが表示されます。

- （）アイコンは、すべての VPN エンドポイントが稼動していることを表します。
- （）アイコンは、すべての VPN エンドポイントが停止していることを表します。

- （  ）アイコンは、稼動しているエンドポイントと停止しているエンドポイントがあることを表します。

ステータスアイコンをクリックして、展開のステータス、および展開内のエンドポイントに関する基本情報（エンドポイント名やIPアドレスなど）を表示することができます。VPNステータスは、毎分、または（エンドポイントが停止した、または稼動したなど）ステータスの変更が生じた場合に更新されます。

関連トピック

VPN ステータスの表示 （1660 ページ）

VPN ステータスの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
該当なし	VPN	7000 & 8000 シリーズ	任意（Any）	Admin/Network Admin

マルチドメイン展開では、システムは現在のドメインで作成された VPN 展開を表示します。また、エンドポイントデバイスの1つがドメインに属している場合は、先祖ドメインで作成された VPN 展開も表示されます。下位のドメインで作成された VPN 展開を表示するには、そのドメインに切り替えます。

ステップ 1 **[Devices]** > **[VPN]** > **[Site to Site]**を選択します。

ステップ 2 ステータスを表示する展開の隣にある、VPN ステータス アイコンをクリックします。

ステップ 3 [OK] をクリックします。

VPN の統計およびログ

VPN 展開を設定した後で、設定した VPN トンネルを通過するデータの統計を表示することができます。また、各エンドポイントについて最新の VPN システムと IKE ログを表示することができます。

システムには、次の統計情報が表示されます。

エンドポイント（Endpoint）

VPN エンドポイントとして指定されたルーテッド インターフェイスおよび IP アドレスへのデバイス パス。

Status

VPN 接続の状態（稼動または停止のどちらか）。

Protocol

暗号化で使用されるプロトコル（ESP または AH）。

Packets Received

IPsec SA ネゴシエーション中に VPN トンネルが受信する、インターフェイスあたりのパケット数。

Packets Forwarded

IPsec SA ネゴシエーション中に VPN トンネルが送信する、インターフェイスあたりのパケット数。

Bytes Received

IPsec SA ネゴシエーション中に VPN トンネルが受信する、インターフェイスあたりのバイト数。

Bytes Forwarded

IPsec SA ネゴシエーション中に VPN トンネルが送信する、インターフェイスあたりのバイト数。

Time Created

VPN 接続が作成された日時。

Time Last Used

ユーザが最後に VPN 接続を開始した時間。

NAT トラバーサル（NAT Traversal）

[はい（Yes）] が表示されている場合、ネットワーク アドレス変換を備えたデバイスの背後に少なくとも 1 つの VPN エンドポイントが存在します。

IKE 状態（IKE State）

IKE SA の状態（接続、確立、削除、または廃棄）。

IKE Event

IKE SA イベント（再認証、またはキー再生成）。

IKE Event Time

次のイベントが発生する時間（秒）。

IKE Algorithm

VPN 展開で使用されている IKE アルゴリズム。

IPSec 状態（IPSec State）

IPSec SA の状態（インストール中、インストール済み、更新中、キー再生成、削除、および廃棄）。

IPSec イベント（IPSec Event）

IPSec SA イベントがキーを再生成するタイミングの通知。

IPSec イベント時間（IPSec Event Time）

次のイベントが発生するまでの時間（秒）。

IPSec アルゴリズム（IPSec Algorithm）

VPN 展開で使用されている IPSec アルゴリズム。

関連トピック

VPN 統計情報およびログの表示 （1662 ページ）

VPN 統計情報およびログの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
該当なし	VPN	7000 & 8000 シリーズ	任意（Any）	Admin/Network Admin

マルチドメイン展開では、システムは現在のドメインで作成された VPN 展開を表示します。また、エンドポイントデバイスの1つがドメインに属している場合は、先祖ドメインで作成された VPN 展開も表示されます。下位のドメインで作成された VPN 展開を表示するには、そのドメインに切り替えます。

ステップ 1 **[Devices]** > **[VPN]** > **[Site to Site]**を選択します。

ステップ 2 統計情報を表示する展開の隣にある、VPN ステータス アイコンをクリックします。

ステップ 3 統計情報の表示アイコン（  ）をクリックします。

ステップ 4 オプションで、[更新（Refresh）] をクリックして、VPN の統計情報を更新することもできます。

ステップ 5 オプションで、[最新のログの表示（View Recent Log）] をクリックして、各エンドポイントの最新のデータ ログを表示することもできます。ハイ アベイラビリティ ペアの 7000 または 8000 シリーズ デバイスおよびスタック デバイスのログを表示するには、アクティブ/プライマリ、またはバックアップ/セカンダリのいずれかのデバイスへのリンクをクリックします。

第 XVI 部

アクセス コントロール

第 62 章

アクセス コントロール ポリシーの開始

ここでは、アクセス コントロール ポリシーの使用を開始する方法について説明します。

アクセス制御の概要

アクセス制御は、（非高速パスを通る）ネットワーク トラフィックの指定、検査、ロギングが可能な階層型ポリシーベースの機能です。アクセス コントロール ポリシーはネストすることができ、これはマルチドメイン展開で特に有用です。このポリシーでは各ポリシーが先祖（または基本）ポリシーからルールや設定を継承します。この継承を強制することもできますが、下位のポリシーによる先祖ポリシーの上書きを許可することもできます。各管理対象デバイスは 1 つのアクセス コントロール ポリシーのターゲットにすることができます。

ポリシーのターゲット デバイスがネットワーク トラフィックについて収集したデータは、以下に基づいてそのトラフィックのフィルタや制御に使用できます。

- トランスポート層およびネットワーク層の特定しやすい単純な特性（送信元と宛先、ポート、プロトコルなど）
- レピュテーション、リスク、ビジネスとの関連性、使用されたアプリケーション、または訪問した URL などの特性を含む、トラフィックに関する最新のコンテキスト情報
- レルム、ユーザ、ユーザ グループ、または ISE の属性
- カスタム セキュリティ グループ タグ（SGT）

- 暗号化されたトラフィックの特性（このトラフィックを復号してさらに分析することもできます）
- 暗号化されていないトラフィックまたは復号されたトラフィックに、禁止されているファイル、検出されたマルウェア、または侵入の試みが存在するかどうか

各タイプのトラフィックのインスペクションと制御は、最大限の柔軟性とパフォーマンスを引き出すために最も意味がある局面で実行されます。たとえば、レピュテーションベースのブラックリストはシンプルな送信元と宛先のデータを使用しているため、禁止されているトラフィックを初期の段階でブロックできます。これに対し、侵入およびエクスプロイトの検知とブロックは最終防衛ラインです。

展開のライセンスを取得せずにシステムを設定することはできますが、多くの機能では、展開する前に適切なライセンスを有効にする必要があります。また、一部の機能は、特定のデバイスモデルでのみ使用できます。サポートされていない機能は、警告アイコンおよび確認ダイアログ ボックスに示されます。

（注） システムがトラフィックに影響を与えるためには、ルーテッド、スイッチド、トランスペアレント インターフェイスまたはインライン インターフェイスのペアを使用して関連する設定を管理対象デバイスに展開する必要があります。場合によっては、タップ モードのインライン デバイスを含むパッシブに展開されたデバイスにインライン設定を展開することがシステムによって阻害されます。それ以外の場合、ポリシーは正常に展開されますが、パッシブに展開されたデバイスを使用してトラフィックのブロックや変更を試みると、予期しない結果になる可能性があります。ブロックされた接続はパッシブ展開で実際にはブロックされないため、システムにより、ブロックされた各接続に対し複数の接続開始イベントが報告される場合があります。

アクセス コントロール ポリシーのコンポーネント

新しく作成したアクセス コントロール ポリシーは、デフォルト アクションを使用して、すべてのトラフィックを処理するようにターゲット デバイスに指示します。

次のリストに、簡単なポリシーの作成後に変更可能な設定を示します。

（注） 現在のドメインで作成されたアクセス コントロール ポリシーのみ編集できます。また、先祖アクセス コントロール ポリシーによってロックされている設定は編集できません。

名前（Name）と説明（Description）

各アクセス コントロール ポリシーには一意の名前が必要です。説明は任意です。

継承設定（Inheritance Settings）

ポリシー継承により、アクセス コントロール ポリシーの階層を作成することができます。親（または基本）ポリシーは子孫のデフォルト設定を定義、実行します。これはマルチドメイン導入環境で特に有効です。

ポリシーの継承設定で基本ポリシーを選択できます。また、現在のポリシーで設定をロックすることで、子孫にも同じ設定を継承させることできます。ロック解除された設定については、子孫ポリシーによる上書きが可能です。

ポリシー割り当て

各アクセス コントロール ポリシーがそのポリシーを使用するデバイスを識別します。1つのデバイスに適用されるアクセス コントロール ポリシーは 1 つのみです。マルチドメイン導入環境では、1 ドメイン内のすべてのデバイスで同じ基本ポリシーを使用させることができます。

ルール（Rule）

アクセス コントロール ルールは、ネットワーク トラフィックをきめ細かく処理する方法を提供します。先祖ポリシーから継承したルールを含むアクセス コントロール ポリシーのルールには、1 から始まる番号が付いています。システムは、ルール番号の昇順で上から順に、アクセス コントロール ルールをトラフィックと照合します。

通常、システムは、ルールのすべての条件がトラフィックに一致する最初のアクセス コントロール ルールに従ってネットワーク トラフィックを処理します。条件は単純または複雑にできます。条件の使用は特定のライセンスによって異なります。

デフォルト アクション（Default Action）

デフォルトアクションは、他のアクセス制御設定で処理されないトラフィックをどのように処理し、ロギングするかを定義します。デフォルトアクションにより、追加のインスペクションなしですべてのトラフィックをブロックまたは信頼することができます。また、侵入およびディスカバリ データの有無についてトラフィックを検査することもできます。

アクセス コントロール ポリシーのデフォルト アクションは先祖ポリシーから継承することもできますが、継承を強制的に実施することはできません。

セキュリティ インテリジェンス（Security Intelligence）

セキュリティ インテリジェンスは、悪意のあるインターネット コンテンツに対する最初の防衛ラインです。この機能により、最新の IP アドレス、URL、ドメイン名レピュテーションインテリジェンスをもとに接続をブラックリストに登録（ブロック）することができます。重要なリソースへの継続的なアクセスを確保するために、ブラックリストはカスタム ホワイトリストで上書きできます。

HTTP 応答（HTTP Responses）

システムによりユーザの Web サイト リクエストがブロックされた場合、システム提供の汎用的な応答ページを表示するか、カスタム ページを表示させることができます。ユーザに警告するページを表示するものの、ユーザが最初に要求したサイトに進めるようにすることもできます。

ログ

アクセス コントロール ポリシー ロギングの設定を使用して、現在のアクセス コントロール ポリシーのデフォルトの syslog の宛先を設定できます。この設定は、syslog の宛先設定で組み込まれているルールおよびポリシーのカスタム設定で明示的にオーバーライドされない限り、アクセス コントロール ポリシーと、組み込まれているすべての SSL、プレフィルタ、および侵入のポリシーに適用されます。

アクセス コントロールの詳細オプション（Advanced Access Control Options）

通常、アクセス コントロール ポリシーの詳細設定を変更する必要はほとんど、あるいはまったくありません。多くの場合、デフォルト設定が適切です。詳細設定では、トラフィックの前処理、SSL インスペクション、ID、種々のパフォーマンス オプションなどを変更できます。

関連トピック

ルール管理：共通の特性 （463 ページ）

アクセス コントロール ポリシーのデフォルト アクション

単純なアクセス コントロール ポリシーでは、デフォルト アクションは、ターゲット デバイスがすべてのトラフィックをどう処理するかを指定します。より複雑なポリシーでは、デフォルト アクションは次のトラフィックを処理します。

- インテリジェント アプリケーション バイパスで信頼されないトラフィック
- セキュリティ インテリジェンスによってブラックリスト登録されていないトラフィック
- SSL インスペクションによってブロックされていないトラフィック（暗号化トラフィックのみ）
- ポリシー内のどのルールにも一致しないトラフィック（トラフィックの照合とロギングは行うが、処理または検査はしないモニタ ルールを除く）

アクセス コントロール ポリシーのデフォルト アクションにより、追加のインスペクションなしでトラフィックをブロックまたは信頼することができます。また、侵入およびディスカバリ データの有無についてトラフィックを検査することもできます。

（注） デフォルト アクションで処理されるトラフィックでは、ファイルまたはマルウェアのインスペクションを実行**できません**。デフォルト アクションで処理される接続のロギングは、初期設定では無効ですが、有効にすることもできます。

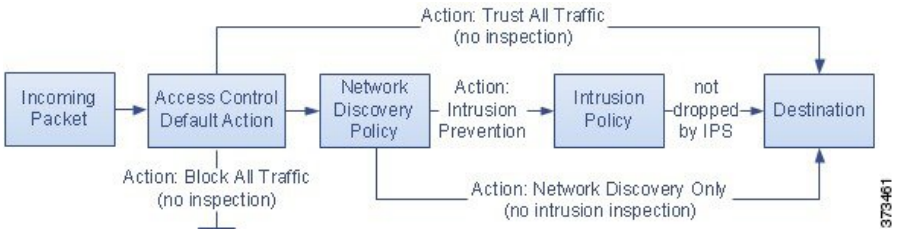
ポリシーを継承している場合、最下位の子孫のデフォルト アクションによってトラフィックの最終的な処理が決まります。アクセス コントロール ポリシーのデフォルト アクションは基本ポリシーから継承することもできますが、継承したデフォルト アクションを強制的に実施することはできません。

次の表に各デフォルトアクションが処理するトラフィックに対して実施可能なインスペクションの種類を示します。

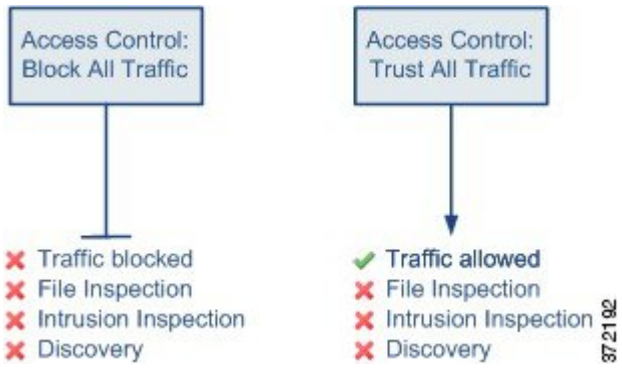
表 *107*: アクセス コントロール ポリシーのデフォルト アクション

デフォルト アクション	トラフィックに対して行う処理	インスペクションのタイプとポリシー
Access Control: Block All Traffic	それ以上のインスペクションは行わずにブロックする	なし
Access Control: Trust All Traffic	信頼（追加のインスペクションなしで最終宛先に許可）	なし
Intrusion Prevention	ユーザが指定した侵入ポリシーに合格する限り、許可する	侵入、指定した侵入ポリシーおよび関連する変数セットを使用、および 検出（discovery）、ネットワーク検出ポリシーを使用
ネットワーク検出のみ（Network Discovery Only）	許可（allow）	検出のみ（discovery only）、ネットワーク検出ポリシーを使用
基本ポリシーから継承	基本ポリシーで定義	基本ポリシーで定義

次の図は、表を図で表したものです。



次の図は、[すべてのトラフィックをブロック（Block All Traffic）]および[すべてのトラフィックを信頼（Trust All Traffic）] のデフォルト アクションを示しています。



次の図は、[侵入防御（Intrusion Prevention）]および[ネットワーク検出のみ（Network Discovery Only）] のデフォルト アクションを説明しています。

ヒント [Network Discovery Only] の目的は、検出のみの展開でパフォーマンスを向上させることです。侵入検知および防御のみを目的としている場合は、さまざまな設定でディスカバリを無効にできます。

関連トピック

限定的な導入のパフォーマンスに関する考慮事項 （460 ページ）
ポリシーのデフォルト アクションによる接続のロギング （3018 ページ）

アクセス コントロール ポリシーの継承

アクセス制御は階層型ポリシーベース実装となっています。ドメイン階層を作成するのと同様に、対応するアクセス コントロール ポリシーの階層を作成できます。子孫（あるいは子）アクセス コントロール ポリシーは、直接の親（あるいは基本）ポリシーからルールや設定を継承します。この基本ポリシーにもさらに親ポリシーがあり、その親ポリシーにもさらに、というようにルールや設定が継承されている場合もあります。

アクセス コントロール ポリシーのルールは、親ポリシーの [強制（Mandatory）] ルール セクションと [デフォルト（Default）] のルール セクションの間にネストされています。この実装により、先祖ポリシーの [強制（Mandatory）] ルールは実施される一方、先祖ポリシーの [デフォルト（Default）] ルールは現在のポリシーでプリエンプション処理することが可能です。

次の設定をロックすることで、すべての子孫ポリシーに設定を実行させることができます。ロック解除された設定については、子孫ポリシーによる上書きが可能です。

- セキュリティ インテリジェンス：IP アドレス、URL、ドメイン名の最新のレピュテーション インテリジェンスをもとに接続をブラックリストおよびホワイトリストに登録します。
- HTTP 応答ページ：ユーザの Web サイト リクエストをブロックした際、カスタム応答ページあるいはシステム提供の応答ページを表示します。
- 詳細設定：関連するサブポリシー、ネットワーク分析設定、パフォーマンス設定、その他の一般設定オプションを指定します。

アクセス コントロール ポリシーのデフォルト アクションは先祖ポリシーから継承することもできますが、継承を強制的に実施することはできません。

ポリシーの継承とマルチテナンシー

アクセス制御の階層型ポリシーベース実装はマルチテナンシーを補完します。

通常のマルチドメイン導入環境では、アクセス コントロール ポリシーの階層がドメイン構造に対応しており、管理対象デバイスに最下位レベルのアクセス コントロール ポリシーを適用します。この実装により、ドメインの上層レベルでは選択的にアクセス制御を実施しながらも、ドメインの下層レベルの管理者は展開ごとに設定を調整することが可能です（子孫ドメインの管理者を制限するには、ポリシー継承と適用だけでなく、ロールによる制限を行う必要があります）。

たとえば、所属している部門のグローバル ドメイン管理者は、グローバル レベルのアクセス コントロール ポリシーを作成できます。そして、そのグローバル レベルのポリシーを基本ポリシーとして、機能別にサブドメインに分けられたすべてのデバイスで使用するよう要求することがことが可能です。

サブドメインの管理者が Firepower Management Center にログインしてアクセス制御を設定する際、グローバル レベルのポリシーはそのまま展開できます。あるいは、グローバル レベルのポリシーの範囲内の子孫アクセス コントロール ポリシーを作成、展開することも可能です。

（注） アクセス制御の継承および適用が最も有効に実装されるのは、マルチテナンシーを補完する場合ですが、1 つのドメイン内においてもアクセス制御ポリシーを階層化することが可能です。また、任意のレベルでアクセス コントロール ポリシーを割り当て、展開することもできます。

関連トピック

アクセス コントロール ポリシーの継承の管理 （1676 ページ）
セキュリティ インテリジェンス ブラックリスト （1741 ページ）
HTTP 応答ページとインタラクティブなブロッキング （1735 ページ）
アクセス コントロール ポリシーの詳細設定 （1681 ページ）
アクセス コントロール ポリシーのロギング設定 （1681 ページ）

アクセス コントロール ポリシーの管理

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin Access Admin Network Admin

Firepower システムでは、システム付属のアクセス コントロール ポリシーの編集と、カスタム アクセス コントロール ポリシーの作成が可能です。デバイスの初期設定に応じて、システム付属のポリシーには次のものが含まれます。

- デフォルト アクセス制御：詳細な検査なしで、すべてのトラフィックをブロックします。
- デフォルト侵入防御：すべてのトラフィックを許可しますが、Balanced Security and Connectivity 侵入ポリシーおよびデフォルトの侵入変数セットを使用して検査も実行します。
- デフォルト ネットワーク検出：すべてのトラフィックを許可すると同時に検出データについて検査しますが、侵入やエクスプロイトについては検査しません。

マルチドメイン展開では、編集できる現在のドメインで作成されたポリシーが表示されます。また、編集できない先祖ドメインで作成されたポリシーも表示されます。下位のドメインで作成されたポリシーを表示および編集するには、そのドメインに切り替えます。

ステップ 1 **[Policies]** > **[Access Control]** を選択します。

ステップ 2 アクセス コントロール ポリシーを管理します。

- コピー：コピー アイコン（  ）をクリックします。
- 作成：[新規ポリシー（New Policy）] をクリックします。基本的なアクセス コントロール ポリシーの作成 （1673 ページ）を参照してください。
- 削除：削除アイコン（  ）をクリックします。
- 展開：[展開（Deploy）] をクリックします（設定変更の展開 （447 ページ） を参照）。
- 編集：編集アイコン（  ）をクリックします。アクセス コントロール ポリシーの編集 （1674 ページ）を参照してください。
- 継承：子孫を持つポリシーの横にあるプラスアイコン（  ）をクリックすると、ポリシーの階層ビューが展開されます。
- インポート/エクスポート：[インポート/エクスポート（Import/Export）] をクリックします。コンフィギュレーションのインポートとエクスポート （229 ページ）を参照してください。
- [レポート（Report）]：レポート アイコン（  ）をクリックします（現在のポリシー レポートの生成 （459 ページ） を参照）。

関連トピック

失効ポリシー （459 ページ）

基本的なアクセス コントロール ポリシーの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Access Admin/Network Admin

新規アクセス コントロール ポリシーを作成する場合は、少なくとも、デフォルト アクションを選択する必要があります。

ほとんどの場合、デフォルトアクションにより処理される接続のロギングは最初は無効になっています。例外は、マルチドメイン導入でサブポリシーを作成する場合です。この場合、継承されたデフォルト アクションのロギング設定に応じて、接続のロギングが有効になります。

ステップ 1 **[Policies]** > **[Access Control]** を選択します。

ステップ 2 [新しいポリシー（New Policy）] をクリックします。

ステップ 3 [名前（Name）] に一意の名前を入力し、オプションで [説明（Description）] を入力します。

ステップ 4 オプションで、[基本ポリシーの選択（Select Base Policy）] ドロップダウンリストから基本ポリシーを選択します。

ドメインにアクセス コントロール ポリシーが適用されている場合は、この手順はオプションではありません。適用されているポリシーまたはその子孫のいずれかを基本ポリシーとして選択する必要があります。

ステップ 5 初期デフォルト アクションを指定します。

- 基本ポリシーを選択すると、新しいポリシーではそのデフォルト アクションが継承されます。ここで変更することはできません。
- [すべてのトラフィックをブロック（Block All Traffic）] を選択すると、[アクセス コントロール：すべてのトラフィックをブロック（Access Control: Block All Traffic）] をデフォルト アクションとするポリシーが作成されます。
- [侵入防御（Intrusion Prevention）] を選択すると、[侵入防御：セキュリティと接続性のバランス（Intrusion Prevention: Balanced Security and Connectivity）] をデフォルト アクションとし、デフォルトの侵入変数セットが関連付けられたポリシーが作成されます。
- [ネットワーク検出（Network Discovery）] を選択すると、[ネットワーク検出のみ（Network Discovery Only）] をデフォルト アクションとするポリシーが作成されます。

ヒント デフォルトですべてのトラフィックを信頼するか、基本ポリシーを選択しデフォルトアクションは継承しないようにする場合は、後でデフォルト アクションを変更できます。

ステップ 6 必要に応じて、ポリシーを展開する [使用可能なデバイス（Available Devices）] を選択し、[ポリシーに追加（Add to Policy）] をクリック（またはドラッグ アンド ドロップ）して、選択したデバイスを追加します。表示されるデバイスを絞り込むには、[検索（Search）] フィールドに検索文字列を入力します。

このポリシーをすぐに展開するには、この手順を実行する必要があります。

ステップ 7 [保存（Save）] をクリックします。

次のタスク

- 必要に応じて、アクセス コントロール ポリシーの編集（1674 ページ）の説明に従って、さらに新しいポリシーを設定します。
- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

関連トピック

アクセス コントロール ポリシーのデフォルト アクション （1668 ページ）
アクセス コントロール ポリシーのターゲット デバイスの設定 （1680 ページ）

アクセス コントロール ポリシーの編集

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Access Admin/Network Admin

ポリシーの編集は、1 つのブラウザ ウィンドウを使用して、一度に 1 人のみで行う必要があります。複数のユーザが同じポリシーを保存した場合は、最後に保存された変更が保持されます。ユーザにとっての便宜性を考慮して、各ポリシーを現在編集している人（いる場合）の情報が表示されます。セッションのプライバシーを保護するために、ポリシー エディタが非アクティブになってから 30 分後に警告が表示されます。60 分後には、システムにより変更が破棄されます。

ステップ 1 **[Policies]** > **[Access Control]** を選択します。

ステップ 2 編集するアクセス コントロール ポリシーの横にある編集アイコン（  ）をクリックします。

代わりに表示アイコン（  ）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 アクセス コントロール ポリシーを編集します。

- 名前と説明：いずれかのフィールドをクリックし、新しい情報を入力します。
- デフォルト アクション：[デフォルト アクション（Default Action）] ドロップダウン リストから値を選択します。

- デフォルトアクションの変数セット：[侵入防御（Intrusion Prevention）] のデフォルトアクションに関連付けられている変数セットを変更するには、変数アイコン（  ）をクリックします。表示されるポップアップ ウィンドウで、新しい変数セットを選択して [OK] をクリックします。また、編集アイコン（  ）をクリックして、選択した変数セットを新しいウィンドウで編集することもできます。詳細については、変数の管理 （554 ページ）を参照してください。
- デフォルトアクションのロギング：デフォルトアクションで処理される接続のロギングを設定するには、ロギング アイコン（  ）をクリックします。ポリシーのデフォルト アクションによる接続のロギング （3018 ページ）を参照してください。
- HTTP 応答：システムが Web サイトの要求をブロックする際にブラウザに表示される情報を指定するには、[HTTP 応答（HTTP Responses）] タブをクリックします。HTTP 応答ページの選択 （1737 ページ）を参照してください。
- 継承：基本ポリシーの変更：このポリシーの基本アクセス コントロール ポリシーを変更するには、[継承設定（Inheritance Settings）] をクリックします。基本アクセス コントロール ポリシーの選択 （1677 ページ）を参照してください。
- 継承：子孫での設定のロック：このポリシーの設定を子孫ポリシーに適用するには、[継承設定（Inheritance Settings）] をクリックします。子孫アクセス コントロール ポリシーのロックの設定 （1678 ページ）を参照してください。
- ポリシー割り当て：ターゲット：このポリシーの対象となっている管理対象デバイスを特定するには、[ポリシー割り当て（Policy Assignment）] をクリックします。アクセス コントロール ポリシーのターゲット デバイスの設定 （1680 ページ）を参照してください。
- ポリシー割り当て：ドメインで必須：このポリシーをサブドメインに適用するには、[ポリシー割り当て（Policy Assignment）] をクリックします。ドメインでのアクセス コントロール ポリシーの強制 （1679 ページ）を参照してください。
- ルール：アクセス コントロール ルールを管理し、侵入とファイル ポリシーを使用して悪意のあるトラフィックを検査およびブロックするには、[ルール（Rules）] タブをクリックします。アクセス コントロール ルールの作成および編集 （1698 ページ）を参照してください。
- ルールの競合：ルールの競合の警告を表示するには、[ルールの競合の表示（Show rule conflicts）] を有効にします。ルールの競合は、より古いルールが先にトラフィックに一致することが原因で、ルールがトラフィックに一致することがない場合に発生します。ルールの競合を判別するには多くのリソースを消費するため、それらを表示するには時間がかかることがあります。詳細については、ルールの順序指定のガイドライン （503 ページ）を参照してください。
- セキュリティ インテリジェンス：最新のレピュテーション インテリジェンスに基づいてすぐに接続をブラックリストに載せる（ブロックする）には、[セキュリティ インテリジェンス（Security Intelligence）] タブをクリックします。セキュリティ インテリジェンスの設定 （1744 ページ）を参照してください。
- 詳細オプション：前処理、SSL インスペクション、アイデンティティ、パフォーマンス、およびその他の詳細オプションを設定するには、[詳細（Advanced）] タブをクリックします。アクセス コントロール ポリシーの詳細設定 （1681 ページ）を参照してください。

- 警告：アクセス コントロール ポリシー（およびその子孫ポリシーと関連ポリシー）の警告またはエラーのリストを表示するには、[警告の表示（Show Warnings）] をクリックします。警告とエラーによって、トラフィック分析やフローに悪影響を及ぼしたり、ポリシーの展開を妨げたりする構成がマークされます。警告がない場合、ボタンは表示されません。ルールの競合の警告を表示するには、まず、[ルールの競合の表示（Show rule conflicts）] を有効にします。

ステップ 4 **[保存（Save）]** をクリックします。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

関連トピック

ルールとその他のポリシーの警告 （501 ページ）
ディープ インスペクションについて （1707 ページ）

アクセス コントロール ポリシーの継承の管理

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Access Admin/Network Admin

ステップ 1 変更する継承設定を持つアクセス コントロール ポリシーを編集します。アクセス コントロール ポリシーの編集 （1674 ページ）を参照してください。

ステップ 2 ポリシーの継承を管理します。

- 基本ポリシーの変更：このポリシーの基本アクセス コントロール ポリシーを変更するには、[継承設定（Inheritance Settings）] をクリックして、基本アクセス コントロール ポリシーの選択 （1677 ページ）で説明する手順を実行します。
- 子孫の設定のロック：このポリシーの設定を子孫ポリシーで強制適用するには、[継承設定（Inheritance Settings）] をクリックして、子孫アクセス コントロール ポリシーのロックの設定 （1678 ページ）で説明する手順を実行します。
- ドメインで必須：このポリシーをサブドメインで強制適用するには、[ポリシーの割り当て（Policy Assignment）] をクリックして、ドメインでのアクセス コントロール ポリシーの強制 （1679 ページ）で説明する手順を実行します。
- 基本ポリシーからの設定の継承：基本アクセス コントロール ポリシーから設定を継承するには、[セキュリティ インテリジェンス（Security Intelligence）] タブ、[HTTP 応答（HTTP Responses）] タブ、

または[詳細（Advanced）]タブをクリックして、基本ポリシーからのアクセス コントロール ポリシー設定の継承 （1677 ページ）で説明する手順を実行します。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

基本アクセス コントロール ポリシーの選択

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Access Admin/Network Admin

1 つのアクセス コントロール ポリシーを別の基本（親）として使用できます。デフォルトでは、子のポリシーが基本ポリシーから設定を継承します。ロック解除された設定を変更することも可能です。

既存のアクセス コントロール ポリシーの基本ポリシーを変更すると、システムで現在のポリシー設定が新しい基本ポリシーの任意のロックされた設定に更新されます。

ステップ 1 アクセス コントロール ポリシーのエディタで、[継承設定（Inheritance Settings）] をクリックします。

ステップ 2 [基本ポリシーの選択（Select Base Policy）] ドロップダウンリストからポリシーを選択します。

マルチドメイン展開では、アクセス コントロール ポリシーが既存のドメインで必要になることがあります。基本ポリシーとして、強制ポリシーまたはその子孫ポリシーの一つを選択できます。

ステップ 3 **[保存（Save）]** をクリックします。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

基本ポリシーからのアクセス コントロール ポリシー設定の継承

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Access Admin/Network Admin

新しい子ポリシーは、基本ポリシーから多数の設定を継承します。これらの設定は、基本ポリシーでロックされていない場合はオーバーライドできます。

基本ポリシーから後で設定を再継承すると、システムによって基本ポリシーの設定が表示され、コントロールが淡色表示されます。ただし、オーバーライドした内容はシステムによって保存され、その内容は継承を再度無効にすると復元されます。

ステップ 1 アクセス コントロール ポリシー エディタで、[セキュリティ インテリジェンス（Security Intelligence）] タブ、[HTTP 応答（HTTP Responses）] タブまたは [詳細（Advanced）] タブをクリックします。

ステップ 2 継承する設定ごとに、[基本ポリシーから継承（Inherit from base policy）] チェックボックスをオンにします。

コントロールが淡色表示されている場合、設定は先祖ポリシーから継承され、設定を変更する権限がありません。

ステップ 3 **[保存（Save）]** をクリックします。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

子孫アクセス コントロール ポリシーのロックの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Access Admin/Network Admin

アクセス コントロール ポリシーの設定をロックして、すべての子孫ポリシーで設定を適用します。子孫ポリシーでは、ロックされていない設定をオーバーライドできます。

設定をロックするときに、すでに子孫ポリシーで実行されていたオーバーライドを保存して、設定のロックを再度解除したときにオーバーライドを復元できるようにします。

ステップ 1 アクセス コントロール ポリシー エディタで、[設定の継承（Inheritance Settings）] をクリックします。

ステップ 2 [子ポリシーの継承設定（Child Policy Inheritance Settings）] 領域で、ロックする設定をオンにします。

コントロールが淡色表示されている場合、設定は先祖ポリシーから継承され、設定を変更する権限がありません。

ステップ 3 [OK] をクリックして継承設定を保存します。

ステップ 4 [保存（Save）] をクリックして、アクセス コントロール ポリシーを保存します。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

ドメインでのアクセス コントロール ポリシーの強制

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Access Admin/Network Admin

ドメイン内の各デバイスが同一の基本アクセス コントロール ポリシーまたは、そのポリシーの子孫ポリシーの 1 つを使用するように強制できます。

始める前に

- 少なくとも 1 つのグローバル ドメイン以外のドメインを設定します。

ステップ 1 アクセス コントロール ポリシー エディタで、[ポリシーの割り当て（Policy Assignments）] をクリックします。

ステップ 2 [ドメインに強制（Required on Domains）] タブをクリックします。

ステップ 3 ドメイン リストを作成します。

- 追加：現在のアクセス コントロール ポリシーを強制適用するドメインを選択して [追加（Add）] をクリックするか、選択したドメインのリストにドラッグ アンド ドロップします。
- 削除：リーフ ドメインの横にある削除アイコン（）をクリックするか、先祖ドメインを右クリックして [選択項目の削除（Delete Selected）] を選択します。
- 検索：検索フィールドに検索文字列を入力します。クリア アイコン（）をクリックして、検索をクリアします。

ステップ 4 [OK] をクリックしてドメインに強制適用する設定を保存します。

ステップ 5 [保存（Save）] をクリックして、アクセス コントロール ポリシーを保存します。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

アクセス コントロール ポリシーのターゲット デバイスの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Access Admin/Network Admin

アクセス コントロール ポリシーは、それを使用するデバイスを指定します。それぞれのデバイスは、1つのアクセス コントロール ポリシーのみのターゲットに設定できます。マルチドメイン展開では、ドメイン内のすべてのデバイスが同一の基本ポリシーを使用するように強制できます。

ステップ 1 アクセス コントロール ポリシー エディタで、[ポリシーの割り当て（Policy Assignments）] をクリックします。

ステップ 2 [ターゲット デバイス（Targeted Devices）] タブで、ターゲット リストを作成します。

- 追加：1 つ以上の [使用可能なデバイス（Available Devices）] を選択して、[ポリシーに追加（Add to Policy）] をクリックするか、[選択したデバイス（Selected Devices）] のリストにドラッグ アンド ドロップします。
- 削除：1つのデバイスの横にある削除アイコン（）をクリックするか、複数のデバイスを選択して、右クリックしてから [選択済み項目の削除（Delete Selected）] を選択します。
- 検索：検索フィールドに検索文字列を入力します。クリアアイコン（）をクリックして、検索をクリアします。

[影響を受けるデバイス（Impacted Devices）] の下に、割り当てられたアクセス コントロール ポリシーが現在のポリシーの子であるデバイスが一覧表示されます。現在のポリシーを変更すると、これらのデバイスに影響します。

ステップ 3 必要に応じて、[ドメインで強制（Required on Domains）] タブをクリックして、選択したサブドメイン内のすべてのデバイスが同じ基本ポリシーを使用するように強制します。ドメインでのアクセス コントロール ポリシーの強制 （1679 ページ）を参照してください。

ステップ 4 [OK] をクリックしてターゲット デバイス設定を保存します。

ステップ 5 [保存（Save）] をクリックして、アクセス コントロール ポリシーを保存します。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

アクセス コントロール ポリシーのロギング設定

アクセス コントロール ポリシー ロギングの設定を使用して、現在のアクセス コントロール ポリシーのデフォルトの syslog の宛先と syslog アラートを設定できます。この設定は、syslog の宛先設定で組み込まれているルールおよびポリシーのカスタム設定で明示的にオーバーライドされない限り、アクセス コントロール ポリシーと、組み込まれているすべての SSL、プレフィルタ、および侵入のポリシーに適用されます。

デフォルト Syslog 設定

[特定の syslog アラートを使用して送信する（Send using specific syslog alert）]：このオプションを選択すると、Syslog アラート応答の作成（2810 ページ）の手順を使用して設定したとおりに、選択した syslog アラートに基づいてイベントが送信されます。リストから syslog アラートを選択するか、名前、ロギング ホスト、ポート、機能および重大度を指定することにより syslog アラートを追加できます。詳細については、侵入 syslog アラートの重大度（2821 ページ）を参照してください。このオプションはすべてのデバイスに適用されます。

[FTD 6.3 以降：デバイスに展開されている FTD プラットフォーム設定のポリシーで設定されている syslog 設定を使用（FTD 6.3 and later: Use the syslog settings configured in the FTD Platform Settings policy deployed on the device）]：このオプションを選択し、重大度を選択すると、接続イベントまたは侵入イベントが選択した重大度で [プラットフォーム設定（Platform Settings）] で設定した syslog コレクタに送信されます。このオプションを使用し、[プラットフォーム設定（Platform Settings）] で行った syslog 設定を統合して、アクセス コントロール ポリシーでその設定を再利用できます。このセクションで選択した重大度はすべての接続イベントと侵入イベントに適用されます。デフォルトの重大度は ALERT です。

このオプションは、Firepower Threat Defense デバイス 6.3 以降のみに適用されます。

（注） 両方のオプションを選択すると、オプションの動作が変更されます。[ダイナミック サマリ（Dynamic Summary）] セクションに、選択の結果が表示されます。

[ファイルおよびマルウェアの設定（File and Malware Settings）] は通常、syslog メッセージの送信についてページの上部のオプションを選択した後に有効になります。

アクセス コントロール ポリシーの詳細設定

通常、アクセス コントロール ポリシーの詳細設定を変更する必要はほとんど、あるいはまったくありません。デフォルト設定は、ほとんどの展開環境に適しています。侵入ルールの更新（185 ページ）で説明しているように、アクセス コントロール ポリシーの前処理およびパフォーマンスの詳細オプションの多くは、ルールの更新によって変更される可能性があることに注意してください。

代わりに表示アイコン（）が表示される場合、設定は先祖ポリシーから継承され、設定を変更する権限がありません。 設定がロック解除されている場合は、[Inherit from base policy] をオフにして、編集を有効にします。

注意 Snort プロセスを再起動し、トラフィック インスペクションを一時的に中断する詳細設定変更のリストについては、展開またはアクティブ化された際に Snort プロセスを再起動する設定 （454 ページ） を参照してください。 この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、ターゲットデバイスがトラフィックを処理する方法に応じて異なります。詳細はSnort® の再起動によるトラフィックの動作 （451 ページ） を参照してください。

全般設定

ユーザが要求した各 URL に対して保存する文字数をカスタマイズするには、長い URL のロギングの制限 （3020 ページ） を参照してください。

ユーザが最初のブロックをバイパスした後に Web サイトを再度ブロックするまでの時間間隔をカスタマイズするには、ブロックされた Web サイトのユーザ バイパス タイムアウトの設定 （1739 ページ） を参照してください。

[URL キャッシュ ミス ルックアップを再試行する（Retry URL cache miss lookup）] を無効にすると、カテゴリがキャッシュされない場合には、クラウドルックアップを使用せずに、すぐにトラフィックが URL に渡されるようにすることができます。クラウドルックアップで別のカテゴリが用意されるまで、クラウドルックアップを必要とする URL は未分類の URL として処理されます。パッシブ展開では、システムはルックアップを再試行しません。これは、システムがパケットを保持できないからです。

[Enable Threat Intelligence Director] を無効にすると、設定したデバイスへの TID データの公開が停止されます。TID の詳細については、Cisco Threat Intelligence Director（TID） （1967 ページ） を参照してください。

特定の設定で Snort プロセスを再起動する必要がない限り設定の変更を展開する場合にトラフィックを検査するには、必ず、[ポリシーの適用時にトラフィックを検査する（Inspect traffic during policy apply）] がデフォルト値（有効）に設定してください。このオプションを有効にすると、リソースの需要が高まった場合にいくつかのパケットが検査なしでドロップされることがあります。また、一部のコンフィギュレーションを展開すると、トラフィックのインスペクションを中断する Snort プロセスが再開します。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、ターゲットデバイスがトラフィックを処理する方法に応じて異なります。詳細については、Snort® の再起動シナリオ （450 ページ） を参照してください。

関連するポリシー

詳細設定を使用して、サブポリシー（SSL、ID、プレフィルタ）をアクセス制御に関連付けます。アクセス制御への他のポリシーの関連付け （1684 ページ） を参照してください。

ネットワーク分析ポリシーと侵入ポリシー

ネットワーク分析ポリシーおよび侵入ポリシーの詳細設定によって、以下が可能になります。

- システムがトラフィックを検査する方法を正確に決定する前に、最初にそのトラフィックを検査するために使用される、アクセス コントロール ポリシーのデフォルトの侵入ポリシーと関連付けられている変数セットの変更。
- 多くの前処理オプションを制御する、アクセス コントロール ポリシーのデフォルト ネットワーク分析ポリシーの変更。
- カスタム ネットワーク分析ルールおよびネットワーク分析ポリシーを使用した、特定のセキュリティ ゾーン、ネットワーク、および VLAN に対する前処理オプションの調整。

詳細については、ネットワーク分析/侵入ポリシーのための高度なアクセス制御の設定 （2287 ページ）を参照してください。

Threat Defense サービス ポリシー

Threat Defense サービス ポリシーを使用して、特定のトラフィック クラスにサービスを適用することができます。たとえば、サービス ポリシーを使用すると、すべての TCP アプリケーションに適用されるタイムアウト コンフィギュレーションではなく、特定の TCP アプリケーションに固有のタイムアウト コンフィギュレーションを作成できます。このポリシーは Firepower Threat Defense デバイスのみに適用され、その他のデバイス タイプの場合には無視されます。このサービス ポリシー ルールは、アクセス制御ルールの後に適用されます。詳細については、Threat Defense サービス ポリシー （1179 ページ）を参照してください。

ファイルおよびマルウェアの設定

ファイルとマルウェアのインスペクション パフォーマンスとストレージの調整 （1961 ページ）に、ファイル制御と ネットワーク向け AMP のパフォーマンス オプションに関する情報が記載されています。

インテリジェント アプリケーション バイパスの設定

インテリジェント アプリケーション バイパス（IAB）は、トラフィックがインスペクション パフォーマンスとフローしきい値の組み合わせを超過したときにバイパスするアプリケーションを指定する、または、バイパスに関するテストを行うための、エキスパート レベルの設定です。詳細については、インテリジェント アプリケーション バイパス （1783 ページ）を参照してください。

トランスポート層とネットワーク層のプリプロセッサの設定

トランスポート/ネットワーク プリプロセッサの詳細設定は、アクセス コントロール ポリシーを展開するすべてのネットワーク、ゾーン、VLAN にグローバルに適用されます。これらの詳細設定は、ネットワーク分析ポリシーではなくアクセス コントロール ポリシーで設定します。詳細については、トランスポート/ネットワーク プリプロセッサの詳細設定 （2398 ページ）を参照してください。

検出拡張の設定

検出拡張の詳細設定では、次のことを実行できるようにアダプティブプロファイルを設定することができます。

- アクセス コントロール ルールでファイル ポリシーとアプリケーションを使用する。
- 侵入ルールでサービス メタデータを使用する。
- パッシブ展開で、ネットワークのホスト オペレーティング システムに基づいてパケット フラグメントと TCP ストリームのリアセンブルを向上させる。

詳細については、適応型プロファイル （2463 ページ）を参照してください。

パフォーマンス設定および遅延ベースのパフォーマンス設定

侵入防御のパフォーマンスチューニングについて （2271 ページ）では、侵入行為についてトラフィックを分析する際のシステムのパフォーマンスを向上させるための情報を提供しています。

遅延ベースのパフォーマンス設定固有の情報については、パケットおよび侵入ルールの遅延しきい値構成 （2276 ページ）を参照してください。

アクセス制御への他のポリシーの関連付け

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	機能に応じて異なる	機能に応じて異なる	いずれか（Any）	Admin/Access Admin/Network Admin

次のサブポリシーのいずれかとアクセス コントロール ポリシーとを関連付けるには、アクセス コントロール ポリシーの詳細設定を使用します。

- SSL ポリシー：セキュア ソケット レイヤ（SSL）または Transport Layer Security（TLS）で暗号化されたアプリケーション層プロトコル トラフィックをモニタ、復号化、ブロック、または許可します。

注意 SSL ポリシーを追加または削除すると設定の変更を展開する際に Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、ターゲット デバイスがトラフィックを処理する方法に応じて異なります。詳細はSnort® の再起動によるトラフィックの動作 （451 ページ）を参照してください。

- アイデンティティ ポリシー：トラフィックに関連付けられているレルムと認証方式に基づいて、ユーザ認証を実行します。
- プレフィルタ ポリシー：（レイヤ4の）アウターヘッダによりネットワーク限定を使用した早期のトラフィック処理を実行します。

ステップ 1 アクセス コントロール ポリシー エディタで、[詳細（Advanced）] タブをクリックします。

ステップ 2 適切な [ポリシー設定（Policy Settings）] 領域の編集アイコン（  ）をクリックします。

代わりに表示アイコン（  ）が表示される場合、設定は先祖ポリシーから継承され、設定を変更する権限がありません。 設定がロック解除されている場合は、[Inherit from base policy] をオフにして、編集を有効にします。

ステップ 3 ドロップダウン リストからポリシーを選択します。

ユーザが作成したポリシーを選択する場合は、表示される編集アイコンをクリックしてポリシーを編集できます。

ステップ 4 [OK] をクリックします。

ステップ 5 [保存（Save）] をクリックして、アクセス コントロール ポリシーを保存します。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

関連トピック

Snort® の再起動シナリオ （450 ページ）

ポリシー ヒット カウントの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	Firepower Threat Defense	任意（Any）	管理/アクセス Admin/Network Admin

ヒット カウントは、一致する接続に対してポリシー ルールがトリガーされた回数を示します。この情報を使用してルールの有効性を特定することができます。ヒット カウント情報は、アクセス制御とプレフィルタ ルールに対してのみ使用できます。サポート対象のポリシーの場合、ポリシーに設定されているデフォルト アクションのヒットカウント情報も表示されます。

（注）
- Firepower Threat Defense デバイスを再起動すると、すべてのヒット カウント情報がリセットされます。
- デバイスで展開またはタスクが進行中の場合、デバイスからヒット カウント情報を取得することはできません。

ステップ 1 アクセス制御またはプレフィルタ ポリシーのページに移動します。

ステップ 2 ヒット カウント情報を表示するポリシーをクリックします。

ステップ 3 ポリシーのページで、そのページの右上にある [ヒット カウントの分析（Analyze Hit Counts）] ボタンをクリックします。

ステップ 4 [ヒット カウント（Hit Count）] ページで、[デバイスの選択（Select a device）] ドロップダウン リストからデバイスを選択します。

（注） このデバイスのヒット カウントを生成するのが初めてではない場合は、ドロップダウン ボックスの横に最後に取得したヒット カウント情報が表示されます。また、[最終展開（Last Deployed）] の時刻を確認して、最新のポリシー変更を確認します。

ステップ 5 ヒット カウント データを取得するには、[現在のヒット カウントの取得（Fetch Current Hit Count）] ボタンをクリックします。

選択したデバイスのヒット カウント情報にアクセスしようとしたのが初めてではない場合、[現在のヒット カウントの取得（Fetch Current Hit Count）] ではなく、[更新（Refresh）] ボタンが表示されます。最新のヒット カウント情報を取得するには、[更新（Refresh）] ボタンをクリックします。

ステップ 6 （オプション）テーブルとテーブル内のリストをカスタマイズするには、[ルール/ポリシーのフィルタ処理（Filter Rules/Policy）] ボックスか、または [フィルタ条件（Filter by）] と [過去（In Last）] ドロップダウン ボックスおよび設定アイコン（⚙）を使用します。

ステップ 7 （オプション）ルール名をクリックして編集するか、最後の列の表示アイコン（🔍）をクリックしてルールの詳細を表示します。

ルール名をクリックすると、ポリシー ページ内でその名前がハイライトされ、編集できるようになります。

（注） [アクセスコントロールポリシー（Access Control Policy）] ページから [ヒットカウント（Hit Count）] ページにアクセスした場合、プレフィルタ ルールを表示または編集することはできません。また、その逆も同様です。

ステップ 8 （オプション）ルールを右クリックし、[ヒット カウントのクリア（Clear Hit Count）] を選択してルールのヒット カウント情報をクリアします。

複数のルールのヒット カウント情報をクリアするには、**Ctrl** ボタンを使用してルールを選択し、選択したルールのいずれかを右クリックした後に [ヒットカウントのクリア（Clear Hit Count）] を選択します。

（注） ヒット カウント情報をクリアすると、ヒット カウントが元のゼロに設定されます。

ステップ 9 （オプション）ページの左下にある [Generate CSV] ボタンをクリックして、詳細情報の CSV レポートをページ上で生成します。

ステップ 10 [閉じる（Close）] をクリックしてポリシー ページに戻ります。

第 63 章

アクセス コントロール ルール

次の各トピックでは、アクセス コントロール ルールの設定方法について説明します。

アクセス コントロール ルールの概要

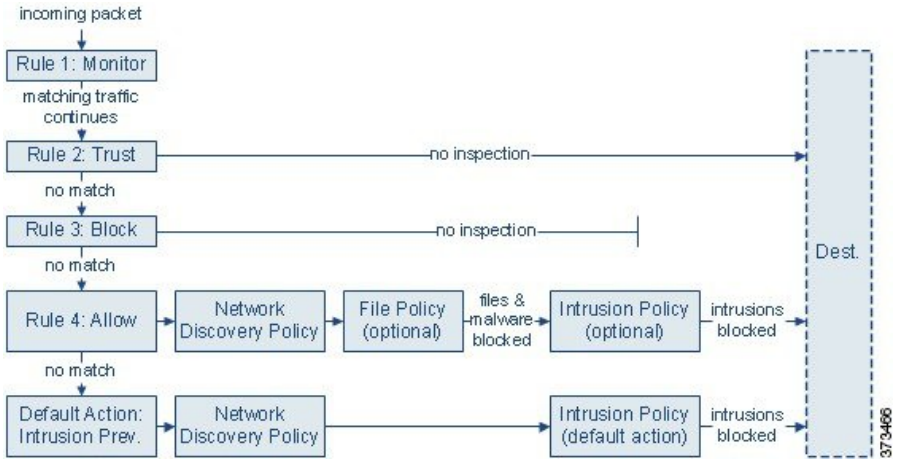
アクセス コントロール ポリシー内では、アクセス コントロール ルールによって複数の管理対象デバイスでネットワーク トラフィックを処理するきめ細かい制御方法が提供されます。

（注） アクセス コントロール ルールがネットワーク トラフィックを評価する前に、プレフィルタ評価/8000 シリーズ高速パス、セキュリティ インテリジェンスのフィルタリング、SSL インスペクション、ユーザの識別、および一部の復号と前処理が発生します。

システムは、指定した順にアクセス コントロール ルールをトラフィックと照合します。ほとんどの場合、システムは、すべてのルールの条件がトラフィックに一致する場合、最初のアクセス コントロール ルールに従ってネットワーク トラフィックを処理します。

また、各ルールにはアクションがあり、これによって一致するトラフィックをモニタ、信頼、ブロック、または許可するかを決定します。トラフィックを許可するときは、システムが侵入ポリシーまたはファイル ポリシーを使用してトラフィックを最初に検査し、アセットに到達したりネットワークを出る前に、エクスプロイト、マルウェア、または禁止されたファイルをブロックするように指定できます。

次のシナリオでは、インラインの侵入防御展開環境で、アクセス コントロール ルールによってトラフィックを評価できる方法を要約しています。



このシナリオでは、トラフィックは次のように評価されます。

- **ルール 1**：**モニタ**はトラフィックを最初に評価します。モニタルールはネットワークトラフィックを追跡してログに記録します。システムはトラフィックと追加ルールの照合を継続して、許可するか拒否するかを決定します（ただし、重要な例外と注意事項をアクセス コントロール ルールのモニタ アクション （1701 ページ）で確認してください）。
- **ルール 2**：**信頼**はトラフィックを 2 番目に評価します。一致するトラフィックは追加のインスペクションなしで宛先まで通過することが許可されますが、引き続きアイデンティティの要件とレート制限の対象となります。一致しなかったトラフィックは、次のルールへと進められます。
- **ルール 3**：**ブロック**はトラフィックを 3 番目に評価します。一致したトラフィックは、それ以上のインスペクションは行わずに、ブロックされます。一致しないトラフィックは、引き続き最後のルールと照合されます。
- **ルール 4**：**許可**は最後のルールです。このルールの場合、一致するトラフィックは許可されますが、そのトラフィック内の禁止されたファイル、マルウェア、侵入およびエクスプロイトは検出されてブロックされます。残りの禁止されていない悪意のないトラフィックは宛先まで通過することが許可されますが、引き続きアイデンティティの要件とレート制限の対象となります。ファイルインスペクションのみを実行する、または侵入インスペクションのみを実行する、もしくは両方とも実行しない許可ルールを設定できます。
- **デフォルト アクション**はルールのいずれにも一致しないすべてのトラフィックを処理します。このシナリオでは、デフォルトアクションは、悪意のないトラフィックの通過を許可する前に侵入防御を実行します。別の展開では、追加のインスペクションなしですべてのトラフィックを信頼またはブロックするデフォルト アクションが存在する場合があります。（デフォルトアクションで処理されるトラフィックでは、ファイルまたはマルウェアのインスペクションを実行できません）。

アクセス コントロール ルールまたはデフォルト アクションによって許可したトラフィックは、自動的にホスト、アプリケーション、およびユーザ データについてネットワーク検出ポリシーによるインスペクションの対象になります。明示的に検出を有効にしなくても、それを拡張または無効にできます。ただし、トラフィックを許可すると、検出データの収集は自動的に保証

されません。システムは、ネットワーク検出ポリシーによって明示的にモニタされる IP アドレスを含む接続に対してのみ、ディスカバリを実行します。また、アプリケーション検出は、暗号化されたセッションに限定されます。

暗号化されたトラフィックの通過がSSLインスペクション設定で許可される場合、またはSSLインスペクションが設定されていない場合は、そのトラフィックがアクセスコントロールルールによって処理されることに注意してください。ただし、一部のアクセス コントロール ルールの条件では暗号化されていないトラフィックを必要とするため、暗号化されたトラフィックに一致するルール数が少なくなる場合があります。また、デフォルトでは、システムは暗号化されたペイロードの侵入およびファイルのインスペクションを無効にしていますこれにより、侵入およびファイル インスペクションが設定されたアクセス コントロール ルールに暗号化接続が一致したときの誤検出が減少し、パフォーマンスが向上します。

アプリケーション制御に関する推奨事項

アプリケーションによるネットワークへのアクセスを次のように制御することをお勧めします。

- 安全性の低いネットワークからより安全なネットワークへのアプリケーションアクセスを許可またはブロックするには、アクセス コントロール ルールで [ポート（Port）]（[選択した宛先ポート（Selected Destination Port）]）条件を使用します。

  たとえば、インターネット（安全性が低い）から内部ネットワーク（安全性が高い）への ICMP トラフィックを許可します。

- ユーザ グループによるアプリケーションへのアクセスを許可またはブロックするには、アクセス コントロール ルールで [アプリケーション（Application）] 条件を使用します。

  たとえば、契約業者グループのメンバーによる Facebook へのアクセスをブロックします。

注意 アクセス コントロール ルールを適切に設定しないと、ブロックされるべきトラフィックが許可されるなど、予期しない結果が発生する可能性があります。一般的に、アプリケーション制御ルールは、たとえば IP アドレスに基づくルールよりも照合に時間がかかるため、アクセス コントロール リスト内の順位を低くする必要があります。

特定の条件（ネットワークや IP アドレスなど）を使用するアクセス コントロール ルールは、一般的な条件（アプリケーションなど）を使用するルールの前に順位付けする必要があります。オープン システム相互接続（OSI）モデルに精通している場合は、考え方として同様の順位付けを使用してください。レイヤ1、2、および3（物理、データリンク、およびネットワーク）の条件を持つルールは、アクセス コントロール ルールの最初に順位付けする必要があります。レイヤ5、6、および7（セッション、プレゼンテーション、およびアプリケーション）の条件は、アクセス コントロール ルールの後ろのほうに順序付けする必要があります。OSI モデルの詳細については、こちらの Wikipedia の記事を参照してください。

次の表に、アクセス コントロール ルールを設定する方法の例を示します。

コントロールの種類	操作	ゾーン、ネットワーク、VLAN タグ	Users	アプリケーション	ポート	URL	SGT/ISE 属性	インスペクション、ロギング、コメント
アプリケーションがポート（SSH など）を使用する場合の、安全性の高いネットワークから安全性の低いネットワークへのアプリケーション	お客様の選択（この例では [許可（Allow）]）	外部インターフェイスを使用する宛先ゾーンまたはネットワーク	任意（Any）	設定しない	使用可能なポート：**SSH** [選択した宛先ポート（Selected Destination Port）] に追加	任意（Any）	ISE/ISE-PIC でのみ使用。	任意（Any）
アプリケーションがポートを使用していない場合の（ICMP など）、安全性の高いネットワークから安全性の低いネットワークへのアプリケーション	お客様の選択（この例では [許可（Allow）]）	外部インターフェイスを使用する宛先ゾーンまたはネットワーク	任意（Any）	設定しない	選択された宛先ポート プロトコル：**ICMP** **タイプ**：**Any**	設定しない	ISE/ISE-PIC でのみ使用。	任意（Any）

コントロールの種類	操作	ゾーン、ネットワーク、VLAN タグ	Users	アプリケーション	ポート	URL	SGT/ISE 属性	インスペクション、ロギング、コメント
ユーザ グループによるアプリケーション アクセス	お客様の選択（この例では [ブロック（Block）]）	お客様の選択	ユーザ グループ（この例では契約業者グループ）を選択。	アプリケーションの名前（この例では [Facebook]）を選択。	設定しない	設定しない	ISE/ISE-PIC でのみ使用。	お客様の選択

アクセス コントロール ルールの管理

アクセス コントロール ポリシー エディタの [Rules] タブでは、現在のポリシー内のアクセスコントロールルールの追加、編集、分類、検索、移動、有効化、無効化、削除、その他の管理が行えます。

ポリシー エディタでは、各アクセス コントロール ルールに対してルールの名前、条件の概要、ルール アクションが表示され、さらにルールのインスペクション オプションや状態を示すアイコンが表示されます。各アイコンの意味は次のとおりです。

- 侵入ポリシー オプション（  ）
- ファイル ポリシー オプション（  ）
- セーフ サーチ オプション（  ）
- YouTube EDU オプション（  ）
- ロギング オプション（  ）
- 発信元クライアント オプション（  ）
- コメント（  ）
- 警告（  ）
- エラー（  ）
- 重要な情報（  ）

無効なルールはグレー表示され、ルール名の下に [（無効）（(disabled)）] というマークが付きます。

ルールを作成または編集するには、アクセス コントロール ルール エディタを使用します。次の操作を実行できます。

- エディタの上部で、ルールの名前、状態、位置、アクションなどの基本的なプロパティを設定します。
- エディタの左下にあるタブを使用して、条件を追加します。
- インスペクションおよびロギングのオプションを設定し、さらにルールにコメントを追加するには、右下にあるタブを使用します。便宜上、どのタブを表示しているかに関係なく、エディタにはルールのインスペクションおよびロギングのオプションがリストされます。

（注） アクセス コントロール ルールの適切な作成と順序付けは複雑なタスクですが、効果的な展開を構築するためには必須なものです。慎重なポリシーの設計を怠ると、他のルールをプリエンプション処理したり、追加ライセンスが必要となったり、無効な設定を含んだルールになる可能性があります。システムが想定どおりにトラフィックを確実に処理できるように、アクセス コントロール ポリシー インターフェイスにはルールに対する強力な警告およびエラーのフィードバック システムがあります。

関連トピック

アクセス コントロール ルールのコンポーネント （1694 ページ）
カスタム ユーザ ロールの作成 （82 ページ）
ルールのパフォーマンスに関するガイドライン （502 ページ）

アクセス コントロール ルールのコンポーネント

一意の名前に加え、各アクセス コントロール ルールには次の基本コンポーネントがあります。

状態

デフォルトでは、ルールが有効状態になります。ルールを無効にすると、システムはそのルールを使用せず、そのルールに対する警告とエラーの生成を停止します。

位置

アクセス コントロール ポリシー内の各ルールには、1 から始まる番号が付きます。ポリシー継承を使用する場合、ルール 1 は再外部ポリシーの 1 番目のルールです。システムは、ルール番号の昇順で上から順に、ルールをトラフィックと照合します。モニタ ルールを除き、トラフィックが一致する最初のルールがそのトラフィックを処理するルールになります。

また、ルールはセクションおよびカテゴリに属していることがあります。これは、単に整理のためであり、ルールの位置に影響しません。ルールの位置は、すべてのセクションとカテゴリにまたがって設定されます。

セクションおよびカテゴリ

アクセス コントロール ルールの整理に役立つように、アクセス コントロール ポリシーには、システムで用意されている 2 つのルール セクションとして「必須（Mandatory）」と「デフォルト（Default）」があります。アクセス コントロール ルールをさらに細かく整理するため、「必須（Mandatory）」セクション内と「デフォルト（Default）」セクション内にカスタム ルール カテゴリを作成することができます。

ポリシーの継承を使用する場合、現在のポリシーのルールは、その親ポリシーの「必須（Mandatory）」セクションと「デフォルト（Default）」セクションの間にネストされます。

条件

条件は、ルールで処理する特定のトラフィックを指定します。条件は単純または複雑にできます。条件の使用はライセンスによって異なります。

Action

ルールのアクションは、一致したトラフィックの処理方法を決定します。一致するトラフィックをモニタ、信頼、ブロック、または許可（追加のインスペクションあり/なしで）することができます。信頼できるトラフィック、ブロックされたトラフィック、または暗号化されたトラフィックに対しては、詳細な検査は実行**されません**。

インスペクション（Inspection）

詳細検査オプションは、悪意のあるトラフィックをどのように検査してブロックし、それ以外のものは許可するかを決定します。ルールを使用してトラフィックを許可するときは、システムが侵入ポリシーまたはファイル ポリシーを使用してトラフィックを最初に検査し、アセットに到達したりネットワークを出る前に、エクスプロイト、マルウェア、または禁止されたファイルをブロックするように指定できます。

ロギング

ルールのロギング設定は、システムが処理するトラフィックのレコードの維持を制御します。各ルールに一致したトラフィックのレコードを維持できます。一般的に、接続の開始時または終了時（あるいは、その両方）にセッションをログに記録できます。接続のログは、データベースの他に、システム ログ（Syslog）または SNMP トラップ サーバに記録できます。

説明

アクセス コントロール ルールで変更を保存するたびに、コメントを追加できます。

関連トピック

ルールのパフォーマンスに関するガイドライン （502 ページ）
アクセス コントロール ルールの管理 （1693 ページ）
アクセス コントロール ルールの作成および編集 （1698 ページ）
ルール条件タイプ （465 ページ）
アクセス コントロール ルールのアクション （1701 ページ）

ディープ インスペクションについて （1707 ページ）
接続のロギングのベスト プラクティス （3012 ページ）
アクセス コントロール ルールのコメント （1704 ページ）

アクセス コントロール ルールの順序

アクセス コントロール ポリシー内の各ルールには、1 から始まる番号が付きます。システムは、ルール番号の昇順で先頭から順にアクセス コントロール ルールをトラフィックと照合します。

ほとんどの場合、システムは、すべてのルールの条件がトラフィックに一致する場合、最初のアクセス コントロール ルールに従ってネットワーク トラフィックを処理します。モニタルールを除いて、トラフィックがルールに一致した後、システムは優先度の低い追加のルールに対してトラフィックの評価は続行しません。

アクセス コントロール ルールの整理に役立つように、アクセス コントロール ポリシーには、システムで用意されている 2 つのルール セクションとして「必須（Mandatory）」と「デフォルト（Default）」があります。さらに細かく整理するため、「必須（Mandatory）」セクション内や「デフォルト（Default）」セクション内にカスタム ルール カテゴリを作成することができます。カテゴリを作成した後は、そのカテゴリの削除と名前の変更に加え、カテゴリへのルールの挿入、ルールの削除、カテゴリ内またはカテゴリ間のルールの移動はできますが、カテゴリ自体の移動はできません。システムはセクションとカテゴリに横断的にルール番号を割り当てます。

ポリシーの継承を使用する場合、現在のポリシーのルールは、その親ポリシーの「必須（Mandatory）」ルール セクションと「デフォルト（Default）」ルール セクションの間にネストされます。ルール 1 は、現在のポリシーではなく、最外部ポリシーの 1 番目のルールです。ルールの番号は、すべてのポリシー、セクション、カテゴリにまたがって割り当てられます。

アクセス コントロール ポリシーの変更を許可する定義済みユーザ ロールによって、ルールのカテゴリ内またはカテゴリ間でアクセス コントロール ルールを移動および変更することもできます。しかし、ユーザがルールを移動および変更することを制限するには、カスタム ロールを作成できます。アクセス コントロール ポリシーの変更権限が割り当てられているユーザは、制限なく、カスタム カテゴリにルールを追加することや、カテゴリ内のルールを変更することができます。

ヒント アクセス コントロール ルールの順序を適切にすることで、ネットワーク トラフィックの処理に必要なリソースが減り、ルールのプリエンプションを回避できます。ユーザが作成するルールはすべての組織と展開に固有のものですが、ユーザのニーズに対処しながらもパフォーマンスを最適化できるルールを順序付けする際に従うべきいくつかの一般的なガイドラインがあります。

関連トピック

ルールの順序指定のガイドライン （503 ページ）

アクセス制御ルール カテゴリの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Access Admin/Network Admin

アクセス コントロール ポリシーの必須ルールセクションとデフォルトルールセクションをカスタムカテゴリに分割できます。カテゴリを作成した後は、そのカテゴリの削除と名前の変更に加え、カテゴリへのルールの挿入、ルールの削除、カテゴリ内またはカテゴリ間のルールの移動はできますが、カテゴリ自体の移動はできません。システムはセクションとカテゴリに横断的にルール番号を割り当てます。

ステップ 1 アクセス コントロール ポリシー エディタで、[カテゴリの追加（Add Category）] をクリックします。

ヒント ポリシーにルールがすでに含まれている場合は、既存のルールの行の空白部分をクリックして、新しいカテゴリを追加する前にその位置を設定できます。既存のルールを右クリックし、[新規カテゴリの挿入（Insert new category）] を選択することもできます。

ステップ 2 名前を入力します。

ステップ 3 [挿入（Insert）] ドロップダウン リストから、カテゴリを追加する先を選択します。

- カテゴリをセクションのすべての既存カテゴリの下に挿入するには、[必須ルール内（Into Mandatory）] または [デフォルトルール内（into Default）] を選択します。
- 既存のカテゴリの上に挿入するには、[カテゴリの上（above category）] を選択した後、カテゴリを選択します。
- アクセス制御ルールの上または下に挿入するには、[ルールの上（above rule）] または [ルールの下（below rule）] を選択した後、既存のルール番号を入力します。

ステップ 4 [OK] をクリックします。

ステップ 5 [保存（Save）] をクリックしてポリシーを保存します。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

アクセス コントロール ルールの作成および編集

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Access Admin/Network Admin

ステップ 1 アクセス コントロール ポリシー エディタには、以下のオプションがあります。

- 新しいルールを追加するには、[ルールの追加（Add Rule）] をクリックします。
- 既存のルールを編集するには、編集アイコン（  ）をクリックします。

代わりに表示アイコン（  ）がルールの横に表示される場合、ルールは先祖ポリシーに属しており、ルールを変更する権限がありません。

ステップ 2 [Name] を入力します。

ステップ 3 ルール コンポーネントを設定するか、またはデフォルトを受け入れます。

- [有効（Enabled）] : ルールを有効にするかどうかを指定します。
- [位置（Position）] : ルールの位置を指定します。アクセス コントロール ルールの順序 （1696 ページ）を参照してください。
- [アクション（Action）] : ルールの [アクション（Action）] を選択します。アクセス コントロール ルールのアクション （1701 ページ）を参照してください。
- [条件（Conditions）] : 追加する条件に対応するタブをクリックします。詳細は、ルール条件タイプ （465 ページ）を参照してください。
- [ディープ インスペクション（Deep Inspection）] : 許可ルールおよびインタラクティブ ブロック ルールの場合、侵入調査アイコン（  ）またはファイルおよびマルウェア調査アイコン（  ）をクリックして、ルールの [インスペクション（Inspection）] オプションを設定します。アイコンが淡色表示の場合、そのタイプのポリシーがルールに選択されていません。詳細については、侵入ポリシーとファイル ポリシーを使用したアクセス制御 （1707 ページ）を参照してください。
- [コンテンツの制限（Content Restriction）] : セーフ サーチ アイコン（  ）または YouTube EDU アイコン（  ）をクリックして、ルール エディタの [アプリケーション（Applications）] タブでコンテンツ制限設定を行います。アイコンが淡色表示の場合、ルールに対してコンテンツ制限は無効になっています。詳細については、コンテンツ制限について （1793 ページ）を参照してください。
- [ロギング（Logging）] : アクティブな（青の）ロギング アイコン（  ）をクリックして、[ロギング（Logging）] オプションを指定します。アイコンが淡色表示の場合、接続ロギングがそのルールで無

効になっています。詳細については、接続のロギングのベストプラクティス（3012ページ）を参照してください。

- [コメント（Comments）]：コメント列の数字をクリックして、[コメント（Comments）] を追加します。数字は、ルールにすでに含まれているコメントの数を示します。詳細については、アクセス コントロール ルールのコメント（1704 ページ）を参照してください。

ステップ 4 ルールを保存します。

ステップ 5 [保存（Save）] をクリックして、ポリシーを保存します。

次のタスク

- 設定変更を展開します。設定変更の展開（447 ページ）を参照してください。

関連トピック

ルールのパフォーマンスに関するガイドライン（502 ページ）

アクセス コントロール ルールの有効化と無効化

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Access Admin/Network Admin

アクセス コントロール ルールを作成すると、デフォルトで有効になります。無効にしたルールはネットワーク トラフィックの評価には使用されなくなり、そのルールについての警告とエラーが停止されます。アクセス コントロール ポリシーでルールのリストを表示するとき、無効状態のルールはグレーで表示されますが、変更は可能です。

ヒント また、ルール エディタを使用してアクセス コントロール ルールを有効化または無効化することもできます。

ステップ 1 アクセス コントロール ポリシー エディタで、ルールを右クリックし、ルールの状態を選択します。

代わりに表示アイコン（  ）がルールの横に表示される場合、ルールは先祖ポリシーに属しており、ルールを変更する権限がありません。

ステップ 2 **[保存（Save）]** をクリックします。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

関連トピック

アクセス コントロール ルールのコンポーネント （1694 ページ）

アクセス コントロール ルールの配置

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Access Admin/Network Admin

既存のルールは、アクセス コントロール ポリシー内で移動できますが、アクセス コントロール ポリシー間では移動できません。カテゴリにルールを追加または移動すると、そのルールはシステムによってカテゴリの最後に配置されます。

ヒント 複数のルールを一度に移動するには、移動するルールを選択し、右クリック メニューを使用してカット アンド ペーストします。

ステップ 1 アクセス制御ルール エディタには、次のオプションがあります。

- 新しいルールを追加する場合は、[挿入（Insert）] ドロップダウンリストを使用します。
- 既存のルールを編集する場合、[移動（Move）] をクリックします。

ステップ 2 ルールを移動またはルールを挿入する場所を選択します。

- [必須に挿入（into Mandatory）] または [デフォルトに挿入（into Default）] を選択します。
- [カテゴリに挿入（into Category）] を選択して、ユーザ定義カテゴリを選択します。
- [ルールの上（above rule）] または [ルールの下（below rule）] を選択してから、適切なルール番号を入力します。

ステップ 3 [保存（Save）] をクリックします。

ステップ 4 [保存（Save）] をクリックして、ポリシーを保存します。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

アクセス コントロール ルールのアクション

アクセス コントロール ルールには、システムが一致するトラフィックをどのように処理し、ロギングするのかを指定するアクションがあります。モニタ、信頼、ブロック、または許可（追加のインスペクションあり/なしで）することができます。

アクセス コントロール ポリシーのデフォルトアクションは、モニタ以外のアクションをもつどのアクセスコントロールルールの条件にも一致しないトラフィックを処理します。

アクセス コントロール ルールのモニタ アクション

[Monitor] アクションは、トラフィックを許可または拒否するように設計されていません。むしろ、その主な目的は、一致するトラフィックが最終的にどのように処理されるかに関係なく、接続ロギングを強制することです。

接続がモニタルールに一致する場合、接続が一致する次の非モニタルールがトラフィック処理とそれ以降のインスペクションを決定する必要があります。さらに一致するルールがない場合、システムはデフォルトアクションを使用する必要があります。

ただし、例外があります。モニタルールにレイヤ7の条件（アプリケーション条件など）が含まれている場合、そのシステムでは早期パケットを通過させ、接続を確立（またはSSLハンドシェイクの完了）することができます。これは、接続が後続のルールによってブロックされる必要がある場合でも発生します。これらの早期パケットが後続のルールに対して評価されないためです。こうしたパケットが完全に検査されていない宛先に到達しないように、アクセスコントロールポリシーのデフォルト侵入ポリシーによって検査されます。デフォルトの侵入ポリシー（2287ページ）を参照してください。システムはレイヤ7の識別を完了した後、残りのセッショントラフィックに適切なアクションを適用します。

注意 ベストプラクティスとして、広範に定義されたモニタルールのレイヤ7の条件をルールの優先順位内で高く設定しないようにすることで、不注意でトラフィックがネットワークに流入することを防ぎます。さらに、ローカルでバインドされているトラフィックがレイヤ3展開のモニタルールに一致する場合、そのトラフィックは検査をバイパスすることがあります。トラフィックのインスペクションを確実に実行するには、トラフィックをルーティングしている管理対象デバイスの詳細設定で [Inspect Local Router Traffic] を有効にします。

関連トピック

モニタされた監視接続のロギング （3005 ページ）

アクセス コントロール ルールの信頼アクション

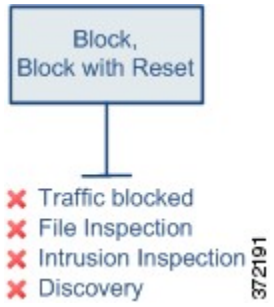
[信頼（Trust）] アクションは、ディープ インスペクションやネットワーク検出をせずにトラフィックを通過させます。信頼処理されたトラフィックも、ID 条件およびレート制限の対象です。

関連トピック

信頼されている接続のロギング （3005 ページ）

アクセス コントロール ルールのブロック アクション

ブロック アクションおよび**リセットしてブロック** アクションはトラフィックを拒否し、いかなる追加のインスペクションも行われません。



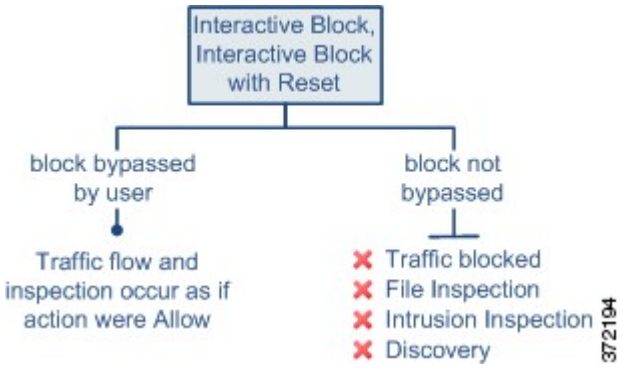
[HTTP 応答（HTTP response）] ページに一致する Web 要求を除き、リセット ルールを持つブロックが接続をリセットします。これは、システムが Web 要求をブロックするときに表示されるように設定した応答ページは、接続がすぐにリセットされた場合は表示できないためです。詳細については、「HTTP応答ページとインタラクティブなブロッキング （1735ページ）」を参照してください。

関連トピック

ブロックされた接続のロギング （3006 ページ）
HTTP 応答ページについて （1735 ページ）

アクセス コントロール ルール インタラクティブ ブロック アクション

詳細については、HTTP応答ページとインタラクティブなブロッキング （1735ページ）を参照してください。



ユーザがブロックをバイパスしている場合、ルールは許可ルールを模倣します。したがって、インタラクティブ ブロック ルールをファイル ポリシーと侵入ポリシーに関連付けることができるため、一致するトラフィックもネットワーク検出の対象となります。

ユーザがブロックをバイパスしない（できない）場合は、ルールはブロック ルールを模倣します。一致するトラフィックは、追加のインスペクションなしで拒否されます。

インタラクティブブロックを有効にした場合は、ブロックされているすべての接続をリセットできません。これは、接続がすぐにリセットされた場合は応答ページを表示できないためです。[リセットしてインタラクティブ ブロック（Interactive Block with reset）] アクションを（非インタラクティブに）Web 以外のすべてのトラフィックをリセットしてブロックしても、Web 要求についてはインタラクティブ ブロックは有効になっています。

詳細については、HTTP 応答ページとインタラクティブなブロッキング （1735 ページ）を参照してください。

関連トピック

許可された接続のロギング （3008 ページ）
TLS/SSL ルールのブロック アクション （1865 ページ）

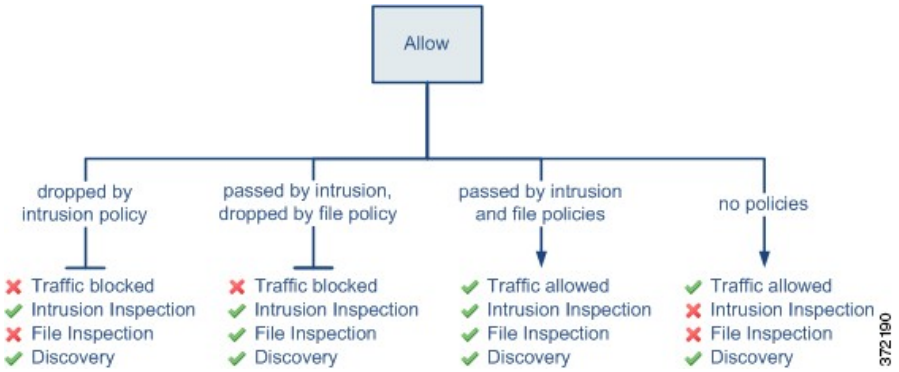
アクセス コントロール ルールの許可アクション

[許可（Allow）] アクションは、一致するトラフィックを通過させます。ただし、引き続き ID 条件およびレート制限の対象となります。

任意で、ディープインスペクションを行い、トラフィックが接続先に到達する前に暗号化されていないトラフィックや復号されたトラフィックを検査、ブロックすることも可能です。

- 侵入ポリシーでは、侵入検知と防御設定に応じてネットワーク トラフィックを分析し、設定内容に応じて違反パケットをドロップすることが可能です。
- ファイルポリシーでは、ファイルの制御ができます。ファイル制御により、ユーザが特定のアプリケーションプロトコルを介して特定のタイプのファイルをアップロード（送信）またはダウンロード（受信）するのを検出およびブロックすることができます。
- ネットワークベースの高度なマルウェア保護（AMP）もファイル ポリシーを使用して実行できます。ネットワーク向け AMP はファイルのマルウェアを調べ、検出したマルウェアを設定に応じてブロックします。

下の図は、許可ルールの条件（またはユーザによりバイパスされるインタラクティブブロック ルール）を満たすトラフィックに対して実行されるインスペクションの種類を示しています。侵入インスペクションの前にファイルインスペクションが行われることに注意してください。そこでブロックされたファイルに対しては、侵入関連のエクスプロイトについては検査されません。



単純化のために、侵入ポリシーとファイル ポリシーの両方がアクセス コントロール ルールに関連付けられている状態（またはどちらも関連付けられていない状態）のトラフィック フローを図に示しています。ただし、いずれか一方を設定して他方は設定なしにすることもできます。ファイル ポリシーがない場合、トラフィック フローは侵入ポリシーによって決定されます。侵入ポリシーがない場合、トラフィック フローはファイル ポリシーによって決定されます。

トラフィックが侵入ポリシーとファイルポリシーのどちらかによって検査またはドロップされるかどうかに関わらず、システムはネットワーク検出を使ってトラフィックを検査できます。ただし、トラフィックを許可することは検出インスペクションが自動的に保証されることではありません。システムは、ネットワーク検出ポリシーによって明示的にモニタされる IP アドレスを含む接続に対してのみ、ディスカバリを実行します。また、アプリケーション検出は、暗号化されたセッションに限定されます。

関連トピック

許可された接続のロギング （3008 ページ）

アクセス コントロール ルールのコメント

アクセス コントロール ルールを作成または編集するときは、コメントを追加できます。たとえば、他のユーザのために設定全体を要約したり、ルールの変更時期と変更理由を記載することができます。あるルールの全コメントのリストを表示し、各コメントを追加したユーザやコメント追加日を確認することができます。

ルールを保存すると、最後に保存してから追加されたすべてのコメントは読み取り専用になります。

関連トピック

アクセス コントロール ポリシーの設定の構成

アクセス制御ルールへのコメントの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Access Admin/Network Admin

ステップ 1 アクセス コントロール ルール エディタで、[コメント（Comments）] タブをクリックします。

ステップ 2 [New Comment] をクリックします。

ステップ 3 コメントを入力し、[OK] をクリックします。ルールを保存するまでこのコメントを編集または削除できます。

ステップ 4 [保存（Save）] をクリックします。

ステップ 5 [保存（Save）] をクリックして、ポリシーを保存します。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

第 64 章

侵入ポリシーとファイル ポリシーを使用したアクセス制御

次の各トピックでは、侵入ポリシーとファイルポリシーを使用するようにアクセス コントロール ポリシーを設定する方法について説明します。

ディープ インスペクションについて

侵入ポリシーとファイルポリシーは、トラフィックが宛先に対して許可される前の最後のとりでとして連携して動作します。

- 侵入ポリシーは、システムの侵入防御機能を制御します。
- ファイル ポリシーは、システムのファイル制御と ネットワーク向け AMP の機能を管理します。

アクセス コントロールはディープ インスペクションの前に発生し、アクセス コントロール ルールおよびアクセス コントロールのデフォルト アクションによって、侵入ポリシーおよびファイル ポリシーで検査されるトラフィックが決まります。

侵入ポリシーまたはファイル ポリシーをアクセス コントロール ルールに関連付けることで、アクセスコントロールルールの条件に一致するトラフィックを通過させる前に、侵入ポリシーまたはファイルポリシー（またはその両方）を使ってトラフィックを検査するよう、システムに指示できます。

（注） デフォルトでは、暗号化ペイロードの侵入およびファイル インスペクションは無効化されます。これにより、侵入およびファイル インスペクションが設定されたアクセス コントロール ルールに暗号化接続が一致したときの誤検出が減少し、パフォーマンスが向上します。

システムは、AMP クラウドからエンドポイント向け AMP データを受信し、このデータを任意の ネットワーク向け AMP データと一緒に表示できます。

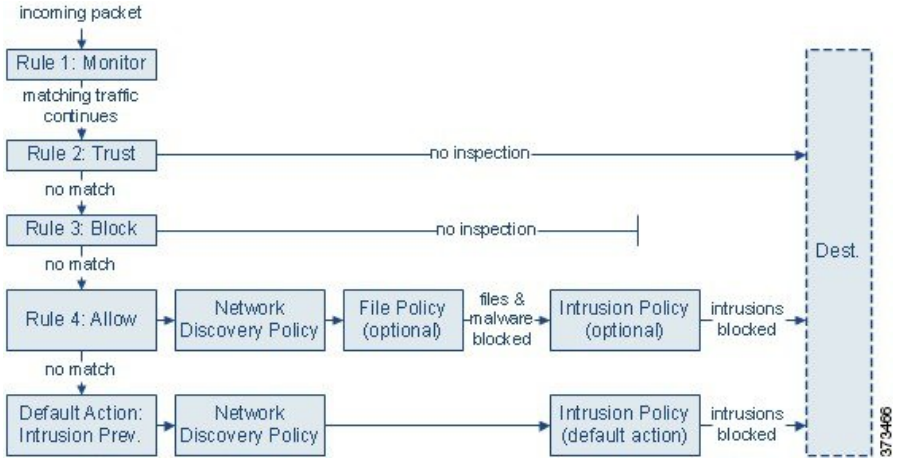
関連トピック

ポリシーが侵入についてトラフィックを検査する仕組み （2026 ページ）
ファイル ポリシー （1912 ページ）

アクセス コントロール トラフィック処理

アクセス コントロール ルールは、複数の管理対象デバイスでネットワーク トラフィックを処理する詳細な方法を提供します。システムは、指定した順にアクセス コントロール ルールをトラフィックと照合します。ほとんどの場合、システムは、すべてのルールの条件がトラフィックに一致する場合、最初のアクセス コントロール ルールに従ってネットワーク トラフィックを処理します。アクセス コントロール ルールのアクションによって、システムが一致するトラフィックをどのように処理するかが決まります。一致したトラフィックをモニタ、信頼、ブロック、または許可（追加のインスペクションあり/なしで）することができます。

次の図は、4 つの異なるタイプのアクセス コントロール ルールとデフォルト アクションを含むアクセス コントロール ポリシーによって制御されている、インラインの侵入防御と ネットワーク向け AMP の展開におけるトラフィックのフローを示します。



上記のシナリオでは、ポリシー内の最初の 3 つのアクセス コントロール ルール（モニタ、信頼およびブロック）は一致するトラフィックを検査できません。モニタ ルールはネットワーク トラフィックの追跡とロギングを行いますが検査はしないので、システムは引き続きトラフィックを追加のルールと照合し、許可または拒否を決定します。（ただし、重要な例外と注意事項をアクセス コントロール ルールのモニタ アクション （1701 ページ）で確認してください）。

信頼ルールおよびブロック ルールは、どのような種類のインスペクションも追加で行うことなく一致するトラフィックを処理しますが、一致しないトラフィックは引き続き次のアクセス コントロール ルールに照合されます。

ポリシー内の4番目と最後のルールである許可ルールは、次の順序で他のさまざまなポリシーを呼び出し、一致するトラフィックを検査および処理します。

- **ディスカバリ**：**ネットワーク検出ポリシー**：最初に、ネットワーク検出ポリシーがトラフィックのディスカバリ データの有無を検査します。ディスカバリはパッシブ分析で、トラフィックのフローに影響しません。明示的に検出を有効にしなくても、それを拡張または無効にできます。ただし、トラフィックを許可すると、検出データの収集は自動的に保証されません。システムは、ネットワーク検出ポリシーによって明示的にモニタされるIPアドレスを含む接続に対してのみ、ディスカバリを実行します。
- [とファイル制御：ファイル ポリシー（and File Control: File Policy）]**ネットワーク向け AMP**：トラフィックが検出により調査された後、システムが禁止ファイルやマルウェアを調査します。ネットワーク向け AMP は PDF や Microsoft Office ドキュメントなど、多くのタイプのファイルでマルウェアを検出し、必要に応じてブロックします。部門がマルウェア ファイル伝送のブロックに加えて、（ファイルにマルウェアが含まれるかどうかにかかわらず）特定のタイプのすべてのファイルをブロックする必要がある場合は、ファイル制御機能により、特定のファイル タイプの伝送についてネットワーク トラフィックをモニタし、ファイルをブロックまたは許可できます。
- **侵入防御**：**侵入ポリシー**：ファイル インスペクションの後、システムは侵入およびエクスプロイトについてトラフィックを検査できます。侵入ポリシーは、復号されたパケットの攻撃をパターンに基づいて調査し、悪意のあるトラフィックをブロックしたり、変更したりします。侵入ポリシーは変数セットとペアになり、それによって名前付き値を使用してネットワーク環境を正確に反映できます。
- **接続先**：前述のすべてのチェックを通過したトラフィックは、その接続先に渡されます。

インタラクティブ ブロック ルール（この図には表示されていません）には、許可ルールと同じインスペクション オプションがあります。これにより、あるユーザが警告ページをクリックスルーすることによってブロックされた Web サイトをバイパスした場合に、悪意のあるコンテンツがないかトラフィックを検査できます。

モニタ以外のアクションに関するポリシー内のアクセスコントロールルールのいずれにも一致しないトラフィックは、デフォルトアクションによって処理されます。このシナリオでは、デフォルトアクションは侵入防御アクションとなり、トラフィックは指定された侵入ポリシーを通過する限りその最終接続先に許可されます。別の展開では、追加のインスペクションなしですべてのトラフィックを信頼またはブロックするデフォルトアクションが割り当てられている場合もあります。システムはデフォルト アクションによって許可されたトラフィックに対しディスカバリ データおよび侵入の有無を検査できますが、禁止されたファイルまたはマルウェアの有無は検査できないことに注意してください。アクセス コントロールのデフォルト アクションにファイル ポリシーを関連付けることは**できません**。

（注） 場合によっては、接続がアクセス コントロール ポリシーによって分析される場合、システムはトラフィックを処理するアクセス コントロール ルール（存在する場合）を決定する前に、その接続の最初の数パケットを処理し**通過を許可する**必要があります。しかし、これらのパケットは検査されないまま宛先に到達することはないので、デフォルト侵入ポリシーと呼ばれる侵入ポリシーを使用して、パケットを検査し侵入イベントを生成できます。

ファイルインスペクションおよび侵入インスペクションの順序

アクセス コントロール ポリシーで、複数の許可ルールとインタラクティブ ブロック ルールを異なる侵入ポリシーおよびファイル ポリシーに関連付けて、インスペクション プロファイルをさまざまなタイプのトラフィックに照合できます。

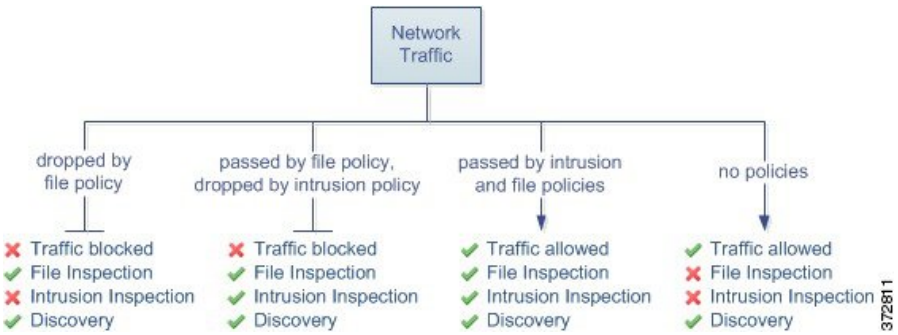
（注） 侵入防御またはネットワーク検出のみのデフォルトアクションによって許可されたトラフィックは、検出データおよび侵入の有無について検査されますが、禁止されたファイルまたはマルウェアの有無については検査されません。アクセス コントロールのデフォルト アクションにファイル ポリシーを関連付けることは**できません**。

同じルールでファイルインスペクションと侵入インスペクションの両方を実行する必要はありません。許可ルールまたはインタラクティブ ブロック ルールに一致する接続の場合：

- ファイル ポリシーがない場合、トラフィック フローは侵入ポリシーによって決まります
- 侵入ポリシーがない場合、トラフィック フローはファイル ポリシーによって決まります
- どちらもない場合、許可されたトラフィックはネットワーク検出のみで検査されます

ヒント システムは、信頼されたトラフィックに対してはどんなインスペクションも実行しません。侵入ポリシーもファイルポリシーも含めずに許可ルールを設定すると、信頼ルールの場合と同様にトラフィックが通過しますが、許可ルールでは一致するトラフィックに対して検出を実行できます。

以下の図は、「許可」アクセスコントロールルール、またはユーザによりバイパスされた「インタラクティブブロック」アクセスコントロールルールのどちらかの条件を満たすトラフィックに対して実行できるインスペクションの種類を示しています。単純化のために、侵入/ファイル ポリシーの両方が 1 つのアクセス コントロール ルールに関連付けられている（またはどちらも関連付けられていない）状態でのトラフィック フローを図に示しています。



アクセス コントロール ルールによって処理される単一接続の場合、ファイル インスペクションは侵入インスペクションの前に行われます。つまり、システムは侵入の有無についてファイル ポリシーによってブロックされたファイルを検査しません。ファイル インスペクション内では、タイプによる単純なブロッキングの方が、マルウェア インスペクションおよびブロッキングよりも優先されます。

たとえば、アクセス コントロール ルールで定義された特定のネットワーク トラフィックを正常に許可するシナリオを考えてください。ただし、予防措置として、実行可能ファイルのダウンロードをブロックし、ダウンロードされた PDF のマルウェア インスペクションを行って検出された場合はブロックし、トラフィックに対して侵入インスペクションを実行する必要があるとします。

一時的に許可するトラフィックの特性に一致するルールを持つアクセス コントロール ポリシーを作成し、それを侵入ポリシーとファイル ポリシーの両方に関連付けます。ファイル ポリシーはすべての実行可能ファイルのダウンロードをブロックし、マルウェアを含む PDF の検査およびブロックも行います。

- まず、システムはファイル ポリシーで指定された単純なタイプ マッチングに基づいてすべての実行可能ファイルのダウンロードをブロックします。これはすぐにブロックされるため、これらのファイルは、マルウェア インスペクションの対象にも侵入インスペクションの対象にもなりません。
- 次に、システムは、ネットワーク上のホストにダウンロードされた PDF に対するマルウェア クラウド ルックアップを実行します。マルウェアの性質を持つ PDF はすべてブロックされ、侵入インスペクションの対象にはなりません。
- 最後に、システムはアクセス コントロール ルールに関連付けられている侵入ポリシーを使用して、ファイル ポリシーでブロックされなかったファイルを含む残りのトラフィック全体を検査します。

（注） ファイルがセッションで検出されブロックされるまで、セッションからのパケットは侵入インスペクションの対象になります。

マルウェア保護のためのアクセスコントロールルールの設定

アクセス コントロール ポリシーは、複数のアクセス コントロール ルールをファイル ポリシーに関連付けることができます。ファイル インスペクションを許可アクセス コントロール ルールまたはインタラクティブ ブロック アクセス コントロール ルールに設定でき、これによって、トラフィックが最終宛先に到達する前に、異なるファイルおよびマルウェアのインスペクション プロファイルをネットワーク上のさまざまなタイプのトラフィックと照合できます。

システムはファイル ポリシーの設定に従って禁止されたファイル（マルウェアを含む）を検出すると、イベントを Firepower Management Center データベースに自動的にロギングします。ログファイルまたはマルウェア イベントが必要ない場合は、アクセス コントロール ルールごとにこのロギングを無効にできます。

また、システムは、呼び出し元のアクセス コントロール ルールのロギング設定にかかわらず、関連付けられた接続の終了を Firepower Management Center データベースにロギングします。

マルウェア保護のためのアクセス コントロール ルールの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス（**Access**）
脅威（ファイル制御） マルウェア（AMP）	保護（ファイル制御） マルウェア（AMP）	いずれか（Any）	いずれか（Any）	Admin/Access Admin/Network Admin

注意 [ファイルの検出（Detect Files）] または [ファイルのブロック（Block Files）] ルールで [ファイルの保存（Store files）] を有効化/無効化した場合、または [マルウェア クラウド ルックアップ（Malware Cloud Lookup）] または [マルウェア ブロック（Block Malware）] ファイル ルール アクションを分析オプション（[Spero 分析または MSEXE（Spero Analysis or MSEXE）]、[動的分析（Dynamic Analysis）]、または [ローカル マルウェア分析（Local Malware Analysis）]）またはファイルの保存オプション（[マルウェア（Malware）]、[不明（Unknown）]、[正常（Clean）]、または [カスタム（Custom）]）と結合する最初のファイル ルールを追加または最後のファイル ルールを削除した場合には、設定の変更を展開する際に Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、ターゲット デバイスがトラフィックを処理する方法に応じて異なります。詳細はSnort® の再起動によるトラフィックの動作 （451 ページ）を参照してください。

始める前に

- AMP を含むファイル制御をアクセス コントロール ルールで実行するためには、適応型プロファイルの設定（2466ページ） で説明されているように、アダプティブ プロファイルを有効（デフォルト状態）にする**必要があります**。

ステップ 1 アクセス制御ルール エディタで、[許可（Allow）]、[インタラクティブ ブロック（Interactive Block）]、または [リセットしてインタラクティブ ブロック（Interactive Block with reset）] の [アクション（Action）] を選択します。

ステップ 2 [インスペクション（Inspection）] タブをクリックします。

ステップ 3 アクセス コントロール ルールに一致するトラフィックを検査する場合は [マルウェア ポリシー（Malware Policy）]（ファイル ポリシー）を選択し、または一致するトラフィックに対するファイル インスペクションを無効にする場合は [なし（None）] を選択します。

ステップ 4 （オプション）[ロギング（Logging）] タブをクリックし、[ログ ファイル（Log Files）] チェックボックスをオフにして、一致する接続のファイルまたはマルウェア イベントのロギングを無効にします。

（注） シスコでは、ファイル イベントおよびマルウェア イベントのロギングを有効のままにすることを推奨しています。

ステップ 5 ルールを保存します。

ステップ 6 [保存（Save）] をクリックして、ポリシーを保存します。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

関連トピック

ファイル ポリシーの作成 （1932 ページ）
Snort® の再起動シナリオ （450 ページ）

侵入防御のためのアクセス コントロール ルールの設定

アクセス コントロール ポリシーは、複数のアクセス コントロール ルールを侵入ポリシーに関連付けることができます。侵入インスペクションを許可アクセス コントロール ルールまたはインタラクティブ ブロック アクセス コントロール ルールに設定でき、これによって、トラフィックが最終宛先に到達する前に、異なる侵入インスペクション プロファイルをネットワーク上のさまざまなタイプのトラフィックと照合できます。

システムが侵入ポリシーを使用してトラフィックを評価する場合、システムは関連付けられた変数セットを使用します。セット内の変数は、侵入ルールで一般的に使用される値を表し、送信元および宛先の IP アドレスおよびポートを識別します。侵入ポリシーにある変数を使用して、ルール抑制および動的ルール状態にある IP アドレスを表すこともできます。

ヒント　システム提供の侵入ポリシーを使用する場合であっても、正確にネットワーク環境を反映するためにシステムの侵入変数を設定することを**強く**推奨します。少なくとも、デフォルトセットにあるデフォルトの変数を変更します。

システムによって提供される侵入ポリシーとカスタム侵入ポリシーについて

Firepower システムには複数の侵入ポリシーが付属しています。システム提供の侵入ポリシーを使用することで、Cisco Talos Intelligence Group（Talos）の経験を活用できます。これらのポリシーでは、Talos は侵入ルールおよびプリプロセッサ ルールの状態を設定し、詳細設定の初期設定も提供します。システムによって提供されるポリシーをそのまま使用するか、またはカスタム ポリシーのベースとして使用できます。カスタム ポリシーを作成すれば、環境内のシステムのパフォーマンスを向上させ、ネットワーク上で発生する悪意のあるトラフィックやポリシー違反に焦点を当てたビューが提供されます。

接続イベントおよび侵入イベントのロギング

アクセス コントロール ルールによって呼び出された侵入ポリシーが侵入を検出すると、侵入イベントを生成し、そのイベントを Firepower Management Center に保存します。また、システムはアクセス コントロール ルールのロギング設定に関係なく、侵入が発生した接続の終了を Firepower Management Center データベースに自動的にロギングします。

関連トピック

定義済みデフォルト変数 （541 ページ）

アクセス コントロール ルール設定と侵入ポリシー

1 つのアクセス コントロール ポリシーで使用可能な一意の侵入ポリシーの数は、ターゲット デバイスのモデルによって異なります。より強力なデバイスは、より多数のポリシーを処理できます。侵入ポリシーと変数セットの固有の**ペア**はすべて、1 つのポリシーと見なされます。異なる侵入ポリシーと変数セットのペアをそれぞれの許可ルールおよびインタラクティブ ブロック ルール（およびデフォルト アクション）と関連付けることができますが、ターゲット デバイスが設定されたとおりに検査を実行するのに必要なリソースが不足している場合は、アクセス コントロール ポリシーを展開できません。

侵入防御を実行するアクセス コントロール ルールの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Access Admin/Network Admin

ステップ 1 アクセス コントロール ポリシー エディタで、新しいルールを作成するか、既存のルールを編集します。アクセス コントロール ルールのコンポーネント （1694 ページ）を参照してください。

ステップ 2 ルール アクションが [許可（Allow）]、[インタラクティブ ブロック（Interactive Block）]、または [リセットしてインタラクティブ ブロック（Interactive Block with reset）] に設定されていることを確認します。

ステップ 3 [削除 タブを選択します。

ステップ 4 システムによって提供されるまたはカスタムの**侵入ポリシー**を選択するか、またはアクセス コントロール ルールに一致するトラフィックに対する侵入インスペクションを無効にするには [なし（None）] を選択します。

ステップ 5 侵入ポリシーに関連付けられた変数セットを変更するには、[変数セット（Variable Set）] ドロップダウン リストから値を選択します。

ステップ 6 [保存（Save）] をクリックしてルールを保存します。

ステップ 7 [保存（Save）] をクリックしてポリシーを保存します。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

関連トピック

変数セット （538 ページ）
Snort® の再起動シナリオ （450 ページ）

第 65 章

URL Filtering

URL フィルタリングの概要

URL フィルタリング機能を使用してネットワークのユーザがアクセスできる Web サイトを制御します。

- カテゴリおよびレピュテーションベースの URL フィルタリング：URL フィルタリング ライセンスでは、URL の一般的な分類（カテゴリ）とリスク レベル（レピュテーション）に基づいて Web サイトへのアクセスを制御することができます。これは推奨オプションです。
- 手動 URL フィルタリング：任意のライセンスで、個々の URL、URL のグループおよび URL リストとフィードを手動で指定し、Web トラフィックのきめ細かいカスタム制御を実現できます。詳細については、「手動URLフィルタリング （1729ページ）」を参照してください。

カテゴリおよびレピュテーションによるURLのフィルタリングについて

URL フィルタリング ライセンスでは、要求された URL のカテゴリおよびレピュテーションに基づいて、Web サイトへのアクセスを制御できます。

- カテゴリ：URL の一般的な分類。たとえば ebay.com はオークション カテゴリ、monster.com は求職カテゴリに属します。

  1 つの URL は複数のカテゴリに属することができます。

- レピュテーション：この URL が、組織のセキュリティ ポリシーに違反するかもしれない目的で使用される可能性がどの程度であるか。レピュテーションの範囲は、[高リスク（High Risk）]（レベル 1）から [ウェルノウン（Well Known）]（レベル 5）までがあります。

カテゴリおよびレピュテーションベースの URL フィルタリングのメリット

URL カテゴリとレピュテーションによって、URL フィルタリングをすぐに設定できます。たとえば、アクセス コントロールを使用して、ハッキング カテゴリの高リスク URL をブロックできます。または、QoS を使用してストリーミング メディア カテゴリのサイトからのトラフィックをレート制限できます。スパイウェアおよびアドウェア カテゴリなど、脅威のタイプのカテゴリもあります。

カテゴリおよびレピュテーションデータを使用すると、ポリシーの作成と管理がより簡単になります。この方法では、システムが Web トラフィックを期待どおりに確実に制御します。脅威インテリジェンスは、新しい URL だけでなく、既存の URL に対する新しいカテゴリとリスクで常に更新されるため、システムは最新の情報を使用して要求された URL をフィルタ処理します。セキュリティに対する脅威を表すサイトや望ましくないコンテンツが表示されるサイトは、ユーザが新しいポリシーを更新したり展開したりするペースを上回って次々と現れては消える可能性があります。

システムはどのように適応するのか、いくつかの例を示します。

- アクセス コントロール ルールですべてのゲーム サイトをブロックする場合、新しいドメインが登録されてゲームに分類されると、これらのサイトをシステムで自動的にブロックできます。同様に、QoS ルールですべてのストリーミング メディア サイトをレート制限する場合、システムは新しいストリーミング メディア サイトへのトラフィックを自動的に制限できます。

- アクセス コントロール ルールですべてのマルウェア サイトをブロックし、あるショッピング ページがマルウェアに感染すると、システムはその URL をショッピング サイトからマルウェア サイトに再分類して、そのサイトをブロックすることができます。

- アクセス コントロール ルールでリスクの高いソーシャル ネットワーキング サイトをブロックし、誰かがプロファイル ページに悪意のあるペイロードへのリンクが含まれるリンクを掲載すると、システムはそのページのレピュテーションを [無害なサイト（Benign Sites）] から [高リスク（High Risk）] に変更してブロックすることができます。

関連トピック

Snort® の再起動シナリオ （450 ページ）

Cisco Cloud からの URL フィルタリングのデータ

カテゴリおよびレピュテーションに基づく URL フィルタリングには、クラウド サービスである Cisco Collective Security Intelligence（Cisco CSI）から提供されたデータ セットが必要です。

一般に、デフォルトでは、有効な URL フィルタリング ライセンスがアクティブなデバイスに適用されると、URL カテゴリおよびレピュテーションのデータ セットが Cisco Cloud から Firepower Management Center にダウンロードされ、デバイスにプッシュされます。このローカルに保存されたデータ セットは定期的に更新されます。

ネットワーク上のユーザが URL にアクセスすると、システムはローカル（ダウンロードした）データ セット内の一致を検索します。一致がない場合、システムが Cisco Cloud で以前に検索した結果のキャッシュをチェックします。それでも一致がなければ、システムは Cisco Cloud で URL を検索し、結果をキャッシュに追加します。

URL フィルタリングのベスト プラクティス

- 手動フィルタリングではなく、カテゴリとレピュテーションに基づく URL フィルタリングを使用
- カテゴリとレピュテーションを使用した URL フィルタリングの設定方法（1723 ページ）の手順に従います。
- 次を詳しく確認してください。URL フィルタリングのガイドラインと制限事項（1719 ページ）

URL フィルタリングのガイドラインと制限事項

URL 識別の制限

システムは以下の動作の前に URL をフィルタリングできません。

- モニタ対象の接続がクライアントとサーバの間で確立される。
- システムによりセッションで HTTP または HTTPS アプリケーションが識別される。
- 要求された URL がシステムにより識別される（ClientHello メッセージまたはサーバ証明書から暗号化されたセッションの場合）。

この識別は 3 ～ 5 パケット以内で、またはトラフィックが暗号化されている場合は、TLS/SSL ハンドシェイクのサーバ証明書交換の後に行われる必要があります。

早期のトラフィックがその他のすべてのルール条件に一致するが、識別が不完全な場合、システムは、パケットの受け渡しと接続の確立（または、TLS/SSL ハンドシェイクの完了）を許可します。システムは識別を完了した後、残りのセッション トラフィックに適切なルール アクションを適用します。

アクセス制御の場合、これらの受け渡されたパケットは、デフォルトアクション侵入ポリシーでもほぼ一致するルールの侵入ポリシーでもなく、アクセス制御ポリシーのデフォルトの侵入ポリシーによりインスペクションが実行されます。

URL 条件とルールの順序

- URL マッチングを最も効果的に行うには、URL 条件を含むルールを他のルール（アプリケーション ルールなど）より前に配置します。特に、URL ルールがブロック ルールで、他のルールが次の条件を両方とも満たす場合には、URL 条件を含むルールを前に配置します。
  - その他のルールがアプリケーション条件を含んでいる。
  - 検査対象のトラフィックが暗号化されている。
- URL は複数のカテゴリに属することができます。Web サイトの 1 つのカテゴリを許可し、別のカテゴリをブロックすることができます（明示的に行うか、デフォルトアクションに依存して）。この場合、許可またはブロックが優先されるかどうかに応じて、適切な効果が得られるように URL ルールを作成して順序付けしてください。

ルールに関するその他のガイドラインについては、ルール条件の仕組み（467 ページ）およびルールのパフォーマンスに関するガイドライン（502 ページ）を含め、ルール管理：共通の特性（463 ページ）の章を参照してください。

未分類またはレピュテーションのない URL

URL ルールを作成するときは、まず一致させるカテゴリを選択します。[未分類（Uncategorized）] URL を明示的に選択した場合は、レピュテーションによりさらに制約を追加することはできません。

URL のカテゴリおよびレピュテーションが不明な場合、Web サイトの閲覧は、カテゴリおよびレピュテーションベースの URL 条件を持つルールには一致しません。カテゴリとレピュテーションを URL に手動で割り当てることはできませんが、アクセス コントロール ポリシーと QoS ポリシーでは、特定の URL を手動でブロックできます。手動 URL フィルタリング（1729 ページ）を参照してください。

暗号化された Web トラフィックの URL フィルタリング

暗号化された Web トラフィックに対して URL フィルタリングを実行すると、システムは次のように動作します。

- 暗号化プロトコルを無視します。ルールに URL 条件はあるがプロトコルを指定するアプリケーション条件がない場合、ルールは HTTPS および HTTP 両方のトラフィックを照合します。
- URL リストを使用しません。代わりに、URL オブジェクトとグループを使用する必要があります。

- トラフィックを暗号化するために使用する公開キー証明書のサブジェクト共通名に基づいて HTTPS トラフィックを照合し、サブジェクト共通名に含まれるサブドメインを無視します。
- アクセス制御ルール（または、その他の設定）によってブロックされている暗号化された接続の場合は HTTP 応答ページを表示しません。HTTP 応答ページの制限（1736 ページ）を参照してください。

HTTP/2

システムは、TLS 証明書から HTTP/2 URL を抽出できますが、ペイロードから抽出することはできません。

URL での検索クエリ パラメータ

システムでは、URL 条件の照合に URL 内の検索クエリ パラメータを使用しません。たとえば、すべてのショッピング トラフィックをブロックする場合を考えます。amazon.com を探すために Web 検索を使用してもブロックされませんが、amazon.com を閲覧しようとするとブロックされます。

高可用性展開での URL フィルタリング

高可用性での Firepower Management Center を使用した URL フィルタリングのガイドラインについては、URL フィルタリングとセキュリティ インテリジェンス（267 ページ）を参照してください。

選択したデバイス モデルのメモリ制限

- NGIPSv を使用する場合、カテゴリおよびレピュテーションベースの URL フィルタリングを実行するために正しい量のメモリを割り当てる方法については、『Cisco Firepower NGIPSv（VMware 向け）クイック スタート』を参照してください。
- メモリが不足しているデバイスモデルでは、ローカルで格納される URL データが減少します。したがって、システムはクラウドをより頻繁にチェックして、ローカルデータベースにないサイトのカテゴリとレピュテーションを判断します。

  低メモリ デバイスには、次のデバイスが含まれます。

  - 7100 シリーズ
  - ASA 5508-X および ASA 5516-X
  - ASA 5515-X および ASA 5525-X

手動 URL フィルタリング

特定の URL を手動でフィルタリングする場合は、影響を受ける可能性のある他のトラフィックを慎重に考慮してください。ネットワーク トラフィックが URL 条件に一致するかどうか判

別するために、システムは単純な部分文字列マッチングを実行します。要求された URL が文字列の任意の部分に一致する場合、URL は一致するとみなされます。

関連トピック

デフォルトの侵入ポリシー （2287 ページ）

HTTPS トラフィックのフィルタリング

暗号化されたトラフィックをフィルタリングするには、システムは TLS/SSL ハンドシェイク時に渡される情報（トラフィックを暗号化するために使用される公開キー証明書のサブジェクト共通名）に基づいて、要求された URL を決定します。

HTTPS フィルタリングは、HTTP フィルタリングとは異なり、サブジェクト共通名内のサブドメインを無視します。アクセス コントロールまたは QoS ポリシーで HTTPS URL を手動でフィルタリングする場合は、サブドメイン情報を含めないでください。たとえば、www.example.com ではなく、example.com を使用します。

また、HTTPS フィルタリングは URL リストもサポートしていません。代わりに、URL オブジェクトとグループを使用する必要があります。

ヒント SSL ポリシーでは、特定の URL に対するトラフィックの処理と復号は、識別名の SSL ルール条件を定義することで行えます。証明書のサブジェクト識別名にある共通名属性には、サイトの URL が含まれています。HTTPS トラフィックを復号することで、復号されたセッションをアクセス コントロール ルールによって評価できるようになり、URL フィルタリングの質が向上します。

暗号化プロトコルによるトラフィックの制御

アクセス コントロールまたは QoS ポリシー内で URL フィルタリングを実行する場合、暗号化プロトコル（HTTP または HTTPS）は無視されます。これは、手動およびレピュテーションベース両方の URL 条件で発生します。つまり、URL フィルタリングは、次の Web サイトへのトラフィックを同じように扱います。

- http://example.com/
- https://example.com/

HTTP または HTTPS トラフィックのみに一致するルールを設定するには、アプリケーション条件をルールに追加します。たとえば、あるサイトへの HTTPS アクセスを許可する一方で、HTTP アクセスを許可しないようにできます。そのためには、2 つのアクセス コントロール ルールを作成し、それぞれにアプリケーションと URL の条件を割り当てます。

最初のルールは Web サイトへの HTTPS トラフィックを許可します。

Action: Allow
Application: HTTPS
URL: example.com

2 番目のルールは同じ Web サイトへの HTTP アクセスをブロックします。

Action: Block
Application: HTTP
URL：example.com

カテゴリとレピュテーションを使用した URL フィルタリングの設定方法

	操作手順	詳細情報
ステップ 1	NGIPSv デバイスでカテゴリおよびレピュテーションベースの URL フィルタリングを使用する場合は、必要なメモリ量を割り当てます。	Cisco Firepower NGIPSv（VMware 向け）クイック スタート
ステップ 2	正しいライセンスがあることを確認します。	Firepower システムのライセンス （93 ページ）次のようなものがあります。 • Firepower Threat Defense デバイスの URL フィルタリング ライセンス （106 ページ） • 従来のデバイスの URL フィルタリング ライセンス （147 ページ） URL フィルタリング ライセンスを URL をフィルタ処理する各管理対象デバイスに割り当てます。 機能を有効にするには、そのデバイスに割り当てられた URL フィルタリング ライセンスが少なくても 1 台の管理対象デバイスにある必要があります。
ステップ 3：	Firepower Management Center はクラウドと通信して URL フィルタリング データを取得できることを確認します。	インターネット アクセス要件 （3281 ページ）、通信ポートの要件 （3284 ページ）
ステップ 4：	制限事項とガイドラインを理解し、必要なアクションを実行します。	URL フィルタリングのガイドラインと制限事項 （1719 ページ）
ステップ 5：	URL フィルタリング機能を有効にします。	カテゴリとレピュテーションを使用した URL フィルタリングの有効化 （1724 ページ）

	操作手順	詳細情報
ステップ 6：	カテゴリとレピュテーションによってURLをフィルタ処理するポリシーを設定します。	URL 条件の設定 （1726 ページ）
ステップ 7	（オプション）警告ページをクリック スルーすることで Web サイトのブロックをバイパスできるようにします。	HTTP応答ページとインタラクティブなブロッキング （1735 ページ）
ステップ 8	トラフィックがキールールに最初にヒットするようにルールを順序付けます。	URL ルールの順序 （508 ページ）
ステップ 9	（オプション）クラウドルックアップを必要とする URL の処理を変更します。	アクセス コントロール ポリシーの詳細設定 （1681 ページ）の [URLキャッシュミスルックアップを再試行する（Retry URL cache miss lookup）] オプションに関する情報。
ステップ 10	変更を展開します。	設定変更の展開 （447 ページ）
ステップ 11	システムが将来の URL データの更新を予想どおりに受信することを確認します。	URL フィルタリングのヘルス モニタの設定 （1729 ページ）

カテゴリとレピュテーションを使用したURLフィルタリングの有効化

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス（Access）
URL フィルタリング	URL フィルタリング	いずれか（Any）	いずれか（Any）	Admin

始める前に

カテゴリとレピュテーションを使用したURLフィルタリングの設定方法 （1723 ページ） で説明されている前提条件をすべて満たします。

ステップ 1 **[System]** > **[Integration]**を選択します。

ステップ 2 **[[Cloud Services]]** タブをクリックします。

ステップ 3 URL フィルタリング オプション （1725 ページ） を設定します。

ステップ 4 **[保存（Save）]** をクリックします。

URL フィルタリング オプション

次のオプションは、[システム（System）] > [統合（Integration）] ページにあります。

Enable URL Filtering

Web サイトの一般的な分類、カテゴリ、リスク レベル、またはレピュテーションに基づくトラフィックのフィルタリングを可能にします。URL フィルタリング ライセンスを追加すると、[URLフィルタンリングを有効にする（Enable URL Filtering）] が自動的に有効になります。URL フィルタリングは、他の URL フィルタリング オプションを選択する前に有効にする必要があります。

URL フィルタリングを有効にする場合は、URL フィルタリングが最後に有効になってから経過した時間に応じて、またはURL フィルタリングを今回初めて有効にするかどうかに応じて、Firepower Management Center が Cisco Collective Security Intelligence（Cisco CSI）から URL データをダウンロードします。このプロセスには、時間がかかる場合があります。

自動更新を有効にする（Enable Automatic Updates）

URL フィルタリング脅威データを更新するためのオプション。

- [システム（System）] > [統合（Integration）] ページの [自動更新を有効にする（Enable Automatic Updates）] オプションを有効にすると、Firepower Management Center は 30 分ごとにクラウドの更新をチェックします。 このオプションは、URL フィルタリング ライセンスを追加すると、デフォルトで有効になります。
- システムが外部リソースに接触する時間を厳格に制御する必要がある場合、このページの自動更新を無効にし、代わりにスケジューラを使用して定期的なタスクを作成します。スケジュール設定されたタスクを使用したURL フィルタリング更新の自動化（255 ページ）を参照してください。

[今すぐアップデート（Update Now）]

このダイアログ ボックスの上部にある [今すぐアップデート（Update Now）] ボタンをクリックすると、ワンタイムのオンデマンド更新を実行できますが、自動更新を有効にするか、スケジューラを使用して定期的なタスクを作成する必要があります。更新がすでに進行中である場合は、オンデマンド更新を開始できません。

通常、毎日の更新は小規模ですが、最終更新日から 5 日を超えると、帯域幅によっては新しい URL データのダウンロードに最長 20 分かかる場合があります。その後、更新自体を実行するのに最長で 30 分かかることがあります。

[不明 URL を Cisco Cloud に問い合わせる（Query Cisco Cloud for Unknown URLs）]

カテゴリとレピュテーションがローカル データセットにない Web サイトをユーザが閲覧するときに、脅威インテリジェンス評価のために URL がクラウドに送信されるようにします。プ

ライバシー上の理由などで未分類の URL を送信したくない場合は、このオプションを無効にしてください。

このオプションは、少なくとも 1 台の管理対象デバイスに有効な URL フィルタリング ライセンスがある場合にデフォルトで有効になります。

未分類の URL への接続は、カテゴリまたはレピュテーションベースの URL 条件を含むルールに一致**しません**。URL に手動でカテゴリやレピュテーションを割り当てることはできません。

暗号化されたトラフィックを SSL ルールを使用して処理する場合は、TLS/SSL ルールのガイドラインと制限事項 （1848 ページ）も参照してください。

キャッシュされた URL の期限切れ

この設定は、[不明 URL を Cisco CSI に問い合わせる（Query Cisco CSI for Unknown URL）][不明 URL を Cisco Cloud に問い合わせる（Query Cisco Cloud for Unknown URLs）] が有効になっている場合にのみ該当します。

カテゴリおよびレピュテーション データのキャッシングにより、Web ブラウジングが高速化されます。デフォルトでは、最速のパフォーマンスを得るため、URL のキャッシュされたデータの有効期限はありません。

古いデータと一致する URL のインスタンスを最小限に抑えるため、キャッシュ内の URL を期限切れに設定できます。脅威データの正確性と即時性を向上させるため、短い有効期限を選択します。

キャッシュされた URL は、指定された時間が経過した後、ネットワーク上のユーザが初めてアクセスした後に更新されます。最初のユーザに更新済みの結果は表示されませんが、この URL に次にアクセスしたユーザには更新済みの結果が表示されます。

URL データのキャッシングについては、Cisco Cloud からの URL フィルタリングのデータ （1719 ページ） を参照してください。

URL 条件の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス（Access）
URL フィルタリング（カテゴリ/レピュテーション） 任意（手動）	URL フィルタリング（カテゴリ/レピュテーション） 任意（手動）	いずれか（Any）	いずれか（Any）	Admin/Access Admin/Network Admin

URL 条件を作成するときに、トラフィックを制御する URL カテゴリを選択します。必要に応じて、URL カテゴリをレピュテーションで制約できます。

アクセス コントロールおよび QoS ルールでは、事前定義された URL オブジェクト、URL リストとフィード、および手動のルールごとの URL を使用して個々の URL をフィルタ処理する

こともできます。これらの URL はレピュテーションで制約できません。手動 URL フィルタリングは SSL ルールではサポートされません。その代わりに、識別名の条件を使用します。

ステップ 1 ルール エディタで、URL 条件のタブをクリックします。

- アクセス コントロールまたは QoS：[URL（URLs）] タブをクリックします。
- SSL：[カテゴリ（Categoy）] タブをクリックします。

ステップ 2 制御する URL を見つけて選択します。

- カテゴリ：URL カテゴリを選択するか、デフォルトの [任意（Any）] のままにします。アクセス コントロールまたは QoS ルールでは、[カテゴリ（Categoy）] サブタブをクリックしてカテゴリを選択します。
- URL オブジェクト、リスト、およびフィード：定義済みの URL オブジェクトおよび URL リストとフィードを選択します。アクセス コントロールまたは QoS ルールでは、[URL（URLs）] サブタブをクリックして URL を選択します。

ステップ 3 （オプション）レピュテーションを選択して URL カテゴリを制約します。

[未分類（Uncategorized）] URL を明示的に照合する場合は、未分類 URL にはレピュテーションがないため、レピュテーションによりさらに制約を追加することはできないことに注意してください。レピュテーション レベルを選択すると、ルール アクションに応じて、選択したレベルよりも重大または重大でない他のレピュテーションも含められます。

- [より重大でないレピュテーションを含める（Includes less severe reputations）]：ルールで Web トラフィックを許可または信頼する場合。たとえば、[無害なサイト（Benign Sites）]（レベル 4）を許可するようアクセス コントロール ルールを設定した場合、[ウェルノウン（Well Known）]（レベル 5）サイトも自動的に許可されます。
- [より重大なレピュテーションを含める（Includes more severe reputations）]：ルールで Web トラフィックをレート制限、復号、ブロック、またはモニタする場合。たとえば、[疑わしいサイト（Suspicious Sites）]（レベル 2）をブロックするようアクセス コントロール ルールを設定した場合、[高リスク（High Risk）]（レベル 1）のサイトも自動的にブロックされます。

ルール アクションを変更すると、URL 条件のレピュテーション レベルが自動的に変更されます。

ステップ 4 [ルールに追加（Add to Rule）] をクリックするか、ドラッグ アンド ドロップします。

ステップ 5 （オプション）アクセス コントロールまたは QoS ルールでは、URL を入力し、[追加（Add）] をクリックして、手動で指定する URL を追加します。

URL または IP アドレスを入力できます。このフィールドでは、ワイルドカードはサポートされません。

ステップ 6 ルールを保存するか、編集を続けます。

例：アクセス コントロール ルールの URL 条件

次の図は、すべてのマルウェア サイト、すべての [高リスク（High Risk）] サイト、およびすべての有害なソーシャル ネットワーキング サイト（）をブロックするアクセス コントロール ルールの URL 条件を示しています。また、単一サイト example.com（URL オブジェクトによって表されます）もブロックされます。

次の表では、条件を作成する方法を要約します。

ブロックする URL	カテゴリまたは URL オブジェクト	レピュテーション
マルウェア サイト（レピュテーションに関係なく）	Malware Sites	任意
高リスクの URL（レベル 1）	いずれか（Any）	1：[高リスク（High Risk）]
無害よりも大きいリスクがある（）ソーシャル ネットワーキング サイト（レベル 1 ～ 3）	Social Network	3：[セキュリティリスクのある無害なサイト（Benign sites with security risks）]
example.com	example.com という名前の URL オブジェクト	なし

次のタスク

- カテゴリとレピュテーションを使用した URL フィルタリングの設定方法（1723 ページ）に戻ってください。
- 変更を行った場合についてです。 設定変更を展開します。設定変更の展開（447 ページ）を参照してください。

URL 条件を伴うルール

次の表に、URL 条件をサポートするルールと、各ルール タイプがサポートするフィルタリングのタイプを一覧します。

ルール タイプ	カテゴリとレピュテーションフィルタリングをサポートしますか。	手動フィルタリングのサポート
アクセス コントロール	あり	あり
SSL	Yes	なし。代わりに識別名条件を使用
QoS	あり	あり

URL ルールの順序

URL マッチングを最も効果的に行うには、URL 条件を含むルールを他のルールより前に配置します。特に、URL ルールがブロック ルールで、他のルールが次の条件を両方とも満たす場合には、URL 条件を含むルールを前に配置します。

- その他のルールがアプリケーション条件を含んでいる。
- 検査対象のトラフィックが暗号化されている。

URL フィルタリングのヘルス モニタの設定

次のヘルス ポリシーは、システムに URL カテゴリとレピュテーション データを取得または更新に問題がある場合は通知します。

- URL フィルタリング モニタ
- デバイスでの脅威データの更新

これらが考えているとおりに設定されていることを確認するには、ヘルス モジュール （350 ページ）およびヘルス モニタリングの設定 （361 ページ）を参照します。

手動 URL フィルタリング

アクセス コントロール ルールおよび QoS ルールでは、個々の URL、URL のグループ、または URL のリストとフィードを手動でフィルタリングすることで、カテゴリとレピュテーション ベースの URL のフィルタリングを補足したり、選択的にオーバーライドしたりできます。

（注） 多数の URL をフィルタリングする場合、個別の、またはグループ化された URL オブジェクトを使用する代わりに、URL リストを使用します。詳細については、セキュリティ インテリジェンスのリストとフィード （557 ページ）を参照してください。

特殊なライセンスなしでこのタイプの URL フィルタリングを実行することができます。手動 URL フィルタリングは SSL ルールではサポートされません。その代わりに、識別名の条件を使用します。

たとえば、アクセス コントロールを使用して組織に適していない Web サイトのカテゴリをブロックできます。ただし、カテゴリに適切な Web サイトが含まれていて、そこにアクセスを提供する必要がある場合は、そのサイトに手動で許可ルールを作成し、カテゴリのブロック ルールの前に配置できます。

警告

特定の URL を手動でフィルタリングする場合は、影響を受ける可能性のある他のトラフィックを慎重に考慮してください。ネットワーク トラフィックが URL 条件に一致するかどうか判別するために、システムは単純な部分文字列マッチングを実行します。要求された URL が文字列の任意の部分に一致する場合、URL は一致するとみなされます。

例 1:

ign.com （ゲーム サイト）を明示的にブロックする必要があります。部分文字列マッチングにより ign.com 自体だけでなく verisign.com もブロックされることになり、意図しない動作が生じる可能性があります。

例 2：

example.com へのすべてのトラフィックを許可する場合、ユーザは次の URL サイトを参照できます。

- http://example.com/
- http://example.com/newexample
- http://www.example.com/

関連トピック

セキュリティ インテリジェンスのリストとフィード （557 ページ）

URL フィルタリングのトラブルシューティング

特定の URL のカテゴリとレピュテーションはどのようにしたら確認できますか。

手動ルックアップを実行します。URL カテゴリとレピュテーションの検索（2878 ページ）を参照してください。

手動ルックアップ試行時のエラー：「<URL> のクラウド ルックアップに失敗しました（Cloud Lookup Failure for <URL>）」

機能が適切に有効になっていることを確認します。URL カテゴリとレピュテーションの検索（2878 ページ）の前提条件を参照してください。

URL はその URL カテゴリとレピュテーションに基づいて誤って処理されたように見えます。

問題： システムはURL カテゴリとレピュテーションに基づいてURL を正しく処理しません。

対処方法:

- URL カテゴリと URL に関連付けられているレピュテーションが想定どおりであることを確認します。URL カテゴリとレピュテーションの検索 （2878 ページ）を参照してください。
- 次の問題は、カテゴリとレピュテーションを使用したURL フィルタリングの有効化 （1724 ページ）を使用してアクセスできる、URL フィルタリング オプション （1725 ページ）で説明した設定で対処できる場合があります。
  - URL キャッシュに古い情報が保存されている可能性があります。URL フィルタリング オプション （1725 ページ）の [キャッシュされたURLの期限切れ（Cached URLs Expire）] 設定に関する情報を参照してください。
  - クラウドからの最新情報でローカルのデータセットが更新されていない可能性があります。URL フィルタリング オプション （1725 ページ）の [自動更新を有効にする（Enable Automatic Updates）] 設定に関する情報を参照してください。
  - 最新のデータに関してクラウドを確認しないようにシステムが設定されている可能性があります。URL フィルタリング オプション （1725 ページ）の [不明 URL を Cisco CSI に問い合わせる（Query Cisco CSI for Unknown URL）][不明 URL を Cisco Cloud に問い合わせる（Query Cisco cloud for unknown URLs）] の設定に関する情報を参照してください。
- クラウドを確認せずに URL にトラフィックを渡すようにアクセス コントロール ポリシーが設定されている可能性があります。アクセス コントロール ポリシーの詳細設定 （1681 ページ） で、[URL キャッシュ ミス ルックアップを再試行する（Retry URL cache miss lookup）] 設定に関する情報を参照してください。
- URL フィルタリングのガイドラインと制限事項 （1719 ページ）も参照してください。
- SSL ルールを使用して URL を処理した場合は、TLS/SSL ルールのガイドラインと制限事項 （1848 ページ）およびSSL ルールの順序 （507 ページ）を参照してください。
- URL を処理している思われるアクセス制御ルールを使用して URL が処理されていることを確認し、アクセス制御ルールが想定どおりに機能していることを確認します。ルールの順序を考慮します。
- Firepower Management Center のローカル URL カテゴリおよびレピュテーション データベースがクラウドから正常に更新されており、管理対象デバイスが Firepower Management Center から正常に更新されていることを確認します。

  これらのプロセスのステータスは、[URL フィルタリング モニタ（URL Filtering Monitor）] モジュールおよび [デバイスでの脅威データの更新（Threat Data Updates on Devices）] モジュールのヘルス モニタでレポートされます。詳細は、ヘルス モニタリング （349 ページ）を参照してください。

ローカルURLカテゴリおよびレピュテーションデータベースを即座に更新する場合、**[System]** > **[Integration]** に移動し、**[Cloud Services]** タブをクリックしてから [今すぐアップデート（Update Now）] をクリックします。詳細については、URL フィルタリング オプション （1725 ページ）を参照してください。

URL カテゴリまたはレピュテーションが正しくありません

アクセス コントロールまたは QoS ルールの場合：ルールの順序に細心の注意を払って、手動フィルタリングを使用します。手動URL フィルタリング （1729 ページ）およびURL 条件の設定 （1726 ページ）を参照してください。

SSL ルールの場合：手動フィルタリングはサポートされていません。代わりに識別名条件を使用します。

Web ページのロードに時間がかかる

セキュリティとパフォーマンスのトレードオフがあります。いくつかのオプションを次に示します。

- [キャッシュされたURLの期限切れ（Cached URLs Expire）] 設定の変更を検討します。**[System]** > **[Integration]** をクリックしてから、**[Cloud Services]** タブを選択します。詳細については、URL フィルタリング オプション （1725 ページ）を参照してください。
- アクセス コントロール ポリシーの詳細設定 （1681 ページ）の [URL キャッシュのミス検索の再試行（Retry URL cache miss lookup）] 設定の選択解除を検討します。

イベントに URL カテゴリおよびレピュテーションは含まれていません

- アクセス コントロール ポリシーに適用可能な URL ルールが含まれていること、ルールがアクティブになっていること、およびポリシーが関連するデバイスに展開されていることを確認します。
- URL ルールと一致する前に接続が処理される場合、URL カテゴリとレピュテーションはイベントに表示されません。

URL フィルタリングの履歴

機能	バージョン	詳細
[Cisco CSI] タブの名前が [クラウド サービス（Cloud Services）] に変更されました。	6.4	変更された画面と移動：[システム（System）] > [統合（Integration）] > [Cisco CSI] は [システム（System）] > [統合（Integration）] > [クラウド サービス（Cloud Services）] になりました。 サポート対象プラットフォーム: FMC

機能	バージョン	詳細
URL フィルタリング情報をさまざまな場所から新しい URL フィルタリングの章に移動しました。	6.3	URL フィルタリングのクラウド通信の設定に関する情報を新しい URL フィルタリングの章に移動しました。その他の特定の URL フィルタリングの情報をこの章の他の場所に移動しました。章内の Cisco CSI のトピックの構成に関連する変更を加えました。
新規オプション：キャッシュされた URL の期限切れ	6.3	この新しいコントロールを使用して、古いデータで一致している URL のインスタンスを最小限に抑えるため、新しい URL カテゴリおよびレピュテーションとパフォーマンスとのバランスを取ります。 変更された画面：[システム（System）] > [統合（Integration）] > [Cisco CSI]。 サポート対象プラットフォーム：すべて
変更されたメニュー パス	6.3	[手動 URL ルックアップ（Manual URL Lookup）] へのパスが [分析（Analysis）] > [ルックアップ（Lookup）] > [URL] から [分析（Analysis）] > [詳細（Advanced）] > [URL] に変更されました。

第 66 章

HTTP 応答ページとインタラクティブなブロッキング

ここでは、システムが Web 要求をブロックしたときに表示されるカスタム ページの設定方法について説明します。

HTTP 応答ページについて

アクセス制御の一部として、アクセス コントロール ルールあるいはアクセス コントロール ポリシーのデフォルト アクションを使って、システムが Web リクエストをブロックしたときに表示する *HTTP* 応答ページを設定できます。

表示される応答ページは、セッションのブロック方法によって異なります。

- **ブロック応答ページ**により、接続が拒否されたことを示すデフォルトのブラウザ ページまたはサーバ ページは上書きされます。
- [インタラクティブ ブロック応答（Interactive Block Response）] ページ：ユーザに警告しますが、ユーザはボタンをクリック（あるいはページを更新）して要求したサイトをロードできます。応答ページをバイパスした後、ロードされなかったページの要素をロードするために、ページを最新表示しなければならない場合があります。

応答ページを選択していない場合、インタラクションや説明なしでシステムはセッションをブロックします。

HTTP 応答ページの制限

応答ページはアクセス制御のルール/デフォルト アクションのみ

システムは、アクセス制御ルールまたはアクセス制御ルールのデフォルトアクションのいずれかによってブロックされた（またはインタラクティブにブロックされた）暗号化されていないか、または復号された HTTP/HTTPS 接続の場合にのみ、応答ページを表示します。システムは、他のポリシーまたはメカニズムによってブロックされたか、またはブラックリストに掲載されている接続の応答ページは表示しません。

応答ページによる接続リセットの無効化の表示

システムは、接続がリセットされた場合（RSTパケットが送信）された場合は、応答ページを表示できません。応答ページを有効にすると、システムその接続を優先します。[リセットしてブロック（Block with reset）] または [リセットしてインタラクティブ ブロック（Interactive Block with reset）] をルール アクションとして選択した場合、システムは応答ページを表示し、一致する Web 接続をリセットしません。ブロックされた Web 接続のリセットを確認するには、応答ページを無効にする必要があります。

ルールに一致する Web 以外のすべてのトラフィックがリセットによりブロックされます。

暗号化された接続の応答ページなし（複合が必要）

アクセス制御ルール（または、その他の設定）によってブロックされている暗号化された接続の場合、システムは応答ページを表示しません。アクセス制御ルールはSSLポリシーを設定しなかった場合に暗号化された接続を評価し、それ以外の場合は、SSLポリシーが暗号化されたトラフィックを受け渡します。

たとえば、システムはHTTP/2 またはSPDY セッションを復号できません。これらのプロトコルのいずれかを使用して暗号化された Web トラフィックがアクセス制御ルールの評価に達したが、セッションがブロックされている場合、システムは応答ページを表示しません。

ただし、システムは、SSLポリシーによって復号された後に、アクセス制御ルールまたはアクセス制御ルールのデフォルトアクションのいずれかによってブロックされた（またはインタラクティブにブロックされた）接続の場合に、応答ページを表示します。このような場合、システムは応答ページを暗号化して、再暗号化されたSSLストリームの最後にそれを送信します。

「昇格した」接続の応答ページなし

Web トラフィックがプロモートされたアクセス制御ルール（単純なネットワーク条件のみの早期に適用されたブロッキングルール）の結果としてブロックされている場合、システムは応答ページを表示しません。

特定のリダイレクトされた接続の応答ページなし

URLが「http」または「https」を指定せずに入力され、ブラウザがポート80で接続を開始し、ユーザが応答ページをクリックスルーし、その後、接続がポート443にリダイレクトされる場

合、この URL への応答はすでにキャッシュされているため、ユーザには 2 番目のインタラクティブな応答ページが表示されません。

URL 識別の前に応答ページなし

システムは、システムが要求された URL を識別する前にトラフィックがブロックされた場合は、応答ページを表示しません。URL フィルタリングのガイドラインと制限事項 （1719 ページ）を参照してください。

HTTP 応答ページの選択

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Access Admin/Network Admin

HTTP応答ページを確実に表示できるかは、ネットワーク設定、トラフィック負荷、およびページのサイズによって異なります。ページが小さいほど、正常に表示される傾向にあります。

ステップ 1 アクセス コントロール ポリシーのエディタで、[HTTP 応答（HTTP Responses）] タブをクリックします。

コントロールが淡色表示されている場合、設定は先祖ポリシーから継承され、設定を変更する権限がありません。 設定がロック解除されている場合は、[Inherit from base policy] をオフにして、編集を有効にします。

ステップ 2 [応答ページをブロック（Block Response Page）]および[応答ページのインタラクティブブロック（Interactive Block Response Page）] を選択します。

- [System-provided]：一般的な応答が表示されます。表示アイコン（）をクリックすると、このページのコードが表示されます。
- [Custom]：カスタム応答ページが作成されます。ポップアップ ウィンドウが表示されます。このウィンドウに事前入力されているシステムによって提供されるコードを編集アイコン（）をクリックして置換または変更できます。カウンタで使用した文字数が表示されます。
- [None]：応答ページを無効にして、インタラクションや説明なしでセッションをブロックします。アクセス コントロール ポリシー全体でインタラクティブ ブロッキングを無効にするには、このオプションを選択します。

ステップ 3 [保存（Save）] をクリックして、ポリシーを保存します。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

HTTP 応答ページでのインタラクティブ ブロッキング

インタラクティブブロッキングを設定すると、ユーザは警告を読んだ後に当初要求したサイトを読み込むことができます。応答ページをバイパスした後、ロードされなかったページの要素をロードするために、ページを最新表示しなければならない場合があります。

ヒント　アクセス コントロール ポリシー全体に対してインタラクティブ ブロッキングを素早く無効にするには、システム提供のページもカスタムページも表示しないでください。そうすると、システムにより操作なしですべての接続がブロックされます。

ユーザがインタラクティブ ブロックをバイパスしない場合、一致するトラフィックは拒否され、追加のインスペクションは行われません。ユーザがインタラクティブブロックをバイパスするとアクセス コントロール ルールはトラフィックを許可しますが、引き続きトラフィックはディープ インスペクションやブロッキングの対象となる場合があります。

デフォルトでは、ユーザのバイパスは後続のアクセスで警告ページを表示することなく、10分（600 秒）間有効です。期間を 1 年に設定したり、ユーザに毎回ブロックをバイパスするように強制できます。この制限は、ポリシー内のすべてのインタラクティブ ブロック ルールに適用されます。ルールごとに制限を設定することはできません。

インタラクティブ ブロックされるトラフィックに関するロギング オプションは、許可されたトラフィックに関するオプションと同じですが、ユーザがインタラクティブブロックをバイパスしない場合、システムがログに記録できるのは接続開始イベントだけです。システムが最初にユーザに警告すると、ロギングされた接続開始イベントはシステムにより [インタラクティブ ブロック（Interactive Block）] または [リセットしてインタラクティブ ブロック（Interactive Block with reset）] アクションでマークされます。ユーザがブロックをバイパスすると、セッションが記録される追加の接続イベントに [許可（Allow）] アクションが付きます。

インタラクティブ ブロッキングの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin Access Admin Network Admin

ステップ 1　アクセス コントロールの一部として、Web トラフィックと一致するアクセス コントロール ルールを設定します。アクセス コントロール ルールの作成および編集 （1698 ページ）を参照してください。

- アクション：ルール アクションを [インタラクティブ ブロック（Interactive Block）]、または [リセットしてインタラクティブ ブロック（Interactive Block with reset）] に設定します。アクセス コントロール ルール インタラクティブ ブロック アクション （1702 ページ）を参照してください。

- 条件：URL条件を使用して、インタラクティブにブロックするWebトラフィックを指定します。URL条件（URL フィルタリング）（489 ページ）を参照してください。
- ロギング：ユーザがブロックをバイパスすると想定し、それに応じてロギング オプションを選択します。許可された接続のロギング（3008 ページ）を参照してください。
- インスペクション：ユーザがブロックをバイパスすると想定し、それに応じてディープ インスペクション オプションを選択します。侵入ポリシーとファイル ポリシーを使用したアクセス制御（1707 ページ）を参照してください。

ステップ 2 （オプション）アクセス コントロール ポリシーの [HTTP 応答（HTTP Responses）] タブで、カスタム インタラクティブ ブロックの HTTP 応答ページを選択します。HTTP 応答ページの選択（1737 ページ）を参照してください。

ステップ 3 （オプション）アクセス コントロール ポリシーの [詳細（Advanced）] タブで、ユーザのバイパス タイムアウトを変更します。ブロックされた Web サイトのユーザ バイパス タイムアウトの設定（1739 ページ）を参照してください。

ユーザはブロックをバイパスした後、そのページを参照でき、タイムアウト期間が経過するまで警告は表示されません。

ステップ 4 アクセス コントロール ポリシーを保存します。

ステップ 5 設定変更を展開します。設定変更の展開（447 ページ）を参照してください。

ブロックされた Web サイトのユーザ バイパス タイムアウトの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Access Admin/Network Admin

ステップ 1 アクセス コントロール ポリシー エディタで、[詳細（Advanced）] タブをクリックします。

ステップ 2 [全般設定（General Settings）] の横にある編集アイコン（  ）をクリックします。

代わりに表示アイコン（  ）が表示される場合、設定は先祖ポリシーから継承され、設定を変更する権限がありません。設定がロック解除されている場合は、[Inherit from base policy] をオフにして、編集を有効にします。

ステップ 3 [ブロックをバイパスするためのインタラクティブ ブロックを許可する期間（秒）（Allow an Interactive Block to bypass blocking for (seconds)）] フィールドに、ユーザ バイパスの期限が切れるまでの経過時間を秒数で入力します。ゼロを指定すると、ユーザはブロックを毎回強制的にバイパスします。

ステップ 4 [OK] をクリックします。

ステップ 5 [保存（Save）] をクリックしてポリシーを保存します。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

第 67 章

セキュリティ インテリジェンス ブラックリスト

以下のトピックでは、セキュリティインテリジェンスの概要（トラフィックのブラックリストとホワイトリストの使用、基本設定など）を示します。

セキュリティ インテリジェンスについて

悪意のあるインターネットコンテンツに対する防御の前線として、セキュリティインテリジェンスは疑わしい IP アドレス、URL、ドメイン名が関連する接続をレピュテーション インテリジェンスを使用して迅速にブロックします。これは、セキュリティ インテリジェンス ブラックリスト登録と呼ばれます。

セキュリティインテリジェンスはアクセス制御の初期のフェーズであり、大量のリソースを消費する評価をシステムが実行する前に行われます。ブラックリスト登録により、インスペクションの必要がないトラフィックを迅速に除外することで、パフォーマンスが向上します。

（注） FastPath が適用されたトラフィックをブラックリストに登録することはできません。8000 シリーズの FastPath 適用およびプレフィルタ評価は、セキュリティインテリジェンスによるフィルタリングの前に行われます。FastPath が適用されたトラフィックは、セキュリティインテリジェンスを含め、以降のすべての評価をバイパスします。

カスタム ブラックリストを設定することはできますが、CIsco は定期的に更新されるインテリジェンスフィードへのアクセスを提供しています。マルウェア、スパム、ボットネット、フィッシングなど、セキュリティに対する脅威を表すサイトは目まぐるしく現れては消えるため、カスタム設定を更新して導入するのでは最新の状況に追いつきません。

セキュリティインテリジェンスのブラックリスト登録を改良するには、ホワイトリストとモニタ専用ブラックリストを併せて使用するという方法があります。これらのメカニズムは、トラフィックをブラックリストに登録しないようにしますが、一致するトラフィックを自動的に信頼したりFastPathを適用したりすることは**しません**。ホワイトリストに登録されたトラフィックや、セキュリティインテリジェンスの段階でモニタされるトラフィックは、意図的に残りのアクセス コントロールによる分析が適用されます。

関連トピック

セキュリティ インテリジェンスのリストとフィード （557 ページ）
ログ可能なその他の接続 （3003 ページ）
接続およびセキュリティ インテリジェンス イベント テーブルの使用 （3050 ページ）

セキュリティ インテリジェンスのための要件

特定の IP アドレス、URL、ドメイン名をホワイトリストまたはブラックリストに登録したりモニタしたりするためには、カスタム オブジェクト、リスト、またはフィードを設定する必要があります。次の選択肢があります。

- ネットワーク、URL、DNS フィールドを設定するには、セキュリティ インテリジェンス フィードの作成 （564 ページ）を参照してください。
- ネットワーク、URL、DNS リストを設定するには、セキュリティ インテリジェンス リストの更新 （568 ページ）を参照してください。
- ネットワーク オブジェクトとオブジェクト グループを設定するには、ネットワーク オブジェクトの作成 （527 ページ）を参照してください。
- URL オブジェクトとオブジェクト グループを設定するには、URL オブジェクトの作成 （533 ページ）を参照してください。

DNS リストまたはフィードに基づくトラフィックのブラックリスト/ホワイトリスト登録あるいはモニタリングには、以下の条件もあります。

- DNS ポリシーを作成します。詳細については、基本 DNS ポリシーの作成 （1753 ページ）を参照してください。
- DNS リストまたはフィードを参照する DNS ルールを設定します。詳細については、DNS ルールの作成および編集 （1756 ページ）を参照してください。

DNS ポリシーはアクセス コントロール ポリシーの一部として展開するため、両方のポリシーを関連付ける必要があります。詳細については、「DNS ポリシーの展開 （1764 ページ）」を参照してください。

セキュリティ インテリジェンスのガイドライン

セキュリティ インテリジェンス戦略では、次の要素を使用します。

- Cisco 提供のフィード：Cisco では、定期的に更新されるインテリジェンス フィードへのアクセスを提供しています。マルウェア、スパム、ボットネット、フィッシングなど、セキュリティに対する脅威を表すサイトは目まぐるしく現れては消えるため、カスタム設定を更新して導入するのでは最新の状況に追いつきません。
- サードパーティのフィード：Cisco 提供のフィードをサードパーティのフィードで補完できます。これらのフィードは、Firepower Management Center が定期的にインターネットからダウンロードする動的リストです。
- グローバルおよびカスタム ブラックリスト：特定の IP アドレス、URL、ドメイン名をブラックリストに登録します。パフォーマンスを向上させるために、スパムのブラックリスト登録を電子メール トラフィックを処理するセキュリティ ゾーンに制限するなどして、適用対象を絞り込むこともできます。
- 誤検出をなくすためのホワイトリスト：ブラックリストの範囲が広すぎる場合、または残りのアクセス コントロールでさらに分析するトラフィックを前もってブロックしてしまう場合は、ブラックリストをカスタム ホワイトリストでオーバーライドできます。
- ブラックリスト登録に代わるモニタリング：特にパッシブ展開や、フィードを実装する前にテストする場合に有用です。違反しているセッションをブロックする代わりに単にモニタしてログに記録し、接続終了イベントを生成できます。

（注） パッシブ展開環境では、パフォーマンスを最適化するために、モニタ専用の設定を使用することを推奨しています。パッシブに展開された管理対象デバイスはトラフィック フローに影響を与えることができないため、トラフィックをブロックするようにシステムを構成しても何のメリットもありません。また、ブロックされた接続はパッシブ展開で実際にはブロックされないため、システムにより、ブロックされた各接続に対し複数の接続開始イベントが報告される場合があります。

例：ホワイトリスト登録

信頼できるフィードにより、重要なリソースへのアクセスが不適切にブロックされたものの、そのフィードが全体としては組織にとって有用である場合は、そのフィード全体をブラックリストから削除するのではなく、不適切に分類された IP アドレスだけをホワイトリストに登録するという方法を取ることができます。

例：ゾーンを使用したセキュリティ インテリジェンス

不適切に分類された IP アドレスをホワイトリストに登録した後、組織内でそれらの IP アドレスにアクセスする必要があるユーザが使用しているセキュリティ ゾーンによりホワイトリストのオブジェクトを制限するという方法が考えられます。この方法では、ビジネス ニーズを持つユーザだけが、ホワイトリストに登録された URL にアクセスできます。あるいは、サードパーティのスパム フィードを使用して、電子メール サー

バのセキュリティ ゾーンのトラフィックをブラックリスト登録するという方法もあります。

例：モニタ専用のブラックリスト登録

たとえば、サードパーティのフィードを使用したブロッキングを実装する前に、そのフィードをテストする必要があるとします。フィードをモニタ専用に設定すると、ブロックされるはずの接続をシステムで詳細に分析できるだけでなく、そのような接続のそれぞれをログに記録して、評価することもできます。

セキュリティ インテリジェンスの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Access Admin/Network Admin

各アクセス コントロール ポリシーには、セキュリティ インテリジェンス オプションがあります。ネットワーク オブジェクト、URL オブジェクトとリスト、およびセキュリティ インテリジェンス フィードとリストをホワイトリストまたはブラックリストに追加でき、これらはすべてセキュリティ ゾーンによって制約できます。アクセス コントロール ポリシーに DNS ポリシーを関連付け、ドメイン名をホワイトリストまたはブラックリストに追加することもできます。

ホワイトリスト内のオブジェクトの数とブラックリスト内の数の合計が、255 個のネットワーク オブジェクトまたは 32767 個の URL オブジェクトとリストを超えることはできません。

（注） システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。 上書き対応オブジェクトを使用すると、子孫ドメインの管理者は、グローバル コンフィギュレーションを自分のローカル環境に調整できます。

始める前に

- すべてのオプションを選択できるようにするには、少なくとも 1 つの管理対象デバイスを Management Center に追加します。
- パッシブ展開の場合、またはモニタのみにセキュリティ インテリジェンス フィルタリングを設定する場合は、ロギングを有効にします。セキュリティインテリジェンスによる接続のロギング （3016 ページ）を参照してください。

ステップ 1 アクセス コントロール ポリシー エディタで、[セキュリティ インテリジェンス（Security Intelligence）] タブをクリックします。

コントロールが淡色表示されている場合、設定は先祖ポリシーから継承され、設定を変更する権限がありません。 設定がロック解除されている場合は、[Inherit from base policy] をオフにして、編集を有効にします。

ステップ 2 次の選択肢があります。

- [ネットワーク（Networks）] タブをクリックして、ネットワーク オブジェクトを追加します。
- [URL（URLs）] タブをクリックして、URL オブジェクトを追加します。

ステップ 3 ホワイトリストまたはブラックリストに追加する利用可能なオブジェクトを探します。次の選択肢があります。

- [名前または値で検索（Search by name or value）] フィールドに入力して、利用可能なオブジェクトを検索します。[リロード（reload）]（）または [クリア（clear）]（）をクリックして、検索文字列をクリアします。
- 既存のリストまたはフィードがニーズを満たしていない場合は、追加アイコン（）をクリックし、[新規ネットワーク リスト（New Network List）] または [新規 URL リスト（New URL List）] を選択し、セキュリティ インテリジェンス フィードの作成（564 ページ）または新しいセキュリティ インテリジェンス リストの Firepower Management Center へのアップロード（567 ページ）の説明に従って続行します。
- 既存のオブジェクトがニーズを満たしていない場合は、追加アイコン（）をクリックし、[新規ネットワーク オブジェクト（New Network Object）] または [新規 URL オブジェクト（New URL Object）] を選択し、ネットワーク オブジェクトの作成（527 ページ）の説明に従って続行します。

セキュリティ インテリジェンスは、/0 ネットマスクを使用して、IP アドレス ブロックを無視します。

ステップ 4 追加する 1 つ以上の**利用可能なオブジェクト**を選択します。

ステップ 5 （オプション）[利用可能なゾーン（Available Zone）] を選択して、選択したオブジェクトをゾーンごとに制約します。

システムが提供するセキュリティ インテリジェンス リストをゾーンで制約することはできません。

ステップ 6 [ホワイトリストに追加（Add to Whitelist）] または [ブラックリストに追加（Add to Blacklist）] をクリックするか、選択したオブジェクトをクリックしていずれかのリストにドラッグします。

ホワイトリストまたはブラックリストからオブジェクトを削除するには、その削除アイコン（）をクリックします。複数のオブジェクトを削除するには、オブジェクトを選択し、右クリックして [選択項目の削除（Delete Selected）] を選択します。

ステップ 7 （オプション）ブラックリスト登録されたオブジェクトをモニタ専用に設定するには、[ブラックリスト（Blacklist）]にリストされている該当するオブジェクトを右クリックし、[モニタ専用（ブロックしない）（Monitor-only (do not block)）] を選択します。

システムが提供するセキュリティ インテリジェンス リストをモニタ専用に設定することはできません。

ステップ 8 [DNS ポリシー（DNS Policy）] ドロップダウン リストから DNS ポリシーを選択します。DNS ポリシーの概要 （1751 ページ） を参照してください。

ステップ 9 **[保存（Save）]** をクリックします。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

関連トピック

セキュリティ インテリジェンスのリストとフィード （557 ページ）
Snort® の再起動シナリオ （450 ページ）

セキュリティ インテリジェンス オプション

アクセス制御ポリシーエディタのセキュリティインテリジェンスタブを使用して、ネットワーク（IP アドレス）と URL セキュリティ インテリジェンスを設定し、アクセス制御ポリシーを DNS ポリシーに関連付けます。

オブジェクト、ゾーン、ブラックリスト アイコン

アクセス制御ポリシー エディタのセキュリティ インテリジェンス タブで、オブジェクトまたはゾーンのそれぞれのタイプを別のアイコンと区別します。

ブラックリストでは、ブロックに設定したオブジェクトにはブロック アイコン（  ）を付け、監視対象のみのオブジェクトには、監視アイコン（  ）を付けます。監視のみの場合には、アクセス制御を使用して、ブラックリストの IP アドレスと URL を含む接続を処理し、ブラックリストに一致する接続をロギングします。

ホワイトリストがブラックリストをオーバーライドするため、両方のリストに同じオブジェクトを追加すると、ブラックリスト登録されたオブジェクトに取り消し線が表示されます。

設定されている場合、TID は、アクションの優先順位付けに影響を与えます。詳細については、TID-Firepower Management Center のアクションの優先順位付け （1994 ページ）を参照してください。

ゾーンの制約

システムが提供したグローバル リスト以外、ゾーンごとにセキュリティ インテリジェンス フィルタリングを制約できます。複数のゾーンでオブジェクトのセキュリティ インテリジェンス フィルタリングを適用するには、ゾーンのそれぞれについて、オブジェクトをホワイトリストまたはブラックリストに追加する必要があります。

ログ

デフォルトで有効になっているセキュリティ インテリジェンス ロギングは、アクセス制御ポリシー対象のデバイスが処理するブロックされ、監視対象である接続はすべてロギングされます。ただし、システムはホワイトリストの一致はロギングしません。ホワイトリストに登録された接続のロギングは、その接続の最終的な傾向によって異なります。ブラックリストの接続については、ブラックリスト対象のオブジェクトを監視のみに設定する前にロギングを有効にする必要があります。

セキュリティ インテリジェンス カテゴリ

これらのカテゴリは、アクセス コントロール ポリシーの [セキュリティインテリジェンス（Security Intelligence）] タブの [利用可能なオブジェクト（Available Objects）] の下にある [ネットワーク（Networks）] タブに表示されます。

（注） 組織で Cisco Threat Intelligence Director（TID）を使用している場合：イベントを表示すると、アクションが TID によって実行されたことを示すカテゴリ（`TID URL ブロック`など）が表示されることがあります。

セキュリティ インテリジェンス カテゴリ	説明
Attacker	アクティブ スキャナと悪意のある発信アクティビティが知られているブラックリストのホスト。
Bogon	Bogon ネットワークおよび割り当てられていない IP アドレス
Bots	バイナリ マルウェア ドロッパをホストするサイト
CnC	botnets 用のホスト C & C サーバを有するサイト
Dga	C & C サーバのランデブー ポイントとして機能するさまざまなドメイン名を生成するために使用されるマルウェア アルゴリズム
Exploitkit	クライアントのソフトウェアの脆弱性を特定するために設計されたソフトウェア キット
Malware	マルウェアバイナリまたはエクスプロイト キットを有するサイト
OpenProxy	匿名 Web ブラウジングを許可するオープン プロキシ
OpenRelay	スパム用に使用されることが既知のオープン メール リレー
Phishing	フィッシングページを有するサイト
応答	悪意があるか疑わしいアクティブに積極的に参加している IP アドレスと URL

セキュリティインテリジェンス カテゴリ	説明
Spam	スパムを送信することが知られているメール ホスト
Suspicious	疑いがあり、既知のマルウェアと同様の特性を持つようなファイル
TorExitNode	Tor exit ノード

関連トピック

[今すぐブラックリストに登録（Blacklist Now）]、[今すぐホワイトリストに登録（Whitelist Now）]、およびグローバル リスト （560 ページ）
セキュリティ インテリジェンス リストとマルチテナンシー （561 ページ）

セキュリティインテリジェンスのトラブルシューティング

セキュリティインテリジェンスのカテゴリが使用可能なオプションのリストに表示されない

症状：アクセス コントロール ポリシーの [セキュリティインテリジェンス（Security Intelligence）] タブで、[利用可能なオプション（Available Options）] の下にある [ネットワーク（Networks）] タブにセキュリティ インテリジェンス カテゴリ（CnC や Exploitkit など）が表示されない。

原因：Management Center に少なくとも 1 つの管理対象デバイスが追加されるまで、これらのオプションは表示されません。すべての TALOS フィードを取得するには、デバイスを追加する必要があります。

メモリ使用のトラブルシューティング

症状：セキュリティ インテリジェンスによってブラックリストに登録される必要がある接続が、代わりにアクセス コントロール ルールによって評価されます。セキュリティ インテリジェンスのヘルス モジュールにより、メモリ不足であることが警告されています。

原因：メモリの制限です。シスコのインテリジェンス フィードは、Cisco Talos Intelligence Group（Talos）の最新の脅威インテリジェンスに基づいています。このフィードは、時間が経つにつれてサイズが大きくなる傾向があります。FirePOWER デバイスがフィード更新を受信すると、セキュリティ インテリジェンス用に割り当てられたメモリに可能な限り多くのエントリがロードされます。デバイスがすべてのエントリをロードできない場合は、想定どおりにトラフィックがブロックされないことがあります。ブラックリストに登録する必要がある一部の接続は、代わりに引き続きアクセス コントロール ルールによって評価されます。

影響を受けるプラットフォーム：低メモリ デバイスでは、特に多数のセキュリティ インテリジェンス カテゴリをブラックリストに登録している場合や、カテゴリおよびレピュテーションに基づいて URL をフィルタリングしている場合に、この問題が発生する可能性が高くなります。これらのデバイスには、Firepower 7010、7020、および 7030、ASA5508-X、5516-X、5515-X、および 5525-X、NGIPSv が含まれます。

回避策：この問題が発生していると思われる場合は、影響を受けるデバイスに設定を再展開します。これにより、セキュリティ インテリジェンスにより多くのメモリを割り当てることができます。問題が解決しない場合は、Cisco Technical Assistance Center（TAC）にお問い合わせください。問題の確認と、展開に適したソリューションの提案に役立つことができます。

第 68 章

DNS ポリシー

次のトピックでは、DNS ポリシーと DNS ルールについて、および管理対象デバイスに DNS ポリシーを導入する方法について説明します。

DNS ポリシーの概要

DNS ベースのセキュリティ インテリジェンスにより、クライアントが要求したドメイン名に基づいて、トラフィックをホワイトリスト/ブラックリストに登録できるようになります。シスコが提供するドメイン名のインテリジェンスを使用して、トラフィックをフィルタリングできます。また、環境に合わせて、ドメイン名のカスタム リストやフィードを設定することも可能です。

DNS ポリシーによってブラックリスト登録されたトラフィックは即座にブロックされるため、他のさらなるインスペクションの対象にはなりません（侵入、エクスプロイト、マルウェアなどについてだけでなくネットワーク検出についても）。ブラックリストをホワイトリストで上書きしてアクセス コントロール ルールによる評価を強制することができます。また、セキュリティ インテリジェンス フィルタリングに「モニタ専用」設定を使用でき、パッシブ展開環境ではこの設定が推奨されます。この設定では、ブラックリスト登録されたであろう接続をシステムが分析できるだけでなく、ブラックリストに一致する接続がログに記録され、接続終了セキュリティ インテリジェンス イベントが生成されます。

（注） 期限切れのため、またはクライアントの DNS キャッシュやローカル DNS サーバのキャッシュがクリアされているか、期限切れであるために、DNS サーバでドメイン キャッシュが削除されない場合に、DNS ベースのセキュリティ インテリジェンスが意図したとおりに機能しないことがあります。

DNS ポリシーおよび関連付けられた DNS ルールを使用して DNS ベースのセキュリティ インテリジェンスを設定します。デバイスにこれを展開するには、アクセス コントロール ポリシーに DNS ポリシーを関連付けてから管理対象デバイスに設定を展開する必要があります。

DNS ポリシーのコンポーネント

DNSポリシーにより、ドメイン名に基づいて、接続をホワイトリストまたはブラックリストに登録できます。以下のリストでは、DNS ポリシーの作成後に変更できる設定を説明しています。

名前と説明

各 DNS ポリシーには一意の名前が必要です。説明は任意です。

マルチドメイン展開では、ポリシー名をドメイン階層内で一意にする必要があります。システムは、現在のドメインでは表示できないポリシーの名前との競合を特定することができます。

ルール

ルールは、ドメイン名に基づいてネットワーク トラフィックを処理するための詳細な方法を提供します。DNS ポリシーのルールには 1 から始まる番号が付いています。システムは、ルール番号の昇順で、DNS ルールを上から順にトラフィックと照合します。

DNS ポリシーを作成すると、システムはこれをデフォルトのグローバル DNS ホワイトリスト ルールおよびデフォルトのグローバル DNS ブラックリスト ルールに入力します。両方のルールは、それぞれのカテゴリで先頭の位置に固定されます。これらのルールは変更できませんが無効にすることはできます。

マルチドメイン展開では、子孫 DNS ホワイトリスト ルールおよび子孫 DNS ブラックリスト ルールも先祖ドメインの DNS ポリシーに追加されます。これらのルールは、それぞれのカテゴリの 2 番目の位置に固定されます。

（注） Firepower Management Center でマルチテナンシーが有効になっている場合、システムは先祖ドメインと子孫ドメインを含むドメインの階層に編成されます。これらのドメインは、DNS 管理で使用されるドメイン名とは別になります。

子孫のリストには、Firepower システムのサブドメイン ユーザによってホワイトリストまたはブラックリストに登録されたドメインが含まれます。先祖ドメインから、子孫のリストの内容を表示することはできません。サブドメイン ユーザをホワイトリストまたはブラックリストに登録しない場合は、次を実行します。

- 子孫のリストのルールを無効にします。
- アクセス コントロール ポリシーの継承設定を使用してセキュリティ インテリジェンスを適用します。

ルールはシステムにより次の順序で評価されます。

- グローバル DNS ホワイトリスト ルール（有効な場合）
- 子孫 DNS ホワイトリスト ルール（有効な場合）
- ホワイトリスト ルール
- グローバル DNS ブラックリスト ルール（有効な場合）
- 子孫 DNS ブラックリスト ルール（有効な場合）
- ブラックリスト ルールおよびモニタ ルール

通常、システムによるDNベースのネットワーク トラフィックの処理は、すべてのルールの条件がトラフィックに一致する最初の DNS ルールに従って行われます。トラフィックに一致する DNS ルールがない場合、システムは、関連付けられたアクセス コントロール ポリシー ルールに基づいてトラフィックの評価を続行します。DNS ルール条件は単純または複雑のどちらでも構いません。

基本 DNS ポリシーの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Access Admin/Network Admin

ステップ 1 **[Policies]** > **[Access Control]** > **[DNS]**を選択します。

ステップ 2 [DNS ポリシーの追加（Add DNS Policy）] をクリックします。

ステップ 3 [名前（Name）] に一意のポリシー名を入力し、オプションで [説明（Description）] にポリシーの説明を入力します。

ステップ 4 [保存（Save）] をクリックします。

次のタスク

- 必要に応じて、セキュリティ インテリジェンスによる接続のロギング （3016ページ）の説明に従って、さらに新しいポリシーを設定します。
- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

DNS ポリシーの編集

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Access Admin/Network Admin

DNS ポリシーを同時に編集できるのは 1 ユーザのみであり、使用できるのは単一のブラウザ ウィンドウのみです。複数のユーザが同じポリシーを保存しようとすると、最初に保存された変更のセットのみが保持されます。

セッションのプライバシーを保護するために、ポリシー エディタで活動が行われずに 30 分が経過すると、警告が表示されます。60 分後には、システムにより変更が破棄されます。

ステップ 1 **[Policies]** > **[Access Control]** > **[DNS]**を選択します。

ステップ 2 編集する DNS ポリシーの横にある編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 DNS ポリシーを編集します。

- 名前と説明：名前または説明を変更するには、フィールドをクリックして新しい情報を入力します。
- ルール：DNS ルールを追加、分類、有効化、無効化、または管理する場合は、[ルール（Rules）] タブをクリックして、DNS ルールの作成および編集 （1756 ページ）の説明に従って続行します。

ステップ 4 [保存（Save）] をクリックします。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

DNS ポリシーの管理

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Access Admin/Network Admin

[DNS ポリシー（DNS Policy）] ページ（**[Policies]** > **[Access Control]** > **[DNS]**）を使用して、DNS のカスタム ポリシーを管理します。自分で作成したカスタム ポリシーに加えて、システムにはデフォルトの DNS ポリシーが用意されています。このポリシーは、デフォルトのブラックリストとホワイトリストを使用します。このシステム付属のカスタム ポリシーは編集して使用できます。マルチドメイン展開では、このデフォルト ポリシーはデフォルトのグローバル DNS ブラックリスト、グローバル DNS ホワイトリスト、子孫 DNS ブラックリスト、および子孫 DNS ホワイトリストを使用します。また、このポリシーはグローバル ドメインでのみ編集できます。

マルチドメイン展開では、編集できる現在のドメインで作成されたポリシーが表示されます。また、編集できない先祖ドメインで作成されたポリシーも表示されます。下位のドメインで作成されたポリシーを表示および編集するには、そのドメインに切り替えます。

ステップ 1 **[Policies]** > **[Access Control]** > **[DNS]** を選択します。

ステップ 2 DNS ポリシーを以下のように管理します。

- 比較：DNS ポリシーを比較するには、[ポリシーの比較（Compare Policies）] をクリックして、ポリシーの比較 （457 ページ）で説明する手順を実行します。
- コピー：DNS ポリシーをコピーするには、コピー アイコン（  ）をクリックして、DNS ポリシーの編集 （1754 ページ）で説明する手順を実行します。
- 作成：新しい DNS ポリシーを作成するには、[DNS ポリシーの追加（Add DNS Policy）] をクリックし、基本 DNS ポリシーの作成 （1753 ページ）で説明する手順を実行します。
- 削除：DNS ポリシーを削除するには、削除アイコン（  ）をクリックし、ポリシーの削除を確認します。
- 編集：既存の DNS ポリシーを変更するには、編集アイコン（  ）をクリックし、DNS ポリシーの編集 （1754 ページ）で説明する手順を実行します。

DNS ルール

DNS ルールは、ホストにより要求されるドメイン名に基づいてトラフィックを処理します。セキュリティ インテリジェンスの一部として、この評価はすべてのトラフィック復号の後、およびアクセス コントロールの評価の前に実行されます。

システムは指定した順序でトラフィックを DNS ルールと照合します。ほとんどの場合、システムによるネットワーク トラフィックの処理は、すべてのルールの条件がトラフィックに一致する最初の DNS ルールに従って行われます。DNS ルールを作成すると、システムは、モニタ ルールとブラックリスト ルールの前にホワイトリスト ルールを配置し、最初にホワイトリスト ルールに対してトラフィックを評価します。

各 DNS ルールには、一意の名前以外にも、次の基本コンポーネントがあります。

状態

デフォルトでは、ルールが有効状態になります。無効にしたルールはネットワーク トラフィックの評価には使用されなくなり、そのルールの場合の警告とエラーの生成が停止されます。

位置

DNS ポリシーのルールには 1 から始まる番号が付いています。システムは、ルール番号の昇順で上から順に、ルールをトラフィックと照合します。Monitor ルールを除き、トラフィックが最初に一致するルールが、当該トラフィックを処理するためのルールになります。

条件

条件は、ルールで処理する特定のトラフィックを指定します。DNS ルールには、DNS フィードまたはリスト条件が含まれている必要があり、セキュリティ ゾーン、ネットワーク、または VLAN によってトラフィックと照合することができます。

操作（Action）

ルールのアクションによって、一致したトラフィックの処理方法が決まります。

- ホワイトリスト トラフィックが許可され、さらにアクセス コントロール インスペクションを受けます。
- モニタされるトラフィックは、残りの DNS ブラックリスト ルールによりさらに評価されます。トラフィックが DNS ブラックリスト ルールに一致しない場合、アクセス コントロール ルールによりインスペクションを受けます。そのトラフィックのセキュリティ インテリジェンス イベントは、システムにより記録されます。
- ブラックリストに登録されたトラフィックは、それ以上のインスペクションは行われずにブロックされます。[Domain Not Found] 応答を返したり、DNS クエリをシンクホール サーバにリダイレクトしたりすることもできます。

関連トピック

セキュリティ インテリジェンスについて （1741 ページ）

DNS ルールの作成および編集

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Access Admin/Network Admin

DNS ポリシーでは、ホワイトリスト ルールおよびブラックリスト ルールに合計 32767 個まで DNS リストを追加できます。つまり、DNS ポリシーのリストの数が 32767 を超えることはできません。

ステップ 1 DNS ポリシー エディタには、以下のオプションがあります。

- 新しいルールを追加するには、[DNS ルールの追加（Add DNS Rule）] をクリックします。
- 既存のルールを編集するには、編集アイコン（）をクリックします。

ステップ 2 [Name] を入力します。

ステップ 3 ルール コンポーネントを設定するか、またはデフォルトを受け入れます。

- [アクション（Action）]：ルールの [アクション（Action）] を選択します。DNS ルールのアクション（1759 ページ）を参照してください。
- [条件（Conditions）]：ルールの条件を設定します。DNS ルールの条件（1760 ページ）を参照してください。
- [有効（Enabled）]：ルールを有効にするかどうかを指定します。

ステップ 4 [保存（Save）] をクリックします。

次のタスク

- 設定変更を展開します。設定変更の展開（447 ページ）を参照してください。

DNS ルールの管理

DNS ポリシー エディタの [ルール（Rules）] タブでは、ポリシー内の DNS ルールの追加、編集、移動、有効化、無効化、削除、その他の管理が行えます。

各ルールについて、ポリシー エディタでは、その名前、条件のサマリー、およびルール アクションが表示されます。他のアイコンにより、警告（）、エラー（）、その他の重要な情報（）が示されます。無効なルールはグレー表示され、ルール名の下に [無効（disabled）] というマークが付きます。

DNS ルールの有効化と無効化

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Access Admin/Network Admin

作成した DNS ルールは、デフォルトで有効になっています。ルールを無効にすると、システムはネットワーク トラフィックの評価にそのルールを使用せず、そのルールに対する警告とエラーの生成を停止します。DNS ポリシーのルール リストを表示すると、無効なルールは淡色表示されますが、変更は可能です。DNS ルール エディタを使用して DNS ルールをイネーブルまたはディセーブルにできることにも注意してください。

ステップ 1 DNS ポリシー エディタで、ルールを右クリックしてルール状態を選択します。
ステップ 2 **[保存（Save）]** をクリックします。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

DNS ルールの評価順序

DNS ポリシーのルールには 1 から始まる番号が付いています。システムは、ルール番号の昇順で、DNS ルールを上から順にトラフィックと照合します。ほとんどの場合、システムによるネットワーク トラフィックの処理は、すべてのルールの条件がトラフィックに一致する最初の DNS ルールに従って行われます。

- モニタ ルールでは、システムはまずトラフィックを記録し、その後、優先順位の低い DNS ブラックリスト ルールに対してトラフィックの評価を続行します。
- モニタ ルール以外では、トラフィックがルールに一致した後、システムは優先順位の低い追加の DNS ルールに対してトラフィックの評価は続行**しません**。

ルールの順序に関して、次の点に注意してください。

- グローバル ホワイトリストは必ず最初に使用され、他のすべてのルールに優先します。
- 子孫 DNS ホワイトリスト ルールは、マルチドメイン展開の非リーフ ドメインでのみ表示されます。これは常に 2 番目であり、グローバル ホワイトリストを除き、他のすべてルールよりも優先されます。
- [Whitelist] セクションは [Blacklist] セクションに優先します。ホワイトリスト ルールは他のルールにいつでも必ず優先します。
- グローバル ブラックリストは [Blacklist] セクション内で必ず最初に使用され、他のすべてのモニタ ルールやブラックリスト ルールに優先します。
- 子孫 DNS ブラックリスト ルールは、マルチドメイン展開の非リーフ ドメインでのみ表示されます。これは常にブラックリスト セクションの 2 番目であり、グローバル ブラックリストを除き、他のすべてのモニタ ルールおよびブラックリスト ルールよりも優先されます。
- ブラックリスト セクションには、モニタ ルールおよびブラックリスト ルールが含まれます。
- 初めて DNS ルールを作成したときは、ホワイトリスト アクションを割り当てるとそれはシステムによりホワイトリスト セクションの最後に配置され、他のアクションを割り当てるとブラックリスト セクションの最後に配置されます。

ルールをドラッグ アンド ドロップして、これらの順序を変更できます。

DNS ルールのアクション

すべての DNS ルールには、一致するトラフィックについて次のことを決定するアクションがあります。

- 処理：まずルールアクションは、システムがルールの条件に一致するトラフィックをホワイトリスト登録、モニタ、またはブラックリスト登録するかどうかを制御します。
- ロギング：ルールアクションによって、一致するトラフィックの詳細をいつ、どのようにログに記録できるかが決まります。

インラインで展開されたデバイスのみがトラフィックをブラックリスト登録できることに留意してください。パッシブに展開されたデバイスまたはタップモードで展開されたデバイスは、トラフィックをホワイトリスト登録およびロギングできますが、トラフィックに影響を与えることはできません。

設定されている場合、TID は、アクションの優先順位付けに影響を与えます。詳細については、TID-Firepower Management Center のアクションの優先順位付け （1994 ページ）を参照してください。

ホワイトリスト アクション

ホワイトリストアクションにより、一致するトラフィックの通過が許可されます。トラフィックをホワイトリストに登録する場合、一致するアクセス コントロール ルール、またはアクセス コントロール ポリシーのデフォルト アクションのいずれかによって、トラフィックはさらに検査を受けます。

システムは、ホワイトリストの一致はロギングしません。しかし、ホワイトリストに登録された接続のロギングは、その最終的な傾向により決まります。

モニタ アクション

[Monitor] アクションは接続ロギングを強制するように設計されています。つまり、一致するトラフィックが即時にホワイトリストまたはブラックリストに登録されることはありません。その代わり、追加のルールに照らしてトラフィックが照合され、許可/拒否が決定されます。モニタ ルール以外の一致する最初の DNS ルールが、システムがトラフィックをブラックリスト登録するかどうかを決定します。一致する追加のルールがなければ、トラフィックはアクセス コントロール評価の対象となります。

DNS ポリシーによってモニタされる接続については、システムは、接続終了セキュリティ インテリジェンスと接続イベントを Firepower Management Center データベースにロギングします。

ブラックリスト アクション

ブラックリストアクションは、どのような追加検査も実行せずにトラフィックをブラックリストに登録します。

- [Drop] アクションはトラフィックをドロップします。
- [Domain Not Found] アクションは、存在しないインターネット ドメイン応答を DNS クエリに返します。これによりクライアントは DNS 要求を解決できなくなります。
- [Sinkhole] アクションは、シンクホール オブジェクトの IPv4 または IPv6 アドレスを DNS クエリに応答して返します。シンクホール サーバは、IP アドレスへの後続の接続をログに記録するか、ログに記録してブロックすることができます。[Sinkhole] アクションを設定する場合、シンクホール オブジェクトも設定する必要があります。

[ドロップ（Drop）] または [検出されないドメイン（Domain Not Found）] アクションに基づいてブラックリスト登録された接続については、システムは接続開始セキュリティ インテリジェンスイベントと接続イベントをロギングします。ブラックリスト登録されたトラフィックは追加のインスペクションなしですぐに拒否されるため、ログに記録できる固有の接続の終了イベントはありません。

[Sinkhole] アクションに基づいてブラックリストに登録される接続の場合、ロギングはシンクホール オブジェクトの設定に応じて決まります。シンクホール オブジェクトを、シンクホール接続をロギングのみするよう設定している場合、システムは、後続の接続の接続終了イベントをロギングします。シンクホール オブジェクトを、シンクホール接続をロギングしてブロックするよう設定している場合、システムは、後続の接続の接続開始イベントをロギングし、その後、その接続をブロックします。

（注） ASA FirePOWER デバイスでシンクホール アクションを使用して DNS ルールを設定し、トラフィックがルールに一致する場合、デフォルトでは ASA によって、後続のシンクホール接続がブロックされます。回避策として、ASA コマンド ラインから次のコマンドを実行します。

```
asa(config)# policy-map global_policy
asa(config-pmap)# class inspection_default
asa(config-pmap-c)# no inspect dns preset_dns_map
```

ASA が引き続き接続をブロックする場合は、サポートにお問い合わせください。

関連トピック

ルールとポリシーのアクションによるロギングへの影響 （3004 ページ）

DNS ルールの条件

DNS ルールの条件は、ルールで処理するトラフィックのタイプを特定します。条件は単純なものにも複雑なものにもできます。DNS ルール内の DNS フィードまたはリスト条件を定義する必要があります。また、必要に応じてセキュリティ ゾーン、ネットワーク、または VLAN によってトラフィックを制御できます。

DNS ルールに条件を追加するときは、以下に留意してください。

- ルールに対し特定の条件を設定しない場合、システムはその基準に基づいてトラフィックを照合しません。

- 1 つのルールにつき複数の条件を設定できます。ルールがトラフィックに適用されるには、トラフィックがそのルールの**すべての**条件に一致する必要があります。たとえば、DNS フィードまたはリスト条件およびネットワーク条件を含み、VLAN タグ条件を含まないルールは、セッション中の VLAN タグに関係なく、ドメイン名と送信元または宛先に基づいてトラフィックを評価します。
- ルールの条件ごとに、最大 50 の基準を追加できます。条件の基準の**いずれかに**一致するトラフィックはその条件を満たします。たとえば、最大で 50 DNS のリストとフィードに基づいてトラフィックをブラックリストに登録する単一のルールを使用できます。

DNS およびセキュリティ ゾーンに基づくトラフィックの制御

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Access Admin/Network Admin

DNS ルール内のゾーン条件によって、その送信元および宛先セキュリティ ゾーン別にトラフィックを制御することができます。セキュリティ ゾーンは、複数のデバイス間に配置されている場合がある 1 つ以上のインターフェイスのグループです。検出モードと呼ばれる、デバイスの初期セットアップ時に選択するオプションによって、システムが最初にデバイスのインターフェイスをどのように設定するか、およびこれらのインターフェイスがセキュリティ ゾーンに属するかどうかが決定します。

ステップ 1 DNS ルール エディタで、[ゾーン（Zones）] タブをクリックします。

ステップ 2 [Available Zones] から追加するゾーンを見つけて選択します。追加するゾーンを検索するには、[Available Zones] リストの上にある [Search by name] プロンプトをクリックし、ゾーン名を入力します。入力すると、リストが更新されて一致するゾーンが表示されます。

ステップ 3 セキュリティ ゾーンをクリックするか、または右クリックして、[Select All] を選択します。

ステップ 4 [送信元に追加（Add to Source）] をクリックするか、ドラッグ アンド ドロップします。

ステップ 5 ルールを保存するか、編集を続けます。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

DNS およびネットワークに基づくトラフィックの制御

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Access Admin/Network Admin

DNS ルール内のネットワーク条件によって、その送信元 IP アドレス別にトラフィックを制御することができます。制御するトラフィックの送信元 IP アドレスを明示的に指定できます。

ステップ 1 DNS ルール エディタで、[ネットワーク（Networks）] タブをクリックします。

ステップ 2 [Available Networks] から、次のように追加するネットワークを見つけて選択します。

- ここでネットワーク オブジェクトを追加するには（後で条件に追加できます）、[利用可能なネットワーク（Available Networks）] リストの上にある追加アイコン（  ）をクリックし、ネットワーク オブジェクトの作成 （527 ページ）の説明に従って進みます。
- 追加するネットワーク オブジェクトを検索するには、[利用可能なネットワーク（Available Networks）] リストの上にある [名前または値で検索（Search by name or value）] プロンプトをクリックし、オブジェクトのいずれかのコンポーネントのオブジェクト名または値を入力します。入力すると、リストが更新されて一致するオブジェクトが表示されます。

ステップ 3 [送信元に追加（Add to Source）] をクリックするか、ドラッグ アンド ドロップします。

ステップ 4 手動で指定する送信元 IP アドレスまたはアドレス ブロックを追加します。[送信元ネットワーク（Source Networks）] リストの下にある [IP アドレスの入力（Enter an IP address）] プロンプトをクリックし、1 つの IP アドレスまたはアドレス ブロックを入力して [追加（Add）] をクリックします。

システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。 上書き対応オブジェクトを使用すると、子孫ドメインの管理者は、グローバル コンフィギュレーションを自分のローカル環境に調整できます。

ステップ 5 ルールを保存するか、編集を続けます。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

DNS および VLAN に基づくトラフィックの制御

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Access Admin/Network Admin

DNS ルールで VLAN 条件を設定すると、トラフィックの VLAN タグに応じてそのトラフィックを制御できます。システムは、最も内側の VLAN タグを使用して VLAN を基準にパケットを識別します。

VLAN ベースの DNS ルール条件を作成するときは、VLAN タグを手動で指定できます。または、VLAN タグ オブジェクトを使用して VLAN 条件を設定することもできます。VLAN タグ オブジェクトとは、いくつかの VLAN タグに名前を付けて再利用可能にしたものを指します。

ステップ 1 DNS ルール エディタで、[VLAN タグ（VLAN Tags）] タブを選択します。

ステップ 2 [利用可能な VLAN タグ（Available VLAN Tags）] で、追加する VLAN を選択します。

- VLAN タグ オブジェクトをここで追加するには（後で条件に追加できます）、[利用可能な VLAN タグ（Available VLAN Tags）] リストの上にある追加アイコン（  ）をクリックし、VLAN タグ オブジェクトの作成 （531 ページ）の説明に従って進みます。
- 追加する VLAN タグ オブジェクトおよびグループを検索するには、[利用可能な VLAN タグ（Available VLAN Tags）] リストの上にある [名前または値で検索（Search by name or value）] プロンプトをクリックし、オブジェクト名またはオブジェクトの VLAN タグの値を入力します。入力すると、リストが更新されて一致するオブジェクトが表示されます。

ステップ 3 [ルールに追加（Add to Rule）] をクリックするか、ドラッグ アンド ドロップします。

ステップ 4 手動で指定する VLAN タグを追加します。[Selected VLAN Tags] リストの下にある [Enter a VLAN Tag] プロンプトをクリックし、VLAN タグまたはその範囲を入力して、[Add] をクリックします。1 から 4094 までの任意の VLAN タグを指定できます。VLAN タグの範囲を指定するにはハイフンを使用します。

システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、実際の VLAN タグを使用してこの設定を抑制すると、予期しない結果になる可能性があります。 上書き対応オブジェクトを使用すると、子孫ドメインの管理者は、グローバル コンフィギュレーションを自分のローカル環境に調整できます。

ステップ 5 ルールを保存するか、編集を続けます。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

DNS リスト、フィード、またはカテゴリに基づくトラフィックの制御

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Access Admin/Network Admin

DNS リスト、フィード、またはカテゴリにクライアントにより要求されたドメイン名が含まれる場合、DNS ルール内の DNS 条件によりトラフィックを制御できます。DNS ルール内で DNS 条件を定義する必要があります。

グローバルまたはカスタムのホワイトリストまたはブラックリストを DNS 条件に追加するかどうかに関わらず、システムは設定されたルールアクションをトラフィックに適用します。たとえばルールにグローバル ホワイトリストを追加し、[ドロップ（Drop）] アクションを設定すると、システムはホワイトリスト登録されている必要があるすべてのトラフィックをブラックリスト登録します。

ステップ 1 DNS ルール エディタで、[DNS] タブをクリックします。

ステップ 2 追加する DNS リストとフィードを、以下のように [DNS Lists and Feeds] から見つけて選択します。

- DNS リストまたはフィードをここで追加するには（後で条件に追加できます）、[DNS リストおよびフィード（DNS Lists and Feeds）] リストの上にある追加アイコン（  ）をクリックし、セキュリティ インテリジェンス フィードの作成 （564 ページ）の説明に従って進みます。
- 追加する DNS リスト、フィード、またはカテゴリを検索するには、[DNS リストおよびフィード（DNS Lists and Feeds）] リストの上にある [名前または値で検索（Search by name or value）] プロンプトをクリックし、オブジェクトのコンポーネントの 1 つのオブジェクト名または値を入力します。入力すると、リストが更新されて一致するオブジェクトが表示されます。

ステップ 3 [Add to Rule] をクリックするか、ドラッグ アンド ドロップします。

ステップ 4 ルールを保存するか、編集を続けます。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

DNS ポリシーの展開

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数
Threat	Protection	いずれか（Any）	いずれか（Any）

DNS のポリシー設定の更新を終了した後に、アクセス コントロール設定の一部としてこれを展開する必要があります。

- セキュリティインテリジェンスの設定（1744ページ）で説明されているように、DNSポリシーをアクセス コントロール ポリシーに関連付けます。
- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

第 69 章

プレフィルタ処理とプレフィルタ ポリシー

以下のトピックでは、プレフィルタを設定する方法について説明します。

プレフィルタリングについて

プレフィルタはアクセス制御の最初のフェーズで、システムがより大きいリソース消費の評価を実行する前に行われます。プレフィルタリングはシンプルかつ高速で、初期に実行されます。プレフィルタリングでは、限定された外部ヘッダーを基準にしてトラフィックを迅速に処理します。内部ヘッダーを使用し、より堅牢なインスペクション機能を備えた後続の評価とこのプレフィルタリングを比較します。

次の目的でプレフィルタリングを設定します。

- パフォーマンスの向上：インスペクションを必要としないトラフィックの除外は、早ければ早いほど適切です。特定のタイプのプレーン テキストをファストパスまたはブロックし、カプセル化された接続を検査することなく外側のカプセル化ヘッダーに基づいてトンネルをパススルーします。早期処理のメリットがあるその他の接続についても、ファストパスやブロックをすることができます。
- カプセル化トラフィックに合わせたディープインスペクションの調整：同じ検査基準を使用してカプセル化接続を後で処理できるように、特定のタイプのトンネルを再区分できます。アクセス制御はプレフィルタ後に内側のヘッダーを使用するため、再区分は必須です。

プレフィルタリングとアクセス コントロール

プレフィルタとアクセスコントロールポリシーのどちらを使用しても、トラフィックをブロックしたり信頼したりできますが、プレフィルタリングの「信頼」機能の方がより多くのインス

ペクションをスキップするため、「高速パス」と呼ばれます。次の表ではこれについて説明し、プレフィルタリングとアクセス コントロールのその他の違いを示します。これは、カスタム プレフィルタリングを設定するかどうかの決定に役立ちます。

カスタム プレフィルタリングを設定しない場合は、アクセス コントロール ポリシーに初期に配置されたブロックおよび信頼ルールにより、プレフィルタ機能に近づけることのみ可能です（複製するのではなく）。

特性	プレフィルタリング	アクセス制御	詳細
主な機能	特定のタイプのプレーンテキストのパススルートンネル（カプセル化の条件 （479 ページ）を参照）を迅速に高速パス処理またはブロックしたり、後続のインスペクションをそのカプセル化されたトラフィックに適合させたりします。 早期処理による利点が得られる他の接続を高速パス処理またはブロックします。	コンテキスト情報やディープインスペクションの結果など、単純または複雑な基準を使用して、すべてのネットワーク トラフィックを検査および制御します。	プレフィルタリングについて （1767 ページ）
実装	プレフィルタ ポリシー プレフィルタ ポリシーは、アクセス コントロール ポリシーによって呼び出されます。	アクセス コントロール ポリシー アクセス コントロール ポリシーは、マスター構成です。サブポリシーの呼び出しに加えて、アクセス コントロール ポリシーの独自のルールがあります。	プレフィルタ ポリシーについて （1773 ページ） アクセス制御への他のポリシーの関連付け （1684 ページ）
アクセス コントロール内のシーケンス	最初。 トラフィックは、他のすべてのアクセス コントロール構成の前にプレフィルタ基準と照合されます。	—	—
ルール アクション	少ない。 追加のインスペクションを停止したり（高速パス処理とブロック）、他のアクセス コントロールによる追加の分析を許可したり（分析）できます。	多い。 アクセス コントロール ルールには、モニタリング、ディープインスペクション、リセットしてブロック、インタラクティブ ブロッキングなどのさまざまなアクションがあります。	トンネルとプレフィルタ ルールのコンポーネント （1775 ページ） アクセス コントロール ルールのアクション （1701 ページ）

特性	プレフィルタリング	アクセス制御	詳細
バイパス機能	高速パス ルール アクション。 プレフィルタ段階のトラフィックの高速パス処理では、その後のすべてのインスペクションと次のような処理をバイパスします。 • セキュリティ インテリジェンス • アイデンティティ ポリシーによって課される認証要件 • SSL 復号 • アクセス コントロール ルール • パケット ペイロードのディープ インスペクション • 検出 • レート制限	信頼ルール アクション。 アクセス コントロール ルールによって信頼されるトラフィックのみがディープ インスペクションとディスカバリを免除されます。	アクセス コントロール ルールの概要 （1689 ページ）
ルール基準	制限。 プレフィルタ ポリシーのルールでは、単純なネットワーク基準、つまりIPアドレス、VLANタグ、ポート、およびプロトコルを使用します。 トンネルについては、トンネル エンドポイント条件によって、トンネルの両側にあるネットワーク デバイスのルーテッド インターフェイスのIPアドレスを指定します。	堅牢。 アクセス コントロール ルールでは、ネットワーク基準を使用しますが、パケット ペイロードで使用できるユーザ、アプリケーション、要求されたURL、およびその他のコンテキスト情報も使用します。 ネットワーク条件によって、送信元と宛先ホストの IP アドレスが指定されます。	トンネルとプレフィルタのルール （1774 ページ） ルール条件タイプ （465 ページ）

特性	プレフィルタリング	アクセス制御	詳細
IP ヘッダーの使用（トンネル処理）	最も外側。 外部ヘッダーを使用して、プレーンテキストのパススルー トンネル全体を処理できます。 カプセル化されていないトラフィックについては、プレフィルタリングで引き続き「外部」ヘッダーが使用され、この場合は唯一のヘッダーになります。	可能な限り内側。 カプセル化されていないトンネルについては、アクセス コントロールは、トンネル全体ではなく、個々のカプセル化された接続に適用されます。	パススルー トンネルとアクセス制御 （1770 ページ）
さらに分析するためのカプセル化された接続の再ゾーン化	トンネルされたトラフィックを再ゾーン化します。 トンネルゾーンにより、後続のインスペクションをプレフィルタされたカプセル化トラフィックに適合させることができます。	トンネル ゾーンを使用。 アクセス コントロールでは、プレフィルタリング中に割り当てたトンネル ゾーンを使用します。	トンネル ゾーンおよびプレフィルタリング （1777 ページ）
接続のロギング	高速パス処理およびブロックされたトラフィックのみ。許可された接続は、他の構成によってログに記録されることがあります。	任意の接続。	ログ可能なその他の接続 （3003 ページ）
サポートされるデバイス	Firepower Threat Defense のみ。	すべて。	プレフィルタリングのガイドラインと制限事項 （1771 ページ）

パススルー トンネルとアクセス制御

プレーンテキスト（暗号化されていない）トンネルでは、複数の接続をカプセル化できます。これらのトンネルは、多くの場合、連続していないネットワーク間をつなぎます。したがって、IP ネットワークでカスタム プロトコルをルーティングする場合や、IPv4 ネットワークで IPv6 トラフィックをルーティングする場合などには特に役立ちます。

外側のカプセル化ヘッダーには、トンネル エンドポイント（トンネルのいずれかの側にあるネットワーク デバイスのルーテッド インターフェイス）の送信元と宛先の IP アドレスが指定されます。内側のペイロードヘッダーには、カプセル化された接続の実際のエンドポイントの送信元と宛先の IP アドレスが指定されます。

通常、ネットワーク セキュリティ デバイスは、プレーンテキスト トンネルをパススルー トラフィックとして扱います。つまり、ネットワーク セキュリティ デバイスはトンネル エンドポイントのうちの 1 つではないということです。代わりに、ネットワーク セキュリティ デバイ

スはトンネルエンドポイントの間に展開されて、それらのエンドポイント間を流れるトラフィックをモニタします。

一部のネットワーク セキュリティ デバイスは、外側の IP ヘッダーを使用してセキュリティ ポリシーを適用します。その一例は、（Firepower Threat Defense ではなく）Cisco ASA ソフトウェアを実行する Cisco ASA ファイアウォールです。プレーン テキスト トンネルの場合でも、これらのデバイスはカプセル化された個々の接続とそのペイロードを制御したりその内容を把握したりすることはできません。

それとは対照的に、Firepower システムは以下のようにアクセス制御を活用します。

- 外側のヘッダーの評価：まず、プレフィルタで外側のヘッダーを使用してトラフィックを処理します。この段階で、プレーン テキストのパススルー トンネル全体をブロックすることも、FastPath を適用することもできます。
- 内側のヘッダーの評価：次に、アクセス制御の残り（および QoS などのその他の機能）では、最も内側にあるヘッダーの検出可能レベルを使用して、可能な限り詳細なレベルでインスペクションと処理が行われるようにします。

  パススルー トンネルが暗号化されていなければ、システムはこの段階で、カプセル化された個々の接続に対処します。カプセル化されたすべての接続に対処するには、トンネルの再ゾーン分割（トンネル ゾーンおよびプレフィルタリング （1777 ページ）を参照）を行う必要があります。

アクセス制御では、暗号化されたパススルー トンネルの内容を把握しません。たとえば、アクセス制御ルールは、パススルー VPN トンネルを 1 つの接続と見なします。システムは外側のカプセル化ヘッダーに含まれる情報だけを使用して、トンネル全体を処理します。

プレフィルタリングのガイドラインと制限事項

モデルの要件

プレフィルタリングは Firepower Threat Defense デバイス上でのみサポートされています。プレフィルタリングの設定はその他のデバイスに影響しません。

その他のデバイスでのプレフィルタと同様の機能

従来型デバイス（7000/8000 シリーズ、ASA FirePOWER、NGIPSv）の場合：

- プレフィルタとほぼ同様の機能を持つ以前から用意されてる信頼およびブロック アクセス コントロール ルールを、機能の違いに留意しつつ使用してください。プレフィルタリングとアクセス コントロール （1767 ページ）を参照してください。
- アクセス制御ルールを使用して GRE でカプセル化されたトンネル全体を照合しますが、いくつかの制限事項があります。ポートおよび ICMP コードの条件 （477 ページ）を参照してください。

- （8000 シリーズのみ）デバイス固有の fastpath ルールによってアクセス制御をバイパスできますが、トラフィックをブロックすることはできません。高速パス ルールの設定（8000 シリーズ） （307 ページ）を参照してください。

プレフィルタリングの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin/Access Admin/Network Admin

カスタム プレフィルタリングを実行するには、アクセス コントロールの一部として管理対象デバイスにプレフィルタ ポリシーを設定し、展開します。

ポリシーの編集は、1 つのブラウザ ウィンドウを使用して、一度に 1 人のみで行う必要があります。複数のユーザが同じポリシーを保存した場合は、最後に保存された変更が保持されます。ユーザにとっての便宜性を考慮して、各ポリシーを現在編集している人（いる場合）の情報が表示されます。セッションのプライバシーを保護するために、ポリシー エディタが非アクティブになってから 30 分後に警告が表示されます。60 分後には、システムにより変更が破棄されます。

ステップ 1 **[Policies]** > **[Access Control]** > **[Prefilter]**を選択します。

ステップ 2 [新しいポリシー（New Policy）] をクリックして、カスタム プレフィルタ ポリシーを作成します。

新しいプレフィルタ ポリシーには、ルールや、すべてのトンネル トラフィックを分析するデフォルト アクションはありません。新しいプレフィルタ ポリシーでは、ロギングやトンネルの再ゾーン分割は実行されません。また、既存のポリシーをコピー（  ）したり編集（  ）したりすることもできます。

ステップ 3 プレフィルタ ポリシーのデフォルト アクションとそのロギング オプションを設定します。

- デフォルト アクション：サポートされるプレーンテキスト、パススルー トンネルのデフォルト アクションを選択します。[すべてのトンネル トラフィックを分析（Analyze all tunnel traffic）]（アクセス コントロールあり）または [すべてのトンネル トラフィックをブロック（Block all tunnel traffic）]。
- デフォルト アクションのロギング：デフォルト アクションの横にあるロギング アイコン（  ）をクリックします。ポリシーのデフォルト アクションによる接続のロギング （3018 ページ）を参照してください。デフォルト アクションのロギングは、ブロックされたトンネルに対してのみ設定できます。

ステップ 4 トンネルおよびプレフィルタ ルールを設定します。

カスタム プレフィルタ ポリシーでは、両方の種類のルールを任意の順序で使用できます。照合する特定のタイプのトラフィックおよび実行するアクションまたは追加の分析に応じてルールを作成します。トンネルとプレフィルタのルール （1774 ページ）を参照してください。

注意 トンネル ルールを使用してトンネル ゾーンを割り当てる場合は、注意してください。再ゾーン分割されたトンネルでの接続は、後の評価でセキュリティ ゾーンの制約に一致しない可能性があります。詳細については、トンネル ゾーンおよびプレフィルタリング（1777 ページ）を参照してください。

ルール コンポーネントの設定の詳細については、トンネルとプレフィルタ ルールのコンポーネント（1775 ページ）およびルール管理：共通の特性（463 ページ）を参照してください。

ステップ 5 ルールの順序を評価します。ルールを移動するには、クリックしてドラッグするか、または右クリック メニューを使用してカット アンド ペーストを実行します。

ルールを適切に作成して順序付けることは複雑な作業ですが、効果的な展開を構築する上で不可欠な作業です。慎重に計画しないと、ルールが他のルールをプリエンプション処理したり、ルールに無効な設定が含まれてしまう可能性があります。詳細については、ルールのパフォーマンスに関するガイドライン（502 ページ）を参照してください。

ステップ 6 プレフィルタ ポリシーを保存します。

ステップ 7 トンネル ゾーンの制約をサポートする設定では、再ゾーン分割されたトンネルを適切に処理します。

トンネル ゾーンを送信元ゾーンの制約として使用して、再ゾーン分割されたトンネルでの接続を照合します。インターフェイス条件の設定（470 ページ）を参照してください。

ステップ 8 プレフィルタ ポリシーを管理対象デバイスに展開されたアクセス コントロール ポリシーに関連付けます。

アクセス制御への他のポリシーの関連付け（1684 ページ）を参照してください。

ステップ 9 設定変更を展開します。設定変更の展開（447 ページ）を参照してください。

プレフィルタ ポリシーについて

プレフィルタリングは、ポリシーベースの機能です。Firepower システムでは、アクセス コントロール ポリシーは、プレフィルタ ポリシーを含む、サブポリシーおよびその他の設定を呼び出すマスター設定です。

ポリシー コンポーネント：ルールとデフォルト アクション

プレフィルタ ポリシーでは、トンネル ルール、プレフィルタ ルール、デフォルト アクションに基づいてネットワーク トラフィックを処理します。

- トンネル ルールとプレフィルタ ルール：最初にプレフィルタ ポリシーのルールが、指定した順序でトラフィックを処理します。トンネル ルールは指定のトンネルのみを照合するもので、再ゾーニングをサポートします。プレフィルタ ルールはより広範囲の制約を設けるもので、再ゾーニングをサポートしていません。詳細については、トンネルとプレフィルタのルール（1774 ページ）を参照してください。
- デフォルト アクション（トンネルのみ）：トンネルがどのルールとも一致しない場合は、デフォルト アクションによって処理されます。デフォルト アクションは、そのトンネル

をブロックするか、あるいは個々のカプセル化された接続のアクセス制御を継続します。デフォルト アクションでトンネルの再ゾーニングを行うことはできません。

カプセル化されていないトラフィックに対するデフォルトアクションはありません。カプセル化されていない接続がどのプレフィルタ ルールにも一致しない場合、システムはアクセス制御を継続します。

接続ロギング

プレフィルタ ポリシーでFastPathされた接続およびブロックされた接続のログを記録することができます。ログ可能なその他の接続 （3003 ページ）を参照してください。

接続イベントには、すべてのトンネルを含め、ロギングされる接続がプレフィルタ処理されるのかどうか、また、どのようなプレフィルタ処理を行うのかに関する情報が含まれています。この情報は、イベント表示（ワークフロー）、ダッシュボード、およびレポートで表示することができ、相関基準として使用できます。FastPathされた接続やブロックされた接続は、ディープインスペクションの対象外であるため、これらの接続に関連する接続イベントに含まれる情報は限定的となります。

デフォルト プレフィルタ ポリシー

すべてのアクセス コントロール ポリシーにプレフィルタ ポリシーが関連付けられています。

カスタム プレフィルタリングを設定しなければ、システムはデフォルト ポリシーを使用します。このシステム提供のポリシーの初期設定では、すべてのトラフィックをアクセス制御の次のフェーズに渡します。デフォルト ポリシーのデフォルト アクションを変更し、ロギングのオプションを設定することはできますが、ルールの追加や削除はできません。

プレフィルタ ポリシーの継承とマルチテナンシー

アクセス制御は、マルチテナンシーを補完する階層型実装となっています。プレフィルタ ポリシーの関連付けは、その他の詳細設定と同様にロックすることが可能で、これによりすべての子孫アクセス コントロール ポリシーでこの関連付けが強制的に継承されます。詳細については、アクセス コントロール ポリシーの継承 （1670 ページ）を参照してください。

マルチドメイン展開では、編集できる現在のドメインで作成されたポリシーが表示されます。また、編集できない先祖ドメインで作成されたポリシーも表示されます。下位のドメインで作成されたポリシーを表示および編集するには、そのドメインに切り替えます。デフォルトプレフィルタ ポリシーは、グローバル ドメインに属しています。

トンネルとプレフィルタのルール

トンネルとプレフィルタのどちらのルールを設定するかは、照合するトラフィックのタイプと、実行するアクションや詳細な分析によって異なります。

特性	トンネル ルール	プレフィルタ ルール
主な機能	プレーンテキストのパススルー トンネルをすばやく高速パス化、ブロック、または再ゾーニングします。	初期段階の操作の影響を受ける他の接続をすばやく高速パス化またはブロックします。
カプセル化とポート/プロトコル条件	カプセル化の条件は、カプセル化の条件 （479 ページ） にリストされる選択済みプロトコルについて、プレーンテキスト トンネルのみと照合されます。	ポート条件では、トンネル ルールより広範囲のポートおよびプロトコル制約を使用できます。ポートおよび ICMP コードの条件 （477 ページ） を参照してください。
ネットワーク条件	トンネル エンドポイント条件は、処理対象にするトンネルのエンドポイントを制約します。トンネル エンドポイント条件 （474 ページ） を参照してください。	ネットワーク条件は、各接続の送信元ホストと宛先ホストを制約します。ネットワーク条件 （471 ページ） を参照してください。
方向（Direction）	双方向または単方向（構成可）。 トンネル ルールはデフォルトで双方向であるため、トンネル エンドポイント間のすべてのトラフィックを処理できます。	単方向のみ（構成不可）。 プレフィルタ ルールは、送信元から宛先へ送信されるトラフィックのみと照合されます。
詳細分析のためのセッションの再ゾーニング	トンネル ゾーンを使用する場合にサポートされます。トンネル ゾーンおよびプレフィルタリング （1777 ページ） を参照してください。	未サポート

トンネルとプレフィルタ ルールのコンポーネント

状態（有効/無効）

デフォルトでは、ルールは有効になっています。ルールを無効にすると、システムはそのルールを使用せず、そのルールに対する警告とエラーの生成を停止します。

位置

ルールの番号は1から始まります。システムは、ルール番号の昇順で上から順に、ルールをトラフィックと照合します。トラフィックが一致する最初のルールは、ルール タイプ（トンネルまたはプレフィルタ）に関係なく、そのトラフィックを処理するルールです。

操作

ルールのアクションによって、一致したトラフィックの処理とログ記録の方法が決まります。

- [高速パス（Fastpath）]：アクセス制御、ID 要件、レート制限を含む、すべての詳細な検査および制御の対象から、一致するトラフィックを除外します。トンネルを高速パス化すると、すべてのカプセル化された接続が高速パス化されます。
- [ブロック（Block）]：どのような種類の検査も行わずにトラフィックを照合します。トンネルをブロックすると、カプセル化されたすべての接続がブロックされます。
- [分析（Analyze）]：残りのアクセス制御で内部ヘッダーを使用して引き続きトラフィックを分析できるようにします。アクセス制御および関連するディープ インスペクションによって渡された場合、このトラフィックはレート制限も行われる場合があります。トンネル ルールの場合は、[トンネル ゾーンの割り当て（Assign Tunnel Zone）] オプションを指定して、再ゾーニングを有効にします。

方向（トンネル ルールのみ）

トンネル ルールの方向によって、システムの送信元と宛先の条件に従った処理方法が決まります。

- 送信元からのトンネルのみを照合します（単方向）。送信元から宛先へ送信されるトラフィックのみを照合します。一致するトラフィックは、指定された送信元インターフェイスまたはトンネル エンドポイントから発信され、宛先インターフェイスまたはトンネル エンドポイントを通過する必要があります。
- 送信元と宛先からのトンネルを照合します（双方向）。送信元から宛先へ送信されるトラフィックと宛先から送信元へ送信されるトラフィックの両方を照合します。この効果は、単方向のルールを2つ作成した場合と同じで、一方のルールがもう一方のルールのミラーとなります。

プレフィルタ ルールは常に単方向です。

トンネル ゾーンの割り当て（トンネル ルールのみ）

トンネル ルールで、トンネル ゾーン（既存のゾーンまたはオンザフライで作成したゾーン）を割り当てると、一致するゾーンが再ゾーニングされます。再ゾーニングするには、分析アクションが必要です。

トンネルを再ゾーン化すると、アクセス コントロール ルールなどの他の設定で、そのトンネルのすべてのカプセル化された接続をグループとして認識できます。トンネルの割り当てられたトンネル ゾーンをインターフェイスの制約として使用することで、インスペクションをそのカプセル化された接続に合わせて調整できます。詳細については、トンネル ゾーンおよびプレフィルタリング （1777 ページ）を参照してください。

注意 トンネル ゾーンを割り当てるときには注意が必要です。再ゾーニングされたトンネルの接続は、後から実行される評価でセキュリティ ゾーンの制約と一致しないことが検出される可能性があります。トンネル ゾーン実装の簡単なウォークスルーと、再ゾーニングするトラフィックを明示的に処理せずに再ゾーニングする理由については、トンネル ゾーンの使用 （1778 ページ）を参照してください。

条件

条件は、ルールで処理する特定のトラフィックを指定します。トラフィックは、ルールのすべての条件と一致し、ルールと一致する必要があります。各条件の種類には、ルールエディタ内に独自のタブがあります。

トラフィックをプレフィルタするには、次の外部ヘッダー制約を使用します。

- インターフェイス：インターフェイス条件 （468 ページ）
- ネットワーク：トンネル エンドポイント条件 （474 ページ）またはネットワーク条件 （471 ページ）
- ポート：カプセル化の条件 （479 ページ）またはポートおよび ICMP コードの条件 （477 ページ）
- VLAN：VLAN 条件 （476 ページ）

トンネル ルールは、カプセル化プロトコルで制約する必要があります。

ログ

システムが記録する処理済みトラフィックのレコードは、ルールのロギング設定によって管理します。

トンネルとプレフィルタのルールでは、高速パスが適用されたトラフィックとブロックされたトラフィック（[高速パス（Fastpach）] と [ブロック（Block）] のアクション）をログに記録することができます。詳細分析（[分析（Analyze）] アクション）の対象となるトラフィックでは、一致する接続が他の構成で記録されている可能性がありますが、プレフィルタ ポリシーでのログ記録は無効になります。詳細については、トンネル ルールおよびプレフィルタ ルールによる接続のロギング （3015 ページ）を参照してください。

説明

ルールで変更を保存するたびに、コメントを追加することができます。たとえば、他のユーザのために設定全体を要約したり、ルールの変更時期と変更理由を記載することができます。

ルールを保存した後で、これらのコメントを編集または削除することはできません。

関連トピック

ルールのパフォーマンスに関するガイドライン （502 ページ）

トンネル ゾーンおよびプレフィルタリング

トンネルゾーンを使用すれば、プレフィルタリングを使って後続のトラフィック処理をカプセル化された接続に合わせることができます。

システムは通常最も内側の検出可能なレベルのヘッダーを使用してトラフィックを処理するため、特殊なメカニズムが必要になります。これにより、可能な限りきめ細かなインスペクションが保証されます。ただし、これは、パススルー トンネルが暗号化されていない場合、システ

ムは個々のカプセル化された接続に対して処理を行うことも意味しています。パススルー トンネルとアクセス制御 （1770 ページ）を参照してください。

トンネル ゾーンはこの問題を解決します。アクセス制御の最初のフェーズ（プレフィルタリング）で、特定のタイプのプレーン テキスト、パススルー トンネルを識別するために、外側のヘッダーを使用することができます。次に、それらのトンネルは、カスタム トンネル ゾーンを割り当てることで再ゾーン化できます。

トンネルを再ゾーン化すると、アクセス コントロール ルールなどの他の設定で、そのトンネルのすべてのカプセル化された接続をグループとして認識できます。トンネルの割り当てられたトンネル ゾーンをインターフェイスの制約として使用することで、インスペクションをそのカプセル化された接続に合わせて調整できます。

トンネル ゾーンは、その名称にもかかわらず、セキュリティ ゾーンではありません。トンネル ゾーンは、インターフェイスの一式を表すわけではありません。トンネル ゾーンは、場合によっては、カプセル化された接続に関連付けられているセキュリティ ゾーンに置き換わるタグとして考える方がより正確です。

注意 トンネル ゾーンの制約をサポートする設定の場合、再ゾーン化されたトンネル内の各接続はセキュリティ ゾーンの制約とは一致**しません**。たとえば、トンネルを再ゾーン化した後、アクセス コントロール ルールでは、そのカプセル化された各接続を、それらの新しく割り当てられたトンネル ゾーンと突き合わせることができますが、元のセキュリティ ゾーンと突き合わせることはできません。

トンネル ゾーンの導入の簡潔なウォークスルー、および再ゾーン化されたトラフィックを明示的に処理せずに再ゾーン化することの影響の説明については、トンネル ゾーンの使用 （1778 ページ）を参照してください。

トンネル ゾーンの制約をサポートする設定

トンネル ゾーンの制約をサポートするのは、アクセス コントロール ルールだけです。

他のどの設定もトンネル ゾーンの制約をサポートしません。たとえば、QoS を使用してプレーン テキスト トンネル全体をレート制限することはできず、個々のカプセル化されたセッションをレート制限できるだけです。

トンネル ゾーンの使用

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	FTD	いずれか（Any）	Admin/Access Admin/Network Admin

この例の手順は、トンネル ゾーンを使用してさらに分析するために GRE トンネルを再ゾーン化する方法をまとめたものです。この例で説明されている概念は、プレーンテキストのパスス

ルー トンネルにカプセル化された接続に合わせてトラフィック インスペクションを調整する必要があるシナリオにも適応できます。

組織の内部トラフィックが信頼済みセキュリティ ゾーンを通過する FirePOWER システムの展開について考えてみましょう。信頼済みセキュリティ ゾーンは、さまざまな場所に展開された複数の管理対象デバイス間における一連のセンシング インターフェイスを表します。組織のセキュリティ ポリシーでは、エクスプロイトとマルウェアのディープ インスペクション後の内部トラフィックを許可する必要があります。

内部トラフィックには、特定のエンドポイント間のプレーンテキストのパススルー GRE トンネルが含まれている場合があります。このカプセル化されたトラフィックのトラフィック プロファイルは、「通常」の局間アクティビティとは異なるため（おそらく既知かつ無害）、セキュリティ ポリシーに従いながら、特定のカプセル化された接続のインスペクションを制限できます。

この例では、構成の変更を展開した後、次のようになります。

- 信頼済みゾーンで検出されたプレーンテキストのパススルーGREカプセル化トンネルは、個別のカプセル化接続が1セットの侵入およびファイル ポリシーによって評価されます。
- 信頼済みゾーンの他のすべてのトラフィックは、侵入およびファイル ポリシーの別のセットで評価されます。

このタスクは、GRE トンネルの再ゾーン化によって実行します。再ゾーン化を実行すると、アクセス コントロールによって、GRE カプセル化接続が元の信頼済みセキュリティ ゾーンではなくカスタム トンネル ゾーンに関連付けられます。再ゾーン化が必要になるのは、FirePOWER システムとアクセス コントロールが、カプセル化されたトラフィックを処理する方法によります。パススルー トンネルとアクセス制御（1770ページ）およびトンネル ゾーンおよびプレフィルタリング （1777 ページ）を参照してください。

ステップ 1 カプセル化されたトラフィック向けのディープ インスペクションを実行するカスタムの侵入およびファイル ポリシーを設定し、カプセル化されていないトラフィックには別の侵入およびファイル ポリシーのセットを設定します。

ステップ 2 信頼済みセキュリティ ゾーンを通過する GRE トンネルを再ゾーン化するようにカスタム プレフィルタリングを設定します。

カスタム プレフィルタ ポリシーを作成し、アクセス コントロールに関連付けます。そのカスタム プレフィルタ ポリシーで、トンネル ルール（この例では **GRE_tunnel_rezone**）と対応するトンネル ゾーン（**GRE_tunnel**）を作成します。詳細については、プレフィルタリングの設定 （1772ページ）を参照してください。

表 *108 : GRE_tunnel_rezone* トンネル ルール

ルール コンポーネント	説明
インターフェイス オブジェクト条件	信頼済みセキュリティ ゾーンを送信元インターフェイス オブジェクトと宛先インターフェイス オブジェクトの両方の制約として使用して、内部のみのトンネルを照合します。

ルール コンポーネント	説明
トンネル エンドポイント条件	組織で使用されている GRE トンネルの送信元と宛先のエンドポイントを指定します。 トンネル ルールは、デフォルトでは双方向です。[トンネルの照合（Match tunnels from）] オプションを変更しない場合は、どのエンドポイントを送信元として指定し、どのエンドポイントを宛先として指定するかは重要ではありません。
カプセル化条件	GRE トラフィックを照合します。
トンネル ゾーンの割り当て	**GRE_tunnel** トンネル ゾーンを作成し、ルールに一致するトンネルに割り当てます。
操作	（残りのアクセス コントロールで）分析します。

ステップ 3 再ゾーン化されたトンネルの接続を処理するようにアクセス コントロールを設定します。

管理対象デバイスに展開されたアクセス コントロール ポリシーでは、再ゾーン化したトラフィックを処理するルール（この例では**GRE_inspection**）を設定します。詳細については、アクセス コントロール ルールの作成および編集 （1698 ページ）を参照してください。

表 *109 : GRE_inspection* アクセス コントロール ルール

ルール コンポーネント	説明
セキュリティ ゾーン条件	GRE_tunnel セキュリティ ゾーンを送信元ゾーン制約として使用して、再ゾーン化されたトンネルを照合します。インターフェイス条件 （468 ページ）を参照してください。
操作	ディープ インスペクションを有効にして許可します。 カプセル化された内部トラフィックのインスペクションを実行するように調整されたファイルおよび侵入ポリシーを選択します。

注意 この手順をスキップすると、再ゾーン化された接続は、セキュリティ ゾーンによって制約されていない**任意の**アクセス コントロール ルールに一致する場合があります。再ゾーン化された接続がどのアクセス コントロール ルールにも一致しない場合は、アクセス コントロール ポリシーのデフォルト アクションによって処理されます。意図してそのようにしていることを確認してください。

ステップ 4 信頼済みセキュリティ ゾーンを通過するカプセル化されていない接続を処理するようにアクセス コントロールを設定します。

同じアクセス コントロール ポリシーで、信頼済みセキュリティ ゾーン内の再ゾーン化されていないトラフィックを処理するルール（この例では **internal_default_inspection**）を設定します。

表 *110 : internal_default_inspection* アクセス コントロール ルール

ルール コンポーネント	説明
セキュリティ ゾーン条件	信頼済みセキュリティ ゾーンを送信元ゾーンと宛先ゾーンの両方の制約として使用して、再ゾーン化されていない内部のみのトラフィックを照合します。
操作	ディープ インスペクションを有効にして許可します。 カプセル化されていない内部トラフィックのインスペクションを実行するように適合されたファイルおよび侵入ポリシーを選択します。

ステップ 5 既存のルールに対して相対的な新しいアクセス コントロール ルールの位置を評価します。ルールの順序を必要に応じて変更します。

2 つの新しいアクセス コントロール ルールを隣同士に配置した場合は、最初にどちらを配置するかは重要ではありません。GRE トンネルを再ゾーン化したため、2 つのルールは互いをプリエンプション処理することはできません。

ステップ 6 すべての変更された構成を保存します。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

トンネル ゾーンの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	Firepower Threat Defense	いずれか（Any）	Admin/Access Admin/Network Admin

ステップ 1 **[Objects]** > **[Object Management]**を選択します。
ステップ 2 オブジェクト タイプのリストから [トンネル ゾーン（Tunnel Zone）] を選択します。
ステップ 3 [トンネル ゾーンの追加（Add Tunnel Zone）] をクリックします。
ステップ 4 [名前（Name）] を入力し、必要に応じて [説明（Description）] を入力します。
ステップ 5 [保存（Save）] をクリックします。

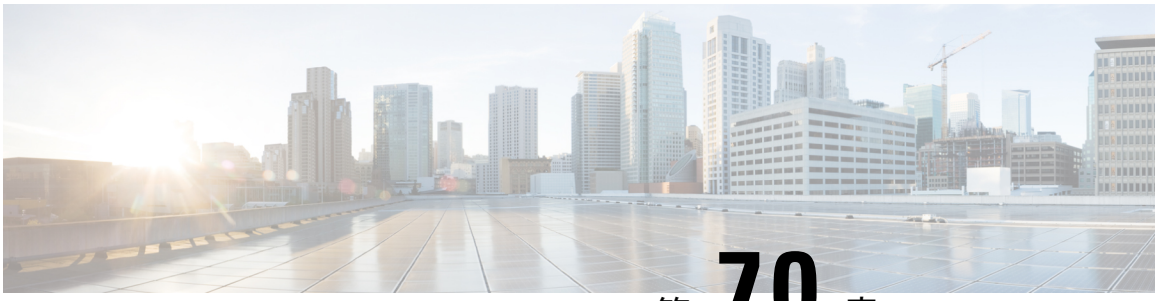
次のタスク

- カスタム事前フィルタリングの一部として、トンネル ゾーンをプレーン テキストのパススルー トンネルに割り当てます。プレフィルタリングの設定（1772ページ）を参照してください。

プレフィルタ ポリシーのヒット カウント

ヒットカウントは、一致する接続に対してポリシールールがトリガーされた回数を示します。

プレフィルタ ポリシー ヒット カウントの表示に関する詳細については、ポリシー ヒット カウントの表示 （1685 ページ）を参照してください。



第 70 章

インテリジェント アプリケーション バイパス

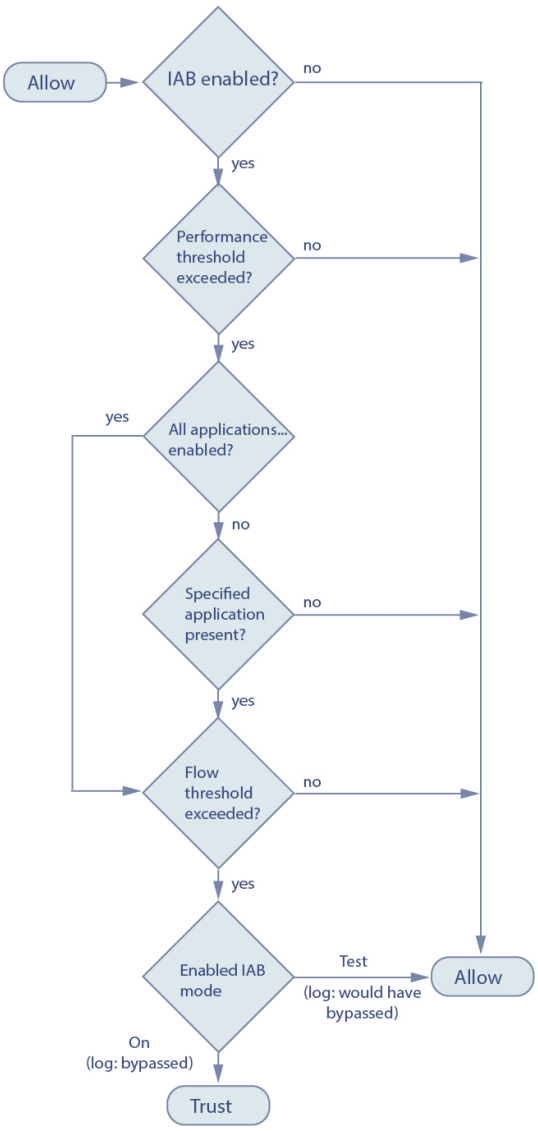
次のトピックでは、インテリジェントアプリケーションバイパス（IAB）を使用するようアクセス コントロール ポリシーを設定する方法について説明します。

IAB の概要

IABは、パフォーマンスとフローのしきい値を超過した場合に追加のインスペクションなしでネットワークを通過する信頼されるアプリケーションを特定します。たとえば、毎晩のバックアップがシステム パフォーマンスに大きく影響する場合、しきい値を超えてもバックアップ アプリケーションが生成したトラフィックを信頼するように設定できます。オプションで、インスペクション パフォーマンスしきい値を超過したときに、IAB が、いずれかのフロー バイパスしきい値を超えるすべてのトラフィックをアプリケーションのタイプに関係なく信頼するように IAB を設定できます。

システムはトラフィックがディープインスペクションの対象となる前に、アクセス コントロール ルールまたはアクセス コントロール ポリシーのデフォルトのアクションで許可されたトラフィック上で IAB を実行します。テスト モードでは、しきい値を超過しているかどうか判断することと、しきい値を超過している場合、IAB を実際に有効化している状態（バイパス モードといいます）であればバイパスされたであろうアプリケーション フローを特定することが可能です。

次の図に、IAB の判断決定プロセスの説明を示します。



IAB オプション

状態（State）

IAB を有効または無効にします。

パフォーマンス サンプル インターバル（Performance Sample Interval）

IAB パフォーマンス サンプリング スキャンの間隔を秒で指定します。この間隔で、システムは、IAB パフォーマンスしきい値と比較するためのシステム パフォーマンス測定値を収集します。値を 0 にすると、IAB が無効になります。

バイパス可能なアプリケーションとフィルタ（Bypassable Applications and Filters）

この機能には、相互に排他的な、次の 2 つのオプションがあります。

アプリケーション/フィルタ（Applications/Filters）
バイパス可能なアプリケーションおよびアプリケーション（フィルタ）のセットを指定できるエディタが提供されます。アプリケーション条件（アプリケーション制御） （479ページ）を参照してください。

未確認アプリケーションを含むすべてのアプリケーション
インスペクション パフォーマンスしきい値を超過すると、アプリケーションのタイプに関係なく、いずれかのフローバイパスしきい値を超過するすべてのトラフィックを信頼します。

パフォーマンスおよびフローのしきい値

少なくとも 1 つのインスペクション パフォーマンスしきい値と 1 つのフロー バイパスしきい値を設定する必要があります。パフォーマンスしきい値を超えていると、システムはフローしきい値を調べ、1 つのしきい値を超えていた場合は、指定されたトラフィックを信頼します。いずれかの複数のものを有効にする場合は、それぞれ 1 つしか超過できません。

インスペクション パフォーマンスしきい値は、侵入インスペクションのパフォーマンスの限界を定めるもので、この限界を超えると、フローしきい値のインスペクションがトリガーされます。IAB は、**0** に設定されている検査パフォーマンスしきい値を使用しません。次の 1 つまたは複数のインスペクション パフォーマンスしきい値を設定できます。

ドロップ率（Drop Percentage）

高価な侵入ルール、ファイル ポリシー、圧縮解除などによるパフォーマンスのオーバーロードのためにパケットがドロップされたときの、パケット全体に対する割合としてドロップされた平均パケット数。これは、侵入ルールなどの通常の設定によってドロップされたパケットを参照するものではありません。1 より大きい整数を指定すると、指定されたパーセンテージのパケットがドロップされたときにIABがアクティブ化することに注意が必要です。**1** を指定すると、0 ～ 1 の任意の割合によって IAB がアクティブになります。これにより、少ないパケット数で IAB がアクティブ化します。

プロセッサ使用率（Processor Utilization Percentage）

使用されたプロセッサ リソースの平均比率。

パッケージ遅延（Package Latency）

マイクロ秒単位の平均パケット遅延。

フロー レート（Flow Rate）

1秒あたりのフロー数で測定される、システムによるフロー処理率。このオプションでは、IAB は、フローを件数ではなくレートで測定するように設定されることに注意が必要です。

フローバイパスしきい値はフローの限界を定めるもので、この限界を超えると、IABは、バイパス モードではバイパス可能なアプリケーションを信頼し、テスト モードでは、アプリケーション トラフィックを許可してさらなるインスペクションの対象にします。IABは、**0** に設定

されているフロー バイパスしきい値を使用しません。次の 1 つまたは複数のフロー バイパスしきい値を設定できます。

フローあたりのバイト数（Bytes per Flow）

フローに含めることができる最大キロバイト数。

フローあたりのパケット数（Packets per Flow）

フローに含めることができる最大パケット数。

フロー継続時間（Flow Duration）

フローを開いたままにできる最大秒数。

フロー速度（Flow Velocity）

最大転送速度（KB/秒）。

IAB の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	Control	いずれか（Any）	いずれか（Any）	Admin Access Admin Network Admin

注意 すべての展開にIABが必要なわけではありません。IABを使用する展開では、限定的な方法でIAB を使用する場合があります。ネットワーク トラフィック、特にアプリケーション トラフィックと、予測可能なパフォーマンスの問題の原因を含むシステムパフォーマンスの専門知識がない場合は、IABを有効にしないでください。IABをバイパスモードで実行する場合は、指定したトラフィックを信頼することでリスクが生じないことを事前に確認してください。

ステップ 1 アクセス コントロール ポリシー エディタで [詳細（Advanced）] タブをクリックし、[インテリジェント アプリケーション バイパス設定（Intelligent Application Bypass Settings）] の横にある編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ポリシーから継承され、設定を変更する権限がありません。 設定がロック解除されている場合は、[Inherit from base policy] をオフにして、編集を有効にします。

ステップ 2 IAB の各オプションを設定します。

- [状態（State）] : IAB を [オフ（Off）] または [オン（On）]、あるいは [テスト（Test）] モードで有効にします。

- [パフォーマンス サンプル間隔（Performance Sample Interval）]：IAB のパフォーマンス サンプリング スキャン間の時間を秒単位で入力します。IAB を有効にする場合は、テスト モードであっても、0 以外の値を入力します。**0** を入力すると、IAB は無効になります。
- バイパス可能なアプリケーションとフィルタ（Bypassable Applications and Filters）：次のいずれかを実行します。
  - バイパスされるアプリケーションとフィルタの数をクリックし、トラフィックをバイパスするアプリケーションを指定します。アプリケーション条件とフィルタの設定 （481 ページ）を参照してください。
  - [未確認アプリケーションを含むすべてのアプリケーション（All applications including unidentified applications）] をクリックし、インスペクション パフォーマンスしきい値を超過したときに、IAB が、いずれかのフロー バイパスしきい値を超えるすべてのトラフィックをアプリケーションのタイプに関係なく信頼するように設定します。
- [インスペクション パフォーマンスしきい値（Inspection Performance Thresholds）]：[設定（Configure）] をクリックし、1 つ以上のしきい値を入力します。
- [フロー バイパスしきい値（Flow Bypass Thresholds）]：[設定（Configure）] をクリックし、1 つ以上のしきい値を入力します。

少なくとも 1 つのインスペクション パフォーマンスしきい値と 1 つのフロー バイパスしきい値を指定する必要があります。IAB がトラフィックを信頼するには、両方を超過する必要があります。各タイプのしきい値を複数入力した場合は、各タイプの 1 つのみを超過する必要があります。詳細については、IAB オプション （1784 ページ）を参照してください。

ステップ 3 [OK] をクリックして IAB 設定を保存します。

ステップ 4 [保存（Save）] をクリックしてポリシーを保存します。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

IAB のロギングと分析

IAB は、接続ロギングを有効にしたかどうかを問わず、バイパスされたフローやバイパスされることが予想されるフローをロギングする接続終了イベントを強制します。接続イベントは、バイパス モードでバイパスされたフロー、またはテスト モードでバイパスされることが予想されるフローを示します。接続イベントに基づいたカスタムのダッシュボード ウィジェットやレポートでは、バイパスされたフローおよびバイパスされることが予想されるフローの長期的な統計情報を表示できます。

IAB の接続イベント

アクション（Action）

[理由（Reason）] に [インテリジェント アプリケーション バイパス（Intelligent App Bypass）] が含まれる場合：

許可（Allow）：

適用された IAB 設定がテスト モードであり、[アプリケーション プロトコル（Application Protocol）] によって指定されたアプリケーションのトラフィックが、インスペクション用に使用可能のままであることを示します。

信頼する（Trust）：

適用された IAB 設定がバイパス モードであり、[アプリケーション プロトコル（Application Protocol）] によって指定されたアプリケーションのトラフィックが信頼されているため、それ以上インスペクションが行われずにネットワークを通過することを示します。

理由（Reason）

[インテリジェント アプリケーション バイパス（Intelligent App Bypass）] は、IAB がバイパス モードまたはテスト モードでイベントをトリガーしたことを示します。

アプリケーション プロトコル（Application Protocol）

このフィールドには、イベントをトリガーしたアプリケーション プロトコルが表示されます。

例

次の省略された図では、一部のフィールドが省かれています。図は、2 つの別個のアクセス コントロール ポリシーの異なる IAB 設定から生成された 2 つの接続イベントの [アクション（Action）]、[理由（Reason）]、および [アプリケーション プロトコル（Application Protocol）] フィールドを示しています。

最初のイベントの場合、[信頼する（Trust）] アクションは、IAB がバイパス モードで有効にされており、Bonjour プロトコル トラフィックが信頼されているため、それ以上インスペクションが行われずに受け渡されることを示します。

2 番目のイベントの場合、[許可（Allow）] アクションは、IAB がテスト モードで有効にされているため、Ubuntu Update Manager トラフィックはさらにインスペクションが行われる必要がありますが、IAB がバイパス モードであればバイパスされることが予想されることを示します。

例

次の省略された図では、一部のフィールドが省かれています。2 番目のイベントのフローは両方とも（[アクション（Action）] : [信頼する（Trust）]、[理由（Reason）] : [インテリジェント アプリケーション バイパス（Intelligent App Bypass）]）をバイパスし、侵入ルール（[理由（Reason）] : [侵入モニタ（Intrusion Monitor）]）によって検査されました。[侵入モニタ（Intrusion Monitor）] の理由は、[イベントの生成（Generate Events）] に設定された侵入ルールが検出されたが、接続時にエクスプロイトをブロックしなかったことを示しています。この例では、これはアプリケーションが検出される前に発生しました。アプリケーションが検出された後、IAB は、アプリケーションがバイパス可能であると認識し、フローを信頼しました。

Last Packet ×	Action ×	Reason ×	Application Protocol ×
2015-06-12 10:53:09	Trust	Intelligent App Bypass	Skype Probe
2015-06-12 10:53:08	Trust	Intelligent App Bypass, Intrusion Monitor	HTTP

404541

IAB のカスタム ダッシュボード ウィジェット

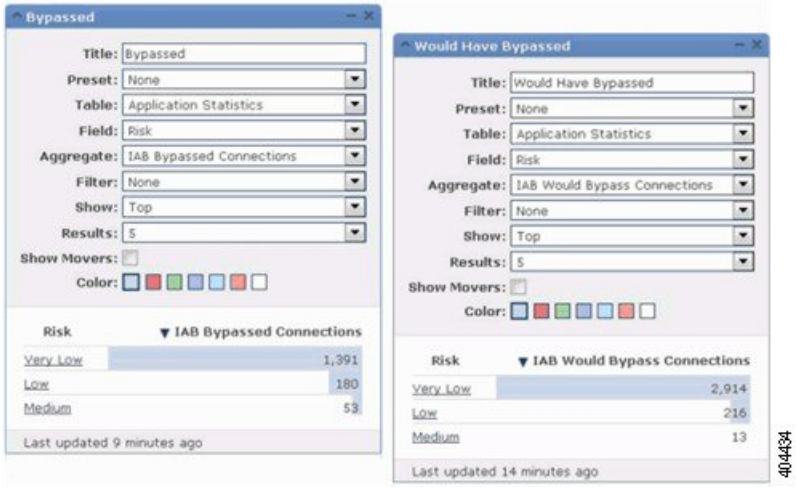
接続イベントに基づいて長期的な IAB の統計情報を表示するカスタム分析ダッシュボード ウィジェットを作成できます。ウィジェットを作成する際には、次の項目を指定します。

- プリセット（Preset）：なし（None）
- テーブル（Table）：**アプリケーションの統計（Application Statistics）**
- フィールド（Field）：任意（any）
- 集約（Aggregate）：次のいずれか
  - IAB が接続をバイパスした（IAB Bypassed Connections）
  - IAB が接続をバイパスすることが予想された（IAB Would Bypass Connections）
- フィールド（Field）：任意（any）

例

次のカスタム分析ダッシュボード ウィジェットの例では、次のようになっています。

- 「*Bypassed*」の例は、アプリケーションがバイパス可能として指定され、IAB が展開済みのアクセス コントロール ポリシーにおいてバイパス モードで有効になっているためにバイパスされたアプリケーション トラフィックの統計を示しています。
- 「*Would Have Bypassed*」の例は、アプリケーションがバイパス可能として指定され、IAB が展開済みのアクセス コントロール ポリシーにおいてテスト モードで有効になっているためにバイパスされることが予想されたアプリケーション トラフィックの統計を示しています。.



IAB のカスタム レポート

接続イベントに基づいて長期的な IAB の統計情報を表示するカスタム レポートを作成できます。レポートを作成する際には、次の項目を指定します。

- テーブル（Table）：**アプリケーションの統計（Application Statistics）**
- プリセット（Preset）：なし（None）
- フィールド（Field）：任意（any）
- X 軸（X-Axis）：任意（any）
- Y 軸（Y-Axis）：以下のいずれか
  - IAB が接続をバイパスした（IAB Bypassed Connections）
  - IAB が接続をバイパスすることが予想された（IAB Would Bypass Connections）

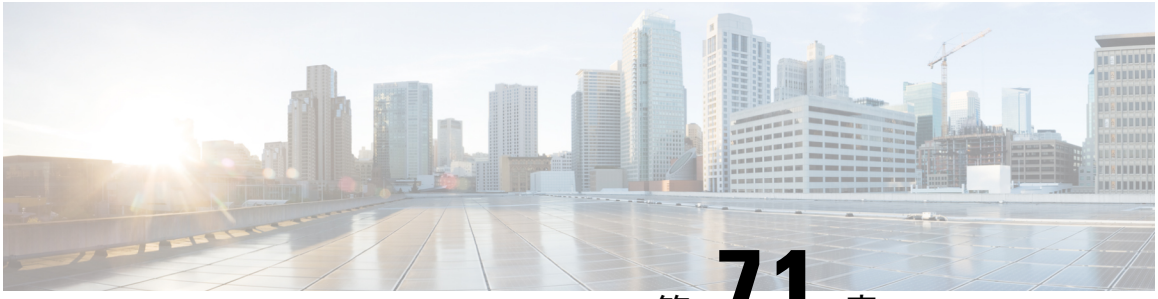
例

次の図は、2 つのレポートの例の抜粋を示します。

- 「*Bypassed*」の例は、アプリケーションがバイパス可能として指定され、IAB が展開済みのアクセス コントロール ポリシーにおいてバイパス モードで有効になっているためにバイパスされたアプリケーション トラフィックの統計を示しています。
- 「*Would Have Bypassed*」の例は、アプリケーションがバイパス可能として指定され、IAB が展開済みのアクセス コントロール ポリシーにおいてテスト モードで有効になっているためにバイパスされることが予想されたアプリケーション トラフィックの統計を示しています。

関連トピック

接続イベントとセキュリティ インテリジェンス イベントのフィールド （3024 ページ）
[カスタム分析（Custom Analysis）] ウィジェット （327 ページ）
ダッシュボードへのウィジェットの追加 （340 ページ）
レポート テンプレート （2775 ページ）



第 71 章

コンテンツ制限を使用したアクセス制御

次のトピックでは、コンテンツ制限機能を使用するようにアクセス コントロール ポリシーを設定する方法について説明します。

コンテンツ制限について

主要な検索エンジンやコンテンツ配信サービスは、検索結果と Web サイトのコンテンツを制限できる機能を提供しています。たとえば学校では、「子どもをインターネットから保護する法律」（CIPA）を順守するために、コンテンツ制限機能を使用します。

コンテンツ制限機能は、検索エンジンやコンテンツ配信サービスで実行する場合には、個々のブラウザやユーザを対象にしか実施できません。FirePOWER システムは、これらの機能をご使用のネットワーク全体に拡大できます。

このシステムにより、以下を実施できます。

- セーフサーチ：多くの主要な検索エンジンでサポートされているこのサービスは、ビジネス、行政、および教育の環境で不愉快であると分類されている、露骨なアダルト向けコンテンツを除外します。システムは、サポートされている検索エンジンのホームページへのユーザのアクセス機能は制限しません。
- *YouTube EDU*：このサービスは、教育環境向けに YouTube コンテンツをフィルタリングします。これにより学校は、教育的なコンテンツへのアクセスを設定しながら、非教育的なコンテンツへのアクセスを制限できます。YouTube EDU は YouTube 制限付きモードとは別の機能であり、Google のセーフサーチ機能の一部として YouTube 検索に対する制限を実施します。YouTube 制限付きモードは、セーフサーチのサブ機能であることに注意してください。YouTube EDU を使用すると、ユーザは標準の YouTube ホームページではなく、YouTube EDU ホームページにアクセスします。

次の 2 つの方法を使用して、これらの機能を実施するようにシステムを設定できます。

方法：アクセス コントロール ルール
コンテンツ制限機能は、検索またはコンテンツ照会の制限状態を、要求URIの要素、関連するCookie、またはカスタムHTTPヘッダー要素により通信します。システムがトラフィックを処理するときに、これらの要素を変更するためのアクセス コントロール ルールを設定できます。

方法：DNS シンクホール
Google 検索では、セーフサーチ（YouTube 制限付きモードを含む）のフィルタを課すGoogle SafeSearch 仮想 IP アドレス（VIP）にトラフィックをリダイレクトするように、システムを設定できます。

次の表では、これらの実施方法の違いについて説明します。

表 *111 :* コンテンツ制限方法の比較

属性	方法：アクセス コントロール ルール	方法：DNS シンクホール
サポートされるデバイス	任意（Any）	Firepower Threat Defense のみ
[サポートされる検索エンジン（Search engines supported）]	ルールエディタの[アプリケーション（Applications）]タブのタグ付きのすべての `safesearch supported`	Google のみ
[サポートされる YouTube 制限付きモード（YouTube Restricted Mode supported）]	あり	あり
[サポートされる YouTube EDU（YouTube EDU supported）]	あり	なし
[SSL ポリシーが必要（SSL policy required）]	あり	なし
[ホストは IPv4 の使用が必要（Hosts must be using IPv4）]	なし	あり
[接続イベント ロギング（Connection event logging）]	あり	あり

使用する方法を決定する際には、次の制限事項を考慮します。

- アクセス コントロール ルール方法には SSL ポリシーが必要で、これはパフォーマンスに影響を及ぼします。
- Google セーフサーチ VIP は IPv4 トラフィックのみをサポートします。Google 検索を管理するように DNS シンクホールを設定する場合は、影響を受けるネットワークのすべてのホストが IPv4 を使用している必要があります。

接続イベントの[理由（Reason）]フィールドに、方法に応じて異なる値がログ記録されます。

- アクセス コントロール ルール：[コンテンツの制限（Content Restriction）]
- DNS シンクホール：[DNS ブロック（DNS Block）]

アクセスコントロールルールを使用したコンテンツ制限の実施

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	Control	いずれか（Any）	いずれか（Any）	Admin/Access Admin/Network Admin

注意 ルールのプリエンプションを避けるため、SSL とアクセス コントロール ポリシーの両方で、YouTube EDU を制御するルールは、セーフサーチを制御するルールの上に配置します（コンテンツ規制ルールの順序 （506 ページ）を参照）。

ステップ 1 SSL ポリシーを作成します。基本的な SSL ポリシーの作成 （1842 ページ）を参照してください。

ステップ 2 セーフサーチと YouTube EDU のトラフィックを処理するための SSL ルールを追加します。

- ルールの [アクション（Action）] として [復号 - 再署名（Decrypt - Resign）] を選択します。システムは、コンテンツ制限処理にこれ以外のアクションをサポートしません。
- [アプリケーション（Applications）] タブで、選択内容を [選択済みのアプリケーションとフィルタ（Selected Applications and Filters）] リストに追加します。
  - YouTube EDU：`YouTube` と `YouTube Upload` アプリケーションを追加します。
  - セーフサーチ：[カテゴリ：検索エンジン（Category: search engine）] フィルタを追加します。

詳細については、アプリケーション条件（アプリケーション制御） （479 ページ）を参照してください。

ステップ 3 追加した SSL ルールのための、ルールの位置を設定します。クリックしてドラッグするか、または右クリック メニューを使用してカット アンド ペーストを実行します。

プリエンプションを避けるため、セーフサーチ ルールを YouTube EDU ルールの後に配置します。

ステップ 4 アクセス コントロール ポリシーを作成または編集して、SSL ポリシーとアクセス コントロール ポリシーを関連付けます。

詳細については、アクセス制御への他のポリシーの関連付け （1684 ページ）を参照してください。

ステップ 5 アクセス コントロール ポリシーに、セーフサーチと YouTube EDU トラフィックを処理するためのルールを追加します。

- ルールの [Action] として [Allow] を選択します。システムは、コンテンツ制限処理にこれ以外のアクションは許可しません。
- [アプリケーション（Applications）] タブで、セーフサーチ（）または YouTube EDU（）のいずれかの淡色表示されているアイコンをクリックして、関連オプションを設定します（アクセス制御ルールのセーフサーチ オプション （1796 ページ）およびアクセス制御ルールの YouTube EDU オプション（1797 ページ）を参照）。

  ルールに [Allow] 以外の [Action] を選択すると、これらのアイコンは淡色表示されるのではなく無効になります。

  同じアクセス コントロール ルールに対してセーフサーチと YouTube EDU の制限を有効にすることはできません。
- [Applications] タブで、[Selected Applications and Filters] リストのアプリケーション選択を絞り込みます。

  たいていの場合、セーフサーチまたは YouTube EDU を有効にすると、[Selected Applications and Filters] リストに適切な値が入力されます。セーフサーチまたは YouTube アプリケーションを有効にしたときにそれらの機能がすでにリストにある場合、システムはリストへの自動入力を行いません。予期したとおりにアプリケーションが入力を行わない場合は、それらを以下のように手動で追加します。

  - YouTube EDU：`YouTube` と `YouTube Upload` アプリケーションを追加します。
  - セーフサーチ：[カテゴリ：検索エンジン（Category: search engine）] フィルタを追加します。

詳細については、アプリケーション条件とフィルタの設定 （481 ページ）を参照してください。

ステップ 6 追加したアクセス コントロール ルールに対してルールの位置を設定します。クリックしてドラッグするか、または右クリック メニューを使用してカット アンド ペーストを実行します。

プリエンプションを避けるため、セーフサーチ ルールを YouTube EDU ルールの後に配置します。

ステップ 7 システムが制限付きコンテンツをブロックするときに表示する HTTP 応答ページを設定します（HTTP 応答ページの選択 （1737 ページ）を参照）。

ステップ 8 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

アクセス制御ルールのセーフサーチ オプション

Firepower System は、特定の検索エンジンのセーフサーチ フィルタリングにのみ対応しています。対応している検索エンジンのリストについては、アクセス制御ルール エディタの [アプリケーション（Applications）] タブのアプリケーションにタグ付けされている `safesearch supported` を参照してください。対応していない検索エンジンのリストについては、アプリケーションにタグ付けされている `safesearch` を参照してください。

アクセス コントロール ルールに対してセーフサーチを有効にするには、次のパラメータを設定します。

セーフサーチを有効にする
このルールに一致するトラフィックに対して、セーフサーチフィルタリングを有効にします。

サポートされない検索トラフィック
サポートされていない検索エンジンからのトラフィックを処理するときにシステムが取るアクションを指定します。[ブロック（Block）] または [リセットによるブロック（Block with Reset）] を選択すると、いつ制限されたコンテンツをブロックするかを表示する HTTP 応答ページを設定する必要があります。HTTP 応答ページの選択 （1737 ページ）

アクセス制御ルールの YouTube EDU オプション

アクセス コントロール ルールに対して YouTube EDU を有効にするには、次のパラメータを設定します。

YouTube EDU の有効化
このルールに一致するトラフィックに対して、YouTube EDU フィルタリングを有効にします。

カスタム ID
学校または地域のネットワークを固有に識別する値を YouTube EDU イニシアチブに指定します。YouTube は、学校または地域が YouTube EDU アカウントの登録をすると、この ID を提供します。

（注） [Enable YouTube EDU] をオンにした場合は、[Custom ID] を入力する必要があります。この ID は、YouTube によって外部に定義されます。システムは、YouTube システムに対するユーザの入力内容は検証しません。無効な ID を入力すると、YouTube EDU の制限が予期したとおりに実行されない場合があります。

DNS シンクホールを使用したコンテンツ制限の実施

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	Firepower Threat Defense	いずれか（Any）	Admin/Access Admin/Network Admin

通常、DNS シンクホールは、トラフィックを特定のターゲットからそらします。この手順では、Google セーフサーチ仮想 IP アドレス（VIP）にトラフィックをリダイレクトする（つまり、Google と YouTube の検索結果にコンテンツ フィルタを適用する）ように DNS シンクホールを設定する方法について説明します。

Google セーフ サーチは VIP に単一の IPv4 アドレスを使用するため、ホストは IPv4 アドレッシングを使用する必要があります。

注意 ネットワークにプロキシ サーバが含まれる場合、Firepower Threat Defense デバイスをプロキシ サーバとインターネットの間に配置しない限り、この方法でのコンテンツ制限は効果的ではありません。

この手順では、Google検索のみにコンテンツ制限を適用する方法について説明します。他の検索エンジンに対してコンテンツ制限を適用する場合は、アクセス コントロール ルールを使用したコンテンツ制限の実施 （1795 ページ）を参照してください。

ステップ 1 次の URL を使用して、サポートされる Google ドメインのリストを取得します。https://www.google.com/supported_domains

ステップ 2 ローカル コンピュータにカスタム DNS リストを作成し、次のエントリを追加します。

- Google セーフサーチを適用するには、サポートされる Google ドメインごとにエントリを追加します。
- YouTube 制限モードを適用するには、「youtube.com」エントリを追加します。

カスタム DNS リストは、テキスト ファイル（.txt）形式にする必要があります。テキスト ファイルの各行に、先頭ピリオドを除いた状態で、個々のドメイン名を指定する必要があります。たとえば、サポートされるドメインが「.google.com」の場合、「google.com」として指定する必要があります。

ステップ 3 カスタム DNS リストを Firepower Management Center にアップロードします（新しいセキュリティ インテリジェンス リストの Firepower Management Center へのアップロード （567 ページ）を参照）。

ステップ 4 Google セーフサーチ VIP の IPv4 アドレスを判別します。たとえば、forcesafesearch.google.com で `nslookup` を実行します。

ステップ 5 セーフサーチ VIP のシンクホール オブジェクトを作成します（シンクホール オブジェクトの作成 （569 ページ）を参照）。

このオブジェクトでは、次の値が使用されます。

- [IPv4 アドレス（IPv4 Address）]：セーフ サーチ VIP アドレスを入力します。
- [IPv6 アドレス（IPv6 Address）]：IPv6 ループバック アドレスを入力します（`::1`）。
- [ログをシンクホールに接続する（Log Connections to Sinkhole）]：このラジオ ボタンをクリックします。
- [タイプ（Type）]：[なし（None）] を選択します。

ステップ 6 基本 DNS ポリシーを作成します（基本 DNS ポリシーの作成 （1753 ページ）を参照）。

ステップ 7 シンクホールの DNS ルールを追加します（DNS ルールの作成および編集 （1756 ページ）を参照）。

このルールでは、

- [有効（Enabled）] チェックボックスをオンにします。
- [アクション（Action）] ドロップダウン リストから [シンクホール（Sinkhole）] を選択します。
- [シンクホール（Sinkhole）] ドロップダウン リストから、作成したシンクホール オブジェクトを選択します。

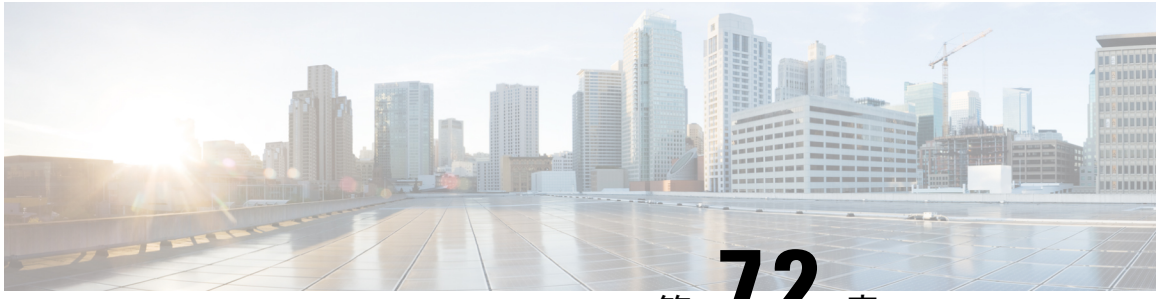
- 作成したカスタム DNS リストを [DNS] タブの [選択した項目（Selected Items）] リストに追加します。
- （オプション）[ネットワーク（Networks）] タブでネットワークを選択し、コンテンツ制限を特定のユーザに限定します。たとえば、学生ユーザにコンテンツ制限を限定したい場合、学生を教員とは別のサブネットに割り当て、このルールにそのサブネットを指定します。

ステップ 8 アクセス コントロール ポリシーと DNS ポリシーを関連付けます（アクセス制御への他のポリシーの関連付け （1684 ページ）を参照）。

ステップ 9 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

第 XVII 部

暗号化トラフィックの処理



第 72 章

トラフィック復号の概要

以下のトピックでは TLS/SSL（Transport Layer Security/Secure Sockets Layer）インスペクションの概要を示し、TLS/SSL インスペクション設定の前提条件と詳細な導入シナリオについて説明します。

（注）

TLS と SSL は相互に使用されることが多いため、*TLS/SSL* という表現を使用していずれかのプロトコルについて説明していることを示しています。SSL プロトコルは、よりセキュアな TLS プロトコルを選択することにより IETF によって廃止されました。そのため、*TLS/SSL* は通常、TLS のみを指すものとして解釈できます。

例外は SSL ポリシーです。FMC 設定オプションは **[Policies]** > **[Access Control]** > **[SSL]** となるため、これらのポリシーは TLS および SSL のトラフィックのルールを定義するために使用されますが、「SSL ポリシー」という用語を使用します。

SSL プロトコルと TLS プロトコルの詳細については、「SSL と TLS：その違いとは（SSL vs. TLS - What's the Difference?）」を参照してください。

トラフィック復号について

デフォルトでは、Firepower システムは SSL（Secure Socket Layer）プロトコルまたはその後継である TLS（Transport Layer Security）プロトコルで暗号化されたトラフィックを検査できません。*TLS/SSL* インスペクションを使用すると、暗号化トラフィックを検査せずにブロックしたり、暗号化または復号化されたトラフィックをアクセス コントロールで検査したりすることができます。システムは、暗号化されたセッションを処理する際にトラフィックに関する詳細を

ログに記録します。暗号化トラフィックのインスペクションと暗号化セッションのデータ分析を組み合わせることで、ネットワーク内の暗号化されたアプリケーションやトラフィックをより詳細に把握したり制御したりできます。

TLS/SSL インスペクションはポリシーベースの機能です。FirePOWER システムでは、アクセス コントロール ポリシーは、SSL ポリシーを含む、サブポリシーおよびその他の設定を呼び出すマスター設定です。アクセス コントロールと SSL ポリシーを関連付ければ、システムはアクセス コントロール ルールで評価する前に、その SSL ポリシーを使用して暗号化セッションを処理します。TLS/SSLインスペクションを設定していない場合、またはデバイスでSSLインスペクションをサポートしていない場合は、アクセス コントロール ルールですべての暗号化トラフィックが処理されます。

TLS/SSLインスペクションの設定で暗号化トラフィックの通過が許可されている場合、アクセスコントロールルールによっても暗号化トラフィックが処理されることに注意してください。ただし、一部のアクセス コントロール ルールの条件では暗号化されていないトラフィックを必要とするため、暗号化されたトラフィックに一致するルール数が少なくなる場合があります。またデフォルトでは、システムは暗号化ペイロードの侵入およびファイルインスペクションを無効にしています。これにより、侵入およびファイルインスペクションが設定されたアクセス コントロール ルールに暗号化接続が一致したときの誤検出が減少し、パフォーマンスが向上します。

システムで TCP 接続での TLS/SSL ハンドシェイクが検出された場合、その検出されたトラフィックを復号できるかどうかが判定されます。復号できない場合は、設定されたアクションが適用されます。以下のアクションを設定できます。

- 暗号化トラフィックをブロックする
- 暗号化トラフィックをブロックし、TCP 接続をリセットする
- 暗号化トラフィックを復号しない

システムによるトラフィックの復号が可能な場合、システムでは、それ以上のインスペクションを行わずにトラフィックをブロックするか、復号されていないトラフィックをアクセスコントロールによって評価するか、または次のいずれかの方法を使用して復号します。

- 既知の秘密キーを使用して復号化する。外部ホストがネットワーク上のサーバとのTLS/SSLハンドシェイクを開始すると、交換されたサーバ証明書とシステムにアップロード済みのサーバ証明書が照合されます。次に、アップロード済みの秘密キーを使用してトラフィックを復号します。
- サーバ証明書の再署名によって復号する。ネットワーク上のホストが外部サーバとのTLS/SSLハンドシェイクを開始すると、システムによって、交換されたサーバ証明書が、アップロード済みの認証局（CA）証明書で再署名されます。次に、アップロード済みの秘密キーを使用してトラフィックを復号します。

復号されたトラフィックに対しては、はじめから暗号化されていないトラフィックと同じトラフィックの処理と分析（ネットワーク、レピュテーション、およびユーザベースの各アクセスコントロール、侵入検知と防御、Cisco Advanced Malware Protection（Cisco AMP）、およびディ

スカバリ（検出））が実行されます。システムで、復号されたトラフィックのポスト分析をブロックしない場合、トラフィックを再暗号化してから宛先ホストに渡します。

（注） 管理対象デバイスが暗号化されたトラフィックを処理する場合にのみ、復号ルールをセットアップします。復号ルールには、パフォーマンスに影響を及ぼす可能性があるオーバーヘッドの処理が必要です。

Firepower システムは現在、TLS バージョン 1.3 の暗号化または復号化をサポートしていません。ユーザが TLS 1.3 暗号化をネゴシエートする Web サイトにアクセスすると、Web ブラウザに次のようなエラーが表示されることがあります。

- **ERR_SSL_PROTOCOL_ERROR**
- **SEC_ERROR_BAD_SIGNATURE**
- **ERR_SSL_VERSION_INTERFERENCE**

この動作を制御する方法の詳細については、Cisco TAC にお問い合わせください。

TLS/SSL ハンドシェイク処理

このマニュアルでは、*TLS/SSL* ハンドシェイクという用語は SSL プロトコルとその後継プロトコルである TLS の両方の暗号化セッションを開始する、2 ウェイ ハンドシェイクを表します。

インライン展開では、Firepower システムは TLS/SSL ハンドシェイクを処理し、ClientHello メッセージを修正する可能性があり、セッションの TCP プロキシ サーバとして機能します。

（正常に TCP 3 ウェイ ハンドシェイクが完了した後）クライアントがサーバとの TCP 接続を確立すると、管理対象デバイスは TCP セッションでの暗号化されたセッションの開始の試行をモニタします。TLS/SSL ハンドシェイクは、クライアントとサーバ間の特殊なパケットの交換によって、暗号化セッションを確立します。SSL と TLS プロトコルでは、これらの特殊なパケットはハンドシェイク メッセージと呼ばれます。ハンドシェイク メッセージは、クライアントとサーバの両方がサポートする暗号化属性を伝えます。

- ClientHello：クライアントは各暗号化属性に複数のサポートされる値を指定します。
- ServerHello：サーバはシステムがセキュリティで保護されたセッション中に使用する暗号化方式を決定する、各暗号化属性に 1 つのサポートされる値を指定します。

セッション中に伝送されるデータは暗号化されますが、ハンドシェイク メッセージは暗号化されません。

TLS/SSL ハンドシェイクが完了すると、管理対象デバイスは暗号化セッション データをキャッシュに保存し、それによりフル ハンドシェイクを必要とせずにセッションを再開できます。管理対象デバイスもサーバ証明書データをキャッシュに保存し、それにより後続のセッションでのより速いハンドシェイクの処理が可能になります。

ClientHello メッセージ処理

セキュアな接続が確立できる場合、クライアントはパケットの宛先として機能するサーバに ClientHello メッセージを送信します。クライアントは TLS/SSL ハンドシェイクを開始するメッセージを送信するか、または宛先サーバからの Hello Request メッセージへの応答に含めます。

TLS/SSL 復号化を設定した場合、管理対象デバイスが ClientHello メッセージを受信すると、システムはそのメッセージを [復号-再署名（Decrypt - Resign）] アクションを含む TLS/SSL ルールと照合しようとします。照合は ClientHello メッセージからのデータとキャッシュされたサーバ証明書データからのデータに依存します。考えられるデータには次のものがあります。

表 *112 : TLS/SSL* ルール条件のデータ可用性

TLS/SSL ルール条件	データの存在場所
ゾーン	ClientHello
Networks	ClientHello
VLAN タグ	ClientHello
ポート	ClientHello
ユーザ	ClientHello
アプリケーション	ClientHello（サーバ名インジケータの拡張機能）
カテゴリ	ClientHello（サーバ名インジケータの拡張機能）
Certificate	サーバ証明書（キャッシュされている可能性あり）
Distinguished Names	サーバ証明書（キャッシュされている可能性あり）
証明書のステータス	サーバ証明書（キャッシュされている可能性あり）
暗号スイート	ServerHello
Versions	ServerHello

ClientHello メッセージが [復号 - 再署名（Decrypt - Resign）] ルールに一致しない場合、システムはメッセージを変更しません。次に、メッセージがアクセス コントロール評価（ディープインスペクションを含めることができる）で合格するかどうかを決定します。メッセージが合格すれば、システムはそれを宛先サーバに送信します。

メッセージが [復号 - 再署名（Decrypt - Resign）] ルールに一致したら、システムは ClientHello メッセージを次のように変更します。

- 圧縮方法：クライアントがサポートする圧縮方法を指定する、`compression_methods` 要素を削除します。FirePOWER システムは圧縮されたセッションを復号化することはできません。この変更により、復号化できないトラフィックの圧縮されたセッションタイプが削減されます。
- 暗号スイート：Firepower システムがサポートしない場合、`cipher_suites` 要素から暗号スイートを削除します。FirePOWER システムが指定した暗号スイートのいずれもサポートしない場合、システムは、元の変更されていない要素を送信します。この変更により、復号化できないトラフィックのサポートされない暗号スイートと不明な暗号スイートが削減されます。
- セッション識別子：キャッシュされたセッション データと一致しない SessionTicket 拡張機能と `Session Identifier` 要素から値を削除します。ClientHello 値がキャッシュされたデータと一致した場合、一時停止したセッションは、クライアントとサーバが完全な TLS/SSL ハンドシェイクを実行せずに、中断したセッションを再開できます。この変更は、セッション再開の可能性を高め、復号化できないトラフィックのセッションが未キャッシュのタイプを削減します。
- 楕円曲線：FirePOWER システムがサポートしない場合、サポートされる楕円曲線拡張機能から楕円曲線を削除します。Firepower システムが指定した楕円曲線のいずれもサポートしない場合、管理対象デバイスは拡張機能を削除し、`cipher_suites` 要素から関連する暗号スイートを削除します。
- ALPN 拡張機能：Firepower システムでサポートされていないアプリケーション層プロトコル ネゴシエーション（ALPN）拡張機能から値を削除します（たとえば、SPDY と HTTP/2 プロトコル）。
- 他の拡張機能：Next Protocol Negotiation（NPN）および TLS チャネル ID 拡張機能を削除します。

（注） システムはデフォルトで ClientHello の変更を実行します。SSL ポリシーが正しく設定されていると、このデフォルトの動作により、トラフィックの復号化がより頻繁に発生します。各ネットワークにおけるデフォルトの動作を調整するには、Cisco TAC にお問い合わせください。

システムが ClientHello メッセージを変更した後、メッセージがアクセス コントロール評価（ディープインスペクションを含めることができる）を合格するかどうかを決定します。メッセージが合格すれば、システムはそれを宛先サーバに送信します。

メッセージを変更した後はクライアントおよびサーバで計算されたメッセージ認証コード（MAC）が一致しなくなるため、TLS/SSL ハンドシェイク時のクライアントとサーバの間の直接通信はできなくなります。すべての後続のハンドシェイク メッセージ（および一度設定された暗号化セッションに対し）、管理対象デバイスは、中間者（MITM）として機能します。ここでは 2 つの TLS/SSL セッションが作成され、1 つはクライアントと管理対象デバイスの間、もう 1 つは管理対象デバイスとサーバの間で使用されます。その結果、暗号セッションの詳細はセッションごとに異なります。

（注） Firepower システムが復号できる暗号スイートは頻繁に更新されるので、TLS/SSL ルールの条件で使用可能な暗号スイートと直接対応しません。復号できる暗号スイートの現在のリストについては、Cisco TAC に連絡してください。

関連トピック

復号できないトラフィックのデフォルト処理オプション （1839 ページ）
インライン展開での再署名証明書を使用した暗号化トラフィック インスペクション （1831 ページ）

ServerHello とサーバ証明書メッセージの処理

ServerHello メッセージは、正常な TLS/SSL ハンドシェイクの ClientHello メッセージへの応答です。

管理対象デバイスが ClientHello メッセージを処理し、宛先サーバに送信した後、サーバはクライアントがメッセージで指定した復号属性をサポートするかどうかを決定します。その属性をサポートしない場合、サーバはクライアントにハンドシェイクの失敗のアラートを送信します。その属性をサポートする場合、サーバは ServerHello メッセージを送信します。同意済みキー交換方式が認証に証明書を使用する場合、サーバ証明書メッセージはすぐに ServerHello メッセージに続きます。

管理対象デバイスがこれらのメッセージを受信すると、TLS/SSL ルールとの一致を試みます。これらのメッセージには、ClientHello メッセージまたはセッション データ キャッシュにはなかった情報が含まれます。具体的には、システムは、識別名、証明書のステータス、暗号スイート、およびバージョン条件でのこれらのメッセージと一致する可能性があります。

メッセージが TLS/SSL ルールと一致しない場合、管理対象デバイスは、SSL ポリシーのデフォルトのアクションを実行します。詳細については、SSL ポリシーのデフォルト アクション （1838 ページ）を参照してください。

メッセージが SSL ルールに一致する場合、管理対象デバイスは、必要に応じて次に進みます。

アクション：Monitor
TLS/SSL ハンドシェイクは完了に進みます。管理対象デバイスは追跡およびログに記録しますが、暗号化トラックを復号化しません。

アクション：Block または Block with Reset
管理対象デバイスは、TLS/SSL セッションをブロックします。必要に応じて、TCP 接続もリセットします。

アクション：Do Not Decrypt
TLS/SSL ハンドシェイクは完了に進みます。管理対象デバイスは、TLS/SSL セッションの間で交換されるアプリケーション データを復号しません。

アクション：復号 - 既知のキー（Decrypt - Known Key）

管理対象デバイスは、以前に Firepower Management Center にインポートした内部証明書オブジェクトをサーバ証明書データに一致させようとします。内部証明書オブジェクトは作成できないため、また、秘密キーを所有する必要があるため、既知のキー復号化を使用しているサーバを所有していることを想定しています。

証明書が既知の証明書と一致した場合、TLS/SSL ハンドシェイクは完了に進みます。管理対象デバイスはアップロードされた秘密キーを使用して、TLS/SSL セッション中に交換されたアプリケーション データを復号および再暗号化します。

クライアントとの初回接続と後続の接続の間でサーバが証明書を変更した場合、将来の接続を復号化するには、Firepower Management Center に新しいサーバ証明書をインポートする必要があります。

アクション：復号 - 再署名（Decrypt - Resign）

管理対象デバイスはサーバ証明書メッセージを処理し、サーバ証明書に以前にインポートまたは生成した認証局（CA）で再署名します。TLS/SSL ハンドシェイクは完了に進みます。管理対象デバイスはアップロードされた秘密キーを使用して、TLS/SSL セッション中に交換されたアプリケーション データを復号および再暗号化します。

TLS 暗号化アクセラレーション

TLS 暗号化アクセラレーション 次のことを促進します。

- TLS/SSL 暗号化および復号化
- VPN（TLS/SSL および IPsec を含む）

サポート対象ハードウェア

以下のハードウェア モデルは TLS 暗号化アクセラレーションをサポートしています。

- Firepower Threat Defense を搭載した Firepower 2100
- Firepower Threat Defense を搭載した Firepower 4100/9300

  Firepower 4100/9300 FTD コンテナ インスタンスでの TLS 暗号化アクセラレーションのサポートの詳細については、『*FXOS Configuration Guide*』を参照してください。

仮想アプライアンス上および上記以外のハードウェアでの TLS 暗号化アクセラレーション はサポートされていません。

（注） TLS 暗号化アクセラレーションおよび 4100/9300 の詳細については、『*FXOS Configuration Guide*』を参照してください。

サポートしている機能 TLS 暗号化アクセラレーション

TLS 暗号化アクセラレーション でサポートしている機能は次のとおりです。

- IPv4-in-IPv4 tunneled protocols only are supported; other tunneled IP protocols are *not* supported.
- Generic Routing Encapsulation（GRE）トンネルでカプセル化された TLS/SSL トラフィックの復号化

サポートしていない機能 TLS 暗号化アクセラレーション

TLS 暗号化アクセラレーション でサポートしていない機能は次のとおりです。

- インスペクション エンジンが接続を維持するように設定されていて、インスペクション エンジンが予期せず失敗した場合は、エンジンが再起動されるまでTLS/SSL トラフィックはドロップされます。

  この動作はによって制御されます、**configure snort preserve-connection {enable | disable}**コマンド。

TLS 暗号化アクセラレーション 注意事項と制約事項

管理対象デバイスが TLS 暗号化アクセラレーションが有効になっている場合は、次の点に留意してください。

HTTP のみのパフォーマンス

トラフィックを復号しない管理対象デバイスでTLS暗号化アクセラレーションを使用すると、パフォーマンスに影響を与えることがあります。

Federal Information Processing Standards（FIPS）

TLS暗号化アクセラレーションと連邦情報処理標準（FIPS）が両方とも有効になっている場合は、次のオプションの接続が失敗します。

- サイズが 2048 バイト未満の RSA キー
- Rivest 暗号 4（RC4）
- Single Data Encryption Standard (single DES)
- Merkle–Damgard 5（MD5）
- SSL v3

セキュリティ認定準拠モードで動作するようにFirepower Management Center と管理対象デバイスを設定すると、FIPSが有効になります。このモードで動作しているときに接続を許可するには、よりセキュアなオプションを採用するように Web ブラウザを設定します。

詳細については、次を参照してください。

- FIPS でサポートされている暗号方式：SSL 設定について （1372 ページ）。

- セキュリティ認定準拠のモード （1411 ページ）。
- コモン クライテリア。

TLS ハートビート

一部のアプリケーションでは、RFC6520 で定義されている Transport Layer Security（TLS）および Datagram Transport Layer Security（DTLS）プロトコルに対して、TLS ハートビート エクステンションが使用されます。TLS ハートビートは、接続がまだ有効であることを確認する方法を提供します。クライアントまたはサーバが指定されたバイト数のデータを送信し、応答を返すように相手に要求します。これが成功した場合は、暗号化されたデータが送信されます。

TLS 暗号化アクセラレーションが有効になっている管理対象デバイスが TLS ハートビート エクステンションを使用するパケットを扱うときは、管理対象デバイスは SSL ポリシーの [Undecryptable Actions] の [Decryption Errors] の設定で指定されたアクションを行います。

- Block
- Block with reset

詳細については、復号できないトラフィックのデフォルト処理オプション （1839ページ）を参照してください。

アプリケーションが TLS ハートビートを使用しているかどうかを判断するには、TLS ハートビートのトラブルシューティング （1900 ページ）を参照してください。

管理対象デバイスが をサポートしていない場合、または TLS 暗号化アクセラレーションが無効になっている場合は、ネットワーク分析ポリシー（NAP）で [Max Heartbeat Length] を設定して TLS ハートビートの処理方法を決定できます。詳細については、SSL プリプロセッサ （2379 ページ）を参照してください。

TLS/SSL オーバーサブスクリプション

TLS/SSL オーバーサブスクリプションとは、管理対象デバイスが TLS/SSL トラフィックにより過負荷になっている状態です。すべての管理対象デバイスで TLS/SSL オーバーサブスクリプションが発生する可能性がありますが、TLS 暗号化アクセラレーションをサポートする管理対象デバイスでのみ処理方法を設定できます。

TLS 暗号化アクセラレーションが有効になっている管理対象デバイスがオーバーサブスクライブされた場合、管理対象デバイスによって受信されるパケットの扱いは、SSL ポリシーの [Undecryptable Actions] の [Handshake Errors] の設定に従います。

- デフォルト アクションを継承（Inherit default action）
- Do not decrypt
- Block
- Block with reset

SSL ポリシーの [Undecryptable Actions] の [Handshake Errors] の設定が [Do Not decrypt] で、関連付けられたアクセス コントロール ポリシーがトラフィックを検査するように設定されている場合は、インスペクションが行われます。復号は行われません。

大量のオーバーサブスクリプションが発生している場合は、次のオプションがあります。

- 管理対象デバイスをアップグレードして、TLS/SSL の処理能力を向上させます。
- SSL ポリシーを変更して、復号の優先順位が高くないトラフィック用に [Do Not Decrypt] ルールを追加します。

のステータスの表示 TLS 暗号化アクセラレーション

このトピックでは、TLS暗号化アクセラレーションが有効になっているかどうかを確認する方法について説明します。

Firepower Management Center で次のタスクを実行します。

ステップ 1 Firepower Management Center にログインします。

ステップ 2 **[デバイス（Devices）] > [デバイス管理（Device Management）]** をクリックします。

ステップ 3 （編集）をクリックして、管理対象デバイスを編集します。

ステップ 4 [デバイス（Device）] タブ ページをクリックします。TLS 暗号化アクセラレーション ステータスが [全般（General）] セクションに表示されます。

TLS/SSL ベスト プラクティス

ここでは、復号化ポリシーとルールの作成時に注意する必要がある情報について説明します。

（注） TLS と SSL は相互に使用されることが多いため、*TLS/SSL* という表現を使用していずれかのプロトコルについて説明していることを示しています。SSLプロトコルは、よりセキュアなTLSプロトコルを選択することによりIETFによって廃止されました。そのため、*TLS/SSL* は通常、TLS のみを指すものとして解釈できます。

例外は SSL ポリシーです。FMC 設定オプションは **[Policies]** > **[Access Control]** > **[SSL]** となるため、これらのポリシーは TLS および SSL のトフィックのルールを定義するために使用されますが、「SSL ポリシー」という用語を使用します。

SSL プロトコルと TLS プロトコルの詳細については、「SSL と TLS：その違いとは（SSL vs. TLS - What's the Difference?）」を参照してください。

関連トピック

復号化のケース （1813 ページ）

復号化のケース

Firepower システムの脅威に対する防御およびポリシーの適用機能を利用できるのは、復号化されたトラフィックのみです。Firepower システムを通過するときに暗号化されたトラフィックは許可またはブロックできるだけで、ディープインスペクションまたはすべての範囲のポリシー適用（侵入防御など）を対象にすることはできません。

すべての暗号化された接続は次のように処理されます。

- 復号化またはブロックする必要があるかどうかを判断するために、TLS/SSL 復号化ポリシーを介して送信されます。

  また、TLS/SSL の復号化ルールを設定し、非セキュアな SSL プロトコルを使用するトラフィックや、期限切れまたは無効な証明書を使用するトラフィックなど、ネットワークに必要ないとわかっているタイプの暗号化トラフィックをブロックすることもできます。

- ブロックされていない接続は、復号化されているかどうかにかかわらず、許可またはブロックの最終的な決定のためアクセス コントロール ポリシーを経由します。

トラフィックの復号とその後の再暗号化は、全体的なシステム パフォーマンスを低下させるデバイスの処理負荷が増加することに注意してください。

次に要約を示します。

- 暗号化されたトラフィックはポリシーで許可またはブロックすることができます。暗号化されたトラフィックは検査できません
- 復号化されたトラフィックは脅威に対する防御とポリシーの適用に従います。復号化されたトラフィックはポリシーで許可またはブロックできます

関連トピック

ディープ インスペクションについて （1707 ページ）

トラフィックを復号化する場合としない場合

ここでは、トラフィックを復号する場合と暗号化されたファイアウォールの通過を許可する場合のガイドラインを示します。

トラフィックを復号化しない場合

次によって禁止されている場合は、トラフィックを復号してはいけません。

- 法律：たとえば、一部の法域では、財務情報の復号化が禁止されています

- 会社のポリシー：たとえば、会社によって特権的な通信の復号化が禁止されている場合があります
- プライバシー規制
- 証明書のピン留め（*TLS/SSL* ピニングとも呼ばれる）を使用するトラフィックは、接続の切断を防ぐため、暗号化されたままにする必要があります

特定の種類のトラフィックで復号をバイパスする場合、トラフィックの処理は行われません。暗号化トラフィックは、最初に SSL ポリシーによって評価された後でアクセス コントロール ポリシーに進み、そこで最終的な許可またはブロックの決定が行われます。暗号化されたトラフィックは、次のものを含むがこれらに限定されない任意の TLS/SSL ルール条件で許可またはブロックできます。

- 証明書のステータス（期限切れまたは無効な証明書など）
- プロトコル（セキュアでない SSL プロトコルなど）
- ネットワーク（セキュリティ ゾーン、IP アドレス、VLAN タグなど）
- 正確な URL または URL カテゴリ
- [ポート（Port）]
- ユーザ グループ

SSL ポリシーは、このトラフィックに対して [復号しない（Do not Decrypt）] アクションを提供します。詳細については、TLS/SSL ルール：復号しないアクション（1865 ページ）を参照してください。

（注） このトピックの最後にある関連情報リンクでは、ルール評価のいくつかの側面について説明します。URL やアプリケーション フィルタリングなどの条件には、暗号化されたトラフィックに関する制限があります。これらの制限事項を必ず確認してください。

トラフィックを復号化する場合

Firepower システムの脅威に対する防御とポリシーの適用機能を利用できるのは、暗号化されたすべてのトラフィックです。管理対象デバイスでトラフィックの復号化を許可する場合（メモリと処理能力に基づいて）、法律または規制によって保護されていないトラフィックを復号化する必要があります。復号化するトラフィックを決定する必要がある場合は、ネットワーク上のトラフィックを許可するリスクに基づいて決定します。Firepower システムは、URL の評価、暗号スイート、プロトコル、その他多くの要因を含む、ルール条件を使用してトラフィックを分類するための柔軟なフレームワークを提供します。

Firepower システムには 2 つの復号方式があります。これについては次の項で説明します。

関連トピック

復号と再署名（発信トラフィック） （1815 ページ）

既知のキーでの復号（着信トラフィック） （1815 ページ）
TLS/SSL ルールのガイドラインと制限事項 （1848 ページ）
SSL ルールの順序 （507 ページ）
URL 条件（URL フィルタリング） （489 ページ）
アプリケーション ルールの順序 （506 ページ）

復号と再署名（発信トラフィック）

[復号と再署名（Decrypt - Resign）] TLS/SSLルール アクションでは、Firepower システムは中間者となり、傍受、復号化、および検査（トラフィックが許可されている場合）し、再暗号化することができます。[復号と再署名（Decrypt - Resign）] ルール アクションは発信トラフィックで使用されます。つまり、宛先サーバは保護ネットワーク外にあります。

FTD デバイスは、ルールで指定された内部認証局（CA）オブジェクトを使用してクライアントとネゴシエートし、クライアントと FTD デバイス間に SSL トンネルを構築します。同時に、デバイスは宛先 web サイトに接続し、サーバと FTD デバイス間に SSL トンネルを作成します。

このため、クライアントには、宛先サーバからの証明書ではなく、SSL 復号化ルールで設定された CA 証明書が表示されます。クライアントは、接続を完了するために証明書を信頼する必要があります。FTD デバイスは、クライアントと宛先サーバ間のトラフィックで両方向に復号化/再暗号化を実行します。

前提条件

[復号と再署名（Decrypt - Resign）] ルール アクションを使用するには、CA ファイルとペアの秘密キー ファイルを使用して、内部 CA オブジェクトを作成する必要があります。CA と秘密キーをまだ使用していない場合は、Firepower システムで生成できます。

関連トピック

TLS/SSL ルールの復号アクション （1866 ページ）
外部証明書オブジェクト （589 ページ）

既知のキーでの復号（着信トラフィック）

[復号 - 既知のキー（Decrypt - Known Key）] TLS/SSLルール アクションでは、サーバの秘密キーを使用してトラフィックを復号化します。[復号 - 既知のキー（Decrypt - Known Key）] ルール アクションは着信トラフィックで使用されます。つまり、宛先サーバは保護ネットワーク内にあります。

既知のキーを使用して復号化する主な目的は、社内サーバを外部の攻撃から保護することです。

前提条件

[復号 - 既知のキー（Decrypt - Known Key）] ルール アクションを使用するには、サーバの証明書ファイルとペアの秘密キーファイルを使用して、内部証明書オブジェクトを作成する必要があります。

関連トピック

TLS/SSL ルールの復号アクション （1866 ページ）
内部証明書オブジェクト （590 ページ）

TLS/SSL のその他のルール アクション

次の項では、TLS/SSL のその他のルール アクションについて説明します。

関連トピック

TLS/SSL ルールのブロック アクション （1865 ページ）
TLS/SSL ルールのモニタ アクション （1864 ページ）

TLS/SSL ルールの例

次の項では、TLS/SSL の推奨ルールの設定例を示します。

関連トピック

非セキュアなプロトコルのブロック （1816 ページ）

非セキュアなプロトコルのブロック

この例では、TLS 1.0、TLS 1.1、SSLv3 などのセキュアと見なされなくなったネットワーク上の TLS および SSL プロトコルをブロックする方法を示します。

非セキュアなプロトコルはすべてエクスプロイト可能なため、ネットワークから除外する必要があります。この例では、以下の通りなります。

- SSL ルールの [バージョン（Version）] タブ ページを使用して、一部のプロトコルをブロックすることができます。
- Firepower システムでは SSLv2 が復号化できないと見なされるため、SSL ポリシーの [復号不可のアクション（Undecryptable Actions）] を使用してブロックできます。

ステップ 1 まだ Firepower 管理システムにログインしていない場合は、ログインします。

ステップ 2 **[ポリシー（Policies）] > [アクセスコントロール（Access Control）] > [SSL]** の順にクリックします。

ステップ 3 SSL ポリシーを追加または編集します。

ステップ 4 [ルールの追加（Add Rule）] をクリックします。

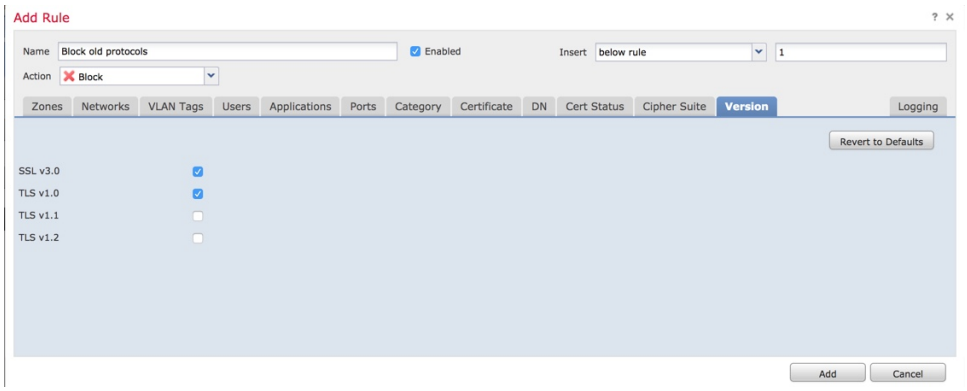
ステップ 5 [名前（Name）] フィールドにルールの名前を入力します。

ステップ 6 [アクション（Action）] リストから [ブロック（Block）] または [リセットしてブロック（Block with reset）] をクリックします。

ステップ 7 [バージョン（Version）] タブ ページをクリックします。

ステップ 8 **SSL v3.0**、**TLS 1.0**、**TLS 1.1** など、セキュアでなくなったプロトコルのチェックボックスをオンにします。引き続きセキュアと見なされているプロトコルのチェックボックスをオフにします。

次の図は例を示しています。

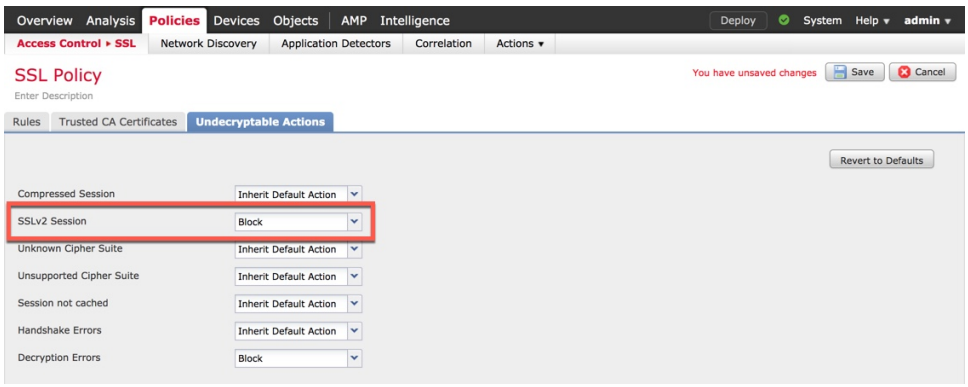


ステップ 9 必要に応じて他のルール条件を選択します。

ステップ 10 ルールを保存します。

ステップ 11 SSL ポリシー ページで [復号できないアクション（Undecryptable Actions）] をクリックします。

ステップ 12 [SSLv2セッション（SSLv2 Session）] リストから [ブロック（Block）] または [リセットしてブロック（Block with reset）] をクリックします。次の図は例を示しています。



ステップ 13 [保存（Save）] をクリックします。

ステップ 14 これは特定のルールであるため、アプリケーション一致ルールなどの一般的なルールよりもポリシー内で上位に配置します。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

関連トピック

TLS/SSL ルール条件 （1861 ページ）

TLS/SSL ルールのコンポーネント

各 TLS/SSL ルールには、次のコンポーネントがあります。

状態

デフォルトでは、ルールが有効状態になります。無効にしたルールはネットワーク トラフィックの評価には使用されなくなり、そのルールの場合の警告とエラーの生成が停止されます。

位置

SSL ポリシーのルールには 1 から始まる番号が付いています。システムは、ルール番号の昇順で上から順に、ルールをトラフィックと照合します。Monitor ルールを除き、トラフィックが最初に一致するルールが、当該トラフィックを処理するためのルールになります。

条件

条件は、ルールで処理する特定のトラフィックを指定します。こうした条件では、セキュリティゾーン、ネットワークまたは地理的位置、VLAN、ポート、アプリケーション、要求された URL、ユーザ、証明書、証明書のサブジェクトまたは発行元、証明書ステータス、暗号スイート、暗号化プロトコルバージョンなどによってトラフィックを照合できます。使用する条件は、ターゲット デバイスのライセンスによって異なります。

操作（Action）

ルールのアクションは、一致したトラフィックの処理方法を決定します。暗号化された一致したトラフィックは、モニタ、許可、ブロック、または復号できます。復号および許可された暗号化トラフィックは、さらなる検査の影響下に置かれます。システムは、ブロックされた暗号化トラフィックに対してはインスペクションを実行**しない**ことに注意してください。

ログ

ルールのロギング設定は、システムが処理するトラフィックのレコードの維持を制御します。各ルールに一致したトラフィックのレコードを維持できます。SSL ポリシーでの設定に従って、システムが暗号化セッションをブロックするか、あるいは復号なしで渡すことを許可するときに、その接続をログに記録できます。アクセス コントロール ルールに従ってより詳細な評価のために復号化した場合の接続ログを記録するようにシステムを強制することも可能で、これはその後でどのような処理やトラフィックの検査がされるかとは無関係です。接続のログは、Firepower Management Center のデータベースの他に、システム ログ（Syslog）または SNMP トラップ サーバに記録できます。

ログ方法の詳細については、接続のロギングのベストプラクティス（3012 ページ）を参照してください。

ヒント　TLS/SSL ルールを適切に作成し順序付けするのは複雑なタスクです。ポリシーを慎重に計画しないと、ルールが他のルールをプリエンプション処理したり、追加のライセンスが必要となったり、ルールに無効な設定が含まれる場合があります。予期したとおりにトラフィックが確実に処理されるようにするために、SSL ポリシー インターフェイスには、ルールに関する強力な警告およびエラーのフィードバック システムが用意されています。

関連トピック

インターフェイス条件 （468 ページ）
ネットワーク条件 （471 ページ）
VLAN 条件 （476 ページ）
ポートおよび ICMP コードの条件 （477 ページ）
アプリケーション条件（アプリケーション制御） （479 ページ）
URL 条件（URL フィルタリング） （489 ページ）
ユーザ条件、レルム条件、および ISE 属性条件（ユーザ制御） （490 ページ）
ルールのパフォーマンスに関するガイドライン （502 ページ）
TLS/SSL ルールのガイドラインと制限事項 （1848 ページ）

TLS/SSL ルールの順序の評価

SSL ポリシーで TLS/SSL ルールを作成する場合、ルール エディタの [挿入（Insert）] リストを使用してその位置を指定します。SSL ポリシー内の TLS/SSL ルールには、1 から始まる番号が付けられています。システムは、ルール番号の昇順で上から順に、TLS/SSL ルールをトラフィックと照合します。

ほとんどの場合、システムによるネットワーク トラフィックの処理は、すべてのルールの条件がトラフィックに一致する最初の TLS/SSLSSL ルールに従って行われます。モニタ ルール（トラフィックをログに記録するがトラフィック フローには影響しないルール）の場合を除き、システムは、そのトラフィックがルールに一致した後、追加の優先順位の低いルールに対してトラフィックを評価し続けることはありません。こうした条件には、単純なものと複雑なものがあります。セキュリティ ゾーン、ネットワークまたは地理的位置、VLAN、ポート、アプリケーション、要求された URL、ユーザ、証明書、証明書の識別名、証明書ステータス、暗号スイート、暗号化プロトコル バージョンなどによってトラフィックを制御できます。

各ルールにはアクションも設定されます。アクションにより、アクセス制御と一致する暗号化または復号化トラフィックに対してモニタ、ブロック、検査のいずれを行うかが決まります。システムがブロックした暗号化トラフィックは、それ以上のインスペクションが行われないことに注意してください。暗号化されたトラフィックおよび復号化できないトラフィックはアクセス コントロールの対象です。ただし、アクセス コントロール ルールの条件では暗号化されていないトラフィックを必要とするため、暗号化されたトラフィックに一致するルール数が少なくなります。

特定の条件（ネットワークや IP アドレスなど）を使用するルールは、一般的な条件（アプリケーションなど）を使用するルールの前に順位付けする必要があります。オープン システム相互接続（OSI）モデルに精通している場合は、考え方として同様の順位付けを使用してください。レイヤ 1、2、および 3（物理、データリンク、およびネットワーク）の条件を持つルールは、ルールの最初に順位付けする必要があります。レイヤ 5、6、および 7（セッション、プレゼンテーション、およびアプリケーション）の条件は、ルールの後ろのほうに順序付けする必要があります。OSI モデルの詳細については、こちらの Wikipedia の記事を参照してください。

ヒント 適切な TLS/SSL ルールの順序を指定することで、ネットワーク トラフィックの処理に必要なリソースが削減され、ルールのプリエンプションを回避できます。ユーザが作成するルールはすべての組織と展開に固有のものですが、ユーザのニーズに対処しながらもパフォーマンスを最適化できるルールを順序付けする際に従うべきいくつかの一般的なガイドラインがあります。

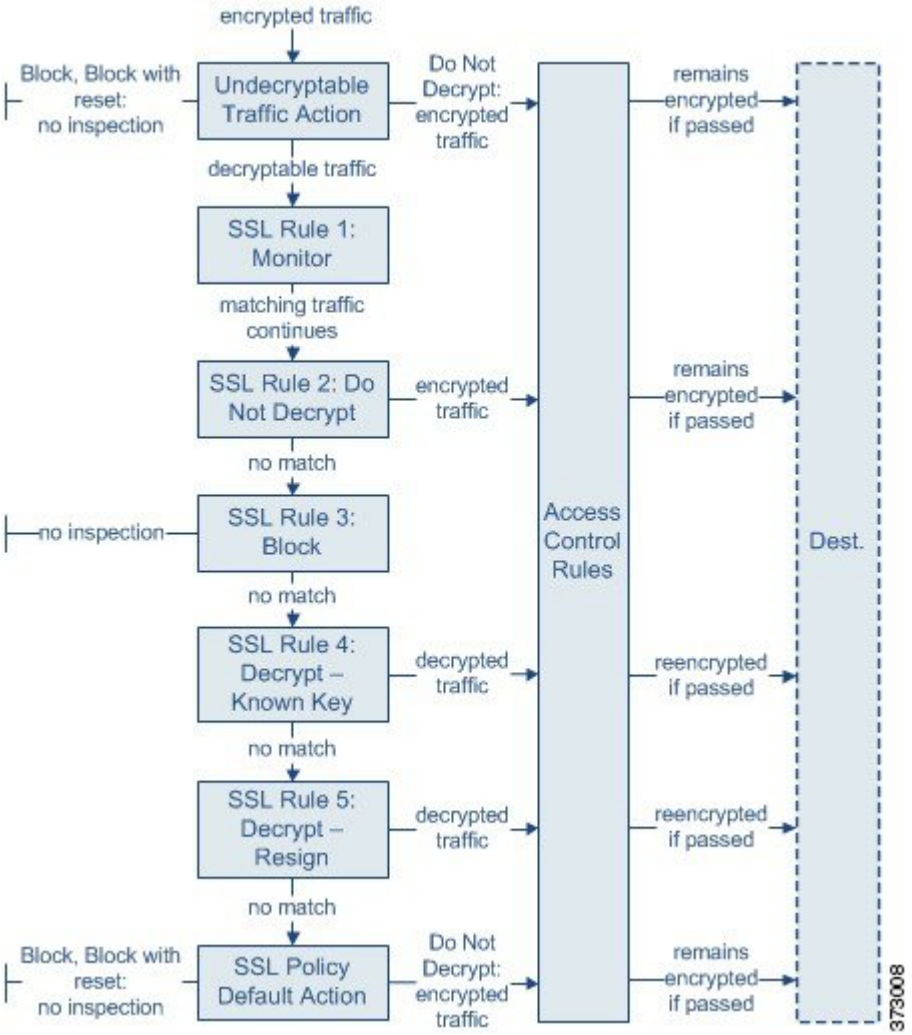
ルールは数値で順序付けするだけでなく、カテゴリ別にグループ化することもできます。デフォルトで、システムには3つのカテゴリ（管理者、標準、ルート）があります。カスタム カテゴリを追加できますが、システム提供のカテゴリを削除したり、それらの順序を変更したりすることはできません。

関連トピック

復号できないトラフィックのデフォルト処理オプション （1839 ページ）
SSL ルールの順序 （507 ページ）
ルールのパフォーマンスに関するガイドライン （502 ページ）

複数ルールの例

次のシナリオは、インライン展開での SSL ルールによるトラフィックの処理を要約しています。



このシナリオでは、トラフィックは次のように評価されます。

- **復号できないトラフィック アクション（Undecryptable Traffic Action）**は、暗号化されたトラフィックを最初に評価します。復号化できないトラフィックについてシステムは、それ以上のインスペクションなしでブロックするか、あるいはアクセス コントロールによる検査用に渡します。一致しなかった暗号化トラフィックは、次のルールへと進められます。
- **TLS/SSLルール 1：モニタ（Rule 1: Monitor）**は、暗号化トラフィックを次に評価します。モニタ ルールは、暗号化トラフィックのログ記録と追跡を行いますが、トラフィック フローには影響しません。システムは引き続きトラフィックを追加のルールと照合し、許可するか拒否するかを決定します。
- **TLS/SSLルール 2：復号しない（Rule 2: Do Not Decrypt）**は、暗号化トラフィックを 3 番目に評価します。一致したトラフィックは復号されません。システムはこのトラフィックをアクセス コントロールにより検査しますが、ファイルや侵入インスペクションは行いません。一致しなかったトラフィックは、次のルールへと進められます。

- **TLS/SSLルール 3**：**ブロック**（**Rule 3: Block**）は、暗号化トラフィックを 4 番目に評価します。一致したトラフィックは、それ以上のインスペクションは行わずに、ブロックされます。一致しなかったトラフィックは、次のルールへと進められます。
- **TLS/SSLルール 4**：**復号 - 既知のキー**（**Rule 4: Decrypt - Known Key**）は、暗号化トラフィックを 5 番目に評価します。ネットワークへの着信トラフィックで一致したものは、ユーザのアップロードする秘密キーを使用して復号化されます。復号化トラフィックはその後、アクセス コントロール ルールで評価されます。アクセス コントロール ルールは、復号されたトラフィックと暗号化されていないトラフィックで同じ処理をします。この追加検査の結果、システムがトラフィックをブロックする場合があります。他のすべてのトラフィックは、宛先への送信が許可される前に再暗号化されます。SSL ルールに一致しなかったトラフィックは、次のルールへと進められます。
- **TLS/SSLルール 5**：**復号 - 再署名**（**Rule 5: Decrypt - Resign**）は、最後のルールです。トラフィックがこのルールに一致した場合、システムはアップロードされた CA 証明書を使用してサーバ証明書を再署名してから、中間者（man-in-the-middle）としてトラフィックを復号します。復号化トラフィックはその後、アクセス コントロール ルールで評価されます。アクセス コントロール ルールは、復号されたトラフィックと暗号化されていないトラフィックで同じ処理をします。この追加検査の結果、システムがトラフィックをブロックする場合があります。他のすべてのトラフィックは、宛先への送信が許可される前に再暗号化されます。SSL ルールに一致しなかったトラフィックは、次のルールへと進められます。
- **SSL ポリシーのデフォルト アクション**（**SSL Policy Default Action**）は、どの TLS/SSL ルールにも一致しなかったすべてのトラフィックを処理します。デフォルトアクションでは、暗号化トラフィックをそれ以上のインスペクションなしでブロックするか、あるいは復号しないで、アクセス コントロールによる検査を行います。

TLS/SSL ポリシーとルールの設定方法

このトピックでは、ネットワーク上の TLS/SSL トラフィックをブロック、モニタ、または許可する SSL ポリシーとこれらのポリシーの TLS/SSL ルールを設定するために必要なタスクの概要を説明します。

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	任意（NGIPSv を除く）	任意（Any）	Administrator/Access Admin/Network Admin

手順

	コマンドまたはアクション	目的
ステップ 1	SSL ポリシーを作成します。	SSL ポリシーは、1 つ以上のルールのコンテナです。アクセス制御のために SSL ポリシーとそのルールを使用するには、後で SSL ポリシーをアクセス コントロール ポリシーに関連付ける必要があります。基本的な SSL ポリシーの作成 （1842 ページ）を参照してください。
ステップ 2	SSL ポリシーのデフォルト アクションを設定します。	デフォルト アクションは、トラフィックが SSL ポリシーによって定義されたルールに一致しない場合に実行されます。SSL ポリシーのデフォルト アクション （1838 ページ）を参照してください。
ステップ 3	復号化できないトラフィックの処理方法を指定します。	トラフィックは、セキュアでないプロトコル、不明な暗号スイートの使用、またはハンドシェイクや復号化でエラーが発生した場合など、さまざまな理由で復号できなくなる可能性があります。復号できないトラフィックのデフォルト処理オプション （1839 ページ）を参照してください。
ステップ 4	[復号-既知のキー（Decrypt - Known Key）]（ネットワーク内のサーバに着信トラフィックを復号するための）TLS/SSL ルールの場合、内部証明書オブジェクトを作成します。	内部証明書オブジェクトは、サーバの証明書と秘密キーを使用します。内部証明書オブジェクト （590 ページ）を参照してください。
ステップ 5	[復号-再署名（Decrypt - Resign）]（ネットワーク外部のサーバに発信トラフィックを復号するための）TLS/SSL ルールの場合、内部認証局（CA）オブジェクトを作成します。	内部 CA オブジェクトは、CA と秘密キーを使用します。内部認証局オブジェクト （580 ページ）を参照してください。
ステップ 6	TLS/SSL ルールを作成します。	• [ブロック（Block）]、[リセットしてブロック（Block with reset）]、[インタラクティブ ブロック（Interactive block）]：TLS/SSL ルール アクション設定 （1866 ページ）。 • [復号しない（Do Not Decrypt）]：TLS/SSL ルール アクション設定 （1866 ページ）を参照してください。 • [復号-再署名（Decrypt - Resign）]：復号 - 再署名アクションの設定 （1867 ページ）を参照してください。 • [復号-既知のキー（Decrypt - Known Key）]：復号-既知のキー アクションの設定 （1868 ページ）を参照してください。

	コマンドまたはアクション	目的
		• [モニタ（Monitor）]：TLS/SSL ルール アクション設定 （1866 ページ）を参照してください。
ステップ 7	SSL ポリシーをアクセス コントロール ポリシーに関連付けます。	SSL ポリシーをアクセス コントロール ポリシーに関連付けていない限り、SSL ポリシーの影響はありません。関連付けた後、アクセス コントロール ルールに一致するトラフィックを許可またはブロックし、その他のアクションを実行することができます。アクセス制御への他のポリシーの関連付け （1684 ページ）を参照してください。
ステップ 8	復号化されたトラフィックを許可またはブロックするようにアクセス コントロール ルールを設定します。	アクセス コントロール ポリシーのコンポーネント（1666 ページ）を参照してください。
ステップ 9	管理対象デバイスにアクセス コントロール ポリシーを展開します。	ポリシーを有効にするには、事前に管理対象デバイスに展開しておく必要があります。設定変更の展開（447 ページ）を参照してください。

TLS/SSL インスペクション アプライアンス展開シナリオ

ここでは Life Insurance Example, Inc.（LifeIns）という架空の生命保険会社で使われる複数のシナリオを例にして、同社のプロセス監査で利用されている暗号化トラフィックの SSL インスペクションについて解説します。LifeIns はそのビジネス プロセスに基づいて、以下の展開を計画しています。

- 契約審査部門では、単一の FTD デバイスをインライン展開する
- 上記の両方のデバイスを単一のFirepower Management Centerで管理する

カスタマー サービスのビジネス プロセス

LifeIns はすでに顧客対応用の Web サイトを構築済みです。LifeIns は、保険契約に関する加入見込み客からの暗号化された質問や要求を、この Web サイトおよび電子メールで受け取ります。LifeIns のカスタマー サービスは、これらの要求を処理して 24 時間以内に必要な情報を返信しなければなりません。カスタマー サービスでは、着信するコンタクト メトリックのコレクションを拡張したいと思っています。LifeIns では、すでにカスタマー サービスに対する内部監査用のレビューが確立されています。

また、LifeIns は暗号化された申請書もオンラインで受信します。カスタマー サービス部門は申請書を 24 時間以内に処理し、申請書類のファイルを契約審査部門に送信しなければなりません。カスタマー サービスでは、オンライン フォームからの不正な申請をすべて除外するようにしていますが、この作業が同部門での作業のかなりの部分を占めています。

契約審査部門のビジネス プロセス

LifeIns の契約審査担当者は、Medical Repository Example, LLC（MedRepo）という医療データリポジトリに、オンラインで暗号化された医療情報要求を送信します。MedRepo はこれらの要求を評価し、LifeIns に暗号化されたレコードを 72 時間以内に送信します。その後は契約審査担当者が申請書類を査定し、保険契約および保険料に関連する判定を送信します。契約審査部門では、そのメトリック コレクションを拡張したいと思っています。

最近、不明な送信元からのスプーフィング（なりすまし）応答が LifeIns に送られてくるようになりました。LifeIns の契約審査担当者はインターネット使用に関する適切なトレーニングを受けていますが、LifeIns の IT 部門はまず、医療応答の形式で送られてくる暗号化トラフィックをすべて分析し、すべてのスプーフィング行為をブロックしたいと思っています。

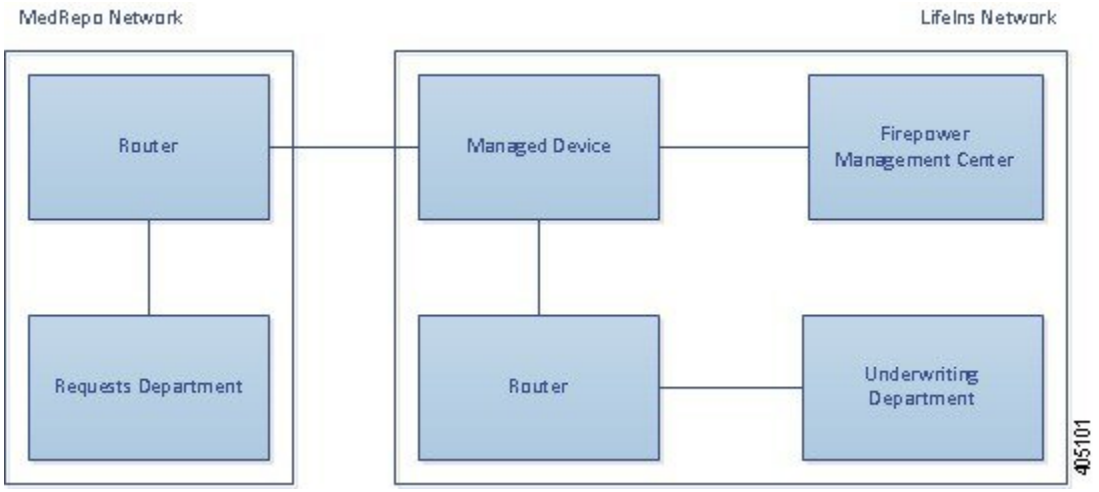
LifeIns では、経験の浅い契約審査担当者に対して 6 ヵ月のトレーニング期間を設けています。最近、こうした契約審査担当者が MedRepo のカスタマー サービス部門への暗号化された医療規制リクエストの送信を正しく行わない事例がありました。そのため MedRepo から LifeIns に複数の苦情が提出されています。LifeIns は、新任の契約審査担当者用のトレーニング期間を延長し、契約審査担当者から MedRepo への要求についても監査を入れることを計画しています。

インライン展開でのトラフィックの復号

LifeIns のビジネス要件では、契約審査部門に次の要求をしています。

- 新採用および経験の浅い契約審査担当者を監査し、MedRepo への情報要求が適切なすべての規則に準じていることを検証する。
- その契約審査によるメトリック コレクション プロセスを改善する。
- MedRepo が送信元と思われるすべての要求を調査し、スプーフィング行為を排除する。
- 契約審査部門から MedRepo のカスタマー サービス部門へのすべての不適切な規制要求を排除する。
- 経験豊富な契約審査担当者は監査しない。

LifeIns の契約審査部門では、デバイスのインライン展開を計画しています。



MedRepo のネットワークからのトラフィックは、MedRepo のルータに流されます。そこから LifeInsのネットワークにトラフィックがルーティングされます。管理対象デバイスはトラフィックを受信し、許可されたトラフィックを LifeIns のルータに転送して、管理しているFirepower Management Centerにイベントを送信します。LifeIns のルータは、トラフィックを宛先ホストにルーティングします。

管理元の Firepower Management Center で、[アクセス コントロール（Access Control）] および [SSL エディタ（SSL Editor）] のカスタム ロールを持つユーザが、SSL アクセス コントロール ルールの設定を次のように行います。

- 契約審査部門に送信された暗号化トラフィックをすべてログに記録する。
- LifeIns の契約審査部門から MedRepo のカスタマー サービス部門に不正に送信された暗号化トラフィックをすべてブロックする。
- MedRepo から LifeIns の契約審査部門宛て、および LifeIns の経験の浅い契約審査担当者から MedRepo のリクエスト部門宛てに送信される暗号化トラフィックをすべて復号化する。
- 経験豊富な契約審査担当者から送信される暗号化トラフィックは復号化しない。

さらに、カスタムの侵入ポリシーと以下の設定を使用して、復号化トラフィックを検査するアクセス コントロールを設定します。

- 復号化トラフィックでスプーフィング行為が検出された場合はそのトラフィックをブロックし、スプーフィング行為をログに記録する。
- 規制に準拠しない情報を含んでいる復号化トラフィックをブロックし、不適切な情報をログに記録する。
- 他の暗号化および復号化されたトラフィックをすべて許可する。

許可された復号化トラフィックは、再暗号化されて宛先ホストに転送されます。

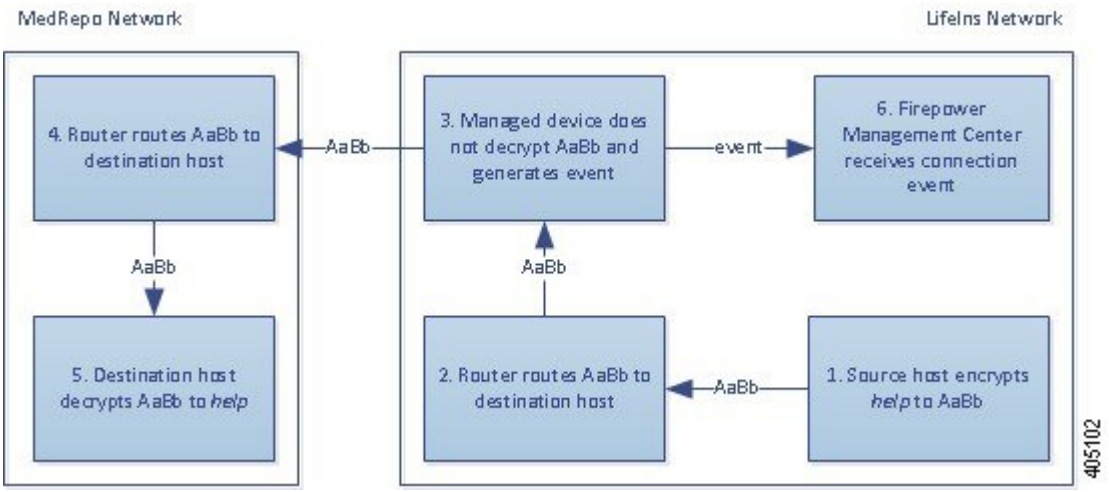
また、TLS/SSL アクセス コントロール ルールを使用して、[復号 - 再署名（Decrypt - Resign）] アクションでシステムにトラフィックを復号化して再署名させることもできます。トラフィックが TLS/SSL ルールに一致する場合、システムは ClientHello メッセージを変更した後、メッ

セージがアクセス コントロール評価（ディープ インスペクションを含めることができる）に合格するかどうかを判断します。メッセージが合格すれば、システムはそれを宛先サーバに送信します。詳細については、ClientHello メッセージ処理（1806 ページ）を参照してください。

次のシナリオでは、ユーザが情報をオンラインでリモート サーバに送信します。ユーザのブラウザは、サーバとの TCP 接続を確立してから、SSL ハンドシェイクを開始します。管理対象デバイスはこのトラフィックを受信し、ハンドシェイクと接続の詳細に応じて、システムが接続ログの記録およびトラフィックの処理をします。システムがトラフィックをブロックした場合、TCP 接続も切断されます。トラフィックがブロックされない場合、クライアントとサーバが SSL ハンドシェイクを完了することで、暗号化されたセッションが確立されます。

インライン展開での暗号化トラフィック モニタリング

契約審査部門で送受信されるすべての SSL 暗号化トラフィックについて、接続のログが記録されます。



次のステップが実行されます。

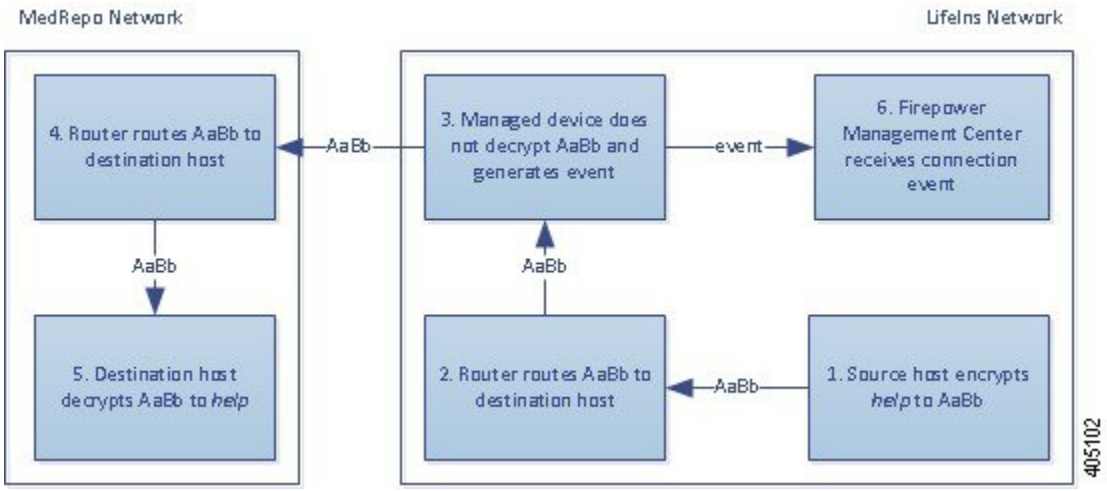
1. ユーザがプレーン テキストの要求（`help`）を送信します。クライアントがこれを暗号化（`AaBb`）し、MedRepo のリクエスト部門のサーバに暗号化トラフィックを送信します。
2. LifeIns のルータが暗号化トラフィックを受信し、リクエスト部門のサーバにルーティングします。
3. 管理対象デバイスはトラフィックを復号化しません。

   アクセス コントロール ポリシーが暗号化トラフィックの処理を続行してこれを許可し、セッション終了後に接続イベントを生成します。
4. 外部ルータがトラフィックを受信し、これをリクエスト部門のサーバにルーティングします。
5. 契約審査部門のサーバは、暗号化された情報の要求（`AaBb`）を受信し、これをプレーンテキスト（`help`）に復号化します。

6. Firepower Management Centerが接続イベントを受信します。

インライン展開で復号される暗号化トラフィック

経験豊富な契約審査担当者から送信されるすべてのTLS/SSL暗号化トラフィックについては、管理対象デバイスはそのトラフィックを復号せずに許可し、接続のログを記録します。



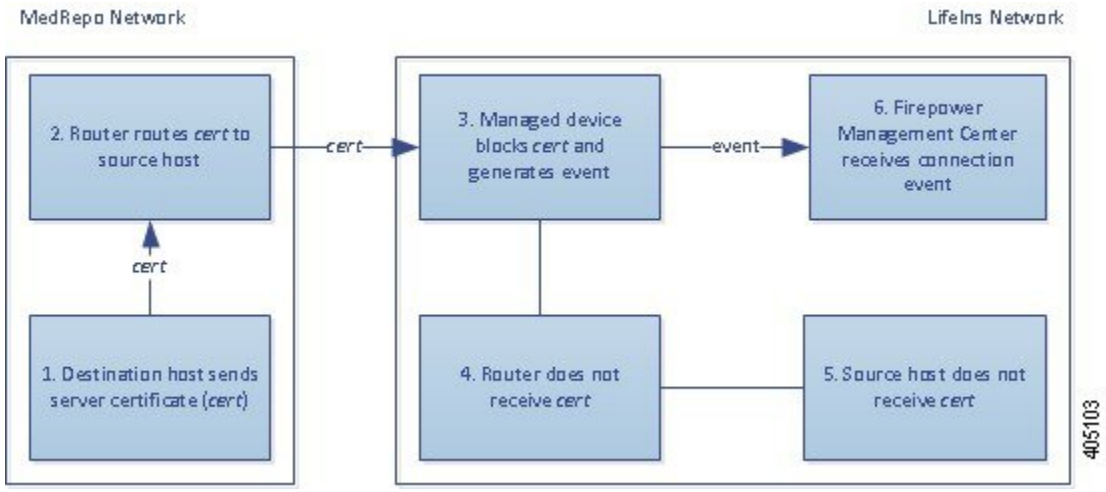
次のステップが実行されます。

1. ユーザがプレーン テキストの要求（`help`）を送信します。クライアントがこれを暗号化（`AaBb`）し、MedRepo のリクエスト部門のサーバに暗号化トラフィックを送信します。
2. LifeIns のルータが暗号化トラフィックを受信し、リクエスト部門のサーバにルーティングします。
3. 管理対象デバイスはこのトラフィックを復号化しません。

   アクセス コントロール ポリシーが暗号化トラフィックの処理を続行してこれを許可し、セッション終了後に接続イベントを生成します。
4. 外部ルータがトラフィックを受信し、これをリクエスト部門のサーバにルーティングします。
5. リクエスト部門のサーバは、暗号化された情報の要求（`AaBb`）を受信し、これをプレーンテキスト（`help`）に復号化します。
6. Firepower Management Centerが接続イベントを受信します。

インライン展開での暗号化トラフィックのブロック

LifeIns の契約審査部門から MedRepo のカスタマー サービス部門に不正に送信されるすべてのSMTPS 電子メール トラフィックは SSL ハンドシェイク時にブロックされ、追加の検査なしで接続のログが記録されます。

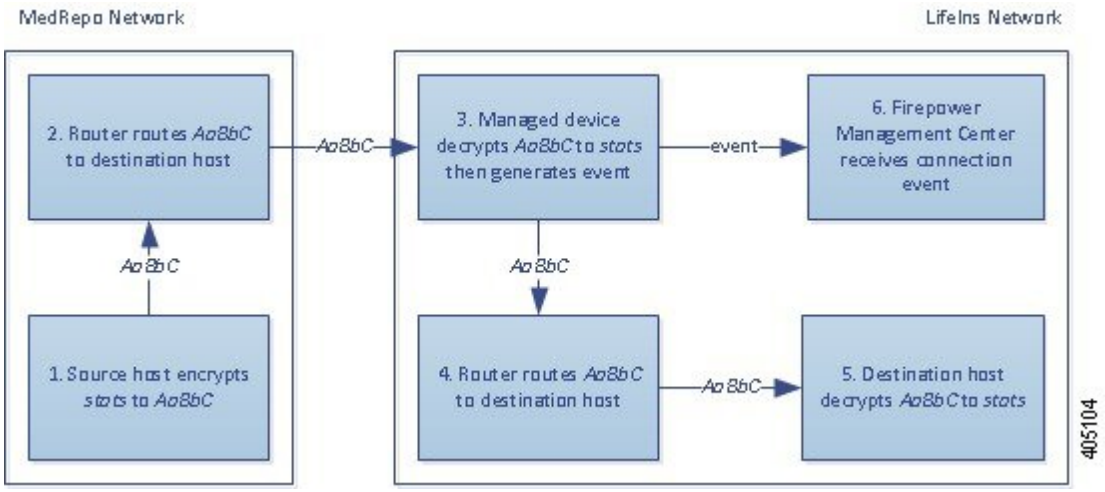


次のステップが実行されます。

1. カスタマー サービス部門のサーバは、クライアント ブラウザから TLS/SSL ハンドシェイクの確立要求を受信すると、TLS/SSL ハンドシェイクの次のステップとして、サーバ証明書（cert）を LifeIns の契約審査担当者に送信します。
2. MedRepo のルータが証明書を受信し、これを LifeIns の契約審査担当者にルーティングします。
3. 管理対象デバイスは追加の検査を行わずにトラフィックをブロックし、TCP 接続を終了します。これにより、接続イベントが生成されます。
4. 内部ルータは、ブロックされたトラフィックを受信しません。
5. 契約審査担当者は、ブロックされたトラフィックを受信しません。
6. Firepower Management Centerが接続イベントを受信します。

インライン展開での暗号化トラフィックの秘密キーによる検査

MedRepo から LifeIns の契約審査部門に送信されるすべての TLS/SSL 暗号化トラフィックは復号され、接続のログが記録されます。復号には、アップロードされたサーバ秘密キーを使って取得されたセッション キーが使用されます。正規のトラフィックは許可され、再暗号化されて契約審査部門に送信されます。

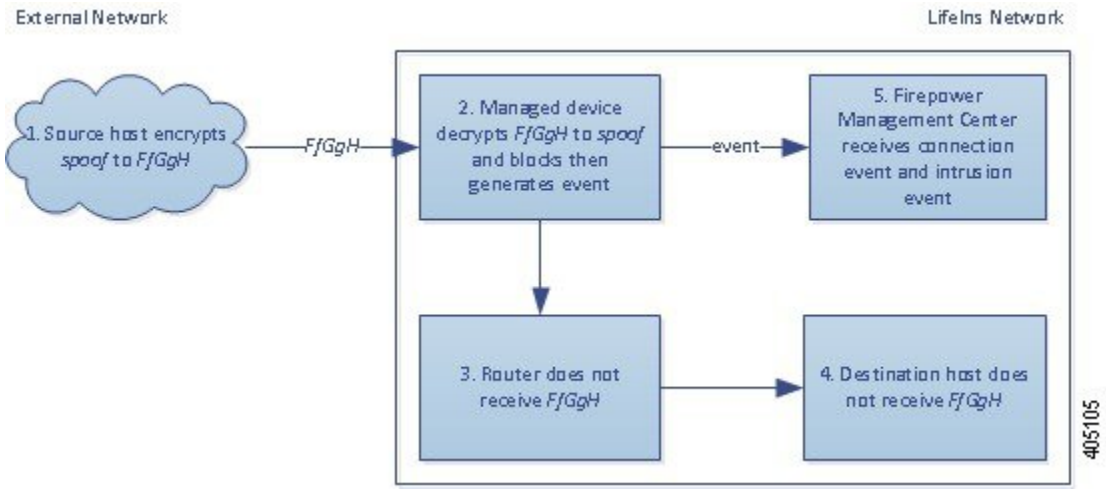


次のステップが実行されます。

1. ユーザがプレーン テキストの要求（stats）を送信します。クライアントがこれを暗号化（AaBbC）し、契約審査部門のサーバに暗号化トラフィックを送信します。
2. 外部ルータがトラフィックを受信し、これを契約審査部門のサーバにルーティングします。
3. 管理対象デバイスは、アップロードされた既知の秘密キーで取得したセッション キーを使用して、このトラフィックをプレーン テキスト（stats）に復号化します。

   アクセス コントロール ポリシーは、カスタムの侵入ポリシーを使用して復号化トラフィックの処理を継続します。スプーフィング行為は検出されません。デバイスは暗号化トラフィック（AaBbC）を転送し、セッション終了後に接続イベントを生成します。
4. 内部ルータがトラフィックを受信し、これを契約審査部門のサーバにルーティングします。
5. 契約審査部門のサーバは、暗号化された情報（AaBbC）を受信し、これをプレーン テキスト（stats）に復号化します。
6. Firepower Management Centerは、暗号化および復号化されたトラフィックの情報とともに、接続イベントを受信します。

これに対し、スプーフィング行為の復号化トラフィックはすべてドロップされ、接続およびスプーフィング行為についてのログが記録されます。



次のステップが実行されます。

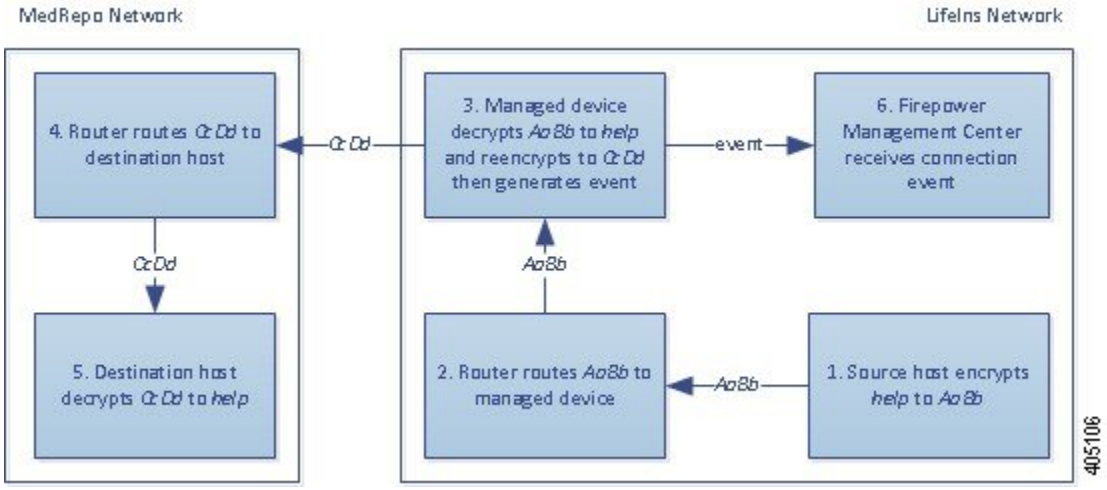
1. ユーザがプレーン テキストの要求（`spoof`）を送信しますが、このトラフィックは改変されており、発信元が MedRepo, LLC であるかのように偽装されています。クライアントがこれを暗号化（`FfGgH`）し、契約審査部門のサーバに暗号化トラフィックを送信します。
2. 管理対象デバイスは、アップロードされた既知の秘密キーで取得したセッション キーを使用して、このトラフィックをプレーン テキスト（`spoof`）に復号化します。

   アクセス コントロール ポリシーは、カスタムの侵入ポリシーを使用して復号化トラフィックの処理を継続し、スプーフィング行為を検出します。デバイスはトラフィックをブロックし、侵入イベントを生成します。セッション終了後、接続イベントを生成します。
3. 内部ルータは、ブロックされたトラフィックを受信しません。
4. 契約審査部門のサーバは、ブロックされたトラフィックを受信しません。
5. Firepower Management Centerは、暗号化および復号されたトラフィックの情報とともに、接続イベントおよびスプーフィング行為の侵入イベントを受信します。

インライン展開での再署名証明書を使用した暗号化トラフィック インスペクション

新任および経験の浅い契約審査担当者から MedRepo のリクエスト部門に送信されるすべての TLS/SSL 暗号化トラフィックは復号され、接続のログが記録されます。復号には、再署名されたサーバ証明書を使って取得されたセッション キーが使用されます。正規のトラフィックは許可され、再暗号化されて MedRepo に送信されます。

（注） インライン展開においてサーバ証明書の再署名によりトラフィックを復号化する場合、デバイスは中間者（man-in-the-middle）として機能します。ここでは、1 つはクライアントと管理対象デバイスの間、もう 1 つは管理対象デバイスとサーバの間をつなぐ、2 つの TLS/SSL セッションが作成されます。その結果、暗号セッションの詳細はセッションごとに異なります。



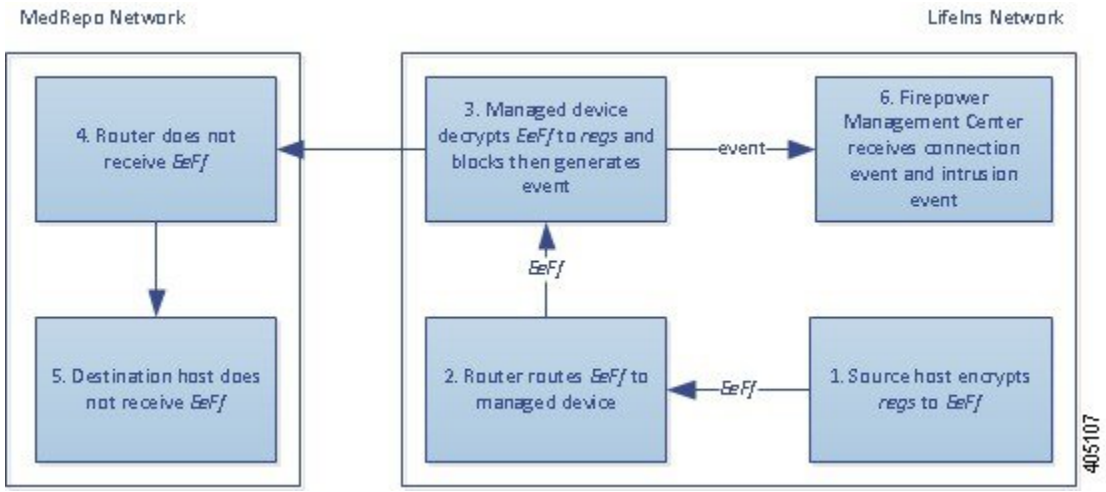
次のステップが実行されます。

1. ユーザがプレーン テキストの要求（help）を送信します。クライアントがこれを暗号化（AaBb）し、リクエスト部門のサーバに暗号化トラフィックを送信します。
2. 内部ルータがトラフィックを受信し、これをリクエスト部門のサーバにルーティングします。
3. 管理対象デバイスは、再署名されたサーバ証明書と秘密キーで取得したセッション キーを使用して、このトラフィックをプレーン テキスト（help）に復号します。

   アクセス コントロール ポリシーは、カスタムの侵入ポリシーを使用して復号トラフィックの処理を継続します。不適切な要求は検出されません。デバイスはトラフィックを再暗号化（CcDd）して、送信を許可します。セッション終了後、接続イベントを生成します。
4. 外部ルータがトラフィックを受信し、これをリクエスト部門のサーバにルーティングします。
5. リクエスト部門のサーバは、暗号化された情報（CcDd）を受信し、これをプレーンテキスト（help）に復号化します。
6. Firepower Management Centerは、暗号化および復号されたトラフィックの情報とともに、接続イベントを受信します。

（注） 再署名されたサーバ証明書で暗号化されたトラフィックにより、信頼できない証明書についての警告がクライアントのブラウザに表示されます。この問題を避けるには、組織のドメインルートにある信頼できる証明書ストアまたはクライアントの信頼できる証明書ストアにCA証明書を追加します。

これに対し、規制要件を満たさない情報を含んでいる復号化トラフィックは、すべてドロップされます。接続および非準拠情報についてのログが記録されます。



次のステップが実行されます。

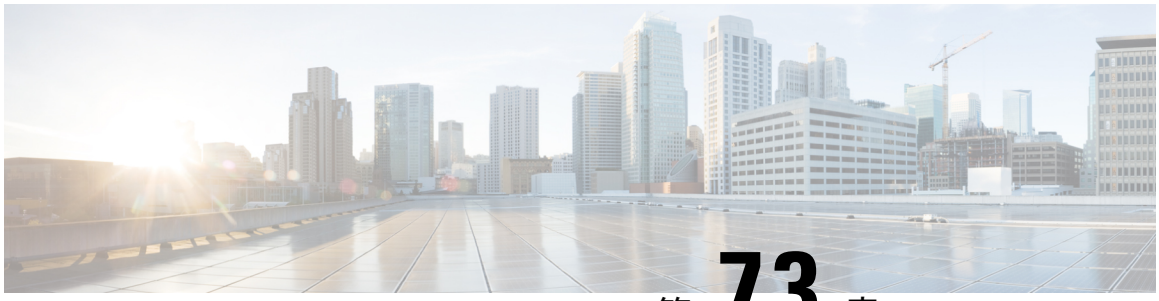
1. ユーザが規制要件に準拠していない要求をプレーンテキスト（regs）で送信します。クライアントがこれを暗号化（EeFf）し、リクエスト部門のサーバに暗号化トラフィックを送信します。
2. 内部ルータがトラフィックを受信し、これをリクエスト部門のサーバにルーティングします。
3. 管理対象デバイスは、再署名されたサーバ証明書と秘密キーで取得したセッションキーを使用して、このトラフィックをプレーン テキスト（regs）に復号します。

   アクセス コントロール ポリシーは、カスタムの侵入ポリシーを使用して復号トラフィックの処理を継続し、不適切な要求を検出します。デバイスはトラフィックをブロックし、侵入イベントを生成します。セッション終了後、接続イベントを生成します。
4. 外部ルータは、ブロックされたトラフィックを受信しません。
5. リクエスト部門のサーバは、ブロックされたトラフィックを受信しません。
6. Firepower Management Centerは、暗号化および復号化されたトラフィックの情報とともに、接続イベントおよび不適切な要求の侵入イベントを受信します。

TLS/SSL の履歴

機能	バージョン	詳細
TLS 暗号化アクセラレーション 無効化できません	6.4	TLS 暗号化アクセラレーション すべてのサポート対象デバイスで有効にします。 ネイティブ インターフェイスを持つ管理対象デバイスでは、TLS 暗号化アクセラレーションを無効にできません。 FTD コンテナ インスタンス の TLS 暗号化アクセラレーションは、この表の次の行で示すように限定されています。 削除されたコマンド： **system support ssl-hw-accel enable** **system support ssl-hw-accel disable** **system support ssl-hw-status**
Firepower 4100/9300 モジュール/セキュリティ エンジンのいずれかの FTD コンテナ インスタンスでの TLS 暗号化アクセラレーションのサポート	6.4	モジュール/セキュリティ エンジンのいずれかの FTD コンテナ インスタンスで TLS 暗号化アクセラレーションを有効にできるようになりました。他のコンテナ インスタンスの TLS 暗号化アクセラレーションは無効ですが、ネイティブ インスタンスでは有効になっています。 新しい/変更されたコマンド： **config hwCrypto enable** **system support ssl-hw-status** を **show crypto accelerator status** に変更
TLS/SSL ハードウェア アクセラレーション 次のように参照されています *TLS* 暗号化アクセラレーション	6.4	名前の変更は、TLS/SSL 暗号化と復号化アクセラレーションがより多くのデバイスでサポートされていることを反映しています。デバイスによっては、アクセラレーションがソフトウェアまたはハードウェアで実行される場合があります。 影響を受ける画面：TLS 暗号化アクセラレーションのステータスを表示するには、**[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > **[デバイス（Device）]**、[全般（General）] タブ ページ。
Extended Master Secret 拡張機能がサポートされています（RFC 7627 を参照）	6.3.0.1	TLS Extended Master Secret 拡張機能は、SSL ポリシー（具体的には、[復号 - 再署名（Decrypt - Resign）] または [復号 - 既知のキー（Known Key）] のルール アクションを持つポリシー）でサポートされています。
Extended Master Secret 拡張機能はサポートされていません。	6.3	拡張機能は [復号 - 再署名（Decrypt - Resign）] ルールの ClientHello 変更時に削除されます。

機能	バージョン	詳細
TLS/SSL ハードウェア アクセラレーションデフォルトでは有効になっています	6.3	TLS/SSL ハードウェア アクセラレーション デフォルトですべてのサポート対象デバイスで有効になっていますが、必要に応じて無効にすることができます。
Extended Master Secret 拡張機能がサポートされています（RFC 7627 を参照）	6.2.3.9	TLS Extended Master Secret 拡張機能は、SSL ポリシー（具体的には、[復号 - 再署名（Decrypt - Resign）] または [復号 - 既知のキー（Known Key）] のルール アクションを持つポリシー）でサポートされています。
アグレッシブ TLS 1.3 ダウングレード	6.2.3.7	**system support ssl-client-hello-enabled aggressive-tls13-downgrade {true|false}** CLI コマンドを使用して、TLS 1.2 への TLS 1.3 トラフィックのダウングレードの動作を決定できます。詳細については、『*Command Reference for Firepower Threat Defense*』を参照してください。
TLS/SSL ハードウェア アクセラレーション introduced	6.2.3	特定の管理対象デバイス モデルでは、パフォーマンスが向上する、ハードウェアでの TLS/SSL 暗号化および復号が実行されます。デフォルトでは、この機能は有効です。 影響を受ける画面：TLS/SSL ハードウェア アクセラレーションのステータスを表示するには、**[デバイス（Devices）] > [デバイス管理（Device Management）] > [デバイス（Device）]**、[全般（General）] タブ ページ。
カテゴリとレピュテーションの条件をサポート	6.2.2	カテゴリ/レピュテーションの条件を使用したアクセス コントロール ルールまたは SSL ルール。
SafeSearch をサポート	6.1.0	• SSL ポリシーにより復号され、その後アクセス コントロール ルールまたはアクセス コントロール ポリシーのデフォルト アクションによりブロック（またはインタラクティブにブロック）された接続については、HTTP 応答ページが表示されます。このような場合、システムは応答ページを暗号化して、再暗号化された SSL ストリームの最後にそれを送信します。 • SafeSearch により好ましくないコンテンツがフィルタリングされ、成人向けサイトの検索が停止されます。



第 73 章

SSL ポリシーの作成の開始

ここでは、SSL ポリシーの作成、設定、管理、およびロギングの概要を示します。

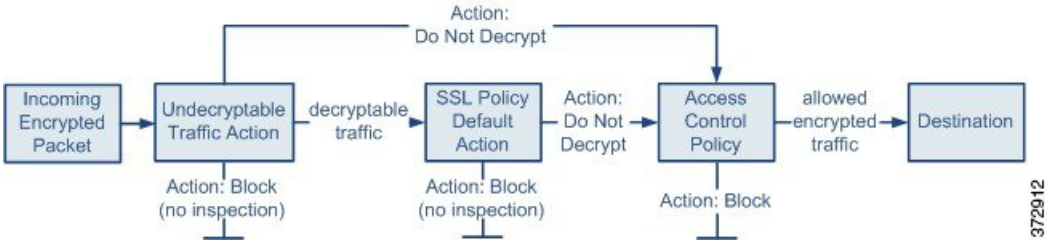
SSL ポリシーの概要

SSL ポリシーは、ネットワーク上の暗号化トラフィックをシステムがどのように処理するかを決定します。1 つ以上の SSL ポリシーを設定し、SSL ポリシーをアクセス コントロール ポリシーに関連付けてから、そのアクセス コントロール ポリシーを管理対象デバイスに展開することができます。デバイスで TCP ハンドシェイクが検出されると、アクセス コントロール ポリシーは最初にトラフィックを処理して検査します。次に TCP 接続上で TLS/SSL 暗号化セッションが識別された場合は、SSL ポリシーが引き継いで、暗号化トラフィックの処理および復号を行います。

注意 SSL ポリシーを追加または削除すると 設定の変更を展開する際に Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、ターゲットデバイスがトラフィックを処理する方法に応じて異なります。詳細はSnort® の再起動によるトラフィックの動作 （451 ページ）を参照してください。

最も単純な SSL ポリシーは、次の図のように、単一のデフォルト アクションで暗号化トラフィックを処理するように展開先のデバイスに指示します。デフォルト アクションの設定では、それ以上のインスペクションなしで復号可能トラフィックをブロックするか、復号されていない復号可能トラフィックをアクセス コントロールで検査するように指定できます。システ

ムは、暗号化されたトラフィックを許可するか、またはブロックできます。デバイスは復号できないトラフィックを検出すると、トラフィックをそれ以上のインスペクションなしでブロックするか、あるいは復号しないままにして、アクセス コントロールによる検査を行います。



より複雑なSSLポリシーでは、各種の復号化できないトラフィックをさまざまなアクションで処理することが可能であり、認証局（CA）が証明書を発行したか、または暗号化証明書を信頼するかどうかに応じてトラフィックを制御したり、SSLルールを使ってきめ細かな暗号化トラフィックの制御およびログの記録を行ったりできます。これらのルールには、単純なものや複雑なものがあり、複数の基準を使用して暗号化トラフィックの照合および検査を行います。

（注） TLS と SSL は相互に使用されることが多いため、*TLS/SSL* という表現を使用していずれかのプロトコルについて説明していることを示しています。SSL プロトコルは、よりセキュアな TLS プロトコルを選択することにより IETF によって廃止されました。そのため、*TLS/SSL* は通常、TLS のみを指すものとして解釈できます。

例外は SSL ポリシーです。FMC 設定オプションは **[Policies]** > **[Access Control]** > **[SSL]** となるため、これらのポリシーは TLS および SSL のトフィックのルールを定義するために使用されますが、「SSL ポリシー」という用語を使用します。

SSL プロトコルと TLS プロトコルの詳細については、「SSL と TLS：その違いとは（SSL vs. TLS - What's the Difference?）」を参照してください。

関連トピック

TLS/SSL ルール条件 （1861 ページ）

SSL ポリシーのデフォルト アクション

SSLポリシーのデフォルトアクションは、ポリシーのモニタ以外のルールと一致しない復号可能な暗号化トラフィックについてシステムがどのように処理するかを決定します。TLS/SSLルールがまったく含まれないSSLポリシーを適用する場合、ネットワーク上のすべての復号可能トラフィックの処理方法を、デフォルト アクションが決定します。デフォルト アクションでブロックされた暗号化トラフィックに対しては、システムはいかなる種類のインスペクションも行わないことに注意してください。

表 *113* : *SSL* ポリシーのデフォルト アクション

デフォルト アクション	暗号化トラフィックに対して行う処理
Block	それ以上のインスペクションは行わずにTLS/SSLセッションをブロックします。
Block with reset	それ以上のインスペクションは行わずにTLS/SSLセッションをブロックし、TCP接続をリセットします。トラフィックにUDPのようなコネクションレス型プロトコルが使用される場合は、このオプションを選択します。この場合、コネクションレス型プロトコルにより、リセットされるまで接続の再確立が試みられます。 また、このアクションでは、ブラウザの接続リセット エラーも表示されるため、接続がブロックされたことがユーザに通知されます。
復号しない（Do not decrypt）	アクセス コントロールを使用して暗号化トラフィックを検査します。

関連トピック

基本的な SSL ポリシーの作成 （1842 ページ）

復号できないトラフィックのデフォルト処理オプション

表 *114* : 復号化できないトラフィック タイプ

タイプ	説明	デフォルト アクション	使用可能なアクション
圧縮されたセッション（Compressed Session）	TLS/SSL セッションはデータ圧縮メソッドを適用します。	デフォルト アクションを継承（Inherit default action）	Do not decrypt Block Block with reset デフォルト アクションを継承（Inherit default action）
SSLv2 Session	セッションは SSL バージョン 2 で暗号化されます。 トラフィックが復号可能となるのは、ClientHello メッセージが SSL 2.0 で、送信トラフィックの残りが SSL 3.0 であることに注意してください。	デフォルト アクションを継承（Inherit default action）	Do not decrypt Block Block with reset デフォルト アクションを継承（Inherit default action）

タイプ	説明	デフォルト アクション	使用可能なアクション
Unknown Cipher Suite	システムが認識できない暗号スイートです。	デフォルト アクションを継承（Inherit default action）	Do not decrypt Block Block with reset デフォルト アクションを継承（Inherit default action）
Unsupported Cipher Suite	検出された暗号スイートに基づく復号化を、システムはサポートしていません。	デフォルト アクションを継承（Inherit default action）	Do not decrypt Block Block with reset デフォルト アクションを継承（Inherit default action）
セッションが未キャッシュ（Session not cached）	TLS/SSL セッションでセッションの再利用が有効化されており、クライアントとサーバがセッション識別子を使ってセッションを再確立しているのに、システムでセッション識別子がキャッシュされていません。	デフォルト アクションを継承（Inherit default action）	Do not decrypt Block Block with reset デフォルト アクションを継承（Inherit default action）
ハンドシェイク エラー（Handshake Errors）	TLS/SSL ハンドシェイクのネゴシエーション中にエラーが発生しました。	デフォルト アクションを継承（Inherit default action）	Do not decrypt Block Block with reset デフォルト アクションを継承（Inherit default action）
Decryption Errors	トラフィックの復号化中にエラーが発生しました。	Block	Block Block with Reset

SSL ポリシーを最初に作成する場合、デフォルト アクションによって処理される接続のログは、デフォルトでは無効化されています。復号化できないトラフィックの処理ではデフォルト アクションのログ設定も適用されるため、復号化できないトラフィック用のアクションで処理される接続のログは、デフォルトでは無効化されています。

ブラウザが証明書ピニングを使用してサーバ証明書を確認する場合は、サーバ証明書に再署名しても、このトラフィックを復号できないことに注意してください。詳細については、TLS/SSL ルールのガイドラインと制限事項 （1848 ページ）を参照してください。

関連トピック

復号できないトラフィックのデフォルト処理を設定する （1843 ページ）

SSL ポリシーの管理

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	すべて（NGIPSv を除く）	いずれか（Any）	Admin/Access Admin/Network Admin

SSL ポリシー エディタでは、次の操作を実行できます。

- ポリシーを設定する。
- TLS/SSL ルールを追加、編集、削除、有効化、無効化、および編成する。
- 信頼できる CA 証明書を追加する。
- システムが復号できない暗号化トラフィックに対する処理を決定する。
- デフォルト アクションおよび復号できないトラフィック アクションで処理されるトラフィックのログを記録する。

マルチドメイン展開では、編集できる現在のドメインで作成されたポリシーが表示されます。また、編集できない先祖ドメインで作成されたポリシーも表示されます。下位のドメインで作成されたポリシーを表示および編集するには、そのドメインに切り替えます。

ステップ 1 **[Policies]** > **[Access Control]** > **[SSL]**を選択します。

ステップ 2 SSL ポリシーを管理します。

- 関連付け：アクセス コントロール ポリシーに SSL ポリシーを関連付ける場合は、アクセス制御への他のポリシーの関連付け （1684 ページ）を参照してください。
- [比較（Compare）]：[ポリシーの比較（Compare Policies）] をクリックします（ポリシーの比較 （457 ページ） を参照）。
- コピー：コピー アイコン（  ）をクリックします。
- 作成：[新規ポリシー（New Policy）] をクリックします。基本的な SSL ポリシーの作成 （1842 ページ）を参照してください。
- 削除：削除アイコン（  ）をクリックします。コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。
- 展開：[展開（Deploy）] をクリックします（設定変更の展開 （447 ページ） を参照）。
- 編集：編集アイコン（  ）をクリックします。SSL ポリシーの編集 （1844 ページ）を参照してください。代わりに表示アイコン（  ）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

- インポート/エクスポート：コンフィギュレーションのインポート/エクスポートについて （229 ページ）を参照してください。
- [レポート（Report）]：レポート アイコン（）をクリックします（現在のポリシー レポートの生成（459 ページ） を参照）。

基本的な SSL ポリシーの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	すべて（NGIPSv を除く）	いずれか（Any）	Admin/Access Admin/Network Admin

SSL ポリシーの設定では、ポリシーに一意の名前を付け、デフォルト アクションを指定する必要があります。

ステップ 1 **[Policies]** > **[Access Control]** > **[SSL]** を選択します。

ステップ 2 [新しいポリシー（New Policy）] をクリックします。

ステップ 3 [名前（Name）] に一意のポリシー名を入力し、オプションで [説明（Description）] にポリシーの説明を入力します。

ステップ 4 [デフォルト アクション（Default Action）] を指定します。SSL ポリシーのデフォルト アクション （1838 ページ）を参照してください。

ステップ 5 ポリシーのデフォルト アクションによる接続のロギング （3018 ページ）の説明に従って、デフォルト アクションのロギング オプションを設定します。

ステップ 6 [保存（Save）] をクリックします。

次の作業

- SSL ポリシーに追加するルールを設定します。TLS/SSL ルールの作成と変更 （1855 ページ）を参照してください。
- 復号化できないトラフィックのデフォルト処理を設定します。復号できないトラフィックのデフォルト処理を設定する （1843 ページ）を参照してください。
- 復号化できないトラフィックのデフォルト処理のロギング オプションを設定します。ポリシーのデフォルト アクションによる接続のロギング （3018 ページ）を参照してください。
- アクセス制御への他のポリシーの関連付け （1684 ページ）の説明に従って、SSL ポリシーをアクセス コントロール ポリシーに関連付けます。
- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

復号できないトラフィックのデフォルト処理を設定する

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	すべて（NGIPSvを除く）	いずれか（Any）	Admin/Access Admin/Network Admin

システムによる復号や検査ができない特定タイプの暗号化トラフィックの処理については、SSL ポリシー レベルで、復号できないトラフィックのアクションを設定できます。TLS/SSL ルールが含まれないSSLポリシーを展開する場合、ネットワーク上のすべての復号できない暗号化トラフィックの処理方法は、復号できないトラフィックのアクションによって決定されます。

復号できないトラフィックのタイプによって、次の選択ができます。

- 接続をブロック。
- 接続をブロックした後でリセットする。接続がブロックされるまで接続を試行し続ける UDP などのコネクションレス型プロトコルの場合、このオプションをお勧めします。
- アクセス コントロールを使用して暗号化トラフィックを検査します。
- SSL ポリシーのデフォルト アクションを継承する。

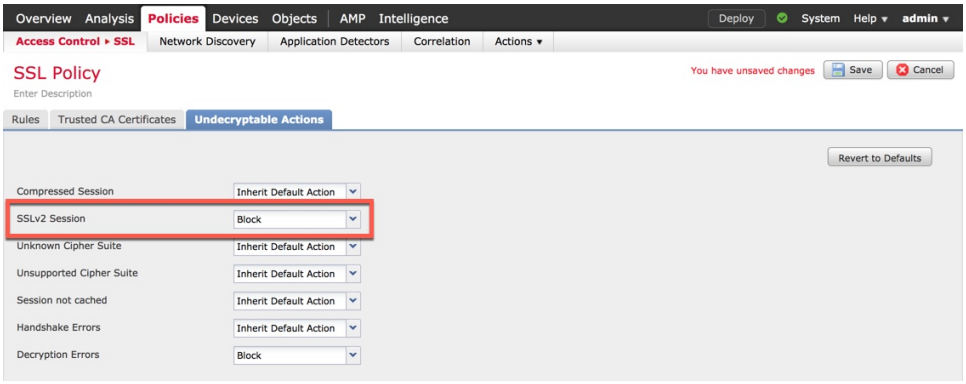
ステップ 1 SSL ポリシー エディタで、[復号できないアクション（Undecryptable Actions）] タブをクリックします。

ステップ 2 各フィールドで、SSL ポリシーのデフォルト アクションを選択するか、復号できないタイプのトラフィックに対して実行する別のアクションを選択します。詳細については、復号できないトラフィックのデフォルト処理オプション（1839 ページ）と SSL ポリシーのデフォルト アクション（1838 ページ）を参照してください。

ステップ 3 [保存（Save）] をクリックしてポリシーを保存します。

例

たとえば、すべての SSLv2 トラフィックをブロックするには、次のようにオプションを設定します。



次のタスク

- 復号できないトラフィックのアクションで処理される接続に関するデフォルトロギングを設定します。ポリシーのデフォルトアクションによる接続のロギング（3018ページ）を参照してください。
- 設定変更を展開します。設定変更の展開（447 ページ）を参照してください。

SSL ポリシーの編集

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	すべて（NGIPSvを除く）	いずれか（Any）	Admin/Access Admin/Network Admin

ポリシーの編集は、1 つのブラウザ ウィンドウを使用して、一度に 1 人のみで行う必要があります。複数のユーザが同じポリシーを保存した場合は、最後に保存された変更が保持されます。ユーザにとっての便宜性を考慮して、各ポリシーを現在編集している人（いる場合）の情報が表示されます。セッションのプライバシーを保護するために、ポリシーエディタが非アクティブになってから 30 分後に警告が表示されます。60 分後には、システムにより変更が破棄されます。

ステップ 1 **[Policies]** > **[Access Control]** > **[SSL]**を選択します。

ステップ 2 設定する SSL ポリシーの横にある編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 SSL ポリシーを設定します。

- 説明：SSL ポリシーの説明を更新するには、[説明（Description）] フィールドをクリックし、新しい説明を入力します。

- ログ：復号できないトラフィックの処理および SSL ルールに一致しないトラフィックについて接続を記録するには、ポリシーのデフォルトアクションによる接続のロギング（3018 ページ）を参照してください。
- 名前の変更：SSL ポリシーの名前を変更するには、[名前（Name）] フィールドをクリックし、新しい名前を入力します。
- デフォルトアクションの設定：SSL ポリシーが SSL ルールに一致しないトラフィックをどのように処理するかを設定するには、SSL ポリシーのデフォルトアクション（1838 ページ）を参照してください。
- 復号できないトラフィックのデフォルト アクションの設定：SSL ポリシーが復号できないトラフィックをどのように処理するかを設定するには、復号できないトラフィックのデフォルト処理を設定する（1843 ページ）を参照してください。
- 信頼：SSL ポリシーに信頼された CA 証明書を追加するには、外部認証局の信頼（1884 ページ）を参照してください。

ステップ 4 SSL ポリシー内のルールを編集します。

- 追加：ルールを追加するには、[ルールの追加（Add Rule）] をクリックします。
- コピー：ルールをコピーするには、選択したルールを右クリックして、[コピー（Copy）] を選択します。
- 切り取り：ルールを切り取るには、選択したルールを右クリックして、[切り取り（Cut）] を選択します。
- 削除：ルールを削除するには、ルールの横にある削除アイコン（  ）をクリックして、[OK] をクリックします。
- 無効化：有効なルールを無効にするには、選択したルールを右クリックして、[状態（State）] を選択し、[無効（Disable）] を選択します。
- 表示：特定のルール属性の設定ページを表示するには、ルールの行にある条件の列で名前、値、またはアイコンをクリックします。たとえば、[送信元ネットワーク（Source Networks）] カラムに示されている名前または値をクリックすると、選択したルールの [ネットワーク（Networks）] ページが表示されます。ネットワーク条件 （471 ページ）を参照してください。
- 編集：ルールを編集するには、ルールの横にある編集アイコン（  ）をクリックします。
- 有効化：無効なルールを有効にするには、選択したルールを右クリックして、[状態（State）] を選択し、[有効（Enable）] を選択します。無効なルールはグレー表示され、ルール名の下に [（無効）（(disabled)）] というマークが付きます。
- 貼り付け：切り取られたルールまたはコピーされたルールを貼り付けるには、選択したルールを右クリックして、[上に貼り付け（Paste above）] または [下に貼り付け（Paste below）] を選択します。

ステップ 5 設定を保存または廃棄します。

- 変更を保存し、編集を続行する場合は、[保存（Save）] をクリックします。

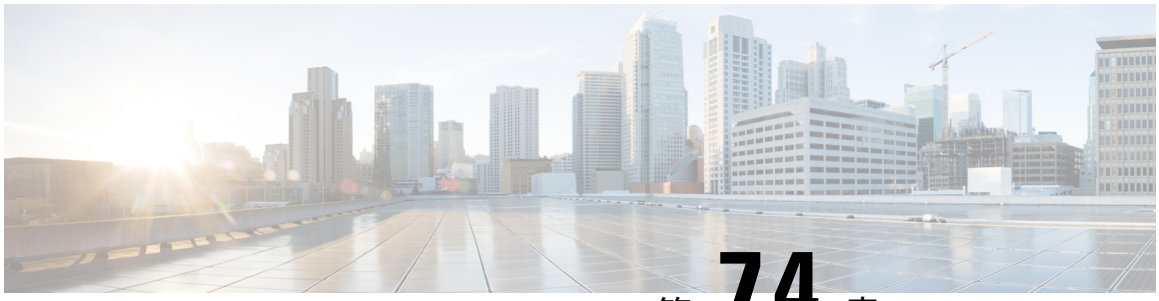
- 変更を廃棄する場合は、[キャンセル（Cancel）] をクリックし、プロンプトが出たら [OK] をクリックします。

次のタスク

- SSL ポリシーがアクセス コントロール ポリシーにまだ関連付けられていない場合は、アクセス制御への他のポリシーの関連付け （1684 ページ）の説明に従って関連付けます。
- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

関連トピック

TLS/SSL ルールの作成と変更 （1855 ページ）



第 74 章

TLS/SSL ルールの使用を開始するには

ここでは、TLS/SSL ルールの作成、設定、管理、トラブルシューティングの概要を示します。

（注） TLS と SSL は相互に使用されることが多いため、*TLS/SSL* という表現を使用していずれかのプロトコルについて説明していることを示しています。SSL プロトコルは、よりセキュアな TLS プロトコルを選択することにより IETF によって廃止されました。そのため、*TLS/SSL* は通常、TLS のみを指すものとして解釈できます。

例外は SSL ポリシーです。FMC 設定オプションは **[Policies]** > **[Access Control]** > **[SSL]** となるため、これらのポリシーは TLS および SSL のトラフィックのルールを定義するために使用されますが、「SSL ポリシー」という用語を使用します。

SSL プロトコルと TLS プロトコルの詳細については、「SSL と TLS：その違いとは（SSL vs. TLS - What's the Difference?）」を参照してください。

TLS/SSL規則の概要

TLS/SSL ルールを設定することで、それ以上のインスペクションなしでトラフィックをブロックする、トラフィックを復号せずにアクセス コントロールで検査する、あるいはアクセス コントロールの分析用にトラフィックを復号するなど、複数の管理対象デバイスをカバーしたきめ細かな暗号化トラフィックの処理メソッドを構築できます。

TLS/SSL ルールのガイドラインと制限事項

TLS/SSL ルールを設定するときは、次の点に注意してください。TLS/SSL ルールを適切に設定するのは複雑なタスクですが、暗号化トラフィックを処理する有効な導入には不可欠のタスクです。ルールをどのように設定するかには、制御できない特定のアプリケーションの動作を含む、多くの要素が影響します。

さらに、ルールが互いをプリエンプトしたり、追加ライセンスが必要になったりすることがあります。また、ルールに無効な設定が含まれる可能性もあります。慎重に設定された SSL ルールは、ネットワーク トラフィックの処理に必要なリソースの軽減にも寄与します。過度に複雑なルールを作成し、ルールを誤って順序付けすると、パフォーマンスに悪影響を与える可能性があります。

詳細については、ルールのパフォーマンスに関するガイドライン （502 ページ）を参照してください。

TLS 暗号化アクセラレーションに特に関連するガイドラインについては、TLS 暗号化アクセラレーション （1809 ページ）を参照してください。

関連トピック

ルールとその他のポリシーの警告 （501 ページ）
ルールのパフォーマンスに関するガイドライン （502 ページ）
TLS/SSL 復号の使用上のガイドライン （1848 ページ）
TLS/SSL ルールのサポートされない機能 （1849 ページ）
TLS/SSL 復号化禁止のガイドライン （1849 ページ）
TLS/SSL 復号化：再署名のガイドライン （1850 ページ）
TLS/SSL 復号 - 既知のキーのガイドライン （1852 ページ）
TLS/SSL ブロックのガイドライン （1852 ページ）
TLS/SSL 証明書のピン留めのガイドライン （1853 ページ）
TLS/SSL ハートビートのガイドライン （1853 ページ）
TLS/SSL 匿名の暗号スイートの制限事項 （1853 ページ）
TLS/SSL 正規化のガイドライン （1854 ページ）
TLS/SSL のその他のルールのガイドライン （1854 ページ）
SSL ルールの順序 （507 ページ）

TLS/SSL 復号の使用上のガイドライン

管理対象デバイスが暗号化されたトラフィックを処理する場合にのみ、[復号 - 再署名（Decrypt - Resign）] または [復号 - 既知のキー（Decrypt - Known Key）] のルールをセットアップします。復号ルールには、パフォーマンスに影響を及ぼす可能性があるオーバーヘッドの処理が必要です。

パッシブまたはインライン タップ モード インターフェイスを使用するデバイスでトラフィックを復号化することはできません。

TLS/SSL ルールのサポートされない機能

RC4 暗号スイーツはサポートされていません

Rivest Cipher 4（*RC4* または *ARC4* ともいう）暗号スイーツは脆弱性があることで知られており、安全でないと見なされています。SSL ポリシーでは RC4 暗号スイーツをサポート対象外として識別しています。組織の要件と一致するようにポリシーの [復号不可のアクション（Undecryptable Actions）] タブ ページの [サポート対象外の暗号スイーツ（Unsupported Cipher Suite）] のアクションを設定する必要があります。詳細については、復号できないトラフィックのデフォルト処理オプション（1839ページ）を参照してください。

パッシブおよびインライン タップ モードのインターフェイスはサポートされていません。

TLS/SSL トラフィックはパッシブまたはインライン タップ モードのインターフェイスでは復号できません。

TLS 1.3 はサポートされません

Firepower システムは現在、TLS バージョン 1.3 の暗号化または復号化をサポートしていません。ユーザが TLS 1.3 暗号化をネゴシエートする Web サイトにアクセスすると、Web ブラウザに次のようなエラーが表示されることがあります。

- **ERR_SSL_PROTOCOL_ERROR**
- **SEC_ERROR_BAD_SIGNATURE**
- **ERR_SSL_VERSION_INTERFERENCE**

この動作を制御する方法の詳細については、Cisco TAC にお問い合わせください。

TLS/SSL 復号化禁止のガイドライン

次によって禁止されている場合は、トラフィックを復号してはいけません。

- 法律：たとえば、一部の法域では、財務情報の復号化が禁止されています
- 会社のポリシー：たとえば、会社によって特権的な通信の復号化が禁止されている場合があります
- プライバシー規制
- 証明書のピン留め（*TLS/SSL* ピニングとも呼ばれる）を使用するトラフィックは、接続の切断を防ぐため、暗号化されたままにする必要があります

特定の種類のトラフィックで復号をバイパスする場合、トラフィックの処理は行われません。暗号化トラフィックは、最初に SSL ポリシーによって評価された後でアクセス コントロール ポリシーに進み、そこで最終的な許可またはブロックの決定が行われます。暗号化されたトラフィックは、次のものを含むがこれらに限定されない任意の TLS/SSL ルール条件で許可またはブロックできます。

- 証明書のステータス（期限切れまたは無効な証明書など）

- プロトコル（セキュアでない SSL プロトコルなど）
- ネットワーク（セキュリティ ゾーン、IP アドレス、VLAN タグなど）
- 正確な URL または URL カテゴリ
- [ポート（Port）]
- ユーザ グループ

TLS/SSL 復号化：再署名のガイドライン

[Decrypt - Resign] アクションには、1 つの内部認証局（CA）証明書と秘密キーを関連付けることができます。トラフィックがこのルールに一致した場合、システムは CA 証明書を使用してサーバ証明書を再署名してから、中間者（man-in-the-middle）として機能します。ここでは 2 つの TLS/SSL セッションが作成され、1 つはクライアントと管理対象デバイスの間、もう 1 つは管理対象デバイスとサーバの間で使用されます。各セッションにはさまざまな暗号セッションの詳細が含まれており、システムはこれを使用することでトラフィックの復号化と再暗号化が行えます。

ベスト プラクティス

次の点を推奨します。

- [Decrypt - Known Key] ルールアクションを推奨する着信トラフィックとは対照的に、発信トラフィックの復号化に対しては [Decrypt - Resign] ルールアクションを使用します。

  [Decrypt - Known Key] の詳細については、TBD を参照してください。

- [Decrypt - Resign] ルールアクションを設定する場合は、必ず **[Replace Key Only]** チェックボックスをオンにします。

  ユーザが自己署名証明書を使用する web サイトを参照すると、web ブラウザにセキュリティ警告が表示され、セキュリティで保護されていないサイトと通信していることに気付きます。

  ユーザが信頼できる証明書を使用する web サイトを参照すると、セキュリティ警告は表示されません。

Details

[復号 - 再署名（Decrypt - Resign）] アクションをルールに設定すると、ルールによるトラフィックの照合は、設定されている他のルール条件に加えて、参照する内部 CA 証明書の署名アルゴリズム タイプに基づいて実施されます。各 [復号 - 再署名（Decrypt - Resign）] アクションにはそれぞれ 1 つの CA 証明書が関連付けられるので、異なる署名アルゴリズムで暗号化された複数のタイプの発信トラフィックを復号化する TLS/SSL ルールは作成できません。また、ルールに追加する暗号スイートと外部証明書のオブジェクトのすべては、関連する CA 証明書の暗号化アルゴリズム タイプに一致する必要があります。

たとえば、楕円曲線暗号（EC）アルゴリズムで暗号化された発信トラフィックが [復号 - 再署名（Decrypt - Resign）] ルールに一致するのは、アクションが EC ベースの CA 証明書を参照している場合だけです。証明書と暗号スイートのルール条件を作成する場合は、EC ベースの外部証明書と暗号スイートをルールに追加する必要があります。

同様に、RSA ベースの CA 証明書を参照する [復号 - 再署名（Decrypt - Resign）] ルールは、RSA アルゴリズムで暗号化された発信トラフィックとのみ一致します。EC アルゴリズムで暗号化された発信トラフィックは、設定されている他のルール条件がすべて一致したとしても、このルールには一致しません。

注意事項と制約事項

また次の点に注意してください。

匿名の暗号スイートはサポート対象外

匿名の暗号スイートはその性質から、認証には使用されず、キー交換を使用しません。匿名の暗号スイートには限定的な用途があります。詳細については、RFC 5246 のセクション A.5 を参照してください。

匿名の暗号スイートは認証に使用されないため、ルールに [復号-再署名（Decrypt - Resign）] または [復号 - 既知のキー（Decrypt - Known Key）] アクションは使用できません。

一致しない暗号スイート

証明書と一致しない暗号スイートで TLS/SSL ルールを保存しようとすると、次のエラーが表示されます。この問題を解決するには、TLS/SSL 暗号スイートの確認 （1905 ページ）を参照してください。

```
Traffic cannot match this rule; none of your selected cipher suites contain a
signature algorithm that the resigning CA's signature algorithm
```

信頼できない認証局

サーバ証明書の再署名に使用する認証局（CA）をクライアントが信頼していない場合、証明書が信頼できないという警告がユーザに出されます。これを防ぐには、クライアントの信頼できる CA ストアに CA 証明書をインポートします。または組織にプライベート PKI がある場合は、組織の全クライアントで自動的に信頼されるルート CA が署名する中間 CA 証明書を発行して、その CA 証明書をデバイスにアップロードすることもできます。

HTTP プロキシの制限

クライアントと管理対象デバイスの間に HTTP プロキシがあって、クライアントとサーバが CONNECT HTTP メソッドを使用してトンネル TLS/SSL 接続を確立する場合、システムはトラフィックを復号化できません。システムによるこのトラフィックの処理法は、ハンドシェイク エラー（**Handshake Errors**）の復号できないアクションが決定します。

署名済み CA のアップロード

内部 CA オブジェクトを作成して証明書署名要求（CSR）の生成を選択した場合は、オブジェクトに署名付き証明書をアップロードするまで、この CA を [復号 - 再署名（Decrypt - Resign）] アクションに使用できません。

TLS/SSL 復号 - 既知のキーのガイドライン

[復号 - 既知のキー（Decrypt - Known Key）] アクションを設定した場合は、1 つまたは複数のサーバ証明書と秘密キーペアをアクションに関連付けることができます。トラフィックがルールに一致して、トラフィックの暗号化に使用された証明書とアクションに関連付けられた証明書が一致した場合、システムは適切な秘密キーを使用してセッションの暗号化と復号化キーを取得します。秘密キーへのアクセスが必要なため、このアクションが最も適しているのは、組織の管理下にあるサーバへの入力トラフィックを復号する場合です。

また次の点に注意してください。

匿名の暗号スイートはサポート対象外

匿名の暗号スイートはその性質から、認証には使用されず、キー交換を使用しません。匿名の暗号スイートには限定的な用途があります。詳細については、RFC 5246 のセクション A.5 を参照してください。

匿名の暗号スイートは認証に使用されないため、ルールに [復号-再署名（Decrypt - Resign）] または [復号 - 既知のキー（Decrypt - Known Key）] アクションは使用できません。

識別名または証明書が一致しない

[復号 - 既知のキー（Decrypt - Known Key）] アクションを指定して TLS/SSL ルールを作成した場合は、[識別名（Distinguished Name）] や [証明書（Certificate）] 条件による照合はできません。ここでの前提は、このルールがトラフィックと一致する場合、証明書、サブジェクト DN、および発行元 DN は、ルールに関連付けられた証明書とすでに一致済みであることです。

署名アルゴリズムの不一致

[復号 - 再署名（Decrypt - Resign）] アクションをルールに設定し、1 つまたは複数の外部証明書オブジェクトまたは暗号スイートで署名アルゴリズム タイプの不一致が生じた場合、ポリシー エディタでルールの横に情報アイコン（）が表示されます。すべての外部証明書オブジェクトまたはすべての暗号スイートで署名アルゴリズム タイプの不一致が生じた場合、ポリシーのルールの横には警告アイコン（[]）が表示され、SSL ポリシーに関連付けたアクセス コントロール ポリシーは適用できなくなります。

証明書のピン留め

ブラウザが証明書ピニングを使用してサーバ証明書を確認する場合は、サーバ証明書に再署名しても、このトラフィックを復号できません。このトラフィックを許可するには、サーバ証明書の共通名または識別名と一致させるために、[復号しない（Do not decrypt）] アクションを使用して TLS/SSL ルールを設定します。

TLS/SSL ブロックのガイドライン

[インタラクティブ ブロック（Interactive Block）] または [リセット付きインタラクティブ ブロック（Interactive Block with reset）] アクション付きのアクセス コントロール ルールと復号化トラフィックが一致する場合、システムは応答ページを表示します。

ルールでロギングを有効にすると、（**[分析（Analysis）] > [イベント（Events）] > [接続（Connections）]** で）2 つの接続イベントが表示されます。インタラクティブ ブロックのイベントと、ユーザがサイトの継続を選択したかどうかを示す別のイベントです。

関連トピック

HTTP 応答ページについて （1735 ページ）

TLS/SSL 証明書のピン留めのガイドライン

一部のアプリケーションでは、アプリケーション自体に元のサーバ証明書のフィンガープリントを埋め込む、ピニングまたは証明書ピニングと呼ばれる技術が使用されます。*TLS/SSL* そのため、[復号 - 再署名（Decrypt - Resign）] アクションで TLS/SSL ルールを設定した場合は、アプリケーションが管理対象デバイスから再署名された証明書を受信すると、検証が失敗し、接続が中断されます。

TLS/SSL のピン留めは中間者攻撃を避けるために使用されるため、防止または回避する方法はありません。次の選択肢があります。

- そのアプリケーション用に、[復号-再署名（Decrypt - Resign）] ルールよりも順序が前の、[復号しない（Do Not Decrypt）] ルールを作成します。
- Web ブラウザを使用してアプリケーションにアクセスするようユーザに指示します。

ルールの順序の詳細については、SSL ルールの順序 （507 ページ）を参照してください。

アプリケーションが TLS/SSL のピン留めを使用しているかどうかを判断するには、TLS/SSL ピニングのトラブルシューティング （1903 ページ）を参照してください。

TLS/SSL ハートビートのガイドライン

一部のアプリケーションでは、RFC6520 で定義されている Transport Layer Security（TLS）および Datagram Transport Layer Security（DTLS）プロトコルに対して、TLS ハートビート エクステンションが使用されます。TLS ハートビートは、接続がまだ有効であることを確認する方法を提供します。クライアントまたはサーバが指定されたバイト数のデータを送信し、応答を返すように相手に要求します。これが成功した場合は、暗号化されたデータが送信されます。

管理対象デバイスが をサポートしていない場合、または TLS 暗号化アクセラレーションが無効になっている場合は、ネットワーク分析ポリシー（NAP）で [Max Heartbeat Length] を設定して TLS ハートビートの処理方法を決定できます。詳細については、SSL プリプロセッサ （2379 ページ）を参照してください。

詳細については、「TLS ハートビートについて （1900 ページ）」を参照してください。

TLS/SSL 匿名の暗号スイートの制限事項

匿名の暗号スイートはその性質から、認証には使用されず、キー交換を使用しません。匿名の暗号スイートには限定的な用途があります。詳細については、RFC 5246 のセクション A.5 を参照してください。

匿名の暗号スイートは認証に使用されないため、ルールに [復号-再署名（Decrypt - Resign）] または [復号 - 既知のキー（Decrypt - Known Key）] アクションは使用できません。

TLS/SSL ルールの [暗号スイート（Cipher Suite）] 条件に匿名の暗号スイートを追加することはできますが、システムは、ClientHello 処理中に自動的に匿名の暗号スイートを削除します。ルールを使用するシステムでは、ClientHello の処理を防止するために TLS/SSL ルールを設定する必要があります。詳細については、SSL ルールの順序 （507 ページ）を参照してください。

TLS/SSL 正規化のガイドライン

インライン正規化プリプロセッサで [余剰ペイロードの正規化（Normalize Excess Payload）] オプションを有効にすると、プリプロセッサによる復号トラフィックの標準化時に、パケットがドロップされてトリミングされたパケットに置き換えられる場合があります。これで TLS/SSL セッションは終了しません。トラフィックが許可された場合、トリミングされたパケットは TLS/SSL セッションの一部として暗号化されます。

TLS/SSL のその他のルールのガイドライン

ユーザとグループ

ルールにグループまたはユーザを追加した後、そのグループまたはユーザを除外するようにレルムの設定を変更すると、ルールは適用されなくなります。（レルムを無効にする場合も同様です。）レルムの詳細については、レルムの作成 （2576 ページ）を参照してください。

TLS/SSL ルールのカテゴリ

SSL ポリシーに [復号-再署名（Decrypt - Resign）] アクションがあるにもかかわらず Web サイトが復号されない場合は、そのポリシーに関連付けられているルールの [カテゴリ（Category）] タブ ページを確認します。

場合によっては、認証などの目的で Web サイトが別のサイトにリダイレクトされ、リダイレクト先のサイトの URL カテゴリが復号を試みているサイトとは異なることがあります。たとえば、`gmail.com`（[Webベース電子メール（Web based email）] カテゴリ）は認証のために `accounts.gmail.com`（[インターネットポータル（Internet Portals）] カテゴリ）にリダイレクトされます。関連するすべてのカテゴリを必ず SSL ルールに含めます。

ローカル データベースにない URL のクエリ

[復号-再署名（Decrypt - Resign）] ルールを作成し、ローカル データベースにカテゴリとレピュテーションがない Web サイトをユーザが参照すると、データが復号されないことがあります。一部の Web サイトはローカル データベースで分類されません。分類されない場合、その Web サイトのデータはデフォルトでは復号されません。

この動作は **[システム（System）] > [統合（Integration）] > の設定を使用し [Cloud Services]、[不明 URL を Cisco Cloud に問い合わせる（Query Cisco cloud for unknown URLs）]** を使用して制御できます。

このオプションの詳細については、シスコ クラウド （1928 ページ）を参照してください。

TLS/SSL ルールの作成と変更

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	すべて（NGIPSv を除く）	いずれか（Any）	Admin/Access Admin/Network Admin

ステップ 1 Firepower Management Center にログインします。

ステップ 2 **[Policies]** > **[Access Control]** > **[SSL]** をクリックします。

ステップ 3 SSL ポリシーの横にある編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 4 次の選択肢があります。

- 新しいルールを追加するには、[ルールの追加（Add Rule）] をクリックします。
- 既存のルールを編集するには、編集アイコン（）をクリックします。

ステップ 5 ルールの [名前（Name）] を入力します。

ステップ 6 ルールを有効にするかどうか [Enabled] を指定します。

ステップ 7 ルールの位置を指定します。TLS/SSL ルールの順序の評価 （1819 ページ） を参照してください。

ステップ 8 ルールの [アクション（Action）] をクリックします。TLS/SSL ルール アクション設定 （1866 ページ）を参照してください。

ステップ 9 ルール条件とオプションを設定します。

a) セキュリティ ゾーンに基づいてルール条件を設定するには、[ゾーン（Zones）] をクリックします。インターフェイス条件 （468 ページ）を参照してください。

b) ネットワークまたは位置情報に基づいてルール条件を設定するには、[ネットワーク（Networks）] をクリックします。ネットワーク条件 （471 ページ）を参照してください。

c) VLAN に基づいてルール条件を設定するには、[VLAN] をクリックします。VLAN 条件 （476 ページ）を参照してください。

d) ユーザおよびグループに基づいてルール条件を設定するには、[ユーザ（Users）] をクリックします。ユーザ条件、レルム条件、および ISE 属性条件（ユーザ制御） （490 ページ）を参照してください。

e) アプリケーションに基づいてルール条件を設定するには、[アプリケーション（Applications）] をクリックします。アプリケーション条件（アプリケーション制御） （479 ページ）を参照してください。

f) 通信ポートに基づいてルール条件を設定するには、[ポート（Ports）] をクリックします。ポートおよび ICMP コードの条件 （477 ページ）を参照してください。

g) URL レピュテーションに基づいてルール条件を設定するには、[カテゴリ（Category）]をクリックします。HTTPS トラフィックのフィルタリング （1722 ページ）を含む、URL Filtering （1717 ページ）の章を参照してください。

h) TLS/SSL サーバ証明書に基づいてルール条件を設定するには、[証明書（Certificate）] をクリックします。サーバ証明書ベースの TLS/SSL ルール条件 （1874 ページ）を参照してください。

i) 識別名に基づいてルール条件を設定するには、[DN] をクリックします。証明書の識別名の TLS/SSL ルール条件 （1875 ページ）を参照してください。

j) TLS/SSL 証明書のステータスに基づいてルール条件を設定するには、[証明書ステータス（Cert Status）]をクリックします。証明書ステータスの TLS/SSL ルール条件 （1879 ページ）を参照してください。

k) 暗号スイートに基づいてルール条件を設定するには、[暗号スイート（Cipher Suite）]をクリックします。暗号スイートの TLS/SSL ルール条件 （1887 ページ）を参照してください。

l) TLS または SSL プロトコル バージョンに基づいてルール条件を設定するには、[バージョン（Version）] をクリックします。暗号化プロトコル バージョンの TLS/SSL ルール条件 （1891 ページ）を参照してください。

m) ルールのロギング オプションを設定するには、[ロギング（Logging）] をクリックします。接続のロギングのベスト プラクティス （3012 ページ）を参照してください。

ステップ 10 [保存（Save）] をクリックします。

次のエラーが表示されている場合は、TLS/SSL 暗号スイートの確認 （1905 ページ）：**Traffic cannot match this rule; none of your selected cipher suites contain a signature algorithm that the resigning CA's signature algorithm**を参照してください。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

TLS/SSL ルールをルール カテゴリに追加する

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	すべて（NGIPSv を除く）	いずれか（Any）	Admin/Access Admin/Network Admin

ステップ 1 SSL ルール エディタの [挿入（Insert）] ドロップダウン リストで [カテゴリ（Into Category）] を選択し、使用するカテゴリを選択します。

ステップ 2 [保存（Save）] をクリックします。

ヒント ルールを保存すると、そのカテゴリの最後に配置されます。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

番号による TLS/SSL ルールの位置指定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	すべて（NGIPSv を除く）	いずれか（Any）	Admin/Access Admin/Network Admin

ステップ 1 SSL ルール エディタの [挿入（Insert）] ドロップダウンリストで、[ルールの上（above rule）] または [ルールの下（below rule）] を選択して、適切なルール番号を入力します。

ステップ 2 [保存（Save）] をクリックします。

ヒント ルールを保存すると、指定した場所に配置されます。

次のタスク

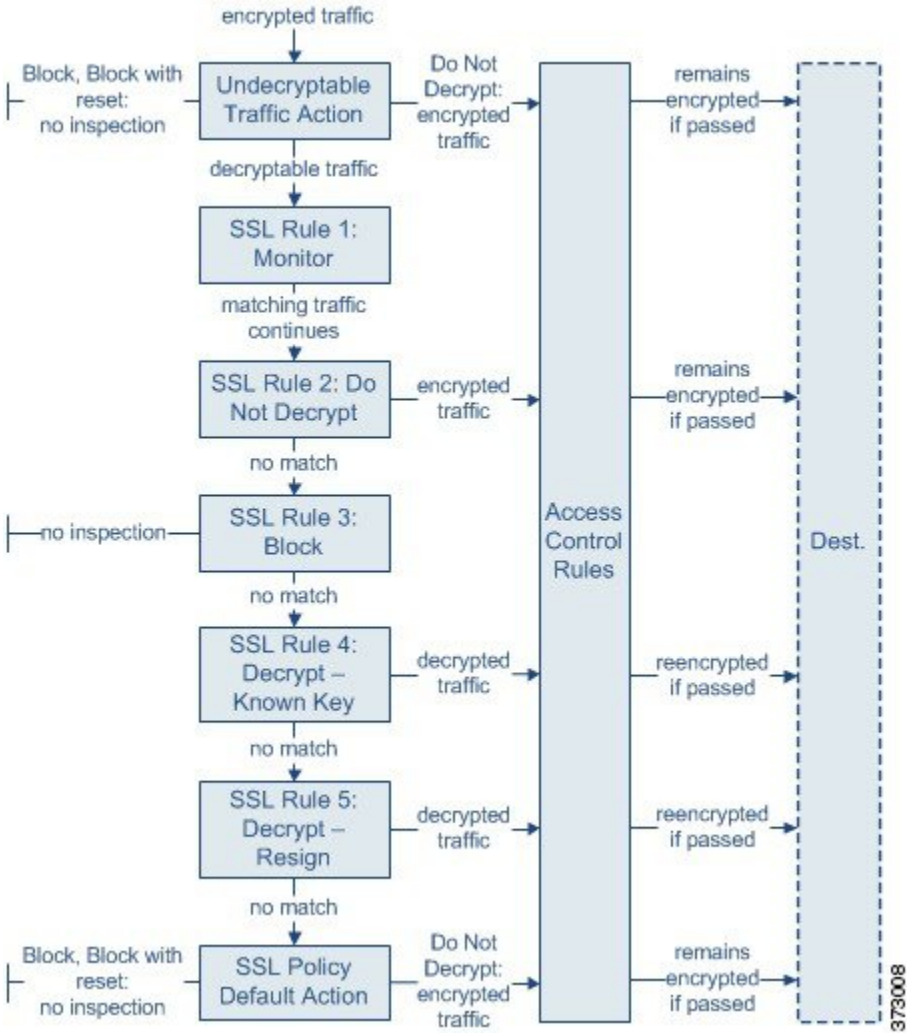
- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

TLS/SSL ルールのトラフィック処理

システムは指定した順序で TLS/SSL ルールをトラフィックと照合します。ほとんどの場合、システムによる暗号化トラフィックの処理は、すべてのルールの条件がトラフィックに一致する TLS/SSL最初の SSL ルールに従って行われます。こうした条件には、単純なものと複雑なものがあります。セキュリティゾーン、ネットワークまたは地理的位置、VLAN、ポート、アプリケーション、要求された URL、ユーザ、証明書、証明書の識別名、証明書ステータス、暗号スイート、暗号化プロトコル バージョンなどによってトラフィックを制御できます。

各ルールにはアクションも設定されます。アクションにより、アクセス制御と一致する暗号化または復号化トラフィックに対してモニタ、ブロック、検査のいずれを行うかが決まります。システムがブロックした暗号化トラフィックは、それ以上のインスペクションが行われないことに注意してください。暗号化されたトラフィックおよび復号できないトラフィックは、アクセス コントロールを使用して検査します。ただし、一部のアクセス コントロール ルールの条件では暗号化されていないトラフィックを必要とするため、暗号化されたトラフィックに一致するルール数が少なくなる場合があります。また、デフォルトでは、システムは暗号化されたペイロードの侵入およびファイルのインスペクションを無効にしています

次のシナリオは、インライン展開での SSL ルールによるトラフィックの処理を要約しています。



このシナリオでは、トラフィックは次のように評価されます。

- **復号できないトラフィック アクション（Undecryptable Traffic Action）**は、暗号化されたトラフィックを最初に評価します。復号化できないトラフィックについてシステムは、それ以上のインスペクションなしでブロックするか、あるいはアクセス コントロールによる検査用に渡します。一致しなかった暗号化トラフィックは、次のルールへと進められます。
- **TLS/SSLルール 1：モニタ（Rule 1: Monitor）**は、暗号化トラフィックを次に評価します。モニタ ルールは、暗号化トラフィックのログ記録と追跡を行いますが、トラフィック フローには影響しません。システムは引き続きトラフィックを追加のルールと照合し、許可するか拒否するかを決定します。
- **TLS/SSLルール 2：復号しない（Rule 2: Do Not Decrypt）**は、暗号化トラフィックを 3 番目に評価します。一致したトラフィックは復号されません。システムはこのトラフィックをアクセス コントロールにより検査しますが、ファイルや侵入インスペクションは行いません。一致しなかったトラフィックは、次のルールへと進められます。

- **TLS/SSLルール 3**：**ブロック（Rule 3: Block**）は、暗号化トラフィックを 4 番目に評価します。一致したトラフィックは、それ以上のインスペクションは行わずに、ブロックされます。一致しなかったトラフィックは、次のルールへと進められます。
- **TLS/SSLルール 4**：**復号 - 既知のキー（Rule 4: Decrypt - Known Key**）は、暗号化トラフィックを 5 番目に評価します。ネットワークへの着信トラフィックで一致したものは、ユーザのアップロードする秘密キーを使用して復号化されます。復号化トラフィックはその後、アクセス コントロール ルールで評価されます。アクセス コントロール ルールは、復号されたトラフィックと暗号化されていないトラフィックで同じ処理をします。この追加検査の結果、システムがトラフィックをブロックする場合があります。他のすべてのトラフィックは、宛先への送信が許可される前に再暗号化されます。SSL ルールに一致しなかったトラフィックは、次のルールへと進められます。
- **TLS/SSLルール 5**：**復号 - 再署名（Rule 5: Decrypt - Resign**）は、最後のルールです。トラフィックがこのルールに一致した場合、システムはアップロードされた CA 証明書を使用してサーバ証明書を再署名してから、中間者（man-in-the-middle）としてトラフィックを復号します。復号化トラフィックはその後、アクセス コントロール ルールで評価されます。アクセス コントロール ルールは、復号されたトラフィックと暗号化されていないトラフィックで同じ処理をします。この追加検査の結果、システムがトラフィックをブロックする場合があります。他のすべてのトラフィックは、宛先への送信が許可される前に再暗号化されます。SSL ルールに一致しなかったトラフィックは、次のルールへと進められます。
- **SSL ポリシーのデフォルト アクション（SSL Policy Default Action**）は、どの TLS/SSL ルールにも一致しなかったすべてのトラフィックを処理します。デフォルトアクションでは、暗号化トラフィックをそれ以上のインスペクションなしでブロックするか、あるいは復号しないで、アクセス コントロールによる検査を行います。

暗号化トラフィック インスペクションの設定

暗号化セッションの特性に基づいた暗号化トラフィックの制御および暗号化トラフィックの復号化には、再利用可能な公開キーインフラストラクチャ（PKI）オブジェクトの作成が必要です。この情報の追加は、信頼できる認証局（CA）の証明書の SSL ポリシーへのアップロード、SSL ルール条件の作成、およびプロセスでの関連オブジェクトの作成時に、臨機応変に実行できます。ただし、これらのオブジェクトを事前に設定しておくと、不適切なオブジェクトが作成される可能性を抑制できます。

証明書とキー ペアによる暗号化トラフィックの復号化

セッション暗号化に使用するサーバ証明書と秘密キーをアップロードして内部証明書オブジェクトを設定しておくと、システムは着信する暗号化トラフィックを復号化できます。**Decrypt - Known Key** アクションが設定された SSL ルールでそのオブジェクトを参照し、当該ルールにトラフィックが一致すると、システムはアップロードされた秘密キーを使用してセッションを復号化します。

CA 証明書と秘密キーをアップロードして内部 CA オブジェクトを設定した場合、システムは発信トラフィックの復号化もできます。[復号 - 再署名（Decrypt - Resign）] アクションが設定

された TLS/SSL ルールでそのオブジェクトを参照し、当該ルールにトラフィックが一致すると、システムはクライアント ブラウザに渡されたサーバ証明書を再署名した後、中間者（man-in-the-middle）としてセッションを復号します。オプションで、証明書全体ではなく自己署名証明書キーのみを置き換えることができます。この場合、ユーザはブラウザで自己署名証明書キー通知を確認します。

暗号化セッションの特性に基づいたトラフィック制御

システムによる暗号化トラフィックの制御は、セッション ネゴシエートに使用されたサーバ証明書または暗号スイートに基づいて実行できます。複数の異なる再利用可能オブジェクトの 1 つを設定し、TLS/SSL ルール条件でオブジェクトを参照してトラフィックを照合することができます。次の表に、設定できる再利用可能なオブジェクトのタイプを示します。

設定する内容	暗号化トラフィック制御に使用する条件
1 つまたは複数の暗号スイートが含まれる暗号スイートのリスト	暗号化セッションのネゴシエートに使用される暗号スイートが、暗号スイート リストにある暗号スイートのいずれかに一致する
組織が信頼する CA 証明書のアップロードによる信頼できる CA オブジェクト	この信頼できる CA は、次のいずれかにより、セッションの暗号化に使用されたサーバ証明書を信頼する • CA が証明書を直接発行した • サーバ証明書を発行した中間 CA に CA が証明書を発行した
サーバ証明書のアップロードによる外部証明書オブジェクト	セッションの暗号化に使用されたサーバ証明書が、アップロードされたサーバ証明書と一致する
発行元の識別名または証明書サブジェクトを含む識別名オブジェクト	セッション暗号化に使用された証明書で、サブジェクトまたは発行元の共通名、国、組織、組織単位のいずれかが、設定された識別名と一致する

関連トピック

暗号スイート リスト （576 ページ）
識別名オブジェクト （577 ページ）
PKI オブジェクト （579 ページ）

TLS/SSL ルールの順序の評価

SSL ポリシーで TLS/SSL ルールを作成する場合、ルール エディタの [挿入（Insert）] リストを使用してその位置を指定します。SSL ポリシー内の TLS/SSL ルールには、1 から始まる番号が付けられています。システムは、ルール番号の昇順で上から順に、TLS/SSL ルールをトラフィックと照合します。

ほとんどの場合、システムによるネットワーク トラフィックの処理は、すべてのルールの条件がトラフィックに一致する最初の TLS/SSLSSL ルールに従って行われます。モニタ ルール（ト

ラフィックをログに記録するがトラフィック フローには影響しないルール）の場合を除き、システムは、そのトラフィックがルールに一致した後、追加の優先順位の低いルールに対してトラフィックを評価し続けることはありません。こうした条件には、単純なものと複雑なものがあります。セキュリティ ゾーン、ネットワークまたは地理的位置、VLAN、ポート、アプリケーション、要求されたURL、ユーザ、証明書、証明書の識別名、証明書ステータス、暗号スイート、暗号化プロトコル バージョンなどによってトラフィックを制御できます。

各ルールにはアクションも設定されます。アクションにより、アクセス制御と一致する暗号化または復号化トラフィックに対してモニタ、ブロック、検査のいずれを行うかが決まります。システムがブロックした暗号化トラフィックは、それ以上のインスペクションが行われないことに注意してください。暗号化されたトラフィックおよび復号化できないトラフィックはアクセス コントロールの対象です。ただし、アクセス コントロール ルールの条件では暗号化されていないトラフィックを必要とするため、暗号化されたトラフィックに一致するルール数が少なくなります。

特定の条件（ネットワークや IP アドレスなど）を使用するルールは、一般的な条件（アプリケーションなど）を使用するルールの前に順位付けする必要があります。オープン システム相互接続（OSI）モデルに精通している場合は、考え方として同様の順位付けを使用してください。レイヤ1、2、および3（物理、データリンク、およびネットワーク）の条件を持つルールは、ルールの最初に順位付けする必要があります。レイヤ5、6、および7（セッション、プレゼンテーション、およびアプリケーション）の条件は、ルールの後ろのほうに順序付けする必要があります。OSI モデルの詳細については、こちらの Wikipedia の記事を参照してください。

ヒント 適切な TLS/SSL ルールの順序を指定することで、ネットワーク トラフィックの処理に必要なリソースが削減され、ルールのプリエンプションを回避できます。ユーザが作成するルールはすべての組織と展開に固有のものですが、ユーザのニーズに対処しながらもパフォーマンスを最適化できるルールを順序付けする際に従うべきいくつかの一般的なガイドラインがあります。

ルールは数値で順序付けするだけでなく、カテゴリ別にグループ化することもできます。デフォルトで、システムには3つのカテゴリ（管理者、標準、ルート）があります。カスタム カテゴリを追加できますが、システム提供のカテゴリを削除したり、それらの順序を変更したりすることはできません。

関連トピック

復号できないトラフィックのデフォルト処理オプション （1839 ページ）
SSL ルールの順序 （507 ページ）
ルールのパフォーマンスに関するガイドライン （502 ページ）

TLS/SSL ルール条件

SSL ルールの条件は、ルールで処理する暗号化トラフィックのタイプを特定します。条件には、単純なものと複雑なものがあり、ルールごとに複数の条件タイプを指定できます。トラ

フィックにルールが適用されるのは、トラフィックがルールの条件をすべて満たしている場合だけです。

特定の条件がルールに設定されていない場合、その条件に基づくトラフィック照合は行われません。たとえば、証明書の条件が設定され、バージョンの条件が設定されていないルールは、セッション SSL または TLS のバージョンにかかわりなく、セッションのネゴシエーションに使用されるサーバ証明書に基づいてトラフィックを評価します。

すべての TLS/SSL ルールには、一致する暗号化トラフィックに対して次の判定をする関連アクションがあります。

- 処理：最も重要なこととして、ルール アクションはルールの条件に一致する暗号化トラフィックに対して、モニタ、信頼、ブロック、または復号を行うかどうかを判定します。
- ロギング：ルールアクションは一致する暗号化トラフィックの詳細をいつ、どのようにログに記録するかを判定します。

TLS/SSLインスペクション設定では、次のように復号されたトラフィックの処理、検査、ログ記録を行います。

- SSLポリシーの復号できないアクションは、システムが復号できないトラフィックを処理します。
- ポリシーのデフォルト アクションは、モニタ以外のどの TLS/SSL ルールの条件にも一致しないトラフィックを処理します。

システムが暗号化セッションを信頼またはブロックしたときに、接続イベントをログに記録できます。アクセス コントロール ルールに従ってより詳細な評価のために復号化した場合の接続ログを記録するようにシステムを強制することも可能で、これはその後でどのような処理やトラフィックの検査がされるかとは無関係です。暗号化セッションの接続ログには、セッションの暗号化に使用される証明書など、暗号化の詳細が含まれます。ただし次の場合は、接続終了イベントだけをログに記録できます。

- ブロックされた接続（[ブロック（Block）]、[リセットしてブロック（Block with reset）]）の場合、システムは即座にセッションを終了し、イベントを生成します。
- 信頼された接続（Do not decrypt）の場合、システムはセッション終了時にイベントを生成します。

TLS/SSL ルールの条件タイプ

SSLルールを追加および編集するときは、ルールエディタ下部の左側にあるタブを使用して、ルール条件の追加と編集を行います。

表 *115 : TLS/SSL* ルールの条件タイプ

条件	一致する暗号化トラフィック	詳細
ゾーン	特定のセキュリティゾーンでインターフェイスを介したデバイスへの着信またはデバイスからの発信	セキュリティ ゾーンとは、展開やセキュリティ ポリシーに従って1つまたは複数のインターフェイスを論理的にグループ化したものです。ゾーン内のインターフェイスは、複数のデバイスにまたがって配置される場合があります。 （注） 、インラインまたはタップ モード インターフェイスでトラフィックを復号することはできません。
ネットワーク	その送信元または宛先 IP アドレス、国、または大陸による	明示的にIPアドレスを指定できます。位置情報の機能では、送信元または宛先となる国や大陸を基準にしたトラフィック制御もできます。
VLAN タグ	VLAN のタグ	システムは、最も内側の VLAN タグを使用して VLAN を基準にパケットを識別します。
ポート	送信元ポートまたは宛先ポート	TCP ポートに基づいて暗号化トラフィックを制御できます。
Users	セッションに関与するユーザによる	暗号化されたモニタ対象セッションの関連ホストにログインしている LDAP ユーザに基づいて暗号化トラフィックを制御できます。Microsoft Active Directory サーバから取得された個別ユーザまたはグループに基づいてトラフィックを制御できます。
アプリケーション	セッションで検出されたアプリケーションによる	タイプ、リスク、ビジネスとの関連性、カテゴリの基本的な特性に従って、フィルタ アクセスまたは暗号化セッションの各アプリケーションへのアクセスを制御できます。
カテゴリ	証明書サブジェクトの識別名に基づいてセッションで要求される URL	URL の一般分類とリスク レベルに基づいて、ネットワークのユーザがアクセスできる Web サイトを制限できます。

条件	一致する暗号化トラフィック	詳細
識別名	ブラウザでユーザが入力した URL が共通名（CN）と一致するか、または URL が証明書のサブジェクト代替名（SAN）に含まれています	サーバ証明書を発行した CA またはサーバ証明書ホルダーに基づいて、暗号化トラフィックを制御できます。
証明書（Certificates）	暗号化セッションのネゴシエートに使用されるサーバ証明書	暗号化セッションのネゴシエート用にユーザのブラウザに渡されるサーバ証明書に基づいて、暗号化されたトラフィックを制御できます。
証明書のステータス（Certificate Status）	暗号化セッションのネゴシエートに使用されるサーバ証明書のプロパティ	サーバ証明書のステータスに基づいて、暗号化トラフィックを制御できます。
暗号スイート	暗号化セッションのネゴシエートに使用する暗号スイート	暗号化セッションのネゴシエート用にサーバで選択された暗号スイートに基づいて、暗号化トラフィックを制御できます。
バージョン	セッションの暗号化に使用される SSL または TLS のバージョン	セッションの暗号化に使用される SSL または TLS のバージョンに基づいて、暗号化トラフィックを制御できます。

関連トピック

TLS/SSL のルールの条件
ユーザベースの TLS/SSL ルールの条件
暗号化トラフィックでのレピュテーションベースの URL ブロッキング
サーバ証明書ベースの TLS/SSL ルール条件 （1874 ページ）
ClientHello メッセージ処理 （1806 ページ）

TLS/SSL 規則アクション

ここでは、TLS/SSL ルールで利用可能なアクションについて説明します。

TLS/SSL ルールのモニタ アクション

[Monitor]アクションは、トラフィックを許可または拒否するように設計されていません。むしろ、その主な目的は、一致するトラフィックが最終的にどのように処理されるかに関係なく、接続ロギングを強制することです。その後、追加のルールが存在する場合はそのルールに照らしてトラフィックが照合され、信頼するか、ブロックするか、復号化するかが決定されます。モニタ ルール以外の一致する最初のルールが、トラフィック フローおよび追加のインスペク

ションを決定します。さらに一致するルールがない場合、システムはデフォルトアクションを使用します。

モニタ ルールの主要な目的はネットワーク トラフィックを追跡することであるため、ルールのロギング設定や、あとで接続を処理するデフォルトのアクションにかかわらず、システムはモニタ対象トラフィックの接続終了イベントを自動的に Firepower Management Center データベースに記録します。

TLS/SSL ルール：復号しないアクション

[復号しない（Do Not Decrypt）] アクションは、アクセス コントロール ポリシーのルールおよびデフォルトアクションに従って暗号化トラフィックを評価するため転送します。一部のアクセス コントロール ルールの条件では暗号化されていないトラフィックを必要とするため、こうしたトラフィックに一致するルール数が少なくなる場合があります。暗号化トラフィックに対しては、侵入やファイル インスペクションなどのディープ インスペクションを行うことはできません。

[復号しない（Do Not Decrypt）] ルール アクションの一般的な理由は、以下のとおりです。

- TLS/SSL トラフィックの復号が法律によって禁止されている。
- 信頼できると判明しているサイトである。
- トラフィックを調べることによって中断できるサイト（Windows Update など）である。
- TLS/SSL フィールドの値を表示するには、接続イベントを使用します。（接続イベント フィールドを表示するためにトラフィックを復号化する必要はありません。）詳細については、接続イベント フィールドの入力の要件 （3042 ページ）を参照してください。

詳細については、復号できないトラフィックのデフォルト処理オプション （1839ページ）を参照してください。

TLS/SSL ルールのブロック アクション

Firepower システムは、システムを通過させないトラフィックに対して次の TLS/SSL ルール アクションを提供します。

- [ブロック（Block）] では、接続が終了するため、クライアント ブラウザにエラーが表示されます。

  エラー メッセージには、ポリシーによってサイトがブロックされたことは示されません。代わりに、一般的な暗号化アルゴリズムがないと示される場合があります。このメッセージからは、故意に接続がブロックされたことは明らかになりません。

- [インタラクティブブロック（Interactive block）] では、宛先サーバへの接続が中断され、サーバへのアクセスが会社のポリシーに違反している可能性があることをユーザは確認する必要があります。

  デフォルトの確認応答ページを使用したり、カスタム ページを作成したりできます。

接続イベントは、ユーザが宛先サーバの継続を選択したかどうかを示します。

- [リセットしてブロック（Block with reset）] では、接続がリセットされるため、クライアント ブラウザにエラーが表示されます。

  このエラーでは、接続がリセットされたことはわかりますが、その理由はわかりません。

ヒント パッシブまたはインライン（タップ モード）展開では、デバイスがトラフィックを直接検査しないため、[ブロック（Block）] と [リセットしてブロック（Block with reset）] アクションを使用できないことに注意してください。パッシブまたはインライン（タップ モード）インターフェイスを含むセキュリティ ゾーン条件内で、[ブロック（Block）] と [リセットしてブロック（Block with reset）] アクションを使用したルールを作成すると、ポリシー エディタでルールの横に警告アイコン（⚠）が表示されます。

TLS/SSL ルールの復号アクション

[復号 - 既知のキー（Decrypt - Known Key）] および [復号 - 再署名（Decrypt - Resign）] アクションは、暗号化トラフィックを復号します。復号されたトラフィックは、アクセス制御を使用して検査されます。アクセス コントロール ルールは、復号化されたトラフィックと暗号化されていないトラフィックで同じ処理をします。ここではデータの確認に加えて、侵入、禁止ファイル、マルウェアの検出とブロックができます。システムは、許可されたトラフィックを再暗号化してから宛先に渡します。

信頼できる認証局（CA） からの証明書を使用してトラフィックを復号することをお勧めします。これにより、**Invalid Issuer** が接続イベント内の SSL 証明書ステータス列に表示されないようにします。

信頼できるオブジェクトを追加する方法の詳細については、信頼できる認証局オブジェクト（586 ページ）を参照してください。

TLS/SSL ルール アクション設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	すべて（NGIPSv を除く）	いずれか（Any）	Admin/Access Admin/Network Admin

始める前に

次を参照してください。

- TLS/SSL ルールのブロック アクション （1865 ページ）
- TLS/SSL ルール：復号しないアクション （1865 ページ）

- TLS/SSL ルールのモニタ アクション （1864 ページ）

ステップ 1 SSL ポリシー エディタには、次のオプションがあります。

- 新しいルールを追加するには、[ルールの追加（Add Rule）] をクリックします。
- 既存のルールを編集するには、編集アイコン（  ）をクリックします。

ステップ 2 [アクション（Action）] ドロップダウン リストからルール アクションを選択します。

- 暗号化トラフィックをブロックするには、[ブロック（Block）] を選択します。
- 暗号化トラフィックをブロックし、接続をリセットするには、[リセットでブロック（Block with reset）] を選択します。
- 着信トラフィックの復号の詳細については、復号 - 既知のキー アクションの設定 （1868 ページ）を参照してください。
- 発信トラフィックの復号の詳細については、復号 - 再署名アクションの設定 （1867 ページ）を参照してください。
- 暗号化トラフィックを記録するには、[モニタ（Monitor）] を選択します。
- 暗号化トラフィックを復号しない場合は、[復号化しない（Do Not Decrypt）] を選択します。

ステップ 3 [追加（Add）] をクリックします。

次のタスク

- ルールの概要 （463 ページ）の説明に従ってルール条件を設定します。
- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

復号 - 再署名アクションの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	すべて（NGIPSv を除く）	いずれか（Any）	Admin/Access Admin/Network Admin

始める前に

TLS/SSL 復号化：再署名のガイドライン （1850 ページ）を参照してください。

ステップ 1 SSL ルール エディタで、[アクション（Action）] リストから [復号 - 再署名（Decrypt - Resign）] を選択します。

ステップ 2 リストから内部 CA 証明書のオブジェクトを選択します。

ステップ 3 **[Replace key Only]** をオンにします。

[Decrypt - Resign] ルールアクションを設定する場合は、必ず **[Replace Key Only]** チェックボックスをオンにします。

ユーザが自己署名証明書を使用する web サイトを参照すると、web ブラウザにセキュリティ警告が表示され、セキュリティで保護されていないサイトと通信していることに気付きます。

ユーザが信頼できる証明書を使用する web サイトを参照すると、セキュリティ警告は表示されません。

ステップ 4 [追加（Add）] をクリックします。

ステップ 5 オプション信頼できる CA 署名書を SSL に使用して、接続イベントの SSL 証明書ステータス列に **Invalid Issuer** が表示されるのを回避するには、証明書をポリシーに追加します。

a) SSL ポリシー エディタ ページで、[信頼できる CA 証明書（Trusted CA Certificates）] タブをクリックします。

b) 既知のキーに対応する CA 証明書を SSL ポリシーに追加します。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

復号 - 既知のキー アクションの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	すべて（NGIPSv を除く）	いずれか（Any）	Admin/Access Admin/Network Admin

始める前に

TLS/SSL 復号 - 既知のキーのガイドライン （1852 ページ）を参照してください。

ステップ 1 SSL ルール エディタで、[アクション（Action）] ドロップダウン リストから、[復号 - 既知のキー（Decrypt - Known Key）] を選択します。

ステップ 2 [クリックして復号証明書を選択（Click to select decryption certs）] フィールドをクリックします。

ステップ 3 [使用可能な証明書（Available Certificates）] リストの 1 つ以上の内部証明書のオブジェクトを選択し、[ルールに追加（Add to Rule）] をクリックします。

ステップ 4 [OK] をクリックします。

ステップ 5 [追加（Add）] をクリックします。

ステップ 6 オプション信頼できる CA 署名書を SSL に使用して、接続イベントの SSL 証明書ステータス列に **Invalid Issuer** が表示されるのを回避するには、証明書をポリシーに追加します。

a) SSL ポリシー エディタ ページで、[信頼できる CA 証明書（Trusted CA Certificates）] タブをクリックします。

b) 既知のキーに対応する CA 証明書を SSL ポリシーに追加します。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

TLS/SSL Rules Management

SSL ポリシー エディタの [ルール（Rules）] タブ ページでは、ポリシー内の TLS/SSL ルールの追加、編集、検索、移動、有効化、無効化、削除、およびその他の管理を行うことができます。

TLS/SSL ルールの検索

スペースおよび印刷可能な特殊文字を含む英数字文字列を使用して、TLS/SSL ルールのリストで一致する値を検索できます。この検索では、ルール名およびルールに追加したルール条件が検査されます。ルール条件の場合は、条件タイプ（ゾーン、ネットワーク、アプリケーションなど）ごとに追加できる任意の名前または値が検索照合されます。これには、個々のオブジェクト名または値、グループ オブジェクト名、グループ内の個々のオブジェクト名または値、およびリテラル値が含まれます。

検索文字列のすべてまたは一部を使用できます。照合ルールごとに、一致する値のカラムが強調表示されます。たとえば、 `100Bao` という文字列のすべてまたは一部を基準に検索すると、少なくとも、100Bao アプリケーションを追加した各ルールの [Applications] カラムが強調表示されます。`100Bao` という名前のルールもある場合は、[Name] カラムと [Applications] カラムの両方が強調表示されます。

1 つ前または次の照合ルールに移動することができます。ステータス メッセージには、現行の一致および合計一致数が表示されます。

複数ページのルール リストでは、どのページでも一致が検出される可能性があります。最初の一致が検出されたのが最初のページではない場合は、最初の一致が検出されたページが表示されます。最後の一致が現行の一致となっている場合、次の一致を選択すると、最初の一致が表示されます。また、最初の一致が現行の一致となっている場合、前の一致を選択すると、最後の一致が表示されます。

TLS/SSL ルールの検索

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	すべて（NGIPSvを除く）	いずれか（Any）	Admin/Access Admin/Network Admin

ステップ 1 SSL ポリシー エディタで、[検索ルール（Search Rules）] プロンプトをクリックし、検索文字列を入力してから Enter キーを押します。

ヒント 一致する値を含むルールのカラムが強調表示されます。表示されている（最初の）一致は、他とは区別できるように強調表示されます。

ステップ 2 目的のルールを探すには次の操作が利用できます。

- 照合ルールの間を移動する場合は、次の一致アイコン（▼）または前の一致アイコン（▲）をクリックします。
- ページを更新し、検索文字列および強調表示をクリアするには、クリアアイコン（✖）をクリックします。

TLS/SSL ルールの有効化と無効化

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	すべて（NGIPSvを除く）	いずれか（Any）	Admin/Access Admin/Network Admin

作成した TLS/SSL ルールは、デフォルトで有効になっています。ルールを無効にすると、システムはネットワーク トラフィックの評価にそのルールを使用せず、そのルールに対する警告とエラーの生成を停止します。SSL ポリシーのルール リストを表示すると、無効なルールはグレー表示されますが、変更は可能です。またはルール エディタを使用して TLS/SSL ルールを有効または無効にできることに注意してください。

ステップ 1 SSL ポリシー エディタで、ルールを右クリックしてルール状態を選択します。

ステップ 2 **[保存（Save）]** をクリックします。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

TLS/SSL ルールの移動

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	すべて（NGIPSv を除く）	いずれか（Any）	Admin/Access Admin/Network Admin

ステップ 1 SSL ポリシー エディタで、各ルールの空白部分をクリックしてルールを選択します。

ステップ 2 ルールを右クリックして、[切り取り（Cut）] を選択します。

ステップ 3 切り取ったルールを貼り付けたい位置に隣接するルールの空白部分を右クリックし、[上に貼り付け（Paste above）] または [下に貼り付け（Paste below）] を選択します。

ヒント 2 つの異なる TLS/SSL ポリシーの間では、SSL ルールのコピー アンド ペーストはできません。

ステップ 4 **[保存（Save）]** をクリックします。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

新しい TLS/SSL ルール カテゴリの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	すべて（NGIPSv を除く）	いずれか（Any）	Admin/Access Admin/Network Admin

余計なポリシーを作成することなくルールをさらに整理するため、標準ルールとルート ルールのカテゴリの間にカスタム カテゴリを作成できます。追加したカテゴリは、名前変更と削除ができます。これらのカテゴリの移動はできませんが、ルールのカテゴリ間およびカテゴリ内外への移動は可能です。

ステップ 1 ポリシー エディタで、[カテゴリの追加（Add Category）] をクリックします。

ヒント ポリシーにルールがすでに含まれている場合は、既存のルールの行の空白部分をクリックして、新しいカテゴリを追加する前にその位置を設定できます。既存のルールを右クリックし、[新規カテゴリの挿入（Insert new category）] を選択することもできます。

ステップ 2 [名前（Name）] を入力します。

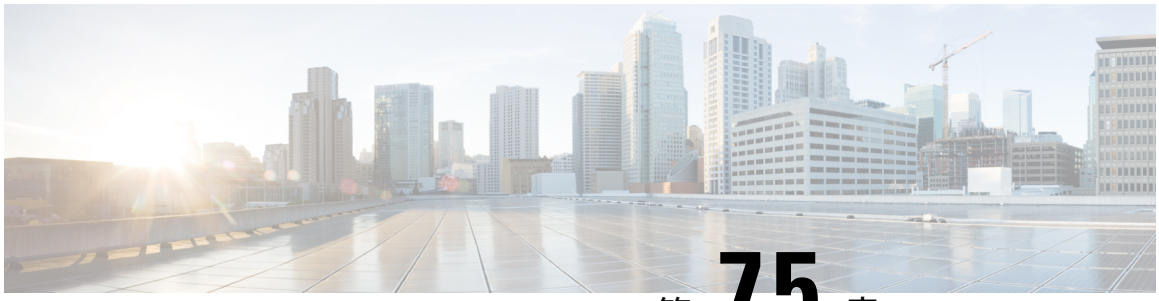
ステップ 3 次の選択肢があります。

- 最初の [Insert] ドロップダウン リストから [above Category] を選択した後、2 番目のドロップダウン リストからカテゴリを選択します。ここで選択したカテゴリの上にルールが配置されます。
- ドロップダウン リストから [below rule] を選択し、既存のルール番号を入力します。このオプションが有効なのは、ポリシーに少なくとも 1 つのルールが存在する場合のみです。
- ドロップダウン リストから [above rule] を選択し、既存のルール番号を入力します。このオプションが有効なのは、ポリシーに少なくとも 1 つのルールが存在する場合のみです。

ステップ 4 [OK] をクリックします。

ヒント 削除するカテゴリに含まれるルールは、その上にあるカテゴリに追加されます。

ステップ 5 **[保存（Save）]** をクリックします。



第 75 章

TLS/SSL ルールを使用した復号の調整

次のトピックでは、TLS/SSL ルール条件を設定する方法の概要を示します。

TLS/SSL ルール条件の概要

デバイスで検査されるすべての暗号化トラフィックには、基本的な TLS/SSL ルールに基づいたアクションが適用されます。暗号化トラフィックをより詳細に復号化および制御するには、特定タイプのトラフィックの処理およびログ記録を制御するルール条件を設定します。各 TLS/SSL ルールには 0 個、1 個、または複数の条件を設定できますが、トラフィックに TLS/SSL ルールが適用されるのは、そのルールのすべての条件にトラフィックが一致する場合のみです。

（注） トラフィックがルールに一致すると、デバイスは設定されたルールアクションをトラフィックに適用します。ログの記録が指定されている場合、接続が終了した時点でトラフィックに関するログが記録されます。

各ルール条件には、照合するトラフィックのプロパティを 1 つまたは複数指定できます。たとえば、以下のプロパティを指定できます。

- 通過するセキュリティ ゾーン、IP アドレスおよびポート、送信元または宛先の国、送信元または宛先の VLAN などのトラフィック フロー。
- 検出された IP アドレスに関連付けられたユーザ。
- トラフィックで検出されたアプリケーションなどのトラフィック ペイロード。
- 接続の暗号化に使用された TLS/SSL プロトコル バージョン、暗号スイート、サーバ証明書などの接続暗号化。
- サーバ証明書の識別名に指定された URL のカテゴリおよびレピュテーション。

関連トピック

インターフェイス条件 （468 ページ）
ネットワーク条件 （471 ページ）
VLAN 条件 （476 ページ）
ユーザ条件、レルム条件、および ISE 属性条件（ユーザ制御） （490 ページ）
アプリケーション条件（アプリケーション制御） （479 ページ）
ポートおよび ICMP コードの条件 （477 ページ）
HTTPS トラフィックのフィルタリング （1722 ページ）
サーバ証明書ベースの TLS/SSL ルール条件 （1874 ページ）
証明書の識別名の TLS/SSL ルール条件 （1875 ページ）
証明書ステータスの TLS/SSL ルール条件 （1879 ページ）
暗号スイートの TLS/SSL ルール条件 （1887 ページ）
暗号化プロトコル バージョンの TLS/SSL ルール条件 （1891 ページ）
ClientHello メッセージ処理 （1806 ページ）

サーバ証明書ベースの TLS/SSL ルール条件

TLS/SSL ルールでは、サーバ証明書の特性に基づいて暗号化トラフックを処理および復号できます。TLS/SSL ルールは、以下のサーバ証明書属性に基づいて設定することができます。

- 識別名条件を設定すると、証明書所有者またはサーバ証明書の発行元 CA に応じて暗号化トラフィックを処理および検査できます。発行元の識別名を基準にすると、サイトのサーバ証明書を発行した CA に基づいてトラフィックを処理できます。
- TLS/SSL ルールで証明書条件を設定すると、トラフィックの暗号化に使用されているサーバ証明書に応じて暗号化トラフィックを処理および検査できます。1 つの条件に 1 つまたは複数の証明書を設定でき、トラフィックの証明書がいずれかの条件の証明書と一致するとそのルールが適用されます。
- TLS/SSL ルールの証明書ステータス条件では、トラフィックの暗号化に使用されたサーバ証明書のステータスに基づいて暗号化されたトラフィックを処理して、証明書が有効か、失効しているか、期限切れか、まだ有効でないか、自己署名済みか、信頼できる CA によって署名済みか、証明書失効リスト（CRL）が有効かどうか、証明書のサーバ名指定（SNI）が要求内のサーバと一致するかどうかなどの検査を行うことができます。
- TLS/SSL ルールで暗号スイート条件を設定すると、暗号化セッションのネゴシエートに使用される暗号スイートに応じて暗号化トラフィックを処理および検査できます。
- TLS/SSL ルールでセッション条件を設定すると、トラフィックの暗号化に使用されている SSL または TLS のバージョンに応じて暗号化トラフィックを検査できます。

複数の暗号スイートを 1 つのルールで検出したり、証明書の発行元や証明書ホルダーを検出する場合は、再利用可能な暗号スイートのリストおよび識別名オブジェクトを作成してルールに

追加できます。サーバ証明書および特定の証明書ステータスを検出するには、ルール用の外部証明書と外部 CA オブジェクトの作成が必要です。

証明書の識別名の TLS/SSL ルール条件

ルール条件を設定する場合は、手動でリテラル値を指定するか、識別名オブジェクトを参照するか、または複数のオブジェクトを含んでいる識別名グループを参照できます。

（注） [復号 - 既知のキー（Decrypt - Known Key）] アクションを選択した場合、識別名条件を設定することはできません。このアクションでは、トラフィック復号用のサーバ証明書の選択が必要であるため、トラフィックの照合はすでにこの証明書で行われています。

複数のサブジェクトおよび発行元の識別名との一致を単一の証明書ステータスのルール条件で行うことも可能ですが、ルールとの照合で一致する必要があるのは1つの共通名または識別名だけです。

識別名を手動で追加する場合、共通名属性（**CN**）を含めることができます。`CN=` なしで共通名を追加すると、オブジェクトを保存する前に `CN=` が追加されます。

また、以降の属性ごとに1つずつ識別名をカンマで区切って追加することができます。たとえば、**C, CN, O, OU** というようにします。

1 つの識別名条件で、[サブジェクト DN（Subject DNs）] リストおよび [発行元 DN（Issuer DNs）] リストにそれぞれ最大 50 のリテラル値および識別名オブジェクトを追加できます。

システム提供の識別名オブジェクト グループである Cisco-Undecryptable-Sites には、システムで復号できないトラフィックの Web サイトが含まれます。このグループを識別名条件に追加すると、該当する Web サイトとのトラフィックがブロックしたり復号化を無効にしたりでき、これらのトラフィックの復号化に使用されるシステム リソースの浪費を回避できます。グループ内の各エントリは変更できますが、このグループを削除することはできません。システムによる更新によってこのリストのエントリが変更されることがありますが、ユーザによる変更は保持されます。

システムが新しいサーバへの暗号化セッションを最初に検出したときは、DN データを ClientHello の処理には使用できません。これは復号化されていない最初のセッションとなる可能性があります。最初のセッション後に、管理対象デバイスは、サーバの証明書メッセージからのデータをキャッシュします。同じクライアントからの後続の接続で、システムは識別名条件を含むルールに ClientHello メッセージを最終的に一致させ、メッセージを処理して、復号化の可能性を最大化できます。

証明書の識別名による暗号化トラフィックの制御

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	すべて（NGIPSvを除く）	いずれか（Any）	Admin/Access Admin/Network Admin

ステップ 1 SSL ルール エディタで、[DN] タブを選択します。

ステップ 2 [使用可能な DN（Available DNs）] で、追加する識別名を探します。

- ここで識別名オブジェクトを作成してリストに追加するには（後で条件に追加できます）、[使用可能な DN（Available DNs）] リストの上にある追加アイコン（  ）をクリックします。
- 追加する識別名オブジェクトおよびグループを検索するには、[Available DNs] リストの上にある [Search by name or value] プロンプトをクリックし、オブジェクトの名前またはオブジェクトの値を入力します。入力を開始するとリストが更新され、一致するオブジェクトが表示されます。

ステップ 3 オブジェクトを選択するには、そのオブジェクトをクリックします。すべてのオブジェクトを選択するには、右クリックして [Select All] を選択します。

ステップ 4 [サブジェクトに追加（Add to Subject）] または [発行元に追加（Add to Issuer）] をクリックします。

ヒント 選択したオブジェクトをドラッグ アンド ドロップでリストに追加することもできます。

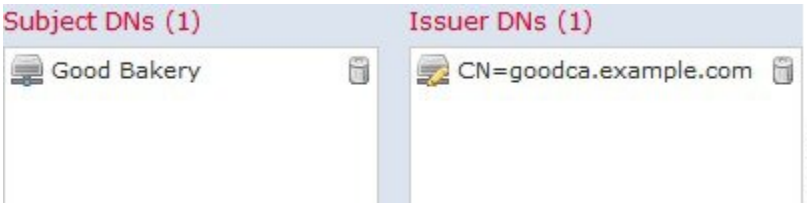
ステップ 5 手動で指定するリテラル共通名または識別名がある場合は、それらを追加します。[Subject DNs] または [Issuer DNs] リストの下にある [Enter DN or CN] プロンプトをクリックし、共通名または識別名を入力して [Add] をクリックします。

ステップ 6 ルールを追加するか、編集を続けます。

例

例

次の図は、goodbakery.example.com に対して発行された証明書および goodca.example.com によって発行された証明書を検索する識別名ルール条件を示しています。これらの証明書で暗号化されたトラフィックは許可され、アクセス コントロールにより制御されます。



次の図は、badbakery.example.com および関連ドメインに対して発行された証明書およびbadca.example.com によって発行された証明書を検索する識別名ルール条件を示しています。これらの証明書で暗号化されたトラフィックは、再署名された証明書を使用して復号されます。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

関連トピック

識別名オブジェクト （577 ページ）

証明書の TLS/SSL ルール条件

証明書ベースの TLS/SSL ルール条件を作成するときにサーバ証明書をアップロードしたり、再利用可能な外部証明書オブジェクトとして保存してサーバ証明書の名前を関連付けたりできます。また、既存の外部証明書オブジェクトやオブジェクト グループを使用して証明書条件を設定することもできます。

ルール条件の [Available Certificates] フィールドでは、外部証明書オブジェクトやオブジェクト グループを証明書の識別名に関する以下の特性に基づいて検索できます。

- 件名または発行元の共通名（CN）
- 件名または発行元の組織（O）
- 件名または発行元の部門（OU）

1 つの証明書のルール条件で複数の証明書に一致させることもでき、トラフィックの暗号化に使用されている証明書がアップロードされた証明書のいずれかと一致した場合、その暗号化トラフィックはルールに一致したと判定されます。

1 つの証明書条件で、[Selected Certificates] リストに最大 50 の外部証明書オブジェクトおよび外部証明書オブジェクト グループを追加できます。

次の点に注意してください。

- **Decrypt - Known Key** アクションを選択した場合、証明書条件を設定することはできません。このアクションでは、トラフィック復号化用のサーバ証明書の選択が必要であり、トラフィックの照合はすでにこの証明書で行われることになります。
- 証明書条件に外部証明書オブジェクトを設定する場合、暗号スイート条件に追加する暗号スイートまたは **Decrypt - Resign** アクションに関連付ける内部 CA オブジェクトのいずれ

かが、外部証明書の署名アルゴリズム タイプと一致する必要があります。たとえば、ルールの証明書条件で EC ベースのサーバ証明書を参照する場合は、追加する暗号スイート、または [復号 - 再署名（Decrypt - Resign）] アクションに関連付ける CA 証明書も EC ベースでなければなりません。署名アルゴリズム タイプの不一致が検出されると、ポリシー エディタでルールの横に警告アイコンが表示されます。

- システムが新しいサーバへの暗号化セッションを最初に検出したときは、証明書データを ClientHello の処理には使用できません。これは復号化されていない最初のセッションとなる可能性があります。最初のセッション後に、管理対象デバイスは、サーバの証明書メッセージからのデータをキャッシュします。同じクライアントからの後続の接続で、システムは証明書条件を含むルールに ClientHello メッセージを最終的に一致させ、メッセージを処理して、復号化の可能性を最大化できます。

証明書による暗号化トラフィックの制御

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	すべて（NGIPSv を除く）	いずれか（Any）	Admin/Access Admin/Network Admin

ステップ 1 SSL ルール エディタで、[証明書（Certificate）] タブを選択します。

ステップ 2 [使用可能な証明書（Available Certificates）] で、追加するサーバ証明書を探します。

- ここで外部証明書オブジェクトを作成してリストに追加するには（後で条件に追加できます）、[使用可能な証明書（Available Certificates）] リストの上にある追加アイコン（  ）をクリックします。
- 追加する証明書オブジェクトおよびグループを検索するには、[Available Certificates] リストの上にある [Search by name or value] プロンプトをクリックし、オブジェクトの名前またはオブジェクトの値を入力します。入力を開始するとリストが更新され、一致するオブジェクトが表示されます。

ステップ 3 オブジェクトを選択するには、そのオブジェクトをクリックします。すべてのオブジェクトを選択するには、右クリックして [Select All] を選択します。

ステップ 4 [Add to Rule] をクリックします。

ヒント 選択したオブジェクトをドラッグ アンド ドロップすることもできます。

ステップ 5 ルールを追加するか、編集を続けます。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

関連トピック

外部証明書オブジェクト （589 ページ）

証明書ステータスの TLS/SSL ルール条件

証明書ステータスの TLS/SSL ルール条件では、各ステータスの有無を基準にしたトラフィックの照合ができます。1 つのルール条件で複数のステータスを選択でき、いずれかのステータスと証明書が一致すれば、ルールとトラフィックが一致したと判定されます。

複数の証明書ステータスの有無を単一の証明書ステータス ルール条件で照合するように選択できます（いずれか 1 つの基準に一致するだけで、その証明書はルールに一致します）。

このパラメータを設定するときは、復号ルールを設定するのか、ブロック ルールを設定するのかを検討する必要があります。通常、ブロック ルールでは [はい（Yes）]、復号ルールでは [いいえ（No）] をクリックします。次に例を示します。

- [復号 - 再署名（Decrypt - Resign）] ルールを設定している場合、デフォルトの動作は、期限切れの証明書でのトラフィックを復号します。その動作を変更するには、[期限切れ（Expired）] で [いいえ（No）] をクリックし、期限切れの証明書を持つトラフィックが復号され、再署名されないようにします。
- [ブロック（Block）] ルールを設定している場合、デフォルトの動作は、期限切れの証明書を持つトラフィックを許可します。その動作を変更するには、[期限切れ（Expired）] で [はい（Yes）] をクリックし、期限切れの証明書を持つトラフィックをブロックします。

次の表は、暗号化用のサーバ証明書のステータスを基準に、システムが暗号化トラフィックを評価する方法を示しています。

表 *116*：証明書ステータスのルール条件の基準

ステータス チェック	Yes を設定	No を設定
Revoked	ポリシーは、サーバ証明書を発行した CA を信頼しており、ポリシーにアップロードされた CA 証明書にはこのサーバ証明書を失効させる CRL が含まれています。	ポリシーは、サーバ証明書を発行した CA を信頼しており、ポリシーにアップロードされた CA 証明書にはこのサーバ証明書を失効させる CRL が含まれていません。
Self-signed	検出されたサーバ証明書が、同じサブジェクトと発行元の識別名を含んでいます。	検出されたサーバ証明書が、異なるサブジェクトと発行元の識別名を含んでいます。

ステータス チェック	Yes を設定	No を設定
Valid	以下のすべてを満たしています。 • ポリシーが証明書を発行した CA を信用できる。 • 署名は有効である。 • 発行元は有効である。 • ポリシーの信頼できる CA のいずれも証明書を失効させていません。 • 現在の日付が証明書の有効期間の開始日と終了日の範囲内にある。	以下の 1 つ以上を満たしています。 • 証明書を発行した CA をポリシーが信頼していない。 • 署名が無効である。 • 発行元が無効である。 • ポリシーの信用できる CA の 1 つが原因で証明書が失効している。 • 現在の日付が証明書の有効期間の開始日より前です。 • 現在の日付が証明書の有効期限の終了日より後です。
Invalid signature	証明書の内容に対して証明書の署名が適切に検証されません。	証明書の内容に対して証明書の署名が適切に検証されます。
Invalid issuer	発行元の CA 証明書が、ポリシーの信頼できる CA 証明書のリストに登録されていません。	発行元の CA 証明書が、ポリシーの信頼できる CA 証明書のリストに登録されています。
Expired	現在の日付が証明書の有効期限の終了日より後です。	現在の日付が証明書の有効期限の終了日であるかそれより前です。
Not yet valid	現在の日付が証明書の有効期限の開始日より前です。	現在の日付が証明書の有効期限の開始日であるかそれより後です。

ステータス チェック	Yes を設定	No を設定
無効な証明書		証明書は有効です。以下のすべてを満たしています。 • 有効な証明書の拡張子。 • 指定した目的に証明書を使用できる。 • 有効な基本的制約のパス長。 • 有効な発行日付または有効期限の値。 • 有効な名前制約。 • 指定された目的に関してルート証明書を信頼できる。 • ルート証明書が指定した目的を受け入れている。

ステータス チェック	Yes を設定	No を設定
	証明書が有効ではありません。以下の 1 つ以上を満たしています。 • 証明書の拡張子が無効であるか一貫していません。つまり、証明書の拡張子に無効な値（たとえば間違ったエンコーディング）が含まれているか、他の拡張子と矛盾する値がいくつか含まれています。 • 指定された目的に証明書を使用できません。 • 基本的制約のパス長パラメータを超過しています。 詳細については、RFC 5280、セクション 4.2.1.9 を参照してください。 • 証明書の発行日付または有効期限の値が無効です。これらの日付は、UTCTime または GeneralizedTime としてエンコードできます。 詳細については、RFC 5280、セクション 4.1.2.5 を参照してください。 • 名前制約の形式が認識されていません。たとえば、電子メールアドレス形式のフォームは RFC 5280、セクション 4.2.1.10 で言及されていません。これは、不適切な拡張子や、一部の新機能が現時点でサポートされていないことが原因で発生する場合があります。	

ステータス チェック	Yes を設定	No を設定
	サポートされていない名前制約タイプが見つかりました。OpenSSL では、ディレクトリ名、DNS 名、電子メール、および URI タイプのみがサポートされています。 • 指定された目的に関してルート認証局を信頼できません。 • ルート認証局が指定された目的を拒否しています。	
無効な CRL	証明書失効リスト（CRL）のデジタル署名が有効ではありません。以下の 1 つ以上を満たしています。 • CRL の [次回の更新（Next Update）] または [最後の更新（Last Update）] フィールドの値が無効である。 • CRL がまだ有効ではない。 • CRL の期限が切れている。 • CRL パスを確認する際にエラーが発生した。拡張 CRL の確認が有効になっている場合にのみ、このエラーが発生する。 • CRL が検出できない。 • 検出できた唯一の CRL が証明書の範囲と一致しなかった。	CRL が無効です。以下のすべてを満たしています。 • [次回の更新（Next Update）] と [最後の更新（Last Update）] フィールドの値が有効である。 • CRL の日付が有効である。 • パスが有効である。 • CRL が検出された。 • CRL が証明書の範囲と一致する。

ステータス チェック	Yes を設定	No を設定
サーバの不一致	サーバ名がサーバのサーバ名指定（SNI）名と一致しません。これは、サーバ名を偽装しようとする試みを示している可能性があります。	サーバ名は、クライアントがアクセスを要求しているサーバの SNI 名と一致します。

1 つの証明書が複数のステータスに一致する場合でも、ルールがトラフィックに行うアクションは一度に 1 つだけであることに注意してください。

CA が証明書を発行したか失効したかを確認するには、ルートおよび中間 CA 証明書とその CRL をオブジェクトとしてアップロードする必要があります。その後で SSL ポリシーの信頼できる CA 証明書のリストに、これらの信頼できる CA のオブジェクトを追加します。

外部認証局の信頼

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	すべて（NGIPSv を除く）	いずれか（Any）	Admin/Access Admin/Network Admin

SSL ポリシーでルートおよび中間 CA 証明書を追加することで信頼できる CA が設定され、トラフィックの暗号化に使用されているサーバ証明書の検証に、これらの信頼できる CA を使用できるようになります。

信頼できる CA 証明書の中にアップロードされた証明書失効リスト（CRL）が含まれている場合は、信頼できる CA により、暗号化証明書が失効されているかどうかも確認できます。

ステップ 1 SSL ルール エディタで、[信頼できる CA 証明書（Trusted CA Certificates）] タブを選択します。

ステップ 2 次のように、[使用可能な信頼できる CA（Available Trusted CAs）] で追加する信頼できる CA を見つけます。

- ここで信頼できる CA のオブジェクトを作成してリストに追加するには、[使用可能な信頼できる CA（Available Trusted CAs）] リストの上にある追加アイコン（  ）をクリックします。
- 追加する信頼できる CA オブジェクトおよびグループを検索するには、[Available Trusted CAs] リストの上にある [Search by name or value] プロンプトをクリックし、オブジェクトの名前またはオブジェクトの値を入力します。入力を開始するとリストが更新され、一致するオブジェクトが表示されます。

ステップ 3 オブジェクトを選択するには、そのオブジェクトをクリックします。すべてのオブジェクトを選択するには、右クリックして [Select All] を選択します。

ステップ 4 [Add to Rule] をクリックします。

ヒント 選択したオブジェクトをドラッグ アンド ドロップすることもできます。

ステップ 5 ルールを追加するか、編集を続けます。

次のタスク

- TLS/SSL ルールに証明書ステータスの SSL ルール条件を追加します。詳細については、「証明書ステータスでのトラフィックの照合 （1885 ページ）」を参照してください。
- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

関連トピック

信頼できる認証局オブジェクト （586 ページ）

信頼できる外部認証局の設定

検証されたサーバ証明書には、信頼できる CA によって署名された証明書が含まれます。TLS/SSL ポリシーに信頼できる CA 証明書を追加した後は、トラフィックと照合する証明書ステータス条件を SSL ルールに設定することができます。

ヒント 信頼できるルート CA の信頼チェーン内にあるすべての証明書を、信頼できる CA 証明書のリストにアップロードしますが、これにはルート CA 証明書およびすべての中間 CA 証明書が含まれます。これを行わないと、中間 CA から発行された信頼できる証明書の検出が困難になります。また、ルート発行者 CA に基づいてトラフィックを信頼するように証明書ステータス条件を設定する場合、信頼できる CA の信頼チェーン内のすべてのトラフィックは、復号する必要はなく、復号せずに許可することができます。

SSL ポリシーを作成すると、[信頼できる CA 証明書（Trusted CA Certificates）] タブにデフォルトの信頼できる CA オブジェクト グループ Cisco Trusted Authorities が入力されます。

このグループ内の各エントリは変更が可能で、SSL ポリシーにこのグループを含めるかどうかを選択できます。このグループを削除することはできません。システムによる更新によりこのリストのエントリが変更されることがありますが、ユーザによる変更は保持されます。

証明書ステータスでのトラフィックの照合

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	すべて（NGIPSv を除く）	いずれか（Any）	Admin/Access Admin/Network Admin

始める前に

- 信頼できる CA オブジェクトまたはグループを SSL ポリシーに追加します。詳細については、外部認証局の信頼 （1884 ページ）を参照してください。

ステップ 1 Firepower Management Center で、[ポリシー（Policies）]>[アクセス コントロール（Access Control）]>[SSL] を選択します。

ステップ 2 新しいポリシーを追加するか、既存のポリシーを編集します。

ステップ 3 新しい TLS/SSL ルールを追加するか、既存のルールを編集します。

ステップ 4 [ルールの追加（Add Rule）] または [ルールの編集（Editing Rule）] ダイアログボックスで [証明書ステータス（Cert Status）] タブを選択します。

ステップ 5 各証明書ステータスには次のオプションがあります。

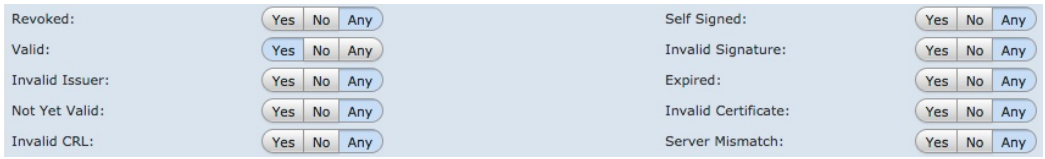
- 該当する証明書ステータスが存在するときに照合する場合は、[はい（Yes）] を選択します。
- 該当する証明書ステータスが存在しないときに照合する場合は、[いいえ（No）] を選択します。
- ルールが一致する場合、[任意（Any）] を選択して条件をスキップします。つまり、[任意（Any）] を選択すると、証明書ステータスの有無に関わらずルールは一致します。

ステップ 6 ルールを追加するか、編集を続けます。

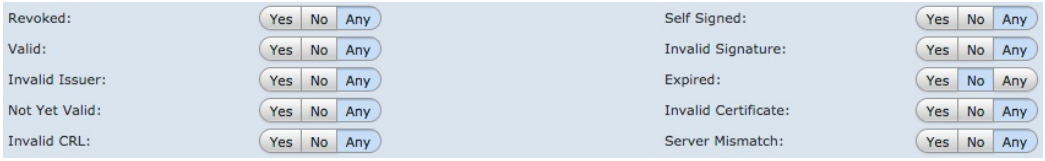
例

組織は Verified Authority という認証局を信頼しています。組織は Spammer Authority という認証局を信頼していません。システム管理者は、Verified Authority の証明書および、Verified Authority の発行した中間 CA 証明書をアップロードします。Verified Authority が以前に発行した証明書の 1 つを失効させたため、システム管理者は Verified Authority から提供された CRL をアップロードします。

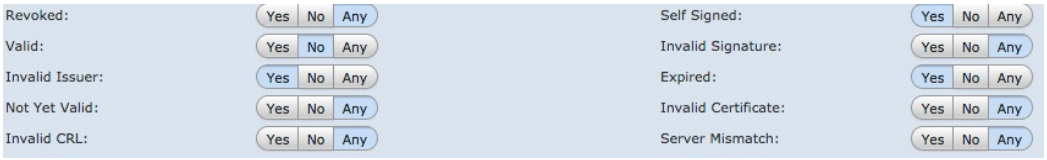
次の図は、有効な証明書をチェックする証明書ステータスのルール条件を示しています。これにより、Verified Authority から発行されたが CRL には登録されておらず、現状で有効期間の開始日と終了日の範囲内にあるかどうかがチェックされます。この設定では、これらの証明書で暗号化されたトラフィックはアクセス コントロールにより復号および検査されません。



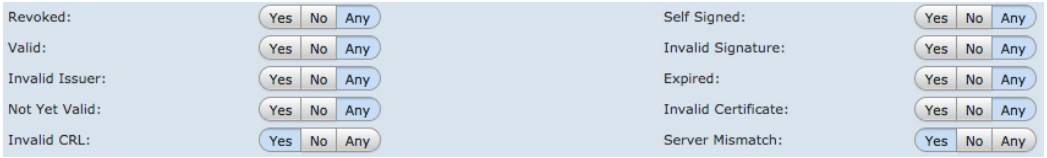
次の図は、ステータスの不在をチェックする証明書ステータスのルール条件を示しています。この設定では、期限切れになっていない証明書を使用して暗号化されたトラフィックに一致し、そのトラフィックをモニタします。



次の図は、さまざまなステータスの有無に一致する証明書ステータスのルール条件を示しています。この設定でルールが一致するのは、着信トラフィックを暗号化した証明書が無効なユーザが発行元、自己署名、無効、または期限切れであった場合で、そうしたトラフィックを既知のキーで復号します。



次の図は、要求の SNI がサーバ名に一致する、または CRL が有効でない場合に一致する証明書ステータスのルール条件を示しています。この設定のため、ルールがいずれかの条件に一致する場合に、トラフィックがブロックされます。



次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

暗号スイートの TLS/SSL ルール条件

暗号スイートのルール条件に追加できる、システム定義の暗号スイートが提供されています。複数の暗号スイートを含む、暗号スイートのリストのオブジェクトを追加することもできます。

（注） 新しい暗号スイートを追加することはできません。定義済みの暗号スイートは変更も削除もできません。

1 つの暗号スイート条件で、[選択した暗号スイート（Selected Cipher Suites）] リストに最大 50 の暗号スイートおよび暗号スイートリストを追加できます。暗号スイート条件に追加できる暗号スイートとして、次のものがサポートされています。

- SSL_RSA_FIPS_WITH_3DES_EDE_CBC_SHA
- SSL_RSA_FIPS_WITH_DES_CBC_SHA
- TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256

- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
- TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA256
- TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
- TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA256
- TLS_DHE_RSA_WITH_DES_CBC_SHA
- TLS_DH_Anon_WITH_AES_128_GCM_SHA256
- TLS_DH_Anon_WITH_AES_256_GCM_SHA384
- TLS_DH_Anon_WITH_CAMELLIA_128_CBC_SHA
- TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA256
- TLS_DH_Anon_WITH_CAMELLIA_256_CBC_SHA
- TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_NULL_SHA
- TLS_ECDHE_ECDSA_WITH_RC4_128_SHA
- TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_NULL_SHA
- TLS_ECDHE_RSA_WITH_RC4_128_SHA

- TLS_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
- TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256
- TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
- TLS_RSA_WITH_CAMELLIA_256_CBC_SHA256
- TLS_RSA_WITH_DES_CBC_SHA
- TLS_RSA_WITH_NULL_MD5
- TLS_RSA_WITH_NULL_SHA
- TLS_RSA_WITH_RC4_128_MD5
- TLS_RSA_WITH_RC4_128_SHA

次の点に注意してください。

- 展開でサポートされていない暗号スイートを追加すると、設定を展開できません。たとえば、パッシブ展開では、一時 Diffie-Hellman（DHE）および一時的楕円曲線 Diffie-Hellman（ECDHE）暗号スイートを使用したトラフィックの復号がサポートされません。それらの暗号スイートを使用してルールを作成すると、アクセス コントロール ポリシーを展開できなくなります。
- 暗号スイート条件に暗号スイートを設定する場合、証明書条件に追加する外部証明書オブジェクトまたは **Decrypt - Resign** アクションに関連付ける内部 CA オブジェクトのいずれかが、暗号スイートの署名アルゴリズム タイプと一致する必要があります。たとえば、ルールの暗号スイート条件で EC ベースの暗号スイートを参照する場合、追加するサーバ証明書または **[復号 - 再署名（Decrypt - Resign）]** アクションに関連付ける CA 証明書も EC ベースである必要があります。署名アルゴリズム タイプの不一致が検出されると、ポリシー エディタでルールの横に警告アイコンが表示されます。
- SSL ルールの**暗号スイート**条件に匿名の暗号スイートを追加できますが、次の点に注意してください。
  - システムは ClientHello 処理中に自動的に匿名の暗号スイートを削除します。ルールを使用するシステムでは、ClientHello の処理を防止するために TLS/SSL ルールを設定する必要があります。詳細については、SSL ルールの順序 （507 ページ）を参照してください。

- システムでは、匿名の暗号スイートで暗号化されたトラフィックは復号化できないため、ルールに **Decrypt - Resign** または **Decrypt - Known Key** アクションを使用できません。

- 暗号スイーをルール条件として指定する際、ルールをClientHelloメッセージで指定された暗号スイートの完全なリストではなく、ServerHelloメッセージのネゴシエートされた暗号スイートと照合することを検討してください。ClientHelloの処理中に、管理対象デバイスはClientHelloメッセージからサポートされていない暗号スイートを削除します。ただし、これにより指定されたすべての暗号スイートが削除されることになる場合、システムでは元のリストを保持します。システムがサポートされていない暗号スイートを保持する場合、後続の評価は復号化されないセッションになります。

暗号スイートによる暗号化トラフィックの制御

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	すべて（NGIPSvを除く）	いずれか（Any）	Admin/Access Admin/Network Admin

ステップ 1 SSL ルール エディタで、[暗号スイート（Cipher Suite）] タブを選択します。

ステップ 2 [使用可能な暗号スイート（Available Cipher Suites）] で、追加する暗号スイートを探します。

- ここで暗号スイートリストを作成してリストに追加するには（後で条件に追加できます）、[使用可能な暗号スイート（Available Cipher Suites）] リストの上にある追加アイコン（  ）をクリックします。
- 追加する暗号スイートおよびリストを検索するには、[Available Cipher Suites] リストの上にある [Search by name or value] プロンプトをクリックし、暗号スイートの名前または暗号スイートの値を入力します。入力を開始するとリストが更新され、一致する暗号スイートが表示されます。

ステップ 3 暗号スイートをクリックして選択します。すべての暗号スイートを選択するには、右クリックして[すべて選択（Select All）] を選択します。

ステップ 4 [ルールに追加（Add to Rule）] をクリックします。

ヒント 選択した暗号スイートをドラッグ アンド ドロップでリストに追加することもできます。

ステップ 5 ルールを追加するか、編集を続けます。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

関連トピック

暗号スイート リスト （576 ページ）

暗号化プロトコル バージョンの TLS/SSL ルール条件

SSL バージョン 3.0 または TLS バージョン 1.0、1.1、1.2 のいずれかで暗号化されたトラフィックとの照合を選択できます。デフォルトでは、ルールの作成時にすべてのプロトコルのバージョンが選択されます。複数のバージョンが選択されている場合、いずれかのバージョンと一致する暗号化トラフィックがルールに一致したと判定されます。ルール条件を保存するには、最低 1 つのプロトコル バージョンを選択する必要があります。

バージョンのルール条件で SSL バージョン 2.0 を選択することはできません。これは、SSL バージョン 2.0 で暗号化されたトラフィックの復号化がサポートされていないためです。復号できないアクションを設定すれば、それ以上のインスペクションなしで、これらのトラフィックを許可またはブロックできます。

暗号化プロトコルのバージョンによるトラフィックの制御

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	すべて（NGIPSv を除く）	いずれか（Any）	Admin/Access Admin/Network Admin

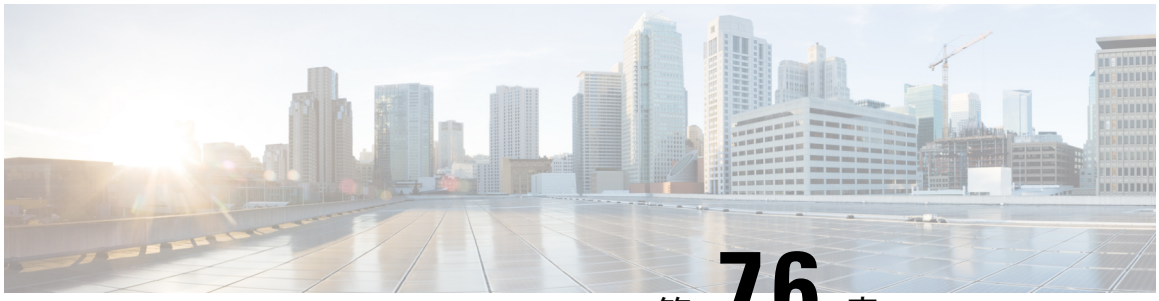
ステップ 1 SSL ルール エディタで、[バージョン（Version）] タブを選択します。

ステップ 2 照合するプロトコル バージョンを選択します。

ステップ 3 ルールを追加するか、編集を続けます。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。



第 76 章

SSLハードウェアアクセラレーションのモニタ

TLS 暗号化アクセラレーションの動作を評価するには、CLI で show counters コマンドを使用します。このコマンドにより、通常のアクティビティ、アラート、および潜在する致命的な問題について通知するさまざまなメトリックが一覧表示されます。

（注） **show counters description** コマンドを使用して各カウンタの説明を表示します。TLS 暗号化アクセラレーションに関連するカウンタのみを表示するには、**show counters description | include TLS_TRK** を使用します。

情報カウンタ

負荷のかかっているシステムが正常に動作している場合は、次のカウンタのカウントが大きくなります。接続ごとにトラッカープロセスには2つの側面があるため、これらのカウンタは接続ごとに 2 ずつ増加します。PRIV_KEY_RECV カウンタと SECU_PARAM_RECV カウンタが最も重要で、強調表示されています。CONTEXT_CREATED カウンタと CONTEXT_DESTROYED カウンタは、暗号化チップ メモリの割り当てに関連しています。

```
> show counters
Protocol      Counter                        Value   Context
SSLENC        CONTEXT_CREATED               258225   Summary
SSLENC        CONTEXT_DESTROYED             258225   Summary
TLS_TRK       OPEN_SERVER_SESSION           258225   Summary
TLS_TRK       OPEN_CLIENT_SESSION           258225   Summary
TLS_TRK       UPSTREAM_CLOSE                516450   Summary
TLS_TRK       DOWNSTREAM_CLOSE              516450   Summary
TLS_TRK       FREE_SESSION                  516450   Summary
TLS_TRK       CACHE_FREE                    516450   Summary
```

```
TLS_TRK      PRIV_KEY_RECV                    258225   Summary
TLS_TRK      NO_KEY_ENABLE                    258225   Summary
TLS_TRK      SECU_PARAM_RECV                  516446   Summary
TLS_TRK      DECRYPTED_ALERT                  258222   Summary
TLS_TRK      DECRYPTED_APPLICATION          33568976   Summary
TLS_TRK      ALERT_RX_CNT                     258222   Summary
TLS_TRK      ALERT_RX_WARNING_ALERT           258222   Summary
TLS_TRK      ALERT_RX_CLOSE_NOTIFY            258222   Summary
TCP_PRX      OPEN_SESSION                     516450   Summary
TCP_PRX      FREE_SESSION                     516450   Summary
TCP_PRX      UPSTREAM_CLOSE                   516450   Summary
TCP_PRX      DOWNSTREAM_CLOSE                 516450   Summary
TCP_PRX      FREE_CONN                        258222   Summary
TCP_PRX      SERVER_CLEAN_UP                  258222   Summary
TCP_PRX      CLIENT_CLEAN_UP                  258222   Summary
```

アラート カウンタ

TLS 1.2 の仕様に従い、次のカウンタを実装しました。FATAL アラートまたは BAD アラートは問題を示している可能性があります。ただし、ALERT_RX_CLOSE_NOTIFY は正常です。

詳細については、RFC 5246 のセクション 7.2 を参照してください。

```
TLS_TRK      ALERT_RX_CNT                       311   Summary
TLS_TRK      ALERT_TX_CNT                         2   Summary
TLS_TRK      ALERT_TX_IN_HANDSHAKE_CNT            2   Summary
TLS_TRK      ALERT_RX_IN_HANDSHAKE_CNT            2   Summary
TLS_TRK      ALERT_RX_WARNING_ALERT             308   Summary
TLS_TRK      ALERT_RX_FATAL_ALERT                 3   Summary
TLS_TRK      ALERT_TX_FATAL_ALERT                 2   Summary
TLS_TRK      ALERT_RX_CLOSE_NOTIFY              308   Summary
TLS_TRK      ALERT_RX_BAD_RECORD_MAC              2   Summary
TLS_TRK      ALERT_TX_BAD_RECORD_MAC              2   Summary
TLS_TRK      ALERT_RX_BAD_CERTIFICATE             1   Summary
```

エラー カウンタ

このカウンタは、システムエラーを示します。このカウントは、正常なシステムでは小さい値になります。BY_PASS カウンタは、復号せずに（ソフトウェアで実行される）インスペクション エンジン（Snort）プロセスとの間で直接渡されたパケットを示します。次の例は、いくつかの問題があるカウンタの一覧を示しています。

値が 0 のカウンタは表示されません。カウンタの完全な一覧を表示するには、次のコマンドを使用します。 **show counters description | include TLS_TRK**

```
> show counters
Protocol     Counter                        Value   Context
TCP_PRX      BYPASS_NOT_ENOUGH_MEM           2134   Summary
TLS_TRK      CLOSED_WITH_INBOUND_PACKET         2   Summary
TLS_TRK      ENC_FAIL                          82   Summary
TLS_TRK      DEC_FAIL                         211   Summary
TLS_TRK      DEC_CKE_FAIL                   43194   Summary
TLS_TRK      ENC_CB_FAIL                     4335   Summary
TLS_TRK      DEC_CB_FAIL                      909   Summary
TLS_TRK      DEC_CKE_CB_FAIL                  818   Summary
```

```
TLS_TRK      RECORD_PARSE_ERR                  123   Summary
TLS_TRK      IN_ERROR                        44948   Summary
TLS_TRK      ERROR_UPSTREAM_RECORD           43194   Summary
TLS_TRK      INVALID_CONTENT_TYPE              123   Summary
TLS_TRK      DOWNSTREAM_REC_CHK_ERROR          123   Summary
TLS_TRK      DECRYPT_FAIL                    43194   Summary
TLS_TRK      UPSTREAM_BY_PASS                  127   Summary
TLS_TRK      DOWNSTREAM_BY_PASS                127   Summary
```

重大カウンタ

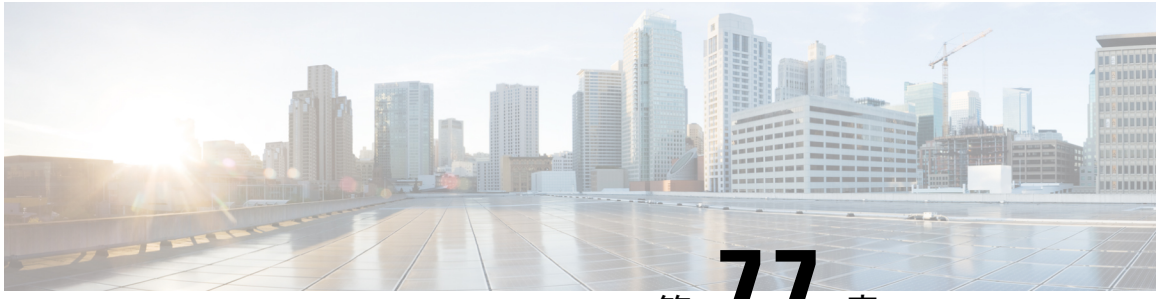
重大カウンタは、重大なエラーを示します。正常なシステムでは、このカウンタは 0 または 0 に近い値になります。次の例は、重大カウンタの一覧を示しています。

```
> show counters
Protocol     Counter                           Value   Context
CRYPTO       RING_FULL                             1   Summary
CRYPTO       ACCELERATOR_CORE_TIMEOUT              1   Summary
CRYPTO       ACCELERATOR_RESET                     1   Summary
CRYPTO       RSA_PRIVATE_DECRYPT_FAILED            1   Summary
```

RING_FULL カウンタは重大カウンタではなく、システムが暗号化チップに過負荷を与える頻度を示します。ACCELERATOR_RESET カウンタは、TLS 暗号化アクセラレーション プロセスが予期せず失敗した回数です。これは、保留中の操作が失敗する原因にもなり、この失敗の回数は ACCELERATOR_CORE_TIMEOUT および RSA_PRIVATE_DECRYPT_FAILED に表示されます。

永続的な問題がある場合は、TLS 暗号化アクセラレーションを無効にして（**system support ssl-hw-offload disable** または **config hwCrypto disable**）、問題を解決するために Cisco TAC と協力してください。

（注） **show snort tls-offload** コマンドと **debug snort tls-offload** コマンドを使用して、追加のトラブルシューティングを行うことができます。**clear snort tls-offload** コマンドを使用して、**show snort tls-offload** コマンドに表示されているカウンタをゼロにリセットします。



第 77 章

TLS/SSL ルールのトラブルシューティング

接続イベントを使用して、さまざまなエラー状態を診断できます。たとえば、TLS/SSL トラフィックにより管理対象デバイスが過負荷状態になっていることや、アプリケーションが TLS/SSL ピニングまたは TLS ハートビートを使用していることがあります。このような場合は、SSL ルールの調整や、ネットワークの通常の動作を復元するためのその他のアクションが必要になることがあります。

TLS/SSL オーバーサブスクリプションについて

TLS/SSL オーバーサブスクリプションとは、管理対象デバイスが TLS/SSL トラフィックにより過負荷になっている状態です。すべての管理対象デバイスで TLS/SSL オーバーサブスクリプションが発生する可能性がありますが、TLS 暗号化アクセラレーションをサポートする管理対象デバイスでのみ処理方法を設定できます。

TLS 暗号化アクセラレーションが有効になっている管理対象デバイスがオーバーサブスクライブされた場合、管理対象デバイスによって受信されるパケットの扱いは、SSL ポリシーの [Undecryptable Actions] の [Handshake Errors] の設定に従います。

- デフォルト アクションを継承（Inherit default action）
- Do not decrypt
- Block
- Block with reset

SSL ポリシーの [Undecryptable Actions] の [Handshake Errors] の設定が [Do Not decrypt] で、関連付けられたアクセス コントロール ポリシーがトラフィックを検査するように設定されている場合は、インスペクションが行われます。復号は行われません。

TLS/SSL オーバーサブスクリプションのトラブルシューティング

管理対象デバイスで TLS 暗号化アクセラレーションを有効にした場合は、接続イベントを表示して、デバイスに SSL オーバーサブスクリプションが発生しているかどうかを確認できます。接続イベント テーブル ビューに、少なくとも [SSLフローフラグ（SSL Flow Flags）] イベントを追加する必要があります。

始める前に

- [復号できないアクション（Undecryptable Actions）] タブ ページの [ハンドシェイクエラー（Handshake Error）] の設定で、SSL ポリシーを設定します。

  詳細については、復号できないトラフィックのデフォルト処理を設定する （1843 ページ）を参照してください。

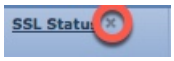
- SSL ルールによる復号可能接続のロギング （3016 ページ）の説明に従って、SSL ルールのログを有効にします。

ステップ 1 まだ Firepower Management Center にログインしていない場合は、ログインします。

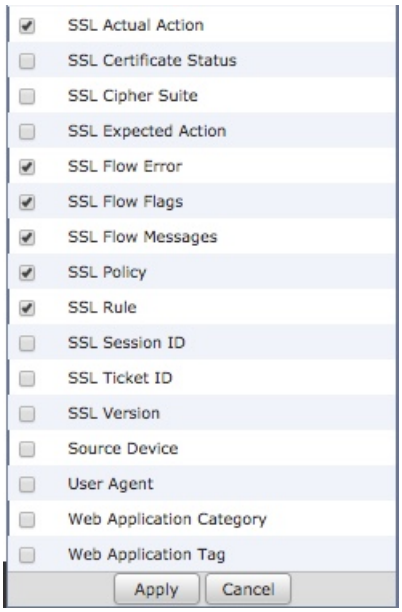
ステップ 2 **[分析（Analysis）] > [接続（Connection）] > [イベント（Events）]** をクリックします。

ステップ 3 [接続イベントのテーブルビュー（Table View of Connection Events）] をクリックします。

ステップ 4 接続イベントのテーブル ビューで、任意の列の [x] をクリックして、少なくとも [SSLフローフラグ（SSL Flow Flags）] 列をテーブルに追加します。



次の例では、接続イベントのテーブル ビューに、[SSLの実際の動作（SSL Actual Action）]、[SSLフローエラー（SSL Flow Error）]、[SSLフローフラグ（SSL Flow Flags）]、[SSLフローメッセージ（SSL Flow Messages）]、[SSLポリシー（SSL Policy）]、および [SSLルール（SSL Rule）] 列を追加します。



接続イベントとセキュリティインテリジェンスイベントのフィールド（3024ページ）で説明した順序で列が追加されます。

ステップ 5 [適用（Apply）] をクリックします。
TLS/SSL オーバーサブスクライブは、[SSLフローフラグ（SSL Flow Flags）]列の `ERROR_EVENT_TRIGGERED` および `OVER_SUBSCRIBED` の値で示されます。

次の図は例を示しています。

SSL Flow Error	SSL Actual Action	SSL Flow Flags
Success	Block With Reset	ERROR_EVENT_TRIGGERED, OVER_SUBSCRIBED
Success	Block With Reset	ERROR_EVENT_TRIGGERED, OVER_SUBSCRIBED
Success	Block With Reset	ERROR_EVENT_TRIGGERED, OVER_SUBSCRIBED
Success	Block With Reset	ERROR_EVENT_TRIGGERED, OVER_SUBSCRIBED
Success	Block With Reset	ERROR_EVENT_TRIGGERED, OVER_SUBSCRIBED
Success	Block With Reset	ERROR_EVENT_TRIGGERED, OVER_SUBSCRIBED

ステップ 6 TLS/SSL オーバーサブスクライブが発生している場合は、管理対象デバイスにログインして、次のコマンドのいずれかを入力します。

コマンド（Command）	結果
show counters	**TCP_PRX BYPASS_NOT_ENOUGH_MEM** の値が大きい場合は、SSL トラフィックに対してより大きな容量を持つデバイスへのアップグレードを検討するか、または優先順位の低いトラフィックに [復号しない（Do Not Decrypt）] を使用します。
show snort tls-offload	**BYPASS_NOT_ENOUGH_MEM** の値が大きい場合は、SSL トラフィックに対してより大きな容量を持つデバイスへのアップグレードを検討するか、または優先順位の低いトラフィックに [復号しない（Do Not Decrypt）] を使用します。

関連トピック

接続およびセキュリティ インテリジェンス イベント テーブルの使用 （3050 ページ）
接続イベントとセキュリティ インテリジェンス イベントのフィールド （3024 ページ）
接続イベント フィールドで利用可能な情報 （3044 ページ）
イベントの検索 （2967 ページ）

TLS ハートビートについて

一部のアプリケーションでは、RFC6520 で定義されている Transport Layer Security（TLS）および Datagram Transport Layer Security（DTLS）プロトコルに対して、TLS ハートビート エクステンションが使用されます。TLS ハートビートは、接続がまだ有効であることを確認する方法を提供します。クライアントまたはサーバが指定されたバイト数のデータを送信し、応答を返すように相手に要求します。これが成功した場合は、暗号化されたデータが送信されます。

TLS 暗号化アクセラレーションが有効になっている管理対象デバイスが TLS ハートビート エクステンションを使用するパケットを扱うときは、管理対象デバイスは SSL ポリシーの [Undecryptable Actions] の [Decryption Errors] の設定で指定されたアクションを行います。

- Block
- Block with reset

関連トピック

TLS ハートビートのトラブルシューティング （1900 ページ）

TLS ハートビートのトラブルシューティング

管理対象デバイスで TLS 暗号化アクセラレーションを有効にした場合は、接続イベントを表示して、デバイスが TLS ハートビート エクステンションを使用してトラフィックを監視して

いるかどうかを確認できます。接続イベント テーブル ビューに、少なくとも [SSLフローメッセージ（SSL Flow Messages）] イベントを追加する必要があります。

始める前に

SSL ハートビートは、接続イベント テーブル ビューの [SSLフローメッセージ（SSL Flow Messages）] 列の `HEARTBEAT` の値で示されます。ネットワーク内のアプリケーションが SSL ハートビートを使用しているかどうかを確認するには、最初に次のタスクを実行します。

- [復号できないアクション（Undecryptable Actions）] タブ ページの [復号化エラー（Decryption Error）] の設定で、SSL ポリシーを設定します。

  詳細については、復号できないトラフィックのデフォルト処理を設定する（1843 ページ）を参照してください。

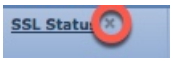
- SSL ルールによる復号可能接続のロギング（3016 ページ）の説明に従って、SSL ルールのログを有効にします。

ステップ 1 まだ Firepower Management Center にログインしていない場合は、ログインします。

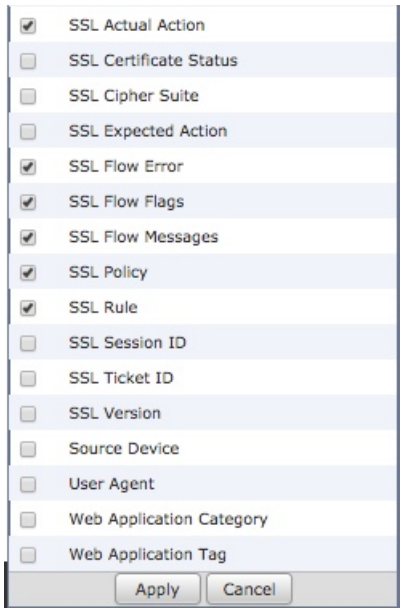
ステップ 2 **[分析（Analysis）] > [接続（Connection）] > [イベント（Events）]** をクリックします。

ステップ 3 [接続イベントのテーブルビュー（Table View of Connection Events）] をクリックします。

ステップ 4 接続イベントのテーブル ビューで、任意の列の [x] をクリックして、少なくとも [SSLフローメッセージ（SSL Flow Messages）] 列をテーブルに追加します。



次の例では、接続イベントのテーブル ビューに、[SSLの実際の動作（SSL Actual Action）]、[SSLフローエラー（SSL Flow Error）]、[SSLフローフラグ（SSL Flow Flags）]、[SSLフローメッセージ（SSL Flow Messages）]、[SSLポリシー（SSL Policy）]、および [SSLルール（SSL Rule）] 列を追加します。



接続イベントとセキュリティ インテリジェンス イベントのフィールド（3024 ページ）で説明した順序で列が追加されます。

ステップ 5 [適用（Apply）] をクリックします。
TLS ハートビートは、[SSL Flow Messages] 列の `HEARTBEAT` の値で示されます。

ステップ 6 ネットワーク上のアプリケーションで SSL ハートビートを使用する場合は、TLS/SSL ルールのガイドラインと制限事項 （1848 ページ）を参照してください。

関連トピック

TLS ハートビートのトラブルシューティング （1900 ページ）
TLS ハートビートについて （1900 ページ）
接続およびセキュリティ インテリジェンス イベント テーブルの使用 （3050 ページ）
接続イベントとセキュリティ インテリジェンス イベントのフィールド （3024 ページ）
接続イベント フィールドで利用可能な情報 （3044 ページ）
イベントの検索 （2967 ページ）

TLS/SSL のピニングについて

一部のアプリケーションでは、アプリケーション自体に元のサーバ証明書のフィンガープリントを埋め込む、ピニングまたは証明書ピニングと呼ばれる技術が使用されます。*TLS/SSL* そのため、[復号 - 再署名（Decrypt - Resign）] アクションで TLS/SSL ルールを設定した場合は、アプリケーションが管理対象デバイスから再署名された証明書を受信すると、検証が失敗し、接続が中断されます。

TLS/SSL ピニングが行われていることを確認するには、Facebook などのモバイル アプリケーションへのログインを試みます。ネットワーク接続エラーが表示された場合は、Web ブラウザ

を使用してログインします。（たとえば、Facebook のモバイル アプリケーションにログインすることはできませんが、Safari または Chrome を使用して Facebook にログインすることはできます）。Firepower Management Center の接続イベントは、TLS/SSL ピニングのさらなる証明として使用できます

（注） TLS/SSL ピニングはモバイル アプリケーションに限定されません。

ネットワーク上のアプリケーションで SSL ピニングを使用する場合は、次を参照してください。 TLS/SSL ルールのガイドラインと制限事項 （1848 ページ）

関連トピック

TLS/SSL ピニングのトラブルシューティング （1903 ページ）

TLS/SSL ピニングのトラブルシューティング

デバイスで SSL ピニングが発生しているかどうかを確認するには、接続イベントを表示します。接続イベント テーブル ビューに、少なくとも [SSLフローフラグ（SSL Flow Flags）] と [SSLフローメッセージ（SSL Flow Messages）] 列を追加する必要があります。

始める前に

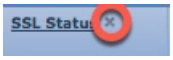
- SSL ルールによる復号可能接続のロギング （3016 ページ）の説明に従って、TLS/SSL ルールのログを有効にします。
- Facebook のようなモバイルアプリケーションにログインします。ネットワーク接続エラーが表示されたら、Chrome または Safari を使用して Facebook にログインします。Web ブラウザを使用してログインできても、ネイティブ アプリケーションではできない場合は、SSL ピニングが発生している可能性があります。

ステップ 1 まだ Firepower Management Center にログインしていない場合は、ログインします。

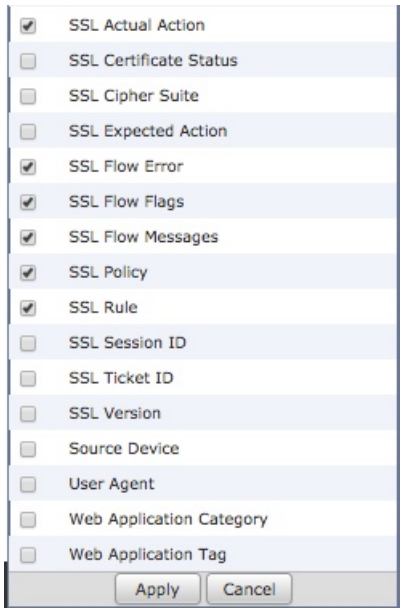
ステップ 2 **[分析（Analysis）] > [接続（Connection）] > [イベント（Events）]** をクリックします。

ステップ 3 [接続イベントのテーブルビュー（Table View of Connection Events）] をクリックします。

ステップ 4 任意の列の [x] をクリックして、少なくとも [SSLフローフラグ（SSL Flow Flags）] と [SSLフローメッセージ（SSL Flow Messages）] 列を接続イベント テーブルに追加します。



次の例では、接続イベントのテーブル ビューに、[SSLの実際の動作（SSL Actual Action）]、[SSLフローエラー（SSL Flow Error）]、[SSLフローフラグ（SSL Flow Flags）]、[SSLフローメッセージ（SSL Flow Messages）]、[SSLポリシー（SSL Policy）]、および [SSLルール（SSL Rule）] 列を追加します。



接続イベントとセキュリティインテリジェンスイベントのフィールド（3024ページ）で説明した順序で列が追加されます。

ステップ 5 [適用（Apply）] をクリックします。

ステップ 6 次に SSL ピニングの動作を特定する方法について説明します。

ステップ 7 ネットワーク内のアプリケーションで SSL ピニングが使用されていることを確認する場合は、TLS/SSL ルールのガイドラインと制限事項（1848 ページ）を参照してください。

次のタスク

TLS/SSL 接続イベントを使用して、次のいずれかが表示されれば、TLS/SSL ピニングの発生を確認できます。

- クライアントがサーバから SERVER_HELLO、SERVER_CERTIFICATE、SERVER_HELLO_DONE メッセージを受信した後に TCP Reset を受信すると、SSL ALERT メッセージを送信するアプリケーションの場合、次のように表示されます。（パケットキャプチャを使用すると、アラート `Unknown CA (48)` が表示される場合があります）。
  - [SSLフローフラグ（SSL Flow Flags）] 列に `ALERT_SEEN` は表示されますが、`APP_DATA_C2S` や `APP_DATA_S2C` は表示されません。
  - 管理対象デバイスでSSLハードウェアアクセラレーションが有効になっている場合、[SSLフローメッセージ（SSL Flow Messages）] 列には通常、`CLIENT_ALERT`、`CLIENT_HELLO`、`SERVER_HELLO`、`SERVER_CERTIFICATE`、`SERVER_KEY_EXCHANGE`、`SERVER_HELLO_DONE` が表示されます。
  - 管理対象デバイスがSSLハードウェアアクセラレーションをサポートしていないか、機能が無効になっている場合は、[SSLフローメッセージ（SSL Flow Messages）] 列に

は通常、CLIENT_HELLO、SERVER_HELLO、SERVER_CERTIFICATE、SERVER_KEY_EXCHANGE、SERVER_HELLO_DONE が表示されます。

- [SSLフローエラー（SSL Flow Error）] 列には、Success が表示されます。

- SSL ハンドシェイク終了後にアラートではなく TCP Reset を送信するアプリケーションの場合は、次のように表示されます。
  - [SSLフローフラグ（SSL Flow Flags）] 列に ALERT_SEEN、APP_DATA_C2S、APP_DATA_S2C は表示されません。
  - 管理対象デバイスでSSLハードウェアアクセラレーションが有効になっている場合、[SSLフローメッセージ（SSL Flow Messages）] 列には通常、CLIENT_HELLO、SERVER_HELLO、SERVER_CERTIFICATE、SERVER_KEY_EXCHANGE、SERVER_HELLO_DONE、CLIENT_KEY_EXCHANGE、CLIENT_CHANGE_CIPHER_SPEC、CLIENT_FINISHED、SERVER_CHANGE_CIPHER_SPEC、SERVER_FINISHED が表示されます。
  - 管理対象デバイスがSSLハードウェアアクセラレーションをサポートしていないか、機能が無効になっている場合は、[SSLフローメッセージ（SSL Flow Messages）] 列には通常、CLIENT_HELLO、SERVER_HELLO、SERVER_CERTIFICATE、SERVER_KEY_EXCHANGE、SERVER_HELLO_DONE、CLIENT_KEY_EXCHANGE、CLIENT_CHANGE_CIPHER_SPEC、CLIENT_FINISHED、SERVER_CHANGE_CIPHER_SPEC、SERVER_FINISHED が表示されます。
  - [SSLフローエラー（SSL Flow Error）] 列には、Success が表示されます。

関連トピック

接続およびセキュリティ インテリジェンス イベント テーブルの使用 （3050 ページ）
接続イベントとセキュリティ インテリジェンス イベントのフィールド （3024 ページ）
接続イベント フィールドで利用可能な情報 （3044 ページ）
イベントの検索 （2967 ページ）

TLS/SSL 暗号スイートの確認

始める前に

このトピックでは、暗号スイートの条件を持つ TLS/SSL ルールを保存する際に次のエラーが表示された場合に実行する必要があるアクションについて説明します。

```
Traffic cannot match this rule; none of your selected cipher suites contain a signature algorithm that the resigning CA's signature algorithm
```

エラーは、TLS/SSL ルールの条件として選択した 1 つ以上の暗号スイーツが TLS/SSL ルールに使用されている証明書と互換性がないことを示します。この問題を解決するには、使用している証明書へのアクセス権が必要です。

（注） このトピックでのタスクには、TLS/SSL 暗号化がどのように機能するかの知識が必要です。

ステップ 1 指定した暗号スイーツで [復号 - 再署名（Decrypt - Resign）] または [復号 - 既知のキー（Known Key）] のいずれかを持つ SSL ルールを保存しようとしたときに次のエラーが表示されます。

例：

```
Traffic cannot match this rule; none of your selected cipher suites contain a
signature algorithm that the resigning CA's signature algorithm
```

ステップ 2 トラフィックの復号に使用している証明書を見つけ、必要に応じて、openssl コマンドを実行できるシステムにその総名所をコピーします。

ステップ 3 次のコマンドを実行し、証明書で使用されている署名アルゴリズムを表示します。

openssl x509 -in *CertificateName* **-text -noout**

出力の最初に次のような数行が表示されます。

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 4105 (0x1009)
    Signature Algorithm: ecdsa-with-SHA256
```

ステップ 4 **Signature algorithm** によって次が通知されます。

- 使用されている暗号化関数（前の例では、**ECDSA** は楕円曲線デジタル署名アルゴリズム（楕円曲線 DSA）を意味します）。
- 暗号化されたメッセージのダイジェストの作成に使用されたハッシュ関数（前の例では **SHA256**）。

ステップ 5 それらの値に一致する暗号スイーツのリソース（OpenSSL at University of Utah など）を検索します。暗号スイートは RFC 形式である必要があります。
また、その他のさまざまなサイト（Mozilla wiki の Server Side TLS や RFC 5246 の Appendix C など）も検索できます。マイクロソフトのドキュメントの Cipher Suites in TLS/SSL（Schannel SSP）[英語] には、暗号スイーツの詳細な説明があります。

ステップ 6 必要に応じて、OpenSSL 名を Firepower Management システムが使用している RFC 名に変換します。`https://testssl.sh` サイトの『RFC mapping list』を参照してください。

ステップ 7 前の例の **ecdsa-with-SHA256** では、Mozilla wiki で『Modern Compatibility List』を参照できます。

a) 名前に **ECDSA** または **SHA-256** を持つ暗号スイートのみを選択します。これらの暗号スイートは次のように動作します。

```
ECDHE-ECDSA-AES128-GCM-SHA256
ECDHE-ECDSA-AES128-SHA256
```

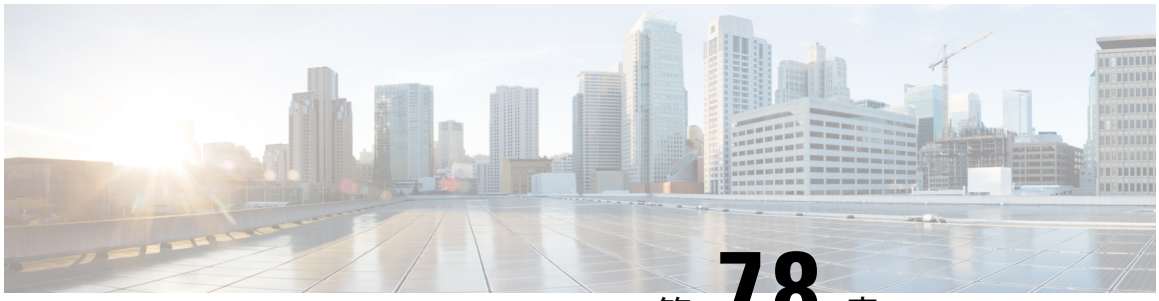
b) 対応する RFC 暗号スイートを RFC マッピング リストで検索します。これらの暗号スイートは次のように動作します。

```
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
```

ステップ 8 前述の暗号スイートを TLS/SSL ルールに追加します。

第 XVIII 部

高度なマルウェア防御（AMP）とファイル制御



第 78 章

ファイル ポリシーと高度なマルウェア防御

次のトピックでは、ファイル制御、ファイル ポリシー、ファイル ルール、AMP クラウド接続、および動的分析接続の概要を示します。

ファイル ポリシーと高度なマルウェア防御について

マルウェアを検出してブロックするには、ファイル ポリシーを使用します。また、ファイル ポリシーを使用して、ファイル タイプごとにトラフィックを検出および制御することもできます。

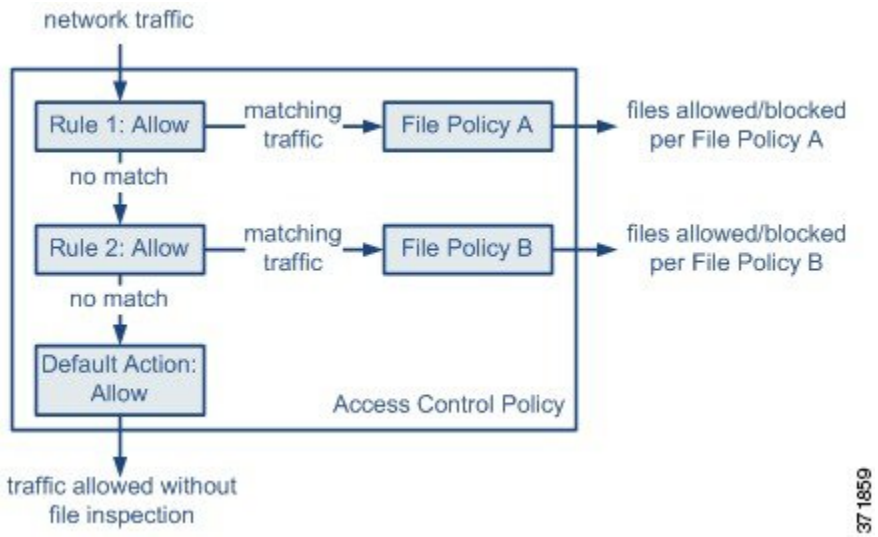
Firepower の高度なマルウェア防御（AMP）は、ネットワーク トラフィックでのマルウェアの伝送を検出、キャプチャ、追跡、分析、ロギング、および必要に応じてブロックできます。Firepower Management Center Web インターフェイスでは、この機能は ネットワーク向け *AMP* と呼ばれ、以前は *AMP for Firepower* とも呼ばれていました。高度なマルウェア防御は、シスコ クラウドからインラインおよび脅威データを展開した管理対象デバイスを使用してマルウェアを特定します。

すべてのアクセス コントロール設定に含まれるネットワーク トラフィックを処理するアクセス コントロール ルールとファイル ポリシーを関連付けます。

システムがネットワーク上のマルウェアを検出すると、ファイルおよびマルウェア イベントを生成します。ファイルおよびマルウェア イベント データを分析するには、ファイル/マルウェア イベントとネットワーク ファイル トラジェクトリ （3115 ページ）を参照してください。

ファイル ポリシー

ファイル ポリシーは、いくつかの設定からなるセットです。システムは全体的なアクセス コントロール設定の一部としてこれを使用して、マルウェア防御とファイル制御を実行できます。この関連付けにより、アクセス コントロール ルールの条件と一致するトラフィック内のファイルを通過させる前に、システムは必ずファイルを検査するようになります。次の図のような、インライン展開での単純なアクセス コントロール ポリシーがあるとします。



このポリシーには 2 つのアクセス コントロール ルールがあり、両方とも許可アクションを使用し、ファイル ポリシーに関連付けられています。このポリシーのデフォルト アクションもまた「トラフィックの許可」ですが、ファイル ポリシー インスペクションはありません。このシナリオでは、トラフィックは次のように処理されます。

- `Rule 1` に一致するトラフィックは`File Policy A` で検査されます。
- `Rule 1` に一致しないトラフィックは`Rule 2` に照らして評価されます。`Rule 2` に一致するトラフィックは`File Policy B` で検査されます。
- どちらのルールにも一致しないトラフィックは許可されます。デフォルト アクションにファイル ポリシーを関連付けることはできません。

1 つのファイル ポリシーを、**許可**、**インタラクティブ ブロック**、または **リセット付きインタラクティブ ブロック** アクションを含むアクセス コントロール ルールに関連付けることができます。その後、システムはそのファイル ポリシーを使用して、アクセス コントロール ルールの条件を満たすネットワーク トラフィックを検査します。

異なるファイル ポリシーを個々のアクセス コントロール ルールに関連付けることにより、ネットワークで伝送されるファイルを識別/ブロックする方法をきめ細かく制御できます。

ファイルおよびマルウェア ポリシーのライセンス要件

操作内容	必要なライセンス	[ファイルルールのアクション（File Rule Action）]
特定のタイプのすべてのファイルをブロックまたは許可します（すべての .exe ファイルをブロックなど）	脅威（FTD デバイスの場合） 保護（従来のデバイスの場合）	許可（Allow）、ブロック（Block）、リセットしてブロック（Block with reset）
マルウェアが含まれているか、または含まれている可能性があると判断した場合に、ファイルを選択的に許可またはブロックします	脅威（FTD デバイスの場合） 保護（従来のデバイスの場合） Malware	マルウェア クラウド ルックアップ（Malware Cloud Lookup）、マルウェア ブロック（Block Malware）
ファイルの保存（Store files）	脅威（FTD デバイスの場合） 保護（従来のデバイスの場合） Malware	[ファイルの保存（Store Files）] で選択されたファイル ルール アクション

マルウェアライセンスの詳細については、次を参照してください。

- Firepower Threat Defense デバイスのマルウェア ライセンス （105 ページ）
- 従来のデバイスのマルウェア ライセンス （147 ページ）

マルウェア防御のベストプラクティス

- マルウェア防御の設定方法 （1914 ページ）およびそのサブトピックの手順に従います。
- 手順の前提条件を必ず満たしてください。
- ファイル ポリシーとファイル ルールの注意事項と制限事項 （1929 ページ）も参照してください。

マルウェア防御の設定方法

ここでは、悪意のあるソフトウェアからネットワークを保護するために Firepower システムの設定で実行する必要がある手順を説明します。

ステップ 1 マルウェア防御の計画と準備 （1914 ページ）

ステップ 2 ファイル ポリシーの設定 （1915 ページ）

ステップ 3 アクセス コントロール設定へのファイル ポリシーの追加 （1916 ページ）

ステップ 4 ネットワーク検出ポリシーを設定して、ファイルとマルウェア イベントをネットワーク上のホストと関連付けます。

（ネットワーク検出をオンにするだけでなく、ネットワーク上のホストを検出して組織のネットワーク マップを構築するように設定する必要があります。）

ネットワーク検出ポリシー （2647 ページ）およびサブトピックを参照してください。

ステップ 5 管理対象デバイスにポリシーを展開します。

設定変更の展開 （447 ページ）を参照してください。

ステップ 6 予想したとおりに悪意のあるファイルを処理していることを確認するためにシステムをテストします。

ステップ 7 マルウェア防御のメンテナンスとモニタリングの設定 （1917 ページ）

次のタスク

- （オプション）ネットワーク内のマルウェアの検出をさらに強化するには、シスコの AMP for Endpoints 製品を導入して統合します。（オプション）AMP for Endpoints を使用したマルウェア防御 （1953 ページ）およびサブトピックを参照してください。
- ファイルおよびマルウェア イベントを調査する方法を理解します。

  ファイル/マルウェア イベントとネットワーク ファイル トラジェクトリ （3115 ページ）を参照してください。

マルウェア防御の計画と準備

この手順は、マルウェアを防御するようにシステムを設定するための完全なプロセスの最初の手順です。

ステップ 1 ライセンスを購入してインストールします。

ファイルおよびマルウェア ポリシーのライセンス要件 （1913 ページ）およびFirepower システムのライセンス （93 ページ）を参照してください。

ステップ 2 ファイル ポリシーおよびマルウェア防御がアクセス コントロール プランにどのように適合するかを理解します。

侵入ポリシーとファイル ポリシーを使用したアクセス制御 （1707 ページ）の章を参照してください。

ステップ 3 ファイル分析およびマルウェア防御ツールについて理解します。

ファイル ルール アクション （1942 ページ）およびサブトピックを参照してください。

また、 詳細オプションおよびアーカイブ ファイル検査オプション （1933 ページ）も考慮してください。

ステップ 4 マルウェア防御（ファイル分析と動的分析）にパブリック クラウドまたはプライベート（オンプレミス）クラウドを使用するかどうかを決定します。

マルウェア防御のためのクラウド接続 （1917 ページ）およびサブトピックを参照してください。

ステップ 5 マルウェア防御にプライベート（オンプレミス）クラウドを使用する場合は、これらの製品を購入、展開、テストします。

詳細については、シスコのセールス担当者または認定リセラーにお問い合わせください。

ステップ 6 選択したクラウドとの通信を許可するようにファイアウォールを設定します。

セキュリティ、インターネット アクセス、および通信ポート （3281 ページ）を参照してください。

ステップ 7 Firepower およびマルウェア防御クラウド（パブリックまたはプライベート）間の接続を設定します。

- AMP クラウドについては、AMP オプションの変更 （1924 ページ）を参照してください。
- オンプレミスの Cisco Threat Grid アプライアンスを展開した場合は、オンプレミスの動的分析アプライアンスへの接続 （1926 ページ）を参照してください。（パブリック Threat Grid クラウドへのアクセスに設定は必要ありません。）

次のタスク

マルウェア防御ワークフローの次の手順に進みます。

マルウェア防御の設定方法 （1914 ページ）を参照してください。

ファイル ポリシーの設定

始める前に

マルウェア防御ワークフローで、この時点までのタスクを実行します。

マルウェア防御の設定方法 （1914 ページ）を参照してください。

ステップ 1 ファイル ポリシーおよびファイル ルールの制限事項を確認します。

ファイル ポリシーとファイル ルールの注意事項と制限事項（1929ページ）およびサブトピックを参照してください。

ステップ 2 ファイル ポリシーを作成します。

ファイル ポリシーの作成 （1932 ページ）を参照してください。

ステップ 3 ファイル ポリシー内にルールを作成します。

ファイル ルール （1939 ページ）およびサブトピックを参照してください。

ステップ 4 詳細オプションを設定します。

詳細オプションおよびアーカイブ ファイル検査オプション （1933 ページ）を参照してください。

次のタスク

マルウェア防御ワークフローの次の手順に進みます。

マルウェア防御の設定方法 （1914 ページ）を参照してください。

アクセス コントロール設定へのファイル ポリシーの追加

始める前に

マルウェア防御ワークフローで、この時点までのタスクを実行します。

マルウェア防御の設定方法 （1914 ページ）を参照してください。

ステップ 1 アクセス コントロール ポリシーでファイル ポリシーのガイドラインを確認します。（これらは以前に確認したファイル ルールおよびファイル ポリシーのガイドラインとは異なります。）

ファイル インスペクションおよび侵入インスペクションの順序 （1710 ページ）を確認してください。

ステップ 2 アクセス コントロール ポリシーとファイル ポリシーを関連付けます。

マルウェア保護のためのアクセス コントロール ルールの設定 （1712 ページ）を参照してください

ステップ 3 管理対象デバイスにアクセス コントロール ポリシーを割り当てます。

アクセス コントロール ポリシーのターゲット デバイスの設定 （1680 ページ）を参照してください。

次のタスク

マルウェア防御ワークフローの次の手順に進みます。

マルウェア防御の設定方法 （1914 ページ）を参照してください。

マルウェア防御のメンテナンスとモニタリングの設定

ネットワークの保護には継続的なメンテナンスが必要不可欠です。

始める前に

マルウェアからネットワークを保護するようにシステムを設定します。

マルウェア防御の設定方法 （1914 ページ）および参照手順を確認してください。

ステップ 1 システムが常に最新かつ効果的に保護されていることを確認します。

システムの保守：動的分析の対象となるファイル タイプの更新 （1928 ページ）を参照してください。

ステップ 2 マルウェア関連のイベントおよびヘルス モニタリングのアラートを設定します。

次のモジュールについては、ヘルス モニタリング （349 ページ）のネットワーク向け AMP アラートの設定（2815 ページ）を参照してください。

- ローカル マルウェア分析（Local Malware Analysis）
- Security Intelligence
- デバイスでの脅威データの更新
- 侵入およびファイル イベント レート
- AMP for Firepower のステータス
- AMP for Endpoint のステータス

次のタスク

マルウェア防御ワークフローの「次の項目について」を確認してください。

マルウェア防御の設定方法 （1914 ページ）を参照してください。

マルウェア防御のためのクラウド接続

マルウェアからネットワークを保護するためには、パブリック クラウドまたはプライベート クラウドに接続する必要があります。

AMP クラウド

高度なマルウェア防御（AMP）クラウドは、ビッグ データ分析や連続分析によりネットワーク上のマルウェアを検出およびブロックするシスコ ホステッド サーバです。

AMP クラウドは、管理対象デバイスがネットワーク トラフィックから検出した潜在的なマルウェアの性質と、ローカルマルウェア分析とファイルの事前分類のデータ更新を提供します。

組織で AMP for Endpoints を展開し、データをインポートするように Firepower を設定している場合、システムは、スキャン レコード、マルウェア検出、隔離、侵害の兆候（IOC）など、AMP クラウドからこのデータをインポートします。

シスコでは、既知のマルウェアの脅威についてシスコ クラウドからデータを取得するために次のオプションを提供しています。

- **AMP パブリック クラウド**

  Firepower Management Center がパブリック シスコ クラウドと直接通信します。米国、欧州、アジアに 3 つのパブリック AMP クラウドがあります。

- **AMP プライベート クラウド**

  ネットワーク上に展開された AMP プライベート クラウドは、圧縮型、オンプレミス AMP クラウドおよびパブリック AMP クラウドに接続するための匿名プロキシとして機能します。詳細は、Cisco AMP プライベート クラウド （1921 ページ）を参照してください。

  AMP for Endpoints と統合する場合、AMP プライベート クラウドにはいくつかの制限があります。AMP for Endpoints と AMP プライベート クラウド（1956 ページ）を参照してください。

動的分析クラウド

- **Cisco Threat Grid クラウド**

  動的分析の送信に適したファイルを処理し、脅威スコアと動的分析レポートを提供するパブリック クラウド。

- **オンプレミス Cisco Threat Grid アプライアンス**

  組織のセキュリティ ポリシーが Firepower システムによるネットワーク外部へのファイルの送信を許可しない場合は、オンプレミス アプライアンスを設定できます。このアプライアンスはパブリック Cisco Threat Grid クラウドには接続しません。

  詳細については、オンプレミス アプライアンスの動的分析（Cisco Threat Grid） （1925 ページ）を参照してください。

AMP および Threat Grid クラウドへの接続の設定

- AMP クラウド接続の設定 （1918 ページ）
- 動的分析接続 （1925 ページ）

AMP クラウド接続の設定

次のトピックでは、さまざまなシナリオでの AMP クラウド接続の設定について説明します。

- AMP クラウドの選択 （1920 ページ）
- AMP プライベート クラウドへの接続 （1921 ページ）
- Firepower と AMP for Endpoints の統合 （1956 ページ）

次のトピックも関連しています。

- Cisco AMP プライベート クラウド （1921 ページ）
- AMP クラウド接続の要件とガイドライン （1919 ページ）
- AMP クラウドへの接続の管理（パブリックまたはプライベート） （1923 ページ）

AMP クラウド接続の要件とガイドライン

AMP クラウド接続要件

FMC が AMP クラウドと通信できるようにするには、セキュリティ、インターネット アクセス、および通信ポート （3281 ページ）のトピックを参照してください。

AMP の通信にレガシー ポートを使用するには通信ポートの要件 （3284 ページ） を参照してください。

AMP とハイ アベイラビリティ

ハイ アベイラビリティ ペアの Firepower Management Center はファイル ポリシーおよび関連する設定を共有しますが、クラウド接続、キャプチャされたファイル、ファイルイベント、マルウェアイベントを共有することはありません。運用の継続性を確保し、検出されたファイルのマルウェア処理が両方の Firepower Management Center で同じであるようにするためには、アクティブとスタンバイ両方の Firepower Management Center がクラウドにアクセスできる必要があります。

ハイ アベイラビリティの設定では、Firepower Management Center のアクティブ インスタンスとスタンバイ インスタンスで AMP クラウド接続を個別に設定する必要があります。これらの設定は同期されません。

これらの要件は、パブリック、プライベート両方の AMP クラウドに適用されます。

AMP クラウド接続とマルチテナンシー

マルチドメイン展開では、ネットワーク向け AMP 接続はグローバル レベルでのみ設定します。各 Firepower Management Center には、ネットワーク向け AMP 接続を 1 つだけ設定できます。

AMP クラウドの選択

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス（Access）
マルウェア	マルウェア	いずれか（Any）	いずれか（Any）	Admin

Firepower システムでは、デフォルトで米国（US）AMP パブリック クラウドへの接続が設定され、有効になっています。（この接続は web インターフェイスに ネットワーク向け AMP と表示されますが、AMP for Firepower と表示される場合もあります。）ネットワーク向け AMP クラウド接続の削除または無効化はできませんが、地理的に異なる AMP クラウドの切り替え、または AMP プライベート クラウドの接続が設定が可能です。

始める前に

- AMP プライベート クラウドを使用する場合は、このトピックの代わりにAMP プライベート クラウドへの接続 （1921 ページ）を参照してください。
- Firepower が AMP for Endpoints と統合されていない場合は、AMP クラウド接続を 1 つだけ設定できます。この接続には、**AMP for Networks** または **AMP for Firepower** というラベルが付けられています。
- AMP for Endpoints を展開し、このアプリケーションを Firepower と統合するために 1 つ以上の AMP クラウドを追加する場合は、Firepower と AMP for Endpoints の統合 （1956 ページ）を参照してください。
- AMP クラウド接続の要件とガイドライン （1919 ページ）を参照してください。

ステップ 1 **[AMP]** > **[AMP Management]**を選択します。

ステップ 2 鉛筆アイコンをクリックし、既存のクラウド接続を編集します。

ステップ 3 [クラウド名（Cloud Name）] ドロップダウン リストから、Firepower Management Center から最も近い地域にあるクラウドを選択します。

APJC はアジア/太平洋/日本/中国です。

ステップ 4 [保存（Save）] をクリックします。

次のタスク

- 展開がハイ アベイラビリティ構成の場合は、AMP クラウド接続の要件とガイドライン （1919 ページ）を参照してください。
- （任意）AMP オプションの変更 （1924 ページ）。

Cisco AMP プライベート クラウド

Firepower Management Center は AMP クラウドに接続し、ネットワーク トラフィックで検出されたファイルの判定結果をクエリしたり、レトロスペクティブ マルウェア イベントを受信したりします。このクラウドはパブリックまたはプライベートに指定することができます。

部門のプライバシーやセキュリティ保護の観点から、モニタ対象ネットワークと AMP クラウドとの間で頻繁にあるいは直接接続することが困難、または不可能な場合があります。このような場合、AMP クラウドの圧縮型、オンプレミス バージョンとして機能するシスコ独自の製品、ユーザのネットワークと AMP クラウドの安全なメディエータである、Cisco AMP プライベート クラウドを設定できます。Firepower Management Center を AMP プライベート クラウドに接続すると、パブリック AMP クラウドとの既存の直接接続は無効化されます。

AMP プライベート クラウドを介した AMP クラウド ファネルとのすべての接続は、監視対象ネットワークのセキュリティとプライバシーを確保するための匿名プロキシとして機能します。これには、ネットワーク トラフィックで検出されたファイルの判定結果のクエリ、レトロスペクティブ マルウェア イベントの受信などが含まれます。AMP プライベート クラウドは、エンドポイント データを外部接続では一切共有しません。

（注） AMP プライベート クラウドは動的分析を実行**しません**。また、Cisco Collective Security Intelligence（CSI）に依存するその他の機能（URL フィルタリングやセキュリティ インテリジェンス フィルタリングなど）のための脅威インテリジェンスの匿名での取得もサポートしていません。

AMP プライベート クラウド（「AMPv」とも呼ばれる）の詳細については、https://www.cisco.com/c/en/us/products/security/fireamp-private-cloud-virtual-appliance/index.html を参照してください。

AMP プライベート クラウドへの接続

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス（Access）
マルウェア（ネットワーク向け AMP） 任意（AMP for Endpoints）	マルウェア（ネットワーク向け AMP） 任意（AMP for Endpoints）	いずれか（Any）	いずれか（Any）	Admin

始める前に

- AMP のマニュアルの指示に従って、Cisco AMP プライベート クラウドまたはクラウドを設定します。設定時に、プライベート クラウドのホスト名をメモしてください。このホスト名は、Firepower Management Center で接続を設定するときに必要になります。
- Firepower Management Center が AMP プライベート クラウドと通信できることを確認し、プライベート クラウドがインターネットにアクセスし、パブリック AMP クラウドと通信

できることを確認します。セキュリティ、インターネット アクセス、および通信ポート（3281 ページ）のトピックを参照してください。

- 展開で AMP for Endpoints と統合されていない場合は、Firepower Management Center ごとに AMP クラウド接続を 1 つだけ設定できます。この接続には、**AMP for Networks** または **AMP for Firepower** というラベルが付けられています。

  AMP for Endpoints と統合する場合は、複数の AMP for Endpoints クラウド接続を設定できます。

ステップ 1 **[AMP]** > **[AMP Management]**を選択します。

ステップ 2 [AMP クラウド接続の作成（Create AMP Cloud Connection）] をクリックします。

ステップ 3 [クラウド名（Cloud Name] ドロップダウン リストから [プライベート クラウド（Private Cloud）] を選択します。

ステップ 4 名前を入力します。

この情報は、AMP プライベート クラウドによって生成または送信されるマルウェア イベントに表示されます。

ステップ 5 [ホスト（Host）] フィールドに、プライベート クラウドの設定時に設定したプライベート クラウドのホスト名を入力します。

ステップ 6 [証明書アップロードパス（Certificate Upload Path）] フィールドの横にある [参照（Browse）] をクリックして、プライベート クラウドの有効な TLS または SSL 暗号化証明書の場所を参照します。詳細については、AMP プライベート クラウドのマニュアルを参照してください。

ステップ 7 このプライベート クラウドを ネットワーク向け AMP と AMP for Endpoints の両方に使用する場合は、[AMP for Firepowerに使用（Use for AMP for Firepower）] チェックボックスをオンにします。

ネットワーク向け AMP 通信を処理する別のプライベート クラウドを設定した場合は、このチェックボックスをオフにすることができます。これが唯一の AMP プライベート クラウド接続の場合は、オフにできません。

マルチドメイン展開では、このチェックボックスはグローバル ドメインにのみ表示されます。各 Firepower Management Center には、ネットワーク向け AMP 接続を 1 つだけ設定できます。

ステップ 8 プロキシを使用して AMP プライベート クラウドと通信するには、[接続にプロキシを使用（Use Proxy for Connection）] チェックボックスをオンにします。

ステップ 9 [登録（Register）] をクリックし、AMP クラウドへの既存の直接接続を無効にすることを確認し、最後に AMP プライベート クラウド管理コンソールを続行して登録を完了することを確認します。

ステップ 10 管理コンソールにログインして登録プロセスを完了します。詳細については、AMP プライベート クラウドのマニュアルを参照してください。

次のタスク

ハイ アベイラビリティの設定では、Firepower Management Center のアクティブ インスタンスとスタンバイ インスタンスで AMP クラウド接続を個別に設定する必要があります。これらの設定は同期されません。

AMP クラウドへの接続の管理（パブリックまたはプライベート）

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス（Access）
マルウェア（ネットワーク向け AMP ） 任意（AMP for Endpoints）	マルウェア（ネットワーク向け AMP ） 任意（AMP for Endpoints）	いずれか（Any）	いずれか（Any）	Admin

Firepower Management Center を使用して、ネットワーク向け AMP や AMP for Endpoints またはその両方に使用されるパブリックおよびプライベート AMP クラウドへの接続を管理します。

クラウドからマルウェア関連の情報を受信する必要がなくなった場合は、パブリックまたはプライベート AMP クラウドとの接続を削除します。AMP for Endpoints または AMP プライベート クラウド管理コンソールを使用して接続の登録を解除しても、システムから接続を削除することにはならない点に注意してください。登録解除した接続は、Firepower Management Center の Web インターフェイスに障害発生状態で表されます。

また、接続は一時的に無効にすることもできます。クラウド接続を再度有効化すると、クラウドは、無効化されていた期間にキューに保持していたデータを含めて、システムへのデータ送信を再開します。

⚠

注意 無効化された接続の場合、プライベート AMP クラウドは、接続を再有効化するまでマルウェア イベントや侵害の兆候などを保存できます。まれに、イベント レートが非常に高い場合や接続が長期間無効になっていた場合など、接続無効中に生成されたすべての情報をクラウドで保存できないことがあります。

マルチドメイン展開では、現在のドメインで作成された接続が表示されます。これは、管理が可能な接続です。また、先祖ドメインで作成した接続も表示されますが、この接続は管理できません。下位ドメインの接続を管理するには、そのドメインに切り替えます。各 Firepower Management Center は、グローバル ドメインに属する ネットワーク向け AMP 接続を 1 つのみ保持できます。

ステップ 1 **[AMP]** > **[AMP Management]** を選択します。

ステップ 2 AMP クラウド接続を管理します。

- 削除：削除アイコン（🗑）をクリックして、選択内容を確認します。

• 有効化または無効化：スライダをクリックして、選択内容を確認します。

次のタスク

ハイ アベイラビリティの設定では、Firepower Management Center のアクティブ インスタンスとスタンバイ インスタンスで AMP クラウド接続を個別に設定する必要があります。これらの設定は同期されません。

AMP オプションの変更

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス（Access）
マルウェア	マルウェア	いずれか（Any）	いずれか（Any）	Admin

ステップ 1 **[System]** > **[Integration]**を選択します。

ステップ 2 [**[Cloud Services]**] タブをクリックします。

ステップ 3 次のオプションを選択します。

表 *117 : AMP for Networks* のオプション

オプション	説明
ローカル マルウェア検出の自動更新を有効にする（Enable Automatic Local Malware Detection Updates）	ローカル マルウェア検出エンジンは、Cisco が提供する署名を使用して統計的にファイルを分析し、事前に分類します。このオプションを有効にすると、Firepower Management Center が 30 分ごとに署名の更新を確認します。
マルウェア イベントの URL を Cisco と共有する（Share URI from Malware Events with Cisco）	ネットワーク トラフィックで検出されたファイルに関する情報を AMP クラウドに送信することができます。この情報には、検出されたファイルに関連する URI 情報と SHA-256 ハッシュ値が含まれます。共有はオプトインですが、この情報を Cisco に送信すると、マルウェアを識別して追跡する今後の取り組みに役立ちます。
レガシー ポート 32137 を ネットワーク向け AMP に使用する（Use Legacy Port 32137 for AMP for Networks）	デフォルトでは、Firepower はポート 443/HTTPS を使用して AMP パブリック クラウドまたはプライベート クラウドと通信し、ファイルの性質データを取得します。このオプションは、システムによるポート 32137 の使用を許可します。 システムを以前のバージョンから更新する場合は、このオプションを有効にすることができます。 FMC がプロキシ設定で設定されている場合、このオプションはグレー表示されます。

ステップ 4 **[保存（Save）]** をクリックします。

動的分析接続

動的分析の要件

適切なライセンスを使用すると、Firepower システムが Cisco Threat Grid パブリック クラウドに自動的にアクセスします。

動的分析では、管理対象デバイスがポート 443 から Cisco Threat Grid パブリック クラウドまたはオンプレミス Cisco Threat Grid アプライアンスに、直接あるいはプロキシを介してアクセスできる必要があります。

動的分析の対象となるファイル （1948 ページ）も参照してください。

オンプレミス Threat Grid アプライアンスに接続する場合は、オンプレミスの動的分析アプライアンスへの接続 （1926 ページ）の前提条件も参照してください。

デフォルトの動的分析接続の表示

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス（Access）
マルウェア	マルウェア	いずれか（Any）	グローバルだけ	Admin/Access Admin/Network Admin

デフォルトで、Firepower Management Center は、ファイルを送信したり、レポートを取得したりするために、パブリック Cisco Threat Grid クラウドに接続できます。この接続は、設定したり、削除したりすることはできません。

ステップ 1 **[AMP]** > **[Dynamic Analysis Connections]**を選択します。

ステップ 2 編集アイコン（）をクリックします。

（注） **[AMP]** > **[ダイナミック分析接続（Dynamic Analysis Connections）]** ページの ボタンの詳細については、パブリック クラウドでの動的分析の結果へのアクセスの有効化 （1927ページ）を参照してください。

オンプレミス アプライアンスの動的分析（Cisco Threat Grid）

組織にパブリックの Cisco Threat Grid クラウドへのファイルの送信に関してプライバシーまたはセキュリティ上の懸念がある場合、オンプレミスの Cisco Threat Grid アプライアンスを展開することができます。このオンプレミス アプライアンスは、パブリック クラウドと同様に適

格なファイルをサンドボックス環境で実行し、脅威スコアと動的分析レポートを Firepower システムに返します。ただし、このオンプレミスアプライアンスは、ご使用のネットワークの外部にあるパブリック クラウドや他のすべてのシステムとは通信しません。

オンプレミス Cisco Threat Grid アプライアンスの詳細については、https://www.cisco.com/c/en/us/products/security/threat-grid/index.htmlを参照してください。

オンプレミスの動的分析アプライアンスへの接続

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス（Access）
マルウェア	マルウェア	いずれか（Any）	グローバルだけ	Admin/Access Admin/Network Admin

ネットワークでオンプレミスの Cisco Threat Grid アプライアンスをインストールする場合は、動的分析接続を設定して、ファイルを送信し、アプライアンスからレポートを取得できます。オンプレミスのアプライアンスの動的分析接続を設定するには、オンプレミスのアプライアンスに Firepower Management Center を登録します。

始める前に

- オンプレミスの Cisco Threat Grid アプライアンスを設定します。『*Cisco Threat Grid Appliance Setup and Configuration Guide*』を参照してください。

  このアプライアンスのドキュメントは、https://www.cisco.com/c/en/us/support/security/amp-threat-grid-appliances/tsd-products-support-series-home.html から入手できます。

  バージョンの要件については、Firepower バージョンのリリース ノートを参照してください。

- ログインに使用する公開キー証明書を Cisco Threat Grid アプライアンスからオンプレミスのアプライアンスにダウンロードします。『*Cisco Threat Grid Appliance Administrator's Guide*』を参照してください。

- プロキシを使用してオンプレミスのアプライアンスに接続する場合は、プロキシを設定します。Firepower Management Center 管理インターフェイスの設定 （1273 ページ）を参照してください。

- 管理対象デバイスは、ポート 443 で Cisco Threat Grid アプライアンスへの直接またはプロキシを介したアクセスが必要です。

ステップ 1 **[AMP]** > **[Dynamic Analysis Connections]**を選択します。

ステップ 2 [新しい接続を追加（Add New Connection）] をクリックします。

ステップ 3 名前を入力します。

ステップ 4 [ホスト URL（Host URL）] を入力します。

ステップ 5 [証明書のアップロード（Certificate Upload）] の横にある [参照（Browse）] をクリックして、オンプレミスのアプライアンスとの接続を確立するために使用する公開キー証明書をアップロードします。

ステップ 6 設定されているプロキシを使用して接続を確立する場合は、[可能な場合はプロキシを使用（Use Proxy When Available）] を選択します。

ステップ 7 [登録（Register）] をクリックします。

ステップ 8 [はい（Yes）] をクリックして、オンプレミスの Cisco Threat Grid アプライアンスのログイン ページを表示します。

ステップ 9 オンプレミスの Cisco Threat Grid アプライアンスにユーザ名とパスワードを入力します。

ステップ 10 [サインイン（Sign in）] をクリックします。

ステップ 11 次の選択肢があります。

- 以前にオンプレミスのアプライアンスに Firepower Management Center を登録した場合は、[戻る（Return）] をクリックします。
- Firepower Management Center を登録していない場合は、[アクティブ化（Activate）] をクリックします。

パブリック クラウドでの動的分析の結果へのアクセスの有効化

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス（Access）
マルウェア	マルウェア	いずれか（Any）	グローバルだけ	Admin/Access Admin/Network Admin

Cisco Threat Grid 分析されたファイルに関して、Firepower Management Center で使用できるレポートよりもさらに詳細なレポートが提供されます。組織に Cisco Threat Grid パブリック クラウドのアカウントがあれば、Cisco Threat Grid ポータルに直接アクセスして、管理対象デバイスから分析のために送信されたファイルに関する追加の詳細を表示することができます。ただし、プライバシー上の理由から、ファイル分析の詳細は、そのファイルを提出した組織だけが使用できます。そのため、この情報を表示するためには、Firepower Management Center を、管理対象デバイスによって提出されたファイルと関連付ける必要があります。

始める前に

Cisco Threat Grid パブリック クラウドにアカウントがあること、およびアカウントのクレデンシャルを持っている必要があります。

ステップ 1 [AMP] > [ダイナミック分析接続（Dynamic Analysis Connections）] を選択します。

ステップ 2 Cisco Threat Grid パブリック クラウドに対応するテーブル行で、をクリックします。

Cisco Threat Grid ポータル ウィンドウが開きます。

ステップ 3 Cisco Threat Grid パブリック クラウドにサインインします。

ステップ 4 [クエリの送信（Submit Query）] をクリックします。

（注） [デバイス（Devices）] フィールドのデフォルト値を変更しないでください。

このプロセスで問題が発生した場合は、Cisco Threat Grid 担当者にお問い合わせください。

この変更が有効になるまでに最大で 24 時間かかることがあります。

次のタスク

関連付けが有効化された後、Cisco Threat Grid パブリック クラウドの動的分析結果の表示 （3141 ページ）を参照してください。

システムの保守：動的分析の対象となるファイル タイプの更新

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	グローバルだけ。	Admin

動的分析の対象となるファイル タイプのリストは、定期的に更新される（多くても 1 日 1 回）脆弱性データベース（VDB）によって決定されます。

システムに現在のリストがあることを次のように確認します。

ステップ 1 次のいずれかを実行します。

- （推奨）参照します 脆弱性データベースの更新の自動化 （252 ページ）
- 新しい VDB の更新を定期的に確認し、必要に応じて脆弱性データベース（VDB）の手動による更新（181 ページ）を確認します。

  このオプションを選択した場合は、定期的な通知をスケジュールすることをお勧めします。

ステップ 2 ファイル ポリシーで [動的分析可能（Dynamic Analysis Capable）] ファイル タイプ カテゴリではなく個々のファイル タイプを指定する場合は、ファイル ポリシーを更新して新しくサポートされるファイル タイプを使用します。

ステップ 3 対応するファイル タイプのリストが変更されている場合は、管理対象デバイスに展開します。

シスコ クラウド

FMC は次の機能でシスコ クラウドのリソースと通信します。

- 高度なマルウェア防御

パブリック クラウドはデフォルトで設定されています。変更を加えるには、AMP オプションの変更 （1924 ページ）を参照してください。

- **URL フィルタリング**

  詳細については、次を参照してください。

  - URL フィルタリング オプション （1725 ページ）
  - カテゴリとレピュテーションを使用した URL フィルタリングの有効化 （1724 ページ）

- **統合 Cisco Threat Response**

  詳細については、によるイベントの分析 Cisco Threat Response （2881 ページ）を参照してください。

ファイル ポリシーとファイル ルール

ファイル ポリシーとファイル ルールの注意事項と制限事項

ファイル ルール設定の注意事項と制限事項

- パッシブ展開でファイルをブロックするよう設定されたルールは、一致するファイルをブロックしません。接続ではファイル伝送が続行されるため、接続の開始をログに記録するルールを設定した場合、この接続に関して複数のイベントが記録されることがあります。
- ポリシーには複数のルールを含めることができます。ルールを作成する場合、このルールが以前のルールよりも「優先されている」ことを確認します。
- 動的分析でサポートされているファイル タイプは、他のタイプの分析でサポートされているファイル タイプのサブセットです。各分析タイプでサポートされているファイル タイプを表示するには、ファイル ルール設定ページに移動し、[マルウェアブロック（Block Malware）] アクションを選択して、対象のチェックボックスをオンにします。

  システムがすべてのファイル タイプを検査するには、動的分析と他の分析タイプで個別のルール（同じポリシー内）を作成します。
- [マルウェア クラウドルックアップ（Malware Cloud Lookup）] アクションまたは [マルウェア ブロック（Block Malware）] アクションを使ってファイル ルールが設定されている場合、Firepower Management Center が AMP クラウドとの接続を確立できないと、接続が復元されるまで、システムは設定済みルール アクション オプションを実行できません。
- シスコでは、[ファイルブロック（Block Files）] アクションと [マルウェア ブロック（Block Malware）] アクションで [接続のリセット（Reset Connection）] を有効にすることを推奨しています。これにより、ブロックされたアプリケーション セッションが TCP 接続リセットまで開いたままになることを防止できます。接続をリセットしない場合、TCP 接続が自身をリセットするまで、クライアント セッションが開いたままになります。

- 大量のトラフィックをモニタしている場合、キャプチャしたすべてのファイルを保存したり、動的分析用に送信したり**しないでください**。そのようにすると、システムパフォーマンスに悪影響が及ぶことがあります。
- システムで検出されるすべてのファイルタイプに対してマルウェア分析を実行できるわけではありません。[アプリケーション プロトコル（Application Protocol）]、[転送の方向（Direction of Transfer）]、および [アクション（Action）] ドロップダウン リストで値を選択すると、システムはファイル タイプのリストを限定します。

ファイル検出に関する注意事項と制約事項

- アダプティブ プロファイリングが有効でなければ、アクセス コントロール ルールは、AMP を含め、ファイルの制御を実行できません。
- ファイルがアプリケーション プロトコル条件を持つルールに一致する場合、ファイル イベントの生成は、システムがファイルのアプリケーションプロトコルを正常に識別した後に行われます。識別されていないファイルは、ファイル イベントを生成しません。
- FTP は、さまざまなチャネルを介してコマンドおよびデータを転送します。パッシブまたはインライン タップ モードの展開では、FTP データ セッションとその制御セッションからのトラフィックは同じ内部リソースに負荷分散されない場合があります。
- POP3、POP、SMTP、または IMAP セッションでのすべてのファイル名の合計バイト数が 1024 を超えると、セッションのファイル イベントでは、ファイル名バッファがいっぱいになった後で検出されたファイルの名前が正しく反映されないことがあります。
- SMTP 経由でテキストベースのファイルを送信すると、一部のメール クライアントは改行を CRLF 改行文字標準に変換します。MAC ベースのホストはキャリッジ リターン（CR）文字を使用し、UNIX/Linux ベースのホストはライン フィード（LF）文字を使用するので、メール クライアントによる改行変換によってファイルのサイズが変更される場合があります。一部のメール クライアントは、認識できないファイル タイプを処理する際に改行変換を行うようデフォルト設定されていることに注意してください。
- ISO ファイルを検出するには、ファイルおよびマルウェアのインスペクション パフォーマンスとストレージのオプション（1961 ページ） の説明のように、[ファイルタイプを検知する前に検閲するバイト数制限（Limit the number of bytes inspected when doing file type detection）] オプションを 36870 を超える値に設定します。

ファイル ブロックに関する注意事項と制約事項

- ファイルの終わりを示す End of File マーカーが検出されない場合、転送プロトコルとは無関係に、そのファイルは**マルウェア ブロック** ルールでもカスタム検出リストでもブロックされません。システムは、End of File マーカーで示されるファイル全体の受信が完了するまでファイルのブロックを待機し、このマーカーが検出された後にファイルをブロックします。

- FTP ファイル転送で End of File マーカーが最終データ セグメントとは別に伝送される場合、マーカーがブロックされ、ファイル転送失敗が FTP クライアントに表示されますが、実際にはそのファイルは完全にディスクに転送されます。
- [ファイル ブロック（Block Files）] アクションおよび [マルウェア ブロック（Block Malware）] アクションを持つファイル ルールでは、最初のファイル転送試行後 24 時間で検出される、同じファイル、URL、サーバ、クライアントアプリケーションを使った新しいセッションをブロックすることにより、HTTP 経由のファイル ダウンロードの自動再開をブロックします。
- まれに、HTTP アップロードセッションからのトラフィックが不適切である場合、システムはトラフィックを正しく再構築できなくなり、トラフィックのブロックやファイルイベントの生成を行いません。
- **ファイル ブロック** ルールでブロックされる NetBios-ssn 経由ファイル転送（SMB ファイル転送など）の場合、宛先ホストでファイルが見つかることがあります。ただし、ダウンロード開始後にファイルがブロックされ、結果としてファイル転送が不完全になるため、そのファイルは使用できません。
- （SMB ファイル転送などの）NetBIOS-ssn 経由で転送されたファイルを検出またはブロックするファイル ルールを作成した場合、進行中のファイル転送はシステムにより検査されません。ただし、ファイル ポリシーを呼び出すアクセス コントロール ポリシーを展開した後に、転送された新しいファイルがシステムにより検査されます。
- SMB には、同じ IP アドレスと異なるポートを持つ複数のパラレル セッションを作成する、マルチチャネルと呼ばれる機能があります。マルチチャネルを使用するトランザクションでは、ファイルのダウンロードはこれらのセッションにわたって多重化され、システムにより単一のファイルとして検査されません。
- 1 つの TCP または SMB セッションで同時に転送されたファイルは検査されません。
- クラスタ環境では、クラスタ ロールの変更またはデバイス障害が原因で既存の SMB セッションが新しいデバイスに移動されると、進行中のファイル転送のファイルが検査されないことがあります。
- Microsoft Windows システム間での一部の SMB ファイル転送では、迅速なファイル転送のため、非常に大きな TCP ウィンドウ サイズを使用します。このようなファイル転送を検出またはブロックするには、[ネットワーク分析ポリシー（Network Analysis Policy）] の [TCP ストリームの設定（TCP Stream Configuration）] タブの [トラブルシューティング オプション（Troubleshooting Options）] にある [最大キューイング バイト（Maximum Queued Bytes）] と [最大キューイング セグメント（Maximum Queued Segments）] の値を大きくすることを推奨します。
- Firepower Threat Defense のハイ アベイラビリティを設定したときに、元のアクティブなデバイスがファイルを識別している間にフェイル オーバーが発生した場合、ファイル タイプは同期されません。ファイル ポリシーでそのファイル タイプがブロックされている場合でも、新しいアクティブ デバイスはファイルをダウンロードします。

ファイル ポリシーの一般的な注意事項と制限事項

- ただし、アクセス コントロールのデフォルト アクションによって処理されるトラフィックを検査するためにファイル ポリシーを使用**できない**ことに注意してください。
- 新しいポリシーの場合、ポリシーが使用中でないことが Web インターフェイスに示されます。使用中のファイル ポリシーを編集している場合は、そのファイル ポリシーを使用しているアクセス コントロール ポリシーの数が Web インターフェイスに示されます。どちらの場合も、テキストをクリックすると [アクセス コントロール ポリシー（Access Control Policies）] ページに移動できます。
- FTP に関する [マルウェア ブロック（Block Malware）] ルールを持つファイル ポリシーを使用するアクセス コントロール ポリシーでは、[インライン時にドロップ（Drop when Inline）] を無効にした侵入ポリシーをデフォルト アクションに設定した場合、システムはルールに一致するファイルやマルウェアの検出でイベントを生成しますが、ファイルをドロップしません。FTP ファイル転送をブロックし、ファイル ポリシーを選択するアクセス コントロール ポリシーのデフォルト アクションとして侵入ポリシーを使用するには、[インライン時にドロップ（Drop when Inline）] を有効にした侵入ポリシーを選択する必要があります。
- 設定に応じて、システムがファイルを初めて検出したときに、そのファイルを検査してクラウド ルックアップの結果を待機するか、または、クラウド ルックアップの結果を待機せずにファイルを通過させることができます。

ファイル ポリシーの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス（Access）
脅威（ファイル制御） マルウェア（ネットワーク向け AMP）	Protection（ファイル制御） マルウェア（ネットワーク向け AMP）	いずれか（Any）	いずれか（Any）	Admin/Access Admin

始める前に

マルウェア保護のポリシーを設定する場合は、ファイル ポリシーの設定（1915 ページ）を参照してください。

ステップ 1 **[Policies]** > **[Access Control]** > **[Malware & File]** を選択します。

ヒント 既存のファイル ポリシーのコピーを作成するには、コピー アイコン（  ）をクリックして、表示されるダイアログ ボックスで新しいポリシーの固有名を入力します。その後、そのコピーを変更できます。

ステップ 2 [新しいファイル ポリシー（New File Policy）] をクリックします。

ステップ 3 新しいポリシーの [名前（Name）] とオプションの [説明（Description）] を入力します。

ステップ 4 [保存（Save）] をクリックします。

ステップ 5 ファイル ルールの作成（1951 ページ）の説明に従って、ファイル ポリシーに 1 つ以上のルールを追加します。

ステップ 6 必要に応じて、[詳細（Advanced）] タブを選択し、詳細オプションおよびアーカイブ ファイル検査オプション （1933 ページ）の説明に従って詳細オプションを設定します。

ステップ 7 ファイル ポリシーを保存します。

次のタスク

- マルウェア保護のポリシーを設定する場合は、ファイル ポリシーの設定（1915 ページ）に戻ります。
- 該当しない場合は、次のようになります。
  - マルウェア保護のためのアクセス コントロール ルールの設定（1712 ページ）の説明に従って、アクセス コントロール ルールにファイル ポリシーを追加します。
  - 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

詳細オプションおよびアーカイブ ファイル検査オプション

ファイル ポリシー エディターの [詳細設定（Advanced）] タブには、次の一般オプションがあります。

- [初回ファイル分析（First Time File Analysis）]：最初に表示された（不明な）ファイルを保存し、ローカルで分析すると同時に AMP クラウドでの処理を保留にする場合にこのオプションを選択します。ファイルは、マルウェア クラウド ルックアップと Spero 分析、ローカル マルウェア分析、またはダイナミック分析を実行するように設定されているルールに一致する必要があります。ストレージと処理リソースを節約するには、このオプションの選択を解除します。このオプションの選択を解除すると、初めて検出されたファイルは「不明（Unknown）」とマークされます。
- [カスタム検出リストを有効にする（Enable Custom Detection List）]：カスタム検出リストにあるファイルをブロックします。
- [クリーンリストを有効にする（Enable Clean List）]：有効にすると、このポリシーはクリーン リストにあるファイルを許可します。
- [脅威スコアに基づいてAMPクラウド判定結果を上書きする（Override AMP Cloud Disposition Based upon Threat Score）]：しきい値の脅威スコアを設定します。スコアがしきい値以上のファイルはマルウェアと見なされます。

  しきい値に低い値を選択すると、マルウェアとして扱われるファイルの数が増えます。ファイル ポリシーで選択したアクションによっては、その結果、ブロックされるファイルの数が増える可能性があります。

ファイル ポリシー エディターの [詳細設定（Advanced）] タブには、次のアーカイブ ファイル検査オプションがあります。

- [アーカイブを検査する（Inspect Archives）]：アクセス コントロールの詳細設定の [保存する最大ファイルサイズ（Maximum file size to store）] と同じ大きさのアーカイブ ファイルまで、アーカイブ ファイルのコンテンツのインスペクションをできるようにします。
- [暗号化されたアーカイブをブロックする（Block Encrypted Archives）]：暗号化されたコンテンツを含むアーカイブ ファイルをブロックします。
- [検査不可能なアーカイブをブロックする（Block Uninspectable Archives）]：暗号化以外の理由でシステムが検査できないコンテンツを含むアーカイブ ファイルをブロックします。これは通常、破損したファイル、または指定した最大アーカイブ深度を超えるファイルに適用されます。
- **[最大アーカイブ深度（Max Archive Depth）]**：指定した深度を超えるネストされたアーカイブ ファイルをブロックします。トップレベルのアーカイブ ファイルはこの数で考慮されません。深さは最初にネストされたファイルで 1 から始まります。

アーカイブ ファイル

アーカイブ ファイルとは、`.zip` や `.rar` ファイルなどの他のファイルを含むファイルです。

ブロック アクションを含むファイル ルールにアーカイブ内のいずれかの個別ファイルが一致する場合は、その個別ファイルだけでなくアーカイブ全体がブロックされます。

アーカイブ ファイルのインスペクションのオプションについては、詳細オプションおよびアーカイブ ファイル検査オプション （1933 ページ）を参照してください。

検査可能なアーカイブ ファイル

- **ファイル タイプ**

  検査可能なアーカイブ ファイル タイプの完全なリストがファイル ルール設定ページに表示されます。このページを表示するには、ファイル ルールの作成 （1951 ページ）を参照してください。

  検査可能な格納ファイルが同じページに表示されます。

- **ファイルサイズ（File size）**

  アクセス コントロールの詳細設定の [保存する最大ファイルサイズ（Maximum file size to store）] ファイル ポリシーと同じ大きさのアーカイブ ファイルまで検査できます。

- **ネストされたアーカイブ**

  アーカイブ ファイルには他のアーカイブ ファイルを含められます。その結果、複数のアーカイブ ファイルが含めることができます。ファイルがネストされるレベルは、そのアーカイブ ファイルの深さです。トップレベルのアーカイブ ファイルは深さの数に含まれないことに注意してください。深さは最初にネストされたファイルで 1 から始まります。

システムは、最も外側のアーカイブ ファイル（レベル 0）の下にネストされた最大 3 つのレベルのファイルを検査できます。その深さ（または指定したそれより低い最大深さ）を超えるアーカイブ ファイルをブロックするようファイル ポリシーを設定できます。

最大アーカイブ ファイルの深さ 3 を超えるファイルをブロックしないよう選択した場合、抽出可能な内容と深さ 3 以上でネストされた内容を含むアーカイブ ファイルがモニタ対象のトラフィックに現れると、システムは検査可能だったファイルについてのみデータを検査して報告します。

圧縮解除されたファイルに適用できるすべての機能（動的分析やファイル ストレージなど）は、アーカイブ ファイル内のネストされたファイルに使用可能です。

- **暗号化ファイル**

  コンテンツが暗号化されているか検査できないアーカイブをブロックするように設定できます。

- **検査されないアーカイブ**

  アーカイブ ファイルを含むトラフィックがセキュリティ インテリジェンスによってブラックリスト登録またはホワイトリスト登録された場合、またはトップレベルのアーカイブ ファイルの SHA-256 値がカスタム検出リストにある場合、システムはアーカイブ ファイルの内容を検査しません。ネストされたファイルがブラックリスト登録された場合、アーカイブ全体がブロックされます。しかし、ネストされたファイルがホワイトリスト登録された場合、アーカイブは自動的に渡されません（他のネストされたファイルおよび特性による）。

アーカイブ ファイルの性質

アーカイブ ファイルの性質は、アーカイブ内部のファイルに割り当てられた性質に基づきます。識別されたマルウェア ファイルを含んでいる**すべて**のアーカイブは、マルウェア（Malware）の性質になります。識別されたマルウェア ファイルを含んでいないアーカイブの場合、不明なファイルが 1 つでも含まれていれば 不明（Unknown）の性質、クリーン ファイルのみが含まれていれば クリーン（Clean）の性質になります。

表 *118 :* 内容に基づくアーカイブ ファイルの性質

アーカイブ ファイルの性質	不明なファイルの数	クリーン ファイルの数	マルウェア ファイルの数
不明	1 つ以上	任意	0
クリーン（Clean）	0	1 つ以上	0
マルウェア	いずれか（Any）	いずれか（Any）	1 つ以上

他のファイルと同様に、アーカイブ ファイルにも、該当する性質に関する条件が適用される場合はカスタム検出（Custom Detection）または利用不可（Unavailable）の性質が割り当てられます。

アーカイブの内容と詳細の表示

アーカイブ ファイルの内容を検査するようにファイル ポリシーが設定されている場合は、[分析（Analysis）] > [ファイル（Files）] メニューのページにあるコンテキスト メニューおよびネットワーク ファイル トラジェクトリ ビューアを使用して、アーカイブ ファイルがファイル イベント、マルウェア イベントに現れた場合、またはキャプチャされたファイルとして現れた場合に、アーカイブ内のファイルに関する情報を表示できます。

アーカイブのすべてのファイル コンテンツは表形式でリストされます。そのリストには、名前、SHA-256ハッシュ値、タイプ、カテゴリ、およびアーカイブの深さといった関連情報の概略が含まれています。ネットワーク ファイル トラジェクトリ アイコンはファイルごとに表示されます。そのアイコンをクリックすることで、特定のファイルに関する詳細な情報を表示することができます。

カスタム リストを使用したファイル性質のオーバーライド

AMP クラウドにあるファイルの性質が不正確だとわかっている場合、クラウドから性質を上書きするファイルの SHA-256 値をファイル リストに追加できます。

- AMP クラウドがクリーンの性質を割り当てた場合と同じ方法でファイルを扱うには、クリーン リストにファイルを追加します。
- AMP クラウドがマルウェアの性質を割り当てた場合と同じ方法でファイルを扱うには、カスタム検出リストにファイルを追加します。

これ以降に検出された場合、デバイスでは、ファイルの性質を再評価せずに許可またはブロックできます。ファイル ポリシーに応じてクリーン リストまたはカスタム検出リストを使用できます。

（注） ファイルの SHA-256 値を計算するには、マルウェア クラウド ルックアップを実行するか、一致ファイルでマルウェアをブロックするルールをファイル ポリシーで設定する必要があります。

Firepower でのファイル リストの使用の詳細については、ファイル リスト （569 ページ）を参照してください。

または、該当する場合はAMP for Endpoints からの一元的なファイル リスト （1936 ページ）を参照します。

AMP for Endpoints からの一元的なファイル リスト

組織で AMP for Endpoints を展開している場合、Firepower は AMP クラウドにファイルの性質を照会するときに、AMP for Endpoints で作成されたブラックリストおよびホワイトリストを使用できます。

要件：

- 組織で AMP パブリック クラウドを使用している必要がある。

- 組織で AMP for Endpoints を展開している。
- Firepower と AMP for Endpoints の統合 （1956 ページ）の手順を使用して、Firepower システムを AMP for Endpoints に登録している。

これらのリストを作成して展開するには、AMP for Endpoints のマニュアルまたはオンラインヘルプを参照してください。

（注） AMP for Endpoints で作成された Firepower オーバーライド ファイル リストで作成されたファイルリスト。

ファイル ポリシーの編集

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス（Access）
脅威（ファイル制御） マルウェア（ネットワーク向け AMP）	Protection（ファイル制御） マルウェア（ネットワーク向け AMP）	いずれか（Any）	いずれか（Any）	Admin/Access Admin

ステップ 1 **[Policies]** > **[Access Control]** > **[Malware & File]** を選択します。

ステップ 2 編集するファイル ポリシーの横にある編集アイコン（）をクリックします。 代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 次の選択肢があります。

- [ファイル ルールの追加（Add File Rule）] を選択して、ファイル ルールを追加します。詳細については、ファイル ルール （1939 ページ）を参照してください。
- 既存のファイル ルールを編集するには、そのルールの横にある編集アイコン（）をクリックします。
- 詳細オプションおよびアーカイブ ファイル検査オプション （1933ページ）の説明に従って詳細オプションを設定します。

（注） ファイル ポリシー エディタに、現在編集中のファイル ポリシーを使用しているアクセス コントロール ポリシーの数が表示されます。この通知をクリックすると、親ポリシーのリストが表示され、オプションで [アクセス コントロール ポリシー（Access Control Policies）] ページに進むことができます。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

ファイル ポリシーの管理

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス（Access）
脅威（ファイル制御） マルウェア（ネットワーク向け AMP ）	Protection（ファイル制御） マルウェア（ネットワーク向け AMP ）	いずれか（Any）	いずれか（Any）	Admin/Access Admin

[ファイル ポリシー（File Policies）] ページには、既存のファイル ポリシーが最終更新日とともに表示されます。このページは、ファイル ポリシーの管理に使用できます。

マルチドメイン展開では、編集できる現在のドメインで作成されたポリシーが表示されます。また、編集できない先祖ドメインで作成されたポリシーも表示されます。下位のドメインで作成されたポリシーを表示および編集するには、そのドメインに切り替えます。

（注） 動的分析の対象となるファイル タイプのリストが更新されたかどうか検査するために、システムは更新をチェックします（多くても 1 日に 1 回）。対象になるファイル タイプのリストが変更された場合、これはファイル ポリシーの変更を意味します。このファイル ポリシーを使用するアクセス コントロール ポリシーがいずれかのデバイスに展開されている場合、そのアクセス コントロール ポリシーには失効マークが付けられます。更新したファイル ポリシーがデバイスで有効になるには、まず、ポリシーを展開しておく必要があります。システムの保守：動的分析の対象となるファイル タイプの更新 （1928 ページ）を参照してください。

ステップ 1 **[Policies]** > **[Access Control]** > **[Malware & File]** を選択します。

ステップ 2 ファイル ポリシーを管理します。

- [比較（Compare）] : [ポリシーの比較（Compare Policies）] をクリックします（ポリシーの比較 （457 ページ） を参照）。
- 作成：ファイル ポリシーを作成するには、[新規ファイル ポリシー（New File Policy）] をクリックし、ファイル ポリシーの作成 （1932 ページ）で説明する手順を実行します。
- コピー：ファイル ポリシーをコピーするには、コピー アイコン（）をクリックします。

  代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

- 削除：ファイル ポリシーを削除するには、削除アイコン（）をクリックし、プロンプトが表示されたら [はい（Yes）] と [OK] をクリックします。

  コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

- 展開：[展開（Deploy）] をクリックします（設定変更の展開 （447 ページ） を参照）。

- 編集：既存のファイル ポリシーを変更するには、編集アイコン（  ）をクリックします。

- [レポート（Report）]：レポート アイコン（  ）をクリックします（現在のポリシー レポートの生成 （459 ページ） を参照）。

ファイル ルール

ファイル ポリシーには、親アクセス コントロール ポリシーと同様に、各ルールの条件に一致するファイルの処理方法を決定するルールがいくつか含まれています。ファイル タイプ、アプリケーション プロトコル、転送方向の違いに応じて異なるアクションを実行する別個のファイル ルールを設定できます。

たとえば、あるファイルがルールに一致する場合、ルールで以下を実行できます。

- 単純なファイル タイプ照合に基づいてファイルを許可またはブロックする
- 性質に基づいてファイルをブロックする（悪意があることを示す評価の有無に関係なく）
- デバイスにファイルを保存する（詳細については、キャプチャされたファイルとファイル ストレージ （1949 ページ）を参照してください）
- ローカル マルウェア分析、Spero 分析、または動的分析のために、保存（キャプチャ）したファイルを送信する

さらに、ファイル ポリシーによって以下を実行できます。

- クリーン リストまたはカスタム検出リストのエントリに基づいて、ファイルがクリーンまたはマルウェアである場合と同じ方法で自動的にファイルを扱う
- ファイルの脅威スコアが、設定可能なしきい値を超えた場合、マルウェアと同じ方法でファイルを扱う
- アーカイブ ファイル（`.zip` や `.rar` など）の内容を検査する
- アーカイブ ファイルの内容が暗号化されている場合、アーカイブのネスト レベルが最大レベル指定値より深い場合、あるいはその反対で検査できない場合、アーカイブ ファイルをブロックする

ファイル ルールのコンポーネント

表 *119 :* ファイル ルールのコンポーネント

ファイル ルールのコンポーネント	説明
アプリケーション プロトコル	システムは、FTP、HTTP、SMTP、IMAP、POP3、NetBIOS-ssn（SMB）を介して伝送されるファイルを検出し、検査できます。デフォルトの [任意（Any）] は、HTTP、SMTP、IMAP、POP3、FTP、および NetBIOS-ssn（SMB）トラフィック内のファイルを検出します。パフォーマンスを向上させるには、ファイル ルールごとに、これらのアプリケーション プロトコルのうち 1 つだけでファイルを検出するよう限定できます。
転送の方向	ダウンロードされるファイルに対して、FTP、HTTP、IMAP、POP3、および NetBIOS-ssn（SMB）の着信トラフィックを検査できます。アップロードされるファイルに対しては、FTP、HTTP、SMTP、および NetBIOS-ssn（SMB）の発信トラフィックを検査できます。 **ヒント** [任意（Any）] を使用すると、ユーザが送信しているか受信しているかには関係なく、多数のアプリケーション プロトコルを介したファイルが検出されます。

ファイル ルールのコンポーネント	説明
ファイルのカテゴリとタイプ	システムは、さまざまなタイプのファイルを検出できます。これらのファイル タイプは、マルチメディア（swf、mp3）、実行可能ファイル（exe、トレント）、PDF などの基本的なカテゴリにグループ分けされます。個々のファイル タイプを検出したり、ファイル タイプ カテゴリ全体を検出したりするよう、ファイルルールを設定できます。 たとえば、すべてのマルチメディア ファイルをブロックしたり、Shockwave Flash（swf）ファイルのみをブロックしたりできます。または、ユーザが BitTorrent（torrent）ファイルをダウンロードしたときにアラートを出すよう、システムを設定できます。 システムで検査可能なファイル タイプのリストについては、[ポリシー（Policies）] > [アクセス制御（Access Control）] > [マルウェアとファイル（Malware & File）] を選択して、一時的な新しいファイル ポリシーを作成してから、[ルールの追加（Add Rule）] をクリックします。ファイル タイプ カテゴリを選択すると、システムが検査できるファイル タイプが [ファイルタイプ（File Types）] リストに表示されます。 （注） 頻繁にトリガーされるファイル ルールは、システム パフォーマンスに影響を与える可能性があります。たとえば、HTTP トラフィックでマルチメディア ファイルを検出しようとすると（たとえば YouTube は多量の Flash コンテンツを伝送します）、膨大な数のイベントが生成される可能性があります。

ファイル ルールのコンポーネント	説明
ファイル ルール アクション	ファイル ルール アクションは、ルールの条件に一致するトラフィックがシステムによってどのように処理されるかを決定します。 選択したアクションに応じて、システムでファイルを保存するか、ファイルに対してSpero分析、ローカルマルウェア分析、または動的分析を実行するかを設定できます。[ブロック（Block）]アクションを選択すると、システムでブロックされた接続をリセットするかどうかも設定できます。 これらのアクションおよびオプションの説明については、ファイル ルール アクション （1942 ページ）を参照してください。 ファイルルールは数値上の順番ではなく、ルールアクションの順番で評価されます。詳細については、「ファイル ルールアクション：評価順序 （1951 ページ）」を参照してください。

ファイル ルール アクション

ファイル ルールを使用すると、ロギング、ブロック、またはマルウェア スキャンの対象となるファイル タイプを詳細に制御できます。各ファイル ルールには、ルールの条件に一致するトラフィックがシステムによってどのように処理されるかを決定する1つのアクションが関連付けられます。効果を発揮するには、ファイルポリシーに1つ以上のルールが含まれている必要があります。1 つのファイル ポリシー内に、ファイル タイプ、アプリケーション プロトコル、転送方向の違いに応じて異なるアクションを実行する別々のルールを使用できます。

ファイル ルール アクション

- [ファイル検出（Detect Files）] ルールを使用すると、ファイルの伝送を許可しながら、特定のファイル タイプの検出をデータベースに記録できます。
- ファイルブロック ルールを使用すると、特定のファイル タイプをブロックできます。ファイル転送がブロックされたときに接続をリセットするオプション、およびキャプチャされたファイルを管理対象デバイスに保存するオプションを設定できます。
- [マルウェア クラウド ルックアップ（Malware Cloud Lookup）] ルールを使用すると、ネットワークを通過するファイルの性質を取得して記録したうえでその伝送を許可できます。
- [マルウェア ブロック（Block Malware）] ルールを使用すると、特定のファイル タイプの SHA-256 ハッシュ値を計算した後、AMP クラウドを照会して、ネットワークを通過するファイルにマルウェアが含まれているかどうかを判断し、脅威を示すファイルをブロックできます。

ファイル ルール アクションのオプション

選択したアクションに応じて、さまざまなオプションがあります。

ファイル ルール アクションのオプション	ファイルのブロックが可能か	マルウェアのブロックが可能か	ファイルの検出が可能か	マルウェア クラウド ルックアップが可能か
MSEXE 用の Spero 分析*（Spero Analysis* for MSEXE）	No	はい：実行可能ファイルを送信できます	No	はい：実行可能ファイルを送信できます
動的分析*（Dynamic Analysis*）	No	はい：不明なファイルの性質の実行可能ファイルを送信できます	No	はい：不明なファイルの性質の実行可能ファイルを送信できます
容量処理（Capacity Handling）	いいえ	はい	いいえ	はい
ローカル マルウェア分析*（Local Malware Analysis*）	いいえ	はい	いいえ	はい
接続のリセット（Reset Connection）	はい（推奨）	はい（推奨）	いいえ	いいえ
ファイルの保存（Store files）	はい：一致するすべてのファイルを保存できます	はい：選択したファイルの性質に一致するファイル タイプを保存できます	はい：一致するすべてのファイルを保存できます	はい：選択したファイルの性質に一致するファイル タイプを保存できます

* これらのオプションの詳細については、マルウェア防御オプション（ファイル ルール アクション） （1944 ページ）およびそのサブトピックを参照してください。

⚠

注意 [ファイルの検出（Detect Files）] または [ファイルのブロック（Block Files）] ルールで [ファイルの保存（Store files）] を有効化または無効化、または [マルウェア クラウド ルックアップ（Malware Cloud Lookup）] または [マルウェア ブロック（Block Malware）] ファイル ルール アクションを分析オプション（[Spero 分析または MSEXE（Spero Analysis or MSEXE）]、[動的分析（Dynamic Analysis）]、または [ローカル マルウェア分析（Local Malware Analysis）]）またはファイルの保存オプション（[マルウェア（Malware）]、[不明（Unknown）]、[正常（Clean）]、または [カスタム（Custom）]）と結合する最初のファイル ルールを追加または最後のファイル ルールを削除すると、設定の変更を展開する際に Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、ターゲット デバイスがトラフィックを処理する方法に応じて異なります。詳細はSnort® の再起動によるトラフィックの動作 （451 ページ）を参照してください。

マルウェア防御オプション（ファイル ルール アクション）

Firepower システムでは、ファイルにマルウェアが含まれるかどうかを判断するために、ファイル インスペクションと分析のいくつかの方法が適用されます。

ファイル ルールでオプションを有効にするオプションに応じて、システムは次のツールと順序でファイルを検査します。

1. Spero 分析 （1947 ページ）およびAMP クラウドのルックアップ （1947 ページ）
2. ローカル マルウェア分析（Local Malware Analysis） （1947 ページ）
3. 動的分析（Dynamic Analysis） （1948 ページ）

これらのツールの比較については、マルウェア防御のオプションの比較 （1944 ページ）を参照してください。

（該当する場合は、そのファイル タイプに基づいてすべてのファイルをブロックすることもできます。詳細については、タイプ別にすべてのファイルをブロック （1951 ページ）を参照してください）。

（オプション）AMP for Endpoints を使用したマルウェア防御 （1953 ページ）およびサブトピックからシスコの AMP for Endpoints 製品に関する情報も参照してください。

マルウェア防御のオプションの比較

次の表では、各タイプのファイル分析の利点と欠点、および各マルウェア防御方法によってファイルの性質が決定される方法について説明します。

分析タイプ	利点	制限事項	マルウェアの特定
Spero 分析	実行可能ファイルの構造分析。Spero シグネチャを分析のために AMP クラウドに送信します	ローカルマルウェア分析または動的分析よりも詳細度が低くなります。実行可能ファイル専用です	マルウェアの特定がポジティブの場合にのみ、性質が [不明（Unknown）] から [マルウェア（Malware）] に変更されます。
ローカルマルウェア分析（Local Malware Analysis）	動的分析より消費するリソースが少なく、特に検出されたマルウェアが一般的な場合は結果がより迅速に返されます	動的分析よりも結果の詳細度が低くなります	マルウェアの特定がポジティブの場合にのみ、性質が [不明（Unknown）] から [マルウェア（Malware）] に変更されます。
動的分析（Dynamic Analysis）	を使用した不明なファイルの詳細な分析 Cisco Threat Grid	対象ファイルはパブリック クラウドまたはオンプレミスアプライアンスにアップロードされます。分析の完了には少し時間がかかります	脅威スコアによってファイルの悪意の度合いが決定されます。性質はファイルポリシーに設定されている脅威スコアしきい値に基づいている場合があります。
Spero 分析とローカル マルウェア分析	AMP クラウドのリソースを使用してマルウェアを特定しながら、ローカルマルウェア分析と動的分析を設定するよりも少ないリソースを消費します	動的分析、Spero 分析よりも詳細度が低くなります。実行可能ファイル専用です	マルウェアの特定がポジティブの場合にのみ、性質が [不明（Unknown）] から [マルウェア（Malware）] に変更されます。
Spero 分析と動的分析	ファイルおよび Spero シグネチャの送信時に AMP クラウドの全機能を使用します	ローカルマルウェア分析を使用する場合よりも結果の取得に時間がかかります	マルウェアの可能性があるとして事前分類されているファイルの場合、動的分析の結果に基づいて脅威スコアが変更されます。ファイル ポリシーで設定されている脅威スコアしきい値に基づいて、および Spero 分析でマルウェアが特定された場合は、性質が [不明（Unknown）] から [マルウェア（Malware）] に変更されます。

分析タイプ	利点	制限事項	マルウェアの特定
ローカルマルウェア分析と動的分析	両方のタイプのファイル分析を使用することで詳細な結果が得られます	どちらか一方の場合よりも消費するリソースが多くなります	マルウェアの可能性があるとして事前分類されているファイルの場合、動的分析の結果に基づいて脅威スコアが変更されます。ローカル マルウェア分析でマルウェアが特定された場合、またはファイル ポリシーで設定されている脅威スコアしきい値に基づいて、性質が [不明（Unknown）] から [マルウェア（Malware）] に変更されます。
Spero 分析、ローカルマルウェア分析、および動的分析	詳細結果	3 つすべてのタイプのファイル分析を実行するため消費するリソースが最も多くなります	マルウェアの可能性があるとして事前分類されているファイルの場合、動的分析の結果に基づいて脅威スコアが変更されます。Spero 分析またはローカル マルウェア分析でマルウェアが特定された場合、またはファイル ポリシーで設定されている脅威スコアしきい値に基づいて、性質が [不明（Unknown）] から [マルウェア（Malware）] に変更されます。
（指定されたファイルタイプのすべてのファイルの送信をブロック）	マルウェア ライセンスは必要ありません （このオプションは技術的なマルウェア防御オプションではありません。）	正規ファイルもブロックされます	（分析は実行されません。）

（注） 事前分類はファイルの性質を決定するものではありません。ファイルが動的分析の対象であるかどうかを判断する要因の 1 つにすぎません。

Spero 分析

Spero分析では、実行可能なファイルのファイル構造の特性（メタデータやヘッダー情報など）を調べます。この情報に基づいてSperoシグネチャを生成した後、ファイルが対象の実行可能なファイルである場合、デバイスはそれをAMPクラウド内のSperoヒューリスティック エンジンに送信します。Sperooシグネチャに基づいて、そのファイルがマルウェアかどうかをSperoエンジンが決定します。また、ファイルをAMPクラウドに送信することなく、Spero分析用に送信するようにルールを設定することもできます。

Spero 分析用にファイルを手動で送信することはできません。

AMP クラウドのルックアップ

高度なマルウェア防御を使用した評価の対象となるファイルの場合、Firepower Management Centerはマルウェア クラウドルックアップを実行し、そのSHA-256ハッシュ値に基づいてファイルの性質をAMP クラウドに照会します。

パフォーマンスを改善するために、システムはクラウドから返される性質をキャッシュ化し、AMP クラウドでクエリを実行する代わりに、既知のファイルのキャッシュ済みの性質を使用します。このキャッシュの詳細については、キャッシュ済み性質の有効期間 （1947ページ）を参照してください。

ローカル マルウェア分析（*Local Malware Analysis*）

ローカル マルウェア分析では、管理対象デバイスで Cisco Talos Intelligence Group（Talos） から提供される検出ルールを使用して、実行可能ファイル、PDF、Office 文書、およびその他のタイプのファイルで最も一般的なタイプのマルウェアの有無をローカルで検査することができます。ローカル分析ではAMPクラウドにクエリを実行せず、ファイルも実行しないため、ローカル マルウェア分析では時間とシステム リソースが節約できます。

システムはローカルマルウェアによってマルウェアを識別すると、その既存のファイルの性質を [不明（Unknown）] から [マルウェア（Malware）] に更新します。その上で、システムは新しいマルウェア イベントを生成します。システムはマルウェアを識別しなかったとしても、ファイルの性質を [不明（Unknown）] から [正常（Clean）] に更新することはしません。ローカル マルウェア分析を実行した後、システムはファイル情報（SHA-256 ハッシュ値、タイムスタンプ、ファイルの性質など）をキャッシュに入れて、特定の期間内にそのファイルを再度検出した場合に再び分析を行わなくてもマルウェアを識別できるようにします。このキャッシュの詳細については、キャッシュ済み性質の有効期間 （1947ページ）を参照してください。

ローカル マルウェア分析では、Cisco Threat Grid クラウドとの通信を確立する必要はありません。ただし、マルウェアとして事前に分類したファイルをダイナミック分析用にクラウドに送信するため、また、アップデートをローカルマルウェア分析ルールセットにダウンロードするために、クラウドとの通信を設定する必要があります。

キャッシュ済み性質の有効期間

AMP クラウドのクエリから返された、脅威スコアに関連付けられた性質、およびローカル マルウェア分析によって割り当てられた性質には、存続可能時間（TTL）が設定されます。性質が更新されないまま、TTL値で指定された期間にわたって保持された後は、キャッシュ情報が消去されます。性質および関連する脅威スコアには次の TTL 値が割り当てられます。

- クリーン：4 時間
- 不明：1 時間
- マルウェア：1 時間

このキャッシュに対するクエリで、キャッシュされた性質がタイムアウトになったことが識別された場合、システムはローカル マルウェア分析データベースおよび AMP クラウドに新しい性質を再びクエリします。

動的分析（*Dynamic Analysis*）

Cisco Threat Grid（以前の AMP Threat Grid）、シスコのファイル分析、および脅威インテリジェンス プラットフォームを使用して動的分析用ファイルを自動的に送信するようにファイル ポリシーを設定できます。

デバイスは、デバイスがファイルを保存するかどうかに関係なく、適格なファイルを Cisco Threat Grid（指定したいずれかのパブリック クラウドまたはオンプレミス アプライアンス）に送信します。

Cisco Threat Grid 悪意のあるファイルかどうかを判断するためにサンドボックス環境でファイルを実行してファイルの動作を分析し、ファイルにマルウェアが含まれる可能性を示す脅威スコアを返します。脅威スコアから、脅威スコアを割り当てた理由が含まれる動的分析のサマリー レポートを表示できます。また、Cisco Threat Grid では、組織が送信したファイルの詳細レポートを表示したり、組織が送信しなかったファイルのデータが限定されたスクラビング処理レポートを表示したりすることもできます。

Cisco Cisco Threat Grid の詳細については、https://www.cisco.com/c/en/us/products/security/threat-grid/index.html を参照してください

動的分析を実行するようにシステムを設定するには、動的分析接続（1925 ページ）のトピックを参照してください。

動的分析の対象となるファイル

動的分析用ファイルの対象は、次の条件によって異なります。

- ファイル タイプ
- ファイル サイズ
- ファイル ルールのアクション

さらに、次のパターンがあります。

- システムは設定したファイル ルールに一致するファイルのみを送信します。
- 分析用の送信時にファイルのマルウェア クラウド ルックアップの性質が不明または使用不可になっている必要があります。
- システムは潜在的なマルウェアとしてファイルを事前分類する必要があります。

動的分析とキャパシティ処理

キャパシティ処理を使用すると、デバイスがクラウドと通信できない場合、または送信の最大数に達した場合に、システムがクラウドにファイルを一時的に送信できないと、動的分析の対象となるファイルを一時的に保存することができます。システムは、妨害状態が経過すると保存したファイルを送信します。

8000 シリーズ デバイスの場合：デバイスはそのハード ドライブまたはマルウェア ストレージ パックにファイルを保存できます。マルウェア ストレージ パック（8000 シリーズ デバイスのみ）（1950 ページ）も参照してください。

他のすべてのデバイス：デバイスはハード ドライブにファイルを保存します。

キャプチャされたファイルとファイル ストレージ

ファイル ストレージ機能を使用すると、選択したファイル（トラフィックで検出された）をキャプチャして、ファイルのコピーをデバイスのハード ドライブかマルウェア ストレージ パック（インストールされている場合）に自動的に保存できます。

デバイスがファイルをキャプチャした後に、以下の選択肢があります。

- 後で分析するために、キャプチャしたファイルをデバイスのハードドライブに保存する。
- さらに手動で分析したりアーカイブしたりするために、保存したファイルをローカル コンピュータにダウンロードする。
- AMP クラウド ルックアップまたは動的分析の対象となるキャプチャ ファイルを手動で送信します。

注意すべき点として、デバイスがファイルを保存した後は、以後それを検出しても、デバイスが引き続きそれを保存していれば、そのファイルを再度キャプチャすることはありません。

（注） ファイルがネットワーク上で初めて検出された際には、ファイルの検出を表すファイル イベントを生成できます。ただし、ファイル ルールがマルウェア クラウド ルックアップを行う場合は、システムが AMP クラウドにクエリを行い、判定結果が返るまで、より多く時間を要します。この遅延により、システムはネットワークでこのファイルが 2 回目に検出され、ファイルの判定結果を即座に判断できるまでは、このファイルを保存できません。

システムがファイルをキャプチャするか保存するかに関わらず、以下が可能です。

- [分析（Analysis）] > [ファイル（Files）] > [キャプチャされたファイル（Captured Files）] からのキャプチャされたファイルに関する情報（動的分析のためにファイルが保存されたのか送信されたかどうか、ファイルの性質、脅威スコアなど）を確認することにより、ネットワーク上で検出されたマルウェアの潜在的な脅威について迅速に検討する。
- ファイルのトラジェクトリを表示して、ネットワークのトラバースの仕方およびコピーを保持しているホストを判別する。
- ファイルをクリーン リストまたはカスタム検出リストに追加することで、以後の検出時には常に、クリーンまたはマルウェアの判定結果を持つファイルとして扱う。

ファイル ポリシーでファイル ルールを設定して、特定のタイプまたは特定のファイル判定結果（使用できる場合）のファイルをキャプチャして保存します。ファイルポリシーをアクセス コントロール ポリシーと関連付けて、それをデバイスに展開した後、トラフィック内の一致ファイルが検出され、保存されます。また、保存するファイルサイズの最小値と最大値を設定できます。

システム バックアップに保存ファイルは含まれません。

キャプチャしたファイル情報は、[分析（Analysis）]>[ファイル（Files）]>[キャプチャファイル（Captured Files）] で表示し、コピーをオフライン分析用にダウンロードすることができます。

マルウェア ストレージ パック（8000 シリーズ デバイスのみ）

ファイル ポリシー構成によっては、デバイスがハード ドライブにかなりの量のファイル データを保存することがあります。デバイスにマルウェア ストレージ パックを設置できます。システムがファイルをマルウェア ストレージ パックに保存することにより、イベントおよび設定ファイルを保存するために、プライマリ ハード ドライブにより多くスペースを確保できます。システムは定期的に古いファイルを削除します。デバイスのプライマリ ハード ドライブに使用可能な領域が十分でなく、マルウェア ストレージパックも設置されていない場合、ファイルを保存することはできません。

⚠

注意 Cisco から供給されたハード ドライブ以外はデバイスに取り付けないでください。サポートされていないハード ドライブを取り付けると、デバイスが破損する可能性があります。マルウェア ストレージパック キットは、シスコから**のみ**購入でき、8000 シリーズ デバイスで**のみ**使用できます。マルウェア ストレージ パックのサポートが必要な場合は、サポートにお問い合わせください。詳細については、*Firepower System Malware Storage Pack Guide*を参照してください。

マルウェア ストレージ パックが設置されていない場合、ファイルを保存するデバイスを設定すると、プライマリ ハード ドライブのスペースの特定の部分がキャプチャ ファイル ストレージに割り当てられます。ダイナミック分析用に一時的にファイルに保存するよう容量処理を設定すると、システムはファイルをクラウドに再送信できるようになるまで、同じハード ドライブ割り当てを使用してそれらのファイルを保存します。

デバイスにマルウェア ストレージ パックを設置してファイル ストレージまたは容量処理を設定すると、デバイスはマルウェア ストレージ パック全体をこれらのファイルの保存用として割り当てます。デバイスは、マルウェア ストレージ パックに他の情報を保存することはできません。

キャプチャ ファイル ストレージに割り当てられたスペースがいっぱいになると、システムは割り当てられたスペースがシステム定義しきい値に達するまで、保管されている古いファイルを削除します。保存されていたファイルの数によっては、システムがファイルを削除した後、ディスク使用率がかなり減る場合があります。

マルウェア ストレージ パックを設置する時点で、デバイスがすでにファイルを保存している場合、次にデバイスを再起動したときに、プライマリ ハード ドライブに保存されていたキャプチャ ファイルまたは容量処理ファイルはすべて、マルウェア ストレージ パックに移動しま

す。それ以降デバイスが保存するファイルはすべて、マルウェア ストレージ パックに保存されます。

タイプ別にすべてのファイルをブロック

マルウェア ファイル伝送のブロックに加えて、マルウェアを含むかどうかにかかわらず、特定のタイプのすべてのファイルをブロックする必要がある場合は、それを実行できます。

システムでマルウェアを検出できるすべてのファイル タイプだけでなく、さらに多数のファイル タイプに対するファイル制御がサポートされています。これらのファイル タイプは、マルチメディア（swf、mp3）、実行可能ファイル（exe、トレント）、PDF などの基本的なカテゴリにグループ分けされます。

タイプに基づいてすべてのファイルをブロックすることは、技術的にはマルウェア防御機能ではありません。マルウェア ライセンスは不要であり、AMP クラウドにクエリしません。

ファイル ルール アクション：評価順序

ファイルポリシーには、状況に応じて異なるアクションを持つ複数のルールが含まれる可能性があります。複数のルールを特定の状況に適用できる場合、このトピックで説明する評価順序が適用されます。通常、（優先度の高い順に）単純なブロッキング、次にマルウェア インスペクションとブロッキング、さらにその次に単純な検出とロギングとなります。

ファイル ルール アクションの優先度は次のとおりです。

- ファイル ブロック（*Block Files*）
- マルウェア ブロック（*Block Malware*）
- マルウェア クラウド ルックアップ（*Malware Cloud Lookup*）
- ファイル検出（*Detect Files*）

設定されている場合、TID は、アクションの優先順位付けに影響を与えます。詳細については、「TID-Firepower Management Center のアクションの優先順位付け （1994 ページ）」を参照してください。

ファイル ルールの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス（Access）
脅威（ファイル制御） マルウェア（ネットワーク向け AMP）	Protection（ファイル制御） マルウェア（ネットワーク向け AMP）	いずれか（Any）	いずれか（Any）	Admin/Access Admin

⚠

注意 [ファイルの検出（Detect Files）] または [ファイルのブロック（Block Files）] ルールで [ファイルの保存（Store files）] を有効化/無効化した場合、または [マルウェア クラウド ルックアップ（Malware Cloud Lookup）] または [マルウェア ブロック（Block Malware）] ファイル ルール アクションを分析オプション（[Spero 分析または MSEXE（Spero Analysis or MSEXE）]、[動的分析（Dynamic Analysis）]、または [ローカル マルウェア分析（Local Malware Analysis）]）またはファイルの保存オプション（[マルウェア（Malware）]、[不明（Unknown）]、[正常（Clean）]、または [カスタム（Custom）]）と結合する最初のファイル ルールを追加または最後のファイル ルールを削除した場合には、設定の変更を展開する際に Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、ターゲット デバイスがトラフィックを処理する方法に応じて異なります。詳細はSnort® の再起動によるトラフィックの動作 （451 ページ）を参照してください。

始める前に

マルウェア保護のルールを設定する場合は、ファイル ポリシーの設定 （1915 ページ）を参照してください。

ステップ 1 ファイル ポリシー エディタで、[ファイル ルールの追加（Add File Rule）] をクリックします。

ステップ 2 ファイル ルールのコンポーネント （1940 ページ）の説明に従って、[アプリケーション プロトコル（Application Protocol）] および [転送の宛先（Direction of Transfer）] を選択します。

ステップ 3 [ファイル タイプ（File Types）] を 1 つ以上選択します。

表示されるファイル タイプは、選択したアプリケーション プロトコル、転送の方向、およびアクションによって異なります。

ファイル タイプのリストを、次のようにフィルタ処理できます。

- 1 つ以上の [ファイル タイプ カテゴリ（File Type Categories）] を選択し、[選択したカテゴリのすべてのタイプ（All types in selected Categories）] をクリックします。
- 名前または説明でファイル タイプを検索します。たとえば、Microsoft Windows 固有のファイルのリストを表示するには、[Search name and description] フィールドに **`Windows`** と入力します。

ヒント ファイル タイプの上にポインタを移動すると、説明が表示されます。

ステップ 4 ファイル ルール アクション：評価順序 （1951 ページ）を確認し、ファイル ルール アクション （1942 ページ）の説明に従ってファイル ルール [アクション（Action）] を選択します。

利用可能なアクションは、インストールしたライセンスによって異なります。ファイルおよびマルウェア ポリシーのライセンス要件 （1913 ページ）を参照してください。

ステップ 5 選択したアクションに応じて、以下のオプションを設定します。

- ファイルのブロック後に接続をリセットする

- ルールに一致するファイルを保存する
- Spero 分析*を有効にする
- ローカル マルウェア分析*を有効にする
- 動的分析*およびキャパシティ処理を有効にする

* これらのオプションの詳細については、ファイル ルール アクション（1942 ページ）とマルウェア防御オプション（ファイル ルール アクション）（1944 ページ）およびそのサブトピックを参照してください。

ステップ 6 [追加（Add）] をクリックします。

ステップ 7 [保存（Save）] をクリックしてポリシーを保存します。

次のタスク

- マルウェア保護のポリシーを設定する場合は、ファイル ポリシーの設定（1915 ページ）に戻ります。
- 設定変更を展開します。設定変更の展開（447 ページ）を参照してください。

レトロスペクティブな性質の変更

ファイルの性質は変更される可能性があります。たとえば、新しい情報が見つかると、AMP クラウドによる判定の結果、以前はクリーンであると考えられていたファイルが今はマルウェアとして識別されるようになったり、その逆、つまりマルウェアと識別されたファイルが実際にはクリーンであったりする可能性があります。過去 1 週間にクエリを行ったファイルの性質が変更された場合、AMP クラウドはシステムに通知して、システムが次回そのファイルの送信を検出した際に自動的にアクションをとれるようにします。変更された性質は、レトロスペクティブな性質と呼ばれます。

（オプション）AMP for Endpoints を使用したマルウェア防御

シスコの AMP for Endpoints は、Firepower システムから提供され、Firepower 展開と統合し、マルウェア防御を補完できる個別のマルウェア防御製品です。

AMP for Endpoints はシスコのエンタープライズクラスの高度なマルウェア防御ソリューションです。個別ユーザのエンドポイント（コンピュータやモバイルデバイス）で軽量コネクタとして実行し、高度なマルウェアの発生、高度で継続的な脅威、およびターゲット型攻撃を検出、分析、ブロックします。

AMP for Endpoints の利点は次のとおりです。

- 部門全体のためにカスタム マルウェア検出ポリシーとプロファイルを設定し、すべてのユーザのファイルに対してフラッシュ スキャンおよび完全スキャンを実行する
- マルウェア分析の実行：ヒートマップ、詳細なファイル情報、ネットワーク ファイル トラジェクトリ、脅威の根本原因の表示など
- アウトブレイク制御のさまざまな局面を設定する：自動検疫、検疫されていない実行可能ファイルの実行を停止するアプリケーション ブロッキング、除外リストなど
- カスタム保護の作成、グループ ポリシーに基づく特定のアプリケーションの実行ブロッキング、およびカスタム ホワイトリストの作成
- AMP for Endpoints 管理コンソールを使用してマルウェアの影響を軽減する。管理コンソールの堅牢かつ柔軟な Web インターフェイスを使用すると、エンドポイント向け AMP 展開のあらゆる側面を制御し、アウトブレイクのすべての段階を管理できます。

AMP for Endpoints の詳細については、次の項目を参照してください。

- https://www.cisco.com/c/en/us/products/security/amp-for-endpoints/index.html。
- AMP for Endpoints 管理コンソールのオンライン ヘルプ。
- AMP for Endpoints のマニュアル入手先：http://docs.amp.cisco.com。

マルウェア防御の比較：Firepower と AMP for Endpoints

表 *120*：製品の検出による高度なマルウェア保護の違い

機能	Firepower Malware Protection（ネットワーク向け AMP）	AMP for Endpoints
ファイル タイプの検出とブロッキングの方法（ファイル制御）	ネットワーク トラフィックでアクセス コントロール ポリシーとファイル ポリシーを使用	未サポート
マルウェアの検出とブロッキングの方法	ネットワーク トラフィックでアクセス コントロール ポリシーとファイル ポリシーを使用	個々のエンドポイント（エンドユーザ コンピュータとモバイルデバイス）で AMP クラウドとの通信を行うコネクタを使用
ネットワーク トラフィックを検査	管理対象デバイスを通過するトラフィック	なし（エンドポイントにインストールされたコネクタがファイルを直接検査する）
マルウェア インテリジェンスのデータ ソース	AMP クラウド（パブリックまたはプライベート）	AMP クラウド（パブリックまたはプライベート）
マルウェア検出の堅牢性	限定されたファイル タイプ	すべてのファイル タイプ

機能	Firepower Malware Protection（ネットワーク向け AMP）	AMP for Endpoints
マルウェア分析の選択肢	FMC ベース、および AMP クラウドでの分析	FMC ベース、およびエンドポイント向け AMP 管理コンソールの追加オプション
マルウェアの影響軽減	ネットワーク トラフィックでのマルウェア ブロッキング、FMC が開始する修復	エンドポイント向け AMP ベースの検疫およびアウトブレイク コントロール オプション、FMC が開始する修復
生成されるイベント	ファイルイベント、キャプチャされたファイル、マルウェアイベント、およびレトロスペクティブ マルウェア イベント	マルウェア イベント
マルウェア イベントに含まれる情報	基本的なマルウェアイベント情報、および接続データ（IP アドレス、ポート、アプリケーション プロトコル）	詳細なマルウェアイベント情報（接続データなし）
ネットワーク ファイル トラジェクトリ	FMC ベース	FMC と AMP for Endpoints の管理コンソールには、それぞれネットワーク ファイル トラジェクトリがあります。いずれも使用可能です。
必要なライセンスまたはサブスクリプション	ファイル制御の実行に必要なライセンスと ネットワーク向け AMP	AMP for Endpoints サブスクリプション。FMC への AMP for Endpoints データの取り込みに必要なライセンスはありません。

Firepower と AMP for Endpoints の統合について

組織で AMP for Endpoints が導入されている場合、必要に応じてその製品を Firepower 展開と統合できます。

AMP for Endpoints との統合に専用の Firepower ライセンスは必要ありません。

Firepower と AMP for Endpoints の統合の利点

AMP for Endpoints 展開を Firepower システムに統合すると、次のような利点があります。

- AMP for Endpoints で設定する中央集中型ブラックリストおよびホワイトリストによって、Firepower から AMP クラウドに送信されるファイル SHA の判定が決まります。

  AMP for Endpoints からの一元的なファイル リスト （1936 ページ）を参照してください。

- システムは AMP for Endpoints によって検出されたマルウェア イベントを Firepower Management Center にインポートできるため、Firepower システムによって生成されたマル

ウェアイベントとともにこれらのイベントを管理できます。これらのイベントでインポートされたデータには、スキャン、マルウェア検出、隔離、ブロックされた実行、クラウドの呼び出し、およびモニタするホストに対して FMC が表示する侵害の兆候（IOC）が含まれます。

詳細については、AMP for Endpoints を使用したマルウェア イベント分析 （3119 ページ）を参照してください。

- AMP for Endpoints コンソールでは、ファイルの軌跡およびその他の詳細を表示できます。

  詳細は、AMP for Endpoints コンソールでのイベント データの使用 （3157 ページ）を参照してください。

重要 Cisco AMP プライベート クラウドを使用する場合は、AMP for Endpoints と AMP プライベート クラウド （1956 ページ）の制限事項を参照してください。

AMP for Endpoints と AMP プライベート クラウド

ネットワーク上の AMP エンドポイント データを収集するように Cisco AMP プライベート クラウドを設定した場合、すべての AMP for Endpoints コネクタはプライベート クラウドにデータを送信します。そのデータは Firepower Management Center に転送されます。プライベート クラウドは、エンドポイント データを外部接続では一切共有しません。

組織で AMP プライベート クラウドを展開している場合、プライベート クラウドを介した AMP クラウド ファネルとのすべての接続は、監視対象ネットワークのセキュリティとプライバシーを確保するための匿名プロキシとして機能します。これには AMP for Endpoints データのインポートが含まれます。プライベート クラウドは、エンドポイント データを外部接続では一切共有しません。

AMP プライベート クラウドを使用する場合、次の統合機能は使用できません。AMP for Endpoints で設定されたブラックリストとホワイトリストの使用、Firepower から生成されたマルウェア イベントの AMP for Endpoints での表示。

必要なキャパシティをサポートするように複数のプライベート クラウドを設定できます。

Firepower と AMP for Endpoints の統合

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin

組織がシスコの AMP for Endpoints 製品を展開している場合は、そのアプリケーションを Firepower と統合し、Firepower と AMP for Endpoints の統合の利点 （1955 ページ）で説明されている利点を実現できます。

AMP for Endpoints と統合する場合、ネットワーク向け AMP （AMP for Firepower）接続がすでに設定されていても、AMP for Endpoints 接続を設定する必要があります。複数の AMP for Endpoints クラウド接続を設定できます。

注意 マルチドメイン展開では、特にリーフ ドメインに重複する IP スペースがある場合は、AMP for Endpoints 接続をリーフ レベルのみで設定します。複数のサブドメインに同じ IP-MAC アドレス ペアを持つホストがある場合、システムが誤ったリーフ ドメインにエンドポイント向けの AMP が生成したマルウェア イベントを保存したり、誤ったホストに IOC を関連付けたりする可能性があります。

ただし、AMP for Endpoints 接続は、どのドメイン レベルでも設定可能です。ただし、各接続にそれぞれ個別の AMP for Endpoints アカウントを使用する必要があります。たとえば、MSSP の各クライアントは、それぞれ独自のエンドポイント向け AMP を展開している場合があります。

（注） AMP for Endpoints 接続が正しく登録されていなくても、ネットワーク向け AMP は影響を受けません。

始める前に

- 展開で Cisco AMP プライベート クラウドを使用している場合は、AMP for Endpoints と AMP プライベート クラウド （1956 ページ）の制限事項を参照してください。
- ネットワークで AMP for Endpoints が設定されていて、正しく機能している必要があります。
- Firepower Management Center はインターネットに直接アクセスできる必要があります。
- FMC および AMP for Endpoints が相互に通信できることを確認します。セキュリティ、インターネット アクセス、および通信ポート （3281 ページ）のトピックを参照してください。
- Firepower Management Center を工場出荷時の初期状態に復元した後、または以前のバージョンに戻した後に AMP クラウドに接続している場合は、AMP for Endpoints 管理コンソールを使用して以前の接続を削除します。
- この手順中に AMP for Endpoints コンソールにログインするには、AMP for Endpoints クレデンシャルが必要です。

ステップ 1 **[AMP]** > **[AMP Management]**を選択します。

ステップ 2 [AMPクラウド接続の追加（Add AMP Cloud Connection）] をクリックします。

ステップ 3 [クラウド名（Cloud Name）] ドロップダウン リストから、使用するクラウドを選択します。

- Firepower Management Center の地理的な場所に最も近い AMP クラウド。

APJC はアジア/太平洋/日本/中国です。

- AMP プライベート クラウド（AMPv）の場合、[プライベートクラウド（Private Cloud）] を選択し、Cisco AMP プライベート クラウド （1921 ページ）の手順に進みます。

ステップ 4 このクラウドを ネットワーク向け AMP と AMP for Endpoints の両方に使用する場合は、[AMP for Firepower に使用（Use for AMP for Firepower）] チェックボックスをオンにします。

ネットワーク向け AMP （AMP for Firepower）通信を処理する別のクラウドを設定した場合は、このチェックボックスをオフにすることができます。これが唯一の AMP 接続の場合は、オフにできません。

マルチドメイン展開では、このチェックボックスはグローバル ドメインにのみ表示されます。各 Firepower Management Center には、ネットワーク向け AMP 接続を 1 つだけ設定できます。

ステップ 5 [登録（Register）] をクリックします。

回転状態のアイコンは、たとえば、Firepower Management Center で接続を設定した後、AMP for Endpoints 管理コンソールの使用を許可する前に、接続が保留中であることを示します。失敗または拒否を示すアイコン（  ）は、クラウドが接続を拒否したこと、または他の理由で接続が失敗したことを示します。

ステップ 6 AMP for Endpoints 管理コンソールを続行することを確認し、管理コンソールにログインします。

ステップ 7 管理コンソールを使用して、AMP for Endpoints データを Firepower Management Center に送信することを AMP クラウドに許可します。

ステップ 8 FMC が受信するデータを制限する場合は、情報を受け取る組織内の特定のグループを選択します。

デフォルトでは、AMP クラウドはすべてのグループのデータを送信します。グループを管理するには、AMP for Endpoints 管理コンソールで **[管理（Management）]** > **[グループ（Groups）]** を選択します。詳細については、管理コンソールのオンライン ヘルプを参照してください。

ステップ 9 [許可（Allow）] をクリックして接続を有効にして、データの転送を開始します。

[拒否（Deny）] をクリックすると Firepower Management Center に戻りますが、接続には拒否マークが付きます。接続を拒否/許可しないまま AMP for Endpoints 管理コンソールの [アプリケーション（Applications）] ページから別のページに移動した場合、Firepower Management Center の Web インターフェイスでは接続に保留中のマークが付きます。これらのいずれの状況でも、ヘルス モニタは失敗した接続のアラートを生成**しません**。後で AMP クラウドに接続するには、失敗した接続または保留中の接続を削除してから再作成します。

AMP for Endpoints 接続の登録が未完了であっても、ネットワーク向け AMP 接続は無効になりません。

ステップ 10 接続が正しく設定されていることを確認するには、次の手順を実行します。

a) **[AMP]** > **[AMP Management]** ページで、[Cisco AMP ソリューション タイプ（Cisco AMP Solution Type）] 列に **AMP for Endpoints** が含まれている [クラウド名（Cloud Name）] をクリックします。

b) 表示される AMP for Endpoints コンソール ウィンドウで、[アカウント（Accounts）] > [アプリケーション（Applications）] を選択します。

c) Firepower Management Center が一覧に含まれていることを確認します。

d) AMP for Endpoints コンソール ウィンドウで、[管理（Manage）] > [コンピュータ（Computers）] を選択します。

e) Firepower Management Center が一覧に含まれていることを確認します。

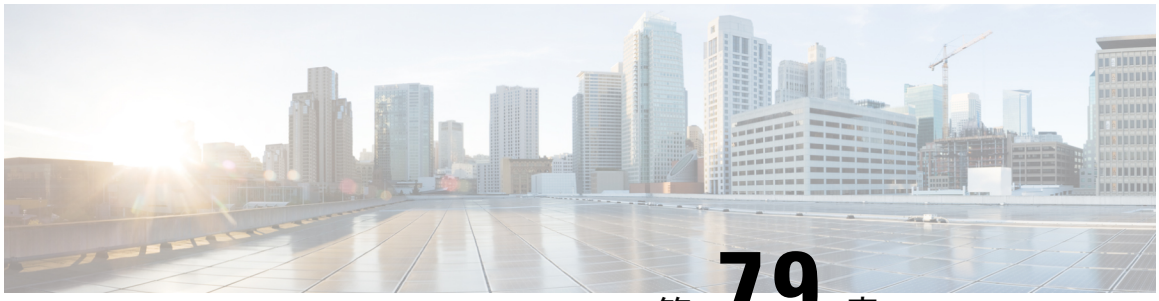
次のタスク

- AMP for Endpoints コンソール ウィンドウで、必要に応じて設定を行います。たとえば、管理センターのグループ メンバーシップの定義や、ポリシーの割り当てを行います。詳細については、AMP for Endpoints のオンライン ヘルプまたはその他のドキュメントを参照してください。
- ハイ アベイラビリティの設定では、Firepower Management Center のアクティブ インスタンスとスタンバイ インスタンスで AMP クラウド接続を個別に設定する必要があります。これらの設定は同期されません。
- デフォルトのヘルス ポリシーは、Firepower Management Center から AMP for Endpoints への最初の接続が成功した後で接続できなくなった場合、または AMP ポータルを使って接続が登録解除された場合に警告を出します。

  [システム（System）] > [ヘルス（Health）] > [ポリシー（Policy）] の [AMP for Endpointのステータス（AMP for Endpoints Status）] モニタが有効になっていることを確認します。

ファイルとマルウェアの履歴の章

機能	バージョン	詳細
章の再構成	変更は 6.4 で行われましたが、再発行されたすべてのバージョンに適用されます	混乱を避けるため、この章の内容が再構成されました。 ファイル/マルウェア イベントとネットワーク ファイル トラジェクトリ（3115ページ）の章との間で一部の内容の移動がありました。
URL フィルタリング情報を新しい URL フィルタリングの章に移動しました	6.3	URL フィルタリングのクラウド通信の設定に関する情報を新しい URL フィルタリングの章に移動しました。章内の Cisco CSI のトピックの構成に関連する変更を加えました。



第 79 章

ファイルとマルウェアのインスペクション パフォーマンスとストレージの調整

次のトピックでは、ファイルとマルウェアのインスペクション パフォーマンスとストレージを設定する方法について説明します。

ファイルおよびマルウェアのインスペクションパフォーマンスとストレージのオプション

ファイル サイズを増やすと、システムのパフォーマンスに影響を与える可能性があります。

表 *121 :* アクセス コントロール ファイルおよび ネットワーク向け *AMP* の詳細オプション

フィールド	説明	ガイドラインと制限
ファイルタイプを検知する前に検閲するバイト数制限（Limit the number of bytes inspected when doing file type detection）	ファイル タイプを検出するときに検査するバイト数を指定します。	0 ～ 4294967295（4 GB） 0 にすると制限が解除されます。 デフォルト値は、TCP パケットの最大セグメント サイズ（1460バイト）です。ほとんどの場合、システムは最初のパケットによって、一般的なファイル タイプを特定できます。 ISO ファイルを検出するには、36870 よりも大きい値を入力します。

フィールド	説明	ガイドラインと制限
ファイルを許可するのにかかるマルウェア ブロックのクラウドルックアップの制限時間（秒）（Allow file if cloud lookup for Block Malware takes longer than (seconds)）	マルウェア クラウド ルックアップの実行中に、システムが [マルウェア ブロック（Block Malware）] ルールに一致し、性質がキャッシュに入っていないファイルの最後のバイトを保持する期間を指定します。システムが性質を取得する前にこの期間が満了すると、ファイルが渡されます。「使用不可」の性質はキャッシュに入れられません。	0 ～ 30 秒 サポートに連絡することなく、このオプションを 0 に設定しないでください。 シスコは、接続の障害によってトラフィックのブロックを防ぐために、デフォルト値を使用することをお勧めします。
SHA-256 ハッシュ値を計算するファイルの上限サイズ（バイト）（Do not calculate SHA--256 hash values for files larger than (in bytes)）	システムが特定のサイズを超えるファイルを保管すること、ファイルでマルウェア クラウド ルックアップを実行すること、またはカスタム検出リストに追加されたファイルをブロックすることを防止します。	0 ～ 4294967295（4 GB） 0 にすると制限が解除されます。 この値は、[保存する最大ファイルサイズ（バイト）（Maximum file size to store (bytes)）] および [動的分析テストの最大ファイルサイズ (バイト)（Maximum file size for dynamic analysis testing (bytes)）] の値以上に設定する必要があります。

[高度なファイル インスペクションと保存のための最小ファイル サイズ（バイト）（Minimum file size for advanced file inspection and storage (bytes)）]	これらの設定は以下を指定します。
	• 次のディテクタを使用してシステムが検査できるファイルサイズ：
	  • Spero 分析
	  • サンドボクシングと事前分類
	  • ローカル マルウェア分析/ClamAV
	  • アーカイブ インスペクション
	• システムがファイル ルールを使用して保存できるファイルサイズ。
		0 ～ 10485760（10MB）
		0 にするとファイル ストレージが無効になります。
		[保存する最大ファイルサイズ（バイト）（Maximum file size to store (bytes)）] および [SHA-256ハッシュ値を計算するファイルの上限サイズ（バイト）（Do not calculate SHA-256 hash values for files larger than (in bytes)）] の値以下に設定する必要があります。

[高度なファイル インスペクションと保存のための最大ファイル サイズ（Minimum file size for advanced file inspection and storage (bytes)）]		0 ～ 10485760（10MB） 0 にするとファイル ストレージが無効になります。 [保存する最小ファイルサイズ（バイト）（Minimum file size to store (bytes)）] の値以上、および [SHA-256 ハッシュ値を計算するファイルの上限サイズ（バイト）（Do not calculate SHA-256 hash values for files larger than (in bytes)）] の値以下に設定する必要があります。

フィールド	説明	ガイドラインと制限
ダイナミック分析の最小ファイルサイズ（バイト）（Minimum file size for dynamic analysis testing (bytes)）	システムが AMP クラウドに動的分析対象として送信できるファイルの最小サイズを指定します。	0 ~ 10485760（10 MB） [動的分析テストの最大ファイルサイズ（バイト）（Maximum file size for dynamic analysis testing (bytes)）] および [SHA-256ハッシュ値を計算するファイルの上限サイズ（バイト）（Do not calculate SHA-256 hash values for files larger than (in bytes)）] の値以下に設定する必要があります。 動的分析のファイルサイズは、ファイル分析の最小および最大設定で定義された制限内のサイズにする必要があります。 システムは AMP クラウドをチェックして、送信可能なファイルの最小サイズが更新されているかどうかを調べます（最大で 1 日 1 回）。新しい最小サイズが現在の値より大きい場合、現在の値が新しい最小サイズに更新され、ポリシーは古いポリシーとしてマークされます。
ダイナミック分析の最大ファイルサイズ(バイト)（Maximum file size for dynamic analysis testing (bytes)）	システムが AMP クラウドに動的分析対象として送信できるファイルの最大サイズを指定します。	0 ~ 10485760（10 MB） [動的分析の最小ファイルサイズ（バイト）（Minimum file size for dynamic analysis testing (bytes)）] の値以上、[SHA-256ハッシュ値を計算するファイルの上限サイズ（バイト）（Do not calculate SHA-256 hash values for files larger than (in bytes)）] の値以下に設定する必要があります。 動的分析のファイルサイズは、ファイル分析の最小および最大設定で定義された制限内のサイズにする必要があります。 システムは AMP クラウドをチェックして、送信可能なファイルの最大サイズが更新されているかどうかを調べます（最大で 1 日 1 回）。新しい最大サイズが現在の値より小さい場合、現在の値が新しい最大サイズに更新され、ポリシーは古いポリシーとしてマークされます。

ファイルおよびマルウェアのインスペクションパフォーマンスおよびストレージの調整

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス（Access）
脅威（ファイル制御） マルウェア（AMP）	保護（ファイル制御） マルウェア（AMP）	いずれか（Any）	いずれか（Any）	Admin/Access Admin/Network Admin

ステップ 1 アクセス コントロール ポリシー エディタで、[詳細（Advanced）] タブをクリックします。

ステップ 2 [ファイルおよびマルウェアの設定（Files and Malware Settings）] の横にある編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ポリシーから継承され、設定を変更する権限がありません。 設定がロック解除されている場合は、[Inherit from base policy] をオフにして、編集を有効にします。

ステップ 3 ファイルおよびマルウェアのインスペクション パフォーマンスとストレージのオプション （1961 ページ）で説明されている任意のオプションを設定します。

ステップ 4 [OK] をクリックします。

ステップ 5 [保存（Save）] をクリックしてポリシーを保存します。

次のタスク

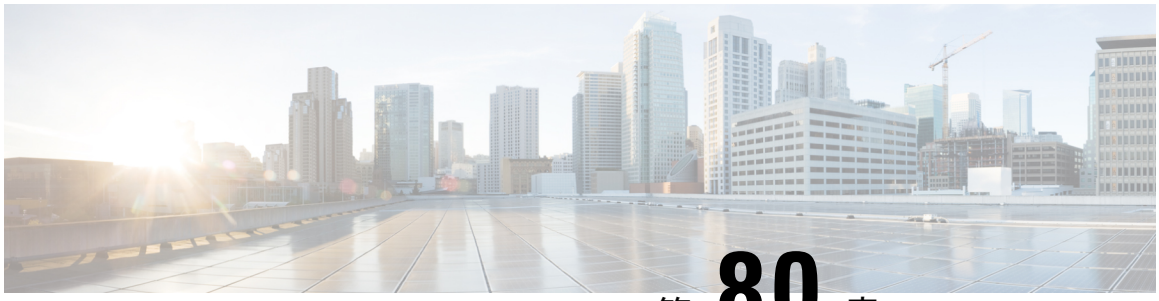
- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

関連トピック

Snort® の再起動シナリオ （450 ページ）

第 XIX 部

TID インテリジェンスおよび攻撃分析



第 80 章

Cisco Threat Intelligence Director（TID）

この章のトピックでは、Firepower システムで TID を設定および使用する方法について説明します。

Cisco Threat Intelligence Director（TID） の概要

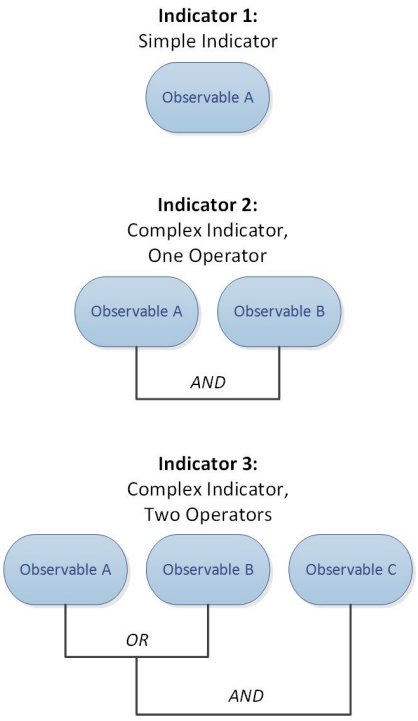
Cisco Threat Intelligence Director（TID） は脅威インテリジェンス データを操作可能にし、インテリジェンスデータの集約、防衛アクションの設定、環境内の脅威の分析を支援します。この機能は、Firepower の他の機能を補完するもので、脅威に対する追加の防衛線を提供します。

TID をホスティング プラットフォームに設定すると、脅威インテリジェンス ソースからデータが取り込まれ、設定されたすべての管理対象デバイス（要素）にそのデータが公開されます。このリリースでサポートされているホスティングプラットフォームと要素の詳細については、プラットフォーム、要素、およびライセンスに関する要件（1971 ページ） を参照してください。

ソースには、オブザーバブルを含むインジケータが含まれています。インジケータは、脅威に関連するすべての特性を伝達し、個々のオブザーバブルは、その脅威に関連付けられた個々の特性（例えば、SHA-256 値）を表します。単純なインジケータには単一のオブザーバブルが含まれ、複合インジケータには 2 つ以上のオブザーバブルが含まれます。

オブザーバブルとそれらの間の AND/OR 演算子は、次の例に示すように、インジケータのパターンを形成します。

図 *52 :* 例：インジケータ パターン



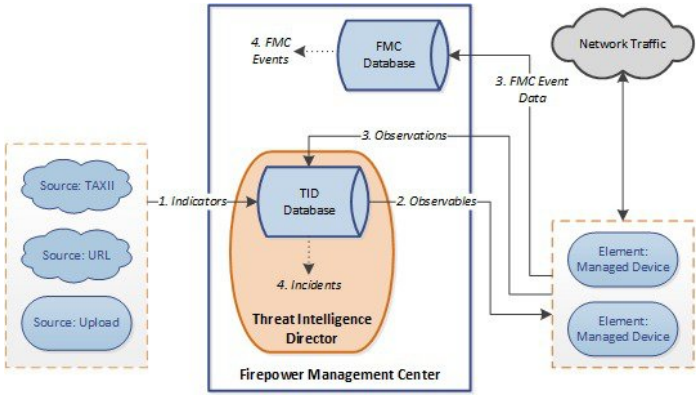
オブザーバブルが要素に公開された後、要素はトラフィックをモニタし、システムがトラフィック内のオブザーバブルを識別すると、Firepower Management Center にオブザベーションを報告します。

Firepower Management Center は、すべての要素からのオブザベーションを収集し、TID インジケータに対してオブザベーションを評価して、オブザーバブルの親インジケータに関連付けられたインシデントを生成または更新します。

インシデントは、インジケータのパターンが満たされたときに完全に実現されます。トラフィックがインジケータ内の 1 つまたは複数のオブザーバブルに一致するが、パターン全体では一致しない場合、インシデントは部分的に実現されます。詳細については、監視とインシデント生成 （1983 ページ）を参照してください。

次の図に、サンプルの Firepower システム構成におけるデータ フローを示します。

図 *53 : Firepower Management Center* のデータ フロー



TIDインシデントが完全または部分的に実現されると、システムは設定されたアクション（モニタ、ブロック、部分的なブロック、またはアクションなし）を実行します。詳細については、「アクションに影響を与える要因 （1993 ページ）」を参照してください。

TID およびセキュリティ インテリジェンス

アクセス コントロール ポリシーの一部として、セキュリティ インテリジェンスではレピュテーション インテリジェンスを使用して、IP アドレス、URL、およびドメインとの間の接続をすばやくブロックします。セキュリティ インテリジェンスは、Cisco Talos Intelligence Group（Talos）からの業界をリードする脅威インテリジェンスへのアクセスを一意に提供します。セキュリティ インテリジェンスの詳細については、セキュリティ インテリジェンスについて （1741 ページ）を参照してください。

TID は、サードパーティのソースからのセキュリティ インテリジェンスに基づいて接続をブロックするシステムの機能を次のように拡張します。

- **TIDは、追加のトラフィック フィルタリング基準をサポート**：セキュリティ インテリジェンスは、IP アドレス、URL、および（DNS ポリシーが有効な場合は）ドメイン名に基づいてトラフィックをフィルタリングできるようにします。TIDでも、これらの基準によるフィルタリングをサポートし、SHA-256ハッシュ値に基づくフィルタリングのサポートを追加します。

- **TID は、追加のインテリジェンス取り込み方法をサポート**：セキュリティ インテリジェンスおよびTIDの両方を使用して、フラット ファイルを手動でアップロードするか、サードパーティ ホストからフラット ファイルを取得するようにシステムを構成することで、システムに脅威インテリジェンスをインポートできます。TIDは、これらのフラット ファイルの管理における柔軟性を向上させます。また、TID は Structured Threat Information eXpression（STIX™）形式で提供されるインテリジェンスを取得して取り込むことができます。

- **TID は、フィルタリング処理のきめ細かい制御を提供**：セキュリティ インテリジェンスにより、ネットワーク、URL、または DNS オブジェクトによるフィルタリング基準を指定できます。セキュリティ インテリジェンス オブジェクト（特にリストおよびフィード）には、複数の IP アドレス、URL、DNS ドメイン名を含めることができますが、ブラック

リストまたはホワイトリストに含めることができるのは、オブジェクトの個別のコンポーネント単位ではなく、オブジェクト単位です。TIDを使用すると、個別の基準（つまり簡易インジケータまたは個別のオブザーバブル）に対するフィルタリング処理を構成できます。

- **TID 構成の変更には再展開は不要**：アクセス コントロール ポリシーでセキュリティ インテリジェンス設定を変更したら、管理対象デバイスに変更された構成を再展開する必要があります。TID では、管理対象デバイスへのアクセス コントロール ポリシーの初期展開後に、ソース、インジケータ、およびオブザーバブルを再展開せずに構成でき、システムによって新しい TID データが要素に自動的に公開されます。

セキュリティ インテリジェンスまたは TID が特定のインシデントに対処できるときに、システムがどのように機能するかについては、TID-Firepower Management Center のアクションの優先順位付け （1994 ページ）を参照してください。

Threat Intelligence Director のパフォーマンスへの影響

Firepower Management Center

いくつかのケースで、次のような場合があります。

- 特に大きな STIX ソースを取り込んでいる間にシステムのパフォーマンスがわずかに低下することがあり、取り込みが完了するまでに時間がかかることがあります。
- 新しいまたは変更された TID データを要素に公開するまでに、最大 15 分かかることがあります。

管理対象デバイス（Managed Device）

例外的なパフォーマンスの影響はありません。TID は、Firepower Management Center セキュリティ インテリジェンスの機能と同じようにパフォーマンスに影響します。

Cisco Threat Intelligence Director（TID） およびハイ アベイラビリティ構成

ハイ アベイラビリティ構成のアクティブな Firepower Management Center で TID をホスティングする場合、システムは TID 構成と TID データをスタンバイ Firepower Management Center に同期しません。フェールオーバー後にデータを復元できるように、アクティブ Firepower Management Center で TID データの定期的なバックアップを実行することを推奨します。

詳細については、「TIDデータのバックアップおよび復元について（1982ページ）」を参照してください。

Threat Intelligence Director の要件

プラットフォーム、要素、およびライセンスに関する要件

ホスティング プラットフォーム

次の物理および仮想 Firepower Management Center で TID をホスティングできます。

- Firepower システムのバージョン 6.2.2 以降を実行している。
- 最小 15 GB のメモリで構成されている。
- REST API アクセスが有効な状態で構成されている。REST API アクセスの有効化 （1325 ページ）を参照してください。

要素

デバイスが Firepower システムのバージョン 6.2.2 以降を実行している場合は、任意の Firepower Management Center 管理対象デバイスを TID 要素として使用できます。

ライセンシング

SHA-256 のオブザーバブルの公開用のファイル ポリシーを設定する場合は、Firepower システムにマルウェア ライセンス（従来またはスマート）が必要です。

詳細については、TID をサポートするためのポリシーの設定 （1974 ページ）およびFirepower ライセンスについて （93 ページ）を参照してください。

ソース要件

ソース タイプの要件：

STIX

ファイルは、STIX バージョン 1.0、1.1、1.1.1、または 1.2 であり、STIX ドキュメントのガイドライン（http://stixproject.github.io/documentation/suggested-practices/）に準拠していなければなりません。

STIX ファイルには複雑なインジケータを含めることができます。

フラット ファイル（Flat File）

ファイルは、1 行に 1 つのオブザーバブル値を持つ ASCII テキスト ファイルでなければなりません。

フラットファイルには、簡易インジケータ（インジケータごとに1つのオブザーバブル）しか含まれていません。

TID では、以下はサポートされません。

- オブザーバブル値を区切る区切り文字（たとえば、`observable,` は無効です）。
- オブザーバブル値を囲む囲み文字（たとえば、`"observable"` は無効です）。

各ファイルには、コンテンツ タイプを 1 つしか含めることができません。

- `SHA-256`：SHA-256 ハッシュ値。
- `Domain`：RFC 1035 で規定されているドメイン名。
- `URL`：RFC 1738 で規定されている URL。

（注） TIDは、ポート、プロトコル、または認証情報を含むURLを正規化し、インジケータを検出するときに正規化されたバージョンを使用します。たとえば、TID は次の URL を正規化します。

```
http://google.com/index.htm
http://google.com:8080/index.htm
google.com:8080/index.htm
google.com/index.htm
```

as:

```
google.com/index.htm
```

または、TID はたとえば次の URL を正規化します。

```
http://abc@google.com:8080/index.htm
```

これを次のように更新します。

```
abc@google.com/index.htm/
```

- `IPv4`：RFC 791 で規定されている IPv4 アドレス。

  TID は CIDR ブロックを受け入れません。

- `IPv6`：RFC 4291 で規定されている IPv6 アドレス。

  TID はプレフィックス長を受け入れません。

ソースの配信要件：

アップロードするファイルとしては、500 MB 以下のものが可能です。

ソース コンテンツの制限事項

システムにより、URL オブザーバブルの最初の 1000 文字のみが取り込まれ、照合されます。

Cisco Threat Intelligence Director（TID） のセットアップ方法

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	グローバル	管理/Threat Intelligence Director（TID）ユーザ

（注） TID の設定や操作中に問題が発生した場合は、Cisco Threat Intelligence Director（TID） のトラブルシューティング （2019 ページ）を参照してください。

ステップ 1 インストールしたものが TID を実行するための要件を満たしていることを確認します。

プラットフォーム、要素、およびライセンスに関する要件 （1971 ページ）を参照してください

ステップ 2 管理対象デバイスごとに、TID をサポートするために必要なポリシーを設定し、それらのポリシーをデバイスに展開します。

TID をサポートするためのポリシーの設定 （1974 ページ）を参照してください。

インテリジェンス データ ソースを取り込む前または後で要素を設定できます。

ステップ 3 TID で取り込むインテリジェンス ソースを設定します。

ソース要件 （1971 ページ）とデータ ソースを取り込むためのオプション （1975 ページ）の下のトピックを参照してください。

ステップ 4 要素にデータをまだ公開していない場合は、公開します。ソース、インジケータ、またはオブザーバブル レベルでの TID データの一時停止または公開 （2015 ページ）を参照してください。

次のタスク

- 定期的にスケジュールされたバックアップに TID を含めます。TID データのバックアップおよび復元について （1982 ページ）を参照してください。

  Firepower Management Center の展開がハイ アベイラビリティ構成である場合は、Cisco Threat Intelligence Director（TID） およびハイ アベイラビリティ構成 （268 ページ） も参照してください。

- （オプション）必要に応じて、TID 機能に管理アクセスを付与します。TID アクセス権を持つユーザ ロール （1982 ページ）および管理アクセス用のユーザ アカウント （51 ページ）を参照してください。
- 操作中に必要に応じて、設定を微調整します。たとえば、誤検出インシデントを生成するオブザーバブルをホワイトリストに登録します。Cisco Threat Intelligence Director（TID）設定の表示および変更 （2000 ページ）を参照してください。

TID をサポートするためのポリシーの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	グローバル	管理/Threat Intelligence Director（TID）ユーザ

Firepower Management Center から管理対象デバイス（要素）に TID データを公開するには、アクセス コントロール ポリシーを設定する必要があります。さらに、最大限のオブザベーションおよび Firepower Management Center イベント生成を行うためにアクセス コントロール ポリシーを設定することを推奨します。

TID をサポートする各管理対象デバイスに対し、次の手順を実行して関連付けられたアクセス コントロール ポリシーを設定します。

データが公開された後に TID を使用するように設定されている要素は、現在公開されているすべてのオブザーバブルを自動的に受信します。

ステップ 1 アクセス コントロール ポリシーの [詳細設定（Advanced Settings）] タブで、[Threat Intelligence Director を有効にする（Enable Threat Intelligence Director）] チェックボックスがオンになっていることを確認します。このオプションは、デフォルトで有効です。

詳細については、アクセス コントロール ポリシーの詳細設定 （1681 ページ）を参照してください。

ステップ 2 まだ設定されていない場合は、アクセス コントロール ポリシーにルールを追加します。TID では、アクセス コントロール ポリシーで 1 つ以上のルールを指定する必要があります。

詳細については、基本的なアクセス コントロール ポリシーの作成 （1673 ページ）を参照してください。

ステップ 3 アクセス コントロール ポリシーのデフォルト アクションとして [侵入防御（Intrusion Prevention）] を選択し、TID 検出のためにトラフィックを復号する場合は、SSL ポリシーをアクセス コントロール ポリシーに関連付けます。アクセス制御への他のポリシーの関連付け （1684 ページ）を参照してください。

ステップ 4 SHA-256 オブザーバブルにオブザベーションおよび Firepower Management Center イベントを生成させる場合：

a) 1 つ以上の [マルウェアクラウドルックアップ（Malware Cloud Lookup）] または [マルウェアブロック（Block Malware）] ファイル ルールを含むファイル ポリシーを作成します。

詳細については、マルウェア保護のためのアクセス コントロール ルールの設定 （1712 ページ）を参照してください。

b) このファイル ポリシーを、アクセス コントロール ポリシーの 1 つ以上のルールと関連付けます。

ステップ 5 [IPv4]、[IPv6]、[URL]、または [ドメイン名（Domain Name）] のオブザベーションで接続およびセキュリティ インテリジェンス イベントを生成する場合は、アクセス コントロール ポリシーで接続およびセキュリティ インテリジェンスのロギングを有効にします。

a) ファイル ポリシーを呼び出したアクセス コントロール ルールで、[接続の終了時にロギング（Log at End of Connection）] および [ファイル イベント：ログファイル（File Events: Log Files）] を有効にします（まだ有効になっていない場合）。

詳細については、アクセス制御ルールによる接続のロギング （3017 ページ）を参照してください。

b) セキュリティ インテリジェンス設定でデフォルトのロギング（[DNS ポリシー（DNS Policy）]、[ネットワーク（Networks）]、および [URL（URLs）]）が有効になっていることを確認します。

詳細については、セキュリティ インテリジェンスによる接続のロギング （3016 ページ）を参照してください。

ステップ 6 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

次のタスク

残りの項目を入力します。Cisco Threat Intelligence Director（TID） のセットアップ方法 （1973 ページ）

データ ソースを取り込むためのオプション

使用するデータ タイプと配信メカニズムに基づいて構成オプションを選択します。

これらのデータ タイプの詳細については、ソース要件 （1971 ページ） を参照してください。

表 *122 :* データ ソースを取り込むためのオプション

データ タイプ	取り込みオプション
STIX	• TAXII サーバからの STIX フィードの取り込み： ソースとして使用する TAXII フィードの取得 （1976 ページ）を参照してください • URL からの STIX データのダウンロード： URL からのソースの取得 （1977 ページ）を参照してください • STIX ファイルのアップロード： ソースとして使用するローカル ファイルのアップロード （1979 ページ）を参照してください

データ タイプ	取り込みオプション
フラット ファイル	• URL からのデータのダウンロード： URL からのソースの取得 （1977 ページ）を参照してください • フラット ファイルのアップロード： ソースとして使用するローカルファイルのアップロード （1979ページ）を参照してください

ソースとして使用する TAXII フィードの取得

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	グローバル	管理/Threat Intelligence Director（TID）ユーザ

TID の設定や操作中に問題が発生した場合は、を参照してください。 Cisco Threat Intelligence Director（TID） のトラブルシューティング （2019 ページ）

ステップ 1 次の要件をソースが満たしていることを確認します。 ソース要件 （1971 ページ）

ステップ 2 **[インテリジェンス（Intelligence）] > [ソース（Sources）]** の順に選択します。

ステップ 3 追加アイコン（＋）をクリックします。

ステップ 4 ソースの [配信（Delivery）] 方法として [TAXII] を選択します。

ステップ 5 情報を入力します。

- ホスト サーバで暗号化された接続が必要な場合は、TID ソースの TLS/SSL 設定の構成 （1980 ページ）の説明に従って [SSL 設定（SSL Settings）] を構成します。
- TAXII ソースの [アクション（Action）] 選択を変更することはできません。

  STIX データに（システムがブロックできない）複雑なインジケータが含まれている可能性があるため、TAXII ソースの `Block` が [アクション（Action）] オプションになりません。デバイス（要素）は、単一のオブザーバブルに基づいて保存してアクションを実行します。複数のオブザーバブルに基づいてアクションを実行することはありません。

  ただし、取り込み後は、個々のオブザーバブルと、そのソースから取得した簡易インジケータをブロックすることができます。詳細については、ソース、インジケータ、またはオブザーバブル レベルでの TID アクションの編集 （2013 ページ）を参照してください。
- フィードのリストが読み込まれるまでには時間がかかることがあります。
- [更新頻度（Update Every）] 間隔は、TID が TAXII ソースから更新を取得する頻度を指定します。

データ ソースを更新する有効な更新頻度を設定します。たとえば、ソースを 1 日に 3 回更新する場合、更新間隔を 1440/3 または 480 分に設定して、定期的に最新データをキャプチャします。

- [TTL] に指定された日数の経過後に、TID が以下のものを削除します。
  - 以降のソース更新に含まれないソースのインジケータのすべて。
  - 残ったインジケータによって参照されないすべてのオブザーバブル。

ステップ 6 要素への公開をすぐに開始する場合は、[公開（Publish）] スライダ（  ）が有効になっていることを確認します。

このオプションを有効にすると、システムは自動的に初期ソース データとそれに続く変更を公開します。

詳細は、ソース、インジケータ、またはオブザーバブル レベルでの TID データの一時停止または公開 （2015 ページ）を参照してください。

ステップ 7 [保存（Save）] をクリックします。

次のタスク

- TAXII フィードには大量のデータが含まれている可能性があるため、システムがすべてのデータを取り込むまでに時間がかかることがあります。取り込みステータスを表示するには、[ソース（Sources）] ページを更新します。
- このソースのエラーが表示される場合は、ステータス アイコンにマウスオーバーすると詳細を確認できます。
- 初期の TID 設定を行っている場合は、Cisco Threat Intelligence Director（TID） のセットアップ方法 （1973 ページ） に戻ります。

URL からのソースの取得

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	グローバル	管理/Threat Intelligence Director（TID）ユーザ

TID でホストからファイルを取得する場合は、URL ソースを設定します。

TID の設定や操作中に問題が発生した場合は、を参照してください。 Cisco Threat Intelligence Director（TID） のトラブルシューティング （2019 ページ）

ステップ 1 次の要件をソースが満たしていることを確認します。 ソース要件 （1971 ページ）

ステップ 2 **[インテリジェンス（Intelligence）]** > **[ソース（Sources）]** の順に選択します。

ステップ 3 追加アイコン（＋）をクリックします。

ステップ 4 ソースの [配信（Delivery）] 方法として [URL] を選択します。

ステップ 5 フォームに入力します。

- フラット ファイルを取り込む場合は、ソース内に含まれるデータを記述する [コンテンツ（Content）] タイプを選択します。
- ホスト サーバで暗号化された接続が必要な場合は、TID ソースの TLS/SSL 設定の構成 （1980 ページ）の説明に従って **SSL 設定**を構成します。
- 名前の場合：インジケータに基づいてインシデントの並び替えと処理を簡単にするには、 TID送信元全体に一貫した命名スキームを使用します。たとえば、 <source>-<type>。

  ソース名も追加すると、追加の情報やフィードバックのためにソースに返信することが簡単になります。

  一貫性のある名前を入力してください。たとえば、IPv4 アドレスを含むソースの場合、常に IPV4 を使用します（IPv4、ipv4、IP_v4、IP_V4、ip-v4、IP-v4、IP-V4 などは使用しません）。
- STIX ファイルを取り込む場合は、STIX データに（システムがブロックできない）複雑なインジケータが含まれている可能性があるため、`Block` が [アクション（Action）] オプションになりません。デバイス（要素）は、単一のオブザーバブルに基づいて保存してアクションを実行します。複数のオブザーバブルに基づいてアクションを実行することはありません。

  ただし、取り込み後は、個々のオブザーバブルと、そのソースから取得した簡易インジケータをブロックすることができます。詳細については、ソース、インジケータ、またはオブザーバブル レベルでの TID アクションの編集 （2013 ページ）を参照してください。
- データ ソースを更新する有効な更新頻度を設定します。たとえば、ソースを 1 日に 3 回更新する場合、更新間隔を 1440/3 または 480 分に設定して、定期的に最新データをキャプチャします。
- [TTL] 間隔に指定された日数の経過後に、TID が以下のものを削除します。
  - 以降のソース更新に含まれないソースのインジケータのすべて。
  - 残ったインジケータによって参照されないすべてのオブザーバブル。

ステップ 6 要素への公開をすぐに開始する場合は、[公開（Publish）] スライダ（  ）が有効になっていることを確認します。

このオプションを有効にすると、システムは自動的に初期ソース データとそれに続く変更を公開します。

詳細は、ソース、インジケータ、またはオブザーバブル レベルでの TID データの一時停止または公開 （2015 ページ）を参照してください。

ステップ 7 [保存（Save）] をクリックします。

次のタスク

- 取り込みステータスを表示するには、[ソース（Sources）]ページを更新します。エラーが表示される場合は、ステータス アイコンにマウスオーバーすると詳細を確認できます。
- 初期の TID 設定を行っている場合は、Cisco Threat Intelligence Director（TID） のセットアップ方法 （1973 ページ） に戻ります。

ソースとして使用するローカル ファイルのアップロード

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	グローバル	管理/Threat Intelligence Director（TID）ユーザ

この手順は、ローカル ファイルのワンタイム手動アップロードに使用します。

STIX ファイルを取り込むと、TID によって STIX ファイルの内容から単純または複雑なインジケータが作成されます。

フラット ファイルを取り込むと、TID によってファイル内のオブザーバブル値ごとに簡易インジケータが作成されます。

TID の設定や操作中に問題が発生した場合は、Cisco Threat Intelligence Director（TID） のトラブルシューティング （2019 ページ）を参照してください。

ステップ 1 の要件をファイルが満たしていることを確認します。 ソース要件 （1971 ページ）

ステップ 2 **[インテリジェンス（Intelligence）] > [ソース（Sources）]** の順に選択します。

ステップ 3 追加アイコン（**+**）をクリックします。

ステップ 4 ソースの [配信（Delivery）] 方法として [アップロード（Upload）] を選択します。

ステップ 5 フォームに入力します。

- フラット ファイルをアップロードする場合は、ソース内に含まれるデータを記述する [コンテンツ（Content）] タイプを選択します。
- 名前の場合：インジケータに基づいてインシデントの並び替えと処理を簡単にするには、 TID送信元全体に一貫した命名スキームを使用します。たとえば、 <source>-<type>。

  ソース名も追加すると、追加の情報やフィードバックのためにソースに返信することが簡単になります。

  一貫性のある名前を入力してください。たとえば、IPv4 アドレスを含むソースの場合、常に IPV4 を使用します（IPv4、ipv4、IP_v4、IP_V4、ip-v4、IP-v4、IP-V4 などは使用しません）。
- STIX ファイルをアップロードする場合は、STIX データに複雑なインジケータが含まれている可能性があるため、`Block`が [アクション（Action）] オプションになりません。デバイス（要素）は、単一の

オブザーバブルに基づいて保存してアクションを実行します。複数のオブザーバブルに基づいてアクションを実行することはありません。

ただし、インジケータまたはオブザーバブル レベルで簡易インジケータをブロックすることはできます。詳細については、ソース、インジケータ、またはオブザーバブル レベルでの TID アクションの編集 （2013 ページ）を参照してください。

- [TTL] 間隔に指定された日数の経過後に、TID が以下のものを削除します。
  - 以降のアップロードに含まれないソースのインジケータのすべて。
  - 残ったインジケータによって参照されないすべてのオブザーバブル。

ステップ 6 要素への公開をすぐに開始する場合は、[公開（Publish）]スライダ（  ）が有効になっていることを確認します。

取り込み時にソースを公開しない場合、後ですべてのソース インジケータを一度に公開することはできません。代わりに、各オブザーバブルを個別に公開する必要があります。ソース、インジケータ、またはオブザーバブル レベルでの TID データの一時停止または公開 （2015 ページ）を参照してください。

ステップ 7 [保存（Save）] をクリックします。

次のタスク

- 取り込みステータスを表示するには、[ソース（Sources）]ページを更新します。エラーが表示される場合は、ステータス アイコンにマウスオーバーすると詳細を確認できます。
- 初期の TID 設定を行っている場合は、Cisco Threat Intelligence Director（TID） のセットアップ方法 （1973 ページ） に戻ります。

TID ソースの TLS/SSL 設定の構成

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	グローバル	管理/Threat Intelligence Director（TID）ユーザ

ホスト サーバで暗号化された接続が必要な場合は、**SSL 設定**を構成します。

始める前に

- ソースとして使用する TAXII フィードの取得 （1976 ページ） またはURL からのソースの取得 （1977 ページ） の説明に従って、`TAXII` または `URL` ソースの設定を開始します。

ステップ 1 [ソースの編集（Edit Source）] ダイアログで、[SSL 設定（SSL Settings）] セクションを展開します。

ステップ 2 サーバ証明書が自己署名されている場合：

a) [自己署名証明書（Self-Signed Certificate）] を有効にします。

b) [SSL ホスト名検証（SSL Hostname Verification）] 方式を選択します。

- [厳格（Strict）]：TID では、ソース **URL** がサーバ証明書に指定されたホスト名と一致する必要があります。

  ホスト名にワイルドカードが含まれる場合、TID は複数のサブドメインと一致することはできません。

- [ブラウザ互換性あり（Browser Compatible）]：TID では、ソース **URL** がサーバ証明書に指定されたホスト名と一致する必要があります。

  ホスト名にワイルドカードが含まれる場合、TID はすべてのサブドメインに一致します。

- [すべて許可（Allow All）]：TID では、ソース **URL** がサーバ証明書に指定されたホスト名と一致する必要はありません。

たとえば、`subdomain1.subdomain2.cisco.com` がソース **URL** で、`*.cisco.com` がサーバ証明書で指定されたホスト名である場合は、次のようになります。

- [厳格（Strict）] ホスト名検証は失敗します。
- [ブラウザ互換性あり（Browser Compatible）] ホスト名検証は成功します。
- [すべて許可（Allow All）] ホスト名検証では、ホスト名の値は完全に無視されます。

c) [サーバ証明書（Server Certificate）] の場合：

- PEM エンコードおよび自己署名されたサーバ証明書にアクセスできる場合は、テキスト エディタで証明書を開き、`BEGIN CERTIFICATE` 行と `END CERTIFICATE` 行を含むテキスト ブロック全体をコピーします。この文字列全体をフィールドに入力します。
- 自己署名されたサーバ証明書にアクセスできない場合は、フィールドを空白のままにします。ソースを保存すると、TID はサーバから証明書を取得します。

ステップ 3 サーバにユーザ証明書が必要な場合：

a) [ユーザ証明書（User Certificate）] を入力します。

テキスト エディタで PEM エンコードされた証明書を開いて、`BEGIN CERTIFICATE` 行と `END CERTIFICATE` 行を含むテキストのブロック全体をコピーします。この文字列全体をフィールドに入力します。

b) [ユーザ秘密キー（User Private Key）] を入力します。

テキストエディタで秘密キーファイルを開き、BEGIN RSA PRIVATE KEYおよびEND RSA PRIVATE KEY 行を含むテキスト ブロック全体をコピーします。この文字列全体をフィールドに入力します。

次のタスク

- 証明書の有効期限を記録します。現在の証明書の有効期限が切れた後に、新しいサーバ証明書を入力するためのカレンダー通知を設定することもできます。
- ソースの設定を続けます。
  - ソースとして使用する TAXII フィードの取得 （1976 ページ）
  - URL からのソースの取得 （1977 ページ）

TID アクセス権を持つユーザ ロール

Firepower Management Center ユーザ アカウントを使用して、TID のメニューやページにアクセスすることができます。

- [管理者（Admin）] または [Threat Intelligence Director ユーザ（Threat Intelligence Director User）] のユーザ ロールを持つアカウント。
- [インテリジェンス（Intelligence）] 権限を含むカスタム ユーザ ロールを持つアカウント。

さらに、[管理者（Admin）]、[アクセス管理者（Access Admin）]、または [ネットワーク管理者（Network Admin）] のユーザ ロールを持つ Firepower Management Center ユーザ アカウントを使用して、アクセス コントロール ポリシーで TID を有効または無効にすることができます。

ユーザ アカウントの詳細については、管理アクセス用のユーザ アカウント （51 ページ）を参照してください。

TID データのバックアップおよび復元について

Firepower Management Center を使用して、TID に必要なすべてのデータ（要素データ、セキュリティ インテリジェンス イベント、接続イベント、TID 構成、および TID データ）をバックアップおよび復元できます。詳細については、バックアップと復元 （199 ページ）を参照してください。

（注） ハイ アベイラビリティ構成のアクティブな Firepower Management Center で TID をホスティングする場合、システムは TID 構成と TID データをスタンバイ Firepower Management Center に同期しません。フェールオーバー後にデータを復元できるように、アクティブ Firepower Management Center で TID データの定期的なバックアップを実行することを推奨します。

表 *123 : TID* 関連のバックアップおよび復元ファイルの内容

TID 関連ファイルの内容	バックアップの選択	復元の選択
要素データ	バックアップ構成	設定データの復元（Restore Configuration Data）
Firepower Management Center イベント データ	イベントのバックアップ	イベント データの復元（Restore Event Data）
TID 構成および TID データ	Threat Intelligence Director のバックアップ	Threat Intelligense Director データの復元

TID インシデントおよびオブザベーション データの分析

TID 要素によって生成されたインシデントおよびオブザベーションデータを分析するには、インシデント表およびインシデント詳細ページを使用します。

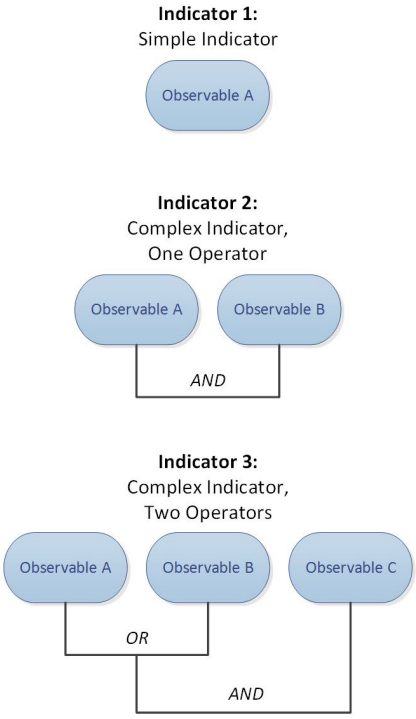
監視とインシデント生成

TIDは、インジケータに対する最初のオブザーバブルがトラフィックに見られたときにインシデントを生成します。単一の監視後、簡易インジケータが完全に実現されます。複雑なインジケータは、1 つ以上の追加の監視がそのパターンを実行するまで、部分的に実現されます。複雑なインジケータは、必ずしも単一のトランザクション中に達成される必要はありません。各オブザーバブルは、異なるトランザクションにより、時間の経過とともに個別に達成できます。

（注） TIDは、インジケータのパターンを評価するときに、サポートされていない、無効な、およびホワイトリストに登録されたオブザーバブルを無視します。

インシデントが完全に実現された後、その後の監視で新しいインシデントがトリガーされます。

図 *54 :* 例：インジケータ パターン



TIDが上記の例からのオブザーバブルを取り込み、オブザーバブルが順番に確認されると、インシデント生成は次のように進行します。

1. システムがトラフィック中のオブザーバブル A を識別すると、TID は次のようになります。
   - インジケータ 1 に対して完全に実現されたインシデントを生成します。
   - インジケータ 2 とインジケータ 3 に対して、部分的に実現されたインシデントを生成します。
2. システムがトラフィック中のオブザーバブル B を識別すると、TID は次のようになります。
   - インジケータ 2 については、パターンが達成されたのでインシデントを [完全に実現（fully-realized）] に更新します。
   - インジケータ 3 については、インシデントを [部分的に実現（partially-realized）] に更新します。
3. システムがトラフィック中のオブザーバブル C を識別すると、TID は次のようになります。
   - インジケータ 3 については、パターンが達成されたのでインシデントを [完全に実現（fully-realized）] に更新します。

4. システムがオブザーバブル A をもう一度識別すると、TID は次のようになります。
   - インジケータ 1 に対して新しい完全に実現されたインシデントを生成します。
   - インジケータ 2 とインジケータ 3 に対して、新しい部分的に実現されたインシデントを生成します。

特定のインジケータが複数のソースに存在する場合、重複インシデントが表示される場合があります。詳細については、Cisco Threat Intelligence Director（TID） のトラブルシューティング（2019 ページ）を参照してください。

インシデントは実際のトラフィックによってのみ生成されることに注意してください。URL B のオブザーバブルがあり、ユーザが URL B へのリンクを表示する URL A にアクセスした場合は、ユーザが URL B のリンクをクリックしない限り、インシデントは発生しません。

インシデントの表示と管理

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	グローバル	管理/Threat Intelligence Director（TID）ユーザ

[インシデント（Incidents）] ページには、最大 110 万件の最新の TID インシデントに関する要約情報が表示されます。（インシデント サマリー情報 （1986 ページ）を参照）。

始める前に

- Cisco Threat Intelligence Director（TID） のセットアップ方法 （1973 ページ）の説明に従って機能を設定します。
- 監視とインシデント生成 （1983 ページ）の説明を読んで、オブザベーションとインシデント生成について理解します。

ステップ 1 **[インテリジェンス（Intelligence）] > [インシデント（Incidents）]** の順に選択します。

ステップ 2 次のようにインシデントを確認します。

- 1 つ以上のフィルタを追加するには、[フィルタ（Filter）] アイコン（🔍）をクリックします。デフォルトのフィルタは 6 時間です。詳細については、テーブル ビューでの TID データのフィルタ処理 （2010 ページ）を参照してください。
- TID でインシデントが最後に更新された日時を表示するには、[最終更新日（Last Updated）] 列内の値の上にカーソルを置きます。

- インシデントに関連付けられているインジケータについての詳細を表示するには、[インジケータ名（Indicator Name）]列内のテキストをクリックします（インジケータの表示と管理（2005 ページ）を参照）。

ステップ 3 [インシデントID（Incident ID）] 列の値をクリックして、その他の詳細を表示します。

表示される詳細の説明については、インシデントの詳細（1987 ページ）を参照してください。

- インジケータの詳細を表示するには、ウィンドウ下部の [インジケータ（Indicator）] 見出しのインジケータ値（IP アドレスや SHA-256 の値など）をクリックします。
- オブザベーションの詳細を表示するには、[オブザベーション（Observations）] 見出しのすぐ下のオブザベーションの左にある矢印をクリックします。
- [Security Intelligence Events（セキュリティ インテリジェンス イベント）] ページでこのインシデントを表示するには、オブザベーション詳細セクションで[イベント（Events）] リンクをクリックします。

ステップ 4 （オプション）インシデント詳細ページで詳細情報を入力します。

ヒント：次のオプションの一貫性と有用性を最大化するには、方針を作成したうえで、命名規則、カテゴリの選択、および信頼度レベル基準を文書化します。

- [名前（Name）]、[説明（Description）]および[カテゴリ（Category）]フィールドに任意の値を入力します。
- [信頼度（Confidence）] の評価レベルをクリックします。
- インシデントの調査ステータスを指定するには、[ステータス（Status）]フィールドのドロップダウンリストから値を選択します。

インシデント サマリー情報

[インシデント（Incidents）] ページには、すべての TID インシデントのサマリー情報が表示されます。

表 *124*：インシデント サマリー情報

フィールド	説明
最終更新日	システムまたはユーザが最後にインシデントを更新してからの日数。更新の日時を表示するには、この列の値にマウスオーバーします。

フィールド	説明
[インシデントID（Incident ID）]	インシデントの固有識別子。この ID の形式は次のとおりです。 `<type>-<date>-<number>` • `<type>`：インシデントに関係するインジケータまたはオブザーバブルのタイプ。単純なインジケータの場合、この値はオブザーバブルのタイプ（`IP`（IPv4 または IPv6）、`URL`（URL）、`DOM`（ドメイン）、または `SHA`（SHA-256））を示します。複雑なインジケータの場合、この値は `COM` です。 • `<date>`：インシデントが作成された日付（*yyyymmdd*）。 • `<number>`：インシデント番号。これは、1 日に作成されたインシデントの中での順序を示す番号です。この順序は 0 で始まることに注意してください。たとえば、`DOM-20170828-10` はその日に作成された 11 番目のインシデントです。 識別子の隣には、インシデントが部分的に実現された（）か、完全に実現された（）かを示すアイコンが表示されます。詳細については、監視とインシデント生成（1983 ページ）を参照してください。
[インジケータ名（Indicator Name）]	インシデントに関係するインジケータの名前。インジケータの追加情報を表示するには、この列の値をクリックします。インジケータの表示と管理（2005 ページ）を参照してください。
Type	インシデントに関係するインジケータのタイプ。 • 単一のオブザーバブルを含むインジケータでは、データ型（`URL`、`SHA-256` など）が表示されます。 • 2 つ以上のオブザーバブルを含むインジケータは、`Complex` として表示されます。
[実施アクション（Action Taken）]	インシデントに関してシステムが実行するアクション。詳細については、インシデントの詳細（1987 ページ）を参照してください。
Status（ステータス）	インシデントに関する調査のステータスです。詳細については、インシデントの詳細（1987ページ）を参照してください。
	このアイコンをクリックすると、インシデントが完全に削除されます。

インシデントの詳細

[インシデントの詳細（Incident Details）] ウィンドウには、単一の TID インシデントに関する情報が表示されます。このウィンドウは、2 つのセクションで構成されています。

- インシデントの詳細：基本情報（1988 ページ）
- インシデントの詳細：インジケータとオブザベーション（1989 ページ）

インシデントの詳細：基本情報

[インシデントの詳細（Incident Details）] ウィンドウの上部セクションでは、次の情報が提供されます。

表 *125*：基本的なインシデント情報フィールド

フィールド	説明
IncidentID または *IncidentID*	インシデントのステータス（部分的に実現または完全に実現）およびインシデントの一意の ID を示すアイコン。 （注） TID は、インシデントのステータスを決定するときに、サポートされていない、無効な、およびホワイトリストに登録されたオブザーバブルを無視します。
[既読（Opened）]	インシデントが最後に更新された日時。
Name	手動で入力するオプションのカスタム インシデント名。 ヒント：[説明（Description）]フィールド（ウィンドウの下部）にソースからの情報がある場合は、そのフィールドの情報を使用してインシデントに名前を付けます。
Description	手動で入力するオプションのカスタム インシデント説明。 ヒント：[説明（Description）]フィールド（ウィンドウの下部）にソースからの情報がある場合は、そのフィールドの情報を使用してインシデントについて説明します。
[オブザベーション（Observations）]	インシデント内のオブザベーションの数。
信頼性（Confidence）	インシデントの相対的な重要度を示すために手動で選択できるオプションの評価。
[実施アクション（Action Taken）]	システムによって実行されるアクション：[モニタ済み（Monitored）]、[ブロック済み（Blocked）]、または [部分的にブロック済み（Partially Blocked）]。 [部分的にブロック済み（Partially Blocked）] は、インシデントに [モニタ済み（Monitored）] と [ブロック済み（Blocked）] の両方のオブザベーションが含まれていることを示します。 （注） [実施アクション（Action Taken）] は、システムによって実行されるアクションを示しますが、必ずしも TID で選択されているアクションではありません。詳細については、TID-Firepower Management Center のアクションの優先順位付け （1994 ページ）を参照してください。
カテゴリ（Category）	インシデントに手動で追加するオプションのカスタム タグまたはキーワード。

フィールド	説明
Status（ステータス）	インシデントの分析の現在の段階を示す値。すべてのインシデントは、[ステータス（Status）] を初めて変更するまでは [新規（New）] です。 このフィールドは任意です。組織のニーズに応じて、以下のステータス値を使用することを検討してください。 • [新規（New）]：インシデントには調査が必要ですが、まだ調査を開始していません。 • [オープン（Open）]：現在インシデントを調査しています。 • [クローズ済み（Closed）]：インシデントを調査し、対処しました。 • [却下（Rejected）]：インシデントを調査し、実行するアクションはないと判断しました。
🗑	このアイコンをクリックすると、このインシデントが完全に削除されます。

インシデントの詳細：インジケータとオブザベーション

[インシデントの詳細（Incident Details）] ウィンドウの下部セクションには、インジケータとオブザベーションの詳細情報が表示されます。この情報は、[インジケータ（Indicator）] フィールド、インジケータ パターン、および [オブザベーション（Observations）] フィールドとして編成されています。

[インジケータ（Indicator）] セクション

インジケータの詳細を初めて表示するときには、このセクションにはインジケータ名のみが表示されます。

[インジケータ（Indicator）] ページでインジケータを表示するには、インジケータ名をクリックします。

インジケータ名の隣にある下矢印をクリックすると、インシデントを閉じることなくインジケータの詳細を表示できます。詳細フィールドには、次のものがあります。

表 *126*：インジケータのフィールド

フィールド	説明
Description	ソースから提供されたインジケータの説明。
ソース（Source）	このインジケータを含んでいたソース。このリンクをクリックすると、完全なソースの詳細にアクセスできます。
[有効期限（Expires）]	ソースの [TTL] 値に基づく、インシデントが期限切れになる日時。

フィールド	説明
[操作（Action）]	インジケータに関連付けられたアクション。詳細については、ソース、インジケータ、またはオブザーバブル レベルでの TID アクションの編集（2013 ページ）を参照してください。
パブリッシュ	インジケータのパブリッシュ設定。詳細については、ソース、インジケータ、またはオブザーバブル レベルでの TID データの一時停止または公開（2015 ページ）を参照してください。
[STIX のダウンロード（Download STIX）]	ソース タイプが `STIX` の場合は、このボタンをクリックして STIX ファイルをダウンロードします。

[インジケータ パターン（Indicator Pattern）]

インジケータ パターンは、インジケータを構成するオブザーバブルおよび演算子のグラフィカル表示です。演算子はインジケーター内のオブザーバブルをリンクします。AND 関係は[AND] 演算子で示されます。OR 関係は、[OR] 演算子で示されるか、いくつかのオブザーバブルの密接なグループ化により示されます。

パターンのオブザーバブルがすでに観測されている場合、オブザーバブル ボックスは白色です。オブザーバブルがまだ観測されていない場合、オブザーバブル ボックスは灰色です。

インジケータ パターンで、次のようにします。

- ホワイトリスト アイコン（）をクリックして、オブザーバブルをホワイトリストに追加します。このアイコンは、白色と灰色の両方のオブザーバブル ボックスに表示されます。詳細については、TID オブザーバブルのホワイトリスト登録について（2017 ページ）を参照してください。
- 白色のオブザーバブル ボックスにマウスオーバーすると、[オブザベーション（Observations）] セクションで関連するオブザベーションが強調表示されます。
- 白色のオブザーバブル ボックスをクリックすると、[オブザベーション（Observations）] セクションで関連するオブザベーションが強調表示され、そのオブザベーションがスクロールされて表示されて（複数のオブザベーションが存在する場合）、そのオブザベーションの詳細表示が展開されます。
- インジケータ パターンで灰色のオブザーバブル ボックスをマウスオーバーまたはクリックした場合、[オブザベーション（Observations）] セクションに変化はありません。これは、オブザーバブルがまだ観測されていないため、表示するオブザベーションの詳細がないためです。

[オブザベーション（Observations）] セクション

デフォルトでは、[オブザベーション（Observations）] セクションには、次のような概要情報が表示されます。

- オブザベーションをトリガーしたオブザーバブルのタイプ（たとえば、[ドメイン（Domain）]）
- オブザーバブルを構成するデータ
- オブザベーションが最初のオブザベーションか、それ以降のオブザベーションか（たとえば、[最初の（1st）] または [3 つ目（3rd）]）

（注） 1 つのオブザーバブルが 3 回以上観測された場合、TID では最初と最後のオブザベーションの詳細を表示します。中間のオブザベーションの詳細は表示されません。

- オブザベーションの日時
- オブザーバブルに設定されているアクション

[オブザベーション（Observations）]セクションでオブザベーションにマウスオーバーすると、インジケータ パターンの関連するオブザーバブルが強調表示されます。

[オブザベーション（Observations）]セクションでオブザベーションをクリックした場合は、インジケータ パターンで関連するオブザーバブルが強調表示され、関連する最初のオブザーバブルがスクロールされて表示されます（複数のオブザーバブルが存在する場合）。また、オブザベーションをクリックすると、[オブザベーション（Observations）] セクションのオブザベーションの詳細が展開されます。

オブザベーションの詳細には、次のようなフィールドがあります。

表 *127*：オブザベーションの詳細のフィールド

フィールド	説明
[送信元（SOURCE）]	オブザベーションをトリガーしたトラフィックの送信元 IP アドレスおよびポート。
DESTINATION	オブザベーションをトリガーしたトラフィックの宛先 IP アドレスおよびポート。
[その他の情報（ADDITIONAL INFORMATION）]	オブザベーションをトリガーしたトラフィックに関連する DNS および認証情報。
イベント	このクリッカブル リンクは、オブザベーションによって接続、セキュリティ インテリジェンス、ファイル、またはマルウェア イベントが生成された場合に表示されます。リンクをクリックして、Firepower Management Center イベント テーブルでイベントを表示します。接続イベントについて（3021ページ）を参照してください。

TID オブザベーションのイベントの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	グローバル	管理/Threat Intelligence Director（TID）ユーザ

TID オブザベーションによって生成される Firepower Management Center イベントについて詳しくは、Firepower Management Center イベントでの TID オブザベーション （1992 ページ） を参照してください。

TID 関連のイベントについてログに記録されるシステム アクションは、TID の相互作用やその他の Firepower Management Center 機能によって異なります。アクションの優先順位付けについて詳しくは、TID-Firepower Management Center のアクションの優先順位付け （1994 ページ） を参照してください。

始める前に

- Cisco Threat Intelligence Director（TID） のセットアップ方法 （1973 ページ） の説明に従って機能を設定します。
- TID をサポートするためのポリシーの設定 （1974 ページ） の説明に従って、アクセス コントロール ポリシーで TID に必要なイベント ロギングを有効にしたことを確認します。

ステップ 1 **[インテリジェンス（Intelligence）] > [インシデント（Incidents）]** の順に選択します。

ステップ 2 インシデントの [インシデント ID（Incident ID）] 値をクリックします。

ステップ 3 [インジケータ（Indicator）] セクションでオブザベーションをクリックして、オブザベーション ボックスを表示します。

ステップ 4 オブザベーション ボックスの左上隅にある矢印をクリックしてボックスを展開します。

ステップ 5 オブザベーション情報で [イベント（Events）] リンクをクリックします。セキュリティ インテリジェンスの表示内容について詳しくは、接続イベントについて （3021 ページ） を参照してください。

Firepower Management Center イベントでの TID オブザベーション

アクセス コントロール ポリシーを完全に制御する場合、TID オブザベーションによって、次の Firepower Management Center イベントが生成されます。

表 *128* : オブザベーションによって生成される *Firepower Management Center* イベント

オブザベーションの内容	接続イベントの表	セキュリティ インテリジェンス イベントの表	ファイル イベントの表	マルウェア イベントの表
SHA-256	あり	なし	あり	○（判定結果がマルウェアまたはカスタム検出の場合）。
[ドメイン名（Domain Name）]、[URL]、または [IPv4/IPv6]	○ TID 関連の接続イベントは、TID 関連の [セキュリティ インテリジェンス カテゴリ（Security Intelligence Category）] 値によって識別されます。	○ TID 関連のセキュリティ インテリジェンス イベントは、TID 関連の [セキュリティ インテリジェンス イベント（Security Intelligence Category）] 値により識別されます。	なし	なし

アクションに影響を与える要因

システムがアクションを取るタイミングや、TIDオブザーバブルと一致するトラフィックを検出したときにシステムが取るアクションは多くの要因によって決定されます。

- セキュリティ インテリジェンスのような機能は、TIDがアクションを起こす前にアクションを起こします。詳細は、TID-Firepower Management Center のアクションの優先順位付け（1994 ページ）を参照してください。
- 実行されるアクションは一般に、オブザーバブルに対して構成されたアクション（親インジケータまたはソースに対して構成されたアクションとは異なる可能性がある）となります。
- STIX ソースには複雑なインジケータが含まれている可能性があるため、ソースのアクション設定は [モニタ（Monitor）] にのみ設定できます。ただし、STIX フィードまたはファイルに含まれている個々の簡易インジケータまたはオブザーバブルは [ブロック（Block）] に設定できます。
- インジケータおよびオブザーバブルのアクション設定は、継承するかまたは継承をオーバーライドするように個別に設定できます。TID設定における継承（2011ページ）およびソース、インジケータ、またはオブザーバブル レベルでの TID アクションの編集（2013 ページ）を参照してください。
- それ以外の場合、アクション可能なトラフィックはホワイトリストに登録される可能性があります。詳細は、TIDオブザーバブルのホワイトリスト登録（2018ページ）を参照してください。

- 設定されたアクションは、部分的および完全に実現されたインシデントの両方に対して実行されます。
- 複雑なインジケータに基づくインシデントは部分的にブロックできます。これは、インジケータにモニタ対象のオブザーバブルとブロックされたオブザーバブルの両方が含まれている場合に発生する可能性があります。
- 公開の一時停止は、システムが実行するアクションに影響します。公開の一時停止について （2014 ページ）およびソース、インジケータ、またはオブザーバブル レベルでの TID データの一時停止または公開 （2015 ページ）を参照してください。
- TID機能を一時停止すると、すべての操作ができなくなります。この機能を再開した後、実行可能なデータが以前と異なる場合があります。詳細については、「TIDの一時停止と要素からの TID データの消去 （2015 ページ）」を参照してください。

TID-Firepower Management Center のアクションの優先順位付け

TID のオブザーバブル アクションが Firepower Management Center のポリシー アクションと競合する場合は、システムが次のようにアクションに優先順位を付けます。

- セキュリティ インテリジェンス ホワイトリスト
- セキュリティ インテリジェンス ブラックリスト
- TID ブロック （TID Block）
- セキュリティ インテリジェンス ブラックリスト（モニタ）
- TID モニタ

具体的には次のとおりです。

表 *129 : TID URL* 監視可能アクション対セキュリティ インテリジェンス アクション

設定：セキュリティ インテリジェンス アクション	設定：TID 監視可能アクション	TID インシデント フィールド：実行されるアクション	セキュリティ インテリジェンス イベントのフィールド：		
			操作	セキュリティ インテリジェンス カテゴリ	理由
WHITELIST	[モニタ （Monitor）] または [ブロック （Block）]	TID インシデントなし	セキュリティ インテリジェンス イベントなし		

設定：セキュリティインテリジェンス アクション	設定：TID 監視可能アクション	TID インシデント フィールド：実行されるアクション	セキュリティ インテリジェンス イベントのフィールド：		
			操作	セキュリティ インテリジェンス カテゴリ	理由
ブロック（Block）	モニタ	ブロック	ブロック（Block）	システム分析により決定（を参照） セキュリティ インテリジェンス オプション （1746 ページ）	URL Block
	ブロック（Block）	TID インシデントなし	ブロック（Block）	システム分析により決定（を参照） セキュリティ インテリジェンス オプション （1746 ページ）	URL Block
モニタ	モニタ	TID インシデントなし	セキュリティ インテリジェンスと TID の後に処理されたアクセス制御ルールによって決定されます。	システム分析により決定（を参照） セキュリティ インテリジェンス オプション （1746 ページ）	URL Monitor
	ブロック（Block）	ブロック	ブロック（Block）	TID URL ブロック	URL Block

表 *130 : TID IPv4/IPv6* 監視可能アクション対セキュリティ インテリジェンス アクション

設定：セキュリティインテリジェンス アクション	設定：TID 監視可能アクション	TID インシデント フィールド：実行されるアクション	セキュリティ インテリジェンス イベントのフィールド：		
			操作	セキュリティ インテリジェンス カテゴリ	理由
WHITELIST	[モニタ（Monitor）] または [ブロック（Block）]	TID インシデントなし	セキュリティ インテリジェンス イベントなし		

設定：セキュリティ インテリジェンス アクション	設定：TID 監視可能アクション	TID インシデント フィールド：実行されるアクション	セキュリティ インテリジェンス イベントのフィールド：		
			操作	セキュリティ インテリジェンス カテゴリ	理由
ブロック（Block）	モニタ	ブロック	ブロック（Block）	システム分析により決定（を参照） セキュリティ インテリジェンス オプション （1746 ページ）	IP Block
	ブロック（Block）	TID インシデントなし	ブロック（Block）	システム分析により決定（を参照） セキュリティ インテリジェンス オプション （1746 ページ）	IP Block
モニタ	モニタ	TID インシデントなし	セキュリティ インテリジェンスと TID の後に処理されたアクセス制御ルールによって決定されます。	システム分析により決定（を参照） セキュリティ インテリジェンス オプション （1746 ページ）	IP Monitor
	ブロック（Block）	ブロック	ブロック（Block）	TID IPv4 ブロック TID IPv6 ブロック	IP Block

表 *131 : TID* ドメイン名の監視可能アクション対 *DNS* ポリシー アクション

設定：DNS ポリシー アクション	設定：TID ドメイン名の監視可能アクション	TIDインシデント フィールド：実行されるアクション	セキュリティ インテリジェンス イベントのフィールド：		
			操作	セキュリティインテリジェンス カテゴリ	理由
WHITELIST	[モニタ（Monitor）] または [ブロック（Block）]	TID インシデントなし	セキュリティ インテリジェンス イベントなし		
ドロップ、ドメインが見つからない シンクホール：ログ シンクホール：ブロックとログ	モニタ	ブロック	ブロック（Block）	システム分析により決定（を参照）セキュリティインテリジェンス オプション（1746ページ）	DNS ブロック（DNS Block）
	ブロック（Block）	ブロック	ブロック（Block）	TID ドメイン名ブロック	DNS ブロック（DNS Block）
モニタ	モニタ	監視対象	セキュリティインテリジェンスと TID の後に処理されたアクセス制御ルールによって決定されます。	システム分析により決定（を参照）セキュリティインテリジェンス オプション（1746ページ）	DNS モニタ（DNS Monitor）
	ブロック（Block）	ブロック	ブロック（Block）	TID ドメイン名ブロック	DNS ブロック（DNS Block）

表 *132 : TID SHA-256* 監視可能アクション対マルウェア クラウド ルックアップ ファイル ポリシー

ファイル傾向	TID SHA-256 監視可能アクション	TID インシデントで行われるアクション	ファイルイベントでのアクション	マルウェアイベントでのアクション
クリーン（Clean）	[モニタ（Monitor）] または [ブロック（Block）]	監視対象	マルウェア クラウド ルックアップ（Malware Cloud Lookup）	適用対象外

ファイル傾向	TID SHA-256 監視可能アクション	TID インシデントで行われるアクション	ファイルイベントでのアクション	マルウェアイベントでのアクション
マルウェア	[モニタ（Monitor）] または [ブロック（Block）]	監視対象	マルウェア クラウド ルックアップ（Malware Cloud Lookup）	適用対象外
Custom	[モニタ（Monitor）] または [ブロック（Block）]	監視対象	• SHA-256 がカスタム検出リストにない場合は、[マルウェア クラウド ルックアップ（Malware Cloud Lookup）]。 • SHA-256 がカスタム検出リストにある場合は、[カスタム検出（Custom Detection）]。	• SHA-256 がカスタム検出リストにない場合は、[マルウェア クラウド ルックアップ（Malware Cloud Lookup）]。 • SHA-256 がカスタム検出リストにある場合は、[カスタム検出（Custom Detection）]。
不明	[モニタ（Monitor）] または [ブロック（Block）]	監視対象	マルウェア クラウド ルックアップ（Malware Cloud Lookup）	適用対象外

（注） TID の一致は、システムが動的分析用にファイルを送信する前に発生します。

表 *133 : TID SHA-256* 監視可能アクション対マルウェア ブロック ファイル ポリシー

ファイル傾向	TID SHA-256 監視可能アクション	TID インシデントで行われるアクション	ファイルイベントでのアクション	マルウェアイベントでのアクション
[正常（Clean）] または [不明（Unknown）]	モニタ	監視対象	マルウェア クラウド ルックアップ（Malware Cloud Lookup）	適用対象外
	ブロック（Block）	ブロック	• SHA-256 がカスタム検出リストにない場合は、[TID ブロック（TID Block）]。 変更されたファイル性質は [カスタム（Custom）] です。 • SHA-256 がカスタム検出リストにある場合は、[カスタム検出ブロック（Custom Detection Block）]。	TID ブロック（TID Block） 変更されたファイル性質は [カスタム（Custom）] です。

ファイル傾向	TID SHA-256 監視可能アクション	TID インシデントで行われるアクション	ファイルイベントでのアクション	マルウェアイベントでのアクション
[マルウェア（Malware）] または [カスタム（Custom）]	モニタ	ブロック	マルウェア ブロック（Block Malware）	マルウェア ブロック（Block Malware）
	ブロック（Block）	ブロック	• SHA-256 がカスタム検出リストにない場合は、[TID ブロック（TID Block）]。 変更されたファイル性質は [カスタム（Custom）] です。 • SHA-256 がカスタム検出リストにある場合は、[カスタム検出ブロック（Custom Detection Block）]。	TID ブロック（TID Block） 変更されたファイル性質は [カスタム（Custom）] です。

Cisco Threat Intelligence Director（TID） 設定の表示および変更

必要に応じて、次の情報を使用して設定を見直し、微調整します。

要素（管理対象デバイス）の TID ステータスの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	グローバル	管理/Threat Intelligence Director（TID）ユーザ

管理対象デバイスとして Firepower Management Center に登録されているすべてのデバイスは、[要素（Elements）] ページに自動的に表示されます。すべての（TID をサポートするためのポリシーの設定（1974 ページ） で指定されたとおりに）適切に構成された要素は、要素が追加さ

れる前に取り込まれたものを含めて、現在公開されているすべてのオブザーバブルを受信します。

ステップ 1 **[インテリジェンス（Intelligence）] > [要素（Elements）]** を選択します。

ステップ 2 設定した要素を確認します。

- [名前（Name）] の横にあるアイコンは、その要素が接続されて TID が有効になっているかどうかを示します。
- TID が有効化されてこのデバイスに展開されたときのアクセス コントロール ポリシーを確認するには、[アクセス コントロール ポリシー（Access Control Policy）] 列を調べます。詳細については、「TID をサポートするためのポリシーの設定 （1974 ページ）」を参照してください。

ソースの表示と管理

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	グローバル	管理/Threat Intelligence Director（TID）ユーザ

[ソース（Sources）] ページには、設定済みのすべてのソースに関する概要情報が表示されます（ソース サマリー情報 （2002 ページ）を参照）。

ステップ 1 **[インテリジェンス（Intelligence）] > [ソース（Sources）]** の順に選択します。

ステップ 2 ソースを次のように表示します。

- ページに表示されるソースをフィルタリングするには、[フィルタ（Filter）] アイコン（🔍）をクリックします。詳細については、テーブル ビューでの TID データのフィルタ処理 （2010 ページ）を参照してください。
- 詳細な取り込みステータスを表示するには、[ステータス（Status）] 列のテキストの上にカーソルを移動します。詳細については、ソース ステータスの詳細 （2003 ページ）を参照してください。

ステップ 3 ソースを次のように管理します。

- [アクション（Action）] 設定を編集するには、ソース、インジケータ、またはオブザーバブル レベルでの TID アクションの編集 （2013 ページ）を参照してください。固定されているアクションがある場合、ソースの [タイプ（Type）] には、そのアクションだけがサポートされます。

- [公開（Publish）] 設定を編集するには、スライダ（）をクリックします。詳細については、ソース、インジケータ、またはオブザーバブル レベルでの TID データの一時停止または公開 （2015 ページ）を参照してください。
- TID によるソースの更新を一時停止または再開する場合は、[更新の一時停止（Pause Updates）] または [更新の再開（Resume Updates）] をクリックします。更新を一時停止すると、更新は中断されますが、既存のインジケータとオブザーバブルは TID 内に残ります。
- ソースを削除するには、削除アイコン（）をクリックします。ソースが現在処理中の場合、このアイコンはグレー表示になります。ソースを削除すると、そのソースに関連付けられているすべてのインジケータも削除されます。関連付けられているオブザーバブルも削除される可能性があります。ただし、システム内に残っているインジケータに関連付けられたオブザーバブルは保持されます。

ソース サマリー情報

[ソース（Sources）]ページには、設定されているすべてのソースの概要情報が表示されます。次の表で、概要表示に含まれるフィールドについて簡単に説明します。これらのフィールドの詳細については、ソースの関連設定トピックの説明を参照してください。データ ソースを取り込むためのオプション （1975 ページ） を参照してください。

表 *134 :* ソース サマリー情報

フィールド	説明
[名前（Name）]	ソース名。
Type	ソースのデータ形式（[STIX] または [フラットファイル（Flat File）]）。
配信	TID がソースを取得するのに使用する手法。
操作（Action）	このソースに含まれるデータと一致するトラフィックに対してシステムで実行するように設定されているアクション（[ブロック（Block）] または [モニタ（Monitor）]）。 可用性、継承、および継承のオーバーライドを含むTID のアクションの詳細については、アクションに影響を与える要因 （1993 ページ） を参照してください。
パブリッシュ	[オン（On）] または [オフ（Off）] トグル。登録されている要素（TID をサポートするために設定された管理対象デバイス）に TID がソースからのデータを公開するかどうかを指定します。 インジケータは親ソースから [公開（Publish）] 設定を継承でき、オブザーバブルは親インジケータから [公開（Publish）] 設定を継承できます。詳細については、TID 設定における継承 （2011 ページ）を参照してください。
最終更新日	TID が最後にソースを更新した日時。

フィールド	説明
Status（ステータス）	ソースの現在のステータス。 • [新規（New）]：ソースは新規に作成されます。 • [スケジュール済み（Scheduled）]：初回のダウンロードまたはその後の更新がスケジュールされていますが、まだ進行中ではありません。 • [ダウンロード 中（Downloading）]：TID が初回のダウンロードまたは更新を処理中です。 • [解析中（Parsing）] または [処理中（Processing）]（）：TID がソースを取り込んでいます。 • [完了（Completed）]（）：TID はソースの取り込みを終了しました。 • [完了（エラーあり）（Completed with Errors）]（）：TID はソースの取り込みを終了しましたが、一部のオブザーバブルがサポートされていないか無効です。 • [エラー（Error）]（）：TID による処理にエラーが発生しました。[更新間隔（Update Frequency）] が指定された TAXII ソースまたは URL ソースの場合、更新が一時停止でなければ、 TID はスケジュールされている次回の更新で再試行します。 ページを更新してステータスを更新します。
	このアイコンをクリックすると、ソースの設定を編集できます。
	このアイコンをクリックすると、ソースが完全に削除されます。

ソース ステータスの詳細

ソースの概要ページに表示されるソースの [ステータス（Status）] 値にマウスオーバーすると、TID は次の詳細情報を表示します。

データ	説明
ステータス メッセージ	ソースの現在のステータスを簡単に説明します。
最終更新日（Last Updated）	TID が最後にソースを更新した日時を表示します。
次回更新日（Next Update）	TAXII および URL ソースの場合、この値は TID が次にソースを更新する時期を指定します。

データ	説明
インジケータ（Indicators）	インジケータ カウントを表示します。 • [使用済み（Consumed）]：最近のソース更新中に TID が処理したインジケータの数。この数値は、取り込みや破棄が行われたかどうかに関係なく、その更新に含まれていたすべてのインジケータを表します。 • [破棄済み（Discarded）]：最近の更新でシステムが TID に追加しなかった無効なインジケータの数。 （注） `TAXII` ソースの場合、 TID は [最終更新（Last Update）] と [合計（Total）] とに分けてインジケータ数を表示します。これは、TAXII の場合、既存のデータを置換する形式ではなく、増分データを追加する形式で更新が行われるからです。他のソース タイプのインジケータの場合、これらのソースの更新では既存のデータ セットが完全に置換されるので、TID は [最終更新（Last Update）] の値のみを表示します。 あるインジケータのオブザーバブルがすべて [無効（Invalid）] の場合、 TID はそのインジケータを破棄します。
オブザーバブル（Observables）	オブザーバブルの数を表示します。 • [使用済み（Consumed）]：最近のソース更新中に TID が処理したオブザーバブルの数。この数値は、取り込みや破棄が行われたかどうかに関係なく、その更新に含まれていたすべてのオブザーバブルを表します。 • [サポート対象外（Unsupported）]：最近の更新でシステムが TID に追加しなかったサポートされないオブザーバブルの数。 サポートされているオブザーバブルのタイプに関する詳細については、ソース要件（1971 ページ） でコンテンツ タイプに関する情報を参照してください。 • [無効（Invalid）]：最近の更新でシステムが TID に追加しなかった無効なオブザーバブルの数。 オブザーバブルが正しく作成されていない場合は無効になります。たとえば、`10.10.10.10.123` は有効な IPv4 アドレスではありません。 （注） `TAXII` ソースの場合、 TID は [最終更新（Last Update）] と [合計（Total）] とに分けてオブザーバブル数を表示します。これは、TAXII の場合、既存のデータを置換する形式ではなく、増分データを追加する形式で更新が行われるからです。他のソース タイプのオブザーバブルの場合、これらのソースの更新では既存のデータ セットが完全に置換されるので、TID は [最終更新（Last Update）] の値のみを表示します。

インジケータの表示と管理

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	グローバル	管理/Threat Intelligence Director（TID）ユーザ

インジケータは、取り込まれたソースから自動的に生成されます。このページの詳細については、インジケータ サマリー情報 （2006 ページ） を参照してください。

ステップ 1 **[インテリジェンス（Intelligence）] > [ソース（Sources）]** の順に選択します。

ステップ 2 [インジケータ（Indicators）] をクリックします。

ステップ 3 現在のインジケータを次のように表示します。

- ページに表示されるインジケータをフィルタリングするには、[フィルタ（Filter）] アイコン（🔍）をクリックします。詳細については、テーブル ビューでの TID データのフィルタ処理 （2010 ページ）を参照してください。
- インジケータの詳細情報（関連付けられているオブザーバブルなど）を表示するには、インジケータ名をクリックします。詳細については、インジケータの詳細 （2007 ページ）を参照してください。
- インジケータに関連付けられているインシデントについての情報を表示するには、[インシデント（Incidents）] 列内の番号をクリックします。また、アイコンの上にカーソルを移動すると、インシデントが完全に実現されたか、部分的に実現されたかを確認できます。
- ソースからのインジケータの調査が TID で完了したかどうかを判別するには、[ステータス（Status）] 列を確認します。

ステップ 4 現在のインジケータを次のように管理します。

- [アクション（Action）] を編集するには、ソース、インジケータ、またはオブザーバブル レベルでの TID アクションの編集 （2013 ページ）を参照してください。固定されているアクションがある場合、ソースの [タイプ（Type）] には、そのアクションだけがサポートされます。
- [公開（Publish）] 設定を編集するには、ソース、インジケータ、またはオブザーバブル レベルでの TID データの一時停止または公開 （2015 ページ）を参照してください。
- インジケータの 1 つ以上のオブザーバブルをホワイトリストに入れるには、インジケータ名をクリックして [インジケータの詳細（Indicator Details）] ページにアクセスします。詳細については、「TID オブザーバブルのホワイトリスト登録について （2017 ページ）」を参照してください。

インジケータ サマリー情報

[インジケータ（Indicators）]ページには、設定されたソースに関連付けられているすべてのインジケータの概要情報が表示されます。

表 *135*：インジケータ サマリー情報

フィールド	説明
タイプ	• 1 つオブザーバブルを持つインジケータには、そのオブザーバブルのデータ タイプがリストされます（URL、SHA-256 など）。 • 2 つ以上のオブザーバブルを持つインジケータは、[複合（Complex）] としてリストされます。 特定のオブザーバブルを確認するには、タイプの上にカーソルを移動します。
Name	インジケータ名。
ソース（**Source**）	インジケータが含まれていたソース（親ソース）。
[インシデント（**Incidents**）]	インジケータに関連付けられたすべてのインシデントに関する情報。 • インシデントが部分的に実現（）されるか、完全に実現（）されるかを指定するアイコン。 • インジケータに関連付けられたインシデント数。
[操作（**Action**）]	インジケータに関連付けられたアクション。詳細については、ソース、インジケータ、またはオブザーバブル レベルでの TID アクションの編集 （2013 ページ）を参照してください。 インジケータは親ソースから[アクション（Action）]設定を継承でき、オブザーバブルは親インジケータから [アクション（Action）] 設定を継承できます。詳細については、TID 設定における継承 （2011 ページ）を参照してください。
パブリッシュ	インジケータのパブリッシュ設定。詳細については、ソース、インジケータ、またはオブザーバブル レベルでの TID データの一時停止または公開 （2015 ページ）を参照してください。 インジケータは親ソースから[公開（Publish）]設定を継承でき、オブザーバブルは親インジケータから[公開（Publish）]設定を継承できます。詳細については、TID 設定における継承 （2011 ページ）を参照してください。
最終更新日	TID が最後にインジケータを更新した日時。

フィールド	説明
Status（ステータス）	インジケータの現在のステータス。 • [保留中（Pending）]（）：TID はインジケータのオブザーバブルを取り込み中です。 • [完了（Completed）]（）：TID はインジケータのオブザーバブルをすべて正常に取り込みました。 • [完了（エラーあり）（Completed With Errors）]（）：TID はインジケータを取り込みましたが、一部のオブザーバブルがサポートされていないか無効です。

インジケータの詳細

[インジケーターの詳細（Indicator Details）] ページには、インシデントのインジケータとオブザーバブル（監視可能）データが表示されます。

表 *136*：インジケータの詳細情報

フィールド	説明
[名前（Name）]	インジケータ名。
Description	ソースから提供されたインジケータの説明。
ソース（Source）	このインジケータを含んでいたソース。
有効期限	ソースの [TTL] 値に基づく、インジケータが期限切れになる日時。
[操作（Action）]	インジケータに関連付けられたアクション。詳細については、ソース、インジケータ、またはオブザーバブル レベルでの TID アクションの編集 （2013 ページ）を参照してください。 インジケータは親ソースから [アクション（Action）] 設定を継承でき、オブザーバブルは親インジケータから [アクション（Action）] 設定を継承できます。詳細については、TID 設定における継承 （2011 ページ）を参照してください。
パブリッシュ	インジケータのパブリッシュ設定。詳細については、ソース、インジケータ、またはオブザーバブル レベルでの TID データの一時停止または公開 （2015 ページ）を参照してください。 インジケータは親ソースから [パブリッシュ（Publish）] 設定を継承でき、オブザーバブルは親インジケータから [パブリッシュ（Publish）] 設定を継承できます。詳細については、TID 設定における継承 （2011 ページ）を参照してください。

フィールド	説明
インジケータのパターン（Indicator Pattern）	インジケーターのパターンを形成するオブザーバブルと演算子。演算子はインジケーター内のオブザーバブルをリンクします。AND 関係は[AND] 演算子で示されます。OR 関係は、[OR] 演算子で示されるか、いくつかのオブザーバブルの密接なグループ化により示されます。 必要に応じて、ホワイトリスト アイコン（）をクリックし、オブザーバブルをホワイトリストに入れます。詳細については、「TID オブザーバブルのホワイトリスト登録について （2017 ページ）」を参照してください。

オブザーバブルの表示と管理

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	グローバル	管理/Threat Intelligence Director（TID）ユーザ

[オブザーバブル（Observables）]ページには、正常に取り込まれたすべてのオブザーバブルが表示されます（オブザーバブル サマリー情報 （2009 ページ）を参照）。

始める前に

- ソースとして使用する TAXII フィードの取得 （1976 ページ）、URL からのソースの取得（1977ページ）、またはソースとして使用するローカルファイルのアップロード（1979ページ）の説明に従って 1 つ以上のソースを設定します。

ステップ 1 **[インテリジェンス（Intelligence）] > [ソース（Sources）]** の順に選択します。

ステップ 2 [オブザーバブル（Observables）] をクリックします。

ステップ 3 現在のオブザーバブルを次のように表示します。

- ページに表示されるオブザーバブルをフィルタリングするには、[フィルタ（Filter）] アイコン（）をクリックします。詳細については、テーブル ビューでの TID データのフィルタ処理 （2010 ページ）を参照してください。
- [値（Value）] 列の情報が途切れている場合は、値の上にカーソルを移動します。
- そのオブザーバブルを含むインジケータを表示するには、[インジケータ（Indicators）] 列内の番号をクリックします。[インシデント（Incidents）]ページが開き、オブザーバブルの値がフィルタとして適用されます。詳細については、インジケータの表示と管理 （2005 ページ）を参照してください。

ステップ 4 現在のオブザーバブルを次のように管理します。

- [アクション（Action）] を編集するには、ソース、インジケータ、またはオブザーバブル レベルでの TID アクションの編集 （2013 ページ）を参照してください。
- オブザーバブルの [公開（Publish）] 設定を編集するには、ソース、インジケータ、またはオブザーバブル レベルでの TID データの一時停止または公開 （2015 ページ）を参照してください。
- オブザーバブルの有効期限を変更するには、親ソースの [TTL] を変更します。詳細については、ソースの表示と管理 （2001 ページ）を参照してください。
- オブザーバブルをホワイトリストに入れるには、[ホワイトリスト（Whitelist）] アイコン（）をクリックします。詳細については、「TIDオブザーバブルのホワイトリスト登録について （2017ページ）」を参照してください。

オブザーバブル サマリー情報

[オブザーバブル（Observables）]ページには、取り込まれたすべてのオブザーバブルの概要情報が表示されます。

表 *137*：オブザーバブル サマリー情報

フィールド	説明
タイプ	オブザーバブル（監視可能）データのタイプ：SHA-256、Domain、URL、IPv4、または IPv6。
値	オブザーバブルを構成するデータ。
インジケータ（Indicators）	オブザーバブルを含む親インジケータの数。
操作（Action）	オブザーバブルに対して設定されている操作。詳細については、ソース、インジケータ、またはオブザーバブル レベルでの TID アクションの編集 （2013 ページ）を参照してください。 インジケータは親ソースから [アクション（Action）]設定を継承でき、オブザーバブルは親インジケータから [アクション（Action）] 設定を継承できます。詳細については、TID 設定における継承 （2011 ページ）を参照してください。
パブリッシュ	オブザーバブルのパブリッシュ設定（ソース、インジケータ、またはオブザーバブル レベルでの TID データの一時停止または公開 （2015 ページ）を参照）。 インジケータは親ソースから [公開（Publish）]設定を継承でき、オブザーバブルは親インジケータから [公開（Publish）]設定を継承できます。詳細については、TID 設定における継承 （2011 ページ）を参照してください。

フィールド	説明
更新時刻（Updated At）	TID が最後にオブザーバブルを更新した日時。
有効期限	親インジケータの [TTL] に基づいて、オブザーバブルが TID から自動的に消去される日付。
	このアイコンをクリックすると、オブザーバブルがホワイトリストに入ります（TID オブザーバブルのホワイトリスト登録について（2017 ページ）を参照）。

テーブル ビューでの TID データのフィルタ処理

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	グローバル	管理/Threat Intelligence Director（TID）ユーザ

ステップ 1 次のいずれかの TID テーブル ビューを選択します。

- **[インテリジェンス（Intelligence）] > [インシデント（Incidents）]**
- **[インテリジェンス（Intelligence）] > [ソース（Sources）]**
- **[インテリジェンス（Intelligence）] > [送信元（Sources）] > [インジケータ（Indicators）]**
- **[インテリジェンス（Intelligence）] > [送信元（Sources）] > [監視可能（Observables）]**

ステップ 2 フィルタ アイコン（🔍）をクリックし、フィルタ属性を選択します。

ステップ 3 そのフィルタ属性の値を選択または入力します。

フィルタでは大文字/小文字が区別されます。

ステップ 4 （オプション）複数の属性でフィルタリングするには、フィルタ アイコン（🔍）をクリックし、手順 2 と手順 3 を繰り返します。

ステップ 5 前回フィルタを適用してから行った変更を取り消すには、[キャンセル（Cancel）] をクリックします。

ステップ 6 フィルタを適用してテーブルを更新するには、[適用（Apply）] をクリックします。

ステップ 7 フィルタ属性を個別に削除するには、フィルタ属性の横にある削除アイコン（✕）をクリックし、[適用（Apply）] をクリックしてテーブルを更新します。

TID 設定における継承

TIDはソースからインテリジェンスデータを取り込むと、そのソースの子オブジェクトとしてインジケータとオブザーバブルを作成します。作成時に、これらの子オブジェクトは、親設定から [アクション（Action）] および [公開（Publish）] 設定を継承します。

インジケータは、親ソースからこれらの設定を継承します。インジケータは、親ソースを1つしか持てません。

オブザーバブルは、親インジケータからこれらの設定を継承します。オブザーバブルは、複数の親インジケータを持つことができます。

詳細については、以下を参照してください。

- 複数の親からの TID 設定の継承 （2011 ページ）
- 継承された TID 設定の上書きについて （2012 ページ）

複数の親からの TID 設定の継承

オブザーバブルに複数の親インジケータがある場合、システムはすべての親から継承した設定を比較し、オブザーバブルに最もセキュアなオプションを割り当てます。つまり、

- [アクション（Action）] : [ブロック（Block）] は [モニタ（Monitor）] よりもセキュアです。
- [公開（Publish）] : [オン（On）] は [オフ（Off）] よりもセキュアです。

たとえば、SourceA は IndicatorA と関連する ObservableA に関与する可能性があります。

設定	SourceA	IndicatorA	ObservableA
操作（Action）	ブロック（Block）	ブロック（Block）	ブロック（Block）
パブリッシュ	オフ（Off）	オフ（Off）	オフ（Off）

SourceB が後で ObservableA を含む IndicatorB に関与する場合、システムは ObservableA を次のように変更します。

設定	SourceB	IndicatorB	ObservableA
操作（Action）	モニタ	モニタ	[ブロック（Block）]（IndicatorA から継承）
パブリッシュ	オン（On）	オン（On）	[オン（On）]（IndicatorB から継承）

この例では、ObservableA には 2 つの親があります。1 つは [アクション（Action）] 設定の親で、もう 1 つは [公開（Publish）] 設定の親です。オブザーバブルの設定を手動で編集してから

設定を元に戻した場合、[アクション（Action）] 設定が IndicatorA 値に設定され、[公開（Publish）] 設定が IndicatorB 値に設定されます。

継承された TID 設定の上書きについて

継承された設定を上書きするには、子レベルで設定を変更します。ソース、インジケータ、またはオブザーバブル レベルでの TID アクションの編集 （2013 ページ）およびソース、インジケータ、またはオブザーバブル レベルでの TID データの一時停止または公開 （2015 ページ）を参照してください。継承された設定を上書きすると、親オブジェクトに変更にかかわらず、子オブジェクトではその設定が保持されます。

たとえば、上書きを設定せずに、次の元の設定で開始するとします。

設定	SourceA	IndicatorA	ObservableA1	ObservableA2
パブリッシュ	オフ（Off）	オフ（Off）	オフ（Off）	オフ（Off）

IndicatorA の設定を上書きした場合、設定は次のようになります。

設定	SourceA	IndicatorA	ObservableA1	ObservableA2
パブリッシュ	オフ（Off）	オン（On）	オン（On）	オン（On）

この場合、SourceA の [公開（Publish）] 設定への変更は、IndicatorA に自動的にはカスケードされなくなります。ただし、オブザーバブルの設定は現在値を上書きするようには設定されていないため、IndicatorA から ObservableA1 および ObservableA2 への継承は続行されます。

後から ObservableA1 の設定を上書きする場合は、次のようになります。

設定	SourceA	IndicatorA	ObservableA1	ObservableA2
パブリッシュ	オフ（Off）	オン（On）	オフ（Off）	オン（On）

IndicatorA の [公開（Publish）] 設定への変更は、ObservableA1 に自動的にはカスケードされなくなります。ただし、ObservableA2 は上書き値には設定されていないため、これらの変更は引き続き ObservableA2 にカスケードされます。

オブザーバブル レベルでは、上書き設定から継承された設定に戻すことができ、システムは、親インジケータからそのオブザーバブルへの設定変更のカスケードを自動的に再開します。

ソース、インジケータ、またはオブザーバブル レベルでの TID アクションの編集

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	グローバル	管理/Threat Intelligence Director（TID）ユーザ

（注）

- 親のアクションを編集すると、すべての子に対しアクションが設定されます。ソース レベルでアクションを編集すると、そのすべてのインジケータにアクションが設定されます。インジケータ レベルでアクションを編集すると、そのオブザーバブルのすべてに対してアクションが設定されます。
- 子のアクションを編集すると、継承が中断されます。インジケータ レベルでアクションを編集し、続いてソース レベルで編集すると、個々のインジケータのアクションを編集するまで、インジケータのアクションが保持されます。監視可能レベルでアクションを編集し、続いてインジケータ レベルで編集すると、個々のオブザーバブルのアクションを編集するまで、オブザーバブルのアクションが保持されます。監視可能レベルでは、親インジケータのアクションに自動的に復元できます。継承の詳細については、TID設定における継承 （2011 ページ）を参照してください。

他の アクションに影響を与える要因 （1993 ページ） を確認することもできます。

ステップ 1 次のいずれかを選択します。

- **[インテリジェンス（Intelligence）] > [ソース（Sources）]**

  （注） TID は、ソース レベルでの TAXII ソースのブロックをサポートしていません。TAXII ソースに簡易インジケータが含まれている場合、インジケータ レベルまたは監視可能レベルでブロックすることができます。

- **[インテリジェンス（Intelligence）] > [送信元（Sources）] > [インジケータ（Indicators）]**

  （注） TID は、複雑なインジケータのブロックをサポートしていません。代わりに、複雑なインジケータ内で個々のオブザーバブルをブロックします。

- **[インテリジェンス（Intelligence）] > [送信元（Sources）] > [監視可能（Observables）]**

ステップ 2 [アクション（Action）] ドロップダウンを使用して、[モニタ（Monitor）]（）または [ブロック（Block）]（）を選択します。

ステップ 3 （オブザーバブルのみ）親インジケータからアクション設定を継承し直すには、オブザーバブルの [アクション（Action）] 設定の横にある復元アイコン（↩）をクリックします。

公開の一時停止について

- 機能レベルで公開を一時停止すると、要素に保存されているすべての TID オブザーバブルが消去されます。つまり、TID は脅威を検出、監視、ブロックすることはできません。システム上の他のセキュリティ機能は影響を受けません。
- ソース、インジケータ、またはオブザーバブル レベルで公開を一時停止すると、システムは一時停止された TID オブザーバブルを要素から削除し、トラフィックと一致しないようにします。
- 親のパブリケーションを一時停止すると、すべての子が一時停止します。ソース レベルで公開を一時停止すると、そのすべてのインジケータの公開が一時停止されます。インジケータ レベルで公開を一時停止すると、そのすべてのオブザーバブルの公開が一時停止されます。
- 子のパブリケーションを一時停止すると、継承が中断されます。インジケータ レベルで公開を一時停止し、その後にソース レベルで公開すると、インジケータの個別設定を変更するまで、インジケータの公開は一時停止されたままになります。監視可能レベルで公開を一時停止し、その後にインジケータ レベルで公開すると、オブザーバブルの個別設定を変更するまで、オブザーバブルの公開は一時停止されたままになります。監視可能レベルでは、親インジケータの公開ステータスに自動的に復元できます。継承の詳細については、TID 設定における継承 （2011 ページ）を参照してください。
- アップロードされたソースの公開は、インジケータ レベルでのみ一時停止することができます。
- オブザーバブルのホワイトリスト化と公開の一時停止の比較については、TID オブザーバブルのホワイトリスト登録について （2017 ページ） を参照してください。
- 個々のオブザーバブルまたはインジケータに対して公開または一時停止の設定を指定した場合、更新プログラムに同じオブザーバブルまたはインジケータが含まれている場合、ソースの更新によってその設定が変わることはありません。
- オブジェクト管理ページで公開を無効にすることができます。オブザーバブルのパブリケーション頻度の変更 （2017 ページ）を参照してください。
- 更新を一時停止する [ソース（Sources）] ページ上のオプションは、要素へのデータの公開には関連しません。フィードから Firepower Management Center 上のソースを更新する場合に適用されます。

TID の一時停止と要素からの TID データの消去

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	グローバル	管理/Threat Intelligence Director（TID）ユーザ

注意 この設定により、すべての要素への公開が一時停止され、要素に保存されたすべての TID オブザーバブルが消去され、TID 機能を使用したトラフィックの検査が停止されます。

より細かいレベルでオブザーバブルを無効にするには、ソース、インジケータ、またはオブザーバブル レベルでの TID データの一時停止または公開（2015 ページ）を参照してください。

管理センター上のデータ（既存のインシデントと設定済みのソース、インジケータ、オブザーバブル、およびソースの取り込み）は、この設定の影響を受けません。

ステップ 1 **[インテリジェンス（Intelligence）] > [設定（Settings）]** の順に選択します。

ステップ 2 [一時停止（Pause）] をクリックします。

次のタスク

要素への TID データの同期とオブザベーションの生成を再開する準備ができたら、このページから手動で公開を [再開（Resume）] します。管理センター上の既存のオブザーバブルがすべての要素に公開されます。

ソース、インジケータ、またはオブザーバブル レベルでの TID データの一時停止または公開

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	グローバル	管理/Threat Intelligence Director（TID）ユーザ

ソース レベルで公開が有効になっている場合、システムは最初のソース データとそれに続く以下のような変更を自動的に公開します。

- 定期的なソースの更新からの変更
- システム アクションに起因する変更（**TTL** の有効期限など）
- ユーザが開始した変更（インジケータやオブザーバブルの [アクション（Action）] 設定の変更など）

（注） デバイス（要素）から一度にすべての TID オブザーバブルを消去するには、TID の一時停止と要素からの TID データの消去 （2015 ページ） を参照してください。

始める前に

公開を一時停止する前に、公開の一時停止について （2014 ページ） に記載されている影響を把握してください。

ステップ 1 次のいずれかを選択します。

- **[インテリジェンス（Intelligence）] > [ソース（Sources）]**
- **[インテリジェンス（Intelligence）] > [送信元（Sources）] > [インジケータ（Indicators）]**
- **[インテリジェンス（Intelligence）] > [送信元（Sources）] > [監視可能（Observables）]**

ステップ 2 [公開（Publish）] スライダ（）を検索して、要素への公開を切り替えるために使用します。

ステップ 3 （オブザーバブルのみ）親インジケータからパブリケーション設定を継承し直す場合は、オブザーバブルの [公開（Publish）] 設定の横にある復元アイコン（）をクリックします。

次のタスク

- 要素が変更を受け取るまで少なくとも 10 分間待機します。大規模なソースが含まれる変更には時間がかかります。
- （オプション）オブザーバブル レベルで TID データのパブリケーション頻度を変更します。オブザーバブルのパブリケーション頻度の変更 （2017 ページ） を参照してください。

オブザーバブルのパブリケーション頻度の変更

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	グローバル	管理/Threat Intelligence Director（TID）ユーザ

デフォルトでは、監視可能データ（オブザーバブル）が TID 要素に 5 分ごとに公開されます。この間隔を別の値に設定するには、次の手順を実行します。

始める前に

- 監視可能レベルで TID データのパブリケーションを有効にします。ソース、インジケータ、またはオブザーバブル レベルでの TID データの一時停止または公開 （2015 ページ）を参照してください。

ステップ 1 **[Objects]** > **[Object Management]**を選択します。

ステップ 2 **[セキュリティ インテリジェンス（Security Intelligence）]** > **[ネットワーク フィードとリスト（Network Feeds and Lists）]** を選択します。

ステップ 3 [Cisco-TID フィード（Cisco-TID-Feed）] の横にある編集アイコンをクリックします。

ステップ 4 [更新間隔:（Update Frequency）] ドロップダウンリストから値を選択します。

- 監視可能なデータの要素への公開を停止するには、[無効（Disable）] を選択します。
- その他の値を選択して、監視可能なパブリケーションの間隔を設定します。

ステップ 5 **[保存（Save）]** をクリックします。

TID オブザーバブルのホワイトリスト登録について

指定された [アクション（Action）] から簡易インジケータ内の 1 つのオブザーバブルを除外する（モニタリング/ブロッキングなしでトラフィックを通過させる）には、オブザーバブルをホワイトリストに入れることができます。

複雑なインジケータでは、TIDはトラフィックを評価するときにホワイトリスト登録されたオブザーバブルを無視しますが、そのインジケータ内の他のオブザーバブルは引き続き評価されます。たとえば、インジケータにAND演算子でリンクされているオブザーバブル1とオブザーバブル 2 が含まれていて、オブザーバブル 1 をホワイトリストに入れると、TID はオブザーバブル 2 が認識されたときに完全に実現されたインシデントを生成します。

これに対して、同じ複雑なインジケータで、オブザーバブル 1 をホワイトリスト登録するのではなく、その公開を無効にすると、TID はオブザーバブル 2 が認識されたときに部分的に実現されたインシデントを生成します。

（注） オブザーバブルをホワイトリストに追加する場合、オブザーバブルの設定が継承されるか上書き値であるかにかかわらず、ホワイトリストが常に [アクション（Action）] 設定より優先されます。

更新プログラムに同じオブザーバブルが含まれている場合、ソースの更新は個々のオブザーバブルのホワイトリスト設定に影響しません。

TID オブザーバブルのホワイトリスト登録

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	グローバル	管理/Threat Intelligence Director（TID）ユーザ

ホワイトリスト登録の詳細については、TID オブザーバブルのホワイトリスト登録について（2017 ページ） を参照してください。

ヒント ホワイトリストのアイコン（）は、Web インターフェイスの複数の場所に表示できます。アイコンをクリックすることで、それらの場所のいずれかでオブザーバブルをホワイトリストに登録することができます。

ステップ 1 [インテリジェンス（Intelligence）] > [ソース（Sources）] > [オブザーバブル（Observables）] をクリックします。

ステップ 2 無視するオブザーバブルに移動します。

ステップ 3 そのオブザーバブルのホワイトリストのアイコン（）をクリックします。

次のタスク

（オプション）ホワイトリストからオブザーバブルを削除する必要がある場合は、アイコンをもう一度クリックします。

STIX ソース ファイルの表示

ステップ 1 [インテリジェンス（Intelligence）] > [ソース（Sources）] > [インジケータ（Indicators）] を選択します。
ステップ 2 インジケータ名をクリックします。
ステップ 3 [STIXのダウンロード（Download STIX）] をクリックします。
ステップ 4 テキスト エディタでこのファイルを開きます。

Cisco Threat Intelligence Director（TID） のトラブルシューティング

以下のセクションでは、TIDの一般的な問題について、可能な解決策と軽減策を説明します。

フラット ファイル ソースを取得またはアップロードするとエラーが発生する

システムがフラットファイルソースを取得またはアップロードできない場合は、フラットファイル内のデータが [インテリジェンス（Intelligence）] > [ソース（Sources）] ページの [タイプ（Type）] 列と一致することを確認してください。

TAXII または URL のソース アップデートでエラーが発生する

TAXII またはURL のソース アップデートでソース ステータス エラーが発生した場合は、サーバ証明書の期限が切れていないことを確認してください。証明書の有効期限が切れている場合は、新しい**サーバ証明書**を入力するか、または既存の**サーバ証明書**を削除して、TIDが新しい証明書を取得できるようにします。詳細については、TID ソースの TLS/SSL 設定の構成 （1980 ページ）を参照してください。

インジケータまたはソースに対して「ブロック」アクションは使用できず、「モニタ」アクションのみを使用できます。

インジケータまたはソースの個々のオブザーバブルのアクションを変更できます。

TID テーブル ビューで「結果なし」と表示される

テーブル ビューには、[ソース（Sources）]、[インジケータ（Indicators）]、[オブザーバブル（Observables）]、および [インシデント（Incidents）] ページが含まれます。

いずれかの TID テーブル ビューにデータが表示されない場合：

- テーブル フィルタを確認し、[最終更新日（Last Updated）] フィルタ属性の時間枠を拡大することを検討します（テーブル ビューでの TIDデータのフィルタ処理 （2010ページ）を参照）。
- ソースが正しく設定されていることを確認します（データ ソースを取り込むためのオプション （1975 ページ）を参照）。

- TIDをサポートするのに必要なアクセス コントロール ポリシー、および関連するポリシーが設定されていることを確認します（TIDをサポートするためのポリシーの設定 （1974ページ）を参照）。たとえば、SHA 256オブザーバブルがオブザベーションを生成していない場合、展開されているアクセス コントロール ポリシーに、[マルウェアクラウドルックアップ（Malware Cloud Lookup）] または [マルウェアブロック（Block Malware）] ファイル ポリシーを呼び出すアクセス制御ルールが 1 つ以上含まれていることを確認します。
- TID をサポートするアクセス コントロール ポリシーおよび関連するポリシーが要素に展開されていることを確認します（設定変更の展開 （447 ページ）を参照）。
- 機能レベルでTIDデータ パブリケーションを一時停止していないことを確認します（TIDの一時停止と要素からの TID データの消去 （2015 ページ）を参照）。

システムが低速またはパフォーマンス低下を起こしている

パフォーマンスの影響の詳細については、Threat Intelligence Director のパフォーマンスへの影響 （1970 ページ） を参照してください。

Firepower Management Center テーブル ビューに TID データが表示されない

オブザーバブルを要素に公開しても、接続、セキュリティ インテリジェンス、ファイル、またはマルウェア イベントのテーブルに TID データが表示されない場合は、要素に展開されたアクセス コントロール ポリシーとファイル ポリシーを確認してください。詳細については、TIDをサポートするためのポリシーの設定 （1974 ページ）を参照してください。

1 つまたは複数の要素が TID データによって圧倒される

TID データが 1 つまたは複数のデバイスを圧倒している場合は、TID による要素に保存されているデータの公開と消去を一時停止することを検討してください。詳細については、TIDの一時停止と要素からの TID データの消去 （2015 ページ）を参照してください。

システムが TID ブロックの代わりにマルウェア クラウド ルックアップを実行している

これは設計によるものです。詳細については、TID-Firepower Management Center のアクションの優先順位付け （1994 ページ）を参照してください。

システムが TID アクションではなく、セキュリティ インテリジェンスまたは DNS ポリシー アクションを実行している

これは設計によるものです。詳細については、TID-Firepower Management Center のアクションの優先順位付け （1994 ページ）を参照してください。

TID が無効化されている

- アプライアンスにメモリを追加します。Threat Intelligence Director を使用するには、少なくとも 15 GB のメモリをアプライアンスに搭載する必要があります。
- Firepower Management Center の REST API アクセスを有効化します。詳細については、REST API アクセスの有効化 （1325 ページ）を参照してください。

システムが TID インシデントを生成しないか、または予期される TID アクションを実行しない

- すべての管理対象デバイスがTIDに対し適切に有効になっており、設定されていることを確認します。要素（管理対象デバイス）のTIDステータスの表示（2000ページ）およびTIDをサポートするためのポリシーの設定（1974ページ）を参照してください。
- 変更内容が要素に公開されるまでには少なくとも5～10分かかり、大規模なデータフィードを公開する場合は、かかる時間がそれよりも著しく長くなります。
- オブザーバブルに対するアクション設定を確認します。オブザーバブルの表示と管理（2008ページ）を参照してください。
- システムが実行する TID アクションに影響を与える他の要因のリストについては、アクションに影響を与える要因（1993ページ）を参照してください。
- 要素（管理対象デバイス）に、予想していた脅威データが含まれていない可能性があります。公開の一時停止について（2014ページ）を参照してください。

特定の脅威との一度の遭遇によって、複数のインシデントが生成される

これは、単一のインジケータが複数のソースに含まれている場合に発生します。

- フラット ファイル ソースからのインジケータ：インジケータの各インスタンスがインシデントを生成するため、特定の脅威を一度検出すると複数のインシデントを生成する場合があります。
- STIX ソースからのインジケータ：異なる STIX ソースからのインジケータが同じ ID を共有している場合、含んでいるソースの数にかかわらず、そのインジケータに対して1つのインシデントのみが生成されます。

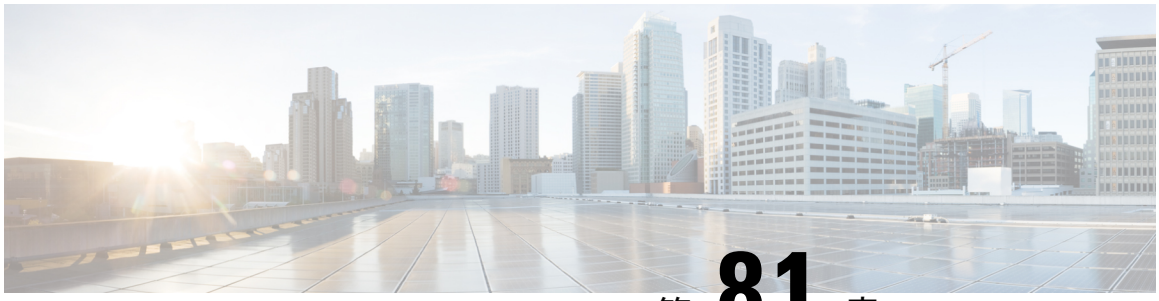
今後の重複インシデントを回避するには、重複インジケータの1つを除くすべてのインジケータの公開を一時停止します。ソース、インジケータ、またはオブザーバブル レベルでの TID データの一時停止または公開（2015ページ）を参照してください。

の履歴Cisco Threat Intelligence Director（TID）

機能	バージョン	詳細
Cisco Threat Intelligence Director（TID）	6.2.2	導入された機能：外部送信元から脅威のインテリジェンスを使用して脅威を特定し処理できます。 新規画面：複数のタブがあるトップレベルの新しい [インテリジェンス（Intelligence）] メニュー サポートされるプラットフォーム Firepower Management Center

第 XX 部

侵入検知と防御



第 81 章

ネットワーク分析ポリシーと侵入ポリシーの概要

以下のトピックでは、ネットワーク分析ポリシーと侵入ポリシーの概要を示します。

ネットワーク分析ポリシーと侵入ポリシーの基本

ネットワーク分析ポリシーと侵入ポリシーは、Firepower システムの侵入検知および防御機能の一部として連携して動作します。

- 侵入検知という用語は、一般に、ネットワーク トラフィックへの侵入の可能性を受動的にモニタおよび分析し、セキュリティ分析用に攻撃データを保存するプロセスを指します。これは「IDS」とも呼ばれます。
- 侵入防御という用語には、侵入検知の概念が含まれますが、さらにネットワークを通過中の悪意のあるトラフィックをブロックしたり変更したりする機能も追加されます。これは「IPS」とも呼ばれます。

侵入防御の展開では、システムがパケットを検査するときに次のことが行われます。

- **ネットワーク分析ポリシー**は、トラフィックのデコードと前処理の方法を管理し、特に、侵入を試みている兆候がある異常なトラフィックについて、さらに評価できるようにします。
- **侵入ポリシー**では侵入およびプリプロセッサ ルール（総称的に「侵入ルール」とも呼ばれる）を使用し、パターンに基づき、デコードされたパケットを検査して攻撃の可能性を調べます。侵入ポリシーは変数セットとペアになっており、これにより、ユーザは指定された値を使用してネットワーク環境を正確に反映できます。

ネットワーク分析ポリシーと侵入ポリシーは、どちらも親のアクセス コントロール ポリシーによって呼び出されますが、呼び出されるタイミングが異なります。システムでトラフィックが分析される際には、侵入防御（追加の前処理と侵入ルール）フェーズよりも前に、別にネットワーク分析（デコードと前処理）フェーズが実行されます。ネットワーク分析ポリシーと侵入ポリシーを一緒に使用すると、広範囲で詳細なパケットインスペクションを行うことができます。これらのポリシーは、ホストとそのデータの可用性、整合性、機密性を脅かす可能性のあるネットワーク トラフィックの検知、アラート、防御に役立ちます。

Firepower システムには、同様の名前（Balanced Security and Connectivity など）が付いた複数のネットワーク分析ポリシーと侵入ポリシーが付属しており、それらは相互に補完して連携します。システム付属のポリシーを使用することで、Cisco Talos Intelligence Group（Talos）の経験を活用できます。これらのポリシーでは、Talos は侵入ルールおよびプリプロセッサ ルールの状態を設定し、プリプロセッサおよび他の詳細設定の初期設定も提供します。

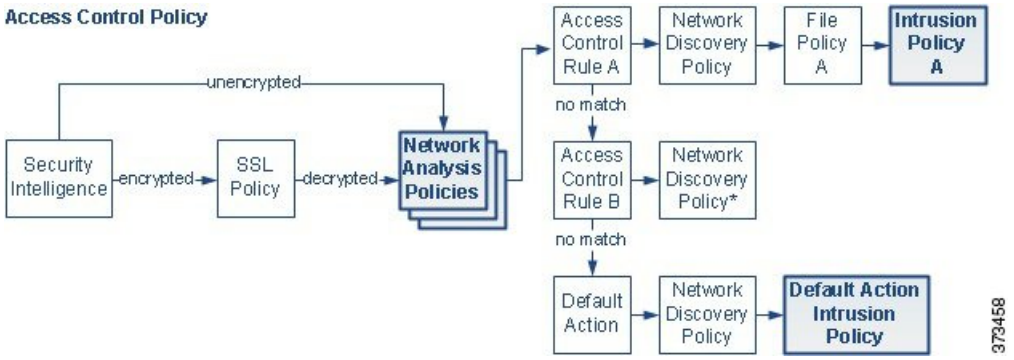
また、カスタムのネットワーク分析ポリシーや侵入ポリシーも作成できます。カスタム ポリシーの設定を調整することで、各自にもっとも役立つ方法でトラフィックを検査できます。これによって、管理対象デバイスのパフォーマンスが向上し、ユーザは生成されたイベントにさらに効率的に対応できるようになります。

Web インターフェイスで同様のポリシーエディタを使用し、ネットワーク分析ポリシーや侵入ポリシーを作成、編集、保存、管理します。いずれかのタイプのポリシーを編集するときには、Web インターフェイスの左側にナビゲーション パネルが表示され、右側にさまざまな設定ページが表示されます。

ポリシーが侵入についてトラフィックを検査する仕組み

アクセス コントロールの展開の一部としてシステムがトラフィックを分析すると、ネットワーク分析（復号化と前処理）フェーズが侵入防御（侵入ルールおよび詳細設定）フェーズとは別にその前に実行されます。

次の図は、インラインの侵入防御およびネットワーク向け AMP 展開におけるトラフィック分析の順序を簡略化して示しています。アクセス コントロール ポリシーが他のポリシーを呼び出してトラフィックを検査するしくみ、およびそれらのポリシーが呼び出される順序を示しています。ネットワーク分析ポリシーと侵入ポリシーの選択フェーズは強調表示されています。



インライン展開（つまり、ルーテッド、スイッチド、トランスペアレントインターフェイスまたはインラインインターフェイスのペアを使用して関連設定がデバイスに展開される展開）では、システムは上図のプロセスのほぼすべての段階において、追加のインスペクションなしでトラフィックをブロックすることができます。セキュリティインテリジェンス、SSLポリシー、ネットワーク分析ポリシー、ファイルポリシー、および侵入ポリシーのすべてで、トラフィックをドロップまたは変更できます。唯一の例外として、パッシブにパケットを検査するネットワーク検出ポリシーは、トラフィック フローに影響を与えることができません。

同様に、プロセスの各ステップで、パケットによってシステムがイベントを生成する場合があります。侵入およびプリプロセッサイベント（総称的に「侵入イベント」とも呼ばれる）は、パケットまたはそのコンテンツがセキュリティリスクを含んでいる可能性を示唆しています。

ヒント SSLインスペクションの設定で暗号化トラフィックの通過が許可されている場合や、SSLインスペクションが設定されていない場合について、この図は、そのような場合のアクセス コントロール ルールによる暗号化トラフィックの処理を反映していません。デフォルトでは、暗号化ペイロードの侵入およびファイルインスペクションは無効化されます。これにより、侵入およびファイル インスペクションが設定されたアクセス コントロール ルールに暗号化接続が一致したときの誤検出が減少し、パフォーマンスが向上します。

単一の接続の場合は、図に示すように、アクセス コントロール ルールよりも前にネットワーク分析ポリシーが選択されますが、いくつかの前処理（特にアプリケーション層の前処理）はアクセス コントロール ルールの選択後に実行されます。これは、カスタム ネットワーク分析ポリシーでの前処理の設定には影響**しません**。

復号化、正規化、前処理：ネットワーク分析ポリシー

デコードと前処理を実行しないと、プロトコルの相違によりパターンマッチングを行えなくなるので、侵入についてトラフィックを適切に評価できません。これらのトラフィック処理タスクは、以下のタイミングでネットワーク分析ポリシーによる処理の対象となります。

- 暗号化トラフィックがセキュリティ インテリジェンスによってフィルタリングされた**後**
- 暗号化トラフィックがオプションの SSL ポリシーによって復号化された**後**
- ファイルまたは侵入ポリシーによってトラフィックを検査できるようになる**前**

ネットワーク分析ポリシーは、フェーズでのパケット処理を制御します。まず、最初の3つのTCP/IP レイヤを経由するパケットがデコードされ、続いて、標準化、前処理、プロトコルの異常の検出が行われます。

- パケット デコーダは、パケット ヘッダーとペイロードを、プリプロセッサや以降の侵入ルールで簡単に使用できる形式に変換します。TCP/IP スタックの各レイヤのデコードは、データリンク層から開始され、ネットワーク層、トランスポート層へと順番に行われます。パケット デコーダは、パケット ヘッダーからさまざまな異常動作を検出します。
- インライン展開では、インライン正規化プリプロセッサは、攻撃者が検出を免れる可能性を最小限にするために、トラフィックを再フォーマット（正規化）します。その他のプリ

プロセッサや侵入ルールによる検査に向けてパケットを準備し、システムで処理されるパケットがネットワーク上のホストで受信されるパケットと同じものになるようにします。

（注） パッシブな展開の場合、シスコでは、ネットワーク分析レベルでインライン正規化を行うのではなく、アクセス コントロール ポリシー レベルでアダプティブプロファイルの更新を有効にすることを推奨しています。

- ネットワーク層とトランスポート層のさまざまなプリプロセッサは、IP フラグメントを悪用する攻撃を検出したり、チェックサム検証を実行したり、TCP および UDP セッションの前処理を実行したりします。

  トランスポートおよびネットワーク プリプロセッサの一部の詳細設定は、アクセス コントロール ポリシーのターゲット デバイスで処理されるすべてのトラフィックにグローバルに適用されます。これらの詳細設定は、ネットワーク分析ポリシーではなくアクセス コントロール ポリシーで設定します。

- 各種のアプリケーション層プロトコル デコーダは、特定タイプのパケット データを侵入ルールエンジンで分析可能な形式に正規化します。アプリケーション層プロトコルのエンコードを正規化することにより、システムはデータ表現が異なるパケットに同じコンテンツ関連の侵入ルールを効果的に適用し、大きな結果を得ることができます。

- Modbus と DNP3 のプリプロセッサは、トラフィックの異常を検出し、データを侵入ルールに提供します。Supervisory Control and Data Acquisition（SCADA）プロトコルは、製造、水処理、配電、空港、輸送システムなどの工業プロセス、インフラストラクチャ プロセス、および設備プロセスからのデータをモニタ、制御、取得します。

- 一部のプリプロセッサでは、Back Orifice、ポートスキャン、SYN フラッドおよび他のレート ベース攻撃など、特定の脅威を検出できます。

  侵入ポリシーで、ASCII テキストのクレジット カード番号や社会保障番号などの機密データを検出する機密データ プリプロセッサを設定することに注意してください。

新たに作成されたアクセス コントロール ポリシーでは、1 つのデフォルト ネットワーク分析ポリシーが、同じ親アクセス コントロール ポリシーによって呼び出されるすべての侵入ポリシー向けのすべてのトラフィックについて、前処理を制御します。最初に、デフォルトでは Balanced Security and Connectivity ネットワーク分析ポリシーが使用されますが、別のシステム付属ポリシーやカスタム ネットワーク分析ポリシーに変更できます。より複雑な展開では、上級ユーザは、一致するトラフィックの前処理にさまざまなカスタム ネットワーク分析ポリシーを割り当てることによって、特定のセキュリティ ゾーン、ネットワーク、VLAN に合わせてトラフィックの前処理オプションを調整できます。

アクセス コントロール ルール：侵入ポリシーの選択

最初の前処理の後、トラフィックはアクセス コントロール ルール（設定されている場合）によって評価されます。ほとんどの場合、パケットが一致した最初のアクセス コントロール ルー

ルがそのトラフィックを処理することになります。ユーザは一致したトラフィックをモニタ、信頼、ブロック、または許可することができます。

アクセス コントロール ルールでトラフィックを許可すると、ディスカバリ データ、マルウェア、禁止ファイル、侵入について、この順序でトラフィックを検査できます。アクセス コントロール ルールに一致しないトラフィックは、アクセス コントロール ポリシーのデフォルト アクションによって処理されます。デフォルト アクションでは、ディスカバリ データと侵入についても検査できます。

（注） どのネットワーク分析ポリシーによって前処理されるかに**関わらず**、すべてのパケットは、設定されているアクセス コントロール ルールと上から順に照合されます（したがって、侵入ポリシーによる検査の対象となります）。

ポリシーが侵入についてトラフィックを検査する仕組み（2026ページ）の図は、インラインの侵入防御およびネットワーク向けAMP 展開でデバイスを通過する、次のようなトラフィックのフローを示しています。

- アクセス コントロール ルール A により、一致したトラフィックの通過が許可されます。次にトラフィックは、ネットワーク検出ポリシーによるディスカバリ データの検査、ファイル ポリシーA による禁止ファイルおよびマルウェアの検査、侵入ポリシー A による侵入の検査を受けます。
- アクセス コントロール ルール B も一致したトラフィックを許可します。ただし、このシナリオでは、トラフィックは侵入（あるいは、ファイルまたはマルウェア）について検査されないので、ルールに関連付けられている侵入ポリシーやファイル ポリシーはありません。通過を許可されたトラフィックは、デフォルトでネットワーク検出ポリシーによって検査されます。したがって、これを設定する必要はありません。
- このシナリオでは、アクセス コントロール ポリシーのデフォルト アクションは一致したトラフィックを許可します。次に、トラフィックはネットワーク検出ポリシーによって検査されてから、侵入ポリシーによって検査されます。アクセス コントロール ルールまたはデフォルト アクションに侵入ポリシーを関連付けるときに、必要に応じて、別の侵入ポリシーを使用できます。

ブロックされたトラフィックや信頼済みトラフィックは検査されないので、図の例には、ブロック ルールや信頼ルールは含まれていません。

侵入インスペクション：侵入ポリシー、ルール、変数セット

トラフィックが宛先に向かうことを許可する前に、システムの最終防御ラインとして侵入防御を使用できます。侵入ポリシーは、セキュリティ違反に関するトラフィックの検査方法を制御し、インライン展開では、悪意のあるトラフィックをブロックまたは変更することができます。侵入ポリシーの主な機能は、有効にする侵入ルールとプリプロセッサ ルールの選択および設定方法を管理することです。

侵入ルールとプリプロセッサ ルール

侵入ルールはキーワードと引数のセットとして指定され、ネットワーク上の脆弱性を悪用する試みを検出します。システムは侵入ルールを使用してネットワーク トラフィックを分析し、トラフィックがルールの条件に合致しているかどうかをチェックします。システムが各ルール内で指定された条件とパケットを照らし合わせます。そして、パケットデータとルール内で指定されたすべての条件が一致した場合に、ルールがトリガーとして使用されます。

システムには、Cisco Talos Intelligence Group（Talos） によって作成された次のタイプのルールが含まれています。

- 共有オブジェクト侵入ルール：コンパイルされており、変更できません（ただし、送信元と宛先のポートや IP アドレスなどのルール ヘッダー情報を除く）
- 標準テキスト侵入ルール：ルールの新しいカスタム インスタンスとして保存および変更できます。
- プリプロセッサ ルール：ネットワーク分析ポリシーのプリプロセッサおよびパケット デコーダ検出オプションに関連付けられています。プリプロセッサ ルールはコピーまたは編集できません。ほとんどのプリプロセッサ ルールはデフォルトで無効になっています。プリプロセッサを使用してイベントを生成し、インライン展開では、違反パケットをドロップします。 するにはそれらを有効にする必要があります。

システムで侵入ポリシーに従ってパケットを処理するとき、最初にルール オプティマイザが、基準（トランスポート層、アプリケーション プロトコル、保護されたネットワークへの入出力方向など）に基づいて、サブセット内のすべてのアクティブなルールを分類します。次に、侵入ルール エンジンが、各パケットに適用する適切なルールのサブセットを選択します。最後に、マルチルール検索エンジンが 3 種類の検索を実行して、トラフィックがルールに一致するかどうかを検査します。

- プロトコル フィールド検索は、アプリケーション プロトコル内の特定のフィールドでの一致を検索します。
- 汎用コンテンツ検索は、パケット ペイロードの ASCII またはバイナリ バイトでの一致を検索します。
- パケット異常検索では、特定のコンテンツが含まれているかどうかではなく、確立されたプロトコルに違反しているパケット ヘッダーやペイロードが検索されます。

カスタム侵入ポリシーでは、ルールを有効化および無効化し、独自の標準テキスト ルールを記述および追加することで、検出を調整できます。Firepower 推奨機能を使用して、ネットワーク上で検出されたオペレーティング システム、サーバ、およびクライアント アプリケーション プロトコルを、それらの資産を保護するために作成されたルールに関連付けることができます。

変数セット

システムが侵入ポリシーを使用してトラフィックを評価する場合、システムは関連付けられた変数セットを使用します。大部分の変数は、侵入ルールで一般的に使用される値を表し、送信

元および宛先のIPアドレスおよびポートを識別します。侵入ポリシーにある変数を使用して、ルール抑制および動的ルール状態にあるIPアドレスを表すこともできます。

システムには、定義済みのデフォルト変数から構成される1つのデフォルト変数セットが含まれています。システム提供の共有オブジェクトルールと標準テキストルールは、これらの定義済みのデフォルト変数を使用してネットワークおよびポート番号を定義します。たとえば、ルールの大半は、保護されたネットワークを指定するために変数 `$HOME_NET` を使用して、保護されていない（つまり外部の）ネットワークを指定するために変数 `$EXTERNAL_NET` を使用します。さらに、特殊なルールでは、他の定義済みの変数がしばしば使用されます。たとえば、Webサーバに対するエクスプロイトを検出するルールは、`$HTTP_SERVERS` 変数および `$HTTP_PORTS` 変数を使用します。

ヒント システム提供の侵入ポリシーを使用する場合でも、シスコでは、デフォルトセットの主要なデフォルト変数を変更すること**強く**推奨します。ネットワーク環境を正確に反映する変数を使用すると、処理が最適化され、システムによって疑わしいアクティビティに関連するシステムをモニタできます。上級ユーザはカスタム変数セットを作成して、1つ以上のカスタム侵入ポリシーと組合わせることができます。

関連トピック

定義済みデフォルト変数 （541 ページ）

侵入イベントの生成

侵入されている可能性を特定すると、システムは侵入イベントまたはプリプロセッサイベント（まとめて侵入イベントと呼ばれることもあります）を生成します。管理対象デバイスはFirepower Management Centerにイベントを送信します。ここで、集約データを確認し、ネットワークアセットに対する攻撃を的確に把握できます。インライン展開では、管理対象デバイスは、有害であると判明しているパケットをドロップまたは置き換えることがきます。

データベース内の各侵入イベントにはイベントヘッダーがあり、イベント名と分類、送信元と宛先のIPアドレス、ポート、イベントを生成したプロセス、およびイベントの日時に関する情報、さらに攻撃の送信元とそのターゲットに関するコンテキスト情報が含まれています。パケットベースのイベントの場合、システムは復号化されたパケットヘッダーとイベントをトリガーしたパケット（複数の場合あり）のペイロードのコピーもログに記録します。

パケットデコーダ、プリプロセッサ、および侵入ルールエンジンはすべて、システムによるイベントの生成を引き起こします。次に例を示します。

- （ネットワーク分析ポリシーで設定された）パケットデコーダが20バイト（オプションやペイロードのないIPデータグラムのサイズ）未満のIPパケットを受け取った場合、デコーダはこれを異常なトラフィックと解釈します。以降、パケットを検査する侵入ポリシーで付随するデコーダルールが有効な場合は、システムによってプリプロセッサイベントが生成されます。

- IP最適化プリプロセッサが重複する一連のIPフラグメントを検出した場合、プリプロセッサはこれを潜在的な攻撃と解釈し、付随するプリプロセッサルールが有効な場合はシステムによってプリプロセッサ イベントが生成されます。
- 侵入ルールエンジン内では、ほとんどの標準テキストルールおよび共有オブジェクトルールはパケットによってトリガーされた場合に侵入イベントを生成するように記述されます。

データベースに侵入イベントが蓄積されると、ユーザは攻撃の可能性について分析を開始できます。システムは、ユーザが侵入イベントを確認し、ネットワーク環境とセキュリティ ポリシーのコンテキストでそのイベントが重要であるかどうかを評価するために必要なツールを提供します。

システム提供およびカスタムのネットワーク分析ポリシーと侵入ポリシー

Firepower システムを使用してトラフィック フローを管理する最初のステップの 1 つは、新しいアクセス コントロール ポリシーを作成することです。デフォルトでは、新たに作成されたアクセスコントロールポリシーは、システム付属のネットワーク分析ポリシーと侵入ポリシーを呼び出してトラフィックを検査します。

次の図は、インラインの侵入防御展開で、新たに作成されたアクセス コントロール ポリシーが最初にトラフィックを処理するしくみを示しています。前処理および侵入防御のフェーズが強調表示されています。

以下の点に注意してください。

- デフォルトのネットワーク分析ポリシーによって、アクセス コントロール ポリシーで処理されるすべてのトラフィックの前処理が制御されます。最初は、システム付属の*Balanced Security and Connectivity* ネットワーク分析ポリシーがデフォルトになります。
- アクセス コントロール ポリシーのデフォルト アクションは、システム付属の *Balanced Security and Connectivity* 侵入ポリシーによる検査に従って、悪意のないトラフィックをすべて許可します。デフォルトアクションはトラフィックの通過を許可するので、侵入ポリシーが悪意のあるトラフィックを検査して潜在的にブロックする前に、検出機能によって、ホスト、アプリケーション、ユーザ データについてトラフィックを検査できます。
- ポリシーは、デフォルトのセキュリティ インテリジェンス オプション（グローバルなホワイトリストとブラックリストのみ）を使用し、SSLポリシーによる暗号化トラフィックの復号化や、アクセス コントロール ルールによるネットワーク トラフィックの特別な処理や検査を実行しません。

侵入防御展開を調整するために実行できる簡単な手順は、システム付属のネットワーク分析ポリシーと侵入ポリシーの別のセットをデフォルトとして使用することです。Firepower システムには、これらのポリシーの複数のペアが提供されています。

または、カスタムポリシーを作成して使用することで、侵入防御展開を調整できます。それらのポリシーに設定されたプリプロセッサ オプション、侵入ルール、およびその他の詳細設定が、ネットワークのセキュリティ ニーズに適合しない場合があります。設定できるネットワーク分析ポリシーおよび侵入ポリシーを調整することにより、システムがネットワーク上のトラフィックを処理して侵入の有無について検査する方法を非常にきめ細かく設定できます。

システム提供のネットワーク分析ポリシーと侵入ポリシー

Firepower システムには、ネットワーク分析ポリシーと侵入ポリシーのペアがいくつか付属しています。システム提供のネットワーク分析ポリシーおよび侵入ポリシーを使用して、Cisco Talos Intelligence Group（Talos） のエクスペリエンスを活用することができます。これらのポリシーでは、Talos が侵入ルールおよびプリプロセッサ ルールの状態、ならびにプリプロセッサおよび他の詳細設定の初期設定も指定しています。

すべてのネットワーク プロファイル、最小トラフィック、または防御ポスチャに対応したシステム付属ポリシーはありません。これらの各ポリシーは一般的なケースとネットワークのセットアップに対応しているため、これらのポリシーに基づいて適切に調整された防御ポリシーを策定することができます。システム付属ポリシーは、変更せずにそのまま使用できますが、カスタム ポリシーのベースとして使用し、カスタム ポリシーを各自のネットワークに合わせて調整することが推奨されます。

ヒント システム付属のネットワーク分析ポリシーと侵入ポリシーを使用する場合でも、ネットワーク環境が正確に反映されるように、システムの侵入変数を設定する必要があります。少なくとも、デフォルトのセットにある主要なデフォルトの変数を変更します。

新しい脆弱性が知られるようになると、Talos が侵入ルールの更新をリリースします（Snort ルールの更新とも呼ばれます）。これらのルールアップデートにより、システム付属のネットワーク分析ポリシーや侵入ポリシーが変更され、侵入ルールとプリプロセッサルールの新規作成または更新、既存ルールの状態の変更、およびデフォルトのポリシー設定の変更が実施されます。ルールアップデートでは、システム付属のポリシーからルールが削除されたり、新しいルール カテゴリが提供されたり、さらにデフォルトの変数セットが変更されることもあります。

ルール更新によって展開が影響を受けると、Web インターフェイスは影響を受けた侵入ポリシーやネットワーク分析ポリシー、およびそれらの親のアクセス コントロール ポリシーを失効したものとして扱います。変更を有効にするには、更新されたポリシーを再展開する必要があります。

必要に応じて、影響を受けた侵入ポリシーを（単独で、または影響を受けたアクセス コントロール ポリシーと組み合わせて）自動的に再展開するように、ルールの更新を設定できます。これにより、新たに検出されたエクスプロイトおよび侵入から保護するために展開環境を容易に自動的に最新に維持することができます。

前処理の設定を最新の状態に保つには、アクセス コントロール ポリシーを再展開する**必要があります**。これにより、現在実行されているものとは異なる、関連するSSLポリシー、ネットワーク分析ポリシー、ファイルポリシーが再展開され、前処理とパフォーマンスの詳細設定オプションのデフォルト値も更新できるようになります。

Firepowerシステムに付属しているネットワーク分析ポリシーと侵入ポリシーのペアは以下のとおりです。

[バランスのとれたセキュリティと接続性（Balanced Security and Connectivity）] ネットワーク分析ポリシーおよび侵入ポリシー

これらのポリシーは、速度と検出の両方を目的として作成されています。一緒に使用すると、ほとんどの組織および展開タイプにとって最適な出発点となります。ほとんどの場合、システムはBalanced Security and Connectivityのポリシーおよび設定をデフォルトとして使用します。

Connectivity Over Security ネットワーク分析ポリシーおよび侵入ポリシー

これらのポリシーは、接続（すべてのリソースに到達可能な）の方がネットワークインフラストラクチャのセキュリティより優先される組織向けに作られています。この侵入ポリシーは、Security over Connectivityポリシー内で有効になっているルールよりもはるかに少ないルールを有効にします。トラフィックをブロックする最も重要なルールだけが有効にされます。

Security over Connectivity ネットワーク分析ポリシーおよび侵入ポリシー

これらのポリシーは、ネットワークインフラストラクチャのセキュリティがユーザの利便性より優先される組織向けに作られています。この侵入ポリシーは、正規のトラフィックにアラートを発したり、それらのトラフィックをドロップする可能性のある膨大な数のネットワーク異常侵入ルールを有効にします。

Maximum Detection ネットワーク分析ポリシーおよび侵入ポリシー

このポリシーは、Security over Connectivityポリシー以上にネットワーク インフラストラクチャのセキュリティを重視する組織のために作成されています。動作への影響がさらに高くなる可能性があります。たとえば、この侵入ポリシーでは、マルウェア、エクスプロイト キット、古い脆弱性や一般的な脆弱性、および既知の流行中のエクスプロイトを含め、多数の脅威カテゴリのルールを有効にします。

No Rules Active 侵入ポリシー

No Rules Active侵入ポリシーでは、すべての侵入ルールと侵入ルールのしきい値を除くすべての詳細設定が無効にされます。このポリシーは、他のシステムによって提供されるポリシーのいずれかで有効になっているルールをベースにするのではなく、独自の侵入ポリシーを作成する場合の出発点を提供します。

（注） 選択されているシステムから提供されるベースポリシーによって、ポリシーの設定が異なります。ポリシー設定を表示するには、ポリシーの横にある [編集（Edit）] アイコンをクリックしてから、[ベース ポリシーの管理（Manage Base Policy）] リンクをクリックします。

カスタム ネットワーク分析とカスタム侵入ポリシーの利点

システム付属のネットワーク分析ポリシーと侵入ポリシーに設定されているプリプロセッサオプション、侵入ルール、およびその他の詳細設定が、組織のネットワークのセキュリティニーズに完全に合致しない場合があります。

カスタム侵入ポリシーを作成すると、環境内のシステムのパフォーマンスを向上させ、ネットワークで発生する悪意のあるトラフィックやポリシー違反に焦点を当てたビューを提供できます。設定できるカスタムポリシーを作成および調整することにより、システムがネットワーク上のトラフィックを処理して侵入の有無について検査する方法を非常にきめ細かく設定できます。

すべてのカスタムポリシーには基本ポリシー（別名「基本レイヤ」）があり、それによって、ポリシー内のすべてのコンフィギュレーションのデフォルト設定が定義されます。レイヤは、複数のネットワーク分析ポリシーまたは侵入ポリシーを効率的に管理するために使用できる構成要素です。

ほとんどの場合、カスタムポリシーはシステム付属のポリシーに基づきますが、別のカスタムポリシーを使用することもできます。ただし、すべてのカスタム ポリシーには、ポリシーチェーンの最終的なベースとしてシステム付属ポリシーが含まれています。システム付属のポリシーはルールアップデートによって変更される可能性があるので、カスタムポリシーを基本として使用している場合でも、ルールアップデートをインポートするとポリシーに影響が及びます。ルール更新によって展開が影響を受けると、Webインターフェイスは影響を受けたポリシーを失効として扱います。

ユーザが作成するカスタム ポリシーに加えて、システムには、初期インライン ポリシーと初期パッシブ ポリシーという2つのカスタム侵入ポリシーと2つのネットワーク分析ポリシーが用意されています。これらのポリシーは、該当する「Balanced Security and Connectivity」ポリシーを基本ポリシーとして使用します。両者の唯一の相違点はドロップ動作です。インラインポリシーではトラフィックのブロックと変更が有効化され、パッシブ ポリシーでは無効化されます。これらのシステム提供のカスタム ポリシーは編集して使用できます。

カスタム ネットワーク分析ポリシーの利点

デフォルトでは、1つのネットワーク分析ポリシーによって、アクセス コントロール ポリシーで処理されるすべての暗号化されていないトラフィッが前処理されます。これは、侵入ポリシー（および侵入ルールセット）に関係なく、すべてのパケットが同じ設定に基づいてデコードされ、処理されることを意味します。

初期段階では、システムによって提供される Balanced Security and Connectivity ネットワーク分析ポリシーがデフォルトです。前処理を調整する簡単な方法は、デフォルトとしてカスタム ネットワーク分析ポリシーを作成して使用することです。

使用可能な調整オプションはプリプロセッサによって異なりますが、プリプロセッサおよびデコーダを調整できる方法には次のものがあります。

- モニタしているトラフィックに適用されないプリプロセッサを無効にします。たとえば、HTTP Inspect プリプロセッサは HTTP トラフィックを正規化します。ネットワークに Microsoft インターネット インフォメーション サービス（IIS）を使用する Web サーバが

含まれていないことが確実な場合は、IIS 特有のトラフィックを検出するプリプロセッサ オプションを無効にすることで、システム処理のオーバーヘッドを軽減できます。

（注） カスタム ネットワーク分析ポリシーでプリプロセッサが無効化されているときに、パケットを有効な侵入ルールまたはプリプロセッサ ルールと照合して評価するために、プリプロセッサを使用する必要がある場合、システムはプリプロセッサを有効化して使用します。ただし、ネットワーク分析ポリシーの Web インターフェイスではプリプロセッサは無効なままになります。

- 必要に応じて、特定のプリプロセッサのアクティビティを集中させるポートを指定します。たとえば、DNS サーバの応答や暗号化 SSL セッションをモニタするための追加ポートを特定したり、Telnet、HTTP、SMTP トラフィックをデコードするポートを特定できます。

複雑な環境内の上級ユーザの場合は、複数のネットワーク分析ポリシーを作成して、それぞれが異なる方法でトラフィックを処理するように調整できます。さらに、トラフィックのセキュリティ ゾーン、ネットワーク、または VLAN に応じて前処理が制御されるようにこれらのポリシーを設定できます。（ASA FirePOWER モジュールでは、VLAN に応じて前処理を制限することはできません）。

（注） カスタム ネットワーク分析ポリシー（特に複数のネットワーク分析ポリシー）を使用して前処理を調整することは、高度なタスクです。前処理と侵入インスペクションは非常に密接に関連しているため、単一のパケットを検査するネットワーク分析ポリシーと侵入ポリシーが相互補完することを許可する場合は、注意する**必要があります**。

カスタム侵入ポリシーの利点

侵入防御を実行するように初期設定して、新規にアクセス コントロール ポリシーを作成した場合、そのポリシーでは、デフォルト アクションはすべてのトラフィックを許可しますが、最初にシステム付属の Balanced Security and Connectivity 侵入ポリシーでトラフィックをチェックします。アクセス コントロール ルールを追加するか、またはデフォルト アクションを変更しない限り、すべてのトラフィックがその侵入ポリシーによって検査されます。

侵入防御の展開をカスタマイズするために、複数のネットワーク分析ポリシーを作成し、それぞれがトラフィックを異なる方法で処理するように調整できます。次に、どのポリシーがどのトラフィックを検査するかを指定するルールを、アクセス コントロール ポリシーに設定します。アクセス コントロール ルールは単純でも複雑でもかまいません。セキュリティ ゾーン、ネットワークまたは地理的位置、VLAN、ポート、アプリケーション、要求された URL、またはユーザなど、複数の基準を使用してトラフィックを照合および検査します。

侵入ポリシーの主な機能は、次のように、どの侵入ルールおよびプリプロセッサ ルールを有効にしてどのように設定するかを管理することです。

- 各侵入ポリシーで、環境に適用されるすべてのルールが有効であることを確認し、環境に適用されないルールを無効化することによって、パフォーマンスを向上させます。インライン展開では、どのルールによって悪質なパケットをドロップまたは変更するかを指定できます。
- Firepower 推奨機能を使用すると、ネットワーク上で検出されたオペレーティング システム、サーバ、およびクライアント アプリケーション プロトコルを、それらの資産を保護するために作成されたルールに関連付けることができます。
- 必要に応じて、既存のルールの変更や、新しい標準テキストルールの作成により、新たなエクスプロイトの検出やセキュリティ ポリシーの適用が可能です。

侵入ポリシーに対して行えるその他のカスタマイズは次のとおりです。

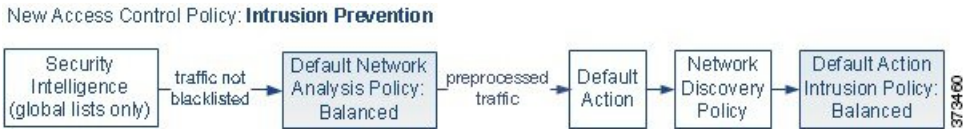
- 機密データ プリプロセッサは、ASCII テキストのクレジット カード番号や社会保障番号などの機密データを検出します。特定の脅威（Back Orifice 攻撃、何種類かのポートスキャン、および過剰なトラフィックによってネットワークを過負荷状態に陥らせようとするレートベース攻撃）を検出するプリプロセッサは、ネットワーク分析ポリシーで設定します。
- グローバルしきい値を設定すると、侵入ルールに一致するトラフィックが、指定期間内に特定のアドレスまたはアドレス範囲で送受信される回数に基づいて、イベントが生成されます。これにより、大量のイベントによってシステムに過剰な負荷がかかることを回避できます。
- また、個々のルールまたは侵入ポリシー全体に対して、侵入イベント通知を抑制し、しきい値を設定することで、大量のイベントによってシステムに過剰な負荷がかかることを回避することもできます。
- Web インターフェイス内での侵入イベントをさまざまな形式で表示することに加えて、syslog ファシリティへのロギングを有効にしたり、イベント データを SNMP トラップ サーバに送信したりできます。ポリシーごとに、侵入イベントの通知限度を指定したり、外部ロギング ファシリティに対する侵入イベントの通知をセットアップしたり、侵入イベントへの外部応答を設定したりできます。これらのポリシー単位のアラート設定に加えて、各ルールまたはルール グループの侵入イベントを通知する電子メール アラートをグローバルに有効化/無効化できます。どの侵入ポリシーがパケットを処理するかに関わらず、ユーザの電子メール アラート設定が使用されます。

カスタム ポリシーの制限

前処理と侵入インスペクションは非常に密接に関連しているため、単一のパケットを処理および検査する、ネットワーク分析ポリシーと侵入ポリシーが相互補完することを設定で許可する場合は、注意する**必要があります**。

デフォルトでは、システムは、管理対象デバイスでアクセス コントロール ポリシーにより処理されるすべてのトラフィックを、1つのネットワーク分析ポリシーを使用して前処理します。次の図は、インラインの侵入防御展開で、新たに作成されたアクセス コントロール ポリシー

が最初にトラフィックを処理するしくみを示しています。前処理および侵入防御のフェーズが強調表示されています。



アクセス コントロール ポリシーで処理されるすべてのトラフィックの前処理が、デフォルトのネットワーク分析ポリシーによってどのように制御されるのか注意してください。初期段階では、システムによって提供される Balanced Security and Connectivity ネットワーク分析ポリシーがデフォルトです。

前処理を調整する簡単な方法は、デフォルトとしてカスタム ネットワーク分析ポリシーを作成して使用することです。ただし、カスタム ネットワーク分析ポリシーでプリプロセッサが無効化されているときに、前処理されたパケットを有効な侵入ルールまたはプリプロセッサ ルールと照合して評価する必要がある場合、システムはプリプロセッサを有効化して使用します。ただし、ネットワーク分析ポリシーの Web ユーザ インターフェイスではプリプロセッサは無効なままになります。

（注） プリプロセッサを無効化してパフォーマンスを向上させるには、どの侵入ポリシーでもプリプロセッサを要求するルールが有効になっていないことを確認する**必要があります**。

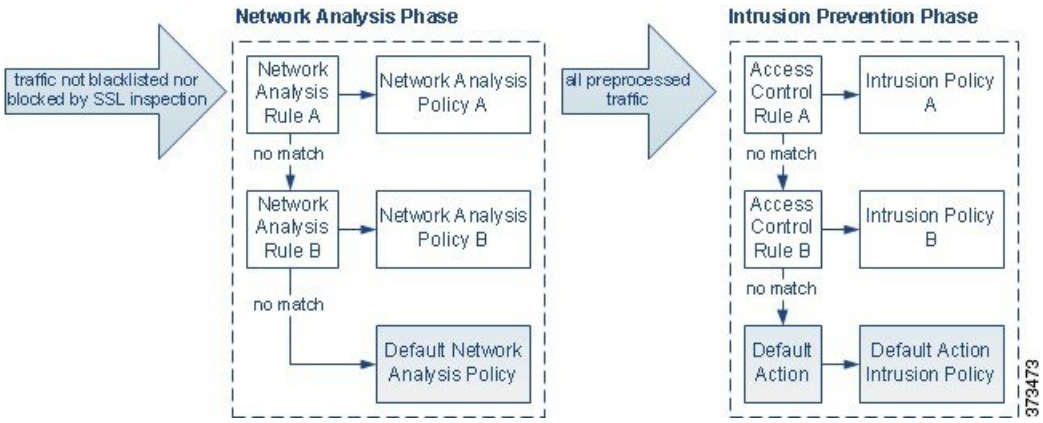
複数のカスタム ネットワーク分析ポリシーを使用する場合は、さらに課題があります。複雑な展開内の上級ユーザの場合は、一致したトラフィックの前処理にカスタム ネットワーク分析ポリシーを割り当てることによって、特定のセキュリティ ゾーン、ネットワーク、VLAN に合わせて前処理を調整できます。（ただし、ASA FirePOWER VLAN による前処理を制限できません）。これを実現するには、アクセス コントロール ポリシーにカスタム ネットワーク分析ルールを追加します。各ルールには、ルールに一致したトラフィックの前処理を制御するネットワーク分析ポリシーが関連付けられています。

ヒント アクセス コントロール ポリシーの詳細設定としてネットワーク分析ルールを設定します。Firepower システムの他のタイプのルールとは異なり、ネットワーク分析ルールは、ネットワーク分析ポリシーに含まれるのではなく、ネットワーク分析ポリシーを呼び出します。

システムは、ルール番号の昇順で、設定済みネットワーク分析ルールとパケットを照合します。ネットワーク分析ルールーに一致しなかったトラフィックは、デフォルトのネットワーク分析ポリシーによって前処理されます。これにより非常に柔軟にトラフィックを前処理できます。ただし、留意すべき点として、パケットがどのネットワーク分析ポリシーによって前処理されるかに**関係なく**、すべてのパケットは、アクセス コントロール ルール独自のプロセスで引き続きアクセス コントロール ルールと照合されます（つまり、侵入ポリシーにより検査される可能性があります）。つまり、特定のネットワーク分析ポリシーでパケットを前処理しても、そのパケットが確実に特定の侵入ポリシーで検査されるわけでは**ありません**。適切なネッ

トワーク分析ポリシーと侵入ポリシーを呼び出して特定のパケットを評価するように、注意してアクセス コントロール ポリシーを設定する**必要があります**。

次の図は、侵入防御（ルール）フェーズよりも前に、別にネットワーク分析ポリシー（前処理）の選択フェーズが発生するしくみを詳細に示しています。簡略化するために、図では検出フェーズとファイル/マルウェア インスペクション フェーズが省かれています。また、デフォルトのネットワーク分析ポリシーとデフォルト アクションの侵入ポリシーは強調表示されています。



このシナリオでは、アクセス コントロール ポリシーは、2 つのネットワーク分析ルールとデフォルトのネットワーク分析ポリシーで設定されています。

- ネットワーク分析ルール A は、ネットワーク分析ポリシー A とトラフィックとの照合を前処理します。その後、このトラフィックを侵入ポリシー A によって検査できます。
- ネットワーク分析ルール B は、ネットワーク分析ポリシー B とトラフィックとの照合を前処理します。その後、このトラフィックを侵入ポリシー B によって検査できます。
- 残りのトラフィックはすべて、デフォルトのネットワーク分析ポリシーにより前処理されます。その後、アクセス コントロール ポリシーのデフォルト アクションに関連付けられている侵入ポリシーによってこのトラフィックを検査できます。

システムはトラフィックを前処理した後、侵入についてトラフィックを検査できます。図は、2つのアクセスコントロールルールとデフォルトアクションが設定されたアクセスコントロール ポリシーを示しています。

- アクセス コントロール ルール A は、一致したトラフィックを許可します。その後、トラフィックは侵入ポリシー A により検査されます。
- アクセス コントロール ルール B は、一致したトラフィックを許可します。その後、トラフィックは侵入ポリシー B により検査されます。
- アクセス コントロール ポリシーのデフォルト アクションは一致したトラフィックを許可します。その後、トラフィックはデフォルト アクションの侵入ポリシーによって検査されます。

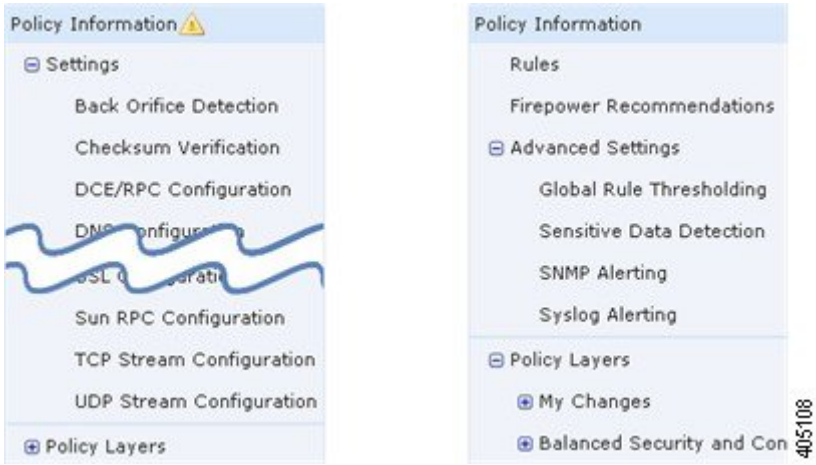
各パケットの処理は、ネットワーク分析ポリシーと侵入ポリシーのペアにより制御されますが、このペアはユーザに合わせて調整**されません**。アクセス コントロール ポリシーが誤って設定されているため、ネットワーク分析ルール A とアクセス コントロール ルール A が同じトラフィックを処理しない場合を想定してください。たとえば、特定のセキュリティ ゾーンのトラフィックの処理を制御するポリシーペアを意図していた場合に、誤って、異なるゾーンを使用するように 2 つのルールの条件を設定したとします。この誤設定により、トラフィックが誤って前処理される可能性があります。このような理由から、ネットワーク分析ルールとカスタム ポリシーを使用して前処理を調整することは、**高度な**タスクです。

単一の接続の場合、アクセス コントロール ルールよりも前にネットワーク分析ポリシーが選択されますが、いくつかの前処理（特にアプリケーション層の前処理）はアクセス コントロール ルールの選択後に実行されます。これは、カスタム ネットワーク分析ポリシーでの前処理の設定方法に**影響しません**。

ナビゲーション ウィンドウ: ネットワーク分析と侵入ポリシー

ネットワーク分析ポリシーと侵入ポリシーは同様の Web インターフェイスを使用して、設定への変更を編集して保存します。

いずれかのタイプのポリシーを編集するときに、Web インターフェイスの左側にナビゲーション パネルが表示されます。次の図は、ネットワーク分析ポリシー（左）および侵入ポリシー（右）のナビゲーション パネルを示しています。



ナビゲーション パネルは境界線によって複数のポリシー設定項目リンクに分割されており、ポリシー層との直接対話により（下側）または直接対話なしで（上側）ポリシー設定項目を設定できます。いずれかの設定ページに移動するには、ナビゲーション パネル内の名前をクリックします。ナビゲーション パネルで影付きで強調表示されている項目は、現在の設定ページを示しています。たとえば、上の図では、[Policy Information] ページがナビゲーション パネルの右側に表示されます。

Policy Information

[Policy Information] ページには、一般的に使用される設定の設定オプションが表示されます。上記のネットワーク分析ポリシーパネルの図に示すように、ポリシーに未保存の変更がある場合は、ナビゲーションパネルの [Policy Information] の横にポリシー変更アイコン（  ）が表示されます。このアイコンは、変更を保存すると表示されなくなります。

Rules（侵入ポリシーのみ）

侵入ポリシーの [ルール（Rules）] ページでは、共有オブジェクト ルール、標準テキスト ルール、およびプリプロセッサ ルールのルール ステータスとその他の設定項目を設定できます。

[Firepower の推奨事項（Firepower Recommendations）]（侵入ポリシーのみ）

侵入ポリシーの [Firepower の推奨事項（Firepower Recommendations）] ページでは、ネットワーク上で検出されたオペレーティング システム、サーバ、およびクライアント アプリケーション プロトコルを、それらの資産を保護するために作成されたルールに関連付けることができます。これにより、モニタ対象のネットワークの特定ニーズに合わせて侵入ポリシーを調整できます。

Settings（ネットワーク分析ポリシーのみ）と Advanced Settings（侵入ポリシーのみ）

ネットワーク分析ポリシーの [Settings] ページでは、プリプロセッサとアクセス プリプロセッサの設定ページを有効または無効にすることができます。[Settings] リンクを展開すると、ポリシー内で有効になっているすべてのプリプロセッサを個々に設定する設定ページへのサブリンクが表示されます。

侵入ポリシーの [Advanced Settings] ページでは、詳細設定ページと詳細設定のアクセス設定ページを有効または無効にすることができます。[Advanced Settings] リンクを展開すると、ポリシー内で有効になっているすべての詳細設定を個々に設定する設定ページへのサブリンクが表示されます。

Policy Layers

[Policy Layers] ページには、ネットワーク分析ポリシーまたは侵入ポリシーを構成するレイヤの要約が表示されます。[Policy Layers] リンクを展開すると、ポリシー内のレイヤに関するサマリ ページへのサブリンクが表示されます。各レイヤのサブリンクを展開すると、レイヤで有効になっているすべてのルール、プリプロセッサ、または詳細設定を個々に設定する設定ページへのサブリンクが表示されます。

競合と変更：ネットワーク分析および侵入ポリシー

ネットワーク分析ポリシーや侵入ポリシーを編集するときに、ポリシーに未保存の変更がある場合は、そのことを示すために、ナビゲーション パネルの [ポリシー情報（Policy Information）] の横にポリシー変更アイコン（  ）が表示されます。変更をシステムに認識させるには、変更を保存（確定）する必要があります。

（注） 保存後は、変更を反映させるためにネットワーク分析ポリシーまたは侵入ポリシーを展開する必要があります。保存しないでポリシーを展開すると、最後に保存された設定が使用されます。

編集競合の解決

[ネットワーク分析ポリシー（Network Analysis Policy）] ページ（**[Policies]** > **[Access Control]**、次に **[Network Analysis Policy]** または **[Policies]** > **[Access Control]** > **[Intrusion]**、次に **[Network Analysis Policy]**）および [侵入ポリシー（Intrusion Policy）] ページ（**[Policies]** > **[Access Control]** > **[Intrusion]**）には、各ポリシーの未保存の変更の有無、および現在ポリシーを編集中のユーザ情報が表示されます。シスコでは、同時に1人だけがポリシーを編集することを推奨します。同時編集を実行すると、次のようになります。

- ネットワーク分析ポリシーまたは侵入ポリシーを編集しているときに、同時に他のユーザが同じポリシーを編集し、ポリシーへの変更を保存した場合、ポリシーを確定すると、他のユーザの変更が上書きされることを警告するメッセージが表示されます。
- 同一ユーザとして複数の Web インターフェイス経由で同じネットワーク分析ポリシーまたは侵入ポリシーを編集し、1 つのインスタンスの変更を保存すると、他のインスタンスの変更を保存できなくなります。

設定の依存関係の解決

特定の分析を実行する場合、多くのプリプロセッサ ルールとセキュリティ ルールでは、最初に特定の方法でトラフィックをデコードまたは前処理するか、他の依存関係を割り当てる必要があります。ネットワーク分析ルールまたは侵入ポリシーを保存すると、システムは必要な設定を自動的に有効にするか、または警告を発して、設定を無効化してもトラフィックに影響がないことを示します。

- SNMPルールアラートを追加しても、SNMPアラートを設定しなかった場合は、侵入ポリシーを保存できません。SNMPアラートを設定するかルールアラートを無効化してから、再度保存する必要があります。
- 侵入ポリシーに有効なセンシティブ データ ルールが含まれているときに、センシティブ データ プリプロセッサが有効になっていない場合は、侵入ポリシーを保存できません。システムがプリプロセッサを有効化してポリシーを保存することを許可するか、ルールを無効化して再度保存する必要があります。
- ネットワーク分析ポリシーで必要なプリプロセッサを無効化しても、まだポリシーを保存できます。ただし、ネットワーク分析ポリシーの Web インターフェイスでプリプロセッサは無効になっていても、システムは無効になっているプリプロセッサを自動的に現在の設定で使用します。
- ネットワーク分析ポリシーでインラインモードを無効にして、インライン正規化プリプロセッサを有効化した場合は、ポリシーを保存できます。ただし、正規化設定が無視されることが警告されます。インラインモードを無効化すると他の設定が無視されるので、プリ

プロセッサは、チェックサム検証やレートベース攻撃の防御を含めて、トラフィックを変更またはブロックできます。

ポリシー変更のコミット、破棄、およびキャッシュ

ネットワーク分析ポリシーまたは侵入ポリシーの編集時に、変更を保存しないでポリシー エディタを終了した場合、それらの変更はシステムによってキャッシュされます。変更は、システムからログアウトしたり、システムクラッシュが発生したりした場合でもキャッシュされます。システム キャッシュには、ユーザごとに1つのネットワーク分析ポリシーと1つの侵入ポリシーの未保存の変更しか格納されないため、同じタイプの別のポリシーを編集する場合は、その前に、行った変更を確定または破棄する必要があります。システムは、ユーザが最初のポリシーへの変更を保存せずに別のポリシーを編集したり、侵入ルールの更新をインポートした場合に、キャッシュされた変更内容を破棄します。

ネットワーク分析ポリシー エディタまたは侵入ポリシー エディタの [ポリシー情報（Policy Information）] ページでポリシーの変更内容をコミットまたは破棄できます。

Firepower Management Center 設定では、以下を制御できます。

- ネットワーク分析ポリシーまたは侵入ポリシーへの変更を確定するときに、それに関するコメントの入力を求めるか（または、コメントの入力を必須とするか）
- 変更内容とコメントを監査ログに記録するか

関連トピック

ネットワーク解析ポリシーの設定の構成
侵入ポリシー設定の構成

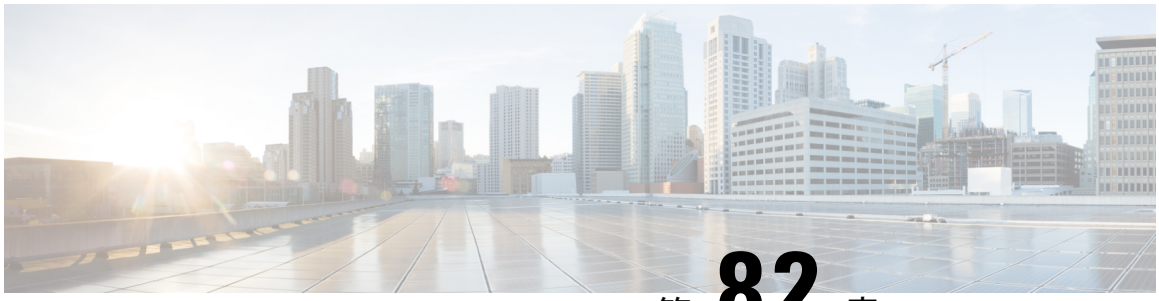
ネットワーク分析または侵入ポリシーの終了

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Intrusion Admin

ネットワーク分析、または侵入ポリシーの拡張エディタを終了するには、以下の方法があります。

- キャッシュ：ポリシーを終了し、変更をキャッシュするには、いずれかのメニューを選択するか、別のページへのほかのパスを選択します。終了時に表示される [ページを移動（Leave page）] をクリックするか、[ページを移動しない（Stay on page）] をクリックして拡張エディタに残ります。
- 破棄：保存されていない変更を破棄するには、[ポリシー情報（Policy Information）] ページの [変更の破棄（Discard Changes）] をクリックし、[OK] をクリックします。

- 保存：ポリシーの変更を保存するには、[ポリシー情報（Policy Information）] ページの [変更の確定（ommit Changes）] をクリックします。プロンプトが表示される場合、コメントを入力し、[OK] をクリックします。



第 82 章

侵入ポリシーおよびネットワーク分析ポリシーのレイヤ

以下のトピックでは、侵入ポリシーおよびネットワーク分析ポリシーでレイヤ（層）を使用する方法について説明します。

レイヤの基本

多数の管理対象デバイスが存在する大規模な組織では、さまざまな部署や事業部門、場合によってはさまざまな企業の固有のニーズをサポートするために、多数の侵入ポリシーやネットワーク分析ポリシーが存在することがあります。両方のポリシータイプでの設定はレイヤと呼ばれる構成要素に含まれており、それを使用することで効率的に複数のポリシーを管理することができます。

侵入ポリシーとネットワーク分析ポリシーのレイヤは、基本的に同じように動作します。どちらのポリシータイプも、レイヤを意識せずに作成したり編集することができます。ポリシー設定を変更でき、ポリシーにユーザ レイヤを追加していない場合は、システムによって自動的に変更内容が単一の設定可能なレイヤ（最初は *My Changes* という名前が付けられています）に含められます。また、最大200までレイヤを追加して、それらのレイヤで設定を任意に組み合わせて構成することもできます。ユーザ レイヤのコピー、マージ、移動、削除を実行できます。最も重要なこととして、個々のユーザ レイヤを同じタイプの他のポリシーと共有できます。

レイヤ スタック

レイヤ スタックは、次の各レイヤから構成されています。

ユーザ レイヤ

ユーザ設定可能なレイヤです。ユーザ設定可能なレイヤは、コピー、マージ、移動、または削除を行うことができます。また、任意のユーザ設定可能なレイヤが同じタイプの他のポリシーと共有されるように設定することもできます。このレイヤには、最初にMy Changesという名前が付けられた自動生成されたレイヤが含まれています。

組み込み型レイヤ

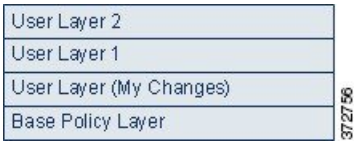
読み取り専用の基本ポリシー レイヤです。このレイヤ内のポリシーは、システムによって提供されるポリシー、または自分で作成したカスタム ポリシーにできます。

ネットワーク分析ポリシーまたは侵入ポリシーには、デフォルトでは基本ポリシー レイヤとMy Changes レイヤが含まれています。ユーザ レイヤは必要に応じて追加できます。

各ポリシー レイヤには、ネットワーク分析ポリシーのすべてのプリプロセッサの全設定、または、侵入ポリシーの侵入ルールと詳細設定がすべて含まれています。最下位の基本ポリシー レイヤには、ポリシーの作成時に選択した基本ポリシーのすべての設定が含まれています。上位レイヤの設定は、下位レイヤの同じ設定よりも優先されます。レイヤで明示的に設定されていない機能は、明示的に設定されている次に上位のレイヤの設定を継承します。システムはレイヤをフラット化します。つまり、ネットワーク トラフィックの処理時にすべての設定の蓄積効果のみを適用します。

ヒント 侵入またはネットワークの分析ポリシーは、基本ポリシーのデフォルト設定のみに基づいて作成できます。侵入ポリシーの場合に、モニタ対象ネットワークの特定のニーズに合わせて侵入ポリシーを調整したいときは、Firepower のルール状態の推奨を使用することもできます。

次の図は、基本ポリシー レイヤと初期設定の My Changes レイヤの他に、2 つの追加のユーザ設定可能なレイヤ *User Layer 1* と *User Layer 2* も含まれているレイヤ スタックの例を示しています。この図では、ユーザが追加したユーザ設定可能なレイヤそれぞれがスタックの最上位レイヤとして最初に配置されるため、図内のUser Layer 2が最後に追加されたもので、このスタックの最上位になっていることに注目してください。



ルール アップデートによるポリシーの変更を許可しているかどうかに関わらず、ルール アップデートによる変更は、ユーザがレイヤで行った変更を上書きしません。これは、ルールアップデートよる変更は、基本ポリシー レイヤのデフォルト設定を決定する基本ポリシーに対して行われるからです。ユーザによる変更はより上位のレイヤで行われるので、その変更によって、ルール アップデートによる基本ポリシーの変更が上書きされます。

基本レイヤ

侵入ポリシーまたはネットワーク分析ポリシーの基本レイヤ（基本ポリシーとも呼ばれる）は、ポリシーのすべての設定のデフォルト設定を定義し、ポリシーの最下位に位置します。新しいポリシーを作成し、新しいレイヤを追加しないで設定を変更すると、その変更はMy Changesレイヤに保存され、基本ポリシーの設定を変更するのではなく、上書きます。

システム提供の基本ポリシー

Firepowerシステムには、ネットワーク分析ポリシーと侵入ポリシーのペアがいくつか提供されています。システム提供のネットワーク分析ポリシーおよび侵入ポリシーを使用して、Cisco Talos Intelligence Group（Talos） のエクスペリエンスを活用することができます。これらのポリシーでは、Talosは侵入ルールおよびプリプロセッサ ルールの状態を設定し、プリプロセッサおよび他の詳細設定の初期設定も提供します。これらのシステム付属のポリシーはそのまま使用することも、カスタム ポリシーの基本として使用することもできます。

システム付属のポリシーを基本として使用する場合は、ルールアップデートをインポートすると基本ポリシーの設定が変更されます。ただし、カスタムポリシーを設定して、これらの変更内容がシステム提供の基本ポリシーに自動的に反映されないようにすることもできます。これにより、ルール更新とは関係ないスケジュールで、システム提供の基本ポリシーを手動で更新できます。いずれの場合も、ルール更新が基本ポリシーに加えた変更によってMy Changesまたは他のレイヤの設定が変更または上書きされることはありません。

システム付属の侵入ポリシーとネットワーク分析ポリシーには同じような名前が付いていますが、異なる設定が含まれています。たとえば、「Balanced Security and Connectivity」ネットワーク分析ポリシーと「Balanced Security and Connectivity」侵入ポリシーは連携して動作し、どちらも侵入ルールのアップデートで更新できます。

カスタム基本ポリシー

カスタム ポリシーを基本（ベース）として使用することができます。カスタム ポリシーの設定を調整することで、最も役立つ方法でトラフィックを検査できます。これによって、管理対象デバイスのパフォーマンスが向上し、ユーザは生成されたイベントにさらに効率的に対応できるようになります。

別のポリシーのベースとして使用するカスタムポリシー変更すると、変更内容はこのベースを使用するポリシーのデフォルト設定として自動的に使用されます。

また、ポリシーはすべて、システムが提供するポリシーをポリシーチェーンにおける最終的なベースとしているため、たとえカスタム基本ポリシーを使っていても、ルールが更新されればポリシーに影響する可能性があります。チェーン内の最初のカスタム ポリシー（システムによって提供されるポリシーをベースとして使用するポリシー）によってルール更新がその基本ポリシーを変更することが許可されている場合は、ポリシーが影響を受ける可能性があります。

基本ポリシーがどのように変更されたかに関わらず（ルール更新による変更でも、基本ポリシーとして使用するカスタム ポリシーを変更でも）、ユーザの基本ポリシーに対する変更によってMy Changesやその他のレイヤの設定が変更または上書きされることはありません。

基本ポリシーに対するルール更新の影響

ルール更新をインポートすると、システム提供の侵入ポリシー、アクセス コントロール ポリシー、ネットワーク分析ポリシーが変更されます。ルール更新には次の要素が含まれる場合があります。

- 変更されたネットワーク分析プリプロセッサの設定
- 変更された侵入ポリシーおよびアクセス コントロール ポリシーの詳細設定
- 新規または更新された侵入ルール
- 既存のルールの変更された状態
- 新しいルール カテゴリとデフォルト変数

ルール更新により、既存のルールがシステム提供のポリシーから削除される場合もあります。

デフォルト変数とルール カテゴリに対する変更はシステム レベルで処理されます。

システム提供のポリシーを侵入またはネットワーク分析の基本ポリシーとして使用するときは、ルール更新が基本ポリシー（この場合はシステムによって提供されるポリシーのコピー）を変更することを許可することができます。ルール更新で基本ポリシーの更新を許可する場合は、新しいルール更新によって、基本ポリシーとして使用するシステム提供のポリシーに対する変更と同じ変更が基本ポリシーにも加えられます。対応する設定を変更しなかった場合は、基本ポリシー内の設定によって、新しいポリシー内の設定が決定されます。ただし、ユーザがポリシーに加えた変更は、新しいルール アップデートによって上書きされません。

ルール更新による基本ポリシーの変更を許可しない場合は、1 つ以上のルール更新のインポート後に、基本ポリシーを手動で更新できます。

ルール更新では、侵入ポリシー内のルール状態またはルール更新による基本の侵入ポリシーの変更が許可されているかどうかに関係なく、Talos が削除した侵入ルールが常に削除されます。

ネットワーク トラフィックに変更を再展開するまで、現在展開されている侵入ポリシー ルールは次のように動作します。

- 無効になっている侵入ルールは無効のままになります。
- [イベントを生成する（Generate Events）] に設定されたルールでは、トリガーされたときのイベントの生成が継続されます。
- [ドロップしてイベントを生成する（Drop and Generate Events）] に設定されたルールでは、トリガーされたときのイベントの生成と違反パケットのドロップが継続されます。

次の両方の条件が満たされていない場合、ルールアップデートはカスタム基本ポリシーを変更しません。

- ルール アップデートによる親ポリシーのシステム付属基本ポリシー（カスタム基本ポリシーの元となるポリシー）の変更が許可されている。
- 親の基本ポリシー内の対応する設定が上書きされる親ポリシー内の変更を実施していない。

両方の条件が満たされている場合は、親ポリシーを保存したときに、ルール更新内の変更が子ポリシー（つまり、カスタム基本ポリシーを使用したポリシー）に渡されます。

たとえば、無効化されていた侵入ルールがルールアップデートによって有効化され、親となる侵入ポリシーのルールの状態がユーザによって変更されていない場合は、親ポリシーの保存時に、変更されたルール状態が基本ポリシーに渡されます。

同様に、ルールアップデートによってデフォルトのプリプロセッサ設定が変更され、親となるネットワーク分析ポリシーの設定がユーザによって変更されていない場合は、親ポリシーの保存時に、変更された設定が基本ポリシーに渡されます。

ベースポリシーの変更

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Intrusion Admin

別のシステム提供のポリシーまたはカスタム ポリシーを基本ポリシーとして使用できます。

最大 5 つのカスタム ポリシーをチェーンすることができます。5 つのうちの 4 つのポリシーで事前に作成されたポリシーが基本ポリシーとして使用され、5つ目のポリシーでシステムによって提供されたポリシーをベースとして使用する必要があります。

ステップ 1 ポリシーの編集中に、ナビゲーション パネルで [ポリシー情報（Policy Information）] をクリックします。

ステップ 2 次の選択肢を設定できます。

- 基本ポリシーを選択する：[基本ポリシー（Base Policy）] ドロップダウンリストから選択します。
- ベースポリシーを変更するルール更新を許可する：[ベースポリシーの管理（Manage Base Policy）] をクリックし、[新しいルール更新のインストールでポリシーを更新する（Update when a new Rule Update is installed）] チェックボックスをオンにします。

  ヒント このチェックボックスをオフにしてポリシーを保存してから、ルール更新をインポートすると、[基本ポリシー（Base Policy）] 概要ページに [今すぐ更新（Update Now）] ボタンが表示され、そのページ上のステータス メッセージが更新されて、ポリシーが期限切れであることが示されます。最近インポートしたルール更新内の変更で基本ポリシーを更新するには、[今すぐ更新（Update Now）] をクリックします。

ステップ 3 最後にポリシーを確定してからこのポリシーで加えた変更を保存するには、[ポリシー情報（Policy Information）] をクリックし、[変更の確定（Commit Changes）] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後の変更は破棄されます。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

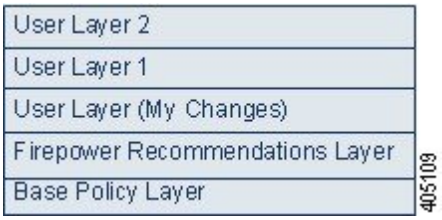
関連トピック

競合と変更：ネットワーク分析および侵入ポリシー （2041 ページ）

Firepower 推奨レイヤ

侵入ポリシーでルール状態の推奨を生成する場合は、その推奨に基づいてルール状態を自動的に変更するかどうかを選択できます。

下記の図に示すように、推奨されたルール状態を使用すると、侵入ポリシーの基本レイヤのすぐ上に読み取り専用の組み込み Firepower 推奨レイヤが挿入されます。



このレイヤは侵入ポリシー固有のものです。

それ以後、推奨されたルール状態を使用しないことを選択すると、Firepower 推奨レイヤは削除されます。このレイヤは手動で削除できませんが、推奨されるルール状態を使用するかどうかを選択することで、サービスを追加したり削除することができます。

Firepower 推奨レイヤを追加すると、ナビゲーション パネルの [ポリシー階層（Policy Layers）] の下に Firepower 推奨リンクが追加されます。このリンクから Firepower 推奨レイヤ ページの読み取り専用ビューにアクセスして、[ルール（Rules）]ページの推奨でフィルタリングされたビューを読み取り専用モードで表示できます。

推奨されたルール状態を使用すると、ナビゲーション パネルの Firepower 推奨リンクの下に [ルール（Rules）] サブリンクも追加されます。[ルール（Rules）] サブリンクから、Firepower 推奨レイヤの [ルール（Rules）] ページの読み取り専用画面にアクセスできます。このビューでは次の点に注意してください。

- 状態列にルール状態のアイコンがない場合、状態は基本ポリシーから継承されます。
- このビューまたは他の [ルール（Rules）] ページ ビューの Firepower 推奨列にルール状態のアイコンがない場合、このルールに対する推奨は存在しません。

関連トピック

ネットワーク資産に応じた侵入防御の調整 （2107 ページ）

レイヤ管理

[ポリシー層（Policy Layers）] ページには、ネットワーク分析ポリシーまたは侵入ポリシーの完全なレイヤスタックの単一ページの概要が示されます。このページでは、共有レイヤや非共有レイヤを追加したり、レイヤをコピー、マージ、移動、削除したり、各レイヤの概要ページにアクセスすることができます。また、各レイヤ内の設定を有効化、無効化、上書きするための設定ページにもアクセスできます。

各レイヤについて、次の情報が表示されます。

- レイヤが組み込み型レイヤ、共有ユーザ レイヤ、または非共有ユーザ レイヤであるかどうか
- どのレイヤが、最も上位の（つまり、効率的な）プリプロセッサまたは詳細設定を含んでいるか（機能名別に表示）
- 侵入ポリシーにおける、レイヤに状態が設定されている侵入ルールの数、および各ルール状態に対して設定されているルールの数。

[ポリシー層（Policy Layers）] ページには、有効なすべてのプリプロセッサ（ネットワーク分析）または詳細設定（侵入）、また侵入ポリシーの場合は侵入ルールの最終的な効果の概要も示されます。

各レイヤのサマリーにある機能名は、以下のように、設定がレイヤで有効、無効、上書き、または継承されているかを示します。

機能の状態	機能名
レイヤで有効	プレーン テキストで表示
レイヤで無効	取り消し線が引かれる
上位レイヤの設定によって上書きされる	イタリック テキストで表示
下位レイヤから継承される	表示されない

最大200のレイヤをネットワーク分析ポリシーまたは侵入ポリシーに追加できます。レイヤを追加すると、そのレイヤがポリシーの最上位レイヤとして表示されます。すべての機能の初期状態が継承され、侵入ポリシーでは、イベント フィルタリング、動的状態、アラート ルール アクションは設定されません。

レイヤをポリシーに追加する際は、ユーザが設定可能なレイヤに一意の名前を指定します。その名前は後で変更できます。また、必要に応じて、レイヤを編集する際に表示される説明を追加あるいは変更することもできます。

レイヤはコピーすることも、[ユーザ レイヤ（User Layers）] ページ内での表示位置を上下に移動することもできます。また、初期の My Changes レイヤを含め、ユーザ レイヤを削除することも可能です。以下の点に注意してください。

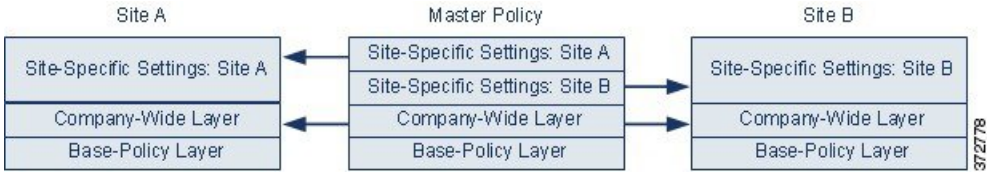
- レイヤをコピーすると、そのコピーが最上位レイヤとして表示されます。
- 共有レイヤをコピーすると、初期状態ではそのレイヤは共有されませんが、必要に応じて、後から共有できます。
- 共有レイヤは削除できません。共有が有効になっているレイヤで別のポリシーと共有していないものは、共有レイヤではありません。

ユーザ設定可能なレイヤの直下に、別のユーザ設定可能なレイヤをマージできます。マージされたレイヤは、どちらかのレイヤに固有だったすべての設定を保持します。また、両方のレイヤに同じプリプロセッサ、侵入ルールまたは詳細設定の設定が含まれている場合は、上位のレイヤの設定を受け入れます。マージされたレイヤでは、下位レイヤの名前が保持されます。他のポリシーに追加できる共有可能なレイヤを作成するポリシーでは、共有可能なレイヤのすぐ上に非共有レイヤのある共有可能なレイヤをマージできますが、共有可能なレイヤの直下には非共有レイヤのある共有可能なレイヤをマージすることはできません。別のポリシーに作成した共有レイヤを追加するポリシーでは、共有レイヤをそのすぐ下の非共有レイヤとマージできますが、作成されたレイヤは共有されなくなります。非共有レイヤをその下の共有レイヤとマージすることはできません。

共有レイヤ

共有レイヤとは、あるポリシー内で作成して共有を許可し、別のポリシーに追加されたレイヤのことです。共有可能レイヤとは、共有が許可されているレイヤのことです。

以下の図に示すマスター ポリシーの例では、全社的レイヤと、サイト A およびサイト B に固有のレイヤを作成し、これらのサイト固有のレイヤの共有を許可しています。その上で、これらのサイト固有のレイヤを共有レイヤとしてサイト A とサイト B のポリシーに追加しています。



マスター ポリシーの全社的なレイヤには、サイト A とサイト B に適用される設定が含まれる一方、サイト固有のレイヤには各サイトに固有の設定が含まれています。たとえば、ネットワーク分析ポリシーの場合、サイト A にはモニタ対象ネットワークに Web サーバがないため、保護したり、HTTP インスペクション プリプロセッサのオーバーヘッドを処理したりする必要はありませんが、両方のサイトで TCP ストリームの前処理が必要になる場合があります。両方のサイトで共有する全社的レイヤで TCP ストリーム処理を有効にし、サイト A で共有するサイト固有のレイヤで HTTP Inspect プリプロセッサを無効にして、サイト B で共有するサイト固有のレイヤで HTTP Inspect プリプロセッサを有効にできます。サイト固有のポリシーで上位レイヤの設定を編集することで、必要に応じて、設定の調整によって各サイトのポリシーをさらに調整することもできます。

この例のマスターポリシーでフラット化された設定値そのものがトラフィックをモニタするのに役立つわけではありませんが、サイト固有のポリシーを設定および更新する際に時間が節約されるため、ポリシー階層で活用することができます。

その他にも多くのレイヤ設定が可能です。たとえば、企業、部門、ネットワーク、さらにはユーザごとにポリシーのレイヤを定義できます。侵入ポリシーの場合は、一方のレイヤに詳細設定を含め、もう一方にルール設定を含めることもできます。

ユーザ設定可能なレイヤを同じタイプの他のポリシー（侵入またはネットワーク分析）と共有できるように設定できます。共有可能レイヤ内の設定を変更し、変更をコミットすると、そのレイヤを共有するすべてのポリシーが更新され、影響を受けたすべてのポリシーのリストが提供されます。レイヤを作成したポリシーの機能設定のみを変更できます。

別のポリシーに追加しているレイヤの共有を無効にすることはできません。まずレイヤを他のポリシーから削除するか、他のポリシーを削除する必要があります。

基本ポリシーが共有するレイヤが作成されたカスタムポリシーである場合、ポリシーに共有レイヤを追加することはできません。追加した場合、ポリシーで依存関係が循環することになります。

マルチドメイン展開では、先祖ポリシーの共有レイヤを子孫ドメインのポリシーに追加できます。

レイヤの管理

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Intrusion Admin

ステップ 1 ポリシーの編集中に、ナビゲーション パネルで [ポリシー層（Policy Layers）] をクリックします。

ステップ 2 [ポリシー層（Policy Layers）] ページでは、次に示す管理アクションを実行できます。

- 別のポリシーからの共有レイヤの追加：[ユーザ レイヤ（User Layers）] の横にある共有レイヤの追加アイコン（  ）をクリックし、[共有レイヤの追加（Add Shared Layer）] ドロップダウンリストからレイヤを選択して、[OK] をクリックします。
- 非共有レイヤの追加：[ユーザ レイヤ（User Layers）] の横にあるレイヤの追加アイコン（  ）をクリックし、[名前（Name）] を入力して、[OK] をクリックします。
- レイヤの説明の追加または変更：レイヤの横にある編集アイコン（  ）をクリックして、[説明（Description）] を追加または変更します。
- 別のポリシーとのレイヤの共有の許可：レイヤの横にある編集アイコン（  ）をクリックして、[共有（Sharing）] チェックボックスをオフにします。
- レイヤの名前の変更：レイヤの横にある編集アイコン（  ）をクリックして、[名前（Name）] を変更します。

- レイヤのコピー：レイヤのコピー アイコン（）をクリックします。
- レイヤの削除：レイヤの削除アイコン（）をクリックして、[OK] をクリックします。
- 2 つのレイヤのマージ：2 つのレイヤの上部のマージ アイコン（）をクリックして、[OK] をクリックします。
- レイヤの移動：レイヤ サマリ内の任意の空いている場所をクリックし、位置矢印（）が移動するレイヤの上または下の行を指すまでドラッグします。

ステップ 3 最後にポリシーを確定してからこのポリシーで加えた変更を保存するには、[ポリシー情報（Policy Information）] をクリックし、[変更の確定（Commit Changes）] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後の変更は破棄されます。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

関連トピック

競合と変更：ネットワーク分析および侵入ポリシー （2041 ページ）

レイヤ間のナビゲーション

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Intrusion Admin

ステップ 1 ポリシーの編集中に、ナビゲーション パネルで [ポリシー層（Policy Layers）] をクリックします。

ステップ 2 レイヤの移動は、次のいずれかのアクションで実行できます。

- プリプロセッサ ページまたは詳細設定ページにアクセスする：レイヤ レベルのプリプロセッサまたは詳細設定の設定ページにアクセスするには、そのレイヤに対応する行の機能名をクリックします。基本ポリシーおよび共有レイヤでは、設定ページは読み取り専用です。
- ルール ページにアクセスする：ルールの状態タイプでフィルタ処理されたレイヤ レベルのルール設定ページにアクセスする場合は、レイヤの概要でイベントのドロップおよび生成アイコン（）、イベントの生成アイコン（）、または無効化アイコン（）をクリックします。選択したルール状態に設定されているルールがレイヤに含まれていない場合、ルールは表示されません。
- [ポリシー情報ページ（Policy Information）] ページを表示する：[ポリシー情報ページ（Policy Information）]ページを表示するには、ナビゲーション ウィンドウで [ポリシーの概要（Policy Summary）] をクリックします。

- レイヤの概要ページを表示する：レイヤの概要ページを表示するには、レイヤに対応する行のレイヤ名をクリックするか、ユーザ レイヤの横にある編集アイコン（  ）をクリックします。表示アイコン（  ）をクリックして、共有レイヤの読み取り専用のサマリ ページにアクセスすることもできます。

ステップ 3 最後にポリシーを確定してからこのポリシーで加えた変更を保存するには、[ポリシー情報（Policy Information）] をクリックし、[変更の確定（Commit Changes）] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後の変更は破棄されます。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

関連トピック

競合と変更：ネットワーク分析および侵入ポリシー （2041 ページ）

レイヤでの侵入ルール

レイヤの [Rules] ページで個々の設定を表示することも、[Rules] ページのポリシー ビューですべての設定の実質的な効果を表示することもできます。[ルール（Rules）] ページのポリシー ビューのルール設定を変更する場合、ポリシーの最上位のユーザ設定可能なレイヤを変更します。[ルール（Rules）] ページにあるレイヤ ドロップダウンリストを使用して、別のレイヤに切り替えることができます。

次の表では、複数のレイヤで同じ種類の設定を構成した場合の結果について説明しています。

表 *138 :* レイヤ ルールの設定

設定可能なレイヤ数	設定の種類	目的
1	ルール状態	下位レイヤのルールに対して設定されたルール状態を上書きします。また、下位レイヤで設定されたそのルールのすべてのしきい値、抑制、レートベースのルール状態、およびアラートを無視します。 基本ポリシーまたは下位レイヤからルールのルール状態を継承したい場合は、ルール状態を [継承（Inherit）] に設定します。侵入ポリシーの [ルール（Rules）] ページは、すべてのルール設定の最終的な効果を示す複合ビューであるため、このページでの作業中にルールの状態を [継承（Inherit）] に設定することはできないことに注意してください。
1	しきい値 SNMP アラート	下位レイヤのルールの同じ種類の設定を上書きします。しきい値を設定すると、レイヤのルールの既存のしきい値が上書きされることに注意してください。
1 つ以上	抑制 レートベースのルール状態	選択した各ルールの同じ種類の設定を、ルール状態がそのルールに対して設定された最初の下位レイヤまで累積的に組み合わせます。ルール状態が設定されているレイヤより下の設定は無視されます。
1 つ以上	コメント	ルールにコメントを追加します。コメントは、ポリシー固有またはレイヤ固有ではなく、ルール固有です。任意のレイヤの 1 つのルールに 1 つ以上のコメントを追加できます。

たとえば、あるレイヤでルール状態を [Drop and Generate Events] に設定し、それよりも上位のレイヤで [Disabled] に設定した場合、侵入ポリシーの [Rules] ページには、ルールが無効であることが示されます。

別の例として、あるレイヤでルールの送信元ベースの抑制を 192.168.1.1 に設定し、別のレイヤでそのルールの宛先ベースの抑制を 192.168.1.2 に設定した場合、[Rules] ページには、送信元

アドレス 192.168.1.1 と宛先アドレス 192.168.1.2 に関するイベントを抑制する累積的な結果が示されます。抑制およびレートベースのルール状態の設定では、選択した各ルールの同じ種類の設定が、ルール状態がそのルールに対して設定された最初の下位レイヤまで累積的に組み合わせられることに注意してください。ルール状態が設定されているレイヤより下の設定は無視されます。

特定のレイヤの各 [ルール（Rules）] ページの色分けでは、有効状態が上位レイヤ、下位レイヤ、現在のレイヤのどれに該当するのかが次の色で示されます。

- 赤：上位レイヤでの有効状態
- 黄色：下位レイヤでの有効状態
- 陰影なし：現在のレイヤでの有効状態

侵入ポリシーの [ルール（Rules）] ページはすべてのルール設定の最終的な効果の複合ビューであるため、ルール状態はこのページでは色分けされません。

レイヤでの侵入ルールの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Intrusion Admin

侵入ポリシーでは、すべてのユーザ設定可能なレイヤのルールに対して、ルール状態、イベント フィルタリング、動的状態、アラート、およびルール コメントを設定できます。変更を加えるレイヤにアクセスした後、そのレイヤの [ルール（Rules）] ページの設定を、侵入ポリシーの [ルール（Rules）] ページの設定と同じように追加します。

ステップ 1 侵入ポリシーの編集中に、ナビゲーション パネルで [ポリシー層（Policy Layers）] を展開します。

ステップ 2 変更するポリシー階層を展開します。

ステップ 3 変更するポリシー レイヤのすぐ下にある [ルール（Rules）] をクリックします。

ステップ 4 ルールを使用した侵入ポリシーの調整 （2073 ページ） に示されている任意の設定を変更します。

ヒント 編集可能なレイヤから個々の設定を削除するには、そのレイヤの [ルール（Rules）] ページでルール メッセージをダブルクリックして、ルールの詳細を表示します。削除する設定の横にある [Delete] をクリックして [OK] を 2 回クリックします。

ステップ 5 最後にポリシーを確定してからこのポリシーで加えた変更を保存するには、[ポリシー情報（Policy Information）] をクリックし、[変更の確定（Commit Changes）] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後の変更は破棄されます。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

関連トピック

競合と変更：ネットワーク分析および侵入ポリシー （2041 ページ）

複数のレイヤからのルール設定の削除

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Intrusion Admin

侵入ポリシーの複数のレイヤから、特定のタイプのイベント フィルタ、動的状態、またはアラートを同時に削除できます。システムは選択された設定を削除し、ルールの残りの設定をポリシーの最上位の編集可能なレイヤにコピーします。

システムは、すべての設定を削除するか、ルール状態がルールに対して設定されているレイヤに遭遇するまで、下位方向にある各レイヤの同じ種類の設定を削除します。後者の場合、そのレイヤから設定が削除され、設定タイプの削除が停止されます。

共有レイヤまたは基本ポリシーに指定されたタイプの設定があり、ポリシーの最上位レイヤが編集可能である場合は、ルールの残りの設定とルール状態がその編集可能なレイヤにコピーされます。そうではない場合、ポリシーの最上位のレイヤが共有レイヤであれば、システムは新しい編集可能なレイヤをその共有レイヤの上に作成し、そのルールの残りの設定およびルール状態をその編集可能なレイヤにコピーします。

（注） 共有レイヤまたは基本ポリシーに由来するルール設定を削除すると、下位レイヤまたは基本ポリシーにおけるこのルールへの変更は無視されます。下位レイヤまたは基本ポリシーにおける変更が無視されないようにするには、最上位レイヤのサマリ ページでルール状態を [Inherit] に設定します。

ステップ 1 侵入ポリシーの編集中に、ナビゲーション ウィンドウで [ポリシー情報（Policy Information）] のすぐ下にある [ルール（Rules）] をクリックします。

ヒント また、任意のレイヤの [ルール（Rules）] ページでレイヤのドロップダウンリストから [ポリシー（Policy）] を選択するか、[ポリシー情報（Policy Information）] ページの [ルールの管理（Manage Rules）] をクリックすることもできます。

ステップ 2 複数の設定を削除するルールを選択します。

- 特定の選択（Choose specific）：特定のルールを選択するには、各ルールの横にあるチェックボックスをオンにします。

- すべて選択（Choose all）：現在のリストのルールをすべて選択するには、列の上部にあるチェックボックスをオンにします。

ステップ 3 次のいずれかのオプションを選択します。

- **[イベントのフィルタリング（Event Filtering）] > [しきい値の削除（Remove Thresholds）]**
- **[イベントのフィルタリング（Event Filtering）] > [抑制の削除（Remove Suppressions）]**
- **[動的状態（Dynamic State）] > [レート ベースのルール状態の削除（Remove Rate-Based Rule States）]**
- **[アラート（Alerting）] > [SNMP アラートの削除（Remove SNMP Alerts）]**

（注） 共有レイヤまたは基本ポリシーに由来するルール設定を削除すると、下位レイヤまたは基本ポリシーにおけるこのルールへの変更は無視されます。下位レイヤまたは基本ポリシーにおける変更が無視されないようにするには、最上位レイヤのサマリ ページでルール状態を [Inherit] に設定します。

ステップ 4 [OK] をクリックします。

ステップ 5 最後にポリシーを確定してからこのポリシーで加えた変更を保存するには、[ポリシー情報（Policy Information）] をクリックし、[変更の確定（Commit Changes）] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後の変更は破棄されます。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

関連トピック

競合と変更：ネットワーク分析および侵入ポリシー （2041 ページ）

カスタム基本ポリシーからのルール変更の受け入れ

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Intrusion Admin

レイヤを追加していないカスタム ネットワーク分析ポリシーまたは侵入ポリシーが別のカスタム ポリシーを基本ポリシーとして使用するとき、以下を行う場合は、そのルール状態を継承するようにルールを設定する必要があります。

- 基本ポリシーのルールに設定されたイベント フィルタ、動的状態、または SNMP アラートを削除する場合、および

- 基本ポリシーとして使用する他のカスタムポリシー内のルールに行った後続の変更をルールが受け入れるようにする場合

ステップ 1 侵入ポリシーの編集中に、ナビゲーション パネルで [ポリシー層（Policy Layers）] を展開します。

ステップ 2 [個人用の変更（My Changes）] を展開します。

ステップ 3 [個人用の変更（My Changes）] のすぐ下にある [ルール（Rules）] リンクをクリックします。

ステップ 4 設定を受け入れるルールを選択します。次の選択肢があります。

- [特定ルールの選択（Choose specific rules）]：特定のルールを選択するには、各ルールの横にあるチェックボックスをチェックします。
- [すべてのルールを選択（Choose all rules）]：現在のリストのすべてのルールを選択する場合は、列の最上部にあるチェックボックスをチェックします。

ステップ 5 [ルール状態（Rule State）] ドロップダウンリストから、[継承（Inherit）] を選択します。

ステップ 6 最後にポリシーを確定してからこのポリシーで加えた変更を保存するには、[ポリシー情報（Policy Information）] をクリックし、[変更の確定（Commit Changes）] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後の変更は破棄されます。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

関連トピック

競合と変更：ネットワーク分析および侵入ポリシー （2041 ページ）

レイヤでのプリプロセッサと詳細設定

ネットワーク分析ポリシーでのプリプロセッサの設定および侵入ポリシーでの詳細設定の設定と同様の方法を使用します。ネットワーク分析の [Settings] ページでプリプロセッサを有効化/無効化したり、侵入ポリシーの [Advanced Settings] ページで侵入ポリシーの詳細設定を有効化/無効化することができます。これらのページには、すべての関連機能の有効状態の概要も表示されます。たとえば、ネットワーク分析 SSL プリプロセッサが、あるレイヤで無効になっており、そのレイヤよりも上位のレイヤで有効になっている場合、[Settings] ページではそのプリプロセッサが有効であると表示されます。このページで加えられる変更は、ポリシーの最上位のレイヤに表示されます。Back Orifice プリプロセッサにはユーザ設定可能なオプションがないことに注意してください。

また、プリプロセッサまたは詳細設定を有効化または無効化したり、ユーザ設定可能なレイヤのサマリ ページの設定ページにアクセスしたりできます。このページで、レイヤの名前および説明を変更し、レイヤを同じタイプの他のポリシーと共有するかどうかを設定できます。ナビ

ゲーション パネルの [ポリシー層（Policy Layers）] の下のレイヤの名前を選択することによって、別のレイヤのサマリー ページに切り替えることができます。

プリプロセッサまたは詳細設定を有効にすると、ナビゲーション パネルのレイヤ名の下にその機能の設定ページへのサブリンクが表示され、レイヤのサマリ ページの機能の横に編集アイコン（  ）が表示されます。これらは、レイヤで機能を無効化するか [Inherit] に設定すると表示されなくなります。

プリプロセッサまたは詳細設定の状態（有効または無効）を設定すると、下位レイヤでこの機能の状態と設定が上書きされます。プリプロセッサまたは詳細設定に、基本ポリシーまたは下位レイヤの状態と設定を継承させる場合は、状態を [Inherit] に設定します。[Settings or Advanced Settings] ページで作業するときは、[Inherit] の選択が表示されません。また、現在有効にされている機能を継承すると、ナビゲーション パネルではその機能のサブリンクが表示されなくなり、設定ページではその機能の編集アイコンが表示されなくなることにも注意してください。

システムでは、設定が有効になっている最も上位のレイヤの設定が使用されます。設定を明示的に変更しなかった場合は、デフォルト設定が使用されます。たとえば、ネットワーク分析 DCE/RPC プリプロセッサをあるレイヤで有効にして変更し、それよりも上位のレイヤでは有効にするが、変更しない場合は、上位レイヤのデフォルト設定が使用されます。

各レイヤのサマリ ページは次のようにカラーコード化されており、有効な設定が上位レイヤ、下位レイヤ、または現在のレイヤのいずれにあるかが示されます。

- 赤色：有効な設定は上位レイヤにあります
- 黄色：有効な設定は下位レイヤにあります
- 陰影なし：有効な設定は現在のレイヤにあります

[設定（Settings）] および [詳細設定（Advanced Settings）] ページは、関連するすべての設定の複合ビューであるため、これらのページは有効な設定の位置を示すためにカラー コーディングを使用しません。

層のプリプロセッサと詳細の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Intrusion Admin

ステップ 1 ポリシーの編集中に、ナビゲーション パネルで [ポリシー層（Policy Layers）] を展開し、変更するレイヤの名前をクリックします。

ステップ 2 次の選択肢があります。

- 層の名前を変更します。
- 説明を追加または変更します。

- [共有（Sharing）] チェックボックスをオンまたはオフにして、層を別のポリシーと共有できるようにするかどうかを指定します。
- 有効にしたプリプロセッサ/詳細設定の設定ページにアクセスするには、編集アイコン（  ）または機能のサブリンクをクリックします。
- 現在の層のプリプロセッサ/詳細設定を無効にするには、機能の横にある [無効化（Disabled）] をクリックします。
- 現在の層のプリプロセッサ/詳細設定を有効にするには、機能の横にある [有効化（Enabled）] をクリックします。
- 現在の層の下にある最上位レイヤの設定からプリプロセッサ/詳細設定の状態および構成を継承するには、[継承（Inherit）] をクリックします。

ステップ 3 最後にポリシーを確定してからこのポリシーで加えた変更を保存するには、[ポリシー情報（Policy Information）] をクリックし、[変更の確定（Commit Changes）] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後の変更は破棄されます。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

関連トピック

競合と変更：ネットワーク分析および侵入ポリシー （2041 ページ）

第 83 章

侵入ポリシーの使用を開始するには

ここでは、侵入ポリシーの使用を開始する方法について説明します。

侵入ポリシーの基本

侵入ポリシーは定義済みの侵入検知のセットであり、セキュリティ違反についてトラフィックを検査し、インライン展開の場合は、悪意のあるトラフィックをブロックまたは変更することができます。侵入ポリシーは、アクセス コントロール ポリシーによって呼び出され、システムの最終防御ラインとして、トラフィックが宛先に到達することを許可するかどうかを判定します。

各侵入ポリシーの中核となるのは、侵入ルールです。ルールを有効にすると、ルールに一致するトラフィックに対して侵入イベントが生成されます（さらに、必要に応じてトラフィックがブロックされます）。ルールを無効にすると、ルールの処理が停止されます。

Firepower システムが提供するいくつかの基本的な侵入ポリシーにより、Cisco Talos Intelligence Group（Talos）の経験を活用できます。これらのポリシーでは、Talos が侵入およびプリプロセッサ ルールの状態（有効または無効）を設定し、他の詳細設定の初期設定も行います。

ヒント システム付属の侵入ポリシーとネットワーク分析ポリシーには同じような名前が付いていますが、異なる設定が含まれています。たとえば、「Balanced Security and Connectivity」ネットワーク分析ポリシーと「Balanced Security and Connectivity」侵入ポリシーは連携して動作し、どちらも侵入ルールのアップデートで更新できます。ただし、ネットワーク分析ポリシーは主に前処理オプションを管理し、侵入ポリシーは主に侵入ルールを管理します。

カスタム侵入ポリシーを作成すると、以下を実行できます。

- ルールを有効化/無効化することに加え、独自のルールを作成して追加し、検出を調整する。
- ネットワーク上で検出されたオペレーティング システム、サーバ、およびクライアント アプリケーションプロトコルをそれらの資産を保護するために明確に書き込まれたルールに関連付けるには、Firepower の推奨事項を使用します。
- 外部アラート、センシティブ データの前処理、グローバル ルールのしきい値設定など、さまざまな詳細設定を設定する。
- レイヤを基本構成要素として使用し、複数の侵入ポリシーを効率的に管理する。

インライン展開では、侵入ポリシーによってトラフィックを変更したりブロックすることができます。

- 廃棄ルールを使用すると、一致したパケットをドロップして、侵入イベントを生成できます。侵入またはプリプロセッサの廃棄ルールを設定するには、そのステータスを [ドロップしてイベントを生成する（Drop and Generate Events）] に設定します。
- 侵入ルールでは、`replace` キーワードを使用して悪意のあるコンテンツを置き換えることができます。

侵入ルールがトラフィックに影響を与えるようにするには、廃棄ルールおよびコンテンツを置き換えるルールを適切に設定し、さらに管理対象デバイスを適切にインライン展開する（つまり、インラインインターフェイスセットを設定する）必要があります。最後に、侵入ポリシーのドロップ動作（[インライン時にドロップ（Drop when Inline）] 設定）を有効にします。

留意事項として、侵入ポリシーを調整する場合（特にルールを有効化して追加する場合）、一部の侵入ルールでは、最初に特定の方法でトラフィックをデコードまたは前処理する必要があります。侵入ポリシーによって検査される前に、パケットはネットワーク分析ポリシーの設定に従って前処理されます。必要なプリプロセッサを無効にすると、システムは自動的に現在の設定でプリプロセッサを使用します。ただし、ネットワーク分析ポリシーのWebインターフェイスではプリプロセッサは無効のままになります。

注意 前処理と侵入インスペクションは非常に密接に関連しているため、単一パケットを検査するネットワーク分析ポリシーと侵入ポリシーは、相互補完する**必要があります**。前処理の調整、特に複数のカスタム ネットワーク分析ポリシーを使用して調整することは、**高度な**タスクです。

カスタム侵入ポリシーを設定した後、それを 1 つ以上のアクセス コントロール ルールまたはアクセス コントロール ポリシーのデフォルト アクションに関連付けることによって、カスタム侵入ポリシーをアクセスコントロール設定の一部として使用できます。これによって、システムは、最終宛先に渡す前に、特定の許可されたトラフィックを侵入ポリシーによって検査します。変数セットを侵入ポリシーと組み合わて使用することにより、ホーム ネットワークと外部ネットワークに加えて、必要に応じてネットワーク上のサーバを正確に反映させることができます。

デフォルトでは、暗号化ペイロードの侵入インスペクションは無効化されます。これにより、侵入インスペクションが設定されているアクセス コントロール ルールと暗号化された接続を照合する際の誤検出が減少し、パフォーマンスが向上します。

侵入ポリシーの管理

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Intrusion Admin

[侵入ポリシー（Intrusion Policy）] ページ（**[Policies]** > **[Access Control]** > **[Intrusion]**）では、次に示す情報とともに、現在のカスタム侵入ポリシーを表示できます。

- ポリシーが最後に変更された日時（ローカル時間）とそれを変更したユーザ
- [Drop when Inline] 設定が有効になっているかどうか。この設定が有効な場合、インライン展開でトラフィックをドロップしたり変更することができます。
- トラフィックの検査に侵入ポリシーを使用しているアクセス コントロール ポリシーとデバイス
- ポリシーに保存されていない変更があるかどうか、およびポリシーを現在編集している人（いれば）に関する情報
- マルチドメイン展開では、ポリシーが作成されたドメイン

マルチドメイン展開では、編集できる現在のドメインで作成されたポリシーが表示されます。また、編集できない先祖ドメインで作成されたポリシーも表示されます。下位のドメインで作成されたポリシーを表示および編集するには、そのドメインに切り替えます。

ステップ 1 **[Policies]** > **[Access Control]** > **[Intrusion]**を選択します。

ステップ 2 侵入ポリシーを管理します。

- [比較（Compare）] : [ポリシーの比較（Compare Policies）] をクリックします（ポリシーの比較 （457 ページ） を参照）。
- 作成 : [ポリシーの作成（Create Policy）] をクリックします。カスタム侵入ポリシーの作成 （2067 ページ）を参照してください。

- 削除：削除するポリシーの横にある削除アイコン（）をクリックします。別のユーザが保存していないポリシーの変更がある場合は、システムによって確認と通知のプロンプトが表示されます。[OK] をクリックして確認します。

  コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

- 編集：編集するポリシーの横にある編集アイコン（）をクリックします。侵入ポリシーの編集（2067 ページ）を参照してください。

  代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

- エクスポート：別の Firepower Management Center にインポートするために、侵入ポリシーをエクスポートするには、エクスポート アイコン（）をクリックします。設定のエクスポート（232 ページ）を参照してください。

- 展開：[展開（Deploy）] をクリックします（設定変更の展開（447 ページ）を参照）。

- [レポート（Report）]：レポート アイコン（）をクリックします（現在のポリシー レポートの生成（459 ページ）を参照）。

カスタム侵入ポリシーの作成

新しい侵入ポリシーを作成する場合は、、一意の名前を付けて基本ポリシーを指定し、ドロップ動作を指定する必要があります。

基本ポリシーは侵入ポリシーのデフォルト設定を定義します。新しいポリシーの設定の変更は、基本ポリシーの設定を変更するのではなく、オーバーライドします。システム付属のポリシーまたはカスタム ポリシーを基本ポリシーとして使用できます。

侵入ポリシーのドロップ動作、または [Drop when Inline] の設定によって、廃棄ルール（ルール状態が [Drop and Generate Events] に設定されている侵入ルールまたはプリプロセッサ ルール）、およびトラフィックに影響を与えるその他の侵入ポリシー設定のシステムにおける処理方法が決まります。悪意のあるパケットをドロップまたは置き換える場合は、インライン展開でドロップ動作を有効にする必要があります。パッシブ展開では、ドロップ動作に関わらず、システムはトラフィック フローに影響を与えることはできません。

カスタム侵入ポリシーの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Intrusion Admin

ステップ 1 **[Policies]** > **[Access Control]** > **[Intrusion]**を選択します。

ステップ 2 [Create Policy] をクリックします。別のポリシー内に未保存の変更が存在する場合は、[Intrusion Policy] ページに戻るかどうか尋ねられたときに [Cancel] をクリックします。

ステップ 3 [名前（Name）] に一意の名前を入力し、オプションで [説明（Description）] を入力します。

ステップ 4 [基本ポリシー（Base Policy）] で最初の基本ポリシーを指定します。

システム提供のポリシーまたは別のカスタム ポリシーを基本ポリシーとして使用できます。

ステップ 5 インライン展開でのドロップ動作の設定 （2069ページ）の説明に従って、インライン導入でのシステムのドロップ動作を設定します。

ステップ 6 ポリシーを作成します。

- 新しいポリシーを作成して、[Intrusion Policy] ページに戻るには、[Create Policy] をクリックします。新しいポリシーには基本ポリシーと同じ設定項目が含まれています。
- ポリシーを作成し、高度な侵入ポリシー エディタでそれを開いて編集するには、[Create and Edit Policy] をクリックします（侵入ポリシーの変更 （2069 ページ）を参照）。

関連トピック

レイヤでの侵入ルール （2055 ページ）
競合と変更：ネットワーク分析および侵入ポリシー （2041 ページ）

侵入ポリシーの編集

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Intrusion Admin

ステップ 1 **[Policies]** > **[Access Control]** > **[Intrusion]**を選択します。

ステップ 2 設定する侵入ポリシーの横にある編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 ポリシーを編集します。

- 基本ポリシーの変更：[基本ポリシー（Base Policy）] ドロップダウン リストから基本ポリシーを選択します。ベースポリシーの変更 （2049 ページ）を参照してください。
- 詳細設定の構成：ナビゲーション パネルで [詳細設定（Advanced Settings）] をクリックします。侵入ポリシーの詳細設定 （2070 ページ）を参照してください。
- Firepower 推奨ルールの設定：ナビゲーション パネルで [Firepower 推奨ルール（Firepower Recommended Rules）] をクリックします。Firepower の推奨事項の生成と適用 （2111 ページ）を参照してください。
- インライン展開でのドロップ動作：[インライン時にドロップ（Drop when Inline）] をオンまたはオフにします。インライン展開でのドロップ動作の設定 （2069 ページ）を参照してください。
- 推奨ルール状態によるルールのフィルタ：推奨を生成した後、各推奨タイプの横にある [表示（View）] をクリックします。すべての推奨を表示するには、[推奨される変更の表示（View Recommended Changes）] をクリックします。
- 現在のルール状態によるルールのフィルタ：ルール状態タイプ（イベントを生成する、ドロップしてイベントを生成する）の横にある [表示（View）] をクリックします。侵入ポリシー内の侵入ルール フィルタ （2082 ページ）を参照してください。
- ポリシー階層の管理：ナビゲーション パネルで、[ポリシー層（Policy Layers）] をクリックします。レイヤ管理 （2051 ページ）を参照してください。
- 侵入ルールの管理：[ポリシー情報（Policy Information）] をクリックします。侵入ポリシー内の侵入ルールの表示 （2075 ページ）を参照してください。
- 基本ポリシーの設定の表示：[基本ポリシーの管理（Manage Base Policy）] をクリックします。基本レイヤ （2047 ページ）を参照してください。

ステップ 4 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報（Policy Information）] を選択して、[変更を確定（Commit Changes）] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後の変更は破棄されます。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

関連トピック

Firepower の推奨事項の生成と適用 （2111 ページ）
レイヤでの侵入ルールの設定 （2057 ページ）
競合と変更：ネットワーク分析および侵入ポリシー （2041 ページ）

侵入ポリシーの変更

新しい侵入ポリシーを作成すると、そのポリシーには基本ポリシーと同じ侵入ルールと詳細設定が付与されます。

システムは、ユーザごとに1つのセキュリティポリシーをキャッシュします。侵入ポリシーの編集中に、メニューまたは別のページへのパスを選択すると、そのページから移動しても、変更内容はシステム キャッシュに残ります。

インライン展開でのドロップ動作

実際にトラフィックを変更せず、使用している設定がインライン展開（つまり、ルーテッド、スイッチド、またはトランスペアレントインターフェイス、あるいはインラインインターフェイスペアを使用して、関連する設定がデバイスに展開されている）でどのように機能するかを評価する場合は、ドロップ動作を無効にすることができます。その場合、システムは侵入イベントを生成しますが、廃棄ルールをトリガーしたパケットをドロップしません。結果を確認したら、ドロップ動作を有効化できます。

パッシブ展開またはタップモードでのインライン展開では、ドロップ動作に関わらず、システムはトラフィックに影響を与えることはできません。つまり、パッシブ展開では、[ドロップしてイベントを生成する（Drop and Generate Events）] に設定されたルールは [イベントを生成する（Generate Events）] に設定されたルールと同様に動作します。システムは侵入イベントを生成しますが、パケットをドロップできません。

（注） FTP を介してマルウェアの転送をブロックするには、ネットワーク向け AMP を正しく設定するだけでなく、アクセス コントロール ポリシーのデフォルトの侵入ポリシーで [インライン時にドロップ（Drop when Inline）] を有効にする必要があります。

侵入イベントを表示する際に、ワークフローにインライン結果を含めることができます。インライン結果は、トラフィックが実際にドロップされたのか、あるいはドロップが想定に過ぎなかったのかを示します。

インライン展開でのドロップ動作の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Intrusion Admin

ステップ 1 **[Policies]** > **[Access Control]** > **[Intrusion]**を選択します。

ステップ 2 編集するポリシーの横にある編集アイコン（）をクリックします。

代わりに表示アイコン（  ）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 ポリシーのドロップ動作を設定します。

- [インライン時にドロップ（Drop when Inline）] チェックボックスをオンにして、侵入ルールのトラフィックへの適用とイベントの生成を許可します。
- [インライン時にドロップ（Drop when Inline）] チェックボックスをオフにすると、侵入ルールのトラフィックへの適用が禁止されますが、イベントは生成されます。

ステップ 4 [変更を確定（Commit Changes）] をクリックして、最後のポリシーの確定以降に、このポリシーに加えた変更を保存します。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後の変更は破棄されます。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

デュアル システム展開でのドロップ動作

ネットワーク内で2つのシステムが連続して接続されている場合、最初のシステムでドロップイベントが発生しても、2番目のシステムでドロップイベントまたは「ドロップ想定」イベントが記録されることは正常です。最初のシステムがファイルの最後のパケットをスキャンするまでにパケットをドロップすることを決定する一方で、2 番目のシステムもトラフィックを調査して「ドロップされる」と識別します。

たとえば、最初のパケットがルールをトリガーする 5 パケット HTTP GET リクエストは、最初のシステムによりブロックされ、最後のパケットのみがドロップされます。2 番目のシステムは 4 パケットのみを受信し、接続はドロップされますが、2 番目のシステムがセッションをプルーニングしている間に部分的な GET リクエストを最後にフラッシュすると、インライン結果として「ドロップ想定」と同じルールがトリガーされます。

侵入ポリシーの詳細設定

侵入ポリシーの詳細設定を設定するには、特定の専門知識が必要です。デフォルトで有効になる詳細設定や、詳細設定ごとのデフォルトは、侵入ポリシーの基本ポリシーに応じて決まります。

侵入ポリシーのナビゲーション パネルで [詳細設定（Advanced Settings）] を選択すると、ポリシーの詳細設定がタイプ別に一覧表示されます。[Advanced Settings] ページでは、侵入ポリシー

の詳細設定を有効または無効にしたり、詳細設定の設定ページにアクセスすることができます。詳細設定を行うには、それを有効にする必要があります。

詳細設定を無効にすると、サブリンクと [Edit] リンクは表示されなくなりますが、設定は保持されます。侵入ポリシーの一部の設定（センシティブ データ ルール、侵入ルールの SNMP アラート）では、詳細設定を有効化して適切に設定する必要があります。

詳細設定を変更する場合、変更する設定と、その変更がネットワークに及ぼす可能性のある影響について理解していることが必要です。

特定の脅威の検出（Specific Threat Detection）

機密データ プリプロセッサは、ASCII テキストのクレジット カード番号や社会保障番号などの機密データを検出します。

特定の脅威（Back Orifice 攻撃、何種類かのポートスキャン、および過剰なトラフィックによってネットワークを過負荷状態に陥らせようとするレートベース攻撃）を検出するプリプロセッサは、ネットワーク分析ポリシーで設定します。

侵入ルールしきい値（Intrusion Rule Thresholds）

グローバル ルールのしきい値を設定すると、しきい値を使用して、システムが侵入イベントを記録したり表示したりする回数を制限できるので、多数のイベントでシステムが圧迫されないようにすることができます。

外部レスポンス（External Responses）

Web インターフェイス内での侵入イベントをさまざまな形式で表示することに加えて、システム ログ（syslog）ファシリティへのロギングを有効にしたり、イベント データを SNMP トラップ サーバに送信したりできます。ポリシーごとに、侵入イベントの通知限度を指定したり、外部ロギング ファシリティに対する侵入イベントの通知をセットアップしたり、侵入イベントへの外部応答を設定したりできます。

これらのポリシー単位のアラート設定に加えて、各ルールまたはルール グループの侵入イベントを通知する電子メール アラートをグローバルに有効化/無効化できます。どの侵入ポリシーがパケットを処理するかに関わらず、ユーザの電子メール アラート設定が使用されます。

関連トピック

機密データ検出の基本 （2113 ページ）
グローバル ルールのしきい値の基本 （2129 ページ）

侵入検知および防御のパフォーマンスの最適化

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Access Admin/Network Admin (access control); Admin/Discovery Admin (network discovery)

Firepower システムを使用して侵入検知および防御を実行するものの検出データを利用する必要がない場合は、以下の説明に従って新しい検出を無効にしてパフォーマンスを最適化できます。

ステップ 1 ターゲット デバイスに導入したアクセス コントロール ポリシーと関連付けられたルールを変更または削除します。そのデバイスに関連付けられたアクセス制御ルールはいずれも、ユーザ、アプリケーション、またはURL の条件を指定できません（アクセス コントロール ルールの作成および編集 （1698 ページ）を参照）。

ステップ 2 ターゲット デバイスのネットワーク検出ポリシーからすべてのルールを削除します（ネットワーク検出ルールの設定 （2650 ページ）を参照）。

ステップ 3 変更された設定をターゲット デバイスに導入します（設定変更の展開 （447 ページ）を参照）。

第 84 章

ルールを使用した侵入ポリシーの調整

ここでは、ルールを使用して侵入ポリシーを調整する方法について説明します。

侵入ルールの調整の基本

侵入ポリシーの [ルール（Rules）] ページを使用して、共有オブジェクト ルール、標準テキスト ルール、プリプロセッサ ルールに関するルール状態とその他の設定を構成できます。

ルールは、ルール状態を [Generate Events] または [Drop and Generate Events] に設定することによって有効にします。ルールを有効にすると、システムがそのルールと一致するトラフィックに対するイベントを生成します。ルールを無効にすると、ルールの処理が停止されます。また、インライン展開で [ドロップしてイベントを生成する（Drop and Generate Events）] に設定されたルールによって、一致するトラフィックに対するイベントが生成され、そのトラフィックが破棄されるように、侵入ポリシーを設定できます。パッシブ展開では、[Drop and Generate Events] に設定されたルールによって、一致するトラフィックに対するイベントが生成されるだけです。

ルールのサブセットを表示するようにルールをフィルタ処理することによって、ルール状態やルール設定を変更するルールのセットを正確に選択できます。

侵入ルールまたはルールの引数がプリプロセッサの無効化を必要とする場合、ネットワーク分析ポリシーの Web インターフェイスではプリプロセッサが無効化されたままになりますが、システムは自動的に現在の設定でプリプロセッサを使用します。

侵入ルールのタイプ

侵入ルールとは、ネットワーク内の脆弱性を不正利用する試みを検出するためにシステムが使用する、指定されたキーワードと引数のセットのことです。システムはネットワークトラフィックを分析する際に、パケットを各ルールに指定された条件に照らし合わせ、データパケットがルールに指定されたすべての条件を満たす場合、そのルールをトリガーします。

侵入ポリシーには以下の構成要素があります。

- 侵入ルール。共有オブジェクト ルールと標準テキスト ルールに分割されます。
- プリプロセッサ ルール。パケット デコーダの検出オプション、または Firepower システムに付属のプリプロセッサの 1 つに関連付けられます。

次の表に、以上のルール タイプの属性を要約します。

表 *139 :* 侵入ルールのタイプ

タイプ	ジェネレータ ID（GID）	[Snort ID]（SID）	ソース	コピーの可否	編集の可否
共有オブジェクト ルール	3	1000000 未満	Cisco Talos Intelligence Group（Talos）	Yes	制限付き
標準テキストルール	1（グローバル ドメインまたはレガシー GID）	1000000 未満	Talos	Yes	制限付き
	1000～2000（子孫ドメイン）	1000000 以上	ユーザが作成またはインポート	はい	はい
プリプロセッサルール	デコーダまたはプリプロセッサに固有	1000000 未満	Talos	いいえ	いいえ
		1000000 以上	オプション設定時にシステムにより生成	いいえ	いいえ

Talos によって作成されたルールを変更して保存することはできませんが、変更されたルールのコピーをカスタム ルールとして保存することはできます。ルールで使用される変数またはルール ヘッダー情報（送信元と宛先のポートや IP アドレスなど）を変更できます。マルチドメイン展開では、Talos によって作成されるルールはグローバル ドメインに属します。子孫ドメインの管理者は、ルールのローカル コピーを保存してから、ルールを編集できます。

Talos によって作成されるルールには、各デフォルト侵入ポリシー内でデフォルトのルール状態が割り当てられます。ほとんどのプリプロセッサルールがデフォルトで無効になっているた

め、システムにプリプロセッサ ルールに対するイベントの生成とインライン展開での違反パケットの破棄を行わせる場合は、これらのルールを有効にする必要があります。

侵入ポリシー内の侵入ルールの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Intrusion Admin

侵入ポリシー内のルールの表示方法を調整したり、複数の条件によってルールをソートできます。特定のルールの詳細を表示して、ルール設定、ルール ドキュメント、およびその他のルール仕様を確認することもできます。

ステップ 1 **[Policies]** > **[Access Control]** > **[Intrusion]**を選択します。

ステップ 2 編集するポリシーの横にある編集アイコン（）をクリックします。

代わりに表示アイコン（  ）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 ナビゲーション パネルの [ポリシー情報（Policy Information）] の下にある [ルール（Rules）] をクリックします。

ステップ 4 ルールを表示している間、以下を実行できます。

- 侵入ポリシー内のルール フィルタの設定 （2091 ページ）の説明に従ってルールをフィルタリングします。
- ソートの基準とするカラムの一番上のタイトルまたはアイコンをクリックすることによって、ルールをソートします。
- 侵入ルール詳細の表示 （2077 ページ）の説明に従って、侵入ルールの詳細を表示します。
- [ポリシー（Policy）] ドロップダウン リストから階層を選択することによって、異なるポリシー階層のルールを表示します。

[侵入ルール（Intrusion Rules）] ページの列

[侵入ルール（Intrusion Rules）] ページでは、メニュー バーおよび列ヘッダーに同じアイコンが使用されます。たとえば、[ルール状態（Rule State）] メニューでは、ルール リストの [ルール状態（Rule State）] 列と同じアイコン（）が使用されます。

表 *140 : [*ルール（*Rules*）*]* ページの列

見出し	説明
GID	ルールのジェネレータ ID（GID）を表す整数。
SID	ルールの固有識別子として機能する [Snort ID]（SID）を表す整数。 カスタム ルールの場合、SID は 1000000 以上です。
Message	このルールによって生成されるイベントに含まれるメッセージ。ルールの名前としても機能します。
	ルールのルール状態。 • ドロップしてイベントを生成する（） • イベントを生成する（  ） • 無効（  ） 無効なルールのアイコンは、トラフィックをドロップせずにイベントを生成するように設定されたルールのアイコンのグレー表示されたバージョンです。また、ルールのルール状態アイコンをクリックすると、ルール状態を変更できます。
	ルールの Firepower 推奨ルール状態。
	ルールに適用されるイベントしきい値やイベント抑制などのイベント フィルタ。
	ルールの動的ルール状態。指定されたレート異常が発生した場合に有効になります。
	ルールに対して設定されたアラート（現在は SNMP アラートのみ）。
	ルールに追加されたコメント。

階層ドロップダウン リストを使用して、ポリシー内の他の階層の [Rules] ページに切り替えることもできます。ポリシーにレイヤを追加しなかった場合にドロップダウンリストに表示される編集可能なビューはポリシーの [ルール（Rules）] ページと、元は `My Changes` という名前だったポリシー階層の [ルール（Rules）] ページだけであることに注意してください。これらのビューの一方を変更すると、もう一方も同じように変更されることにも注意してください。ドロップダウンリストには、読み取り専用の基本ポリシーの [ルール（Rules）] ページも表示されます。

侵入ルールの詳細

[ルールの詳細（Rule Detail）] ビューで、ルール ドキュメント、Firepower の推奨事項、およびルール オーバーヘッドを表示できます。また、ルール固有の機能を表示および追加できます。

表 *141* : ルールの詳細

項目	説明
Summary	ルールの概要。ルール ベースのイベントでは、ルール ドキュメントに概要情報が含まれている場合にこのローが表示されます。
Rule State	ルールの現在のルール状態。ルール状態が設定された階層も示します。
Firepower の推奨事項（Firepower Recommendation）	Firepower の推奨事項が生成されている場合は、推奨されるルール状態を表すアイコン。[侵入ルール（Intrusion Rules）]ページの列（2075 ページ）を参照してください。ルールを有効にすることが推奨されている場合、システムは推奨事項をトリガーしたネットワーク アセットまたは設定も示します。
ルールのオーバーヘッド（Rule Overhead）	システム パフォーマンスに対するルールの潜在的影響とルールが誤検出を引き起こす確率。脆弱性にマップされていないローカル ルールにはオーバーヘッドが割り当てられていません。
Thresholds	このルールに現在設定されているしきい値と、ルールのしきい値を追加するための機能。
Suppressions	このルールに現在設定されている抑制設定と、ルールの抑制を追加するための機能。
Dynamic State	このルールに現在設定されているレート ベースのルール状態と、ルールの動的ルール状態を追加するための機能。
Alerts	このルールに設定されている SNMP アラートと、ルールのアラートを追加するための機能。
Comments	このルールに追加されたコメントと、ルールのコメントを追加するための機能。
Documentation	Cisco Talos Intelligence Group（Talos）によって提供される現在のルールのルール ドキュメント。必要に応じて、[ルール ドキュメンテーション（Rule Documentation）]をクリックして、ルールの詳細を表示します。

侵入ルール詳細の表示

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Intrusion Admin

ステップ 1 **[Policies]** > **[Access Control]** > **[Intrusion]**を選択します。

ステップ 2 編集するポリシーの横にある編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 ナビゲーション ペインで [ルール（Rules）] をクリックします。

ステップ 4 ルールの詳細を表示したいルールをクリックし、ページの下部にある [詳細の表示（Show Details）] をクリックします。
侵入ルールの詳細 （2076 ページ）で説明されているように、ルールの詳細が表示されます。

ステップ 5 ルールの詳細から、以下を設定できます。

- アラート：侵入ルールの SNMP アラートの設定 （2081 ページ）を参照してください。
- コメント：侵入ルールへのコメントの追加 （2081 ページ）を参照してください。
- ダイナミック ルールの状態：[ルール詳細（Rule Details）] ページからの動的ルール状態の設定 （2080 ページ）を参照してください。
- しきい値：侵入ルールのしきい値の設定 （2078 ページ）を参照してください。
- 抑制：侵入ルールの抑制の設定 （2079 ページ）を参照してください。

侵入ルールのしきい値の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Intrusion Admin

[Rule Detail] ページで、ルールの単一のしきい値を設定できます。しきい値を追加すると、ルールの既存のしきい値が上書きされます。

無効な値を入力するとフィールドに復元アイコン（）が表示される点に注意してください。そのアイコンをクリックすると、そのフィールドの最後の有効値に戻るか、以前の値が存在しない場合はフィールドが空になります。

ステップ 1 侵入ルールの詳細で、[しきい値（Thresholds）] の横にある [追加（Add）] をクリックします。

ステップ 2 [タイプ（Type）] ドロップダウンリストから、設定するしきい値のタイプを選択します。

- 指定された期間あたりのイベントインスタンス数に通知を制限する場合は、[制限（Limit）] を選択します。
- 指定された期間あたりのイベントインスタンス数ごとに通知を提供する場合は、[しきい値（Threshold）] を選択します。
- 指定されたイベントインスタンス数に達した後で、期間あたり 1 回ずつ通知を提供する場合は、[両方（Both）] を選択します。

ステップ 3 [追跡対象（Track By）] ドロップダウンリストから、[送信元（Source）] または [宛先（Destination）] を選択し、イベント インスタンスが送信元 IP アドレスまたは宛先 IP アドレスのどちらによって追跡されるかを指定します。

ステップ 4 [カウント（Count）] フィールドに、しきい値として使用するイベント インスタンスの数を入力します。

ステップ 5 [秒数（Seconds）] フィールドに、イベント インスタンスを追跡する期間（秒数）を指定する数値を入力します。

ステップ 6 [OK] をクリックします。

ヒント [イベント フィルタリング（Event Filtering）] カラムのルールの横にイベント フィルタ アイコン（）が表示されます。ルールに複数のイベント フィルタを追加すると、アイコン上にイベント フィルタの数が表示されます。

侵入ルールの抑制の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Intrusion Admin

侵入ポリシーのルールに対して 1 つ以上の抑制を設定できます。

無効な値を入力するとフィールドに復元アイコン（）が表示されることに注意してください。そのアイコンをクリックすると、そのフィールドの最後の有効値に戻るか、以前の値が存在しない場合はフィールドが空になります。

ステップ 1 侵入ルールの詳細で、[抑制（Suppressions）] の横にある [追加（Add）] をクリックします。

ステップ 2 [抑制タイプ（Suppression Type）] ドロップダウンリストから、次のいずれかのオプションを選択します。

- 選択したルールのイベントを完全に抑制する場合は、[ルール（Rule）] を選択します。
- 指定した送信元 IP アドレスから送信されるパケットによって生成されるイベントを抑制する場合は、[送信元（Source）] を選択します。
- 指定した宛先 IP アドレスに送信されるパケットによって生成されるイベントを抑制する場合は、[宛先（Destination）] を選択します。

ステップ 3 抑制タイプとして [送信元（Source）] または [宛先（Destination）] を選択した場合は、[ネットワーク（Network）] フィールドに IP アドレス、アドレス ブロック、またはそれらの任意の組み合わせで構成されたカンマ区切りのリストを入力します。

侵入ポリシーがアクセス コントロール ポリシーのデフォルト アクションに関連付けられている場合は、デフォルト アクション変数セットでネットワーク変数を指定または列挙することもできます。

システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。

ステップ 4 [OK] をクリックします。

ヒント　抑制するルールの横にある [イベント フィルタリング（Event Filtering）] カラムのルールの横にイベント フィルタ アイコン（  ）が表示されます。ルールに複数のイベント フィルタを追加した場合は、アイコン上の数字がフィルタの数を示します。

[ルール詳細（Rule Details）] ページからの動的ルール状態の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Intrusion Admin

1 つのルールに対して 1 つ以上の動的ルール状態を設定できます。最初に表示される動的ルール状態に最も高いプライオリティが割り当てられます。2 つの動的ルール状態が競合している場合は、最初のアクションが実行されます。

動的ルール状態はポリシー固有です。

無効な値を入力するとフィールドに復元アイコン（  ）が表示される点に注意してください。そのアイコンをクリックすると、そのフィールドの最後の有効値に戻るか、以前の値が存在しない場合はフィールドが空になります。

ステップ 1　侵入ルールの詳細で、[動的状態（Dynamic State）] の横にある [追加（Add）] をクリックします。

ステップ 2　[追跡対象（Track By）] ドロップダウンリストから、ルール一致の追跡方法を指定するオプションを選択します。

- 特定の送信元または送信元のセットからのそのルールのヒット数を追跡する場合は、[送信元（Source）] を選択します。
- 特定の宛先または宛先のセットへのそのルールのヒット数を追跡する場合は、[宛先（Destination）] を選択します。
- そのルールのすべての一致を追跡する場合は、[ルール（Rule）] を選択します。

ステップ 3　[追跡対象（Track By）] を [送信元（Source）] または [宛先（Destination）] に設定した場合は、[ネットワーク（Network）] フィールドに追跡する各ホストのアドレスを入力します。

システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。

ステップ 4　[レート（Rate）] の横で、攻撃レートを設定する期間あたりのルール一致の数を指定します。

- [カウント（Count）] フィールドで、しきい値として使用するルール一致の数を指定します。
- [秒（Seconds）] フィールドで、攻撃を追跡する期間を表す秒数を指定します。

ステップ 5　[新しい状態（New State）] ドロップダウンリストから、条件が満たされたときに実行する新しいアクションを選択します。

ステップ 6 [タイムアウト（Timeout）] フィールドに値を入力します。

タイムアウトが発生すると、ルールが元の状態に戻ります。新しいアクションがタイムアウトしないようにする場合は、0 を入力します。

ステップ 7 [OK] をクリックします。

ヒント [動的状態（Dynamic State）] 列のルールの横に動的状態アイコン（）が表示されます。ルールに複数の動的ルール状態フィルタを追加した場合は、アイコン上の数字がフィルタの数を示します。

侵入ルールの SNMP アラートの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Intrusion Admin

[ルールの詳細（Rule Detail）] ページで、ルールの SNMP アラートを設定できます。

侵入ルールの詳細で、[アラート（Alerts）] の横にある [SNMP アラートの追加（Add SNMP Alert）] をクリックします。

ヒント [アラート（Alerting）] 列のルールの横にアラート アイコン（）が表示されます。ルールに複数のアラートを追加した場合は、アイコン上にアラートの数が表示されます。

侵入ルールへのコメントの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Intrusion Admin

ステップ 1 侵入ルールの詳細で、[コメント（Comments）] の横の [追加（Add）] をクリックします。

ステップ 2 [コメント（Comments）] フィールドに、ルール コメントを入力します。

ステップ 3 [OK] をクリックします。

ヒント システムは [コメント（Comments）] カラムのルールの横にコメント アイコン（）を表示します。ルールに複数のコメントを追加した場合は、アイコン上の数字がコメントの数を示します。

ステップ 4 ルール コメントを削除するには、ルール コメント セクションで [Delete] をクリックします。侵入ポリシーの変更がコミットされずにコメントがキャッシュされている場合にだけコメントを削除できます。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

侵入ポリシー内の侵入ルール フィルタ

[ルール（Rules）] ページに表示するルールは、1 つの基準または 1 つ以上の基準の組み合わせに基づいてフィルタ処理できます。

ルール フィルタ キーワードは、ルール状態やイベント フィルタなどのルール設定を適用するルールを見つけやすくします。[Rules] ページのフィルタ パネルで必要な引数を選択することによって、キーワードでフィルタ処理すると同時に、キーワードの引数を選択することができます。

侵入ルール フィルタの注意事項

作成したフィルタが [Filter] テキスト ボックスに表示されます。フィルタ パネルでキーワードとキーワード引数をクリックしてフィルタを作成できます。複数のキーワードを選択した場合は、システムがそれらを AND ロジックを使用して結合し、複合検索フィルタを生成します。たとえば、[カテゴリ（Category）] で [プリプロセッサ（preprocessor）] を選択してから、**[ルール コンテンツ（Rule Content）]** > **[GID]** の順に選択して、「116」と入力すると、プリプロセッサ ルールで、**かつ**、GID が 116 のすべてのルールを取得する「`Category: "preprocessor" GID:"116"`」というフィルタが返されます。

[カテゴリ（Category）]、[Microsoft 脆弱性（Microsoft Vulnerabilities）]、[Microsoft ワーム（Microsoft Worms）]、[プラットフォーム特有（Platform Specific）]、[プリプロセッサ（Preprocessor）]、および [優先度（Priority）] の各フィルタ グループを使用すれば、カンマで区切られたキーワードの複数の引数を送信できます。たとえば、[カテゴリ（Category）] から [os-linux] と [os-windows] を選択すると、`os-linux` カテゴリまたは `os-windows` カテゴリ内のルールを取得する「`Category:"os-windows,os-linux"`」というフィルタを作成できます。

フィルタ パネルを表示するには、表示アイコン（  ）をクリックします。

フィルタ パネルを非表示にするには、非表示アイコン（  ）をクリックします。

侵入ポリシー ルール フィルタ構築のガイドライン

ほとんどの場合、フィルタを作成するときに、侵入ポリシー内の [ルール（Rules）] ページの左側にあるフィルタ パネルを使用して必要なキーワード/引数を選択できます。

フィルタ パネルでは、ルール フィルタがルール フィルタ グループに分類されます。多くのルール フィルタ グループにサブ基準が含まれているため、探している特定のルールを簡単に見つけることができます。一部のルール フィルタには複数のレベルが設定されているので、それを展開して個別のルールにドリルダウンできます。

フィルタ パネル内の項目は、場合によって、フィルタ タイプ グループを表したり、キーワードを表したり、キーワードの引数を表したりします。次の点に注意してください。

- キーワード（[ルール設定（Rule Configuration）]、[ルール コンテンツ（Rule Content）]、[プラットフォーム特有（Platform Specific）]、および [優先度（Priority）]）以外のフィルタ タイプ グループ見出しを選択すると、そのグループが展開されて使用可能なキーワードが一覧表示されます。

  基準リスト内のノードをクリックしてキーワードを選択すると、フィルタ条件とする引数を指定するためのポップアップ ウィンドウが表示されます。

  そのキーワードがすでにフィルタで使用されていた場合は、そのキーワードの既存の引数が指定した引数に置き換えられます。

  たとえば、フィルタ パネルの **[ルール設定（Rule Configuration）]** > **[推奨（Recommendation）]** で [ドロップしてイベントを生成する（Drop and Generate Events）] をクリックすると、「`Recommendation:"Drop and Generate Events"`」がフィルタ テキスト ボックスに追加されます。その後で、**[ルール設定（Rule Configuration）]** > **[推奨（Recommendation）]** で [イベントを生成する（Generate Events）] をクリックすると、フィルタが「`Recommendation:"Generate Events"`」に変更されます。

- キーワード（[カテゴリ（Category）]、[分類（Classifications）]、[Microsoft 脆弱性（Microsoft Vulnerabilities）]、[Microsoft ワーム（Microsoft Worms）]、[優先度（Priority）]、および [ルール アップデート（Rule Update）]）になっているフィルタ タイプ グループ見出しを選択すると、使用可能な引数が一覧表示されます。

  このタイプのグループから項目を選択すると、適用される引数とキーワードがすぐにフィルタに追加されます。キーワードがすでにフィルタ内に存在していた場合は、そのグループに対応するキーワードの既存の引数が置き換えられます。

  たとえば、フィルタ パネルの [カテゴリ（Category）] で [os-linux] をクリックすると、「`Category:"os-linux"`」がフィルタ テキストボックスに追加されます。その後で、[カテゴリ（Category）] で [os-windows] をクリックすると、フィルタが「`Category:"os-windows"`」に変更されます。

- [ルール コンテンツ（Rule Content）] の下の [参照（Reference）] はキーワードであり、その下に特定の参照 ID タイプが列挙されます。参照キーワードのいずれかを選択すると、引数を指定するためのポップアップ ウィンドウが表示され、キーワードが既存のフィルタに追加されます。キーワードがすでにフィルタ内で使用されていた場合は、既存の引数が指定した新しい引数に置き換えられます。

  たとえば、フィルタ パネルで **[ルール コンテンツ（Rule Content）]** > **[参照（Reference）]** > **[CVE ID]** の順にクリックすると、ポップアップ ウィンドウが開いて CVE ID を指定するよう求められます。「`2007`」と入力すると、「`CVE:"2007"`」がフィルタ テキストボックスに追加されます。別の例では、フィルタ パネルで **[ルール コンテンツ（Rule Content）]** >

[参照（Reference）] の順にクリックすると、ポップアップ ウィンドウが開いて、参照を指定するよう求められます。「2007」と入力すると、「Reference:"2007"」がフィルタ テキストボックスに追加されます。

- 複数のグループからルール フィルタ キーワードを選択した場合は、各フィルタ キーワードがフィルタに追加され、既存のキーワードが維持されます（同じキーワードの新しい値で上書きされなかった場合）。

  たとえば、フィルタ パネルの [カテゴリ（Category）] で [os-linux] をクリックすると、「Category:"os-linux"」がフィルタ テキストボックスに追加されます。その後で、[Microsoft 脆弱性（Microsoft Vulnerabilities）] で [MS00-006] をクリックすると、フィルタが「Category:"os-linux" MicrosoftVulnerabilities:"MS00-006"」に変更されます。

- 複数のキーワードを選択した場合は、システムがそれらを AND ロジックを使用して結合し、複合検索フィルタを生成します。たとえば、[カテゴリ（Category）] で [プリプロセッサ（preprocessor）] を選択してから、**[ルール コンテンツ（Rule Content）]** > **[GID]** の順に選択して、「116」と入力すると、プリプロセッサ ルールで、**かつ**、GID が 116 のすべてのルールを取得する「Category: "preprocessor" GID:"116"」というフィルタが返されます。

- [カテゴリ（Category）]、[Microsoft 脆弱性（Microsoft Vulnerabilities）]、[Microsoft ワーム（Microsoft Worms）]、[プラットフォーム特有（Platform Specific）]、および [優先度（Priority）] の各フィルタ グループを使用すれば、カンマで区切られたキーワードの複数の引数を送信できます。たとえば、[カテゴリ（Category）] から [os-linux] と [os-windows] を選択すると、os-linux カテゴリまたは os-windows カテゴリ内のルールを取得する「Category:"os-windows,app-detect"」というフィルタを作成できます。

複数のフィルタ キーワード/引数のペアで同じルールが取得される場合があります。たとえば、ルールを [dos] カテゴリによってフィルタ処理する場合や [High] 優先度でフィルタ処理する場合は、DOS Cisco 試行ルール（SID 1545）が表示されます。

（注） Cisco Talos Intelligence Group（Talos） がルール更新メカニズムを使用してルール フィルタを追加または削除する場合があります。

[ルール（Rules）] ページのルールは、共有オブジェクト ルール（ジェネレータ ID 3）または標準テキスト ルール（ジェネレータ ID 1、グローバル ドメインまたはレガシー GID（1000 ～ 2000）、子孫ドメイン）のいずれかになります。次の表に、さまざまなルール フィルタの説明を示します。

表 *142 :* ルール フィルタ グループ

フィルタ グループ	説明	複数の引数をサポートするか	見出し	リスト内の項目
Rule Configuration	ルールの設定に基づいてルールを検索します。	いいえ	グループ	キーワード
Rule Content	ルールの内容に基づいてルールを検索します。	いいえ	グループ	キーワード
Category	ルールエディタで使用されるルールカテゴリに基づいてルールを検索します。ローカルルールはローカルサブグループに表示されることに注意してください。	はい	キーワード	引数
Classifications	ルールによって生成されるイベントのパケット画面内に表示される攻撃分類に基づいてルールを検索します。	いいえ	キーワード	引数
Microsoft Vulnerabilities	Microsoft セキュリティ情報番号に従ってルールを検索します。	はい	キーワード	引数
Microsoft Worms	Microsoft Windows ホストに影響する特定のワームに基づいてルールを検索します。	はい	キーワード	引数

フィルタ グループ	説明	複数の引数をサポートするか	見出し	リスト内の項目
Platform Specific	オペレーティングシステムの特定のバージョンとの関連性に基づいてルールを検索します。 ルールが複数のオペレーティングシステムまたは1つのオペレーティングシステムの複数のバージョンに影響する場合があることに注意してください。たとえば、SID 2260を有効にすると、Mac OS X、IBM AIX、およびその他のオペレーティングシステムの複数のバージョンに影響します。	はい	キーワード	引数 サブリストからいずれかの項目を選択すると、引数に修飾子が追加されることに注意してください。
プリプロセッサ（Preprocessors）	個別のプリプロセッサのルールを検索します。 プリプロセッサが有効になっている場合にプリプロセッサオプションに対するイベントを生成し、インライン展開では、違反パケットをドロップします。するためには、そのオプションに関連付けられたプリプロセッサルールを有効にする必要があることに注意してください。	はい	グループ	サブグループ

フィルタ グループ	説明	複数の引数をサポートするか	見出し	リスト内の項目
プライオリティ（Priority）	高、中、および低の優先度に基づいてルールを検索します。 ルールに割り当てられた分類によってその優先度が決定されます。これらのグループは、さらにルールカテゴリに分類されます。ローカルルール（つまり、ユーザがインポートまたは作成したルール）は優先度グループに表示されないことに注意してください。	はい	キーワード	引数 サブリストからいずれかの項目を選択すると、引数に修飾子が追加されることに注意してください。
ルールの更新（Rule Update）	特定のルール更新を通して追加または変更されたルールを検索します。ルール更新ごとに、更新内のすべてのルール、更新でインポートされた唯一の新しいルール、または更新によって変更された唯一の既存のルールを表示します。	いいえ	キーワード	引数

侵入ルール構成フィルタ

[ルール（Rules）]ページに表示されたルールをいくつかのルール構成設定でフィルタ処理できます。たとえば、ルール状態が推奨ルール状態と一致しない一連のルールを表示する場合は、[推奨と一致しない（Does not match recommendation）] を選択することによってルール状態をフィルタ処理できます。

基準リスト内のノードをクリックしてキーワードを選択すると、フィルタ条件とする引数を指定できます。そのキーワードがすでにフィルタで使用されていた場合は、そのキーワードの既存の引数が指定した引数に置き換えられます。

たとえば、フィルタ パネルの **[ルール設定（Rule Configuration）]** > **[推奨（Recommendation）]** で [ドロップしてイベントを生成する（Drop and Generate Events）] をクリックすると、「`Recommendation:"Drop and Generate Events"`」がフィルタ テキスト ボックスに追加されます。その後で、**[ルール設定（Rule Configuration）]** > **[推奨（Recommendation）]** で [イベント

を生成する（Generate Events）] をクリックすると、フィルタが「`Recommendation:"Generate Events"`」に変更されます。

侵入ルール コンテンツ フィルタ

[ルール（Rules）] ページに表示されたルールをいくつかのルール コンテンツ項目でフィルタ処理できます。たとえば、ルールの SID を検索することによって、ルールをすばやく取得できます。特定の宛先ポートに送信されるトラフィックを検査するすべてのルールを検索することもできます。

基準リスト内のノードをクリックしてキーワードを選択すると、フィルタ条件とする引数を指定できます。そのキーワードがすでにフィルタで使用されていた場合は、そのキーワードの既存の引数が指定した引数に置き換えられます。

たとえば、フィルタ パネルの [Rule Content] で [SID] をクリックすると、ポップアップ ウィンドウが開いて SID の入力が促されます。「`1045`」と入力すると、「`SID:"1045"`」がフィルタ テキスト ボックスに追加されます。その後で、再度 [SID] をクリックして、SID フィルタを「`1044`」に変更すると、フィルタが「`SID:"1044"`」に変更されます。

表 *143 :* ルール コンテンツ フィルタ

フィルタ	検索するルールの内容
メッセージ	メッセージ フィールドで指定された文字列を含む。
SID	指定された SID がある。
GID	指定された GID がある。
参照	参照フィールドで指定された文字列を含む。また、特定のタイプの参照および指定された文字列でフィルタリングすることもできます。
操作	`alert` または `pass` から開始する。
プロトコル	選択されたプロトコルを含む。
方向（Direction）	ルールに、指定された方向設定が含まれているかどうかに基づく。
ソース IP	ルール内の送信元 IP アドレス宛先に指定されたアドレスまたは変数を使用する。有効な IP アドレス、CIDR ブロック/プレフィックス長、または `$HOME_NET` や `$EXTERNAL_NET` などの変数を使用してフィルタ処理できます。
宛先 IP（Destination IP）	ルール内の送信元 IP アドレス宛先に指定されたアドレスまたは変数を使用する。有効な IP アドレス、CIDR ブロック/プレフィックス長、または `$HOME_NET` や `$EXTERNAL_NET` などの変数を使用してフィルタ処理できます。

フィルタ	検索するルールの内容
ソース ポート	指定された送信元ポートを含む。ポート値は、1 ～ 65535 の整数またはポート変数にする必要があります。
接続先ポート（Destination port）	指定された宛先ポートを含む。ポート値は、1 ～ 65535 の整数またはポート変数にする必要があります。
ルールのオーバーヘッド	選択されたルールのオーバーヘッドがある。
メタデータ	一致するキーと値のペアを含むメタデータがある。たとえば、HTTP アプリケーション プロトコルに関連するメタデータを使用したルールを検索するには、「`metadata:"service http"`」と入力します。

侵入ルール カテゴリ

Firepower システムは、ルールが検出するトラフィックのタイプに基づいてカテゴリにルールを配置します。[ルール（Rules）] ページで、ルール カテゴリでフィルタ処理することによって、カテゴリ内のすべてのルールにルール属性を設定できます。たとえば、ネットワーク上に Linux ホストが存在しない場合は、**os-linux** カテゴリでフィルタ処理してから、表示されたすべてのルールを無効にすることによって、**os-linux** カテゴリ全体を無効にすることができます。

カテゴリ名の上にポインタを移動すると、そのカテゴリ内のルールの数を表示できます。

（注） Cisco Talos Intelligence Group（Talos） がルール更新メカニズムを使用してルール カテゴリを追加または削除する場合があります。

侵入ルールのフィルタ コンポーネント

フィルタ パネルでフィルタをクリックしたときに入力される特殊なキーワードとその引数を変更するようにフィルタを編集できます。[Rules] ページのカスタム フィルタはルール エディタで使用されるものと同様に機能しますが、フィルタ パネルを通してフィルタを選択したときに表示される構文を使用して、[Rules] ページのフィルタに入力されたキーワードのいずれかを使用することもできます。今後使用するキーワードを決定するには、右側のフィルタ パネルで該当する引数をクリックします。フィルタ キーワードと引数構文がフィルタ テキスト ボックスに表示されます。キーワードのカンマ区切りの複数の引数は Category と Priority のフィルタ タイプでしかサポートされないことに注意してください。

引用符内のキーワードと引数、文字列、およびリテラル文字列と一緒に、複数のフィルタ条件を区切るスペースを使用できます。ただし、正規表現、ワイルドカード文字、または否定文字（!）、大なり記号（>）、小なり記号（<）などの特殊な演算子を含めることはできません。キーワードなし、キーワードの先頭文字の大文字表記なし、または引数の周りの引用符なしの検索語を入力すると、検索が文字列検索として扱われ、[Category]、[Message]、および [SID] の各フィールドで指定された単語が検索されます。

gid キーワードと sid キーワードを除き、すべての引数と文字列は部分的な文字列として扱われます。gid と sid の引数は完全一致のみを返します。

各ルール フィルタに、次の形式で 1 つ以上のキーワードを含めることができます。

keyword:*"argument"*

ここで、Keyword は侵入ルール フィルタ グループ内のキーワードのいずれかで、argument は二重引用符で囲まれ、キーワードに関連した特定のフィールド内で検索される単一の大文字と小文字が区別されない英数字文字列です。キーワードは先頭文字を大文字にして入力する必要があることに注意してください。

gid と sid を除くすべてのキーワードの引数が部分文字列として扱われます。たとえば、引数の 123 は、"12345"、"41235"、"45123" などを返します。gid と sid の引数は完全一致のみを返します。たとえば、sid:3080 は SID 3080 のみを返します。

各ルール フィルタに、1 つ以上の英数字文字列を含めることもできます。文字列はルールの [メッセージ（Message）] フィールド、[Snort ID]（SID）、およびジェネレータ ID（GID）を検索します。たとえば、文字列 123 は、ルール メッセージ内の文字列 "Lotus123" や "123mania" などを返し、SID 6123 や SID 12375 なども返します。1 つ以上の文字列でフィルタ処理することによって、SID を部分的に検索できます。

すべての文字列で大文字と小文字が区別されず、部分文字列として扱われます。たとえば、文字列 ADMIN、admin、または Admin はすべて、「admin」、「CFADMIN」、「Administrator」などを返します。

文字列を引用符で囲むと、完全一致を返すことができます。たとえば、引用符付きのリテラル文字列 "overflow attempt" は完全一致のみを返しますが、引用符なしの 2 つの文字列 overflow と attempt で構成されるフィルタは "overflow attempt"、"overflow multipacket attempt"、"overflow with evasion attempt" などを返します。

複数のキーワード、文字列、またはその両方をスペースで区切って任意に組み合わせて入力することで、フィルタ結果を絞り込むことができます。結果には、すべてのフィルタ条件に一致するルールが含まれます。

複数のフィルタ条件を任意の順序で入力できます。たとえば、次のフィルタはそれぞれ同じルールを返します。

- url:at login attempt cve:200
- login attempt cve:200 url:at
- login cve:200 attempt url:at

侵入ルール フィルタの使用

侵入ポリシー内の [Rules] ページの左側にあるフィルタ パネルから事前定義のフィルタ キーワードを選択できます。フィルタを選択すると、ページに、すべての一致するルールが表示されるか、どのルールも一致しなかったことが表示されます。

フィルタにキーワードを追加してさらに絞り込むことができます。入力されたすべてのフィルタが、ルールデータベース全体を検索して、一致するすべてのルールを返します。ページに前回のフィルタ結果が表示されている状態でフィルタを入力すると、ページが消去され、代わりに新しいフィルタの結果が返されます。

また、フィルタを選択したとき、または、フィルタを選択後にその中の引数値を変更したときに指定したものと同じキーワードと引数の構文を使用してフィルタを入力することもできます。キーワードなし、キーワードの先頭文字の大文字表記なし、または引数の周りの引用符なしの検索語を入力すると、検索が文字列検索として扱われ、[Category]、[Message]、および [SID] の各フィールドで指定された単語が検索されます。

侵入ポリシー内のルール フィルタの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Intrusion Admin

[ルール（Rules）]ページで、ルールのサブセットを表示するようにルールをフィルタ処理できます。その後で、いずれかのページ機能を使用できます。これには、コンテキストメニューで使用可能な機能の選択も含まれます。これは、特定のカテゴリのすべてのルールのしきい値を設定する場合などに便利です。フィルタ処理されたリスト内のルールとフィルタ処理されていないリスト内のルールで同じ機能を使用できます。たとえば、新しいルール状態を、フィルタ処理されたリスト内のルールまたはフィルタ処理されていないリスト内のルールに適用できます。

すべてのフィルタのキーワード、キーワード引数、および文字列では大文字と小文字が区別されません。フィルタ内に存在するキーワードの引数をクリックすると、既存の引数が置き換えられます。

ステップ 1 **[Policies]** > **[Access Control]** > **[Intrusion]**を選択します。

ステップ 2 編集するポリシーの横にある編集アイコン（  ）をクリックします。

代わりに表示アイコン（  ）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 **[ルール（Rules）]** をクリックします。

ステップ 4 次に示す方法を個別に使用したり、組み合わせて使用することでフィルタを作成します。

- [フィルタ（Filter）] テキスト ボックスに値を入力して、Enter キーを押します。
- 事前定義されたキーワードのいずれかを展開します。たとえば、[ルール設定（Rule Configuration）] をクリックします。
- キーワードをクリックして、プロンプトが表示されたら引数の値を指定します。次に例を示します。

- [ルール設定（Rule Configuration）] の下で、[ルール状態（Rule State）] をクリックし、ドロップダウンリストから [イベントの生成（`Generate Events`）] を選択して、[OK] をクリックします。
- [ルール設定（Rule Configuration）] の下で、[コメント（Comment）] をクリックし、フィルタ条件として使用するコメント テキストの文字列を入力して、[OK] をクリックします。
- [カテゴリ（Category）] の下で、[アプリ検出（app-detect）] をクリックします。システムは、これを引数の値として使用します。

- キーワードを展開して、引数の値をクリックします。たとえば、[ルール状態（Rule State）] を展開して、[イベントの生成（Generate Events）] をクリックします。

侵入ルールの状態

侵入ルールの状態により、個々の侵入ポリシー内のルールを有効または無効にできるだけでなく、モニタ対象の条件によってルールがトリガーされたときにシステムが実行するアクションを指定できます。

各デフォルト ポリシーの侵入ルールとプリプロセッサ ルールのデフォルト状態は、Cisco Talos Intelligence Group（Talos）が設定します。たとえば、ルールを Security over Connectivity デフォルト ポリシーでは有効にして、Connectivity over Security デフォルト ポリシーでは無効にすることができます。Talos がルール更新を使用してデフォルト ポリシー内の 1 つ以上のルールのデフォルト状態を変更する場合があります。ルール更新での基本ポリシーの更新を許可すると、ポリシーの作成時に使用されたデフォルト ポリシー（または基礎となるデフォルト ポリシー）のデフォルト状態が変更されたときの、そのポリシー内のルールのデフォルト状態の変更も許可することになります。ただし、ルール状態を変更している場合は、ルール更新でその変更が上書きされないことに注意してください。

侵入ルールを作成すると、そのルールは、ポリシーの作成時に使用されたデフォルトポリシー内のルールのデフォルト状態を継承します。

侵入ルールの状態オプション

侵入ポリシーでは、ルールの状態を次の値に設定できます。

イベントを生成する（Generate Events）

システムで特定の侵入試行を検出して、一致したトラフィックが見つかった時点で侵入イベントを生成する場合。悪意のあるパケットがネットワークを通過してルールをトリガーすると、そのパケットが宛先に送信され、システムが侵入イベントを生成します。悪意のあるパケットはその対象に到達しますが、イベント ロギングによって通知されます。

ドロップおよびイベントの生成（Drop and Generate Events）

システムで特定の侵入試行を検出して、その攻撃を含むパケットをドロップし、一致したトラフィックが見つかった時点で侵入イベントを生成する場合。悪意のあるパケットはその対象に到達せず、イベント ロギングによって通知されます。

このルール状態に設定されたルールはイベントを生成しますが、7000 または 8000 シリーズ デバイスのインライン インターフェイス セットがタップ モードの場合の展開を含むパッシブ展開ではパケットをドロップしないことに注意してください。システムがパケットをドロップするには、侵入ポリシーで[インライン時にドロップ（Drop when Inline）] を有効にして、デバイス インラインを展開する必要もあります。

Disable

システムで一致するトラフィックを評価しない場合。

（注） [イベントを生成する（Generate Events）] または [ドロップおよびイベントの生成（Drop and Generate Events）] オプションのいずれかを選択すると、ルールが有効になります。[無効（Disable）] を選択すると、ルールが無効になります。

シスコでは、侵入ポリシー内のすべての侵入ルールを有効に**しない**ことを**強く**推奨しています。すべてのルールが有効になっている場合は、管理対象デバイスのパフォーマンスが低下する可能性があります。代わりに、できるだけネットワーク環境に合わせてルールセットを調整してください。

侵入ルール状態の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Intrusion Admin

侵入ルール状態は、ポリシー固有です。

ステップ 1 **[Policies]** > **[Access Control]** > **[Intrusion]**を選択します。

ステップ 2 編集するポリシーの横にある編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ヒント このページには、有効なルールの総数、[イベントを生成する（Generate Events）] に設定された有効なルールの総数、および [ドロップしてイベントを生成する（Drop and Generate Events）] に設定された有効なルールの総数が表示されます。また、パッシブ展開では、[Drop and Generate Events] に設定されたルールで行われるのはイベントの生成のみであることにも注意してください。

ステップ 3 ナビゲーション ウィンドウで、[ポリシー情報（Policy Information）] のすぐ下にある [ルール（Rules）] をクリックします。

ステップ 4 ルール状態を設定する 1 つ以上のルールを選択します。

ステップ 5 次のいずれかを実行します。

- **[Rule State] > [Generate Events]**
- **[Rule State] > [Drop and Generate Events]**
- **[Rule State] > [Disable]**

ステップ 6 最後のポリシー確定後にこのポリシーで行った変更を保存するには、ナビゲーション パネルで [ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後の変更は破棄されます。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

侵入ポリシーの侵入イベント通知のフィルタ

侵入イベントの重要度は、発生頻度、送信元 IP アドレス、または宛先 IP アドレスに基づいて設定できます。イベントが特定の回数発生するまで注意が必要ない場合もあります。たとえば、何者かがサーバにログインしようとしても、特定の回数失敗するまで、気にする必要はありません。一方、ほんの少数の発生を見れば、広範な問題があることを理解できる場合もあります。たとえば、Web サーバに対して DoS 攻撃が行われた場合は、少数の侵入イベントの発生を確認しただけで、その状況に対処しなければならないことが分かります。同じイベントが何百回も確認されれば、システムの機能が麻痺します。

侵入イベントのしきい値

指定された期間内にイベントが生成された回数に基づいて、システムが侵入イベントを記録して表示する回数を制限するための個別のルールのしきい値を侵入ポリシー単位で設定できます。これにより、大量の同じイベントが原因で機能が麻痺するのを避けることができます。共有オブジェクトのルール、標準テキスト ルール、またはプリプロセッサ ルールごとにしきい値を設定できます。

侵入イベントしきい値の設定

しきい値を設定するには、最初にしきい値のタイプを指定します。

表 *144 :* しきい値設定オプション

オプション	説明
Limit	指定された数のパケット（カウント引数によって指定される）が、指定された期間内にルールをトリガーとして使用した場合に、イベントを記録して表示します。たとえば、タイプを [Limit] に、[Count] を 10 に、[Seconds] を 60 に設定し、14 個のパケットがルールをトリガーとして使用した場合、システムはその 1 分の間に発生した最初の 10 個を表示した後、イベントの記録を停止します。
Threshold	指定された数のパケット（カウント引数によって指定される）が、指定された期間内にルールをトリガーとして使用した場合に、1 つのイベントを記録して表示します。イベントのしきい値カウントに達し、システムがそのイベントを記録した後、時間のカウンタは再び開始されることに注意してください。たとえば、タイプを [Threshold] に、[Count] を 10 に、[Seconds] を 60 に設定して、ルールが 33 秒間で 10 回トリガーされたとします。システムは、1 個のイベントを生成してから、[Seconds] と [Count] のカウンタをリセットします。次の 25 秒間にルールがさらに 10 回トリガーされたとします。33 秒でカウンタが 0 にリセットされたため、システムが別のイベントを記録します。
Both	指定された数（カウント）のパケットがルールをトリガーとして使用した後で、指定された期間ごとに 1 回イベントを記録して表示します。たとえば、タイプを [Both] に、[Count] を 2 に、[Seconds] を 10 に設定した場合、イベント数は以下のようになります。 • ルールが 10 秒間に 1 回トリガーされた場合、システムはイベントを生成しません（しきい値が満たされていない）。 • ルールが 10 秒間に 2 回トリガーされた場合、システムは 1 つのイベントを生成します（ルールが 2 回トリガーとして使用した場合、しきい値が満たされるため）。 • ルールが 10 秒間に 4 回トリガーされた場合、システムは 1 つのイベントを生成します（ルールが 2 回目にトリガーとして使用されたときにしきい値に達し、それ以降のイベントは無視される）。

次に、トラッキングを指定します。これにより、イベントしきい値が送信元 IP アドレス単位と宛先 IP アドレス単位のどちらで計算されるかが決まります。

表 *145 : IP* しきい値設定オプション

オプション	説明
Source	送信元 IP アドレス単位でイベント インスタンス カウントを計算します。
Destination	宛先 IP アドレス単位でイベント インスタンス カウントを計算します。

最後に、しきい値を定義するインスタンスの数と期間を指定します。

表 *146 :* インスタンス/時間のしきい値設定オプション

オプション	説明
Count	しきい値を満たすために必要な、追跡する IP アドレス単位で指定された期間単位のイベント インスタンスの数。
Seconds	カウントがリセットされるまでの秒数。しきい値タイプを [limit] に、トラッキングを [Source IP] に、[count] を [10] に、[seconds] を [10] に設定した場合は、システムが指定された送信元ポートから 10 秒間に発生した最初の 10 のイベントを記録して表示します。最初の 10 秒間に 7 つのイベントしか発生しなかった場合は、システムがそれらのイベントを記録して表示します。最初の 10 秒間に 40 のイベントが発生した場合は、システムが 10 のイベントを記録して表示してから 10 秒後にカウントを再開します。

侵入イベントのしきい値設定は、単独で使用することも、レート ベースの攻撃防御、`detection_filter` キーワード、および侵入イベント抑制のいずれかと組み合わせて使用することもできます。

ヒント 侵入イベントのパケット ビューでしきい値を追加することもできます。

関連トピック

detection_filter キーワード （2252 ページ）
パケット ビュー内でのしきい値オプションの設定 （3092 ページ）

侵入イベントのしきい値の変更と追加

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Intrusion Admin

侵入ポリシーの1つ以上の特定のルールにしきい値を設定できます。既存のしきい値設定を個別にまたは同時に変更することもできます。それぞれに1つずつのしきい値を設定できます。しきい値を追加すると、ルールの既存のしきい値が上書きされます。

また、侵入ポリシーに関係したすべてのルールとプリプロセッサ生成イベントにデフォルトで適用されるグローバルしきい値を変更することもできます。

無効な値を入力するとフィールドに復元アイコン（）が表示されます。そのアイコンをクリックすると、そのフィールドの最後の有効値に戻るか、以前の値が存在しない場合はフィールドが空になります。

ヒント 複数の CPU を搭載した管理対象デバイスでグローバルしきい値または個別のしきい値を設定すると、予想より多くのイベントが生成される場合があります。

ステップ 1 **[Policies]** > **[Access Control]** > **[Intrusion]**を選択します。

ステップ 2 編集するポリシーの横にある編集アイコン（  ）をクリックします。

代わりに表示アイコン（  ）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 ナビゲーション ウィンドウで、[ポリシー情報（Policy Information）] のすぐ下にある [ルール（Rules）] をクリックします。

ステップ 4 しきい値を設定するルールを選択します。

ステップ 5 [イベントのフィルタリング（Event Filtering）] > [しきい値（Threshold）] を選択します。 >

ステップ 6 [タイプ（Type）] ドロップダウン リストからしきい値のタイプを選択します。

ステップ 7 [追跡対象（Track By）] ドロップダウンリストから、イベント インスタンスが [送信元（Source）] IP アドレスまたは [宛先（Destination）] IP アドレスのどちらによって追跡されるかを選択します。

ステップ 8 [カウント（Count）] フィールドに値を入力します。

ステップ 9 [秒（Seconds）] フィールドに値を入力します。

ステップ 10 [OK] をクリックします。

ヒント [イベント フィルタリング（Event Filtering）] カラムのルールの横にイベント フィルタ アイコン（  ）が表示されます。ルールに複数のイベント フィルタを追加した場合は、アイコン上の数字がイベント フィルタの数を示します。

ステップ 11 最後にポリシーを確定してからこのポリシーで加えた変更を保存するには、[ポリシー情報（Policy Information）] をクリックし、[変更の確定（Commit Changes）] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後の変更は破棄されます。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

関連トピック

グローバル ルールのしきい値の基本 （2129 ページ）

侵入イベントしきい値の表示と削除

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Intrusion Admin

ルールに関する既存のしきい値設定を表示または削除することができます。[Rules Details] ビューを使用してしきい値の既存の設定を表示することによって、それらがシステムに適切かどうかを確認できます。そうでない場合は、新しいしきい値を追加して既存の値を上書きすることができます。

侵入ポリシーによって記録されるすべてのルールとプリプロセッサ生成イベントにデフォルトで適用されるグローバルしきい値を変更することもできます。

ステップ 1 **[Policies]** > **[Access Control]** > **[Intrusion]**を選択します。

ステップ 2 編集するポリシーの横にある編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 ナビゲーション ウィンドウで、[ポリシー情報（Policy Information）] のすぐ下にある [ルール（Rules）] をクリックします。

ステップ 4 表示または削除する、しきい値が設定された 1 つまたは複数のルールを選択します。

ステップ 5 選択した各ルールのしきい値を削除するには、**[イベント フィルタリング（Event Filtering）]** > **[しきい値の削除（Remove Thresholds）]** の順に選択します。

ステップ 6 [OK] をクリックします。

ステップ 7 最後にポリシーを確定してからこのポリシーで加えた変更を保存するには、[ポリシー情報（Policy Information）] をクリックし、[変更の確定（Commit Changes）] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後の変更は破棄されます。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

関連トピック

グローバル ルールのしきい値の基本 （2129 ページ）

侵入ポリシーの抑制の設定

特定の IP アドレスまたは IP アドレスの範囲が特定のルールまたはプリプロセッサをトリガーしたときの侵入イベント通知を抑制できます。これは、誤検出を回避するのに役立ちます。たとえば、ユーザのメール サーバが特定のエクスプロイトのように見えるパケットを送信している場合、そのメール サーバによってイベントがトリガーされたされたときに、そのイベントに関する通知を抑制できます。ルールはすべてのパケットに対してトリガーとして使用されますが、本物の攻撃に対するイベントだけが表示されます。

侵入ポリシー抑制タイプ

侵入イベント抑制は、単独で使用することも、レート ベースの攻撃防御、`detection_filter` キーワード、および侵入イベントしきい値構成のいずれかと組み合わせて使用することもできることに注意してください。

ヒント 侵入イベントのパケット ビュー内から抑制を追加できます。また、侵入ルール エディタ ページ（**[Objects]** > **[Intrusion Rules]**）や任意の侵入イベント ページ（イベントが侵入ルールによってトリガーされた場合）で右クリック コンテキスト メニューを使用して、抑制設定にアクセスすることもできます。

関連トピック

detection_filter キーワード （2252 ページ）
パケット ビュー内でのしきい値オプションの設定 （3092 ページ）

特定のルールの侵入イベントの抑制

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Intrusion Admin

侵入ポリシーのルールに関連する侵入イベント通知を抑制できます。ルールに関する通知が抑制されると、ルールはトリガーとして使用されますが、イベントは生成されません。ルールの 1 つまたは複数の抑制を設定できます。リスト内の最初の抑制に最も高いプライオリティが割り当てられます。2つの抑制が競合している場合は、最初の抑制のアクションが実行されます。

無効な値を入力するとフィールドに復元アイコン（）が表示される点に注意してください。そのアイコンをクリックすると、そのフィールドの最後の有効値に戻るか、以前の値が存在しない場合はフィールドが空になります。

ステップ 1 **[Policies]** > **[Access Control]** > **[Intrusion]**を選択します。

ステップ 2 編集するポリシーの横にある編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 [ナビゲーション（navigation）] パネルの [ポリシー情報（Policy Information）] のすぐ下にある [ルール（Rules）] をクリックします。

ステップ 4 抑制条件を設定する 1 つまたは複数のルールを選択します。

ステップ 5 **[イベント フィルタリング（Event Filtering）]** > **[抑制（Suppression）]** を選択します。

ステップ 6 [抑制タイプ（Suppression Type）] を選択します。

ステップ 7 抑制タイプとして [送信元（Source）] または [宛先（Destination）] を選択した場合は、[ネットワーク（Network）] フィールドに、IP アドレス、アドレス ブロック、または送信元 IP アドレスまたは宛先 IP アドレスとして指定する変数、あるいは、これらの任意の組み合わせで構成されたカンマ区切りのリストを入力します。

システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。

ステップ 8 [OK] をクリックします。

ヒント 抑制するルールの横にある [イベント フィルタリング（Event Filtering）] カラムのルールの横にイベント フィルタ アイコン（）が表示されます。ルールに複数のイベント フィルタを追加した場合は、アイコン上の数字がイベント フィルタの数を示します。

ステップ 9 最後にポリシーを確定してからこのポリシーで加えた変更を保存するには、[ポリシー情報（Policy Information）] をクリックし、[変更の確定（Commit Changes）] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後の変更は破棄されます。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

抑制条件の表示と削除

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Intrusion Admin

既存の抑制条件を表示または削除することもできます。たとえば、メールサーバが悪用のように見えるパケットを普段から送信しているという理由で、そのメール サーバの IP アドレスから送信されたパケットに関するイベント通知を抑制できます。その後、そのメールサーバが使用停止になり、その IP アドレスが別のホストに再割り当てされたら、その送信元 IP アドレスの抑制条件を削除する必要があります。

ステップ 1 **[Policies]** > **[Access Control]** > **[Intrusion]**を選択します。

ステップ 2 編集するポリシーの横にある編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 [ナビゲーション（navigation）] パネルの [ポリシー情報（Policy Information）] のすぐ下にある [ルール（Rules）] をクリックします。

ステップ 4 抑制を表示または削除する 1 つまたは複数のルールを選択します。

ステップ 5 次の選択肢があります。

- ルールのすべての抑制を削除するには、**[イベント フィルタリング（Event Filtering）]** > **[抑制の削除（Remove Suppressions）]** を選択します。
- 特定の抑制設定を削除するには、ルールをクリックして、[詳細の表示（Show Details）] をクリックします。抑制設定を展開して、削除する抑制設定の横にある [削除（Delete）] をクリックします。

ステップ 6 [OK] をクリックします。

ステップ 7 最後にポリシーを確定してからこのポリシーで加えた変更を保存するには、[ポリシー情報（Policy Information）] をクリックし、[変更の確定（Commit Changes）] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後の変更は破棄されます。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

動的侵入ルール状態

レート ベースの攻撃は、ネットワークまたはホストに過剰なトラフィックを送信することによって、低速化または正規の要求の拒否を引き起こし、ネットワークまたはホストを混乱させようとします。レートベースの防御を使用して、特定のルールの過剰なルール一致に対応してルール アクションを変更することができます。

侵入ポリシーにレートベースのフィルタを含めることにより、一定期間においてルールの一致が過剰に発生した時点を検出できます。インライン展開された管理対象デバイス上でこの機能

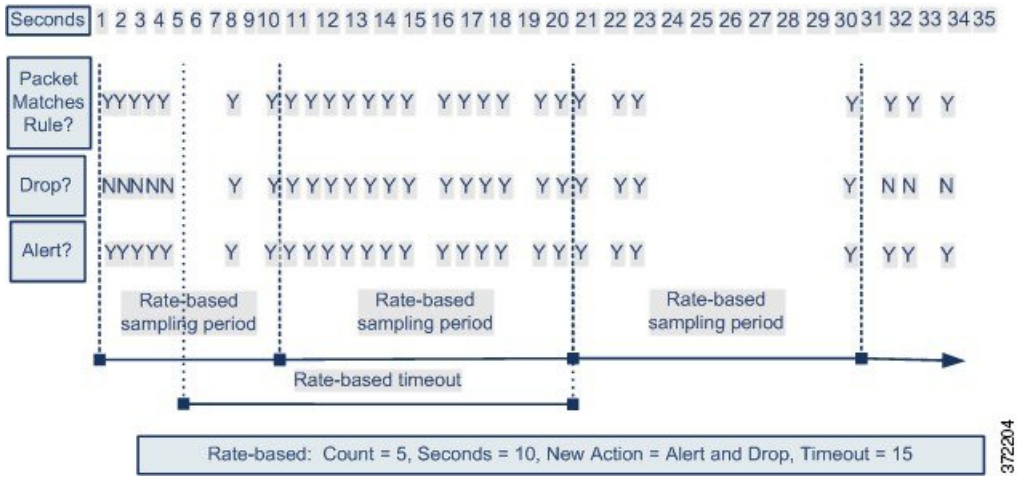
を使用して、指定された時刻のレートベースの攻撃をブロックしてから、ルール一致がイベントを生成するだけでトラフィックをドロップしないルール状態に戻すことができます。

レート ベースの攻撃防御は、異常なトラフィック パターンを識別し、正規の要求に対するそのトラフィックの影響を最小限に抑えようとします。特定の宛先 IP アドレスに送信されるトラフィックまたは特定の送信元 IP アドレスから送信されるトラフィックの過剰なルール一致を識別できます。また、検出されたすべてのトラフィックを通して特定のルールの過剰な一致に対処することもできます。

ルールと一致したすべてのパケットをドロップするのではなく、指定された期間に特定の一致率に達した場合にルールと一致したパケットをドロップするために、ルールを [Drop and Generate Events] 状態に設定しない場合があります。動的ルール状態を使用すれば、ルールのアクションの変更をトリガーするレート、あるレートに達したときに変更すべきアクション、および新しいアクションの継続時間を設定できます。

次の図は、攻撃者がホストにアクセスしようとしている例を示しています。繰り返しパスワードを特定しようとする試みが、レート ベースの攻撃防御が設定されたルールをトリガーします。レートベースの設定は、ルール一致が 10 秒間に 5 回発生した時点で、ルール属性を [Drop and Generate Events] に変更します。新しいルール属性は 15 秒後にタイムアウトします。

タイムアウト後も、そのパケットは後続のレートベースのサンプリング期間にドロップされることに注意してください。サンプリング レートが現在または過去のサンプリング期間のしきい値を上回っている場合は、新しいアクションが継続されます。新しいアクションは、サンプリング レートがしきい値レートを下回るサンプリング期間の終了後にのみ、[Generate Events] に戻ります。



ダイナミックな侵入ルール状態の設定

侵入ポリシーでは、侵入ルールまたはプリプロセッサ ルールのレート ベースのフィルタを設定できます。レート ベースのフィルタは次の 3 つの要素で構成されます。

- 特定の秒数以内のルール一致のカウントとして設定されるルール一致率

- レートを超えた時点で実行される新しいアクション（Generate Events、Drop and Generate Events、および Disable の 3 種類がある）
- タイムアウト値として設定されるアクションの継続期間

新しいアクションは、開始されると、レートがその期間内に設定されたレートを下回っても、タイムアウトに達するまで継続されることに注意してください。タイムアウトに達したときに、レートがしきい値を下回っている場合は、ルールのアクションが初期設定に戻ります。

インライン展開のレートベースの攻撃防御は、攻撃を一時的または永続的にブロックするように設定できます。レート ベースの設定を使用しない場合、[Generate Events] に設定されたルールはイベントを生成しますが、システムはそのようなルールに関するパケットをドロップしません。ただし、攻撃トラフィックが、レートベースの基準が設定されたルールと一致した場合は、そのようなルールが最初から [Drop and Generate Events] に設定されていなかったとしても、レート アクションがアクティブな期間にパケットのドロップが実行されます。

（注） レート ベースのアクションは、無効なルールを有効にしたり、無効なルールと一致したトラフィックをドロップしたりできません。

同じルールに対して複数のレートベースのフィルタを定義できます。侵入ポリシーに列挙された最初のフィルタに最も高い優先度が割り当てられます。2つのレートベースのフィルタアクションが競合している場合は、最初のレートベースのフィルタのアクションが実行されることに注意してください。

[ルール（Rule）] ページからの動的ルール状態の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Intrusion Admin

1 つのルールに対して 1 つ以上の動的ルール状態を設定できます。最初に表示される動的ルール状態に最も高いプライオリティが割り当てられます。2 つの動的ルール状態が競合している場合は、最初のアクションが実行されます。

動的ルール状態はポリシー固有です。

無効な値を入力するとフィールドに復元アイコン（）が表示されます。そのアイコンをクリックすると、そのフィールドの最後の有効値に戻るか、以前の値が存在しない場合はフィールドが空になります。

（注） 動的ルール状態は、無効なルールを有効にしたり、無効なルールと一致したトラフィックをドロップしたりできません。

ステップ 1 **[Policies]** > **[Access Control]** > **[Intrusion]**を選択します。

ステップ 2 編集するポリシーの横にある編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 ナビゲーション ウィンドウで、[ポリシー情報（Policy Information）] のすぐ下にある [ルール（Rules）] をクリックします。

ステップ 4 動的ルール状態を追加する 1 つまたは複数のルールを選択します。

ステップ 5 **[動的状態（Dynamic State）]** > **[レート ベースのルール状態の追加（Add Rate-Based Rule State）]** を選択します。

ステップ 6 [追跡対象（Track By）] ドロップダウンリストから値を選択します。

ステップ 7 [Track By] を [Source] または [Destination] に設定した場合は、[Network] フィールドに追跡する各ホストのアドレスを入力します。単一のIPアドレス、アドレスブロック、変数、またはこれらの任意の組み合わせで構成されたカンマ区切りのリストを指定できます。

システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。

ステップ 8 [レート（Rate）] の横で、攻撃レートを設定する期間あたりのルール一致の数を指定します。

- [カウント（Count）] フィールドに値を入力します。
- [秒（Seconds）] フィールドに値を入力します。

ステップ 9 [新しい状態（New State）] ドロップダウンリストから、条件が満たされたときに実行する新しいアクションを指定します。

ステップ 10 [タイムアウト（Timeout）] フィールドに値を入力します。

タイムアウトが発生すると、ルールが元の状態に戻ります。新しいアクションのタイムアウトを阻止する場合は、[0] を指定するか、[Timeout] フィールドを空白のままにします。

ステップ 11 [OK] をクリックします。

ヒント [動的状態（Dynamic State）] 列のルールの横に動的状態アイコン（）が表示されます。ルールに複数の動的ルール状態フィルタを追加した場合は、アイコン上の数字がフィルタの数を示します。

ヒント ルールのセットに対する動的ルール設定を削除するには、[ルール（Rules）] ページでルールを選択して、**[動的状態（Dynamic State）]** > **[レート ベースの状態の削除（Remove Rate-Based States）]** を選択します。また、ルールのルール詳細から個別のレート ベースのルール状態フィルタを削除するには、ルールを選択して、[詳細の表示（Show Details）] をクリックしてから、削除するレート ベースのフィルタのそばにある [削除（Delete）] をクリックします。

ステップ 12 最後にポリシーを確定してからこのポリシーで加えた変更を保存するには、[ポリシー情報（Policy Information）] をクリックし、[変更の確定（Commit Changes）] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後の変更は破棄されます。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

侵入ルールのコメントの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Intrusion Admin

侵入ポリシーのルールにコメントを追加できます。このようにして追加されたコメントはポリシー専用のコメントとなります。よって、ある侵入ポリシーのルールに追加したコメントは、他の侵入ポリシーでは表示されません。追加したコメントは、侵入ポリシーの[ルール（Rules）] ページ上の [ルールの詳細（Rule Details）] ビューで確認できます。

コメントを含む侵入ポリシーの変更をコミットしてから、ルールの [編集（Edit）] ページで [ルール コメント（Rule Comment）] をクリックしてコメントを表示することもできます。

ステップ 1 **[Policies]** > **[Access Control]** > **[Intrusion]**を選択します。

ステップ 2 編集するポリシーの横にある編集アイコン（  ）をクリックします。

代わりに表示アイコン（  ）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 [ナビゲーション（navigation）] パネルの [ポリシー情報（Policy Information）] のすぐ下にある [ルール（Rules）] をクリックします。

ステップ 4 コメントを追加する 1 つまたは複数のルールを選択します。

ステップ 5 [コメント（Comments）] > [ルール コメントの追加（Add Rule Comment）] の順に選択します。 >

ステップ 6 [コメント（Comments）] フィールドに、ルール コメントを入力します。

ステップ 7 [OK] をクリックします。

ヒント システムは [コメント（Comments）] カラムのルールの横にコメント アイコン（  ）を表示します。ルールに複数のコメントを追加した場合は、アイコン上の数字がコメントの数を示します。

ステップ 8 必要に応じて、コメントの横にある [削除（Delete）] をクリックし、ルールのコメントを削除します。

侵入ポリシーの変更がコミットされずにコメントがキャッシュされている場合にだけコメントを削除できます。侵入ポリシーの変更がコミットされた後は、ルール コメントを削除できなくなります。

ステップ 9 最後にポリシーを確定してからこのポリシーで加えた変更を保存するには、[ポリシー情報（Policy Information）] をクリックし、[変更の確定（Commit Changes）] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後の変更は破棄されます。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

第 85 章

ネットワーク資産に応じた侵入防御の調整

以下のトピックでは、Firepower 推奨ルールの使用方法について説明します。

Firepower 推奨ルールについて

Firepower の侵入ルールの推奨事項を使用して、ネットワーク上で検出されたオペレーティング システム、サーバ、およびクライアント アプリケーション プロトコルを、それらのアセットを保護するために作成されたルールに関連付けることができます。これにより、モニタ対象のネットワークの特定ニーズに合わせて侵入ポリシーを調整できます。

システムは、侵入ポリシーごとに個別の推奨事項のセットを作成します。これにより、通常、標準テキスト ルールと共有オブジェクト ルールのルール状態の変更が推奨されます。ただし、プリプロセッサおよびデコーダのルールの変更も推奨されます。

ルール状態の推奨事項を生成する場合は、デフォルト設定を使用するか、詳細設定を指定できます。詳細設定では次の操作が可能です。

- システムが脆弱性をモニタするネットワーク上のホストを再定義する。
- ルール オーバーヘッドに基づき、システムが推奨するルールに影響を与える。
- ルールを無効にする推奨事項を生成するかどうかを指定する。

推奨事項をすぐに使用するか、推奨事項（および影響を受けるルール）を確認してから受け入れることができます。

推奨ルール状態を使用することを選択すると、読み取り専用の Firepower 推奨レイヤが侵入ポリシーに追加されますが、後で、推奨ルール状態を使用しないことを選択すると、そのレイヤが削除されます。

侵入ポリシーに最近保存された構成設定に基づいて自動的に推奨を生成するためのタスクをスケジュールできます。

システムは、手動で設定されたルール状態を変更しません。

- 推奨を生成する前に指定したルールの状態を手動で設定すると、その後、システムはそのルールの状態を変更できなくなる。
- 推奨の生成後に指定したルールの状態を手動で設定すると、そのルールの推奨状態が上書きされる。

ヒント 侵入ポリシー レポートには、推奨状態と異なるルール状態を持つルールのリストを含めることができます。

推奨が絞り込まれた [ルール（Rules）] ページを表示している最中に、あるいは、ナビゲーション パネルまたは [ポリシー情報（Policy Information）] ページから [ルール（Rules）] ページに直接アクセスした後に、手動で、ルール状態を設定したり、ルールをソートしたり、[ルール（Rules）] ページで可能なその他の操作（ルールの抑制やルールしきい値の設定など）を実行することができます。

（注） Cisco Talos Intelligence Group（Talos）は、システム提供のポリシーでの各ルールの適切な状態を決定します。システム提供のポリシーを基本ポリシーとして使用し、システムがルールを Firepower の推奨ルール状態に設定できるようにする場合、侵入ポリシーのルールは、シスコが推奨するネットワーク アセットの設定と一致します。

推奨ルールおよびマルチテナンシー

システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、先祖ドメインの侵入ポリシーでこの機能を有効にすると、システムはすべての子孫のリーフ ドメインからのデータを使用して、推奨事項を生成します。これにより、侵入ルールをすべてのリーフ ドメインに存在しない可能性があるアセットに調整することができ、パフォーマンスに影響を与えることができます。

Firepower 推奨のデフォルト設定

Firepower 推奨を生成すると、システムがネットワーク資産に関連付けられた脆弱性から保護するルールの基本ポリシーを検索して、その基本ポリシー内のルールの現在の状態を特定します。システムによってルールの状態が推奨されますが、自身で設定する場合はルールを推奨される状態に設定します。

システムによって次の基本的な分析が実行され、推奨が生成されます。

表 *147*：脆弱性に基づく ルール状態推奨

検出された資産がルールにより保護されるか	基本ポリシー ルール状態	推奨ルール状態
Yes	ディセーブル	イベントを生成する（Generate Events）
	イベントを生成する（Generate Events）	イベントを生成する（Generate Events）
	ドロップおよびイベントの生成	ドロップおよびイベントの生成（Drop and Generate Events）
なし	任意（Any）	無効

表の次の点に注意してください。

- ベース ポリシーでルールが無効になっているか、または[イベントの生成（Generate Events）]に設定されている場合、推奨される状態は常に[イベントの生成（Generate Events）]です。

  たとえば、ベース ポリシーが [アクティブなルールなし（No Rules Active）] の場合（すべてのルールが無効になっている）、[ドロップしてイベントを生成する（Drop and Generate Events）] は推奨されません。

- [ドロップしてイベントを生成する（Drop and Generate Events）] は、ベース ポリシーですでに[ドロップしてイベントを生成する（Drop and Generate Events）]に設定されているルールにのみ推奨します。

  ルールを [ドロップしてイベントを生成する（Drop and Generate Events）] に設定して、そのルールを無効にするか、またはベース ポリシーで [イベントの生成（Generate Events）] に設定した場合は、ルールの状態を手動でリセットする必要があります。

Firepower 推奨ルールの詳細設定を変更せずに推奨を生成する場合は、システムが検出対象のネットワーク全体のすべてのホストのルール状態の変更を推奨します。

デフォルトで、システムは、オーバーヘッドが低または中のルールに対してのみ推奨を生成し、ルールを無効にする推奨を生成します。

システムは、Impact Qualification 機能を使用して無効にされた脆弱性に基づく侵入ルールのルール状態を推奨しません。

システムは、常に、ホストにマップされたサードパーティの脆弱性に関連付けられたローカル ルールを有効にするように推奨します。

マップされていないローカル ルールに対する状態推奨は生成されません。

関連トピック

個々の脆弱性の非アクティブ化 （3189 ページ）
サードパーティ製品のマッピング （2509 ページ）

Firepower 推奨の詳細設定

推奨とルール状態とのすべての差をポリシー レポートに含める（Include all differences between recommendations and rule states in policy reports）

デフォルトで、侵入ポリシー レポートには、ポリシーで有効になっているルール、つまり、[イベントを生成する（Generate Events）] と [ドロップしてイベントを生成する（Drop and Generate Events）] のいずれかに設定されているルールが表示されます。また、[すべての差を含める（Include all differences）] オプションを有効にすると、推奨されている状態が保存されている状態と異なるルールが一覧表示されます。ポリシー レポートの詳細については、ポリシー レポート （458 ページ）を参照してください。

検査対象のネットワーク（Networks to Examine）

モニタ対象のネットワークまたは推奨について検査する個々のホストを指定します。1 つの IP アドレスまたはアドレス ブロックを指定するか、そのいずれかまたは両方から成るカンマで区切ったリストを指定できます。

指定したホスト内のアドレスのリストは、否定以外の OR 演算でリンクされ、すべての OR 演算の実行後に AND 演算でリンクされます。

ホスト情報に基づいて特定のパケットのアクティブ ルール処理を動的に適応させる場合は、アダプティブ プロファイルの更新 を有効にすることもできます。

推奨しきい値（ルール オーバーヘッドの指定）（Recommendation Threshold (By Rule Overhead)）

選択したしきい値をオーバーヘッドが超える侵入ルールが推奨または自動的に有効にされないようにします。

オーバーヘッドは、システム パフォーマンスに対するルールの潜在的影響とルールが誤検出を引き起こす確率に基づいています。オーバーヘッドが高いルールを許可すると、通常、より多くの推奨が生成されるようになりますが、システム パフォーマンスに影響を及ぼす可能性があります。[侵入ルール（Intrusion Rules）] ページのルール詳細ビューでルールのオーバーヘッドの評価を確認できます。

ただし、ルールを無効にする推奨ではルール オーバーヘッドが考慮されません。また、ローカル ルールは、サードパーティの脆弱性にマップされていない限り、オーバーヘッドがないものと見なされます。

特定の設定のオーバーヘッド評価のルールについて推奨を生成した場合でも、別のオーバーヘッドの推奨を生成してから、再び元のオーバーヘッド設定の推奨を生成することができます。推奨を生成した回数や異なるオーバーヘッド設定の数に関係なく、同じルール セットの推奨を生成するたびに、オーバーヘッド設定ごとに同じルール状態推奨が生成されます。たとえば、オーバーヘッドを「中」に設定して推奨を生成し、次に「高」にして推奨を生成してから、再び「中」にして推奨を生成することができます。ネットワーク上のホストとアプリケーションが変更されていなければ、オーバーヘッドが「中」の推奨は、どちらも、そのルール セットに対して同じになります。

ルールを無効にする推奨を受け入れる（Accept Recommendations to Disable Rules）

Firepower の推奨に基づいて侵入ルールを無効にするかどうかを指定します。

ルールを無効にする推奨を受け入れると、ルールの適用範囲が制限されます。ルールを無効にする推奨を無視すると、ルールの適用範囲が拡大されます。

関連トピック

Firepower システムの IP アドレス表記法 （20 ページ）
アダプティブプロファイルの更新および Firepower 推奨ルール （2464 ページ）

Firepower の推奨事項の生成と適用

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Intrusion Admin

Firepower の推奨事項の使用を開始または停止する場合、ネットワークのサイズと侵入ルールセットに応じて、数分かかる場合があります。

システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、先祖ドメインの侵入ポリシーでこの機能を有効にすると、システムはすべての子孫のリーフ ドメインからのデータを使用して、推奨事項を生成します。これにより、侵入ルールをすべてのリーフ ドメインに存在しない可能性があるアセットに調整することができ、パフォーマンスに影響を与えることができます。

ステップ 1 侵入ポリシー エディタのナビゲーション ウィンドウで、[Firepower の推奨事項（Firepower Recommendations）] をクリックします。

ステップ 2 （オプション）詳細設定を設定します。Firepower 推奨の詳細設定 （2110 ページ）を参照してください。

ステップ 3 推奨事項を生成して適用します。

- 推奨事項の生成および使用（Generate and Use Recommendations）：推奨事項を生成して、一致するようにルール状態を変更します。これまでに推奨事項を生成したことがない場合にのみ使用できます。
- 推奨事項の生成（Generate Recommendations）：推奨事項を使用しているかどうかに関係なく、新しい推奨事項を生成しますが、一致するようにルールの状態を変更しません。
- 推奨事項の更新（Update Recommendations）：推奨事項を使用している場合は、推奨事項を生成してルールの状態を一致するように変更します。それ以外の場合は、ルールの状態を変更することなく、新しい推奨事項を生成します。
- 推奨事項の使用（Use Recommendations）：ルールの状態を未実装の推奨事項に一致するように変更します。
- 推奨事項を使用しない（Do Not Use Recommendations）：推奨事項の使用を停止します。推奨事項の適用前にルールの状態を手動で変更した場合、ルールの状態は指定した値に戻ります。それ以外の場合、ルールの状態はデフォルト値に戻ります。

推奨事項の生成時に、システムは推奨される変更の概要を表示します。システムによって状態の変更が推奨されるルールのリストを表示するには、新しく提案されたルール状態の横にある [表示（View）] をクリックします。

ステップ 4 実装した推奨事項を評価して調整します。

ほとんどの Firepower の推奨事項を承認する場合でも、ルールの状態を手動で設定することで、個別の推奨事項を上書きできます。侵入ルール状態の設定 （2093 ページ）を参照してください。

ステップ 5 最後にポリシーを確定してからこのポリシーで加えた変更を保存するには、[ポリシー情報（Policy Information）] をクリックし、[変更の確定（Commit Changes）] をクリックします。

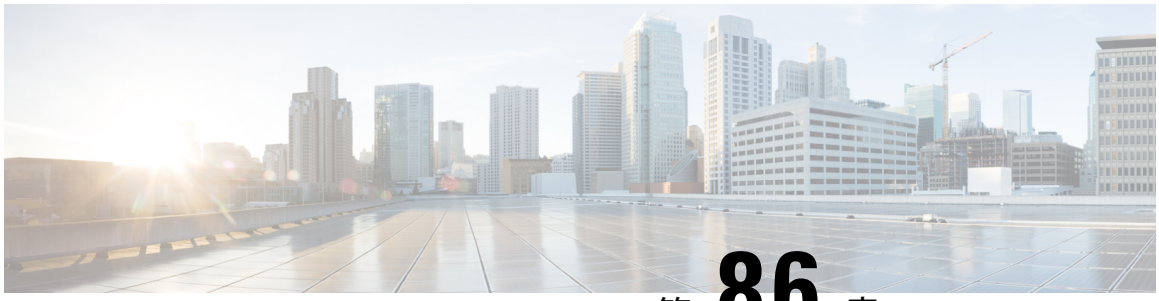
変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後の変更は破棄されます。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

関連トピック

Firepower 推奨の自動化 （247 ページ）



第 86 章

機密データの検出

ここでは、機密データ検出とその設定方法について説明します。

機密データ検出の基本

社会保障番号、クレジット カード番号、運転免許証番号などのセンシティブ データは、インターネットに意図的に、または誤って漏洩される可能性があります。システムには、ASCII テキストのセンシティブ データに関するイベントを検出し、生成できるセンシティブ データ プロセッサが用意されています。このプロセッサは、特に誤って漏洩されたデータの検出に役立ちます。

グローバル センシティブ データ プリプロセッサ オプションは、プリプロセッサの動作を制御します。以下のことを指定するグローバル オプションを変更できます。

- プリプロセッサが、ルールをトリガーしたパケットで、クレジット カード番号または社会保障番号の下位 4 桁を除くすべての桁を置換するかどうか
- センシティブ データをモニタする、ネットワーク上の宛先ホスト
- イベントの生成基準となる、単一のセッションでの全データ タイプの合計オカレンス数

個別のデータ タイプによって、指定した宛先ネットワーク トラフィックで検出しイベントを生成できるセンシティブ データを特定します。以下のことを指定するデータ タイプ オプションのデフォルト設定を変更できます。

- 検出されたデータ タイプに対して単一のセッションごとのイベントを生成する基準とするしきい値
- 各データ タイプをモニタする宛先ポート
- 各データ タイプをモニタするアプリケーション プロトコル

指定するデータ パターンを検出するためのカスタム データ タイプを作成および変更することができます。たとえば、病院で患者番号を保護するためのデータ タイプを作成したり、大学で固有の番号パターンを持つ学生番号を検出するためのデータ タイプを作成したりすることが考えられます。

システムはトラフィックに対して個別のデータ タイプを照合することによって、TCP セッションごとにセンシティブ データを検出します。侵入ポリシーの、各データ タイプのデフォルト設定およびすべてのデータ タイプに適用されるグローバル オプションのデフォルト設定は変更できます。Firepower システムには、一般的に使用されているデータ タイプがすでに定義されています。カスタム データ タイプを作成することも可能です。

センシティブ データ プリプロセッサ ルールは、各データ タイプに関連付けられます。各データ タイプのセンシティブ データ検出とイベント生成を有効にするには、そのデータ タイプに対応するプリプロセッサ ルールを有効にします。設定ページのリンクを使用すると、センシティブ データ ルールにフィルタリングされたビューが [Rules] ページに表示されます。このビューで、ルールを有効または無効にしたり、その他のルール属性を設定したりできます。

変更を侵入ポリシーに保存する際に提示されるオプションによって、データ タイプに関連付けられたルールが有効になっていてセンシティブ データ検出が無効になっている場合には、自動的にセンシティブ データ プリプロセッサを有効にすることができます。

ヒント 機密データ プリプロセッサでは、FTP または HTTP を使用してアップロードおよびダウンロードされる暗号化されていない Microsoft Word ファイル内の機密データを検出できます。これが可能である理由は、Word ファイルが ASCII テキストとフォーマット設定コマンドを分けてグループ化する方式だからです。

このシステムは、暗号化または難読化された機密データ、あるいは圧縮または符号化された形式の機密データ（たとえば、Base64 でエンコードされた電子メールの添付ファイルなど）の検出は行いません。たとえば、システムは電話番号 (555)123-4567 を検出しますが、(5 5 5) 1 2 3 - 4 5 6 7 のようにスペースで難読化されたバージョン、あるいは (555)-123--4567 のように HTML コードが介在するバージョンは検出しません。ただし、(555)-123-4567 のように、HTML にコーディングされた番号のパターンの途中にコードが入っていなければ検出されます。

グローバル センシティブ データ検出オプション

グローバル センシティブ データ オプションはポリシーに固有であり、すべてのデータ タイプに適用されます。

マスク

ルールをトリガーしたパケットで、クレジット カード番号および社会保障番号の下位4桁を除くすべての桁を「X」に置換します。Web インターフェイスの侵入イベント パケット ビューおよびダウンロードされたパケットでは、マスクされた番号が表示されます。

ネットワーク

センシティブ データをモニタする 1 つ以上の宛先ホストを指定します。単一の IP アドレス、アドレスブロック、あるいはこのいずれかまたは両方のカンマ区切りリストを指定できます。空白のフィールドは、`any` として解釈されます。これは、任意の宛先 IP アドレスを意味します。

システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。 上書き対応オブジェクトを使用すると、子孫ドメインの管理者は、グローバル コンフィギュレーションを自分のローカル環境に調整できます。

グローバルしきい値（Global Threshold）

グローバルしきい値イベントの生成基準となる、単一セッションでの全データ タイプの合計オカレンス数を指定します。データ タイプの組み合わせを問わず、プリプロセッサは指定された数のデータ タイプを検出すると、グローバルしきい値イベントを生成します。1 ～ 65535 の値を指定できます。

シスコでは、このオプションに、ポリシーで有効にする個々のデータ タイプに対するしきい値のどれよりも大きい値を設定することを推奨しています。

グローバルしきい値については、以下の点に注意してください。

- 複数のデータ タイプを合わせたオカレンス数を検出して イベントを生成し、インライン展開では、違反パケットをドロップします。 するには、プリプロセッサ ルールの 139:1 を有効にする必要があります。
- プリプロセッサが生成するグローバルしきい値イベントは、セッションあたり最大1件です。
- グローバルしきい値イベントと個別データ タイプ イベントは、互いに独立しています。つまり、グローバルしきい値に達すると、個別データ タイプに対するイベントしきい値に達しているかどうかに関わらず、プリプロセッサがイベントを生成します。その逆も当てはまります。

関連トピック

Firepower システムの IP アドレス表記法 （20 ページ）

個別のセンシティブ データ タイプのオプション

最低でも、カスタム データ タイプごとにイベントしきい値を指定し、モニタする少なくとも 1 つのポートまたはアプリケーション プロトコルを指定する必要があります。

各システム定義済みデータ タイプでは、デフォルト値が変更されない限り、アクセス不能な `sd_pattern` キーワードを使用して、トラフィックで検出する組み込みデータ パターンを定義します。カスタム データ タイプを作成して、そのデータ タイプに対し、単純な正規表現を使用して独自のデータ パターンを指定することもできます。

センシティブ データ タイプは、センシティブ データ検出が有効になっているすべての侵入ポリシーに表示されます。システム提供のデータ タイプは読み取り専用として表示されます。カスタム データ タイプの場合、名前とパターン フィールドは読み取り専用として表示されますが、他のオプションはポリシー固有の値に設定できます。

マルチドメイン展開では、現在のドメインで作成されたセンシティブ データ タイプが表示されます。これは編集できます。また、先祖ドメインで作成されたデータ タイプも表示されます。これは限定的な方法で編集できます。先祖のデータ タイプについては、名前およびパターン フィールドは読み取り専用として表示されますが、その他のオプションはポリシー固有の値に設定できます。

表 *148 :* 個別のデータ タイプのオプション

オプション	説明
データ タイプ	データ タイプの一意の名前を指定します。
しきい値（Threshold）	イベント生成の基準とする、データ タイプのオカレンス数を指定します。1 ～ 255 の値を指定できます。 プリプロセッサが検出したデータ タイプに対して生成するイベント数は、セッションごとに1つであることに注意してください。グローバルしきい値イベントと個別データ タイプ イベントは、互いに独立していることにも注意してください。つまり、データ タイプ イベントしきい値に達すると、グローバル イベントしきい値に達しているかどうかに関わらず、プリプロセッサがイベントを生成します。その逆も同様です。
宛先ポート（Destination Ports）	データ タイプでモニタする宛先ポートを指定します。単一のポート、複数のポートをカンマで区切ったリスト、または任意の宛先ポートを意味する `any` を指定できます。
アプリケーション プロトコル（Application Protocols）	データ タイプでモニタする最大 8 つのアプリケーション プロトコルを指定します。モニタするアプリケーション プロトコルを識別するには、アプリケーション ディテクタをアクティブにする必要があります。 従来のデバイスの場合、この機能には制御ライセンスが必要であることに注意してください。
パターン	検出するパターンを指定します。このフィールドは、カスタム データ タイプの場合にのみ存在します。

関連トピック

ディテクタのアクティブおよび非アクティブの設定 （2567 ページ）

システム提供のセンシティブ データのタイプ

それぞれの侵入ポリシーには、よく使用されるデータ パターンを検出するためのシステム提供のデータ タイプが含まれています。これらのデータ パターンには、クレジット カード番号、電子メールアドレス、米国の電話番号、および米国の社会保障番号などがあります（番号にはハイフン付きのパターン、ハイフン抜きのパターンがあります）。

それぞれのシステム提供のデータ タイプは、ジェネレータ ID（GID）が 138 に設定された単一のセンシティブ データのプリプロセッサ ルールに関連付けられます。侵入ポリシーで関連する機密データ ルールを有効にして、ポリシーで使用する各データ タイプに対して イベントを生成し、インライン展開では、違反パケットをドロップします。 する必要があります。

次の表に、各データ タイプの説明と対応するプリプロセッサ ルールの一覧を示します。

表 *149*: システム提供のセンシティブ データのタイプ

データ タイプ	説明	プリプロセッサ ルール GID：SID
クレジットカード番号	Visa®、MasterCard®、Discover®、および American Express® の 15 桁または 16 桁のクレジット カード番号（通常の区切り文字として使用されるハイフンまたはスペースが含まれるパターンと含まれないパターン）に一致します。また、Luhn アルゴリズムを使用してクレジット カード番号の検査数字を確認します。	138:2
Email Addresses	電子メール アドレスに一致します。	138:5
米国の電話番号	米国の電話番号（`(\d{3})?\d{3}-\d{4}` のパターンに準拠）に一致します。	138:6
米国の 社会保障番号（ハイフンなし）	米国の 9 桁の 社会保障番号（有効な 3 桁のエリア番号と有効な 2 桁のグループ番号が含まれ、ハイフンを使用していない番号）に一致します。	138:4

データ タイプ	説明	プリプロセッサ ルール **GID**：**SID**
米国の 社会保障番号（ハイフンあり）	米国の 9 桁の 社会保障番号（有効な 3 桁のエリア番号と有効な 2 桁のグループ番号が含まれ、ハイフンを使用した番号）に一致します。	138:3

社会保障番号以外の 9 桁の番号からの誤検出を軽減するために、プリプロセッサでは、各社会保障番号の 4 桁のシリアル番号の前にある 3 桁のエリア番号と 2 桁のグループ番号を検証するアルゴリズムを使用します。プリプロセッサは 2009 年 11 月末までの社会保障グループ番号を検証します。

センシティブ データ検出の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	保護またはコントロール	いずれか（Any）	いずれか（Any）	Admin/Intrusion Admin

センシティブ データ検出は、Firepower システムのパフォーマンスに非常に大きな影響を与える可能性があるため、以下のガイドラインに従うことをお勧めします。

- 基本侵入ポリシーとして [アクティブなルールなし（No Rules Active）] デフォルト ポリシーを選択します。
- 次の設定が対応するネットワーク分析ポリシーで有効になっていることを確認します。
  - **アプリケーション層プリプロセッサ**での **FTP と Telnet の設定**
  - [トランスポートまたはネットワーク レイヤ プロセッサ（Transport/Network Layer Preprocessors）] の下の [IP 最適化（IP Defragmentation）] および [TCP ストリームの構成（TCP Stream Configuration）]

マルチドメイン展開では、編集できる現在のドメインで作成されたポリシーが表示されます。また、編集できない先祖ドメインで作成されたポリシーも表示されます。下位のドメインで作成されたポリシーを表示および編集するには、そのドメインに切り替えます。

ステップ 1 **[Policies]** > **[Access Control]** > **[Intrusion]** を選択します。

ステップ 2 編集するポリシーの横にある編集アイコン（  ）をクリックします。

代わりに表示アイコン（  ）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 ナビゲーション ウィンドウで [詳細設定（Advanced Settings）] をクリックします。

ステップ 4 [特定の脅威検出（Specific Threat Detection）] の下の [センシティブ データ検出（Sensitive Data Detection）] が無効になっている場合は、[有効（Enabled）] をクリックします。

ステップ 5 [センシティブ データ検出（Sensitive Data Detection）] の横にある編集アイコン（  ）をクリックします。

ステップ 6 次の選択肢があります。

- グローバル センシティブ データ検出オプション （2114 ページ）の説明に従って、グローバル設定を変更します。
- [ターゲット（Targets）]セクションでデータ タイプを選択し、個別のセンシティブ データ タイプのオプション （2115 ページ）の説明に従って、データ タイプ構成を変更します。
- カスタム センシティブ データを検査するには、カスタム 機密データ タイプ （2122 ページ）を参照してください。

ステップ 7 データ タイプでモニタするアプリケーション プロトコルを追加または削除します。監視対象のアプリケーション プロトコルおよび機密データ （2120 ページ）を参照してください。

（注） FTP トラフィックでセンシティブ データを検出するには、`Ftp data` アプリケーション プロトコルを追加します。

ステップ 8 オプションで、センシティブ データ プリプロセッサ ルールを表示するには、[センシティブ データ検出のルールの設定（Configure Rules for Sensitive Data Detection）] をクリックします。

リストされているルールを有効または無効にすることができます。[ルール（Rules）] ページで使用可能なその他の操作（ルールの抑制、レートベース攻撃防止など）のセンシティブ データ ルールも設定できます。詳細については、侵入ルールのタイプ （2074 ページ）を参照してください。

ステップ 9 最後のポリシー確定後にこのポリシーで行った変更を保存するには、ナビゲーション パネルで [ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。

ポリシーでセンシティブ データ プリプロセッサ ルールを有効にして、センシティブ データ検出を有効にしていなければ、変更をポリシーに保存する際に、センシティブ データ検出を有効にするよう求めるプロンプトが出されます。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後の変更は破棄されます。

次のタスク

- 侵入イベントを生成する場合は、センシティブ データ検出ルール（138:2、138:3、138:4、138:5、138:6、138:>999999、または 139:1）を有効にします。詳細については、侵入ルールの状態 （2092 ページ）、グローバル センシティブ データ検出オプション （2114 ページ）、システム提供のセンシティブ データのタイプ （2117 ページ）、およびカスタム 機密データ タイプ （2122 ページ）を参照してください。
- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

関連トピック

特別なケース：FTP トラフィックでのセンシティブ データの検出 （2121 ページ）

監視対象のアプリケーションプロトコルおよび機密データ

各データ タイプでモニタするアプリケーション プロトコルを最大 8 つ指定できます。選択するアプリケーションプロトコルごとに、少なくとも1つのディテクタを有効にする必要があります。デフォルトでは、すべてのディテクタがアクティブになっています。有効になっているディテクタがないアプリケーションプロトコルについては、システム提供のすべてのディテクタが自動的に有効になります。ディテクタが存在しない場合は、そのアプリケーションについて最後に変更されたユーザ定義ディテクタが有効になります。

各データ タイプをモニタするアプリケーション プロトコルまたはポートを少なくとも 1 つ指定する必要があります。ただし、FTP トラフィックでセンシティブデータを検出する場合を除き、シスコでは最も包括的なカバレッジにするために、アプリケーションプロトコルを指定する際には対応するポートを指定することを推奨しています。たとえば、HTTP を指定するとしたら、既知の HTTP ポート 80 を設定することお勧めします。このように設定すると、ネットワークの新しいホストが HTTP を実装する場合には、システムは新しい HTTP アプリケーション プロトコルを検出する間、ポート 80 をモニタします。

FTP トラフィックでセンシティブ データを検出する場合は、`FTP data` アプリケーション プロトコルを指定する必要があります。この場合、ポート番号を指定する利点はありません。

関連トピック

ディテクタのアクティブおよび非アクティブの設定 （2567 ページ）
特別なケース：FTP トラフィックでのセンシティブ データの検出 （2121 ページ）

モニタ対象のアプリケーション プロトコルの選択

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Control	いずれか（Any）	いずれか（Any）	Admin/Intrusion Admin

モニタ対象のアプリケーション プロトコルは、システムが提供するセンシティブ データ タイプとカスタムのセンシティブ データ タイプの両方で指定できます。選択するアプリケーション プロトコルはポリシー固有になります。

ステップ 1 **[Policies]** > **[Access Control]** > **[Intrusion]**を選択します。

ステップ 2 編集するポリシーの横にある編集アイコン（  ）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 ナビゲーション ウィンドウで [詳細設定（Advanced Settings）] をクリックします。

ステップ 4 [特定の脅威検出（Specific Threat Detection）] の下の [センシティブ データ検出（Sensitive Data Detection）] が無効になっている場合は、[有効（Enabled）] をクリックします。

ステップ 5 [センシティブ データ検出（Sensitive Data Detection）] の横にある編集アイコン（）をクリックします。

ステップ 6 [データ タイプ（Data Types）] の下でデータ タイプの名前をクリックします。

ステップ 7 [アプリケーション プロトコル（Application Protocols）] フィールドの横にある編集アイコン（）をクリックします。

ステップ 8 次の選択肢があります。

- モニタするアプリケーション プロトコルを追加するには、[使用可能（Available）] リストからアプリケーション プロトコルを 1 つ以上選択して、右矢印（[>]）ボタンをクリックします。モニタするアプリケーション プロトコルは、8 つまで追加できます。
- モニタ対象からアプリケーション プロトコルを削除するには、[有効（Enabled）] リストから削除するプロトコルを選択して、左矢印（[<]）ボタンをクリックします。

ステップ 9 [OK] をクリックします。

ステップ 10 最後のポリシーの確定以降に、このポリシーに加えた変更を保存するには、ナビゲーション ウィンドウで [ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後の変更は破棄されます。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

関連トピック

特別なケース：FTP トラフィックでのセンシティブ データの検出 （2121 ページ）

特別なケース：FTP トラフィックでのセンシティブ データの検出

一般に、センシティブ データをモニタするトラフィックを決めるには、導入でのモニタ対象のポートを指定するか、アプリケーション プロトコルを指定します。

ただし、FTP トラフィックでセンシティブ データを検出するには、ポートまたはアプリケーション プロトコルを指定するだけでは不十分です。FTP トラフィックのセンシティブ データ

は、FTPアプリケーションプロトコルのトラフィックで検出されますが、これは断続的に発生し、一時的なポート番号が使用されるため、検出が困難です。FTP トラフィックでセンシティブ データを検出するには、以下の設定を含めることが**必須**となります。

- `FTP data` アプリケーション プロトコルを指定すると、FTP トラフィックでのセンシティブ データの検出が可能になります。

  FTP トラフィックでセンシティブ データを検出するという特殊な場合では、`FTP data` アプリケーションプロトコルを指定すると、検出が呼び出される代わりに、FTP トラフィックでセンシティブ データを検出するために FTP/Telnet プロセッサの高速処理が呼び出されます。

- FTP データ ディテクタが有効であることを確認します（デフォルトで有効にされています）。
- 設定に、センシティブデータをモニタするポートが少なくとも 1 つ含まれていることを確認します。

FTP トラフィックでセンシティブデータを検出することだけが目的の場合を除き（そのような場合はほとんどありません）、FTP ポートを指定する必要はありません。通常のセンシティブデータ設定には、HTTP ポートや電子メール ポートなどの他のポートが含まれることになります。モニタ対象の FTP ポートを 1 つだけ指定し、他のポートを指定しない場合、シスコでは FTP コマンド ポート `23` を指定することを推奨しています。

関連トピック

FTP/Telnet デコーダ （2323 ページ）
ディテクタのアクティブおよび非アクティブの設定 （2567 ページ）
センシティブ データ検出の設定 （2118 ページ）

カスタム 機密データ タイプ

作成するカスタム データ タイプごとに、単一の機密データ プリプロセッサ ルールも作成します。このルールのジェネレータ ID（GID）は 138 で、[Snort ID]（SID）は 1000000 以上（これは、ローカル ルールの SID）です。

ポリシーで使用する各カスタム データ タイプに対し、関連付けられた機密データ ルールを有効にして検出を有効にし、イベントを生成し、インライン展開では、違反パケットをドロップします。 する必要があります。

機密データ ルールを有効にするには、設定ページに表示されるリンクを利用できます。このリンクを使用すると、すべてのシステム定義済み機密データ ルールおよびカスタム機密データ ルールを表示するフィルタリングされたビューの侵入ポリシーの [ルール（Rules）] ページが表示されます。また、侵入ポリシーの [ルール（Rules）] ページでローカル フィルタリング カテゴリを選択することで、カスタム機密データ ルールをカスタム ローカル ルールとともに表示できます。カスタム機密データ ルールは、侵入ルール エディタ ページ（**[Objects]** > **[Intrusion Rules]**）には表示されないことに注意してください。

カスタム データ タイプを作成すると、システム内の任意の侵入ポリシーで、マルチドメイン展開の場合は現在のドメイン内の侵入ポリシーでそれを有効にすることができます。カスタム データ タイプを有効にするには、そのカスタム データ タイプの検出に使用するポリシーで、関連する機密データ ルールを有効にする必要があります。

カスタム機密データ タイプのデータ パターン

カスタム データ タイプのデータ パターンを定義するには、以下の要素からなる単純な正規表現のセットを使用します。

- 3 つのメタ文字
- メタ文字をリテラル文字として使用するためのエスケープ文字
- 6 文字クラス

メタ文字は正規表現内で特別な意味を持つリテラル文字です。

表 *150* : 機密データ パターンのメタ文字

メタ文字	説明	例
?	先行する文字またはエスケープ シーケンスのゼロまたは 1 つのオカレンスに一致します。つまり、先行する文字またはエスケープ シーケンスはオプションです。	colou?r は、color または colour に一致します。
{n}	先行する文字またはエスケープ シーケンスの n 回の繰り返しに一致します。	たとえば、\d{2} は 55、12 などに\l{3} は AbC、www など、\w{3} は a1B、 25C など、x{5} はxxxxx に一致します
\	メタ文字を実際の文字として使用できます。また、事前定義された文字クラスを指定するためにも使われます。	\? は疑問符、\\ はバックスラッシュ、\d は数字に一致します。

特定の文字をリテラル文字として機密データ プリプロセッサに正しく解釈させるには、バックスラッシュで文字をエスケープする必要があります。

表 *151* : 機密データ パターンのエスケープ文字

使用するエスケープ文字	表現されるリテラル文字
\?	?
\{	{
\}	}
\\	\

カスタム機密データ パターンを定義するときは、文字クラスを使用できます。

表 *152 :* 機密データ パターンの文字クラス

文字クラス	説明	文字クラスの定義
\d	ASCII 文字の数字 0 ～ 9 に一致します。	0 ～ 9
\D	ASCII 文字の数字ではないバイトに一致します。	0 ～ 9 以外
\l （小文字の「エル」）	任意の ASCII 文字に一致します。	a ～ zA ～ Z
\L	ASCII 文字ではないバイトに一致します。	a ～ z および A ～ Z 以外
\w	任意の ASCII 英数字に一致します。 PCRE 正規表現とは異なり、アンダースコア（_）は含まれないことに注意してください。	a ～ z、A ～ Z、および 0 ～ 9
\W	ASCII 英数字でないバイトに一致します。	a ～ z、A ～ Z、および 0 ～ 9 以外

プリプロセッサは、そのまま入力された文字を、正規表現の一部ではなく、リテラル文字として扱います。たとえば、データ パターン 1234 は `1234` に一致します。

以下に、システム定義済み機密データ ルール 138:4 で使用するデータ パターンの例を示します。このパターンでは、エスケープされた数値の文字クラス、複数個を示すメタ文字およびオプション指定子のメタ文字、リテラル ハイフン（-）文字、および左右の括弧 () 文字を使用して、米国の電話番号を検出します。

```
(\d{3}) ?\d{3}-\d{4}
```

カスタム データ パターンを作成する際には注意が必要です。以下に、電話番号を検出するための別のデータ パターンを示します。このパターンでは有効な構文を使用しているものの、多数の誤検出が発生する可能性があります。

```
(?\d{3})? ?\d{3}-?\d{4}
```

上記の2番目の例では、オプションの括弧、オプションのスペース、オプションのハイフンを組み合わせているため、目的とする以下のパターンの電話番号が検出されます。

- `(555)123-4567`
- `555123-4567`
- `5551234567`

ただし、2 番目の例のパターンでは、以下の潜在的に無効な無効なパターンも検出されて、結果的に誤検出となります。

- `(555 1234567`
- `555)123-4567`
- `555) 123-4567`

最後に、説明目的の極端な例として、小規模な企業ネットワーク上のすべての宛先トラフィックで小さいイベントしきい値を使用して、小文字の `a` を検出するデータ パターンを作成するとします。このようなデータ パターンは、わずか数分で文字通り数百万ものイベントを生成することになり、システムを過負荷に陥らせる可能性があります。

カスタム センシティブ データ タイプの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Intrusion Admin

マルチドメイン展開では、現在のドメインで作成されたセンシティブ データ タイプが表示されます。これは編集できます。また、先祖ドメインで作成されたデータ タイプも表示されます。これは限定的な方法で編集できます。先祖のデータ タイプについては、名前およびパターン フィールドは読み取り専用として表示されますが、その他のオプションはポリシー固有の値に設定できます。

データ タイプのセンシティブ データ ルールがいずれかの侵入ポリシーで有効にされている場合、そのデータ タイプを削除することはできません。

ステップ 1 **[Policies]** > **[Access Control]** > **[Intrusion]** を選択します。

ステップ 2 編集するポリシーの横にある編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 ナビゲーション ウィンドウで [詳細設定（Advanced Settings）] をクリックします。

ステップ 4 [特定の脅威検出（Specific Threat Detection）] の下の [センシティブ データ検出（Sensitive Data Detection）] が無効になっている場合は、[有効（Enabled）] をクリックします。

ステップ 5 [センシティブ データ検出（Sensitive Data Detection）] の横にある編集アイコン（）をクリックします。

ステップ 6 [データ タイプ（Data Types）] の横にある追加アイコン（）をクリックします。

ステップ 7 データ タイプの名前を入力します。

ステップ 8 このデータ タイプで検出するパターンを入力します。カスタム機密データ タイプのデータ パターン （2123 ページ）を参照してください。

ステップ 9 [OK] をクリックします。

ステップ 10 必要に応じて、データ タイプ名をクリックし、個別のセンシティブ データ タイプのオプション （2115 ページ）で説明されているオプションを変更します。

ステップ 11 必要に応じて、削除アイコン（）をクリックしてカスタム データ タイプを削除し、[OK] をクリックして確認します。

（注） いずれかの侵入ポリシーでデータ タイプのセンシティブ データ ルールが有効になっている場合は、そのデータ タイプを削除できないことが警告されます。再度削除を試みる前に、影響を受けるポリシーでセンシティブ データ ルールを無効にする必要があります。侵入ルール状態の設定 （2093 ページ）を参照してください。

ステップ 12 最後のポリシー確定後にこのポリシーで行った変更を保存するには、ナビゲーション パネルで[ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後の変更は破棄されます。

次のタスク

- データ型を使用する各ポリシーで、関連付けられたカスタム センシティブ データの前処理ルールを有効にします。侵入ルール状態の設定 （2093 ページ）を参照してください。
- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

関連トピック

カスタムセンシティブ データ タイプの編集 （2126 ページ）

カスタムセンシティブ データ タイプの編集

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Intrusion Admin

カスタム センシティブ データ タイプのすべてのフィールドを編集できます。ただし、名前またはパターン フィールドを変更すると、システム内のすべての侵入ポリシーのこれらの設定が変更されることに注意してください。その他のオプションは、ポリシー固有の値に設定できます。

マルチドメイン展開では、現在のドメインで作成されたセンシティブ データ タイプが表示されます。これは編集できます。また、先祖ドメインで作成されたデータ タイプも表示されます。これは限定的な方法で編集できます。先祖のデータ タイプについては、名前およびパターン フィールドは読み取り専用として表示されますが、その他のオプションはポリシー固有の値に設定できます。

ステップ 1 **[Policies]** > **[Access Control]** > **[Intrusion]** を選択します。

ステップ 2 編集するポリシーの横にある編集アイコン（  ）をクリックします。

代わりに表示アイコン（  ）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 ナビゲーション ウィンドウで [詳細設定（Advanced Settings）] をクリックします。

ステップ 4 [特定の脅威検出（Specific Threat Detection）] の下の [センシティブ データ検出（Sensitive Data Detection）] が無効になっている場合は、[有効（Enabled）] をクリックします。

ステップ 5 [センシティブ データ検出（Sensitive Data Detection）] の横にある [編集（Edit）] をクリックします。

ステップ 6 [ターゲット（Targets）] セクションで、カスタム データ タイプの名前をクリックします。

ステップ 7 [データ タイプの名前およびパターンの編集（Edit Data Type Name and Pattern）] をクリックします。

ステップ 8 データ タイプの名前およびパターンを変更します。カスタム機密データ タイプのデータ パターン（2123 ページ）を参照してください。

ステップ 9 [OK] をクリックします。

ステップ 10 残りのオプションをポリシー固有の値に設定します。個別のセンシティブ データ タイプのオプション（2115 ページ）を参照してください。

ステップ 11 最後のポリシー確定後にこのポリシーで行った変更を保存するには、ナビゲーション パネルで [ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後の変更は破棄されます。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

第 87 章

侵入イベント ロギングのグローバル制限

次のトピックでは、侵入イベントロギングをグローバルに制限する方法について説明します。

グローバル ルールのしきい値の基本

グローバル ルールのしきい値は、侵入ポリシーによってイベント ロギングの限界を設定します。すべてのトラフィックに対するグローバルルールのしきい値を設定して、指定された期間に特定の送信元または宛先からのイベントがポリシーで記録および表示される頻度を制限できます。ポリシー内で共有オブジェクトのルール、標準テキストルール、またはプリプロセッサルールごとにしきい値を設定できます。グローバルしきい値を設定すると、上書きする特定のしきい値を指定していないポリシー内の各ルールでそのしきい値が適用されます。しきい値により、多数のイベントでいっぱいになることを回避できます。

すべての侵入ポリシーにはデフォルトのグローバル ルールしきい値が含まれていて、デフォルトですべての侵入ルールとプリプロセッサ ルールに適用されます。このデフォルトのしきい値は、宛先へのトラフィックでのイベントの数を 60 秒あたり 1 個のイベントに制限しています。

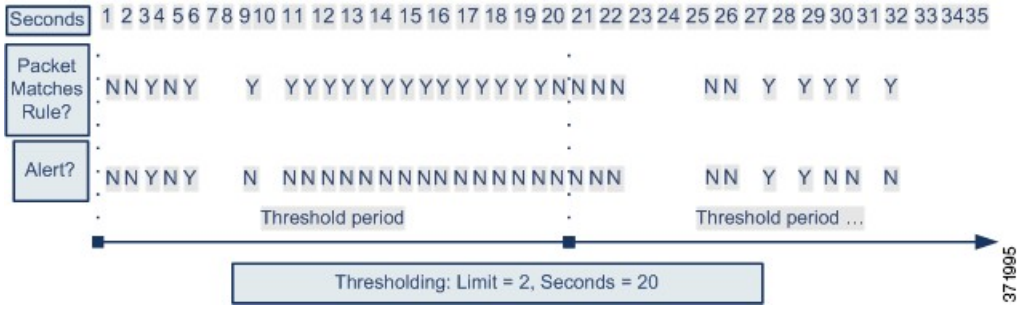
次の操作を実行できます。

- グローバルしきい値の変更。
- グローバルしきい値の無効化。
- 特定のルールに個別のしきい値を設定して、グローバルしきい値の上書き。

  たとえば、グローバル制限しきい値を 60 秒ごとに 5 個のイベントに設定してから、SID 1315 について特定のしきい値として 60 秒ごとに 10 個のイベントに設定できます。他のすべてのルールでは 60 秒ごとに 6 個以上のイベントは生成されませんが、SID 1315 では 60 秒ごとに最大 10 個のイベントが生成されます。

ヒント　複数の CPU を搭載した管理対象デバイスでグローバルしきい値または個別のしきい値を設定すると、予想より多くのイベントが生成される場合があります。

次の図で、グローバルルールのしきい値がどのように機能するかを示します。この例では、特定のルールに対して攻撃が進行中です。グローバル制限しきい値は、各ルールのイベント生成が 20 秒あたり 2 つのイベントに制限されるように設定されています。期間は 1 秒で始まり 21 秒で終わることに注意してください。期間が終了すると、サイクルが再び開始され、次の2つのルール一致によってイベントが生成されます。その後、その期間にさらにイベントが生成されることはありません。



グローバル ルールしきい値オプション

デフォルトのしきい値では、各ルールのイベント生成が、同じ宛先に送られるトラフィックで 60 秒あたり 1 つのイベントに制限されます。グローバル ルールしきい値オプションのデフォルト値は次のとおりです。

- **Type** — Limit
- **Track By** — Destination
- **Count** — 1
- **Seconds** — 60

これらのデフォルト値は次のように変更することができます。

表 *153 :* しきい値のタイプ

オプション	説明
Limit	指定された数のパケット（カウント引数によって指定される）が、指定された期間内にルールをトリガーとして使用した場合に、イベントを記録して表示します。 たとえば、タイプを [制限（Limit）] に、[カウント（Count）] を 10 に、[秒（Seconds）] を 60 に設定し、14 個のパケットがルールをトリガーとして使用した場合、システムはその 1 分の間に発生した最初の 10 個を表示した後、イベントの記録を停止します。
Threshold	指定された数のパケット（カウント引数によって指定される）が、指定された期間内にルールをトリガーとして使用した場合に、1 つのイベントを記録して表示します。イベントのしきい値カウントに達し、システムがそのイベントを記録した後、時間のカウンタは再び開始されることに注意してください。 たとえば、タイプを [Threshold] に、[Count] を 10 に、[Seconds] を 60 に設定して、ルールが 33 秒間で 10 回トリガーされたとします。システムは 1 つのイベントを生成すると、[Seconds] と [Count] のカウンタを 0 にリセットします。次の 25 秒間にルールがさらに 10 回トリガーされたとします。33 秒でカウンタが 0 にリセットされたため、システムが別のイベントを記録します。

オプション	説明
Both	指定された数（カウント）のパケットがルールをトリガーとして使用した後で、指定された期間ごとに1回イベントを記録して表示します。 たとえば、タイプを [Both] に、[Count] を 2 に、[Seconds] を 10に設定した場合、イベント数は以下のようになります。 • ルールが 10 秒間に 1 回トリガーされた場合、システムはイベントを生成しません（しきい値が満たされていない）。 • ルールが 10 秒間に 2 回トリガーされた場合、システムは 1 つのイベントを生成します（ルールが 2 回トリガーとして使用した場合、しきい値が満たされるため）。 • ルールが 10 秒間に 4 回トリガーされた場合、システムは 1 つのイベントを生成します（ルールが 2 回トリガーされると、しきい値が満たされ、以後のイベントは無視されるため）。

[追跡対象（Track By）] オプションにより、イベント インスタンスの数が送信元 IP アドレスと宛先 IP アドレスのどちらに基づいて計算されるかが決まります。

また、しきい値を定義するインスタンスの数と期間を次のように指定できます。

表 *154 :* インスタンス/時間のしきい値設定オプション

オプション	説明
Count	[制限（Limit）] しきい値の場合は、しきい値を満たすために必要な、追跡する IP アドレスまたはアドレス範囲単位で指定された期間単位のイベント インスタンスの数。 [しきい値（Threshold）] しきい値の場合は、しきい値として使用するルールの一致回数。

オプション	説明
秒（Seconds）	[制限（Limit）] しきい値の場合は、攻撃を追跡する期間の秒数。 [しきい値（Threshold）] しきい値の場合は、カウントをリセットするまでの経過時間（秒数）。しきい値タイプを [Limit] に、トラッキングを [Source] に、[Count] を 10 に、[Seconds] を 10 に設定した場合、特定のソース ポートで 10 秒間に発生した最初の 10 のイベントを記録し表示します。最初の 10 秒で 7 個のイベントだけが発生した場合、システムはそれらを記録して表示します。最初の 10 秒で 40 個のイベントが発生した場合、システムは 10 個を記録して表示し、10 秒経過してからカウントを再度開始します。

関連トピック

グローバルなしきい値の設定 （2133 ページ）
侵入イベントのしきい値 （2094 ページ）

グローバルなしきい値の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Intrusion Admin

マルチドメイン展開では、編集できる現在のドメインで作成されたポリシーが表示されます。また、編集できない先祖ドメインで作成されたポリシーも表示されます。下位のドメインで作成されたポリシーを表示および編集するには、そのドメインに切り替えます。

ステップ 1 **[Policies]** > **[Access Control]** > **[Intrusion]**を選択します。

ステップ 2 編集するポリシーの横にある編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 ナビゲーション ウィンドウで [詳細設定（Advanced Settings）] をクリックします。

ステップ 4 [侵入ルールしきい値（Intrusion Rule Thresholds）] で [グローバル ルールしきい値（Global Rule Thresholding）] が無効になっている場合は、[有効化（Enabled）] をクリックします。

ステップ 5 [グローバル ルールしきい値（Global Rule Thresholding）] の横にある編集アイコン（）をクリックします。

ステップ 6 [タイプ（Type）] オプション ボタンを使用して、[秒（Seconds）] フィールドで指定された時間内に適用するしきい値のタイプを指定します。

ステップ 7 [追跡対象（Track By）] オプション ボタンを使用して、追跡方法を指定します。

ステップ 8 [カウント（Count）] フィールドに値を入力します。

ステップ 9 [秒（Seconds）] フィールドに値を入力します。

ステップ 10 最後にポリシーを確定してからこのポリシーで加えた変更を保存するには、[ポリシー情報（Policy Information）] をクリックし、[変更の確定（Commit Changes）] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後の変更は破棄されます。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

関連トピック

グローバル ルールしきい値オプション （2130 ページ）
レイヤでの侵入ルールの設定 （2057 ページ）
競合と変更：ネットワーク分析および侵入ポリシー （2041 ページ）

グローバルしきい値の無効化

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Intrusion Admin

デフォルトですべてのルールにしきい値を適用するのではなく、特定のルールに関するイベントにしきい値を適用する場合は、最高位のポリシー階層でグローバルしきい値を無効にできます。

マルチドメイン展開では、編集できる現在のドメインで作成されたポリシーが表示されます。また、編集できない先祖ドメインで作成されたポリシーも表示されます。下位のドメインで作成されたポリシーを表示および編集するには、そのドメインに切り替えます。

ステップ 1 **[Policies]** > **[Access Control]** > **[Intrusion]** を選択します。

ステップ 2 編集するポリシーの横にある編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 ナビゲーション ウィンドウで [詳細設定（Advanced Settings）] をクリックします。

ステップ 4 [侵入ルールしきい値（Intrusion Rule Thresholds）] で、[グローバル ルールしきい値（Global Rule Thresholding）] の隣にある [無効（Disabled）] をクリックします。

ステップ 5 最後にポリシーを確定してからこのポリシーで加えた変更を保存するには、[ポリシー情報（Policy Information）] をクリックし、[変更の確定（Commit Changes）] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後の変更は破棄されます。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

関連トピック

競合と変更：ネットワーク分析および侵入ポリシー （2041 ページ）
レイヤでの侵入ルールの設定 （2057 ページ）

第 88 章

侵入ルール エディタ

以下のトピックでは、侵入ルール エディタの使用方法について説明します。

侵入ルールの編集について

侵入ルールは、ネットワークの脆弱性を不正利用する試みを検出するために使用するキーワードや引数です。ネットワーク トラフィックの分析では、パケットを各ルールで指定した条件と比較します。パケットのデータがルールで指定したすべての条件に一致すると、そのルールがトリガーされます。アラート ルールであれば、侵入イベントが生成されます。通過ルールであれば、トラフィックを無視します。インライン展開の廃棄ルールでは、システムがパケットを破棄してイベントを生成します。侵入イベントは、Firepower Management Center の Web インターフェイスから表示して評価できます。

Firepower システムの侵入ルールには、共有オブジェクト ルールと標準テキスト ルールの 2 種類があります。Cisco Talos Intelligence Group（Talos） では、共有オブジェクト ルールを使うことにより、従来の標準テキスト ルールではできなかった方法で脆弱性に対する攻撃を検出できます。共有オブジェクト ルールを作成することはできません。独自の侵入ルールを作成する場合は、標準テキスト ルールを作成します。

発生する可能性のあるイベントのタイプを調整するために、カスタム標準テキスト ルールを作成することができます。このマニュアルでは特定のエクスプロイトの検出を目的とするルールについて説明することもありますが、優秀なルールのほとんどは、特定の既知のエクスプロイトではなく既知の脆弱性を悪用しようとするトラフィックをターゲットとすることに注意してください。ルールを作成してルールのイベント メッセージを指定することにより、攻撃とポリシー回避を示唆するトラフィックをより簡単に識別できます。

カスタム侵入ポリシーでカスタム標準テキストルールを有効にすると、一部のルールキーワードと引数では、トラフィックを特定の方法で最初に復号化または前処理する必要があることに留意してください。この章では、前処理を制御するネットワーク分析ポリシーに設定する必要があるオプションについて説明します。注意点として、必要なプリプロセッサを無効にすると、システムは自動的に現在の設定でプリプロセッサを使用します。ただし、ネットワーク分析ポリシーの Web インターフェイスではプリプロセッサは無効のままになります。

⚠

注意 作成した侵入ルールを実稼働環境で使用する前に、制御されたネットワーク環境で必ずテストしてください。不適切に作成された侵入ルールは、システムのパフォーマンスに重大な影響を与える可能性があります。

マルチドメイン展開では、現在のドメインで作成されたルールが表示されます。これは編集できます。先祖ドメインで作成されたルールも表示されますが、これは編集できません。下位のドメインで作成されたルールを表示および編集するには、そのドメインに切り替えます。システム提供の侵入ルールはグローバル ドメインに属します。子孫ドメインの管理者は、これらのシステム ルールをローカルにコピーして編集できます。

ルールの詳細

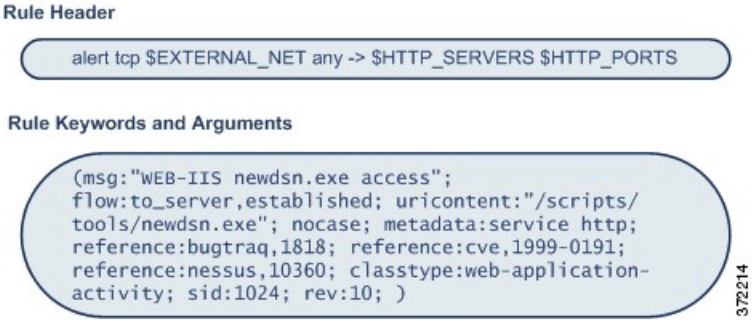
すべての標準テキスト ルールには、ルール ヘッダーとルール オプションという 2 つの論理セクションが含まれています。ルール ヘッダーの内容は次のとおりです。

- ルールのアクションまたはタイプ
- プロトコル
- 送信元および宛先の IP アドレスとネットマスク
- 送信元から宛先へのトラフィック フローを示す方向インジケータ
- 送信元ポートと宛先ポート

ルール オプション セクションの内容は次のとおりです。

- イベント メッセージ
- キーワードとそのパラメータおよび引数
- ルールをトリガーとして使用するためにパケットのペイロードが一致しなければならないパターン
- パケットのどの部分をルール エンジンで検査するかの指定

次の図に、ルールの構成要素を示します。



ルールのオプションセクションは、カッコで囲まれたセクションであることに注意してください。侵入ルール エディタは、標準テキスト ルールの作成を支援する使いやすいインターフェイスを備えています。

侵入ルール ヘッダー

すべての標準テキストルールおよび共有オブジェクトルールに、パラメータと引数を含むルール ヘッダーがあります。ルール ヘッダーの構成要素を以下に示します。

次の表では、上記のルール ヘッダーの各部分について説明します。

表 *155 :* ルール ヘッダーの値

ルールヘッダーのコンポーネント	値の例	機能
アクション	`alert`	トリガー時に侵入イベントを生成します。
プロトコル	`tcp`	TCP トラフィックのみをテストします。
送信元 IP アドレス	`$EXTERNAL_NET`	内部ネットワーク上に存在しないホストから送られてきたトラフィックをテストします。
Source Ports	任意	発信元ホスト上の任意のポートから送られてきたトラフィックをテストします。
Operator	`->`	（このネットワーク上の Web サーバに向かう）外部トラフィックをテストします。
宛先 IP アドレス	`$HTTP_SERVERS`	この内部ネットワーク上の Web サーバとして指定された任意のホストに送られるトラフィックをテストします。

ルールヘッダーのコンポーネント	値の例	機能
Destination Ports	`$HTTP_PORTS`	この内部ネットワーク上の HTTP ポートに送られるトラフィックをテストします。

（注） 前述の例では、ほとんどの侵入ルールの場合と同様に、デフォルト変数が使用されています。

関連トピック

変数セット （538 ページ）

侵入ルール ヘッダー アクション

各ルールヘッダーには、パケットがルールをトリガーとして使用したときにシステムで行われるアクションを指定するパラメータが 1 つ含まれています。アクションが *alert* に設定されたルールは、それをトリガーとして使用したパケットに関する侵入イベントを生成し、そのパケットの詳細をログに記録します。アクションが *pass* に設定されたルールは、それをトリガーとして使用したパケットに関するイベントを生成せず、そのパケットの詳細も記録しません。

（注） インライン展開において、ルール状態が [Drop and Generate Events] に設定されたルールは、それをトリガーとして使用したパケットに関する侵入イベントを生成します。また、パッシブ展開で廃棄ルールを適用した場合は、ルールがアラート ルールとして機能します。

デフォルトでは、パス ルールがアラート ルールをオーバーライドします。パス ルールを作成することで、アラート ルールを無効にする代わりに、パス ルールで定義された基準を満たすパケットが特定の状況でアラート ルールをトリガーとして使用しないことを指定できます。たとえば、ユーザ "anonymous" として FTP サーバにログインする試行を検索するルールをアクティブのままにする必要があるとします。ただし、1 つ以上の正式な匿名 FTP サーバがネットワークに存在する場合、そのような特定のサーバで匿名ユーザにより最初のルールがトリガーとして使用されないことを指定するパス ルールを作成し、アクティブにすることができます。

侵入ルール エディタで、[アクション（Action）] リストからルール タイプを選択します。

侵入ルール ヘッダー プロトコル

各ルールヘッダーで、ルールにより検査されるトラフィックのプロトコルを指定する必要があります。次のネットワーク プロトコルを分析対象として指定できます。

- ICMP（インターネット制御メッセージ プロトコル）
- IP（インターネット プロトコル）

（注） プロトコルが ip に設定されている場合、システムは侵入ルールヘッダー内のポート定義を無視します。

- 伝送制御プロトコル（TCP）
- UDP（ユーザ データグラム プロトコル）

TCP、UDP、ICMP、IGMP など、IANA によって割り当てられたすべてのプロトコルを検査するには、プロトコル タイプとして **IP** を使用します。

（注） 現在のところ、IP ペイロード内の次のヘッダー（TCP ヘッダーなど）でパターンを照合するルールを作成することはできません。代わりに、最後にデコードされたプロトコルからコンテンツ照合が始まります。次善策として、ルール オプションを使用して TCP ヘッダー内のパターンを照合できます。

侵入ルール エディタで、[プロトコル（Protocol）] リストからプロトコル タイプを選択します。

関連トピック

侵入ルール ヘッダー プロトコル （2140 ページ）

侵入ルール ヘッダーの方向

ルールによる検査対象となるパケットが進むべき方向を、ルールヘッダー内で指定できます。以下の表は、それらのオプションを示しています。

表 *156 :* ルール ヘッダー内の方向オプション

使用するフィルタ	テスト対象
Directional	指定された送信元 IP アドレスから指定された宛先 IP アドレスに向かうトラフィックのみ
Bidirectional	指定された送信元 IP アドレスと宛先 IP アドレスの間を移動するすべてのトラフィック

侵入ルール ヘッダーの送信元と宛先の IP アドレス

パケット検査の対象を、特定の IP アドレスから発信されたパケットまたは特定の IP アドレスに向かうパケットに制限すると、システムが実行しなければならないパケット検査の量が減ります。さらに、ルールをより具体化し、送信元および宛先 IP アドレスが疑わしい動作を示していないパケットに対してルールがトリガーとして使用される可能性をなくすと、誤検出も減ります。

ヒント　システムは IP アドレスのみを認識し、送信元/宛先 IP アドレスのホスト名を受け入れません。

侵入ルール エディタの [送信元 IP（Source IPs）] フィールドと [宛先 IP（Destination IPs）] フィールドで、送信元および宛先の IP アドレスを指定します。

標準テキスト ルールの作成時には、必要に応じて、さまざまな方法で IPv4 アドレスと IPv6 アドレスを指定できます。単一の IP アドレス、any、IP アドレス リスト、CIDR 表記、プレフィクス長、またはネットワーク変数を指定できます。加えて、1 つの特定の IP アドレスまたは IP アドレスのセットを除外するよう指定できます。IPv6 アドレスを指定するときには、RFC 4291 で定義された任意のアドレス指定規則を使用できます。

侵入ルールの IP アドレスの構文

次の表では、送信元と宛先の IP アドレスを指定するさまざまな方法を要約します。

表 *157*：送信元/宛先 *IP* アドレスの構文

指定する項目	指定内容	例
任意の IP アドレス	任意	任意
1 つの特定の IP アドレス	その IP アドレス 同じルール内に IPv4 と IPv6 の送信元アドレスと宛先アドレスを混在させないでください。	192.168.1.1 2001:db8::abcd
IP アドレスのリスト	複数の IP アドレスをカンマで区切り、それを大カッコ（[]）で囲む	[192.168.1.1,192.168.1.15] [2001:db8::b3ff, 2001:db8::0202]
IP アドレスのブロック	IPv4 CIDR ブロックまたは IPv6 アドレス プレフィクス表記	192.168.1.0/24 2001:db8::/32
特定の 1 つの IP アドレスまたはアドレス セットを除くすべて	拒否する IP アドレスの前に付ける「!」記号	!192.168.1.15 !2001:db8::0202:b3ff:fe1e
特定の 1 つ以上の IP アドレスを除く、IP アドレスブロック内のすべて	アドレス ブロックの後に、否定されるアドレスのリストまたはブロック	[10.0.0/8, !10.2.3.4, !10.1.0.0/16] [2001:db8::/32, !2001:db8::8329, !2001:db8::0202]
ネットワーク変数で定義された IP アドレス	$ で始まる大文字の変数名 プリプロセッサルールは、侵入ルールで使われているネットワーク変数で定義されたホストとは無関係に、イベントをトリガーできることに注意してください。	$HOME_NET

指定する項目	指定内容	例
IP アドレス変数で定義されたアドレスを除く、すべての IP アドレス	大文字の変数名の前に `!$` を付ける	`!$HOME_NET`

以下の説明では、いくつかの IP アドレス入力方法に関する追加情報を提供します。

任意の IP アドレス

任意の IPv4 または IPv6 アドレスを示す「`any`」という単語を、ルールの送信元 IP アドレスまたは宛先 IP アドレスとして指定できます。

たとえば、次のルールでは [Source IPs] フィールドと [Destination IPs] フィールドで引数 **any** を使用して、任意の IPv4 または IPv6 の送信元または宛先アドレスを持つパケットを評価します。

```
alert tcp any any -> any any
```

また、任意の IPv6 アドレスを示すために `::` を指定することもできます。

複数の IP アドレス

次の例に示すように、カンマを使って複数の IP アドレスを区切り、オプションで、非拒否リストを大カッコで囲むことにより、個別の IP アドレスを列挙できます。

```
[192.168.1.100,192.168.1.103,192.168.1.105]
```

IPv4 アドレスと IPv6 アドレスのいずれかだけを列挙することも、任意に組み合わせて列挙することもできます（次の例を参照）。

```
[192.168.1.100,2001:db8::1234,192.168.1.105]
```

以前のソフトウェア リリースでは IP アドレス リストを大カッコで囲む必要がありましたが、現在ではこれが必須でないことに注意してください。また、オプションで、リストを入力するときに各カンマの前または後にスペースを含めることができます。

（注） 否定リストは、大カッコで囲む必要があります。

また、IPv4 クラスレス ドメイン間ルーティング（CIDR）表記または IPv6 プレフィクス長を使用してアドレス ブロックを指定することもできます。次に例を示します。

- 192.168.1.0/24 は、サブネット マスク 255.255.255.0 の 192.168.1.0 ネットワーク内の IPv4 アドレス、つまり 192.168.1.0 ～ 192.168.1.255 を指定します。
- 2001:db8::/32 は、プレフィクス長 32 ビットの 2001:db8:: ネットワーク内の IPv6 アドレス、つまり 2001:db8:: ～ 2001:db8:ffff:ffff:ffff:ffff:ffff:ffff を指定します。

ヒント IP アドレスのブロックを指定する必要があるが、CIDR またはプレフィクス長表記を単独で使ってそれを表現できない場合は、1 つの IP アドレス リスト内でいくつかの CIDR ブロックとプレフィクス長を使用できます。

IP アドレスの否定

特定の IP アドレスを否定するために感嘆符（!）を使用できます。つまり、1 つ以上の特定の IP アドレスを除く、すべての IP アドレスに一致させることができます。たとえば、`!192.168.1.1` は 192.168.1.1 以外の任意の IP アドレスを、`!2001:db8:ca2e::fa4c` は 2001:db8:ca2e::fa4c 以外の任意の IP アドレスを指定します。

一連の IP アドレスを拒否するには、大かっこで囲んだ IP アドレスのリストの前に「!」記号を付けます。たとえば、`![192.168.1.1,192.168.1.5]` は 192.168.1.1 と 192.168.1.5 を除くすべての IP アドレスを定義します。

（注） IP アドレスのリストを否定するには、大カッコを使用する必要があります。

否定文字と一緒に IP アドレス リストを使用する場合は注意が必要です。たとえば、192.168.1.1 と 192.168.1.5 を除くすべてのアドレスと一致させるために `[!192.168.1.1,!192.168.1.5]` を使用した場合、システムはこの構文を「192.168.1.1 以外のすべて、**または** 192.168.1.5 以外のすべて」と解釈します。

192.168.1.5 は 192.168.1.1 ではなく、192.168.1.1 は 192.168.1.5 ではないため、この両方の IP アドレスが `[!192.168.1.1,!192.168.1.5]` という IP アドレス値に一致します。つまり、実質的に「`any`」を使用するのと同じです。

代わりに `![192.168.1.1,192.168.1.5]` を使用してください。システムはこの構文を「192.168.1.1 **でなく、しかも** 192.168.1.5 **でない**」と解釈し、大カッコ内に列挙されたものを除くすべての IP アドレスに一致します。

論理的に言って、`any` を除外（negation）と同時に使用できないことに注意してください。any を除外すると「アドレスなし」を意味することになります。

関連トピック

変数セット （538 ページ）

侵入ルール ヘッダーの送信元および宛先ポート

侵入ルール エディタの [送信元ポート（Source Port）] フィールドと [宛先ポート（Destination Port）] フィールドで、送信元および宛先ポートを指定します。

侵入ルールのポート構文

Firepower System では、特定のタイプの構文を使用して、ルール ヘッダーで使用されるポート番号を定義できます。

（注） プロトコルが ip に設定されている場合、システムは侵入ルール ヘッダー内のポート定義を無視します。

次の例に示すように、カンマでポートを区切ることによって、ポートのリストを指定できます。

```
80, 8080, 8138, 8600-9000, !8650-8675
```

オプションで、次の例に示すように、ポートリストを大カッコで囲むこともできます（以前のソフトウェア バージョンではこれが必須でしたが、現在は必須ではありません）。

```
[80, 8080, 8138, 8600-9000, !8650-8675]
```

なお、次の例に示すように、ポートリストの否定を大カッコで囲む**必要がある**ことに注意してください。

```
![20, 22, 23]
```

次の表に、使用可能な構文を要約します。

表 *158* : 送信元/宛先ポート構文

指定する項目	指定内容	例
任意のポート	任意	任意
1 つの特定のポート	そのポート番号	80
ポートの範囲	範囲内の最初のポート番号と最後のポート番号をダッシュでつなぐ	80-443
1 つの特定のポートに等しい、またはより小さいすべてのポート	ポート番号の前にダッシュを付ける	-21
1 つの特定のポートに等しい、またはより大きいすべてのポート	ポート番号の後ろにダッシュを付ける	80-
1 つの特定のポートまたはポート範囲を除く、すべてのポート	否定する場合には、ポート、ポート リスト、ポート範囲の前に文字 ! を付けます。 否定が「ポートなし」を示す場合を除いて、すべてのポート宛先に論理上、否定を使用できる点にご注意ください。	!20
ポート変数で定義されるすべてのポート	$ の後ろに英大文字の変数名	$HTTP_PORTS
ポート変数で定義されるポートを除く、すべてのポート	大文字の変数名の前に !$ を付ける	!$HTTP_PORTS

侵入イベント詳細

標準のテキストルールを作成するときには、ルールでエクスプロイト試行を検出する対象となる脆弱性についてのコンテキスト情報を含めることができます。また、脆弱性データベースへの外部参照を含めたり、組織内でイベントに設定するプライオリティを定義したりすることもできます。アナリストがイベントを認識すると、そのプライオリティ、エクスプロイト、および既知の対策についての情報をすぐに入手できます。

メッセージ

ルールのトリガー時にメッセージとして表示される、意味のあるテキストを指定できます。メッセージを読むと、ルールで攻撃試行を検出する対象となった脆弱性の特性をすぐに理解できます。中カッコ（{}）を除く、印字可能な任意の標準ASCII文字を使用できます。システムは、メッセージ全体を囲んでいる引用符を取り除きます。

ヒント　ルール メッセージの指定は必須です。また、空白文字のみ、1 つ以上の引用符のみ、1 つ以上のアポストロフィのみ、あるいは空白文字/引用符/アポストロフィだけの組み合わせでメッセージを構成することはできません。

侵入ルール エディタでイベント メッセージを定義するには、[メッセージ（Message）] フィールドにイベント メッセージを入力します。

分類

ルールごとに、イベントのパケット表示に含める攻撃分類を指定できます。次の表に、それぞれの分類の名前と番号を示します。

表 *159 :* ルールの分類

番号	分類名	説明
1	not-suspicious	不審ではないトラフィック
2	unknown	不明なトラフィック
3	bad-unknown	有害な可能性のあるトラフィック
4	attempted-recon	情報漏えいが試行された
5	successful-recon-limited	情報漏えいが発生
6	successful-recon-largescale	大規模な情報漏えい
7	attempted-dos	サービス拒否が試行された
8	successful-dos	サービス拒否が発生
9	attempted-user	ユーザ特権の獲得が試行された

番号	分類名	説明
10	unsuccessful-user	ユーザ特権の獲得が失敗した
11	successful-user	ユーザ特権の獲得に成功
12	attempted-admin	管理者特権の獲得が試行された
13	successful-admin	管理者特権の獲得に成功
14	rpc-portmap-decode	RPC クエリのデコード
15	shellcode-detect	実行可能コードが検出された
16	string-detect	疑わしい文字列が検出された
17	suspicious-filename-detect	疑わしいファイル名が検出された
18	suspicious-login	疑わしいユーザ名を使用したログイン試行が検出された
19	system-call-detect	システム コールが検出された
20	tcp-connection	TCP 接続が検出された
21	trojan-activity	ネットワーク トロイの木馬が検出された
22	unusual-client-port-connection	通常とは異なるポートをクライアントが使用していた
23	network-scan	ネットワーク スキャンの検出
24	denial-of-service	サービス拒否攻撃の検出
25	non-standard-protocol	標準的でないプロトコルまたはイベントの検出
26	protocol-command-decode	一般的なプロトコル コマンド デコード
27	web-application-activity	脆弱な可能性のある Web アプリケーションへのアクセス
28	web-application-attack	Web アプリケーション攻撃
29	misc-activity	その他のアクティビティ
30	misc-attack	その他の攻撃
31	icmp-event	一般的な ICMP イベント
32	inappropriate-content	不適切な内容が検出された

番号	分類名	説明
33	policy-violation	企業プライバシー侵害の可能性
34	default-login-attempt	デフォルトのユーザ名とパスワードによるログイン試行
35	sdf	機密データ
36	malware-cnc	既知のマルウェア コマンドと制御トラフィック
37	client-side-exploit	既知のクライアント側 exploit 試行
38	file-format	既知の有害ファイルまたはファイル ベースの exploit

カスタム分類

定義したルールによって生成されるイベントのパケット表示記述の内容をもっとカスタマイズする必要がある場合には、カスタム分類を作成できます。

引数	説明
分類名	分類の名前。40 文字を超える文字を使用すると、ページが読みにくくなります。`<>()\'"&$;` 文字および空白文字はサポートされていません。
分類の説明	分類の説明。英数字とスペースを使用できます。`<>()\'"&$;` 文字はサポートされていません。
[プライオリティ（Priority）]	[高（High）]、[中（medium）]、または [低（low）]。

カスタム プライオリティ

デフォルトでは、ルールのイベント分類からルールのプライオリティが派生します。ただし、`priority` キーワードをルールに追加し、高、中、または低のプライオリティを選択することで、ルールの分類優先度を上書きすることができます。たとえば、Webアプリケーション攻撃を検出するルールに高プライオリティを割り当てるには、`priority`キーワードをルールに追加して、プライオリティとして [高（high）] を選択します。

カスタム参照

`reference` キーワードを使用すると、イベントに関する外部 Web サイトや追加情報への参照を追加できます。参照を追加すると、アナリストは参照情報をすぐに利用できるため、パケットがルールをトリガーとして使用した理由を特定するのに役立ちます。次の表に、既知のエクスプロイトや攻撃についてのデータを提供する外部システムをいくつか示します。

表 *160 :* 外部攻撃識別システム

システム ID	説明	ID の例
`bugtraq`	[Bugtraq] ページ	`8550`
`cve`	[Common Vulnerabilities and Exposure] ページ	`CAN-2003-0702`
`mcafee`	[McAfee] ページ	`98574`
`url`	Web サイト参照	`www.example.com?exploit=14`
`msb`	Microsoft セキュリティ情報	`MS11-082`
`nessus`	[Nessus] ページ	`10039`
`secure-url`	セキュア Web サイト参照（https://...）	`intranet/exploits/exploit=14` 任意のセキュア Web サイトで `secure-url` を使用できることに注意してください。

次のように、参照値を入力して参照を指定します。

```
id_system,id
```

ここで、id_system はプレフィックスとして使用されるシステム、id は Bugtraq ID、CVE 番号、Arachnids ID、または URL（`http://`なし）です。

たとえば、Bugtraq ID 17134 に記載されている Microsoft Commerce Server 2002 サーバ上の認証バイパス脆弱性を指定するには、次の値を入力します。

```
bugtraq,17134
```

参照をルールに追加するときには、次の点に注意してください。

- カンマの後ろにスペースを入力しないでください。
- システム ID に大文字を使用しないでください。

関連トピック

カスタム分類の追加 （2150 ページ）
イベント優先順位の定義 （2150 ページ）
イベント参照の定義 （2151 ページ）

カスタム分類の追加

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Intrusion Admin

マルチドメイン展開では、現在のドメインで作成されたカスタム分類がシステムで表示されます。これらの分類には、優先度を設定できます。先祖ドメインで作成されたカスタム分類も表示されますが、これらの分類には優先度は設定できません。下位のドメインで作成されたカスタム分類を表示および編集するには、そのドメインに切り替えます。

ステップ 1 ルールの作成または編集時に、[分類（Classification）] ドロップダウン リストから [分類の編集（Edit Classifications）] を選択します。

代わりに [分類の表示（View Classifications）] が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 2 侵入イベント詳細 （2146 ページ） の説明に従い、[分類名（Classification Name）] と [分類の説明（Classification Description）] を入力します。

ステップ 3 [優先度（Priority）] ドロップダウン リストから分類の優先度を選択します。

ステップ 4 [追加（Add）] をクリックします。

ステップ 5 [完了（Done）] をクリックします。

次のタスク

- ルールの作成または編集を続けます。詳細については、新規ルールの作成 （2153 ページ） または 既存のルールの変更 （2154 ページ） を参照してください。

関連トピック

カスタム ルールの作成 （2151 ページ）

イベント優先順位の定義

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Intrusion Admin

ステップ 1 ルールの作成または編集時に、[検出オプション（Detection Options）] ドロップダウン リストから [優先順位（priority）] を選択します。

ステップ 2 [Add Option] をクリックします。

ステップ 3 [優先順位（priority）] ドロップダウン リストから値を選択します。

ステップ 4 [保存（Save）] をクリックします。

次のタスク

- ルールの作成または編集を続けます。詳細については、新規ルールの作成 （2153 ページ）または 既存のルールの変更 （2154 ページ） を参照してください。

関連トピック

カスタム ルールの作成 （2151 ページ）

イベント参照の定義

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Intrusion Admin

ステップ 1 ルールの作成または編集時に、[検出オプション（Detection Options）] ドロップダウン リストから [参照（reference）] を選択します。

ステップ 2 [Add Option] をクリックします。

ステップ 3 侵入イベント詳細 （2146 ページ）の説明に従って、[参照（reference）] フィールドに値を入力します。

ステップ 4 [保存（Save）] をクリックします。

次のタスク

- ルールの作成または編集を続けます。詳細については、新規ルールの作成 （2153 ページ）または 既存のルールの変更 （2154 ページ） を参照してください。

関連トピック

カスタム ルールの作成 （2151 ページ）

カスタム ルールの作成

カスタム侵入ルールは以下の方法で作成できます。

- 独自の標準テキスト ルールを作成する
- 既存の標準テキスト ルールを新規ルールとして保存する
- システムが提供する共有オブジェクト ルールを新規ルールとして保存する

- 先祖ルールを子孫ドメインにおける新規ルールとして保存する（マルチドメイン展開の場合）
- ローカル ルール ファイルをインポートする

作成方法に関わらず、システムはカスタム ルールをローカル ルールに分類して保存します。

カスタム侵入ルールを作成すると、システムは一意のルール番号（番号の形式は`GID:SID:Rev`）を割り当てます。この番号には次の要素が含まれます。

GID

ジェネレータ ID。すべての標準テキスト ルールでは、この値は 1（グローバル ドメインまたはレガシー GID）または 1000 ～ 2000（子孫ドメイン）です。共有オブジェクト ルールを新規ルールとして保存する場合、値は 1 です。

SID

[Snort ID]。ルールがシステム ルールのローカル ルールであるかどうかを示します。新しいルールを作成すると、システムは次に使用可能なローカル ルール SID 番号を割り当てます。

ローカル ルールの SID 番号は 1000000 から始まり、新しいローカル ルールにつき番号が 1 ずつ増えます。

Rev

改訂番号。新しいルールのリビジョン番号は 1 です。カスタム ルールを変更するたびに、リビジョン番号が 1 ずつ増えます。

カスタム標準テキスト ルールでは、ルール ヘッダー設定、ルール キーワード、およびルール引数を設定できます。特定のプロトコルを使用する、特定の IP アドレスまたはポートを行き来するトラフィックだけをルールで照合するよう、ルール ヘッダーを設定できます。

システムが提供する標準テキスト ルールまたは共有オブジェクト ルールのカスタム ルールで変更できるルール ヘッダー情報は、送信元と宛先ポートと IP アドレスなどの情報に限られます。ルール キーワードやルール引数は変更できません。

共有オブジェクト ルールのヘッダー情報を変更して変更内容を保存すると、ルールの新しいインスタンスが作成され、ジェネレータ ID（GID） 1（グローバル ドメイン）または 1000 ～ 2000（子孫ドメイン）、およびカスタム ルールとして次に使用可能な SID が割り当てられます。システムは、共有オブジェクト ルールの新しいインスタンスを予約済み `soid` キーワードにリンクします。これにより、新しく作成したルールが Cisco Talos Intelligence Group（Talos）作成のルールにマップされます。ユーザが作成した共有オブジェクト ルールのインスタンスは削除できますが、Talos が作成した共有オブジェクト ルールは削除できません。

新規ルールの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Intrusion Admin

ステップ 1 次のいずれかの方法を使用して侵入ルールにアクセスします。

- **[Policies]** > **[Access Control]** > **[Intrusion]** を選択し、[侵入ルール（Intrusion Rules）] をクリックします。
- **[Objects]** > **[Intrusion Rules]**を選択します。

ステップ 2 [Create Rule] をクリックします。

ステップ 3 [メッセージ（Message）] フィールドに値を入力します。

ステップ 4 次の各ドロップダウン リストから値を選択します。

- **[分類（Classification）]**
- **操作**
- **[Protocol]**
- **方向（Direction）**

ステップ 5 次のフィールドに値を入力します。

- **[送信元 IP（Source IPs）]**
- **[宛先 IP（Destination IPs）]**
- **送信元ポート**
- **宛先ポート**

これらのフィールドに値を指定しない場合、システムは値 [すべて（any）] を使用します。

（注） システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。

ステップ 6 [検出オプション（Detection Options）] ドロップダウン リストから値を選択します。

ステップ 7 [Add Option] をクリックします。

ステップ 8 追加したキーワードの引数を入力します。

ステップ 9 必要に応じて、手順 6 ～ 8 を繰り返します。

ステップ 10 複数のキーワードを追加した場合、以下を実行できます。

- キーワードの並べ替え：移動するキーワードの横にある上矢印または下矢印をクリックします。
- キーワードの削除：そのキーワードの横にある [X] をクリックします。

ステップ 11 [新規として保存（Save As New）] をクリックします。

次のタスク

- 該当する侵入ポリシー内の新規または変更されたルールを有効にします（侵入ポリシー内の侵入ルールの表示 （2075 ページ）を参照）。
- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

既存のルールの変更

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Intrusion Admin

カスタム侵入ルールは変更できます。マルチドメイン展開では、現在のドメインに属しているカスタム侵入ルールのみを変更できます。

システム提供のルールと先祖ドメインに属しているルールは、新しいカスタム ルールとしてローカル ルール カテゴリに保存してから変更できます。

ステップ 1 次のいずれかの方法を使用して侵入ルールにアクセスします。

- **[Policies]** > **[Access Control]** > **[Intrusion]** を選択し、[侵入ルール（Intrusion Rules）] をクリックします。
- **[Objects]** > **[Intrusion Rules]** を選択します。

ステップ 2 変更するルールを見つけます。次の選択肢があります。

- フォルダからルールに移動します。
- ルールを探します。ルールの検索 （2158 ページ） を参照してください。
- ルールが属しているグループにフィルタを適用します。フィルタリング ルール （2163 ページ）を参照してください。

ステップ 3 ルールの横にある編集アイコン（  ）をクリックします。検索結果の場合はルール メッセージをクリックします。

代わりに表示アイコン（  ）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 4 ルール タイプに応じて、ルールを変更します。

（注） 共有オブジェクト ルールのプロトコルは変更しないでください。これを変更すると、ルールの効果がなくなる可能性があります。

ステップ 5 次の選択肢があります。

- カスタム ルールを編集していて、そのルールの現在のバージョンを上書きする場合は、[保存（Save）] をクリックします。
- システム提供のルールまたは先祖ドメインに属しているルールを編集している場合や、カスタム ルールを編集しているときに変更を新しいルールとして保存する場合は、[新規に保存（Save As New）] をクリックします。

次のタスク

- システム提供のルールの代わりにローカルで変更したルールを使用するには、侵入ルールの状態（2092 ページ）の手順に従ってシステム提供のルールを非アクティブ化してから、ローカル ルールをアクティブ化します。
- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

関連トピック

ルールの検索 （2158 ページ）
侵入ルール エディタ ページでのルールのフィルタリング （2160 ページ）

ルール ドキュメンテーションの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Intrusion Admin

[ルールの編集（Rule Edit）] ページから、Cisco Talos Intelligence Group（Talos） によって提供されるルール ドキュメンテーションを表示できます。表示中に、[ルール ドキュメンテーション（Rule Documentation）] およびその他の外部参照をクリックして、Talos によって提供される追加情報を表示できます。[コンテキスト エクスプローラ（Context Explorer）] をクリックして、ルールによって生成されたイベントのコンテキスト情報を表示することもできます。

ステップ 1 次のいずれかの方法を使用して侵入ルールにアクセスします。

- **[Policies]** > **[Access Control]** > **[Intrusion]** を選択し、[侵入ルール（Intrusion Rules）] をクリックします。
- **[Objects]** > **[Intrusion Rules]** を選択します。

ステップ 2 表示するルールを探します。次の選択肢があります。

- フォルダからルールに移動します。
- ルールを探します。ルールの検索 （2158 ページ） を参照してください。
- ルールが属しているグループにフィルタを適用します。フィルタリング ルール （2163 ページ）を参照してください。

ステップ 3 ルールの横にある編集アイコン（）をクリックします。検索結果の場合はルール メッセージをクリックします。

代わりに表示アイコン（  ）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 4 [ドキュメントの表示（View Documentation）] をクリックします。

ステップ 5 状況に応じて、次のいずれかのリンクをクリックします。

- [ルール ドキュメンテーション（Rule Documentation）]：ルール固有の詳細を表示します。
- [その他の外部参照（Other external references）]：利用可能な外部参照に関する情報については、キーワードフィルタリング （2161 ページ）および侵入イベント詳細 （2146 ページ）の「カスタム リファレンス」を参照してください。
- [コンテキスト エクスプローラ（Context Explorer）]：コンテキスト エクスプローラでのルールのコンテクスチュアル データの表示に関する情報については、[侵入情報（Intrusion Information）] セクション （2837 ページ）を参照してください。

ヒント 外部リンクを選択するとドキュメンテーションのポップアップ ウィンドウが閉じます。ルールを変更せずにルール編集ページを終了するには、任意のメニュー パスを選択します。

侵入ルールへのコメントの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Intrusion Admin

任意の侵入ルールにコメントを追加できます。コメントにより、環境や条件の説明と、ルールやルールが検出する悪意あるプログラム、スクリプト（エクスプロイト）やポリシー違反の詳細を示すことができます。

マルチドメイン展開では、現在のドメインで作成されたコメントが表示されます。これは削除できます。先祖ドメインで作成されたコメントも表示されますが、これは削除できません。下位のドメインで作成されたコメントを表示するには、そのドメインに切り替えます。

ステップ 1 次のいずれかの方法を使用して侵入ルールにアクセスします。

- **[Policies]** > **[Access Control]** > **[Intrusion]** を選択し、[侵入ルール（Intrusion Rules）] をクリックします。
- **[Objects]** > **[Intrusion Rules]** を選択します。

ステップ 2 注釈を付けるルールを探します。次の選択肢があります。

- フォルダからルールに移動します。
- ルールを探します。ルールの検索 （2158 ページ） を参照してください。

- ルールが属するグループをフィルタします。フィルタリング ルール （2163 ページ） を参照してください。

ステップ 3 ルールの横にある編集アイコン（  ）をクリックします。検索結果の場合はルール メッセージをクリックします。

代わりに表示アイコン（  ）がルールの横に表示される場合、ルールは先祖ポリシーに属しており、ルールを変更する権限がありません。

ステップ 4 [Rule Comment] をクリックします。

ステップ 5 テキスト ボックスにコメントを入力します。

ステップ 6 [コメントを追加（Add a Comment）] をクリックします。

ヒント また、侵入イベントのパケット ビューで、ルール コメントを追加して表示することもできます。

次のタスク

- ルールの作成または編集を続けます。詳細については、新規ルールの作成 （2153 ページ） または 既存のルールの変更 （2154 ページ） を参照してください。

関連トピック

ルールの検索 （2158 ページ）
イベント情報のフィールド （3086 ページ）

カスタム ルールの削除

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Intrusion Admin

侵入ポリシーで現在有効になっていないカスタム ルールを削除することができます。システムにより提供されている標準テキスト ルールおよび共有オブジェクト ルールは削除できません。マルチドメイン導入では、現在のドメインで作成されたローカル ルールのみを削除できます。

削除されたルールは削除済みカテゴリに保存されます。削除済みのルールを、新しいルールの基準として使用することができます。侵入ポリシーの [Rules] ページには削除済みカテゴリが表示されないため、削除したカスタム ルールを有効にすることはできません。

ヒント　カスタム ルールには、変更されたヘッダー情報で保存する共有オブジェクト ルールが含まれます。また、これらはローカル ルール カテゴリに保存され、1（グローバル ドメインまたはレガシー GID）または 1000 ～ 2000（子孫ドメイン）の GID を使用してリストされます。変更した共有オブジェクト ルールは削除できますが、元の共有オブジェクト ルールは削除できません。

ステップ 1　次のいずれかの方法を使用して侵入ルールにアクセスします。

- **[Policies]** > **[Access Control]** > **[Intrusion]** を選択し、[侵入ルール（Intrusion Rules）] をクリックします。
- **[Objects]** > **[Intrusion Rules]**を選択します。

ステップ 2　次の 2 つの選択肢があります。

- すべてのローカル ルールを削除します：[ローカル ルールの削除（Delete Local Rules）] をクリックし、[OK] をクリックします。
- 1 つのルールを削除します：[ルールのグループ化基準（Group Rules By）] ドロップダウンから [ローカル ルール（Local Rules）] を選択し、削除するルールの隣にある削除アイコン（）をクリックし、[OK] をクリックして削除を確認します。

関連トピック

侵入ルールの状態 （2092 ページ）

ルールの検索

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Intrusion Admin

Firepower システムには、数千もの標準テキスト ルールが用意されています。また、Cisco Talos Intelligence Group（Talos） は新しい脆弱性およびエクスプロイトが見つかったときのルールを追加を継続します。特定のルールを簡単に検索して、そのルールをアクティブ化、非アクティブ化、または編集することができます。

ステップ 1　次のいずれかの方法を使用して侵入ルールにアクセスします。

- **[Policies]** > **[Access Control]** > **[Intrusion]** を選択し、[侵入ルール（Intrusion Rules）] をクリックします。
- **[Objects]** > **[Intrusion Rules]**を選択します。

ステップ 2　ツールバーで [検索（Search）] をクリックします。

ステップ 3 検索条件を追加します。

ステップ 4 [検索（Search）] をクリックします。

次のタスク

- 見つかったルール（システム ルールの場合はルールのコピー）を表示または編集する場合は、ハイパーリンクが付いたルール メッセージをクリックします。詳細については、新規ルールの作成（2153 ページ）または既存のルールの変更（2154 ページ）を参照してください。

侵入ルールの検索条件

次の表には、利用可能な検索オプションについて説明しています。

表 *161* : ルール検索規則

オプション	説明
署名 ID	[Snort ID]（SID）に基づいて 1 つのルールを検索するには、SID 番号を入力します。複数のルールを検索するには、SID 番号リストをカンマで区切って入力します。このフィールドは、80 文字以内です。
ジェネレータ ID	標準テキスト ルールを検索するには、[1] を選択します。共有オブジェクトのルールを検索するには、[3] を選択します。
メッセージ	特定のメッセージを含むルールを検索するには、ルール メッセージの 1 つの単語を [Message] フィールドに入力します。たとえば、DNS exploit を検索するには「`DNS`」と入力し、バッファ オーバーフロー exploit を検索するには「`overflow`」と入力します。
Protocol	特定のプロトコルのトラフィックを評価するルールを検索には、プロトコルを選択します。プロトコルを選択しない場合、検索結果にはすべてのプロトコルのルールが含まれます。
送信元ポート	指定したポートから送信されたパケットを検査するルールを検索するには、送信元ポート番号またはポート関連変数を入力します。
宛先ポート	特定のポートに向けて送られるパケットを検査するルールを検索するには、宛先ポート番号またはポート関連変数を入力します。
送信元 IP	指定した IP アドレスから送信されたパケットを検査するルールを検索するには、送信元 IP アドレスまたは IP アドレス関連の変数を入力します。
宛先 IP	指定した IP アドレスに向けて送られるパケットを検査するルールを検索するには、宛先 IP アドレスまたは IP アドレス関連の変数を入力します。

オプション	説明
キーワード	特定のキーワードを検索するには、キーワード検索オプションを使用できます。キーワードを選択して、検索するキーワード値を入力します。特定値以外の任意の値に一致させるには、キーワードの前に疑問符（!）を入力します。
Category	特定のカテゴリ内のルールを検索するには、[Category] リストからカテゴリを選択します。
Classification	特定の分類が設定されたルールを検索するには、[Classification] リストから分類名を選択します。
Rule State	特定のポリシー内のルールや特定のルール状態を検索するには、最初のルール状態リストからポリシーを選択し、第2のリストから状態を選択して、イベントの作成、イベントのドロップ、作成、無効に設定されたルールを検索します。

侵入ルールエディタページでのルールのフィルタリング

侵入ルール エディタ ページ上でルールをフィルタリングして、ルールのサブセットを表示することができます。たとえば、あるルールまたはその状態を変更したいが、数千ものルールの中からそれを見つけるのが困難な場合に、この機能が役立つことがあります。

フィルタを入力すると、1 つ以上の一致するルールを含むフォルダがページに表示され、一致するルールがない場合はメッセージが表示されます。

フィルタリング ガイドライン

フィルタには、特殊なキーワードとその引数、文字列、引用符で囲んだリテラル文字列、さらに複数のフィルタ条件を区切るスペースを含めることができます。ただし、正規表現、ワイルドカード文字、および否定文字（!）、「大なり」記号（>）、「小なり」記号（<）などの特殊な演算子をフィルタに含めることはできません。

キーワード、キーワード引数、および文字列では、いずれも大文字と小文字が区別されません。`gid` キーワードと `sid` キーワードを除き、すべての引数と文字列は部分的な文字列として扱われます。`gid` と `sid` の引数は、完全一致のみを返します。

フィルタ処理前の元のページで 1 つのフォルダを展開すると、その後のフィルタ処理でそのフォルダ内の一致が返されるときにフォルダが展開したままになります。探しているルールが多数のルールを含むフォルダ内に存在する場合には、これが役立つことがあります。

1 つのフィルタを後続の別のフィルタで制約することはできません。入力されたすべてのフィルタが、ルールデータベース全体を検索して、一致するすべてのルールを返します。ページに前回のフィルタ結果が表示されている状態でフィルタを入力すると、ページが消去され、代わりに新しいフィルタの結果が返されます。

フィルタ処理されている場合もされていない場合も、リスト内のルールで同じ機能を使用できます。たとえば、侵入ルール エディタ ページでは、リストがフィルタ処理されているかどう

かに関わらず、リスト内のルールを編集できます。また、ページのコンテキスト メニューの任意のオプションを使用することもできます。

ヒント すべてのサブグループ内のルールの合計数が多い場合は、フィルタリングに長い時間がかかることがあります。これは、個別のルールの数がかなり少なくても、1 つのルールが複数のカテゴリに出現することがあるためです。

キーワード フィルタリング

各ルール フィルタに、次の形式で 1 つ以上のキーワードを含めることができます。

```
keyword:argument
```

ここで、keyword は次の表のいずれかのキーワード、argument はキーワードに関連する特定のフィールドで検索される単一の、大文字/小文字を区別しない英数字文字列です。

`gid` と `sid` を除くすべてのキーワードの引数が部分文字列として扱われます。たとえば、引数 `123` によって `"12345"`、`"41235"`、`"45123"` などが返されます。`gid` と `sid` の引数は完全一致のみを返します。たとえば、`sid:3080` によって SID 3080 のみが返されます。

ヒント 部分的な SID を検索するには、1 つ以上の文字列を使ってフィルタ処理できます。

次の表に、ルールのフィルタ処理に使用できる特定のフィルタリング キーワードと引数を示します。

表 *162:* ルール フィルタ キーワード

キーワード	説明	例
`arachnids`	ルール参照内の Arachnids ID 全体またはその一部分に基づいて 1 つ以上のルールを返します。	`arachnids:181`
`bugtraq`	ルール参照内の Bugtraq ID 全体またはその一部分に基づいて 1 つ以上のルールを返します。	`bugtraq:2120`
`cve`	ルール参照内の CVE 番号全体またはその一部分に基づいて 1 つ以上のルールを返します。	`cve:2003-0109`
`gid`	引数 `1` は標準のテキスト ルールを返します。引数 `3` は共有オブジェクト ルールを返します。	`gid:3`
`mcafee`	ルール参照内の McAfee ID 全体またはその一部分に基づいて 1 つ以上のルールを返します。	`mcafee:10566`

キーワード	説明	例
msg	ルールの [メッセージ（Message）] フィールド（イベント メッセージとも呼ばれる）の全体またはその一部分に基づいて 1 つ以上のルールを返します。	msg:chat
nessus	ルール参照内の Nessus ID 全体またはその一部分に基づいて 1 つ以上のルールを返します。	nessus:10737
ref	ルール参照内またはルールの [メッセージ（Message）] フィールド内の単一の英数字文字列の全体または一部分に基づいて、1 つ以上のルールを返します。	ref:MS03-039
sid	正確な [Snort ID] を持つルールを返します。	sid:235
url	ルール参照内の URL 全体またはその一部分に基づいて 1 つ以上のルールを返します。	url:faqs.org

関連トピック

イベント参照の定義 （2151 ページ）
侵入イベント詳細 （2146 ページ）
プリプロセッサのジェネレータ ID （3076 ページ）

文字列フィルタリング

各ルール フィルタに 1 つ以上の英数字文字列を含めることができます。文字列により、ルールの [メッセージ（Message）] フィールド、[Snort ID] ID（SID）、およびジェネレータ ID が検索されます。たとえば、文字列 `123` を指定すると、ルール メッセージ内の文字列「`Lotus123`」や「`123mania`」などが返され、さらに、SID 6123、SID 12375 なども返されます。

すべての文字列では大文字と小文字が区別されず、部分的な文字列として扱われます。たとえば、文字列 `ADMIN`、`admin`、または `Admin` はすべて、「`admin`」、「`CFADMIN`」、「`Administrator`」などを返します。

文字列を引用符で囲むと、完全一致を返すことができます。たとえば、引用符付きのリテラル文字列 `"overflow attempt"` は完全一致のみを返しますが、引用符なしの 2 つの文字列 `overflow` と `attempt` で構成されるフィルタは `"overflow attempt"`、`"overflow multipacket attempt"`、`"overflow with evasion attempt"` などを返します。

関連トピック

侵入イベント詳細 （2146 ページ）
プリプロセッサのジェネレータ ID （3076 ページ）

キーワードと文字列の組み合わせによるフィルタリング

複数のキーワード、文字列、またはその両方をスペースで区切って任意に組み合わせて入力することで、フィルタ結果を絞り込むことができます。結果には、すべてのフィルタ条件に一致するルールが含まれます。

複数のフィルタ条件を任意の順序で入力できます。たとえば、次のフィルタはそれぞれ同じルールを返します。

- `url:at login attempt cve:200`
- `login attempt cve:200 url:at`
- `login cve:200 attempt url:at`

フィルタリング ルール

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Intrusion Admin

[侵入ルール（Intrusion Rules）]ページで、ルールをサブセットにフィルタ処理すると、より簡単に特定のルールを見つけることができます。その後で、いずれかのページ機能を使用できます。これには、コンテキスト メニューで使用可能な機能の選択も含まれます。

編集する特定のルールを見つけるのに、規則のフィルタリングはとても役立ちます。

ステップ 1 次のいずれかの方法を使用して侵入ルールにアクセスします。

- **[Policies]** > **[Access Control]** > **[Intrusion]** を選択し、[侵入ルール（Intrusion Rules）] をクリックします。
- **[Objects]** > **[Intrusion Rules]**を選択します。

ステップ 2 フィルタリングする前に、次の選択を行います。

- 該当のルール グループを展開します。複数のルール グループにも、展開できるサブグループがあります。

  また、ルールがどのグループに含まれているか予想できる場合は、フィルタ処理前の元のページでそのグループを展開しておくと便利な場合があります。その後のフィルタ処理でそのフォルダ内の一致した結果が返されるとき、およびフィルタ消去アイコン（ ）をクリックしてフィルタ処理前のページに戻ったときに、グループが展開されたままになります。

- [グループ ルール（Group Rules By）] ドロップダウンリストから別のグループ メソッドを選択します。

ステップ 3 [グループ ルール（Group Rules By）] リストでフィルタ アイコン（ ）の横にあるテキスト ボックスにフィルタ制約を入力します。

ステップ 4 Enter を押します。

（注） フィルタ クリア アイコン（ ）をクリックして、現在のフィルタ処理されたリストをクリアします。

侵入ルールのキーワードと引数

ルール言語では、キーワードを組み合わせることによってルールの動作を指定できます。キーワードとそれに関連する値（引数と呼ばれる）は、ルールエンジンによって検査されるパケットおよびパケット関連値をシステムがどのように評価するかを決定します。Firepower システムでは現在、コンテンツマッチング、プロトコル固有のパターンマッチング、状態固有のマッチングなどのインスペクション機能を実行するためのキーワードがサポートされています。キーワードあたり最大100個の引数を定義し、互換性のある任意の数のキーワードを組み合わせて非常に具体的なルールを作成できます。これにより、誤検出や検出漏れの可能性が減少し、受け取った侵入情報に集中的に取り組むことができます。

また、パッシブ展開でアダプティブ プロファイルの更新を使用すると、ルール メタデータとホスト情報に基づいて特定のパケットに対するアクティブルール処理を動的に調整できます。

ここに記載されているキーワードは、ルールエディタの検出オプションとして表示されます。

関連トピック

アダプティブ プロファイルについて （2463 ページ）

content キーワードと protected_content キーワード

`content` キーワードまたは `protected_content` キーワードを使用すると、パケット内から検出するコンテンツを指定できます。

ほとんどの場合、`content` または `protected_content` キーワードの後ろに修飾子を付けて、コンテンツを検索すべき場所、検索で大文字/小文字を区別するかどうか、およびその他のオプションを指定する必要があります。

ルールでイベントがトリガーとして使用されるためには、すべてのコンテンツマッチングが真でなければならないことに注意してください。つまり、各コンテンツマッチングは相互にAND関係にあります。

また、インライン展開では、有害なコンテンツを照合した後でそれを同じ長さの独自のテキスト文字列に置き換えるルールをセットアップできることにも注意してください。

content

`content` キーワードを使用すると、ルールエンジンはパケットペイロードまたはストリームでその文字列を検索します。たとえば、いずれかの `content` キーワードの値として `/bin/sh` と入力した場合、ルール エンジンはパケット ペイロード内で文字列 `/bin/sh` を検索します。

ASCII 文字列、16 進コンテンツ（バイナリ バイト コード）、またはその両方の組み合わせを使用してコンテンツを照合できます。キーワード値の中で 16 進コンテンツをパイプ文字（|）で囲みます。たとえば、`|90C8 C0FF FFFF|/bin/sh` のように 16 進コンテンツと ASCII コンテンツを混在させることができます。

1 つのルール内で複数のコンテンツ マッチングを指定できます。これを行うには、`content` キーワードの追加のインスタンスを使用します。コンテンツ マッチングごとに、ルールをトリガーとして使用させるにはパケット ペイロードまたはストリームでコンテンツ一致が見つからなければならないことを指定できます。

注意 **Not** オプションが選択された 1 つの `content` キーワードだけを含むルールを作成した場合、侵入ポリシーの効果がなくなる可能性があります。

protected_content

`protected_content` キーワードを使用すると、ルール引数を設定する前に、検索コンテンツ文字列をエンコードすることができます。キーワードを設定する前に、ルール作成者がハッシュ関数（SHA-512、SHA-256、または MD5）を使用して文字列をエンコードします。

`content` キーワードの代わりに `protected_content` キーワードを使用した場合でも、ルール エンジンがパケット ペイロードまたはストリームの中で文字列を検索する方法に違いはなく、ほとんどのキーワード オプションが想定どおりに機能します。次の表は、`protected_content` キーワード オプションと `content` キーワード オプションの間の例外的な相違点を要約しています。

表 *163 : protected_content* オプションの例外

オプション	説明
Hash Type	`protected_content` ルール キーワードの新しいオプション。
[大文字小文字の区別なし（Case Insensitive）]	サポート対象外
Within	サポート対象外
Depth	サポート対象外
Length	`protected_content` ルール キーワードの新しいオプション。
高速パターンマッチ機能を使用（Use Fast Pattern Matcher）	サポート対象外
Fast Pattern Matcher Only	サポート対象外
Fast Pattern Matcher Offset and Length	未サポート

Cisco では、protected_content キーワードを含むルールに 1 つ以上の content キーワードを含めることを推奨しています。こうすると、ルール エンジンが常に高速パターン マッチ機能を使用することで処理速度が上がり、パフォーマンスが向上します。ルール内の protected_content キーワードの前に content キーワードを配置します。ルールに 1 つ以上の content キーワードが含まれている場合は、content キーワードの Use Fast Pattern Matcher 引数が有効になっているかどうかに関係なく、ルール エンジンが高速パターン マッチ機能を使用することに注意してください。

注意 **Not** オプションが選択された 1 つの protected_content キーワードだけを含むルールを作成した場合、侵入ポリシーの効果がなくなる可能性があります。

関連トピック

カスタム ルールの作成 （2151 ページ）
基本コンテンツおよび protected_content キーワードの引数 （2166 ページ）
replace キーワード （2178 ページ）

基本コンテンツおよび protected_content キーワードの引数

content または protected_content キーワードを変更するパラメータを使用すると、コンテンツ検索の位置や大文字/小文字の区別を制約できます。content または protected_content キーワードを変更するオプションを設定して、検索対象となるコンテンツを指定します。

[大文字小文字の区別なし（Case Insensitive）]

（注） このオプションは protected_content キーワードの設定では**サポートされません**。

ASCII 文字列でコンテンツ一致を検索するときに大文字/小文字の区別を無視するようルール エンジンに指示できます。検索で大文字と小文字を区別しないようにするには、コンテンツ検索の指定時に [大文字小文字の区別なし（Case Insensitive）] をオンにします。

Hash Type

（注） このオプションは protected_content キーワードで**のみ**設定できます。

[ハッシュ タイプ（Hash Type）] ドロップダウンを使用して、検索文字列のエンコードに使用されたハッシュ関数を特定します。システムは、protected_content 検索文字列のハッシュ方式として SHA-512、SHA-256、および MD5 をサポートしています。選択したハッシュ タイプとハッシュされたコンテンツの長さが一致しない場合、システムはルールを保存**しません**。

自動的に Cisco 設定のデフォルト値が選択されます。[デフォルト（Default）] が選択される場合、ルールに特定のハッシュ関数は含まれず、SHA-512 がハッシュ関数であると見なされます。

Raw Data

[raw データ（Raw Data）] オプションを使用すると、ルール エンジンは、正規化されたペイロードデータ（ネットワーク分析ポリシーによってデコードされたデータ）を分析する前にオリジナルのパケットペイロードを分析します。引数値は使用されません。正規化の前に、ペイロード内の Telnet ネゴシエーション オプションを検査するために Telnet トラフィックを分析する場合に、このキーワードを使用できます。

同じ `content` または `protected_content` キーワードで、**Raw Data** オプションを HTTP コンテンツ オプションと一緒に使用することはできません。

ヒント HTTP トラフィックで raw データを検査するかどうか、また、どの程度の量の raw データを検査するかを決定するため、HTTP 検査プリプロセッサの [クライアント フローの深さ（Client Flow Depth）] オプションと [サーバ フローの深さ（Server Flow Depth）] オプションを設定することができます。

注

指定したコンテンツと一致しないコンテンツを検索するには、[一致しない（Not）] オプションを選択します。[Not] オプションがオンになっている `content` または `protected_content` キーワードを含むルールを作成する場合は、そのルール内に、[Not] オプションがオフになっている別の `content` または `protected_content` キーワードを 1 つ以上含める必要があります。

注意 `content` または `protected_content` キーワードに対して [Not] オプションをオンにした場合は、そのキーワードだけを含むルールを作成しないでください。侵入ポリシーの効果がなくなる可能性があります。

たとえば、SMTP ルール 1:2541: 9 に 3 つの `content` キーワードが含まれており、そのうちの 1 つで [一致しない（Not）] オプションが選択されているとします。**Not** オプションが選択されたキーワード以外のすべての `content` キーワードを仮に削除すると、このルールに基づくカスタム ルールが無効になります。このようなルールを侵入ポリシーに追加すると、そのポリシーの効果がなくなる可能性があります。

ヒント 同じ `content` キーワードで、[Not] チェック ボックスと [Use Fast Pattern Matcher] チェック ボックスを同時に選択することはできません。

コンテンツ（content）および保護コンテンツ（protected_content）キーワード検索位置

検索位置オプションを使用すると、指定したコンテンツの検索をどこから開始するか、どこまで検索するかを指定できます。

許可された組み合わせ：content 検索位置の引数

次のように、2 つの content 位置ペアのいずれかを使用すると、指定したコンテンツの検索をどこから開始するか、どこまで検索するかを指定できます。

- パケット ペイロードの先頭を基準にして検索する場合は、**Offset** と **Depth** を一緒に使用します。
- 現在の検索位置を基準にして検索する場合は、**Distance** と **Within** を一緒に使用します。

ペアに含まれるオプションのどちらか 1 つだけを指定した場合は、そのペアのもう 1 つのオプションのデフォルトが想定されます。

Offset および **Depth** オプションと、**Distance** および **Within** オプションを混合することはできません。たとえば、**Offset** と **Within** をペアにすることはできません。1 つのルール内で任意の数の位置オプションを使用できます。

位置が指定されない場合は、**Offset** と **Depth** のデフォルトが想定されます。つまり、コンテンツ検索はパケット ペイロードの先頭から始まってパケットの末尾まで続きます。

また、既存の byte_extract 変数を使用して位置オプションの値を指定することもできます。

ヒント　1 つのルール内で任意の数の位置オプションを使用できます。

関連トピック

byte_extract キーワード （2184 ページ）

許可された組み合わせ：protected_content 検索位置の引数

次のように、必須の **Length** protected_content 位置オプションを **Offset** または **Distance** 位置オプションと組み合わせて使用すると、指定されたコンテンツの検索をどこから開始するか、どこまで検索するかを指定できます。

- パケット ペイロードの先頭を基準にして、保護された文字列を検索するには、**Length** と **Offset** を一緒に使用します。
- 現在の検索位置を基準にして、保護された文字列を検索するには、**Length** と **Distance** を一緒に使用します。

ヒント　1 つのキーワード設定内で **Offset** オプションと **Distance** オプションを混合することはできませんが、1 つのルール内では任意の数の位置オプションを使用できます。

位置が指定されない場合は、デフォルトが想定されます。つまり、コンテンツ検索はパケット ペイロードの先頭から始まってパケットの末尾まで続きます。

また、既存の byte_extract 変数を使用して位置オプションの値を指定することもできます。

関連トピック

byte_extract キーワード （2184 ページ）

content および protected_content の検索位置の引数

奥行

（注） このオプションは、content キーワードを設定する場合に**のみ**サポートされます。

オフセット値の先頭からの（またはオフセットが設定されていない場合はパケット ペイロード先頭からの）コンテンツ検索の最大の深さをバイト単位で指定します。

たとえば、ルールのコンテンツ値が cgi-bin/phf、offset 値が 3、depth 値が 22 である場合、ルール 見出しで指定されたパラメータを満たすパケット内で、cgi-bin/phf 文字列との一致の検索がバイト位置 3 から始まり、22 バイト処理した後（バイト位置 25 で）停止します。

指定したコンテンツの長さ以上の、最大65535バイトまでの値を指定する必要があります。値 0 は指定できません。

デフォルトの深さは、「パケットの末尾まで検索」です。

距離（Distance）

以前に見つかったコンテンツ一致から数えて、指定されたバイト数の後に出現する後続のコンテンツ一致を見つけるようルール エンジンに指示します。

Distance（距離）カウンタはバイト 0 から始まるため、最後に見つかったコンテンツ一致から順方向に移動すべきバイト数よりも 1 つ少ない数値を指定してください。たとえば 4 を指定した場合、5 番目のバイトから検索が始まります。

-65535 ～ 65535 バイトを値として指定できます。負の Distance 値を指定した場合は、検索を開始するバイト位置がパケットの先頭から外れる可能性があります。実際にはパケットの第 1 バイトから検索が開始されますが、計算ではパケットの外側のバイトも考慮されます。たとえば、パケット内の現在の位置が第 5 バイトで、次のコンテンツ ルール オプションで Distance 値 -10 および Within 値 20 が指定された場合、検索はペイロードの先頭から開始され、Within オプションが 15 に調整されます。

デフォルトの距離は0で、これは最後のコンテンツ一致の後のパケット内の現在位置という意味です。

長さ（Length）

（注） このオプションは protected_content キーワードを設定する場合に**のみ**サポートされます。

Length protected_content キーワード オプションは、ハッシュされていない検索文字列の長さをバイト単位で示します。

たとえば、コンテンツ `Sample1` を使ってセキュア ハッシュを生成した場合には、**Length** 値として `7` を使用します。このフィールドに値を入力することは**必須**です。

Offset

パケット ペイロードの先頭を基準とする、コンテンツの検索を開始するパケット ペイロード内の位置をバイト単位で指定します。65535 ～ 65535 バイトを値として指定できます。

オフセット カウンタはバイト 0 から始まるため、パケット ペイロードの先頭から順方向に移動すべきバイト数よりも 1 つ少ない数値を指定してください。たとえば 7 を指定した場合は、8 番目のバイトから検索が始まります。

デフォルトのオフセットは 0 で、これはパケットの先頭を意味します。

Within

（注） このオプションは、`content` キーワードを設定する場合に**のみ**サポートされます。

[次の範囲内（Within）] オプションを使用すると、ルールをトリガーとして使用させるには、最後に見つかったコンテンツ一致の末尾以降、指定のバイト数以内に次のコンテンツ一致が発生する必要があることを指示できます。たとえば **Within** 値として `8` を指定した場合、次のコンテンツ一致がパケット ペイロードの次の 8 バイト以内に発生する必要があります。発生しない場合は、ルールをトリガーとして使用する基準が満たされません。

指定したコンテンツの長さ以上の、最大 65535 バイトまでの値を指定できます。

[次の範囲内（Within）] のデフォルトは「パケットの末尾まで検索」です。

概要：HTTP content および protected_content キーワードの引数

HTTP `content` または `protected_content` キーワード オプションを使用すると、HTTP Inspect プリプロセッサによってデコードされた HTTP メッセージ内の一致コンテンツを検索する位置を指定できます。

次の 2 つのオプションは、HTTP 応答内のステータス フィールドを検索します。

- **HTTP ステータス コード（HTTP Status Code）**
- **HTTP ステータス メッセージ（HTTP Status Message）**

ルール エンジンは未加工の正規化されていないステータス フィールドを検索しますが、ここでは、他の Raw HTTP フィールドと正規化された HTTP フィールドを併用する際に考慮すべき制限についての説明を簡略化するために、これらのオプションが別個に列挙されていることに注意してください。

次の 5 つのオプションは、必要に応じて HTTP 要求、応答、またはその両方の中で正規化フィールドを検索します。

- **HTTP URI**

- **HTTP メソッド（HTTP Method）**
- **HTTP ヘッダー（HTTP Header）**
- **HTTP Cookie**
- **HTTP クライアント ボディ（HTTP Client Body）**

次の 3 つのオプションは、必要に応じて HTTP 要求、応答、またはその両方の中で未加工の（正規化されていない）非ステータス フィールドを検索します。

- **HTTP Raw URI**
- **HTTP Raw ヘッダー（HTTP Raw Header）**
- **HTTP Raw Cookie**

HTTP `content` オプションを選択する場合は、次のガイドラインに従ってください。

- HTTP `content` オプションは TCP トラフィックにのみ適用されます。
- パフォーマンスへの悪影響を避けるために、指定したコンテンツが出現する可能性のあるメッセージ部分だけを選択してください。

  たとえば、ショッピング カート メッセージの場合のように大きな cookie がトラフィックに含まれている可能性がある場合は、HTTP cookie ではなく HTTP ヘッダーの中で指定のコンテンツを検索することができます。

- HTTP Inspect プリプロセッサの正規化機能を活用し、パフォーマンスを向上させるには、作成するすべての HTTP 関連ルールの中に少なくとも 1 つの `content` または `protected_content` キーワードを含め、それに対して **HTTP URI**、**HTTP Method**、**HTTP Header**、または **HTTP Client Body** オプションを選択します。

- HTTP `content` または `protected_content` キーワード オプションと組み合わせて `replace` キーワードを使用することはできません。

単一の正規化された HTTP オプションまたはステータス フィールドを指定できます。または、複数の正規化 HTTP オプションとステータス フィールドを任意に組み合わせて、コンテンツ領域をマッチング対象にすることもできます。ただし、HTTP フィールド オプションを使用する場合には次の制限事項に注意してください。

- 同じ `content` または `protected_content` キーワード内で、**Raw Data** オプションと HTTP オプションを一緒に使用することはできません。
- 未加工 HTTP フィールド オプション（**HTTP Raw URI**、**HTTP Raw Header**、または **HTTP Raw Cookie**）と、それぞれに対応する正規化されたオプション（**HTTP URI**、**HTTP Header**、または **HTTP Cookie**）を同じ `content` または `protected_content` キーワード内で一緒に使用することはできません。
- **Use Fast Pattern Matcher** を、次の 1 つ以上の HTTP フィールド オプションと組み合わせて選択することはできません。

[HTTP Raw URI]、[HTTP raw ヘッダー（HTTP Raw Header）]、[HTTP Raw Cookie]、[HTTP Cookie]、[HTTP メソッド（HTTP Method）]、[HTTP ステータス メッセージ（HTTP Status Message）]、[HTTP ステータス コード（HTTP Status Code）]

ただし、次のいずれかの正規化フィールドを検索するために高速パターンマッチ機能を使用する `content` または `protected_content` キーワードでは、上記のオプションを含めることができます。

[HTTP URI]、[HTTP ヘッダー（HTTP Header）]、または [HTTP クライアント ボディ（HTTP Client Body）]

たとえば、[HTTP Cookie]、[HTTP Header]、および [Use Fast Pattern Matcher] を選択した場合、ルール エンジンは HTTP cookie と HTTP ヘッダーの両方でコンテンツを検索しますが、高速パターン マッチ機能は HTTP cookie ではなく、HTTP ヘッダーにのみ適用されます。

- 制限付きオプションと制限なしオプションを併用した場合、高速パターンマッチ機能は、指定された制限なしフィールドのみを検索することで、侵入ルールエディタにルールを渡して（制限付きフィールドの評価を含む）完全な評価を行うべきかどうかを検査します。

関連トピック

content キーワードの高速パターン マッチ機能の引数 （2175 ページ）

HTTP コンテンツと protected_content キーワードの引数

HTTP URI

正規化された要求 URI フィールド内でコンテンツ一致を検索するには、このオプションを選択します。

このオプションと `pcre` キーワードの HTTP URI（U）オプションを一緒に使用して、同じコンテンツを検索できないことに注意してください。

（注） パイプライン処理された HTTP 要求パケットには複数の URI が含まれています。[HTTP URI] が選択されている場合、パイプライン処理された HTTP 要求パケットをルールエンジンが検出すると、そのパケット内のすべての URI でコンテンツ一致が検索されます。

HTTP Raw URI

正規化された要求 URI フィールド内でコンテンツ一致を検索するには、このオプションを選択します。

このオプションと `pcre` キーワードの HTTP URI（U）オプションを一緒に使用して、同じコンテンツを検索できないことに注意してください。

（注） パイプライン処理された HTTP 要求パケットには複数の URI が含まれています。[HTTP URI] が選択されている場合、パイプライン処理された HTTP 要求パケットをルールエンジンが検出すると、そのパケット内のすべての URI でコンテンツ一致が検索されます。

HTTP メソッド

（URI で識別されるリソースに対して行う GET や POST などのアクションを特定する）要求メソッド フィールド内のコンテンツ一致を検索するには、このオプションを選択します。

HTTP Header

HTTP 要求内の（cookie を除く）正規化されたヘッダー フィールドでコンテンツ一致を検索するには、このオプションを選択します。また、HTTP Inspect プリプロセッサの [Inspect HTTP Responses] オプションが有効になっている場合は応答内でも検索されます。

このオプションと `pcre` キーワードの HTTP 見出し（H）オプションを一緒に使用して、同じコンテンツを検索できないことに注意してください。

HTTP Raw Header

HTTP 要求内の（cookie を除く）raw ヘッダー フィールドでコンテンツ一致を検索するには、このオプションを選択します。また、HTTP Inspect プリプロセッサの [Inspect HTTP Responses] オプションが有効になっている場合は応答内でも検索されます。

このオプションと `pcre` キーワードの HTTP 未加工見出し（D）オプションを一緒に使用して、同じコンテンツを検索できないことに注意してください。

HTTP Cookie

正規化された HTTP クライアント要求見出し内で識別される cookie でコンテンツ一致を検索するには、このオプションを選択します。また、HTTP Inspect プリプロセッサの [HTTP 応答の検査（Inspect HTTP Responses）] オプションが有効になっている場合は応答 set-cookie データ内でも検索されます。システムは、メッセージ本文に含まれる cookie を本文の内容として扱うことに注意してください。

cookie 内だけで一致を検索するには、HTTP Inspect プリプロセッサの [HTTP Cookie の検査（Inspect HTTP Cookies）] オプションを有効にする必要があります。これを有効にしない場合、ルール エンジンは cookie を含む見出し全体を検索します。

次の点に注意してください。

- このオプションと `pcre` キーワードの HTTP cookie（C）オプションを一緒に使用して、同じコンテンツを検索することはできません。
- `Cookie:` ヘッダー名と `Set-Cookie:` ヘッダー名、ヘッダー行の先行スペース、およびヘッダー行の終わりを示す `CRLF` は cookie の一部としてではなく、ヘッダーの一部として検査されます。

HTTP Raw Cookie

未加工 HTTP クライアント要求見出し内で識別される cookie でコンテンツ一致を検索するには、このオプションを選択します。また、HTTP Inspect プリプロセッサの [HTTP 応答の検査（Inspect HTTP Responses）] オプションが有効になっている場合は応答 set-cookie データ内でも検索されます。システムは、メッセージ本文に含まれる cookie を本文の内容として扱うことに注意してください。

cookie 内だけで一致を検索するには、HTTP Inspect プリプロセッサの [HTTP Cookie の検査（Inspect HTTP Cookies）] オプションを有効にする必要があります。これを有効にしない場合、ルール エンジンは cookie を含む見出し全体を検索します。

次の点に注意してください。

- このオプションと `pcre` キーワードの HTTP 未加工 cookie（K）オプションを一緒に使用して同じコンテンツを検索することはできません。
- `Cookie:` ヘッダー名と `Set-Cookie:` ヘッダー名、ヘッダー行の先行スペース、およびヘッダー行の終わりを示す `CRLF` は cookie の一部としてではなく、ヘッダーの一部として検査されます。

HTTP Client Body

HTTP クライアント要求内のメッセージ本文でコンテンツ一致を検索するには、このオプションを選択します。

このオプションが機能するためには、HTTP Inspect プリプロセッサの [HTTP クライアント ボディの抽出の深さ（HTTP Client Body Extraction Depth）] オプションで 0 ～ 65535 の値を指定する必要があることに注意してください。

HTTP ステータス コード（HTTP Status Code）

HTTP 応答内の 3 桁のステータス コードでコンテンツ一致を検索するには、このオプションを選択します。

このオプションで一致が返されるようにするには、HTTP Inspect プリプロセッサの [HTTP 応答の検査（Inspect HTTP Responses）] オプションを有効にする必要があります。

HTTP Status Message

HTTP 応答のステータス コードに付加されるテキスト記述の中でコンテンツ一致を検索するには、このオプションを選択します。

このオプションで一致が返されるようにするには、HTTP Inspect プリプロセッサの [HTTP 応答の検査（Inspect HTTP Responses）] オプションを有効にする必要があります。

関連トピック

PCRE 修飾子のオプション （2193 ページ）
サーバレベルの HTTP 正規化オプション （2335 ページ）

概要：content キーワードによる高速パターン マッチ機能

（注） これらのオプションは、protected_content キーワードの設定では**サポートされません**。

高速パターン マッチ機能は、パケットをルール エンジンに渡す前に、評価するルールをすばやく決定します。この初期決定により、パケット評価で使用されるルール数が大幅に減るため、パフォーマンスが向上します。

デフォルトで、高速パターンマッチ機能は、ルールで指定された最長のコンテンツをパケットで検索します。これは、不必要なルール評価をできるだけ減らすためです。次の例のようなルール フラグメントがあるとします。

```
alert tcp any any -> any 80 (msg:"Exploit"; content:"GET";
http_method; nocase; content:"/exploit.cgi"; http_uri;
nocase;)
```

ほとんどすべての HTTP クライアント要求にはコンテンツ GET が含まれていますが、コンテンツ /exploit.cgi を含む要求は稀です。GET を高速パターン コンテンツとして使用した場合、ルール エンジンはほとんどのケースでこのルールを評価し、一致はほとんど検出されないでしょう。しかし、/exploit.cgi を使用するとほとんどのクライアントの GET 要求は評価されないため、パフォーマンスが向上します。

指定されたコンテンツが高速パターン マッチ機能で検出された場合にのみ、ルール エンジンはパケットをルールに照らして評価します。たとえば、ルール内の 1 つの content キーワードでコンテンツ short を指定し、別のキーワードで longer、さらに 3 番目のキーワードで longest を指定した場合、高速パターン マッチ機能はコンテンツ longest を使用し、ルール エンジンがペイロード内で longest を検出した場合にのみ、ルールが評価されます。

content キーワードの高速パターン マッチ機能の引数

Use Fast Pattern Matcher

使用する高速パターンマッチ機能の短い検索パターンを指定するには、このオプションを使用します。理論的には、指定したパターンの方が最長パターンよりもパケット内で見つかる可能性が低いため、より的を絞って対象のエクスプロイトを識別できます。

Use Fast Pattern Matcher と他のオプションを同じ content キーワード内で選択する場合は、次の制限事項に注意してください。

- ルールごとに 1 回だけ、**Use Fast Pattern Matcher** を指定できます。
- **Use Fast Pattern Matcher** と **Not** を組み合わせて選択した場合は、**Distance**、**Within**、**Offset**、および **Depth** を使用できません。
- Use Fast Pattern Matcher を、次のいずれかの HTTP フィールド オプションと組み合わせて選択することはできません。

  HTTP Raw URI、**HTTP Raw Header**、**HTTP Raw Cookie**、**HTTP Cookie**、**HTTP Method**、**HTTP Status Message**、または **HTTP Status Code**

ただし、次のいずれかの正規化フィールドを検索するために高速パターンマッチ機能を使用する content キーワードでは、上記のオプションを含めることができます。

HTTP URI、**HTTP Header**、または **HTTP Client Body**

たとえば、**HTTP Cookie**、**HTTP Header**、および **Use Fast Pattern Matcher** を選択した場合、ルール エンジンは HTTP cookie と HTTP 見出しの両方でコンテンツを検索しますが、高速パターン マッチ機能は HTTP cookie ではなく、HTTP 見出しにのみ適用されます。

未加工 HTTP フィールド オプション（[HTTP Raw URI]、[HTTP raw ヘッダー（HTTP Raw Header）]、または [HTTP raw クッキー（HTTP Raw Cookie）]）と、それぞれに対応する正規化されたオプション（[HTTP URI]、[HTTP ヘッダー（HTTP Header）]、または [HTTP クッキー（HTTP Cookie）]）を同じ content キーワード内で一緒に使用できないことに注意してください。

制限付きオプションと制限なしオプションを併用した場合、高速パターンマッチ機能は、指定された制限なしフィールドのみを検索することで、ルールエンジンにパケットを渡して（制限付きフィールドの評価を含む）完全な評価を行うべきかどうかを検査します。

- オプションで、**Use Fast Pattern Matcher** を選択した場合には **Fast Pattern Matcher Only** または **Fast Pattern Matcher Offset and Length** を選択することもできますが、この両方は選択できません。
- Base64 データの検査時には高速パターン マッチ機能を使用できません。

Fast Pattern Matcher Only

このオプションを使用すると、content キーワードをルール オプションとしてではなく、高速パターン マッチ機能オプションとしてのみ使用できます。指定したコンテンツをルール エンジンで評価する必要がない場合、このオプションを使ってリソースを節約できます。たとえば、ペイロード内のいずれかの場所にコンテンツ 12345 が存在することだけを必要とするルールがあるとします。高速パターンマッチ機能でパターンが検出された場合に、ルール内の追加のキーワードに照らしてパケットを評価できます。パターン 12345 が含まれているかどうかを判断するために、ルール エンジンがパケットを再評価する必要はありません。

指定されたコンテンツに関連する他の条件がルールに含まれている場合は、このオプションを使用しないでください。たとえば、別のルール条件で abcd が 1234 の前に出現するかどうかを判断する場合には、このオプションを使ってコンテンツ 1234 を検索しないでください。**Fast Pattern Matcher Only** を指定すると、指定されたコンテンツがルール エンジンによって検索されないため、このケースではルール エンジンが相対的な位置を判断できません。

このオプションを使用するときには、次の条件に注意してください。

- 指定されたコンテンツは位置に依存しない、つまり、ペイロードのどこにでも出現する可能性があるため、位置オプション（**Distance**、**Within**、**Offset**、**Depth**、**Fast Pattern Matcher Offset and Length**）を使用することはできません。
- このオプションを **Not** と組み合わせて使用することはできません。
- このオプションを **Fast Pattern Matcher Offset and Length** と組み合わせて使用することはできません。

- 大文字/小文字を区別しない方法ですべてのパターンが高速パターン マッチ機能に挿入されるため、指定したコンテンツは「大文字/小文字の区別なし」として扱われます。これは自動的に処理されるため、このオプションの選択時に **Case Insensitive** を選択する必要はありません。
- **Fast Pattern Matcher Only** オプションを使用する `content` キーワードの直後に、現在の検索位置を基準にして検索位置を設定する次のキーワードを続けないようにしてください。
  - `isdataat`
  - `pcre`
  - `content`（**Distance** または **Within** が選択されている場合）
  - `content`（**HTTP URI** が選択されている場合）
  - `asn1`
  - `byte_jump`
  - `byte_test`
  - `byte_math`
  - `byte_extract`
  - `base64_decode`

Fast Pattern Matcher Offset and Length

[高速パターン マッチ機能オフセットおよび長さ（Fast Pattern Matcher Offset and Length）] オプションを使用すると、検索するコンテンツの一部分を指定できます。これにより、パターンが非常に長く、ルールの一致の可能性を判断するのにパターンの一部分だけで十分な場合に、メモリ消費を抑えることができます。高速パターンマッチ機能によってルールが選択されたときに、パターン全体がルールに照らして評価されます。

次の構文に従い、検索を開始する位置（オフセット）およびコンテンツ内をどれほど検索するか（長さ）をバイト単位で指定することにより、高速パターンマッチ機能で使用する部分を決定します。

```
offset,length
```

たとえば、次のコンテンツに対して

```
1234567
```

次のようにオフセットと長さのバイト数を指定した場合、

```
1,5
```

高速パターン マッチ機能はコンテンツ `23456` のみを検索します。

このオプションを [Fast Pattern Matcher Only] と一緒に使用できないことに注意してください。

関連トピック

概要：HTTP content および protected_content キーワードの引数 （2170 ページ）
base64_decode キーワードと base64_data キーワード （2268 ページ）

replace キーワード

インライン導入で `replace` キーワードを使用すると、指定したコンテンツ、または Cisco SSL アプライアンスによって検出された SSL トラフィック内のコンテンツを置き換えることができます。

`replace` キーワードを使用するには、`content` キーワードを使って特定の文字列を検索するカスタムの標準テキスト ルールを作成します。その後、`replace` キーワードを使用して、コンテンツを置き換える文字列を指定します。置換値とコンテンツ値は同じ長さである必要があります。

（注） `protected_content` キーワード内でハッシュされたコンテンツを置き換えるために `replace` キーワードを使用することは**できません**。

オプションで、以前の Firepower システム ソフトウェア バージョンとの下位互換性を維持するために、置換文字列を引用符で囲むことができます。引用符を含めない場合は、それらが自動的にルールに追加されるため、構文的に正しいルールになります。置換テキストの一部として先行引用符または後続引用符を含めるには、次の例に示すように、バックスラッシュを使ってエスケープする必要があります。

```
"replacement text plus \"quotation\" marks""
```

1 つのルール内に複数の `replace` キーワードを含めることができますが、`content` キーワードごとに 1 つずつしか含めることができません。ルールによって検出されたコンテンツの最初のインスタンスだけが置き換えられます。

次に、`replace` キーワードの使用例を示します。

- エクスプロイトを含んでいる着信パケットをシステムが検出した場合、有害な文字列を無害な文字列に置き換えることができます。このテクニックは、有害なパケットを単に破棄するよりも効果的である場合があります。破棄されたパケットを攻撃者が単に再送信し続け、やがてネットワーク防御を通り抜けるか、ネットワークを氾濫させるという攻撃シナリオがあります。パケットを破棄する代わりに別の文字列に置き換えることで、脆弱ではないターゲットに対して攻撃が実行されたと攻撃者に思い込ませることができます。
- （たとえば Web サーバの）脆弱なバージョンが稼働しているかどうかを調べる偵察攻撃が懸念される場合は、発信パケットを検出して、バナーを独自のテキストに置き換えることができます。

（注） 置換ルールを使用するインライン侵入ポリシー内でルール状態が [Generate Events] に設定されていることを確認してください。ルールを [Drop and Generate events] に設定した場合はパケットが破棄され、コンテンツが置き換えられません。

文字列置換プロセスでは、宛先ホストがエラーなしでパケットを受信できるように、パケットチェックサムがシステムによって自動的に更新されます。

`replace` キーワードは、HTTP 要求メッセージの `content` キーワード オプションと組み合わせて使用できないことに注意してください。

関連トピック

content キーワードと protected_content キーワード （2164 ページ）
概要：HTTP content および protected_content キーワードの引数 （2170 ページ）

byte_jump キーワード

`byte_jump` キーワードは、指定されたバイト セグメントで定義されるバイト数を計算し、指定したオプションに応じて、指定されたバイト セグメントの末尾から、パケット ペイロードの先頭または末尾から、あるいは最後のコンテンツ一致に対して相対的なポイントから順方向に、パケット内でそのバイト数だけスキップします。パケットの特定のバイト セグメントが、パケット内の可変データに含まれるバイト数を示す場合には、これが役立ちます。

次の表では、`byte_jump` キーワードで必要な引数を説明します。

表 *164 : byte_jump* の必須引数

引数	説明
Bytes	パケットから抽出するバイト数。 DCE/RPC を指定せずに使用する場合、許可される値は 0 ～ 10 ですが、次の制限があります。 • `From End` 引数とともに使用すると、バイト数は 0 になることがあります。Bytes が 0 の場合、抽出された値は 0 です。 • 1、2、または 4 以外のバイト数を指定する場合は、番号タイプ（16 進数、8 進数、または 10 進数）を指定する必要があります。 DCE/RPC とともに使用する場合、許可される値は 1、2、および 4 です。

引数	説明
Offset	ペイロード内で処理を開始するバイト数。`offset` カウンタはバイト 0 から始まるため、パケット ペイロードの先頭、または最後に見つかったコンテンツ一致から順方向にジャンプさせるバイト数から 1 を差し引いて `offset` 値を計算してください。 -65535 ～ 65535 バイトを指定できます。 また、既存の `byte_extract` 変数または `byte_math` 結果を使用してこの引数の値を指定することもできます。

次の表で説明するオプションを使用すると、必須の引数に指定された値をシステムがどのように解釈するかを定義できます。

表 *165 : byte_jump* の追加のオプション引数

引数	説明
Relative	最後に見つかったコンテンツ一致で検出された最後のパターンを基準にしてオフセットを計算します。
Align	変換されたバイト数を、次の 32 ビット境界に切り上げます。
Multiplier	ルール エンジンで最終的な `byte_jump` 値を算出するために、パケットから得られた `byte_jump` 値に掛ける値を示します。 つまり、ルール エンジンは、指定されたバイト セグメントで定義されるバイト数だけスキップする代わりに、Multiplier 引数で指定される整数を乗算したバイト数だけスキップします。
Post Jump Offset	他の `byte_jump` 引数を適用した後に、順方向または逆方向にスキップするバイト数（-65535 ～ 65535）。正の値は順方向にスキップし、負の値は逆方向にスキップします。無効にするには、フィールドを空白のままにするか、`0` を入力します。 **DCE/RPC** 引数を選択すると、一部の `byte_jump` 引数が適用されないことに注意してください。
From Beginning	ルール エンジンが、パケット内の現在の位置からではなく、パケット ペイロードの先頭からペイロード内の指定されたバイト数をスキップする必要があることを示します。
From End	ジャンプは、バッファの最後のバイトのすぐ後のバイトから実行されます。

引数	説明
Bitmask	AND 演算子を使用して、指定した 16 進数のビットマスクを、Bytes 引数から抽出したバイトに適用します。 ビットマスクは 1 ー 4 バイトです。 結果は、マスク内の末尾のゼロの数と等しい数のビット分だけ右にシフトされます。

DCE/RPC、**Endian**、または **Number Type** のうち 1 つだけを指定できます。

バイト数を `byte_extract` キーワードでどのように計算するか定義するには、次の表の中から引数を選択します。バイト順引数を選択しなかった場合、ルール エンジンはビッグ エンディアンのバイト順を使用します。

表 *166 : byte_jump* のバイト順引数

引数	説明
Big Endian	デフォルトのネットワーク バイト順であるビッグ エンディアン バイト順でデータを処理します。
Little Endian	リトル エンディアン バイト順でデータを処理します。
DCE/RPC	DCE/RPC プリプロセッサで処理されるトラフィック用に `byte_jump` キーワードを指定します。 DCE/RPC プリプロセッサがビッグ エンディアンまたはリトル エンディアン バイト順を決定します。**Number Type** 引数と **Endian** 引数は適用されません。 この引数を有効にした場合は、他の特定の DCE/RPC キーワードと組み合わせて `byte_jump` を使用することもできます。

次の表に示すいずれか1つの引数を使用して、パケット内のストリング データをシステムがどのように表示するかを定義します。

表 *167 :* 番号タイプ引数

引数	説明
Hexadecimal String	変換後のストリング データを 16 進形式で表現します。
Decimal String	変換後のストリング データを 10 進形式で表現します。
Octal String	変換後のストリング データを 8 進形式で表現します。

たとえば、次のような値を `byte_jump` に設定した場合、

- Bytes = 4

- Offset = 12
- Relative enabled
- Align enabled

ルール エンジンは、最後に見つかったコンテンツ一致から 13 バイト後に出現する 4 つのバイトで記述される数値を計算して、そのバイト数だけパケット内を順方向にスキップします。たとえば、ある特定のパケット内で計算される 4 つのバイトが `00 00 00 1F` である場合、ルール エンジンはこれを 31 に変換します。`align` が指定されている（次の 32 ビット境界まで移動するようエンジンに指示する）ため、ルール エンジンはパケット内を 32 バイト先までスキップします。

あるいは、次のような値を `byte_jump` に設定した場合、

- Bytes = 4
- Offset = 12
- From Beginning enabled
- Multiplier = 2

ルール エンジンは、パケットの先頭から 13 バイト後に出現する 4 つのバイトで記述される数値を計算します。その後、その数値に 2 を掛けてスキップする総バイト数を計算します。たとえば、ある特定のパケット内で計算される 4 つのバイトが `00 00 00 1F` である場合、ルール エンジンはこれを 31 に変換し、それに 2 を掛けて 62 にします。[From Beginning] が有効になっているため、ルール エンジンはパケット内の最初の 63 バイトをスキップします。

関連トピック

byte_extract キーワード （2184 ページ）
DCE/RPC キーワード （2223 ページ）

byte_test キーワード

`byte_test` キーワードは、指定されたバイト セグメントを Value 引数およびその演算子に対してテストします。

次の表に、`byte_test` キーワードで必要な引数を説明します。

表 *168 : byte_test* の必須引数

引数	説明
Bytes	パケットから計算するバイト数。 DCE/RPC を指定せずに使用する場合、許可される値は 1 ～ 10 です。ただし、1、2、または 4 以外のバイト数を指定する場合は、番号タイプ（16 進数、8 進数、または 10 進数）を指定する必要があります。 DCE/RPC とともに使用する場合、許可される値は 1、2、および 4 です。

引数	説明
値	テストする値（演算子を含む）。 サポート対象演算子：<、>、=、!、&、^、!>、!<、!=、!&、または !^。 たとえば `!1024` と指定した場合、`byte_test` は指定された数値を変換し、それが 1024 と等しくなければイベントが生成されます（他のすべてのキーワード パラメータが一致する場合）。 「!」と「!=」は等価であることに注意してください。 また、既存の `byte_extract` 変数または `byte_math` 結果を使用してこの引数の値を指定することもできます。
Offset	ペイロード内で処理を開始するバイト数。`offset` カウンタはバイト 0 から始まるため、パケット ペイロードの先頭、または最後に見つかったコンテンツ一致から順方向にカウントするバイト数から 1 を差し引いて `offset` 値を計算してください。 既存の `byte_extract` 変数または `byte_math` result 変数を使用して、この引数の値を指定することができます。

次の表に示す引数を使用すると、システムで `byte_test` 引数がどのように使用されるかをさらに定義できます。

表 *169 : byte_test* の追加のオプション引数

引数	説明
Bitmask	AND 演算子を使用して、指定した 16 進数のビットマスクを、Bytes 引数から抽出したバイトに適用します。 ビットマスクは 1 ー 4 バイトです。 結果は、マスク内の末尾のゼロの数と等しい数のビット分だけ右にシフトされます。
Relative	最後に見つかったパターン一致を基準にしてオフセットを計算します。

DCE/RPC、**Endian**、または **Number Type** のうち 1 つだけを指定できます。

検査対象となるバイトを `byte_test` キーワードでどのように計算するか定義するには、次の表の中から引数を選択します。バイト順引数を選択しなかった場合、ルール エンジンはビッグ エンディアンのバイト順を使用します。

表 *170 : byte_test* のバイト順引数

引数	説明
Big Endian	デフォルトのネットワーク バイト順であるビッグ エンディアン バイト順でデータを処理します。

引数	説明
Little Endian	リトル エンディアン バイト順でデータを処理します。
DCE/RPC	DCE/RPC プリプロセッサで処理されるトラフィック用に `byte_test` キーワードを指定します。 DCE/RPC プリプロセッサがビッグ エンディアンまたはリトル エンディアン バイト順を決定します。**Number Type** 引数と **Endian** 引数は適用されません。 この引数を有効にした場合は、他の特定の DCE/RPC キーワードと組み合わせて `byte_test` を使用することもできます。

次の表に示すいずれか1つの引数を使用して、パケット内のストリングデータをシステムがどのように表示するかを定義できます。

表 *171 : byte-test* の番号タイプ引数

引数	説明
Hexadecimal String	変換後のストリング データを 16 進形式で表現します。
Decimal String	変換後のストリング データを 10 進形式で表現します。
Octal String	変換後のストリング データを 8 進形式で表現します。

たとえば、次のような値を `byte_test` に指定した場合、

- Bytes = 4
- Operator and Value > 128
- Offset = 8
- Relative enabled

ルールエンジンは、最後に見つかったコンテンツ一致から（それを基準にして）9バイト後に出現する 4 つのバイトで記述される数値を計算し、その計算値が 128 バイトを超えた場合に、ルールがトリガーとして使用されます。

関連トピック

byte_extract キーワード （2184 ページ）
DCE/RPC キーワード （2223 ページ）

byte_extract キーワード

`byte_extract` キーワードを使用すると、指定したバイト数をパケットから変数の中に読み込むことができます。後で、その変数を、同じルール内で他の検出キーワードの特定の引数の値として使用できます。

たとえば、パケット データに含まれるバイト数が特定のバイト セグメントで記述されている場合、パケットからデータ サイズを抽出するには、これが役立ちます。たとえば、特定のバイト セグメントにおいて、後続データが 4 バイト構成であると記述されている場合、データ サイズ 4 バイトを抽出して変数値として使用できます。

byte_extract を使用するとき、1 つのルール内で最大 2 つの異なる変数を同時に作成できます。byte_extract 変数を何回でも再定義できます。同じ変数名と別の変数定義を使って新しい byte_extract キーワードを入力した場合、その前の変数定義がオーバーライドされます。

次の表に、byte_extract キーワードで必要な引数について説明します。

表 *172 : byte_extract* の必須引数

引数	説明
Bytes to Extract	パケットから抽出するバイト数。 1、2、または4以外のバイト数を指定する場合は、番号タイプ（16進数、8 進数、または 10 進数）を指定する必要があります。
Offset	ペイロード内でデータの抽出を開始するバイト数。-65535 ～ 65535 バイトを指定できます。オフセット カウンタはバイト0から始まるため、順方向に数えるバイト数から1を差し引いてオフセット値を計算してください。たとえば、順方向に8バイト数えるには7を指定します。ルール エンジンは、パケット ペイロードの先頭から（**Relative** も一緒に指定した場合は最後に見つかったコンテンツ一致の後から）順方向に数えます。負の数は、**Relative** も指定した場合にのみ指定できます。 既存の byte_math の結果を使用して、この引数の値を指定することもできます。
Variable Name	他の検出キーワードの引数で使用する変数名。英数字の文字列を指定できます（ただし文字で始まる必要があります）。

抽出対象のデータを見つける方法をさらに詳しく定義するには、次の表に示す引数を使用できます。

表 *173 : byte_extract* の追加のオプション引数

引数	説明
Multiplier	パケットから抽出された値の乗数。0 ～ 65535 を指定できます。乗数を指定しない場合のデフォルト値は 1 です。
Align	抽出された値を、最も近い 2 バイトまたは 4 バイト境界に調整します。**Multiplier** も一緒に選択した場合、システムはこの調整の前に乗数を適用します。
Relative	ペイロードの先頭ではなく、最後に見つかったコンテンツ一致の末尾を基準にして **Offset** を計算します。

引数	説明
Bitmask	AND 演算子を使用して、指定した 16 進数のビットマスクを、Bytes to Extract 引数から抽出したバイトに適用します。 ビットマスクは 1 ー 4 バイトです。 結果は、マスク内の末尾のゼロの数と等しい数のビット分だけ右にシフトされます。

DCE/RPC、**Endian**、または **Number Type** のうち 1 つだけを指定できます。

検査対象となるバイトを `byte_extract` キーワードでどのように計算するか定義するには、次の表の中から引数を選択できます。バイト順引数を選択しなかった場合、ルール エンジンはビッグ エンディアンのバイト順を使用します。

表 *174 : byte_extract* のバイト順引数

引数	説明
Big Endian	デフォルトのネットワーク バイト順であるビッグ エンディアン バイト順でデータを処理します。
Little Endian	リトル エンディアン バイト順でデータを処理します。
DCE/RPC	DCE/RPC プリプロセッサで処理されるトラフィック用に `byte_extract` キーワードを指定します。 DCE/RPC プリプロセッサがビッグ エンディアンまたはリトル エンディアン バイト順を決定します。**Number Type** 引数と **Endian** 引数は適用されません。 この引数を有効にした場合は、他の特定の DCE/RPC キーワードと組み合わせて `byte_extract` を使用することもできます。

データを読み取るときの数値タイプを ASCII 文字列として指定できます。パケット内のストリング データをシステムがどのように認識するかを定義するには、次の表のいずれかの引数を選択できます。

表 *175 : byte_extract* の番号タイプ引数

引数	説明
Hexadecimal String	抽出されたストリング データを 16 進形式で読み取ります。
Decimal String	抽出されたストリング データを 10 進形式で読み取ります。
Octal String	抽出されたストリング データを 8 進形式で読み取ります。

たとえば、`byte_extract` の値を次のように指定した場合、

- Bytes to Extract = 4

- Variable Name = var
- Offset = 8
- Relative = enabled

ルールエンジンは、最後に見つかったコンテンツ一致から（それを基準にして）9バイト後に出現する、4 バイトで表現される数値を `var` という名前の変数の中に読み込みます。後でこの変数を、特定のキーワード引数の値としてルール内で指定できます。

`byte_extract` キーワードで定義した変数を指定できるキーワード引数を、次の表に列挙します。

表 *176 : byte_extract* 変数を使用できる引数

キーワード	引数
content	Depth、Offset、Distance、Within
byte_jump	Offset
byte_test	Offset、Value
byte_math	RValue、Offset
isdataat	Offset

関連トピック

DCE/RPC プリプロセッサ （2306 ページ）
DCE/RPC キーワード （2223 ページ）
基本コンテンツおよび protected_content キーワードの引数 （2166 ページ）
byte_jump キーワード （2179 ページ）
byte_test キーワード （2182 ページ）
パケット特性 （2247 ページ）

byte_math キーワード

`byte_math` キーワードは、抽出された値と指定された値または既存の変数の算術演算を実行し、その結果を新しい結果変数に格納します。結果の変数は、他のキーワードの引数として使用することができます。

ルール内で複数の `byte_math` キーワードを使用して、複数の byte_math 操作を実行できます。

次の表で、`byte_math` キーワードで必要な引数について説明します。

表 *177 : byte_math* の必須引数

引数	説明
Bytes	パケットから計算するバイト数。 DCE/RPC を指定せずに使用する場合、許可される値は 1 ～ 10 です。 • 演算子が +、-、*、または / の場合、バイト数は 1 ー 10 になります。 • 演算子が << または >> の場合、バイト数は 1 ー 4 になります。 • 1、2、または4以外のバイト数を指定する場合は、番号タイプ（16進数、8 進数、または 10 進数）を指定する必要があります。 DCE/RPC とともに使用する場合、許可される値は 1、2、および 4 です。
Offset	ペイロード内で処理を開始するバイト数。`offset` カウンタはバイト 0 から始まるため、パケットペイロードの先頭、または最後に見つかったコンテンツ一致（Relative を指定した場合）から順方向にジャンプさせるバイト数から 1 を差し引いて `offset` 値を計算してください。 -65535 ～ 65535 バイトを指定できます。 ここでは、`byte_extract` 変数を指定することもできます。
演算子	+、-、*、/、<<、または >>
RValue	演算子に続く値。これは、符号なし整数または `byte_extract` から渡される変数です。
Result Variable	`byte_math` の計算結果が格納される変数の名前。この変数は、他のキーワードの引数として使用することができます。 この値は符号なし整数として格納されます。 この変数名には次の条件があります。 • 英数字を使用する必要がある • 先頭を数字にすることはできない • Microsoft のファイル名/変数名の規則でサポートされている特殊文字を含めることができる • 特殊文字のみの名前にすることはできない

次の表で説明するオプションを使用すると、必須の引数に指定された値をシステムがどのように解釈するかを定義できます。

表 *178 : byte_math* の追加のオプション引数

引数	説明
Relative	ペイロードの先頭ではなく、最後に見つかったコンテンツ一致で検出された最後のパターンを基準にしてオフセットを計算します。
Bitmask	AND 演算子を使用して、指定した 16 進数のビットマスクを、Bytes 引数から抽出したバイトに適用します。 ビットマスクは 1 ー 4 バイトです。 結果は、マスク内の末尾のゼロの数と等しい数のビット分だけ右にシフトされます。

DCE/RPC、**Endian**、または **Number Type** のうち 1 つだけを指定できます。

バイト数を `byte_math` キーワードでどのように計算するか定義するには、次の表の中から引数を選択します。バイト順引数を選択しなかった場合、ルール エンジンはビッグ エンディアンのバイト順を使用します。

表 *179 : byte_math* のバイト順引数

引数	説明
Big Endian	デフォルトのネットワーク バイト順であるビッグ エンディアン バイト順でデータを処理します。
Little Endian	リトル エンディアン バイト順でデータを処理します。
DCE/RPC	DCE/RPC プリプロセッサで処理されるトラフィック用に `byte_math` キーワードを指定します。 DCE/RPC プリプロセッサがビッグ エンディアンまたはリトル エンディアン バイト順を決定します。**Number Type** 引数と **Endian** 引数は適用されません。 この引数を有効にした場合は、他の特定の DCE/RPC キーワードと組み合わせて `byte_math` を使用することもできます。

次の表に示すいずれか1つの引数を使用して、パケット内のストリング データをシステムがどのように表示するかを定義します。

表 *180 :* 番号タイプ引数

引数	説明
Hexadecimal String	ストリング データを 16 進形式で表現します。
Decimal String	ストリング データを 10 進形式で表現します。
Octal String	ストリング データを 8 進形式で表現します。

たとえば、次のような値を byte_math に設定した場合、

- Bytes = 2
- Offset = 0
- Operator = *
- RValue = height
- Result Variable = area

ルール エンジンは、パケット内の最初の 2 バイトに記述された番号を抽出し、RValue（既存の変数 height を使用）を乗じて新しい変数 area を作成します。

表 *181 : byte_math* 変数を使用できる引数

キーワード	引数
byte_jump	Offset
byte_test	Offset、Value
byte_extract	Offset
isdataat	Offset

概要：pcre キーワード

pcre キーワードを使用すると、指定されたコンテンツをパケット ペイロード内で検査するために Perl 互換正規表現（PCRE）を使用できます。PCRE を使用すると、同じ内容のわずかなバリエーションにそれぞれ一致する複数のルールを作成する手間が省けます。

正規表現は、さまざまな方法で表現されることのあるコンテンツを検索する場合に役立ちます。パケットのペイロード内でコンテンツを検索するときには、コンテンツがさまざまな属性を持つ可能性があることを考慮すべき場合があります。

侵入ルールで使われる正規表現構文は完全な正規表現ライブラリのサブセットであり、完全なライブラリ内のコマンドで使用される構文とはいくつかの点で異なることに注意してください。侵入ルール エディタを使用して pcre キーワードを追加するときには、次の形式で完全な値を入力します。

```
!/pcre/ ismxAEGRBUIPHDMCKSY
```

引数の説明

- 「!」は否定オプションです（正規表現に**一致しない**パターンを照合する場合に使用します）。
- /pcre/ は Perl 互換正規表現です。
- ismxAEGRBUIPHDMCKSY は修飾子オプションの任意の組み合わせです。

また、次の表に示す文字をエスケープする必要があることに注意してください。これにより、パケット ペイロード内で特定のコンテンツを検索するために PCRE でこれらの文字を使用した場合、ルール エンジンがそれを正しく解釈するようになります。

表 *182 :* エスケープする *PCRE* 文字

エスケープする必要のある文字	バックスラッシュを使用した場合	16進コードを使用した場合
#（ナンバー記号）	\#	\x23
;（セミコロン）	\;	\x3B
|（縦棒）	\\|	\x7C
:（コロン）	\:	\x3A

`m?regex?` を使用することもできます。ここで、`?` は「/」以外のデリミタです。正規表現内でスラッシュと一致させる必要があり、バックスラッシュを使ってそれをエスケープしたくない場合には、これを使用できます。たとえば、「`m?`regex`? ismxAEGRBUIPHDMCKSY`」のように使用できます。regex は Perl 互換正規表現、`ismxAEGRBUIPHDMCKSY` は修飾子オプションの任意の組み合わせです。

ヒント 必要に応じて、Perl 互換正規表現を引用符で囲むことができます。たとえば、pcre_expression は "pcre_expression" となります。引用符が任意ではなく必須であった旧バージョンに慣れている経験豊富なユーザのために、引用符を使用するオプションが提供されています。保存後のルールを侵入ルール エディタで表示すると、引用符が表示されません。

PCRE の構文

`pcre` キーワードでは、標準の Perl 互換正規表現（PCRE）構文を使用できます。以下の項では、この構文について説明します。

ヒント ここでは PCRE で使用可能な基本的な構文について説明しますが、Perl および PCRE 専用のオンライン リファレンスやブックで、さらに詳しい情報を参照することもできます。

メタ文字

メタ文字は正規表現内で特別な意味を持つリテラル文字です。メタ文字を正規表現内で使用するときには、その前にバックスラッシュを付けて「エスケープする」必要があります。

次の表に、PCRE で使用可能なメタ文字について説明し、それぞれの例を示します。

表 *183 : PCRE* メタ文字

メタ文字	説明	例
。	改行以外の任意の文字と一致します。修飾オプションとして s が使用されている場合は、改行文字も含まれます。	abc. は、abcd、abc1、abc# などと一致します。
*。	ある文字または式の 0 回以上の出現と一致します。	abc* は、abc、abcc、abccc、abcccccc などと一致します。
?	ある文字または式の 0 回または 1 回の出現と一致します。	abc? は abc に一致します。
+	ある文字または式の 1 回以上の出現と一致します。	abc+ は、abc、abcc、abccc、abcccccc などと一致します。
()	式をグループ化します。	(abc)+ は、abc、abcabc、abcabcabc などと一致します。
{}	ある文字または式の一致回数の限度を指定します。下限と上限を設定する場合には、下限と上限をカンマで区切ります。	a{4,6} は、aaaa、aaaaa、または aaaaaa と一致します。 (ab){2} は abab と一致します。
[]	文字クラスを定義できます。セットの中で記述される任意の文字または文字の組み合わせに一致します。	[abc123] は、a または b または c などと一致します。
^	文字列の先頭でコンテンツを照合します。また、文字クラスの中で否定としても使用されます。	^in は、info 内の “in” と一致しますが、bin では一致しません。[^a] は、a を含まない任意の文字列と一致します。
$	文字列の末尾でコンテンツを照合します。	ce$ は、announce 内の “ce” と一致しますが、cent では一致しません。
|	OR 式を示します。	(MAILTO|HELP) は、MAILTO または HELP と一致します。
\	メタ文字を実際の文字として使用できます。また、事前定義された文字クラスを指定するためにも使われます。	\. はピリオドと一致し、* はアスタリスクと一致し、\\ はバックスラッシュと一致します。\d は数字と一致し、\w は英数字と一致します。

文字クラス

文字クラスには、英字、数字、英数字、および空白文字があります。大カッコで囲んで独自の文字クラスを作成できます。また、事前定義のクラスをさまざまな文字タイプのショートカットとして使用することもできます。追加の修飾子なしで文字クラスを使用すると、1 つの文字クラスは 1 桁または 1 文字に一致します。

次の表に、PCRE で使用できる事前定義の文字クラスの説明と例を示します。

表 *184 : PCRE* 文字クラス

文字クラス	説明	文字クラスの定義
\d	数字（桁）と一致します。	[0-9]
\D	数字以外の任意の文字と一致します。	[^0-9]
\w	英数字（語）と一致します。	[a-zA-Z0-9_]
\W	英数字以外の任意の文字と一致します。	[^a-zA-Z0-9_]
\s	スペース、復帰、タブ、改行、および改ページを含む空白文字と一致します。	[\r\t\n\f]
\S	空白文字以外の任意の文字と一致します。	[^ \r\t\n\f]

PCRE 修飾子のオプション

pcre キーワードの値の中で正規表現構文を指定した後、修飾オプションを使用できます。これらの修飾子は、Perl、PCRE、および Snort 固有の処理機能を実行します。修飾子は、常に PCRE 値の末尾に、次の形式で出現します。

```
/pcre/ismxAEGRBUIPHDMCKSY
```

ここで、ismxAEGRBUPHMC には、次の表に示す任意の修飾オプションを含めることができます。

ヒント オプションで、正規表現と修飾オプションを引用符で囲むことができます（たとえば "/pcre/ismxAEGRBUIPHDMCKSY"）。引用符が任意ではなく必須であった旧バージョンに慣れている経験豊富なユーザのために、引用符を使用するオプションが提供されています。保存後のルールを侵入ルール エディタで表示すると、引用符が表示されません。

次の表に、Perl 処理機能を実行するために使用できるオプションを説明します。

表 *185 : Perl* 関連の正規表現後オプション

オプション	説明
i	正規表現で大文字と小文字を区別しないようにします。
s	ドット文字（.）は、改行または \n 文字を除くすべての文字を表します。オプションとして "s" を使用すると、これをオーバーライドして、改行文字を含むすべての文字をドット文字に一致させることができます。

オプション	説明
m	デフォルトで、1 つの文字列は複数文字からなる単一行として扱われ、^ と $ は特定の文字列の先頭および末尾に一致します。オプションとして "m" を使用すると、^ および $ はバッファの先頭または末尾だけでなく、バッファ内の改行文字の直前または直後のコンテンツとも一致します。
x	エスケープされた（バックスラッシュが先行する）場合、および文字クラスに含まれる場合を除き、空白データ文字がパターン内に出現してもそれを無視します。

次の表に、正規表現の後ろに使用できる PCRE 修飾子の説明を示します。

表 *186 : PCRE* 関連の正規表現後オプション

オプション	説明
A	文字列の先頭でパターンが一致する必要があります（正規表現で ^ を使用した場合と同じ）。
E	対象の文字列の末尾でのみ一致するように $ を設定します（E を伴わない $ は、それが改行である場合には最後の文字の直前とも一致しますが、他の改行文字の直前とは一致しません）。
G	デフォルトでは、* + と ? は「最長マッチ」を実行します。つまり、複数の一致が見つかった場合は最も長い一致が選択されます。G 文字を使用するとこの動作が変更され、常に最初の一致がこれらの文字で選択されます。ただし後ろに疑問符（?）が続く場合を除きます。たとえば、*? +? と ?? は G 修飾子を使った構造内で最長マッチを実行し、疑問符が付いていない *、+、または ? は最長マッチではありません。

次の表に、正規表現の後ろに使用できる Snort 固有の修飾子の説明を示します。

.

表 *187 : Snort* 固有の正規表現後の修飾子

オプション	説明
R	ルールエンジンで見つかった最後の一致の末尾を基準にして、一致するコンテンツを検索します。
B	プリプロセッサによってデコードされる前のデータ内のコンテンツを検索します（このオプションは、`content` または `protected_content` キーワードで `Raw Data` 引数を使用する場合と似ています）。

オプション	説明
U	HTTP Inspect プリプロセッサによってデコードされた正規化済み HTTP 要求メッセージの URI 内のコンテンツを検索します。このオプションと `content` または `protected_content` キーワードの **HTTP URI** オプションを一緒に使用して、同じコンテンツを検索することはできません。 パイプライン処理された HTTP 要求パケットには複数の URI が含まれていることに注意してください。U オプションを含む PCRE 式を使用すると、ルールエンジンは、パイプライン処理された HTTP 要求パケット内の最初の URI でのみコンテンツ一致を検索します。パケット内のすべての URI を検索するには、**HTTP URI** を選択して `content` または `protected_content` キーワードを使用します。U オプションを含む PCRE 式を一緒に使用するかどうかは問いません。
I	HTTP Inspect プリプロセッサによってデコードされた raw HTTP 要求メッセージの URI 内のコンテンツを検索します。このオプションと `content` または `protected_content` キーワードの **HTTP Raw URI** オプションを一緒に使用して、同じコンテンツを検索することはできません。
P	HTTP Inspect プリプロセッサによってデコードされた正規化済み HTTP 要求メッセージ本文の中でコンテンツを検索します。
H	HTTP Inspect プリプロセッサによってデコードされた HTTP 要求または応答メッセージの（cookie を除く）ヘッダー内のコンテンツを検索します。このオプションと `content` または `protected_content` キーワードの **HTTP Header** オプションを一緒に使用して、同じコンテンツを検索することはできません。
D	HTTP Inspect プリプロセッサによってデコードされた未加工の HTTP 要求または応答メッセージの（cookie を除く）ヘッダー内のコンテンツを検索します。このオプションと `content` または `protected_content` キーワードの **HTTP Raw Header** オプションを一緒に使用して、同じコンテンツを検索することはできません。
M	HTTP Inspect プリプロセッサによってデコードされた正規化済み HTTP 要求メッセージのメソッドフィールド内のコンテンツを検索します。メソッドフィールドは、URI で識別されるリソースに対して実行すべきアクション（GET、PUT、CONNECT など）を特定します。

オプション	説明
C	HTTP Inspect プリプロセッサの [Inspect HTTP Cookies] オプションが有効になっている場合は、HTTP 要求見出しの cookie 内の正規化済みコンテンツを検索します。さらに、プリプロセッサの [Inspect HTTP Responses] オプションが有効になっている場合は、HTTP 応答見出しの set-cookie 内も検索します。[Inspect HTTP Cookies] が有効になっていない場合は、cookie または set-cookie データを含む見出し全体を検索します。 次の点に注意してください。 • メッセージ本文に含まれる cookie は、本文のコンテンツとして扱われます。 • このオプションと `content` または `protected_content` キーワードの **HTTP Cookie** オプションを一緒に使用して、同じコンテンツを検索することはできません。 • `Cookie:` 見出し名と `Set-Cookie:` 見出し名、見出し行の先行スペース、および見出し行の終わりを示す `CRLF` は cookie の一部としてではなく、見出しの一部として検査されます。
K	HTTP Inspect プリプロセッサの [Inspect HTTP Cookies] オプションが有効になっている場合は、HTTP 要求見出しの cookie 内の未加工コンテンツを検索します。さらに、プリプロセッサの [Inspect HTTP Responses] オプションが有効になっている場合は、HTTP 応答見出しの set-cookie 内も検索します。[Inspect HTTP Cookies] が有効になっていない場合は、cookie または set-cookie データを含む見出し全体を検索します。 次の点に注意してください。 • メッセージ本文に含まれる cookie は、本文のコンテンツとして扱われます。 • このオプションと `content` または `protected_content` キーワードの **HTTP Raw Cookie** オプションを一緒に使用して、同じコンテンツを検索することはできません。 • `Cookie:` 見出し名と `Set-Cookie:` 見出し名、見出し行の先行スペース、および見出し行の終わりを示す `CRLF` は cookie の一部としてではなく、見出しの一部として検査されます。
S	HTTP 応答内の 3 桁のステータス コードを検索します。
Y	HTTP 応答内のステータス コードに付加されるテキスト記述を検索します。

（注） UオプションとRオプションを組み合わせて使用しないでください。パフォーマンスの問題が発生する可能性があります。また、他のHTTPコンテンツオプション（I、P、H、D、M、C、K、S または Y）と組み合わせて U オプションを使用しないでください。

関連トピック

概要：HTTP content および protected_content キーワードの引数 （2170 ページ）

PCRE のキーワード値の例

次に、pcre で入力できる値の例を示し、それぞれの例で何が一致するかを説明します。

- **/feedback[(\d{0,1})]?\.cgi/U**

この例では、URI データにのみ配置された、feedback の後に 0 個または 1 個の数字、さらに .cgi が続くインスタンスをパケット ペイロード内で検索します。

この例は以下のものと一致します。

- feedback.cgi
- feedback1.cgi
- feedback2.cgi
- feedback3.cgi

この例は、以下のものとは**一致しません**。

- feedbacka.cgi
- feedback11.cgi
- feedback21.cgi
- feedbackzb.cgi

- **/^ez(\w{3,5})\.cgi/iU**

この例では、先頭の ez の後に 3 ～ 5 文字の単語、さらに .cgi が続く文字列をパケット ペイロード内で検索します。この検索では大文字と小文字を区別せず、URI データだけを検索します。

この例は以下のものと一致します。

- EZBoard.cgi
- ezman.cgi
- ezadmin.cgi
- EZAdmin.cgi

この例は、以下のものとは**一致しません**。

- ezez.cgi
- fez.cgi
- abcezboard.cgi
- ezboardman.cgi

- **/mail(file|seek)\.cgi/U**

この例では、URI データ内の mail の後に file と seek のどちらかが続くインスタンスをパケット ペイロードで検索します。

この例は以下のものと一致します。

- mailfile.cgi
- mailseek.cgi

この例は、以下のものとは**一致しません**。

- MailFile.cgi
- mailfilefile.cgi

- **m?http\\x3a\x2f\x2f.*(\n|\t)+?U**

この例では、任意の数の文字の後ろにある、HTTP 要求内のタブまたは改行文字を示す URI コンテンツをパケット ペイロード内で検索します。この例では、式で m?regex? を使用して、http\:\/\/ を使用しないようにしています。コロンの前にバックスラッシュがあることに注意してください。

この例は以下のものと一致します。

- http://www.example.com?scriptvar=x&othervar=\n\..\..
- http://www.example.com?scriptvar=\t

この例は、以下のものとは**一致しません**。

- ftp://ftp.example.com?scriptvar=&othervar=\n\..\..
- http://www.example.com?scriptvar=|/bin/sh -i|

- **m?http\\x3a\x2f\x2f.*=\|.*\|+?sU**

この例では、（改行を含む）任意の数の文字の後に 1 つの等号、さらに任意の数の文字または空白を含むパイプ文字が続くという構成の URL をパケット ペイロード内で検索します。この例では、式で m?regex? を使用して、http\:\/\/ を使用しないようにしています。

この例は以下のものと一致します。

- http://www.example.com?value=|/bin/sh/ -i|
- http://www.example.com?input=|cat /etc/passwd|

この例は、以下のものとは**一致しません**。

- `ftp://ftp.example.com?value=|/bin/sh/ -i|`
- `http://www.example.com?value=x&input?|cat /etc/passwd|`
- **`/[0-9a-f]{2}\:[0-9a-f]{2}\:[0-9a-f]{2}\:[0-9a-f]{2}\:[0-9a-f]{2}\:[0-9a-f]{2}/i`**

この例では、MAC アドレスをパケット ペイロード内で検索します。コロン文字がバックスラッシュでエスケープされていることに注意してください。

metadata キーワード

`metadata` キーワードを使用すると、記述情報をルールに追加できます。また、`metadata` キーワードを `service` 引数とともに使用すると、ネットワーク トラフィック内のアプリケーションとポートを特定することができます。追加する情報を使用して、要件に適合するルールを編成または識別することができ、追加する情報や `service` 引数についてルールを検索することができます。

システムは次の形式の引数に基づいてメタデータを検証します。

key value

ここで、*key* と *value* は、スペースで区切られた記述の組み合わせです。これは、Cisco 提供のルールにメタデータを追加するために Cisco Talos Intelligence Group（Talos） VRT で使用されている形式です。

または、次の形式を使用することもできます。

key = *value*

たとえば、*key value* 形式で次のようにカテゴリとサブカテゴリを使用し、作成者と日付によってルールを識別できます。

```
author SnortGuru_20050406
```

1 つのルール内で複数の `metadata` キーワードを使用できます。また、以下の例に示すように、単一の `metadata` キーワード内で複数の *key value* 引数をカンマで区切ることもできます。

```
author SnortGuru_20050406, revised_by SnortUser1_20050707,
revised_by SnortUser2_20061003,
revised_by SnortUser1_20070123
```

使用できる形式は *key value* と *key*=*value* だけに限定されません。ただし、これらの形式に基づく検証に起因する制限事項を把握しておく必要があります。

注意すべき制限のある文字

次の文字制限に注意してください。

- セミコロン（;）またはコロン（:）を使用しないでください。

- システムはカンマを、複数の *key value* 引数または *key=value* 引数の区切り文字であると解釈します。次に例を示します。

  key value,*key value*,*key value*

- システムは等号（=）または余白文字を、*key* と *value* の間の区切り文字であると解釈します。次に例を示します。

  key value

  key=value

その他のすべての文字が使用可能です。

注意すべき予約済みメタデータ

`metadata` キーワードでは、次の単語を単一の引数として、または *key value* 引数内の *key* として使用しないでください。これらは Talos 用に予約されています。

```
application
engine
impact_flag
os
policy
rule-type
rule-flushing
soid
```

（注） ローカル ルールを適切に機能させるために制限付きメタデータをどうしても追加する必要がある場合は、サポート担当にお問い合わせください。

影響レベル 1

`metadata` キーワードでは、次に示す予約済み *key value* 引数を使用できます。

```
impact_flag red
```

この *key value* 引数は、インポートしたローカル ルールまたは侵入ルール エディタを使って作成したカスタム ルールに関する影響フラグを赤（レベル 1）に設定します。

「送信元または宛先のホストがウイルス、トロイの木馬、その他の有害ソフトウェアによって侵害されている可能性があることを、ルールをトリガーしているパケットが示している」と Talos が判断した場合、Talos は Cisco 提供のルールに `impact_flag red` 引数を含めます。

関連トピック

ローカル侵入ルールのインポートのガイドライン （190 ページ）
侵入イベントのクリップボード （3102 ページ）

サービス メタデータ

システムは、ネットワークのホストで動作しているアプリケーションを検出し、ネットワークトラフィックにアプリケーションプロトコル情報を挿入します。これは、検出ポリシーの設定に関係なく実行されます。TCP または UDP ルールで `metadata` キーワード `service` 引数を使用して、ネットワーク トラフィックのアプリケーション プロトコルとポートを照合することができます。ルールで 1 つ以上の `service` アプリケーション引数を単一のポート引数と組み合わせることができます。

サービス アプリケーション

`metadata` キーワードとともに `service` を *key* として、アプリケーションを *value* として使用し、パケットを識別されたアプリケーションプロトコルと一致させることができます。たとえば、次に示す `metadata` キーワード内の *key value* 引数は、ルールを HTTP トラフィックに関連付けます。

```
service http
```

複数のアプリケーションをカンマで区切って指定することもできます。次に例を示します。

```
service http, service smtp, service ftp
```

注意 侵入ルールでサービス メタデータを使用するためには、適応型プロファイルの設定（2466 ページ） で説明されているように、アダプティブ プロファイルを有効（デフォルト状態）にする**必要があります**。

次の表に、`service` キーワードとともに使用される最も一般的なアプリケーション値を示します。

（注） 表にないアプリケーションを特定することが難しい場合は、サポートにお問い合わせください。

表 *188 : service* 値

値	説明
`cvs`	Concurrent Versions System（バージョン管理システム）
`dcerpc`	分散コンピューティング環境/リモート プロシージャ コール システム
`dns`	Domain Name System; ドメイン ネーム システム
`finger`	Finger User Information Protocol
`FTP`	File Transfer Protocol
`ftp-data`	ファイル転送プロトコル（データ チャネル）

値	説明
`http`	Hypertext Transfer Protocol
`imap`	Internet Message Access Protocol
`isakmp`	Internet Security Association and Key Management Protocol
`mysql`	My Structured Query Language（構造化照会言語）
`netbios-dgm`	NETBIOS Datagram Service
`netbios-ns`	NETBIOS Name Service
`netbios-ssn`	NETBIOS セッション サービス
`nntp`	Network News Transfer Protocol
`oracle`	Oracle Net Services
`shell`	OS Shell
`pop2`	Post Office Protocol バージョン 2
`pop3`	Post Office Protocol バージョン 3
`smtp`	Simple Mail Transfer Protocol
`snmp`	簡易ネットワーク管理プロトコル
`ssh`	セキュア シェル ネットワーク プロトコル
`sunrpc`	Sun リモート プロシージャ コール プロトコル
`telnet`	Telnet ネットワーク プロトコル
`tftp`	Trivial File Transfer Protocol
`x11`	X Window システム

サービス ポート

`Metadata` キーワードとともに `service` を *key* として、指定したポート引数を *value* として使用し、ルールがアプリケーションと組み合わせてポートを照合する方法を定義できます。

次の表の任意のポート値を、ルールごとに 1 つ指定できます。

表 *189 : service* ポート値

値	説明
`else-ports` または `unknown`	次の条件のいずれかが満たされるとルールが適用されます。 • パケット アプリケーションが既知で、ルール アプリケーションと一致する。 • パケット アプリケーションが不明で、パケット ポートがルール ポートと一致する。 `else-ports` および `unknown` の値では、`service` がポート修飾子なしでアプリケーションプロトコルを指定する場合にシステムで使用されるデフォルトの動作が生成されます。
`and-ports`	パケットアプリケーションが既知で、ルールアプリケーションと一致し、パケット ポートがルール ヘッダーのポートと一致する場合、ルールが適用されます。アプリケーションを指定しないルールで `and-ports` を使用することはできません。
`or-ports`	次の条件のいずれかが満たされるとルールが適用されます。 • パケット アプリケーションが既知で、ルール アプリケーションと一致する。 • パケット アプリケーションが不明で、パケット ポートがルール ポートと一致する。 • パケット アプリケーションはルール アプリケーションと一致せず、パケット ポートはルール ポートと一致する。 • ルールはアプリケーションを指定せず、パケット ポートはルール ポートと一致する。

次の点に注意してください。

- `service` アプリケーション引数を `service and-ports` 引数とともに含める必要があります。
- ルールで上記の表の値が複数指定されている場合、ルールの一番最後にある値が適用されます。
- ポートおよびアプリケーション引数は任意の順序にすることができます。

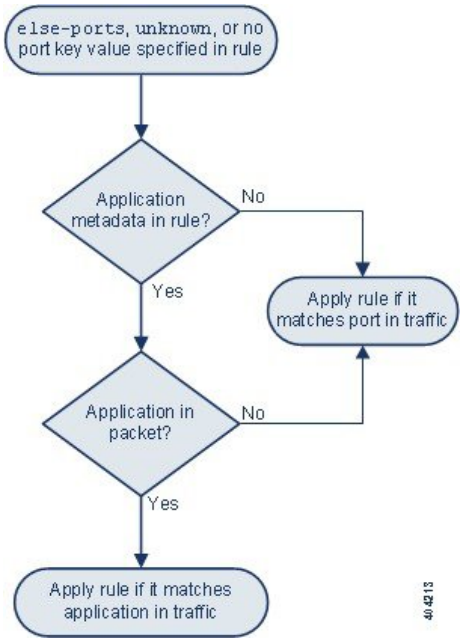
`and-ports` 値を除き、1 つ以上の `service` アプリケーション引数の有無にかかわらず、`service` ポート引数を含めることができます。次に例を示します。

```
service or-ports, service http, service smtp
```

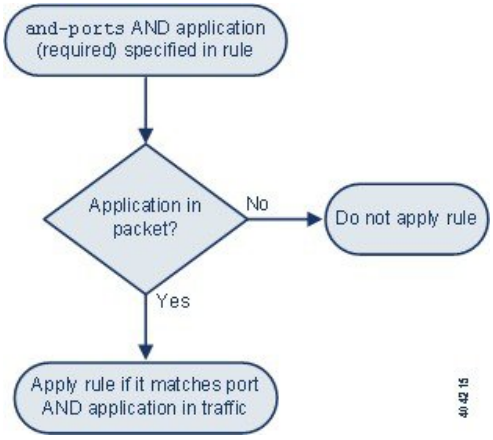
トラフィックのアプリケーションとポート

次の図は、侵入ルールでサポートされるアプリケーションとポートの組み合わせ、およびパケット データにこれらのルール制約を適用した結果を示しています。

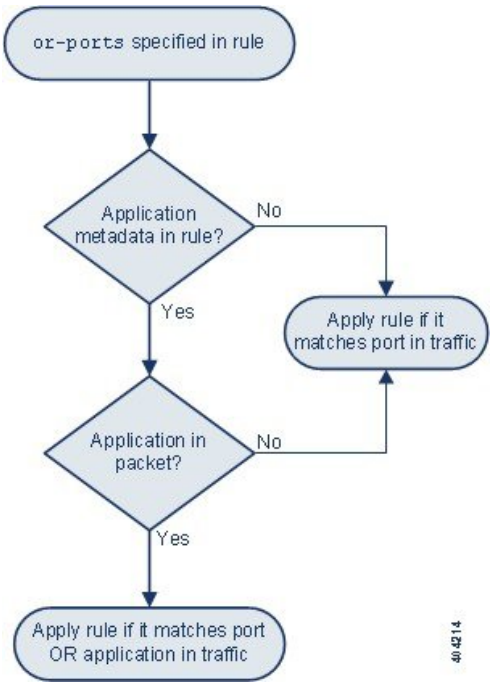
ホスト アプリケーション プロトコル else 送信元/宛先ポート：



ホスト アプリケーション プロトコル and 送信元/宛先ポート：



ホスト アプリケーション プロトコル **or** 送信元/宛先ポート：



一致する例

`metadata` キーワードを `service` 引数とともに使用した次のサンプル ルールを、一致するデータおよび一致しないデータの例とともに示します。

- `alert tcp any any -> any [80,8080] (metadata:service and-ports, service http, service smtp;)`

一致する例	一致しない例
• TCP ポート 80 経由の HTTP トラフィック • TCP ポート 8080 経由の HTTP トラフィック • TCP ポート 80 経由の SMTP トラフィック • TCP ポート 8080 経由の SMTP トラフィック	• ポート 80 または 8080 の POP3 トラフィック • ポート 80 または 8080 の不明なアプリケーション トラフィック • ポート 9999 の HTTP トラフィック

- `alert tcp any any -> any [80,8080] (metadata:service or-ports, service http;)`

一致する例	一致しない例
• あらゆるポートの HTTP トラフィック • ポート 80 の SMTP トラフィック • ポート 8080 の SMTP トラフィック • ポート 80 および 8080 の不明なアプリケーションのトラフィック	• 80 または 8080 以外のポートの非 HTTP および非 SMTP トラフィック

- 次のいずれかの規則：
  - `alert tcp any any -> any [80,8080] metadata:service else-ports, service http;)`
  - `alert tcp any any -> any [80,8080] metadata:service unknown, service http;)`
  - `alert tcp any any -> any [80,8080] metadata:service http;)`

一致する例	一致しない例
• あらゆるポートの HTTP トラフィック • パケット アプリケーションが不明な場合はポート 80 • パケット アプリケーションが不明な場合はポート 8080	• ポート 80 または 8080 の SMTP トラフィック • ポート 80 または 8080 の POP3 トラフィック

メタデータ検索のガイドライン

`metadata` キーワードを使用するルールを検索するには、ルールの [検索（Search）] ページで `metadata` キーワードを選択して、オプションで、メタデータの一部分を入力します。たとえば次のように入力できます。

- `search` と入力すると、*key* として `search` が使用されているすべてのルールが表示されます。
- `search http` と入力すると、*key* として `search`、*value* として `http` がそれぞれ使用されているすべてのルールが表示されます。
- `author snortguru` と入力すると、*key* として `author`、*value* として `SnortGuru` がそれぞれ使用されているすべてのルールが表示されます。
- `author s` と入力すると、*key* として `author`、さらに *value* として `SnortGuru`、`SnortUser1`、`SnortUser2` などの語が使用されているすべてのルールが表示されます。

ヒント *key* と *value* の両方を検索するときには、ルール内の *key value* 引数で使用されているのと同じ接続演算子（等号 [=] または空白文字）を検索で使用してください。*key* の後に等号（=）と空白文字のどちらを入力するかに応じて、異なる結果が検索で返されます。

なお、メタデータ追加のために使用する形式とは無関係に、システムはメタデータ検索語を *key value* または *key=value* 引数の全部または一部として解釈します。たとえば、次に示すメタデータは *key value* または *key=value* 形式に従っていませんが、有効なメタデータです。

```
ab cd ef gh
```

ただし、この例に含まれる各スペースは *key* と *value* の間の区切り文字としてシステムで解釈されます。次に示す並列語や単一語を検索で使用すると、この例のメタデータを含むルールを正しく検出できます。

```
cd ef
ef gh
ef
```

一方、次の検索を使用した場合、単一の *key value* 引数としてシステムによって解釈されるため、ルールを検出できません。

```
ab ef
```

関連トピック

ルールの検索 （2158 ページ）

IP ヘッダー値

キーワードを使用すると、パケットの IP ヘッダーの中で攻撃やセキュリティ ポリシー違反の可能性を識別できます。

fragbits

`fragbits` キーワードは、IP 見出し内のフラグメント ビットと予約ビットを検査します。パケットごとに、予約ビット、More Fragments ビット、および Don't Fragment ビットを任意に組み合わせて検査できます。

表 *190 : Fragbits* 引数の値

引数	説明
R	予約ビット
M	More Fragments ビット

引数	説明
D	Don’t Fragment ビット

fragbits キーワードを使ってルールを微調整するために、次の表に示す演算子をルール内の引数値の後ろに指定できます。

表 *191 : Fragbit* 演算子

演算子	説明
プラス記号（**+**）	パケットは、指定されたすべてのビットと一致する必要があります。
アスタリスク（*****）	パケットは、指定されたどのビットと一致することもできます。
感嘆符（**!**）	指定されたどのビットも設定されていない場合、パケットが基準を満たします。

たとえば、（他のビットの有無とは無関係に）少なくとも予約済みビットが設定されたパケットに対してイベントを生成するには、fragbits 値として R+ を使用します。

id

id キーワードは、キーワード引数で指定される値に照らして IP 見出しフラグメント識別フィールドを検査します。一部のサービス拒否ツールやスキャナは、このフィールドを、容易に検出できる特定の番号に設定します。たとえば、Synscan ポートスキャンを検出する SID 630 では、id 値が 39426（スキャナから伝送されるパケットの ID 番号として使われる静的な値）に設定されます。

（注） id 引数値は数値でなければなりません。

ipopts

IPopts キーワードを使用すると、指定された IP 見出しオプションをパケット内で検索できます。次の表に、使用可能な引数値を示します。

表 *192 : IPoption* 引数

引数	説明
rr	経路を記録
eol	リストの末尾
nop	オペレーションなし
ts	タイム スタンプ

引数	説明
sec	IP セキュリティ オプション
lsrr	厳密でない送信元ルーティング
ssrr	厳密な送信元ルーティング
satid	ストリーム識別子

アナリストが最も頻繁に監視するのは、厳密な送信元ルーティングと厳密でない送信元ルーティングです。これらのオプションは送信元 IP アドレスのスプーフィングを示している可能性があるためです。

ip_proto

`ip_proto` キーワードを使用すると、キーワードの値として指定された IP プロトコルを含むパケットを識別できます。IP プロトコルは 0 ～ 255 の数値として指定できます。これらの番号を、<、>、または ! 演算子と組み合わせることができます。たとえば、ICMP 以外のプロトコルを使用しているトラフィックを検査するには、`ip_proto` キーワードの値として `!1` を使用します。1 つのルール内で `ip_proto` キーワードを複数回にわたって使用できます。ただし、ルール エンジンはキーワードの複数インスタンスをブール和関係（AND）と解釈することに注意してください。たとえば、`ip_proto:!3; ip_proto:!6` を含むルールを作成した場合、このルールは GGP プロトコルおよび TCP プロトコルを使用するトラフィックを無視します。

tos

一部のネットワークでは、ネットワーク上を移動するパケットの優先度を設定するタイプオブサービス（ToS）値が使用されます。`tos` キーワードを使用すると、キーワードの引数で指定された値に照らしてパケットの IP 見出し ToS 値を検査できます。`tos` キーワードを使用するルールは、ToS が指定の値に設定され、しかもルール内の残りの基準を満たすパケットに対してトリガーとして使用されます。

（注） `tos` の引数値は数値でなければなりません。

[ToS] フィールドは IP ヘッダー プロトコルでは非推奨になり、[Differentiated Services Code Point (DSCP)] フィールドに置き換えられています。

ttl

パケットの存続可能時間（time-to-live、ttl）値は、パケットが破棄される前に生成できるホップ数を示します。`ttl` キーワードを使用すると、キーワードの引数として指定された値または値の範囲に照らしてパケットの IP 見出し ttl 値を検査できます。`ttl` キーワード パラメータを 0 や 1 などの低い値に設定すると役立つことがあります。これは、低い存続可能時間値がトレースルートや侵入回避の試みを示している場合があるためです。（ただし、このキーワードの適

切な値は、管理対象デバイスの配置やネットワーク トポロジによって異なります）。次のように構文を使用します。

- TTL 値に特定の 1 つの値を設定するには、0 ～ 255 の整数を使用します。値の前に等号（=）を付けることもできます（たとえば 5 または =5 を指定できます）。
- TTL 値の範囲を指定するには、ハイフン（-）を使用します（たとえば、0-2 は 0 ～ 2 のすべての値、-5 は 0 ～ 5 のすべての値、5- は 5 ～ 255 のすべての値をそれぞれ指定します）。
- 特定の値より大きい TTL 値を指定するには、「大なり」記号（>）を使用します（たとえば、>3 は 3 より大きいすべての値を指定します）。
- 特定の値以上の TTL 値を指定するには、「大なりイコール」記号（>=）を使用します（たとえば、>=3 は 3 以上のすべての値を指定します）。
- 特定の値より小さい TTL 値を指定するには、「小なり」記号（<）を使用します（たとえば、<3 は 3 より小さいすべての値を指定します）。
- 特定の値以下の TTL 値を指定するには、「小なりイコール」記号（<=）を使用します（たとえば、<=3 は 3 以下のすべての値を指定します）。

ICMP ヘッダー値

Firepower システムでサポートされるキーワードを使用すると、ICMP パケット ヘッダー内の攻撃やセキュリティ ポリシー違反を識別できます。なお、ほとんどの ICMP タイプおよびコードを検出する事前定義ルールがあることに注意してください。既存のルールを有効にするか、既存のルールに基づいてローカル ルールを作成することを考慮してください。ICMP ルールを最初から作成するよりも、ニーズを満たすルールを見つける方が時間の節約になる可能性があります。

icmp_id と icmp_seq

ICMP の識別番号とシーケンス番号は、ICMP 応答と ICMP 要求を関連付けるうえで役立ちます。通常のトラフィックでは、これらの値はパケットに動的に割り当てられます。一部のコバート チャネルおよび Distributed Denial of Server（DDoS）プログラムは、静的な ICMP ID およびシーケンス値を使用します。次のキーワードを使用すると、静的な値を含む ICMP パケットを識別できます。

キーワード	定義（Definition）
icmp_id	ICMP エコー要求または応答パケットの ICMP ID 番号を検査します。ICMP ID 番号に対応する数値を `icmp_id` キーワードの引数として使用します。
icmp_seq	`icmp_seq` キーワードは、ICMP エコー要求または応答パケットの ICMP シーケンスを検査します。ICMP シーケンス番号に対応する数値を `icmp_seq` キーワードの引数として使用します。

itype

itype キーワードを使用して、特定の ICMP メッセージ タイプ値を含むパケットを検索します。有効な ICMP タイプ値と無効な ICMP タイプ値のいずれかを指定して、さまざまなタイプのトラフィックを検査できます。たとえば、サービス拒否攻撃やフラッディング攻撃を発生させるために攻撃者が範囲外の ICMP タイプ値を設定することがあります。

「小なり」（<）と「大なり」（>）を使用して itype 引数値の範囲を指定できます。

次に例を示します。

- <35
- >36
- 3<>55

icode

ICMP メッセージには、宛先が到達不能である場合の詳細を示すコード値が含まれることがあります。

icode キーワードを使用すると、特定の ICMP コード値を含むパケットを識別できます。有効な ICMP コード値と無効な ICMP コード値のいずれかを指定することにより、さまざまなタイプのトラフィックを検査できます。

「小なり」（<）と「大なり」（>）を使用して icode 引数値の範囲を指定できます。

次に例を示します。

- 35 より小さい値を検索するには <35 と指定します。
- 36 より大きい値を検索するには >36 と指定します。
- 3 ～ 55 の間にある値を検索するには、3<>55 と指定します。

ヒント icode キーワードと itype キーワードを一緒に使用すると、両方に一致するトラフィックを識別できます。たとえば、ICMP 宛先到達不能コード タイプと ICMP ポート到達不能コード タイプを含む ICMP トラフィックを特定するには、値 3 の itype キーワード（宛先到達不能）と、値 3 の icode キーワード（ポート到達不能）を指定します。

TCP ヘッダー値とストリーム サイズ

Firepower システムでは、パケットの TCP ヘッダーと TCP ストリーム サイズを使って試行される攻撃を識別するためのキーワードを使用できます。

ack

ack キーワードを使用すると、パケットの TCP 確認応答番号と特定の値を比較できます。パケットの TCP 確認応答番号が、ack キーワードに指定された値と一致した場合に、ルールがトリガーとして使用されます。

ack の引数値は数値でなければなりません。

フラグ（Flags）

flags キーワードを使用すると、複数の TCP フラグを任意に組み合わせて指定できます。検査対象のパケットでこれらが設定されている場合、ルールがトリガーとして使用されます。

（注） 従来、flags の値として A+ を使用していたケースでは、代わりに flow キーワードおよび値 established を使用してください。一般に、フラグのすべての組み合わせが検出されるようにするには、フラグの使用時に flow キーワードおよび値 stateless を使用する必要があります。

次の表に示す flags キーワードの値を確認または無視することができます。

表 *193 : flags* の引数

引数	TCP フラグ
Ack	データを確認応答します。
Psh	このパケットでデータが送信される必要があります。
Syn	新しい接続。
Urg	パケットに緊急データが含まれています。
Fin	接続が閉じられました。
Rst	接続が異常終了しました。
CWR	ECN 輻輳ウィンドウが減少しました。旧 R1 引数（下位互換性を維持するために引き続きサポートされています）。
ECE	ECN エコー。旧 R2 引数（下位互換性を維持するために引き続きサポートされています）。

flags キーワードを使用する場合、複数のフラグに対する照合方法をシステムに指示するための演算子を使用できます。次の表に、これらの演算子の説明を示します。

表 *194 : flags* と一緒に使用する演算子

演算子	説明	例
all	パケットは、指定されたすべてのフラグを含んでいる必要があります。	`Urg` と `all` を選択すると、パケットが緊急フラグを含んでいる必要があること、および他のフラグが含まれる可能性があることを指定できます。
any	パケットは、指定された任意のフラグを含むことができます。	`Ack`、`Psh`、および `any` を選択すると、ルールをトリガーとして使用するためには `Ack` と `Psh` のどちらか（または両方）のフラグが設定される必要があること、およびパケット内で他のフラグも設定されている可能性があることを指定できます。
not	パケットは、指定されたフラグセットを**含んではなりません**。	`Urg` と `not` を選択すると、このルールをトリガーとして使用するパケットに関して緊急フラグが設定**されない**ことを指定できます。

flow

`flow` キーワードを使用すると、セッション特性に基づいてルールで検査されるパケットを選択できます。`flow` キーワードを使用することで、ルールの適用対象となるトラフィック フロー方向を指定して、クライアント フローとサーバ フローのどちらかにルールを適用できます。`flow` キーワードによるパケット検査の方法を指定するには、分析すべきトラフィックの方向、検査するパケットの状態、およびパケットが再構築ストリームの一部かどうかを設定できます。

ルールの処理時に、パケットのステートフル インスペクションが実行されます。ステートレス トラフィック（セッション コンテキストが確立されていないトラフィック）を TCP ルールで無視するには、`flow` キーワードをルールに追加して、そのキーワードで **Established** 引数を選択する必要があります。UDP ルールでステートレス トラフィックを無視するには、`flow` キーワードをルールに追加して、**Established** 引数と方向引数のどちらか（または両方）を選択する必要があります。これにより、TCP または UDP ルールでパケットのステートフル インスペクションが実行されます。

方向引数を追加した場合、ルール エンジンは、指定された方向と一致するフローを伴う確立された状態のパケットだけを検査します。たとえば、TCP または UDP 接続が検出されたときトリガーとして使用されるルールに、`flow` キーワードおよび `established` 引数と `From Client` 引数を 追加した場合、ルール エンジンはクライアントから送信されたパケットだけを検査します。

ヒント パフォーマンスを最大にするには、必ず TCP ルールまたは UDP セッション ルールに `flow` キーワードを含めてください。

次の表に、`flow` キーワードで指定できるストリーム関連引数の説明を示します。

表 *195 : flow* の状態関連引数

引数	説明
Established	確立された接続でトリガーとして使用されます。
Stateless	ストリーム プロセッサの状態に関係なくトリガーとして使用されます。

次の表に、`flow` キーワードで指定できる方向オプションの説明を示します。

表 *196 : flow* の方向引数

引数	説明
To Client	サーバ応答でトリガーとして使用されます。
To Server	クライアント応答でトリガーとして使用されます。
From Client	クライアント応答でトリガーとして使用されます。
From Server	サーバ応答でトリガーとして使用されます。

`From Server` と `To Client` の機能が同じであること、および `To Server` と `From Client` の機能も同じであることに注意してください。これらのオプションは、ルールに文脈と読みやすさを加味するために提供されています。たとえば、サーバからクライアントへの攻撃を検出するよう設計されたルールを作成する場合は、`From Server` を使用します。一方、クライアントからサーバへの攻撃を検出するように設計されたルールを作成する場合は、`From Client` を使用します。

次の表に、`flow` キーワードで指定できるストリーム関連引数の説明を示します。

表 *197 : flow* のストリーム関連引数

引数	説明
Ignore Stream Traffic	再構築されたストリーム パケットでトリガーとして使用されません。
Only Stream Traffic	再構築されたストリーム パケットでのみトリガーとして使用されます。

たとえば、`flow` キーワードの値として `To Server, Established, Only Stream Traffic` を使用すると、ストリームプリプロセッサで再構築された、確立済みセッションでクライアントからサーバに移動するトラフィックを検出できます。

seq

`seq` キーワードを使用すると、静的なシーケンス番号値を指定できます。パケットのシーケンス番号が、指定された引数と一致する場合、そのキーワードを含むルールがトリガーとして使

用されます。このキーワードはあまり使用されませんが、静的シーケンス番号付きの生成済みパケットを使用する攻撃やネットワーク スキャンを識別するうえでこれが役立ちます。

window

`window` キーワードを使用すると、特定の TCP ウィンドウ サイズを指定できます。このキーワードを含むルールは、指定された TCP ウィンドウ サイズのパケットが検出されるたびにトリガーされます。このキーワードはあまり使用されませんが、静的 TCP ウィンドウ サイズ付きの生成済みパケットを使用する攻撃やネットワーク スキャンを識別するうえでこれが役立ちます。

stream_size

次に示す形式で、`stream_size` キーワードとストリーム プリプロセッサを組み合わせて使用すると、TCP ストリームのサイズをバイト単位で特定できます。

```
direction,operator,bytes
```

ここで、bytes はバイト数です。引数内の各オプションをカンマ（,）で区切る必要があります。

次の表は、`stream_size` キーワードで指定できる大文字/小文字を区別しない方向オプションを示しています。

表 *198 : stream_size* キーワードの方向引数

引数	説明
クライアント	指定されたストリーム サイズに一致するクライアントからのストリームでトリガーとして使用されます。
server	指定されたストリーム サイズに一致するサーバからのストリームでトリガーとして使用されます。
both	指定されたストリーム サイズに一致するクライアントからのトラフィックとサーバからのトラフィックの両方によってトリガーとして使用されます。 たとえば `both, >, 200` という引数は、クライアントからのトラフィックが 200 バイトを超え、しかもサーバからのトラフィックが 200 バイトを超えている場合にトリガーとして使用されます。
either	指定されたストリーム サイズに一致するクライアントまたはサーバからのトラフィック（どちらか先に出現した方）によってトリガーとして使用されます。 たとえば `both, >, 200` という引数は、クライアントからのトラフィックが 200 バイトを超え、しかもサーバからのトラフィックが 200 バイトを超えている場合にトリガーとして使用されます。

次の表に、`stream_size` キーワードで使用できる演算子の説明を示します。

表 *199 : stream_size* キーワードの引数演算子

演算子	説明
=	等しい
!=	等しくない
>	より大きい
<	より小さい
>=	以上
<=	以下

たとえば、クライアントからサーバに移動する 5001216 バイト以上の TCP ストリームを検出するには、`stream_size` キーワードの引数として `client, >=, 5001216` を使用できます。

stream_reassembly キーワード

`stream_reassemble` キーワードを使用すると、接続での検査対象トラフィックがルールの条件と一致した場合に、1 つの接続の TCP ストリーム再構築を有効/無効にすることができます。オプションで、このキーワードを 1 つのルール内で複数回使用することができます。

ストリーム再構築を有効または無効にするには、次の構文を使用します。

```
enable|disable, server|client|both, option, option
```

次の表に、`stream_reassemble` キーワードで使用できるオプション引数の説明を示します。

表 *200 : stream_reassemble* のオプション引数

引数	説明
noalert	ルールで他にどの検出オプションが指定されているかに関係なく、イベントを生成しません。
fastpath	一致の検出時に残りの接続トラフィックを無視します。

たとえば、次のルールは、HTTP 応答で 200 OK ステータス コードが検出される接続に対してイベントを生成せずに、TCP クライアント側ストリーム再構築を無効にします。

```
alert tcp any 80 -> any any (flow:to_client, established; content: “200 OK”;
stream_reassemble:disable, client, noalert
```

SSL キーワード

SSL ルール キーワードを使用すると、Secure Sockets Layer（SSL）プリプロセッサを呼び出し、暗号化セッションのパケットから SSL のバージョンとセッション状態に関する情報を抽出できます。

SSL または Transport Layer Security（TLS）を使用する暗号化セッションを確立するためにクライアントとサーバが通信するとき、ハンドシェイク メッセージが交換されます。セッション中に伝送されるデータは暗号化されますが、ハンドシェイク メッセージは暗号化されません。

SSL プリプロセッサは、特定のハンドシェイク フィールドから状態とバージョンの情報を抽出します。ハンドシェイク内の 2 つのフィールドは、セッション暗号化に使われる SSL または TLS のバージョンとハンドシェイクのステージを示します。

ssl_state

`ssl_state` キーワードを使用すると、暗号化されたセッションの状態情報と照合することができます。同時に使用される複数の SSL バージョンを検査するには、1 つのルール内で複数の `ssl_version` キーワードを使用します。

ルールで `ssl_state` キーワードが使用されている場合、ルール エンジンは SSL プリプロセッサを呼び出して、トラフィック内の SSL 状態情報を検査します。

たとえば、チャレンジ長が非常に長く、データが多すぎる `ClientHello` メッセージを送信することによってサーバ上のバッファ オーバーフローを引き起こそうとする攻撃者の試みを検出するには、`ssl_state` キーワードと引数 `client_hello` を使用し、異常に大きなパケットを検査することができます。

SSL 状態に関する複数の引数を指定するには、カンマ区切りのリストを使用します。複数の引数を列挙した場合、システムは OR 演算子を使ってそれらを評価します。たとえば、引数として `client_hello` および `server_hello` を指定すると、システムは `client_hello` または `server_hello` のどちらかを含むトラフィックに照らしてルールを評価します。

次のように、引数を除外することもできます。

```
!client_hello, !unknown
```

接続が一連の状態のそれぞれに到達したことを確認するには、ssl_state ルール オプションを使用する複数のルールを使う必要があります。`ssl_state` キーワードは、次の識別子を引数として受け入れます。

表 *201 : ssl_state* の引数

引数	目的
`client_hello`	クライアントが暗号化セッションを要求する、メッセージ タイプ `ClientHello` のハンドシェイク メッセージを照合します。
`server_hello`	クライアントからの暗号化セッション要求に対してサーバが応答する、メッセージ タイプ `ServerHello` のハンドシェイク メッセージを照合します。

引数	目的
client_keyx	サーバからのキーの受信を確認するためにクライアントがサーバにキーを伝送する、メッセージ タイプ ClientKeyExchange のハンドシェイク メッセージを照合します。
server_keyx	サーバからのキーの受信を確認するためにクライアントがサーバにキーを伝送する、メッセージ タイプ ServerKeyExchange のハンドシェイク メッセージを照合します。
unknown	任意のハンドシェイク メッセージ タイプを照合します。

ssl_version

ssl_version キーワードを使用すると、暗号化されたセッションのバージョン情報と照合することができます。ルールで ssl_version キーワードが使用されている場合、ルール エンジンは SSL プリプロセッサを呼び出して、トラフィック内の SSL バージョン情報を検査します。

たとえば、SSL バージョン 2 にバッファ オーバーフロー脆弱性があることがわかっている場合、ssl_version キーワードで sslv2 引数を使用して、その SSL バージョンを使用するトラフィックを識別できます。

SSL バージョンに関する複数の引数を指定するには、カンマ区切りのリストを使用します。複数の引数を列挙した場合、システムは OR 演算子を使ってそれらを評価します。たとえば、SSLv2 を使用していない暗号化トラフィックを識別するには、ssl_version:ssl_v3,tls1.0,tls1.1,tls1.2 をルールに追加できます。このルールは、SSL バージョン 3、TLS バージョン 1.0、TLS バージョン 1.1、または TLS バージョン 1.2 を使用するトラフィックを評価します。

ssl_version キーワードは、次の SSL/TLS バージョン識別子を引数として受け入れます。

表 *202: ssl_version* の引数

引数	目的
sslv2	Secure Sockets Layer（SSL）バージョン 2 を使用してエンコードされたトラフィックを照合します。
sslv3	Secure Sockets Layer（SSL）バージョン 3 を使用してエンコードされたトラフィックを照合します。
tls1.0	Transport Layer Security（TLS）バージョン 1.0 を使用してエンコードされたトラフィックを照合します。
tls1.1	Transport Layer Security（TLS）バージョン 1.1 を使用してエンコードされたトラフィックを照合します。
tls1.2	Transport Layer Security（TLS）バージョン 1.2 を使用してエンコードされたトラフィックを照合します。

appid キーワード

パケットからアプリケーションプロトコル、クライアントアプリケーション、Webアプリケーションを特定するために appid キーワードを使用できます。たとえば、ある脆弱性をもつことが知られている特定のアプリケーションを検出することを考えます。

侵入ルールの appid キーワードの中で、[AppID の設定（Configure AppID）] をクリックし、検出するアプリケーションを 1 つまたは複数選択します。

使用可能なアプリケーションの参照

条件の作成を初めて開始するときは、[使用可能なアプリケーション（Available Applications）] リストは制約されておらず、システムが検出するすべてのアプリケーションをページごとに 100 個ずつ表示します。

- アプリケーションを確認していくには、リストの下にある矢印をクリックします。
- アプリケーションの特性に関するサマリー情報と参照できるインターネットの検索リンクが示されているポップアップ ウィンドウを表示するには、アプリケーションの横にある情報アイコン（  ）をクリックします。

アプリケーション フィルタの使用

照合するアプリケーションを見つけやすくするために、[Available Applications] リストを次のように制約できます。

- アプリケーションを検索するには、リスト上部にある [Search by name] プロンプトをクリックし、名前を入力します。入力していくと、リストが更新されて一致するアプリケーションが表示されます。
- フィルタを適用してアプリケーションを制約するには、[アプリケーション フィルタ（Application Filters）] リストを使用します。フィルタを適用すると、[使用可能なアプリケーション（Available Applications）] リストが更新されます。便宜上、システムはロック解除アイコン（）を使用して、復号化されたトラフィック（暗号化されているトラフィックまたは暗号化されていないトラフィックではなく）でのみ識別できるアプリケーションをマークします。

（注） [アプリケーション フィルタ（Application Filters）] リストで 1 つ以上のフィルタを選択し、しかも [使用可能なアプリケーション（Available Applications）] リストを検索した場合、選択内容と検索フィルタ適用後の [使用可能なアプリケーション（Available Applications）] リストが AND 演算を使って結合されます。

アプリケーションの選択

アプリケーションを 1 つだけ選択するには、そのアプリケーションを選択し、[ルールへの追加（Add to Rule）] をクリックします。フィルタで限定されている現在の表示のすべてのアプリケーションを選択するには、右クリックして [すべて選択（Select All）] を選択します。

アプリケーション層プロトコル値

アプリケーション層プロトコル値の正規化と検査はほとんどがプリプロセッサによって実行されますが、種々のプリプロセッサオプションを使用して、アプリケーション層値をさらに検査できます。

RPC キーワード

`rpc` キーワードは、TCP または UDP パケットでオープン ネットワーク コンピューティング リモート プロシージャ コール（ONC RPC）サービスを識別します。これにより、ホスト上の RPC プログラムの識別試行を検出することができます。ネットワークで実行中のいずれかの RPC サービスを exploit できるかどうか判断するために、侵入者は RPC ポートマッパーを使用できます。また、ポートマッパーを使用せずに RPC を実行中の他のポートへのアクセスを試みることもできます。次の表に、`rpc` キーワードで使用できる引数を列挙します。

表 *203 : rpc* キーワードの引数

引数	説明
application	RPC アプリケーション番号
procedure	呼び出される RPC プロシージャ
version	RPC バージョン

`rpc` キーワードの引数を指定するには、次の構文を使用します。

```
application,procedure,version
```

ここで、application は RPC アプリケーション番号、procedure は RPC プロシージャ番号、version は RPC バージョン番号です。`rpc` キーワードのすべての引数を指定する必要があります。引数のいずれかを指定できない場合は、アスタリスク（`*`）で置き換えてください。

たとえば、任意のプロシージャまたはバージョンの RPC ポートマッパー（100000 という番号で示される RPC アプリケーション）を検索するには、引数として `100000,*,*` を使用します。

ASN.1 キーワード

`asn1` キーワードを使用すると、さまざまな有害エンコードを検索しながら、パケットまたはパケットの一部分をデコードできます。

次の表に、`asn1` キーワードの引数について説明します。

表 *204 : asn.1* キーワードの引数

引数	説明
Bitstring Overflow	無効な、リモート exploit 可能なビットストリング エンコードを検出します。
Double Overflow	標準バッファより大きい二重 ASCII エンコードを検出します。これは Microsoft Windows の悪用可能な機能であることが知られていますが、現時点でどのサービスが悪用可能であるかは不明です。
Oversize Length	指定された引数より大きい ASN.1 タイプ長を検出します。たとえば Oversize Length を 500 に設定した場合、500 を上回る ASN.1 タイプによってルールがトリガーとして使用されます。
Absolute Offset	パケット ペイロードの先頭からの絶対オフセットを設定します（offset カウンタがバイト 0 から始まることに注意してください）。たとえば SNMP パケットをデコードするには、Absolute Offset を 0 に設定し、Relative Offset を設定しません。Absolute Offset として正または負の値が可能です。
Relative Offset	これは、最後に見つかったコンテンツ一致、`pcre`、または `byte_jump` からの相対オフセットです。コンテンツ "foo" の直後の ASN.1 シーケンスをデコードするには、Relative Offset を 0 に設定し、Absolute Offset を設定しません。Relative Offset として正または負の値が可能です（オフセット カウンタが 0 から始まることに注意してください）。

たとえば、Microsoft ASN.1 ライブラリにおける既知の脆弱性ではバッファ オーバーフローが発生し、攻撃者は特別に細工した認証パケットを使ってその状態を exploit できます。システムが asn.1 データをデコードするとき、パケット内の exploit コードは、システム レベル特権付きでホスト上で動作したり、DoS 状態を引き起こしたりすることができます。次のルールは、`asn1` キーワードを使用して、この脆弱性を悪用する試みを検出します。

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 445
(flow:to_server, established; content:"|FF|SMB|73|";
nocase; offset:4; depth:5;
asn1:bitstring_overflow,double_overflow,oversize_length 100,
relative_offset 54;)
```

上記のルールの場合、任意のポートおよび $EXTERNAL_NET 変数で定義された任意の IP アドレスから発信され、ポート 445 を使用する $HOME_NET 変数で定義された任意の IP アドレスに向かう TCP トラフィックに対して、イベントが生成されます。加えて、サーバへの TCP 接続が確立された時点でのみルールを実行します。その後、ルールは特定の位置にある特定のコンテンツを検査します。最後に、ルールは `asn1` キーワードを使用して、ビットストリング エンコードと二重 ASCII エンコードを検出し、最後に見つかったコンテンツ一致の末尾から 55 バイト目以降、長さ 100 バイトを超える asn.1 タイプ長を識別します（`offset` カウンタがバイト 0 から始まることに注意してください。）

urilen キーワード

urilen キーワードと HTTP Inspect プリプロセッサを組み合わせて使用すると、特定の長さ、最大長を下回る、最小長を上回る、または指定された範囲内の URI を HTTP トラフィック内で検査できます。

HTTP Inspect プリプロセッサがパケットを正規化して検査した後、ルール エンジンはルールに照らしてそのパケットを評価し、urilen キーワードで指定された長さ条件に URI が一致するかどうか判断します。このキーワードを使用すると、URI 長の脆弱性を exploit しようとする試みを検出できます。たとえばバッファ オーバーフローを発生させて、攻撃者が DoS 状態を引き起こしたり、システム レベル特権付きでホスト上でコードを実行したりしようと試みる可能性があります。

ルール内で urilen キーワードを使用するときには、次の点に注意してください。

- 必ず flow:established キーワードおよび他の 1 つ以上のキーワードを組み合わせて、urilen キーワードを使用してください。
- ルール プロトコルは常に TCP です。
- ターゲット ポートは常に HTTP ポートです。

URI 長を指定するときには、10 進のバイト数、「小なり」（<）、および「大なり」（>）を使用します。

次に例を示します。

- 5 バイト長の URI を検出するには、5 を指定します。
- 5 バイト長を下回る URI を検出するには、< 5（1 つの空白文字で区切る）を指定します。
- 5 バイト長を上回る URI を検出するには、> 5（1 つの空白文字で区切る）を指定します。
- 3 ～ 5 バイト長の URI を検出するには、3 <> 5（<> の前後に空白文字を 1 つずつ含む）を指定します。

たとえば、Novell の eDirectory バージョン 8.8 に付属のサーバ モニタリングおよび診断ユーティリティ iMonitor バージョン 2.4 に脆弱性があることが知られています。長すぎる URI を含むパケットはバッファ オーバーフローを発生させるため、攻撃者はシステム レベル特権付きでホスト上で動作したり、DoS 状態を引き起こしたりできる特別に細工したパケットを使ってその状態を exploit できます。次のルールは、urilen キーワードを使用して、この脆弱性を悪用する試みを検出します。

```
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS
(msg:"EXPLOIT eDirectory 8.8 Long URI iMonitor buffer
overflow attempt"; flow:to_server,established;
urilen:> 8192; uricontent:"/nds/"; nocase;
classtype:attempted-admin; sid:x; rev:1;)
```

上記のルールの場合、任意のポートおよび $EXTERNAL_NET 変数で定義された任意の IP アドレスから発信され、$HTTP_PORTS 変数で定義されたポートを使用して、$HOME_NET 変数で

定義された任意のIPアドレスに向かうTCPトラフィックに対して、イベントが生成されます。さらに、サーバへの TCP 接続が確立された場合にのみ、パケットがルールに対して評価されます。ルールは、urilen キーワードを使用して、長さ 8192 バイトを超える URI を検出します。最後に、ルールは URI を検索して、大文字/小文字を区別しない特定のコンテンツ /nds/ を探します。

関連トピック

侵入ルール ヘッダー プロトコル （2140 ページ）
侵入ルール ヘッダーの送信元および宛先ポート （2144 ページ）
定義済みデフォルト変数 （541 ページ）

DCE/RPC キーワード

次の表で説明する 3 つの DCE/RPC キーワードを使用して、DCE/RPC セッション トラフィックのエクスプロイトをモニタできます。これらのキーワードを含むルールを処理するとき、システムは DCE/RPC プリプロセッサを呼び出します。

表 *205 : DCE/RPC* キーワード

使用するフィルタ	使用方法	検出対象
dce_iface	単独	特定の DCE/RPC サービスを特定するパケット
dce_opnum	dce_iface の後ろ	特定の DCE/RPC サービス オペレーションを特定するパケット
dce_stub_data	dce_iface + dce_opnum の後ろ	特定の処理要求または応答を定義するスタブ データ

表に示されているように、dce_opnum の前に必ず dce_iface を配置し、dce_stub_data の前に必ず dce_iface + dce_opnum を配置する必要があることに注意してください。

また、これらの DCE/RPC キーワードを他のルール キーワードと組み合わせて使用することもできます。DCE/RPC ルールでは、**DCE/RPC** の引数が選択された状態で byte_jump、byte_test、byte_extract の各キーワードを使用することに注意してください。

シスコでは、DCE/RPC キーワードを含むルールに 1 つ以上の content キーワードを含めることを推奨しています。こうすると、ルール エンジンが常に高速パターン マッチ機能を使用することで処理速度が上がり、パフォーマンスが向上します。ルールに 1 つ以上の content キーワードが含まれている場合は、content キーワードの [高速パターン マッチ機能を使用（Use Fast Pattern Matcher）] 引数が有効になっているかどうかに関係なく、ルール エンジンが高速パターン マッチ機能を使用することに注意してください。

次のケースでは、DCE/RPC バージョンおよび隣接ヘッダー情報を一致コンテンツとして使用できます。

- ルールに他の content キーワードが含まれていない
- ルールにもう 1 つ content キーワードが含まれているが、DCE/RPC バージョンおよび隣接情報が、他方の content よりも特有のパターンを表している

たとえば、DCE/RPC バージョンおよび隣接情報は通常、1 バイトのコンテンツよりも特有です。

次に示すバージョンおよび隣接情報コンテンツ一致のいずれか 1 つを使用して、ルール限定を終了する必要があります。

- コネクション型 DCE/RPC ルールでは、コンテンツ `|05 00 00|`（メジャー バージョン 05、マイナー バージョン 00、および要求 PDU（プロトコル データ ユニット）タイプ 00 ）を使用します。
- コネクションレス型 DCE/RPC ルールでは、コンテンツ `|04 00|`（バージョン 04、要求 PDU タイプ 00）を使用します。

いずれの場合も、DCE/RPC プリプロセッサで完了済みの処理を繰り返すことなく高速パターンマッチ機能を呼び出すために、ルール内の最後のキーワードとしてバージョンおよび隣接情報の `content` キーワードを配置してください。ルールの末尾に配置される `content` キーワードは、高速パターン マッチ機能を呼び出す手段として使われるバージョン コンテンツに当てはまりますが、ルール内の他のコンテンツ一致には必ずしも当てはまらないことに注意してください。

関連トピック

DCE/RPC プリプロセッサ （2306 ページ）
content キーワードと protected_content キーワード （2164 ページ）
content キーワードの高速パターン マッチ機能の引数 （2175 ページ）
概要：byte_jump および byte_test キーワード
byte_extract キーワード （2184 ページ）

dce_iface

`dce_iface` キーワードを使用すると、特定の DCE/RPC サービスを識別できます。

オプションで、`dce_iface` キーワードを `dce_opnum` キーワードおよび `dce_stub_data` キーワードと組み合わせて使用すると、検査する DCE/RPC トラフィックをさらに限定することができます。

固定型 16 バイト Universally Unique Identifier（UUID）は、それぞれの DCE/RPC サービスに割り当てられるアプリケーション インターフェイスを識別します。たとえば、UUID 4b324fc8-670-01d3-1278-5a47bf6ee188 は、srvsvc サービスとしても知られる DCE/RPC lanmanserver サービスを識別します。このサービスは、ピアツーピア プリンタ、ファイル、および SMB 名前付きパイプを共有するためのさまざまな管理機能を提供します。DCE/RPC プリプロセッサは UUID および関連する見出し値を使用して DCE/RPC セッションを追跡します。

インターフェイス UUID は、次のように、ハイフンで区切られた 5 つの 16 進文字列で構成されます。

```
<4hexbytes>-<2hexbytes>-<2hexbytes>-<2hexbytes>-<6hexbytes>
```

次に示す netlogon インターフェイスの UUID のように、ハイフンを含む UUID 全体を入力することで、インターフェイスを指定します。

```
12345678-1234-abcd-ef00-01234567cffb
```

UUID 内の最初の 3 つの文字列はビッグ エンディアン バイト順で指定される必要があることに注意してください。通常、公開されたインターフェイス リストやプロトコル アナライザには UUID が正しいバイト順で表示されますが、それを入力する前に UUID バイト順を変更しなければならない場合もあります。次に示すメッセンジャー サービス UUID の場合、リトル エンディアン バイト順の最初の 3 つの文字列を含む未加工 ASCII テキストで表示されることがあります。

```
f8 91 7b 5a 00 ff d0 11 a9 b2 00 c0 4f b6 e6 fc
```

この同じ UUID を `dce_iface` キーワードに指定するには、次のようにハイフンを挿入し、最初の 3 つの文字列をビッグ エンディアン バイト順で配置できます。

```
5a7b91f8-ff00-11d0-a9b2-00c04fb6e6fc
```

1 つの DCE/RPC セッションに複数のインターフェイスへの要求を含めることができますが、1 つのルールには 1 つの `dce_iface` キーワードだけを含めてください。追加のインターフェイスを検出するには、追加のルールを作成します。

DCE/RPC アプリケーション インターフェイスにはインターフェイス バージョン番号も割り当てられます。オプションで、インターフェイス バージョンを指定できます。その際、バージョンが指定値に等しい、等しくない、指定値より小さい、または大きいことを示す演算子を使用します。

TCP セグメンテーションや IP フラグメンテーションに加えて、コネクション型とコネクションレス型の両方の DCE/RPC をフラグメント化することができます。通常、先頭以外の DCE/RPC フラグメントを指定のインターフェイスに関連付けるのはあまり効率的ではありません。このようにすると、多数の誤検出が発生する可能性があります。ただし、柔軟性を維持するために、オプションで、指定されたインターフェイスに照らしてすべてのフラグメントを評価できます。

次の表に、`dce_iface` キーワードの引数を要約します。

表 *206：dce_iface* の引数

引数	説明
Interface UUID	DCE/RPC トラフィック内で検出対象となる特定のサービスのアプリケーション インターフェイスを識別する、ハイフンを含む UUID。指定されたインターフェイスに関連付けられたすべての要求がインターフェイス UUID に一致します。
Version	オプションで、アプリケーション インターフェイス バージョン番号 0 ～ 65535 と、検出対象のバージョンが指定値より大きい（>）、小さい（<）、等しい（=）、または等しくない（!）を示す演算子。

引数	説明
All Fragments	オプションで、関連するすべてのDCE/RPCフラグメント内のインターフェイスの照合、およびインターフェイスバージョン（指定されている場合）での照合を有効にします。この引数はデフォルトで無効になっています。これは、最初のフラグメントまたはフラグメント化されていないパケット全体が指定のインターフェイスに関連付けられている場合にのみ、キーワードが一致することを意味します。この引数を有効にすると、誤検出が発生する可能性があることに注意してください。

dce_opnum キーワード

dce_opnum キーワードを DCE/RPC プリプロセッサと組み合わせて使用すると、DCE/RPC サービスが提供する 1 つ以上の特定のオペレーションを識別するパケットを検出できます。

クライアント関数呼び出しは、DCE/RPC 仕様で「オペレーション」と呼ばれる特定のサービス関数を要求します。オペレーション番号（opnum）は DCE/RPC 見出し内の特定のオペレーションを識別します。exploit は特定のオペレーションを標的にすることがあります。

たとえば UUID 12345678-1234-abcd-ef00-01234567cffb は、数十種類のオペレーションを提供する netlogon サービスのインターフェイスを識別します。その 1 つがオペレーション 6（NetrServerPasswordSet オペレーション）です。

オペレーション用のサービスを識別するには、dce_opnum キーワードの前に dce_iface キーワードを指定する必要があります。

特定のオペレーションを示す 1 つの 10 進数値（0 ～ 65535 の範囲）、ハイフンで区切られたオペレーション範囲、またはカンマ区切りのオペレーション/範囲リストを任意の順序で指定できます。

次の例は、すべて有効な netlogon オペレーション番号を表しています。

```
15
15-18
15, 18-20
15, 20-22, 17
15, 18-20, 22, 24-26
```

dce_stub_data キーワード

dce_stub_data キーワードを DCE/RPC プリプロセッサと組み合わせて使用すると、他のルールオプションとは無関係に、スタブ データの先頭からインスペクションを開始するようルールエンジンに指示できます。dce_stub_data キーワードの後に続くパケット ペイロード ルール オプションは、スタブ データ バッファを基準にして適用されます。

DCE/RPC スタブ データは、クライアント プロシージャ コールと DCE/RPC ランタイム システム（DCE/RPC の中核をなすルーチンとサービスを提供するメカニズム）の間のインターフェイスを提供します。DCE/RPC exploit は、DCE/RPC パケットのスタブ データ部分で識別されます。スタブ データは特定のオペレーションまたは関数呼び出しに関連付けられているため、必ず dce_stub_data の前に dce_iface と dce_opnum を指定して、関連するサービスとオペレーションを識別してください。

dce_stub_data キーワードには引数がありません。

SIP キーワード

4 つの SIP キーワードを使用すると、SIP セッション トラフィックでエクスプロイトを監視できます。

SIP プロトコルはサービス拒否（DoS）攻撃に対して脆弱であることに注意してください。このような攻撃に対処するルールでは、レート ベースの攻撃防御を活用できます。

sip_header キーワード

sip_header キーワードを使用すると、抽出された SIP 要求または応答ヘッダーの先頭から検査を開始し、検査対象をヘッダー フィールドに限定することができます。

sip_header キーワードには引数がありません。

次の例のルール フラグメントは SIP ヘッダーを指し示し、CSeq ヘッダー フィールドに一致します。

```
alert udp any any -> any 5060 ( sip_header; content:"CSeq"; )
```

関連トピック

動的侵入ルール状態 （2101 ページ）
レート ベースの攻撃防御 （2449 ページ）

sip_body キーワード

sip_body キーワードを使用すると、抽出された SIP 要求または応答メッセージ本文の先頭から検査を開始し、検査対象をメッセージ本文に限定することができます。

sip_body キーワードには引数がありません。

次の例のルール フラグメントは SIP メッセージ本文を指し示し、抽出された SDP データの c（接続情報）フィールド内の特定の IP アドレスに一致します。

```
alert udp any any -> any 5060 ( sip_body; content:"c=IN 192.168.12.14"; )
```

ルールが SDP コンテンツの検索だけに限定されないことに注意してください。SIP プリプロセッサはメッセージ本文全体を抽出し、それをルール エンジンで使用できるようにします。

sip_method キーワード

各 SIP 要求内の *method* フィールドは要求の目的を識別します。sip_method キーワードを使用すると、SIP 要求の中で特定のメソッドを検査することができます。複数のメソッドはカンマで区切ります。

次に示す現在定義されている SIP メソッドを指定できます。

```
ack, benotify, bye, cancel, do, info, invite, join, message, notify, options, prack,
publish, quath, refer, register, service, sprack, subscribe, unsubscribe, update
```

メソッドでは大文字と小文字が区別されません。複数のメソッドをカンマで区切ることができます。

今後、新しいSIPメソッドが定義される可能性があるため、カスタムメソッド、つまり現在定義されているSIPメソッド以外のメソッドを指定することもできます。可能なフィールド値はRFC 2616で定義されています。=、(、)などの制御文字と区切り文字を除いて、すべての文字を使用できます。除外されている区切り文字の完全なリストについては、RFC 2616を参照してください。指定されたカスタムメソッドがトラフィックで検出されると、システムはパケット見出しを検査しますが、メッセージは検査されません。

現在定義されている21個のメソッドと追加の11個のメソッドを含む、最大32個のメソッドがシステムでサポートされます。未定義のメソッドを設定した場合、システムはそれを無視します。合計32個のメソッドには、SIPプリプロセッサのオプション[検査するメソッド（Methods to Check）]を使って指定されるメソッドが含まれることに注意してください。

否定を使用する場合は、1つのメソッドだけを指定できます。次に例を示します。

```
!invite
```

ただし、1つのルール内の複数の `sip_method` キーワードが **AND** 演算で結合されることに注意してください。たとえば、`invite` と `cancel` を除くすべての抽出されたメソッドを検査するには、次のような2つの除外付き `sip_method` キーワードを使用します。

```
sip_method: !invite
sip_method: !cancel
```

Ciscoでは、`sip_method` キーワードを含むルールに1つ以上の `content` キーワードを含めることを推奨しています。こうすると、ルールエンジンが常に高速パターンマッチ機能を使用することで処理速度が上がり、パフォーマンスが向上します。ルールに1つ以上の `content` キーワードが含まれている場合は、`content` キーワードの[高速パターンマッチ機能を使用（Use Fast Pattern Matcher）]引数が有効になっているかどうかに関係なく、ルールエンジンが高速パターンマッチ機能を使用することに注意してください。

関連トピック

SIPプリプロセッサのオプション （2354ページ）
content キーワードと protected_content キーワード （2164ページ）
content キーワードの高速パターンマッチ機能の引数 （2175ページ）

sip_stat_code キーワード

各SIP応答内の3桁のステータスコードは、要求されたアクションの結果を示します。`sip_stat_code` キーワードを使用すると、SIP応答の中で特定のステータスコードを検査することができます。

1桁の応答タイプ番号1～9、特定の3桁の番号100～999、またはこれらを任意に組み合わせたカンマ区切りリストを指定できます。リスト内のいずれか1つの番号がSIP応答内のコードに一致する場合、そのリストが一致します。

次の表に、指定可能なSIPステータスコード値の説明を示します。

表 *207: sip_stat_code* の値

検出対象	指定する内容	例	検出結果
1 つの特定のステータス コード	3 桁のステータス コード	189	189
指定された 1 桁で始まる 3 桁のコード	1 桁	1	1xx、つまり 100、101、102 など
値のリスト	特定のコードおよび 1 桁を任意に組み合わせてカンマで区切る	222, 3	222 および 300、301、302 など

また、ルールに content キーワードが含まれているかどうかに関係なく、sip_stat_code キーワードを使って指定された値を検索するためにルール エンジンが高速パターン マッチ機能を使用しないことにも注意してください。

GTP キーワード

3 つの GSRP トンネリング プロトコル（GTP）キーワードを使用すると、GTP バージョン、メッセージタイプ、および情報要素をコマンドチャネル内で検査できます。contentやbyte_jump などの他の侵入ルール キーワードと組み合わせて GTP キーワードを使用することはできません。gtp_info または gtp_type キーワードを使用するそれぞれのルールで、gtp_version キーワードを使用する**必要があります**。

gtp_version キーワード

gtp_version キーワードを使用すると、GTP 制御メッセージの中で GTP バージョン 0、1、または 2 を検査することができます。

定義されているメッセージタイプと情報要素はGTPバージョンによって異なるため、gtp_type または gtp_info キーワードを使用するときには、gtp_version を使用する必要があります。値として 0、1、または 2 を指定できます。

gtp_type キーワード

それぞれの GTP メッセージは、数値と文字列で構成されるメッセージ タイプによって識別されます。gtp_type キーワードを使用すると、特定の GTP メッセージ タイプのトラフィックを検査できます。定義されているメッセージ タイプと情報要素は GTP バージョンによって異なるため、gtp_type または gtp_info キーワードを使用するときには、gtp_version も使用する必要があります。

次の例に示すように、メッセージ タイプとして定義済みの 10 進数値、定義済み文字列、あるいはどちらか（または両方）を任意に組み合わたカンマ区切りリストを指定できます。

```
10, 11, echo_request
```

リスト内のそれぞれの値または文字列を照合するとき、システムはOR演算を使用します。値と文字列を列挙する順序は重要ではありません。リスト内のいずれか1つの値または文字列の一致により、キーワードが一致します。認識されない文字列または範囲外の値を含むルールを保存しようとすると、エラーが発生します。

表に示されているように、GTPバージョンに応じて、同じメッセージ タイプの値が異なる場合があることに注意してください。たとえば `sgsn_context_request` メッセージ タイプの値はGTPv0とGTPv1では50ですが、GTPv2では130です。

パケット内のバージョン番号に応じて、`gtp_type` キーワードは異なる値と一致します。上記の例の場合、GTPv0またはGTPv1パケットではキーワードがメッセージ タイプ値50と一致しますが、GTPv2パケットでは値130と一致します。パケット内のメッセージ タイプ値が、パケットで指定されたバージョンの既知の値でない場合は、キーワードがパケットと一致しません。

メッセージタイプに整数を指定した場合、パケット内で指定されたバージョンとは無関係に、キーワード内のメッセージ タイプがGTPパケット内の値と一致すればキーワードが一致します。

次の表に、GTPメッセージ タイプごとにシステムで認識される定義済みの値と文字列を示します。

表 *208 : GTP* メッセージ タイプ

値	バージョン 0	バージョン 1	バージョン 2
1	echo_request	echo_request	echo_request
2	echo_response	echo_response	echo_response
3	version_not_supported	version_not_supported	version_not_supported
4	node_alive_request	node_alive_request	該当なし
5	node_alive_response	node_alive_response	該当なし
6	redirection_request	redirection_request	該当なし
7	redirection_response	redirection_response	該当なし
16	create_pdp_context_request	create_pdp_context_request	該当なし
	create_pdp_context_response	create_pdp_context_response	該当なし
	update_pdp_context_request	update_pdp_context_request	該当なし
19	update_pdp_context_response	update_pdp_context_response	該当なし
20	delete_pdp_context_request	delete_pdp_context_request	該当なし
21	delete_pdp_context_response	delete_pdp_context_response	該当なし

値	バージョン 0	バージョン 1	バージョン 2
22	create_aa_pdp_context_request	init_pdp_context_activation_request	該当なし
23	create_aa_pdp_context_response	init_pdp_context_activation_response	該当なし
24	delete_aa_pdp_context_request	該当なし	該当なし
25	delete_aa_pdp_context_response	該当なし	該当なし
26	error_indication	error_indication	該当なし
27	pdu_notification_request	pdu_notification_request	該当なし
28	pdu_notification_response	pdu_notification_response	該当なし
29	pdu_notification_reject_request	pdu_notification_reject_request	該当なし
30	pdu_notification_reject_response	pdu_notification_reject_response	該当なし
31	該当なし	supported_ext_header_notification	該当なし
32	send_routing_info_request	send_routing_info_request	create_session_request
33	send_routing_info_response	send_routing_info_response	create_session_response
34	failure_report_request	failure_report_request	modify_bearer_request
35	failure_report_response	failure_report_response	modify_bearer_response
36	note_ms_present_request	note_ms_present_request	delete_session_request
37	note_ms_present_response	note_ms_present_response	delete_session_response
38	該当なし	該当なし	change_notification_request
39	該当なし	該当なし	change_notification_response
48	identification_request	identification_request	該当なし
49	identification_response	identification_response	該当なし
50	sgsn_context_request	sgsn_context_request	該当なし
51	sgsn_context_response	sgsn_context_response	該当なし
52	sgsn_context_ack	sgsn_context_ack	該当なし
53	該当なし	forward_relocation_request	該当なし
54	該当なし	forward_relocation_response	該当なし
55	該当なし	forward_relocation_complete	該当なし

値	バージョン 0	バージョン 1	バージョン 2
56	該当なし	relocation_cancel_request	該当なし
57	該当なし	relocation_cancel_response	該当なし
58	該当なし	forward_srns_contex	該当なし
59	該当なし	forward_relocation_complete_ack	該当なし
60	該当なし	forward_srns_contex_ack	該当なし
64	該当なし	該当なし	modify_bearer_command
65	該当なし	該当なし	modify_bearer_failure_indication
66	該当なし	該当なし	delete_bearer_command
67	該当なし	該当なし	delete_bearer_failure_indication
68	該当なし	該当なし	bearer_resource_command
69	該当なし	該当なし	bearer_resource_failure_indication
70	該当なし	ran_info_relay	downlink_failure_indication
71	該当なし	該当なし	trace_session_activation
72	該当なし	該当なし	trace_session_deactivation
73	該当なし	該当なし	stop_paging_indication
95	該当なし	該当なし	create_bearer_request
96	該当なし	mbms_notification_request	create_bearer_response
97	該当なし	mbms_notification_response	update_bearer_request
98	該当なし	mbms_notification_reject_request	update_bearer_response
99	該当なし	mbms_notification_reject_response	delete_bearer_request
100	該当なし	create_mbms_context_request	delete_bearer_response
101	該当なし	create_mbms_context_response	delete_pdn_request
102	該当なし	update_mbms_context_request	delete_pdn_response
103	該当なし	update_mbms_context_response	該当なし
104	該当なし	delete_mbms_context_request	該当なし
105	該当なし	delete_mbms_context_response	該当なし

値	バージョン 0	バージョン 1	バージョン 2
112	該当なし	mbms_register_request	該当なし
113	該当なし	mbms_register_response	該当なし
114	該当なし	mbms_deregister_request	該当なし
115	該当なし	mbms_deregister_response	該当なし
116	該当なし	mbms_session_start_request	該当なし
117	該当なし	mbms_session_start_response	該当なし
118	該当なし	mbms_session_stop_request	該当なし
119	該当なし	mbms_session_stop_response	該当なし
120	該当なし	mbms_session_update_request	該当なし
121	該当なし	mbms_session_update_response	該当なし
128	該当なし	ms_info_change_request	identification_request
129	該当なし	ms_info_change_response	identification_response
130	該当なし	該当なし	sgsn_context_request
131	該当なし	該当なし	sgsn_context_response
132	該当なし	該当なし	sgsn_context_ack
133	該当なし	該当なし	forward_relocation_request
134	該当なし	該当なし	forward_relocation_response
135	該当なし	該当なし	forward_relocation_complete
136	該当なし	該当なし	forward_relocation_complete_ack
137	該当なし	該当なし	forward_access
138	該当なし	該当なし	forward_access_ack
139	該当なし	該当なし	relocation_cancel_request
140	該当なし	該当なし	relocation_cancel_response
141	該当なし	該当なし	configuration_transfer_tunnel
149	該当なし	該当なし	detach
150	該当なし	該当なし	detach_ack

値	バージョン 0	バージョン 1	バージョン 2
151	該当なし	該当なし	cs_paging
152	該当なし	該当なし	ran_info_relay
153	該当なし	該当なし	alert_mme
154	該当なし	該当なし	alert_mme_ack
155	該当なし	該当なし	ue_activity
156	該当なし	該当なし	ue_activity_ack
160	該当なし	該当なし	create_forward_tunnel_request
161	該当なし	該当なし	create_forward_tunnel_response
162	該当なし	該当なし	suspend
163	該当なし	該当なし	suspend_ack
164	該当なし	該当なし	resume
165	該当なし	該当なし	resume_ack
166	該当なし	該当なし	create_indirect_forward_tunnel_request
167	該当なし	該当なし	create_indirect_forward_tunnel_response
168	該当なし	該当なし	delete_indirect_forward_tunnel_request
169	該当なし	該当なし	delete_indirect_forward_tunnel_response
170	該当なし	該当なし	release_access_bearer_request
171	該当なし	該当なし	release_access_bearer_response
176	該当なし	該当なし	downlink_data
177	該当なし	該当なし	downlink_data_ack
179	該当なし	該当なし	pgw_restart
180	該当なし	該当なし	pgw_restart_ack
200	該当なし	該当なし	update_pdn_request
201	該当なし	該当なし	update_pdn_response
211	該当なし	該当なし	modify_access_bearer_request
212	該当なし	該当なし	modify_access_bearer_response

値	バージョン 0	バージョン 1	バージョン 2
231	該当なし	該当なし	mbms_session_start_request
232	該当なし	該当なし	mbms_session_start_response
233	該当なし	該当なし	mbms_session_update_request
234	該当なし	該当なし	mbms_session_update_response
235	該当なし	該当なし	mbms_session_stop_request
236	該当なし	該当なし	mbms_session_stop_response
240	data_record_transfer_request	data_record_transfer_request	該当なし
241	data_record_transfer_response	data_record_transfer_response	該当なし
254	該当なし	end_marker	該当なし
255	pdu	pdu	該当なし

gtp_info キーワード

1 つの GTP メッセージには多数の情報要素が含まれることがあり、それぞれの要素は定義済み数値および定義済み文字列によって識別されます。`gtp_info` キーワードを使用すると、指定された情報要素の先頭から検査を開始し、検査対象を指定の情報要素に限定することができます。定義されているメッセージ タイプと情報要素は GTP バージョンによって異なるため、このキーワードを使用するときには、`gtp_version` も使用する必要があります。

情報要素に対して定義された 10 進数値と定義された文字列のどちらでも指定できます。単一の値または文字列を指定することも、1 つのルール内で複数の `gtp_info` キーワードを使って複数の情報要素を検査することもできます。

1 つのメッセージに同じタイプの複数の情報要素が含まれている場合は、すべてが照合対象として検査されます。情報要素が無効な順序で出現する場合は、最後のインスタンスだけが検査されます。

GTP バージョンに応じて、同じ情報要素の値が異なる場合があることに注意してください。たとえば `cause` 情報要素の値は GTPv0 と GTPv1 では 1 ですが、GTPv2 では 2 です。

パケット内のバージョン番号に応じて、`gtp_info` キーワードは異なる値と一致します。上記の例の場合、GTPv0 または GTPv1 パケットではキーワードが情報要素値 1 と一致しますが、GTPv2 パケットでは値 2 と一致します。パケット内の情報要素値が、パケットで指定されたバージョンの既知の値でない場合は、キーワードがパケットと一致しません。

情報要素に整数を指定した場合、パケット内で指定されたバージョンとは無関係に、キーワード内のメッセージ タイプが GTP パケット内の値と一致すればキーワードが一致します。

次の表に、GTP 情報要素ごとにシステムで認識される値と文字列を示します。

表 *209 : GTP* 情報要素

値	バージョン 0	バージョン 1	バージョン 2
1	cause	cause	imsi
2	imsi	imsi	cause
3	rai	rai	復旧
4	tlli	tlli	該当なし
5	p_tmsi	p_tmsi	該当なし
6	qos	該当なし	該当なし
8	recording_required	recording_required	該当なし
9	authentication	authentication	該当なし
11	map_cause	map_cause	該当なし
12	p_tmsi_sig	p_tmsi_sig	該当なし
13	ms_validated	ms_validated	該当なし
14	復旧	復旧	該当なし
15	selection_mode	selection_mode	該当なし
16	flow_label_data_1	teid_1	該当なし
	flow_label_signalling	teid_control	該当なし
	flow_label_data_2	teid_2	該当なし
19	ms_unreachable	teardown_ind	該当なし
20	該当なし	nsapi	該当なし
21	該当なし	ranap	該当なし
22	該当なし	rab_context	該当なし
23	該当なし	radio_priority_sms	該当なし
24	該当なし	radio_priority	該当なし
25	該当なし	packet_flow_id	該当なし
26	該当なし	charging_char	該当なし
27	該当なし	trace_ref	該当なし

値	バージョン 0	バージョン 1	バージョン 2
28	該当なし	trace_type	該当なし
29	該当なし	ms_unreachable	該当なし
71	該当なし	該当なし	apn
72	該当なし	該当なし	ambr
73	該当なし	該当なし	ebi
74	該当なし	該当なし	ip_addr
75	該当なし	該当なし	mei
76	該当なし	該当なし	msisdn
77	該当なし	該当なし	indication
78	該当なし	該当なし	pco
79	該当なし	該当なし	paa
80	該当なし	該当なし	bearer_qos
80	該当なし	該当なし	flow_qos
82	該当なし	該当なし	rat_type
83	該当なし	該当なし	serving_network
84	該当なし	該当なし	bearer_tft
85	該当なし	該当なし	tad
86	該当なし	該当なし	uli
87	該当なし	該当なし	f_teid
88	該当なし	該当なし	tmsi
89	該当なし	該当なし	cn_id
90	該当なし	該当なし	s103pdf
91	該当なし	該当なし	s1udf
92	該当なし	該当なし	delay_value
93	該当なし	該当なし	bearer_context
94	該当なし	該当なし	charging_id

値	バージョン 0	バージョン 1	バージョン 2
95	該当なし	該当なし	charging_char
96	該当なし	該当なし	trace_info
97	該当なし	該当なし	bearer_flag
99	該当なし	該当なし	pdn_type
100	該当なし	該当なし	pti
101	該当なし	該当なし	drx_parameter
103	該当なし	該当なし	gsm_key_tri
104	該当なし	該当なし	umts_key_cipher_quin
105	該当なし	該当なし	gsm_key_cipher_quin
106	該当なし	該当なし	umts_key_quin
107	該当なし	該当なし	eps_quad
108	該当なし	該当なし	umts_key_quad_quin
109	該当なし	該当なし	pdn_connection
110	該当なし	該当なし	pdn_number
111	該当なし	該当なし	p_tmsi
112	該当なし	該当なし	p_tmsi_sig
113	該当なし	該当なし	hop_counter
114	該当なし	該当なし	ue_time_zone
115	該当なし	該当なし	trace_ref
116	該当なし	該当なし	complete_request_msg
117	該当なし	該当なし	guti
118	該当なし	該当なし	f_container
119	該当なし	該当なし	f_cause
120	該当なし	該当なし	plmn_id
121	該当なし	該当なし	target_id
123	該当なし	該当なし	packet_flow_id

値	バージョン 0	バージョン 1	バージョン 2
124	該当なし	該当なし	rab_contex
125	該当なし	該当なし	src_rnc_pdcp
126	該当なし	該当なし	udp_src_port
127	charge_id	charge_id	apn_restriction
128	end_user_address	end_user_address	selection_mode
129	mm_context	mm_context	src_id
130	pdp_context	pdp_context	該当なし
131	apn	apn	change_report_action
132	protocol_config	protocol_config	fq_csid
133	gsn	gsn	channel
134	msisdn	msisdn	emlpp_pri
135	該当なし	qos	node_type
136	該当なし	authentication_qu	fqdn
137	該当なし	tft	ti
138	該当なし	target_id	mbms_session_duration
139	該当なし	utran_trans	mbms_service_area
140	該当なし	rab_setup	mbms_session_id
141	該当なし	ext_header	mbms_flow_id
142	該当なし	trigger_id	mbms_ip_multicast
143	該当なし	omc_id	mbms_distribution_ack
144	該当なし	ran_trans	rfsp_index
145	該当なし	pdp_context_pri	uci
146	該当なし	addi_rab_setup	csg_info
147	該当なし	sgsn_number	csg_id
148	該当なし	common_flag	cmi
149	該当なし	apn_restriction	service_indicator

値	バージョン 0	バージョン 1	バージョン 2
150	該当なし	radio_priority_lcs	detach_type
151	該当なし	rat_type	ldn
152	該当なし	user_loc_info	node_feature
153	該当なし	ms_time_zone	mbms_time_to_transfer
154	該当なし	imei_sv	throttling
155	該当なし	camel	arp
156	該当なし	mbms_ue_context	epc_timer
157	該当なし	tmp_mobile_group_id	signalling_priority_indication
158	該当なし	rim_routing_addr	tmgi
159	該当なし	mbms_config	mm_srvcc
160	該当なし	mbms_service_area	flags_srvcc
161	該当なし	src_rnc_pdcp	nmbr
162	該当なし	addi_trace_info	該当なし
163	該当なし	hop_counter	該当なし
164	該当なし	plmn_id	該当なし
165	該当なし	mbms_session_id	該当なし
166	該当なし	mbms_2g3g_indicator	該当なし
167	該当なし	enhanced_nsapi	該当なし
168	該当なし	mbms_session_duration	該当なし
169	該当なし	addi_mbms_trace_info	該当なし
170	該当なし	mbms_session_repetition_num	該当なし
171	該当なし	mbms_time_to_data	該当なし
173	該当なし	bss	該当なし
174	該当なし	cell_id	該当なし
175	該当なし	pdu_num	該当なし
177	該当なし	mbms_bearer_capab	該当なし

値	バージョン 0	バージョン 1	バージョン 2
178	該当なし	rim_routing_disc	該当なし
179	該当なし	list_pfc	該当なし
180	該当なし	ps_xid	該当なし
181	該当なし	ms_info_change_report	該当なし
182	該当なし	direct_tunnel_flags	該当なし
183	該当なし	correlation_id	該当なし
184	該当なし	bearer_control_mode	該当なし
185	該当なし	mbms_flow_id	該当なし
186	該当なし	mbms_ip_multicast	該当なし
187	該当なし	mbms_distribution_ack	該当なし
188	該当なし	reliable_inter_rat_handover	該当なし
189	該当なし	rfsp_index	該当なし
190	該当なし	fqdn	該当なし
191	該当なし	evolved_allocation1	該当なし
192	該当なし	evolved_allocation2	該当なし
193	該当なし	extended_flags	該当なし
194	該当なし	uci	該当なし
195	該当なし	csg_info	該当なし
196	該当なし	csg_id	該当なし
197	該当なし	cmi	該当なし
198	該当なし	apn_ambr	該当なし
199	該当なし	ue_network	該当なし
200	該当なし	ue_ambr	該当なし
201	該当なし	apn_ambr_nsapi	該当なし
202	該当なし	ggsn_backoff_timer	該当なし
203	該当なし	signalling_priority_indication	該当なし

値	バージョン 0	バージョン 1	バージョン 2
204	該当なし	signalling_priority_indication_nsapi	該当なし
205	該当なし	high_bitrate	該当なし
206	該当なし	max_mbr	該当なし
251	charging_gateway_addr	charging_gateway_addr	該当なし
255	private_extension	private_extension	private_extension

SCADA キーワード

ルール エンジンは Modbus、DNP3、および CIP のルールを使用して特定のプロトコル フィールドにアクセスします。

Modbus キーワード

Modbus キーワードを単独で使用することも、`content` や `byte_jump` など他のキーワードと組み合わせて使用することもできます。

modbus_data

`modbus_data` キーワードを使用すると、Modbus 要求または応答内の [Data] フィールドの先頭を指し示すことができます。

modbus_func

`modbus_func` キーワードを使用すると、Modbus アプリケーション層要求または応答見出し内の [Function Code（機能コード）] フィールドを照合できます。Modbus 機能コードとして、1 つの定義済み 10 進数値または 1 つの定義済み文字列を指定できます。

次の表に、Modbus機能コードとしてシステムで認識される定義済みの値と文字列を示します。

表 *210 : Modbus* 機能コード

値	文字列
1	read_coils
2	read_discrete_inputs
3	read_holding_registers
4	read_input_registers
5	write_single_coil
6	write_single_register

値	文字列
7	read_exception_status
8	diagnostics
11	get_comm_event_counter
12	get_comm_event_log
15	write_multiple_coils
16	write_multiple_registers
	report_slave_id
20	read_file_record
21	write_file_record
22	mask_write_register
23	read_write_multiple_registers
24	read_fifo_queue
43	encapsulated_interface_transport

modbus_unit

`modbus_unit` キーワードを使用すると、Modbus 要求または応答ヘッダー内の [Unit ID] フィールドで 1 つの 10 進数値を照合できます。

DNP3 キーワード

DNP3 キーワードを単独で使用することも、`content` や `byte_jump` など他のキーワードと組み合わせて使用することもできます。

dnp3_data

`dnp3_data` キーワードを使用すると、再構築された DNP3 アプリケーション層フラグメントの先頭を指し示すことができます。

DNP3 プリプロセッサが、リンク層フレームをアプリケーション層フラグメントに再構築します。`dnp3_data` キーワードは、各アプリケーション層フラグメントの先頭を指し示します。他のルール オプションは、16 バイトごとにデータを分離してチェックサムを追加せずに、フラグメント内の再構築されたデータを照合することができます。

dnp3_func

`dnp3_func` キーワードを使用すると、DNP3 アプリケーション層要求または応答ヘッダー内の [機能コード（Function Code）] フィールドを照合できます。DNP3 機能コードとして、1 つの定義済み 10 進数値または 1 つの定義済み文字列を指定できます。

次の表に、DNP3 機能コードとしてシステムで認識される定義済みの値と文字列を示します。

表 *211 : DNP3* 機能コード

値	文字列
0	confirm
1	read
2	write
3	select
4	operate
5	direct_operate
6	direct_operate_nr
7	immed_freeze
8	immed_freeze_nr
9	freeze_clear
10	freeze_clear_nr
11	freeze_at_time
12	freeze_at_time_nr
13	cold_restart
14	warm_restart
15	initialize_data
16	initialize_appl
	start_appl
	stop_appl
19	save_config
20	enable_unsolicited
21	disable_unsolicited
22	assign_class
23	delay_measure
24	record_current_time
25	open_file

値	文字列
26	close_file
27	delete_file
28	get_file_info
29	authenticate_file
30	abort_file
31	activate_config
32	authenticate_req
33	authenticate_err
129	response
130	unsolicited_response
131	authenticate_resp

dnp3_ind

`dnp3_ind` キーワードを使用すると、DNP3 アプリケーション層応答ヘッダー内の [Internal Indications] フィールド内のフラグを照合できます。

1 つの既知のフラグ、または次の例のようなカンマ区切りのフラグ リストを示す文字列を指定できます。

```
class_1_events, class_2_events
```

複数のフラグを指定した場合、キーワードはリスト内の任意のフラグと一致します。いくつかのフラグの組み合わせを検出するには、1 つのルール内で `dnp3_ind` キーワードを複数回使用します。

定義済みの DNP3 内部通知フラグとしてシステムによって認識される文字列構文を以下に示します。

```
class_1_events
class_2_events
class_3_events
need_time
local_control
device_trouble
device_restart
no_func_code_support
object_unknown
parameter_error
event_buffer_overflow
already_executing
config_corrupt
reserved_2
reserved_1
```

dnp3_obj

dnp3_obj キーワードを使用すると、要求または応答内の DNP3 オブジェクト ヘッダーを照合できます。

DNP3データは、アナログ入力やバイナリ入力など、さまざまなタイプの一連のDNP3オブジェクトで構成されます。各タイプは、それぞれ 10 進数値で識別されるグループ を使って区別されます（アナログ入力グループ、バイナリ入力グループなど）。各グループ内のオブジェクトは、それぞれオブジェクト データ形式を指定するオブジェクト バリエーション によってさらに区別されます（16 ビット整数、32 ビット整数、短精度浮動小数点など）。また、オブジェクト バリエーションの各タイプは 10 進数値でも識別可能です。

オブジェクト 見出しを識別する際には、オブジェクト 見出し グループのタイプを示す10進数値とオブジェクト バリエーションのタイプを示す 10 進数値を指定します。この 2 つの組み合わせによって DNP3 オブジェクトの特定のタイプが定義されます。

CIP および ENIP のキーワード

次のキーワードを単体でまたは組み合わせて使用すると、CIP プリプロセッサで検出された CIP および ENIP トラフィックに対する攻撃を識別するカスタム侵入ルールを作成できます。設定可能なキーワードについては、許容範囲内の単一の整数を指定します。詳細については、CIP プリプロセッサ （2390 ページ）を参照してください。

表 *212*:

対象キーワード	照合先	範囲
cip_attribute	CIP メッセージの [オブジェクト クラス/インスタンス属性（Object Class/Instance Attribute）] フィールド。定義された 1 つの整数値を指定します。	0 ～ 65535
cip_class	CIP メッセージの [オブジェクト クラス（Object Class）] フィールド。定義された 1 つの整数値を指定します。	0 ～ 65535
cip_conn_path_class	接続パスのオブジェクト クラス。1 つの整数値を指定します。	0 ～ 65535
cip_instance	CIP メッセージの [インスタンス ID（Instance ID）] フィールド。1 つの整数値を指定します。	0 ～ 4284927295
cip_req	サービス要求メッセージ。	該当なし

対象キーワード	照合先	範囲
cip_rsp	サービス応答メッセージ。	該当なし
cip_service	CIP サービス要求メッセージの [サービス（Service）] フィールド。1つの整数値を指定します。	0 ～ 127
cip_status	CIP サービス応答メッセージの [ステータス（Status）] フィールド。1つの整数値を指定します。	0 ～ 255
enip_command	EthNet/IP ヘッダーのコマンドコード。1つの整数値を指定します。	0 ～ 65535
enip_req	EthNet/IP 要求メッセージ。	該当なし
enip_rsp	EthNet/IP 応答メッセージ。	該当なし

パケット特性

特定のパケット特性を持つパケットに対してのみイベントを生成するルールを作成できます。

dsize

dsize キーワードはパケット ペイロード サイズを検査します。「大なり」演算子と「小なり」演算子（<、>）を使って値の範囲を指定することができます。次の構文をに従って範囲を指定できます。

```
>number_of_bytes
<number_of_bytes
number_of_bytes<>number_of_bytes
```

たとえば、400 バイトを超えるパケット サイズを指定するには、dtype 値として >400 を使用します。500 バイト未満のパケット サイズを指定するには、<500 を使用します。400 ～ 500 バイトのパケットに対してルールをトリガーとして使用するよう指定するには、400<>500 を使用します。

⚠

注意 dsize キーワードは、プリプロセッサによってデコードされる前のパケットを検査します。

isdataat

isdataat キーワードは、ペイロード内の特定の位置にデータが存在することを確認するよう、ルール エンジンに指示します。

次の表に、isdataat キーワードで使用可能な引数を列挙します。

表 213 : isdataat の引数

引数	タイプ	説明
Offset	必須	ペイロード内の特定の位置。たとえば、パケット ペイロード内のバイト位置 50 にデータが出現することを検査するには、オフセット値として 50 を指定します。! 修飾子は isdataat 検査の結果を否定します。特定量のデータがペイロードに存在しない場合は警告が出されます。 また、既存の byte_extract 変数または byte_math 結果を使用してこの引数の値を指定することもできます。
Relative	任意	最後に見つかったコンテンツ一致を基準にして相対的な位置を計算します。相対位置を指定する場合は、カウンタがバイト 0 から始まることに注意してください。最後に見つかったコンテンツ一致から順方向に移動するバイト数から 1 を差し引いて位置を計算します。たとえば、最後に見つかったコンテンツ一致から 9 バイト後にデータが出現すべきことを指定するには、相対オフセットとして 8 を指定します。
Raw Data	オプション	Firepower システム プリプロセッサによるデコードやアプリケーション層の正規化が行われる前の、元のパケット ペイロードにデータが配置されていることを指定します。前のコンテンツ一致が未加工パケット データ内に存在していた場合は、この引数を **Relative** と一緒に使用できます。

たとえば、foo というコンテンツを検索するルールで isdataat の値が次のように指定される場合、

- Offset = !10
- Relative = enabled

ルール エンジンが foo の後ろからペイロード末尾までに 10 バイトを検出しない場合、システムは警告を出します。

sameip

sameip キーワードは、パケットの送信元 IP アドレスと宛先 IP アドレスが同じであることを検査します。このキーワードは引数を受け入れません。

fragoffset

fragoffset キーワードは、フラグメント化されたパケットのオフセットを検査します。一部の exploit（WinNuke サービス拒否攻撃など）では、特定のオフセットを持つ手動生成されたパケット フラグメントが使われるため、このキーワードが役立ちます。

たとえば、フラグメント化されたパケットのオフセットが 31337 バイトかどうかを検査するには、fragoffset 値として 31337 を指定します。

fragoffset キーワードの引数を指定するときには、次の演算子を使用できます。

表 *214 : fragoffset* キーワードの引数演算子

演算子	説明
!	not
>	より大きい
<	より小さい

否定（!）演算子を < や > と組み合わせて使用できないことに注意してください。

cvs

cvs キーワードは、Concurrent Versions System（CVS）トラフィック内で不正な形式の CVS エントリを検査します。攻撃者は不正な形式のエントリを使用して、ヒープオーバーフローを強制的に発生させ、CVS サーバ上で有害コードを実行することができます。このキーワードを使用すると、2 つの既知の CVS 脆弱性 CVE-2004-0396（CVS 1.11.x ～ 1.11.15 と 1.12.x ～ 1.12.7）および CVS-2004-0414（CVS 1.12.x ～ 1.12.8 と 1.11.x ～ 1.11.16）に対する攻撃を識別できます。cvs キーワードは、正しい形式のエントリであることを検査して、不正な形式のエントリが検出された場合はアラートを生成します。

CVS が動作するポートをルールに含める必要があります。さらに、トラフィックが発生する可能性のあるポートを TCP ポリシー内のストリーム再構築用のポートリストに追加することで、CVS セッションの状態を保持できるようにする必要があります。ストリーム再構築が行われるクライアントポートのリストには、TCP ポート 2401（pserver）と 514（rsh）が含まれています。ただし、サーバが xinetd サーバ（つまり pserver）として動作する場合は、任意の TCP ポート上で動作できることに注意してください。すべての非標準ポートを、ストリーム再構築の [クライアント ポート（Client Ports）] リストに追加します。

関連トピック

byte_extract キーワード （2184 ページ）
TCP ストリームのプリプロセス オプション （2425 ページ）

アクティブ応答のキーワード

resp キーワードおよび **react** キーワードにより、2 つの方法でアクティブ応答を開始できます。パケットがどちらかのキーワードを含む侵入ルールをトリガーとして使用すると、その侵入ルールにより、1 つのアクティブ応答が開始します。アクティブ応答のキーワードは、トリガーとして使用された TCP ルールに応答して TCP 接続を閉じるために、またはトリガーとして使用された UDP ルールに応答して UDP セッションを閉じるために、アクティブ応答を開始します。侵入廃棄ルールでのアクティブ応答 （2398 ページ）を参照してください。（攻撃者がアクティブ応答を無視または回避するよう選択する可能性があるなど）さまざまな理由で、アクティブ応答はファイアウォールの代わりとして想定されていません。

アクティブ応答は、ルーテッド展開またはトランスペアレント展開を含むインライン展開でサポートされます。たとえば、インライン展開での `react` キーワードに応答して、システムは接続の両端用のトラフィックに TCP リセット（RST）パケットを直接挿入でき、通常はこれによって接続が閉じます。アクティブ応答は、パッシブ展開ではサポートされていないか、または適していません。

アクティブ応答は戻って来ることがあるため、システムは TCP リセットによる TCP リセットの開始を許可しません。これにより、アクティブ応答が無限に続くことを防止できます。また、システムは、標準的な慣行に従って ICMP 到達不能パケットによる ICMP 到達不能パケットの開始を許可しません。

侵入ルールがアクティブ応答をトリガーとして使用した後、TCP接続で追加のトラフィックを検出するよう、TCP ストリーム プリプロセッサを設定できます。追加のトラフィックが検出されると、プリプロセッサは、指定された最大値まで、追加のアクティブ応答を接続またはセッションの両端に送信します。トランスポート/ネットワーク プリプロセッサの詳細オプション（2399 ページ）の「**アクティブ応答の最大数（Maximum Active Responses）**」および「**最小応答時間（秒）（Minimum Response Seconds）**」を参照してください。

関連トピック

侵入廃棄ルールでのアクティブ応答 （2398 ページ）

resp キーワード

`resp` キーワードを使用すると、ルール ヘッダーで TCP プロトコルと UDP プロトコルのどちらが指定されているかに基づいて、TCP 接続または UDP セッションにアクティブに（能動的に）応答できます。

キーワード引数を使用すると、パケットの方向、および TCP リセット（RST）パケットと ICMP 到達不能パケットのどちらをアクティブ応答として使用するかを指定できます。

任意の TCP リセット引数または ICMP 到達不能引数を使用して、TCP 接続を閉じることができます。UDP セッションを閉じるには、ICMP 到達不能引数だけを使用する必要があります。

また、さまざまな TCP リセット引数を使用することで、パケットの送信元、宛先、またはその両方にアクティブ応答を送ることができます。すべての ICMP 到達不能引数はパケット送信元に送られます。ICMP ネットワーク、ホスト、またはポートのどの到達不能パケットを使用するか（または 3 つすべてを使用するか）を指定できます。

ルールがトリガーとして使用されたときに Firepower システムで実行されるアクションを正確に指定するために、`resp` キーワードで使用できる引数を次の表に列挙します。

表 *215 : resp* 引数

引数	説明
reset_source	ルールをトリガーとして使用したパケットを送信元エンドポイントに TCP リセット パケットを送ります。この代わりに、下位互換性のためにサポートされている `rst_snd` を指定することもできます。

引数	説明
reset_dest	ルールをトリガーとして使用したパケットの宛先であるエンドポイントに TCP リセット パケットを送ります。この代わりに、下位互換性のためにサポートされている `rst_rcv` を指定することもできます。
reset_both	送信側エンドポイントと受信側エンドポイントの両方に TCP リセット パケットを送ります。この代わりに、下位互換性のためにサポートされている `rst_all` を指定することもできます。
icmp_net	送信側に ICMP ネットワーク到達不能メッセージを送ります。
icmp_host	送信側に ICMP ホスト到達不能メッセージを送ります。
icmp_port	送信側に ICMP ポート到達不能メッセージを送ります。この引数は、UDP トラフィックを終了するために使われます。
icmp_all	送信側に次の ICMP メッセージを転送します。 • ネットワーク到達不能 • ホスト到達不能 • ポート到達不能

たとえば、ルールがトリガーとして使用されたときに接続の両側をリセットするようルールを設定するには、`resp` キーワードの値として `reset_both` を使用します。

次のように、カンマ区切りのリストを使用して複数の引数を指定できます。

```
argument,argument,argument
```

関連トピック

config response コマンド

react キーワード

`react` キーワードを使用すると、パケットがルールをトリガーとして使用した時点でデフォルト HTML ページを TCP 接続クライアントに送信できます。HTML ページの送信後に、システムは TCP リセット パケットを使って接続の両端へのアクティブ応答を開始します。`react` キーワードは UDP トラフィックのアクティブ応答をトリガーとして使用しません。

オプションで、次の引数を指定できます。

```
msg
```

`msg` 引数を使用する `react` ルールがパケットによってトリガーとして使用されると、HTML ページにルール イベント メッセージが表示されます。

`msg` 引数を指定しない場合、HTML ページには次のメッセージが含まれます。

```
You are attempting to access a forbidden site.
Consult your system administrator for details.
```

（注） アクティブ応答は戻されることがあるため、HTML 応答ページによって react ルールがトリガーとして使用されないようにしてください（結果としてアクティブ応答が無限に続く可能性があります）。Cisco では、react ルールを十分にテストしてから実稼動環境でアクティブにするよう推奨しています。

関連トピック

ルールの詳細 （2138 ページ）
config response コマンド

detection_filter キーワード

detection_filter キーワードを使用すると、指定された時間内に指定された数のパケットがルールをトリガーとして使用しない限り、ルールでイベントが生成されないようにすることができます。これにより、早すぎるタイミングでルールがイベントを生成することを回避できます。たとえば、数秒間にログイン試行が 2 ～ 3 回失敗することは想定の範囲内ですが、同じ時間内に多数の試行が発生した場合は総当たり攻撃を示唆している可能性があります。

detection_filter キーワードの必須の引数は、送信元/宛先のどちらの IP アドレスをシステムで追跡するか、イベントをトリガーすめたに検出基準が満たされるべき回数、およびカウントの継続時間を定義します。

イベントのトリガーを遅らせるには、次の構文を使用します。

```
track by_src/by_dst, count count, seconds number_of_seconds
```

track 引数は、ルールの検出基準を満たすパケット数をカウントするときに、パケットの送信元 IP アドレスと宛先 IP アドレスのどちらを使用するかを指定します。システムでイベントインスタンスを追跡する方法を指定するには、次の表の中から引数値を選択します。

表 *216 : detection_filter* の追跡引数

引数	説明
by_src	送信元 IP アドレスによる検出基準カウント。
by_dst	宛先 IP アドレスによる検出基準カウント。

count 引数は、ルールでイベントを生成するために、指定された時間内に指定された IP アドレスのルールをトリガーすべきパケットの数を指定します。

seconds 引数は、ルールでイベントを生成するために、指定された数のパケットがルールをトリガーすべき時間枠を秒数で指定します。

パケット内でコンテンツ foo を検索するルールが、次の引数を含む detection_filter キーワードを使用するとします。

```
track by_src, count 10, seconds 20
```

この例のルールは、特定の送信元 IP アドレスから 20 秒以内に 10 個のパケットで foo を検出するまでは、イベントを生成しません。システムが最初の 20 秒以内に foo を含むパケットを 7 つしか検出しなかった場合は、イベントが生成されません。しかし、最初の 20 秒間で foo が 40 回出現した場合は、ルールで 30 個のイベントが生成され、20 秒が経過するとカウントが再開されます。

しきい値と detection_filter キーワードの比較

detection_filter キーワードは、非推奨の threshold キーワードに代わるものです。threshold キーワードは、下位互換性を維持するために引き続きサポートされていますが、侵入ポリシー内で設定されるしきい値と同じ機能です。

detection_filter キーワードは、パケットがルールをトリガーとして使用する前に適用される検出機能です。ルールは、指定されたパケット カウントの前に検出されたトリガー パケットに関してイベントを生成しません。また、インライン展開では、パケットを破棄するようルールで設定されていても、そのようなパケットを破棄しません。逆に、指定されたパケット カウントの後に出現する、ルールをトリガーとして使用するパケットに関してルールはイベントを生成します。また、インライン展開でパケットを破棄するよう設定されている場合は、そのようなパケットを破棄します。

しきい値は、検出アクションを発生させないイベント通知機能です。これは、パケットがイベントをトリガーとして使用した後に適用されます。インライン展開において、パケットを破棄するよう設定されたルールは、ルール しきい値とは無関係に、ルールをトリガーとして使用するすべてのパケットを破棄します。

侵入ポリシー内で detection_filter キーワードを侵入イベントしきい値、侵入イベント抑制、および Rate-Based 攻撃防御機能と任意に組み合わせて使用できることに注意してください。また、侵入ポリシー内の侵入イベントしきい値機能と組み合わせて非推奨の threshold キーワードを使用するインポートされたローカル ルールを有効にした場合、ポリシー検証が失敗することに注意してください。

関連トピック

侵入イベントのしきい値 （2094 ページ）
侵入ポリシーの抑制の設定 （2099 ページ）
[ルール（Rule）] ページからの動的ルール状態の設定 （2103 ページ）
ローカル侵入ルールのインポートのガイドライン （190 ページ）

tag キーワード

ホストまたはセッションに関する追加のトラフィックをログに記録するようシステムに指示するには、tag キーワードを使用します。tag キーワードを使って検出するトラフィックのタイプと量を指定するときには、次の構文を使用します。

```
tagging_type, count, metric, optional_direction
```

次の 3 つの表に、その他の使用可能な引数について説明します。

2 つのタイプのタグ機能から選択できます。次の表に、これらのタグ機能の説明を示します。侵入ルールでルール見出しオプションのみを設定した場合、sessionタグ引数タイプによって、同じセッションからのパケットが別のセッションからのパケットのように記録されることに注意してください。同じセッションからのパケットをまとめてグループ化するには、同じ侵入ルール内で 1 つ以上のルール オプション（`flag` キーワードや `content` キーワードなど）を設定します。

表 *217 : tag* の引数

引数	説明
session	ルールをトリガーとして使用したセッション内のパケットをログに記録します。
host	ルールをトリガーとして使用したパケットを送信したホストからのパケットをログに記録します。ホストからのトラフィックのみ（`src`）、またはホストへのトラフィックのみ（`dst`）を記録する方向修飾子を追加できます。

ログに記録するトラフィック量を指定するには、次の引数を使用します。

表 *218 :* カウント引数

引数	説明
count	ルールがトリガーとして使用された後にログに記録するパケット数または秒数。 この単位を指定するには、count 引数の後に測定基準引数を使用します。

次の表の中から、トラフィックの時間または量ごとにログで使用する測定基準を選択してください。

⚠

注意 高帯域ネットワークでは、1 秒あたり数千パケットが発生する可能性があり、多数のパケットにタグを付けるとパフォーマンスに重大な影響が及ぶ可能性があるため、必ずネットワーク環境に合わせてこの設定を調整してください。

表 *219 :* ログの測定基準引数

引数	説明
packets f f	ルールのトリガー後に、カウントで指定されるパケット数をログに記録します。

引数	説明
seconds	ルールのトリガー後に、カウントで指定される秒数の間、トラフィックを記録します。

たとえば、次の tag キーワード値を使用するルールがトリガーとして使用された場合、

```
host, 30, seconds, dst
```

次の30秒間にクライアントからホストに送信されるすべてのパケットがログに記録されます。

flowbits キーワード

状態名をセッションに割り当てるには、flowbits キーワードを使用します。すでに名前が付けられた状態に基づいてセッション内の後続パケットを分析することにより、システムは単一セッション内で複数のパケットに及ぶエクスプロイトを検出して警告を出すことができます。

flowbits 状態名は、セッションの特定部分でパケットに割り当てられるユーザー定義のラベルです。パケットの内容に基づいてパケットに状態名を付けると、警告の必要のないパケットと有害なパケットを区別しやすくなります。管理対象デバイスごとに最大 1024 個の状態名を定義できます。たとえば、ログイン成功後にのみ発生することがわかっている有害パケットについて警告するには、flowbits キーワードを使用して、初期ログイン試行を構成するパケットを除去することにより、有害パケットに焦点を絞ることができます。このような機能を実装するには、まず、セッション内のすべてのログイン確立済みパケットに logged_in 状態のラベルを付けるルールを作成した後、2 番目のルールを作成し、最初のルールで設定された状態を持つパケットを検査してそのようなパケットだけを処理する flowbits をそのルールに含めます。

オプションの *group name* を使用すると、状態のグループに状態名を含めることができます。1 つの状態名は複数のグループに属することができます。グループに関連付けられていない状態は相互排他的ではないため、トリガーとして使用されたルールがグループに関連付けられていない状態を設定した場合、現在設定されている他の状態には影響がありません。

flowbits キーワードのオプション

次の表に、flowbits キーワードで使用できる演算子、状態、およびグループのさまざまな組み合わせについて説明します。なお、状態名には、英数字、ピリオド（.）、アンダースコア（_）、およびダッシュ（-）を含めることができます。

表 *220 : flowbits* のオプション

演算子	状態オプション	グループ	説明
set	state_name	オプション	パケットに関する指定された状態を設定します。グループが定義されている場合は、指定されたグループ内で状態を設定します。

演算子	状態オプション	グループ	説明
set	state_name&state_name	オプション	パケットに関する、指定された複数の状態を設定します。グループが定義されている場合は、指定されたグループ内で状態を設定します。
setx	state_name	入力必須	指定されたグループ内でパケットに関して指定された状態を設定し、グループ内の他のすべての状態を解除します。
setx	state_name&state_name	入力必須	指定されたグループ内でパケットに関して指定された状態を設定し、グループ内の他のすべての状態を解除します。
unset	state_name	グループなし	パケットに関する指定された状態を解除します。
unset	state_name&state_name	グループなし	パケットに関する指定された状態を解除します。
unset	all	入力必須	指定されたグループ内のすべての状態を解除します。
toggle	state_name	グループなし	指定された状態が設定されている場合はそれを解除し、指定された状態が解除されている場合にはそれを設定します。
toggle	state_name&state_name	グループなし	指定された複数の状態が設定されている場合はそれらを解除し、指定された複数の状態が解除されている場合はそれらを設定します。
toggle	all	入力必須	指定されたグループ内で設定されているすべての状態を解除し、指定されたグループ内で解除されているすべての状態を設定します。
isset	state_name	グループなし	指定された状態がパケット内で設定されているかどうかを判別します。
isset	state_name&state_name	グループなし	指定された複数の状態がパケット内で設定されているかどうかを判別します。
isset	state_name|state_name	グループなし	指定されたいずれかの状態がパケット内で設定されているかどうかを判別します。
isset	any	入力必須	指定されたグループ内で、いずれかの状態が設定されているかどうかを判別します。
isset	all	入力必須	指定されたグループ内で、すべての状態が設定されているかどうかを判別します。
isnotset	state_name	グループなし	指定された状態がパケット内で設定されていないかどうかを判別します。

演算子	状態オプション	グループ	説明
isnotset	state_name&state_name	グループなし	指定された複数の状態がパケット内で設定されていないかどうかを判別します。
isnotset	state_name|state_name	グループなし	指定されたいずれかの状態が、パケット内で設定されていないかどうかを判別します。
isnotset	any	入力必須	パケット内でいずれかの状態が設定されていないかどうかを判別します。
isnotset	all	入力必須	パケット内ですべての状態が設定されていないかどうかを判別します。
reset	（状態なし）	オプション	すべてのパケットのすべての状態を解除します。グループが指定されている場合、グループ内のすべての状態を解除します。
noalert	（状態なし）	グループなし	イベント生成を抑制するには、これを他の演算子と組み合わせて使用します。

flowbits キーワードの使用に関するガイドライン

flowbits キーワードを使用するときには、次の点に注意してください。

- setx 演算子を使用する場合、指定した状態は、指定したグループ以外のグループに属することができません。
- setx 演算子を複数回定義して、それぞれのインスタンスで別々の状態と同じグループを指定できます。
- setx 演算子を使用してグループを指定する場合、そのグループに対して set、toggle、unset 演算子を使用することはできません。
- isset 演算子と isnotset 演算子は、指定された状態がグループに含まれるかどうかに関係なく、その状態を評価します。
- 侵入ポリシーの保存時、侵入ポリシーの再適用時、および（アクセス コントロール ポリシーで参照される侵入ポリシー数に関係なく）アクセス コントロール ポリシーの適用時には、グループ**指定のない** isset または isnotset 演算子を含むルールを有効にした場合、対応する状態名とプロトコルに関する flowbits 割り当て（set、setx、unset、toggle）に影響する 1 つ以上のルールを有効にしないと、対応する状態名の flowbits 割り当てに影響するすべてのルールが有効になります。
- 侵入ポリシーの保存時、侵入ポリシーの再適用時、および（アクセス コントロール ポリシーで参照される侵入ポリシー数に関係なく）アクセス コントロール ポリシーの適用時には、グループを**指定した** isset 演算子または isnotset 演算子を含むルールを有効にした場合、flowbits 割り当て（set、setx、unset、toggle）に影響し、対応するグループ名を定義するすべてのルールもまた有効になります。

flowbits キーワードの例

この項では、flowbits キーワードを使用する 3 つの例を示します。

flowbits キーワードの例：state_name を使用した設定

これは、state_name を使用した flowbits 設定の例です。

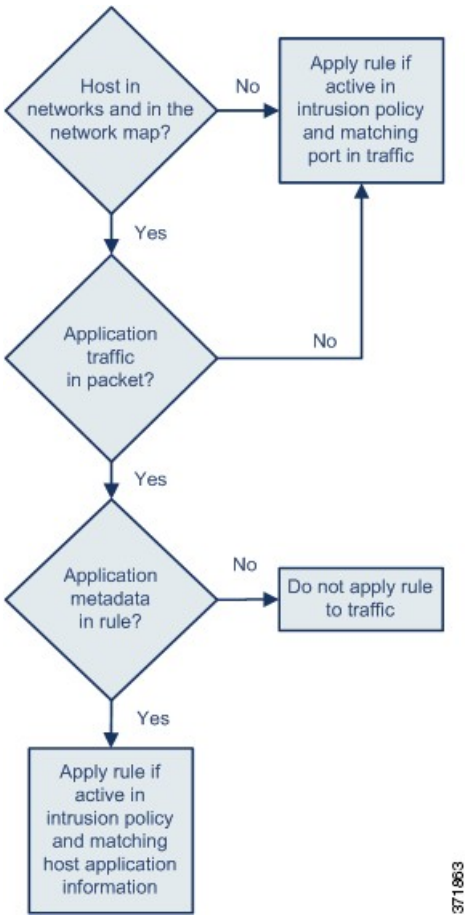
Bugtraq ID #1110 に記述されている IMAP 脆弱性について考えてみます。この脆弱性は、IMAP の実装（具体的にはLIST、LSUB、RENAME、FIND、およびCOPY コマンド）で見られます。ただし、攻撃者がこの脆弱性を悪用するには、IMAP サーバにログインする必要があります。IMAP サーバからの LOGIN 確認とそれに続く exploit は必然的に別々のパケットに存在するため、この exploit を検出する非フロー ベースのルールを作成するのは困難です。flowbits キーワードを使って一連のルールを作成すると、ユーザがIMAPサーバにログイン済みかどうかを追跡し、ログイン済みの場合は、いずれかの攻撃が検出された時点でイベントを生成できます。ユーザがログイン済みでない場合、攻撃によって脆弱性が悪用されることはないため、イベントが生成されません。

下記の 2 つのルール フラグメントはこの例を示しています。最初のルール フラグメントは IMAP サーバからの IMAP ログイン確認を検索します。

```
alert tcp any 143 -> any any (msg:"IMAP login"; content:"OK

LOGIN"; flowbits:set,logged_in; flowbits:noalert;)
```

次の図は、上記のルール フラグメントにおける flowbits キーワードの効果を示しています。

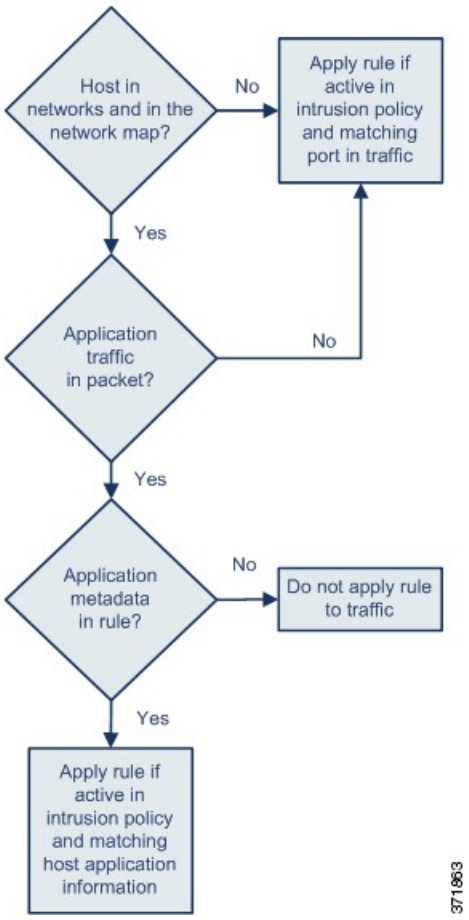


`flowbits:set` は `logged_in` 状態を設定しますが、`flowbits:noalert` がアラートを抑制することに注意してください。これは、IMAP サーバ上で多数の無害なログインセッションが見つかる可能性があるためです。

次のルール フラグメントは LIST 文字列を検索しますが、セッション内の先行パケットの結果として logged_in 状態が設定済みでない限り、イベントを生成しません。

```
alert tcp any any -> any 143 (msg:"IMAP LIST";
content:"LIST"; flowbits:isset,logged_in;)
```

次の図は、上記のルール フラグメントにおける `flowbits` キーワードの効果を示しています。



この場合、最初のフラグメントを含むルールが先行パケットによってトリガーとして使用した場合、2 番目のフラグメントを含むルールがトリガーとして使用し、イベントを生成します。

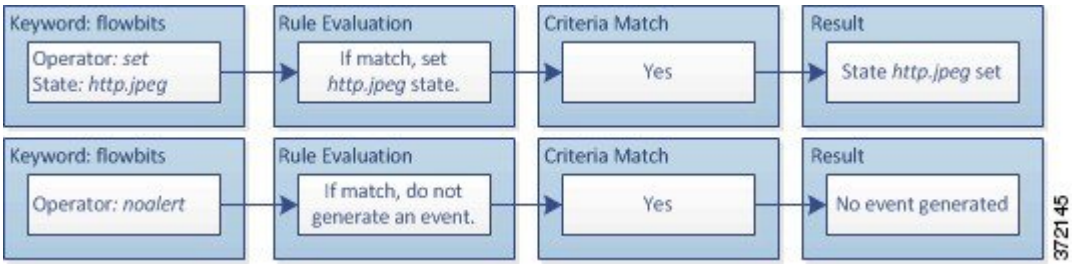
flowbits キーワードの例：誤検出イベントを引き起こす設定

後続パケット内コンテンツが、効力を失った状態を持つルールに一致することによって誤検出イベントが発生する可能性があります。複数のルールで設定された複数の状態名をグループに含めることでこれを回避できます。次の例は、複数の状態名をグループに含めない場合に誤検出が発生する可能性があることを示しています。

1 つのセッションで次の 3 つのルール フラグメントがこの順序でトリガーとして使用される場合を考えてみます。

```
(msg:"JPEG transfer";
content:"image/";pcre:"/^Content-?Type\x3a(\s*|\s*\r?\n\s+)image\x2fp?jpe?g/smi";
?flowbits:set,http.jpeg; flowbits:noalert;)
```

次の図は、上記のルール フラグメントにおける `flowbits` キーワードの効果を示しています。

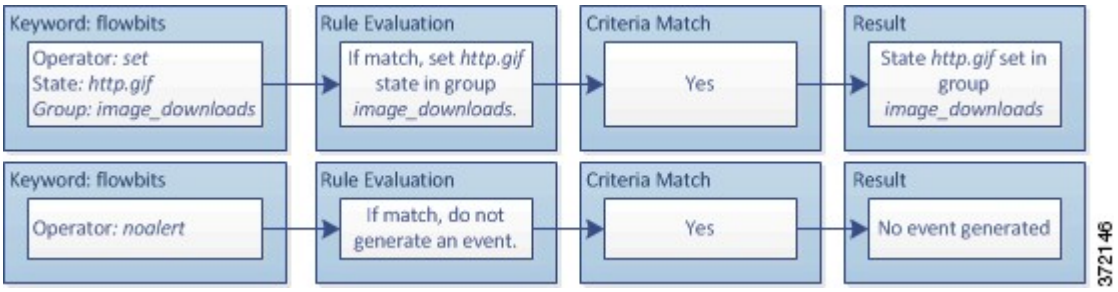


最初のルール フラグメント内の `content` キーワードと `pcre` キーワードが JPEG ファイル ダウンロードに一致し、`flowbits:set,http.jpeg` が `http.jpeg flowbits` ステートを設定し、`flowbits:noalert` はルールでのイベント生成を抑制します。イベントが生成されない理由は、このルールの目的がファイル ダウンロードを検出して `flowbits` 状態を設定することだからです。これにより、1つ以上のコンパニオン ルールで状態名を検査して有害コンテンツを探し、有害コンテンツが検出された時点でイベントを生成できます。

次のルール フラグメントは、上記の JPEG ファイル ダウンロードに続く GIF ファイル ダウンロードを検出します。

```
(msg:"GIF transfer"; content:"image/";
pcre:"/^Content-?Type\x3a(\s*|\s*\r?\n\s+)image\x2fgif/smi";
?flowbits:set,http.jpg,image_downloads; flowbits:noalert;)
```

次の図は、上記のルール フラグメントにおける `flowbits` キーワードの効果を示しています。

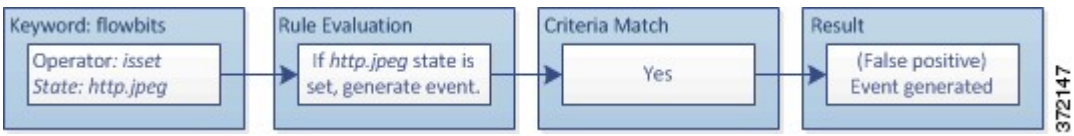


2 番目のルール内の `content` キーワードと `pcre` キーワードは GIF ファイル ダウンロードを照合し、`flowbits:set,http.jpg` は `http.jpg` flowbit ステートを設定し、`flowbits:noalert` はルールでのイベント生成を抑制します。最初のルール フラグメントで設定された `http.jpeg` 状態が不要になっても引き続き設定されていることに注意してください。これは、後続の GIF ダウンロードが検出されたときに JPEG ダウンロードが既に終了しているはずであるためです。

次に示す 3 番目のルール フラグメントは最初のルール フラグメントのコンパニオンです。

```
(msg:"JPEG exploit";?flowbits:isset,http.jpeg;content:"|FF|";
pcre:"?/\xFF[\xE1\xE2\xED\xFE]\x00[\x00\x01]/";)
```

次の図は、上記のルール フラグメントにおける `flowbits` キーワードの効果を示しています。



3 番目のルール フラグメントでは、もはや無意味になった `http.jpeg` ステートが設定されていることを `flowbits:isset,http.jpeg` が判別し、`content` と `pcre` は（GIF ファイルでは無害でも）JPEG ファイル内では有害とみなされるコンテンツを照合します。3 番目のルール フラグメントによって、JPEG ファイル内に存在しないエクスプロイトに関する誤検出イベントが生成されます。

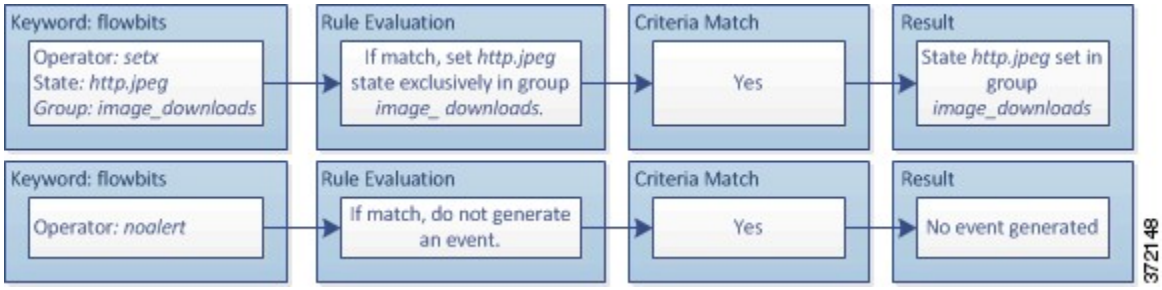
flowbits キーワードの例：誤検出イベントを防ぐための設定

次の例は、状態名をグループに含めて `setx` 演算子を使用することで、どのように誤検出を防止できるかを示しています。

前の例とほぼ同じケースを考えます。ただし、最初の 2 つのルールで、同じ状態グループに 2 つの異なる状態名が含まれるようになった点が異なります。

```
(msg:"JPEG transfer";
content:"image/";pcre:"/^Content-?Type\x3a(\s*|\s*\r?\n\s+)image\x2fp?jpe?g/smi";
?flowbits:setx,http.jpeg,image_downloads; flowbits:noalert;)
```

次の図は、上記のルール フラグメントにおける `flowbits` キーワードの効果を示しています。

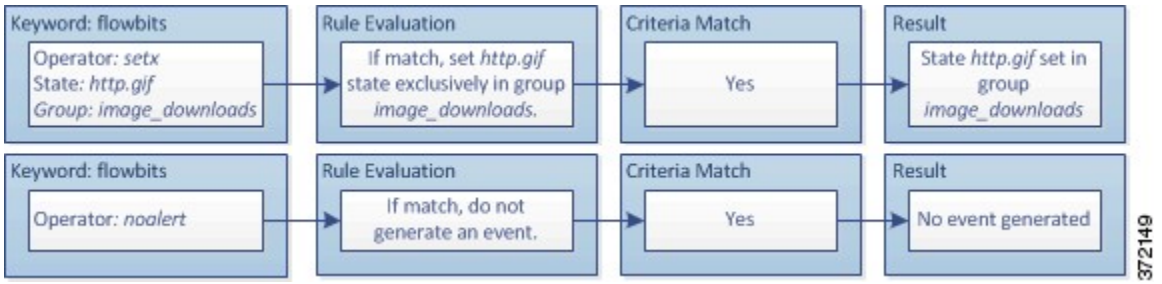


最初のルール フラグメントが JPEG ファイル ダウンロードを検出すると、`flowbits:setx,http.jpeg,image_downloads` キーワードが `flowbits` 状態を `http.jpeg` に設定し、その状態を `image_downloads` グループに含めます。

その後、次のルールが後続の GIF ファイル ダウンロードを検出します。

```
(msg:"GIF transfer"; content:"image/";
pcre:"/^Content-?Type\x3a(\s*|\s*\r?\n\s+)image\x2fgif/smi";
?flowbits:setx,http.jpg,image_downloads; flowbits:noalert;)
```

次の図は、上記のルール フラグメントにおける `flowbits` キーワードの効果を示しています。

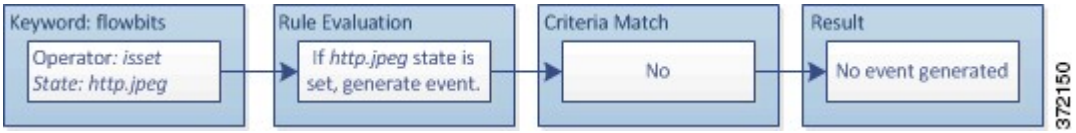


2 番目のルール フラグメントが GIF ダウンロードに一致すると、`flowbits:setx,http.jpg,image_downloads` キーワードが `http.jpg flowbits` ステートを設定し、グループ内の他のステートである `http.jpeg` を解除します。

次に示す 3 番目のルール フラグメントで誤検出は発生しません。

```
(msg:"JPEG exploit"; ?flowbits:isset,http.jpeg;content:"|FF|";
pcre:"/?\xFF[\xE1\xE2\xED\xFE]\x00[\x00\x01]/";)
```

次の図は、上記のルール フラグメントにおける `flowbits` キーワードの効果を示しています。



`flowbits:isset,http.jpeg` が false であるため、ルール エンジンはルールの処理を停止し、イベントは生成されません。こうして、GIF ファイル内のコンテンツが JPEG ファイルに関するエクスプロイト コンテンツと一致した場合でも誤検出が回避されます。

http_encode キーワード

`http_encode` キーワードを使用すると、HTTP URI、HTTP ヘッダー内の非 cookie データ、HTTP 要求ヘッダー内の cookie、HTTP 応答内の set-cookie データのいずれかにおいて、正規化前の HTTP 要求または応答内のエンコード タイプに基づいてイベントを生成できます。

HTTP 応答と HTTP cookie を検査し、`http_encode` キーワードを使用しているルールに一致したものを返すように、HTTP Inspect プリプロセッサを設定する必要があります。

また、侵入ルール内の `http_encode` キーワードで特定のエンコード タイプによってイベントがトリガーとして使用されるようにするには、HTTP Inspect プリプロセッサ設定で個々の特定のエンコード タイプのデコード オプションとアラート オプションの両方を有効にする必要があります。

次の表は、このオプションでイベントを生成できる、HTTP URI、ヘッダー、cookie、set-cookie のエンコード タイプを説明しています。

表 *221 : http_encode* エンコード タイプ

エンコード タイプ	説明
utf8	HTTP Inspect プリプロセッサによるデコードで UTF-8 エンコード タイプが有効になっている場合、指定された場所で UTF-8 エンコードを検出します。
double_encode	HTTP Inspect プリプロセッサによるデコードで二重エンコード タイプが有効になっている場合、指定された場所で二重エンコードを検出します。
non_ascii	非 ASCII 文字が検出されても、検出されたエンコード タイプが有効になっていない場合に、指定された場所で非 ASCII 文字を検出します。

エンコード タイプ	説明
uencode	HTTP Inspect プリプロセッサによるデコードで Microsoft %u エンコード タイプが有効になっている場合、指定された場所で Microsoft %u エンコードを検出します。
bare_byte	HTTP Inspect プリプロセッサによるデコードで空白バイト エンコード タイプが有効になっている場合、指定された場所で空白バイト エンコードを検出します。

関連トピック

HTTP Inspect プリプロセッサ （2333 ページ）
サーバレベルの HTTP 正規化オプション （2335 ページ）

http_encode キーワードの構文

エンコーディングの場所

HTTP URI、ヘッダー、または set-cookie などの Cookie で指定されたエンコーディング タイプを検索するかどうかを指定します。

エンコード タイプ

次のいずれかの形式を使用して、1 つ以上のエンコード タイプを指定します。

```
encode_type
encode_type|encode_type|encode_type...
```

ここで、`encode_type` は次のいずれかです。

```
utf8
double_encode
non_ascii
uencode
bare_byte.
```

否定（!）演算子と OR（|）演算子を一緒に使用できないことに注意してください。

http_encode キーワードの例：2 つの http_endcode キーワードを使用した 2 つのエンコーディングの検索

次に、同じルールで 2 つの `http_encode` キーワードを使用して、UTF-8 および Microsoft IIS %u エンコーディングの HTTP URI を検索する例を示します。

最初に、`http_encode` キーワードを使用します。

- **エンコーディングの場所**：`HTTP URI`
- **エンコーディングのタイプ**：`utf8`

次に、追加の http_encode キーワードを使用します。

- **エンコーディングの場所**：HTTP URI
- **エンコーディングのタイプ**：uencode

概要：file_type および file_group キーワード

file_type と file_group キーワードを使用すると、タイプとバージョンに基づいて、FTP、HTTP、SMTP、IMAP、POP3、NetBIOS-ssn（SMB）を介して伝送されるファイルを検出できます。1 つの侵入ルール内で複数の file_type キーワードや file_group キーワードを使用**しない**でください。

ヒント 脆弱性データベース（VDB）を更新すると、最新のファイル タイプ、バージョン、グループが侵入ルール エディタに表示されます。

（注） システムは、file_type および file_group キーワードに値を代入するためにプリプロセッサを自動的に有効にすることはしません。

file_type または file_group キーワードに一致するトラフィックに対してイベントを生成し、インライン展開では、違反パケットをドロップします。 するには、特定のプリプロセッサを有効にする**必要があります**。

表 *222 : file_type* および *file_group* の侵入イベントの生成

プロトコル	必要なプリプロセッサまたはプリプロセッサ オプション
FTP	FTP/Telnet プリプロセッサおよび [TCP ペイロードの正規化（Normalize TCP Payload）] インライン正規化プリプロセッサ オプション
HTTP	HTTP トラフィックでの侵入イベントを生成する HTTP Inspect プリプロセッサ。
SMTP	HTTP トラフィックでの侵入イベントを生成する SMTP プリプロセッサ
IMAP	IMAP プリプロセッサ
POP3	POP プリプロセッサ
NetBIOS-ssn（SMB）	DCE/RPC プリプロセッサおよび [SMB ファイル インスペクション（SMB File Inspection）] DCE/RPC プリプロセッサ オプション

関連トピック

FTP/Telnet デコーダ （2323 ページ）

インライン正規化プリプロセッサ （2403 ページ）
HTTP Inspect プリプロセッサ （2333 ページ）
SMTP プリプロセッサ （2368 ページ）
IMAP プリプロセッサ （2361 ページ）
POP プリプロセッサ （2364 ページ）
DCE/RPC プリプロセッサ （2306 ページ）

file_type キーワードと file_group キーワード

file_type

file_type キーワードを使用すると、トラフィック内で検出対象となるファイルのタイプとバージョンを指定できます。ファイル タイプ引数（**JPEG** や **PDF** など）は、トラフィックで検出するファイルの形式を識別します。

（注） 同じ侵入ルール内で file_type キーワードを別の file_type キーワードまたは file_group キーワードと一緒に**使用しないでください**。

デフォルトでは **Any Version** が選択されますが、一部のファイル タイプではバージョン オプション（たとえば PDF バージョン **1.7**）を選択することにより、トラフィックで検出対象となる特定のファイル タイプ バージョンを識別できます。

file_group

file_group キーワードを使用すると、トラフィック内で検出する類似のファイル タイプからなる Cisco 定義のグループを選択できます（**マルチメディア**、**オーディオ**など）。また、ファイル グループには、グループ内の各ファイル タイプに関する Cisco 定義のバージョンも含まれています。

（注） 同じ侵入ルール内で file_group キーワードを別の file_group キーワードまたは file_type キーワードと一緒に使用**しない**でください。

file_data キーワード

file_data キーワードは、content、byte_jump、byte_test、pcre などの他のキーワードで使用可能な位置引数の参照として機能するポインタです。file_data キーワードが指し示すデータのタイプは、検出されるトラフィックによって決まります。file_data キーワードを使用すると、次のペイロード タイプの先頭を指し示すことができます。

- HTTP 応答本文

HTTP 応答パケットを検査するには、HTTP Inspect プリプロセッサを有効にして、HTTP 応答を検査するようプリプロセッサを設定する必要があります。HTTP Inspect プリプロセッサが HTTP 応答本文データを検出した場合に、`file_data` キーワードが一致します。

- 非圧縮 gzip ファイル データ

  HTTP 応答本文内の非圧縮 gzip ファイルを検査するには、HTTP Inspect プリプロセッサを有効にする必要があり、さらに HTTP 応答を検査して HTTP 応答本文内の gzip 圧縮ファイルを復元するようプリプロセッサを設定する必要があります。詳細については、サーバレベルの HTTP 正規化オプション [HTTP 応答の検査（Inspect HTTP Responses）] および [圧縮データの検査（Inspect Compressed Data）] を参照してください。`file_data` キーワードは、HTTP Inspect プリプロセッサが HTTP 応答本文内で非圧縮 gzip データを検出した場合に一致します。

- 正規化された Javascript

  正規化された JavaScript データを検査するには、HTTP Inspect プリプロセッサを有効にして、HTTP 応答を検査するようプリプロセッサを設定する必要があります。`file_data` キーワードは、HTTP Inspect プリプロセッサが応答本文データ内で JavaScript を検出した場合に一致します。

- SMTP ペイロード

  SMTP ペイロードを検査するには、SMTP プリプロセッサを有効にする必要があります。`file_data` キーワードは、SMTP プリプロセッサが SMTP データを検出した場合に一致します。

- SMTP、POP、または IMAP トラフィック内のエンコードされた電子メール添付ファイル

  SMTP、POP、または IMAP トラフィック内の電子メール添付ファイルを検査するには、それぞれ SMTP、POP、または IMAP プリプロセッサを単独で、または任意に組み合わせて有効にする必要があります。その後、有効にしたプリプロセッサごとに、デコード対象のそれぞれの添付ファイル エンコード タイプをデコードするようプリプロセッサが設定されていることを確認する必要があります。プリプロセッサごとに設定可能な添付ファイル デコード オプションは、[Base64 復号の深さ（Base64 Decoding Depth）]、[7 ビット/8 ビット/バイナリ復号の深さ（7-Bit/8-Bit/Binary Decoding Depth）]、[Quoted Printable 復号の深さ（Quoted-Printable Decoding Depth）]、および [UNIX 間復号の深さ（Unix-to-Unix Decoding Depth）] です。

  1 つのルール内で複数の `file_data` キーワードを使用できます。

関連トピック

HTTP Inspect プリプロセッサ （2333 ページ）
サーバレベルの HTTP 正規化オプション （2335 ページ）
SMTP プリプロセッサ （2368 ページ）
IMAP プリプロセッサ （2361 ページ）

pkt_data キーワード

pkt_data キーワードは、content、byte_jump、byte_test、pcre などの他のキーワードで使用可能な位置引数の参照として機能するポインタです。

正規化された FTP、Telnet、または SMTP トラフィックが検出された場合、pkt_data キーワードは、正規化されたパケットペイロードの先頭を指します。その他のトラフィックが検出された場合、pkt_data キーワードは、未加工の TCP または UDP ペイロードの先頭を指します。

侵入ルールで検査するために、該当するトラフィックをシステムで正規化するには、次の正規化オプションを有効にする必要があります。

- 検査のために FTP トラフィックを正規化するには、FTP & Telnet プリプロセッサの [FTP コマンドでの Telnet エスケープ コードの検出（Detect Telnet Escape codes within FTP commands）] オプションを有効にします。
- 検査のために Telnet トラフィックを正規化するには、FTP & Telnet プリプロセッサの Telnet の [正規化（Normalize）] オプションを有効にします。
- 検査のために SMTP トラフィックを正規化するには、SMTP プリプロセッサの [正規化（Normalize）] オプションを有効にします。

1 つのルール内で複数の pkt_data キーワードを使用できます。

関連トピック

クライアントレベルの FTP オプション （2329 ページ）
Telnet オプション （2324 ページ）
SMTP プリプロセッサのオプション （2368 ページ）

base64_decode キーワードと base64_data キーワード

base64_decode キーワードと base64_data キーワードを組み合わせて使用すると、指定したデータを Base64 データとしてデコードおよび検査するようルール エンジンに指示できます。たとえば HTTP PUT および POST 要求内の Base64 エンコード HTTP 認証要求見出しと Base64 エンコード データを検査する場合に、これが役立つ可能性があります。

これらのキーワードは特に、HTTP 要求内の Base64 データをデコードして検査するうえで役立ちます。また、長い見出し行を複数行に拡張するために HTTP で使われるのと同じ方法でスペース文字やタブ文字を使用する SMTP などのプロトコルでも、これらを使用できます。この行拡張（折り返しとも言う）を使用するプロトコル内に行拡張が存在しない場合、後続スペース/タブを伴わない復帰または改行が出現した箇所で検査が終了します。

base64_decode

base64_decode キーワードは、パケット データを Base64 データとしてデコードするようルール エンジンに指示します。オプションの引数を使用すると、デコードするバイト数と、デコードを開始するデータ内の位置を指定できます。

base64_decode キーワードは 1 つのルール内で 1 回だけ使用可能です。また、少なくとも 1 つの base64_data キーワードのインスタンスの前にこれを配置する必要があります。

Base64 データをデコードする前に、ルール エンジンは、複数行にわたって折り返された長いヘッダーを元どおりに広げます。ルール エンジンが次のいずれかに遭遇するとデコードが終了します。

- 見出し行の末尾
- デコード対象として指定されたバイト数
- パケットの末尾

次の表に、base64_decode キーワードで使用可能な引数の説明を示します。

表 *223 : base64_decode* のオプション引数

引数	説明
Bytes	デコードするバイト数を指定します。これを指定しない場合、見出し行の末尾またはパケット ペイロード末尾のどちらかが先に出現するまでデコードが続行されます。ゼロ以外の正の値を指定できます。
Offset	パケット ペイロードの先頭を基準にしたオフセットを決定します。さらに **Relative** も指定した場合は、現在の検査位置を基準にしたオフセットを決定します。ゼロ以外の正の値を指定できます。
Relative	現在の検査位置を基準にして検査することを指定します。

base64_data

base64_data キーワードは、base64_decode キーワードを使ってデコードされた Base64 データを検査するための参照を提供します。base64_data キーワードは、デコードされた Base64 データの先頭から検査を開始するよう設定します。オプションで、content や byte_test などの他のキーワードで使用可能な位置引数を使用して、検査位置をさらに指定することもできます。

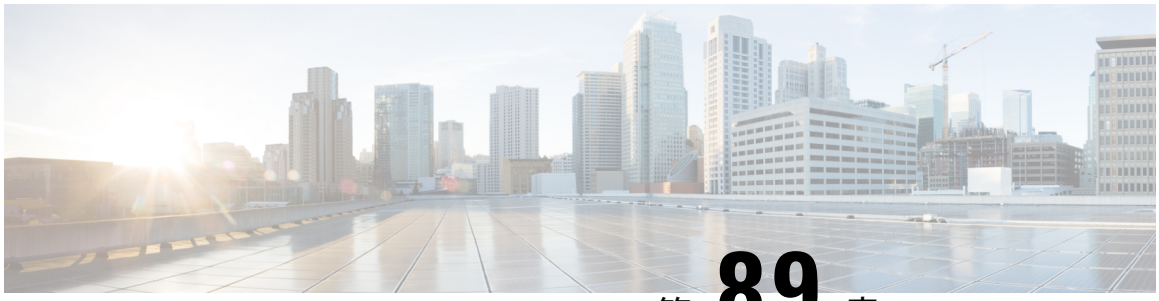
base64_decode キーワードを使用した後に base64_data キーワードを 1 回以上使用する必要があります。オプションで、base64_data を複数回使用して、デコードされた Base64 データの先頭に戻ることができます。

Base64 データを検査するときには、次の点に注意してください。

- 高速パターン マッチ機能は使用できません。
- 中間的な HTTP コンテンツ引数を使ってルール内で Base64 検査を中断する場合は、Base64 データをさらに検査する前に、別の base64_data キーワードをルールに挿入する必要があります。

関連トピック

概要：HTTP content および protected_content キーワードの引数 （2170 ページ）
content キーワードの高速パターン マッチ機能の引数 （2175 ページ）



第 89 章

侵入防御パフォーマンスの調整

以下のトピックでは、侵入防御のパフォーマンスを調整する方法について説明します。

侵入防御のパフォーマンス チューニングについて

Cisco では、侵入行為のトラフィックを分析する際のシステムのパフォーマンスを向上するための機能を提供しています。次の操作を実行できます。

- イベントキューで許可するパケット数を指定できます。ストリーム再構成の前後に、より大きなストリームに再構築されるパケットのインスペクションを有効または無効にできます。
- パケットペイロードの内容を検査するための侵入ルールで使用される PCRE のデフォルトの一致および再帰の制限をオーバーライドできます。
- 複数のイベントが生成された場合にパケットまたはパケットストリームごとに複数のイベントをルールエンジンがログに記録するようにして、レポートされるイベント以外の情報も収集できます。
- デバイスの遅延をパケットおよびルール遅延しきい値構成の許容レベルで保持する必要性とセキュリティのバランスを保つことができます。
- デバイスがそのパフォーマンスをモニタおよび報告する動作に関する基本的なパラメータを設定できます。システムがデバイスのパフォーマンス統計情報を更新する間隔を指定できます。

これらのパフォーマンス設定は、各アクセス コントロール ポリシーごとに設定し、その設定はその親のアクセス コントロール ポリシーによって呼び出されるすべての侵入ポリシーに適用されます。

侵入に対するパターン一致の制限

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Access Admin/Network Admin

ステップ 1 アクセス コントロール ポリシー エディタで、[詳細（Advanced）] タブをクリックします。

ステップ 2 [パフォーマンス設定（Performance Settings）] の横にある編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ポリシーから継承され、設定を変更する権限がありません。設定がロック解除されている場合は、[Inherit from base policy] をオフにして、編集を有効にします。

ステップ 3 [パフォーマンス設定（Performance Settings）] ポップアップ ウィンドウ内の [パターン一致の制限（Pattern Matching Limits）] タブをクリックします。

ステップ 4 [パケットごとに分析するパターン状態の最大値（Maximum Pattern States to Analyze Per Packet）] フィールドに、キューに含めるイベントの最大数の値を入力します。

ステップ 5 ストリーム再構成の前後で、データのより大きなストリームに再構築されるパケットのインスペクションを無効にするには、[今後の再構成の対象となるトラフィックでコンテンツ チェックを無効にする（Disable Content Checks on Traffic Subject to Future Reassembly）] チェックボックスをオンにします。再構成の前後の検査はより多くの処理オーバーヘッドを必要とするため、パフォーマンスが低下する可能性があります。

ステップ 6 [OK] をクリックします。

ステップ 7 [保存（Save）] をクリックしてポリシーを保存します。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

正規表現による侵入ルールのオーバーライドの制限

デフォルトの正規表現の制限によってパフォーマンスの最低レベルが確保されます。これらの制限をオーバーライドすると、セキュリティが向上する可能性がありますが、非効率的な正規

表現に対してパケット評価を許可することで、パフォーマンスが著しく影響を受ける可能性もあります。

⚠

注意 非効率的なパターンの影響に関する知識があり、侵入ルールの作成経験が豊富であるユーザ以外は、デフォルトの PCRE の制限をオーバーライドしないでください。

表 *224*: 正規表現の制約オプション

オプション	説明
Match Limit State	[Match Limit] をオーバーライドするかどうかを指定します。次の選択肢があります。 • [デフォルト（Default）] を選択して、[制限に合わせる（Match Limit）] に設定した値を使用する • [Unlimited] を選択して、無制限の数の試行を許可する • [カスタム（Custom）] を選択して、[制限に合わせる（Match Limit）] に対して 1 以上の制限を指定するか、または PCRE の一致の評価を完全に無効化するために 0 を指定する
Match Limit	PCRE 正規表現で定義されたパターンに一致することを試行する回数を指定します。
Match Recursion Limit State	[Match Recursion Limit] をオーバーライドするかどうかを指定します。次の選択肢があります。 • [Default] を選択して、[Match Recursion Limit] に設定した値を使用する • [Unlimited] を選択して、無制限の数の再帰を許可する • [Custom] を選択して、[Match Recursion Limit] に対して 1 以上の制限を指定するか、または PCRE の再帰を完全に無効化するために 0 を指定する [Match Recursion Limit] が意味を持つためには、[Match Limit] よりも小さい必要があることに注意してください。

オプション	説明
Match Recursion Limit	パケット ペイロードに対して PCRE 正規表現を評価する際の再帰数を指定します。

関連トピック

概要：pcre キーワード （2190 ページ）

侵入ルールの正規表現制限のオーバーライド

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Access Admin/Network Admin

ステップ 1 アクセス コントロール ポリシー エディタで、[詳細（Advanced）] タブをクリックします。

ステップ 2 [パフォーマンス設定（Performance Settings）] の横にある編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ポリシーから継承され、設定を変更する権限がありません。設定がロック解除されている場合は、[Inherit from base policy] をオフにして、編集を有効にします。

ステップ 3 [パフォーマンス設定（Performance Settings）] ポップアップ ウィンドウ内の [正規表現の制限（Regular Expression Limits）] タブをクリックします。

ステップ 4 正規表現による侵入ルールのオーバーライドの制限（2272 ページ）に示したオプションを変更できます。

ステップ 5 [OK] をクリックします。

ステップ 6 [保存（Save）] をクリックしてポリシーを保存します。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

パケットごとの侵入イベント生成の制限

侵入ルールエンジンがルールに対してトラフィックを評価する場合、特定のパケットまたはパケット ストリームに生成されたイベントをイベント キューに配置し、キュー内の上位のイベントをユーザインターフェイスに報告します。侵入イベントロギングの制限を設定する場合、

キュー内に配置可能なイベントの数および記録されるイベントの数を指定できます。また、キュー内のイベントの順序を決定する条件を選択できます。

表 *225 :* 侵入イベント ロギング制限のオプション

オプション	説明
Maximum Events Stored Per Packet	特定のパケットまたはパケット ストリームに対して保存できるイベントの最大数。
Maximum Events Logged Per Packet	特定のパケットまたはパケット ストリームに対して記録されるイベントの数。これは、[Maximum Events Stored Per Packet] の値を超えてはいけません。
Prioritize Event Logging By	イベント キュー内のイベントの順序を決定するために使用する値。最上位のイベントがユーザ インターフェイスから報告されます。次の中から選択できます。 • `priority`。イベントの優先順位によってキュー内のイベントを並べ替えます。 • `content_length`。最も長い識別コンテンツの一致によってイベントを並べ替えます。イベントがコンテンツ長によって並べ替えられる場合、ルール イベントは常にデコーダ イベントおよびプリプロセッサ イベントよりも優先されます。

パケットごとに生成される侵入イベントの制限

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Access Admin/Network Admin

ステップ 1 アクセス コントロール ポリシー エディタで、[詳細（Advanced）] タブをクリックします。

ステップ 2 [パフォーマンス設定（Performance Settings）] の横にある編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ポリシーから継承され、設定を変更する権限がありません。設定がロック解除されている場合は、[Inherit from base policy] をオフにして、編集を有効にします。

ステップ 3 [パフォーマンス設定（Performance Settings）] ポップアップ ウィンドウ内の [侵入イベントのログ制限（Intrusion Event Logging Limits）] タブをクリックします。

ステップ 4 パケットごとの侵入イベント生成の制限 （2274 ページ） に示したオプションを変更できます。

ステップ 5 [OK] をクリックします。

ステップ 6 [保存（Save）] をクリックしてポリシーを保存します。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

パケットおよび侵入ルールの遅延しきい値構成

各アクセス コントロール ポリシーには、しきい値を使用してパケットとルールの処理パフォーマンスを管理する、遅延ベースの設定があります。

パケット遅延しきい値構成は、該当するデコーダ、プリプロセッサ、およびルールによるパケット処理の総経過時間を測定し、処理時間が設定可能なしきい値を超えるとパケットのインスペクションを終了します。

ルール遅延しきい値構成は、各ルールが個別のパケットの処理に費やした時間を測定し、処理時間が遅延しきい値ルールをある回数（設定可能）連続して超えた場合は、そのルールに違反した処理を、関連するルールのグループとともに指定された期間中断し、中断期間終了後にルールを回復します。

遅延ベースのパフォーマンス設定

デフォルトでシステムが使用するパフォーマンス設定は、システムに導入された最新の侵入ルールの更新の遅延ベースのパフォーマンス設定です。

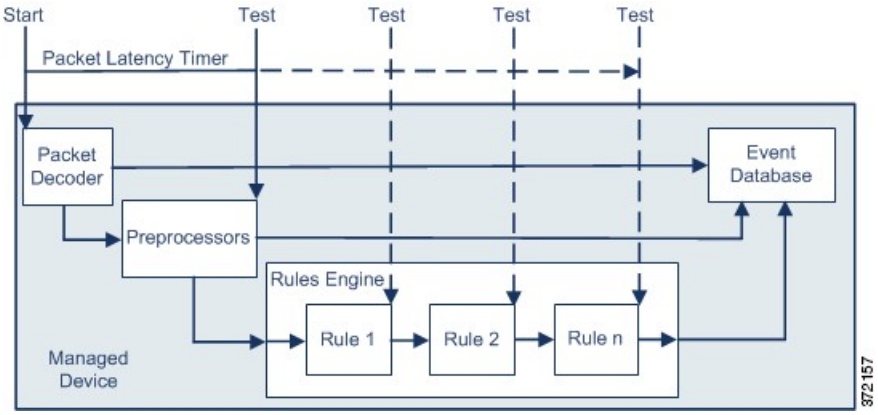
実際に適用される遅延の設定は、アクセス コントロール ポリシーと関連付けられているネットワーク分析ポリシー（NAP）のセキュリティ レベルによって異なります。通常、デフォルトの NAP ポリシーが関連付けられます。ただし、カスタム ネットワーク分析ルールが設定されている場合、ルールの中にデフォルトの NAP ポリシーより強力な NAP ポリシーを指定しているものがあれば、カスタム ルールの中で最もセキュアな NAP ポリシーが、遅延の設定のベースとなります。デフォルトの NAP ポリシーまたはカスタム ルールによってカスタム NAP ポリシーが呼び出された場合、評価で使用されるセキュリティ レベルは、それぞれのカスタム NAP ポリシーがベースとするシステム提供のベース ポリシーになります。

以上の説明は、有効なしきい値やネットワーク分析の設定が継承されるか、ポリシーに直接構成されるかにかかわらず当てはまります。

パケット遅延しきい値構成

パケット遅延しきい値構成は、ルールがパケットを処理する際に必要な実際の時間をより正確に反映するために、処理時間のみでなく、経過時間を測定します。ただし、遅延しきい値構成は、厳密なタイミングを強制しないソフトウェア ベースの遅延実装です。

遅延しきい値構成から生じるパフォーマンスと遅延のメリットに関するトレードオフは、未検査パケットに攻撃が含まれる可能性があることです。デコーダの処理の開始時に各パケットのタイマーが起動します。タイミングは、パケットのすべての処理が終了するか、または処理時間がタイミング テスト ポイントでしきい値を超えるまで継続します。



上の図に示すように、パケット遅延タイミングは次のテスト ポイントでテストされます。

- すべてのデコーダおよびプリプロセッサの処理の完了後、ルールの処理が開始される前
- 各ルールによる処理の後

処理時間がいずれかのテスト ポイントでしきい値を超えると、パケット インスペクションは終了します。

ヒント パケットの合計処理時間にルーチン TCP ストリームまたは IP フラグメント再構成の時間は含まれません。

パケット遅延しきい値構成は、パケットを処理するデコーダ、プリプロセッサ、またはルールによってトリガーされるイベントに影響を与えません。該当するデコーダ、プリプロセッサ、またはルールは、パケットが完全に処理されるか、または遅延しきい値を超えたためにパケット処理が終了されるか、どちらか先に発生した時点まで通常通りトリガーされます。廃棄ルールがインライン展開の侵入を検知すると、その廃棄ルールがイベントをトリガーし、パケットは廃棄されます。

（注） パケット遅延しきい値違反のためにパケットの処理が終了した後は、ルールに対してパケットは評価されません。イベントを引き起こす可能性があったルールはそのイベントをトリガーできず、廃棄ルールに対してパケットを廃棄できません。

パケット遅延しきい値構成は、パッシブとインラインの両方の展開でシステムのパフォーマンスを向上することができます。また、過剰な処理時間を必要とするパケットのインスペクションを停止することで、インライン展開の遅延を減らすことができます。これらのパフォーマンスのメリットは、たとえば次の場合に得られる可能性があります。

- パッシブ展開およびインライン展開の両方で、複数のルールによるパケットの順次検査に長時間かかる場合
- インライン展開で、ユーザが非常に大きなファイルをダウンロードするときなど、ネットワーク パフォーマンスの低下がパケット処理を遅らせる場合

パッシブ展開では、パケットの処理を停止しても、処理が単に次のパケットに移るだけで、ネットワーク パフォーマンスの回復につながらない可能性があります。

パケット遅延しきい値構成の注意事項

デフォルトでは、パケットとルールの両方の処理に関する遅延ベースのパフォーマンス設定が、展開された最新の侵入ルールの更新によって自動的に入力されるため、デフォルトを変更しないことをお勧めします。

このトピックの情報は、カスタム値の指定を選択した場合にのみ適用されます。

表 *226*：パケット遅延しきい値構成オプション

オプション	説明
しきい値（マイクロ秒）	パケットのインスペクションが終了する時間をマイクロ秒単位で指定します。

ルール 134:3 を有効にして、パケット遅延しきい値を超えたためにシステムがパケットのインスペクションを終了する場合に イベントを生成し、インライン展開では、違反パケットをドロップします。 できます。詳細については、侵入ルールの状態オプション（2092 ページ）を参照してください。

パケット遅延しきい値の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Access Admin/Network Admin

（注） デフォルトでは、パケットとルールの両方の処理に関する遅延ベースのパフォーマンス設定が、展開された最新の侵入ルールの更新によって自動的に入力されるため、デフォルトを変更しないことをお勧めします。

ステップ 1 アクセス コントロール ポリシー エディタで、[詳細（Advanced）] タブをクリックします。

ステップ 2 [遅延ベースのパフォーマンス設定（Latency-Based Performance Settings）] の横にある編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ポリシーから継承され、設定を変更する権限がありません。

ステップ 3 設定がロック解除されている場合は、[Inherit from base policy] をオフにして、編集を有効にします。

ステップ 4 [遅延ベースのパフォーマンス設定（Latency-Based Performance Settings）] ポップアップ ウィンドウで [パケット処理（Packet Handling）] タブをクリックします。

デフォルトでは、[インストールされたルールの更新（Installed Rule Update）] が選択されます。シスコはこのデフォルトを使用することを推奨します。

表示される値は、自動化された設定を反映しません。

ステップ 5 カスタム値を指定する場合は、次の点に注意してください。

- 推奨される最小しきい値の設定については、パケット遅延しきい値構成の注意事項（2278 ページ）を参照してください。
- パケット処理タブとルール処理タブの両方にカスタム値を指定する必要があります。

ステップ 6 [OK] をクリックします。

ステップ 7 [保存（Save）] をクリックしてポリシーを保存します。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

ルール遅延しきい値構成

ルール遅延しきい値構成は、ルールがパケットを処理する際に必要な実際の時間をより正確に反映するために、処理時間のみでなく、経過時間を測定します。ただし、遅延しきい値構成は、厳密なタイミングを強制しないソフトウェア ベースの遅延実装です。

遅延しきい値構成から生じるパフォーマンスと遅延のメリットに関するトレードオフは、未検査パケットに攻撃が含まれる可能性があることです。パケットがルールのグループに対して処理されるたびに、タイマーが処理時間を測定します。ルール処理時間が指定されたルール遅延

しきい値を超えると、システムでカウンタが増加します。連続したしきい値違反の数が指定した数に達すると、システムは次のアクションを実行します。

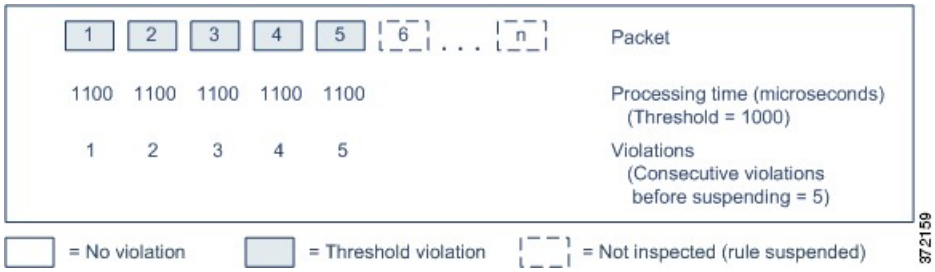
- 指定された時間、ルールを一時停止する
- ルールが一時停止されたことを示すイベントをトリガーとして使用する
- 一時停止期間が過ぎたらルールを再度有効にする
- ルールが再び有効になったことを示すイベントをトリガーとして使用する

ルールのグループが一時停止しているか、またはルール違反が連続していない場合は、カウンタがゼロになります。ルールを一時停止する前に連続する違反の一部を許可することにより、パフォーマンスへの影響がわずかであると考えられる散発的なルール違反を無視し、繰り返しルール遅延しきい値を超えるルールのより重大な影響に焦点を当てることができます。

次の例は、ルールが一時停止にならない、5 つの連続したルール処理時間を示します。

上の例で、最初の 3 個の各パケットの処理に必要な時間は 1000 マイクロ秒というルール遅延しきい値に違反し、違反カウンタは各違反のたびに増加します。4 個目のパケット処理はしきい値に違反しないので、違反カウンタはゼロにリセットされます。5 個目のパケットはしきい値に違反し、違反カウンタは 1 から再開します。

次の例は、ルールが一時停止になる、5 つの連続したルール処理時間を示します。



2 番目の例で、5 個のパケットのそれぞれの処理に必要な時間は 1000 マイクロ秒というルール遅延しきい値に違反します。各パケットの 1100 マイクロ秒というルール処理時間が指定された連続する 5 回の違反に対する 1000 マイクロ秒というしきい値に違反するため、ルールのグループは一時停止されます。図中のパケット 6 から n で表される後続のパケットは、一時停止期間が経過するまで、一時停止されたルールに対して検査されません。ルールが再有効化された後にさらにパケットが発生すると、違反カウンタはゼロから再開されます。

ルール遅延しきい値構成は、パケットを処理するルールによってトリガーされる侵入イベントに影響を及ぼしません。ルール処理時間がしきい値を超えるかどうかにかかわらず、パケット内で検出されるすべての侵入に対して、ルールはイベントをトリガーします。侵入を検知するルールがインライン展開の廃棄ルールである場合、パケットは廃棄されます。廃棄ルールがパケット内で侵入を検出し、その結果ルールが一時停止されると、廃棄ルールは侵入イベントをトリガーし、パケットは廃棄され、そのルールと関連するすべてのルールが一時停止されます。

（注） パケットは一時停止されたルールに対して評価されません。イベントを引き起こす可能性があった一時停止ルールはそのイベントをトリガーできず、廃棄ルールに対してパケットを廃棄できません。

ルール遅延しきい値構成は、パッシブとインラインの両方の展開でシステムのパフォーマンスを向上することができます。また、パケットの処理に最も多くの時間を必要とするルールを一時停止することで、インライン展開の遅延を減らすことができます。設定可能な時間が過ぎるまで、パケットは一時停止されたルールに対して再度評価されず、過負荷のデバイスに回復の時間が与えられます。これらのパフォーマンスのメリットは、たとえば次の場合に得られる可能性があります。

- 短期間で作成され、ほとんどテストされていないルールが過剰な処理時間を必要とする場合
- ユーザが非常に大きなファイルをダウンロードするときなど、ネットワーク パフォーマンスの低下がパケット インスペクションを遅らせる場合

ルール遅延しきい値構成の注記

デフォルトでは、パケットとルールの両方の処理に関する遅延ベースのパフォーマンス設定が、展開された最新の侵入ルールの更新によって自動的に入力されるため、デフォルトを変更しないことをお勧めします。

このトピックの情報は、カスタム値の指定を選択した場合にのみ適用されます。

ルールによるパケット処理時間が、[Consecutive Threshold Violations Before Suspending Rule] で指定された回数連続して [Threshold] を超えると、ルール遅延しきい値構成は [Suspension Time] で指定された時間、ルールを一時停止します。

ルール 134:1 を有効にして、ルールが一時停止されるときにイベントを生成できます。また、ルール 134:2 を有効にして、一時停止されたルールが有効化されるときにイベントを生成できます。侵入ルールの状態オプション （2092 ページ）を参照してください。

表 *227:* ルール遅延しきい値構成のオプション

オプション	説明
Threshold	ルールがパケットを検査する際に超えることができない時間をマイクロ秒単位で指定します。
Consecutive Threshold Violations Before Suspending Rule	ルールが一時停止される前に、ルールによるパケットの検査時間が [Threshold] で設定された時間を超えることができる、連続した回数を指定します。
Suspension Time	ルールのグループを一時停止する秒数を指定します。

ルール遅延しきい値の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Access Admin/Network Admin

（注） デフォルトでは、パケットとルールの両方の処理に関する遅延ベースのパフォーマンス設定が、展開された最新の侵入ルールの更新によって自動的に入力されるため、デフォルトを変更しないことをお勧めします。

ステップ 1 アクセス コントロール ポリシー エディタで、[詳細（Advanced）] タブをクリックします。

ステップ 2 [遅延ベースのパフォーマンス設定（Latency-Based Performance Settings）] の横にある編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ポリシーから継承され、設定を変更する権限がありません。 設定がロック解除されている場合は、[Inherit from base policy] をオフにして、編集を有効にします。

ステップ 3 [遅延ベースのパフォーマンス設定（Latency-Based Performance Settings）] ポップアップ ウィンドウで [ルール処理（Rule Handling）] タブをクリックします。

デフォルトでは、[インストールされたルールの更新（Installed Rule Update）] が選択されます。シスコはこのデフォルトを使用することを推奨します。

表示される値は、自動化された設定を反映しません。

ステップ 4 カスタム値を指定する場合は、次の点に注意してください。

- ルール遅延しきい値構成の注記 （2281 ページ）の任意のオプションを設定できます。
- パケット処理タブとルール処理タブの両方にカスタム値を指定する必要があります。

ステップ 5 [OK] をクリックします。

ステップ 6 [保存（Save）] をクリックしてポリシーを保存します。

次のタスク

- イベントを生成するには、遅延ルール（134:1 と 134:2）を有効にします。詳細については、「侵入ルールの状態オプション （2092 ページ）」を参照してください。
- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

侵入パフォーマンス統計情報のロギング設定

[サンプル時間（秒）（Sample time (seconds)）] と [パケットの最小数（Minimum number of packets）]

パフォーマンス統計情報の各更新の間で指定した秒数が経過すると、システムは指定したパケット数を分析したかを検証します。分析していた場合、システムはパフォーマンス統計情報を更新します。それ以外の場合、システムは指定したパケット数を分析するまで待機します。

Troubleshooting Options：Log Session/Protocol Distribution

トラブルシューティングの電話中に、プロトコル分布、パケット長、およびポートの統計情報のログを取るようにサポートから依頼される場合があります。

注意 サポートによって指示された場合を除き、[ログセッション/プロトコル分布（Log Session/Protocol Distribution）] を有効にしないでください。

トラブルシューティング オプション：[概要（Summary）]

トラブルシューティングの電話中に、Snortプロセスのシャットダウンまたは再起動時に限り、パフォーマンス統計情報を計算するようにシステムを設定するようにサポートから依頼される場合があります。このオプションを有効にするには、[ログ セッション/プロトコル分布（Log Session/Protocol Distribution）] トラブルシューティング オプションも有効にする必要があります。

注意 サポートから指示された場合を除き、[概要（Summary）] を有効にしないでください。

侵入パフォーマンス統計情報のロギングの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Access Admin/Network Admin

ステップ 1 アクセス コントロール ポリシー エディタで [詳細（Advanced）] タブをクリックし、[パフォーマンス設定（Performance Settings）] の横にある編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ポリシーから継承され、設定を変更する権限がありません。設定がロック解除されている場合は、[Inherit from base policy] をオフにして、編集を有効にします。

ステップ 2 表示されるポップアップ ウィンドウの [パフォーマンス統計情報（Performance Statistics）] タブをクリックします。

ステップ 3 前述のように、[Sample time] または [Minimum number of packets] を変更します。

ステップ 4 任意で、サポートによって求められた場合にのみ、[Troubleshoot Options] セクションを展開し、そのオプションを変更します。

ステップ 5 [OK] をクリックします。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

第 XXI 部

高度なネットワーク分析と前処理

第 90 章

ネットワーク分析/侵入ポリシーのための高度なアクセス制御の設定

以下のトピックでは、ネットワーク分析ポリシーと侵入ポリシー用の高度な設定を行う手順を示します。

ネットワーク分析および侵入ポリシーのアクセスコントロールの詳細設定について

アクセス コントロール ポリシーにおける詳細設定の多くは、設定のために特定の専門知識を要する侵入検知設定と予防設定を制御します。通常、詳細設定はほとんど、あるいはまったく変更する必要がありません。詳細設定は導入環境ごとに異なります。

デフォルトの侵入ポリシー

各アクセス コントロール ポリシーは、システムがトラフィックを検査する方法を正確に決定する前に、デフォルトの侵入ポリシーを使用してそのトラフィックを最初に検査します。これは、場合によってシステムがトラフィックを処理するアクセス コントロール ルール（存在する場合）を決定する前に、接続の最初の数パケットを処理し**通過を許可する**必要があるため必要となります。しかし、これらのパケットは検査されないまま宛先に到達することはないので、デフォルト侵入ポリシーと呼ばれる侵入ポリシーを使用して、パケットを検査し侵入イベントを生成できます。デフォルトでは、デフォルトの侵入ポリシーでデフォルトの変数セットが使用されます。

システムはクライアントとサーバの間で接続が完全に確立される前にアプリケーションを識別したり URL をフィルタ処理することはできないので、デフォルトの侵入ポリシーは、アプリ

ケーション制御およびURLフィルタリングを実行する場合に特に有用です。たとえば、パケットがアプリケーションまたはURL条件を持つアクセス コントロール ルールのその他のすべての条件に一致する場合、そのパケットと後続のパケットは、接続が確立されてアプリケーションまたはURLの識別が完了するまで通過することを許可されます。通常は3～5パケットです。

システムはこれらの許可されたパケットをデフォルトの侵入ポリシーで検査し、これによってイベントを生成したり、インラインで配置されている場合は、悪意のあるトラフィックをブロックできます。システムが接続を処理する必要があるアクセス コントロール ルールまたはデフォルトアクションを識別した後、接続内の残りのパケットが適宜処理され検査されます。

アクセス コントロール ポリシーを作成する場合、そのデフォルトの侵入ポリシーは**最初に**選択したデフォルト アクションによって異なります。アクセス コントロールの初期のデフォルト侵入ポリシーは次のとおりです。

- 最初に [Intrusion Prevention] デフォルト アクションを選択した場合、アクセス コントロール ポリシーのデフォルトの侵入ポリシーはBalanced Security and Connectivity（システムによって提供されるポリシー）になります。
- 最初に [Block all traffic] または [Network Discovery] デフォルト アクションを選択した場合、アクセス コントロール ポリシーのデフォルトの侵入ポリシーはNo Rules Activeになります。このオプションを選択すると、前述の許可されたパケットでの侵入インスペクションが無効になりますが、侵入データが必要なければ、パフォーマンスを向上できます。

（注） （たとえば、検出専用の導入において）侵入インスペクションを実行していない場合は、デフォルトの侵入ポリシーとしてNo Rules Activeポリシーを保持してください。

アクセスコントロールポリシーを作成した後にデフォルトアクションを変更する場合、デフォルトの侵入ポリシーは自動的には変更され**ません**。手動で変更するには、アクセスコントロール ポリシーの詳細オプションを使用します。

システムによって作成されたポリシーまたはユーザが作成したポリシーを選択できます。

（注） 最初に一致したネットワーク分析ルールに関連付けられているネットワーク分析ポリシーが、デフォルトの侵入ポリシーに対してトラフィックを前処理します。ネットワーク分析ルールがない場合、あるいはどのルールも一致しない場合は、デフォルトのネットワーク分析ポリシーが使用されます。

デフォルトの侵入ポリシーの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Access Admin/Network Admin

ステップ 1 アクセス コントロール ポリシー エディタで、[詳細設定（Advanced）] タブをクリックし、[ネットワーク分析と侵入ポリシー（Network Analysis and Intrusion Policies）] セクションの横にある編集アイコン（）をクリックします。

代わりに表示アイコン（  ）が表示される場合、設定は先祖ポリシーから継承され、設定を変更する権限がありません。 設定がロック解除されている場合は、[Inherit from base policy] をオフにして、編集を有効にします。

ステップ 2 [アクセス制御ルールが決定される前に使用されている侵入ポリシー（ntrusion Policy used before Access Control rule is determined）] ドロップダウン リストから、侵入ポリシーを選択します。

ユーザが作成したポリシーを選択した場合は、編集アイコン（）をクリックして、新しいウィンドウでポリシーを編集できます。システムによって提供されたポリシーは編集できません。

ステップ 3 必要に応じて、[侵入ポリシーの変数セット（Intrusion Policy Variable Set）] ドロップダウン リストから別の変数セットを選択します。変数セットの横にある編集アイコン（）を選択して、変数セットを作成および編集することもできます。変数セットを変更しない場合、システムはデフォルトのセットを使用します。

ステップ 4 [OK] をクリックします。

ステップ 5 [保存（Save）] をクリックしてポリシーを保存します。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

関連トピック

変数セット （538 ページ）

ネットワーク分析プロファイルの詳細設定

ネットワーク分析ポリシーは、特に侵入の試みの前兆となるかもしれない異常トラフィックに対し、そのトラフィックがさらに評価されるようにトラフィックをデコードおよび前処理する方法を制御します。トラフィックの前処理は、セキュリティインテリジェンスのブラックリスト登録およびトラフィックの復号化の後、侵入ポリシーによるパケットインスペクションの前

に行われます。デフォルトでは、システム提供の [バランスの取れたセキュリティと接続（Balanced Security and Connectivity）] ネットワーク分析ポリシーが、デフォルト ネットワーク分析ポリシーです。

ヒント　システムによって提供される [バランスの取れたセキュリティと接続（Balanced Security and Connectivity）] ネットワーク分析ポリシーおよび [バランスの取れたセキュリティと接続（Balanced Security and Connectivity）] 侵入ポリシーは共に機能し、侵入ルールの更新の際に両方とも更新できます。ただし、ネットワーク分析ポリシーは主に前処理オプションを管理し、侵入ポリシーは主に侵入ルールを管理します。

前処理を調整する簡単な方法は、カスタム ネットワーク分析ポリシーを作成し、それをデフォルトとして使用することです。複雑な環境での高度なユーザの場合は、複数のネットワーク分析ポリシーを作成し、それぞれがトラフィックを別々に前処理するように調整することができます。さらに、トラフィックのセキュリティ ゾーン、ネットワーク、または VLAN に応じて前処理が制御されるようにこれらのポリシーを設定できます。

これを実現するには、アクセス コントロール ポリシーにカスタム ネットワーク分析ルールを追加します。ネットワーク分析ルールは、これらの条件に一致するトラフィックを前処理する方法を指定する設定および条件の単純なセットにすぎません。既存のアクセス コントロール ポリシーの詳細オプションでネットワーク分析ルールを作成および編集します。各ルールは 1 つのポリシーにのみ属します。

各ルールに含まれる内容は、次のとおりです。

- 一連のルール条件。前処理の対象となる特定のトラフィックを識別します
- 関連付けられたネットワーク分析ポリシー。すべてのルールの条件を満たすトラフィックを前処理するために使用できます

システムがトラフィックを前処理するときに、パケットはルール番号の上位から下位の順序でネットワーク分析ルールに照合されます。いずれのネットワーク分析ルールにも一致しないトラフィックは、デフォルトのネットワーク分析ポリシーによって前処理されます。

デフォルトのネットワーク分析ポリシーの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Access Admin/Network Admin

システムによって作成されたポリシーまたはユーザが作成したポリシーを選択できます。

（注） プリプロセッサを無効にしているが、システムは有効になっている侵入ルールまたはプリプロセッサルールと照合して前処理されたパケットを評価する必要がある場合、システムはプリプロセッサを自動的に有効にして使用します。しかし、ネットワーク分析ポリシーWebインターフェイスでは無効のままです。前処理の調整、特に複数のカスタムネットワーク分析ポリシーを使用して調整することは、**高度な**タスクです。前処理および侵入インスペクションは密接に関連しているため、単一パケットを検査するネットワーク分析ポリシーと侵入ポリシーが互いに補完することを許可する場合は慎重になる**必要があります**。

ステップ 1 アクセス コントロール ポリシー エディタで、[詳細設定（Advanced）] タブをクリックし、[ネットワーク分析と侵入ポリシー（Network Analysis and Intrusion Policies）] セクションの横にある編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ポリシーから継承され、設定を変更する権限がありません。 設定がロック解除されている場合は、[Inherit from base policy] をオフにして、編集を有効にします。

ステップ 2 [デフォルトのネットワーク分析ポリシー（Default Network Analysis Policy）] ドロップダウンリストから、デフォルトのネットワーク分析ポリシーを選択します。

ユーザが作成したポリシーを選択した場合は、編集アイコン（）をクリックして、新しいウィンドウでポリシーを編集できます。システムによって提供されたポリシーは編集できません。

ステップ 3 [OK] をクリックします。

ステップ 4 [保存（Save）] をクリックしてポリシーを保存します。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

関連トピック

カスタム ポリシーの制限 （2037 ページ）

ネットワーク分析ルール

アクセスコントロールポリシーの詳細設定で、ネットワーク分析ルールを使用してネットワーク トラフィックへの前処理設定を調整できます。

ネットワーク分析ルールには1から番号が付けられます。システムがトラフィックを前処理するときに、パケットはルール番号の昇順で上から順にネットワーク分析ルールに照合され、すべてのルールの条件が一致する最初のルールに従ってトラフィックが前処理されます。

ルールには、ゾーン、ネットワーク、VLANタグの条件を追加できます。ルールに対し特定の条件を設定しない場合、システムはその基準に基づいてトラフィックを照合しません。たとえ

ば、ネットワーク条件を持つがゾーン条件を持たないルールは、その入力または出力インターフェイスに関係なく、送信元または宛先 IP アドレスに基づいてトラフィックを評価します。いずれのネットワーク分析ルールにも一致しないトラフィックは、デフォルトのネットワーク分析ポリシーによって前処理されます。

ネットワーク分析ルールの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Access Admin/Network Admin

ステップ 1 アクセス コントロール ポリシー エディタで [詳細（Advanced）] タブをクリックし、[ネットワーク分析（Network Analysis）] および [侵入ポリシー（Intrusion Policies）] セクションの横にある編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ポリシーから継承され、設定を変更する権限がありません。設定がロック解除されている場合は、[Inherit from base policy] をオフにして、編集を有効にします。

ヒント [ネットワーク分析ポリシー リスト（Network Analysis Policy List）] をクリックし、既存のカスタム ネットワーク分析ポリシーを表示および編集します。

ステップ 2 [ネットワーク分析ルール（Network Analysis Rules）] の横にある、所持しているカスタム ルールの数を示したステートメントをクリックします。

ステップ 3 [ルールの追加（Add Rule）] をクリックします。

ステップ 4 追加する条件に対応するタブをクリックして、ルールの条件を設定します。ルール条件タイプ （465 ページ）を参照してください。

ステップ 5 [ネットワーク分析（Network Analysis）] タブをクリックし、このルールに一致するトラフィックの前処理に使用する [ネットワーク分析ポリシー（Network Analysis Policy）] を選択します。

編集アイコン（）をクリックして、新しいウィンドウでカスタム ポリシーを編集します。システムによって提供されたポリシーは編集できません。

ステップ 6 [追加（Add）] をクリックします。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

ネットワーク分析ルールの管理

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Access Admin/Network Admin

ネットワーク分析ルールは、これらの条件に一致するトラフィックを前処理する方法を指定する設定および条件の単純なセットにすぎません。既存のアクセス コントロール ポリシーの詳細オプションでネットワーク分析ルールを作成および編集します。各ルールは1つのポリシーにのみ属します。

ステップ 1 アクセス コントロール ポリシー エディタで、[詳細（Advanced）] タブをクリックして、[侵入およびネットワーク分析ポリシー（Intrusion and Network Analysis Policies）] セクションの横にある編集アイコン（  ）をクリックします。

代わりに表示アイコン（  ）が表示される場合、設定は先祖ポリシーから継承され、設定を変更する権限がありません。設定がロック解除されている場合は、[Inherit from base policy] をオフにして、編集を有効にします。

ステップ 2 [ネットワーク分析ルール（Network Analysis Rules）] の横にある、所持しているカスタム ルールの数を示したステートメントをクリックします。

ステップ 3 カスタム ルールを編集します。次の選択肢があります。

- ルールの条件を編集する、またはルールによって呼び出されるネットワーク分析ポリシーを変更するには、ルールの横にある編集アイコン（  ）をクリックします。
- ルールの評価順序を変更するには、ルールをクリックして正しい位置にドラッグします。複数のルールを選択するには、Shift キーおよび Ctrl キーを使用します。
- ルールを削除するには、ルールの横にある削除アイコン（  ）をクリックします。

ヒント ルールを右クリックするとコンテキスト メニューが表示され、新しいネットワーク分析ルールの切り取り、コピー、貼り付け、編集、削除、および追加を実行できます。

ステップ 4 [OK] をクリックします。

ステップ 5 [保存（Save）] をクリックしてポリシーを保存します。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

第 91 章

ネットワーク分析ポリシーの使用を開始するには

ここでは、ネットワーク分析ポリシーの使用を開始する方法について説明します。

ネットワーク分析ポリシーの基本

ネットワーク分析ポリシーは、多数のトラフィックの前処理オプションを制御し、アクセス コントロール ポリシーの詳細設定で呼び出されます。ネットワーク分析に関連する前処理は、Security Intelligence によるブラックリスト化や SSL 復号化の後、侵入またはファイル検査の開始前に実行されます。

デフォルトでは、システムは *Balanced Security and Connectivity* ネットワーク分析ポリシーを使用して、アクセス コントロール ポリシーによって処理されるすべてのトラフィックを前処理します。ただし、この前処理を実行するために別のデフォルトのネットワーク分析ポリシーを選択できます。便宜を図るため、システムによっていくつかの変更不可能なネットワーク分析ポリシーが提供されます。これらのポリシーは、Cisco Talos Intelligence Group（Talos）によってセキュリティおよび接続の一定のバランスがとれるように調整されています。カスタム前処理設定を使用して、カスタム ネットワーク分析ポリシーを作成することもできます。

ヒント システム付属の侵入ポリシーとネットワーク分析ポリシーには同じような名前が付いていますが、異なる設定が含まれています。たとえば、「Balanced Security and Connectivity」ネットワーク分析ポリシーと「Balanced Security and Connectivity」侵入ポリシーは連携して動作し、どちらも侵入ルールのアップデートで更新できます。ただし、ネットワーク分析ポリシーは主に前処理オプションを管理し、侵入ポリシーは主に侵入ルールを管理します。ネットワーク分析ポリシーと侵入ポリシーが連動してトラフィックを検査します。

複数のカスタム ネットワーク分析ポリシーを作成し、それらに異なるトラフィックの前処理を割り当てることにより、特定のセキュリティ ゾーン、ネットワーク、VLAN 用に前処理オプ

ションを調整できます。（ただし、ASA FirePOWER VLAN による前処理を制限することはできないことに注意してください）。

ネットワーク分析ポリシーの管理

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Intrusion Admin

マルチドメイン展開では、編集できる現在のドメインで作成されたポリシーが表示されます。また、編集できない先祖ドメインで作成されたポリシーも表示されます。下位のドメインで作成されたポリシーを表示および編集するには、そのドメインに切り替えます。

ステップ 1 **[Policies]** > **[Access Control]**、次に **[Network Analysis Policy]** または **[Policies]** > **[Access Control]** > **[Intrusion]**、次に **[Network Analysis Policy]** を選択します。

（注） カスタムユーザロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

ステップ 2 ネットワーク分析ポリシーを管理します。

- [比較（Compare）]：[ポリシーの比較（Compare Policies）] をクリックします（ポリシーの比較 （457 ページ） を参照）。
- 作成：新しいネットワーク分析ポリシーを作成する場合は、[ポリシーの作成（Create Policy）] をクリックして、カスタム ネットワーク分析ポリシーの作成（2297ページ）で説明する手順を実行します。
- 削除：ネットワーク分析ポリシーを削除する場合は、削除アイコン（）をクリックして、ポリシーの削除を確認します。アクセス コントロール ポリシーが参照しているネットワーク分析ポリシーは削除できません。

  コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。
- 展開：[展開（Deploy）] をクリックします（設定変更の展開 （447 ページ） を参照）。
- 編集:既存のネットワーク分析ポリシーを編集する場合は、編集アイコン（）をクリックして、ネットワーク分析ポリシーの設定とキャッシュされた変更（2299 ページ）で説明する手順を実行します。

  代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

- [レポート（Report）]：レポート アイコン（  ）をクリックします（現在のポリシー レポートの生成（459 ページ） を参照）。

カスタム ネットワーク分析ポリシーの作成

新しいネットワーク分析ポリシーを作成するときは、一意の名前を付け、基本ポリシーを指定し、インライン モードを選択する必要があります。

基本ポリシーはネットワーク分析ポリシーのデフォルト設定を定義します。新しいポリシーの設定の変更は、基本ポリシーの設定を変更するのではなく、オーバーライドします。システム付属のポリシーまたはカスタム ポリシーを基本ポリシーとして使用できます。

ネットワーク分析ポリシーのインライン モードでは、プリプロセッサでトラフィックを変更（正規化）したりドロップしたりして、攻撃者が検出を回避する可能性を最小限にすることができます。パッシブな展開では、インライン モードに関係なく、システムはトラフィック フローに影響を与えることができないことに注意してください。

関連トピック

基本レイヤ （2047 ページ）
インライン導入でのプリプロセッサによるトラフィックの変更 （2302 ページ）
カスタム ネットワーク分析ポリシーの作成 （2297 ページ）
ネットワーク分析ポリシーの編集 （2299 ページ）

カスタム ネットワーク分析ポリシーの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Intrusion Admin

マルチドメイン展開では、編集できる現在のドメインで作成されたポリシーが表示されます。また、編集できない先祖ドメインで作成されたポリシーも表示されます。下位のドメインで作成されたポリシーを表示および編集するには、そのドメインに切り替えます。

ステップ 1 **[Policies]** > **[Access Control]**、次に **[Network Analysis Policy]**または**[Policies]** > **[Access Control]** > **[Intrusion]**、次に **[Network Analysis Policy]**を選択します。

（注） カスタムユーザロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

ステップ 2 [ポリシーの作成（Create Policy）] をクリックします。別のポリシー内に未保存の変更が存在する場合は、[ネットワーク分析ポリシー（Network Analysis Policy）] ページに戻るかどうか尋ねられたときに [キャンセル（Cancel）] をクリックします。

ステップ 3 [名前（Name）] に一意の名前を入力します。

マルチドメイン展開では、ポリシー名をドメイン階層内で一意にする必要があります。システムは、現在のドメインでは表示できないポリシーの名前との競合を特定することができます。

ステップ 4 必要に応じて、[説明（Description）] を入力します。

ステップ 5 [基本ポリシー（Base Policy）] で最初の基本ポリシーを選択します。システム提供のポリシーまたはカスタム ポリシーを基本ポリシーとして使用できます。

ステップ 6 プリプロセッサがインライン導入でのトラフィックに影響するようにする場合は、[インライン モード（Inline Mode）] を有効化します。

ステップ 7 ポリシーを作成します。

- 新しいポリシーを作成して、[Network Analysis Polic] ページに戻るには、[Create Policy] をクリックします。新しいポリシーには基本ポリシーと同じ設定項目が含まれています。
- ポリシーを作成し、高度なネットワーク分析ポリシー エディタでそれを開いて編集するには、[ポリシーの作成と編集（Create and Edit Policy）] をクリックします。

関連トピック

Web インターフェイス用のユーザ ロールのカスタマイズ （81 ページ）

ネットワーク分析ポリシーの管理

[ネットワーク分析ポリシー（Network Analysis Policy）] ページ（**[Policies]** > **[Access Control]**、次に **[Network Analysis Policy]**、または**[Policies]** > **[Access Control]** > **[Intrusion]**、次に **[Network Analysis Policy]**）で、現在のカスタム ネットワーク分析ポリシーを次の情報とともに確認できます。

- ポリシーが最後に変更された日時（ローカル時間）とそれを変更したユーザ
- プリプロセッサがトラフィックに影響を与えることを許可する [Inline Mode] 設定が有効になっているかどうか
- どのアクセス コントロール ポリシーとデバイスが、ネットワーク分析ポリシーを使用してトラフィックを前処理しているか
- ポリシーに保存されていない変更があるかどうか、およびポリシーを現在編集している人（いれば）に関する情報

ユーザが作成するカスタム ポリシーに加えて、システムには、初期インライン ポリシーと初期パッシブ ポリシーの 2 つのカスタム ポリシーが用意されています。これら 2 つのネットワーク分析ポリシーは、基本ポリシーとして「Balanced Security and Connectivity」ネットワーク分析ポリシーを使用します。両者の唯一の相違点はインライン モードの設定です。インライン ポリシーではプリプロセッサによるトラフィックの影響が有効化され、パッシブ ポリシーでは無効化されています。これらのシステム付属のカスタム ポリシーは編集して使用できます。

ただし、Firepowerシステムのユーザアカウントの権限が侵入ポリシーまたは修正侵入ポリシーに限定されている場合は、ネットワーク分析ポリシーに加えて、侵入ポリシーを作成して編集できます。

関連トピック

カスタム ネットワーク分析ポリシーの作成 （2297 ページ）
ネットワーク分析ポリシーの編集 （2299 ページ）

ネットワーク分析ポリシーの設定とキャッシュされた変更

新しいネットワーク分析ポリシーを作成すると、そのポリシーには基本ポリシーと同じ設定が付与されます。

ネットワーク分析ポリシーの調整時、特にプリプロセッサを無効化するときは、プリプロセッサおよび侵入ルールによっては、トラフィックを特定の方法で最初にデコードまたは前処理する必要があることに留意してください。必要なプリプロセッサを無効にすると、システムは自動的に現在の設定でプリプロセッサを使用します。ただし、ネットワーク分析ポリシーのWebインターフェイスではプリプロセッサは無効のままになります。

（注） 前処理と侵入インスペクションは非常に密接に関連しているため、単一パケットを検査するネットワーク分析ポリシーと侵入ポリシーは、相互補完する**必要があります**。前処理の調整、特に複数のカスタム ネットワーク分析ポリシーを使用して調整することは、**高度な**タスクです。

システムは、ユーザごとに1つのネットワーク分析ポリシーをキャッシュします。ネットワーク分析ポリシーの編集中に、任意のメニューまたは別のページへの他のパスを選択した場合、変更内容はそのページを離れてもシステム キャッシュにとどまります。

関連トピック

ポリシーが侵入についてトラフィックを検査する仕組み （2026 ページ）
カスタム ポリシーの制限 （2037 ページ）

ネットワーク分析ポリシーの編集

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Intrusion Admin

マルチドメイン展開では、編集できる現在のドメインで作成されたポリシーが表示されます。また、編集できない先祖ドメインで作成されたポリシーも表示されます。下位のドメインで作成されたポリシーを表示および編集するには、そのドメインに切り替えます。

ステップ 1 **[Policies]** > **[Access Control]**、次に **[Network Analysis Policy]**または**[Policies]** > **[Access Control]** > **[Intrusion]**、次に **[Network Analysis Policy]**を選択します。

（注） カスタムユーザロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

ステップ 2 設定するネットワーク分析ポリシーの横にある編集アイコン（  ）をクリックします。

代わりに表示アイコン（  ）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 ネットワーク分析ポリシーを編集します。

- 基本ポリシーの変更：基本ポリシーを変更するには、[ポリシー情報（Policy Information）] ページの [基本ポリシー（Base Policy）] ドロップダウン リストから、ポリシーを選択します。
- ポリシー階層の管理：ポリシー階層を管理するには、ナビゲーション パネルで [ポリシー層（Policy Layers）] をクリックします。
- プリプロセッサの変更：プリプロセッサの設定有効または無効にするか、あるいは編集するには、ナビゲーション パネルで [設定（Settings）] をクリックします。
- トラフィックの変更：プリプロセッサがトラフィックを変更またはドロップできるようにするには、[ポリシー情報（Policy Information）] ページで [インライン モード（Inline Mode）] チェックボックスをオンにします。
- 設定の表示：基本ポリシーの設定を表示するには、[ポリシー情報（Policy Information）] ページで [基本ポリシーの管理（Manage Base Policy）] をクリックします。

ステップ 4 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報（Policy Information）] を選択して、[変更を確定（Commit Changes）] をクリックします。変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後の変更は破棄されます。

次のタスク

- プリプロセッサでイベントを生成し、インライン展開では、違反パケットをドロップします。 を行うには、プリプロセッサのルールを有効にします。詳細については、「侵入ルール状態の設定 （2093 ページ）」を参照してください。
- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

関連トピック

基本レイヤ （2047 ページ）
ベースポリシーの変更 （2049 ページ）
ネットワーク分析ポリシーでのプリプロセッサの設定 （2301 ページ）
インライン導入でのプリプロセッサによるトラフィックの変更 （2302 ページ）
レイヤの管理 （2053 ページ）
競合と変更：ネットワーク分析および侵入ポリシー （2041 ページ）

ネットワーク分析ポリシーでのプリプロセッサの設定

プリプロセッサは、トラフィックを正規化し、プロトコルの異常を識別することで、トラフィックの詳細な検査に備えます。プリプロセッサは、ユーザが設定したプリプロセッサ オプションをパケットがトリガーしたときに、プリプロセッサ イベントを生成できます。デフォルトで有効になるプリプロセッサや、それぞれのデフォルト設定は、ネットワーク分析ポリシーの基本ポリシーに応じて決まります。

（注） 多くの場合、プリプロセッサの設定には特定の専門知識が必要で、通常は、ほとんどあるいはまったく変更を必要としません。前処理の調整、特に複数のカスタム ネットワーク分析ポリシーを使用して調整することは、**高度な**タスクです。前処理と侵入インスペクションは非常に密接に関連しているため、単一パケットを検査するネットワーク分析ポリシーと侵入ポリシーは、相互補完する**必要があります**。

プリプロセッサの設定を変更するには、その設定とネットワークへの潜在的影響を理解する必要があります。

トランスポート/ネットワーク プリプロセッサの詳細設定は、アクセス コントロール ポリシーを展開するすべてのネットワーク、ゾーン、VLANにグローバルに適用されることに注意してください。これらの詳細設定は、ネットワーク分析ポリシーではなくアクセス コントロール ポリシーで設定します。

また、侵入ポリシーではASCIIテキストのクレジット カード番号や社会保障番号などの機密データを検出する機密データ プリプロセッサを設定することにも注意してください。

関連トピック

DCE/RPC プリプロセッサ （2306 ページ）
DNP3 プリプロセッサ （2388 ページ）
DNS プリプロセッサ （2319 ページ）
FTP/Telnet デコーダ （2323 ページ）
GTP プリプロセッサ （2359 ページ）
HTTP Inspect プリプロセッサ （2333 ページ）
IMAP プリプロセッサ （2361 ページ）
インライン正規化プリプロセッサ （2403 ページ）
IP 最適化プリプロセッサ （2411 ページ）
Modbus プリプロセッサ （2385 ページ）
パケット デコーダ （2417 ページ）
POP プリプロセッサ （2364 ページ）
機密データ検出の基本 （2113 ページ）
SIP プリプロセッサ （2354 ページ）
SMTP プリプロセッサ （2368 ページ）
SSH プリプロセッサ （2374 ページ）
SSL プリプロセッサ （2379 ページ）

Sun RPC プリプロセッサ （2351 ページ）
TCP ストリームの前処理 （2422 ページ）
UDP ストリームの前処理 （2435 ページ）
カスタム ポリシーの制限 （2037 ページ）

インライン導入でのプリプロセッサによるトラフィックの変更

インライン導入（つまり、ルーテッド インターフェイス、スイッチド インターフェイス、トランスペアレント インターフェイス、あるいはインライン インターフェイスのペアを使用して関連する設定をデバイスに展開する導入）では、一部のプリプロセッサがトラフィックを変更およびブロックできます。次に例を示します。

- インライン正規化プリプロセッサは、パケットを正規化し、他のプリプロセッサおよび侵入ルールエンジンで分析されるようにパケットを準備します。ユーザは、プリプロセッサの [これらの TCP オプションを許可（Allow These TCP Options）] と [回復不能な TCP ヘッダーの異常をブロック（Block Unresolvable TCP Header Anomalies）] オプションを使用して、特定のパケットをブロックすることもできます。
- システムは無効なチェックサムを持つパケットをドロップできます。
- システムはレート ベースの攻撃防御設定に一致するパケットをドロップできます。

ネットワーク分析ポリシーに設定したプリプロセッサがトラフィックに影響を与えるようにするには、プリプロセッサを有効にして正しく設定するとともに、管理対象デバイスをインラインで正しく展開する必要があります。最後に、ネットワーク分析ポリシーの [インライン モード（Inline Mode）] 設定を有効にする必要があります。

ネットワーク分析ポリシーの注記におけるプリプロセッサの設定

ネットワーク分析ポリシーのナビゲーション パネルで [設定（Settings）] を選択すると、ポリシーによりタイプ別のプリプロセッサがリストされます。[Settings] ページでは、ネットワーク分析ポリシーのプリプロセッサを有効化/無効化することに加えて、プリプロセッサの設定ページにアクセスできます。

設定を行うには、プリプロセッサを有効にする必要があります。プリプロセッサを有効にすると、ナビゲーション パネルの [Settings] リンクの下にプリプロセッサの設定ページへのサブリンクが表示され、[Settings] ページのプリプロセッサの横に設定ページへの [Edit] リンクが表示されます。

ヒント プリプロセッサの設定を基本ポリシーの設定に戻すには、プリプロセッサの設定ページで [Revert to Defaults] をクリックします。プロンプトが表示されたら、復元することを確認します。

プリプロセッサを無効にすると、サブリンクと [Edit] リンクは表示されなくなりますが、設定は保持されます。特定の分析を実行するには、多くのプリプロセッサおよび侵入ルールで、トラフィックをある方法で最初に復号化または前処理する必要があることに注意してください。必要なプリプロセッサを無効にすると、システムは自動的に現在の設定でプリプロセッサを使

用します。ただし、ネットワーク分析ポリシーの Web インターフェイスではプリプロセッサは無効のままになります。

実際にトラフィックを変更せずに、設定がインライン展開でどのように機能するかを評価する場合は、インライン モードを無効にできます。タップ モードでのパッシブ展開またはインライン展開では、インライン モード設定に関係なくシステムがトラフィックに影響を及ぼすことはありません。

（注） インライン モードを無効にすることで、侵入イベントのパフォーマンス統計グラフに影響を及ぼす可能性があります。インライン展開でインライン モードが有効の場合、侵入イベント パフォーマンス ページ（**[Overview]** > **[Summary]** > **[Intrusion Event Performance]**）には、正規化し、ブロックされたパケットを示すグラフが表示されます。インライン モードが無効の場合、またはパッシブ展開である場合、多くのグラフによりシステムが正規化するか、またはドロップするトラフィックに関するデータが表示されます。

（注） インライン展開では、インライン モードを有効にし、[TCP ペイロードの正規化（Normalize TCP Payload）] オプションを有効にして、インライン正規化プリプロセッサを設定することをお勧めします。パッシブ展開では、アダプティブ プロファイルの更新を使用することをお勧めします。

関連トピック

トランスポート/ネットワーク プリプロセッサの詳細設定 （2398 ページ）
チェックサム検証 （2401 ページ）
インライン正規化プリプロセッサ （2403 ページ）
侵入イベントのパフォーマンス統計情報グラフの種類 （3107 ページ）

第 92 章

アプリケーション層プリプロセッサ

次のトピックでは、アプリケーション層プリプロセッサおよびその設定方法について説明します。

アプリケーション層のプリプロセッサの概要

アプリケーション層プロトコルにより、同一データをさまざまな方法で表すことができます。Firepowerシステムは、特定タイプのパケットデータを侵入ルールエンジンが分析可能なフォーマットに正規化する、アプリケーション層プロトコルデコーダを提供しています。アプリケーション層プロトコル エンコードを正規化することにより、ルール エンジンでさまざまなデータ形式のパケットに同じコンテンツ関連ルールを効果的に適用し、有意な結果を得ることができます。

侵入ルールまたはルールの引数がプリプロセッサの無効化を必要とする場合、ネットワーク分析ポリシーの Web インターフェイスではプリプロセッサが無効化されたままになりますが、システムは自動的に現在の設定でプリプロセッサを使用します。

ほとんどの場合、侵入ルールで関連するプリプロセッサルールが有効になっていないと、プリプロセッサはイベントを生成しません。

DCE/RPC プリプロセッサ

DCE/RPC プロトコルにより、別々のネットワーク ホスト上のプロセスが、同一ホストに配置されている場合と同様に通信できます。通常、このようなプロセス間通信はホスト間で TCP および UDP 経由で転送されます。TCP 転送では、DCE/RPC が Windows Server Message Block（SMB）プロトコルまたは Samba にさらにカプセル化されることがあります。Samba は、Windows および UNIX 系または Linux 系のオペレーティング システムで構成される混合環境でのプロセス間通信に使用されるオープンソース SMB 実装です。また、ネットワーク上の Windows IIS Web サーバが、IIS RPC over HTTP を使用することがあります。IIS RPC over HTTP は、プロキシ TCP により伝送される DCE/RPC トラフィックに対し、ファイアウォールを介した分散通信を提供します。

DCE/RPC プリプロセッサ オプションとその機能の説明には、Microsoft による DCE/RPC の実装である MSRPC が含まれることに注意してください。SMB のオプションと機能についての説明は、SMB と Samba の両方に当てはまります。

ほとんどの DCE/RPC エクスプロイトは、DCE/RPC サーバ（ネットワーク上の Windows または Samba が稼働している任意のホスト）を対象とした DCE/RPC クライアント要求で発生します。またエクスプロイトはサーバ応答でも発生することがあります。DCE/RPC プリプロセッサは、TCP、UDP、および SMB トランスポートでカプセル化された DCE/RPC 要求と応答を検出します。これには、RPC over HTTP バージョン 1 を使用して TCP により伝送される DCE/RPC を含みます。プリプロセッサは DCE/RPC データ ストリームを分析し、DCE/RPC トラフィックにおける異常な動作と回避技術を検出します。また、SMB データ ストリームを分析し、異常な SMB 動作と回避技術を検出します。

IP 最適化プリプロセッサによる IP 最適化および TCP ストリーム プリプロセッサによる TCP ストリームの再構成に加えて、DCE/RPC プリプロセッサは、SMB のセグメント化解除と DCE/RPC の最適化も行います。

最後に、DCE/RPC プリプロセッサはルール エンジンで処理できるように DCE/RPC トラフィックを正規化します。

コネクションレス型およびコネクション型 DCE/RPC トラフィック

DCE/RPC メッセージは、2 種類の DCE/RPC Protocol Data Unit（PDU）の 1 つに準拠します。

コネクション型 DCE/RPC PDU プロトコル

DCE/RPC プリプロセッサは、TCP、SMB、および RPC over HTTP トランスポートでコネクション型 DCE/RPC を検出します。

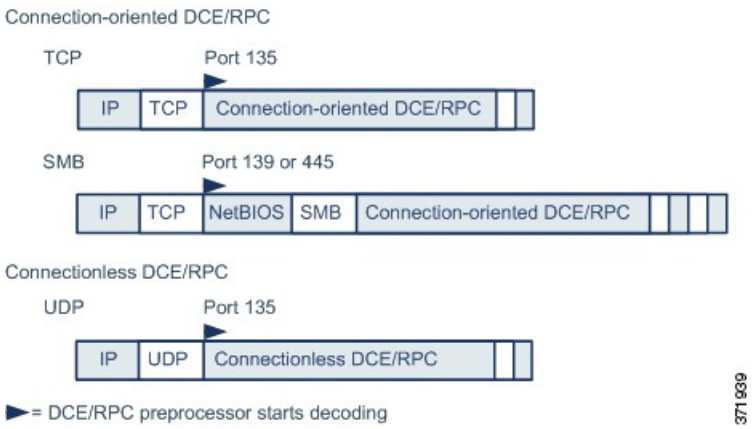
コネクションレス型 DCE/RPC PDU プロトコル

DCE/RPC プリプロセッサは、UDP トランスポートでコネクションレス型 DCE/RPC を検出します。

この 2 つの DCE/RPC PDU プロトコルには、それぞれ固有の見出しとデータ特性があります。たとえば、コネクション型 DCE/RPC 見出しの長さは通常は 24 バイトであり、コネクションレ

ス型DCE/RPCの見出しの長さは80バイト（固定）です。また、フラグメント化コネクションレス型 DCE/RPC のフラグメントの正しい順序は、コネクションレス型トランスポートでは処理できないため、代わりにコネクションレス型 DCE/RPC 見出し値により維持される必要があります。これとは対照的に、コネクション型 DCE/RPC の正しいフラグメント順序はトランスポート プロトコルによって維持されます。DCE/RPC プリプロセッサは、これらや他のプロトコル固有の特性を使用して、両方のプロトコルで異常やその他の回避技術をモニタし、トラフィックをデコードおよび最適化してからルール エンジンに渡します。

次の図は、DCE/RPCプリプロセッサが各種トランスポートのDCE/RPCトラフィックの処理を開始するポイントを示します。



この図の次の点に注意してください。

- ウェルノウンTCPまたはUDPポート135は、TCPおよびUDPトランスポートのDCE/RPCトラフィックを特定します。
- この図には RPC over HTTP は含まれていません。

  RPC over HTTP の場合、コネクション型 DCE/RPC は、図に示すように、HTTP を介した初期設定シーケンスの後、TCP 経由で直接伝送されます。
- DCE/RPC プリプロセッサは通常、NetBIOS セッション サービス用のウェルノウン TCP ポート 139 か、同様に実装されたウェルノウン Windows ポート 445 で SMB トラフィックを受信します。

  SMB には DCE/RPC 伝送以外にも多数の機能があるため、プリプロセッサは SMB トラフィックが DCE/RPC トラフィックを伝送しているかどうかをまず検査します。伝送していない場合は処理を停止し、伝送している場合は処理を続行します。
- IP によりすべての DCE/RPC トランスポートがカプセル化されます。
- TCP は、すべてのコネクション型 DCE/RPC を伝送します。
- UDP はコネクションレス型 DCE/RPC を伝送します。

DCE/RPC ターゲット ベース ポリシー

Windows および Samba の DCE/RPC の実装は大きく異なります。たとえば、Windows のすべてのバージョンは、DCE/RPC トラフィックの最適化時に最初のフラグメントの DCE/RPC コンテキスト ID を使用しますが、Samba のすべてのバージョンは、最後のフラグメントのコンテキスト ID を使用します。また、特定の関数呼び出しを識別するために、Windows Vista では最初のフラグメントの opnum（操作番号）見出しフィールドを使用しますが、Samba とその他のすべてのバージョンの Windows では最後のフラグメントの opnum フィールドを使用します。

Windows と Samba の SMB の実装にも、大きな違いがあります。たとえば、Windows は名前付きパイプの操作時に SMB OPEN および READ コマンドを認識しますが、Samba はこれらのコマンドを認識しません。

DCE/RPC プリプロセッサを有効にすると、デフォルトのターゲットベース ポリシーが自動的に有効になります。必要に応じて、異なる Windows や Samba バージョンを実行する他のホストを対象としたターゲット ベース ポリシーを追加できます。デフォルトのターゲットベース ポリシーは、別のターゲットベース ポリシーに含まれていないホストに適用されます。

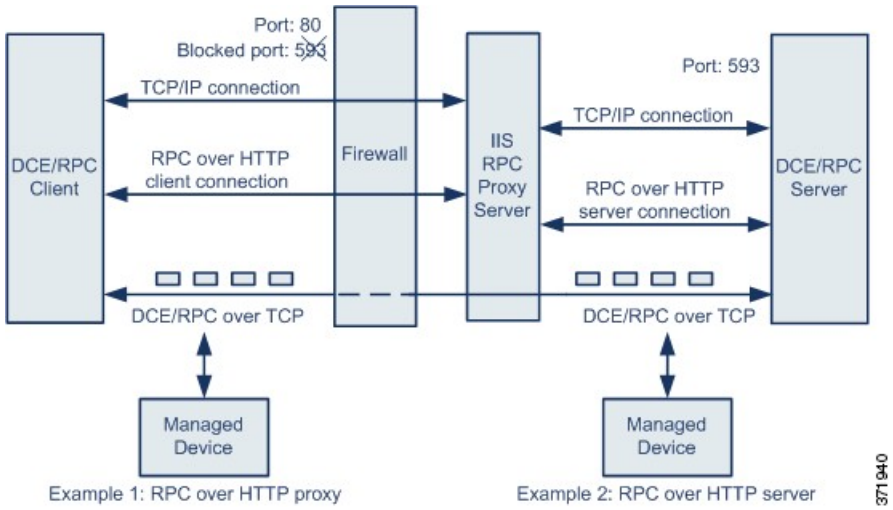
各ターゲットベースのポリシーでは次の設定が可能です。

- 1 つ以上のトランスポートを有効にし、それぞれについて検出ポートを指定します。
- 自動検出ポートを有効にして指定します。
- 指定した 1 つ以上の共有 SMB リソースへの接続が試行された場合にそのことを検出するように、プリプロセッサを設定します。
- SMB トラフィックでファイルを検出し、検出されたファイルで指定されたバイト数を検査するように、プリプロセッサを設定します。
- SMB プロトコルの知識を持つユーザだけが変更すべき拡張オプションを変更できます。このオプションでは、連結された SMB AndX コマンドの数が指定された最大数を超えた場合にそのことを検出するようにプリプロセッサを設定します。

DCE/RPC プリプロセッサで SMB トラフィック ファイル検出を有効にするほかに、オプションでこれらのファイルをキャプチャしてブロックするか、またはダイナミック分析のために Cisco AMP クラウドに送信するように、ファイル ポリシーを設定できます。そのポリシー内で、[アクション（Action）] として [ファイル検出（Detect Files）] または [ファイル ブロック（Block Files）] を選択し、[アプリケーション プロトコル（Application Protocol）] として [任意（Any）] または [NetBIOS-ssn (SMB)] を選択して、ファイル ルールを作成する必要があります。

RPC over HTTP トランスポート

Microsoft RPC over HTTP では、次の図に示すように、DCE/RPC トラフィックをトンネリングして、ファイアウォールを通過させることができます。DCE/RPC プリプロセッサは Microsoft RPC over HTTP バージョン 1 を検出します。



Microsoft IIS プロキシ サーバと DCE/RPC サーバは、同じホストまたは別々のホストにインストールできます。いずれの場合でも、個別のプロキシ オプションとサーバ オプションがあります。この図の次の点に注意してください。

- DCE/RPC サーバはポート 593 で DCE/RPC クライアント トラフィックをモニタしますが、ファイアウォールはこのポート 593 をブロックします。

  通常、ファイアウォールではデフォルトでポート 593 がブロックされます。

- RPC over HTTP は、ファイアウォールによって許可される可能性が高いウェルノウン HTTP ポート 80 を使用して、HTTP 経由で DCE/RPC を伝送します。

- 例 1 のように、DCE/RPC クライアントと Microsoft IIS RPC プロキシ サーバの間のトラフィックをモニタする場合は、[RPC over HTTP プロキシ（RPC over HTTP proxy）] オプションを選択します。

- 例 2 のように、Microsoft IIS RPC プロキシ サーバと DCE/RPC サーバが異なるホスト上にあり、デバイスが 2 つのサーバ間のトラフィックをモニタしている場合は、[RPC over HTTP サーバ（RPC over HTTP server）] オプションを選択します。

- RPC over HTTP により DCE/RPC クライアントとサーバ間でのプロキシ セットアップが完了した後、トラフィックは TCP を経由したコネクション型 DCE/RPC だけで構成されます。

DCE/RPC グローバル オプション

グローバル DCE/RPC プリプロセッサ オプションは、プリプロセッサの機能を制御します。[到達したメモリ容量（Memory Cap Reached）] および [SMB セッションの自動検出ポリシー（Auto-Detect Policy on SMB Session）] オプション以外のオプションを変更すると、パフォーマンスまたは検出機能に悪影響を及ぼす可能性があります。プリプロセッサについて、またプリプロセッサと有効にされている DCE/RPC ルールとの間の相互作用について十分に理解していない場合は、これらのオプションを変更しないでください。

以下の説明でプリプロセッサ ルールが言及されていない場合、オプションにはプリプロセッサ ルールが関連付けられていません。

最大フラグメント サイズ（Maximum Fragment Size）

[最適化の有効化（Enable Defragmentation）] が選択されている場合、DCE/RPC フラグメントの許容最大長を指定します。これよりも大きなフラグメントの場合、プリプロセッサは処理のためにフラグメントの一部を切り捨て、指定のサイズにしてから最適化を行いますが、実際のパケットは変更されません。空白フィールドの場合、このオプションは無効になります。

[最大フラグメント サイズ（Maximum Fragment Size）] オプションは、ルールが検出する必要がある深さと同じかそれ以上にしてください。

リアセンブリしきい値（Reassembly Threshold）

[最適化の有効化（Enable Defragmentation）] が選択されている場合、0 を指定するとこのオプションは無効になります。あるいは、フラグメント化された DCE/RPC の最小バイト数を、該当する場合は、再構成されたパケットをルールエンジンに送信する前にキューに入れるセグメント化 SMB のバイト数を指定します。低い値を指定すると、早期検出の可能性が高くなりますが、パフォーマンスに悪影響を及ぼす可能性があります。このオプションを有効にする場合は、パフォーマンスの影響をテストしておく必要があります。

[リアセンブリしきい値（Reassembly Threshold）] オプションは、ルールが検出する必要がある深さと同じかそれ以上にしてください。

最適化の有効化（Enable Defragmentation）

フラグメント化された DCE/RPC トラフィックを最適化するかどうかを指定します。無効にすると、プリプロセッサは引き続き異常を検出して DCE/RPC データをルール エンジンに送信しますが、フラグメント化された DCE/RPC データでのエクスプロイトを見落とすリスクがあります。

このオプションには、DCE/RPC トラフィックを最適化しないという柔軟性がありますが、ほとんどの DCE/RPC エクスプロイトでは、フラグメント化を利用してエクスプロイトを隠ぺいする試みが行われます。このオプションを無効にすると、ほとんどの既知のエクスプロイトがバイパスされ、検出漏れが大量に発生します。

Memory Cap Reached

プリプロセッサに割り当てられた最大メモリ制限に達したか、またはこの制限を超過したことを検出します。最大メモリ制限に達したか、またはこの制限を超過した場合、プリプロセッサはメモリ キャップイベントを引き起こしたセッションに関連付けられているすべての保留データを解放し、セッションのそれ以降の部分を無視します。

ルール 133:1 を有効にすることができます。イベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定（2093 ページ） を参照してください。

SMB セッションの自動検出ポリシー（Auto-Detect Policy on SMB Session）

SMB `Session Setup AndX` 要求および応答に指定されている Windows または Samba のバージョンを検出します。検出されたバージョンが、[ポリシー（Policy）] 設定オプションで設定されている Windows または Samba のバージョンと異なる場合、そのセッションに限り、検出されたバージョンが設定バージョンをオーバーライドします。

たとえば、[ポリシー（Policy）] に Windows XP を設定した場合に、プリプロセッサが Windows Vista を検出すると、プリプロセッサはそのセッションでは Windows Vista ポリシーを使用します。その他の設定は引き続き有効です。

DCE/RPC トランスポートが SMB ではない場合は（トランスポートが TCP または UDP の場合）、バージョンを検出できず、ポリシーを自動的に設定できません。

このオプションを有効にするには、ドロップダウン リストで次のいずれかを選択します。

- サーバ/クライアント トラフィックでポリシー タイプを検査するには、[クライアント（Client）] を選択します。
- クライアント/サーバ トラフィックでポリシータイプを検査するには、[サーバ（Server）] を選択します。
- サーバ/クライアント トラフィックとクライアント/サーバ トラフィックの両方でポリシータイプを検査するには、[両方（Both）] を選択します。

レガシー SMB 検査モード（Legacy SMB Inspection Mode）

検査する SMB バージョンを指定します。[レガシー SMB 検査モード（Legacy SMB Inspection Mode）] が有効になっている場合、DCE/RPC プリプロセッサは、SMB バージョン 1 のトラフィックのみを検査します。このオプションを無効にすると、DCE/RPC プリプロセッサは、SMB バージョン 1、2、および 3 を使用するトラフィックを調査します。

関連トピック

基本コンテンツおよび protected_content キーワードの引数 （2166 ページ）
概要：byte_jump および byte_test キーワード

DCE/RPC ターゲットベース ポリシー オプション

各ターゲットベース ポリシーでは、TCP、UDP、SMB、および RPC over HTTP トランスポートのうち 1 つ以上を有効にできます。トランスポートを有効にする場合は、1 つ以上の検出ポート（DCE/RPC トラフィックを伝送することがわかっているポート）を指定する必要があります。

シスコでは、デフォルトの検出ポート（ウェルノウンポートまたは各プロトコルで一般に使用されているポート）を使用することを推奨しています。検出ポートを追加するのは、デフォルト以外のポートで DCE/RPC トラフィックを検出した場合だけです。

Windows のターゲットベース ポリシーでは、ネットワークのトラフィックに一致するように、1 つ以上の任意のトランスポートのポートを任意の組み合わせで指定できます。しかし、Samba のターゲットベース ポリシーでは SMB トランスポートのポートだけを指定できます。

（注） 少なくとも 1 つのトランスポートが有効になっている DCE/RPC ターゲットベース ポリシーを追加した場合を除き、デフォルトのターゲットベースポリシーでは少なくとも 1 つの DCE/RPC トランスポートを有効にする必要があります。たとえば、すべての DCE/RPC 実装に対してホストを指定し、未指定のホストにはデフォルトのターゲットベースポリシーを展開したくない場合があります。そのような場合は、デフォルトのターゲットベースポリシーのトランスポートを有効化しないようにします。

（オプション）自動検出ポートを有効にして指定できます。プリプロセッサは、自動検出ポートとして指定されたポートを最初にテストして、そのポートが DCE/RPC トラフィックを伝送しているかどうかを判別し、DCE/RPC トラフィックを検出した場合にのみ処理を続行します。

自動検出ポートを有効にする場合は、エフェメラルポート範囲全体に対応するよう、自動検出ポートが 1024 から 65535 の範囲に設定されていることを確認してください。

自動検出は、トランスポート検出ポートによって識別されていないポートでのみ発生する点にも注意してください。

[RPC over HTTP プロキシ自動検出ポート（RPC over HTTP Proxy Auto-Detect Ports）] オプションまたは [SMB 自動検出ポート（SMB Auto-Detect Ports）] オプションで自動検出ポートを有効にしたり指定したりすることはほとんどありません。これは、指定されているデフォルト検出ポートを除き、どちらの場合もトラフィックが発生することはほとんどなく、その見込みも少ないためです。

各ターゲットベース ポリシーでは、次に示すさまざまなオプションを指定できます。以下の説明でプリプロセッサ ルールが言及されていない場合、オプションにはプリプロセッサ ルールが関連付けられていません。

ネットワーク

DCE/RPC ターゲットベース サーバ ポリシーを展開するホストの IP アドレス。また、ターゲットベース ポリシーを追加する場合は、[ターゲットの追加（Add Target）] ポップアップ ウィンドウの [サーバ アドレス（Server Address）] フィールドに指定した名前。

単一の IP アドレスまたはアドレス ブロック、あるいはこれらのいずれかまたは両方をカンマで区切ったリストを指定できます。デフォルト ポリシーを含め、合計で最大 255 個のプロファイルを設定できます。

（注） システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。 上書き対応オブジェクトを使用すると、子孫ドメインの管理者は、グローバル コンフィギュレーションを自分のローカル環境に調整できます。

デフォルト ポリシーの `default` 設定では、別のターゲットベース ポリシーでカバーされていないモニタ対象ネットワーク セグメントのすべての IP アドレスが指定されることに注意してください。したがって、デフォルト ポリシーの IP アドレスまたは CIDR ブロック/プレフィク

ス長は指定できず、また指定する必要もありません。また、別のポリシーでこの設定を空白にしたり、すべて を表すアドレス表記（0.0.0.0/0 または ::/0）を使用したりすることはできません。

Policy

モニタ対象ネットワーク セグメントのターゲット ホストが使用する Windows または Samba DCE/RPC の実装。

[SMB セッションの自動検出ポリシー（Auto-Detect Policy on SMB Session）] グローバル オプションを有効にすると、SMB が DCE/RPC トランスポートの場合に、このオプションの設定をセッションごとに自動的にオーバーライドできます。

SMB の無効な共有（SMB Invalid Shares）

指定した共有リソースへの接続が試行されると、プリプロセッサが検出する 1 つ以上の SMB 共有リソースを識別します。複数の共有をカンマで区切って指定できます。また必要に応じて、共有を引用符で囲むこともできます。これは、以前のソフトウェア バージョンでは必須でしたが、現在は必須ではありません。次に例を示します。

```
"C$", D$, "admin", private
```

[SMB ポート（SMB Ports）] が有効に設定されている場合、プリプロセッサは SMB トラフィックで無効な共有を検出します。

ほとんどの場合、Windows により名前が指定されたドライブを無効な共有として指定するには、このドライブにドル記号を付加する必要があることに注意してください。たとえば、ドライブ C は C$ または "C$" として指定します。

SMB の無効な共有を検出するには、[SMB ポート（SMB Ports）] か、[SMB 自動検出ポート（SMB Auto-Detect Ports）] を有効にする必要があることにも注意してください。

ルール 133:26 を有効にすることができます イベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定（2093ページ） を参照してください。

SMB 最大 AndX チェーン（SMB Maximum AndX Chain）

連結された SMB AndX コマンドの許容最大数です。通常、多数の連結 AndX コマンドは異常な動作を表し、場合によっては回避試行を示している可能性があります。連結コマンドを許可しない場合は 1 を指定し、連結コマンドの数の検出を無効にするには 0 を指定します。

プリプロセッサは最初に連結コマンドの数をカウントし、関連する SMB プリプロセッサ ルールが有効であり、連結コマンドの数が設定されている値と等しいかそれ以上の場合にはイベントを生成することに注意してください。その後、処理が続行されます。

⚠

注意 SMB プロトコルに詳しいユーザだけが [SMB AndX の最大チェーン（SMB Maximum AndX Chains）] オプションのデフォルト設定を変更するようにしてください。

ルール 133:20 を有効にすることができます イベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定 （2093 ページ） を参照してください。

RPC プロキシ トラフィックのみ（RPC proxy traffic only）

[RPC over HTTP プロキシ ポート（RPC over HTTP Proxy Ports）] が有効である場合、検出されるクライアント側の RPC over HTTP トラフィックがプロキシ トラフィックのみであるか、または他の Web サーバ トラフィックを含んでいる可能性があるかどうかを示します。たとえば、ポート 80 はプロキシ トラフィックとその他の Web サーバ トラフィックの両方を伝送する可能性があります。

このオプションが無効になっている場合は、プロキシ トラフィックとその他の Web サーバ トラフィックの両方が想定されます。たとえばサーバが専用プロキシサーバである場合などに、このオプションを有効にします。有効にすると、プリプロセッサはトラフィックを調べて DCE/RPC を伝送しているかどうかを判別し、伝送していない場合はそのトラフィックを無視し、伝送している場合は処理を続行します。このオプションを有効にすることで機能が追加されるのは、[RPC over HTTP Proxy Ports] チェック ボックスも有効にされている場合だけであることに注意してください。

RPC over HTTP プロキシ ポート（RPC over HTTP Proxy Ports）

管理対象デバイスが DCE/RPC クライアントと Microsoft IIS RPC プロキシ サーバの間に配置されている場合に、指定の各ポートで RPC over HTTP によりトンネリングされる DCE/RPC トラフィックの検出を有効にします。

有効である場合、DCE/RPC トラフィックが確認されるポートを追加できますが、Web サーバは一般に DCE/RPC トラフィックとその他のトラフィックの両方にデフォルト ポートを使用するため、この操作が必要になることはあまりありません。有効である場合、[RPC over HTTP プロキシ自動検出ポート（RPC over HTTP Proxy Auto-Detect Ports）] は有効にしませんが、検出されるクライアント側の RPC over HTTP トラフィックがプロキシ トラフィックのみであり、その他の Web サーバ トラフィックを含んでいない場合は、[RPC プロキシ トラフィックのみ（RPC Proxy Traffic Only）] を有効にします。

（注） このオプションを選択することがあるとすれば、きわめて稀なケースです。

RPC over HTTP サーバ ポート（RPC over HTTP Server Ports）

Microsoft IIS RPC プロキシ サーバと DCE/RPC サーバが異なるホスト上に配置されており、デバイスがこの 2 つのサーバ間のトラフィックをモニタしている場合、指定の各ポートで RPC over HTTP によりトンネリングされる DCE/RPC トラフィックの検出を有効にします。

一般に、このオプションを有効にするときは、ネットワーク上のプロキシ Web サーバに注意を払わない場合でも、1025 ～ 65535 のポート範囲で [RPC over HTTP サーバ自動検出ポート（RPC over HTTP Server Auto-Detect Ports）] も有効にする必要があります。場合によっては

RPC over HTTP サーバ ポートを再設定することがあり、その際には再設定したサーバ ポートをこのオプションのポート リストに追加する必要があることに注意してください。

TCP Ports

指定の各ポートでの TCP の DCE/RPC トラフィックの検出を有効にします。

正当な DCE/RPC トラフィックとエクスプロイトは、さまざまなポートを使用する可能性があります。ポート 1024 より大きい番号のポートが一般的です。通常、このオプションを有効にする場合は、1025 から 65535 までのポート範囲で [TCP Auto-Detect Ports] も有効にする必要もあります。

UDP Ports

指定の各ポートでの UDP の DCE/RPC トラフィックの検出を有効にします。

正当な DCE/RPC トラフィックとエクスプロイトは、さまざまなポートを使用する可能性があります。ポート 1024 より大きい番号のポートが一般的です。通常、このオプションを有効にする場合は、1025 から 65535 までのポート範囲で [UDP Auto-Detect Ports] も有効にする必要があります。

SMB Ports

指定の各ポートでの SMB の DCE/RPC トラフィックの検出を有効にします。

デフォルトの検出ポートを使用した SMB トラフィックが発生することがあります。他のポートはほとんどありません。通常はデフォルト設定を使用してください。

[SMB セッションの自動検出ポリシー（Auto-Detect Policy on SMB Session）] グローバル オプションを有効にすると、SMB が DCE/RPC トランスポートの場合に、ターゲット ポリシーに対して設定されているポリシータイプをセッションごとに自動的にオーバーライドできます。

RPC over HTTP プロキシ自動検出ポート（RPC over HTTP Proxy Auto-Detect Ports）

管理対象デバイスが DCE/RPC クライアントと Microsoft IIS RPC プロキシ サーバの間に配置されている場合に、指定のポートで RPC over HTTP によりトンネリングされる DCE/RPC トラフィックの自動検出を有効にします。

有効である場合は、エフェメラル ポート範囲全体をカバーするため、一般にポート範囲として 1025 から 65535 を指定します。

RPC over HTTP サーバ自動検出ポート（RPC over HTTP Server Auto-Detect Ports）

Microsoft IIS RPC プロキシ サーバおよび DCE/RPC サーバが異なるホスト上に配置されており、デバイスがこの 2 つのサーバ間のトラフィックをモニタしている場合、指定のポートで RPC over HTTP によりトンネリングされる DCE/RPC トラフィックの自動検出を有効にします。

TCP 自動検出ポート（TCP Auto-Detect Ports）

指定のポートで TCP の DCE/RPC トラフィックの自動検出を有効にします。

UDP Auto-Detect Ports

指定の各ポートで UDP の DCE/RPC トラフィックの自動検出を有効にします。

SMB Auto-Detect Ports

SMB の DCE/RPC トラフィックの検出を有効にします。

（注） このオプションを選択することがあるとすれば、きわめて稀なケースです。

SMB ファイル インスペクション（SMB File Inspection）

ファイル検出のための SMB トラフィックのインスペクションを有効にします。次の選択肢があります。

- ファイル インスペクションを無効にするには、[Off] を選択します。
- SMB でファイルデータを検査するが、DCE/RPC トラフィックは検査しない場合は、[Only] を選択します。このオプションを選択すると、ファイルと DCE/RPC トラフィックの両方を検査する場合よりもパフォーマンスが向上する可能性があります。
- SMB でファイルと DCE/RPC トラフィックの両方を検査するには、[On] を選択します。このオプションを選択すると、パフォーマンスに影響する可能性があります。

SMB トラフィックでの次のファイルについてのインスペクションはサポートされていません。

- 1 つの TCP または SMB セッションで同時に転送されたファイル
- 複数の TCP または SMB セッションにわたって転送されたファイル
- メッセージ署名のネゴシエート時など、非連続データを使用して転送されたファイル
- 同一オフセットに異なるデータが含まれており、データがオーバーラップしている転送ファイル
- リモート クライアントがファイル サーバに保存し、そのクライアントで編集用に開かれたファイル

SMB File Inspection Depth

[SMB File Inspection] が [Only] または [On] に設定されている場合に、SMB トラフィックでファイルが検出された時に検査されるデータのバイト数です。次のいずれかを指定します。

- 正の値
- `0`：ファイル全体を検査する場合
- `-1`：ファイル インスペクションを無効にする場合

アクセス コントロール ポリシーの [詳細（Advanced）] タブの [ファイルおよびマルウェアの設定（File and Malware Settings）] セクションで定義された値以下になるように、このフィール

ドに値を入力します。[ファイルタイプを検知する前に検閲するバイト数制限（Limit the number of bytes inspected when doing file type detection）] で定義されている値よりも大きい値をこのオプションに設定すると、アクセス コントロール ポリシーの設定が、有効な最大値として使用されます。

[SMB ファイル インスペクション（SMB File Inspection）] が [オフ（Off）] に設定されている場合、このフィールドは無効になります。

関連トピック

Firepower システムの IP アドレス表記法 （20 ページ）

トラフィックに関連する DCE/RPC ルール

ほとんどの DCE/RPC プリプロセッサ ルールでは、SMB、コネクション型 DCE/RPC、またはコネクションレス型 DCE/RPC のトラフィックで検出される異常や検知回避技術に対してトリガーします。トラフィック タイプ別に有効にできるルールを次の表に示します。

表 *228*：トラフィックに関連する *DCE/RPC* ルール

トラフィック	プリプロセッサ ルール GID：SID
SMB	133:2 ～ 133:26、133:48 ～ 133:59
コネクション型 DCE/RPC	133:27 ～ 133:39
Detect Connectionless DCE/RPC	133:40 ～ 133:43

DCE/RPC プリプロセッサの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Intrusion Admin

DCE/RPC プリプロセッサを設定するには、プリプロセッサの機能を制御するグローバル オプションを変更するか、IP アドレスと稼働している Windows または Samba のバージョンによってネットワーク上の DCE/RPC サーバを識別する 1 つ以上のターゲットベース サーバ ポリシーを指定します。ターゲットベース ポリシー構成では、トランスポート プロトコルの有効化、DCE/RPC トラフィックをホストに伝送するポートの指定、およびその他のサーバ固有オプションの設定も行います。

システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。 上書き対応オブジェクトを使用すると、子孫ドメインの管理者は、グローバル コンフィギュレーションを自分のローカル環境に調整できます。

始める前に

- カスタム ターゲットベースのポリシーで指定するネットワークが一致しているか、または親のネットワーク分析ポリシーで処理されるネットワーク、ゾーン、および VLAN のサブセットであることを確認します。詳細については、ネットワーク分析プロファイルの詳細設定 （2289 ページ）を参照してください。

ステップ 1 **[Policies]** > **[Access Control]**、次に **[Network Analysis Policy]** または **[Policies]** > **[Access Control]** > **[Intrusion]**、次に **[Network Analysis Policy]** を選択します。

（注） カスタム ユーザ ロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

ステップ 2 編集するポリシーの横にある編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 左側のナビゲーション パネルで [設定（Settings）] をクリックします。

ステップ 4 [アプリケーション層プリプロセッサ（Application Layer Preprocessors）] の下の [DCE/RPC の構成（DCE/RPC Configuration）] が無効になっている場合は、[有効化（Enabled）] をクリックします。

ステップ 5 [DCE/RPC の構成（DCE/RPC Configuration）] の横にある編集アイコン（）をクリックします。

ステップ 6 [グローバル設定（Global Settings）] セクションのオプションを変更します。DCE/RPC グローバル オプション （2309 ページ）を参照してください。

ステップ 7 次の選択肢があります。

- サーバ プロファイルの追加：[サーバ（Servers）] の横にある追加アイコン（）をクリックします。1 つ以上の IP アドレスを [サーバ アドレス（Server Address）] フィールドに指定し、[OK] をクリックします。
- サーバ プロファイルの削除：ポリシーの横にある削除アイコン（）をクリックします。
- サーバ プロファイルの編集：[サーバ（Servers）] の下にあるプロファイルの設定済みアドレスをクリックするか、[デフォルト（default）] をクリックします。[設定（Configuration）] セクションの設定を変更できます。DCE/RPC ターゲットベース ポリシー オプション （2311 ページ）を参照してください。

ステップ 8 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後にキャッシュされた変更は破棄されます。

次のタスク

- 侵入イベントを生成する場合は、DCE/RPC プリプロセッサ ルール（GID 132 または 133）を有効にします。詳細については、侵入ルール状態の設定 （2093 ページ）、DCE/RPC グローバル オプション （2309 ページ）、DCE/RPC ターゲットベース ポリシー オプション （

2311 ページ）、およびトラフィックに関連する DCE/RPC ルール（2317 ページ）を参照してください。

- 設定変更を展開します。設定変更の展開（447 ページ）を参照してください。

関連トピック

Firepower システムの IP アドレス表記法（20 ページ）
ファイルおよびマルウェアのインスペクション パフォーマンスとストレージのオプション（1961 ページ）
DCE/RPC キーワード（2223 ページ）
レイヤの管理（2053 ページ）
競合と変更：ネットワーク分析および侵入ポリシー（2041 ページ）

DNS プリプロセッサ

DNS プリプロセッサは、DNS ネーム サーバ応答を検査し、次に示す特定のエクスプロイトがあるかどうかを確認します。

- RData テキスト フィールドに対するオーバーフローの試行
- 古い DNS リソース レコード タイプ
- 試験的な DNS リソース レコード タイプ

最も一般的なタイプの DNS ネーム サーバ応答には、応答を求めたクエリ内のドメイン名に対応する 1 つ以上の IP アドレスが示されています。その他のタイプのサーバ応答には、たとえば、電子メール メッセージの宛先や、元のクエリの対象のサーバからは取得できない情報を提供できるネーム サーバの位置などが記述されています。

DNS 応答には以下の構成要素があります。

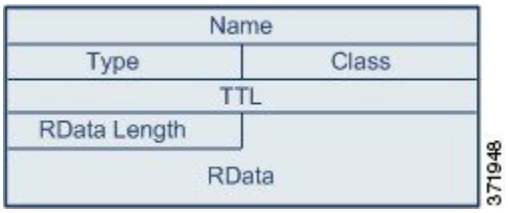
- メッセージ ヘッダー
- 1 つ以上の要求が含まれる [質問（Question）] セクション
- [質問（Question）] セクションの要求に応答する 3 つのセクション
  - 応答
  - 権限（Authority）
  - その他の情報（Additional Information）

この 3 セクションの応答には、ネーム サーバに保持されているリソース レコード（RR）の情報が反映されます。次の表で、これらの 3 つのセクションについて説明します。

表 *229 : DNS* ネーム サーバ *RR* 応答

セクション	内容	例
Answer	クエリに対する特定の回答を提供する 1 つ以上のリソース レコード（オプション）	ドメイン名に対応する IP アドレス
Authority	権威ネーム サーバを指し示す 1 つ以上のリソース レコード（オプション）	応答の権威ネームサーバの名前
Additional Information	[Answer] セクションに関連する追加情報を提供する 1 つ以上のリソース レコード（オプション）	クエリ対象の別のサーバの IP アドレス

さまざまなタイプのリソース レコードがありますが、これらはすべて一貫して次の構造を保っています。



理論上、すべてのタイプのリソース レコードを、ネーム サーバ応答メッセージの [応答（Answer）]、[権威（Authority）]、または [追加情報（Additional Information）] セクションで使用できます。DNS プリプロセッサは、検出されたエクスプロイトについて、3 つの各応答セクションのすべてのリソース レコードを検査します。

[Type] および [RData] リソース レコード フィールドは、DNS プリプロセッサでは特に重要です。[Type] フィールドは、リソース レコードのタイプを示します。[RData]（リソース データ）フィールドは、応答の内容を示します。[RData] フィールドのサイズと内容は、リソース レコードのタイプによって異なります。

DNS メッセージは通常、UDP トランスポート プロトコルを使用しますが、信頼性のある配信を必要とするメッセージ タイプである場合や、メッセージ サイズが UDP で処理可能なサイズを超えている場合は、TCP を使用します。DNS プリプロセッサは、UDP および TCP の両方のトラフィックで DNS サーバ応答を検査します。

DNS プリプロセッサは、ミッドストリームで検出された TCP セッションを検査せず、ドロップされたパケットが原因でセッションの状態が失われるとインスペクションを終了します。

DNS プリプロセッサ オプション

ポート

このフィールドは、送信元ポート、またはDNSプリプロセッサがDNSサーバ応答をモニタする必要があるポートを指定します。複数のポートを指定する場合は、カンマで区切ります。

DNSプリプロセッサ用に設定する一般的なポートは、ウェルノウン ポート53です。これは、DNS ネーム サーバがUDPおよびTCPの両方でDNSメッセージに使用するポートです。

RData テキスト フィールドでのオーバーフローの試行の検出

リソース レコード タイプがTXT（テキスト）の場合、RDataフィールドは可変長のASCIIテキスト フィールドになります。

このオプションを選択した場合は、MITREのCurrent Vulnerabilities and Exposuresデータベースの CVE-2006-3441エントリで指定した特定の脆弱性を検出します。これは、Microsoft Windows 2000 Service Pack 4、Windows XP Service Pack 1およびService Pack 2、Windows Server 2003 Service Pack 1の既知の脆弱性です。攻撃者はこの脆弱性を悪用して、[RData]テキスト フィールドの長さの誤算を引き起こし、結果としてバッファ オーバーフローを発生させるよう悪意をもって作られたネームサーバ応答をホストに送信するか受信させることで、ホストを完全に制御できます。

アップグレードによってこの脆弱性が修正されていないオペレーティング システムが稼働しているホストがネットワーク内に含まれている可能性がある場合は、このオプションを有効にする必要があります。

ルール131:3を有効にすることができますイベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定（2093ページ）を参照してください。

古い DNS RR タイプの検知

RFC 1035ではさまざまなリソース レコード タイプが古いタイプとして指定されています。これらは古いレコード タイプであるため、一部のシステムはこれらのレコード タイプに対応しておらず、エクスプロイトの対象となることがあります。このようなレコードタイプを含めるようにネットワークを意図的に設定している場合を除き、通常のDNS応答でこのようなレコード タイプが検出されることは想定されません。

既知の古いリソース レコード タイプを検出するようにシステムを設定できます。次の表に、これらのレコード タイプとその説明を示します。

表 *230*：古い *DNS* リソース レコード タイプ

RR タイプ	コード	説明
3	MD	メールの宛先
4	MF	メールのフォワーダ

ルール 131:1 を有効にすることができますイベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定 （2093 ページ） を参照してください。

試験的な DNS RR タイプの検出

RFC 1035 ではさまざまなリソース レコード タイプが試験的なタイプとして指定されています。これらは試験的なレコード タイプであるため、一部のシステムはこれらのレコード タイプに対応しておらず、エクスプロイトの対象となることがあります。このようなレコードタイプを含めるようにネットワークを意図的に設定している場合を除き、通常の DNS 応答でこのようなレコード タイプが検出されることは想定されません。

既知の試験的なレコードタイプを検出するようにシステムを設定できます。次の表に、これらのレコード タイプとその説明を示します。

表 *231 :* 試験的な *DNS* リソース レコード タイプ

RR タイプ	コード	説明
7	MB	メールボックスのドメイン名
8	MG	メール グループ メンバー
9	MR	メール リネーム ドメイン名
10	NUL	空白のリソース レコード

ルール 131:2 を有効にすることができますイベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定 （2093 ページ） を参照してください。

DNS プリプロセッサの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Intrusion Admin

マルチドメイン展開では、編集できる現在のドメインで作成されたポリシーが表示されます。また、編集できない先祖ドメインで作成されたポリシーも表示されます。下位のドメインで作成されたポリシーを表示および編集するには、そのドメインに切り替えます。

ステップ 1 **[Policies]** > **[Access Control]**、次に **[Network Analysis Policy]** または **[Policies]** > **[Access Control]** > **[Intrusion]**、次に **[Network Analysis Policy]** を選択します。

（注） カスタム ユーザ ロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

ステップ 2 編集するポリシーの横にある編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 ナビゲーション パネルで [設定（Settings）] をクリックします。

ステップ 4 [アプリケーション層プリプロセッサ（Application Layer Preprocessors）] の下の [DNS の構成（DNS Configuration）] が無効になっている場合は、[有効化（Enabled）] をクリックします。

ステップ 5 [DNS の構成（DNS Configuration）] の横にある編集アイコン（）をクリックします。

ステップ 6 DNS プリプロセッサ オプション （2321 ページ）で説明されている設定を変更します。

ステップ 7 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後にキャッシュされた変更は破棄されます。

次のタスク

- 侵入イベントを生成する場合は、DNS プリプロセッサ ルール（GID 131）を有効にします。詳細については、侵入ルール状態の設定 （2093 ページ）およびDNS プリプロセッサ オプション （2321 ページ）を参照してください。
- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

関連トピック

侵入ポリシーおよびネットワーク分析ポリシーのレイヤ （2045 ページ）
競合と変更：ネットワーク分析および侵入ポリシー （2041 ページ）

FTP/Telnet デコーダ

FTP/Telnet デコーダは FTP および Telnet データ ストリームを分析して、ルール エンジンによる処理の前に FTP および Telnet コマンドを正規化します。

グローバル FTP および Telnet オプション

FTP/Telnet デコーダがパケットのステートフル インスペクションまたはステートレス インスペクションを実行するかどうか、デコーダが暗号化 FTP または Telnet セッションを検出するかどうか、およびデコーダが暗号化データの検出後にデータ ストリームの検査を続行するかどうかを決定するグローバル オプションを設定できます。

以下の説明でプリプロセッサ ルールが言及されていない場合、オプションにはプリプロセッサ ルールが関連付けられていません。

ステートフル インスペクション（Stateful Inspection）

選択されている場合、FTP/Telnetデコーダは状態を保存し、各パケットにセッション コンテキストを提供し、再構成されたセッションだけを検査します。選択されていない場合、セッション コンテキストなしで個々のパケットを分析します。

FTP データ転送を検査するには、このオプションを選択する必要があります。

Detect Encrypted Traffic

暗号化 Tenet および FTP セッションを検出します。

ルール 125:7 と 126:2 を有効にすることができます。イベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定（2093 ページ）を参照してください。

暗号化データの検査を続行（Continue to Inspect Encrypted Data）

プリプロセッサに対し、データ ストリームの暗号化後もデータ ストリームの検査を続行し、最終的に処理できるデコードされたデータを検索するように指示します。

Telnet オプション

FTP/Telnet デコーダによる Telnet コマンドの正規化を有効または無効にし、特定の異常ケースを有効または無効にし、許容可能な Are You There（AYT）攻撃数のしきい値を設定できます。

以下の説明でプリプロセッサ ルールが言及されていない場合、オプションにはプリプロセッサ ルールが関連付けられていません。

ポート

Telnet トラフィックを正規化するポートを示します。通常、Telnet は TCP ポート 23 に接続します。インターフェイスで、複数のポートをカンマで区切って指定します。

⚠

注意 暗号化トラフィック（SSL）はデコードできないので、ポート 22（SSH）を追加すると、予想外の結果が生じる可能性があります。

正規化（Normalize）

指定のポートへの Telnet トラフィックを正規化します。

Detect Anomalies

対応する SE（サブネゴシエーション終了）がない Telnet SB（サブネゴシエーション開始）の検出を有効にします。

Telnet がサポートするサブネゴシエーションは、SB（サブネゴシエーション開始）で開始し SE（サブネゴシエーション終了）で終了していなければなりません。しかし、一部の Telnet

サーバ実装では、対応する SE のない SB が無視されます。これは、回避事例につながるおそれのある異常な動作です。FTP はコントロール接続で Telnet プロトコルを使用するため、FTP もこの動作の影響を受けます。

ルール 126:3 を有効にすることでイベントを生成でき、インライン展開では、この異常が Telnet トラフィックで検出される場合に違反パケットをドロップできます。FTP コマンドチャネルで検出される場合はルール 125:9 を有効にできます。侵入ルール状態の設定（2093 ページ）を参照してください。

Are You There 攻撃のしきい値（Are You There Attack Threshold Number）

連続する AYT コマンドの数が指定のしきい値を超えた場合にそのことを検出します。Cisco は、AYT しきい値としてデフォルト値以下の値を設定することを推奨します。

ルール 126:1 を有効にすることができます。イベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定（2093 ページ）を参照してください。

サーバレベルの FTP オプション

複数の FTP サーバでデコード オプションを設定できます。作成する各サーバ プロファイルには、トラフィックをモニタするサーバのサーバ IP アドレスとポートが含まれます。検証する FTP コマンドと、特定のサーバで無視する FTP コマンドを指定し、コマンドの最大パラメータ長を設定できます。また、デコーダが特定のコマンドで検証する特定のコマンド構文を設定し、代替最大コマンド パラメータ長を設定することもできます。

以下の説明でプリプロセッサ ルールが言及されていない場合、オプションにはプリプロセッサ ルールが関連付けられていません。

Networks

FTP サーバの 1 つ以上の IP アドレスを指定するには、このオプションを使用します。

単一 IP アドレスまたはアドレス ブロック、あるいはこのいずれかまたは両方をカンマで区切ったリストを指定できます。設定できる最大文字数は 1024 文字です。デフォルト プロファイルを含め最大 255 個のプロファイルを設定できます。

（注） システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。 上書き対応オブジェクトを使用すると、子孫ドメインの管理者は、グローバル コンフィギュレーションを自分のローカル環境に調整できます。

デフォルト ポリシーの `default` 設定では、別のターゲットベース ポリシーでカバーされていないモニタ対象ネットワーク セグメントのすべての IP アドレスが指定されることに注意してください。したがって、デフォルト ポリシーの IP アドレスまたはアドレス ブロックは指定できず、また指定する必要もありません。また、別のポリシーでこの設定を空白にしたり、すべてを表すアドレス表記（0.0.0.0/0 または ::/0）を使用することはできません。

Ports

管理対象デバイスがトラフィックをモニタするFTPサーバのポートを指定するには、このオプションを使用します。インターフェイスで、複数のポートをカンマで区切って指定します。ポート 21 は FTP トラフィック用のウェルノウン ポートです。

File Get コマンド（File Get Commands）

サーバからクライアントにファイルを転送するために使用するFTPコマンドを定義するには、このオプションを使用します。サポートからの指示がない限り、これらの値を変更しないでください。

⚠

注意 サポートからの指示がない限り、[File Get コマンド（File Get Commands）] フィールドを変更しないでください。

File Put コマンド（File Put Commands）

クライアントからサーバにファイルを転送するために使用するFTPコマンドを定義するには、このオプションを使用します。サポートからの指示がない限り、これらの値を変更しないでください。

⚠

注意 サポートからの指示がない限り、[File Put コマンド（File Put Commands）] フィールドを変更しないでください。

追加 FTP コマンド（Additional FTP Commands）

デコーダが検出するコマンドを追加で指定するには、この行を使用します。複数のコマンドを追加する場合は、コマンドをスペースで区切ってください。

追加できるコマンドには、`XPWD`、`XCWD`、`XCUP`、`XMKD`、`XRMD` があります。これらのコマンドの詳細については、RFC 775（Network Working Group によるディレクトリに基づく FTP コマンドの仕様）を参照してください。

デフォルト最大パラメータ長（Default Max Parameter Length）

代替最大パラメータ長が設定されていないコマンドの最大パラメータ長を検出するには、このオプションを使用します。代替最大パラメータ長は、必要な数だけ追加できます。

ルール 125:3 を有効にすることができますイベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定 （2093 ページ） を参照してください。

代替最大パラメータ長（Alternate Max Parameter Length）

異なる最大パラメータ長を検出するコマンドを指定し、それらのコマンドの最大パラメータ長を指定するには、このオプションを使用します。[Add] をクリックして行を追加し、特定のコマンドで検出する異なる最大パラメータ長を指定します。

Check Commands for String Format Attacks

指定されたコマンドでフォーマット文字列攻撃を検査するには、このオプションを使用します。

ルール 125:5 を有効にすることができます。イベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定（2093 ページ）を参照してください。

コマンドの妥当性（Command Validity）

特定のコマンドの有効な形式を入力するには、このオプションを使用します。[追加（Add）] をクリックして、コマンド検証行を追加します。

ルール 125:2 と 125:4 を有効にすることができます。イベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定（2093 ページ）を参照してください。

FTP 転送を無視（Ignore FTP Transfers）

データ転送チャネルで状態インスペクション以外のすべてのインスペクションを無効にして FTP データ転送のパフォーマンスを改善するには、このオプションを使用します。

（注） データ転送を検査するには、グローバル FTP/Telnet オプション [ステートフル インスペクション（Stateful Inspection）] を選択する必要があります。

FTP コマンドでの Telnet エスケープ コードの検出（Detect Telnet Escape Codes within FTP Commands）

FTP コマンド チャネルで Telnet コマンドが使用された場合にそのことを検出するには、このオプションを使用します。

ルール 125:1 を有効にすることができます。イベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定（2093 ページ）を参照してください。

正規化時に消去コマンドを無視（Ignore Erase Commands during Normalization）

[Detect Telnet Escape Codes within FTP Commands] が選択されている場合に、FTP トラフィックの正規化時に Telnet の文字および行の消去コマンドを無視するには、このオプションを使用します。この設定は、FTP サーバによる Telnet 消去コマンドの処理方法と一致する必要がありま

す。一般に、新しい FTP サーバは Telnet 消去コマンドを無視しますが、ほとんどの古いサーバは Telnet 消去コマンドを処理する点に注意してください。

トラブルシューティング オプション：FTP コマンドの検証設定のログを記録（Troubleshooting Options：Log FTP Command Validation Configuration）

トラブルシューティングについてサポートに問い合わせた際に、サーバ用にリストされている FTP コマンドごとに設定情報を出力するように、システムを設定することを指示される場合があります。

⚠

注意 サポートからの指示がない限り [FTP コマンドの検証設定のログを記録（Log FTP Command Validation Configuration）] を有効にしないでください。

FTP コマンドの検証ステートメント

FTP コマンドに対する検証ステートメントを設定するときには、複数の代替パラメータをスペースで区切って指定できます。2 つのパラメータ間にバイナリ OR 関係を作成するには、検証ステートメントでこの2つのパラメータをパイプ文字（|）で区切って指定します。パラメータを大カッコ（[]）で囲むと、これらのパラメータがオプションであることを示します。パラメータを中カッコ（{}）で囲むと、これらのパラメータが必須であることを示します。

FTP 通信の一部として受信したパラメータの構文を検証する FTP コマンド パラメータ検証ステートメントを作成できます。

FTP コマンド パラメータ検証ステートメントに使用できるパラメータを次の表に示します。

表 *232 : FTP* コマンド パラメータ

使用するパラメータ	実行される検証
`int`	示されるパラメータが整数である必要があります。
`number`	示されるパラメータが 1 ～ 255 の範囲内の整数である必要があります。
`char` _chars	示されるパラメータが単一文字であり、かつ _chars 引数に指定した文字の 1 つである必要があります。 たとえば、検証引数 `char` SBC を使用して `MODE` のコマンド検証を定義すると、`MODE` コマンドのパラメータが、文字 `S`（Stream モードを示す）、文字 `B`（Block モードを示す）、または文字 `C`（Compressed モードを示す）を含んでいるかどうかが検証されます。

使用するパラメータ	実行される検証
`date` _datefmt	_datefmt に `#` が含まれている場合、示されるパラメータは数値である必要があります。 _datefmt に `c` が含まれている場合、示されるパラメータは文字である必要があります。 _datefmt にリテラル文字列が含まれている場合、示されるパラメータはリテラル文字列に一致している必要があります。
`string`	示されるパラメータが文字列である必要があります。
`host_port`	示されるパラメータは、RFC 959（Network Working Group による File Transfer Protocol 仕様）で定義されている有効なホスト ポート指定子である必要があります。

上記の表の構文を必要に応じて組み合わせることにより、トラフィックを検証する必要がある各 FTP コマンドを正しく検証するパラメータ検証ステートメントを作成できます。

（注） TYPE コマンドに複合式を含める場合は、式をスペースで囲んでください。また、式内の各オペランドをスペースで囲んでください。たとえば、`char A|B` ではなく `char A | B` と入力します。

関連トピック

サーバレベルの FTP オプション （2325 ページ）
Firepower システムの IP アドレス表記法 （20 ページ）
FTP コマンドの検証ステートメント （2328 ページ）

クライアントレベルの FTP オプション

カスタム FTP クライアント プロファイルを設定するには、これらのオプションを使用します。オプション記述にプリプロセッサ ルールが含まれない場合、そのオプションはプリプロセッサ ルールに関連付けられません。

ネットワーク

FTP クライアントの 1 つ以上の IP アドレスを指定するには、このオプションを使用します。

単一 IP アドレスまたはアドレス ブロック、あるいはこのいずれかまたは両方をカンマで区切ったリストを指定できます。指定できる最大文字数は 1024 文字です。デフォルト プロファイルを含め最大 255 個のプロファイルを設定できます。

（注） システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。 上書き対応オブジェクトを使用すると、子孫ドメインの管理者は、グローバル コンフィギュレーションを自分のローカル環境に調整できます。

デフォルト ポリシーの `default` 設定では、別のターゲットベース ポリシーでカバーされていないモニタ対象ネットワーク セグメントのすべての IP アドレスが指定されることに注意してください。したがって、デフォルト ポリシーの IP アドレスまたはアドレス ブロックは指定できず、また指定する必要もありません。また、別のポリシーでこの設定を空白にしたり、すべてを表すアドレス表記（0.0.0.0/0 または ::/0）を使用することはできません。

最大応答長（Max Response Length）

このオプションを使用して、クライアントが受け入れる FTP コマンドに許可される最大応答長を指定します。これにより、基本的なバッファ オーバーフローを検出できます。

ルール 125:6 を有効にすることができますイベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定（2093 ページ） を参照してください。

FTP バウンス試行の検出（Detect FTP Bounce Attempts）

FTP バウンス攻撃を検出するには、このオプションを使用します。

ルール 125:8 を有効にすることができますイベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定（2093 ページ） を参照してください。

FTP バウンスの許可（Allow FTP Bounce to）

FTP PORT コマンドを FTP バウンス攻撃として扱わない追加のホストとそれらのホスト上のポートのリストを設定するには、このオプションを使用します。

Detect Telnet Escape Codes within FTP Commands

FTP コマンド チャネルで Telnet コマンドが使用された場合にそのことを検出するには、このオプションを使用します。

ルール 125:1 を有効にすることができます。イベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定（2093 ページ） を参照してください。

正規化時に消去コマンドを無視（Ignore Erase Commands during Normalization）

[Detect Telnet Escape Codes within FTP Commands] が選択されている場合に、FTP トラフィックの正規化時に Telnet の文字および行の消去コマンドを無視するには、このオプションを使用します。この設定は、FTP クライアントによる Telnet 消去コマンドの処理方法に一致している必

要があります。一般に、新しい FTP クライアントは Telnet 消去コマンドを無視しますが、ほとんどの古いクライアントは Telnet 消去コマンドを処理する点に注意してください。

関連トピック

Firepower システムの IP アドレス表記法 （20 ページ）

FTP/Telnet デコーダの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Intrusion Admin

クライアントからのFTP トラフィックをモニタするように、FTPクライアントのクライアントプロファイルを設定できます。

システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。 上書き対応オブジェクトを使用すると、子孫ドメインの管理者は、グローバルコンフィギュレーションを自分のローカル環境に調整できます。

始める前に

- カスタム ターゲットベース ポリシーで識別するネットワークが、親ネットワーク分析ポリシーによって処理されるネットワーク、ゾーン、および VLAN のサブセットと一致するか、サブセットであることを確認します。詳細については、ネットワーク分析プロファイルの詳細設定 （2289 ページ）を参照してください。

ステップ 1 **[Policies]** > **[Access Control]**、次に **[Network Analysis Policy]**または**[Policies]** > **[Access Control]** > **[Intrusion]**、次に **[Network Analysis Policy]**を選択します。

（注） カスタム ユーザ ロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

ステップ 2 編集するポリシーの横にある編集アイコン（）をクリックします。

代わりに表示アイコン（  ）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 ナビゲーション パネルで [設定（Settings）] をクリックします。

ステップ 4 [アプリケーション層プリプロセッサ（Application Layer Preprocessors）] の下の [FTP と Telnet の構成（FTP and Telnet Configuration）] が無効になっている場合は、[有効化（Enabled）] をクリックします。

ステップ 5 [FTP と Telnet の構成（FTP and Telnet Configuration）] の横にある編集アイコン（  ）をクリックします。

ステップ 6 グローバル FTP および Telnet オプション （2323 ページ）の説明に従って、[グローバル設定（Global Settings）] セクションのオプションを設定します。

ステップ 7 Telnet オプション （2324 ページ）の説明に従って、[Telnet の設定（Telnet Settings）] セクションのオプションを設定します。

ステップ 8 FTP サーバ プロファイルを管理します。

- サーバ プロファイルの追加：[FTP サーバ（FTP Server）] の横にある追加アイコン（）をクリックします。クライアントの 1 つ以上の IP アドレスを [サーバ アドレス（Server Address）] フィールドに指定し、[OK] をクリックします。単一の IP アドレスまたはアドレス ブロック、あるいはこれらのいずれかまたは両方をカンマで区切ったリストを指定できます。指定できる最大文字数は 1024 文字です。デフォルト ポリシーを含め最大 255 個のポリシーを設定できます。
- サーバ プロファイルの編集：[FTP サーバ（FTP Server）] の下にあるカスタム プロファイルの設定済みアドレスをクリックするか、[デフォルト（default）] をクリックします。[設定（Configuration）] セクションの設定を変更できます。サーバレベルの FTP オプション （2325 ページ）を参照してください。
- サーバ プロファイルの削除：プロファイルの横にある削除アイコン（）をクリックします。

ステップ 9 FTP クライアント プロファイルを管理します。

- クライアント プロファイルの追加：[FTP クライアント（FTP Client）] の横にある追加アイコン（）をクリックします。クライアントの 1 つ以上の IP アドレスを [クライアント アドレス（Client Address）] フィールドに指定し、[OK] をクリックします。単一の IP アドレスまたはアドレス ブロック、あるいはこれらのいずれかまたは両方をコンマで区切ったリストを指定できます。指定できる最大文字数は 1024 文字です。デフォルト ポリシーを含め最大 255 個のポリシーを設定できます。
- クライアント プロファイルの編集：[FTP クライアント（FTP Client）] の下にあるプロファイルの設定済みアドレスをクリックするか、[デフォルト（default）] をクリックします。[設定（Configuration）] ページエリアの設定を変更できます。クライアントレベルの FTP オプション （2329 ページ）を参照してください。
- クライアント プロファイルの削除：カスタム プロファイルの横にある削除アイコン（）をクリックします。

ステップ 10 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後にキャッシュされた変更は破棄されます。

次のタスク

- 侵入イベントを生成する場合は、FTP および telnet プリプロセッサ ルール（GID 125 および 126）を有効にします。詳細については、「侵入ルール状態の設定 （2093 ページ）」を参照してください。
- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

関連トピック

Firepower システムの IP アドレス表記法 （20 ページ）

レイヤの管理 （2053 ページ）
競合と変更：ネットワーク分析および侵入ポリシー （2041 ページ）

HTTP Inspect プリプロセッサ

HTTP Inspect プリプロセッサは、次の処理を行います。

- ネットワーク上の Web サーバに送信される HTTP 要求と Web サーバから受信する HTTP 応答をデコードおよび正規化する。
- HTTP 関連の侵入ルールのパフォーマンス向上のため、Web サーバに送信されたメッセージを URI、非 cookie の見出し、cookie 見出し、メソッド、メッセージ ボディの各コンポーネントに分ける。
- HTTP 関連の侵入ルールのパフォーマンス向上のため、Web サーバから受信したメッセージをステータス コード、ステータス メッセージ、非 set-cookie 見出し、cookie 見出し、および応答ボディの各コンポーネントに分ける。
- URI エンコード攻撃の可能性を検出する。
- 正規化データを追加ルール処理に使用できるようにする。

HTTP トラフィックはさまざまな形式でエンコードされている可能性があり、このことが、ルールによる適切な検査の実施を困難にしています。HTTP Inspect は 14 種類のエンコードをデコードし、HTTP トラフィックが最良のインスペクションを受けられるようにします。

HTTP Inspect のオプションは、グローバルに設定するか、1 つのサーバで設定するか、またはサーバ リストに対して設定することができます。

プリプロセッサ エンジンは HTTP の正規化をステートレスに実行することに注意してください。つまり、パケット単位で HTTP 文字列を正規化し、TCP ストリーム プリプロセッサにより再構成された HTTP 文字列のみを処理できます。

グローバル HTTP 正規化オプション

HTTP Inspect プリプロセッサのグローバル HTTP オプションは、プリプロセッサの機能を制御します。Web サーバ ポートとして指定されていないポートが HTTP トラフィックを受信する場合の HTTP 正規化を有効または無効にするには、このオプションを使用します。

次の点に注意してください。

- [無制限の圧縮解除（Unlimited Decompression）] を有効にすると、変更のコミット時に [圧縮データの最大深さ（Maximum Compressed Data Depth）] および [圧縮解除データの最大深さ（Maximum Decompressed Data Depth）] オプションが自動的に 65535 に設定されます。
- 最大値は、[圧縮データの最大深さ（Maximum Compressed Data Depth）] または [圧縮解除データの最大深さ（Maximum Decompressed Data Depth）] の値が異なる場合に使用されます。

- デフォルトのネットワーク分析ポリシー
- 同じアクセス コントロール ポリシーのネットワーク分析ルールによって呼び出される、他のカスタム ネットワーク分析ポリシー

以下の説明でプリプロセッサルールが言及されていない場合、オプションにはプリプロセッサルールが関連付けられていません。

異常な HTTP サーバの検出（Detect Anomalous HTTP Servers）

Web サーバ ポートとして指定されていないポートに送信された HTTP トラフィックまたはこのポートで受信した HTTP トラフィックを検出します。

（注） このオプションをオンにする場合は、[HTTP 設定（HTTP Configuration）] ページで、HTTP トラフィックを受信するすべてのポートがサーバプロファイルにリストされていることを確認してください。確認せずにこのオプションと関連するプリプロセッサ ルールを有効にすると、サーバとの間の通常のトラフィックによってイベントが生成されます。デフォルトのサーバプロファイルには、HTTP トラフィックに一般に使用されるすべてのポートが含まれていますが、このプロファイルを変更した場合は、イベントの生成を防ぐために別のプロファイルにそれらのポートを追加する必要があります。

ルール 120:1 を有効にすることができます。イベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定（2093 ページ） を参照してください。

HTTP プロキシ サーバの検出（Detect HTTP Proxy Servers）

[HTTP プロキシの使用を許可（Allow HTTP Proxy Use）] オプションで定義されていないプロキシ サーバを使用する HTTP トラフィックを検出します。

ルール 119:17 を有効にすることができます。イベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定（2093 ページ） を参照してください。

圧縮データの最大深さ（Maximum Compressed Data Depth）

[圧縮データの検査（Inspect Compressed Data）]（および任意で、[SWF ファイルの圧縮解除（LZMA）（Decompress SWF File（LZMA））]、[SWF ファイルの圧縮解除（Deflate）（Decompress SWF File（Deflate））]、または [PDF ファイルの圧縮解除（Deflate）（Decompress PDF File（Deflate））]）が有効な場合に、圧縮解除する圧縮データの最大サイズを設定します。

圧縮解除データの最大深さ（Maximum Decompressed Data Depth）

[圧縮データの検査（Inspect Compressed Data）]（および任意で、[SWF ファイルの圧縮解除（LZMA）（Decompress SWF File（LZMA））]、[SWF ファイルの圧縮解除（Deflate）

（Decompress SWF File（Deflate））]、または [PDF ファイルの圧縮解除（Deflate）（Decompress PDF File（Deflate））]）が有効な場合に、正規化された圧縮データの最大サイズを設定します。

サーバレベルの HTTP 正規化オプション

サーバレベルのオプションは、モニタ対象サーバごとに設定するか、すべてのサーバに対してグローバルに設定するか、またはサーバリストに対して設定することができます。また、事前定義のサーバプロファイルを使用してこれらのオプションを設定するか、またはご使用の環境のニーズに合わせて個別に設定することができます。これらのオプション、またはこれらのオプションを設定するデフォルト プロファイルの 1 つを使用して、トラフィックを正規化する HTTP サーバポート、正規化するサーバ応答ペイロードの量、および正規化するエンコードのタイプを指定します。

以下の説明でプリプロセッサルールが言及されていない場合、オプションにはプリプロセッサルールが関連付けられていません。

Networks

1 つ以上のサーバの IP アドレスを指定するには、このオプションを使用します。1 つの IP アドレスまたはアドレス ブロックを指定するか、そのいずれかまたは両方から成るカンマで区切ったリストを指定できます。

デフォルト プロファイルを含めてプロファイルの合計数は最大 255 ですが、さらに、HTTP サーバ リストに最大 496 文字（約 26 エントリ）を含めることができ、すべてのサーバ プロファイルに対して合計 256 のアドレス エントリを指定できます。

（注） システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。 上書き対応オブジェクトを使用すると、子孫ドメインの管理者は、グローバル コンフィギュレーションを自分のローカル環境に調整できます。

デフォルト ポリシーの `default` 設定では、別のターゲットベース ポリシーでカバーされていないモニタ対象ネットワーク セグメントのすべての IP アドレスが指定されることに注意してください。したがって、デフォルト ポリシーの IP アドレスまたは CIDR ブロック/プレフィクス長は指定できず、また指定する必要もありません。また、別のポリシーでこの設定を空白にしたり、`すべて` を表すアドレス表記（0.0.0.0/0 または ::/0）を使用したりすることはできません。

Ports

プリプロセッサエンジンが HTTP トラフィックを正規化するポート。ポート番号が複数ある場合は、カンマで区切ります。

サイズ超過のディレクトリ長（Oversize Dir Length）

指定された値よりも長い URL ディレクトリを検出します。

指定された長さよりも長い URL の要求をプロセッサが検出した場合にイベントを生成し、インライン展開では、違反パケットをドロップします。するには、ルール 119:15 を有効にします。

クライアント フローの深さ（Client Flow Depth）

[Ports] で定義されているクライアント側 HTTP トラフィックで、ルールにより検査される raw HTTP パケットのバイト数（見出しとペイロード データを含む）を指定します。ルール内の HTTP コンテンツ ルール オプションによって要求メッセージの特定の部分が検査される場合は、[クライアント フローの深さ（Client Flow Depth）] は適用されません。

次のいずれかを指定します。

- 正の値によって、最初のパケットで指定のバイト数が検査されます。最初のパケットのバイト数が指定のバイト数よりも少ない場合は、パケット全体が検査されます。指定された値は、セグメント化されたパケットと再構成されたパケットの両方に適用されることに注意してください。

  また、値 300 を指定すると、通常は、多くのクライアント要求ヘッダーの終わりにある大きな HTTP Cookie のインスペクションが排除されることにも注意してください。

- 0 を指定すると、すべてのクライアント側トラフィックが検査されます。これにはセッション内の複数のパケットが含まれ、必要な場合にはバイトの上限を超えることもあります。この値はパフォーマンスに影響する可能性があることに注意してください。

- -1 を指定すると、クライアント側のすべてのトラフィックが無視されます。

Server Flow Depth

[Ports] で指定されたサーバ側 HTTP トラフィックで、ルールにより検査される raw HTTP パケットのバイト数を指定します。[Inspect HTTP Responses] が無効である場合は raw 見出しとペイロードが検査され、[Inspect HTTP Response] が有効である場合は、raw 応答ボディのみが検査されます。

Server Flow Depth は、[Ports] で定義されているサーバ側 HTTP トラフィックで、ルールにより検査されるセッション内の raw サーバ応答データのバイト数を指定します。このオプションを使用して、HTTP サーバ応答データのインスペクションのレベルとパフォーマンスのバランスを調整できます。ルール内の HTTP コンテンツ オプションによって要求メッセージの特定の部分が検査される場合は、Server Flow Depth は適用されません。

クライアント フローの深さ（Client Flow Depth）とは異なり、サーバ フローの深さ（Server Flow Depth）では、ルールが検査するバイト数を、HTTP 要求パケットごとではなく、HTTP 応答ごとのバイト数として指定します。

次のいずれかの値を指定できます。

- 正の値：

[HTTP 応答の検査（Inspect HTTP Responses）] が**有効**である場合、raw HTTP 応答ボディのみが検査され、raw HTTP ヘッダーは検査されません。また、[圧縮データの検査（Inspect Compressed Data）] が有効である場合は、圧縮解除データも検査されます。

[Inspect HTTP Responses] が**無効**である場合、raw パケット 見出しとペイロードが検査されます。

セッションの応答バイト数が指定の値よりも少ない場合は、そのセッションで、ルールにより（必要に応じて複数パケットにわたって）すべての応答パケットが完全に検査されます。セッションの応答バイト数が指定の値よりも多い場合、そのセッションで、ルールにより（必要に応じて複数パケットにわたって）指定のバイト数だけが検査されます。

Flow Depth の値が小さい場合、[Ports] で定義されているサーバ側トラフィックを対象とするルールで、検出漏れが発生する可能性があります。これらのルールのほとんどは HTTP 見出しまたはコンテンツ（これは多くの場合非見出しデータの先頭の約 100 バイト内にあります）を対象とします。通常見出しの長さは 300 バイト未満ですが、見出しサイズは異なることがあります。

指定された値は、セグメント化されたパケットと再構成されたパケットの両方に適用されることにも注意してください。

- 0 を指定すると、[Port] で定義されているすべての HTTP サーバ側トラフィックでパケット全体が検査されます。これにはセッションでの 65535 バイトよりも大きな応答データも含まれます。

  この値はパフォーマンスに影響する可能性があることに注意してください。

- -1：

  [Inspect HTTP Responses] が**有効**な場合、raw HTTP 見出しだけが検査され、raw HTTP 応答ボディは検査されません。

  [Inspect HTTP Responses] が**無効**である場合、[Ports] で定義されているすべてのサーバ側トラフィックは無視されます。

Maximum Header Length

[HTTP 応答の検査（Inspect HTTP Responses）] が有効である場合は、HTTP 要求、および HTTP 応答で、指定されている最大バイト数よりも長いヘッダー フィールドを検出します。値 0 を指定すると、このオプションが無効になります。これを有効にするため正の値を指定します。

ルール 119:19 を有効にすることができます。イベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定（2093 ページ） を参照してください。

最大ヘッダー数（Maximum Number of Headers）

HTTP 要求でヘッダー数がこの設定を超えている場合にそのことを検出します。値 0 を指定すると、このオプションが無効になります。これを有効にするため正の値を指定します。

ルール 119:20 を有効にすることができます。イベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定（2093ページ）を参照してください。

最大スペース数（Maximum Number of Spaces）

折りたたみ行のスペースの数がHTTP要求のこの設定と等しいか、超えている場合にそのことを検出します。値0を指定すると、このオプションが無効になります。これを有効にするため正の値を指定します。

ルール 119:26 を有効にすることができます。イベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定（2093ページ）を参照してください。

HTTP クライアント ボディの抽出の深さ（HTTP Client Body Extraction Depth）

HTTP クライアント要求のメッセージボディから抽出するバイト数を指定します。侵入ルールを使用して抽出データを検査するには、`content` または `protected_content` キーワードを [HTTP クライアント ボディ（HTTP Client Body）] オプションと共に選択します。

クライアント ボディを無視するには、-1 を指定します。クライアント ボディ全体を抽出するには、0を指定します。抽出対象のバイト数を指定すると、システムパフォーマンスが向上することがある点に注意してください。また、侵入ルールで[HTTP クライアントボディ（HTTP Client Body）] オプションが機能するためには、0 か 0 より大きい値を指定する必要があることに注意してください。

小さいチャンク サイズ（Small Chunk Size）

チャンクが小さいとみなされるサイズの最大バイト数を指定します。正の値を指定します。値 0 を指定すると、異常な小さなセグメントの連続の検出が無効になります。詳細については、[Consecutive Small Chunks] オプションを参照してください。

Consecutive Small Chunks

チャンク転送エンコードを使用するクライアント トラフィックまたはサーバ トラフィックで異常に大量であるとみなされる、連続する小さなチャンクの数を指定します。[Small Chunk Size] オプションは、小さなチャンクの最大サイズを指定します。

たとえば、10 バイト以下のチャンクが 5 つ連続していることを検出するには、[小さいチャンク サイズ（Small Chunk Size）] に 10 を設定し、[連続する小さいチャンク（Consecutive Small Chunks）] に 5 を設定します。

大量の小さなチャンクが検出される場合に イベントを生成し、インライン展開では、違反パケットをドロップします。するには、クライアントトラフィックの場合はプリプロセッサルール 119:27 を有効にし、サーバトラフィックの場合はルール 120:7 を有効にします。[小さいチャンク サイズ（Small Chunk Size）] が有効であり、このオプションが 0 または 1 に設定されている場合にこれらのルールを有効にすると、指定されたサイズ以下のすべてのチャンクでイベントがトリガーとして使用されます。

HTTP メソッド（HTTP Methods）

システムがトラフィックで検出すると予期される、GET および POST 以外の HTTP 要求メソッドを指定します。複数の値はカンマで区切ります。

侵入ルールでは、HTTP メソッドのコンテンツを検索するために、`content` または `protected_content` キーワードが **HTTP Method** 引数と共に使用されます。GET、POST、およびこのオプションで設定されているメソッド以外のメソッドがトラフィックで検出される場合にイベントを生成し、インライン展開では、違反パケットをドロップします。するには、ルール 119:31 を有効にします。侵入ルール状態の設定 （2093 ページ）を参照してください。

アラートなし（No Alerts）

関連するプリプロセッサ ルールが有効である場合に、侵入イベントを無効にします。

（注） このオプションは、HTTP の標準テキスト ルールと共有するオブジェクト ルールを無効にしません。

HTTP ヘッダーの正規化（Normalize HTTP Headers）

[Inspect HTTP Responses] が有効である場合は、要求見出しと応答見出しで非 cookie データの正規化が有効になります。[Inspect HTTP Responses] が有効**ではない**場合は、要求見出しと応答見出しで cookie を含む HTTP 見出し全体の正規化が有効になります。

Inspect HTTP Cookies

HTTP 要求見出しからの cookie の抽出を有効にします。また、[Inspect HTTP Responses] が有効である場合は、応答見出しの set-cookie データの抽出も有効になります。cookie の抽出が不要な場合は、このオプションを無効にするとパフォーマンスが向上します。

`Cookie:` および `Set-Cookie:` の見出し名、見出し行の先頭のスペース、および見出し行の末尾の `CRLF` は、cookie の一部ではなく見出しの一部として検査されます。

Normalize Cookies in HTTP headers

HTTP 要求見出しの cookie の正規化を有効にします。[Inspect HTTP Responses] が有効である場合は、応答見出しで set-cookie データの正規化が有効になります。このオプションを選択する前に、[Inspect HTTP Cookies] を選択する必要があります。

Allow HTTP Proxy Use

モニタ対象 Web サーバを HTTP プロキシとして使用できるようにします。このオプションは、HTTP 要求のインスペクションでのみ使用されます。

Inspect URI Only

正規化された HTTP 要求パケットの URI 部分のみを検査します。

Inspect HTTP Responses

HTTP 応答の拡張インスペクションが有効になり、プリプロセッサは、HTTP 要求メッセージのデコードと正規化の他に、ルールエンジンによるインスペクションのために応答フィールドを抽出します。このオプションを有効にすると、応答ヘッダー、ボディ、ステータスコードなどがシステムにより抽出されます。また [HTTP Cookie の検査（Inspect HTTP Cookies）] が有効な場合は、set-cookie データも抽出されます。

イベントを生成し、インライン展開では、違反パケットをドロップします。するには、ルール 120:2 と120:3 を次のように有効にします。

表 *233 : HTTP* 応答ルールのインスペクション

ルール	以下の場合にトリガーする
120:2	無効な HTTP 応答のステータス コードが発生します。
120:3	HTTP 応答にはコンテンツ長または転送エンコーディングは含まれません。

UTF エンコードの UTF-8 への正規化（Normalize UTF Encodings to UTF-8）

[HTTP 応答の検査（Inspect HTTP Responses）] が有効である場合、HTTP 応答で UTF-16LE、UTF-16BE、UTF-32LE、および UTF32-BE エンコードが検出され、UTF-8 に正規化されます。

UTF 標準化が失敗した場合にイベントを生成し、インライン展開では、違反パケットをドロップします。 するには、ルール 102:4 を有効にします。

圧縮データの検査（Inspect Compressed Data）

[Inspect HTTP Responses] が有効である場合、HTTP 応答ボディでの gzip および deflate 互換圧縮データの圧縮解除と、正規化された圧縮解除データのインスペクションが有効になります。システムは、チャンク HTTP 応答データと非チャンク HTTP 応答データを検査します。システムは、必要に応じて複数のパケットにわたり圧縮解除データをパケット単位で検査します。つまり、システムが異なるパケットの圧縮解除データをインスペクションのために結合させることはありません。[Maximum Compressed Data Depth]、[Maximum Decompressed Data Depth]、または圧縮データの終わりに到達すると、圧縮解除が終了します。[無制限の圧縮解除（Unlimited Decompression）] を選択していない場合は、[サーバ フローの深さ（Server Flow Depth）] に到達すると、圧縮解除データのインスペクションが終了します。圧縮解除データを検査するには、`file_data` ルール キーワードを使用できます。

イベントを生成し、インライン展開では、違反パケットをドロップします。 するには、ルール 120:6 と120:24 を次のように有効にします。

表 *234 :* 圧縮された *HTTP* 応答ルールのインスペクション

ルール	以下の場合にトリガーする
120:6	圧縮された HTTP 応答の圧縮が失敗しました。

ルール	以下の場合にトリガーする
120:24	圧縮された HTTP 応答の部分的な圧縮が失敗しました。

無制限の圧縮解除（Unlimited Decompression）

[Inspect Compressed Data]（および任意で、[Decompress SWF File (LZMA)]、[Decompress SWF File (Deflate)]、または [Decompress PDF File (Deflate)]）が有効な場合、複数のパケットにわたって [Maximum Decompressed Data Depth] がオーバーライドされます。つまり、このオプションにより、複数のパケットにわたる無制限の圧縮解除が有効になります。このオプションを有効にしても、単一パケット内での [圧縮データの最大深さ（Maximum Compressed Data Depth）] または [圧縮解除データの最大深さ（Maximum Decompressed Data Depth）] には影響しないことに注意してください。また、このオプションを有効にすると、変更のコミット時に、[圧縮データの最大深さ（Maximum Compressed Data Depth）] と [圧縮解除データの最大深さ（Maximum Decompressed Data Depth）] が 65535 に設定されることにも注意してください。

Javascript の正規化（Normalize Javascript）

[Inspect HTTP Responses] が有効な場合、HTTP 応答ボディ内での Javascript の検出と正規化を有効にします。プリプロセッサは unescape 関数や decodeURI 関数、String.fromCharCode メソッドなどの難読化 Javascript データを正規化します。プリプロセッサは、unescap、decodeURI、および decodeURIComponent 関数内の次のエンコードを正規化します。

- %XX
- %uXXXX
- 0xXX
- \xXX
- \uXXXX

プリプロセッサは連続するスペースを検出し、1 つのスペースに正規化します。このオプションが有効である場合、設定フィールドでは、難読化 Javascript データで許容する連続スペースの最大数を指定できます。入力できる値は、1 ～ 65535 です。値 0 を指定すると、このフィールドに関連付けられているプリプロセッサルール（120:10）が有効かどうかに関係なく、イベントの生成が無効になります。

プリプロセッサは、Javascript の正符号（+）演算子も正規化し、この演算子を使用して文字列を連結します。

`file_data` 侵入ルール キーワードを使用して、正規化された Javascript データに対し侵入ルールを指し示すことができます。

イベントを生成し、インライン展開では、違反パケットをドロップします。するには、次に示すように、ルール 120:9、120:10、および 120:11 を有効にします。

表 *235 : [Javascript* の正規化（***Normalize Javascript***）*]* オプションのルール（***Normalize Javascript Option Rules***）

ルール	以下の場合にトリガーする
120:9	プリプロセッサ内の難読化レベルが 2 以上である。
120:10	Javascript 難読化データで連続するスペースの数が、許容される連続スペースの最大数として設定された値以上である。
120:11	エスケープされたデータまたはエンコードされたデータに、複数のエンコード タイプが含まれている。

SWF ファイルの圧縮解除（LZMA）（Decompress SWF File（LZMA））および SWF ファイルの圧縮解除（Deflate）（Decompress SWF File（Deflate））

[HTTP Inspect の応答（HTTP Inspect Responses）] が有効な場合、これらのオプションは、HTTP 要求の HTTP 応答ボディ内にあるファイルの圧縮部分を圧縮解除します。

（注） HTTP GET 応答で見つかったファイルの圧縮部分**のみ**を圧縮解除できます。

- [SWF ファイルの圧縮解除（LZMA）（Decompress SWF File（LZMA））] は、Adobe ShockWave Flash（.swf）ファイルの LZMA 互換の圧縮部分を圧縮解除します。
- [SWF ファイルの圧縮解除（Deflate）（Decompress SWF File（Deflate））] は、Adobe ShockWave Flash（.swf）ファイルの deflate 互換の圧縮部分を圧縮解除します。

[圧縮データの最大深さ（Maximum Compressed Data Depth）]、[圧縮解除データの最大深さ（Maximum Decompressed Data Depth）]、または圧縮データの終わりに到達すると、圧縮解除が終了します。[無制限の圧縮解除（Unlimited Decompression）] を選択していない場合は、[サーバ フローの深さ（Server Flow Depth）] に到達すると、圧縮解除データのインスペクションが終了します。圧縮解除データを検査するには、file_data 侵入ルール キーワードを使用できます。

イベントを生成し、インライン展開では、違反パケットをドロップします。するには、次に示すように、ルール 120:12 および 120:13 を有効にします。

表 *236 : [SWF* ファイルの圧縮解除（***Decompress SWF File***）*]* オプションのルール

ルール	以下の場合にトリガーする
120:12	deflate ファイルの圧縮解除に失敗
120:13	LZMA ファイルの圧縮解除に失敗

PDF ファイルの圧縮解除（Deflate）（Decompress PDF File（Deflate））

[HTTP Inspect の応答（HTTP Inspect Responses）] が有効な場合、[PDF ファイルの圧縮解除（Deflate）（Decompress PDF File（Deflate）] は、HTTP 要求の HTTP 応答ボディ内にある Portable Document Format（`.pdf`）ファイルの deflate 互換の圧縮部分を圧縮解除します。システムは、`/FlateDecode` ストリーム フィルタが付いた PDF ファイルだけを圧縮解除できます。他のフィルタ（`/FlateDecode /FlateDecode` など）はサポートしていません。

（注） HTTP GET 応答で見つかったファイルの圧縮部分**のみ**を圧縮解除できます。

[圧縮データの最大深さ（Maximum Compressed Data Depth）]、[圧縮解除データの最大深さ（Maximum Decompressed Data Depth）]、または圧縮データの終わりに到達すると、圧縮解除が終了します。[無制限の圧縮解除（Unlimited Decompression）] を選択していない場合は、[サーバ フローの深さ（Server Flow Depth）] に到達すると、圧縮解除データのインスペクションが終了します。圧縮解除データを検査するには、`file_data` 侵入ルール キーワードを使用できます。

イベントを生成し、インライン展開では、違反パケットをドロップします。するには、次に示すように、ルール 120:14、120:15、120:16、および 120:17 を有効にします。

表 *237 : [PDF* ファイルの圧縮解除（*Deflate*）（*Decompress PDF File*（*Deflate*））*]* オプションのルール（*Decompress PDF File (Deflate) Option Rules*）

ルール	以下の場合にトリガーする
120:14	ファイルの圧縮解除に失敗
120:15	圧縮タイプがサポート対象外のタイプであるため、ファイルの圧縮解除に失敗
120:16	PDF ストリーム フィルタがサポート対象外のフィルタであるため、ファイルの圧縮解除に失敗
120:17	ファイルの解析に失敗

元のクライアント IP アドレスの抽出（Extract Original Client IP Address）

侵入検査中の、元のクライアント IP アドレスの調査を有効にします。システムは元のクライアント IP アドレスを、X-Forwarded-For（XFF）、True-Client-IP、または [XFF ヘッダーの優先順位（XFF Header Priority）] オプションで定義したカスタム HTTP ヘッダーから抽出します。侵入イベント テーブルで、抽出された元のクライアント IP アドレスを表示できます。

イベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定（2093 ページ） を参照してください。するには、ルール 119:23、119:29、および 119:30 を有効にします。

XFF ヘッダーの優先順位（XFF Header Priority）

HTTP 要求に複数のヘッダーが存在する場合は、システムが元のクライアント IP ヘッダーを処理する順序を指定します。デフォルトでは、システムはまず X-Forwarded-For（XFF）ヘッダーを、次に True-Client-IP ヘッダーを調査します。追加したら、各ヘッダー タイプの横にある上下矢印アイコンを使用して、優先順位を調整します。

このオプションでは、抽出と評価のために、XFF または True-Client-IP 以外の元のクライアント IP ヘッダーを指定できます。[Add] をクリックして、カスタム ヘッダー名をプライオリティ リストに追加します。システムは、XFF または True-Client-IP ヘッダーと同じ構文を使用するカスタム ヘッダーのみをサポートします。

このオプションを設定する場合は、以下の点に留意してください。

- アクセス コントロールと侵入検査の両方で、システムは元のクライアント IP アドレス ヘッダーを評価するときにこの優先順位を使用します。
- 元のクライアント IP ヘッダーが複数ある場合、システムは優先順位が最も高いヘッダーのみを処理します。
- XFF ヘッダーには、要求が渡されたときに経由したプロキシ サーバを表す、IP アドレスのリストが含まれています。スプーフィングを防止するために、システムはリスト内の最後の IP アドレス（つまり、信頼されるプロキシにより追加されたアドレス）を、元のクライアント IP アドレスとして使用します。

URI のログ（Log URI）

raw URI が存在する場合に、HTTP 要求パケットから raw URI を抽出できるようにし、このセッションで生成されるすべての侵入イベントにこの URI を関連付けます。

このオプションが有効である場合、侵入イベント テーブル ビューの [HTTP URI] 列に、抽出された URI の先頭 50 文字を表示できます。パケット ビューでは、URI 全体（最大 2048 バイト）を表示できます。

ホスト名のログ（Log Hostname）

ホスト名が存在する場合に、HTTP 要求の Host 見出しから raw URI を抽出できるようにし、このセッションで生成されるすべての侵入イベントにこのホスト名を関連付けます。複数の Host 見出しがある場合は、1 番目の見出しからホスト名を抽出します。

このオプションが有効である場合、侵入イベント テーブル ビューの [HTTP Hostname] 列に、抽出されたホスト名の先頭 50 文字を表示できます。パケット ビューでは、ホスト名全体（最大 256 バイト）を表示できます。

ルール 119:25 を有効にすることができます。イベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定（2093 ページ） を参照してください。

有効にすると、このオプションの設定に関係なく、HTTP 要求で複数のホスト ヘッダーが検出された場合、ルール 119:24 がトリガーされます。

プロファイル（Profile）

HTTP トラフィック向けに正規化されたエンコードのタイプを指定します。システムには、ほとんどのサーバに適用できるデフォルトプロファイル、Apache サーバと IIS サーバ用のデフォルトプロファイル、およびモニタ対象トラフィックのニーズに合わせて調整できるカスタムのデフォルト設定があります。

- すべてのサーバに対して適切な標準のデフォルト プロファイルを使用するには、[すべて（All）] を選択します。
- システムによって提供される IIS プロファイルを使用するには、[IIS] を選択します。
- システムによって提供される Apache プロファイルを使用するには、[Apache] を選択します。
- 独自のサーバ プロファイルを作成するには、[カスタム（Custom）] を選択します。

サーバレベルの HTTP 正規化エンコード オプション

HTTP サーバレベルの [プロファイル（Profile）] オプションを `Custom` に設定すると、HTTP トラフィックに対して正規化されるエンコードタイプを指定できます。また、HTTP のプリプロセッサ ルールを有効にして、異なるエンコード タイプを含むトラフィックに対してイベントを生成できます。

以下の説明でプリプロセッサ ルールが言及されていない場合、オプションにはプリプロセッサ ルールが関連付けられていません。

ASCII エンコード

エンコードされた ASCII 文字をデコードし、ルール エンジンが ASCII エンコード URI でイベントを生成するかどうかを指定します。

ルール 119:1 を有効にすることができますイベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定（2093 ページ） を参照してください。

UTF-8 エンコード

URI の標準 UTF-8 Unicode シーケンスをデコードします。

ルール 119:6 を有効にすることができますイベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定（2093 ページ） を参照してください。

Microsoft %U エンコード

%u とその後に続く 4 文字を使用する IIS %u エンコード スキームをデコードします。この 4 文字は、IIS Unicode コードポイントに関連する 16 進数のエンコード値です。

ヒント　正規のクライアントが %u エンコードを使用することはほとんどないため、シスコは、%u エンコードによってエンコードされている HTTP トラフィックをデコードすることを推奨します。

ルール 119:3 を有効にすることができますイベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定（2093 ページ）を参照してください。

ベア バイト UTF-8 エンコード

ベア バイト エンコードをデコードします。ベア バイト エンコードは、UTF-8 値のデコード時に非 ASCII 文字を有効な値として使用します。

ヒント　ベア バイト エンコードにより、ユーザは IIS サーバをエミュレートし、非標準エンコードを正しく解釈することができます。正規のクライアントはこの方法で UTF-8 をエンコードしないため、シスコは、このオプションを有効にすることを推奨します。

ルール 119:4 を有効にすることができますイベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定（2093 ページ）を参照してください。

Microsoft IIS エンコード

Unicode コードポイント マッピングを使用してデコードします。

ヒント　これは主に攻撃と回避の試行で見られるため、シスコはこのオプションを有効にすることを推奨します。

ルール 119:7 を有効にすることができますイベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定（2093 ページ）を参照してください。

二重符号化

要求 URI を 2 回通過し、それぞれでデコードを実行するようにすることで、IIS 二重エンコード トラフィックをデコードします。これは通常は攻撃シナリオでのみ検出されるため、シスコはこのオプションを有効にすることを推奨します。

ルール 119:2 を有効にすることができますイベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定（2093 ページ）を参照してください。

マルチスラッシュ オブファスケーション

1 つの行内の複数のスラッシュを 1 つのスラッシュに正規化します。

ルール 119:8 を有効にすることができますイベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定（2093 ページ）を参照してください。

IIS バックスラッシュ オブファスケーション

バックスラッシュをスラッシュに正規化します。

ルール 119:9 を有効にすることができますイベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定（2093 ページ）を参照してください。

ディレクトリ トラバーサル

ディレクトリ トラバーサルおよび自己参照用ディレクトリを正規化します。一部の Web サイトはディレクトリ トラバーサルを使用してファイルを参照するため、このタイプのトラフィックに対してイベントを生成するために、関連するプリプロセッサ ルールを有効にすると、誤検出が発生する可能性があります。

ルール 119:10 と 119:11 を有効にすることができます イベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定（2093 ページ）を参照してください。

タブ オブファスケーション

スペース区切り記号としてタブを使用する非 RFC 標準を正規化します。Apache やその他の IIS 以外の Web サーバは、URL の区切り文字としてタブ文字（0x09）を使用します。

（注） このオプションの設定に関係なく、空白文字（0x20）がタブの前にある場合、HTTP Inspect プリプロセッサはそのタブをスペースとして扱います。

ルール 119:12 を有効にすることができます イベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定（2093 ページ）を参照してください。

無効な RFC 区切り文字

URI データの改行（\ n）を正規化します。

ルール 119:13 を有効にすることができます イベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定（2093 ページ）を参照してください。

Webroot ディレクトリ トラバーサル

URL の初期ディレクトリを越えて横断するディレクトリ トラバーサルを検出します。

ルール 119:18 を有効にすることができます イベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定（2093 ページ） を参照してください。

タブ区切り（URI）

URI の区切り文字としてタブ文字（0x09）を有効にします。Apache、新しいバージョンの IIS、およびその他の一部の Web サーバは、URL の区切り文字としてタブ文字を使用します。

（注） このオプションの設定に関係なく、空白文字（0x20）がタブの前にある場合、HTTP Inspect プリプロセッサはそのタブをスペースとして扱います。

非 RFC 文字

対応するフィールドに追加された非 RFC 文字リストが、着信または発信 URI データ内に含まれている場合にそれを検出します。このフィールドを変更する場合は、バイト文字を表す 16 進表記を使用します。このオプションを設定する場合は、値を慎重に設定してください。非常に一般的な文字を使用すると、イベントが大量に発生する可能性があります。

ルール 119:14 を有効にすることができます イベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定（2093 ページ） を参照してください。

チャンク形式の最大エンコード サイズ

URI データで異常に大きなチャンク サイズを検出します。

ルール 119:16 と 119:22 を有効にすることができます イベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定（2093 ページ） を参照してください。

パイプライン デコードの無効化

パイプライン処理された要求の HTTP デコードを無効にします。このオプションが無効である場合、パイプラインで待機する HTTP 要求には、デコードおよび分析は行われず、汎用パターン マッチングを使用した検査のみが行われるため、パフォーマンスが向上します。

Non-Strict URI 解析

Non-Strict URI 解析を有効にします。このオプションは、「GET /index.html abc xo qr \n」という形式の非標準 URI を受け入れるサーバのみで使用します。このオプションを使用すると、デコーダは URI が 1 番目のスペースと 2 番目のスペースで囲まれているものと想定します。これは、2 番目のスペースの後に有効な HTTP 識別子がない場合でも同様です。

拡張 ASCII エンコード

HTTP 要求 URI の拡張 ASCII 文字の解析を有効にします。このオプションは、カスタム サーバ プロファイルでのみ使用可能であり、Apache、IIS、またはすべてのサーバ向けに提供されるデフォルト プロファイルでは使用できないことに注意してください。

関連トピック

概要：HTTP content および protected_content キーワードの引数 （2170 ページ）
Firepower システムの IP アドレス表記法 （20 ページ）

HTTP 検査プリプロセッサの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Intrusion Admin

システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。 上書き対応オブジェクトを使用すると、子孫ドメインの管理者は、グローバル コンフィギュレーションを自分のローカル環境に調整できます。

始める前に

- カスタム ターゲットベース ポリシーで識別するネットワークが、親ネットワーク分析ポリシーによって処理されるネットワーク、ゾーン、および VLAN のサブセットと一致するか、サブセットであることを確認します。詳細については、ネットワーク分析プロファイルの詳細設定 （2289 ページ）を参照してください。

ステップ 1 **[Policies]** > **[Access Control]**、次に **[Network Analysis Policy]**または**[Policies]** > **[Access Control]** > **[Intrusion]**、次に **[Network Analysis Policy]**を選択します。

（注） カスタムユーザ ロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

ステップ 2 編集するポリシーの横にある編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 ナビゲーション パネルで [設定（Settings）] をクリックします。

ステップ 4 [アプリケーション層プリプロセッサ（Application Layer Preprocessors）] の下の [HTTP の設定（HTTP Configuration）] が無効になっている場合は、[有効化（Enabled）] をクリックします。

ステップ 5 [HTTP の設定（HTTP Configuration）] の横にある編集アイコン（）をクリックします。

ステップ 6 [グローバル設定（Global Settings）] ページ エリアのオプションを変更します。グローバル HTTP 正規化オプション （2333 ページ）を参照してください。

ステップ 7 次の 3 つの選択肢があります。

- サーバ プロファイルの追加：[サーバ（Servers）] セクションの追加アイコン（  ）をクリックします。クライアントの 1 つ以上の IP アドレスを [サーバ アドレス（Server Address）] フィールドに指定し、[OK] をクリックします。単一の IP アドレスまたはアドレス ブロック、あるいはこれらのいずれかまたは両方をカンマで区切ったリストを指定できます。リストに入力できる文字数は最大496 文字、すべてのサーバ プロファイルで指定できるアドレス項目の総数は 256、作成できるプロファイルの総数はデフォルト プロファイルを含めて 255 です。
- サーバ プロファイルの編集：[サーバ（Servers）] の下で追加したプロファイルの設定済みアドレスをクリックするか、[デフォルト（default）] をクリックします。[設定（Configuration）] セクションの設定を変更できます。サーバレベルの HTTP 正規化オプション （2335 ページ）を参照してください。プロファイル値で [カスタム（Custom）] を選択した場合は、サーバレベルの HTTP 正規化エンコード オプション （2345 ページ）で説明されているエンコーディング オプションを変更することもできます。
- サーバ プロファイルの削除：カスタム プロファイルの横にある削除アイコン（  ）をクリックします。

ステップ 8 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後にキャッシュされた変更は破棄されます。

次のタスク

- イベントを生成し、インライン展開では、違反パケットをドロップします。する場合は、HTTP プリプロセッサ ルール（GID 119）を有効にします。詳細については、「侵入ルール状態の設定 （2093 ページ）」を参照してください。
- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

関連トピック

レイヤの管理 （2053 ページ）
競合と変更：ネットワーク分析および侵入ポリシー （2041 ページ）

その他の HTTP 検査プリプロセッサ ルール

特定の設定オプションに関連付けられていない HTTP Inspect プリプロセッサ ルールのイベントを生成するには、次の表の「プリプロセッサ ルール GID：SID」列のルールを有効にできます。

表 *238 :* その他の *HTTP* 検査プリプロセッサ ルール

プリプロセッサ ルール GID:SID	以下の場合にトリガーする
119:21	HTTP 要求ヘッダーに複数の `content-length` フィールドがあります。
119:24	HTTP 要求に複数の Host ヘッダーがあります。
119:28	HTTP POST メソッドに `content-length` ヘッダーも chunked に設定された `transfer-encoding` もありません。
119:32	HTTP バージョン 0.9 がトラフィックで検出されました。TCP ストリームの設定も有効にする必要があることに注意してください。
119:33	HTTP URI にエスケープされていないスペースが含まれています。
119:34	TCP 接続に 24 以上のパイプライン処理された HTTP 要求が含まれています。
120:5	HTTP 応答トラフィックで UTF-7 エンコードが検出されました。UTF-7 は、SMTP トラフィックなどで 7 ビット パリティが必要な場合にのみ使用してください。
120:8	`content-length` またはチャンク サイズが無効です。
120:18	HTTP サーバ応答はクライアント要求の前に実行されます。
120:19	HTTP 応答に複数のコンテンツ長が含まれています。
120:20	HTTP 応答に複数のコンテンツのエンコーディングが含まれています。
120:25	HTTP 応答に無効なヘッダーの折返しが含まれています。
120:26	HTTP 応答ヘッダーの前に不正な行があります。
120:27	HTTP 応答にヘッダーの末尾が含まれていません。
120:28	無効なチャンク サイズが発生したか、またはチャンク サイズの後に不正な文字が続いています。

Sun RPC プリプロセッサ

リモート プロシージャ コール（RPC）の正規化では、フラグメント化された複数の RPC レコードを取得し、それらを 1 つのレコードに正規化するので、ルール エンジンがそのレコード

全体を検査できます。たとえば、攻撃者が RPC `admind` が実行されているポートの検出を試行するとします。一部の UNIX ホストは、RPC `admind` を使用してリモート分散システム タスクを実行します。ホストが弱い認証を実行する場合、悪意のあるユーザがリモート管理のコントロールを獲得できることがあります。[Snort ID]（SID）575 の標準テキスト ルール（GID：1）では、特定のロケーションでコンテンツを検索して、不適切な `portmap GETPORT` 要求を特定することで、この攻撃を検出します。

Sun RPC プリプロセッサのオプション

ポート

トラフィックを正規化するポートを示します。インターフェイスで、複数のポートをカンマで区切って指定します。一般的な RPC ポートは 111 および 32771 です。ネットワークが他のポートに RPC トラフィックを送信する場合は、それらのポートの追加を検討してください。

RPC フラグメント化レコードの検出（Detect fragmented RPC records）

RPC フラグメント化レコードを検出します。

ルール 106:1 と 106:5 を有効にすることができますイベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定（2093 ページ）を参照してください。

1 パケットの複数レコードの検出（Detect multiple records in one packet）

パケット（または再構成されたパケット）ごとに、複数の RPC 要求を検出します。

ルール 106:2 を有効にすることができますイベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定（2093 ページ）を参照してください。

1 フラグメントを超えるフラグメント化レコード合計の検出（Detect fragmented record sums which exceed one fragment）

現在のパケット長を超える再構成されたフラグメント化レコード長を検出します。

ルール 106:3 を有効にすることができますイベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定（2093 ページ）を参照してください。

1 パケットのサイズを超える単一フラグメント レコードの検出（Detect single fragment records which exceed the size of one packet）

部分的なレコードを検出します。

ルール 106:4 を有効にすることができますイベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定（2093 ページ）を参照してください。

Sun RPC プリプロセッサの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Intrusion Admin

ステップ 1 **[Policies]** > **[Access Control]**、次に **[Network Analysis Policy]** または **[Policies]** > **[Access Control]** > **[Intrusion]**、次に **[Network Analysis Policy]** を選択します。

（注） カスタムユーザロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

ステップ 2 編集するポリシーの横にある編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 ナビゲーション パネルで [設定（Settings）] をクリックします。

ステップ 4 [アプリケーション層プリプロセッサ（Application Layer Preprocessors）] の下の [Sun RPC の構成（Sun RPC Configuration）] が無効になっている場合は、[有効化（Enabled）] をクリックします。

ステップ 5 [Sun RPC の構成（Sun RPC Configuration）] の横にある編集アイコン（）をクリックします。

ステップ 6 Sun RPC プリプロセッサのオプション （2352 ページ）で説明されている設定を変更します。

ステップ 7 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後にキャッシュされた変更は破棄されます。

次のタスク

- イベントを生成し、インライン展開では、違反パケットをドロップします。する場合は、Sun RPC プリプロセッサ ルール（GID 106）を有効にします。詳細については、「侵入ルール状態の設定 （2093 ページ）」を参照してください。
- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

関連トピック

レイヤの管理 （2053 ページ）
競合と変更：ネットワーク分析および侵入ポリシー （2041 ページ）

SIP プリプロセッサ

Session Initiation Protocol（SIP）は、インターネット テレフォニー、マルチメディア会議、インスタント メッセージング、オンライン ゲーム、ファイル転送などのクライアント アプリケーションの 1 人以上のユーザに対し、1 つ以上のセッションのコールのセットアップ、変更、およびティアダウンを提供します。各 SIP 要求の *method* フィールドは要求の目的を示し、Request-URI に要求の送信先が指定されます。各 SIP 応答のステータス コードは、要求されたアクションの結果を示します。

SIP を使用してコールがセットアップされた後、後続の音声およびビデオによる通信は Real-time Transport Protocol（RTP）により処理されます。セッションのこの部分は、コール チャネル、データ チャネル、または音声/ビデオ データ チャネルと呼ばれることがあります。RTP は、データチャネル パラメータ ネゴシエーション、セッション通知、およびセッションへの招待のための SIP メッセージ ボディ内で Session Description Protocol（SDP）を使用します。

SIP プリプロセッサは次の処理を実行します。

- SIP 2.0 トラフィックのデコードおよび分析
- SDP データが存在する場合はこのデータを含む SIP ヘッダーとメッセージ ボディを抽出し、抽出したデータを今後のインスペクションのためにルール エンジンに受け渡す
- 次の状態が検出され、対応するプリプロセッサ ルールが有効な場合にイベントを生成する
  - SIP パケット内の異常と既知の脆弱性
  - 順序が間違っているコール シーケンスと無効なコール シーケンス
- コール チャネルの無視（オプション）

プリプロセッサは、SIP メッセージ ボディに組み込まれている SDP メッセージに示されているポートに基づいて RTP チャネルを識別しますが、RTP プロトコル インスペクションを実行しません。

SIP プリプロセッサを使用するときは、次の点に注意してください。

- UDP は通常、SIP でサポートされるメディア セッションを伝送します。UDP ストリームの前処理により、SIP プリプロセッサに対し SIP セッション トラッキングが提供されます。
- SIP ルール キーワードにより、SIP パケット ヘッダーまたはメッセージ ボディを指し示し、検出対象を特定の SIP メソッドまたはステータス コードのパケットに限定できます。

SIP プリプロセッサのオプション

次のオプションでは、1 から 65535 バイトの正の値を指定するか 0 を指定して、関連するルールが有効にされているかどうかにかかわらず、オプションのイベント生成を無効にできます。

- **要求 URI の最大長（Maximum Request URI Length）**

- コール ID の最大長（Maximum Call ID Length）
- 要求名の最大長（Maximum Request Name Length）
- 送信元の最大長（Maximum From Length）
- 送信先の最大長（Maximum To Length）
- 経由の最大長（Maximum Via Length）
- 連絡先の最大長（Maximum Contact Length）
- コンテンツの最大長（Maximum Content Length）

以下の説明でプリプロセッサルールが言及されていない場合、オプションにはプリプロセッサルールが関連付けられていません。

Ports

SIP トラフィックを検査するポートを指定します。0 ～ 65535 の整数を指定できます。複数のポート番号を指定する場合は、カンマで区切ります。

Methods to Check

検出する SIP メソッドを指定します。次に示す現在定義されている SIP メソッドを指定できます。

```
ack, benotify, bye, cancel, do, info, invite, join, message,
notify, options, prack, publish, quath, refer, register,
service, sprack, subscribe, unsubscribe, update
```

メソッドでは大文字と小文字が区別されません。メソッド名には英字、数字、下線文字を使用できます。その他の特殊文字は使用できません。複数のメソッドを指定する場合は、カンマで区切ります。

新しいSIPメソッドが今後定義される可能性があるため、設定には、現在定義されていない英字文字列を含めることができます。システムでは最大 32 個のメソッド（現在定義されている 21 個のメソッドと追加の 11 個のメソッド）がサポートされます。システムは、設定される未定義のメソッドをすべて無視します。

合計32個のメソッドには、このオプションに指定するメソッドの他に、侵入ルールで`sip_method`キーワードを使用して指定するメソッドも含まれることに注意してください。

セッション内のダイアログ最大数（Maximum Dialogs within a Session）

ストリームセッション内で許容されるダイアログの最大数を指定します。この数より多くのダイアログが作成されると、ダイアログの数が、指定されている最大数以下になるまで、最も古いダイアログから順に削除されます。1 ～ 4194303 の整数を指定できます。

ルール 140:27 を有効にすることができます。イベントを生成し、インライン展開では、このオプションの違反パケットをドロップします。侵入ルール状態の設定（2093ページ）を参照してください。

要求 URI の最大長（Maximum Request URI Length）

[要求 URI（Request-URI）] ヘッダー フィールドの最大許容バイト数を指定します。ルール 140:3 が有効である場合、URI が長いと イベントを生成し、インライン展開では、違反パケットをドロップします。。[要求 URI（Request-URI）] フィールドは、要求の宛先のパスまたはページを示します。

Maximum Call ID Length

[要求または応答のコール ID（request or response Call-ID）] ヘッダー フィールドの最大許容バイト数を指定します。ルール 140:5 が有効である場合、Call-ID が長いと イベントを生成し、インライン展開では、違反パケットをドロップします。。[コール ID（Call-ID）] フィールドによって、要求や応答内の SIP セッションが一意に識別されます。

Maximum Request Name Length

要求名で許容される最大バイト数を指定します。要求名は、CSeq トランザクション ID に指定されるメソッドの名前です。ルール 140:7 が有効である場合、リクエスト名が長いと イベントを生成し、インライン展開では、違反パケットをドロップします。。

送信元の最大長（Maximum From Length）

要求または応答の [送信元（From）] ヘッダー フィールドで許容される最大バイト数を指定します。ルール 140:9 が有効である場合、[送信元（From）] が長いと イベントを生成し、インライン展開では、違反パケットをドロップします。。[送信元（From）] フィールドは、メッセージの発信側を識別します。

Maximum To Length

要求または応答の [送信先（To）] ヘッダー フィールドで許容される最大バイト数を指定します。ルール 140:11 が有効である場合、[送信先（To）] が長いと イベントを生成し、インライン展開では、違反パケットをドロップします。。[送信先（To）] フィールドは、メッセージの受信側を識別します。

Maximum Via Length

要求または応答の [経由（Via）] ヘッダー フィールドで許容される最大バイト数を指定します。ルール 140:13 が有効である場合、[経由（Via）] が長いと イベントを生成し、インライン展開では、違反パケットをドロップします。。[経由（Via）] フィールドには要求がたどるパスが示され、応答の場合は受信者情報が示されます。

Maximum Contact Length

要求または応答の [連絡先（Contact）] ヘッダー フィールドで許容される最大バイト数を指定します。ルール 140:15 が有効である場合、[連絡先（Contact）] が長いと イベントを生成し、インライン展開では、違反パケットをドロップします。。[連絡先（Contact）] フィールドには、後続のメッセージについての連絡先を指定する URI が示されます。

Maximum Content Length

要求または応答のメッセージ ボディのコンテンツで許容される最大バイト数を指定します。ルール 140:16 が有効である場合、コンテンツが長いと イベントを生成し、インライン展開では、違反パケットをドロップします。。

音声/ビデオ データ チャネルを無視（Ignore Audio/Video Data Channel）

データ チャネル トラフィックのインスペクションを有効または無効にします。このオプションを有効にすると、プリプロセッサはその他の非データ チャネルSIP トラフィックのインスペクションを続行するので注意してください。

関連トピック

SIP キーワード （2227 ページ）

SIP プリプロセッサの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Intrusion Admin

ステップ 1 **[Policies]** > **[Access Control]**、次に **[Network Analysis Policy]**または**[Policies]** > **[Access Control]** > **[Intrusion]**、次に **[Network Analysis Policy]**を選択します。

（注） カスタムユーザ ロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

ステップ 2 編集するポリシーの横にある編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 ナビゲーション パネルで [設定（Settings）] をクリックします。

ステップ 4 [アプリケーション層プリプロセッサ（Application Layer Preprocessors）] の下の [SIP の設定（SIP Configuration）] が無効になっている場合は、[有効化（Enabled）] をクリックします。

ステップ 5 [SIP の設定（SIP Configuration）] の横にある編集アイコン（）をクリックします。

ステップ 6 SIP プリプロセッサのオプション （2354 ページ）の説明に従ってオプションを変更します。

ステップ 7 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後にキャッシュされた変更は破棄されます。

次のタスク

- イベントを生成し、インライン展開では、違反パケットをドロップします。 を行うには、SIP プリプロセッサ ルール（GID 140）を有効にします。詳細については、「侵入ルール状態の設定 （2093 ページ）」を参照してください。
- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

関連トピック

レイヤの管理 （2053 ページ）
競合と変更：ネットワーク分析および侵入ポリシー （2041 ページ）

その他の SIP プリプロセッサ ルール

次の表に示す SIP プリプロセッサ ルールは、特定の設定オプションに関連付けられていません。その他の SIP プリプロセッサ ルールと同様に、これらのルールによって イベントを生成し、インライン展開では、違反パケットをドロップします。 する場合は、これらのルールを有効にする必要があります。

表 *239 :* その他の *SIP* プリプロセッサ ルール

プリプロセッサ ルール GID:SID	以下の場合にトリガーする
140:1	プリプロセッサがモニタしている SIP セッションの数が、システムで許容される最大数である。
140:2	SIP 要求で [要求 URI（Request URI）] 必須フィールドが空である。
140:4	SIP 要求または応答の Call-ID ヘッダー フィールドが空である。
140:6	SIP 要求または応答の CSeq フィールドのシーケンス番号値が、231 未満の 32 ビット符号なし整数ではない。
140:8	SIP 要求または応答の [送信元（From）] 必須フィールドが空である。
140:10	SIP 要求または応答の [送信先（To）] ヘッダー フィールドが空である。
140:12	SIP 要求または応答の [経由（Via）] ヘッダー フィールドが空である。
140:14	SIP 要求または応答で [連絡先（Contact）] 必須フィールドが空である。

プリプロセッサ ルール GID:SID	以下の場合にトリガーする
140:17	UDP トラフィック内の 1 つの SIP 要求または応答パケットに複数のメッセージが含まれている。SIP の旧バージョンでは複数メッセージがサポートされていますが、SIP 2.0 ではパケットあたり 1 メッセージだけがサポートされていることに注意してください。
140:18	UDP トラフィック内の SIP 要求または応答のメッセージ本文の実際の長さが SIP 要求または応答の [コンテンツ長（Content-Length）] ヘッダー フィールドに指定されている値と一致しない。
140:19	プリプロセッサが SIP 応答の [CSeq] フィールドのメソッド名を認識しない。
140:20	SIP サーバが、認証済み招待メッセージに対してチャレンジを送信しない。これは InviteReplay 請求攻撃の場合に発生することに注意してください。
140:21	呼び出しが設定される前に、セッション情報が変更される。これは FakeBusy 請求攻撃の場合に発生することに注意してください。
140:22	応答ステータス コードが 3 桁の数字でない。
140:23	[コンテンツ タイプ（Content-Type）] ヘッダー フィールドにコンテンツ タイプが指定されておらず、メッセージ ボディにデータが含まれている。
140:24	SIP バージョンが 1、1.1、2.0 でない。
140:25	SIP 要求で、[CSeq] ヘッダーで指定されたメソッドとメソッド フィールドが一致しない。
140:26	プリプロセッサが SIP 要求のメソッド フィールドに指定されたメソッドを認識しない。

GTP プリプロセッサ

General Packet Radio Service（GPRS）Tunneling Protocol（GTP）により、GTP コア ネットワークを介した通信が実現します。GTP プリプロセッサは、GTP トラフィックの異常を検出し、コマンド チャネル シグナリング メッセージをインスペクションのためにルール エンジンに転送します。GTP コマンド チャネル トラフィックでエクスプロイトがあるかどうかを検査するには、`gtp_version`、`gtp_type`、および `gtp_info` ルール キーワードを使用します。

1つの構成オプションで、プリプロセッサがGTPコマンドチャネルメッセージを検査するポートのデフォルト設定を変更できます。

GTP プリプロセッサ ルール

イベントを生成し、インライン展開では、違反パケットをドロップします。するには、次の表に示す GTP プリプロセッサ ルールを有効にする必要があります。

表 *240 : GTP* プリプロセッサ ルール

プリプロセッサ ルール GID:SID	説明
143:1	プリプロセッサが無効なメッセージの長さを検出すると、イベントが生成されます。
143:2	プリプロセッサが無効な情報要素の長さを検出すると、イベントが生成されます。
143:3	プリプロセッサが誤った順序の情報要素を検出すると、イベントが生成されます。

GTP プリプロセッサの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Intrusion Admin

GTP プリプロセッサが GTP コマンド メッセージをモニタするポートを変更するには、次の手順を使用します。

ステップ 1 **[Policies]** > **[Access Control]**、次に **[Network Analysis Policy]**または**[Policies]** > **[Access Control]** > **[Intrusion]**、次に **[Network Analysis Policy]**を選択します。

（注） カスタムユーザロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

ステップ 2 編集するポリシーの横にある編集アイコン（  ）をクリックします。

代わりに表示アイコン（  ）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 左側のナビゲーション パネルで [設定（Settings）] をクリックします。

ステップ 4 [アプリケーション層プリプロセッサ（Application Layer Preprocessors）] の下の [GTP コマンド チャネル構成（GTP Command Channel Configuration）] が無効になっている場合は、[有効化（Enabled）] をクリックします。

ステップ 5 [GTP コマンド チャネル構成（GTP Command Channel Configuration）] の横にある編集アイコン（  ）をクリックします。

ステップ 6 ポート値を入力します。

複数のポートを指定する場合は、カンマで区切ります。

ステップ 7 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後にキャッシュされた変更は破棄されます。

次のタスク

- 侵入イベントを有効にする場合は、GTP プリプロセッサ ルール（GID 143）を有効にします。詳細については、「侵入ルール状態の設定 （2093 ページ）」を参照してください。
- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

IMAP プリプロセッサ

Internet Message Application Protocol（IMAP）は、リモート IMAP サーバから電子メールを取得するときに使用されます。IMAP プリプロセッサはサーバ/クライアント IMAP4 トラフィックを検査し、関連するプリプロセッサルールが有効である場合は異常なトラフィックがあるとイベントを生成します。プリプロセッサは、クライアント/サーバ IMAP4 トラフィックの電子メール添付ファイルを抽出してデコードし、添付ファイル データをルール エンジンに送信することもできます。添付ファイルデータを指し示すには、侵入ルールで `file_data` キーワードを使用します。

抽出とデコードでは、複数の添付ファイル（存在する場合）や、複数パケットにまたがる大きな添付ファイルなども処理されます。

IMAP プリプロセッサ オプション

MIME 電子メール添付ファイルのデコードが不要な場合のデコードまたは抽出では、複数の添付ファイル（存在する場合）および複数パケットにまたがる大きな添付ファイルが処理されることに注意してください。

[Base64 Decoding Depth]、[7-Bit/8-Bit/Binary Decoding Depth]、[Quoted-Printable Decoding Depth]、または [Unix-to-Unix Decoding Depth] オプションの値が以下のポリシーで異なる場合は、最も大きい値が使用されます。

- デフォルトのネットワーク分析ポリシー
- 同じアクセス コントロール ポリシーのネットワーク分析ルールによって呼び出される、他のカスタム ネットワーク分析ポリシー

以下の説明でプリプロセッサルールが言及されていない場合、オプションにはプリプロセッサルールが関連付けられていません。

Ports

IMAP トラフィックを検査するポートを指定します。0 ～ 65535 の整数を指定できます。ポート番号が複数ある場合は、カンマで区切ります。

Base64 デコーディングの深さ（Base64 Decoding Depth）

各 Base64 エンコード MIME 電子メール添付ファイルから抽出してデコードできる最大バイト数を指定します。正の数を指定するか、またはすべての Base64 データをデコードする場合は 0 を指定します。Base64 データを無視するには、-1 を指定します。

4 で割り切れない正の値は、次に大きい 4 の倍数に切り上げられることに注意してください。ただし 65533、65534、および 65535 は 65532 に切り下げられます。

このオプションが有効である場合、ルール 141:4 を有効にすると、デコードの失敗時にイベントを生成し、インライン展開では、違反パケットをドロップします。することができます（エンコードが誤っている場合やデータが破損している場合などにデコードが失敗することがあります）。

7 ビット/8 ビット/バイナリのデコーディングの深さ（7-Bit/8-Bit/Binary Decoding Depth）

デコードを必要としない各 MIME 電子メール添付ファイルから抽出するデータの最大バイト数を指定します。これらの添付ファイル タイプには、7 ビット、8 ビット、バイナリ、およびさまざまなマルチパート コンテンツ タイプ（プレーンテキスト、jpeg イメージ、mp3 ファイルなど）があります。正値またはパケット内のすべてのデータを抽出するには 0 を指定できます。非デコード データを無視するには、-1 を指定します。

このオプションが有効である場合、ルール 141:6 を有効にすると、抽出の失敗時にイベントを生成し、インライン展開では、違反パケットをドロップします。することができます（たとえばデータの破損のために抽出が失敗することがあります）。

Quoted-Printable（QP）のデコーディングの深さ（Quoted-Printable Decoding Depth）

各 quoted-printable（QP）エンコード MIME 電子メール添付ファイルから抽出してデコードできる最大バイト数を指定します。正の数を指定するか、またはパケットのすべての QP エンコード済みデータを復号化する場合は 0 を指定します。QP エンコード データを無視するには、-1 を指定します。

このオプションが有効である場合、ルール 141:5 を有効にすると、デコードの失敗時にイベントを生成し、インライン展開では、違反パケットをドロップします。することができます（エンコードが誤っている場合やデータが破損している場合などにデコードが失敗することがあります）。

Unix-to-Unix（UU）のデコーディングの深さ（Unix-to-Unix Decoding Depth）

各 Unix-to-Unix エンコード（UU エンコード）電子メール添付ファイルから抽出してデコードできる最大バイト数を指定します。パケットのすべてのUUエンコードデータをデコードするには、正値を指定するか、0 を指定できます。UU エンコード データを無視するには、-1 を指定します。

このオプションが有効である場合、ルール 141:7 を有効にして、デコードの失敗時にイベントを生成し、インライン展開では、違反パケットをドロップします。 することができます。デコードは、エンコードが誤っている場合やデータが破損している場合などに失敗する可能性があります。

関連トピック

file_data キーワード （2266 ページ）

IMAP プリプロセッサの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Intrusion Admin

ステップ 1 **[Policies]** > **[Access Control]**、次に **[Network Analysis Policy]**または**[Policies]** > **[Access Control]** > **[Intrusion]**、次に **[Network Analysis Policy]**を選択します。

（注） カスタムユーザ ロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

ステップ 2 編集するポリシーの横にある編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 ナビゲーション パネルで [設定（Settings）] をクリックします。

ステップ 4 [アプリケーション層プリプロセッサ（Application Layer Preprocessors）] の下の [IMAP の構成（IMAP Configuration）] が無効になっている場合は、[有効化（Enabled）] をクリックします。

ステップ 5 [IMAP の構成（IMAP Configuration）] の横にある編集アイコン（）をクリックします。

ステップ 6 IMAP プリプロセッサ オプション （2361 ページ）で説明されている設定を変更します。

ステップ 7 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後にキャッシュされた変更は破棄されます。

次のタスク

- 侵入イベントを有効にする場合は、IMAP プリプロセッサ ルール（GID 141）を有効にします。侵入ルール状態の設定 （2093 ページ）を参照してください。
- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

関連トピック

侵入ポリシーおよびネットワーク分析ポリシーのレイヤ （2045 ページ）
競合と変更：ネットワーク分析および侵入ポリシー （2041 ページ）

その他の IMAP プリプロセッサ ルール

次の表に示すIMAPプリプロセッサルールは、特定の設定オプションに関連付けられていません。他のIMAPプリプロセッサルールの場合と同様に、これらのルールでイベントを生成し、インライン展開では、違反パケットをドロップします。するには、ルールを有効にする必要があります。

表 *241 :* その他の *IMAP* プリプロセッサ ルール

プリプロセッサ ルール GID:SID	説明
141:1	プリプロセッサが RFC 3501 に定義されていないクライアント コマンドを検出すると、イベントが生成されます。
141:2	プリプロセッサが RFC 3501 に定義されていないサーバ応答を検出すると、イベントが生成されます。
141:3	プリプロセッサが使用しているメモリの量が、システムでの最大許容量に達している場合に、イベントが生成されます。この時点で、プリプロセッサはメモリが使用可能になるまでデコードを停止します。

POP プリプロセッサ

Post Office Protocol（POP）は、リモート POP メール サーバから電子メールを取得するときに使用されます。POPプリプロセッサはサーバ/クライアントPOP3トラフィックを検査し、関連するプリプロセッサルールが有効である場合は異常なトラフィックがあるとイベントを生成します。プリプロセッサは、クライアント/サーバPOP3トラフィックで電子メール添付ファイルを抽出してデコードし、添付ファイル データをルール エンジンに送信することもできます。添付ファイル データを指し示すには、侵入ルールで `file_data` キーワードを使用します。

抽出とデコードでは、複数の添付ファイル（存在する場合）や、複数パケットにまたがる大きな添付ファイルなども処理されます。

POP プリプロセッサ オプション

MIME 電子メール添付ファイルのデコードが不要な場合のデコードまたは抽出では、複数の添付ファイル（存在する場合）および複数パケットにまたがる大きな添付ファイルが処理されることに注意してください。

[Base64 Decoding Depth]、[7-Bit/8-Bit/Binary Decoding Depth]、[Quoted-Printable Decoding Depth]、または [Unix-to-Unix Decoding Depth] オプションの値が以下のポリシーで異なる場合は、最も大きい値が使用されます。

- デフォルトのネットワーク分析ポリシー
- 同じアクセス コントロール ポリシーのネットワーク分析ルールによって呼び出される、他のカスタム ネットワーク分析ポリシー

以下の説明でプリプロセッサ ルールが言及されていない場合、オプションにはプリプロセッサ ルールが関連付けられていません。

Ports

POP トラフィックを検査するポートを指定します。0 ～ 65535 の整数を指定できます。ポート番号が複数ある場合は、カンマで区切ります。

Base64 デコーディングの深さ（Base64 Decoding Depth）

各 Base64 エンコード MIME 電子メール添付ファイルから抽出してデコードできる最大バイト数を指定します。正の数を指定するか、またはすべての Base64 データをデコードする場合は 0 を指定します。Base64 データを無視するには、-1 を指定します。

4 で割り切れない正の値は、次に大きい 4 の倍数に切り上げられることに注意してください。ただし 65533、65534、および 65535 は 65532 に切り下げられます。

このオプションが有効である場合、ルール 142:4 を有効にして、デコードの失敗時にイベントを生成し、インライン展開では、違反パケットをドロップします。 することができます。デコードは、エンコードが誤っている場合やデータが破損している場合などに失敗する可能性があります。

7 ビット/8 ビット/バイナリのデコーディングの深さ（7-Bit/8-Bit/Binary Decoding Depth）

デコードを必要としない各 MIME 電子メール添付ファイルから抽出するデータの最大バイト数を指定します。これらの添付ファイル タイプには、7 ビット、8 ビット、バイナリ、およびさまざまなマルチパート コンテンツ タイプ（プレーンテキスト、jpeg イメージ、mp3 ファイルなど）があります。正値またはパケット内のすべてのデータを抽出するには 0 を指定できます。非デコード データを無視するには、-1 を指定します。

このオプションが有効であれば、抽出が失敗したときにルール 142:6 を有効にしてイベントを生成し、インライン展開では、違反パケットをドロップします。 できます。抽出は、たとえば、データの破損により失敗することがあります。

Quoted-Printable（QP）のデコーディングの深さ（Quoted-Printable Decoding Depth）

各 quoted-printable（QP）エンコード MIME 電子メール添付ファイルから抽出してデコードできる最大バイト数を指定します。正の数を指定するか、またはパケットのすべての QP エンコード済みデータを復号化する場合は 0 を指定します。QP エンコード データを無視するには、-1 を指定します。

このオプションが有効である場合、ルール 142:5 を有効にして、デコードの失敗時にイベントを生成し、インライン展開では、違反パケットをドロップします。 することができます。デコードは、エンコードが誤っている場合やデータが破損している場合などに失敗する可能性があります。

Unix-to-Unix（UU）のデコーディングの深さ（Unix-to-Unix Decoding Depth）

各 Unix-to-Unix エンコード（UU エンコード）電子メール添付ファイルから抽出してデコードできる最大バイト数を指定します。パケットのすべてのUUエンコードデータをデコードするには、正値を指定するか、0 を指定できます。UU エンコード データを無視するには、-1 を指定します。

このオプションが有効である場合、ルール 142:7 を有効にして、デコードの失敗時にイベントを生成し、インライン展開では、違反パケットをドロップします。 することができます。デコードは、エンコードが誤っている場合やデータが破損している場合などに失敗する可能性があります。

関連トピック

レイヤの管理 （2053 ページ）
競合と変更：ネットワーク分析および侵入ポリシー （2041 ページ）
file_data キーワード （2266 ページ）

POP プリプロセッサの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Intrusion Admin

ステップ 1 **[Policies]** > **[Access Control]**、次に **[Network Analysis Policy]**または**[Policies]** > **[Access Control]** > **[Intrusion]**、次に **[Network Analysis Policy]**を選択します。

（注） カスタム ユーザ ロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

ステップ 2 編集するポリシーの横にある編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 ナビゲーション パネルで [設定（Settings）] をクリックします。

ステップ 4 [アプリケーション層プリプロセッサ（Application Layer Preprocessors）] の下の [POP の構成（POP Configuration）] が無効になっている場合は、[有効化（Enabled）] をクリックします。

ステップ 5 [POP の構成（POP Configuration）] の横にある編集アイコン（  ）をクリックします。

ステップ 6 POP プリプロセッサ オプション （2365 ページ）で説明されている設定を変更します。

ステップ 7 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後にキャッシュされた変更は破棄されます。

次のタスク

- 侵入イベントを有効にする場合は、POP プリプロセッサ ルール（GID 142）を有効にします。詳細については、「侵入ルール状態の設定 （2093 ページ）」を参照してください。
- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

関連トピック

レイヤの管理 （2053 ページ）
競合と変更：ネットワーク分析および侵入ポリシー （2041 ページ）

その他の POP プリプロセッサ ルール

次の表に示す POP プリプロセッサ ルールは、特定の設定オプションに関連付けられていません。その他の POP プリプロセッサ ルールと同様に、これらのルールによってイベントを生成し、インライン展開では、違反パケットをドロップします。する場合は、これらのルールを有効にする必要があります。

表 *242*：その他の *POP* プリプロセッサ ルール

プリプロセッサ ルール GID:SID	説明
142:1	プリプロセッサが RFC 1939 に定義されていないクライアント コマンドを検出すると、イベントが生成されます。
142:2	プリプロセッサが RFC 1939 に定義されていないサーバ応答を検出すると、イベントが生成されます。
142:3	プリプロセッサが使用しているメモリの量が、システムでの最大許容量に達している場合に、イベントが生成されます。この時点で、プリプロセッサはメモリが使用可能になるまでデコードを停止します。

SMTP プリプロセッサ

SMTP プリプロセッサはルール エンジンに対し、SMTP コマンドを正規化するように指示します。このプリプロセッサは、クライアントからサーバへのトラフィック内の電子メールの添付ファイルを抽出して復号化（デコード）することもできます。またソフトウェアのバージョンによっては、SMTP トラフィックによりトリガーされた侵入イベントの表示時にコンテキストを提供するために、電子メールのファイル名、アドレス、およびヘッダー データも抽出します。

SMTP プリプロセッサのオプション

正規化を有効または無効にし、SMTP デコーダが検出する異常トラフィックのタイプを制御するオプションを設定できます。

MIME 電子メール添付ファイルのデコードが不要な場合のデコードまたは抽出では、複数の添付ファイル（存在する場合）および複数パケットにまたがる大きな添付ファイルが処理されることに注意してください。

[Base64 Decoding Depth]、[7-Bit/8-Bit/Binary Decoding Depth]、[Quoted-Printable Decoding Depth]、または [Unix-to-Unix Decoding Depth] オプションの値が以下のポリシーで異なる場合は、最も大きい値が使用されます。

- デフォルトのネットワーク分析ポリシー
- 同じアクセス コントロール ポリシーのネットワーク分析ルールによって呼び出される、他のカスタム ネットワーク分析ポリシー

以下の説明でプリプロセッサ ルールが言及されていない場合、オプションにはプリプロセッサ ルールが関連付けられていません。

Ports

SMTP トラフィックを正規化するポートを指定します。0 以上の値を指定できます。複数のポートを指定する場合は、カンマで区切ります。

ステートフル インスペクション（Stateful Inspection）

選択されている場合、SMTP デコーダは状態を保存し、各パケットのセッション コンテキストを提供し、再構成されたセッションだけを検査します。選択されていない場合、セッション コンテキストなしで個々のパケットを分析します。

Normalize

[すべて（All）] に設定すると、すべてのコマンドが正規化されます。コマンドの後に複数のスペース文字があるかどうかを確認します。

[なし（None）] に設定すると、コマンドは正規化されません。

[Cmds] に設定すると、[カスタム コマンド（Custom Commands）] にリストされているコマンドが正規化されます。

カスタム コマンド（Custom Commands）

[正規化（Normalize）] が [Cmds] に設定されている場合に、リストされているコマンドが正規化されます。

正規化する必要があるコマンドをテキスト ボックスに指定します。コマンドの後に複数のスペース文字があるかどうかを確認します。

スペース文字（ASCII 0x20）とタブ文字（ASCII 0x09）は、正規化の ためにスペース文字としてカウントされます。

Ignore Data

メール データを処理せず、MIME メール 見出し データだけを処理します。

Ignore TLS Data

Transport Layer Security プロトコルで暗号化されたデータを処理しません。

No Alerts

関連するプリプロセッサ ルールが有効である場合に、侵入イベントを無効にします。

Detect Unknown Commands

SMTP トラフィックで不明なコマンドを検出します。

このオプションに関するイベントを生成し、インライン展開では、違反パケットをドロップします。 を行うには、ルール 124:5 を有効にできます。

コマンドラインの最大長（Max Command Line Len）

SMTP コマンドラインがこの値より長い場合にそのことを検出します。コマンドラインの長さを検出しない場合は、0 を指定します。

RFC 2821（Network Working Group による Simple Mail Transfer Protocol 仕様）では、コマンドラインの最大長として 512 が推奨されています。

このオプションに関するイベントを生成し、インライン展開では、違反パケットをドロップします。 を行うには、ルール 124:1 を有効にできます。

ヘッダー行の最大長（Max Header Line Len）

SMTP データ 見出し行がこの値より長い場合にそのことを検出します。データ ヘッダー行の長さを検出しない場合は、0 を指定します。

このオプションに関してイベントを生成し、インライン展開では、違反パケットをドロップします。 を行うには、ルール 124:2 および 124:7 を有効にします。

応答行の最大長（Max Response Line Len）

SMTP応答行がこの値より長い場合にそのことを検出します。応答行の長さを検出しない場合は、0 を指定します。

RFC 2821 では、応答行の最大長として 512 が推奨されています。

ルール 124:3 を有効にすると、このオプションに関して、および [代替のコマンドラインの最大長（Alt Max Command Line Len）] オプション（有効になっている場合）に関して イベントを生成し、インライン展開では、違反パケットをドロップします。 を行うことができます。

代替のコマンドラインの最大長（Alt Max Command Line Len）

指定のコマンドのSMTPコマンドラインがこの値より長い場合にそのことを検出します。指定したコマンドのコマンドライン長を検出しない場合は、0 を指定します。多数のコマンドに対して、さまざまなデフォルト ライン長が設定されています。

この設定は、指定されたコマンドの [コマンドラインの最大長（Max Command Line Len）] の設定をオーバーライドします。

ルール124:3を有効にすると、このオプションに関して、および[応答行の最大長（Max Response Line Len）] オプション（有効になっている場合）に関して イベントを生成し、インライン展開では、違反パケットをドロップします。 を行うことができます。

無効なコマンド（Invalid Commands）

これらのコマンドがクライアント側から送信された場合にそのことを検出します。

ルール 124:6 を有効にすると、このオプションに関して、および [無効なコマンド（Invalid Commands）] に関して イベントを生成し、インライン展開では、違反パケットをドロップします。 を行うことができます。

有効なコマンド（Valid Commands）

このリストのコマンドを許可します。

このリストが空の場合でも、プリプロセッサにより許可される有効なコマンドは、ATRN AUTH BDAT DATA DEBUG EHLO EMAL ESAM ESND ESOM ETRN EVFY EXPN HELO HELP IDENT MAIL NOOP ONEX QUEU QUIT RCPT RSET SAML SEND SIZE SOML STARTTLS TICK TIME TURN TURNME VERB VRFY XADR XAUTH XCIR XEXCH50 X-EXPS XGEN XLICENSE X-LINK2STATE XQUE XSTA XTRN XUSR です。

（注） RCPT TO および MAIL FROM は SMTP コマンドです。プリプロセッサ設定では、コマンド名 RCPT と MAIL がそれぞれ使用されます。プリプロセッサはコード内で RCPT および MAIL を正しいコマンド名にマッピングします。

ルール 124:4 を有効にすると、このオプションに関して、および [無効なコマンド（Invalid Commands）] オプション（設定済みの場合）に関して イベントを生成し、インライン展開では、違反パケットをドロップします。 を行うことができます。

データ コマンド（Data Commands）

RFC 5321 に基づく SMTP DATA コマンドによるデータの送信と同じ方法でデータ送信を開始するコマンドを指定します。複数のコマンドはスペースで区切ります。

Binary Data Commands

RFC 3030 に基づく BDATA コマンドによるデータの送信と類似の方法でデータ送信を開始するコマンドを指定します。複数のコマンドはスペースで区切ります。

Authentication Commands

クライアントおよびサーバ間で認証交換を開始するコマンドを指定します。複数のコマンドはスペースで区切ります。

Detect xlink2state

X-Link2State Microsoft Exchange バッファ データ オーバーフロー攻撃の一部であるパケットを検出します。インライン展開では、システムはこれらのパケットをドロップすることもできます。

このオプションに関するイベントを生成し、インライン展開では、違反パケットをドロップします。 を行うには、ルール 124:8 を有効にできます。

Base64 デコーディングの深さ（Base64 Decoding Depth）

[データを無視（Ignore Data）] が無効である場合、各 Base64 エンコード MIME 電子メール添付ファイルから抽出してデコードする最大バイト数を指定します。正の値から指定するか0を指定して、すべての Base64 データをデコードします。Base64 データを無視するには、-1 を指定します。[Ignore Data] が選択されている場合、プリプロセッサはデータをデコードしません。

4 で割り切れない正の値は、次に大きい 4 の倍数に切り上げられることに注意してください。ただし 65533、65534、および 65535 は 65532 に切り下げられます。

このオプションが有効である場合、ルール 124:10 を有効にすると、デコードの失敗時に イベントを生成し、インライン展開では、違反パケットをドロップします。 を行うことができます（エンコードが誤っている場合やデータが破損している場合などにデコードが失敗することがあります）。

このオプションは、廃止されたオプション [MIME デコーディングの有効化（Enable MIME Decoding）] および [MIME デコーディングの最大の深さ（Maximum MIME Decoding Depth）] の代わりに使用されます。廃止されたこれらのオプションは、既存の侵入ポリシーでは後方互換性を維持する目的で引き続きサポートされています。

7-Bit/8-Bit/Binary Decoding Depth

[Ignore Data] が無効である場合、デコードを必要としない各 MIME 電子メール添付ファイルから抽出する最大バイト数を指定します。これらの添付ファイル タイプには、7 ビット、8 ビット、バイナリ、およびさまざまなマルチパート コンテンツ タイプ（プレーンテキスト、jpeg イメージ、mp3 ファイルなど）があります。正値またはパケット内のすべてのデータを抽出す

るには 0 を指定できます。非デコード データを無視するには、-1 を指定します。[Ignore Data] が選択されている場合、プリプロセッサはデータを抽出しません。

Quoted-Printable Decoding Depth

[Ignore Data] が無効である場合、各 quoted-printable（QP）エンコード MIME 電子メール添付ファイルから抽出してデコードする最大バイト数を指定します。

1 ～ 65535 バイトを指定するか、または、パケットのすべての QP エンコード データをデコードする場合は 0 を指定します。QP エンコードデータを無視するには、-1 を指定します。[データを無視（Ignore Data）] が選択されている場合、プリプロセッサはデータをデコードしません。

このオプションが有効である場合、ルール 124:11 を有効にすると、デコードの失敗時に イベントを生成し、インライン展開では、違反パケットをドロップします。 することができます（エンコードが誤っている場合やデータが破損している場合などにデコードが失敗することがあります）。

Unix-to-Unix（UU）のデコーディングの深さ（Unix-to-Unix Decoding Depth）

[Ignore Data] が無効である場合、各 Unix-to-Unix（UU エンコード）電子メール添付ファイルから抽出してデコードする最大バイト数を指定します。1 ～ 65535 バイトを指定するか、または、パケットのすべての UU エンコード データをデコードする場合は 0 を指定します。UU エンコード データを無視するには、-1 を指定します。[データを無視（Ignore Data）] が選択されている場合、プリプロセッサはデータをデコードしません。

このオプションが有効である場合、ルール 124:13 を有効にすると、デコードの失敗時に イベントを生成し、インライン展開では、違反パケットをドロップします。 することができます（エンコードが誤っている場合やデータが破損している場合などにデコードが失敗することがあります）。

MIME 添付ファイル名のログ（Log MIME Attachment Names）

MIME Content-Disposition 見出しからの MIME 添付ファイル名の抽出を有効にし、セッションで生成されるすべての侵入イベントをこのファイル名に関連付けます。複数ファイル名がサポートされています。

このオプションが有効である場合、侵入イベントのテーブル ビューの [電子メール添付（Email Attachment）] 列に、イベントに関連付けられているファイル名が表示されます。

受信者アドレスのログ（Log To Addresses）

SMTP RCPT TO コマンドからの受信者の電子メール アドレスの抽出を有効にし、セッションで生成されるすべての侵入イベントにこの受信者アドレスに関連付けます。複数の受信者がサポートされます。

このオプションが有効である場合、侵入イベントのテーブル ビューの [電子メール受信者（Email Recipient）] 列に、イベントに関連付けられている受信者が表示されます。

送信者アドレスのログ（Log From Addresses）

SMTP MAIL FROM コマンドからの送信者の電子メール アドレスの抽出を有効にし、セッションで生成されるすべての侵入イベントにこの送信者アドレスを関連付けます。複数の送信者アドレスがサポートされます。

このオプションが有効である場合、侵入イベントのテーブル ビューの[電子メール送信者（Email Sender）] 列に、イベントに関連付けられている送信者が表示されます。

ヘッダーのログ（Log Headers）

電子メール 見出しの抽出を有効にします。抽出されるバイト数は、[ヘッダーのログの深さ（Header Log Depth）] に指定されている値によって決まります。

キーワード `content` または `protected_content` を使用して、電子メール ヘッダー データをパターンとして使用する侵入ルールを作成できます。侵入イベント パケット ビューに、抽出された電子メール ヘッダーが表示されます。

ヘッダーのログの深さ（Header Log Depth）

[Log Headers] が有効である場合、抽出する見出しのバイト数を指定します。0 ～ 20480 バイトを指定できます。値 0 を指定すると、[ヘッダーのログ（Log Headers）] が無効になります。

関連トピック

基本コンテンツおよび protected_content キーワードの引数 （2166 ページ）

SMTP デコードの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Intrusion Admin

マルチドメイン展開では、編集できる現在のドメインで作成されたポリシーが表示されます。また、編集できない先祖ドメインで作成されたポリシーも表示されます。下位のドメインで作成されたポリシーを表示および編集するには、そのドメインに切り替えます。

ステップ 1 **[Policies]** > **[Access Control]**、次に **[Network Analysis Policy]**または**[Policies]** > **[Access Control]** > **[Intrusion]**、次に **[Network Analysis Policy]**を選択します。

（注） カスタム ユーザ ロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

ステップ 2 編集するポリシーの横にある編集アイコン（  ）をクリックします。

代わりに表示アイコン（  ）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 ナビゲーション ウィンドウで [設定（Settings）] をクリックします。

ステップ 4 [アプリケーション層プリプロセッサ（Application Layer Preprocessors）] の下の [SMTP の設定（SMTP Configuration）] が無効になっている場合は、[有効化（Enabled）] をクリックします。

ステップ 5 [SMTP の設定（SMTP Configuration）] の横にある編集アイコン（  ）をクリックします。

ステップ 6 SMTP プリプロセッサのオプション （2368 ページ）の説明に従ってオプションを変更します。

ステップ 7 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後にキャッシュされた変更は破棄されます。

次のタスク

- イベントを生成し、インライン展開では、違反パケットをドロップします。 を行うには、SMTP プリプロセッサ ルール（GID 124）を有効にします。詳細については、「侵入ルール状態の設定 （2093 ページ）」を参照してください。
- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

関連トピック

レイヤの管理 （2053 ページ）
競合と変更：ネットワーク分析および侵入ポリシー （2041 ページ）

SSH プリプロセッサ

SSH プリプロセッサでは、次の攻撃を検出します。

- チャレンジレスポンス バッファ オーバーフロー エクスプロイト
- CRC-32 エクスプロイト
- SecureCRT SSH クライアント バッファ オーバーフロー エクスプロイト
- プロトコル不一致
- 不正な SSH メッセージの方向
- バージョン 1 または 2 以外のすべてのバージョン文字列

チャレンジレスポンス バッファ オーバーフロー攻撃と CRC--32 攻撃はいずれもキー交換の後に発生するので、暗号化されています。いずれの攻撃でも、20 KB を超える普通よりも大きなペイロードが認証チャレンジ直後にサーバに送信されます。CRC-32 攻撃の対象となるのは SSH バージョン 1 のみであり、チャレンジレスポンス バッファ オーバーフロー エクスプロイトの対象となるのは SSH バージョン 2 のみです。バージョン文字列は、セッションの開始時に読み取られます。バージョン文字列の違いを除き、この両方の攻撃は同様に扱われます。

SecureCRT SSH エクスプロイトとプロトコル不一致攻撃は、鍵交換前に接続をセキュリティで保護しようとするときに発生します。SecureCRT エクスプロイトでは、非常に長いプロトコル ID 文字列がクライアントに送信され、これが原因でバッファ オーバーフローが発生します。プロトコル不一致は、非 SSH クライアント アプリケーションがセキュア SSH サーバに接続しようとした場合、またはサーバとクライアントのバージョン番号が一致しない場合に発生します。

SSH プリプロセッサは、指定のポートまたはポートのリストでトラフィックを検査するか、または SSH トラフィックを自動的に検出するように設定できます。指定バイト数に達するまでに指定数の暗号化パケットが渡されたか、指定パケット数に達するまでにバイト数が指定最大バイト数を超えるまで、SSH トラフィックの検査が続行されます。最大バイト数を超えた場合は、CRC--32（SSH バージョン 1）攻撃またはチャレンジレスポンス バッファ オーバーフロー（SSH バージョン 2）攻撃が発生したとみなされます。プリプロセッサは、設定していない場合でもバージョン 1 または 2 以外のバージョン文字列を検出することに注意してください。

SSH プリプロセッサでは、ブルートフォース攻撃が処理されないことにも注意してください。

SSH プリプロセッサのオプション

次のいずれかが発生すると、プリプロセッサはセッションのトラフィックの検査を停止します。

- この数の暗号化パケットで、サーバとクライアント間で有効な交換が行われた場合。接続は続行します。
- 検査対象の暗号化パケットの数に達する前に、[Number of Bytes Sent Without Server Response] に達した場合。この場合、攻撃があったものと想定されます。

[Number of Encrypted Packets to Inspect] に達するまでの有効な各サーバ応答により、[Number of Bytes Sent Without Server Response] がリセットされ、パケット カウントが続行します。

次に示す SSH のプリプロセッサの設定例で説明します。

- [Server Ports]：22
- [Autodetect Ports]：off
- [Maximum Length of Protocol Version String]：80
- [Number of Encrypted Packets to Inspect]：25
- [Number of Bytes Sent Without Server Response]：19,600
- 検出オプションはすべて有効です。

この例では、プリプロセッサはポート 22 のトラフィックだけを検査します。つまり自動検出が無効であるため、指定のポートでのみ検査をします。

また、次のいずれかが発生すると、この例のプリプロセッサはトラフィックの検査を停止します。

- クライアントが 25 個の暗号化パケットを送信したが、すべてのパケットのデータ合計が 19,600 バイト以下であった。攻撃はなかったと想定されます。
- クライアントが、25 個の暗号化パケットで 19,600 バイトを超えるデータを送信した。この場合、この例のセッションは SSH バージョン 2 セッションであるため、プリプロセッサはこの攻撃がチャレンジレスポンスバッファ オーバーフロー攻撃であるとみなします。

この例のプリプロセッサは、トラフィックの処理時に以下の状況が発生しているかどうかも検出します。

- 80 バイトより長いバージョン文字列によりトリガーとして使用されるサーバ オーバーフロー（これは SecureCRT エクスプロイトを示します）
- プロトコルの不一致
- 誤った方向に流れるパケット

最後に、プリプロセッサは、バージョン 1 または 2 以外のすべてのバージョン文字列を自動的に検出します。

以下の説明でプリプロセッサ ルールが言及されていない場合、オプションにはプリプロセッサ ルールが関連付けられていません。

Server Ports

SSH プリプロセッサがトラフィックを検査する必要があるポートを指定します。

1 つのポートか、複数ポートをカンマで区切ったリストを設定できます。

Autodetect Ports

SSH トラフィックを自動的に検出するようにプリプロセッサを設定します。

このオプションが選択されている場合、プリプロセッサはすべてのトラフィックで SSH バージョン番号を検査します。クライアント パケットにもサーバ パケットにもバージョン番号が含まれていない場合は、処理が停止します。無効である場合、プリプロセッサは [Server Ports] オプションで指定されているトラフィックだけを検査します。

検査する暗号化パケットの最大数（Number of Encrypted Packets to Inspect）

セッションあたりのストリーム再構成された検査対象の暗号化パケットの数を指定します。

このオプションをゼロに設定すると、すべてのトラフィックの通過が許可されます。

検査対象の暗号化パケットの数を減らすと、一部の攻撃が検出されなくなることがあります。検査対象の暗号化パケットの数を増やすと、パフォーマンスに悪影響を及ぼす可能性があります。

Number of Bytes Sent Without Server Response

SSHクライアントが、応答なしでサーバに送信できる最大バイト数を指定します。この最大バイト数を超えると、チャレンジレスポンス バッファ オーバーフロー攻撃または CRC-32 攻撃が想定されます。

プリプロセッサがチャレンジレスポンス バッファ オーバーフローまたは CRC-32 エクスプロイトを誤検出する場合は、このオプションの値を増やしてください。

Maximum Length of Protocol Version String

サーバのバージョン文字列の最大許容バイト数を指定します。この値を超えると、SecureCRT エクスプロイトとみなされます。

Detect Challenge-Response Buffer Overflow Attack

チャレンジレスポンス バッファ オーバーフロー エクスプロイトの検出を有効または無効にします。

このオプションに関するイベントを生成し、インライン展開では、違反パケットをドロップします。 を行うには、ルール 128:1 を有効にできます。SFTP セッションはルール 128:1 をトリガーする場合があることに注意してください。

SSH1 CRC-32 攻撃の検出（Detect SSH1 CRC-32 Attack）

CRC-32 エクスプロイトの検出を有効または無効にします。

このオプションに関するイベントを生成し、インライン展開では、違反パケットをドロップします。 を行うには、ルール 128:2 を有効にできます。

サーバ オーバーフローの検出（Detect Server Overflow）

SecureCRT SSH クライアント バッファ オーバーフロー エクスプロイトの検出を有効または無効にします。

このオプションにイベントを生成し、インライン展開では、違反パケットをドロップします。するには、ルール 128:3 を有効にします。

プロトコル不一致の検出（Detect Protocol Mismatch）

プロトコル不一致の検出を有効または無効にします。

このオプションに関するイベントを生成し、インライン展開では、違反パケットをドロップします。 を行うには、ルール 128:4 を有効にできます。

正しくないメッセージ方向の検出（Detect Bad Message Direction）

トラフィックのフロー方向が正しくない場合（つまり、推定されるサーバがクライアント トラフィックを生成したり、クライアントがサーバ トラフィックを生成したりした場合）の検出を有効または無効にします。

このオプションに関するイベントを生成し、インライン展開では、違反パケットをドロップします。 を行うには、ルール 128:5 を有効にできます。

特定のペイロードに正しくないペイロード サイズの検出（Detect Payload Size Incorrect for the Given Payload）

SSH パケットに指定された長さが IP ヘッダーに指定されている合計長と矛盾する場合や、メッセージが切り捨てられる場合、つまり完全な SSH ヘッダーを形成できる十分なデータがない場合などの、誤ったペイロード サイズのパケットの検出を有効または無効にします。

このオプションに関するイベントを生成し、インライン展開では、違反パケットをドロップします。 を行うには、ルール 128:6 を有効にできます。

正しくないバージョン ストリングの検出（Detect Bad Version String）

有効である場合、プリプロセッサは、設定していない場合でもバージョン 1 または 2 以外のバージョン文字列を検出することに注意してください。

このオプションに関するイベントを生成し、インライン展開では、違反パケットをドロップします。 を行うには、ルール 128:7 を有効にできます。

SSH プリプロセッサの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Intrusion Admin

ステップ 1 **[Policies]** > **[Access Control]**、次に **[Network Analysis Policy]** または **[Policies]** > **[Access Control]** > **[Intrusion]**、次に **[Network Analysis Policy]** を選択します。

（注） カスタム ユーザ ロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

ステップ 2 編集するポリシーの横にある編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 ナビゲーション パネルで [設定（Settings）] をクリックします。

ステップ 4 [アプリケーション層プリプロセッサ（Application Layer Preprocessors）] の下の [SSH の構成（SSH Configuration）] が無効になっている場合は、[有効化（Enabled）] をクリックします。

ステップ 5 [SSH の構成（SSH Configuration）] の横にある編集アイコン（）をクリックします。

ステップ 6 SSH プリプロセッサのオプション （2375 ページ）の説明に従ってオプションを変更します。

ステップ 7 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後にキャッシュされた変更は破棄されます。

次のタスク

- 侵入イベントを有効にする場合は、SSH プリプロセッサ ルール（GID 128）を有効にします。詳細については、「侵入ルール状態の設定 （2093 ページ）」を参照してください。
- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

関連トピック

レイヤの管理 （2053 ページ）
競合と変更：ネットワーク分析および侵入ポリシー （2041 ページ）

SSL プリプロセッサ

SSL プリプロセッサでは、SSL インスペクション（検査）を設定できます。SSL インスペクションでは、暗号化トラフィックのブロック、暗号化トラフィックの復号化、またはアクセスコントロール（アクセス制御）によるトラフィックの検査を実行します。SSL インスペクションが設定されているかどうかに関係なく、SSL プリプロセッサでは、トラフィックで検出された SSL ハンドシェイク メッセージも分析し、セッションを暗号化するタイミングを決定します。暗号化トラフィックを識別することにより、システムは暗号化ペイロードの侵入およびファイルインスペクションを停止できます。これによって、誤検出が減少し、パフォーマンスが向上します。

SSL プリプロセッサは、暗号化トラフィックを検査して Heartbleed バグを悪用する試みを検出し、そのような悪用の検出時にイベントを生成することもできます。

セッションが暗号化されると、侵入およびマルウェアに対するトラフィックの検査を一時停止できます。SSL インスペクションを設定した場合、SSL プリプロセッサでは、ユーザがアクセスコントロールによってブロック、復号化、または検査を行える暗号化トラフィックも識別します。

SSL プリプロセッサを使用して暗号化トラフィックを復号化するために、ライセンスは必要ありません。マルウェアおよび侵入に対する暗号化ペイロードのインスペクションの停止、Heartbleed バグの悪用の検出など、他のすべての SSL プリプロセッサ機能には保護ライセンスが必要です。

SSL 前処理の仕組み

SSL インスペクションを設定すると、SSL プリプロセッサは暗号化データに対する侵入およびファイル インスペクションを停止して、SSL ポリシーにより暗号化トラフィックを検査しま

す。これにより誤検出を排除できます。SSL プリプロセッサは、SSL ハンドシェイクを検査するときに状態情報を保持し、そのセッションの状態と SSL バージョンの両方を追跡します。セッションの状態が暗号化されていることをプリプロセッサが検出すると、そのセッションのトラフィックは暗号化されているものとしてシステムによりマークされます。暗号化が確定した場合に暗号化セッションにおけるすべてのパケット処理を停止し、Heartbleed のバグを悪用する試みが検出された場合にイベントを生成するように、システムを設定できます。

パケットごとに、IP ヘッダー、TCP ヘッダー、および TCP ペイロードがトラフィックに含まれており、このトラフィックが SSL 前処理用に指定されているポートで発生することが SSL プリプロセッサにより確認されます。次に示す状況では、対象トラフィックについて、トラフィックが暗号化されているかどうかが判別されます。

- システムがセッションのすべてのパケットを監視し、[サーバ側のデータを信頼する（Server side data is trusted）] が有効にされておらず、サーバとクライアントの両方からの完了メッセージ、および Application レコードが存在するが Alert レコードがない各側からの 1 つ以上のパケットが、セッションに含まれている。
- システムがトラフィックの一部を検出せず、[サーバ側のデータを信頼する（Server side data is trusted）] が有効にされておらず、Alert レコードによる応答がない Application レコードが存在する各側からの 1 つ以上のパケットが、セッションに含まれている。
- システムがセッションのすべてのパケットを監視し、[サーバ側のデータを信頼する（Server side data is trusted）] が有効であり、クライアントからの完了メッセージ、および Application レコードが存在するが Alert レコードがないクライアントからの 1 つ以上のパケットが、セッションに含まれている。
- システムがトラフィックの一部を検出せず、[サーバ側のデータを信頼する（Server side data is trusted）] が有効であり、Alert レコードによる応答がない Application レコードが存在するクライアントからの 1 つ以上のパケットが、セッションに含まれている。

暗号化トラフィックの処理を停止することを選択する場合、セッションが暗号化されているものとしてマークされると、そのセッションのその後のパケットは無視されます。

また、SSL ハンドシェイク時、プリプロセッサはハートビート要求と応答をモニタします。プリプロセッサは、以下を検出したときにイベントを生成します。

- ペイロード自体よりも大きいペイロード長の値を含むハートビート要求
- [Max Heartbeat Length] フィールドに格納されている値よりも大きいハートビート応答

（注） ルール内で SSL 状態またはバージョン情報を使用するには、キーワード `ssl_state` および `ssl_version` をルールに追加します。

関連トピック

SSL キーワード （2217 ページ）
TLS/SSL インスペクションの要件

SSL プリプロセッサのオプション

（注） システム付属のネットワーク分析ポリシーは、デフォルトでSSLプリプロセッサを有効にします。暗号化トラフィックがネットワークを通過することを予想している場合、シスコは、カスタム展開で SSL プリプロセッサを無効にしないことを推奨します。

SSLインスペクションを設定しないと、システムは暗号化トラフィックを復号化せずに、マルウェアと侵入について暗号化トラフィックの検査を試行します。SSLプリプロセッサを有効にすると、セッションが暗号化されたときにそのことを検出します。SSLプリプロセッサが有効にされると、ルールエンジンがこのプリプロセッサを呼び出し、SSLの状態およびバージョン情報を取得できるようになります。侵入ポリシーでキーワード `ssl_state` および `ssl_version` を使用してルールを有効にする場合は、そのポリシーでSSLプリプロセッサも有効にする必要があります。

ポート

SSLプリプロセッサは、暗号化されたセッションのトラフィックをモニタする必要があるポートを、カンマで区切って指定します。このフィールドで指定されるポートでのみ、暗号化トラフィックが検査されます。

（注） SSLプリプロセッサは、SSLモニタの対象として指定されたポートでSSL以外のトラフィックを検出すると、そのトラフィックをSSLトラフィックとしてデコードすることを試みた後、破損しているものとしてマークします。

暗号化トラフィックの検査を停止する（Stop inspecting encrypted traffic）

セッションが暗号化されているとしてマークされた後、セッションのトラフィックの検査を有効または無効にします。

暗号化されたセッションの検査を無効化しリアセンブルするには、このオプションを有効にします。SSLプリプロセッサによりセッションの状態が維持されるため、セッションのすべてのトラフィックのインスペクションを無効にできます。このオプションが有効になっている場合は、フローが暗号化されていることを確認するためセッションのいくつかのパケットが検証され、その後でディープ インスペクションがバイパスされます。バイパスされたすべてのセッションによって **show snort statistics** コマンドの応答に示される高速転送フローのカウントが増加します。さらに、ディープインスペクションがバイパスされているため、接続イベントのイニシエータとレスポンダのバイト数は正確ではありません。これらは実際のセッションの値よりも少なくなります。これは、Snortによって検査されたパケットのみが含まれており、ディープインスペクションがバイパスされた後のパケットは含まれていないためです。この動作は接続サマリ イベントとウィジェットに表示されるすべてのトラフィックの値に有効です。

システムは、次の両方の場合に、暗号化されたセッションのトラフィックの検査のみを停止します。

- SSL の前処理が有効にされている
- このオプションが選択されている

このオプションをクリアすると、[サーバ側のデータを信頼する（Server side data is trusted）] オプションを変更できません。

サーバ側のデータを信頼する（Server side data is trusted）

[暗号化トラフィックの検査を停止する（Stop inspecting encrypted traffic）] が有効にされてあり、クライアント側のトラフィックにのみ基づいて暗号化されたトラフィックの識別を有効にすると、

ハートビートの最大長（Max Heartbeat Length）

バイト数を指定して、ハートビート バグ悪用の試みに対する SSL ハンドシェイク内のハートビート要求と応答の検査を有効にします。1 ～ 65535 の整数を指定できます。このオプションを無効にする場合は 0 を入力します。

プリプロセッサがハートビート要求を検出し、このペイロード長が実際のペイロード長より大きく、ルール 137:3 が有効にされている場合、または、ルール 137:4 が有効にされている際に、このオプションに設定された値よりハートビート応答のサイズが大きい場合は、プリプロセッサはイベントを生成し、インライン展開では、違反パケットをドロップします。。

SSL プリプロセッサの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Intrusion Admin

ステップ 1 **[Policies]** > **[Access Control]**、次に **[Network Analysis Policy]** または **[Policies]** > **[Access Control]** > **[Intrusion]**、次に **[Network Analysis Policy]** を選択します。

（注） カスタム ユーザ ロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

ステップ 2 編集するポリシーの横にある編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 ナビゲーション パネルで [設定（Settings）] をクリックします。

ステップ 4 [アプリケーション層プリプロセッサ（Application Layer Preprocessors）] の下の [SSL 設定（SSL Configuration）] が無効になっている場合は、[有効化（Enabled）] をクリックします。

ステップ 5 [SSL 設定（SSL Configuration）] の横にある編集アイコン（）をクリックします。

ステップ 6 SSL プリプロセッサのオプション （2381 ページ） に示されている任意の設定を変更します。

- [ポート（Ports）] フィールドに値を入力します。複数の値を指定する場合は、カンマで区切ります。
- [暗号化トラフィックの検査の停止（Stop inspecting encrypted traffic）] チェックボックスをオンまたはオフにします。
- [暗号化トラフィックの検査の停止（Stop inspecting encrypted traffic）] チェックボックスをオンにした場合は、[サーバ側データは信頼済み（Server side data is trusted）] チェックボックスをオンまたはオフにします。
- [最大ハートビート長（Max Heartbeat Length）] フィールドに値を入力します。

ヒント 値 0 を指定すると、このオプションが無効になります。

ステップ 7 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後にキャッシュされた変更は破棄されます。

次のタスク

- 侵入イベントを有効にする場合は、SSL プリプロセッサ ルール（GID 137）を有効にします。詳細については、「侵入ルール状態の設定 （2093 ページ）」を参照してください。
- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

関連トピック

レイヤの管理 （2053 ページ）
競合と変更：ネットワーク分析および侵入ポリシー （2041 ページ）
TLS/SSL インスペクションの要件

SSL プリプロセッサ ルール

イベントを生成し、インライン展開では、違反パケットをドロップします。するには、SSL プリプロセッサ ルール（GID 137）を有効にします。

次の表に、有効にできる SSL プリプロセッサ ルールを示します。

表 *243 : SSL* プリプロセッサ ルール

プリプロセッサ ルール GID:SID	説明
137:1	ServerHello メッセージの後の ClientHello メッセージを検出します。これは無効であり、異常な動作とみなされます。

プリプロセッサ ルール GID:SID	説明
137:2	SSL プリプロセッサ オプション [サーバ側のデータを信頼する（Server side data is trusted）] が無効な場合に、ClientHello メッセージのない ServerHello メッセージを検出します。これは無効であり、異常な動作としてみなされます。
137:3	SSL プリプロセッサ オプション [ハートビートの最大長（Max Heartbeat Length）] にゼロ以外の値が含まれている場合に、ペイロード自体よりも大きいペイロード長の値を含むハートビート要求を検出します。このようなハートビート要求は、Heartbleed バグを悪用する試みを示しています。
137:4	SSL プリプロセッサ オプション [ハートビートの最大長（Max Heartbeat Length）] で指定されているゼロ以外の値よりも大きいハートビート応答を検出します。このようなハートビート応答は、Heartbleed バグを悪用する試みを示しています。

第 93 章

SCADA プリプロセッサ

以下のトピックでは、遠隔監視制御・情報取得（SCADA）プロトコルのプリプロセッサとその設定方法について説明します。

SCADA プリプロセッサの概要

Supervisory Control and Data Acquisition（SCADA）プロトコルは、製造、水処理、配電、空港、輸送システムなどの工業プロセス、インフラストラクチャプロセス、および設備プロセスからのデータをモニタ、制御、取得します。Firepower システムは、ネットワーク分析ポリシーの一部として設定できる Modbus、Distributed Network Protocol（DNP3）、および Common Industrial Protocol（CIP）SCADA プロトコル用のプリプロセッサを提供します。

Modbus、DNP3、または CIP プリプロセッサが無効になっており、これらのプリプロセッサのいずれかを必要とする侵入ルールを有効にして展開した場合、システムはプリプロセッサを現在の設定で使用しますが、対応するネットワーク分析ポリシーの Web インターフェイスではプリプロセッサは無効になったままとなります。

Modbus プリプロセッサ

Modbus プロトコルは 1979 年に Modicon が初めて発表した、広く利用されている SCADA プロトコルです。Modbus プリプロセッサは、Modbus トラフィックの異常を検出し、ルール エンジンによる処理のために Modbus プロトコルをデコードします。ルール エンジンは Modbus キーワードを使用して特定のプロトコル フィールドにアクセスします。

1 つの構成オプションで、プリプロセッサが Modbus トラフィックを検査するポートのデフォルト設定を変更できます。

関連トピック

SCADA キーワード （2242 ページ）

Modbus プリプロセッサ ポート オプション

ポート

プリプロセッサが Modbus トラフィックを検査するポートを指定します。複数のポートを指定する場合は、カンマで区切ります。

Modbus プリプロセッサの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Intrusion Admin

ネットワークに Modbus 対応デバイスが含まれていない場合は、トラフィックに適用するネットワーク分析ポリシーでこのプリプロセッサを有効にしないでください。

マルチドメイン展開では、編集できる現在のドメインで作成されたポリシーが表示されます。また、編集できない先祖ドメインで作成されたポリシーも表示されます。下位のドメインで作成されたポリシーを表示および編集するには、そのドメインに切り替えます。

ステップ 1 **[Policies]** > **[Access Control]**、次に **[Network Analysis Policy]**または**[Policies]** > **[Access Control]** > **[Intrusion]**、次に **[Network Analysis Policy]**を選択します。

（注） カスタム ユーザ ロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

ステップ 2 編集するポリシーの横にある編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 ナビゲーション パネルで [設定（Settings）] をクリックします。

ステップ 4 [SCADA プリプロセッサ（SCADA Preprocessors）] の下の [Modbus の構成（Modbus Configuration）] が無効になっている場合は、[有効化（Enabled）] をクリックします。

ステップ 5 [Modbus の構成（Modbus Configuration）] の横にある編集アイコン（）をクリックします。

ステップ 6 [ポート（Ports）] フィールドに値を入力します。

複数の値を指定する場合は、カンマで区切ります。

ステップ 7 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後にキャッシュされた変更は破棄されます。

次のタスク

- イベントを生成し、インライン展開では、違反パケットをドロップします。 を行うには、Modbus プリプロセッサ ルール（GID 144）を有効にします。詳細については、侵入ルール状態の設定 （2093 ページ）およびModbus プリプロセッサ ルール （2387 ページ）を参照してください。
- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

関連トピック

レイヤの管理 （2053 ページ）
競合と変更：ネットワーク分析および侵入ポリシー （2041 ページ）

Modbus プリプロセッサ ルール

次の表に示す Modbus プリプロセッサ ルールによって イベントを生成し、インライン展開では、違反パケットをドロップします。 するには、これらのルールを有効にする必要があります。

表 *244 : Modbus* プリプロセッサ ルール

プリプロセッサ ルール GID:SID	説明
144:1	Modbus の見出しの長さが、Modbus 機能コードに必要な長さと一致していない場合に、イベントが生成されます。 各 Modbus 機能の要求と応答には期待される形式があります。メッセージの長さが、期待される形式と一致しない場合に、このイベントが生成されます。
144:2	Modbus プロトコル ID がゼロ以外の場合に、イベントが生成されます。プロトコル ID フィールドは、Modbus と共にその他のプロトコルを多重伝送するために使用されます。プリプロセッサはこのような他のプロトコルを処理しないため、代わりにこのイベントが生成されます。
144:3	プリプロセッサが予約済み Modbus 機能コードを検出すると、イベントが生成されます。

DNP3 プリプロセッサ

Distributed Network Protocol（DNP3）は、当初は発電所間で一貫性のある通信を実現する目的で開発された SCADA プロトコルです。DNP3 も、水処理、廃棄物処理、輸送などさまざまな産業分野で幅広く利用されるようになっています。

DNP3 プリプロセッサは、DNP3 トラフィックの異常を検出し、ルール エンジンによる処理のために DNP3 プロトコルをデコードします。ルール エンジンは、DNP3 キーワードを使用して特定のプロトコル フィールドにアクセスします。

関連トピック

DNP3 キーワード （2243 ページ）

DNP3 プリプロセッサ オプション

ポート

指定された各ポートでの DNP3 トラフィックのインスペクションを有効にします。1 つのポートを指定するか、複数のポートをカンマで区切ったリストを指定できます。

無効な CRC を記録（Log bad CRCs）

DNP3 リンク層フレームに含まれているチェックサムを検証します。無効なチェックサムを含むフレームは無視されます。

ルール 145:1 を有効にすると、無効なチェックサムが検出されたときにイベントを生成し、インライン展開では、違反パケットをドロップします。 できます。

DNP3 プリプロセッサの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Intrusion Admin

ネットワークに DNP3 対応デバイスが含まれていない場合は、トラフィックに適用するネットワーク分析ポリシーでこのプリプロセッサを有効にしないでください。

マルチドメイン展開では、編集できる現在のドメインで作成されたポリシーが表示されます。また、編集できない先祖ドメインで作成されたポリシーも表示されます。下位のドメインで作成されたポリシーを表示および編集するには、そのドメインに切り替えます。

ステップ 1 **[Policies]** > **[Access Control]**、次に **[Network Analysis Policy]**または**[Policies]** > **[Access Control]** > **[Intrusion]**、次に **[Network Analysis Policy]**を選択します。

（注） カスタムユーザロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

ステップ 2 編集するポリシーの横にある編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 ナビゲーション パネルで [設定（Settings）] をクリックします。

ステップ 4 [SCADA プリプロセッサ（SCADA Preprocessors）] の下の [DNP3 の構成（DNP3 Configuration）] が無効になっている場合は、[有効化（Enabled）] をクリックします。

ステップ 5 [DNP3 の構成（DNP3 Configuration）] の横にある編集アイコン（）をクリックします。

ステップ 6 ポートの値を入力します。

複数の値を指定する場合は、カンマで区切ります。

ステップ 7 [不良 CRC の記録（Log bad CRCs）] チェックボックスをオンまたはオフにします。

ステップ 8 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後にキャッシュされた変更は破棄されます。

次のタスク

- イベントを生成し、インライン展開では、違反パケットをドロップします。 を行うには、DNP3 プリプロセッサ ルール（GID 145）を有効にします。詳細については、侵入ルール状態の設定（2093ページ）、DNP3プリプロセッサ オプション（2388ページ）、およびDNP3 プリプロセッサ ルール （2389 ページ）を参照してください。
- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

関連トピック

レイヤの管理 （2053 ページ）
競合と変更：ネットワーク分析および侵入ポリシー （2041 ページ）

DNP3 プリプロセッサ ルール

次の表に示すDNP3プリプロセッサルールによってイベントを生成し、インライン展開では、違反パケットをドロップします。 するには、これらのルールを有効にする必要があります。

表 *245 : DNP3* プリプロセッサ ルール

プリプロセッサ ルール GID:SID	説明
145:1	[Log bad CRC] が有効である場合に、無効なチェックサムを含むリンク層フレームがプリプロセッサにより検出されると、イベントが生成されます。
145:2	無効な長さの DNP3 リンク層フレームがプリプロセッサにより検出されると、イベントが生成され、パケットがブロックされます。
145:3	再構成中に無効なシーケンス番号のトランスポート層セグメントがプリプロセッサにより検出されると、イベントが生成され、パケットがブロックされます。
145:4	完全なフラグメントを再構成する前に DNP3 再構成バッファがクリアされると、イベントが生成されます。このことは、FIR フラグを伝送するセグメントが、他のセグメントがキューに入れられた後で現れる場合に発生します。
145:5	予約済みアドレスを使用する DNP3 リンク層フレームをプリプロセッサが検出すると、イベントが生成されます。
145:6	予約済み機能コードを使用する DNP3 要求または応答をプリプロセッサが検出すると、イベントが生成されます。

CIP プリプロセッサ

Common Industrial Protocol（CIP）は、産業自動化アプリケーションをサポートするために広く使用されているアプリケーション プロトコルです。EtherNet/IP（ENIP）は、イーサネット ベースのネットワークで使用される CIP の実装です。

CIP プリプロセッサは、TCP で実行される CIP および ENIP トラフィックを検出し、それを侵入ルール エンジンに送信します。カスタム侵入ルールで CIP および ENIP のキーワードを使用すると、CIP および ENIP トラフィックで攻撃を検出できます。「CIP および ENIP のキーワード」を参照してください。さらに、アクセス コントロール ルールで CIP および ENIP アプリケーションの条件を指定することによって、トラフィックを制御できます。アプリケーション条件とフィルタの設定 （481 ページ）を参照してください。

CIP プリプロセッサのオプション

ポート

CIP および ENIP トラフィックを検査するポートを指定します。0 ～ 65535 の整数を指定できます。ポート番号が複数ある場合は、カンマで区切ります。

（注） リストするデフォルトの CIP 検出ポート 44818 およびその他のポートを、TCP ストリームのリスト [ストリームの再構成をどちらのポートでも実行する（Perform Stream Reassembly on Both Ports）]に追加する必要があります。TCP ストリームのプリプロセス オプション （2425 ページ）およびカスタム ネットワーク分析ポリシーの作成 （2297 ページ）を参照してください。

デフォルトの未接続タイムアウト（秒）

CIP 要求メッセージにプロトコル固有のタイムアウト値が含まれておらず、[Maximum number of concurrent unconnected requests per TCP connection] に達した場合は、このオプションで指定した秒数の間、システムがメッセージの時間を測定します。タイマーが満了すると、他の要求用のスペースを確保するために、メッセージが削除されます。0 ～ 360 の整数を指定できます。0 を指定すると、プロトコル固有のタイムアウト値を持たないすべてのトラフィックは、最初にタイムアウトになります。

Maximum number of concurrent unconnected requests per TCP connection

システムが接続を閉じるまで無応答にすることができる同時要求の数。1 ～ 10000 の整数を指定できます。

Maximum number of CIP connections per TCP connection

システムが TCP 接続ごとに許可する同時 CIP 接続の最大数。1 ～ 10000 の整数を指定できます。

CIP イベント

設計上、セッションごとに1回ずつ、同じアプリケーションがアプリケーションディテクタで検出されてイベント ビューアに表示されます。1 つの CIP セッションでは複数のアプリケーションを別々のパケットに含めることができ、単一の CIP パケットに複数のアプリケーションを格納できます。CIP プリプロセッサは、対応する侵入ルールに従ってすべての CIP と ENIP のトラフィックを処理します。

次の表にイベント ビューに表示される CIP の値を示します。

表 *246 : CIP* イベント フィールドの値

イベント フィールド	表示される値
アプリケーション プロトコル（Application Protocol）	CIP または ENIP
クライアント	CIP クライアントまたは ENIP クライアント
[Webアプリケーション（Web Application）]	次に示す特定のアプリケーションを検出しました。 • トラフィックを許可またはモニタするアクセス制御ルールの場合、セッションで検出された最後のアプリケーション プロトコル。 接続をログに記録するよう設定されたアクセス 制御 ルールが、指定された CIP アプリケーションのイベントを生成しないことがあります。一方、接続をログに記録するよう設定されていないアクセス コントロール ルールが、CIP アプリケーションのイベントを生成することがあります。 • トラフィックをブロックするアクセス制御ルールの場合、ブロックをトリガーしたアプリケーション プロトコル。 アクセス コントロール ルールが CIP アプリケーションのリストをブロックすると、イベント ビューアに、検出された最初のアプリケーションが表示されます。

CIP プリプロセッサ ルール

次の表に示す CIP プリプロセッサ ルールでイベントを生成するには、それらのルールを有効にする必要があります。ルールの有効化については、侵入ルール状態の設定（2093 ページ）を参照してください。

表 *247 : CIP* プリプロセッサ ルール

GID:SID	ルール メッセージ
148:1	CIP_MALFORMED
148:2	CIP_NON_CONFORMING
148:3	CIP_CONNECTION_LIMIT

GID:SID	ルール メッセージ
148:4	CIP_REQUEST_LIMIT

CIP プリプロセッサの設定のガイドライン

CIP プリプロセッサを設定する際には次の点に注意してください。

- リストするデフォルトの CIP 検出ポート 44818 およびその他の CIP **ポート**を TCP ストリームのリスト [ストリームの再構成をどちらのポートでも実行する（Perform Stream Reassembly on Both Ports）] に追加する必要があります。CIP プリプロセッサのオプション （2391 ページ）、カスタム ネットワーク分析ポリシーの作成 （2297ページ）、およびTCP ストリーム のプリプロセス オプション （2425 ページ）を参照してください。
- イベント ビューアには、CIP アプリケーションに対する特別な処理が用意されています。CIP イベント （2391 ページ）を参照してください。
- アクセス コントロール ポリシーのデフォルトのアクションとして侵入防御アクションを使用することをお勧めします。
- CIP プリプロセッサは、アクセス コントロール ポリシーのデフォルト アクション [アクセス制御：すべてのトラフィックを信頼（Access Control: Trust All Traffic）] をサポートしていません。このアクションを実行すると、侵入ルールとアクセス コントロール ルールで指定された CIP アプリケーションによりトリガーされたトラフィックがドロップされないなど、望ましくない動作が生じる可能性があるためです。
- CIP プリプロセッサは、アクセス コントロール ポリシーのデフォルト アクション [アクセス制御：すべてのトラフィックをブロック（Access Control: Block All Traffic）] をサポートしていません。このアクションを実行すると、ブロックされると想定されない CIP アプリケーションがブロックされるなど、望ましくない動作が生じる可能性があるためです。
- CIP プリプロセッサは、CIP アプリケーションのアプリケーション可視性（ネットワーク検出を含む）をサポートしていません。
- CIP および ENIP アプリケーションを検出し、それらをアクセス コントロール ルールや侵入ルールなどで使用するには、対応するカスタム ネットワーク分析ポリシーで CIP プリプロセッサを手動で有効にする必要があります。カスタム ネットワーク分析ポリシーの作成（2297ページ）、「デフォルトのネットワーク分析ポリシーの設定」、およびネットワーク分析ルールの設定 （2292 ページ）を参照してください。
- CIP のプリプロセッサ ルールおよび CIP 侵入ルールをトリガーするトラフィックをドロップするには、対応する侵入ポリシーの [インラインの場合ドロップする（Drop when Inline）] オプションが有効になっていることを確認します。「インライン展開でのドロップ動作の設定」を参照してください。
- アクセス コントロール ルールを使用して CIP または ENIP アプリケーション トラフィックをブロックするには、対応するネットワーク分析ポリシーでインライン正規化プリプロセッサおよびその [インライン モード（Inline Mode）] オプションが有効になっている（デフォルト設定）ことを確認してください。カスタム ネットワーク分析ポリシーの作成 （

2297ページ）、「デフォルトのネットワーク分析ポリシーの設定」、およびインライン導入でのプリプロセッサによるトラフィックの変更 （2302 ページ）を参照してください。

CIP プリプロセッサの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	任意	いずれか（Any）	Admin/Intrusion Admin

始める前に

- CIP **ポート**としてリストするデフォルトの CIP 検出ポート 44818 およびその他のポートを TCP ストリームのリスト [ストリームの再構成をどちらのポートでも実行する（Perform Stream Reassembly on Both Ports）] に追加する必要があります。CIP プリプロセッサのオプション （2391 ページ）、カスタム ネットワーク分析ポリシーの作成 （2297ページ）、およびTCP ストリームのプリプロセス オプション （2425 ページ）を参照してください。
- CIP プリプロセッサの設定のガイドライン （2393ページ） の内容についてよく理解しておきます。

ステップ 1 **[Policies]** > **[Access Control]**、次に **[Network Analysis Policy]**または**[Policies]** > **[Access Control]** > **[Intrusion]**、次に **[Network Analysis Policy]**を選択します。

（注） カスタム ユーザ ロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

ステップ 2 編集するポリシーの横にある編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 ナビゲーション パネルで [設定（Settings）] をクリックします。

ステップ 4 [SCADA プリプロセッサ（SCADA Preprocessors）] の下の [CIP 設定（CIP Configuration）] が無効になっている場合は、[有効（Enabled）] をクリックします。

ステップ 5 CIP プリプロセッサのオプション （2391 ページ） で説明するオプションを変更できます。

ステップ 6 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後にキャッシュされた変更は破棄されます。

次のタスク

- イベントを生成し、インライン展開では、違反パケットをドロップします。する場合は、CIP侵入ルールを有効にします。詳細については、侵入ルール状態の設定 （2093 ページ）およびCIP イベント （2391 ページ）を参照してください。
- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

第 94 章

トランスポート層およびネットワーク層プリプロセッサ

以下のトピックでは、トランスポート層およびネットワーク層プリプロセッサとそれらの設定方法について説明します。

トランスポート層およびネットワーク層のプリプロセッサの概要

トランスポート層およびネットワーク層のプリプロセッサは、IP フラグメンテーション、チェックサム検証、TCP および UDP セッションの前処理を悪用する攻撃を検出します。パケットがプリプロセッサに送信される前に、パケット デコーダは,パケット ヘッダーとペイロードをプリプロセッサや侵入ルールエンジンで使用しやすいフォーマットに変換し、パケットヘッダー内のさまざまな異常動作を検出します。インライン正規化プリプロセッサは、パケットをデコードした後、他のプリプロセッサにパケットを送信する前に、インライン型展開を対象にトラフィックを正規化します。

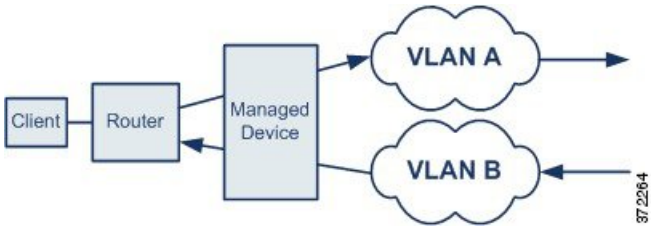
侵入ルールまたはルールの引数がプリプロセッサの無効化を必要とする場合、ネットワーク分析ポリシーの Web インターフェイスではプリプロセッサが無効化されたままになりますが、システムは自動的に現在の設定でプリプロセッサを使用します。

トランスポート/ネットワークプリプロセッサの詳細設定

トランスポート/ネットワーク プリプロセッサの詳細設定は、アクセス コントロール ポリシーを展開するすべてのネットワーク、ゾーン、VLANにグローバルに適用されます。これらの詳細設定は、ネットワーク分析ポリシーではなくアクセス コントロール ポリシーで設定します。

無視される VLAN ヘッダー

同じ接続で異なる方向に流れるトラフィックの VLAN タグが異なると、トラフィックのリアセンブルやルールの処理に影響を与える場合があります。たとえば、以下の図では、同じ接続のトラフィックを VLAN A で送信し、VLAN B で受信できます。



展開でパケットを正しく処理するため、VLANヘッダーを無視するようにシステムを設定できます。

（注） このオプションは、ASA FirePOWER ではサポートされません。

侵入廃棄ルールでのアクティブ応答

廃棄ルールは、ルール状態が [ドロップしてイベントを生成する（Drop and Generate Events）] に設定された侵入ルールまたはプリプロセッサルールです。インライン展開では、システムは TCP または UDP 廃棄ルールに応答するために、トリガーしたパケットをドロップし、そのパケットが開始されたセッションをブロックします。

ヒント UDP データ ストリームは一般にセッションという観点では考慮されないため、ストリーム プリプロセッサはカプセル化 IP データグラム ヘッダーの送信元と宛先の IP アドレス フィールドと UDP ヘッダーのポート フィールドを使用してフローの方向を判別し、UDP セッションを識別します。

問題のあるパケットによって TCP または UDP 廃棄ルールがトリガーされた時点で、1 つ以上のアクティブ応答を開始して、より正確かつ明示的に TCP 接続または UDP セッションを閉じるようにシステムを設定することができます。アクティブ応答は、ルーテッド展開およびトラ

ンスペアレント展開を含むインライン展開で使用できます。アクティブ応答は、パッシブ展開には適していないか、またはサポートされていません。

アクティブ応答を設定するには、次の手順を実行します。

- TCP または UDP（**resp** キーワードのみ）の侵入ルールを作成または変更します。侵入ルール ヘッダー プロトコル （2140 ページ）を参照してください。
- 侵入ルールに **react** キーワードまたは **resp** キーワードを追加します。アクティブ応答のキーワード （2249 ページ）を参照してください。
- 必要に応じて、TCP 接続の場合は、送信する追加のアクティブ応答の最大数と、アクティブ応答の間に待機する秒数を指定します。トランスポート/ネットワーク プリプロセッサの詳細オプション （2399 ページ）の「**アクティブ応答の最大数（Maximum Active Responses）**」および「**最小応答時間（秒）（Minimum Response Seconds）**」を参照してください。

アクティブ応答は、一致するトラフィックが廃棄ルールをトリガーとして使用したときに、次のように、そのトラフィックをクローズします。

- **TCP**：トリガーを使用したパケットを廃棄し、クライアントとサーバ両方のトラフィックに TCP リセット（RST）パケットを挿入します。
- **UDP**：セッションの両端に ICMP 到達不能パケットを送信します。

トランスポート/ネットワーク プリプロセッサの詳細オプション

接続の追跡時に VLAN ヘッダーを無視する（Ignore the VLAN header when tracking connections）

トラフィックの識別時に VLAN ヘッダーを無視するか、それとも考慮するかを指定します。次のようになります。

- このオプションを選択すると、VLANヘッダーが無視されます。この設定は、異なる方向に移動するトラフィックで同じ接続について異なる VLAN タグを検出する可能性がある展開済みデバイスに使用します。
- このオプションを無効にすると、VLANヘッダーが考慮されます。この設定は、異なる方向に移動するトラフィックで同じ接続について異なる VLAN タグを検出しない展開済みデバイスに使用します。

（注） このオプションは、ASA FirePOWER ではサポートされていません。

アクティブ応答の最大数（Maximum Active Responses）

TCP接続あたりのアクティブ応答の最大数を指定します。アクティブ応答が開始された接続でさらにトラフィックが発生し、前のアクティブ応答を送信してから [最小応答秒数（Minimum

Response Seconds）]を超えるトラフィックが発生した場合、システムは指定された最大数に達するまで、別のアクティブ応答を送信します。0を設定すると、**resp**または**react**ルールによってトリガーされる追加のアクティブ応答が無効になります。侵入廃棄ルールでのアクティブ応答（2398ページ）およびアクティブ応答のキーワード（2249ページ）を参照してください。

トリガーされた**resp**または**react**ルールは、このオプションの設定に関係なく、アクティブ応答を開始することに注意してください。

最小応答時間（秒）（Minimum Response Seconds）

[最大アクティブ応答数（Maximum Active Responses）]に達するまで、システムがアクティブ応答を開始した接続で発生した追加のトラフィックに対して次のアクティブ応答を送信するまで待機する時間を指定します。

トラブルシューティングオプション：セッション終了ロギングしきい値（Troubleshooting Options: Session Termination Logging Threshold）

注意 [セッション終了ロギングしきい値（Session Termination Logging Threshold）]は、サポート担当から指示されない限り変更しないでください。

トラブルシューティングの電話中に、個別の接続が指定したしきい値を超えた場合にメッセージを記録するようにシステムを設定することをサポートから依頼される場合があります。このオプションの設定を変更するとパフォーマンスに影響するので、必ずサポートのガイダンスに従って実行してください。

このオプションは、ログに記録されるメッセージのバイト数を指定します。セッションが終了し、メッセージが指定のバイト数を超えた場合は、ログに記録されます。

（注） 上限は1 GBですが、管理対象デバイスでストリーム処理のために割り当てられるメモリの量によっても制限されます。

関連トピック

アクティブ応答のキーワード（2249ページ）

トランスポート/ネットワーク プリプロセッサの詳細設定の構成

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Access Admin/Network Admin

ステップ 1 アクセス コントロール ポリシー エディタで、[詳細（Advanced）] タブをクリックします。

ステップ 2 [トランスポート/ネットワーク レイヤ設定（Transport/Network Layer Settings）] セクションの横にある編集アイコン（  ）をクリックします。

ステップ 3 トラブルシューティング オプション [セッション終了のロギングしきい値（Session Termination Logging Threshold）] を除き、トランスポート/ネットワーク プリプロセッサの詳細オプション （2399 ページ）の説明に従ってオプションを変更します。

（注） [接続のトラッキング時は VLAN ヘッダーを無視（Ignore the VLAN header when tracking connectons）] オプションは、ASA FirePOWER モジュールでは使用できません。

注意 [セッション終了のロギングしきい値（Session Termination Logging Threshold）] は、サポートからの指示がない限り変更しないでください。

ステップ 4 [OK] をクリックします。

次のタスク

- 必要に応じて、アクセス コントロール ポリシーの編集 （1674 ページ）の説明に従ってさらにポリシーを設定します。
- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

チェックサム検証

システムは、あらゆるプロトコル レベルのチェックサムを検証することで、IP、TCP、UDP、および ICMP による送信データが完全に受信されていることを確認できます。さらに基本的なレベルで、パケットが転送中に改ざんされたり、誤って変更されたりしていないことも確認できます。チェックサムはアルゴリズムを使用して、パケットでのプロトコルの整合性を検証します。システムが終端のホストでパケットに書き込まれた値を計算し、それがチェックサムと同じであれば、そのパケットは変更されていないと見なされます。

チェックサムの検証を無効にすると、ネットワークがインジェクション攻撃にさらされる危険があります。システムは、チェックサム検証イベントを生成しないことに注意してください。インライン展開では、パケットのチェックサムが正しくない場合、そのパケットをドロップするようにシステムを設定できます。

チェックサム検証オプション

次のオプションは、いずれも、パッシブ展開またはインライン展開で [有効（Enabled）] または [無効（Disabled）] に設定することができます。インライン展開では [ドロップ（Drop）] に設定することもできます。

- **ICMP チェックサム（ICMP Checksums）**
- **IP チェックサム（IP Checksums）**
- **TCP チェックサム（TCP Checksums）**
- **UDP チェックサム（UDP Checksums）**

違反パケットをドロップするには、オプションを[ドロップ（Drop）]に設定するだけでなく、関連付けられているネットワーク分析ポリシーの [インライン モード（Inline Mode）] を有効にし、確実にデバイスがインラインで展開されるようにする必要があります。

パッシブ展開またはタップ モードでのインライン展開で、これらのオプションを [ドロップ（Drop）] に設定することは、[有効（Enabled）] に設定するのと同じです。

すべてのチェックサム検証オプションは、デフォルトで、[有効（Enabled）]になっています。ただし、FTD ルーテッド トランスペアレント インターフェイスでは、IP チェックサム検証に失敗したパケットは常にドロップされます。FTD ルーテッドおよびトランスペアレント インターフェイスが、パケットを Snort プロセスに渡す前に、正しくないチェックサムを使用して UDP パケットを修正することに注意してください。

関連トピック

インライン導入でのプリプロセッサによるトラフィックの変更 （2302 ページ）

チェックサムの確認

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Intrusion Admin

ステップ 1 **[Policies]** > **[Access Control]**、次に **[Network Analysis Policy]** または**[Policies]** > **[Access Control]** > **[Intrusion]**、次に **[Network Analysis Policy]** を選択します。

（注） カスタム ユーザ ロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

ステップ 2 編集するポリシーの横にある編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 ナビゲーション パネルで [設定（Settings）] をクリックします。

ステップ 4 [トランスポート層/ネットワーク層のプロセッサ（Transport/Network Layer Preprocessors）] の下にある [チェックサムの確認（Checksum Verification）] が無効になっている場合、[有効（Enabled）] をクリックします。

ステップ 5 [チェックサムの確認（Checksum Verification）] の横にある編集アイコン（）をクリックします。

ステップ 6 チェックサム検証 （2401 ページ）の説明に従ってオプションを変更します。

ステップ 7 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後にキャッシュされた変更は破棄されます。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

関連トピック

レイヤ管理 （2051 ページ）
競合と変更：ネットワーク分析および侵入ポリシー （2041 ページ）

インライン正規化プリプロセッサ

インライン正規化プリプロセッサは、インライン展開で攻撃者が検出を免れる可能性を最小限にするために、トラフィックを正規化します。

（注） システムでトラフィックに影響を与えるには、ルーテッド、スイッチド、またはトランスペアレント インターフェイスあるいはインライン インターフェイス ペアを使用して、関連する設定を管理対象デバイスに展開する必要があります。

IPv4、IPv6、ICMPv4、ICMPv6、TCP トラフィックを任意に組み合わせて正規化を指定できます。ほとんどの正規化は、パケット単位で行われ、インライン正規化プリプロセッサによって処理されます。ただし、TCP ストリーム プリプロセッサは、TCP ペイロードの正規化を含む、ほとんどの状態関連パケットおよびストリームの正規化を処理します。

インライン正規化は、パケット デコーダによるデコードの直後に行われます。その後で、別のプリプロセッサによる処理が行われます。正規化は、パケット層の内部から外部への方向で行われます。

インライン正規化プリプロセッサはイベントを生成しません。インライン正規化プリプロセッサの役割は、インライン展開の別のプリプロセッサおよびルール エンジンで使用できるようにパケットを準備することです。また、システムが処理するパケットが、ネットワーク上のホストで受信したパケットと同じであるようにする役割もあります。

（注） インライン展開では、インライン モードを有効にし、[TCP ペイロードの正規化（Normalize TCP Payload）] オプションを有効にして、インライン正規化プリプロセッサを設定することをお勧めします。パッシブ展開では、アダプティブ プロファイルの更新を使用することをお勧めします。

関連トピック

インライン導入でのプリプロセッサによるトラフィックの変更 （2302 ページ）
アダプティブ プロファイルについて （2463 ページ）

インライン正規化オプション

最小 TTL（Minimum TTL）

[TTL のリセット（Reset TTL）] がこのオプションに設定する値以上の値に設定されている場合、このオプションは以下を指定します。

- [IPv4 の正規化（Normalize IPv4）] が有効にされている場合は、[IPv4 存続可能時間（TTL）（IPv4 Time to Live (TTL)）] フィールドの最小許容値。TTL のパケット値がこの値を下回る場合、[TTL のリセット（Reset TTL）] に設定された値に正規化されます。
- [Normalize IPv6] が有効にされている場合は、[IPv6 Hop Limit] フィールドの最小許容値。ホップ リミットの値がこの値を下回る場合、[Reset TTL] に設定された値に正規化されます。

このフィールドが空白の場合、システムは値が 1 であると想定します。

（注） FTD ルーテッドおよびトランスペアレント インターフェイスの場合、[最小 TTL（Minimum TTL）] および [TTL のリセット（Reset TTL）] オプションは無視されます。接続の最大 TTL は最初のパケットの TTL によって決定します。後続パケットの TTL は削減できますが、増やすことはできません。システムは、TTL をその接続の以前の最小 TTL にリセットします。これにより、TTL 回避攻撃を阻止します。

パケット復号化の [プロトコル ヘッダー異常の検出（Detect Protocol Header Anomalies）] オプションが有効になっている場合、デコーダ ルール カテゴリで次のルールを有効にして、このオプションに関する イベントを生成し、インライン展開では、違反パケットをドロップします。 を行うことができます。

- 指定の最小値を下回る TTL が設定された IPv4 パケットが検出された場合にトリガーするには、ルール 116:428 を有効にします。
- 指定の最小値を下回るホップ リミットが設定された IPv6 パケットが検出された場合にトリガーするには、ルール 116:270 を有効にします。

TTL のリセット（Reset TTL）

[最小 TTL（Minimum TTL）] の値以上の値を設定した場合、以下のフィールドが正規化されます。

- [IPv4 の正規化（Normalize IPv4）] が有効にされている場合は、[IPv4 TTL] フィールド
- [Normalize IPv6] が有効にされている場合は、[IPv6 Hop Limit] フィールド

パケット値が [最小 TTL（Minimum TTL）] を下回る場合、システムはパケットの TTL またはホップ リミットの値をこのオプションに対して設定された値に変更して、パケットを正規化します。このフィールドを空白のままにするか、0 に設定するか、または [最小 TTL（Minimum TTL）] 未満の値に設定すると、このオプションは無効になります。

IPv4 の正規化（Normalize IPv4）

IPv4 トラフィックの正規化を有効にします。システムは、以下の場合にも必要に応じて TTL フィールドを正規化します。

- このオプションが有効になっていて、さらに、
- [TTL のリセット（Reset TTL）] に設定された値によって TTL の正規化が有効になっている。

このオプションを有効にすると、追加の IPv4 オプションを有効にすることもできます。

このオプションを有効にすると、システムは以下の基本の IPv4 正規化を実行します。

- 過剰なペイロードを持つパケットを、IP ヘッダーに指定されたデータグラム長まで切り捨てます。
- [Differentiated Services (DS)] フィールド（旧称 [Type of Service (TOS)] フィールド）をクリアします。
- すべてのオプション オクテットを 1（[操作なし（No Operation）]）に設定します。

このオプションは FTD ルーテッド インターフェイスとトランスペアレント インターフェイスでは無視されます。FTD デバイスは、ルーテッド インターフェイスまたはトランスペアレント インターフェイスのルーテッド アラート、End of Options List（EOOL）、オペレーションなし（NOP）オプション以外の IP オプションを含んでいるすべての RSVP パケットをドロップします。

フラグメント禁止ビットの正規化（Normalize Don't Fragment Bit）

[IPv4 Flags] 見出し フィールドの単一ビットの [Don’t Fragment] サブフィールドをクリアします。このオプションを有効にすると、ダウンストリームのルータがパケットをドロップする代わりに、必要に応じてパケットをフラグメント化できます。また、このオプションを有効にすることで、ドロップされるパケットを巧妙に作成してポリシーを回避する試みを防ぐこともできます。このオプションを選択するには、[Normalize IPv4] を有効にする必要があります。

Normalize Reserved Bit

[IPv4 Flags] 見出し フィールドの単一ビットの [Reserved] サブフィールドをクリアします。通常は、このオプションを有効にします。このオプションを選択するには、[Normalize IPv4] を有効にする必要があります。

TOS ビットの正規化（Normalize TOS Bit）

1バイトの差別化サービス（DS）フィールド（旧「タイプ オブ サービス（ToS）フィールド」）をクリアします。このオプションを選択するには、[IPv4 の正規化（Normalize IPv4）] を有効にする必要があります。

Normalize Excess Payload

過剰なペイロードを持つパケットを、IP 見出しに指定されたデータグラム長にレイヤ 2（たとえば、イーサネット）見出しを合計した長さにまで切り捨てます。ただし、最小フレーム長より小さく切り捨てることはしません。このオプションを選択するには、[IPv4の正規化（Normalize IPv4）] を有効にする必要があります。

このオプションは、FTD ルーテッドおよびトランスペアレント インターフェイスでは無視されます。過剰なペイロードを持つパケットは、常にこれらのインターフェイスでドロップされます。

IPv6 の正規化（Normalize IPv6）

[Hop-by-Hop Options] および [Destination Options] 拡張見出しに含まれるすべてのオプション タイプ フィールドを 00（スキップして処理を続行）に設定します。このオプションが有効にされていて、[Reset TTL] に設定された値が ホップ リミット正規化を有効にしている場合、システムは必要に応じてホップ リミット フィールドも正規化します。

Normalize ICMPv4

ICMPv4 トラフィックのエコー（要求）およびエコー応答メッセージで8ビットのコードフィールドをクリアします。

Normalize ICMPv6

ICMPv6 トラフィックのエコー（要求）およびエコー応答メッセージで8ビットのコードフィールドをクリアします。

予約済みビットの正規化またはクリア（Normalize/Clear Reserved Bits）

TCP ヘッダーの予約ビットをクリアします。

Normalize/Clear Option Padding Bytes

TCP オプションの埋め込みバイトをクリアします。

URG=0 の場合に緊急ポインタをクリア（Clear Urgent Pointer if URG=0）

緊急（URG）制御ビットが設定されていない場合、16 ビットの TCP ヘッダー [緊急ポインタ（Urgent Pointer）] フィールドをクリアします。

空のペイロードに設定された緊急ポインタまたは URG をクリア（Clear Urgent Pointer/URG on Empty Payload）

ペイロードがない場合、TCP ヘッダーの緊急ポインタ フィールドと URG 制御ビットをクリアします。

Clear URG if Urgent Pointer is Not Set

緊急ポインタが設定されていない場合、TCP ヘッダーの緊急制御ビットをクリアします。

緊急ポインタの正規化（Normalize Urgent Pointer）

ポインタがペイロード長を上回る場合、2 バイトの TCP ヘッダー [緊急ポインタ（Urgent Pointer）] フィールドをペイロード長に設定します。

TCP ペイロードの正規化（Normalize TCP Payload）

再送信されるデータの一貫性が確保されるように [TCP データ（TCP Data）] フィールドの正規化を有効にします。正しく再構成できないセグメントはすべてドロップされます。

SYN に関するデータを削除（Remove Data on SYN）

TCP オペレーティング システム ポリシーが Mac OS **以外**の場合、同期（SYN）パケットのデータを削除します。

また、このオプションにより、TCP ストリーム プリプロセッサの [ポリシー（Policy）] オプションが [Mac OS] に設定されていない場合にトリガー可能なルール 129:2 もまた無効になります。

RST に関するデータを削除（Remove Data on RST）

TCP リセット（RST）パケットからデータを削除します。

Trim Data to Window

TCP データ フィールドを [Window] フィールドで指定されたサイズに切り詰めます。

Trim Data to MSS

ペイロードが MSS より長い場合、[TCP データ（TCP Data）] フィールドを最大セグメント サイズ（MSS）にまで切り捨てます。

解決不可能な TCP ヘッダーの異常をブロック（Block Unresolvable TCP Header Anomalies）

このオプションを有効にすると、システムは無効になり受信ホストによってブロックされる可能性が高い異常な TCP パケット（正規化されている場合）をブロックします。たとえば、システムは、確立されたセッションに送信される以降の SYN パケットをブロックします。

ルールが有効になっているかどうかに関係なく、以下に示す TCP ストリーム プリプロセッサのいずれかのルールに一致するパケットもすべてドロップされます。

- 129:1

- 129:3
- 129:4
- 129:6
- 129:8
- 129:11
- 129:14 ～129:19

[ブロックされたパケットの合計（Total Blocked Packets）] パフォーマンス グラフには、インライン展開でブロックされたパケットの数が示され、パッシブ展開とタップ モードでのインライン展開の場合は、インライン展開でブロックされる予想数が示されます。

明示的な混雑通知（ECN）（Explicit Congestion Notification）

明示的輻輳通知（ECN）フラグのパケット単位またはストリーム単位の正規化を以下のように有効にします。

- [パケット（Packet）] を選択すると、ネゴシエーションに関係なく、パケット単位で ECN フラグがクリアされます。
- [ストリーム（Stream）] を選択すると、ECN の使用がネゴシエートされていない場合、ストリーム単位で ECN フラグがクリアされます。

[ストリーム（Stream）] を選択した場合、この正規化が実行されるようにするには、TCP ストリーム プリプロセッサの [TCP 3 ウェイ ハンドシェイク必須（Require TCP 3-Way Handshake）] オプションも有効にされている必要があります。

既存の TCP オプションをクリア（Clear Existing TCP Options）

[これらの TCP オプションを許可（Allow These TCP Options）] を有効にします。

.

これらの TCP オプションを許可（Allow These TCP Options）

トラフィックで許可する特定の TCP オプションの正規化を無効にします。

明示的に許可されたオプションは、正規化されません。オプションを [操作なし（No Operation）]（TCP オプション 1）に設定して明示的に許可していないオプションは、正規化されます。

[これらの TCP オプションを許可（Allow These TCP Options）] の設定に関係なく、次のオプションは最適な TCP パフォーマンスに一般的に使用されるため、システムは常にこれらのオプションを許可します。

- 最大セグメント サイズ（MSS）（Maximum Segment Size (MSS)）
- ウィンドウ スケール（Window Scale）
- タイム スタンプ TCP（Time Stamp TCP）

他のそれほど一般的に使用されないオプションについては、システムは自動的に許可しません。

特定のオプションを許可するには、オプションキーワード、オプション番号、またはこの両方のカンマ区切りリストを設定します。以下に、一例を示します。

```
sack, echo, 19
```

オプション キーワードを指定するということは、そのキーワードと関連付けられた1つ以上のTCP オプションの番号を指定することと同じです。たとえば、`sack` を指定することは、TCP オプション 4（Selective Acknowledgement Permitted）および TCP オプション 5（Selective Acknowledgement）を指定することと同じです。オプション キーワードでは、大文字と小文字が区別されません。

また、`any` を指定すると、すべての TCP オプションが許可されるため、実質的にすべての TCP オプションの正規化が無効にされます。

次の表に、許可する TCP オプションを指定する方法を要約します。フィールドを空のままにすると、システムは MSS、ウィンドウ スケール、およびタイムスタンプのオプションのみを許可します。

指定するキーワード	許可されるオプション
sack	TCP オプション 4（Selective Acknowledgement Permitted）および 5（Selective Acknowledgement）
echo	TCP オプション 6（Echo Request）および 7（Echo Reply）
partial_order	TCP オプション 9（Partial Order Connection Permitted）および 10（Partial Order Service Profile）
conn_count	TCP 接続カウント オプション 11（CC）、12（CC.New）、および 13（CC.Echo）
alt_checksum	TCP オプション 14（Alternate Checksum Request）および 15（Alternate Checksum）
md5	TCP オプション 19（MD5 Signature）
オプション番号 2 ～ 255	キーワードのないオプションを含む、特定のオプション
any	すべての TCP オプション（この設定は、実質的に TCP オプションの正規化を無効にします）

このオプションに `any` を指定しない場合、正規化に以下が含まれます。

- MSS、ウィンドウ スケール、タイムスタンプ、およびその他の明示的に許可されたオプションを除き、すべてのオプションのバイトを [操作なし（No Operation）]（TCP オプション 1）に設定します。

- タイムスタンプは存在していても無効な場合、あるいは有効であってもネゴシエートされない場合、タイムスタンプ オクテットを [操作なし（No Operation）] に設定します。
- タイムスタンプがネゴシエートされているが存在しない場合、パケットをブロックします。
- 確認応答（ACK）制御ビットが設定されていない場合、タイムスタンプ エコー応答T（TSecr）オプション フィールドをクリアします。
- SYN 制御ビットが設定されていない場合、[MSS] および [ウィンドウ スケール（Window Scale）] オプションを [操作なし（No Operation）]（TCP オプション 1）に設定します。

関連トピック

侵入イベントのパフォーマンス統計情報グラフの種類 （3107 ページ）

インライン正規化の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Intrusion Admin

始める前に

- 問題を起こすパケットを正規化またはドロップするには、インライン導入でのプリプロセッサによるトラフィックの変更（2302ページ）の説明に従って[インラインモード（Inline Mode）]を有効にします。また、管理対象デバイスは、インラインで展開する必要があります。

ステップ 1 **[Policies]** > **[Access Control]**、次に **[Network Analysis Policy]**または**[Policies]** > **[Access Control]** > **[Intrusion]**、次に **[Network Analysis Policy]**を選択します。

（注） カスタムユーザロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

ステップ 2 編集するポリシーの横にある編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 ナビゲーション パネルで [設定（Settings）] をクリックします。

ステップ 4 [トランスポートまたはネットワーク レイヤ プリプロセッサ（Transport/Network Layer Preprocessors）] で [インライン正規化（Inline Normalization）] が無効になっている場合は、[有効化（Enabled）] をクリックします。

ステップ 5 [インライン正規化（Inline Normalization）] の横にある編集アイコン（）をクリックします。

ステップ 6 インライン正規化プリプロセッサ （2403 ページ）で説明されているオプションを設定します。

ステップ 7 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後にキャッシュされた変更は破棄されます。

次のタスク

- インライン正規化 [最小 TTL（Minimum TTL）] オプションで侵入イベントを生成する場合は、パケット デコーダ ルール 116:429（IPv4）と 116:270（IPv6）のいずれかまたは両方を有効にします。詳細については、侵入ルール状態の設定 （2093 ページ）およびインライン正規化オプション （2404 ページ）を参照してください。
- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

関連トピック

レイヤ管理 （2051 ページ）
競合と変更：ネットワーク分析および侵入ポリシー （2041 ページ）

IP 最適化プリプロセッサ

最大伝送ユニット（MTU）より大きいために IP データグラムが複数の小さい IP データグラムに分割されると、その IP データグラムはフラグメント化されたことになります。単一の IP データグラム フラグメントには、隠れた攻撃を識別するのに十分な情報が含まれない場合があります。そのため、攻撃者はエクスプロイトの検出を免れるために、フラグメント化されるパケットで攻撃データを送信する可能性があります。IP デフラグ プリプロセッサは、ルール エンジンが IP データグラムに対してルールを実行する前に、パケットに仕込まれた攻撃をルールで識別しやすくするために、フラグメント化された IP データグラムを再アセンブルします。フラグメント化されたデータグラムを再構成できない場合、それらのデータグラムに対しては、ルールが実行されません。

IP フラグメンテーション エクスプロイト

IP 最適化を有効にすると、ネットワーク上のホストに対する攻撃（ティアドロップ攻撃など）や、システム自体に対するリソース消費攻撃（Jolt2 攻撃など）を検出するのに役立ちます。

ティアドロップ攻撃は、特定のオペレーティング システムのバグを悪用して、そのオペレーティング システムがオーバーラップした IP フラグメントを再アセンブルしようとするとクラッシュするように仕掛けます。IP デフラグ プリプロセッサを有効にして、オーバーラップしたフラグメントを識別するように設定すれば、該当するフラグメントを識別できます。IP デフラグ プリプロセッサは、ティアドロップ攻撃などのオーバーラップ フラグメント攻撃で、最初のパケットだけを検出するだけで、同じ攻撃での後続のパケットは検出しません。

Jolt2 攻撃では、IP デフラグ機能を酷使させるという方法でサービス拒絶攻撃を仕掛けるために、フラグメント化された同じ IP パケットのコピーを大量に送信します。IP デフラグ プリプロセッサでは、メモリ使用量の上限によって、このような攻撃を阻止し、包括的検査においてシステムを自己防衛状態にします。システムは攻撃によって過負荷にならず、運用可能な状態を維持し、ネットワーク トラフィックの検査を続行します。

フラグメント化されたパケットを再アセンブルする方法は、オペレーティング システムによって異なります。ホストがどのオペレーティング システムで実行されているのかを攻撃者が特定できれば、その攻撃者はターゲット ホストが特定の方法で再アセンブルするように不正なパケットをフラグメント化することも可能です。モニタ対象のネットワーク上でホストを実行しているオペレーティング システムは、システムには不明です。したがって、プリプロセッサがパケットを誤った方法で再アセンブリして検査し、それによってエクスプロイトが検出されないままパススルーする可能性があります。このような攻撃を軽減するために、ネットワーク上のホストごとに適切な方法でパケットを最適化するよう、最適化プリプロセッサを設定できるようになっています。

パッシブ展開でアダプティブ プロファイルの更新を使用することで、パケットのターゲット ホストのホスト オペレーティング システム情報に応じて、IP 最適化プリプロセッサに適用するターゲットベースのポリシーが動的に選択されるようにすることもできます。

ターゲット ベースの最適化ポリシー

ホストのオペレーティング システムは以下の 3 つの基準を使用して、パケットを再構成する際に優先するパケット フラグメントを決定します。

- オペレーティング システムがフラグメントを受信した順序
- フラグメントのオフセット（パケットの先頭からのそのフラグメントの距離（バイト単位））
- オーバーラップしているフラグメントとの相対開始位置と相対終了位置

これらの基準はすべてのオペレーティング システムで使用されているものの、フラグメント化されたパケットを再構成するときに優先するフラグメントは、オペレーティング システムによって異なります。したがって、ネットワーク上で異なるオペレーティング システムを使用する 2 台のホストが、同じオーバーラップ フラグメントをまったく異なる方法で再アセンブルする場合も考えられます。

いずれかのホストのオペレーティング システムを認識している攻撃者が、オーバーラップしたパケット フラグメントに不正なコンテンツを忍ばせて送信することによって、エクスプロイトの検出を免れ、そのホストを悪用する可能性があります。このパケットが他のホストで再アセンブルされて検査されても、パケットに害はないように見えますが、ターゲット ホストで再アセンブルされる場合には不正なエクスプロイトが含まれています。ただし、モニタ対象のネットワーク セグメントで稼働するオペレーティング システムを認識するように IP 最適化プリプロセッサを設定すれば、このプリプロセッサがターゲット ホストと同じ方法でフラグメントを再構成することによって、攻撃を識別できます。

IP 最適化オプション

IP最適化を有効または無効にすることだけを選択することもできますが、シスコでは、それよりも細かいレベルで、有効にする IP 最適化プリプロセッサの動作を指定することを推奨しています。

以下の説明でプリプロセッサルールが言及されていない場合、オプションにはプリプロセッサルールが関連付けられていません。

次のグローバル オプションを構成できます。

事前に割り当てられたフラグメント（Preallocated Fragments）

プリプロセッサが一度に処理できる個々のフラグメントの最大数。事前割り当てするフラグメント ノードの数を指定すると、静的メモリ割り当てが有効になります。

注意 個々のフラグメントの処理には、約 1550 バイトのメモリが使用されます。プリプロセッサで個々のフラグメントを処理するために必要なメモリが、管理対象デバイスに事前定義された使用可能なメモリ量の制限を上回る場合は、管理対象デバイスのメモリ制限が優先されます。

IP 最適化ポリシーごとに、以下のオプションを設定できます。

Networks

最適化ポリシーを適用するホスト（複数可）の IP アドレス。

単一の IP アドレスまたはアドレス ブロック、あるいはこれらのいずれかまたは両方をコンマで区切ったリストを指定できます。デフォルトポリシーを含め、合計で最大255個のプロファイルを指定できます。

（注） システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。 上書き対応オブジェクトを使用すると、子孫ドメインの管理者は、グローバル コンフィギュレーションを自分のローカル環境に調整できます。

デフォルト ポリシーの `default` 設定では、別のターゲットベース ポリシーでカバーされていないモニタ対象ネットワーク セグメントのすべての IP アドレスが指定されることに注意してください。したがって、デフォルト ポリシーの IP アドレスまたは CIDR ブロック/プレフィクス長は指定できず、また指定する必要もありません。また、別のポリシーでこの設定を空白にしたり、すべて を表すアドレス表記（0.0.0.0/0 または ::/0）を使用したりすることはできません。

Policy

モニタ対象ネットワーク セグメント上のホスト一式に使用する最適化ポリシー。

ターゲット ホストのオペレーティング システムに応じて、7 つの最適化ポリシーの 1 つを選択できます。以下の表に、7 つのポリシーと、それぞれのポリシーを使用するオペレーティング システムを記載します。First と Last というポリシー名は、これらのポリシーが元のオーバーラップ パケットまたは後続のオーバーラップ パケットのどちらを優先するかを反映しています。

このオプションは、FTD ルーテッドおよびトランスペアレント インターフェイスでは無視されます。

表 *248 :* ターゲットベースの最適化ポリシー

ポリシー	オペレーティング システム
BSD	AIX FreeBSD IRIX VAX/VMS
BSD-right	HP JetDirect
First	Mac OS HP-UX
Linux	Linux OpenBSD
Last	Cisco IOS
Solaris	SunOS
Windows	Windows

Timeout

プリプロセッサエンジンがフラグメント化されたパケットを再構成する際に使用できる最大時間（秒数）を指定します。指定された時間内にパケットを再構成できない場合、プリプロセッサ エンジンはパケットの再構成試行を停止し、受信したフラグメントを破棄します。

最小 TTL（Min TTL）

パケットに許容される最小 TTL 値を指定します。このオプションは、TTL ベースの挿入攻撃を検出します。

このオプションにイベントを生成し、インライン展開では、違反パケットをドロップします。するには、ルール 123:11 を有効にします。

異常検知（Detect Anomalies）

オーバーラップ フラグメントのようなフラグメンテーション問題を識別します。

このオプションは、FTD ルーテッドおよびトランスペアレント インターフェイスでは無視されます。

このオプションにイベントを生成し、インライン展開では、違反パケットをドロップします。するには、次のルールを有効にすることができます：

- 123:1 ～ 123:4
- 123:5（BSD ポリシー）
- 123:6 ～123:8

オーバーラップ範囲（Overlap Limit）

セッション内で重複しているセグメントの設定された数が検出されると、そのセッションの最適化を停止することを指定します。

このオプションを設定するには、[異常検知（Detect Anomalies）] を有効にする必要があります。値が空白の場合、このオプションは無効になります。値 0 は、無制限の重複セグメント数を指定します。

このオプションは、FTD ルーテッドおよびトランスペアレント インターフェイスでは無視されます。重複フラグメントは、それらのインターフェイスでは常にドロップされます。

このオプションに関するイベントを生成し、インライン展開では、違反パケットをドロップします。 を行うには、ルール 123:12 を有効にできます。

最小フラグメント サイズ（Minimum Fragment Size）

設定されたバイト数より小さい最後でないフラグメントが検出された場合、そのパケットは悪意のあるものとみなされることを指定します。

このオプションを設定するには、[異常検知（Detect Anomalies）] を有効にする必要があります。値が空白の場合、このオプションは無効になります。値 0 は、無制限のバイト数を指定します。

このオプションに関するイベントを生成し、インライン展開では、違反パケットをドロップします。 を行うには、ルール 123:13 を有効にできます。

関連トピック

Firepower システムの IP アドレス表記法 （20 ページ）

IP 最適化の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Intrusion Admin

システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。上書き対応オブジェクトを使用すると、子孫ドメインの管理者は、グローバルコンフィギュレーションを自分のローカル環境に調整できます。

始める前に

- カスタム ターゲットベース ポリシーで識別するネットワークが、親ネットワーク分析ポリシーによって処理されるネットワーク、ゾーン、および VLAN のサブセットと一致するか、サブセットであることを確認します。詳細については、ネットワーク分析プロファイルの詳細設定 （2289 ページ）を参照してください。

ステップ 1 **[Policies]** > **[Access Control]**、次に **[Network Analysis Policy]** または **[Policies]** > **[Access Control]** > **[Intrusion]**、次に **[Network Analysis Policy]** を選択します。

（注） カスタム ユーザ ロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

ステップ 2 編集するポリシーの横にある編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 ナビゲーション パネルで [設定（Settings）] をクリックします。

ステップ 4 [トランスポートまたはネットワーク レイヤ プリプロセッサ（Transport/Network Layer Preprocessors）] で [IP 最適化（IP Defragmentation）] が無効になっている場合は、[有効化（Enabled）] をクリックします。

ステップ 5 [IP 最適化（IP Defragmentation）] の横にある編集アイコン（）をクリックします。

ステップ 6 必要に応じて、[事前割り当て済みフラグメント（Preallocated Fragments）] フィールドに値を入力します。

ステップ 7 次の選択肢があります。

- サーバ プロファイルの追加：ページの左側の [サーバ（Servers）] の横にある追加アイコン（）をクリックし、[ホスト アドレス（Host Address）] フィールドに値を入力して、[OK] をクリックします。単一の IP アドレスまたはアドレス ブロック、あるいはこれらのいずれかまたは両方をカンマで区切ったリストを指定できます。デフォルト ポリシーを含め、合計で最大 255 個のターゲットベースのポリシーを作成できます。
- サーバ プロファイルの編集：ページの左側の [サーバ（Servers）] で設定済みのアドレスをクリックするか、[デフォルト（default）] をクリックします。
- プロファイルの削除：ポリシーの横にある削除アイコン（）をクリックします。

ステップ 8 IP 最適化オプション （2413 ページ）の説明に従ってオプションを変更します。

ステップ 9 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後にキャッシュされた変更は破棄されます。

次のタスク

- イベントを生成し、インライン展開では、違反パケットをドロップします。 を行うには、IP 最適化ルール（GID 123）を有効にします。詳細については、侵入ルール状態の設定 （2093 ページ）およびIP 最適化オプション （2413 ページ）を参照してください。
- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

関連トピック

Firepower システムの IP アドレス表記法 （20 ページ）
レイヤの基本 （2045 ページ）
競合と変更：ネットワーク分析および侵入ポリシー （2041 ページ）

パケット デコーダ

キャプチャしたパケットをプリプロセッサに送信する前に、システムはパケットをパケットデコーダに送信します。パケット デコーダは、プリプロセッサやルール エンジンが容易に使用できる形式に、パケット 見出しおよびペイロードを変換します。データリンク層から開始して、ネットワーク層、トランスポート層へと、各スタック層が順にデコードされます。

パケット デコーダ オプション

以下の説明でプリプロセッサ ルールが言及されていない場合、オプションにはプリプロセッサ ルールが関連付けられていません。

GTP データ チャネルのデコード（Decode GTP Data Channel）

カプセル化された GTP（General Packet Radio Service（GPRS）トンネリング プロトコル）データ チャネルをデコードします。デフォルトでは、デコーダはポート 3386 ではバージョン 0 のデータをデコードし、ポート 2152 ではバージョン 1 のデータをデコードします。`GTP_PORTS` デフォルト変数を使用して、カプセル化された GTP トラフィックを識別するポートを変更できます。

このオプションにイベントを生成し、インライン展開では、違反パケットをドロップします。するには、ルール 116:297 および 116:298 を有効にします。

[標準外ポートで Teredo を検知（Detect Teredo on Non-Standard Ports）]

ポート 3544 以外の UDP ポートで識別される IPv6 トラフィックの Teredo トンネリングを検査します。

IPv6 トラフィックが存在する場合、システムは常にこのトラフィックを検査します。デフォルトでは、IPv6 インスペクションには 4in6、6in4、6to4、および 6in6 トンネリング方式が含まれます。また、UDP 見出しがポート 3544 を指定している場合は、Teredo トンネリングも含まれます。

IPv4 ネットワークでは、IPv4 ホストが Teredo プロトコルを使用して、IPv4 Network Address Translation（NAT）デバイスを介して IPv6 トラフィックをトンネリングできます。Teredo は、IPv6 パケットを IPv4 UDP データグラムにカプセル化して、IPv4 NAT デバイスの背後で IPv6 接続を許可します。システムは通常、UDP ポート 3544 を使用して Teredo トラフィックを識別します。ただし、攻撃者が検出を免れるために標準以外のポートを使用する可能性も考えられます。[Detect Teredo on Non-Standard Ports] を有効にすることで、システムに Teredo トンネリングのすべての UDP ペイロードを検査させることができます。

Teredo のデコードは、外側のネットワーク層に IPv4 が使用されている場合に限り、最初の UDP 見出しに対してのみ行われます。UDP データが IPv6 データにカプセル化されるため、Teredo IPv6 層の後に 2 つめの UDP 層が存在する場合、ルール エンジンは UDP 侵入ルールを使用して、内側および外側の両方の UDP 層を分析します。

policy-other ルール カテゴリの侵入ルール 12065、12066、12067、および 12068 は Teredo トラフィックを検出しますが、デコードはしないことに注意してください。（オプション）これらのルールを使用してインライン展開で Teredo トラフィックをドロップすることができます。ただし、[非標準ポートでの Teredo の検出（Detect Teredo on Non-Standard Ports）] を有効にする場合は、これらのルールを無効化するか、トラフィックをドロップせずにイベントを生成するように設定する必要があります。

[余長値の検知（Detect Excessive Length Value）]

パケット ヘッダーが実際のパケット長を超えるパケット長を指定しているかどうかを検出します。

このオプションは、FTD ルーテッド、トランスペアレント、およびインライン インターフェイスでは無視されます。超過ヘッダー長を持つパケットは常にドロップされます。ただし、このオプションは FTD インライン タップおよびパッシブ インターフェイスに適用されます。

このオプションに関してイベントを生成し、インライン展開では、違反パケットをドロップします。 を行うには、ルール 116:6、116:47、116:97、および 116:275 を有効にできます。

[間違いな IP オプションを検知（Detect Invalid IP Options）]

無効な IP オプションを使用したエクスプロイトを識別するために、無効な IP ヘッダー オプションを検出します。たとえば、ファイアウォールに対するサービス拒絶攻撃は、システムをフリーズさせる原因になります。ファイアウォールが無効なタイムスタンプおよび IP セキュリティ オプションを解析しようとして、ゼロ長のチェックに失敗すると、回復不可能な無限ループが発生します。ルールエンジンはゼロ長のオプションを識別し、ファイアウォールでの攻撃を軽減するために使用できる情報を提供します。

FTD デバイスは、各ルーテッドまたはトランスペアレント インターフェイスのルータ アラート、End of Options List（EOOL）、およびオペレーションなし（NOP）オプションを持つ RSVP

パケットをドロップします。インライン、インライン タップ、またはパッシブ インターフェイスについては、IP オプションは上記のように処理されます。

このオプションに関してイベントを生成し、インライン展開では、違反パケットをドロップします。 を行うには、ルール 116:4 および 116:5 を有効にします。

[実験的 TCP オプションを検知（Detect Experimental TCP Options）]

試験的な TCP オプションが設定された TCP ヘッダーを検出します。以下の表は、それらのオプションを示しています。

TCP オプション	説明
9	Partial Order Connection Permitted
10	Partial Order Service Profile
14	Alternate Checksum Request
15	Alternate Checksum Data
	Trailer Checksum
20	Space Communications Protocol Standards（SCPS）
21	Selective Negative Acknowledgements（SCPS）
22	Record Boundaries（SCPS）
23	Corruption（SPCS）
24	SNAP
26	TCP Compression Filter

これらのオプションは試験的なものであるため、一部のシステムでは考慮されず、悪用される恐れがあります。

（注） 上記の表に記載されている試験的オプションに加えて、26 より大きいオプション番号を持つ TCP オプションは、試験的オプションと見なされます。

このオプションにイベントを生成し、インライン展開では、違反パケットをドロップします。するには、ルール 116:58 を有効にします。

廃止された TCP オプションを検知

廃止された TCP オプションが設定された TCP ヘッダーを検出します。これらのオプションは廃止されたものであるため、一部のシステムでは考慮されず、悪用される恐れがあります。以下の表は、それらのオプションを示しています。

TCP オプション	説明
6	Echo
7	Echo Reply
16	Skeeter
17	Bubba
19	MD5 Signature
25	Unassigned（未定義）

このオプションにイベントを生成し、インライン展開では、違反パケットをドロップします。するには、ルール 116:57 を有効にします。

[T または TCP を検知（Detect T/TCP）]

CC.ECHO オプションが設定された TCP ヘッダーを検出します。CC.ECHO オプションは、TCP for Transactions（T/TCP）が使用されていることを確認します。T/TCP ヘッダー オプションは幅広く使用されていないため、一部のシステムでは考慮されず、悪用される恐れがあります。

このオプションにイベントを生成し、インライン展開では、違反パケットをドロップします。するには、ルール 116:56 を有効にします。

[その他の TCP オプションを検知（Detect Other TCP Options）]

他の TCP デコード イベント オプションでは検出されない無効な TCP オプションが設定された TCP ヘッダーを検出します。たとえば、このオプションは、無効な長さ、またはオプション データが TCP ヘッダーに収まらない長さの TCP オプションを検出します。

このオプションは、FTD ルーテッドおよびトランスペアレント インターフェイスでは無視されます。無効な TCP オプションを持つパケットは常にドロップされます。

このオプションに関してイベントを生成し、インライン展開では、違反パケットをドロップします。 を行うには、ルール 116:54、116:55、および 116:59 を有効にできます。

[プロトコルヘッダの異常を検知（Detect Protocol Header Anomalies）]

より具体的な IP および TCP デコーダ オプションでは検出されない他のデコード エラーを検出します。たとえば、このデコーダは、不正な形式のデータ リンク プロトコル ヘッダーを検出する場合があります。

このオプションは、FTD ルーテッド、トランスペアレント、およびインライン インターフェイスでは無視されます。ヘッダー異常があるパケットは常にドロップされます。ただし、このオプションは Threat Defense インライン タップおよびパッシブ インターフェイスに適用されます。

このオプションに関するイベントを生成し、インライン展開では、違反パケットをドロップします。 を行うには、次のルールを有効にすることができます。

GID:SID	該当する場合にイベントを生成
116:467	パケットが Cisco FabricPath ヘッダーにカプセル化されるパケットの最小サイズより小さい。
116:468	ヘッダーの Cisco メタデータ（CMD）フィールドに、有効な CMD ヘッダの最小サイズより小さいヘッダー長が含まれている。CMD フィールドは、Cisco TrustSec プロトコルと関連付けられています。
116:469	ヘッダーの CMD フィールドに、無効なフィールド長が含まれている。
116:470	ヘッダーの CMD フィールドに、無効なセキュリティ グループ タグ（SGT）オプションのタイプがあります。
116:471	ヘッダーの CMD フィールドに、値が予約されている SGT が含まれています。

その他のパケット デコーダ オプションに関連付けられていないパケット デコーダ ルールを有効にすることもできます。

関連トピック

定義済みデフォルト変数 （541 ページ）

パケット復号化の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Intrusion Admin

ステップ 1 **[Policies]** > **[Access Control]**、次に **[Network Analysis Policy]**または**[Policies]** > **[Access Control]** > **[Intrusion]**、次に **[Network Analysis Policy]**を選択します。

（注） カスタムユーザ ロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

ステップ 2 編集するポリシーの横にある編集アイコン（  ）をクリックします。

代わりに表示アイコン（  ）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 ナビゲーション パネルで [設定（Settings）] をクリックします。

ステップ 4 [トランスポートまたはネットワーク レイヤ プリプロセッサ（Transport/Network Layer Preprocessors）] の下の [パケット復号化（Packet Decoding）] が無効になっている場合は、[有効化（Enabled）] をクリックします。

ステップ 5 [パケット復号化（Packet Decoding）] の横にある編集アイコン（  ）をクリックします。

ステップ 6 パケット デコーダ オプション （2417 ページ）で説明されているオプションを有効または無効にします。

ステップ 7 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後にキャッシュされた変更は破棄されます。

次のタスク

- イベントを生成し、インライン展開では、違反パケットをドロップします。 を行うには、パケット デコーダ ルール（GID 116）を有効にします。詳細については、侵入ルール状態の設定 （2093 ページ）およびパケット デコーダ オプション （2417 ページ）を参照してください。
- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

関連トピック

レイヤの基本 （2045 ページ）
競合と変更：ネットワーク分析および侵入ポリシー （2041 ページ）

TCP ストリームの前処理

TCP プロトコルは、接続で生じ得るさまざまな状態を定義します。各 TCP 接続は、送信元と宛先の IP アドレス、および送信元と宛先のポートによって識別されます。TCP では、接続パラメータ値が同じ接続は、一度に 1 つしか存在できません。

状態に関連する TCP エクスプロイト

侵入ルールに `established` 引数と組み合わせた `flow` キーワードを追加すると、侵入ルール エンジンはステートフル モードでルールとフロー ディレクティブに一致するパケットを検査します。ステートフル モードでは、クライアントとサーバの間で正当な 3 ウェイ ハンドシェイクによって確立された TCP セッションの一部となっているトラフィックだけが評価されます。

確立された TCP セッションの一部として識別できない TCP トラフィックをプリプロセッサが検出するようにシステムを設定することは可能です。しかし、このようなイベントは、システムをすぐに過負荷状態に陥らせ、しかも意味のあるデータを提供しないため、通常の使用法では推奨されません。

Stick や Snot などの攻撃では、システムの自身に対する広範なルール セットとパケット インスペクションを悪用します。これらのツールは、Snort ベースの侵入ルールのパターンに基づいてパケットを生成してネットワークに送信します。ステートフルインスペクションに対して設定するルールに `flow` または `flowbits` キーワードを含めなければ、パケットのそれぞれがルールをトリガーするため、システムが過負荷状態になります。ステートフルインスペクションを使用することで、確立された TCP セッションに含まれず、意味のある情報を提供しないこれらのパケットを無視できます。ステートフル インスペクションを実行すると、ルール エンジンは確立された TCP セッションに含まれる攻撃のみを検出するため、アナリストが stick や snot によって大量に生成されるイベントに時間を取られることがなくなります。

ターゲット ベースの TCP ポリシー

オペレーティング システムによって、TCP の実装方法は異なります。たとえば、セッションをリセットするために、Windows やその他のオペレーティング システムの一部では TCP リセット セグメントに正確な TCP シーケンス番号を割り当てる必要があるのに対し、Linux や他のオペレーティング システムではシーケンス番号の範囲を使用できます。この例の場合、ストリーム プリプロセッサは、シーケンス番号に基づき、宛先ホストがリセットにどのように応答するかを正確に把握しなければなりません。ストリーム プリプロセッサがセッションの追跡を停止するのは、宛先ホストがリセットが有効であると見なした場合のみです。したがって、プリプロセッサがストリームの検査を停止した後は、パケットを送信することによって攻撃が検出を免れることはできません。TCP の実装方法の違いには、オペレーティング システムで TCP タイムスタンプ オプションを採用しているかどうか、採用している場合にはどのようにタイムスタンプを処理するか、そしてオペレーティング システムで SYN パケットのデータを受け入れるか、無視するかどうかも含まれます。

また、オーバーラップ TCP セグメントを再アセンブルする方法も、オペレーティング システムによって異なります。オーバーラップ TCP セグメントは、確認応答済み TCP トラフィックの通常の再送信を反映する場合があります。あるいは、ホストのオペレーティング システムを認識している攻撃者が、エクスプロイトの検出を免れるためにオーバーラップ セグメントに不正なコンテンツを忍ばせて送信し、そのホストを悪用しようとしている場合もあります。ただし、モニタ対象のネットワーク上で稼働するオペレーティング システムを認識するようにストリーム プリプロセッサを設定すれば、そのプリプロセッサがターゲット ホストと同じ方法でセグメントを再アセンブルすることによって、攻撃を識別できます。

モニタ対象のネットワーク セグメント上のさまざまなオペレーティング システムに合わせて TCP ストリーム インスペクションおよび再アセンブリを調整するために、1 つ以上の TCP ポリシーを作成することができます。ポリシーごとに、13 のオペレーティング システム ポリシーのうちの 1 つを特定します。異なるオペレーティング システムを使用するホストのいずれか、あるいはすべてを識別するために必要な数だけ TCP ポリシーを使用し、各 TCP ポリシーを特定の IP アドレスまたはアドレス ブロックにバインドします。デフォルトの TCP ポリシーは、他の TCP ポリシーで指定されていないモニタ対象ネットワーク上のすべてのホストに適用されます。したがって、デフォルトの TCP ポリシーに IP アドレスまたはアドレス ブロックを指定する必要はありません。

パッシブ展開で アダプティブ プロファイルの更新 を使用することで、パケットのターゲットホストのホスト オペレーティング システム情報に応じて、TCP ストリーム プリプロセッサに適用するターゲットベースのポリシーが動的に選択されるようにすることもできます。

TCP ストリームの再構成

ストリーム プリプロセッサは、TCP セッションでのサーバからクライアントへの通信ストリーム、クライアントからサーバへの通信ストリーム、またはその両方の通信ストリームに含まれるすべてのパケットを収集して再構成します。これにより、ルール エンジンは、特定のストリームに含まれる個々のパケットだけを検査するのではなく、ストリームを再構成された単一のエンティティとして検査できます。

ストリームの再構成により、ルールエンジンは、個々のパケットを検査する場合には検出できない可能性のあるストリームベースの攻撃を識別できます。ルールエンジンの再アセンブリ対象とする通信ストリームは、ネットワークのニーズに応じて指定できます。たとえば、Web サーバ上のトラフィックをモニタする際に、独自の Web サーバから不正なトラフィックを受信する可能性がほとんどないため、クライアント トラフィックだけを検査するという場合もあります。

各 TCP ポリシーに、ストリーム プリプロセッサが再構成するトラフィックを識別するポートのカンマ区切りのリストを指定できます。アダプティブ プロファイルの更新 が有効にされている場合、再構成するトラフィックを識別するサービスを、ポートの代わりとして、あるいはポートと組み合わせてリストすることもできます。

ポート、サービス、またはその両方を指定できます。クライアント ポート、サーバ ポート、またはその両方を任意に組み合わせた個別のポートリストを指定できます。また、クライアント サービス、サーバ サービス、またはその両方を任意に組み合わせた個別のサービス リストを指定することもできます。たとえば、以下を再アセンブルする必要があるとします。

- クライアントからの SMTP（ポート 25）トラフィック
- FTP サーバ応答（ポート 21）
- 両方向の Telnet（ポート 23）トラフィック

この場合、以下のように設定できます。

- クライアント ポートとして、`23, 25` を指定
- サーバ ポートとして、`21, 23` を指定

あるいは、以下のように設定することもできます。

- クライアント ポートとして、`25` を指定
- サーバ ポートとして、`21` を指定
- 両方のポートとして、`23` を指定

さらに、ポートとサービスを組み合わせた以下の設定例は、アダプティブ プロファイルの更新が有効にされている場合、有効になります。

- クライアント ポートとして、23 を指定
- クライアント サービスとして、smtp を指定
- サーバ ポートとして、21 を指定
- サーバ サービスとして、telnet を指定

ポートを否定すると（!80など）、そのポートのトラフィックがTCPストリームプリプロセッサで処理されなくなり、パフォーマンスが向上します。

all を引数として指定して、すべてのポートに対して再構成を指定することもできますが、ではポートを all に**設定しない**よう推奨しています。この設定では、このプリプロセッサで検査するトラフィックの量が増え、不必要にパフォーマンスが低下するためです。

TCP再構成には、自動的かつ透過的にその他のプリプロセッサに追加するポートが含まれています。ただし、他のプリプロセッサ設定に追加済みの TCP 再構成リストに明示的にポートを追加すると、それらのポートは通常どおりに処理されます。これには以下のプリプロセッサのポート リストが含まれます。

- FTP/Telnet（サーバ レベル FTP）
- DCE/RPC
- HTTP インスペクション
- SMTP
- Session Initiation Protocol
- POP
- IMAP
- SSL

追加のトラフィック タイプ（クライアント、サーバ、両方）を再構成すると、リソースの需要が増大することに注意してください。

TCP ストリームのプリプロセス オプション

以下の説明でプリプロセッサ ルールが言及されていない場合、オプションにはプリプロセッサ ルールが関連付けられていません。

次のグローバル TCP オプションを構成できます。

パケット タイプ パフォーマンスの向上（Packet Type Performance Boost）

送信元ポートおよび宛先ポートの両方を any に設定した TCP ルールで、flow または flowbits オプションが使用されている場合を除き、有効化された侵入ルールに指定されていないポートおよびアプリケーション プロトコルのすべてについて、TCP トラフィックを無視するように設定します。このオプションはパフォーマンスを向上させますが、攻撃を見逃す可能性があります。

TCP ポリシーごとに、以下のオプションを設定できます。

ネットワーク（Network）

TCP ストリーム再アセンブリ ポリシーを適用するホストの IP アドレスを指定します。

単一の IP アドレスまたはアドレス ブロックを指定できます。デフォルト ポリシーを含め、合計で最大 255 個のプロファイルを指定できます。

（注） システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。上書き対応オブジェクトを使用すると、子孫ドメインの管理者は、グローバル コンフィギュレーションを自分のローカル環境に調整できます。

デフォルト ポリシーの `default` 設定では、別のターゲットベース ポリシーでカバーされていないモニタ対象ネットワーク セグメントのすべての IP アドレスが指定されることに注意してください。したがって、デフォルト ポリシーの IP アドレスまたは CIDR ブロック/プレフィクス長は指定できず、また指定する必要もありません。また、別のポリシーでこの設定を空白にしたり、すべて を表すアドレス表記（0.0.0.0/0 または ::/0）を使用したりすることはできません。

Policy

TCP ポリシーを適用するターゲット ホスト（複数可）のオペレーティング システムを識別します。[Mac OS] 以外のポリシーを選択すると、システムは同期（SYN）パケットからデータを削除し、ルール 129:2 に対するイベントの生成を無効にします。インライン正規化プリプロセッサの [SYN に関するデータを削除（Remove Data on SYN）] オプションを有効にすると、ルール 129:2 も無効になることに注意してください。

以下の表に、オペレーティング システム ポリシーとそれを使用するホスト オペレーティング システムをリストします。

表 *249 : TCP* オペレーティング システム ポリシー

ポリシー	オペレーティング システム
First	不明な OS
Last	Cisco IOS
BSD	AIX FreeBSD OpenBSD
Linux	Linux 2.4 カーネル Linux 2.6 カーネル

ポリシー	オペレーティング システム
Old Linux	Linux 2.2 以前のカーネル
Windows	Windows 98 Windows NT の場合 Windows 2000 Windows XP
Windows 2003	Windows 2003
Windows Vista	Windows Vista
Solaris	Solaris OS SunOS
IRIX	SGI Irix
HPUX	HP-UX 11.0 以降
HPUX 10	HP-UX 10.2 以前
Mac OS	Mac OS 10（Mac OS X）

ヒント First オペレーティング システム ポリシーは、ホストのオペレーティング システムが不明な場合にはある程度の保護対策になります。ただし、攻撃を見逃す可能性もあります。オペレーティング システムが既知であれば、ポリシーを編集して、その正しいオペレーティング システムを指定してください。

Timeout

侵入ルール エンジンが非アクティブなストリームを状態テーブルで保持する秒数（1 ～ 86400 秒）。指定された期間内にストリームが再アセンブルされない場合、侵入ルール エンジンはそのストリームを状態テーブルから削除します。

（注） ネットワーク トラフィックがデバイスの帯域幅制限に到達しやすいセグメントに、管理対象デバイスが展開されている場合は、処理のオーバーヘッド量を削減するために、この値を大きい値（たとえば、600 秒）に設定することを検討してください。

FTD デバイスはこのオプションを無視します。その代りに高度なアクセス制御の **Threat Defense サービス ポリシー**の設定を使用します。詳細については、サービス ポリシー ルールの設定 （1183 ページ）を参照してください。

最大 TCP ウィンドウ（Maximum TCP Window）

受信側ホストで指定されている TCP ウィンドウの最大許容サイズを 1 ～ 1073725440 バイトの範囲で指定します。値を 0 に設定すると、TCP ウィンドウ サイズのチェックが無効になります。

⚠

注意 上限は RFC で許可される最大ウィンドウ サイズです。これは、攻撃者が検出を回避できないようにすることを目的としていますが、あまりにも大きな最大ウィンドウ サイズを設定すると、システム自体がサービス妨害を招く可能性があります。

[ステートフル インスペクションの異常（Stateful Inspection Anomalies）] が有効になっている場合は、ルール 129:6 を有効にして、このオプションに対しイベントを生成し、インライン展開では、違反パケットをドロップします。 することができます。

オーバーラップ範囲（Overlap Limit）

セッションで許容するオーバーラップ セグメントの数を 0（無制限）～ 255 の範囲で指定します。セッションで、この指定された値に達すると、セグメントの再構成が停止します。[ステートフル インスペクションの異常（Stateful Inspection Anomalies）] が有効にされていて、それに付随するプリプロセッサ ルールが有効にされている場合、イベントも生成されます。

このオプションにイベントを生成し、インライン展開では、違反パケットをドロップします。するには、ルール 129:7 を有効にします。

ファクタをフラッシュ（Flush Factor）

インライン展開では、ここで設定するサイズ減少なしのセグメントの数（1 ～ 2048）の後にサイズが減少したセグメントが検出されると、システムは検出用に累積されたセグメントデータをフラッシュします。値を 0 に設定すると、要求または応答の終わりを示す可能性のあるこのセグメント パターンの検出が無効になります。このオプションを有効にするには、インライン正規化の [TCP ペイロードの正規化（Normalize TCP Payload）] オプションを有効にする必要があることに注意してください。

ステートフル インスペクションの異常（Stateful Inspection Anomalies）

TCP スタックの異常な動作を検出します。付随するプリプロセッサ ルールが有効にされている場合、TCP/IP スタックが不完全に作成されていると、多数のイベントが生成される可能性があります。

このオプションは、FTD ルーテッドおよびトランスペアレント インターフェイスでは無視されます。

このオプションにイベントを生成し、インライン展開では、違反パケットをドロップします。するには、次のルールを有効にすることができます：

- 129:1 ～ 129:5
- 129:6（Mac OS のみ）

- 129:8 ～129:11
- 129:13 ～ 129:19

次の点に注意してください。

- ルール 129:6 でトリガーするには、さらに [最大 TCP ウィンドウ（Maximum TCP Window）] に 0 より大きい値を設定する必要があります。
- ルール 129:9 および 129:10 でトリガーするには、さらに [TCP セッションのハイジャック（TCP Session Hijacking）] を有効にする必要があります。

TCP セッションのハイジャック（TCP Session Hijacking）

スリーウェイ ハンドシェイク中に TCP 接続の両端から検出されたハードウェア（MAC）アドレスの有効性を、セッションで受信した後続のパケットに照合して検査することにより、TCP セッション ハイジャックを検出します。[ステートフル インスペクションの異常（Stateful Inspection Anomalies）] が有効にされていて、2 つの対応するプリプロセッサ ルールのいずれかが有効にされている場合、接続のどちらかの側の MAC アドレスが一致しないと、システムがイベントを生成します。

このオプションは、FTD ルーテッドおよびトランスペアレント インターフェイスでは無視されます。

このオプションに対しイベントを生成し、インライン展開では、違反パケットをドロップします。 するには、ルール 129:9 および 129:10 を有効にします。これらのルールのいずれかを使用してイベントを生成するには、[ステートフル インスペクションの異常（Stateful Inspection Anomalies）] を有効にする必要があります。

連続した小型セグメント（Consecutive Small Segments）

[ステートフル インスペクションの異常（Stateful Inspection Anomalies）] が有効にされている場合、連続する小さな TCP セグメントの許容数を 1 ～ 2048 の範囲で指定します。値を 0 に設定すると、連続する小さな TCP セグメントのチェックが無効になります。

このオプションは、[Small Segment Size] オプションと同時に設定し、両方とも無効にするか、両方にゼロ以外の値を設定する必要があります。通常は、それぞれのセグメントの長さが 1 バイトであったとしても、ACK が介在することなく 2000 個もの連続するセグメントを受信することはないので注意してください。

このオプションは、FTD ルーテッドおよびトランスペアレント インターフェイスでは無視されます。

このオプションにイベントを生成し、インライン展開では、違反パケットをドロップします。するには、ルール 129:12 を有効にします。

小型セグメントのサイズ（Small Segment Size）

[ステートフル インスペクションの異常（Stateful Inspection Anomalies）] が有効にされている場合、小さいと見なされる TCP セグメントのサイズを 1 ～ 2048 バイトの範囲で指定します。値を 0 に設定すると、小さいセグメントのサイズの指定が無効になります。

このオプションは、FTD ルーテッドおよびトランスペアレント インターフェイスでは無視されます。

このオプションは、[連続する小さなセグメント（Consecutive Small Segments）] オプションと同時に設定し、両方とも無効にするか、両方にゼロ以外の値を設定する必要があります。2048 バイトの TCP セグメントは、標準的な 1500 バイトのイーサネット フレームより大きいことに注意してください。

小型セグメントを無視したポート（Ports Ignoring Small Segments）

[ステートフル インスペクションの異常（Stateful Inspection Anomalies）]、[連続する小さなセグメント（Consecutive Small Segments）]、および [小さなセグメント サイズ（Small Segment Size）] が有効になっている場合は、小さい TCP セグメントの検出を無視する 1 つ以上のポートのカンマ区切りリストを指定します。このオプションを空白のままにすると、ポートはすべて無視されないように指定されます。

このオプションは、FTD ルーテッドおよびトランスペアレント インターフェイスでは無視されます。

リストには任意のポートを追加できますが、このリストが適用されるのは、TCP ポリシーの [ストリーム再構成を実行（Perform Stream Reassembly on）] ポート リストに指定されているポートのみです。

Require TCP 3-Way Handshake

TCP スリーウェイ ハンドシェイクの完了時に確立されたセッションだけを処理することを指定します。パフォーマンスを向上させ、SYN フラッド攻撃から保護し、部分的に非同期の環境での運用を可能にするには、このオプションを無効にします。確立された TCP セッションには含まれていない情報を送信して誤検出を発生させようとする攻撃を回避するには、このオプションを有効にします。

このオプションにイベントを生成し、インライン展開では、違反パケットをドロップします。するには、ルール 129:20 を有効にします。

3 ウェイ ハンドシェイク タイムアウト（3-Way Handshake Timeout）

[Require TCP 3-Way Handshake] が有効にされている場合、ハンドシェークを完了するまでの時間制限を 0（無制限）～ 86400 秒（24 時間）の範囲で指定します。このオプションの値を変更するには、[TCP 3 ウェイ ハンドシェイク必須（Require TCP 3-Way Handshake）] を有効にする必要があります。

Firepower ソフトウェア デバイスと FTD インライン、インラインタップ、およびパッシブ インターフェイスの場合、デフォルトは 0 です。FTD のルーティッド インターフェイスおよびトランスペアレント インターフェイスの場合、タイムアウトは常に 30 秒であり、ここで設定した値は無視されます。

パケット サイズ パフォーマンスの向上（Packet Size Performance Boost）

再アセンブリ バッファで大きいパケットをキューに入れないようにプリプロセッサを設定します。このオプションはパフォーマンスを向上させますが、攻撃を見逃す可能性があります。1 ～ 20 バイトの小さなパケットを使用した検出回避の試行から保護するには、このオプションを無効にします。すべてのトラフィックが非常に大きなパケットからなるため、そのような攻撃は起こらないと確信できる場合は、このオプションを有効にします。

Legacy Reassembly

パケットを再構成する際に、廃止されたストリーム4プリプロセッサをエミュレートするようにストリーム プリプロセッサを設定します。これにより、ストリーム プリプロセッサで再構成されたイベントを、ストリーム4プリプロセッサで再構成された、同じデータ ストリームに基づくイベントと比較できます。

非同期ネットワーク（Asynchronous Network）

モニタ対象ネットワークが非同期ネットワーク（システムにトラフィックの半分だけが見えるネットワーク）であるかどうかを指定します。このオプションを有効にすると、システムは TCP ストリームを再構成しないため、パフォーマンスが向上します。

このオプションは、FTD ルーテッドおよびトランスペアレント インターフェイスでは無視されます。

クライアント ポートでのストリーム再構成の実行（Perform Stream Reassembly on Client Ports）

接続のクライアント側のポートに基づくストリームの再アセンブリを有効にします。つまり、Web サーバ、メール サーバ、または一般に $HOME_NET で指定された IP アドレスによって定義されたその他の IP アドレスを宛先とするストリームが再アセンブルされます。不正なトラフィックがクライアントから発生する可能性がある場合は、このオプションを使用します。

このオプションは、FTD ルーテッドおよびトランスペアレント インターフェイスでは無視されます。

クライアント サービスでのストリーム再構成の実行（Perform Stream Reassembly on Client Services）

接続のクライアント側のサービスに基づくストリームの再アセンブリを有効にします。不正なトラフィックがクライアントから発生する可能性がある場合は、このオプションを使用します。

選択するクライアント サービスごとに、1つ以上のクライアント ディテクタを有効にする必要があります。デフォルトでは、Cisco が提供するすべてのディテクタはアクティブになっています。関連するクライアント アプリケーションに有効にされているディレクタがない場合、システムは自動的に Cisco 提供のすべてのディテクタをアプリケーションに対して有効にします。そのようなディテクタが提供されていない場合は、最後に変更されたユーザ定義のディテクタをアプリケーションに対して有効にします。

この機能には、保護ライセンスと制御ライセンスが必要です。

このオプションは、FTD ルーテッドおよびトランスペアレント インターフェイスでは無視されます。

サーバ ポートでのストリーム再構成の実行（Perform Stream Reassembly on Server Ports）

接続のサーバ側のポートに基づくストリームの再アセンブリのみを有効にします。つまり、Web サーバ、メール サーバ、または一般に $EXTERNAL_NET で指定された IP アドレスによって定義されたその他の IP アドレスから発信されたストリームが再アセンブリされます。サーバ側の攻撃を監視する必要がある場合は、このオプションを使用します。ポートを指定しないことによって、このオプションを無効にできます。

このオプションは、FTD ルーテッドおよびトランスペアレント インターフェイスでは無視されます。

（注） サービスを徹底的に検査するには、Perform Stream Reassembly on Server Ports フィールドにポート番号を追加することに加えて、Perform Stream Reassembly on Server Services フィールドにサービス名を追加します。たとえば、HTTP サービスを検査するには、Perform Stream Reassembly on Server Ports フィールドにポート番号 80 を追加することに加えて、Perform Stream Reassembly on Server Services フィールドに **'HTTP'** サービスを追加します。

サーバ サービスでのストリーム再構成の実行（Perform Stream Reassembly on Server Services）

接続のサーバ側のサービスに基づくストリームの再アセンブリのみを有効にします。サーバ側の攻撃を監視する必要がある場合は、このオプションを使用します。サービスを指定しないことによって、このオプションを無効にできます。

1 つ以上のディテクタを有効にする必要があります。デフォルトでは、Cisco が提供するすべてのディテクタはアクティブになっています。サービスに有効にされているディレクタがない場合、システムは自動的に Cisco 提供のすべてのディテクタを関連するアプリケーション プロトコルに対して有効にします。そのようなディテクタが提供されていない場合は、最後に変更されたユーザ定義のディテクタをアプリケーション プロトコルに対して有効にします。

この機能には、保護ライセンスと制御ライセンスが必要です。

このオプションは、FTD ルーテッドおよびトランスペアレント インターフェイスでは無視されます。

両方のポートでのストリーム再構成の実行（Perform Stream Reassembly on Both Ports）

接続のクライアント側とサーバ側の両方のポートに基づくストリーム再構成を有効にします。同じポートで、不正なトラフィックがクライアントとサーバ間のいずれの方向でも移動する可能性がある場合は、このオプションを使用します。ポートを指定しないことによって、このオプションを無効にできます。

このオプションは、FTD ルーテッドおよびトランスペアレント インターフェイスでは無視されます。

両方のサービスでのストリーム再構成の実行（Perform Stream Reassembly on Both Services）

接続のクライアント側とサーバ側の両方のサービスに基づくストリーム再構成を有効にします。同じサービスで、不正なトラフィックがクライアントとサーバ間のいずれの方向でも移動する可能性がある場合は、このオプションを使用します。サービスを指定しないことによって、このオプションを無効にできます。

1 つ以上のディテクタを有効にする必要があります。デフォルトでは、Cisco が提供するすべてのディテクタはアクティブになっています。関連するクライアントアプリケーションまたはアプリケーションプロトコルに対して有効になっているディレクタがない場合、システムは自動的に Cisco 提供のすべてのディテクタをアプリケーションまたはアプリケーション プロトコルに対して有効にします。そのようなディテクタが提供されていない場合は、最後に変更されたユーザ定義のディテクタをアプリケーションまたはアプリケーションプロトコルに対して有効にします。

この機能には、保護ライセンスと制御ライセンスが必要です。

このオプションは、FTD ルーテッドおよびトランスペアレント インターフェイスでは無視されます。

トラブルシューティング オプション：最大キューイング バイト（Troubleshooting Options: Maximum Queued Bytes）

トラブルシューティングについてサポートに問い合わせた際に、TCP 接続の片側でキューイングできるデータ量を指定するように指示されることがあります。値 0 は、無制限のバイト数を指定します。

⚠

注意 このトラブルシューティング オプションの設定を変更するとパフォーマンスに影響を与えるので、サポートからガイダンスを受けた場合にのみ変更してください。

Troubleshooting Options：Maximum Queued Segments

トラブルシューティングについてサポートに問い合わせた際に、TCP 接続の片側でキューイングできるデータ セグメントの最大バイト数を指定するように指示されることがあります。値 0 は、無制限のデータ セグメント バイト数を指定します。

⚠

注意 このトラブルシューティング オプションの設定を変更するとパフォーマンスに影響するので、必ずガイダンスに従って実行してください。

関連トピック

Firepower システムの IP アドレス表記法 （20 ページ）
ディテクタのアクティブおよび非アクティブの設定 （2567 ページ）
レイヤ管理 （2051 ページ）
競合と変更：ネットワーク分析および侵入ポリシー （2041 ページ）

TCP ストリームの前処理の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Intrusion Admin

システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。上書き対応オブジェクトを使用すると、子孫ドメインの管理者は、グローバル コンフィギュレーションを自分のローカル環境に調整できます。

始める前に

- カスタム ターゲットベースのポリシーで指定するネットワークが一致しているか、または親のネットワーク分析ポリシーで処理されるネットワーク、ゾーン、および VLAN のサブセットであることを確認します。詳細については、ネットワーク分析プロファイルの詳細設定 （2289 ページ）を参照してください。

ステップ 1 **[Policies]** > **[Access Control]**、次に **[Network Analysis Policy]** または **[Policies]** > **[Access Control]** > **[Intrusion]**、次に **[Network Analysis Policy]** を選択します。

（注） カスタム ユーザ ロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

ステップ 2 変更するポリシーの横にある編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 左側のナビゲーション パネルで [設定（Settings）] をクリックします。

ステップ 4 [トランスポートまたはネットワーク レイヤ プリプロセッサ（Transport/Network Layer Preprocessors）] の下の [TCP ストリームの構成（TCP Stream Configuration）] 設定が無効になっている場合は、[有効化（Enabled）] をクリックして有効にします。

ステップ 5 [TCP ストリームの構成（TCP Stream Configuration）] の横にある編集アイコン（）をクリックします。

ステップ 6 [グローバル設定（Global Settings）] セクションの [パケット タイプ パフォーマンス ブースト（Packet Type Performance Boost）] チェックボックスをオンまたはオフにします。

ステップ 7 次の操作を実行できます。

- ターゲットベースのポリシーの追加：[ターゲット（Targets）] セクションの [ホスト（Hosts）] の横にある追加アイコン（）をクリックします。[ホスト アドレス（Host Address）] フィールドに 1 つまたは複数の IP アドレスを指定します。単一の IP アドレスまたはアドレス ブロックを指定できます。デフォルト ポリシーを含め、合計で最大 255 個のターゲットベースのポリシーを作成できます。作業が完了したら [OK] をクリックします。

- 既存のターゲットベースのポリシーの編集：[ホスト（Hosts）] の下で、編集するポリシーのアドレスをクリックするか、またはデフォルトの構成値を編集します。
- TCP ストリームの前処理オプションの変更：TCP ストリームのプリプロセス オプション （2425 ページ）を参照してください。

注意 サポートから指示がない限り、[最大キュー済みバイト（Maximum Queued Bytes）] または [最大キュー済みセグメント（Maximum Queued Segments）] を変更しないでください。

ヒント クライアント サービス、サーバ サービス、またはその両方に基づくストリーム リアセンブル設定を変更するには、変更するフィールドの内側をクリックするか、そのフィールドの横にある [編集（Edit）] をクリックします。ポップアップ ウィンドウで矢印ボタンを使用して、サービスを [利用可能（Available）] リストと [有効化（Enabled）] リスト間で移動し、[OK] をクリックします。

- 既存のターゲットベースのポリシーの削除：削除するポリシーの横にある削除アイコン（  ）をクリックします。

ステップ 8 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後にキャッシュされた変更は破棄されます。

次のタスク

- イベントを生成し、インライン展開では、違反パケットをドロップします。 を行うには、SMTP ストリーム プリプロセッサ ルール（GID 129）を有効にします。詳細については、侵入ルール状態の設定 （2093 ページ）およびTCP ストリームのプリプロセス オプション （2425 ページ）を参照してください。
- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

関連トピック

レイヤ管理 （2051 ページ）
競合と変更：ネットワーク分析および侵入ポリシー （2041 ページ）
Firepower システムの IP アドレス表記法 （20 ページ）

UDP ストリームの前処理

UDP ストリームの前処理が行われるのは、ルール エンジンがパケットを処理するために使用する UDP ルールに、以下の引数のいずれかを使用した `flow` キーワードが含まれる場合です。

- `Established`
- `To Client`

- `From Client`
- `To Server`
- `From Server`

UDPデータ ストリームは一般に、セッションという観点で考慮されません。UDPはコネクションレス型プロトコルであり、2つのエンドポイントが通信チャネルを確立してデータを交換し、チャネルを終了する手段は提供していません。ただし、ストリームプリプロセッサは、カプセル化 IP データグラム ヘッダーの送信元および宛先 IP アドレス フィールドと、UDP ヘッダーのポート フィールドを使用して、フローの方向を判断し、セッションを識別します。セッションが終了するのは、設定可能なタイマーの時間を超えた場合、または一方のエンドポイントで、もう一方のエンドポイントが到達不能、あるいは要求されたサービスが利用不可という内容の ICMP メッセージを受け取った場合です。

システムは UDP ストリームの前処理に関連するイベントを生成しないことに注意してください。ただし、関連するパケット デコーダ ルールを有効にすることで、UDP プロトコル ヘッダーの異常を検出することができます。

関連トピック

TCP ヘッダー値とストリーム サイズ （2211 ページ）

UDP ストリームのプリプロセス オプション

Timeout

プリプロセッサが非アクティブなストリームを状態テーブルに保持する秒数を指定します。指定した時間内に追加のデータグラムが現れなかった場合、プリプロセッサはそのストリームを状態テーブルから削除します。

FTDデバイスはこのオプションを無視します。その代りに高度なアクセス制御の **Threat Defense サービス ポリシー**の設定を使用します。詳細については、サービス ポリシー ルールの設定 （1183 ページ）を参照してください。

パケット タイプ パフォーマンスの向上（Packet Type Performance Boost）

送信元および宛先ポートの両方を `any` に設定した UDP ルールで `flow` または `flowbits` オプションが使用されている場合を除き、有効化されたルールに指定されていないポートおよびアプリケーション プロトコルのすべてについて、UDP トラフィックを無視するようにプリプロセッサを設定します。このオプションはパフォーマンスを向上させますが、攻撃を見逃す可能性があります。

UDP ストリームの前処理の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Intrusion Admin

ステップ 1 **[Policies]** > **[Access Control]**、次に **[Network Analysis Policy]** または **[Policies]** > **[Access Control]** > **[Intrusion]**、次に **[Network Analysis Policy]** を選択します。

（注） カスタム ユーザ ロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

ステップ 2 編集するポリシーの横にある編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 ナビゲーション パネルで [設定（Settings）] をクリックします。

ステップ 4 [トランスポートまたはネットワーク レイヤ プリプロセッサ（Transport/Network Layer Preprocessors）] の下の [UDP ストリームの構成（UDP Stream Configuration）] が無効になっている場合は、[有効化（Enabled）] をクリックします。

ステップ 5 [UDP ストリームの構成（UDP Stream Configuration）] の横にある編集アイコン（）をクリックします。

ステップ 6 UDP ストリームのプリプロセス オプション （2436 ページ）で説明されているオプションを設定します。

ステップ 7 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後にキャッシュされた変更は破棄されます。

次のタスク

- イベントを生成し、インライン展開では、違反パケットをドロップします。を行うには、関連するパケット デコーダ ルール（GID 116）を有効にします。詳細については、侵入ルール状態の設定 （2093 ページ）およびパケットデコーダ （2417 ページ）を参照してください。
- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

関連トピック

レイヤ管理 （2051 ページ）
競合と変更：ネットワーク分析および侵入ポリシー （2041 ページ）

第 95 章

特定の脅威の検出

次のトピックでは、特定の脅威を検出するためにネットワーク分析ポリシーでプリプロセッサを使用する方法について説明します。

特定の脅威の検出の概要

ネットワーク分析ポリシーでさまざまなプリプロセッサを使用して、モニタ対象ネットワークへの特定の攻撃、たとえば、Back Orifice 攻撃、複数のポートスキャン タイプ、過剰なトラフィックによってネットワークを過負荷状態に陥らせようとするレートベース攻撃などを検出できます。ただし、侵入ルールまたはルールの引数が無効化されたプリプロセッサを必要とする場合、ネットワーク分析ポリシーの Web インターフェイスではプリプロセッサが無効化されたままになりますが、システムは自動的に現在の設定でプリプロセッサを使用します。

侵入ポリシーで設定する機密データ検出を使用して、センシティブな数値データの保護なし送信を検出することもできます。

Back Orifice の検出

Firepower システムは、Back Orifice プログラムの存在を検出するプリプロセッサを提供しています。Back Orifice プログラムにより Windows ホストに対する管理者アクセス権を取得される可能性があります。

Back Orifice 検出プリプロセッサ

Back Orifice プリプロセッサは、UDP トラフィックを分析し、Back Orifice マジック クッキー「*!*QWTY?」を調べます。このクッキーは、パケットの最初の 8 バイトにあり、XOR で暗号化されています。

Back Orifice プリプロセッサには設定ページがありますが、設定オプションはありません。Back Orifice プリプロセッサが有効になっていても、プリプロセッサ ルールを有効にしなければ、イベントを生成し、インライン展開では、違反パケットをドロップします。。

表 *250 : Back Orifice GID:SID*

プリプロセッサ ルール GID:SID	説明
105:1	バック オリフィス トラフィック検出
105:2	バック オリフィス クライアント トラフィック検出
105:3	バック オリフィス サーバ トラフィック検出
105:4	Back Orifice Snort バッファ攻撃検出

Back Orifice の検出

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Intrusion Admin

ステップ 1 **[Policies]** > **[Access Control]**、次に **[Network Analysis Policy]**または**[Policies]** > **[Access Control]** > **[Intrusion]**、次に **[Network Analysis Policy]**を選択します。

（注） カスタムユーザ ロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

ステップ 2 編集するポリシーの横にある編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 ナビゲーション パネルで [設定（Settings）] をクリックします。

ステップ 4 [特定の脅威の検出（Specific Threat Detection）] の下の [Back Orifice の検出（Back Orifice Detection）] が無効になっている場合は、[有効（Enabled）] をクリックします。

（注） Back Orifice にユーザが設定できるオプションはありません。

ステップ 5 最後にポリシーを確定してからこのポリシーで加えた変更を保存するには、[ポリシー情報（Policy Information）] をクリックし、[変更の確定（Commit Changes）] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後の変更は破棄されます。

次のタスク

- イベントを生成し、インライン展開では、違反パケットをドロップします。を行うには、Back Orifice 検出ルール 105:1、105:2、105:3、または 105:4 を有効にします。詳細については、侵入ルールの状態 （2092 ページ）およびBack Orifice 検出プリプロセッサ （2439 ページ）を参照してください。
- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

ポートスキャン検出

ポートスキャンとは、攻撃者が攻撃の準備段階としてよく使用する、ネットワーク調査の形式です。ポートスキャンでは、攻撃者が特別に細工したパケットをターゲットホストに送信します。攻撃者は多くの場合、ホストが応答するパケットを調べることで、ホストでどのポートが開かれているか、そして開かれているポートでどのアプリケーションプロトコルが実行されているかを、直接あるいは推論によって判断できます。

ポートスキャンは、それ自体では攻撃の証拠になりません。実際、攻撃者が使用するポートスキャン手法の中には、正当なユーザがネットワークで使用する可能性があるものもあります。Cisco のポートスキャン ディテクタは、アクティビティのパターンを検出するという方法で、悪意のあるポートスキャンの可能性があるポートスキャンを判別できるように設計されています。

ポートスキャン タイプ、プロトコル、フィルタリング感度レベル

攻撃者がネットワークを調査するために複数の手法を使用することはよくあります。通常、攻撃者は異なる複数のプロトコルを使用して、ターゲットホストからさまざまな応答を引き出します。その目的は、ブロックされた特定タイプのプロトコルを基に、使用できる可能性のあるプロトコルを絞り込んでいくことです。

表 *251 :* プロトコル タイプ

プロトコル	説明
TCP	TCP プローブを検出します。たとえば、SYN スキャン、ACK スキャン、TCP connect() スキャン、および Xmas tree、FIN、NULL といった異常なフラグを組み合わせたスキャンなどです。
UDP	UDP プローブを検出します。たとえば、ゼロ バイトの UDP パケットなどです。

プロトコル	説明
ICMP	ICMP エコー要求（ping）を検出します。
IP	IP プロトコル スキャンを検出します。これらのスキャンは、攻撃者が開いているポートを見つけようとしているのではなく、ターゲット ホストでサポートされている IP プロトコルを発見しようとするためのスキャンであるため、TCP スキャンおよび UDP スキャンとは異なります。

一般に、ターゲットホストの数、スキャン側ホストの数、およびスキャン対象のポートの数に応じて、ポートスキャンは 4 つのタイプに分けられます。

表 *252 :* ポートスキャン タイプ

タイプ	説明
ポート スキャン検出	1 対 1 のポートスキャン。攻撃者が 1 つまたは少数のホストを使用して、単一のターゲット ホスト上の複数のポートをスキャンする場合です。 1 対 1 の ポートスキャンには次のような特徴があります。 • 少数のホストを使用してスキャン • 単一のホストをスキャン • 多数のポートをスキャン このオプションでは、TCP、UDP、および IP ポートスキャンが検出されます。
ポートスイープ	攻撃者が少数のホストを使用して、複数の対象ホスト上で 1 つのポートをスキャンする 1 対複数のポートスイープ。 ポートスイープには次のような特徴があります。 • 少数のホストを使用してスキャン • 多数のホストをスキャン • 少数の固有のポートをスキャン このオプションでは、TCP、UDP、ICMP、および IP ポートスイープが検出されます。

タイプ	説明
デコイ ポートスキャン	攻撃者がスプーフィングされた送信元 IP アドレスと実際にスキャンされた IP アドレスとを組み合わせた 1 対 1 ポートスキャン。 デコイ ポートスキャンには次のような特徴があります。 • 多数のホストを使用してスキャン • 少数のポートを一度だけスキャン • 単一（または少数）のホストをスキャン デコイ ポートスキャン オプションでは、TCP、UDP、および IP プロトコル ポートスキャンが検出されます。
分散型ポートスキャン	複数のホストが開いているポストに対して 1 つのホストをクエリする複数対 1 のポートスキャン。 分散型ポートスキャンには次のような特徴があります。 • 多数のホストを使用してスキャン • 多数のポートを一度だけスキャン • 単一（または少数）のホストをスキャン 分散型ポートスキャン オプションでは、TCP、UDP、および IP プロトコル ポートスキャンが検出されます。

ポートスキャンディテクタは、主にプローブ対象ホストからの否定応答に基づいて、プローブに関する情報を取得します。たとえば、Web クライアントが Web サーバに接続するときに、クライアントはサーバのポート 80/tcp が開いていることを頼りに、そのポートを使用します。ただし、攻撃者がサーバをプローブする場合、そのサーバがウェブ サービスを提供するかどうかを攻撃者があらかじめ知っていることはありません。ポートスキャンディテクタは否定応答（つまり、ICMP 到達不能または TCP RST パケット）を見つけると、その応答を潜在的ポートスキャンとして記録します。否定応答をフィルタリングするデバイス（ファイアウォールやルータなど）の向こう側にターゲット ホストがある場合、このプロセスはさらに困難になります。この場合、ポートスキャンディテクタは、選択された機密レベルに基づいてフィルタリングされた ポートスキャン イベントを生成することができます。

表 *253 :* 感度レベル

レベル	説明
Low	ターゲット ホストからの否定応答だけが検出されます。誤検出を抑えるためには、この機密レベルを選択します。ただし、特定のタイプのポートスキャン（時間をかけたスキャン、フィルタリングされたスキャン）が見逃される可能性があることに注意してください。 このレベルを使用すると、ポートスキャン検出の所要時間が最短になります。
Medium	ホストへの接続数に基づいてポートスキャンが検出されます。したがって、フィルタリングされたポートスキャンを検出できます。ただし、ネットワーク アドレス変換プログラムやプロキシなど、ホストが非常にアクティブな場合は、誤検出が発生する可能性があります。 [Ignore Scanned] フィールドにアクティブなホストの IP アドレスを追加すると、そのような誤検出を軽減できます。 このレベルを使用すると、ポートスキャン検出の所要時間が長くなります。
High	期間に基づいてポートスキャンが検出されます。したがって、時間ベースのポートスキャンを検出できます。ただし、このオプションを使用する場合は、[スキャン済みの無視（Ignore Scanned）] および [スキャナの無視（Ignore Scanner）] フィールドに IP アドレスを指定するという方法で、時間をかけて慎重にディテクタを調整してください。 このレベルを使用すると、ポートスキャン検出の所要時間が大幅に長くなります。

ポートスキャン イベント生成

ポートスキャン検出が有効の場合、さまざまなポートスキャンおよびポートスイープを検出するには、ジェネレータ ID（GID）122 および SID 1 ～ 27 の [Snort ID]（SID）によりルールを有効にする必要があります。

（注） イベントがポートスキャン接続ディテクタによって生成された場合、プロトコル番号は255に設定されます。デフォルトでは、ポートスキャンに特定のプロトコルは関連付けられません。したがって、インターネット割り当て番号局（IANA）にはプロトコル番号が割り当てられません。IANA では 255 を予約番号として指定しているため、ポートスキャン イベントでは、そのイベントに関連付けられている番号がないことを示すために、この番号が使用されます。

表 *254*：ポートスキャン検出 *SID*（*GID 122*）

ポートスキャン タイプ	プロトコル	機密レベル	プリプロセッサ ルール SID
ポート スキャン検出	TCP UDP ICMP IP	Low Medium または High Low Medium または High Low Medium または High Low Medium または High	1 5 21 イベントを生成しません。 イベントを生成しません。 9 13
ポートスイープ	TCP UDP ICMP IP	Low Medium または High Low Medium または High Low Medium または High Low Medium または High	3、27 7 19 23 25 26 11 15
デコイ ポートスキャン	TCP UDP ICMP IP	Low Medium または High Low Medium または High Low Medium または High Low Medium または High	2 6 22 イベントを生成しません。 イベントを生成しません。 10 14

ポートスキャン タイプ	プロトコル	機密レベル	プリプロセッサ ルール SID
分散型ポートスキャン	TCP	Low	4
	UDP	Medium または High	8
	ICMP	Low	。
	IP	Medium または High	24
		Low	イベントを生成しません。
		Medium または High	イベントを生成しません。
		Low	12
		Medium または High	16

ポートスキャン イベント パケット ビュー

関連するプリプロセッサ ルールを有効にすると、ポートスキャン ディテクタによって侵入イベントが生成されるようになります。生成されたイベントは、他のすべての侵入イベントと同じように表示できます。ただし、ポートスキャン イベントのパケット ビューに表示される情報は、他のタイプの侵入イベントとは異なります。

侵入イベント ビューを出発点に、ポートスキャン イベントのパケット ビューまでドリルダウンします。各ポートスキャンイベントは複数のパケットに基づくため、単一のポートスキャンパケットをダウンロードすることはできません。ただし、ポートスキャンパケットビューで、使用可能なすべてのパケット情報を確認できます。

任意の IP アドレスをクリックしてコンテキスト メニューを表示し、[whois（whois）] を選択して、そのIPアドレスでルックアップを実行するか、[ホストプロファイルの表示（View Host Profile）] を選択して、そのホストのホスト プロファイルを表示できます。

表 *255 :* ポートスキャン パケット ビュー

情報	説明
Device	イベントを検出したデバイス。
時刻（Time）	イベントが発生した時刻。
Message	プリプロセッサによって生成されたイベント メッセージ。
送信元 IP	スキャン側ホストの IP アドレス。
Destination IP	スキャンされたホストの IP アドレス。
Priority Count	スキャンされたホストからの否定応答（TCP RST、ICMP 到達不能など）の数。否定応答の数が多ければ多いほど、プライオリティ カウントが高くなります。

情報	説明
Connection Count	ホスト上でアクティブな接続数。この値は、TCP や IP などの接続ベースのスキャンより正確です。
IP カウント	スキャン対象のホストに接続する IP アドレスが変更された回数。たとえば、最初の IP アドレスが 10.1.1.1、2 番目の IP アドレスが 10.1.1.2、3 番目の IP アドレスが 10.1.1.1 の場合、IP カウントは 3 となります。 プロキシや DNS サーバなどのアクティブ ホストでは、この数値はそれほど正確ではありません。
Scanner/Scanned IP Range	スキャン対象ホストまたはスキャン側ホスト（スキャンのタイプに依存）の IP アドレスの範囲。ポートスイープの場合、このフィールドにはスキャン対象ホストの IP アドレス範囲が示されます。ポートスキャンの場合は、スキャン側ホストの IP アドレス範囲が示されます。
Port/Proto Couont	TCP および UDP ポートスキャンの場合は、スキャン対象のポートが変更された回数です。たとえば、スキャンされた最初のポートが 80、2 番目のポートが 8080、3 番目のポートが再び 80 の場合、ポート カウントは 3 となります。 IP プロトコル ポートスキャンの場合は、スキャン対象ホストに接続するために使用されたプロトコルが変更された回数です。
Port/Proto Range	TCP および UDP ポートスキャンの場合は、スキャンされたポートの範囲です。 IP プロトコル ポートスキャンの場合は、スキャン対象ホストへの接続試行で使用された IP プロトコル番号の範囲です。
Open Ports	スキャン対象ホストで開かれた TCP ポート。このフィールドは、ポートスキャンで 1 つ以上の開かれたポートが検出された場合にのみ表示されます。

関連トピック

侵入イベントについて （3057 ページ）

ポートスキャン検出の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Intrusion Admin

ポートスキャン検出の設定オプションを使用して、ポートスキャンディテクタによるスキャンアクティビティのレポート方法を微調整できます。

システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。 上書き対応オブジェクトを使用すると、子孫ドメインの管理者は、グローバルコンフィギュレーションを自分のローカル環境に調整できます。

ステップ 1 **[Policies]** > **[Access Control]**、次に **[Network Analysis Policy]**または**[Policies]** > **[Access Control]** > **[Intrusion]**、次に **[Network Analysis Policy]**を選択します。

（注） カスタム ユーザ ロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

ステップ 2 編集するポリシーの横にある編集アイコン（  ）をクリックします。

代わりに表示アイコン（  ）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 [設定（Settings）] をクリックします。

ステップ 4 [特定の脅威検出（Specific Threat Detection）] の下の [ポートスキャン検出（Portscan Detection）] が無効になっている場合は、[有効化（Enabled）] をクリックします。

ステップ 5 [ポートスキャン検出（Portscan Detection）] の横にある編集アイコン（  ）をクリックします。

ステップ 6 [プロトコル（Protocol）] フィールドで、有効にするプロトコルを指定します。

（注） TCP を介してスキャンを検出するには TCP ストリーム処理が有効になっていること、UDP を介してスキャンを検出するには UDP ストリーム処理が有効になっていることを確認する必要があります。

ステップ 7 [スキャン タイプ（Scan Type）] フィールドで、検出するポートスキャン タイプを指定します。

ステップ 8 [重要度レベル（Sensitivity Level）] リストからレベルを選択します。ポートスキャン タイプ、プロトコル、フィルタリング感度レベル （2441 ページ）を参照してください。

ステップ 9 特定のホストのポートスキャン アクティビティのサインをモニタする場合は、[IP の監視（Watch IP）] フィールドにホストの IP アドレスを入力します。

単一の IP アドレスまたはアドレスブロック、あるいはこれらのいずれかまたは両方をカンマで区切ったリストを指定できます。すべてのネットワーク トラフィックを監視するには、フィールドを空白のままにします。

ステップ 10 ホストをスキャナとして無視するには、[スキャナの無視（Ignore Scanners）] フィールドにホストの IP アドレスを入力します。

単一の IP アドレスまたはアドレスブロック、あるいはこれらのいずれかまたは両方をカンマで区切ったリストを指定できます。

ステップ 11 ホストをスキャンのターゲットとして無視するには、[スキャン対象の無視（Ignore Scanned）] フィールドにホストの IP アドレスを入力します。

単一の IP アドレスまたはアドレスブロック、あるいはこれらのいずれかまたは両方をカンマで区切ったリストを指定できます。

ヒント 特にアクティブなネットワーク上のホストを示すには、[スキャナの無視（Ignore Scanners）] と [スキャン対象の無視（Ignore Scanned）] を使用します。このホストリストは、時間経過とともに変更しなければならない場合があります。

ステップ 12 ミッドストリームでピックアップされたセッションのモニタリングを中断するには、[ACK スキャンの検出（Detect Ack Scans）] チェックボックスをオフにします。

（注） ミッドストリームセッションの検出は ACK スキャンの識別に役立ちますが、大量のトラフィックとパケットのドロップが発生するネットワークでは、誤ってイベントが生成される可能性があります。

ステップ 13 最後にポリシーを確定してからこのポリシーで加えた変更を保存するには、[ポリシー情報（Policy Information）] をクリックし、[変更の確定（Commit Changes）] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後の変更は破棄されます。

次のタスク

- さまざまなポートスキャンおよびポートスイープを検出するためにポートスキャン検出を行う場合は、ルール 122:1 ～ 122:27 を有効にします。詳細については、侵入ルールの状態（2092 ページ）およびポートスキャン イベント生成（2444 ページ）を参照してください。
- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

関連トピック

Firepower システムの IP アドレス表記法 （20 ページ）

レート ベースの攻撃防御

レート ベース攻撃とは、接続の頻度または攻撃を行うための反復試行に依存する攻撃のことです。レート ベースの検出基準を使用することで、レート ベース攻撃が行われていることを検出し、攻撃が発生するごとに対応できます。また、攻撃が収まった後は、通常の検出設定に戻すことができます。

レート ベース フィルタを含めたネットワーク分析ポリシーを設定することで、ネットワーク上のホストを対象とした過剰なアクティビティを検出できます。インライン モードで展開されている管理対象デバイスでこの機能を使用すると、指定の期間だけレートベース攻撃をブロックし、その後イベントだけを生成してトラフィックをドロップしない状態に戻せます。

ネットワークのホストを SYN フラッドから保護するには、SYN 攻撃防止オプションを利用します。一定期間中に認められたパケットの数を基準に、個々のホストまたはネットワーク全体を保護することができます。パッシブ導入のデバイスでは、イベントを生成できます。インライン導入のデバイスでは、不正なパケットをドロップすることもできます。タイムアウト期間の満了時にレート条件に達しなくなっていれば、イベントの生成およびパケットのドロップが停止します。

たとえば、1 つの IP アドレスからの SYN パケットの最大許容数を設定し、このしきい値に達すると、その IP アドレスからの以降の接続を 60 秒間ブロックするように設定できます。

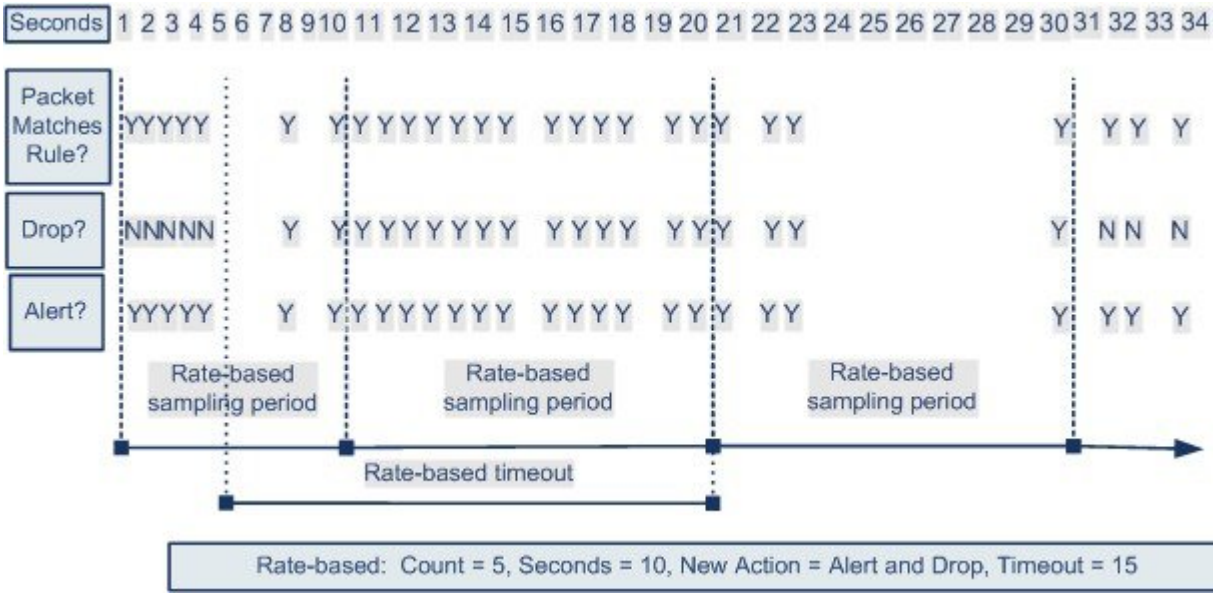
ネットワーク上のホストでの TCP/IP 接続数を制限することで、サービス妨害（DoS）攻撃や、ユーザによる過剰なアクティビティを防止できます。システムが、指定の IP アドレスまたはアドレス範囲で正常に行われている接続が設定された許容数に達したことを検出すると、以降の接続に対してイベントを生成します。タイムアウト期間が満了するまでは、レート条件に達しなくなっても、レートベースのイベント生成が続行されます。インライン導入では、レート条件がタイムアウトになるまでパケットをドロップするように設定できます。

たとえば、1 つの IP アドレスからの同時接続の最大許容数を 10 に設定し、このしきい値に達すると、その IP アドレスからの以降の接続を 60 秒間ブロックするように設定できます。

（注） デバイスは、内部リソースにインスペクションの負荷を分散させます。レートベースの攻撃防御を設定する際は、デバイスごとではなく、リソースごとのトリガー レートを設定します。レート ベースの攻撃防御が期待どおりに機能しない場合、トリガー レートを下げなければならないことが考えられます。正しいレートの決定する方法については、サポートに問い合わせてください。

次の図は、攻撃者がホストにアクセスしようとしている例を示しています。繰り返しパスワードを特定しようとする試みが、レート ベースの攻撃防御が設定されたルールをトリガーします。レートベースの設定は、ルール一致が 10 秒間に 5 回発生した時点で、ルール属性を [Drop and Generate Events] に変更します。新しいルール属性は 15 秒後にタイムアウトします。

タイムアウト後も、そのパケットは後続のレートベースのサンプリング期間にドロップされることに注意してください。サンプリング レートが現在または前回のサンプリング期間中にしきい値を超えている場合は、新しいアクションが続行されます。新しいアクションが元の「イベントの生成」アクションに戻されるのは、サンプリング期間の完了時にサンプルリング レートがしきい値を下回っている場合のみです。



関連トピック

動的侵入ルール状態 （2101 ページ）

レート ベースの攻撃防御の例

トラフィック自体またはシステムが生成するイベントをフィルタリングする手段としては、`detection_filter` キーワード、しきい値および抑制機能も使用できます。レート ベースの攻撃防御は、単独で使用することも、しきい値構成、抑制、または `detection_filter` キーワードと任意に組み合わせて使用することもできます。

`detection_filter` キーワード、しきい値構成または抑制、およびレート ベースの基準のすべてが同じトラフィックに適用される場合もあります。抑制をルールに適用すると、レート ベースの変更が発生しても、指定の IP アドレスに対するイベントの生成は抑制されます。

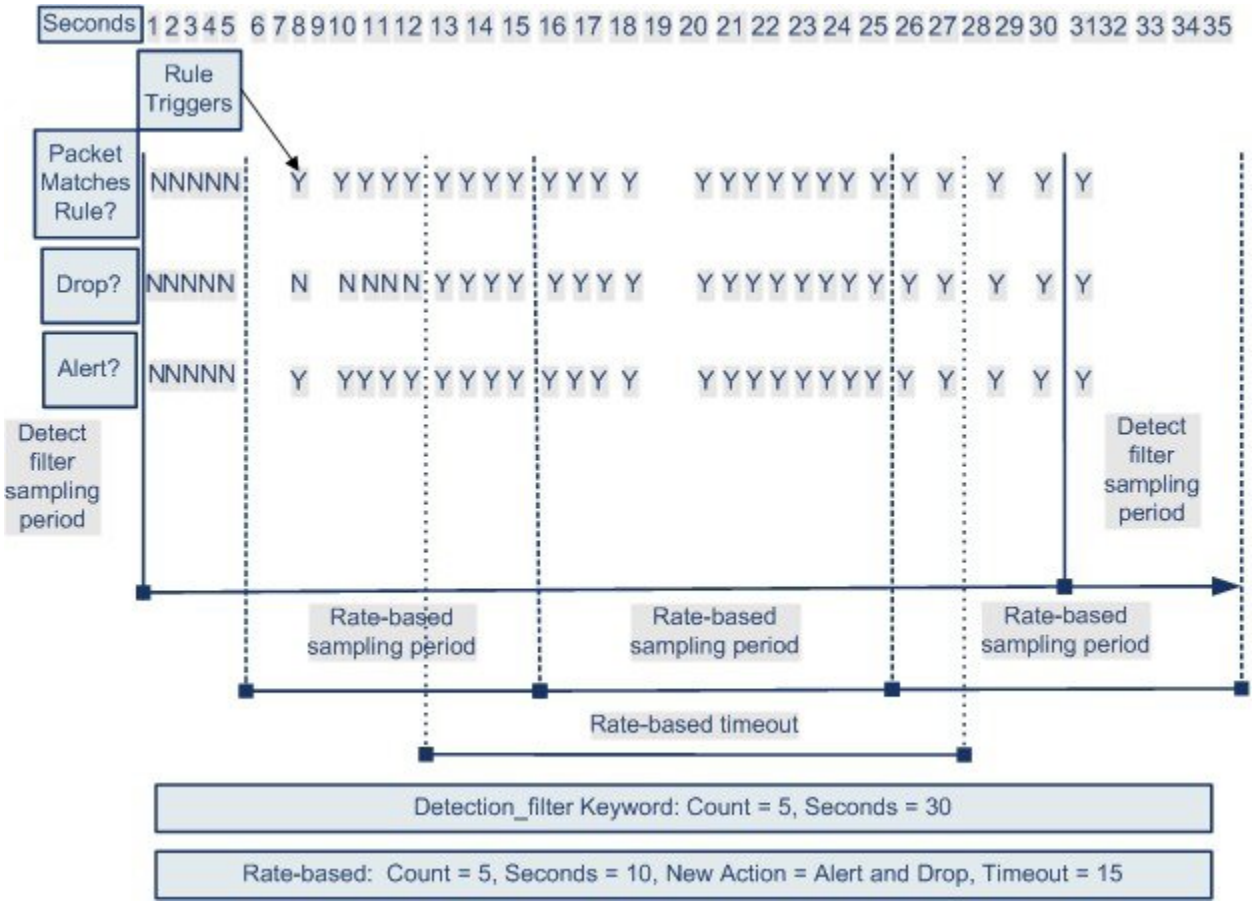
detection_filter キーワードの例

以下に、攻撃者がブルートフォース ログインを仕掛ける例を示します。パスワードの検出試行が繰り返されると、カウントが 5 に設定された `detection_filter` キーワードも含むルールがトリガーされます。このルールには、レート ベース攻撃防止が設定されています。10 秒以内にルールに 5 回ヒットすると、レート ベースの設定により、ルール属性が 20 秒間、[Drop and Generate Events] に変更されます。

図に示されているように、最初の 5 個のパケットがルールに一致しても、イベントは生成されません。それは、レートが `detection_filter` キーワードで指定されたレートを超過するまで、ルールはトリガーされないためです。ルールがトリガーされると、イベント通知が開始されますが、さらに 5 個のパケットが通過するまでは、レート ベースの基準によって新しいルールとして [Drop and Generate Events] がトリガーされることはありません。

レート ベースの基準に一致すると、イベントが生成されて、パケットがドロップされます。これは、レート ベースのタイムアウト期間が満了し、かつレートがしきい値未満になるまで続き

ます。20 秒が経過すると、レート ベース アクションがタイムアウトになります。タイムアウトが発生した後は、それに続くレート ベースのサンプリング期間中、パケットが引き続きドロップされることに注意してください。タイムアウトが発生した時点で、サンプリングされたレートは前のサンプリング期間のしきい値レートを超過しているため、レート ベースのアクションは続行されます。



この例には示されていませんが、[ドロップしてイベントを生成する（Drop and Generate Events）] ルール状態を `detection_filter` キーワードと組み合わせて使用することで、ルールのヒット数が指定のレートに達するとトラフィックのドロップが開始されるようにすることができることにも注意してください。ルールにレート ベースの設定を使用するかどうかを決定する際は、ルールを [ドロップしてイベントを生成する（Drop and Generate Events）] に設定した場合の結果と `detection_filter` キーワードを含めた場合の結果が同じであるかどうか、あるいは侵入ポリシーでレートとタイムアウトの設定を管理する必要があるかどうかを検討してください。

関連トピック

侵入ルールの状態 （2092 ページ）

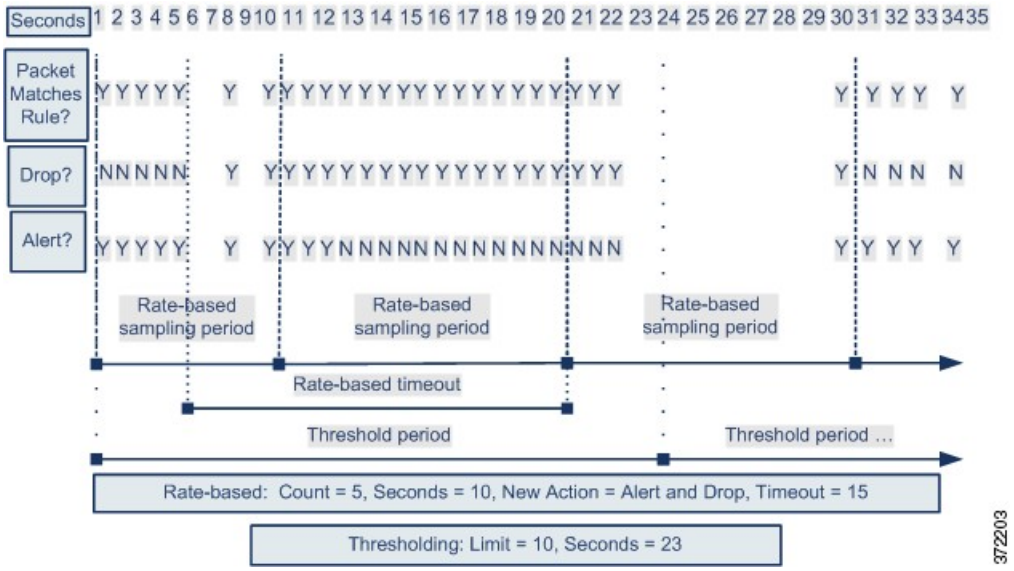
ダイナミック ルール状態のしきい値構成または抑制の例

以下に、攻撃者がブルート フォース ログインを仕掛ける例を示します。パスワードを検出しようとする試行が繰り返されると、レートベース攻撃防止が設定されたルールがトリガーされ

ます。10 秒以内にルールに 5 回ヒットすると、レート ベースの設定により、ルール属性が15秒間、[Drop and Generate Events] に変更されます。さらに、上限しきい値により、ルールで生成可能なイベントの数が 23 秒間で 10 に制限されます。

図に示されているように、最初の5個のパケットが一致すると、ルールはイベントを生成します。5 個のパケットがルールに一致した後、レート ベースの基準が新しいアクションとして [Drop and Generate Events] をトリガーし、次の 5 個のパケットがルールに一致した時点でイベントが生成され、パケットをドロップします。10個目のパケットがルールに一致すると、上限しきい値に達するため、システムは残りのパケットについてはイベントを生成することなくドロップします。

タイムアウトが発生した後は、それに続くレートベースのサンプリング期間中、パケットが引き続きドロップされることに注意してください。サンプリング レートが現在または前回のサンプリング期間中にしきい値レートを超えた場合は、新しいアクションが続行されます。新しいアクションが元の [Generate Events] アクションに戻されるのは、サンプリング期間の完了時にサンプルリング レートがしきい値を下回っている場合のみです。



この例には示されていませんが、しきい値に達した後に、レートベースの基準によって新しいアクションがトリガーされた場合、システムはアクションが変更されたことを示す単一のイベントを生成することに注意してください。したがって、たとえば上限しきい値の 10 に達してシステムがイベントの生成を停止し、14 番目のパケットでアクションが [イベントを生成する（Generate Events）] から [ドロップしてイベントを生成する（Drop and Generate Events）] に変更されると、システムはアクションが変更されたことを示す11番目のイベントを生成します。

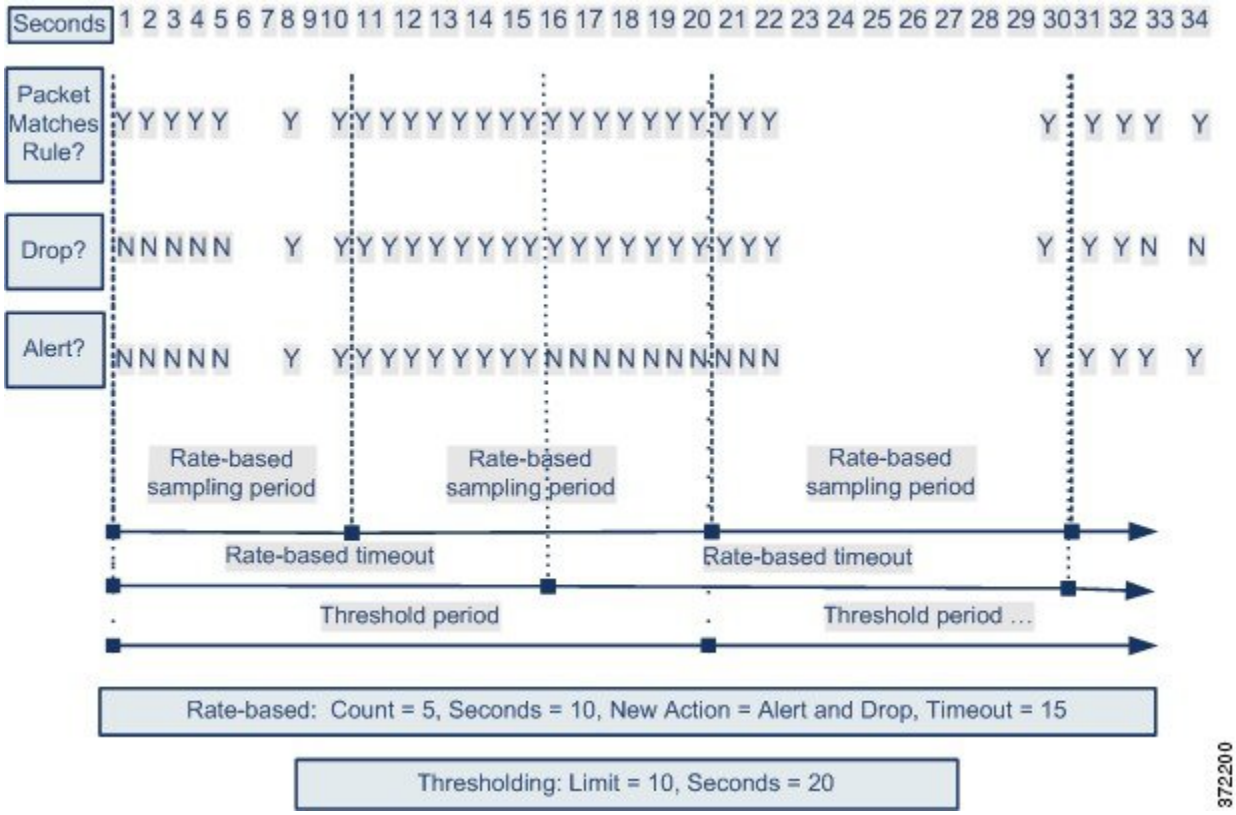
ポリシー全体のレート ベース検出としきい値構成または抑制の例

以下に、ネットワーク上のホストに対して、攻撃者がサービス妨害（DoS）攻撃を仕掛ける例を示します。同じ送信元から多数のホストに対して同時接続が行われると、ポリシー全体の [Control Simultaneous Connections] 設定がトリガーされます。この設定は、1 つの送信元からの接続数が 10 秒間で 5 つに達すると、イベントを生成して悪意のあるトラフィックをドロップ

します。さらに、グローバル上限しきい値により、ルールまたは設定で生成可能なイベントの数が 20 秒間で 10 件に制限されます。

この図に示されているように、ポリシー全体の設定により、一致する最初の 10 個のパケットに対してイベントが生成され、トラフィックがドロップされます。10個目のパケットがルールに一致すると、上限しきい値に達するため、システムは残りのパケットについてはイベントを生成せずにドロップします。

タイムアウトが発生した後は、それに続くレートベースのサンプリング期間中、パケットが引き続きドロップされることに注意してください。サンプリングされたレートが、現在または前のサンプリング期間のしきい値レートを超過している場合、レートベースのアクションによるイベントの生成とトラフィックのドロップが続行されます。レート ベース アクションが停止するのは、サンプリング期間が完了した時点で、サンプリングされたレートがしきい値レートを下回っている場合のみです。



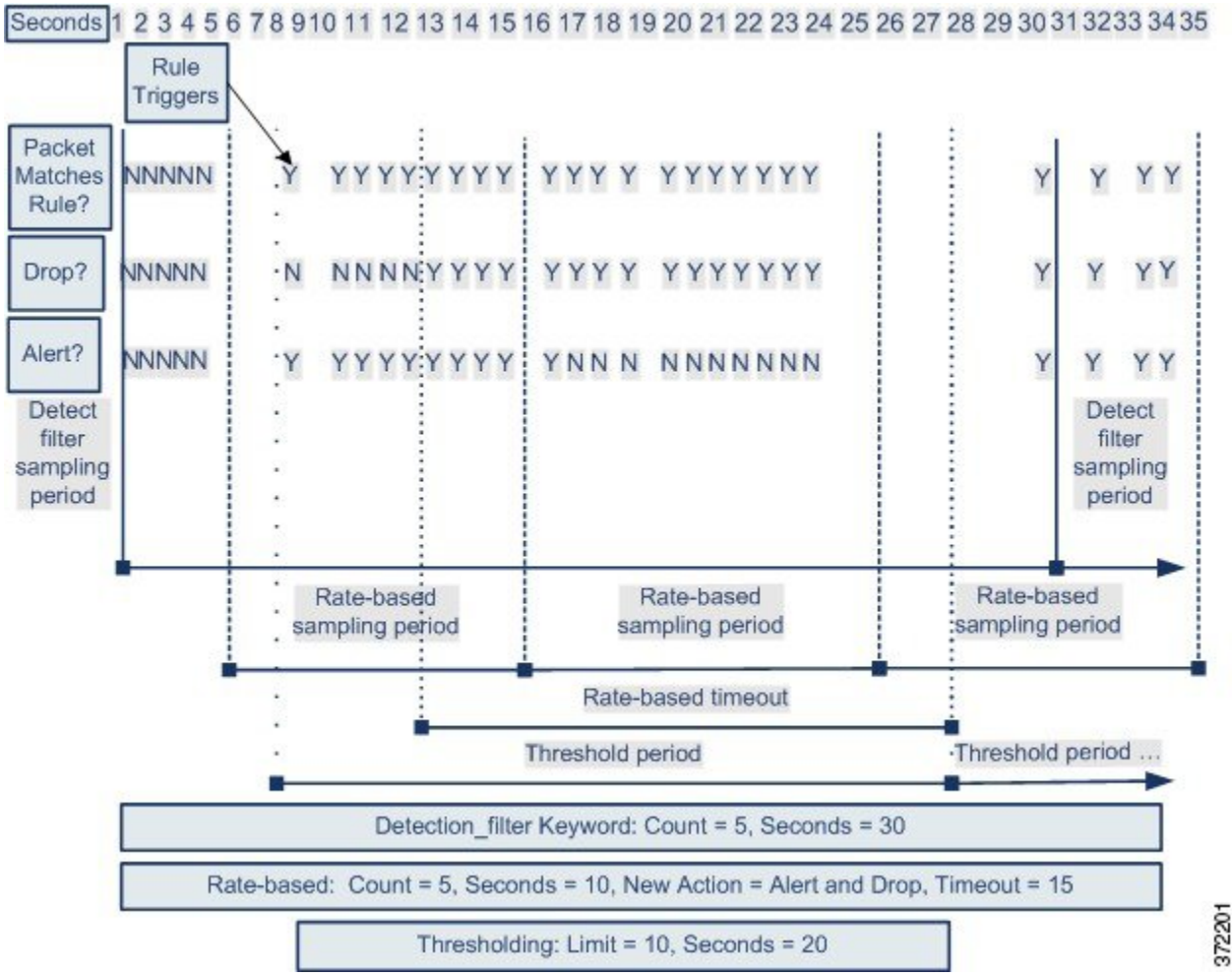
この例には示されていませんが、しきい値に達した後に、レートベースの基準によって新しいアクションがトリガーされた場合、システムはアクションが変更されたことを示す単一のイベントを生成することに注意してください。したがって、たとえば上限しきい値の 10 に達してシステムがイベントの生成を停止し、14 番目のパケットでアクションが [ドロップしてイベントを生成する（Drop and Generate Events）] に変更されると、システムはアクションが変更されたことを示す 11 番目のイベントを生成します。

複数のフィルタリング方法によるレート ベース検出の例

以下に、攻撃者がブルートフォース ログインを仕掛ける例で、`detection_filter` キーワード、レート ベースのフィルタリング、およびしきい値が相互作用する場合を説明します。パスワードの検出試行が繰り返されると、カウントが 5 に設定された `detection_filter` キーワードを含むルールがトリガーされます。このルールには、レート ベース攻撃防止も設定されています。その設定では、15 秒間にルールのヒット数が 5 に達すると、ルール属性が 30 秒間、[Drop and Generate Events] に変更されます。さらに、上限しきい値により、ルールによって生成されるイベントは 30 秒間で 10 件に制限されます。

図に示されているように、最初の 5 個のパケットがルールに一致しても、イベント通知は行われません。それは、`detection_filter` キーワードで指定されたレートを超過するまで、ルールはトリガーされないためです。ルールがトリガーされると、イベント通知が開始されますが、さらに 5 個のパケットが通過するまでは、レート ベースの基準によって新しいルールとして [Drop and Generate Events] がトリガーされることはありません。レート ベースの基準が満たされると、システムは 11 個目から 15 個目のパケットに対してイベントを生成し、パケットをドロップします。15 個目のパケットがルールに一致すると、上限しきい値に達するため、システムは残りのパケットについてはイベントを生成せずにドロップします。

レート ベースのタイムアウトが発生した後は、それに続くレート ベースのサンプリング期間中、パケットが引き続きドロップされることに注意してください。サンプリング レートが前回のサンプリング期間中にしきい値レートを超えた場合は、新しいアクションが続行されます。



レート ベースの攻撃防御オプションと設定

レート ベース攻撃の防御では、異常なトラフィック パターンを識別して、そのトラフィックが正当な要求に与える影響を最小限に抑えるようにします。一般に、レート ベース攻撃には次のいずれかの特性があります。

- 任意のトラフィックに、ネットワーク上のホストに対して過剰な未完了接続が含まれています。これは、SYN フラッド攻撃を意味します。
- 任意のトラフィックには、ネットワーク上のホストに対して過剰な接続が含まれています。これは、TCP/IP 接続フラッド攻撃を意味します。
- 1 つ以上の特定の宛先 IP アドレスへのトラフィック、または 1 つ以上の特定の送信元 IP アドレスからのトラフィックで、ルールとの一致が過剰に発生します。
- すべてのトラフィックで、特定のルールとの一致が過剰に発生します。

ネットワーク分析ポリシーでは、ポリシー全体に対して SYN フラッドまたは TCP/IP 接続フラッドのいずれかの検出を設定することができます。または個々の侵入ルールもしくはプリプロセッサルールに対してレート ベース フィルタを設定できます。GID 135 ルールに手動でレート ベース フィルタを追加すること、またはルールの状態を変更することはできない点に注意してください。GID 135 のルールでは、クライアントを送信元の値、サーバを宛先の値として使用します。

（注） デバイスは、内部リソースにインスペクションの負荷を分散させます。レートベースの攻撃防御を設定する際は、デバイスごとではなく、リソースごとのトリガー レートを設定します。レート ベースの攻撃防御が期待どおりに機能しない場合、トリガー レートを下げなければならないことが考えられます。正しいレートの決定する方法については、サポートに問い合わせてください。

[SYN 攻撃の防御（SYN Attack Prevention）] オプションを有効にすると、ルール 135:1 もアクティブになります。このルールを手動でアクティブにしても効果はありません。ルール状態は常に [Disabled] として表示され、変更されることはありません。このオプションを有効にすると、定義されたレート条件を超過した時点で、ルールによってイベントが生成されます。

[同時接続の制御（Control Simultaneous Connections）] オプションを有効にすると、ルール 135:2 および 135:3 もアクティブになります。このルールを手動でアクティブにしても効果はありません。ルール状態は常に [無効（Disabled）] として表示され、変更されることはありません。定義されたレート条件を超過した時点で、135:2 のルールによってイベントが生成されます。セッションが終了するかタイムアウトすると、ルール 135:3 はイベントを生成します。

各レート ベース フィルタには、以下のコンポーネントが含まれます。

- ポリシー全体またはルール ベースの送信元/宛先の設定の場合、ネットワーク アドレスの指定
- 特定の秒数以内のルール一致のカウントとして設定されるルール一致率
- レートを超過した場合に実行する新しいアクション

  ポリシー全体に対してレート ベースを設定すると、システムはレート ベース攻撃を検出した時点でイベントを生成します。インライン展開では、トラフィックをドロップすることもできます。個々のルールにレート ベース アクションを設定する場合は、[イベントの生成（Generate Events）]、[イベントのドロップと作成（Drop and Generate Events）]、[無効（Disable）] の 3 つの利用可能なアクションから選択できます。
- タイムアウト値として設定されるアクションの継続期間

新しいアクションは、開始されると、レートがその期間内に設定されたレートを下回っても、タイムアウトに達するまで継続されることに注意してください。タイムアウト期間が満了し、レートがしきい値を下回っている場合、ルールのアクションはそのルールに最初に設定されたアクションに戻ります。ポリシー全体に適用される設定の場合、アクションは、トラフィックと一致する個々のルールのアクションに戻ります。一致するアクションがなければ、アクションは停止されます。

インライン導入では、攻撃を一時的または永続的にブロックするようにレートベース攻撃防止を設定できます。レートベースの設定が使用されていない場合、ルールが [Generate Events] に設定されていればイベントが生成されますが、パケットがドロップされることはありません。ただし、攻撃トラフィックが、レートベースの基準が設定されたルールと一致した場合は、そのようなルールが最初から [Drop and Generate Events] に設定されていなかったとしても、レートアクションがアクティブな期間にパケットのドロップが実行されます。

（注） レートベースのアクションは、無効なルールを有効にしたり、無効なルールと一致したトラフィックをドロップしたりできません。ただし、ポリシー レベルでレート ベース フィルタを設定すると、指定した期間内の過剰な数の SYN パケットまたは SYN/ACK インタラクションを含むトラフィックに対してイベントを生成するか、イベントを生成してトラフィックをドロップすることができます。

同じルールに対して複数のレートベースのフィルタを定義できます。侵入防御ポリシーで最初にリストされているフィルタに、最大のプライオリティが割り当てられます。2 つのレート ベース フィルタ アクションが競合する場合は、最初のレート ベース フィルタのアクションが実行されることに注意してください。同様に、ポリシー全体に対するレート ベース フィルタと個々のルールに設定されたレート ベース フィルタが競合する場合は、ポリシー全体のレート ベース フィルタが優先されます。

関連トピック

[ルール（Rule）] ページからの動的ルール状態の設定 （2103 ページ）

レートベースの攻撃防御、検出フィルタリング、しきい値処理または抑制

キーワード `detection_filter` により、ルールに一致するしきい値が指定の時間内に発生するまで、ルールのトリガーを阻止します。ルールに `detection_filter` キーワードが含まれている場合、システムは指定の期間、ルールのパターンに一致する着信パケットの数を追跡します。システムはそのルールについて、特定の送信元 IP アドレスからのヒット数、または特定の宛先 IP アドレスからのヒット数をカウントできます。レートがルールのレートを超過すると、そのルールに関するイベント通知が開始されます。

しきい値処理と抑制を用いて、ルール、送信元または宛先に関するイベント通知数を制限することまたはそのルールをすべて一緒に通知を抑制することで、過剰なイベントを低減できます。また、オーバーライドする特定のしきい値がない各ルールに適用するグローバルルールのしきい値を設定できます。

ルールに抑制を提供する場合、ポリシー全体またはルールにより指定されたレートベースの設定であるため、レートベースでアクションの変更が発生した場合でも、システムは、すべての適用可能な IP アドレスのそのルールのイベント通知を抑制します。

関連トピック

侵入イベントのしきい値 （2094 ページ）
侵入ポリシーの抑制の設定 （2099 ページ）
グローバル ルールのしきい値の基本 （2129 ページ）

レートベース攻撃防止の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Intrusion Admin

ポリシー レベルでレートベース攻撃防止を設定することで、SYN フラッド攻撃を阻止できます。特定の送信元からの過剰な接続、または特定の宛先への過剰な接続を阻止することもできます。

ステップ 1 **[Policies]** > **[Access Control]**、次に **[Network Analysis Policy]**または**[Policies]** > **[Access Control]** > **[Intrusion]**、次に **[Network Analysis Policy]**を選択します。

（注） カスタム ユーザ ロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

ステップ 2 編集するポリシーの横にある編集アイコン（  ）をクリックします。

代わりに表示アイコン（  ）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 [設定（Settings）] をクリックします。

ステップ 4 [特定の脅威検出（Specific Threat Detection）] の下の [レートベース攻撃防止（Rate-Based Attack Prevention）] が無効になっている場合は、[有効化（Enabled）] をクリックします。

ステップ 5 [レートベース攻撃防止（Rate-Based Attack Prevention）] の横にある編集アイコン（  ）をクリックします。

ステップ 6 次の 2 つの選択肢があります。

- ホストのフラッディングを目的とする不完全な接続を防ぐには、[SYN 攻撃の防止（SYN Attack Prevention）] の下にある [追加（Add）] をクリックします。
- 過剰な数の接続を防ぐには、[同時接続の制御（Control Simultaneous Connections）] の下にある [追加（Add）] をクリックします。

ステップ 7 トラフィックを追跡する方法を指定します。

- 特定の送信元または送信元の範囲からのすべてのトラフィックを追跡するには、[追跡対象（Track By）] ドロップダウン リストから [送信元（Source）] を選択し、[ネットワーク（Network）] フィールドに単一の IP アドレスまたはアドレス ブロックを入力します。
- 特定の宛先または宛先の範囲へのすべてのトラフィックを追跡するには、[追跡対象（Track By）] ドロップダウン リストから [宛先（Destination）] を選択し、[ネットワーク（Network）] フィールドに単一の IP アドレスまたはアドレス ブロックを入力します。

（注） システムは、[ネットワーク（Network）] フィールドに含まれる各 IP アドレスのトラフィックを個別に追跡します。ある特定の IP アドレスからの設定されたレートを超過するトラフィックがある場合、その IP アドレスに関するイベントだけが生成されることになります。例として、ネットワーク設定で `10.1.0.0/16` の送信元 CIDR ブロックを設定し、10 個の同時接続が開始された時点でイベントを生成するようにシステムを設定するとします。10.1.4.21 から 8 つの接続が開始され、10.1.5.10 から 6 つの接続が開始されている場合、いずれの送信元も開始されている接続がトリガーを引き起こす数になっていないため、システムはイベントを生成しません。一方、10.1.4.21 から 11 個の同時接続が開始されている場合、システムは 10.1.4.21 からの接続に対してだけイベントを生成します。

システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。 上書き対応オブジェクトを使用すると、子孫ドメインの管理者は、グローバル コンフィギュレーションを自分のローカル環境に調整できます。

ステップ 8 レート追跡設定をトリガーとして使用するレートを指定します。

- SYN 攻撃に対する構成の場合は、[レート（Rate）] フィールドに、一定の秒数あたりの SYN パケット数を入力します。
- 同時接続に対する構成の場合は、[カウント（Count）] フィールドに、接続数を入力します。

デバイスは、内部リソースにインスペクションの負荷を分散させます。レート ベースの攻撃防御を設定する際は、デバイスごとではなく、リソースごとのトリガー レートを設定します。レートベースの攻撃防御が期待どおりに機能しない場合、トリガー レートを下げなければならないことが考えられます。正しいレートの決定する方法については、サポートに問い合わせてください。

ステップ 9 レートベース攻撃防止設定に一致するパケットをドロップするには、[ドロップ（Drop）] チェックボックスをオンにします。

ステップ 10 [タイムアウト（Timeout）] フィールドに、イベント生成のタイムアウト期間を入力します。この期間を経過すると、SYN または同時接続のパターンに一致するトラフィックに対するイベント生成が（該当する場合はドロップも）停止されます。

注意 インライン展開では、大きいタイムアウト値を指定するとホストへの接続が完全にブロックされる可能性があります。

ステップ 11 [OK] をクリックします。

ステップ 12 最後にポリシーを確定してからこのポリシーで加えた変更を保存するには、[ポリシー情報（Policy Information）] をクリックし、[変更の確定（Commit Changes）] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後の変更は破棄されます。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

関連トピック

Firepower システムの IP アドレス表記法 （20 ページ）

第 96 章

適応型プロファイル

ここでは、適応型プロファイルの設定方法について説明します。

アダプティブ プロファイルについて

アダプティブプロファイルを使うと、次の操作を実行できます。

- アクセス コントロール ルールは AMP を含むアプリケーション制御およびファイル制御が可能になり、侵入ルールはサービス メタデータを使用できるようになります。

  注意 アクセス コントロール ルールが AMP を含むアプリケーション制御およびファイル制御を行い、侵入ルールがサービス メタデータを使用するためには、適応型プロファイルの設定 （2466ページ）で説明されているように、アダプティブ プロファイルが**必ず**有効になっている（デフォルト状態）必要があります。

- パッシブ展開では、アダプティブプロファイルの更新を有効にして、宛先ホストのオペレーティング システムに従って IP トラフィックに最適化とリアセンブルを行います。

  （注） インライン展開では、アダプティブ プロファイルの更新を有効にする代わりに、インライン正規化プリプロセッサを設定し、[TCP ペイロードの正規化（Normalize TCP Payload）] オプションを有効にすることを推奨します。

アダプティブプロファイルの更新

通常、システムはネットワーク分析ポリシーの静的な設定を使用して、トラフィックの前処理と分析を行います。アダプティブプロファイルの更新では、ネットワーク検出で検出したホスト情報またはサードパーティからインポートしたホスト情報に合わせて、システムが処理動作を変更します。

プロファイルの更新は、ネットワーク分析ポリシーに手動で設定可能なターゲットベースプロファイルと同様に、ターゲット ホストのオペレーティング システムと同じ方法で、IP パケットの最適化およびストリームのリアセンブルを行うのに役立ちます。その後、侵入ルールエンジンは宛先ホストによって使用されるものと同じ形式でデータを分析します。

手動で設定されたターゲットベースのプロファイルは、選択したデフォルトのオペレーティングシステムか固有のホストに構築したプロファイルのいずれかに適用されます。ただし、プロファイルの更新は、ターゲット ホストのホスト プロファイルのオペレーティング システムに基づいて適切なオペレーティング システム プロファイルに切り替わります。

10.6.0.0/16 サブネット向けにプロファイルの更新を設定し、Linux にデフォルトの IP 最適化ターゲットベース ポリシーを設定するシナリオを考えてみます。設定を構成する Firepower Management Center には 10.6.0.0/16 サブネットを含むネットワーク マップがあります。

- システムが 10.6.0.0/16 サブネットにないホスト A からのトラフィックを検出すると、Linux ターゲットベース ポリシーを使用して IP フラグメントのリアセンブルを行います。
- システムが 10.6.0.0/16 サブネット上にあるホスト B からのトラフィックを検出すると、ネットワーク マップからホスト B のオペレーティング システム データを取得します。システムは、このオペレーティング システムに基づいたプロファイルを使用し、ホスト B を宛先とするトラフィックを最適化します。

アダプティブプロファイルの更新および Firepower 推奨ルール

アダプティブ プロファイルの更新機能は、アクセス コントロール ポリシーの詳細設定で、そのアクセス コントロール ポリシーによって呼び出されるすべての侵入ポリシーにグローバルに適用されます。Firepower 推奨ルールの機能は、設定する個々の侵入ポリシーに適用されます。

Firepower 推奨ルールと同様に、プロファイルの更新はルールのメタデータをホスト情報と比較し、ルールを特定のホストに適用すべきかどうかを判別します。ただし、Firepower 推奨ルールがその情報を使用してルールの有効化または無効化を行うための推奨事項を提供するのに対して、プロファイルの更新はその情報を使用して特定のトラフィックに特定のルールを適用します。

Firepower 推奨ルールでは、提案された変更をルール状態に実装するために、ユーザの対話が必要になります。一方、プロファイルの更新は侵入ポリシーを変更しません。プロファイル更新に基づくルールの処理は、パケット単位で行われます。

さらに、Firepowerでは、推奨ルールが無効化されたルールを有効にできます。これに対して、プロファイルの更新では、侵入ポリシーですでに有効になっているルールの適用のみに影響を与えます。プロファイルの更新 はルール状態を変更することはありません。

プロファイルの更新と Firepower 推奨ルールは組み合わせて使用できます。侵入ポリシーを展開すると、プロファイルの更新はルールの状態を使用して適用の候補に含めるかどうかを判別し、推奨事項の承認または拒否はそのルール状態に反映されます。両方の機能を使用して、監視対象の各ネットワークに最適なルールを有効化または無効化することができ、特定のトラフィックに対する有効化したルールの適用を最も効率的に行うことができます。

関連トピック

Firepower 推奨ルールについて （2107 ページ）

適応型プロファイルのオプション

有効（Enable）

次のことを可能にします。

- アクセス コントロール ルールで AMP を含めたアプリケーションとファイルの制御を実行する
- 侵入ルールでサービス メタデータを使用する

プロファイルの更新を有効にする（Enable Profile Updates）

パッシブ展開で、プロファイルの更新を有効にして、ネットワーク マップでホストが使用するオペレーティング システムのプロファイルに応じて IP トラフィックがデフラグおよびリアセンブルされるようにします。

アダプティブ プロファイル - 属性の更新間隔（Adaptive Profiles - Attribute Update Interval）

プロファイルの更新を有効にすると、Firepower Management Center から管理対象デバイスに対するネットワーク マップ データの同期の頻度を分単位で制御することができます。システムはデータを使用して、トラフィックを処理する際に使用するプロファイルを判別します。このオプションの値を大きくすると、大規模なネットワークでパフォーマンスを向上させることができます。

アダプティブ プロファイル - ネットワーク（Adaptive Profiles - Networks）

任意で、プロファイルの更新を有効にすると、IP アドレス、アドレス ブロック、およびネットワーク変数のカンマ区切りリストに対する プロファイルの更新 を制限して、パフォーマンスを向上させることができます。ネットワーク変数を使用すると、アクセス コントロール ポ

リシーのデフォルトの侵入ポリシーにリンクされている変数セットの変数の値が使用されるようになります。たとえば、**192.168.1.101**、**192.168.4.0/24**、**$HOME_NET** というように入力することができます。

（注） システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。上位ポリシーでプロファイルの更新を有効にして適用する場合、Cisco では、デフォルトのネットワークの制約 **0.0.0.0/0** を保持するか、または値 any を指定してネットワーク変数を使用することをお勧めしています。この設定により、すべてのサブドメインのすべてのモニタ対象ホストに プロファイルの更新 が適用されるようになります。

関連トピック

デフォルトの侵入ポリシー （2287 ページ）
Firepower システムの IP アドレス表記法 （20 ページ）
変数セット （538 ページ）

適応型プロファイルの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Access Admin/Network Admin

パッシブ展開では、アダプティブ プロファイルの更新を設定することをお勧めします。インライン展開の場合、インライン正規化プリプロセッサの設定で [TCP ペイロードの正規化（Normalize TCP Payload）] オプションを有効にします。

注意 アクセス コントロール ルールが AMP を含むアプリケーション制御およびファイル制御を行い、侵入ルールがサービス メタデータを使用するためには、この手順で説明されているように、アダプティブ プロファイルが**必ず**有効になっている（デフォルト状態）必要があります。

ステップ 1 アクセス コントロール ポリシー エディタで [詳細（Advanced）] タブをクリックし、[検出拡張の設定（Detection Enhancement Settings）] セクションの横にある編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ポリシーから継承され、設定を変更する権限がありません。設定がロック解除されている場合は、[Inherit from base policy] をオフにして、編集を有効にします。

ステップ 2 適応型プロファイルのオプション（2465 ページ）の説明に従って適応型プロファイルのオプションを設定します。

ステップ 3 [OK] をクリックします。

ステップ 4 [保存（Save）] をクリックしてポリシーを保存します。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

関連トピック

インライン正規化プリプロセッサ （2403 ページ）
Snort® の再起動シナリオ （450 ページ）

第 XXII 部

検出とアイデンティティ

第 97 章

ネットワーク検出とアイデンティティの概要

次のトピックでは、ネットワーク検出およびアイデンティティ ポリシーとデータの概要を示します。

ホスト、アプリケーション、およびユーザのデータの検出について

Firepower システムは、ネットワーク検出およびアイデンティティ ポリシーを使用して、ネットワーク トラフィックのホスト、アプリケーション、およびユーザのデータを収集します。特定のタイプの検出およびアイデンティティ データを使用すると、ネットワーク アセットの包括的なマップを作成し、フォレンジック分析、動作プロファイリング、アクセス制御を行い、組織が影響を受ける脆弱性およびエクスプロイトに対応して軽減することができます。

ホストおよびアプリケーション データ

ホストやアプリケーションデータは、ネットワーク検出ポリシーの設定に従ってホストのアイデンティティ ソースとアプリケーション ディテクタによって収集されます。管理対象デバイスは、指定したネットワーク セグメントのトラフィックを確認します。

詳細については、ホストおよびアプリケーション検出の基礎 （2473 ページ）を参照してください。

ユーザ データ（User Data）

ユーザ データはネットワーク検出およびアイデンティティ ポリシーの設定に従ってユーザのアイデンティティ ソースによって収集されます。データはユーザ認識とユーザ制御のために使用できます。

詳細については、ユーザアイデンティティについて（2481ページ）を参照してください。

検出データとアイデンティティ データをロギングすることにより、次のようなFirepowerシステムのさまざまな機能を活用できます。

- ネットワーク アセットとトポロジの詳細を示すネットワーク マップを表示します。その際、ホストとネットワーク デバイス、ホスト属性、アプリケーション プロトコル、または脆弱性をグループ化して表示できます。
- アプリケーション、レルム、ユーザ、ユーザ グループ、およびISE属性の各条件を使ってアクセス コントロール ルールを作成することにより、アプリケーション制御およびユーザ制御を実行します。
- 検出されたホストで利用可能なすべての情報の完全なビューであるホストプロファイルを表示します。
- （さまざまな機能の1つとして）ネットワーク アセットとユーザ アクティビティの概要を示すダッシュボードを表示します。
- システムによって記録された検出イベントとユーザアクティビティに関する詳細情報を表示します。
- ホストおよびそこで実行されているサーバ/クライアントと、被害を及ぼす可能性のあるエクスプロイトとを関連付けます。

  これにより、脆弱性を特定して軽減したり、ネットワークに対する侵入イベントの影響を評価したり、ネットワークアセットを最大限に保護できるように侵入ルール状態を調整したりできます。
- システムで特定の影響フラグ付きの侵入イベントまたは特定のタイプの検出イベントが生成された場合に、電子メール、SNMPトラップ、またはsyslogによるアラートを発行します。
- 許可されたオペレーティング システム、クライアント、アプリケーション プロトコル、およびプロトコルのホワイトリストを使用して組織のコンプライアンスをモニタします。
- システムが検出イベントを生成するかユーザアクティビティを検出したときにトリガーして相関イベントを生成するルールを使って、相関ポリシーを作成します。
- 該当する場合、NetFlow接続をロギングして使用します。

関連トピック

ホスト ID ソース （2495 ページ）
アプリケーションの検出 （2547 ページ）
ユーザ アイデンティティ ソース

ホストおよびアプリケーション検出の基礎

ネットワーク検出ポリシーを設定すると、ホストおよびアプリケーション検出を実行できます。

詳細については、概要：ホストのデータ収集（2495ページ）および概要：アプリケーション検出（2547ページ）を参照してください。

オペレーティング システムおよびホスト データのパッシブ検出

パッシブ検出は、システムがネットワーク トラフィック（およびエクスポートされたNetFlowデータ）を分析してネットワーク マップにデータを取り込む際のデフォルト方式です。パッシブ検出では、ネットワーク アセットに関するコンテキスト情報（オペレーティング システムや実行中のアプリケーションなど）が提供されます。

モニタ対象のホストからのトラフィックが、ホストで実行されているオペレーティング システムを示す決定的証拠とならない場合、使用されている可能性が最も高いオペレーティングがネットワーク マップに表示されます。たとえば、複数のホストがNATデバイスの「背後」にあることから、NATデバイスが複数のオペレーティング システムを実行しているように表示される場合があります。この最も可能性の高いオペレーティングを決定するためにシステムが使用するのは、検出された各オペレーティング システムに割り当てられた信頼度の値と、検出されたオペレーティング システムの中でその特定のオペレーティング システムが使用されていることを裏付けるデータの量です。

（注） この決定を行う際、システムは「unknown」として報告されたアプリケーションとオペレーティング システムを考慮しません。

パッシブ検出でネットワーク アセットが正確に識別されない場合は、管理対象デバイスの配置について検討してください。また、システムのパッシブ検出機能をオペレーティング システムのカスタム フィンガープリントとカスタム アプリケーション ディテクタで増補することもできます。あるいは、アクティブ検出を使用するという方法もあります。アクティブ検出では、トラフィック分析をベースとするのではなく、スキャン結果やその他の情報ソースを使用して直接ネットワーク マップを更新できます。

オペレーティング システムおよびホスト データのアクティブ検出

アクティブ検出では、アクティブ ソースによって収集されたホスト情報をネットワーク マップに追加します。たとえば、Nmap スキャナを使用して、ネットワーク上の対象ホストをアクティブにスキャンできます。Nmapは、ホストでオペレーティング システムおよびアプリケーションを検出します。

さらに、ホスト入力機能によって、ネットワーク マップにホスト入力データをアクティブに追加することができます。ホスト入力データには2種類のカテゴリがあります。

- ユーザ入力データ：FirePOWER システム ユーザ インターフェイスで追加されたデータ。このユーザ インターフェイスを使用して、ホストのオペレーティング システムやアプリケーションの ID を変更できます。
- ホスト インポート入力データ：コマンド ライン ユーティリティを使用してインポートされたデータ。

システムは、それぞれのアクティブ ソースに対して 1 個の ID を保持します。たとえば、Nmap スキャンインスタンスを実行すると、以前のスキャンの結果は新しいスキャン結果に置き換えられます。ただし、Nmap スキャンを実行し、それらの結果をクライアントからのデータ（コマンド ラインを使用してインポートした結果）と交換する場合、システムは Nmap の結果の ID とインポート クライアントの ID の両方を保持します。システムは、ネットワーク検出ポリシーで設定された優先順位を使用して、現在の ID として使用するアクティブ ID を判別します。

複数のユーザが入力したとしても、ユーザ入力は 1 ソースと見なされることに注意してください。たとえば、UserA がホスト プロファイルを使用してオペレーティング システムを設定し、UserB がホスト プロファイルを使用してその定義を変更した場合、UserB によって設定された定義が保持され、UserA によって設定された定義は破棄されます。また、ユーザ入力によって、他のアクティブ ソースすべてが上書きされ、存在する場合、現在の ID として使用されることに注意してください。

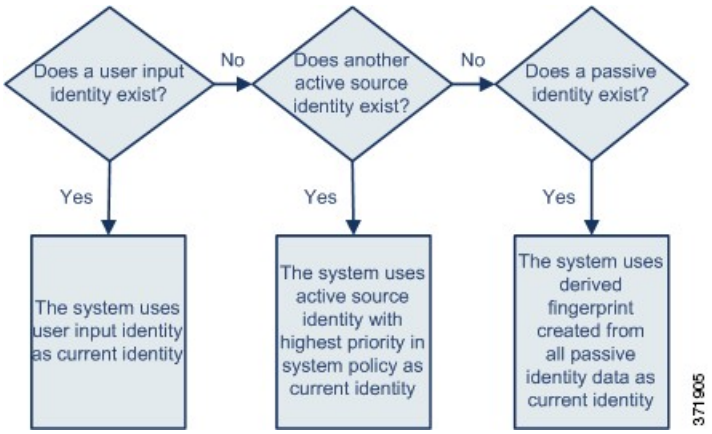
アプリケーションおよびオペレーティング システムの現在の ID

ホストのアプリケーションまたはオペレーティング システムの現在の *ID* は、ホストが最も正しい可能性が高いと認識する ID です。

システムは、以下の目的で、オペレーティング システムまたはアプリケーションの現在の ID を使用します。

- 脆弱性のホストへの割り当て
- 影響評価
- オペレーティング システムの識別、ホスト プロファイルの認定、およびコンプライアンスのホワイトリストに対して記述された相関ルールの評価
- ワークフローのホストおよびサーバのテーブル ビューでの表示
- ホスト プロファイルでの表示
- [Discovery Statistics] ページでのオペレーティング システムとアプリケーションの統計の計算

システムは、ソースの優先順位を使用して、アプリケーションまたはオペレーティング システムの現在の ID として使用するアクティブ ID を判別します。



たとえば、ユーザがホストでオペレーティング システムを Windows 2003 Server に設定した場合、Windows 2003 Server が現在の ID になります。そのホストの Windows 2003 Server の脆弱性を狙った攻撃により大きな影響力があると見なされ、ホストプロファイルのそのホストについてリストされた脆弱性に、Windows 2003 Server の脆弱性が含められます。

データベースは、ホストのオペレーティングシステムや特定のアプリケーションに関する複数のソースからの情報を保持する場合があります。

データのソースに最も高いソースの優先順位が付けられている場合に、システムはオペレーティング システムまたはアプリケーションの ID を現在の ID として扱います。使用される可能性のあるソースには、次の優先順位があります。

1.ユーザ

2. スキャナとアプリケーション（ネットワーク検出ポリシーで設定）

3. 管理対象デバイス

4. ：NetFlow レコード

新しい優先順位の高いアプリケーション ID は、現在のアプリケーション ID ほど詳細でない場合、現在の ID を上書きしません。

また、ID の競合が発生した場合、競合の解決はネットワーク検出ポリシーの設定または手動解決によります。

現在のユーザ アイデンティティ

異なる複数のユーザによる同じホストへの複数のログインがシステムにより検出されると、特定のホストに同時にログインできるのは 1 ユーザのみであり、ホストの現在のユーザが最新の正式なユーザ ログインであると見なされます。権限のないユーザ ログインだけがホストにログインしている場合は、最後にログインしたものが現在のユーザと見なされます。複数のユーザがリモート セッション経由でログインしている場合は、サーバによって報告された最後のユーザが Firepower Management Centerに報告されるユーザです。

同じユーザによる同じホストへの複数のログインがシステムにより検出されると、システムは指定のホストへのユーザの最初のログインを記録し、それ以降のログインは無視します。ある

ユーザが特定のホストにログインしている唯一の人物の場合は、システムが記録する唯一のログインがオリジナルのログインです。

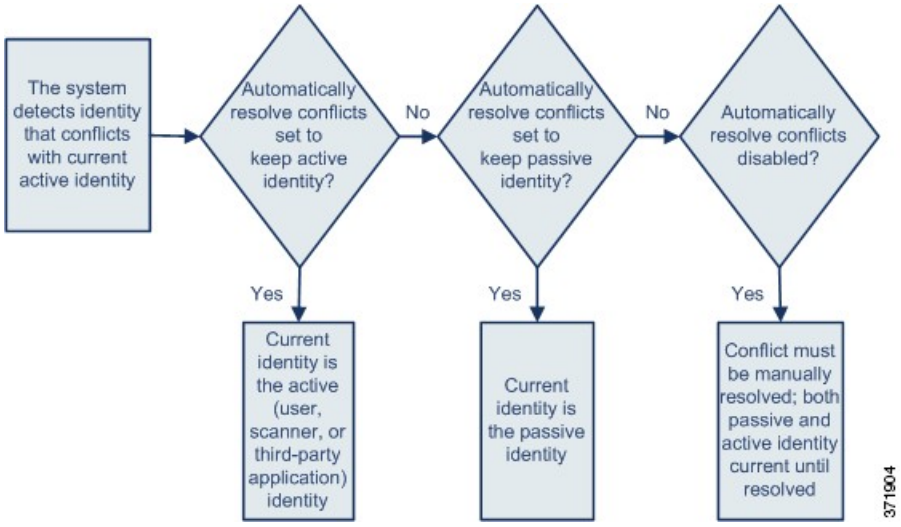
ただし、そのホストに別のユーザがログインした時点で、システムは新しいログインを記録します。その後で、オリジナルのユーザが再度ログインすると、その人物の新しいログインが記録されます。

アプリケーションおよびオペレーティング システムの ID の競合

現在のアクティブ ID および以前に報告されたパッシブ ID と競合する新しいパッシブ ID が報告されると、*ID* の競合が発生します。たとえば、オペレーティング システムの以前のパッシブ ID は Windows 2000 と報告され、Windows XP のアクティブ ID が現在の ID になります。次に、システムが Ubuntu Linux 8.04.1 の新しいパッシブ ID を検出します。Windows XP と Ubuntu Linux の ID が競合状態になります。

ホストのオペレーティング システムまたはホスト上のいずれかのアプリケーションの ID に対して ID の競合が存在する場合、システムは現在の ID として競合する両方の ID をリストし、競合が解決されるまで影響評価に両方の ID を使用します。

管理者特権を持つユーザは、パッシブ ID を常に使用するか、またはアクティブ ID を常に使用するかを選択することによって、自動的に ID の競合を解決できます。ID の競合の自動解決を無効にしない限り、ID の競合は常に自動的に解決されます。



管理者特権を持つユーザは、ID の競合が発生した場合に、イベントを生成するようにシステムを設定することもできます。そのユーザは、相関応答として Nmap スキャンを使用する相関ルールで相関ポリシーを設定できます。イベントが発生すると、Nmap はホストをスキャンして、更新されたホストのオペレーティング システムとアプリケーション データを取得します。

Firepower システムの NetFlow データ

NetFlowは、ルータを通過するパケットの統計情報を提供する、CiscoIOSアプリケーションの1つです。NetFlow は Cisco ネットワーキング デバイスで使用できます。また、Juniper、FreeBSD、OpenBSD デバイスに組み込むことも可能です。

NetFlow がネットワーク デバイスで有効にされている場合、そのデバイス上のデータベース（NetFlowキャッシュ）に、ルータを通過するフローのレコードが格納されます。Firepowerシステムで接続と呼ばれるフローは、特定のポート、プロトコル、およびアプリケーションプロトコルを使用する送信元ホストと宛先ホスト間のセッションを表すパケットのシーケンスです。このNetFlowデータをエクスポートするようにネットワーク デバイスを設定できます。本書では、そのように設定されたネットワーク デバイスを NetFlow エクスポータと呼びます。

Firepowerシステムの管理対象デバイスは、NetFlowエクスポータからレコードを収集して、それらのレコードに含まれるデータに基づいて単方向の接続終了イベントを生成し、それらのイベントを接続イベントデータベースに記録するためにFirepower Management Centerに送信するように設定できます。また、NetFlow接続内の情報に基づいて、ホストとアプリケーションプロトコルに関する情報をデータベースに追加するためのネットワーク検出ポリシーを設定することもできます。

この検出データと接続データを使用して、管理対象デバイスによって直接収集されたデータを補完できます。これは、管理対象デバイスでモニタできないネットワークを NetFlow エクスポータにモニタさせる場合には特に有効です。

NetFlow データを使用するための要件

NetFlow データを分析するために Firepower System を設定する前に、ルータまたは使用する他のNetFlowが有効なネットワーク デバイス上でNetFlow機能を有効にし、管理対象デバイスのセンシング インターフェイスを接続する宛先ネットワークへNetFlowデータをブロードキャストするようにデバイスを設定する必要があります。

Firepower System では、NetFlow バージョン 5 レコードと NetFlow バージョン 9 レコードをいずれも解析できます。Firepower System にデータをエクスポートするには、使用する NetFlow エクスポータのバージョンが次のいずれかである**必要があります**。さらに、このシステムでは、特定のフィールドがエクスポートされたNetFlowテンプレートとレコードに存在する必要があります。NetFlowエクスポータがカスタマイズ可能なバージョン9を使用している場合は、エクスポートされたテンプレートとレコードに次のフィールドが任意の順序で含まれていることを確認する**必要があります**。

- IN_BYTES (1)
- IN_PKTS (2)
- PROTOCOL (4)
- TCP_FLAGS (6)
- L4_SRC_PORT (7)
- IPV4_SRC_ADDR (8)
- L4_DST_PORT (11)

- IPV4_DST_ADDR (12)
- LAST_SWITCHED (21)
- FIRST_SWITCHED (22)
- IPV6_SRC_ADDR (27)
- IPV6_DST_ADDR (28)

Firepower System は管理対象デバイスを使用して NetFlow データを分析するため、NetFlow エクスポータの監視可能な 1 つ以上の管理対象デバイスを展開に含める必要があります。この管理対象デバイス上の 1 つ以上のセンシング インターフェイスを、エクスポートされた NetFlow データを収集可能なネットワークに接続する必要があります。通常、管理対象デバイス上のセンシング インターフェイスには IP アドレスが割り当てられないため、システムは NetFlow レコードの直接収集をサポートしません。

一部のネットワーク デバイス上で使用可能な Sampled NetFlow 機能は、デバイスを通過するパケットのサブセットだけに基づく NetFlow 統計情報を収集することに注意してください。この機能を有効にすると、ネットワーク デバイス上の CPU 使用率が改善される可能性がありますが、Firepower System で分析するために収集されている NetFlow データに影響する場合があります。

NetFlow データと管理対象デバイス データの違い

Firepowerは、NetFlowデータによって表されるトラフィックを直接分析しません。代わりに、エクスポートしたNetFlowレコードを接続ログおよびホストとアプリケーションのプロトコルデータに変換します。

その結果、変換されたNetFlowデータと、管理対象デバイスによって直接収集された検出および接続データにはいくつかの違いがあります。以下のことを必要とする分析を実行する場合に、これらの違いを意識しなければなりません。

- 検出された接続数に基づく統計情報
- オペレーティング システムとその他のホスト関連情報（脆弱性を含む）
- クライアント情報、Web アプリケーション情報、ベンダーおよびバージョン サーバ情報を含むアプリケーション データ
- 接続内の発信側のホストと応答側のホストの認識

ネットワーク検出ポリシーとアクセス コントロール ポリシーの違い

接続ロギングを含むNetFlowデータ収集は、ネットワーク検出ポリシー内のルールを使用して設定します。これを、アクセス コントロール ルールごとに設定した FirePOWER システム管理対象デバイスによって検出された接続の接続ロギングと比較してください。

接続イベントのタイプ

NetFlowデータ収集はアクセス コントロール ルールではなくネットワークにリンクされているため、システムがログに記録する NetFlow 接続をきめ細かく制御することはできません。

NetFlow データは、セキュリティ インテリジェンス イベントを生成することはできません。

NetFlowベースの接続イベントは、接続イベント データベースにのみ保存できます。システム ログまたは SNMP トラップ サーバに送信することはできません。

モニタ対象セッションごとに生成される接続イベントの数

管理対象デバイスによって直接検出された接続の場合は、アクセス コントロール ルールを設定して、接続の最初か最後またはその両方で双方向接続イベントをログに記録できます。

それに対し、エクスポートされた NetFlow レコードには単方向接続データが含まれているため、システムは処理する各 NetFlow レコードに対し少なくとも 2 つの接続イベントを生成します。これは、概要の接続数が NetFlow データに基づいた接続ごとに 2 ずつ増加することも意味しており、ネットワーク上で実際に発生している接続数が急増することになります。

接続がまだ実行中であっても、NetFlow エクスポータは固定間隔でレコードを出力するため、長時間実行しているセッションの場合は複数のエクスポートされたレコードが生成される場合があり、その各レコードが接続イベントを生成します。たとえば、NetFlow エクスポータが 5 分ごとにエクスポートする場合に、特定の接続が 12 分間続いている場合、システムはそのセッションに対し 6 つの接続イベントを生成します。

- 最初の 5 分間の 1 つのイベント ペア
- 次の 5 分間の 1 つのペア
- 接続が終了した時点の最後のペア

ホスト データとオペレーティング システム データ

NetFlowデータからのネットワーク マップに追加されたホストには、オペレーティング システム、NetBIOS、またはホスト タイプ（ホストまたはネットワーク デバイス）の情報がありません。ただし、ホスト入力機能を使用してホストのオペレーティング システム ID を手動で設定できます。

アプリケーション データ

管理対象デバイスによって直接検出された接続の場合は、接続内のパケットを検査することによって、システムはアプリケーション プロトコル、クライアント、およびWebアプリケーションを識別できます。

システムは NetFlow レコードを処理するときに、`/etc/sf/services` 内のポート関連付けを使用して、アプリケーション プロトコル ID を推測します。ただし、これらのアプリケーション プロトコルに関するベンダーまたはバージョン情報が存在しないため、接続ログにはセッションで使用されるクライアントまたは Web アプリケーションに関する情報が含まれません。しかし、ホスト入力機能を使用してこの情報を手動で提供できます。

単純なポート関連付けでは、非標準ポート上で動作しているアプリケーションプロトコルが特定されないまたは誤認される可能性があることに注意してください。加えて、関連付けが存在しない場合は、システムがそのアプリケーションプロトコルを接続ログで `unknown` としてマークします。

脆弱性マッピング

システムは、ホスト入力機能を使用してホストのオペレーティング システム ID またはアプリケーション プロトコル ID を手動で設定しない限り、NetFlow エクスポータによってモニタされるホストに脆弱性をマッピングできません。NetFlow 接続内にクライアント情報が存在しないため、クライアントの脆弱性を NetFlow データから作成されたホストに関連付けることはできないことに注意してください。

接続内の発信側情報と応答側情報

管理対象デバイスによって直接検出された接続の場合、システムは発信側または送信元のホストと応答側または宛先のホストを識別できます。ただし、NetFlow データには発信側または応答側の情報が含まれていません。

Firepower システムは、NetFlow レコードを処理するときに、それぞれのホストが使用しているポートとそれらのポートが既知かどうかに基づいて、この情報を判断するアルゴリズムを使用します。

- 使用されているポートの両方が既知のポートの場合、または、どちらも既知のポートでない場合、システムは番号の若い方のポートを使用しているホストを応答側と見なします。
- どちらかのホストだけが既知のポートを使用している場合は、システムがそのホストを応答側と見なします。

したがって、既知のポートは、1 ～ 1023 の番号が割り当てられたポートまたは管理対象デバイス上の `/etc/sf/services` にアプリケーション プロトコル情報が保存されているポートです。

さらに、管理対象デバイスによって直接検出された接続の場合、システムは対応する接続イベントの 2 バイト数を記録します。

- [イニシエータ バイト数（Initiator Bytes）] フィールドは送信バイト数を記録します。
- [レスポンダ バイト数（Responder Bytes）] フィールドは受信バイト数を記録します。

単方向 NetFlow レコードに基づく接続イベントには、1 バイト数しか含まれておらず、ポートベース アルゴリズムに応じて、システムが [イニシエータ バイト数（Initiator Bytes）] または [レスポンダ バイト数（Responder Bytes）] に割り当てます。システムによって他のフィールドは 0 に設定されます。NetFlow レコードの接続の概要（集約接続データ）を表示している場合に、両方のフィールドに値が読み込まれる場合があることに注意してください。

NetFlow のみの接続イベント フィールド

いくつかのフィールドは、NetFlow レコードから生成された接続イベントでのみ表示されます（接続イベント フィールドで利用可能な情報 （3044 ページ）を参照）。

関連トピック

接続イベント フィールドで利用可能な情報 （3044 ページ）

ユーザ アイデンティティについて

ユーザアイデンティティ情報を使用すると、ポリシー違反、攻撃、ネットワークの脆弱性の発生源を特定し、特定のユーザまで遡って追跡することができます。たとえば、以下について決定できます。

- 脆弱（レベル 1：赤）影響レベルの侵入イベントの対象になっているホストの所有者。
- 内部攻撃またはポートスキャンを開始した人物。
- 特定のホストへの不正アクセスを試みている人物。
- 過度に大量の帯域幅を使用している人物。
- 重要なオペレーティング システム更新を適用しなかった人物。
- 会社のポリシーに違反してインスタント メッセージング ソフトウェアまたはピアツーピア ファイル共有アプリケーションを使用している人物。
- ネットワーク上の侵害の兆候に関連付けられている人物。

この情報を入手すれば、Firepower システムの他の機能を使用して、リスクを低減し、アクセス制御を実行し、他のユーザを破壊行為から保護するためのアクションを実行できます。これらの機能により、監査制御が大幅に改善され、規制の順守が促進されます。

ユーザ アイデンティティ ソースを設定してユーザ データを収集すると、ユーザ認識とユーザ制御を実行できます。

関連トピック

アイデンティティの用語 （2481 ページ）
アイデンティティ導入 （2484 ページ）
ユーザ アイデンティティ ソースについて （2482 ページ）
アイデンティティ ポリシーの設定方法 （2485 ページ）

アイデンティティの用語

このトピックでは、ユーザアイデンティティおよびユーザ制御の一般的な用語について説明します。

ユーザ認識

アイデンティティ ソース（ユーザ エージェントや TS エージェントなど）を使用して、ネットワーク上のユーザを識別します。ユーザ認識によって、権限のあるソース（Active Directory など）および権限のないソース（アプリケーションベース）の両方からユーザを識別できます。Active Directory をアイデンティティ ソースとして使用するには、レルムお

よびディレクトリを設定する必要があります。詳細については、ユーザアイデンティティ ソースについて （2482 ページ）を参照してください。

ユーザ制御

アクセス コントロール ポリシーに関連付けるアイデンティティ ポリシーを構成します。（アイデンティティ ポリシーは、アクセス コントロール サブポリシーと呼ばれるようになります。）アイデンティティ ポリシーはアイデンティティ ソースを指定し、オプションで、そのソースに属するユーザおよびグループを指定します。

アイデンティティ ポリシーをアクセス コントロール ポリシーに関連付けることで、ネットワークのトラフィックでユーザまたはユーザアクティビティをモニタ、信頼、ブロックまたは許可するかどうかを決定します。詳細については、アクセス コントロール ポリシーの開始 （1665 ページ）を参照してください。

権限のあるアイデンティティ ソース

信頼できるサーバによってユーザ ログインが検証されています（たとえば、Active Directory）。正規のログインから取得されるデータを使用して、ユーザ対応とユーザ制御を実行できます。正規のユーザ ログインは、パッシブ認証とアクティブ認証から取得されます。

- パッシブ認証は、ユーザが外部ソース経由で認証されるときに発生します。ユーザ エージェント、ISE/ISE-PIC、および TS エージェントは、Firepower システムでサポートされるパッシブ認証方式です。
- アクティブ認証は、ユーザが事前設定済みの管理対象デバイス経由で認証されるときに発生します。キャプティブ ポータルおよびリモート アクセス VPN は、Firepower システムでサポートされるアクティブ認証方式です。

権限のないアイデンティティ ソース

ユーザ ログインの検証を行った不明または信頼できないサーバ。トラフィック ベースの検出は、Firepower システムでサポートされている唯一の権限のないアイデンティティ ソースです。権限のないログインから取得されたデータを使用すると、ユーザ認識を実行できます。

ユーザ アイデンティティ ソースについて

次の表に、Firepower システムでサポートされているユーザ アイデンティティ ソースの概要を示します。各アイデンティティ ソースは、ユーザ認識のためのユーザの記憶域を提供します。これらのユーザは、アイデンティティおよびアクセス コントロール ポリシーで制御できます。

ユーザ アイデンティティ ソース	ポリシー	サーバ要件	タイプ（Type）	認証タイプ	ユーザ認識	ユーザ制御	詳細情報の参照先
ユーザ エージェント	アイデンティティ	Microsoft Active Directory	権限のあるログイン	パッシブ	あり	あり	ユーザ エージェントのアイデンティティ ソース （2633 ページ）
ISE/ISE-PIC	アイデンティティ	Microsoft Active Directory	権限のあるログイン	パッシブ	あり	あり	ISE/ISE-PIC アイデンティティ ソース （2593 ページ）
TS エージェント	アイデンティティ	Microsoft Windows Terminal Server	権限のあるログイン	パッシブ	あり	あり	ターミナル サービス（TS）エージェントのアイデンティティ ソース （2629 ページ）
キャプティブ ポータル	アイデンティティ	Microsoft Active Directory	権限のあるログイン	Active	あり	あり	キャプティブ ポータルのアイデンティティ ソース （2607 ページ）
リモート アクセス VPN	ID（Identity）	OpenLDAP または Microsoft Active Directory	権限のあるログイン	Active	あり	あり	リモート アクセス VPN アイデンティティ ソース （2623 ページ）
	Identity	RADIUS	権限のあるログイン	Active	あり	なし	

ユーザ アイデンティティ ソース	ポリシー	サーバ要件	タイプ（Type）	認証タイプ	ユーザ認識	ユーザ制御	詳細情報の参照先
トラフィック ベースの検出	ネットワーク検出	適用対象外	権限のないログイン	n/a	あり	なし	トラフィック ベース検出のアイデンティティ ソース （2659 ページ）

展開するアイデンティティ ソースを選択する際には、以下を検討してください。

- 非 LDAP ユーザ ログインにはトラフィック ベースの検出を使用する必要があります。たとえば、ユーザ エージェントのみを使用してユーザ アクティビティを検出している場合は、非 LDAP ログインを制限しても効果はありません。
- 失敗したログインまたは認証アクティビティを記録するには、トラフィック ベースの検出またはキャプティブ ポータルを使用する必要があります。失敗したログインまたは認証試行で新しいユーザがデータベース内のユーザのリストに追加されることはありません。
- キャプティブ ポータルのアイデンティティ ソースには、ルーテッド インターフェイスを備えた管理対象デバイスが必要です。キャプティブ ポータルでインライン（タップ モードとも呼ばれます）インターフェイスを使用することはできません。

これらのアイデンティティ ソースからのデータは、Firepower Management Center のユーザ データベースとユーザ アクティビティ データベースに格納されます。Firepower Management Center サーバ ユーザ ダウンロードを設定して、新しいユーザ データがデータベースに自動的かつ定期的にダウンロードされるようにできます。

必要なアイデンティティ ソースを使用してアイデンティティ ルールを設定したら、各ルールにアクセス コントロール ポリシーを関連付け、ポリシーを有効にするために管理対象デバイスに展開する必要があります。アクセス コントロール ポリシーおよび展開の詳細については、ユーザ条件、レルム条件、および ISE 属性条件（ユーザ制御） （490 ページ）を参照してください。

Firepower システムでのユーザ検出の一般情報については、ユーザ アイデンティティについて（2481 ページ）を参照してください。

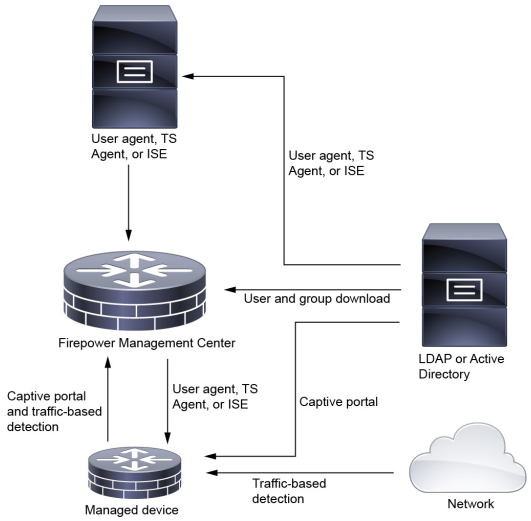
アイデンティティ導入

システムがユーザ ログイン、またはアイデンティティ ソースからのユーザ データを検出すると、そのログインからのユーザは、Firepower Management Center ユーザ データベース内のユーザのリストに照らしてチェックされます。ログイン ユーザが既存のユーザと一致した場合は、ログインからのデータがそのユーザに割り当てられます。ログインが SMTP トラフィック内に

存在しない場合は、既存のユーザと一致しないログインによって新しいユーザが作成されます。SMTP トラフィック内の一致しないログインは破棄されます。

ユーザが所属するグループは、Firepower Management Center でユーザが認識されるとすぐに、ユーザに関連付けられます。

次の図は、Firepower システムがユーザ データをどのように収集して保存するかを示しています。



アイデンティティ ポリシーの設定方法

このトピックでは、使用可能な任意のユーザ アイデンティティ ソース（TS エージェント、ユーザ エージェント、ISE/ISE-PIC、キャプティブ ポータル、またはリモート アクセス VPN）を使用してアイデンティティ ポリシーを設定する方法の概要を説明します。

手順

	コマンドまたはアクション	目的
ステップ 1	レルムを作成します。	レルムとは、信頼されたユーザおよびグループの領域で、Microsoft Active Directory リポジトリなどがあります。Firepower Management Center は、指定した間隔でユーザとグループをダウンロードします。ユーザとグループは、ダウンロードに含めることも、ダウンロードから除外することもできます。ユーザとグループのダウンロード（2583 ページ）を参照してください。 （注） アイデンティティ ポリシーを使用するためのレルムの作成の例外については、このセクションの最後を参照してください。

	コマンドまたはアクション	目的
ステップ 2	レルムにディレクトリを作成します。	ディレクトリとは、コンピュータ ネットワークのユーザとネットワーク共有に関する情報を編成する Active Directory ドメイン コントローラのことです。Active Directory コントローラはレルムにディレクトリ サービスを提供します。Active Directory は、ユーザ オブジェクトやグループ オブジェクトを複数のドメイン コントローラ間に分散させます。これらのドメイン コントローラは、ディレクトリ サービスを使用してローカルの変更を互いに伝達するピアです。詳細については、MSDN の『Active Directory technical specification glossary』[英語] を参照してください。 1 つのレルムに複数のディレクトリを指定できます。この場合、ユーザ制御用のユーザ クレデンシャルとグループ クレデンシャルを照合するために、そのレルムの [ディレクトリ（Directory）] タブ ページにリストされている順序で、各ドメイン コントローラがクエリされます。 レルムディレクトリの設定（2582ページ）を参照してください。
ステップ 3	レルムからユーザやグループをダウンロードします。	ユーザやグループを制御するには、それらを Firepower Management Center にダウンロードする必要があります。ユーザやグループを必要に応じて手動でダウンロードすることも、指定した間隔でシステムがそれらをダウンロードするように設定することもできます。 ユーザやグループをダウンロードするときに、例外を指定できます。たとえば、そのレルムのすべてのユーザ制御から Engineering というグループを除外したり、Engineering グループに適用されるユーザ制御から **joe.smith** というユーザを除外したりできます。 ユーザとグループのダウンロード（2583ページ）を参照してください。
ステップ 4	レルムを有効化します。	ユーザ制御でレルムを使用するには、そのレルムを有効化する必要があります。レルムを有効化するには、[状態（State）] スライダを右にスライドさせます。レルムの管理（2584ページ）を参照してください .

	コマンドまたはアクション	目的
ステップ 5	ユーザ データやグループ データを取得するための手法（アイデンティティ ソース）を作成します。	レルムに保存されたデータを使用してユーザやグループを制御するには、固有の設定を使って ID ストアをセットアップします。アイデンティティ ソースには、TS エージェント、ユーザ エージェント、キャプティブ ポータル、またはリモート VPN が含まれます。次のいずれかを参照してください。 • ユーザ制御のためのキャプティブ ポータルの設定方法 （2610 ページ） • ユーザ制御のためのユーザ エージェントの設定 • ユーザ制御用 ISE/ISE-PIC の設定 （2601 ページ） • ユーザ制御用 RA VPN の設定 （2625 ページ）
ステップ 6	アイデンティティ ポリシーを作成します。	アイデンティティ ポリシーには、1 つ以上のアイデンティティ ルールが含まれており、 必要に応じてこれらをカテゴリにまとめることができます。アイデンティティ ポリシーの作成 （2643 ページ）を参照してください。 （注） アイデンティティ ポリシーの作成の例外については、このセクションの最後で説明します。
ステップ 7	1 つ以上のアイデンティティ ルールを作成します。	アイデンティティ ルールを使用すると、認証の種類、ネットワーク ゾーン、ネットワークまたは地理位置情報、レルムなど、多数の一致条件を指定できます。アイデンティティ ルールの作成 （2638 ページ）を参照してください。
ステップ 8	アイデンティティ ポリシーをアクセス コントロール ポリシーに関連付けます。	アクセス コントロール ポリシーはトラフィックをフィルタリングし、必要に応じてトラフィックを検査します。アクセス制御への他のポリシーの関連付け （1684 ページ）を参照してください。
ステップ 9	少なくとも 1 つの管理対象デバイスにアクセス コントロール ポリシーを展開します。	ポリシーを使用してユーザ アクティビティを制御するには、クライアントの接続先となる管理対象デバイスにそのポリシーを展開する必要があります。設定変更の展開 （447 ページ）を参照してください。
ステップ 10	ユーザ アクティビティをモニタします。	ユーザ アイデンティティ ソースによって収集されたアクティブ セッションの一覧、またはユーザ ア

	コマンドまたはアクション	目的
		イデンティティ ソースによって収集されたユーザ情報の一覧を確認します。ワークフローの使用 （2931 ページ）を参照してください。 次のすべてに該当する場合、アイデンティティ ポリシーは必要ありません。 • ISE/ISE-PIC アイデンティティ ソースを使用できます。 • アクセス コントロール ポリシーのユーザまたはグループは使用しません。 • アクセスコントロールポリシーのセキュリティ グループ タグ（SGT）を使用します。詳細については、「ISE SGT とカスタム SGT ルール条件との比較（496 ページ）」を参照してください。

関連トピック

トラフィック ベースのユーザ検出の設定 （2661 ページ）

ユーザ アクティビティ データベース

Firepower Management Center のユーザ アクティビティ データベースには、設定されたすべてのアイデンティティ ソースによって検出または報告されたネットワーク上のユーザ アクティビティのレコードが含まれています。システムがイベントを記録するのは以下のような状況です。

- 個別のログインまたはログオフを検出したとき。
- 新しいユーザを検出したとき。
- システム管理者が手動でユーザを削除したとき。
- データベース内に存在しないユーザをシステムが検出したものの、ユーザ数の制限に達したためにそのユーザを追加できなかったとき。
- ユーザに関連付けられている侵害の兆候を解決したとき、またはユーザに対して侵害の兆候ルールを有効または無効にしたとき。

（注） TS エージェントが別のパッシブ認証のアイデンティティ ソース（ユーザ エージェントや ISE/ISE-PIC など）と同じユーザをモニタする場合、Firepower Management Center では TS エージェントのデータを優先します。TS エージェントと別のパッシブのソースが同じ IP アドレスからの同じアクティビティを報告した場合、TS エージェントのデータだけが Firepower Management Center に記録されます。

システムで検出されたユーザ アクティビティは、Firepower Management Center Web インターフェイスを使用して表示できます。（[分析（Analysis）] > [ユーザ（Users）] > [ユーザ アクティビティ（User Activity）]）。

ユーザ データベース

Firepower Management Center のユーザ データベースには、設定されたすべてのアイデンティティ ソースによって検出または報告されたユーザごとのレコードが含まれています。権限のあるソースから取得したデータをユーザ制御に使用できます。

サポートされている権限のないアイデンティティ ソースと権限のあるアイデンティティ ソースの詳細については、ユーザ アイデンティティ ソースについて （2482 ページ） を参照してください。

Firepower システムのユーザの制限 （2492 ページ） で説明されているように、Firepower Management Center で保存できるユーザの合計数は、Firepower Management Center のモデルごとに異なります。ユーザ制限に達した後、システムは、アイデンティティ ソースに基づいて未検出ユーザ データを次のように優先順位付けします。

- 新しいユーザが権限のないアイデンティティ ソースからである場合、ユーザはデータベースに追加されません。新規ユーザを追加できるようにするには、手動またはデータベースの消去によってユーザを削除する必要があります。
- 新しいユーザが権限のあるアイデンティティ ソースからである場合、システムは最も長い期間にわたって非アクティブのままになっている権限のないユーザを削除し、データベースに新しいユーザを追加します。

アイデンティティ ソースが特定のユーザ名を除外するように設定されている場合、それらのユーザ名のユーザ アクティビティ データは Firepower Management Center に報告されません。これらの除外されたユーザ名はデータベースに残りますが、IP アドレスに関連付けられません。システムによって保存されるデータのタイプの詳細については、ユーザ データ（User Data） （3256 ページ）を参照してください。

Firepower Management Center ハイ アベイラビリティが設定済みで、プライマリに障害が発生した場合、ユーザ エージェント、ISE/ISE-PIC、TS エージェント、リモート アクセス VPN、またはキャプティブ ポータル デバイスから報告されるログインはフェールオーバー ダウンタイム中に識別不能になります（たとえユーザが以前に確認されて Firepower Management Center にダウンロードされた場合でも）。未確認のユーザは Firepower Management Center には不明なユーザとして記録されます。ダウンタイム後、不明のユーザはアイデンティティ ポリシーのルールに従って再確認され、処理されます。

（注） TS エージェントが別のパッシブ認証のアイデンティティ ソース（ユーザ エージェントまたは ISE/ISE-PIC）と同じユーザをモニタする場合、Firepower Management Center では TS エージェントのデータを優先します。TS エージェントと別のパッシブのソースが同じ IP アドレスからの同じアクティビティを報告した場合、TS エージェントのデータだけが Firepower Management Center に記録されます。

システムが新しいユーザ セッションを検出すると、そのユーザ セッションのデータは、次のいずれかが発生するまでユーザ データベースに残ります。

- Firepower Management Center のユーザが手動でユーザ セッションを削除した。
- アイデンティティ ソースがそのユーザ セッションのログオフを報告した。
- レルムがレルムの [ユーザ セッションのタイムアウト：認証されたユーザ（User Session Timeout: Authenticated Users）] 設定、[ユーザ セッションのタイムアウト：認証に失敗したユーザ（User Session Timeout: Failed Authentication Users）] 設定、または [ユーザ セッションのタイムアウト：ゲスト ユーザ（User Session Timeout: Guest Users）] 設定で指定されているユーザ セッションを終了した。

Firepower システムのホストとユーザの制限

Firepower Management Center モデルにより、展開でモニタできる個別のホストの数、モニタし、ユーザ制御を実行するために使用できるユーザの数が決定されます。

関連トピック

FMC データベースからのデータの消去 （261 ページ）

Firepower システムのホスト制限

システムは（ネットワーク検出ポリシーで定義されている）モニタ対象ネットワークで IP アドレスに関連付けられたアクティビティを検出すると、ネットワーク マップにホストを追加します。Firepower Management Center がモニタでき、ネットワーク マップに保存できるホストの数。モデルによって異なります。

***表 256 : Firepower Management Center* モデル別のホスト制限**

FMC モデル	ホスト
MC750	2,000
MC1000	50,000
MC1500	50,000
MC1600	50,000

FMC モデル	ホスト
FS2000	150,000
MC2500	150,000
MC2600	150,000
MC3500	300,000
MC4000	600,000
MC4500	600,000
MC4600	600,000
virtual	50,000

ネットワーク マップに存在しないホストのコンテキスト データは表示できません。ただし、アクセス制御は実行できます。たとえば、コンプライアンス ホワイトリストを使用してホストのネットワーク コンプライアンスをモニタできない場合でも、ネットワーク マップに存在しないホストとの間のトラフィックでアプリケーション制御を実行できます。

（注） システムでは、IPアドレスとMACアドレスの両方によって識別されるホストとは別に、MAC専用ホストがカウントされます。1つのホストに関連付けられているすべてのIPアドレスは、まとめて1つのホストとしてカウントされます。

ホスト制限への到達とホストの削除

ホスト制限に到達した後に新しいホストを検出すると、ネットワーク検出ポリシーが制御を行います。新しいホストをドロップするか、または非アクティブになっている期間が最も長いホストを置換することができます。また、システムが非アクティブであるためネットワークからホストを削除するまでの期間を設定できます。ホスト、サブネット全体、またはすべてのホストをネットワーク マップから手動で削除できますが、システムは、削除されたホストに関連付けられたアクティビティを検出した場合は、ホストを再追加します。

マルチドメイン展開では、各リーフ ドメインに自身のネットワーク検出ポリシーがあります。したがって、各リーフ ドメインによって、システムが新しいホストを検出したときの独自の動作が決定されます。

関連トピック

ドメインのプロパティ （435 ページ）
ネットワーク検出のデータ ストレージ設定 （2669 ページ）

Firepower システムのユーザの制限

Firepower Management Center モデルにより、モニタできる個々のユーザ数が決まります。システムが新しいユーザのアクティビティを検出すると、そのユーザはFirepower Management Centerの Users データベースに追加されます。任意のアイデンティティ ソースを使用して、ユーザを検出できます。

検討するユーザ制限には 2 つのタイプがあります。

- 同時使用ユーザ制限は、システムに同時にログインできるユーザの人数です。これらのユーザはすべて権限のあるユーザであり、権限のあるユーザ ソース（ユーザ エージェント、ISE/ISE-PIC、TS エージェント、およびキャプティブ ポータル）によって Firepower Management Center にレポートされることを意味します。

  権限のあるユーザのみがアクセス コントロール ポリシーによるユーザ制御を使用できます。

- ユーザ総数の制限。データベースに保存できる、権限のあるユーザと権限のないユーザの数です。権限のないユーザ データは、トラフィック ベースの検出を使用して収集されます。

表 *257 : Firepower Management Center* モデル別のユーザ制限

FMC モデル	同時使用ユーザ	ユーザ総数
MC750	2,000	2,000
MC1000	50,000	50,000
MC1500	50,000	50,000
MC1600	50,000	50,000
FS2000	64,000	150,000
MC2500	64,000	150,000
MC2600	64,000	150,000
MC3500	64,000	300,000
MC4000	64,000	600,000
MC4500	64,000	600,000
MC4600	64,000	600,000
virtual	50,000	50,000

制限に達してから、新しい、以前検出されなかったユーザをシステムが検出すると、アイデンティティ ソースに基づいてユーザ データに優先順位が付けられます。

- 新しいユーザが権限のないソースからである場合、権限のないユーザはデータベースに追加されません。新規ユーザを追加できるようにするには、手動でユーザを削除するか、データベースを消去する必要があります。
- 新しいユーザが権限のあるアイデンティティ ソースからである場合、システムは最も長い期間にわたって非アクティブのままになっている権限のないユーザを削除し、データベースに新しい権限のあるユーザを追加します。

  権限のあるユーザ以外いない場合、システムは最も長い期間にわたって非アクティブのままになっている権限のないユーザを削除し、データベースに新しいユーザを追加します。

（注） 展開に ASDM によって管理される ASA FirePOWER モジュールが含まれる場合、Firepower Management Center モデルに関係なく、最大 2,000 の権限のあるユーザを保存できます。

ヒント トラフィック ベースの検出を使用している場合、プロトコルによるユーザ ロギングを制限すると、ユーザ名の散乱を最小限に抑え、データベースのスペースを残しておくことができます。たとえば、システムが AIM、POP3、および IMAP トラフィックで検出されたユーザを追加できないようにすることができます（モニタを望んでいない特定の契約業者または訪問者からのトラフィックであることがわかっているため）。

第 98 章

ホスト ID ソース

次のトピックでは、ホスト ID ソースについて説明します。

概要：ホストのデータ収集

Firepower システムはネットワークを通過するトラフィックを受動的に監視するため、ネットワーク トラフィックからの特定のパケット ヘッダー値とその他の固有データを設定された定義と比較して（フィンガープリントと呼ばれる）、ネットワーク上のホストに関する次の情報を判断します。

- ホストの台数と種類（ブリッジ、ルータ、ロード バランサ、NAT デバイスなどのネットワーク デバイスを含む）
- ネットワーク上の検出ポイントからホストまでのホップ数を含む、基本的なネットワーク トポロジ データ
- ホスト上で実行中のオペレーティング システム
- ホスト上のアプリケーションとそのアプリケーションに関連付けられているユーザ

システムがホストのオペレーティング システムを特定できない場合、カスタムのクライアントまたはサーバのフィンガープリントを作成できます。システムはこれらのフィンガープリントを使用して新しいホストを特定します。フィンガープリントを脆弱性データベース（VDB）内のシステムにマップすることにより、カスタム フィンガープリントを使用してホストが特定されるたびに適切な脆弱性情報を表示できます。

（注） システムはモニタ対象のネットワーク トラフィックからだけでなく、エクスポートされた NetFlow レコードからもホスト データを収集することができ、また Nmap スキャンやホスト入力機能を使用してアクティブにホスト データを追加することもできます。

システムが検出できるホストオペレーティングシステムの判別

システムがどのオペレーティング システムのフィンガープリントを作成できるかを確認するには、カスタム OS フィンガープリントの作成プロセス中に表示される、使用可能なフィンガープリントの一覧を表示します。

ステップ 1 **[Policies]** > **[Network Discovery]**を選択します。

ステップ 2 [カスタム OS（Custom Operating Systems）] をクリックします。

ステップ 3 [カスタム フィンガープリントの作成（Create Custom Fingerprint）] をクリックします。

ステップ 4 [OS 脆弱性マッピング（OS Vulnerability Mappings）] セクションにあるドロップダウン リスト内のオプションのリストを表示します。これらのオプションが、システムがフィンガープリントを作成できるオペレーティング システムになります。

次のタスク

必要に応じて、ホスト オペレーティング システムの識別（2496 ページ）を参照してください。

ホスト オペレーティング システムの識別

システムがホストのオペレーティング システムを正しく識別しない場合（たとえばホスト プロファイル「不明」を示したり間違って識別したりする場合）には、下記の方法を試してください。

次のいずれかの方法を試します。

- ネットワーク検出アイデンティティ競合設定を確認します。
- ホストのカスタム フィンガープリントを作成します。
- ホストに対して Nmap スキャンを実行します。
- ホスト入力機能を使用して、ネットワーク マップにデータをインポートします。

- オペレーティング システム情報を手動で入力します。

カスタムフィンガープリント

Firepower システムには、検出された各ホストのオペレーティング システムを識別するためにシステムが使用するオペレーティング システムのフィンガープリントが含まれます。しかし、オペレーティング システムに一致するフィンガープリントがないため、システムがホスト オペレーティング システムを識別できない、または誤って識別することがあります。この問題を解決するために、不明または誤認されたオペレーティング システムに固有のオペレーティング システム特性のパターンを提供するカスタム フィンガープリントを作成し、識別用のオペレーティング システムの名前を提供することができます。

システムはオペレーティング システムのフィンガープリントから各ホストの脆弱性リストを取得するため、システムがホストのオペレーティング システムを照合できない場合、ホストの脆弱性を識別することはできません。たとえば、システムが Microsoft Windows を実行中のホストを検出した場合、そのシステムには保存された Microsoft Windows の脆弱性リストが存在します。このリストは、検出した Windows オペレーティング システムに基づいて、そのホストのホスト プロファイルに追加されます。

たとえば、ネットワーク上に Microsoft Windows の新しいベータ バージョンを実行中の複数のデバイスがある場合、システムはそのオペレーティング システムを識別できず、脆弱性をそれらのホストにマッピングすることもできません。しかし、システムに Microsoft Windows に関する脆弱性のリストがあるならば、同じオペレーティング システムを実行中の他のホストを識別できるように、いずれか 1 台のホストに対してカスタム フィンガープリントを作成できます。フィンガープリントに Microsoft Windows の脆弱性リストのマッピングを含め、フィンガープリントに一致する各ホストとそのリストを関連付けることができます。

カスタム フィンガープリントを作成すると Firepower Management Center は、同じオペレーティング システムを実行中のすべてのホストに関するそのフィンガープリントに関連付けられた脆弱性のセットをリストします。ユーザが作成したカスタム フィンガープリントに脆弱性マッピングが 1 つも存在しない場合、システムはフィンガープリントを使用して、フィンガープリントで提供するカスタム オペレーティング システムの情報を割り当てます。以前に検出されたホストからの新しいトラフィックが確認されると、システムはそのホストを新しいフィンガープリント情報で更新します。さらに、そのオペレーティング システムを実行する新しいホストの最初の検出時に、新しいフィンガープリントを使用して識別します。

カスタム フィンガープリントを作成する前に、ホストが正しく識別されない理由を特定して、カスタム フィンガープリントが実行可能なソリューションであるかどうかを判断する必要があります。

以下の 2 種類のフィンガープリントを作成できます。

- クライアントのフィンガープリント。ネットワーク上の別のホストで実行中の TCP アプリケーションに接続されている場合、ホストが送信する SYN パケットに基づいてオペレーティング システムを識別します。

- サーバのフィンガープリント。実行中の TCP アプリケーションへの着信接続に応答するためにホストが使用する SYN-ACK パケットに基づいてオペレーティング システムを識別します。

（注） クライアントとサーバの両方のフィンガープリントが同じホストに一致する場合、クライアントのフィンガープリントが使用されます。

フィンガープリントを作成した後、システムがフィンガープリントをホストに関連付けるには、その前に、フィンガープリントを有効化する必要があります。

関連トピック

クライアント用のカスタム フィンガープリントの作成 （2501 ページ）
サーバ用のカスタム フィンガープリントの作成 （2504 ページ）

フィンガープリントの管理

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	リーフのみ	Admin/Discovery Admin

フィンガープリントを作成してアクティブにした後、フィンガープリントを編集して変更を加えたり、脆弱性マッピングを追加したりできます。

ステップ 1 **[Policies]** > **[Network Discovery]**を選択します。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 2 [カスタム OS（Custom Operating Systems）] をクリックします。システムがフィンガープリントを作成するデータを待機している場合、フィンガープリントが作成されるまで 10 秒ごとに自動的に更新されます。

ステップ 3 カスタムのフィンガープリントを管理します。

- アクティブ化/非アクティブ化：フィンガープリントをアクティブ化または非アクティブ化します。詳細については、フィンガープリントのアクティブおよび非アクティブの設定 （2499 ページ）を参照してください。
- 作成：フィンガープリントを作成します。詳細については、クライアント用のカスタム フィンガープリントの作成 （2501 ページ）およびサーバ用のカスタム フィンガープリントの作成 （2504 ページ）を参照してください。
- 編集：フィンガープリントを編集します。詳細については、アクティブなフィンガープリントの編集 （2499 ページ）および非アクティブなフィンガープリントの編集 （2500 ページ）を参照してください。

- 削除：削除するフィンガープリントの横にある削除アイコン（）をクリックして、確認のために [OK] をクリックします。削除できるのは、非アクティブ化したフィンガープリントのみです。

フィンガープリントのアクティブおよび非アクティブの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	リーフのみ	Admin/Discovery Admin

ホストを識別するためにシステムがカスタム フィンガープリントを使用できるようにするには、その前に、カスタムフィンガープリントをアクティブにする必要があります。新しいフィンガープリントがアクティブにされた後は、以前に検出したホストを再識別し、新しいホストを検出するために使用されます。

フィンガープリントの使用を停止する場合は、それを非アクティブにすることができます。フィンガープリントを非アクティブにすると、フィンガープリントは使用できなくなりますが、システム上で維持できます。フィンガープリントを非アクティブにすると、オペレーティング システムは、フィンガープリントを使用しているホストに対して不明としてマークされます。ホストが再度検出され、別のアクティブなフィンガープリントに一致すると、ホストはそのアクティブなフィンガープリントによって識別されます。

フィンガープリントを削除すると、システムから完全に削除されます。フィンガープリントを非アクティブにした後に削除できます。

ステップ 1 **[Policies]** > **[Network Discovery]**を選択します。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 2 [カスタム OS（Custom Operating Systems）] をクリックします。

ステップ 3 アクティブまたは非アクティブにするフィンガープリントの横にあるスライダをクリックします。

（注） アクティブ化オプションは、作成したフィンガープリントが有効である場合に限り使用できます。スライダが使用できない場合、フィンガープリントを再作成してください。

アクティブなフィンガープリントの編集

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	リーフのみ	Admin/Discovery Admin

フィンガープリントがアクティブである場合、フィンガープリントの名前、説明、オペレーティング システムのカスタム表示の変更、および追加の脆弱性のフィンガープリントへのマッピングを行えます。

フィンガープリントの名前、説明、オペレーティング システムのカスタム表示の変更、および追加の脆弱性のフィンガープリントへのマッピングを行えます。

ステップ 1 **[Policies]** > **[Network Discovery]**を選択します。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 2 [カスタム オペレーティング システム（Custom Operating Systems）] をクリックします。

ステップ 3 編集するフィンガープリントの横にある編集アイコン（  ）をクリックします。

ステップ 4 必要に応じて、フィンガープリントの名前、説明、およびカスタム OS 表示を変更します。

ステップ 5 脆弱性マッピングを削除する場合は、ページの [事前定義された OS 製品マップ（Pre-Defined OS Product Maps）] セクションのマッピングの横にある [削除（Delete）] をクリックします。

ステップ 6 脆弱性マッピングにその他のオペレーティング システムを追加する場合は、[製品（Product）] を選択し（該当する場合は [メジャー バージョン（Major Version）]、[マイナー バージョン（Minor Version）]、[リビジョン バージョン（Revision Version）]、[ビルド（Build）]、[パッチ（Patch）]、および [拡張（Extension）] も選択します）、[OS 定義の追加（Add OS Definition）] をクリックします。

脆弱性マッピングが、[事前定義された OS 製品マップ（Pre-Defined OS Product Maps）] リストに追加されます。

ステップ 7 **[保存（Save）]** をクリックします。

非アクティブなフィンガープリントの編集

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	リーフのみ	Admin/Discovery Admin

フィンガープリントが非アクティブである場合は、フィンガープリントのすべての要素を変更し、それらを Firepower Management Center に再送信できます。これには、フィンガープリントのタイプ、ターゲットの IP アドレスとポート、脆弱性マッピングなど、フィンガープリントの作成時に指定したすべてのプロパティが含まれます。非アクティブのフィンガープリントを編集および送信すると、システムに再送信されます。また、それがクライアントのフィンガープリントである場合、アクティブにする前に、アプライアンスにトラフィックを再送信する必要があります。非アクティブのフィンガープリントに対して選択できる脆弱性マッピングは 1 つだけであることに注意してください。フィンガープリントをアクティブにした後、追加のオペレーティング システムおよびバージョンを脆弱性リストにマッピングすることができます。

ステップ 1 **[Policies]** > **[Network Discovery]**を選択します。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 2 [カスタム OS（Custom Operating Systems）] をクリックします。

ステップ 3 編集するフィンガープリントの横にある編集アイコン（  ）をクリックします。

ステップ 4 必要に応じてフィンガープリントを変更します。

- クライアントのフィンガープリントを変更している場合は、クライアント用のカスタム フィンガープリントの作成 （2501 ページ）を参照してください。
- サーバのフィンガープリントを変更している場合は、サーバ用のカスタム フィンガープリントの作成（2504 ページ）を参照してください。

ステップ 5 [保存（Save）] をクリックします。

次のタスク

- クライアントのフィンガープリントを変更した場合は、ホストからフィンガープリントを収集しているアプライアンスにトラフィックを必ず送信してください。

クライアント用のカスタム フィンガープリントの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	リーフのみ	Admin/Discovery Admin

クライアントのフィンガープリントは、クライアントがネットワーク上の別のホストで実行する TCP アプリケーションに接続されている場合、ホストが送信する SYN パケットに基づいてオペレーティング システムを識別します。

Firepower Management Centerが監視対象ホストと直接通信することがない場合は、クライアントのフィンガープリントのプロパティを指定するときに、FMCによって管理され、フィンガープリントを作成するホストに最も近いデバイスを指定することができます。

フィンガープリント作成プロセスを開始する前に、フィンガープリントを作成するホストに関する次の情報を取得します。

- ホストとフィンガープリントを取得するために使用する Firepower Management Center またはデバイスの間のネットワーク ホップの数。（Cisco では、ホストが接続されている同じサブネットに Firepower Management Center またはデバイスを直接接続することを強く推奨します）。

- ホストが存在するネットワークに接続されているネットワーク インターフェイス（Firepower Management Center またはデバイス上）。
- ホストの実際のオペレーティング システム ベンダー、製品、バージョン。
- クライアント トラフィックを生成するためのホストへのアクセス。

ステップ 1 **[Policies]** > **[Network Discovery]**を選択します。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 2 [カスタム OS（Custom Operating Systems）] をクリックします。

ステップ 3 [カスタム フィンガープリントの作成（Create Custom Fingerprint）] をクリックします。

ステップ 4 [デバイス（Device）] ドロップダウンリストから、フィンガープリントを収集するために使用する Firepower Management Center またはデバイスを選択します。

ステップ 5 [フィンガープリント名（Fingerprint Name）] を入力します。

ステップ 6 [フィンガープリントの説明（Fingerprint Description）] を入力します。

ステップ 7 [フィンガープリント タイプ（Fingerprint Type）] リストから、[クライアント（Client）] を選択します。

ステップ 8 [ターゲット IP アドレス（Target IP Address）] フィールドで、フィンガープリントを作成するホストの IP アドレスを入力します。

フィンガープリントは、ホストに他の IP アドレスが存在していても、ユーザが指定したホスト IP アドレスから送受信されるトラフィックにのみ基づくことに注意してください。

ステップ 9 [ターゲット距離（Target Distance）] フィールドで、前の手順で選択したフィンガープリントを収集するデバイスとホストの間のネットワーク ホップ数を入力します。

注意 これは、ホストへの実際の物理ネットワーク ホップ数である必要があります。システムによって検出されるホップ数と同じになる場合も、同じにならない場合もあります。

ステップ 10 [インターフェイス（Interface）] リストから、ホストが存在するネットワーク セグメントに接続されているネットワーク インターフェイスを選択します。

注意 Cisco では、いくつかの理由でフィンガープリントの作成に管理対象デバイスのセンシング インターフェイスを使用**しない**ことを推奨します。まず、フィンガープリントは、センシング インターフェイスが SPAN ポート上にあると機能しません。また、デバイスでセンシング インターフェイスを使用する場合、デバイスはフィンガープリントを収集している間、ネットワークの監視を停止します。ただし、フィンガープリントの収集を実行するために、管理インターフェイスまたはその他の使用可能なネットワーク インターフェイスを使用できます。どのインターフェイスがデバイスのセンシング インターフェイスであるかがわからない場合は、フィンガープリントの作成に使用している特定のモデルのインストレーション ガイドを参照してください。

ステップ 11 フィンガープリントを作成したホストのホストプロファイルのカスタム情報を表示する場合（またはフィンガープリントを作成するホストが [OS 脆弱性マッピング（OS Vulnerability Mappings）] セクションに

存在しない場合）、[カスタム OS 表示の使用（Use Custom OS Display）] を選択して、次に示すように表示する値を指定します。

- [ベンダー文字列（Vendor String）] フィールドに、オペレーティング システムのベンダー名を入力します。たとえば、Microsoft Windows のベンダーは「Microsoft」になります。
- [製品文字列（Product String）] フィールドに、オペレーティング システムの製品名を入力します。たとえば、Microsoft Windows 2000 の製品名は「Windows」になります。
- [バージョン文字列（Version String）] フィールドに、オペレーティング システムのバージョン番号を入力します。たとえば、Microsoft Windows 2000 のバージョン番号は「2000」になります。

ステップ 12 [OS 脆弱性マッピング（OS Vulnerability Mappings）] セクションで、脆弱性マッピングに使用するオペレーティング システム、製品、およびバージョンを選択します。

フィンガープリントを使用して一致するホストの脆弱性を識別する場合、またはオペレーティング システムのカスタム表示情報を割り当てない場合、このセクションで[ベンダー（Vendor）] と [製品（Product）] の値名を指定する必要があります。

オペレーティング システムのすべてのバージョンの脆弱性をマッピングするには、[ベンダー（Vendor）] および [製品（Product）] の値のみを指定します。

（注） [メジャー バージョン（Major Version）]、[マイナー バージョン（Minor Version）]、[リビジョン バージョン（Revision Version）]、[ビルド（Build）]、[パッチ（Patch）]、および [拡張（Extension）] ドロップダウンリストのオプションの中には、選択したオペレーティング システムに該当しないものもあります。また、フィンガープリントを作成するオペレーティング システムに一致するリストに表示される定義がない場合は、それらの値を空のままにすることができます。フィンガープリントで OS の脆弱性マッピングを作成しない場合、システムはそのフィンガープリントを使用して、脆弱性リストをフィンガープリントによって識別されるホストに割り当てることはできないことに注意してください。

例：

たとえば、カスタム フィンガープリントで Redhat Linux 9 の脆弱性リストを一致するホストに割り当てる場合、ベンダーとして [Redhat, Inc.]、製品として [Redhat Linux]、メジャー バージョンとして [9] を選択します。

例：

Palm OS のすべてのバージョンを追加するには、[ベンダー（Vendor）] リストから [PalmSource, Inc.]、[製品（Product）] リストから [Palm OS] を選択し、その他のすべてのリストはデフォルトの設定のままにします。

ステップ 13 [作成（Create）] をクリックします。

ステータスは一時的に [新規（New）] になってから、[保留中（Pending）] に切り替わります。フィンガープリントのトラフィックが確認されるまで、このステータスが維持されます。トラフィックが確認されると、[使用可（Ready）] に切り替わります。

当該のホストからデータを受信するまで、[カスタム フィンガープリント（Custom Fingerprint）] ステータス ページは 10 秒ごとに更新されます。

ステップ 14 ターゲット IP アドレスとして指定した IP アドレスを使用して、フィンガープリントを作成しようとしているホストにアクセスし、アプライアンスへの TCP 接続を開始します。

正確なフィンガープリントを作成するためには、トラフィックがフィンガープリントを収集するアプライアンスで認識される**必要**があります。スイッチを経由して接続している場合は、アプライアンス以外のシステムへのトラフィックはシステムによって認識されない場合があります。

例：

フィンガープリントを作成しようとしているホストから Firepower Management Center の Web インターフェイスにアクセスするか、ホストから SSH で FMC にアクセスします。SSH を使用する場合は、次に示すコマンドを使用します。このコマンドの localIPv6address は、現在ホストに割り当てられているステップ 7 で指定した IPv6 アドレスです。DCmanagementIPv6address は、FMC の管理 IPv6 アドレスです。[カスタム フィンガープリント（Custom Fingerprint）] ページが [使用可（Ready）] ステータスでリロードされるようになります。

```
ssh -b localIPv6address DCmanagementIPv6address
```

次のタスク

- フィンガープリントのアクティブおよび非アクティブの設定（2499 ページ） で説明するように、フィンガープリントをアクティブにします。

サーバ用のカスタム フィンガープリントの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	リーフのみ	Admin/Discovery Admin

サーバのフィンガープリントは、実行中の TCP アプリケーションへの着信接続に応答するためにホストが使用する SYN-ACK パケットに基づいてオペレーティング システムを識別します。開始する前に、フィンガープリントを作成するホストに関する次の情報を取得します。

- ホストとフィンガープリントを取得するために使用するアプライアンスの間のネットワーク ホップの数。Cisco では、ホストが接続されている同じサブネットにアプライアンスの使用されていないインターフェイスを直接接続することを強く推奨します。
- ホストが存在するネットワークに接続されているネットワーク インターフェイス（アプライアンス上）。
- ホストの実際のオペレーティング システム ベンダー、製品、バージョン。
- 現在使用されておらず、ホストが存在するネットワーク上で許可されている IP アドレス。

ヒント　Firepower Management Center が監視対象ホストと直接通信することがない場合は、サーバのフィンガープリントのプロパティを指定するときに、フィンガープリントを作成するホストに最も近い管理対象デバイスを指定することができます。

ステップ 1　**[Policies]** > **[Network Discovery]**を選択します。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 2　[カスタム OS（Custom Operating Systems）] をクリックします。

ステップ 3　[カスタム フィンガープリントの作成（Create Custom Fingerprint）] をクリックします。

ステップ 4　[デバイス（Device）] リストから、フィンガープリントを収集するために使用する Firepower Management Center または管理対象デバイスを選択します。

ステップ 5　[フィンガープリント名（Fingerprint Name）] を入力します。

ステップ 6　[フィンガープリントの説明（Fingerprint Description）] を入力します。

ステップ 7　[フィンガープリント タイプ（Fingerprint Type）] リストから、サーバのフィンガープリント作成オプションを表示する [サーバ（Server）] を選択します。

ステップ 8　[ターゲット IP アドレス（Target IP Address）] フィールドで、フィンガープリントを作成するホストの IP アドレスを入力します。

フィンガープリントは、ホストに他の IP アドレスが存在していても、ユーザが指定したホスト IP アドレスから送受信されるトラフィックにのみ基づくことに注意してください。

注意　Firepower システムのバージョン 5.2 以降を実行するアプライアンスでのみ IPv6 フィンガープリントをキャプチャできます。

ステップ 9　[ターゲット距離（Target Distance）] フィールドで、前の手順で選択したフィンガープリントを収集するデバイスとホストの間のネットワーク ホップ数を入力します。

注意　これは、ホストへの実際の物理ネットワーク ホップ数である必要があります。システムによって検出されるホップ数と同じになる場合も、同じにならない場合もあります。

ステップ 10　[インターフェイス（Interface）] リストから、ホストが存在するネットワーク セグメントに接続されているネットワーク インターフェイスを選択します。

注意　Cisco では、いくつかの理由でフィンガープリントの作成に管理対象デバイスのセンシング インターフェイスを使用**しない**ことを推奨します。まず、フィンガープリントは、センシング インターフェイスが SPAN ポート上にあると機能しません。また、デバイスでセンシング インターフェイスを使用する場合、デバイスはフィンガープリントを収集している間、ネットワークの監視を停止します。ただし、フィンガープリントの収集を実行するために、管理インターフェイスまたはその他の使用可能なネットワーク インターフェイスを使用できます。どのインターフェイスがデバイスのセンシング インターフェイスであるかがわからない場合は、フィンガープリントの作成に使用している特定のモデルのインストレーション ガイドを参照してください。

ステップ 11 [アクティブなポートを取得（Get Active Ports）] をクリックします。

ステップ 12 [サーバ ポート（Server Port）] フィールドに、フィンガープリントを収集するように選択したデバイスが通信を開始するポートを入力します。または、[アクティブ ポートの取得（Get Active Ports）] ドロップダウンリストからポートを選択します。

ホストでオープンしていると判明しているすべてのサーバ ポートを使用できます（たとえば、ホストで Web サーバを実行している場合は 80）。

ステップ 13 [送信元 IP アドレス（Source IP Address）] フィールドで、ホストとの通信を試行するために使用する IP アドレスを入力します。

ネットワークでの使用が許可されていて、現在未使用の送信元 IP アドレス（たとえば、現在使用されていない DHCP プール アドレス）を使用する必要があります。これにより、フィンガープリントの作成中に、別のホストを一時的にオフラインにすることを防ぎます。

フィンガープリントを作成している間は、その IP アドレスをネットワーク検出ポリシーでモニタリングから除外する必要があります。そうしていないと、ネットワーク マップおよびディスカバリ イベント ビューに、その IP アドレスによって表されるホストに関する不正確な情報が混在することになります。

ステップ 14 [送信元サブネット マスク（Source Subnet Mask）] フィールドには、ユーザが使用している IP アドレスのサブネット マスクを入力します。

ステップ 15 [送信元ゲートウェイ（Source Gateway）] フィールドが表示されたら、ホストへのルートを確立するために使用するデフォルトのゲートウェイ IP アドレスを入力します。

ステップ 16 フィンガープリントを作成したホストのホスト プロファイルのカスタム情報を表示する場合、または使用するフィンガープリントの名前が [OS 定義（OS Definition）] セクションに存在しない場合、[カスタム OS 表示（Custom OS Display）] セクションの [カスタム OS 表示の使用（Use Custom OS Display）] を選択します。

以下のように、ホスト プロファイルで表示する値を入力します。

- [ベンダー文字列（Vendor String）] フィールドに、オペレーティング システムのベンダー名を入力します。たとえば、Microsoft Windows のベンダーは「Microsoft」になります。
- [製品文字列（Product String）] フィールドに、オペレーティング システムの製品名を入力します。たとえば、Microsoft Windows 2000 の製品名は「Windows」になります。
- [バージョン文字列（Version String）] フィールドに、オペレーティング システムのバージョン番号を入力します。たとえば、Microsoft Windows 2000 のバージョン番号は「2000」になります。

ステップ 17 [OS 脆弱性マッピング（OS Vulnerability Mappings）] セクションで、脆弱性マッピングに使用するオペレーティング システム、製品、およびバージョンを選択します。

フィンガープリントを使用して一致するホストの脆弱性を識別する場合、またはオペレーティング システムのカスタム表示情報を割り当てない場合、このセクションでベンダーと製品名を指定する必要があります。

オペレーティング システムのすべてのバージョンの脆弱性をマッピングするには、ベンダーおよび製品名のみを指定します。

（注） [メジャー バージョン（Major Version）]、[マイナー バージョン（Minor Version）]、[リビジョン バージョン（Revision Version）]、[ビルド（Build）]、[パッチ（Patch）]、および [拡張（Extension）] ドロップダウンリストのオプションの中には、選択したオペレーティング システムに該当しないものもあります。また、フィンガープリントを作成するオペレーティング システムに一致するリストに表示される定義がない場合は、それらの値を空のままにすることができます。フィンガープリントで OS の脆弱性マッピングを作成しない場合、システムはそのフィンガープリントを使用して、脆弱性リストをフィンガープリントによって識別されるホストに割り当てることはできないことに注意してください。

例：

カスタム フィンガープリントで Redhat Linux 9 の脆弱性リストを一致するホストに割り当てる場合、ベンダーとして [Redhat, Inc.]、製品として [Redhat Linux]、バージョンとして [9] を選択します。

例：

Palm OS のすべてのバージョンを追加するには、[ベンダー（Vendor）] リストから [PalmSource, Inc.]、[製品（Product）] リストから [Palm OS] を選択し、その他のすべてのリストはデフォルトの設定のままにします。

ステップ 18 [作成（Create）] をクリックします。
[カスタム フィンガープリント（Custom Fingerprint）] ステータス ページは 10 秒ごとに更新され、[使用可（Ready）] ステータスでリロードされます。

（注） ターゲット システムがフィンガープリント作成プロセス中に応答を停止した場合、ステータスにはメッセージ「エラー：応答がありません（ERROR: No Response）」が示されます。このメッセージが表示された場合は、フィンガープリントを再度送信します。3 ～ 5 分間（時間はターゲット システムによって異なる場合があります）待機して、編集アイコン（）をクリックし、[カスタム フィンガープリント（Custom Fingerprint）] ページにアクセスしてから [作成（Create）] をクリックします。

次のタスク

- フィンガープリントのアクティブおよび非アクティブの設定（2499 ページ） で説明するように、フィンガープリントをアクティブにします。

ホスト入力データ

サードパーティからネットワーク マップ データをインポートすることで、ネットワーク マップを増強することができます。また、Web インターフェイスを使用して、オペレーティング システムまたはアプリケーションの ID を変更するか、アプリケーション プロトコル、プロトコル、ホスト属性、クライアントを削除することによって、ホスト入力機能を使用することができます。

システムは複数のソースからのデータを照合して、オペレーティング システムまたはアプリケーションの現行 ID を判別できます。

ネットワークマップから影響を受けるホストを削除すると、サードパーティの脆弱性を除くすべてのデータは破棄されます。スクリプトまたはインポートファイルの設定方法の詳細については、『*Firepower* システム ホスト入力 *API* ガイド』を参照してください。

影響の関連付けにインポートしたデータを含めるには、データベースのオペレーティングシステムおよびアプリケーション定義にデータをマッピングする必要があります。

サードパーティのデータを使用するための要件

ネットワーク上のサードパーティのシステムから検出データをインポートできます。ただし、Firepower の推奨、アダプティブ プロファイルの更新、影響評価などの侵入データおよび検出データを共に使用する機能を有効にするには、対応する定義に対して、可能な限り多くのエレメントをマッピングする必要があります。サードパーティのデータを使用するには、以下の要件を考慮してください：

- サードパーティのシステムにネットワーク アセット上に特定のデータがある場合、ホスト入力機能によりそのデータをインポートできます。しかし、サードパーティが異なる製品名をつける可能性があることから、対応する Cisco 製品の定義に対して、サードパーティベンダー、製品、バージョンをマッピングする必要があります。製品をマッピング後、Firepower Management Center 設定の影響を評価するために脆弱性のマッピングを有効にして、影響相関を可能にします。バージョンまたはベンダーに関係のないアプリケーション プロトコルでは、Firepower Management Center 設定におけるアプリケーション プロトコルの脆弱性をマッピングする必要があります。
- サードパーティからパッチ情報をインポートし、そのパッチで修正されたすべての脆弱性に無効とマークする場合は、サードパーティの修正名をデータベースの修正定義にマッピングする必要があります。修正によって解決された脆弱性はすべて、その修正を加えるホストから排除されます。
- オペレーティング システムやアプリケーション プロトコルの脆弱性をサードパーティからインポートし、これらを影響相関に使用する場合、サードパーティの脆弱性識別文字列をデータベース内の脆弱性にマッピングする必要があります。多くのクライアントは、脆弱性と関連があり、影響評価に使用されますが、サードパーティのクライアントの脆弱性をインポートし、マッピングすることはできない点にご注意ください。脆弱性のマッピング後、Firepower Management Center 設定の影響評価のためにサードパーティの脆弱性のマッピングを有効にします。ベンダー情報やバージョン情報のないアプリケーションプロトコルを脆弱性にマッピングするには、管理ユーザは、Firepower Management Center 設定のアプリケーションの脆弱性もマッピングする必要があります。
- アプリケーションデータをインポートし、そのデータを影響相関に使用する場合、各アプリケーションプロトコルのベンダー文字列を対応する Cisco アプリケーションプロトコルの定義にマッピングする必要があります。

関連トピック

サードパーティの製品のマッピング （2509 ページ）
サード パーティ製品の修正のマッピング （2511 ページ）
サードパーティの脆弱性のマッピング （2512 ページ）

サーバの脆弱性のマッピング （1316 ページ）
カスタム製品マッピングの作成 （2513 ページ）

サードパーティ製品のマッピング

ユーザ入力機能を使用して各サードパーティからのデータをネットワーク マップに追加する場合、サードパーティで使用するベンダー、製品、およびバージョンの各名前を Cisco 製品定義にマッピングする必要があります。各製品を Cisco の定義にマッピングすると、これらの定義に基づいて脆弱性が割り当てられます。

同様に、パッチ管理製品などのサードパーティからのパッチ情報をインポートする場合、その修正の名前をデータベース内の適切なベンダー、製品、および対応する修正にマッピングする必要があります。

サードパーティの製品のマッピング

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin

サード パーティからデータをインポートする場合、そのデータを使用して脆弱性を指定したり、影響の関連付けを行ったりするために、シスコの製品をサードパーティの名前にマッピングする必要があります。製品をマッピングすることにより、シスコの脆弱性情報をサードパーティ製品の名前に関連付けます。これにより、システムはそのデータを使用して影響の関連付けを行うことができます。

ホスト入力のインポート機能を使用してデータをインポートする場合、AddScanResult 機能を使用して、インポート中にサードパーティ製品をオペレーティング システムとアプリケーションの脆弱性にマップピングすることもできます。

たとえば、Apache Tomcat をアプリケーションとしてリストしているサード パーティのデータをインポートする場合で、それがバージョン 6 の Apache Tomcat であれば、以下のように設定し、サード パーティのマッピングを追加します。

- ベンダー名を [Apache] に設定します。
- プロダクト名に [Tomcat] 設定します。
- ベンダーのドロップダウン リストから [Apache] を選択します。
- 製品のドロップダウン リストから [Tomcat] を選択します。
- バージョンのドロップダウン リストから [6] を選択します。

このマッピングによって、Apache Tomcat 6 のすべての脆弱性が、Apache Tomcat をアプリケーションとしてリストアップするホストに割り当てられます。

バージョン情報やベンダー情報のないのアプリケーションの場合、Firepower Management Center 構成のアプリケーション タイプで脆弱性をマッピングする必要があります。多くのクライアン

トには関連付けられた脆弱性があり、クライアントが影響アセスメントに使用されますが、サードパーティのクライアントの脆弱性をインポートしてマッピングすることはできないことに注意してください。

ヒント　すでに別の Firepower Management Center にサードパーティのマッピングを作成している場合、そのマッピングをエクスポートして、この FMC にインポートすることができます。その後、必要に応じてインポートしたマッピングを編集できます。

ステップ 1　**[Policies]** > **[Application Detectors]**を選択します。

ステップ 2　[ユーザ サードパーティ マッピング（User Third-Party Mappings）] をクリックします。

ステップ 3　次の 2 つの選択肢があります。

- [作成（Creat）] : 新しいマップ セットを作成するには、[製品マップ セットの作成（Create Product Map Set）] をクリックします。
- [編集（Edit）] : 既存のマップ セットを編集するには、そのマップ セットの横にある編集アイコン（）をクリックします。代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 4　[マッピング セット名（Mapping Set Name）] を入力します。

ステップ 5　[説明（Description）] を入力します。

ステップ 6　次の 2 つの選択肢があります。

- [作成（Creat）] : サード パーティ製品をマッピングするには、[製品マップの追加（Add Product Map）] をクリックします。
- [編集（Edit）] : 既存のサードパーティの製品のマッピングを編集するには、そのマッピングの横にある編集アイコン（）をクリックします。代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 7　サードパーティの製品で使用される [ベンダーの文字列（Vendor String）] を入力します。

ステップ 8　サードパーティの製品で使用される [製品の文字列（Product String）] を入力します。

ステップ 9　サードパーティの製品で使用される [バージョン文字列（Version String）] を入力します。

ステップ 10　製品マッピング セクションで、ベンダーの脆弱性のマッピングに使用するオペレーティング システム、製品、製品バージョンを、以下の項目から選択します。[ベンダー（Vendor）]、[製品（Product）]、[メジャー バージョン（Major Version）]、[マイナー バージョン（Minor Version）]、[改訂バージョン（Revision Version）]、[ビルド（Build）]、[パッチ（Patch）]、[拡張子（Extension）]。

例：

名前がサードパーティの文字列で構成される製品を実行するホストで Red Hat Linux 9 の脆弱性マッピングを使用する場合、ベンダーとして [Redhat, Inc.]、製品として [Red Hat Linux]、バージョンとして [9] を選択します。

ステップ 11　**[保存（Save）]** をクリックします。

関連トピック

サーバの脆弱性のマッピング （1316 ページ）

サード パーティ製品の修正のマッピング

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin

修正名をデータベースの特定の修正セットにマッピングする場合、サードパーティのパッチ管理アプリケーションからデータをインポートし、修正を一連のホストに適用することができます。修正名がホストにインポートされると、システムはその修正によって解決されるすべての脆弱性をそのホストに対して無効としてマークします。

ステップ 1 **[Policies]** > **[Application Detectors]**を選択します。

ステップ 2 [ユーザ サードパーティ マッピング（User Third-Party Mappings）] をクリックします。

ステップ 3 次の 2 つの選択肢があります。

- [作成（Creat）]：新しいマップ セットを作成するには、[製品マップ セットの作成（Create Product Map Set）] をクリックします。
- [編集（Edit）]：既存のマップ セットを編集するには、そのマップ セットの横にある編集アイコン（  ）をクリックします。代わりに表示アイコン（  ）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 4 [マッピング セット名（Mapping Set Name）] を入力します。

ステップ 5 [説明（Description）] を入力します。

ステップ 6 次の 2 つの選択肢があります。

- 作成：サードパーティ製品をマッピングするには、[修正マップの追加（Add Fix Map）] をクリックします。
- 編集：既存のサードパーティ製品マップを編集するには、その横にある編集アイコン（  ）をクリックします。代わりに表示アイコン（  ）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 7 [サードパーティの修正名（Third-Party Fix Name）] フィールドにマッピングする修正の名前を入力します。

ステップ 8 [製品マッピング（Product Mappings）] セクションで、次のフィールドから修正マッピングに使用するオペレーティング システム、製品、およびバージョンを選択します。

- **Vendor**
- **製品**
- **メジャー バージョン**
- **マイナー バージョン**
- **リビジョン バージョン**
- **ビルド（Build）**

- パッチ
- 内線番号（**Extension**）

例：

Red Hat Linux 9 からパッチが適用されるホストにマッピングで修正を割り当てる場合は、ベンダーとして [Redhat, Inc.]、製品として [Redhat Linux]、バージョンとして [9] を選択します。

ステップ 9 [保存（Save）] をクリックして、修正マップを保存します。

サードパーティの脆弱性のマッピング

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin

サードパーティからの脆弱性情報を VDB に追加するには、インポートしたそれぞれの脆弱性のサードパーティ識別文字列を、既存の SVID、Bugtraq、または SID にマッピングする必要があります。脆弱性のマッピングを作成したら、マッピングはネットワーク マップのホストにインポートされたすべての脆弱性に対して機能し、それらの脆弱性に対する影響の関連付けを可能にします。

サードパーティの脆弱性に対する影響の関連付けを有効にし、関連付けの実行を可能にする必要があります。バージョンレスまたはベンダーレスのアプリケーションの場合、Firepower Management Center の設定でアプリケーション タイプの脆弱性をマッピングする必要もあります。

多くのクライアントには関連付けられた脆弱性があり、クライアントが影響評価に使用されますが、サードパーティのクライアントの脆弱性は影響評価に使用できません。

ヒント すでに別の Firepower Management Center にサードパーティのマッピングを作成している場合、そのマッピングをエクスポートして、この FMC にインポートすることができます。その後、必要に応じてインポートしたマッピングを編集できます。

ステップ 1 **[Policies]** > **[Application Detectors]**を選択します。

ステップ 2 [ユーザ サードパーティ マッピング（User Third-Party Mappings）] をクリックします。

ステップ 3 次の 2 つの選択肢があります。

- 作成：新しい脆弱性セットを作成するには、[脆弱性マップ セットの作成（Create Vulnerability Map Set）] をクリックします。
- 編集：既存の脆弱性セットを編集するには、脆弱性セットの横にある編集アイコン（ ）をクリックします。代わりに表示アイコン（ ）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 4 [脆弱性マップの追加（Add Vulnerability Map）] をクリックします。

ステップ 5 [脆弱性 ID（Vulnerability ID）] フィールドに脆弱性のサードパーティ ID を入力します。

ステップ 6 [脆弱性の説明（Vulnerability Description）] を入力します。

ステップ 7 必要に応じて、次の操作を実行します。

- [Snort 脆弱性 ID マッピング（Snort Vulnerability ID Mappings）] フィールドに [Snort ID] を入力します。
- [SVID マッピング（SVID Mappings）] フィールドに、レガシー脆弱性 ID を入力します。
- [Bugtraq 脆弱性 ID マッピング（Bugtraq Vulnerability ID Mappings）] フィールドに、Bugtraq ID 番号を入力します。

ステップ 8 [追加（Add）] をクリックします。

関連トピック

ネットワーク検出の脆弱性影響評価の有効化 （2666 ページ）
サーバの脆弱性のマッピング （1316 ページ）

カスタム製品マッピング

製品マッピングを使用して、サードパーティによるサーバ入力が適切なシスコ定義に関連付けられていることを確認できます。製品マッピングを定義し有効化した後、マッピングされたベンダー文字列を持つモニタ対象ホスト上のすべてのサーバまたはクライアントが、カスタム製品マッピングを使用します。したがって、サーバのベンダー、製品、バージョンを明示的に設定する代わりに、特定のベンダー文字列でネットワーク マップのすべてのサーバの脆弱性をマップすることをお勧めします。

カスタム製品マッピングの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin

システムが VDB のベンダーおよび製品にサーバをマッピングできない場合は、手動でマッピングを作成できます。カスタム製品マッピングをアクティブにすると、システムは指定されたベンダーおよび製品の脆弱性を、そのベンダー文字列が発生するネットワーク マップのすべてのサーバにマッピングします。

（注） カスタム製品マッピングは、アプリケーション データのソース（Nmap、ホスト入力機能、Firepower システム自体など）に関係なく、アプリケーション プロトコルのすべての発生に適用されます。ただし、ホスト入力機能を使用してインポートしたデータのサードパーティの脆弱性マッピングが、カスタム製品マッピングを介して設定したマッピングと競合する場合、サードパーティの脆弱性マッピングはカスタム製品マッピングをオーバーライドし、入力が発生したときにサードパーティの脆弱性マッピング設定を使用します。

製品マッピングリストを作成し、各リストをアクティブ化/非アクティブ化することによって、複数のマッピングの同時使用を有効にするか、無効にします。マッピングするベンダーを指定すると、そのベンダーによって作成された製品のみを含むように製品リストが更新されます。

カスタム製品マッピングを作成した後で、カスタム製品マッピングリストをアクティブにする必要があります。カスタム製品マッピングリストをアクティブにすると、指定されたベンダー文字列が発生するすべてのサーバが更新されます。ホスト入力機能を介してインポートされるデータでは、このサーバの製品マッピングをすでに明示的に設定していない限り、脆弱性が更新されます。

たとえば、組織が Apache Tomcat Web サーバのバナーの文字列を `Internal Web Server` に変更した場合、ベンダー文字列 `Internal Web Server` をベンダー **Apache** および製品 **Tomcat** にマッピングできます。その後、そのマッピングを含むリストをアクティブにすると、`Internal Web Server` とラベル付けされたサーバが存在するすべてのホストのデータベースに Apache Tomcat の脆弱性が想定されます。

ヒント この機能を使用して、もう 1 つの脆弱性にルールの SID をマッピングすることによって、ローカルの侵入ルールに脆弱性をマッピングすることができます。

ステップ 1 **[Policies]** > **[Application Detectors]**を選択します。

ステップ 2 [カスタム製品マッピング（Custom Product Mappings）] をクリックします。

ステップ 3 [カスタム製品マッピング リストの作成（Create Custom Product Mapping List）] をクリックします。

ステップ 4 [カスタム製品マッピング リスト名（Custom Product Mapping List Name）] を入力します。

ステップ 5 [ベンダー文字列の追加（Add Vendor String）] をクリックします。

ステップ 6 [ベンダー文字列（Vendor String）]フィールドに、選択したベンダーおよび製品値にマッピングする必要があるアプリケーションを識別するベンダー文字列を入力します。

ステップ 7 [ベンダー（Vendor）] ドロップダウン リストから、マッピングするベンダーを選択します。

ステップ 8 [製品（Product）] ドロップダウン リストから、マッピングする製品を選択します。

ステップ 9 [追加（Add）] をクリックして、マッピングしたベンダー文字列をリストに追加します。

ステップ 10 オプションで、さらにベンダー文字列のマッピングをリストに追加するには、必要に応じて手順 4 ～ 8 を繰り返します。

ステップ 11 [保存（Save）] をクリックします。

次のタスク

- カスタム製品マッピングリストをアクティブにします。詳細については、「カスタム製品マッピングのアクティブおよび非アクティブの設定（2515ページ）」を参照してください。

カスタム製品マッピング リストの編集

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin

ベンダー文字列を追加または削除したり、リスト名を変更したりして、既存のカスタム製品マッピング リストを変更できます。

ステップ 1 **[Policies]** > **[Application Detectors]**を選択します。

ステップ 2 [カスタム製品のマッピング（Custom Product Mappings）] をクリックします。

ステップ 3 編集する製品マッピング リストの横にある編集アイコン（  ）をクリックします。

代わりに表示アイコン（  ）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 4 カスタム製品マッピングの作成 （2513 ページ）の説明に従って、リストを変更します。

ステップ 5 終了したら、[保存（Save）] をクリックします。

カスタム製品マッピングのアクティブおよび非アクティブの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin

カスタム製品マッピング リスト全体の使用を一度に有効または無効にすることができます。カスタム製品マッピング リストをアクティブにすると、そのリストの各マッピングが、管理対象デバイスによって検出されたか、またはホスト入力機能を介してインポートされたかに関わらず、指定したベンダー文字列を持つすべてのアプリケーションに適用されます。

ステップ 1 **[Policies]** > **[Application Detectors]**を選択します。

ステップ 2 [カスタム製品のマッピング（Custom Product Mappings）] をクリックします。

ステップ 3 アクティブまたは非アクティブにするカスタム製品のマッピング リストの横にあるスライダをクリックします。

コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ホスト入力クライアントの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
機能に応じて異なる	機能に応じて異なる	FMC	いずれか（Any）	Admin/Discovery Admin

ホスト入力機能を使用すると、別のアプライアンスで実行されているクライアントプログラムから Firepower Management Center のネットワーク マップを更新できます。たとえば、ネットワーク マップからホストを追加または削除したり、ホストOSおよびサービス情報を更新したりできます。詳細については、*Firepower* システム ホスト入力 *API* ガイドを参照してください。

リモート クライアントを実行するには、その前に、[ホスト入力クライアント（Host Input Client）] ページから Firepower Management Center のピア データベースにクライアントを追加する必要があります。また、FMC によって生成された認証証明書をクライアントにコピーする必要もあります。この手順を完了すると、クライアントは FMC に接続できます。

マルチドメイン展開では、すべてのドメインにクライアントを作成できます。認証証明書を使用すると、クライアントは、クライアント証明書のドメインに関連付けられているリーフ ドメインにネットワーク マップ アップデートを送信できます。先祖ドメインの証明書を作成した場合（または後で証明書ドメインが子孫ドメインの追加後に先祖ドメインになった場合）、その証明書を使用するクライアントは、*Firepower* システム ホスト入力 *API* ガイドで説明するように、すべてのトランザクションのターゲット リーフ ドメインを指定する必要があります。

[ホスト入力クライアント（Host Input Client）] タブには、現在のドメインに関連付けられているクライアントのみが表示されるため、証明書をダウンロードまたは失効させるには、クライアントが作成されたドメインに切り替えます。

ステップ 1 **[System]** > **[Integration]**を選択します。

ステップ 2 [ホスト入力クライアント（Host Input Client）] タブをクリックします。

ステップ 3 [クライアントの作成（Create Client）] をクリックします。

ステップ 4 [ホスト名（Hostname）] フィールドに、ホスト入力クライアントを実行しているホストのホスト名または IP アドレスを入力します。

（注） DNS 解決を設定していない場合は、IP アドレスを使用します。

ステップ 5 証明書ファイルを暗号化するには、[Password] フィールドにパスワードを入力します。

ステップ 6 **[Save]** をクリックします。
ホスト入力サービスは、ホストが Firepower Management Center 上のポート 8307 にアクセスすることを許可し、クライアント/サーバ認証時に使用する認証証明書を作成します。

ステップ 7 証明書ファイルの横にあるファイル ダウンロード アイコン（  ）をクリックします。

ステップ 8 SSL/TLS 認証のためにクライアントが使用するディレクトリに証明書ファイルを保存します。

ステップ 9 クライアントのアクセスを取り消すには、削除するホストの横にある削除アイコン（）をクリックします。

Nmap スキャン

Firepower システムは、ネットワークのトラフィックをパッシブ分析してネットワーク マップを構築します。このパッシブ分析によって取得される情報は、システムの状態によっては不完全なことがよくあります。ただし、ホストをアクティブにスキャンすることで、完全な情報を取得できます。たとえば、オープンポート上で実行中のサーバがホストにあり、システムによるネットワークのモニタリング中にそのサーバがトラフィックを送受信しなかった場合、システムではそのサーバに関する情報をネットワークマップに追加しません。しかし、アクティブスキャナを使用して直接そのホストをスキャンすると、サーバの存在を検出できます。

Firepower システムには、Nmap™ という、ネットワーク調査およびセキュリティ監査を目的としたオープン ソースのアクティブ スキャナが統合されています。

Nmap を使用してホストをスキャンすると、システムは以下のように動作します。

- 前に検出されていないオープン ポート上のサーバを、該当するホストのホスト プロファイルの [サーバ（Servers）] リストに追加します。ホスト プロファイルの [スキャン結果（Scan Results）] セクションには、フィルタ処理されていたり閉じていたりしている TCP ポートやUDP ポート上で検出されたサーバがリストされます。デフォルトでは、Nmap は 1660 を超える TCP ポートをスキャンします。

  Nmap スキャンで識別されたサーバがシステムで認識され、対応するサーバ定義がシステムにある場合、システムは Nmap がそのサーバに使用する名前を、対応する Cisco サーバ定義にマップします。

- スキャン結果と 1500 を超える既知のオペレーティング システムのフィンガープリントを比較して、オペレーティング システムを判別し、それぞれにスコアを割り当てます。最高スコアのオペレーティング システムのフィンガープリントが、ホストに割り当てられるオペレーティング システムになります。

  システムは Nmap のオペレーティング システム名を Cisco のオペレーティング システム定義にマップします。

- 追加されたサーバおよびオペレーティング システムのホストに脆弱性を割り当てます。

（注）

- ホストがネットワーク マップ内になければ、Nmap は結果をホストプロファイルに追加することはできません。
- ホストがネットワーク マップから削除されると、そのホストに関する Nmap スキャン結果が破棄されます。

ヒント　スキャンオプションによっては（ポートスキャンなど）低帯域幅のネットワークに非常に負荷をかけることがあります。ネットワーク使用率が低い時間帯にこのようなタスクを実行するよう、スケジュールしてください。

スキャンに使用される基礎的な Nmap テクノロジーの詳細については、http://insecure.org/ にある Nmap のマニュアルを参照してください。

関連トピック

Nmap スキャンの自動化 （243 ページ）

Nmap 修復オプション

Nmap 修復を作成して、Nmap スキャンの設定を定義します。Nmap 修復は、相関ポリシー内で応答として使用したり、オンデマンドで実行したり、特定の時間に実行するようにスケジュールしたりできます。

Nmap により提供されるサーバやオペレーティング システムのデータは、もう 1 度 Nmap スキャンを実行するまで静的な状態のままであることに注意してください。Nmap を使用してホスト内でオペレーティング システムやサーバのデータをスキャンすることを計画している場合は、定期的なスキャンのスケジュールをセットアップして、Nmapによって提供されるオペレーティング システムやサーバのデータを最新に保つこともできます。

次の表に、Firepower システム上で設定できる Nmap 修復オプションを示します。

表 *258 : Nmap* 修復オプション

オプション	説明	対応する Nmap オプション
[スキャンの開始元イベント（Scan Which Address(es) From Event?）]	Nmap スキャンを相関ルールに対する応答として使用する場合、イベント内の送信元ホスト、宛先ホスト、またはその両方のどのアドレスをスキャンするのか制御する次のいずれかのオプションを選択します。 • [送信元アドレスと宛先アドレスのスキャン（Scan Source and Destination Addresses）] は、イベントの送信元 IP アドレスと宛先 IP アドレスによって表されるホストをスキャンします。 • [送信元アドレスのみのスキャン（Scan Source Address Only）] は、イベントの送信元 IP アドレスによって表されるホストをスキャンします。 • [宛先アドレスのみのスキャン（Scan Destination Address Only）] は、イベントの宛先 IP アドレスによって表されるホストをスキャンします。	該当なし

オプション	説明	対応する Nmap オプション
Scan Types		**TCP Syn**：`-sS` **TCP Connect**：`-sT` **TCP ACK**：`-sA` **TCP Window**：`-sW` **TCP Maimon**：`-sM`

オプション	説明	対応する Nmap オプション
	Nmap がポートをスキャンする方法を選択します。 • [TCP Syn] スキャンは、完全な TCP ハンドシェイクを使用せずに数千のポートにただちに接続します。このオプションを使用すると、TCP 接続が開始されますが完了はしていない状態で、`admin` アカウントが raw パケットアクセス権を持つホストや IPv6 が実行されていないホスト上でステルスモードでクイック スキャンできます。ホストが TCP Syn スキャンで送信される SYN パケットを確認応答すると、Nmap は接続をリセットします。 • [TCP 接続（TCP Connect）] スキャンは、`connect()` システム コールを使用して、ホスト上のオペレーティング システムを介して接続を開きます。TCP Connect スキャンは、Firepower Management Center 上の `admin` ユーザや管理対象デバイスがホストに対する raw パケット特権を持っていない場合や、IPv6 ネットワークをスキャンしている場合に使用できます。つまり、このオプションは TCP Syn スキャンを使用できない状況で使用します。 • [TCP ACK] スキャンは、ACK パケットを送信して、ポートがフィルタ処理されているかいないかを検査します。 • [TCP Window] スキャンは、TCP ACK スキャンと同じ機能に加えて、ポートが開いているか閉じているかも判別します。 • [TCP Maimon] スキャンは、FIN/ACK プローブを使用して BSD 派生システムを識別します。	

オプション	説明	対応する Nmap オプション
Scan for UDP ports	TCP ポートに加えて UDP ポートのスキャンも有効にします。UDP ポートのスキャンには時間がかかることがあるので、クイック スキャンする場合はこのオプションを使用しないように注意してください。	`-sU`
Use Port From Event	相関ポリシー内で応答として修復を使用する計画の場合に、修復によるスキャンの対象として、相関応答をトリガーするイベントで指定されたポートのみを有効にします。 • 相関イベント内のポートをスキャンし、Nmap 修復構成中に指定するポートをスキャンしない場合は、[オン（On）] を選択します。相関イベント内のポートをスキャンする場合は、Nmap 修復構成中に指定する IP アドレス上のポートが修復によりスキャンされることに注意してください。これらのポートも修復の動的スキャンのターゲットに追加されます。 • Nmap 修復構成中に指定するポートのみスキャンするには、[オフ（Off）] を選択します。 Nmap がオペレーティング システムやサーバに関する情報を収集するかどうかも制御できます。新しいサーバに関連付けられたポートをスキャンするには、[Use Port From Event] オプションを有効にします。	該当なし

オプション	説明	対応する Nmap オプション
Scan from reporting detection engine	ホストを報告した検出エンジンがあるアプライアンスからホストへのスキャンを有効にします。 • レポート検出エンジンを実行しているアプライアンスからスキャンするには、[オン（On）] を選択します。 • 修復内で設定されているアプライアンスからスキャンするには、[オフ（Off）] を選択します。	該当なし
Fast Port Scan	スキャン元デバイス上の `/var/sf/nmap/share/nmap/nmap-services` ディレクトリ内にある `nmap-services` ファイルにリストされている TCP ポートのみに対するスキャンを有効にし、その他のポート設定を無視できるようにします。このオプションと [ポート範囲とスキャンの順序（Port Ranges and Scan Order）] オプションを併用できないことに注意してください。 • スキャン元デバイス上の `/var/sf/nmap/share/nmap/nmap-services` ディレクトリ内の `nmap-services` ファイルにリストされているポートのみスキャンし、その他のポート設定を無視するには、[オン（On）] を選択します。 • すべての TCP ポートをスキャンするには、[オフ（Off）] を選択します。	`-F`
Port Ranges and Scan Order	Nmap ポート仕様シンタックスを使用して、スキャンする特定のポートを設定し、スキャンする順序も設定します。このオプションと [Fast Port Scan] オプションを併用できないことに注意してください。	`-p`

オプション	説明	対応する Nmap オプション
Probe open ports for vendor and version information	サーバベンダーとバージョン情報の検出を有効にします。オープンポートでサーバベンダーとバージョン情報を調査する場合、Nmap はサーバの識別に使用するサーバデータを取得します。次に、シスコのサーバ データをそのサーバに置き換えます。 • ホスト上のオープンポートでサーバ情報をスキャンして、サーバベンダーとバージョンを識別するには、[オン（On）] を選択します。 • ホストのシスコのサーバ情報を使用して続行するには、[オフ（Off）] を選択します。	`-sV`
Service Version Intensity	サービス バージョンに対する Nmap プローブの強度を選択します。 • 選択する数値が大きいほど使用するプローブの数が増えるので、スキャンは長時間になり精度が上がります。 • 選択する数値が小さいほど、使用するプローブの数が減るので、スキャンは高速になり精度が下がります。	`--version-intensity` <intensity>

オプション	説明	対応する Nmap オプション
[オペレーティング システムの検出（Detect Operating System）]	ホストのオペレーティング システム情報の検出を有効にします。 ホストでのオペレーティング システムの検出を設定した場合、Nmap はホストをスキャンし、その結果を使用してオペレーティング システムごとに評価を作成します。この評価は、ホスト上でそのオペレーティング システムが実行されている可能性を反映します。 • ホストに対してオペレーティング システムを識別する情報をスキャンするには、[オン（On）] を選択します。 • ホストに関するシスコのオペレーティング システム情報を使い続ける場合は、[オフ（Off）] を選択します。	`-o`
Treat All Hosts As Online	ホスト ディスカバリ プロセスを省略し、ターゲット範囲内のすべてのホスト上でのポート スキャンを有効にします。このオプションを有効にすると、Nmap は [ホスト ディスカバリ方式（Host Discovery Method）] と [ホスト ディスカバリ ポート リスト（Host Discovery Port List）] の設定を無視するので注意してください。 • ホスト ディスカバリ プロセスを省略し、ターゲット範囲内のすべてのホスト上でのポート スキャンを実行するには、[オン（On）] を選択します。 • [ホスト ディスカバリ方式（Host Discovery Method）] と [ホスト ディスカバリ ポート リスト（Host Discovery Port List）] の設定を使用してホスト ディスカバリを実行し、使用不能なホスト上でのポート スキャンを省略するには、[オフ（Off）] を選択します。	`-PN`

オプション	説明	対応する Nmap オプション
Host Discovery Method		**TCP SYN**：`-PS` **TCP ACK**：`-PA` **UDP**：`-PU`

オプション	説明	対応する Nmap オプション
	ホストディスカバリを、ターゲット範囲内のすべてのホストに対して実行するか、[Host Discovery Port List] にリストされているポートを経由して実行するか、または、ポートがリストされていない場合にそのホストディスカバリ方式のデフォルトポートを経由するかを選択します。 ここで、[Treat All Hosts As Online] も有効にすると、[Host Discovery Method] オプションは無効になり、ホストディスカバリが実行されないことに注意してください。 ホストが存在していて利用可能であるかどうかを Nmap がテストする際に使用する方式を以下から選択します。 • [TCP SYN] オプションは、SYN フラグが設定された空の TCP パケットを送信し、応答を受信するとホストが利用可能であると認識します。デフォルトでは TCP SYN はポート 80 をスキャンします。TCP SYN スキャンは、ステートフル ファイアウォール ルールが指定されたファイアウォールでブロックされる可能性が低いことに注意してください。 • [TCP ACK] オプションは、ACK フラグが設定された空の TCP パケットを送信し、応答を受信するとホストが利用可能であると認識します。デフォルトでは TCP ACK もポート 80 をスキャンします。TCP ACK スキャンは、ステートレス ファイアウォール ルールが指定されたファイアウォールでブロックされる可能性が低いことに注意してください。 • [UDP] オプションは、UDP パケットを送信し、クローズポートからポート到達不能応答が戻されると	

オプション	説明	対応する Nmap オプション
	ホストが利用可能であると想定します。デフォルトではUDPはポート 40125 をスキャンします。	
Host Discovery Port List	ホストディスカバリの実行時にスキャンするポートを、カスタマイズしたカンマ区切りリストで指定します。	ホストディスカバリ方式に応じたポート リスト
Default NSE Scripts	ホストディスカバリを行い、サーバ、オペレーティングシステム、脆弱性を検出する Nmap スクリプトのデフォルトセットを実行できるようにします。デフォルトスクリプトのリストについては、https://nmap.org/nsedoc/categories/default.html を参照してください。 • Nmap スクリプトのデフォルトセットを実行するには、[オン（On）] を選択します。 • Nmap スクリプトのデフォルトセットを省略するには、[オフ（Off）] を選択します。	`-sC`
Timing Template	スキャンプロセスのタイミングを選択します。選択する数値が大きいほど、スキャンは高速になり包括的ではなくなります。	**0**：`T0`（paranoid） **1**：`T1`（sneaky） **2**：`T2`（polite） **3**：`T3`（normal） **4**：`T4`（aggressive） **5**：`T5`（insane）

Nmap スキャンのガイドライン

アクティブ スキャンにより重要な情報が得られることがありますが、Nmap などのツールを多用すると、ネットワーク リソースに負荷がかかり、重要なホストがクラッシュすることさえあります。アクティブ スキャナを使用する際には、以下のガイドラインに従ってスキャン戦略を作成し、スキャンする必要があるホストとポートのみスキャンするようにしてください。

適切なスキャン ターゲットの選択

Nmap を設定する際に、スキャン対象のホストを識別するスキャン ターゲットを作成できます。スキャン ターゲットには 1 つの IP アドレス、IP アドレスの CIDR ブロックまたはオクテット範囲、IP アドレス範囲、スキャンする IP アドレスまたは範囲のリスト、および 1 つ以上のホスト上のポートが含まれます。

次の方法でターゲットを指定できます。

- IPv6 ホストの場合：
  - 厳密な IP アドレス（`192.168.1.101` など）
- IPv4 ホストの場合：
  - 厳密な IP アドレス（`192.168.1.101` など）またはカンマかスペースで区切った IP アドレスのリスト
  - CIDR 表記を使用した IP アドレス ブロック（たとえば、`192.168.1.0/24` は、両端を含めて 192.168.1.1 から 192.168.1.254 の間の 254 個のホストをスキャンします）
  - オクテットの範囲アドレッシングを使用した IP アドレス範囲（たとえば、`192.168.0-255.1-254` は、192.168.x.x の範囲内の末尾が .0 と .255 以外のすべてのアドレスをスキャンします）
  - ハイフンを使用した IP アドレス範囲（たとえば、`192.168.1.1 - 192.168.1.5` は、両端を含めて 192.168.1.1 から 192.168.1.5 の間の 6 つのホストをスキャンします）
  - カンマかスペースで区切ったアドレスか範囲のリスト（たとえば、`192.168.1.0/24, 194.168.1.0/24` は、両端を含めて 192.168.1.1 から 192.168.1.254 の間の 254 個のホストと、両端を含めて 194.168.1.1 から 194.168.1.254 の間の 254 個のホストをスキャンします）

理想的な Nmap スキャンのスキャン ターゲットには、システムで識別できないオペレーティング システムがあるホスト、識別されていないサーバがあるホスト、最近ネットワーク上で検出されたホストが含まれます。ネットワーク マップ内にないホストに関する Nmap 結果は、ネットワーク マップに追加できないことに注意してください。

⚠

注意

- Nmap によって提供されるサーバやオペレーティング システムのデータは、もう 1 度 Nmap スキャンを実行するまで静的な状態のままになります。Nmap でホストをスキャンする場合は、定期的なスケジュールを組んでスキャンします。
- ホストがネットワーク マップから削除されると、Nmap スキャンの結果は破棄されます。
- ターゲットをスキャンする権限を持っていることを確認してください。Nmap を使用して自分や自社に属さないホストをスキャンすると違法になる場合があります。

スキャン対象にする適切なポートの選択

設定するスキャンターゲットごとに、スキャン対象のポートを選択できます。各ターゲット上でスキャンする必要があるポートのセットを正確に識別するため、個々のポート番号、ポート範囲、または一連のポート番号やポート範囲を指定できます。

デフォルトでは、Nmap は 1 から 1024 までの TCP ポートをスキャンします。相関ポリシー内で応答として修復を使用する計画の場合は、相関応答をトリガーするイベントで指定されたポートのみを修復でスキャンできます。オンデマンドまたはスケジュール済みタスクとして修復を実行する場合、または Use Port From Event を使用しない場合は、その他のポート オプションを使用して、スキャンするポートを決定できます。`nmap-services` ファイルにリストされている TCP ポートのみスキャンし、その他のポート設定を無視するよう選択できます。TCP ポートの他に UDP ポートもスキャンできます。UDP ポートに対するスキャンには時間がかかることがあるので、すばやくスキャンする場合はこのオプションを使用しないように注意してください。スキャン対象として特定のポートかポート範囲を選択するには、Nmap ポート仕様シンタックスを使用してポートを識別します。

ホスト ディスカバリ オプションの設定

ホストに対してポート スキャンを始める前にホスト ディスカバリを実行するかどうかを決めるか、またはスキャンを計画しているすべてのホストがオンラインであると想定できます。すべてのホストをオンラインとして扱わないことを選択した場合、使用するホストディスカバリ方式を選択でき、必要に応じて、ホストディスカバリ時のスキャン対象ポートのリストをカスタマイズできます。ホストディスカバリ時には、リストされているポートでオペレーティング システムやサーバの情報は調査されません。特定のポートを経由する応答を使用して、ホストがアクティブで使用可能かどうかのみを判別します。ホストディスカバリを実行して、ホストが利用可能でなかった場合には、そのホスト上のポートは Nmap でスキャンされません。

関連トピック

Firepower システムの IP アドレス表記法 （20 ページ）
Nmap スキャンの自動化 （243 ページ）

例：Nmap を使用した不明なオペレーティング システムの解決

この例では、不明なオペレーティング システムを解決するように設計された、Nmap 設定について説明します。Nmap 設定の詳細については、Nmap スキャンの管理 （2533 ページ）を参照してください。

システムでネットワーク上のホストのオペレーティング システムを判別できない場合、Nmap を使用してホストをアクティブ スキャンできます。Nmap は、スキャンから得られた情報を利用して、使用されている可能性のあるオペレーティング システムを評価します。次に、最高の評価のオペレーティング システムを、ホストのオペレーティング システムを識別したものとして使用します。

Nmap を使用して新しいホストにオペレーティング システムやサーバの情報を要求すると、スキャン対象のホストに対するシステムによるそのデータのモニタリングは非アクティブになります。Nmap を使用してホスト検出を実行し、システムにより不明なオペレーティング システムがあるとマークが付けられたホストのサーバ オペレーティング システムを検出すると、同

種のホストのグループを識別できる場合があります。その場合、それらのホストのうちの1つに基づいたカスタム フィンガープリントを作成し、システムでそのフィンガープリントを、Nmap スキャンに基づいてそのホスト上で実行されていると判明したオペレーティング システムと関連付けるようにすることができます。可能な限り、Nmap などのサードパーティ製の静的データを入力するよりも、カスタムフィンガープリントを作成してください。カスタムフィンガープリントを使用すると、システムはホストのオペレーティング システムを継続してモニタし、必要に応じて更新できるからです。

この例では、次のことを実行します。

1. Nmap スキャン インスタンスの追加（2534 ページ）の説明に従って、スキャン インスタンスを設定します。
2. 次の設定を使用して Nmap 修復を作成します。
   - [イベントからのポートを使用（Use Port From Event）] を有効にして、新しいサーバに関連付けられたポートをスキャンします。
   - [Detect Operating System] を有効にして、ホストのオペレーティング システムの情報を検出します。
   - [Probe open ports for vendor and version information] を有効にして、サーバ ベンダーとバージョン情報を検出します。
   - ホストが既存であることが判明しているので、[すべてのホストをオンラインとして扱う（Treat All Hosts as Online）] を有効にします。
3. システムで不明なオペレーティング システムがあるホストが検出されたときにトリガーされる相関ルールを作成します。このルールは、**検出イベントが発生**し、**ホストの OS 情報が変更**されており、**OS 名が不明**という条件が満たされている場合にトリガーされる必要があります。
4. 相関ルールを組み込む相関ポリシーを作成します。
5. 相関ポリシー内で、ステップ 2 で応答として作成した Nmap 修復をステップ 3 で作成したルールに追加します。
6. 相関ポリシーをアクティブにします。
7. ネットワーク マップ上のホストを消去し、強制的にネットワーク検出が再起動されてネットワーク マップが再構築されるようにします。
8. 1 日後か2 日後に、相関ポリシーによって生成されたイベントを検索します。Nmap 結果から、ホスト上で検出されたオペレーティング システムを分析し、システムで認識されない特定のホスト設定がネットワーク上にあるかどうか調べます。
9. 不明なオペレーティング システムがあるホストが複数検出され、Nmap 結果が同一の場合は、それらのホストの 1 つに対してカスタム フィンガープリントを作成し、将来類似のホストを識別する際に使用します。

関連トピック

Nmap 修復の作成 （2539 ページ）
相関ルールの設定 （2701 ページ）
Nmap スキャンの結果 （2543 ページ）
クライアント用のカスタム フィンガープリントの作成 （2501 ページ）
相関ポリシーの設定 （2699 ページ）

例：Nmap を使用した新しいホストへの応答

この例では、新しいホストに応答するように設計された、Nmap 設定について説明します。Nmap 設定の詳細については、Nmap スキャンの管理 （2533 ページ）を参照してください。

システムにより、侵入の可能性があるサブネット内で新しいホストが検出された場合、そのホストをスキャンして、そのホストの脆弱性に関する正確な情報を入手できます。

そのためには、このサブネット内に新しいホストが出現した時点で検出し、そのホスト上で Nmap スキャンを実行する修復を起動する相関ポリシーを作成してアクティブにします。

そのためには、次のことを実行します。

1. Nmap スキャン インスタンスの追加 （2534 ページ）の説明に従って、スキャン インスタンスを設定します。
2. 次の設定を使用して Nmap 修復を作成します。
   - [イベントからのポートを使用（Use Port From Event）] を有効にして、新しいサーバに関連付けられたポートをスキャンします。
   - [Detect Operating System] を有効にして、ホストのオペレーティング システムの情報を検出します。
   - [Probe open ports for vendor and version information] を有効にして、サーバ ベンダーとバージョン情報を検出します。
   - ホストが既存であることが判明しているので、[すべてのホストをオンラインとして扱う（Treat All Hosts as Online）] を有効にします。
3. システムが特定のサブネット上で新しいホストを検出したときにトリガーされる相関ルールを作成します。このルールは、**検出イベントが発生**し、**新しいホストが検出**されたときにトリガーされる必要があります。
4. 相関ルールを組み込む相関ポリシーを作成します。
5. 相関ポリシー内で、ステップ 2 で応答として作成した Nmap 修復をステップ 3 で作成したルールに追加します。
6. 相関ポリシーをアクティブにします。
7. 新しいホストが通知されたら、ホスト プロファイルを調べて Nmap スキャンの結果を確認し、ホストに適用されている脆弱性に対処します。

このポリシーをアクティブにした後で、修復状態の表示（**[Analysis]** > **[Correlation]** > **[Status]**）を定期的に検査して、修復が起動された時点を調べることができます。修復の動的なスキャンターゲットには、サーバ検出の結果としてスキャンされたホストの IP アドレスを含める必要があります。これらのホストのホストプロファイルを調べて、Nmap によって検出されたオペレーティングシステムとサーバに基づいて、対処する必要がある脆弱性がホストにあるかどうか確認します。

注意 大規模なネットワークや動的なネットワークがある場合、新しいホストの検出は頻繁に発生するので、スキャンを使用して応答するには不向きな場合があります。リソースの過負荷を避けるために、頻繁に発生するイベントへの応答として Nmap スキャンを使用しないでください。また、Nmap を使用して新しいホストのオペレーティングシステムやサーバの情報を要求すると、スキャン対象のホストに対するによるそのデータのシスコモニタリングが非アクティブになることに注意してください。

関連トピック

Nmap 修復の作成 （2539 ページ）
相関ルールの設定 （2701 ページ）
相関ポリシーの設定 （2699 ページ）

Nmap スキャンの管理

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Discovery Admin

Nmap スキャンを使用するには、少なくとも 1 つの Nmap スキャン インスタンスと 1 つの Nmap 修復を設定する必要があります。Nmap スキャン ターゲットの設定はオプションです。

ステップ 1 Nmap スキャンを設定します。

- Nmap スキャン インスタンスを追加します。詳細については、Nmap スキャン インスタンスの追加 （2534 ページ）を参照してください。
- Nmap 修復を作成します。詳細については、Nmap 修復の作成 （2539 ページ）を参照してください。
- 必要に応じて、Nmap スキャン ターゲットを追加します。詳細については、Nmap スキャン ターゲットの追加 （2537 ページ）を参照してください。

ステップ 2 Nmap スキャンを実行します。

- オンデマンド Nmap スキャンを実行します。詳細については、オンデマンド Nmap スキャンの実行 （2542 ページ）を参照してください。
- 自動 Nmap スキャンを設定します。詳細については、Nmap スキャンの自動化 （243 ページ）を参照してください。

- 自動 Nmap スキャンをスケジュールします。詳細については、Nmap スキャンのスケジュール （244 ページ）を参照してください。

次のタスク

- 関連タスクを表示することで、進行中のNmapスキャンをモニタします。タスク メッセージの表示 （417 ページ）を参照してください。
- 必要に応じて、次に示すようにスキャンを調整します。
  - Nmap スキャン インスタンスを編集します。詳細については、Nmap スキャン インスタンスの編集 （2536 ページ）を参照してください。
  - Nmap スキャン ターゲットを編集します。詳細については、Nmap スキャン ターゲットの編集 （2538 ページ）を参照してください。
  - Nmap修復を編集します。詳細については、Nmap修復の編集 （2541 ページ）を参照してください。

Nmap スキャン インスタンスの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Discovery Admin

脆弱性についてネットワークをスキャンするのに使用する Nmap モジュールごとに別々のスキャン インスタンスをセットアップできます。Firepower Management Center 上のローカル Nmap モジュールか、リモートでスキャンを実行するために使用するデバイスに対してスキャン インスタンスをセットアップできます。各スキャンの結果は常に Firepower Management Center に保存されます。リモートデバイスからスキャンを実行する場合でも、この場所でスキャンを設定できます。ミッションクリティカルなホストへの不慮のスキャンや悪意のあるスキャンを防ぐには、インスタンスのブラックリストを作成し、そのインスタンスで決してスキャンしてはならないホストを指示できます。

既存のスキャン インスタンスと同じ名前のスキャン インスタンスは追加できません。

マルチドメイン展開では、現在のドメインで作成されたスキャン インスタンスが表示されます。これは編集できます。先祖ドメインで作成されたスキャン インスタンスも表示されますが、これは編集できません。下位のドメインのスキャン インスタンスを表示および編集するには、そのドメインに切り替えます。

ステップ 1 以下のいずれかの方法を使用して、Nmap スキャン インスタンスのリストにアクセスします。

- **[Policies]** > **[Actions]** > **[Instances]**を選択します。

- **[Policies]** > **[Actions]** > **[Scanners]**を選択します。

ステップ 2 以下の場合、修復を追加します。

- 上記の最初の方法でリストにアクセスした場合は、[新しいインスタンスの追加（Add a New Instance）] セクションを探し、ドロップダウン リストから Nmap 修復モジュールを選択し、[追加（Add）] をクリックします。
- 上記の 2 番目の方法でリストにアクセスした場合は、[Nmap インスタンスの追加（Add Nmap Instance）] をクリックします。

ステップ 3 [インスタンス名（Instance Name）] を入力します。

ステップ 4 [説明（Description）] を入力します。

ステップ 5 オプションで、[ブラックリスト化されたスキャン ホスト（Black Listed Scan hosts）] フィールドで、このスキャン インスタンスがスキャンしないホストまたはネットワークを指定します。

- IPv6 ホストの場合、厳密な IP アドレス（`2001:DB8::fedd:eeff` など）
- IPv4 ホストの場合、厳密な IP アドレス（`192.168.1.101` など）または CIDR 表記を使用した IP アドレス ブロック（たとえば、`192.168.1.0/24` は、両端を含めて `192.168.1.1` から `192.168.1.254` の間の 254 個のホストをスキャンします）
- 感嘆符（!）を使用してアドレス値の否定はできないことに注意してください。

（注） ブラックリストに含まれるネットワーク内のホストをスキャン対象として特定すると、スキャンは実行されません。

ステップ 6 オプションで、Firepower Management Centerの代わりにリモート デバイスからスキャンを実行するには、そのデバイスの IP アドレスか名前を指定します。この情報は、FMC Web インターフェイス内のそのデバイスに関する [Information] ページの [Remote Device Name] フィールドに表示されます。

ステップ 7 [作成（Create）] をクリックします。
システムがインスタンスの作成を終えると、編集モードでこのインスタンスが表示されます。

ステップ 8 必要に応じて、インスタンスに Nmap の修復を追加します。そのためには、インスタンスの [設定されている修復（Configured Remediations）] を探し、[追加（Add）] をクリックし、Nmap 修復の作成 （2539 ページ）の説明に従って修復を作成します。

ステップ 9 インスタンスのリストに戻るには、[キャンセル（Cancel）] をクリックします。

（注） [スキャナ（Scanners）] オプションにより Nmap スキャン インスタンスのリストにアクセスした場合は、インスタンスの修復も併せて追加しないと追加したインスタンスは表示されません。修復が追加されていないインスタンスをすべて表示するには、[インスタンス（Instances）] メニュー オプションを使ってリストにアクセスします。

Nmap スキャン インスタンスの編集

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Discovery Admin

スキャン インスタンスを編集する場合、インスタンスに関連付けられている修復を表示、追加、および削除できます。インスタンス内でプロファイルが作成されたNmapモジュールを使用しなくなった場合には、Nmapスキャンインスタンスを削除します。スキャンインスタンスを削除すると、そのインスタンスを使用する修復も削除されることに注意してください。

マルチドメイン展開では、現在のドメインで作成されたスキャン インスタンスが表示されます。これは編集できます。先祖ドメインで作成されたスキャン インスタンスも表示されますが、これは編集できません。下位のドメインのスキャンインスタンスを表示および編集するには、そのドメインに切り替えます。

ステップ 1 以下のいずれかの方法を使用して、Nmap スキャン インスタンスのリストにアクセスします。

- **[Policies]** > **[Actions]** > **[Instances]**を選択します。
- **[Policies]** > **[Actions]** > **[Scanners]**を選択します。

ステップ 2 編集するインスタンスの横にある表示アイコン（）をクリックします。

ステップ 3 Nmap スキャン インスタンスの追加 （2534 ページ）の説明に従って、スキャンインスタンスの設定を変更します。

ステップ 4 [保存（Save）] をクリックします。

ステップ 5 [Done] をクリックします。

次のタスク

- 必要に応じて、スキャン インスタンスに新しい修復を追加します。次を参照してください。 Nmap 修復の作成 （2539 ページ）
- 必要に応じて、インスタンスに関連付けられている修復を編集します。Nmap 修復の編集 （2541 ページ）を参照してください。
- 必要に応じて、インスタンスに関連付けられる修復を削除します。オンデマンド Nmap スキャンの実行 （2542 ページ）を参照してください。
- 必要に応じて、その横にある削除アイコン（）をクリックして、スキャンインスタンスを削除します。

Nmap スキャン ターゲットの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Discovery Admin

Nmapモジュールを設定する際にスキャンターゲットを作成して保存できます。スキャンターゲットは、オンデマンドまたはスケジュール済みのスキャンの実行時にターゲットにするホストとポートを識別します。これにより、毎回新しいスキャンターゲットを作成する必要がなくなります。スキャン ターゲットには、スキャンする 1 つの IP アドレスか IP アドレスのブロック、および 1 つ以上のホスト上のポートが含まれます。Nmap ターゲットの場合、オクテット範囲による Nmap のアドレッシングや IP アドレスの範囲も使用できます。Nmap のオクテット範囲によるアドレッシングの詳細については、http://insecure.org にある Nmap のマニュアルを参照してください。

（注）

- スキャンターゲットに多数のホストが含まれている場合、スキャンに要する時間が延びる場合があります。回避策として、一度にスキャンするホストを減らしてください。
- Nmap によって提供されるサーバやオペレーティング システムのデータは、もう 1 度 Nmap スキャンを実行するまで静的な状態のままになります。Nmap でホストをスキャンする場合は、定期的なスケジュールを組んでスキャンします。ホストがネットワーク マップから削除されると、Nmap スキャンの結果は破棄されます。
- マルチドメイン展開では、現在のドメインで作成されたスキャンターゲットが表示されます。これは編集できます。先祖ドメインで作成されたスキャンターゲットも表示されますが、これは編集できません。下位のドメインのスキャンターゲットを表示および編集するには、そのドメインに切り替えます。

ステップ 1 **[Policies]** > **[Actions]** > **[Scanners]**を選択します。

ステップ 2 ツールバーで、[ターゲット（Targets）] をクリックします。

ステップ 3 [スキャン ターゲットの作成（Create Scan Target）] をクリックします。

ステップ 4 [名前（Name）] フィールドに、このスキャン ターゲットに使用する名前を入力します。

ステップ 5 [IP 範囲（IP Range）] テキストボックスで、Nmap スキャンのガイドライン （2528 ページ）で説明しているシンタックスを使用して、スキャンする 1 つ以上のホストを指定します。

（注） スキャンターゲット内の IP アドレスか範囲のリストでカンマを使用した場合、ターゲットを保存する際にカンマはスペースに変換されます。

ステップ 6 [ポート（Ports）] フィールドで、スキャンするポートを指定します。

1 から 65535 までの値を使用して、次のいずれかを入力できます。

- 1 つのポート番号

- カンマで区切ったポートのリスト
- ハイフンで区切ったポート番号の範囲
- ハイフンで区切ったポート番号の複数の範囲をカンマで区切ったもの

ステップ 7 **[保存（Save）]** をクリックします。

関連トピック

Nmap スキャンの自動化 （243 ページ）

Nmap スキャン ターゲットの編集

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Discovery Admin

ヒント 修復を使用して特定の IP アドレスをスキャンするつもりがないのに、修復を起動した相関ポリシー違反にホストが関係していたためにその IP アドレスがターゲットに追加された場合は、修復の動的スキャン ターゲットを編集できます。

スキャン ターゲットにリストされているホストをスキャンする必要がなくなった場合は、そのスキャン ターゲットを削除します。

マルチドメイン展開では、現在のドメインで作成されたスキャン ターゲットが表示されます。これは編集できます。先祖ドメインで作成されたスキャン ターゲットも表示されますが、これは編集できません。下位のドメインのスキャン ターゲットを表示および編集するには、そのドメインに切り替えます。

ステップ 1 **[Policies]** > **[Actions]** > **[Scanners]** を選択します。

ステップ 2 ツールバーで、[ターゲット（Targets）] をクリックします。

ステップ 3 編集するスキャン ターゲットの横にある編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 4 必要に応じて変更を加えます。詳細については、Nmap スキャン ターゲットの追加 （2537 ページ）を参照してください。

ステップ 5 **[保存（Save）]** をクリックします。

ステップ 6 必要に応じて、その横にある削除アイコン（）をクリックして、スキャン ターゲットを削除します。

Nmap 修復の作成

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Discovery Admin

Nmap 修復は、既存の Nmap スキャン インスタンスに修復を追加することによってのみ作成できます。修復では、スキャンの設定を定義します。これは相関ポリシーで応答として使用したり、オンデマンドで実行したり、スケジュール タスクとして特定の時刻に実行したりできます。

Nmap によって提供されるサーバやオペレーティング システムのデータは、もう 1 度 Nmap スキャンを実行するまで静的な状態のままになります。Nmap でホストをスキャンする場合は、定期的なスケジュールを組んでスキャンします。ホストがネットワーク マップから削除されると、Nmap スキャンの結果は破棄されます。

Nmap の機能に関する一般情報については、http://insecure.org にある Nmap のマニュアルを参照してください。

マルチドメイン導入では、現在のドメインで作成された Nmap 修復が表示されます。これは編集できます。先祖ドメインで作成された Nmap 修復も表示されますが、これは編集できません。下位ドメインの Nmap 修復を表示および編集するには、そのドメインに切り替えます。

始める前に

- Nmap スキャン インスタンスの追加 （2534 ページ）の説明に従って、Nmap スキャン インスタンスを追加します。

ステップ 1 **[Policies]** > **[Actions]** > **[Instances]**を選択します。

ステップ 2 修復を追加するインスタンスの横にある表示アイコン（  ）をクリックします。

ステップ 3 [設定済みの修復（Configured Remediations）] セクションで、[追加（Add）] をクリックします。

ステップ 4 [修復名（Remediation Name）] を入力します。

ステップ 5 [説明（Description）] を入力します。

ステップ 6 侵入イベント、接続イベント、ユーザ イベントをトリガーする相関ルールに応じてこの修復を使用する場合は、[スキャンするイベントのアドレス（Scan Which Address(es) From Event?）] オプションを設定します。

ヒント ディスカバリ イベントまたはホスト入力イベントに対してトリガーする相関ルールへの応答としてこの修復を使用する計画の場合は、デフォルトでそのイベントに関連するホストの IP アドレスが修復によってスキャンされます。このオプションを設定する必要はありません。

（注） トラフィック プロファイルの変更に対してトリガーする相関ルールへの応答として Nmap 修復を割り当て**ないでください**。

ステップ 7 [スキャン タイプ（Scan Type）] オプションを設定します。

ステップ 8 オプションで、TCP ポートに加えて UDP ポートをスキャンするには、[UDP ポートのスキャン（Scan for UDP ports）] オプションで [オン（On）] を選択します。

ヒント UDP ポートスキャンは TCP ポートスキャンよりも時間がかかります。スキャン時間を短縮するには、このオプションを無効のままにします。

ステップ 9 相関ポリシー違反への応答としてこの修復を使用する計画の場合は、[イベントからポートを使用（Use Port From Event）] オプションを設定します。

ステップ 10 相関ポリシー違反への応答としてこの修復を使用する計画で、イベントを検出した検出エンジンを実行しているアプライアンスを使用してスキャンを実行するには、[レポート検出エンジンからスキャン（Scan from reporting detection engine）] オプションを設定します。

ステップ 11 [高速ポート スキャン（Fast Port Scan）] オプションを設定します。

ステップ 12 [ポート範囲およびスキャン順序（Port Ranges and Scan Order）] フィールドに、デフォルトでスキャンするポートを入力します。Nmap ポート指定シンタックスを使用し、ポートをスキャンする順序で入力します。

次の形式を使用します。

- 1 から 65535 までの値を指定します。
- ポートを区切るには、カンマかスペースを使用します。
- ポート範囲を示すには、ハイフンを使用します。
- TCP ポートと UDP ポートの両方ともスキャンする場合は、スキャン対象の TCP ポートのリストの先頭に T を挿入し、UDP ポートのリストの先頭に U を挿入します。

（注） 手順 8 で説明されているように、相関ポリシー違反への応答として修復が起動する場合には、[イベントからポートを使用（Use Port From Event）] オプションによりこの設定が上書きされます。

例：

UDP トラフィックのポート 53 と 111 をスキャンしてから、TCP トラフィックのポート 21 から 25 までスキャンするには、`U:53,111,T:21-25` と入力します。

ステップ 13 開いているポートでサーバ ベンダーおよびバージョン情報をプローブするには、[ベンダーおよびバージョン情報に関するオープン ポートのプローブ（Probe open ports for vendor and version information）] を設定します。

ステップ 14 開いているポートをプローブすることにした場合、[サービス バージョンの強さ（Service Version Intensity）] ドロップダウン リストから数値を選択することにより、使用されるプローブの数を設定します。

ステップ 15 オペレーティング システム情報をスキャンするには、[オペレーティング システムの検出（Detect Operating System）] 設定を行います。

ステップ 16 ホスト ディスカバリが行われるかどうか、およびポートのスキャンが使用可能なホストのみに対して実行されるかどうかを決めるには、[すべてのホストをオンラインとして扱う（Treat All Hosts As Online）] を設定します。

ステップ 17 Nmap でホストの使用可能性をテストする際に使用する方法を設定するには、[ホスト ディスカバリ方式（Host Discovery Method）] ドロップダウン リストから方式を選択します。

ステップ 18 ホストディスカバリ時にポートのカスタム リストをスキャンする場合は、選択したホストディスカバリ方式に適したポートのリストを、[ホスト ディスカバリ ポート リスト（Host Discovery Port List）] フィールドにカンマで区切って入力します。

ステップ 19 [デフォルト NSE スクリプト（Default NSE Scripts）] オプションを設定して、ホスト ディスカバリおよび、サーバ、オペレーティング システム、脆弱性のディスカバリに Nmap スクリプトのデフォルト セットを使用するかどうかを制御します。

ヒント デフォルト スクリプトのリストについては、http://nmap.org/nsedoc/categories/default.html を参照してください。

ステップ 20 スキャン プロセスのタイミングを設定するには、[タイミング テンプレート（Timing Template）] ドロップダウン リストからタイミング テンプレート番号を選択します。

より高速だが、包括的でないスキャンを実行する場合は大きい番号を選択し、低速で、より包括的なスキャンを実行する場合は小さい番号を選択します。

ステップ 21 [作成（Create）] をクリックします。
修復の作成が完了すると、修復が編集モードで表示されます。

ステップ 22 [完了（Done）] をクリックして、関連インスタンスに戻ります。

ステップ 23 [キャンセル（Cancel）] をクリックすると、インスタンス リストに戻ります。

関連トピック

Nmap スキャンの自動化 （243 ページ）
Nmap 修復オプション （2518 ページ）

Nmap 修復の編集

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Discovery Admin

Nmap 修復に加えた変更は、進行中のスキャンには影響しません。新しい設定は、次回スキャンが開始されたときに有効になります。Nmap 修復が不要になったら削除します。

マルチドメイン導入では、現在のドメインで作成された Nmap 修復が表示されます。これは編集できます。先祖ドメインで作成された Nmap 修復も表示されますが、これは編集できません。下位ドメインの Nmap 修復を表示および編集するには、そのドメインに切り替えます。

ステップ 1 以下のいずれかの方法を使用して、Nmap スキャン インスタンスのリストにアクセスします。

- **[Policies]** > **[Actions]** > **[Instances]**を選択します。
- **[Policies]** > **[Actions]** > **[Scanners]**を選択します。

ステップ 2 編集する修復にアクセスします。

- 上記の最初の方法でリストにアクセスした場合は、関連するインスタンスの横にある表示アイコン（）をクリックし、次に、[設定済み修復（Configured Remediations）]セクションで、編集する修復の横にある表示アイコンを再度クリックします。
- 上記の 2 番目の方法でリストにアクセスした場合は、編集する修復の横にある表示アイコン（）をクリックします。

ステップ 3 Nmap 修復の作成 （2539 ページ）の説明に従って、必要に応じて変更を加えます。

ステップ 4 変更を保存する場合は[保存（Save）]をクリックし、保存せずに終了する場合は[完了（Done）]をクリックします。

ステップ 5 必要に応じて、その横にある削除アイコン（）をクリックして修復を削除します。

オンデマンド Nmap スキャンの実行

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Discovery Admin

オンデマンド Nmap スキャンは、いつでも必要なときに起動できます。スキャンする IP アドレスとポートを入力するか、既存のスキャン ターゲットを選択することで、オンデマンド スキャンのターゲットを指定できます。

Nmap によって提供されるサーバやオペレーティング システムのデータは、もう 1 度 Nmap スキャンを実行するまで静的な状態のままになります。Nmap でホストをスキャンする場合は、定期的なスケジュールを組んでスキャンします。ホストがネットワーク マップから削除されると、Nmap スキャンの結果は破棄されます。

始める前に

- 必要に応じて、Nmap スキャン ターゲットを追加します。Nmap スキャン ターゲットの追加 （2537 ページ）を参照してください。

ステップ 1 **[Policies]** > **[Actions]** > **[Scanners]**を選択します。

ステップ 2 スキャンの実行時に使用する Nmap 修復の横にあるスキャン アイコン（）をクリックします。

ステップ 3 必要に応じて、保存済みのスキャン ターゲットを使用してスキャンする場合は、[保存済ターゲット（Saved Targets）] ドロップダウンリストからターゲットを選択して、[ロード（Load）] をクリックします。

ステップ 4 [IP 範囲（IP Range(s)）] フィールドで、スキャンするホストの IP アドレスを指定するかロードされたリストを変更します。

（注）

- IPv4 アドレスのホストの場合は、複数の IP アドレスをカンマで区切って指定するか、CIDR 表記を使用できます。感嘆符（!）を前に挿入して IP アドレスを否定することもできます。
- IPv6 アドレスのホストの場合は、厳密な IP アドレスを使用します。インターフェイスの範囲は入力できません。

ステップ 5 [Ports] フィールドで、スキャンするポートを指定するか、ロードされたリストを変更します。

ポート番号、カンマで区切ったポートのリスト、ハイフンで区切ったポート番号の範囲を入力できます。

ステップ 6 マルチドメイン展開では、[ドメイン（Domain）] フィールドを使用して、スキャンを実行するリーフ ドメインを指定します。

ステップ 7 [今すぐスキャン（Scan Now）] をクリックします。

次のタスク

- 必要に応じて、タスクのステータスをモニタします（タスク メッセージの表示（417 ページ） を参照）。

関連トピック

Nmap スキャンの自動化 （243 ページ）
Firepower システムの IP アドレス表記法 （20 ページ）
検索でのポート （2972 ページ）

Nmap スキャンの結果

進行中の Nmap スキャンをモニタし、Firepower システムによって実行されたスキャンの結果あるいは Firepower システム外部で行われたスキャンの結果をインポートして、スキャン結果を表示および分析することができます。

ローカル Nmap モジュールを使用して作成したスキャン結果を、レンダリングされたページとしてポップアップ ウィンドウで表示できます。Nmap 結果ファイルを raw XML 形式でダウンロードすることもできます。

Nmapによって検出されたオペレーティングシステムやサーバの情報を、ホストプロファイルやネットワーク マップ内で参照することもできます。ホストのスキャンが生成するサーバ情報がフィルタ除去されているかクローズ状態のポートのサーバに関する情報の場合、または、スキャンが収集した情報がオペレーティング システム情報やサーバのセクションに含めることができない情報の場合、それらの結果は、ホスト プロファイルの [Nmap スキャン結果（Nmap Scan Results）] セクションに含めることができます。

Nmap スキャン結果の表示

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Discovery Admin

Nmap スキャンが完了したら、スキャン結果のテーブルを表示できます。

ユーザは検索する情報に応じて結果のビューを操作することができます。スキャン結果にアクセスすると表示されるページは、使用するワークフローに応じて異なります。定義済みのワークフローを使用できます。このワークフローにはスキャン結果のテーブル ビューが含まれます。また、特定のニーズを満たす情報だけを表示するカスタム ワークフローを作成することもできます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

http://insecure.org で使用可能な Nmap バージョン 1.01 DTD を使用して Nmap の結果をダウンロードして表示することができます。

スキャン結果をクリアすることもできます。

ステップ 1 **[Policies]** > **[Actions]** > **[Scanners]**を選択します。

ステップ 2 ツールバーで、[スキャン結果（Scan Results）] をクリックします。

ステップ 3 次の選択肢があります。

- イベント時間の制約 （2952 ページ）の説明に従って、時間範囲を調整します。
- カスタム ワークフローなど、別のワークフローを使用するには、ワークフローのタイトルの横の[（ワークフローの切り替え）（(switch workflow)）] をクリックします。
- スキャン結果をレンダリングされたページとしてポップアップ ウィンドウで表示するには、スキャン ジョブの横にある [表示（View）] をクリックします。
- テキスト エディタで raw XML コードを表示できるようにスキャン結果ファイルのコピーを保存するには、スキャン ジョブの横の [ダウンロード（Download）] をクリックします。
- スキャン結果をソートするには、カラムのタイトルをクリックします。ソート順を逆にするには、カラムのタイトルをもう一度クリックします。
- 表示されるカラムを制約にするには、非表示にするカラムの見出しにある閉じるアイコン（✖）をクリックします。表示されるポップアップ ウィンドウで、[適用（Apply）] をクリックします。

  ヒント 他のカラムを表示または非表示にするには、[適用（Apply）]をクリックする前に、該当するチェック ボックスをオンまたはオフにします。無効にしたカラムをビューに戻すには、展開の矢印をクリックして検索制約を展開し、[無効にされたカラム（Disabled Columns）] の下のカラム名をクリックします。

- ワークフローの次のページにドリルダウンするには、ドリルダウン ページの使用 （2940 ページ）を参照してください。

- スキャン インスタンスや修復を設定するには、ツールバーの [スキャナ（Scanners）] をクリックしてください（Nmap スキャンの管理 （2533 ページ）を参照）。
- ワークフローページ内およびワークフローページ間で移動するには、ワークフローページのナビゲーション ツール （2937 ページ）を参照してください。
- その他のイベント ビューに移動して関連するイベントを表示するには、[ジャンプ（Jump to）] ドロップダウン リストから、表示するイベント ビューの名前を選択します。
- スキャン結果を検索するには、該当するフィールドに検索条件を入力します。

関連トピック

Nmap スキャン結果のフィールド （2545 ページ）

Nmap スキャン結果のフィールド

Nmap スキャンを実行すると、Firepower Management Center でデータベース内のスキャン結果が収集されます。次の表に、表示および検索できるスキャン結果テーブルのフィールドを示します。

表 *259* : スキャン結果のフィールド

フィールド	説明
Start Time	この結果を作成したスキャンの開始日時。
End Time	この結果を作成したスキャンの終了日時。
ターゲット（Target）	この結果を作成したスキャンのスキャン ターゲットの IP アドレス（DNS 解決が有効になっている場合はホスト名）。
Scan Type	この結果を作成したスキャンのタイプを示す、`Nmap` またはサードパーティのスキャナ名。
Scan Mode	この結果を作成したスキャンのモード： • `On Demand`：オン デマンドで実行されたスキャンからの結果。 • `Imported`：別のシステムでスキャンされてFirepower Management Centerにインポートされた結果 • [スケジュール済み（Scheduled）]：スケジュール済みタスクとして実行されたスキャンからの結果。
結果	スキャンの結果。
ドメイン	スキャン ターゲットのドメイン。このフィールドは、マルチドメイン展開の場合にのみ存在します。

関連トピック

イベントの検索 （2967 ページ）

Nmap スキャン結果のインポート

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Discovery Admin

Firepower システムの外部で実行した Nmap スキャンによって作成された XML 結果ファイルをインポートできます。以前に Firepower システムからダウンロードした XML 結果ファイルもインポートできます。Nmap スキャン結果をインポートする場合、結果ファイルは XML 形式で、Nmap バージョン 1.01 DTD に準拠している必要があります。Nmap 結果の作成と Nmap DTD の詳細については、http://insecure.org にある Nmap のマニュアルを参照してください。

Nmap がホスト プロファイルに結果を追加できるようにするには、その前にホストがネットワーク マップ内に存在している必要があります。

ステップ 1 **[Policies]** > **[Actions]** > **[Scanners]**を選択します。

ステップ 2 ツールバーで、[結果のインポート（Import Results）] をクリックします。

ステップ 3 マルチドメイン展開では、インポートされた結果の保存場所を指定するために、[ドメイン（Domain）] ドロップダウンリストからリーフ ドメインを選択します。

ステップ 4 [参照（Browse）] をクリックして、結果ファイルに移動します。

ステップ 5 [インポートの結果（Import Results）] ページに戻ったら、[インポート（Import）] をクリックして結果をインポートします。

第 99 章

アプリケーションの検出

次のトピックでは、Firepower システム アプリケーション検出について説明します。

概要：アプリケーション検出

Firepower システムは IP トラフィックを分析するときに、ネットワーク上でよく使用されているアプリケーションを特定しようとします。アプリケーション認識は、アプリケーションを制御するために不可欠です。

システムによって検出されるアプリケーションには以下の 3 種類があります。

- HTTP や SSH などのホスト間の通信を表すアプリケーション プロトコル
- Web ブラウザや電子メール クライアントなどのホスト上で動作しているソフトウェアを表すクライアント
- HTTP トラフィックの内容または要求された URL を表す MPEG ビデオや Facebook などの *Web* アプリケーション

システムは、ディテクタに指定されている特性に従って、ネットワーク トラフィック内のアプリケーションを識別します。たとえば、システムはパケット ヘッダーに含まれる ASCII パターンによってアプリケーションを確認できます。加えて、Secure Socket Layer（SSL）プロトコル ディテクタは、セキュアなセッションからの情報を使用して、セッションからアプリケーションを識別します。

Firepower システムのアプリケーション ディテクタには以下の 2 つのソースがあります。

- システム提供ディテクタ。Web アプリケーション、クライアント、およびアプリケーション プロトコルを検出します。

  アプリケーション（およびオペレーティング システム）に対して使用できるシステム提供ディテクタは、インストールされている Firepower システムのバージョンと VDB のバージョンによって異なります。リリース ノートとアドバイザリに、新しいディテクタと更新されたディテクタに関する情報が記載されています。また、プロフェッショナル サービスが作成した個別のディテクタをインポートすることもできます。

- カスタム アプリケーション プロトコル ディテクタ。Web アプリケーション、クライアント、アプリケーション プロトコルを検出するためにユーザが作成するディテクタです。

また、暗黙的アプリケーション プロトコル検出を通してアプリケーション プロトコルを検出することもできます。これは、クライアントの検出に基づいてアプリケーションプロトコルの存在を推測するものです。

ネットワーク検出ポリシーで定義されているように、システムはモニタ対象ネットワーク内のホスト上で動作しているアプリケーションプロトコルだけを識別します。たとえば、モニタされていないリモート サイト上の FTP サーバに内部ホストがアクセスする場合、システムはアプリケーション プロトコルを FTP として識別しません。一方、モニタされているホスト上の FTP サーバにリモートまたは内部ホストがアクセスする場合、システムはアプリケーションプロトコルを肯定的に識別できます。

モニタ対象ホストが非モニタ対象サーバに接続するために使用するクライアントをシステムで識別できる場合、システムはクライアントの対応するアプリケーションプロトコルを識別することができますが、そのプロトコルをネットワーク マップに追加することはしません。アプリケーション検出が発生するためには、クライアント セッションにサーバからの応答が含まれている必要があることに注意してください。

システムは、検出した各アプリケーションの特徴を把握します（アプリケーションの特性 （484ページ）を参照）。システムはこれらの特徴を使用して、アプリケーション フィルタと呼ばれるアプリケーションのグループを作成します。アプリケーション フィルタは、アクセス制御するため、およびレポートとダッシュボード ウィジェットで使用する検索結果とデータを制限するために使用されます。

また、エクスポートした NetFlow レコード、Nmap のアクティブ スキャン、ホスト入力機能を使用してアプリケーション ディテクタ データを補完することもできます。

関連トピック

アプリケーション制御に関する推奨事項 （1691 ページ）
アプリケーション ディテクタの基本 （2548 ページ）

アプリケーション ディテクタの基本

Firepower システムは、アプリケーション ディテクタを使用して、ネットワーク上で一般的に使用されるアプリケーションを識別します。[ディテクタ（Detectors）] ページ（**[Policies]** >

[Application Detectors]）を使用してディテクタ リストを表示し、検出機能をカスタマイズします。

ディテクタまたはその状態（アクティブ/非アクティブ）を変更できるかどうかは、そのタイプによって異なります。システムは、アクティブなディテクタのみを使用して、アプリケーション トラフィックを分析します。

（注） シスコが提供するディテクタは、Firepowerシステムおよび VDB のアップデートによって変更される可能性があります。更新されたディテクタに関する情報については、リリース ノートおよびアドバイザリを参照してください。

シスコが提供する内部ディテクタ

内部ディテクタは、クライアント、Web アプリケーション、およびアプリケーション プロトコルのトラフィック用の特別なディテクタ カテゴリです。内部ディテクタはシステム アップデートによって配信され、常にオンになっています。

アプリケーションがクライアント関連のアクティビティを検出するように設計された内部ディテクタと照合する場合で、特定のクライアントディテクタがない場合は、汎用クライアントが報告される場合があります。

シスコが提供するクライアント ディテクタ

クライアントディテクタは、クライアント トラフィックを検出し、VDB またはシステム アップデートを介して配信されるか、または Cisco Professional サービスによってインポート用に提供されます。クライアントディテクタを有効または無効にすることができます。インポートしたクライアント ディテクタのみエクスポートできます。

シスコが提供する Web アプリケーション ディテクタ

Web アプリケーションディテクタは、HTTP トラフィック ペイロード内の Web アプリケーションを検出し、VDB またはシステム アップデートを介して配信されます。Web アプリケーション ディテクタは常にオンになっています。

シスコが提供するアプリケーション プロトコル（ポート）ディテクタ

ポートベースのアプリケーション プロトコル ディテクタは、ウェルノウン ポートを使用してネットワーク トラフィックを識別します。これらは VDB またはシステム アップデートを介して配信されるか、または Cisco Professional サービスによってインポート用に提供されます。アプリケーション プロトコル ディテクタを有効または無効にしたり、カスタム ディテクタの基礎として使用するためにディテクタ定義を表示することができます。

シスコが提供するアプリケーション プロトコル（Firepower）ディテクタ

Firepower ベースのアプリケーション プロトコル ディテクタは、Firepower アプリケーション フィンガープリントを使用してネットワーク トラフィックを分析し、VDB またはシステム

アップデートを介して配信されます。アプリケーション プロトコル ディテクタを有効または無効にすることができます。

カスタム アプリケーション ディテクタ

カスタムアプリケーションディテクタはパターンベースです。クライアント、Webアプリケーション、またはアプリケーションプロトコルのトラフィックからのパケット内のパターンを検出します。インポートされたカスタム ディテクタを完全に制御できます。

Web インターフェイスでのアプリケーション プロトコルの識別

次の表に、Firepower システムが検出されたアプリケーション プロトコルを識別する方法について概略を示します。

表 *260 : Firepower* システムのアプリケーション プロトコルの識別

ID	説明
アプリケーション プロトコル名	Firepower Management Center は、次のアプリケーション プロトコルの場合に、名前でアプリケーション プロトコルを識別します。 • システムによって肯定的に識別された • NetFlow データを使用して識別され、`/etc/sf/services` にポートとアプリケーション プロトコルの関連付けが存在する • ホスト入力機能を使用して手動で識別された • Nmap または別のアクティブな発生源によって識別された
`pending`	Firepower Management Center は、システムが肯定的と否定的のどちらでもアプリケーションを識別できない場合に、アプリケーション プロトコルを `pending` として識別します。 多くの場合、システムが保留中のアプリケーションを識別するには、より多くの接続データを収集して分析する必要があります。 [アプリケーションの詳細（Application Details）] および [サーバ（Servers）] テーブルやホスト プロファイルで `pending` ステータスが表示されるのは、特定のアプリケーション プロトコル トラフィック（検出されたクライアントまたは Web アプリケーション トラフィックから推論されたトラフィック以外）が検出されたアプリケーション プロトコルだけです。

ID	説明
unknown	Firepower Management Center は、以下の場合にアプリケーション プロトコルを unknown として識別します。 • アプリケーションがシステムのディテクタのどれとも一致しない • アプリケーション プロトコルが NetFlow データを使用して識別されたものの、/etc/sf/services にポートとアプリケーション プロトコルの関連付けが存在しない
空白	使用可能なすべての検出データが検証されましたが、アプリケーション プロトコルが識別されませんでした。[アプリケーションの詳細（Application Details）] および [サーバ（Servers）] テーブルとホスト プロファイルでは、アプリケーション プロトコルが検出されなかった非 HTTP 汎用クライアント トラフィックに対して、アプリケーション プロトコルが空白として表示されます。

クライアント検出からの暗黙的アプリケーション プロトコル検出

非監視対象サーバにアクセスするために監視対象ホストが使用しているクライアントをシステムが識別できる場合、Firepower Management Center はその接続でクライアントに対応するアプリケーションプロトコルが使用されていると推測します（システムは監視対象ネットワーク上のアプリケーションだけを追跡するため、通常、接続ログには監視対象ホストが非監視対象サーバにアクセスしている接続に関するアプリケーション プロトコル情報が含まれていません）。

暗黙的アプリケーション プロトコル検出と呼ばれるこのプロセスの結果は次のようになります。

- システムはこれらのサーバの New TCP Port イベントまたは New UDP Port イベントを生成しないため、サーバが [サーバ（Servers）] テーブルに表示されません。加えて、これらのアプリケーションプロトコルの検出を基準にして、検出イベントアラートまたは相関ルールをトリガーすることはできません。
- アプリケーション プロトコルはホストに関連付けられないため、ホスト プロファイルの詳細を表示したり、サーバ ID を設定したり、トラフィック プロファイルまたは相関ルールに関するホストプロファイル資格内の情報を使用したりできません。加えて、システムはこの種の検出に基づいて脆弱性とホストを関連付けません。

ただし、アプリケーションプロトコル情報が接続内に存在するかどうかに対する相関イベントをトリガーできます。また、接続ログ内のアプリケーションプロトコル情報を使用して、接続トラッカーとトラフィック プロファイルを作成できます。

ホスト制限と検出イベント ロギング

システムがクライアント、サーバ、または Web アプリケーションを検出すると、関連するホストがすでにクライアント、サーバ、または Web アプリケーションの最大数に達していなければ、検出イベントが生成されます。

ホスト プロファイルには、ホストごとに最大 16 のクライアント、100 のサーバ、および 100 の Web アプリケーションが表示されます。

クライアント、サーバ、または Web アプリケーションの検出によって異なるアクションはこの制限の影響を受けないことに注意してください。たとえば、サーバ上でトリガーするように設定されたアクセス コントロール ルールでは、引き続き、接続イベントが記録されます。

アプリケーション検出に関する特別な考慮事項

SFTP

SFTP トラフィックを検出するためには、同じルールが SSH も検出する必要があります。

Squid

システムは、次のいずれかの場合に Squid サーバ トラフィックを肯定的に識別します。

- モニタ対象ネットワーク上のホストからプロキシ認証が有効になっている Squid サーバへの接続をシステムが検出した場合
- モニタ対象ネットワーク上の Squid プロキシ サーバからターゲット システム（つまり、クライアントが情報または別のリソースを要求する宛先サーバ）への接続をシステムが検出した場合

ただし、システムは次の場合に Squid サービス トラフィックを識別できません。

- 監視対象ネットワーク上のホストが、プロキシ認証が無効になっている Squid サーバに接続している場合
- Squid プロキシ サーバが HTTP 応答から Via: ヘッダー フィールドを除去するように設定されている場合

SSL アプリケーション検出

システムは、Secure Socket Layer（SSL）セッションからのセッション情報を使用してセッション内のアプリケーション プロトコル、クライアント アプリケーション、または Web アプリケーションを識別するアプリケーション ディテクタを備えています。

システムは暗号化された接続を検出すると、その接続を汎用 HTTPS 接続として、または、該当する場合には SMTPS などのより特殊なセキュア プロトコルとしてマークします。システムは SSL セッションを検出すると、そのセッションに対する接続イベント内の **Client** フィールドに `SSL client` を追加します。セッションの Web アプリケーションが識別されると、システムでトラフィックの検出イベントが生成されます。

SSLアプリケーショントラフィックの場合は、管理対象デバイスも、サーバ証明書から一般名を検出してSSLホストパターンからのクライアントまたはWebアプリケーションと照合できます。システムが特定のクライアントを識別すると、`SSL client`をそのクライアントの名前に置き換えます。

SSLアプリケーショントラフィックは暗号化されるため、システムは暗号化されたストリーム内のアプリケーションデータではなく、証明書内の情報しか識別に使用できません。そのため、SSLホストパターンではアプリケーションを制作した会社しか識別できない場合があり、同じ会社が作成したSSLアプリケーションは識別情報が同じ可能性があります。

HTTPSセッションがHTTPセッション内から起動される場合などは、管理対象デバイスがクライアント側のパケット内のクライアント証明書からサーバ名を検出します。

SSLアプリケーション識別を有効にするには、応答側のトラフィックを監視するアクセスコントロールルールを作成する必要があります。このようなルールには、SSLアプリケーションに関するアプリケーション条件またはSSL証明書からのURLを使用したURL条件を含める必要があります。ネットワーク検出では、応答側のIPアドレスがネットワーク上に存在しなくても、ネットワーク検出ポリシーでモニタできます。アクセスコントロールポリシーの設定によって、トラフィックが識別されるかどうかが決まります。SSLアプリケーションの検出を識別するには、アプリケーションディテクタリストで、または、アプリケーション条件をアクセスコントロールルールに追加するときに、`SSL protocol`タグでフィルタ処理します。

参照先 Web アプリケーション

Webサーバがトラフィックを他のWebサイト（通常は、アドバタイズメントサーバ）に参照する場合があります。ネットワーク上で発生するトラフィック参照のコンテキストをわかりやすくするために、システムは、参照セッションに対するイベント内の[Webアプリケーション（Web Application）]フィールドにトラフィックを参照したWebアプリケーションを列挙します。VDBに既知の照会先サイトのリストが含まれています。システムがこのようなサイトのいずれかからのトラフィックを検出すると、照会元サイトがそのトラフィックに対するイベントと一緒に保存されます。たとえば、Facebook経由でアクセスされるアドバタイズメントが実際はAdvertising.com上でホストされている場合は、検出されたAdvertising.comトラフィックがFacebook Webアプリケーションに関連付けられます。また、システムは、Webサイトで他のサイトへの単リンクが提供されている場合などは、HTTPトラフィック内の参照元URLを検出することもできます。この場合、参照元URLは[HTTP参照元（HTTP Referrer）]イベントフィールドに表示されます。

イベントでは、参照元アプリケーションが存在する場合に、それがトラフィックのWebアプリケーションとして列挙されますが、URLは参照先サイトのURLです。上の例では、トラフィックに対する接続イベントのWebアプリケーションはFacebookですが、URLはAdvertising.comです。参照元Webアプリケーションが検出されない場合、ホストが自身を参照している場合、または参照がチェインしている場合は、参照先アプリケーションがWebアプリケーションとして表示される場合もあります。ダッシュボードでは、Webアプリケーションの接続カウントとバイトカウントに、Webアプリケーションが参照先のトラフィックに関連付けられたセッションが含まれます。

照会先トラフィックに対して明示的に機能するルールを作成する場合は、照会元アプリケーションではなく、照会先アプリケーションに関する条件を追加する必要があることに注意して

ください。Facebook から参照される Advertising.com トラフィックをブロックするには、Advertising.com アプリケーションのアクセス コントロール ルールにアプリケーション条件を追加します。

カスタム アプリケーション ディテクタ

ネットワーク上でカスタムアプリケーションを使用する場合、アプリケーションの識別に必要な情報をシステムに提供するカスタム Web アプリケーション、クライアント、またはアプリケーションプロトコルディテクタを作成します。アプリケーションディテクタの種類は、[プロトコル（Protocol）]、[タイプ（Type）]、および [検出方向（Direction）] フィールドで選択した内容によって決まります。

システムがサーバ トラフィックでアプリケーション プロトコルの検出および識別を開始するように、クライアントセッションにサーバからの応答パケットを含める必要があります。UDP トラフィックの場合、応答パケットの送信元がサーバとして指定されることに注意してください。

すでに別の Firepower Management Center にディテクタを作成している場合、そのディテクタをエクスポートして、この Firepower Management Center にインポートすることができます。その後、必要に応じてインポートしたディテクタを編集できます。カスタムディテクタおよびCisco Professional サービスが提供するディテクタをエクスポートおよびインポートすることができます。ただし、シスコが提供するその他の種類のディテクタをエクスポートおよびインポートすることは**できません**。

カスタム アプリケーション ディテクタおよびユーザ定義アプリケーション フィールド

次のフィールドを使用して、カスタム アプリケーション ディテクタおよびユーザ定義アプリケーションを設定できます。

カスタム アプリケーション ディテクタ フィールド：概要

基本および高度なカスタム アプリケーション ディテクタを設定するには、次のフィールドを使用します。

アプリケーション プロトコル（Application Protocol）

検出するアプリケーションプロトコル。これには、システムが提供するアプリケーションまたはユーザ定義のアプリケーションを指定できます。

アプリケーションを（アイデンティティ ルールで設定された）アクティブな認証から除外できるようにする場合は、**User-Agent Exclusion** タグを使用してアプリケーション プロトコルを選択するか、作成する必要があります。

説明

アプリケーション ディテクタの説明。

[名前（Name）]

アプリケーション ディテクタの名前。

ディテクタ タイプ（Detector Type）

ディテクタのタイプ（[基本（Basic）] または [高度（Advanced）]）。基本的なアプリケーションディテクタは、一連のフィールドとして Web インターフェイスで作成されます。高度なアプリケーション ディテクタは、外部で作成され、カスタム .lua ファイルとしてアップロードされます。

カスタム アプリケーション ディテクタ（Custom Application Detector）フィールド：検出パターン

基本的なカスタム アプリケーション ディテクタの検出パターンを設定するには、次のフィールドを使用します。

方向（Direction）

ディテクタが検出するトラフィックの送信元。[クライアント（Client）] または [サーバ（Server）]。

オフセット（Offset）

システムがパターンの検索を開始する必要がある、パケット ペイロードの先頭からのパケットの場所（バイト単位）。

パケット ペイロードは 0 バイトから始まるため、パケット ペイロードの先頭から数えたバイト数から 1 を減算することでオフセットを計算します。たとえば、パケットの 5 桁目のビット パターンを検索するには、[オフセット（Offset）] フィールドに「4」と入力します。

パターン

パターン文字列は、選択した [タイプ（Type）] に関連付けられます。

ポート

ディテクタが検出するトラフィックのポート。

プロトコル

検出するプロトコル。選択するプロトコルによって、[タイプ（Type）] フィールドが表示されるか [URL（URL）] フィールドが表示されるかが決まります。

プロトコル（および、場合によっては、[タイプ（Type）] フィールドと [方向（Direction）] フィールドの後続の選択）によって、作成するアプリケーションディテクタのタイプ（Web アプリケーション、クライアント、またはアプリケーションプロトコル）が決まります。

ディテクタ タイプ（**Detector Type**）	プロトコル	タイプ（**Type**）または 方向（**Direction**）
Web アプリケーション（Web Application）	HTTP	[タイプ（Type）] は [コンテンツ タイプ（Content Type）] または [URL（URL）] です。
	RTMP	任意（Any）
	SSL	任意（Any）
クライアント（Client）	HTTP	[タイプ（Type）] は [ユーザ エージェント（User Agent）] です。
	SIP	任意（Any）
	TCP または UDP	[方向（Direction）] は [クライアント（Client）] です。
アプリケーション プロトコル（Application Protocol）	TCP または UDP	[方向（Direction）] は [サーバ（Server）] です。

タイプ（Type）

入力したパターン文字列のタイプ。表示されるオプションは、選択した [プロトコル（Protocol）] によって決まります。プロトコルとして [RTMP（RTMP）] を選択すると、[タイプ（Type）] フィールドの代わりに [URL（URL）] フィールドが表示されます。

（注） [タイプ（Type）] として [ユーザ エージェント（User Agent）] を選択すると、システムはアプリケーションの [タグ（Tag）] を **User-Agent Exclusion** に自動的に設定します。

タイプの選択	文字列特性
Ascii	文字列は ASCII でエンコードされます。
Common Name	文字列は、サーバ応答メッセージ内の commonName フィールドの値です。
コンテンツ タイプ（Content Type）	文字列は、サーバ応答ヘッダー内のコンテンツ タイプ フィールドの値です。
16 進数	文字列は、16 進表記です。
組織	文字列は、サーバ応答メッセージ内の organizationName フィールドの値です。

タイプの選択	文字列特性
SIP サーバ	文字列は、メッセージ ヘッダー内の From フィールドの値です。
SSL ホスト（SSL Host）	文字列は、ClientHello メッセージ内の server_name フィールドの値です。
URL	文字列は URL です。 （注） ディテクタは、ユーザが入力する文字列が URL の完全なセクションであると想定します。たとえば、**cisco.com** と入力した場合、**www.cisco.com/support** や **www.cisco.com** と一致しますが、**www.wearecisco.com** とは一致しません。
ユーザ エージェント（User Agent）	文字列は、GET リクエスト ヘッダー内の user-agent フィールドの値です。これは SIP プロトコルにも使用可能であり、文字列が SIP メッセージ ヘッダー内の User-Agent フィールドの値であることを示します。

URL

RTMP パケットの C2 メッセージ内の swfURL フィールドの完全な URL または URL のセクション。[プロトコル（Protocol）] として [RTMP（RTMP）] を選択すると、[タイプ（Type）] フィールドの代わりにこのフィールドが表示されます。

（注） ディテクタは、ユーザが入力する文字列がURLの完全なセクションであると想定します。たとえば、**cisco.com** と入力した場合、**www.cisco.com/support** や **www.cisco.com** と一致しますが、**www.wearecisco.com** とは一致しません。

ユーザ定義のアプリケーション フィールド

基本および高度なカスタム アプリケーション ディテクタでユーザ定義のアプリケーションを設定するには、次のフィールドを使用します。

ビジネスとの関連性（Business Relevance）

アプリケーションが娯楽ではなく組織のビジネス活動のコンテキストで使用される可能性。[非常に高い（Very High）]、[高（High）]、[中（Medium）]、[低（Low）]、または [非常に低い（Very Low）]。アプリケーションを最も的確に説明するオプションを選択します。

カテゴリ（Categories）

アプリケーションの最も重要な機能を説明する一般分類。

説明

アプリケーションの説明。

[名前（Name）]

アプリケーションの名前。

リスク（Risk）

アプリケーションが組織のセキュリティ ポリシーに対抗する目的で使用される可能性。[非常に高い（Very High）]、[高（High）]、[中（Medium）]、[低（Low）] または [非常に低い（Very Low）]。アプリケーションを最も的確に説明するオプションを選択します。

タグ（Tags）

アプリケーションに関する追加情報を提供する 1 つ以上の事前定義されたタグ。アプリケーションを（アイデンティティ ルールで設定された）アクティブな認証から除外できるようにする場合は、**User-Agent Exclusion** タグをアプリケーションに追加する必要があります。

カスタム アプリケーション ディテクタの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Discovery Admin

基本または高度なカスタム アプリケーション ディテクタを設定できます。

ステップ 1 **[Policies]** > **[Application Detectors]** を選択します。

ステップ 2 [カスタム ディテクタの作成（Create Custom Detector）] をクリックします。

ステップ 3 [名前（Name）] と [説明（Description）] を入力します。

ステップ 4 [アプリケーション プロトコル（Application Protocol）] を選択します。次の選択肢があります。

- 既存のアプリケーション プロトコルのディテクタを作成する場合（たとえば、非標準ポートで特定のアプリケーション プロトコルを検出する場合）、ドロップダウン リストからアプリケーション プロトコルを選択します。
- ユーザ定義アプリケーションのディテクタを作成する場合は、ユーザ定義のアプリケーションの作成（2559 ページ）に示されている手順に従います。

ステップ 5 [ディテクタ タイプ（Detector Type）] を選択します。

ステップ 6 [OK] をクリックします。

ステップ 7 [検出パターン（Detection Patterns）] または [検出基準（Detection Criteria）] を設定します。

- 基本ディテクタを設定する場合は、基本ディテクタでの検出パターンの指定（2560 ページ）の説明に従って、プリセットした [検出パターン（Detection Patterns）] を指定します。

- 高度なディテクタを設定する場合は、高度なディテクタでの検出条件の指定（2561ページ）の説明に従って、カスタム [検出基準（Detection Criteria）] を指定します。

注意 高度なカスタム ディテクタは複雑で、有効な .lua ファイルを作成すること以外の知識も必要になります。ディテクタを誤って設定すると、パフォーマンスや検出機能にマイナスの影響を与える可能性があります。

ステップ 8 必要に応じて、カスタム アプリケーション プロトコル ディテクタのテスト（2563 ページ）の説明に従って、[パケット キャプチャ（Packet Captures）] を使用して新しいディテクタをテストします。

ステップ 9 [保存（Save）] をクリックします。

（注） アクセス コントロール ルールにアプリケーションを含めると、ディテクタは自動的にアクティブにされ、使用中は非アクティブにできません。

次のタスク

- ディテクタのアクティブおよび非アクティブの設定（2567ページ）の説明に従ってディテクタをアクティブにします。

関連トピック

カスタム アプリケーション ディテクタおよびユーザ定義アプリケーション フィールド（2554 ページ）

ユーザ定義のアプリケーションの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Discovery Admin

ここで作成するアプリケーション、カテゴリ、およびタグは、アクセス コントロール ルールやアプリケーション フィルタ オブジェクト マネージャで使用できます。

注意 ユーザ定義アプリケーションを作成すると、展開プロセスを経由することなく、ただちにSnortプロセスが再起動します。Snort プロセスの再起動を続行することが警告され、キャンセルが可能になります。再起動は、現在のドメインまたはそのいずれかの子ドメイン内のいずれかの管理対象デバイスで発生します。 この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、ターゲットデバイスがトラフィックを処理する方法に応じて異なります。詳細はSnort® の再起動によるトラフィックの動作（451 ページ）を参照してください。

始める前に

- カスタム アプリケーション ディテクタの設定 （2558 ページ）の説明に従って、カスタム アプリケーション プロトコル ディテクタの設定を開始します。

ステップ 1 [ディテクタの作成（Create Detector）] ページで、[追加（Add）] をクリックします。

ステップ 2 [名前（Name）] を入力します。

ステップ 3 [説明（Description）] を入力します。

ステップ 4 [ビジネスとの関連性（Business Relevance）] を選択します。

ステップ 5 [リスク（Risk）] を選択します。

ステップ 6 [カテゴリ（Categories）] の横にある [追加（Add）] をクリックしてカテゴリを追加し、新しいカテゴリの名前を入力するか、または [カテゴリ（Categories）] ドロップダウン リストから既存のカテゴリを選択します。

ステップ 7 オプションで、[タグ（Tags）] の横にある [追加（Add）] をクリックしてタグを追加し、新しいタグの名前を入力するか、または [タグ（Tags）] ドロップダウン リストから既存のタグを選択します。

ステップ 8 [OK] をクリックします。

次のタスク

- カスタム アプリケーション ディテクタの設定 （2558 ページ）の説明に従って、カスタム アプリケーション プロトコル ディテクタの設定を続けます。トラフィックを分析するためにシステムがディテクタを使用できるようにするには、その前に、ディテクタを保存してアクティブにする必要があります。

関連トピック

カスタム アプリケーション ディテクタおよびユーザ定義アプリケーション フィールド （2554 ページ）

基本ディテクタでの検出パターンの指定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Discovery Admin

アプリケーション プロトコルのパケット ヘッダーで特定のパターン文字列を検索するよう、カスタム アプリケーション プロトコル ディテクタを設定できます。また、複数のパターンを検索するようにディテクタを設定することもできます。この場合は、アプリケーションプロトコルのトラフィックは、アプリケーションプロトコルを確実に識別するため、ディテクタのすべてのパターンとマッチングさせる必要があります。

アプリケーション プロトコル ディテクタは、オフセットを使用して ASCII または 16 進数のパターンを検索できます。

始める前に

- カスタム アプリケーション ディテクタの設定 （2558 ページ）の説明に従って、カスタム アプリケーション プロトコル ディテクタの設定を開始します。

ステップ 1 [ディテクタの作成（Create Detector）] ページの [検出パターン（Detection Patterns）] セクションで、[追加（Add）] をクリックします。

ステップ 2 ディテクタの検査対象とするトラフィックの [プロトコル（Protocol）] を選択します。

ステップ 3 ユーザが検出するパターン [タイプ（Type）] を指定します。

ステップ 4 指定した [タイプ（Type）] に一致する [パターン文字列（Pattern String）] を入力します。

ステップ 5 オプションで、[オフセット（Offset）] を入力します（バイト単位）。

ステップ 6 オプションで、使用するポートに基づいてアプリケーション プロトコルのトラフィックを指定するには、1 から 65535 までのポートを [ポート（Port(s)）] フィールドに入力します。複数のポートを使用する場合は、カンマで区切ります。

ステップ 7 オプションで、[クライアント（Client）] または [サーバ（Server）] のいずれかの [方向（Direction）] を選択します。

ステップ 8 [OK] をクリックします。

ヒント パターンを削除する場合、削除するパターンの横の削除アイコン（）をクリックします。

次のタスク

- カスタム アプリケーション ディテクタの設定 （2558 ページ）の説明に従って、カスタム アプリケーション プロトコル ディテクタの設定を続けます。トラフィックを分析するためにシステムがディテクタを使用できるようにするには、その前に、ディテクタを保存してアクティブにする必要があります。

関連トピック

高度なディテクタでの検出条件の指定 （2561 ページ）

高度なディテクタでの検出条件の指定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Discovery Admin

注意 高度なカスタムディテクタは複雑で、有効な.luaファイルを作成すること以外の知識も必要になります。ディテクタを誤って設定すると、パフォーマンスや検出機能にマイナスの影響を与える可能性があります。

注意 信頼できないソースから .lua ファイルをアップロードしないでください。

カスタム.luaファイルには、カスタムアプリケーションのディテクタ設定を含めます。カスタム .lua ファイルを作成するには、lua プログラミング言語に関する高度な知識とシスコの C-lua API に関する経験が求められます。以下を使用して、.lua ファイルを準備することを強くお勧めします。

- lua プログラミング言語に関するサードパーティの説明書と参考資料
- オープン ソース ディテクタ開発者ガイド： https://www.snort.org/downloads
- OpenAppID Snort コミュニティ リソース： http://blog.snort.org/search/label/openappid

（注） システムは、システム コールまたはファイル I/O を参照する .lua ファイルをサポートしていません。

始める前に

- カスタム アプリケーション ディテクタの設定 （2558 ページ）の説明に従って、カスタム アプリケーション プロトコル ディテクタの設定を開始します。
- 該当する .lua ファイルをダウンロードし、内容を調べることによって、有効な .lua ファイルを作成する準備を進めます。ディテクタ ファイルのダウンロードの詳細については、ディテクタ詳細の表示またはダウンロード （2564 ページ）を参照してください。
- カスタム アプリケーションのディテクタ設定を含む有効な .lua ファイルを作成します。

ステップ 1 高度なカスタム アプリケーション ディテクタの [ディテクタの作成（Create Detector）] ページにある [検出条件（Detection Criteria）] セクションで、[追加（Add）] をクリックします。

ステップ 2 [参照...（Browse...）] をクリックして、**`.lua`** ファイルに移動し、アップロードします。

ステップ 3 [OK] をクリックします。

次のタスク

- カスタム アプリケーション ディテクタの設定 （2558 ページ）の説明に従って、カスタム アプリケーション プロトコル ディテクタの設定を続けます。トラフィックを分析するた

めにシステムがディテクタを使用できるようにするには、その前に、ディテクタを保存してアクティブにする必要があります。

関連トピック

基本ディテクタでの検出パターンの指定 （2560 ページ）

カスタム アプリケーション プロトコル ディテクタのテスト

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Discovery Admin

検出するアプリケーションプロトコルからのトラフィックを持つパケットが格納されたパケット キャプチャ（pcap）ファイルが存在する場合、その pcap ファイルに対してカスタム アプリケーション プロトコル ディテクタをテストできます。シスコでは、不要なトラフィックのない単純でクリーンな pcap ファイルを使用することをお勧めします。

pcap ファイルは 256 KB 以下でなければなりません。それより大きい pcap ファイルに対してディテクタのテストを試行すると、Firepower Management Center は自動的にファイルを切り捨て、不完全なファイルをテストします。ディテクタをテストするためにファイルを使用する前に、pcap の未解決のチェックサムを修正する必要があります。

始める前に

- カスタム アプリケーション ディテクタの設定 （2558 ページ）の説明に従って、カスタム アプリケーション プロトコル ディテクタを設定します。

ステップ 1 [ディテクタの作成（Create Detector）] ページの [パケット キャプチャ（Packet Captures）] セクションで、[追加（Add）] をクリックします。

ステップ 2 ポップアップ ウィンドウで pcap ファイルを参照し、[OK] をクリックします。

ステップ 3 pcap ファイルの内容に対してディテクタをテストするには、pcap ファイルの横にある評価アイコンをクリックします。メッセージに、テストが成功したかどうかが示されます。

ステップ 4 必要に応じて手順 1 ～ 3 を繰り返し、その他の pcap ファイルに対してディテクタをテストします。

ヒント pcap ファイルを削除するには、削除するファイルの横の削除アイコン（）をクリックします。

次のタスク

- カスタム アプリケーション ディテクタの設定 （2558 ページ）の説明に従って、カスタム アプリケーション プロトコル ディテクタの設定を続けます。トラフィックを分析するためにシステムがディテクタを使用できるようにするには、その前に、ディテクタを保存してアクティブにする必要があります。

ディテクタ詳細の表示またはダウンロード

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Discovery Admin

ディテクタ リストを使用して、アプリケーション ディテクタの詳細を表示（すべてのディテクタ）したり、ディテクタの詳細をダウンロード（カスタム アプリケーション ディテクタのみ）したりできます。

ステップ 1 アプリケーション ディテクタの詳細を表示するには、次のいずれかを実行します。

- 関連する VDB バージョンについては、https://www.cisco.com/c/en/us/support/security/defense-center/products-technical-reference-list.html の『*Cisco Firepower Application Detector Reference*』[英語] を参照してください。
- a. **[Policies]** > **[Application Detectors]** を選択します。

  b. リストをフィルタ処理して、特定のディテクタを検索します。

  c. 情報アイコン（）をクリックします。

ステップ 2 カスタム アプリケーション ディテクタのディテクタ詳細をダウンロードするには、ダウンロード アイコン（）をクリックします。

コントロールが淡色表示されている場合、設定が先祖ドメインに属しているか、またはユーザが必要な権限を持っていません。

ディテクタ リストのソート

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Discovery Admin

[ディテクタ（Detectors）] ページには、デフォルトで名前のアルファベット順にディテクタがリストされます。列見出しの横にある上または下矢印は、ページがその列でその方向にソートされていることを示します。

ステップ 1 **[Policies]** > **[Application Detectors]** を選択します。
ステップ 2 該当する列見出しをクリックします。

検出機能リストのフィルタリング

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Discovery Admin

ステップ 1 **[Policies]** > **[Application Detectors]** を選択します。
ステップ 2 ディテクタ リストのフィルタ グループ （2565 ページ）に記載されているフィルタ グループの 1 つを展開し、フィルタの横にあるチェックボックスを選択します。グループ内のすべてのフィルタを選択するには、グループ名を右クリックし、[すべて選択（Check All）] を選択します。
ステップ 3 あるフィルタを削除するには、[フィルタ（Filters）]フィールドにあるフィルタの名前の削除アイコン（ ）をクリックするか、フィルタ リストでフィルタを無効にします。グループ内のすべてのフィルタを削除するには、グループ名を右クリックし、[すべて選択解除（Uncheck All）] を選択します。
ステップ 4 すべてのフィルタを削除するには、検出機能に適用されるフィルタ リストの横の [すべてクリア（Clear all）] をクリックします。

ディテクタ リストのフィルタ グループ

複数のフィルタ グループを別個にまたは組み合わせて使用し、ディテクタのリストをフィルタリングすることができます。

名前

ユーザが入力した文字列を含む名前または説明でディテクタを検索します。文字列には任意の英数字または特殊文字を含めることができます。

カスタム フィルタ

オブジェクト管理ページで作成したカスタム アプリケーション フィルタに一致するディテクタを検索します。

作成者（Author）

ディテクタを作成したユーザに照らしてディテクタを検索します。次によってディテクタをフィルタリングできます。

- カスタム ディテクタを作成またはインポートした個々のユーザ
- Cisco。これは、個別にインポートされたアドオン ディテクタを除く、シスコが提供するすべてのディテクタを表します（ディテクタをインポートした場合、そのユーザはそのディテクタの作成者になります）。
- 任意のユーザ（Any User）。これは、によって提供されたのではないすべてのディテクタを表します。

状態（State）

状態（つまり、アクティブまたは非アクティブ）に照らしてディテクタを検索します。

タイプ（Type）

アプリケーションディテクタの基本（2548ページ）に示すように、ディテクタ タイプに従ってディテクタを検索します。

プロトコル

ディテクタが検査するトラフィック プロトコルに照らしてディテクタを検索します。

カテゴリ（Category）

検出するアプリケーションに割り当てられたカテゴリに照らしてディテクタを検索します。

タグ

検出するアプリケーションに割り当てられたタグに照らしてディテクタを検索します。

リスク

検出するアプリケーションに割り当てられたリスク（Very High、 High、 Medium、 Low、 Very Low）に照らしてディテクタを検索します。

ビジネスとの関連性

検出するアプリケーションに割り当てられたビジネスとの関連性（[非常に高い（Very High）]、[高（High）]、[中（Medium）]、[低（Low）]、[非常に低い（Very Low）]）に照らしてディテクタを検索します。

別のディテクタ ページへの移動

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Discovery Admin

ステップ 1 **[Policies]** > **[Application Detectors]** を選択します。

ステップ 2 次のページを表示するには、右下矢印アイコン（ ）をクリックします。

ステップ 3 前のページを表示するには、左矢印のアイコン（ ）をクリックします。

ステップ 4 別のページを表示するには、ページ番号を入力して、Enter キーを押します。

ステップ 5 最後のページに移動するには、右矢印アイコン（ ）をクリックします。

ステップ 6 最初のページに移動するには、左矢印アイコン（ ）をクリックします。

ディテクタのアクティブおよび非アクティブの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Discovery Admin

ネットワーク トラフィックを分析するためにディテクタを使用できるようにするには、その前に、ディテクタをアクティブにする必要があります。デフォルトでは、Cisco が提供するすべてのディテクタはアクティブになっています。

システムの検出機能を補完するために、ポートごとに複数のアプリケーションディテクタをアクティブにすることができます。

ポリシーのアクセス コントロール ルールにアプリケーションを含め、そのポリシーを導入するときに、そのアプリケーションに対してアクティブなディテクタがない場合、1つ以上のディテクタが自動的にアクティブになります。同様に、導入されているポリシーのアプリケーションが使用されているときに、そのアプリケーションのアクティブなディテクタをすべて非アクティブにしようとしても、ディテクタを非アクティブにすることはできません。

ヒント パフォーマンスを向上させるために、使用する予定のないアプリケーションプロトコル、クライアント、または Web アプリケーションのディテクタはすべて非アクティブにします。

⚠

注意 システムまたはカスタムのアプリケーション ディテクタをアクティブ化/非アクティブ化すると、展開プロセスを経由することなく、ただちにSnortプロセスが再起動します。Snortプロセスの再起動を続行することが警告され、キャンセルが可能になります。再起動は、現在のドメインまたはそのいずれかの子ドメイン内のいずれかの管理対象デバイスで発生します。 この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、ターゲット デバイスがトラフィックを処理する方法に応じて異なります。詳細はSnort® の再起動によるトラフィックの動作 （451 ページ）を参照してください。

ステップ 1 **[Policies]** > **[Application Detectors]** を選択します。

ステップ 2 アクティブまたは非アクティブにするディテクタの横にあるスライダをクリックします。 コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

（注） 一部のアプリケーションディテクタはその他のディテクタによって必要とされることに注意してください。そのようなディテクタのいずれかを非アクティブにすると、それに依存するディテクタも無効となることを示す警告が表示されます。

カスタム アプリケーション ディテクタの編集

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Discovery Admin

カスタム アプリケーション ディテクタを変更するには、次の手順を使用します。

ステップ 1 **[Policies]** > **[Application Detectors]** を選択します。

ステップ 2 変更するディテクタの横にある編集アイコン（  ）をクリックします。代わりに表示アイコン（  ）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 カスタム アプリケーションディテクタの設定 （2558ページ）の説明に従って、ディテクタを変更します。

ステップ 4 ディテクタの状態に応じて、次の保存オプションがあります。

- 非アクティブなディテクタを保存するには、[保存（Save）] をクリックします。
- 非アクティブなディテクタを新規の非アクティブなディテクタとして保存するには、[新規保存（Save as New）] をクリックします。
- アクティブなディテクタを保存してすぐに使用を開始するには、[保存して再アクティブ化（Save and Reactivate）] をクリックします。

注意 カスタムアプリケーションディテクタを保存して再びアクティブ化すると、展開プロセスを経由することなく、ただちに Snort プロセスが再起動します。Snort プロセスの再起動を続行することが警告され、キャンセルが可能になります。再起動は、現在のドメインまたはそのいずれかの子ドメイン内のいずれかの管理対象デバイスで発生します。 この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、ターゲット デバイスがトラフィックを処理する方法に応じて異なります。詳細はSnort® の再起動によるトラフィックの動作 （451 ページ）を参照してください。

- アクティブなディテクタを新規の非アクティブなディテクタとして保存するには、[新規保存（Save as New）] をクリックします。

ディテクタの削除

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Discovery Admin

カスタムディテクタおよびCisco Professional サービスが提供する個別にインポートされたアドオンディテクタを削除することができます。その他の Cisco が提供するディテクタを削除することはできませんが、その多くを非アクティブにすることはできます。

（注） ディテクタが展開されたポリシーで使用されている間は、そのディテクタを削除できません。

注意 アクティブ化されたカスタム アプリケーション ディテクタを削除すると、展開プロセスを経由することなく、ただちにSnortプロセスが再起動します。Snortプロセスの再起動を続行することが警告され、キャンセルが可能になります。再起動は、現在のドメインまたはそのいずれかの子ドメイン内のいずれかの管理対象デバイスで発生します。 この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、ターゲットデバイスがトラフィックを処理する方法に応じて異なります。詳細はSnort® の再起動によるトラフィックの動作 （451 ページ）を参照してください。

ステップ 1 **[Policies]** > **[Application Detectors]** を選択します。

ステップ 2 削除するディテクタの横にある削除アイコン（）をクリックします。 代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 [OK] をクリックします。

第 100 章

レルムの作成および管理

次のトピックでは、ユーザの認識と制御のためのユーザ ストアであるレルムの作成方法と管理方法について説明します。

レルムについて

レルムとは、Firepower Management Center とモニタリング対象のサーバ上にあるユーザ アカウントの間の接続です。レルムでは、サーバの接続設定と認証フィルタの設定を指定します。レルムでは次のことを実行できます。

- アクティビティをモニタするユーザとユーザ グループを指定する。
- 権限のあるユーザ、および権限のあるユーザ以外の一部のユーザ（トラフィック ベースの検出で検出された POP3 および IMAP ユーザ、およびトラフィック ベースの検出、ユーザ エージェント、TS エージェント、ISE/ISE-PIC によって検出されたユーザ）のユーザ メタデータについてユーザ リポジトリに照会する。

レルム内のディレクトリとして複数のドメイン コントローラを追加できますが、同じ基本レルム情報を共有する必要があります。レルム内のディレクトリは、LDAP サーバのみ、または Active Directory（AD）サーバのみである必要があります。レルムを有効にすると、保存された変更は次回 Firepower Management Centerがサーバに照会するときに適用されます。

ユーザ認識を行うには、レルムがサポートされているサーバのレルムを設定する必要があります。システムは、これらの接続を使用して、POP3 および IMAP ユーザに関連するデータについてサーバにクエリし、トラフィック ベースの検出で検出された LDAP ユーザに関するデータを収集します。

システムは、POP3 および IMAP ログイン内の電子メール アドレスを使用して、Active Directory または OpenLDAP 上の LDAP ユーザに関連付けます。たとえば、LDAP ユーザと電子メール ア

ドレスが同じユーザの POP3 ログインを管理対象デバイスが検出すると、システムは LDAP ユーザのメタデータをそのユーザに関連付けます。

ユーザ制御を実行するために以下のいずれかを設定できます。

- ユーザ エージェントまたは ISE/ISE-PIC 用の AD サーバのレルム

  ユーザ エージェントまたは ISE/ISE-PIC 用の AD サーバのレルム

（注） SGT ISE 属性条件を設定することを計画しているものの、ユーザ、グループ、レルム、エンドポイント ロケーション、エンドポイント プロファイルの条件の設定は計画していない場合、レルムの設定はオプションです。

- TS エージェント用の AD サーバのレルム
- キャプティブ ポータル用の AD または OpenLDAP サーバのレルム

。

ユーザ ダウンロードについて

特定の検出されたユーザの、次のユーザとユーザ グループのメタデータを取得するために、Firepower Management Center と LDAP サーバまたは AD サーバとの間の接続を確立するためのレルムを設定することができます。

- キャプティブ ポータルで認証されたか、あるいはユーザ エージェントまたは ISE/ISE-PIC で報告された LDAP および AD のユーザ。このメタデータは、ユーザ認識とユーザ制御に使用できます。
- トラフィック ベースの検出により検出された POP3 と IMAP ユーザ ログイン（ユーザが LDAP または AD ユーザと同じ電子メール アドレスを持つ場合）。このメタデータは、ユーザ認識に使用できます。

レルム内のディレクトリとして、LDAP サーバまたは Active Directory ドメイン コントローラ接続を設定します。ユーザ認識とユーザ制御のためにレルムのユーザおよびユーザ グループ データをダウンロードするには、[アクセス コントロールのためのユーザおよびユーザ グループのダウンロード（Download users and user groups for access control）] をオンにする必要があります。

Firepower Management Centerは、ユーザごとに次の情報とメタデータを取得します。

- LDAP ユーザ名
- 姓と名
- 電子メール アドレス（Email address）
- 部署名（Department）
- 電話番号（Telephone number）

ユーザ アクティビティ データについて

ユーザ アクティビティ データはユーザ アクティビティ データベースに保存され、ユーザのアイデンティティ データはユーザ データベースに保存されます。アクセス制御で保存できる使用可能なユーザの最大数は Firepower Management Center モデルによって異なります。含めるユーザとグループを選択するときは、ユーザの総数がモデルの上限より少ないことを確認してください。アクセス制御パラメータの範囲が広すぎる場合、Firepower Management Center はできるだけ多くのユーザに関する情報を取得し、取得できなかったユーザの数をメッセージセンターの [タスク（Tasks）] タブ ページで報告します。

（注） ユーザ リポジトリからシステムによって検出されたユーザを削除しても、Firepower Management Center はユーザ データベースからそのユーザを削除しません。そのため、手動で削除する必要があります。ただし、LDAP に対する変更は、次に権限のあるユーザのリストを Firepower Management Center が更新したときにアクセス 制御ルールに反映されます。

レルムおよび信頼できるドメイン

Firepower Management Center でレルムを設定すると、そのレルムは Active Directory または LDAP ドメインに関連付けられます。

互いに信頼する Microsoft Active Directory（AD）ドメインのグループ化は、一般的にフォレストと呼ばれます。この信頼関係により、ドメインは異なる方法で互いのリソースにアクセスできます。たとえば、ドメイン A で定義されたユーザ アカウントに、ドメイン B で定義されたグループのメンバーとしてマークを付けることができます。

Firepower システムは、信頼できる AD ドメインをサポートしていません。つまり、Firepower システムは、どのドメインが互いに信頼しているかを追跡せず、どのドメインが互いの親ドメインまたは子ドメインかを認識しません。また、Firepower システムでは、信頼関係が Firepower システム外で実施される場合でも、クロスドメイン信頼を使用する環境のサポートを保証するテストがまだ行われていません。

詳細については、「レルムとユーザのダウンロードのトラブルシュート（2586ページ）」を参照してください。

レルムがサポートされているサーバ

レルムを設定して次のサーバ タイプに接続すると、Firepower Management Centerからの TCP/IP アクセスを提供できます。

サーバ タイプ（Server Type）	ユーザ エージェントによるデータ取得のサポート	ISE/ISE-PIC によるデータ取得のサポート	TS エージェントによるデータ取得のサポート	キャプティブ ポータルによるデータ取得のサポート
Windows Server 2008 と Windows Server 2012 上の Microsoft Active Directory	あり	あり	あり	あり
Linux 上の OpenLDAP	なし	なし	なし	あり

（注） TS エージェントが別のパッシブ認証 ID ソース（ユーザ エージェントまたは /ISE-PIC）と共有されている Windows サーバ上の Microsoft Active Directory にインストールされている場合、Firepower Management Center は TS エージェントのデータを優先します。TS エージェントとパッシブ ID ソースが同じ IP アドレスによるアクティビティを報告した場合は、TS エージェントのデータのみが Firepower Management Center に記録されます。

サーバ グループの設定に関して次の点に注意してください。

- ユーザ グループまたはグループ内のユーザに対してユーザ制御を実行するには、LDAP または Active Directory サーバでユーザ グループを設定する必要があります。サーバが基本的なオブジェクト階層でユーザを整理している場合、Firepower Management Centerはユーザ グループ制御を実行できません。
- グループ名は LDAP で内部的に使用されているため、**s-** で開始することはできません。

  グループ名または組織単位名には、アスタリスク（*）、イコール（=）、バックスラッシュ（\）などの特殊文字は使用できません。使用すると、それらのグループまたは組織単位内のユーザはダウンロードされず、アイデンティティ ポリシーでは使用できません。
- サーバ上のサブグループのメンバーであるユーザを含む（または除外する）Active Directory レルムを設定するには、Windows Server 2008 または 2012 では、Active Directory のグループあたりのユーザ数が 5000 人以下であることが Microsoft により推奨されていることに注意してください。詳細については、MSDN の「Active Directory Maximum Limits—Scalability」を参照してください。

  必要に応じて、より多くのユーザをサポートするため、このデフォルトの制限を引き上げるよう Active Directory サーバの設定を変更できます。
- リモート デスクトップ サービス環境でサーバにより報告されるユーザを一意に識別するには、Cisco Terminal Services（TS）エージェントを設定する必要があります。TS エージェントをインストールし、設定すると、このエージェントは各ユーザに別個のポートを割り当て、Firepower System はこれらのユーザを一意に識別できるようになります。（Microsoft

により、ターミナル サービスという名称はリモート デスクトップ サービスに変更されました）。

TS エージェントの詳細については、『*Cisco Terminal Services (TS) Agent Guide*』を参照してください。

サポートされているサーバ オブジェクト クラスと属性名

Firepower Management Center がサーバからユーザ メタデータを取得できるようにするには、レルム内のサーバが、次の表に記載されている属性名を使用する必要があります。サーバ上の属性名が正しくない場合、Firepower Management Center はその属性の情報を使ってデータベースに入力できなくなります。

表 *261 : Firepower Management Center* フィールドへの属性名のマップ

メタデータ	FMC 属性	LDAP オブジェクト クラス	Active Directory 属性	OpenLDAP 属性
LDAP ユーザ名	Username	• user • inetOrgPerson	samaccountname	cn uid
名	First Name		givenname	givenname
姓	Last Name		sn	sn
電子メール アドレス	Email		mail userprincipalname（mail に値が設定されていない場合）	mail
department	department		department distinguishedname（department に値が設定されていない場合）	ou
telephone number	Phone		telephonenumber	telephonenumber

（注） グループの LDAP オブジェクト クラスは、`group`、`groupOfNames`（Active Directory の場合は `group-of-names`）、または `groupOfUniqueNames` です。

オブジェクト クラスと属性の詳細については、次のリファレンスを参照してください。

- Microsoft Active Directory：
  - オブジェクト クラス：MSDN の「All Classes」

- 属性：MSDN の「All Attributes」

- OpenLDAP：RFC 4512

レルムの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	Control	いずれか（Any）	いずれか（Any）	Administrator、Access Admin、Network Admin

レルム設定フィールドの詳細については、レルム フィールド （2577ページ）を参照してください。

（注） すべての Microsoft Active Directory（AD）レルムに固有の [ADプライマリドメイン（AD Primary Domain）] を指定する必要があります。ユーザとグループが適切に識別されないため、同じ [AD プライマリ ドメイン（AD Primary Domain）] を使用して複数のレルムを指定することはできません。これは、システムが一意の ID を各レルムのすべてのユーザとグループに割り当てるために発生します。そのため、システムは特定のユーザまたはグループを明確に識別できません。

ステップ 1 Firepower Management Center にログインします。

ステップ 2 **[System]** > **[Integration]** をクリックします。

ステップ 3 [レルム（Realms）] をクリックします。

ステップ 4 新しいレルムを作成するには、[新規レルム（New Realm）] をクリックします。

ステップ 5 その他のタスク（レルムの有効化、無効化、削除など）を実行する場合は、レルムの管理 （2584ページ）を参照してください。

ステップ 6 レルム フィールド （2577 ページ）で説明したように、レルム情報を入力します。

ステップ 7 （オプション）[AD参加のテスト（Test AD Join）] をクリックして、レルムへの接続をテストします。

（注） Microsoft Active Directory のレルム テストを成功させるには、[AD参加ユーザ名（AD Join Username）] フィールドと [AD参加パスワード（AD Join Password）] フィールドの両方に値を入力し、ドメインにコンピュータを追加するための十分な権限がユーザにある必要があります。詳細については、レルム フィールド （2577 ページ）を参照してください。

ステップ 8 [OK] をクリックします。

ステップ 9 レルム ディレクトリの設定 （2582ページ）で説明したように、少なくとも 1 つのディレクトリを設定します。

ステップ 10 ユーザとグループのダウンロード（2583ページ）の説明に従って、（アクセス コントロールに必要な）ユーザとユーザ グループのダウンロードを設定します。

ステップ 11 [レルム設定（Realm Configuration）] タブをクリックします。

ステップ 12 [ユーザエージェントおよびISE/ISE-PICユーザ（User Agent and ISE/ISE-PIC Users）]、[TSエージェントユーザ（TS Agent Users）]、[キャプティブポータルユーザ（Captive Portal Users）]、[失敗したキャプティブポータルユーザ（Failed Captive Portal Users）]、および [ゲストキャプティブポータルユーザ（Guest Captive Portal Users）] のユーザ セッション タイムアウト値を分単位で入力します。

次のタスク

- レルム ディレクトリの設定 （2582 ページ）
- レルムの編集、削除、有効化、または無効化を行います。レルムの管理 （2584ページ）を参照してください
- レルムの比較 （2585 ページ）。
- 必要に応じて、タスクのステータスをモニタします（タスク メッセージの表示 （417ページ） を参照）。

レルム フィールド

次のフィールドを使用して、レルムを設定します。

レルムの設定（Realm Configuration）フィールド

これらの設定は、レルム内のすべてのActive Directoryサーバまたはドメイン コントローラ（別名ディレクトリ）に適用されます。

Name

レルムの一意の名前。

- アイデンティティ ポリシーにレルムを使用する場合、英数字や特殊文字に対応しています。
- RA VPN 設定でレルムを使用する場合は、英数字、ハイフン（-）、下線（_）、プラス（+）に対応しています。

説明

（オプション）レルムの説明を入力します。

AD プライマリ ドメイン（AD Primary Domain）

Microsoft Active Directory レルム専用です。ユーザ認証が必要となる Active Directory サーバのドメインです。

（注） すべての Microsoft Active Directory（AD）レルムに固有の [ADプライマリドメイン（AD Primary Domain）] を指定する必要があります。ユーザとグループが適切に識別されないため、同じ [AD プライマリ ドメイン（AD Primary Domain）] を使用して複数のレルムを指定することはできません。これは、システムが一意の ID を各レルムのすべてのユーザとグループに割り当てるために発生します。そのため、システムは特定のユーザまたはグループを明確に識別できません。

AD 参加ユーザ名（AD Join Username）、AD 参加パスワード（AD Join Password）

Kerberos キャプティブ ポータル アクティブ認証を目的とした Microsoft Active Directory レルムでは、Active Directory ドメインでドメイン コンピュータ アカウントを作成するための適切な権限を持つ Active Directory ユーザの識別用のユーザ名とパスワード。

次の点を考慮してください。

- DNS は、ドメイン名を Active Directory ドメイン コントローラの IP アドレスに解決できる必要があります。
- 指定するユーザは、コンピュータを Active Directory ドメインに参加させることができる必要があります。
- ユーザ名は完全修飾名である必要があります（たとえば、**administrator** ではなく **administrator@mydomain.com** を使用します）。

アイデンティティ ルールの **[認証プロトコル（Authentication Protocol）]** に **Kerberos** を選択する場合（または Kerberos をオプションとして **HTTP Negotiate** を選択する場合）、Kerberos キャプティブ ポータル アクティブ認証を実行するには、[アクティブディレクトリ参加ユーザ名（AD Join Username）] と [アクティブディレクトリ参加パスワード（AD Join Password）] を使用して、選択した [レルム（Realm）] を設定する必要があります。

[ディレクトリ ユーザ名（Directory Username）] と [ディレクトリ パスワード（Directory Password）]

取得するユーザ情報に適切なアクセス権を持っているユーザの識別用のユーザ名とパスワード。

次の点に注意してください。

- Microsoft Active Directory では、ユーザに昇格された特権は必要ありません。ドメイン内の任意のユーザを指定できます。
- OpenLDAP では、ユーザのアクセス権限は、OpenLDAP の仕様書のセクション 8 で説明されている `<level>` パラメータにより決定されます。ユーザの `<level>` は、`auth` 以上にする必要があります。
- ユーザ名は完全修飾名である必要があります（たとえば、**administrator** ではなく **administrator@mydomain.com** を使用します）。

ベース DN（Base DN）

Firepower Management Center がユーザ データの検索を開始するサーバのディレクトリ ツリー。

通常、ベース識別名（DN）には企業ドメイン名および部門を示す基本構造があります。たとえば、Example 社のセキュリティ部門のベース DN は、**ou=security,dc=example,dc=com** となります。

Group DN

Firepower Management Centerがグループ属性を持つユーザを検索するサーバのディレクトリ ツリー。サポートされているグループ属性の一覧については、サポートされているサーバ オブジェクト クラスと属性名 （2575 ページ）を参照してください。

（注） グループ名または組織単位名には、アスタリスク（*）、イコール（=）、バックスラッシュ（\）などの特殊文字は使用できません。使用した場合、それらのグループのユーザはダウンロードされず、アイデンティティ ポリシーで使用できないためです。

グループ属性（Group Attribute）

（オプション）サーバのグループ属性：メンバー、または一意のメンバー。

タイプ（Type）

レルムのタイプで、Microsoft Active Directory 用の **AD** またはその他のサポートされている LDAP リポジトリ用の **LDAP** です。サポートされている LDAP リポジトリの一覧については、レルムがサポートされているサーバ （2573 ページ）を参照してください。

（注） キャプティブ ポータルのみ、LDAP レルムをサポートします。

既存のレルムを編集する場合、次のフィールドを使用できます。

[ユーザ セッション タイムアウト（User Session Timeout）]

ユーザセッションがタイムアウトするまでの分数を入力します。デフォルトは、ユーザのログイン イベントから 1440 分（24 時間）後です。このタイムアウトを過ぎると、ユーザのセッションは終了します。ユーザが再度ログインせずにネットワークにアクセスし続けている場合、ユーザは Firepower Management Center により不明として認識されます（[失敗したキャプティブポータルユーザ（Failed Captive Portal Users）] を除く）。

次のタイムアウト値を設定できます。

- [ユーザエージェントおよびISE/ISE-PICユーザ（User Agent and ISE/ISE-PIC Users）]：パッシブ認証タイプであるユーザ エージェントまたは ISE/ISE-PIC によってトラッキングされるユーザのタイムアウト。詳細については、ISE/ISE-PIC アイデンティティ ソース （2593 ページ）を参照してください。

- [TSエージェントユーザ（TS Agent Users）]：パッシブ認証タイプである TS エージェントによってトラッキングされるユーザのタイムアウト。詳細については、ターミナル サービス（TS）エージェントのアイデンティティ ソース（2629ページ）を参照してください。
- [キャプティブポータルユーザ（Captive Portal Users）]：アクティブ認証タイプであるキャプティブ ポータルを使用して正常にログインしたユーザのタイムアウト。詳細については、キャプティブ ポータルのアイデンティティ ソース（2607ページ）を参照してください。
- [失敗したキャプティブポータルユーザ（Failed Captive Portal Users）]：キャプティブ ポータルを使用して正常にログインしていないユーザのタイムアウト。Firepower Management Center によってユーザが認証失敗ユーザとして認識されるまでの、[最大ログイン試行回数（Maximum login attempts）] を設定できます。アクセス コントロール ポリシーを使用して、認証失敗ユーザにネットワークへのアクセス権を付与することもできます。この場合は、そのユーザにこのタイムアウト値が適用されます。

  失敗したキャプティブ ポータル ログインの詳細については、キャプティブ ポータル フィールド（2618 ページ）を参照してください。
- [ゲストキャプティブポータルユーザ（Guest Captive Portal Users）]：キャプティブ ポータルにゲスト ユーザとしてログインしているユーザのタイムアウト。詳細については、キャプティブ ポータルのアイデンティティ ソース（2607ページ）を参照してください。

レルムのディレクトリ フィールド（Realm Directory Fields）

これらの設定は、レルム内の個々のサーバ（Active Directory ドメイン コントローラなど）に適用されます。

暗号化（Encryption）

Firepower Management Center サーバ接続に使用する暗号化方式。

- **STARTTLS**：暗号化 LDAP 接続
- **LDAPS**：暗号化 LDAP 接続
- **なし**：非暗号化 LDAP 接続（保護されていないトラフィック）

ホスト名/IP アドレス（Hostname/IP Address）

Active Directory ドメイン コントローラのホスト名または IP アドレス。[暗号化（Encryption）] 方式を指定する場合は、このフィールドでホスト名を指定します。

[ポート（Port）]

Firepower Management Center コントローラ接続に使用するポート。

SSL 証明書（SSL Certificate）

サーバへの認証に使用する SSL 証明書。SSL 証明書を使用するにために、STARTTLS または LDAPS を [暗号化（Encryption）] タイプとして設定できます。

認証に証明書を使用する場合、証明書のサーバ名は、サーバの [Hostname/IP Address] と一致する必要があります。たとえば、IP アドレスとして 10.10.10.250 を使用しているのに、証明書で **computer1.example.com** を使用している場合は、接続が失敗します。

ユーザのダウンロード フィールド

[使用可能なグループ（Available Groups）]、[含むに追加する（Add to Include）]、[除外するに追加する（Add to Exclude）]

ダウンロードしてユーザ認識やユーザ制御に使用できるようにするグループを特定します。

- [使用可能グループ ボックス（Available Groups）] にグループが残っている場合、グループのダウンロードは行われません。
- グループを [含むに追加する（Add to Include）] ボックスに移動させた場合、そのグループはダウンロードされ、ユーザ データはユーザ認識やユーザ制御に利用できます。
- グループを [除外するに追加する（Add to Exclude）] ボックスに追加すると、グループ名のみがダウンロードされます。グループ内のユーザはダウンロードされません。
- 含まれないグループのユーザを含めるには、[含めるグループ（Groups to Include）] の下のフィールドにそのユーザ名を入力し、[追加（Add）] をクリックします。
- 除外されないグループのユーザを除外するには、[除外するグループ（Groups to Exclude）] の下のフィールドにそのユーザ名を入力し、[追加（Add）] をクリックします。

（注） Firepower Management Center にダウンロードされるユーザは、数式 **R = I - (E+e) + i** を使用して計算されます。

- R はダウンロードしたユーザのリストです。
- I は含まれているグループです。
- E は除外されているグループです。
- e は除外されているユーザです。
- i は含まれているユーザです。

自動ダウンロードの開始、繰り返し設定（Begin automatic download at, Repeat every）

自動ダウンロードの回数を指定します。

ユーザおよびグループのダウンロード（ユーザアクセス制御に必須）

ユーザ認識用およびユーザ制御用にユーザとグループをダウンロードできるようになります。

レルム ディレクトリの設定

この手順では、LDAP サーバまたは Microsoft Active Directory ドメイン コントローラに対応するレルムディレクトリを作成できます。それぞれ異なるユーザやグループを認証する複数のドメイン コントローラを、1 つの Active Directory サーバに設定することができます。

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	Control	いずれか（Any）	いずれか（Any）	Administrator、Access Admin、Network Admin

レルムディレクトリの設定フィールドに関する詳細については、レルム フィールド（2577ページ）を参照してください。

始める前に

オプションで SSL 証明書を使用してディレクトリで認証するには、Firepower Management Center のアクセス元となるマシンでPKI オブジェクトするか、証明書データとキーを利用可能にします。

ステップ 1 まだ実行していない場合は、Firepower Management Center にログインし、[統合（Integration）] > [レルム（Realms）] をクリックします。

ステップ 2 [レルム（Realms）] タブ ページで、ディレクトリの設定対象となるレルムの名前をクリックします。

ステップ 3 [ディレクトリ（Directory）] タブページで、[ディレクトリの追加（Add Directory）] をクリックします。

ステップ 4 LDAP サーバまたは Active Directory ドメイン コントローラの [ホスト名/IPアドレス（Hostname / IP Address）] と [ポート（Port）] を入力します。
システムにより、指定したホスト名または IP アドレスに LDAP クエリが送信されます。ホスト名が LDAP サーバまたは Active Directory ドメイン コントローラの IP アドレスに解決される場合は、[テスト（Test）] が成功します。

ステップ 5 [暗号化モード（Encryption Mode）] を選択します。

ステップ 6 （オプション）リストから [SSL 証明書（SSL Certificate）] を 1 つ選択するか、追加アイコン（  ）をクリックして証明書を追加します。

ステップ 7 接続をテストするには、[テスト（Test）] をクリックします。

ステップ 8 [OK] をクリックします。

ステップ 9 [保存（Save）] をクリックします。[レルム（Realms）] タブ ページに戻ります。

ステップ 10 レルムをまだ有効にしていない場合は、[レルム（Realms）] タブ ページで、[状態（State）] を有効にします。

次のタスク

- ユーザとグループのダウンロード （2583 ページ）。

ユーザとグループのダウンロード

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	Control	いずれか（Any）	いずれか（Any）	Administrator、Access Admin、Network Admin

このセクションでは、Active Directory サーバから Firepower Management Center にユーザとグループをダウンロードする方法について説明します。含めるグループを指定しなかった場合、システムは指定されたパラメータと一致するすべてのグループのユーザデータを取得します。パフォーマンス上の理由から、アクセス コントロールに使用するユーザを表すグループだけを明示的に含めることをお勧めします。

Firepower Management Center がサーバから取得可能なユーザの最大数は Firepower Management Center モデルによって異なります。レルムのダウンロードパラメータの範囲が広すぎる場合、Firepower Management Center はできるだけ多くのユーザに関する情報を取得し、取得できなかったユーザ数を Message Center の [タスク（Task）] タブで報告します。

（注） Firepower Management Center では、Unicode 文字を含むユーザ名は表示されません。ユーザやグループをダウンロードする前に、Unicode 文字を英数字に置き換えてください。

レルム設定フィールドの詳細については、レルム フィールド （2577 ページ）を参照してください。

ステップ 1 Firepower Management Center にログインします。

ステップ 2 [システム（System）] > [統合（Integration）] > [レルム（Realms）] をクリックします。

ステップ 3 ユーザとグループを手動でダウンロードするには、ユーザやユーザ グループをダウンロードするレルムの横にあるダウンロードアイコン（）をクリックします。コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。残りの手順をスキップできます。

ステップ 4 自動でユーザとグループをダウンロードするようにレルムを設定するには、自動でユーザやグループをダウンロードするように設定するレルムの横にある編集アイコン（）をクリックします。

ステップ 5 [ユーザアクセス制御（User Access Control）] タブ ページで、[（ユーザアクセス制御に必要な）ユーザとグループをダウンロードする（Download users and groups (required for user access control)）] をオンにします。

ステップ 6 一覧から [自動ダウンロードの開始時間（Begin automatic download at）] の時間を選択します。

ステップ 7 [繰り返し設定（Repeat Every）] 一覧からダウンロード間隔を選択します。

ステップ 8 ダウンロードにユーザ グループを含めるか除外するには、[選択可能なグループ（Available Groups）] 列からユーザ グループを選択し、[含めるに追加（Add to Include）] または [除外に追加（Add to Exclude）] をクリックします。

複数のユーザはカンマで区切ります。このフィールドでは、アスタリスク（*）をワイルドカード文字として使用できます。

（注） そのグループのユーザに対してユーザ制御を実行する場合は、[含めるに追加（Add to Include）] をクリックする必要があります。

次の注意事項に従ってください。

- [使用可能グループ ボックス（Available Groups）] にグループが残っている場合、グループのダウンロードは行われません。
- グループを [含むに追加する（Add to Include）] ボックスに移動させた場合、そのグループはダウンロードされ、ユーザ データはユーザ認識やユーザ制御に利用できます。
- [除外に追加する（Add to Exclude）] ボックスにグループを移動させると、グループがダウンロードされ、ユーザ データはユーザ認識に利用できますが、ユーザ制御には利用できません。
- 含まれないグループのユーザを含めるには、[含めるグループ（Groups to Include）] の下のフィールドにそのユーザ名を入力し、[追加（Add）] をクリックします。
- 除外されないグループのユーザを除外するには、[除外するグループ（Groups to Exclude）] の下のフィールドにそのユーザ名を入力し、[追加（Add）] をクリックします。

レルムの管理

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	Control	いずれか（Any）	いずれか（Any）	Administrator、Access Admin、Network Admin

このセクションでは、[レルム（Realms）] ページ上のコントロールを使用して、レルムに関するさまざまなメンテナンス タスクを実行する方法について説明します。次の点に注意してください。

- コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。
- 代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 1 Firepower Management Center にログインします。
ステップ 2 **[System]** > **[Integration]** をクリックします。
ステップ 3 [レルム（Realms）] をクリックします。
ステップ 4 レルムを削除するには、削除アイコン（）をクリックします。
ステップ 5 レルムを編集するには、レルムの横にある編集アイコン（）をクリックし、レルムの作成（2576ページ）の説明に従って変更を行います。
ステップ 6 レルムを有効にするには、[状態（State）] を右にスライドします。レルムを無効にするには、左にスライドします。
ステップ 7 ユーザおよびユーザ グループをダウンロードするには、ダウンロードアイコン（）をクリックします。
ステップ 8 レルムをコピーするには、コピー アイコン（）をクリックします。
ステップ 9 レルムを比較する方法については、レルムの比較 （2585 ページ）を参照してください。

レルムの比較

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	Control	いずれか（Any）	いずれか（Any）	Administrator、Security Approver、Access Admin、Network Admin

ステップ 1 Firepower Management Center にログインします。
ステップ 2 **[System]** > **[Integration]** をクリックします。
ステップ 3 [レルム（Realms）] をクリックします。
ステップ 4 **[System]** > **[Integration]** をクリックします。
ステップ 5 [レルム（Realms）] をクリックします。
ステップ 6 [レルムの比較（Compare Realms）] をクリックします。
ステップ 7 [比較対象（Compare Against）] リストから [レルムの比較（Compare Realm）] を選択します。
ステップ 8 [レルム A（Realm A）] および [レルム B（Realm B）] リストから比較するレルムを選択します。

ステップ 9 [OK] をクリック

ステップ 10 個々の変更を選択するには、タイトル バーの上の [前へ（Previous）] または [次へ（Next）] をクリックします。

ステップ 11 （オプション）[比較レポート（Comparison Report）] をクリックして、レルム比較レポートを生成します。

ステップ 12 （オプション）[新しい比較（New Comparison）] をクリックして、新しいレルム比較ビューを生成します。

レルムとユーザのダウンロードのトラブルシュート

予期しないサーバ接続の動作に気付いたら、レルム設定、デバイス設定、またはサーバ設定の調整を検討してください。関連の他のトラブルシューティングについては、次を参照してください。

- ユーザ エージェント アイデンティティ ソースのトラブルシューティング （2634 ページ）
- ISE/ISE-PIC アイデンティティ ソースのトラブルシューティング （2604 ページ）
- TS エージェント アイデンティティ ソースのトラブルシューティング （2631 ページ）
- キャプティブ ポータルのアイデンティティ ソースのトラブルシューティング （2620 ページ）
- リモート アクセス VPN アイデンティティ ソースのトラブルシューティング （2626ページ）
- ユーザ制御のトラブルシューティング （494 ページ）

症状：レルムとグループは報告されますが、ダウンロードされません

Firepower Management Center のヘルス モニタは、次のように定義されたユーザまたはレルムの不一致を通知します。

- [ユーザの不一致（User mismatch）]：ユーザはダウンロードされることなく Firepower Management Center に報告されます。

  ユーザの不一致の一般的な理由は、ユーザが Firepower Management Center へのダウンロードから除外したグループに所属していることです。レルム フィールド （2577ページ）で検討した情報を確認してください。

- [レルムの不一致（Realm mismatch）]：Firepower Management Center に通知されていないレルムに対応するドメインにユーザがログインしています。

たとえば、Firepower Management Center で **domain.example.com** というドメインに対応するレルムを定義していても、**another-domain.example.com** というドメインからログインが報告される場合にレルムの不一致となります。このドメイン内のユーザは Firepower Management Center によって不明（Unknown）と識別されます。

不一致のしきい値をヘルス警告がトリガーされる値を上回るパーセンテージとして設定します。次に例を示します。

- デフォルトの不一致しきい値に 50% を使用しており、8 つの着信セッションに 2 つの不一致レルムがある場合、不一致のパーセンテージは 25% であり、警告はトリガーされません。
- 不一致のしきい値を 30% に設定し、5 つの着信セッションに 3 つの不一致レルムがある場合は、不一致のパーセンテージは 60% となり、警告がトリガーされます。

アイデンティティ ルールに一致しない不明なユーザに、適用されているポリシーがありません。（不明ユーザに対してアイデンティティ ルールをセットアップすることはできますが、ユーザとレルムを正確に識別することによってルールの数を最小限に保つことをお勧めします。）

詳細については、レルムまたはユーザの不一致の検出 （2590 ページ）を参照してください。

症状：アクセス コントロール ポリシーがグループのメンバーシップと一致しない

この解決策は、他の AD ドメインとの信頼関係にある AD ドメインに適用されます。以下の説明で、外部ドメイン ドメインは、ユーザがログインするドメイン以外のドメインを指します。

ユーザが信頼されている外部ドメインで定義されたグループに属している場合、Firepower は外部ドメインのメンバーシップを追跡しません。たとえば、次のシナリオを考えてください。

- ドメイン コントローラ 1 と 2 は相互に信頼している
- グループ A はドメイン コントローラ 2 で定義されている
- コントローラ 1 のユーザ `mparvinder` はグループ A のメンバーである

ユーザ `mparvinder` はグループ A に属しているが、メンバーシップ グループ A を指定する Firepower のアクセス コントロール ポリシー ルールが一致しません。

解決策：グループ A に属する、すべてのドメイン 1 のアカウントを含むドメイン コントローラ 1 に同様のグループを作成します。グループ A またはグループ B のすべてのメンバーに一致するように、アクセス コントロール ポリシー ルールを変更します。

症状：アクセス コントロール ポリシーが子ドメインのメンバーシップと一致しない

ユーザが親ドメインの子であるドメインに属している場合、Firepower はドメイン間の親/子関係を追跡しません。たとえば、次のシナリオを考えてください。

- ドメイン `child.parent.com` はドメイン `parent.com` の子である
- ユーザ `mparvinder` は `child.parent.com` で定義されている

ユーザ `mparvinder` が子ドメインに属しているが、`parent.com` と一致する Firepower アクセス コントロール ポリシーが `child.parent.com` ドメインの `mparvinder` と一致しません。

解決策：`parent.com` または `child.parent.com` のいずれかのメンバーシップに一致するようにアクセス コントロール ポリシー ルールを変更します。

症状：レルムまたはレルム ディレクトリのテストが失敗する

ディレクトリ ページの [テスト（Test）] ボタンは、入力したホスト名または IP アドレスに LDAP クエリを送信します。失敗した場合は、次を確認してください。

- 入力した [ホスト名（Hostname）] が、LDAP サーバまたは Active Directory ドメイン コントローラの IP アドレスに解決される。
- 入力した [IPアドレス（IP Address）] が有効である。

レルム設定ページの [AD参加のテスト（Test AD Join）] ボタンは、次のことを確認します。

- DNS が、[ADプライマリドメイン（AD Primary Domain）] を LDAP サーバまたは Active Directory ドメイン コントローラの IP アドレスに解決される。
- [AD参加ユーザ名（AD Join Username）] と [AD参加パスワード（AD Join Password）] が正しい。

  [AD参加ユーザ名（AD Join Username）] は完全修飾名である必要があります（たとえば、**`administrator`** ではなく **`administrator@mydomain.com`** を使用します）。
- ドメイン内にコンピュータを作成し、ドメインに Firepower Management Center をドメイン コンピュータとして参加させるための十分な権限がユーザにある。

症状：予期しない時間にユーザ タイムアウトが発生する

予期しない間隔でユーザ タイムアウトが実行されていることに気付いたら、ユーザ エージェント、ISE/ISE-PIC、TS エージェント サーバの時間が Firepower Management Centerの時間と同期されていることを確認します。アプライアンスが同期されていないと、予想外の間隔でユーザのタイムアウトが実行される可能性があります。

症状：レルム設定で指定したようにユーザが含まれない、または除外されない

サーバのサブグループのメンバーであるユーザを選別できる Active Directory レルムを設定する際は、Microsoft Windows サーバが報告するユーザの数を以下に制限することに注意します。

- Windows サーバ 2008 または 2012 では、グループごとに 5000 ユーザまで。Windows Server 2008 上の Oracle Directory Server Enterprise Edition 7.0

必要に応じて、より多くのユーザをサポートするため、このデフォルトの制限を引き上げるようサーバの設定を変更できます。

症状：ユーザがダウンロードされない

考えられる原因は次のとおりです。

- レルムの [タイプ（Type）] が正しく設定されていない場合は、FirePOWER システムにより必要とされる属性とリポジトリにより提供される属性が一致しないため、ユーザとグ

ループをダウンロードできません。たとえば、Microsoft Active Directory レルムの [タイプ（Type）] を [LDAP] として設定すると、FirePOWER システムでは `uid` 属性が必要になり、この属性は Active Directory では `none` に設定されています。（Active Directory リポジトリでは、ユーザ ID に `sAMAccountName` が使用されます。）

ソリューション：レルムの [タイプ（Type）] フィールドを適切に設定します。Microsoft Active Directory の場合は [AD] に設定し、サポートされている別の LDAP リポジトリの場合は [LDAP] に設定します。

- グループ名または組織単位名に特殊文字が使用されている Active Directory グループのユーザは、アイデンティティ ポリシー ルールで使用できない可能性があります。たとえば、グループ名または組織単位名にアスタリスク（*）、イコール（=）、バックスラッシュ（\）などの特殊文字が含まれている場合、これらのグループ内のユーザはダウンロードされず、アイデンティティ ポリシーで使用できません。

  解決策：グループ名または組織単位名から特殊文字を削除します。

症状：未知の ISE とユーザ エージェントのユーザのユーザ データが Web インターフェイスで表示されない

システムはデータがまだデータベースにない ISE/ISE-PIC、ユーザエージェントまたは TS エージェントユーザのアクティビティを検出すると、サーバからそれらに関する情報を取得します。状況によっては、システムが Microsoft Windows サーバからこの情報を正常に取得するためにさらに時間がかかることもあります。データ取得が成功するまで、ISE/ISE-PIC、ユーザエージェント、TS エージェントユーザから見えるアクティビティは Web インターフェイスに表示されません。

これにより、アクセス制御ルールを使ったユーザトラフィックの処理も妨げられることがある点に注意します。

症状：イベントのユーザ データが想定外の内容になる

ユーザやユーザアクティビティイベントに想定外の IP アドレスが含まれる場合は、レルムを確認します。複数のレルムに同一の [AD プライマリ ドメイン（AD Primary Domain）] の値を設定することはできません。

症状：ターミナル サーバからログインしたユーザが、システムによって一意に識別されない

導入されている構成にターミナルサーバが含まれ、これに接続されている 1 つまたは複数のサーバにレルムが設定されている場合は、ターミナルサーバ環境でのユーザログインを正確に報告するため Cisco Terminal Services（TS）エージェントを設定する必要があります。TS エージェントをインストールし、設定すると、このエージェントは各ユーザに別個のポートを割り当て、Firepower System はこれらのユーザを Web インターフェイスで一意に識別できるようになります。

TS エージェントの詳細については、『*Cisco Terminal Services (TS) Agent Guide*』を参照してください。

レルムまたはユーザの不一致の検出

この項では、レルムまたはユーザの不一致を検出する方法について説明します。これらは次のように定義されています。

- [ユーザの不一致（User mismatch）]：ユーザはダウンロードされることなく Firepower Management Center に報告されます。

  ユーザの不一致の一般的な理由は、ユーザが Firepower Management Center へのダウンロードから除外したグループに所属していることです。レルム フィールド（2577ページ）で検討した情報を確認してください。

- [レルムの不一致（Realm mismatch）]：Firepower Management Center に通知されていないレルムに対応するドメインにユーザがログインしています。

詳細については、レルムとユーザのダウンロードのトラブルシュート（2586ページ）を参照してください。

アイデンティティ ルールに一致しない不明なユーザに、適用されているポリシーがありません。（不明ユーザに対してアイデンティティ ルールをセットアップすることはできますが、ユーザとレルムを正確に識別することによってルールの数を最小限に保つことをお勧めします。）

ステップ 1 レルムまたはユーザの不一致の検出を有効にします。

a) まだ Firepower Management Center にログインしていない場合は、ログインします。
b) **[システム（System）] > [ヘルス（Health）] > [ポリシー（Policy）]** をクリックします。
c) 新しいヘルス ポリシーを作成するか、または既存のポリシーを編集します。
d) [ポリシーの編集（Editing Policy）] ページで、[ポリシーのランタイム間隔（Policy Runtime Interval）] を設定します。
これは、すべてのヘルス モニタ タスクが実行される頻度です。
e) 左側のペインで、[レルム（Realm）] をクリックします。
f) 次の情報を入力します。

- [有効（Enabled）]：[オン（On）] をクリックします
- [一致しきい値（%）のユーザへの警告（Warning Users match threshold %）]：ヘルス モニタで警告をトリガーしたレルム不一致またはユーザ不一致のいずれかのパーセンテージ。詳細については、レルムとユーザのダウンロードのトラブルシュート（2586 ページ）を参照してください。

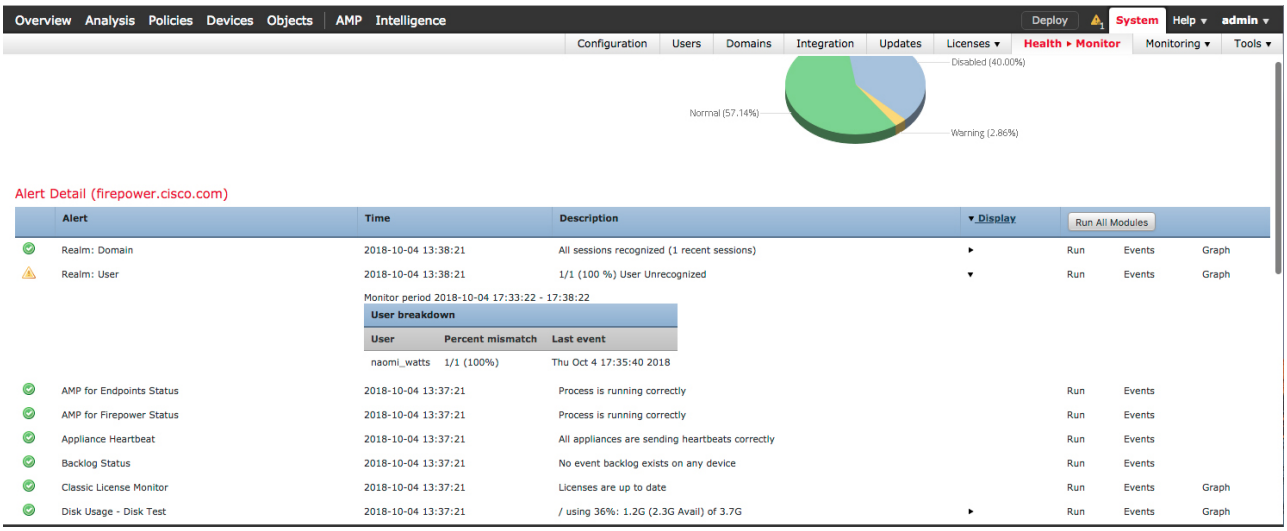
g) ページの下部で [ポリシーを保存して終了（Save Policy & Exit）] をクリックします。
h) 正常性ポリシーの適用（363 ページ） の説明に従って、管理対象デバイスにヘルス ポリシーを適用します。

ステップ 2 次の方法のいずれかでユーザとレルムの不一致を表示します。

- 警告しきい値を超過した場合は（  ）をクリックし、Firepower Management Center の上部のナビゲーションで [ヘルス（Health）] をクリックします。これにより、ヘルス モニタが開きます。

- **[システム（System）] > [ヘルス（Health）] > [モニタ（Monitor）]** をクリックします。

ステップ 3 [ヘルス モニタ（Health Monitor）] ページの [表示（Display）] 列で、[レルム：ドメイン（Realm: Domain）] または [レルム：ユーザ（Realm: User）] を展開し、不一致に関する詳細を表示します。
次に、100% のユーザ不一致の例を示します。この例では、Firepower Management Center で **naomi_watts** は検出されているものの、ダウンロードされていませんでした。



関連トピック

正常性ポリシー （361 ページ）
ヘルス モニタリングの設定 （361 ページ）
ヘルス モニタ ステータスのカテゴリ （372 ページ）

第 101 章

ISE/ISE-PIC によるユーザの制御

次のトピックでは、ISE/ISE-PIC によりユーザ認識とユーザ制御を実行する方法について説明します。

ISE/ISE-PIC アイデンティティ ソース

Cisco Identity Services Engine（ISE）または ISE Passive Identity Connector（ISE-PIC）の展開を Firepower システムと統合して、ISE/ISE-PIC をパッシブ認証に使用できます。

ISE/ISE-PIC は、信頼できるアイデンティティ ソースで、Active Directory（AD）、LDAP、RADIUS、または RSA を使用して認証するユーザに関するユーザ認識データを提供します。さらに、Active Directory ユーザのユーザ制御を行えます。ISE/ISE-PIC は、ISE ゲスト サービス ユーザの失敗したログイン試行またはアクティビティは報告しません。

（注） Firepower システムは IEEE 802.1x マシン認証を解析しませんが、802.1x ユーザ認証を解析します。ISE で 802.1x を使用している場合は、ユーザ認証を含める必要があります。802.1x マシン認証は、ポリシーで使用できる FMC にユーザ ID を提供しません。

Cisco ISE/ISE-PIC の詳細については、*Cisco Identity Services Engine Administrator Guide* および『*Identity Services Engine Passive Identity Connector (ISE-PIC) Installation and Administrator Guide*』を参照してください。

ISE/ISE-PIC のガイドラインと制限事項

Firepower システムで ISE/ISE-PIC を構成する際に、このセクションで説明されているガイドラインを使用してください。

ISE/ISE-PIC バージョンと設定の互換性

ご使用の ISE/ISE-PIC バージョンと設定は、次のように Firepower との統合や相互作用に影響を与えます。

- ISE/ISE-PIC サーバと Firepower Management Center の時刻を同期します。そうしないと、システムが予期しない間隔でユーザのタイムアウトを実行する可能性があります。
- ISE または ISE-PIC データを使用してユーザ制御を実装するには、レルムの作成（2576 ページ） の説明に従って、pxGrid のペルソナを想定して ISE サーバのレルムを設定し有効にします。
- ISE サーバに接続する各 Firepower Management Center ホスト名は一意である必要があります。そうでない場合、Firepower Management Center のいずれかへの接続は廃棄されます。
- ISE のバージョン 2.0 パッチ 4 以降には、IPv6 対応エンドポイントのサポートが含まれています。
- ISE の展開で ISE Endpoint Protection Service（EPS）が有効で設定されている場合は、ISE 接続を使用して、相関ポリシー違反に関与している送信元または宛先ホストに対する ISE EPS 修復を実行できます。
- ユーザの EPSStatus が変更された後でユーザの SGT を更新するように ISE の展開を設定した場合は、ISE EPS 修復により、Firepower Management Center 上の SGT も更新されます。
- ISE-PIC は、ISE 属性データを提供しないか、または ISE EPS の修復をサポートしません。

システムのこのバージョンと互換性がある特定のバージョンの ISE/ISE-PIC については、『*Cisco Firepower Compatibility Guide*』を参照してください。

ISE でのクライアントの認証

ISE サーバと Firepower Management Center の間の接続が成功するには、ISE でクライアントを手動で承認する必要があります。（通常、接続テスト用と ISE エージェント用の 2 つのクライアントがあります）。

『*Cisco Identity Services Engine Administrator Guide*』の「Managing users and external identity sources」の章で説明しているように、ISE で [新しいアカウントを自動的に承認（Automatically approve new accounts）] を有効にすることもできます。

セキュリティ グループ タグ（SGT）

セキュリティ グループ タグ（SGT）は、信頼ネットワーク内のトラフィックの送信元の権限を指定します。Cisco ISE および Cisco TrustSec は、ネットワークに入るときに、セキュリティ グループ アクセス（SGA）と呼ばれる機能を使用して、パケットに SGT 属性を適用します。これらの SGT は、ISE または TrustSec 内のユーザの割り当てられたセキュリティ グループに対応します。ID ソースとして ISE を設定すると、Firepower システムは、これらの SGT を使用してトラフィックをフィルタリングできます。

（注） ISE SGT 属性タグのみを使用してユーザ制御を実装する場合、ISE サーバのレルムを設定する必要はありません。ISE SGT 属性条件は、関連するアイデンティティ ポリシーの有無にかかわらずポリシーで設定できます。詳細については、ISE 属性条件の設定 （493 ページ）を参照してください。

（注） 一部のルールでは、カスタム SGT 条件が ISE によって割り当てられなかった SGT 属性にタグ付けされたトラフィックを照合できます。これはユーザ制御とみなされず、アイデンティティ ソースとして ISE/ISE-PIC を使用しない場合にのみ機能します。カスタム SGT 条件 （495 ページ） を参照してください。

ISE と高可用性

プライマリ Firepower Management Center が失敗すると、次の処理が行われます。

- スタンバイがプライマリに昇格するまで、セカンダリ Firepower Management Center ユーザ データベースは読み取り専用になります。

  リポジトリに追加されたユーザ（Active Directory など）は Firepower Management Center にダウンロードされず、それらのユーザは [不明（Unknown）] と識別されます。

  新しい SGT は使用されません。

- スタンバイがプライマリに昇格すると、すべての動作が正常に戻ります。つまり、ユーザがダウンロードされ、SGT が使用され、可能な場合はユーザが識別されます。

ISE プライマリ サーバが失敗した場合は、セカンダリをプライマリに手動で昇格させる必要があります。自動でフェール オーバーすることはありません。

エンドポイント ロケーション（Endpoint Location）（またはロケーション IP（Location IP））

[エンドポイント ロケーション（Endpoint Location）] 属性は、ISE によって識別される、ユーザの認証に ISE を使用したネットワーク デバイスの IP アドレスです。

[エンドポイント ロケーション（Endpoint Location）]（[ロケーション IP（Location IP）]）に基づいてトラフィックを制御するには、アイデンティティ ポリシーを設定し、展開する必要があります。

ISE 属性

ISE 接続を設定すると、ISE 属性データが Firepower Management Center データベースに入力されます。ユーザ認識とユーザ制御に使用できる ISE 属性は、次のとおりです。 これは、ISE-PIC ではサポートされません。

エンドポイント プロファイル（Endpoint Profile）（またはデバイス タイプ（Device Type））

[エンドポイント プロファイル（Endpoint Profile）] 属性は、ISE によって識別されるユーザのエンドポイント デバイス タイプです。

[エンドポイント プロファイル（Endpoint Profile）]（[デバイス タイプ（Device Type）]）に基づいてトラフィックを制御するには、アイデンティティ ポリシーを設定し、展開する必要があります。

ユーザ制御用 ISE/ISE-PIC の設定方法

ISE/ISE-PIC は、次の設定のいずれかで使用できます。

- レルム、アイデンティティ ポリシー、および関連付けられたアクセス コントロール ポリシーを使用。

  レルムを使用して、ポリシー内のネットワーク リソースへのユーザ アクセスを制御します。ポリシーでは、ISE/ISE-PIC セキュリティ グループ タグ（SGT）のメタデータを引き続き使用できます。

- アクセス コントロール ポリシーのみを使用。レルムまたはアイデンティティ ポリシーは必要ありません。

  SGT メタデータのみを使用してネットワーク アクセスを制御するには、この方法を使用します。

関連トピック

レルムなしで ISE を設定する方法 （2596 ページ）
レルムを使用したユーザ制御用 ISE/ISE-PIC の設定方法 （2597 ページ）

レルムなしで ISE を設定する方法

このトピックでは、SGT タグを使用してネットワークへのアクセスを許可またはブロックできるように ISE を設定するために必要なタスクの概要について説明します。

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	Control	任意（NGIPSv を除く）	任意（Any）	Administrator/Access Admin/Network Admin

手順

	コマンドまたはアクション	目的
ステップ 1	ISE/ISE-PIC からシステム証明書をエクスポートします。	証明書は、ISE/ISE-PIC pxGrid、モニタリング（MNT）サーバ、および FMC の間で安全に接続するために必要です。FMC で使用するための ISE/ISE-PIC サーバからの証明書のエクスポート （2599 ページ）を参照してください
ステップ 2	ISE/ISE-PIC アイデンティティ ソースを作成します。	ISE/ISE-PIC アイデンティティ ソースを使用すると、ISE/ISE-PIC によって提供されるセキュリティ グループ タグ（SGT）を使用してユーザ アクティビティを制御できます。ユーザ制御用 ISE/ISE-PIC の設定 （2601 ページ）を参照してください。
ステップ 3	アクセス コントロール ルールを作成します。	アクセス コントロール ルールは、トラフィックがルール基準に一致する場合に実行するアクション（許可またはブロックなど）を指定します。アクセス コントロール ルール内の一致基準として、送信元の SGT メタデータを使用できます。アクセス コントロール ルールの概要 （1689 ページ）を参照してください。
ステップ 4	管理対象デバイスにアクセス コントロール ポリシーを展開します。	ポリシーを有効にするには、事前に管理対象デバイスに展開しておく必要があります。設定変更の展開 （447 ページ）を参照してください。

次のタスク

FMC で使用するための ISE/ISE-PIC サーバからの証明書のエクスポート （2599 ページ）

レルムを使用したユーザ制御用 ISE/ISE-PIC の設定方法

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	Control	任意（NGIPSv を除く）	任意（Any）	Administrator/Access Admin/Network Admin

始める前に

このトピックでは、ユーザ制御用 ISE/ISE-PIC を設定し、ユーザまたはグループによるネットワークへのアクセスを許可またはブロックできるようにするために必要なタスクの概要について説明します。ユーザおよびグループは、レルムがサポートされているサーバ （2573 ページ）に記載されている任意のサーバに保存できます。

手順

	コマンドまたはアクション	目的
ステップ 1	ISE/ISE-PIC からシステム証明書をエクスポートします。	証明書は、ISE/ISE-PIC pxGrid、モニタリング（MNT）サーバ、および FMC の間で安全に接続するために必要です。FMC で使用するための ISE/ISE-PIC サーバからの証明書のエクスポート （2599 ページ）を参照してください
ステップ 2	レルムを作成します。	レルムの作成は、選択したユーザおよびグループによるネットワークへのアクセスを制御するためにのみ必要です。 レルムの作成 （2576 ページ）を参照してください。
ステップ 3	ユーザおよびグループをダウンロードし、レルムを有効にします。	ユーザおよびグループをダウンロードすると、それらをアクセス コントロール ルールで使用できるようになります。ユーザとグループのダウンロード （2583 ページ）を参照してください。
ステップ 4	ISE/ISE-PIC アイデンティティ ソースを作成します。	ISE/ISE-PIC アイデンティティ ソースを使用すると、ISE/ISE-PIC によって提供されるセキュリティ グループ タグ（SGT）を使用してユーザ アクティビティを制御できます。ユーザ制御用 ISE/ISE-PIC の設定 （2601 ページ）を参照してください。
ステップ 5	アイデンティティ ポリシーを作成します。	アイデンティティ ポリシーは、1 つ以上のアイデンティティ ルールのコンテナです。アイデンティティ ポリシーの作成（2643 ページ）を参照してください。
ステップ 6	アイデンティティ ルールを作成します。	アイデンティティ ルールは、ユーザおよびグループによるネットワークへのアクセスを制御するためにレルムがどのように使用されるかを指定します。アイデンティティ ルールの作成（2638 ページ）を参照してください。
ステップ 7	アクセス コントロール ポリシーとアイデンティティ ポリシーを関連付けます。	これにより、アクセス コントロール ポリシーがレルム内のユーザとグループを使用できるようになります。
ステップ 8	アクセス コントロール ルールを作成します。	アクセス コントロール ルールは、トラフィックがルール基準に一致する場合に実行するアクション（許可またはブロックなど）を指定します。アクセス コントロール ルール内の一致基準として、送信元の SGT メタデータを使用できます。アクセス コントロール ルールの概要（1689 ページ）を参照してください。

	コマンドまたはアクション	目的
ステップ 9	管理対象デバイスにアクセス コントロール ポリシーを展開します。	ポリシーを有効にするには、事前に管理対象デバイスに展開しておく必要があります。設定変更の展開（447 ページ）を参照してください。

次のタスク

FMC で使用するための ISE/ISE-PIC サーバからの証明書のエクスポート （2599 ページ）

ISE/ISE-PIC の設定

次のトピックでは、FMC のアイデンティティ ポリシーで使用するように ISE/ISE-PIC サーバを設定する方法について説明します。

FMC で認証するには、ISE/ISE-PIC サーバから証明書をエクスポートする必要があります。

関連トピック

FMC で使用するための ISE/ISE-PIC サーバからの証明書のエクスポート （2599 ページ）

FMC で使用するための ISE/ISE-PIC サーバからの証明書のエクスポート

ここでは、次のことを行う方法について説明します。

- ISE/ISE-PIC サーバからシステム証明書をエクスポートします。

  これらの証明書は、ISE/ISE-PIC サーバに安全に接続するために必要です。ISE システムの設定に応じ、次のうち 1 つまたは最大 3 つの証明書をエクスポートする必要があります。

  - pxGrid サーバ用の証明書
  - モニタリング（MNT）サーバ用の証明書
  - FMC 用の証明書（秘密キーを含む）

- これらの証明書を FMC にインポートします。

関連トピック

システム証明書のエクスポート （2599 ページ）
ISE/ISE-PIC 証明書のインポート （2600 ページ）

システム証明書のエクスポート

選択したシステム証明書とその証明書に関連付けられている秘密キーをエクスポートできます。証明書とその秘密キーをバックアップ用にエクスポートする場合は、それらを必要に応じて後で再インポートできます。

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 **[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [システム証明書（System Certificates）]** を選択します。

ステップ 2 エクスポートする証明書の横にあるチェックボックスをオンにし、[エクスポート（Export）] をクリックします。

ステップ 3 証明書のみをエクスポートするか、証明書と証明書に関連付けられている秘密キーをエクスポートするかを選択します。

ヒント　値が公開される可能性があるため、証明書に関連付けられている秘密キーのエクスポートは推奨しません。秘密キーをエクスポートする必要がある場合（たとえば、ワイルドカードシステム証明書をエクスポートしてノード間通信用に他のノードにインポートする場合）は、その秘密キーの暗号化パスワードを指定します。このパスワードは、証明書を別の Cisco ISE ノードにインポートするときに指定して、秘密キーを復号化する必要があります。

ステップ 4 秘密キーをエクスポートする場合は、パスワードを入力します。パスワードは、8 文字以上にする必要があります。

ステップ 5 [エクスポート（Export）] をクリックして、クライアント ブラウザを実行しているファイル システムに証明書を保存します。

証明書のみをエクスポートする場合、証明書は Privacy Enhanced Mail 形式で保存されます。証明書と秘密キーの両方をエクスポートする場合、証明書は Privacy Enhanced Mail 形式の証明書と暗号化された秘密キーファイルを含む .zip ファイルとしてエクスポートされます。

ISE/ISE-PIC 証明書のインポート

この手順は任意です。ユーザ制御用 ISE/ISE-PIC の設定 （2601 ページ）で説明されているように、ISE/ISE-PIC アイデンティティソースを作成するときに ISE サーバ証明書をインポートすることもできます。

始める前に

システム証明書のエクスポート （2599 ページ）の説明に従って、ISE/ISE-PIC サーバから証明書をエクスポートします。証明書とキーは、FMC へのログイン元のマシンに存在している必要があります。

次の 2 種類の証明書オブジェクトをインポートします。

- ISE/ISE-PIC で認証するための FMC の内部証明書と秘密キー。
- pxGrid および ISE モニタリング（MNT）サーバ用の 1 つ以上の信頼できる認証局（CA）。

  これは、ISE/ISE-PIC システムのセットアップ方法に応じ、2 つの個別の証明書である場合と 1 つの証明書である場合があります。

ステップ 1 FMC にまだログインしていない場合はログインします。
ステップ 2 **[オブジェクト（Objects）] > [オブジェクト管理（Object Management）]** をクリックします。
ステップ 3 [PKI] を展開します。
ステップ 4 [内部証明書（Internal Cert）] をクリックします。
ステップ 5 [内部証明書の追加（Add Internal Cert）] をクリックします。
ステップ 6 画面の指示に従って、証明書と秘密キーをインポートします。
ステップ 7 [信頼できるCA（Add Trusted CAs）] をクリックします。
ステップ 8 [信頼できるCAの追加（Add Trusted CA）] をクリックします。
ステップ 9 画面の指示に従って、pxGrid サーバ証明書をインポートします。
ステップ 10 必要に応じ、上記の手順を繰り返して MNT サーバの信頼できる CA をインポートします。

次のタスク

ユーザ制御用 ISE/ISE-PIC の設定 （2601 ページ）

ユーザ制御用 ISE/ISE-PIC の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	グローバルだけ	Admin/Access Admin/Network Admin

始める前に

- Microsoft Active Directory サーバまたはサポート対象の LDAP サーバからユーザ セッションを取得するには、レルムの作成 （2576ページ）の説明に従って、pxGridペルソナを想定し、ISE サーバのレルムを設定して有効にします。
- ISE または ISE-PIC への接続を設定します。詳細については、ISE/ISE-PIC アイデンティティ ソース （2593ページ）およびISE/ISE-PIC設定フィールド （2602ページ）を参照してください。
- ISE/ISE-PIC サーバから証明書をエクスポートし、必要に応じて、FMC で使用するための ISE/ISE-PIC サーバからの証明書のエクスポート （2599 ページ）の説明に従って証明書を FMC にインポートします。

ステップ 1 Firepower Management Center にログインします。
ステップ 2 **[System] > [Integration]** をクリックします。

ステップ 3 [アイデンティティの送信元（Identity Sources）] タブをクリックします。

ステップ 4 [サービス タイプ（Service Type）] で [Identity Services Engine] をクリックし、ISE 接続を有効にします。

（注） 接続を無効にするには、[なし（None）] をクリックします。

ステップ 5 [プライマリ ホスト名/IP アドレス（Primary Host Name/IP Address）]、およびオプションで [セカンダリ ホスト名/IP アドレス（Secondary Host Name/IP Address）] を入力します。

ステップ 6 [pxGrid サーバ CA（pxGrid Server CA）] および [MNT サーバ CA（MNT Server CA）] リストから該当する認証局を、[FMC サーバ証明書（FMC Server Certificate）] リストから適切な証明書をそれぞれクリックします。また、追加アイコン（  ）をクリックして証明書を追加することもできます。

（注） [FMC サーバ証明書（FMC Server Certificate）] には、**clientAuth** 拡張キー使用値が含まれている必要があります。そうでない場合、拡張キー使用値は含まれていてはなりません。

ステップ 7 （オプション）CIDR ブロック表記を使用して [ISE ネットワーク フィルタ（ISE Network Filter）] を入力します。

ステップ 8

ステップ 9 接続をテストするには、[テスト（Test）] をクリックします。

テストが失敗した場合、接続障害に関する詳細については、[その他のログ（Additional Logs）] をクリックします。

次のタスク

- アイデンティティ ポリシーの作成 （2643 ページ）の説明に従い、アイデンティティ ポリシーを使用して、制御するユーザおよびその他のオプションを指定します。
- アクセス制御への他のポリシーの関連付け （1684 ページ）の説明に従って、アイデンティティ ルールをアクセス コントロール ポリシーに関連付けます。このポリシーは、トラフィックをフィルタし、オプションで検査します。
- 設定変更の展開 （447 ページ）の説明に従って、使用するアイデンティティ ポリシーとアクセス コントロール ポリシーを管理対象デバイスに展開します。
- ワークフローの使用 （2931 ページ）の説明に従って、ユーザアクティビティをモニタします。

関連トピック

ISE/ISE-PIC アイデンティティ ソースのトラブルシューティング （2604 ページ）
信頼できる認証局オブジェクト （586 ページ）
内部証明書オブジェクト （590 ページ）

ISE/ISE-PIC 設定フィールド

次のフィールドを使用して ISE/ISE-PIC への接続を設定します。

Primary and Secondary Host Name/IP Address

プライマリ（およびオプションでセカンダリ）pxGrid ISE サーバのホスト名または IP アドレス。

指定するホスト名により使用されるポートには、ISE と Firepower Management Center の両方から到達可能である必要があります。

pxGrid Server CA

pxGrid フレームワークの認証局。展開にプライマリとセカンダリの pxGrid ノードがある場合、両方のノードの証明書が同じ認証局によって署名されている必要があります。

MNT Server CA

一括ダウンロード実行時の ISE 証明書の認証局。展開にプライマリとセカンダリの MNT ノードがある場合、両方のノードの証明書が同じ認証局によって署名されている必要があります。

FMC サーバ証明書（FMC Server Certificate）

ISE/ISE-PIC への接続時、または一括ダウンロードの実行時に Firepower Management Center が ISE/ISE-PIC に提供する必要がある証明書およびキー。

（注） [FMC サーバ証明書（FMC Server Certificate）] には、clientAuth 拡張キー使用値が含まれている必要があります。そうでない場合、拡張キー使用値は含まれていてはなりません。

ISE ネットワーク フィルタ（ISE Network Filter）

オプションのフィルタで、ISE が Firepower Management Center にレポートするデータを制限するために設定できます。ネットワーク フィルタを指定する場合、ISE はそのフィルタ内のネットワークからデータをレポートします。次の方法でフィルタを指定できます。

- **任意（Any）**のフィルタを指定する場合はフィールドを空白のままにします。
- CIDR 表記を使用して単一の IPv4 アドレス ブロックを入力します。
- CIDR 表記を使用して IPv4 アドレス ブロックのリストをカンマで区切って入力します。

（注） このバージョンの Firepower システムは、ISE のバージョンに関係なく、IPv6 アドレスを使用したフィルタリングをサポートしません。

関連トピック

信頼できる認証局オブジェクト （586 ページ）
内部証明書オブジェクト （590 ページ）

ISE/ISE-PIC アイデンティティ ソースのトラブルシューティング

関連の他のトラブルシューティングについては、レルムとユーザのダウンロードのトラブルシュート（2586 ページ）およびユーザ制御のトラブルシューティング（494 ページ）を参照してください。

ISE または ISE-PIC 接続に問題が起こった場合は、次のことを確認してください。

- ISE と FirePOWER システムを正常に統合するには、ISE 内の pxGrid アイデンティティ マッピング機能を有効にする必要があります。
- プライマリ サーバが失敗した場合は、セカンダリをプライマリに手動で昇格させる必要があります。自動でフェール オーバーすることはありません。
- ISE サーバと Firepower Management Center の間の接続が成功するには、ISE でクライアントを手動で承認する必要があります。（通常、接続テスト用と ISE エージェント用の 2 つのクライアントがあります）。

  『*Cisco Identity Services Engine Administrator Guide*』の「Managing users and external identity sources」の章で説明しているように、ISE で [新しいアカウントを自動的に承認（Automatically approve new accounts）] を有効にすることもできます。
- [FMC サーバ証明書（FMC Server Certificate）] には、[clientAuth] 拡張キー使用値が含まれている必要があります。そうでない場合、拡張キー使用値は含まれていてはなりません。
- ISE サーバの時刻は、Firepower Management Center の時刻と同期している必要があります。アプライアンスが同期されていないと、予想外の間隔でユーザのタイムアウトが実行される可能性があります。
- 展開にプライマリとセカンダリの pxGrid ノードが含まれている場合は、
  - 両方のノードの証明書が、同じ認証局によって署名される必要があります。
  - ホスト名により使用されるポートが、ISE サーバと Firepower Management Center の両方により到達可能である必要があります。
- 展開にプライマリとセカンダリの MNT ノードがある場合、両方のノードの証明書が同じ認証局によって署名されている必要があります。

ISE または ISE-PIC によって報告されるユーザ データに関する問題が発生した場合は、次の点に注意してください。

- システムはデータがまだデータベースにない ISE ユーザのアクティビティを検出すると、サーバからそれらに関する情報を取得します。ISE ユーザから見えるアクティビティは、システムがユーザのダウンロードで情報の取得に成功するまでアクセス コントロール ルールで処理されず、Web インターフェイスに表示されません。

- LDAP、RADIUS、または RSA ドメイン コントローラで認証された ISE ユーザに対するユーザ制御は実行できません。
- Firepower Management Center は、ISE ゲスト サービス ユーザのユーザ データを受信できません。
- ISE が TS エージェントと同じユーザをモニタした場合、Firepower Management Center は TS エージェントのデータを優先します。TS エージェントと ISE が同じ IP アドレスによる同一のアクティビティを報告した場合は、TS エージェントのデータのみが Firepower Management Center に記録されます。
- 使用する ISE バージョンと設定は、FirePOWER システムでの ISE の使用方法に影響を与えます。詳細については、ISE/ISE-PIC アイデンティティ ソース （2593 ページ）を参照してください。
- Firepower Management Center に高可用性を設定しており、プライマリに障害が発生した場合は、ISE/ISE-PIC のガイドラインと制限事項 （2594 ページ）のISE と高可用性に関する項を参照してください。
- ISE-PIC は ISE 属性のデータを提供しません。
- ISE-PIC は ISE EPS の修復を実行できません。
- アクティブ FTP セッションは、イベントの **Unknown** ユーザとして表示されます。これは正常な処理です。アクティブ FTP では、（クライアントではない）サーバが接続を開始し、FTP サーバには関連付けられているユーザ名がないはずだからです。アクティブ FTP の詳細については、RFC 959 を参照してください。

サポートされている機能に問題がある場合は、ISE/ISE-PIC アイデンティティ ソース （2593 ページ）で詳細を参照してバージョンの互換性を確認してください。

ISE/ISE-PIC の履歴

機能	バージョン	詳細
ISE-PIC との統合	6.2.1	ISE-PIC のデータを使用できるようになりました。
ユーザ制御用の SGT タグ。	6.2.0	ISE セキュリティ グループ タグ（SGT）データに基づいてユーザ制御を実行するために、レルムまたはアイデンティティ ポリシーを作成する必要がなくなりました。

機能	バージョン	詳細
ISE との統合。	6.0	導入された機能。シスコの Platform Exchange Grid（PxGrid）に登録することで、Firepower Management Center で追加のユーザ データ、デバイス タイプデータ、デバイスロケーションデータ、およびセキュリティ グループ タグ（SGT：ネットワーク アクセス コントロールを提供するために ISE によって使用される方式）をダウンロードできます。

第 102 章

キャプティブ ポータルによるユーザの制御

キャプティブ ポータルのアイデンティティ ソース

キャプティブ ポータルは、Firepower システムでサポートされる権限のあるアイデンティティ ソースの 1 つです。これは、ユーザがネットワークに対し、管理対象デバイスを使用して認証を行うアクティブ認証方式です。

通常、キャプティブ ポータルを使用して、インターネットにアクセスするため、または制限されている内部リソースにアクセスするための認証を要求します。必要に応じて、リソースへのゲスト アクセスを設定することができます。システムはキャプティブ ポータル ユーザを認証した後、それらのユーザのトラフィックをアクセス制御ルールに従って処理します。キャプティブ ポータルは、HTTP および HTTPS のトラフィックのみで認証を行います。

（注） キャプティブ ポータルが認証を実行する前に、HTTPS トラフィックを復号化する必要があります。

キャプティブ ポータルはまた、失敗した認証の試行を記録します。失敗した試行によって新しいユーザがデータベース内のユーザのリストに追加されることはありません。キャプティブ ポータルで報告される失敗した認証アクティビティのユーザ アクティビティ タイプは、[Failed Auth User] です。

キャプティブ ポータルから取得された認証データはユーザ認識とユーザ制御に使用できます。

関連トピック

ユーザ制御のためのキャプティブ ポータルの設定方法 （2610 ページ）

キャプティブ ポータルのガイドラインと制約事項

アイデンティティ ポリシーでキャプティブ ポータルを設定して展開すると、指定されたレルムのユーザは以下のデバイスを介して認証を行ってからネットワークにアクセスします。

- 7000 および 8000 シリーズ デバイス上の仮想ルータ
- バージョン 9.5(2) 以降で稼働するルーテッド モードの ASA FirePOWER デバイス
- ルーテッド モードの Firepower Threat Defense デバイス

（注） リモート アクセス VPN ユーザがセキュア ゲートウェイとして機能している管理対象デバイスを介してアクティブに認証されている場合、アイデンティティ ポリシーで設定されている場合でも、キャプティブ ポータルのアクティブ認証は実行されません。

必要なルーテッド インターフェイス

キャプティブ ポータル アクティブ認証を実行できるのは、ルーテッド インターフェイスが設定されているデバイスのみです。キャプティブ ポータルにルールを設定していて、キャプティブ ポータル デバイスにインライン インターフェイスとルーテッド インターフェイスが含まれている場合は、デバイス上のルーテッドインターフェイスのみを対象とするインターフェイス条件を設定する必要があります。

アクセス コントロール ポリシーで参照されているアイデンティティ ポリシーに 1 つ以上のキャプティブ ポータルのアイデンティティ ルールが含まれ、以下を管理する Firepower Management Centerにポリシーを展開する場合、次のようになります。

- ルーテッド インターフェイスが設定されている 1 つ以上のデバイスの場合、ポリシー導入は成功し、ルーテッド インターフェイスがアクティブ認証を実行します。

  システムは ASA with FirePOWER デバイスでインターフェイス タイプを検証しません。ASA with FirePOWER デバイス上でインライン（タップ モード）インターフェイスにキャプティブ ポータル ポリシーを適用すると、ポリシーは正常に展開されますが、これらのルールに一致するトラフィック内のユーザは「不明」と識別されます。

- 1 つ以上の NGIPSv デバイスの場合、ポリシー導入は失敗します。

キャプティブ ポータルとポリシー

アイデンティティ ポリシーのキャプティブ ポータルを設定し、アイデンティティ ルールのアクティブ認証を呼び出します。アイデンティティ ポリシーは、アクセス コントロール ポリシーに関連付けられます。

キャプティブ ポータルのいくつかのアイデンティティ ポリシー設定はアクセス コントロール ポリシーの [アクティブ認証（Active Authentication）] タブページで行い、残りの設定はアクセス コントロール ポリシーに関連付けられたアイデンティティ ルールで行います。

注意 SSL 復号が無効の場合（つまりアクセス コントロール ポリシーに SSL ポリシーが含まれない場合）に、アクティブな最初の認証ルールを追加するか、アクティブな最後の認証ルールを削除すると 設定の変更を展開する際に Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、ターゲットデバイスがトラフィックを処理する方法に応じて異なります。詳細はSnort® の再起動によるトラフィックの動作 （451 ページ）を参照してください。

キャプティブ ポータルの要件と制約事項

以下の要件と制約事項に注意してください。

- システムがサポートするキャプティブ ポータル ログインの数は 1 秒あたり最大 20 です。
- 最大ログイン試行回数のカウントとして数えられるログイン試行の失敗から次の失敗までには最大 5 分という制限があります。5 分という制限の設定は変更できません

  （最大ログイン試行回数は **[分析（Analysis）]** > **[接続（Connections）]** > **[イベント（Events）]** で接続イベントに表示されます）。

  ログイン失敗の間に 5 分以上の間隔がある場合は、ユーザは引き続き認証のキャプティブ ポータルにリダイレクトされ、失敗したログイン ユーザまたはゲスト ユーザには指定されず、Firepower Management Center に報告されることはありません。
- ユーザが確実にログアウトする唯一の方法は、ブラウザをいったん閉じ、再度開くことです。それを実行しなくても、ユーザがキャプティブ ポータルからログアウトし、同じブラウザを使用して認証を受けずにネットワークにアクセスできる場合があります。
- 親ドメインのレルムを作成し、管理対象デバイスがその親ドメインの子へのログインを検出した場合、管理対象デバイスはそのユーザのその後のログアウトを検出しません。
- （ルーテッド モードで ASA バージョン 9.5(2) 以降を実行する）ASA FirePOWER デバイスをキャプティブ ポータルに使用するには、**captive-portal** ASA CLI コマンドを使用してキャプティブ ポータルでのアクティブ認証を有効にし、https://www.cisco.com/c/en/us/support/security/adaptive-security-appliance-asa-software/products-installation-and-configuration-guides-list.htmlの『*ASA Firewall Configuration Guide*』（バージョン 9.5(2) 以降）の説明に従ってポートを定義します。
- キャプティブ ポータルに使用する予定のデバイスの IP アドレスおよびポートを宛先とするトラフィックを許可する必要があります。
- キャプティブ ポータル アクティブ認証を HTTPS トラフィックで行う場合、SSL ポリシーを使用して、認証対象のユーザからのトラフィックを復号する必要があります。キャプティブ ポータル ユーザの Web ブラウザと管理対象デバイス上のキャプティブ ポータル

デーモンとの間の接続では、トラフィックを復号できません。この接続は、キャプティブ ポータル ユーザの認証に使用されます。

- 管理対象デバイスの通過が許可されている HTTP 以外のトラフィックまたは HTTPS トラフィックの量を制限するには、アイデンティティ ポリシーの [ポート（Ports）] タブ ページで一般的な HTTP ポートと HTTPS ポートを入力する必要があります。

  管理対象デバイスは、着信要求に HTTP プロトコルまたは HTTPS プロトコルが使用されていないと判断した場合、以前に非表示にしたユーザを [保留中（Pending）] から [不明（Unknown）] に変更します。管理対象デバイスがユーザを [保留中（Pending）] から別の状態に変更するとすぐに、そのトラフィックに対してアクセス コントロール ポリシー、QoS ポリシー、および SSL ポリシーを適用できます。他のポリシーで HTTP 以外のトラフィックまたは HTTPS トラフィックが許可されていない場合は、キャプティブ ポータルのポートにアイデンティティ ポリシーを設定することによって、望ましくないトラフィックが管理対象デバイスを通過できないようにします。

ユーザ制御のためのキャプティブ ポータルの設定方法

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	Control	任意（NGIPSv を除く）	任意（Any）	Administrator/Access Admin/Network Admin

キャプティブ ポータルを使用したユーザ アクティビティの制御方法のハイレベルな概要は次のとおりです。

始める前に

アクティブ認証にキャプティブ ポータルを使用するには、アクセス コントロール ポリシー、アイデンティティ ポリシー、SSL ポリシーを設定して、アイデンティティおよび SSL ポリシーをアクセス コントロール ポリシーと関連付ける必要があります。最後にポリシーを管理対象デバイスに展開します。このトピックでは、このタスクのハイレベルな概要について説明します。

手順全体の例は、キャプティブ ポータルの設定パート 1：アイデンティティ ポリシーの作成（2612 ページ）にあります。

最初に次のタスクを実行します。

- ルーテッド インターフェイスが設定された 1 つ以上のデバイスが、 Firepower Management Center によって管理されていることを確認します。

  Firepower Management Center で ASA with FirePOWER デバイスを管理している場合には、キャプティブ ポータルのガイドラインと制約事項（2608 ページ） を参照してください。

- キャプティブ ポータルで暗号化認証を使用するには、Firepower Management Center のアクセス元となるマシンで証明書データとキーを利用可能にするか、PKI オブジェクトを作成します。PKI オブジェクトの作成方法については、PKI オブジェクト （579 ページ） を参照してください。

ステップ 1 次のトピックに記載されているようにレルムを作成し、有効化します。

- レルムの作成 （2576 ページ）
- レルム ディレクトリの設定 （2582 ページ）
- ユーザとグループのダウンロード （2583 ページ）

ステップ 2 キャプティブ ポータル用のアクティブ認証アイデンティティ ポリシーを作成します。
アイデンティティ ポリシーによって、キャプティブ ポータルで認証後にレルム アクセス リソースで選択したユーザを有効にします。

詳細については、キャプティブ ポータルの設定パート 1：アイデンティティ ポリシーの作成 （2612 ページ） を参照してください。

ステップ 3 キャプティブ ポータル ポート（デフォルトでは TCP 885）上のトラフィックを許可するキャプティブ ポータルに関するアクセス コントロール ルールを設定します。
キャプティブポータルが使用可能な TCP ポートのいずれかを選択できます。どれを選択しても、そのポートでトラフィックを許可するルールを作成する必要があります。

詳細については、キャプティブ ポータルの設定パート 2：TCP ポートアクセス コントロール ルールの作成 （2614 ページ） を参照してください。

ステップ 4 別のアクセス コントロール ルールを追加して、選択したレルムのユーザがキャプティブ ポータルを使用してリソースにアクセスできるようにします。
これにより、ユーザはキャプティブ ポータルで認証できます。 詳細については、キャプティブ ポータルの設定パート 3：ユーザ アクセス コントロール ルールの作成 （2615 ページ） を参照してください。

ステップ 5 キャプティブ ポータル ユーザが HTTPS プロトコルを使用して Web ページにアクセスできるように、[不明（Unknown）] なユーザ用の SSL 復号 - 再署名ポリシーを設定します。
HTTPS トラフィックがキャプティブ ポータルへ送信される前に復号化される場合のみ、キャプティブ ポータルはユーザを認証できます。システムは、キャプティブ ポータルを [不明（Unknown）] ユーザと認識します。

詳細については、キャプティブ ポータルの設定パート 4：SSL 復号 - 再署名ポリシーの作成 （2616 ページ） を参照してください。

ステップ 6 アイデンティティ ポリシーと SSL ポリシーをアクセス コントロール ポリシーに関連付けます（ステップ 2）。
この最後の手順により、システムはキャプティブ ポータルを使用してユーザを認証します。

詳細については、キャプティブ ポータルの設定パート 5：アクセス コントロール ポリシーへのアイデンティティ ポリシーと SSL ポリシーの関連付け （2617 ページ） を参照してください。

次のタスク

キャプティブ ポータルの設定パート 1：アイデンティティ ポリシーの作成（2612 ページ）を参照してください。

関連トピック

キャプティブ ポータルからのアプリケーションの除外（2619 ページ）
PKI オブジェクト（579 ページ）
キャプティブ ポータルのアイデンティティ ソースのトラブルシューティング（2620 ページ）
Snort® の再起動シナリオ（450 ページ）

キャプティブ ポータルの設定パート 1：アイデンティティ ポリシーの作成

始める前に

5 つのパートに分かれたこの手順では、デフォルトの TCP ポート 885 を使用し、キャプティブ ポータルと SSL 復号の両方に Firepower Management Center サーバ証明書を使用して、キャプティブ ポータルを設定する方法を示します。この例の各パートでは、キャプティブ ポータルでアクティブ認証を実行できるようにするために必要なタスクについて説明します。

すべての手順を実行すると、ドメイン内のユーザ用に機能するようにキャプティブ ポータルを設定できます。必要に応じて、手順の各パートで説明されている追加のタスクを実行できます。

手順全体の概要については、ユーザ制御のためのキャプティブ ポータルの設定方法（2610 ページ）を参照してください。

ステップ 1 まだ Firepower Management Center にログインしていない場合は、ログインします。

ステップ 2 **[ポリシー（Policies）]** > **[アクセス コントロール（Access Control）]** > **[アイデンティティ（Identity）]** の順にクリックして、アイデンティティ ポリシーを作成または編集します。

ステップ 3 （オプション）[カテゴリの追加（Add Category）] をクリックし、そのキャプティブ ポータル アイデンティティ ルール用にカテゴリを追加して、カテゴリの [名前（Name）] を入力します。

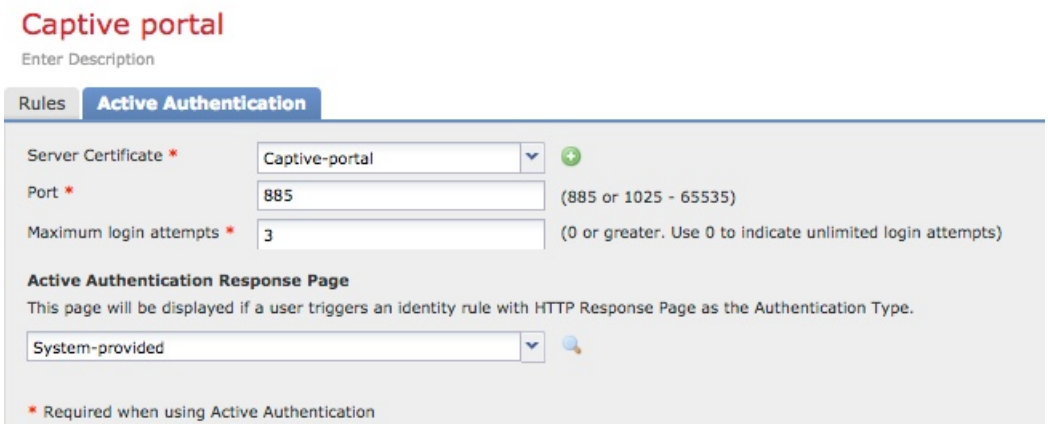
ステップ 4 [アクティブ認証（Active Authentication）] タブをクリックします。

ステップ 5 リストから適切な [サーバ証明書（Server Certificate）] を選択するか、追加アイコン（  ）をクリックして証明書を追加します。

（注） キャプティブ ポータルは、デジタル署名アルゴリズム（DSA）証明書または楕円曲線デジタル署名アルゴリズム（ECDSA）証明書の使用をサポートしていません。

ステップ 6 [ポート（Port）] フィールドに **885** と入力し、[最大ログイン試行回数（Maximum login attempts）] を指定します。

ステップ 7 （オプション）キャプティブ ポータル フィールド（2618 ページ）の説明に従って、[アクティブ認証応答ページ（Active Authentication Response Page）] を選択します。
次の図は例を示しています。



ステップ 8 [保存（Save）] をクリックします。

ステップ 9 [ルール（Rules）] タブをクリックします。

ステップ 10 [ルールの追加（Add Rule）] をクリックして新しいキャプティブ ポータル アイデンティティ ポリシー ルールを追加するか、編集アイコン（ ）をクリックして既存のルールを編集します。

ステップ 11 ルールの [名前（Name）] を入力します。

ステップ 12 [アクション（Action）] リストから [アクティブ認証（Active Authentication）] を選択します。

システムは、HTTP および HTTPS トラフィックにのみキャプティブ ポータル アクティブ認証を適用できます。アイデンティティ ルールの [アクション（Action）] が [アクティブ認証（Active Authentication）] である（つまりキャプティブ ポータルを使用している）場合、またはパッシブ認証を使用しており、[レルムおよび設定（Realms & Settings）] タブ ページのオプションで [パッシブ/VPN アイデンティティを確立できない場合にアクティブ認証を使用（Use active authentication if passive or VPN identity cannot be established）] がオンに設定されている場合、TCP ポート制約のみを使用します。

ステップ 13 [レルムおよび設定（Realm & Settings）] タブをクリックします。

ステップ 14 [レルム（Realms）] 一覧から、ユーザ認証に使用するレルムを選択します。

ステップ 15 （オプション）[認証でユーザを識別できない場合はゲストとして識別する（Identify as Guest if authentication cannot identify user）] をオンにします。詳細については、キャプティブ ポータル フィールド（2618 ページ）を参照してください。

ステップ 16 リストから [認証プロトコル（Authentication Protocol）] を 1 つ選択します。

ステップ 17 （オプション）キャプティブ ポータルから特定のアプリケーション トラフィックを除外する方法については、キャプティブ ポータルからのアプリケーションの除外（2619 ページ）を参照してください。

ステップ 18 ルール条件タイプ（465 ページ）の説明に従って、ルールに条件を追加します（ポートやネットワークなど）。

ステップ 19 [追加（Add）] をクリックします。

ステップ 20 ページの上部にある [保存（Save）] をクリックします。

次のタスク

キャプティブ ポータルの設定パート 2：TCP ポートアクセス コントロール ルールの作成 （2614 ページ）に進みます。

キャプティブ ポータルの設定パート 2：TCP ポートアクセス コントロール ルールの作成

この手順では、キャプティブ ポータルのデフォルト ポートである TCP ポート 885 を使用して、キャプティブ ポータルがクライアントと通信できるようにするアクセス コントロール ルールを作成する方法を示します。必要に応じて別のポートを選択できますが、キャプティブ ポータルの設定パート 1：アイデンティティ ポリシーの作成 （2612 ページ）で選択したポートと一致している必要があります。

始める前に

キャプティブ ポータル設定全体の概要については、ユーザ制御のためのキャプティブ ポータルの設定方法 （2610 ページ）を参照してください。

ステップ 1 アクセス コントロール ポリシー エディタで、[ルールの追加（Add Rule）] をクリックします。

ステップ 2 ルールの [名前（Name）] を入力します。

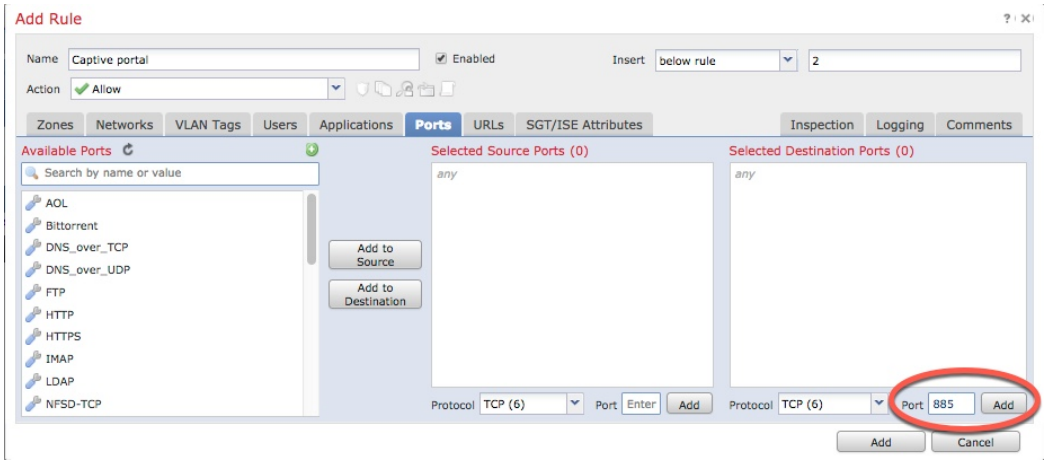
ステップ 3 [アクション（Action）] 一覧から、[許可（Allow）] を選択します。

ステップ 4 [ポート（Ports）] タブをクリックします。

ステップ 5 [選択した宛先ポート（Selected Destination Ports）] フィールの [プロトコル（Protocol）] 一覧から、[TCP] を選択します。

ステップ 6 [ポート（Port）] フィールドに **885** と入力します。

ステップ 7 [ポート（Port）] フィールドの横にある [追加（Add）] をクリックします。
次の図は例を示しています。



ステップ 8 ページ下部の [追加（Add）] をクリックします。

次のタスク

キャプティブ ポータルの設定パート 3：ユーザ アクセス コントロール ルールの作成（2615 ページ）に進みます。

キャプティブ ポータルの設定パート 3：ユーザ アクセス コントロール ルールの作成

この手順では、レルム内のユーザがキャプティブ ポータルを使用して認証できるようにするアクセス コントロール ルールを追加する方法について説明します。

始める前に

キャプティブ ポータル設定全体の概要については、ユーザ制御のためのキャプティブ ポータルの設定方法 （2610 ページ）を参照してください。

ステップ 1 ルール エディタで、[ルールの追加（Add Rule）] をクリックします。

ステップ 2 ルールの [名前（Name）] を入力します。

ステップ 3 [アクション（Action）] 一覧から、[許可（Allow）] を選択します。

ステップ 4 [ユーザ（Users）] タブをクリックします。

ステップ 5 [使用可能なレルム（Available Realms）] 一覧で、許可するレルムをクリックします。

ステップ 6 レルムが表示されない場合は、（更新）をクリックします。

ステップ 7 [使用可能なユーザ（Available Users）] 一覧で、ルールに追加するユーザを選択し、[ルールに追加（Add to Rule）] をクリックします。

ステップ 8 （オプション）ルール条件タイプ （465 ページ）の説明に従って、アクセス コントロール ポリシーに条件を追加します。

ステップ 9 [追加（Add）] をクリックします。

ステップ 10 [アクセス制御ルール（access control rule）] ページで、[保存（Save）] をクリックします。

ステップ 11 ポリシー エディタで、ルールの位置を設定します。クリックしてドラッグするか、または右クリック メニューを使用してカット アンド ペーストを実行します。ルールには 1 から番号が付けられます。システムは、ルール番号の昇順で上から順に、ルールをトラフィックと照合します。トラフィックが一致する最初のルールは、そのトラフィックを処理するルールです。適切なルールの順序を指定することで、ネットワーク トラフィックの処理に必要なリソースが削減され、ルールのプリエンプションを回避できます。

次のタスク

キャプティブ ポータルの設定パート 4：SSL 復号 - 再署名ポリシーの作成 （2616 ページ）に進みます。

キャプティブ ポータルの設定パート 4：SSL 復号 - 再署名ポリシーの作成

この手順では、トラフィックがキャプティブ ポータルに到達する前に、トラフィックを復号して再署名する SSL アクセス ポリシーを作成する方法について説明します。キャプティブ ポータルは、トラフィックが復号された後にのみトラフィックを認証できます。

始める前に

キャプティブ ポータル設定全体の概要については、ユーザ制御のためのキャプティブ ポータルの設定方法 （2610 ページ）を参照してください。

ステップ 1 PKI オブジェクト （579 ページ）の説明に従って、SSL トラフィックを複合化するための証明書オブジェクトを作成します（まだ作成していない場合）。

ステップ 2 **[ポリシー（Policies）] > [アクセス コントロール（Access Control）] > [SSL]** の順にクリックします。

ステップ 3 [新しいポリシー（New Policy）] をクリックします。

ステップ 4 ポリシーの [名前（Name）] を入力し、[デフォルトのアクション（Default Action）] を選択します。デフォルトのアクションについては、SSL ポリシーのデフォルト アクション （1838 ページ）を参照してください。

ステップ 5 [保存（Save）] をクリックします。

ステップ 6 [ルールの追加（Add Rule）] をクリックします。

ステップ 7 ルールの [名前（Name）] を入力します。

ステップ 8 [アクション（Action）] 一覧から、[復号-再署名（Decrypt - Resign）] を選択します。

ステップ 9 [with] 一覧から、使用する PKI オブジェクトを選択します。

ステップ 10 [ユーザ（Users）] タブをクリックします。

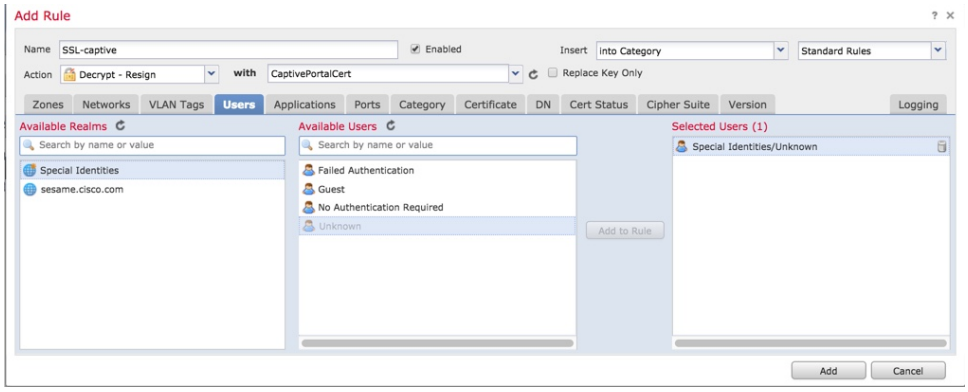
ステップ 11 [使用可能なレルム（Available Realms）] 一覧の上にある （更新）をクリックします。

ステップ 12 [使用可能なレルム（Available Realms）] 一覧で、[特殊なアイデンティティ（Special Identities）] をクリックします。

ステップ 13 [使用可能なユーザ（Available Users）] 一覧で、[不明（Unknown）] をクリックします。

ステップ 14 [ルールに追加（Add to Rule）] をクリックします。

次の図は例を示しています。



ステップ 15 （オプション）TLS/SSL ルール条件 （1861 ページ）の説明に従って、他のオプションを設定します。

ステップ 16 [追加（Add）] をクリックします。

ステップ 17 ページの上部にある [保存（Save）] をクリックします。

次のタスク

キャプティブ ポータルの設定パート 5：アクセス コントロール ポリシーへのアイデンティティ ポリシーと SSL ポリシーの関連付け （2617 ページ）に進みます。

キャプティブ ポータルの設定パート 5：アクセス コントロール ポリシーへのアイデンティティ ポリシーと SSL ポリシーの関連付け

この手順では、アイデンティティ ポリシーと SSL [復号-再署名（Decrypt - Resign）] ルールを、以前に作成したアクセス コントロール ポリシーに関連付ける方法について説明します。この手順を実行すると、ユーザはキャプティブ ポータルを使用して認証できるようになります。

始める前に

キャプティブ ポータル設定全体の概要については、ユーザ制御のためのキャプティブ ポータルの設定方法 （2610 ページ）を参照してください。

ステップ 1 **[ポリシー（Policies）] > [アクセス制御（Access Control）] > [アクセス制御（Access Control）]** をクリックして、キャプティブ ポータルの設定パート 2：TCP ポート アクセス コントロール ルールの作成 （2614 ページ）の説明に従い作成したアクセス コントロール ポリシーを編集します。 代わりに表示アイコン（🔍）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 2 新しいアクセス コントロール ポリシーを作成するか、既存のポリシーを編集します。

ステップ 3 ページ上部の [アイデンティティ ポリシー（Identity Policy）] の横にあるリンクをクリックします。

ステップ 4 一覧から、使用するアイデンティティ ポリシーの名前を選択し、ページ上部にある [保存（Save）] をクリックします。

ステップ 5 上記の手順を繰り返して、使用するキャプティブ ポータル SSL ポリシーをアクセス コントロール ポリシーに関連付けます。

ステップ 6 アクセス コントロール ポリシーのターゲット デバイスの設定（1680 ページ）の説明に従って、管理対象デバイスでそのポリシーをターゲットにします（この手順をまだ行っていない場合）。

次のタスク

- 設定変更の展開（447 ページ）の説明に従って、使用するアイデンティティ ポリシーとアクセス コントロール ポリシーを管理対象デバイスに展開します。
- ワークフローの使用（2931 ページ）の説明に従って、ユーザ アクティビティをモニタします。

キャプティブ ポータル フィールド

次のフィールドを使用して、アイデンティティ ポリシーの [アクティブ認証（Active Authentication）] タブでキャプティブ ポータルを設定します。アイデンティティ ルール フィールド（2639 ページ）も参照してください。

Server Certificate

キャプティブ ポータル デーモンが示すサーバ証明書。

（注） キャプティブ ポータルは、デジタル署名アルゴリズム（DSA）証明書または楕円曲線デジタル署名アルゴリズム（ECDSA）証明書の使用をサポートしていません。

[ポート（Port）]

キャプティブ ポータル接続のために使用するポート番号。ASA FirePOWER デバイスをキャプティブ ポータルに使用しようとする場合は、このフィールドのポート番号が、**captive-portal** CLI コマンドを使用して ASA FirePOWER デバイスで設定したポート番号と一致している必要があります。

最大ログイン試行回数（Maximum login attempts）

ユーザのログイン要求がシステムによって拒否されるまでに許容されるログイン試行失敗の最大数。

Active Authentication Response Page

システム提供の HTTP 応答ページには、[ユーザ名（Username）] と [パスワード（Password）] フィールドに加え、[ゲストとしてログイン（Login as guest）] ボタンがあり、ユーザはゲストとしてネットワークにアクセスできます。単一のログイン方法を表示するには、カスタム HTTP 応答ページを設定します。

次のオプションから選択します。

- 汎用的な応答を使用する場合は、[システム提供（System-provided）] をクリックします。表示アイコン（  ）をクリックすると、このページの HTML コードが表示されます。
- カスタム応答を作成する場合は、[カスタム（Custom）]をクリックします。システム提供コードを示すウィンドウが表示され、これを置換または変更できます。完了したら、変更を保存します。カスタム ページは、編集アイコン（  ）をクリックすると編集できます。

関連トピック

内部証明書オブジェクト （590 ページ）

キャプティブ ポータルからのアプリケーションの除外

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	Control	任意（NGIPSv を除く）	任意（Any）	Administrator、Access Admin、Network Admin

アプリケーション（HTTP ユーザ エージェント文字列によって指定される）を選択し、キャプティブ ポータルのアクティブ認証から除外することができます。これにより、選択されたアプリケーションからのトラフィックが認証を受けずにアイデンティティ ポリシーを通過できるようになります。

（注） このリストに表示されるのは、**User-Agent Exclusion タグ**が付けられたアプリケーションのみです。

ステップ 1 アイデンティティ ルール エディタ ページの [レルムおよび設定（Realm & Settings）] タブで、[アプリケーション フィルタ（Application Filters）] リストのシスコ提供のフィルタを使用して、フィルタに追加するアプリケーションのリストを絞り込みます。

- リストを展開および縮小するには、各フィルタ タイプの横にある矢印をクリックします。
- フィルタ タイプを右クリックし、[Check All] または [Uncheck All] をクリックします。このリストには、各タイプで選択したフィルタ数が示されることに注意してください。
- 表示されるフィルタを絞り込むには、[Search by name] フィールドに検索文字列を入力します。これは、カテゴリとタグの場合に特に有効です。検索をクリアするには、クリア アイコン（）をクリックします。
- フィルタのリストを更新し、選択したフィルタをすべてクリアするには、リロードアイコン（  ）をクリックします。

- すべてのフィルタと検索フィールドをクリアするには、[すべてのフィルタをクリア（Clear All Filters）] をクリックします。

（注） リストには一度に 100 のアプリケーションが表示されます。

ステップ 2 [Available Applications] リストから、フィルタに追加するアプリケーションを選択します。

- 表示される個別のアプリケーションを絞り込むには、[名前で検索（Search by name）] フィールドに検索文字列を入力します。検索をクリアするには、クリア アイコン（ ）をクリックします。
- 使用可能な個別のアプリケーションのリストを参照するには、リストの下部にあるページング アイコンを使用します。
- アプリケーションのリストを更新し、選択したアプリケーションをすべてクリアするには、リロード アイコン（ ）をクリックします。

ステップ 3 外部認証から除外する、選択したアプリケーションを追加します。クリックしてドラッグするか、[ルールに追加（Add to Rule）] をクリックできます。結果は、選択したアプリケーション フィルタの組み合わせになります。

次のタスク

- アイデンティティ ルールの作成（2638 ページ）の説明に従ってアイデンティティ ルールの設定を続けます。

キャプティブポータルのアイデンティティソースのトラブルシューティング

関連の他のトラブルシューティングについては、レルムとユーザのダウンロードのトラブルシュート（2586 ページ）およびユーザ制御のトラブルシューティング（494 ページ）を参照してください。

キャプティブ ポータルに関する問題が発生した場合は、次の点を確認してください。

- キャプティブ ポータル サーバの時刻は、Firepower Management Center の時刻と同期している必要があります。
- 設定済みの DNS 解決があり、**Kerberos**（または Kerberos をオプションとする場合は **HTTP ネゴシエート**）キャプティブ ポータルを実行するアイデンティティ ルールを作成する場合は、キャプティブ ポータルデバイスの完全修飾ドメイン名（FQDN）を解決するように DNS サーバを設定する必要があります。FQDN は、DNS 設定時に指定したホスト名と一致する必要があります。

ASA with FirePOWER Services および Firepower Threat Defense デバイスの場合、FQDN は、キャプティブ ポータルに使用されるルーテッド インターフェイスの IP アドレスに解決される必要があります。

- **Kerberos**（または Kerberos をオプションとする場合に**HTTP ネゴシエート**）を、アイデンティティ ルールの [認証タイプ（Authentication Type）] として選択する場合、選択する [レルム（Realm）] は、Kerberos キャプティブ ポータル アクティブ認証を実行できるように、[アクティブディレクトリ参加ユーザ名（AD Join Username）] と [アクティブディレクトリ参加パスワード（AD Join Password）] を使用して設定する必要があります。
- アイデンティティ ルールの [認証タイプ（Authentication Type）] として [HTTP 基本（HTTP Basic）] を選択した場合、ネットワーク上のユーザはセッションがタイムアウトしたことを認識しない場合があります。ほとんどの Web ブラウザは、**HTTP 基本**ログインからクレデンシャルをキャッシュし、古いセッションがタイムアウトした後にシームレスに新しいセッションを開始するためにそのクレデンシャルを使用します。
- Firepower Management Center と管理対象デバイスとの間の接続に障害が発生した場合、ユーザが以前に認識され Firepower Management Center にダウンロードされた場合を除き、デバイスによって報告されたすべてのキャプティブ ポータル ログインはダウンタイム中に特定できません。識別されていないユーザは、Firepower Management Center で [不明（Unknown）] のユーザとして記録されます。ダウンタイム後、不明のユーザはアイデンティティ ポリシーのルールに従って再確認され、処理されます。
- キャプティブ ポータルに使用する予定のデバイスにインライン インターフェイスとルーテッドインターフェイスの両方が含まれる場合、キャプティブ ポータルデバイス上でルーテッドインターフェイスだけを対象とするようにキャプティブ ポータルアイデンティティ ルールでゾーン条件を設定する必要があります。
- システムは ASA with FirePOWER デバイスでインターフェイス タイプを検証しません。ASA with FirePOWER デバイス上でインライン（タップ モード）インターフェイスにキャプティブ ポータル ポリシーを適用すると、ポリシーは正常に展開されますが、これらのルールに一致するトラフィック内のユーザは「不明」と識別されます。
- ユーザが確実にログアウトする唯一の方法は、ブラウザをいったん閉じ、再度開くことです。それを実行しなくても、ユーザがキャプティブ ポータルからログアウトし、同じブラウザを使用して認証を受けずにネットワークにアクセスできる場合があります。
- アクティブ FTP セッションは、イベントの **Unknown** ユーザとして表示されます。これは正常な処理です。アクティブ FTP では、（クライアントではない）サーバが接続を開始し、FTP サーバには関連付けられているユーザ名がないはずだからです。アクティブ FTP の詳細については、RFC 959 を参照してください。

キャプティブ ポータルの履歴

機能	バージョン	詳細
ゲスト ログイン。	6.1.0	ユーザは、キャプティブ ポータルを使用してゲストとしてログインできます。
キャプティブ ポータル。	6.0	導入された機能。キャプティブ ポータルを使用して、ブラウザ ウィンドウにプロンプトが表示されたときにクレデンシャルを入力するよう、ユーザに要求することができます。このマッピングでは、ユーザまたはユーザのグループに基づいたポリシーを使用することもできます。

第 103 章

リモート アクセス VPN によるユーザの制御

次のトピックでは、リモート アクセス VPN によりユーザ認識とユーザ制御を実行する方法について説明します。

リモート アクセス VPN アイデンティティ ソース

Firepower Threat Defense は、リモート アクセス SSL と IPsec-IKEv2 VPN をサポートするセキュアなゲートウェイ機能を提供します。完全なトンネル クライアントである AnyConnect Secure Mobility Client[AnyConnectSecureMobilityClient] は、セキュリティ ゲートウェイへのセキュアな SSL および IPsec-IKEv2 接続をリモート ユーザに提供します。AnyConnect はエンドポイント デバイスでサポートされている唯一のクライアントで、Firepower Threat Defense デバイスへのリモート VPN 接続が可能です。

新しいリモート アクセス VPN ポリシーの作成 （1098 ページ）の説明に従って安全な VPN ゲートウェイを設定する場合、ユーザが Active Directory リポジトリ内にいる場合は、それらのユーザのアイデンティティ ポリシーを設定して、アクセス コントロール ポリシーにアイデンティティ ポリシーを関連付けることができます。

リモート ユーザから提供されるログイン情報は、LDAP または AD レルムまたは RADIUS サーバ グループによって検証されます。これらのエンティティは、Firepower Threat Defense セキュア ゲートウェイと統合されます。

（注） ユーザが認証ソースとして Active Directory を使用して RA VPN で認証を受ける場合、ユーザは自分のユーザ名を使用してログインする必要があります。`domain\username` または `username@domain` 形式は失敗します。（Active Directory はこのユーザ名をログオン名、または場合によっては `sAMAccountName` と呼んでいます）。詳細については、MSDN でユーザの命名属性 [英語] を参照してください。

認証に RADIUS を使用する場合、ユーザは前述のどの形式でもログインできます。

VPN 接続経由で認証されると、リモート ユーザには *VPN ID* が適用されます。この VPN ID は、そのリモート ユーザに属しているネットワーク トラフィックを認識し、フィルタリングするために Firepower Threat Defense のセキュア ゲートウェイ上のアイデンティティ ポリシーで使用されます。

アイデンティティ ポリシーはアクセス コントロール ポリシーと関連付けられ、これにより、誰がネットワーク リソースにアクセスできるかが決まります。リモート ユーザがブロックされるか、またはネットワーク リソースにアクセスできるかはこのようにして決まります。

関連トピック

Firepower Threat Defense の VPN の概要 （1053 ページ）
Firepower Threat Defense リモート アクセス VPN の概要 （1085 ページ）
VPN の基本 （1054 ページ）
リモート アクセス VPN の機能 （1086 ページ）
リモート アクセス VPN のガイドラインと制限事項 （1093 ページ）
新しいリモート アクセス VPN ポリシーの作成 （1098 ページ）

ユーザ制御用 RA VPN の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス（Access）
エクスポート制御機能が有効なスマート ライセンス アカウントに関連付けられている次の AnyConnect ライセンスのいずれか。 • AnyConnect VPN Only • AnyConnect Plus • AnyConnect Apex	該当なし	FTD	グローバルだけ	Admin/Access Admin/Network Admin

始める前に

- レルムの作成 （2576 ページ）の説明に従って、レルムを作成します。
- 認証、認可、および監査（AAA）を使用するには、RADIUS サーバ グループ （635 ページ）の説明に従って RADIUS サーバ グループを設定します。

ステップ 1 Firepower Management Center にログインします。

ステップ 2 **[デバイス（Devices）] > [VPN] > [リモートアクセス（Remote Access）]** の順にクリックします。

ステップ 3 新しいリモート アクセス VPN ポリシーの作成 （1098 ページ）を参照してください。

次のタスク

- アイデンティティ ポリシーの作成 （2643 ページ）の説明に従い、アイデンティティ ポリシーを使用して、制御するユーザおよびその他のオプションを指定します。
- アクセス制御への他のポリシーの関連付け （1684 ページ）の説明に従って、アイデンティティ ルールをアクセス コントロール ポリシーに関連付けます。このポリシーは、トラフィックをフィルタし、オプションで検査します。

- 設定変更の展開（447ページ）の説明に従って、使用するアイデンティティ ポリシーとアクセス コントロール ポリシーを管理対象デバイスに展開します。
- VPN セッションとユーザ情報（1162ページ）の説明に従って、VPN ユーザ トラフィックをモニタします。

リモート アクセス VPN アイデンティティ ソースのトラブルシューティング

- 関連する他のトラブルシューティングについては、レルムとユーザのダウンロードのトラブルシュート（2586ページ）、ユーザ制御のトラブルシューティング（494ページ）、および Firepower Threat Defense の VPN のトラブルシューティング（1165ページ）を参照してください。
- リモート アクセス VPN の問題が発生した場合は、Firepower Management Center と管理対象デバイスとの間の接続を確認します。接続に障害が発生している場合、ユーザが既に認識されて Firepower Management Center にダウンロードされている場合を除き、デバイスによって報告されたすべてのリモート アクセス VPN ログインはダウンタイム中に識別されません。

  識別されていないユーザは、Firepower Management Center で [不明（Unknown）] のユーザとして記録されます。ダウンタイム後、[不明（Unknown）] ユーザはアイデンティティ ポリシーのルールに従って再び識別され、処理されます。
- アクティブ FTP セッションは、イベントの **Unknown** ユーザとして表示されます。これは正常な処理です。アクティブ FTP では、（クライアントではない）サーバが接続を開始し、FTP サーバには関連付けられているユーザ名がないはずだからです。アクティブ FTP の詳細については、RFC 959 を参照してください。

RA VPN の履歴

機能	バージョン	詳細
リモート アクセス VPN	6.2.1	導入された機能。RA VPN により、インターネットに接続されたラップトップまたはデスクトップ コンピュータや、Android または Apple iOS モバイル デバイスを使用して、個々のユーザがリモート ロケーションからプライベート ビジネス ネットワークに接続することができます。リモート ユーザは、共有メディアやインターネットを介してデータを転送するために不可欠な暗号化技術を使用して、セキュアに機密性を保持してデータを転送します。

第 104 章

TS エージェントによるユーザの制御

次のトピックでは、TS エージェントによりユーザ認識とユーザ制御を実行する方法について説明します。

ターミナルサービス（TS）エージェントのアイデンティティ ソース

TS エージェントはパッシブ認証方式で、Firepower システムでサポートされる権限のあるアイデンティティ ソースの 1 つです。Windows Terminal Server が認証を実行し、TS エージェントがスタンドアロンまたはハイ アベイラビリティの Firepower Management Center にその認証の実行を報告します。

TS エージェントは、Windows Terminal Server にインストールされると、個々のユーザがモニタ対象ネットワークにログインまたはログアウトする際にそのユーザに固有のポート範囲を割り当てます。Firepower Management Center では、この固有のポートを使用して Firepower システムの個々のユーザを識別します。1 つの TS エージェントを使用して、1 つの Windows Terminal Server 上のユーザ アクティビティをモニタし、暗号化データを Firepower Management Center に送信できます。

TS エージェントは失敗したログイン試行を報告しません。TS エージェントから取得されたデータは、ユーザ認識とユーザ制御に使用できます。

TS エージェントのガイドライン

TS エージェントには段階的な設定が必要で、次のものがあります。

1. TS エージェントがインストールおよび設定された Windows Terminal Server。
2. サーバがモニタするユーザを対象とする 1 つ以上のアイデンティティ レルム。

TS エージェントは、Microsoft Windows Terminal Server にインストールします。段階的な TS エージェントのインストールと設定、およびサーバと Firepower システムの要件の詳細については、『*Cisco Terminal Services (TS) Agent Guide*』を参照してください。

TS エージェントのデータは [ユーザ（Users）] テーブル、[ユーザ アクティビティ（User Activity）] テーブル、および [接続イベント（Connection Event）] テーブルに表示され、ユーザ認識とユーザ制御に使用できます。

（注） TS エージェントが別のパッシブ認証のアイデンティティ ソース（ユーザ エージェントまたは ISE/ISE-PIC）と同じユーザをモニタする場合、Firepower Management Center では TS エージェントのデータを優先します。TS エージェントと別のパッシブのアイデンティティ ソースが同じ IP アドレスでアクティビティを報告した場合、TS エージェントのデータだけが Firepower Management Center に記録されます。

TS エージェントのユーザ制御の構成

TS エージェントをユーザ認識およびユーザ制御のアイデンティティ ソースとして使用するには、『*Cisco Terminal Services (TS) Agent Guide*』の説明に従って TS エージェント ソフトウェアをインストールして構成してください。

次に行う作業：

- アイデンティティ ポリシーの作成 （2643 ページ）の説明に従い、アイデンティティ ポリシーを使用して、制御するユーザおよびその他のオプションを指定します。
- アクセス制御への他のポリシーの関連付け （1684 ページ）の説明に従って、アイデンティティ ルールをアクセス コントロール ポリシーに関連付けます。このポリシーは、トラフィックをフィルタし、オプションで検査します。
- 設定変更の展開 （447 ページ）の説明に従って、使用するアイデンティティ ポリシーとアクセス コントロール ポリシーを管理対象デバイスに展開します。
- ワークフローの使用 （2931 ページ）の説明に従って、ユーザ アクティビティをモニタします。

TS エージェント アイデンティティ ソースのトラブルシューティング

関連の他のトラブルシューティングについては、レルムとユーザのダウンロードのトラブルシュート（2586 ページ）およびユーザ制御のトラブルシューティング（494 ページ）を参照してください。

TS エージェントと Firepower システムの統合に問題が起こった場合は、次のことを確認してください。

- TS エージェントサーバと Firepower Management Center の時計を同期させる必要があります。
- TS エージェントが別のパッシブ認証 ID ソース（ユーザ エージェントまたは ISE）と同じユーザをモニタしている場合、Firepower Management Center は TS エージェントのデータを優先します。TS エージェントとパッシブ ID ソースが同じ IP アドレスによるアクティビティを報告した場合は、TS エージェントのデータのみが Firepower Management Center に記録されます。
- アクティブ FTP セッションは、イベントの **Unknown** ユーザとして表示されます。これは正常な処理です。アクティブ FTP では、（クライアントではない）サーバが接続を開始し、FTP サーバには関連付けられているユーザ名がないはずだからです。アクティブ FTP の詳細については、RFC 959 を参照してください。

トラブルシューティングのすべての情報は、『*Cisco Terminal Services (TS) Agent Configuration Guide*』を参照してください。

TS エージェントの履歴

機能	バージョン	詳細
ユーザ制御用の TS エージェント。	6.2.0	導入された機能。FirePOWER が、Citrix の仮想デスクトップインフラストラクチャ（VDI）などの共有環境で個々のユーザをより正確に識別して、ファイアウォールにユーザベースのポリシールールを正確に適用できるようになりました。ユーザは使用されるポートによって識別されます。 TS エージェント ソフトウェアは、Firepower Management Center とは独立して更新されます。詳細については、以下を参照してください。 • cisco.com で利用可能な『*Cisco Terminal Services (TS) Agent Guide*』 • 『Cisco Firepower Compatibility Guide』

第 105 章

ユーザ エージェントによるユーザの制御

次のトピックでは、ユーザエージェントによりユーザ認識とユーザ制御を実行する方法について説明します。

ユーザ エージェントのアイデンティティ ソース

Cisco Firepower User Agent は、パッシブ認証方法で、信頼できるアイデンティティ ソース（つまり、信頼された Active Directory サーバでユーザ情報が提供されます）でもあります。ユーザ エージェントは、Firepower システムと統合されると、ユーザが Active Directory クレデンシャルでホストにログインする、またはホストからログアウトするときに、そのユーザをモニタします。ユーザ エージェントから取得されたデータは、ユーザ認識とユーザ制御に使用できます。

ユーザ エージェントは、各ユーザを IP アドレスと関連付けます。これにより、ユーザ条件を使用するアクセス コントロール ルールをトリガーすることができます。1 つのユーザ エージェントを使用して、最大 5 つの Active Directory サーバでユーザ アクティビティをモニタでき、最大 5 つの Firepower Management Center に暗号化データを送信できます。

ユーザ エージェントは失敗したログイン試行を報告しません。

ユーザ エージェントのガイドライン

ユーザ エージェントは、以下を含む段階的な設定が必要です。

- ユーザ エージェントがインストールされている少なくとも 1 台のコンピュータ 。
- ユーザ エージェントがインストールされたコンピュータまたは Active Directory サーバと Firepower Management Center との間の接続。

- ユーザ エージェントからユーザ データを受け取る各 Firepower Management Center で設定されたアイデンティティ レルム。

段階的なユーザ エージェントの設定とサーバの要件の詳細については、『*Cisco Firepower* ユーザ エージェント コンフィギュレーション ガイド』を参照してください。

（注） コンピュータまたは Active Directory サーバの時間が Firepower Management Center の時間と同期されていることを確認します。アプライアンスが同期されていないと、予想外の間隔でユーザのタイムアウトが実行される可能性があります。

Firepower Management Center接続は、ログインとログオフがユーザ エージェントによって検出されたユーザのメタデータを取得可能にするだけでなく、アクセス コントロール ルール内で使用するユーザとグループを指定するためにも使用されます。ユーザ エージェントが特定のユーザ名を除外するように設定されている場合は、そのようなユーザ名のログイン データは Firepower Management Center に報告されません。ユーザ エージェントのデータは、Firepower Management Center のユーザ データベースとユーザ アクティビティ データベースに保存されます。

（注） ユーザ エージェントは $ 記号で終わる Active Directory ユーザ名を Firepower Management Center に送信できません。これらのユーザをモニタする場合は、最後の $ の文字を削除する必要があります。

複数のユーザがリモート セッションを使用してホストにログインしている場合は、エージェントがそのホストからのログインを正確に検出しない場合があります。これを防ぐ方法の詳細については、『*Cisco Firepower* ユーザ エージェント コンフィギュレーション ガイド』を参照してください。

ユーザ エージェント アイデンティティ ソースのトラブルシューティング

ユーザエージェント接続に問題が起こった場合は、*Cisco Firepower* ユーザ エージェント コンフィギュレーション ガイド を確認してください。

このガイドの関連するトラブルシューティング情報については、レルムとユーザのダウンロードのトラブルシュート （2586ページ）とユーザ制御のトラブルシューティング （494ページ）を参照してください。

ユーザ エージェントによって報告されるユーザ データに関する問題が発生した場合は、次の点に注意してください。

- システムはデータがまだデータベースにないユーザ エージェント ユーザのアクティビティを検出すると、サーバからそれらに関する情報を取得します。ユーザのアクティビティ

は、システムがユーザのダウンロードでユーザに関する情報の取得に成功するまでルールで処理されず、Web インターフェイスに表示されません。

- Firepower Management Center のハイ アベイラビリティが設定されており、プライマリが失敗した場合、たとえ以前ユーザを確認できており、Firepower Management Center にダウンロード済みであっても、フェールオーバーダウンタイム中にユーザエージェントが報告したすべてのログインが特定不能となります。未確認のユーザは Firepower Management Center には不明なユーザとして記録されます。ダウンタイム後、[不明（Unknown）] ユーザはアイデンティティ ポリシーのルールに従って再び識別され、処理されます。
- ユーザ エージェントが TS エージェントと同じユーザをモニタした場合、システムは TS エージェントのデータを優先します。TS エージェントとユーザエージェントが同じ IP アドレスによる同一のアクティビティを報告した場合は、TS エージェントのデータのみがログに記録されます。
- アクティブ FTP セッションは、イベントの **Unknown** ユーザとして表示されます。これは正常な処理です。アクティブ FTP では、（クライアントではない）サーバが接続を開始し、FTP サーバには関連付けられているユーザ名がないはずだからです。アクティブ FTP の詳細については、RFC 959 を参照してください。

ユーザ エージェントの履歴

機能	バージョン	詳細
ユーザ エージェント バージョン 2.5	6.4	ユーザエージェントが FMC での認証に使用するデフォルトのパスワードを変更できます。 新しい FMC コマンド： **configure user-agent**
ユーザ制御用のユーザ エージェント。	—	バージョン 6.0 よりも前に導入された機能です。ユーザ エージェントにより Active Directory ユーザのログインの詳細が提供され、ユーザ認識とユーザ制御に使用できます。

第 106 章

アイデンティティ ポリシーの作成および管理

次のトピックでは、アイデンティティ ルールとアイデンティティ ポリシーの作成方法と管理方法について説明します。

アイデンティティ ポリシーについて

アイデンティティ ポリシーには、アイデンティティ ルールが含まれます。アイデンティティ ルールでは、トラフィックのセットを、レルムおよび認証方式（パッシブ認証、アクティブ認証、または認証なし）と関連付けます。

このトピックの最後に記載されている例外を除き、使用する予定のレルムと認証方式を、アイデンティティ ルールで起動する前に設定する必要があります。

- **[システム（System）] > [統合（Integration）] > [レルム（Realms）]** でアイデンティティ ポリシー外のレルムを設定します。詳細については、レルムの作成 （2576ページ）を参照してください。
- パッシブ認証のアイデンティティ ソースであるユーザ エージェントと ISE/ISE-PIC は、**[システム（System）] > [統合（Integration）] > [アイデンティティ ソース（Identity Sources）]** で設定します。詳細については、ユーザ制御のためのユーザ エージェントの設定およびユーザ制御用 ISE/ISE-PIC の設定 （2601 ページ）を参照してください。
- パッシブ認証のアイデンティティ ソースである TS エージェントについては、Firepower システムの外で設定します。詳細については、『*Cisco Terminal Services (TS) Agent Guide*』を参照してください。

- アクティブ認証のアイデンティティ ソースであるキャプティブ ポータルについては、アイデンティティ ポリシー内で設定します。詳細については、ユーザ制御のためのキャプティブ ポータルの設定方法 （2610 ページ）を参照してください。
- リモート アクセス VPN ポリシー内では、アクティブな認証アイデンティティ ソースであるリモート アクセス VPN を設定します。詳細については、リモート アクセス VPN 認証（1088 ページ）を参照してください。

単一のアイデンティティ ポリシーに複数のアイデンティティ ルールを追加した後、ルールの順番を決めます。システムは、ルール番号の昇順で上から順に、ルールをトラフィックと照合します。トラフィックが一致する最初のルールがそのトラフィックを処理するルールです。

1 つ以上のアイデンティティ ポリシーを設定した後、1 つのアイデンティティ ポリシーをアクセス コントロール ポリシーに関連付ける必要があります。ネットワークのトラフィックがアイデンティティ ルールの条件と一致する場合、システムはトラフィックを指定されたレルムと関連付け、指定されたアイデンティティ ソースを使用してトラフィックのユーザを認証します。

アイデンティティ ポリシーを設定しない場合、システムはユーザ認証を実行しません。

アイデンティティ ポリシーの作成に関する例外

次のすべてに該当する場合、アイデンティティ ポリシーは必要ありません。

- ISE/ISE-PIC アイデンティティ ソースを使用できます。
- アクセス コントロール ポリシーのユーザまたはグループは使用しません。
- アクセス コントロール ポリシーのセキュリティ グループ タグ（SGT）を使用します。詳細については、「ISE SGT とカスタム SGT ルール条件との比較 （496 ページ）」を参照してください。

関連トピック

アイデンティティ ポリシーの設定方法 （2485 ページ）

アイデンティティ ルールの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	Control	いずれか（Any）	いずれか（Any）	Administrator、Access Admin、Network Admin

アイデンティティ ルールの設定オプションに関する詳細については、アイデンティティ ルール フィールド （2639 ページ）を参照してください。

ステップ 1 まだ Firepower Management Center にログインしていない場合は、ログインします。

ステップ 2 **[Policies]** > **[Access Control]** > **[Identity]** をクリックします。

ステップ 3 アイデンティティ ルールの追加先となるアイデンティティ ポリシーの横にある [編集（edit）]（  ）をクリックします。

代わりに表示アイコン（  ）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 4 [ルールの追加（Add Rule）] をクリックします。

ステップ 5 名前を入力します。

ステップ 6 ルールを**有効**にするかどうかを指定します。

ステップ 7 既存のカテゴリにルールを追加するには、ルールを [挿入（Insert）] する場所を指定します。新しいカテゴリを追加するには、[カテゴリの追加（Add Category）] をクリックします。

ステップ 8 一覧からルール [アクション（Action）] を選択します。

ステップ 9 [レルムおよび設定（Realms & Settings）] タブをクリックします。

ステップ 10 [レルム（Realms）] 一覧から、アイデンティティ ルールのレルムを選択します。各アイデンティティ ルールにレルムを関連付ける必要があります。

レルム要件の唯一の例外は、ISE SGT 属性タグのみを使用してユーザ制御を実装する場合です。この場合は、ISE サーバのレルムを設定する必要はありません。ISE SGT 属性条件は、関連するアイデンティティ ポリシーの有無にかかわらずポリシーで設定できます。

ステップ 11 キャプティブ ポータルを設定する場合は、ユーザ制御のためのキャプティブ ポータルの設定方法（2610 ページ）を参照してください。

ステップ 12 （オプション）アイデンティティ ルールに条件を追加するには、ルール条件タイプ （465 ページ）を参照してください。

ステップ 13 [Add] をクリックします。

ステップ 14 ポリシー エディタで、ルールの位置を設定します。クリックしてドラッグするか、または右クリック メニューを使用してカット アンド ペーストを実行します。ルールには 1 から番号が付けられます。システムは、ルール番号の昇順で上から順に、ルールをトラフィックと照合します。トラフィックが一致する最初のルールは、そのトラフィックを処理するルールです。適切なルールの順序を指定することで、ネットワーク トラフィックの処理に必要なリソースが削減され、ルールのプリエンプションを回避できます。

ステップ 15 **[保存（Save）]** をクリックします。

アイデンティティ ルール フィールド

次のフィールドを使用して、アイデンティティ ルールを設定します。

Enabled

このオプションを選択すると、アイデンティティ ポリシーのアイデンティティ ルールが有効になります。このオプションの選択を解除すると、アイデンティティ ルールが無効になります。

Action

指定したレルムでユーザに対して実行する認証のタイプを指定します。これには、[パッシブ認証（Passive Authentication）]（デフォルト）、[アクティブ認証（Active Authentication）]、または [認証なし（No Authentication）] があります。アイデンティティ ルールのアクションとして選択する前に、認証方式、またはアイデンティティ ソースを完全に設定する必要があります。

さらに、VPN が有効になっている場合（少なくとも 1 つの管理対象デバイスで設定されている場合）、リモート アクセス VPN セッションは VPN によってアクティブに認証されます。他のセッションはルール アクションを使用します。つまり、VPN が有効になっている場合は、選択したアクションに関係なく、すべてのセッションで VPN ID の判別が最初に行われます。指定されたレルム上に VPN ID が見つかった場合、これは使用されるアイデンティティ ソースになります。選択されていても、追加のキャプティブ ポータル アクティブ認証は実行されません。

VPN アイデンティティ ソースが見つからない場合は、指定されたアクションに従ってプロセスが続行されます。アイデンティティ ポリシーを VPN 認証のみに制限することはできません。VPN ID が見つからない場合は、選択されたアクションに従ってルールが適用されるためです。

注意 SSL 復号が無効の場合（つまりアクセス コントロール ポリシーに SSL ポリシーが含まれない場合）に、アクティブな最初の認証ルールを追加するか、アクティブな最後の認証ルールを削除すると 設定の変更を展開する際に Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、ターゲット デバイスがトラフィックを処理する方法に応じて異なります。詳細はSnort® の再起動によるトラフィックの動作 （451 ページ）を参照してください。

アクティブ認証ルールには [アクティブ認証（Active Authentication）] ルール アクションが含まれているか、または **[パッシブまたは VPN ID を確立できない場合はアクティブ認証を使用する（Use active authentication if passive or VPN identity cannot be established）]** が選択された [パッシブ認証（Passive Authentication）] ルール アクションが含まれています。

Firepower システムのバージョンでサポートされるパッシブおよびアクティブ認証方式の詳細については、ユーザアイデンティティ ソースについて （2482 ページ）を参照してください。

Realm

指定された**アクション**の実行対象になるユーザが含まれるレルム。アイデンティティ ルールのレルムとして選択する前に、レルムを完全に設定する必要があります。

（注） リモート アクセス VPN が有効で、展開で VPN 認証に RADIUS サーバ グループを使用している場合は、この RADIUS サーバ グループに関連付けられているレルムを指定してください。

（注） [Kerberos]（または [Kerberos] をオプションとする場合は [HTTP ネゴシエート（HTTP Negotiate）]）を、アイデンティティ ルールの [認証プロトコル（Authentication Protocol）] として選択する場合、選択する [レルム（Realm）] は、Kerberos キャプティブ ポータル アクティブ認証を実行できるように、[AD 参加ユーザ名（AD Join Username）] と [AD 参加パスワード（AD Join Password）] を使用して設定する必要があります。

パッシブまたは VPN ID を確立できない場合は、アクティブ認証を使用します。

このオプションを選択すると、パッシブまたは VPN 認証でユーザを識別できない場合にキャプティブ ポータル アクティブ認証を使用してユーザが認証されます。このオプションを選択するには、アイデンティティ ポリシーでキャプティブ ポータル アクティブ認証を設定する必要があります。

このオプションを無効にすると、VPN ID を持たないユーザまたはパッシブ認証では識別できないユーザは、「不明（Unknown）」と識別されます。

認証でユーザを識別できない場合は特別 ID/ゲストとして識別する（Identify as Special Identities/Guest if authentication cannot identify user）

このオプションを選択すると、キャプティブ ポータル アクティブ認証に指定された回数失敗したユーザがゲストとしてネットワークにアクセスできます。これらのユーザは、Firepower Management Console ではユーザ名（ユーザ名が AD または LDAP サーバに存在する場合）または [ゲスト（Guest）]（ユーザ名が不明の場合）で表示されます。これらのユーザのレルムは、アイデンティティ ルールで指定されたレルムです。（デフォルトでは、失敗したログインの数は 3 回です。）

ルール アクションとして [アクティブ認証（Active Authentication）]（つまり、キャプティブ ポータル認証）を設定している場合にのみ、このフィールドが表示されます。

認証プロトコル

キャプティブ ポータル アクティブ認証を実行するために使用する方法です。選択は、レルム、LDAP、または AD のタイプによって異なります。

- 暗号化されていない HTTP 基本認証（BA）接続を使用してユーザを認証するには、[HTTP 基本（HTTP Basic）] を選択します。ユーザはブラウザのデフォルトの認証ポップアップ ウィンドウを使用してネットワークにログインします。

  ほとんどの Web ブラウザは、**HTTP 基本**ログインからクレデンシャルをキャッシュし、古いセッションがタイムアウトした後にシームレスに新しいセッションを開始するためにそのクレデンシャルを使用します。

- NT LAN Manager（NTLM）接続を使用してユーザを認証するには **NTLM** を選択します。この選択はADレルムを選択するときにのみ使用できます。透過的な認証がユーザのブラウザで設定されている場合、ユーザは自動的にログインします。透過的な認証が設定されていない場合、ユーザは各自のブラウザでデフォルトの認証ポップアップ ウィンドウを使用してネットワークにログインします。
- Kerberos 接続を使用してユーザを認証する場合は、[Kerberos] を選択します。この選択は、セキュアLDAP（LDAPS）が有効になっているサーバに対してADレルムを選択する場合にのみ可能です。透過的な認証がユーザのブラウザで設定されている場合、ユーザは自動的にログインします。透過的な認証が設定されていない場合、ユーザは各自のブラウザでデフォルトの認証ポップアップ ウィンドウを使用してネットワークにログインします。

（注） 選択する [レルム（Realm）] は、Kerberos キャプティブ ポータル アクティブ認証を実行するために、[AD 参加ユーザ名（AD Join Username）] および [AD 参加パスワード（AD Join Password）] を使用して設定する必要があります。

（注） Kerberosキャプティブ ポータルを実行するアイデンティティ ルールを作成しようとしており、DNS解決は設定済みである場合は、キャプティブ ポータルデバイスの完全修飾ドメイン名（FQDN）を解決する DNS サーバを設定する必要があります。FQDN は、DNS の設定時に指定したホスト名と一致する必要があります。

ASA with FirePOWER Services および Firepower Threat Defense デバイスの場合、FQDNは、キャプティブ ポータルに使用されるルーテッド インターフェイスの IP アドレスに解決される必要があります。

- キャプティブ ポータル サーバが認証接続にHTTP基本認証、Kerberos、またはNTLMを選択できるようにするには、[HTTP ネゴシエート（HTTP Negotiate）] を選択します。このタイプはADレルムを選択するときにのみ使用できます。

（注） 選択する [レルム（Realm）] は、[HTTP ネゴシエート（HTTP Negotiate）] で Kerberos キャプティブ ポータル アクティブ認証を選択するために、[AD参加ユーザ名（AD Join Username）] および [AD 参加パスワード（AD Join Password）] を使用して設定する必要があります。

（注） [HTTP ネゴシエート（HTTP Negotiate）] キャプティブ ポータルを実行するアイデンティティ ルールを作成しようとしており、DNS 解決は設定済みである場合は、キャプティブ ポータル デバイスの完全修飾ドメイン名（FQDN）を解決する DNS サーバを設定する必要があります。キャプティブ ポータルに使用するデバイスの FQDN は、DNS の設定時に入力したホスト名と一致している必要があります。

ASA with FirePOWER Services デバイスの場合、FQDN は ASA FirePOWER モジュールの FQDN です。

アイデンティティ ポリシーの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	Control	いずれか（Any）	いずれか（Any）	Administrator、Access Admin、Network Admin

始める前に

アイデンティティ ポリシーは、アクセス コントロール ポリシーのレルムでユーザやグループを使用するために必要です。レルムの作成（2576 ページ）の説明に従って 1 つ以上のレルムを作成し、有効にします。

次のすべてに該当する場合、アイデンティティ ポリシーは必要ありません。

- ISE/ISE-PIC アイデンティティ ソースを使用できます。
- アクセス コントロール ポリシーのユーザまたはグループは使用しません。
- アクセス コントロール ポリシーのセキュリティ グループ タグ（SGT）を使用します。詳細については、「ISE SGT とカスタム SGT ルール条件との比較（496 ページ）」を参照してください。

ステップ 1 Firepower Management Center にログインします。

ステップ 2 **[Policies]** > **[Access Control]** > **[Identity]** をクリックし、[新しいポリシー（New Policy）] をクリックします。

ステップ 3 [名前（Name）] を入力し、必要に応じて [説明（Description）] を入力します。

ステップ 4 [保存（Save）] をクリックします。

ステップ 5 ポリシーにルールを追加するには、アイデンティティ ルールの作成 （2638 ページ）で説明されているように、[ルールの追加（Add Rule）] をクリックします。

ステップ 6 ルール カテゴリを作成するには、[カテゴリの追加（Add Category）] をクリックします。

ステップ 7 キャプティブ ポータルのアクティブ認証を設定するには、ユーザ制御のためのキャプティブ ポータルの設定方法 （2610 ページ）で説明されているように、[アクティブ認証（Active Authentication）] タブをクリックします。

ステップ 8 [保存（Save）] をクリックして、アイデンティティ ポリシーを保存します。

次のタスク

- 照合するユーザおよび他のオプションを指定するルールを、アイデンティティ ポリシーに追加します（ アイデンティティ ルールの作成 （2638 ページ）を参照）。
- 指定したリソースへのアクセスを特定のユーザに許可またはブロックするには、このアイデンティティ ポリシーをアクセス コントロール ポリシーに関連付けます（アクセス制御への他のポリシーの関連付け （1684 ページ）を参照）。
- 設定変更を管理対象デバイスに展開します（設定変更の展開 （447 ページ）を参照）。

問題が発生した場合は、ユーザ制御のトラブルシューティング （494 ページ）を参照してください。

関連トピック

ユーザ制御のトラブルシューティング （494 ページ）

アイデンティティ ルールの管理

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	Control	いずれか（Any）	いずれか（Any）	Administrator、Access Admin、Network Admin

ステップ 1 まだ Firepower Management Center にログインしていない場合は、ログインします。

ステップ 2 **[Policies]** > **[Access Control]** > **[Identity]** をクリックします。

ステップ 3 編集するポリシーの横にある編集アイコン（ ）をクリックします。代わりに表示アイコン（ ）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 4 アイデンティティ ルールを編集するには、編集アイコン（ ）をクリックし、アイデンティティ ポリシーの作成 （2643 ページ）の説明に従って変更を行います。

ステップ 5 アイデンティティ ルールを削除するには、削除アイコン（ ）をクリックします。

ステップ 6 ルール カテゴリを作成するには、[カテゴリの追加（Add Category）] をクリックし、位置とルールを選択します。

ステップ 7 **[保存（Save）]** をクリックします。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

アイデンティティ ポリシーの管理

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	Control	いずれか（Any）	いずれか（Any）	Administrator、Access Admin、Network Admin

マルチドメイン展開では、編集できる現在のドメインで作成されたポリシーが表示されます。また、編集できない先祖ドメインで作成されたポリシーも表示されます。下位のドメインで作成されたポリシーを表示および編集するには、そのドメインに切り替えます。

ステップ 1 まだ Firepower Management Center にログインしていない場合は、ログインします。

ステップ 2 **[Policies]** > **[Access Control]** > **[Identity]** をクリックします。

ステップ 3 ポリシーを削除するには、[削除（Delete）]（）をクリックします。 コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 4 ポリシーを編集するには、ポリシーの横にある [編集（Edit）]（）をクリックし、アイデンティティ ポリシーの作成 （2643 ページ）の説明に従って変更を行います。代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 5 ポリシーをコピーするには、コピー アイコン（）をクリックします。

ステップ 6 ポリシーのレポートを生成するには、現在のポリシー レポートの生成 （459 ページ）の説明に従ってレポート アイコン（）をクリックします。

ステップ 7 ポリシーを比較する方法については、ポリシーの比較 （457 ページ）を参照してください。

第 107 章

ネットワーク検出ポリシー

以下のトピックでは、ネットワーク検出ポリシーを作成、設定、管理する方法について説明します。

概要：ネットワーク検出ポリシー

Firepower Management Center 上のネットワーク検出ポリシーは、システムが組織のネットワーク アセットに関するデータを収集する方法と、どのネットワーク セグメントとポートをモニタ対象とするかを制御します。

マルチドメイン展開では、各リーフ ドメインがそれぞれ独立したネットワーク検出ポリシーを使用します。ネットワーク検出ポリシーのルールやその他の設定をドメイン間で共有、継承、コピーすることはできません。新しいドメインを作成するたびに、システムにより、その新しいドメインに対してデフォルト設定を使用したネットワーク検出ポリシーが作成されます。カスタマイズが必要な場合は、新しいポリシーに明示的に適用する必要があります。

Firepower システムがモニタしてトラフィック内のネットワーク データに基づいて検出データを生成するネットワークおよびポート、ポリシーを適用するゾーンは、ポリシー内の検出ルールで指定します。ルール内では、ホスト、アプリケーション、権限のないユーザを検出するかどうかを設定できます。検出からネットワークとゾーンを除外するルールを作成できます。NetFlow エクスポータからのデータの検出を設定して、ネットワーク上でユーザ データが検出されるトラフィックのプロトコルを制限できます。

ネットワーク検出ポリシーに用意されている単一のデフォルト ルールは、すべてのモニタ対象トラフィックからアプリケーションを検出するように設定されています。このルールが除外するネットワーク、ゾーン、ポートはなく、ホストとユーザの検出も設定されていません。また、このルールは NetFlow エクスポータをモニタするように設定されてはいません。このポリシーは、管理対象デバイスが Firepower Management Center に登録されると、デフォルトでその

デバイスに導入されます。ホストまたはユーザデータの収集を開始するには、検出ルールを追加または変更して、ポリシーをデバイスに再展開する必要があります。

ネットワーク検出の範囲を調整する場合は、追加の検出ルールを作成して、デフォルトルールを変更または削除できます。

管理対象デバイスごとのアクセス コントロール ポリシーは、そのデバイスに許可されたトラフィック、つまり、ネットワーク検出を使用してモニタ可能なトラフィックを定義することに注意してください。アクセスコントロールを使用して特定のトラフィックをブロックすると、システムでホスト、ユーザ、またはアプリケーションのアクティビティに関するトラフィックを検査できなくなります。たとえば、アクセスコントロールポリシーでソーシャルネットワーキングアプリケーションへのアクセスをブロックすると、システムはそれらのアプリケーションに関する検出データを一切提供できなくなります。

検出ルールでトラフィック ベースのユーザ検出を有効にすると、一連のアプリケーション プロトコル全体のトラフィック内のユーザ ログイン アクティビティを通して権限のないユーザを検出できます。必要に応じて、すべてのルールにわたって特定のプロトコル内の検出を無効にできます。一部のプロトコルを無効にすると、Firepower Management Center モデルに関連付けられたユーザ制限に達するのを防ぐのに役立ち、他のプロトコルからのユーザに使用可能なユーザ カウントを確保できます。

詳細ネットワーク検出設定を使用すれば、記録するデータの種類、検出データの保存方法、アクティブにする侵害の兆候（IOC）ルール、影響評価に使用する脆弱性マッピング、送信元からの検出データが競合していた場合の対処を管理できます。また、ホスト入力の送信元やNetFlow エクスポータをモニタ対象として追加することもできます。

ネットワーク検出のカスタマイズ

Firepower システムによって収集されるネットワーク トラフィックに関する情報は、この情報を関連付けて最も脆弱で最も重要なネットワークのホストを識別することができる場合に、最もその価値を発揮します。

たとえば、ネットワーク上に SuSE Linux のカスタマイズ バージョンを実行している複数のデバイスがある場合、システムはそのオペレーティング システムを識別することができません。そのため、脆弱性をそれらのホストにマッピングすることはできません。しかし、システムに SuSE Linux に関する脆弱性のリストがあるならば、同じオペレーティング システムを実行する他のホストを識別するために使用できるカスタムフィンガープリントを、ホストのいずれか 1 台に対して作成することができます。フィンガープリントに SuSE Linux の脆弱性リストのマッピングを含め、フィンガープリントに一致する各ホストとそのリストを関連付けることができます。

また、ホストの入力機能を使用して、ホストデータをサードパーティ システムからネットワーク マップに直接入力することもできます。ただし、サードパーティのオペレーティング システムやアプリケーションデータは、脆弱性情報に自動的にマッピングされません。脆弱性を確認し、サードパーティのオペレーティング システム、サーバ、アプリケーション プロトコル データを使用してホストの影響の関連付けを実行する場合、サードパーティ システムからのベンダーとバージョンの情報を、脆弱性データベース（VDB）にリストされているベンダーと

バージョンにマッピングする必要はあります。また、ホストの入力データを継続的に維持する必要がある場合もあります。アプリケーション データを Firepower システムのベンダーおよびバージョン定義にマッピングしたとしても、インポートされたサードパーティの脆弱性はクライアントまたは Web アプリケーションの影響評価に使用されないことに注意してください。

システムがネットワーク上のホストで実行されているアプリケーションプロトコルを識別できない場合は、システムがポートまたはパターンに基づいてアプリケーションを識別できるようにする、ユーザ定義のアプリケーション プロトコル ディテクタを作成できます。また、特定のアプリケーション ディテクタをインポートしたり、アクティブ/非アクティブにしたりすることによって、Firepower システムのアプリケーション検出機能をカスタマイズすることができます。

さらに、Nmap アクティブ スキャナのスキャン結果を使用してオペレーティング システムやアプリケーションデータの検出を置き換えたり、サードパーティの脆弱性で脆弱性リストを拡張したりすることもできます。システムは複数のソースからのデータを照合して、アプリケーションの ID を判別できます。

ネットワーク検出ポリシーの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	リーフのみ	Admin/Discovery Admin

マルチドメイン展開では、各ドメインに個別のネットワーク検出ポリシーがあります。ユーザアカウントで複数のドメインを管理できる場合は、ポリシーを設定するリーフ ドメインに切り替えます。

ステップ 1 **[Policies]** > **[Network Discovery]**を選択します。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 2 ポリシーの次のコンポーネントを設定します。

- 検出ルール：ネットワーク検出ルールの設定 （2650 ページ）を参照してください。
- ユーザのトラフィックベースの検出：トラフィック ベースのユーザ検出の設定 （2661 ページ）を参照してください。
- 高度なネットワーク検出オプション：高度なネットワーク検出オプションの設定 （2662 ページ）を参照してください。
- カスタム オペレーティング システム定義（フィンガープリント）：クライアント用のカスタム フィンガープリントの作成 （2501 ページ）およびサーバ用のカスタム フィンガープリントの作成 （2504 ページ）を参照してください。

ネットワーク検出ルール

ネットワーク検出ルールを使用すれば、ネットワーク マップに対して検出される情報を調整し、必要な特定のデータだけを含めるようにすることができます。ネットワーク検出ポリシー内のルールは順番に評価されます。モニタリング基準が重複したルールを作成できますが、その場合はシステム パフォーマンスに影響する可能性があります。

モニタリングからホストまたはネットワークを除外すると、そのホストまたはネットワークがネットワーク マップに表示されず、それに対するイベントが報告されません。Cisco では、モニタリングからロード バランサ（またはロード バランサ上の特定のポート）と NAT デバイスを除外することを推奨しています。これらのデバイスは紛らわしいイベントを過剰に生成するため、データベースがいっぱいになったり、Firepower Management Center が過負荷になったりする可能性があります。たとえば、監視対象 NAT デバイスが短期間にオペレーティング システムの複数の更新を表示する場合があります。ロード バランサと NAT デバイスの IP アドレスがわかっている場合は、モニタリングからそれらを除外できます。

ヒント システムは、ネットワーク トラフィックを検査することにより、複数のロード バランサと NAT デバイスを識別できます。

加えて、カスタム サーバ フィンガープリントを作成する必要がある場合は、フィンガープリントを行っているホストとの通信に使用されている IP アドレスをモニタリングから一時的に除外する必要があります。そうしないと、ネットワーク マップおよびディスカバリ イベント ビューに、その IP アドレスによって表されるホストに関する不正確な情報が混在することになります。フィンガープリントを作成したら、その IP アドレスをモニタするようにポリシーを設定し直すことができます。

Cisco では、NetFlow エクスポータと Firepower システム管理対象デバイスを使用して、同じネットワーク セグメントをモニタ**しない**ことも推奨しています。重複しないルールを使用してネットワーク検出ポリシーを設定するのが理想です。管理対象デバイスによって生成された重複接続ログはシステムによって破棄されます。ただし、管理対象デバイスと NetFlow エクスポータの両方で検出された接続に関する重複接続ログを破棄することは**できません**。

ネットワーク検出ルールの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	リーフのみ	Admin/Discovery Admin

検出ルールを設定し、ニーズに合わせてホスト データとアプリケーション データの検出を調整できます。

始める前に

- ネットワークデータを検出するトラフィックの接続を記録していることを確認します。接続のロギングのベスト プラクティス （3012 ページ）を参照してください。
- エクスポートされた NetFlow レコードを収集する場合は、NetFlow エクスポータのネットワーク検出ポリシーへの追加 （2668 ページ）の説明に従ってNetFlowエクスポータを追加します。
- ディスカバリ パフォーマンス グラフを表示するには、検出ルールでホスト、ユーザ、およびアプリケーションを有効にする必要があります。これは、システムパフォーマンスに影響を与える可能性があることに注意してください。

ステップ 1 **[Policies]** > **[Network Discovery]**を選択します。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 2 [ルールの追加（Add Rule）] をクリックします。

ステップ 3 アクションと検出されるアセット （2651 ページ）の説明に従って、ルールの[アクション（Action）]を設定します。

ステップ 4 オプションの検出パラメータを設定します。

- ルールアクションを特定のネットワークに制限します。監視対象ネットワークの制限 （2653 ページ）を参照してください。
- ルール アクションを特定のゾーン内のトラフィックに制限します。ネットワーク検出ルールでのゾーンの設定 （2658 ページ）を参照してください。
- ポートをモニタリングから除外します。ネットワーク検出ルールでのポートの除外 （2656 ページ）を参照してください。
- NetFlowデータ検出のルールの設定します。NetFlowデータ検出のルールの設定 （2654 ページ）を参照してください。

ステップ 5 **[保存（Save）]** をクリックします。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

アクションと検出されるアセット

検出ルールを設定する場合は、ルールのアクションを選択する必要があります。アクションの効果は、管理対象デバイスとNetFlowエクスポータのどちらからデータを検出するルールを使用しているかによって異なります。

次の表に、これら2つのシナリオで指定されたアクション設定を使用したルールで検出されるアセットの説明を示します。

表 *262 :* 検出ルールのアクション

操作	オプション	管理対象デバイス	NetFlow エクスポータ
除外（Exclude）	--	指定されたネットワークをモニタリング対象から除外します。接続の発信元ホストまたは宛先ホストを検出から除外すると、接続は記録されますが、除外したホストの検出イベントは作成されません。	指定されたネットワークをモニタリング対象から除外します。接続の発信元ホストまたは宛先ホストを検出から除外すると、接続は記録されますが、除外したホストの検出イベントは作成されません。
Discover	ホスト（Hosts）	検出イベントに基づいて、ネットワーク マップにホストを追加します。（任意。ユーザ検出が有効になっていない場合は必須）。	NetFlow レコードに基づいて、ネットワーク マップにホストを追加し、接続をログに記録します。（必須）
Discover	アプリケーション	アプリケーション検出に基づいて、ネットワーク マップにアプリケーションを追加します。アプリケーションも検出しないルールでは、ホストまたはユーザを検出できないことに注意してください。（必須）	NetFlow レコードと `/etc/sf/services` 内のポートとアプリケーション プロトコルの関連付けに基づいて、ネットワーク マップにアプリケーション プロトコルを追加します。（オプション）
Discover	Users	ネットワーク検出ポリシーで設定されたユーザ プロトコルに関するトラフィック ベースの検出に基づいてユーザをユーザ テーブルに追加し、ユーザ アクティビティをログに記録します。（オプション）	n/a
NetFlow 接続のロギング（Log NetFlow Connections）	--	適用対象外	NetFlow 接続のみを記録します。ホストまたはアプリケーションは検出しません。

ルールを使用して管理対象デバイスのトラフィックをモニタする場合は、アプリケーション ロギングが必要です。ルールを使用してユーザをモニタする場合は、ホスト ロギングが必要です。ルールを使用して、エクスポートされた NetFlow レコードをモニタする場合は、ユーザをログに記録するように設定することはできず、アプリケーション ロギングは任意です。

（注） ネットワーク検出ポリシーの [アクション（Action）] の設定に基づいて、エクスポートされた NetFlow レコードで接続が検出されます。アクセス コントロール ポリシーの設定に基づいて、管理対象デバイス ラフィックで接続が検出されます。

モニタ対象ネットワーク

検出ルールは、モニタ対象アセットの検出を、指定されたネットワーク上のホストとの間のトラフィックだけを対象にして行います。検出ルールでは、指定されたネットワーク内の 1 つ以上の IP アドレスが割り当てられた接続に対して検出が行われ、モニタ対象ネットワーク内の IP アドレスに対してのみイベントが生成されます。デフォルトの検出ルールでは、モニタされているすべてのトラフィックのアプリケーションを検出します（すべての IPv4 トラフィックについては `0.0.0.0/0`、すべての IPv6 トラフィックについては `::/0`）。

NetFlow 検出を処理し、接続データだけを記録するルールを設定すると、システムは、指定のネットワークの接続元と接続先の IP アドレスを記録します。ネットワーク検出ルールが NetFlow ネットワーク接続を記録する唯一の方法を提供することに注意してください。

また、ネットワーク オブジェクトまたはオブジェクト グループを使用してモニタ対象ネットワークを指定することもできます。

監視対象ネットワークの制限

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	リーフのみ	Admin/Discovery Admin

すべての検出ルールに 1 つ以上のネットワークを含める必要があります。

ステップ 1 **[Policies]** > **[Network Discovery]**を選択します。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 2 [ルールの追加（Add Rule）] をクリックします。

ステップ 3 [ネットワーク（Networks）] タブが表示されていない場合は、そのタブをクリックします。

ステップ 4 必要に応じて、[使用可能なネットワーク（Available Networks）] リストにネットワーク オブジェクトを追加します。詳細については、検出ルール設定時のネットワーク オブジェクトの作成（2655 ページ）を参照してください。

（注） ネットワーク検出ポリシーで使用されるネットワーク オブジェクトを変更した場合、その変更は設定の変更を展開するまで反映されません。

ステップ 5 ネットワークを指定します。

- [使用可能なネットワーク（Available Networks）] リストからネットワークを選択します。

  ヒント　ネットワークがすぐにリストに表示されない場合は、リロードアイコン（）をクリックします。

- [使用可能なネットワーク（Available Networks）] ラベルの下にあるテキスト ボックスに IP アドレスを入力します。

ステップ 6　[追加（Add）] をクリックします。

ステップ 7　必要に応じて、別のネットワークを追加するために、前の 2 つの手順を繰り返します。

ステップ 8　[保存（Save）] をクリックして、変更を保存します。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

NetFlow データ検出のルールの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	リーフのみ	Admin/Discovery Admin

Firepower システムでは、NetFlow エクスポータからのデータを使用して、接続および検出イベントを生成したり、ネットワーク マップにホストとアプリケーションのデータを追加したりできます。

検出ルール内で NetFlow エクスポータを選択する場合、ルールは指定されたネットワークの NetFlow データの検出に制限されます。NetFlow デバイスを選択すると使用可能なルール アクションが変更されるため、モニタする NetFlow デバイスを選択してからルール動作の他の側面を設定します。NetFlow エクスポータをモニタするためのポートの除外を設定することはできません。

始める前に

- NetFlow-enabled デバイスをネットワーク検出ポリシーに追加します。NetFlow エクスポータのネットワーク検出ポリシーへの追加 （2668 ページ）を参照してください。

ステップ 1　**[Policies]** > **[Network Discovery]**を選択します。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 2　[ルールの追加（Add Rule）] をクリックします。

ステップ 3　[NetFlow デバイス（NetFlow Device）] タブを選択します。

ステップ 4 [NetFlow デバイス（NetFlow Device）] ドロップダウン リストから、モニタする NetFlow エクスポータの IP アドレスを選択します。

ステップ 5 Firepower システムの管理対象デバイスで収集する NetFlow データのタイプを指定します。

- 接続のみ：[アクション（Action）] ドロップダウン リストから `Log NetFlow Connections` を選択します。
- ホスト、アプリケーション、および接続：[アクション（Action）] ドロップダウン リストから `Discover` を選択します。[ホスト（Hosts）] チェックボックスが自動的にオンになり、接続データの収集が有効になります。オプションで、[アプリケーション] チェックボックスをオンにして、アプリケーション データを収集できます。

ステップ 6 **[保存（Save）]** をクリックします。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

検出ルール設定時のネットワーク オブジェクトの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	リーフのみ	Admin/Discovery Admin

新規ネットワーク オブジェクトを再使用可能なネットワーク オブジェクトおよびグループのリストに追加することで、検出ルールに表示される使用可能なネットワークのリストにそれらのオブジェクトを追加できます。

ステップ 1 **[Policies]** > **[Network Discovery]**を選択します。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 2 [ネットワーク（Networks）] タブで、[ルールの追加（Add Rule）] をクリックします。

ステップ 3 [利用可能なネットワーク（Available Networks）] の隣にある追加アイコン（  ）をクリックします。

ステップ 4 ネットワーク オブジェクトの作成 （527 ページ）の説明に従って、ネットワーク オブジェクトを作成します。

ステップ 5 ネットワーク検出ルールの設定 （2650 ページ）の説明に従って、ネットワーク検出ルールの追加を完了します。

ポート除外

モニタリングからホストを除外できるのと同様に、モニタリングから特定のポートを除外できます。次に例を示します。

- ロードバランサは短期間に同じポート上の複数のアプリケーションを報告する可能性があります。モニタリングからそのポートを除外する（Web ファームを処理するロード バランサ上のポート 80 を除外するなど）ようにネットワーク検出ルールを設定できます。
- 組織で特定の範囲のポートを使用するカスタム クライアントを使用しているとします。このクライアントからのトラフィックが紛らわしいイベントを過剰に生成する場合は、モニタリングからそれらのポートを除外できます。同様に、DNS トラフィックをモニタしないように設定することもできます。この場合は、検出ポリシーがポート 53 をモニタしないように、ルールを設定します。

除外するポートを追加するときには、[利用可能なポート（Available Ports）] リストから再利用可能なポート オブジェクトを選択するのか、送信元または宛先除外リストにポートを直接追加するのか、新しい再利用可能なポートを作成してからそれを除外リストに移動するのかを決定できます。

（注） NetFlow データの検出を処理するルールでポートを除外することはできません。

ネットワーク検出ルールでのポートの除外

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	リーフのみ	Admin/Discovery Admin

NetFlow データ検出を処理するルールにあるポートを除外することはできません。

ステップ 1 **[Policies]** > **[Network Discovery]**を選択します。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 2 [ルールの追加（Add Rule）] をクリックします。

ステップ 3 [ポートの除外（Port Exclusions）] タブをクリックします。

ステップ 4 必要に応じて、検出ルール設定時のポート オブジェクトの作成（2657 ページ）で説明されているように、使用可能なポート リストにポート オブジェクトを追加します。

ステップ 5 次のいずれかの方法を使用して、モニタリング対象から特定の送信元ポートを除外します。

- [使用可能なポート（Available Ports）] リストから 1 つまたは複数のポートを選択して、[送信元に追加（Add to Source）] をクリックします。

- ポート オブジェクトを追加せずに特定の送信元ポートからのトラフィックを除外するには、[選択済の送信元ポート リスト（Selected Source Ports）] で、[プロトコル（Protocol）] を選択し、[ポート（Port）] 番号（1 から 65535 の数値）を入力して、[追加（Add）] をクリックします。

ステップ 6 次のいずれかの方法を使用して、モニタリング対象から特定の宛先ポートを除外します。

- [使用可能なポート（Available Ports）] リストから 1 つまたは複数のポートを選択して、[宛先に追加（Add to Destination）] をクリックします。
- ポート オブジェクトを追加せずに特定の宛先ポートからのトラフィックを除外するには、[選択済の宛先ポート リスト（Selected Destination Ports）] で、[プロトコル（Protocol）] を選択し、[ポート（Port）] 番号を入力して、[追加（Add）] をクリックします。

ステップ 7 [保存（Save）] をクリックして、変更内容を保存します。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

検出ルール設定時のポート オブジェクトの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	リーフのみ	Admin/Discovery Admin

新規ポート オブジェクトを、Firepower システム内の任意の場所で使用できる再使用可能なポート オブジェクトおよびグループのリストに追加することで、検出ルールに表示される使用可能なポートのリストにそれらのオブジェクトを追加できます。

ステップ 1 **[Policies]** > **[Network Discovery]**を選択します。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 2 [ネットワーク（Networks）] タブで、[ルールの追加（Add Rule）] をクリックします。

ステップ 3 [ポートの除外（Port Exclusions）] をクリックします。

ステップ 4 [利用可能なポート（Available Ports）] リストにポートを追加するには、オブジェクトの追加アイコン（）をクリックします。

ステップ 5 [名前（Name）] を入力します。

ステップ 6 [プロトコル（Protocol）] フィールドで、除外するトラフィックのプロトコルを指定します。

ステップ 7 [ポート（Port）] フィールドに、モニタリングから除外するポートを入力します。

単一のポート、ダッシュ（-）を使用したポートの範囲、またはポートとポート範囲のカンマ区切りのリストを指定できます。許容されるポート値は 1 ～ 65535 です。

ステップ 8 [保存（Save）] をクリックします。

ステップ 9 ポートがすぐにリストに表示されない場合は、更新アイコン（  ）をクリックします。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

ネットワーク検出ルールのゾーン

パフォーマンスを向上させるために、ルール内の監視対象ネットワークに物理的に接続されている管理対象デバイス上のセンシング インターフェイスがルール内のゾーンに含まれるように、検出ルールを設定することができます。

残念ながら、ネットワーク設定の変更は通知されないことがあります。ネットワーク管理者が通知せずにルーティングやホストの変更によりネットワーク設定を変更した場合、正しいネットワーク検出ポリシー設定を完全に把握するのが難しくなります。管理対象デバイス上のセンシングインターフェイスがどのようにネットワークに物理的に接続されているかが不明な場合は、ゾーンの設定はデフォルト値のままにしておいてください。このデフォルト値によって、システムは展開環境内のすべてのゾーンに検出ルールを展開します（ゾーンが除外されない場合、システムではすべてのゾーンに検出ポリシーを展開します。）。

ネットワーク検出ルールでのゾーンの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	リーフのみ	Admin/Discovery Admin

ステップ 1 **[Policies]** > **[Network Discovery]**を選択します。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 2 [ルールの追加（Add Rule）] をクリックします。

ステップ 3 [ゾーン（Zones）] タブをクリックします。

ステップ 4 [使用可能なゾーン（Available Zones）] リストでゾーンを選択します。

ステップ 5 [保存（Save）] をクリックして、加えた変更を保存します。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

トラフィック ベース検出のアイデンティティ ソース

トラフィック ベース検出は、Firepower システムでサポートされている唯一の権限のないアイデンティティ ソースです。トラフィック ベース検出を設定すると、管理対象デバイスは、指定したネットワークでの LDAP、AIM、POP3、IMAP、Oracle、SIP（VoIP）、FTP、HTTP、MDNS、SMTP のログインを検出します。トラフィック ベースの検出から取得されたデータは、ユーザ認識にのみ使用できます。権威のあるアイデンティティ ソースとは異なり、トラフィック ベースの検出はネットワーク検出ポリシーで設定します。トラフィック ベースのユーザ検出の設定 （2661 ページ）を参照してください。

次の制限事項に注意してください。

- トラフィック ベースの検出では、LDAP 接続に対する Kerberos ログインのみを LDAP 認証として解釈します。また、管理対象デバイスは、SSL や TLS などのプロトコルを使用して暗号化された LDAP 認証を検出できません。
- トラフィック ベースの検出では OSCAR プロトコルを使用した AIM ログインだけを検出します。TOC2 を使用する AIM ログインは検出できません。
- トラフィック ベースの検出では SMTP ロギングを制限することができません。これは、ユーザが SMTP ログインに基づいてデータベースに追加されていないためです。システムが SMTP ログインを検出しても、一致する電子メール アドレスのユーザがデータベース内に存在しなければ、そのログインは記録されません。

トラフィック ベースの検出は、失敗したログイン試行も記録します。失敗ログイン試行で新しいユーザがデータベース内のユーザのリストに追加されることはありません。トラフィック ベースの検出により検出された失敗ログイン アクティビティのユーザ アクティビティ タイプは [失敗したユーザ ログイン（Failed User Login）] です。

（注） システムは失敗した HTTP ログインと成功した HTTP ログインを区別できません。HTTP ユーザ情報を表示するには、トラフィック ベースの検出設定で [失敗したログイン試行の取得（Capture Failed Login Attempts）] を有効にする必要があります。

注意 ネットワーク検出ポリシーを使用して、HTTP、FTP、MDNS プロトコルを介した非権限、トラフィック ベースのユーザ検出を有効/無効にすると 設定の変更を展開する際に Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、ターゲット デバイスがトラフィックを処理する方法に応じて異なります。詳細はSnort® の再起動によるトラフィックの動作 （451 ページ）を参照してください。

トラフィック ベースの検出データ

デバイスがトラフィック ベースの検出を使用してログインを検出すると、次の情報をユーザ アクティビティとして記録するために Firepower Management Centerに送信します。

- ログインで識別されたユーザ名
- ログインの時刻
- ログインに関係する IP アドレス。このアドレスは、ユーザのホスト（LDAP、POP3、IMAP、およびAIM ログインの場合）、サーバ（HTTP、MDNS、FTP、SMTP およびOracle ログインの場合）、またはセッション発信元（SIP ログインの場合）の IP アドレスになります。
- ユーザの電子メール アドレス（POP3、IMAP、および SMTP ログインの場合）
- ログインを検出したデバイスの名前

ユーザがすでに検出されている場合、Firepower Management Centerはそのユーザのログイン履歴を更新します。Firepower Management Center は POP3 および IMAP ログイン内の電子メールアドレスを使用してLDAPユーザに関連付ける場合があることに注意してください。これは、Firepower Management Center が新しい IMAP ログインを検出して、その IMAP ログイン内の電子メール アドレスが既存のLDAPユーザのアドレスと一致した場合は、IMAP ログインで新しいユーザが作成されるのではなく、LDAP ユーザの履歴が更新されることを意味します。

ユーザが以前に検出されなかった場合、Firepower Management Center はユーザ データベースにユーザを追加します。AIM、SIP、Oracle ログインでは、常に新しいユーザ レコードが作成されます。これは、それらのログイン イベントにはFirepower Management Center が他のログインタイプに関連付けることができるデータが含まれていないためです。

Firepower Management Center は、次の場合に、ユーザ アイデンティティまたはユーザ ID を記録**しません**。

- そのログイン タイプを無視するようにネットワーク検出ポリシーを設定した場合
- 管理対象デバイスが SMTP ログインを検出したものの、ユーザ データベースに電子メール アドレスが一致する、検出済みの LDAP、POP3、または IMAP ユーザが含まれていない場合

ユーザ データはユーザ テーブルに追加されます。

トラフィック ベースの検出戦略

ユーザアクティビティを検出するプロトコルを制限して、検出するユーザの総数を削減することにより、ほぼ完全なユーザ情報を提供していると思われるユーザに焦点を絞ることができます。プロトコルの検出を制限すると、ユーザ名の散乱を最小限に抑え、Firepower Management Center 上の記憶域を節約することができます。

トラフィック ベースの検出プロトコルを選択する際には、以下を検討してください。

- AIM、POP3、IMAP などのプロトコル経由でユーザ名を取得すると、契約業者、訪問者、およびその他のゲストからのネットワーク アクセスによって組織に無関係なユーザ名が収集される可能性があります。
- AIM、Oracle、および SIP ログインは、無関係なユーザ レコードを作成する可能性があります。この現象は、このようなログイン タイプが、システムが LDAP サーバから取得す

るユーザ メタデータのいずれにも関連付けられていないうえ、管理対象デバイスが検出するその他のログイン タイプに含まれている情報のいずれにも関連付けられていないために発生します。そのため、Firepower Management Centerは、これらのユーザとその他のユーザ タイプを関連付けることができません。

トラフィック ベースのユーザ検出の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	リーフのみ	Admin/Discovery Admin

ネットワーク検出ルールでトラフィック ベースのユーザ検出を有効にすると、ホスト検出が自動で有効になります。トラフィック ベースの検出の詳細については、トラフィック ベース検出のアイデンティティ ソース （2659 ページ）を参照してください。

ステップ 1 **[Policies]** > **[Network Discovery]**を選択します。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 2 [ユーザ（Users）] をクリックします。

ステップ 3 編集アイコン（  ）をクリックします。

ステップ 4 ログインを検出するプロトコルのチェック ボックスをオンにするか、ログインを検出しないプロトコルのチェック ボックスをオフにします。

ステップ 5 オプションで、LDAP、POP3、FTP、IMAP トラフィックで検出されたログイン試行の失敗を記録したり、HTTP ログインのユーザ情報を取得するには、[失敗したログイン試行のキャプチャ（Capture Failed Login Attempts）] を有効にします。

ステップ 6 [保存（Save）] をクリックします。

次のタスク

注意 ネットワーク検出ポリシーを使用して、HTTP、FTP、MDNS プロトコルを介した非権限、トラフィック ベースのユーザ検出を有効/無効にすると 設定の変更を展開する際に Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、ターゲット デバイスがトラフィックを処理する方法に応じて異なります。詳細はSnort® の再起動によるトラフィックの動作 （451 ページ）を参照してください。

- ネットワーク検出ルールの設定 （2650ページ）の説明に従って、ユーザを検出するようにネットワーク検出ルールを設定します。

• 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

高度なネットワーク検出オプションの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	リーフのみ	Admin/Discovery Admin

ネットワーク検出ポリシーの [詳細（Advanced）] タブを使用すれば、検出するイベント、検出データの保存期間と更新頻度、影響相関に使用する脆弱性マッピング、およびオペレーティング システム ID とサーバ ID の競合の解決方法に関するポリシー全体の設定を構成できます。加えて、ホスト入力ソースと NetFlow エクスポータを追加して、他のソースからのデータのインポートを許可できます。

（注） 検出イベントとユーザ活動イベントのデータベースイベント制限はシステム構成で設定されます。

ステップ 1 **[Policies]** > **[Network Discovery]** を選択します。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 2 [詳細設定（Advanced）] をクリックします。

ステップ 3 変更する設定の横にある編集アイコン（）または追加アイコン（）をクリックします。

- [データ ストレージ設定（Data Storage Settings）]：ネットワーク検出データ ストレージの設定 （2671 ページ）の説明に従って、設定を更新します。
- [イベント ロギング設定（Event Logging Settings）]：ネットワーク検出イベント ロギングの設定 （2671 ページ）の説明に従って、設定を更新します。
- [全般設定（General Settings）]：ネットワーク検出全般設定 （2663 ページ）の説明に従って、設定を更新します。
- [ID 競合設定（Identity Conflict Settings）]：ネットワーク検出アイデンティティ競合の解決の設定 （2665 ページ）の説明に従って、設定を更新します。
- [侵害の兆候設定（General Settings）]：侵害の兆候ルールの有効化 （2667 ページ）の説明に従って、設定を更新します。
- [NetFlow エクスポータ（NetFlow Exporters）]：NetFlow エクスポータのネットワーク検出ポリシーへの追加 （2668 ページ）の説明に従って、設定を更新します。
- [OS およびサーバの ID ソース（OS and Server Identity Sources）]：ネットワーク検出 OS およびサーバ アイデンティティ ソースの追加 （2672 ページ）の説明に従って、設定を更新します。

- [影響評価に使用する脆弱性（Vulnerabilities to use for Impact Assessment）]：ネットワーク検出の脆弱性影響評価の有効化 （2666 ページ）の説明に従って、設定を更新します。

ステップ 4 **[保存（Save）]** をクリックします。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

関連トピック

データベース イベント数の制限 （1264 ページ）

ネットワーク検出の一般設定

一般設定は、システムがネットワーク マップを更新する頻度と、検出中にサーババナーをキャプチャするかどうかを制御します。

[バナーのキャプチャ（Capture Banners）]

サーバ ベンダーとバージョン（「バナー」）をアドバタイズするネットワーク トラフィックからの見出し情報をシステムで保存させる場合、このチェック ボックスをオンにします。この情報は、収集された情報に追加のコンテキストを提供できます。サーバ詳細にアクセスすることによって、ホストに関して収集されたサーバ バナーにアクセスできます。

Update Interval

システムが情報を更新する時間間隔（ホストの IP アドレスのいずれかが最後に検出された時点、アプリケーションが使用された時点、アプリケーションのヒット数など）。デフォルト設定は 3600 秒（1 時間）です。

更新タイムアウトの時間間隔を短く設定すると、より正確な情報がホスト画面に表示されますが、より多くのネットワーク イベントが生成されることに注意してください。

ネットワーク検出全般設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	リーフのみ	Admin/Discovery Admin

ステップ 1 **[Policies]** > **[Network Discovery]**を選択します。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 2 [詳細設定（Advanced）] をクリックします。

ステップ 3 [全般設定（General Settings）] の横にある編集アイコン（  ）をクリックします。

ステップ 4 ネットワーク検出の一般設定 （2663 ページ）の説明に従って設定を更新します。

ステップ 5 [保存（Save）] をクリックして、全般設定を保存します。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

ネットワーク検出アイデンティティ競合の設定

システムは、オペレーティング システムとサーバのフィンガープリントをトラフィック内のパターンに照合することで、どのオペレーティング システムおよびアプリケーションがホストで実行されているかを判別します。最も信頼できるオペレーティング システムとサーバの ID 情報を提供するために、システムは複数のソースからのフィンガープリント情報を照合します。

システムは、すべてのパッシブ データを使用して、オペレーティング システム ID を抽出し、信頼値を割り当てます。

デフォルトでは、ID 競合が存在しなければ、スキャナまたはサード パーティ アプリケーションによって追加された ID データで、Firepower System によって検出された ID データが上書きされます。[アイデンティティ ソース（Identity Sources）] 設定を使用して、スキャナとサードパーティ アプリケーションのフィンガープリント ソースをプライオリティでランク付けできます。システムはソースごとに 1 つずつの ID を保持しますが、プライオリティが最も高いサードパーティ アプリケーションまたはスキャナ ソースからのデータのみが最新の ID として使用されます。ただし、プライオリティに関係なく、ユーザ入力データによって、スキャナまたはサードパーティ アプリケーションのデータが上書きされることに注意してください。

ID 競合は、[アイデンティティ ソース（Identity Sources）] 設定に列挙されたアクティブ スキャナ ソースまたはサードパーティ アプリケーション ソースと Firepower システム ユーザのどちらかから取得された既存の ID と競合する ID をシステムが検出した場合に発生します。デフォルトでは、ID 競合は自動的に解決されないため、ホスト プロファイルを通して、または、ホストをスキャンし直すか新しい ID データを追加し直してパッシブ ID を上書きすることにより、解決する必要があります。ただし、パッシブ ID またはアクティブな ID のいずれかを維持することで、競合を自動的に解決するようにシステムを設定できます。

[ID 競合イベントを生成する（Generate Identity Conflict Event）]

ID 競合が発生したときにシステムがイベントを生成するかどうかを指定します。

[自動的に競合を解決する（Automatically Resolve Conflicts）]

[自動的に競合を解決する（Automatically Resolve Conflicts）] ドロップダウン リストから、次のいずれかを選択します。

- ID 競合の手動での競合解決を強制する場合は、[無効（Disabled）]

- ID 競合が発生したときにシステムがパッシブ フィンガープリントを使用するようにする場合は、[アイデンティティ（Identity）]
- ID 競合が発生したときにシステムが優先度が最も高いアクティブなソースの現在の ID を使用するようにする場合は、[キープアクティブ（Keep Active）]

ネットワーク検出アイデンティティ競合の解決の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	リーフのみ	Admin/Discovery Admin

ステップ 1 **[Policies]** > **[Network Discovery]**を選択します。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 2 [詳細設定（Advanced）] をクリックします。

ステップ 3 [ID 競合設定（Identity Conflict Settings）] の横にある編集アイコン（  ）をクリックします。

ステップ 4 ネットワーク検出アイデンティティ競合の設定 （2664 ページ）の説明に従って、[ID 競合設定の編集（Edit Identity Conflict Settings）] ポップアップ ウィンドウの設定を更新します。

ステップ 5 [保存（Save）] をクリックして、ID 競合設定を保存します。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

ネットワーク検出の脆弱性の影響の評価オプション

Firepower システムで侵入イベントとの影響相関を実行する方法を設定できます。有効な選択肢は次のとおりです。

- システム ベースの脆弱性情報を使用して影響相関を実行する場合は、[ネットワーク検出の脆弱性マッピングを使用（Use Network Discovery Vulnerability Mappings）] チェックボックスをオンにします。
- サードパーティの脆弱性参照を使用して影響相関を実行する場合は、[サードパーティの脆弱性マッピングを使用（Use Third-Party Vulnerability Mappings）] チェックボックスをオンにします。詳細については、*Firepower* システム ホスト入力 *API* ガイドを参照してください。

チェックボックスのどちらかまたは両方を選択できます。システムが侵入イベントを生成し、選択された脆弱性マッピング セット内の脆弱性のあるサーバまたはオペレーティング システムがそのイベントに関係するホストに含まれている場合、侵入イベントは脆弱（レベル1：赤）影響アイコンでマークされます。ベンダーまたはバージョン情報のないサーバの場合は、Firepower Management Center 構成で脆弱性マッピングを有効にする必要があることに注意してください。

両方のチェックボックスをオフにした場合は、侵入イベントが脆弱（レベル 1：赤）影響アイコンでマークされません。

関連トピック

サードパーティの脆弱性のマッピング （2512 ページ）
サーバの脆弱性のマッピング （1316 ページ）

ネットワーク検出の脆弱性影響評価の有効化

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	リーフのみ	Admin/Discovery Admin

ステップ 1 **[Policies]** > **[Network Discovery]**を選択します。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 2 [詳細設定（Advanced）] をクリックします。

ステップ 3 [影響評価に使用する脆弱性（Vulnerabilities to use for Impact Assessment）] の横にある編集アイコン（  ）をクリックします。

ステップ 4 ネットワーク検出の脆弱性の影響の評価オプション （2665ページ） 説明に従って、[脆弱性設定の編集（Edit Vulnerability Settings）] ポップアップ ウィンドウで設定を更新します。

ステップ 5 [保存（Save）] をクリックして、脆弱性設定を保存します。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ） を参照してください。

侵害の兆候

Firepower システムでは、ネットワーク検出ポリシー内の IOC ルールを使用して悪意のある手段によって侵害されている可能性があるホストを特定します。ホストがこれらのシステム提供のルールで指定されている条件を満たしている場合、そのホストはシステムによって侵害の兆

候（IOC）でタグ付けされます。関連のルールは *IOC* ルールと呼ばれます。各 IOC ルールは 1 種類の IOC タグに対応しています。*IOC* タグは可能性のある侵害の性質を指定します。

次のうちいずれかの事態が発生すると、関与しているホストおよびユーザに Firepower Management Center がタグを付けます。

- システムは、侵入、接続、セキュリティ インテリジェンス、およびファイルまたはマルウェアイベントを使用してモニタ対象のネットワークとそのトラフィックについて集められたデータを関連付け、潜在的な IOC が発生したと判断します。
- Firepower Management Center は AMP クラウドを経由してエンドポイント向け AMP の展開から IOC データをインポートすることができます。このデータがホスト自体の活動（個別のプログラムによってまたはプログラム上で実行されるアクションなど）を検査するため、ネットワーク専用データでは理解するのが難しい可能性がある脅威に対する理解が促されます。便宜上、Firepower Management Center はシスコが開発した新しい IOC タグを AMP クラウドから自動的に取得します。

この機能を設定するには、侵害の兆候ルールの有効化 （2667 ページ）を参照してください。

また、ホストの IOC データに対する相関ルールと、IOC でタグ付けされたホストから成るコンプライアンス ホワイトリストも記述することができます。

タグ付けされた IOC の調査や操作を行うには、侵害の兆候データ （3221 ページ）とそのサブトピック参照してください。

侵害の兆候ルールの有効化

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	リーフのみ	Admin/Discovery Admin

システムで侵害の兆候（IOC）を検出してタグを付けるには、まず、ネットワーク検出ポリシーで 1 つ以上の IOC ルールを有効化する必要があります。IOC ルールのそれぞれが IOC タグの 1 つのタイプに対応します。すべての IOC ルールはシスコが事前定義しています。オリジナルルールを作成することはできません。ネットワークや組織のニーズに合わせて、一部またはすべてのルールを有効にすることができます。たとえば、Microsoft Excel などのソフトウェアを使用しているホストが絶対に監視対象ネットワーク上に出現しない場合は、Excel ベースの脅威に関係する IOC タグを有効にしないようにできます。

ヒント 個別のホストまたはその関連ユーザの IOC ルールを無効にするには、単一ホストまたはユーザにおける侵害の兆候のルール状態の編集 （3225 ページ）を参照してください。

始める前に

IOC ルールは Firepower システムの他のコンポーネントと、AMP for Endpoints によって提供されるデータに基づいてトリガーされるため、これらのコンポーネントが正しくライセンス付与され、IOC タグを設定できるように設定されている必要があります。侵入検知および防御（IPS）および Advanced Malware Protection（AMP）など、有効にする予定の IOC ルールに関連付けられている Firepower システムの機能を有効にします。IOC ルールの関連機能が有効になっていないと、関連データが収集されず、ルールをトリガーできません。

ステップ 1 **[Policies]** > **[Network Discovery]**を選択します。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 2 [詳細設定（Advanced）] をクリックします。

ステップ 3 [侵害の兆候設定（Indications of Compromise Settings）] の横にある編集アイコン（  ）をクリックします。

ステップ 4 IOC 機能全体のオンとオフを切り替えるには、[IOC の有効化（Enable IOC）] の横にあるスライダをクリックします。

ステップ 5 個別の IOC ルールをグローバルに有効または無効にするには、ルールの [有効（Enabled）] 列のスライダをクリックします。

ステップ 6 [保存（Save）] をクリックして IOC ルール設定を保存します。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

NetFlow エクスポータのネットワーク検出ポリシーへの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	リーフのみ	Admin/Discovery Admin

始める前に

- Firepower システムの NetFlow データ （2477 ページ） の説明に従い、使用する NetFlow エクスポータを設定します。
- NetFlow の他の要件については、NetFlow データを使用するための要件 （2477 ページ）の説明を参照してください。

ステップ 1 **[Policies]** > **[Network Discovery]**を選択します。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 2 [詳細設定（Advanced）] をクリックします。

ステップ 3 [NetFlow デバイス（NetFlow Devices）] の横にある追加アイコン（  ）をクリックします。

ステップ 4 [IP アドレス（IP Address）] フィールドに、NetFlow データを収集する対象デバイスの管理を行うネットワークデバイスの IP アドレスを入力します。

ステップ 5 必要に応じて、以下を行います。

- NetFlow エクスポータをさらに追加するには、上記の 2 つのステップを繰り返します。
- 削除アイコン（）をクリックして、NetFlow エクスポータを削除します。検出ルールで NetFlow エクスポータを使用する場合は、先にルールを削除しないと、[詳細（Advanced）] ページからデバイスを削除できないことに注意してください。

ステップ 6 [保存（Save）] をクリックします。

次のタスク

- ネットワーク検出ルールの設定 （2650 ページ） の説明に従い、NetFlow トラフィックをモニタリングするネットワーク検出ルールを設定します。
- 設定変更を展開します。設定変更の展開 （447 ページ） を参照してください。

ネットワーク検出のデータ ストレージ設定

ディスカバリのデータ ストレージ設定では、ホスト制限とタイムアウトの設定が行われます。

ホスト制限の到達時（When Host Limit Reached）

Firepower Management Center がモニタでき、ネットワーク マップに保存できるホストの数。モデルによって異なります。ホスト制限に到達した後に新しいホストを検出すると、[ホスト制限の到達時（When Host Limit Reached）] オプションが制御を行います。次の操作を実行できます。

ホストをドロップ（Drop hosts）

システムは、長期間非アクティブになっているホストをドロップして、新しいホストを追加します。これがデフォルトの設定です。

新しいホストを挿入しない（Don't insert new hosts）

システムは、新たに検出されたホストを追跡しません。システムが新しいホストを追跡するのは、管理者がドメインのホスト制限を増加させた後などに、ホストカウントが制限を下回る場合、ネットワーク マップからホストを手動で削除する場合、またはホストが非アクティブであることからタイムアウトと見なされる場合のみです。

マルチドメイン展開では、リーフ ドメインは使用可能なモニタされたホストのプールを共有します。各リーフ ドメインがネットワーク マップに値を入力できるように、ホスト制限をサブドメイン レベルのドメイン プロパティで設定できます。各リーフ ドメインには独自のネットワーク検出ポリシーがあるため、次の表で説明するように各リーフ ドメインは、システムが新しいホストを検出すると、独自の動作を制御します。

表 *263 :* マルチテナンシーによるホスト制限への到達

設定	ドメインのホスト制限の有無	ドメインのホスト制限に到達した場合	先祖ドメインのホスト制限に到達した場合
ホストをドロップ	Yes	制限付きドメインの最も古いホストをドロップします。	ホストをドロップするように設定されているすべての子孫リーフ ドメインで最も古いホストをドロップします。 ドロップされるホストがなければ、ホストの追加は行われません。
	No	適用対象外	ホストをドロップし、一般プールを共有するように設定されているすべての子孫リーフ ドメインで最も古いホストをドロップします。
新しいホストを挿入しない	YesまたはNo	ホストの追加は行われません。	ホストの追加は行われません。

ホスト タイムアウト（Host Timeout）

システムが、非アクティブであるという理由でネットワーク マップからホストを除外するまでの分単位の時間。デフォルト設定は 10080 分（1 週間）です。ホスト IP アドレスと MAC アドレスは個別にタイムアウトすることができますが、関連するアドレスのすべてがタイムアウトするまで、ホストはネットワーク マップから削除されません。

ホストの早期タイムアウトを避けるために、ホストのタイムアウト値がネットワーク検出ポリシーの一般設定内の更新間隔より長いことを確認します。

サーバ タイムアウト（Server timeout）

システムが、非アクティブであるという理由でネットワーク マップからサーバを除外するまでの分単位の時間。デフォルト設定は 10080 分（1 週間）です。

サーバの早期タイムアウトを避けるために、サービスのタイムアウト値がネットワーク検出ポリシーの一般設定内の更新間隔より長いことを確認します。

クライアント アプリケーションのタイムアウト（Client Application Timeout）

システムが、非アクティブであるという理由でネットワーク マップからクライアントを除外するまでの分単位の時間。デフォルト設定は 10080 分（1 週間）です。

クライアントのタイムアウト値がネットワーク検出ポリシーの一般設定内の更新間隔より長いことを確認します。

関連トピック

Firepower システムのホスト制限 （2490 ページ）
ドメインのプロパティ （435 ページ）

ネットワーク検出データ ストレージの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	リーフのみ	Admin/Discovery Admin

ステップ 1 **[Policies]** > **[Network Discovery]**を選択します。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 2 [詳細設定（Advanced）] をクリックします。

ステップ 3 [データ ストレージ設定（Data Storage Settings）] の横にある編集アイコン（  ）をクリックします。

ステップ 4 ネットワーク検出のデータ ストレージ設定（2669ページ）の説明に従って、[データ ストレージ設定（Data Storage Settings）] ダイアログの設定を更新します。

ステップ 5 [保存（Save）] をクリックして、データ ストレージ設定を保存します。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

ネットワーク検出イベント ロギングの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	リーフのみ	Admin/Discovery Admin

イベント ロギング設定は、検出イベントとホスト入力イベントを記録するかどうかを制御します。イベントを記録しない場合は、イベント ビューで検索することも、相関ルールをトリガーするために使用することもできません。

ステップ 1 **[Policies]** > **[Network Discovery]**を選択します。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 2 [詳細設定（Advanced）] をクリックします。

ステップ 3 [イベント ロギング設定（Event Logging Settings）] の横にある編集アイコン（ ）をクリックします。

ステップ 4 ディスカバリ イベント タイプ（3202 ページ）およびホスト入力イベント タイプ（3207 ページ）の説明に従って、データベースに記録する検出イベント タイプとホスト入力イベント タイプの横にあるチェックボックスをオンまたはオフにします。

ステップ 5 [保存（Save）] をクリックして、イベント ロギング設定を保存します。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

ネットワーク検出 OS およびサーバ アイデンティティ ソースの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	リーフのみ	Admin/Discovery Admin

ネットワーク検出ポリシーの [詳細（Advanced）] タブで、新しいアクティブ ソースを追加し、また、既存の送信元の優先度やタイムアウトの設定を変更できます。

このページにスキャナを追加しても、Nmap スキャナ用の完全な統合機能は追加されませんが、インポートされたサードパーティ アプリケーションまたはスキャン結果の統合が可能になります。

サードパーティ アプリケーションまたはスキャナからデータをインポートする場合は、ソースからの脆弱性がネットワークで検出された脆弱性にマップされていることを確認してください。

ステップ 1 **[Policies]** > **[Network Discovery]**を選択します。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 2 [詳細設定（Advanced）] をクリックします。

ステップ 3 [OS とサーバ ID ソース（OS and Server Identity Sources）] の横にある編集アイコン（  ）をクリックします。

ステップ 4 新しいソースを追加するには、[ソースの追加（Add Sources）] をクリックします。

ステップ 5 名前を入力します。

ステップ 6 ドロップダウン リストからインプット ソースの [タイプ（Type）] を選択します。

- AddScanResult 機能を使用してスキャン結果をインポートする場合は、[スキャナ（Scanner）] を選択します。
- スキャン結果をインポートしない場合は、[アプリケーション（Application）] を選択します。

ステップ 7 このソースによるネットワーク マップへの ID の追加からその ID の削除までの期間を指定するには、[タイムアウト（Timeout）] ドロップダウンリストから、[時間（Hours）]、[日（Days）]、または [週（Weeks）] を選択し、該当する期間を入力します。

ステップ 8 必要に応じて、以下を行います。

- ソースを昇格させて、オペレーティング システム ID とアプリケーション ID よりもリストでは下にあるソースを優先的に使用するには、そのソースを選択して上矢印をクリックします。
- ソースを降格させて、リストで上にあるソースから提供される ID が存在しない場合にのみオペレーティング システム ID とアプリケーション ID を使用するには、そのソースを選択して下矢印をクリックします。
- ソースを削除するには、ソースの横にある削除アイコン（  ）をクリックします。

ステップ 9 [保存（Save）] をクリックして、ID ソース設定を保存します。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

関連トピック

サードパーティの脆弱性のマッピング （2512 ページ）

ネットワーク検出戦略のトラブルシューティング

システムのデフォルトの検出機能に変更を加える前に、実装すべきソリューションを決定できるように、どのホストが正しく識別されていないかと、その原因を分析してください。

管理対象デバイスは正しく配置されていますか

ロードバランサ、プロキシ サーバ、NAT デバイスなどのネットワーク デバイスが、識別されないホストまたは誤って識別されたホストと管理対象デバイスとの間に存在する場合は、カスタム フィンガープリントを使用するのではなく、誤って識別されたホストのより近くに管理対象デバイスを配置します。このシナリオでは、カスタム フィンガープリントの使用は推奨しません。

識別されないオペレーティング システムに一意の TCP スタックがありますか

システムがホストを誤って識別した場合、カスタム フィンガープリントを作成してアクティブにするか、検出（ディスカバリ）データの代わりにNmapまたはホストの入力データを使用するかを決定するために、ホストが誤って識別された理由を調べる必要があります。

⚠

注意 ホストの誤認が発生した場合は、カスタム フィンガープリントを作成する前にサポート担当者にお問い合わせください。

ホストがデフォルトではシステムに検出されないオペレーティング システムを実行していて、識別している TCP スタックの特性を既存の検出されているオペレーティング システムと共有していない場合、カスタム フィンガープリントを作成する必要があります。

たとえば、システムが識別できない一意の TCP スタックで Linux のカスタマイズ バージョンが存在する場合、継続的に自分でデータを更新する必要のあるスキャン結果またはサードパーティのデータを使用するのではなく、システムがホストを監視し続けながらそのホストを識別できるカスタム フィンガープリントを作成すると便利です。

オープン ソースのLinuxディストリビューションの多くは同じカーネルを使用し、システムは Linux カーネル名を使用してそれらを識別します。Red Hat Linux システム用のカスタム フィンガープリントを作成する場合、同じフィンガープリントが複数の Linux ディストリビューションに一致するために、その他のオペレーティング システム（Debian Linux、Mandrake Linux、Knoppix など）が Red Hat Linux として識別されることがあります。

フィンガープリントはすべての状況で使用できるわけではありません。たとえば、ホストのTCPスタックに変更が加えられ、別のオペレーティング システムと類似する(または同じ)ものになることがあります。たとえば、Apple Mac OS X ホストが Linux 2.4 ホストと同じフィンガープリントになるように変更されると、システムはホストを Mac OS X ではなく Linux 2.4 として識別します。Mac OS X ホストのカスタム フィンガープリントを作成すると、すべての正規の Linux 2.4 ホストが誤って Mac OS X ホストとして識別される場合があります。この場合、Nmap が正しくホストを識別するならば、そのホストに対して定期的なNmapスキャンをスケジュールできます。

ホスト入力を使用して、サードパーティ製のシステムからデータをインポートする場合、サーバおよびアプリケーション プロトコルを説明するためにサードパーティが使用するベンダー、製品、およびバージョンの文字列を、それらの製品の Cisco の定義にマッピングする必要があります。アプリケーション データを Firepower システムのベンダーとバージョンの定義にマッピングした場合でも、インポートされたサードパーティ製の脆弱性はクライアントまたはWebアプリケーションの影響評価には使用されないことに注意してください。

システムは複数のソースからのデータを照合して、オペレーティング システムまたはアプリケーションの現在の ID を判別することがあります。

Nmap データの場合、定期的な Nmap スキャンをスケジュールできます。ホスト入力データの場合、インポート用の Perl スクリプトまたはコマンド ライン ユーティリティを定期的に実行できます。ただし、アクティブのスキャン データとホスト入力データは、検出（ディスカバリ）データの頻度で更新されないことがあるので注意してください。

Firepower システムがすべてのアプリケーションを識別できますか

ホストがシステムによって正しく識別されるものの、識別されないアプリケーションがホストにある場合、ユーザ定義のディテクタを作成して、アプリケーションを識別するために役立つポートおよびパターン マッチング情報をシステムに提供することができます。

脆弱性を修正するパッチを適用しましたか

システムがホストを正しく識別するものの、適用した修正が反映されない場合、ホスト入力機能を使用してパッチ情報をインポートすることができます。パッチ情報をインポートする場合、修正名をデータベース内の修正にマッピングする必要があります。

サードパーティ製の脆弱性を追跡しますか

影響の関連付け（相関）に使用したいサードパーティ製システムからの脆弱性情報がある場合、サーバおよびアプリケーションプロトコル用のサードパーティの脆弱性 ID を Cisco のデータベース内の脆弱性 ID にマッピングしてから、ホスト入力機能を使用してそれらの脆弱性をインポートすることができます。ホスト入力機能の使用の詳細については、『*Firepower* システム ホスト入力 *API* ガイド』を参照してください。アプリケーション データを Firepower システムのベンダーとバージョンの定義にマッピングした場合でも、インポートされたサードパーティ製の脆弱性はクライアントまたは Web アプリケーションの影響評価には使用されないことに注意してください。

第 XXIII 部

相関とコンプライアンス

第 108 章

コンプライアンス ホワイトリスト

次のトピックでは、相関ポリシーに追加する前にコンプライアンス ホワイトリストを設定する方法について説明します。

コンプライアンス ホワイトリストの概要

コンプライアンス ホワイトリスト（ホワイトリストと省略されることもある）は、どのオペレーティング システム、アプリケーション（Web とクライアント）、およびプロトコルがネットワーク上のホストで許可されるかを指定する一連の条件です。システムはホストがホワイトリストに違反するとイベントを生成します。

コンプライアンス ホワイトリストには 2 つの主要な構成要素があります。

- ターゲットは、ホワイトリスト評価の対象として選択するホストです。サブネット、VLAN、およびホスト属性で制約して、全部または一部のモニタ対象ホストを評価できます。マルチドメイン展開では、ドメインと、ドメイン内またはドメインをまたいだサブネットを対象にすることができます。
- ホスト プロファイルは、ターゲットのコンプライアンス基準を指定します。グローバル ホストプロファイルはオペレーティング システムに依存しません。1つのホワイトリスト固有として、またはホワイト リスト間で共有される、オペレーティング システム固有のホスト プロファイルを設定することもできます。

Cisco Talos Intelligence Group（Talos）は、推奨設定が指定されたデフォルトのホワイトリストを提供しています。カスタム ホワイトリストを作成することも可能です。単純なカスタム ホワイトリストでは、特定のオペレーティング システムを実行するホストのみを許可できます。より複雑なホワイトリストでは、すべてのオペレーティング システムを許可するとともに、特定のポートで特定のアプリケーション プロトコルを実行する際にホストが使用する必要のあるオペレーティング システムを指定できます。

（注） システムは、エクスポートされたNetFlowレコードからネットワークマップにホストを追加できますが、これらのホストに使用できる情報は限られます（NetFlowデータと管理対象デバイスデータの違い（2478ページ）を参照）。この制限は、コンプライアンスホワイトリストの作成方法に影響する場合があります。

コンプライアンス ホワイトリストの実装

ホワイトリストを実装するには、アクティブな相関ポリシーにホワイトリストを追加します。システムはターゲットを評価し、対応する属性を各ホストに割り当てます。

- 準拠（Compliant）：ホストはホワイトリストに違反していません。
- 非準拠（Non-Compliant）：ホストはホワイトリストに違反しています。
- 評価されていない（Not Evaluated）：ホストがホワイトリストのターゲットではないか、現在評価中であるか、またはシステムに十分な情報がないためホストが準拠しているかどうかを判断できません。

（注） ホスト属性を削除するには、対応するホワイトリストを削除します。1つのホワイトリストを非アクティブ化、削除、または相関ポリシーから削除しても、各ホストのホスト属性は削除**されず**、属性の値が変更されることもありません。

最初の評価後、モニタ対象ホストがアクティブなホワイトリストに違反するたびにホワイトリストイベントが生成されます。また、ホワイトリスト違反が記録されます。

ワークフロー、ダッシュボード、およびネットワークマップを使用して、システム全体のコンプライアンスアクティビティをモニタし、個々のホストがホワイトリストにいつどのように違反したのかを判断できます。修復およびアラートでホワイトリスト違反に自動的に応答することもできます。

例：Web サーバへの HTTP の制限

セキュリティポリシーは、Webサーバのみが HTTP を実行できることを指定しています。HTTP を実行しているホストを特定するために Web ファーム以外のネットワーク全体を評価するホワイトリストを作成します。

ネットワークマップとダッシュボードを使用して、ネットワークのコンプライアンスの概要を一目で把握できます。数秒で、ポリシーに違反して HTTP を実行している組織内のホストを正確に特定して適切に対処できます。

その後で、相関機能を使用して、Web ファーム内に存在しないホストが HTTP の実行を開始するたびに警告するようにシステムを設定できます。

関連トピック

相関ポリシーの設定 （2699 ページ）

コンプライアンス ホワイトリストのターゲット ネットワーク

ターゲット ネットワークは、ホワイトリスト コンプライアンス評価の対象となるホストを指定します。ホワイトリストには、複数のターゲット ネットワークを含めることができ、いずれかのターゲットの基準を満たすホストが評価されます。

最初は、ターゲット ネットワークは IP アドレスまたはアドレス範囲で制約されています。マルチドメイン展開では、初期の制約にドメインも含まれます。

システム提供のデフォルトのホワイトリストでは、すべての監視対象ホスト 0.0.0.0/0 および ::/0 がターゲット設定されています。マルチドメイン展開では、デフォルトのホワイトリストはグローバル ドメインに制約されています（グローバル ドメインでのみ使用可能です）。

ホストがホワイトリストに対して有効ではなくなるようにターゲット ネットワークまたはホストを変更すると、ホストはホワイトリストで評価されなくなり、準拠と非準拠のいずれとしてもみなされなくなります。

ターゲット ネットワークの調査と改善

ホワイトリストにターゲット ネットワークを追加すると、システムにより、準拠ホストの特徴を確認できるようにネットワーク マップを調査するよう求められます。調査により、ターゲットは、調査済みのホストを表すホワイトリストに追加されます。

サブネットまたは個別のホストを調査できます。マルチドメイン展開では、ドメイン全体を調査することも、ドメインをまたいで調査することもできます。先祖ドメインを調査すると、システムによってこのドメインの子孫が調査されます。

追加されたターゲットに加えて、調査では、調査で検出されたオペレーティング システムごとに 1 つのホスト プロファイルがホワイトリストに入力されます。デフォルトで、これらのホスト プロファイルは、システムが該当するオペレーティング システム上で検出したクライアント、アプリケーション プロトコル、Web アプリケーション、およびプロトコルのすべてを許可します。

ターゲット ネットワークを調査（または調査をスキップ）した後、対象を絞り込みます。IP アドレスを使用してホストを除外するか、ホスト属性または VLAN によりターゲット ネットワークを制約します。

コンプライアンス ホワイトリストを使用したドメインの対象化

マルチドメイン展開では、ドメインとターゲット ネットワークは密接にリンクされています。

- リーフ ドメインの管理者は、自分のリーフ ドメイン内のホストを評価するホワイトリストを作成できます。
- 上位ドメインの管理者は、ドメインをまたいでホストを評価するホワイトリストを作成できます。同じホワイトリストで、ドメインの異なるさまざまなサブネットを対象にすることができます。

グローバル ドメインの管理者であり、展開全体の Web サーバに同じコンプライアンス基準を導入する必要があるというシナリオを考えてみます。コンプライアンス基準を定義するグローバル ドメインに 1 つのホワイトリストを作成できます。次に、各リーフ ドメイン内の Web サーバの IP スペース（または個別の IP アドレス）を指定するターゲット ネットワークを使用して、ホワイトリストを制約します。

（注） リーフ ドメインの IP アドレスと範囲を対象にすることに加えて、上位のドメインを使用してターゲットネットワークを制約することもできます。上位ドメインのサブネットを対象にすることにより、各子孫リーフ ドメインの同じサブネットが対象となります。 システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。

コンプライアンス ホワイト リストのホスト プロファイル

コンプライアンス ホワイト リストにおいて、ホスト プロファイルは、ターゲット ホスト上で実行を許可するオペレーティング システム、クライアント、アプリケーション プロトコル、Web アプリケーション、およびプロトコルを指定します。コンプライアンス ホワイト リストで使用できるホスト プロファイルは 3 種類あります。3 種類のホスト プロファイルはそれぞれ、エディタ上での表示が異なります。

表 *264 :* コンプライアンス ホワイト リストのホスト プロファイル タイプ

ホスト プロファイル タイプ	表示	説明
グローバル	すべてのオペレーティング システム	オペレーティング システムに関係なく、ターゲット ホスト上で実行が許可されている内容を指定します。
オペレーティング システム別	プレーン テキストで表示	特定のオペレーティング システムを使用するターゲット ホスト上で実行が許可されている内容を指定します。
共有	イタリックで表示	複数のホワイト リストで使用可能なオペレーティング システム条件を指定します。

オペレーティング システム固有のホスト プロファイル

コンプライアンス ホワイト リストでは、オペレーティング システム固有のホスト プロファイルで、ネットワーク上での実行を許可するオペレーティング システムだけでなく、それらのオペレーティング システム上での実行を許可するアプリケーション プロトコル、クライアント、Web アプリケーション、およびプロトコルも指定します。

たとえば、準拠ホストでは Microsoft Windows の特定のバージョンを実行することを要件にすることができます。別の例として、SSH の実行を Linux ホストのポート 22 で許可した上で、SSH クライアントのベンダーとバージョンをさらに制限することもできます。

ネットワーク上での実行を許可するオペレーティング システムごとに 1 つのホスト プロファイルを作成します。ネットワーク上でオペレーティング システムを禁止する場合は、そのオペレーティング システム用のホスト プロファイルを作成しないでください。たとえば、ネットワーク上のすべてのホストで Windows が実行されるようにするには、そのオペレーティング システム用のホスト プロファイルのみを含めるようにホワイト リストを設定します。

（注） 未確認ホストは、確認されるまで、すべてのホワイトリストに準拠していると見なされます。ただし、不明ホストのホワイト リスト ホスト プロファイルを作成することはできます。未確認ホストとは、オペレーティング システムを識別するために十分な情報が収集されていないホストのことです。不明ホストとは、既知のフィンガープリントと一致しないオペレーティング システムを使用しているホストのことです。

共有ホスト プロファイル

コンプライアンス ホワイトリストでは、共有ホスト プロファイルが特定のオペレーティング システムに関連付けられますが、それぞれの共有ホストプロファイルを複数のホワイトリスト内で使用できます。

たとえば、世界中にオフィスがあり、拠点ごとに別々のホワイトリストを使用する一方、Apple Mac OS X を実行しているすべてのホストに対しては常に同じプロファイルを使用するとします。その場合、該当するオペレーティング システム用の共有プロファイルを作成し、そのプロファイルをすべてのホワイトリストで使用するという方法があります。

デフォルト ホワイトリストでは、組み込みホスト プロファイルと呼ばれる特殊なカテゴリの共有ホスト プロファイルが使用されます。これらのプロファイルは、組み込みのアプリケーション プロトコル、Web アプリケーション、プロトコル、クライアントを使用します。コンプライアンス ホワイトリスト エディタでは、システムはこれらのプロファイルを組み込みホスト プロファイル アイコン（  ）で示します。

マルチドメイン展開では、現在のドメインで作成された共有ホストプロファイルが表示されます。これは、編集が可能なプロファイルです。先祖ドメインで作成された共有ホストプロファイルも表示されますが、これは編集できません。下位のドメインで作成された共有ホストプロファイルを表示および編集するには、そのドメインに切り替えます。

（注） 共有ホストプロファイル（組み込みプロファイルを含む）を変更したり、組み込みアプリケーションプロトコル、プロトコル、クライアントを変更したりすると、そのプロファイルを使用するすべてのホワイトリストに変更が適用されます。意図しない変更を加えた場合や、該当する組み込みの要素を削除した場合は、工場出荷時の初期状態にリセットできます。

ホワイト リスト違反のトリガー

ホストのホワイト リスト コンプライアンスは、システムで次のことが発生すると変化する場合があります。

- ホストのオペレーティング システムの変更を検出
- ホストのオペレーティング システムまたはホスト上のアプリケーション プロトコルに関するアイデンティティの競合を検出
- ホスト上でアクティブになっている新しい TCP サーバ ポート（SMTP または Web サーバによって使用されるポートなど）、または、ホスト上で実行中の新しい UDP サーバを検出
- ホスト上で実行中の検出された TCP サーバまたは UDP サーバで、アップグレードのためのバージョン変更などの変更を検出
- ホスト上で実行中の新しいクライアント アプリケーションまたは Web アプリケーションを検出
- クライアント アプリケーションまたは Web アプリケーションを非アクティブを理由にそのデータベースからドロップ
- ホストが新しいネットワークまたはトランスポート プロトコルと通信していることを検出
- 新しいジェイルブレイクされたモバイル デバイスを検出
- ホスト上で TCP ポートまたは UDP ポートが閉じられたか、タイムアウトしたことを検出

さらに、ホスト入力機能またはホスト プロファイルを使用して次の操作を実行することによって、ホストのコンプライアンスの変化をトリガーできます。

- ホストにクライアント、プロトコル、またはサーバを追加する
- ホストからクライアント、プロトコル、またはサーバを削除する
- ホストのオペレーティング システム定義を設定する
- ホストが有効なターゲットでなくなるようにホストのホスト属性を変更する

（注） 非常に多数のイベントが発生しないように、システムでは、その最初の評価に基づいて非準拠のホストにホワイト リスト イベントを生成せず、またユーザがアクティブなホワイト リストまたは共有ホスト プロファイルを変更した結果としてホストを非準拠にしません。ただし、違反は記録されます。すべての非準拠ターゲットに対してホワイト リスト イベントを生成する場合は、検出データを消去してください。ネットワーク アセットを再検出すると、ホワイト リスト イベントをトリガーすることがあります。

例：オペレーティング システムのコンプライアンス

ホワイト リストで Microsoft Windows ホストのみがネットワーク上で許可されるように指定されている場合、システムでは、Mac OS X を実行中のホストを検出するとホワイト リスト イベントを生成します。さらに、ホワイト リストに関連付けられているホスト属性が、そのホストに関して [準拠（Compliant）] から [非準拠（Non-Compliant）] に変更されます。

この例のホストが [準拠（Compliant）] に復帰するには、次のいずれかが行われる必要があります。

- Mac OS X オペレーティング システムを許可するようにホワイト リストを編集する
- ホストのオペレーティング システム定義を手動で Microsoft Windows に変更する
- オペレーティング システムが変更されて Microsoft Windows に戻ったことをシステムが検出する

例：非準拠のアセットをネットワーク マップから削除する

ホワイト リストで FTP の使用が許可されていない場合に、アプリケーション プロトコルのネットワーク マップ、またはイベント ビューから FTP を削除すると、FTP を実行中のホストは準拠になります。ただし、システムがこのアプリケーション プロトコルを再度検出すると、システムによってホワイト リスト イベントが生成され、そのホストは非準拠になります。

例：完全な情報に基づいてのみトリガーを実行

ホワイト リストでポート 21 で TCP FTP トラフィックだけを許可していた場合、システムでポート 21/TCP で不明なアクティビティを検出すると、ホワイト リストはトリガーを実行しません。ホワイト リストがトリガーを実行するのは、システムがトラフィックを FTP 以外のトラフィックとして識別するか、またはユーザがホスト入力機能を使用してトラフィックを非 FTP トラフィックとして指定した場合だけです。システムは、部分的な情報のみを使用して違反を記録することはありません。

コンプライアンス ホワイト リストの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin

ホワイト リストを作成する際には、ネットワークを調べて最初のターゲットを作成するよう求めるプロンプトが表示されます。これは、コンプライアンスに準拠するホストの特徴を指定するのに役立ちます。

ステップ 1 **[Policies]** > **[Correlation]** を選択し、[ホワイト リスト（White List）] タブをクリックします。

ステップ 2 [新規ホワイト リスト（New White List）] をクリックします。

ステップ 3 必要に応じて、最初のターゲット ネットワークの [IP アドレス（IP Address）] および [ネットマスク（Netmask）] を入力します。マルチドメイン導入では、ターゲット ネットワークが存在する [ドメイン（Domain）] を選択します。

ヒント モニタリング対象のネットワーク全体を調査するには、デフォルト値の 0.0.0.0/0 と ::/0 を使用します。

（注） ターゲット ネットワークのドメインを選択した後は、ドメインを変更できません。より高いレベルのドメインのサブネットをターゲットにすると、各子孫リーフ ドメイン内の同じサブネットがターゲットになります。 システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。

ステップ 4 ターゲット ネットワークを追加します。

- [追加（Add）]：調査せずにターゲット ネットワークを追加する場合は、[追加（Add）] をクリックします。
- [ネットワークの追加および調査（Add and Survey Network）]：ターゲット ネットワークを追加して調査する場合は、[ネットワークの追加および調査（Add and Survey Network）] をクリックします。
- [スキップ（Skip）]：ネットワークを調査せずにホワイトリストを作成する場合は、[スキップ（Skip）] をクリックします。

ステップ 5 必要に応じて、ホワイト リストの新しい [名前（Name）] および [説明（Description）] を入力します。

ステップ 6 必要に応じて、[脱獄モバイルデバイスを許可（Allow Jailbroken Mobile Devices）] を選択して、ネットワークで脱獄モバイルデバイスを許可します。このオプションを無効にすると、ジェイルブレイクされたデバイスによってホワイトリスト違反が生成されます。

ステップ 7 コンプライアンスホワイトリストのターゲットネットワークの設定（2687ページ）の説明に従って、1つ以上の [ターゲット ネットワーク（Target Network）] をホワイト リストに追加します。

ステップ 8 [許可されるホスト プロファイル（Allowed Host Profiles）] を使用して、準拠ホストの特徴を指定します。

- グローバル ホスト プロファイル：ホワイト リストのグローバル ホスト プロファイルを編集するには、[任意のオペレーティング システム（Any Operating System）] をクリックし、ホワイト リスト ホスト プロファイルの作成（2688 ページ）の説明に従います。
- 調査済みプロファイルの編集：ネットワーク調査によって作成された既存のオペレーティング システム固有のホスト プロファイルを編集するには、その名前をクリックし、ホワイト リスト ホスト プロファイルの作成（2688 ページ）の説明に従います。
- 新規プロファイルの作成：このホワイト リストに新しいオペレーティング システム固有のホスト プロファイルを作成するには、[許可されるホスト プロファイル（Allowed Host Profiles）] の隣にある追加アイコン（）をクリックし、ホワイトリストホストプロファイルの作成（2688ページ）の説明に従います。

- 共有ホストプロファイルの追加：ホワイトリストに既存の共有ホストプロファイルを追加するには、[共有ホスト プロファイルの追加（Add Shared Host Profile）] をクリックし、追加する共有ホスト プロファイルを選択して、[OK] をクリックします。共有ホスト プロファイルは斜体で表示されます。

ステップ 9 [ホワイト リストの保存（Save White List）] をクリックします。

次のタスク

- 相関ポリシーの設定（2699ページ）の説明に従って、アクティブな相関ポリシーにホワイト リストを追加します。システムはすぐにホワイト リストの評価および違反の生成を開始します。

関連トピック

コンプライアンス ホワイトリストのターゲット ネットワーク （2681 ページ）
選択したホストに基づいたコンプライアンスのホワイト リストの作成 （3218 ページ）
Firepower システムの IP アドレス表記法 （20 ページ）

コンプライアンス ホワイト リストのターゲット ネットワークの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin

ターゲット ネットワークを追加するときには、ターゲット ネットワークを調査して、準拠しているホストを特定することができます。この調査によって、調査で検出された各オペレーティング システムの 1 つのホスト プロファイルがホワイトリストに追加されます。これらのホスト プロファイルは、システムが該当するオペレーティング システム上で検出したクライアント、アプリケーション プロトコル、Web アプリケーション、およびプロトコルのすべてを許可します。

ステップ 1 コンプライアンス ホワイト リスト エディタで、[ターゲット ネットワークの追加（Add Target Network）] をクリックします。
ステップ 2 ターゲット ネットワークの [IP アドレス（IP Address）] と [ネットマスク（Netmask）] を入力します。
ステップ 3 マルチドメイン展開では、ターゲット ネットワークが存在する [ドメイン（Domain）] を選択します。

（注） ターゲット ネットワークのドメインを選択した後は、ドメインを変更できません。より高いレベルのドメインのサブネットをターゲットにすると、各子孫リーフ ドメイン内の同じサブネットがターゲットになります。 システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。

ステップ 4 ターゲット ネットワークを追加します。

- 追加（Add）：調査なしでターゲット ネットワークを追加するには、[追加（Add）] をクリックします。
- ネットワークの追加と調査（Add and Survey Network）：ターゲット ネットワークを追加および調査するには、[ネットワークの追加と調査（Add and Survey Network）] をクリックします。

ステップ 5 必要に応じて、新しいターゲットをクリックしてさらに構成します。

- 名前（Name）：新しい [名前（Name）] を入力します。
- ネットワークの追加（Add Networks）：追加のホストをターゲットにするには、追加アイコン（  ）をクリックして、[IP アドレス（IP Address）] と [ネットマスク（Netmask）] を入力します。ネットワークをホワイト リスト コンプライアンスから除外するには、[除外（Exclude）] を選択します。
- ホスト属性の追加（Add Host Attributes）：特定のホスト属性を持つホストをターゲットにするには、追加アイコン（  ）をクリックして、[属性（Attribute）] とその [値（Value）] を指定します。
- VLAN の追加（Add VLANs）：VLAN をターゲットにするには、追加アイコン（  ）をクリックして VLAN 番号を入力します（802.1q VLAN の場合）。
- 削除（Delete）：ターゲット制限を削除するには、削除アイコン（  ）をクリックします。

ステップ 6 最後に保存した後で行ったすべての変更をすぐに実装するには、[ホワイトリストの保存（Save White List）] をクリックします。

関連トピック

コンプライアンス ホワイトリストのターゲット ネットワーク （2681 ページ）
Firepower システムの IP アドレス表記法 （20 ページ）

ホワイト リスト ホスト プロファイルの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin

ホストプロファイルは、ターゲットホスト上での実行を許可するオペレーティング システム、クライアント、アプリケーション プロトコル、Web アプリケーション、およびプロトコルといった、ホワイトリストの適合基準を指定します。

すべてのホワイト リストには、オペレーティング システムに依存しないグローバル ホスト プロファイルがあります。たとえば、Mozilla Firefox を許可するように複数の Microsoft Windows ホスト プロファイルと Linux ホスト プロファイルを編集する代わりに、検出されたオペレーティング システムに関係なく、Firefox を許可するようにグローバル ホスト プロファイルを設定できます。

また、各オペレーティング システム専用のホスト プロファイルを設定できます。これは、単一のホワイトリスト専用としても、複数のホワイトリストの共有プロファイルとしても設定できます。

（注） 共有ホストプロファイル（組み込みプロファイルを含む）を変更したり、組み込みアプリケーションプロトコル、プロトコル、クライアントを変更したりすると、そのプロファイルを使用するすべてのホワイトリストに変更が適用されます。意図しない変更を加えた場合や、該当する組み込みの要素を削除した場合は、工場出荷時の初期状態にリセットできます。

始める前に

- コンプライアンスホワイトリストの編集（2694ページ）の説明に従い、ホワイトリスト内でホストプロファイルを作成または編集します。または、共有ホストプロファイルの管理（2695 ページ）の説明に従い、共有ホストプロファイルを作成または編集します。

ステップ 1 ホワイトリスト適合ホストプロファイル エディタで、以下のホストプロファイルを設定します。

- 名前：[名前（Name）] を入力します。
- オペレーティング システム：ホスト プロファイルを特定のオペレーティング システム専用にするには、[OS ベンダ（OS Vendor）]、[OS 名（OS Name）]、[バージョン（Version）] ドロップダウンリストを使用します。グローバルホストプロファイルはすべてのオペレーティング システムを実行するホストへ適用されることを目的としたプロファイルであるため、これに制限を設定することはできません。
- アプリケーションプロトコル：アプリケーションプロトコルを許可するには、追加アイコン（）をクリックし、アプリケーション プロトコルのホワイトリスト （2690 ページ）の説明に従います。
- クライアント：クライアントを許可するには、追加アイコン（）をクリックし、クライアントのホワイトリスト （2691 ページ）の説明に従います。
- Web アプリケーション：Web アプリケーションを許可するには、追加アイコン（）をクリックし、Web アプリケーションのホワイトリスト （2691 ページ）の説明に従います。
- プロトコル：プロトコルを許可するには、追加アイコン（）をクリックし、プロトコルのホワイトリスト （2692 ページ）の説明に従います。
- 削除：一度許可した項目への許可を解除するには、削除アイコン（）をクリックします。
- プロパティの編集：許可されているアプリケーション プロトコルのプロパティ、クライアント、プロトコルを編集するには、その名前をクリックします。変更は、変更した要素を使用する各ホストプロファイルに反映されます。

ヒント プロファイルに一致するホストにすべてのアプリケーションプロトコル、クライアント、web アプリケーションを許可するには、該当する [すべて許可（Allow all...）] チェックボックスを選択します。

ステップ 2 最後の保存以降に施した変更をすぐに適用するには、[ホワイトリストを保存（Save White List）]（または、共有ホストプロファイルを編集している場合は [すべてのプロファイルを保存（Save All Profiles）]）をクリックします。

アプリケーション プロトコルのホワイトリスト

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin

ホワイトリスト ホスト プロファイルを使用して、グローバルにまたは特定のオペレーティング システムに対して、アプリケーション プロトコルのホワイトリストを作成できます。オプションで、ポート、ベンダー、バージョンによって、アプリケーションプロトコルを制限できます。たとえば、ポート 22/TCP で、Linux ホスト上で実行する OpenSSH の特定のバージョンを許可することができます。

ステップ 1 ホワイトリスト ホスト プロファイルを作成または変更しているときに、[許可されるアプリケーション プロトコル（Allowed Application Protocols）]（またはグローバル ホスト プロファイルを変更している場合は [グローバルに許可されるアプリケーション プロトコル（Globally Allowed Application Protocols）]）の横にある追加アイコン（  ）をクリックします。

ステップ 2 次の 2 つの対処法があります。

- 許可するアプリケーション プロトコルが表示されたら、これらを選択します。Web インターフェイスには、ホワイトリストによって、過去に許可されたアプリケーション プロトコル、または今許可しようとしているアプリケーション プロトコルが表示されます。
- リストにないアプリケーション プロトコルを許可するには、[<新規アプリケーション プロトコル>（<New Application Protocol>）] を選択し、[OK] をクリックしてアプリケーション プロトコル エディタを表示します。許可するアプリケーションプロトコル[タイプ（Type）] と [プロトコル（Protocol）] を選択します。オプションで、[ポート（port）]、[ベンダー（Vendor）]、[バージョン（Version）] によって、アプリケーション プロトコルを制限します。

  （注） アプリケーションのテーブル ビューに表示されているとおり正確にベンダーやバージョンを入力する必要があります。ベンダーまたはバージョンを指定しなかった場合は、タイプとプロトコルが一致している限り、ホワイトリストではすべてのベンダーとバージョンが許可されます。

ステップ 3 [OK] をクリックします。

ステップ 4 最後に保存した後に加えられたすべての変更をすぐに実施するには、[ホワイトリストの保存（Save White List）] をクリックします。

クライアントのホワイトリスト

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin

ホワイトリスト ホスト プロファイルを使用して、グローバルにまたは特定のオペレーティング システムに対して、クライアントのホワイトリストを作成できます。オプションで、クライアントを特定のバージョンに限定することができます。たとえば、Microsoft Windows ホスト上での実行を Microsoft Internet Explorer 10 のみに許可することができます。

ステップ 1 ホワイトリストホストプロファイルを作成または変更しているときに、[許可されるクライアント（Allowed Clients）]（またはグローバル ホスト プロファイルを変更している場合は [グローバルに許可されるクライアント（Globally Allowed Clients）]）の横にある追加アイコン（  ）をクリックします。

ステップ 2 次の 2 つの対処法があります。

- 許可するクライアントが表示されたら、これらを選択します。Web インターフェイスには、ホワイトリストによって、過去に許可されたクライアント、または今許可しようとしているクライアントが表示されます。
- リストにないクライアントを許可するには、[<新規クライアント>（<New Client>）] を選択し、[OK] をクリックしてクライアント エディタを表示します。ドロップダウン リストから許可する [クライアント（Client）] を選択し、オプションで許可するクライアントの [バージョン（Version）] を制限します。

  （注） クライアントのテーブル ビューに表示されているとおり正確にバージョンを入力する必要があります。バージョンを指定しない場合、ホワイトリストはすべてのバージョンを許可します。

ステップ 3 [OK] をクリックします。

ステップ 4 最後に保存した後に加えられたすべての変更をすぐに実施するには、[ホワイトリストの保存（Save White List）] をクリックします。

Web アプリケーションのホワイトリスト

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin

ホワイトリスト ホスト プロファイルを使用して、グローバルにまたは特定のオペレーティング システムに対して、Web アプリケーションのホワイトリストを作成できます。

ステップ 1 ホワイト リスト ホスト プロファイルを作成または変更しているときに、[許可される Web アプリケーション（Allowed Web Applications）]（またはグローバル ホスト プロファイルを変更している場合は [グローバルに許可される Web アプリケーション（Globally Allowed Web Applications）]）の横にある追加アイコン（）をクリックします。

ステップ 2 許可する Web アプリケーションを選択します。

ステップ 3 [OK] をクリックして、

ステップ 4 最後に保存した後に加えられたすべての変更をすぐに実施するには、[ホワイトリストの保存（Save White List）] をクリックします。

プロトコルのホワイトリスト

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin

ホワイトリスト ホスト プロファイルを使用して、グローバルにまたは特定のオペレーティング システムに対して、プロトコルのホワイトリストを作成できます。ARP、IP、TCP、UDP は、常にすべてのホスト上での実行が許可されます。これらを禁止することはできません。

ステップ 1 ホワイトリスト ホスト プロファイルを作成または変更しているときに、[許可されるプロトコル（Allowed Protocols）]（またはグローバル ホスト プロファイルを変更している場合は [グローバルに許可されるプロトコル（Globally Allowed Protocols）]）の横にある追加アイコン（）をクリックします。

ステップ 2 次の 2 つの対処法があります。

- 許可するプロトコルが表示されたら、これらを選択します。Web インターフェイスには、ホワイトリストによって、過去に許可されたプロトコル、または今許可しようとしているプロトコルが表示されます。
- リストにないプロトコルを許可するには、[<新規プロトコル>（<New Protocol>）] を選択し、[OK] をクリックしてプロトコル エディタを表示します。[タイプ（Type）] ドロップダウン リストから、プロトコル タイプ（[ネットワーク（Network）] や [トランスポート（Transport）]）を選択し、ドロップダウン リストから [プロトコル（Protocol）] を選択します。

  ヒント リスト内に存在しないプロトコルを指定するには、[その他 (手動入力)（Other (manual entry)）] を選択します。ネットワーク プロトコルの場合は、http://www.iana.org/assignments/ethernet-numbers/ に記載されている適切な番号を入力します。トランスポート プロトコルの場合は、http://www.iana.org/assignments/protocol-numbers/ に記載されている適切な番号を入力します。

ステップ 3 [OK] をクリックします。

ステップ 4 最後に保存した後に加えられたすべての変更をすぐに実施するには、[ホワイトリストの保存（Save White List）] をクリックします。

コンプライアンス ホワイト リストの管理

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin

[ホワイト リスト（White List）] ページは、コンプライアンス ホワイト リストと共有ホスト プロファイルの管理に使用できます。デフォルト ホワイト リストは、推奨設定を表すものであり、組み込みホスト プロファイルと呼ばれる特殊なカテゴリの共有ホスト プロファイルを使用します。

マルチドメイン展開では、現在のドメインで作成されたコンプライアンス ホワイト リストが表示されます。これは、編集が可能なリストです。また、先祖ドメインからの選択したホワイト リストも表示されますが、これは編集できません。下位のドメインで作成されたホワイト リストを表示および編集するには、そのドメインに切り替えます。

（注） 設定に無関係なドメイン（名前、管理対象デバイスなど）に関する情報が公開されている場合、システムは先祖ドメインからの設定を表示しません。 デフォルト ホワイト リストは、グローバル ドメインでのみ使用できます。

ステップ 1 **[Policies]** > **[Correlation]** を選択して、[ホワイト リスト（White List）] タブをクリックします。

ステップ 2 コンプライアンス ホワイト リストを管理します。

- 作成：新しいホワイト リストを作成するには、[新規ホワイト リスト（New White List）] をクリックして、コンプライアンス ホワイト リストの作成 （2685 ページ） で説明する手順を実行します。
- 削除：使用していないホワイト リストを削除するには、削除アイコン（）をクリックして、ホワイト リストの削除を確認します。また、ホワイト リストを削除すると、ネットワーク上のすべてのホストから、そのリストに関連付けられたホスト属性も削除されます。 コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。
- 編集：既存のホワイト リストを変更するには、編集アイコン（）をクリックし、コンプライアンス ホワイトリストの編集 （2694 ページ） で説明する手順を実行します。 代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

- 共有ホストプロファイル：ホワイトリストの共有ホストプロファイルを管理するには、[共有プロファイルの編集（Edit Shared Profiles）] をクリックして、共有ホストプロファイルの管理（2695 ページ）で説明する手順を実行します。

コンプライアンス ホワイトリストの編集

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin

アクティブな相関ポリシーに含まれるコンプライアンス ホワイトリストを修正して保存すると、システムは、ホワイトリストのターゲットネットワークのホストのコンプライアンスを再評価します。この再評価で一部のホストがコンプライアンス準拠または違反とされた場合でも、ホワイトリスト イベントは生成されません。

ステップ 1 **[Policies]** > **[Correlation]** を選択し、[ホワイトリスト（White List）] タブをクリックします。

ステップ 2 変更するホワイトリストの横にある編集アイコン（  ）をクリックします。

代わりに表示アイコン（  ）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 コンプライアンス ホワイト リストを編集します。

- 名前と説明：名前または説明を変更するには、左側のパネルでホワイトリストの名前をクリックしてホワイトリストの基本情報を表示し、新しい情報を入力します。
- ジェイルブレイクされたデバイスの許可：ネットワーク上でジェイルブレイクされたモバイル デバイスを許可するには、左側のパネルでホワイトリストの名前をクリックしてホワイトリストの基本情報を表示し、[ジェイルブレイクされたモバイル デバイスを許可（Allow Jailbroken Mobile Devices）] を有効にします。このオプションを無効にすると、ジェイルブレイクされたデバイスによってホワイトリスト違反が生成されます。
- 許可されるホストプロファイルの追加：このホワイトリストに対してオペレーティング システム固有のホストプロファイルを作成するには、[許可されているホストプロファイル（Allowed Host Profiles）] の横にある追加アイコン（  ）をクリックし、ホワイトリストホストプロファイルの作成（2688 ページ）の説明に従って続行します。
- 共有ホストプロファイルの追加：ホワイトリストに既存の共有ホストプロファイルを追加するには、[共有ホスト プロファイルの追加（Add Shared Host Profile）] をクリックし、追加する共有ホスト プロファイルを選択して [OK] をクリックします。共有ホスト プロファイルは斜体で表示されます。

- ターゲットネットワークの追加：ホストを調査することなく新しいターゲットネットワークを追加するには、ターゲットネットワークの横にある追加アイコン（）をクリックし、コンプライアンス ホワイト リストのターゲット ネットワークの設定 （2687 ページ）の説明に従って続行します。
- ホストプロファイルの削除：ホワイトリストから共有またはオペレーティング システム固有のホストプロファイルを削除するには、ホストプロファイルの横にある削除アイコン（）をクリックし、選択内容を確認します。共有ホスト プロファイルを削除すると、それがホワイトリストから除外されますが、プロファイルは削除されず、それを使用する他のホワイトリストからも除外されません。ホワイトリストのグローバル ホスト プロファイルは削除できません。
- ターゲットネットワークの削除：ホワイトリストからターゲットネットワークを削除するには、ネットワークの横にある削除アイコン（）をクリックし、選択内容を確認します。
- グローバル ホスト プロファイルの編集：ホワイトリストのグローバル ホスト プロファイルを編集するには、[任意のオペレーティング システム（Any Operating System）] をクリックし、ホワイト リスト ホスト プロファイルの作成 （2688 ページ）の説明に従って続行します。
- 他のホスト プロファイルの編集：共有またはオペレーティング システム固有のホスト プロファイルを編集するには、ホスト プロファイルの名前をクリックし、ホワイト リスト ホスト プロファイルの作成 （2688 ページ）の説明に従って続行します。
- ターゲットネットワークの編集：ターゲットネットワークを編集するには、ネットワークの名前をクリックし、コンプライアンス ホワイト リストのターゲット ネットワークの設定 （2687ページ）の指示に従って続行します。

ステップ 4 前回の保存以降に行ったすべての変更をすぐに実装するには、[ホワイトリストの保存（Save White List）] をクリックします。

共有ホスト プロファイルの管理

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin

コンプライアンス ホワイト リストでは、共有ホストプロファイルは特定のオペレーティング システムに関連付けられますが、それぞれの共有ホスト プロファイルを複数のホワイト リスト内で使用できます。複数のホワイト リストを作成するが、同じホスト プロファイルを使用して複数のホワイト リストで特定のオペレーティング システムを実行するホストを評価する場合は、共有のホスト プロファイルを使用します。

マルチドメイン展開では、現在のドメインで作成された共有ホストプロファイルが表示されます。これは、編集が可能なプロファイルです。先祖ドメインで作成された共有ホストプロファイルも表示されますが、これは編集できません。下位のドメインで作成された共有ホストプロファイルを表示および編集するには、そのドメインに切り替えます。

（注） 共有ホストプロファイル（組み込みプロファイルを含む）を変更したり、組み込みアプリケーションプロトコル、プロトコル、クライアントを変更したりすると、そのプロファイルを使用するすべてのホワイトリストに変更が適用されます。意図しない変更を加えた場合や、該当する組み込みの要素を削除した場合は、工場出荷時の初期状態にリセットできます。

ステップ 1 **[Policies]** > **[Correlation]** を選択して、[ホワイト リスト（White List）] タブをクリックします。

ステップ 2 [共有プロファイルの編集（Edit Shared Profiles）] をクリックします。

ステップ 3 共有ホスト プロファイルを管理します。

- 共有ホスト プロファイルの作成：ホストの調査なしで新しい共有ホスト プロファイルを作成するには、[共有ホスト プロファイル（Shared Host Profiles）] の横にある追加アイコン（  ）をクリックし、ホワイト リスト ホスト プロファイルの作成 （2688 ページ）で説明する手順を実行します。
- 調査によるホスト プロファイルの作成：ネットワークの調査によって複数の新しい共有ホスト プロファイルを作成するには、[ターゲット ネットワークの追加（Add Target Network）] をクリックして、コンプライアンス ホワイトリストのターゲット ネットワークの設定 （2687ページ）で説明する手順を実行します。
- 削除：共有ホストプロファイルを削除するには、削除アイコン（  ）をクリックして、選択内容を確認します。
- 編集：既存の共有ホストプロファイル（組み込み共有ホストプロファイルを含む）を変更するには、そのプロファイルの名前をクリックして、ホワイトリスト ホストプロファイルの作成 （2688ページ）で説明する手順を実行します。
- 組み込みのホストプロファイルのリセット：すべての組み込みホストプロファイルを工場出荷時の初期状態にリセットするには、[組み込みホストプロファイル（Built-in Host Profiles）] をクリックして、[工場出荷時の初期状態にリセット（Reset to Factory Defaults）] をクリックしてから、選択内容を確認します。

ステップ 4 最後の保存以降に行われたすべての変更をすぐに実装するには、[すべてのプロファイルの保存（Save All Profiles）] をクリックします。

第 109 章

相関ポリシー

次のトピックでは、相関ポリシーおよびルールの設定方法について説明します。

相関ポリシーとルールの概要

相関機能を使用することで、ネットワークへの脅威に対して相関ポリシーを使用してリアルタイムで応答できます。

ネットワーク上のアクティビティによって、アクティブな相関ポリシー内の相関ルールまたはコンプライアンスホワイトリストのいずれかがトリガーされると、相関ポリシー違反が発生します。

相関ルール

アクティブな相関ポリシー内の相関ルールがトリガーされると、システムによって相関イベントが生成されます。相関ルールは、以下の場合にトリガーされます。

- 特定のタイプのイベント（接続、侵入、マルウェア、ディスカバリ、ユーザ アクティビティなど）がシステムによって生成された。
- ネットワーク トラフィックが通常のプロファイルから逸脱している。

以下の方法で相関ルールを制約することもできます。

- ホスト プロファイル限定を追加すると、トリガー イベントに関連するホストのプロファイルからの情報に基づいてルールを制約できます。
- 接続トラッカーを相関ルールに追加すると、ルールの初期基準に一致した場合、システムは特定の接続を追跡し始めます。その後、追跡対象の接続がさらに追加の基準を満たす場合にのみ、相関イベントが生成されます。

- ユーザ限定を相関ルールに追加すると、特定のユーザまたはユーザ グループを追跡します。たとえば、特定のユーザのトラフィックや特定の部門からのトラフィックに対してのみトリガーされるように相関ルールを制約することができます。
- スヌーズ期間の追加。相関ルールがトリガーされた後、スヌーズ期間により指定したインターバルの間、そのルールは再びトリガーされません。スヌーズ期間が経過すると、ルールは再びトリガー可能になり、新しいスヌーズ期間が始まります。
- 非アクティブ期間の追加。非アクティブ期間中は、相関ルールはトリガーされません。

展開のライセンスなしでも相関ルールを設定できますが、ライセンス許可のないコンポーネントを使用するルールはトリガーされません。

コンプライアンス ホワイトリスト

コンプライアンス ホワイト リストは、ネットワーク上のホストでどのオペレーティング システム、アプリケーション（Webおよびクライアント）、プロトコルが許可されるかを指定します。アクティブな相関ポリシーで使用されているホワイトリストにホストが違反した場合、ホワイト リスト イベントがシステムによって生成されます。

相関応答

相関ポリシー違反への応答には、シンプルなアラートや、さまざまな修復（ホストのスキャンなど）が含まれます。それぞれの相関ルールまたはホワイトリストを、単一の応答または応答グループに関連付けることができます。

ネットワーク トラフィックが複数のルールまたはホワイトリストをトリガーとして使用した場合、システムはそれぞれのルールとホワイトリストに関連付けられているすべての応答を起動します。

相関およびマルチテナンシー

マルチドメイン展開では、ドメイン レベルで利用可能な任意のルール、ホワイトリスト、応答を使って、任意のドメイン レベルで相関ポリシーを作成できます。高位レベル ドメインの管理者はドメイン内、および複数ドメインで関連付けを実行できます。

- ドメインによって相関ルールを制約すると、そのドメインの子孫で報告されるイベントが照合されます。
- 高位レベル ドメインの管理者は複数ドメインでホストを評価するコンプライアンス ホワイトリストを作成できます。同じホワイトリストで、異なるドメイン内の異なるサブネットを対象にすることができます。

（注） システムは、各リーフ ドメインに個別のネットワーク マップを作成します。リテラルの設定（IP アドレス、VLAN タグ、ユーザ名など）を使用してドメイン間の相関ルールを制約すると、予期しない結果になる可能性があります。

関連トピック

コンプライアンス ホワイトリストの概要 （2679 ページ）
Firepower Management Center アラート応答 （2807 ページ）
修復の概要 （2755 ページ）

相関ポリシーの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Discovery Admin

相関ルール、コンプライアンスのホワイトリスト、アラート応答、および修復を使用して相関ポリシーを作成します。

マルチドメイン展開では、任意のドメイン レベルで、そのレベルで使用可能な構成設定を使用して相関ポリシーを作成できます。

各相関ポリシーと、そのポリシーで使用される各ルールとホワイトリストにプライオリティを割り当てることができます。ルールとホワイトリストのプラオリティは、相関ポリシーのプライオリティをオーバーライドします。ネットワーク トラフィックが相関ポリシーに違反した場合、違反があったルールまたはホワイトリストに独自のプライオリティがない限り、結果の相関イベントでポリシーのプライオリティ値が表示されます。

ステップ 1 **[Policies]** > **[Correlation]**を選択します。

ステップ 2 [ポリシーの作成（Create Policy）] をクリックします。

ステップ 3 [ポリシー名（Policy Name）] と [ポリシーの説明（Policy Desription）] を入力します。

ステップ 4 [デフォルト プライオリティ（Default Priority）] ドロップダウン リストから、ポリシーのプライオリティを選択します。ルールのプライオリティのみを使用するには、[なし（None）] を選択します。

ステップ 5 [ルールの追加（Add Rules）] をクリックし、ポリシーで使用するルールとホワイトリストを選択して、[追加（Add）] をクリックします。

ステップ 6 各ルールまたはホワイトリストの [優先順位（Priority）] リストから、プライオリティを選択します。

- 1 ～ 5 のプライオリティ値
- **None**
- [デフォルト（Default）]（ポリシーのデフォルト プライオリティを使用）

ステップ 7 ルールとホワイトリストに応答を追加する （2700 ページ）の説明に従ってルールとホワイトリストに応答を追加します。

ステップ 8 [保存（Save）] をクリックします。

次のタスク

- スライダをクリックして、ポリシーをアクティブにします。

ルールとホワイトリストに応答を追加する

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Discovery Admin

それぞれの相関ルールまたはホワイトリストを、単一の応答または応答グループに関連付けることができます。ネットワーク トラフィックが複数のルールまたはホワイトリストをトリガーとして使用した場合、システムはそれぞれのルールとホワイトリストに関連付けられているすべての応答を起動します。トラフィック プロファイルの変更への応答として使用された場合は、Nmap 修復が開始されないことに注意してください。

マルチドメイン展開では、現在のドメインまたは先祖ドメインで作成された応答を使用できます。

ステップ 1 相関ポリシーエディタで、応答を追加するルールまたはホワイトリストの横にある応答アイコン（  ）をクリックします。

ステップ 2 [未割り当ての応答（Unassigned Responses）] の下で、ルールまたはホワイトリストがトリガーとして使用された場合に起動する応答を選択して、上矢印（^）をクリックします。

ステップ 3 [更新（Update）] をクリックします。

関連トピック

Firepower Management Center アラート応答 （2807 ページ）
修復の概要 （2755 ページ）

相関ポリシーの管理

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Discovery Admin

アクティブな相関ポリシーへの変更は、即座に反映されます。

相関ポリシーを有効化すると、システムは即座にイベントの処理を開始して、応答をトリガーします。システムは、最初の有効化後の評価時に、非準拠ホストのホワイト リスト イベントを生成しない点に注意してください。

マルチドメイン展開では、現在のドメインで作成された相関ポリシーが表示されます。このポリシーは編集可能です。また、先祖ドメインからの選択した相関ポリシーも表示されますが、これは編集できません。下位のドメインで作成された相関ポリシーを表示および編集するには、そのドメインに切り替えます。

（注） 設定に無関係なドメイン（名前、管理対象デバイスなど）に関する情報が公開されている場合、システムは先祖ドメインからの設定を表示しません。

ステップ 1 **[Policies]** > **[Correlation]**を選択します。

ステップ 2 相関ポリシーを管理します。

- アクティブ化または非アクティブ化：スライダをクリックします。 コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。
- 作成：[ポリシーの作成（Create Policy）]をクリックします。相関ポリシーの設定 （2699 ページ）を参照してください。
- 編集：編集アイコン（）をクリックします。相関ポリシーの設定 （2699ページ）を参照してください。 代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。
- 削除：削除アイコン（）をクリックします。 コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

相関ルールの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Discovery Admin

単純な相関ルールでは、特定のタイプのイベントが発生することのみが必要です。より具体的な条件を指定する必要はありません。たとえば、トラフィック プロファイル変化に基づく相関ルールでは、条件を指定する必要はありません。また、複数の条件と追加した制約を使用して複雑な相関ルールを作成することもできます。

相関ルール トリガー基準、ホスト プロファイル限定、ユーザ限定、または接続トラッカーを作成するときの構文はそれぞれに異なりますが、メカニズムはすべて同じです。

（注） マルチドメイン展開では、相関ルールを先祖ドメインで制約すると、そのドメインの子孫によってレポートされるイベントと一致します。

始める前に

- 相関イベントをトリガーするために使用するタイプの情報が展開で収集されていることを確認します。たとえば、個々の接続イベントまたは接続サマリーイベントで使用可能な情報は、検出方法、ロギング方法、イベント タイプなど、いくつかの要因により異なります。 システムは、エクスポートされた NetFlow レコードからネットワーク マップにホストを追加できますが、これらのホストに使用できる情報は限られます（NetFlow データと管理対象デバイス データの違い （2478 ページ）を参照）。

ステップ 1 **[Policies]** > **[Correlation]** を選択し、[ルール管理（Rule Management）] タブをクリックします。

ステップ 2 [ルールの作成（Create Rule）] をクリックします。

ステップ 3 [ルール名（Rule Name）] と [ルールの説明（Rule Description）] を入力します。

ステップ 4 必要に応じて、ルールの [ルール グループ（Rule Group）] を選択します。

ステップ 5 基本イベント タイプを選択し、必要に応じて、相関ルールの追加のトリガー条件を指定します。次の基本イベント タイプを選択できます。

- **侵入イベントが発生**：侵入イベント トリガー条件の構文 （2703 ページ）を参照してください。
- **マルウェア イベントが発生**：マルウェア イベント トリガー条件の構文 （2706 ページ）を参照してください。
- **検出イベントが発生**：ディスカバリ イベント トリガー条件の構文 （2708 ページ）を参照してください。
- **ユーザ アクティビティが検出された**：ユーザ アクティビティのイベント トリガー条件の構文 （2712 ページ）を参照してください。
- **ホスト入力イベントが発生**：ホスト入力イベント トリガー条件の構文 （2713 ページ）を参照してください。
- **接続イベントが発生**：接続イベント トリガー条件の構文 （2714 ページ）を参照してください。
- **トラフィック プロファイルの変更**：トラフィック プロファイル変化の構文 （2718 ページ）を参照してください。

ステップ 6 必要に応じて、次のいずれかまたはすべてを追加することによって相関ルールをさらに制約します。

- ホスト プロファイル限定：[ホスト プロファイル限定の追加（Add Host Profile Qualification）] をクリックします。相関ホスト プロファイル限定の構文 （2720 ページ）を参照してください。
- 接続トラッカー：[接続トラッカーの追加（Add Connection Tracker）] をクリックします。接続トラッカー （2725 ページ）を参照してください。
- ユーザ限定：[ユーザ限定の追加（Add User Qualification）] をクリックします。ユーザ限定の構文 （2723 ページ）を参照してください。

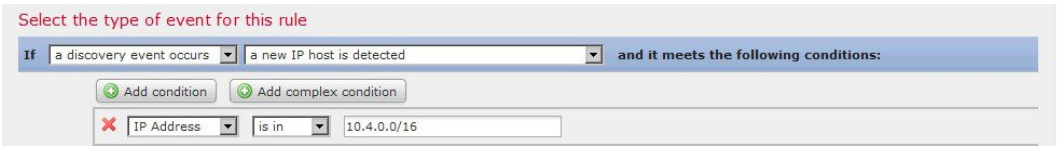
- スヌーズ期間：ルール オプションで、[スヌーズ（Snooze）]テキスト フィールドとドロップダウン リストを使用して、相関ルールのトリガー後、次に相関ルールをトリガーするまで待機する間隔を指定します。
- 非アクティブ期間：ルール オプションで、[非アクティブ期間の追加（Add Inactive Period）] をクリックします。テキスト フィールドとドロップダウン リストを使用して、相関ルールに基づくネットワーク トラフィック評価をシステムに停止させる時点および頻度を指定します。

ヒント　スヌーズ期間を削除するには、間隔を **0**（秒、分、または時間）に指定します。

ステップ 7　[Save Rule] をクリックします。

相関ルールの単純な例

新しいホストが特定のサブネットで検出されると、次の単純な相関ルールがトリガーされます。カテゴリが IP アドレスを表す場合、演算子として [is in] または [is not in] を選択すると、CIDR などの特殊な表記で表される IP アドレス ブロックにその IP アドレスが含まれるのか、含まれないのかを指定できます。



次のタスク

- 相関ポリシーの設定（2699ページ）の説明に従って、相関ポリシーでルールを使用します。

関連トピック

相関ルールの管理 （2738 ページ）
相関ルールの作成メカニズム （2735 ページ）
スヌーズ期間および非アクティブ期間 （2734 ページ）
NetFlow データと管理対象デバイス データの違い （2478 ページ）

侵入イベント トリガー条件の構文

侵入イベントを基本イベントとして選択した場合、次の表で説明する方法に従って相関ルールの条件を作成します。

表 *265*：侵入イベントの構文

指定する項目	選択する演算子と内容
アクセス コントロール ポリシー	侵入イベントを生成した侵入ポリシーを使用するアクセス コントロール ポリシーを 1 つ以上選択します。

指定する項目	選択する演算子と内容
アクセス コントロール ルール名	侵入イベントを生成した侵入ポリシーを使用するアクセス コントロール ルールの名前の全体またはその一部を入力します。
アプリケーション プロトコル	侵入イベントに関連付けられたアプリケーション プロトコルを 1 つ以上選択します。
アプリケーション プロトコル カテゴリ	アプリケーション プロトコルのカテゴリを 1 つ以上選択します。
分類	分類を 1 つ以上を選択します。
クライアント	侵入イベントに関連付けられたクライアントを 1 つ以上選択します。
クライアント カテゴリ	クライアントのカテゴリを 1 つ以上選択します。
接続先（国）または送信元（国）	侵入イベントの送信元または宛先 IP アドレスに関連付けられた国を 1 つ以上選択します。
宛先 IP、送信元 IP、送信元 IP と宛先 IP の両方、または、送信元 IP か宛先 IP のいずれか	単一の IP アドレスまたはアドレス ブロックを入力します。
宛先ポート/ICMP コードまたは送信元ポート/ICMP タイプ	送信元トラフィックのポート番号または ICMP タイプ、または宛先トラフィックのポート番号または ICMP コードを入力します。
Device	イベントを生成した可能性があるデバイスを 1 つ以上選択します。
ドメイン	1 つ以上のドメインを選択してください。マルチドメイン展開環境では、先祖ドメインによる制約条件がそのドメインの子孫によって報告されるデータにも適用されます。This field is only present if you have ever configured the Firepower Management Center for multitenancy.
出力インターフェイスまたは入力インターフェイス	インターフェイスを 1 つ以上選択します。
出力セキュリティ ゾーンまたは入力セキュリティ ゾーン	1 つ以上のセキュリティ ゾーンまたはトンネルゾーンを選択します。
ジェネレータ ID	プリプロセッサを 1 つ以上選択します。

指定する項目	選択する演算子と内容
影響フラグ	侵入イベントに割り当てられた影響レベルを選択します。 NetFlow データからネットワーク マップに追加されたホストに使用可能なオペレーティング システムの情報はないので、システムは、それらのホストに作用する侵入イベントに対し脆弱な（インパクト レベル 1：赤）インパクト レベルを割り当てることができません。このような場合は、ホスト入力機能を使用して、ホストのオペレーティング システム ID を手動で設定します。
インライン結果	システムは、侵入ポリシーの結果としてパケットを [ドロップした（dropped）] か [ドロップしたと想定（would have dropped）] したのかを選択します。 システムは、インライン展開、スイッチド展開、またはルーテッド展開のパケットをドロップできます。侵入ポリシーのドロップ動作や侵入ルール状態とは無関係に、パッシブ展開（インライン セットがタップ モードである場合を含む）ではシステムがパケットをドロップしません。
侵入ポリシー	侵入イベントを生成した侵入ポリシーを 1 つ以上選択します。
IOC タグ	侵入イベントの結果として侵害の兆候タグが設定されているかどうかを選択します。
[プライオリティ（Priority）]	ルールの優先順位を選択します。 ルール ベースの侵入イベントの場合、優先順位は `priority` キーワードまたは `classtype` キーワードのいずれかの値に対応します。その他の侵入イベントの場合、プライオリティはデコーダまたはプリプロセッサによって決定されます。
プロトコル	http://www.iana.org/assignments/protocol-numbers にリストされているトランスポート プロトコルの名前または番号を入力します。
ルール メッセージ	ルール メッセージの全体またはその一部を入力します。
ルール SID	単一の（[Snort ID]SID）またはカンマ区切りの複数の SID を入力します。 演算子として [に含まれる（is in）] または [に含まれない（is not in）] を選択する場合、複数選択ポップアップ ウィンドウを使用することはできません。SID のカンマ区切りリストを入力する必要があります。
ルール タイプ	ルールをローカルにするかどうかを指定します。 ローカル ルールには、カスタマイズされた標準テキスト侵入ルール、ユーザが変更した標準テキスト ルール、見出し情報を変更してルールを保存するときに作成される共有オブジェクト ルールの新規インスタンスが含まれます。
実際の SSL アクション	システムが暗号化された接続をどのように処理したかを示す SSL ルール アクションを選択します。
SSL 証明書のフィンガープリント	トラフィックの暗号化に使用された証明書のフィンガープリントを入力するか、フィンガープリントに関連付けられたサブジェクトの共通名を選択します。

指定する項目	選択する演算子と内容
SSL証明書のサブジェクトの共通名（CN）	セッションの暗号化に使用された証明書のサブジェクトの共通名のすべてまたはその一部を入力します。
SSL証明書のサブジェクトの国（C）	セッションの暗号化に使用された証明書のサブジェクトの国番号を 1 つ以上選択します。
SSL証明書のサブジェクトの組織（O）	セッションの暗号化に使用された証明書のサブジェクトの組織名のすべてまたはその一部を入力します。
SSL証明書のサブジェクトの部門（OU）	セッションの暗号化に使用された証明書のサブジェクトの部門名のすべてまたはその一部を入力します。
SSL フローのステータス	システムによるトラフィック復号化試行の結果に基づくステータスを 1 つ以上選択します。
[ユーザ名（Username）]	侵入イベントで送信元ホストにログインしたユーザを示すユーザ名を入力します。
VLAN ID（Admin. VLAN ID）	侵入イベントをトリガーとして使用したパケットに関連付けられた最も内側の VLAN ID を入力します。
Web アプリケーション	侵入イベントに関連付けられた Web アプリケーションを 1 つ以上選択します。
Web アプリケーションのカテゴリ	Web アプリケーションのカテゴリを 1 つ以上選択します。

関連トピック

侵入イベント フィールド （3059 ページ）
Firepower システムの IP アドレス表記法 （20 ページ）

マルウェア イベント トリガー条件の構文

マルウェア イベントで相関ルールをベースとして使用するには、まず、使用するマルウェア イベントのタイプを指定します。選択肢が使用可能なトリガー条件の設定を決定します。次のオプションを選択できます。

- [エンドポイントベースのマルウェアの検出（by endpoint-based malware detection）]（エンドポイント向け AMP による検出）
- [ネットワークベースのマルウェアの検出（by network-based malware detection）]（ネットワーク向け AMP）（ネットワーク向け AMP による検出）
- [レトロスペクティブ ネットワークベースのマルウェアの検出（by retrospective network-based malware detection）]（ネットワーク向け AMP によるレトロアクティブ検出）

マルウェアイベントを基本イベントとして選択する場合、次の表で説明する方法に従って相関ルールの条件を作成します。

表 *266 :* マルウェア イベントの構文

指定する項目	選択する演算子と内容
アプリケーション プロトコル	マルウェア イベントに関連付けられたアプリケーション プロトコルを 1 つ以上選択します。
アプリケーション プロトコル カテゴリ	アプリケーション プロトコルのカテゴリを 1 つ以上選択します。
クライアント	マルウェア イベントに関連付けられたクライアントを 1 つ以上選択します。
クライアント カテゴリ	クライアントのカテゴリを 1 つ以上選択します。
接続先（国）または送信元（国）	マルウェア イベントの送信元または宛先 IP アドレスに関連付けられた国を 1 つ以上選択します。
宛先 IP、ホスト IP、または送信元 IP	単一の IP アドレスまたはアドレス ブロックを入力します。
送信先ポート/ICMP コード	宛先トラフィックのポート番号または ICMP コードを入力します。
傾向	[マルウェア（Malware）] または [カスタム検出（Custom Detection）]、あるいはその両方を選択します。
ドメイン	1 つ以上のドメインを選択してください。マルチドメイン展開環境では、先祖ドメインによる制約条件がそのドメインの子孫によって報告されるデータにも適用されます。This field is only present if you have ever configured the Firepower Management Center for multitenancy.
イベント タイプ（Event Type）	エンドポイント向け AMP により検出されたマルウェア イベントと関連付けられた 1 つ以上のイベント タイプを選択します。
ファイル名	ファイルの名前を入力します。
ファイル タイプ	ファイル タイプを選択します。
ファイル タイプ カテゴリ	ファイル タイプ カテゴリを 1 つ以上選択します。
IOC タグ	マルウェア イベントの結果として侵害の兆候タグが設定 [される（is）] か、設定 [されない（is not）] かを選択します。
SHA-256	ファイルの SHA-256 ハッシュ値を入力するか貼り付けます。

指定する項目	選択する演算子と内容
実際の SSL アクション	システムが暗号化された接続をどのように処理したかを示す SSL ルール アクションを選択します。
SSL 証明書のフィンガープリント	トラフィックの暗号化に使用された証明書のフィンガープリントを入力するか、フィンガープリントに関連付けられたサブジェクトの共通名を選択します。
SSL 証明書のサブジェクトの共通名（CN）	セッションの暗号化に使用された証明書のサブジェクトの共通名のすべてまたはその一部を入力します。
SSL 証明書のサブジェクトの国（C）	セッションの暗号化に使用された証明書のサブジェクトの国番号を 1 つ以上選択します。
SSL 証明書のサブジェクトの組織（O）	セッションの暗号化に使用された証明書のサブジェクトの組織名のすべてまたはその一部を入力します。
SSL 証明書のサブジェクトの部門（OU）	セッションの暗号化に使用された証明書のサブジェクトの部門名のすべてまたはその一部を入力します。
SSL フローのステータス	システムによるトラフィック復号化試行の結果に基づくステータスを 1 つ以上選択します。
送信元ポート/ICMP タイプ	送信元トラフィックのポート番号または ICMP タイプを入力します。
Web アプリケーション	マルウェア イベントに関連付けられた Web アプリケーションを 1 つ以上選択します。
Web アプリケーションのカテゴリ	Web アプリケーションのカテゴリを 1 つ以上選択します。

関連トピック

ファイルおよびマルウェア イベント フィールド （3121 ページ）
Firepower システムの IP アドレス表記法 （20 ページ）

ディスカバリ イベント トリガー条件の構文

ディスカバリ イベントで相関ルールをベースとして使用するには、まず、使用するディスカバリ イベントのタイプを指定します。選択肢が使用可能なトリガー条件の設定を決定します。次の表は、選択可能なディスカバリ イベントのタイプを示しています。

ホップ変更によって相関ルールをトリガーとして使用したり、ホスト制限到達のためにシステムが新しいホストをドロップした時点で相関ルールをトリガーとして使用したりすることはできません。ただし、[任意のタイプのイベントがある（there is any type of event）] を選択することで、任意のタイプのディスカバリ イベントの発生時にルールをトリガーできます。

表 *267* : 相関ルールのトリガー条件とディスカバリ イベント タイプ

選択するオプション	選択内容
クライアントが変更された	クライアント更新
a client timed out	クライアント タイムアウト
a host IP address is reused	DHCP：IP アドレスの再割り当て
a host is deleted because the host limit was reached	ホスト削除：ホスト制限に到達
a host is identified as a network device	ネットワーク デバイスへのホスト タイプの変更
a host timed out	ホスト タイムアウト
a host's IP address has changed	DHCP：IP アドレスの変更
a NETBIOS name change is detected	NetBIOS 名の変更
a new client is detected	新しいクライアント
a new IP host is detected	新しいホスト
a new MAC address is detected	ホストの追加 MAC の検出
a new MAC host is detected	新しいホスト
a new network protocol is detected	新しいネットワーク プロトコル
a new transport protocol is detected	新しいトランスポート プロトコル
a TCP port closed	TCP ポート クローズ
a TCP port timed out	TCPポート タイムアウト
a UDP port closed	UDP ポート クローズ
a UDP port timed out	UDP ポート タイムアウト
a VLAN tag was updated	VLAN タグ情報の更新
an IOC was set	侵害の兆候
an open TCP port is detected	新しい TCPポート
an open UDP port is detected	新しい UDP ポート
the OS information for a host has changed	新しい OS
the OS or server identity for a host has a conflict	アイデンティティ競合
the OS or server identity for a host has timed out	アイデンティティ タイムアウト

選択するオプション	選択内容
there is any kind of event	（任意のイベント タイプ）
there is new information about a MAC address	MAC 情報の変更
there is new information about a TCP server	TCP サーバ情報の更新
there is new information about a UDP server	UDP サーバ情報の更新

次の表では、ディスカバリ イベントを基本イベントとして選択するときに、相関ルールの条件を作成する方法を説明します。

表 *268 :* ディスカバリ イベントの構文

指定する項目	選択する演算子と内容
アプリケーション プロトコル	アプリケーション プロトコルを 1 つ以上選択します。
[アプリケーション プロトコル カテゴリ（Application Protocol Category）]	アプリケーション プロトコルのカテゴリを 1 つ以上選択します。
アプリケーション ポート	アプリケーションプロトコルのポート番号を入力します。
クライアント	クライアントを 1 つ以上選択します。
[クライアント カテゴリ（Client Category）]	クライアントのカテゴリを 1 つ以上選択します。
クライアント バージョン	クライアントのバージョン番号を入力します。
Device	ディスカバリ イベントを生成した可能性があるデバイスを 1 つ以上選択します。
ドメイン	1 つ以上のドメインを選択してください。マルチドメイン展開環境では、先祖ドメインによる制約条件がそのドメインの子孫によって報告されるデータにも適用されます。This field is only present if you have ever configured the Firepower Management Center for multitenancy.
[ハードウェア（Hardware）]	モバイル デバイスのハードウェア モデルを入力します。たとえば、すべての Apple iPhone に一致させるには **`iPhone`** と入力します。
[ホスト タイプ（Host Type）]	ホスト タイプを 1 つ以上選択します。ホスト、またはいずれかのタイプのネットワーク デバイスを選択できます。
IP アドレスまたは新しい IP アドレス	単一の IP アドレスまたはアドレス ブロックを入力します。

指定する項目	選択する演算子と内容
[ジェイルブロークン（Jailbroken）]	イベントのホストがジェイルブレイクされたモバイル デバイスであることを示すには [はい（Yes）] を、そうでない場合は [いいえ（No）] を選択します。
MAC アドレス	ホストの MAC アドレス全体またはその一部を入力します。 たとえば、特定のハードウェア製造元のデバイスの MAC アドレスが 0A:12:34 で始まることがわかっている場合、演算子として [開始（begins with）] を選択し、値として **`0A:12:34`** を入力できます。
MAC タイプ	MAC アドレスが [ARP/DHCP で検出（ARP/DHCP Detected）] されたかどうかを選択します。 つまり、MAC アドレスがホストに属していることをシステムがポジティブに識別したのか（[ARP/DHCP で検出（is ARP/DHCP Detected）]）、または、管理対象デバイスとホストの間にルータがあるなどの理由で、その MAC アドレスを持つ多数のホストをシステムが認識しているのか（[ARP/DHCP で検出されない（is not ARP/DHCP Detected）]）を選択します。
MAC ベンダー	ディスカバリ イベントをトリガーとして使用したネットワーク トラフィックで使われている NIC の MAC ハードウェア ベンダーの名前全体またはその一部を入力します。
Mobile	イベントのホストがモバイル デバイスであることを示すには [はい（Yes）] を、そうでない場合は [いいえ（No）] を選択します。
NETBIOS 名	ホストの NetBIOS 名を入力します。
ネットワーク プロトコル	http://www.iana.org/assignments/ethernet-numbers にリストされているネットワーク プロトコル番号を入力します。
OS 名	オペレーティング システムの名前を 1 つ以上選択します。
OS ベンダー	オペレーティング システムのベンダーを 1 つ以上選択します。
OS バージョン	オペレーティング システムのバージョンを 1 つ以上選択します。
プロトコルまたは トランスポート プロトコル	http://www.iana.org/assignments/protocol-numbers にリストされているトランスポート プロトコルの名前または番号を入力します。

指定する項目	選択する演算子と内容
ソース（Source）	ホスト入力データのソースを選択します（オペレーティング システムとサーバのアイデンティティ変更およびタイムアウトの場合）。
ソース タイプ	ホスト入力データのソースのタイプを選択します（オペレーティング システムとサーバのアイデンティティ変更およびタイムアウトの場合）。
VLAN ID（Admin. VLAN ID）	イベントに関連しているホストのVLAN IDを入力します。
[Web アプリケーション（Web Application）]	Web アプリケーションを選択します。

関連トピック

ディスカバリ イベント タイプ （3202 ページ）
ディスカバリ イベントのフィールド （3210 ページ）
Firepower システムの IP アドレス表記法 （20 ページ）

ユーザ アクティビティのイベント トリガー条件の構文

ユーザ アクティビティで相関ルールをベースとして使用するには、まず、使用するユーザ アクティビティのタイプを選択します。選択肢が使用可能なトリガー条件の設定を決定します。次のオプションを選択できます。

- **a new user identity was detected（新しいユーザ ID の検出）**
- **a user logs into a host（ユーザがホストにログイン）**

ユーザアクティビティを基本イベントとして選択する場合、次の表で説明する方法に従って相関ルールの条件を作成します。

表 *269 :* ユーザ アクティビティの構文

指定する項目	選択する演算子と内容
Device	ユーザ アクティビティを検出した可能性のあるデバイスを 1 つ以上選択します。
ドメイン	1 つ以上のドメインを選択してください。マルチドメイン展開環境では、先祖ドメインによる制約条件がそのドメインの子孫によって報告されるデータにも適用されます。This field is only present if you have ever configured the Firepower Management Center for multitenancy.
[IPアドレス（IP Address）]	単一のIPアドレスまたはアドレスブロックを入力します。
[ユーザ名（Username）]	ユーザ名を入力します。

関連トピック

ユーザ アクティビティ データのフィールド
Firepower システムの IP アドレス表記法 （20 ページ）

ホスト入力イベント トリガー条件の構文

ホスト入力イベントで相関ルールをベースとして使用するには、まず、使用するホスト入力イベントのタイプを指定します。選択肢が使用可能なトリガー条件の設定を決定します。次の表では、選択可能なホスト入力イベントのタイプを示しています。

ユーザ定義によるホスト属性定義を追加/削除/変更するとき、あるいは脆弱性の影響限定を設定するときに、相関ルールをトリガーとして使用することはできません。

表 *270*：相関ルールのトリガー条件とホスト入力イベント タイプ

選択するオプション	ルールをトリガーとして使用するイベント タイプ
a client is added	クライアントの追加
a client is deleted	クライアントの削除
a host is added	ホストの追加
a protocol is added	プロトコルの追加
a protocol is deleted	プロトコルの削除
a scan result is added	スキャン結果の追加
a server definition is set	サーバ定義の設定
a server is added	ポートの追加
a server is deleted	ポートの削除
a vulnerability is marked invalid	脆弱性を無効に設定
a vulnerability is marked valid	脆弱性を有効に設定
an address is deleted	ホスト/ネットワークの削除
an attribute value is deleted	ホスト属性値の削除
an attribute value is set	ホスト属性値の設定
an OS definition is set	オペレーティング システム定義の設定
host criticality is set	ホスト重要度の設定（Set Host Criticality）

次の表では、ホスト入力イベントを基本イベントとして選択するときに、相関ルールの条件を作成する方法を説明します。

表 *271* : ホスト入力イベントの構文

指定する項目	選択する演算子と内容
ドメイン	1 つ以上のドメインを選択してください。マルチドメイン展開環境では、先祖ドメインによる制約条件がそのドメインの子孫によって報告されるデータにも適用されます。This field is only present if you have ever configured the Firepower Management Center for multitenancy.
[IPアドレス（IP Address）]	単一のIPアドレスまたはアドレスブロックを入力します。
ソース（Source）	ホスト入力データのソースを選択します。
ソース タイプ（Source Type）	ホスト入力データのソースのタイプを選択します。

関連トピック

ホスト入力イベント タイプ （3207 ページ）
ディスカバリ イベントのフィールド （3210 ページ）
Firepower システムの IP アドレス表記法 （20 ページ）

接続イベント トリガー条件の構文

接続イベントで相関ルールをベースとして使用するには、まず、使用する接続イベントのタイプを指定します。接続イベントで利用可能な情報は、システムが接続をログに記録した方法、理由、および時によって変わることに注意してください。次のオプションを選択できます。

- **接続の開始または終了時のいずれか**
- **接続の開始時**
- **接続の終了時**

次の表では、接続イベントを基本イベントとして選択するときに、相関ルールの条件を作成する方法を説明します。

表 *272* : 接続イベントの構文

指定する項目	選択する演算子と内容
アクセス コントロール ポリシー	接続をログに記録したアクセス コントロール ポリシーを 1 つ以上選択します。

指定する項目	選択する演算子と内容
アクセス コントロール ルールのアクション	接続をログに記録したアクセス コントロール ルールに関連付けられたアクションを 1 つ以上選択します。 あとで接続を処理するルールまたはデフォルト アクションとは無関係に、ネットワーク トラフィックがいずれかのモニタ ルールの条件に一致した場合に相関イベントをトリガーとして使用するには、[モニタ（Monitor）] を選択します。
アクセス コントロール ルール	接続をログに記録したアクセス コントロール ルールの名前のすべてまたは一部を入力します。 あとで接続を処理したルールまたはデフォルト アクションとは無関係に、接続と一致した条件を持つモニタ ルールの名前を入力できます。
アプリケーション プロトコル	接続に関連付けられたアプリケーション プロトコルを 1 つ以上選択します。
アプリケーション プロトコル カテゴリ	アプリケーション プロトコルのカテゴリを 1 つ以上選択します。
クライアント	クライアントを 1 つ以上選択します。
[クライアント カテゴリ（Client Category）]	クライアントのカテゴリを 1 つ以上選択します。
クライアント バージョン	クライアントのバージョン番号を入力します。
接続時間	接続イベントの時間（秒数）を入力します。
接続タイプ	接続情報がどのように取得されたかに基づいて、相関ルールをトリガーするかどうかを指定します。 • エクスポートされた NetFlow データから生成された接続イベントに、[生成元（is）] および [Netflow] を選択します。 • Firepower システムの管理対象デバイスによって検出された接続イベントに、[生成元でない（is not）] および [Netflow] を選択します。
接続先（国）または送信元（国）	接続イベントの送信元または宛先 IP アドレスに関連付けられた国を 1 つ以上選択します。
Device	接続を検出したデバイスを 1 つ以上選択します。または（エクスポートされた NetFlow レコードからの接続データの場合）接続を処理したデバイスを 1 つ以上選択します。
ドメイン	1 つ以上のドメインを選択してください。マルチドメイン展開環境では、先祖ドメインによる制約条件がそのドメインの子孫によって報告されるデータにも適用されます。This field is only present if you have ever configured the Firepower Management Center for multitenancy.

指定する項目	選択する演算子と内容
出力インターフェイスまたは入力インターフェイス	インターフェイスを 1 つ以上選択します。
出力セキュリティ ゾーンまたは入力セキュリティ ゾーン	1 つ以上のセキュリティ ゾーンまたはトンネルゾーンを選択します。
イニシエータ バイト数、レスポンダ バイト数、または合計バイト数	次のいずれかを入力します。 • 送信されたバイト数（[イニシエータ バイト数（Initiator Bytes）]）。 • 受信されたバイト数（[レスポンダ バイト数（Responder Bytes）]）。 • 送受信されたバイト数（[合計バイト数（Total Bytes）]）。
イニシエータ IP、レスポンダ IP、イニシエータ IP およびレスポンダ IP の両方、あるいはイニシエータ IP またはレスポンダ IP のいずれか	単一の IP アドレスまたはアドレス ブロックを指定します。
イニシエータ パケット数、レスポンダ パケット数、または合計パケット数	次のいずれかを入力します。 • 送信されたパケット数（[イニシエータ パケット（Initiator Packets）]）。 • 受信されたパケット数（[レスポンダ パケット数（Responder Packets）]）。 • 送受信されたパケット数（[合計パケット数（Total Packets）]）
イニシエータ ポート/ICMP タイプまたはレスポンダ ポート/ICMP コード	イニシエータ トラフィックのポート番号または ICMP タイプ、あるいはレスポンダ トラフィックのポート番号または ICMP コードを入力します。
IOC タグ	接続イベントにより侵害の兆候タグが設定[される（is）]または設定[されない（is not）]かどうかを指定します。
NetBIOS 名	接続におけるモニタ対象ホストの NetBIOS 名を入力します。
NetFlow デバイス	相関ルールをトリガーするために使用する NetFlow エクスポータの IP アドレスを選択します。ネットワーク検出ポリシーに NetFlow エクスポータを追加していない場合、[NetFlow デバイス（NetFlow Device）] ドロップダウン リストは空白になります。
プレフィルタ ポリシー	接続を処理したプレフィルタ ポリシーを 1 つ以上選択します。
理由（Reason）	接続イベントに関連付けられた理由を 1 つ以上選択します。

指定する項目	選択する演算子と内容
セキュリティ インテリジェンス カテゴリ（Security Intelligence Category）	接続イベントに関連付けられたセキュリティインテリジェンスのカテゴリを1つ以上選択します。 接続終了イベントの条件としてセキュリティ インテリジェンス カテゴリを使用するには、アクセス コントロール ポリシーでカテゴリを [ブロック（Block）] ではなく [モニタ（Monitor）] に設定します。
実際の SSL アクション	システムが暗号化された接続をどのように処理したかを示す SSL ルール アクションを指定します。
SSL証明書のフィンガープリント	トラフィックの暗号化に使用された証明書のフィンガープリントを入力するか、フィンガープリントに関連付けられたサブジェクトの共通名を選択します。
SSL 証明書ステータス（SSL Certificate Status）	セッションの暗号化に使用された証明書に関連付けられたステータスを1つ以上選択します。
SSL証明書のサブジェクトの共通名（CN）	セッションの暗号化に使用された証明書のサブジェクトの共通名のすべてまたはその一部を入力します。
SSL証明書のサブジェクトの国（C）	セッションの暗号化に使用された証明書のサブジェクトの国番号を 1 つ以上選択します。
SSL証明書のサブジェクトの組織（O）	セッションの暗号化に使用された証明書のサブジェクトの組織名のすべてまたはその一部を入力します。
SSL証明書のサブジェクトの部門（OU）	セッションの暗号化に使用された証明書のサブジェクトの部門名のすべてまたはその一部を入力します。
SSL 暗号スイート（SSL Cipher Suite）	セッションの暗号化に使用された暗号スイートを 1 つ以上選択します。
SSL 暗号化セッション	[正常に復号（Successfully Decrypted）] を選択します。
SSL フローのステータス	システムによるトラフィック復号化試行の結果に基づくステータスを1つ以上選択します。
SSL ポリシー	暗号化された接続をログに記録した SSL ポリシーを 1 つ以上選択します。
SSL ルール名	暗号化された接続をログに記録した SSL ルールの名前のすべてまたは一部を入力します。
SSL サーバ名	クライアントが暗号化された接続を確立したサーバの名前のすべてまたは一部を入力します。
SSL URL カテゴリ	暗号化された接続でアクセスされた URL のカテゴリを 1 つ以上選択します。
SSL バージョン	セッションの暗号化に使用された SSL または TLS バージョンを 1 つ以上選択します。

指定する項目	選択する演算子と内容
TCP フラグ	相関ルールをトリガーとして使用するために接続イベントに含まれていなければならない TCP フラグを選択します。NetFlow レコードから生成された接続データにのみ TCP フラグが含まれます。
トランスポート プロトコル	接続で使用されたトランスポート プロトコル：**TCP** または **UDP** を入力します。
トンネル/プレフィルタ ルール	接続を処理したトンネルまたはプレフィルタ ルールの名前のすべてまたは一部を入力します。
URL	接続でアクセスされた URL 全体またはその一部を入力します。
URL カテゴリ	接続でアクセスされた URL のカテゴリを 1 つ以上選択します。
URLレピュテーション	接続でアクセスされた URL のレピュテーション値を 1 つ以上選択します。
[ユーザ名（Username）]	接続でいずれかのホストにログインしたユーザのユーザ名を入力します。
Web アプリケーション	接続に関連付けられた Web アプリケーションを 1 つ以上選択します。
Web アプリケーションのカテゴリ	Web アプリケーションのカテゴリを 1 つ以上選択します。

関連トピック

接続イベントとセキュリティ インテリジェンス イベントのフィールド （3024 ページ）
Firepower システムの IP アドレス表記法 （20 ページ）

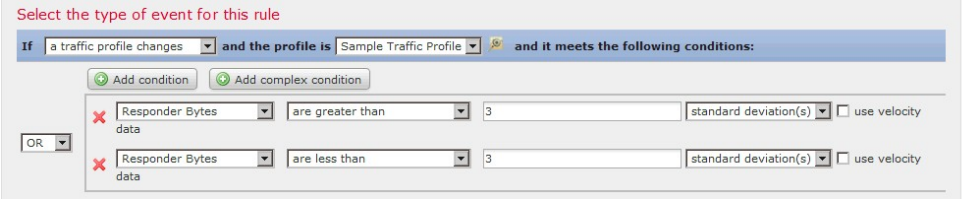
トラフィック プロファイル変化の構文

トラフィック プロファイル変化で相関ルールをベースとして使用するには、まず、使用するトラフィック プロファイルを選択します。ルールは、選択するプロファイルによって特徴付けられるパターンからネットワーク トラフィックが逸脱するときにトリガーされます。

raw データ、またはデータから計算された統計情報のいずれかに基づいてルールをトリガーできます。たとえば、ネットワーク内を移動するデータ量（バイト数で測定）が急激に変化した場合、攻撃または他のセキュリティー ポリシー違反が発生した可能性がありますが、そのような変動時にトリガーとして使用されるルールを作成できます。以下のいずれかの場合にトリガーとして使用されるよう、ルールを指定できます。

- ネットワーク内を移動するバイト数が特定のバイト数を上回る場合
- ネットワーク内を移動するバイト数が、平均トラフィック量より上または下の特定数の標準偏差を超えて急激に変化した場合

  ネットワーク内を移動するバイト数が、特定数の標準偏差からなる範囲を（上または下に）超えたときにトリガーとして使用されるルールを作成するには、次の図に示すように、上限と下限を指定する必要があります。



移動するバイト数が、平均より上側の特定数の標準偏差を超えた場合にトリガーするルールを作成するには、以下の図に示されている最初の条件だけを使用します。

移動するバイト数が、平均を基準とした特定数の標準偏差の下側を超えた場合にトリガーとして使用されるルールを作成するには、2 番目の条件だけを使用します。

[速度データを使用する（use velocity data）] チェックボックスを選択すると、データ ポイント間の変化率に基づいて相関ルールをトリガーできます。上記の例で仮に速度データを使用する場合は、次のいずれかの時点でルールがトリガーとして使用されるように指定できます。

- ネットワーク内を移動するバイト数の変化が、平均変化率より上または下の特定数の標準偏差を超えた場合
- ネットワーク内を移動するバイト数の変化が、特定のバイト数を上回った場合

トラフィック プロファイル変化を基準イベントとして選択した場合、以下の表で説明する方法に従って相関ルールの条件を作成します。

表 *273*：トラフィック プロファイル変化の構文

指定する項目	選択する演算子と入力内容	いずれかを選択
接続数	検出された接続の合計数 **または** 平均より上または下の標準偏差の数（検出された接続数がこれを超えるとルールがトリガーとして使用されます）	connections：接続数 standard deviation(s)：標準偏差の数
合計バイト数、イニシエータ バイト数、またはレスポンダ バイト数	次のいずれかになります。 • 送信された合計バイト数（[Total Bytes]） • イニシエータから送信されたバイト数（[Initiator Bytes]） • レスポンダで受信されたバイト数（[Responder Bytes]） **または** 平均より上または下の標準偏差の数（検出された接続数がこれを超えるとルールがトリガーとして使用されます）	bytes：バイト数 standard deviation(s)：標準偏差の数

指定する項目	選択する演算子と入力内容	いずれかを選択
合計パケット数、イニシエータ パケット数、またはレスポンダ パケット数	次のいずれかになります。 • 送信された合計パケット数（[Total Packets]） • イニシエータから送信されたパケット数（[Initiator Packets]） • レスポンダで受信されたパケット数（[Responder Packets]） **または** 平均より上または下の標準偏差の数（上記のいずれかの基準がこれを超えると、ルールがトリガーとして使用されます）	packets：パケット数 standard deviation(s)：標準偏差の数
Unique Initiators	セッションを開始した個別のホストの数 **または** 平均より上または下の標準偏差の数（検出された接続数がこれを超えるとルールがトリガーとして使用されます）	initiators：イニシエータ数 standard deviation(s)：標準偏差の数
Unique Responders	セッションに応答した個別のホストの数 **または** 平均より上または下の標準偏差の数（検出された接続数がこれを超えるとルールがトリガーとして使用されます）	responders：レスポンダ数 standard deviation(s)：標準偏差の数

相関ホスト プロファイル限定の構文

イベントに関連するホストのホスト プロファイルに基づいて相関ルールを制約するには、[ホスト プロファイル限定（host profile qualification）] を追加します。マルウェア イベント、トラフィック プロファイル変化、または新しい IP ホスト検出によってトリガーとして使用される相関ルールには、ホスト プロファイル限定を追加することはできません。

ホストプロファイル限定を作成するときには、まず、相関ルールを制約するために使用するホストを指定します。選択可能なホストは、ルールの基盤となるイベントのタイプによって異なります。

- 接続イベント：[レスポンダ ホスト（Responder Host）] または [イニシエータ ホスト（Initiator Host）] を選択します。
- 侵入イベント：[宛先ホスト（Destination Host）] または [送信元ホスト（Source Host）] を選択します。
- ディスカバリ イベント、ホスト入力イベントは、またはユーザ アクティビティ：[ホスト（Host）] を選択します。

次の表では、相関ルールのホスト プロファイル限定を作成する方法について説明します。

表 *274*：ホスト プロファイル限定の構文

指定する項目	選択する演算子と内容
[アプリケーション プロトコル（Application Protocol）] > [アプリケーション プロトコル（Application Protocol）]	アプリケーション プロトコルを選択します。
[アプリケーション プロトコル（Application Protocol）] > [アプリケーション ポート（Application Port）]	アプリケーションプロトコルのポート番号を入力します。
[アプリケーション プロトコル（Application Protocol）] > [プロトコル（Protocol）]	プロトコルを選択します。
[アプリケーション プロトコル カテゴリ（Application Protocol Category）]	カテゴリを選択します。
[クライアント（Client）] > [クライアント（Client）]	クライアントを選択します。
[クライアント（Client）] > [クライアント バージョン（Client Version）]	クライアント バージョンを入力します。
[クライアント カテゴリ（Client Category）]	カテゴリを選択します。
ドメイン	1 つ以上のドメインを選択してください。マルチドメイン展開環境では、先祖ドメインによる制約条件がそのドメインの子孫によって報告されるデータにも適用されます。This field is only present if you have ever configured the Firepower Management Center for multitenancy.
[ハードウェア（Hardware）]	モバイル デバイスのハードウェア モデルを入力します。たとえば、すべての Apple iPhone に一致させるには **`iPhone`** と入力します。
[ホストの重要度（Host Criticality）]	ホストの重要度を選択します。
[ホスト タイプ（Host Type）]	ホスト タイプを 1 つ以上選択します。通常のホスト、またはいずれかのタイプのネットワーク デバイスを選択できます。
[IOC タグ（IOC Tag）]	侵害の兆候タグを 1 つ以上選択します。
[ジェイルブロークン（Jailbroken）]	イベントのホストがジェイルブレイクされたモバイル デバイスであることを示すには [はい（Yes）] を、そうでない場合は [いいえ（No）] を選択します。
[MAC アドレス（MAC Address）] > [MAC アドレス（MAC Address）]	ホストの MAC アドレス全体またはその一部を入力します。

指定する項目	選択する演算子と内容
[MAC アドレス（MAC Address）] > [MAC タイプ（MAC Type）]	MAC タイプが ARP/DHCP で検出されるかどうかを選択します。 • システムは MAC アドレスがホストに属していることをポジティブに識別した（[ARP/DHCP で検出（is ARP/DHCP Detected）]） • たとえば、デバイスとホスト間にはルータがあるため、システムはその MAC アドレスを持つ多くのホストを認識している（[ARP/DHCP で検出されない（is not ARP/DHCP Detected）]） • MAC タイプが無関係（[どれでもない（is any）]）
[MAC ベンダー（MAC Vendor）]	ホストが使用するハードウェアの MAC ベンダー全体またはその一部を入力します。
Mobile	イベントのホストがモバイル デバイスであることを示すには [はい（Yes）] を、そうでない場合は [いいえ（No）] を選択します。
[NetBIOS 名（NetBIOS Name）]	ホストの NetBIOS 名を入力します。
ネットワーク プロトコル	http://www.iana.org/assignments/ethernet-numbers にリストされているネットワーク プロトコル番号を入力します。
[オペレーティング システム（Operating System）] > [OS ベンダー（OS Vendor）]	オペレーティング システムのベンダー名を 1 つ以上選択します。
[オペレーティング システム（Operating System）] > [OS 名（OS Name）]	オペレーティング システムの名前を 1 つ以上選択します。
[オペレーティング システム（Operating System）] > [OS バージョン（OS Version）]	オペレーティング システムのバージョンを 1 つ以上選択します。
[トランスポート プロトコル（Transport Protocol）]	http://www.iana.org/assignments/protocol-numbers にリストされているトランスポート プロトコルの名前または番号を入力します。
VLAN ID（Admin. VLAN ID）	ホストの VLAN ID 番号を入力します。
[Web アプリケーション（Web Application）]	Web アプリケーションを選択します。
[Web アプリケーションのカテゴリ（Web Application Category）]	カテゴリを選択します。
使用可能な任意のホスト属性（デフォルト コンプライアンス ホワイトリスト ホスト属性を含む）	ホスト属性タイプに応じて適切な値を入力または選択します。

暗黙的または汎用のクライアントを使用したホスト プロファイル限定の作成

システムが client が続くアプリケーション プロトコルの名前（たとえば、HTTPS client）を使用して検出されたクライアントをレポートする場合、このクライアントは暗黙的または汎用のクライアントです。これらの場合、システムは特定のクライアントを検出していませんが、サーバ応答トラフィックに基づいてクライアントの存在を推測しています。

暗黙的または汎用のクライアントを使用してホスト プロファイル限定を作成するには、クライアントではなく、レスポンダ ホストで実行されているアプリケーション プロトコルを使用して制約します。

イベント データを使用したホスト プロファイル限定の作成

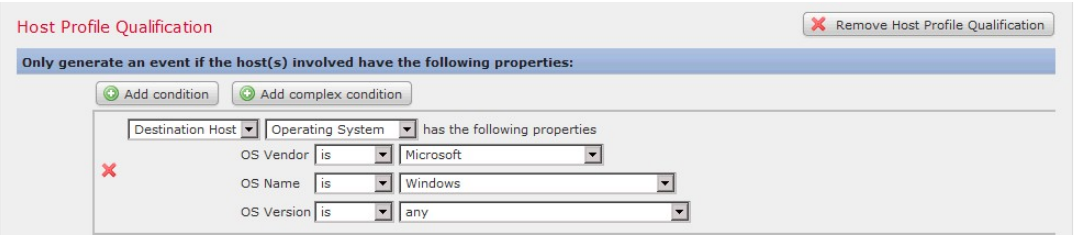
ホスト プロファイル限定の制約時に、多くの場合、相関ルールの基本イベントからデータを使用できます。

たとえば、モニタ対象のいずれかのホストで特定のブラウザが使用されていることをシステムが検出した場合に、相関ルールがトリガーとして使用されるとします。さらに、この使用を検出するときに、ブラウザのバージョンが最新でない場合はイベントを生成すると仮定します。

この場合、[クライアント（Client）] は [イベント クライアント（Event Client）] ですが、[クライアント バージョン（Client Version）] が最新のバージョンでない場合にのみルールがトリガーされるように、この相関ルールをホスト プロファイル限定に追加できます。

ホスト プロファイル限定の例

次のホスト プロファイル限定は、ルールの基礎となるディスカバリ イベントに関連するホストが Microsoft Windows のバージョンを実行している場合にのみ、ルールがトリガーとして使用されるように相関ルールを制約します。



関連トピック

ホスト データ フィールド （3212 ページ）

ユーザ限定の構文

接続、侵入、ディスカバリ、またはホスト入力のいずれかのイベントを使用して相関ルールをトリガーとして使用する場合、イベントに関連するユーザのアイデンティティに基づいてルールを制約することができます。この制約は、ユーザ限定と呼ばれます。たとえば、送信元または宛先ユーザのアイデンティティが販売部門所属である場合にのみトリガーとして使用するよう、相関ルールを制約できます。

トラフィック プロファイル変化やユーザ アクティビティ検出によってトリガーとして使用される相関ルールに、ユーザ限定を追加することはできません。また、システムは、アイデンティティ レルムで確立された Firepower Management Center サーバの接続を介してユーザの詳細を取得します。この情報は、データベース内のすべてのユーザに関して入手可能とは限りません。

ユーザ限定を作成するときには、まず、相関ルールを制約するために使用するアイデンティティを指定します。選択可能なアイデンティティは、ルールの基本イベントのタイプによって異なります。

- 接続イベント：[イニシエータのアイデンティティ（Identity on Initiator）] または [レスポンダのアイデンティティ（Identity on Responder）] を選択します。
- 侵入イベント：[宛先のアイデンティティ（Identity on Destination）] または [送信元のアイデンティティ（Identity on Source）] を選択します。
- ディスカバリ イベント：[ホストのアイデンティティ（Identity on Host）] を選択します。
- ホスト入力イベント：[ホストのアイデンティティ（Identity on Host）] を選択します。

次の表では、相関ルールのユーザ限定を作成する方法について説明します。

表 *275* : ユーザ限定の構文

指定する項目	選択する演算子と内容
認証プロトコル（Authentication Protocol）	ユーザを検出するために使用される認証プロトコル（またはユーザ タイプ）プロトコルを選択します。
部署名（Department）	部署を入力します。
ドメイン（Domain）	1 つ以上のドメインを選択してください。マルチドメイン展開環境では、先祖ドメインによる制約条件がそのドメインの子孫によって報告されるデータにも適用されます。This field is only present if you have ever configured the Firepower Management Center for multitenancy.
E メール	電子メール アドレスを入力します。
名	名を入力します。
姓	姓を入力します。
電話	電話番号を入力します。
[ユーザ名（Username）]	ユーザ名を入力します。

関連トピック

ユーザ データのフィールド

接続トラッカー

接続トラッカー は、ルールの最初の基準（ホスト プロファイルおよびユーザ認定を含む）に一致した後にシステムが特定の接続のトラッキングを始めるよう、相関ルールを制約します。追跡される接続が、指定した期間にわたって収集された追加の基準を満たす場合には、システムがルールの相関イベントを生成します。

ヒント 通常、接続トラッカーは特定のトラフィックだけをモニタし、トリガーとして使用された場合には指定された一定期間だけ実行されます。接続トラッカーは、広範なネットワーク トラフィックをモニタして持続的に実行されるトラフィック プロファイルとは対照的です。

接続トラッカーがイベントを生成する方法は 2 つあります。

条件に一致するとただちに起動する接続トラッカー

ネットワーク トラフィックが接続トラッカーの条件に一致すると即座に相関ルールが起動するよう、接続トラッカーを設定できます。この場合、タイムアウト期間が満了していなくても、システムはその接続トラッカー インスタンスでの接続追跡を停止します。相関ルールをトリガーとして使用したのと同じタイプのポリシー違反が再び発生した場合、システムは新しい接続トラッカーを作成します。

ただし、ネットワーク トラフィックが接続トラッカーの条件に一致する前にタイムアウト期間が満了した場合、システムは相関イベントを生成せず、そのルール インスタンスの接続のトラッキングを停止します。

たとえば、特定のタイプの接続が特定の期間中に特定回数を超えて発生した場合にのみ相関イベントを生成させることで、接続トラッカーをある種のイベントしきい値として機能させることができます。あるいは、初回接続後に過剰なデータ転送量をシステムが検出した場合にのみ、相関イベントを生成させることもできます。

タイムアウト期間の満了時に起動する接続トラッカー

タイムアウト期間全体にわたって収集されるデータに依存するよう、接続トラッカーを設定できます。この場合、タイムアウト期間が満了するまでは起動しません。

たとえば、特定の期間内に検出された転送量が特定のバイト数を下回った場合に接続トラッカーを起動するよう設定すると、システムはその期間が経過するまで待って、ネットワーク トラフィックがその条件に一致した場合はイベントを生成します。

接続トラッカーの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Discovery Admin

始める前に

- 接続、侵入、検出、ユーザID、ホスト入力イベントに基づいて相関ルールを作成します。マルウェア イベントやトラフィック プロファイルの変更に基づいたルールに接続トラッカーを追加することはできません。

ステップ 1 相関ルールエディタで、[接続トラッカーの追加（Add Connection Tracker）] をクリックします。

ステップ 2 追跡する接続を指定します。接続トラッカーの構文 （2726 ページ） を参照してください。

ステップ 3 追跡する接続に応じて、いつ相関イベントを生成するかを指定します。接続トラッカーイベントの構文（2729 ページ） を参照してください。

ステップ 4 トラッカーの条件が満たされなければならない時間の間隔（秒、分または時）を指定します。

接続トラッカーの構文

次の表は、どのような接続を追跡するかを指定する接続トラッカー条件の作成方法を説明しています。

表 *276 :* 接続トラッカーの構文

指定する項目	選択する演算子と内容
アクセス コントロール ポリシー	追跡対象の接続を処理したアクセス コントロール ポリシーを 1 つ以上選択します。
アクセス コントロール ルールのアクション	追跡対象の接続をログに記録したアクセス コントロール ルールに関連付けられたアクセス コントロール ルール アクションを 1 つ以上選択します。 あとで接続を処理するルールまたはデフォルト アクションとは無関係に、任意のモニタ ルールの条件に一致する接続を追跡するには、[モニタ（Monitor）] を選択します。
アクセス コントロール ルール名	追跡対象の接続をログに記録したアクセス コントロール ルールの名前のすべてまたはその一部を入力します。 モニタ ルールに一致する接続を追跡するには、モニタ ルールの名前を入力します。あとで接続を処理するルールまたはデフォルト アクションとは無関係に、システムは該当する接続を追跡します。
アプリケーション プロトコル	アプリケーション プロトコルを 1 つ以上選択します。
[アプリケーション プロトコル カテゴリ（Application Protocol Category）]	アプリケーション プロトコル カテゴリを 1 つ以上選択します。
クライアント	クライアントを 1 つ以上選択します。

指定する項目	選択する演算子と内容
[クライアント カテゴリ（Client Category）]	クライアント カテゴリを 1 つ以上選択します。
クライアント バージョン	クライアントのバージョンを入力します。
接続時間	接続時間（秒数）を入力します。
接続タイプ	接続情報がどのように取得されたかに基づいて、相関ルールをトリガーするかどうかを指定します。 • エクスポートされた NetFlow レコードから生成された接続イベントに、[生成元（is）] および [Netflow] を選択します。 • Firepower システムの管理対象デバイスによって検出された接続イベントに、[生成元でない（is not）] および [Netflow] を選択します。
接続先（国）または送信元（国）	国を 1 つ以上選択します。
Device	追跡対象の接続を検出したデバイスを 1 つ以上選択します。NetFlow 接続を追跡する場合は、エクスポートされた NetFlow レコードからの接続データを処理するデバイスを選択します。
入力インターフェイスまたは出力インターフェイス	インターフェイスを 1 つ以上選択します。
入力セキュリティ ゾーンまたは出力セキュリティ ゾーン	1 つ以上のセキュリティ ゾーンまたはトンネルゾーンを選択します。
イニシエータ IP、レスポンダ IP、またはイニシエータ/レスポンダ IP	単一の IP アドレスまたはアドレス ブロックを入力します。
イニシエータ バイト数、レスポンダ バイト数、または合計バイト数	次のいずれかを入力します。 • 送信されたバイト数（[イニシエータ バイト数（Initiator Bytes）]） • レスポンダで受信されたバイト数（[Responder Bytes]） • 送受信されたバイト数（[合計バイト数（Total Bytes）]）

指定する項目	選択する演算子と内容
イニシエータ パケット数、レスポンダ パケット数、または合計パケット数	次のいずれかを入力します。 • 送信されたパケット数（[イニシエータ パケット（Initiator Packets）]） • レスポンダで受信されたパケット数（[Responder Packets]） • 送受信されたパケット数（[Total Packets]）
イニシエータ ポート/ICMP タイプまたはレスポンダ ポート/ICMP コード	イニシエータ トラフィックのポート番号または ICMP タイプ、あるいはレスポンダ トラフィックのポート番号または ICMP コードを入力します。
IOC タグ	侵害の兆候タグが設定されて [いる（is）] または設定されて [いない（is not）] かどうかを選択します。
NETBIOS 名	接続におけるモニタ対象ホストの NetBIOS 名を入力します。
NetFlow デバイス	追跡する NetFlow エクスポータの IP アドレスを選択します。ネットワーク検出ポリシーに NetFlow エクスポータを追加していない場合、[NetFlow デバイス（NetFlow Device）] ドロップダウン リストは空白になります。
プレフィルタ ポリシー	追跡対象の接続を処理したプレフィルタ ポリシーを 1 つ以上選択します。
理由（Reason）	追跡対象の接続に関連付けられている理由を 1 つ以上選択します。
セキュリティ インテリジェンス カテゴリ	追跡対象の接続に関連付けられているセキュリティ インテリジェンスのカテゴリを 1 つ以上選択します。
TCP フラグ	接続を追跡するために接続に含まれている必要のある TCP フラグを選択します。TCP フラグ データは、エクスポートされた NetFlow レコードから生成された接続にのみ含まれます。
トランスポート プロトコル	接続に使用されるトランスポート プロトコルを選択します。
URL	追跡対象の接続でアクセスされた URL のすべてまたはその一部を入力します。
URL Category	追跡対象の接続でアクセスされた URL のカテゴリを 1 つ以上選択します。

指定する項目	選択する演算子と内容
URLレピュテーション	追跡対象の接続でアクセスされた URL のレピュテーション値を 1 つ以上選択します。
[ユーザ名（Username）]	追跡対象の接続でいずれかのホストにログインしたユーザのユーザ名を入力します。
[Web アプリケーション（Web Application）]	Web アプリケーションを 1 つ以上選択します。
Web アプリケーションのカテゴリ	Webアプリケーションのカテゴリを1つ以上選択します。

イベント データを使用した接続トラッカーの作成

接続トラッカーを作成するときに、多くの場合、相関ルールの基本イベントからデータを使用できます。

たとえば、システムが新しいクライアントを検出するときに、相関ルールがトリガーされると想定します。接続トラッカーをこのタイプの相関ルールに追加すると、システムは次の基本イベントを参照する制約のあるトラッカーを自動的に入力します。

- [イニシエータ/レスポンダ IP（Initiator/Responder IP）] が [イベント IP アドレス（Event IP Address）] に設定される。
- [クライアント（Client）] が [イベント クライアント（Event Client）] に設定される。

ヒント 特定の IP アドレスまたは IP アドレス ブロックに関連する接続を追跡するには、[手動エントリにスイッチ（switch to manual entry）] をクリックして、手動で IP を指定します。[イベントフィールドにスイッチ（switch to event fields）] をクリックすると、イベントの IP アドレスを使用する設定に戻ります。

関連トピック

接続イベントとセキュリティ インテリジェンス イベントのフィールド （3024 ページ）
Firepower システムの IP アドレス表記法 （20 ページ）

接続トラッカー イベントの構文

追跡対象の接続に基づいてどのようなときに相関イベントを生成するかを指定する接続トラッカー条件を作成するには、次の表の説明に従います。

表 *277*：接続トラッカー イベントの構文

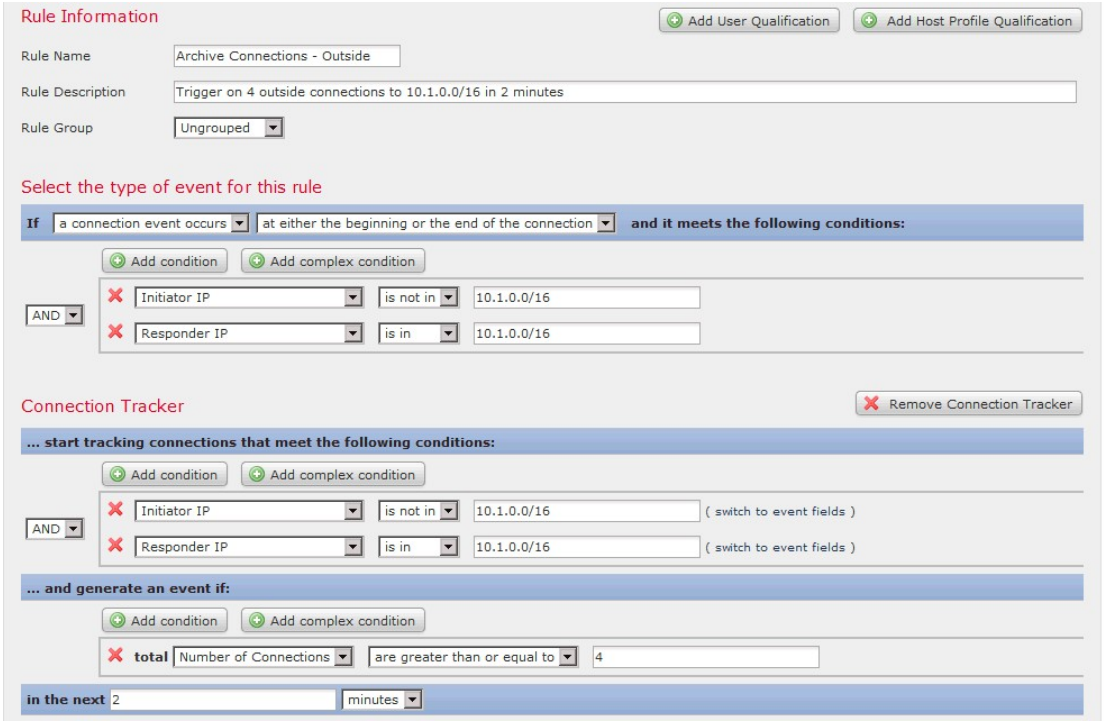
指定する項目	選択する演算子と入力内容
接続数	検出された接続の合計数
SSL 暗号化セッションの数	検出された SSL または TLS 暗号化セッションの合計数

指定する項目	選択する演算子と入力内容
合計バイト数、イニシエータ バイト数、またはレスポンダ バイト数	次のいずれかになります。 • 送信された合計バイト数（[Total Bytes]） • イニシエータから送信されたバイト数（[Initiator Bytes]） • 受信されたバイト数（[レスポンダ バイト数（Responder Bytes）]）
合計パケット数、イニシエータ パケット数、またはレスポンダ パケット数	次のいずれかになります。 • 送信された合計パケット数（[Total Packets]） • イニシエータから送信されたパケット数（[Initiator Packets]） • 受信されたパケット数（[レスポンダ パケット数（Responder Packets）]）
一意のイニシエータまたは一意のレスポンダ	次のいずれかになります。 • 検出されたセッションを開始した個別のホスト数（[一意のイニシエータ（Unique Initiators）]） • 検出された接続に応答した個別のホスト数（[一意のレスポンダ（Unique Responders）]）

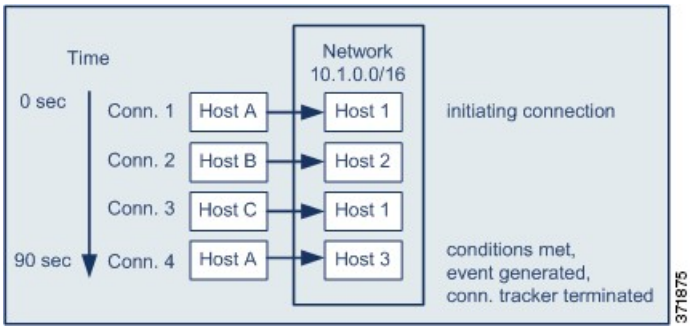
外部ホストからの過剰な接続の設定例

ネットワーク 10.1.0.0/16 のセンシティブ ファイルをアーカイブし、通常、ネットワーク外のホストはネットワーク内のホストへの接続を開始することはないシナリオを考慮します。時にはネットワーク外部から接続が開始されることもありますが、2 分以内に 4 つ以上の接続が開始された場合には注意が必要だと判断するとします。

次の図に示すルールでは、接続が 10.1.0.0/16 ネットワーク外からネットワーク内に発生したときに、基準に適合するトラッキング接続を開始するように指定します。その後、2 分以内に署名に一致する 4 つの接続（発信側の接続を含む）が検出されても相関イベントを生成します。



以下の図は、ネットワーク トラフィックが上記の相関ルールをトリガーとして使用できる方法を示します。



この例では、相関ルールの基本条件に一致する接続をシステムが検出しました。つまり、ネットワーク 10.1.0.0/16 の外部にあるホストからネットワーク内部のホストへの接続をシステムが検出しました。これにより、接続トラッカーが作成されました。

接続トラッカーは、次のステージで処理します。

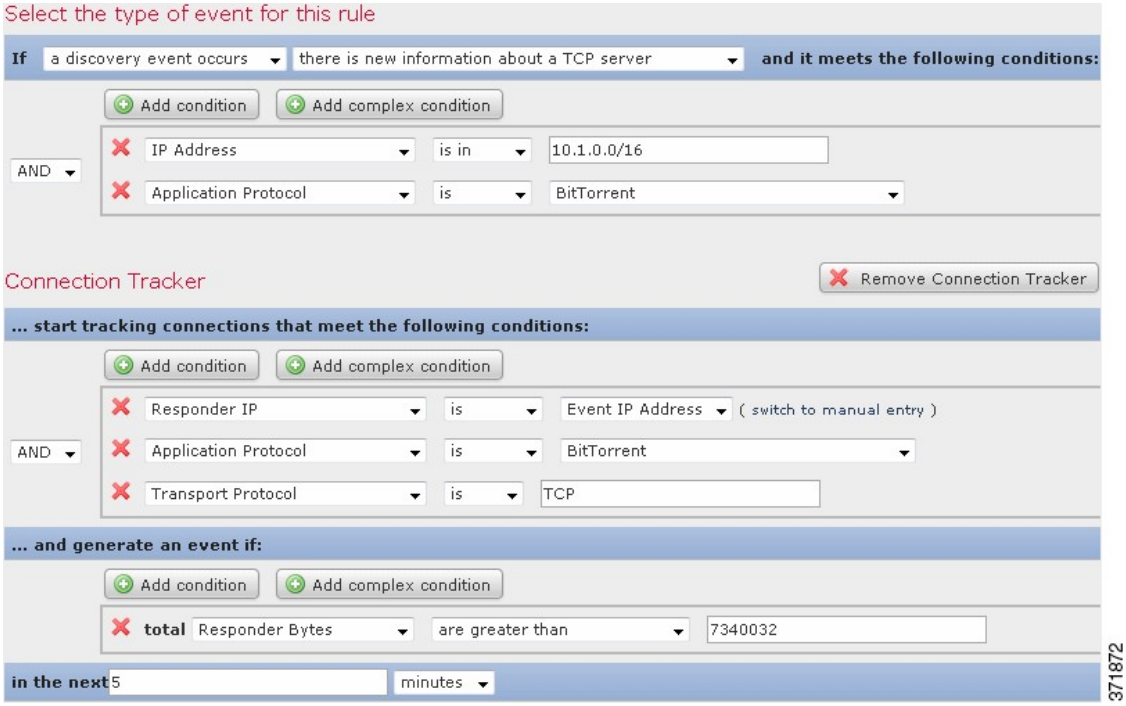
- ネットワーク外のホスト A からネットワーク内のホスト 1 への接続が検出されると、トラッキング接続を開始します。
- 接続トラッカーの署名に一致する 2 つ以上の接続（ホスト B ～ホスト 2、ホスト C ～ホスト 1）を検出します。
- 2 分の制限時間内にホスト A がホスト 3 に接続すると、システムは 4 番目の該当する接続を検出します。ルール条件が適合します。

• 最後に、相関イベントを生成し、トラッキング接続を停止します。

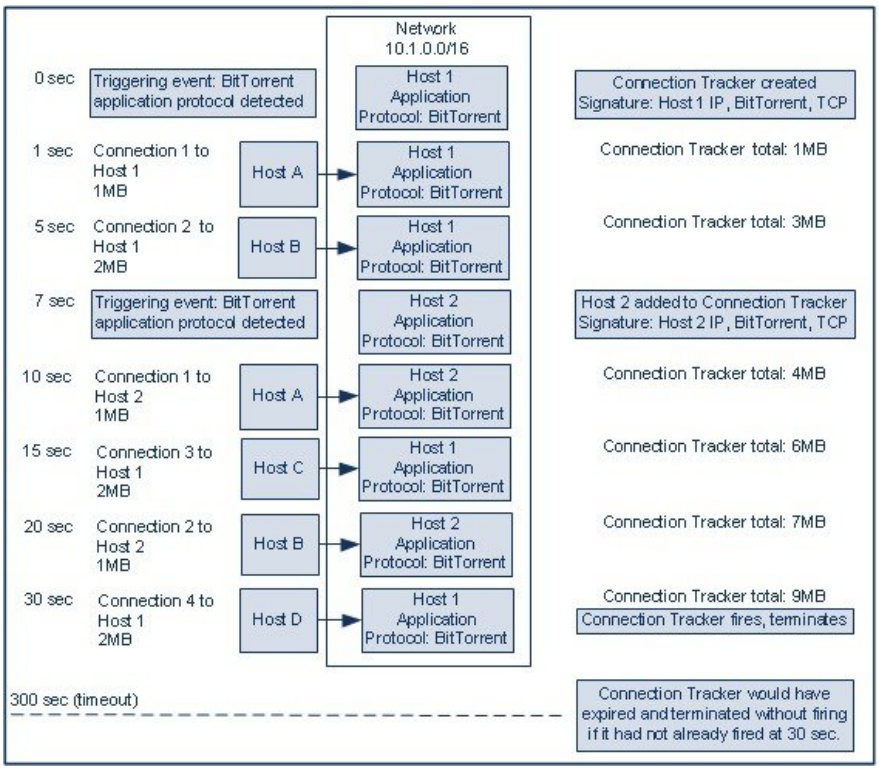
BitTorrent の過剰なデータ転送の設定例

最初に監視対象のネットワークのホストに接続後、過剰な BitTorrent データの転送が検出された場合は相関イベントを生成するシナリオを考慮します。

モニタ対象ネットワークでシステムが BitTorrent アプリケーション プロトコルを検出したときにトリガーとして使用される相関ルールを以下の図に示します。このルールには、監視対象ネットワークのホスト（この例では 10.1.0.0/16）が、最初のポリシー違反後の 5 分間に 7 MB を超えるデータ（7340032 バイト）を BitTorrent を介してまとめて転送する場合にのみルールがトリガーとして使用されるように制約する接続トラッカーがあります。



以下の図は、ネットワーク トラフィックが上記の相関ルールをトリガーとして使用できる方法を示します。



この例では、2 つのホスト（ホスト 1、ホスト 2）に BitTorrent TCP アプリケーション プロトコルが検出されました。この 2 つのホストは、他の 4 つのホスト（ホスト A、ホスト B、ホスト C、ホスト D）に BitTorrent を介してデータを転送しました。

接続トラッカーは、次の工程で処理しました。

- まず、ホスト 1 で BitTorrent アプリケーション プロトコルが検出されると、0 秒マーカーで接続のトラッキングを開始します。次の 5 分の間に 7MB の BitTorrent TCP データの転送が検出されない場合（300 秒マーカーにより）、接続トラッカーは無効になる点にご注意ください。
- 5 秒経過した時点で、ホスト 1 はシグニチャに一致する 3MB のデータを次のように送信しました。
  - 1 秒マーカーの時点で、ホスト 1 からホスト A に 1MB を転送（接続トラッカーの条件適合に向けて合計 1MB の BitTorrent トラフィックをカウント）
  - 2 秒マーカーの時点で、ホスト 1 からホスト B に 2MB（合計 3MB）
- 7 秒経過した時点で、システムはホスト 2 での BitTorrent アプリケーション プロトコルを検出し、そのホストでも BitTorrent 接続を追跡し始めます。
- 20 秒経過した時点で、システムは、シグニチャに一致するさらに他のデータがホスト 1 およびホスト 2 から転送されていることを検出しました。
  - 10 秒マーカーの時点で、ホスト 2 からホスト A に 1MB（合計 4MB）

- 15 秒マーカーの時点で、ホスト 1 からホスト C に 2MB（合計 6MB）
- 20 秒マーカーの時点で、ホスト 2 からホスト B に 1MB（合計 7MB）

- ホスト 1 とホスト 2 が転送した BitTorrent データは合計で 7MB になりましたが、転送された合計バイト数が 7MB を**超過**していることが条件となっているため（**Responder Bytes are greater than 7340032**）、ルールはトリガーとして使用されません。この時点で、トラッカーのタイムアウト期間内の残りの 280 秒の間、追加の BitTorrent 転送が検出されない場合に、トラッカーは無効になり、相関イベントは作成されません。
- ただし、30 秒の時点で、別の BitTorrent 転送が検出され、次のルールの条件が満たされます。
  - 30 秒マーカーでは、ホスト 1 からホスト D へ 2 MB（合計 9 MB）
- 最後に、相関イベントが生成されます。また、5分間が無効にならなくても接続トラッカーインスタンスについてはトラッキング接続を停止します。この時点で BitTorrent TCP アプリケーションプロトコルを用いて新しい接続が検出されると、新しい接続トラッカーが生成されます。ホスト 1 が 2 MB すべてをホスト D に転送した後に相関イベントが生成される点にご注意ください。これは、セッションが終了するまで接続データを計算することはないためです。

スヌーズ期間および非アクティブ期間

相関ルールでスヌーズ期間を設定することができます。スヌーズ期間を設定すると、相関ルールがトリガーとして使用されたとき、指定した時間間隔内にルール違反が再び発生しても、システムはその期間中はルールのトリガーを停止します。スヌーズ期間が経過すると、ルールは再びトリガー可能になります（新しいスヌーズ期間が始まります）。

たとえば、通常はトラフィックを全く生成しないはずのホストがネットワーク上にあるとします。このホストが関与する接続がシステムで検出されるたびにトリガーとして使用される単純な相関ルールの場合、このホストで送受信されるネットワークトラフィックによっては、短時間に多数の相関イベントが生成される可能性があります。ポリシー違反を示す相関イベントの数を制限するために、スヌーズ期間を追加できます。これにより、（指定した期間内に）システムで検出されたそのホストに関連する最初の接続に対してのみ、システムは相関イベントを生成します。

また、相関ルールで非アクティブ期間を設定することもできます。非アクティブ期間中は、相関ルールはトリガーとして使用されません。非アクティブ期間を毎日、毎週、または毎月繰り返すように設定できます。たとえば、ホスト オペレーティング システム変更を探すために内部ネットワークで夜間に Nmap スキャンを実行するとします。この場合、相関ルールが誤ってトリガーとして使用されないよう、毎日のスキャン時間帯に、該当する相関ルールで非アクティブ期間を設定することができます。

相関ルールの作成メカニズム

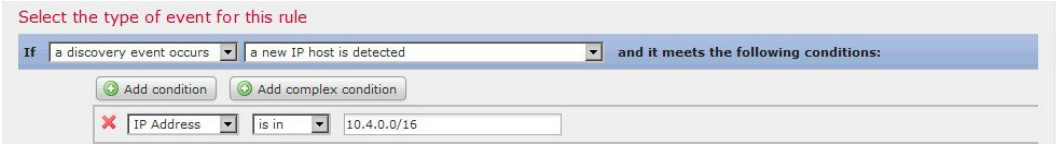
相関ルールは、ルールがトリガーされる条件を指定して作成します。条件で使用できるシンタックスは、作成しようとしている要素により異なりますが、メカニズムはすべて同じです。

ほとんどの条件は、カテゴリ、演算子、値の 3 つの部分からなります。

- 相関ルール トリガー、ホスト プロファイル認定、接続トラッカー、ユーザ認定のどれを作成しているのかに応じて、選択できるカテゴリが異なります。相関ルール トリガーでは、さらにルールの基本イベント タイプにより選択できるカテゴリが異なります。条件によっては、それぞれ独自の演算子と値を持つ複数のカテゴリが含まれることがあります。
- 条件に使用可能な演算子はカテゴリによって異なります。
- 条件の値を指定するために使用できるシンタックスは、カテゴリと演算子に応じて異なります。場合によっては、テキスト フィールドに値を入力する必要があります。それ以外の場合、ドロップダウン リストから値（1 つあるいは複数の値）を選択できます。

たとえば、新しいホストが検出されるたびに相関イベントを生成するには、条件を一切含まない単純なルールを作成できます。

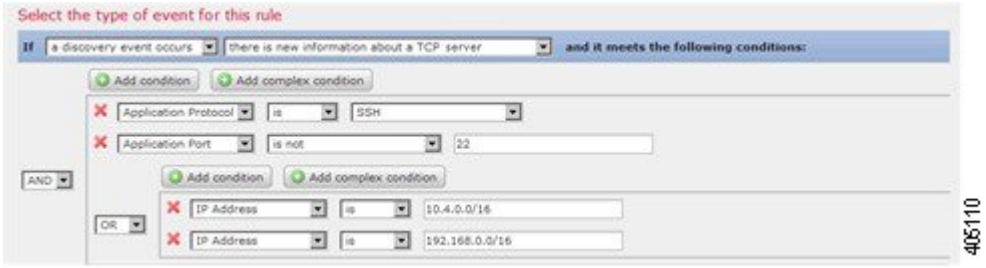
ルールをさらに制約して、新しいホストが 10.4.x.x ネットワークで検出された場合にのみイベントを生成するには、1 つの条件を追加できます。



構造に複数の条件を含める場合は、それらの条件を [および（AND）] 演算子または [または（OR）] 演算子で結合する必要があります。同じレベルにある複数の条件は、一緒に評価されます。

- **AND** 演算子は、制御対象のレベルにあるすべての条件が満たされなければならないことを示します。
- [または（OR）] 演算子は、制御対象のレベルにある複数の条件の少なくとも 1 つが満たされている必要があることを示します。

10.4.x.x ネットワークおよび 192.168.x.x ネットワーク上の非標準ポートで SSH アクティビティを検出する以下のルールには、4 つの条件が設定されており、下の 2 つは複合条件を形成しています。



論理的には、ルールは次のように評価されます。

```
(A and B and (C or D))
```

表 *278 :* ルールの評価

条件	条件で指定する内容
A	アプリケーション プロトコルが SSH である
B	アプリケーション ポートが 22 ではない
C	IP アドレスが 10.0.0.0/8 内にある
D	IP アドレスが 196.168.0.0/16 内にある

⚠

注意 頻繁に発生するイベントによってトリガーされる複雑な相関ルールを評価することにより、システムパフォーマンスが低下する可能性があります。たとえば、ロギングするすべての接続に対して、複数の条件からなるルールをシステムが評価しなければならない場合、リソースが過負荷になる可能性があります。

相関ルールへの条件の追加とリンク設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Discovery Admin

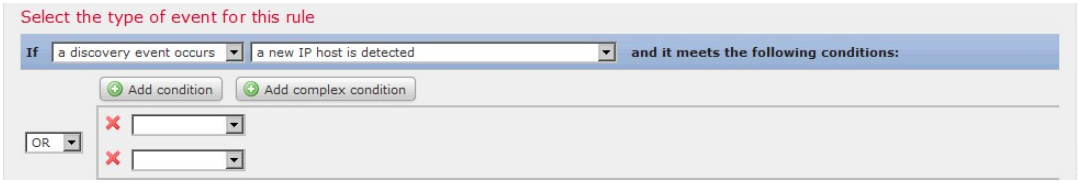
ステップ 1 相関ルールエディタで、単純条件または複合条件を追加します。

- 単純：[条件の追加（Add condition）] をクリックします。
- 複合：[複合条件の追加（Add complex condition）] をクリックします。

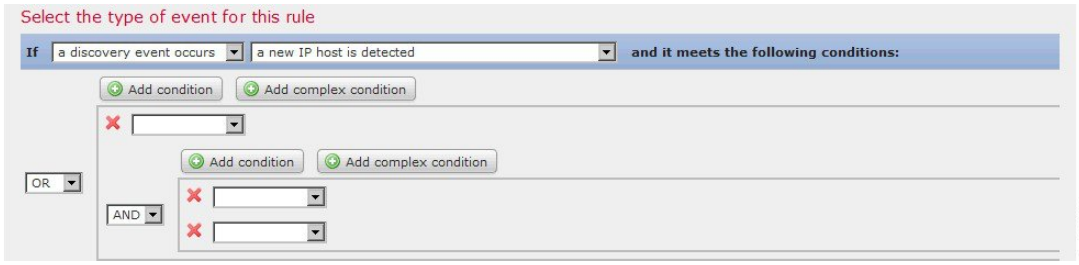
ステップ 2 条件の左にあるドロップダウン リストから [AND] または [OR] 演算子を選択して条件を結合します。

例:単純条件と複合条件の対比

次の図は、単純条件 2 つを [OR] 演算子で結合した相関ルールを示したものです。



次の図は、単純条件 1 つと、複合条件 1 つを [OR] 演算子で結合した相関ルールを示したものです。複合条件は 2 つの単純条件を [AND] 演算子で結合して構成します。



相関ルール条件での複数の値の使用

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Discovery Admin

相関条件を作成するときに、条件の構文でドロップダウン リストから値を選択できる場合、通常はリストから複数の値を選択できます。

ステップ 1 相関ルール エディタで、演算子として [存在する（is in）] または [存在しない（is not in）] を選択して 1 つの条件を作成します。

ステップ 2 テキスト フィールド内の任意の場所または [編集（Edit）] リンクをクリックします。

ステップ 3 [使用可能（Available）] の下にある複数の値を選択します。また、クリックしてドラッグすることで、隣接する複数の値を選択できます。

ステップ 4 右矢印（>）をクリックして、選択した項目を [Selected] に移動します。

ステップ 5 [OK] をクリックします。

相関ルールの管理

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Discovery Admin

マルチドメイン展開では、現在のドメインで作成された相関ルールとグループが表示されます。これらは編集可能です。また、先祖ドメインからの選択した相関ルールとグループも表示されますが、これらは編集できません。下位のドメインで作成された相関ルールとグループを表示および編集するには、そのドメインに切り替えます。

（注） 設定に無関係なドメイン（名前、管理対象デバイスなど）に関する情報が公開されている場合、システムは先祖ドメインからの設定を表示しません。

アクティブな相関ポリシーのルールへの変更は、即座に反映されます。

始める前に

- ルールを削除する場合は、そのルールをすべての相関ポリシーから削除します。詳細については、相関ポリシーの管理 （2700 ページ）を参照してください。

ステップ 1 **[Policies]** > **[Correlation]** を選択して、[ルール管理（Rule Management）] タブをクリックします。

ステップ 2 ルールを管理します。

- 作成：[ルールの作成（Create Rule）] をクリックします。相関ルールの設定 （2701 ページ）を参照してください。
- グループの作成：[グループの作成（Create Group）] をクリックし、グループの名前を入力して、[保存（Save）] をクリックします。グループにルールを追加するには、ルールを編集します。
- 編集：編集アイコン（）をクリックします。相関ルールの設定 （2701 ページ）を参照してください。

  代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。
- ルールまたはルール グループの削除：削除アイコン（）をクリックします。ルール グループを削除すると、ルールのグループ化が解除されます。 コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

相関応答グループの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Discovery Admin

アラートおよび修復の相関応答グループを作成し、グループをアクティブにして、アクティブな相関ポリシー内の相関ルールに割り当てることができます。システムは、ネットワーク トラフィックが相関ルールに一致すると、すべてグループ化された応答を開始します。

アクティブなグループまたはいずれかのグループ化された応答に対する変更は、アクティブな相関ポリシーで行う場合、ただちに有効になります。

ステップ 1 **[Policies]** > **[Correlation]** を選択し、[グループ（Group）] をクリックします。

ステップ 2 [グループの作成（Create Group）] をクリックします。

ステップ 3 名前を入力します。

ステップ 4 作成時にグループをアクティブにする場合は、[アクティブ（Active）]チェックボックスをオンにします。

非アクティブ化されたグループは応答を開始しません。

ステップ 5 グループに[使用可能な応答（Available Responses）]を選択し、右矢印（>）をクリックして、それらを[グループ内の応答（Responses in Group）] に移動します。応答を他の方法で移動するには、左矢印（<）を使用します。

ステップ 6 [保存（Save）] をクリックします。

次のタスク

- 作成時にグループをアクティブにしなかった場合、アクティブにするには、スライダをクリックします。

関連トピック

Firepower Management Center アラート応答 （2807 ページ）
修復の概要 （2755 ページ）

相関応答グループの管理

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Discovery Admin

応答グループは、相関ポリシーで使用されていない場合は削除できます。応答グループを削除することで、その応答のグループ化を解除します。また、応答グループを削除せずに、一時的に非アクティブにすることもできます。これにより、グループはシステムに残りますが、ポリシーに違反するときにはグループが開始されなくなります。

マルチドメイン展開では、現在のドメインで作成されたグループが表示されます。これは編集できます。先祖ドメインで作成されたグループも表示されますが、これは編集できません。下位のドメインで作成されたグループを表示および編集するには、そのドメインに切り替えます。

アクティブな使用中の応答グループへの変更は、即座に反映されます。

ステップ 1 **[Policies]** > **[Correlation]** を選択して、[グループ（Group）] をクリックします。

ステップ 2 応答グループを管理します。

- アクティブ化または非アクティブ化：スライダをクリックします。 コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。
- 作成：[グループの作成（Create Group）] をクリックします。相関応答グループの設定 （2739 ページ）を参照してください。
- 編集：編集アイコン（  ）をクリックします。相関応答グループの設定 （2739 ページ）を参照してください。 代わりに表示アイコン（  ）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。
- 削除：削除アイコン（  ）をクリックします。 コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

第 110 章

トラフィック プロファイル

ここでは、トラフィック プロファイルの設定方法について説明します。

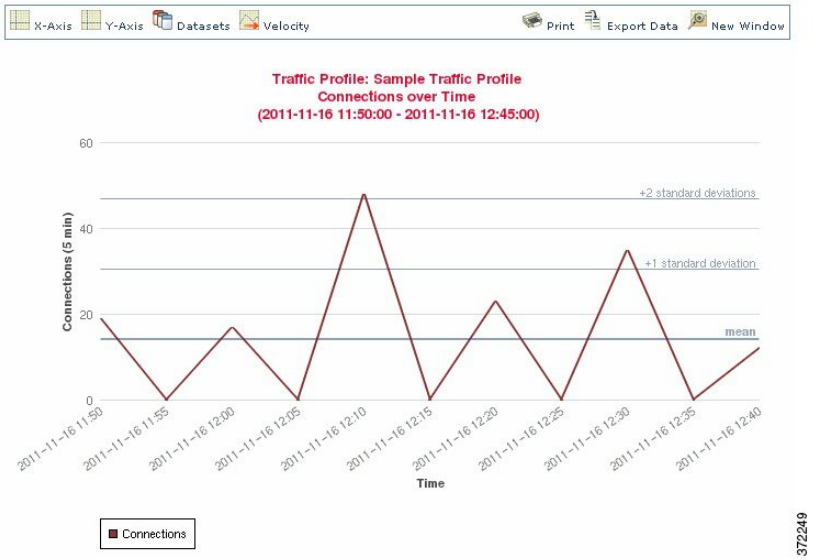
トラフィック プロファイルの概要

トラフィック プロファイルはプロファイル生成時間枠（PTW）内に収集した接続データを基に、ネットワーク トラフィックをグラフで表したものです。この測定結果が正常なネットワーク トラフィックを表しているものと推定します。学習期間が経過すると、新たなトラフィックをプロファイルに照らして評価することで異常なネットワーク トラフィックを検出します。

デフォルト PTW は 1 週間ですが、最短で 1 時間、最長で数週間に変更できます。デフォルトで、トラフィック プロファイルは 5 分間隔でシステム生成の接続イベントに関する統計情報を生成します。ただし、このサンプリング レートは最大 1 時間間隔まで拡大することができます。

ヒント シスコは少なくとも 100 のデータ ポイントを含む PTW の設定を推奨します。統計的に意味のある十分なデータがトラフィック プロファイルに含まれるように、PTW とサンプリング レートを設定する必要があります。

次の図は、PTW を 1 日、サンプリング レートを 5 分としたトラフィック プロファイルを示しています。



また、トラフィック プロファイルの非アクティブ期間を設定することもできます。トラフィック プロファイルは非アクティブ期間もデータ収集を行いますが、収集したデータをプロファイル統計の計算に使用しません。トラフィック プロファイルの時系列グラフでは、非アクティブ期間が網掛け領域として示されます。

たとえば、すべてのワークステーションが毎日深夜 0:00 にバックアップされるネットワーク インフラストラクチャがあるとします。バックアップには約30分かかり、その間はネットワーク トラフィックが急増します。予定されたバックアップ時間に合わせてトラフィック プロファイルの非アクティブ期間を繰り返すよう設定します。

（注） システムは接続の終了データを使って接続グラフとトラフィック プロファイルを作成します。トラフィック プロファイルを使用するには、必ずFirepower Management Centerデータベースに接続の終了イベントをロギングしてください。

トラフィック プロファイルの実装

トラフィック プロファイルを有効にすると、システムは設定した学習期間（PTW）の間接続データを収集し、評価します。システムは学習期間が経過すると、トラフィック プロファイルを対象にした相関ルールを評価します。

たとえば、ネットワークを通過するデータ量（パケット数、KB数、または接続数で測定）が、平均トラフィック量に比べて標準偏差の3倍も急激に上昇した場合、攻撃または他のセキュリティ ポリシー違反を示す可能性があると判断してトリガーするルールを作成できます。その後、このルールを相関ポリシーに組み込んで、トラフィックの急増に関するアラートを出したり、応答として修復を実行したりできます。

トラフィック プロファイルの対象設定

トラフィック プロファイルは、プロファイル条件とホスト プロファイル限定による制約を受けます。

プロファイル条件を使って、すべてのネットワーク トラフィックをプロファイリングすることもできます。また、トラフィック プロファイルの対象を絞って、特定のドメイン、特定のドメイン内や複数のドメイン内のサブネット、または個別のホストをモニタすることもできます。マルチドメイン展開では次のプロファイリングが可能です。

- リーフ ドメイン管理者は、リーフ ドメイン内のネットワーク トラフィックをプロファイリングできます。
- 高位レベル ドメインの管理者は、ドメイン内または複数ドメインでトラフィックのプロファイリングができます。

また、プロファイル条件では接続データに基づく基準を設けてトラフィック プロファイルを制約することもできます。たとえば、特定のポート、プロトコル、アプリケーションが使われているセッションのみトラフィック プロファイルでプロファイリングを行うようにプロファイル条件を設定できます。

また、トラッキング対象のホストに関する情報を使用してトラフィック プロファイルを制約することもできます。この制約は、ホストプロファイル限定と呼ばれます。たとえば、重要度の高いホストに限定して接続データを収集できます。

（注） トラフィック プロファイルを高レベルのドメインに制約すると、各子孫リーフ ドメインの同じタイプのトラフィックが集約およびプロファイルされます。システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、ドメイン間のトラフィックをプロファイルすると、予期しない結果になる可能性があります。

関連トピック

相関ポリシーとルールの概要 （2697 ページ）

トラフィック プロファイル条件

単純なトラフィック プロファイル条件とホスト プロファイル限定を作成できます。また、複数の条件の組み合わせとネストによってより複雑な構造を作成することもできます。

条件には、カテゴリ、演算子、および値という 3 つの部分があります。

- 使用できるカテゴリは、トラフィック プロファイル条件を作成しているか、それともホスト プロファイル限定を作成しているかに応じて異なります。
- 使用できる演算子は、選択したカテゴリによって異なります。
- 条件の値を指定するために使用できる構文は、カテゴリと演算子に応じて異なります。場合によっては、テキスト フィールドに値を入力する必要があります。それ以外の場合、ドロップダウン リストから 1 つ以上の値を選択できます。

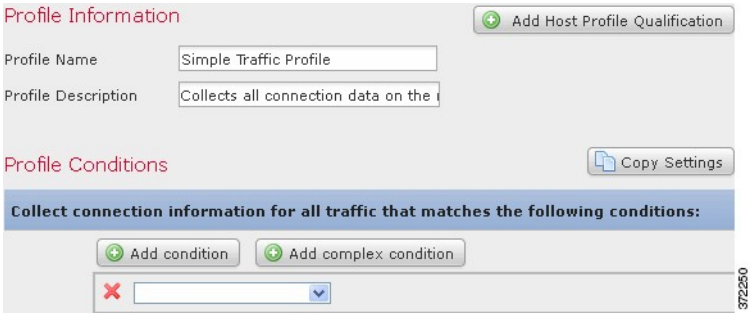
ホストプロファイル限定の場合、開始側または応答側のホストに関する情報のデータを使用して、トラフィック プロファイルに制約を適用するかどうかを指定する必要もあります。

構造に複数の条件を含める場合は、それらの条件を [および（AND）] 演算子または [または（OR）] 演算子で結合する必要があります。同じレベルにある複数の条件は、一緒に評価されます。

- **AND** 演算子は、制御対象のレベルにあるすべての条件が満たされなければならないことを示します。
- [または（OR）] 演算子は、制御対象のレベルにある複数の条件の少なくとも 1 つが満たされている必要があることを示します。

制約が適用されていないトラフィック プロファイル

モニタ対象ネットワーク セグメント全体のデータを収集するトラフィック プロファイルを作成する場合、次の図に示すように、条件を含まない非常に単純なプロファイルを作成できます。



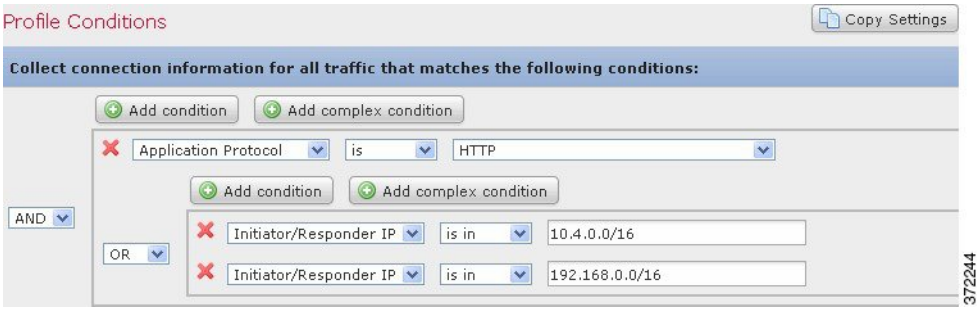
単純なトラフィック プロファイル

プロファイルに制約を適用して、1 つのサブネットのデータのみを収集するには、次の図に示すように 1 つの条件を追加できます。

複雑なトラフィック プロファイル

次のトラフィック プロファイルには、[および（AND）] で結合された 2 つの条件が含まれています。つまり、両方の条件とも満たされる場合に限り、このトラフィック プロファイルは接続データを収集します。この例では、特定のサブネット内の IP アドレスを持つすべてのホストに関する HTTP 接続を収集します。

一方、次のトラフィック プロファイルでは、2 つのサブネットのいずれかの HTTP アクティビティに関する接続データを収集しますが、最後は複合条件を構成しています。



論理的には、上記のトラフィック プロファイルは次のように評価されます。

```
(A and (B or C))
```

条件	条件で指定する内容
A	アプリケーション プロトコル名が HTTP である
B	IP アドレスが 10.4.0.0/16 内にある
C	IP アドレスが 192.168.0.0/16 内にある

トラフィック プロファイルの管理

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Discovery Admin

アクティブで完全なトラフィック プロファイルに対して記述されたルールのみが、相関ポリシー違反をトリガーできます。各トラフィック プロファイルの横にあるスライダ アイコンは、プロファイルがアクティブでありデータを収集しているかどうかを示します。経過表示バーは、トラフィック プロファイルの学習期間のステータスを示します。

マルチドメイン展開では、現在のドメインで作成されたトラフィック プロファイルが表示されます。これは、編集が可能なプロファイルです。また、先祖ドメインからの選択したトラフィック プロファイルも表示されますが、これは編集できません。下位のドメインで作成されたトラフィック プロファイルを表示および編集するには、そのドメインに切り替えます。

（注） プロファイルの条件が無関係なドメインに関する情報（名前や管理対象デバイスなど）を公開する場合、システムは先祖ドメインからのトラフィック プロファイルを表示しません。

ステップ 1 **[Policies]** > **[Correlation]** を選択して、[トラフィック プロファイル（Traffic Profiles）] タブをクリックします。

ステップ 2 トラフィック プロファイルを管理します。

- アクティブ化/非アクティブ化：トラフィック プロファイルをアクティブ化または非アクティブ化するには、スライダをクリックします。トラフィック プロファイルを非アクティブ化すると、そのプロファイルに関連するデータが削除されます。プロファイルを再度アクティブ化する場合は、そのプロファイルに関して作成されたルールがトリガーするようになるまで、PTW の長さだけ待つ必要があります。
- 作成：新しいトラフィック プロファイルを作成するには、[新規プロファイル（New Profile）] をクリックして、トラフィック プロファイルの設定 （2746 ページ） で説明する手順を実行します。また、コピー アイコン（）をクリックして、既存のトラフィック プロファイルのコピーを編集することもできます。
- 削除：トラフィック プロファイルを削除するには、削除アイコン（）をクリックして、選択内容を確認します。
- 編集：既存のトラフィック プロファイルを変更するには、編集アイコン（）をクリックして、トラフィック プロファイルの設定 （2746 ページ） で説明する手順を実行します。トラフィック プロファイルがアクティブな場合は、そのプロファイルの名前と説明のみを変更できます。
- グラフ：グラフとしてトラフィック プロファイルを表示するには、グラフ アイコン（）をクリックします。マルチドメイン展開では、グラフが無関係なドメインに関する情報を公開する場合、先祖ドメインに属しているトラフィック プロファイルのグラフを表示できません。

トラフィック プロファイルの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Discovery Admin

トラフィック プロファイルを高レベルのドメインに制約すると、各子孫リーフ ドメインの同じタイプのトラフィックが集約およびプロファイルされます。システムは、各リーフ ドメインに個別のネットワークマップを作成します。マルチドメイン展開では、ドメイン間のトラフィックをプロファイルすると、予期しない結果になる可能性があります。

ステップ 1 **[Policies]** > **[Correlation]** を選択し、[トラフィック プロファイル（Traffic Profiles）] タブをクリックします。

ステップ 2 [新規プロファイル（New Profile）] をクリックします。

ステップ 3 プロファイル名を入力し、オプションでプロファイルの説明を入力します。

ステップ 4 オプションで、トラフィック プロファイルを制約します。

- 設定のコピー：既存のトラフィック プロファイルから設定をコピーするには、[設定のコピー（Copy Settings）] をクリックし、使用するトラフィック プロファイルを選択して [ロード（Load）] をクリックします。
- プロファイル条件：トラッキング対象の接続の情報を使用してトラフィック プロファイルを制約するには、トラフィック プロファイル条件の追加 （2747 ページ）の説明に従って続行します。
- ホストプロファイル認定：トラッキング対象のホストの情報を使用してトラフィック プロファイルを制約するには、トラフィック プロファイルへのホストプロファイル認定の追加 （2748 ページ）の説明に従って続行します。
- プロファイルの時間帯（PTW）：プロファイルの時間帯を変更するには、時間の単位を入力し、[時間（hour(s)）]、[日（day(s)）]、または [週（week(s)）] を選択します。
- サンプリング レート：サンプリング レートを分単位で選択します。
- 非アクティブ期間：[非アクティブ期間の追加（Add Inactive Period）] をクリックし、ドロップダウンリストを使用して、トラフィック プロファイルを非アクティブなままにする日時と頻度を指定します。非アクティブなトラフィック プロファイルは、相関ルールをトリガーしません。トラフィック プロファイルでは、プロファイルの統計情報に非アクティブな期間のデータを含めません。

ステップ 5 トラフィック プロファイルを保存します。

- プロファイルを保存し、ただちにデータを収集し始めるには、[保存してアクティブにする（Save & Activate）] をクリックします。
- アクティブ化せずにプロファイルを保存するには、[保存（Save）] をクリックします。

トラフィック プロファイル条件の追加

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Discovery Admin

ステップ 1 トラフィック プロファイル エディタの [プロファイル条件（Profile Conditions）] で、追加する各条件について [条件の追加（Add condition）] または [複合条件の追加（Add complex condition）] をクリックします。同レベルの条件は一緒に評価されます。

- 演算子で結ばれた同一のレベルのすべての条件が満たされるべきことを指定するには、[AND] を選択します。
- 演算子で結ばれた同一のレベルの 1 つの条件だけが満たされるべきことを指定するには、[OR] を選択します。

ステップ 2 トラフィック プロファイル条件の構文（2749 ページ）とトラフィック プロファイル条件（2743 ページ）の説明に従い、各条件のカテゴリ、演算子、値を指定します。

演算子として [含まれる（is in）] または [含まれない（is not in）] を選択した場合は、トラフィック プロファイル条件での複数の値の使用（2754 ページ）に説明してあるように単一の条件で複数の値を選択できます。

カテゴリが IP アドレスを表している場合、演算子として [含まれる（is in）] または [含まれない（is not in）] を選択すると、IP アドレス範囲内にその IP アドレスが含まれるのか、含まれないのかを指定できます。

例

次のトラフィック プロファイルは、特定のサブネットの情報を集めます。条件のカテゴリは [イニシエータ/レスポンダ IP（Initiator/Responder IP）]、演算子は [含まれる（is in）]、値は `10.4.0.0/16` です。

関連トピック

Firepower システムの IP アドレス表記法 （20 ページ）

トラフィック プロファイルへのホスト プロファイル認定の追加

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Discovery Admin

ステップ 1 トラフィック プロファイル エディタで、[ホスト プロファイル認定の追加（Add Host Profile Qualification）] をクリックします。

ステップ 2 [ホスト プロファイル認定（Host Profile Qualification）] で、追加する各条件について [条件の追加（Add condition）] または [複合条件の追加（Add complex condition）] をクリックします。同レベルの条件は一緒に評価されます。

- 演算子で結ばれた同一のレベルのすべての条件が満たされるべきことを指定するには、[AND] を選択します。
- 演算子で結ばれた同一のレベルの 1 つの条件だけが満たされるべきことを指定するには、[OR] を選択します。

ステップ 3 トラフィック プロファイルのホスト プロファイル限定の構文（2751 ページ）とトラフィック プロファイル条件（2743 ページ）の説明に従い、各条件のホストタイプ、カテゴリ、演算子、値を指定します。

演算子として [含まれる（is in）] または [含まれない（is not in）] を選択した場合は、トラフィック プロファイル条件での複数の値の使用（2754 ページ）に説明してあるように単一の条件で複数の値を選択できます。

例

次のホスト プロファイル認定によりトラフィック プロファイルが制約され、検出された接続内の応答側ホストで任意のバージョンの Microsoft Windows が実行されている場合にのみ、接続データが収集されます。

トラフィック プロファイル条件の構文

次の表で、トラフィック プロファイル条件を作成する方法について説明します。トラフィック プロファイルの作成に使用可能な接続データは、トラフィックの特性と検出方法を含む複数の要因によって変わることに留意してください。

表 *279*: トラフィック プロファイル条件の構文

次を選択できます。	選択する演算子と内容
アプリケーション プロトコル	アプリケーション プロトコルを 1 つ以上選択します。

次を選択できます。	選択する演算子と内容
[アプリケーション プロトコル カテゴリ（Application Protocol Category）]	アプリケーション プロトコル カテゴリを 1 つ以上選択します。
クライアント	クライアントを 1 つ以上選択します。
[クライアント カテゴリ（Client Category）]	クライアント カテゴリを 1 つ以上選択します。
接続タイプ	プロファイルが Firepower システムの管理対象デバイスによってモニタされるトラフィックからの接続データ、またはエクスポートされた NetFlow レコードからの接続データを使用するかどうかを選択します。 接続タイプを指定しない場合、トラフィック プロファイルには両方が含まれます。
接続先（国）または送信元（国）	国を 1 つ以上選択します。
ドメイン	1 つ以上のドメインを選択してください。マルチドメイン展開環境では、先祖ドメインによる制約条件がそのドメインの子孫によって報告されるデータにも適用されます。
イニシエータ IP、レスポンダ IP、またはイニシエータ/レスポンダ IP	IP アドレス、または IP アドレスの範囲を入力します。 システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。
NetFlow デバイス	トラフィック プロファイルの作成に使用するデータの NetFlow エクスポータを選択します。
レスポンダ ポート/ICMP コード	ポート番号または ICMP コードを入力します。
セキュリティ インテリジェンス カテゴリ	セキュリティ インテリジェンスのカテゴリを 1 つ以上選択します。 トラフィック プロファイル条件にセキュリティ インテリジェンスのカテゴリを使用するには、アクセス コントロール ポリシーでそのカテゴリを [ブロック（Block）] ではなく [モニタ（Monitor）] に設定する必要があります。
SSL 暗号化セッション	[正常に復号（Successfully Decrypted）] を選択します。
トランスポート プロトコル	トランスポート プロトコルとして **TCP** または **UDP** と入力します。
[Web アプリケーション（Web Application）]	Web アプリケーションを 1 つ以上選択します。
Web アプリケーションのカテゴリ	Web アプリケーションのカテゴリを 1 つ以上選択します。

関連トピック

接続イベント フィールドの入力の要件 （3042 ページ）
Firepower システムの IP アドレス表記法 （20 ページ）

トラフィック プロファイルのホスト プロファイル限定の構文

ホスト プロファイル限定の条件を作成するときには、まず、トラフィック プロファイルを制約するために使用するホストを選択する必要があります。[レスポンダ ホスト（Responder Host）] または [イニシエータ ホスト（Initiator Host）] のいずれかを選択できます。ホスト ロールを選択したら、ホスト プロファイル限定の条件の作成を続行します。

NetFlow レコードを使用してネットワーク マップにホストを追加できますが、これらのホストに関する利用可能な情報は限定されています。たとえば、これらのホストに利用可能なオペレーティング システム データは得られません（ただしホスト入力機能を使って指定する場合を除く）。さらに、エクスポートされた NetFlow レコードからの接続データをトラフィック プロファイルで使用する場合、NetFlow レコードには、どのホストが接続のイニシエータで、どのホストがレスポンダであるかを示す情報が含まれないことに注意してください。システムは、NetFlow レコードを処理するときに、それぞれのホストが使用しているポートとそれらのポートが既知かどうかに基づいて、この情報を判断するアルゴリズムを使用します。

暗黙的（または汎用の）クライアントを照合するには、クライアントに応答するサーバで使われるアプリケーション プロトコルに基づいてホスト プロファイル限定を作成します。接続のイニシエータ（または送信元）として機能するホスト上のクライアント リストに含まれるアプリケーション プロトコル名の後に**クライアント**が続いている場合、そのクライアントは実際には暗黙的クライアントである可能性があります。つまり、検出されたクライアント トラフィックに基づいてではなく、そのクライアントのアプリケーション プロトコルを使用するサーバ応答トラフィックに基づいて、システムがそのクライアントを報告します。

たとえば、ホスト上のクライアントとして **HTTPS クライアント**がシステムにより報告される場合、[アプリケーション プロトコル（Application Protocol）] を [HTTPS] に設定した [レスポンダ ホスト（Responder Host）] のホスト プロファイル限定を作成します。これは、レスポンダまたは宛先ホストから送られる HTTPS サーバ応答トラフィックに基づいて HTTPS クライアントが汎用クライアントとして報告されるためです。

表 *280* : ホスト プロファイル限定の構文

次を選択できます。	選択する演算子と内容
[アプリケーション プロトコル（Application Protocol）] > [アプリケーション プロトコル（Application Protocol）]	アプリケーション プロトコルを 1 つ以上選択します。
[アプリケーション プロトコル（Application Protocol）] > [アプリケーション ポート（Application Port）]	アプリケーション プロトコルのポート番号を入力します。
[アプリケーション プロトコル（Application Protocol）] > [プロトコル（Protocol）]	プロトコルを選択します。

次を選択できます。	選択する演算子と内容
[アプリケーション プロトコル カテゴリ（Application Protocol Category）]	アプリケーション プロトコル カテゴリを 1 つ以上選択します。
[クライアント（Client）] > [クライアント（Client）]	クライアントを 1 つ以上選択します。
[クライアント（Client）] > [クライアント バージョン（Client Version）]	クライアント バージョンを入力します。
[クライアント カテゴリ（Client Category）]	クライアント カテゴリを 1 つ以上選択します。
ドメイン	1 つ以上のドメインを選択してください。マルチドメイン展開環境では、先祖ドメインによる制約条件がそのドメインの子孫によって報告されるデータにも適用されます。
[ハードウェア（Hardware）]	モバイル デバイスのハードウェア モデルを入力します。たとえば、すべての Apple iPhone に一致させるには `iPhone` と入力します。
[ホストの重要度（Host Criticality）]	ホストの重要度を選択します。
[ホスト タイプ（Host Type）]	ホスト タイプを 1 つ以上選択します。通常のホスト、またはいずれかのタイプのネットワーク デバイスを選択できます。
[IOC タグ（IOC Tag）]	IOC タグを 1 つ以上選択します。
[ジェイルブロークン（Jailbroken）]	イベントのホストがジェイルブレイクされたモバイル デバイスであることを示すには [はい（Yes）] を、そうでない場合は [いいえ（No）] を選択します。
[MAC アドレス（MAC Address）] > [MAC アドレス（MAC Address）]	ホストの MAC アドレス全体またはその一部を入力します。
[MAC アドレス（MAC Address）] > [MAC タイプ（MAC Type）]	MAC タイプが [ARP/DHCP で検出（ARP/DHCP Detected）] されるかどうかを選択します。つまり、次のいずれかです。 • システムは MAC アドレスがホストに属していることをポジティブに識別した（[ARP/DHCP で検出（is ARP/DHCP Detected）]） • たとえば、デバイスとホスト間にはルータがあるため、システムはその MAC アドレスを持つ多くのホストを認識している（[ARP/DHCP で検出されない（is not ARP/DHCP Detected）]） • MAC タイプが無関係（[どれでもない（is any）]）

次を選択できます。	選択する演算子と内容
[MAC ベンダー（MAC Vendor）]	ホストが使用するハードウェアの MAC ベンダー全体またはその一部を入力します。
Mobile	イベントのホストがモバイル デバイスであることを示すには [はい（Yes）] を、そうでない場合は [いいえ（No）] を選択します。
NETBIOS 名	ホストの NetBIOS 名を入力します。
ネットワーク プロトコル	http://www.iana.org/assignments/ethernet-numbers にリストされているネットワーク プロトコル番号を入力します。
[オペレーティング システム（Operating System）] > [OS ベンダー（OS Vendor）]	オペレーティング システムのベンダー名を 1 つ以上選択します。
[オペレーティング システム（Operating System）] > [OS 名（OS Name）]	オペレーティング システムの名前を 1 つ以上選択します。
[オペレーティング システム（Operating System）] > [OS バージョン（OS Version）]	オペレーティング システムのバージョンを 1 つ以上選択します。
[トランスポート プロトコル（Transport Protocol）]	http://www.iana.org/assignments/protocol-numbers にリストされているトランスポート プロトコルの名前または番号を入力します。
VLAN ID（Admin. VLAN ID）	ホストの VLAN ID 番号を入力します。 システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、実際の VLAN タグを使用してこの設定を抑制すると、予期しない結果になる可能性があります。
[Web アプリケーション（Web Application）]	Web アプリケーションを 1 つ以上選択します。
Web アプリケーションのカテゴリ	Web アプリケーションのカテゴリを 1 つ以上選択します。

次を選択できます。	選択する演算子と内容
使用可能な任意のホスト属性（デフォルト コンプライアンス ホワイトリスト ホスト属性を含む）	選択するホスト属性のタイプに応じて、適切な値を次のように指定します。 • ホスト属性タイプが Integer の場合、その属性で定義されている範囲内の整数値を入力します。 • ホスト属性タイプが Text の場合、テキスト値を入力します。 • ホスト属性タイプが List の場合、有効なリスト文字列を選択します。 • ホスト属性タイプが URL の場合、URL 値を入力します。

トラフィック プロファイル条件での複数の値の使用

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Discovery Admin

条件を作成するときに、条件の構文でドロップダウン リストから値を選択できる場合、通常はリストから複数の値を選択できます。

たとえば、ホストで何らかの UNIX フレーバを実行している必要があることを示すホスト プロファイル限定をトラフィック プロファイルに追加するには、多数の条件を OR 演算子で結合する代わりに、以下の手順を使用できます。

ステップ 1 トラフィック プロファイルまたはホスト プロファイルの資格条件を作成するときに、演算子として [存在する（is in）] または [存在しない（is not in）] を選択します。
ドロップダウン リストがテキスト フィールドに変わります。

ステップ 2 テキスト フィールド内の任意の場所または [編集（Edit）] リンクをクリックします。

ステップ 3 [使用可能（Available）] の下にある複数の値を選択します。

ステップ 4 右矢印をクリックして、選択した項目を [選択済み（Selected）] に移動します。

ステップ 5 [OK] をクリックします。

第 111 章

修復

以下のトピックでは、修復の設定について説明します。

修復の概要

修復は Firepower システムが相関ポリシー違反に応じて起動するプログラムです。

修復を実行すると、システムは修復ステータス イベントを生成します。修復ステータス イベントには、修復の名前、相関ポリシー、修復をトリガーしたルール、終了ステータス メッセージなどの詳細が含まれています。

システムは以下に挙げる複数の修復モジュールをサポートしています。

- Cisco ISE のエンドポイント保護サービス（EPS）：相関ポリシー違反に関連するホストやネットワークへ送信されるトラフィックを検疫、隔離解除、またはシャットダウンします。
- Cisco IOS Null ルート：相関ポリシー違反に関連するホストやネットワークへ送信されるトラフィックをブロックします（Cisco IOS バージョン 12.0 以降が必要）。
- Nmap スキャン：ホストをスキャンして、実行中のオペレーティング システムおよびサーバを決定します。
- 属性値の設定：相関ポリシー違反に関連するホストのホスト属性を設定します。

ヒント 他のタスクを実行するカスタム モジュールをインストールすることもできます。*Firepower* システム修復 *API* ガイドを参照してください。

修復の実装

修復を実装するには、まず選択したモジュールに対して少なくとも1つのインスタンスを作成します。モジュールごとに複数のインスタンスを作成することができ、各インスタンスは別々に設定できます。たとえば、Cisco IOS Null ルート修復モジュールを使用して複数のルータと通信するには、そのモジュールのインスタンスを複数設定します。

次に、ポリシー違反の際に実行するアクションを説明する複数の修復を各インスタンスに追加します。

最後に、相関ポリシーに応じてシステムが修復を開始するように相関ポリシーで修復とルールを関連付けます。

修復およびマルチテナンシー

マルチドメイン展開では、どのドメインのレベルでもカスタムの修復モジュールをインストールできます。システム提供のモジュールはグローバル ドメインに属します。

先祖ドメインで作成したインスタンスに修復を追加することはできませんが、同様の設定済みインスタンスを現在のドメインに作成して、そのインスタンスに修復を追加することはできます。また、先祖ドメインで作成した修復は、相関応答として使用することもできます。

関連トピック

Firepower Management Center アラート応答 （2807 ページ）
Nmap スキャン （2517 ページ）
ルールとホワイトリストに応答を追加する （2700 ページ）

Cisco ISE EPS 修復

ISE 導入環境で、エンドポイント保護サービス（EPS）が設定され、有効になっている場合、Firepower Management Center を設定することで、ISE を使った修復を起動させることが可能です。ISE EPS 修復は、完全に設定された状態では、相関ポリシー違反を起こした送信元または宛先ホストに対し、次の**緩和アクション（Mitigation Actions）**を実行します。

- **検疫（quarantine）**：エンドポイントのネットワークへのアクセスを制限または拒否します。
- **隔離解除（unquarantine）**：エンドポイントの検疫ステータスを解除し、ネットワークへのフル アクセスを許可します。
- **シャットダウン（shotdown）**：エンドポイントのNASポートを非アクティブ化し、ネットワークから切断します。

また、ネットワークを**ホワイトリストに登録（Whitelist）**して、システムが当該アドレスに対して ISE EPS 修復を行わないようにすることも可能です。

（注） 使用するISEバージョンと構成は、Firepowerシステムでの ISE の使用方法に影響を与えます。たとえば、ISE-PIC では、ISE EPS 修復を実行できません。詳細については、ISE/ISE-PIC アイデンティティ ソース （2593 ページ）を参照してください。

ISE EPS アクションの詳細については、『*Cisco Identity Services Engine User Guide*』を参照してください。

ISE EPS 修復の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin Discovery Admin

送信元または宛先ホストで ISE EPS 修復を実行することによって、相関ポリシー違反に応答できます。

（注） ISE-PIC は ISE EPS 修復を実行できません。

始める前に

- ISE サーバ上で EPS 操作を設定します。
- ユーザ制御用 ISE/ISE-PIC の設定 （2601 ページ）の説明に従って ISE への接続を設定します。

ステップ 1 **[Policies]** > **[Actions]** > **[Instances]**を選択します。

ステップ 2 ISE EPS インスタンスの追加 （2758 ページ）の説明に従って pxGrid 緩和インスタンスを追加します。

ステップ 3 ISE EPS 修復の追加 （2758 ページ）の説明に従って 1 つ以上の ISE EPS 修復を追加します。

次のタスク

- ルールとホワイトリストに応答を追加する （2700ページ）の説明に従って相関ポリシー違反への応答として修復を割り当てます。

ISE EPS インスタンスの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin Discovery Admin

ISE EPS インスタンスを作成し、ロギング タイプごとに個々の修復をグループ化します。

ステップ 1 **[Policies]** > **[Actions]** > **[Instances]**を選択します。

ステップ 2 [新規インスタンスの追加（Add a New Instance）] リストから、モジュール タイプとして [pxGrid Mitigation(v1.0)] を選択し、[追加（Add）] をクリックします。

ステップ 3 [インスタンス名（Instance Name）] と [説明（Description）] に入力します。

ステップ 4 [ロギングの有効化（Enable Logging）] オプションを設定し、システム ロギングを有効または無効にします。

ステップ 5 [作成（Create）] をクリックします。

次のタスク

- セット属性値修復の追加 （2767 ページ）の説明に従って ISE EPS 修復を作成します。

関連トピック

Firepower システムの IP アドレス表記法 （20 ページ）

ISE EPS 修復の追加

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin Discovery Admin

相関ポリシー違反に含まれる送信元または宛先ホストで[緩和アクション（Mitigation Actions）] を実行するため、インスタンス内に 1 つ以上の ISE EPS 修復を作成します。

マルチドメイン展開では、先祖ドメインで作成されたインスタンスに修復を追加することはできません。

始める前に

- ISE EPS インスタンスの追加 （2758 ページ）の説明に従って ISE EPS インスタンスを作成します。

ステップ 1 **[Policies]** > **[Actions]** > **[Instances]**を選択します。

ステップ 2 修復を追加するインスタンスの横にある表示アイコン（）をクリックします。

ステップ 3 [設定済み修復（Configured Remediations）] セクションで、[宛先の緩和（Mitigate Destination）] または [送信元の緩和（Mitigate Source）] を選択し、[追加（Add）] をクリックします。

コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 4 [修復名（Remediation Name）] と [説明（Description）] に入力します。

ステップ 5 次のいずれかの緩和アクションを選択します。[検疫（quarantine）]、[隔離解除（unquarantine）]、[シャットダウン（shutdown）] 。

ステップ 6 （オプション）ホワイトリストに目的の IP アドレスまたは範囲を入力し、修復から除外します。

ステップ 7 [作成（Create）] をクリックし、次に [完了（Done）] をクリックします。

次のタスク

- 相関ポリシー違反への応答として修復を割り当てます（ルールとホワイトリストに応答を追加する （2700 ページ） を参照）。

Cisco IOS Null ルート修復

Cisco IOS Null ルート修復モジュールでは、シスコ「null route」コマンドを使って、個別の IP アドレスまたは IP アドレスの範囲をブロックすることができます。これにより、ホストまたはネットワークに送信されるすべてのトラフィックがルータの NULL インターフェイスにルーティングされ、ドロップされます。違反ホストまたはネットワークから送信されるトラフィックはブロックされません。

（注） 検出またはホスト入力イベントに基づく相関ルールへの応答として、宛先ベースの修復を使用しないでください。これらのイベントは、送信元ホストに関連付けられています。

注意 Cisco IOS 修復がされている間は、タイムアウト期間はありません。IP アドレスまたはネットワークのブロックを解除するには、ルータから手動でルーティング変更をクリアする必要があります。

Cisco IOS ルータ用修復の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin Discovery Admin

（注） 検出またはホスト入力イベントに基づく相関ルールへの応答として、宛先ベースの修復を使用しないでください。これらのイベントは、送信元ホストに関連付けられています。

注意 Cisco IOS 修復がされている間は、タイムアウト期間はありません。IP アドレスまたはネットワークのブロックを解除するには、ルータから手動でルーティング変更をクリアする必要があります。

始める前に

- Cisco ルータが Cisco IOS 12.0 以降を実行していることを確認します。
- ルータへのレベル 15 の管理アクセス権を持っていることを確認します。

ステップ 1 Cisco ルータまたは IOS ソフトウェアに付属のドキュメントの説明に従って、Cisco ルータで Telnet を有効にします。

ステップ 2 Firepower Management Center で、使用する予定の各 Cisco IOS ルータに対する Cisco IOS ヌル ルート インスタンスを追加します。Cisco IOS インスタンスの追加 （2760 ページ）を参照してください。

ステップ 3 相関ポリシーに違反した場合にルータで実現する応答のタイプに基づき、インスタンスごとに修復を作成します。

- Cisco IOS ブロック宛先の修復の追加 （2762 ページ）
- Cisco IOS ブロック宛先ネットワークの修復の追加 （2762 ページ）
- Cisco IOS ブロック送信元の修復の追加 （2764 ページ）
- Cisco IOS ブロック送信元ネットワークの修復の追加 （2764 ページ）

次のタスク

- 相関ポリシー違反への応答として修復を割り当てます（ルールとホワイトリストに応答を追加する （2700 ページ） を参照）。

Cisco IOS インスタンスの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin Discovery Admin

修復を送信するルータが複数ある場合は、各ルータに対して別々のインスタンスを作成します。

始める前に

- ルータまたはIOSソフトウェアのドキュメントの説明に従って、Cisco IOSルータのTelnetアクセスを設定します。

ステップ1 **[Policies]** > **[Actions]** > **[Instances]**を選択します。

ステップ2 [新しいインスタンスの追加（Add a New Instance）] リストから [Cisco IOS Null ルート（Cisco IOS Null Route）] を選択し、[追加（Add）] をクリックします。

ステップ3 [インスタンス名（Instance Name）] と [説明（Description）] を入力します。

ステップ4 [ルータ IP（Router IP）] フィールドに、修復のために使用する Cisco IOS ルータの IP アドレスを入力します。

ステップ5 [Username] フィールドに、ルータの Telnet ユーザ名を入力します。このユーザは、ルータでレベル 15 管理アクセスを持っている必要があります。

ステップ6 [接続パスワード（Connection Password）] フィールドに、Telnet ユーザのパスワードを入力します。

ステップ7 [イネーブル パスワード（Enable Password）] フィールドに、Telnet ユーザのイネーブル パスワードを入力します。これは、ルータの特権モードに入るために使用するパスワードです。

ステップ8 [ホワイトリスト（White List）] フィールドに、修復から除外する IP アドレスまたは範囲を 1 行につき 1 つ入力します。

（注） システムは、各リーフドメインに個別のネットワークマップを作成します。マルチドメイン展開では、実際のIPアドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。

ステップ9 [作成（Create）] をクリックします。

次のタスク

- Cisco IOSブロック宛先の修復の追加 （2762ページ）、Cisco IOSブロック宛先ネットワークの修復の追加 （2762ページ）、Cisco IOSブロック送信元の修復の追加 （2764ページ）、およびCisco IOSブロック送信元ネットワークの修復の追加 （2764ページ）の説明に従い、相関ポリシーで使用する特定の修復を追加します。

関連トピック

Firepower システムの IP アドレス表記法 （20 ページ）

Cisco IOS ブロック宛先の修復の追加

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin Discovery Admin

Cisco IOS ブロック宛先修復は、ルータから、相関ポリシー違反に関与している宛先ホストに送信されるトラフィックをブロックします。この修復を、検出またはホスト入力イベントに基づく相関ルールへの応答として使用しないでください。これらのイベントは、送信元ホストに関連付けられています。

マルチドメイン展開では、先祖ドメインで作成されたインスタンスに修復を追加することはできません。

始める前に

- Cisco IOS インスタンスの追加 （2760 ページ） の説明に従い、Cisco IOS インスタンスを追加します。

ステップ 1 **[Policies]** > **[Actions]** > **[Instances]**を選択します。

ステップ 2 修復を追加するインスタンスの横にある表示アイコン（  ）をクリックします。

ステップ 3 [設定されている修復（Configured Remediations）] セクションで、[宛先のブロック（Block Destination）] を選択し、[追加（Add）] をクリックします。

コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 4 [修復名（Remediation Name）] と [説明（Description）] を入力します。

ステップ 5 [作成（Create）] をクリックし、次に [完了（Done）] をクリックします。

次のタスク

- 相関ポリシー違反への応答として修復を割り当てます（ルールとホワイトリストに応答を追加する （2700 ページ） を参照）。

Cisco IOS ブロック宛先ネットワークの修復の追加

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin Discovery Admin

Cisco IOS ブロック宛先ネットワーク修復は、ルータから、相関ポリシー違反に関与している宛先ホストのネットワークに送信されるトラフィックをブロックします。この修復を、検出またはホスト入力イベントに基づく相関ルールへの応答として使用しないでください。これらのイベントは、送信元ホストに関連付けられています。

マルチドメイン展開では、先祖ドメインで作成されたインスタンスに修復を追加することはできません。

始める前に

- Cisco IOS インスタンスの追加 （2760 ページ） の説明に従い、Cisco IOS インスタンスを追加します。

ステップ 1 **[Policies]** > **[Actions]** > **[Instances]**を選択します。

ステップ 2 修復を追加するインスタンスの横にある表示アイコン（  ）をクリックします。

ステップ 3 [設定されている修復（Configured Remediations）] セクションで、[宛先ネットワークのブロック（Block Destination Network）] を選択し、[追加（Add）] をクリックします。

コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 4 [修復名（Remediation Name）] と [説明（Description）] を入力します。

ステップ 5 [ネットマスク（Netmask）] フィールドに、サブネット マスクを入力するか、または CIDR 表記を使用して、トラフィックをブロックするネットワークを記述します。

たとえば、1 つのホストがルールをトリガーとして使用したときにクラス C ネットワーク全体へのトラフィックをブロックするには、ネットマスクとして `255.255.255.0` または `24` を使用します。

別の例として、トリガーの IP アドレスを含む 30 個のアドレスへのトラフィックをブロックするには、ネットマスクとして `255.255.255.224` または `27` を指定します。この場合、IP アドレス `10.1.1.15` が修復をトリガーとして使用し、`10.1.1.1` と `10.1.1.30` の間のすべての IP アドレスがブロックされます。トリガーの IP アドレスのみをブロックするには、このフィールドは空のままにして、`32` を入力するか、または `255.255.255.255` を入力します。

ステップ 6 [作成（Create）] をクリックし、次に [完了（Done）] をクリックします。

次のタスク

- 相関ポリシー違反への応答として修復を割り当てます（ルールとホワイトリストに応答を追加する （2700 ページ） を参照）。

関連トピック

Firepower システムの IP アドレス表記法 （20 ページ）

Cisco IOS ブロック送信元の修復の追加

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin Discovery Admin

Cisco IOS ブロック送信元修復は、ルータから、相関ポリシー違反に関与している送信元ホストに送信されるトラフィックをブロックします。

マルチドメイン展開では、先祖ドメインで作成されたインスタンスに修復を追加することはできません。

始める前に

- Cisco IOS インスタンスの追加 （2760 ページ） の説明に従い、Cisco IOS インスタンスを追加します。

ステップ 1 **[Policies]** > **[Actions]** > **[Instances]**を選択します。

ステップ 2 修復を追加するインスタンスの横にある表示アイコン（  ）をクリックします。

ステップ 3 [設定されている修復（Configured Remediations）] セクションで、[送信元のブロック（Block Source）] を選択し、[追加（Add）] をクリックします。

コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 4 [修復名（Remediation Name）] と [説明（Description）] を入力します。

ステップ 5 [作成（Create）] をクリックし、次に [完了（Done）] をクリックします。

次のタスク

- 相関ポリシー違反への応答として修復を割り当てます（ルールとホワイトリストに応答を追加する （2700 ページ） を参照）。

Cisco IOS ブロック送信元ネットワークの修復の追加

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin Discovery Admin

Cisco IOS ブロック送信元ネットワーク修復は、ルータから、相関ポリシー違反に関与している送信元ホストのネットワークに送信されるトラフィックをブロックします。

マルチドメイン展開では、先祖ドメインで作成されたインスタンスに修復を追加することはできません。

始める前に

- Cisco IOS インスタンスの追加 （2760 ページ） の説明に従い、Cisco IOS インスタンスを追加します。

ステップ 1 **[Policies]** > **[Actions]** > **[Instances]**を選択します。

ステップ 2 修復を追加するインスタンスの横にある表示アイコン（  ）をクリックします。

ステップ 3 [設定されている修復（Configured Remediations）] セクションで、[送信元ネットワークのブロック（Block Source Network）] を選択し、[追加（Add）] をクリックします。

コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 4 [修復名（Remediation Name）] と [説明（Description）] を入力します。

ステップ 5 [ネットマスク（Netmask）] フィールドに、トラフィックをブロックするネットワークの説明となるサブネット マスクまたは CIDR 表記を入力します。

たとえば、1 つのホストがルールをトリガーとして使用したときにクラス C ネットワーク全体へのトラフィックをブロックするには、ネットマスクとして `255.255.255.0` または `24` を使用します。

別の例として、トリガーの IP アドレスを含む 30 個のアドレスへのトラフィックをブロックするには、ネットマスクとして `255.255.255.224` または `27` を指定します。この場合、IP アドレス `10.1.1.15` が修復をトリガーとして使用し、`10.1.1.1` と `10.1.1.30` の間のすべての IP アドレスがブロックされます。トリガーの IP アドレスのみをブロックするには、このフィールドは空のままにして、`32` を入力するか、または `255.255.255.255` を入力します。

ステップ 6 [作成（Create）] をクリックし、次に [完了（Done）] をクリックします。

次のタスク

- 相関ポリシー違反への応答として修復を割り当てます（ルールとホワイトリストに応答を追加する （2700 ページ） を参照）。

関連トピック

Firepower システムの IP アドレス表記法 （20 ページ）

Nmap スキャン修復

Firepower システムには、Nmap™ という、ネットワーク調査およびセキュリティ監査を目的としたオープン ソースのアクティブ スキャナが統合されています。Nmap 修復を使用して、相関ポリシー違反に対応できます。これは、Nmap スキャン修復をトリガーします。

Nmap スキャンの詳細については、Nmap スキャン （2517 ページ）を参照してください。

セット属性値修復

トリガーイベントが発生したホストでホスト属性値を設定することにより、相関ポリシー違反に応答できます。テキストのホスト属性の場合、イベントの説明を属性値として使用できます。

セット属性修復の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin Discovery Admin

ステップ 1 **[Policies]** > **[Actions]** > **[Instances]**を選択します。

ステップ 2 セット属性値インスタンスの追加 （2766 ページ）の説明に従って、セット属性インスタンスを作成します。

ステップ 3 セット属性値修復の追加 （2767 ページ）の説明に従って、セット属性修復を追加します。

次のタスク

- 相関ポリシー違反への応答として修復を割り当てます（ルールとホワイトリストに応答を追加する （2700 ページ） を参照）。

関連トピック

定義済みホスト属性 （3180 ページ）
ユーザ定義のホスト属性 （3181 ページ）

セット属性値インスタンスの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin Discovery Admin

ステップ 1 **[Policies]** > **[Actions]** > **[Instances]**を選択します。

ステップ 2 [新しいインスタンスの追加（Add a New Instance）] リストから [セット属性値（Set Attribute Value）] を選択し、[追加（Add）] をクリックします。

ステップ 3 [インスタンス名（Instance Name）] と [説明（Description）] を入力します。

ステップ 4 [作成（Create）] をクリックします。

次のタスク

- セット属性値修復の追加 （2767 ページ） の説明に従って、セット属性修復を作成します。

セット属性値修復の追加

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin Discovery Admin

セット属性値修復は相関ポリシー違反に関与したホストにホスト属性を設定します。属性を設定する各属性の値について修復を作成します。テキスト属性の場合、トリガーイベントの説明を属性値として使用できます。

マルチドメイン展開では、先祖ドメインで作成されたインスタンスに修復を追加することはできません。

始める前に

- セット属性値インスタンスの追加 （2766 ページ） の説明に従って、セット属性インスタンスを作成します。

ステップ 1 **[Policies]** > **[Actions]** > **[Instances]**を選択します。

ステップ 2 修復を追加するインスタンスの横にある表示アイコン（）をクリックします。

ステップ 3 [設定されている修復（Configured Remediations）] セクションで、[セット属性値（Set Attribute Value）] を選択し、[追加（Add）] をクリックします。

コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 4 [修復名（Remediation Name）] と [説明（Description）] を入力します。

ステップ 5 送信元データ、宛先データをもつイベントへの応答としてこの修復を使用するには、[イベントが決定するホストを更新（Update Which Host(s) From Event）] オプションを選択します。

ステップ 6 テキスト属性の場合、以下に従い [属性値にイベントからの説明を使用（Use Description From Event For Attribute Value）] を指定します。

- イベントの説明を属性値として使用するには、[オン（On）] をクリックし、設定する [属性値（Attribute Value）] を入力します。
- 修復の [属性値（Attribute Value）] 設定を属性値として使用するには、[オフ（Off）] をクリックします。

ステップ 7 [作成（Create）] をクリックし、次に [完了（Done）] をクリックします。

次のタスク

- 相関ポリシー違反への応答として修復を割り当てます（ルールとホワイトリストに応答を追加する （2700 ページ） を参照）。

修復モジュールの管理

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin Discovery Admin

マルチドメイン展開では、現在のドメインでインストールされた修復モジュールが表示されます。このモジュールは削除可能です。また、先祖ドメインでインストールされたモジュールも表示されますが、これは削除できません。下位ドメインの修復モジュールを管理するには、そのドメインに切り替えます。

ステップ 1 **[Policies]** > **[Actions]** > **[Modules]**を選択します。

ステップ 2 修復モジュールを管理します。

- 設定：モジュールの [モジュール詳細（Module Detail）] ページを表示して、そのモジュールのインスタンスと修復を設定するには、表示アイコン（）をクリックします。マルチドメイン展開では、[モジュール詳細（Module Detail）] ページを使用して、先祖ドメインでインストールされたモジュールに対応する現在のドメイン内のインスタンスを追加、削除、または編集することはできません。代わりに、[インスタンス（Instances）] ページ（**[Policies]** > **[Actions]** > **[Instances]**）を使用します。修復インスタンスの管理 （2769 ページ） を参照してください。
- 削除：使用されていないカスタム モジュールを削除するには、削除アイコン（）をクリックします。システム付属のモジュールは削除できません。
- インストール：カスタム モジュールをインストールするには、[ファイルの選択（Choose File）] をクリックしてモジュールを参照し、[インストール（Install）] をクリックします。詳細については、*Firepower* システム修復 *API* ガイドを参照してください。

修復インスタンスの管理

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin Discovery Admin

[インスタンス（Instances）] ページには、すべての修復モジュールのすべての設定済みインスタンスがリスト表示されます。

マルチドメイン展開では、現在のドメインで作成された修復インスタンスが表示されます。このインスタンスは編集可能です。また、先祖ドメインで作成されたインスタンスも表示されますが、これは編集できません。下位ドメインの修復インスタンスを管理するには、そのドメインに切り替えます。

先祖ドメインで作成したインスタンスに修復を追加することはできませんが、同様の設定済みインスタンスを現在のドメインに作成して、そのインスタンスに修復を追加することはできます。また、先祖ドメインで作成した修復は、相関応答として使用することもできます。

ステップ 1 **[Policies]** > **[Actions]** > **[Instances]**を選択します。

ステップ 2 修復インスタンスを管理します。

- 追加：インスタンスを追加するには、インスタンスを追加する修復モジュールを選択して、[追加（Add）] をクリックします。システム付属のモジュールについては、次を参照してください。
  - ISE EPS インスタンスの追加 （2758 ページ）
  - Cisco IOS インスタンスの追加 （2760 ページ）
  - Nmap スキャン インスタンスの追加 （2534 ページ）
  - セット属性値インスタンスの追加 （2766 ページ）

  カスタム モジュールを追加する際のヘルプは、そのモジュールのドキュメントを参照してください（使用可能な場合）。
- 設定：インスタンスの詳細を設定して、インスタンスに修復を追加するには、表示アイコン（）をクリックします。
- 削除：使用されていないインスタンスを削除するには、削除アイコン（）をクリックします。

1 つの修復モジュールのインスタンスの管理

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin Discovery Admin

[モジュール詳細（Module Detail）] ページには、特定の修復モジュールに設定されたインスタンスと修復がすべて表示されます。

マルチドメイン展開では、現在のドメインと先祖ドメインにインストールされた修復モジュールの [モジュール詳細（Module Detail）] ページにアクセスできます。ただし、[モジュール詳細（Module Detail）] ページを使用して、先祖ドメインにインストールされているモジュールに対応する現在のドメイン内のインスタンスを追加、削除または編集することはできません。代わりに、[インスタンス（Instances）] ページ（**[Policies]** > **[Actions]** > **[Instances]**）を使用します。修復インスタンスの管理 （2769 ページ）を参照してください。

ステップ 1 **[Policies]** > **[Actions]** > **[Modules]**を選択します。

ステップ 2 管理するインスタンスを持つ修復モジュールの横にある表示アイコン（  ）をクリックします。

ステップ 3 修復インスタンスを管理します。

- 追加：インスタンスを追加するには、[追加（Add）] をクリックします。システム付属のモジュールについては、次を参照してください。
  - ISE EPS インスタンスの追加 （2758 ページ）
  - Cisco IOS インスタンスの追加 （2760 ページ）
  - Nmap スキャン インスタンスの追加 （2534 ページ）
  - セット属性値インスタンスの追加 （2766 ページ）

  カスタム モジュールのインスタンスを追加する際のヘルプは、そのモジュールのドキュメントを参照してください（提供されている場合）。

- 設定：インスタンスの詳細を設定して、インスタンスに修復を追加するには、表示アイコン（  ）をクリックします。
- 削除：使用されていないインスタンスを削除するには、削除アイコン（  ）をクリックします。

第 XXIV 部

レポートとアラート

第 112 章

レポートの操作

以下のトピックでは、Firepower システムでレポートを操作する方法について説明します。

レポートの概要

Firepower システムは、次の 2 つのタイプのレポートを提供します。

- リスク レポート （2773ページ） - ネットワーク上で検出されたリスクの高レベル サマリ。
- 標準レポートの概要 （2775ページ） - Firepower システムのあらゆる側面に関する詳細でカスタマイズ可能なレポート。

リスク レポート

リスク レポートは、組織で検出されたリスクの概要を理解しやすい形で示す、移植可能なサマリーです。これらのレポートを使用することで、システムへのアクセス権がない人々や、ネットワーク セキュリティのエキスパートではない人々とも、リスク領域に関する情報やそれらのリスクに対処するための推奨案を共有できます。これらのレポートは、ネットワーク セキュリティへの投資領域に関する話し合いを促進することを目的としています。

リスク レポートの生成、表示および印刷

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Any Security Analyst/Maintenance User

標準レポートのテンプレートは、リスク レポートには適用されません。

レポートは現在のドメインに関するものになります。

各リスク レポートは、HTML ファイルとして生成されます。

リスク レポートの生成をスケジュールするには、レポートの生成の自動化（245 ページ）を参照してください。

始める前に

- 概要を取得するリスクを検出するように、システムが設定されていることを確認します。
- レポートを電子メールで送信しようとしていて、まだリレーホストを設定していない場合は、ここで設定できます。詳細については、メール リレー ホストおよび通知アドレスの設定 （1303 ページ）を参照してください。

ステップ 1 **[Overview]** > **[Reporting]**を選択します。

ステップ 2 [レポート テンプレート（Report Templates）] タブをクリックします。

ステップ 3 目的のレポートの [レポートの生成（Report）] アイコンをクリックします。

ステップ 4 情報を入力します。

- [入力パラメータ（Input Parameters）] セクションに入力した情報は、レポートのタイトル ページに表示されます。これらのフィールドは、空のままでもかまいません。

ステップ 5 [生成（Generate）] をクリックします。

ステップ 6 [OK] をクリックします。

次のタスク

- リスク レポートを表示、ダウロード、移動、または削除するには、生成されたレポートの操作について （2802 ページ）を参照してください。
- ほとんどのサポート対象ブラウザから、リスク レポートを PDF に出力できます。最適な結果を得るために、ブラウザの印刷または印刷プレビューの設定で、背景色、画像、およ

びオプションでヘッダーとフッターを有効にします。サポートされるページ サイズは、A4 および US Letter です。

標準レポートの概要

Firepowerシステムは柔軟なレポート作成システムを提供しており、Firepower Management Centerで表示されるイベント ビューやダッシュボードを使用して、複数のセクションがあるレポートを短時間で簡単に生成できます。独自のカスタム レポートを最初から設計することもできます。

レポートは、通信しようとしている内容が含まれるドキュメント ファイルで、PDF、HTML、または CSV 形式になります。レポート テンプレートは、データの検索設定とレポートおよびそのセクションの形式を指定します。Firepower システムには強力なレポート デザイナが含まれていて、レポート テンプレートの設計を自動的に行います。Web インターフェイスに表示されるイベント ビュー テーブルやダッシュボードのグラフィックの内容を複製できます。

レポート テンプレートは必要な数だけ作成できます。各レポート テンプレートは、レポートの個々のセクションを定義し、レポートの内容を作成するデータベース検索設定を指定し、表示形式（表、グラフ、詳細表示など）とタイムフレームも指定します。さらに、テンプレートでは、表紙や目次の情報、ドキュメントページに見出しとフッターを付けるかどうかなどのドキュメント属性も指定します（PDF 形式のレポートでのみ指定可能）。レポート テンプレートを 1 つの設定パッケージ ファイルとしてエクスポートし、別のFirepower Management Centerにインポートして再使用できます。

テンプレートに入力パラメータを組み込んで実用性を向上させることができます。入力パラメータを使用すると、同じレポートを用途に合わせて異なる様々なレポートに変えることができます。入力パラメータのあるレポートを生成するときには、生成プロセスで各入力パラメータの値を入力するよう求められます。ユーザが入力する値は、レポートの内容をその1回だけ決定するものです。たとえば、侵入イベントのレポートを作成する検索の宛先 IP フィールドに入力パラメータを使用できます。この場合、レポートの生成時に、宛先 IP アドレスの入力を求められたときに特定の部門のネットワーク セグメントを指定できます。その結果、この特定の部門に関する情報だけが含まれるレポートが生成されます。

レポートの設計について

レポート テンプレート

レポート テンプレートを使用して、レポートの各セクション内のデータの内容と形式や、レポート ファイルのドキュメント属性（表紙、目次、ページ ヘッダー、ページ フッター）を定義します。レポートの生成後、削除しない限りテンプレートは再利用可能な状態になります。

レポートには、1 つ以上の情報セクションが含まれます。個々のセクションごとに形式（テキスト、表、またはグラフ）を選択します。セクションの形式の選択内容によっては、組み込めるデータが制約される場合があります。たとえば、円グラフの形式を使用すると、特定の表に

時間ベースの情報を表示できません。いつでもセクションのデータの基準や形式を変更して、表示を最適にすることができます。

定義済みイベント ビューのレポートの初期設計をベースにするか、定義済みのダッシュボード、ワークフロー、または要約から内容をインポートして設計を開始できます。空のテンプレート シェルから始めて、1つずつセクションを追加したり属性を定義したりすることもできます。

（注） マルチドメイン導入では、先祖ドメインに属するレポートテンプレートを表示することはできますが、編集することはできません。これらのテンプレートからレポートを生成するには、テンプレートを現在のドメインにコピーする必要があります。

レポート テンプレート フィールド

次の表では、レポートテンプレートにセクションを作成するために使用できるフィールドについて説明します。すべてのフィールドが、すべてのタイプのセクションで使用されるわけではありません。セクション フォーマットを選択すると、システムにより適切なフィールドが表示されます。

フィールド名	セクションタイプ	定義（Definition）
フォーマット（Format）	適用対象外	セクション データのフォーマットを選択します。 棒グラフ：選択した変数の数量を比較します。 折れ線グラフ：選択した変数の時間の経過に伴う傾向/変化を示します。時間ベースのテーブルにのみ使用できます。 円グラフ：選択した各変数を全体の割合として示します。数量がゼロの変数はグラフからドロップされます。ごくわずかな数量は、[その他（Other）]というラベルのカテゴリに集められます。 表形式の表示：レコードごとの属性の値を示します。要約や統計のデータには使用できません。 詳細表示：パケット（侵入イベントの場合）やホスト プロファイル（ホスト イベントの場合）など、特定のイベントに関連付けられた複合オブジェクトのデータを示します。このフォーマットは、この種のオブジェクトが関係する特定のイベント タイプだけに使用できます。出力が多数要求されている場合には、パフォーマンスが低下することがあります。
テーブル	すべて（All）	セクション データが抽出されるテーブルを選択します。
プリセット（Preset）	すべて（All）	定義済みの検索。新しい検索設定を定義する際に、該当するプリセットを選択して、検索条件を初期化します。

フィールド名	セクションタイプ	定義（Definition）
検索またはフィルタ（Search or Filter）	すべて（All）	ほとんどのテーブルの場合、定義済みまたは保存済みの [検索（Search）] を使用してレポートを制約できます。編集アイコン（）をクリックして、新しい検索を作成することもできます。 アプリケーション統計表では、ユーザ定義のアプリケーションの[フィルタ（Filter）] を使用して、レポートを制約できます。
X 軸（X-Axis）	棒グラフ 折れ線グラフ 円グラフ	選択したグラフの X 軸に利用可能なデータ。 折れ線グラフの場合、X 軸の値は常に [時刻（Time）] です。棒グラフと円グラフの場合、X 軸の値として**時刻**を選択できません。
Y 軸（Y-Axis）	棒グラフ 折れ線グラフ 円グラフ	選択したグラフの Y 軸に利用可能なデータ。
セクションの説明（Section Description）	すべて（All）	セクション内で検索データの前にある説明テキスト。 テキストと入力パラメータの組み合わせを入力します。新しいセクションのデフォルトは `$<Time Window>` と `$<Constraints>` です。
時間枠（Time Window）	すべて（All）	セクションに表示されるデータの時間枠。 セクションで時間ベースのテーブルを検索する場合、チェックボックスを選択して、レポートのグローバル時間枠を継承できます。または、セクションの特定の時間枠を設定することもできます。
最大結果数（Maximum Results）	テーブルビュー 詳細ビュー	含める一致するレコードの最大数。 PDF レポートには、CSV または HTML レポートよりも少ないレコードを含めることができます。数が大きすぎる場合、Web インターフェイスでは警告およびエラーのアイコンが使用されて、そのことが示されます。ポインタをアイコンの上に移動させると、制限が表示されます。
結果（Results）	棒グラフ 円グラフ	[上（Top）] または [下（Bottom）] を選択し、チャートを作成するために使用する一致するレコードの数を入力します。
カラー（Color）	棒グラフ 折れ線グラフ	セクション内でグラフ化されるデータの色。

レポート テンプレートの作成

レポート テンプレートは、独自のデータベース クエリから個別に構築されたセクションのフレームワークです。

新しいレポートテンプレートを作成するには、新しいテンプレートを作成する、既存のテンプレートを使用する、イベント ビューをテンプレートのベースにする、ダッシュボードまたはワークフローをインポートするという方法があります。

既存のレポートテンプレートをコピーしない場合は、まったく新しいテンプレートを作成できます。テンプレート作成の最初の手順として、セクションを追加したり形式設定したりできるフレームワーク シェルを生成します。次に、ご希望の順序で、個々のテンプレート セクションを設計し、レポート ドキュメントの属性を設定します。

各テンプレートセクションは、検索設定やフィルタによって生成されたデータセットで構成され、表示モードを確定する形式の仕様（表や円グラフなど）があります。出力に含めるデータレコードのフィールドを選択し、タイムフレームと表示するレコード数も選択して、さらにセクションの内容を確定します。

（注） セクション プレビュー ユーティリティを使用して、カラムの選択内容や、円グラフの色などの出力の特性を検査します。このインジケータは、設定済みの検索設定を必ずしも正確に反映するとは限りません。

テンプレートから生成したレポートには、表紙、ヘッダーとフッター、ページ番号など、すべてのセクションにまたがって機能を制御する複数のドキュメント属性があります。

CSVをドキュメントの形式として選択した場合は、ドキュメントの属性を設定できないことに注意してください。

既存のテンプレートの中に適切なモデルがあれば、そのテンプレートをコピーして属性を編集することで、新しいレポート テンプレートを作成できます。また、Cisco から一連の定義済みレポートテンプレートも提供されています。これらのテンプレートは、[レポート（Reports）] タブのテンプレートの一覧で確認できます。

イベントビューからレポートテンプレートを作成し、必要に応じて変更することができます。セクションを追加したり、自動的に組み込まれるセクションを変更したり、セクションを削除したりできます。

ダッシュボード、ワークフロー、統計の要約をインポートして、新しいレポートをすばやく作成できます。インポートすると、ダッシュボードのウィジェット グラフィックごと、およびワークフローのイベントビューごとにセクションが作成されます。最も重要な情報に焦点が当たるように不要なセクションを削除できます。

カスタム レポート テンプレートの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Any Security Analyst

ステップ 1 **[Overview]** > **[Reporting]**を選択します。

ステップ 2 [レポート テンプレート（Report Templates）] タブをクリックします。

ステップ 3 [レポート テンプレートの作成（Create Report Template）] をクリックします。

ステップ 4 [レポートタイトル（Report Title）] フィールドに、新しいテンプレートの名前を入力します。

ステップ 5 レポート タイトルに入力パラメータを追加するには、タイトル内でパラメータ値を表示する位置にカーソルを置き、入力パラメータの挿入アイコン（  ）をクリックします。

ステップ 6 必要に応じて、[レポート セクション（Report Sections）] タイトル バーの下にある追加アイコンのセットを使用し、セクションを挿入します。

ステップ 7 レポート テンプレートの設定 （2782 ページ）の説明に従ってセクション コンテンツを設定します。

ヒント セクションのウィンドウの下部にある [プレビュー（Preview）] をクリックして、選択したカラムのレイアウトやグラフィックの形式を表示できます。

ステップ 8 [詳細（Advanced）] をクリックし、レポート テンプレート内のドキュメント属性 （2792 ページ）の説明に従って PDF および HTML レポートの属性を設定します。

ステップ 9 [保存（Save）] をクリックします。

エラーが表示された場合は、各セクションの結果値の横にある黄色の三角形を探します。このような三角形が見つかった場合は、次のいずれかの操作を行います。

- 黄色の三角形が表示されたフィールドごとに、三角形をマウス オーバーして、結果の数を表示された数まで削減します。
- [生成（Generate）] をクリックして、PDF 以外の出力形式を含めます。

既存のテンプレートからのレポート テンプレートの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Any Security Analyst

ステップ 1 **[Overview]** > **[Reporting]** を選択します。

ステップ 2 [レポート テンプレート（Report Templates）] タブをクリックします。

ステップ 3 コピーするレポート テンプレートの横にあるコピー アイコン（  ）をクリックします。

ステップ 4 [レポート タイトル（Report Title）] フィールドに、名前を入力します。

ステップ 5 [保存（Save）] をクリックします。

ステップ 6 必要に応じてテンプレートを変更します。

イベント ビューからのレポート テンプレートの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Any Security Analyst

ステップ 1 レポートに含めるイベントをイベント ビューに入力します。

- イベント検索設定を使用して、表示するイベントを定義します。
- イベント ビューに該当するイベントが表示されるまでワークフローをドリルダウンします。

ステップ 2 イベント ビューのページから、[レポート デザイナ（Report Designer）] をクリックします。

[レポート セクション（Report Sections）]ページが表示され、キャプチャされるワークフロー内のビューごとにセクションが示されます。

ステップ 3 オプションで、[レポート タイトル（Report Title）] フィールドに新しい名前を入力し、[保存（Save）] をクリックします。

ステップ 4 次の操作を実行できます。

- 表紙、目次、開始ページ番号、またはヘッダーおよびフッター テキストを追加します：[詳細設定（Advanced Settings）] をクリックします。
- 改ページを追加します：改ページの追加アイコン（  ）をクリックし、新しい改ページオブジェクトを、テンプレートの下部から新しいページを開始するセクションの先頭にドラッグします。
- テキスト セクションを追加します：テキスト セクションの追加アイコン（  ）をクリックし、新しいテキストセクションを、テンプレートの下部からレポートテンプレート内で表示する位置にドラッグします。
- セクションのタイトルを変更します：タイトルバーでセクションタイトルをクリックし、セクションタイトルを入力して、[OK] をクリックします。
- レポート セクションを設定します。各セクションのフィールド設定を調整します。

  ヒント セクションの現在のカラムのレイアウトやグラフの形式を表示する場合は、そのセクションの [プレビュー（Preview）] リンクをクリックします。

- レポートからテンプレートセクションを除外します：セクションのタイトルバーで削除アイコン（  ）をクリックし、削除を確認します。

  （注） 一部のワークフロー内の最後のレポート セクションには詳細ビューが含まれ、ワークフローに応じてパケット、ホスト プロファイル、または脆弱性が示されます。レポートの生成時に、これらの詳細ビューがあるイベントを多数取得すると、Firepower Management Center のパフォーマンスに影響を与えることがあります。

ステップ 5 **[保存（Save）]** をクリックします。

ダッシュボードまたはワークフローのインポートによるレポート テンプレートの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Any Security Analyst

ステップ 1 レポート内で複製するダッシュボード、ワークフロー、または要約を識別します。

ステップ 2 **[Overview]** > **[Reporting]**を選択します。

ステップ 3 [レポート テンプレート（Report Templates）] タブをクリックします。

ステップ 4 [レポート テンプレートの作成（Create Report Template）] をクリックします。

ステップ 5 [レポート タイトル（Report Title）] フィールドに新しいレポート テンプレートの名前を入力します。

ステップ 6 [保存（Save）] をクリックします。

ステップ 7 インポート セクション アイコン（  ）をクリックします。[インポート レポート セクション（Import Report Sections）] のデータ ソース オプション （2781 ページ）で説明されているデータ ソースのいずれかを選択できます。

ステップ 8 ドロップダウン メニューからダッシュボード、ワークフロー、または要約を選択します。

ステップ 9 追加するデータ ソースの、[インポート（Import）] をクリックします。

ダッシュボードの場合、ウィジェット グラフィックごとに独自のセクションがあります。ワークフローの場合、イベント ビューごとに独自のセクションがあります。

ステップ 10 必要に応じてセクションの内容を変更します。

（注） 一部のワークフロー内の最後のレポート セクションには詳細ビューが含まれ、ワークフローに応じてパケット、ホスト プロファイル、または脆弱性が示されます。レポートの生成時に、これらの詳細ビューがあるイベントを多数取得すると、Firepower Management Center のパフォーマンスに影響を与えることがあります。

ステップ 11 **[保存（Save）]** をクリックします。

[インポート レポート セクション（Import Report Sections）] のデータ ソース オプション

表 *281 : [インポート レポート セクション（Import Report Sections）]* ウィンドウのデータ ソース オプション

選択オプション	インポート対象
Import Dashboard	選択したダッシュボード上のカスタム分析ウィジェット。

選択オプション	インポート対象
Import Workflow	定義済みのワークフローまたはカスタム ワークフロー。 選択項目の形式は次のようになっています。 `Table - Workflow name` たとえば、`Connection Events - Traffic by Port` は、Connection Events テーブルから生成された Traffic by Port ワークフロー内のビューをインポートします。
Import Summary Sections	次の一般的な要約： • Intrusion Detailed Summary • Intrusion Short Summary • Discovery Detailed Summary • ディスカバリの概要サマリー（Discovery Short Summary）

レポート テンプレートの設定

レポートテンプレートを作成すれば、そのテンプレートを変更およびカスタマイズできます。さまざまなレポートセクションの属性を変更して、セクションとそのデータ表示の内容を調整できます。

レポート テンプレート内の各セクションでは、データベース テーブルを照会して、そのセクションの内容を生成します。セクションのデータ形式を変更する際にも同じデータ クエリーが使用されますが、形式のタイプごとの分析の目的に従って、セクションに表示されるフィールドが変わります。たとえば、侵入イベントの表形式の表示では、イベント レコードごとに多数のデータ フィールドがセクションに入力され、円グラフのセクションでは、選択した各属性が表すすべての一致レコードの割合が示され、個々のイベントに関する詳細情報は表示されません。棒グラフのセクションでは、特定の属性を持つ一致レコードの合計数が比較されます。折れ線グラフでは、1 つの属性に関係する一致レコード数の変化が時系列で要約されます。折れ線グラフは時間ベースのデータの場合のみ使用でき、ホスト、ユーザ、サードパーティの脆弱性などに関する情報の場合は使用できません。

レポートセクションの検索設定やフィルタは、セクションの内容のベースになるデータベース クエリーを指定します。ほとんどのテーブルの場合、定義済み検索設定か保存済み検索設定を使用してレポートを制約するか、新しい検索設定を即座に作成することができます。

- 定義済み検索設定は特定のイベント テーブルの検索サンプルの役割を果たし、レポートに含めようとしている、ネットワークに関する重要情報にクイック アクセスできます。
- 保存済みイベント検索設定には、自分や他のユーザが作成したすべてのパブリック イベント検索設定と、自分で保存したすべてのプライベート イベント検索設定が含まれます。

- 現在のレポート テンプレートの保存済み検索設定は、そのレポート テンプレート自体に限りアクセスできます。保存済みレポートテンプレートの検索設定の名前は、末尾が文字列「Custom Search」になります。ユーザは、レポートの設計時にこれらの検索設定を作成します。

[アプリケーションの統計（Application Statistics）] テーブルにユーザ定義のアプリケーション フィルタを使用して、レポートに制約を適用します。

セクション内にテーブルのデータを組み込む場合、データ レコード内のどのフィールドを表示するか選択できます。表形式のすべてのフィールドを組み込みに対象にも除外対象にもすることができます。レポートの目的を達成するのに必要なフィールドを選択し、それに従って配列したりソートしたりします。

テンプレートにテキストセクションを追加して、レポート全体や個々のセクションに概要などのカスタム テキストを用意することができます。

テンプレート内のどのセクションの前後にも改ページを追加できます。この機能は、複数のセクションから成るレポートで、各種セクションの概要を示すテキスト ページがある場合に特に便利です。

レポートテンプレートの時間枠によって、テンプレートのレポート作成期間が定義されます。

（注） セキュリティ アナリストは、自分が作成したレポート テンプレートだけを編集できます。マルチドメイン導入では、先祖ドメインのレポートテンプレートは編集できませんが、レポートテンプレートをコピーして子孫バージョンを作成することができます。

レポート テンプレート セクションのテーブルとデータ形式の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Any Security Analyst

ステップ 1 [レポート テンプレート（Rreport Template）] セクションで、[テーブル（Table）] ドロップダウン メニューを使用して、問い合わせるテーブルを選択します。

選択したテーブルで使用できる出力形式ごとに、アイコンが [形式（Format）] フィールドに表示されます。

ステップ 2 セクションに該当する出力形式のアイコンを選択します。

ステップ 3 検索制約を変更するには、[検索（Search）] フィールドか [ファイルタ（Filter）] フィールドの横にある編集アイコン（ ）クリックします。

ステップ 4 グラフ出力形式（円グラフや棒グラフなど）の場合、ドロップダウンメニューを使用して、[X軸（X-Axis）] と [Y 軸（Y-Axis）] のパラメータを調整します。

X 軸の値を選択すると、互換性のある値だけが Y 軸のドロップダウンメニューに表示されます。その逆も同様です。

ステップ 5 テーブル出力の場合、出力内のカラム、表示順序、ソート順序を選択します。

ステップ 6 **[保存（Save）]** をクリックします。

関連トピック

レポート テンプレート フィールド （2776 ページ）

レポート テンプレート セクションの検索またはフィルタの指定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Any Security Analyst

ステップ 1 [レポート テンプレート（Rreport Template）] セクションで、[テーブル（Table）] ドロップダウン メニューからクエリを行うデータベース テーブルを選択します。

- ほとんどのテーブルでは、[検索（Search）] ドロップダウン リストが表示されます。
- [アプリケーション統計（Application Statistics）] テーブルでは、[フィルタ（Filter）] ドロップダウン リストが表示されます。

ステップ 2 レポートの制約に使用する検索かフィルタを選択します。

編集アイコン（）をクリックして、検索条件を表示したり、新しい検索を作成したりできます。

関連トピック

アプリケーション フィルタ （530 ページ）

表形式のセクションに表示される検索フィールドの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Any Security Analyst

ステップ 1 表形式のレポート セクションで、[フィールド（Fields）] パラメータの横にある編集アイコン（）をクリックします。

ステップ 2 セクションを変更する場合、フィールドを追加/削除し、望むカラムの順番にそれらのフィールドアイコンをドラッグします。

ステップ 3 どの列でもソート順序を変更する場合、各フィールドアイコンのドロップダウン リストを使用して、ソート順序および優先順位を設定する必要があります。

ステップ 4 [OK] をクリックします。

レポート テンプレートへのテキスト セクションの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Any Security Analyst

テキスト セクションには、複数のフォント サイズやフォント スタイル（太字や斜体など）を使用できるリッチ テキスト、入力パラメータ、インポート済みイメージを使用できます。

ヒント テキスト セクションは、レポートやそのセクションの概要説明に役立ちます。

ステップ 1 レポート テンプレート エディタで、テキスト セクション追加アイコン（）をクリックします。

ステップ 2 新しいテキスト セクションを、レポート テンプレート内のご希望の位置にドラッグします。

ステップ 3 テキスト セクションをページの最初または最後に移動するには、テキスト セクションの前または後に改ページを挿入します。

ステップ 4 テキストセクションの総称名を変更するには、タイトルバーのセクション名をクリックし、新しい名前を入力します。

ステップ 5 テキスト セクションの本文に形式設定済みのテキストやイメージを追加します。

レポートの生成時に動的に更新する入力パラメータを組み込むことができます。

ステップ 6 **[保存（Save）]** をクリックします。

関連トピック

入力パラメータ （2789 ページ）

レポート テンプレートへの改ページの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Any Security Analyst

ステップ 1 レポート テンプレート エディタで、改ページアイコン（）をクリックします。

改ページがテンプレートの下部に表示されます。

ステップ 2 改ページを、セクションの前後のご希望の場所にドラッグします。

ステップ 3 **[保存（Save）]** をクリックします。

グローバル時間枠とレポート テンプレート セクション

時間ベースのデータ（侵入イベントや検出イベントなど）があるレポートテンプレートにはグローバル時間枠があります。この時間枠は、テンプレート内の時間ベースのセクションでデフォルトで作成時に継承されます。グローバル時間枠を変更すると、グローバル時間枠を継承するように設定されているセクションのローカル時間枠が変更されます。[Inherit Time Window] チェック ボックスをクリアすると、個々のセクションの時間枠の継承を無効にできます。それから、ローカル時間枠を編集できます。

（注） グローバル時間枠の継承は、侵入イベントや検出イベントなど、時間ベースのテーブルからのデータがあるレポート セクションだけに適用されます。ネットワーク アセット（ホストやデバイス）と関連情報（脆弱性など）を報告するセクションの場合、各時間枠を個別に設定する必要があります。

レポート テンプレートとそのセクションのグローバル時間枠の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Any Security Analyst

ヒント レポート内のセクションごとに別の時間枠を使用できます。たとえば、最初のセクションを月の要約にして、残りのセクションで週レベルの詳細情報へドリルダウンするようにできます。この場合、セクション レベルの時間枠を個別に設定します。

ステップ 1 レポート テンプレート エディタで [生成（Generate）] をクリックします。

ステップ 2 グローバル時間枠を変更するには、時間枠のアイコン（）をクリックします。

ステップ 3 [イベント時間枠（Events Time Window）] タブで時間設定を変更します。

ステップ 4 [適用（Apply）] をクリックします。

ステップ 5 [生成（Generate）] をクリックしてレポートを生成し、[はい（Yes）] をクリックして確認します。

レポート テンプレート セクションのローカル時間枠の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Any Security Analyst

ステップ 1 テンプレートの [レポート セクション（Report Sections）] ページで、セクションの [時間枠の継承（Inherit Time Window）] チェック ボックスが存在する場合はクリアします。

ステップ 2 セクションのローカル時間枠を変更するには、時間枠のアイコン（）をクリックします。

（注） 統計テーブルからのデータがあるセクションでは、スライド式の時間枠のみ使用できます。

ステップ 3 [イベント時間枠（Events Time Window）] で [適用（Apply）] をクリックします。

ステップ 4 **[保存（Save）]** をクリックします。

レポート テンプレート セクションの名前変更

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Any Security Analyst

ステップ 1 レポート テンプレート エディタで、セクション ヘッダーの現在のセクション名をクリックします。

ステップ 2 新しいセクション名を入力します。

ステップ 3 [OK] をクリックします。

レポート テンプレート セクションのプレビュー

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Any Security Analyst

プレビュー機能は、表形式の表示のフィールドのレイアウトとソート順序や、円グラフの色などのグラフの読みやすさに関する重要な特性を表示します。

ステップ 1 レポート テンプレート セクションの編集中は、いつでも、そのセクションの [プレビュー（Preview）] をクリックできます。

ステップ 2 プレビューを閉じるには、[OK] をクリックします。

レポート テンプレート セクションでの検索

レポートが正常に作成されるかどうかは、レポートのセクションへの入力内容を決める検索設定の定義が重要な要素になります。Firepower システムには検索エディタが備わっており、レポートテンプレートで使用できる検索設定を表示したり、新しいカスタム検索設定を定義したりできます。

レポート テンプレートのセクションの検索

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Any Security Analyst

ステップ 1 レポート テンプレート内の関連するセクションから、[検索（Search）] フィールドの横にある編集アイコン（  ）をクリックします。

ステップ 2 事前定義済みの検索に基づいてカスタム検索を作成する場合は、[保存済み検索（Saved Searches）] ドロップダウンリストから事前定義された検索を選択する必要があります。

このリストには、このテーブルに対して使用可能な事前定義済みの検索設定がすべて表示されます。システム規模の事前定義済み検索設定とレポート固有の事前定義済み検索設定も含まれています。

ステップ 3 該当するフィールドで検索条件を編集します。

特定のフィールドでは、制約にイベント検索設定と同じ演算子（< や <> など）を含めることができます。複数の条件を入力すると、すべての基準を満たすレコードだけが検索で返されます。

ステップ 4 制約値を入力する代わりに、ドロップダウン メニューから入力パラメータを挿入する場合は、入力パラメータ アイコン（  ）をクリックする必要があります。

（注） レポートの検索設定の制約を編集すると、システムにより *section* custom search という名前で編集済みの検索設定が保存されます。*section* は、セクションのタイトル バーに示される文字列 custom search の前の名前の部分です。保存するカスタム検索設定の名前をわかりやすくするには、セクション名を変更した後に編集済みの検索設定を保存するようにしてください。保存したレポートの検索設定の名前は変更できません。

ステップ 5 [OK] をクリックします。

入力パラメータ

レポートの生成時に動的に更新できる入力パラメータをレポートテンプレート内で使用できます。入力パラメータのアイコン（  ）は、入力パラメータを処理できるフィールドを示します。次の 2 種類の入力パラメータがあります。

- 定義済みの入力パラメータは、内部システム関数か設定情報によって解決されます。たとえば、レポートの生成時に、システムにより `$<Time>` パラメータは現在の日時に置き換えられます。
- ユーザ定義の入力パラメータは、セクション検索で制約を行えます。入力パラメータを使用して検索設定を制約すると、レポートの生成時に要求者から値を収集するようにシステムに指示できます。この方法で、テンプレートを変更せずに、レポートを生成時に動的に調整して特定のデータのサブセットを表示できます。たとえば、レポートセクションの検索設定の [接続先 IP（Destination IP）] フィールドに入力パラメータを指定できます。指定後、レポートの生成時に、特定の部門の IP ネットワークのセグメントを入力して、その部門のデータだけを取得できます。

  文字列タイプの入力パラメータを定義して、電子メール（件名または本文）、レポートファイル名、テキストセクションなどのレポートの特定のフィールドに動的テキストを追加することもできます。すべて同じテンプレートを利用し、カスタマイズしたレポートファイル名、電子メール アドレス、電子メール メッセージを使用して、さまざまな部門用にレポートをパーソナライズできます。

定義済み入力パラメータ

表 *282*：定義済み入力パラメータ

このパラメータを入力すると、	テンプレートに含められる情報
`$<Logo>`	選択したアップロード済みのロゴ
`$<Report Title>`	レポート タイトル
`$<Time>`	レポートを実行する日付、時刻、粒度 1 秒
`$<Month>`	現在の月
`$<Year>`	現在の年
`$<System Name>`	Firepower Management Centerの名前
`$<Model Number>`	Firepower Management Center のモデル番号
`$<Time Window>`	レポート セクションに現在適用されている時間窓
`$<Constraints>`	レポート セクションに現在適用されている検索制約

表 *283 :* 定義済み入力パラメータの使用法

パラメータ	Report Template Cover Page	Report Template Report Title	Report Template Section Description	Report Template Text Section	Generate Report File Name	Generate Report Email Subject, Body
$<Logo>	はい	いいえ	いいえ	いいえ	いいえ	いいえ
$<Report Title>	はい	いいえ	はい	はい	はい	はい
$<Time>	はい	はい	はい	はい	はい	はい
$<Month>	はい	はい	はい	はい	はい	はい
$<Year>	はい	はい	はい	はい	はい	はい
$<System Name>	はい	はい	はい	はい	はい	はい
$<Model Number>	はい	はい	はい	はい	はい	はい
$<Time Window>	いいえ	いいえ	はい	いいえ	いいえ	いいえ
$<Constraints>	いいえ	いいえ	はい	いいえ	いいえ	いいえ

ユーザ定義の入力パラメータ

入力パラメータを使用して、検索設定の実用性を向上させます。入力パラメータにより、レポートの生成時に要求者から値を収集するようにシステムに指示できます。この方法で、検索設定を変更せずに、レポートを生成時に動的に制約して特定のデータのサブセットを表示できます。たとえば、レポートセクションの [Destination IP] フィールドに入力パラメータを指定して、部門レベルでセキュリティ イベントをドリル ダウンできます。レポートの生成時に、特定の部門の IP ネットワークのセグメントを入力して、その部門のデータだけを取得できます。

入力パラメータのタイプにより、そのパラメータを使用できる検索フィールドが決まります。特定のタイプは、該当するフィールドでのみ使用できます。たとえば、ユーザパラメータを文字列タイプとして定義すると、テキスト フィールド内への挿入には使用できますが、IP アドレスを使用するフィールドでは使用できません。

定義する入力パラメータごとに名前とタイプがあります。

表 *284 :* ユーザ定義の入力パラメータのタイプ

パラメータのタイプ	使用先のフィールド内のデータ
ネットワーク/IP	CIDR 形式の IP アドレスまたはネットワーク セグメント
アプリケーション	アプリケーション プロトコル、クライアント アプリケーション、または Web アプリケーションの名前
イベント メッセージ	イベント ビュー メッセージ

パラメータのタイプ	使用先のフィールド内のデータ
Device	FMC または管理対象デバイス
[ユーザ名（Username）]	イニシエータ ユーザやレスポンダ ユーザなどのユーザ ID
番号（VLAN ID、Snort ID、Vuln ID）（Number (VLAN ID, Snort ID, Vuln ID)）	VLAN ID、[Snort ID]、または脆弱性 ID
文字列	アプリケーションや OS のバージョン、注記、説明などのテキスト フィールド

ユーザ定義の入力パラメータの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Any Security Analyst

ステップ 1 レポート テンプレート エディタで、[詳細（Advanced）] をクリックします。

ステップ 2 入力パラメータ追加アイコン（  ）をクリックします。

ステップ 3 パラメータの [名前（Name）] を入力します。

ステップ 4 [タイプ（Type）] ドロップダウン リストから値を選択します。

ステップ 5 [OK] をクリックしてパラメータを追加します。

ステップ 6 [OK] をクリックしてエディタに戻ります。

ユーザ定義の入力パラメータの編集

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Any Security Analyst

レポート テンプレートの [入力パラメータ（Input Parameters）] セクションに、テンプレートに使用可能なユーザ定義パラメータがすべてリストされます。

ステップ 1 レポート テンプレート エディタで、[詳細設定（Advanced）] をクリックします。

ステップ 2 変更するパラメータの横にある編集アイコン（  ）をクリックします。

ステップ 3 [名前（Name）] に新しい名前を入力します。

ステップ 4 [タイプ（Type）] ドロップダウン リストを使用して、パラメータ タイプを変更します。

ステップ 5 [OK] をクリックして変更を保存します。

ステップ 6 入力パラメータを削除するには、入力パラメータの横にある削除アイコン（）をクリックし、確認します。

ステップ 7 [OK] をクリックしてレポート テンプレート エディタに戻ります。

ユーザ定義の入力パラメータによる検索の制約

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Any Security Analyst

定義した入力パラメータは、そのパラメータのタイプと一致する検索フィールドでのみ使用できます。たとえば、**ネットワーク/IP** タイプのパラメータは、CIDR 形式の IP アドレスまたはネットワーク セグメントを受け入れるフィールドだけで使用できます。

ステップ 1 レポート テンプレート エディタで、セクション内の [検索（Search）] フィールドの横にある編集アイコン（）をクリックします。

入力パラメータを使用できるフィールドは、入力パラメータのアイコン（）のマークが付けられます。

ステップ 2 フィールドの横にある入力パラメータのアイコン（）をクリックして、ドロップダウン メニューから入力パラメータを選択します。

ユーザ定義の入力パラメータは、アイコン（）のマークが付けられます。

ステップ 3 [OK] をクリックします。

レポート テンプレート内のドキュメント属性

レポートを生成する前に、レポートの外観に影響を与えるドキュメント属性を設定できます。これらの属性には、オプションの表紙と目次が含まれます。一部の属性のサポートは、レポートの形式に PDF、HTML、CSV のいずれを選択したかによって異なります。

表 *285 :* ドキュメント属性のサポート

属性	PDF のサポート	HTML のサポート	CSV のサポート
表紙	可能、オプションでロゴと外観のカスタマイズ	可能、オプションでロゴと外観のカスタマイズ	no
目次	はい	はい	いいえ（No）

属性	PDF のサポート	HTML のサポート	CSV のサポート
ページの見出しとフッター	可能、オプションでフィールド内にテキストかロゴ	いいえ	いいえ
カスタムの開始ページ番号	はい	いいえ	いいえ
先頭ページに番号を付けないオプション	はい	いいえ	いいえ

レポート テンプレート内のドキュメント属性の編集

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Any Security Analyst

ステップ 1 レポート テンプレート エディタで、[詳細（Advanced）] をクリックします。

ステップ 2 次の選択肢があります。

- 表紙の追加：表紙を追加するには、[表紙を含める（Include Cover Page）] チェックボックスをオンにします。
- 表示のカスタマイズ：表紙のデザインを編集するには、表紙のカスタマイズ（2794 ページ）を参照してください。
- 目次の追加：目次を追加するには、[目次を含める（Include Table of Contents）] チェックボックスをオンにします。
- ロゴの管理：テンプレートに関連付けられたロゴイメージを管理するには、レポートテンプレートのロゴの管理 （2794 ページ）を参照してください。
- ヘッダーとフッターの設定：テンプレートのヘッダーとフッターの要素を指定するには、[ヘッダー（Header）] フィールドと [フッター（Footer）] フィールのドロップダウン リストを使用します。
- 最初のページ番号の設定：レポートの最初のページ番号を指定するには、[ページ番号の開始（Page Number Start）] の値を入力します。
- 最初のページ番号の表示：レポートの最初のページのページ番号を表示するには、[最初のページに番号を付けますか（Number First Page?）] チェックボックスをオンにします。このオプションを選択すると、表紙には番号が付けられません。

ステップ 3 [OK] をクリックして変更を保存します。

表紙のカスタマイズ

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Any Security Analyst

レポート テンプレートの表紙をカスタマイズできます。表紙には、複数のフォント サイズやフォント スタイル（太字や斜体など）を使用できるリッチ テキスト、入力パラメータ、インポート済みイメージを使用できます。

ステップ 1 レポート テンプレート エディタで、[詳細（Advanced）] をクリックします。

ステップ 2 [表紙のデザイン（Cover Page Design）] の横にある編集アイコン（  ）をクリックします。

ステップ 3 リッチ テキスト エディタで表紙のデザインを編集します。

ステップ 4 [OK] をクリックします。

レポート テンプレートのロゴの管理

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Any Security Analyst

Firepower Management Center で複数のロゴを保存し、さまざまなレポート テンプレートに関連付けることができます。テンプレートを設計する際に、ロゴの関連付けを設定します。テンプレートをエクスポートすると、エクスポート パッケージにロゴが含まれます。

Firepower Management Center にロゴをアップロードすると、そのロゴは次のものに使用できます。

- Firepower Management Center のすべてのレポート テンプレート、または
- マルチドメイン展開では、現在のドメイン内のすべてのレポート テンプレート

ロゴ画像は、PNG 形式、JPG 形式、または GIF 形式することができます。

レポート内のロゴは、Firepower Management Center にアップロードされているいずれかの JPG 画像に変更できます。たとえば、テンプレートを再使用する場合は、別の組織のロゴをレポートに関連付けることができます。

アップロードしたロゴは、削除できます。ロゴを削除すると、そのロゴが使用されているすべてのテンプレートから削除されます。削除を取り消すことはできません。事前定義済のシスコ ロゴは削除できない点に注意してください。

ステップ 1 レポート テンプレート エディタで、[詳細（Advanced）] をクリックします。

テンプレートに現在関連付けられているロゴは、[一般設定（General Settings）] の [ロゴ（Logo）] の下に表示されます。

ステップ 2 ロゴの横にある編集アイコン（）をクリックします。

ステップ 3 次の選択肢があります。

- 追加：新しいロゴを追加します。詳細については、新しいロゴの追加（2795 ページ）を参照してください。
- 変更：レポート テンプレートのロゴを変更します。詳細については、レポート テンプレートのロゴの変更（2795 ページ）を参照してください。
- 削除：ロゴを削除します。詳細については、ロゴの削除（2796 ページ）を参照してください。

新しいロゴの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Any Security Analyst

ステップ 1 レポート テンプレート エディタで、[詳細（Advanced）] をクリックします。

ステップ 2 [ロゴ（Logo）] フィールドの横にある編集アイコン（）をクリックします。

ステップ 3 [ロゴのアップロード（Upload Logo）] をクリックします。

ステップ 4 [参照（Browse）] ボタンをクリックし、ファイルの場所を参照し、[開く（Open）] をクリックします。

ステップ 5 [アップロード（Upload）] をクリックします。

ステップ 6 新しいロゴを現在のテンプレートに関連付けるには、それを選択し、[OK] をクリックします。

レポート テンプレートのロゴの変更

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Any Security Analyst

ステップ 1 レポート テンプレート エディタで、[詳細（Advanced）] をクリックします。

ステップ 2 [ロゴ（Logo）] フィールドの横にある編集アイコン（）をクリックします。

ステップ 3 [ロゴの選択（Select Logo）] ダイアログで、レポート テンプレートに関連付けるロゴを選択します。
ステップ 4 [OK] をクリックします。

ロゴの削除

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Any Security Analyst

ステップ 1 レポート テンプレート エディタで、[詳細（Advanced）] をクリックします。
ステップ 2 [ロゴ（Logo）] フィールドの横にある編集アイコン（  ）をクリックします。
ステップ 3 [ロゴの選択（Select Logo）] ダイアログで、削除するロゴを選択します。
ステップ 4 [ロゴの削除（Delete Logo）] をクリックします。
ステップ 5 [OK] をクリックします。

レポート テンプレートの管理

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin

マルチドメイン展開では、現在のドメインで作成されたレポート テンプレートが表示されます。このテンプレートは編集可能です。先祖ドメインで作成されたレポートテンプレートも表示されますが、これは編集できません。下位のドメインのレポートテンプレートを表示および編集するには、そのドメインに切り替えます。システムによって表示されるレポートは、現在のドメインで作成されたもののみです。

ステップ 1 **[Overview]** > **[Reporting]**を選択します。
ステップ 2 [レポート テンプレート（Report Templates）] タブをクリックします。
ステップ 3 次の選択肢があります。

- 削除：削除するテンプレートの横にある削除アイコン（  ）をクリックして確認します。

  システム付属のレポートテンプレートは削除できません。セキュリティアナリストは、自分が作成したレポートテンプレートのみを削除できます。マルチドメイン展開では、現在のドメインに属しているレポート テンプレートのみを削除できます。

- 編集：レポートテンプレートを編集する場合は、レポートテンプレートの編集（2797ページ）を参照してください。

- エクスポート：レポート テンプレートをエクスポートする場合は、レポート テンプレートのエクスポート （2798 ページ）を参照してください。

  ヒント　また、標準設定のエクスポート プロセスを使用してレポート テンプレートをエクスポートすることもできます。設定のエクスポート （232 ページ）を参照してください。

- インポート：レポート テンプレートをインポートする場合は、設定のインポート （233 ページ）を参照してください。

レポート テンプレートの編集

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Any Security Analyst

マルチドメイン展開では、現在のドメインで作成されたレポート テンプレートが表示されます。このテンプレートは編集可能です。先祖ドメインで作成されたレポートテンプレートも表示されますが、これは編集できません。下位のドメインのレポートテンプレートを表示および編集するには、そのドメインに切り替えます。

ステップ 1　**[Overview]** > **[Reporting]**を選択します。

ステップ 2　[レポート テンプレート（Report Templates）] タブをクリックします。

ステップ 3　編集するテンプレートの編集アイコン（ ）をクリックします。

代わりに表示アイコン（ ）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 4　次の選択肢があります。

- 改ページを追加します。レポートテンプレートへの改ページの追加 （2785 ページ）を参照してください。
- テキストセクションを追加します。レポートテンプレートへのテキストセクションの追加 （2785 ページ）を参照してください。
- レポート テンプレートの設定 （2782 ページ）の説明に従ってセクション コンテンツを設定します。
- 入力パラメータを作成します。ユーザ定義の入力パラメータの作成 （2791 ページ）を参照してください。
- 入力パラメータを編集します。ユーザ定義の入力パラメータの編集 （2791 ページ）参照してください。
- ドキュメントの属性を編集します。レポートテンプレート内のドキュメント属性の編集 （2793 ページ）を参照してください。
- テンプレートセクションを検索します。レポートテンプレートのセクションの検索 （2788 ページ）を参照してください。

- [詳細設定（Advanced）]をクリックし、レポート テンプレート内のドキュメント属性（2792 ページ）の説明に従ってドキュメント属性を設定します。
- グローバル時間枠を設定します。レポート テンプレートとそのセクションのグローバル時間枠の設定（2786 ページ）を参照してください。
- ローカル時間枠を設定します。レポート テンプレート セクションのローカル時間枠の設定（2787 ページ）を参照してください。
- 検索フィールドを設定します。表形式のセクションに表示される検索フィールドの設定（2784 ページ）参照してください。
- 表とデータ形式を設定します。レポート テンプレート セクションのテーブルとデータ形式の設定（2783 ページ）を参照してください。
- 検索とフィルタを指定します。レポート テンプレート セクションの検索またはフィルタの指定（2784 ページ）を参照してください。

レポート テンプレートのエクスポート

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin

ステップ 1 **[Overview]** > **[Reporting]**を選択します。

ステップ 2 [レポート テンプレート（Report Templates）] タブを選択します。

ステップ 3 エクスポートするテンプレートのエクスポート アイコン（  ）をクリックします。

ステップ 4 [ファイルの保存（Save file）] と [OK] をクリックして、ローカル コンピュータにファイルを保存します。

レポートの生成について

レポートの生成

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Any Security Analyst

レポート テンプレートを作成してカスタマイズすると、レポート生成の準備は完了です。生成プロセスで、レポートの形式（HTML、PDF、または CSV）を選択できます。レポートのグローバル時間枠を調整することもできます。この時間枠は、除外されていないすべてのセクションに一貫したタイム フレームを適用します。

PDF レポートの場合：

- Unicode（UTF-8）文字を使用したファイル名はサポートされません。
- 特殊なUnicodeファイル名が含まれるレポートセクション（ファイルイベントやマルウェアイベントで表示されるセクションなど）では、そのファイル名は書き直された形式で表示されます。
- 各レポートセクションに設定する結果の数は、特定の制限内にする必要があります。この制限を表示するには、レポートテンプレートに表示された黄色の三角形をマウスオーバーします。

レポートテンプレートの検索の指定にユーザ入力パラメータが含まれている場合、生成プロセスで値を入力するよう求められ、このレポートの実行内容がデータのサブセットに合わせて調整されます。

DNS サーバの設定および IP アドレス解決が有効化されている場合、正常に解決されたホスト名がレポートに取り込まれます。

マルチドメイン展開では、先祖ドメインでレポートを生成すると、そのレポートにはすべての子孫ドメインからの結果を含めることができます。特定のリーフ ドメインのレポートを生成するには、そのドメインに切り替えます。

ステップ 1 **[Overview]** > **[Reporting]**を選択します。

ステップ 2 [レポート テンプレート（Report Templates）] タブをクリックします。

ステップ 3 レポートの生成に使用するテンプレートの横にあるレポート アイコン（  ）をクリックします。

コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ヒント 先祖のテンプレートからレポートを生成するには、そのテンプレートを現在のドメインにコピーします。

ステップ 4 必要に応じて、レポート名を設定します。

- 新しい [ファイル名（File Name）] を入力します。新しい名前を入力しないと、システムはレポートテンプレートで指定した名前を使用します。
- 入力パラメータのアイコン（  ）を使用して、1 つ以上の入力パラメータをファイル名に追加します。

ステップ 5 対応するアイコン（HTML、PDF、または CSV）をクリックして、レポートの出力形式を選択します。

PDF オプションがグレー表示されている場合は、1 つ以上のレポート セクションで設定されている結果件数が大きすぎる可能性があります。特定の制限については、レポート テンプレートで黄色の三角形を探して、見つかったらそれにマウス オーバーします。

ステップ 6 グローバル時間枠を変更する場合は、時間枠のアイコン（  ）をクリックします。

（注） グローバル時間枠の設定は、個々のレポート セクションのうちグローバル設定を継承するように設定されているものの内容だけに影響します。

ステップ 7 [入力パラメータ（Input Parameters）] セクションに表示されるフィールドの値を入力します。

ヒント フィールドにワイルドカード文字 * を入力すると、ユーザ パラメータを無視できます。こうすると、検索設定がユーザ パラメータで制約されなくなります。

（注） システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、リテラルの IP アドレスまたは VLAN タグを使用してレポート結果を制約すると、予期しない結果になる可能性があります。

ステップ 8 電子メール リレー ホストを Firepower Management Center 構成で有効化した場合は、[電子メール（Email）] をクリックして、レポートの生成時にレポートが自動的に電子メール配信されるようにします。

ステップ 9 プロンプトが表示されたら、**[生成（Generate）]** をクリックして確認します。

[生成（Generate）] をクリックすると、レポート テンプレートと共に生成設定が保存されます。

[閉じる（Close）] または [キャンセル（Cancel）]をクリックすると、セッション期間中の選択のみが保存されます。

ステップ 10 次の選択肢があります。

- レポート リンクをクリックして、新しいウィンドウにレポートを表示します。
- [OK] をクリックして、レポート テンプレート エディタに戻ります。

レポートの生成オプション

レポートの生成オプションは、以下のように設定できます。

- 1 回のみまたは定期のいずれかの将来のレポート生成をスケジュールします。レポートの生成の自動化（245 ページ）を参照してください。毎日、毎週、毎月など、さまざまな範囲のタイム フレームに基づいたスケジュールでもカスタマイズできます。
- スケジューラを使用してメール レポートを配信します。タスクをスケジュールする**前に**、レポート テンプレートとメール リレー ホストを設定する必要があります。
- レポートを生成すると、そのレポートが受信者リストにメールの添付ファイルとして自動的に送信されます。レポートを電子メールで配信するように、メール リレー ホストを適切に設定する必要があります。
- 新しく生成されたレポート ファイルを、設定されたリモート ストレージの場所に保存します。リモート ストレージを使用するには、まずリモート ストレージの場所を設定します。

（注） リモートに保存してから、ローカル ストレージに切り替えた場合、リモート ストレージ内のレポートは [レポート（Reports）] タブのリストに表示されません。同様に、あるリモート ストレージの場所から別の場所に切り替えた場合、以前の場所にあるレポートはリストに表示されません。

レポートの生成時の電子メール配布

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Any Security Analyst

ステップ 1 **[Overview]** > **[Reporting]** を選択します。

ステップ 2 [レポート テンプレート（Report Templates）] タブをクリックします。

ステップ 3 レポートの生成に使用するテンプレートの横にあるレポート アイコン（  ）をクリックします。

コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ヒント 先祖のテンプレートからレポートを生成するには、そのテンプレートを現在のドメインにコピーします。

ステップ 4 このウィンドウの [電子メール（Email）] セクションを展開します。

ステップ 5 [電子メール オプション（Email Options）] フィールドで、[電子メールの送信（Send Email）] を選択します。

ステップ 6 [受信者リスト（Recipient List）]、[CC] および [BCC] フィールドで、カンマ区切りリストの形式で受信者の電子メール アドレスを入力します。

ステップ 7 [件名（Subject）] フィールドに、電子メールの件名を入力します。

ヒント [件名（Subject）] フィールドやメッセージ本文に入力パラメータを使用して、電子メール内にタイムスタンプや Firepower Management Center の名前などの情報を動的に生成できます。

ステップ 8 必要に応じて、電子メールの本文にカバー レターを入力します。

ステップ 9 [OK] をクリックして確定します。

関連トピック

メール リレー ホストおよび通知アドレスの設定 （1303 ページ）

将来のレポートのスケジュール

レポートの生成の自動化 （245 ページ）を参照してください。

生成されたレポートの操作について

以前に生成されたレポートには、[レポート（Reports）] タブのページからアクセスして操作します。

レポートの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Any Security Analyst

[レポート（Reports）] タブには、以前に生成されたすべてのレポートと、そのレポート名、生成日時、生成したユーザ、そのレポートがローカルに保存されたかリモートに保存されたかが一覧表示されます。ステータスのカラムには、レポートがすでに生成されているか、生成キュー内にある（スケジュール済みタスクの場合など）か、それとも生成できなかった（ディスク領域不足などの理由で）かが示されます。

管理者アクセス権を持つユーザはすべてのレポートを表示でき、その他のユーザは自分が生成したレポートだけを表示できることに注意してください。

マルチドメイン展開では、現在のドメインで作成されたレポートだけを表示できます。

[レポート（Reports）] タブのページには、ローカルに保存されたレポートがすべて示されます。現在リモート ストレージが設定されている場合、リモートに保存されたレポートも示されます。リモートで保存されたレポートの [場所（Location）] カラム データは、「`Remote`」になります。

（注） リモートに保存してから、ローカル ストレージに切り替えた場合、リモート ストレージ内のレポートは [レポート（Reports）] タブのリストに表示されません。同様に、あるリモート ストレージの場所から別の場所に切り替えた場合、以前の場所にあるレポートはリストに表示されません。

ステップ 1 **[Overview]** > **[Reporting]** を選択します。

ステップ 2 [レポート（Reports）] タブをクリックします。

ステップ 3 表示するレポートを選択します。

レポートのダウンロード

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Any Security Analyst

ローカル コンピュータにレポート ファイルをダウンロードできます。そのコンピュータから、電子メールや他の使用可能な方法で電子的に配布できます。

マルチドメイン導入では、現在のドメインで生成されたレポートのみをダウンロードできます。

ステップ 1 **[Overview]** > **[Reporting]**を選択します。

ステップ 2 [レポート（Reports）] タブをクリックします。

ステップ 3 ダウンロードするレポートの横にあるチェック ボックスをオンにして、[ダウンロード（Download）] をクリックします。

ヒント ページ上のすべてのレポートをダウンロードするには、そのページの左上にあるチェック ボックスをオンにします。複数のレポートが複数のページにある場合は、2 つ目のチェック ボックスが表示されます。これをクリックすると、すべてのページ上のすべてのレポートをダウンロードできます。

ステップ 4 ブラウザのプロンプトに従って、レポートをダウンロードします。複数のレポートを選択すると、1 つの `.zip` ファイルでダウンロードされます。

リモートでのレポートの保存

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Any Security Analyst

[概要（Overview）] > [レポート（Reporting）] > [レポート（Reports）] ページの下部に、現在設定されているレポート ストレージの場所が表示され、ローカル、NFS、SMB ストレージの場合はディスク使用率も表示されます。SSH を使用してリモート ストレージにアクセスする場合、ディスク使用率のデータは利用できません。

（注） リモートに保存してから、ローカル ストレージに切り替えた場合、リモート ストレージ内のレポートは [レポート（Reports）] タブのリストに表示されません。同様に、あるリモート ストレージの場所から別の場所に切り替えた場合、以前の場所にあるレポートはリストに表示されません。

始める前に

- リモート ストレージの場所を設定します。詳細については、リモート ストレージ管理 （1283 ページ）を参照してください。

ステップ 1 **[Overview]** > **[Reporting]**を選択します。

ステップ 2 [レポート（Reports）] タブを選択します。

ステップ 3 ページ下部の [レポートのリモート ストレージの有効化（Enable Remote Storage of Reports）] チェック ボックスをオンにします。

次のタスク

- ローカル ストレージからリモート ストレージにレポートを移動します（リモート ストレージへのレポートの移動 （2804 ページ）を参照）。

関連トピック

リモート ストレージ管理 （1283 ページ）
リモート ストレージへのレポートの移動 （2804 ページ）

リモート ストレージへのレポートの移動

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Any Security Analyst

バッチ モードまたは単独で、ローカル ストレージ内のレポートをリモート ストレージの場所に移動できます。

（注） リモートに保存してから、ローカル ストレージに切り替えた場合、リモート ストレージ内のレポートは [レポート（Reports）] タブのリストに表示されません。同様に、あるリモート ストレージの場所から別の場所に切り替えた場合、以前の場所にあるレポートはリストに表示されません。

始める前に

- リモート ストレージの場所を設定します。詳細については、リモート ストレージ管理 （1283 ページ）を参照してください。

ステップ 1 **[Overview]** > **[Reporting]**を選択します。

ステップ 2 [レポート（Reports）] タブを選択します。

ステップ 3 移動するレポートの横にあるチェックボックスをオンにして、[移動（Move）] をクリックします。

ヒント ページ上のすべてのレポートを移動するには、そのページの左上にあるチェックボックスをオンにします。レポートのページが複数にわたる場合は、2つ目のチェックボックスが表示されます。すべてのページのすべてのレポートを移動する場合は、このチェックボックスをオンにします。

ステップ 4 レポートの移動を確認します。

レポートの削除

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Any Security Analyst

レポート ファイルはいつでも削除できます。この手順ではファイルが完全に削除され、リカバリは不可能になります。レポートの生成に使用したレポートテンプレートがまだ残っていますが、時間枠を拡大したりスライドしたりした場合は、特定のレポート ファイルを再生成するのは難しくなることがあります。テンプレートで入力パラメータを使用した場合も、再生成するのが難しくなることがあります。

マルチドメイン導入では、現在のドメインで生成されたレポートのみを削除できます。

ステップ 1 **[Overview]** > **[Reporting]**を選択します。

ステップ 2 [レポート（Reports）] タブをクリックします。

ステップ 3 次の選択肢があります。

- [選択項目の削除（Delete selected）]：削除するレポートの隣のチェック ボックスをオンにしてから、[削除（Delete）] をクリックします。
- [すべて削除（Delete all）]：ページ上のすべてのレポートを削除するには、そのページの左上にあるチェック ボックスをオンにします。複数のレポートが複数のページにある場合は、2 つ目のチェックボックスが表示され、すべてのページ上のすべてのレポートを削除するよう選択できます。

ステップ 4 削除を確認します。

第 113 章

アラート応答による外部アラート

次のトピックでは、アラート応答を使用して Firepower Management Center から外部イベント アラートを送信する方法を示します。

Firepower Management Center アラート応答

SNMP、syslog、または電子メールでの外部イベント通知はクリティカルなシステムのモニタリングに役立ちます。Firepower Management Center はアラート応答を構成して外部サーバと対話します。アラート応答は、電子メール、SNMP、syslog サーバへの接続を表す構成です。これが応答と呼ばれるのは、これを使用して Firepower により検出されたイベントに応答してアラートを送信できるためです。異なるタイプのアラートを異なるモニタリング サーバまたはユーザ（あるいはその両方）に送信するための複数のアラート応答を構成できます。

（注） デバイスおよび Firepower のバージョンによっては、アラート応答は syslog メッセージを送信する最適な方法ではない可能性があります。Syslog について （1385 ページ）およびセキュリティ イベント syslog メッセージングを設定するためのベストプラクティス （2895 ページ）を参照してください。

（注） アラート応答を使用するアラートは、Firepower Management Center によって送信されます。アラート応答を使用しない侵入の電子メール アラートも、Firepower Management Center によって送信されます。対照的に、個別の侵入ルールのトリガーに基づく SNMP および syslog アラートは管理対象デバイスから直接送信されます。詳細については、侵入イベントに関する外部アラート （2817 ページ）を参照してください。

ほとんどの場合、外部アラートに含まれる情報はデータベースにロギングされたいずれかの関連イベントに含まれる情報と同じです。ただし、相関ルールに接続トラッカーが含まれる相関イベントアラートについては、受信する情報はベースのイベントの種類に関係なく、トラフィック プロファイル変更のアラート情報と同じです。

アラート応答の作成や管理は [アラート（Alerts）] ページ（**[Policies]** > **[Actions]** > **[Alerts]**）で行います。新しいアラート応答は自動的に有効になります。アラート応答を削除するのではなく無効にすることで、アラートの生成を一時的に止めることができます。

アラート応答への変更は、接続ログを SNMP トラップまたは syslog サーバに送信する場合を除き、ただちに有効になります。

マルチドメイン展開では、アラート応答を作成すると、作成された応答は現在のドメインに属します。このアラート応答は子孫ドメインでも使用できます。

アラート応答のサポート設定

アラート応答を作成した後、それを使用して、次のような外部アラートを Firepower Management Center から送信できます。

アラート/イベントのタイプ	詳細情報
侵入イベント（インパクト フラグ別）	影響フラグ アラートの設定 （2814 ページ）
検出イベント（タイプ別）	検出イベント アラートの設定 （2815 ページ）
ネットワーク向け AMP（「ネットワークベース」）によって検出されたマルウェアとレトロスペクティブ マルウェア イベント	ネットワーク向け AMP アラートの設定 （2815 ページ）
相関イベント（相関ポリシー違反ごと）	ルールとホワイトリストに応答を追加する （2700 ページ）
相関イベント（ログ ルールまたはデフォルト アクション別）（電子メールアラートのサポートなし）	ログ可能なその他の接続 （3003 ページ）
ヘルス イベント（ヘルス モジュールおよび重大度レベル別）	ヘルス モニタ アラートの作成 （369 ページ）

SNMP アラート応答の作成

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	を除きFTD任意	いずれか（Any）	Admin

SNMPv1、SNMPv2、または SNMPv3 を使用して SNMP アラート応答を作成できます。

（注） SNMP プロトコルの SNMP バージョンを選択する場合、SNMPv2 では読み取り専用コミュニティのみがサポートされ、SNMPv3 では読取り専用ユーザのみがサポートされることに注意してください。SNMPv3 は、AES128 での暗号化をサポートします。

SNMP で 64 ビット値を監視する場合は、SNMPv2 または SNMPv3 を使用する必要があります。SNMPv1 は 64 ビットのモニタリングをサポートしていません。

始める前に

- ネットワーク管理システムで Firepower Management Center の管理情報ベース（MIB）ファイルが必要な場合は、`/etc/sf/DCEALERT.MIB` で取得できます。

ステップ 1 **[Policies]** > **[Actions]** > **[Alerts]**を選択します。

ステップ 2 [アラートの作成（Create Alert）] ドロップダウン メニューから、[SNMP アラートの作成（Create SNMP Alert）] を選択します。

ステップ 3 SNMP 応答を識別する [名前（Name）] を入力します。

ステップ 4 [トラップサーバ（Trap Server）] フィールドに、SNMP トラップ サーバのホスト名または IP アドレスを入力します。

（注） このフィールドに無効な IPv4 アドレス（192.169.1.456 など）を入力した場合でも、システムは警告を**表示しません**。無効なアドレスはホスト名として扱われます。

ステップ 5 [バージョン（Version）] ドロップダウンリストから、使用する SNMP バージョンを選択します。SNMP v3 がデフォルトです。

ステップ 6 使用する SNMP のバージョンに応じて、次のいずれかを実行します。

- [Version 1] または [Version 2]：[Community String] フィールドに読み取り専用の SNMP コミュニティ名を入力してから、手順の最後までスキップします。

  （注） SNMP コミュニティストリング名には、特殊文字（<>/%#&?', etc.）を使用できません。

- SNMP v3 の場合、[ユーザ名（User Name）] フィールドに SNMP サーバで認証するユーザの名前を入力し、次の手順に進みます。

ステップ 7 [認証プロトコル（Authentication Protocol）] ドロップダウンリストから、認証に使用するプロトコルを選択します。

ステップ 8 [認証パスワード（Authentication Password）] フィールドに、SNMP サーバの認証に必要なパスワードを入力します。

ステップ 9 [プライバシー プロトコル（Privacy Protocol）] リストから、[なし（None）] を選択してプライバシー プロトコルを使用しないか、または [DES] を選択してプライバシー プロトコルにデータ暗号規格を使用します。

ステップ 10 [プライバシー パスワード（Privacy Password）] フィールドに、SNMP サーバに必要なプライバシー パスワードを入力します。

ステップ 11 [エンジン ID（Engine ID）] フィールドに、SNMP エンジンの識別子を偶数桁の 16 進表記で入力します。

SNMPv3 を使用する場合、メッセージの符号化には Engine ID 値が使用されます。SNMP サーバでは、メッセージを復号化するためにこの値が必要です。

Firepower Management Center の IP アドレスの 16 進数バージョンを使用することを推奨します。たとえば、Firepower Management Center の IP アドレスが `10.1.1.77` である場合、`0a01014D0` を使用します。

ステップ 12 [保存（Save）] をクリックします。

次のタスク

変更内容は、次の場合を除き、ただちに有効になります。

アラート応答を使って接続ログを送信している場合、これらのアラート応答を編集した後に設定の変更を展開する必要があります。

Syslog アラート応答の作成

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin

syslog アラート応答を設定する際、syslog サーバで確実に正しく処理されるようにするために、syslog メッセージに関連付けられる重大度とファシリティを指定できます。ファシリティはメッセージを作成するサブシステムを示し、重大度はメッセージの重大度を定義します。ファシリティと重大度は syslog に示される実際のメッセージには表示されませんが、syslog メッセージを受信するシステムに対して、メッセージの分類方法を指示するために使用されます。

ヒント syslog の機能とその設定方法の詳細については、ご使用のシステムのマニュアルを参照してください。UNIX システムでは、`syslog` および `syslog.conf` の `man` ページで概念情報および設定手順が説明されています。

syslog アラート応答の作成時に任意のタイプのファシリティを選択できますが、syslog サーバに基づいて意味のあるものを選択する必要があります。すべての syslog サーバがすべてのファシリティをサポートしているわけではありません。UNIX syslog サーバの場合、`syslog.conf` ファイルで、どのファシリティがサーバ上のどのログ ファイルに保存されるかを示す必要があります。

始める前に

- この手順は、多くの場合、syslog メッセージを送信するための推奨される方法ではありません。詳細については、セキュリティ イベント syslog メッセージングを設定するためのベストプラクティス （2895 ページ）を参照してください。
- syslog サーバがリモート メッセージを受け入れられることを確認します。

ステップ 1 **[Policies]** > **[Actions]** > **[Alerts]**を選択します。

ステップ 2 [アラートの作成（Create Alert）] ドロップダウン メニューから、[Syslog アラートの作成（Create Syslog Alert）] を選択します。

ステップ 3 [名前（Name）] にアラートの名前を入力します。

ステップ 4 [ホスト（Host）] フィールドに、syslog サーバのホスト名または IP アドレスを入力します。

（注） このフィールドに無効な IPv4 アドレス（192.168.1.456 など）を入力した場合でも、システムは警告を**表示しません**。無効なアドレスはホスト名として扱われます。

ステップ 5 [ポート（Port）] フィールドに、サーバが syslog メッセージに使用するポートを入力します。この値はデフォルトで 514 です。

ステップ 6 Syslog アラート ファシリティ （2812 ページ）で説明されているとおりに、[ファシリティ（Facility）] リストからファシリティを選択します。

ステップ 7 syslog 重大度レベル （2813 ページ）で説明されているとおりに、[重大度（Severity）] リストから重大度を選択します。

ステップ 8 [タグ（Tag）] フィールドに、syslog メッセージとともに表示するタグ名を入力します。

たとえば、syslog に送信されるすべてのメッセージの前に `FromMC` を付ける場合、このフィールドに `FromMC` と入力します。

ステップ 9 [保存（Save）] をクリックします。

次のタスク

変更内容は、次の場合を除き、ただちに有効になります。

アラート応答を使って syslog サーバに接続ログを送信している場合、これらのアラート応答を編集した後に設定の変更を展開する必要があります。

セキュリティ イベントに対するこのアラート応答を使用する場合は、ポリシーにアラート応答を指定する必要があります。セキュリティ イベントの syslog の設定場所（2895 ページ）を参照してください。

Syslog アラート ファシリティ

次の表に、選択可能な syslog ファシリティを示します。

表 *286 :* 使用可能な *syslog* ファシリティ

ファシリティ	説明
ALERT	アラート メッセージ。
AUDIT	監査サブシステムによって生成されるメッセージ。
AUTH	セキュリティと承認に関連するメッセージ。
AUTHPRIV	セキュリティと承認に関連する制限付きアクセス メッセージ。多くのシステムで、これらのメッセージはセキュア ファイルに転送されます。
CLOCK	クロック デーモンによって生成されるメッセージ。 Windows オペレーティング システムを実行している syslog サーバは CLOCK ファシリティを使用することに注意してください。
CRON	クロック デーモンによって生成されるメッセージ。 Linux オペレーティング システムを実行している syslog サーバは CRON ファシリティを使用することに注意してください。
DAEMON	システム デーモンによって生成されるメッセージ。
FTP	FTP デーモンによって生成されるメッセージ。
KERN	カーネルによって生成されるメッセージ。多くのシステムでは、これらのメッセージは表示されるときにコンソールに出力されます。
LOCAL0-LOCAL7	内部プロセスによって生成されるメッセージ。
LPR	印刷サブシステムによって生成されるメッセージ。
MAIL	メール システムで生成されるメッセージ。
NEWS	ネットワーク ニュース サブシステムによって生成されるメッセージ。

ファシリティ	説明
NTP	NTP デーモンによって生成されるメッセージ。
SYSLOG	syslog デーモンによって生成されるメッセージ。
USER	ユーザ レベルのプロセスによって生成されるメッセージ。
UUCP	UUCP サブシステムによって生成されるメッセージ。

syslog 重大度レベル

次の表に、選択可能な標準の syslog 重大度レベルを示します。

表 *287 : syslog* 重大度レベル

レベル	説明
ALERT	ただちに修正する必要がある状態。
CRIT	クリティカルな状態。
DEBUG	デバッグ情報を含むメッセージ。
EMERG	すべてのユーザに配信されるパニック状態。
ERR	エラー状態。
INFO	情報メッセージです。
NOTICE	エラー状態ではないが、注意が必要な状態。
WARNING	警告メッセージ。

電子メール アラート応答の作成

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin

始める前に

- Firepower Management Center で、自身の IP アドレスを逆解決できることを確認します。

- メール リレー ホストおよび通知アドレスの設定 （1303 ページ）の説明に従って、メール リレー ホストを設定します。

（注） 電子メール アラートを使用して、接続をログに記録することはできません。

ステップ 1 **[Policies]** > **[Actions]** > **[Alerts]**を選択します。

ステップ 2 [アラートの作成（Create Alert）] ドロップダウン メニューから、[電子メール アラートの作成（Create Email Alert）] を選択します。

ステップ 3 [名前（Name）] にアラート応答の名前を入力します。

ステップ 4 [宛先（To）] フィールドに、アラートを送信する電子メール アドレスをカンマで区切って入力します。

ステップ 5 [送信元（From）] フィールドに、アラートの送信者として表示する電子メール アドレスを入力します。

ステップ 6 [リレー ホスト（Relay Host）] の横に表示されるメール サーバが、アラートの送信に使用するサーバであることを確認します。

ヒント 電子メール サーバを変更するには、編集アイコン（）をクリックします。

ステップ 7 **[保存（Save）]** をクリックします。

影響フラグ アラートの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin

特定のインパクト フラグを持つ侵入イベントが発生するたびにアラートが生成されるようにシステムを設定できます。インパクト フラグは、侵入データ、ネットワーク検出データ、および脆弱性情報を関連付けることにより、侵入がネットワークに与える影響を評価するのに役立ちます。

ステップ 1 **[Policies]** > **[Actions]** > **[Alerts]**を選択します。

ステップ 2 [インパクト フラグ アラート（Impact Flag Alerts）] タブをクリックします。

ステップ 3 [アラート（Alerts）] セクションで、各アラート タイプで使用するアラート応答を選択します。

ヒント 新しいアラート応答を作成するには、任意のドロップダウン リストから [新規（New）] を選択します。

ステップ 4 [インパクト設定（Impact Configuration）] セクションで、該当するチェックボックスをオンにして、各インパクト フラグに対して受信するアラートを指定します。

インパクト フラグの定義については、侵入イベント影響レベル （3071 ページ）を参照してください。

ステップ 5 **[保存（Save）]** をクリックします。

検出イベント アラートの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin

特定のタイプの検出イベントが発生するたびにアラートが生成されるようにシステムを設定できます。

始める前に

- ネットワーク検出イベント ロギングの設定 （2671 ページ）の説明に従って、アラートを設定する検出イベント タイプを記録するようにネットワーク検出ポリシーを設定します。

ステップ 1 **[Policies]** > **[Actions]** > **[Alerts]** を選択します。

ステップ 2 [検出イベント アラート（Discovery Event Alerts）] タブをクリックします。

ステップ 3 [アラート（Alerts）] セクションで、各アラート タイプで使用するアラート応答を選択します。

ヒント 新しいアラート応答を作成するには、任意のドロップダウン リストから [新規（New）] を選択します。

ステップ 4 [イベント設定（Events Configuration）] セクションで、各検出イベント タイプに対して、受信するアラートに対応するチェックボックスを選択します。

ステップ 5 **[保存（Save）]** をクリックします。

ネットワーク向け AMP アラートの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス（Access）
マルウェア	マルウェア	いずれか（Any）	いずれか（Any）	Admin

レトロスペクティブインベントなどのマルウェアイベントがネットワーク向けAMPによって生成された（つまり、「ネットワークベースのマルウェアイベント」が生成された）場合は常に通知するようにシステムを設定できます。エンドポイント向け AMP によって生成されたマルウェア イベント（「エンドポイントベースのマルウェア イベント」）にはアラートを生成できません。

始める前に

- マルウェア クラウド ルックアップを実行するファイル ポリシーを設定し、侵入ポリシーとファイル ポリシーを使用したアクセス制御 （1707 ページ）の説明に従って、そのポリシーをアクセス コントロール ルールに関連付けます。

ステップ 1 **[Policies]** > **[Actions]** > **[Alerts]**を選択します。

ステップ 2 [高度なマルウェア保護アラート（Advanced Malware Protections Alerts）] タブをクリックします。

ステップ 3 [アラート（Alerts）] セクションで、各アラート タイプで使用するアラート応答を選択します。

ヒント 新しいアラート応答を作成するには、任意のドロップダウン リストから [新規（New）] を選択します。

ステップ 4 [イベント設定（Event Configuration）] セクションで、各マルウェア イベント タイプに対して、受信するアラートに対応するチェックボックスを選択します。

[すべてのネットワークベースのマルウェア イベント（All network-based malware events）] には [レトロスペクティブ イベント（Retrospective Events）] が含まれることに注意してください。

（定義により、ネットワークベースのマルウェア イベントにはエンドポイント向け AMP によって生成されたイベントは含まれません。）

ステップ 5 **[保存（Save）]** をクリックします。

第 114 章

侵入イベントに関する外部アラート

次のトピックでは、侵入イベントに関する外部アラートを設定する方法について説明します。

侵入イベントの外部アラートについて

外部侵入イベント通知は、クリティカルなシステム モニタリングに役立ちます。

- SNMP：侵入ポリシーごとに設定し、管理対象デバイスが送信します。SNMP アラートは侵入ルールごとに有効にすることができます。
- syslog：侵入ポリシーごとに設定し、管理対象デバイスが送信します。1 つの侵入ポリシーの syslog アラートを有効にすると、ポリシーに含まれるすべてのルールに適用されます。
- 電子メール：すべての侵入ポリシーに設定され、Firepower Management Center が送信します。電子メール アラートは侵入ルールごとに有効にすることができ、長さと頻度を制限することもできます。

侵入イベントの抑制やしきい値を設定すると、システムは、ルールがトリガーされるたびに侵入イベントを生成しなくなる（したがってアラートを送信しなくなる）場合があるのでご注意ください。

マルチドメイン導入環境では、どのドメインでも外部アラートを設定できます。先祖ドメインでは、システムは子孫ドメインの侵入イベントの通知を生成します。

（注） Firepower Management Center も SNMP、syslog、および電子メール アラート応答を使って種々の外部アラートを送信します。Firepower Management Center アラート応答 （2807 ページ）を参照してください。システムは、個々の侵入イベントに対するアラートを送信するためにアラート応答を使用**しません**。

関連トピック

侵入ポリシーの侵入イベント通知のフィルタ （2094 ページ）

侵入イベントの SNMP アラートの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Intrusion Admin

侵入ポリシーで外部 SNMP アラートを有効にした後、トリガー時に SNMP アラートを送信する個々のルールを設定できます。これらのアラートは管理対象デバイスから送信されます。

ステップ 1 侵入ポリシー エディタのナビゲーション ウィンドウで、[詳細設定（Advanced Settings）] をクリックします。

ステップ 2 [SNMP アラート（SNMP Alerting）] が有効になっていることを確認し、[編集（Edit）] をクリックします。ページ下部のメッセージは、設定を含む侵入ポリシー階層を示します。

ステップ 3 SNMP バージョンを選択し、侵入 SNMP アラートのオプション （2818 ページ）の説明に従って構成オプションを指定します。

ステップ 4 ナビゲーション ウィンドウで [ルール（Rules）] をクリックします。

ステップ 5 [ルール（rules）] ペインで、SNMP アラートを設定するルールを選択し、**[アラート（Alerting）] > [SNMP アラートの追加（Add SNMP Alert）]** を選択します。

ステップ 6 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報（Policy Information）] を選択して、[変更を確定（Commit Changes）] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後の変更は破棄されます。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

侵入 SNMP アラートのオプション

ネットワーク管理システムで Management Information Base（MIB）ファイルが必要な場合は、Firepower Management Center の `/etc/sf/DCEALERT.MIB` から取得できます。

SNMP v2 オプション

オプション	説明
Trap Type	アラートに表示される IP アドレスに使用するトラップ タイプ。 ネットワーク管理システムによって INET_IPV4 アドレス タイプが正常にレンダリングされた場合は、[バイナリとして（as Binary）] を選択します。それ以外の場合は、[文字列として（as String）] を選択します。たとえば、HP OpenView では [文字列として（as String）] が必要になります。
Trap Server	SNMP トラップ通知を受信するサーバ。 単一の IP アドレスまたはホスト名を指定できます。
Community String	コミュニティ名。

SNMP v3 オプション

管理対象デバイスは、エンジン ID の値を使用して SNMPv3 アラートをエンコードします。アラートをデコードするには、SNMP サーバにこの値が必要です。この値は、送信デバイスの管理インターフェイスの IP アドレスの 16 進数のバージョンで、「01」が付加されています。

たとえば、SNMP アラートを送信するデバイスの管理インターフェイスの IP アドレスが 172.16.1.50 である場合、エンジン ID の値は 0xAC10013201 です。

オプション	説明
Trap Type	アラートに表示される IP アドレスに使用するトラップ タイプ。 ネットワーク管理システムによって INET_IPV4 アドレス タイプが正常にレンダリングされた場合は、[バイナリとして（as Binary）] を選択します。それ以外の場合は、[文字列として（as String）] を選択します。たとえば、HP OpenView では [文字列として（as String）] が必要になります。
Trap Server	SNMP トラップ通知を受信するサーバ。 単一の IP アドレスまたはホスト名を指定できます。
Authentication Password	認証に必要なパスワード。SNMP v3 は、設定に応じて Message Digest 5（MD5）ハッシュ関数または Secure Hash Algorithm（SHA）ハッシュ関数のいずれかを使用し、このパスワードを暗号化します。 認証パスワードを指定すると、認証が有効になります。

オプション	説明
Private Password	プライバシー用の SNMP キー。SNMP v3 は Data Encryption Standard（DES）ブロック暗号を使用して、このパスワードを暗号化します。SNMP v3 パスワードを入力すると、パスワードは初期設定時にはプレーン テキストで表示されますが、暗号化形式で保存されます。 プライベートパスワードを指定すると、プライバシーが有効になり、認証パスワードも指定する必要があります。
User Name	SNMP ユーザ名。

侵入イベントの Syslog アラートの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Intrusion Admin

侵入ポリシーでsyslogアラートを有効にすると、管理対象デバイス自体または外部ホスト上の syslog にすべての侵入イベントが送信されます。外部ホストを指定した場合、syslog アラートは管理対象デバイスから送信されます。

ステップ 1 侵入ポリシー エディタのナビゲーション ウィンドウで、[詳細設定（Advanced Settings）] をクリックします。

ステップ 2 [Syslog アラート（Syslog Alerting）] が有効になっていることを確認し、[編集（Edit）] をクリックします。ページ下部のメッセージは、設定を含む侵入ポリシー階層を示します。[Syslog アラート（Syslog Alerting）] ページが [詳細設定（Advanced Settings）] ページの下に追加されます。

ステップ 3 syslog アラートを送信するロギング ホストの IP アドレスを入力します。

[ロギング ホスト（Logging Hosts）] フィールドを空白のままにした場合、ロギング ホストの詳細は関連付けられているアクセス制御ポリシーの [ロギング（Logging）] タブから取得されます。

システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。 上書き対応オブジェクトを使用すると、子孫ドメインの管理者は、グローバル コンフィギュレーションを自分のローカル環境に調整できます。

ステップ 4 侵入 syslog アラートの重大度 （2821 ページ）の説明に従って、[ファシリティ（Facility）] と **[重大度（Severity）]** のレベルを選択します。

ステップ 5 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報（Policy Information）] を選択して、[変更を確定（Commit Changes）] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後の変更は破棄されます。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

侵入 syslog アラートの重大度

管理対象デバイスは、特定のファシリティと**重大度**を使用して、侵入イベントをsyslogアラートとして送信できるため、ロギングホストがアラートを分類できます。ファシリティには、それを生成したサブシステムを指定します。これらのファシリティと**重大度**の値は実際の syslog メッセージに表示されません。

ご使用の環境に基づいて意味のある値を選択します。ローカル設定ファイル（UNIX ベースのロギング ホストの syslog.conf など）では、どのログ ファイルにどのファシリティを保存するかを示すことができます。

Syslog アラート ファシリティ

ファシリティ	説明
AUTH	セキュリティと承認に関連するメッセージ。
AUTHPRIV	セキュリティと承認に関連する制限付きアクセス メッセージ。多くのシステムで、これらのメッセージはセキュア ファイルに転送されます。
CRON	クロック デーモンによって生成されるメッセージ。
DAEMON	システム デーモンによって生成されるメッセージ。
FTP	FTP デーモンによって生成されるメッセージ。
KERN	カーネルによって生成されるメッセージ。多くのシステムでは、これらのメッセージは表示されるときにコンソールに出力されます。
LOCAL0-LOCAL7	内部プロセスによって生成されるメッセージ。
LPR	印刷サブシステムによって生成されるメッセージ。
MAIL	メール システムで生成されるメッセージ。
NEWS	ネットワーク ニュース サブシステムによって生成されるメッセージ。
SYSLOG	syslog デーモンによって生成されるメッセージ。
USER	ユーザ レベルのプロセスによって生成されるメッセージ。

ファシリティ	説明
UUCP	UUCP サブシステムによって生成されるメッセージ。

syslog アラートの重大度

レベル	説明
EMERG	すべてのユーザにブロードキャストするパニック状態
ALERT	すぐに修正する必要がある状態
CRIT	重大な状態
ERR	エラー状態
WARNING	警告メッセージ
NOTICE	エラー状態ではないが、注意が必要な状態
INFO	通知メッセージ
DEBUG	デバッグ情報を含むメッセージ

侵入イベントに対する電子メール アラートの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Intrusion Admin

侵入の電子メールアラートを有効にした場合、どの管理対象デバイスまたは侵入ポリシーが侵入を検出したかに関係なく、システムは侵入イベントの生成時に電子メールを送信できます。これらのアラートは Firepower Management Center から送信されます。

始める前に

- 電子メール アラートを受信するようにメール ホストを設定します。メール リレー ホストおよび通知アドレスの設定 （1303 ページ）を参照してください。
- Firepower Management Center が独自の IP アドレスを逆解決できることを確認します。

ステップ 1 **[Policies]** > **[Actions]** > **[Alerts]**を選択します。

ステップ 2 [侵入電子メール（Intrusion Email）] タブをクリックします。

ステップ 3 侵入電子メール アラートのオプション（2823 ページ）の説明に従って、アラートを生成する侵入ルールや侵入グループを含むアラート オプションを選択します。

ステップ 4 **[保存（Save）]** をクリックします。

侵入電子メール アラートのオプション

On/Off

侵入電子メール アラートを有効または無効にします。

（注） 有効にすると、個々のルールが選択されていない限り、すべてのルールのアラートが有効になります。

アドレス送信元/宛先（From/To Addresses）

電子メールの送信者と受信者。受信者のカンマ区切りリストを指定できます。

最大アラート数と頻度（Max Alerts and Frequency）

Firepower Management Center が時間間隔（[頻度（Frequency）]）ごとに送信する電子メール アラートの最大数（[最大アラート数（Max Alerts）]）。

合同アラート（Coalesce Alerts）

同じ送信元 IP とルール ID を持つアラートをグループ化することによって送信されるアラートの数を減らします。

サマリー出力（Summary Output）

テキスト制限されたデバイスに適した短いアラートを有効にします。短いアラートには、以下の情報が含まれています。

- Timestamp
- プロトコル
- 送信元と宛先の IP とポート
- メッセージ
- 同じ送信元 IP に対して生成された侵入イベントの数

例：`2011-05-18 10:35:10 10.1.1.100 icmp 10.10.10.1:8 -> 10.2.1.3:0 snort_decoder: Unknown Datagram decoding problem! (116:108)`

[サマリー出力（Summary Output）] を有効にする場合は、[合同アラート（Coalesce Alerts）] も有効にすることを検討してください。テキストメッセージの制限を超えないように、[最大アラート数（Max Alerts）] を下げることもできます。

タイム ゾーン

アラート タイムスタンプのタイム ゾーン。

特定のルール設定に基づく電子メール警告（Email Alerting on Specific Rules Configuration）

電子メール アラートを設定するルールを選択できます。

第 XXV 部

イベントとアセットの分析ツール

第 115 章

コンテキスト エクスプローラの使用

以下のトピックでは、Firepower システムでコンテキスト エクスプローラを使用する方法について説明します。

コンテキスト エクスプローラについて

Firepower システムの Context Explorer には、モニタ対象ネットワークのステータスに関するコンテキストでの詳細でインタラクティブなグラフィカル情報が表示されます。これには、アプリケーション、アプリケーション統計、接続、位置情報、侵害の兆候、侵入イベント、ホスト、サーバ、セキュリティ インテリジェンス、ユーザ、ファイル（マルウェア ファイルを含む）、関連 URL に関するデータが含まれます。各セクションには、このデータが鮮やかな色の折れ線グラフ、棒グラフ、円グラフ、ドーナツ グラフの形式で表示され、グラフとともに詳しいリストが示されます。1 番目のセクションに表示される時間の経過に伴うトラフィックとイベント数の変化を示した折れ線グラフは、ネットワークのアクティビティにおける最近の傾向の概要を示します。

分析を細かく調整するためのカスタム フィルタを容易に作成および適用できます。またグラフ エリアをクリックするか、カーソルをグラフ エリアに置くことでデータ セクションを詳しく調べることができます。過去 1 時間から過去 1 年までの期間を反映するように Explorer の時間範囲を設定することもできます。Context Explorer にアクセスできるユーザは、管理者、セキュリティ アナリスト、またはセキュリティ アナリスト（読み取り専用）のユーザ ロールが割り当てられているユーザだけです。

Firepower システムのダッシュボードは細かくカスタマイズすることができます。このダッシュボードは区分化されており、リアルタイムで更新されます。一方、Context Explorer は手動で更新され、より幅広いデータのコンテキストを提供することを目的としており、アクティブなユーザ操作のために単一で一貫性のあるレイアウトを備えています。

特定のニーズに基づいてネットワークとアプライアンスのリアルタイムのアクティビティをモニタするには、ダッシュボードを使用します。逆に、詳細かつ明確なコンテキストで事前に定義されている最新のデータセットを調査するには、Context Explorer を使用します。たとえば、ネットワークのホストのうち Linux を使用しているホストは 15% であるが、ほぼすべての YouTube トラフィックはこれらのホストによるものであることが判明した場合、Linux ホストのデータのみを表示するフィルタ、YouTube 関連のアプリケーション データのみを表示するフィルタ、あるいはこの両方のフィルタを簡単に適用できます。コンパクトで対象が絞り込まれているダッシュボードウィジェットとは異なり、Context Explorer の各セクションは、Firepower システムの専門知識を持つユーザと一般的なユーザの両方に役立つ形式で、システムアクティビティを鮮明なビジュアル表現で提供します。

表示されるデータは、管理対象デバイスのライセンスおよび導入状況や、そのデータを提供する機能を設定しているかどうかによって異なります。また、Context Explorer のすべてのセクションで、フィルタを適用して表示するデータを制限することもできます。

マルチドメイン導入では、先祖ドメインで Context Explorer を表示すると、すべてのサブドメインからの集約データが表示されます。リーフ ドメインでは、そのドメインに固有のデータだけを表示できます。

ダッシュボードと Context Explorer の違い

次の表に、ダッシュボードと Context Explorer の主な相違点の要約を示します。

表 *288 :* 比較：ダッシュボードと *Context Explorer*

機能	ダッシュボード	Context Explorer
表示可能なデータ	Firepower システムによってモニタされる任意の対象	アプリケーション、アプリケーション統計、位置情報、ホストの侵害の兆候、侵入イベント、ファイル（マルウェア ファイルを含む）、ホスト、セキュリティ インテリジェンス イベント、サーバ、ユーザ、および URL
カスタマイズ可能かどうか	• ダッシュボードで選択されているウィジェットはカスタマイズ可能です • 個々のウィジェットはさまざまなレベルでカスタマイズ可能です	• 基本レイアウトは変更できません • 適用されたフィルタは Explorer URL に示され、後で使用するためにブックマークできます
データの更新頻度	自動（デフォルト）、ユーザ設定	手動
データのフィルタリング	一部のウィジェットで可能です（ウィジェット設定を編集する必要があります）	Explorer のすべての部分で可能であり、複数フィルタに対応しています

機能	ダッシュボード	Context Explorer
グラフィカル コンテキスト	一部のウィジェット（特に Custom Analysis）では、データをグラフ形式で表示できます。	すべてのデータの豊富なグラフィカル コンテキスト（独自の詳細なドーナツ グラフを含む）
関連 Web インターフェイス ページへのリンク	一部のウィジェット	すべてのセクション
表示データの時間範囲	ユーザ設定	ユーザ設定

関連トピック

ダッシュボードについて （321 ページ）

[時系列のトラフィックおよび侵入イベント数（TrafficandIntrusionEvent Counts Time）] グラフ

Context Explorer の上部には、時間の経過に伴うトラフィックおよび侵入イベント数の変化を示す折れ線グラフが表示されます。X 軸は時間間隔を示します（選択されている時間枠に応じて、5 分～ 1 か月）。Y 軸は、KB 単位のトラフィック（青色の線）と侵入イベント数（赤色の線）を示します。

X 軸の最小間隔が 5 分であることに注意してください。これに対応するため、選択された時間範囲の開始点と終了点が、システムにより、最も近い 5 分間間隔に調整されます。

デフォルトでは、このセクションには選択された時間範囲のすべてのネットワーク トラフィックおよび生成されたすべての侵入イベントが示されます。フィルタを適用すると、フィルタに指定されている条件に関連するトラフィックおよび侵入イベントだけがグラフに表示されます。たとえば、[OS Name] に `Windows` を指定してフィルタリングすると、時間グラフには Windows オペレーティング システムを使用するホストに関連するトラフィックとイベントだけが表示されます。

侵入イベント データ（[Priority] が`High` に設定されたものなど）に基づいて Context Explorer をフィルタリングすると、青色のトラフィックを示す線が非表示になり、侵入イベントだけに集中することができます。

トラフィックおよびイベント数に関する正確な情報を確認するには、グラフ線上の任意のポイントにポインタを置きます。色付きの線の 1 つにポインタを置くと、その線がグラフの前面に移動し、コンテキストがより明確になります。

このセクションのデータは、主に [侵入イベント（Intrusion Events）] テーブルと [接続イベント（Connection Events）] テーブルから取得されます。

[侵害の兆候（Indications of Compromise）] セクション

コンテキスト エクスプローラの [侵害の兆候（IOC）（Indications of Compromise (IOC)）] セクションには、モニタ対象ネットワーク上でセキュリティが侵害されている可能性があるホスト

の概要を示す 2 つのインタライクティブ セクション（トリガーとして使用された主な IOC 種類の割合のビューと、トリガーとして使用された兆候の数をホストごとに表したビュー）が表示されます。

IOC に関する詳細については、侵害の兆候データ （3221 ページ）を参照してください。

[兆候別ホスト（Hosts by Indication）] グラフ

[兆候別ホスト（Hosts by Indication）] グラフはドーナツ形式であり、モニタ対象ネットワーク上のホストでトリガーとして使用された侵害の兆候（IOC）を割合で表示します。内側のリングは IOC カテゴリ（`CnC Connected` や `Malware Detected` など）ごとに分割されており、外側のリングではそれがさらに具体的なイベントの種類（`Impact 2 Intrusion Event — attempted-admin` や `Threat Detected in File Transfer` など）ごとに分割されています。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタリングまたはドリルダウンされます。

このグラフのデータは主に [ホスト（Hosts）] テーブルと [ホスト侵害の兆候（Indications of Compromise）] テーブルから取得されます。

[ホスト別兆候（Indications by Host）] グラフ

[ホスト別兆候（Indications by Host）] グラフは棒グラフ形式であり、モニタ対象ネットワーク上の最も IOC が顕著な 15 のホストでトリガーとして使用された固有の侵害の兆候（IOC）の数を表示します。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタリングまたはドリルダウンされます。

このグラフのデータは主に [ホスト（Hosts）] テーブルと [ホスト侵害の兆候（Indications of Compromise）] テーブルから取得されます。

[ネットワーク情報（Network Information）] セクション

Context Explorer の [ネットワーク情報（Network Information）] セクションには、モニタ対象ネットワーク上の接続トラフィックの全体の概要（トラフィックに関連付けられている送信元、宛先、ユーザ、およびセキュリティ ゾーン、ネットワーク上のホストで使用されているオペレーティング システムの内訳、Firepower システムがネットワーク トラフィックに対して実行したアクセス制御アクションの割合のビュー）を示す 6 つのインタラクティブ グラフが含まれています。

[オペレーティング システム（Operating Systems）] グラフ

[オペレーティング システム（Operating Systems）] グラフはドーナツ グラフ形式で、モニタ対象ネットワークのホストで検出されたオペレーティング システムを割合で表示します。内側のリングは OS 名（`Windows` や `Linux` など）ごとに分割され、外側のリングではそのデータがさらにオペレーティング システムのバージョン（`Windows Server 2008` や `Linux 11.x` など）ごとに分割されています。密接に関連するいくつかのオペレーティング システム（Windows 2000、

Windows XP、Windows Server 2003 など）は 1 つにまとめられます。ごく少数の認識されないオペレーティング システムは [Other] にまとめられます。

このグラフは日時制約に関係なく、使用可能なすべてのデータを反映することに注意してください。Explorer の時間範囲を変更しても、グラフは変化しません。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタリングまたはドリルダウンされます。

このグラフのデータは、主に [ホスト（Hosts）] テーブルから取得されます。

[送信元 IP 別トラフィック（Traffic by Source IP）] グラフ

[送信元 IP 別トラフィック（Traffic by Source IP）] グラフは棒グラフ形式で、モニタ対象ネットワーク上の最もアクティブな上位 15 の送信元 IP アドレスのネットワーク トラフィック カウント（KB/秒）と固有接続数を表示します。リストされた送信元IPアドレスごとに、青色の棒はトラフィック データ、赤色の棒は接続データを示します。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタリングまたはドリルダウンされます。

（注） 侵入イベントの情報でフィルタリングすると、[Traffic by Source IP] グラフは非表示になります。

このグラフのデータは、主に [接続イベント（Connection Events）] テーブルから取得されます。

[送信元ユーザ別トラフィック（Traffic by Source User）] グラフ

[送信元ユーザ別トラフィック（Traffic by Source User）] グラフは棒グラフ形式で、モニタ対象ネットワーク上の最もアクティブな上位 15 の送信元ユーザのネットワーク トラフィック カウント（KB/秒）と固有接続数を表示します。リストされた送信元IPアドレスごとに、青色の棒はトラフィック データ、赤色の棒は接続データを示します。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタリングまたはドリルダウンされます。

（注） 侵入イベントの情報でフィルタリングすると、[Traffic by Source User] グラフは非表示になります。

このグラフのデータは主に [接続イベント（Connection Events）] テーブルから取得されます。このグラフには、権限のあるユーザのデータが表示されます。

[アクセス コントロール アクション別の接続（Connections by Access Control Action）] グラフ

[アクセス コントロール アクション別の接続（Connections by Access Control Action）] グラフは円グラフ形式であり、Firepower システム導入でモニタ対象トラフィックに対して実行されたアクセス制御アクション（[ブロック（Block）] や [許可（Allow）] など）の割合のビューを表示します。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタリングまたはドリルダウンされます。

（注） 侵入イベントの情報でフィルタリングすると、[Traffic by Source User] グラフは非表示になります。

このグラフのデータは主に [接続イベント（Connection Events）] テーブルから取得されます。

[宛先 IP 別トラフィック（Traffic by Destination IP）] グラフ

[宛先 IP 別トラフィック（Traffic by Destination IP）] グラフは棒グラフ形式で、モニタ対象ネットワーク上の最もアクティブな上位 15 の宛先 IP アドレスのネットワーク トラフィック カウント（KB/秒）と固有接続数を表示します。リストされた宛先IPアドレスごとに、青色の棒はトラフィック データ、赤色の棒は接続データを示します。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタリングまたはドリルダウンされます。

（注） 侵入イベントの情報でフィルタリングすると、[Traffic by Destination IP] グラフは非表示になります。

このグラフのデータは、主に [接続イベント（Connection Events）] テーブルから取得されます。

[入力/出力のセキュリティ ゾーン別トラフィック（TrafficbyIngress/EgressSecurityZone）] グラフ

[入力/出力のセキュリティ ゾーン別トラフィック（Traffic by Ingress/Egress Security Zone）] グラフは棒グラフ形式で、モニタ対象ネットワークで設定されているセキュリティ ゾーンごとに、その着信/発信ネットワーク トラフィック カウント（KB/秒）および固有接続数を表示します。必要に応じて、このグラフに入力（デフォルト）セキュリティ ゾーン情報または出力セキュリティ ゾーン情報のいずれかを表示するように設定できます。

リストされたセキュリティ ゾーンごとに、青色の棒はトラフィック データ、赤色の棒は接続データを示します。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタリングまたはドリルダウンされます。

ヒント　グラフに制約を適用して、出力セキュリティゾーンのトラフィックだけが表示されるようにするには、グラフにポインタを置き、表示されるトグルボタンの [Egress] をクリックします。デフォルト ビューに戻すには [Ingress] をクリックします。Context Explorer から外部へ移動することでも、グラフがデフォルトの [Ingress] ビューに戻ることに注意してください。

（注）　侵入イベントの情報でフィルタリングすると、[Traffic by Ingress/Egress Security Zone] グラフは非表示になります。

このグラフのデータは、主に [接続イベント（Connection Events）] テーブルから取得されます。

[アプリケーション情報（Information）] セクション

Context Explorer の [アプリケーション情報（Information）] セクションには、3 つのインタラクティブ グラフと 1 つの表形式リストが表示されます。これらのグラフとリストは、モニタ対象ネットワーク上でのアプリケーションアクティビティの概要（アプリケーションに関連するトラフィック、侵入イベント、およびホストを、各アプリケーションに割り当てられている推定リスクまたは推定ビジネス関連度ごとに編成したもの）を示します。[Application Details List] は、各アプリケーションとそのリスク、ビジネス関連度、カテゴリ、およびホスト数を示すインタラクティブなリストです。

このセクションのすべての「アプリケーション」インスタンスについて、[Application Information] のグラフのセットは、デフォルトでは特にアプリケーション プロトコル（DNS、SSH など）を検査します。クライアント アプリケーション（PuTTY や Firefox など）や Web アプリケーション（Facebook や Pandora など）を特に検査するように [アプリケーション情報（Application Information）] セクションを設定することもできます。

[アプリケーション情報（Application Information）] セクションへのフォーカスの移動

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
機能に応じて異なる	機能に応じて異なる	いずれか（Any）	いずれか（Any）	Admin/Any Security Analyst

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

ステップ 1　**[Analysis]** > **[Context Explorer]** を選択します。

ステップ 2　[アプリケーション プロトコル情報（Application Protocol Information）] セクションにポインタを重ねます。

（注） 以前に同じContext Explorerセッションでこの設定を変更している場合は、セクションタイトルが [クライアント アプリケーション情報（Client Application Information）] または [Web アプリケーション情報（Web Application Information）] と表示されることがある点に注意してください。

ステップ 3 [アプリケーション プロトコル（Application Protocol）]、[クライアント アプリケーション（Client Application）]、または [Web アプリケーション（Web Application）] をクリックします。

[リスク/ビジネスとの関連性とアプリケーション別トラフィック（TrafficbyRisk/Business Relevance and Application）] グラフ

[リスク/ビジネスとの関連性とアプリケーション別トラフィック（Traffic by Risk/Business Relevance and Application）] グラフはドーナツ形式で、モニタ対象ネットワークで検出されたアプリケーショントラフィックを、アプリケーションの推定リスク（デフォルト）または推定のビジネスとの関連性（ビジネス関連度）ごとの割合で表示します。内側のリングは推定リスク/ビジネス関連度レベル（`Medium` または `High` など）ごとに分割され、外側のリングではそのデータがさらに具体的なアプリケーション（`SSH` または `NetBIOS` など）ごとに分割されます。稀に検出されるアプリケーションは [Other] にまとめられます。

このグラフは日時制約に関係なく、使用可能なすべてのデータを反映することに注意してください。Explorer の時間範囲を変更しても、グラフは変化しません。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタリングまたはドリルダウンされます。

ヒント グラフに制約を適用して、ビジネス関連度とアプリケーションごとにトラフィックが表示されるようにするには、グラフにポインタを置き、表示されるトグルボタンの [Business Relevance] をクリックします。デフォルト ビューに戻すには [Risk] をクリックします。Context Explorer から外部へ移動することでも、グラフがデフォルトの [Risk] ビューに戻ることに注意してください。

（注） 侵入イベントの情報でフィルタリングすると、[Traffic by Risk/Business and Application] グラフは非表示になります。

このグラフのデータは、主に [接続イベント（Connection Events）] テーブルと [アプリケーション統計（Application Statistics）] テーブルから取得されます。

[リスク/ビジネスとの関連度別侵入イベントおよびアプリケーション（IntrusionEventsby Risk/Business Relevance and Application）] グラフ

[リスク/ビジネスとの関連度別侵入イベントおよびアプリケーション（Intrusion Events by Risk/Business Relevance and Application）] グラフはドーナツ形式であり、モニタ対象ネットワークで検出された侵入イベントと、これらのイベントに関連するアプリケーションを、アプリ

ケーションの推定リスク（デフォルト）または推定ビジネス関連度ごとの割合で表示します。内側のリングは推定リスク/ビジネス関連度レベル（Medium または High など）ごとに分割され、外側のリングではそのデータがさらに具体的なアプリケーション（SSH または NetBIOS など）ごとに分割されます。稀に検出されるアプリケーションは [Other] にまとめられます。

ドーナツ グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタリングまたはドリルダウンされるか、または（該当する場合には）アプリケーション情報が表示されます。

ヒント グラフに制約を適用して、ビジネス関連度とアプリケーションごとに侵入イベントが表示されるようにするには、グラフにポインタを置き、表示されるトグルボタンの [Business Relevance] をクリックします。デフォルト ビューに戻すには [Risk] をクリックします。Context Explorer から外部へ移動することでも、グラフがデフォルトの [Risk] ビューに戻ることに注意してください。

このグラフのデータは主に [侵入イベント（Intrusion Events）] テーブルと [アプリケーションの統計（Application Statistics）] テーブルから取得されます。

[リスク/ビジネスとの関連度別ホストおよびアプリケーション（Hosts by Risk/Business Relevance and Application）] グラフ

[リスク/ビジネスとの関連度別ホストおよびアプリケーション（Hosts by Risk/Business Relevance and Application）] グラフはドーナツ形式であり、モニタ対象ネットワークで検出されたホストと、これらのホストに関連するアプリケーションを、アプリケーションの推定リスク（デフォルト）または推定ビジネス関連度ごとの割合で表示します。内側のリングは推定リスク/ビジネス関連度レベル（Medium または High など）ごとに分割され、外側のリングではそのデータがさらに具体的なアプリケーション（SSH または NetBIOS など）ごとに分割されます。非常に少数のアプリケーションは [Other] にまとめられます。

ドーナツ グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタリングまたはドリルダウンされます。

ヒント グラフに制約を適用して、ビジネス関連度とアプリケーションに基づいてホストが表示されるようにするには、グラフにポインタを置き、表示されるトグル ボタンの [Business Relevance] をクリックします。デフォルト ビューに戻すには [Risk] をクリックします。Context Explorer から外部へ移動することでも、グラフがデフォルトの [Risk] ビューに戻ることに注意してください。

このグラフのデータは主に [アプリケーション（Applications）] テーブルから取得されます。

アプリケーション詳細リスト

[アプリケーション情報（Application Information）] セクション下部に表示される [アプリケーション詳細リスト（Application Details List）] は、モニタ対象ネットワークで検出される各アプ

リケーションの推定リスク、推定ビジネス関連度、カテゴリ、ホスト数の情報を示す表です。アプリケーションは、関連ホスト数の降順でリストされます。

[Application Details List] 表はソートできませんが、表の項目をクリックして、その情報でフィルタリングまたはドリルダウンしたり、（該当する場合に）アプリケーション情報を表示したりすることができます。この表のデータは主に [Applications] 表から取得されます。

このリストは日時制約に関係なく、使用可能なすべてのデータを反映することに注意してください。Explorer の時間範囲を変更しても、リストは変化しません。

[セキュリティ インテリジェンス（Security Intelligence）] セクション

Context Explorer の [セキュリティ インテリジェンス（Security Intelligence）] セクションには、3 つのインタラクティブな棒グラフが表示されます。これらのグラフには、モニタ対象ネットワーク上の、ブラックリストに登録されているトラフィック、または Security Intelligence によってモニタされているトラフィックの全体の概要が示されます。これらのグラフでは、カテゴリ、送信元 IP アドレス、および宛先 IP アドレスに基づいてそれらのトラフィックがソートされ、トラフィックの量（KB/秒）と該当する接続の数の両方が表示されます。

[カテゴリ別セキュリティ インテリジェンス トラフィック（Security Intelligence Traffic by Category）] グラフ

[カテゴリ別セキュリティ インテリジェンス トラフィック（Security Intelligence Traffic by Category）] グラフは棒グラフ形式で、モニタ対象ネットワーク上のトラフィックのセキュリティインテリジェンスの上位のカテゴリに関する、ネットワーク トラフィック カウント（KB/秒）と固有接続数を表示します。リストされたカテゴリごとに、青色の棒はトラフィック データ、赤色の棒は接続データを示します。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でドリルダウンされます。

（注） 侵入イベントの情報でフィルタリングすると、[Security Intelligence Traffic by Category] グラフは非表示になります。

このグラフのデータは主に [セキュリティ インテリジェンス イベント（Security Intelligence Events）] テーブルから取得されます。

[送信元 IP 別セキュリティ インテリジェンス トラフィック（Security Intelligence Traffic by Source IP）] グラフ

[送信元 IP 別セキュリティ インテリジェンス トラフィック（Security Intelligence Traffic by Source IP）] グラフは棒グラフ形式で、モニタ対象ネットワーク上でセキュリティ インテリジェンスによってモニタされたトラフィックの上位の送信元 IP アドレスに関する、ネットワーク トラフィック カウント（KB/秒）と固有接続数を表示します。リストされたカテゴリごとに、青色の棒はトラフィック データ、赤色の棒は接続データを示します。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でドリルダウンされます。

（注） 侵入イベントの情報でフィルタリングすると、[Security Intelligence Traffic by Source IP] グラフは非表示になります。

このグラフのデータは主に [セキュリティ インテリジェンス イベント（Security Intelligence Events）] テーブルから取得されます。

[宛先 IP 別セキュリティ インテリジェンス トラフィック（Security Intelligence Traffic by Destination IP）] グラフ

[宛先 IP 別セキュリティ インテリジェンス トラフィック（Security Intelligence Traffic by Destination IP）] グラフは棒グラフ形式で、モニタ対象ネットワーク上でセキュリティ インテリジェンスによってモニタされたトラフィックの上位の宛先 IP アドレスに関する、ネットワーク トラフィック カウント（KB/秒）と固有接続数を表示します。リストされたカテゴリごとに、青色の棒はトラフィック データ、赤色の棒は接続データを示します。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でドリルダウンされます。

（注） 侵入イベントの情報でフィルタリングすると、[Security Intelligence Traffic by Destination IP] グラフは非表示になります。

このグラフのデータは主に [セキュリティ インテリジェンス イベント（Security Intelligence Events）] テーブルから取得されます。

[侵入情報（Intrusion Information）] セクション

Context Explorer の [侵入情報（Intrusion Information）] セクションには 6 つのインタラクティブ グラフと 1 つの表形式リストが表示されます。これらのグラフとリストは、モニタ対象ネットワークの侵入イベントの概要（侵入イベントに関連付けられている影響レベル、攻撃元、攻撃対象先、ユーザ、優先レベル、およびセキュリティ ゾーンと、侵入イベントの分類、優先度、カウントを示す詳細なリスト）を示します。

[影響別侵入イベント（Intrusion Events by Impact）] グラフ

[影響別侵入イベント（Intrusion Events by Impact）] グラフは円グラフ形式であり、モニタ対象ネットワークの侵入イベントを推定影響レベル（0～4）のグループごとの割合で表示します。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタリングまたはドリルダウンされます。

このグラフのデータは、主に侵入検知（[IDS統計（IDS Statistics）] テーブル）および [侵入イベント（Intrusion Events）] テーブルから取得されます。

[上位の攻撃者（Top Attackers）] グラフ

[上位の攻撃者（Top Attackers）] グラフは棒グラフ形式で、モニタ対象ネットワーク上の（侵入イベントを発生させた）上位の各攻撃元ホストIPアドレスの侵入イベント数を表示します。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタリングまたはドリルダウンされます。

このグラフのデータは、主に [侵入イベント（Intrusion Events）] テーブルから取得されます。

[上位のユーザ（Top Users）] グラフ

[上位のユーザ（Top Users）] グラフは棒グラフ形式で、モニタ対象ネットワーク上の最大侵入イベント数に関連付けられたユーザと、イベント数を表示します。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタリングまたはドリルダウンされます。

このグラフのデータは、主に侵入検知（IDS）の [ユーザ統計（User Statistics）] テーブルおよび [侵入イベント（Intrusion Events）] テーブルから取得されます。このグラフには、権限のあるユーザのデータが表示されます。

[優先度別侵入イベント（Intrusion Events by Priority）] グラフ

[優先度別侵入イベント（Intrusion Events by Priority）] グラフは円グラフ形式であり、モニタ対象ネットワークの侵入イベントを、推定優先度レベル（[高（High）]、[中（Medium）]、[低（Low）] など）のグループごとの割合で表示します。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタリングまたはドリルダウンされます。

このグラフのデータは、主に [侵入イベント（Intrusion Events）] テーブルから取得されます。

[上位のターゲット（Top Targets）] グラフ

[上位のターゲット（Top Targets）] グラフは棒グラフ形式で、モニタ対象ネットワーク上の（侵入イベントを発生させた接続で攻撃対象となった）上位のターゲットホスト（攻撃対象ホスト）のIPアドレスの侵入イベント数を表示します。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタリングまたはドリルダウンされます。

このグラフのデータは、主に [侵入イベント（Intrusion Events）] テーブルから取得されます。

[入力/出力の上位セキュリティ ゾーン（Top Ingress/Egress Security Zones）] グラフ

[入力/出力の上位セキュリティ ゾーン（Top Ingress/Egress Security Zones）] グラフは棒グラフ形式で、モニタ対象ネットワーク上で設定されている各セキュリティゾーン（グラフ設定に応じて入力または出力）に関連付けられている侵入イベントの数を表示します。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタリングまたはドリルダウンされます。

ヒント　グラフに制約を適用して、出力セキュリティゾーンのトラフィックだけが表示されるようにするには、グラフにポインタを置き、表示されるトグルボタンの [Egress] をクリックします。デフォルト ビューに戻すには [Ingress] をクリックします。Context Explorer から外部へ移動することでも、グラフがデフォルトの [Ingress] ビューに戻ることに注意してください。

このグラフのデータは主に [Intrusion Events] 表から取得されます。

このグラフは、必要に応じて、入力（デフォルト）セキュリティゾーン情報または出力セキュリティ ゾーン情報のいずれかを表示するように設定できます。

侵入イベント詳細リスト

[侵入情報（Intrusion Information）] セクション下部に表示される [イベント詳細リスト（Event Details List）] は、モニタ対象ネットワークで検出された各侵入イベントの分類、推定優先度、イベント数の情報を示すテーブルです。イベントは、イベント数の降順でリストされます。

[Event Details List] 表はソートできませんが、表の項目をクリックして、その情報でフィルタリングまたはドリルダウンすることができます。このテーブルのデータは主に [侵入イベント（Intrusion Events）] テーブルから取得されます。

[ファイル情報（Files Information）] セクション

Context Explorer の [ファイル情報（Files Information）] セクションには、6 つのインタラクティブ グラフが表示されます。これらのグラフは、モニタ対象ネットワーク上のファイルとマルウェア イベントの概要を示します。

このうち 5 つのグラフには、（以前は AMP for Firepower と呼ばれていた）ネットワーク向け AMP に関連するデータ（ネットワーク トラフィックで検出されたファイルのファイル タイプ、ファイル名、マルウェアの性質、これらのファイルを送信（アップロード）および受信（ダウンロード）したホスト）が表示されます。最後のグラフには、ネットワーク向け AMP または AMP for Endpoints のどちらで検出されたかにかかわらず、組織内で検出されたすべてのマルウェア脅威が表示されます。

（注）　侵入情報でフィルタリングすると、[ファイル情報（File Information）] セクション全体が非表示になります。

[上位のファイル タイプ（Top File Types）] グラフ

[上位のファイル タイプ（Top File Types）] グラフはドーナツ グラフ形式で、ネットワーク トラフィックで検出されたファイル タイプの割合のビュー（外側のリング）と、ファイル カテゴリのグループごとの割合のビュー（内側のリング）を表示します。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタリングまたはドリルダウンされます。

このグラフに ネットワーク向け AMP データを表示するには、マルウェア ライセンスが必要であることに注意してください。

このグラフのデータは主に [ファイル イベント（File Events）] 表から取得されます。

[上位のファイル名（Top File Names）] グラフ

[上位のファイル名（Top File Names）] グラフは棒グラフ形式で、ネットワーク トラフィックで検出された上位の一意のファイル名の数を表示します。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタリングまたはドリルダウンされます。

このグラフに ネットワーク向け AMP データを表示するには、マルウェア ライセンスが必要であることに注意してください。

このグラフのデータは主に [ファイル イベント（File Events）] 表から取得されます。

[性質別ファイル（Files by Disposition）] グラフ

[上位のファイル タイプ（Top File Types）] グラフは円グラフ形式であり、（以前は AMP for Firepower と呼ばれていた）ネットワーク向け AMP 機能で検出されたファイルのマルウェアの性質の割合のビューを表示します。Firepower Management Center がマルウェア クラウド検索を行ったファイルにのみ性質が設定されることに注意してください。クラウド検索をトリガーしなかったファイルには、`N/A` という性質が設定されます。`Unavailable` という性質は、Firepower Management Center がマルウェア クラウド検索を実行できなかったことを示します。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタリングまたはドリルダウンされます。

このグラフに ネットワーク向け AMP データを表示するには、マルウェア ライセンスが必要であることに注意してください。

このグラフのデータは主に [ファイル イベント（File Events）] 表から取得されます。

[送信ファイル数上位のホスト（Top Hosts Receiving Files）] グラフ

[送信ファイル数上位のホスト（Top Hosts Receiving Files）] グラフは棒グラフ形式で、ネットワーク トラフィックで検出された、送信ファイル数上位のホストの IP アドレスに関するファイルの数を表示します。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタリングまたはドリルダウンされます。

ヒント　グラフに制約を適用して、マルウェアを送信するホストだけが表示されるようにするには、グラフにポインタを置き、表示されるトグル ボタンの [Malware] をクリックします。デフォルトのファイルのビューに戻すには [Files] をクリックします。Context Explorer から外部への移動でも、グラフがデフォルトのファイルのビューに戻ることに注意してください。

このグラフに ネットワーク向け AMP データを表示するには、マルウェア ライセンスが必要であることに注意してください。

このグラフのデータは主に [ファイル イベント（File Events）] 表から取得されます。

[受信ファイル数上位のホスト（Top Hosts Receiving Files）] グラフ

[受信ファイル数上位のホスト（Top Hosts Receiving Files）] グラフは棒グラフ形式で、ネットワーク トラフィックで検出された、受信ファイル数上位のホストの IP アドレスに関するファイルの数を表示します。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタリングまたはドリルダウンされます。

ヒント　グラフに制約を適用して、マルウェアを受信するホストだけが表示されるようにするには、グラフにポインタを置き、表示されるトグル ボタンの [Malware] をクリックします。デフォルトのファイルのビューに戻すには [Files] をクリックします。Context Explorer から外部への移動でも、グラフがデフォルトのファイルのビューに戻ることに注意してください。

このグラフに ネットワーク向け AMP データを表示するには、マルウェア ライセンスが必要であることに注意してください。

このグラフのデータは主に [ファイル イベント（File Events）] 表から取得されます。

[上位のマルウェア検出（Top Malware Detections）] グラフ

[上位のマルウェア検出（Top Malware Detections）] グラフは棒グラフ形式で、ネットワーク向け AMP と AMP for Endpoints のいずれによるものかに関係なく、組織で検出された上位のマルウェア脅威の数を表示します。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタリングまたはドリルダウンされます。

このグラフに ネットワーク向け AMP データを表示するには、マルウェア ライセンスが必要であることに注意してください。

このグラフのデータは主に [ファイル イベント（File Events）] 表と [マルウェア イベント（Malware Events）] 表から取得されます。

[地理位置情報（Geolocation Information）] セクション

Context Explorer の [地理位置情報（Geolocation Information）] セクションには、3 つのインタラクティブなドーナツ グラフが表示されます。これらのグラフは、モニタ対象ネットワークのホストがデータを交換している国の概要（イニシエータ国またはレスポンダ国ごとの固有接続数、送信元または宛先の国ごとの侵入イベント数、および送信側または受信側の国ごとのファイル イベント数）を示します。

[イニシエータ/レスポンダの国別接続（Connections by Initiator/Responder Country）] グラフの表示

[イニシエータ/レスポンダの国別接続（Connections by Initiator/Responder Country）] グラフはドーナツ グラフ形式であり、ネットワーク上での接続にイニシエータ（デフォルト）またはレスポンダとして関わる国の割合のビューを表示します。内側のリングでは、これらの国が大陸別にグループ化されています。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタリングまたはドリルダウンされます。

ヒント　グラフに制約を適用して、接続でレスポンダとなっている国だけが表示されるようにするには、グラフにポインタを置き、表示されるトグル ボタンの [Responder] をクリックします。デフォルト ビューに戻すには [Initiator] をクリックします。Context Explorer から外部へ移動することでも、グラフがデフォルトの[Initiator] ビューに戻ることに注意してください。

このグラフのデータは主に [接続サマリー データ（Connection Summary Data）] テーブルから取得されます。

[送信元/宛先国別侵入イベント（Intrusion Events by Source/Destination Country）] グラフ

[送信元/宛先国別侵入イベント（Intrusion Events by Source/Destination Country）] グラフはドーナツ グラフ形式であり、ネットワーク上の侵入イベントにイベントの送信元（デフォルト）または宛先として関わる国の割合を表示します。内側のリングでは、これらの国が大陸別にグループ化されています。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタリングまたはドリルダウンされます。

ヒント　グラフに制約を適用して、侵入イベントの宛先となっている国だけが表示されるようにするには、グラフにポインタを置き、表示されるトグル ボタンの [Destination] をクリックします。デフォルト ビューに戻すには [Source] をクリックします。Context Explorer から外部へ移動することでも、グラフがデフォルトの [Source] ビューに戻ることに注意してください。

このグラフのデータは主に [侵入イベント（Intrusion Events）] テーブルから取得されます。

[送信側/受信側の国別ファイル イベント（File Events by Sending/Receiving Country）] グラフ

[送信側/受信側の国別ファイル イベント（File Events by Sending/Receiving Country）] グラフはドーナツ グラフ形式であり、ネットワーク上のファイルイベントでファイルの送信側（デフォルト）または受信側として検出された国の割合のビューを表示します。内側のリングでは、これらの国が大陸別にグループ化されています。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタリングまたはドリルダウンされます。

ヒント　グラフに制約を適用して、ファイルを受信する国だけが表示されるようにするには、グラフにポインタを置き、表示されるトグル ボタンの [Receiver] をクリックします。デフォルト ビューに戻すには [Sender] をクリックします。Context Explorer から外部へ移動することでも、グラフがデフォルトの [Sender] ビューに戻ることに注意してください。

このグラフのデータは主に [ファイル イベント（File Events）] テーブルから取得されます。

[URL 情報（URL Information）] セクション

Context Explorer の [URL 情報（URL Information）] セクションには、3 つのインタラクティブな棒グラフが表示されます。これらのグラフには、モニタ対象ネットワーク上のホストがデータを交換するために使用する URL の全体の概要（URL に関連付けられているトラフィックと固有接続数を個々の URL、URL カテゴリ、および URL レピュテーションでソートしたもの）が示されます。URL 情報でフィルタリングすることはできません。

（注）　侵入イベントの情報でフィルタ処理を実行すると、[URL 情報（URL Information）] セクション全体が非表示になります。

このグラフで URL カテゴリとレピュテーション データを含めるには、URL フィルタリング ライセンスを所有している必要があることに注意してください。

[URL 別トラフィック（Traffic by URL）] グラフ

[URL 別トラフィック（Traffic by URL）] グラフは棒グラフ形式で、モニタ対象ネットワーク上の最も要求される上位 15 の URL のネットワーク トラフィック カウント（KB/秒）と固有接続数を表示します。リストされた URL ごとに、青色の棒はトラフィック データ、赤色の棒は接続データを示します。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でドリルダウンされます。

（注） 侵入イベントの情報でフィルタ処理を実行すると、[URL 別トラフィック（Traffic by URL）] グラフは非表示になります。

このグラフでURLカテゴリとレピュテーションデータを含めるには、URLフィルタリング ライセンスを所有している必要があることに注意してください。

このグラフのデータは、主に[接続イベント（Connection Events）]テーブルから取得されます。

[URL カテゴリ別トラフィック（Traffic by URL Category）] グラフ

[URL カテゴリ別トラフィック（Traffic by URL Category）] グラフは棒グラフ形式で、モニタ対象ネットワーク上の最も要求される URL カテゴリ（`Search Engines` や `Streaming Media` など）のネットワーク トラフィック カウント（KB/秒）と固有接続数を表示します。リストされたURLカテゴリごとに、青色の棒はトラフィック データ、赤色の棒は接続データを示します。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でドリルダウンされます。

（注） 侵入イベントの情報でフィルタ処理を実行すると、[URL カテゴリ別トラフィック（Traffic by URL Category）] グラフは非表示になります。

このグラフでURLカテゴリとレピュテーションデータを含めるには、URLフィルタリング ライセンスを所有している必要があることに注意してください。

このグラフのデータは、主に[URL 統計（URL Statistics）]テーブルと[接続イベント（Connection Events）] テーブルから取得されます。

[URL レピュテーション別トラフィック（Traffic by URL Reputation）] グラフ

[URLレピュテーション別のトラフィック（Traffic by URL Reputation）] グラフは棒グラフ形式であり、モニタ対象ネットワーク上の最も要求される URL レピュテーション グループ（Well knownまたは Benign sites with security risks）のネットワーク トラフィック カウント（KB/秒）および固有接続数を表示します。リストされた URL レピュテーションごとに、青色の棒はトラフィック データ、赤色の棒は接続データを示します。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でドリルダウンされます。

（注） 侵入イベントの情報でフィルタ処理を実行すると、[URL レピュテーション別トラフィック（Traffic by URL Reputation）] グラフは非表示になります。

このグラフでURLカテゴリとレピュテーションデータを含めるには、URLフィルタリング ライセンスを所有している必要があることに注意してください。

このグラフのデータは、主に [URL 統計（URL Statistics）] テーブルと [接続イベント（Connection Events）] テーブルから取得されます。

Context Explorer の更新

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
機能に応じて異なる	機能に応じて異なる	いずれか（Any）	いずれか（Any）	Admin/Any Security Analyst

Context Explorer は、表示している情報を自動的に更新しません。新しいデータを組み込むには、Explorer を手動で更新する必要があります。

Context Explorer 自体をリロードすると（ブラウザ プログラムの更新または Context Explorer から外部へ移動した後に戻る操作など）、すべての表示情報が更新されますが、セクション設定（Ingress/Egress グラフや [アプリケーション情報（Application Information）] セクションなど）に対して行った変更は保持されず、また、読み込みに時間がかかることがある点に注意してください。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

ステップ 1 **[Analysis]** > **[Context Explorer]** を選択します。

ステップ 2 右上にある [リロード（Reload）] をクリックします。

[リロード（Reload）] ボタンは、更新が終了するまでグレー表示になります。

Context Explorer の時間範囲の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
機能に応じて異なる	機能に応じて異なる	いずれか（Any）	いずれか（Any）	Admin/Any Security Analyst

過去 1 時間（デフォルト）から過去 1 年までの期間を反映するように、Context Explorer の時間範囲を設定できます。時間範囲を変更しても、Context Explorer は変更を反映するために自動的に更新されないことに注意してください。新しい時間範囲を適用するには、Explorer を手動で更新する必要があります。

時間範囲の変更は、Context Explorer から外部に移動したり、ログイン セッションを終了したりしても維持されます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

ステップ 1 **[Analysis]** > **[Context Explorer]**を選択します。

ステップ 2 [リストを表示（Show the last）] ドロップダウンリストから、時間範囲を選択します。

ステップ 3 オプションで、新しい時間範囲のデータを表示するには、[リロード（Reload）] をクリックします。

ヒント [フィルタの適用（Apply Filters）] をクリックすると、時間範囲の更新が適用されます。

Context Explorer のセクションの最小化および最大化

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
機能に応じて異なる	機能に応じて異なる	いずれか（Any）	いずれか（Any）	Admin/Any Security Analyst

Context Explorer では 1 つ以上のセクションを最小化して非表示にできます。これは、特定のセクションだけを強調する場合や、ビューをシンプルにしたい場合に便利です。[トラフィックおよび侵入イベント数/時間（Traffic and Intrusion Event Counts Time）] グラフは最小化できません。

Context Explorer のセクションでは、ページを更新したり、アプライアンスからログアウトしたりしても、設定した最小化または最大化の状態が維持されます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

ステップ 1 **[Analysis]** > **[Context Explorer]**を選択します。

ステップ 2 セクションを最小化するには、セクションのタイトル バーにある最小化アイコン（ー）をクリックします。

ステップ 3 セクションを最大化するには、最小化されたセクションのタイトルバーにある最大化アイコン（□）をクリックします。

Context Explorer データのドリルダウン

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
機能に応じて異なる	機能に応じて異なる	いずれか（Any）	いずれか（Any）	Admin/Any Security Analyst

Context Explorer で許容されている詳細レベルよりもさらに詳細にグラフを調べたりデータをリストしたりするには、当該データのテーブル ビューにドリルダウンします。（[Traffic and Intrusion Events over Time] グラフではドリル ダウンできないことに注意してください）。たとえば、[Traffic by Source IP] グラフの IP アドレスでドリルダウンすると、[Connection Events] 表の [Connections with Application Details] ビューが表示されます。このビューには、選択した送信元 IP アドレスに関連するデータのみが表示されます。

調べるデータのタイプに応じて、コンテキスト メニューに追加のオプションが表示されることがあります。特定の IP アドレスに関連付けられているデータ ポイントの場合、選択した IP アドレスのホストまたは whois 情報を表示するためのオプションが表示されます。特定のアプリケーションに関連付けられているデータ ポイントの場合、選択したアプリケーションに関するアプリケーション情報を表示するためのオプションが表示されます。特定のユーザに関連付けられているデータ ポイントの場合、ユーザのユーザ プロファイル ページを表示するためのオプションが表示されます。侵入イベントのメッセージに関連付けられているデータ ポイントの場合、そのイベントに関連する侵入ルールに関するルール ドキュメントを表示するオプションが表示されます。特定の IP アドレスに関連付けられているデータ ポイントの場合、そのアドレスをブラックリストまたはホワイトリストに追加するためのオプションが表示されます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

ステップ 1 **[Analysis]** > **[Context Explorer]**を選択します。

ステップ 2 [一定期間のトラフィックおよび侵入イベント（Traffic and Intrusion Events over Time）] 以外の任意のセクションで、調査するデータ ポイントをクリックします。

ステップ 3 選択するデータ ポイントに応じて、表示されるオプションが異なります。

- テーブル ビューでこのデータの詳細を表示するには、[詳細な分析を表示（Drill into Analysis）] を選択します。
- 特定の IP アドレスに関連付けられているデータ ポイントを選択している場合に、関連するホストに関する詳細情報を参照するには、[ホスト情報の表示（View Host Information）] を選択します。
- 特定の IP アドレスのデータ ポイントを選択している場合に、そのアドレスで whois 検索を行うには、[Whois] を選択します。
- 特定のアプリケーションに関連付けられているデータ ポイントを選択している場合に、そのアプリケーションに関する詳細情報を参照するには、[アプリケーション情報の表示（View Application Information）] を選択します。

- 特定のユーザに関連付けられているデータ ポイントを選択している場合に、そのユーザに関する詳細情報を参照するには、[ユーザ情報の表示（View User Information）] を選択します。
- 特定の侵入イベント メッセージに関連付けらているデータ ポイントを選択している場合に、関連する侵入ルールに関する詳細情報を参照するには、[ルール ドキュメントの表示（View Rule Documentation）] を選択します。次に、必要に応じて、[ルール ドキュメント（Rule Documentation）] をクリックしてより具体的なルールの詳細を表示します。
- 特定の IP アドレスに関連付けられているデータ ポイントを選択している場合に、Security Intelligence グローバル ブラックリストまたはホワイトリストにその IP アドレスを追加するには、[今すぐブラックリストに追加（Blacklist Now）] または [今すぐホワイトリストに追加（Whitelist Now）] のいずれか該当するオプションを選択します。

コンテキスト エクスプローラのフィルタ

コンテキスト エクスプローラに最初に表示される基本的で広範なデータをフィルタリングして、ネットワーク上のアクティビティのより詳細な状況を把握することができます。フィルタは URL 情報以外のすべての種類の Firepower システム データに対応し、除外と包含がサポートされており、Context Explorer のグラフ データ ポイントをクリックするだけですぐに適用でき、Explorer 全体に反映されます。一度に最大 20 のフィルタを適用できます。

コンテキスト エクスプローラ データにフィルタを追加する方法はいくつかあります。

- [フィルタの追加（Add Filter）] ダイアログを使用する。
- コンテキスト メニューを使用する（エクスプローラのデータ ポイントを選択する場合）。
- 特定の詳細表示ページ（[アプリケーションの詳細（Application Detail）]、[ホスト プロファイル（Host Profile）]、[ルールの詳細（Rule Detail）]、[ユーザ プロファイル（User Profile）]）に表示されるテキスト リンクを使用する。これらのリンクをクリックすると、コンテキスト エクスプローラが自動的に開き、詳細表示ページの当該データに基づいてコンテキスト エクスプローラがフィルタリングされます。たとえば、ユーザ `jenkins` のユーザ詳細ページで [コンテキスト エクスプローラ（Context Explorer）] リンクをクリックすると、エクスプローラにはそのユーザに関連するデータだけが表示されます。

ファイル タイプの中には、相互に互換性がないタイプがあります。たとえば、侵入イベント関連のフィルタ（**Device** や **Inline Result** など）を、接続イベント関連フィルタ（**Access Control Action** など）と同時に適用することはできません。これは、システムでは接続イベント データを侵入イベント データによってソートできないためです。互換性のないフィルタの同時適用はシステムによって自動的に防止されます。互換性の問題が存在する場合、より後に適用された方のフィルタ タイプと互換性のないタイプのフィルタは非表示になります。

複数のフィルタがアクティブな場合、同じデータ タイプの値は OR 検索条件として扱われます。つまり、いずれか 1 つの値と一致するデータがすべて表示されます。異なるデータ タイプの値は AND 検索条件として扱われます。つまり、データは各フィルタ データ タイプの 1 つ以上の値と一致する必要があります。たとえば、`Application: 2channel`、`Application: Reddit`、および `User: edickinson` というフィルタ セットで表示されるデータは、ユーザ `edickinson` に

関連付けられており、**かつ**アプリケーション `2channel` **または**アプリケーション `Reddit` に関連付けられている必要があります。

マルチドメイン展開では、先祖ドメインでコンテキストエクスプローラを表示している場合に複数の子孫ドメインでフィルタリングできます。この場合、**IP Address** フィルタも追加する場合は注意してください。システムは、各リーフ ドメインに個別のネットワーク マップを作成します。実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。

表示されるデータは、管理対象デバイスのライセンスおよび展開方法やデータを提供する機能を設定するかどうかなどの要因によって異なります。

（注） フィルタは、必要とする正確な Firepower データ コンテキストをいつでも取得できるシンプルかつ俊敏性に優れたツールとして機能します。永続的に設定するものではなく、コンテキストエクスプローラから外部に移動するか、セッションを終了すると消去されます。後で使用するためにフィルタ設定を保存するには、フィルタ処理されたコンテキストエクスプローラ ビューの保存 （2854 ページ）を参照してください。

データ タイプ フィールド オプション

次の表に、フィルタとして使用できるデータ タイプと、各データ タイプの例と説明を示します。

表 *289 :* フィルタ データ タイプ

タイプ	値の例	定義
Access Control Action	`Allow`、`Block`	トラフィックを許可またはブロックするためにアクセス コントロール ポリシーにより実行されるアクション。
アプリケーション カテゴリ（Application Category）	`web browser`、`email`	アプリケーションの主要機能の一般的な分類。
アプリケーション	`Facebook`、`HTTP`	アプリケーションの名前。
アプリケーションのリスク（Application Risk）	`Very High`、`Medium`	アプリケーションの推定セキュリティ リスク。
アプリケーションタグ（Application Tag）	`encrypts communications`、`sends mail`	アプリケーションに関する追加情報。アプリケーションには任意の数のタグを使用できます（タグを使用しないことも可能です）。

タイプ	値の例	定義
アプリケーション タイプ（Application Type）	`Client`、`Web Application`	アプリケーションタイプ（アプリケーションプロトコル、クライアント、または Web アプリケーション）。
ビジネスとの関連性（Business Relevance）	`Very Low`、`High`	（娯楽ではない）ビジネスアクティビティに対するアプリケーションの推定関連度。
大陸（Continent）	`North America`、`Asia`	モニタ対象ネットワークで検出されたルーティング可能なIPアドレスに関連付けられている大陸。
国（Country）	`Canada`、`Japan`	モニタ対象ネットワークで検出されたルーティング可能なIPアドレスに関連付けられている国。
Device	`device1.example.com`、`192.168.1.3`	モニタ対象ネットワーク上のデバイスの名前または IP アドレス。
ドメイン（Domain）	`Asia Division`、`Europe Division`	グラフ表示するネットワーク アクティビティを行うデバイスのドメイン。このデータ タイプはマルチドメイン展開の場合にのみ存在します。
イベントの分類（Event Classification）	`Potential Corporate Policy Violation`、`Attempted Denial of Service`	侵入イベントの簡単な説明。侵入イベントをトリガーしたルール、デコーダ、またはプリプロセッサにより決定されます。
イベント メッセージ（Event Message）	`dns response`、`P2P`	イベントによって生成されるメッセージ。イベントをトリガーしたルール、デコーダ、またはプリプロセッサにより決定されます。
ファイル傾向（File Disposition）	`Malware`、`Clean`	Firepower Management Center によるマルウェア クラウド検索の実行対象ファイルの性質。
ファイル名	`Packages.bz2`	ネットワーク トラフィックで検出されたファイルの名前。
ファイル SHA256（File SHA256）	任意の 32 ビット文字列	Firepower Management Center によるマルウェア クラウド検索の実行対象ファイルの SHA-256 ハッシュ値。

タイプ	値の例	定義
ファイル タイプ（File Type）	GZ、SWF、MOV	ネットワーク トラフィックで検出されたファイルのタイプ。
ファイル タイプ カテゴリ（File Type Category）	Archive、Multimedia、Executables	ネットワーク トラフィックで検出されたファイルのタイプの一般カテゴリ。
[IPアドレス（IP Address）]	192.168.1.3、2001:0db8:85a3::0000/24	IPv4 または IPv6 のアドレス、アドレス範囲、またはアドレス ブロック。 IP アドレスを検索すると、そのアドレスが送信元または宛先のいずれかになっているイベントが返されることに注意してください。
影響レベル（Impact Level）	Impact Level 1、Impact Level 2	モニタ対象ネットワークでのイベントの推定影響レベル。
インライン結果（Inline Result）	dropped、would have dropped	トラフィックがドロップされたか、ドロップされた可能性があるか、またはシステムによりトラフィックが処理されていないかのいずれかです。
IOC カテゴリ（IOC Category）	High Impact Attack、Malware Detected	トリガーとして使用された侵害の兆候（IOC）イベントのカテゴリ。
IOC イベント タイプ（IOC Event Type）	exploit-kit、malware-backdoor	特定の侵害の兆候（IOC）に関連付けられている ID。その兆候をトリガーしたイベントを示します。
マルウェア脅威名（Malware Threat Name）	W32.Trojan.a6b1	マルウェア脅威の名前。
OS 名（OS Name）	Windows、Linux	オペレーティング システムの名前。
OS Version	XP、2.6	オペレーティング システムの特定のバージョン。
[プライオリティ（Priority）]	high、low	イベントの推定緊急度。
セキュリティ インテリジェンス カテゴリ（Security Intelligence Category）	Malware、Spam	セキュリティ インテリジェンスにより判別される危険なトラフィックのカテゴリ。
セキュリティ ゾーン	My Security Zone、Security Zone X	トラフィックが分析されたインターフェイスのセット。インライン展開の場合は、トラフィックが通過するインターフェイスのセット。

タイプ	値の例	定義
SSL	`yes`、`no`	SSL暗号化トラフィックまたはTLS暗号化トラフィック。
ユーザ（User）	`wsmith`、`mtwain`	モニタ対象ネットワーク上のホストにログインしたユーザの ID。

[フィルタの追加（Add Filter）] ウィンドウからのフィルタの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
機能に応じて異なる	機能に応じて異なる	いずれか（Any）	いずれか（Any）	Admin/Any Security Analyst

この手順を使用して、[フィルタの追加（Add Filter）] ウィンドウでフィルタを最初から作成します。（コンテキストメニューを使用して、クイック フィルタを作成することもできます。）

Context Explorer の左上にある [フィルタ（Filters）] の下のプラス アイコン（＋）をクリックすると表示される [フィルタの追加（Add Filter）] ウィンドウには、次の 2 つのフィールドだけが表示されます。

- [データ タイプ（Data Type）] ドロップダウンリストには、Context Explorer に制約を適用するために使用できる多数の Firepower システム データ タイプが含まれています。データ タイプの選択後に、そのタイプの固有の値を [フィルタ（Filter）] フィールドに入力します（たとえば、[大陸（Continent）] タイプの場合は値 [アジア（Asia）] など）。ユーザ支援のため、[Filter] フィールドでは、選択したデータ タイプのさまざまな値の例がグレー表示で示されます。（フィールドにデータを入力すると、これらは消去されます。）
- [フィルタ（Filter）] フィールドには、イベント検索と同様に、* や ! などの特殊検索パラメータを入力できます。フィルタ パラメータの前に ! 記号を付けることで排他的なフィルタを作成できます。

（注） 追加したフィルタは自動的には適用されません。Context Explorer でフィルタを表示するには、[フィルタの適用（Apply Filters）] をクリックする必要があります。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

ステップ 1 **[Analysis]** > **[Context Explorer]** を選択します。

ステップ 2 左上にある [フィルタ（Filter）] の下で、プラス アイコン（＋）をクリックします。

ステップ 3 [データ タイプ（Data Type）] ドロップダウンリストから、フィルタリングの条件として使用するデータ タイプを選択します。

ステップ 4 [フィルタ（Filter）] フィールドに、フィルタリングの条件として使用するデータ タイプ値を入力します。

ステップ 5 [OK] をクリックします。

ステップ 6 オプションで、前述の手順を繰り返し、必要なフィルタ セットが設定されるまで、フィルタを追加します。

ステップ 7 [フィルタの適用（Apply Filters）] をクリックします。

関連トピック

データ タイプ フィールド オプション （2849 ページ）
検索の制約 （2968 ページ）

コンテキスト メニューからのクイック フィルタの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
機能に応じて異なる	機能に応じて異なる	いずれか（Any）	いずれか（Any）	Admin/Any Security Analyst

Context Explorer のグラフとリスト データを詳しく調べるときに、データ ポイントをクリックし、コンテキストメニューを使用してそのデータに基づいてフィルタ（包含または除外）を簡単に作成できます。コンテキスト メニューを使用して、Application、User、または Intrusion Event Message データ タイプの情報、あるいは任意の個別ホストでフィルタリングする場合、フィルタ ウィジェットには、そのデータ タイプの該当する詳細ページ（アプリケーションデータの場合は [Application Detail] など）にリンクするウィジェット情報アイコンが表示されます。URL データではフィルタリングできないことに注意してください。

特定のグラフまたはリストのデータを詳しく調査する場合にもコンテキスト メニューを使用できます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

ステップ 1 **[Analysis]** > **[Context Explorer]**を選択します。

ステップ 2 [一定期間のトラフィックおよび侵入イベント（Traffic and Intrusion Events over Time）] セクションと URL データを含むセクション以外の Explorer セクションで、フィルタリングするデータ ポイントをクリックします。

ステップ 3 次の 2 つの対処法があります。

- このデータにフィルタを追加するには、[フィルタの追加（Add Filter）] をクリックします。

- このデータに除外フィルタを追加するには、[除外フィルタの追加（Add Exclude Filter）] をクリックします。このフィルタが適用されると、除外された値に関連付けられて**いない**すべてのデータが表示されます。除外フィルタでは、フィルタ値の前に感嘆符（!）が表示されます。

フィルタ処理されたコンテキスト エクスプローラ ビューの保存

コンテキストエクスプローラから外部に移動した後、またはセッションを終了した後に、コンテキストエクスプローラのフィルタ設定を保持するには、適切なフィルタを適用したコンテキスト エクスプローラのブラウザ ブックマークを作成します。適用されるフィルタはコンテキスト エクスプローラ ページ URL に組み込まれているので、そのページのブックマークを読み込むと、対応するフィルタも読み込まれます。

適切なフィルタが適用されたコンテキスト エクスプ ローラーのブラウザ ブックマークを作成します。

フィルタ データの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
機能に応じて異なる	機能に応じて異なる	いずれか（Any）	いずれか（Any）	Admin/Any Security Analyst

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

ステップ 1 **[Analysis]** > **[Context Explorer]** を選択します。

ステップ 2 該当するフィルタ ウィジェットの情報アイコン（  ）をクリックします。

フィルタの削除

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
機能に応じて異なる	機能に応じて異なる	いずれか（Any）	いずれか（Any）	Admin/Any Security Analyst

ステップ 1 **[Analysis]** > **[Context Explorer]** を選択します。

ステップ 2 左上の [フィルタ（Filters）] の下で、任意のフィルタ ウィジェットのクリア アイコン（ ）をクリックします。

ヒント すべてのフィルタを一括削除するには、[クリア（Clear）] ボタンをクリックします。

第 116 章

ネットワーク マップの使用

ここでは、ネットワーク マップの使用方法について説明します。

ネットワーク マップ

Firepowerシステムは、ネットワークを通じて送信されるトラフィックをモニタし、トラフィック データを復号化してから、設定されているオペレーティング システムおよびフィンガープリントとそのデータを比較します。このシステムでは、次にそのデータを使用して、ネットワーク マップというネットワークの詳細な表示を生成します。マルチドメイン展開では、システムはリーフ ドメインごとの個々のネットワーク マップを生成します。

システムは、ネットワーク検出ポリシーのモニタリングで特定された管理対象デバイスからデータを収集します。管理対象デバイスでは、モニタされたトラフィックから直接ネットワーク アセットを検出したり、処理された NetFlow レコードから間接的にネットワーク アセットを検出したりします。複数のデバイスで同じネットワーク アセットを検出した場合、システムではそれらの情報をまとめてそのアセットの複合表示を生成します。

パッシブ検出からのデータを補完するには、次のようにします。

- オープンソースの Nmap™ スキャナを使用してホストをアクティブにスキャンして、そのスキャン結果をネットワーク マップに追加します。
- ホスト入力機能を使用して、サードパーティ製のアプリケーションからホストデータを手動で追加できます。

ネットワーク マップには、検出されたホストとネットワーク デバイスの観点から見たネットワーク トポロジが表示されます。

ネットワーク マップを使用すれば、次のことを行えます。

- ネットワークの全体的なビューを即座に入手できます。

- 実行する分析に適したさまざまなビューを選択できます。ネットワーク マップの各ビューの形式は、展開可能なカテゴリおよびサブカテゴリを持つ階層ツリーからなる、同一の形式です。カテゴリをクリックすると、展開して、その下のサブカテゴリが表示されます。
- カスタム トポロジ機能を使用してサブネットを整理して識別できます。たとえば、組織の各部署が異なるサブネットを使用している場合、カスタム トポロジ機能を使用して、それらのサブネットに分かりやすいラベルを割り当てることができます。
- 任意のモニタ対象ホストのホスト プロファイルにドリルダウンすれば、詳細情報を表示できます。
- アセットの調査が不要になった場合は、そのアセットを削除できます。

（注） システムは、ネットワーク マップから削除されたホストに関連付けられているアクティビティを検出した場合、そのホストをネットワーク マップに再度追加します。同様に、削除されたアプリケーションは、システムでアプリケーションの変更（たとえば、Apache Web サーバが新しいバージョンにアップグレードされた場合）を検出すると、ネットワーク マップに再度追加されます。システムが特定のホストを脆弱にする変更を検出した場合、それらのホストの脆弱性が再びアクティブにされます。

ヒント ネットワーク マップからホストまたはサブネットを永続的に除外するには、ネットワーク検出ポリシーを変更します。ロード バランサおよび NAT デバイスで過剰なイベントまたは無関係なイベントを生成していることが判明した場合は、それらのデバイスをモニタリングから除外することができます。

関連トピック

ネットワーク検出ポリシーの設定 （2649 ページ）

ホスト ネットワーク マップ

[ホスト（Hosts）] タブのネットワーク マップには、ホスト数と、ホストの IP アドレスと プライマリ MAC アドレスのリストが表示されます。各アドレスまたはアドレスの一部は、次のレベルへのリンクです。このネットワーク マップ ビューは、ホストに 1 つの IP アドレスまたは複数の IP アドレスがあるかを問わず、システムによって検出されたすべての一意のホスト数を表示します。

ホストのネットワーク マップを使用して、サブネットによって階層ツリーに整理されたネットワークのホストを参照でき、特定のホストのホスト プロファイルにドリルダウンできます。

システムは、エクスポートされた NetFlow レコードからネットワーク マップにホストを追加できますが、これらのホストに使用できる情報は限られます（NetFlow データと管理対象デバイス データの違い （2478 ページ）を参照）。

ネットワークのカスタム トポロジを作成して、サブネットに意味のあるラベル（部門名など）を割り当てることができます。これはホストのネットワーク マップで表示されます。また、カスタム トポロジで指定した組織に基づいてホストのネットワーク マップを表示することもできます。

ホストのネットワーク マップからネットワーク全体、サブネット、または個々のホストを削除できます。ホストがネットワークに接続されていないことがわかっている場合など、分析を効率化するために削除できます。システムは削除されたホストに関連付けられたアクティビティを後で検出すると、ネットワーク マップにホストを再追加します。ネットワーク マップからホストまたはサブネットを永続的に除外するには、ネットワーク検出ポリシーを変更します。

⚠

注意 ネットワーク デバイスをネットワーク マップから削除しないでください。システムがネットワーク トポロジを判断するために必要です。

ホストのネットワーク マップのページではプライマリ MAC アドレスのみを検索でき、ホストの [MAC] カウンタにはプライマリ MAC アドレスのみが含まれます。プライマリおよびセカンダリ MAC アドレスの説明については、ホスト プロファイルの基本ホスト情報（3161 ページ）を参照してください。

ネットワーク デバイスのネットワーク マップ

[ネットワーク デバイス（Network Devices）] タブのネットワーク マップには、ネットワークの 1 つのセグメントを別のセグメントに接続するネットワーク デバイス（ブリッジ、ルータ、NAT デバイス、およびロード バランサ）が表示されます。このマップには、IP アドレスで特定されたデバイスと、MAC アドレスで特定されたデバイスがリストされる 2 つのセクションがあります。

また、このマップには、デバイスに保持されている IP アドレスが 1 つか複数かに関係なく、システムによって検出されたすべての一意のネットワーク デバイスの数も表示されます。

ネットワークのカスタム トポロジを作成した場合、サブネットに割り当てられているラベルがネットワーク デバイスのネットワーク マップに表示されます。

ネットワーク デバイスを区別するためにシステムでは次の方法を使用します。

- Cisco Discovery Protocol（CDP）メッセージの分析。ネットワーク デバイスと種類を特定します（シスコ デバイスのみ）。
- スパニング ツリー プロトコル（STP）の検出。デバイスをスイッチまたはブリッジとして識別します。
- 同じ MAC アドレスを使用している複数のホストの検出。MAC アドレスを、ルータに属しているものとして識別します。
- クライアント側からの TTL 値の変更、または通常のブート時間よりも頻繁に変更されている TTL 値の検出。この検出では、NAT デバイスとロード バランサを識別します。

ネットワーク デバイスが CDP を使用して通信している場合、1 つ以上の IP アドレスを持っている可能性があります。ネットワーク デバイスが STP を使用して通信している場合は、1 つの MAC アドレスのみを保持している可能性があります。

ネットワーク デバイスをネットワーク マップから削除することはできません。これは、システムでそれらの場所を使用してネットワーク トポロジを判断するためです。

ネットワーク デバイスのホスト プロファイルには、[オペレーティング システム（Operating Systems）] セクションではなく [システム（Systems）] セクションがあります。このセクションには、ネットワーク デバイスの背後で検出されたモバイル デバイスすべてのハードウェア プラットフォームが反映された [ハードウェア（Hardware）] 列が含まれています。[システム（Systems）] の下にハードウェア プラットフォームの値が表示され場合、システムは、ネットワーク デバイスの背後で 1 つ以上のモバイル デバイスが検出されたことを示しています。モバイル デバイスはハードウェア プラットフォームの情報を持っていることも、持っていないこともありますが、モバイル デバイスではないシステムではハードウェア プラットフォーム情報は検出されないことに注意してください。

モバイル デバイスのネットワーク マップ

[モバイル デバイス（Mobile Devices）] タブのネットワーク マップには、ネットワークに接続されているモバイル デバイスが表示されます。また、このネットワーク マップには、デバイスに設定されている IP アドレスが 1 つか複数かに関係なく、システムによって検出されたすべての一意のモバイル デバイスの数も表示されます。

各アドレスまたはアドレスの一部分は、次のレベルへのリンクです。また、サブネットまたは IP アドレスを削除することもできます。そして、システムでそのデバイスを再検出すると、そのデバイスをネットワーク マップに再度追加します。

さらに、ドリルダウンしてモバイル デバイスのホスト プロファイルを表示することもできます。

モバイル デバイスを特定するために、システムでは次のことを行います。

- モバイル デバイスのモバイル ブラウザからの HTTP トラフィック内のユーザ エージェントの文字列を分析します。
- 特定のモバイル アプリケーションの HTTP トラフィックをモニタします。

ネットワークのカスタム トポロジを作成した場合、サブネットに割り当てられているラベルがモバイル デバイスのネットワーク マップに表示されます。

侵害の兆候のネットワーク マップ

[侵害の兆候（Indications of Compromise）] タブのネットワーク マップには、ネットワーク上で侵害されたホストが IOS カテゴリ別に編成されて表示されます。影響を受けているホストは各カテゴリの下に表示されます。各アドレスまたはアドレスの一部は、次のレベルへのリンクです。

[侵害の兆候（Indications of Compromise）] タブのネットワーク マップから、何らかのセキュリティ侵害を受けたと判断される各ホストのホストプロファイルを表示できます。さらに、IOC カテゴリまたは特定のホストを削除でき（解決済みにする）、これによって当該ホストから IOC タグが削除されます。たとえば、問題が対応済みで、繰り返し発生する可能性が低いと判断した場合に、IOC カテゴリをネットワーク マップから削除できます。

ネットワーク マップのホストや IOC カテゴリを解決済みにしても、ネットワークからは削除されません。システムがその IOC をトリガーする情報を新たに検出すると、解決済みのホストまたは IOC カテゴリはネットワーク マップに再表示されます。

侵害の兆候をシステムがどのように判断しているかの詳細については、侵害の兆候データ （3221 ページ）とサブトピックを参照してください。

アプリケーション プロトコルのネットワーク マップ

[アプリケーション プロトコル（Application Protocols）] タブのネットワーク マップには、ネットワークで稼働しているアプリケーションが、アプリケーション名、ベンダー、バージョン、各アプリケーションを実行しているホストを基準とした階層ツリー形式で表示されます。

システムが検出するアプリケーションは、システム ソフトウェアや VDB が更新された場合や、アドオン ディテクタをインポートした場合に変わることがあります。各システムまたは VDB アップデートのリリース ノートまたはアドバイザリ テキストには、新規および更新されたディテクタの情報が含まれています。ディテクタを網羅した最新のリストについては、Cisco のサポート サイト（http://www.cisco.com/cisco/web/support/index.html）を参照してください。

このネットワーク マップから、特定のアプリケーションを実行している各ホストのホスト プロファイルを確認できます。

また、アプリケーションのカテゴリ、すべてのホストで実行されているアプリケーション、あるいは特定のホストで実行されているアプリケーションを削除することもできます。たとえば、あるアプリケーションがホスト上で無効化されているとわかっており、システムによる影響レベルの認定で使用されないようにする場合は、そのアプリケーションをネットワーク マップから削除します。

ネットワーク マップからアプリケーションを削除しても、ネットワークからは削除されません。削除したアプリケーションは、システムがアプリケーションの変更（たとえば Apache Web サーバが新しいバージョンにアップグレードされた）を検出するか、ユーザがシステムの検出機能を再起動すると、ネットワーク マップに再表示されます。

何を削除するかによって、動作は次のように異なります。

- アプリケーション カテゴリ：アプリケーション カテゴリを削除すると、そのアプリケーション カテゴリがネットワーク マップから除去されます。削除したカテゴリの下にあるすべてのアプリケーションは、そのアプリケーションを含むすべてのホストプロファイルから削除されます。

  たとえば、[http] を削除した場合、[http] として示されるすべてのアプリケーションがすべてのホスト プロファイルから削除され、[http] はネットワーク マップのアプリケーション ビューに表示されなくなります。

- 特定のアプリケーション、ベンダー、バージョン：これらの要素を削除すると、関連するアプリケーションがネットワーク マップから除去され、そのアプリケーションを含むホスト プロファイルからもアプリケーションが除去されます。

  たとえば、[http] カテゴリを展開し、[Apache] を削除すると、[Apache] としてリストされているすべてのアプリケーションは、[Apache] の下にリストされているバージョンを問わず、それらを含むホストプロファイルから削除されます。同様に、[Apache] を削除する代わりに、特定のバージョン（[1.3.17] など）を削除すると、影響を受けるホスト プロファイルから、選択されたバージョンだけが削除されます。

- 特定の IP アドレス：IP アドレスを削除すると、その IP アドレスがアプリケーション リストから除去され、選択した IP アドレスのホスト プロファイルからアプリケーション自体が除去されます。

  たとえば、[http]、[Apache]、[1.3.17 (Win32)] の順に展開し、[172.16.1.50:80/tcp] を削除すると、Apache 1.3.17（Win32）アプリケーションは IP アドレス 172.16.1.50 のホスト プロファイルから削除されます。

[脆弱性（Vulnerabilities）] のネットワーク マップ

[脆弱性（Vulnerabilities）] タブのネットワーク マップには、システムによってネットワークで検出された脆弱性がレガシーの脆弱性 ID（SVID）、Bugtraq ID、CVE ID、または [Snort ID] ごとに編成されて表示されます。脆弱性は、デフォルトでは SVID ごとに表示されます。脆弱性は ID 番号順に並べられ、影響を受けるホストが各脆弱性の下にリストされます。

このネットワーク マップから、特定の脆弱性の詳細、および特定の脆弱性の影響を受けるホストのホストプロファイルを表示できます。この情報は、影響を受ける特定のホストに対するその脆弱性によって生じる脅威を評価するために役立ちます。

特定の脆弱性がネットワーク上のホストに該当しないと判断した場合（たとえば、パッチの適用が完了した場合）、その脆弱性を非アクティブ化できます。非アクティブ化された脆弱性はネットワーク マップに表示され続けますが、これまで影響を受けていたそれらのホストの IP アドレスはグレーのイタリック体で表示されます。それらのホストのホスト プロファイルには、非アクティブ化された脆弱性は無効と表示されますが、個々のホストについて手動で有効とマークすることができます。

ホスト上のアプリケーションまたはオペレーティング システムにアイデンティティの競合がある場合、システムは可能性のあるアイデンティティの両方について脆弱性をリスト表示します。アイデンティティの競合が解決された場合、その脆弱性は現在のアイデンティティに関連付けられたままになります。

ネットワーク マップには、デフォルトではパケットにアプリケーションのベンダーとバージョンが含まれている場合にのみ、検出されたアプリケーションの脆弱性が表示されます。ただし、Firepower Management Center の構成でアプリケーションの脆弱性マッピングの設定を有効化することで、ベンダーとバージョンのデータがないアプリケーションの脆弱性をリストするようにシステムを設定できます。

脆弱性 ID（または脆弱性 ID の範囲）の隣の数字は、次の 2 つのカウントを表しています。

影響を受けるホスト数

最初の数字は、1 つまたは複数の脆弱性の影響を受ける 1 台とは限らないホストのカウントです。ホストが複数の脆弱性の影響を受ける場合、複数回カウントされます。したがって、この数字がネットワーク上のホスト数を上回ることもあります。脆弱性を非アクティブ化すると、その脆弱性の影響を受ける可能性のあるホスト数の分、この数が減ります。1 つまたは複数の脆弱性の影響を受ける可能性のあるホストについて、脆弱性を 1 つも非アクティブ化していない場合、このカウントは表示されません。

影響を受ける可能性のあるホスト数

2 番目の数字は、1 つまたは複数の脆弱性の影響を受ける可能性があるとシステムが判断した 1 台とは限らないホストの総数のカウントです。

脆弱性を非アクティブ化すると、指定したホストについてのみ脆弱性が非アクティブになります。脆弱と判断されたすべてのホストか、指定した個々の脆弱なホストの脆弱性を非アクティブ化することができます。脆弱性が非アクティブ化されると、該当するホストの IP アドレスはネットワーク マップにグレーのイタリック体で表示されます。また、それらのホストのホスト プロファイルでは、非アクティブ化された脆弱性が無効と表示されます。

その後でシステムが脆弱性が非アクティブ化されていないホストに（たとえば、ネットワーク マップ内の新しいホストに）その脆弱性を検出すると、システムはそのホストの脆弱性をアクティブ化します。新たに検出された脆弱性は明示的に非アクティブ化する必要があります。また、システムでは、ホストのオペレーティング システムまたはアプリケーションの変更を検出すると、関連付けられている非アクティブ化された脆弱性を再度アクティブ化することがあります。

ホスト属性のネットワーク マップ

[ホスト属性（Host Attributes）] タブのネットワーク マップには、ネットワーク上のホストがユーザ定義ホスト属性またはコンプライアンス ホワイトリスト ホスト属性のいずれかを基準に編成されて表示されます。この表示では、定義済みホスト属性を使用してホストを編成することはできません。

ホストを編成するために使用するホスト属性を選択すると、Firepower Management Center はネットワーク マップで使用可能なその属性の値をリストし、割り当てられた値に基づいてホストをグループ化します。たとえば、ホワイトリスト ホスト属性でホストを編成することにすると、システムは [準拠（Compliant）]、[非準拠（Non-Compliant）]、[評価されていない（Not Evaluated）] カテゴリでホストを表示します。

また、特定のホスト属性値が割り当てられた任意のホストのホスト プロファイルを表示することもできます。

関連トピック

ホスト プロファイル内のホスト属性 （3180 ページ）

ネットワーク マップの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	リーフのみ	Admin/Any Security Analyst

ステップ 1 **[Analysis]** > **[Hosts]** > **[Network Map]**を選択します。

ステップ 2 表示するネットワーク マップのタブをクリックします。

ステップ 3 必要に応じて、以下の操作を続行します。

- ドメインの選択：マルチドメイン展開では、[ドメイン（Domain）] ドロップダウン リストからリーフ ドメインを選択します。
- ホストのフィルタリング：IP または MAC アドレスでフィルタリングするには、検索フィールドにアドレスを入力します。検索をクリアするには、クリア アイコン（ ）をクリックします。
- ドリルダウン：カテゴリまたはホストプロファイルを調べる場合、マップのカテゴリまたはサブネットからドリルダウンします。カスタム トポロジを定義した場合、[ホスト（host）] タブから [(トポロジ)（(topology)）] をクリックしてそのトポロジを表示し、デフォルトのビューに戻したい場合は、[(ホスト)（(hosts)）] をクリックします。
- 削除：該当する要素の横にある削除アイコン（ ）をクリックし、以下のことを行います。
  - [ホスト（Hosts）]、[ネットワーク デバイス（Network Devices）]、[モバイル デバイス（Mobile Devices）]、[アプリケーション プロトコル（Application Protocols）] タブのマップから要素を削除する。
  - [侵害の兆候（Indications of Compromise）] タブで IOC カテゴリ、侵害されたホスト、侵害されたホストのグループを解決済みとしてマークを付ける。
  - [脆弱性（Vulnerabilities）] タブですべてのホストまたは単一ホストの脆弱性を非アクティブ化する。
- 脆弱性クラスの指定：[脆弱性（Vulnerabilities）] タブで、[タイプ（Type）] ドロップダウン リストから、表示する脆弱性のクラスを選択します。
- 組織属性の指定：[ホスト属性（Host Attributes）] タブで、[属性（Attribute）] ドロップダウン リストから属性を選択します。

関連トピック

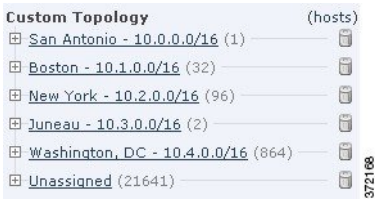
カスタム ネットワーク トポロジ （2865 ページ）
ホスト プロファイル （3159 ページ）

カスタム ネットワーク トポロジ

ホストおよびネットワーク デバイスのネットワーク マップでサブネットを整理および識別するために、カスタム トポロジ機能を使用します。

たとえば、部門内の各部署が異なるサブネットを使用している場合、カスタム トポロジ機能を使用して、これらのサブネットにラベルを付けられます。

また、カスタム トポロジで指定した部門に基づいてホストのネットワーク マップを表示することもできます。



次のいずれかまたはすべての方法でカスタム トポロジのネットワークを指定できます。

- ネットワーク検出ポリシーからネットワークをインポートして、システムでモニタするように設定したネットワークをトポロジに追加します。
- 手動でネットワークをトポロジに追加します。

[カスタム トポロジ（Custom Topology）] ページにカスタム トポロジと各トポロジのステータスが一覧表示されます。ポリシー名の隣の電球アイコンが点灯している場合、そのトポロジはアクティブで、ネットワーク マップに影響します。消灯している場合、トポロジは非アクティブです。

関連トピック

ホスト ネットワーク マップ （2858 ページ）
ネットワーク デバイスのネットワーク マップ （2859 ページ）

カスタム トポロジの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	リーフのみ	Admin/Discovery Admin

ステップ 1 **[Policies]** > **[Network Discovery]**を選択します。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 2 ツールバーで [カスタム トポロジ（Custom Topology）] をクリックします。

ステップ 3 [トポロジの作成（Create Topology）] をクリックします。

ステップ 4 [Name] を入力します。

ステップ 5 （任意）[Description] に説明を入力します。

ステップ 6 トポロジにネットワークを追加します。次の方法のいずれかまたはすべてを使用できます。

- ネットワーク検出ポリシーからのネットワークのインポート （2866 ページ）の説明に従って、ネットワーク検出ポリシーからネットワークをインポートします。
- 手動によるカスタム トポロジへのネットワークの追加 （2867 ページ）の説明に従って、手動でネットワークを追加します。

ステップ 7 [保存（Save）] をクリックします。

次のタスク

- カスタム トポロジのアクティブおよび非アクティブの設定 （2867 ページ）の説明に従って、トポロジをアクティブにします。

ネットワーク検出ポリシーからのネットワークのインポート

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	リーフのみ	Admin/Discovery Admin

ステップ 1 ネットワークをインポートするカスタム トポロジにアクセスします。

- カスタム トポロジを作成します。カスタム トポロジの作成 （2865 ページ）を参照してください。
- 既存のカスタム トポロジを編集します。カスタム トポロジの編集 （2868 ページ）を参照してください。

ステップ 2 [ポリシー ネットワークのインポート（Import Policy Networks）] をクリックします。

ステップ 3 [ロード（Load）] をクリックします。システムにより、ネットワーク検出ポリシーのトポロジ情報が表示されます。

ステップ 4 トポロジを修正するには、次の手順を実行します。

- トポロジ内のネットワーク名を変更するには、ネットワークの横にある編集アイコン（  ）をクリックし、名前を入力してから [名前の変更（Rename）] をクリックします。
- トポロジからネットワークを削除するには、削除アイコン（  ）をクリックしてから [OK] をクリックします。

ステップ 5 [保存（Save）] をクリックします。

次のタスク

- カスタムトポロジのアクティブおよび非アクティブの設定（2867ページ）の説明に従って、トポロジをアクティブにします。

手動によるカスタム トポロジへのネットワークの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	リーフのみ	Admin/Discovery Admin

ステップ 1 ネットワークを追加するカスタム トポロジにアクセスします。

- カスタム トポロジを作成します。カスタム トポロジの作成 （2865 ページ）を参照してください。
- 既存のカスタム トポロジを編集します。カスタム トポロジの編集 （2868 ページ）を参照してください。

ステップ 2 [ネットワークの追加（Add Network）] をクリックします。

ステップ 3 ホストとネットワーク デバイスのネットワーク マップでネットワークのカスタム ラベルを追加するには、[名前（Name）] を入力します。

ステップ 4 追加するネットワークを表す [IP アドレス（IP Address）] と [ネットマスク（Netmask）]（IPv4）を入力します。

ステップ 5 [Add] をクリックします。

ステップ 6 **[保存（Save）]** をクリックします。

次のタスク

- カスタムトポロジのアクティブおよび非アクティブの設定（2867ページ）の説明に従って、トポロジをアクティブにします。

関連トピック

Firepower システムの IP アドレス表記法 （20 ページ）

カスタムトポロジのアクティブおよび非アクティブの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	リーフのみ	Admin/Discovery Admin

（注） 常に 1 つのカスタム トポロジのみアクティブにできます。複数のトポロジを作成した場合、1 つをアクティブ化すると、自動的に現在アクティブなトポロジが非アクティブになります。

ステップ 1 **[Policies]** > **[Network Discovery]**を選択します。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 2 [カスタムトポロジ（Custom Topology）] を選択します。

ステップ 3 アクティブまたは非アクティブにするトポロジの横にあるスライダをクリックします。

カスタム トポロジの編集

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	リーフのみ	Admin/Discovery Admin

アクティブ トポロジに加える変更はただちに有効になります。

ステップ 1 **[Policies]** > **[Network Discovery]**を選択します。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 2 [カスタム トポロジ（Custom Topology）] をクリックします。

ステップ 3 編集するトポロジの横にある編集アイコン（ ）をクリックします。

ステップ 4 カスタム トポロジの作成 （2865 ページ）の説明に従って、トポロジを編集します。

ステップ 5 **[保存（Save）]** をクリックします。

第 117 章

インシデント

次のトピックでは、インシデント処理を設定する方法について説明します。

インシデント対応について

インシデント対応とは、セキュリティ ポリシーの違反が疑われる場合に組織が取る対応を指します。Firepower システムには、インシデントの調査に関連する情報の収集および処理をサポートする機能が含まれます。これらの機能を使用して、インシデントに関連する可能性のある侵入イベントおよびパケット データを収集することができます。攻撃の影響を軽減するために Firepower システムの外部で実行するアクティビティに関する記録のためのリポジトリとしてインシデントを使用できます。たとえば、セキュリティ ポリシーによって、ネットワークの安全性に問題のあるホストの検疫が要求される場合は、インシデントにそのことを記録できます。

Firepower システムはインシデントのライフ サイクルもサポートします。これにより、攻撃への対応を進めるごとに、インシデントのステータスを変更できます。インシデントを閉じるときに、学んだ教訓の結果としてセキュリティ ポリシーに加えた変更を記録できます。

インシデントの定義

一般的に、インシデントとは、セキュリティ ポリシー違反の可能性があることが疑われる、1 つ以上の侵入イベントと定義されます。Firepower システムでは、この用語は、インシデントへの応答を追跡するために使用できる機能について記述しています。

一部の侵入イベントは、ネットワーク資産の可用性、機密性、および整合性の点で他のイベントよりも重要になります。たとえば、ポート スキャン検出では、ネットワークでのポート スキャン アクティビティについて通知することができます。しかし、セキュリティ ポリシーでは、ポート スキャンが明確に禁止されていなかったり、優先度の高い脅威とは見なされていな

かったりすることがあります。それで、直接的なアクションの実行はしないで、代わりにすべてのポート スキャンのログを後の調査のために保持しておくことができます。

一方、ネットワーク内のホストが侵害されていることを示す、分散型サービス拒否（DDoS）攻撃に関係したイベントをシステムが生成する場合、そのアクティビティはセキュリティ ポリシーの明確な違反であると考えられます。それで、これらのイベントを調査して追跡できるように、Firepower システムでインシデントを作成する必要があります。

共通のインシデント対応プロセス

準備（Preparation）

インシデントの準備には次の 2 通りの方法があります。

- 明確で包括的なセキュリティ ポリシーと、それらを施行するためのハードウェアおよびソフトウェア リソースを配置する
- インシデントに対応するための明確に定義された計画と、その計画を実行できる適切なトレーニングを受けたチームを配置する

インシデント対応において重要なのは、ネットワークのどの部分が最も大きなリスクとなるかを理解することです。これらのネットワーク セグメントに Firepower システムを展開することで、インシデントがいつどのように発生するかについて理解を深めることができます。また、時間をかけて各管理対象デバイスに対する侵入ポリシーを慎重に調整することによって、生成されるイベントの品質を最大限に高めることができます。

検出と通知

インシデントを検出できなければ、インシデントに対応できません。インシデント対応プロセスは、検出できるセキュリティ関連イベントの種類と、それらを検出するために使用するメカニズム（ソフトウェアとハードウェアの両方）を識別する必要があります。また、セキュリティ ポリシーの違反を検出できるケースにも注意する必要があります。積極的あるいは受動的にモニタされないセグメントがネットワークに含まれている場合は、それらのセグメントにも注意する必要があります。

ユーザがネットワークに展開する管理対象デバイスは、それらがインストールされているセグメントのトラフィックの分析、侵入の検知、およびそれらを説明するイベントの生成を行う必要があります。各管理対象デバイスに展開するアクセス コントロール ポリシーが、検出するアクティビティの種類と優先度に影響を与えることに注意してください。インシデント チームが数百のイベントを取捨選択しなくてもよいように、特定のタイプの侵入イベントに対して通知オプションを設定することもできます。特定の優先順位の高い、重大度の高いイベントが検出されたときに自動的に通知するように指定できます。

調査と認定

インシデント対応プロセスでは、セキュリティ インシデントの検出後に、どのように調査を実施するかを指定する必要があります。一部の組織では、経験の浅いチーム メンバーがすべてのインシデントのトリアージを行い、重大度と優先度が比較的に低いケースは自分たちで処理

し、熟練のチームメンバーが重大度と優先度が高いインシデントを処理しています。各チームメンバーがインシデントの重要度を繰り上げる基準について理解するように、エスカレーション プロセスの概要を慎重にまとめる必要があります。

エスカレーションプロセスでは、検出されたイベントがネットワーク資産のセキュリティにどのような影響を与えるかについての理解が不可欠です。たとえば、Microsoft SQL Server を実行するホストに対する攻撃は、それとは異なるデータベース サーバを使用する組織にとって優先度は高くありません。同様に、ネットワークで SQL Server を使用しているものの、すべてのサーバにパッチを適用済みで、その攻撃に対する脆弱性がないことを確信している場合には、その攻撃の重要度は低くなります。しかし、最近誰かが脆弱性のあるバージョンのソフトウェア コピーを（テスト目的などで）インストールしていたりすれば、簡易調査で指摘されるよりも大きな問題が発生するおそれがあります。

Firepower システムは、調査および認定のプロセスをサポートするのに特に適しています。独自のイベント分類を作成し、ネットワークの脆弱性を最も適切に示す方法で、それらを適用することができます。ネットワークのトラフィックによってイベントがトリガーされると、自動的に、そのイベントの優先度判別と認定が行われ、脆弱性があることが判明しているホストに対してどのような攻撃が行われるかを示す特別なインジケータが付けられます。

Firepower システムのインシデント トラッキング機能には、エスカレーションされたインシデントを示すためにユーザが変更できるステータス インジケータも含まれています。

コミュニケーション（Communication）

すべてのインシデント対応プロセスでは、インシデント対応チームと内部および外部の対象者の間でのインシデントについての連絡の方法が指定されている必要があります。たとえば、どの種類のインシデントが管理介入を必要とし、どのレベルでの介入が必要かを考慮する必要があります。また、プロセスでは、組織の外部との連絡の方法とタイミングが説明されている必要があります。次の点に注意してください。

- あるインシデントについて、法執行機関に通知する必要がありますか。
- ホストがリモート サイトに対する分散サービス拒否（DDoS）に関与している場合、そのことを通知しますか。
- CERT 調整センター（CERT/CC）や FIRST などの組織と情報を共有する必要があるでしょうか。

Firepower システムには、HTML、PDF、CSV（カンマ区切り値）などの標準形式で侵入データを収集するために使用できる機能があり、侵入データを他のユーザと簡単に共有できます。

たとえば、CERT/CC は Web サイトのセキュリティ インシデントに関する標準情報を収集します。CERT/CC は、Firepower システムから簡単に抽出できる次のような情報を探します。

- 影響を受けるマシンに関する次のような情報
  - ホスト名および IP
  - 時間帯
  - ホストの目的や機能

- 攻撃元に関する次のような情報：
  - ホスト名および IP
  - 時間帯
  - 攻撃者と接触したことがあるかどうか
  - インシデントを扱う概算コスト
- 次のようなインシデントの説明：
  - 日付
  - 侵入方法
  - 使用された侵入者のツール
  - ソフトウェア バージョンとパッチ レベル
  - 侵入者のツールの出力
  - 悪用された脆弱性の詳細
  - 攻撃元
  - その他の関連情報

また、インシデントのコメントセクションを使用して、問題を伝えた日時と相手を記録することができます。

封じ込めとリカバリ

インシデント対応プロセスでは、ホストまたはその他のネットワーク コンポーネントが侵害された場合に、どのような手順を実行するかを明確に示す必要があります。封じ込めとリカバリの方法には、脆弱なホストへのパッチの適用から、ターゲットのシャットダウンとネットワークからの削除まで、さまざまなオプションがあります。攻撃の性質と重大度によっては、刑事責任を追求する場合に備えて証拠を保存しておくことの重要性を考慮する必要もあります。

Firepower システムのインシデント機能を使用して、インシデントの封じ込めとリカバリのフェーズ中に実行するアクションを記録しておくことができます。

学んだ教訓

それぞれのセキュリティ インシデントは、攻撃が成功したかどうかに関わりなく、セキュリティ ポリシーを見直す機会となります。ファイアウォール ルールを更新する必要はありますか。パッチ管理へのより構造化されたアプローチが必要ですか。不正なワイヤレス アクセス ポイントは新しいセキュリティ問題となりますか。それぞれの学んだ教訓は、セキュリティ ポリシーにフィードバックし、次のインシデントへのより良い対処のために役立てる必要があります。

Firepower システムのインシデント タイプ

作成する各インシデントにインシデント タイプを割り当てることができます。Firepower システムでは、以下のタイプがデフォルトでサポートされます。

- 侵入（Intrusion）
- DoS
- 不正な管理者アクセス
- Web サイトの改変
- システム整合性の侵害
- デマ ウイルス
- 盗難
- ダメージ
- 不明

独自のインシデント タイプを作成することもできます。

カスタム インシデント タイプの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Intrusion Admin

ステップ 1 **[Analysis]** > **[Intrusions]** > **[Incidents]**を選択します。

ステップ 2 [インシデントの作成（Create Incident）] をクリックします。

ステップ 3 [タイプ（Type）] エリアで、[タイプ（Types）] をクリックします。

デフォルトのインシデント タイプがページの下部に表示されます。

ステップ 4 [インシデント タイプ名（Incident Type Name）] フィールドに、新しいインシデント タイプの名前を入力します。

ステップ 5 [追加（Add）] をクリックします。

ステップ 6 [完了（Done）] をクリックします。

次にインシデントを作成または編集するときに、新しいインシデント タイプを使用できます。

インシデントの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Intrusion Admin

マルチドメイン導入では、現在のドメインで作成されたインシデントのみを表示および変更できます。先祖ドメインでは、任意の子孫ドメインからのインシデントにイベントを追加できます。

ステップ 1 **[Analysis]** > **[Intrusions]** > **[Incidents]**を選択します。

ステップ 2 [インシデントの作成（Create Incident）] をクリックします。

ステップ 3 [タイプ（Type）] ドロップダウン メニューから、インシデントを最も適切に説明するオプションを選択します。

ステップ 4 [滞留時間（Time Spent）] フィールドに、インシデントで費やした時間の合計を #d #h #m #s の形式で入力します。ここで、# は日数、時間数、分数、秒数を表します。

ステップ 5 [概要（Summary）]テキストボックスに、インシデントの簡単な説明（最大255文字の英数字、スペース、記号）を入力します。

ステップ 6 [コメントを追加（Add Comment）]テキストボックスに、インシデントのより詳細な説明（最大8191文字の英数字、スペース、記号）を入力します。

ステップ 7 インシデントにイベントを追加します。

- 選択したイベントを追加するには、クリップボードのイベントを選択して、[インシデントに追加（Add to Incident）] をクリックします。
- クリップボードからすべてのイベントを追加するには、[すべてをインシデントに追加（Add All to Incident）] をクリックします。

（注） クリップボードの複数のページにある個々のイベントを追加する場合は、1 つのページのイベントを追加してから、他のページのイベントを追加します（ページごとに追加します）。

ステップ 8 **[保存（Save）]** をクリックします。

インシデントの編集

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Intrusion Admin

マルチドメイン導入では、現在のドメインで作成されたインシデントのみを表示および変更できます。先祖ドメインでは、すべての子孫ドメインからインシデントにイベントを追加できます。

ステップ 1 **[Analysis]** > **[Intrusions]** > **[Incidents]**を選択します。

ステップ 2 編集するインシデントの横にある編集アイコン（  ）をクリックします。

ステップ 3 インシデントの以下の側面を編集できます。

- ステータスの変更
- タイプの変更
- クリップボードからのイベントの追加
- イベントの削除

ステップ 4 [Time Spent] フィールドに、インシデントに費やした追加の時間の合計を入力します。

ステップ 5 [Add Comment] テキスト ボックスで、インシデントに対する変更点（最大 8191 文字の英数字、スペース、および記号）を示します。

ステップ 6 オプションで、インシデントにイベントを追加したり、削除したりすることができます。

- クリップボードからイベントを追加するには、クリップボードのイベントを選択して、[インシデントに追加（Add to Incident）] をクリックします。
- クリップボードからすべてのイベントを追加するには、[インシデントにすべてを追加（Add All to Incident）] をクリックします。
- インシデントから特定のイベントを削除するには、イベントを選択し、[削除（Delete）]をクリックします。
- インシデントからすべてのイベントを削除するには、[すべて削除（Delete All）] をクリックします。
- イベントを追加または削除せずにインシデントを更新するには、[保存（Save）] をクリックします。

インシデント レポートの生成

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Intrusion Admin

Firepower システムを使用して、インシデント レポートを生成できます。このレポートには、インシデントの概要、インシデントのステータス、およびコメントに加えて、インシデントに追加するイベントの情報を含めることができます。また、レポートにイベントの概要情報を含めるかどうかも指定できます。

ステップ 1 **[Analysis]** > **[Intrusions]** > **[Incidents]**を選択します。

ステップ 2 レポートに含めるインシデントの横にある編集アイコン（  ）をクリックします。

ステップ 3 次の 2 つのオプションから選択できます。

- レポートにインシデントのすべてのイベントを含める場合は、[すべてのレポートの生成（Generate Report All）] をクリックします。
- レポートにインシデントの特定のイベントを含める場合は、目的のイベントの横にあるチェックボックスをオンにしてから、[レポートの生成（Generate Report）] をクリックします。

ステップ 4 レポートの名前を入力します。

ステップ 5 [インシデント レポートのセクション（Incident Report Sections）] で、レポートに含めるインシデントの部分（[ステータス（status）]、[概要（summary）]、および [コメント（comments）] のチェックボックスをオンにします。

ステップ 6 レポートにイベント情報を含める場合は、使用するワークフローを選択し、[レポートのセクション（Report Sections）] で、イベントの概要情報を含めるかどうかを指定します。

ステップ 7 レポートに含めるワークフロー ページの横にあるチェックボックスをオンにします。

ステップ 8 レポートに使用する出力形式（[PDF]、[HTML]、および [CSV]）の横にあるチェックボックスをオンにします。

（注） CSVベースのインシデント レポートには、イベント情報のみが含まれます。また、インシデントのステータス、概要、コメントは含まれ**ません**。

ステップ 9 [レポートの生成（Generate Report）] をクリックして、レポート プロファイルの更新を確認します。

第 118 章

ルックアップの使用

以下のトピックでは、Firepower システムで既知の（または未知の）エンティティに関する情報を検索する方法について説明します。

ルックアップの概要

Firepower Management Center がインターネットに接続している場合、手動ルックアップ機能を使って次の情報を検索できます。

- 任意の IP アドレスについての Regional Information Registries（RIR）情報（whois）。
- URL フィルタリング機能によって分類された URL カテゴリおよびレピュテーション。
- 任意の IP アドレスについての地理位置情報（国名、国番号および大陸名）（最新の地理位置情報を確実に使用するように、Firepower Management Center 上の地理位置情報データベース（GeoDB）を定期的に更新することを強くお勧めします）。

関連トピック

地理位置情報データベース（GeoDB）の更新 （183 ページ）

Whois ルックアップの実行

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）

始める前に

- Firepower Management Center がインターネットにアクセスできることを確認します。セキュリティ、インターネット アクセス、および通信ポート （3281 ページ）を参照してください。

ステップ 1 **[Analysis]** > **[Advanced]** > **[Whois]**を選択します。

ステップ 2 IP アドレスを入力して、[検索（Search）] をクリックします。

関連トピック

コンテキスト メニュー （13 ページ）

URL カテゴリとレピュテーションの検索

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス（**Access**）
URL フィルタリング	URL フィルタリング	Management Center	任意（Any）	Admin/Any Security Analyst

URL のカテゴリとレピュテーションは手動で検索できます。この機能は、ポリシー処理を計画、調整、またはトラブルシューティングするために特定の URL をどのように評価するかを確認する場合や、Cisco ソリューションの外部のソースから明らかになる問題のある可能性のある URL を調査する場合に使用します。次に示す結果のカテゴリとレピュテーションは、URL フィルタリング機能で使用されているものと同じです。

始める前に

- Firepower Management Center はインターネットにアクセスできる必要があります。セキュリティ、インターネット アクセス、および通信ポート （3281 ページ）を参照してください。
- URL フィルタ リングと **[不明な URL を Cisco Cloud に問い合わせる（Query Cisco cloud for unknown URLs）]** オプションを有効にする必要があります。カテゴリとレピュテーションを使用した URL フィルタリングの有効化 （1724 ページ）および URL フィルタリング オプション （1725 ページ）を参照してください。
- 少なくとも 1 台のデバイスが FMC に登録されており、そのデバイスには有効な URL フィルタリング ライセンスが割り当てられている必要があります。

ステップ 1 **[Analysis]** > **[Advanced]** > **[URL]** を選択します。

ステップ 2 最大 250 個の URL およびパブリックなルーティング可能 IP アドレスを一般的な任意の形式で入力します（たとえば、URL には "http"、"www" またはサブドメインが含まれていても、省略されていてもよく、短縮形式であってもかまいません）。各エンティティは、スペースまたは改行で区切ります。

アスタリスク（*）などのワイルドカードはサポートされていません。

ステップ 3 [検索（Search）] をクリックします。

入力した URL が多数あり、ネットワークが遅い場合は、処理に数分かかることがあります。

URL が無効であることを示すエラー メッセージが表示された場合は、スペリングを確認するか、URL の別のバリエーションを試行します。たとえば、"www" や "http(s)" のプレフィックスを省略します。

URL は最大 6 つのカテゴリに属する可能性がありますが、レピュテーションは 1 つのみです。

ステップ 4 （オプション）列ヘッダーをクリックして、結果をソートします。

ステップ 5 （オプション）CSV ファイルとして結果を保存するには、[CSV のエクスポート（Export CSV）] をクリックします。

CSV ファイルには、レピュテーション レベル用の追加の列が含まれているため、リスク基準でのソートが可能です。ゼロ（0）は、システムにリスク データが不足している URL に対する不明なリスクを表しています。

次のタスク

有効なカテゴリとレピュテーションのリストを表示する場合は、[ポリシー（Policies）]>[アクセス制御（Access Control）] > [アクセス制御（Access Control）] に移動し、ポリシーをクリックするか新しいポリシーを追加して、[ルールの追加（Add Rule）] をクリックし、[URL（URLs）] タブをクリックします。

IP アドレスの地理位置情報の検出

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
該当なし	いずれか（Any）	FMC	いずれか（Any）	いずれか（Any）

地理位置情報ルックアップ機能を使用して、国名、ISO 3166-1 の 3 桁の国番号と、任意の IP アドレスに関連付けられた大陸名を検索します。

ステップ 1 **[Analysis]** > **[Advanced]** > **[Geolocation]**を選択します。

ステップ 2 1 つ以上の IP アドレスの地理位置情報を表示するには、アドレス（複数可）を入力して、[検索（Search）] をクリックします。IPv4 アドレス、IPv6 アドレスのいずれか、または両方を指定できます。複数のアドレスは、カンマ、セミコロン、改行、スペース文字を使用して区切ります。

ヒント テキストボックスをクリアするには、[クリア（Clear）] をクリックします。

ステップ 3 データを並べ替えるには、列見出しをクリックします。IP アドレスを除くすべてのフィールドによって並べ替えが可能です。

ステップ 4 （オプション）CSV として結果を保存するには、[CSV をエクスポートする（Export CSV）] をクリックします。

関連トピック

地理位置情報データベース（GeoDB）の更新 （183 ページ）

第 119 章

外部ツールを使用したイベントの分析

によるイベントの分析 Cisco Threat Response

Cisco Threat Response を使用して脅威を迅速に検出、調査、対応する Cisco Cloud の統合プラットフォームでは、Firepower を含む複数の製品から集約されたデータを使用してインシデントを分析することができます。

- Cisco Threat Response の一般情報については、次を参照してください。

  https://www.cisco.com/c/en/us/products/security/threat-response.html。

- Firepower と Cisco Threat Response の統合の詳細な手順については、次を参照してください。

- https://cisco.com/go/firepower-ctr-integration-docs にある『*Firepower and Cisco Threat Response Integration Guide*』

Cisco Threat Response でのイベント データの表示

始める前に

- https://www.cisco.com/c/en/us/support/security/defense-center/products-installation-and-configuration-guides-list.html にある『*Firepower and Cisco Threat Response integration Guide* 』の説明に従って、統合をセットアップします。

- Cisco Threat Response のオンライン ヘルプを確認し、脅威の検出、調査、およびアクションを実行する方法を習得します。
- Cisco Threat Response にアクセスするにはクレデンシャルが必要です。

ステップ 1 Firepower Management Center で、次のいずれかを実行します。

- 特定のイベントから Cisco Threat Response にピボットするには、次の手順を実行します。

  a. [分析（Analysis）] > [侵入（Intrusions）] メニューで、サポートされているイベントが表示されているページに移動します。

  b. 送信元または宛先の IP アドレスを右クリックし、[Threat Response に表示（View in Threat Response）] を選択します。

- 通常のイベントの情報を表示するには、次の手順を実行します。

  a. [システム（System）] > [統合（Integrations）] > [クラウド サービス（Cloud Services）] に移動します。

  b. リンクをクリックして Cisco Threat Response にイベントを表示します。

ステップ 2 プロンプトが表示されたら、Cisco Threat Response にサインインします。

Splunk でのイベント分析

Cisco Firepower App for Splunk を使用し、Splunk 上に転送した Firepower イベント データを使用してネットワーク上の脅威をハントおよび調査します。

詳細については、「https://cisco.com/go/firepower-for-splunk」を参照してください。

を使用したイベント調査 Cisco Security Packet Analyzer

組織が Cisco Security Packet Analyzer（Firepower システムとは別個の製品）を展開している場合、Cisco Security Packet Analyzer を使用して Firepower システムが検出するインシデントや不審なイベントのコンテキスト情報を、フル パケット キャプチャの形式で収集できます。

Firepower Management Center のイベントから複数のCisco Security Packet Analyzer インスタンスで即座にクエリを実行し、Cisco Security Packet Analyzer の結果を処理したり、結果をダウンロードしてWireshark（TM）などの他のツールを使用したりしてタイムライン分析を実行することができます。

Cisco Security Packet Analyzer および Firepower Management Center は互いに独立して展開され、Firepower システムは Cisco Security Packet Analyzer の導入を認識しません。キャプチャされたデータはパケット アナライザと管理センター間を移動しません。

パケット アナライザの展開の要件

Cisco Security Packet Analyzer インスタンスを展開する際は次の点に留意してください。

- 最大 500 の Cisco Security Packet Analyzer インスタンスを Firepower Management Center に登録できます。スタック内の各パケット アナライザ インスタンスは個別に登録する必要があります。
- この統合でのサポート対象の Cisco Security Packet Analyzer モデルとバージョンについては、https://www.cisco.com/c/en/us/support/security/defense-center/products-device-support-tables-list.html の『*Cisco Firepower Compatibility Guide*』を参照してください。
- 1 つのキャプチャ セッションで同時に複数の目的に対応でき、クエリによって展開の負荷が過大にならない場合を除いて、Firepower システムで使用するパケット アナライザのインスタンスは一般に、この目的専用とする必要があります。
- Cisco Security Packet Analyzer 分析するトラフィックをキャプチャでき、また、パケット アナライザ インスタンスと Firepower 管理対象デバイスが確認するトラフィックが同じである必要があります。
- Firepower Management Center はネットワーク上の各パケット アナライザにアクセスできる必要があります。
- パケット アナライザのインスタンスをセットアップし、この展開の前提条件を満たすには、https://www.cisco.com/c/en/us/support/security/security-packet-analyzer/tsd-products-support-series-home.html の Cisco Security Packet Analyzer のドキュメントとパケット アナライザのオンライン ヘルプを使用します。
- 各パケット アナライザは、Firepower Management Center とその管理対象デバイスとして同じ NTP サーバを使用して時刻を同期させる必要があります。
- 各パケット アナライザで次を満たす必要があります。
  - パケット アナライザへの Web アクセスが有効になっている必要があります。
  - クエリのキャプチャ権限を持つ次のアカウントが必要です。
    - Firepower Management Center がクエリをパケット アナライザに送信するときに使用するユーザ アカウント。
    - 自分と、パケット アナライザにクエリの結果を表示する他の人のユーザ アカウント。

    Web ユーザ パスワードの制限文字については、Cisco Security Packet Analyzer のドキュメントを参照してください。

    ヒント：パケットアナライザでこれらのアカウントのクレデンシャルをテストし、機能することを確認します。
  - パケット アナライザの Web インターフェイスでクエリが正常に実行できる必要があります。

- パケットアナライザのキャプチャセッションの要件と推奨事項（2884ページ）で説明したキャプチャ セッションの要件を満たします。

これらのタスクの手順については、パケットアナライザのドキュメントを参照してください。

パケット アナライザのキャプチャ セッションの要件と推奨事項

- 各 Cisco Security Packet Analyzer インスタンスでキャプチャ セッションを作成する必要があります。
- 各パケット アナライザ インスタンスに設定する必要があるキャプチャ セッションは 1 つのみです。
- Firepower Management Center の登録形式のデフォルト キャプチャ セッション名は **`firepower_rolling_capture`** です。わかりやすくするために、別の名前を使用する理由がある場合を除いて、すべてのパケットアナライザインスタンスにこのキャプチャセッション名を使用します。
- 残りの値は次のとおりです。

オプション	値
[パケット スライス サイズ（Packet Slice Size）]	パケット全部をキャプチャする場合は ゼロ（0）
ストレージ タイプ	ファイル
[ディスク使用率（%）（Disk Utilization (%)）]	80
ファイルサイズ（MB）（File Size (MB)）	パケット アナライザ モデルでベスト パフォーマンスを得るための最大サイズ（2000 または 500）
ローテートファイル（Rotate Files）	ローリング キャプチャを有効にする場合に選択
All others	展開で有効な値

- 任意のユーザがクエリを実行する前にキャプチャ セッションを実行する必要があります。セッションを保存した後、[キャプチャ セッション（Capture Sessions）] ページに移動してキャプチャ セッションを選択し、[開始（Start）] ボタンをクリックします。

パケット アナライザ インスタンスの登録

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Security Analyst

マルチドメイン展開環境では、現在のドメインの Cisco Security Packet Analyzer インスタンスのみを作成、変更、または削除できます。現在のドメインおよび子孫ドメインのパケット アナライザ インスタンスに対してクエリを実行し、クエリの結果を表示できます。1 つのパケット アナライザ インスタンスは複数のドメインに登録できます。

始める前に

- Cisco Security Packet Analyzer の展開は、分析するパケットをキャプチャするようにパケット アナライザの展開の要件（2883 ページ）のガイドラインに従ってインストールし、設定し、適切に動作している必要があります。
- 各パケット アナライザ インスタンスには、パケット アナライザのキャプチャ セッションの要件と推奨事項（2884 ページ）のガイドラインを満たす 1 つのキャプチャ セッションが必要です。
- 登録するパケット アナライザごとに次の情報を収集します。
  - ホスト名または IP アドレス
  - ポート
  - 接続するために Firepower Management Center が使用するユーザ アカウントのクレデンシャル
  - キャプチャ セッション名

ステップ 1 [システム（System）] > [統合（Integration）] を選択します。

ステップ 2 [パケット アナライザ（Packet Analyzers）] タブをクリックします。

ステップ 3 [新規（New）] をクリックします。

ステップ 4 この手順のために前提条件で収集した値をフォームに入力します。

キャプチャ セッションの名前は、パケット アナライザで設定されているキャプチャ セッションの名前と一致する必要があります。

パケット アナライザが CA 署名付き証明書を提供しない場合は、[SSL/TLS 証明書の確認（Verify SSL/TLS certificate）] を無効にします。

ステップ 5 [保存（Save）] をクリックします。

システムはすぐに接続をテストして、キャプチャ セッションを検証します。

ステップ 6 各パケット アナライザ インスタンスに対してこれを繰り返します。

次のタスク

まだ実行していない場合は、各パケット アナライザ インスタンスでキャプチャ セッションを開始します。

クエリ パケット アナライザ

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Any Security Analyst

特定のイベントに基づいて自動的に入力されるパラメータを持つ1つのクエリを使用して最大500 の Cisco Security Packet Analyzer インスタンスに同時にクエリを実行できます。

ヒント 特定のイベントに基づいていないクエリを実行するには、[分析（Analysis）] > [詳細（Advanced）] > [パケット アナライザのクエリ（Packet Analyzer Queries）] を選択し、[新しいクエリ（New Query）] をクリックします。

ステップ 1 パケット キャプチャ内に含まれているタイプのデータなどのイベントを表示する Firepower Management Center の次のページのいずれかに移動します。

- ダッシュ ボード（[概要（Overview）] > [ダッシュボード（Dashboards）]）、または
- イベント ビューア ページ（イベントのテーブルが含まれている [分析（Analysis）] メニューのメニュー オプション）

ステップ 2 イベントを右クリックし、[クエリ パケット アナライザ（Query Packet Analyzer）] を選択します。

使用可能なイベント データがクエリ フォームに事前に入力されます。

イベントまたはダッシュボード ページの時間枠でクエリのデフォルトの開始時刻と終了時刻が決まります。

ステップ 3 調査するチケットの数など、このクエリの名前を入力します。

ステップ 4 必要に応じてクエリ パラメータを編集します。

たとえば、30 秒ごとか、または数分ごとに時間枠を拡大してイベントに関してより多くのパケットをキャプチャします。

開始時刻と終了時刻の両方がないクエリの場合は、完了するまで時間がかかります。

アスタリスクの付いたフィールドには値が必要です。

[PCAP の分割（Split Pcaps At）] の値を大きくした場合は、選択したすべてのパケット アナライザ インスタンスと、クエリ結果を処理するその他のツールで入力するファイル サイズがサポートされていることを確認します。このオプションは、パケット アナライザ自体のクエリ ダイアログの [PCAP ファイルの最大サイズ（Max PCAP File Size）] オプションです。

[プレビューのフィルタ処理（Filter Preview）] のクエリ文字列を編集する場合は注意が必要です。シンタックスは検証されません。

ステップ 5 クエリを実行するパケット アナライザのインスタンスを選択します。

マルチドメイン展開環境では、現在のドメインと子孫のドメインから Cisco Security Packet Analyzer インスタンスを組み込むことができます。

ステップ 6 [クエリ（Query）] をクリックします。

次のタスク

クエリのステータスと結果を確認します。パケット アナライザのクエリ ステータスの表示（2887 ページ）およびパケット アナライザのクエリ結果の表示（2888 ページ）を参照してください。

パケット アナライザのクエリ ステータスの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Any Security Analyst

クエリ ステータス ページの各テーブル行にはすべての Cisco Security Packet Analyzer インスタンスの各クエリのステータスがまとめられており、行を展開することで個々のインスタンスの結果を表示できます。

マルチドメイン展開環境では、現在のドメインと子孫のドメインについてのみ、パケット アナライザのクエリ ステータスと結果を表示を表示できます。

ステップ 1 次のいずれかを実行します。

- ウィンドウ上部にあるメニュー バーの [メッセージ センター（Message Center）] アイコンをクリックし、次に [タスク（Tasks）] タブをクリックします。[クエリ パケット アナライザ（Query Packet Analyzers）] のタスクを検索し、[詳細の表示（View Details）] または [結果の表示（View Results）] をクリックします。
- [分析（Analysis ）] > [詳細（Advanced）] > [パケット アナライザのクエリ（Packet Analyzer Queries）] を選択します。

ステップ 2 クエリのステータスを特定するには、次を確認します。

[ステータス（Status）] 列には、クエリが正常に実行されたパケット アナライザ インスタンスの数と、失敗したインスタンスの数が表示されます。特定のステータスを表示するには、カーソルをアイコンの上に置きます。

[継続時間（Duration）] 列には、クエリが完了または失敗するまでにかかった時間が表示されます。

継続時間は、クエリ、ネットワーク状態などの特異性の影響を受けます。

ステップ 3 次のいずれかを実行します。

- クエリの結果を表示します。パケット アナライザのクエリ結果の表示 （2888 ページ）を参照してください。
- どのパケット アナライザ インスタンスが失敗したか、クエリの完了までに時間がかかったかを特定するには、キャレット記号をクリックしてクエリの行を展開した後、失敗したインスタンスや通常よりも長い時間を要したインスタンスを探します。
- 問題または予期していなかったステータスのトラブルシューティングを実行します。Packet Analyzer クエリのトラブルシューティング （2889 ページ）を参照してください。
- 進行中のクエリをキャンセルするか、または個々のパケット アナライザ インスタンスのクエリをキャンセルします。キャンセルすると、パケット アナライザのクエリもキャンセルされます。
- 完了済みまたは失敗したクエリか、または個々のパケット アナライザ インスタンスのクエリを削除します。クエリを削除してもパケット アナライザでキャプチャされたデータは削除されません。

ステップ 4 このページの結果を更新するには、ページをリロードします。

パケット アナライザのクエリ結果の表示

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Any Security Analyst

Cisco Security Packet Analyzer でクエリに一致するパケットの表示および分析したり、または別のツールで表示および分析するパケットをダウンロードすることができます。

マルチドメイン展開環境では、現在のドメインと子孫のドメインについてのみ、パケット アナライザのクエリの結果を表示できます。

始める前に

表示するクエリの結果を保持するパケット アナライザ インスタンスにアクセスできる Cisco Security Packet Analyzer ユーザ アカウントのクレデンシャルがあることを確認します。

ステップ 1 [分析（Analysis）] > [詳細（Advanced）] > [パケット アナライザのクエリ（Packet Analyzer Queries）] を選択します。

ステップ 2 キャレット記号をクリックし、クエリに対応する行を展開します。

ステップ 3 次のアイコンが表示されている 1 つ以上のパケット アナライザ インスタンスを見つけます。

[該当なし（No results）] は、クエリに一致するそのパケット アナライザ インスタンスのパケットがなかったことを示します。

予想どおりの結果が得られなかった場合は、Packet Analyzer クエリのトラブルシューティング （2889 ページ）を参照してください。

ステップ 4 次のいずれかを実行します。

a) キャプチャしたパケットを Cisco Security Packet Analyzer で表示して処理するには、[Open link] アイコン（  ） をクリックします。

b) PCAP ファイルをダウンロードし、サードパーティ製のパケット分析ツールに表示するには、[Download] アイコン（） をクリックします。

パケット アナライザ インスタンスによって別の Web ブラウザ ウィンドウが開かれ、クレデンシャルが要求されます。

ステップ 5 パケット アナライザにサインインします。

ステップ 6 Firepower Management Center に戻り、ダウンロード アイコンかリンクを開くためのアイコンをもう一度クリックします。

ステップ 7 キャプチャされたパケットを希望のアプリケーションまたはツールで処理します。たとえば、Cisco Security Packet Analyzer では、キャプチャされたパケットを復号してから、秘密キーの復号化やファイルの抽出などのタスクを実行して何が転送されたかを確認します。

Packet Analyzer クエリのトラブルシューティング

クエリの結果が出ない

考えられる原因と解決策：

- キャプチャ セッションは、Packet Analyzer では実行されません。これが問題の原因である場合は、クエリを実行しているイベントのデータはありません。将来のイベントのパケット収集を有効にするには、パケット アナライザでキャプチャ セッションを開始します。
- クエリの時間枠がキャプチャされたファイルの時間枠から外れているか、キャプチャ セッションが上書きされています。
- Packet Analyzer が正しいパケットをキャプチャしていません。
- 関連データを含むキャプチャ セッション ファイルがバッファに書き込まれ続けています。ファイルへの書き込みが完了するまで、セッションに対するクエリを実行できません。数分間待ってからもう一度試してください。
- https://www.cisco.com/c/en/us/support/security/security-packet-analyzer/products-user-guide-list.html の *Cisco Security Packet Analyzer*ユーザ ガイド のトラブルシューティングの情報を参照してください。

クエリに時間がかかりすぎる

- 各 Packet Analyzer で一度に 1 つのみのクエリを実行できます。特定のクエリに先立ってキューイングされた複数のクエリが存在する場合、クエリの完了までに長い時間がかかります。複数のクエリ送信元がある場合でも、存在するのは単一のキューです。
- 開始時刻と終了時刻を両方とも指定していないクエリの場合、プロセスの時間は大幅に長くなります。
- 開始時刻から終了時刻までの期間が長くなるほど、システムで検索を完了するのにかかる時間も長くなります。

Web ベースのリソースを使用したイベントの調査

Firepower Management Center 外部の Web ベースのリソースにおける潜在的な脅威についての情報をすばやく検索するには、contextual cross-launch 機能を使用します。例：

- Cisco または既知の疑わしい脅威に関する情報を公開するサードパーティ製クラウドホステッド サービスの疑わしい送信元 IP アドレスを検索する、または
- 組織の履歴ログで特定の脅威に関する過去のインスタンスを検索する（組織がセキュリティ情報とイベント管理（SIEM）アプリケーションでそのデータを格納している場合）。
- 組織で Cisco AMP for Endpoints を導入している場合は、ファイル トラジェクトリ情報などの特定のファイルに関する情報を検索します。

イベントを調査する際は、Firepower Management Center のイベント ビューアまたはダッシュボードのイベントから直接、外部リソースの関連情報をクリックできます。これにより、その IP アドレス、ポート、プロトコル、ドメイン、または SHA 256 ハッシュに基づいて、特定のイベントに関連するコンテキストを迅速に収集できます。

たとえば、[上位攻撃者（Top Attackers）] ダッシュボード ウィジェットを表示し、記載されている送信元 IP アドレスのいずれかに関する詳細情報を検索すると仮定します。この IP アドレスに関して、Talos がどのような情報を公開しているか確認したいので、「Talos IP」リソースを選択します。Talos Web サイトが開き、この特定の IP アドレスに関する情報が書かれたページが表示されます。

一般的に使用されているシスコやサードパーティ製の脅威インテリジェンス サービスへの一連の事前定義されたリンクから選択し、その他の Web ベースのインターフェイスおよび Web インターフェイスを持つ SIEM または他の製品へのカスタム リンクを追加できます。一部のリソースでは、アカウントまたは製品の購入が必要になる場合があります。

コンテキスト クロス起動のリソースの管理について

[分析（Analysis）]>[詳細（Advanced）]>[コンテキスト クロス起動（Contextual Cross-Launch）] ページを使用して外部の Web ベースのリソースを管理します。

シスコが提供している事前定義のリソースにはシスコのロゴが付いています。残りのリンクはサードパーティのリソースです。

必要がないリソースは無効にするか、または削除できます。あるいは、たとえば名前の前に小文字の「z」を追加するなどして名前を変更し、そのリソースをリストの下部に分類することができます。削除されたリソースは、元に戻すことはできませんが、再作成できます。

リソースを追加するには、コンテキスト クロス起動のリソースの追加（2891 ページ）を参照してください。

カスタム コンテキスト クロス起動のリソースの要件

カスタム contextual cross-launch リソースを追加する場合は、次の点に留意します。

- リソースは Web ブラウザを介してアクセスできる必要があります。
- http プロトコルと https プロトコルのみがサポートされています。
- GET 要求のみがサポートされています。POST 要求はサポートされていません。
- URL の変数のエンコーディングはサポートされていません。IPv6 アドレスをエンコードするにはコロンで区切る必要がある場合がありますが、ほとんどのサービスでこのエンコーディングは必要ありません。
- 事前に定義されたリソースを含めて、最大 100 のリソースを設定できます。

コンテキスト クロス起動のリソースの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Security Analyst

脅威インテリジェンス サービスやセキュリティ情報とイベント管理（SIEM）の ツールなどの contextual cross-launch リソースを追加できです。

マルチドメイン展開環境では、親ドメインのリソースを表示および使用できますが、現在のドメインで実行できるのはリソースの作成と編集のみです。すべてのドメインのリソースの合計数は 100 に制限されています。

始める前に

- カスタム コンテキスト クロス起動のリソースの要件（2891 ページ）を参照してください。
- リソースに必要な場合は、アクセスに必要なアカウントとクレデンシャルにリンクするか、作成するか、または取得します。必要に応じて、アクセスが必要な各ユーザにクレデンシャルを割り当てて配布します。
- リンク先のリソースのクエリ リンクのシンタックスを特定します。

ブラウザ経由でリソースにアクセスし、必要に応じてそのリソースのドキュメントを使用して、たとえばIP アドレスなど、検索するクエリ リンクの特定のタイプの情報の検索に必要なクエリ リンクを作成します。

クエリを実行して、結果の URL をブラウザのロケーション バーからコピーします。

たとえば、クエリ URL **`https://www.talosintelligence.com/reputation_center/lookup?search=10.10.10.10`** が表示される場合があります。

ステップ 1 [分析（Analysis）] > [詳細（Advanced）] > [コンテキストクロス起動（Contextual Cross-Launch）] を選択します。

ステップ 2 [新しいクロス起動（New Cross-Launch）] をクリックします。

表示されたフォームのアスタリスクの付いたすべてのフィールドに値が必要です。

ステップ 3 一意のリソース名を入力します。

ステップ 4 作業中のURLの文字列をリソースから[URLテンプレート（URL Template）]フィールドに貼り付けます。

ステップ 5 クエリ文字列内の特定のデータ（IP アドレスなど）を適切な変数で置き換えます。変数を挿入するには、カーソルを置いて変数ボタン（[ip] など）を 1 回クリックします。

上記の「開始する前に」の項の例では、URL は **`https://www.talosintelligence.com/reputation_center/lookup?search= {ip}`** になります。contextual cross-launch リンクを使用すると、URL 内の {ip} 変数は、イベント ビューアまたはダッシュボードでユーザが右クリックする IP アドレスに置き換わります。

各変数の説明については、変数ボタンの上にカーソルを置きます。

1 つのツールまたはサービスに複数の contextual cross-launch リンクを作成するには、それぞれに異なる変数を使用します。

ステップ 6 [データ例を使用したテスト（Test with example data）] アイコン（）をクリックしてデータ例を使用してリンクをテストします。

ステップ 7 問題を修正します。

ステップ 8 **[保存（Save）]** をクリックします。

コンテキスト クロス起動を使用したイベントの調査

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	[管理者（Admin）]/[セキュリティ アナリスト（Security Analyst）]/[セキュリティ アナリスト（読み取り専用）（Security Analyst (Read-only)）]

始める前に

アクセスするリソースにクレデンシャルが必要な場合は、それらのクレデンシャルがあることを確認します。

ステップ 1 Firepower Management Center でイベントが表示される次のページのいずれかに移動します。

- ダッシュ ボード（[概要（Overview）] > [ダッシュボード（Dashboards）]）、または
- イベント ビューア ページ（イベントのテーブルが含まれている [分析（Analysis）] メニューのメニュー オプション）

ステップ 2 対象のイベントを右クリックして、使用する contextual cross-launch のリソースを選択します。

必要に応じて、コンテキスト メニューを下にスクロールして使用可能なすべてのオプションを確認します。

右クリックしたデータ タイプによって表示されるオプションが異なります。たとえば、IP アドレスを右クリックした場合は、IP アドレスに関連する contextual cross-launch のオプションのみが表示されます。

そのため、たとえば、[上位攻撃者（Top Attackers）] ダッシュボード ウィジェットに送信元 IP アドレスに関して Cisco Talos からの脅威情報を表示させるには、[Talos SrcIP] または [Talos IP] を選択します。

リソースに複数の変数が含まれている場合、そのリソースを選択するオプションは、含まれている各変数に可能な 1 つの値を持つイベントにのみ使用できます。

別のブラウザ ウィンドウに contextual cross-launch のリソースが開きます。

クエリを実行するデータの量、リソースの速度と需要によってはクエリが処理されるまでに時間がかかる場合があります。

ステップ 3 必要に応じて、リソースにサインインします。

セキュリティ イベントの syslog メッセージの送信について

接続、セキュリティインテリジェンス、侵入、およびファイルとマルウェアのイベントに関連するデータは、syslog を介してセキュリティ情報およびイベント管理（SIEM）ツールまたは、外部のイベント ストレージおよび管理ソリューションに送信できます。

これらのイベントを Snort® イベントと呼ぶこともあります。

syslog にセキュリティ イベントのデータを送信するためのシステムの設定について

セキュリティ イベントを syslog に送信するようにシステムを設定するには、次を知っておく必要があります。

- セキュリティ イベント syslog メッセージングを設定するためのベストプラクティス（2895 ページ）
- セキュリティ イベントの syslog の設定場所 （2895 ページ）
- セキュリティ イベントの syslog メッセージに適用する FTD プラットフォームの設定 （1393 ページ）
- ポリシーで syslog の設定を変更した場合、それらの変更を有効にするには展開する必要があります。

セキュリティ イベント syslog メッセージングを設定するためのベストプラクティス

デバイスとバージョン	設定の場所
Firepower Threat Defense バージョン 6.3 以降	1. FTD プラットフォーム設定（[デバイス（Devices）] > [プラットフォーム設定（Platform Settings）] > [脅威に対する防御設定（Threat Defense Settings）] > [Syslog]）を設定します。 セキュリティ イベントの syslog メッセージに適用する FTD プラットフォームの設定（1393 ページ）も参照してください。 2. アクセス コントロール ポリシーの [ロギング（Logging）] タブで、FTD プラットフォーム設定の使用を選択します。 3. （侵入イベントの場合）アクセス コントロール ポリシーの [ロギング（Logging）] タブの設定を使用するように侵入ポリシーを設定します。（これはデフォルトです）。 これらの設定の上書きは推奨していません。
その他のすべてのデバイス	1. アラート応答を作成します。 2. アラート応答を使用するには、アクセス コントロール ポリシーの [ロギング（Logging）] タブを設定します。 3. （侵入イベントの場合）侵入ポリシーで syslog 設定を構成します。

セキュリティ イベントの syslog の設定場所

- 接続およびセキュリティ インテリジェンス イベント の syslog の設定場所（すべてのデバイス）（2895 ページ）
- 侵入イベントの syslog の設定場所（FTD 6.3 デバイス）（2898 ページ）
- 侵入イベントの syslog の設定場所（FTD 以外のデバイスと 6.3 よりも前のバージョン）（2899 ページ）
- ファイルとマルウェア イベントの syslog の設定場所（2899 ページ）

接続およびセキュリティ インテリジェンス イベント の syslog の設定場所（すべてのデバイス）

多くの場所でロギング設定を実行できます。次の表を使用して、必要なオプションが設定されていることを確認します。

重要

- syslog の設定を行う場合、特に他の設定から継承したデフォルトを使用する際には細心の注意が必要です。下の表に示すように、オプションの中にはすべての管理対象デバイス モデルやソフトウェア バージョンに使用できないものもあります。
- 接続ロギングを設定する際の重要な情報については、接続ロギング（3001 ページ）の章を参照してください。

設定の場所	説明と詳細情報
[デバイス（Devices）]>[プラットフォーム設定（Platform Settings）]、[Threat Defense 設定ポリシー（Threat Defense Settings policy）]、[Syslog]	このオプションは、バージョン 6.3 以降を実行している Firepower Threat Defense のデバイスにのみ適用されます。 ここで行う設定は、アクセス コントロール ポリシーのロギング設定に指定でき、この表の残りのポリシーとルールに使用するか、それらをオーバーライドできます。 セキュリティ イベントの syslog メッセージに適用する FTD プラットフォームの設定（1393 ページ）と Syslog について（1385 ページ）およびサブトピックを参照してください。
[ポリシー（Policies）]>[アクセス制御（Access Control）]、<各ポリシー>、[ロギング（Logging）] タブ	ここで行う設定は、この表の残りの行で指定する場所の子孫のポリシーおよびルールにあるデフォルトをオーバーライドしない限り、すべての接続イベントとセキュリティ インテリジェンス イベントの syslog のデフォルト設定になります。 6.3 以降を実行している FTD デバイスの推奨設定：FTD プラットフォーム設定を使用します。詳細については、セキュリティ イベントの syslog メッセージに適用する FTD プラットフォームの設定（1393 ページ）と Syslog について（1385 ページ）およびサブトピックを参照してください。 その他のすべてのデバイスに必要な設定：syslog アラートを使用します。 syslog アラートを指定する場合は、Syslog アラート応答の作成（2810 ページ）を参照してください。 [ロギング（Logging）] タブの設定に関する詳細については、アクセス コントロール ポリシーのロギング設定（1681 ページ）を参照してください。

設定の場所	説明と詳細情報
[ポリシー（Policies）]>[アクセス制御（Access Control）]、<各ポリシー>[ルール（Rules）] タブ、[デフォルト アクション（Default Action）] 行、[ロギング（Logging）] ボタン（  ））	ロギングのアクセス コントロール ポリシーに関連付けられているデフォルト アクションを設定します。 アクセス コントロール ルール（1689ページ）章とポリシーのデフォルト アクションによる接続のロギング（3018ページ）のロギングに関する情報を参照してください。
[ポリシー（Policies）]>[アクセス制御（Access Control）]、<各ポリシー>、[ルール（Rules）] タブ、<各ルール>、[ロギング（Logging）] タブ	特定のルールの設定をアクセス制御ポリシーにログインします。 アクセス コントロール ルール（1689ページ）章のロギングに関する情報を参照してください。
[ポリシー（Policies）]>[アクセス制御（Access Control）]、<各ポリシー>、[セキュリティ インテリジェンス（Security Intelligence）] タブ、[ロギング オプション（Logging Options）] ボタン（  ）	セキュリティ インテリジェンス ブラックリストのロギング設定 次のボタンをクリックして設定します。 • [DNS ブラックリスト ロギング オプション（DNS Blacklist Logging Options）] • [URL ブラックリスト ロギング オプション（URL Blacklist Logging Options）] • [ネットワーク ブラックリスト ロギング オプション（Network Blacklist Logging Options）]（ブロックされたリスト上の IP アドレス用） 前提条件を含めてセキュリティ インテリジェンスの設定（1744ページ）とサブトピックおよびリンクを参照してください。
[ポリシー（Policies）]>[SSL]、[デフォルト アクション（Default Action）] 行、[ロギング（Logging）]（）ボタン	SSL ポリシーに関連付けられているデフォルト アクションのロギング設定。 ポリシーのデフォルト アクションによる接続のロギング（3018 ページ）を参照してください。
[ポリシー（Policies）]>[SSL]、<各ポリシー>、<各ルール>、[ロギング（Logging）] タブ	SSL ルールのロギング設定。 TLS/SSL ルールのコンポーネント（1817ページ）を参照してください。

設定の場所	説明と詳細情報
[ポリシー（Policies）]>[プレフィルタ（Prefilter）]、<各ポリシー>、[デフォルト アクション（Default Action）] 行、[ロギング（Logging）]（🔲）ボタン	プレフィルタ ポリシーに関連付けられているデフォルト アクションのロギング設定。 ポリシーのデフォルト アクションによる接続のロギング（3018 ページ）を参照してください。
[ポリシー（Policies）]>[プレフィルタ（Prefilter）]、<各ポリシー>、<各プレフィルタ>、[ロギング（Logging）] タブ	プレフィルタ ポリシーの各プレフィルタのロギング設定。 トンネルとプレフィルタ ルールのコンポーネント（1775 ページ）を参照してください
[ポリシー（Policies）]>[プレフィルタ（Prefilter）]、<各ポリシー>、<各トンネル ルール>、[ロギング（Logging）] タブ	プレフィルタ ポリシーの各トンネル ルールのロギング設定。 トンネルとプレフィルタ ルールのコンポーネント（1775 ページ）を参照してください
FTD クラスタ設定の追加 syslog の設定：	Firepower Threat Defense 用のクラスタリング（907 ページ）の章には syslog について複数の言及があります。「syslog」の章を検索してください。

侵入イベントの syslog の設定場所（FTD 6.3 デバイス）

侵入ポリシーの syslog 設定はさまざまな場所で指定でき、必要に応じてアクセス コントロール ポリシーまたは FTD プラットフォーム設定、あるいはその両方から設定を継承できます。

設定の場所	説明と詳細情報
[デバイス（Devices）]>[プラットフォーム設定（Platform Settings）]、[Threat Defense 設定ポリシー（Threat Defense Settings policy）]、[Syslog]	ここで設定した syslog の宛先は、侵入ポリシーのデフォルトとして使用可能なアクセス コントロール ポリシーの [ロギング（Logging）] タブで指定できます。 セキュリティ イベントの syslog メッセージに適用する FTD プラットフォームの設定（1393 ページ）と Syslog について（1385 ページ）およびサブトピックを参照してください。
[ポリシー（Policies）]>[アクセス制御（Access Control）]、<各ポリシー>、[ロギング（Logging）] タブ	侵入ポリシーに他のロギング ホストが指定されていない場合は、侵入イベントの syslog の宛先のデフォルト設定。 アクセス コントロール ポリシーのロギング設定（1681 ページ）を参照してください。

設定の場所	説明と詳細情報
[ポリシー（Policies）] > [侵入（Intrusion）]、<各ポリシー>、[詳細設定（Advanced Settings）]、[syslog アラート（Syslog Alerting）] を有効化、[編集（Edit）] をクリック	アクセス コントロール ポリシーの [ロギング（Logging）] タブで指定した宛先以外の syslog コレクタを指定するには、侵入イベントの Syslog アラートの設定（2820 ページ）を参照してください。 [重大度（Severity）] または [ファシリティ（Facility）]、あるいはその両方を侵入ポリシーで設定されているとおりに使用する場合は、ポリシーにロギング ホストを設定する必要があります。アクセス コントロール ポリシーに指定されているロギング ホストを使用する場合は、侵入ポリシーに指定されている重大度とファシリティは使用されません。

侵入イベントの syslog の設定場所（FTD 以外のデバイスと 6.3 よりも前のバージョン）

- （デフォルト）アクセス コントロール ポリシー（アクセス コントロール ポリシーのロギング設定（1681 ページ）syslog アラートを指定した場合）（Syslog アラート応答の作成（2810 ページ）を参照）
- または侵入イベントの Syslog アラートの設定（2820 ページ）を参照してください。

デフォルトでは、侵入ポリシーはアクセス コントロール ポリシーの [ロギング（Logging）] タブの設定を使用します。FTD 6.3 以外のデバイスに適用される設定がない場合は、FTD 6.3 以外のデバイスに syslog は送信されず、警告は表示されません。

ファイルとマルウェア イベントの syslog の設定場所

設定の場所	説明と詳細情報
アクセス コントロール ポリシーで次の手順を実行します。 [ポリシー（Policies）]>[アクセス制御（Access Control）]、<各ポリシー>、[ロギング（Logging）] タブ	これは、ファイルとマルウェアのイベントの syslog を送信するようにシステムを設定するための主要な場所です。 FTD プラットフォームの syslog 設定を使用しない場合は、アラート応答も作成する必要があります。Syslog アラート応答の作成（2810 ページ）を参照してください。

設定の場所	説明と詳細情報
Firepower Threat Defense プラットフォーム設定で、次の手順を実行します。 [デバイス（Devices）] > [プラットフォーム設定（Platform Settings）]、[Threat Defense 設定ポリシー（Threat Defense Settings policy）]、[Syslog]	これらの設定は、サポート対象のバージョンを実行しており、FTD プラットフォームを使用するようにアクセス コントロール ポリシーの [ロギング（Logging）] タブを設定している場合にのみ、Firepower Threat Defense デバイスにのみ適用されます。 セキュリティ イベントの syslog メッセージに適用する FTD プラットフォームの設定 （1393 ページ） と Syslog について （1385 ページ） およびサブトピックを参照してください。
アクセス コントロール ルールで次の手順を実行します。 [ポリシー（Policies）] > [アクセス制御（Access Control）]、<各ポリシー>、<各ルール>、[ロギング（Logging）] タブ	FTD プラットフォームの syslog 設定を使用しない場合は、アラート応答も作成する必要があります。Syslog アラート応答の作成 （2810 ページ） を参照してください。

セキュリティイベントの syslog メッセージの分析

FTD 6.3 以降からのセキュリティ イベント メッセージの例（侵入イベント）

```
          1                 2           3      4   5    6
Sep 24 13:42:01 192.168.0.81 SFIMS : %FTD-5-430001:SrcIP:
192.168.1.10, DstIP: 192.168.1.102, SrcPort: 33994, DstPort: 445,
Protocol: tcp, Priority: 2, GID: 133, SID: 17, Revision: 2,
Message: "DCE2_EVENT__SMB_INVALID_DSIZE", Classification:
Potentially Bad Traffic, User: No Authentication Required,
Client: NetBIOS-ssn (SMB) client, ApplicationProtocol: NetBIOS-
ssn (SMB), ACPolicy: test, NAPPolicy: Balanced Security and
Connectivity, InlineResult: Blocked
```

表 *290* : セキュリティ イベントの *syslog* メッセージのコンポーネント

サンプル メッセージの項目数	ヘッダー要素	説明
1	タイムスタンプ	syslog メッセージがデバイスから送信された日付と時刻。 • （バージョン 6.3 以降を実行している FTD デバイスから送信された syslog）アクセス コントロール ポリシーとその子孫の設定を使用して送信した syslog の場合か、または [FTD プラットフォーム設定（FTD Platform Settings）] のこの形式を使用するように指定されている場合、日付形式は RFC 5424 に指定されている ISO 8601 タイムスタンプ形式（yyyy-MM-ddTHH:mm:ssZ）に定義されている形式になります。この形式では文字 Z は UTC タイム ゾーンを示しています。 • （バージョン 6.3 以降を実行しているその他すべてのデバイスから送信された syslog）アクセス コントロール ポリシーとその子孫の設定を使用して送信した syslog の場合、日付形式は RFC 5424 に指定されている ISO 8601 タイムスタンプ形式（yyyy-MM-ddTHH:mm:ssZ）に定義されている形式になります。この形式では文字 Z は UTC タイム ゾーンを示しています。 • それ以外の場合は UTC タイム ゾーンの月、日、時刻になりますが、タイム ゾーンは表示されません。 [FTD プラットフォーム設定（FTD Platform Settings）] のタイムスタンプの設定を行うには、Syslog 設定 （1400 ページ）を参照してください。

サンプル メッセージの項目数	ヘッダー要素	説明
2	メッセージが送信されたデバイスまたはインターフェイス。 ここに表示される値は次のとおりです。 • インターフェイスの IP アドレス • デバイスのホスト名 • カスタム デバイス識別子	（FTD デバイス バージョン 6.3 以降のみから送信された syslog の場合） [FTD プラットフォーム設定（FTD Platform Settings）] を使用して syslog メッセージが送信された場合で、[Syslog デバイス ID の有効化（Enable Syslog Device ID）] オプションが指定されているときは、これはそのオプションの [Syslog 設定（Syslog Settings）] タブに設定されている値になります。 それ以外の場合、この要素はヘッダーには表示されません。 [FTD プラットフォーム設定（FTD Platform Settings）] でこの設定を行うには、Syslog 設定 （1400 ページ） を参照してください。
3	カスタム値	アラート応答を使用してメッセージが送信された場合、これは、メッセージを送信したアラート応答に設定されている**タグ**値がある場合は、その値になります。（Syslog アラート応答の作成 （2810 ページ） を参照）。 それ以外の場合、この要素はヘッダーには表示されません。
4	%FTD %NGIPS	メッセージを送信したデバイスのタイプ。 • %FTD は Firepower Threat Defense バージョン 6.3 以降 • %NGIPS はバージョン 6.3 以降を実行しているその他すべてのデバイス • バージョン 6.2.3 以前を実行しているデバイスから送信されたメセージの場合、この要素は表示されません。
5	Severity	メッセージをトリガーしたポリシーの syslog 設定に指定されている重要度。 重大度の説明については、重大度 （1386 ページ） または syslog 重大度レベル （2813 ページ） を参照してください。

サンプル メッセージの項目数	ヘッダー要素	説明
6	イベント タイプ識別子	バージョン 6.3 以降を実行しているデバイスから送信されたメッセージの場合： • 430001：侵入イベント • 430002：接続の開始時に記録された接続イベント • 430003：接続の終了時に記録された接続イベント バージョン 6.4 以降を実行しているデバイスから送信されたメッセージの場合は、次のイベント タイプ ID も使用されます。 • 430004：ファイル イベント • 430005：ファイル マルウェア イベント バージョン 6.2.3 以前を実行しているデバイスから送信されたメッセージの場合、イベント タイプ識別子は表示されません。
--	ファシリティ	セキュリティ イベントの syslog メッセージのファシリティ（2904 ページ）を参照してください。

サンプル メッセージの項目数	ヘッダー要素	説明
--	メッセージの残りの部分	コロンで区切られたフィールドと値。 空または不明な値のあるフィールドはメッセージから省略されます。 フィールドの説明については、次を参照してください。 • 接続イベントとセキュリティ インテリジェンス イベントのフィールド （3024 ページ）。 • 侵入イベント フィールド （3059 ページ） • ファイルおよびマルウェア イベント フィールド （3121 ページ） （注） フィールド説明のリストには、syslog フィールドとイベント ビューア（Firepower Management Center の Web インターフェイスの [分析（Analysis）] メニューのメニュー オプション）に表示されるフィールドの両方が含まれています。syslog 経由で使用可能なフィールドはそれを示すラベルが付けられます。 イベント ビューアに表示される一部のフィールドは、syslog 経由では使用できません。また、一部の syslog フィールドはイベント ビューアには含まれていません（ただし、検索を使用すると表示できる場合があります）。また、一部のフィールドは結合されているか、または個別になっています。

セキュリティ イベントの syslog メッセージのファシリティ

一般に、セキュリティ イベントの syslog メッセージではファシリティ値は関連性がありません。ただし、ファシリティが必要な場合は、次の表を使用してください。

Device	接続イベントにファシリティを含める場合	侵入イベントにファシリティを含める場合	syslog メッセージ内の場所
FTD 6.3 以降	[FTD プラットフォーム設定（FTD Platform Settings）] の [EMBLEM] オプションを使用します。 [FTD プラットフォーム設定（FTD Platform Settings）] を使用して syslog メッセージを送信すると、ファシリティは常に、接続イベントに対して [アラート（ALERT）] になります。	[FTD プラットフォーム設定（FTD Platform Settings）] の [EMBLEM] オプションを使用するか、または侵入ポリシーの syslog 設定を使用してロギングを設定します。侵入ポリシーを使用した場合は、侵入ポリシー設定にロギング ホストも指定する必要があります。	ファシリティはメッセージ ヘッダーには表示されませんが、syslog コレクタが RFC 5424、セクション 6.2.1 に基づいて値を派生させることができます。
6.3 より前の FTD	アラート応答を使用します。	侵入ポリシーの高度な設定の syslog 設定、またはアクセス コントロール ポリシーの [ロギング（Logging）] タブで識別されているアラート応答を使用します。	
FTD 以外のデバイス	アラート応答を使用します。	侵入ポリシーの高度な設定の syslog 設定、またはアクセス コントロール ポリシーの [ロギング（Logging）] タブで識別されているアラート応答を使用します。	

詳細については、侵入 syslog アラートの重大度 （2821 ページ）およびSyslog アラート応答の作成 （2810 ページ）を参照してください。

Firepower syslog メッセージのタイプ

Firepower は、次の表で説明するように、複数の syslog データ タイプを送信できます。

syslog データ タイプ	参照先
FMC からの監査ログ	syslog への監査ログのストリーミング （1293 ページ）およびシステムの監査 （397 ページ）の章

syslog データ タイプ	参照先
従来型デバイス（7000/8000 シリーズ、ASA FirePOWER、NGIPSv）からの監査ログ	従来型デバイスからの監査ログのストリーミング （1338 ページ）およびシステムの監査 （397 ページ）の章 CLI コマンド： syslog （3318 ページ）
FTD デバイスからのデバイス ヘルスとネットワーク関連のログ	Syslog について （1385 ページ） およびサブトピック
FTD デバイスからの接続、セキュリティ インテリジェンスおよび侵入イベント ログ	syslog にセキュリティ イベントのデータを送信するためのシステムの設定について （2894 ページ）。
クラッシック デバイスからの接続、セキュリティ インテリジェンスおよび侵入イベント ログ	syslog にセキュリティ イベントのデータを送信するためのシステムの設定について （2894 ページ）
ファイルおよびマルウェアのイベントのログ	syslog にセキュリティ イベントのデータを送信するためのシステムの設定について （2894 ページ）

セキュリティ イベントの syslog の制限事項

- syslog コレクタにイベントを表示するには最大 15 分かかる場合があります。
- 次のファイルおよびマルウェアのイベントのデータは syslog 経由で使用できません。
  - レトロスペクティブ イベント
  - エンドポイント向け AMP によって生成されたイベント

eStreamer サーバ ストリーミング

Event Streamer（eStreamer）を使用すると、Firepower Management Center または 7000 または 8000 シリーズ デバイスからの数種類のイベント データを、カスタム開発されたクライアント アプリケーションにストリーム配信できます。詳細については、『*Firepower System Event Streamer Integration Guide*』を参照してください。

eStreamer サーバとして使用するアプライアンスで eStreamer イベントの外部クライアントへのストリームを開始するには、その前に、イベントをクライアントに送信するように eStreamer サーバを設定し、クライアントに関する情報を指定して、通信を確立するときに使用する認証クレデンシャルを生成する必要があります。アプライアンスのユーザインターフェイスからこれらすべてのタスクを実行できます。設定が保存されると、選択したイベントが、要求時に、eStreamer クライアントに転送されます。

要求したクライアントに eStreamer サーバが送信できるイベント タイプを制御できます。

表 *291 : eStreamer* サーバで送信可能なイベント タイプ

イベント タイプ	説明	FMC で使用可能	7000 & 8000 シリーズ デバイスで使用可能
侵入イベント	管理対象デバイスによって生成される侵入イベント	はい	はい
侵入イベント パケット データ	侵入イベントに関連付けられたパケット	はい	はい
侵入イベント追加データ	HTTP プロキシまたはロードバランサ経由で Web サーバに接続しているクライアントの発信元 IP アドレスのような侵入イベントに関連付けられた追加データ	はい	はい
検出イベント	ネットワーク検出イベント	はい	いいえ（No）
相関およびホワイトリスト イベント	相関およびホワイトリスト イベント	はい	いいえ（No）
インパクト フラグ アラート	FMC によって生成されたインパクト アラート	はい	いいえ（No）
ユーザ イベント	ユーザ イベント	はい	いいえ（No）
マルウェア イベント	マルウェア イベント	はい	いいえ（No）
ファイル イベント	ファイル イベント	はい	いいえ（No）
接続イベント	モニタ対象のホストとその他のすべてのホスト間のセッション トラフィックに関する情報	はい	はい

セキュリティ イベントの syslog と eStreamer の比較

一般に、現在 eStreamer に重大な既存イベントがない組織は、セキュリティ イベント データを外部で管理するのに eStreamer ではなく syslog を使用する必要があります。

Syslog	eStreamer
カスタマイズの必要なし	各リリースの変更に対応するには、大幅なカスタマイズと継続メンテナンスが必要
標準（Standard）	専用

Syslog	eStreamer
syslog 標準規格では、データ損失に対する保護はありません（特に UDP を使用している場合）	データ損失に対する保護
デバイスから直接送信	FMC から送信（処理オーバーヘッドが加わる）
ファイルイベントとマルウェアイベント、接続イベント（セキュリティ インテリジェンス イベントを含む）、および侵入イベントをサポートします。	eStreamer サーバストリーミング （2906 ページ）に示されているすべてのイベント タイプをサポートします。
一部のイベントデータは、FMC からのみ送信できます。eStreamer 経由でのみ送信され、syslog 経由では送信されないデータ （2908 ページ）を参照してください。	デバイスから syslog を介して直接送信することができないデータが含まれます。eStreamer 経由でのみ送信され、syslog 経由では送信されないデータ （2908 ページ）を参照してください。

eStreamer 経由でのみ送信され、syslog 経由では送信されないデータ

次のデータは Firepower Management Center からのみ使用可能であるため、デバイスから syslog を介して送信することはできません。

- パケット ログ
- 侵入イベント追加データ イベント

  説明については、eStreamer サーバ ストリーミング （2906 ページ）を参照してください。
- 統計情報と集約イベント
- ネットワーク検出イベント
- ユーザ アクティビティとログイン イベント
- 相関イベント
- ホワイトリスト イベント
- マルウェア イベントの場合：
  - レトロスペクティブな判定
  - 関連する SHA に関する情報がすでにデバイスに同期されている場合を除き、脅威の名前と性質
- 次のフィールド：
  - [Impact] および [ImpactFlag] フィールド

説明については、eStreamer サーバ ストリーミング （2906 ページ）を参照してください。

- [IOC_Count] フィールド

- ほとんどの raw ID と UUID。

  次に例外を示します。

  - 接続イベントの syslog には次のものがあります。FirewallPolicyUUID、FirewallRuleID、TunnelRuleID、MonitorRuleID、SI_CategoryID、SSL_PolicyUUID、および SSL_RuleID
  - 侵入イベントの syslog には、IntrusionPolicyUUID、GeneratorID、および SignatureID が含まれます。

- 以下を含むがこれらに限定されない拡張メタデータ：

  - 氏名、部署、電話番号などの LDAP によって提供されるユーザの詳細。

    syslog では、イベントのユーザ名のみが提供されます。

  - SSL 証明書の詳細などの状態ベースの情報の詳細。

    syslog は、証明書のフィンガープリントなどの基本的な情報を提供しますが、cert CN など、証明書のその他の詳細は提供しません。

  - アプリケーション タグやカテゴリなどの詳細なアプリケーション情報。

    syslog はアプリケーション名のみを提供します。

  一部のメタデータ メッセージには、オブジェクトに関する追加情報も含まれています。

- 地理位置情報

eStreamer イベントタイプの選択

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
機能に応じて異なる	機能に応じて異なる	FMC 7000 & 8000 シリーズ	いずれか（Any）	Admin

eStreamer サーバで送信可能なイベントの [eStreamer イベント設定（eStreamer Event Configuration）]チェックボックス管理。クライアントは、eStreamer サーバに送信する要求メッセージで受信するイベント タイプを具体的に要求する必要があります。詳細については、『*Firepower System Event Streamer Integration Guide*』を参照してください。

マルチドメイン展開では、どのドメインのレベルでも eStreamer のイベント構成を設定できます。ただし、先祖ドメインで特定のイベントタイプが有効になっている場合は、子孫ドメインのそのイベントタイプを無効にすることはできません。

ステップ 1 **[System]** > **[Integration]**を選択します。

ステップ 2 [eStreamer] タブをクリックします。

ステップ 3 [eStreamer イベント設定（eStreamer Event Configuration）] の下で、eStreamer サーバ ストリーミング （2906 ページ）の説明に従って要求元のクライアントに転送するイベントタイプの横にあるチェックボックスをオンまたはオフにします。

ステップ 4 **[保存（Save）]** をクリックします。

eStreamer クライアント通信の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
機能に応じて異なる	機能に応じて異なる	FMC 7000 & 8000 シリーズ	いずれか（Any）	Admin/Discovery Admin

eStreamer がクライアントに eStreamer イベントを送信するには、その前に、eStreamer ページから eStreamer サーバのピア データベースにクライアントを追加しておく必要があります。また、eStreamer サーバによって生成された認証証明書をクライアントにコピーする必要もあります。この手順を完了した後、クライアントが eStreamer サーバに接続できるように eStreamer サービスを再起動する必要はありません。

マルチドメイン展開では、任意のドメインで eStreamer クライアントを作成できます。認証証明書では、クライアントはクライアント証明書のドメインと子孫ドメインからのみイベントを要求することが許可されます。eStreamer 設定ページには、現在のドメインに関連付けられているクライアントのみが表示されるため、証明書をダウンロードまたは取り消す場合は、クライアントが作成されたドメインに切り替えます。

ステップ 1 **[System]** > **[Integration]**を選択します。

ステップ 2 [eStreamer] タブをクリックします。

ステップ 3 [クライアントの作成（Create Client）] をクリックします。

ステップ 4 [ホスト名（Hostname）] フィールドに、eStreamer クライアントを実行しているホストのホスト名または IP アドレスを入力します。

（注） DNS 解決を設定していない場合は、IP アドレスを使用します。

ステップ 5 証明書ファイルを暗号化するには、[Password] フィールドにパスワードを入力します。

ステップ 6 **[Save]** をクリックします。
これで、eStreamer サーバは、ホストが eStreamer サーバ上のポート 8302 にアクセスすることを許可し、クライアント/サーバ認証時に使用する認証証明書を作成します。

ステップ 7 クライアントのホスト名の横にあるファイルのダウンロードアイコン（）をクリックして、証明書ファイルをダウンロードします。

ステップ 8 SSL 認証のためにクライアントが使用する適切なディレクトリに証明書ファイルを保存します。

ステップ 9 クライアントのアクセスを取り消すには、削除するホストの横にある削除アイコン（）をクリックします。

eStreamer サービスを再起動する必要はありません。アクセスはただちに取り消されます。

外部ツールを使用したイベント データの分析の履歴

機能	バージョン	詳細
Cisco Threat Response との統合	6.3（syslog 経由、プロキシ コレクタを使用） 6.4（直接）	Cisco Threat Response の強力な分析ツールを使用し、Firepower 侵入イベント データを他のソースのデータと統合して、ネットワーク上の脅威を統合ビューに表示します。 変更された画面（バージョン 6.4）：[システム（System）] > [統合（Integration）] > [クラウドサービス（Cloud Services）] の新規オプション。 サポートされるプラットフォーム：バージョン 6.3（syslog 経由）または 6.4 を実行している Firepower Threat Defense デバイス

機能	バージョン	詳細
ファイルとマルウェアのイベントの syslog サポート	6.4	完全修飾ファイルおよびマルウェアのイベント データが syslog 経由で管理対象デバイスから送信できるようになりました。 変更された画面：[ポリシー（Policies）] > [アクセス制御（Access Control）] > [アクセス制御（Access Control）] > [ロギング（Logging）] タブ。 サポート対象プラットフォーム：バージョン 6.4 を実行している管理対象のすべてのデバイス
Splunk との統合	すべての 6.x バージョンのサポート	Splunk のユーザは、新しい個別の Splunk アプリケーションである Cisco Firepower App for Splunk を使用してイベントを分析できます。 どの機能を使用できるかは、Firepower のバージョンによって異なります。 Splunk でのイベント分析 （2882 ページ）を参照してください。

機能	バージョン	詳細
Cisco Security Packet Analyzer との統合	6.3	導入された機能：Cisco Security Packet Analyzer にイベントに関連するパケットについてすぐにクエリを実行した後、クリックして Cisco Security Packet Analyzer の結果を調べるか、またはダウンロードして別の外部ツールで分析します。 新規画面： **[システム（System）] > [統合（Integration）] > [パケット アナライザ（Packet Analyzer）]** **[分析（Analysis）] > [詳細（Advanced）] > [パケット アナライザのクエリ（Packet Analyzer Queries）]** 新規メニュー オプション：[ダッシュボード（Dashboard）] ページおよび [分析（Analysis）] メニューのページのイベント テーブルを右クリックしたときの [クエリ パケット アナライザ（Query Packet Analyzer）] のメニュー項目 サポートされるプラットフォーム Firepower Management Center
コンテキスト クロス起動	6.3	導入された機能：イベントを右クリックし、事前に定義されているか、またはカスタム URL ベースの外部リソースの関連情報を検索します。 新規画面：**[分析（Analysis）] > [詳細（Advanced）] > [コンテキスト クロス起動（Contextual Cross-Launch）]** 新規メニュー オプション：[ダッシュボード（Dashboard）] ページおよび [分析（Analysis）] メニュー ページのイベント テーブルを右クリックしたときに表示される複数のオプション サポートされるプラットフォーム Firepower Management Center

機能	バージョン	詳細
接続イベントと侵入イベントの syslog メッセージ	6.3	統合され、簡略化された新しい設定を使用して、完全修飾接続および侵入イベントを外部ストレージおよびツールに syslog 経由で送信する機能。メッセージヘッダーが標準化されてイベント タイプ識別子が組み込まれ、メッセージが小型になりました。これは、不明な値や空の値が含まれたフィールドが省略されるためです。 サポート対象プラットフォーム： • すべての新機能：バージョン 6.3 を実行している FTD デバイス。 • 一部の新機能：バージョン 6.3 を実行している FTD 以外のデバイス。 • 少数の新機能：6.3 よりも前のバージョンを実行しているすべてのデバイス。 詳細については、セキュリティ イベントの syslog メッセージの送信について（2894ページ）のトピックとサブトピックを参照してください。
eStreamer	6.3	eStreamer の内容をホストのアイデンティティ ソースに関する章からこの章に移動し、eStreamer と syslog を比較した概要を追加しました。

第 XXVI 部

Workflows

第 120 章

ワークフロー

以下のトピックでは、ワークフローの使用方法について説明します。

概要：ワークフロー

ワークフローは Firepower Management Center Web インターフェイス上でユーザに合わせて作成された一連のデータ ページで、アナリストはワークフローを使用して、システムで生成されたイベントを評価することができます。

Firepower Management Center では、以下のタイプのワークフローを使用できます。

定義済みワークフロー

システムに付属のプリセット ワークフローです。定義済みのワークフローの編集や削除を行うことはできません。ただし、定義済みワークフローをコピーして、そのコピーをカスタム ワークフローの基礎として使用することができます。

保存済みのカスタム ワークフロー

Firepower Management Center に付属の保存済みカスタム テーブルに基づくカスタム ワークフロー。これらのワークフローは編集、削除、コピーすることができます。

カスタム ワークフロー

特定のニーズに対応するために作成してカスタマイズするワークフロー、またはカスタム テーブルを作成するとシステムによって自動的に生成されるワークフローです。これらのワークフローは編集、削除、コピーすることができます。

通常、ワークフローに表示されるデータは、管理対象デバイスのライセンスおよび展開状況や、データを提供する機能を設定しているかどうかによって異なります。

定義済みワークフロー

以下の項で説明する定義済みワークフローは、システムに付属しているものです。定義済みワークフローを編集または削除することはできません。ただし、定義済みワークフローをコピーして、そのコピーをカスタム ワークフローのベースとして使用することができます。

定義済み侵入イベントのワークフロー

次の表では、Firepower System に備わっている定義済み侵入イベントのワークフローについて説明します。

表 *292 :* 定義済み侵入イベントのワークフロー

ワークフロー名	説明
Destination Port（宛先ポート）	宛先ポートは通常、アプリケーションに関連付けられているため、このワークフローは、通常以上に大量のアラートが発生しているアプリケーションを検出するのに役に立ちます。接続先ポート カラムにより、ネットワーク上に存在してはならないアプリケーションを特定できます。
イベント特定	このワークフローには、2 つの便利な機能があります。頻繁に発生するイベントには、以下のことを示している可能性があります。 • 誤検出 • ワーム • 設定が大幅に間違っているネットワーク 発生頻度の低いイベントは、対象となる攻撃を最も確実に示す証拠であり、特別な注意を必要とします。
優先度および分類によるイベント	このワークフローでは、イベントとタイプのリストをそれぞれのイベントが発生した回数と共にイベントの優先度の順に示します。
接続先に対するイベント	このワークフローでは、攻撃されているホスト IP アドレスや攻撃の本質のハイレベル ビューを提示します。利用可能な場合、攻撃に関与する国に関する情報を確認することもできます。

ワークフロー名	説明
IP 特定	このワークフローは、最も多くのアラートを生成しているホスト IP アドレスを示します。最も多くのイベントが生じているホストは、公開されていて、ワーム タイプのトラフィックを受け取っている（チューニングに適した場所であることを示している）か、あるいはアラートの原因を決定するためにさらに調査が必要です。カウントが最も少ないホストも攻撃の対象となる可能性があるため、調査が必要です。イベント数が少ない場合は、ホストがネットワークに属していないことを示す場合もあります。
影響度と優先度	このワークフローを使用して、影響が大きく、繰り返し発生するイベントをすばやく見つけることができます。報告される影響レベルは、イベントが発生した回数と合わせて表示されます。この情報を使用して、最も頻繁に再発する影響度の高いイベントを特定できます。これがネットワーク上での広範な攻撃の指標となります。
影響度と送信元	このワークフローは、進行中の攻撃の発生源を特定する場合に役立ちます。報告される影響レベルは、イベントに関連付けられている送信元 IP アドレスと合わせて表示されますたとえば、影響レベルが 1 のイベントは、同じ送信元 IP アドレスから繰返し発生している場合、これらは特定された脆弱なシステムであり、送信元 IP アドレスを対象としている攻撃者を示すこともあります。
接続先への影響	このワークフローを使用して、脆弱なコンピュータ上で繰返し発生しているイベントを特定できます。このため、これらのシステムでの脆弱性を指定し、進行中の攻撃を停止できます。
送信元ポート	このワークフローは、最も多くのアラートを生成しているサーバを示します。この情報を使用して、調整が必要なエリアを特定し、注意を要するサーバを決定できます。
送信元と接続先	このワークフローは、高レベルのアラートを共有しているホスト IP アドレスを特定します。リストの先頭のペアは誤検出である可能性がありますが、調整が必要なエリアを特定している場合があります。評価する必要のないリソースを評価するユーザまたはネットワークに属していないホストについては、対象となる攻撃リストの下部にあるペアを確認できます。

定義済みマルウェアのワークフロー

次の表では、Firepower Management Center に備えられた定義済みマルウェアのワークフローについて説明します。定義済みマルウェアのワークフローでは、必ずマルウェア イベントのテーブル ビューを使用します。

表 *293 :* 定義済みマルウェアのワークフロー

ワークフロー名	説明
マルウェア サマリ	このワークフローでは、ネットワーク トラフィック内で検出されたか、または AMP for Endpoints Connector によって検出されたマルウェアのリストを提供します。これらのリストは、それぞれの脅威ごとにグループ化されます。
マルウェア イベント サマリ	このワークフローは、さまざまなマルウェア イベントのタイプおよびサブタイプについて詳細な情報を迅速に提供します。
Hosts Receiving Malware（マルウェアを受信したホスト）	このワークフローは、マルウェアを受信したホスト IP アドレスのリストを、マルウェア ファイルに関連付けられている処理ごとにグループ化して提供します。
Hosts Sending Malware（マルウェアを送信したホスト）	このワークフローは、マルウェアを送信したホスト IP アドレスのリストを、マルウェア ファイルに関連付けられている処理ごとにグループ化して提供します。
Applications Introducing Malware（マルウェアを取り込んだアプリケーション）	このワークフローでは、ファイルを受信したホスト IP アドレスのリストが表示されます。このリストは、受信したファイルの関連したマルウェアの処理によってグループ化されます。

定義済みファイルのワークフロー

次の表では、Firepower Management Center に備えられる定義済みファイル イベントのワークフローについて説明しています。定義済みファイルイベントのワークフローでは、必ずファイル イベントのテーブル ビューを使用します。

表 *294 :* 定義済みファイルのワークフロー

ワークフロー名	説明
File Summary（ファイルの概要）	このワークフローは、さまざまなファイル イベントのカテゴリとタイプ、および関連するすべてのマルウェアの処理について詳細な情報を迅速に提供します。

ワークフロー名	説明
Hosts Receiving Files（ファイルを受信したホスト）	このワークフローは、ファイルを受信したホスト IP アドレスのリストを、これらのファイルに関連付けられているマルウェアの処理ごとにグループ化して提供します。
Hosts Sending Files（ファイルを送信したホスト）	このワークフローでは、ファイルを送信したホスト IP アドレスのリストを表示します。このリストは、これらのファイルの関連したマルウェアの処理によってグループ化されます。

定義済みキャプチャ ファイルのワークフロー

次の表では、Firepower Management Center での定義済みキャプチャ ファイルのワークフローについて説明しています。定義済みキャプチャ ファイルのワークフローは、必ずキャプチャ ファイルのテーブル ビューを使用します。

表 *295* : 定義済みキャプチャ ファイルのワークフロー

ワークフロー名	説明
Captured File Summary（キャプチャ ファイルの概要）	このワークフローは、タイプ、カテゴリ、および脅威のスコアに基づいてキャプチャ ファイルについての詳細な情報を提供します。
Dynamic Analysis Status（動的解析のステータス）	このワークフローでは、ダイナミック分析用に提示されたか否かに基づいて、キャプチャ ファイルの数を表示します。

定義済み接続データのワークフロー

次の表では、Firepower Management Center に備えられる定義済み接続データのワークフローについて説明しています。定義済み接続データ ワークフローでは、必ず接続データのテーブル ビューを使用します。

表 *296* : 定義済み接続データのワークフロー

ワークフロー名	説明
Connection Events（接続イベント）	このワークフローは、基本的な接続および検出されたアプリケーションの情報についての概要ビューを提供します。ユーザはこれを使用して、イベントのテーブル ビューへドリル ダウンすることができます。

ワークフロー名	説明
Connections by Application（接続に基づいたアプリケーション）	このワークフローには、検出された接続の数に基づいて、モニタリング対象のネットワーク セグメントにおける最もアクティブな 10 個のアプリケーションのグラフが含まれています。
Connections by Initiator（接続に基づいた発信側）	このワークフローには、ホストが接続トランザクションを開始した接続の数に基づいて、モニタリング対象のネットワーク セグメントにおける最もアクティブな 10 個のホスト IP アドレスのグラフが含まれています。
Connections by Port（接続に基づいたポート）	このワークフローには、検出された接続の数に基づいて、モニタリング対象のネットワーク セグメントにおける最もアクティブな10個のポートのグラフが含まれています。
Connections by Responder（接続に基づいた応答側）	このワークフローには、ホスト IP が接続トランザクションの応答側であった接続の数に基づいて、モニタリング対象のネットワーク セグメントにおける最もアクティブな 10 個のホスト IP アドレスのグラフが含まれています。
Connections over Time（一定期間の接続）	このワークフローには、モニタリング対象のネットワーク セグメントにおける、一定期間の接続の合計数のグラフが含まれています。

ワークフロー名	説明
Traffic by Application（トラフィックに基づいたアプリケーション）	このワークフローには、送信されたキロバイト数に基づいて、モニタリング対象のネットワーク セグメントにおける最もアクティブな 10 個のアプリケーションのグラフが含まれています。 アプリケーション カウントは、アプリケーション接続と照合した各ディテクタが反映されます。トラフィックを照合したアプリケーション プロトコル、Web アプリケーション、クライアント ディテクタ、または内部ディテクタと、トラフィックがモバイル デバイスから発信されたか、または暗号化セッションの一部かによって、同じアプリケーション セッションがリスト内に複数回表示される場合があります。アプリケーションがクライアント フローに表示されていても特定のクライアント ディテクタがない場合は、汎用クライアントが報告される場合があります。 たとえば、同じ YouTube セッションが（YouTube Web アプリケーション ディテクタと照合したため）**YouTube** と（内部 YouTube ディテクタがクライアント セッション内に通常観られる特性と照合したため）**YouTube client** として表示される場合があります。 接続イベント内の情報とネットワークのネットワーク マップを使用して特定のアプリケーション接続の他のコンテキストを特定します。
トラフィックに基づいた発信側（Traffic by Initiator）	このワークフローには、各アドレスから送信されたキロバイト数の合計に基づいて、モニタリング対象のネットワーク セグメントにおける最もアクティブな 10 個のホスト IP アドレスのグラフが含まれています。
Traffic by Port（トラフィックに基づいたポート）	このワークフローには、送信されたキロバイト数に基づいて、モニタリング対象のネットワーク セグメントにおける最もアクティブな 10 個のポートのグラフが含まれています。
Traffic by Responder（トラフィックに基づいた応答側）	このワークフローには、各アドレスが受信したキロバイト数の合計に基づいて、モニタリング対象のネットワーク セグメントにおける最もアクティブな 10 個のホスト IP アドレスのグラフが含まれています。
Traffic over Time（一定期間のトラフィック）	このワークフローには、モニタリング対象のネットワーク セグメントにおける、一定期間に送信されたキロバイト数の合計のグラフが含まれています。

ワークフロー名	説明
Unique Initiators by Responder（一意の発信側に基づいた応答側）	このワークフローには、各アドレスに接続した一意の発信側の数に基づいて、モニタリング対象のネットワーク セグメントにおける最もアクティブな応答側の 10 個のホスト IP アドレスのグラフが含まれています。
Unique Responders by Initiator（一意の応答側に基づいた発信側）	このワークフローには、アドレスにコンタクトする一意レスポンダの数に基づく、監視対象のネットワーク セグメントでの 10 個の最もアクティブな開始ホスト IP アドレスのグラフが含まれています。

定義済みセキュリティ インテリジェンスのワークフロー

次の表では、Firepower Management Center に備えられている定義済みセキュリティ インテリジェンスのワークフローについて説明しています。定義済みセキュリティインテリジェンスのワークフローでは、必ずセキュリティ インテリジェンス イベントのテーブル ビューを使用します。

表 *297*: 定義済みセキュリティ インテリジェンスのワークフロー

ワークフロー名	説明
Security Intelligence Events（セキュリティ インテリジェンス イベント）	このワークフローは、基本的なセキュリティインテリジェンスおよび検出されたアプリケーションの情報についての概要ビューを提供します。ユーザはこれを使用して、イベントのテーブル ビューへドリル ダウンすることができます。
Security Intelligence Summary（キュリティ インテリジェンスの概要）	このワークフローは、セキュリティ インテリジェンス イベントのワークフローと同じものですが、セキュリティ インテリジェンス サマリ ページから始まり、カテゴリや数ごとにセキュリティ インテリジェンス イベントのみのリストを表示します。
セキュリティ インテリジェンスと DNS 詳細	このワークフローは、セキュリティ インテリジェンス イベントのワークフローと同じものですが、DNS 詳細のあるセキュリティ インテリジェンス ページから始まり、カテゴリや DNS 関連特性ごとにセキュリティ インテリジェンス イベントのリストを表示します。

定義済みホストのワークフロー

次の表では、ホスト データと共に使用できる定義済みワークフローについて説明します。

表 *298* : 定義済みホストのワークフロー

ワークフロー名	説明
Hosts（ホスト）	このワークフローには、ホストのテーブル ビューが含まれており、その後にホスト ビューが続きます。ホスト テーブルに基づくワークフロー ビューでは、ホストに関連付けられているすべての IP アドレスのデータを容易に表示できます。
オペレーティング システム サマリ（Operating System Summary）	このワークフローを用いて、ネットワーク上で使用中のオペレーティング システムを分析できます。

定義済み侵害の兆候のワークフロー

次の表では、IOC（侵害の兆候）と共に使用できる定義済みワークフローについて説明します。

表 *299* : 定義済み侵害の兆候のワークフロー

ワークフロー名	説明
ホストの侵害の兆候	このワークフローは、数とカテゴリごとにグループ化した IOC データのサマリー ビューから始まり、さらにサマリ データをイベント タイプごとに分割した詳細ビューを表示します。 [分析（Analysis）] > [ホスト（Hosts）] メニューからこのワークフローにアクセスします。
ホストごとの侵害の兆候	このワークフローを使用して、最も侵害する可能性の高いネットワーク上のホストを判断できます（IOCデータに基づく）。 [分析（Analysis）] > [ホスト（Hosts）] メニューからこのワークフローにアクセスします。
ユーザの侵害の兆候	このワークフローは、数とカテゴリごとにグループ化した IOC データのサマリー ビューから始まり、さらにサマリ データをイベント タイプごとに分割した詳細ビューを表示します。 [分析（Analysis）] > [ユーザ（Users）] メニューからこのワークフローにアクセスします。

ワークフロー名	説明
ユーザごとの侵害の兆候	このワークフローを使用して、侵害に関与している可能性が最も高いネットワーク上のユーザを判断します（IOC データに基づく）。 [分析（Analysis）] > [ユーザ（Users）] メニューからこのワークフローにアクセスします。

定義済みアプリケーション ワークフロー

次の表では、アプリケーションデータと共に使用できる定義済みワークフローについて説明しています。

表 *300*：定義済みアプリケーション ワークフロー

ワークフロー名	説明
Application Business Relevance（アプリケーションのビジネスの関連性）	このワークフローを使用して、ネットワーク上で実行中のそれぞれ予想されるビジネスとの関連性レベルのアプリケーションを分析できます。そのため、ネットワーク リソースが適切に使用されているかを監視できます。
アプリケーション カテゴリ	このワークフローを使用して、ネットワーク上で各カテゴリの実行中のアプリケーションを分析できます（電子メール、検索エンジン、ソーシャルネットワーキングなど）。そのため、ネットワーク リソースが適切に使用されているかを監視できます。
アプリケーションのリスク	このワークフローを使用して、ネットワーク上でそれぞれ予想されるセキュリティ リスク レベルの実行中のアプリケーションを分析できます。このため、ユーザのアクティビティの考えられるリスクを予想し、適切なアクションを取ることできます。
アプリケーション サマリ	このワークフローを使用して、ネットワークのアプリケーションや関連するホストに関する詳細情報を取得できます。このため、ホストのアプリケーションのアクティビティを正確に調べることができます。
アプリケーション	このワークフローを使用して、ネットワーク上の実行中のアプリケーションを分析できます。このため、ネットワークの使用状況の概要を取得できます。

定義済みアプリケーション詳細ワークフロー

次の表では、アプリケーションの詳細とクライアントデータと共に使用できる定義済みワークフローについて説明しています。

表 *301* : 定義済みアプリケーション詳細ワークフロー

ワークフロー名	説明
Application Details（アプリケーションの詳細）	このワークフローを用いて、ネットワーク上のクライアント アプリケーションをさらに詳しく分析することができます。また、このワークフローでは、クライアント アプリケーションのテーブル ビューを表示し、その後ホスト ビューを表示します。
Clients	このワークフローには、クライアント アプリケーションのテーブル ビューと、その後にホスト ビューが含まれます。

定義済みサーバのワークフロー

次の表では、サーバ データと共に使用できる定義済みワークフローについて説明します。

表 *302* : 定義済みサーバのワークフロー

ワークフロー名	説明
Network Applications by Count（カウントに基づいたネットワーク アプリケーション）	このワークフローを使用して、ネットワーク上で最も多く使用されるアプリケーションを分析できます。
ヒット別ネットワーク アプリケーション	このワークフローを使用して、ネットワーク上で最もアクティブなアプリケーションを分析できます。
サーバの詳細	このワークフローを使用して、ベンダや検出されたサーバ アプリケーション プロトコルのバージョンを詳細に分析できます。
サーバ	このワークフローには、アプリケーションのテーブル ビューと、その後にホスト ビューが含まれます。

定義済みホスト属性のワークフロー

次の表では、ホスト属性データと共に使用できる定義済みワークフローについて説明します。

表 *303 :* 定義済みホスト属性のワークフロー

ワークフロー名	説明
Attributes（属性）	このワークフローを使用して、ネットワーク上のホスト IP アドレスやホスト ステータスを監視できます。

定義済み検出イベントのワークフロー

次の表では、検出データとアイデンティティ データの表示に使用できる定義済みワークフローについて説明しています。

表 *304 :* 定義済み検出イベント ワークフロー

ワークフロー名	説明
Discovery Events（ディスカバリ イベント）	このワークフルーでは、テーブル ビュー形式の検出イベント詳細リストが提示され、その次にホスト ビューが提示されます。

定義済みユーザ ワークフロー

次の表では、ユーザ検出データとユーザ アイデンティティ データの表示に使用できる定義済みワークフローを説明します。

表 *305 :* 定義済みユーザ ワークフロー

ワークフロー名	説明
アクティブ セッション（Active Sessions）	このワークフローでは、ユーザ ID ソースによって収集されるアクティブ セッションが表示されます。
Users	このワークフローでは、ユーザ ID ソースによって収集されるユーザ情報リストが表示されます。

定義済み脆弱性のワークフロー

次の表では、Firepower Management Center に備えられている定義済み脆弱性のワークフローについて説明します。

表 *306* : 定義済み脆弱性のワークフロー

ワークフロー名	説明
脆弱性（Vulnerabilities）	このワークフローを使用して、ネットワーク上で検出されたホストに適用するこれらのアクティブな脆弱性のみのテーブル ビューなど、データベース内の脆弱性を検討できます。このワークフローにより脆弱性詳細ビューが提供され、これには制約に適合するそれぞれの脆弱性に関する詳細な説明が含まれています。

定義済みのサードパーティ脆弱性のワークフロー

次の表では、Firepower Management Centerに備えられた定義済みのサードパーティ脆弱性のワークフローについて説明します。

表 *307* : 定義済みのサードパーティ脆弱性のワークフロー

ワークフロー名	説明
IP アドレスごとの脆弱性	このワークフローを使用して、監視対象のネットワーク上のホスト IP アドレスごとに検出されたサードパーティの脆弱性の数をすぐに確認できます。
送信元ごとの脆弱性	このワークフローを使用して、QualysGuard Scanner などサードパーティの脆弱性の送信元ごとに検出されたサードパーティの脆弱性の数をすぐに確認できます。

定義済み相関ワークフロー、ホワイト リスト ワークフロー

相関データ、ホワイト リスト イベント、ホワイト リスト違反、修復ステータス イベントのそれぞれのタイプには、定義済みワークフローがあります。

表 *308* : 定義済み相関ワークフロー

ワークフロー名	説明
Correlation Events（相関イベント）	このワークフローには、相関イベントのテーブル ビューが含まれています。
ホワイト リスト イベント（White List Events）	このワークフローには、ホワイト リスト イベントのテーブル ビューが含まれています。
ホスト違反数（Host Violation Count）	このワークフローには、少なくとも 1 つのホワイト リストに違反しているすべてのホスト IP アドレスのリストを示す一連のページが表示されます。

ワークフロー名	説明
ホワイト リスト違反（White List Violations）	ワークフローには、すべての違反を示すホワイトリスト違反のテーブル ビューも含まれ、最後に検出された違反がリストの最上部に示されます。テーブル内の各列には、検出された違反が 1 つずつ表示されます。
ステータス（Status）	このワークフローには、修復ステータスのテーブル ビューを含み、違反したポリシー名、適用された修復名や修復状況が表示されています。

定義済みのシステムのワークフロー

Firepower System には、監査イベントやヘルスイベントなどのシステム イベントなど、いくつかの追加のワークフロー、ルール更新インポート、アクティブ スキャンの結果をリストにしたワークフローが提供されています。

表 *309* : 追加の定義済みワークフロー

ワークフロー名	説明
Audit Log（監査ログ）	このワークフローでは、監査イベントをリストした監査ログのテーブル ビューを含みます。
ヘルス イベント（Health Events）	このワークフローでは、ヘルス監視ポリシーによりトリガーされるイベントを表示します。
ルール更新インポート ログ（Rule Update Import Log）	このワークフローは、成功したルールの更新インポートと失敗したルールの更新インポートに関する情報をリストしたテーブル ビューを含みます。
スキャン結果（Scan Results）	このワークフローには、それぞれ完了したスキャンをリストしたテーブル ビューを含みます。

カスタム テーブル ワークフロー

カスタム テーブルの機能を使用して、複数のイベント タイプのデータを使用するテーブルを作成することができます。これにより、たとえば、ユーザが侵入イベントのデータとディスカバリ データを関連付けるテーブルおよびワークフローを作成して、重要なシステムに影響を及ぼすイベントを簡単に検索できるようになるため、役立ちます。

カスタムテーブルを作成すると、システムは自動的にワークフローを作成します。このテーブルを使って関連するイベントを表示することができます。ワークフローの機能は、使用する

テーブルのタイプによって異なります。たとえば、侵入イベントテーブルに基づいたカスタムテーブルのワークフローは、必ずパケットビューで終了します。ただし、検出イベントに基づいたカスタム テーブルのワークフローは、必ずホスト ビューで終了します。

事前定義のイベント テーブルに基づいたワークフローとは異なり、カスタム テーブルに基づいたワークフローには、他のタイプのワークフローへのリンクがありません。

ワークフローの使用

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Maint/Any Security Analyst（ワークフローに応じて異なります）

ステップ 1 ワークフローの選択 （2933 ページ）に記載されているように、適切なメニューパスとオプションを選択します。

ステップ 2 現在のワークフロー内で移動します。

- 選択したイベント データタイプで利用可能な列をすべて表示するには、テーブル ビュー ページを使用します。テーブル ビュー ページの使用 （2941 ページ）を参照してください。
- 選択したイベントデータタイプで利用可能な列のサブセットを表示するには、ドリルダウン ページを使用します。ドリルダウン ページの使用 （2940 ページ）を参照してください。
- ワークフローの次のページの対応する行を表示するには、青い下矢印アイコン（  ）をクリックします。
- マルチページ ワークフローのページ間を移動するには、各ページの下部にあるツールを使用します。ワークフロー ページのトラバーサル ツール （2937 ページ）を参照してください。
- 別のタイプのイベントに対してワークフロー内で適用された同じ制約を表示するには、[移動先（Jump to）] をクリックし、ドロップダウンリストからイベント ビューを選択します。

ステップ 3 現在のワークフローの表示を変更します。

- ページ上で 1 つ以上の行のチェックボックスにマークを付けて、処理を反映させる行を表示し、ページの下部にあるいずれかのボタン（[表示（View）] ボタンなど）をクリックして、選択したすべての行に対してそのアクションを実行します。
- 行の上部にあるチェックボックスにマークを付けて、ページ上のすべての行を選択し、ページの下部にあるいずれかのボタン（[表示（View）] ボタンなど）をクリックして、ページ上のすべての行に対してそのアクションを実行します。

- 非表示にする列ヘッダーの閉じるアイコン（ ）をクリックして、表示する列を制約します。表示されるポップアップ ウィンドウで、[適用（Apply）] をクリックします。

  ヒント 他のカラムを表示または非表示にするには、[適用（Apply）] をクリックする前に、該当するチェック ボックスをオンまたはオフにします。無効にしたカラムをビューに戻すには、展開の矢印をクリックして検索制約を展開し、[無効にされたカラム（Disabled Columns）] の下のカラム名をクリックします。

- 選択したフィールドに対して選択した値でデータ ビューを制約します。詳細については、イベント ビューの制約（2960ページ）および複合イベント ビューの制約（2962ページ）を参照してください。
- イベント ビューの時間の制約を変更します。ページの右上隅に表示される日付の範囲は、ワークフローに含めるイベントの時間範囲を設定します。詳細については、イベント時間の制約（2952ページ）を参照してください。

  （注） イベント ビューを時間によって制約している場合は、（グローバルかイベント固有かに関係なく）アプライアンスに設定されている時間枠の外で生成されたイベントが、イベント ビューに表示されます。アプライアンスに対してスライドする時間枠を設定した場合でも、この状況が発生することがあります。

- データを列でソートするには、列の名前をクリックします。ソート順序を反転させるには、もう一度列の名前をクリックします。矢印のアイコンは、データのソート基準になっている列、およびソートが昇順である（ ）か、または降順である（ ）かを表します。
- ワークフロー ページのリンクをクリックして、アクティブな制約を使用しているページを表示します。ワークフロー ページのリンクは、事前定義されたワークフロー テーブル ビュー、およびドリルダウン ページの左上隅の、イベントの上で、ワークフロー名の下に示されます。

ステップ 4 現在のワークフロー内の追加データを表示します。

- ファイルのトラジェクトリ マップを新しいウィンドウで表示するには、ファイル名と SHA-256 ハッシュ値の列のネットワーク ファイル トラジェクトリ アイコンをクリックします。アイコンは、ファイル ステータスによって異なります。ファイル トラジェクトリ アイコン（2938ページ）を参照してください。
- IP アドレスに関連付けられたホスト プロファイルのポップアップ ウィンドウを表示するには、IP アドレスの列のホスト プロファイル アイコンをクリックします。アイコンは、ファイル ステータスによって異なります。ホスト プロファイルのアイコン（2938 ページ）を参照してください。
- ファイルに関連付けられた最も高い脅威スコアの動的分析サマリー レポートを表示するには、いずれかの脅威スコア列の脅威スコア アイコンをクリックします。アイコンは、ファイルの最も高い脅威スコアによって異なります。脅威スコア アイコン（2939 ページ）を参照してください。
- ユーザ プロファイル情報を表示するには、いずれかのユーザ ID 列でユーザ アイコン（ 、または侵害の兆候に関連付けられたユーザの場合は ）をクリックします。ユーザ アイコンは、そのユーザがデータベースにない場合（つまり、AMP for Endpoints Connector ユーザの場合）は淡色表示されます。

- サードパーティの脆弱性の脆弱性詳細を表示するには、いずれかのサードパーティの脆弱性のID列の脆弱性アイコン（  ）をクリックします。
- 集約データ ポイントを表示する場合は、ポインタをフラグ アイコンの上に合わせて国名を表示します。
- 個々のデータ ポイントを表示する場合は、フラグアイコンをクリックして、位置情報 （2942 ページ）に記載されている地理位置情報詳細を表示します。

ステップ 5 別のワークフローに移動します。

別のワークフローを使用して同じイベント タイプを表示するには、ワークフローのタイトルの横にある（**ワークフローの切り替え**）をクリックして、使用するワークフローを選択します。スキャン結果には別のワークフローを使用**できない**ことに注意してください。

ユーザ ロールによるワークフローへのアクセス

ワークフローへのアクセスはユーザのロールにより異なります。詳細については、次の表を参照してください。

ユーザ ロール	アクセス可能なワークフロー
管理者（Administrator）	すべてのワークフローにアクセスできます。また、Administrator は監査ログ、スキャン結果、およびルール更新のインポート ログにアクセスできる唯一のユーザです。
メンテナンスユーザ	ヘルス イベントにアクセスできます。
セキュリティ アナリストとセキュリティ アナリスト（読み取り専用）	侵入、マルウェア、ファイル、接続、検出、脆弱性、相関、ヘルスワークフローにアクセスできます。

ワークフローの選択

Firepower システムには、次の表に記載されているデータのタイプに対して、事前定義のワークフローが用意されています。

表 *310 :* ワークフローを使用する機能

機能	メニュー パス	オプション
侵入イベント	[Analysis] > [Intrusions]	Event Reviewed Events Clipboard Incidents
マルウェア イベント	[Analysis] > [Files]	Malware Events
ファイル イベント	[Analysis] > [Files]	File Events
キャプチャ ファイル	[Analysis] > [Files]	Captured Files
接続イベント	[Analysis] > [Connections]	Event
セキュリティ インテリジェンス イベント	[Analysis] > [Connections]	Security Intelligence Events
ホスト イベント	[Analysis] > [Hosts]	Network Map Hosts Indications of Compromise Applications Application Details Servers Host Attributes Discovery Events
ユーザ イベント	[分析（Analysis）]>[ユーザ（Users）]	アクティブ セッション（Active Sessions） ユーザ アクティビティ Users 侵害の兆候
脆弱性イベント	[分析（Analysis）]>[ホスト（Hosts）]	脆弱性 Third-Party Vulnerabilities
相関イベント	[Analysis] > [Correlation]	Correlation Events White List Events White List Violations Status

機能	メニュー パス	オプション
監査イベント	[System] > [Monitoring]	Audit
ヘルス イベント	[ヘルス（Health）] > [イベント（Events）]	適用対象外
ルール更新のインポート ログ	[System] > [Updates]	n/a
スキャン結果	[ポリシー（Policies）] > [アクション（Actions）] > [スキャナ（Scanners）]	適用対象外

上記の表に記載されているいずれかの種類のデータを表示する場合、そのデータのデフォルトのワークフローの最初のページにイベントが表示されます。イベント ビューの設定項目を設定することによって、別のデフォルト ワークフローを指定することができます。ワークフローへのアクセス権限は、ユーザの役割によって異なります。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

関連トピック

イベント ビュー設定の設定 （43 ページ）

ワークフローのページ

ワークフローのタイプによってデータは異なりますが、すべてのワークフローで共通の機能セットを共有しています。ワークフローには、数種類のページを含めることができます。ユーザがワークフローのページ上で実行できるアクションは、ページのタイプによって異なります。

ワークフローのドリル ダウンのページとテーブル ビューのページを使用すれば、データのビューをすばやく絞り込むことができるため、分析にとって重要なイベントに集中できます。テーブル ビューのページとドリルダウンのページの両方で、ユーザが表示するイベント セットに制約を適用したり、ワークフローをナビゲートしたりするために使用できる機能が多数サポートされています。ドリルダウン ページ、またはワークフロー内のテーブル ビューでデータを表示する場合、ソートに使用できる任意のカラムに基づいてデータを昇順または降順でソートできます。1 つのワークフローのページに表示できるイベント数よりも多くのイベントがデータベースに含まれている場合は、ページの下部にあるリンクをクリックして、さらにイベントを表示できます。これらのリンクの1つをクリックすると時間枠が自動的に一時停止されるため、同じイベントが2回表示されません。準備ができたら時間枠の一時停止を解除できます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

テーブル ビュー

ページがデフォルトで有効になっている場合、テーブル ビューには、ワークフローのベースとなるデータベースの各フィールドに対するカラムが含まれています。

テーブル ビューでカラムを無効にし、それによって同じ行が複数生成される場合、Firepower システムによってイベント ビューに [カウント（Count）] カラムが追加されます。テーブル ビューページで1つの値をクリックすると、その値によって制約することができます。カスタム ワークフローを作成する場合は、[テーブル ビューの追加（Add Table View）] をクリックしてテーブル ビューを追加します。

ドリルダウン ページ

ドリルダウン ページは、通常テーブル ビューのページに移動する前に調査対象を絞り込むために使用する中間ページです。ドリルダウンページには、データベースで使用できるカラムのサブセットが含まれています。

たとえば、検出イベントのドリルダウン ページには、[IP アドレス（IP Address）]、[MAC アドレス（MAC Address）]、および [時刻（Time）] カラムだけが含まれています。また、侵入イベントのドリルダウン ページには、[優先順位（Priority）]、[影響フラグ（Impact Flag）]、[インラインの結果（Inline Result）]、および [メッセージ（Message）] カラムが含まれています。

ドリルダウンページを使用すれば、表示するイベントの範囲を絞り込んだり、ワークフローで先へ進んだりできます。ドリルダウンページで1つの値をクリックすると（たとえば、その値によって制約を行い、ワークフローの次のページへ進むと）、選択した値に一致するイベントに絞り込むことができます。ドリルダウンページで値をクリックした場合、次のページがテーブル ビューであっても、値が存在するカラムは無効になりません。事前定義のワークフローのドリルダウン ページには、必ず [カウント（Count）] カラムがあることに注意してください。カスタム ワークフローを作成する場合は、[ページの追加（Add Page）] をクリックしてドリルダウン ページを追加します。

グラフ

接続データに基づくワークフローには、グラフ ページ（接続グラフとも呼ばれる）を含めることができます。

たとえば接続グラフには、一定期間にシステムで検出された接続の数を示す線グラフを表示することができます。一般的に接続グラフは、ドリルダウン ページと同様に、ユーザが調査対象を絞り込むために使用する中間ページです。

最終ページ

ワークフローの最終ページは、ワークフローがベースとするイベントのタイプによって異なります。

- ホスト ビューとは、アプリケーション、アプリケーションの詳細、検出イベント、ホスト、侵害の兆候（IOC）、サーバ、ホワイトリスト違反、ホスト属性、またはサードパーティ製の脆弱性に基づいたワークフローの最終ページです。このページからホスト プロ

ファイルを表示することにより、ユーザは、複数のアドレスを持つホストに関連付けられているすべての IP アドレス上のデータを簡単に表示することができます。

- ユーザの詳細ビューとは、ユーザ、ユーザアクティビティ、およびユーザの侵害の兆候に基づいたワークフローの最終ページです。
- 脆弱性の詳細ビューとは、Cisco の脆弱性に基づいたワークフローの最終ページです。
- パケット ビューは、侵入イベントに基づいたワークフローの最終ページです。

他の種類のイベント（監査ログイベントやマルウェアイベントなど）に基づいたワークフローには、最終ページがありません。

ワークフローの最終ページで詳細セクションを展開して、ワークフローの進行中に絞り込んだセットの各オブジェクトについて、具体的な情報を表示することができます。Web インターフェイスでは、ワークフローの最終ページに制約が表示されませんが、以前に設定した制約は保持されており、データのセットに適用されます。

ワークフロー ページのナビゲーション ツール

ワークフローのページには、ページ間の移動と、イベントの分析中に表示する情報の選択を容易にする視覚的なキューが用意されています。

ワークフロー ページのトラバーサル ツール

ワークフローに複数のデータ ページが含まれている場合は、各ページの下部にワークフロー内のページ数と、ページ間を移動するために使用できるツールが表示されます。これらのツールを次の表に示します。

表 *311* : ワークフロー ページのトラバーサル ツール

ページのトラバーサル ツール	操作
ページ番号 （別のページを表示するには、表示する番号を入力して Enter キーを押します。）	別のページを表示する
>	次のページを表示する
<	前のページを表示する
>|	最後のページに移動する
|<	最初のページに移動する

ファイル トラジェクトリ アイコン

ワークフロー ページで、新しいウィンドウにファイルのトラジェクトリ マップを表示する機会があるときは、ネットワーク トラジェクトリ アイコンが表示されます。このアイコンは、ファイルのステータスによって変わります。

表 *312*：ファイル トラジェクトリ アイコン

ファイル トラジェクトリ アイコン	ファイル ステータス
	正常（Clean）
	マルウェア
	カスタム検出
	不明
	使用不可

ホスト プロファイルのアイコン

ワークフロー ページでは、IP アドレスに関連付けられたホスト プロファイルをポップアップ ウィンドウで表示でき、ホスト プロファイル アイコンが表示されます。ホスト プロファイルのアイコンがグレー表示になっている場合は、ネットワーク マップ内にそのホストが存在できないため、ホスト プロファイルを表示できません（`0.0.0.0` など）。このアイコンは、ホストのステータスによって異なって表示されます。

表 *313*：ホスト プロファイルのアイコン

ホスト プロファイルのアイコン	ホスト ステータス
	ホストは潜在的に危険にさらされているとタグ付けされていません。
	ホストは、トリガーされた侵害の兆候（IOC）ルールによって潜在的に危険にさらされているとタグ付けされています。
	ブラックリスト化されています（セキュリティ インテリジェンス データに基づいて、トラフィック フィルタリングを実行している場合にのみ表示されます）。

ホスト プロファイルのアイコン	ホスト ステータス
	ブラックリスト化され、モニタに設定されています（セキュリティ インテリジェンス データに基づいて、トラフィック フィルタリングを実行している場合にのみ表示されます）。

脅威スコア アイコン

ワークフローページで、ファイルに関連付けられているスコアが最も高い脅威に関する動的分析サマリ レポートを表示すると、脅威スコア アイコンが表示されます。このアイコンは、ファイルの最も高い脅威スコアに応じて異なります。

表 *314*：脅威スコア アイコン

脅威スコア アイコン	脅威スコア レベル
	Low
	中
	高
	非常に高い（Very high）

ユーザ アイコン

ワークフロー ページで、ユーザ名に関連付けられているユーザ ID がポップアップ ウィンドウで表示されると、同時にユーザ アイコンも表示されます。

表 *315*：ユーザ アイコン

ユーザ アイコン	ユーザ ステータス
	ユーザは侵害の兆候に関連付けられていません。
	ユーザは 1 つ以上の侵害の兆候に関連付けられています。

ワークフロー ツールバー

ワークフローの各ページには、関連する機能へすばやくアクセスするためのツールバーがあります。次の表で、ツールバー上の各リンクについて説明します。

表 *316 :* ワークフロー ツールバーのリンク

機能	説明
Bookmark This Page	後でそのページに戻れるように、現在のページをブックマークします。ブックマークすると、表示中のページに適用されている制約が取得され、データがまだ存在している場合は後で同じデータに戻ることができます。
レポート作成者	現在制約されているワークフローを選択基準として使用して、レポート デザイナを開きます。
ダッシュボード	現行のワークフローに関連するダッシュボードを開きます。たとえば、[接続イベント（Connection Events）] ワークフローは [接続サマリ（Connection Summary）] ダッシュボードと関連付けられています。
ブックマークの表示	ユーザが選択できる、保存したブックマークのリストを表示します。
検索（Search）	[Search] ページが表示され、ここでワークフローのデータについて高度な検索を実行することができます。下向きの矢印アイコンをクリックし、保存済みの検索を選択して使用することもできます。

関連トピック

イベント ビューからのレポート テンプレートの作成 （2780 ページ）
ダッシュボードについて （321 ページ）
イベントの検索 （2967 ページ）
ブックマーク （2964 ページ）
ブックマークの作成 （2965 ページ）
ブックマークの表示 （2965 ページ）

ドリルダウン ページの使用

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Maint/Any Security Analyst（ワークフローに応じて異なります）

ステップ 1 「ワークフローを使用する機能」の説明に従って、適切なメニュー パスとオプションを選択してワークフローにアクセスします。

ステップ 2 すべてのワークフローで、次のオプションを選択できます。

- 特定の値に制限して、次のワークフロー ページにドリルダウンするには、行内の値をクリックします。この処理はドリルダウン ページでのみ可能でることに注意してください。テーブルの行内の値をクリックしても、テーブル ビューが制約されるだけで、次のページにはドリル ダウンしません。
- いくつかのイベントによって制約したまま次のワークフロー ページにドリルダウンするには、次のワークフロー ページに表示させるイベントの横のチェック ボックスを選択し、[表示（View）] をクリックします。
- 現在の制限を維持して次のワークフロー ページにドリルダウンするには、[すべて表示（View All）] をクリックします。

ヒント テーブル ビューでは、必ずページ名に「Table View」が含まれます。

テーブル ビュー ページの使用

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Maint/Any Security Analyst（ワークフローに応じて異なります）

テーブル ビュー ページには、ドリルダウン、ホスト ビュー、パケット ビュー、脆弱性の詳細ページでは利用できない機能が用意されています。これらの機能は次のように使用します。

ステップ 1 ワークフローの選択 （2933 ページ）の説明に従って、適切なメニュー パスとオプションを選択してワークフローにアクセスします。

ステップ 2 ワークフローの名前の下に表示されるワークフロー パスからテーブル ビューを選択します。

ステップ 3 必要に応じて、次に示す機能を使用してテーブル ビュー内に配置したり、移動したりします。

- 無効なカラムのリストを表示するには、[検索制約（Search Constraints）] の展開矢印（▶）をクリックします。
- 無効なカラムのリストを非表示するには、[検索制約（Search Constraints）] の折りたたみ矢印（◀）をクリックします。

- 無効になったカラムをイベント ビューに戻すには、[検索制約（Search Constraints）] の展開アイコン（）をクリックして検索制約を展開し、[無効カラム（Disabled Columns）] の下にあるカラム名をクリックします。
- カラムを表示または非表示（無効）にするには、各カラム名の横にあるクリア アイコン（）をクリックします。表示されるポップアップ ウィンドウで、該当するチェックボックスをオンまたはオフにして、どのカラムを表示するかを指定し、[適用（Apply）] をクリックします。

位置情報

地理位置情報機能によって、ルート可能なIPアドレスの地理的な送信元についてのデータ（国や大陸など）が提供されます。この情報は、イベント、資産のプロファイル、コンテキストエクスプローラ、ダッシュボードやその他の分析ツールで使用できます。

（注） 国間を移動するモバイルデバイスやその他のホストが検出された場合、システムは特定の国ではなく大陸名を報告する可能性があります。

地理位置情報データを使用してネットワーク トラフィックをフィルタできます。たとえば、接続の発信元または終端が、組織と関連性のない国であるかどうかを判別できます。インライン展開では、これらの接続をブロックするか、またはレート制限を行うことができます。

地理位置情報データはシステムの地理位置情報データベース（GeoDB）内に保存されます。シスコでは、GeoDB の定期的な更新を提供しています。[概要（About）] ページ（**[ヘルプ（Help）] > [概要（About）]**）に GeoDB の現在の更新バージョンが表示されています。

GeoDB の更新を許可する場合、Firepower Management Center Web インターフェイスで小さな国旗のアイコンと ISO 国番号をクリックして特定の IP アドレスに関する地理位置情報の詳細を取得することができます。地理情報の詳細情報（2943ページ）を参照してください。また、サードパーティのマップ ツールを使用して、検出された場所を特定することもできます。GeoDB を更新しない場合、これらの詳細情報は取得できません。

[接続のサマリ（Connection Summary）] ダッシュボードなど、集約的な地理位置情報から詳細の地理位置情報を表示することはできません。

関連トピック

ネットワーク条件 （471 ページ）
地理位置情報オブジェクト （534 ページ）
相関ポリシーとルールの概要 （2697 ページ）
トラフィック プロファイル条件 （2743 ページ）
地理位置情報データベース（GeoDB）の更新 （183 ページ）

地理情報の詳細情報

可用性に応じて、[地理情報の詳細（Geolocation Details）] ページに多数のフィールドが表示される場合があります。次の表で、これらのフィールドの情報について示します。（情報がないフィールドは表示されません。）

表 *317 :* 地理情報の詳細フィールド

フィールド	内容
Country	ホスト IP アドレスに関連付けられている国が国旗とともに示されます。大陸はカッコ内に表示されます。例：`United States (North America)`、`Equatorial Guinea (Africa)`
Region	ホストが存在する国の州、県、またはその他の小区域。例：`VA`、`35`
City	ホストが存在する市。例：`Seattle`、`Fukuoka`
Postal Code	ホストが存在する地域の郵便番号。例：`361000`、`90210`
Latitude/Longitude	ホストの場所の正確な座標。例：`40.0375, -76.1053`、`53.4050, -0.5484`
Maps	外部のマッピング サイト（Google Maps、Yahoo Maps、Bing Maps、OpenStreetMap など）へのリンク。ホストのおよその位置のコンテキスト マップを表示するには、リンクをクリックします。
Timezone	ホストの場所のタイム ゾーン（該当する場合には夏時間が示されます）。例：`GMT+8:00`、`GMT-4:00 (In DST)`
ASN	ホスト IP アドレスに関連付けられている自律システム番号（ASN）、およびその ASN に関する追加情報。例：`14618 (Amazon.com Inc.)`、`4837 (Cncgroup China169 Backbone)`
ISP	ホストの IP アドレスに関連付けられているインターネット サービス プロバイダ（ISP）。例：`Atlantic Broadband`、`China Unicom Ip Network`
Home/Business	ホストの接続が個人または会社のどちらの目的であるかを示します。
Organization	ホストの IP アドレスに関連付けられている組織。例：`Amazon.com`、`Bank of America`
Domain Name	ホストの IP アドレスに関連付けられているドメイン名。例：`amazonaws.com`、`xmcnc.net`

フィールド	内容
Connection Type	ホストの IP アドレスに関連付けられている接続タイプ。例：`Broadband`、`DSL`
Proxy Type	使用するプロキシのタイプ。例：`Anonymous`、`Corporate`

接続イベント グラフ

システムは、テーブル形式のドリル ダウン ページを使ったワークフローや最終的なイベントのテーブル表示に加えて、5 分間隔で集計されたデータを使用して、特定の接続データをグラフィック表示することができます。グラフ表示できるのは、データを集約するのに使用する情報（送信元と宛先の IP アドレス（およびこれらのホストに関連するユーザ）、宛先ポート、トランスポート プロトコルとアプリケーション プロトコル）のみです。

ヒント セキュリティ インテリジェンス イベントを関連する接続イベントとは別にグラフ表示することはできません。セキュリティ インテリジェンスのフィルタリング アクティビティの概要をグラフィック表示するには、ダッシュボードとコンテキスト エクスプローラを使用します。

接続グラフは 3 種類あります。

- 円グラフは、1 つのデータセットのデータをカテゴリ分けして表示します。
- 棒グラフは、1 つあるいは複数のデータセットのデータをカテゴリ分けして表示します。
- 折れ線グラフは、時間の経過に伴って 1 つあるいは複数のデータセットのデータをプロットします。標準ビューあるいは速度（変化のペース）ビューを使用します。

（注） システムは、トラフィック プロファイルを線グラフで表示します。他の接続グラフと同様に操作可能ですが、いくつか規制があります。トラフィック プロファイルを表示するには、管理者アクセス権が必須です。

ワークフロー テーブルと同様に、ワークフロー グラフもドリル ダウンし、制約を加えることで分析の的を絞ることができます。

棒グラフおよび折れ線グラフはどちらも複数のデータセットを表示できます。つまり、各 X 軸データ ポイントに対し、Y 軸に複数の値を表示できます。たとえば、一意のイニシエータとレスポンダの総数を表示できます。円グラフでは、1 つのデータセットのみ表示できます。

X 軸または Y 軸、もしくは両方を変更することによって、接続グラフにさまざまなデータやデータセットを表示できます。円グラフでは、X 軸を変更すると独立変数が変わり、Y 軸を変更すると従属変数が変わります。

関連トピック

接続の概要（グラフ用集約データ） （3022 ページ）

接続イベント グラフの使用方法

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Maint/Any Security Analyst（ワークフローに応じて異なります）

Firepower Management Center では、検索する情報に応じて、接続イベント グラフを表示したり操作したりできます。

接続グラフにアクセスしたときに表示されるページは、使用するワークフローによって異なります。接続イベントのテーブル ビューで終了する、事前定義されたワークフローを使用できます。また、特定のニーズを満たす情報だけを表示するカスタム ワークフローを作成することもできます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

ステップ 1 **[Analysis]** > **[Connections]** > **[Events]**を選択します。

（注） 接続イベント テーブルがグラフの代わりに表示される場合、または別のグラフを表示する場合は、ワークフロー タイトルの横にある（**ワークフローの切り替え**）をクリックし、グラフが含まれる事前定義されたワークフローまたはカスタム ワークフローを選択します。接続グラフを含むすべての事前定義された接続イベント ワークフローは、接続のテーブル ビューで終了します。

ステップ 2 次の選択肢があります。

- [時間範囲（Time Range）]：時間範囲を調整する場合は（グラフがブランクの場合に役立ちます）、時間枠の変更 （2956 ページ）を参照してください。
- [フィールド名（Field Name）]：ユーザが図示可能なデータの詳細については、接続イベントとセキュリティ インテリジェンス イベントのフィールド （3024 ページ）を参照してください。
- [ホスト プロファイル（Host Profiles）]：IP アドレスのホスト プロファイルを表示するには、発信側または応答側による接続データが表示されているグラフで、棒グラフの棒または円グラフの扇形をクリックし、[ホスト プロファイルの表示（View Host Profile）] を選択します。
- [ユーザ プロファイル（User Profile）]：ユーザ プロファイル情報を表示するには、発信側ユーザによる接続データが表示されているグラフで、棒グラフの棒または円グラフの扇形をクリックし、[ユーザ プロファイルの表示（View User Profile）] を選択します。

- [その他の情報（Other Information）]：図示されたデータに関する詳細については、折れ線グラフの点、棒グラフの棒、または円グラフの扇形の上にカーソルを置きます。
- [固定（Constrain）]：ワークフローを次のページに進めずに接続グラフを X 軸（独立した変数）基準で固定するには、折れ線グラフの点、棒グラフの棒、または円グラフの扇形をクリックし、[表示方法（View by）] オプションを選択します。
- [データ選択（Data Selection）]：グラフに表示されるデータを変更するには、[X 軸（X-Axis）] または [Y 軸（Y-Axis）] をクリックし、図示する新しいデータを選択します。X 軸を [時間（Time）] に変更、または [時間（Time）] から変更すると、グラフ タイプも変更されます。Y 軸を変更すると、表示されるデータセットに影響します。
- [データセット（Datasets）]：グラフのデータセットを変更するには、[データセット（Datasets）] をクリックし、新しいデータセットを選択します。
- [切り離し（Detach）]：デフォルトの時間範囲に影響を与えることなくさらに分析を実行できるように接続グラフを分離するには、[切り離し（Detach）] をクリックします。

  ヒント コピーを作成するには、分離したグラフで [新規ウィンドウ] をクリックします。分離した各グラフ上で、別々の分析ができるようになります。トラフィック プロファイルは、分離したグラフです。

- [詳細（Drill-Down）]：ワークフローで次のページにドリルダウンするには、折れ線グラフの点、棒グラフの線、または円グラフの扇形をクリックし、[詳細（Drill-Down）] を選択します。折れ線グラフで点をクリックすると、次のページの時間枠は、クリックした点を中心とする 10 分間に変更されます。棒グラフの棒または円グラフの扇形をクリックすると、その棒または扇形が表す基準に基づいて次のページが制約されます。
- [エクスポート（Export）]：グラフの接続データを CSV（カンマ区切り値）ファイルとしてエクスポートするには、[データのエクスポート（Export Data）] を選択します。次に、[CSV ファイルのダウンロード（Download CSV File）] をクリックし、ファイルを保存します。
- [グラフ タイプ（Graph Type）]：[折れ線（Line）]- 標準と速度（変化のペース）の折れ線グラフを切り替えるには、[速度（Velocity）] をクリックし、[標準（Standard）] または [速度（Velocity）] を選択します。
- [グラフ タイプ（Graph Type）]：[棒と円（Bar and Pie）] - 棒グラフと円グラフを切り替えるには、[棒グラフに切り替え（Switch to Bar）] または [円グラフに切り替え（Switch to Pie）] をクリックします。円グラフには複数のデータセットを表示できないため、複数のデータセットを持つ棒グラフから円グラフに切り替えた場合、円グラフは自動的に選択された 1 つのデータセットだけを表示します。表示するデータセットを選択する際、Firepower Management Center は、発信側と応答側の統計情報よりも全体の統計情報を優先し、応答側の統計情報よりも発信側の統計情報を優先します。
- [ページ間の移動（Navigate Between Pages）]：現在のワークフローで現在の制約を保持したままページ間を移動するには、ワークフロー ページの左上にある該当するページ リンクをクリックします。
- [イベント ビュー間の移動（Navigate Between Event Views）]：他のイベント ビューに移動して関連するイベントを表示するには、[移動先（Jump to）] をクリックし、ドロップダウンリストからイベント ビューを選択します。

- [再センタリング（Recenter）]：時間範囲の長さを変更せずにある時点を中心に折れ線グラフを再センタリングするには、その点をクリックし、[再センタリング（Recenter）] を選択します。
- [ズーム（Zoom）]：ズームインまたはズームアウトしながらある時点を中心に折れ線グラフを再センタリングするには、その点をクリックし、[ズーム（Zoom）]を選択してから新しい時間枠を選択します。

（注） 分離したグラフを使用している場合を除いて、制約、再センタリング、およびズームするとFirepower Management Center のデフォルトの時間範囲が変わります。

例：接続グラフの制約

例：円グラフの X 軸と Y 軸の変更

ある期間の接続のグラフについて考えてみましょう。グラフ上の点をポートによって制約すると、検出された接続イベント数に基づいて、最もアクティブだった 10 のポートを示す棒グラフが表示されますが、クリックした点を中心とする 10 分間の時間枠によって制約されます。

棒の 1 つをクリックし、[発信側 IP による表示（View by Initiator IP）] を選択してグラフをさらに制約すると、それまでと同じ 10 分間の時間枠だけでなく、クリックした棒が表すポートでも制約された新しい棒グラフが表示されます。

ポートごとのキロバイト数を表示する円グラフについて考えてみましょう。この場合、X 軸は **レスポンダ ポート**、Y 軸は **キロバイト** です。この円グラフは、ある間隔に監視対象ネットワークで送信されたデータの合計キロバイト数を表します。円の中の扇形は、各ポートで検出されたデータの比率を表します。

- グラフの X 軸を **アプリケーション プロトコル** に変更すると、引き続き円グラフは送信データの合計キロバイト数を表しますが、円の中の扇形は検出された各アプリケーション プロトコルの送信データの比率を表します。
- グラフの Y 軸を **パケット** に変更すると、円グラフはある間隔に監視対象ネットワークで送信された合計パケット数を表し、円の中の扇形は各ポートで検出された合計パケット数の割合を表します。

関連トピック

ワークフローの使用 （2931 ページ）
イベント ビュー設定の設定 （43 ページ）

接続グラフ データ オプション

X軸またはY軸、もしくは両方を変更することによって、接続グラフにさまざまなデータを表示できます。円グラフでは、X軸を変更すると独立変数が変わり、Y軸を変更すると従属変数を変わります。

表 *318 : X* 軸オプション

X 軸オプション	グラフの種類	次の基準でこのデータをグラフ化する
アプリケーション プロトコル（Application Protocol）	棒グラフまたは円グラフ	最もアクティブな 10 個のアプリケーション プロトコルに基づいて
Device	棒グラフまたは円グラフ	最もアクティブな 10 台の管理対象デバイスに基づいて
イニシエータ IP（Initiator IP）	棒グラフまたは円グラフ	最もアクティブな 10 個のイニシエータ ホスト IP アドレスに基づいて
イニシエータ ユーザ（Initiator User）	棒グラフまたは円グラフ	最もアクティブな 10 名のイニシエータ ユーザに基づいて
レスポンダ IP（Responder IP）	棒グラフまたは円グラフ	最もアクティブな 10 個のレスポンダ ホスト IP アドレスに基づいて
レスポンダ ポート（Responder Port）	棒グラフまたは円グラフ	最もアクティブな 10 個のレスポンダ ポートに基づいて
送信元デバイス（Source Device）	棒グラフまたは円グラフ	最もアクティブな 10 個の NetFlow データ エクスポータと、Firepower システムの管理対象デバイスによって検出されたすべての接続の `Firepower` という名前の送信元デバイスに基づいて。
時刻（Time）	ライン	時系列 Y 軸と [時刻（Time）] を切り替えることでグラフの種類も変わり、データセットを変更できます。

表 *319 : Y* 軸オプション

Y 軸オプション	X軸の基準を使用してこのデータをグラフ化する
バイト（Bytes）	送信バイト数
接続（Connections）	接続数

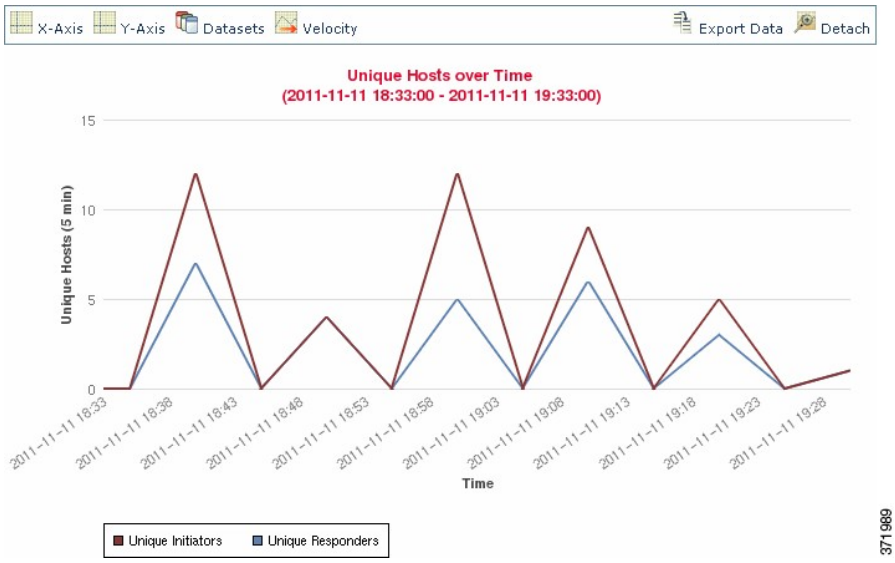
Y 軸オプション	X軸の基準を使用してこのデータをグラフ化する
KB（KBytes）	送信キロバイト数
KB/秒（KBytes Per Second）	KB/秒
パケット（Packets）	送信パケット数
固有のホスト（Unique Hosts）	検出された固有のホスト数
固有のアプリケーション プロトコル（Unique Application Protocols）	固有のアプリケーション プロトコル数
固有ユーザ（Unique Users）	固有ユーザ数

複数のデータセットの接続グラフ

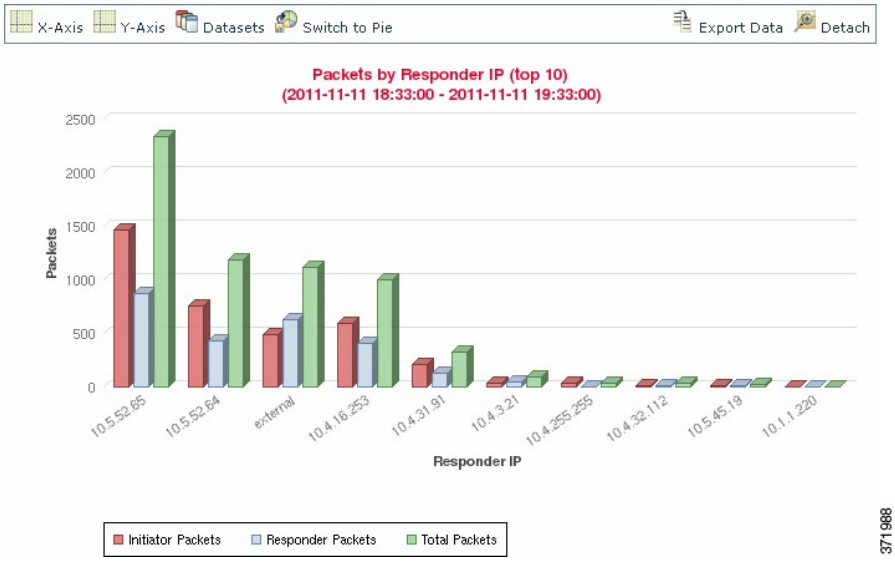
棒グラフおよび折れ線グラフはどちらも複数のデータセットを表示できます。つまり、各X軸データ ポイントに対し、Y軸に複数の値を表示できます。たとえば、一意のイニシエータとレスポンダの総数を表示できます。

（注） 円グラフには複数のデータセットを表示**できません**。複数のデータセットを持つ棒グラフから円グラフに切り替えた場合、円グラフは自動的に選択された1つのデータセットだけを表示します。表示するデータセットを選択する際、Firepower Management Center は、イニシエータとレスポンダの統計情報よりも全体の統計情報を優先し、イニシエータの統計情報よりもレスポンダの統計情報を優先します。

折れ線グラフでは、複数のデータセットは複数の線として、それぞれ異なる色で表示されます。たとえば、次のグラフは、モニタ対象ネットワークにおいて1時間間隔の1回で検出された一意のイニシエータの合計数と一意のレスポンダの合計数を表示しています。



棒グラフでは、複数のデータセットが X 軸データ ポイントごとに色分けされた棒として表示されます。たとえば次の棒グラフは、監視対象ネットワーク上で送信されたパケットの合計数と、イニシエータによって送信されたパケット数、レスポンダによって送信されたパケット数を表示しています。



接続グラフ データセット オプション

次の表では、接続グラフの x 軸に表示できるデータセットについて説明します。

表 *320 :* データセット オプション

y 軸が表示されている場合は、	選択可能なデータセット
接続（Connections）	デフォルトのみです。監視対象のネットワークで検出された接続数（[接続（Connections）]）です。これは、トラフィック プロファイル グラフ用の唯一のオプションです。
KBytes	以下の組み合わせ • 監視対象ネットワーク上で送信された合計キロバイト数（[Total KBytes]） • 監視対象ネットワーク上でホスト IP アドレスから送信されたキロバイト数（[Initiator KBytes]） • 監視対象ネットワーク上でホスト IP アドレスによって受信されたキロバイト数（[Responder KBytes]）
KBytes Per Second	デフォルトの、監視対象ネットワークで 1 秒あたりに送信された合計キロバイト数のみ（[Total KBytes Per Second]）
Packets	以下の組み合わせ • 監視対象ネットワーク上で送信された合計パケット数（[Total Packets]） • 監視対象ネットワーク上でホスト IP アドレスから送信されたパケット数（[Initiator Packets]） • 監視対象ネットワーク上でホスト IP アドレスによって受信されたパケット数（[Responder Packets]）
Unique Hosts	以下の組み合わせ • 監視対象ネットワーク上の一意なセッション開始側の数（[Unique Initiators]） • 監視対象ネットワーク上の一意なセッション応答側の数（[Unique Responders]）

y 軸が表示されている場合は、	選択可能なデータセット
Unique Application Protocols	デフォルトの、監視対象ネットワーク上の一意なアプリケーション プロトコル数のみ（[Unique Application Protocols]）
Unique Users	デフォルトのみです。監視対象のネットワークでのセッション イニシエータにログインした固有ユーザ数（[固有イニシエータ ユーザ（Unique Initiator Users）]）です。

イベント時間の制約

各イベントには、そのイベントがいつ発生したかを示すタイム スタンプがあります。時間枠（時間範囲とも呼ばれる）を設定することによって、いくつかのワークフローに表示される情報を制約することができます。

時間によって制約できるイベントに基づいたワークフローには、ページの上部に時間範囲を表す行が含まれています。

デフォルトでは、ワークフローは、1時間前が開始時間として設定された時間枠を使用します。たとえば、午前 11:30 にログインした場合、午前 10:30～11:30 の間に発生したイベントが表示されます。時間が経過するにしたがって、時間枠が拡張されます。午後 12:30 には、午前 10:30～午後 12:30 の間に発生したイベントが表示されます。

イベント ビューの設定で独自のデフォルト時間枠を設定することによって、この動作を変更することができます。これにより、次の 3 つのプロパティが影響を受けます。

- 時間枠のタイプ（静的、拡張、またはスライディング）
- 時間枠の長さ
- 時間枠の数（複数の時間枠、または単一のグローバル時間枠）

ページの上部にある時間範囲をクリックして [日時（Date/Time）] ポップアップ ウィンドウを表示し、デフォルトの時間枠の設定に関係なく、イベントの分析中に時間枠を手動で変更することができます。設定した時間枠の数、および使用しているアプライアンスのタイプに応じて [日時（Date/Time）] ウィンドウを使用して、表示しているイベントのタイプに対するデフォルトの時間枠を変更することもできます。

最後に、スライディングまたは拡張ワークフローを検討している間は時間枠を一時停止できます。データセットを一時的に凍結するための時間枠の一時停止（2957ページ）を参照してください。

関連トピック

イベント ビュー設定の設定 （43 ページ）
接続およびセキュリティ インテリジェンス イベント テーブルの使用 （3050 ページ）

イベントのセッションごとの時間枠のカスタマイズ

デフォルトの時間枠（タイム ウィンドウ）に関係なく、イベントの分析中に時間枠を手動で変更することができます。

（注） 手動による時間枠の設定は、現行のセッションに対してのみ有効です。いったんログアウトしてからもう一度ログインすると、時間枠はデフォルトにリセットされます。

ユーザが設定した時間枠の数によっては、1 つのワークフローの時間枠の変更が、アプライアンス上の他のワークフローに影響を与えることがあります。たとえば、単一のグローバルな時間枠がある場合、1 つのワークフローの時間枠を変更すると、アプライアンス上の他のすべてのワークフローの時間枠が変更されます。一方、複数の時間枠を使用している場合は、監査ログまたはヘルス イベント ワークフローの時間枠を変更しても、他の時間枠には影響がありませんが、他の種類のイベントで時間枠を変更すると、時間によって制約されるすべてのイベント（監査イベントとヘルス イベントは除く）が影響を受けます。

すべてのワークフローを時間によって制約できるわけではないため、時間枠の設定は、ホスト、ホスト属性、アプリケーション、アプリケーションの詳細、脆弱性、ユーザ、またはホワイトリスト違反に基づいたワークフローには影響を与えないことに注意してください。

[Date/Time] ウィンドウの [Time Window] タブを使用して、時間枠を手動で設定します。デフォルトの時間枠設定で設定した時間枠の数によって、タブのタイトルは以下のいずれかになります。

- [Events Time Window]：複数の時間枠を設定し、監査ログまたはヘルス イベント ワークフロー以外のワークフローに対して時間枠を設定している場合
- [Health Monitoring Time Window]：複数の時間枠を設定し、ヘルス イベント ワークフローに対して時間枠を設定している場合
- [Audit Log Time Window]：複数の時間枠を設定し、監査ログに対して時間枠を設定している場合
- [Global Time Window]：単一の時間枠を設定している場合

時間枠を設定する場合には、最初に、使用する時間枠のタイプを決定する必要があります。

- 静的な時間枠は、特定の開始時間から特定の終了時間の間に生成されたすべてのイベントを表示します。
- 拡張時間枠は、特定の開始時間から現在までの間に生成されたすべてのイベントを表示します。時間の経過とともに時間枠が拡張され、イベント ビューに新しいイベントが追加されます。
- [スライディング（sliding）] 時間枠には、特定の開始時間（1 週間前など）から現在までの間に生成されたすべてのイベントが表示されます。ページを更新すると、時間枠が「スライド」するため設定した時間範囲（この例では過去 1 週間）のイベントのみが表示され

ます。データセットを調べている間に一時的に更新されないようにするには、データセットを一時的に凍結するための時間枠の一時停止 （2957 ページ）を参照してください。

選択したタイプによって、[日付/時刻（Date/Time）] ウィンドウが変化し、さまざまな設定オプションが提供されます。

（注） Firepower システムでは、タイム ゾーンの設定に指定された時間に基づいて、24 時間の時計を使用します。

時間枠の設定

次の表で、[時間枠（Time Window）] タブで設定できるさまざまな項目について説明します。

表 *321* : 時間枠の設定

設定	時間枠のタイプ	説明
時間枠タイプのドロップダウン リスト	n/a	使用する時間枠のタイプを、静的、拡張、またはスライディングのいずれかから選択します。 イベント ビューを時間によって制約している場合は、（グローバルかイベントに特有かに関係なく）アプライアンスに設定されている時間枠の範囲外に生成されたイベントがイベント ビューに表示されることがあることに注意してください。アプライアンスに対してスライドする時間枠を設定した場合でも、この状況が発生することがあります。
[Start Time] カレンダー	静的および拡張	時間枠の開始日と時間を指定します。すべての時間枠の最大時間範囲は、1970 年 1 月 1 日午前 0 時（UTC）～ 2038 年 1 月 19 日午前 3 時 14 分 7 秒です。 カレンダーを使用する代わりに、下記で説明するプリセット オプションを使用できます。

設定	時間枠のタイプ	説明
[End Time] カレンダー	静的	時間枠の終了日付と時間を指定します。すべての時間枠の最大時間範囲は、1970 年 1 月 1 日午前 0 時（UTC）～ 2038 年 1 月 19 日午前 3 時 14 分 7 秒です。 拡張時間枠を使用している場合は、[終了時刻（End Time）] カレンダーがグレー表示になり、終了時刻が「現在の時刻（Now）」と示されることに注意してください。 カレンダーを使用する代わりに、下記で説明するプリセット オプションを使用することもできます。
[Show the Last] フィールドおよびドロップダウン リスト	スライディング	スライディング時間枠の長さを設定します。
[Presets]：[Last]	すべて	リスト内のいずれかの時間範囲をクリックし、アプライアンスのローカル時刻に基づいて時間枠を変更します。たとえば、[1 week] をクリックすると、最後の 1 週間を反映するように時間枠が変わります。プリセットをクリックすると、選択したプリセットを反映するようにカレンダーが変わります。
[Presets]：[Current]	静的および拡張	リスト内のいずれかの時間範囲をクリックし、アプライアンスのローカル時間と日付に基づいて時間枠を変更します。プリセットをクリックすると、選択したプリセットを反映するようにカレンダーが変わります。 次の点に注意してください。 • 現在日付は午前 0 時から始まる • 現在の週は日曜日の午前 0 時から始まる • 現在の月は、月の最初の日の午前 0 時から始まる

設定	時間枠のタイプ	説明
[Presets]：[Synchronize with]	すべて（グローバルな時間枠を使用している場合は使用不可）	以下のいずれかをクリックします • [Events Time Window]：現在の時間枠とイベントの時間枠を同期する場合 • [Health Monitoring Time Window]：現在の時間枠とヘルスモニタリングの時間枠を同期する場合 • [監査ログの時間枠（Audit Log Time Window）]：現在の時間枠と監査ログの時間枠を同期する場合

時間枠の変更

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Maint/Any Security Analyst（ワークフローに応じて異なります）

ステップ 1 時間により制約されたワークフローで、時間範囲のアイコン（）をクリックし、[日付と時間（Date/Time）] ウィンドウを開きます。

ステップ 2 [イベントの時間枠（Events Time Window）] タブで、時間枠の設定（2954 ページ）に記載されているように時間枠を設定します。

ヒント 時間枠をデフォルトの設定に戻すには、[リセット（Reset）] をクリックします。

ステップ 3 [Apply] をクリックします。

データ セットを一時的に凍結するための時間枠の一時停止

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Maint/Any Security Analyst（ワークフローに応じて異なります）

スライディングまたは拡張時間枠を使用している場合、時間枠を一時停止してワークフローが提供するデータのスナップショットを調べることができます。一時停止されないワークフローが更新されると、調査するイベントが削除されたり、調査対象外のイベントが追加されたりすることがあるため、この機能は有用です。

ページの下部にあるリンクをクリックしてイベントの他のページを表示する場合は、時間枠が自動的に一時停止されます。準備ができたら時間枠の一時停止を解除できます。

分析が完了したら、時間枠の一時停止を解除できます。時間枠の一時停止を解除すると、設定に従って時間枠が更新されます。また、一時停止を解除した時間枠を反映するようにイベントビューが更新されます。

イベント時間枠の一時停止はダッシュボードには影響を与えず、ダッシュボードの一時停止もイベント時間枠の一時停止に影響しません。

時間で制約されているワークフローでは、目的の時間範囲コントロールを選択できます。

- 時間枠を一時停止するには、時間範囲コントロールの一時停止アイコン（  ）をクリックします。
- 時間枠の一時停止を解除するには、時間範囲コントロールの再生アイコン（）をクリックします。

イベントのデフォルト時間枠

イベントの分析中に、[日付/時間（Date/Time）] ウィンドウの [設定（Preferences）] タブを使用し、表示しているイベントのタイプに対するデフォルトの時間枠を（イベント ビューの設定を使用せずに）変更することができます。

この方法でデフォルトの時間枠を変更すると、表示しているイベントのタイプのデフォルト時間枠のみが変わります。たとえば、複数の時間枠を設定しており、[Preferences] タブでデフォルトの時間枠を変更すると、イベント、ヘルス モニタリング、または監査ログ ウィンドウのいずれかの設定が変更されます。つまり、最初のタブで示されている時間枠が変更されます。1 つの時間枠を設定している場合に [設定（Preferences）] タブでデフォルトの時間枠を変更すると、イベントのすべてのタイプのデフォルト時間枠が変わります。

関連トピック

デフォルト時間枠 （46 ページ）

イベント タイプのデフォルトの時間枠オプション

次の表で、[設定（Preferences）] タブで設定できるさまざまな設定について説明します。

表 *322 :* 時間枠の設定

設定	説明
更新間隔（Refresh Interval）	イベント ビューの更新間隔を分単位で設定します。ゼロを入力すると、リフレッシュ オプションは無効になります。
Number of Time Windows	使用する時間枠の数を指定します。 • 監査ログ、ヘルス イベント、および時間によって制約可能なイベントに基づいたワークフローに対してそれぞれ別のデフォルト時間枠を設定する場合は、[複数（Multiple）] を選択します。 • すべてのイベントに適用されるグローバルな時間枠を使用する場合は、[単一（Single）] を選択します。
デフォルト時間枠：[最後を表示 - スライディング（Show the Last - Sliding）]	この設定を選択すると、指定する長さのスライディングのデフォルト時間枠を設定できます。 アプライアンスは、特定の開始時刻（たとえば1時間前）から現在までに生成されたすべてのイベントを表示します。イベントビューの変更と共に、時間枠は「スライド」して、常に最後の 1 時間内のイベントが表示されます。
Default Time Window: Show the Last - Static/Expanding	この設定を選択すると、指定する長さの、静的または拡張のデフォルト時間枠を設定できます。 **静的な**時間枠の場合（[Use End Time] チェック ボックスをオンにした場合）、アプライアンスは特定の開始時間（1時間前などの）から、最初にユーザがイベントを参照した時間までに生成されたすべてのイベントを表示します。イベント ビューを変更しても時間枠は固定されており、静的な時間枠の間に発生したイベントのみが表示されます。 **拡張**時間枠の場合（[Use End Time] チェック ボックスをオフにしたの場合）、アプライアンスは特定の開始時間（1時間前などの）から現在までに生成されたすべてのイベントを表示します。イベント ビューを変更すると、時間枠は現在まで拡張されます。

設定	説明
Default Time Window: Current Day - Static/Expanding	この設定を選択すると、現在の日付に対して静的または拡張のデフォルト時間枠を設定できます。現在の日付は、現行セッションのタイム ゾーン設定に基づいて午前 0 時に始まります。 **静的な**時間枠の場合（[Use End Time] チェック ボックスをオンにした場合）、アプライアンスは午前0時から、最初にユーザがイベントを参照した時間までに生成されたすべてのイベントを表示します。イベント ビューを変更しても時間枠は固定されており、静的な時間枠の間に発生したイベントのみが表示されます。 **拡張**時間枠の場合（[Use End Time] チェック ボックスをオフにした場合）、アプライアンスは午前0時から現在までに生成されたすべてのイベントを表示します。イベント ビューを変更すると、時間枠は現在まで拡張されます。ログアウトする前に 24 時間を超えて分析を続けた場合、この時間枠は 24 時間よりも長くなる可能性があることに注意してください。
Default Time Window: Current Week - Static/Expanding	この設定を選択すると、現在の週に対して静的または拡張のデフォルト時間枠を設定できます。現在の週は、現行セッションのタイム ゾーン設定に基づいて直前の日曜日の午前 0 時に始まります。 **静的な**時間枠の場合（[Use End Time] チェック ボックスをオンにした場合）、アプライアンスは午前0時から、最初にユーザがイベントを参照した時間までに生成されたすべてのイベントを表示します。イベント ビューを変更しても時間枠は固定されており、静的な時間枠の間に発生したイベントのみが表示されます。 **拡張**時間枠の場合（[Use End Time] チェック ボックスをオフにした場合）、アプライアンスは日曜日の午前0時から現在までに生成されたすべてのイベントを表示します。イベント ビューを変更すると、時間枠は現在まで拡張されます。ログアウトする前に1週間を超えて分析を続けた場合、この時間枠は1週間よりも長くなる可能性があることに注意してください。

イベント タイプのデフォルトの時間枠の変更

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Maint/Any Security Analyst

ステップ 1 時間により制約されたワークフローで、時間範囲のアイコン（）をクリックし、[日付と時間（Date/Time）] ウィンドウを開きます。

ステップ 2 [優先（Preferences）] タブをクリックし、イベント タイプのデフォルトの時間枠オプション （2958 ページ）に記載されているようにプリファレンスを変更します。

ステップ 3 [設定の保存（Save Preferences）] をクリックします。

ステップ 4 次の 2 つの対処法があります。

- 使用しているイベント ビューに新しいデフォルト時間枠の設定を適用するには、[Apply] をクリックして [Date/Time] ウィンドウを閉じてイベント ビューをリフレッシュします。
- デフォルトの時間枠設定を適用せずに分析を続けるには、[適用（Apply）] をクリックせずに [日付と時間（Date/Time）] ウィンドウを閉じます。

イベント ビューの制約

ワークフローページに表示される情報は、ユーザが設定した制約によって異なります。たとえばイベント ワークフローを最初に開いた場合、情報は、最後の 1 時間に生成されたイベントに制約されています。

ワークフローの次のページに進んで、表示されるデータを特定の値で制約する場合は、ページでこれらの値を持つ行を選択し、[View] をクリックします。現在の制約を保持し、すべてのイベントを含めた状態でワークフローの次のページに進むには、[View All] を選択します。

（注） 複数の不可算値を持つ行を選択し、[表示（View）] を選択すると、複合的な制約が作成されます。

ワークフローのデータを制約するための 3 番目の方法があります。自身が選択した値を持つ行のみが表示されるようページを制約し、ページの上部に示される制約リストに選択した値を追加するには、ページの行で値をクリックします。たとえば、記録された接続のリストを表示する場合に、アクセス制御を使用して、自身が許可したものだけがリストに示されるよう制約する場合は、[アクション（Action）] カラムで [許可（Allow）] をクリックします。他の例では、侵入イベントを表示する場合に、宛先ポートが 80 のイベントのみがリストに示されるよう制約する場合は、[宛先ポート/ICMP コード（Destination Port/ICMP Code）] カラムで [80（http）/tcp（80 (http)/tcp）] をクリックします。

ヒント モニタルールの条件に基づいて接続イベントを制約するための手順は少し異なり、いくつかの追加手順が必要になる場合があります。また、関連付けられているファイルや侵入情報によって接続イベントを制約することはできません。

検索を使用して、ワークフローの情報を制約することもできます。1 つのカラム内の複数の値について制約する場合は、この機能を使用します。たとえば、2 つの IP アドレスに関連しているイベントを表示する場合は、[検索の編集（Edit Search）] をクリックし、[検索（Search）] ページで対象の [IP アドレス（IP address）] フィールドを変更して両方のアドレスが含まれるようにして、[検索（Search）] をクリックします。

検索ページで入力した検索条件はページの上部に制約として表示され、これに従って制約されたイベントが合わせて表示されます。Firepower Management Center では、複合的な制約でない限り、他のワークフローにナビゲートしたときにも現在の制約が適用されます。

検索する場合は、検索対象のテーブルに検索の制約を適用するかどうかに注意する必要があります。たとえば、クライアントデータは接続サマリーでは使用できません。接続で検出されたクライアントに基づいて接続イベントを検索し、結果を接続サマリー イベント ビューで表示すると、Firepower Management Centerでは、制約が設定されていない場合と同じように接続データが表示されます。無効な制約は、非適用（N/A）とラベルが付けられ、取り消し線が付けられます。

イベントの制約

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Maint/Any Security Analyst（ワークフローに応じて異なります）

ステップ 1 ワークフローの選択（2933 ページ）の説明に従って、適切なメニューパスとオプションを選択してワークフローにアクセスします。

ステップ 2 すべてのワークフローで、次のオプションを選択できます。

- ビューを単一の値と一致するイベントに制約するには、ページの行内の目的の値をクリックします。
- ビューを複数の値と一致するイベントに制約するには、その値を持つイベントのチェックボックスをオンにし、[表示（View）] をクリックします。

  （注） 行に複数の不可算値が含まれている場合は、複合的な制約が追加されます。

- 制約を解除するには、[制約の検索（Search Constraints）] の展開矢印（▶）をクリックし、展開された [制約の検索（Search Constraints）] リストで制約の名前をクリックします。

- 検索ページを使用して制約を編集するには、[検索の編集（Edit Search）] をクリックします。
- 保存済み検索として制約を保存するには、[検索の保存（Save Search）] をクリックし、クエリに名前を付けます。

  （注）　複合的な制約が含まれているクエリは保存できません。

- 別のイベント ビューで同じ制約を使用するには、[移動先（Jump to）] をクリックし、イベント ビューを選択します。

  （注）　別のワークフローに切り替えると、複合的な制約は保持されません。

- 制約の表示を切り替えるには、[制約の検索（Search Constraints）] の展開矢印（▶）または [制約の検索（Search Constraints）] の折りたたみ開矢印（▼）をクリックします。制約のリストが長く、画面の大半を占有する場合に、この機能は役立ちます。

複合イベント ビューの制約

複合的な制約は、特定のイベントに対するすべての不可算値に基づいています。複数の不可算値を持つ行を選択する場合は、ページ上の対象行におけるすべての不可算値と一致するイベントのみを取得する複合的な制約を設定します。たとえば、送信元 IP アドレスが `10.10.31.17` で、宛先 IP アドレスが `10.10.31.15` である行と、送信元 IP アドレスが `172.10.10.17` で宛先 IP アドレスが `172.10.10.15` である行を選択すると、次のすべての結果が取得されます。

- 送信元 IP アドレスが 10.10.31.17 で、かつ宛先 IP アドレスが 10.10.31.15 のイベント

  または

- 送信元 IP アドレスが 172.10.31.17 で、かつ宛先 IP アドレスが 172.10.31.15 のイベント

複合的な制約と単純な制約を組み合わせると、複合的な制約の各セットに単純な制約が追加されます。たとえば、上記に記載されている複合的な制約に対して、プロトコル値 `tcp` の単純な制約を追加すると、次のすべての結果が取得されます。

- 送信元 IP アドレスが 10.10.31.17 で、かつ宛先 IP アドレスが 10.10.31.15 で、かつプロトコルが tcp であるイベント

  または

- 送信元 IP アドレスが 172.10.31.17 で、かつ宛先 IP アドレスが 172.10.31.15 で、かつプロトコルが tcp であるイベント

複合的な制約について、検索および検索の保存を実行することはできません。また、別のワークフローに切り替えるのに、イベント ビューのリンクを使用した場合、または [(switch workflow)] をクリックした場合は、複合的な制約は保持できません。複合的な制約が適用されているイベント ビューをブックマークしても、制約はブックマークに保存されません。

複合イベント ビュー制約の使用

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Maint/Any Security Analyst（ワークフローに応じて異なります）

ステップ 1 ワークフローの選択 （2933 ページ）の説明に従って、適切なメニューパスとオプションを選択してワークフローにアクセスします。

ステップ 2 複合制約を管理する場合、次の選択肢があります。

- 複合制約を作成するには、カウント以外の値を持つ 1 つ以上の行を選択し、[表示（View）] をクリックします。
- 複合制約をクリアするには、[検索制約（Search Constraints）] の展開矢印（▶）をクリックし、[複合制約（Compound Constraints）] をクリックします。

ワークフロー間のナビゲーション

ワークフロー ページの [移動（Jump to...）] ドロップダウン リストのリンクを使用して、他のワークフローへ移動できます。ドロップダウン リストを選択し、追加のワークフローを表示および選択します。

新しいワークフローを選択すると、（適切な場合は）、選択する行で共有されているプロパティおよび設定する制約が、新しいワークフローで使用されます。設定した制約またはイベントのプロパティが、新しいワークフローのフィールドにマップされない場合は、これらはドロップされます。また、ワークフローを切り替えた場合には、複合的な制約は保持されません。キャプチャ ファイルのワークフローの制約は、ファイルおよびマルウェアのイベント ワークフローのみに転送されます。

（注） 所定の時間範囲のイベント数を表示する場合、詳細なデータを利用できるイベントの数が、イベントの総数に反映されないことがあります。これは、ディスク領域の使用率を管理するために、古いイベントの詳細がシステムによってプルーニングされることがあるために発生します。イベント詳細のプルーニングを最小限にするために、対象の展開にとって最も重要なイベントだけを記録するようにイベント ロギングを調整できます。

時間枠を一時停止していない場合、または静的な時間枠を設定していない場合、ワークフローを変更したときに時間枠も変更されることに注意してください。

この機能により、疑わしいアクティビティの調査が強化されます。たとえば、接続データを表示していて、内部ホストが異常に大量のデータを外部サイトに転送していることに気付いた場合は、応答側の IP アドレスとポートを制約として選択し、[Applications] ワークフローへ移動することができます。[Applications] ワークフローは応答側の IP アドレスとポートを IP アドレスとポートの制約として使用し、アプリケーションの種類などの追加情報を表示することができます。ページの上部にある [Hosts] をクリックして、リモート ホストのホスト プロファイルを表示することもできます。

アプリケーションに関する詳細を検索した後で、[Correlation Events] を選択して接続データ ワークフローに戻る、制約から応答側の IP アドレスを削除する、制約にイニシエータの IP アドレスを追加する、[Application Details] を選択して、データをリモート ホストに転送するときに開始側のホストでユーザがどのクライアントを使用しているかを確認する、といったことができます。ポートの制約は、[Application Details] ページには転送されないことに注意してください。ローカルホストを制約として保持したまま、追加情報を検索するために他のナビゲートボタンを使用することもできます。

- ローカル ホストがいずれかのポリシーに違反しているかどうかを検出するには、IP アドレスを制約として保持したままで [Jump to] ドロップダウン リストから [Correlation Events] を選択します。
- ホストに対して侵入ルールがトリガーされた（侵害を表している）かどうかを確認するには、[Jump to] ドロップダウン リストから [Intrusion Events] を選択します。
- ローカル ホストのホスト プロファイルを表示し、ホストが、悪用された可能性のある脆弱性の影響を受けやすくなっているかどうかを判断するには、[移動（Jump to）] ドロップダウン リストから [ホスト（Hosts）] を選択します。

ブックマーク

イベントの分析の特定の場所と時間にすばやく戻りたい場合には、ブックマークを作成します。ブックマークは、次の情報を保持します。

- 使用中のワークフロー
- 表示中のワークフローの部分
- ワークフローのページ番号
- 検索の制約
- 無効になっているカラム
- 使用している時間範囲

あるユーザが作成したブックマークは、ブックマーク アクセスを持っているすべてのユーザ アカウントで利用できます。これは、より詳細な分析を必要とするイベントセットを見つけた場合、簡単にブックマークを作成し、適切な権限を持った他のユーザに調査を引き継ぐことが可能であることを意味します。

（注） ブックマークに表示されているイベントが（ユーザによって直接、またはデータベースの自動クリーンアップによって）削除されると、そのブックマークにあった元のイベントは表示されなくなります。

ブックマークの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Maint/Any Security Analyst（ワークフローに応じて異なります）

マルチドメイン導入では、現在のドメインで作成されたブックマークのみを表示できます。

ステップ 1 イベントの分析中に、表示されている対象のイベントで[このページをブックマーク（Bookmark This Page）]をクリックします。

ステップ 2 [名前（Name）] フィールドに、名前を入力します。

ステップ 3 [ブックマークの保存（Save Bookmark）] をクリックします。

ブックマークの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Maint/Any Security Analyst（ワークフローに応じて異なります）

マルチドメイン導入では、現在のドメインで作成されたブックマークのみを表示できます。

すべてのイベント ビューで、以下の 2 つの方法を選択できます。

- [ブックマークの表示（View Bookmarks）] の上にポインタを合わせ、ドロップダウン メニューから目的のブックマークをクリックします。

- [ブックマークの表示（View Bookmarks）] をクリックし、[ブックマークの表示（View Bookmarks）] ページで目的のブックマーク名をクリックするか、その横にある表示アイコン（  ）をクリックします。

  （注） 最初にブックマークに表示されていたイベントが（ユーザによって直接、またはデータベースの自動クリーンアップによって）削除されると、そのブックマークにはイベントの元のセットは表示されません。

第 121 章

イベントの検索

以下のトピックでは、ワークフロー内のイベントの検索方法について説明します。

イベントの検索

Firepower システムでは、データベース テーブルにイベントとして保存される情報が生成されます。イベントには、アプライアンスがイベントを生成する原因となったアクティビティを示すいくつかのフィールドが含まれます。ご使用の環境用にカスタマイズされた、さまざまなイベント タイプの検索を作成および保存し、後で再使用するために保存できます。

検索設定を保存するときには、その検索設定の名前を付け、それを自分だけで使用するか、それともアプライアンスの全ユーザが使用できるようにするかを指定します。カスタム ユーザ ロールのデータの制限として検索を使用する場合は、**必ず**プライベート検索として保存する必要があります。以前に検索設定を保存した場合、それをロードし、必要に応じて修正して、検索を開始することができます。カスタム分析のダッシュボード ウィジェット、レポート テンプレート、カスタム ユーザ ロールも、保存した検索を使用できます。保存済みの検索設定がある場合、[検索（Search）] ページからそれらを削除できます。

いくつかのイベント タイプに関しては、Firepower システムに備わっている定義済みの検索設定をサンプルとして使用すると、ネットワークについての重要な情報にすばやくアクセスできます。ネットワーク環境に合わせて定義済み検索設定のフィールドを変更し、検索設定を保存して、後で再利用することができます。

検索の種類に応じて、使用できる検索条件は異なりますが、メカニズムは同じです。検索により、すべてのフィールドに対して指定した検索条件と一致するレコードのみが返されます。

（注） カスタム テーブルの検索には、若干異なる手順が必要です。

関連トピック

カスタム テーブルの検索 （2996 ページ）

検索の制約

データベーステーブルごとに、検索を制約する値を入力できる独自の検索ページがあります。入力した値は、そのテーブルに定義されているフィールドに適用されます。フィールドのタイプによっては、特殊なシンタックスを使用して、ワイルドカード文字や数値の範囲などの基準を指定できます。

検索結果はワークフローページに表示され、カラム式レイアウトでテーブルの各フィールドが示されます。一部のデータベース テーブルは、ワークフロー ページにカラムとして表示されないフィールドを使用した検索も行えます。ワークフローページで結果を確認する際に、該当する制約が検索結果に適用されているかどうかを判別するには、展開アイコン（▶）をクリックして、検索に現在有効になっている制約を表示します。

一般的な検索の制約

イベントを検索するときは、次の一般的な注意事項を順守してください。

- すべてのフィールドで否定（!）を使用できます。
- すべてのフィールドで検索値のカンマ区切りのリストを使用できます。指定したフィールドのリストされた値のいずれかを含むレコードがその検索条件に一致します。
- すべてのフィールドで、引用符で囲まれたカンマ区切りリストを検索値として使用できます。
  - 単一の値だけを含めることができるフィールドの場合は、引用符内で指定された正確な文字列を含む指定されたフィールドを持つレコードが検索条件と一致します。たとえば、`A, B, "C, D, E"` と検索すると、指定されたフィールドに `"A"` または `"B"` または `"C, D, E"` が含まれるレコードが一致します。この検索では、該当する可能性がある値にカンマが含まれているフィールドを照合できます。
  - 複数の値を同時に含めることができるフィールドの場合は、引用符で囲まれたカンマ区切りリスト内のすべての値が含まれている指定されたフィールドを持つレコードがその検索条件に一致します。
  - 複数の値を同時に含めることができるフィールドの場合は、検索条件に単一の値だけでなく引用符で囲まれたカンマ区切りリストを含めることができます。たとえば、`A, B, "C, D, E"` をこれらの文字の 1 つまたは複数を含むことができるフィールドで検索すると、指定したフィールドに `A` または `B`、または `C`、`D`、`E` のすべてを含むレコードが一致します。
- フィールドでその情報を利用できないイベントを示すには、そのフィールドで `n/a` を指定します。フィールドに情報が入力されているイベントを示すには `!n/a` を使用します。
- 多くの数値フィールドの前には、より大きい（`>`）、以上（`>=`）、より小さい（`<`）、以下（`<=`）、等しい（`=`）または等しくない（`<>`）の演算子を付けることができます。

ヒント　長い複雑な値を（SHA-256ハッシュ値など）を含むフィールドを検索する場合は、ソース資料から検索基準値をコピーし、検索ページの適切なフィールドに貼り付けることができます。

検索で使用するワイルドカードと記号

検索ページの多くのテキストフィールドでは、文字列内の文字に一致させるために、アスタリスク（*）を使用することができます。たとえば`net*`と指定すると、`network`、`netware`、`netscape`などに一致します。

英数字以外の文字（アスタリスク文字を含む）を検索するには、検索文字列を引用符で囲みます。たとえば、次の文字列を検索するとします。

```
Find an asterisk (*)
```

次のように入力します。

```
"Find an asterisk (*)"
```

ワイルドカードを使用できるテキストフィールドで、部分的な文字列に一致させるには、ワイルドカードを使用する**必要**があることに注意してください。たとえば、ページ ビューを含む（つまりメッセージが「Page View」である）すべての監査レコードを監査ログ内で検索する場合、「`Page`」を検索しても結果は返されません。代わりに、「`Page*`」と指定してください。

一部のフィールドでは、アスタリスクを使用せずにフィールドの内容をすべてまたは一部検索することができます。完全一致の場合は、検索文字列を引用符で囲む必要があります。引用符で囲まなかった場合は、部分一致が実行されます。たとえば、フィールド検索で、引用符を使用せずに`Scan Completed with Detection`という文字列を検索すると、該当フィールドに次の文字列が含まれているレコードと、該当フィールドが検索文字列と完全に一致するレコードが返されます。

```
Scan Completed, No Detections
Scan completed With Detections
```

検索でのオブジェクトとアプリケーションのフィルタ

Firepowerシステムでは、ネットワーク構成の一部として使用可能な名前付きオブジェクト、オブジェクト グループ、およびアプリケーション フィルタを作成できます。検索を実行または保存するときには、検索条件としてこれらのオブジェクト、グループ、およびフィルタを使用できます。

検索を実行するときに、オブジェクト、オブジェクトグループ、およびアプリケーションフィルタは`${object_name}`という形式で表示されます。たとえば、オブジェクト名`ten_ten_network`であるネットワーク オブジェクトは、検索では`${ten_ten_network}`と表されます。

検索基準としてオブジェクトを使用できる検索フィールドの横にはオブジェクト追加アイコン（＋）が表示され、これをクリックすることができます。

関連トピック

オブジェクト マネージャ （516 ページ）

検索で指定する時間制約

時間値を指定できる検索条件フィールドで使用可能な形式を、次の表に示します。

表 *323* : 検索フィールドにおける時間指定

時間の形式	例
`today [at HH:MMam|pm]`	`today` `today at 12:45pm`
`YYYY-DDMM- HH:MM:SS`	`2006-03-22 14:22:59`

時間値の前に、以下のいずれか 1 つの演算子を指定できます。

表 *324* : 時間指定の演算子

演算子	例	説明
<	`< 2006-03-22 14:22:59`	2006 年 3 月 22 日午後 2:23 より前のタイムスタンプを持つイベントを返します。
>	`> today at 2:45pm`	今日の午後 2 時 45 分より後のタイムスタンプを持つイベントを返します。

検索での IP アドレス

検索で IP アドレスを指定するときには、個別の IP アドレス、複数アドレスのカンマ区切りリスト、アドレス ブロック、またはハイフン（-）で区切った IP アドレス範囲を入力することができます。また、否定を使用することもできます。

IPv6 をサポートする検索（侵入イベント、接続データ、相関イベントの検索など）では、IPv4 アドレス、IPv6 アドレス、および CIDR/プレフィックス長アドレス ブロックを任意に組み合わせて入力できます。IP アドレスを使用してホストを検索した場合、結果には、少なくとも 1 つの IP アドレスが検索条件と一致するホストがすべて含まれます（つまり、IPv6 のアドレスの検索では、プライマリ アドレスが IPv4 であるホストが返されることがあります）。

CIDR またはプレフィックス長の表記を使用して IP アドレスのブロックを指定する場合、Firepower システムは、マスクまたはプレフィックス長で指定されたネットワーク IP アドレスの部分**のみ**を使用します。たとえば `10.1.2.3/8` と入力すると、Firepower システムは `10.0.0.0/8` を使用します。

IP アドレスをネットワーク オブジェクトによって表すことができるため、IP アドレス検索フィールドの横にあるネットワーク オブジェクト追加アイコン（＋）をクリックして、ネットワーク オブジェクトを IP アドレス検索基準として使用することもできます。

表 *325 :* 使用可能な *IP* アドレス構文

指定する項目	入力内容	例
単一の IP アドレス	その IP アドレス	`192.168.1.1` `2001:db8::abcd`
リストを使用した複数の IP アドレス	IP アドレスからなるカンマ区切りリスト。カンマの前後にスペースを追加**しない**でください。	`192.168.1.1,192.168.1.2` `2001:db8::b3ff,2001:db8::0202`
CIDR ブロックまたはプレフィックス長で指定できる IP アドレスの範囲	IPv4 CIDR または IPv6 プレフィクス長表記の IP アドレス ブロック。	`192.168.1.0/24` これは、サブネット マスク 255.255.255.0 である 192.168.1.0 ネットワーク内の任意の IP を指定します（つまり 192.168.1.0 から 192.168.1.255 まで）。
CIDR ブロックやプレフィクスで指定できない IP アドレスの範囲	ハイフンを使用した IP アドレス範囲。ハイフンの前後にスペースを入力**しない**でください。	`192.168.1.1-192.168.1.5` `2001:db8::0202-2001:db8::8329`

他の方法で否定を使用して IP アドレスまたは IP アドレス範囲を指定	IP アドレス、ブロック、または範囲の先頭に感嘆符を付ける。	`192.168.0.0/32,!192.168.1.10`
		`!2001:db8::/32`
		`!192.168.1.10,!2001:db8::/32`

関連トピック

Firepower システムの IP アドレス表記法 （20 ページ）

検索での管理対象デバイス

デバイスをグループ化している場合（FMC で、または実際のハイ アベイラビリティ設定あるいはスケーラビリティ設定として）、グループの名前を検索すると、グループ内のすべてのデバイスに対する結果が正しく返されます。

システムでグループ、デバイス ハイ アベイラビリティ ペア、またはスタックの一致が検出されると、検索を実行するために、そのグループ名、デバイス ハイ アベイラビリティ ペア名、またはスタック名が適切なメンバー デバイス名に置き換えられます。デバイス フィールドのデバイス グループ、デバイス ハイ アベイラビリティ ペア、またはスタックを使用する検索を保存すると、デバイス フィールドで指定した名前がシステムによって保存され、検索が実行されるたびにデバイス名の置換が再度実行されます。

検索でのポート

Firepower System では、検索においてポート番号の特定の構文に対応しています。次の入力が可能です。

- 単一のポート番号
- 複数のポート番号を含むカンマ区切りリスト
- 2 つのポート番号をハイフンで区切ることにより、ポート番号の範囲を表す
- 1 つのポート番号の後に、スラッシュで区切られたプロトコル省略形（侵入イベントを検索する場合のみ）
- 1 つのポート番号またはポート番号範囲の前に 1 つの感嘆符（指定されたポートの否定を表す）

（注） ポート番号や範囲を指定するときには、スペースを使用**しない**でください。

表 *326 :* ポート構文例

例	説明
`21`	ポート 21 でのすべてのイベントを返します（TCP および UDP イベントを含む）。
`!23`	ポート 23 上のイベントを除くすべてのイベントを返します。
`25/tcp`	ポート 25 でのすべての TCP 関連の侵入イベントを返します。
`21/tcp,25/tcp`	ポート 21、25 の TCP 関連侵入イベントをすべて戻します。
`21-25`	ポート 21 から 25 のイベントをすべて戻します。

検索のイベント フィールド

イベントを検索するときは、検索条件として次のフィールドを使用できます。

- 監査ログのワークフロー フィールド （399 ページ）
- アプリケーション データ フィールド （3232 ページ）
- アプリケーションの詳細データ フィールド （3235 ページ）
- キャプチャされたファイルのフィールド （3143 ページ）

- ホワイト リスト イベントのフィールド （3272 ページ）
- 接続イベントとセキュリティ インテリジェンス イベントのフィールド （3024 ページ）
- 相関イベントのフィールド （3267 ページ）
- ディスカバリ イベントのフィールド （3210 ページ）
- [ヘルス イベント（Health Events）] テーブル （382 ページ）
- ホスト属性データ フィールド （3219 ページ）
- ホスト データ フィールド （3212 ページ）
- ファイルおよびマルウェア イベント フィールド （3121 ページ）
- 侵入イベント フィールド （3059 ページ）
- 侵入ルール更新ログのフィールド （194 ページ）
- 修復ステータスのテーブル フィールド （3277 ページ）
- Nmap スキャン結果のフィールド （2545 ページ）
- サーバ データ フィールド （3228 ページ）
- サードパーティの脆弱性データのフィールド （3244 ページ）
- ユーザ関連フィールド （3245 ページ）
- 脆弱性データのフィールド （3237 ページ）
- ホワイト リスト違反のフィールド （3274 ページ）

検索の実行

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Any Security Analyst

ステップ 1 **[Analysis]** > **[Search]**を選択します。

任意のワークフローのページで [検索の編集（Edit Search）] をクリックすることもできます。

ステップ 2 検索ページの左側にあるドロップダウン リストから、検索するイベントやデータのタイプを選択します。

ステップ 3 該当するフィールドに検索条件を入力します。検索の制約 （2968 ページ）を参照してください。

ステップ 4 （オプション）後で同じ検索を実行する場合は、検索設定の保存 （2974 ページ）の説明に従い、検索を保存します。

ステップ 5 [検索（Search）] をクリックします。

検索結果は、検索しているテーブルのデフォルト ワークフローに表示され、該当する場合は時間の制約があります。

次のタスク

ワークフローを使用して検索結果を分析する場合は、ワークフローの使用（2931ページ）を参照してください。

関連トピック

イベント ビュー設定の設定 （43 ページ）

検索設定の保存

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Any Security Analyst

マルチドメイン展開では、現在のドメインで作成された保存済みの検索が表示されます。これは編集できます。先祖ドメインで作成された保存済みの検索も表示されますが、これは編集できません。下位のドメインで作成された検索を表示および編集するには、そのドメインに切り替えます。

始める前に

- 検索の実行（2973ページ）で説明するように検索条件を設定するか、保存済み検索設定のロード （2975 ページ）で説明するように保存した検索をロードします。

ステップ 1 [検索（Search）]ページから、自分だけがアクセスできるように検索設定をプライベートとして保存する場合は、[プライベート（Private）] チェックボックスをオンにします。

ヒント カスタム ユーザ ロールのデータの制限として検索を使用する場合は、**必ず**プライベート検索として保存する必要があります。

ステップ 2 次の 2 つの対処法があります。

- ロードした検索設定の新しいバージョンを保存する場合は、[新規に保存（Save As New）] をクリックします。
- 新しい検索結果を保存する場合や、同じ名前を使用してカスタム検索を上書きする場合は、[保存（Save）] をクリックします。 コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

保存済み検索設定のロード

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Any Security Analyst

マルチドメイン展開では、現在のドメインで作成された保存済みの検索が表示されます。これは編集できます。先祖ドメインで作成された保存済みの検索も表示されますが、これは編集できません。下位のドメインで作成された検索を表示および編集するには、そのドメインに切り替えます。

ステップ 1 **[Analysis]** > **[Search]**を選択します。

ヒント また、ワークフローの任意のページから [検索（Search）] をクリックすることもできます。

ステップ 2 テーブルのドロップダウンリストから、検索するイベントまたはデータのタイプを選択します。

ステップ 3 [カスタム検索（Custom Searches）] リストまたは [定義済の検索（Predefined Searches）] リストから、ロードする検索を選択します。

ステップ 4 別の検索条件を使用するには、検索の制約を変更します。

ステップ 5 変更した検索を将来再度使用する場合は、検索を保存しておきます。詳細については、検索設定の保存（2974 ページ）を参照してください。

ステップ 6 [検索（Search）] をクリックします。

シェルによるクエリ オーバーライド

システム管理者は、Linux シェル ベースのクエリ管理ツールを使用して、実行時間の長いクエリを検出および停止することができます。

クエリ管理ツールでは指定した分数よりも実行時間が長いクエリを検索し、それらのクエリを停止することができます。ユーザがクエリを停止すると、このツールにより監査ログと syslog にイベントが記録されます。

`admin` 内部ユーザは FMC CLI にアクセスできることに注意してください。CLI アクセスを与える外部認証オブジェクトを使用する場合、シェル アクセス フィルタに一致するユーザもまた CLI にログインできます。

（注） Web インターフェイス内の検索ページを終了しても、クエリは停止しません。長い時間をかけて結果を返すクエリは、クエリ実行中にシステム全体のパフォーマンスに影響を与えます。

シェルベースのクエリ管理の構文

実行時間が長いクエリを管理するには、次の構文を使用します。

```
query_manager [-v] [-l [minutes]] [-k query_id [...]] [--kill-all minutes]
```

表 327 : `query_manager` オプション

オプション	説明
`-h, --help`	短いヘルプ メッセージを出力します。
`-l, --list [minutes]`	指定された時間（分単位）を超えるすべてのクエリをリストします。デフォルトで、1分より長くかかっているすべてのクエリを表示します。
`-k, --kill query_id [...]`	指定された ID を持つクエリを強制終了します。オプションは複数の ID を取得する場合があります。
`--kill-all minutes`	指定された時間（分単位）を超えるすべてのクエリを強制終了します。
`-v, --verbose`	完全な SQL クエリを含む詳細な出力。

注意 システム セキュリティ上の理由から、アプライアンスでは追加の Linux シェル ユーザを確立しないことを強く推奨します。

実行時間が長いクエリの停止

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	シェルまたはCLIアクセス権がある `admin` または外部で認証されたユーザ

ステップ 1 `ssh` を使用してFirepower Management Centerに接続します。

ステップ 2 CLIアクセスが有効になっている場合は、CLI `expert` コマンドを使用してLinuxシェルにアクセスします。

ステップ 3 シェルベースのクエリ管理の構文 （2976ページ）で説明された構文を使用して、`sudo` で `query_manager` を実行します。

第 122 章

カスタム ワークフロー

次のトピックでは、カスタム ワークフローの使用方法について説明します。

カスタム ワークフローの概要

シスコが提供する事前定義のカスタム ワークフローがニーズに合わない場合は、カスタム ワークフローを作成して管理することができます。

カスタム ワークフローは、組織に特有のニーズに合わせて作成するワークフローです。カスタム ワークフローを作成する場合は、ワークフローのベースとなるイベント（またはデータベース テーブル）の種類を選択します。Firepower Management Centerでは、カスタム ワークフローをカスタム テーブルのベースにすることができます。また、カスタム ワークフローに含まれるページを選択することもできます。カスタム ワークフローには、ドリルダウン、テーブル ビュー、ホストまたはパケット ビューのページを含めることができます。

イベント評価プロセスが変わった場合には、新しいニーズを満たすようにカスタム ワークフローを編集することができます。事前定義のワークフローは編集できないことに注意してください。

ヒント 任意のイベント タイプについて、デフォルト ワークフローとしてカスタム ワークフローを設定することができます。

保存済みカスタム ワークフロー

Firepower Management Center は、変更可能な定義済みのワークフローの他に保存済みのカスタム ワークフローを含みます。それぞれのワークフローは、カスタム テーブルに基づき、いずれも変更可能です。

マルチドメイン展開では、これらの保存されたワークフローは、グローバル ドメインに属し、下位ドメインでは変更できません。

表 *328 :* 保存済みカスタム ワークフロー

ワークフロー名	説明
Events by Impact, Priority, and Host Criticality（影響、優先度、およびホストの重大度に基づいたイベント）	このワークフローを使用して、ネットワークにとって重要であり、現在脆弱であり、現在攻撃を受けている可能性のあるホストを迅速に選択して、そのホストに焦点を合わせることができます。 このワークフローは、宛先重要度のカスタム テーブルのある侵入イベントに基づいています。
優先度および分類によるイベント	このワークフローでは、イベントとタイプのリストをそれぞれのイベントが発生した回数と共にイベントの優先度の順に示します。 このワークフローは、侵入イベントのカスタム テーブルに基づきます。
宛先、影響度、ホストの重要度を有するイベント	このワークフローを使用して、ネットワークにとって重要であり、現在脆弱であるホストの最新の攻撃を検出できます。 このワークフローは、宛先重要度のカスタム テーブルのある侵入イベントに基づいています。
サーバのデフォルト ワークフローのあるホスト	このワークフローを使用すると、サーバのカスタム テーブルと共にホストの基本的な情報をすぐに表示できます。 このワークフローは、サーバのカスタム テーブルのあるホストに基づきます。
宛先重要度のデフォルト ワークフローのある侵入イベント	このワークフローを使用すると、宛先重要度のカスタム テーブルと共に侵入イベントの基本的な情報をすぐに表示できます。 このワークフローは、宛先重要度のカスタム テーブルのある侵入イベントに基づいています。

ワークフロー名	説明
送信元重要度のデフォルト ワークフローのある侵入イベント	このワークフローを使用すると、送信元重要度のカスタム テーブルと共に侵入イベントの基本的な情報をすぐに表示できます。 このワークフローは、送信元重要度のカスタム テーブルのある侵入イベントに基づいています。
サーバとホストの詳細	このワークフローを使用して、ネットワークで最も高頻度で使用されているサーバやそのサーバを稼働しているホストを決定できます。 このワークフローは、サーバのカスタム テーブルのあるホストに基づきます。

カスタム ワークフローの作成

シスコが提供する事前定義のカスタム ワークフローがニーズに合わない場合は、カスタム ワークフローを作成することができます。

ヒント 新しいカスタム ワークフローを作成する代わりに、別のアプライアンスからカスタム ワークフローをエクスポートし、それを自身のアプライアンスへインポートすることができます。その後でニーズに合わせて、インポートしたワークフローを編集することができます。

カスタム ワークフローを作成する場合は、次の操作を行います。

- ワークフローのソースとなるテーブルを選択する
- ワークフローの名前を指定する
- ワークフローにドリル ダウン ページおよびテーブル ビュー ページを追加する

ワークフローの各ドリル ダウン ページでは、次のことができます。

- Web インターフェイスのページの上部に表示される名前を指定する
- 1 ページにつき最大 5 個のカラムを含める
- デフォルトのソート順（昇順または降順）を指定する

ワークフロー ページの順序において、任意の場所にテーブル ビュー ページを追加することができます。これらのページには編集可能なプロパティ（ページ名、ソート順、ユーザ定義可能なカラム位置など）がありません。

（注） カスタム ワークフローには、イベントのドリル ダウン ページまたはテーブル ビューを少なくとも 1 つ追加する必要があります。

（注） テーブル タイプに [脆弱性（Vulnerabilities）] を選択し、テーブル カラムに [IP アドレス（IP Address）] を追加しても、検索機能を使用して特定の IP アドレスまたはアドレスのブロックを表示するようワークフローを制約しない限り、カスタム ワークフローを使用して脆弱性を表示する場合に [IP アドレス（IP Address）] カラムは表示されません。

カスタム ワークフローの最終ページは、次の表に記載されているように、ワークフローのベースにしているテーブルによって異なります。これらの最終ページは、ワークフローを作成したときにデフォルトで追加されます。

表 *329* : カスタム ワークフローの最終ページ

イベント/アセット タイプ	最終ページ
ディスカバリ イベント	ホスト
脆弱性	脆弱性の詳細
サードパーティの脆弱性	ホスト
Users	Users
侵害の兆候	ホストまたはユーザ
侵入イベント	パケット

システムは、他の種類のイベント（監査ログやマルウェア イベントなど）に基づくカスタム ワークフローには最終ページを追加しません。

接続データに基づくカスタム ワークフローもその他のカスタム ワークフローと同様です。ただし、接続データに基づくカスタム ワークフローには接続の要約データを含むドリル ダウン ページや個々の接続とテーブル ビュー ページを含むドリル ダウン ページを入れることができます。

非接続データに基づくカスタム ワークフローの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Any Security Analyst

ステップ 1 **[Analysis]** > **[Advanced]** > **[Custom Workflows]**を選択します。

ステップ 2 [カスタム ワークフローの作成（Create Custom Workflow）] をクリックします。

ステップ 3 [名前（Name）] フィールドにワークフローの名前を入力します。

ステップ 4 必要に応じて、[説明（Description）] を入力します。

ステップ 5 [テーブル（Table）] ドロップダウン リストから、対象とするテーブルを選択します。

ステップ 6 ワークフローに1つ以上のドリルダウン ページを追加する場合は、[ページの追加（Add Page）] をクリックします。

ステップ 7 [ページ名（Page Name）] フィールドにページの名前を入力します。

ステップ 8 [カラム 1（Column 1）] で、ソートの優先順位およびテーブルのカラムを選択します。このカラムは、ページの最も左のカラムとして表示されます。

例：

たとえば、対象とする宛先ポートを示すページを作成し、カウントでページをソートするには、[ソートの優先順位（Sort Priority）] ドロップダウン リストから [2] を選択し、[フィールド（Field）] ドロップダウン リストから [宛先ポート/ICMP コード（Destination Port/ICMP Code）] を選択します。

ステップ 9 ページに表示するすべてのフィールドが指定されるまで、含めるフィールドの選択とソートの優先順位の設定を続けます。

ステップ 10 ワークフローにテーブル ビュー ページを追加するには、[テーブル ビューの追加（Add Table View）] をクリックします。

ステップ 11 **[保存（Save）]** をクリックします。

カスタム接続データ ワークフローの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin

接続データに基づいたカスタム ワークフローは他のカスタム ワークフローと似ていますが、ドリルダウン ページとテーブル ビュー ページだけでなく、接続データ グラフのページも含めることができます。必要に応じて、ワークフローにそれぞれのタイプのページを任意の数だけ、任意の順序で含めることができます。それぞれの接続データ グラフのページには1つのグラフ（線グラフ、棒グラフ、または円グラフ）が含まれます。線グラフと棒グラフには、複数のデータセットを含めることができます。

ステップ 1 **[Analysis]** > **[Advanced]** > **[Custom Workflows]**を選択します。

ステップ 2 [カスタム ワークフローの作成（Create Custom Workflow）] をクリックします。

ステップ 3 [名前（Name）] フィールドにワークフローの名前を入力します。

ステップ 4 必要に応じて、[説明（Description）] を入力します。

ステップ 5 [テーブル（Table）] ドロップダウン リストから、[接続イベント（Connection Events）] を選択します。

ステップ 6 ワークフローに 1 つ以上のドリルダウン ページを追加する場合は、次の 2 つのオプションがあります。

- 個々の接続に関するデータが含まれているドリルダウンページを追加するには、[ページの追加（Add Page）] をクリックします。
- 接続の概要データが含まれているドリルダウンページを追加するには、[サマリーページの追加（Add Summary Page）] をクリックします。

ステップ 7 [ページ名（Page Name）] フィールドにページの名前を入力します。

ステップ 8 [カラム 1（Column 1）] で、ソートの優先順位およびテーブルのカラムを選択します。このカラムは、ページの最も左のカラムとして表示されます。

ステップ 9 ページに表示するすべてのフィールドが指定されるまで、含めるフィールドの選択とソートの優先順位の設定を続けます。

例：

たとえば、監視対象ネットワーク経由で転送されるトラフィックの量を表示するページを作成し、トラフィックの転送量が最も多い応答側によってページをソートするには、[ソートの優先順位（Sort Priority）] ドロップダウン リストで [1] を選択し、[フィールド（Field）] ドロップダウン リストで [応答側のバイト数（Responder Bytes）] を選択します。

ステップ 10 ワークフローに 1 つ以上のグラフ ページを追加する場合は、[グラフの追加（Add Graph）] をクリックします。

ステップ 11 [グラフ名（Graph Name）] フィールドにページの名前を入力します。

ステップ 12 ページに含めるグラフのタイプを選択します。

- 線グラフ（  ）
- 棒グラフ（  ）
- 円グラフ（  ）

ステップ 13 グラフの X 軸と Y 軸を選択し、グラフ化するデータの種類を指定します。

円グラフでは、X 軸は独立変数を表し、Y 軸は従属変数を表します。

ステップ 14 グラフに含めるデータセットを選択します。

円グラフには 1 つのデータセットしか含めることができないことに注意してください。

ステップ 15 接続データのテーブル ビューを追加するには、[テーブル ビューの追加（Add Table View）] をクリックします。

テーブル ビューは設定できません。

ステップ 16 **[保存（Save）]** をクリックします。

カスタム ワークフローの使用と管理

ワークフローが、事前定義のイベント テーブルまたはカスタム テーブルのいずれに基づいているかによって、ワークフローの表示に使用する方法が異なります。

カスタム ワークフローが事前定義のイベント テーブルに基づいている場合は、アプライアンスに付属しているワークフローにアクセスするのと同じ方法でアクセスします。たとえば、ホスト テーブルに基づいているカスタム ワークフローにアクセスするには、**[Analysis]** > **[Hosts]** > **[Hosts]** を選びます。また、カスタム ワークフローがカスタム テーブルに基づいている場合は、[カスタム テーブル（Custom Tables）] ページからアクセスする必要があります。

イベント評価プロセスが変わった場合には、新しいニーズを満たすようにカスタム ワークフローを編集することができます。事前定義のワークフローは編集できないことに注意してください。

ヒント 任意のイベント タイプについて、デフォルト ワークフローとしてカスタム ワークフローを設定することができます。

事前定義されたテーブルに基づいたカスタム ワークフローの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Maint/Any Security Analyst（ワークフローに応じて異なります）

ステップ 1 ワークフローの選択 （2933 ページ）の説明に従って、カスタム ワークフローのベースとなるテーブルについて、適切なメニュー パスとオプションを選択します。

ステップ 2 カスタム ワークフローも含め、別のワークフローを使用するには、現在のワークフロータイトルの横にある [(ワークフローの切り替え)（(switch workflow)）] をクリックします。

ステップ 3 イベントが表示されず、ワークフローを時間によって制約できる場合は、時間範囲の調整が必要なことがあります（イベント時間の制約 （2952 ページ）を参照）。

カスタム テーブルに基づいたカスタム ワークフローの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Any Security Analyst

マルチドメイン展開では、現在のドメインで作成されたカスタム ワークフローが表示されます。これは編集できます。先祖ドメインで作成されたカスタム ワークフローも表示されますが、これは編集できません。下位のドメインのカスタム ワークフローを表示および編集するには、そのドメインに切り替えます。

ステップ 1 **[Analysis]** > **[Advanced]** > **[Custom Tables]**を選択します。

ステップ 2 表示するカスタム テーブルの隣にある表示アイコン（  ）をクリックするか、またはカスタム テーブルの名前をクリックします。

ステップ 3 カスタム ワークフローも含め、別のワークフローを使用するには、現在のワークフロー タイトルの横にある [(ワークフローの切り替え)（(switch workflow)）] をクリックします。

ステップ 4 イベントが表示されず、ワークフローを時間によって制約できる場合は、時間範囲の調整が必要なことがあります（イベント時間の制約 （2952 ページ）を参照）。

カスタム ワークフローの編集

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Any Security Analyst

マルチドメイン展開では、現在のドメインで作成されたカスタム ワークフローが表示されます。これは編集できます。先祖ドメインで作成されたカスタム ワークフローも表示されますが、これは編集できません。下位のドメインのカスタム ワークフローを表示および編集するには、そのドメインに切り替えます。

ステップ 1 **[Analysis]** > **[Advanced]** > **[Custom Workflows]**を選択します。

ステップ 2 編集するワークフロー名の横にある編集アイコン（  ）をクリックします。

代わりに表示アイコン（  ）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 ワークフローに必要な変更を加えます。

ステップ 4 **[保存（Save）]** をクリックします。

第 123 章

カスタム テーブル

次のトピックでは、カスタム テーブルの使用方法について説明します。

カスタム テーブルの概要

Firepower システムがネットワークに関する情報を収集し、Firepower Management Center がその情報を一連のデータベース テーブルに保存します。結果として生成される情報を表示するためにワークフローを使用する場合、Firepower Management Center はそれらのテーブルのいずれかからデータを取り出します。たとえば、[Network Applications by Count] ワークフローの各ページのカラムは、[Applications] テーブルのフィールドから取得されます。

さまざまなテーブルのフィールドを結合することにより、ネットワークのアクティビティの分析が向上する場合、カスタム テーブルを作成できます。たとえば、定義済みの [Host Attributes] テーブルのホスト重大度情報と、定義済みの [Connection Data] テーブルのフィールドを結合してから、新しいコンテキストで接続データを検証できます。

定義済みのテーブルまたはカスタム テーブルのどちらについても、カスタム ワークフローを作成できます。

定義済みのカスタム テーブル

カスタム テーブルには、2 つまたは 3 つの定義済みテーブルのフィールドを含みます。Firepower System は、いくつかのシステム定義のカスタム テーブルと共に配布されますが、特定のニーズに適合する情報のみを含む追加のカスタム テーブルを作成できます。

たとえば、Firepower System は、侵入イベントとホスト データを相関するシステム定義のカスタム テーブルと共に配布されます。そのため、クリティカル システムに影響を及ぼすイベントを検索でき、1 つのワークフローにその検索結果を表示できます。

マルチドメイン展開では、定義済みのカスタム テーブルは、グローバル ドメインに属し、下位ドメインで変更することはできません。

次の表では、システムと共に提供されるカスタム テーブルについて説明します。

表 *330 :* システム定義カスタム テーブル

テーブル	説明
Hosts with Servers	ネットワーク上で実行されている検出されたアプリケーションに関する情報と、それらのアプリケーションを実行しているホストに関する基本的なオペレーティング システム情報を提供する、[Hosts] および [Servers] テーブルのフィールドが含まれます。
Intrusion Events with Destination Criticality	侵入イベント テーブルとホスト テーブルのフィールドを含み、侵入イベントに関する情報と各侵入イベントに含まれる宛先ホストのホスト重要度を提供します。 このテーブルを使用して、ホスト重要度の高い宛先ホストに関与する侵入イベントを検索できます。
侵入イベントと送信元重要度（Intrusion Events with Source Criticality）	侵入イベント テーブルとホスト テーブルのフィールドを含み、侵入イベントに関する情報と各侵入イベントに含まれる送信元ホストのホスト重要度を提供します。 このテーブルを使用して、ホスト重要度の高い送信元ホストに関与する侵入イベントを検索できます。

可能なテーブルの組み合わせ

カスタムテーブルを作成する場合、関連データのある定義済みのテーブルのフィールドを組み合わせことができます。次の表は、新しいカスタムテーブルを作成するために結合できる定義済みのテーブルをリストしています。2つ以上の定義済みのカスタムテーブルのフィールドを組み合わせるカスタム テーブルを作成できます。

表 *331 :* カスタム テーブルの組み合わせ

組み合わせ可能なカスタム テーブル	以下のテーブルのフィールドと結合可能
Applications	• Correlation Events • Intrusion Events • Connection Summary Data • Host Attributes • Application Details • Discovery Events • Connection Events • Hosts • Servers • White List Events
Correlation Events	• Applications • Host Attributes • Hosts
Intrusion Events	• Applications • Host Attributes • Hosts • Servers
Connection Summary Data	• Applications • Host Attributes • Hosts • サーバ

組み合わせ可能なカスタム テーブル	以下のテーブルのフィールドと結合可能
ホストの侵害の兆候（Host Indications of Compromise）	• アプリケーション • Application Details • Captured Files • Connection Events • Connection Summary Data • Correlation Events • Discovery Events • Host Attributes • Hosts • Intrusion Events • Security Intelligence Events • Servers • White List Events
Host Attributes	• Applications • Correlation Events • Intrusion Events • Connection Summary Data • Application Details • Discovery Events • Connection Events • Hosts • Servers • White List Events
Application Details	• Applications • Host Attributes • Hosts
Discovery Events	• Applications • Host Attributes • Hosts

組み合わせ可能なカスタム テーブル	以下のテーブルのフィールドと結合可能
Connection Events	• Applications • Host Attributes • Hosts • Servers
Security Intelligence Events	• Applications • Host Attributes • Hosts • Servers
Hosts	• Applications • Correlation Events • Intrusion Events • Connection Summary Data • Host Attributes • Application Details • Discovery Events • Connection Events • Servers • White List Events
Servers	• Applications • Intrusion Events • Connection Summary Data • Host Attributes • Connection Events • Hosts
White List Events	• Applications • Host Attributes • Hosts

あるテーブルのフィールドが、別のテーブルの複数のフィールドにマップされる場合があります。たとえば、定義済みの [Intrusion Events with Destination Criticality] カスタム テーブルは、[Intrusion Events] テーブルと [Hosts] テーブルのフィールドを結合します。[Intrusion Events] テーブルの各イベントは、2 つの IP アドレス（送信元 IP アドレスと宛先 IP アドレス）と関連付けられています。しかし、[ホスト（Hosts）]テーブルの「イベント」はそれぞれ、単一のホスト IP アドレスを表します（ホストに複数の IP アドレスが存在する場合があります）。したがって、[Intrusion Events] テーブルと [Hosts] テーブルに基づいてカスタム テーブルを作成する場合は、[Hosts] テーブルから表示するデータが [Intrusion Events] テーブルのホストの送信元 IP アドレスまたはホストの宛先 IP アドレスのどちらに適用されるかを選択する必要があります。

新しいカスタム テーブルを作成すると、テーブルのすべてのカラムを表示するデフォルトのワークフローが自動的に作成されます。定義済みのテーブルと同じように、ネットワーク分析で使用するデータをカスタムテーブルで検索することもできます。定義済みのテーブルを使用して可能であるように、カスタム テーブルに基づいてレポートを作成できます。

ユーザ定義のカスタム テーブル

ヒント　新しいカスタム テーブルを作成する代わりに、別の Firepower Management Center からカスタム テーブルをエクスポートし、Firepower Management Center にインポートすることができます。

カスタム テーブルを作成するには、Firepower システムに付属しているどの定義済みテーブルに、カスタムテーブルに組み込むフィールドが含まれているかを判断します。その後、組み込むフィールドを選択できます。さらに、必要に応じて、共通フィールドのフィールドマッピングを設定することもできます。

ヒント　[Hosts] テーブルを含むデータでは、1 つの IP アドレスではなく、1 つのホストのすべての IP アドレスに関連したデータを表示できます。

例として、[Correlation Events] テーブルと [Hosts] テーブルのフィールドを結合するカスタム テーブルについて考慮します。このカスタムテーブルを使用して、相関ポリシーの違反に関係するホストの詳細情報を取得できます。注意すべき点として、[Correlation Events] テーブルの送信元 IP アドレスと宛先 IP アドレスのどちらと一致する [Hosts] テーブルのデータを表示するかを決定する必要があります。

このカスタム テーブルのイベントのテーブル ビューを表示する場合、相関イベントが 1 行に 1 つずつ表示されます。次の情報を含むようにカスタム テーブルを設定できます。

- イベントが生成された日時
- 違反された相関ポリシーの名前
- 違反をトリガーとして使用した規則の名前
- 相関イベントに関係する送信元ホスト（開始ホスト）に関連付けられた IP アドレス

- 送信元ホストの NetBIOS 名
- 送信元ホストが実行しているオペレーティング システムおよびバージョン
- 送信元ホストの重大度

ヒント　宛先ホスト（応答ホスト）の同じ情報を表示する同様のカスタムテーブルを作成することもできます。

カスタム テーブルの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Any/Admin

ステップ 1　**[Analysis]** > **[Advanced]** > **[Custom Tables]**を選択します。

ステップ 2　[カスタム テーブルの作成（Create Custom Table）] をクリックします。

ステップ 3　[名前（Name）] フィールドに、カスタム テーブルの名前を入力します。

例：

たとえば、`Correlation Events with Host Information (Src IP)` と入力します。

ステップ 4　[テーブル（Tables）] ドロップダウン リストから、[相関イベント（Correlation Events）] を選択します。

ステップ 5　[フィールド（Fields）] で [時間（Time）] を選択し、[追加（Add）] をクリックして、相関イベントが生成された日時を追加します。

ステップ 6　手順 5 を繰り返して、[ポリシー（Policy）] および [ルール（Rule）] フィールドを追加します。

ヒント　Ctrl または Shift を押しながらクリックすることにより、複数のフィールドを選択できます。また、クリックしてドラッグすることで、隣接する複数の値を選択できます。ただし、テーブルに関連したイベントのテーブル ビューでフィールドが表示される順序を指定する場合は、フィールドを一度に 1 つずつ追加します。

ステップ 7　[テーブル（Tables）] ドロップダウンリストから [ホスト（Hosts）] を選択します。

ステップ 8　[IP アドレス（IP Address）]、[NetBIOS 名（NetBIOS Name）]、[OS 名（OS Name）]、[OS バージョン（OS Version）]、[ホストの重大度（Host Criticality）] フィールドをカスタム テーブルに追加します。

ステップ 9　[相関イベント（Correlation Events）] の隣にある [共通フィールド（Common Fields）] で、[送信元 IP（Source IP）] を選択します。

相関イベントに関係する送信元ホスト（開始ホスト）用に手順 8 で選択したホスト情報を表示するように、カスタム テーブルが設定されます。

ヒント　相関イベントに関係する宛先ホスト（応答ホスト）に関する詳細なホスト情報を表示するカスタム テーブルを作成する場合も、この手順に従いますが、[送信元 IP（Source IP）] ではなく、[送信先 IP（Destination IP）] を選択します。

ステップ 10　**[保存（Save）]** をクリックします。

カスタム テーブルの変更

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Any/Admin

マルチドメイン展開では、現在のドメインで作成されたカスタムテーブルが表示されます。これは編集できます。先祖ドメインで作成されたカスタムテーブルも表示されますが、これは編集できません。下位のドメインのカスタムテーブルを表示および編集するには、そのドメインに切り替えます。

ステップ 1　**[Analysis]** > **[Advanced]** > **[Custom Tables]**を選択します。

ステップ 2　編集するテーブルの横にある編集アイコン（  ）をクリックします。

代わりに表示アイコン（  ）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3　除外するフィールドの横にある削除アイコン（  ）をクリックして、テーブルからフィールドを除外することもできます。

（注）　レポートで現在使用中のフィールドを削除すると、それらのフィールドを使用しているセクションをそれらのレポートから除外するか確認するプロンプトが表示されます。

ステップ 4　必要に応じて、その他の変更を実行します。

ステップ 5　**[保存（Save）]** をクリックします。

カスタム テーブルの削除

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Any/Admin

マルチドメイン導入では、現在のドメインで作成されたカスタムテーブルが表示されます。これは削除できます。先祖ドメインで作成されたカスタムテーブルも表示されますが、これは削除できません。下位のドメインのカスタムテーブルを削除するには、そのドメインに切り替えます。

ステップ 1 **[Analysis]** > **[Advanced]** > **[Custom Tables]**を選択します。

ステップ 2 削除するカスタム テーブルの隣にある削除アイコン（）をクリックします。

コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

カスタム テーブルに基づいたワークフローの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Any/Admin

カスタムテーブルを作成すると、そのデフォルトのワークフローがシステムによって自動的に作成されます。このワークフローの最初のページには、イベントのテーブル ビューが表示されます。カスタム テーブルに侵入イベントを含める場合、ワークフローの 2 番目のページはパケット ビューになります。それ以外の場合、ワークフローの 2 番目のページはホスト ページになります。カスタム テーブルに基づいて、独自のカスタム ワークフローを作成することもできます。

ヒント カスタム テーブルに基づいてカスタム ワークフローを作成する場合、それをそのテーブルのデフォルトのワークフローとして指定できます。

同じ手法を使用して、定義済みのテーブルに基づいたイベント ビューに使用するカスタムテーブルでイベントを表示できます。

マルチドメイン展開では、現在のドメインで作成されたカスタムテーブルが表示されます。これは編集できます。先祖ドメインで作成されたカスタムテーブルも表示されますが、これは編集できません。下位のドメインのカスタムテーブルを表示および編集するには、そのドメインに切り替えます。

ステップ 1 **[Analysis]** > **[Advanced]** > **[Custom Tables]**を選択します。

ステップ 2 表示するワークフローに関連するカスタム テーブルの隣にある表示アイコン（）をクリックします。

カスタム テーブルの検索

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Any/Admin

マルチドメイン展開では、現在のドメインで作成されたカスタムテーブルが表示されます。これは編集できます。先祖ドメインで作成されたカスタムテーブルも表示されますが、これは編集できません。下位のドメインのカスタムテーブルを表示および編集するには、そのドメインに切り替えます。

ステップ 1 **[Analysis]** > **[Advanced]** > **[Custom Tables]**を選択します。

ステップ 2 検索するカスタム テーブルの隣にある表示アイコン（）をクリックします。

ヒント カスタム ワークフローなど、別のワークフローを使用するには、ワークフローのタイトルの横の[（ワークフローの切り替え）（(switch workflow)）] をクリックします。

ステップ 3 [検索（Search）] をクリックします。

ヒント 別の種類のイベントやデータについてデータベースを検索する場合は、その種類をテーブル ドロップダウンリストから選択します。

ステップ 4 該当するフィールドに、検索条件を入力します。

複数のフィールドに条件を入力して検索すると、すべてのフィールドに対して指定された検索条件に一致するレコードのみが返されます。

ヒント 検索基準としてオブジェクトを使用する場合は、検索フィールドの横にあるオブジェクト アイコン（）をクリックします。

ステップ 5 必要に応じて、検索を保存する場合は、[プライベート（Private）] チェックボックスをオンにして、プライベートとして検索を保存すると、その検索に本人のみがアクセスできるようになります。本人のみではなくすべてのユーザを対象にする場合は、このチェックボックスをオフのままにして検索を保存します。

ヒント カスタム ユーザ ロールに関するデータ制約として検索を使用する予定の場合は、それをプライベート検索として保存する**必要があります**。

ステップ 6 （任意）検索を保存して、後でそれを再使用できます。次の選択肢があります。

- [保存（Save）] をクリックして、検索条件を保存します。[プライベート（Private）] チェックボックスをオンにすると、その検索は本人のアカウントでのみ表示できるようになります。
- 新しい検索を保存するか、以前保存した検索を変更して作成した検索に名前を割り当てるには、[新規に保存（Save As New）] をクリックします。[プライベート（Private）] チェックボックスをオンにすると、その検索は本人のアカウントでのみ保存および表示できるようになります。

ステップ 7 [検索（Search）] をクリックして、検索を開始します。
検索結果は、現在の時間範囲によって制限されている、カスタム テーブルのデフォルトのワークフローに表示されます（該当する場合）。

第 XXVII 部

イベントとアセット

第 124 章

接続ロギング

次のトピックでは、モニタ対象ネットワークでホストから実行される接続を記録するよう Firepower システムを設定する方法について説明します。

接続ロギングについて

システムは、管理対象デバイスが検出した接続のログを生成することができます。このログは接続イベントと呼ばれます。ルールやポリシーの設定を行うことで、ログに記録する接続の種類、接続をログに記録するタイミング、およびデータを保存する場所をきめ細かく制御できます。セキュリティ インテリジェンス イベントと呼ばれる特別な接続イベントは、レピュテーションベースのセキュリティ インテリジェンス機能によってブラックリストに登録（ブロック）された接続を表します。

接続イベントには、検出されたセッションに関するデータも含まれています。個々の接続イベントで入手可能な情報はいくつかの要因に応じて異なりますが、一般的には次のものがあります。

- タイムスタンプ、送信元と宛先の IP アドレス、入出力ゾーン、接続を処理したデバイスなど、基本的な接続特性
- アプリケーション、要求されるURL、または接続に関連付けられているユーザなど、システムによって検出または推測される追加の接続特性
- どの設定がトラフィックを処理したか、接続が許可またはブロックされていたかどうか、暗号化された接続および復号された接続に関する詳細など、接続がログに記録された理由に関するメタデータ

部門のセキュリティ上およびコンプライアンス上の要件に従って接続をロギングしてください。接続ロギングを設定する際は、システムはさまざまな理由で接続をロギングすることがあり、1ヵ所でロギングを無効にしても一致する接続がログに記録されなくなるとは限りません。

接続イベント内の情報は、トラフィックの特性、最終的に接続を処理した設定など、いくつかの要因によって異なります。

（注） エクスポートしたNetFlowレコードから生成された接続データを使い、管理対象デバイスで収集された接続ログを補うことができます。これは、Firepowerシステムの管理対象デバイスでモニタできないネットワーク上にNetFlow対応ルータやその他のデバイスを配置した場合に特に有効です。

関連トピック

Firepowerシステムの NetFlow データ （2477 ページ）

常にログに記録される接続

接続イベントのストレージを無効にしない限り、システムは他のロギング設定に関係なく、Firepower Management Center データベースに次の接続終了イベントを保存します。

侵入に関連付けられた接続

システムは、接続がアクセス コントロール ポリシーのデフォルトのアクションで処理される限り、侵入イベントに関連付けられている接続を自動的に記録します。

アクセス コントロールのデフォルト アクションに関連付けられた侵入ポリシーによって侵入イベントが生成された場合、システムは、そのイベントに関連する接続の終了を自動的にログに記録しません。代わりに、デフォルトのアクション接続のロギングを明示的に有効にする必要があります。これは、接続データをログに記録する必要がない、侵入防御専用の展開環境で役立ちます。

ただし、デフォルトアクションで接続開始ロギングを有効にした場合、接続開始のロギングに加えて、関連する侵入ポリシーがトリガーしたときにシステムによって接続終了がログに記録されます。

ファイル イベントとマルウェア イベントに関連付けられた接続

システムは、ファイル イベントとマルウェア イベントに関連付けられた接続を自動的にログに記録します。

（注） NetBIOS-SSN（SMB）トラフィックのインスペクションによって生成されるファイルイベントは、即座には接続イベントを生成しません。これは、クライアントとサーバが持続的接続を確立するためです。システムはクライアントまたはサーバがセッションを終了した後に接続イベントを生成します。

インテリジェント アプリケーション バイパスに関連付けられた接続

システムは、IABに関連付けられたバイパスされた、およびバイパスされるはずだった接続をログに記録します。

モニタ対象の接続

システムは常に、モニタの対象のトラフィックの接続終了をロギングします。このことは、トラフィックに一致する他のルールがなく、デフォルトアクションのロギングを有効にしていない場合でも該当します。詳細については、「モニタされた監視接続のロギング（3005ページ）」を参照してください。

ログ可能なその他の接続

重要な接続のみがロギングされるように、ルールごとの接続ロギングを有効にします。あるルールに対し接続ロギングを有効にすると、システムはそのルールによって処理されたすべての接続をロギングします。

また、ポリシーのデフォルト アクションにより処理された接続をロギングすることもできます。ルールやデフォルトアクションにより（アクセス制御の場合は、ルールのインスペクション設定により）、ロギングのオプションは異なります。

プレフィルタ ポリシー：ルールとデフォルト アクション

プレフィルタ ポリシーによりファースト パスまたはブロックする接続（すべてのプレーン テキスト、パススルー トンネルを含む）をロギングすることができます。

プレフィルタは、外部ヘッダーを基準にしてトラフィックを処理します。ロギングするトンネルでは、結果の接続イベントには、外部のカプセル化ヘッダー情報が含まれます。

継続分析の対象となるトラフィックについては、一致する接続が他の設定によってロギングされることがあるかもしれませんが、プレフィルタ ポリシーによるロギングは無効となります。システムは内部ヘッダーを使ってすべての継続分析を行います。つまり、システムは、許可されたトンネル内の各接続を個別に処理、ロギングします。

SSL ポリシー：ルールとデフォルト アクション

SSL ルールまたは SSL ポリシーのデフォルト アクションに一致する接続をロギングすることができます。

ブロックされた接続の場合、システムは即座にセッションを終了し、イベントを生成します。監視対象の接続やアクセス コントロール ルールに渡す接続の場合、システムはセッションが終了するとイベントを生成します。

アクセス コントロール ポリシー：セキュリティ インテリジェンスによる判断

接続がレピュテーションベースのセキュリティインテリジェンス機能によってブラックリスト登録（ブロック）される場合は、その接続をログに記録できます。

オプションで、セキュリティ インテリジェンス フィルタリングにはモニタ専用設定を使用できます。パッシブ展開環境では、この設定が推奨されます。この設定では、ブラックリスト登録されるはずの接続をシステムがさらに分析できるだけでなく、ブラックリストと一致する接続をログに記録することもできます。セキュリティインテリジェンスモニタリングによって、セキュリティ インテリジェンス情報を使用してトラフィック プロファイルを作成することもできます。

セキュリティインテリジェンスのフィルタリングの結果、システムが接続イベントをロギングすると、一致するセキュリティ インテリジェンス イベントもロギングされます。そのイベントは特殊なタイプの接続イベントで、個別に表示および分析することができ、また個別に保存、プルーニングされます。ブラックリストに掲載されている IP アドレスが接続にあるかどうかを識別できるように、[分析（Analysis）]>[接続（Connections）] メニューのページの表では、ブラックリストに掲載され、モニタされている IP アドレスの横のホスト アイコンは見た目が少し異なります。

アクセス コントロール ポリシー：ルールとデフォルト アクション

アクセス コントロール ルールまたはアクセス コントロール ポリシーのデフォルト アクションに一致する接続をロギングすることができます。

関連トピック

ルールとポリシーのアクションによるロギングへの影響 （3004 ページ）

ルールとポリシーのアクションによるロギングへの影響

接続イベントには、接続がロギングされた理由を記述したメタデータが含まれています。メタデータにはトラフィックがどの設定によって処理されたかなどの情報が含まれます。接続ロギングを設定する場合、ルール アクションおよびポリシーのデフォルト アクションにより、一致するトラフィックをシステムがどのように検査、処理するのかだけでなく、一致するトラフィックの詳細をいつ、どのようにロギングするかが決まります。

関連トピック

トンネルとプレフィルタ ルールのコンポーネント （1775 ページ）
TLS/SSL 規則アクション （1864 ページ）
アクセス コントロール ルールのアクション （1701 ページ）
接続イベントとセキュリティ インテリジェンス イベントのフィールド （3024 ページ）

FastPath された接続のロギング

FastPath された接続や非暗号化トンネルをロギングできます。ロギングには、プレフィルタ ポリシーの以下のルールとアクションに一致するトラフィックを含めることができます。

- トンネル ルール：[ファストパス（FastPath）] アクション（外部セッションをロギングします）
- プレフィルタ ルール：[ファストパス（FastPath）] アクション

FastPath されたトラフィックはアクセス コントロールと QoS の残りをバイパスするため、FastPath された接続の接続イベントに含まれる情報は限られます。8000 シリーズ FastPath ルールで FastPath された接続をロギングすることはできません。

モニタされた監視接続のロギング

システムは常に、以下の設定と一致するトラフィックの接続終了をロギングします。このことは、トラフィックに一致する他のルールがなく、デフォルトアクションのロギングを有効にしていない場合でも該当します。

- セキュリティインテリジェンス：モニタするように設定されたブラックリスト（セキュリティ インテリジェンス イベントも生成されます）
- SSL ルール：[モニタ（Monitor）] アクション
- アクセス コントロール ルール：[モニタ（Monitor）] アクション

システムは、1 つの接続が 1 つのモニタ ルールに一致するたびに 1 つの別個のイベントを生成するわけではありません。1 つの接続が複数のモニタ ルールに一致する可能性があるため、各接続イベントには、接続が一致する最初の 8 つのモニタ アクセス コントロール ルールに関する情報だけでなく、最初の一致する SSL モニタ ルールに関する情報を含めて表示することができます。

同様に、外部 syslog または SNMP トラップ サーバに接続イベントを送る場合、システムは 1 つの接続が 1 つのモニタ ルールに一致するたびに 1 つの別個のアラートを送信するわけではありません。代わりに、接続の終了時にシステムから送られるアラートに、接続が一致したモニタ ルールの情報が含まれます。

信頼されている接続のロギング

信頼されている接続の開始と終了をロギングできます。ロギングには、以下のルールとアクションに一致するトラフィックを含めることができます。

- アクセス コントロール ルール：[信頼する（Trust）] アクション
- アクセス コントロールのデフォルトアクション：[すべてのトラフィックを信頼する（Trust All Traffic）]

（注） 信頼できる接続を記録することはできますが、これはお勧めしません。信頼できる接続はディープインスペクションまたは検出の対象ではないため、信頼できる接続の接続イベントに含まれる情報は限定的であるためです。

システムは、接続を検出したデバイスに応じて異なる方法で、信頼アクセス コントロール ルールによって処理された TCP 接続をロギングします。

- 7000 および 8000 シリーズ デバイスでは、信頼ルールによって最初のパケットで検出された TCP 接続は、すでに有効になっているモニタ ルールの有無に応じて異なるイベントを生成します。モニタ ルールがアクティブな場合、システムはパケットを評価し、接続開始

および接続終了イベントを生成します。アクティブなモニタ ルールがない場合、システムは接続終了イベントだけを生成します。

- 他のすべてのモデルでは、信頼ルールによって最初のパケットで検出されたTCP接続は、接続終了イベントだけを生成します。システムは、最後のセッション パケットの1時間後にイベントを生成します。

ブロックされた接続のロギング

ブロックされた接続をロギングできます。ロギングには、以下のルールとアクションに一致するトラフィックを含めることができます。

- トンネル ルール：[ブロック（Block）]
- プレフィルタ ルール：[ブロック（Block）]
- プレフィルタのデフォルトアクション：[すべてのトンネルトラフィックをブロック（Block all tunnel traffic）]
- セキュリティインテリジェンス：ブロックするブラックリストが設定されます（セキュリティ インテリジェンス イベントも生成されます）
- SSL ルール：[ブロック（Block）] および [リセットしてブロック（Block with reset）]
- SSL のデフォルト アクション：[ブロック（Block）]および[リセットしてブロック（Block with reset）]
- アクセス コントロール ルール：[ブロック（Block）]、[リセットしてブロック（Block with reset）]、[インタラクティブ ブロック（Interactive Block）]
- アクセスコントロールのデフォルトアクション：[すべてのトラフィックをブロック（Block All Traffic）]

トラフィックをブロックできるデバイスは、インライン（つまり、ルーテッドインターフェイス、スイッチド インターフェイス、トランスペアレント インターフェイス、インライン インターフェイスのペア）で展開されているもののみです。ブロックされた接続はパッシブ展開で実際にはブロックされないため、システムにより、ブロックされた各接続に対し複数の接続開始イベントが報告される場合があります。

⚠

注意 サービス妨害（DoS）攻撃の間にブロックされた TCP 接続をロギングすると、システム パフォーマンスに影響し、複数の同様のイベントによってデータベースが過負荷になる可能性があります。ブロック ルールにロギングを有効にする前に、そのルールがインターネット側のインターフェイスまたは DoS 攻撃を受けやすい他のインターフェイス上のトラフィックをモニタするかどうかを検討します。

ブロックされた接続の接続開始ロギングと接続終了ロギングとの比較

ブロックされた接続をロギングするときは、システムがその接続をどのようにロギングするかは接続がブロックされた理由によって異なります。これは、接続ログに基づいて相関ルールを設定する際に留意しておくことが重要です。

- 暗号化されたトラフィックをブロックする SSL ルールおよび SSL ポリシーのデフォルトアクションの場合、システムは接続**終了**イベントをロギングします。これは、システムが接続がセッション内で最初のパケットを使用して暗号化されているかどうかを決定できないためです。
- 他のブロッキング アクションについては、システムは接続**開始**イベントをロギングします。一致するトラフィックは、追加のインスペクションなしで拒否されます。

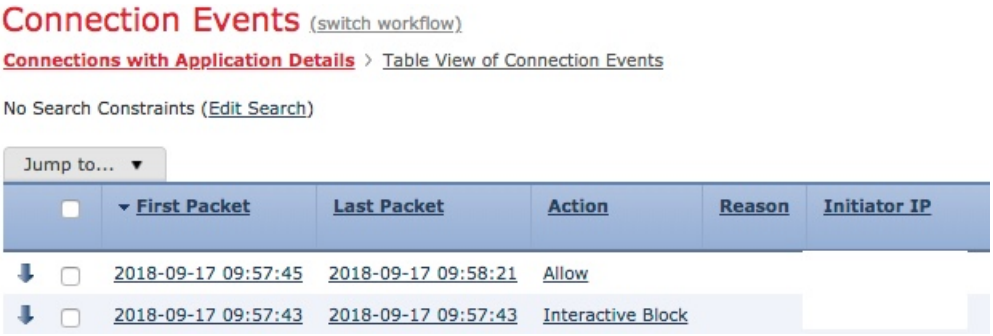
バイパスされるインタラクティブ ブロックのロギング

インタラクティブ ブロッキング アクセス コントロール ルール（このルールではユーザが禁止されている Web サイトを参照するとシステムによって警告ページが表示されます）を使用すると、接続終了ロギングを設定できます。その理由は、警告ページをユーザがクリック スルーすると、その接続は新規の、許可された接続と見なされ、システムによってモニタとロギングができるためです。

したがって、[インタラクティブ ブロック（Interactive Block）] ルールまたは [リセットしてインタラクティブ ブロック（Interactive Block with reset）] ルールにパケットが一致する場合、システムは以下の接続イベントを生成できます。

- ユーザの要求が最初にブロックされ警告ページが表示されたときの接続開始イベント。このイベントにはアクション [インタラクティブ ブロック（Interactive Block）] または [リセットしてインタラクティブ ブロック（Interactive Block with Reset）] が関連付けられます。
- 複数の接続開始または終了イベント（ユーザが警告ページをクリック スルーし、要求した最初のページをロードした場合）。これらのイベントには [許可（Allow）] アクションおよび理由 [ユーザ バイパス（User Bypass）] が関連付けられます。

  次の図に、許可を受けたインタラクティブ ブロックの例を示します。



許可された接続のロギング

許可された接続をロギングができます。ロギングには、以下のルールとアクションに一致するトラフィックを含めることができます。

- SSL ルール：[複合（Decrypt）] アクション
- SSL ルール：[複合しない（Do not decrypt）] アクション
- SSL のデフォルト アクション：[複合しない（Do not decrypt）] アクション
- アクセス コントロール ルール：[許可（Allow）] アクション
- アクセス コントロールのデフォルト アクション：[ネットワーク検出のみ（Network Discovery Only）] および任意の侵入防御オプション

これらの設定に対するロギングを有効にすると、接続が確実にロギングされると同時に、インスペクションおよびトラフィック処理の次のフェーズが許可（または指定）されます。SSL ロギングは常に接続終了ロギングですが、アクセス コントロール設定で接続開始ロギングも可能にすることができます。

トンネルおよびプレフィルタ ルールでの [分析（Analyze）] アクションを使用してアクセス コントロールで接続を続行することもできますが、このアクションを使用するルールではロギングが無効にされます。ただし、他の設定を使用して、一致する接続をロギングすることもできます。許可されたトンネルのカプセル化されたセッションは、個別に評価されてロギングされます。

アクセス コントロール ルールまたはデフォルト アクションでトラフィックを許可する場合、関連する侵入ポリシーを使用してトラフィックをさらに検査し、侵入をブロックすることができます。アクセス コントロール ルールでは、ファイル ポリシーを使用して、マルウェアを含む禁止されたファイルを検出し、ブロックすることもできます。接続イベント ストレージを無効にしない限り、システムは、侵入イベント、ファイル イベント、マルウェア イベントに関連する許可された接続のほとんどを自動的にロギングします。詳細については、常にログに記録される接続 （3002 ページ）を参照してください。

ペイロードが暗号化される接続には、ディープ インスペクションは適用されません。したがって、暗号化接続の接続イベントに含まれる情報は限定されます。

許可された接続のファイルおよびマルウェア イベントのロギング

ファイル ポリシーによってファイルが検出またはブロックされると、以下のいずれかのイベントが Firepower Management Center データベースにロギングされます。

- ファイル イベント：検出またはブロックされたファイル（マルウェア ファイルを含む）を表します。
- マルウェア イベント：検出されたまたはブロックされたマルウェア ファイルのみを表します。
- レトロスペクティブ マルウェア イベント：以前に検出されたファイルでのマルウェア処理が変化した場合に生成されます。

このロギングは、アクセス コントロール ルールごとに無効にすることができます。ファイル イベントおよびマルウェア イベント ストレージを完全に無効にすることもできます。

（注） ファイル イベントおよびマルウェア イベントのロギングは有効のままにすることを推奨しています。

接続開始のロギングと終了のロギングの比較

接続は、次の例外となるブロックされたトラフィックを除き、接続開始時あるいは終了時にログを記録することができます。

- ブロックされたトラフィック：ブロックされたトラフィックは、さらに検査されることなくすぐさま拒否されるため、通常、ブロックされたトラフィックやブラックリストに登録されたトラフィックについては、接続開始イベントのみ記録可能です。ログに記録される個々の接続終了はありません。
- ブロックされた暗号化トラフィック：SSL ポリシーで接続のロギングを有効にすると、システムは接続開始イベントではなく接続終了イベントをログに記録します。これは、システムは接続がセッション内で最初のパケットを使用して暗号化されているかどうかを判定できず、暗号化されたセッションを即座にブロックできないためです。

パフォーマンスを最適化するためには、接続の開始と終了の両方ではなく、どちらか一方をロギングします。何らかの理由で接続をモニタリングすると、接続終了ロギングが強制されます。単一のブロックされていない接続の場合、接続終了イベントには、接続開始イベントに含まれるすべての情報に加えて、セッション期間中に収集された情報も含まれます。

次の表では、接続開始イベントと接続終了イベントの違い（それぞれをロギングする利点を含む）を詳細に説明します。

表 *332 :* 接続開始イベントと接続終了イベントの比較

	接続開始イベント	接続終了イベント
次の場合に生成可能です	システムが接続の開始を検出した場合（または、イベントの生成がアプリケーションまたは URL の識別に依存する場合は最初の数パケットの後）	システムが以下の状態の場合 • 接続のクローズを検出した場合 • 一定期間後に接続の終了を検出しない場合 • メモリ制約によりセッションを追跡できなくなった場合

	接続開始イベント	接続終了イベント
次のものについてロギングが可能です	SSL ポリシーによってブロックされた接続を除くすべての接続	ほとんどの接続
次を含みます	最初のパケット（または、イベントの生成がアプリケーションまたはURL の識別に依存する場合は最初の数パケット）で判定できる情報のみ	接続開始イベント内のすべての情報と、セッション期間を通してトラフィックを検査して判別された情報（たとえば伝送されたデータ総量、接続の最後のパケットのタイムスタンプなど）
次の場合に有用です	ログに記録する場合： • ブロックされた接続。 • 接続終了情報はユーザにとって重要ではないので、接続の開始のみ	目的 • SSL ポリシーによって処理される暗号化接続をロギングする場合 • セッションの期間にわたって収集された情報であらゆる種類の詳細な分析を実行する場合、またはその情報を使用して相関ルールをトリガーする場合 • カスタム ワークフローで接続の概要（集約接続データ）を表示する場合、グラフ形式で接続データを表示する場合、またはトラフィック プロファイルを作成して使用する場合

Firepower Management Center と外部ロギング

接続およびセキュリティ インテリジェンス イベント ログを Firepower Management Center に保存する場合、Firepower システムのレポート、分析、およびデータ相関機能を使用することができます。次に例を示します。

- ダッシュボードおよびコンテキストエクスプローラでは、システムによってロギングされた接続をグラフ形式によって一目で確認できます。

- イベント ビュー（ほとんどのオプションは分析メニューで利用可能）には、システムが記録した接続に関する詳細情報が表示されます。これらの情報はグラフまたは表形式で表示したり、レポートにまとめたりすることもできます。
- トラフィック プロファイリングは、接続データを使用して正常なネットワーク トラフィックのプロファイルを作成します。ユーザはそのプロファイルを基準として使用して、異常な動作を検出および追跡できます。
- 相関ポリシーを使用して、イベントを生成し、特定のタイプの接続またはトラフィック プロファイルの変更に対する応答（アラートや外部修復など）をトリガーできます。

Firepower Management Center に保存できるイベントの数はモデルによって異なります。

（注） これらの機能を使用するには、接続（ほとんどの場合、接続の開始ではなく接続の終了）をロギングする**必要があります**。システムがクリティカルな接続（ログに記録された侵入、禁止されたファイルおよびマルウェアに関連付けられているもの）を自動的にロギングするのはこのためです。

アラート応答と呼ばれる接続を設定し、それを使って外部 syslog や SNMP トラップ サーバにイベントをロギングすることもできます。

関連トピック

Firepower Management Center アラート応答 （2807 ページ）

接続ロギングの制限事項

以下はロギングできません。

- 8000 シリーズのファースト パス ルールでファースト パスされた接続
- カプセル化された接続がアクセス制御によって検査されるプレーンテキスト、パススルートンネルの外部セッション
- 3 ウェイ ハンドシェイクが完了していない場合は TCP 接続。

  Firepower の展開環境に対するサービス拒否攻撃の機会を提供することになるため、これらの接続はログに記録されません。

  ただし、次の回避策を使用して失敗した接続をモニタまたはデバッグできます。

  - コマンドライン インターフェイスで **show asp drops** コマンドを使用します。
  - パケット キャプチャ機能を使用してこれらの接続に関する詳細情報を取得します。パケット キャプチャの概要 （426 ページ）およびサブトピックを参照してください。

接続イベントに必要と思われる情報が含まれていない場合は、接続イベント フィールドの入力の要件（3042 ページ）と接続イベント フィールドで利用可能な情報（3044 ページ）を参照してください。

イベント ビューアにイベントが表示された場合

次のポイントは、すべてのタイプのイベントに該当します。

- [分析（Analysis）] メニューにあるページを見ている場合は、新しいイベントを表示するにはページを更新する必要があります。
- 通常、イベントは、トラフィックが検出されてから数秒以内に表示されます。ただし、トラフィックが非常に多い状態、FMC が低帯域幅のネットワーク上で多数のデバイスを管理している状況、またはイベントのバックアップなどのイベント処理が一時停止される操作が進行中である状況などでは、任意の遅延が生じることがあります。

接続のロギングのベスト プラクティス

次のベスト プラクティスを使用して、記録が必要な接続のみを記録するようにします。

重要な接続のみが記録されるように、アクセス制御ルールごとの接続ロギングを有効にします。

常に記録する接続

システムは次について自動的に記録します。

- 検出されたファイル、マルウェア、侵入、およびインテリジェント アプリケーション バイパス（IAB）に関連付けられている一部の接続。

  詳細については、常にログに記録される接続（3002 ページ）を参照してください。

- モニタ対象の接続。

  詳細については、モニタされた監視接続のロギング（3005 ページ）を参照してください。

記録されることがない接続

次についてはロギングを有効にしないでください。

- 信頼アクションがあるアクセス制御ルール

  信頼されている接続には、ディープ インスペクションまたはディスカバリは適用されません。したがって、信頼されている接続の接続イベントに含まれる情報は限られます。

- パッシブ展開のブロック ルールについてはロギングを有効にしないでください。デバイスがインラインで展開された場合にシステムがブロックする接続を記録するには、ブロック ルールではなく、モニタ ルールを使用します。

トラフィックをブロックできるデバイスは、インライン（つまり、ルーテッド インターフェイス、スイッチド インターフェイス、トランスペアレント インターフェイス、インラインインターフェイスのペア）で展開されているもののみです。ブロックされた接続はパッシブ展開で実際にはブロックされないため、システムにより、ブロックされた各接続に対し複数の接続開始イベントが報告される場合があります。

- 対象外のトラフィック。次に例を示します。
  - 信頼されている DNS ホストへの DNS 要求などの特定の許可トラフィック。
  - サービス提供に関係のないインフラストラクチャ トラフィック。

（前述のように、この場合もこのトラフィックの脅威はモニタできます。）

常にログに記録される接続（3002ページ）で説明したように、前述のロギングを無効にした場合も、侵入イベント、マルウェア、および IAB は記録されます。

どこかで記録されているものの記録の回避

別のデバイスまたはサービスがネットワーク セグメントの接続データを記録している場合は、Firepower Management Center 内のそのセグメントのデータのロギングを無効にします。次に例を示します。

- Firepower Management Center と同じネットワーク セグメント上の接続イベントをルータが記録している場合、相関ポリシーやトラフィック プロファイルなど何らかの目的で接続イベントが必要な場合を除き、Firepower Management Center 上での同じ接続を記録することは避けてください。

  相関ポリシーの詳細については、相関ポリシーとルールの概要（2697ページ）を参照してください。トラフィック プロファイルの詳細については、トラフィック プロファイルの概要（2741 ページ）を参照してください。

- Stealthwatch を使用してスイッチやルータから報告された NetFlow レコードを利用して潜在的な動作の異常や疑わしいトラフィック パターンを特定している場合、それらのセグメントをモニタしているルールの接続ロギングを無効することができます。その代りに、ネットワークのそれらの部分については Stealthwatch の動作分析に依存します。

  詳細については、Stealthwatch のドキュメントを参照してください。

接続の開始または終了のいずれか（両方ではない）のロギング

接続の開始と終了のロギングを選択できる場合は、接続終了時のロギングを有効にします。これは、接続終了時は接続開始イベントからの情報と、セッション中に収集された情報が記録されるからです。

ブロックされた接続を記録するか、または接続終了の情報に関心がない場合にのみ、接続の開始を記録します。

詳細については、接続開始のロギングと終了のロギングの比較（3009ページ）を参照してください。

ブロックされたトラフィックのロギング

ブロックされたトラフィックは、それ以上調査されることなくすぐに拒否されるため、通常は接続開始イベントのみを記録できます。

詳細については、ブロックされた接続のロギング （3006 ページ）を参照してください。

外部の場所へのイベントのロギング

会社のセキュリティ ポリシーで許可されている場合は、次のいずれかを使用して外部ソースにログをストリーミングすることで Firepower Management Center のディスク容量を節約できます。

- eStreamer は、Firepower Management Center あるいは 7000 または 8000 シリーズ デバイスからカスタム展開したクライアント アプリケーションへのログのストリーミングを可能にします。詳細については、『*Firepower eStreamer Integration Guide*』を参照してください。
- アラート応答と呼ばれている syslog または SNMP トラップ。詳細については、Firepower Management Center アラート応答 （2807 ページ）を参照してください。

イベント レコードの最大数を指定します。

データベースに保存できるレコードの最小数と最大数を考慮します。たとえば、デフォルトでは、仮想 Firepower Management Center は 1,000 万のイベントを保存できますが、イベントの最大数は 5,000 万です。**[システム（System）] > [設定（Configuration）] > [データベース（Database）]** に移動してニーズに合ったサイズに調整します。

Firepower Management Center のすべてのモデルとそれらのイベント データベースのサイズのリストについては、データベース イベント数の制限 （1264 ページ）を参照してください。

接続イベントに表示される内容を制御します。

接続イベントに表示される行数を指定するには、Firepower Management Center の右上にある自分のユーザ名をクリックし、**[ユーザ設定（User Preferences）] > [イベント表示設定（Event View Settings）]** をクリックします。設定可能なイベント数は 1 ページあたり最大で 1,000 です。

接続イベント レポートのセットアップ

接続イベントを見逃していないことを確認するには、.csv 形式の自動レポートをセットアップし、必要に応じて定期的に実行されるようにスケジュールを設定することができます。詳細については、次のトピックを参照してください。

- レポート デザイナを使用します（**[分析（Analysis）] > [接続（Connection）] > [イベント（Events）] > [レポート デザイナ（Report Designer）]**）。レポートの設計について （2775 ページ）
- タスクのスケジュールを設定します（**[システム（System）] > [ツール（Tools）] > [スケジュール（Scheduling）]**）。タスクのスケジューリングについて （237 ページ）

接続ロギングの設定

以降の項では、さまざまなルールと条件に一致する接続ロギングのセットアップ方法について説明します。

トンネル ルールおよびプレフィルタ ルールによる接続のロギング

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	Firepower Threat Defense	いずれか（Any）	Admin/Access Admin/Network Admin

始める前に

- ルール アクションを [ブロック（Block）] または [ファストパス（Fastpath）] に設定します。[分析（Analyze）] アクションのロギングは無効にします。これにより、接続のアクセス制御が引き続き可能になり、接続の処理とロギングは別の設定で決定されます。

ステップ 1 プレフィルタ ポリシー エディタで、ロギングを設定するルールの横にある編集アイコン（  ）をクリックします。

代わりに表示アイコン（  ）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 2 [ロギング（Logging）] タブをクリックします。

ステップ 3 [接続の開始時にロギングする（Log at Beginning of Connection）] または [接続の終了時にロギングする（Log at End of Connection）] を指定します。

パフォーマンスを最適化するためには、接続の開始と終了の両方ではなく、どちらか一方をロギングします。ブロックされたトラフィックは、それ以上の検査なしで即座に拒否されるため、[ブロック（Block）] ルールの場合は接続終了時のイベントはロギングできません。

ステップ 4 接続イベントの送信先を指定します。

ステップ 5 [保存（Save）] をクリックしてルールを保存します。

ステップ 6 [保存（Save）] をクリックしてポリシーを保存します。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

SSL ルールによる復号可能接続のロギング

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	すべて（NGIPSv を除く）	いずれか（Any）	Admin/Access Admin/Network Admin

ステップ 1 SSL ポリシーエディタで、ロギングを設定するルールの横にある編集アイコン（  ）をクリックします。

代わりに表示アイコン（  ）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 2 [ロギング（Logging）] タブをクリックします。

ステップ 3 [接続の終了時にロギングする（Log at End of Connection）] をオンにします。

モニタ対象トラフィックに対して、接続の終了時のロギングが必要になります。

ステップ 4 接続イベントの送信先を指定します。

接続イベントについて Firepower Management Center ベースの分析を実行する場合は、イベントをイベントビューアに送信します。モニタ対象トラフィックに対して、これが必要になります。

ステップ 5 [保存（Save）] をクリックしてルールを保存します。

ステップ 6 [保存（Save）] をクリックしてポリシーを保存します。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

セキュリティ インテリジェンスによる接続のロギング

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Access Admin/Network Admin

ステップ 1 アクセス コントロール ポリシー エディタで、[セキュリティ インテリジェンス（Security Intelligence）] タブをクリックします。

ステップ 2 ロギング アイコン（  ）をクリックして、次の条件を使用するセキュリティ インテリジェンス ロギングを有効にします。

- IP アドレス別：[ネットワーク（Networks）] の横にあるロギング アイコンをクリックします。
- URL 別：[URL（URLs）] の横にあるロギング アイコンをクリックします。
- ドメイン名別：[DNS ポリシー（DNS Policy）] ドロップダウンリストの横にあるロギング アイコンをクリックします。

コントロールが淡色表示されている場合、設定は先祖ポリシーから継承され、設定を変更する権限がありません。 設定がロック解除されている場合は、[Inherit from base policy] をオフにして、編集を有効にします。

ステップ 3 [接続のロギング（Log Connections）] チェックボックスをオンにします。

ステップ 4 接続イベントとセキュリティ インテリジェンス イベントの送信先を指定します。

Firepower Management Center ベースの分析を実行する場合や、ブラックリストに登録されたオブジェクトをモニタ専用に設定する場合は、イベントをイベント ビューアに送信します。

ステップ 5 [OK] をクリックしてロギング オプションを設定します。

ステップ 6 [保存（Save）] をクリックして、ポリシーを保存します。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

アクセス制御ルールによる接続のロギング

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Access Admin/Network Admin

ルール アクションと詳細検査のオプションの選択によって、ロギング オプションは異なります。ルールとポリシーのアクションによるロギングへの影響（3004 ページ）を参照してください。

ステップ 1 アクセス コントロール ポリシー エディタで、ロギングを設定するルールの横にある編集アイコン（）をクリックします。

代わりに表示アイコン（  ）が表示される場合、設定は先祖ポリシーから継承され、先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 2 [ロギング（Logging）] タブをクリックします。

ステップ 3 [接続の開始時にロギングする（Log at Beginning of Connection）] または [接続の終了時にロギングする（Log at End of Connection）] を指定します。

パフォーマンスを最適化するためには、接続の開始と終了の両方ではなく、どちらか一方をロギングします。

ステップ 4 （オプション）[ファイルのロギング（Log Files）] チェックボックスをオンにして、接続に関連付けられているファイル イベントとマルウェア イベントをロギングします。

シスコは、このオプションを有効のままにすることを推奨します。

ステップ 5 接続イベントの送信先を指定します。

- [イベント ビューア（Event Viewer）]：接続イベント上での Firepower Management Center ベースの分析を実行する場合、またはルール アクションが [モニタ（Monitor）] の場合は、接続イベントを Firepower Management Center の Web インターフェイスに送信します。
- [Syslog サーバ（Syslog Server）]：オーバーライドする場合を除き、アクセス コントロール ポリシーに設定されている syslog サーバに接続イベントを送信します。

  [オーバーライドの表示（Show Overrides）]：アクセス コントロール ポリシーで設定されている設定をオーバーライドするためのオプションが表示されます。

  - [重大度をオーバーライドする（Override Severity）]：このオプションを選択し、ルールの重大度を選択した場合は、このルールの接続イベントはアクセス コントロール ポリシーの [ロギング（Logging）] タブに設定されている重大度に関わらず、選択した重大度が設定されます。
  - [デフォルトの Syslog の宛先をオーバーライドする（Override Default Syslog Destination）]：このルールの接続イベントに生成された syslog をこのアラートに指定されている宛先に送信します。
- [SNMP トラップ（SNMP Trap）]：接続イベントは、選択した SNMP トラップに送信されます。

ステップ 6 [保存（Save）] をクリックしてルールを保存します。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

ポリシーのデフォルト アクションによる接続のロギング

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Access Admin/Network Admin

ポリシーのデフォルトアクションにより、システムがポリシー内のルールのいずれにも一致しないトラフィックを処理する方法が決定されます（ただし、トラフィックの照合およびロギングを実行し、トラフィックの処理や調査は実行しないアクセス コントロール ポリシーと SSL ポリシー内のモニタ ルールを除きます）。

また、システムが複合化できないセッションをロギングする方法は、SSL ポリシーのデフォルト アクションのロギング設定でも制御されます。

始める前に

- プレフィルタのデフォルトアクション ロギングについては、デフォルトアクションを [すべてのトンネル トラフィックをブロック（Block all tunnel traffic）] に設定します。[すべてのトンネル トラフィックを許可（Allow all tunnel traffic）] アクションのロギングは無効になります。これにより、接続のアクセス制御が引き続き可能になり、接続の処理とロギングは別の設定で決定されます。

ステップ 1 ポリシー エディタで、[デフォルト アクション（Default Action）] ドロップダウンリストの横にあるロギング アイコン（  ）をクリックします。

ステップ 2 一致する接続をロギングするタイミングを指定します。

- 接続の開始時にロギングする：SSL のデフォルト アクションではサポートされていません。
- 接続の終了時にロギングする：アクセス制御の [すべてのトラフィックをブロック（Block All Traffic）] デフォルト アクションまたはプレフィルタの [すべてのトンネル トラフィックをブロック（Block all tunnel traffic）] デフォルト アクションを選択するとサポートされなくなります。

パフォーマンスを最適化するためには、接続の開始と終了の両方ではなく、どちらか一方をロギングします。

コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。アクセス コントロール ポリシーでは、設定が先祖ポリシーから継承されることもあります。

ステップ 3 接続イベントの送信先を指定します。

接続イベントについて Firepower Management Center ベースの分析を実行する場合は、イベントをイベント ビューアに送信します。

ステップ 4 [OK] をクリックします。

ステップ 5 [保存（Save）] をクリックしてポリシーを保存します。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

長い URL のロギングの制限

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Access Admin/Network Admin

HTTP トラフィックの接続の終了イベントは、監視対象ホストによって要求された URL を記録します。URL の保管を無効にすることや保管する URL 文字数を制限することで、システム パフォーマンスが向上する可能性があります。URL のロギングを無効化しても（保管する文字数を 0 にしても）、URL フィルタリングには影響しません。システムは、要求された URL に基づいてトラフィックをフィルタリングします。それらの URL を記録しない場合も同じです。

ステップ 1 アクセス コントロール ポリシー エディタで、[詳細（Advanced）] タブをクリックして、[一般設定（General Settings）] の横にある編集アイコン（  ）をクリックします。

代わりに表示アイコン（  ）が表示される場合、設定は先祖ポリシーから継承され、先祖ドメインに属しており、設定を変更する権限がありません。設定がロック解除されている場合は、[Inherit from base policy] をオフにして、編集を有効にします。

ステップ 2 [接続イベントで保存する URL の最大文字数（Maximum URL characters to store in connection events）] を入力します。

ステップ 3 [OK] をクリックします。

ステップ 4 [保存（Save）] をクリックしてポリシーを保存します。

次のタスク

- 設定変更を展開します。設定変更の展開 （447 ページ）を参照してください。

第 125 章

接続イベントとセキュリティ インテリジェンス イベント

次のトピックでは、接続およびセキュリティ イベント テーブルを使用する方法について説明します。

接続イベントについて

システムは、管理対象デバイスが検出した接続のログを生成することができます。このログは接続イベントと呼ばれます。接続イベントには、セキュリティインテリジェンスイベント（レピュテーションベースのセキュリティ インテリジェンス機能によってブラックリストに登録（ブロック）された接続）が含まれます。

接続イベントには、一般に、次によって検出されたトランザクションが含まれます。

- アクセス コントロール ポリシー
- SSL ポリシー
- （プレフィルタまたはトンネルルールによってキャプチャされた）プレフィルタ ポリシー
- DNS ブラックリスト
- URL ブラック リスト
- ネットワーク（IP アドレス）ブラックリスト

ルールやポリシーの設定を行うことで、ログに記録する接続の種類、接続をログに記録するタイミング、およびデータを保存する場所をきめ細かく制御できます。

詳細については、接続ロギング （3001 ページ）を参照してください。

関連トピック

セキュリティ インテリジェンスについて （1741 ページ）

接続イベントとセキュリティ インテリジェンス イベントの比較

セキュリティ インテリジェンス イベントは、レピュテーションベースのセキュリティ インテリジェンス機能によりセッションがブラックリストに登録された（ブロックされた）ときに生成される接続イベントです。

ただし、すべてのセキュリティインテリジェンスイベントに同一の接続イベントがあります。セキュリティ インテリジェンス イベントは個別に表示して分析できます。また、システムはセキュリティ インテリジェンス イベントを個別に保存およびプルーニングします。

システムは、より多くのリソースを消費する評価を行う前に、セキュリティインテリジェンスを実施することに注意してください。接続がセキュリティインテリジェンスによってブロックされた場合、結果として生成されるイベントには、その後の評価によってシステムで収集されることになっていた情報（ユーザ ID など）が含まれません。

（注） 本書では違うと明記されていない限り、接続イベントに関する情報は、セキュリティインテリジェンス イベントに関する情報でもあります。

NetFlow 接続

管理対象デバイスで収集された接続データを補うために、NetFlowエクスポータによってブロードキャストされたレコードを使用して接続イベントを生成できます。この方法が特に役立つのは、NetFlow エクスポータが、管理対象デバイスでモニタしているネットワークとは別のネットワークをモニタしている場合です。

システムは NetFlow レコードを単方向の接続終了イベントとして Firepower Management Center データベースに記録します。これらの接続に関して使用可能な情報は、アクセス コントロール ポリシーで検出された接続の情報とは若干異なります。NetFlow データと管理対象デバイス データの違い （2478 ページ）を参照してください。

関連トピック

Firepower システムの NetFlow データ （2477 ページ）

接続の概要（グラフ用集約データ）

Firepower システムは 5 分間隔で収集された接続データを集約し、接続の概要を作成します。この概要を使用して、接続グラフとトラフィック プロファイルがシステムで生成されます。必要に応じて、接続の概要データに基づいてカスタム ワークフローを作成できます。これは、個々の接続イベントに基づいたワークフローと同じように使用できます。

セキュリティインテリジェンスイベント専用の接続サマリーはないことに注意してください。ただし、対応する接続終了イベントは接続サマリーのデータに集約できます。

集約するには、複数の接続が次のとおりでなければなりません。

- 接続終了を表している
- 送信元と宛先の IP アドレスが同じで、応答側（宛先）のホストで同じポートを使用している
- 同じプロトコルを使用している（TCP または UDP）
- 同じアプリケーション プロトコルを使用している
- 同じ Firepower システム管理対象デバイスまたは同じ NetFlow エクスポータによって検出される

各接続の概要には、接続数など全トラフィック統計情報が含まれています。NetFlowエクスポータは単一方向接続を生成するので、接続の概要では、NetFlow データに基づく接続ごとに接続数が 2 ずつ増えます。

接続の概要には、概要内の集約された接続に関するすべての情報が含まれているわけではありませんので注意してください。たとえば、接続の概要に集約される接続にはクライアント情報が使用されないため、概要にクライアント情報は含まれません。

長時間接続

接続データを集約する 5 分間隔の 2 回以上に監視対象のセッションがまたがる場合、その接続は長時間接続と見なされます。接続サマリーで接続数を計算する際には、長時間接続が開始された 5 分間隔の回のみカウントします。

また、長時間接続において発信側と応答側が送信したパケット数とバイト数を計算する際は、システムは5分間隔の各回で実際に送信されたパケット数とバイト数を報告しません。代わりにシステムは、送信された合計パケット数と合計バイト数、接続の長さ、5 分間隔の各回で接続のどの部分が行われたかに基づいて、一定の送信速度を仮定し、値を推定します。

外部応答側からの統合接続サマリ

接続データの保存に必要なスペースを減らし、接続グラフのレンダリングを高速化するために、システムは次の場合に接続サマリを統合します。

- 接続に関連するホストの 1 つが監視対象のネットワーク上にない場合
- 外部ホストの IP アドレス以外で、サマリ内の接続がサマリ集約条件を満たす場合

[分析（Analysis）] > [接続（Connections）] サブメニュー ページで接続サマリーを表示する場合や、接続グラフを使用する場合、システムは非モニタ対象ホストの IP アドレスの代わりに `external` と表示します。

この集約の結果として、外部応答側を含む接続サマリーまたはグラフから接続データのテーブル ビューにドリルダウンしようとすると（つまり、個別の接続データへのアクセス）、テーブル ビューには情報が何も表示されません。

接続イベントとセキュリティインテリジェンスイベントのフィールド

（注） 接続に関連付けられたイベントの検索に、接続やセキュリティインテリジェンスのイベントの検索ページは使用できません。

Access Control Policy (Syslog: ACPolicy)

接続をモニタしたアクセス コントロール ポリシー。

アクセス制御ルール (Syslog: AccessControlRuleName)

接続を処理したアクセス コントロール ルールまたはデフォルト アクションと、その接続に一致した最大 8 つのモニタ ルール。

接続が 1 つのモニタ ルールに一致した場合、Firepower Management Center は接続を処理したルールの名前を表示し、その後にモニタ ルール名を表示します。接続が複数のモニタ ルールに一致した場合、一致するモニタ ルールの数が表示されます（`Default Action + 2 Monitor Rules` など）。

接続に一致した最初の 8 つのモニタ ルールのリストをポップアップ ウィンドウに表示するには、[N モニタ ルール（*N*Monitor Rules）] をクリックします。

Action (Syslog: AccessControlRuleAction)

接続をロギングした設定に関連付けられているアクション。

セキュリティ インテリジェンスによってモニタされている接続の場合、そのアクションは、接続によってトリガーされる最初のモニタ以外のアクセス コントロール ルールのアクションであるか、またはデフォルト アクションです。同様に、モニタ ルールに一致するトラフィックは常に後続のルールまたはデフォルト アクションによって処理されるため、モニタ ルールによってロギングされた接続と関連付けられたアクションが [モニタ（Monitor）] になることはありません。ただし、モニタ ルールに一致する接続の相関ポリシー違反をトリガーする可能性があります。

アクション	説明
許可（Allow）	アクセス コントロールによって明示的に許可された、またはユーザがインタラクティブ ブロックをバイパスしたために許可された接続。

アクション	説明
ブロック（Block）、リセットしてブロック（Block with reset）	次を含むブロックされた接続： • プレフィルタ ポリシーによってブロックされたトンネルおよびその他の接続 • セキュリティ インテリジェンスによってブラックリストに載せられた接続 • SSL ポリシーによってブロックされた暗号化接続 • 侵入ポリシーによってエクスプロイトがブロックされた接続 • ファイル ポリシーによってファイル（マルウェアを含む）がブロックされた接続。 システムが侵入またはファイルをブロックする接続では、アクセス コントロールの許可ルールを使用してディープ インスペクションを呼び出す場合にも、システムはブロックを表示します。
高速パス（Fastpath）	プレフィルタ ポリシーによって高速パスが適用された暗号化されていないトンネルおよびその他の接続。
インタラクティブ ブロック（Interactive Block）、リセット付きインタラクティブ ブロック（Interactive Block with reset）	システムがインタラクティブ ブロック ルールを使用してユーザの HTTP 要求を最初にブロックしたときにログに記録された接続。システムにより表示される警告ページでユーザがクリックスルーすると、そのセッションでログに記録されるその後の接続に許可アクションが付きます。
信頼（Trust）	アクセス コントロールによって信頼された接続。The system logs trusted TCP connections differently depending on the device model.
デフォルト アクション（Default Action）	アクセス コントロール ポリシーのデフォルト アクションによって処理される接続。

アプリケーション プロトコル (Syslog: ApplicationProtocol)

In the Firepower Management Center web interface, this value constrains summaries and graphs.

接続で検出された、ホスト間の通信を表すアプリケーション プロトコル。

アプリケーション プロトコル カテゴリとタグ（Application Protocol Category and Tag）

アプリケーションの機能を理解するのに役立つ、アプリケーションの特性を示す基準。

[アプリケーションのリスク（Application Risk）]

接続で検出されたアプリケーション トラフィックに関連するリスク：Very High、High、Medium、Low、または Very Low。接続で検出されたアプリケーションのタイプごとに、関連するリスクがあります。このフィールドでは、それらのうち最も高いものが表示されます。

ビジネスとの関連性（Business Relevance）

接続で検出されたアプリケーション トラフィックに関連するビジネス関連性：Very High、High、Medium、Low、または Very Low。接続で検出されたアプリケーションのタイプごとに、関連するビジネスとの関連性があります。このフィールドでは、それらのうち最も低いもの（関連が最も低い）が表示されます。

クライアントとクライアントのバージョン (Syslog:クライアント、 ClientVersion)

接続で検出されたクライアントのクライアント アプリケーションとバージョン。

接続に使用されている特定のクライアントをシステムが特定できなかった場合、このフィールドは汎用的な名称としてアプリケーション プロトコル名の後に「client」という語を付加して FTP client などと表示します。

クライアント カテゴリとタグ（Client Category and Tag）

アプリケーションの機能を理解するのに役立つ、アプリケーションの特性を示す基準。

[Connection Counter]（Syslog のみ）

ある接続と別の同時接続を区別するカウンタ。このフィールドは、それ自体には意味がありません。

[Sensor UUID]、[First Packet Time]、[Connection Instance ID]、および [Connection Counter] フィールドの情報を総合すると、接続イベントを一意に識別できます。

[Connection Instance ID]（Syslog のみ）

接続イベントを処理した Snort インスタンス。このフィールドは、それ自体には意味がありません。

[Sensor UUID]、[First Packet Time]、[Connection Instance ID]、および [Connection Counter] フィールドの情報を総合すると、接続イベントを一意に識別できます。

ConnectionDuration(Syslog のみ)

このフィールドはのみ存在する syslog フィールド; として存在しない、 Firepower Management Center Web インターフェイス。(Web インターフェイスは、最初のパケットと最後のパケットの列を使用してこの情報を伝達します)。

このフィールドは、接続の終了時にロギングが発生した場合にのみ、値があります。開始-接続の Syslog メッセージのこのフィールドは、出力、これはその時点で知られませんため。

エンド-接続の Syslog メッセージには、このフィールドは、最初のパケットと最後のパケットは、ゼロに短時間の接続があります間の秒数を示します。たとえば、syslog のタイムス

タンプは 12時 34分: 56 と、ConnectionDuration は 5、し、最初のパケットが観察された 12時 34分: 51 にします。

接続（Connections）

接続サマリーに含まれる接続数。長時間接続（複数回の接続サマリー間隔にまたがる接続）の場合、最初の接続サマリー間隔の分だけ増加します。[接続（Connections）] 条件を使用した検索で意味のある結果を表示するには、接続サマリーページを持つカスタム ワークフローを使用する必要があります。

メンバー数（Count）

各行に表示される情報に一致する接続数。同一の行が複数作成される制約を適用した後にのみ、[Count] フィールドが表示されることに注意してください。カスタム ワークフローを作成し、ドリルダウン ページに [カウント（Count）] カラムを追加しない場合、各接続は個別に表示され、パケット数とバイト数は合計されません。

宛先ポート/ICMP コード (Syslog: フィールド - DstPort、 ICMPCodeを分離)

Firepower Management Center Web インターフェイスでは、これらの値がサマリーとグラフを抑制します。

セッション レスポンダが使用するポートまたは ICMP コード。

Device

In the Firepower Management Center web interface, this value constrains summaries and graphs.

接続を検出した管理対象デバイス。または、NetFlowデータから生成された接続の場合は、データを処理した管理対象デバイス。

DNS クエリ (Syslog: DNSQuery)

ドメイン名を検索するために接続でネーム サーバに送信された DNS クエリ。

DNS レコードの種類 (Syslog: DNSRecordType)

接続で送信された DNS クエリを解決するために使用された DNS リソース レコードのタイプ。

DNS 応答 (Syslog: DNSResponseType)

問い合わせ時に接続でネーム サーバに返された DNS レスポンス。

DNS シンクホール名 (Syslog: DNS_Sinkhole)

システムが接続をリダイレクトしたシンクホール サーバの名前。

DNS の TTL (Syslog: DNS_TTL)

DNS サーバが DNS リソース レコードをキャッシュする秒数。

ドメイン（Domain）

接続を検出した管理対象デバイスのドメイン。または、NetFlow データから生成された接続の場合は、データを処理した管理対象デバイスのドメイン。 This field is only present if you have ever configured the Firepower Management Center for multitenancy.

エンドポイント ロケーション（Endpoint Location）

ISE で指定された、ユーザの認証に ISE を使用したネットワーク デバイスの IP アドレス。

エンドポイントのプロファイル (Syslog:エンドポイント プロファイル)

ISE で指定されたユーザのエンドポイント デバイス タイプ。

ファイル (Syslog: FileCount)

(マルウェア ファイルを含む) ファイルの数は、検出または 1 つまたは複数のファイル イベントに関連付けられている接続でブロックします。

In the Firepower Management Center web interface, the view files icon () links to a list of files. アイコンの数字は、その接続で検出またはブロックされたファイル数（マルウェア ファイルを含む）を示します。

最初のパケットまたは最後のパケット (Syslog: ConnectionDuration | フィールドを参照してください)

セッションの最初または最後のパケットが検出された日時。

[First Packet Time]（Syslog のみ）

システムが最初のパケットを検出した時間。

[Sensor UUID]、[First Packet Time]、[Connection Instance ID]、および [Connection Counter] フィールドの情報を総合すると、接続イベントを一意に識別できます。

HTTP Referrer (Syslog: HTTPReferer)

接続で検出された HTTP トラフィックの要求 URL の参照元を示す HTTP 参照元（他の URL へのリンクを提供した Web サイト、他の URL からリンクをインポートした Web サイトなど）。

HTTP 応答コード (Syslog:要求に対する応答)

クライアントからの接続経由の HTTP 要求に応じて送信される HTTP ステータス コード。

入力/出力インターフェイス (Syslog: IngressInterface、 EgressInterface)

接続に関連付けられた入力または出力のインターフェイス。展開に非対称のルーティング設定が含まれている場合は、入力と出力のインターフェイスが同じインラインペアに属する場合があります。

セキュリティ ゾーンの入力/出力 (Syslog: IngressZone、 EgressZone)

接続に関連付けられた入力または出力のセキュリティ ゾーン。

再区分されたカプセル化接続では、元の入力セキュリティ ゾーンの代わりに、割り当てたトンネル ゾーンが入力フィールドに表示されます。出力フィールドは空白です。

イニシエータ/Responder バイト (Syslog: InitiatorBytes、 ResponderBytes)

The total number of bytes transmitted by the session initiator or received by the session responder.

イニシエータ/レスポンダ大陸（Initiator/Responder Continent）

ルーティング可能な IP が検出された場合の、セッション イニシエータまたはレスポンダの IP アドレスに関連付けられた大陸。

イニシエータ/レスポンダ国（Initiator/Responder Country）

ルーティング可能な IP が検出された場合の、セッション イニシエータまたはレスポンダの IP アドレスに関連付けられた国。システムにより、国旗のアイコンと、国の ISO 3166-1 alpha-3 国番号が表示されます。国旗アイコンの上にポインタを移動すると、国の完全な名称が表示されます。

Initiator/Responder IP (Syslog: SrcIP, DstIP)

In the Firepower Management Center web interface, these values constrain summaries and graphs.

The IP address (and host name, if DNS resolution is enabled) of the session initiator (source IP address) or responder (destination IPaddress).

In the Firepower Management Center web interface, host icons next to blacklisted IP addresses look slightly different so that you can identify the blacklisted IP address in a blacklisted connection.

For plaintext, passthrough tunnels either blocked or fastpathed by the prefilter policy, source and destination IP addresses represent the tunnel endpoints—the routed interfaces of the network devices on either side of the tunnel.

イニシエータ/応答側パケット (Syslog: InitiatorPackets、 ResponderPackets)

The total number of packets transmitted by the session initiator or received by the session responder.

Initiator User (Syslog: User)

Firepower Management Centerサマリーとグラフに Web インターフェイス、この値が制限されます。

セッション イニシエータにログインしていたユーザ。このフィールドに [認証なし（No Authentication）] が入力されている場合、ユーザ トラフィックは次のようになります。

- 関連付けられたアイデンティティ ポリシーがないアクセス コントロール ポリシーに一致しました。
- アイデンティティ ポリシーのいずれのルールにも一致しませんでした。

侵入イベント (Syslog: IPSCount)

The number of intrusion events, if any, associated with the connection.

In the Firepower Management Center web interface, the view intrusion events icon () links to a list of events.

IOC

マルウェア イベントが、接続に関与したホストに対する侵入の痕跡（IOC）をトリガーしたかどうか。

NetBIOS ドメイン (Syslog: NetBIOSDomain)

セッションで使用された NetBIOS ドメイン。

NetFlow SNMP 入出力（NetFlow SNMP Input/Output）

NetFlow データから生成された接続の場合、接続トラフィックが NetFlow 対応デバイスに入ったか、NetFlowエクスポータから出た際のインターフェイスのインターフェイスインデックス。

NetFlow 送信元/宛先の自律システム（NetFlow Source/Destination Autonomous System）

NetFlow データから生成された接続の場合、接続のトラフィックの送信元または宛先に対する、Border Gateway Protocol の自律システム番号。

NetFlow 送信元/宛先のプレフィックス（NetFlow Source/Destination Prefix）

NetFlowデータから生成された接続の場合、送信元または宛先の IP アドレスに、送信元と宛先のプレフィックス マスクが追加されたもの。

NetFlow 送信元/宛先 TOS（NetFlow Source/Destination TOS）

NetFlow データから生成された接続の場合、接続トラフィックが NetFlow 対応デバイスに入ったか、NetFlow エクスポータから出たときの Type of Service（TOS）バイトの設定。

Network Analysis Policy (Syslog: NAPPolicy)

イベントの生成に関連付けられているネットワーク分析ポリシー（NAP）（ある場合）。

クライアントのオリジナル国（Original Client Country）

元のクライアントの IP アドレスが属する国。この値を取得するために、システムは元のクライアント IP アドレスを X-Forwarded-For（XFF）、True-Client-IP、またはカスタム定義のHTTPヘッダーから抽出し、それを地理位置情報データベース（GeoDB）を使用して国にマップします。このフィールドに入力するには、元のクライアントに基づいてプロキシ トラフィックを処理するアクセス コントロール ルールを有効にする必要があります。

元のクライアント IP (Syslog: originalClientSrcIP)

X-Forwarded-For（XFF）、True-Client-IP、またはカスタム定義の HTTP ヘッダーからの、元のクライアント IP アドレス。このフィールドに入力するには、元のクライアントに基づいてプロキシ トラフィックを処理するアクセス コントロール ルールを有効にする必要があります。

プレフィルタ ポリシー (Syslog:プレフィルタ ポリシー)

接続を処理したプレフィルタ ポリシー。

プロトコル (Syslog:プロトコル)

In the Firepower Management Center web interface:

- This value constrains summaries and graphs.
- This field is available only as a search field.

接続に使用されるトランスポートプロトコルです。特定のプロトコルを検索するには、名前を使用するか、http://www.iana.org/assignments/protocol-numbers に記載されたプロトコルの番号を指定します。

QoS が適用されたインターフェイス（QoS-Applied Interface）
レート制限された接続で、レート制限を適用するインターフェイスの名前。

QoS がドロップされたイニシエータのバイト数（QoS-Dropped Initiator Bytes）/QoS がドロップされたレスポンダのバイト数（QoS-Dropped Responder Bytes）
レート制限によりセッション イニシエータまたはセッション レスポンダからドロップされたバイト数。

QoS がドロップされたイニシエータのパケット数（QoS-Dropped Initiator Packets）/QoS がドロップされたレスポンダのパケット数（QoS-Dropped Responder Packets）
レート制限によりセッション イニシエータまたはセッション レスポンダからドロップされたパケット数。

QoS ポリシー（QoS Policy）
接続のレートを制限する QoS ポリシー。

QoS ルール（QoS Rule）
接続のレートを制限する QoS ルール。

理由 (Syslog: AccessControlRuleReason)

多くの場合に接続がロギングされた 1 つまたは複数の原因。完全なリストについては、接続イベントの理由 （3040 ページ）を参照してください。

IP ブロック、DNS ブロック、および URL ブロックの理由による接続には、固有のイニシエータ レスポンダ ペアごとに 15 秒のしきい値があります。システムがこれらのいずれかの接続をブロックした後、イベントを生成した時点から 15 秒の間、この 2 つのホスト間で接続がブロックされたとしても、ポートやプロトコルの違いに関わらず、接続イベントを生成しません。

ホストの参照 (Syslog: ReferencedHost)

接続のプロトコルが HTTP または HTTPS の場合、このフィールドにはそれぞれのプロトコルが使用していたホスト名が表示されます。

SecIntMatchingIP(Syslog のみ)

どの IP アドレスが一致します。

有効な値:**なし**、**宛先**、または**送信元**。

Security Context (Syslog: Context)

ASA FirePOWER でマルチ コンテキスト モードで処理される接続で、トラフィックが通過した仮想ファイアウォール グループを特定するメタデータ。

セキュリティ グループ タグ (Syslog:セキュリティ グループ)

接続に関係するパケットのセキュリティ グループ タグ（SGT）属性。SGT は、信頼ネットワーク内での、トラフィックの送信元の権限を指定します。セキュリティ グループ アクセス（Cisco TrustSec と Cisco ISE の両方に共通の機能）は、パケットがネットワークに入るときに属性を適用します。

セキュリティ インテリジェンス カテゴリ (Syslog: URLSICategory、 DNSSICategory、IPReputationSICategory、)

The name of the blacklisted object that represents or contains the blacklisted URL, domain, or IP address in the connection. セキュリティ インテリジェンスのカテゴリは、ネットワーク オブジェクトまたはグループ、ブラックリスト、カスタム セキュリティ インテリジェンスのリストまたはフィード、監視に関連する TID カテゴリ、またはインテリジェンス フィードのカテゴリのいずれかの名前にすることができます。

Firepower Management Center Web インターフェイス、DNS、ネットワーク (IP アドレス)、およびURL のセキュリティ インテリジェンス接続のイベントが 1 つのカテゴリ ()] フィールドに結合されます。Syslog メッセージでは、それらのイベントはタイプによって特定です。

インテリジェンス フィードのカテゴリの詳細については、セキュリティ インテリジェンス オプション （1746 ページ） を参照してください。

[Sensor UUID]（Syslog のみ）

イベントを生成した Firepower デバイスの一意の識別子。

[Sensor UUID]、[First Packet Time]、[Connection Instance ID]、および [Connection Counter] フィールドの情報を総合すると、接続イベントを一意に識別できます。

Source Device

In the Firepower Management Center web interface, this value constrains summaries and graphs.

接続の生成に使用されたデータをブロードキャストする NetFlow エクスポータの IP アドレス。管理対象デバイスによって接続が検出された場合、このフィールドには`Firepower`と表示されます。

送信元ポート/ICMP タイプ (Syslog: SrcPort、 ICMPType)

In the Firepower Management Center web interface, these values constrain summaries and graphs.

セッション イニシエータが使用するポートまたは ICMP タイプ。

SSL Actual Action (Syslog: SSLActualAction)

In the Firepower Management Center web interface, this field is a search field only.

システムにより、検索ワークフローのページの [SSL ステータス（SSL Status）] フィールドにフィールド値が表示されます。

システムが SSL ポリシーの暗号化トラフィックに適用したアクション。

アクション	説明
[ブロック（Block）/リセットしてブロック（Block With Reset）]	ブロックされた暗号化接続を表します。
[復号（再署名）（Decrypt (Resign)）]	再署名サーバ証明書を使用して復号された発信接続を表します。
[復号（キーの交換）（Decrypt (Replace Key)）]	置き換えられた公開キーと自己署名サーバ証明書を使用して復号化された発信接続を表します。
[復号（既知のキー）（Decrypt (Known Key)）]	既知の秘密キーを使用して復号化された着信接続を表します。
[デフォルトアクション（Default Action）]	接続がデフォルト アクションによって処理されたことを示します。
[復号しない（Do not Decrypt）]	システムが復号化しなかった接続を表します。

SSL 証明書情報 (Syslog: SSLCertificate)

In the Firepower Management Center web interface, this field is a search field only.

トラフィックを暗号化するための公開キー証明書に保存される次の情報：

- サブジェクト/発行元共通名（Subject/Issuer Common Name）
- サブジェクト/発行元組織（Subject/Issuer Organization）
- サブジェクト/発行元組織単位（Subject/Issuer Organization Unit）
- 有効期間（Not Valid Before/After）

- シリアル番号（Serial Number）
- 証明書フィンガープリント（Certificate Fingerprint）
- 公開キー フィンガープリント（Public Key Fingerprint）

SSL Certificate Status (Syslog: SSLServerCertStatus)

これは、認証ステータスのSSLルール条件が設定されている場合にのみ適用されます。暗号化されたトラフィックがSSLルールに一致すると、このフィールドに次のサーバの証明書のステータス値の 1 つ以上が表示されます。

- [自署（Self Signed）]
- Valid
- Invalid Signature
- Invalid Issuer
- Expired
- Unknown
- Not Valid Yet
- [失効（Revoked）]

復号できないトラフィックが SSL ルールと一致する場合、このフィールドには [未チェック（Not Checked）] と表示されます。

SSL 暗号スイート (Syslog: SSSLCipherSuite)

接続を暗号化するのに使用される暗号スイートを表すマクロ値。暗号スイート値の指定については、www.iana.org/assignments/tls-parameters/tls-parameters.xhtml を参照してください。

接続に適用された SSL 暗号化（SSL Encryption applied to the connection）

このフィールドは、Firepower Management Center の Web インターフェイスで [検索] フィールドとしてのみ使用できます。

yes または **no** を [SSL（SSL）] 検索フィールドに入力することで、TLS/SSL 暗号化された接続または暗号化されていない接続が表示されます。

SSL 期待アクション (Syslog: SSLExpectedAction)

In the Firepower Management Center web interface, this field is a search field only.

有効なSSLルールで指定された、暗号化トラフィックに適用されると予想されるアクション。

[SSL の実際の動作（SSL Actual Action）] にリストされている値を入力します。

SSL 失敗の理由 (Syslog: SSLFlowStatus)

システムが暗号化されたトラフィックの復号化に失敗した理由。

- 不明

- No Match
- Success
- Uncached Session
- 不明な暗号スイート
- サポートされていない暗号スイート
- Unsupported SSL Version
- SSL Compression Used
- Session Undecryptable in Passive Mode
- Handshake Error
- Decryption Error
- Pending Server Name Category Lookup
- Pending Common Name Category Lookup
- Internal Error
- Network Parameters Unavailable
- Invalid Server Certificate Handle
- Server Certificate Fingerprint Unavailable
- Cannot Cache Subject DN
- Cannot Cache Issuer DN
- Unknown SSL Version
- External Certificate List Unavailable
- External Certificate Fingerprint Unavailable
- Internal Certificate List Invalid
- Internal Certificate List Unavailable
- Internal Certificate Unavailable
- Internal Certificate Fingerprint Unavailable
- Server Certificate Validation Unavailable
- Server Certificate Validation Failure
- 無効なアクション（Invalid Action）

フィールド値は、検索ワークフローのページの [SSL ステータス（SSL Status）] フィールドに表示されます。

SSL フロー エラー（SSL Flow Error）

エラーが TLS/SSL セッション中に発生した場合はエラー名および 16 進数コード。エラーが発生しない場合は [Success]。

SSL フロー フラグ（SSL Flow Flags）

暗号化された接続の最初の 10 個のデバッグ レベル フラグ。On a workflow page, to view all flags, click the ellipsis (**...** 。

管理対象デバイスが過負荷の状態になっている場合は、OVER_SUBSCRIBED というメッセージが表示されます。詳細については、TLS/SSL オーバーサブスクリプションのトラブルシューティング （1898 ページ）を参照してください。

SSL フロー メッセージ（SSL Flow Messages）

次のキーワードは、暗号化トラフィックが TLS/SSL ハンドシェイク時にクライアントとサーバ間で交換される指定されたメッセージ タイプに関連付けられていることを示します。詳細については、http://tools.ietf.org/html/rfc5246を参照してください。

- HELLO_REQUEST
- CLIENT_ALERT
- SERVER_ALERT
- CLIENT_HELLO
- SERVER_HELLO
- SERVER_CERTIFICATE
- SERVER_KEY_EXCHANGE
- CERTIFICATE_REQUEST
- SERVER_HELLO_DONE
- CLIENT_CERTIFICATE
- CLIENT_KEY_EXCHANGE
- CERTIFICATE_VERIFY
- CLIENT_CHANGE_CIPHER_SPEC
- CLIENT_FINISHED
- SERVER_CHANGE_CIPHER_SPEC
- SERVER_FINISHED
- NEW_SESSION_TICKET
- HANDSHAKE_OTHER
- APP_DATA_FROM_CLIENT
- APP_DATA_FROM_SERVER

アプリケーションでSSLハートビートエクステンションが使用されている場合は、TLS/SSLというメッセージが表示されます。詳細については、TLSハートビートについて（1900ページ）を参照してください。

SSL ポリシー (Syslog: SSLPolicy)

接続を処理した SSL ポリシー。

SSL ルール (Syslog: SSLRuleName)

接続を処理した SSL ルールまたはデフォルト アクションと、その接続に一致した最初のモニタ ルール。If the connection matched a Monitor rule, the field displays the name of the rule that handled the connection, followed by the Monitor rule name.

SSLServerName(Syslog のみ)

This field exists ONLY as a syslog field; it does not exist in the Firepower Management Center web interface.

Hostname of the server with which the client established an encrypted connection.

SSL セッション ID (Syslog: SSLSessionID)

TLS/SSL ハンドシェイク時にクライアントとサーバ間でネゴシエートされた 16 進数セッション ID。

SSL ステータス（SSL Status）

暗号化された接続を記録した、[SSL の実際の動作（SSL Actual Action）]（SSL ルール、デフォルトアクション、または復号できないトラフィック アクション）に関連したアクション。ロック アイコン（  ）は、SSL 証明書の詳細にリンクしています。証明書を利用できない場合（たとえば、TLS/SSL ハンドシェイク エラーにより接続がブロックされる場合）、ロック アイコンはグレー表示になります。

システムが暗号化接続を復号できなかった場合は、[SSL の実際の動作（SSL Actual Action）]（実行された復号不能のトラフィック アクション）と、[SSL 失敗理由（SSL Failure Reason）] が表示されます。たとえば、不明な暗号スイートによって暗号化されたトラフィックをシステムが検出し、それ以上のインスペクションをせずにこれを許可した場合、このフィールドには [Do Not Decrypt (Unknown Cipher Suite)] が表示されます。

このフィールドを検索する場合は、[SSL の実際の動作（SSL Actual Action）] と [SSL 失敗理由（SSL Failure Reason）] の 1 つ以上の値を入力することで、システムが処理した、または復号に失敗した暗号化トラフィックが表示されます。

SSL Subject/Issuer Country

このフィールドはでのみ使用可能なFirepower Management CenterWeb インターフェイス、および [検索] フィールドとしてのみ。

暗号化証明書に関連付けられている件名または発行者の国に関する 2 文字の ISO 3166-1 アルファ 2 国コード。

SSL チケット ID (Syslog: SSLTicketID)

TLS/SSL ハンドシェイク時に送信されたセッション チケット情報の 16 進数のハッシュ値。

SSLURLCategory (Syslog Only)

URL categories for the URL visited in the encrypted connection.

このフィールドはのみ存在する syslog フィールド; としてFirepower Management Center URL カテゴリ列で Web インターフェイス、このフィールドに値が含まれています。

URLを参照してください。

SSL バージョン (Syslog: SSLVersion)

接続の暗号化に使用された TLS/SSL プロトコル バージョン。

- 不明
- SSLv2.0
- SSLv3.0
- TLSv1.0
- TLSv1.1
- TLSv1.2

TCP フラグ (Syslog: TCPFlags)

NetFlow データから生成された接続において、接続で検出された TCP フラグ。

このフィールドを検索する場合は、TCP フラグのカンマ区切りリストを入力することで、これらのフラグが *1* つ以上あるすべての接続が表示されます。

時刻（Time）

システムが接続を接続サマリーに集約するために使用した5分間隔の終了時刻。このフィールドは検索できません。

Total Packets

This field is available only as a search field.

接続で送信された合計パケット数。

Traffic (KB)

このフィールドは [検索] フィールドとしてのみ使用できます。

接続で送信されたデータの総量（キロバイト単位）。

トンネル/プレフィルタ ルール (Syslog:トンネルまたはプレフィルター ルール)

トンネル ルール、プレフィルタ ルール、または接続を処理したプレフィルタ ポリシーのデフォルト アクション。

[URL、URLカテゴリ、およびURLレピュテーション（URL, URL Category, and URL Reputation）]（syslog：URL、URLCategory および SSLURLCategory、URLReputation）

セッション中にモニタ対象のホストによって要求された URL と、関連付けられたカテゴリおよびレピュテーション（利用できる場合）。

システムが TLS/SSL アプリケーションを識別またはブロックする場合、要求された URL は暗号化トラフィック内にあるため、システムは、SSL 証明書に基づいてトラフィックを識別します。したがって TLS/SSL アプリケーションの場合、このフィールドは証明書に含まれる一般名を表示します。

上記は**SSLURLCategory**も参照してください。

ユーザ エージェント (Syslog: UserAgent)

接続で検出された HTTP トラフィックから取得したユーザ エージェント文字列アプリケーションの情報。

VLAN ID (Syslog: VLAN_ID)

接続をトリガーしたパケットに関連付けられている最内部 VLAN ID。

Webアプリケーション (Syslog: web アプリケーション)

接続で検出された HTTP トラフィックの内容または要求された URL を表す Web アプリケーション。

Web アプリケーションがイベントの URL に一致しない場合、そのトラフィックは通常、参照先のトラフィックです（アドバタイズメントのトラフィックなど）。システムは、参照先のトラフィックを検出すると、参照元のアプリケーションを保存し（可能な場合）、そのアプリケーションを Web アプリケーションとして表示します。

HTTP トラフィックに含まれる特定の Web アプリケーションをシステムが特定できなかった場合、このフィールドには [Web ブランジング（Web Browsing）] と表示されます。

Web アプリケーションのカテゴリとタグ（Web Application Category and Tag）

アプリケーションの機能を理解するのに役立つ、アプリケーションの特性を示す基準。

接続とセキュリティ インテリジェンス イベントのフィールドについて

Firepower Management Center の Web インターフェイスでは、[分析（Analysis）] > [接続（Connections）] サブメニューのテーブル形式とグラフィカルなワークフローを使用して接続イベントとセキュリティ インテリジェンス イベントを表示したり、検索できます。

（注） 各セキュリティ インテリジェンス イベントには、同一の、個別に保存された接続イベントがあります。すべてのセキュリティ インテリジェンス イベントに、入力済みの [セキュリティ インテリジェンス カテゴリ（Security Intelligence Category）] フィールドがあります。

個別のイベントで使用可能な情報は、システムがいつ、なぜ、どのようにして接続をログに記録したかによって異なります。

検索の制約

検索ページのアスタリスク（*）が付いたフィールドは、接続グラフおよび接続サマリーを制約します。接続グラフは接続サマリーに基づいているため、接続サマリーを制約しているのと同じ条件が接続グラフを制約します。無効な検索条件を使用して接続サマリーを検索し、カスタム ワークフローの接続サマリー ページを使用して結果を見る場合、無効な条件には適用不可（N/A）としてラベルが付けられ、取り消し線が引かれます。

syslog フィールド

ほとんどのフィールドは Firepower Management Center Web インターフェイス内のほか、syslog メッセージとしても表示されます。同等にリストされている syslog のないフィールドは、syslog メッセージでは使用可能できません。いくつかのフィールドは（前述のように）syslog のみのフィールドですが、その他のいくつかは、syslog メッセージ内の個別のフィールドが Web インターフェイス内に統合されたフィールド、またはその逆のフィールドです。

接続イベントの理由

接続イベントの [理由（Reason）] フィールドには、次の状況で接続がロギングされた理由が表示されます。

理由（Reason）	説明
コンテンツ制限（Content Restriction）	セーフサーチまたは YouTube EDU 機能のいずれかに関連したコンテンツ制限を実施するために、パケットが変更されました。
DNS ブロック（DNS Block）	ドメイン名とセキュリティインテリジェンスデータに基づいて、インスペクションなしで接続が拒否されました。[DNS ブロック（DNS Block）] の理由は、DNS ルール アクションに応じて、[ブロック（Block）]、[ドメインが見つかりません（Domain not found）]、[シンクホール（Sinkhole）] のアクションと対として組み合わされます。
DNS モニタ（DNS Monitor）	システムはドメイン名とセキュリティインテリジェンスデータに基づいて接続を拒否するはずでしたが、システムは接続を拒否するのではなくモニタするように設定されています。
[ファイルブロック（File Block）]	ファイルまたはマルウェア ファイルが接続に含まれており、システムがその送信を防いでいます。[ファイルブロック（File Block）] の理由は必ず [ブロック（Block）] アクションと対として組み合わされます。
ファイル カスタム検出（File Custom Detection）	カスタム検出リストにあるファイルが接続に含まれており、システムがその送信を防いでいます。
[ファイルモニタ（File Monitor）]	システムが接続において特定のファイルの種類を検出しました。

理由（**Reason**）	説明
[ファイル復帰許可（File Resume Allow）]	ファイル送信がはじめに [ファイルブロック（Block Files）] ルールまたは [マルウェアブロック（Block Malware）] ファイル ルールによってブロックされました。ファイルを許可する新しいアクセス コントロール ポリシーが展開された後、HTTP セッションが自動的に再開しました。この理由はインライン展開のみで表示されます。
ファイル復帰ブロック（File Resume Block）	ファイル送信がはじめに [ファイル検出（Detect Files）] ルールまたは [マルウェアクラウドルックアップ（Malware Cloud Lookup）] ファイル ルールによって許可されました。ファイルをブロックする新しいアクセス コントロール ポリシーが展開された後、HTTP セッションが自動的に停止しました。この理由はインライン展開のみで表示されます。
インテリジェント アプリケーション バイパス（Intelligent App Bypass）	インテリジェント アプリケーション バイパス（IAB）モード： • アクションが [信頼（Trust）] の場合、IAB はバイパス モードでした。一致するトラフィックは、追加のインスペクションなしで通過しました。 • アクションが [許可（Allow）] の場合、IAB はテスト モードでした。一致するトラフィックは、追加のインスペクションに使用できました。
侵入ブロック（Intrusion Block）	接続で検出されたエクスプロイト（侵入ポリシー違反）をシステムがブロックしたか、ブロックするはずでした。[侵入ブロック（Intrusion Block）] の理由は、ブロックされたエクスプロイトの場合は [ブロック（Block）]、ブロックされるはずだったエクスプロイトの場合は [許可（Allow）] のアクションと対として組み合わされます。
[侵入モニタ（Intrusion Monitor）]	接続で検出されたエクスプロイトをシステムが検出したものの、ブロックしなかったことを示します。これは、トリガーされた侵入ルールの状態が [イベントを生成する（Generate Events）] に設定されている場合に発生します。
[IPブロック（IP Block）]	IP アドレスとセキュリティ インテリジェンス データに基づいて、インスペクションなしで接続が拒否されました。[IPブロック（IP Block）] の理由は必ず [ブロック（Block）] のアクションと対として組み合わされます。
IP モニタ（IP Monitor）	システムは IP アドレスとセキュリティ インテリジェンス データに基づいて接続を拒否するはずでしたが、システムは接続を拒否するのではなくモニタするように設定されています。
SSL ブロック（SSL Block）	システムが TLS/SSL インスペクション設定に基づいて暗号化接続をブロックしました。[SSL ブロック（SSL Block）] の理由は必ず [ブロック（Block）] のアクションと対として組み合わされます。

理由（Reason）	説明
URL ブロック（URL Block）	URL とセキュリティ インテリジェンス データに基づいて、インスペクションなしで接続が拒否されました。[URL ブロック（URL Block）] の理由は必ず [ブロック（Block）] のアクションと対として組み合わされます。
URL モニタ（URL Monitor）	システムは URL とセキュリティ インテリジェンス データに基づいて接続を拒否するはずでしたが、システムは接続を拒否するのではなくモニタするように設定されています。
ユーザ バイパス（User Bypass）	最初にユーザの HTTP 要求をブロックしましたが、ユーザのクリックによって警告ページからサイトを表示しました。[ユーザ バイパス（User Bypass）] の理由は必ず [許可（Allow）] のアクションと対として組み合わされます。

接続イベント フィールドの入力の要件

接続イベント、セキュリティ インテリジェンス イベント、接続サマリーで利用可能な情報は、いくつかの要因によって異なります。

アプライアンス モデルおよびライセンス

多くの機能は、ターゲット デバイスで特定のライセンス付与対象の機能を有効にしなければ使用できません。また、一部のモデルでしか使用できない機能も多くあります。

たとえば、NGIPSv デバイスは TLS/SSL インスペクションをサポートしません。これらのデバイスは暗号化されたトラフィックを検査できないため、記録される接続イベントには暗号化された接続に関する情報は含まれていません。

トラフィックの特性

システムは、ネットワーク トラフィック内に存在する（および検出可能な）情報だけを報告します。たとえば、イニシエータ ホストに関連付けられているユーザがいない、またはプロトコルが DNS、HTTP、または HTTPS ではない接続で検出される参照先ホストがいない可能性があります。

発信元/検出方法：トラフィック ベースの検出と NetFlow

NetFlow 専用フィールドを除き、NetFlow レコードで利用可能な情報は、トラフィック ベースの検出によって生成される情報よりも限定されます。NetFlow データと管理対象デバイス データの違い （2478 ページ）を参照してください。

評価ステージ

各タイプのトラフィックのインスペクションと制御は、最大限の柔軟性とパフォーマンスを引き出すために最も意味がある局面で実行されます。

たとえば、システムは、さらなるリソース集中型評価を行う前に、セキュリティ インテリジェンスを強制します。接続がセキュリティ インテリジェンスによってブロックされた場合、結果

として生成されるイベントには、その後の評価によってシステムで収集されることになっていた情報（ユーザ ID など）が含まれません。

ロギング方法：接続の開始または終了

システムが接続の検出時にその接続の開始または終了（またはその両方）をログに記録できるかどうかは、システムがその接続をどのように検出して処理するように設定されているかによって異なります。

接続開始イベントには、セッション期間にわたってトラフィックを調査して判別しなければならない情報が伴ってません（送信されたデータの合計量や、接続の最終パケットのタイムスタンプなど）。また、接続開始イベントにセッションのアプリケーションや URL トラフィックに関する情報が伴っている保証もなく、セッションの暗号化に関する詳細は含まれていません。通常、ブロックされる接続については、接続開始イベントのログへの記録が唯一のオプションになります。

接続イベント タイプ：個々またはサマリー

接続サマリーには、集約された接続に関連付けられたすべての情報が含まれているわけではありません。たとえば、接続サマリーに接続を集約する際にクライアント情報は使用されないため、サマリーにクライアント情報は含まれません。

接続グラフは、接続終了ログのみを使用する接続サマリーのデータに基づいていることに注意してください。接続開始データだけをロギングするようにシステムが設定されている場合、接続グラフと接続サマリーのイベント ビューにはデータが表示されません。

その他の設定

接続のロギングに影響するその他の設定には以下のものが含まれますが、これらに限定されるわけではありません。

- Active Directory ドメイン コントローラで認証するユーザに関連付けられている接続では、ISE が設定されている場合にのみ、ISE 関連のフィールドにデータが入力されます。接続イベントには、LDAP、RADIUS、RSA ドメイン コントローラで認証するユーザの ISE データは含まれません。
- [セキュリティグループタグ（Security Group Tag）] フィールドにデータが入力されるのは、ISE をアイデンティティ ソースとして設定した場合、またはカスタム SGT ルール条件を追加した場合のみです。
- プレフィルタ関連のフィールド（セキュリティ ゾーン フィールドのトンネル ゾーン情報を含む）には、プレフィルタ ポリシーで処理される接続の場合にのみ、データが入力されます。
- TLS/SSL 関連のフィールドには、SSL ポリシーで処理される暗号化接続の場合にのみ、データが入力されます。トラフィックの復号化が必要ない場合、Do Not Decrypt ルールの操作を使用して、フィールドの値を表示することができます。
- ファイル情報フィールドには、ファイル ポリシーと関連付けられたアクセス コントロール ルールによってログに記録される接続の場合にのみ、データが入力されます。

- 侵入情報フィールドには、侵入ポリシーに関連付けられているアクセス コントロール ルールあるいはデフォルト アクションによってログに記録される接続の場合にのみ、データが入力されます。
- QoS 関連のフィールドには、レート制限が適用される接続の場合にのみ、データが入力されます。
- [理由（Reason）] フィールドには、特定の場合にのみデータが入力されます（ユーザがインタラクティブ ブロック設定をバイパスしている場合など）。
- [ドメイン（Domain）] フィールドが表示されるのは、マルチテナンシー用に Firepower Management Center を設定した場合のみです。
- アクセス コントロール ポリシーの詳細設定では、HTTP セッションのモニタ対象ホストによって要求された URL ごとにシステムが接続ログに保存する文字数を制御できます。この設定を使用して URL のロギングを無効化する場合、システムは接続ログで個々の URL を表示しませんが、カテゴリとレピュテーション データは参照できます（存在する場合）。

関連トピック

NetFlow データと管理対象デバイス データの違い （2478 ページ）

接続イベント フィールドで利用可能な情報

このトピックの表に、システムが接続およびセキュリティ インテリジェンスのフィールドに値を読み込むことができるタイミングを示します。表の列は、次のイベント タイプを示しています。

- [発信元：直接（Origin: Direct）]：Firepower システムの管理対象デバイスで検出および処理される接続を表すイベント。
- [発信元：NetFlow（Origin: NetFlow）]：NetFlow エクスポータでエクスポートされる接続を表すイベント。
- [ロギング：開始（Logging: Start）]：開始時にログに記録される接続を表すイベント。
- [ロギング：終了（Logging: End）]：終了時にログに記録される接続を表すイベント。

表内の「はい（yes）」は、システムが接続イベント フィールドに値を読み込む必要があることを意味するものではなく、読み込むことができることを意味します。システムは、ネットワーク トラフィック内に存在する（および検出可能な）情報だけを報告します。たとえば、TLS/SSL 関連のフィールドには、SSL ポリシーによって処理される暗号化された接続のレコードについてのみ値が読み込まれます。

接続イベント フィールド	発信元：直接（**Origin: Direct**）	発信元：**NetFlow**（**Origin: NetFlow**）	ロギング：開始（**Logging: Start**）	ロギング：終了（**Logging: End**）
アクセス コントロール ポリシー	はい	いいえ	はい	はい
アクセス コントロール ルール（Access Control Rule）	はい	いいえ	はい	はい
Action	はい	いいえ	はい	はい
アプリケーション プロトコル	はい	はい	利用可能な場合	yes
アプリケーション プロトコル カテゴリとタグ（Application Protocol Category & Tag）	はい	いいえ（No）	利用可能な場合	yes
アプリケーションのリスク（Application Risk）	はい	いいえ（No）	利用可能な場合	yes
ビジネス関連性	はい	いいえ（No）	利用可能な場合	yes
クライアント	はい	いいえ（No）	利用可能な場合	yes
クライアント カテゴリとタグ（Client Category & Tag）	はい	いいえ（No）	利用可能な場合	yes
Client Version	はい	いいえ（No）	利用可能な場合	yes
Connections	はい	はい	いいえ	はい
Count	はい	はい	はい	はい
宛先ポート/ICMP タイプ（Destination Port/ICMP Type）	はい	はい	はい	はい
デバイス	はい	はい	はい	はい
ドメイン（Domain）	はい	はい	はい	はい
DNS クエリ（DNS Query）	はい	いいえ	はい	はい
DNS レコード タイプ（DNS Record Type）	はい	いいえ	はい	はい

接続イベント フィールド	発信元：直接（**Origin: Direct**）	発信元：**NetFlow**（**Origin: NetFlow**）	ロギング：開始（**Logging: Start**）	ロギング：終了（**Logging: End**）
DNS レスポンス（DNS Response）	はい	いいえ	はい	はい
DNS シンクホール名（DNS Sinkhole Name）	はい	いいえ	はい	はい
DNS TTL	はい	いいえ	はい	はい
Egress Interface	はい	いいえ	はい	はい
Egress Security Zone	はい	いいえ	はい	はい
エンドポイント ロケーション（Endpoint Location）	はい	いいえ	はい	はい
エンドポイント プロファイル	はい	いいえ	はい	はい
ファイル	はい	いいえ	いいえ	はい
First Packet	はい	はい	はい	はい
HTTP リファラ（HTTP Referrer）	はい	いいえ	いいえ	はい
HTTP 応答コード（HTTP Response Code）	はい	いいえ	はい	はい
Ingress Interface	はい	いいえ	はい	はい
入力セキュリティ ゾーン（Ingress Security Zone）	はい	いいえ	はい	はい
Initiator Bytes	はい	はい	有用でない	yes
Initiator Country	はい	いいえ	はい	はい
イニシエータ IP（Initiator IP）	はい	はい	はい	はい
イニシエータ パケット（Initiator Packets）	はい	はい	有用でない	yes
Initiator User	はい	はい	はい	はい
Intrusion Events	はい	いいえ	いいえ	はい

接続イベント フィールド	発信元：直接（**Origin: Direct**）	発信元：**NetFlow**（**Origin: NetFlow**）	ロギング：開始（**Logging: Start**）	ロギング：終了（**Logging: End**）
侵入ポリシー（Intrusion Policy）	はい	いいえ	はい	はい
IOC（侵害の兆候）（IOC (Indication of Compromise)）	はい	いいえ	はい	はい
最後のパケット（Last Packet）	はい	はい	いいえ	はい
NetBIOS Domain	はい	いいえ	はい	はい
NetFlow 送信元/宛先の自律システム（NetFlow Source/Destination Autonomous System）	いいえ	はい	いいえ	はい
NetFlow 送信元/宛先のプレフィックス（NetFlow Source/Destination Prefix）	いいえ	はい	いいえ	はい
NetFlow 送信元/宛先 TOS（NetFlow Source/Destination TOS）	いいえ	はい	いいえ	はい
NetFlow SNMP 入出力（NetFlow SNMP Input/Output）	いいえ	はい	いいえ	はい
ネットワーク分析ポリシー（Network Analysis Policy）	はい	いいえ	はい	はい
クライアントのオリジナル国（Original Client Country）	はい	いいえ	はい	はい
Original Client IP	はい	いいえ	はい	はい
プレフィルタ ポリシー（Prefilter Policy）	はい	いいえ	はい	はい
QoS が適用されたインターフェイス（QoS-Applied Interface）	はい	いいえ	いいえ	はい
QoS がドロップされたイニシエータのバイト数（QoS-Dropped Initiator Bytes）	はい	いいえ	いいえ	はい

接続イベント フィールド	発信元：直接（**Origin: Direct**）	発信元：**NetFlow**（**Origin: NetFlow**）	ロギング：開始（**Logging: Start**）	ロギング：終了（**Logging: End**）
QoS がドロップされたイニシエータのパケット数（QoS-Dropped Initiator Packets）	はい	いいえ	いいえ	はい
QoS がドロップされたレスポンダのバイト数（QoS-Dropped Responder Bytes）	はい	いいえ	いいえ	はい
QoS がドロップされたレスポンダのパケット数（QoS-Dropped Responder Packets）	はい	いいえ	いいえ	はい
QoS ポリシー	はい	いいえ	いいえ	はい
QoS ルール（QoS Rule）	はい	いいえ	いいえ	はい
理由	はい	いいえ	はい	はい
参照ホスト（Referenced Host）	はい	いいえ	いいえ	はい
Responder Bytes	はい	はい	有用でない	yes
Responder Country	はい	いいえ	はい	はい
Responder IP	はい	はい	はい	はい
Responder Packets	はい	はい	有用でない	yes
Security Context（ASA のみ）	はい	いいえ	はい	はい
セキュリティ グループ タグ（SGT）	はい	いいえ	はい	はい
セキュリティ インテリジェンスのカテゴリ	はい	いいえ	はい	はい
Source Device	はい	はい	はい	はい
Source Port/ICMP Type	はい	はい	はい	はい
SSL Certificate Status	はい	いいえ	いいえ	はい
SSL Cipher Suite	はい	いいえ	いいえ	はい

接続イベント フィールド	発信元：直接（**Origin: Direct**）	発信元：**NetFlow**（**Origin: NetFlow**）	ロギング：開始（**Logging: Start**）	ロギング：終了（**Logging: End**）
SSL Flow Error	はい	いいえ	いいえ	はい
SSL Flow Flags	はい	いいえ	いいえ	はい
SSL Flow Messages	はい	いいえ	いいえ	はい
SSL ポリシー	はい	いいえ	いいえ	はい
SSL Rule	はい	いいえ	いいえ	はい
SSL セッション ID	はい	いいえ	いいえ	はい
SSL Status	はい	いいえ	いいえ	はい
SSL Version	はい	いいえ	いいえ	はい
TCP Flags	いいえ	はい	いいえ	はい
時刻	はい	はい	いいえ	はい
トンネル/プレフィルタ ルール（Tunnel/Prefilter Rule）	はい	いいえ	はい	はい
URL	はい	いいえ（No）	利用可能な場合	yes
URL カテゴリ	はい	いいえ（No）	利用可能な場合	yes
URLレピュテーション（URL Reputation）	はい	いいえ（No）	利用可能な場合	yes
ユーザ エージェント（User Agent）	はい	いいえ	いいえ	はい
VLAN ID	はい	いいえ	はい	はい
Web アプリケーション	はい	いいえ（No）	利用可能な場合	yes
Web アプリケーションのカテゴリとタグ（Web Application Category & Tag）	はい	いいえ（No）	利用可能な場合	yes

接続およびセキュリティインテリジェンスイベントテーブルの使用

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Any Security Analyst

Firepower Management Center を使用して、接続イベントまたはセキュリティ インテリジェンス イベントのテーブルを表示することができます。ここでユーザは、検索する情報に応じてイベント ビューを操作することができます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

接続グラフにアクセスしたときに表示されるページは、使用するワークフローによって異なります。イベントのテーブル ビューで終わる事前定義されたワークフローを使用できます。また、特定のニーズを満たす情報だけを表示するカスタム ワークフローを作成することもできます。

接続またはセキュリティ インテリジェンス ワークフロー テーブルを使用すると、たくさんの一般的なアクションを実行できます。

ドリルダウン ページで接続イベントを制約する場合、同一のイベントからのパケット数とバイト数が合計されることに注意してください。ただし、カスタム ワークフローを使用しており、ドリルダウン ページに [カウント（Count）] カラムを追加していない場合、イベントは個別に表示され、パケット数とバイト数は合計されません。

システムが生成した接続イベントが 25 個を超えると、[接続イベント（Connection Events）] テーブル ビューに、使用可能なイベントのページ数ではなく、「1 of Many」と表示されます。

ステップ 1 次のいずれかを選択します。

- **[Analysis]** > **[Connections]** > **[Events]**（接続イベントの場合）
- **[Analysis]** > **[Connections]** > **[Security Intelligence Events]**

（注） テーブルの代わりに接続グラフが表示された場合、ワークフロー タイトルで [(ワークフローの切り替え)（(switch workflow)）] をクリックし、事前定義された [接続イベント（Connection Events）] ワークフローまたはカスタム ワークフローを選択します。事前定義されたすべての接続イベント（接続グラフを含む）は、接続のテーブル ビューで終了することに注意してください。

ステップ 2 次の選択肢があります。

- 時間範囲：時間範囲を調整（イベントが表示されない場合に役立ちます）する方法については、時間枠の変更 （2956 ページ）を参照してください。

- フィールド名：テーブルのカラムの内容について詳しく調べるには、接続イベントとセキュリティ インテリジェンス イベントのフィールド （3024 ページ）を参照してください。

  ヒント イベントのテーブル ビューでは、各アプリケーション タイプの [カテゴリ（Category）] および [タグ（Tag）] フィールド、NetFlow 関連のフィールド、TLS/SSL 関連のフィールドなど、いくつかのフィールドがデフォルトで非表示です。イベント ビューに非表示フィールドを表示するには、検索制約を展開し、[無効にされたカラム（Disabled Columns）] の下のフィールド名をクリックします。

- トランザクション コンテキストと詳細：（所属する組織でイベント データを外部の Firepower システムに保存している場合）パケットや履歴データなど、イベントに関連する情報を調査するには、イベントの値を右クリックします。表示されるオプションは、データタイプやシステムに設定されている統合によって異なります。詳細については、を使用したイベント調査 Cisco Security Packet Analyzer （2882 ページ）および Web ベースのリソースを使用したイベントの調査 （2890 ページ）を参照してください。

- 外部インテリジェンス：イベントに関する情報を収集するには、テーブルでイベントの値を右クリックして、シスコまたはサードパーティのインテリジェンス ソースを選択します。たとえば、不審な IP アドレスに関する詳細情報を Cisco Talos から入手できます。表示されるオプションは、データタイプやシステムに設定されている統合によって異なります。詳細については、Web ベースのリソースを使用したイベントの調査 （2890 ページ）を参照してください。

- ホスト プロファイル：IP アドレスのホスト プロファイルを表示するには、ホスト プロファイルのアイコン（  ）をクリックします。アクティブな侵害の兆候（IOC）タグのあるホストの場合は、IP アドレスの横に表示される侵害されたホストのアイコン（  ）をクリックします。

- User Profile — To view user identity information, click the user icon that appears next to the user identity ( , or for users associated with IOCs, ).

- ファイルおよびマルウェア：接続で検出されたまたはブロックされたマルウェアを含むファイルを表示するには、ファイルの表示アイコン（  ）をクリックし、接続で検出されたファイルとマルウェアの表示 （3052 ページ）の説明に従って続行します。

- 侵入イベント：接続に関連付けられている侵入イベントを優先順位や影響とともに表示するには、[侵入イベント（Intrusion Events）] カラムの侵入イベント アイコン（  ）をクリックして、接続に関連付けられた侵入イベントの表示 （3054 ページ）の説明に従って続行します。

  ヒント 1 つまたは複数の接続に関連付けられた侵入イベント、ファイル イベント、またはマルウェア イベントをすばやく表示するには、テーブルのチェックボックスを使用して接続を選択し、[ジャンプ（Jump to）] ドロップダウン リストから該当するオプションを選択します。セキュリティ インテリジェンスによりブラックリストに載せられている接続に関連するファイルまたは侵入が、アクセス コントロール ルールの評価の前にブロックされることによって、1 つも存在しない可能性があることに注意してください。ブラックリストではなく、接続をモニタするようにセキュリティ インテリジェンスを設定した場合に限り、セキュリティ インテリジェンス イベントに関するこの情報が表示されます。

- 証明書：接続を暗号化するために使用される利用可能な証明書についての詳細を表示するには、[SSL ステータス（SSL Status）] カラムの有効なロック アイコン（  ）をクリックします。
- 制約：表示されるカラムを制約にするには、非表示にするカラムの見出しにある閉じるアイコン（  ）をクリックします。表示されるポップアップ ウィンドウで、[適用（Apply）] をクリックします。

  ヒント 他のカラムを表示または非表示にするには、[適用（Apply）] をクリックする前に、該当するチェック ボックスをオンまたはオフにします。無効になったカラムをビューに再び追加するには、検索制約を展開し、[無効にされたカラム（Disabled Columns）] の下のカラム名をクリックします。

- イベントの削除：現在の制約されたビューにある一部またはすべての項目を削除するには、削除する項目の横にあるチェックボックスをオンにし、[削除（Delete）] または [すべて削除（Delete All）] をクリックします。
- ドリル ダウン：ドリルダウン ページの使用 （2940 ページ）を参照してください。

  ヒント ロギングされた接続に一致した複数のモニタ ルールのうち 1 つにドリル ダウンするには、[*N* モニタ ルール（N Monitor Rules）] の値をクリックします。表示されるポップアップ ウィンドウで、接続イベントを抑制するために使用するモニタ ルールをクリックします。

- このページに移動する：ワークフロー ページのトラバーサル ツール （2937 ページ）を参照してください。
- ページ間で移動する：現在の制約を維持しながら現在のワークフローのページ間で移動するには、ワークフロー ページの左上にある該当するページ リンクをクリックします。
- [イベント ビュー間の移動（Navigate Between Event Views）]：他のイベント ビューに移動して関連するイベントを表示するには、[移動先（Jump to）] をクリックし、ドロップダウンリストからイベント ビューを選択します。
- ソート：ワークフローでデータをソートするには、カラムのタイトルをクリックします。ソート順を逆にするには、カラムのタイトルをもう一度クリックします。

関連トピック

概要：ワークフロー （2917 ページ）
イベント ビュー設定の設定 （43 ページ）

接続で検出されたファイルとマルウェアの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス（**Access**）
脅威またはマルウェア	保護またはマルウェア	いずれか（Any）	いずれか（Any）	Admin/Any Security Analyst

1 つまたは複数のアクセス コントロール ルールにファイル ポリシーを関連付けると、システムは一致するトラフィックのファイル（マルウェアを含む）を検出できます。[分析（Analysis）] > [接続（Connections）] メニュー オプションを使用して、各ルールによってロギングされた接続と関連付けられているファイル イベント（存在する場合）を確認します。ファイル リストの代わりに、Firepower Management Center はファイル表示アイコン（  ）を [ファイル（Files）] 列に表示します。アイコンの数字は、その接続で検出またはブロックされたファイル数（マルウェア ファイルを含む）を示します。

すべてのファイルおよびマルウェア イベントが接続に関連付けられるわけではありません。具体的には次のとおりです。

- エンドポイント向け AMP によって検出されたマルウェア イベント（「エンドポイント ベースのマルウェアイベント」）は接続に関連付けられません。これらのイベントは AMP for Endpoints 展開からインポートされます。
- IMAP に対応した電子メール クライアントの多くは単一 IMAP セッションを使用し、それはユーザがアプリケーションを終了したときに終了します。長時間接続はシステムによってロギングされますが、セッションでダウンロードされたファイルは、そのセッションが終了するまで接続に関連付けられません。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

ステップ 1 [分析（Analysis）] > [接続（Connections）] の順に移動して、関連するオプションを選択します。

ステップ 2 接続イベント テーブルを使用している場合、ファイル表示アイコン（  ）をクリックします。
ポップアップ ウィンドウが表示され、接続で検出されたファイルのリストとともに、そのタイプと、該当する場合はマルウェア処理が示されます。

ステップ 3 次の選択肢があります。

- 表示：ファイルイベントのテーブル ビューを表示するには、ファイルの表示アイコン（  ）をクリックします。
- 表示：マルウェア イベントのテーブル ビューに詳細を表示するには、マルウェア ファイルの表示アイコン（  ）をクリックします。
- 追跡：ネットワークを経由するファイルの伝送を追跡するには、ファイルのトラジェクトリ アイコン（  ）をクリックします。
- 表示：接続で検出されたファイルまたはネットワーク向け AMP によって検出されたマルウェア イベントすべての詳細を表示するには、[ファイル イベントの表示（View File Events）] または [マルウェア イベントの表示（View Malware Events）] をクリックします。

接続に関連付けられた侵入イベントの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Any Security Analyst

アクセス コントロール ルールまたはデフォルト アクションに侵入ポリシーを関連付けると、システムは一致するトラフィックのエクスプロイトを検出できます。[分析（Analysis）] > [接続（Connections）] メニュー オプションを使用して、ロギングされた接続と関連付けられている侵入イベント（存在する場合）、およびそれらのイベントの優先順位と影響を確認します。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

ステップ 1 [分析（Analysis）] > [接続（Connections）] の順に移動して、関連するオプションを選択します。

ステップ 2 接続イベント テーブルを使用する場合、[侵入イベント（Intrusion Events）] カラムの侵入イベント アイコン（  ）をクリックします。

ステップ 3 表示されるポップアップ ウィンドウで、以下のオプションを選択できます。

- パケット ビューで詳細を表示するには、リストされたイベントの表示アイコン（  ）をクリックします。
- [侵入イベントの表示（View Intrusion Events）] をクリックして、接続に関連付けられた侵入イベントすべての詳細を表示します。

暗号化接続の証明書の詳細

[分析（Analysis）]> [接続（Connections）] メニューを使用して、システムで処理される接続を暗号化するために使用される公開キー証明書（使用可能な場合）を表示できます。証明書には次の情報が含まれています。

表 *333* : 暗号化接続の証明書の詳細

属性	説明
Subject/Issuer Common Name	証明書のサブジェクトまたは証明書発行元のホストおよびドメイン名。
Subject/Issuer Organization	証明書のサブジェクトまたは証明書発行元の組織。
Subject/Issuer Organization Unit	証明書のサブジェクトまたは証明書発行元の部門。

属性	説明
Not Valid Before/After	証明書の有効期間。
Serial Number	発行元 CA によって割り当てられたシリアル番号。
Certificate Fingerprint	証明書の認証に使用する SHA ハッシュ値。
Public Key Fingerprint	証明書に含まれる公開キーの認証に使用する SHA ハッシュ値。

デバイス サマリー ページの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	カスタム（Custom）

[接続サマリー（Connection Summary）] ページは、接続イベントの検索によって制限されたカスタム ロールを持ち、[接続サマリー（Connection Summary）] ページへのメニュー ベースの明示的なアクセスを許可されたユーザにのみ表示されます。このページは、監視対象ネットワーク上のアクティビティをさまざまな条件で整理したグラフを表示します。たとえば [一定期間の接続数（Connections over Time）] グラフでは、選択した間隔における監視対象ネットワーク上の接続の合計数が表示されます。

接続グラフでできる操作と同じことが、接続サマリーのグラフでも、ほぼすべてできます。ただし、[Connection Summary] ページのグラフは集約データに基づいているため、グラフの基になっている個々の接続イベントを調べることはできません。つまり、接続サマリーのグラフから接続データのテーブル ビューにドリルダウンすることはできません。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

ステップ 1 **[Overview]** > **[Summary]** > **[Connection Summary]**を選択します。

ステップ 2 [デバイスの選択（Select Device）] リストから、サマリーを表示したいデバイスを選択するか、もしくはすべてのデバイスのサマリーを表示するために [すべて（All）] を選択します。

ステップ 3 グラフ接続の操作および分析を行うには、接続イベント グラフの使用方法（2945 ページ）の説明に従って続行します。

ヒント デフォルトの時間範囲に影響を与えずにさらに分析を行えるように接続グラフ分離するには、[表示（View）] をクリックします。

関連トピック

ユーザ ロール エスカレーションの有効化 （84 ページ）

第 126 章

侵入イベントの操作

以下のトピックでは、侵入イベントを操作する方法について説明します。

侵入イベントについて

Firepower システムは、ホストとそのデータの可用性、整合性、および機密性に影響する可能性のあるトラフィックがないかどうか、ネットワークをモニタするのに役立ちます。主要なネットワーク セグメントに管理対象デバイスを配置すると、悪意のあるアクティビティを目的としてネットワークを通過するパケットを検査できます。このシステムには、攻撃者が開発したさまざまなエクスプロイトを検索するのに使用できるいくつかのメカニズムがあります。

システムは、潜在的な侵入を特定すると侵入イベント（古い用語で「IPS イベント」と呼ばれることもあります）を生成します。これは、エクスプロイトの日付、時間、タイプ、および攻撃元とそのターゲットに関するコンテキスト情報のデータです。パケットベースのイベントの場合、イベントをトリガーとして使用したパケットのコピーも記録されます。管理対象デバイスは、Firepower Management Centerにイベントを送信します。ここで、集約データを確認し、ネットワーク アセットに対する攻撃を的確に把握できます。

管理対象デバイスをインライン、スイッチド、またはルーテッドの侵入システムとして展開することもできます。これにより、危険だと認識したパケットをドロップまたは置換するようデバイスを設定できます。

侵入イベントの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Intrusion Admin

侵入イベントは、ネットワーク セキュリティに対する脅威があるかどうかを判断するために表示します。

初期の侵入イベント ビューは、ページにアクセスするために使用するワークフローによって異なります。1 つ以上のドリルダウン ページ、侵入イベントのテーブル ビュー、および終了パケット ビューを含む、定義済みワークフローの 1 つを使用するか、独自のワークフローを作成できます。カスタム テーブルに基づいてワークフローを表示することもできます。これには、侵入イベントを含めることができます。

大量の IP アドレスが含まれている状態で、[IP アドレスの解決（Resolve IP Addresses）] イベント ビュー設定が有効になっていると、イベント ビューの表示が遅くなる場合があります。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

ステップ 1 **[Analysis]** > **[Intrusions]** > **[Events]** を選択します。

ステップ 2 次の選択肢があります。

- 時間範囲の調整：時間枠の変更 （2956ページ）の説明に従って、イベント ビューの時間範囲を調整します。
- ワークフローの変更：侵入イベントのテーブル ビューが含まれないカスタム ワークフローを使用している場合、ワークフローのタイトルの横にある [(ワークフローの切り替え)（(switch workflow)）] をクリックして、システム提供のワークフローのいずれかを選択します。
- 制約：表示する対象を分析において重要な侵入イベントに狭めるには、侵入イベント ワークフローの使用 （3080 ページ）を参照してください。
- イベントの削除：データベースからイベントを削除するには、[削除（Delete）] をクリックして表示しているパケットのイベントを削除するか、[すべて削除（Delete All）] をクリックして以前に選択したパケットのすべてのイベントを削除します。
- 確認済みのマークを付ける：侵入イベントに確認済みのマークを付けるには、侵入イベントを確認済みとしてマーク （3074 ページ）を参照してください。
- 接続データの表示：侵入イベントに関連付けられた接続データを表示するには、侵入イベントと関連付けられた接続データの表示 （3073 ページ）を参照してください。
- 内容の表示：侵入イベント フィールド （3059ページ）の説明に従ってテーブルのカラムの内容を表示します。

関連トピック

侵入イベント パケット ビューの使用 （3084 ページ）

侵入イベントのフィールドについて

システムは、潜在的な侵入を特定すると侵入イベントを生成します。これは、エクスプロイトの日付、時間、タイプ、および攻撃元とそのターゲットに関するコンテキスト情報のデータです。パケットベースのイベントの場合、イベントをトリガーとして使用したパケットのコピーも記録されます。

侵入イベント データは [分析（Analysis）] ト> [侵入（Intrusions）] > [イベント（Events）] で Firepower Management Center Web インターフェイスでに表示できます。または外部ツールを使用して使用状況の syslog メッセージの特定のフィールドからデータをエミットします。Syslog のフィールドは下のリストに示されます。同等の syslog がリストされていないフィールドは、syslog メッセージでは使用可能できません。

侵入イベントを検索するときは、個別のイベントで利用可能な情報は、システムがいつ、なぜ、どのようにしてイベントを記録したかによって異なることに注意してください。たとえば、復号化されたトラフィックでトリガーされた侵入イベントだけが TLS/SSL 情報を含んでいます。

（注） Firepower Management Center の Web インターフェイスの侵入イベントのテーブル ビューの一部のフィールドはデフォルトで無効になっています。セッション中にフィールドを有効にするには、検索制約を拡張してから、[無効の列（Disabled Columns）] の下の列名をクリックします。

侵入イベント フィールド

[アクセス コントロール ポリシー（Access Control Policy）]（syslog：ACPolicy）

イベントを生成した侵入ルール、プリプロセッサルール、またはデコーダ ルールが有効になっている侵入ポリシーに関連付けられているアクセス コントロール ポリシー。

アクセス コントロール ルール

イベントを生成した侵入ルールを呼び出したアクセス コントロール ルール。[デフォルト アクション（Default Action）] は、ルールが有効化されている侵入ポリシーが特定のアクセス コントロール ルールに関連付けられておらず、代わりに、アクセス コントロール ポリシーのデフォルト アクションとして設定されていることを示しています。

次の場合、このフィールドは空になります。

- [関連付けられたルールなし/デフォルトアクションなし（No associated rule/default action）]：侵入インスペクションがアクセス コントロール ルールにもデフォルト アクションにも関

連付けられていない場合。たとえば、パケットがデフォルトの侵入ポリシーによって検査された場合などです。

- [関連付けられている接続イベントなし（No associated connection event）]：セッションに記録された接続イベントがデータベースから消去されている場合。たとえば、接続イベントに侵入イベントよりも高いターンオーバーがある場合などです。

[アプリケーション プロトコル（Application Protocol）]（syslog：ApplicationProtocol）

（使用可能な場合）侵入イベントをトリガーとして使用したトラフィックで検出されたホスト間の通信を表す、アプリケーション プロトコル。

アプリケーション プロトコル カテゴリとタグ（Application Protocol Category and Tag）

アプリケーションの機能を理解するのに役立つ、アプリケーションの特性を示す基準。

[アプリケーションのリスク（Application Risk）]

侵入イベントをトリガーしたトラフィックで検出されたアプリケーションに関連付けられているリスク。[非常に高い（Very High）]、[高（High）]、[中（Medium）]、[低（Low）]、および[非常に低い（Very Low）]。接続で検出されるアプリケーションのタイプごとに関連するリスクがあります。このフィールドは、それらのうち最も高いリスクを表示します。

ビジネスとの関連性（Business Relevance）

侵入イベントをトリガーしたトラフィックで検出されたアプリケーションに関連付けられているビジネスとの関連性。[非常に高い（Very High）]、[高（High）]、[中（Medium）]、[低（Low）]、および[非常に低い（Very Low）]。接続で検出されるアプリケーションのタイプごとに関連するビジネスとの関連性があります。このフィールドは、それらのうち最も低い（関連性が最も低い）ものを表示します。

[分類（Classification）]（syslog：Classification）

イベントを生成したルールが属する分類。

侵入イベント詳細 （2146 ページ）で、使用可能な分類値のリストを参照してください。

このフィールドを検索するときは、表示するイベントを生成したルールの分類番号を入力するか、分類名または説明のすべてまたは一部を入力します。また、番号、名前、または説明のカンマ区切りリストを入力することもできます。最後に、カスタム分類を追加した場合、その名前または説明のすべてまたは一部を使用して検索することもできます。

[クライアント（Client）]（syslog：Client）

（使用可能な場合）侵入イベントをトリガーとして使用したトラフィックで検出されたモニタ対象のホストで実行されているソフトウェアを表す、クライアント アプリケーション。

クライアント カテゴリとタグ（Client Category and Tag）

アプリケーションの機能を理解するのに役立つ、アプリケーションの特性を示す基準。

（Syslog のみ）

ある接続と別の同時接続を区別するカウンタ。このフィールドは、それ自体には意味がありません。

[Sensor UUID]、[First Packet Time]、[Connection Instance ID]、および [Connection Counter] フィールドの情報を総合すると、特定の侵入イベントに関連付けられた接続イベントを一意に識別できます。

（Syslog のみ）

接続イベントを処理した Snort インスタンス。このフィールドは、それ自体には意味がありません。

[Sensor UUID]、[First Packet Time]、[Connection Instance ID]、および [Connection Counter] フィールドの情報を総合すると、特定の侵入イベントに関連付けられた接続イベントを一意に識別できます。

メンバー数（Count）

各行に表示された情報と一致するイベントの数。[カウント（Count）] フィールドは、複数の同一行が生成される制限を適用した後でのみ表示されることに注意してください。このフィールドは検索できません。

CVE ID

このフィールドは検索フィールド専用です。

MITRE の Common Vulnerabilities and Exposures（CVE）データベース（https://cve.mitre.org/）の脆弱性に関連付けられた識別番号による検索。

送信先の大陸（Destination Continent）

侵入イベントに関連する受信ホストの大陸。

送信先の国（Destination Country）

侵入イベントに関連する受信ホストの国。

[宛先IP（Destination IP）]（syslog：DstIP）

侵入イベントに関連する受信ホストが使用する IP アドレス。

[宛先ポート/ICMPコード（Destination Port / ICMP Code）]（syslog：DstPort、ICMPCode）

トラフィックを受信するホストのポート番号。ICMP トラフィックの場合は、ポート番号がないため、このフィールドには ICMP コードが表示されます。

宛先ユーザ（Destination User）

宛先ホストにログインしている既知のユーザのユーザ ID。

Device

アクセス コントロール ポリシーが展開された管理対象デバイス。

スタック構成設定では、プライマリ デバイスとセカンダリ デバイスは、別々のデバイスであるかのように侵入イベントをレポートすることに注意してください。

ドメイン（Domain）

侵入を検出したデバイスのドメイン。 This field is only present if you have ever configured the Firepower Management Center for multitenancy.

[出力インターフェイス（Egress Interface）]（syslog：EgressInterface）

イベントをトリガーとして使用したパケットの出力インターフェイス。パッシブインターフェイスの場合、このインターフェイスの列には入力されません。

[出力セキュリティ ゾーン（Egress Security Zone）]：（syslog：EgressZone）

イベントをトリガーとして使用したパケットの出力セキュリティ ゾーン。パッシブ展開環境では、このセキュリティ ゾーンのフィールドには入力されません。

電子メールの添付ファイル（Email Attachments）

MIME の Content-Disposition 見出しから取得された MIME 添付ファイル名。添付ファイルの名前を表示するには、SMTP プリプロセッサの [Log MIME Attachment Names] オプションを有効にする必要があります。複数の添付ファイル名がサポートされます。

電子メールのヘッダー（Email Headers）

このフィールドは検索フィールド専用です。

電子メールのヘッダーから取得したデータ。

電子メールのヘッダーを SMTP トラフィックの侵入イベントと関連付けるには、SMTP プリプロセッサの [ヘッダーのログ（Log Headers）] オプションを有効にする必要があります。

メール受信者（Email Recipient）

SMTP RCPT TO コマンドから取得された電子メール受信者のアドレス。このフィールドの値を表示するには、SMTP プリプロセッサの [Log To Addresses] オプションを有効にする必要があります。複数の受信者アドレスがサポートされます。

メール送信者（Email Sender）

SMTP MAIL FROM コマンドから取得された電子メール送信者のアドレス。このフィールドの値を表示するには、SMTP プリプロセッサの [Log From Address] オプションを有効にする必要があります。複数の送信者アドレスがサポートされます。

（Syslog のみ）

システムが最初のパケットを検出した時間。

[Sensor UUID]、[First Packet Time]、[Connection Instance ID]、および [Connection Counter] フィールドの情報を総合すると、特定の侵入イベントに関連付けられた接続イベントを一意に識別できます。

ジェネレータ（Generator）

イベントを生成したコンポーネント。

次の侵入イベント フィールドに関する情報も参照してください。[GID]、[メッセージ（Message）]、および [Snort ID]

GID（syslog のみ）

ジェネレータ ID。イベントを生成したコンポーネントの ID。

次の侵入イベントフィールドに関する情報も参照してください。[ジェネレータ（Generator）]、[メッセージ（Message）]、および [Snort ID]

HTTP ホスト名（HTTP Hostname）

HTTP 要求のホスト見出しから取得されたホスト名（存在する場合）。要求パケットにホスト名が常に含まれているわけではないことに注意してください。

ホスト名を HTTP クライアント トラフィックの侵入イベントと関連付けるには、HTTP 検査プリプロセッサの [ホスト名のログ（Log Headers）] オプションを有効にする必要があります。

テーブル ビューで、この列には、取得されたホスト名の最初の 50 文字が表示されます。ホストの省略名の表示部分にポインタを合わせると、最大 256 バイトまでの完全な名前を表示することができます。また、最大 256 バイトまでの完全なホスト名をパケット ビューに表示することもできます。

[HTTP 応答コード（HTTP Response Code）]（syslog：HTTPResponse）

イベントをトリガーした接続を介してクライアントの HTTP 要求に応答して送信される HTTP ステータス コード。

HTTP URI

（存在する場合）侵入イベントをトリガーとして使用した HTTP 要求パケットに関連付けられた raw URI。要求パケットに URI が常に含まれているわけではないことに注意してください。

URI を HTTP クライアント トラフィックの侵入イベントと関連付けるには、HTTP 検査プリプロセッサの [URI のログ（Log URI）] オプションを有効にする必要があります。

HTTP 応答によってトリガーとして使用された侵入イベントの関連 HTTP URI を参照するには、[両方のポートでのストリーム再構成の実行（Perform Stream Reassembly on Both Ports）] オプションに HTTP サーバのポートを設定する必要があります。ただし、これにより、トラフィックのリアセンブル用のリソース要求が増加することに注意してください。

この列には、取得された URI の最初の 50 文字が表示されます。省略 URI の表示部分にポインタを合わせると、最大 2048 バイトまでの完全な URI を表示することができます。また、最大 2048 バイトまでの完全な URI をパケット ビューに表示することもできます。

Impact

このフィールドの影響レベルは、侵入データ、ネットワーク検出データ、脆弱性情報との関係を示します。

このフィールドを検索するときは、影響アイコンの色または一部の文字列を指定しないでください。たとえば、**blue**、**level 1**、または **0** を使用しないでください。有効な大文字と小文字を区別しない値は次のとおりです。

- Impact 0、Impact Level 0
- Impact 1、Impact Level 1
- Impact 2、Impact Level 2
- Impact 3、Impact Level 3
- Impact 4、Impact Level 4

NetFlowデータからネットワーク マップに追加されたホストに使用可能なオペレーティング システムの情報はないので、システムは、それらのホストに作用する侵入イベントに対し脆弱な（インパクト レベル1：赤）インパクト レベルを割り当てることができません。このような場合は、ホスト入力機能を使用して、ホストのオペレーティング システム ID を手動で設定します。

入力インターフェイス (Syslog：IngressInterface)

イベントをトリガーとして使用したパケットの入力インターフェイス。パッシブ インターフェイスの場合、このインターフェイスの列だけに入力されます。

[入力セキュリティ ゾーン（Ingress Security Zone）]：（syslog：IngressZone）

イベントをトリガーとして使用したパケットの入力セキュリティ ゾーンまたはトンネル ゾーン。パッシブ展開環境では、このセキュリティ ゾーン フィールドだけに入力されます。

[インライン結果（Inline Result）]（syslog：InlineResult）

ワークフローとテーブル ビューでは、このフィールドには次のいずれかが表示されます。

表 *334*：ワークフロー ビューとテーブル ビューの *[インライン結果（Inline Result）]* フィールドの内容

アイコン	意味
黒の下矢印	ルールをトリガーとして使用したパケットをシステムがドロップしました

アイコン	意味
グレーの下矢印	[インライン時にドロップ（Drop when Inline）] 侵入ポリシー オプション（インライン展開環境）を有効にした場合、またはシステムがプルーニングしている間に [ドロップしてイベントを生成する（Drop and Generate）] ルールがイベントを生成した場合、IPS がパケットをドロップしたことを示します
アイコンなし（空白）	トリガーされたルールは [ドロップしてイベントを生成する（Drop and Generate Events）] に設定されていませんでした

パッシブ展開では、侵入ポリシーのルールの状態やインライン ドロップ動作に関係なく、インライン インターフェイスがタップ モードの場合を含めて、システムはパケットをドロップしません。

このフィールドを検索するときは、次のいずれかを入力します。

- **dropped**：パケットがインライン展開環境でパケットをドロップするかどうかを指定します
- **would have dropped**：インライン展開環境でパケットをドロップするように侵入ポリシーが設定されている場合に、パケットをドロップするかどうかを指定します

[侵入ポリシー（Intrusion Policy）]（syslog：IntrusionPolicy）

イベントを生成した侵入ルール、プリプロセッサ ルール、またはデコーダ ルールが有効にされた侵入ポリシー。アクセス コントロール ポリシーのデフォルト アクションとして侵入ポリシーを選択するか、アクセス コントロール ルールと侵入ポリシーを関連付けることができます。

IOC（syslog：NumIOC）

侵入イベントをトリガーとして使用したトラフィックが、接続に関係するホストに対する侵入の痕跡（IOC）もトリガーとして使用したかどうか。

このフィールドを検索するときは、**triggered** または **n/a** を指定します。

[メッセージ（Message）]（syslog：Message）

イベントを説明するテキスト。ルールベースの侵入イベントの場合、イベント メッセージはルールから取得されます。デコーダベースおよびプリプロセッサベースのイベントの場合は、イベント メッセージはハードコーディングされています。

ジェネレータおよび Snort ID（GID と SID）と SID バージョン（改訂）はカッコで囲んだコロン区切りの数字形式で各メッセージの末尾に付加されます（GID:SID:version）。例：**(1:36330:2)**。

[MPLS ラベル（MPLS Label）]（syslog：MPLS_Label）

侵入イベントをトリガーしたパケットと関連付けられているマルチプロトコル ラベル スイッチング ラベル。

[ネットワーク分析ポリシー（Network Analysis Policy）]（syslog：NAPPolicy）

イベントの生成に関連付けられているネットワーク分析ポリシー（ある場合）。

このフィールドには、取得された URI の最初の 50 文字が表示されます。省略 URI の表示部分にポインタを合わせると、最大 2048 バイトまでの完全な URI を表示することができます。また、最大 2048 バイトまでの完全な URI をパケット ビューに表示することもできます。

クライアントのオリジナル IP（Original Client IP）

X-Forwarded-For（XFF）、True-Client-IP、またはカスタム定義の HTTP ヘッダーから取得された、元のクライアント IP アドレス。

このフィールドの値を表示するには、ネットワーク解析ポリシーで HTTP プリプロセッサ [元のクライアント IP アドレスの抽出（Extract Original Client IP Address）] オプションを有効にする必要があります。オプションで、ネットワーク解析ポリシーの同じエリアで、最大 6 つのカスタム クライアント IP 見出しを指定し、システムが [クライアントのオリジナル IP（Original Client IP）] イベント フィールドの値を選択する優先順位を設定します。

[優先度（Priority）]（syslog：Priority）

Cisco Talos Intelligence Group（Talos） で指定されたイベントの優先度。優先度は、`priority` キーワードの値または `classtype` キーワードの値に対応します。その他の侵入イベントの場合、プライオリティはデコーダまたはプリプロセッサによって決定されます。有効な値は、[高（high）]、[中（medium）]、および [低（low）] です。

[プロトコル（Protocol）]（syslog：Protocol）

Firepower Management Center の Web インターフェイスでは、このフィールドは検索フィールド専用です。

http://www.iana.org/assignments/protocol-numbers に一覧表示されている、接続で使用するトランスポート プロトコルの名前または番号。これは、送信元および宛先ポート/ICMP の列と関連付けられたプロトコルです。

確認者（Reviewed By）

イベントを確認したユーザの名前。このフィールドを検索するときは、**`unreviewed`** と入力すると、まだ確認されていないイベントを検索できます。

Revision（syslog のみ）

イベントの生成に使用された署名のバージョン。

次の侵入イベント フィールドに関する情報も参照してください。[ジェネレータ（Generator）]、[GID]、[メッセージ（Message）]、[SID]、および [Snort ID]

[セキュリティ コンテキスト（Security Context）]（syslog：Context）

トラフィックが通過した仮想ファイアウォール グループを識別するメタデータ。システムがこのフィールドにデータを設定するのは、マルチ コンテキスト モードの ASA FirePOWER だけです。

（Syslog のみ）

イベントを生成した Firepower デバイスの一意の識別子。

[Sensor UUID]、[First Packet Time]、[Connection Instance ID]、および [Connection Counter] フィールドの情報を総合すると、特定の侵入イベントに関連付けられた接続イベントを一意に識別できます。

SID（syslog のみ）

イベントを生成したルールの署名 ID（Snort ID ともいう）

次の侵入イベントフィールドに関する情報も参照してください。[ジェネレータ（Generator）]、[GID]、[メッセージ（Message）]、[改訂（Revision）]、および [Snort ID]

Snort ID

このフィールドは検索フィールド専用です。

（syslog フィールドについては、SID を参照してください。）

検索の実行時：イベントを生成したルールの [Snort ID]（SID）を指定するか、オプションで、ルールの複合ジェネレータ ID（GID）および SID を指定します。ここで、GID および SID は、コロン（:）で区切られ、GID:SID の形式になります。次の表の任意の値を指定できます。

表 *335 : [Snort ID]* 検索値

値	例
単一の SID	10000
SID の範囲	10000-11000
SID より大きい	>10000
SID 以上	>=10000
SID 未満	<10000
SID 以下	<=10000
SID のコンマ区切りリスト	10000,11000,12000
単一の GID:SID の組み合わせ	1:10000
GID:SID の組み合わせのコンマ区切りリスト	1:10000,1:11000,1:12000

値	例
SID および GID:SID の組み合わせのコンマ区切りリスト	10000,1:11000,12000

表示しているイベントの SID が [メッセージ（Message）] 列に表示されます。詳細については、この項の [メッセージ（Message）] フィールドについての説明を参照してください。

ソースの大陸（Source Continent）

侵入イベントに関連する送信ホストのある大陸。

ソースの国（Source Country）

侵入イベントに関連する送信ホストのある国。

[送信元 IP（Source IP）]（syslog：SrcIP）

侵入イベントに関連する送信ホストが使用する IP アドレス。

[送信元ポート/ICMP タイプ（Source Port/ICMP Type）]（syslog：SrcPort、ICMPType）

送信元ホストのポート番号。ICMP トラフィックの場合は、ポート番号がないため、このフィールドには ICMP タイプが表示されます。

[送信元ユーザ（Source User）]（syslog：User）

送信元ホストにログインしている既知のユーザのユーザ ID。

SSL Actual Action (Syslog: SSLActualAction)

In the Firepower Management Center web interface, this field is a search field only.

システムが暗号化されたトラフィックに適用したアクション。

[ブロック（Block）/リセットしてブロック（Block With Reset）]

ブロックされた暗号化接続を表します。

[復号（再署名）（Decrypt (Resign)）]

再署名サーバ証明書を使用して復号された発信接続を表します。

[復号（キーの交換）（Decrypt (Replace Key)）]

置き換えられた公開キーと自己署名サーバ証明書を使用して復号化された発信接続を表します。

[復号（既知のキー）（Decrypt (Known Key)）]

既知の秘密キーを使用して復号化された着信接続を表します。

[デフォルトアクション（Default Action）]

接続がデフォルト アクションによって処理されたことを示します。

[復号しない（Do not Decrypt）]

システムが復号化しなかった接続を表します。

フィールド値は、検索ワークフロー ページの [SSL ステータス（SSL Status）] フィールドに表示されます。

[SSL 証明書情報（SSL Certificate Information）]

このフィールドは検索フィールド専用です。

トラフィックを暗号化するための公開キー証明書に保存される次の情報：

- サブジェクト/発行元共通名（Subject/Issuer Common Name）
- サブジェクト/発行元組織（Subject/Issuer Organization）
- サブジェクト/発行元組織単位（Subject/Issuer Organization Unit）
- 有効期間（Not Valid Before/After）
- シリアル番号（Serial Number）
- 証明書フィンガープリント（Certificate Fingerprint）
- 公開キー フィンガープリント（Public Key Fingerprint）

SSL 失敗理由（SSL Failure Reason）

このフィールドは検索フィールド専用です。

システムが暗号化されたトラフィックの復号化に失敗した理由。

- 不明
- No Match
- Success
- Uncached Session
- 不明な暗号スイート
- サポートされていない暗号スイート
- Unsupported SSL Version
- SSL Compression Used
- Session Undecryptable in Passive Mode
- Handshake Error
- Decryption Error
- Pending Server Name Category Lookup
- Pending Common Name Category Lookup

- Internal Error
- Network Parameters Unavailable
- Invalid Server Certificate Handle
- Server Certificate Fingerprint Unavailable
- Cannot Cache Subject DN
- Cannot Cache Issuer DN
- Unknown SSL Version
- External Certificate List Unavailable
- External Certificate Fingerprint Unavailable
- Internal Certificate List Invalid
- Internal Certificate List Unavailable
- Internal Certificate Unavailable
- Internal Certificate Fingerprint Unavailable
- Server Certificate Validation Unavailable
- Server Certificate Validation Failure
- 無効なアクション（Invalid Action）

フィールド値は、検索ワークフローのページの [SSL ステータス（SSL Status）] フィールドに表示されます。

SSL ステータス（SSL Status）

暗号化接続をログに記録した [SSL の実際のアクション（SSL Actual Action）]（SSL ルール、デフォルトのアクション、または復号化できないトラフィック アクション）に関連付けられているアクション。

システムが暗号化接続を復号できなかった場合は、[SSL の実際の動作（SSL Actual Action）]（実行された復号不能のトラフィック アクション）と、[SSL 失敗理由（SSL Failure Reason）] が表示されます。たとえば、不明な暗号スイートによって暗号化されたトラフィックをシステムが検出し、それ以上のインスペクションをせずにこれを許可した場合、このフィールドには [Do Not Decrypt (Unknown Cipher Suite)] が表示されます。

証明書の詳細を表示するにはロック アイコン（  ）をクリックします。

このフィールドを検索する場合は、[SSL の実際の動作（SSL Actual Action）] と [SSL 失敗理由（SSL Failure Reason）] の 1 つ以上の値を入力することで、システムが処理した、または復号に失敗した暗号化トラフィックが表示されます。

[SSL サブジェクト/発行元国（SSL Subject/Issuer Country）]

このフィールドは検索フィールド専用です。

暗号化証明書に関連付けられている件名または発行者の国に関する 2 文字の ISO 3166-1 アルファ 2 国コード。

時刻（Time）

イベントの日付と時刻。このフィールドは検索できません。

[VLAN ID]（syslog：VLAN_ID）

侵入イベントをトリガーとして使用したパケットと関連付けられた最内部 VLAN ID。

[Web アプリケーション（Web Application）]（syslog：WebApplication）

侵入イベントをトリガーとして使用したトラフィックで検出された HTTP トラフィックの内容または要求された URL を表す、Web アプリケーション。

システムが HTTP のアプリケーション プロトコルを検出し、特定の Web アプリケーションを検出できなかった場合、システムは代わりに一般的な Web ブラウジング指定を提供します。

Web アプリケーションのカテゴリとタグ（Web Application Category and Tag）

アプリケーションの機能を理解するのに役立つ、アプリケーションの特性を示す基準。

関連トピック

イベントの検索 （2967 ページ）

侵入イベント影響レベル

イベントがネットワークに与える影響を評価するために、Firepower Management Center は侵入イベントのテーブル ビューに影響レベルを表示します。イベントごとに、システムは影響レベルアイコンを追加し、侵入データ、ネットワーク検出データ、脆弱性情報との関係を色で示します。

（注） NetFlow データからネットワーク マップに追加されたホストに使用可能なオペレーティング システムの情報はないので、システムは、それらのホストに作用する侵入イベントに対し脆弱な（インパクト レベル 1：赤）インパクト レベルを割り当てることができません。このような場合は、ホスト入力機能を使用して、ホストのオペレーティング システム ID を手動で設定します。

次の表に、影響レベルで使用可能な値を示します。

表 *336 :* 影響レベル

影響レベル	脆弱性	色	説明
0	Unknown	グレー	送信元ホストと宛先ホストは両方ともネットワーク検出によってモニタされているネットワーク上に存在しません。
1	脆弱	レッド	次のいずれかを行います。 • 送信元ホストまたは宛先ホストはネットワーク マップ内にあり、脆弱性はホストにマッピングされます • 送信元ホストまたは宛先ホストは、ウイルス、トロイの木馬、または他の悪意のあるソフトウェアによって侵害される可能性があります。
2	潜在的に脆弱	オレンジ	送信元ホストまたは宛先ホストはネットワーク マップ内にあり、次のいずれかに当てはまります。 • ポート指向のトラフィックの場合、ポートはサーバ アプリケーション プロトコルを実行しています • ポート指向ではないトラフィックの場合、ホストはプロトコルを使用します

影響レベル	脆弱性	色	説明
3	現在は脆弱ではない	黄色	送信元ホストまたは宛先ホストはネットワーク マップ内にあり、次のいずれかに当てはまります。 • ポート指向のトラフィック（たとえば、TCP または UDP）の場合、ポートが開いていません • ポート指向ではないトラフィック（たとえば、ICMP）の場合、ホストはプロトコルを使用しません
4	不明なターゲット	ブルー	送信元ホストまたは宛先ホストがモニタ対象のネットワークにありますが、ネットワーク マップ内にそのホストのエントリがありません。

侵入イベントと関連付けられた接続データの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Intrusion Admin

システムは、侵入イベントが検出された接続を記録できます。このロギングは、アクセス コントロール ルールに関連付けられている侵入ポリシーに対して自動的に行われますが、デフォルト アクションに関連する接続データを参照するには、接続ロギングを手動で有効にする必要があります。

関連データの表示は、イベントのテーブル ビュー間を移動する場合に非常に役立ちます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

ステップ 1 **[Analysis]** > **[Intrusions]** > **[Events]**を選択します。

ステップ 2 テーブルのチェックボックスを使用して侵入イベントを選択してから、[ジャンプ（Jump to）] ドロップダウン リストから [接続（Connections）] を選択します。

ヒント　同じ方法で、特定の接続に関連した侵入イベントを表示できます。詳細については、「ワークフロー間のナビゲーション （2963 ページ）」を参照してください。

関連トピック

許可された接続のロギング （3008 ページ）
侵入イベント ワークフローの使用 （3080 ページ）
接続およびセキュリティ インテリジェンス イベント テーブルの使用 （3050 ページ）

侵入イベントを確認済みとしてマーク

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Intrusion Admin

侵入イベントが悪意のあるものではないことがわかったら、そのイベントを確認済みとしてマークできます。

侵入イベントを調べて、そのイベントがネットワーク セキュリティに対して脅威ではないことがわかったら（たとえば、ネットワーク上のどのホストも検出されたエクスプロイトに対して脆弱でないことがわかっているなど）、そのイベントを確認済みとしてマークできます。確認済みのイベントはイベント データベースに保存され、イベント要約統計に含まれますが、デフォルトの侵入イベントページには表示されなくなります。自分の名前がレビューアとして表示されます。

マルチドメイン展開では、イベントに確認済みのマークを付けると、そのイベントを表示可能なすべてのドメインでシステムによってイベントに確認済みのマークが付けられます。

バックアップを実行してから確認済みの侵入イベントビューを削除した場合、バックアップを復元すると、削除された侵入イベント ビューは復元されますが、確認済みのステータスは復元されません。こうして復元された侵入イベントは、[確認済みイベント（Reviewed Events）] の下ではなく [侵入イベント（Intrusion Events）] の下に表示されます。

侵入イベントが表示されるページで、次の 2 つの方法を選択できます。

- イベントのリストから 1 つまたは複数の侵入イベントにマークを付けるには、イベントの横にあるチェックボックスをオンにして、[レビュー（Review）] をクリックします。
- イベントのリストからすべての侵入イベントにマークを付けるには、[すべて確認（Review All）] をクリックします。

関連トピック

侵入イベント ワークフローの使用 （3080 ページ）

以前に確認された侵入イベントの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Intrusion Admin

マルチドメイン展開では、イベントに確認済みのマークを付けると、そのイベントを表示可能なすべてのドメインでシステムによってイベントに確認済みのマークが付けられます。

ステップ 1 **[Analysis]** > **[Intrusions]** > **[Reviewed Events]**を選択します。

ステップ 2 次の選択肢があります。

- 時間枠の変更 （2956 ページ）の説明に従って、時間範囲を調整します。
- 侵入イベントのテーブル ビューが含まれないカスタム ワークフローを使用している場合、ワークフローのタイトルの横にある [(ワークフローの切り替え)（(switch workflow)）] をクリックして、システム提供のワークフローのいずれかを選択します。
- 表示されるイベントの詳細については、侵入イベント フィールド（3059ページ）を参照してください。

関連トピック

侵入イベント ワークフローの使用 （3080 ページ）

侵入イベントへの未確認としてマーク

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Intrusion Admin

イベントに未確認のマークを付けることで、確認済みイベントをデフォルトの侵入イベント ビューに戻すことができます。

マルチドメイン展開では、イベントに確認済みのマークを付けると、そのイベントを表示可能なすべてのドメインでシステムによってイベントに確認済みのマークが付けられます。

確認済みイベントが表示されるページで、次の 2 つの方法を選択できます。

- 確認済みイベント リストから個別の侵入イベントを削除するには、特定のイベントの横にあるチェックボックスをオンにして、[未確認（Unreview）] をクリックします。

- 確認済みイベント リストからすべての侵入イベントを削除するには、[すべて未確認（Unreview All）] をクリックします。

プリプロセッサ イベント

プリプロセッサが提供する機能は2つあります。1つは、パケットに対して指定されたアクション（HTTP トラフィックを復号して正規化するなど）を実行する機能、もう 1 つは、パケットが特定のプリプロセッサ オプションをトリガーしたときに関連するプリプロセッサ ルールが有効にされている場合は常にイベントを生成することで、指定のプリプロセッサ オプションの実行を報告するという機能です。たとえば、プリプロセッサが IIS の二重にエンコードされたトラフィックを検出した場合にイベントが生成されるようにするには、HTTP Inspect の [二重エンコード（Double Encoding）] オプションと、HTTP Inspect Generator（GID）119 および [Snort ID]（SID）2 が設定された関連するプリプロセッサ ルールを有効にします。

プリプロセッサの実行を報告するイベントを生成すると、異常なプロトコルエクスプロイトを検出するのに役立ちます。たとえば、攻撃者は、ホスト上で DoS 攻撃を引き起こす重複 IP フラグメントを細工することがあります。IP 最適化プリプロセッサはこのタイプの攻撃を検出し、それに関する侵入イベントを生成できます。

プリプロセッサ イベントは、パケット ディスプレイにイベントの詳細なルールの説明が表示されないという点で、ルール イベントとは異なります。代わりに、パケット ディスプレイには、イベント メッセージ、GID、SID、パケット ヘッダー データおよびパケット ペイロードが表示されます。これにより、パケットのヘッダー情報を分析し、そのヘッダー オプションが使用中であるかをどうか判断して、それがシステムをエクスプロイトする可能性がある場合は、パケット ペイロードを検査できます。プリプロセッサによる各パケットの分析が完了すると、ルール エンジンは、その結果に応じて適切なルールを実行し（プリプロセッサが各パケットを最適化し、有効なセッションの一部として確立できた場合）、潜在的なコンテンツ レベルの脅威についてさらに分析を行い、それらのパケットについて報告します。

プリプロセッサのジェネレータ ID

各プリプロセッサには、独自のジェネレータ ID 番号（GID）があり、これはパケットによってトリガーとして使用されたプリプロセッサを示します。一部のプリプロセッサは関連した SID もあり、これは潜在的攻撃を分類する ID 番号です。ルールの（[Snort ID]SID）が、ルールをトリガーとして使用するパケットのコンテキストを提供できる方法とほぼ同じで、この ID 番号によりイベントのタイプを分類することによって、イベントをより効率的に分析するのに役立ちます。侵入ポリシー ルールのページのプリプロセッサ フィルター グループのプリプロセッサごとにプリプロセッサ ルールをリストできます。また、プリプロセッサのプリプロセッサ ルールとカテゴリ フィルター グループのパケット デコーダ サブグループをリストできます。

（注） 標準テキスト ルールによって生成されるイベントは、ジェネレータ ID が 1（グローバル ドメインまたはレガシー GID）または 1000 ～ 2000（子孫ドメイン）です。共有オブジェクト ルールの場合、イベントのジェネレータ ID は 3 です。どちらの場合も、トリガーした特定のルールがイベントの SID に示されます。

次の表では、各 GID を生成するイベントのタイプについて説明します。

表 *337:* ジェネレータ *ID*

ID	コンポーネント	説明
1	標準的なテキストルール	パケットが標準テキスト ルールをトリガーとして使用したときにイベントが生成されました（グローバル ドメインまたはレガシー GID）。
2	タグ付きパケット	タグ付きセッションからパケットを生成するタグ ジェネレータによって、イベントが生成されました。これは、`tag` ルール オプションが使用される場合に発生します。
3	共有オブジェクト ルール	パケットが共有オブジェクト ルールをトリガーとして使用したときにイベントが生成されました。
102	HTTP デコーダ	デコーダ エンジンが、パケット内の HTTP データを復号化しました。
105	Back Orifice ディテクタ	Back Orifice ディテクタが、パケットに関連付けられた Back Orifice 攻撃を特定しました。
106	RPC デコーダ	RPC デコーダがパケットを復号化しました。
116	パケット デコーダ	パケット デコーダによってイベントが生成されました。
119、120	HTTP Inspect プリプロセッサ	HTTP Inspect プリプロセッサによってイベントが生成されました。GID 120 ルールは、サーバ固有の HTTP トラフィックに関するルールです。
122	ポートスキャン ディテクタ	ポートスキャン フロー ディテクタによってイベントが生成されました。

ID	コンポーネント	説明
123	IP デフラグメンタ	断片化されたIPデータグラムを適切に再構成できなかったときに、イベントが生成されました。
124	SMTP デコーダ	SMTP プリプロセッサが SMTP バーブに対するエクスプロイトを検出したときに、イベントが生成されました。
125	FTP デコーダ	FTP/Telnet デコーダが FTP トラフィック内でエクスプロイトを検出したときに、イベントが生成されました。
126	Telnet デコーダ	FTP/Telnet デコーダが Telnet トラフィック内でエクスプロイトを検出したときに、イベントが生成されました。
128	SSH プリプロセッサ	SSH プリプロセッサが SSH トラフィック内でエクスプロイトを検出したときに、イベントが生成されました。
129	ストリーム プリプロセッサ	ストリームプリプロセッサによるストリームの前処理中に、イベントが生成されました。
131	DNSプリプロセッサ	DNS プリプロセッサによってイベントが生成されました。
133	DCE/RPC プリプロセッサ	このイベントは、DCE/RPC プリプロセッサにより生成されました。
134	ルール遅延 パケット遅延	ルール遅延によって侵入ルールのグループが中断された（134:1）または再有効化された（134:2）とき、あるいはパケット遅延しきい値が超過したために、システムがパケットの検査を停止したとき（134:3）に、イベントが生成されました。
135	レートベースの攻撃ディテクタ	レートベースの攻撃ディテクタがネットワークのホストに対する過度の識別したときに、イベントが生成されました。
137	SSL プリプロセッサ	TLS/SSL プリプロセッサによってイベントが生成されました。

ID	コンポーネント	説明
138、139	機密データ プリプロセッサ	機密データ プリプロセッサによってイベントが生成されました。
140	SIP プリプロセッサ	SIP プリプロセッサによってイベントが生成されました。
141	IMAP プリプロセッサ	IMAP プリプロセッサによってイベントが生成されました。
142	POP プリプロセッサ	POP プリプロセッサによってイベントが生成されました。
143	GTP プリプロセッサ	GTP プリプロセッサによってイベントが生成されました。
144	Modbus プリプロセッサ	Modbus SCADA プリプロセッサによってイベントが生成されました。
145	DNP3 プリプロセッサ	DNP3 SCADA プリプロセッサによってイベントが生成されました。
1000～2000	標準的なテキストルール	パケットが標準テキストルールをトリガーとして使用したときにイベントが生成されました（子孫ドメイン）。

侵入イベントのワークフロー ページ

現在の侵入ポリシーで有効になっているプリプロセッサ、デコーダ、および侵入ルールは、モニタしているトラフィックがポリシーに違反するたびに、侵入イベントを生成します。

Firepower システムは、侵入イベントの表示および分析に使用できる、イベント データが入力された定義済みワークフローのセットを提供します。これらのワークフローは、評価する侵入イベントの特定に役立つ一連のページを表示して手順を示します。

定義済みの侵入イベントのワークフローには、次の 3 種類のページまたはイベント ビューがあります。

- 1 つ以上のドリルダウン ページ
- 侵入イベントのテーブル ビュー
- パケット ビュー

ドリルダウン ページには通常、1 つの特定の種類の情報を表示できるように 1 つのテーブル（一部のドリルダウン ビューでは複数のテーブル）に 2 つ以上の列が含まれます。

「ドリルダウン」して1つ以上の宛先ポートの詳細情報を検索すると、これらのイベントは自動的に選択され、ワークフローの次のページが表示されます。このように、ドリルダウンテーブルを使用すると、一度に分析するイベントの数を減らすことができます。

侵入イベントの最初のテーブル ビューでは、各侵入イベントが独自の行にリストされます。テーブルの列には、時間、発信元 IP アドレスおよびポート、宛先 IP アドレスおよびポート、イベントの優先度、イベント メッセージなどの情報が示されます。

イベントを選択してワークフローの次のページを表示する代わりに、テーブル ビューでイベントを選択した場合、イベントはいわゆる制約に追加されます。制約とは、分析するイベントの種類に加える制限のことです。

たとえば、任意の列で列のクローズ アイコン（✖）をクリックして、ドロップダウン リストから [Time] をクリアすると、[Time] を列の 1 つとして削除できます。分析内でイベントのリストを絞り込むには、テーブル ビューの行のいずれかの値のリンクをクリックします。たとえば、分析を送信元 IP アドレスの 1 つ（おそらく、潜在的な攻撃者）から生成されたイベントに制限するには、[Source IP Address] 列の IP アドレスをクリックします。

テーブル ビューの 1 つまたは複数の行を選択し、[表示（View）] をクリックすると、パケット ビューが表示されます。パケット ビューは、ルールをトリガーとして使用したパケットまたはイベントを生成したプリプロセッサに関する情報を提供します。パケット ビューの各セクションには、パケット内の特定の層についての情報が含まれます。折りたたまれたセクションを展開すると、より多くの情報を参照できます。

（注） それぞれのポートスキャン イベントは複数のパケットによってトリガーとして使用されるため、ポートスキャン イベントは特別なバージョンのパケット ビューを使用します。

事前定義済みのワークフローが特定のニーズに合致しない場合は、必要な情報だけを表示するカスタム ワークフローを作成できます。カスタム侵入イベントのワークフローには、ドリルダウン ページ、イベントのテーブル ビュー、またはその両方を含めることができます。システムはパケット ビューを最後のページとして自動的に組み込みます。イベントを調査する方法に応じて、定義済みワークフローと独自のカスタム ワークフローを簡単に切り替えることができます。

侵入イベント ワークフローの使用

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Intrusion Admin

イベントのドリルダウン ビューとテーブル ビューは、イベントのリストを絞り込み、関連するイベントのグループに分析を集中するために使用できる共通機能を共有します。

別のワークフローページで同じ侵入イベントを表示しないようにするため、ページの下部にあるリンクをクリックして別のページのイベントを表示すると時間範囲は一時停止し、クリックして後続のページでその他のアクションを実行すると再開します。

ヒント プロセスの任意の時点で、制約を検索条件のセットとして保存できます。たとえば、ネットワークが数日にわたり単一の IP アドレスから攻撃者によって探られていることに気付いた場合、調査中に制約をいったん保存し、後で使用することができます。ただし、複合制約を検索条件のセットとして保存することはできません。

ステップ 1 **[Analysis]** > **[Intrusions]** > **[Events]** を使用して侵入イベント ワークフローにアクセスします。

ステップ 2 オプションで、侵入イベント ドリルダウン ページの制約 （3083 ページ）または侵入イベント テーブル ビューの制約 （3084 ページ）の説明に従って、イベント ビューに表示される侵入イベントの数を制限します。

ステップ 3 次の選択肢があります。

- 表示されるカラムの詳細については、侵入イベント フィールド （3059 ページ）を参照してください。
- ホストのプロファイルを表示するには、ホスト IP アドレスの横に表示されるホスト プロファイル アイコン（  ）をクリックします。
- 地理位置情報の詳細を表示するには、[送信元の国（Source Country）] または [宛先の国（Destination Country）] カラムに表示されるフラグ アイコンをクリックします。
- （所属する組織でイベント データを外部の Firepower システムに保存している場合）パケットや履歴データなど、イベントに関連する情報を調査するには、イベントの値を右クリックします。表示されるオプションは、データタイプやシステムに設定されている統合によって異なります。詳細については、を使用したイベント調査 Cisco Security Packet Analyzer （2882 ページ）およびWeb ベースのリソースを使用したイベントの調査 （2890 ページ）を参照してください。
- イベントに関する一般的なインテリジェンスを収集するには、テーブルでイベントの値を右クリックして、シスコまたはサードパーティのインテリジェンス ソースを選択します。たとえば、不審な IP アドレスに関する詳細情報を Cisco Talos から入手できます。表示されるオプションは、データタイプやシステムに設定されている統合によって異なります。詳細については、Web ベースのリソースを使用したイベントの調査 （2890 ページ）を参照してください。
- 表示されたイベントの時刻と日付の範囲を変更するには、時間枠の変更 （2956 ページ）を参照してください。

  ヒント 侵入イベントがイベント ビューに表示されない場合、指定した時間範囲を調整すると、結果が返される場合があります。古い時間範囲を指定した場合、その時間範囲内のイベントが削除されることがあります。ルールのしきい値の設定を調整すると、イベントが生成される場合があります。

（注） イベント ビューを時間によって制約している場合は、（グローバルかイベント固有かに関係なく）アプライアンスに設定されている時間枠の外で生成されたイベントがイベント ビューに表示されます。アプライアンスに対してスライドする時間枠を設定した場合でも、この状況が発生することがあります。

- 現在のワークフローページのイベントをソートする、または現在のワークフローページ内で移動するには、ワークフローの使用 （2931 ページ）を参照してください。
- 現在の制約を維持しながら現在のワークフローのページ間で移動するには、ワークフロー ページの左上にある該当するページ リンクをクリックします。
- 後でインシデントにイベントを転送できるように、クリップボードにイベントを追加するには、[コピー（Copy）] または [すべてコピー（Copy All）] をクリックします。
- イベント データベースからイベントを削除するには、削除するイベントの横にあるチェックボックスをオンにし、[削除（Delete）] または [すべて削除（Delete All）] をクリックします。
- イベントに確認済みのマークを付けて、侵入イベントのページからそれらを削除し、イベント データベースからは削除しないようにするには、侵入イベントを確認済みとしてマーク （3074 ページ）を参照してください。
- 選択したイベントをトリガーしたパケットのローカル コピー（libpcap 形式のパケット キャプチャ ファイル）をダウンロードするには、ダウンロードするパケットによってトリガーされたイベントの横にあるチェックボックスをオンにして、[パケットのダウンロード（Download Packets）] または [すべてのパケットのダウンロード（Download All Packets）] をクリックします。キャプチャされたパケットは libpcap 形式で保存されます。この形式は、複数の一般的なプロトコル アナライザで使用されます。
- 他のイベント ビューに移動して関連イベントを表示するには、ワークフロー間のナビゲーション （2963 ページ）を参照してください。
- 別のワークフローを一時的に使用するには、[(ワークフローの切り替え)（(switch workflow)）] をクリックします。
- 現在のページにすぐに戻れるようにページをブックマークするには、[このページをブックマーク（Bookmark This Page）] をクリックします。
- [サマリー ダッシュボード（Summary Dashboard）] の [侵入イベント（Intrusion Events）] セクションを表示するには、[ダッシュボード（Dashboards）] をクリックします。
- ブックマークの管理ページに移動するには、[ブックマークの表示（View Bookmarks）] をクリックします。
- 現在のビューのデータに基づいてレポートを生成するには、イベント ビューからのレポート テンプレートの作成 （2780 ページ）を参照してください。

関連トピック

イベントの検索 （2967 ページ）
ブックマーク （2964 ページ）

侵入イベント ドリルダウン ページの制約

次の表では、ドリルダウン ページの使用方法について説明します。

表 *338 :* ドリルダウン ページでのイベントの制約

目的	操作
次のワークフロー ページのドリルダウンを特定の値に制約する	値をクリックします。 たとえば、[Destination Port（宛先ポート）] ワークフローで、イベントを宛先がポート 80 であるものに制約するには、[DST Port/ICMP Code] 列で [80/tcp] をクリックします。ワークフローの次のページ [Events] が表示され、ポート 80/tcp のイベントだけが含まれます。
次のワークフロー ページのドリルダウンを選択したイベントに制約する	次のワークフロー ページで表示するイベントの横にあるチェック ボックスを選択し、[View] をクリックします。 たとえば、[Destination Port（宛先ポート）] ワークフローで、イベントを宛先がポート 20/tcp および 21/tcp であるものに制約するには、それらのポートの行の横にあるチェック ボックスを選択し、[View] をクリックします。ワークフローの次のページ [イベント（Events）] が表示され、ポート 20/tcp および 21/tcp のイベントだけが含まれます。 複数の行を制約し、テーブルに複数の列が存在する場合（[数（Count）] 列を含まない）は、複合制約と呼ばれるものが作成されることに注意してください。複合制約により、必要以上のイベントを制約に含めないようにすることができます。たとえば、[Event（イベント）] と [Destination（宛先）] のワークフローを使用する場合は、最初のドリルダウン ページで選択した各行により、複合制約が作成されます。宛先 IP アドレス 10.10.10.100 のイベント 1:100 を選択し、宛先 IP アドレス 192.168.10.100 のイベント 1:200 も選択した場合、複合制約により、イベント タイプとして 1:100 を含むイベントや宛先 IP アドレスとして 192.168.10.100 を含むイベント、またはイベント タイプとして 1:200 を含むイベントや宛先 IP アドレスとして 10.10.10.100 を含むイベントが選択されないようになります。
現在の制約を保持しながら、次のワークフロー ページをドリルダウンする	[すべて表示（View All）] をクリックします。

侵入イベント テーブル ビューの制約

次の表では、テーブル ビューの使用方法について説明します。

表 *339 :* イベントのテーブル ビューでのイベントの制約

目的	操作
1 つの属性を持つイベントにビューを制約する	属性をクリックします。 たとえば、宛先がポート 80 であるイベントにビューを制約するには、[DST Port/ICMP Code] 列で [80/tcp] をクリックします。
テーブルから列を削除する	非表示にする列見出しのクローズアイコン（）をクリックします。表示されるポップアップ ウィンドウで、[適用（Apply）] をクリックします。 他のカラムを表示または非表示にするには、[適用（Apply）] をクリックする前に、該当するチェックボックスをオンまたはオフにします。無効になった列をビューに再追加するには、展開矢印（）をクリックして検索制約を拡張し、[無効の列（Disabled Columns）] の下の列名をクリックします。
1 つ以上のイベントに関連付けられたパケットを表示する	次のいずれかを行います。 • パケットを表示するイベントの横にある下矢印アイコン（）をクリックします。 • パケットを表示する 1 つ以上のイベントを選択し、ページの下部にある [表示（View）] をクリックします。 • ページの下部で、[すべて表示（View All）] をクリックして、現在の制約に一致するすべてのイベントのパケットを表示します。

侵入イベント パケット ビューの使用

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Intrusion Admin

パケット ビューは、侵入イベントを生成したルールをトリガーとして使用したパケットに関する情報を表示します。

ヒント イベントを検出するデバイスで [パケットの転送（Transfer Packet）] オプションが無効になっている場合、Firepower Management Center でのパケット ビューにはパケット情報は含まれません。

パケット ビューは、パケットがトリガーとして使用した侵入イベントに関する情報を提供することによって、イベントのタイム スタンプ、メッセージ、分類、優先度、イベントを生成したルール（イベントが標準テキスト ルールによって生成された場合）など、特定のパケットがキャプチャされた理由を示します。パケット ビューは、パケットのサイズなど、パケットに関する一般情報も表示します。

さらに、パケット ビューにはパケット内の各層（データ リンク、ネットワーク、およびトランスポート）について説明したセクションと、パケットを構成するバイトについて説明したセクションがあります。システムがパケットを復号化した場合は、復号化されたバイトを表示できます。折りたたまれたセクションを展開すると、詳細情報を参照できます。

（注） それぞれのポートスキャン イベントは複数のパケットによってトリガーとして使用されるため、ポートスキャン イベントは特別なバージョンのパケット ビューを使用します。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

ステップ 1 侵入イベント テーブル ビューの制約（3084 ページ）の説明に従って、侵入イベントのテーブル ビューで、表示するパケットを選択します。

ステップ 2 複数のイベントを選択した場合は、オプションで、ページの下部にあるページ番号を使用することによって、パケット ビューでパケットのページを切り替えることができます。

ステップ 3 次のオプションもあります。

- 調整：パケット ビューで日時範囲を変更するには、時間枠の変更（2956 ページ）を参照してください。
- クリップボード：後でイベントをインシデントに転送するためクリップボードにそのイベントを追加するには、[コピー（Copy）] をクリックして表示しているパケットのイベントをコピーするか、[すべてコピー（Copy All）] をクリックして以前に選択したパケットのすべてのイベントをコピーします。
- 設定：イベントをトリガした侵入ルールを設定するには、[アクション（Actions）] の横にある矢印をクリックし、パケット ビュー内での侵入ルールの設定（3090 ページ）の説明に従って操作を続けます。
- 削除：データベースからイベントを削除するには、[削除（Delete）] をクリックして表示しているパケットのイベントを削除するか、[すべて削除（Delete All）] をクリックして以前に選択したパケットのすべてのイベントを削除します。
- ダウンロード：イベントをトリガーしたパケットのローカル コピー（libpcap 形式のパケット キャプチャ ファイル）をダウンロードするには、[パケットのダウンロード（Download Packet）] をクリックして表示しているイベントに関するキャプチャしたパケットのコピーを保存するか、[すべてのパケッ

トをダウンロード（Download All Packets）] をクリックして以前に選択したパケットのすべてのイベントのキャプチャしたパケットのコピーを保存します。キャプチャされたパケットはlibpcap形式で保存されます。この形式は、複数の一般的なプロトコル アナライザで使用されます。

（注） 単一のポートスキャン イベントは複数のパケットに基づいているため、ポートスキャン パケットをダウンロードできません。ただし、ポートスキャン ビューは使用可能なすべてのパケット情報を提供します。ダウンロードするには少なくとも15%の使用可能なディスク領域が必要です。

- 確認済みのマークを付ける：イベントデータベースからは削除せずに、イベント ビューから削除するため確認済みのイベントにマークを付けるには、[確認（Review）] をクリックして表示しているパケットのイベントにマークを付けるか、[すべて確認（Review All）] をクリックして以前に選択したパケットのすべてのイベントにマーク付けます。詳細については、侵入イベントを確認済みとしてマーク（3074 ページ）を参照してください。
- 追加情報の表示：ページセクションを展開したり、折りたたんだりするには、セクションの横にある矢印をクリックします。詳細については、イベント情報のフィールド（3086ページ）、フレーム情報のフィールド（3094ページ）、データリンク層情報フィールド（3095ページ）を参照してください。
- ネットワーク層の情報の表示：ネットワーク層情報の表示（3096 ページ）を参照してください。
- パケット バイト情報の表示：パケット バイト情報の表示（3101 ページ）を参照してください。
- トランスポート層の情報の表示：次を参照してください。トランスポート層情報の表示（3098ページ）

関連トピック

ポートスキャン検出（2441 ページ）
侵入イベントのクリップボード（3102 ページ）

イベント情報のフィールド

パケット ビューで、[イベント情報（Event Information）] セクションのパケットに関する情報を表示できます。

Event

イベントのメッセージ。ルールベースのイベントの場合、これはルール メッセージに対応します。他のイベントの場合、これはデコーダまたはプリプロセッサによって決まります。

イベントの ID は、(GID:SID:Rev) の形式でメッセージに付加されます。GID は、ルール エンジン、デコーダ、またはイベントを生成したプリプロセッサのジェネレータ ID です。SID は、ルール、デコーダ メッセージ、またはプリプロセッサ メッセージの ID です。Rev はルールのリビジョン番号です。

Timestamp

パケットがキャプチャされた時刻（UTC タイム ゾーン）。

分類（Classification）

イベントの分類。ルールベースのイベントの場合、これはルールの分類に対応します。他のイベントの場合、これはデコーダまたはプリプロセッサによって決まります。

Priority

イベントの優先度。ルールベースのイベントの場合、これは `priority` キーワードの値または `classtype` キーワードの値に対応します。他のイベントの場合、これはデコーダまたはプリプロセッサによって決まります。

Ingress Security Zone

イベントをトリガーとして使用したパケットの入力セキュリティ ゾーン。パッシブ展開環境では、このセキュリティ ゾーン フィールドだけに入力されます。

出力セキュリティ ゾーン（Egress Security Zone）

イベントをトリガーとして使用したパケットの出力セキュリティ ゾーン。パッシブ展開では、このフィールドには入力されません。

ドメイン（Domain）

管理対象デバイスが属するドメイン。 This field is only present if you have ever configured the Firepower Management Center for multitenancy.

Device

アクセス コントロール ポリシーが展開された管理対象デバイス。

スタック構成設定では、プライマリ デバイスとセカンダリ デバイスは、別々のデバイスであるかのように侵入イベントをレポートすることに注意してください。

セキュリティ コンテキスト（Security Context）

トラフィックが通過した仮想ファイアウォール グループを識別するメタデータ。マルチ コンテキスト モードの ASA FirePOWER の場合に、システムがこのフィールドにデータを設定することに注意してください。

入力インターフェイス（Ingress Interface）

イベントをトリガーとして使用したパケットの入力インターフェイス。パッシブ インターフェイスの場合、このインターフェイスの列だけに入力されます。

出力インターフェイス（Egress Interface）

インライン セットの場合、イベントをトリガーとして使用したパケットの出力インターフェイス。

送信元/宛先 IP（Source/Destination IP）

イベントをトリガーとして使用したパケットの発生元（送信元）であるホスト IP アドレスまたはドメイン名、またはイベントをトリガーとして使用したトラフィックのターゲット（宛先）ホスト。

送信元ポート/ICMP タイプ（Source Port/ICMP Type）

イベントをトリガーとして使用したパケットの送信元ポート。ICMP トラフィックの場合は、ポート番号がないため、システムは ICMP タイプを表示します。

Destination Port/ICMP Code

トラフィックを受信するホストのポート番号。ICMP トラフィックの場合は、ポート番号がないため、システムは ICMP コードを表示します。

Email Headers

電子メール 見出しから取得したデータ。電子メール 見出しは侵入イベントのテーブル ビューには表示されませんが、電子メール 見出し データは検索条件として使用できることに注意してください。

電子メールのヘッダーを SMTP トラフィックの侵入イベントと関連付けるには、SMTP プリプロセッサの [ヘッダーのログ（Log Headers）] オプションを有効にする必要があります。ルールベースのイベントの場合、この行は電子メール データが取得されたときに表示されます。

HTTP Hostname

（存在する場合）HTTP 要求のホスト 見出しから取得されたホスト名。この行には、最大 256 バイトの完全なホスト名が表示されます。ホスト名が 1 行より長い場合は、完全なホスト名を展開できます。

ホスト名を表示するには、HTTP 検査プリプロセッサ [ホスト名のログ（Log Hostname）] オプションを有効にする必要があります。

HTTP 要求パケットにホスト名が常に含まれているわけではないことに注意してください。ルールベースのイベントの場合、この行はパケットに HTTP ホスト名または HTTP URI が含まれる場合に表示されます。

HTTP URI

（存在する場合）侵入イベントをトリガーとして使用した HTTP 要求パケットに関連付けられた raw URI。この行には、最大 2048 バイトの完全な URI が表示されます。URI が 1 行より長い場合は、完全な URI を展開できます。

URI を表示するには、HTTP 検査プリプロセッサ [URI のログ（Log URI）] オプションを有効にする必要があります。

HTTP 要求パケットに URI が常に含まれているわけではないことに注意してください。ルールベースのイベントの場合、この行はパケットに HTTP ホスト名または HTTP URI が含まれる場合に表示されます。

HTTP応答によってトリガーとして使用された侵入イベントの関連HTTP URIを参照するには、[両方のポートでのストリーム再構成の実行（Perform Stream Reassembly on Both Ports）] オプションにHTTPサーバのポートを設定する必要があります。ただし、これにより、トラフィックのリアセンブル用のリソース要求が増加することに注意してください。

侵入ポリシー（Intrusion Policy）

（存在する場合）侵入イベントを生成した侵入、プリプロセッサ、デコーダのルールが有効にされた侵入ポリシー。アクセス コントロール ポリシーのデフォルト アクションとして侵入ポリシーを選択するか、アクセス コントロール ルールと侵入ポリシーを関連付けることができます。

アクセス コントロール ポリシー（Access Control Policy）

イベントを生成した侵入ルール、プリプロセッサ ルール、またはデコーダ ルールが有効にされた侵入ポリシーが含まれるアクセス コントロール ポリシー。

アクセス コントロール ルール（Access Control Rule）

イベントを生成した侵入ルールと関連付けられたアクセス コントロール ルール。[デフォルト アクション（Default Action）] は、ルールが有効にされた侵入ポリシーがアクセス コントロール ルールに関連付けられていないことと、代わりにアクセス コントロール ポリシーのデフォルト アクションとして設定されていることを示します。

ルール（Rule）

標準テキスト ルール イベントの場合、イベントを生成したルール。

イベントが、共有オブジェクト ルール、デコーダ、またはプリプロセッサに基づいている場合は、ルールを使用できないことに注意してください。

ルールデータにはネットワークに関する機密情報が含まれるため、管理者はユーザがローカル ルールの表示権限を使用してパケット ビューでルール情報を表示できる機能を、ユーザ ロール エディタで切り替えることができます。

アクション（Actions）

標準テキスト ルールとカスタム ルールのイベントの場合は、[アクション（Actions）] を展開して、イベントをトリガーとして使用したルールに次の操作のいずれかを実行します。

- ルールを編集する
- ルールのバージョンのドキュメントを表示します。標準的なテキスト ルールのみの場合、[アクション（Actions）] から [ドキュメントの表示（View Documentation）] をクリックした後、ドキュメントのポップアップ ウィンドウの [ルール ドキュメント（Rule Documentation）] をクリックすると、より具体的なルールの詳細を表示することができます。
- ルールにコメントを追加する

- ルールの状態を変更する
- ルールのしきい値を設定する
- ルールを抑制する

イベントが、共有オブジェクトルール、デコーダ、またはプリプロセッサに基づいている場合は、ルールを使用できないことに注意してください。

パケット ビュー内での侵入ルールの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Intrusion Admin

侵入イベントのパケットビュー内で、イベントをトリガーとして使用したルールに対して複数のアクションを実行できます。イベントが、共有オブジェクトルール、デコーダ、またはプリプロセッサに基づいている場合は、ルールを使用できないことに注意してください。

ステップ 1 侵入ルールによって生成された侵入イベントのパケット ビュー内で、[イベント情報（Event Information）] セクションの [アクション（Actions）] を展開します。

ステップ 2 次の選択肢があります。

- コメント：標準テキスト ルール イベントの場合、[ルール コメント（Rule Comment）] をクリックして、イベントを生成したルールにテキスト コメントを追加します。これにより、ルールや、特定されたエクスプロイトまたはポリシー違反に関するコンテキストおよび情報を提供できます。さらに、侵入ルール エディタでルールのコメントの追加および表示を行うこともできます。
- 無効化：[このルールを無効にする...（Disable this rule...）] をクリックして、ルールを無効にします。

  このイベントが標準テキスト ルールによって生成された場合は、必要に応じてルールを無効にできます。ローカルで編集できるすべてのポリシーにルールを設定できます。または、現在のポリシーをローカルで編集できる場合は、現在のポリシー（つまり、イベントを生成したポリシー）のみにルールを設定することもできます。

  現在のポリシー オプションは、現在のポリシーを編集できる場合にのみ表示されることに注意してください。たとえば、カスタム ポリシーを編集できますが、システムが提供するデフォルト ポリシーは編集できません。

  （注） パケット ビューから共有オブジェクト ルールを無効にしたり、デフォルトのポリシーでルールを無効にしたりすることは**できません**。

- パケットのドロップ：[このルールを設定してトリガー パケットをドロップ...（Set this rule to drop the triggering packet...）] をクリックして、トリガーするパケットをドロップするルールを設定します。

  管理対象デバイスがネットワーク上でインライン展開されている場合、イベントをトリガーとして使用したルールを設定して、ローカルで編集できるすべてのポリシーでルールをトリガーするパケット

をドロップできます。または、現在のポリシーをローカルで編集できる場合は、現在のポリシー（つまり、イベントを生成したポリシー）のみにルールを設定することもできます。

現在のポリシー オプションは、現在のポリシーを編集できる場合にのみ表示されることに注意してください。たとえば、カスタム ポリシーを編集できますが、システムが提供するデフォルト ポリシーは編集できません。このオプションは [インラインの場合ドロップ（Drop when Inline）] が現在のポリシーで有効になっている場合のみ表示されることに注意してください。

- 編集：標準テキスト ルール イベントの場合、[編集（Edit）] をクリックして、イベントを生成したルールを編集します。イベントが、共有オブジェクト ルール、デコーダ、またはプリプロセッサに基づいている場合は、ルールを使用できません。

  （注） システムによって提供された（カスタム標準テキスト ルールではない）ルールを編集する場合、実際には新規のローカル ルールを作成していることになります。ローカル ルールを設定して、イベントを生成し、現在の侵入ポリシーで元のルールを無効にしていることを確認してください。ただし、デフォルトのポリシーのローカル ルールは有効に**できない**ことに注意してください。

- イベントの生成：[このルールを設定してイベントを生成...（Set this rule to generate events...）] をクリックして、イベントを生成するルールを設定します。

  このイベントが標準テキスト ルールによって生成された場合は、ルールを設定して、ローカルで編集できるすべてのポリシーでイベントを生成できます。または、現在のポリシーをローカルで編集できる場合は、現在のポリシー（つまり、イベントを生成したポリシー）のみにルールを設定することもできます。

  現在のポリシー オプションは、現在のポリシーを編集できる場合にのみ表示されることに注意してください。たとえば、カスタム ポリシーを編集できますが、システムが提供するデフォルト ポリシーは編集できません。

  （注） 共有オブジェクト ルールでパケット ビューからイベントを生成したり、デフォルト ポリシーでルールを無効にしたりすることは**できません**。

- 抑制オプションの設定：パケット ビュー内での抑制オプションの設定（3093 ページ）の説明に従って、[抑制オプションの設定（Set Suppression Options）] を展開し、続行します。

  このオプションを使用して、ローカルで編集できるすべてのポリシーで、このイベントをトリガーとして使用したルールを抑制できます。または、現在のポリシーをローカルで編集できる場合は、現在のポリシー（つまり、イベントを生成したポリシー）のみでルールを制約することもできます。

  現在のポリシー オプションは、現在のポリシーを編集できる場合にのみ表示されることに注意してください。たとえば、カスタム ポリシーを編集できますが、シスコが提供するデフォルト ポリシーは編集できません。

- しきい値オプションの設定：パケット ビュー内でのしきい値オプションの設定（3092 ページ）の説明に従って、[しきい値オプションの設定（Set Thresholding Options）] を展開し、続行します。

  このオプションを使用して、ローカルで編集できるすべてのポリシーでも、これをトリガーとして使用したルールのしきい値を作成できます。または、現在のポリシーをローカルで編集できる場合は、現在のポリシー（つまり、イベントを生成したポリシー）でのみしきい値を作成することもできます。

現在のポリシー オプションは、現在のポリシーを編集できる場合にのみ表示されることに注意してください。たとえば、カスタム ポリシーは編集できますが、システムが提供するデフォルトの侵入ポリシーは編集できません。

- ドキュメントの表示：[ドキュメントの表示（View Documentation）]をクリックして、イベントを生成したルールの説明を確認します。次に、必要に応じて [ルール ドキュメンテーション（Rule Documentation）] をクリックして、ルールの詳細を表示します。

パケット ビュー内でのしきい値オプションの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Intrusion Admin

侵入イベントのパケット ビューでしきい値オプションを設定することによって、ルールごとに時間の経過とともに生成されるイベントの数を制御できます。ローカルで編集できるすべてのポリシーに、またはローカルで編集できる場合は現在のポリシー（つまり、イベントを生成したポリシー）のみに、しきい値オプションを設定できます。

ステップ 1 侵入ルールによって生成された侵入イベントのパケット ビュー内で、[イベント情報（Event Information）] セクションの [アクション（Actions）] を展開します。

ステップ 2 [しきい値オプションの設定（Set Thresholding Options）] を展開し、次の 2 つの有効なオプションから 1 つを選択します。

- **現在のポリシー（in the current policy）**
- **ローカルで作成されたすべてのポリシー（in all locally created policies）**

（注） 現在のポリシー オプションは、現在のポリシーを編集できる場合にのみ表示されます。たとえば、カスタム ポリシーは編集できますが、システムが提供するデフォルト ポリシーは編集できません。

ステップ 3 設定するしきい値のタイプを選択します。

- 通知を期間ごとに指定したイベント インスタンスの数に制限する場合は、[制限（limit）] をクリックします。
- 期間ごとに指定したイベント インスタンス数に達するたびに通知を行う場合は、[しきい値（threshold）] をクリックします。
- 指定されたイベント インスタンス数に達した後で、期間あたり 1 回ずつ通知を行う場合は、[両方（Both）] をクリックします。

ステップ 4 該当するオプション ボタンをクリックして、イベント インスタンスを [送信元（Source）] IP アドレスと [宛先（Destination）] IP アドレスのどちらで追跡するかを指定します。

ステップ 5 [カウント（Count）] フィールドに、しきい値として使用するイベント インスタンスの数を入力します。

ステップ 6 [秒（Seconds）] フィールドに、イベント インスタンスを追跡する期間を指定する数（1 ～ 86400）を入力します。

ステップ 7 既存の侵入ポリシーでこのルールの現在のしきい値をオーバーライドする場合は、[このルールの既存の設定をオーバーライドする（Override any existing settings for this rule）] チェックボックスをオンにします。

ステップ 8 [しきい値の保存（Save Thresholding）] をクリックします。

パケット ビュー内での抑制オプションの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Intrusion Admin

抑制オプションを使用して、侵入イベントをまとめて、または送信元 IP アドレスまたは宛先 IP アドレスに基づいて抑制できます。ローカルで編集できるすべてのポリシーで抑制オプションを設定できます。または、現在のポリシーをローカルで編集できる場合は、現在のポリシー（つまり、イベントを生成したポリシー）のみに抑制オプションを設定することもできます。

ステップ 1 侵入ルールによって生成された侵入イベントのパケット ビュー内で、[イベント情報（Event Information）] セクションの [アクション（Actions）] を展開します。

ステップ 2 [抑制オプションの設定（Set Suppression Options）] を展開し、次の 2 つの有効なオプションから 1 つを選択します。

- **現在のポリシー（in the current policy）**
- **ローカルで作成されたすべてのポリシー（in all locally created policies）**

（注） 現在のポリシー オプションは、現在のポリシーを編集できる場合にのみ表示されます。たとえば、カスタム ポリシーを編集できますが、シスコが提供するデフォルト ポリシーは編集できません。

ステップ 3 次のいずれかの [追跡対象（Track By）] オプションを選択します。

- 指定した送信元 IP アドレスから送信されるパケットによって生成されるイベントを抑制する場合は、[送信元（Source）] をクリックします。
- 指定した宛先 IP アドレスに送信されるパケットによって生成されるイベントを抑制する場合は、[宛先（Destination）] をクリックします。
- このイベントをトリガーしたルールのイベントを完全に抑制する場合は、[ルール（Rule）] をクリックします。

ステップ 4 [IP アドレス（IP address）] または [CIDR ブロック（CIDR block）] フィールドに、送信元または宛先 IP アドレスとして指定する IP アドレスまたは CIDR ブロック/プレフィクス長を入力します。

ステップ 5 [抑制の保存（Save Suppression）] をクリックします。

関連トピック

Firepower システムの IP アドレス表記法 （20 ページ）

フレーム情報のフィールド

パケット ビューで、[フレーム（Frame）] の横にある矢印をクリックして、キャプチャされたフレームに関する情報を表示します。パケット ビューには単一フレームまたは複数フレームを表示できます。各フレームには、個々のネットワークのパケットに関する情報が表示されます。たとえば、タグ付きパケットまたは再構成された TCP ストリーム内のパケットの場合、複数のフレームが表示されます。

フレーム n（Frame n）

キャプチャされたフレーム。*n* は単一フレーム パケットの場合は 1、複数フレーム パケットの場合は差分フレーム番号です。フレーム内のキャプチャされたバイト数はフレーム番号に追加されます。

Arrival Time

フレームがキャプチャされた日時。

Time delta from previous captured frame

複数フレーム パケットの場合、前のフレームがキャプチャされてからの経過時間。

Time delta from previous displayed frame

複数フレーム パケットの場合、前のフレームが表示されてからの経過時間。

Time since reference or first frame

複数フレーム パケットの場合、最初のフレームがキャプチャされてからの経過時間。

Frame Number

差分フレーム番号。

Frame Length

フレームの長さ（バイト単位）。

Capture Length

キャプチャされたフレームの長さ（バイト単位）。

Frame is marked

フレームがマークされているかどうか（true または false）。

Protocols in frame

フレームに含まれるプロトコル。

関連トピック

tag キーワード （2253 ページ）
TCP ストリームの再構成 （2424 ページ）

データリンク層情報フィールド

パケット ビューで、データリンク層プロトコル（たとえば、[イーサネット II（Ethernet II）]）の横にある矢印をクリックして、パケットに関するデータリンク層情報を表示します。これには、送信元ホストおよび宛先ホストの 48 ビットの Media Access Control（MAC）アドレスが含まれます。ハードウェアプロトコルに応じて、パケットに関する他の情報も表示されることがあります。

（注） この例では、イーサネットリンク層情報について説明していることに注意してください。他のプロトコルも表示されることがあります。

パケット ビューはデータリンク層で使用されるプロトコルを反映します。次のリストでは、パケット ビューでイーサネット II または IEEE 802.3 イーサネット パケットについて参照できる情報について説明します。

Destination

宛先ホストの MAC アドレス。

（注） イーサネットは、宛先アドレスとしてマルチキャストおよびブロードキャストアドレスを使用することもできます。

Source

送信元ホストの MAC アドレス。

タイプ（Type）

イーサネットIIパケットの場合、イーサネットフレームでカプセル化されるパケットの種類。たとえば、IPv6 または ARP データグラム。この項目はイーサネット II パケットの場合にのみ表示されることに注意してください。

Length

IEEE 802.3イーサネットパケットの場合、チェックサムを含まないパケットのトータル長（バイト単位）。この項目はIEEE 802.3 イーサネット パケットの場合にのみ表示されることに注意してください。

ネットワーク層情報の表示

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Intrusion Admin

パケットビューで、パケットにネットワーク層プロトコル（たとえば、[インターネットプロトコル（Internet Protocol）]）の横にある矢印をクリックして、パケットに関連したネットワーク層の情報の詳細情報を表示します。

（注） この例では、IP パケットについて説明していることに注意してください。他のプロトコルも表示されることがあります。

IPv4 ネットワーク層の情報フィールド

以下のリストは、IPv4パケットで表示される可能性があるプロトコル固有の情報の説明です。

バージョン

インターネット プロトコルのバージョン番号。

Header Length

すべての IP オプションを含む、見出しのバイト数。オプションのない IP 見出しの長さは 20 バイトです。

Differentiated Services Field

送信元ホストが明示的輻輳通知（ECN）サポートする方法を示す次の差別化サービスの値。

- `0x0`：ECN-Capable Transport（ECT）をサポートしません
- `0x1` および `0x2`：ECT をサポートします
- `0x3`：Congestion Experienced（CE）

Total Length

IP 見出しを差し引いた IP パケットの長さ（バイト単位）。

ID

送信元ホストから送信される IP データグラムを一意的に識別する値。この値は同じデータグラム フラグメントをトレースするために使用されます。

Flags

IP フラグメンテーションを制御する値。

[Last Fragment] の値は、データグラムに関連付けられた追加のフラグメントが存在するかどうかを次のように示します。

- `0`：データグラムに関連付けられた追加のフラグメントは存在しない
- `1`：データグラムに関連付けられた追加のフラグメントが存在する

[Don't Fragment] フラグの値は、データグラムをフラグメント化できるかどうかを次のように制御します。

- `0`：データグラムをフラグメント化できる
- `1`：データグラムをフラグメント化**してはならない**

Fragment Offset

データグラムの先頭からのフラグメント オフセットの値。

Time to Live (ttl)

データグラムが期限切れになる前にデータグラムがルータ間で作成できるホップの数。

Protocol

IP データグラムにカプセル化されるトランスポート プロトコル。たとえば、ICMP、IGMP、TCP、または UDP。

Header Checksum

IP チェックサムが有効かどうかを示すインジケータ。チェックサムが無効な場合、データグラムが送信中に破損したか、侵入回避の試行において使用中である可能性があります。

Source/Destination

送信元（または宛先）ホストの IP アドレスまたはドメイン名。

ドメイン名を表示するには、IP アドレス解決を有効にする必要があることに注意してください。

アドレスまたはドメイン名をクリックしてコンテキスト メニューを表示してから、whois 検索を実行する場合は [Whois] を、ホスト情報を表示する場合は [ホスト プロファイルの表示（View Host Profile）] を、アドレスをグローバル ブラックリストまたはホワイトリストに追加する場合は [今すぐブラックリスト化する（Blacklist Now）] または [今すぐホワイトリスト化する（Whitelist Now）] を選択します。

IPv6 ネットワーク層の情報フィールド

以下のリストは、IPv6パケットで表示される可能性があるプロトコル固有の情報の説明です。

トラフィック クラス（Traffic Class）

IPv4 で提供される差別化サービス機能と同じように、IPv6 パケット クラスまたは優先度を特定する IPv6 見出し内の Experimental 8 ビットのフィールド。 未使用の場合、このフィールドはゼロに設定されます。

Flow Label

非デフォルトのQoSまたはリアルタイム サービスなどの特別なフローを特定する、1からFFFFまでの、オプションの20ビットのIPv6 16進数値。未使用の場合、このフィールドはゼロに設定されます。

Payload Length

IPv6 ペイロードのオクテットの数を特定する 16 ビット フィールド。これは、任意の拡張子見出しを含む、IPv6 見出しに続くすべてのパケットで構成されます。

Next Header

IPv4 プロトコル フィールドと同じ値を使用して、IPv6 見出しのすぐ後に続く、見出しの種類を特定する 8 ビットのフィールド。

Hop Limit

パケットを転送するノードごとに 1 つずつデクリメントする 8 ビットの 10 進整数。デクリメントした値がゼロになると、パケットは破棄されます。

Source

送信元ホストの 128 ビットの IPv6 アドレス。

Destination

宛先ホストの 128 ビットの IPv6 アドレス。

トランスポート層情報の表示

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Intrusion Admin

ステップ 1 パケット ビューで、トランスポート層プロトコル（たとえば [TCP]、[UDP]、または [ICMP]）の横にある矢印をクリックします。

ステップ 2 オプションで、存在する場合、[データ（Data）] をクリックして、パケット ビューの [パケット情報（Packet Information）] セクションで、プロトコルのすぐ上にあるペイロードの最初の 24 バイトを表示します。

ステップ 3 TCP パケット ビューのフィールド（3099 ページ）、UDP パケット ビューのフィールド（3100 ページ）、またはICMP パケット ビュー フィールド（3100 ページ）の説明に従って、TCP、UDP、ICMP プロトコルのトランスポート層の内容を表示します。

（注） これらの例では、TCP、UDP、ICMP パケットについて説明していますが、他のプロトコルも表示されることがあることに注意してください。

TCP パケット ビューのフィールド

ここでは、TCP パケットのプロトコル固有の情報について説明します。

Source port

発信元のアプリケーション プロトコルを識別する番号。

Destination port

受信側のアプリケーション プロトコルを識別する番号。

Sequence number

TCP ストリームの初期シーケンス番号と連動する、現在の TCP セグメントの最初のバイトの値。

Next sequence number

応答パケットにおける、送信する次のパケットのシーケンス番号。

Acknowledgement number

以前に受信されたデータのシーケンス番号に連動したTCP 確認応答。

Header Length

見出しのバイト数。

Flags

TCP セグメントの転送状態を示す 6 ビット。

- `U`：緊急ポインタが有効
- `A`：確認応答番号が有効
- `P`：受信者はデータをプッシュする必要がある
- `R`：接続をリセットする

- S：シーケンス番号を同期して新しい接続を開始する
- F：送信者はデータ送信を終了した

Window size

受信ホストが受け入れる、確認応答されていないデータの量（バイト単位）。

Checksum

TCPチェックサムが有効かどうかを示すインジケータ。チェックサムが無効な場合、データグラムが送信中に破損したか、回避の試行において使用中である可能性があります。

Urgent Pointer

緊急データが終了する TCP セグメントの位置（存在する場合）。U フラグとともに使用します。

Options

TCP オプションの値（存在する場合）。

UDP パケット ビューのフィールド

ここでは、UDP パケットのプロトコル固有の情報について説明します。

Source port

発信元のアプリケーション プロトコルを識別する番号。

Destination port

受信側のアプリケーション プロトコルを識別する番号。

Length

UDP 見出しとデータを組み合わせた長さ。

Checksum

UDPチェックサムが有効かどうかを示すインジケータ。チェックサムが無効な場合、データグラムが送信中に破損した可能性があります。

ICMP パケット ビュー フィールド

ここでは、ICMP パケットのプロトコル固有の情報について説明します。

Type

ICMP メッセージのタイプ。

- 0：エコー応答

- 3：宛先到達不能
- 4：ソース クエンチ（始点抑制要求）
- 5：リダイレクト
- 8：エコー要求
- 9：ルータ アドバタイズメント
- 10：ルータ送信要求
- 11：時間超過
- 12：パラメータの問題
- 13：タイムスタンプ要求
- 14：タイムスタンプ応答
- 15：情報要求（廃止）
- 16：情報応答（廃止）
- 17：アドレス マスク要求
- 18：アドレス マスク応答

Code

ICMP メッセージ タイプに付随するコード。ICMP メッセージ タイプ 3、5、11、および 12 には、RFC 792 で説明されている対応コードがあります。

Checksum

ICMP チェックサムが有効かどうかを示すインジケータ。チェックサムが無効な場合、データグラムが送信中に破損した可能性があります。

パケット バイト情報の表示

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Intrusion Admin

パケット ビューで、[パケット バイト（Packet Bytes）] の横にある矢印をクリックして、パケットを構成するバイトの 16 進数および ASCII バージョンを表示します。システムがトラフィックを復号化した場合は、復号化されたパケット バイトを表示できます。

侵入イベントのクリップボード

クリップボードは、任意の侵入イベント ビューから侵入イベントをコピーできる保存エリアです。

クリップボードの内容は、イベントが生成された日時別にソートされます。クリップボードに侵入イベントを追加した後、クリップボードからそれらを削除することも、クリップボードの内容のレポートを生成することもできます。

クリップボードの侵入イベントをインシデントに追加することもできます。インシデントとは、セキュリティ ポリシーの違反の可能性に関係していると思われるイベントのコンパイルです。

関連トピック

侵入イベント ワークフローの使用 （3080 ページ）
侵入イベント パケット ビューの使用 （3084 ページ）
インシデントの作成 （2874 ページ）

クリップボードのレポートの生成

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Intrusion Admin

任意のイベント ビューで行うのと同じように、クリップボードのイベントに関するレポートを生成できます。

始める前に

- クリップボードに1つ以上のイベントを追加します。詳細については、侵入イベント ワークフローの使用 （3080ページ）または侵入イベント パケット ビューの使用 （3084ページ）を参照してください。

ステップ 1 **[Analysis]** > **[Intrusions]** > **[Clipboard]**を選択します。

ステップ 2 次の選択肢があります。

- クリップボード上のページの特定のイベントを含めるには、そのページに移動し、イベントの横にあるチェックボックスをオンにして、[レポートの生成（Generate Report）] をクリックします。
- クリップボードのすべてのイベントを含めるには、[すべてのレポートの生成（Generate Report All）] をクリックします。

ステップ 3 レポートの表示方法を指定して、[生成（Generate）] をクリックします。

ステップ 4 1 つ以上の出力形式を選択し、オプションで、他の設定を変更します。

ステップ 5 [生成（Generate）] をクリックしてから、[はい（Yes）] をクリックします。

ステップ 6 次の選択肢があります。

- レポート リンクをクリックして、新しいウィンドウにレポートを表示します。
- [OK] をクリックして、レポートのデザインを変更できる [レポート テンプレート（Report Templates）] ページに戻ります。

関連トピック

レポート テンプレート （2775 ページ）

クリップボードからのイベントの削除

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Intrusion Admin

インシデントに追加したくない侵入イベントがクリップボード上にある場合は、そのイベントを削除できます。

（注） クリップボードからイベントを削除しても、イベントデータベースからイベントは削除**されません**。ただし、イベントデータベースからイベントを削除すると、イベントはクリップボードから削除されます。

ステップ 1 **[Analysis]** > **[Intrusions]** > **[Clipboard]**を選択します。

ステップ 2 次の選択肢があります。

- クリップボードのページの特定の侵入イベントを削除するには、そのページに移動し、イベントの横にあるチェックボックスを選択し、[削除（Delete）] をクリックします。
- クリップボードからすべての侵入イベントを削除するには、[すべて削除（Delete All）] をクリックします。[イベント設定（Event Preferences）] で [全てのアクションを確認（Confirm All Actions）] オプションを選択した場合、最初にすべてのイベントを削除するかどうか確認するプロンプトが出されることに注意してください。

侵入イベントの統計情報の表示

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Intrusion Admin

[侵入イベントの統計情報（Intrusion Event Statistics）] ページは、アプライアンスの現在の状態の概要と、ネットワークで生成されたすべての侵入イベントを表示します。

このページに表示される IP アドレス、ポート、プロトコル、イベント メッセージなどはそれぞれリンクになっています。関連イベントの情報を表示するには、任意のリンクをクリックします。たとえば、上位 10 個の宛先ポートのいずれかが `80 (http) /tcp` である場合、そのリンクをクリックすると、デフォルトの侵入イベント ワークフローの最初のページが表示され、そのポートをターゲットとするイベントがリストされます。現在の時刻範囲で表示されるのはイベント（およびイベントを生成する管理対象デバイス）のみであることに注意してください。さらに、確認済みマークを付けた侵入イベントも統計に引き続き表示されます。たとえば、現在の時刻範囲が過去 1 時間であり、最初のイベントが 5 時間前に生成された場合、[最初のイベント（First Event）] リンクをクリックすると、そのイベントは時刻範囲を変更するまでイベント ページには表示されません。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

ステップ 1 **[Overview]** > **[Summary]** > **[Intrusion Event Statistics]** を選択します。

ステップ 2 ページの上部にある 2 つの選択ボックスから、統計を表示するゾーンおよびデバイスを選択するか、[すべてのセキュリティ ゾーン（All Security Zones）] および [すべてのデバイス（All Devices）] を選択して、侵入イベントを収集するすべてのデバイスの統計を表示します。

ステップ 3 [統計の取得（Get Statistics）] をクリックします。

ヒント カスタム時刻範囲からデータを表示するには、右上のページエリアのリンクをクリックし、時間枠の変更 （2956 ページ）にある指示に従います。

ホスト統計情報

[侵入イベント統計情報（Intrusion Event Statistics）] ページの [ホスト統計情報（Host Statistics）] セクションは、アプライアンス自体に関する情報を提供します。Firepower Management Center では、このセクションはすべての管理対象デバイスに関する情報も提供します。

この情報には、次の内容が含まれます。

時刻（Time）

アプライアンスの現在の時刻。

アップタイム（Uptime）

アプライアンス自体が再起動してから経過した日数、時間、および分数。Firepower Management Center では、[アップタイム（Uptime）] に各管理対象デバイスの最終起動時刻、ログインしたユーザの数、および負荷平均も示されます。

Disk Usage

使用中のディスクの割合。

Memory Usage

使用中のシステム メモリの割合。

Load Average

直前の 1 分間、5 分間、15 分間の CPU キュー内の平均プロセス数。

イベントの概要

[侵入イベント統計（Intrusion Event Statistics）] ページの [イベントの概要（Event Overview）] セクションは、侵入イベント データベースにある情報の概要を示します。

これらの統計には、次の情報が含まれています。

イベント

侵入イベント データベースのイベントの数。

時間範囲内のイベント（Events in Time Range）

現在選択されている時間範囲と、時間範囲内に収まるデータベースのイベントの割合。

最初のイベント（First Event）

イベント データベース内の最初のイベントのイベント メッセージ。

最後のイベント（Last Event）

イベント データベース内の最後のイベントのイベント メッセージ。

（注） Firepower Management Center で侵入イベント データを表示中に管理対象デバイスを選択した場合は、そのデバイスの [イベントの概要（Event Overview）] セクションが代わりに表示されます。

イベント統計

[侵入イベント統計（Intrusion Event Statistics）] ページの [イベント統計（Event Statistics）] セクションでは、侵入イベント データベース内の情報に関する具体的な情報が表示されます。

この情報には、次に関する詳細が含まれます。

- 上位 10 個のイベント タイプ
- 上位 10 個のソース IP アドレス
- 上位 10 個の宛先 IP アドレス
- 上位 10 個の宛先ポート
- イベント数が最大であるプロトコル、イングレスとイーグレスのセキュリティ ゾーン、およびデバイス

（注） マルチドメイン展開では、システムは、各リーフ ドメインに個別のネットワーク マップを作成します。その結果、リーフ ドメインには、ネットワーク内で一意である IP アドレスを含めることができますが、別のリーフ ドメイン内の IP アドレスと同じにすることができます。先祖ドメインでイベントの統計情報を表示すると、システムで、その IP アドレスの複数のインスタンスが繰り返し表示される場合があります。一見すると、エントリが重複しているように見えることがあります。ただし、各 IP アドレスのホスト プロファイル情報までドリル ダウンすると、それらが異なるリーフ ドメインに属していることがわかります。

侵入イベントのパフォーマンス グラフの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Intrusion Admin

[侵入イベントのパフォーマンス（Intrusion Event Performance）] ページでは、Firepower Management Center または管理対象デバイスの指定された期間の侵入イベントのパフォーマンス統計情報を示すグラフを生成できます。グラフを生成することにより、1 秒あたりの侵入イベントの数、1 秒あたりのメガビット数、1 パケットあたりの平均バイト数、Snort によって検査されていないパケットの割合、および TCP 正規化の結果としてブロックされたパケットの数を反映できます。これらのグラフは、過去 1 時間、前日、先週、または先月の操作の統計を表示できます。

（注） 新しいデータは 5 分ごとに統計グラフに蓄積されます。したがって、グラフをすばやくリロードしても、次の 5 分の差分更新が実行されるまでデータは変更されていない場合があります。各グラフには、選択した時間間隔（前月、週、日、または時間）に対応した間隔（日、時間、または 5 分）で平均値が表示されます。平均値が 1 未満の場合は、小数値で表示されます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

ステップ 1 **[Overview]** > **[Summary]** > **[Intrusion Event Performance]**を選択します。

ステップ 2 [デバイスの選択（Select Device）] リストから、データを表示するデバイスを選択します。

ステップ 3 侵入イベントのパフォーマンス統計情報グラフの種類（3107ページ）で説明されているように、[グラフの選択（Select Graph(s)）] リストから、作成するグラフの種類を選択します。

ステップ 4 [時間範囲の選択（Select Time Range）] リストから、グラフに使用する時間範囲を選択します。

ステップ 5 [グラフ（Graph）] をクリックします。

ステップ 6 グラフを保存するには、グラフを右クリックし、ブラウザでイメージを保存する手順に従います。

侵入イベントのパフォーマンス統計情報グラフの種類

次の表に、表示可能なグラフの種類を示します。ネットワーク分析ポリシーの [インライン モード（Inline Mode）] 設定の影響を受けるデータを含むグラフ タイプでは、表示が異なるので注意してください。[インライン モード（Inline Mode）] が無効になっている場合、Web インターフェイスでアスタリスク（*）が付いているグラフタイプ（下記の表では列に [はい（yes）] と記載）には、[インライン モード（Inline Mode）] が有効になっている場合に変更またはドロップされるトラフィックに関するデータが含まれています。

表 *340*：侵入イベントのパフォーマンス グラフの種類

データの生成対象となるグラフ	実行する操作	説明	インライン モードによる影響
Avg Bytes/Packet	n/a	各パケットに含まれる平均バイト数。	no
ECN Flags Normalized in TCP Traffic/Packet	[明示的輻輳通知（Explicit Congestion Notification）] を有効にして、[パケット（Packet）] を選択します。	ネゴシエーションに関係なく、パケット単位で ECN フラグがクリアされたパケットの数。	Yes
ECN Flags Normalized in TCP Traffic/Session	[明示的輻輳通知（Explicit Congestion Notification）] を有効にして、[ストリーム（Stream）] を選択します。	ECN の使用がネゴシエートされなかった場合にストリーム単位で ECN フラグがクリアされた回数。	Yes
Events/Sec	n/a	デバイスで生成された 1 秒あたりのイベント数。	no

データの生成対象となるグラフ	実行する操作	説明	インライン モードによる影響
ICMPv4 Echo Normalizations	[ICMPv4 の正規化（Normalize ICMPv4）] を有効にします。	エコー（要求）またはエコー応答メッセージの 8 ビット コード フィールドがクリアされた ICMPv4 パケットの数。	Yes
ICMPv6 Echo Normalizations	[ICMPv6 の正規化（Normalize ICMPv6）] を有効にします。	エコー（要求）またはエコー応答メッセージの 8 ビット コード フィールドがクリアされた ICMPv6 パケットの数。	Yes
IPv4 DF Flag Normalizations	[IPv4 の正規化（Normalize IPv4）] と [DF ビットの正規化（Normalize Don't Fragment Bit）] を有効にします。	[IPv4 フラグ（IPv4 Flags）] ヘッダー フィールドのシングル ビット [フラグメント禁止（Don't Fragment）] サブフィールドがクリアされた IPv4 パケットの数。	Yes
IPv4 Options Normalizations	[Normalize IPv4] を有効にします。	オプション オクテットが「1」（No Operation）に設定された IPv4 パケットの数	yes
IPv4 Reserved Flag Normalizations	[IPv4 の正規化（Normalize IPv4）] と [予約済みビットの正規化（Normalize Reserved Bit）] を有効にします。	[IPv4 フラグ（IPv4 Flags）] ヘッダー フィールドのシングル ビット [予約済み（Reserved）] サブフィールドがクリアされた IPv4 パケットの数。	Yes
IPv4 Resize Normalizations	[IPv4 の正規化（Normalize IPv4）] を有効にします。	超過ペイロードが IP ヘッダーで指定されたデータグラム長に切り詰められた IPv4 パケットの数。	Yes
IPv4 TOS Normalizations	[IPv4 の正規化（Normalize IPv4）] と [TOS ビットの正規化（Normalize TOS Bit）] を有効にします。	1 バイトの [差別化サービス（DS）（Differentiated Services (DS)）] フィールド（旧 [タイプ オブ サービス（ToS）（Type of Service (TOS)）] フィールド）がクリアされた IPv4 パケットの数。	Yes

データの生成対象となるグラフ	実行する操作	説明	インライン モードによる影響
IPv4 TTL Normalizations	[Normalize IPv4]、[Maximum TTL]、および [Reset TTL] を有効にします。	IPv4 存続時間（TTL）正規化の数。	yes
IPv6 Options Normalizations	[IPv6 の正規化（Normalize IPv6）] を有効にします。	[ホップバイホップ オプション（Hop-by-Hop Options）] または [宛先オプション（Destination Options）] 拡張ヘッダーの [オプション タイプ（Option Type）] フィールドが、00（スキップして処理を続行）に設定された IPv6 パケットの数。	Yes
IPv6 TTL Normalizations	[Normalize IPv6]、[Minimum TTL]、および [Reset TTL] を有効にします。	IPv6 ホップ リミット（TTL）正規化の数。	yes
Mbits/Sec	n/a	デバイスをパススルーするトラフィックの 1 秒あたりのメガビット数。	no
Packet Resized to Fit MSS Normalizations	[Trim Data to MSS] を有効にします。	ペイロードが TCP データ フィールドよりも長かったため、ペイロードが最大セグメント サイズに切り詰められたパケットの数。	yes
Packet Resized to Fit TCP Window Normalizations	[Trim Data to Window] を有効にします。	受信側ホストの TCP ウィンドウに合わせて TCP データ フィールドが切り詰められたパケットの数。	yes

データの生成対象となるグラフ	実行する操作	説明	インライン モードによる影響
Percent Packets Dropped	n/a	選択されたすべてのデバイスにおける未検査のパケットの平均割合。たとえば、2つのデバイスを選択した場合、平均が 50 % であるというのは、1つのデバイスのドロップ率が 90 % であり、もう 1 つのデバイスのドロップ率が 10 % であることを示している可能性があります。また、両方のデバイスのドロップ率が 50% である可能性もあります。グラフは、1つのデバイスを選択した場合にのみ合計ドロップ率を表します。	no
RST Packets With Data Stripped Normalizations	[Remove Data on RST] を有効にします。	TCP リセット（RST）パケットからデータが削除されたパケットの数。	yes
SYN Packets With Data Stripped Normalizations	[Remove Data on SYN] を有効にします。	TCP オペレーティング システムが Mac OS でない場合に、SYN パケットからデータが削除されたパケットの数。	yes
TCP Header Padding Normalizations	[Normalize/Clear Option Padding Bytes] を有効にします。	オプションの埋め込みバイトが 0 に設定された TCP パケットの数。	yes
TCP No Option Normalizations	[Allow These TCP Options] を有効にして、`any`以外のオプションに設定します。	タイムスタンプ オプションがストリップされたパケットの数。	yes
TCP NS フラグの正規化（TCP NS Flag Normalizations）	[明示的輻輳通知（Explicit Congestion Notification）] を有効にして、[パケット（Packet）] を選択します。	ECN Nonce Sum（NS）オプション正規化の数。	yes

データの生成対象となるグラフ	実行する操作	説明	インライン モードによる影響
TCP Options Normalizations	[Allow These TCP Options] を有効にして、any以外のオプションに設定します。	オプション フィールドが「No Operation」（TCP オプション1）に設定されているオプションの数（MSS、ウィンドウ スケール、タイムスタンプ、および明示的に許可されたオプションを除く）。	yes
TCP Packets Blocked By Normalizations	[Normalize TCP Payload] を有効にします（セグメントのリアセンブリは失敗します）。	TCP セグメントを正常にリアセンブルできなかったためにドロップされたパケットの数。	yes
TCP Reserved Flags Normalizations	[Normalize/Clear Reserved Bits] を有効にします。	予約ビットがクリアされたTCPパケットの数。	yes
TCP Segment Reassembly Normalizations	[Normalize TCP Payload] を有効にします（セグメントのリアセンブリは成功します）。	再送信データの一貫性を確保するために TCP データ フィールドが正規化されたパケットの数。（正しくリアセンブルできないセグメントはすべてドロップされます）。	yes
TCP SYN Option Normalizations	[Allow These TCP Options] を有効にして、any以外のオプションに設定します。	SYN 制御ビットが設定されていないため、最大セグメント サイズまたはウィンドウ スケール オプションが「No Operation」（TCP オプション1）に設定されたオプションの数。	yes
TCP Timestamp ECR Normalizations	[Allow These TCP Options] を有効にして、any以外のオプションに設定します。	確認応答（ACK）制御ビットが設定されていないため、タイムスタンプ エコー応答（TSecr）オプション フィールドがクリアされたパケットの数。	yes
TCP Urgent Pointer Normalizations	[緊急ポインタの正規化（Normalize Urgent Pointer）] を有効にします。	TCP ヘッダーの [緊急ポインタ（Urgent Pointer）] フィールド（2バイト）がペイロード長を超えていたため、ペイロード長に合わせて設定されたパケットの数。	Yes

データの生成対象となるグラフ	実行する操作	説明	インライン モードによる影響
Total Blocked Packets	[Inline Mode] または [Drop when Inline] を設定します。	ルール、デコーダ、およびプリプロセッサのドロップを含めて、ドロップされたパケットの総数。	no
Total Injected Packets	[Inline Mode] を設定します。	再送信前にサイズ変更されたパケットの数。	no
Total TCP Filtered Packets	TCP ストリームの前処理を設定します。	TCP ポート フィルタリングのためにストリームによってスキップされたパケットの数。	no
Total UDP Filtered Packets	UDP ストリームの前処理を設定します。	UDP ポート フィルタリングのためにストリームによってスキップされたパケットの数。	no
Urgent Flag Cleared Normalizations	[Clear URG if Urgent Pointer is Not Set] を有効にします。	緊急ポインタが設定されていなかったため、TCPヘッダーの URG 制御ビットがクリアされたパケットの数。	yes
Urgent Pointer and Urgent Flag Cleared Normalizations	[Clear Urgent Pointer/URG on Empty Payload] を有効にします。	ペイロードがなかったため、TCP ヘッダーの緊急ポインタ フィールドと URG 制御ビットがクリアされたパケットの数。	yes
Urgent Pointer Cleared Normalizations	[URG=0 の場合に緊急ポインタをクリア（Clear Urgent Pointer if URG=0）] を有効にします。	緊急（URG）制御ビットが設定されていなかったため、TCP ヘッダーの [緊急ポインタ（Urgent Pointer）] フィールド（16 ビット）がクリアされたパケットの数。	はい

関連トピック

インライン正規化プリプロセッサ （2403 ページ）
インライン導入でのプリプロセッサによるトラフィックの変更 （2302 ページ）
インライン展開でのドロップ動作 （2069 ページ）

侵入イベント グラフの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか（Any）	いずれか（Any）	Admin/Intrusion Admin

Firepower System は、経時的な侵入イベントの傾向を示すグラフを表示します。1 つまたはすべての管理対象デバイスについて、過去1時間から先月までの範囲の経時的な侵入イベント グラフを生成できます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

ステップ 1 **[Overview]** > **[Summary]** > **[Intrusion Event Graphs]**を選択します。

ステップ 2 [デバイスの選択（Select Device）] で、[すべて（all）] を選択してすべてのデバイスを含めるか、グラフに含める特定のデバイスを選択します。

ステップ 3 [グラフの選択（Select Graph(s)）] で、生成するグラフの種類を選択します。

- 上位 10 個の宛先ポート
- 上位 10 個の送信元 IP アドレス
- 上位 10 個のイベント メッセージ

ステップ 4 [時間範囲の選択（Select Time Range）] で、グラフの時間範囲を選択します。

- 直近の 1 時間（Last Hour）
- 前日（Last Day）
- 先週（Last Week）
- 先月（Last Month）

ステップ 5 [グラフ（Graph）] をクリックします。

侵入イベントの履歴

機能	バージョン	詳細
Syslog の接続イベントの固有識別子	6.4.0.4	syslog の [Sensor UUID]、[First Packet Time]、[Connection Instance ID]、および [Connection Counter] フィールドの情報を総合すると、接続イベントを一意に識別できます。これらのフィールドは、侵入イベントの syslog に含まれます。
[IntrusionPolicy] フィールドが syslog に含まれるようになりました。	6.4	侵入イベントの syslog が、イベントをトリガーした侵入ポリシーを指定するようになりました。
新しい侵入イベント検索フィールド：[CVE ID]	6.4	MITRE の Common Vulnerabilities and Exposures 識別番号で検索ができるようになりました。 変更された画面：[分析（Analysis）] > [侵入（Intrusions）] > [イベント（Events）] > [検索の編集（Edit Search）] サポート対象プラットフォーム：すべて

第 127 章

ファイル/マルウェア イベントとネットワーク ファイル トラジェクトリ

次のトピックでは、ファイル/マルウェア イベント、ローカル マルウェア分析、動的分析、キャプチャされたファイル、およびネットワーク ファイル トラジェクトリの概要を示します。

ファイル イベント/マルウェア イベントとネットワーク ファイル トラジェクトリについて

ファイル ポリシーは、一致したトラフィックのファイル イベントおよびマルウェア イベントを自動的に生成し、キャプチャされたファイルの情報をログに記録します。また、ファイル ポリシーでファイル イベントまたはマルウェア イベントが生成されるか、ファイルがキャプチャされると、システムは関連する接続の終了を Firepower Management Center データベースに自動的に記録します。このデータを分析して、悪影響に対処したり、将来の攻撃をブロックしたりすることができます。

ファイル分析結果に基づいて、キャプチャされたファイル、生成されたマルウェアとファイル イベントを、[分析（Analysis）]>[ファイル（Files）] メニューで使用可能なページの表を使用して確認することができます。使用可能な場合は、ファイルの構成、性質、脅威スコア、動的分析のサマリー レポートを調べ、マルウェア分析をさらに詳細に把握できます。

分析のターゲットをさらに絞り込むために、マルウェア ファイルの [ネットワークファイルトラジェクトリ（network file trajectory）]（さまざまなファイル プロパティに加え、ファイルがどのようにネットワークを通過し、ホスト間で渡されてきたかを示すマップ）を使用して、ホスト間での個々の脅威の広がりを時系列で追跡できます。これにより、最も効果的なアウトブレイク制御と防止対策に集中できます。

ファイル ルールでローカル マルウェア分析または動的分析を設定すると、システムによってルールに一致するファイルが事前分類され、ファイル構成レポートが生成されます。

組織で *AMP for Endpoints* が展開されていて、その展開が Firepower Management Center と統合されている場合は、その製品により、スキャン、マルウェア検出、および検疫のレコードと侵害の兆候（IOC）をインポートすることもできます。このデータは、ネットワーク上のマルウェアの全体像をより完全に把握するために、Firepower によって収集されたイベントデータとともに表示されます。

コンテキスト エクスプローラ、およびレポート機能を使用すると、検出/キャプチャ/ブロックされたファイルとマルウェアについてより詳しく理解できます。また、イベントを使用して相関ポリシー違反をトリガーしたり、電子メール、SMTP、または syslog によるアラートを発行したりすることもできます。

（注） マルウェアを検出し、ファイル イベントおよびマルウェア イベントを生成するようにシステムを設定するには、ファイル ポリシーと高度なマルウェア防御（1911 ページ）を参照してください。

ファイルおよびマルウェア イベント

Firepower Management Center は、さまざまなタイプのファイルおよびマルウェア イベントをログに記録できます。個々のイベントに関する情報は、イベントの生成方法と生成理由に応じて異なります。

- ファイル イベントとは、Firepower システム（ネットワーク向け AMP）によって検出されたマルウェアを含むファイルを意味します。ファイル イベントには、AMP for Endpoints 関連のフィールドは含まれません。
- マルウェア イベントとは、ネットワーク向け AMP または AMP for Endpoints によって検出されたマルウェアを意味します。また、マルウェア イベントは、スキャンや検疫など、AMP for Endpoints の導入からの脅威以外のデータを記録できます。
- レトロスペクティブ マルウェア イベントとは、性質（ファイルがマルウェアかどうか）が変更された、ネットワーク向け AMP によって検出されたファイルを意味します。

（注）

- ネットワーク向け AMP によってマルウェアとして識別されたファイルは、ファイル イベントとマルウェア イベントの両方を生成します。エンドポイント向けの AMP によって生成されたマルウェア イベントは対応するファイル イベントを持っていません。
- NetBIOS-ssn（SMB）トラフィックの検査によって生成されるファイル イベントは、即座には接続イベントを生成しません。これは、クライアントとサーバが持続的接続を確立するためです。システムはクライアントまたはサーバがセッションを終了した後に接続イベントを生成します。
- Firepower システムでは、Unicode（UTF-8）文字を使用するファイル名の表示および入力がサポートされます。ただし、Unicode のファイル名は PDF レポートに変換された形式で表示されます。また、SMB プロトコルによって、ファイル名の印刷不能な文字がピリオドに置き換えられます。

ファイル イベントおよびマルウェア イベントの種類

ファイル イベント

システムは、現在展開されているファイル ポリシーのルールに従って、管理対象デバイスがネットワーク トラフィック内のファイルを検出またはブロックしたときに生成されたファイル イベントを記録します。

システムがファイル イベントを生成する際に、呼び出しを行うアクセス コントロール ルールのログ設定に関係なく、システムは Firepower Management Center データベースへの関連する接続の終わりも記録します。

マルウェア イベント（Malware Events）

Firepower システム（特に ネットワーク向け AMP の機能）は、全体的なアクセス コントロール設定の一部としてネットワーク トラフィック内のマルウェアを検出すると、マルウェア イベントを生成します。マルウェアイベントには、結果として生じたイベントの性質や、いつどこでどのようにしてマルウェアが検出されたかに関するコンテキスト データが含まれます。

表 *341* : でのマルウェア イベントの生成シナリオ

システムがファイルを検出し、次の状態になった場合	性質
AMP クラウドにファイルの性質についてクエリを行い（マルウェア クラウド ルックアップを実行）、クエリに成功した場合	マルウェア、クリーン、または不明
AMP クライドにクエリを行ったものの、接続を確立できないか、他の理由でクライドが利用可能でない場合	応対不可 この性質を持つイベントはごくわずかである可能性があります。これは予期された動作です。

システムがファイルを検出し、次の状態になった場合	性質
ファイルに関連付けられている脅威スコアが、ファイルを検出したファイル ポリシーで定義されたマルウェアしきい値の脅威スコアを超えた場合、またはローカルマルウェア分析でマルウェアが識別された場合	マルウェア
ファイルがカスタム検出リストに設定されている場合（手動でマルウェアとしてマークされている場合）	カスタム検出
ファイルがクリーン リストに設定されている場合（手動でクリーンとしてマークされている場合）	クリーン

レトロスペクティブ マルウェア イベント

ネットワーク トラフィックで検出されたマルウェアの場合、性質が変わることがあります。たとえば、AMP クラウドによる判定の結果、以前はクリーンであると考えられていたファイルが今はマルウェアとして識別されるようになったり、その逆、つまりマルウェアと識別されたファイルが実際にはクリーンであったりする可能性があります。先週クエリしたファイルの性質が変わると、AMP クラウドがシステムに通知します。その場合、以下の 2 つが行われます。

- Firepower Management Centerが新しい遡及的マルウェア イベントを生成します。

  この新しい遡及的マルウェア イベントは、前の週に検出され、同じ SHA-256 ハッシュ値を持つ同じすべてのファイルの性質変更を表します。そのため、これらのイベントには限られた情報（Firepower Management Centerに性質変更が通知された日時、新しい性質、ファイルの SHA-256 ハッシュ値、および脅威名）が含まれます。IP アドレスや他のコンテキスト情報は含まれません。

- Firepower Management Centerは遡及的イベントの関連する SHA-256 ハッシュ値を持つ既に検出済みのファイルのファイル性質を変更します。

  ファイルの性質が Malware に変更されると、Firepower Management Centerは新しいマルウェア イベントをデータベースに記録します。新しい性質を除き、この新しいマルウェア イベントの情報は、ファイルが最初に検出されたときに生成されたファイルイベントのものと同じです。

  ファイルの性質が [クリーン（Clean）] に変更された場合、Firepower Management Center はそのマルウェアイベントを削除しません。代わりに、イベントに性質の変更が反映されます。つまり、マルウェア テーブルには性質が [クリーン（Clean）] のファイルが含められることがありますが、それはそのファイルが最初マルウェアと識別されていた場合だけです。マルウェアとして識別されたことのないファイルは、ファイルのテーブルにのみ含められます。

エンドポイント向け AMP によって生成されたマルウェア イベント

所属部門がエンドポイント向けAMPを使用している場合、個々のユーザはエンドポイント（つまり、コンピュータやモバイルデバイス）に軽量コネクタをインストールします。コネクタでは、アップロード、ダウンロード、実行、オープン、コピー、移動などのときにファイルを検査できます。検査対象のファイルにマルウェアが含まれるかどうかを判断するために、これらのコネクタは AMP クラウドと通信します。

ファイルがマルウェアとして識別された場合、AMP クラウドは脅威の特定情報を Firepower Management Center に送ります。さらに AMP クラウドは、スキャン、検疫、実行のブロッキング、クラウドリコールなど、他の種類のデータを Firepower Management Center に送ることもできます。Firepower Management Center はこれらの情報をマルウェア イベントとしてログに記録します。

（注） エンドポイント向け AMP によって生成されたマルウェア イベントで報告される IP アドレスは、ネットワーク マップに（および監視対象ネットワークにも）含まれない場合もあります。展開、コンプライアンスのレベル、およびその他の要因によっては、AMP for Endpoints によってモニタされる組織内のエンドポイントが、ネットワーク向け AMP によってモニタされているものと同じホストではない可能性があります。

AMP for Endpoints を使用したマルウェア イベント分析

組織で Cisco AMP for Endpoints を導入している場合は、次のことができます。

- AMP for Endpoints によって検出されたマルウェア イベントを、AMP for Networks によって検出されたイベントとともに Firepower Management Center のイベント ページに表示するようにシステムを設定できます。
- AMP パブリック クラウドを使用している場合は、AMP for Endpoints の特定の SHA に関するファイル トラジェクトリやその他の情報を表示できます。

上記の機能を設定するには、Firepower と AMP for Endpoints の統合 （1956 ページ）を参照してください。

AMP for Endpoints からのイベントデータ

組織でマルウェア防御のために AMP for Endpoints を導入している場合は、AMP for Endpoints からのファイル データおよびマルウェア データを使用した作業を FMC 上で行えるようにシステムを設定できます。

ただし、AMP for Endpoints からのファイル データおよびマルウェア データと ネットワーク向け AMP （Firepower システムを使用したマルウェア防御）のファイル データおよびマルウェア データとの相違点に注意する必要があります。

管理対象デバイスはネットワーク トラフィックのマルウェアを検出しますが、エンドポイント向けAMPのマルウェア検出はダウンロード時または実行時にエンドポイントで行われるため、この 2 種類のマルウェア イベントの情報は異なります。たとえば、エンドポイントの AMP によって検出されたマルウェア イベントには、ファイル パス、呼び出し元クライアント アプリ

ケーションなどの情報が含まれるのに対して、ネットワーク トラフィックでのマルウェア検出には、ファイル伝送に使われた接続のポート、アプリケーション プロトコル、発信元 IP アドレス情報が含まれます。

その他にも、ネットワークベースの AMP によって検出されたマルウェア イベント（「ネットワークベースのマルウェア イベント」）の場合、ユーザ情報は、ネットワーク検出で判別された、マルウェアの送信先であるホストに最後にログインしたユーザを示すことが挙げられます。一方、エンドポイント向け AMP で報告されるユーザは、マルウェアが検出されたエンドポイントに現在ログインしているユーザを示します。

（注） 展開に応じて、AMP for Endpoints によってモニタされるエンドポイントは AMP for Networks でモニタされるものと同じホストにならない場合があります。このため、エンドポイント向け AMP によって生成されたマルウェア イベントはネットワーク マップにホストを追加しません。ただし、システムは IP アドレスおよび MAC アドレスのデータを使用して、AMP for Endpoints の展開から取得した侵害の兆候をモニタ対象のホストにタグ付けします。異なる AMP ソリューションによってモニタされる 2 つの異なるホストが同じ IP アドレスと MAC アドレスを持っている場合、システムは AMP for Endpoints の IOC をモニタ対象のホストに誤ってタグ付けする場合があります。

次の表に、マルウェア ライセンスを使用する場合に Firepower によって生成されるイベントデータと、AMP for Endpoints によって生成されるイベントデータの違いを要約します。

表 *342 : AMP* 製品間のデータの相違点の要約

機能	ネットワーク向け AMP	エンドポイント向け AMP
生成されるイベント	ファイルイベント、キャプチャされたファイル、マルウェアイベント、およびレトロスペクティブ マルウェア イベント	マルウェア イベント
マルウェア イベントに含まれる情報	基本的なマルウェアイベント情報、および接続データ（IP アドレス、ポート、アプリケーション プロトコル）	詳細なマルウェアイベント情報（接続データなし）
ネットワーク ファイル トラジェクトリ	FMC ベース	FMC と AMP for Endpoints の管理コンソールには、それぞれネットワーク ファイル トラジェクトリがあります。いずれも使用可能です。

関連項目

Firepower と AMP for Endpoints の統合 （1956 ページ）

ファイルおよびマルウェア イベントのワークフローの使用

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
機能に応じて異なる	機能に応じて異なる	いずれか（Any）	いずれか（Any）	Admin/Any Security Analyst

次の手順を使用して、テーブル内のファイルおよびマルウェア イベントを表示し、分析に関連する情報に基づいてイベント ビューを操作します。イベントにアクセスしたときに表示されるページは、ワークフローによって異なります。ワークフローは、大まかなビューから詳細なビューに移動してイベントを評価するために使用できる、一連のページです。また、特定のニーズを満たす情報だけを表示するカスタム ワークフローを作成することもできます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

次のいずれかを実行します。

- **[Analysis]** > **[Files]** > **[File Events]**
- **[Analysis]** > **[Files]** > **[Malware Events]**

ヒント　イベントのテーブル ビューでは、一部のフィールドがデフォルトで非表示にされています。イベント ビューに非表示フィールドを表示するには、検索制約を展開し、[無効にされたカラム（Disabled Columns）] の下のフィールド名をクリックします。

ヒント　特定のファイルが検出された接続をすぐに表示するには、テーブルでチェックボックスを使用してファイルを選択してから、[ジャンプ（Jump to）] ドロップダウン リストで [接続イベント（Connections Events）] を選択します。

ヒント　オプションを表示するには、テーブル内の項目を右クリックします（オプションが表示されない列もあります）。

関連トピック

ファイルおよびマルウェア イベント フィールド （3121 ページ）
定義済みファイルのワークフロー （2920 ページ）
定義済みマルウェアのワークフロー （2920 ページ）
イベント ビュー設定の設定 （43 ページ）

ファイルおよびマルウェア イベント フィールド

ワークフローを使用して表示および検索できるマルウェア イベントには、このセクションにリストするフィールドがあります。個別のイベントで利用可能な情報は、いつ、どのように生成されたかによって異なることに注意してください。

（注） ネットワーク向けAMP によってマルウェアとして識別されたファイルは、ファイルイベントとマルウェア イベントの両方を生成します。エンドポイント向け AMP によって生成されたマルウェア イベントには対応するファイル イベントはありません。また、ファイル イベントにはエンドポイント向け AMP 関連のフィールドはありません。

syslog メッセージにはメッセージに初期値が入力され、たとえば、レトロスペクティブな判定などでFMC Webインターフェイスの同等なフィールドが更新されたとしても更新されません。

[アクション（Action）]（syslog：FileAction）

ファイルを検出したファイル ポリシー ルールに関連したアクション、および関連するファイル アクション オプション。

AMP クラウド（AMP Cloud）

AMP for Endpoints イベントが発信された AMP クラウドの名前。

アプリケーション ファイル名（Application File Name）

AMP for Endpoints 検出が行われたときに、マルウェア ファイルにアクセスしていたクライアントアプリケーション。これらのアプリケーションはネットワーク検出またはアプリケーション制御とは関係**ありません**。

アプリケーション ファイル SHA256（Application File SHA256）

検出が行われたときに、AMP for Endpoints で検出された、または隔離されたファイルにアクセスした親ファイルの SHA-256 のハッシュ値。

[アプリケーション プロトコル（Application Protocol）]（syslog：ApplicationProtocol）

管理対象デバイスがファイルを検出したトラフィックで使用されるアプリケーション プロトコル。

アプリケーション プロトコル カテゴリまたはタグ（Application Protocol Category or Tag）

アプリケーションの機能を理解するのに役立つ、アプリケーションの特性を示す基準。

[アプリケーションのリスク（Application Risk）]

接続で検出されたアプリケーション トラフィックに関連するリスク：Very High、High、Medium、Low、または Very Low。接続で検出されたアプリケーションのタイプごとに、関連するリスクがあります。このフィールドでは、それらのうち最も高いものが表示されます。

[アーカイブの深さ（Archive Depth）]（syslog：ArchiveDepth）

アーカイブ ファイル内でファイルがネストされたレベル（存在する場合）。

[アーカイブ名（Archive Name）]（syslog：ArchiveFileName）

マルウェア ファイルが含まれていたアーカイブ ファイル（ある場合）の名前。

アーカイブ ファイルの内容を表示するには、[分析（Analysis）] >[ファイル（Files）] にある、アーカイブ ファイルの一覧が表示されるいずれかのテーブルに移動し、アーカイブ ファイルのテーブルの行を右クリックしてコンテキスト メニューを開いてから、[アーカイブの内容の表示（View Archive Contents）] をクリックします。

[SHA256 のアーカイブ（Archive SHA256）]（syslog：ArchiveSHA256）

マルウェア ファイルを含むアーカイブ ファイル（ある場合）の SHA-256 ハッシュ値。

アーカイブ ファイルの内容を表示するには、[分析（Analysis）]>[ファイル（Files）] にある、アーカイブ ファイルの一覧が表示されるいずれかのテーブルに移動し、アーカイブ ファイルのテーブルの行を右クリックしてコンテキスト メニューを開いてから、[アーカイブの内容の表示（View Archive Contents）] をクリックします。

ArchiveFileStatus（syslog のみ）

調査中のアーカイブのステータス。次のいずれかの値になります。

- [保留中（Pending）]：アーカイブは調査中です
- [取得済み（Extracted）]：調査が問題なく正常に実行されました
- [失敗（Failed）]：システムのリソース不足のため調査に失敗しました。
- [深度の超過（Depth Exceeded）]：調査は正常に実行されましたが、アーカイブがネストされた調査の深度を超過しました
- [暗号化（Encrypted）]：部分的に正常に実行されましたが、アーカイブが暗号化されているか、暗号化されたアーカイブが含まれています
- [調査できませんでした（Not Inspectable）]：部分的に正常に実行されましたが、ファイルは形式が不正であるか破損しています

ビジネスとの関連性（Business Relevance）

接続で検出されたアプリケーション トラフィックに関連するビジネス関連性：Very High、High、Medium、Low、または Very Low。接続で検出されたアプリケーションのタイプごとに、関連するビジネスとの関連性があります。このフィールドでは、それらのうち最も低いもの（関連が最も低い）が表示されます。

カテゴリ（Category）/ファイル タイプ カテゴリ（File Type Category）

ファイルタイプの一般的なカテゴリ（Office ドキュメント、アーカイブ、マルチメディア、実行可能ファイル、PDF ファイル、エンコード ファイル、グラフィック、システム ファイルなど）。

[クライアント（Client）]（syslog：Client）

1 つのホストで実行され、ファイルを送信するためにサーバに依存するクライアント アプリケーション。

クライアント カテゴリまたはタグ（Client Category or Tag）

アプリケーションの機能を理解するのに役立つ、アプリケーションの特性を示す基準。

（Syslog のみ）

ある接続と別の同時接続を区別するカウンタ。このフィールドは、それ自体には意味がありません。

[Sensor UUID]、[First Packet Time]、[Connection Instance ID]、および [Connection Counter] フィールドの情報を総合すると、特定のファイルまたはマルウェアイベントに関連付けられた接続イベントを一意に識別できます。

（Syslog のみ）

接続イベントを処理した Snort インスタンス。このフィールドは、それ自体には意味がありません。

[Sensor UUID]、[First Packet Time]、[Connection Instance ID]、および [Connection Counter] フィールドの情報を総合すると、特定のファイルまたはマルウェアイベントに関連付けられた接続イベントを一意に識別できます。

メンバー数（Count）

複数の同じ行を作成する制約を適用した後の、各行の情報に一致するイベントの数。

検出名（Detection Name）

検出されたマルウェアの名前。

ディテクタ（Detector）

マルウェアを識別した AMP for Endpoints ディテクタ（ClamAV、Spero、SHA など）。

Device

ネットワーク向け AMP によって生成されたファイル イベントとマルウェア イベントの場合は、ファイルを検出したデバイスの名前。

エンドポイント向け AMP によって生成されたマルウェア イベントと AMP クラウドによって生成されたレトロスペクティブ マルウェア イベントの場合は、Firepower Management Center の名前。

[後処理/ファイルの後処理（Disposition / File Disposition）]（syslog：SHA_Disposition）

ファイルの性質：

マルウェア（Malware）

AMP クラウドでそのファイルがマルウェアとして分類された、ローカル マルウェア分析でマルウェアとして識別された、またはファイル ポリシーで定義されたマルウェアしきい値をファイルの脅威スコアが超えたことを示します。

[クリーン（Clean）]

AMP クラウドでそのファイルがクリーンとして分類されているか、ユーザがファイルをクリーン リストに追加したことを示します。クリーンのファイルがマルウェア テーブルに含められるのは、そのファイルがクリーンに変更された場合だけです。

[不明（Unknown）]

システムが AMP クラウドに問い合わせましたが、ファイルの性質が割り当てられていませんでした。言い換えると、AMPクラウドがファイルを正しく分類していませんでした。

カスタム検出（Custom Detection）

ユーザがカスタム検出リストにファイルを追加したことを示します。

[応対不可（Unavailable）]

システムがAMPクラウドに問い合わせできなかったことを示します。この性質に関するイベントが、わずかながら存在する可能性があります。これは予期された動作です。

[該当なし（N/A）]

[ファイル検出（Detect Files）] または [ファイル ブロック（Block Files）] ルールがファイルを処理し、Firepower Management Center が AMP クラウドに問い合わせなかったことを示します。

ファイルの後処理は、システムが AMP クラウドにクエリを実行したファイルについてのみ表示されます。

syslog フィールドには最初の後処理のみが反映されます。レトロスペクティブな判定を反映するようには更新されません。

ドメイン

ネットワーク向け AMP によって生成されたファイル イベントとマルウェア イベントの場合は、ファイルを検出したデバイスのドメイン。エンドポイント向け AMP によって生成されたマルウェア イベントおよびAMP クラウドによって生成される遡及的マルウェア イベントの場合、イベントを報告した AMP クラウド接続に関連付けられたドメイン。

This field is only present if you have ever configured the Firepower Management Center for multitenancy.

DstIP（syslog のみ）

接続に応答したホストの IP アドレス。これは、FileDirection フィールドの値によってファイルの送信者または受信者の IP アドレスとなる場合があります。

FileDirection が **`Upload`** の場合、これはファイル受信者の IP アドレスです。

FileDirection が **`Download`** の場合、これはファイル送信者の IP アドレスです。

SrcIP も参照してください。

DstPort（syslog のみ）

DstIP で説明されている接続で使用されるポート。

イベント サブタイプ（Event Subtype）

マルウェア検出につながった AMP for Endpoints アクション（[作成（Create）]、[実行（Execute）]、[移動（Move）]、[スキャン（Scan）] など）。

イベント タイプ（Event Type）

マルウェア イベントのサブタイプ。

[ファイル名（File Name）]（syslog：FileName）

ファイルの名前。

ファイル パス（File Path）

AMP for Endpoints によって検出されたマルウェア ファイルのファイル パス（ファイル名を含まない）。

[ファイル ポリシー（File Policy）]（syslog：FilePolicy）

ファイルを検出したファイル ポリシー。

[ファイル ストレージ/保存済み（File Storage / Stored）]（syslog：FileStorageStatus）

イベントに関連付けられたファイルのストレージ ステータス：

保存（Stored）

関連するファイルが現在保存されているすべてのイベントを返します。

関連保存（Stored in connection）

関連するファイルが現在保存されているかどうかに関係なく、関連するファイルをシステムがキャプチャおよび保存したすべてのイベントを返します。

失敗しました（Failed）

関連するファイルをシステムが保存できなかったすべてのイベントを返します。

syslog フィールドには、初期のステータスのみが含まれています。これらのステータスは変更後のステータスを反映するようには更新されません。

ファイルのタイムスタンプ（File Timestamp）

AMP for Endpoints が検出したマルウェア ファイルが作成された日時。

FileDirection（syslog のみ）

接続中にファイルがダウンロードされたか、またはアップロードされたか。値は次のとおりです。

- Download：ファイルは DstIP から SrcIP に転送されました。
- Upload：ファイルは SrcIP から DstIP に転送されました。

FileSandboxStatus（syslog のみ）

ファイルが動的分析のために送信されたかとその場合のステータスを示します。

（Syslog のみ）

システムが最初のパケットを検出した時間。

[Sensor UUID]、[First Packet Time]、[Connection Instance ID]、および [Connection Counter] フィールドの情報を総合すると、特定のファイルまたはマルウェアイベントに関連付けられた接続イベントを一意に識別できます。

FirstPacketSecond（syslog のみ）

ファイルのダウンロード フローまたはアップロード フローが開始された時刻。

イベントが発生した時刻がメッセージ ヘッダーのタイムスタンプにキャプチャされます。

HTTP 応答コード（HTTP Response Code）

ファイルの転送時にクライアントの HTTP 要求に応じて送信される HTTP ステータス コード。

IOC

マルウェア イベントが、接続に関与したホストに対する侵入の痕跡（IOC）をトリガーしたかどうか。AMP for Endpoints データが IOC ルールをトリガーした場合、タイプ AMP IOC で、完全なマルウェア イベントが生成されます。

メッセージ（Message）

マルウェア イベントに関連付けられる追加情報。ファイル イベントおよびネットワーク向け AMP によって生成されたマルウェア イベントでは、このフィールドは、後処理が変更された、つまり関連付けられたレトロスペクティブ イベントがあるファイルに対してのみ入力されます。

Protocol（syslog のみ）

接続に使用されたプロトコル（TCP や UDP など）。

受信側の大陸（Receiving Continent）

ファイルを受信するホストの大陸。

受信側の国（Receiving Country）

ファイルを受信するホストの国。

受信側 IP（Receiving IP）

FMC の Web インターフェイスでは、次のようになります。

ファイルイベントおよびネットワーク向け AMP によって生成されたマルウェア イベントの場合、ファイルを受信するホストの IP アドレス。

エンドポイント向け AMP によって生成されたマルウェアのイベントの場合、コネクタがイベントを報告したエンドポイントの IP アドレス。

同等な syslog については（ネットワーク向け AMP のみ）、 **DstIP** と **SrcIP** を参照してください。

受信側のポート（Receiving Port）

FMC の Web インターフェイスでは、次のようになります。

ファイルが検出されたトラフィックによって使用される宛先ポート。

Syslog と同等なものについては、**DstIP** および **SrcIP** と **DstPort** および **SrcPort** を参照してください。

[セキュリティ コンテキスト（Security Context）]（syslog：Context）

トラフィックが通過した仮想ファイアウォール グループを識別するメタデータ。複数のコンテキスト モードで実行している 1 台以上の ASA FirePOWER デバイスを管理する場合、システムはこのフィールドのみを表示します。

送信側の大陸（Sending Continent）

ファイルを送信するホストの大陸。

送信側の国（Sending Country）

ファイルを送信するホストの国。

送信側 IP（Sending IP）

FMC の Web インターフェイス：ファイルを送信するホストの IP アドレス。

同等な syslog については、 **DstIP** と **SrcIP** を参照してください。

送信側のポート（Sending Port）

FMC の Web インターフェイスでは、次のようになります。

ファイルが検出されたトラフィックによって使用される送信元ポート。

同等な syslog については、**DstIP** および **SrcIP** と **DstPort** および **SrcPort** を参照してください。

（Syslog のみ）

イベントを生成した Firepower デバイスの一意の識別子。

[Sensor UUID]、[First Packet Time]、[Connection Instance ID]、および [Connection Counter] フィールドの情報を総合すると、特定のファイルまたはマルウェアイベントに関連付けられた接続イベントを一意に識別できます。

[SHA256/ファイル SHA256/（SHA256/File SHA256）]（syslog：FileSHA256）

ファイルの SHA-256 ハッシュ値。

SHA256 値を得るには、ファイルが次のいずれかによって処理されている必要があります。

- [ファイルの保存（Store files）] が有効になっているファイル検出ファイル ルール。
- [ファイルの保存（Store files）] が有効になっているファイル ブロック ファイル ルール。
- マルウェア クラウド ルックアップ ファイル ルール
- マルウェア ブロック ファイル ルール
- AMP for Endpoints

また、この列には最後に検出されたファイルイベントおよびファイルの後処理を表し、ネットワーク ファイル トラジェクトリにリンクするネットワーク ファイル トラジェクトリ アイコンも表示されます。

[サイズ（KB）/ファイル サイズ（KB）（Size (KB) / File Size (KB)）]（syslog：FileSize）

FMC の Web インターフェイス：ファイルのサイズ（バイト単位）。

In syslog messages: The size of the file, in bytes.

ファイルが完全に受信される前にシステムがファイルのタイプを特定した場合は、ファイルサイズが計算されない場合があります。この状況では、このフィールドは空白です。

SperoDisposition(Syslog のみ)

SPERO 署名がファイル分析で使用されたかどうかを示します。有効な値：

- ファイルで実行された Spero の検出
- ファイルで実行されなかった Spero の検出

SrcIP（syslog のみ）

接続を開始したホストの IP アドレス。これは、FileDirection フィールドの値によってファイルの送信者または受信者の IP アドレスとなる場合があります。

FileDirection が **`Upload`** の場合、これはファイル送信者の IP アドレスです。

FileDirection が **`Download`** の場合、これはファイル受信者の IP アドレスです。

DstIP も参照してください。

SrcPort（syslog のみ）

SrcIP で説明されている接続で使用されるポート。

[SSL の実際のアクション（SSL Actual Action）]（syslog：SSLActualAction）

システムが暗号化されたトラフィックに適用したアクション。

[ブロック（Block）] または [リセットしてブロック（Block with reset）]

ブロックされた暗号化接続を表します。

[復号（再署名）（Decrypt (Resign)）]

再署名サーバ証明書を使用して復号された発信接続を表します。

[復号（キーの交換）（Decrypt (Replace Key)）]

置き換えられた公開キーと自己署名サーバ証明書を使用して復号化された発信接続を表します。

[復号（既知のキー）（Decrypt (Known Key)）]

既知の秘密キーを使用して復号化された着信接続を表します。

[デフォルトアクション（Default Action）]

接続がデフォルト アクションによって処理されたことを示します。

[復号しない（Do not Decrypt）]

システムが復号化しなかった接続を表します。

フィールド値は、検索ワークフロー ページの [SSL ステータス（SSL Status）] フィールドに表示されます。

[SSL 証明書情報（SSL Certificate Information）]

トラフィックを暗号化するための公開キー証明書に保存される次の情報：

- サブジェクト/発行元共通名（Subject/Issuer Common Name）
- サブジェクト/発行元組織（Subject/Issuer Organization）
- サブジェクト/発行元組織単位（Subject/Issuer Organization Unit）
- 有効期間（Not Valid Before/After）
- シリアル番号（Serial Number）、証明書フィンガープリント（Certificate Fingerprint）
- 公開キー フィンガープリント（Public Key Fingerprint）

syslog の場合は、**SSLCertificate** を参照してください。

[SSL 失敗の理由（SSL Failure Reason）]（syslog：SSLFlowStatus）

システムが暗号化されたトラフィックの復号化に失敗した理由。

- 不明
- No Match
- Success
- Uncached Session
- 不明な暗号スイート
- サポートされていない暗号スイート
- Unsupported SSL Version
- SSL Compression Used
- Session Undecryptable in Passive Mode
- Handshake Error
- Decryption Error
- Pending Server Name Category Lookup
- Pending Common Name Category Lookup
- Internal Error
- Network Parameters Unavailable
- Invalid Server Certificate Handle
- Server Certificate Fingerprint Unavailable
- Cannot Cache Subject DN
- Cannot Cache Issuer DN
- Unknown SSL Version
- External Certificate List Unavailable
- External Certificate Fingerprint Unavailable
- Internal Certificate List Invalid
- Internal Certificate List Unavailable
- Internal Certificate Unavailable
- Internal Certificate Fingerprint Unavailable
- Server Certificate Validation Unavailable
- Server Certificate Validation Failure
- 無効なアクション（Invalid Action）

フィールド値は、検索ワークフローのページの [SSL ステータス（SSL Status）] フィールドに表示されます。

SSL ステータス（SSL Status）

暗号化接続をログに記録した [SSL の実際のアクション（SSL Actual Action）]（SSL ルール、デフォルトのアクション、または復号化できないトラフィック アクション）に関連付けられているアクション。ロック アイコン（  ）は、TLS/SSL 証明書の詳細にリンクしています。証明書を利用できない場合（たとえば、TLS/SSL ハンドシェイク エラーにより接続がブロックされる場合）、ロック アイコンはグレー表示になります。

システムが暗号化接続を復号できなかった場合は、[SSL の実際の動作（SSL Actual Action）]（実行された復号不能のトラフィック アクション）と、[SSL 失敗理由（SSL Failure Reason）] が表示されます。たとえば、不明な暗号スイートによって暗号化されたトラフィックをシステムが検出し、それ以上のインスペクションをせずにこれを許可した場合、このフィールドには [Do Not Decrypt (Unknown Cipher Suite)] が表示されます。

このフィールドを検索する場合は、[SSL の実際の動作（SSL Actual Action）] と [SSL 失敗理由（SSL Failure Reason）] の 1 つ以上の値を入力し、システムが処理した、または復号に失敗した暗号化トラフィックを表示します。

[SSL 件名/発行者の国（SSL Subject/Issuer Country）]

暗号化証明書に関連付けられた件名または発行元国の 2 文字の ISO 3166-1 alpha-2 国番号。

SSLCertificate（syslog のみ）

TLS/SSL サーバの証明書のフィンガープリント。

[脅威の名前（Threat Name）]（syslog：ThreatName）

検出されたマルウェアの名前。

[脅威スコア（Threat Score）]（syslog：ThreatScore）

このファイルに関連付けられている最新の脅威スコア。これは、動的分析中に観察された悪意がある可能性がある動作に基づいた 0 ～ 100 の値です。

脅威スコア アイコンは、[動的分析要約（Dynamic Analysis Summary）] レポートにリンクされています。

時刻（Time）

イベントが生成された日時。このフィールドは検索できません。

syslog メッセージでは、 **FirstPacketSecond** を参照してください。

[タイプ/ファイル タイプ（Type/File Type）]（syslog：FileType）

ファイルのタイプ（HTML や MSEXE など）。

[URI/ファイルURI（URI/File URI）]（syslog：URI）

ファイル トランザクションに関連付けられている接続のURI。たとえば、ユーザがファイルをダウンロードした URL など。

[ユーザ（User）]（syslog：User）

FMC の Web インターフェイスでは、次のようになります。

イベントが発生したホストに関連付られているユーザ名（**Receiving IP**）。

syslog メッセージでは、次のようになります。

ファイルをダウンロードした内部ホストに関連付けられているユーザ名。

ファイルイベントおよびネットワーク向けAMPによって生成されたマルウェアイベントの場合、このユーザはネットワーク検出によって判別されます。ユーザは宛先ホストに関連付けられているため、内部ホストがマルウェア ファイルをアップロードしたマルウェア イベントにユーザは関連付けられません。

エンドポイント向け AMP によって生成されたマルウェア イベントの場合、エンドポイント向け AMP がユーザ名を判別します。これらのユーザをユーザ検出または制御に関連付けることは**できません**。それらは [ユーザ（Users）] テーブルに含まれず、それらのユーザの詳細を表示することもできません。

[Web アプリケーション（Web Application）]（syslog：WebApplication）

接続で検出されたHTTPトラフィックについて、内容を表すまたはURLを要求したアプリケーション。

Web アプリケーションのカテゴリまたはタグ（Web Application Category or Tag）

アプリケーションの機能を理解するのに役立つ、アプリケーションの特性を示す基準。

マルウェア イベントのサブタイプ

次の表に、マルウェア イベントのサブタイプ、そのサブタイプは AMP for Networks によって生成されたマルウェア イベント（「ネットワークベースのマルウェア イベント」）または AMP for Endpoints によって生成されたマルウェア イベント（「エンドポイントベースのマルウェア イベント」）のどちらに該当するか、また、そのサブタイプを使用してネットワーク ファイル トラジェクトリが構築されるかどうかを一覧で示します。

表 *343 :* マルウェア イベントのタイプ

マルウェア イベントのサブタイプ/検索値	ネットワーク向け AMP	エンドポイント向け AMP	ファイル トラジェクトリ
ネットワーク ファイル転送時に検出された脅威（Threat Detected in Network File Transfer）	はい	いいえ	はい

マルウェア イベントのサブタイプ/検索値	ネットワーク向け **AMP**	エンドポイント向け **AMP**	ファイル トラジェクトリ
ネットワーク ファイル転送時に検出された脅威（遡及的）（Threat Detected in Network File Transfer (retrospective)）	はい	いいえ	はい
検出された脅威（Threat Detected）	いいえ	はい	はい
除外項目内で検出された脅威（Threat Detected in Exclusion）	いいえ	はい	はい
検疫された脅威（Threat Quarantined）	いいえ	はい	はい
AMP IOC（侵害の兆候）（AMP IOC (Indications of compromise)）	いいえ	はい	いいえ（No）
ブロックされた実行（Blocked Execution）	いいえ	はい	いいえ（No）
隔離のクラウドリコール（Cloud Recall Quarantine）	いいえ	はい	いいえ（No）
隔離のクラウドリコールの試行に失敗（Cloud Recall Quarantine Attempt Failed）	いいえ	はい	いいえ（No）
隔離のクラウドリコールの開始（Cloud Recall Quarantine Started）	いいえ	はい	いいえ（No）
隔離からのクラウドリコールの復元（Cloud Recall Restore from Quarantine）	いいえ	はい	いいえ（No）
隔離からのクラウドリコールの復元に失敗（Cloud Recall Restore from Quarantine Failed）	いいえ	はい	いいえ（No）

マルウェア イベントのサブタイプ/検索値	ネットワーク向け AMP	エンドポイント向け AMP	ファイル トラジェクトリ
隔離からのクラウドリコールの復元の開始（Cloud Recall Restore from Quarantine Started）	いいえ	はい	いいえ（No）
隔離エラー（Quarantine Failure）	いいえ	はい	いいえ（No）
隔離されたアイテムの復元（Quarantined Item Restored）	いいえ	はい	いいえ（No）
隔離の復元に失敗（Quarantine Restore Failed）	いいえ	はい	いいえ（No）
隔離の復元の開始（Quarantine Restore Started）	いいえ	はい	いいえ（No）
スキャン完了、検出なし（Scan Completed, No Detections）	いいえ	はい	いいえ（No）
スキャンが検出ありで完了（Scan Completed With Detections）	いいえ	はい	いいえ（No）
スキャンに失敗（Scan Failed）	いいえ	はい	いいえ（No）
スキャン開始（Scan Started）	いいえ	はい	いいえ（No）

ファイルおよびマルウェア イベント フィールドで利用可能な情報

次の表に、システムが各ファイルおよびマルウェア イベント フィールドの情報を表示するかどうかを示します。

組織で AMP for Endpoints が導入されていて、その製品を Firepower 展開と統合している場合は、次のようになります。

- エンドポイント向け AMP の展開からインポートされたマルウェア イベントと侵害の兆候（IOC）には、コンテキスト接続情報は含まれていませんが、ダウンロード時または実行時に取得された情報（ファイル パス、呼び出し元クライアント アプリケーションなど）が含まれています。
- ファイル イベント テーブル ビューには、エンドポイント向け AMP 関連のフィールドは表示されません。

表 *344 :* ファイルおよびマルウェア イベント フィールドで利用可能な情報

フィールド	ファイル イベント	Firepower システムによって検出されたマルウェア イベント	Firepower システムによって検出されたレトロスペクティブイベント	AMP for Endpoints によって検出されたマルウェア イベント
Action	はい	はい	はい	いいえ（No）
AMP クラウド（AMP Cloud）	いいえ	いいえ	いいえ	はい
アプリケーションファイル名（Application File Name）	いいえ	いいえ	いいえ	はい
アプリケーションファイル SHA256（Application File SHA256）	いいえ	いいえ	いいえ	はい
アプリケーションプロトコル	はい	はい	いいえ	いいえ
アプリケーションプロトコルカテゴリまたはタグ（Application Protocol Category or Tag）	はい	はい	はい	いいえ（No）
Application Risk	はい	はい	はい	いいえ（No）
アーカイブ深度（Archive Depth）	はい	はい	いいえ	はい
アーカイブ名（Archive Name）	はい	はい	いいえ	はい
アーカイブ SHA256（Archive SHA256）	はい	はい	いいえ	はい
ビジネス関連性	はい	はい	はい	いいえ（No）
カテゴリ/ファイル タイプ カテゴリ（Category / File Type Category）	はい	はい	いいえ	はい
クライアント	はい	はい	はい	いいえ（No）

フィールド	ファイル イベント	**Firepower** システムによって検出されたマルウェア イベント	**Firepower** システムによって検出されたレトロスペクティブイベント	**AMP for Endpoints** によって検出されたマルウェア イベント
クライアントカテゴリまたはタグ（Client Category or Tag）	はい	はい	はい	いいえ（No）
Count	はい	はい	はい	はい
検出名（Detection Name）	いいえ	はい	いいえ	いいえ
ディテクタ（Detector）	いいえ	いいえ	いいえ	はい
デバイス	はい	はい	はい	はい
性質/ファイル性質（Disposition / File Disposition）	はい	はい	はい	いいえ（No）
ドメイン（Domain）	はい	はい	はい	はい
イベント サブタイプ（Event Subtype）	いいえ	いいえ	いいえ	はい
イベント タイプ（Event Type）	いいえ	はい	はい	はい
ファイル名（File Name）	はい	はい	いいえ	はい
ファイル パス（File Path）	いいえ	いいえ	いいえ	はい
ファイル ポリシー（File Policy）	はい	いいえ	いいえ	いいえ
ファイルのタイムスタンプ（File Timestamp）	いいえ	いいえ	いいえ	はい
HTTP 応答コード（HTTP Response Code）	はい	はい	いいえ	いいえ

フィールド	ファイル イベント	**Firepower** システムによって検出されたマルウェア イベント	**Firepower** システムによって検出されたレトロスペクティブイベント	**AMP for Endpoints** によって検出されたマルウェア イベント
IOC（侵害の兆候）（IOC (Indication of Compromise)）	いいえ	はい	はい	はい
メッセージ（Message）	はい	はい	いいえ	はい
受信側の大陸（Receiving Continent）	はい	はい	はい	いいえ（No）
受信側の国（Receiving Country）	はい	はい	いいえ	いいえ
受信側 IP（Receiving IP）	はい	はい	いいえ	はい
受信側のポート（Receiving Port）	はい	はい	いいえ	いいえ
セキュリティコンテキスト（Security Context）	はい	はい	はい	はい
送信側の大陸（Sending Continent）	はい	はい	はい	いいえ（No）
送信側の国（Sending Country）	はい	はい	いいえ	いいえ
送信側 IP（Sending IP）	はい	はい	いいえ	いいえ
送信側のポート（Sending Port）	はい	はい	いいえ	いいえ
SHA256/ファイル SHA256（SHA256 / File SHA256）	はい	はい	はい	はい
サイズ（KB）/ファイルサイズ（KB）（Size (KB) / File Size (KB)）	はい	はい	いいえ	はい

フィールド	ファイル イベント	Firepower システムによって検出されたマルウェア イベント	Firepower システムによって検出されたレトロスペクティブイベント	AMP for Endpoints によって検出されたマルウェア イベント
SSL の実際のアクション（SSL Actual Action）（検索のみ）	はい	はい	いいえ	いいえ
SSL 証明書情報（SSL Certificate Information）（検索のみ）	はい	はい	いいえ	いいえ
SSL 障害の理由（SSL Failure Reason）（検索のみ）	はい	はい	いいえ	いいえ
SSL Status	はい	はい	いいえ	いいえ
SSL 件名/発行者の国（SSL Subject/Issuer Country）（検索のみ）	はい	はい	いいえ	いいえ
ファイル ストレージ/保存済み（File Storage / Stored）（検索のみ）	はい	はい	いいえ	いいえ
脅威名（Threat Name）	いいえ	はい	はい	はい
脅威スコア（Threat Score）	はい	はい	いいえ	いいえ
時刻	はい	はい	はい	はい
タイプ/ファイル タイプ（Type / File Type）	はい	はい	いいえ	はい
URI/ファイル URI（URI / File URI）	はい	はい	いいえ	いいえ
ユーザ（User）	はい	はい	いいえ	はい
Web アプリケーション	はい	はい	はい	いいえ（No）
Web アプリケーション カテゴリまたはタグ（Web Application Category or Tag）	はい	はい	はい	いいえ（No）

分析されたファイルに関する詳細の表示

ヒント　追加のオプションを表示するには、イベント ページのテーブルでファイルの SHA を右クリックします。詳細については、Webベースのリソースを使用したイベントの調査（2890ページ）を参照してください。

ファイル構成レポート

ローカルマルウェアの分析または動的分析を設定すると、ファイルの分析後にファイル構成レポートが生成されます。このレポートを使用して、ファイルをさらに分析し、ファイルにマルウェアが組み込まれているかどうかを判断することができます。

ファイル構成レポートでは、ファイルのプロパティ、ファイルに組み込まれているオブジェクト、および検出されたウイルスが示されます。また、ファイル構成レポートでは、そのファイルタイプに固有の追加情報が示される場合があります。保存されているファイルのプルーニング時に、関連ファイル構成レポートもプルーニングされます。

ファイル構成の情報を表示するには、ネットワーク ファイル トラジェクトリの使用（3155ページ）を参照してください。

AMP プライベート クラウドでのファイルの詳細の表示

AMP プライベート クラウドを導入している場合は、プライベート クラウドで分析されたファイルに関する追加の詳細を表示できます。

詳細については、お使いのプライベート クラウドのマニュアルを参照してください。

AMP プライベート クラウドのコンソールに直接サインインします。

脅威スコアと動的分析のサマリ レポート

脅威スコア

表 *345 :* 脅威スコア レーティング

脅威スコア	アイコン
Low	
Medium	

脅威スコア	アイコン
High	
Very High	

Firepower Management Center は、ファイルの性質と同じ期間だけ、ファイルの脅威スコアをキャッシュに入れます。これらのファイルが後から検出されると、Cisco Threat Grid クラウドまたは Cisco Threat Grid オンプレミス アプライアンスにもう一度クエリが実行される代わりに、キャッシュされた脅威スコアが表示されます。ファイルの脅威スコアが、定義済みのマルウェアしきい値の脅威スコアを超える場合は、そのファイルにマルウェアの性質を自動的に割り当てることができます。

動的分析のサマリ

動的分析のサマリが生成可能な場合、脅威スコアアイコンをクリックすると、サマリが表示されます。複数のレポートが存在する場合、このサマリは、脅威スコアと完全に一致する最新のレポートに基づいて生成されます。完全に一致する脅威スコアがない場合、最も高い脅威スコアに関するレポートが表示されます。複数のレポートがある場合は、脅威スコアを選択して、それぞれのレポートを表示することができます。

サマリには、脅威スコアを構成する各コンポーネントの脅威がリストされます。各コンポーネントの脅威を展開すると、そのコンポーネントの脅威に関連するプロセスだけでなく、AMP クラウドの調査結果もリストされます。

プロセス ツリーには、Cisco Threat Grid クラウドがファイルを実行しようとしたときに開始されたプロセスが示されています。これは、マルウェアを含むファイルが、想定外のプロセスやシステム リソースへアクセスしようとしているかどうか（たとえば、Word ドキュメントを実行すると、Microsoft Word が開き、次に Internet Explorer が起動し、さらに Java Runtime Environment が実行されるなど）を識別するのに役立ちます。

リストされる各プロセスには、実際のプロセスを検査するのに使用できるプロセス ID が含まれます。プロセス ツリー内の子ノードは、親プロセスの結果として開始されたプロセスを表します。

動的分析のサマリから [完全なレポートを表示（View Full Report）] をクリックすることにより、AMP クラウドの完全な分析を詳述する完全版分析レポートを表示できます。レポートには、ファイルの一般情報、検出されたすべてのプロセスの詳細な説明、ファイル分析の概要、およびその他の関連情報が含まれます。

Cisco Threat Grid パブリック クラウドの動的分析結果の表示

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス（Access）
マルウェア	マルウェア	いずれか（Any）	グローバルだけ	Admin/Access Admin/Network Admin

Cisco Threat Grid 分析されたファイルに関して、Firepower Management Center で使用できるレポートよりもさらに詳細なレポートが提供されます。組織に Cisco Threat Grid パブリック クラウドのアカウントがあれば、Cisco Threat Grid ポータルに直接アクセスして、管理対象デバイスから分析のために送信されたファイルに関する追加の詳細を表示することができます。

始める前に

Firepower Management Center を Cisco Threat Grid パブリック クラウド アカウントに関連付けます。パブリック クラウドでの動的分析の結果へのアクセスの有効化（1927 ページ）を参照してください。

ステップ 1 Threat Grid ドキュメントで提供されるアドレスで、Cisco Threat Grid パブリック クラウドのポータルにアクセスします。

ステップ 2 このタスクへの前提条件で関連付けを作成するために使用したアカウントの資格情報を使用してログインします。

ステップ 3 組織によって送信されたファイルを表示するか、SHA を使用して特定のファイルを検索します。

不明な点がありましたら、Threat Grid ドキュメントを参照してください。

キャプチャされたファイル ワークフローの使用

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
機能に応じて異なる	機能に応じて異なる	いずれか（Any）	いずれか（Any）	Admin/Any Security Analyst

管理対象デバイスは、ネットワーク トラフィックで検出されたファイルをキャプチャすると、イベントをログに記録します。

（注） デバイスがマルウェアを含むファイルをキャプチャすると、デバイスは、ファイルを検出した場合はファイル イベント、マルウェアを識別した場合はマルウェア イベントの 2 種類のイベントを生成します。

次の手順を使用して、テーブル内のキャプチャ ファイルの一覧を表示し、分析に関連する情報に基づいてイベント ビューを操作します。キャプチャ ファイルにアクセスしたときに表示されるページは、ワークフローによって異なります。ワークフローは、大まかなビューから詳細なビューに移動してイベントを評価するために使用できる、一連のページです。また、特定のニーズを満たす情報だけを表示するカスタム ワークフローを作成することもできます。

ファイルポリシーの更新など設定を変更した後に、システムがファイルを再キャプチャする場合、そのファイルの既存の情報が更新されます。

たとえば、[マルウェア クラウド ルックアップ（Malware Cloud Lookup）] アクションを使用してファイルをキャプチャするようにファイル ポリシーを設定した場合、システムはそのファイルと一緒にファイル処理と脅威スコアを保存します。その後、ファイル ポリシーを更新し、新しい [ファイルの検出（Detect Files）] アクションのためにシステムが同じファイルを再キャプチャすると、システムはファイルの [最終変更時刻（Last Changed）] の値を更新します。ただし、別のマルウェア クラウド ルックアップを実行しなかったとしても、システムは既存の処理や脅威スコアを削除しません。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

[Analysis] > **[Files]** > **[Captured Files]**を選択します。

ヒント イベントのテーブル ビューでは、一部のフィールドがデフォルトで非表示にされています。イベント ビューに非表示フィールドを表示するには、検索制約を展開し、[無効にされたカラム（Disabled Columns）] の下のフィールド名をクリックします。

関連トピック

キャプチャされたファイルのフィールド （3143 ページ）
定義済みキャプチャ ファイルのワークフロー （2921 ページ）
イベント ビュー設定の設定 （43 ページ）

キャプチャされたファイルのフィールド

キャプチャされたファイルのテーブル ビューは、定義済みファイル イベントのワークフローの最後のページであり、カスタム ワークフローに追加できます。このテーブル ビューには、ファイル テーブルの各フィールドの列が含まれます。

このテーブルを検索する場合、検索結果は、検索対象のイベントで使用可能なデータによって決まることに留意してください。使用可能なデータによって、検索の制約が適用されないことがあります。たとえば、ダイナミック分析のためにファイルが送信されていない場合は、関連する脅威スコアがない可能性があります。

表 *346 :* キャプチャされたファイルのフィールド

フィールド	説明
アーカイブ検査ステータス（Archive Inspection Status）	アーカイブ ファイルのアーカイブ検査ステータスであり、次のいずれかになります。 • [保留中（Pending）] は、システムがアーカイブ ファイルとその内容をまだ検査していることを示します。ファイルが再びシステムを通過すると、完全な情報が使用可能になります。 • [抽出済み（Extracted）] は、アーカイブの内容を抽出し、検査できたことを示します。 • [失敗（Failed）] は、まれなケースですが、システムが抽出を処理できない場合に発生します。 • [深さ超過（Depth Exceeded）] は、許可されている最大深さを超えるネストされたアーカイブ ファイルがアーカイブに含まれていることを示します。 • [暗号化（Encrypted）] は、アーカイブ ファイルの内容が暗号化されていて、検査できなかったことを示します。 • [検査不可（Not Inspectable）] は、システムがアーカイブの内容を抽出して検査しなかったことを示しています。このステータスの主な理由としては、ポリシー ルール アクション、ポリシー設定、破損ファイルの 3 つがあります。 アーカイブ ファイルの内容を表示するには、表で該当の行を右クリックしてコンテキスト メニューを開いてから、[アーカイブの内容の表示（View Archive Contents）] を選択します。
カテゴリ	ファイル タイプの一般的なカテゴリ（Office ドキュメント、アーカイブ、マルチメディア、実行可能ファイル、PDF ファイル、エンコード ファイル、グラフィック、システム ファイルなど）。
検出名（Detection Name）	検出されたマルウェアの名前。

フィールド	説明
傾向（Disposition）	ファイルの ネットワーク向け AMP での性質： • [マルウェア（Malware）] は、ファイルがローカルのマルウェア分析でマルウェアとして認識され、クラウドでマルウェアとして分類されていること、または、ファイルの脅威スコアが、ファイル ポリシーで定義されたマルウェアしきい値を超えていることを示します。 • [クリーン（Clean）] は、ファイルが AMP クラウドでクリーンとして分類されていること、または、ファイルをユーザがクリーン リストに追加したことを示します。 • [不明（Unknown）] は、システムが AMP クラウドに問い合わせましたが、ファイルの傾向が割り当てられていないこと、つまり、ファイルが AMP クラウドで正しく分類されていないことを示します。 • [カスタム検出（Custom Detection）] は、ファイルをユーザがカスタム検出リストに追加したことを示します。 • [使用不可（Unavailable）] は、システムが AMP クラウドに問い合わせできなかったことを示します。この性質を持つイベントはごくわずかである可能性があります。これは予期された動作です。 • [N/A] は、[ファイルを検出する（Detect Files）] または [ファイルをブロックする（Block Files）] ルールによってファイルが処理され、Firepower Management Center が AMP クラウドに問い合わせなかったことを示します。
ドメイン（Domain）	キャプチャされたファイルが検出されたドメイン。 This field is only present if you have ever configured the Firepower Management Center for multitenancy.

フィールド	説明
動的分析ステータス（Dynamic Analysis Status）	

フィールド	説明
	ファイルが動的分析のために送信されたかどうかを示すものであり、次の値のうちの 1 つ以上が表示されます。 • [分析完了（Analysis Complete）]：ファイルがダイナミック分析のために送信され、脅威スコアおよびダイナミック分析のサマリー レポートを受け取りました。 • [処理予定の容量（Capacity Handled）]：送信できなかったため、ファイルが保存されました。 • [処理予定の容量（ネットワークの問題）（Capacity Handled (Network Issue)）]：ネットワーク接続の問題が原因で送信できなかったため、ファイルが保存されました。 • [処理予定の容量（レート制限）（Capacity Handled (Rate Limit)）]：最大数に達したことが原因で送信できなかったため、ファイルが保存されました。 • [非アクティブなデバイス（Device Not Activated）]：デバイスがオンプレミスの Cisco Threat Grid アプライアンスでアクティブになっていないため、ファイルが送信されません。このステータスが表示された場合は、サポート担当に連絡してください。 • [失敗（分析タイムアウト）（Failure (Analysis Timeout)）]：ファイルが送信されましたが、まだ AMP から結果が返されていません。 • [失敗（ファイル実行不可）（Failure (Cannot Run File)）]：ファイルが送信されましたが、AMP クラウドがテスト環境でファイルを実行できませんでした。 • [失敗（ネットワークの問題）（Failure (Network Issue)）]：ネットワーク接続の問題のため、ファイルが送信されませんでした。 • [分析のための送信なし（Not Sent for Analysis）]：ファイルが送信されませんでした。 • [疑わしくないファイル（分析のための送信なし）（Not Suspicious (Not Sent For Analysis)）]：ファイルがマルウェアではないものとして事前に分類されています。 • [以前に分析済み（Previously Analyzed）]：キャッシュされた脅威スコアがあるファイルをユーザが再び送信しようとしました。 • [分析のために送信（Sent for Analysis）]：ファイルが

フィールド	説明
	マルウェアとして事前に分類されており、ダイナミック分析のためにキューに入れられました。
ダイナミック分析ステータスの変更（Dynamic Analysis Status Changed）	前回、ファイルのダイナミック分析のステータスが変更された日時。
ファイル名	ファイルの SHA-256 ハッシュ値に関連付けられているものとして最後に検出されたファイル名。
前回の変更（Last Changed）	このファイルに関連する情報が最後に更新された時刻。
最終送信日時（Last Sent）	ファイルが動的分析のために AMP クラウドに最後に送信された時刻。
ローカル マルウェア分析ステータス（Local Malware Analysis Status）	ローカル マルウェア分析が実行されたかどうかを示すものであり、次のいずれかになります。 • [分析完了（Analysis Complete）]：ローカル マルウェア分析を使用してファイルが検査され、事前に分類されました。 • [分析失敗（Analysis Failed）]：ローカルマルウェア分析を使用してファイルを検査しようとし、失敗しました。 • [手動による要求の送信（Manual Request Submitted）]：ユーザがローカル マルウェア分析のためにファイルを送信しました。 • [分析なし（Not Analyzed）]：システムでローカル マルウェア分析を使用してファイルが検査されませんでした。
SHA256	ファイルの SHA-256 ハッシュ値と、最後に検出されたファイルイベントおよびファイル性質を表すネットワーク ファイル トラジェクトリ アイコン。ネットワーク ファイル トラジェクトリを表示するには、トラジェクトリ アイコンをクリックします。
ストレージ ステータス（Storage Status）	ファイルが管理対象デバイスに保存されているかどうかを示し、次のいずれかになります。 • ファイル保存済み（File Stored） • 保存なし（性質分析の保留）（Not Stored (Disposition Was Pending)）

フィールド	説明
脅威スコア（Threat Score）	このファイルに関連付けられている最新の脅威スコア。 ダイナミック分析のサマリー レポートを表示するには、脅威スコア アイコンをクリックします。
タイプ	ファイルのタイプ（HTML や MSEXE など）。

保存されているファイルのダウンロード

デバイスによって保存されたファイルは、Firepower Management Center がそのデバイスと通信可能であり、ファイルが削除されていない限り、長期間保存し分析するためにローカル ホストにダウンロードし、手動でファイルを分析できます。関連ファイル イベント、マルウェア イベント、キャプチャ ファイル ビュー、またはファイルのトラジェクトリからファイルをダウンロードできます。

マルウェアによる被害を防ぐため、デフォルトでは、ファイルのダウンロードのたびに確認を行う必要があります。ただし、この確認は [ユーザ設定（User Preferences）] で無効にすることもできます。

性質が使用不可のファイルにはマルウェアが含まれている可能性があるため、ファイルをダウンロードすると、システムはまずそのファイルを .zip パッケージにアーカイブします。.zip ファイル名には、ファイルの性質とファイル タイプ（存在する場合）さらに SHA-256 ハッシュ値が含まれます。誤って解凍してしまわないように、.zip ファイルをパスワードで保護できます。.zip ファイルのデフォルト パスワードは、[ユーザ設定（User Preferences）] で編集または削除できます。

⚠

注意 シスコでは、有害な結果が発生することがあるため、マルウェアをダウンロード**しない**ように強くお勧めします。ファイルをダウンロードする際は、マルウェアが含まれている可能性があるので注意してください。ファイルをダウンロードする前に、ダウンロード先を保護するために必要な予防措置を行っていることを確認します。

分析用ファイルの手動での送信

分析用ファイルを手動で送信すると、システムはローカル分析を実行してから、それらのファイルを動的分析対象としてクラウドに送信します。ただし、ローカル分析がファイル ポリシーで有効になっておらず、分析用のファイルを手動で送信する場合は、ファイルが動的分析用としてしか送信されません。

実行可能ファイルの他に、自動送信に適格ではないファイル タイプ（.swf、.jar など）も送信できます。これにより、ファイルの性質に関わらず、さまざまなファイルをより迅速に分析し、問題の正確な原因を突き止めることができます。

（注） 動的分析に適格なファイル タイプのリストと送信可能な最小および最大のファイル サイズに関して更新がないか、システムは AMP クラウドを検査します（この検査は、一日に 1 回だけ行われます）。

分析用ファイルを送信する方法は、状況により、次の 2 種類があります。

始める前に

分析用にキャプチャしたファイルを手動で送信するには、ファイルを保存するように1つまたは複数のファイル ルールを設定する必要があります。詳細については、ファイル ポリシーと高度なマルウェア防御 （1911 ページ）を参照してください。

ステップ 1 1 つの分析用ファイルを送信する場合：

a) 次のいずれかを選択します。

- **[分析（Analysis）] > [ファイル（Files）] > [ファイルイベント（File Events）]**
- **[分析（Analysis）] > [ファイル（Files）] > [マルウェアイベント（Malware Events）]**
- **[分析（Analysis）] > [ファイル（Files）] > [キャプチャファイル（Captured Files）]**

b) <イベント タイプまたはファイル> の [テーブルビュー（Table View）] をクリックします。

c) テーブル内のファイルを右クリックし、[ファイルの分析（Analyze file）] を選択します。

ステップ 2 複数のキャプチャした分析用ファイルを送信する場合（一度に最大 25 ファイル）：

a) [分析（Analysis）] > [ファイル（Files）] > [キャプチャファイル（Captured Files）] を選択します。

b) 分析する各ファイルの横にあるチェック ボックスをオンにします。

c) [Analyze（分析）] をクリックします。

ネットワーク ファイル トラジェクトリ

ネットワーク ファイルのトラジェクトリ機能は、ネットワーク全体でホストがどのようにファイル（マルウェア ファイルを含む）を転送したかをマッピングします。トラジェクトリは、ファイル転送データ、ファイルの性質、ファイル転送がブロックされたかどうか、ファイルが隔離されたかどうかをグラフに示します。これにより、マルウェアを転送したおそれのあるホストおよびユーザやリスクがあるホストがどれであるかを判定したり、ファイル転送の傾向を観測したりできます。

AMP クラウドで性質が割り当てられているファイルであれば、どのファイルの送信でも追跡できます。システムは、ネットワーク向け AMP と AMP for Endpoints の両方によるマルウェアの検出およびブロック情報を使用して、トラジェクトリを作成します。

最近検出されたマルウェアおよび分析済みトラジェクトリ

[ネットワーク ファイル トラジェクトリ リスト（Network File Trajectory List）] ページには、ネットワークで最近検出されたマルウェアと最後に表示したトラジェクトリ マップのファイルが表示されます。これらのリストから、ネットワークで各ファイルが最後に発見されたのはいつか、ファイルのSHA-256のハッシュ値、名前、タイプ、現在のファイルの性質、内容（アーカイブ ファイルの場合）、ファイルに関連付けられたイベント数を確認できます。

また、このページに含まれる検索ボックスを使用して、SHA-256ハッシュ値またはファイル名を基準に、あるいはファイルを送信または受信するホストの IP アドレスによってファイルを見つけることができます。ファイルを見つけた後、[ファイル SHA256（File SHA256）] 値をクリックすると詳細なトラジェクトリ マップが表示されます。

ネットワーク ファイル トラジェクトリの詳細ビュー

詳細なネットワーク ファイル トラジェクトリを表示して、ネットワーク全体でファイルを追跡できます。ファイルの SHA 256 値を検索するか、[ネットワーク ファイル トラジェクトリ（Network File Trajectory）] リスト内の [ファイルの SHA 256（File SHA 256）] リンクをクリックして、そのファイルに関する詳細を表示します。

ネットワーク ファイル トラジェクトリの詳細ページには、3 つの部分があります。

- サマリー情報：ファイルのトラジェクトリ ページには、ファイルに関するサマリー情報（ファイル識別情報、ネットワーク上でファイルが最初に表示された時間および最後に表示された時間と表示したユーザ、ファイルに関連したイベントおよびホストの数、ファイルの現在の性質など）が表示されます。このセクションから、管理対象デバイスがファイルを保存した場合に、そのファイルをローカルにダウンロードしたり、ファイルを動的分析用に送信したり、ファイルをファイル リストに追加したりできます。
- トラジェクトリー マップ：ファイルのトラジェクトリ マップは、ネットワークで最初に検出された時点から直近までファイルを視覚的に追跡します。このマップは、ホストがファイルを転送または受信した時点、ファイルを転送した頻度、ファイルがブロックまたは隔離された時点を示します。データ ポイント間の縦線は、ホスト間のファイル転送を表します。データ ポイントをつなぐ横棒は、時間の経過に応じたホストのファイルアクティビティを示します。

  また、そのファイルでファイルイベントが発生した頻度や、システムがファイルに性質または遡及的性質を割り当てた時点についても示します。マップでデータ ポイントを選択し、ホストがそのファイルを転送した最初のインスタンスに遡るパスを強調表示できます。また、このパスは、ファイルの送信側または受信側としてホストが関与する各オカレンスと交差します。このパスにより、関与するユーザが識別されます。
- 関連イベント：[イベント（Events）] テーブルに、マップ内の各データ ポイントに関するイベント情報がリストされます。テーブルおよびマップを使用して、特定のファイルイベント、このファイルを転送または受信したネットワーク上のホストとユーザ、マップ内の関連するイベント、選択した値で制限されたテーブル内の他の関連するイベントを特定することができます。

ネットワーク ファイル トラジェクトリのサマリー情報

次の概要情報は、ネットワーク ファイル トラジェクトリのリストに表示されるファイルの詳細ページの上部に表示されます。

ヒント　関連するファイルイベントを表示するには、フィールド値のリンクをクリックします。ファイルイベントのデフォルトのワークフローの最初のページが新しいウィンドウで開き、選択した値を含むすべてのファイル イベントも表示されます。

表 *347:* ネットワーク ファイル トラジェクトリのサマリー情報フィールド

名前	説明
コンテンツのアーカイブ（Archive Contents）	検査されたアーカイブ ファイルで、アーカイブに含まれているファイルの数。
現在の性質（Current Disposition）	次のいずれかのネットワーク向けAMP ファイルの性質です。 • [マルウェア（Malware）]：AMP クラウドでそのファイルがマルウェア、マルウェアによって識別されるローカルマルウェア分析として分類されていること、またはファイルの脅威スコアが、ファイル ポリシーで定義されたマルウェアしきい値を超えていることを示します。 • [クリーン（Clean）]：AMP クラウドでそのファイルがクリーンとして分類されているか、ユーザがファイルをクリーン リストに追加したことを示します。 • [不明（Unknown）]：システムが AMP クラウドに問い合わせましたが、ファイルの性質が割り当てられていませんでした。言い換えると、AMPクラウドがファイルを正しく分類していませんでした。 • カスタム検出（Custom Detection）：ユーザがカスタム検出リストにファイルを追加したことを示します。 • 利用不可（Unavailable）：システムが AMP クラウドでクエリを行えなかったことを示します。この性質を持つイベントはごくわずかである可能性があります。これは予期された動作です。 • [該当なし（N/A）]：[ファイル検出（Detect Files）] または [ファイル ブロック（Block Files）] ルールがファイルを処理し、Firepower Management Center がAMPクラウドに問い合わせなかったことを示します。

名前	説明
検出名（Detection Name）	ローカル マルウェア分析によって検出されたマルウェアの名前。
イベント カウント（Event Count）	ファイルに関連付けられたネットワークで発見されたイベントの数、検出されたイベントの数が 250 を超える場合は、マップに表示されるイベントの数。
ファイル カテゴリ（File Category）	ファイル タイプの一般的なカテゴリ（`Office Documents` や `System Files` など）。
ファイル名（File Names）	ネットワーク上で発見された、イベントに関連したファイルの名前。 複数のファイル名が SHA-256 ハッシュ値に関連付けられている場合、最後に検出されたファイル名がリストされます。[詳細（more）] をクリックすると、これが展開されて、残りのファイル名が表示されます。
File SHA256	ファイルの SHA-256 ハッシュ値。 デフォルトで、ハッシュは簡略化された形式で表示されます。完全なハッシュ値を表示するには、その上にポインタを移動させます。複数の SHA-256 ハッシュ値がファイル名に関連付けられている場合、リンクの上にポインタを移動されると、すべてのハッシュ値が表示されます。
[ファイル サイズ（File Size）（KB）]	ファイルのサイズ（KB 単位）。
ファイル タイプ（File Type）	ファイルのタイプ（`HTML` や `MSEXE` など）。
最初の確認日時（First Seen）	ネットワーク向け AMP または AMP for Endpoints による初めてのファイル検出に加えて、ファイルを初めてアップロードしたホストの IP アドレス、および関与するユーザの識別情報。
最終表示（Last Seen）	ネットワーク向け AMP または AMP for Endpoints による最新のファイル検出に加えて、ファイルを最後にダウンロードしたホストの IP アドレス、および関与するユーザの識別情報。
親アプリケーション（Parent Application）	エンドポイント向け AMP による検出が行われたときに、マルウェア ファイルにアクセスしていたクライアント アプリケーション。これらのアプリケーションはネットワーク検出またはアプリケーション制御とは関係**ありません**。

名前	説明
表示日（Seen On）	ファイルを送信または受信したホストの数。1 つのホストが 1 つのファイルのアップロードおよびダウンロードを時を異にして行う場合があるため、ホストの合計数が、[Seen On Breakdown] フィールドの送信側の総数と受信側の総数の合計と一致しないことがあります。
Seen On Breakdown	ファイルを送信したホストの数とファイルを受信したホストの数。
脅威名（Threat Name）	エンドポイント向け AMP によって検出されたマルウェアに関連付けられている脅威の名前。
脅威スコア（Threat Score）	ファイルの脅威スコア。

ネットワーク ファイル トラジェクトリ マップと関連イベント リスト

ファイル トラジェクトリ マップの Y 軸には、ファイルと対話したすべてのホストの IP アドレスがリストされます。IP アドレスは、システムがそのホストでファイルを最初に検出した時点に基づいて降順でリストされます。各行には、その IP アドレスに関連付けられたすべてのイベント（単一のファイル イベント、ファイル転送、遡及的イベント）が含まれます。X 軸には、システムが各イベントを検出した日時が含まれます。タイムスタンプは時間順にリストされます。複数のイベントが 1 分以内に発生する場合、すべてが同じ列内にリストされます。マップを左右および上下にスクロールして、イベントおよび IP アドレスをさらに表示できます。

マップには、ファイルの SHA-256 ハッシュに関連した最大 250 のイベントが表示されます。イベントが 250 を超える場合、マップには最初の 10 個が表示され、余分のイベントは省略されて矢印アイコン（  ）が示されます。その後ろに、マップは残りの 240 個のイベントを表示します。

デフォルトの [File Events（ファイル イベント）] ワークフローの最初のページが新しいウィンドウで開き、ファイル タイプに基づいて制限されて、すべての余分のイベントが表示されます。エンドポイント向け AMP によって生成されたマルウェア イベントが表示されない場合、[マルウェア イベント（Malware Events）] テーブルに切り替えてそれらを表示する必要があります。

各データ ポイントは、イベントの他にファイル性質を表しています。マップの下の凡例を参照してください。たとえば、[マルウェア ブロック（Malware Block）] イベント アイコンは、[悪意のある性質（Malicious Disposition）] アイコンと [ブロック イベント（Block Event）] アイコンを結合したものです。

エンドポイント向け AMP によって生成されたマルウェア イベント（「エンドポイントベースのマルウェア イベント」）には 1 つのアイコンが含まれています。レトロスペクティブ イベントでは、ファイルで検出された各ホストのコラムにアイコンが表示されます。ファイル転送イベントでは、縦線でつながれた 2 つのアイコン（ファイル送信アイコンとファイル受信アイコン）が常に含まれます。矢印は、送信側から受信側へのファイル転送方向を示します。

ネットワークを介したファイルの進行状況を追跡するために、データ ポイントをクリックして、選択したデータ ポイントに関連するすべてのデータ ポイントを含むパスを強調表示できます。これには、次のタイプのイベントに関連付けられたデータ ポイントが含まれます。

- 関連付けられている IP アドレスが送信側または受信側だったファイル転送
- 関連付られた IP アドレスを含めて、エンドポイント向け AMP によって生成されたマルウェア イベント（「エンドポイントベースのマルウェア イベント」）
- 別の IP アドレスが関係する場合、その関連する IP アドレスが送信側または受信側であったすべてのファイル転送
- 別の IP アドレスが関係していた場合、その他方の IP アドレスが関係するエンドポイント向け AMP によって生成されたマルウェア イベント（「エンドポイントベースのマルウェア イベント」）

強調表示されたデータ ポイントに関連付けられたすべての IP アドレスとタイムスタンプも強調表示されます。[Events] テーブルの対応するイベントも強調表示されます。省略されたイベントがパスに含まれている場合、そのパス自体が点線で強調表示されます。省略されたイベントがパスを交差している場合がありますが、マップに表示されません。

ネットワーク ファイル トラジェクトリの使用

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス（Access）
マルウェア（ネットワーク向け AMP ） 任意（AMP for Endpoints）	マルウェア（ネットワーク向け AMP ） 任意（AMP for Endpoints）	いずれか（Any）	いずれか（Any）	Admin/Any Security Analyst

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

ヒント 組織で AMP for Endpoints を導入している場合、その製品にはネットワーク ファイル トラジェクトリ機能もあります。FMC から AMP for Endpoints にピボットするには、AMP for Endpoints コンソールでのイベント データの使用 （3157 ページ）を参照してください。AMP for Endpoints のファイル トラジェクトリ機能の詳細については、AMP for Endpoints のマニュアルを参照してください。

ステップ 1 **[Analysis]** > **[Files]** > **[Network File Trajectory]**を選択します。

ヒント また、ファイル情報を使用して、コンテキスト エクスプローラ、ダッシュボード、またはイベント ビューからファイルのトラジェクトリにアクセスできます。

ステップ 2 リストの [ファイル SHA 256（File SHA 256）] リンクをクリックします。

ステップ 3 オプションで、追跡するファイルの完全な SHA-256 ハッシュ値、ホスト IP アドレス、またはファイル名を検索フィールドに入力して、Enter を押します。

ヒント 1 つの結果だけが一致する場合、そのファイルの [ネットワーク ファイル トラジェクトリ（Network File Trajectory）] ページが表示されます。

ステップ 4 [サマリー情報（Summary Information）] セクションでは、以下を実行できます。

- ファイル リストにファイルを追加する：クリーン リストまたはカスタム検出リストにファイルを追加したり、ファイルを削除したりするには、編集アイコン（  ）をクリックします。
- ファイルをダウンロードする：ファイルをダウンロードするには、ファイルのダウンロード アイコン（  ）をクリックし、プロンプトが表示されたら、ファイルをダウンロードすることを確認します。ファイルをダウンロードできない場合、このアイコンは淡色表示されます。
- レポートする：脅威スコア アイコンをクリックすると、動的分析サマリー レポートが表示されます。
- 動的分析のために送信する：AMP クラウド アイコン（  ）をクリックすると、動的分析のためにファイルを送信できます。ファイルを送信できない場合、または AMP クラウドに接続できない場合は、このアイコンは淡色表示されます。
- アーカイブの内容を表示する：アーカイブ ファイルの内容に関する情報を表示するには、表示アイコン（  ）をクリックします。
- ファイル構成を表示する：ファイルの構成を表示するには、ファイル リスト アイコン（  ）をクリックします。システムがファイル構成レポートを生成していなければ、このアイコンは淡色表示されます。
- 同じ脅威スコアでキャプチャされたファイルを表示する：脅威スコア リンクをクリックすると、その脅威スコアでキャプチャされたすべてのファイルが表示されます。

（注） シスコでは、有害な結果が発生することがあるため、マルウェアをダウンロード**しない**ように強くお勧めします。ファイルをダウンロードする際は、マルウェアが含まれている可能性があるので注意してください。ファイルをダウンロードする前に、ダウンロード先を保護するために必要な予防措置を行っていることを確認します。

ステップ 5 トラジェクトリ マップでは、以下を実行できます。

- 最初のインスタンスを見つける：IP アドレスをクリックして、IP アドレスが含まれる、最初に発生したファイル イベントを見つけます。これにより、そのデータ ポイントへのパスが強調表示され、その最初のファイル イベントに関連した仲介ファイル イベントと IP アドレスがあればそれも強調表示されます。[Events] テーブルの対応するイベントも強調表示されます。そのデータ ポイントが現在表示されていない場合、表示されるまでマップがスクロールされます。
- 追跡する：データ ポイントをクリックすると、選択したデータ ポイントに関連するすべてのデータ ポイントが含まれるパスが強調表示されます。これにより、ネットワークを介してファイルの進捗を追跡できます。

- 非表示のイベントを表示する：矢印アイコンをクリックすると、[ファイル サマリー（File Summary）] イベント ビューに表示されていないすべてのイベントが表示されます。
- ファイルの一致イベントを表示する：イベント アイコン（）の上にポインタを合わせると、イベントのサマリー情報が表示されます。いずれかのイベント サマリー情報リンクをクリックすると、デフォルトの [ファイル イベント（File Events）] ワークフローの最初のページが新しいウィンドウで開き、そのファイル タイプのすべての余分のイベントが表示されます。[ファイル サマリー（File Summary）] イベント ビューが新しいウィンドウで表示され、クリックした条件値に一致するすべてのファイル イベントが表示されます。

ステップ 6 [イベント（Events）] テーブルでは、以下を実行できます。

- 強調表示：テーブル行を選択すると、マップ上のデータ ポイントが強調表示されます。選択したファイル イベントが現在表示されていない場合、表示されるまでマップがスクロールされます。
- ソート：カラム見出しをクリックすると、昇順または降順で情報をソートできます。

AMP for Endpoints コンソールでのイベント データの使用

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin

組織で AMP for Endpoints を導入している場合は、AMP for Endpoints コンソールでマルウェア イベント データを表示して、当該アプリケーションのグローバル ネットワーク ファイル トラジェクトリ ツールを使用することができます。

ヒント AMP for Endpoints とそのコンソールの使用については、コンソールのオンライン ヘルプや、その他のドキュメンテーションを参照してください。 https://www.cisco.com/c/en/us/support/security/fireamp-endpoints/tsd-products-support-series-home.html

Firepower Management Center から AMP for Endpoints コンソールにアクセスするには、次のいずれかを実行します。

始める前に

- AMP for Endpoints への接続が設定され（Firepower と AMP for Endpoints の統合 （1956 ページ） を参照してください）、Firepower Management Center が AMP クラウドに接続可能になっている必要があります。
- AMP for Endpoints のクレデンシャルが必要になります。

- FMC のマルウェア イベントからピボットする場合は、AMP for Endpoints のコンテキストクロス起動オプションが適切に有効になっていることを確認します。Webベースのリソースを使用したイベントの調査 （2890 ページ）の各トピックを参照してください。

ステップ 1 方法 1：

a) **[AMP]** > **[AMP Management]**を選択します。

b) テーブルでクラウド名をクリックします。

ステップ 2 方法 2：

a) [Analysis（分析）] > [ファイル（Files）] にあるテーブルで、マルウェア イベントに移動します。

b) ファイル SHA を右クリックし、[AMP for Endpoints] オプションを選択します。

ファイルおよびマルウェアイベントとネットワークファイル トラジェクトリの履歴

機能	バージョン	詳細
Syslog の接続イベントの固有識別子	6.4.0.4	syslog の [Sensor UUID]、[First Packet Time]、[Connection Instance ID]、および [Connection Counter] フィールドの情報を総合すると、接続イベントを一意に識別できます。これらのフィールドは、ファイルおよびマルウェアイベントの syslog に含まれます。
syslog を介してファイルイベントおよびマルウェアイベントを送信する機能	6.4	この章のフィールドの説明は、syslog メッセージに含まれるフィールドを指しています。 設定情報については、ファイルとマルウェア イベントの syslog の設定場所（2899 ページ）を参照してください。

第 128 章

ホスト プロファイルの使用

ここでは、ホスト プロファイルの使用方法について説明します。

ホスト プロファイル

ホストプロファイルは、システムが1つのホストについて収集したすべての情報の完全なビューを提供します。ホスト プロファイルにアクセスするには、以下のいずれかを実行します。

- 任意のネットワーク マップ ビューから選択します。
- モニタ対象ネットワークでホストの IP アドレスを含む任意のイベント ビューから選択します。

ホストプロファイルは、ホスト名やMACアドレスなど、検出されたホストやデバイスに関する基本的な情報を提供します。ライセンスやシステム設定によっては、ホストプロファイルは次の情報を提供することもできます。

- ホスト上で実行中のオペレーティング システム

- ホスト上で実行中のサーバ
- ホスト上で実行中のクライアントと Web アプリケーション
- ホスト上で実行中のプロトコル
- ホスト上の侵害の兆候（IOC）タグ
- ホスト上の VLAN タグ
- ネットワーク上での過去 24 時間のユーザ アクティビティ
- ホストに関連付けられているホワイト リスト違反
- ホストの最新のマルウェア イベント
- ホストに関連付けられている脆弱性
- ホストの Nmap スキャン結果

プロファイルには、ホスト属性もリストされます。ホスト属性を使用して、ネットワーク環境にとって重要な方法でホストを分類することができます。例えば、以下を行うことができます。

- ホストが存在する建物を示すホスト属性を割り当てる
- ホストの重要度の属性を使用して、特定のホストのビジネス重要度を指定し、ホストの重要度に基づいて相関ポリシーとアラートを作成する

ホストプロファイルで、そのホストに適用されている既存のホスト属性を表示し、そのホスト属性値を変更できます。

パッシブ侵入防御展開の一部としてアダプティブ プロファイルの更新を使用している場合、ホスト上のオペレーティング システム、およびホストが実行しているサーバとクライアントのタイプに最も適合するように、システムがトラフィックを処理する方法を調整することができます。

オプションで、ホストプロファイルから Nmap スキャンを実行し、ホストプロファイルのサーバ情報とオペレーティング システムの情報を増やすことができます。Nmap スキャナはホストをアクティブに調査し、ホストを実行しているオペレーティング システムおよびサーバの情報を取得します。スキャンの結果は、ホストのオペレーティング システムおよびサーバ アイデンティティのリストに追加されます。

関連トピック

ホスト プロファイルの表示 （3161 ページ）

ホストプロファイルの制限事項

利用できないホスト

ホストプロファイルは、ネットワーク上のすべてのホストでは使用できない可能性があります。考えられる原因は次のとおりです。

- タイムアウトしたため、ネットワーク マップからホストが削除された。
- ホストの制限に達した。
- ネットワーク検出ポリシーでモニタリングされないネットワーク セグメントに、ホストが存在している。

利用できない情報

ホストプロファイルに表示される情報は、ホストのタイプ、および利用可能なホストの情報によって異なる可能性があります。

次に例を示します。

- 非 IP ベースのプロトコル（STP、SNAP、IPX など）を使用してシステムでホストを検出した場合、そのホストは MAC ホストとしてネットワーク マップに追加され、IP ホストに比べて使用できる情報はかなり少なくなります。
- システムは、エクスポートされた NetFlow レコードからネットワーク マップにホストを追加できますが、これらのホストに使用できる情報は限られます（NetFlow データと管理対象デバイス データの違い （2478 ページ）を参照）。

ホスト プロファイルの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Any Security Analyst

次の 2 つの選択肢があります。

- ネットワーク マップで、プロファイルを表示するホストの IP アドレスをドリル ダウンします。
- 任意のイベント ビューで、ホスト プロファイル アイコン（  ）をクリックするか、またはプロファイルを表示するホストの IP アドレスの隣にある、侵害されたホスト アイコン（  ）をクリックします。

ホスト プロファイルの基本ホスト情報

各ホストプロファイルは、検出されたホストまたは他のデバイスに関する基本情報を提供します。

次に、基本的なホスト プロファイルのフィールドについて説明します。

ドメイン（Domain）

ホストに関連付けられているドメイン。

IP アドレス

ホストに関連付けられているすべての IP アドレス（IPv4 と IPv6 の両方）。システムは、ホストに関連付けられている IP アドレスを検出し、サポートされている場合は、同じホストで使用される複数の IP アドレスをグループ化します。多くの場合、IPv6 ホストには、少なくとも 2 つの IPv6 アドレス（ローカルのみでルーティング可能なものと、グローバルにルーティング可能なもの）があり、その他に IPv4 アドレスを持っていることがあります。IPv4 専用ホストは、複数の IPv4 アドレスを持っていることがあります。

ホスト プロファイルは、そのホストに関連付けられている、検出されたすべての IP アドレスを一覧で示します。可能な場合は、ルーティング可能なホスト IP アドレスに、フラグ アイコン、およびアドレスに関連付けられている地理情報データを表す国コードも含まれています。

デフォルトでは最初の 3 つのアドレスだけが表示されることに注意してください。[すべて表示（Show All）] をクリックすると、ホストのすべてのアドレスが表示されます。

ホストネーム

ホストの完全修飾ドメイン名（わかる場合）。

NetBIOS 名（NetBIOS Name）

ホストの NetBIOS 名（使用できる場合）。Microsoft Windows ホストだけでなく Macintosh、Linux、または NetBIOS を使用するように設定されたその他のプラットフォームに NetBIOS 名を指定できます。たとえば、Samba サーバとして設定されている Linux ホストに NetBIOS 名を指定します。

デバイス (ホップ数)（Device (Hops)）

次のいずれかを行います。

- ホストが存在しているネットワークに関するレポート作成のデバイス（ネットワーク検出ポリシーで定義されている）、または
- ホストをネットワーク マップへ追加する NetFlow データを処理したデバイス

デバイス名の後に、ホストを検出したデバイスとホスト自身の間のネットワーク ホップの数が丸括弧で囲まれて表示されます。複数のデバイスで対象のホストを参照できる場合は、報告元のデバイスが太字で表示されます。

このフィールドが空白の場合は、次のいずれかになります。

- ホストがデバイスによってネットワーク マップに追加されたが、このデバイスは、ホストが存在しているネットワークに対してネットワーク検出ポリシーに定義されているとおりに明示的に監視していない。または、

- ホストの入力機能を使用してホストが追加されたが、Firepower システムによって検出されていない。

MAC アドレス（TTL）（MAC Addresses (TTL)）

ホストについて検出された 1 つ以上の MAC アドレスおよび関連付けられている NIC ベンダー。NIC のハードウェア ベンダーと現在の存続可能時間（TTL）値が括弧で囲まれて表示されます。

複数のデバイスが同じホストを検出した場合、Firepower Management Center には、どのデバイスがホストを報告したかに関係なく、ホストに関連付けられているすべての MAC アドレスと TTL 値が表示されます。

MAC アドレスが太字で表示されている場合、その MAC アドレスは、ARP および DHCP トラフィックを通じた検出により、IP アドレスに明確に関連付けられた、ホストの実際の/該当する/プライマリの MAC アドレスです。

太字フォントで表示されない MAC アドレスはセカンダリ アドレスなので、ホストの IP アドレスに明確に関連付けることはできません。たとえば、Firepower デバイスが取得できるのは自身のネットワーク セグメント上にあるホストの MAC アドレスのみであるため、トラフィックが Firepower デバイスが直接接続されていないネットワーク セグメントから発生している場合、監視されている MAC アドレス（ルータの MAC アドレス）は、ホストのセカンダリ MAC アドレスとして表示されます。

ホスト タイプ（Host Type）

システムで検出されたデバイスのタイプ（ホスト、モバイルデバイス、ジェイルブレイクされたモバイル デバイス、ルータ、ブリッジ、NAT デバイス、またはロード バランサ）。

ネットワーク デバイスを区別するためにシステムでは次の方法を使用します。

- Cisco Discovery Protocol（CDP）メッセージの分析。ネットワークのデバイスおよびそれらのタイプ（Cisco デバイスのみ）を特定できます。
- スパニング ツリー プロトコル（STP）の検出。デバイスをスイッチまたはブリッジとして識別します。
- 同じ MAC アドレスを使用している複数のホストの検出。MAC アドレスを、ルータに属しているものとして識別します。
- クライアント側からの TTL 値の変更、または通常のブート時間よりも頻繁に変更されている TTL 値の検出。この検出では、NAT デバイスとロード バランサを識別します。
- モバイル デバイスを区別するためにシステムでは次の方法を使用します。
- モバイル デバイスのモバイル ブラウザからの HTTP トラフィックのユーザ エージェント文字列の分析
- 特定のモバイル アプリケーションの HTTP トラフィックのモニタリング

デバイスがネットワーク デバイスまたはモバイル デバイスとして識別されない場合は、ホストとして分類されます。

前回の検出（Last Seen）

ホストのいずれかの IP アドレスが最後に検出された日時。

現在のユーザ（Current User）

このホストに最後にログインしたユーザ。

既存の現在のユーザが権限のあるユーザでない場合、ホストにログインしている権限を持たないユーザは、現在のユーザとして登録されるだけであることに注意してください。

表示（View）

接続、検出、マルウェア、および侵入イベントデータのビューへのリンク。このリンクは、そのイベント タイプのデフォルト ワークフローを使用し、ホストに関連するイベントを表示するように制限されています。可能な場合は、これらのイベントには、ホストに関連付けられているすべての IP アドレスが含まれます。

ホスト プロファイルのオペレーティング システム

システムは、ホストで生成されたトラフィック内のネットワークおよびアプリケーション スタックを分析したり、User Agent でレポートされたホストデータを分析することによって、ホスト上で稼動しているオペレーティング システムのアイデンティティをパッシブに検出します。システムでは、他のソース（Nmap スキャナ、ホストの入力機能によりインポートされたアプリケーション データ）のオペレーティング システムの情報も照合します。どのアイデンティティを使用するかを判断する場合、システムは、各アイデンティティのソース（発生源）に割り当てられている優先度を考慮します。デフォルトでは、ユーザ入力が最も高い優先度を持ち、以降は高い順にアプリケーションまたはスキャナ ソース、検出されたアイデンティティ、となります。

システムでは、オペレーティング システムの具体的な定義ではなく、全般的な定義を提供することがあります。これは、トラフィックおよび他のアイデンティティ ソースで、対象のアイデンティティを詳しく調べるための十分な情報が提供されないためです。システムは、できるだけ詳しい定義を使用するために、ソースの情報を照合します。

オペレーティング システムは、ホストの脆弱性リスト、およびホストを対象とするイベントの影響の相関関係に影響するため、オペレーティング システムの特定の情報を手動で入力することもできます。また、オペレーティング システムに対して、サービス パックやアップデートなどの修正ファイルが適用されたことを示すことも、修正ファイルによって対処された脆弱性を無効にすることもできます。

たとえば、システムでホストのオペレーティング システムが Microsoft Windows 2003 であると特定されたが、実際にはホストが Microsoft Windows XP Professional および Service Pack 2 を実行していることがわかっている場合、オペレーティング システムのアイデンティティを実際のとおりに設定することができます。より具体的なオペレーティング システムのアイデンティ

ティを設定すると、ホストの脆弱性のリストの精度が向上するため、対象のホストに対する影響の相関関係が、より限定的かつ正確になります。

システムでホストに対するオペレーティング システム情報が検出され、その情報が、アクティブなソースによって提供されている現行のオペレーティング システムのアイデンティティと競合している場合、アイデンティティの競合が発生します。実際にアイデンティティの競合が発生している場合、システムは脆弱性と影響の相関関係の両方のアイデンティティを使用します。

ネットワーク検出ポリシーを設定して、NetFlow エクスポータによってモニタされるホストのネットワーク マップに検出データを追加することができます。ただし、オペレーティング システムの ID を設定するためにホスト入力機能の使用を設定しない限り、これらのホストで使用可能なオペレーティング システム データはありません。

オペレーティング システムを実行しているホストが、有効なネットワーク検出ポリシーのコンプライアンスのホワイト リストに違反している場合、Firepower Management Center はオペレーティング システムの情報にホワイト リストの違反アイコン（）のマークを付けます。また、ジェイルブレイクされたモバイル デバイスが有効なホワイト リストに違反している場合、そのデバイスのオペレーティング システムの隣にアイコンが表示されます。

ホストのオペレーティング システムのアイデンティティに対して、カスタム表示文字列を設定できます。この表示文字列は、ホスト プロファイルで使用されます。

（注） あるホストについてオペレーティング システムの情報を変更すると、ホストのコンプライアンス、およびコンプライアンスのホワイト リストが変わる可能性があります。

ネットワーク デバイスに対するホスト プロファイルでは、[オペレーティング システム（Operating Systems）] セクションのラベルが [システム（Systems）] に変わり、[ハードウェア（Hardware）] カラムが新しく表示されます。[システム（Systems）] の下にハードウェア プラットフォームの値が表示され場合、システムは、ネットワーク デバイスの背後で 1 つ以上のモバイルデバイスが検出されたことを示しています。モバイルデバイスはハードウェア プラットフォームの情報を持っていることも、持っていないこともありますが、モバイルデバイスではないシステムではハードウェア プラットフォーム情報は検出されないことに注意してください。

次に、ホスト プロファイルで表示されるオペレーティング システムの情報フィールドについて説明します。

ハードウェア（Hardware）

モバイル デバイスのハードウェア プラットフォーム。

OS Vendor/Vendor

オペレーティング システムのベンダー。

OS 製品/製品（OS Product/Product）

次の値のいずれかを指定します。

- すべてのソースから収集されたアイデンティティ データに基づいて、実行されている可能性が最も高いと判断されたオペレーティング システム。
- [Pending]：システムがオペレーティング システムをまだ識別しておらず、他に使用可能なアイデンティティ データがない場合。
- [unknown]：システムがオペレーティング システムを識別できず、オペレーティング システムに関して他に使用可能なアイデンティティ データがない場合。

（注） ホストのオペレーティング システムをシステムで検出できない場合には、ホスト オペレーティング システムの識別 （2496 ページ）を参照してください。

OS バージョン/バージョン（OS Version/Version）

オペレーティング システムのバージョン。ホストがジェイルブレイクされたモバイル デバイスの場合、バージョンの後に括弧で囲まれて `Jailbroken` と示されます。

ソース（Source）

次の値のいずれかを指定します。

- [ユーザ（User）]：user_name
- [アプリケーション（Application）]：app_name
- [スキャナ（Scanner）]：scanner_type（Nmap またはその他のスキャナ）
- Firepower

システムでは、オペレーティング システムのアイデンティティを判断するために、複数のソースのデータを統合することができます。

オペレーティング システム アイデンティティの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Any Security Analyst

検出された、またはホストに追加された特定のオペレーティング システムのアイデンティティを表示することができます。システムはソースの優先度を使用して、ホストに対する現行のアイデンティティを判断します。アイデンティティのリストでは、現行のアイデンティティが太字で強調されます。

1 つのホストに対して複数のオペレーティング システムのアイデンティティが存在している場合のみ、[表示（View）] ボタンが有効になっていることに注意してください。

ステップ 1 ホスト プロファイルの [オペレーティング システム（Operating System）] または [オペレーティング システムの競合（Operating System Conflicts）] セクションで [表示（View）] をクリックします。

ステップ 2 ホスト プロファイルのオペレーティング システム （3164 ページ）の説明に従って情報を入力します。

ステップ 3 必要に応じて、オペレーティング システムのアイデンティティの横にある削除アイコン（  ）をクリックします。

（注） シスコが検出したオペレーティング システムのアイデンティティは削除できません。

該当する場合は、このシステムは [オペレーティング システムのアイデンティティ情報（Operating System Identity Information）] ポップアップ ウィンドウからアイデンティティを削除し、ホスト プロファイルのオペレーティング システムの現在のアイデンティティを更新します。

現在のオペレーティング システムのアイデンティティの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Any Security Analyst

Firepower システム Web インターフェイスを使用して、ホストに対する現行のオペレーティング システムのアイデンティティを設定できます。Web インターフェイスを介してアイデンティティを設定すると、他のすべてのアイデンティティ ソースが上書きされるため、このアイデンティティが、脆弱性の評価および影響の相関関係で使用されます。ただし、オペレーティング システムを編集した後で、ホストに対するオペレーティング システムのアイデンティティの競合がシステムで検出されると、オペレーティング システムの競合が発生します。競合が解決されるまで、両方のオペレーティング システムが現行のものであるとみなされます。

ステップ 1 ホスト プロファイルの [オペレーティング システム（Operating System）] セクションで [編集（Edit）] をクリックします。

ステップ 2 ここでは次のオプションがあります。

- [OS 定義（OS Definition）] ドロップダウンリストから [現在の定義（Current Definition）] を選択して、ホスト入力によって現行のオペレーティング システムのアイデンティティを確認して、手順 6 に進みます。
- [OS 定義（OS Definition）] ドロップダウン リストから現行のオペレーティング システムのアイデンティティのバリエーションを選択し、手順 6 に進みます。
- [OS 定義（OS Definition）] ドロップダウンリストから [ユーザ定義（User-Defined）] を選択して、手順 3 に進みます。

ステップ 3 必要に応じて、[カスタム表示文字列を使用する（Use Custom Display String）] を選択し、[ベンダー文字列（Vendor String）]、[製品文字列（Product String）]、および [バージョン文字列（Version String）] フィールドに表示するカスタム文字列を変更します。

ステップ 4 必要に応じて、別のベンダーからのオペレーティング システムに変更するには、[ベンダー（Vendor）] と [製品（Product）] のドロップダウンリストから選択します。

ステップ 5 必要に応じて、オペレーティング システムの製品リリース レベルを設定するには、[メジャー（Major）]、[マイナー（Minor）]、[リビジョン（Revision）]、[ビルド（Build）]、[パッチ（Patch）]、および [拡張（Extension）] ドロップダウン リストから選択します。

ステップ 6 必要に応じて、オペレーティング システムに対して修正ファイルが適用されたことを示す場合は、[修正の設定（Configure Fixes）] をクリックします。

ステップ 7 ドロップダウン リストから適用可能な修正を選択し、[追加（Add）] をクリックします。

ステップ 8 必要に応じて、[パッチ（Patch）] および [拡張（Extension）] ドロップダウン リストを使用して、対象のパッチと拡張機能を追加します。

ステップ 9 [完了（Finish）] をクリックします。

関連トピック

オペレーティング システムのアイデンティティの競合 （3168 ページ）

オペレーティング システムのアイデンティティの競合

システムで検出された新しいアイデンティティと現行のアイデンティティが競合しており、そのアイデンティティが、スキャナやアプリケーション、ユーザなどのアクティブなソースによって提供されていた場合、オペレーティング システムのアイデンティティで競合が発生します。

ホスト プロファイルでは、競合状態のオペレーティング システムのアイデンティティのリストは太字で表示されます。

システムの Web インターフェイスを介して、アイデンティティの競合を解決し、ホストに対する現行のオペレーティング システムのアイデンティティを設定することができます。Web インターフェイスを介してアイデンティティを設定すると、他のすべてのアイデンティティ ソースが上書きされるため、このアイデンティティが、脆弱性の評価および影響の相関関係で使用されます。

関連トピック

ネットワーク検出アイデンティティ競合の解決の設定 （2665 ページ）

競合しているオペレーティング システムのアイデンティティの現行化

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Any Security Analyst

ステップ 1 ホスト プロファイルの [オペレーティング システム（Operating System）] セクションに移動します。

ステップ 2 次の 2 つの選択肢があります。

- ホストのオペレーティング システムとして設定するオペレーティング システムのアイデンティティの隣にある、[現行にする（Make Current）] をクリックします。
- アクティブなソースで、現行のアイデンティティとして使用しないアイデンティティが表示された場合は、使用しないアイデンティティを削除します。

オペレーティング システムのアイデンティティ競合の解決

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Any Security Analyst

ステップ 1 ホスト プロファイルの [オペレーティング システムの競合（Operating System Conflicts）] セクションにある [解決（Resolve）] をクリックします。

ステップ 2 次の選択肢があります。

- [OS 定義（OS Definition）] ドロップダウンリストから [現在の定義（Current Definition）] を選択して、ホスト入力によって現行のオペレーティング システムのアイデンティティを確認して、手順 6 に進みます。
- [OS 定義（OS Definition）] ドロップダウンリストから、競合しているオペレーティング システムのアイデンティティのいずれかのバリエーションを選択して、手順 6 に進みます。
- [OS 定義（OS Definition）] ドロップダウンリストから [ユーザ定義（User-Defined）] を選択して、手順 3 に進みます。

ステップ 3 必要に応じて、[カスタム表示文字列の使用（Use Custom Display String）] を選択して、表示するカスタム文字列を [ベンダー文字列（Vendor String）]、[製品文字列（Product String）]、および [バージョン文字列（Version String）] フィールドに入力します。

ステップ 4 必要に応じて、別のベンダーからのオペレーティング システムに変更するには、[ベンダー（Vendor）] と [製品（Product）] のドロップダウンリストから選択します。

ステップ 5 必要に応じて、オペレーティング システムの製品リリース レベルを設定するには、[メジャー（Major）]、[マイナー（Minor）]、[リビジョン（Revision）]、[ビルド（Build）]、[パッチ（Patch）] および [拡張（Extension）] ドロップダウンリストから選択します。

ステップ 6 必要に応じて、オペレーティング システムに対して修正ファイルが適用されたことを示す場合は、[修正の設定（Configure Fixes）] をクリックします。

ステップ 7 適用した修正ファイルを、修正ファイル リストに追加します。

ステップ 8 [完了（Finish）] をクリックします。

関連トピック

ネットワーク検出アイデンティティ競合の解決の設定 （2665 ページ）

ホスト プロファイルのサーバ

ホスト プロファイルのサーバ セクションでは、監視対象ネットワーク上のホストで検出されるか、エクスポートされたNetFlow レコードから追加されるか、スキャナまたはホスト入力機能のようなアクティブなソースを介して追加されるサーバを列挙します。

リストは 1 つのホストにつき最大 100 台のサーバを表示します。100 個の制限に達すると、ホストからサーバを削除するか、またはサーバがタイムアウトになるまで、いずれかのソースの新しいサーバ情報は、アクティブであってもパッシブであっても廃棄されます。

Nmap を使用してホストをスキャンすると、オープンなTCP ポート上で稼動している、以前に検出されなかったサーバの結果がNmap によってServers リストに追加されます。Nmap スキャンを実行した場合、またはNmapの結果をインポートした場合、ホストプロファイルに拡張可能な [スキャン結果（Scan Results）] セクションも表示され、Nmap スキャンによってホスト上で検出されたサーバ情報が示されます。さらに、ネットワーク マップからホストが削除されると、ホストのそのサーバに対する Nmap スキャンの結果は廃棄されます。

（注） システムは、エクスポートされたNetFlow レコードからネットワーク マップにホストを追加できますが、これらのホストに使用できる情報は限られます（NetFlow データと管理対象デバイス データの違い （2478 ページ）を参照）。

ホストプロファイルでサーバを使用するためのプロセスは、ユーザがプロファイルにアクセスする方法によって異なります。

- ネットワーク マップを介したドリル ダウンによりホスト プロファイルにアクセスする場合は、サーバの名前が太字で強調されて、サーバの詳細が表示されます。ホストの他のサーバについて詳細を表示する場合は、対象のサーバ名の隣にある表示アイコン（[]）をクリックします。
- 他の方法でホストプロファイルにアクセスする場合は、[サーバ（Servers）] セクションを展開し、詳細を表示するサーバの隣にある表示アイコン（[]）をクリックします。

（注） ホストが、有効な相関ポリシーにおけるコンプライアンスのホワイトリストに違反しているサーバを実行している場合、Firepower Management Center は非準拠サーバに、ホワイト リストの違反アイコン（[]）のマークを付けます。

次に、[Servers リスト（Servers list）] の列について説明します。

Protocol

サーバが使用するプロトコルの名前。

Port

サーバが実行されているポート。

Application Protocol

次のいずれかになります。

- アプリケーション プロトコルの名前
- [保留中（pending）]：システムで、いずれかの理由のでアプリケーション プロトコルをポジティブまたはネガティブに識別できない場合
- [未知（unknown）]：既知のアプリケーション プロトコルのフィンガープリントに基づいてシステムでアプリケーションプロトコルを識別できない場合、または（対応するサーバは追加せずに、ポート情報での脆弱性を追加することにより）ホストの入力を介してサーバが追加された場合

アプリケーション プロトコルの名前にマウスを重ねると、タグが表示されます。

ベンダーおよびバージョン（Vendor and Version）

Firepower システム、Nmap、または他のアクティブなソースで識別されたベンダーとバージョン、またはホストの入力機能を介して取得したベンダーとバージョン。有効なソースで識別が行われなかった場合、フィールドは空白になります。

関連トピック

ホスト制限と検出イベント ロギング （2552 ページ）
NetFlow データと管理対象デバイス データの違い （2478 ページ）
アプリケーション ディテクタの基本 （2548 ページ）

ホスト プロファイルのサーバの詳細

Firepower Management Center は、1 つのサーバについてパッシブに検出されるアイデンティティを最大 16 個表示します。パッシブな検出ソースには、ネットワーク検出データおよびNetFlow レコードが含まれます。システムで、このサーバの複数のベンダーまたはバージョンを検出した場合、サーバは複数のパッシブなアイデンティティを持つことができます。たとえば、Web サーバが、サーバ ソフトウェアと同じバージョンを実行していない場合、管理対象デバイスと Web サーバ ファーム間にロード バランサがあると、HTTP に対してシステムが複数のパッシブ アイデンティティを識別することがあります。Firepower Management Centerは、ユーザ入力、スキャナ、その他のアプリケーションなど、アクティブなソースからのサーバ アイデンティティの数を制限することはありません。

Firepower Management Centerは現行のアイデンティティを太字で表示します。システムでは、1 つのホストに対する脆弱性の割り当て、影響の評価、ホストプロファイルの証明書およびコン

プライアンスホワイトリストに対して記載された相関ルールの評価など、いくつかの目的のためにサーバの現行のアイデンティティを使用します。

サーバの詳細には、選択されたサーバについて知られている、更新済みのサブサーバ情報が表示されることもあります。

サーバの詳細にサーバのバナーが表示されることもあります。これは、ホストプロファイルからサーバを表示したときに、サーバの詳細の下に表示されます。サーバのバナーは、サーバを識別するのに役立つサーバに関する追加情報を提供します。攻撃者がサーバのバナー文字列を意図的に変更した場合、システムは誤ったアイデンティティが示されたサーバを識別または検出できません。サーバのバナーには、そのサーバについて検出された最初のパケットの最初の256 文字が表示されます。この情報は、サーバがシステムによって最初に検出されたときに一度だけ収集されます。バナーの内容は 2 列で表示されます。左側の列は 16 進表記で示され、右側の列は対応する ASCII 表記で示されます。

（注） サーバのバナーを表示するには、ネットワーク検出ポリシーで [Capture Banners] チェック ボックスを有効にする必要があります。このオプションはデフォルトでは無効になっています。

ホスト プロファイルのサーバの詳細セクションには、次の情報が含まれています。

プロトコル

サーバが使用するプロトコルの名前。

Port

サーバが実行されているポート。

ヒット数（Hits）

Firepower システムの管理対象デバイスまたは Nmap スキャナによってサーバが検出された回数。ホストの入力によってインポートされたサーバについては、システムがそのサーバについてトラフィックを検出しない場合、検出回数は 0 になります。

前回の使用（Last Used）

サーバが最後に検出された日時。システムで対象のサーバについて新しいトラフィックを検出しない場合、ホスト入力のデータが最後に使用された時間は、データの最初のインポート時間を反映しています。ホストの入力機能を介してインポートされたスキャナおよびアプリケーションのデータは、Firepower Management Center の設定に応じてタイム アウトしますが、FMC の Web インターフェイスを介したユーザ入力の場合はタイム アウトしません。

アプリケーション プロトコル（Application Protocol）

サーバによって使用されるアプリケーション プロトコルの名前（既知の場合）。

Vendor

サーバのベンダー。ベンダーがわからない場合、このフィールドは表示されません。

Version

サーバのバージョン。バージョンがわからない場合、このフィールドは表示されません。

Source

次の値のいずれかを指定します。

- [ユーザ（User）]：user_name
- [アプリケーション（Application）]：app_name
- [スキャナ（Scanner）]：scanner_type（Nmap またはその他のスキャナ）
- Firepower システムで検出されたアプリケーションの場合、`Firepower`、`Firepower Port Match`、または `Firepower Pattern Match`
- NetFlow レコードからネットワーク マップに追加されたサーバの場合、`NetFlow`

システムでは、サーバのアイデンティティを判断するために、複数のソースのデータを統合することができます。

関連トピック

アプリケーションおよびオペレーティング システムの現在の ID （2474 ページ）

サーバに関する詳細情報の表示

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Any Security Analyst

ホストプロファイルの[サーバ（Servers）]セクションで、サーバの横にある表示アイコン（  ）をクリックします。

サーバのアイデンティティの編集

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Any Security Analyst

ホスト上のサーバのアイデンティティ設定を手動で更新し、修正ファイルによって対処された脆弱性を削除するために、ホストに適用した何らかの修正ファイルを設定することができます。サーバのアイデンティティを削除することもできます。

アイデンティティを削除した場合、削除したアイデンティティが唯一のアイデンティティであっても、サーバは削除されません。アイデンティティを削除すると、[サーバの詳細（Server Detail）] ポップアップ ウィンドウからアイデンティティが削除されます。可能な場合は、ホスト プロファイルでそのサーバの現行のアイデンティティを更新します。

シスコ管理対象デバイスによって追加されたサーバのアイデンティティは、編集または削除できません。

ステップ 1 ホスト プロファイルの [サーバ（Servers）] セクションに移動します。

ステップ 2 [表示（View）] をクリックし、[サーバの詳細（Server Detail）] ポップアップ ウィンドウを開きます。

ステップ 3 サーバのアイデンティティを削除するには、削除するサーバのアイデンティティの横にある削除アイコン（  ）をクリックします。

ステップ 4 サーバのアイデンティティを変更するには、サーバ リストでサーバの横にある編集アイコン（  ）をクリックします。

ステップ 5 次の 2 つの選択肢があります。

- [サーバ タイプの選択（Select Server Type）] ドロップダウン リストから現行の定義を選択します。
- [サーバ タイプの選択（Select Server Type）] ドロップダウンリストからサーバのタイプを選択します。

ステップ 6 必要に応じて、対象のサーバ タイプのベンダーと製品のみを表示する場合は、[サーバ タイプ別に制限（Restrict by Server Type）] チェックボックスをオンにします。

ステップ 7 オプションでサーバの名前とバージョンをカスタマイズするには、[カスタム表示文字列の使用（Use Custom Display String）] を選択し、[ベンダー文字列（Vendor String）] と [バージョン文字列（Version String）] に入力します。

ステップ 8 [製品マッピング（Product Mappings）] セクションで、使用するオペレーティング システム、製品、およびバージョンを選択します。

例：

たとえば、サーバを Red Hat Linux 9 にマップする場合は、ベンダーとして [Redhat, Inc.] を、製品として [Redhat Linux] を選択し、バージョンとして [9] を選択します。

ステップ 9 サーバの修正が適用されていることを示す場合は、[修正の設定（Configure Fixes）] をクリックして、そのサーバに適用するパッチを修正リストに追加します。

ステップ 10 [完了（Finish）] をクリックします。

サーバ アイデンティティの競合の解決

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Any Security Analyst

アプリケーションやスキャナなどのアクティブなソースが、サーバのアイデンティティデータをホストへ追加したときに、サーバアイデンティティの競合が発生します。その後で、システムはサーバ アイデンティティの競合を示しているポートのトラフィックを検出します。

ステップ 1 ホスト プロファイルで、[サーバ（Servers）] セクションに移動します。

ステップ 2 サーバの横にある解決アイコンをクリックします。

ステップ 3 [サーバ タイプの選択（Select Server Type）] ドロップダウンリストからサーバのタイプを選択します。

ステップ 4 必要に応じて、対象のサーバ タイプのベンダーと製品のみを表示する場合は、[サーバ タイプ別に制限（Restrict by Server Type）] チェックボックスをオンにします。

ステップ 5 必要に応じて、サーバの名前とバージョンをカスタマイズする場合は、[カスタム表示文字列の使用（Use Custom Display String）] を選択して、[ベンダー文字列（Vendor String）] と [バージョン文字列（Version String）] を入力します。

ステップ 6 [製品マッピング（Product Mappings）] セクションで、使用するオペレーティング システム、製品、およびバージョンを選択します。

例：

たとえば、サーバを Red Hat Linux 9 にマップする場合は、ベンダーとして [Redhat, Inc.] を、製品として [Redhat Linux] を選択し、バージョンとして [9] を選択します。

ステップ 7 サーバの修正が適用されていることを示す場合は、[修正の設定（Configure Fixes）] をクリックして、そのサーバに適用するパッチを修正リストに追加します。

ステップ 8 [完了（Finish）] をクリックします。

関連トピック

ネットワーク検出アイデンティティ競合の解決の設定 （2665 ページ）

ホスト プロファイルの Web アプリケーション

ホスト プロファイルの [Web アプリケーション（Web Application）] セクションには、ネットワーク内のホスト上で動作していることをシステムが識別したクライアントと Web アプリケーションが表示されます。システムでは、パッシブ検出ソースとアクティブ検出ソースの両方から取得されるクライアントと Web アプリケーションの情報を識別できます。ただし、NetFlow レコードから追加されたホストに関する情報は一部しか取得することができません。

このセクションには、ホスト上で検出されたアプリケーションの製品とバージョン、使用できるクライアントまたは Web アプリケーションの情報、アプリケーションが最後に使用中であると検出された時間などの詳細情報が表示されます。

ホスト上で稼動している最大 16 個のクライアントが、このセクションに表示されます。16 個の制限に達すると、ユーザがホストからクライアント アプリケーションを削除するか、または非アクティブである（クライアントがタイムアウトしている）ためにシステムによってホスト プロファイルからクライアントが削除されるまで、新しいクライアント情報は、どのソースのものであるか、アクティブかパッシブかにかかわらず、廃棄されます。

また、検出されたそれぞれの Web ブラウザについては、アクセスされた最初の 100 個の Web アプリケーションが表示されます。この制限に達すると、ブラウザに関連付けられている新しい Web アプリケーションは、どのソースのものであるか、アクティブかパッシブかにかかわらず、次の条件を満たすまで廃棄されます。

- Web ブラウザのクライアント アプリケーションがタイムアウトになる、または
- ユーザが、Web アプリケーションに関連付けられているアプリケーション情報をホスト プロファイルから削除する

ホストが、有効な相関ポリシーにおけるコンプライアンスのホワイトリストに違反しているアプリケーションを実行している場合、Firepower Management Center は非準拠アプリケーションに、ホワイト リストの違反アイコン（  ）のマークを付けます。

ヒント　ホスト上の特定のアプリケーションに関連付けられている接続イベントを分析するには、アプリケーションの隣にあるイベント アイコン（  ）をクリックします。接続イベントに対する優先ワークフロー最初のページが表示され、ホストの IP アドレスの他、アプリケーションのタイプ、プロトコル、およびバージョンで制約されて接続イベントが示されます。接続イベントに対する優先ワークフローがない場合、ワークフローを選択する必要があります。

次に、ホスト プロファイルに表示されるアプリケーション情報について説明します。

Application Protocol

アプリケーション（HTTP ブラウザ、DNS クライアントなど）で使用されるアプリケーション プロトコルを表示します。

クライアント（Client）

ペイロードから派生したクライアント情報。この情報は、Firepower システムが識別するか、Nmap がキャプチャするか、またはホスト入力機能によって取得されます。有効なソースで識別が行われなかった場合、フィールドは空白になります。

Version

クライアントのバージョンを表示します。

Web Application

Web ブラウザの場合は、http トラフィックでシステムによって検出されたコンテンツ。Web アプリケーションの情報は、Firepower システムによって識別された、Nmap によってキャプチャされた、他のアクティブなソースによって取得された、またはホストの入力機能を介して取得された特定のタイプのコンテンツ（WMV や QuickTime など）を表します。有効なソースで識別が行われなかった場合、フィールドは空白になります。

ホスト プロファイルからの Web アプリケーションの削除

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Any Security Analyst

ホスト プロファイルからアプリケーションを削除して、ホスト上で稼動していないことがわかっているアプリケーションを削除することができます。ホストからアプリケーションを削除すると、そのホストにホワイト リストのコンプライアンスが適用されることがあります。

（注） システムでアプリケーションが再検出されると、アプリケーションはネットワーク マップおよびホスト プロファイルに再度追加されます。

ステップ 1 ホスト プロファイルで、[アプリケーション（Applications）] セクションに移動します。

ステップ 2 削除するアプリケーションの横にある削除アイコン（）をクリックします。

ホスト プロファイルのホスト プロトコル

各ホスト プロファイルには、ホストに関連付けられているネットワーク トラフィックで検出されたプロトコルに関する情報が含まれています。この情報には次のものが含まれます。

プロトコル

ホストが使用するプロトコルの名前。

Layer

プロトコルを実行しているネットワーク層（ネットワークまたはトランスポート）。

ホストプロファイルに表示されているプロトコルが、有効な相関ポリシーのコンプライアンス ホワイト リストに違反する場合、Firepower Management Center は非準拠プロトコルに、ホワイト リストの違反アイコン（）のマークを付けます。

ホストプロファイルに、ホスト上で実行していないことがわかっているプロトコルがリストされている場合は、これらのプロトコルを削除できます。ホストからプロトコルを削除すると、ホストがコンプライアンス ホワイト リストに準拠する可能性があります。

（注） システムでプロトコルが再検出されると、プロトコルはネットワーク マップおよびホスト プロファイルに再度追加されます。

ホスト プロファイルからのプロトコルの削除

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Any Security Analyst

ステップ 1 ホスト プロファイルの [プロトコル（Protocols）] セクションに移動します。

ステップ 2 削除するプロトコルの横にある削除アイコン（）をクリックします。

ホスト プロファイル内の侵害の兆候

Firepower System は、モニタリング対象のネットワーク上でホストが悪意のある手段によって侵害されている可能性があるかどうかを判断するために、ホストに関連付けられているさまざまなタイプのデータ（侵入イベント、Security Intelligence、接続イベント、ファイルまたはマルウェア イベント）との関連性を示します。イベント データの特定の組み合わせと頻度は、影響を受けたホストの侵害の痕跡（IOC）タグをトリガーとして使用します。

ホスト プロファイルの [侵害の兆候（Indications of Compromise）] セクションには、ホストのすべての侵害の兆候のタグが表示されます。

侵害の兆候にタグを付けるようにシステムを構成するには、侵害の兆候ルールの有効化 （2667 ページ）を参照してください。

侵害の兆候についての作業の詳細については、侵害の兆候データ （3221 ページ）とそのトピックのサブトピックを参照してください。

関連トピック

侵害の兆候 （2666 ページ）

ホスト プロファイルの VLAN タグ

ホストが仮想LAN（VLAN）のメンバである場合、ホストプロファイルの[VLANタグ（VLAN Tag）] セクションが表示されます。

物理ネットワーク機器は、多くの場合に VLAN を使用して、さまざまなネットワーク ブロックから論理ネットワーク セグメントを作成します。システムは 802.1q VLAN タグを検出し、それぞれに対して以下の情報を表示します。

- [VLAN ID] は、ホストがメンバである VLAN を表します。これは、802.1q VLAN の場合、0～4095の任意の整数となります。
- [Type] は、VLAN タグが含まれている、カプセル化されたパケットを表します。値は Ethernet または Token Ring となります。
- [Priority] は、VLAN タグの優先度を表します。これは 0～7 の任意の整数で、7 は最も高い優先度です。

VLAN タグがパケット内でネスト構造になっている場合、システムは最も内側の VLAN タグを処理し、Firepower Management Center は最も内側の VLAN タグを表示します。システムは、ARP および DHCP トラフィックを通じて識別される MAC アドレスのみの VLAN タグ情報を収集し、これらのタグを表示します。

たとえば全体がプリンタで構成されている VLAN があり、システムがこの VLAN で Microsoft Windows 2000 のオペレーティング システムを検出した場合などは、VLAN タグ情報が有用です。VLAN 情報により、システムは正確性の高いネットワーク マップを生成できるようになります。

ホスト プロファイル内のユーザ履歴

ホスト プロファイルのユーザ履歴の部分には、過去 24 時間のユーザ アクティビティがグラフィック表示されます。一般的なユーザは夜間にログオフし、他のユーザとホストのリソースを共有します。電子メールのチェックなどの目的で行われる定期的なログインの要求は、短い標準の棒で示されます。ユーザのアイデンティティ リストは棒グラフで提示され、ユーザのログインが検出されたタイミングを示します。権限のないログインの場合は、棒グラフがグレーになっていることに注意してください。

システムは、ホストに対する権限を持たないユーザのログインを、そのホストの IP アドレスに関連付けて、ホストのユーザ履歴にユーザが表示されるようにします。ただし、権限のあるユーザ ログインが同じホストで検出された場合、その権限のあるユーザ ログインに関連付けられているユーザが、そのホストの IP アドレスとの関連付けを引き継ぐため、新しい権限のないユーザ ログインがそのホストの IP アドレスとのそのユーザの関連付けを壊すことはありません。ネットワーク検出ポリシーで、失敗したログインのキャプチャを設定した場合、リストにはこのホストへのログインに失敗したユーザが含まれます。

ホスト プロファイル内のホスト属性

ホスト属性を使用して、ネットワーク環境にとって重要な方法でホストを分類することができます。Firepower システムには以下の 3 つのタイプの属性があります。

- 定義済みホスト属性
- ホワイトリスト ホスト属性
- ユーザ定義ホスト属性

定義済みホスト属性を設定後、またはユーザ定義ホスト属性を作成後は、ホスト属性の値を割り当てる必要があります。

（注） ホスト属性は、どのドメイン レベルでも定義できます。現在のドメインと先祖ドメインで作成されたホスト属性を割り当てることができます。

定義済みホスト属性

Firepower Management Center には、2 つの定義済みホスト変数が用意されています。

ホストの重要度（Host Criticality）

特定のホストの業務の重要性を指定し、ホストの重要性に応じて相関ポリシーの応答を調整するには、この属性を使用します。たとえば、業務にとって組織のメールサーバが一般的なユーザ ワークステーションよりも重要であるとみなしている場合は、メール サーバと業務に重要なその他のデバイスに [高（High）] の値を割り当て、他のホストには [中（Medium）] または [低（Low）] の値を割り当てることができます。その上で、影響を受けるホストの重要度に基づいて異なるアラートを起動する相関ポリシーを作成できます。

注記（Notes）

他のアナリストに確認してもらいたいホストに関する情報を記録するには、このホスト固有の属性を使用します。たとえば、ネットワーク上のコンピュータに、パッチが適用されていない古いバージョンのテスト用オペレーティング システムが搭載されている場合、[注記（Notes）] 属性を使用して、システムは意図的にパッチを適用していないことを明示できます。

ホワイト リストのホスト属性

ユーザが作成するそれぞれのコンプライアンス ホワイト リストによって、そのホワイト リストと同じ名前でホスト属性が自動的に作成されます。ホワイトリストのホスト属性に設定可能な値は、次のとおりです。

- 準拠（Compliant）：ホワイト リストに準拠しているホストを識別します。
- 非準拠（Non-Compliant）：ホワイト リストに違反しているホストを識別します。

- 未評価（Not Evaluated）：ホワイトリストの有効な対象ではないホスト、または何らかの理由で評価されていないホストを識別します。

ホワイト リストのホスト属性の値を編集したり、ホワイト リストのホスト属性を削除したりすることはできません。

ユーザ定義のホスト属性

定義済みのホスト属性またはホワイトリストのホスト属性で使用されている基準と異なる基準を使用してホストを識別する場合、ユーザ定義のホスト属性を作成することができます。例えば、以下を行うことができます。

- ホストに対してファシリティ コード、市町村、部屋番号などの物理的なロケーション ID を割り当てます。
- 特定のホストを担当するシステム管理者を示す担当者 ID を割り当てます。ホストに関連する問題が検出された場合、相関ルールとポリシーを作成して、適切なシステム管理者にアラートを送信することができます。
- ホストの IP アドレスに基づいて、事前定義されたリストからホストへ自動的に値を割り当てます。この機能は、ネットワーク上にホストが初めて表示されたときに、その新しいホストへ値を割り当てるために役立ちます。

ユーザ定義のホスト属性は、ホストプロファイルのページに表示されます。ここでホストごとに値を割り当てることができます。次のことも実行できます。

- 相関ポリシーと検索でホスト属性を使用します。
- イベントのホスト属性テーブル ビューで属性を表示して、それに基づいてレポートを生成します。

ユーザ定義のホスト属性として、次のタイプのいずれか 1 つを使用できます。

テキスト（Text）

ホストに対してテキスト文字列を手動で割り当てることができます。

整数（Integer）

正の整数の番号範囲の最初の数と最後の数を指定し、ホストに対してこれらの番号を手動で割り当てることができます。

リスト

文字列値のリストを作成し、ホストに対してこの値のいずれかを割り当てることができます。また、ホストの IP アドレスに基づいて、ホストに対して値を自動的に割り当てることもできます。

複数の IP アドレスを持つホストの 1 つの IP アドレスに基づいて値を自動的に割り当てると、これらの値は、ホストに関連付けられているすべてのアドレスに適用されます。[ホスト属性（Host Attributes）] テーブルを表示する場合は、このことに留意してください。

リストの値を自動的に割り当てる場合は、リテラルの IP アドレスではなくネットワークオブジェクトの使用を検討してください。このアプローチによって保守容易性を向上でき、特にマルチドメイン展開で有効です。これは、マルチドメイン展開でオーバーライドが有効になったオブジェクトを使用すると、子孫ドメインの管理者が先祖ドメインの設定を自分のローカル環境に合わせて調整できるためです。マルチドメイン展開では、子孫ドメインで重複した IP アドレスを使用している場合に意図しないホストに一致するのを避けるために、先祖ドメイン レベルで自動割り当てリストを定義する場合は注意してください。

URL

ホストに対して手動で URL の値を割り当てることができます。

ユーザ定義のホスト属性を削除すると、その属性が使用されているすべてのホストプロファイルから削除されます。

テキストまたは URL ベースのホスト属性の作成

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Any Security Analyst

ステップ 1 **[Analysis]** > **[Hosts]** > **[Host Attributes]**を選択します。
ステップ 2 [ホスト属性管理（Host Attribute Management）] をクリックします。
ステップ 3 [属性の作成（Create Attribute）] をクリックします。
ステップ 4 名前を入力します。
ステップ 5 ユーザ定義のホスト属性 （3181 ページ） の説明に従って作成する属性の [タイプ（Type）] を選択します。
ステップ 6 **[保存（Save）]** をクリックします。

整数ベースのホスト属性の作成

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Any Security Analyst

整数ベースのホスト属性を定義する場合は、その属性が受け入れる数値の範囲を指定する必要があります。

ステップ 1 **[Analysis]** > **[Hosts]** > **[Host Attributes]**を選択します。

ステップ 2 [ホスト属性管理（Host Attribute Management）] をクリックします。
ステップ 3 [属性の作成（Create Attribute）] をクリックします。
ステップ 4 名前を入力します。
ステップ 5 ユーザ定義のホスト属性（3181 ページ）の説明に従って、作成する属性の [タイプ（Type）] を選択します。
ステップ 6 [最小（Min）] フィールドに、ホストに対して割り当てることができる範囲の最小の整数値を入力します。
ステップ 7 [Max] フィールドに、ホストに対して割り当てることができる範囲の最大の整数値を入力します。
ステップ 8 **[保存（Save）]** をクリックします。

リストベースのホスト属性の作成

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Any Security Analyst

リストベースのホストの属性を定義する場合は、リストに対してそれぞれの値を提供する必要があります。これらの値には、英数字、スペース、および記号を含めることができます。

ステップ 1 **[Analysis]** > **[Hosts]** > **[Host Attributes]**を選択します。
ステップ 2 [ホスト属性管理（Host Attribute Management）] をクリックします。
ステップ 3 [属性の作成（Create Attribute）] をクリックします。
ステップ 4 名前を入力します。
ステップ 5 ユーザ定義のホスト属性（3181 ページ）の説明に従って、作成する属性の [タイプ（Type）] を選択します。
ステップ 6 リストに値を追加するには、[値の追加（Add Value）] をクリックします。
ステップ 7 [名前（Name）] フィールドに、追加する最初の値を入力します。
ステップ 8 オプションで、ホストに追加した属性値を自動で割り当てるには、[ネットワークを追加（Add Networks）] をクリックします。
ステップ 9 [値（Value）] ドロップダウン リストから、追加した値を選択します。
ステップ 10 [IP アドレス（IP Address）] および [ネットマスク（Netmask）] フィールドに、この値を自動的に割り当てる IP アドレスのブロックを表す IP アドレスとネットワーク マスク（IPv4）を入力します。
ステップ 11 リストにさらに値を追加して、IP アドレス ブロックの範囲内の新しいホストにこれらの値を自動的に割り当てるには、手順 6 ～ 10 を繰り返します。
ステップ 12 **[保存（Save）]** をクリックします。

ホスト属性値の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Any Security Analyst

事前定義またはユーザ定義のホスト属性に値を設定できます。システムによって生成されたホワイト リストのホスト属性値は設定できません。

ステップ 1 変更するホスト プロファイルを開きます。

ステップ 2 [属性（Attributes）] セクションで、[属性の編集（Edit Attributes）] をクリックします。

ステップ 3 必要に応じて、属性を更新します。

ステップ 4 **[保存（Save）]** をクリックします。

ホスト プロファイル内のホワイト リスト違反

コンプライアンス ホワイト リスト（またはホワイト リスト）は一連の基準であり、ユーザはこれを使用して、特定のサブネット上での実行が許可されるオペレーティング システム、アプリケーション プロトコル、クライアント、Web アプリケーション、およびプロトコルを指定することができます。

アクティブな相関ポリシーにホワイト リストを追加した場合に、システムでホワイト リストに違反しているホストが検出されると、Firepower Management Centerはホワイト リストのイベント（相関イベントの特別な種類）をデータベースに記録します。これらのホワイト リスト イベントはそれぞれホワイトリスト違反に関連付けられます。これには、特定のホストがどのようにホワイトリストに違反しているか、および違反している理由が含まれています。あるホストが1つ以上のホワイト リストに違反している場合、ホスト プロファイルにおいて、2つの方法でこれらの違反を参照することができます。

最初に、ホスト プロファイルに、ホストに関連付けられている個々のホワイト リストの違反がすべて一覧表示されます。

次に、ホスト プロファイルにおけるホワイト リスト違反の情報について説明します。

タイプ

違反のタイプ（つまり、違反がオペレーティング システム、アプリケーション、サーバ、またはプロトコルの非準拠の結果として生じたかどうか）。

理由

違反についての特別な理由。たとえば、Microsoft Windows のホストのみを許可するホワイトリストがある場合、ホストプロファイルには、ホストで稼動している現行のオペレーティング システム（`Linux Linux 2.4、2.6` など）が表示されます。

White List

違反に関連付けられているホワイト リストの名前。

次に、オペレーティング システム、アプリケーション、プロトコル、およびサーバに関連付けられているセクションで、Firepower Management Centerは、非準拠の要素にホワイト リスト違反のアイコン（）のマークを付けます。たとえば、Microsoft Windows ホストのみを許可するホワイト リストでは、ホスト プロファイルで、ホストのオペレーティング システム情報の隣にホワイト リスト違反のアイコンが表示されます。

（注） ホストのプロファイルを使用すると、コンプライアンスホワイトリストの共有ホストプロファイルを作成することができます。

共有ホワイト リスト ホスト プロファイルの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Any Security Analyst

コンプライアンス ホワイト リストに対する共有ホスト プロファイルは、複数のホワイト リストをまたがるターゲットホスト上で実行を許可されるオペレーティング システム、アプリケーションプロトコル、クライアント、Webアプリケーション、およびプロトコルを指定します。つまり、複数のホワイト リストを作成するが、同じホスト プロファイルを使用して複数のホワイト リストで特定のオペレーティング システムを実行するホストを評価する場合は、共有のホスト プロファイルを使用します。

既知の IP アドレスを持つ任意のホストのホスト プロファイルを使用して、コンプライアンス ホワイト リストで使用できる共有ホスト プロファイルを作成することができます。ただし、システムでホストのオペレーティング システムをまだ特定していない場合は、個々のホストのホスト プロファイルに基づいて共有ホスト プロファイルを作成することはできないことに注意してください。

ステップ 1 ホスト プロファイルで、[ホワイト リスト プロファイルの生成（Generate White List Profile）] をクリックします。

ステップ 2 特別なニーズに応じて、共有ホスト プロファイルを変更し、保存します。

関連トピック

ホワイト リスト ホスト プロファイルの作成 （2688 ページ）

ホスト プロファイルでのマルウェア検出

[最後に検出されたマルウェア（Most Recent Malware Detections）] セクションには、ホストがマルウェア ファイルを送信または受信した、最近のマルウェア イベントが最大 100 個表示されます。ホスト プロファイルには、ネットワークベースのマルウェア イベント（ネットワーク向け AMP によって生成されたもの）とエンドポイントベースのマルウェア イベント（エンドポイント向け AMP によって生成されたもの）の両方のリストが示されます。

ファイルが遡ってマルウェアと識別されたファイル イベントにホストが関係している場合、ファイルが送信された元のイベントは、マルウェアの特定が行われた後で、マルウェアの検出リストに表示されます。マルウェアとして識別されたファイルが、マルウェアではないと遡って判断された場合、そのファイルに関連するマルウェア イベントはリストには表示されなくなります。たとえば、ファイルの性質が `Malware` であり、これが `Clean` に変わった場合、そのファイルのイベントは、ホスト プロファイル上のマルウェア検出リストから削除されます。

ホスト プロファイルでマルウェアの検出を確認する際には、マルウェア アイコン（  ）をクリックして、そのホストのマルウェア イベントを確認できます。

次に、ホスト プロファイルの [最新のマルウェア検出（Most Recent Malware Detections）] セクションの列について説明します。

Time

イベントが生成された日時。

ファイルがマルウェアであると遡って特定されたイベントでは、これはマルウェアが特定された時刻ではなく、元のイベントの時刻であることに注意してください。

Host Role

検出されたマルウェアの伝送におけるホストのロール（送信側または受信側）。エンドポイント向け AMP によって生成されたマルウェア イベント（「エンドポイントベースのマルウェア イベント」）の場合、ホストは常に受信者になります。

[脅威名（Threat Name）]

検出されたマルウェアの名前。

File Name

マルウェア ファイルの名前。

File Type

ファイルのタイプ（`PDF` や `MSEXE` など）。

ホスト プロファイルの脆弱性

ホスト プロファイルの [脆弱性（Vulnerabilities）] セクションには、ホストに影響を与える脆弱性が示されます。これらの脆弱性は、システムがホスト上で検出したオペレーティング システム、サーバ、およびアプリケーションに基づきます。

ホストのオペレーティング システムのアイデンティティ、またはホスト上のアプリケーション プロトコルのアイデンティティのいずれかで、アイデンティティの競合が発生している場合、システムは、競合が解決するまで両方のアイデンティティに対して脆弱性を表示します。

NetFlowデータからネットワーク マップに追加されたホストに使用可能なオペレーティング システムの情報はないので、システムは、それらのホストに作用する侵入イベントに対し脆弱な（インパクト レベル1：赤）インパクト レベルを割り当てることができません。このような場合は、ホスト入力機能を使用して、ホストのオペレーティング システム ID を手動で設定します。

サーバのベンダーおよびバージョンの情報は、ほとんどの場合はトラフィックに含まれていません。デフォルトでは、システムはこのようなトラフィックの送信側および受信側に対して、関連付けられている脆弱性をマップしません。ただし、ベンダーまたはバージョンの情報を持たない特定のアプリケーション プロトコルに対して脆弱性をマップするよう、システムを設定することができます。

ホストの入力機能を使用して、ネットワーク上のホストにサードパーティの脆弱性情報を追加すると、追加の [脆弱性（Vulnerabilities）] セクションが表示されます。たとえば QualysGuard Scanner から脆弱性をインポートすると、ホスト プロファイルには [QualysGuard 脆弱性（QualysGuard Vulnerabilities）] セクションが含まれます。サードパーティの脆弱性の場合は、ホスト プロファイルの対応する [脆弱性（Vulnerabilities）] セクションの情報は、ホストの入力機能を使用して脆弱性データをインポートしたときに提供した情報に制限されます。

サードパーティの脆弱性をオペレーティング システムおよびアプリケーション プロトコルと関連付けることはできますが、クライアントに関連付けることはできません。サードパーティの脆弱性のインポートについては、『*Firepower* システム ホスト入力 *API* ガイド』を参照してください。

次に、ホスト プロファイルの [脆弱性（Vulnerabilities）] セクションのカラムについて説明します。

[名前（Name）]

脆弱性の名前。

Remote

脆弱性がリモートで不正利用される可能性があるかどうかを示します。この列が空白の場合、脆弱性の定義にはこの情報は含まれていません。

Component

脆弱性に関連付けられているオペレーティング システム、アプリケーション プロトコル、またはクライアントの名前。

Port

ポート番号（脆弱性が、特定のポート上で実行されているアプリケーションプロトコルに関連付けられている場合）。

関連トピック

脆弱性データのフィールド （3237 ページ）
脆弱性の非アクティブ化 （3240 ページ）

脆弱性に対するパッチのダウンロード

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Any Security Analyst

ネットワーク上のホストで検出された脆弱性を軽減するためのパッチをダウンロードできます。

ステップ 1 パッチをダウンロードするホストのホスト プロファイルにアクセスします。
ステップ 2 [Vulnerabilities] セクションを展開します。
ステップ 3 パッチを適用する脆弱性の名前をクリックします。
ステップ 4 [修正（Fixes）] セクションを展開して、脆弱性に対するパッチの一覧を表示します。
ステップ 5 ダウンロードするパッチの隣の [ダウンロード（Download）] をクリックします。
ステップ 6 パッチをダウンロードして、影響を受けるシステムに適用します。

個々のホストに対する脆弱性の非アクティブ化

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Any Security Analyst

ホストの脆弱性エディタを使用して、ホストごとに脆弱性を非アクティブにすることができます。ホストの脆弱性を非アクティブにしても、そのホストの影響の相関に対して脆弱性は使用されますが、影響レベルは自動的に 1 レベル減少します。

ステップ 1 ホスト プロファイルの [脆弱性（Vulnerabilities）] セクションに移動します。

ステップ 2 [脆弱性の編集（Edit Vulnerabilities）] をクリックします。

ステップ 3 [有効な脆弱性（Valid Vulnerabilities）] リストから脆弱性を選択し、下矢印をクリックして [無効な脆弱性（Invalid Vulnerabilities）] リストに移動します。

ヒント 隣接している複数の脆弱性を選択するには、クリックおよびドラッグを使用します。脆弱性をダブルクリックして、リスト間を移動することもできます。

ステップ 4 [保存（Save）] をクリックします。

次のタスク

- 必要に応じて、ホストの脆弱性を [無効な脆弱性（Invalid Vulnerabilities）] リストから [有効な脆弱性（Valid Vulnerabilities）] リストに移動して、脆弱性をアクティブ化します。

関連トピック

個々の脆弱性の非アクティブ化 （3189 ページ）
複数の脆弱性の非アクティブ化 （3242 ページ）

個々の脆弱性の非アクティブ化

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Any Security Analyst

ホスト プロファイルで脆弱性を非アクティブ化すると、ネットワーク マップにあるすべてのホストに対して脆弱性が非アクティブ化されます。ただし、いつでもその脆弱性を再アクティブ化することができます。

マルチドメイン展開では、先祖ドメインで脆弱性を非アクティブ化すると、すべての子孫ドメインでその脆弱性が非アクティブ化されます。リーフ ドメインでは、脆弱性が先祖ドメインでアクティブ化された場合、リーフ ドメインのデバイスの脆弱性をアクティブ化または非アクティブ化できます。

ステップ 1 次のようにして、脆弱性の詳細にアクセスします。

- 影響を受けるホスト プロファイルで、[脆弱性（Vulnerabilities）] セクションを展開し、有効または無効にする脆弱性の名前をクリックします。
- 事前定義されたワークフローで、**[Analysis]** > **[Hosts]** > **[Vulnerabilities]** を選択し、有効または無効にする脆弱性の横にある表示アイコン（  ）をクリックします。

ステップ 2 [影響を受ける条件（Impact Qualification）] ドロップダウン リストから [無効（Disabled）] を選択します。

コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 ネットワーク マップ上のすべてのホストに対して、[影響を受ける条件（Impact Qualification）] の値を変更することを確認します。

ステップ 4 [完了（Done）] をクリックします。

次のタスク

- オプションで、上記の手順を実行中に、[影響を受ける条件（Impact Qualification）] ドロップダウン リストから [有効（Enabled）] を選択することによって、脆弱性をアクティブにします。

関連トピック

個々のホストに対する脆弱性の非アクティブ化 （3188 ページ）
複数の脆弱性の非アクティブ化 （3242 ページ）
オペレーティング システムのアイデンティティの競合 （3168 ページ）

ホスト プロファイルのスキャン結果

Nmap を使用してホストをスキャンする場合、または Nmap のスキャンから結果をインポートする場合、これらの結果は、スキャンに含まれているすべてのホストのホストプロファイルに表示されます。

Nmap が、ホストのオペレーティング システムについて、およびオープンでフィルタリングされていないポート上で稼動している任意のサーバについて収集した情報が、ホストプロファイルの [Operating System] と [Servers] セクションにそれぞれ追加されます。また、Nmap は、そのホストのスキャン結果のリストを [スキャン結果（Scan Results）] セクションに追加します。プロファイルに [スキャン結果（Scan Results）] セクションが表示されるのは、スキャンでホスト上のオープン ポートが検出された場合のみであることに注意してください。

各結果には、情報のソース、スキャンしたポートの番号とタイプ、ポート上で稼動しているサーバの名前、Nmap で検出された任意の追加情報（ポートの状態やサーバのベンダー名など）が示されます。UDP ポートをスキャンする場合、そのポートで検出されたサーバは [Scan Results] セクションにのみ表示されます。

ホスト プロファイルから Nmap スキャンを実行できることに注意してください。

ホスト プロファイルからのホストのスキャン

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin

ホストプロファイルから、ホストに対してNmapスキャンを実行できます。スキャンが完了すると、そのホストのサーバおよびオペレーティング システムの情報は、ホスト プロファイルで更新されます。追加のスキャン結果は、すべてホストプロファイルの[Scan Results]セクションに追加されます。

注意 Nmap 提供のサーバおよびオペレーティング システムのデータは、別の Nmap スキャンを実行するか、より優先度の高いホスト入力で上書きするまでスタティックなままになります。Nmap を使用したホストのスキャンを計画している場合は、定期的にスキャンをスケジュールします。

始める前に

- Nmapスキャンインスタンスを追加します。Nmapスキャンインスタンスの追加（2534ページ）を参照してください。

ステップ1 ホスト プロファイルで、[ホストのスキャン（Scan Host）] をクリックします。

ステップ2 ホストのスキャンに使用するスキャン修復の横にある [スキャン（Scan）] をクリックします。
システムによってホストがスキャンされ、ホスト プロファイルに結果が追加されます。

関連トピック

Nmap スキャンの自動化 （243 ページ）

第 129 章

ディスカバリ イベントの操作

以下のトピックでは、ディスカバリ イベントを操作する方法について説明します。

検出イベントの検出データとアイデンティティ データ

システムは、モニタ対象のネットワークで検出された変更を表すイベントのテーブルを生成します。このテーブルを使用して、ネットワークのユーザアクティビティを確認し、応答方法を決定できます。ネットワーク検出およびアイデンティティポリシーは、収集するデータ、モニタするネットワーク セグメント、およびそのために使用する特定のハードウェア インターフェイスの種類を指定します。

検出およびアイデンティティ イベント テーブルを使用して、ネットワークのホスト、アプリケーション、およびユーザに関連付けられている脅威を特定できます。システムには事前定義のワークフローセットが用意されており、これを使用して、システムで生成されるイベントを分析することができます。また、特定のニーズに合った情報のみを表示するカスタム ワークフローを作成することもできます。

分析用にネットワーク検出およびアイデンティティ データを収集し、保存するには、ネットワーク検出およびアイデンティティ ポリシーを設定する必要があります。アイデンティティ ポリシーを設定した後、アクセス コントロール ポリシーで呼び出して、トラフィックのモニタに使用するデバイスに展開する必要があります。

ネットワーク検出ポリシーは、ホスト、アプリケーション、および権限のないユーザデータを提供します。アイデンティティ ポリシーは、権限のあるユーザ データを提供します。

次の検出イベント テーブルは、[分析（Analysis）] > [ホストおよび分析（Hosts and Analysis）] > [ユーザ（Users）] メニューにあります。

検出イベント テーブル	検出データが入力されますか。	アイデンティティ データが入力されますか。
ホスト（Hosts）	あり	なし
ホストの侵害の兆候	あり	なし
アプリケーション	あり	なし
アプリケーション詳細（Application Details）	あり	なし
サーバ	あり	なし
ホスト属性（Host Attributes）	あり	なし
検出イベント（Discovery Events）	あり	あり
ユーザの侵害の兆候（User Indications of Compromise）	あり	あり
アクティブ セッション（Active Sessions）	あり	あり
ユーザ アクティビティ（User Activity）	あり	あり
ユーザ （Users）	あり	あり
脆弱性（Vulnerabilities）	あり	なし
サード パーティの脆弱性（Third-Party Vulnerabilities）	あり	なし

ディスカバリ イベントの統計情報の表示

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Any Security Analyst

[ディスカバリ統計情報（Discovery Statistics）] ページには、システムで検出されたホスト、イベント、プロトコル、アプリケーション プロトコル、オペレーティング システムの概要が表示されます。

ページには、最後の 1 時間の統計情報、および累計の統計情報が示されます。特定のデバイス、またはすべてのデバイスについての統計情報を表示することができます。サマリに示されているイベント、サーバ、オペレーティング システム、またはオペレーティング システムの

ベンダーをクリックして、ページ上のエントリに一致するイベントを表示することもできます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

ステップ 1 **[Overview]** > **[Summary]** > **[Discovery Statistics]**を選択します。

ステップ 2 [デバイスの選択（Select Device）] リストから、統計情報を表示するデバイスを選択します。オプションで、Firepower Management Center で管理されるすべてのデバイスの統計情報を表示するには、[すべて（All）] を選択します。

ステップ 3 次の選択肢があります。

- [統計情報サマリ（Statistics Summary）] セクション（3195 ページ）で説明されているように、[統計サマリー（Statistics Summary）] に一般的な統計情報を表示します。
- [イベントの中断（Event Breakdown）] で、表示するイベント タイプをクリックします。イベントが 1 つも表示されない場合は、時間枠の変更（2956 ページ）で説明されているように、時間範囲を調整する必要があるかもしれません。
- [プロトコルの中断（Protocol Breakdown）] で、検出されたホストによって現在使用されているプロトコルを表示します。
- [アプリケーション プロトコルの中断（Application Protocol Breakdown）] で、表示するアプリケーション プロトコルの名前をクリックします。
- [OS の中断（OS Breakdown）] で、[OS 名（OS Name）] または [OS ベンダー（OS Vendor）] をクリックします。

関連トピック

[イベント分類（Event Breakdown）] セクション （3197 ページ）
[プロトコル分類（Protocol Breakdown）] セクション （3197 ページ）
[アプリケーション プロトコル分類（Application Protocol Breakdown）] セクション （3197 ページ）
[OS 分類（OS Breakdown）] セクション （3197 ページ）

[統計情報サマリ（Statistics Summary）] セクション

[統計情報サマリ （Statistics Summary）] セクションの行の説明は次のとおりです。

Total Events

Firepower Management Centerに格納されているディスカバリ イベントの合計数。

Total Events Last Hour

最後の 1 時間に生成されたディスカバリ イベントの合計数。

Total Events Last Day

最後の 1 日に生成されたディスカバリ イベントの合計数。

Total Application Protocols

検出されたホストで実行されているサーバのアプリケーション プロトコルの合計数。

Total IP Hosts

一意の IP アドレスによって特定された検出済みホストの合計数。

Total MAC Hosts

IP アドレスで特定されない検出済みホストの合計数。

すべてのデバイス、または特定のデバイスのどちらについてのディスカバリ統計情報を参照している場合でも、[Total MAC Hosts] の統計情報は同じになることに注意してください。これは、管理対象デバイスがIPアドレスに基づいてホストを検出するためです。この統計情報は、他の方法によって識別され、特定の管理対象デバイスに依存しないすべてのホストの合計を表します。

Total Routers

ルータとして識別された検出ノードの合計数

Total Bridges

ブリッジとして識別された検出ノードの合計数

Host Limit Usage

使用中のホスト制限のパーセンテージ合計。ホストの制限は、Firepower Management Center のモデルによって定義されます。すべての管理対象デバイスについての統計情報を表示している場合は、ホストの使用制限のみが表示されることに注意してください。

（注） ホストの制限に達してホストが削除されると、ディスカバリ データを消去するネットワーク マップ上にホストは表示されなくなります。

最後に受け取ったイベント（Last Event Received）

最後のディスカバリ イベントが行われた日付と時間。

Last Connection Received

最後の接続が完了した日付と時間。

[イベント分類（Event Breakdown）] セクション

[イベント分類（Event Breakdown）] セクションには、データベースに格納されている各イベントタイプの合計数のカウントの他に、ネットワーク検出の各タイプのカウント、および最後の 1 時間で発生したホスト入力イベントが示されます。

[イベント分類（Event Breakdown）] セクションを使用して、ディスカバリ イベントおよびホスト入力イベントの詳細を表示することもできます。

関連トピック

検出イベントおよびホスト入力イベント （3201 ページ）

[プロトコル分類（Protocol Breakdown）] セクション

[プロトコル分類（Protocol Breakdown）] セクションには、検出されたホストで使用されているプロトコルが示されます。このセクションには、検出されたそれぞれのプロトコル名、プロトコル スタックの「レイヤ」、およびプロトコルを使用して通信しているホストの合計数が表示されます。

[アプリケーション プロトコル分類（Application Protocol Breakdown）] セクション

[アプリケーション プロトコル分類（Application Protocol Breakdown）] セクションには、検出されたホストで使用されているアプリケーション プロトコルが示されます。このセクションでは、プロトコル名、最後の 1 時間にアプリケーション プロトコルを実行したホストの合計数、いずれかのポイントでプロトコルの実行が検出されたホストの合計数を表示します。

[アプリケーション プロトコル分類（Application Protocol Breakdown）] セクションではさらに、検出されたプロトコルを使用しているサーバの詳細を表示することもできます。

関連トピック

サーバ データ （3226 ページ）

[OS 分類（OS Breakdown）] セクション

[OS 分類（OS Breakdown）] セクションには、監視対象ネットワーク上で稼動しているオペレーティング システム、およびオペレーティング システムのベンダー、各オペレーティング システムを実行しているホストの合計数が示されます。

オペレーティング システムの名前またはバージョンの値が `unknown` の場合は、オペレーティング システムまたはそのバージョンが、システムのフィンガープリントの内容と一致しないことを意味します。値が `pending` の場合は、オペレーティング システムまたはそのバージョンを識別するための十分な情報がシステムで収集されていないことを意味します。

[OS 分類（OS Breakdown）] セクションを使用して、検出されたオペレーティング システムの詳細を表示することができます。

関連トピック

ホスト データ （3211 ページ）

ディスカバリ パフォーマンス グラフの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Maint

ディスカバリ イベントを使用して、管理対象デバイスのパフォーマンス統計情報を示すグラフを生成することができます。

新しいデータは、統計情報のグラフに5分ごとに累積されます。したがって、グラフをすばやくリロードしても、次の5分の差分更新が実行されるまでデータは変更されていない場合があります。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

始める前に

適切なネットワーク検出ポリシーを編集して、アプリケーション、ホスト、およびユーザを含めます（これは、システムパフォーマンスに影響を与える可能性があります）。ネットワーク検出ルールの設定（2650ページ）およびアクションと検出されるアセット（2651ページ）を参照してください。

ステップ 1 **[Overview]** > **[Summary]** > **[Discovery Performance]**を選択します。

ステップ 2 [デバイスの選択（Select Device）] リストから、Firepower Management Center または対象とする管理対象デバイスを選択します。

ステップ 3 ディスカバリ パフォーマンス グラフ タイプ（3198ページ）で説明されているように、[グラフの選択（Select Graph(s)）] リストから、作成するグラフの種類を選択します。

ステップ 4 [時間範囲の選択（Select Time Range）] リストから、グラフに使用する時間範囲を選択します。

ステップ 5 [グラフ（Graph）] をクリックして、選択した統計情報をグラフ化します。

ディスカバリ パフォーマンス グラフ タイプ

次に、使用できるグラフのタイプについて説明します。

Processed Events/Sec

Data Correlator が 1 秒間に処理するイベントの数を表します。

Processed Connections/Sec

Data Correlator が 1 秒間に処理する接続の数を表します。

Generated Events/Sec

システムが 1 秒間に生成するイベントの数を表します。

Mbits/Sec

ディスカバリ プロセスによって 1 秒間に分析されたトラフィック数（メガビット）を表します。

Avg Bytes/Packet

ディスカバリ プロセスによって分析された各パケットに含まれるバイト数の平均を表します。

K Packets/Sec

ディスカバリ プロセスで 1 秒間に分析されるパケット数を 1000 単位で表します。

ディスカバリおよびアイデンティティワークフローの使用

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	タスクに依存

Firepower Management Center は、ネットワークで生成されるディスカバリおよびアイデンティティ データの分析で使用できるイベント ワークフロー セットを提供します。ワークフローはネットワーク マップとともに、ネットワーク資産に関する主要な情報源になります。

Firepower Management Center には、ディスカバリおよびアイデンティティ データ、検出されたホストとそのホストの属性、サーバ、アプリケーション、アプリケーションの詳細、脆弱性、ユーザ アクティビティ、ユーザに関する事前定義されたワークフローが用意されています。ユーザはカスタム ワークフローを作成することもできます。

ステップ 1 事前定義されたワークフローにアクセスするには、以下を実行します。

- ディスカバリとホスト入力データ：ディスカバリ イベントとホスト入力イベントの表示 （3209 ページ）を参照してください。
- ホスト データ：ホスト データの表示 （3211 ページ）を参照してください。
- ホスト属性データ：ホスト属性の表示 （3218 ページ）を参照してください。

- ホストまたはユーザの侵害の兆候データ：侵害兆候データの表示と処理（3221 ページ）を参照してください。
- サーバ データ：サーバ データの表示 （3227 ページ）を参照してください。
- アプリケーション データ：アプリケーション データの表示 （3231 ページ）を参照してください。
- アプリケーション詳細データ：アプリケーション詳細データの表示 （3234 ページ）を参照してください。
- アクティブ セッション データ：アクティブ セッション データの表示 （3255 ページ） を参照してください。
- ユーザ データ：ユーザ データの表示 （3259 ページ）を参照してください。
- ユーザ アクティビティ データ：ユーザ アクティビティ データの表示 （3262 ページ）を参照してください。
- ネットワーク マップ：ネットワーク マップの表示 （2864 ページ）を参照してください。

ステップ 2 カスタム ワークフローにアクセスするには、**[Analysis]** > **[Advanced]** > **[Custom Workflows]** を選択します。

ステップ 3 カスタム テーブルに基づいたワークフローにアクセスするには、**[Analysis]** > **[Advanced]** > **[Custom Tables]** を選択します。

ステップ 4 以下のいずれかのアクションを実行します。これらは、ネットワーク検出ワークフローでアクセスするすべてのページに共通です。

- カラムの制約：表示されるカラムを制約にするには、非表示にするカラムの見出しにある閉じるアイコン（ ）をクリックします。表示されるポップアップ ウィンドウで、[適用（Apply）] をクリックします。

  ヒント 他のカラムを表示または非表示にするには、[適用（Apply）] をクリックする前に、該当するチェック ボックスをオンまたはオフにします。無効にしたカラムをビューに戻すには、展開の矢印をクリックして検索制約を展開し、[無効にされたカラム（Disabled Columns）] の下のカラム名をクリックします。

- 削除：現在の制約されたビューにある一部またはすべての項目を削除するには、削除する項目の横にあるチェックボックスをオンにし、[削除（Delete）] または [すべて削除（Delete All）] をクリックします。これらのアイテムが再検出されても、システムのディスカバリ機能が再開されるまで、これらのアイテムは削除されたままになります。

  注意 [分析（Analysis）] > [ユーザ（Users）] > [アクティブ セッション（Active Sessions）] ページで VPN 以外のセッションを削除する前に、セッションが実際に閉じられていることを確認します。アクティブなセッションを削除すると、該当するポリシーはデバイス上のセッションを検出できなくなります。そのため、モニタしたり、ブロックしたりするようポリシーが設定されていたとしても、セッションはそれらのアクションを実行しません。

  （注） [分析（Analysis）] > [ユーザ（Users）] > [アクティブ セッション（Active Sessions）] ページの VPN セッションに関する詳細については、「リモート アクセス VPN の現在のユーザの表示」を参照してください。

（注） サードパーティの場合とは異なり、シスコの脆弱性は削除**できません**。ただし、確認済みとしてマークすることはできます。

- ドリル ダウン：ワークフローの次のページにドリルダウンするには、ドリルダウン ページの使用 （2940 ページ）を参照してください。
- 現在のページを移動する：現在のワークフローページ内を移動するには、ワークフロー ページのナビゲーション ツール （2937 ページ）を参照してください。
- ワークフロー内で移動する：現在の制約を維持しながら現在のワークフローのページ間で移動するには、ワークフロー ページの左上にある該当するページ リンクをクリックします。
- 他のワークフローに移動する：関連するイベントを調べるために、その他のイベント ビューに移動するには、ワークフロー間のナビゲーション （2963 ページ）を参照してください。
- データのソート：ワークフローでデータをソートするには、カラムのタイトルをクリックします。ソート順を逆にするには、カラムのタイトルをもう一度クリックします。
- ホスト プロファイルの表示：IP アドレスのホスト プロファイルを表示するには、ホスト プロファイルのアイコン（  ）をクリックします。アクティブな侵害の兆候（IOC）タグのあるホストの場合は、IP アドレスの横に表示される侵害されたホストのアイコン（  ）をクリックします。
- User Profile — To view user identity information, click the user icon that appears next to the user identity ( , or for users associated with IOCs, ). の表示

関連トピック

ワークフローの使用 （2931 ページ）
FMC データベースからのデータの消去 （261 ページ）

検出イベントおよびホスト入力イベント

システムは検出イベントを生成します。このイベントは、監視対象ネットワークセグメントにおける変更の詳細をやり取りします。新しく検出されたネットワーク機能に対しては、新しいイベントが生成され、以前に認識されたネットワーク資産における何らかの変更に対しては、変更のイベントが生成されます。

最初のネットワーク検出のフェーズ中に、システムは各ホスト、および各ホスト上での稼動が検出された TCP または UDP サーバについて、新しいイベントを生成します。必要に応じて、エクスポートされた NetFlow レコードを使用してこれらの新しいホストおよびサーバのイベントを生成するよう、システムを設定することができます。

またシステムは、検出された各ホスト上で稼動しているネットワーク、トランスポート、およびアプリケーションプロトコルのそれぞれに対して新しいイベントを生成します。設定されている検出ルールでアプリケーションプロトコルの検出を無効にして、NetFlow エクスポータをモニタできますが、Firepower システムの管理対象デバイスをモニタするよう設定された検出

ルールではできません。NetFlow 以外の検出ルールでホストまたはユーザの検出を有効にすると、アプリケーションが自動的に検出されます。

最初のネットワーク マッピングが完了すると、続けてシステムは、変更イベントを生成し、ネットワークの変更を記録します。変更イベントは、以前に検出された資産の設定が変更されるたびに生成されます。

検出イベントが生成されると、データベースに記録されます。Firepower Management Center の Web インターフェイスを使用して、検出イベントを表示、検索、および削除できます。また、相関ルールで検出イベントを使用することもできます。ユーザが指定する他の基準だけでなく、生成される検出イベントのタイプに基づいて、相関ルールを作成することができます。相関ルールは相関ポリシーで使用され、ネットワーク トラフィックが基準を満たしたときに、修復、syslog、SNMP、および電子メール アラートの応答を起動します。

ホスト入力機能を使用して、ネットワーク マップにデータを追加することができます。オペレーティング システムの情報を追加、修正、または削除することができますが、この場合、システムは対象のホストに対する情報の更新を停止します。アプリケーション プロトコル、クライアント、サーバ、およびホストの属性を手動で追加、変更、または削除することも、脆弱性の情報を変更することもできます。この処理を行う場合、システムはホスト入力機能を生成します。

ディスカバリ イベント タイプ

ネットワーク検出ポリシーにシステムが記録するディスカバリ イベントのタイプを設定できます。ディスカバリ イベントのテーブルを表示すると、[イベント（Event）] カラムにイベント タイプが表示されます。次に、ディスカバリ イベント タイプについて説明します。

ホストの追加 MAC の検出

このイベントは、以前に検出したホストに対してシステムが新しい MAC アドレスを検出したときに生成されます。

このイベントは多くの場合、ルータを通じてトラフィックを渡すホストをシステムが検出したときに生成されます。それぞれのホストには 1 つの IP アドレスがありますが、これらの IP アドレスはすべて、ルータに関連付けられている MAC アドレスを持っているように見えます。システムは IP アドレスに関連付けられている実際の MAC アドレスを検出すると、ホスト プロファイル内でその MAC アドレスを太字で表示し、イベント ビューのイベント説明に「ARP/DHCP detected」のメッセージを表示します。

クライアント タイムアウト

このイベントは、非アクティブであるという理由で、システムがデータベースからクライアントをドロップしたときに生成されます。

クライアント更新

このイベントは、HTTP トラフィック内でシステムがペイロード（つまり音声やビデオ、Web メールなどの特別なタイプのコンテンツ）を検出したときに生成されます。

DHCP：IP アドレスの変更

このイベントは、DHCP アドレスの割り当てによってホスト IP アドレスが変わったことがシステムで検出された場合に生成されます。

DHCP：IP アドレスの再割り当て

このイベントは、ホストが IP アドレスを再利用するとき、つまり他の物理ホストが以前に使用した IP アドレスを、別のホストが DHCP の IP アドレス割り当てによって取得した場合に生成されます。

Hops Change

このイベントは、ホストと、そのホストを検出するデバイス間でシステムがネットワーク ホップ数の変更を検出した場合に生成されます。これは次のような場合に発生します。

- デバイスがさまざまなルータを介してホストのトラフィックを監視しており、ホストの場所についてより適切な決定ができる場合。
- デバイスがホストから ARP 送信を検出し、ホストがローカル セグメント上にあることを示している場合。

ホスト削除：ホスト制限に到達

このイベントは、Firepower Management Center 上でホストの制限を超えて、のネットワーク マップから監視対象のホストが削除されたときに生成されます。

ホスト ドロップ：ホスト制限に到達

このイベントは、Firepower Management Center上でホストの制限に達して新しいホストがドロップされたときに生成されます。このイベントとの相違点として、前述のイベントでは、ホストの制限に達したときに古いホストがネットワーク マップから削除されます。

ホストの制限に達したときに新しいホストをドロップするには、**[ポリシー（Policies）]** > **[ネットワーク検出（Network Discovery）]** > **[詳細（Advanced）]** を選択し、[ホストの制限に達した場合（When Host Limit Reached）] を [ホストをドロップ（Drop hosts）] に設定します。

ホスト IOC 設定

このイベントは、ホストに対して IOC（侵害の痕跡）が設定され、アラートが生成されたときに生成されます。

ホスト タイムアウト

このイベントは、ネットワーク検出ポリシーで定義された間隔内でホストがトラフィックを生成しなかったために、ネットワーク マップからホストがドロップされたときに生成されます。個々のホストの IP アドレスと MAC アドレスはそれぞれタイムアウトになることに注意してください。関連付けられているアドレスがすべてタイムアウトになるまで、ホストはネットワーク マップから消えません。

ネットワーク検出ポリシーで監視するネットワークを変更する場合は、ネットワーク マップから古いホストを手動で削除して、それらのホストがホストの制限に不利に作用しないようにします。

ネットワーク デバイスへのホスト タイプの変更

このイベントは、システムが、検出されたホストが実際はネットワーク デバイスであったことを認識したときに生成されます。

アイデンティティ競合

このイベントは、システムが、新しいサーバまたはオペレーティング システムに対する現行のアクティブなアイデンティティと競合する、そのサーバまたはオペレーティング システムのアイデンティティを検出したときに生成されます。

より新しいアクティブなアイデンティティ データを取得するためにホストを再スキャンして、アイデンティティの競合を解決する場合は、Identity Conflict イベントを使用して Nmap の修復をトリガーできます。

アイデンティティ タイムアウト

このイベントは、アクティブなソースからのサーバまたはオペレーティング システムの ID データがタイムアウトしたときに生成されます。

より新しいアクティブなアイデンティティ データを取得するために、ホストを再スキャンしてアイデンティティ データをリフレッシュする場合は、Identity Conflict イベントを使用して Nmap の修復をトリガーできます。

MAC 情報の変更

このイベントは、特定の MAC アドレスまたは TTL 値に関連付けられている情報で、システムが変更を検出したときに生成されます。

このイベントは多くの場合、ルータを通じてトラフィックを渡すホストをシステムが検出したときに発生します。各ホストにはそれぞれ異なる IP アドレスがありますが、これらの IP アドレスはすべて、ルータに関連付けられている MAC アドレスを持っているように見えます。システムは IP アドレスに関連付けられている実際の MAC アドレスを検出すると、ホスト プロファイル内でその MAC アドレスを太字で表示し、イベント ビューのイベント説明に「ARP/DHCP detected」のメッセージを表示します。TTL は変わる可能性がありますが、これはトラフィックが複数のルータを通じて渡される可能性があるためです。また、システムがホストの実際の MAC アドレスを検出した場合も TTL が変わる可能性があります。

NETBIOS 名の変更

このイベントは、システムがホストの NetBIOS 名に対する変更を検出したときに生成されます。このイベントは、NetBIOS プロトコルを使用するホストに対してのみ生成されます。

新しいクライアント

このイベントは、システムが新しいクライアントを検出したときに生成されます。

（注） 分析用にクライアントデータを収集および格納するには、ネットワーク検出ポリシーのディスカバリ ルールでアプリケーションの検出が有効になっていることを確認します。

新しいホスト

このイベントは、システムがネットワーク上で稼動している新しいホストを検出したときに生成されます。

このイベントは、デバイスが新しいホストを含むNetFlowデータを処理するときも生成できます。この状況でイベントを生成するには、NetFlow データを管理するネットワーク検出ルールでホストを検出するように設定します。

新しいネットワーク プロトコル

このイベントは、ホストが新しいネットワーク プロトコル（IP、ARP など）と通信していることをシステムが検出したときに生成されます。

新しい OS

このイベントは、システムがホストの新しいオペレーティング システムを検出した、またはホストのオペレーティング システムで変更を検出したときに生成されます。

新しい TCP ポート

このイベントは、ホスト上でアクティブな新しい TCP サーバ ポート（SMTP または Web サービスで使用されているポートなど）をシステムが検出したときに生成されます。このイベントは、アプリケーション プロトコル、またはアプリケーション プロトコルに関連付けられているサーバの識別には使用されません。情報は、TCP Server Information Update イベントで伝送されます。

このイベントは、デバイスがネットワーク マップにすでに存在しないモニタ対象ネットワーク上のサーバを含むNetFlowデータを処理するときも生成できます。この状況でイベントを生成するには、NetFlow データを管理するネットワーク検出ルールでアプリケーションを検出するように設定します。

新しいトランスポート プロトコル

このイベントは、ホストが新しいトランスポート プロトコル（TCP、UDP など）と通信していることをシステムが検出したときに生成されます。

新しい UDP ポート

このイベントは、システムが、ホスト上で稼動している新しい UDP サーバ ポートを検出したときに生成されます。

このイベントは、デバイスがネットワーク マップにすでに存在しないモニタ対象ネットワーク上のサーバを含むNetFlowデータを処理するときも生成できます。この状況でイベントを生成

するには、NetFlow データを管理するネットワーク検出ルールでアプリケーションを検出するように設定します。

TCP ポート クローズ

このイベントは、システムが、ホスト上で TCP ポートがクローズしたことを検出したときに生成されます。

TCP ポート タイムアウト

このイベントは、システムのネットワーク検出ポリシーに定義された間隔内で、システムが TCP ポートからアクティビティを検出しなかったときに生成されます。

TCP サーバ情報の更新

このイベントは、ホスト上で稼動しており、すでに検出されている TCP サーバでシステムが変更を検出したときに生成されます。

このイベントは、TCP サーバが更新されたときに生成される場合があります。

UDP ポート クローズ

このイベントは、システムが、ホスト上で UDP ポートがクローズしたことを検出したときに生成されます。

UDP ポート タイムアウト

このイベントは、ネットワーク検出ポリシーに定義された間隔内で、システムが UDP ポートからアクティビティを検出しなかったときに生成されます。

UDP サーバ情報の更新

このイベントは、ホスト上で稼動しており、すでに検出されている UDP サーバでシステムが変更を検出したときに生成されます。

このイベントは、UDP サーバが更新されたときに生成される場合があります。

VLAN タグ情報の更新

このイベントは、システムが、VLAN タグ内でホストに起因する変更を検出したときに生成されます。

関連トピック

ホスト入力イベント タイプ （3207 ページ）
ネットワーク検出のデータ ストレージ設定 （2669 ページ）
アプリケーションおよびオペレーティング システムの ID の競合 （2476 ページ）
ネットワーク検出アイデンティティ競合の設定 （2664 ページ）

ホスト入力イベント タイプ

ディスカバリ イベントのテーブルを表示すると、[イベント（Event）] カラムにイベント タイプが表示されます。

ユーザが（手動でホストを追加するなどの）特定のアクションを実行したときに生成されるホスト入力イベントとは異なり、ディスカバリ イベントは、システムが、監視対象ネットワークで変更を検出したとき（以前は検出されなかったホストでトラフィックを検出した場合など）に生成されます。

ネットワーク検出ポリシーを変更して、システムが記録するホスト入力イベントのタイプを設定できます。

さまざまなタイプのホスト入力イベントが提示する情報を理解すると、どのイベントを記録およびアラートの対象にするか、相関ポリシーでこれらのアラートをどのように使用するかを効率よく判断できるようになります。また、イベントタイプの名前がわかると、より効率のよいイベント検索を作成するうえで役に立ちます。次に、ホスト入力イベントのさまざまなタイプについて説明します。

クライアントの追加（Add Client）

このイベントは、ユーザがクライアントを追加したときに生成されます。

ホストの追加（Add Host）

このイベントは、ユーザがホストを追加したときに生成されます。

プロトコルの追加（Add Protocol）

このイベントは、ユーザがプロトコルを追加したときに生成されます。

スキャン結果の追加（Add Scan Result）

このイベントは、システムがNmapスキャンの結果をホストに追加したときに生成されます。

ポートの追加（Add Port）

このイベントは、ユーザがサーバ ポートを追加したときに生成されます。

クライアントの削除（Delete Client）

このイベントは、ユーザがシステムからクライアントを削除したときに生成されます。

ホスト/ネットワークの削除（Delete Host/Network）

このイベントは、ユーザがシステムからIPアドレスまたはサブネットを削除したときに生成されます。

プロトコルの削除（Delete Protocol）

このイベントは、ユーザがシステムからプロトコルを削除したときに生成されます。

ポートの削除（Delete Port）

このイベントは、ユーザがシステムからサーバ ポートまたはサーバ ポートのグループを削除したときに生成されます。

Host Attribute Add

このイベントは、ユーザが新しいホスト属性を作成したときに生成されます。

Host Attribute Delete

このイベントは、ユーザが、ユーザ定義のホスト属性を削除したときに生成されます。

ホスト属性値の削除（Host Attribute Delete Value）

このイベントは、ユーザが、ホスト属性に割り当てられている値を削除したときに生成されます。

ホスト属性値の設定（Host Attribute Set Value）

このイベントは、ユーザがホストに対してホスト属性値を設定したときに生成されます。

Host Attribute Update

このイベントは、ユーザが、ユーザ定義のホスト属性の定義を変更したときに生成されます。

ホスト重要度の設定（Set Host Criticality）

このイベントは、ユーザがホストに対してホストの重要度の値を設定した、または変更したときに生成されます。

オペレーティング システム定義の設定（Set Operating System Definition）

このイベントは、ユーザがホストに対してオペレーティング システムを設定したときに生成されます。

サーバ定義の設定（Set Server Definition）

このイベントは、ユーザがサーバに対してベンダーおよびバージョンの定義を設定したときに生成されます。

Set Vulnerability Impact Qualification

このイベントは、脆弱性の影響の認定が設定されたときに生成されます。

脆弱性が、影響の認定に対する使用でグローバル レベルで無効になったとき、または脆弱性がグローバル レベルで有効になったときに、このイベントが生成されます。

脆弱性を無効に設定（Vulnerability Set Invalid）

このイベントは、ユーザが 1 つ以上の脆弱性を無効にした（または確認した）ときに生成されます。

脆弱性を有効に設定（Vulnerability Set Valid）

このイベントは、ユーザが、以前に無効であるとマークされた脆弱性を有効にしたときに生成されます。

関連トピック

ディスカバリ イベント タイプ （3202 ページ）

ディスカバリ イベントとホスト入力イベントの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Any Security Analyst

ディスカバリ イベント ワークフローでは、ディスカバリ イベントとホスト入力イベント両方からのデータを表示できます。ユーザは検索する情報に応じてイベント ビューを操作することができます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

ユーザがイベントにアクセスするときに表示されるページは、使用するワークフローによって異なります。ユーザは事前定義のワークフローを使用できますが、これにはディスカバリ イベントのテーブル ビューと、ホスト ビューの最終ページが含まれています。また、特定のニーズを満たす情報だけを表示するカスタム ワークフローを作成することもできます。

ステップ 1 **[Analysis]** > **[Hosts]** > **[Discovery Events]**を選択します。

ステップ 2 次の選択肢があります。

- 時間枠の変更 （2956 ページ）の説明に従って、時間範囲を調整します。

  （注） イベント ビューを時間によって制約している場合は、（グローバルかイベント固有かに関係なく）アプライアンスに設定されている時間枠の外で生成されたイベントが、イベント ビューに表示されます。アプライアンスに対してスライドする時間枠を設定した場合でも、この状況が発生することがあります。

- [(ワークフローの切り替え)（(switch workflow)）] をクリックしてカスタム ワークフローを含む別のワークフローを使用します。
- 基本的なワークフロー操作を実行します（ディスカバリおよびアイデンティティ ワークフローの使用 （3199 ページ）を参照）。

- テーブルのカラムの内容について詳しく調べます（ディスカバリ イベントのフィールド（3210ページ）を参照）。

関連トピック

ディスカバリおよびアイデンティティ ワークフローの使用 （3199 ページ）

ディスカバリ イベントのフィールド

以下に、ディスカバリ イベント テーブルで表示および検索できるフィールドについて説明します。

時刻（Time）

システムがイベントを生成した時間。

イベント

ディスカバリ イベント タイプまたはホスト入力イベント タイプ。

[IPアドレス（IP Address）]

イベントに関連するホストに関連付けられている IP アドレス。

User

イベントが生成される前に、イベントに関係するホストに最後にログインしたユーザ。権限のあるユーザの後に、権限のないユーザのみがログインした場合、権限のあるユーザが次にログインするまで、権限のあるユーザが現行のユーザとして保持されます。

MAC Address

ディスカバリ イベントをトリガーとして使用したネットワーク トラフィックが使用する NIC の MAC アドレス。この MAC アドレスは、イベントに関連するホストの実際の MAC アドレスであるか、またはトラフィックが通過したネットワーク デバイスの MAC アドレスになります。

MAC Vendor

ディスカバリ イベントをトリガーとして使用したネットワーク トラフィックが使用する NIC の MAC ハードウェア ベンダー。

このフィールドを検索する場合は、**virtual_mac_vendor** を入力して、仮想ホストに関係するイベントを照合します。

[ポート（Port）]

イベントをトリガーとして使用したトラフィックが使用するポート（該当する場合）。

Description

テキストによるイベントの説明。

ドメイン

ホストを検出したデバイスのドメイン。 This field is only present if you have ever configured the Firepower Management Center for multitenancy.

Device

イベントを生成した管理対象デバイスの名前。NetFlow データに基づいた新しいホストおよび新しいサーバのイベントの場合、これはそのデータを処理した管理対象デバイスになります。

関連トピック

イベントの検索 （2967 ページ）

ホスト データ

システムがホストを検出し、ホストプロファイルを作成するためにホストに関する情報を収集したときに、イベントが生成されます。Firepower Management Center Web インターフェイスを使用して、ホストを表示、検索、および削除できます。

ホストの表示中に、選択したホストに基づいてトラフィックのプロファイル、およびコンプライアンスのホワイトリストを作成できます。また、（ビジネスの重要度を設定する）ホストの重要度の値などのホスト属性をホストグループに割り当てることもできます。そのあとで、相関ルールおよびポリシーの中でこれらの重要度の値、ホワイト リスト、およびトラフィック プロファイルを使用できます。

システムは、エクスポートされたNetFlow レコードからネットワーク マップにホストを追加できますが、これらのホストに使用できる情報は限られます（NetFlow データと管理対象デバイス データの違い （2478 ページ）を参照）。

関連トピック

NetFlow データと管理対象デバイス データの違い （2478 ページ）

ホスト データの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Any Security Analyst

Firepower Management Center を使用して、システムが検出したホストのテーブルを表示することができます。ここでユーザは、検索する情報に応じてビューを操作できます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

ユーザがホストにアクセスするときに表示されるページは、使用するワークフローによって異なります。事前定義のワークフローは両方とも、ホスト ビューで終了しますが、これにはユーザの制約を満たすすべてのホストのホスト プロファイルが含まれています。また、特定のニーズを満たす情報だけを表示するカスタム ワークフローを作成することもできます。

ステップ 1 次のように、ホスト データにアクセスします。

- 事前定義されたワークフローを使用する場合、**[Analysis]** > **[Hosts]** > **[Hosts]** を選択します。
- ホストのテーブル ビューが含まれないカスタム ワークフローを使用している場合は、[(ワークフローの切り替え)（(switch workflow)）] をクリックして [ホスト（Hosts）] を選択します。

ステップ 2 次の選択肢があります。

- [(ワークフローの切り替え)（(switch workflow)）] をクリックしてカスタム ワークフローを含む別のワークフローを使用します。
- 基本的なワークフロー操作を実行します（ディスカバリおよびアイデンティティ ワークフローの使用（3199 ページ）を参照）。
- テーブルのカラムの内容について詳しく調べます（ホストデータ フィールド（3212ページ）を参照）。
- オプションを表示するには、テーブル内の項目を右クリックします（オプションが表示されない列もあります）。
- ホスト属性を特定のホストに割り当てます（選択したホストのホスト属性の設定（3220ページ）を参照）。
- 特定のホストのトラフィック プロファイルを作成します（選択したホストのトラフィック プロファイルの作成（3217 ページ）を参照）。
- 特定のホストに基づいて、コンプライアンスのホワイト リストを作成します（選択したホストに基づいたコンプライアンスのホワイト リストの作成（3218 ページ）を参照）。

ホスト データ フィールド

システムはホストを検出したときに、そのホストに関するデータを収集します。そのデータには、ホストの IP アドレス、ホストが実行しているオペレーティング システムなどが含めることが可能です。ユーザは、ホストのテーブル ビューでこれらの情報の一部を表示することができます。

ホスト テーブルで表示および検索できるフィールドの説明が続きます。

前回の検出（Last Seen）

システムによっていずれかのホストの IP アドレスが最後に検出された日付と時間。[前回の検出（Last Seen）] の値は、ホストの IP アドレスに対してシステムが新しいホスト イベントを生成したときだけでなく、少なくともユーザがネットワーク検出ポリシーに設定した更新間隔の頻度で更新されます。

ホスト入力機能を使用して、オペレーティング システムのデータを更新しているホストでは、Last Seen の値は、そのデータが最初に追加された日付と時間を表します。

IP Address

ホストに関連付けられている IP アドレス。

MAC Address

ホストが検出した NIC の MAC アドレス。

[MAC Address] フィールドは、[Hosts] ワークフローの [Table View of Hosts] に表示されます。以下のものに対して [MAC Address] フィールドを追加できます。

- Hosts テーブルのフィールドが含まれているカスタム テーブル
- Hosts テーブルに基づいたカスタム ワークフローのドリルダウン ページ

MAC Vendor

ホストが検出した NIC の MAC ハードウェア ベンダー。

[MAC Vendor] フィールドは、[Hosts] ワークフローの [Table View of Hosts] に表示されます。以下のものに対して [MAC Vendor] フィールドを追加できます。

- Hosts テーブルのフィールドが含まれているカスタム テーブル
- [ホスト（Hosts）] テーブルに基づいたカスタム ワークフローのドリルダウン ページ

このフィールドを検索する場合は、`virtual_mac_vendor` を入力して、仮想ホストに関係するイベントを照合します。

現在のユーザ（Current User）

ホストに現在ログインしているユーザの ID（ユーザ名）。

権限のないユーザがホストにログインすると、そのログインはユーザおよびホストの履歴に記録されることに注意してください。権限のあるユーザがホストに関連付けられていない場合、権限のないユーザがそのホストの現行ユーザとなることが可能です。ただし、権限のあるユーザがホストにログインした後は、権限のある別のユーザがログインした場合のみ、現行ユーザが変わります。また、権限のないユーザがホストの現行ユーザである場合、そのユーザを使用してユーザ制御を行うことはできません。

Host Criticality

ホストに割り当てられている、ユーザ指定の重要度の値。

NetBIOS 名（NetBIOS Name）

ホストの NetBIOS 名。NetBIOS プロトコルを実行しているホストにのみ、NetBIOS 名があります。

VLAN ID

ホストが使用する VLAN ID。

ホップ（Hops）

ホストを検出したデバイスからホストへのネットワークのホップ数。

ホスト タイプ（Host Type）

ホストのタイプ。ホスト、モバイル デバイス、jailbroken モバイル デバイス、ルータ、ブリッジ、NAT デバイス、ロード バランサのいずれかにできます。

ネットワーク デバイスを区別するためにシステムでは次の方法を使用します。

- Cisco Discovery Protocol（CDP）メッセージの分析。ネットワークのデバイスおよびそれらのタイプ（Cisco デバイスのみ）を特定できます。
- スパニング ツリープロトコル（STP）の検出。デバイスをスイッチまたはブリッジとして識別します。
- 同じ MAC アドレスを使用している複数のホストの検出。MAC アドレスを、ルータに属しているものとして識別します。
- クライアント側からの TTL 値の変更、または通常のブート時間よりも頻繁に変更されている TTL 値の検出。この検出では、NAT デバイスとロード バランサを識別します。

デバイスがネットワーク デバイスとして識別されない場合は、ホストとして分類されます。

このフィールドを検索するときは、`!host` と入力してすべてのネットワーク デバイスを検索します。

ハードウェア（Hardware）

モバイル デバイスのハードウェア プラットフォーム。

OS

次のいずれかです。

- ホスト上で検出されたオペレーティング システム（名前、ベンダー、およびバージョン）、または Nmap かホスト入力機能を使用して更新されたオペレーティング システム。
- オペレーティング システムが既知のフィンガープリントに一致しない場合は `unknown`
- オペレーティング システムを識別するための十分な情報がシステムで収集されていない場合は `pending`

システムが複数のアイデンティティを検出した場合は、これらのアイデンティティはカンマ区切りリストで表示されます。

このフィールドは、ダッシュボード上で [カスタム分析（Custom Analysis）] ウィジェットからホスト イベント ビューを起動したときに表示されます。また、これは [ホスト（Hosts）] テーブルに基づいたカスタム テーブルのフィールド オプションです。

このフィールドを検索するときは、`n/a` と入力して、オペレーティング システムがまだ識別されていないホストを含めます。

OS 競合（OS Conflict）

このフィールドは検索専用です。

OS ベンダー（OS Vendor）

次のいずれかです。

- ホストで検出されたオペレーティング システムのベンダー、またはNmapかホスト入力機能を使用して更新されたオペレーティング システムのベンダー。
- オペレーティング システムが既知のフィンガープリントに一致しない場合は `unknown`
- オペレーティング システムを識別するための十分な情報がシステムで収集されていない場合は `pending`

システムが複数のベンダーを検出した場合は、これらのベンダーはカンマ区切りリストで表示されます。

このフィールドを検索するときは、`n/a` と入力して、オペレーティング システムがまだ識別されていないホストを含めます。

OS 名（OS Name）

次のいずれかです。

- ホスト上で検出されたオペレーティング システム、またはNmapかホスト入力機能を使用して更新されたオペレーティング システム。
- オペレーティング システムが既知のフィンガープリントに一致しない場合は `unknown`
- オペレーティング システムを識別するための十分な情報がシステムで収集されていない場合は `pending`

システムが複数の名前を検出した場合は、これらの名前はカンマ区切りリストで表示されます。

このフィールドを検索するときは、`n/a` と入力して、オペレーティング システムがまだ識別されていないホストを含めます。

OS バージョン（OS Version）

次のいずれかです。

- ホストで検出されたオペレーティング システムのバージョン、またはNmapかホスト入力機能を使用して更新されたオペレーティング システムのバージョン。
- オペレーティング システムが既知のフィンガープリントに一致しない場合は `unknown`
- オペレーティング システムを識別するための十分な情報がシステムで収集されていない場合は `pending`

システムが複数のバージョンを検出した場合は、これらのバージョンはカンマ区切りリストで表示されます。

このフィールドを検索するときは、`n/a` と入力して、オペレーティング システムがまだ識別されていないホストを含めます。

ソース タイプ（Source Type）

ホストのオペレーティング システムのアイデンティティを確立するために使用されるソースのタイプは次のとおりです。

- [ユーザ（User）]：user_name
- [アプリケーション（Application）]：app_name
- スキャナ：scanner_type（ネットワーク検出の設定を介して追加されたNmapまたはスキャナ）
- システムによって検出されたオペレーティング システムの場合は `Firepower`

システムでは、オペレーティング システムのアイデンティティを判断するために、複数のソースのデータを統合することができます。

信頼性（Confidence）

次のいずれかです。

- システムで検出されたホストについて、ホスト上で稼動しているオペレーティング システムのアイデンティティ内にシステムが保持している信頼度（パーセンテージ）。
- 100%（ホスト入力機能やNmapスキャナなどのアクティブなソースによって識別されたオペレーティング システムの場合）。
- `unknown`（システムがオペレーティング システムのアイデンティティを特定できないホスト、およびNetFlowデータに基づいてネットワーク マップに追加されたホストの場合）。

このフィールドを検索するときは、`n/a` と入力して、NetFlow データに基づいてネットワーク マップに追加されたホストを含めます。

注記（Notes）

[注記（Notes）] ホスト属性の、ユーザ定義のコンテンツ。

ドメイン（Domain）

ホストに関連付けられているドメイン。 This field is only present if you have ever configured the Firepower Management Center for multitenancy.

Device

トラフィックを検出した管理対象デバイスか、NetFlow またはホスト入力データを処理したデバイスのいずれか。

このフィールドが空白の場合は、次のいずれかの条件を満たします。

- ホストがデバイスによってネットワーク マップに追加されたが、このデバイスは、ホストが存在しているネットワークに対してネットワーク検出ポリシーに定義されているとおりに明示的に監視していない。
- ホストの入力機能を使用してホストが追加されたが、システムによって検出されていない。

メンバー数（Count）

各行に表示される情報と一致するイベントの数。このフィールドが表示されるのは、2 つ以上の同一の行を作成する制限を適用した後のみです。

関連トピック

イベントの検索 （2967 ページ）
オペレーティング システムのアイデンティティの競合 （3168 ページ）

選択したホストのトラフィック プロファイルの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin

トラフィック プロファイルは、指定した期間に収集された接続データに基づいた、ネットワーク上のトラフィックのプロファイルです。トラフィック プロファイルを作成した後で、正常なネットワーク トラフィックを表すと思われる新しいトラフィックをプロファイルに対して評価することにより、異常なネットワーク トラフィックを検出することができます。

[Hosts] ページを使用して、指定するホスト グループのトラフィック プロファイルを作成できます。トラフィック プロファイルは、指定したホストのいずれかが発信元ホストである、検出された接続に基づいています。ソートおよび検索機能を使用して、プロファイルを作成するホストを分離することができます。

ステップ 1 ホスト ワークフローのテーブル ビューで、トラフィック プロファイルを作成するホストの隣にあるチェック ボックスをオンにします。

ステップ 2 ページの下部で [トラフィック プロファイルの作成（Create Traffic Profile）] をクリックします。

ステップ 3 特別なニーズに応じて、トラフィック プロファイルを変更し、保存します。

関連トピック

トラフィック プロファイルの概要 （2741 ページ）

選択したホストに基づいたコンプライアンスのホワイト リストの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin

コンプライアンスのホワイト リストでは、ネットワーク上で許可されるオペレーティング システム、クライアント、ネットワーク、トランスポート、またはアプリケーション プロトコルを指定することができます。

[Hosts] ページを使用して、ユーザが指定するホスト グループのホスト プロファイルに基づいて、コンプライアンスのホワイトリストを作成することができます。ソートおよび検索機能を使用して、ホワイト リストの作成に使用するホストを分離することができます。

ステップ 1 ホスト ワークフローのテーブル ビューで、ホワイト リストを作成するホストの隣にあるチェック ボックスをオンにします。

ステップ 2 ページの下部で [ホワイト リストの作成（Create White List）] をクリックします。

ステップ 3 特別なニーズに応じて、ホワイト リストを変更し、保存します。

関連トピック

コンプライアンス ホワイトリストの概要 （2679 ページ）

ホスト属性データ

Firepower システムは、検出したホストに関する情報を収集し、その情報を使用してホスト プロファイルを作成します。ただし、ネットワーク上のホストについて、アナリストに提供する追加情報が存在する場合があります。ユーザは、ホストプロファイルにメモを追加する、ホストのビジネス重要度を設定する、選択する他の情報を提供する、といったことが可能です。それぞれの情報は、ホスト属性と呼ばれます。

ホストプロファイルの認定でホスト属性を使用することができます。これにより、トラフィック プロファイルの作成中に収集するデータを制約し、相関ルールをトリガーする条件を制限することができます。相関ルールに応じて属性値を設定することもできます。

関連トピック

ホスト属性の表示 （3218 ページ）
セット属性修復の設定 （2766 ページ）

ホスト属性の表示

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Any Security Analyst

Firepower Management Center を使用して、システムで検出されたホストのテーブル、およびそのホスト属性を表示することができます。ここでユーザは、検索する情報に応じてビューを操作できます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

ユーザがホスト属性にアクセスするときに表示されるページは、使用するワークフローによって異なります。事前定義のワークフロー（検出されたすべてのホスト、およびそのホストの属性が記載されているホスト属性のテーブル ビューが含まれており、ホスト ビュー ページで終了するワークフロー）を使用することができます。このワークフローには、制約を満たすすべてのホストについて 1 つのホスト プロファイルが含まれています。

また、特定のニーズを満たす情報だけを表示するカスタム ワークフローを作成することもできます。

ステップ 1 次のように、ホスト属性データにアクセスします。

- 事前定義されたワークフローを使用する場合、**[Analysis]** > **[Hosts]** > **[Host Attributes]** を選択します。
- ホスト属性のテーブル ビューが含まれないカスタム ワークフローを使用している場合は、[(ワークフローの切り替え)（(switch workflow)）] をクリックして [属性（Attributes）] を選択します。

ステップ 2 次の選択肢があります。

- [(ワークフローの切り替え)（(switch workflow)）] をクリックしてカスタム ワークフローを含む別のワークフローを使用します。
- 基本的なワークフロー操作を実行します（ディスカバリおよびアイデンティティ ワークフローの使用（3199 ページ）を参照）。
- テーブルのカラムの内容について詳しく調べます（ホスト属性データ フィールド（3219ページ）を参照）。
- ホスト属性を特定のホストに割り当てます（選択したホストのホスト属性の設定（3220ページ）を参照）。

ホスト属性データ フィールド

ホスト属性テーブルには、MAC アドレスでのみ識別されるホストは表示されないことに注意してください。

ホスト属性テーブルで表示および検索できるフィールドの説明が続きます。

[IPアドレス（IP Address）]

ホストに関連付けられている IP アドレス。

Current User

ホストに現在ログインしているユーザの ID（ユーザ名）。

権限のないユーザがホストにログインすると、そのログインはユーザおよびホストの履歴に記録されることに注意してください。権限のあるユーザがホストに関連付けられていない場合、権限のないユーザがそのホストの現行ユーザとなることが可能です。ただし、権限のあるユーザがホストにログインした後は、権限のある別のユーザがログインした場合のみ、現行ユーザが変わります。また、権限のないユーザがホストの現行ユーザである場合、そのユーザを使用してユーザ制御を行うことはできません。

Host Criticality

ユーザが割り当てた、企業にとってのホストの重要度。ホストの重要度を相関ルールおよびポリシーで使用して、イベントに関するホストの重要度に対して、ポリシー違反および違反の応答を作成することができます。ホストの重要度に[低（Low）]、[中（Medium）]、[高（High）]、または [なし（None）] を割り当てることができます。

注記（Notes）

他のアナリストに提示する、ホストに関する情報。

コンプライアンス ホワイトリストの属性を含む、ユーザ定義のホスト属性（Any user-defined host attribute, including those for compliance white lists）

ユーザ定義のホスト属性の値。ホスト属性テーブルには、ユーザ定義のそれぞれのホスト属性のフィールドが含まれています。

ドメイン（Domain）

ホストに関連付けられているドメイン。 This field is only present if you have ever configured the Firepower Management Center for multitenancy.

メンバー数（Count）

各行に表示された情報と一致するイベントの数。[カウント（Count）] フィールドは、複数の同一行が生成される制限を適用した後でのみ表示されることに注意してください。

関連トピック

イベントの検索 （2967 ページ）

選択したホストのホスト属性の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Any Security Analyst

ホスト ワークフローから、事前定義済のホスト属性とユーザ定義のホスト属性を設定できます。

ステップ 1 ホスト ワークフローで、ホスト属性を追加するホストの横にあるチェックボックスをオンにします。

ヒント ソート機能と検索機能を使用して、特別な属性を割り当てるホストを分離することができます。

ステップ 2 ページの下部にある [属性の設定（Set Attributes）] をクリックします。

ステップ 3 必要に応じて、選択したホストに対してホストの重要度を設定します。[なし（None）]、[低（Low）]、[中（Medium）]、または [高（High）] を選択できます。

ステップ 4 必要に応じて、テキスト ボックスで、選択したホストのホスト プロファイルにメモを追加します。

ステップ 5 必要に応じて、自分で設定したユーザ定義のホストの属性を設定します。

ステップ 6 **[保存（Save）]** をクリックします。

侵害の兆候データ

Firepower System は、モニタリング対象のネットワーク上でホストが悪意のある手段によって侵害されている可能性があるかどうかを判断するために、ホストに関連付けられているさまざまなタイプのデータ（侵入イベント、Security Intelligence、接続イベント、ファイルまたはマルウェア イベント）との関連性を示します。イベント データの特定の組み合わせと頻度は、影響を受けたホストの侵害の痕跡（IOC）タグをトリガーとして使用します。このようなホストの IP アドレスは侵害を受けているホストの赤いアイコン（  ）でイベント ビューに表示されます。

ホストが侵害されている可能性があると識別された場合、その侵害に関連付けられているユーザにもタグが付けられます。そのようなユーザは、  のアイコンでイベント ビューに表示されます。

マルウェアが含まれているファイルが 300 秒以内に IOC というタグが付けられて再度表示される場合は、別の IOC は生成されません。同じファイルが 300 秒以上経ってから表示された場合は、新しい IOC が生成されます。

侵害の兆候としてイベントにタグを付けるように設定するには、侵害の兆候ルールの有効化（2667 ページ）を参照してください。

関連トピック

侵害の兆候ルールの有効化 （2667 ページ）

侵害兆候データの表示と処理

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Any Security Analyst

Firepower Management Center を使用して、侵害の兆候（IOC）を示すテーブルを表示できます。検索する情報に応じてイベント ビューを操作します。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

表示されるページは、使用するワークフローによって異なります。事前定義の IOC ワークフローはプロファイル ビューで終了しますが、これには、制約を満たすすべてのホストまたはユーザのホストプロファイルまたはユーザプロファイルが含まれています。また、特定のニーズを満たす情報だけを表示するカスタム ワークフローを作成することもできます。

始める前に

- システムで侵害の兆候（IOC）を検出してタグを付けるには、ネットワーク検出ポリシーの IOC 機能をアクティブにして、少なくとも 1 つの IOC ルールを有効にする必要があります。侵害の兆候ルールの有効化 （2667 ページ）を参照してください。
- アクティブなアイデンティティ ポリシーでユーザが認識される必要があります。

ステップ 1 Web インターフェイスのどの場所のニーズを満たす情報があるかを特定します。

侵害兆候データを表示または処理するには、次の場所を使用できます。

- イベント ビューア（[分析（Analysis）] メニューの各種タブ）：接続、セキュリティ インテリジェンス、侵入、マルウェアや IOC 検出のイベントビューでそのイベントが IOC をトリガーしたかどうかを表示します。IOC ルールをトリガーする、エンドポイント向け AMP によって生成されたマルウェア イベントは、イベント タイプが `AMP IOC` であり、侵害を指定するイベント サブタイプと一緒に表示されることに注意してください。
- ダッシュボード：ダッシュボードでは、サマリー ダッシュボードの [脅威（Threats）] タブに、ホスト別とユーザ別の IOC タグがデフォルトで表示されます。カスタム分析ウィジェットは IOC データに基づくプリセットを提供します。
- コンテキストエクスプローラ：コンテキストエクスプローラの [侵害の兆候（Indications of Compromise）] セクションに、IOC カテゴリ別のホストとホスト別の IOC カテゴリのグラフが表示されます。
- [ネットワーク マップ（Network Map）] ページ：[分析（Analysis）] > [ホスト（Hosts）] > [ネットワーク マップ（Network Map）] にある [侵害の兆候（Indications of Compromise）] タブには、侵害されている可能性があるネットワーク上のホストが侵害のタイプと IP アドレス別にグループ分けして示されます。
- [ネットワーク ファイル トラジェクトリ（Network File Trajectory）] 詳細ページ：[分析（Analysis）] > [ファイル（Files）] > [ネットワーク ファイル トラジェクトリ（Network File Trajectory）] の下に一覧表示されているファイルの詳細ページでは、ネットワークの侵害の兆候を追跡できます。
- [ホストの侵害の兆候（Host Indications of Compromise）] ページ：[分析（Analysis）] > [ホスト（Hosts）] メニューの下の [ホストの侵害の兆候（Host Indications of Compromise）] ページには、モニタ対象ホストの一覧が IOC タグ別にグループ分けされて表示されます。このページのワークフローを使ってデータをドリルダウンできます。

- [ユーザの侵害の兆候（User Indications of Compromise）] ページ：[分析（Analysis）]>[ユーザ（Users）] メニューの下の [ユーザの侵害の兆候（User Indications of Compromise）] ページには、IOC の可能性があるイベントに関連付けられているユーザの一覧が IOC タグ別にグループ分けされて表示されます。このページのワークフローを使ってデータをドリルダウンできます。
- ホスト プロファイル ページ：侵害されている可能性があるホストのホスト プロファイルには、そのホストに関連付けられているすべての IOC タグが表示され、IOC タグの解決と IOC ルール状態の設定ができます。
- ユーザ プロファイル ページ：IOC の可能性があるイベントに関連付けられているユーザのユーザ プロファイルには、そのユーザに関連付けられているすべての IOC タグが表示され、IOC タグの解決と IOC ルール状態の設定ができます（Firepower Management Center の Web インターフェイスでは、ユーザ プロファイルは「ユーザ アイデンティティ（User Identity）」とラベルが付けられています）。

ステップ 2 必要に応じて、次のうちのいずれかを実行し、この手順の残りのステップを使用します。

オプション	説明
ホストの IOC を調べるには、以下を実行します。	• 事前定義されたワークフローを使用する場合、**[Analysis]** > **[Hosts]** > **[Indications of Compromise]** を選択します。 • ホスト IOC のテーブル ビューが含まれないカスタム ワークフローを使用している場合は、[(ワークフローの切り替え)（(switch workflow)）] をクリックして [ホストの侵害の兆候（Host Indications of Compromise）] を選択します。
ユーザに関連付けられている IOC を調べるには、以下を実行します。	• 事前定義されたワークフローを使用する場合、[分析（Analysis）] > [ユーザ（Users）] > [侵害の兆候（Indications of Compromis）] を選択します。 • ユーザ IOC のテーブル ビューが含まれないカスタム ワークフローを使用している場合は、[(ワークフローの切り替え)（(switch workflow)）] をクリックして [ユーザの侵害の兆候（User Indications of Compromise）] を選択します。

ステップ 3 次の選択肢があります。

- [(ワークフローの切り替え)（(switch workflow)）] をクリックしてカスタム ワークフローを含む別のワークフローを使用します。
- 基本的なワークフロー操作を実行します（ディスカバリおよびアイデンティティ ワークフローの使用（3199 ページ）を参照）。
- テーブルのカラムの内容について詳しく調べます（侵害の兆候データ フィールド（3224 ページ）を参照）。
- [ホストの侵害の兆候（Host Indications of Compromise）] ページ：[IP アドレス（IP Address）] カラムにある侵害されたホストのアイコン（  ）をクリックして、侵害されたホストのホスト プロファイルを表示します。

- [ユーザの侵害の兆候（User Indications of Compromise）] : [ユーザ（User）] カラムの赤色のユーザ アイコン（  ）をクリックして、侵害に関連付けられているユーザ プロファイルを表示します。
- IOC イベントに解決済みとマークして、リストに表示されないようにします。これを実行するには、編集する IOC イベントの横にあるチェック ボックスをオンにして、[解決済みとマークを付ける（Mark Resolved）] をクリックします。
- [最初の確認日時（First Seen）] または [前回の検出（Last Seen）] カラムにある表示アイコン（  ）をクリックして、IOC をトリガーしたイベントの詳細を表示します。
- その他のオプションを表示するには、テーブル内の値を右クリックします。

侵害の兆候データ フィールド

以下は、ホストまたはユーザの IOC（侵害の兆候）テーブル内のフィールドです。すべての IOC 関連のテーブルにすべてのフィールドが含まれているわけではありません。

IP アドレス（IP Address）（ホストの IOC データを表示する場合）

IOC をトリガーとして使用したホストに関連付けられている IP アドレス。

ユーザ（User）（ユーザの IOC データを表示する場合）

IOC をトリガーしたイベントに関連付けられているユーザのユーザ名、レルム、および認証ソース。

カテゴリ（Category）

`Malware Executed` や `Impact 1 Attack` など、示された侵害のタイプの簡単な説明。

イベント タイプ（Event Type）

特定の IOC に関連付けられている識別子で、トリガーとして使用したイベントを参照します。

説明

侵害される可能性のあるホストへの影響の説明（[このホストはリモート制御下にある可能性があります（This host may be under remote control）] や [このホスト上でマルウェアが実行されました（Malware has been executed on this host）] など）。

最初の確認日時/最新の確認日時（First Seen/Last Seen）

IOC をトリガーとして使用したイベントが発生した最初（または最新）の日付と時刻。

ドメイン（Domain）

IOC をトリガーとして使用したホストのドメイン。 This field is only present if you have ever configured the Firepower Management Center for multitenancy.

関連トピック

イベントの検索 （2967 ページ）

単一ホストまたはユーザにおける侵害の兆候のルール状態の編集

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Any Security Analyst（読み取り専用を除く）

ネットワーク検出ポリシーで有効になっている場合、侵害の兆候ルールは監視対象ネットワーク内のすべてのホストと、そのネットワーク上のIOCイベントに関連付けられている権限のあるユーザに適用されます。個々のホストまたはユーザのルールを無効にして、無用なIOCタグを回避できます（たとえば、DNSサーバに対するIOCタグが表示されないようにできます）。適用可能なネットワーク検出ポリシーでルールを無効にすると、特定のホストまたはユーザに対して有効にすることができません。特定のホストに対してルールを無効にしても、同じイベントに関与するユーザのタグ付けには影響がなく、その逆もまた同じです。

ステップ 1 ホストまたはユーザ プロファイルの [侵害の兆候（Indications of Compromise）] セクションに移動します。

ステップ 2 [ルール状態の編集（Edit Rule States）] をクリックします。

ステップ 3 ルールの [有効（Enabled）] 列で、スライダをクリックしてこれを有効または無効にします。

ステップ 4 **[保存（Save）]** をクリックします。

侵害の兆候のタグのソース イベントの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Any Security Analyst

ホスト プロファイルやユーザ プロファイルの [侵害の兆候（Indications of Compromise）] セクションを使用して、IOCタグをトリガーしたイベントにすばやく移動することができます。これらのイベントを分析すると、侵害される脅威に対処するのに必要なアクション、およびアクションが必要かどうかを判断するための情報が提供されます。

IOC タグのタイムスタンプの隣の表示アイコン（  ）をクリックすると、関連するイベントタイプのイベントのテーブル ビューにナビゲートします。ここでは、IOCタグをトリガーとして使用したイベントのみが表示されます。

ユーザ IOC の最初のインスタンスのみが Firepower Management Center に表示されます。後続のインスタンスは DNS サーバによって捕捉されます。

ステップ 1 ホストまたはユーザ プロファイルで、[侵害の兆候（Indications of Compromise）] セクションに移動します。

ステップ 2 調べたい IOC タグの [最初の痕跡（First Seen）] または [最後の痕跡（Last Seen）] カラムにある表示アイコン（  ）をクリックします。

侵害の兆候タグの解決

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Any Security Analyst

侵害の兆候（IOC）タグで示された脅威が分析および対処された後、または IOC タグが誤検出を示していると判断した場合、イベントに解決済みのマークを付けることができます。イベントに解決済みのマークを付けると、そのイベントはホストプロファイルおよびユーザプロファイルから削除されます。プロファイル上のアクティブな IOC タグがすべて解決されると、侵害されたホストアイコン（  ）またはユーザが侵害の兆候に関連付けられていることを示すアイコン（  ）は表示されなくなります。解決した IOC についても、IOC のトリガー元であるイベントは引き続き表示できます。

IOC タグをトリガーしたイベントが繰り返された場合、ホストまたはユーザに対する IOC ルールが無効にされていない限り、このタグが再び設定されます。

ステップ 1 ホストまたはユーザ プロファイルで、[侵害の兆候（Indications of Compromise）] セクションに移動します。

ステップ 2 次の 2 つの選択肢があります。

- 個別の IOC タグに解決済みのマークを付けるには、解決するタグの右にある削除アイコン（  ）をクリックします。
- プロファイル上のすべての IOC タグに解決済みのマークを付けるには、[すべてに解決済みのマークを付ける（Mark All Resolved）] をクリックします。

サーバ データ

Firepower システムは、モニタ対象ネットワーク セグメント上のホストで稼動しているすべてのサーバに関する情報を収集します。この情報には次のものが含まれます。

- サーバの名前
- サーバが使用するアプリケーションとネットワーク プロトコル
- サーバのベンダーとバージョン

- サーバを実行しているホストに関連付けられている IP アドレス
- サーバが通信するポート

システムはサーバを検出すると、関連するホストがまだサーバの最大数に達していない場合は、ディスカバリ イベントを生成します。Firepower Management Center の Web インターフェイスを使用して、サーバ イベントを表示、検索、削除できます。

また、サーバイベントを相関ルールのベースにすることもできます。たとえばシステムが、いずれかのホスト上で稼働している ircd などのチャット サーバを検出したときに相関ルールをトリガーできます。

システムは、エクスポートされたNetFlow レコードからネットワーク マップにホストを追加できますが、これらのホストに使用できる情報は限られます（NetFlow データと管理対象デバイス データの違い （2478 ページ）を参照）。

関連トピック

ホスト制限と検出イベント ロギング （2552 ページ）
NetFlow データと管理対象デバイス データの違い （2478 ページ）

サーバ データの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Any Security Analyst

Firepower Management Center を使用して、検出されたサーバのテーブルを表示できます。ここでユーザは、検索する情報に応じてイベント ビューを操作することができます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

ユーザがサーバにアクセスしたときに表示されるページは、使用するワークフローによって異なります。事前定義のすべてのワークフローはホスト ビューで終了しますが、このホスト ビューには、制約を満たすすべてのホストに対して1つずつホスト プロファイルが含まれています。また、特定のニーズを満たす情報だけを表示するカスタム ワークフローを作成することもできます。

ステップ 1 次のように、サーバ データにアクセスします。

- 事前定義されたワークフローを使用する場合、**[Analysis]** > **[Hosts]** > **[Servers]** を選択します。
- サーバのテーブル ビューが含まれていないカスタム ワークフローを使用している場合は、[(ワークフローの切り替え)（(switch workflow)）] をクリックして [サーバ（Servers）] を選択します。

ステップ 2 次の選択肢があります。

- [(ワークフローの切り替え)（(switch workflow)）] をクリックしてカスタム ワークフローを含む別のワークフローを使用します。

- 基本的なワークフロー操作を実行します（ディスカバリおよびアイデンティティ ワークフローの使用（3199 ページ）を参照）。
- テーブルのカラムの内容について詳しく調べます（サーバデータ フィールド（3228ページ）を参照）。
- 編集するサーバのイベントの横にあるチェック ボックスをオンにし、[サーバ アイデンティティの設定（Set Server Identity）] をクリックすることによって、サーバのアイデンティティを編集します。
- オプションを表示するには、テーブル内の項目を右クリックします（オプションが表示されない列もあります）。

関連トピック

サーバのアイデンティティの編集 （3173 ページ）

サーバ データ フィールド

サーバ テーブルで表示および検索できるフィールドの説明は次のとおりです。

前回の使用（Last Used）

ネットワーク上でサーバが最後に使用された日付と時間、またはホスト入力機能を使用してサーバが最初に更新された日付と時間。[前回の使用（Last Used）] の値は、システムがサーバ情報の更新を検出したときだけでなく、少なくともユーザがネットワーク検出ポリシーに設定した更新間隔の頻度で更新されます。

[IPアドレス（IP Address）]

サーバを実行しているホストに関連付けられている IP アドレス。

Port

サーバが稼動しているポート。

Protocol

サーバが使用するネットワークまたはトランスポート プロトコル。

アプリケーション プロトコル（Application Protocol）

次のいずれかです。

- サーバのアプリケーション プロトコルの名前
- `pending`：システムで、いずれかの理由でサーバをポジティブまたはネガティブに識別できない場合
- `unknown`：既知のサーバ フィンガープリントに基づいてシステムでサーバを識別できない場合、またはホストの入力を介してサーバが追加され、アプリケーションプロトコルが含まれていなかった場合

アプリケーションプロトコルのカテゴリ、タグ、リスク、またはビジネスとの関連性（Category, Tags, Risk, or Business Relevance for Application Protocols）

アプリケーション プロトコルに割り当てられているカテゴリ、タグ、リスク レベル、およびビジネス関連性。これらのフィルタを使用して、特定のデータ セットを対象にすることができます。

ベンダー（Vendor）

次のいずれかです。

- サーバのベンダー：システム、Nmap、その他のアクティブなソースで識別された、またはホスト入力機能を使用して指定されたサーバのベンダー
- 空白：システムが既知のサーバフィンガープリントに基づいてベンダーを識別できなかった場合、またはNetFlowデータを使用してサーバがネットワーク マップに追加された場合

バージョン

次のいずれかです。

- サーバのバージョン：システム、Nmap、その他のアクティブなソースで識別された、またはホスト入力機能を使用して指定されたサーバのバージョン
- 空白：システムが既知のサーバ フィンガープリントに基づいてバージョンを識別できなかった場合、またはNetFlowデータを使用してサーバがネットワーク マップに追加された場合

Web アプリケーション（Web Application）

HTTP トラフィックでシステムが検出したペイロード コンテンツに基づいた Web アプリケーション。システムが HTTP のアプリケーション プロトコルを検出したものの、特定の Web アプリケーションを検出できない場合は、一般的な Web ブラウジングの指定が提示されるので注意してください。

Webアプリケーションのカテゴリ、タグ、リスク、またはビジネスとの関連性（Category, Tags, Risk, or Business Relevance for Web Applications）

Web アプリケーションに割り当てられているカテゴリ、タグ、リスク レベル、およびビジネス関連性。これらのフィルタを使用して、特定のデータ セットを対象にすることができます。

ヒット数（Hits）

サーバがアクセスされた回数。ホスト入力機能を使用して追加されたサーバの場合、この値は必ず 0 になります。

ソース タイプ（Source Type）

次の値のいずれかを指定します。

- [ユーザ（User）]：user_name
- [アプリケーション（Application）]：app_name
- スキャナ：scanner_type（ネットワーク検出の設定を介して追加されたNmapまたはスキャナ）
- Firepowerシステムによって検出されたサーバの `Firepower`、`Firepower Port Match`、または `Firepower Pattern Match`
- NetFlowデータを使用して追加されたサーバの `NetFlow`

ドメイン（Domain）

サーバを実行しているホストのドメイン。 This field is only present if you have ever configured the Firepower Management Center for multitenancy.

Device

トラフィックを検出した管理対象デバイスか、NetFlowまたはホスト入力データを処理したデバイスのいずれか。

現在のユーザ（Current User）

ホストに現在ログインしているユーザのID（ユーザ名）。

権限のないユーザがあるホストにログインすると、そのログインはユーザとホストの履歴に記録されます。権限のあるユーザがホストに関連付けられていない場合、権限のないユーザがそのホストの現行ユーザとなることができます。ただし、権限のあるユーザがホストにログインした後は、権限のある別のユーザがログインした場合のみ、現行ユーザが変わります。また、権限のないユーザがホストの現行ユーザである場合、そのユーザを使用してユーザ制御を行うことはできません。

Count

各行に表示される情報と一致するイベントの数。このフィールドが表示されるのは、2つ以上の同一の行を作成する制限を適用した後のみです。

関連トピック

イベントの検索 （2967 ページ）
ネットワーク検出のデータ ストレージ設定 （2669 ページ）

アプリケーション データとアプリケーション詳細データ

監視対象ホストが別のホストに接続すると、システムは多くの場合、どのアプリケーションが使用されたかを判断することができます。Firepowerシステムは、電子メール、インスタントメッセージ、ピアツーピア、Webアプリケーション、およびその他のタイプのアプリケーションが多用されると検出します。

検出されたそれぞれのアプリケーションに対してシステムは、アプリケーションを使用したIPアドレス、製品、バージョン、および使用が検出された回数を記録します。Webインターフェイスを使用して、アプリケーションイベントを表示、検索、および削除できます。ホスト入力機能を使用して、1つ以上のホスト上のアプリケーションデータを更新することもできます。

どのアプリケーションがどのホストで稼動しているかがわかっている場合は、そのことを使用してホスト プロファイルの認定を作成し、この認定によって、トラフィック プロファイルの作成中に収集するデータを制約することができます。また、相関ルールをトリガーする条件を制約することもできます。また、アプリケーションの検出を相関ルールのベースにすることもできます。たとえば、従業員に特定のメール クライアントを使用させたい場合は、システムが、いずれかの対象ホストで別のメールクライアントが稼動していることを検出したときに相関ルールをトリガーすることができます。

Firepowerのアプリケーションディテクタに関する最新情報は、各Firepowerシステム更新のリリース ノート、各 VDB 更新のアドバイザリをよくご確認ください。

分析用にアプリケーションデータを収集および保存するには、ネットワーク検出ポリシーでアプリケーションの検出が有効になっていることを確認します。

アプリケーション データの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Any Security Analyst

Firepower Management Center を使用して、検出されたアプリケーションのテーブルを表示できます。ここでユーザは、検索する情報に応じてイベント ビューを操作することができます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

ユーザがアプリケーションにアクセスするときに表示されるページは、使用するワークフローによって異なります。また、特定のニーズを満たす情報だけを表示するカスタム ワークフローを作成することもできます。

ステップ 1 次のようにして、アプリケーション データにアクセスします。

- 事前定義されたワークフローを使用する場合、**[Analysis]** > **[Hosts]** > **[Application Details]** を選択します。
- アプリケーションの詳細のテーブル ビューが含まれないカスタム ワークフローを使用している場合は、[(ワークフローの切り替え)（(switch workflow)）] をクリックして [クライアント（Clients）] を選択します。

ステップ 2 次の選択肢があります。

- [(ワークフローの切り替え)（(switch workflow)）] をクリックしてカスタム ワークフローを含む別のワークフローを使用します。

- 基本的なワークフロー操作を実行します（ディスカバリおよびアイデンティティ ワークフローの使用（3199 ページ）を参照）。
- テーブルのカラムの内容について詳しく調べます（アプリケーション データ フィールド（3232 ページ）を参照）。
- クライアント、アプリケーション プロトコル、Web アプリケーションの横にあるアプリケーション詳細ビューのアイコン（  ）をクリックすることによって、特定のアプリケーションの[アプリケーション詳細ビュー（Application Detail View）] を開きます。
- （所属する組織でイベント データを外部の Firepower システムに保存している場合）イベントの値を右クリックして、パケットや履歴データなどのイベントに関連する情報を調査します。表示されるオプションは、データタイプやシステムに設定されている統合によって異なります。詳細については、を使用したイベント調査 Cisco Security Packet Analyzer（2882 ページ）および Web ベースのリソースを使用したイベントの調査（2890 ページ）を参照してください。
- テーブルでイベントの値を右クリックしてシスコまたはサードパーティのインテリジェンス ソースを選択して、イベントに関するインテリジェンスを収集します。たとえば、不審な IP アドレスに関する詳細情報を Cisco Talos から入手できます。表示されるオプションは、データタイプやシステムに設定されている統合によって異なります。詳細については、「Web ベースのリソースを使用したイベントの調査（2890 ページ）」を参照してください。

アプリケーション データ フィールド

システムは、既知のクライアント、アプリケーションプロトコル、または Web アプリケーションについてトラフィックを検出すると、アプリケーションおよびそのアプリケーションを実行しているホストに関する情報をログに記録します。

次に、アプリケーション テーブルで表示および検索できるフィールドについて説明します。

Application

検出されたアプリケーションの名前。

IP Address

アプリケーションを使用しているホストに関連付けられている IP アドレス。

タイプ（Type）

アプリケーションのタイプであり、次のものがあります。

アプリケーション プロトコル（Application Protocols）

ホスト間の通信を意味します。

クライアント アプリケーション

ホスト上で動作しているソフトウェアを意味します。

Web アプリケーション（Web Applications）

HTTP トラフィックの内容や要求された URL を意味します。

カテゴリ（Category）

アプリケーションの最も不可欠な機能を表す一般的な分類。各アプリケーションは、少なくとも 1 つのカテゴリに属します。

タグ

アプリケーションに関する追加情報。アプリケーションには任意の数のタグを付けることができます（タグなしも可能）。

リスク（Risk）

アプリケーションが組織のセキュリティポリシーに違反することがある目的で使用される可能性。アプリケーションのリスクの範囲は、[極めて低（Very Low）] から [極めて高（Very High）] までです。

侵入イベントをトリガーしたトラフィックで検出される Application Protocol Risk、Client Risk、Web Application Risk の 3 つ（存在する場合）の中で最も高いものとなります。

ビジネスとの関連性（Business Relevance）

アプリケーションが、娯楽目的ではなく、組織のビジネス活動の範囲内で使用される可能性。アプリケーションのビジネスとの関連性の範囲は、[極めて低（Very Low）] から [極めて高（Very High）] までです。

侵入イベントをトリガーしたトラフィックで検出される Application Protocol Business Relevance、Client Business Relevance、Web Application Business Relevance の 3 つ（存在する場合）の中で最も低いものとなります。

現在のユーザ（Current User）

ホストに現在ログインしているユーザの ID（ユーザ名）。

権限のないユーザがホストにログインすると、そのログインはユーザおよびホストの履歴に記録されることに注意してください。権限のあるユーザがホストに関連付けられていない場合、権限のないユーザがそのホストの現行ユーザとなることが可能です。ただし、権限のあるユーザがホストにログインした後は、権限のある別のユーザがログインした場合のみ、現行ユーザが変わります。また、権限のないユーザがホストの現行ユーザである場合、そのユーザを使用してユーザ制御を行うことはできません。

ドメイン（Domain）

アプリケーションを使用しているホストのドメイン。 This field is only present if you have ever configured the Firepower Management Center for multitenancy.

メンバー数（Count）

各行に表示された情報と一致するイベントの数。[カウント（Count）] フィールドは、複数の同一行が生成される制限を適用した後でのみ表示されることに注意してください。

関連トピック

イベントの検索 （2967 ページ）

アプリケーション詳細データの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Any Security Analyst

Firepower Management Center を使用して、検出されたアプリケーションの詳細テーブルを表示できます。ここでユーザは、検索する情報に応じてイベント ビューを操作することができます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

ユーザがアプリケーションの詳細にアクセスするときに表示されるページは、使用するワークフローによって異なります。2つの事前定義されたワークフローがあります。また、特定のニーズを満たす情報だけを表示するカスタム ワークフローを作成することもできます。

ステップ 1 次のようにして、アプリケーション詳細データにアクセスします。

- 事前定義されたワークフローを使用する場合、**[Analysis]** > **[Hosts]** > **[Application Details]** を選択します。
- アプリケーションの詳細のテーブル ビューが含まれないカスタム ワークフローを使用している場合は、[(ワークフローの切り替え)（(switch workflow)）] をクリックして [クライアント（Clients）] を選択します。

ステップ 2 次の選択肢があります。

- [(ワークフローの切り替え)（(switch workflow)）] をクリックしてカスタム ワークフローを含む別のワークフローを使用します。
- 基本的なワークフロー操作を実行します（ディスカバリおよびアイデンティティ ワークフローの使用（3199 ページ）を参照）。
- テーブルのカラムの内容について詳しく調べます（アプリケーションの詳細データ フィールド（3235 ページ）を参照）。
- クライアントの横にあるアプリケーション詳細ビューのアイコン（  ）をクリックして、特定のアプリケーションの [アプリケーション詳細ビュー（Application Detail View）] を開きます。
- （所属する組織でイベント データを外部の Firepower システムに保存している場合）イベントの値を右クリックして、パケットや履歴データなどのイベントに関連する情報を調査します。表示されるオプションは、データタイプやシステムに設定されている統合によって異なります。詳細については、を使用したイベント調査 Cisco Security Packet Analyzer （2882 ページ）およびWeb ベースのリソースを使用したイベントの調査 （2890 ページ）を参照してください。
- テーブルでイベントの値を右クリックしてシスコまたはサードパーティのインテリジェンス ソースを選択して、イベントに関するインテリジェンスを収集します。たとえば、不審な IP アドレスに関する

詳細情報を Cisco Talos から入手できます。表示されるオプションは、データタイプやシステムに設定されている統合によって異なります。詳細については、「Web ベースのリソースを使用したイベントの調査 （2890 ページ）」を参照してください。

アプリケーションの詳細データ フィールド

システムは、既知のクライアント、アプリケーションプロトコル、またはWebアプリケーションについてトラフィックを検出すると、アプリケーションおよびそのアプリケーションを実行しているホストに関する情報をログに記録します。

次に、アプリケーションの詳細テーブルで表示および検索できるフィールドについて説明します。

前回の使用（Last Used）

アプリケーションが最後に使用された時間、またはホスト入力機能を使用してアプリケーションデータが更新された時間。[前回の使用（Last Used）]の値は、システムがアプリケーション情報の更新を検出したときだけでなく、少なくともユーザがネットワーク検出ポリシーに設定した更新間隔の頻度で更新されます。

[IPアドレス（IP Address）]

アプリケーションを使用しているホストに関連付けられている IP アドレス。

クライアント（Client）

アプリケーションの名前。システムがアプリケーションプロトコルを検出したものの、特定のクライアントを検出できなかった場合は、一般的な名前を提示するために、アプリケーションプロトコル名に `client` が付加されます。

Version

アプリケーションのバージョン。

クライアント、アプリケーション プロトコル、および Web アプリケーションのカテゴリ、タグ、リスク、またはビジネスとの関係性（Category, Tags, Risk, or Business Relevance for Clients, Application Protocols, and Web Applications）

アプリケーションに割り当てられているカテゴリ、タグ、リスク レベル、およびビジネスとの関連性。これらのフィルタを使用して、特定のデータ セットを対象にすることができます。

アプリケーション プロトコル（Application Protocol）

アプリケーションで使用されるアプリケーションプロトコル。ただし、システムがアプリケーションプロトコルを検出したにも関わらず特定のクライアントを検出できなかった場合は、アプリケーション プロトコル名に `client` が付加されて一般名が表示されます。

Web アプリケーション（Web Application）

HTTP トラフィックでシステムが検出したペイロード コンテンツまたは URL に基づく Web アプリケーション。ただし、HTTP のアプリケーション プロトコルが検出されたにも関わらず特定の Web アプリケーションを検出できない場合、ここには、標準の Web 閲覧先が表示されます。

ヒット数（Hits）

システムが使用中のアプリケーションを検出した回数。ホスト入力機能を使用して追加されたアプリケーションの場合、この値は常に 0 になります。

ドメイン（Domain）

アプリケーションを使用しているホストのドメイン。 This field is only present if you have ever configured the Firepower Management Center for multitenancy.

Device

アプリケーションの詳細が含まれている検出イベントを生成したデバイス。

現在のユーザ（Current User）

ホストに現在ログインしているユーザの ID（ユーザ名）。

権限のないユーザがホストにログインすると、そのログインはユーザおよびホストの履歴に記録されることに注意してください。権限のあるユーザがホストに関連付けられていない場合、権限のないユーザがそのホストの現行ユーザとなることが可能です。ただし、権限のあるユーザがホストにログインした後は、権限のある別のユーザがログインした場合のみ、現行ユーザが変わります。また、権限のないユーザがホストの現行ユーザである場合、そのユーザを使用してユーザ制御を行うことはできません。

Count

各行に表示された情報と一致するイベントの数。[カウント（Count）] フィールドは、複数の同一行が生成される制限を適用した後でのみ表示されることに注意してください。

関連トピック

イベントの検索 （2967 ページ）
ネットワーク検出のデータ ストレージ設定 （2669 ページ）

脆弱性データ

Firepower システムには、それ独自の脆弱性追跡データベースが含まれています。そのデータベースは、このシステムのフィンガープリンティング機能と組み合わせて使用されて、ネットワーク上のホストに関連付けられている脆弱性が特定されます。ホストで稼動しているオペレーティング システム、サーバ、およびクライアントには、関連付けられている異なる脆弱性一式があります。

Firepower Management Center を使用して次のことを行えます。

- ホストごとの脆弱性を追跡および確認できます。
- ホストにパッチを適用した後、またはホストが脆弱性に影響されないと判断した場合は、そのホストの脆弱性を非アクティブにすることができます。

サーバで使用されるアプリケーションプロトコルが Firepower Management Center 構成内でマップされない限り、ベンダーレスおよびバージョンレスのサーバの脆弱性はマップされません。ベンダーレスおよびバージョンレスのクライアントの脆弱性はマップできません。

関連トピック

サーバの脆弱性のマッピング （1316 ページ）

脆弱性データのフィールド

以下に説明する脆弱性データのフィールドは、脆弱性のテーブル ビューと脆弱性の詳細表示で次のように表示されます。

表 *348* : 表示場所別の脆弱性データ フィールド

フィールド	テーブル ビュー	詳細の表示
その他の情報	いいえ	はい
使用可能なエクスプロイト（Available Exploits）	はい	はい
Bugtraq ID	はい	はい
CVE ID	いいえ	はい
Count	はい	いいえ（No）
発行日（Date Published）	はい	はい
説明	はい	はい
修正（Fixes）	いいえ	はい
影響修飾子（Impact Qualification）	いいえ	はい
[リモート（Remote）]	はい	はい
Snort ID	はい	はい
ソリューション	はい	はい
SVID	はい	はい

フィールド	テーブル ビュー	詳細の表示
技術的説明（Technical Description）	はい	はい
タイトル（Title）	はい	はい
脆弱性の影響（Vulnerability Impact）	はい	はい

その他の情報

既知の不正利用や可用性、不正利用のシナリオ、脆弱性を軽減する方針など、脆弱性に関する追加情報を（利用可能な場合に）表示するには、矢印をクリックします。

使用可能なエクスプロイト（Available Exploits）

脆弱性に対して既知の不正利用があるかどうかを示します（TRUE/FALSE）。

Bugtraq ID

Bugtraq データベースにおいて脆弱性に関連付けられている識別番号。（http://www.securityfocus.com/bid/）

メンバー数（Count）

各行に表示された情報と一致するイベントの数。[カウント（Count）] フィールドは、複数の同一行が生成される制限を適用した後でのみ表示されることに注意してください。

CVE ID

MITRE の Common Vulnerabilities and Exposures（CVE）データベース（https://cve.mitre.org/）の脆弱性に関連付けられた識別番号。

発行日（Date Published）

脆弱性が公開された日付。

説明（Description）

脆弱性についての簡単な説明。

修正（Fixes）

選択した脆弱性に対して、ダウンロード可能なパッチへのリンクを提供します。

ヒント 修正ファイルまたはパッチのダウンロードに対する直接リンクが表示されている場合は、リンクを右クリックして、自分のローカル コンピュータへ保存します。

影響修飾子（Impact Qualification）

ドロップダウン リストを使用して、脆弱性を有効または無効にします。Firepower Management Centerは、影響の相関関係において、無効な脆弱性を無視します。

ユーザがここで指定する設定によって、システム全体で脆弱性がどのように処理されるか、およびユーザが値を選択するホスト プロファイルに脆弱性が限定されないかが決まります。

リモート（Remote）

脆弱性がリモートで不正利用されるかどうかを示します（TRUE/FALSE）。

Snort ID

[Snort ID]（SID）データベースにおいて脆弱性に関連付けられている識別番号。つまり、侵入ルールで特定の脆弱性を悪用するネットワーク トラフィックを検出できる場合、その脆弱性は、侵入ルールの SID に関連付けられます。

脆弱性は複数のSIDに関連付けることが可能（またはSIDに関連付けないことも可能）であることに注意してください。脆弱性が複数のSIDに関連付けられている場合、脆弱性テーブルには、各 SID に対して 1 つのローが含まれています。

ソリューション（Solution）

脆弱性の修復に関する情報。

SVID

脆弱性を追跡するためにシステムで使用する Cisco の脆弱性識別番号。

SVID について脆弱性の詳細にアクセスするには、表示アイコン（  ）をクリックします。

技術的説明（Technical Description）

脆弱性に関する詳細な技術的説明。

タイトル（Title）

脆弱性のタイトル。

脆弱性の影響（Vulnerability Impact）

Bugtraqデータベースにおいて脆弱性に割り当てられている重大度を示します。0～10の値で、10 は最も重大であることを示します。脆弱性の影響は、Bugtraq エントリの作成者によって決定されます。この作成者は、自身の判断および SANS Critical Vulnerability Analysis（CVA）の基準に従って脆弱性の影響を決定します。

関連トピック

イベントの検索 （2967 ページ）

脆弱性の非アクティブ化

脆弱性を非アクティブ化すると、システムでこの脆弱性を使用して侵入の影響の関連付けを評価することができなくなります。ネットワーク上のホストにパッチを適用した後、またはホストが脆弱性の影響を受けないと判断した後に、脆弱性を非アクティブ化できます。システムが、この脆弱性から影響を受けている新しいホストを検出すると、この脆弱性はこのホストに対して有効であると見なされます（自動的には非アクティブ化されません）。

IPアドレスによって制約されて**いない**脆弱性ワークフロー内である1つの脆弱性を非アクティブ化すると、ネットワーク上の検出されたすべてのホストに対してその脆弱性が非アクティブ化されます。脆弱性ワークフロー内の脆弱性を非アクティブ化できるのは、次の各ページだけです。

- デフォルトの脆弱性ワークフローの2ページ目の[ネットワーク上の脆弱性（Vulnerabilities on the Network）]。これには、ネットワーク上のホストに適用される脆弱性のみが表示されます。
- 脆弱性ワークフロー（カスタムまたは事前定義）のページ。このワークフローは、検索を使用してIPアドレスに基づいて制約されます。

1台のホストに対して1つの脆弱性を非アクティブ化できます。この非アクティブ化は、ネットワーク マップの使用、ホストのホスト プロファイルの使用、または脆弱性を非アクティブ化する対象の1つ以上のホストのIPアドレスに基づいて脆弱性ワークフローを制約することによって行えます。関連付けられた複数のIPアドレスを持つホストの場合、この機能はそのホストの選択された1つのIPアドレスのみに適用されます。

マルチドメイン展開では、先祖ドメインで脆弱性を非アクティブ化すると、すべての子孫ドメインでその脆弱性が非アクティブ化されます。リーフ ドメインでは、脆弱性が先祖ドメインでアクティブ化された場合、リーフ ドメインのデバイスの脆弱性をアクティブ化または非アクティブ化できます。

関連トピック

個々のホストに対する脆弱性の非アクティブ化 （3188 ページ）
個々の脆弱性の非アクティブ化 （3189 ページ）
複数の脆弱性の非アクティブ化 （3242 ページ）

脆弱性データの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Any Security Analyst

Firepower Management Centerを使用して、脆弱性のテーブルを表示できます。ここでユーザは、検索する情報に応じてイベント ビューを操作することができます。

脆弱性にアクセスするときに表示されるページは、使用するワークフローによって異なります。ユーザは事前定義のワークフローを使用できますが、これには脆弱性のテーブル ビューが

含まれています。検出されたいずれかのホストが脆弱性を示しているかどうかに関係なく、テーブル ビューにはデータベース内の各脆弱性に対して 1 つのローが含まれています。事前定義のワークフローの 2 ページ目には、ネットワーク上で検出されたホストに適用されるそれぞれの脆弱性（まだユーザが非アクティブにしていないもの）に対して 1 つのローが含まれています。事前定義のワークフローは脆弱性の詳細ビューで終了しますが、このビューには、制約を満たすすべての脆弱性について詳細な説明が含まれています。

ヒント 単一のホストまたはホストのセットに適用される脆弱性を表示する場合は、ホストの IP アドレスまたは IP アドレスの範囲を指定して、脆弱性の検索を実行します。

また、特定のニーズを満たす情報だけを表示するカスタム ワークフローを作成することもできます。

脆弱性のテーブルは、マルチドメイン展開のドメインによって制限されません。

ステップ 1 次のように、脆弱性のテーブルにアクセスします。

- 事前定義された脆弱性ワークフローを使用する場合、**[Analysis]** > **[Hosts]** > **[Vulnerabilities]** を選択します。
- 脆弱性テーブル ビューが含まれないカスタム ワークフローを使用している場合は、[(ワークフローの切り替え)（(switch workflow)）] をクリックして [脆弱性（Vulnerabilities）] を選択します。

ステップ 2 次の選択肢があります。

- 基本的なワークフロー操作を実行します（ディスカバリおよびアイデンティティ ワークフローの使用（3199 ページ）を参照）。
- 脆弱性を非アクティブにして、現在脆弱な状態にあるホストについて、侵入の影響の相関に使用しないようにします（複数の脆弱性の非アクティブ化 （3242 ページ）を参照）。
- SVID カラムの表示アイコン（）をクリックして、脆弱性に関する詳細を表示します。または、脆弱性 ID を制約して脆弱性の詳細ページへドリルダウンします。
- タイトルを右クリックして [フルテキストの表示（Show Full Text）] を選択することによって、脆弱性タイトルのフルテキストを表示します。

脆弱性の詳細の表示

脆弱性の詳細は、次の方法のいずれかで表示できます。

- **[Analysis]** > **[Hosts]** > **[Vulnerabilities]** を選択し、SVID の横にある表示アイコン（）をクリックします。
- **[Analysis]** > **[Hosts]** > **[Third-Party Vulnerabilities]** を選択し、SVID の横にある表示アイコン（）をクリックします。
- **[Analysis]** > **[Hosts]** > **[Network Map]** を選択し、[脆弱性（Vulnerabilities）] タブをクリックします。

- 脆弱性の影響を受けるホストのプロファイルを表示し、そのプロファイルの [脆弱性（Vulnerabilities）] セクションを展開します。

複数の脆弱性の非アクティブ化

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Any Security Analyst

IPアドレスで制約されて**いない**脆弱性ワークフロー内で脆弱性を非アクティブにすると、ネットワーク上で検出されたすべてのホストに対する脆弱性が非アクティブ化されます。

マルチドメイン導入では、先祖ドメインで脆弱性を非アクティブ化すると、すべての子孫ドメインでも脆弱性が非アクティブ化されます。リーフ ドメインは、先祖ドメインで脆弱性がアクティブ化されていれば、自分のデバイスの脆弱性をアクティブ化または非アクティブ化できます。

ステップ 1 次のように、脆弱性のテーブルにアクセスします。

- 事前定義された脆弱性ワークフローを使用する場合、**[Analysis]** > **[Hosts]** > **[Vulnerabilities]** を選択します。
- 脆弱性テーブル ビューが含まれないカスタム ワークフローを使用している場合は、[(ワークフローの切り替え)（(switch workflow)）] をクリックして [脆弱性（Vulnerabilities）] を選択します。

ステップ 2 [ネットワークの脆弱性（Vulnerabilities on the Network）] をクリックします。

ステップ 3 非アクティブにする脆弱性の横にあるチェックボックスをオンにします。

ステップ 4 ページ下部の [レビュー（Review）] をクリックします。

関連トピック

個々のホストに対する脆弱性の非アクティブ化 （3188 ページ）
個々の脆弱性の非アクティブ化 （3189 ページ）

サードパーティの脆弱性データ

Firepower システムには、それ独自の脆弱性追跡データベースが含まれています。そのデータベースは、このシステムのフィンガープリンティング機能と組み合わせて使用されて、ネットワーク上のホストに関連付けられている脆弱性が特定されます。

システムの脆弱性データは、サードパーティ製のアプリケーションからインポートしたネットワーク マップ データで補完できます。これを行うには、組織で、このデータをインポートするためのスクリプトを記述できるか、コマンドラインでファイルのインポートを作成できなけ

ればなりません。詳細については、*Firepower* システム ホスト入力 *API* ガイドを参照してください。

インポートしたデータを影響の相関に含めるには、サードパーティの脆弱性情報を、データベース内のオペレーティング システムおよびアプリケーションの定義にマップする必要があります。サードパーティの脆弱性情報は、クライアントの定義にマップすることはできません。

サードパーティの脆弱性データの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Any Security Analyst

ホスト入力機能を使用してサードパーティの脆弱性データをインポートした後で、Firepower Management Center を使用してサードパーティの脆弱性のテーブルを表示することができます。ここでユーザは、検索する情報に応じてイベント ビューを操作することができます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

サードパーティの脆弱性にアクセスするときに表示されるページは、使用するワークフローによって異なります。2 つの事前定義されたワークフローがあります。また、特定のニーズを満たす情報だけを表示するカスタム ワークフローを作成することもできます。

ステップ 1 次のようにして、サードパーティの脆弱性データにアクセスします。

- 事前定義されたワークフローを使用する場合、**[Analysis]** > **[Hosts]** > **[Third-Party Vulnerabilities]** を選択します。
- サードパーティの脆弱性のテーブル ビューが含まれないカスタム ワークフローを使用している場合は、[(ワークフローの切り替え)（(switch workflow)）] をクリックして [送信元別の脆弱性（Vulnerabilities by Source）] または [IP アドレス別の脆弱性（Vulnerabilities by IP Address）] を選択します。

ステップ 2 次の選択肢があります。

- [(ワークフローの切り替え)（(switch workflow)）] をクリックしてカスタム ワークフローを含む別のワークフローを使用します。
- 基本的なワークフロー操作を実行します（ディスカバリおよびアイデンティティ ワークフローの使用（3199 ページ）を参照）。
- テーブルのカラムの内容について詳しく調べます（サードパーティの脆弱性データのフィールド（3244 ページ）を参照）。
- SVID カラムの表示アイコン（  ）をクリックして、サードパーティの脆弱性に関する詳細を表示します。または、脆弱性 ID を制約して脆弱性の詳細ページへドリルダウンします。

サードパーティの脆弱性データのフィールド

サードパーティの脆弱性テーブルで表示および検索できるフィールドの詳細は以下のとおりです。

脆弱性ソース（Vulnerability Source）

サードパーティの脆弱性のソース（QualysGuard、NeXpose など）。

Vulnerability ID

ソースで脆弱性に関連付けられている ID 番号。

IP Address

脆弱性の影響を受けるホストに関連付けられている IP アドレス。

Port

ポート番号（脆弱性が、特定のポート上で実行されているサーバに関連付けられている場合）。

Bugtraq ID

Bugtraq データベースにおいて脆弱性に関連付けられている識別番号。（http://www.securityfocus.com/bid/）

CVE ID

MITRE の Common Vulnerabilities and Exposures（CVE）データベース（https://cve.mitre.org/）の脆弱性に関連付けられた識別番号。

SVID

脆弱性を追跡するためにシステムで使用する従来の脆弱性識別番号。

SVID について脆弱性の詳細にアクセスするには、表示アイコン（  ）をクリックします。

Snort ID

[Snort ID]（SID）データベースにおいて脆弱性に関連付けられている識別番号。つまり、侵入ルールで特定の脆弱性を悪用するネットワーク トラフィックを検出できる場合、その脆弱性は、侵入ルールの SID に関連付けられます。

脆弱性は複数の SID に関連付けることが可能（または SID に関連付けないことも可能）であることに注意してください。脆弱性が複数の SID に関連付けられている場合、脆弱性テーブルには、各 SID に対して 1 つのローが含まれています。

Title

脆弱性のタイトル。

Description

脆弱性についての簡単な説明。

ドメイン（Domain）

この脆弱性を持つホストのドメイン。 This field is only present if you have ever configured the Firepower Management Center for multitenancy.

メンバー数（Count）

各行に表示された情報と一致するイベントの数。[カウント（Count）] フィールドは、複数の同一行が生成される制限を適用した後でのみ表示されることに注意してください。

関連トピック

イベントの検索 （2967 ページ）

アクティブ セッション、ユーザ、およびユーザ アクティビティ データ

アイデンティティ ソースは、アクティブなセッション データ、ユーザ データ、およびユーザ アクティビティ データを収集します。データは、次の個々のユーザ関連のワークフローに表示されます。

- [アクティブなセッション（Active Sessions）]：このワークフローには、ネットワーク上の現在のすべてのユーザ セッションが表示されます。複数の同時アクティブ セッションを実行する単一ユーザは、この表で複数の行を占めます。このワークフローに表示されるユーザ データの種類について、詳しくはアクティブ セッション データ （3255 ページ）を参照してください。
- ユーザ：このワークフローは、ネットワークで認識されるすべてのユーザを表示します。この表では 1 ユーザが 1 つの行を占めます。このワークフローに表示されるユーザ データの種類について、詳しくはユーザ データ（User Data） （3256 ページ）を参照してください。
- ユーザ アクティビティ：このワークフローは、ネットワークで認識されるすべてのユーザ アクティビティを表示します。この表では、複数のユーザ アクティビティ インスタンスを持つ 1 ユーザが複数の行を占めます。このワークフローに表示されるユーザ アクティビティの種類の詳細については、ユーザ アクティビティ データ （3260 ページ）を参照してください。

これらのワークフローの入力元であるアイデンティティ ソースの詳細については、ユーザ アイデンティティ ソースについて （2482 ページ）を参照してください。

ユーザ関連フィールド

ユーザ関連データは、アクティブ セッション、ユーザ、およびユーザ アクティビティのテーブルに表示されます。

表 *349*：アクティブ セッション、ユーザ、およびユーザ アクティビティのフィールドの説明

フィールド	説明	[アクティブなセッション（Active Sessions）] テーブル	[ユーザテーブル（Users Table）]	[ユーザアクティビティ（User Activity）] テーブル
アクティブセッション数（Active Session Count）	ユーザに関連付けられているアクティブセッションの数。	なし	あり	なし
認証タイプ（Authentication Type）	認証のタイプ：[認証なし（No Authentication）]、[パッシブ認証（Passive Authentication）]、[アクティブ認証（Active Authentication）]、[ゲスト認証（Guest Authentication）]、[失敗した認証（Failed Authentication）]、または [VPN 認証（VPN Authentication）]。 各認証タイプでサポートされるアイデンティティソースの詳細については、ユーザ アイデンティティ ソースについて（2482ページ）を参照してください。	あり	なし	あり
ポリシーに使用可能	値 [はい（Yes）] は、ユーザがユーザ ストア（Active Directory など）から取得されたことを意味します。 値 [いいえ（No）] は、FMC がそのユーザのログインのレポートを取得したものの、そのユーザがユーザストアに存在しないことを意味します。これは、除外されたグループのユーザがユーザストアにログインした場合に発生することがあります。レルムを設定するときにグループをダウンロード対象から除外することができます。 ポリシーに使用できないユーザは FMC に記録されますが、管理対象デバイスには送信されません。	なし	あり	なし
メンバー数（Count）	（注） [カウント（Count）] フィールドは、制約を適用した結果、同じ行が複数作成された場合にのみ表示されます。 テーブルに応じて、特定の行に表示される情報と一致するセッション、ユーザ、またはアクティビティ イベントの数。	あり	あり	あり

フィールド	説明	[アクティブなセッション（Active Sessions）] テーブル	[ユーザテーブル（Users Table）]	[ユーザアクティビティ（User Activity）] テーブル
現在の IP（Current IP）	ユーザがログインしたホストに関連付けられている IP アドレス。 ユーザにアクティブセッションがない場合、[ユーザ（Users）] テーブルでこのフィールドが空白になります。	あり	あり	なし
部署名（Department）	ユーザの部署（レルムが取得）。サーバ上のユーザに明示的に関連付けられている部門がない場合、この部門は、サーバが割り当てるいずれかのデフォルト グループとして示されます。たとえば、Active Directory では、これは `Users (ad)` となります。以下の場合、このフィールドは空白になります。 • レルムを設定していない。 • Firepower Management Center が、FMC データベースのユーザと LDAP レコードを相関させていない（AIM、Oracle、または SIP ログインによってユーザがデータベースに追加された場合など）。	あり	あり	なし
Description	セッション、ユーザ、またはユーザ アクティビティについての詳細情報（利用可能な場合）。	なし	なし	あり
[デバイス（Device）]	トラフィックベースの検出またはアクティブ認証アイデンティティ ソースによって検出されたユーザアクティビティの場合は、ユーザを識別したデバイスの名前。 他のタイプのユーザアクティビティの場合は、管理している側の Firepower Management Center になります。	あり	なし	あり

フィールド	説明	[アクティブなセッション（**Active Sessions**）] テーブル	[ユーザテーブル（**Users Table**）]	[ユーザアクティビティ（**User Activity**）] テーブル
ディスカバリアプリケーション（Discovery Application）	ユーザの検出に使用されるアプリケーションまたはプロトコル。 • トラフィックベースの検出によって検出されたユーザ アクティビティの場合は、ldap、pop3、imap、oracle、sip、http、ftp、mdns、または aim のいずれか。 （注） ユーザはSMTP ログインに基づいてデータベースに追加されません。 • 他のすべてのユーザアクティビティの場合：ldap。	あり	あり	あり
[現在の IP ドメイン（Current IP Domain）]/[ドメイン（Domain）]	[アクティブセッション（Active Sessions）] テーブルでは、ユーザアクティビティが検出されたマルチテナンシー ドメイン。 [ユーザ（Users）] テーブルでは、ユーザのレルムに関連付けられたマルチテナンシー ドメイン。 [ユーザ アクティビティ（User Activity）] テーブルでは、ユーザアクティビティが検出されたマルチテナンシー ドメイン。 This field is only present if you have ever configured the Firepower Management Center for multitenancy.	あり	あり	あり
電子メール（E-Mail）	ユーザの電子メールアドレス。以下の場合、このフィールドは空白になります。 • AIM ログインによってユーザがデータベースに追加された。 • LDAP ログインによってユーザがデータベースに追加されており、LDAP サーバ上にユーザと関連付けられている電子メールアドレスが存在しない。	あり	あり	なし

フィールド	説明	[アクティブなセッション（Active Sessions）] テーブル	[ユーザテーブル（Users Table）]	[ユーザアクティビティ（User Activity）] テーブル
終了ポート（End Port）	TS エージェントによってユーザが報告され、そのユーザのセッションが現在アクティブである場合、このフィールドは、ユーザに割り当てられたポート範囲の終了値を示します。ユーザの TS エージェントセッションが非アクティブである場合、またはユーザが別のアイデンティティ ソースによって報告された場合、このフィールドは空白になります。	あり	なし	あり
エンドポイントロケーション（Endpoint Location）	ISE で指定された、ユーザの認証に ISE を使用したネットワーク デバイスの IP アドレス。ISE を設定していない場合、このフィールドは空白です。	なし	なし	あり
エンドポイントプロファイル（Endpoint Profile）	Cisco ISE によって識別されるユーザのエンドポイント デバイス タイプ。ISE を設定していない場合、このフィールドは空白です。	なし	なし	あり
イベント	ユーザ アクティビティのタイプ。	なし	なし	あり
First Name	ユーザの名（レルムが取得）。以下の場合、このフィールドは空白になります。 • レルムを設定していない。 • Firepower Management Center が、FMC データベースのユーザと LDAP レコードを相関させていない（AIM、Oracle、または SIP ログインによってユーザがデータベースに追加された場合など）。 • サーバに、対象のユーザと関連付けられている名がない。	あり	あり	なし

フィールド	説明	[アクティブなセッション（Active Sessions）] テーブル	[ユーザテーブル（Users Table）]	[ユーザアクティビティ（User Activity）] テーブル
[IPアドレス（IP Address）]	[ユーザ ログイン（User Login）] ユーザ アクティビティの場合は、次のログインに関連するIPアドレスまたは内部 IP アドレス。 • LDAP、POP3、IMAP、FTP、HTTP、MDNS、および AIM ログイン：ユーザのホストのアドレス • SMTP および Oracle のログイン：サーバのアドレス • SIP ログイン：セッション発信者のアドレス 関連付けられているIPアドレスは、そのユーザがIPアドレスの現行のユーザであることを意味するわけではありません。権限を持たないユーザがホストにログインすると、そのログインはユーザおよびホストの履歴に記録されます。権限のあるユーザがホストに関連付けられていない場合、権限のないユーザがそのホストの現行ユーザとなることができます。ただし、権限のあるユーザがホストにログインした後は、権限のある別のユーザがログインした場合のみ、現行ユーザが変わります。 他のタイプのユーザアクティビティの場合、このフィールドは空白です。	なし	なし	あり
Last Name	ユーザの姓（レルムが取得）。以下の場合、このフィールドは空白になります。 • レルムを設定していない。 • Firepower Management Center が、FMC データベースのユーザと LDAP レコードを相関させていない（AIM、Oracle、または SIP ログインによってユーザがデータベースに追加された場合など）。 • サーバに、対象のユーザと関連付けられている姓がない。	あり	あり	なし

フィールド	説明	[アクティブなセッション（Active Sessions）] テーブル	[ユーザテーブル（Users Table）]	[ユーザアクティビティ（User Activity）] テーブル
前回の検出（Last Seen）	ユーザのセッションが最後に開始された（またはユーザ データが更新された）日時。	あり	あり	なし
ログイン時刻（Login Time）	ユーザのセッションが開始した日時。	あり	なし	なし
Phone	ユーザの電話番号（レルムが取得）。以下の場合、このフィールドは空白になります。 • レルムを設定していない。 • Firepower Management Center が、FMC データベースのユーザと LDAP レコードを相関させていない（AIM、Oracle、または SIP ログインによってユーザがデータベースに追加された場合など）。 • サーバに、対象のユーザと関連付けられている電話番号が存在しない。	あり	あり	なし
レルム	ユーザに関連付けられているアイデンティティ レルム。	あり	あり	あり
セキュリティ グループ タグ（Security Group Tag）	パケットが信頼できる TrustSec ネットワークへ送信されたときに、Cisco TrustSec によって適用される [セキュリティ グループ タグ（Security Group Tag）]（SGT）属性。ISE を設定していない場合、このフィールドは空白です。	なし	なし	あり
セッション時間（Session Duration）	[ログイン時刻（Login Time）] と現在の時刻から計算されたユーザ セッションの期間。	あり	なし	なし
開始ポート（Start Port）	TS エージェントによってユーザが報告され、そのユーザのセッションが現在アクティブである場合、このフィールドは、ユーザに割り当てられたポート範囲の開始値を示します。ユーザの TS エージェント セッションが非アクティブである場合、またはユーザが別のアイデンティティ ソースによって報告された場合、このフィールドは空白になります。	あり	なし	あり

フィールド	説明	[アクティブなセッション（Active Sessions）] テーブル	[ユーザテーブル（Users Table）]	[ユーザアクティビティ（User Activity）] テーブル
時刻（Time）	システムがユーザ アクティビティを検出した時間。	なし	なし	あり
[ユーザ（User）]	このフィールドには少なくとも、ユーザのレルムとユーザ名が表示されます。たとえば、`Lobby\jsmith` と表示された場合は、Lobby がレルム、jsmith がユーザ名です。 レルムが LDAP サーバから追加のユーザ データをダウンロードし、システムがそれをユーザに関連付けた場合は、このフィールドにユーザの名、姓、タイプも表示されます。たとえば、`John Smith (Lobby\jsmith, LDAP)` と表示された場合は、John Smith がユーザの名前、LDAP がそのタイプです。 （注） トラフィックベースの検出では失敗した AIM ログインが記録される可能性があるため（たとえば、ユーザが正しくないユーザ名を入力した場合など）、Firepower Management Center は無効な AIM ユーザを保存する可能性があります。	あり	あり	なし
Username	ユーザに関連付けられているユーザ名。	あり	あり	あり
VPN 受信バイト数（VPN Bytes In）	リモート アクセス VPN の報告によるユーザ アクティビティの場合は、Firepower Threat Defense がリモート ピアまたはクライアントから受信した合計バイト数。 （注） ユーザの VPN セッションが終了した後、受信した合計バイト数を表示できます。継続中の VPN セッションでは、これは動的カウンタではありません。 他のタイプのユーザ アクティビティの場合、このフィールドは空白です。	なし	なし	あり

フィールド	説明	[アクティブなセッション（Active Sessions）] テーブル	[ユーザテーブル（Users Table）]	[ユーザアクティビティ（User Activity）] テーブル
VPN 送信バイト数（VPN Bytes Out）	リモート アクセス VPN の報告によるユーザ アクティビティの場合は、Firepower Threat Defense がリモート ピアまたはクライアントに伝送された合計バイト数。 （注） ユーザの VPN セッションが終了した後、送信した合計バイト数を表示できます。継続中の VPN セッションでは、これは動的カウンタではありません。 他のタイプのユーザ アクティビティの場合、このフィールドは空白です。	なし	なし	あり
VPN クライアントのアプリケーション（VPN Client Application）	リモート アクセス VPN の報告によるユーザ アクティビティの場合は、リモート ユーザの AnyConnect VPN クライアント アプリケーション。 他のタイプのユーザ アクティビティの場合、このフィールドは空白です。	あり	なし	あり
VPN クライアントの国（VPN Client Country）	リモート アクセス VPN の報告によるユーザ アクティビティの場合は、AnyConnect VPN クライアントによって報告された国名。 他のタイプのユーザ アクティビティの場合、このフィールドは空白です。	なし	なし	あり
VPN クライアントの OS（VPN Client OS）	リモート アクセス VPN の報告によるユーザ アクティビティの場合は、AnyConnect VPN クライアントによって報告されたリモート ユーザのエンドポイント オペレーティング システム。 他のタイプのユーザ アクティビティの場合、このフィールドは空白です。	あり	なし	あり
VPN クライアントのパブリック IP（VPN Client Public IP）	リモート アクセス VPN の報告によるユーザ アクティビティの場合は、AnyConnect VPN クライアント デバイスのパブリック ルーティング可能な IP アドレス。 他のタイプのユーザ アクティビティの場合、このフィールドは空白です。	あり	なし	あり

フィールド	説明	[アクティブなセッション（Active Sessions）] テーブル	[ユーザテーブル（Users Table）]	[ユーザアクティビティ（User Activity）] テーブル
VPN 接続期間（VPN Connection Duration）	リモート アクセス VPN の報告によるユーザ アクティビティの場合は、セッションがアクティブだった合計時間（HH:MM:SS）。 他のタイプのユーザアクティビティの場合、このフィールドは空白です。	なし	なし	あり
VPN 接続プロファイル（VPN Connection Profile）	リモート アクセス VPN の報告によるユーザ アクティビティの場合は、VPNセッションで使用される接続プロファイル（トンネル グループ）の名前。接続プロファイルは、リモートアクセスVPNポリシーに含まれます。 他のタイプのユーザアクティビティの場合、このフィールドは空白です。	あり	なし	あり
VPN グループ ポリシー（VPN Group Policy）	リモート アクセス VPN の報告によるユーザ アクティビティの場合は、VPNセッションが確立されたときにクライアントに割り当てられたグループポリシーの名前。これは VPN 接続プロファイルに関連付けられた静的に割り当てられたグループポリシー、またはRADIUSが認証に使用されている場合は動的に割り当てられたグループポリシーです。RADIUS サーバによって割り当てられている場合、このグループ ポリシーは VPN 接続プロファイル用に設定された静的ポリシーよりも優先されます。グループ ポリシーは、リモート アクセス VPN ポリシーのユーザ グループに共通の属性を設定します。 他のタイプのユーザアクティビティの場合、このフィールドは空白です。	あり	なし	あり
VPN セッション タイプ（VPN Session Type）	リモート アクセス VPN の報告によるユーザ アクティビティの場合は、セッションのタイプ（[LAN 間（LAN-to-LAN）] または [リモート（Remote）]）。 他のタイプのユーザアクティビティの場合、このフィールドは空白です。	あり	なし	あり

アクティブ セッション データ

[分析（Analysis）] > [ユーザ（Users）] > [アクティブなセッション（Active Sessions）] ワークフローには、現在のユーザ セッションに関する選択情報が表示されます。ネットワーク上のユーザが複数のセッションを同時に実行するとき、Firepower システムは次の場合にセッションを一意に識別できます。

- 一意の **IP アドレス**値を持っている。
- Cisco Terminal Services（TS）エージェントによって提供される、一意の**開始ポート**値と**終了ポート**値を持っている。
- 一意の**現在の IP ドメイン**値を持っている。
- 異なるアイデンティティ ソースによって認証された。
- 異なるアイデンティティ レルムと関連付けられた。

システムによって保存されるユーザおよびユーザ アクティビティ データの詳細については、ユーザ データ（User Data） （3256 ページ） およびユーザ アクティビティ データ （3260 ページ） を参照してください。

一般的なユーザ関連のイベント トラブルシューティングについては、レルムとユーザのダウンロードのトラブルシュート （2586 ページ） を参照してください。リモート アクセス VPN のトラブルシューティングについては、Firepower Threat Defense の VPN のトラブルシューティング （1165 ページ） を参照してください。

アクティブ セッション データの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Any Security Analyst

アクティブ セッションのテーブルを表示して、検索する情報に応じてイベント ビューを操作することができます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

ユーザにアクセスするときに表示されるページは、使用するワークフローによって異なります。事前定義のワークフローを使用することができますが、これには、検出されたすべてのユーザが記載されているユーザのテーブル ビューが含まれています。このワークフローは、ユーザの詳細ページで終了します。ユーザの詳細ページは、制約を満たす各ユーザについての情報を提供します。

ステップ 1 次のように、ユーザ データにアクセスします。

- 事前定義されたワークフローを使用する場合は、**[分析（Analysis）] > [ユーザ（Users）] > [アクティブなセッション（Active Sessions）]** を選択します。
- アクティブ セッションのテーブル ビューが含まれないカスタム ワークフローを使用している場合は、[(ワークフローの切り替え)（(switch workflow)）] をクリックして [アクティブなセッション（Active Sessions）] を選択します。

ステップ 2 次の選択肢があります。

- [(ワークフローの切り替え)（(switch workflow)）] をクリックしてカスタム ワークフローを含む別のワークフローを使用します。
- 基本的なワークフロー操作を実行します（ディスカバリおよびアイデンティティ ワークフローの使用（3199 ページ）を参照）。
- テーブルのカラムの内容について詳しく調べるには、アクティブ セッション データ （3255 ページ）および ユーザ関連フィールド （3245 ページ） を参照してください。

ユーザ データ（User Data）

アイデンティティ ソースが、データベースに存在しないユーザのユーザ ログインを報告した場合、そのログイン タイプが特に制限されていない限り、そのユーザはデータベースに追加されます。

次のいずれかが発生すると、システムはユーザ データベースを更新します。

- Firepower Management Center のユーザが、[ユーザ（Users）] テーブルから権限のないユーザを手動で削除する。
- アイデンティティ ソースが、そのユーザによるログオフを報告する。
- レルムがレルムの [ユーザ セッションのタイムアウト：認証されたユーザ（User Session Timeout: Authenticated Users）] 設定、[ユーザ セッションのタイムアウト：認証に失敗したユーザ（User Session Timeout: Failed Authentication Users）] 設定、または [ユーザ セッションのタイムアウト：ゲスト ユーザ（User Session Timeout: Guest Users）] 設定で指定されているユーザ セッションを終了した。

（注） ISE/ISE-PIC が設定されている場合は、ユーザ テーブルにホスト データが表示されることがあります。ISE/ISE-PIC によるホスト検出は完全にはサポートされていないため、ISE が報告したホスト データを使用してユーザ制御を実行することはできません。

システムによって検出されたユーザ ログインのタイプに応じて、新しいユーザのどの情報が保存されるかが決まります。

ID ソース	ログイン タイプ	格納されるユーザ データ
ISE/ISE-PIC	Active Directory LDAP RADIUS RSA	• ユーザ名 • 現行の IP アドレス • セキュリティ グループ タグ（SGT）（ISE-PIC ではサポートされていない） • エンドポイントのプロファイル/デバイス タイプ（ISE-PIC ではサポートされていない） • エンドポイントの場所/場所 IP（ISE-PIC ではサポートされていない） • タイプ（LDAP）
ユーザ エージェント	Active Directory	• ユーザ名 • 現行の IP アドレス • タイプ（LDAP）
TS エージェント	Active Directory	• ユーザ名 • 現行の IP アドレス • 開始ポート • 終了ポート • タイプ（LDAP）
キャプティブ ポータル	Active Directory LDAP	• ユーザ名 • 現行の IP アドレス • タイプ（LDAP）

ID ソース	ログイン タイプ	格納されるユーザ データ
トラフィック ベースの検出	LDAP AIM Oracle SIP HTTP FTP MDNS	• ユーザ名 • 現行の IP アドレス • タイプ（AD）
	POP3 IMAP	• ユーザ名 • 現行の IP アドレス • 電子メール アドレス • タイプ（pop3 または imap）

ユーザを自動的にダウンロードするようにレルムを設定すると、Firepower Management Center は指定した間隔に基づいてサーバに対するクエリを実行します。システムが新しいユーザのログインを検出してから、Firepower Management Center データベースがユーザのメタデータを更新するまでに、5～10 分かかることがあります。Firepower Management Centerは、ユーザごとに次の情報とメタデータを取得します。

- ユーザ名
- 姓と名
- 電子メール アドレス
- 部門
- 電話番号
- 現行の IP アドレス
- セキュリティ グループ タグ（SGT）（使用可能な場合）
- エンドポイントのプロファイル（使用可能な場合）
- エンドポイントの場所（使用可能な場合）
- 開始ポート（使用可能な場合）
- 終了ポート（使用可能な場合）

Firepower Management Center がデータベースに格納できるユーザの数は、Firepower Management Center のモデルによって異なります。ホストに対して権限を持たないユーザがログインしていることが検出された場合、そのログインはユーザおよびホストの履歴に記録されます。権限の

あるユーザがホストに関連付けられていない場合、権限のないユーザがそのホストの現行ユーザとなることができます。ただし、ホストに対して権限を持つユーザのログインが検出された後は、権限を持つ別のユーザがログインした場合にのみ、現行ユーザが変わります。

AIM、Oracle、および SIP のログインがトラフィックベースで検出された場合は、システムが LDAP サーバから取得したどのユーザ メタデータにも関連付けられないため、これらのログインにより重複したユーザ レコードが作成されることに注意してください。これらのプロトコルから重複したユーザ レコードを取得することに起因するユーザ カウントの過度な使用を回避するには、これらのプロトコルを無視するようにトラフィックベースの検出を設定します。

データベースからユーザを検索、表示、削除することができます。また、データベースからすべてのユーザを消去することもできます。

一般的なユーザ関連のイベント トラブルシューティングについては、レルムとユーザのダウンロードのトラブルシュート （2586 ページ） を参照してください。

ユーザ データの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Any Security Analyst

ユーザのテーブルを表示して、検索する情報に応じてイベント ビューを操作することができます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

ユーザにアクセスするときに表示されるページは、使用するワークフローによって異なります。事前定義のワークフローを使用することができますが、これには、検出されたすべてのユーザが記載されているユーザのテーブル ビューが含まれています。このワークフローは、ユーザの詳細ページで終了します。ユーザの詳細ページは、制約を満たす各ユーザについての情報を提供します。

ステップ 1 次のように、ユーザ データにアクセスします。

- 事前定義されたワークフローを使用する場合、**[Analysis]** > **[Users]** > **[Users]** を選択します。
- ユーザのテーブル ビューが含まれないカスタム ワークフローを使用している場合は、[(ワークフローの切り替え)（(switch workflow)）] をクリックして [ユーザ（Users）] を選択します。

ステップ 2 次の選択肢があります。

- [(ワークフローの切り替え)（(switch workflow)）] をクリックしてカスタム ワークフローを含む別のワークフローを使用します。
- 基本的なワークフロー操作を実行します（ディスカバリおよびアイデンティティ ワークフローの使用（3199 ページ）を参照）。

- テーブルのカラムの内容について詳しく調べます（ユーザ関連フィールド（3245 ページ）を参照）。

ユーザ アクティビティ データ

Firepower システムでは、ネットワーク上のユーザ アクティビティの詳細を伝達するイベントを生成します。システムがユーザ アクティビティを検出すると、そのユーザ アクティビティ データはデータベースに記録されます。ユーザアクティビティは、表示、検索、および削除することも、すべてのユーザ アクティビティをデータベースから消去することもできます。

あるユーザがネットワーク上で初めて確認されると、システムはそのユーザ アクティビティ イベントをログに記録します。そのユーザがその後に確認された場合、新しいユーザアクティビティイベントはログに記録されません。ただし、そのユーザのIPアドレスが変わった場合、システムは新しいユーザ アクティビティ イベントをログに記録します。

Firepower システムでは、ユーザ アクティビティと他のタイプのイベントとの関連付けも行います。たとえば、侵入イベントは、そのイベントの発生時に送信元ホストと宛先ホストにログインしていたユーザを通知することができます。この関連付けにより、攻撃の対象になったホストにログインしていたユーザ、または内部攻撃やポートスキャンを開始したユーザがわかります。

ユーザ アクティビティは、相関ルールで使用することもできます。相関ルールは、ユーザ アクティビティのタイプだけでなく、指定した他の条件に基づいて作成することができます。相関ルールが相関ポリシーで使用される場合、ネットワーク トラフィックが条件を満たしたときは、相関ルールが修復およびアラートの応答を起動します。

（注） ISE/ISE-PIC が設定されている場合は、ユーザ テーブルにホスト データが表示されることがあります。ISE/ISE-PIC によるホスト検出は完全にはサポートされていないため、ISE が報告したホスト データを使用してユーザ制御を実行することはできません。

次に、4 つのタイプのユーザ アクティビティ データについて説明します。

新しいユーザのアイデンティティ（New User Identity）

このタイプのイベントは、システムがデータベースに存在しない不明なユーザによるログインを検出したときに生成されます。

あるユーザがネットワーク上で初めて確認されると、システムはそのユーザ アクティビティ イベントをログに記録します。そのユーザがその後に確認された場合、新しいユーザアクティビティイベントはログに記録されません。ただし、そのユーザのIPアドレスが変わった場合、システムは新しいユーザ アクティビティ イベントをログに記録します。

ユーザ ログイン（User Login）

このタイプのイベントは、次のことが発生した後に生成されます。

- ユーザ エージェント、ISE/ISE-PIC、または TS エージェントが正常なユーザ ログインを報告した。
- キャプティブ ポータルのユーザ認証の実行が成功または失敗した。
- トラフィック ベースの検出がユーザ ログインの成功または失敗を検出した。

（注） トラフィック ベースの検出で検出された SMTP ログインは、一致する電子メール アドレスを持つユーザがデータベースにすでに存在する場合を除いて記録されません。

権限のないユーザがあるホストにログインすると、そのログインはユーザとホストの履歴に記録されます。権限のあるユーザがホストに関連付けられていない場合、権限のないユーザがそのホストの現行ユーザとなることができます。ただし、権限のあるユーザがそのホストにログインした後は、別の権限のあるユーザによるログインだけが現行ユーザを変更します。

キャプティブ ポータルまたはトラフィック ベースの検出を使用する場合、失敗したユーザ ログインと失敗したユーザ認証データについて、次の点に注意してください。

- トラフィック ベースの検出（LDAP、IMAP、FTP、および POP3 トラフィック）から報告された失敗したログインは、ユーザアクティビティのテーブル ビューに表示されますが、ユーザのテーブル ビューには表示されません。既知のユーザがログインに失敗した場合、システムではそのユーザをそのユーザ名で識別します。不明なユーザがログインに失敗した場合、システムではそのユーザ名として [失敗した認証（Failed Authentication）] を使用します。
- キャプティブ ポータルから報告された失敗した認証は、ユーザ アクティビティのテーブル ビューとユーザのテーブル ビューの両方に表示されます。既知のユーザが認証に失敗した場合、システムではそのユーザをそのユーザ名で識別します。不明なユーザが認証に失敗した場合、システムではそのユーザをそのユーザが入力したユーザ名で識別します。

ユーザのアイデンティティの削除（Delete User Identity）

このタイプのイベントは、データベースからユーザを手動で削除したときに生成されます。

ドロップ（廃棄）されたユーザのアイデンティティ：ユーザ制限に到達（User Identity Dropped: User Limit Reached）

このタイプのイベントは、システムがデータベースに存在しないユーザを検出したものの、Firepower Management Center のモデルで決定されているデータベースの最大ユーザ数に達したためにユーザを追加できなかったときに生成されます。

ユーザ制限に達すると、ほとんどの場合、データベースへの新しいユーザの追加が停止されます。新しいユーザを追加するには、古いユーザまたは非アクティブなユーザをデータベースから手動で削除するか、データベースからすべてのユーザを消去する必要があります。

ただし、システムでは権限のあるユーザが優先されます。すでに制限に達しており、これまでに検出されていない権限のあるユーザのログインが検出された場合、システムは長期間非アク

ティブな状態が続いている権限のないユーザを削除して、権限のある新しいユーザに置き換えます。

ユーザの侵害の兆候イベント

次のユーザの IOC の変化がユーザ アクティビティ データベースに記録されます。

- 侵害の兆候が解決された場合。
- 侵害の兆候ルールがユーザに対して有効または無効にされた場合。

一般的なユーザ関連のイベント トラブルシューティングについては、レルムとユーザのダウンロードのトラブルシュート （2586 ページ） を参照してください。

関連トピック

ユーザ アクティビティ データベース （2488 ページ）

ユーザ アクティビティ データの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Any Security Analyst

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

ユーザ アクティビティのテーブルを表示して、検索する情報に応じてイベント ビューを操作することができます。ユーザアクティビティにアクセスするときに表示されるページは、使用するワークフローによって異なります。事前定義のワークフローを使用することができます。このワークフローにはユーザ アクティビティのテーブル ビューが含まれており、制約を満たすすべてのユーザの詳細が含まれている、ユーザの詳細ページで終了します。また、特定のニーズを満たす情報だけを表示するカスタム ワークフローを作成することもできます。

ステップ 1 次のように、ユーザ アクティビティ データにアクセスします。

- 事前定義されたワークフローを使用する場合、**[Analysis]** > **[Users]** > **[User Activity]** を選択します。
- ユーザアクティビティのテーブル ビューが含まれないカスタム ワークフローを使用している場合は、[(ワークフローの切り替え)（(switch workflow)）] をクリックして [ユーザ アクティビティ（User Activity）] を選択します。

ヒント イベントが表示されない場合は、時間範囲の調整が必要な可能性があります（時間枠の変更 （2956 ページ）を参照）。

ステップ 2 次の選択肢があります。

- [(ワークフローの切り替え)（(switch workflow)）] をクリックしてカスタム ワークフローを含む別のワークフローを使用します。

- 基本的なワークフロー操作を実行します（ディスカバリおよびアイデンティティ ワークフローの使用（3199 ページ）を参照）。
- テーブルのカラムの内容について詳しく調べます（ユーザ関連フィールド（3245 ページ）を参照）。

ユーザ プロファイルとホスト履歴

特定のユーザの詳細については、[ユーザ（User）]ポップアップ ウィンドウを表示して確認することができます。表示されるページ（このマニュアルでは「ユーザプロファイル」と呼んでいます）には、Web インターフェイスで「ユーザのアイデンティティ（User Identity）」というタイトルが付いています。

このウィンドウは、次のビューから表示できます。

- ユーザ データを他の種類のイベントに関連付けるすべてのイベント ビュー
- アクティブなセッションのテーブル ビュー
- ユーザのテーブル ビュー

ユーザ情報は、ユーザ ワークフローの最終ページにも表示されます。

表示されるユーザ データは、ユーザのテーブル ビューで表示されるものと同じです。

[侵害の兆候（Indications of Compromise）] セクション

このセクションについては、次のセクションを参照してください。

- 侵害の兆候 （2666 ページ）
- 侵害の兆候データ フィールド （3224 ページ）
- 単一ホストまたはユーザにおける侵害の兆候のルール状態の編集 （3225 ページ）
- 侵害の兆候タグの解決 （3226 ページ）
- 侵害の兆候のタグのソース イベントの表示 （3225 ページ）

[ホストの履歴（Host History）] セクション

ホストの履歴には、過去 24 時間のユーザ アクティビティがグラフィック表示されます。ユーザがログインおよびログオフしたホストの IP アドレスのリストは、ログインとログアウトの回数の概数を棒グラフで示します。一般的なユーザは、1 日の間に複数のホストに対してログオンおよびログオフする可能性があります。たとえば、メール サーバに対する定期的な自動ログインは複数回の短時間のセッションとして示されますが、（勤務時間中などの）長時間のログインは、長時間のセッションとして示されます。

トラフィック ベースの検出またはキャプティブ ポータルを使用して失敗したログインをキャプチャした場合、ホストの履歴にはユーザがログインに失敗したホストも含まれます。

ホストの履歴を生成するために使用されるデータは、ユーザの履歴データベースに格納されます。このデータベースには、デフォルトで 1000 万のユーザ ログイン イベントが格納されま

す。ホストの履歴に特定のユーザに関するデータが表示されない場合、そのユーザが非アクティブであるか、またはデータベースの制限を増やさなければならないことがあります。

関連トピック

ユーザ データのフィールド

ユーザの詳細およびホスト履歴の表示

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Any Security Analyst

以下の 2 つの対処法があります。

- ユーザをリストする任意のイベント ビューで、ユーザ ID の横に表示されるユーザ アイコン（  または、侵入の痕跡に関連付けられているユーザ  ）をクリックします。
- いずれかのユーザ ワークフローで、[ユーザ（Users）] の最終ページをクリックします。

第 130 章

相関イベントとコンプライアンス イベント

次のトピックでは、相関イベントとコンプライアンスイベントを表示する方法について説明します。

相関イベントの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Any Security Analyst

アクティブな相関ポリシーに含まれる相関ルールがトリガーとして使用されると、システムが相関イベントを生成してデータベースにそれを記録します。

（注） アクティブな相関ポリシーに含まれるコンプライアンス ホワイトリストがトリガーとして使用されると、システムがホワイトリスト イベントを生成します。

相関イベントのテーブルを表示し、検索対象の情報に応じてイベント ビューを操作できます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

相関イベントにアクセスしたときに表示されるページは、使用するワークフローによって異なります。相関イベントのテーブル ビューが含まれる定義済みワークフローを使用できます。また、特定のニーズを満たす情報だけを表示するカスタム ワークフローを作成することもできます。

ステップ 1 **[Analysis]** > **[Correlation]** > **[Correlation Events]**を選択します。

オプションで、カスタム ワークフローなど、別のワークフローを使用するには、ワークフローのタイトルの横の [(ワークフローの切り替え)（(switch workflow)）] をクリックします。

ヒント 相関イベントのテーブル ビューが含まれないカスタム ワークフローを使用している場合は、[(ワークフローの切り替え)（(switch workflow)）] をクリックし、[相関イベント（Correlation Events）] を選択します。

ステップ 2 オプションで、時間枠の変更 （2956 ページ）の説明に従って、時間範囲を調整します。

ステップ 3 次のいずれかの操作を実行します。

- 表示されるカラムの詳細については、相関イベントのフィールド（3267ページ）を参照してください。
- IP アドレスのホスト プロファイルを表示するには、IP アドレスの横に表示されるホスト プロファイル アイコンをクリックします。
- To view user identity information, click the user icon that appears next to the user identity ( , or for users associated with IOCs, ).
- 現在のワークフロー ページ内でイベントをソートしたり制限したり、または移動するには、ワークフローの使用 （2931 ページ）を参照してください。
- 現在の制約を維持しながら現在のワークフローのページ間で移動するには、ワークフロー ページの左上にある該当するページ リンクをクリックします。
- 特定の値に制限して、ワークフロー内の次のページにドリルダウンするには、ドリルダウン ページの使用 （2940 ページ）を参照してください。
- 一部またはすべての相関イベントを削除するには、削除するイベントの横にあるチェックボックスをオンにして [削除（Delete）] をクリックするか、[すべて削除（Delete All）] をクリックして現在の制約されているビューにあるすべてのイベントを削除することを確認します。
- 他のイベント ビューに移動して関連イベントを表示するには、ワークフロー間のナビゲーション （2963 ページ）を参照してください。
- （所属する組織でイベント データを外部の Firepower システムに保存している場合）パケットや履歴データなど、イベントに関連する情報を調査するには、イベントの値を右クリックします。表示されるオプションは、データタイプやシステムに設定されている統合によって異なります。詳細については、を使用したイベント調査 Cisco Security Packet Analyzer （2882 ページ）およびWeb ベースのリソースを使用したイベントの調査 （2890 ページ）を参照してください。
- イベントに関するインテリジェンスを収集するには、テーブルでイベントの値を右クリックして、シスコまたはサードパーティのインテリジェンス ソースを選択します。たとえば、不審な IP アドレスに関する詳細情報を Cisco Talos から入手できます。表示されるオプションは、データタイプやシステム

に設定されている統合によって異なります。詳細については、「Web ベースのリソースを使用したイベントの調査 （2890 ページ）」を参照してください。

関連トピック

データベース イベント数の制限 （1264 ページ）
ワークフローのページ （2935 ページ）

相関イベントのフィールド

相関ルールがトリガーとして使用されると、システムは相関イベントを生成します。次の表では、表示および検索可能な相関イベント テーブルのフィールドについて説明します。

表 *350*：相関イベントのフィールド

フィールド	説明
Description	相関イベントについての説明。説明に示される情報は、ルールがどのようにトリガーとして使用されたかによって異なります。 たとえば、オペレーティング システム情報の更新イベントによってルールがトリガーとして使用された場合、新しいオペレーティング システムの名前と信頼度レベルが表示されます。
Device	ポリシー違反をトリガーとして使用したイベントを生成したデバイスの名前。
ドメイン（Domain）	ポリシー違反をトリガーとして使用したモニタ対象トラフィックのデバイスのドメイン。 This field is only present if you have ever configured the Firepower Management Center for multitenancy.
影響（Impact）	侵入データ、ディスカバリ データ、および脆弱性情報の間の相関に基づいて相関イベントに割り当てられた影響レベル。 このフィールドを検索する場合、大文字と小文字を区別しない有効な値は、`Impact 0`、`Impact Level 0`、`Impact 1`、`Impact Level 1`、`Impact 2`、`Impact Level 2`、`Impact 3`、`Impact Level 3`、`Impact 4`、および `Impact Level 4` です。影響アイコンの色または部分文字列は使用しないでください（たとえば、`blue`、`level 1`、または `0` を使用しないでください）。
入力インターフェイス（Ingress Interface）または出力インターフェイス（Egress Interface）	ポリシー違反をトリガーとして使用した侵入イベントまたは接続イベントの入力または出力インターフェイス。

フィールド	説明
入力セキュリティ ゾーン（Ingress Security Zone）または出力セキュリティ ゾーン（Egress Security Zone）	ポリシー違反をトリガーとして使用した侵入イベントまたは接続イベントの入力または出力セキュリティ ゾーン。
インライン結果（Inline Result）	次のいずれか： • 黒の下矢印：侵入ルールをトリガーとして使用したパケットがシステムによってドロップされたことを示します • グレーの下矢印：侵入ポリシー オプション [Drop when Inline] を有効にした場合、インライン型、スイッチ型、またはルーティング型展開でパケットがシステムによってドロップされたと想定されることを示します • 空白：トリガーとして使用された侵入ルールが [ドロップしてイベントを生成する（Drop and Generate Events）] に設定されていなかったことを示します 侵入イベントによってトリガーとして使用されたポリシー違反を検索するためにこのフィールドを使用する場合は、次のいずれかを入力します。 • `dropped` は、インライン型、スイッチ型、またはルーティング型展開でパケットがドロップされたかどうかを示します。 • would have dropped は仮定を表します。インライン型、スイッチ型、またはルーティング型展開でパケットをドロップするよう侵入ポリシーが設定されていると仮定した場合、パケットがドロップされるかどうかを示します。 侵入ポリシーのドロップ動作やルール状態とは無関係に、パッシブ展開（インライン セットがタップ モードである場合を含む）ではシステムがパケットをドロップしないことに注意してください。
ポリシー	違反が発生したポリシーの名前。
[プライオリティ（Priority）]	相関イベントのプライオリティ。これは、トリガーとして使用されたルールのプライオリティまたは違反が発生した相関ポリシーのプライオリティによって決まります。このフィールドを検索するとき、プライオリティなしの場合は `none` を入力します。
ルール（Rule）	ポリシー違反をトリガーとして使用したルールの名前。

フィールド	説明
セキュリティ インテリジェンス カテゴリ（Security Intelligence Category）	ブラックリスト化されたオブジェクトの名前。これは、ポリシー違反をトリガーとして使用したイベントでブラックリスト化された IP アドレスを示す（またはその IP アドレスを含む）オブジェクトです。 このフィールドを検索する場合は、ポリシー違反をトリガーとして使用した相関イベントに関連付けられたセキュリティインテリジェンスのカテゴリを指定します。セキュリティインテリジェンスのカテゴリとして、セキュリティインテリジェンス オブジェクト、グローバル ブラックリスト、カスタム セキュリティ インテリジェンス リストまたはフィード、あるいはインテリジェンス フィードに含まれるいずれかのカテゴリを指定できます。
送信元の大陸（Source Continent）または宛先の大陸（Destination Continent）	ポリシー違反をトリガーとして使用したイベントの送信元または宛先ホスト IP アドレスに関連付けられた大陸。
送信元の国（Source Country）または宛先の国（Destination Country）	ポリシー違反をトリガーとして使用したイベントの送信元または宛先 IP アドレスに関連付けられた国。
送信元ホストの重大度（Source Host Criticality）または宛先ホストの重大度（Destination Host Criticality）	相関イベントに関連する送信元または宛先ホストにユーザが割り当てたホスト重要度。`None`、`Low`、`Medium`、または `High` のいずれかです。 ディスカバリ イベント、ホスト入力イベント、または接続イベントに基づくルールによって生成された相関イベントにのみ、送信元ホスト重要度が含まれることに注意してください。
送信元 IP（Source IP）または宛先 IP（Destination IP）	ポリシー違反をトリガーとして使用したイベントの送信元または宛先ホストの IP アドレス。
送信元ポート/ICMP タイプ（Source Port/ICMP Type）または宛先ポート/ICMP コード（Destination Port/ICMP Code）	ポリシー違反をトリガーとして使用したイベントに関連付けられた、送信元トラフィックの送信元ポート/ICMP タイプまたは宛先トラフィックの宛先ポート/ICMP コード。
送信元ユーザ（Source User）または宛先ユーザ（Destination User）	ポリシー違反をトリガーとして使用したイベントの送信元または宛先ホストにログインしたユーザの名前。
時刻（Time）	相関イベントが生成された日時。このフィールドは検索できません。
メンバー数（Count）	各行に表示された情報と一致するイベントの数。[カウント（Count）]フィールドは、複数の同一行が生成される制限を適用した後でのみ表示されることに注意してください。このフィールドは検索できません

関連トピック

イベントの検索 （2967 ページ）

コンプライアンス ホワイト リスト ワークフローの使用

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Any Security Analyst/Discovery Admin

Firepower Management Center は、ネットワークで生成されるホワイト リスト イベントおよびホワイト リスト違反の分析で使用できるワークフローセットを提供します。ワークフローはネットワーク マップやダッシュボードとともに、ネットワーク資産のコンプライアンスに関する主要な情報源になります。

システムは、ホワイト リスト イベントとホワイト リスト違反のために事前定義されたワークフローを提供します。ユーザはカスタム ワークフローを作成することもできます。コンプライアンス ホワイト リスト ワークフローを使用すると、多くの一般的なアクションを実行できます。

ステップ 1 **[分析（Analysis）] > [相関（Correlation）]** メニューを使用してホワイト リスト ワークフローにアクセスします。

ステップ 2 次の選択肢があります。

- ワークフローの切り替え：カスタム ワークフローなどの別のワークフローを使用するには、[(ワークフローの切り替え)（(switch workflow)）] をクリックします。
- 時間範囲：時間範囲を調整（イベントが表示されない場合に役立ちます）する方法については、時間枠の変更 （2956 ページ）を参照してください。
- ホスト プロファイル：IP アドレスのホスト プロファイルを表示するには、ホスト プロファイルのアイコン（  ）をクリックします。アクティブな侵害の兆候（IOC）タグのあるホストの場合は、IP アドレスの横に表示される侵害されたホストのアイコン（  ）をクリックします。
- ユーザ プロファイル（イベントのみ）：To view user identity information, click the user icon that appears next to the user identity ( , or for users associated with IOCs, ).
- 制約：表示されるカラムを制約にするには、非表示にするカラムの見出しにある閉じるアイコン（  ）をクリックします。表示されるポップアップ ウィンドウで、[適用（Apply）] をクリックします。

ヒント 他のカラムを表示または非表示にするには、[適用（Apply）]をクリックする前に、該当するチェック ボックスをオンまたはオフにします。無効になったカラムをビューに再び追加するには、検索制約を展開し、[無効にされたカラム（Disabled Columns）] の下のカラム名をクリックします。

- ドリル ダウン：ドリルダウン ページの使用 （2940 ページ）を参照してください。
- ソート：ワークフローでデータをソートするには、カラムのタイトルをクリックします。ソート順を逆にするには、カラムのタイトルをもう一度クリックします。
- このページに移動する：ワークフロー ページのトラバーサル ツール （2937 ページ）を参照してください。
- ページ間で移動する：現在の制約を維持しながら現在のワークフローのページ間で移動するには、ワークフロー ページの左上にある該当するページ リンクをクリックします。
- イベント ビュー間で移動する：関連するイベントを表示するためその他のイベント ビューに移動するには、[ジャンプ（Jump to）] をクリックし、ドロップダウン リストからイベント ビューを選択します。
- イベントの削除（イベントのみ）：現在の制約されているビューにある一部またはすべての項目を削除するには、削除する項目の横にあるチェックボックスをオンにし、[削除（Delete）] または [すべて削除（Delete All）] をクリックします。

関連トピック

ワークフローのページ （2935 ページ）
イベント ビュー設定の設定 （43 ページ）

ホワイトリスト イベントの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Any Security Analyst/Discovery Admin

最初の評価が行われた後、監視対象ホストがアクティブなホワイト リストに準拠しなくなると、システムはホワイト リスト イベントを生成します。ホワイト リスト イベントは、相関イベントの特殊な形態で、FMC 相関イベント データベースに記録されます。

Firepower Management Center を使用して、コンプライアンス ホワイト リスト イベントのテーブルを表示できます。ここでユーザは、検索する情報に応じてイベント ビューを操作することができます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

ホワイト リスト イベントにアクセスしたときに表示されるページは、使用しているワークフローによって異なります。イベントのテーブル ビューで終わる事前定義されたワークフローを使用できます。また、特定のニーズを満たす情報だけを表示するカスタム ワークフローを作成することもできます。

ステップ 1 **[Analysis]** > **[Correlation]** > **[White List Events]**を選択します。

ステップ 2 次の選択肢があります。

- 基本的なワークフロー操作を実行するには、コンプライアンス ホワイト リスト ワークフローの使用（3270 ページ）を参照してください。
- テーブルのカラムの内容について詳しく調べるには、ホワイト リスト イベントのフィールド（3272 ページ）を参照してください。
- その他のオプションを表示するには、テーブル内の値を右クリックします。

ホワイト リスト イベントのフィールド

ワークフローを使用して表示および検索できるホワイト リスト イベントには、次のフィールドがあります。

Device

ホワイト リスト違反を検出した管理対象デバイスの名前。

説明

ホワイト リスト違反の説明。次に例を示します。

```
Client “AOL Instant Messenger” is not allowed.
```

アプリケーション プロトコルに関係する違反は、アプリケーション プロトコルの名前とバージョンだけでなく、それが使用しているポートとプロトコル（TCP または UDP）も示します。禁止を特定のオペレーティング システムに限定する場合は、説明にオペレーティング システム名が含まれます。次に例を示します。

```
Server "ssh / 22 TCP (OpenSSH 3.6.1p2)" is not allowed on Operating
System “Linux Linux 2.4 or 2.6”.
```

ドメイン（Domain）

ホワイト リストに準拠しなくなったホストのドメイン。 This field is only present if you have ever configured the Firepower Management Center for multitenancy.

ホストの重要度（Host Criticality）

ホワイトリストに準拠していないホストに対してユーザが割り当てた重要度（[なし（None）]、[低（Low）]、[中（Medium）]、または [高（High）]）。

[IPアドレス（IP Address）]

ホワイト リストに準拠しなくなったホストの IP アドレス。

ポリシー

違反した相関ポリシー、つまりホワイト リストを含む相関ポリシーの名前。

[ポート（Port）]

アプリケーション プロトコル ホワイト リスト違反（非準拠アプリケーション プロトコルの結果として発生した違反）をトリガーした検出イベントに関連付けられているポート（存在する場合）。他のタイプのホワイト リスト違反の場合、このフィールドは空白です。

[プライオリティ（Priority）]

ポリシーまたはポリシー違反をトリガーしたホワイト リストに指定されている優先度。これは、相関ポリシー内のホワイトリストの優先度または相関ポリシー自体の優先度によって決まります。ホワイトリストの優先度は、そのポリシーの優先度より優先されることに注意してください。このフィールドを検索するとき、プライオリティなしの場合は `none` を入力します。

時刻（Time）

ホワイト リスト イベントが生成された日時。このフィールドは検索できません。

ユーザ（User）

ホワイト リストに準拠しなくなったホストにログインしている既知のユーザのアイデンティティ。

ホワイト リスト（White List）

ホワイト リストの名前。

メンバー数（Count）

各行に表示された情報と一致するイベントの数。[カウント（Count）] フィールドは、複数の同一行が生成される制限を適用した後でのみ表示されることに注意してください。このフィールドは検索できません。

ホワイトリスト違反の表示

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Any Security Analyst/Discovery Admin

システムは、ネットワークの現在のホワイトリスト違反のレコードを保持します。違反はそれぞれ、ホストのいずれかで実行することが禁止されている事柄を表します。ホストが準拠するようになると、システムは、修正された違反をデータベースから削除します。

Firepower Management Center を使用して、アクティブなすべてのホワイトリストに対するホワイトリスト違反のテーブルを表示できます。ここでユーザは、検索する情報に応じてイベントビューを操作することができます。

ホワイトリスト違反にアクセスしたときに表示されるページは使用しているワークフローによって異なります。事前定義されたワークフローはホストビューで終了しますが、このホストビューには、制約を満たすすべてのホストに対して1つずつホストプロファイルが含まれています。また、特定のニーズを満たす情報だけを表示するカスタムワークフローを作成することもできます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

ステップ1 **[Analysis]** > **[Correlation]** > **[White List Violations]**を選択します。

ステップ2 次の選択肢があります。

- 基本的なワークフロー操作を実行するには、コンプライアンス ホワイト リスト ワークフローの使用（3270 ページ）を参照してください。
- テーブルのカラムの内容について詳しく調べるには、ホワイトリスト違反のフィールド（3274ページ）を参照してください。
- その他のオプションを表示するには、テーブル内の値を右クリックします。

ホワイト リスト違反のフィールド

ワークフローを使用して表示および検索できるホワイトリスト違反には、次のフィールドがあります。

ドメイン

非準拠ホストが存在するドメイン。 This field is only present if you have ever configured the Firepower Management Center for multitenancy.

情報

ホワイトリスト違反に関連付けられたすべての利用可能なベンダー、製品、またはバージョン情報。ホワイトリストに違反するプロトコルの場合、このフィールドには、違反の原因がネットワーク プロトコルとトランスポート プロトコルのどちらであるのかも示されます。

[IPアドレス（IP Address）]

非準拠ホストの IP アドレス。

[ポート（Port）]

アプリケーション プロトコル ホワイト リスト違反（非準拠アプリケーション プロトコルの結果として発生した違反）をトリガーしたイベントに関連付けられたポート（存在する場合）他のタイプのホワイト リスト違反の場合、このフィールドは空白です。

Protocol

アプリケーション プロトコル ホワイト リスト違反（非準拠アプリケーション プロトコルの結果として発生した違反）をトリガーしたイベントに関連付けられたプロトコル（存在する場合）他のタイプのホワイト リスト違反の場合、このフィールドは空白です。

時刻（Time）

ホワイト リスト違反が検出された日時。

タイプ（Type）

ホワイト リスト違反のタイプ、つまり、非準拠の結果として違反が発生したかどうか。

- オペレーティング システム（os）（このフィールドを検索する場合は、**os** または **operating system** と入力してください）。
- アプリケーション プロトコル（サーバ）
- クライアント
- プロトコル
- Web アプリケーション（web）（このフィールドを検索する場合は、**web application** と入力してください）。

ホワイト リスト（White List）

違反されたホワイト リストの名前。

Count

各行に表示された情報と一致するイベントの数。[カウント（Count）] フィールドは、複数の同一行が生成される制限を適用した後でのみ表示されることに注意してください。このフィールドは検索できません。

修復ステータス イベント

修復がトリガーされると、システムは修復ステータス イベントをデータベースに記録します。これらのイベントは、[修復ステータス（Remediation Status）] ページで確認できます。修復ステータス イベントを検索、表示、削除できます。

関連トピック

修復ステータスのテーブル フィールド （3277 ページ）

修復ステータス イベントの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin

修復ステータス イベントにアクセスするときに表示されるページは、使用するワークフローにより異なります。修復のテーブル ビューを含む定義済みワークフローを使用できます。テーブル ビューには、各修復ステータス イベントの行が含まれます。また、特定のニーズを満たす情報だけを表示するカスタム ワークフローを作成することもできます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

ステップ 1 **[Analysis]** > **[Correlation]** > **[Status]**を選択します。

ステップ 2 オプションで、時間枠の変更 （2956 ページ）の説明に従って、時間範囲を調整します。

ステップ 3 オプションで、カスタム ワークフローなど、別のワークフローを使用するには、ワークフローのタイトルの横の [(ワークフローの切り替え)（(switch workflow)）] をクリックします。

ヒント 修復のテーブル ビューが含まれないカスタム ワークフローを使用する場合、ワークフローのタイトルの横の [(ワークフローの切り替え)（(switch workflow)）] メニューをクリックし、[修復ステータス（Remediation Status）] を選択します。

ステップ 4 次の選択肢があります。

- 表示されるカラムの詳細については、修復ステータスのテーブル フィールド （3277 ページ）を参照してください。
- イベントをソートしたり、制約したりするには、ワークフローの使用 （2931 ページ）を参照してください。

- 相関イベント ビューに移動し関連するイベントを確認するには、[相関イベント（Correlation Events）] をクリックします。
- 現在のページにすぐに戻れるようにページをブックマークするには、[このページをブックマーク（Bookmark This Page）] をクリックします。ブックマークの管理ページに移動するには、[ブックマークの表示（View Bookmarks）] をクリックします。
- テーブル ビューのデータに基づいてレポートを生成するには、イベント ビューからのレポート テンプレートの作成 （2780 ページ） で説明されているように、[レポート デザイナ（Report Designer）] をクリックします。
- ワークフローの次のページにドリルダウンするには、ドリルダウン ページの使用 （2940 ページ）を参照してください。
- システムから修復ステータス イベントを削除するには、削除するイベントの横にあるチェックボックスをオンにして [削除（Delete）] をクリックするか、[すべて削除（Delete All）] をクリックして現在の制約されているビューにあるすべてのイベントを削除することを確認します。
- 修復ステータス イベントを検索するには、[検索（Search）] をクリックします。

関連トピック

ワークフローの使用 （2931 ページ）

修復ステータスのテーブル フィールド

次の表に、表示および検索できる修復のステート テーブルのフィールドを示します。

表 *351* : 修復ステータス フィールド

フィールド	説明
ドメイン（Domain）	監視対象のトラフィックがポリシー違反をトリガーとして使用し、次に修復をトリガーとして使用するデバイスのドメイン。 This field is only present if you have ever configured the Firepower Management Center for multitenancy.
ポリシー	違反し、修復をトリガーとして使用した相関ポリシーの名前。
Remediation Name	起動された修復の名前。

フィールド	説明
Result Message	修復の起動時に発生した事象を説明するメッセージ。ステータス メッセージには以下が含まれます。 • Successful completion of remediation • Error in the input provided to the remediation module • Error in the remediation module configuration • Error logging into the remote device or server • Unable to gain required privileges on remote device or server • Timeout logging into remote device or server • Timeout executing remote commands or servers • The remote device or server was unreachable • The remediation was attempted but failed • Failed to execute remediation program • Unknown/unexpected error カスタム修復モジュールがインストールされている場合、カスタム モジュールによって実装される追加のステータス メッセージが表示される場合があります。
ルール（Rule）	修復をトリガーとして使用したルールの名前。
時刻（Time）	Firepower Management Centerが修復を起動した日付と時刻。
Count	各行に表示された情報と一致するイベントの数。[カウント（Count）]フィールドは、複数の同一行が生成される制限を適用した後でのみ表示されることに注意してください。このフィールドは検索できません。

関連トピック

イベントの検索 （2967 ページ）

修復ステータス イベント テーブルの使用

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin

イベント ビューのレイアウトを変更したり、ビュー内のイベントをフィールド値で制限したりできます。

カラムを無効にすると、そのカラムは（後で元に戻さない限り）そのセッションの期間中は無効になります。最初のカラムを無効にすると、[カウント（Count）] カラムが追加されます。

テーブル ビューの行内の値をクリックすると、テーブル ビューが制約されます（次のページにはドリルダウンされません）。

ヒント テーブル ビューでは、必ずページ名に「Table View」が含まれます。

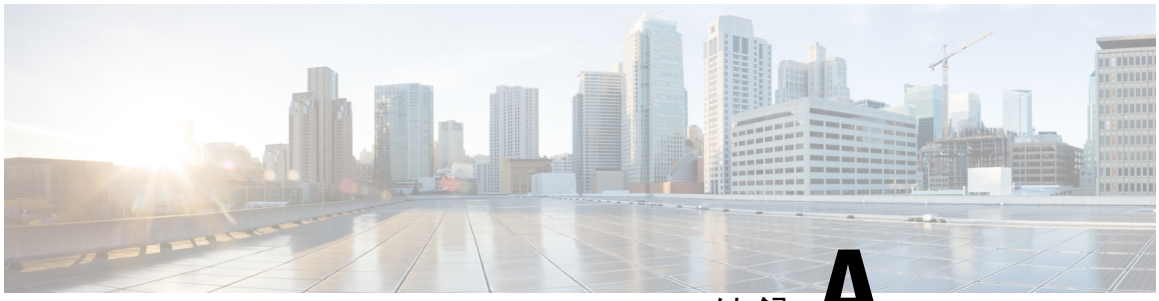
マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

ステップ 1 **[Analysis]** > **[Correlation]** > **[Status]**を選択します。

ヒント 修復のテーブル ビューが含まれないカスタム ワークフローを使用する場合、ワークフローのタイトルの横の [(ワークフローの切り替え)（(switch workflow)）] メニューをクリックし、[修復ステータス（Remediation Status）] を選択します。

ステップ 2 次の選択肢があります。

- 表示されるカラムの詳細については、修復ステータスのテーブル フィールド（3277 ページ）を参照してください。
- イベントをソートしたり、制約したりするには、ワークフローの使用（2931 ページ）を参照してください。



付録 A

セキュリティ、インターネットアクセス、および通信ポート

以下のトピックでは、システム セキュリティ、インターネット アクセス、および通信ポートに関する情報を提供します。

セキュリティ要件

Firepower Management Centerを保護するには、保護された内部ネットワークにそれをインストールしてください。FMCは必要なサービスとポートだけを使用するよう設定されますが、ファイアウォール外部からの攻撃がそこまで（または管理対象デバイスまで）決して到達できないようにする必要があります。

FMCとその管理対象デバイスが同じネットワーク上に存在する場合、FMCと同じ保護された内部ネットワークにデバイス上の管理インターフェイスを接続できます。これにより、FMCからデバイスを安全に制御することができます。また、他のネットワーク上のデバイスからのトラフィックを FMC で管理および分離できるように、複数の管理インターフェイスを設定することもできます。

アプライアンスの展開方法に関係なく、アプライアンス間通信は暗号化されます。それでも、分散型サービス拒否（DDoS）や中間者攻撃などの手段でアプライアンス間の通信が中断、ブロック、または改ざんされないよう何らかの対策を講じる必要があります。

インターネット アクセス要件

デフォルトでは、Firepower アプライアンスはポート 443/tcp（HTTPS）および 80/tcp（HTTP）でインターネットに接続するように設定されています。アプライアンスがインターネットに直接アクセスしないようにするには、プロキシ サーバを設定できます。

セキュリティ、インターネット アクセス、および通信ポート

ほとんどの場合、インターネットにアクセスするのはFirepower Management Centerです。ただし、管理対象デバイスがインターネットにアクセスする場合もあります。たとえば、マルウェア保護設定で動的分析を使用する場合、管理対象デバイスはファイルを直接Cisco Threat Gridクラウドに送信します。または、外部NTPサーバにデバイスを同期することができます。

さらに、Web分析トラッキングを無効にした場合を除き、ブラウザはGoogle Web分析サーバに連絡し、個人を特定可能でない使用状況データをCiscoに送信することができます。

ヒント ネットワーク向けAMPまたはエンドポイント向けAMPを使用中の場合、ロケーションによってFMCがアクセスするAMPクラウドリソースが決定されます。「AMPの適切な操作のために必要なサーバアドレス」トラブルシューティングテクニカルノートには、Firepowerアプライアンスだけでなく、コネクタやプライベートクラウドアプライアンスなどのCisco AMPコンポーネントでも必要なインターネットリソース（静的IPアドレスを含む）を一覧表示します。

高可用性ペアのFMCの両方にインターネットアクセスがある必要があります。機能に応じて、両方のピアがインターネットにアクセスすることも、アクティブピアのみがインターネットにアクセスすることもあります。

表 *352 : Firepower* のインターネット アクセス要件

機能	理由（Reason）	FMCハイ アベイラビリティ	リソース
ネットワーク向けAMP	マルウェアクラウドルックアップ。	両方のピアが検索を実行します。	この表の上に記載の重要なヒントを参照してください。 cloud-sa.amp.cisco.com cloud-sa.eu.amp.cisco.com cloud-sa.apjc.amp.cisco.com cloud-sa-589592150.us-east-1.elb.amazonaws.com
	ファイル事前分類とローカルのマルウェア分析のシグニチャ更新をダウンロードします。	アクティブピアでダウンロードが実行され、スタンバイへ同期します。	updates.vrt.sourcefire.com amp.updates.vrt.sourcefire.com
	動的分析（管理対象デバイス）のファイルを送信します。 動的分析結果のクエリ（FMC）。	両方のピアが動的分析レポートのクエリを実行します。	fmc.api.threatgrid.com fmc.api.threatgrid.eu

セキュリティ、インターネット アクセス、および通信ポート

機能	理由（Reason）	FMCハイ アベイラビリティ	リソース
AMP for Endpoint の統合	エンドポイント向け AMP によって検出されたマルウェア イベントを AMP クラウドから受信します。 Firepower システムによって検出されたマルウェア イベントを AMP for Endpoints で表示します。 AMP クラウドからの性質をオーバーライドするには、AMP for Endpoints で作成された一元的なファイル ブラックリストおよびホワイトリストを使用します。	両方のピアがイベントを受信します。 両方のピア（設定が同期されていない）でクラウド接続を設定する必要もあります。	https://www.cisco.com/c/en/us/support/docs/security/sourcefire-amp-appliances/118121-technote-sourcefire-00.html#anc5 で、Firepower に関する情報を参照してください。 この表の上に記載の重要なヒントも参照してください。
セキュリティ インテリジェンス	セキュリティ インテリジェンス フィードをダウンロードします。	アクティブ ピアでダウンロードが実行され、スタンバイへ同期します。	intelligence.sourcefire.com
URL フィルタリング	URL カテゴリおよびレピュテーション データをダウンロードします。 URL カテゴリおよびレピュテーション データを手動でクエリ（ルックアップ）します。 未分類 URL のクエリ。	アクティブ FMC でダウンロードが実行され、スタンバイへ同期します。	database.brightcloud.com service.brightcloud.com
Cisco Smart Licensing	Cisco Smart Software Manager と通信します。	アクティブなピアが通信します。	tools.cisco.com www.cisco.com
Cisco Success Network	使用状況情報および統計情報を送信します。	アクティブなピアが通信します。	api-sse.cisco.com:8989
システムの更新プログラム	更新プログラムを Cisco から直接 FMC にダウンロードします。 • システム ソフトウェア • 侵入ルール • 脆弱性データベース（VDB） • 位置情報データベース（GeoDB）	侵入ルール、VDB、および GeoDB をアクティブなピアで更新し、アクティブなピアはその後スタンバイへ同期します。 各ピアで個別にシステム ソフトウェアをアップグレードします。Cisco Firepower Management Center Upgrade Guide を参照してください。	cisco.com sourcefire.com

機能	理由（Reason）	FMCハイ アベイラビリティ	リソース
時刻の同期	展開内で時間を同期します。 プロキシサーバではサポートされません。	外部 NTP サーバを使用するアプライアンスはインターネットにアクセスできる必要があります。	0.sourcefire.pool.ntp.org 1.sourcefire.pool.ntp.org 2.sourcefire.pool.ntp.org 3.sourcefire.pool.ntp.org
RSS フィード	ダッシュ ボードで Cisco 脅威調査ブログを表示します。	RSS フィードを表示するアプライアンスはインターネットにアクセスできる必要があります。	blogs.cisco.com/talos cloud.google.com
[Whois]	外部ホストの whois 情報を要求します。 プロキシサーバではサポートされません。	whois 情報を要求するすべてのアプライアンスがインターネットにアクセスできる必要があります。	whois クライアントは、クエリ対象の適切なサーバの推測を試みます。推測できない場合、次を使用します。 • NIC ハンドル：whois.networksolutions.com • IPv4 アドレスとネットワーク名：whois.arin.net

通信ポートの要件

Firepower アプライアンスはポート 8305/tcp 上の双方向 SSL 暗号化通信チャネルを使用して通信します。このポートは、基本的なプラットフォーム内通信のためにオープンの状態で保持する必要があります。

他のポートでは、特定の機能に必要な外部リソースへのアクセスとともにセキュアな管理をすることができます。一般に、機能関連のポートは、該当する機能を有効化または設定する時点まで、閉じたままになります。開いたポートを閉じると展開にどのような影響が及ぶか理解するまでは、開いたポートを変更したり閉じたりしないでください。

表 *353 : Firepower* 通信ポートの要件

ポート	プロトコル/機能	プラットフォーム	方向	詳細
7/UDP	UDP/監査ロギング	FMC、クラシック	発信	監査ロギングの設定時の syslog サーバとの接続を確認します。
22/tcp	SSH	FMC あらゆるデバイス	着信	アプライアンスへのリモート接続を保護します。
25/tcp	SMTP	FMC	発信	電子メール通知とアラートを送信。

セキュリティ、インターネット アクセス、および通信ポート

ポート	プロトコル/機能	プラットフォーム	方向	詳細
53/tcp 53/udp	DNS	FMC あらゆるデバイス	発信	DNS 用です。
67/udp 68/udp	DHCP	FMC あらゆるデバイス	発信	DHCP 用です。
80/tcp	HTTP	FMC 7000 & 8000 シリーズ	発信	RSS フィードをダッシュ ボードに表示します。
80/tcp	HTTP	FMC	発信	URL カテゴリおよびレピュテーション データをダウンロードまたはクエリします（さらにポート 443 も必要）。
80/tcp	HTTP	FMC	発信	HTTP 経由でカスタム セキュリティ インテリジェンス フィードをダウンロードします。
123/udp	NTP	FMC あらゆるデバイス	発信	時刻を同期します。
161/udp	SNMP	FMC あらゆるデバイス	着信	SNMP ポーリング経由で MIB にアクセスできるようにします。
162/udp	SNMP	FMC あらゆるデバイス	発信	リモート トラップ サーバに SNMP アラートを送信します。
389/tcp 636/tcp	LDAP	FMC FTD 7000 & 8000 シリーズ	発信	外部認証用に LDAP サーバと通信します。 検出された LDAP ユーザに関するメタデータを取得します（FMC のみ）。 設定可能。
443/tcp	HTTPS	FMC 7000 & 8000 シリーズ	着信	Web インターフェイスにアクセスします。
443/tcp	リモート アクセス VPN（SSL/IPSec）	FTD	着信	リモート ユーザからネットワークへのセキュアな VPN 接続を許可します。
500/udp 4500/udp	リモート アクセス VPN（IKEv2）	FTD	着信	リモート ユーザからネットワークへのセキュアな VPN 接続を許可します。

セキュリティ、インターネット アクセス、および通信ポート

ポート	プロトコル/機能	プラットフォーム	方向	詳細
443/tcp	HTTPS	FMC FTD	着信	Cisco Terminal Services（TS）エージェントを含め、Firepower REST API を使用して、統合製品やサードパーティ製品と通信します。
443/tcp	HTTPS	FMC	発信	クエリを Cisco Security Packet Analyzer に送信します。
443/tcp	HTTPS	FMC あらゆるデバイス	発信	インターネットからデータを送受信します。詳細は、インターネット アクセス要件 （3281 ページ）を参照してください。
443	HTTPS	FMC	発信	AMP クラウドとの通信（パブリックまたはプライベート） ポート 32137 の情報も参照してください。
443	HTTPS	FMC	着信および発信（Inbound and Outbound）	AMP for Endpoints との統合
514/udp	Syslog（アラート）	FMC あらゆるデバイス	発信	リモート syslog サーバにアラートを送信します。
623/udp	SOL/LOM	FMC 7000 & 8000 シリーズ	着信	Serial Over LAN（SOL）接続を使用した Lights-Out Management（LOM）。
885/tcp	キャプティブポータル	あらゆるデバイス	着信	キャプティブポータルのアイデンティティ ソースと通信します。
1500/tcp 2000/tcp	データベースアクセス	FMC	着信	サードパーティ クライアントによるイベント データベースへの読み取り専用アクセスを可能にします。
1812/udp 1813/udp	RADIUS	FMC FTD 7000 & 8000 シリーズ	発信	外部認証とアカウンティングのために RADIUS サーバと通信します。 設定可能。
3306/tcp	ユーザエージェント	FMC	着信	ユーザ エージェントと通信します。
5222/tcp	ISE	FMC	発信	ISE アイデンティティ ソースと通信します。

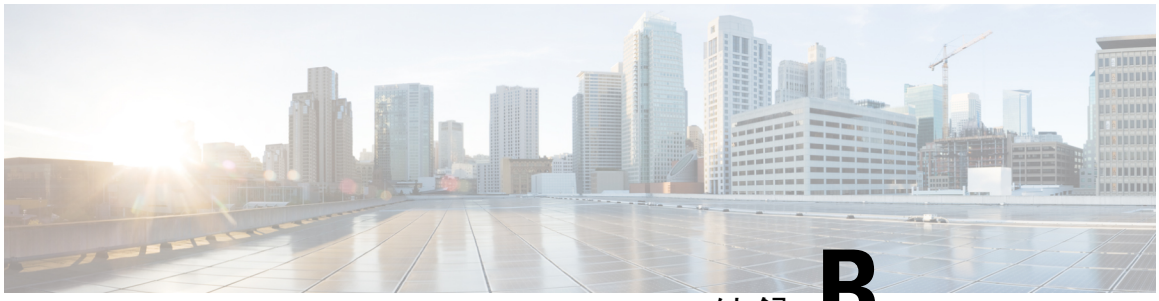
セキュリティ、インターネット アクセス、および通信ポート

ポート	プロトコル/機能	プラットフォーム	方向	詳細
6514/tcp	Syslog（監査イベント）	FMC 7000 & 8000 シリーズ NGIPSv ASA FirePOWER	発信	TLS の設定時にリモート syslog サーバに監査ログを送信します。
8302/tcp	eStreamer	FMC 7000 & 8000 シリーズ	着信	eStreamer クライアントと通信します。
8305/tcp	アプライアンス通信	FMC あらゆるデバイス	両方	展開におけるアプライアンス間で安全に通信します。 設定可能。このポートを変更する場合は、展開内のすべてのアプライアンスについて変更する必要があります。デフォルトを維持することをお勧めします。
8307/tcp	ホスト入力クライアント	FMC	着信	ホスト入力クライアントと通信します。
8989/tcp	Cisco Success Network	FMC	発信	使用状況情報および統計情報を送信します。
32137/tcp	ネットワーク向け AMP	FMC	発信	Cisco AMP クラウドと通信します。 これはレガシー設定です。デフォルト（443）を使用することをお勧めします。

関連トピック

LDAP 外部認証オブジェクトの追加 （64 ページ）
RADIUS 外部認証オブジェクトの追加 （72 ページ）

セキュリティ、インターネット アクセス、および通信ポート



付録 B

従来型デバイスのコマンド ライン リファレンス

従来型デバイスの CLI リファレンスは、次のアプライアンスに適用されます。

- 7000 および 8000 シリーズ
- ASA FirePOWER
- NGIPSv

その他の Firepower アプライアンスの場合：

- Firepower Threat Defense：Cisco Firepower Threat Defense コマンド リファレンスを参照してください。
- Firepower Management Center：Firepower Management Center のコマンド ライン リファレンス （3363 ページ）を参照してください。

クラシック デバイス CLI について

従来型デバイス（7000 および 8000 シリーズ、ASA FirePOWER、NGIPSv）に CLI を使用してログイン（7000/8000 シリーズ、ASA FirePOWER、および NGIPSv デバイスの CLI へのログイン （37ページ）を参照）すると、この付録で説明するコマンドを使用して、デバイスを表示、設定、およびトラブルシューティングすることができます。

（注） 7000 または 8000 シリーズ デバイスをリブートし、できるだけ早く CLI にログインしても、Web インターフェイスが使用できるようになるまで、実行するすべてのコマンドは監査ログに記録されません。

CLI コマンドでは大文字と小文字が区別されません。ただし、ユーザ名や検索フィルタなど、テキストが CLI フレームワークの一部ではないパラメータでは区別されるので注意してください。

関連トピック

Firepower システム ユーザ インターフェイス （28 ページ）

クラシック デバイス CLI モード

CLI には 4 つのモードが含まれています。デフォルト モードである CLI 管理には、CLI 自体の内部を移動するためのコマンドが含まれています。残りのモードには、クラッシック デバイス機能の 3 つの異なる領域に対処するコマンドが含まれています。これらのモード内のコマンドは、モード名: `system`、`show`、または `configure` で始まります。

モードを入力すると、CLI は、現在のモードを反映するように変更を求められます。たとえば、システム コンポーネントのバージョン情報を表示するには、標準 CLI プロンプトに完全なコマンドを入力します。

```
> show version
```

これまでに `show` モードに入ったことがある場合は、show モードの CLI プロンプトで `show` キーワードを使用せずにコマンドを入力できます。

```
show> version
```

クラシック デバイス CLI アクセス レベル

各モードで、ユーザが使用できるコマンドは、ユーザの CLI アクセスによって異なります。ユーザ アカウントを作成する場合は、手動で次のいずれかの CLI アクセス レベルに割り当てることができます。

- [基本（Basic）]：ユーザは読み取り専用のアクセス権を持ち、システム パフォーマンスに影響を与えるコマンドを実行することはできません。
- [設定（Configuration）]：ユーザは、読み取り/書き込みアクセス権があり、システム パフォーマンスに影響を与えるコマンドを実行することができます。
- [なし（None）]：ユーザは CLI にログインできません。

7000 および 8000 シリーズ デバイスでは、ローカル Web インターフェイスの [ユーザ管理（User Management）] ページでコマンド ラインの権限を割り当てることができます。NGIPSv と ASA FirePOWER では、CLI を使用してコマンド ラインの権限を割り当てます。

クラシック デバイス CLI 管理コマンド

CLI 管理コマンドを使用して、CLI とやりとりすることができます。これらのコマンドはデバイスの処理に影響しません。

configure password

現行のユーザは、自身のパスワードを変更することができます。コマンドを発行すると、CLI は現在の（古い）パスワードを入力するようユーザに要求し、その後で新しいパスワードを 2 回入力するよう要求します。

アクセス

Basic

構文

```
configure password
```

例

```
> configure password
Enter current password:
Enter new password:
Confirm new password:
```

exit

CLI コンテキストを、次に高い CLI コンテキスト レベルへ移動します。デフォルト モードからこのコマンドを発行すると、ユーザは現行の CLI セッションからログアウトします。これは、CLI コマンドの `logout` を発行するのと同じです。

アクセス

Basic

構文

```
exit
```

例

```
configure network ipv4> exit
configure network>
```

expert

Linux シェルを起動します。

注意 Cisco TAC またはユーザ マニュアルの明示的な手順による指示がない限り、Linux シェルを使用しないことを強くお勧めします。詳細については、Firepower システム ユーザ アカウント（25 ページ）を参照してください。

アクセス

Configuration

構文

```
expert
```

例

```
> expert
```

history

現行のセッションのコマンドラインの履歴を表示します。

アクセス

Basic

構文

```
history limit
```

ここで `limit` は履歴リストのサイズを設定します。サイズを無制限に設定するには、0 を入力します。

例

```
history 25
```

ログアウト

現行の CLI コンソール セッションから現行のユーザをログアウトします。

アクセス

Basic

構文

```
logout
```

例

```
> logout
```

? （疑問符）

CLI コマンドおよびパラメータの状況依存ヘルプを表示します。次のように、疑問符（?）のコマンドを使用します。

- 現在の CLI コンテキスト内で使用できるコマンドのヘルプを表示するには、コマンド プロンプトで疑問符（?）を入力します。
- 特定文字セットから始まる使用可能なコマンドのリストを表示するには、疑問符（?）に続けて短縮されたコマンドを入力します。
- コマンドの正式な引数のヘルプを表示するには、コマンドプロンプトの引数の代わりに疑問符（?）を入力します。

疑問符（?）は、コンソールにエコーバックされないことに注意してください。

アクセス

Basic

構文

```
?
abbreviated_command ?
command [arguments] ?
```

例

```
> ?
```

クラシック デバイス CLI show コマンド

Show コマンドは、デバイスの状態に関する情報を提供します。これらのコマンドはデバイスの動作モードを変更しません。また、これらのコマンドを実行しても、システムの動作に対する影響は最小限になります。ほとんどの show コマンドはすべての CLI ユーザが利用できますが、`show user` コマンドを発行できるのは、Configuration CLI アクセス権限を持つユーザのみです。

access-control-config

現在展開されている次のようなアクセス制御設定を表示します。

- セキュリティ インテリジェンスの設定
- アクセス コントロール ポリシーで呼び出されるあらゆるサブポリシーの名前
- 侵入変数セット データ
- ロギングの設定
- ポリシー レベルのパフォーマンス、前処理、全般設定などのその他の詳細設定

また、送信元と宛先ポートのデータ（ICMP エントリのタイプとコードを含む）および各アクセス コントロール ルールに一致する接続数（ヒット数）などの、ポリシーに関連する接続情報も表示します。

アクセス

Basic

構文

```
show access-control-config
```

例

```
> show access-control-config
```

alarms

デバイスで現在アクティブ（障害/停止）状態になっているハードウェアのアラームを表示します。このコマンドは NGIPSv および ASA FirePOWER デバイスでは使用できません。

アクセス

Basic

構文

```
show alarms
```

例

```
> show alarms
```

arp-tables

ネットワークに適用できる Address Resolution Protocol テーブルを表示します。このコマンドは NGIPSv および ASA FirePOWER では使用できません。

アクセス

Basic

構文

```
show arp-tables
```

例

```
> show arp-tables
```

audit-log

監査ログを時系列の逆順に表示します。最も新しい監査ログ イベントが先頭になります。

アクセス

Basic

構文

```
show audit-log
```

例

```
> show audit-log
```

audit_cert

現行の監査ログ クライアント証明書を表示します。

アクセス

Basic

構文

```
show audit_cert
```

例

```
> show audit_cert
```

bypass

7000 または 8000 シリーズ デバイスで、使用中のインライン セットを一覧表示し、それらのセットについて次のいずれかのバイパス モード ステータスを表示します。

- `armed`：インターフェイス ペアが、障害発生時にハードウェア バイパスになるように設定されている（[バイパス モード：バイパス（Bypass Mode: Bypass）]）か、または、**configure bypass close** コマンドを使用して強制的にフェールクローズされました。
- `engaged`：インターフェイス ペアが、オープンに失敗したか、または、**configure bypass open** コマンドを使用して強制的にハードウェア バイパスになりました。
- `off`：インターフェイス ペアは、フェールクローズに設定されています（**Bypass Mode: Non-Bypass**）。インターフェイス ペアで障害が発生した場合は、パケットがブロックされます。

アクセス

Basic

構文

```
show bypass
```

例

```
> show bypass
s1p1 ↔ s1p2: status 'armed'
s1p1 ↔ s1p2: status 'engaged'
```

High-availability コマンド

ハイ アベイラビリティの設定、ステータス、メンバー デバイスまたはスタックの情報を表示します。このコマンドは NGIPSv および ASA FirePOWER デバイスでは使用できません。

アクセス

基本

config

デバイスの高可用性の設定を表示します。

構文

```
show high-availability config
```

例

```
> show high-availability config
```

high-availability ha-statistics

高可用性ペアのデバイスの状態共有統計を表示します。

構文

```
show high-availability ha-statistics
```

例

```
> show high-availability ha-statistics
```

cpu

デバイス上のすべての CPU のプラットフォームに適合する現行の CPU の使用率の統計情報を表示します。

7000 および 8000 シリーズ デバイスでは、次の値が表示されます。

- CPU：プロセッサ番号。
- ロード：0 ～ 100 の数値で表される CPU 使用率。0 はロードされていない状態で、100 は完全にロードされたことを表します。

NGIPSv および ASA FirePOWER では、次の値が表示されます。

- CPU：プロセッサ番号。
- %user：ユーザ レベル（アプリケーション）で実行中に生じたCPU使用率の割合（パーセンテージ）。
- %nice：高い優先度のユーザ レベルで実行中に生じた CPU 使用率の割合（パーセンテージ）。
- %sys：システム レベル（カーネル）で実行中に生じた CPU 使用率の割合（パーセンテージ）。これには、サービスの割り込みや softirqs で経過する時間は含まれません。softirq（ソフトウェアの割り込み）は、複数の CPU で同時に実行できる最大 32 個の列挙されたソフトウェア割り込みの 1 つです。
- %iowait：システムに未処理のディスク I/O 要求があったときに、CPUがアイドル状態だった時間の割合（パーセンテージ）。
- %irq：割り込みを行うために CPU が費やした時間の割合（パーセンテージ）。
- %soft：softirqs を行うために CPU が費やした時間の割合（パーセンテージ）。
- %steal：ハイパーバイザが別の仮想プロセッサを実行しているときに、仮想CPUが強制的な待機で費やした時間の割合（パーセンテージ）。
- %guest：仮想プロセッサを実行するために CPU が費やした時間の割合（パーセンテージ）。
- %idle：CPU がアイドル状態で、システムに未処理のディスク I/O 要求がなかった時間の割合（パーセンテージ）。

アクセス

Basic

構文

```
show cpu [procnum]
```

ここで `procnum` は、使用率の情報を表示するプロセッサの数を表します。有効な値は 0 から、システム上の合計プロセッサ数から 1 引いた数までの範囲です。`procnum` が 7000 または 8000 シリーズデバイスで使用されている場合は無視されます。このプラットフォームについては、使用率の情報はすべてのプロセッサについてのみ表示されるためです。

```
> show cpu
```

Database コマンド

データベースの表示（`show database`）コマンドは、デバイスの管理インターフェイスを設定します。

アクセス

基本

processes

実行中のデータベース クエリを表示します。

アクセス

Basic

構文

```
show database processes
```

例

```
> show database processes
```

slow-query-log

データベースのスロー クエリを表示します。

アクセス

Basic

構文

```
show database slow-query-log
```

例

```
> show database slow-query-log
```

device-settings

現行のデバイスに特有のアプリケーションのバイパス設定に関する情報を表示します。

アクセス

Basic

構文

```
show device-settings
```

例

```
> show device-settings
```

disk

現行のディスクの使用率を表示します。

アクセス

Basic

構文

```
show disk
```

例

```
> show disk
```

disk-manager

システムの各パート（サイロ、低水位、高水位など）のディスク使用率の詳細情報を表示します。

アクセス

Basic

構文

```
show disk-manager
```

例

```
> show disk-manager
```

dns

現行の DNS サーバのアドレスと検索ドメインを表示します。

アクセス

Basic

構文

```
show dns
```

例

```
> show dns
```

fan-status

ハードウェア ファンの現在のステータスを表示します。このコマンドは NGIPSv および ASA FirePOWER デバイスでは使用できません。

アクセス

Basic

構文

```
show fan-status
```

例

```
> show fan-status
```

fastpath-rules

現在設定されている 8000 シリーズ の fastpath ルールを表示します。このコマンドは 8000 シリーズ デバイスでは使用できません。

アクセス

Basic

構文

```
show fastpath-rules
```

例

```
> show fastpath-rules
```

gui

Web インターフェイスの現在の状態を表示します。このコマンドは NGIPSv および ASA FirePOWER では使用できません。

アクセス

Basic

構文

```
show gui
```

例

```
> show gui
```

hostname

デバイスのホスト名およびアプライアンス UUID を表示します。CLI を使用してデバイスのホスト名を編集する場合は、管理する Firepower Management Center に変更が反映されることを確認します。場合によっては、デバイス管理設定を手動で編集する必要があります。

アクセス

Basic

構文

```
show hostname
```

例

```
> show hostname
```

hosts

ASA FirePOWER モジュールの /etc/hosts ファイルの内容を表示します。

アクセス

Basic

構文

```
show hosts
```

例

```
> show hosts
```

http-cert-expire-date

アプライアンスに関するデフォルト HTTPS サーバ証明書の現在の有効期限を表示します。このコマンドは NGIPSv および ASA FirePOWER デバイスでは使用できません。

アクセス

Basic

構文

```
show http-cert-expire-date
```

例

```
> show http-cert-expire-date
```

hyperthreading

ハイパースレッディングが有効か無効かを表示します。このコマンドは ASA FirePOWER では使用できません。

アクセス

Basic

構文

```
show hyperthreading
```

例

```
> show hyperthreading
```

inline-sets

すべてのインライン セキュリティ ゾーンと関連するインターフェイスの設定データを表示します。このコマンドは ASA FirePOWER では使用できません。

アクセス

Basic

構文

```
show inline-sets
```

例

```
> show inline-sets
```

interfaces

パラメータが指定されていない場合は、設定されているすべてのインターフェイスのリストが表示されます。パラメータが指定されている場合は、指定されたインターフェイスの詳細情報が表示されます。

アクセス

Basic

構文

```
show interfaces interface
```

ここで *interface* は詳細情報を表示する特定のインターフェイスです。

例

```
> show interfaces
```

ifconfig

ASA FirePOWER モジュールに対するインターフェイスの設定を表示します。

アクセス

Basic

構文

```
show ifconfig
```

例

```
> show ifconfig
```

lcd

LCD のハードウェア ディスプレイが有効か無効かを表示します。このコマンドは NGIPSv および ASA FirePOWER では使用できません。

アクセス

Basic

構文

```
show lcd
```

例

```
> show lcd
```

Link-aggregation コマンド

`show link-aggregation` コマンドは、リンク集約グループ（LAG）の設定および統計情報を表示します。このコマンドは NGIPSv および ASA FirePOWER デバイスでは使用できません。

アクセス

基本

設定：

LAG ID、インターフェイスの数、コンフィギュレーション モード、ロード バランシング モード、LACP 情報、および物理インターフェイスのタイプなど、設定された各 LAG の設定の詳細を表示します。

アクセス

Basic

構文

```
show link-aggregation configuration
```

例

```
> show link-aggregation configuration
```

統計情報

ステータス、リンク ステートと速度、コンフィギュレーション モード、送受信されたパケットのカウンタ、および送受信されたバイトのカウンタなど、設定された各 LAG の統計情報をインターフェイスごとに表示します。

アクセス

Basic

構文

```
show link-aggregation statistics
```

例

```
> show link-aggregation statistics
```

link-state

デバイスのポートのタイプ、リンク、および速度、デュプレックスの状態およびバイパスモードを表示します。このコマンドは ASA FirePOWER デバイスでは使用できません。

アクセス

Basic

構文

```
show link-state
```

例

```
> show link-state
```

log-ips-connection

記録された侵入イベントに関連付けられている接続イベントのロギングが有効か無効かを表示します。

アクセス

Basic

構文

```
show log-ips-connection
```

例

```
> show log-ips-connection
```

managers

Firepower Management Center の設定および通信のステータスを表示します。登録キーおよび NAT ID は、登録が保留中の場合のみ表示されます。

デバイスが、スタック設定のセカンダリ デバイスとして設定されている場合、管理している両方の FMC、およびプライマリ デバイスに関する情報が表示されます。

アクセス

Basic

構文

```
show managers
```

例

```
> show managers
```

memory

デバイスの合計メモリ、使用中のメモリ、使用可能なメモリを表示します。

アクセス

Basic

構文

```
show memory
```

例

```
> show memory
```

model

デバイスのモデル情報を表示します。

アクセス

Basic

構文

```
show model
```

例

```
> show model
```

mpls-depth

管理インターフェイスに設定されている MPLS レイヤ数を 0～6 で表示します。このコマンドは NGIPSv および ASA FirePOWER では使用できません。

アクセス

Basic

構文

```
show mpls-depth
```

例

```
> show mpls-depth
```

NAT コマンド

show nat コマンドは、管理インターフェイスの NAT データと設定情報を表示します。このコマンドは NGIPSv および ASA FirePOWER デバイスでは使用できません。

アクセス

基本

active-dynamic

ダイナミック ルールに従って変換されている NAT フローを表示します。これらのエントリは、フローがルールに一致している場合に、ルールがタイムアウトになるまで表示されます。したがって、リストは正確ではないことがあります。タイムアウトはプロトコルに依存します。ICMP は 5 秒、UDP は 120 秒、TCP は 3600 秒、他のすべてのプロトコルは 60 秒です。

構文

```
show nat active-dynamic
```

例

```
> show nat active-dynamic
```

active-static

スタティック ルールに従って変換されている NAT フローを表示します。これらのエントリは、デバイスにルールが展開されるとすぐに表示されます。リストは、スタティックな NAT ルールに一致しているアクティブなフローを示しているわけではありません。

構文

```
show nat active-static
```

例

```
> show nat active-static
```

allocators

すべての NAT アロケータの情報、ダイナミック ルールで使用されている変換済みアドレスのプールを表示します。

構文

```
show nat allocators
```

例

```
> show nat allocators
```

config

管理インターフェイスの現行の NAT ポリシーの設定を表示します。

構文

```
show nat config
```

例

```
> show nat config
```

dynamic-rules

指定されたアロケータ ID を使用しているダイナミックな NAT ルールを表示します。

構文

```
show nat dynamic-rules allocator_id
```

ここで `allocator_id` は有効なアロケータ ID 番号です。

例

```
> show nat dynamic-rules 9
```

flows

指定されたアロケータ ID を使用しているルールについてフローの数を表示します。

構文

```
show nat flows allocator-id
```

ここで *allocator_id* は有効なアロケータ ID 番号です。

例

```
> show nat flows 81
```

static-rules

すべてのスタティック NAT ルールを表示します。

構文

```
show nat static-rules
```

例

```
> show nat static-rules
```

netstat

ASA FirePOWER モジュールのアクティブなネットワーク接続を表示します。

アクセス

Basic

構文

```
show netstat
```

例

```
> show netstat
```

network

管理インターフェイスの IPv4 および IPv6 の設定、MAC アドレス、HTTP プロキシ アドレス、ポート、ユーザ名（設定されている場合）を表示します。

アクセス

Basic

構文

```
show network
```

例

```
> show network
```

network-modules

インストールされているすべてのモジュール、およびモジュールの情報（シリアル番号など）を表示します。このコマンドは NGIPSv および ASA FirePOWER では使用できません。

アクセス

Basic

構文

```
show network-modules
```

例

```
> show network-modules
```

network-static-routes

インターフェイス、宛先アドレス、ネットワーク マスク、およびゲートウェイ アドレスなど、設定済みのすべてのネットワーク スタティック ルートとその情報が表示されます。

アクセス

Basic

構文

```
show network-static-routes
```

例

```
> show network-static-routes
```

ntp

NTP コンフィギュレーションを表示します。

アクセス

Basic

構文

```
show ntp
```

例

```
> show ntp
```

perfstats

デバイスのパフォーマンスの統計情報を表示します。

アクセス

Basic

構文

```
show perfstats
```

例

```
> show perfstats
```

portstats

デバイスのすべての挿入されたポートのポート統計を表示します。このコマンドは NGIPSv および ASA FirePOWER では使用できません。

アクセス

Basic

構文

```
show portstats [copper | fiber | internal | external | all]
```

銅線は、すべての銅線ポートを指定します。光ファイバはすべての光ファイバ ポートを指定します。内部はすべての内部ポートをします。外部はすべての外部（銅線および光ファイバ）ポートをします。すべてはすべてのポート（外部および内部）を指定します。

例

```
> show portstats fiber
```

power-supply-status

現在のハードウェアの電源状態を表示します。このコマンドはNGIPSvおよびASA FirePOWERでは使用できません。

（注） 8000 シリーズ の管理対象デバイスで電源障害が発生すると、CLI コマンドの show power-supply-status が正しいステータスを反映するまでに 15 分かかる場合があります。

アクセス

Basic

構文

```
show power-supply-status
```

例

```
> show power-supply-status
```

process-tree

デバイスで実行中のプロセスについて、タイプごとにツリー形式でソートして表示します。

アクセス

Basic

構文

```
show process-tree
```

例

```
> show process-tree
```

processes

デバイス上で現在実行中のプロセスについて、CPU 使用率の降順で表示します。

アクセス

Basic

構文

```
show processes sort-flag filter
```

ここで、メモリ（の降順）でソートする場合は、*sort-flag* に `-m` を指定し、プロセス名ではなくユーザ名でソートする場合は `-u` を指定します。また、コマンドのフルネームおよびパスを表示する場合は `verbose` を指定します。*filter* パラメータは、コマンドの検索語または結果をフィルタするために使用するユーザ名を指定します。見出し行は表示されたままです。

例

```
> show processes -u user1
```

ルート

ASA FirePOWER モジュールに関するルーティング情報を表示します。

アクセス

Basic

構文

```
show route
```

例

```
> show route
```

routing-table

パラメータが指定されていない場合は、すべての仮想ルータに関するルーティング情報を表示します。パラメータが指定されている場合は、指定されたルータのルーティング情報、および該当する場合は、指定されたルーティングのプロトコル タイプを表示します。パラメータはすべてオプションです。このコマンドは NGIPSv および ASA FirePOWER では使用できません。

アクセス

Basic

構文

```
show routing-table name [ ospf | rip | static ]
```

name は、情報を必要とする特定のルータ名です。`ospf`、`rip`、`static` は、ルーティング プロトコル タイプを指定します。

例

```
> show routing-table Vrouter1 static
```

serial-number

シャーシのシリアル番号を表示します。このコマンドは NGIPSv では使用できません。

アクセス

Basic

構文

```
show serial-number
```

例

```
> show serial-number
```

ssl-policy-config

現在適用されている SSL ポリシーの設定（ポリシーの説明、デフォルトのロギング設定、有効なすべての SSL ルールとルールの設定など）、信頼できる CA 証明書、および復号化不可能なトラフィックのアクションを表示します。

アクセス

Basic

構文

```
show ssl-policy-config
```

例

```
> show ssl-policy-config
```

stacking

管理対象デバイスのスタッキングの設定とポジションを表示します。プライマリとして設定されているデバイスでは、すべてのセカンダリ デバイスのデータも示されます。高可用性ペアのスタックの場合、このコマンドは、スタックが高可用性ペアのメンバーであることも示します。スタッキングを有効または無効にする（大半の場合は無効にする）には、ユーザは Web インターフェイスを使用する必要があります。スタッキングが有効になっていない場合、コマンドは `Stacking not currently configured` というメッセージを返します。このコマンドは NGIPSv および ASA FirePOWER では使用できません。

アクセス

Basic

構文

```
show stacking
```

例

```
> show stacking
```

summary

デバイスに関して最もよく使用される情報（バージョン、タイプ、UUID など）のサマリーを表示します。詳細は次の `show` コマンドを参照してください。`version`、`interfaces`、`device-settings`、および `access-control-config`。

アクセス

Basic

構文

```
show summary
```

例

```
> show summary
```

syslog

システムのログを時系列の逆順で表示します。オプションでフィルタを指定して、ページ ビューごとに表示するコンテンツとレコード数に基づいて（デフォルトは25）、特定のレコードを表示できます。

アクセス

Basic

構文

```
show syslog ["filter" records_per_page]
```

filter が Grep 互換の検索フィルタを指定し、*records_per_page* が各ページ ビューに表示するレコード数を指定する場合。検索フィルタの詳細については、「システム ログ フィルタの構文（407 ページ）」を参照してください。

例

```
> show syslog "ssh" 20
```

システムは文字列「ssh」を含む 20 件の直近の syslog レコードを表示します。次の 20 件のレコードを表示するにはEnterキーを押し、表示を停止するにはqを入力します。

時刻

現在の日付と時刻を、UTC および現行のユーザに設定されているローカル タイム ゾーンで表示します。

アクセス

Basic

構文

```
show time
```

例

```
> show time
```

traffic-statistics

パラメータが指定されていない場合は、すべてのポートから送信された、および受信したバイトの詳細情報を表示します。ポートが指定されている場合は、指定されたポートの情報のみを表示します。ASA FirePOWER モジュールのポートを指定することはできません。システムはデータ プレーン インターフェイスのみを表示します。

（注） 場合によっては、このコマンドの出力が、実際にはデバイスがトラフィックをドロップしていないときにパケットのドロップを表示することがあります。不正なパケットを受信すると、ドロップ カウンタが増加します。不正なパケットは、ヘッダー内の特定の情報が欠けていたり、巡回冗長検査（CRC）に失敗していた可能性があります。通常、不正なパケットの一般的な根本原因は、不良ケーブルまたは不良インターフェイスなどのデータ リンク層の問題です。ドロップされたパケットはログに記録されません。ただし、送信元が TCP など、信頼できる転送プロトコルの場合は、パケットは再送信されます。

アクセス

Basic

構文

```
show traffic-statistics port
```

ここで *port* は、情報を表示させたい特定のポートです。

例

```
> show traffic-statistics s1p1
```

user

NGIPSv のみに適用できます。指定されたユーザに関する設定の詳細情報を表示します。次の値が表示されます。

- Login：ログイン名
- UID：ユーザ ID（数値）
- Auth（`Local` または `Remote`）：ユーザがどのように認証されているか

- Access（`Basic` または `Config`）：ユーザの権限レベル
- Enabled（`Enabled` または `Disabled`）：ユーザがアクティブかどうか
- Reset（`Yes` または `No`）：次のログイン時にユーザがパスワードを変更する必要があるかどうか
- Exp（`Never` または数値）：ユーザのパスワード変更が必要になるまでの日数
- Warn（`N/A` または数値）：パスワードの有効期限が切れる前に、ユーザがパスワード変更のために与えられる日数
- Str（`Yes` または `No`）：ユーザのパスワードが強度チェックの基準を満たす必要があるかどうか
- Lock（`Yes` または `No`）：ログインの失敗が多すぎる場合に、ユーザのアカウントがロックされるかどうか
- Max（`N/A` または数値）：ユーザのアカウントがロックされる前に失敗するログインの最大回数

アクセス

Configuration

構文

```
show user username username username ...
```

ここで *username* はユーザの名前を表します。複数の username はスペースで区切って指定します。

例

```
> show user jdoe
```

ユーザ

NGIPSv および ASA FirePOWER のみに該当します。すべてのローカル ユーザの設定の詳細情報を表示します。次の値が表示されます。

- Login：ログイン名
- UID：ユーザ ID（数値）
- Auth（`Local` または `Remote`）：ユーザがどのように認証されているか
- Access（`Basic` または `Config`）：ユーザの権限レベル
- Enabled（`Enabled` または `Disabled`）：ユーザがアクティブかどうか

- Reset（Yes または No）：次のログイン時にユーザがパスワードを変更する必要があるかどうか
- Exp（Never または数値）：ユーザのパスワード変更が必要になるまでの日数
- Warn（N/A または数値）：パスワードの有効期限が切れる前に、ユーザがパスワード変更のために与えられる日数
- Str（Yes または No）：ユーザのパスワードが強度チェックの基準を満たす必要があるかどうか
- Lock（Yes または No）：ログインの失敗が多すぎる場合に、ユーザのアカウントがロックされるかどうか
- Max（N/A または数値）：ユーザのアカウントがロックされる前に失敗するログインの最大回数

アクセス

Configuration

構文

```
show users
```

例

```
> show users
```

version

製品のバージョンとビルドを表示します。detail パラメータが指定されている場合は、追加のコンポーネントのバージョンが表示されます。

（注） ASA with FirePOWER Services では detail パラメータは使用できません。

アクセス

Basic

構文

```
show version [detail]
```

例

```
> show version
```

virtual-routers

パラメータが指定されていない場合は、現在設定されているすべての仮想ルータのリスト、および DHCP リレー、OSPF、および RIP の情報が表示されます。パラメータが指定されている場合は、指定されたルータに関する情報が、指定されたルート タイプによって制限されて表示されます。パラメータはすべてオプションです。このコマンドはNGIPSvおよびASA FirePOWERでは使用できません。

アクセス

Basic

構文

```
show virtual-routers [ dhcprelay | ospf | rip ] name
```

ここで `dhcprelay`、`ospf`、および `rip` はルート タイプを表します。*name* は、情報を表示する特定のルータの名前を表します。`ospf` を指定した場合は、ルート タイプ、および（存在する場合は）ルート名に対して `neighbors`、`topology`、または `lsadb` を指定することができます。

例

```
> show virtual-routers ospf VRouter2
```

virtual-switches

パラメータが指定されていない場合は、設定されているすべての仮想スイッチのリストが表示されます。パラメータが指定されている場合は、指定されたスイッチに関する情報が表示されます。このコマンドは NGIPSv および ASA FirePOWER では使用できません。

アクセス

Basic

構文

```
show virtual-switches name
```

例

```
> show virtual-switches Vswitch1
```

vmware-tools

VMware Tools が、仮想デバイス上で現在有効になっているかどうかを示します。このコマンドは、NGIPSv のみで使用できます。

VMware ツールは、仮想マシンのパフォーマンスを向上させるためのユーティリティ スイートです。これらのユーティリティを使用すると、VMware 製品の便利な機能をすべて活用できます。このシステムは、すべての仮想アプライアンスで次のプラグインをサポートします。

- guestInfo
- powerOps
- timeSync
- vmbackup

VMware ツールおよびサポートされるプラグインの詳細については、VMware の Web サイト（http://www.vmware.com）を参照してください。

アクセス

Basic

構文

```
show vmware-tools
```

例

```
> show vmware-tools
```

VPN コマンド

`show VPN` コマンドは、VPN ステータス、および VPN 接続の設定情報を表示します。このコマンドは NGIPSv および ASA FirePOWER デバイスでは使用できません。

アクセス

基本

config

すべての VPN 接続の設定を表示します。

構文

```
show vpn config
```

例

```
> show vpn config
```

config by virtual router

仮想ルータについて、すべての VPN 接続の設定を表示します。

構文

```
show vpn config virtual router
```

例

```
> show vpn config VRouter1
```

status

VPN 接続すべてのステータスを表示します。

構文

```
show vpn status
```

例

```
> show vpn status
```

status by virtual router

仮想ルータについて、すべての VPN 接続のステータスを表示します。

構文

```
show vpn status virtual router
```

例

```
> show vpn status VRouter1
```

counters

すべての VPN 接続のカウンタを表示します。

構文

```
show vpn counters
```

例

```
> show vpn counters
```

counters by virtual router

仮想ルータについて、すべての VPN 接続のカウンタを表示します。

構文

```
show vpn counters virtual router
```

例

```
> show vpn counters VRouter1
```

クラシック デバイス CLI 設定コマンド

コンフィギュレーション コマンドを使用して、システムを設定および管理することができます。これらのコマンドはシステムの動作に影響を与えます。そのため、基本（Baisc）レベルのパスワード設定（`configure password`）コマンドを除き、設定 CLI アクセス権限を持つユーザのみがこれらのコマンドを発行できます。

audit_cert コマンド

`audit_cert` コマンドは、安全性監査ログ ストリーミングを行うためにデバイスの監査ログ クライアント証明書の設定を行います。

アクセス

設定

削除

セキュアな監査ログ ストリーミングの現行のクライアント証明書を削除します。

構文

```
configure audit_cert delete
```

例

```
> configure audit_cert delete
```

import

セキュアな監査ログストリーミングのクライアント証明書をインポートします。ユーザは、コマンドを入力すると、クライアント証明書と秘密キー、または証明書チェーンをCLIから入力するように求められます。

構文

```
configure audit_cert import
```

例

```
> configure audit_cert import
***************Import Audit Client Certificate**************

1 Import Client Certificate and Private Key
2 Import Certificate Chain
0 Exit

************************************************************
Enter choice: 1
Enter your audit client certificate (PEM format) here:
-----BEGIN CERTIFICATE-----
MIIEoTCCA4mgAwIBAgICAR4wDQYJK0ZIhvcNaQALBWAugYICzAJBqNVBATYAiVT
   ...certificate details ...
Tx*FAhnXeUZ78hFepg1yHQMYWTkD7hCqmSN3UkAb1l0IoBcxTA==
-----END CERTIFICATE-----

Enter your private key (PEM format) here:
-----BEGIN RSA PRIVATE KEY-----
miiieOWobabkc3qwaOgVx0Tt61eY83Mrqa+bek_qPetcHRAw6ea4p0TlMVVsE7qr
   ...private key details ...
nRI6QNkoumLUT9EvjF6bFoT3M6eDI7+NdDIhjVeOP*E4+hxEX50jM
-----END RSA PRIVATE KEY-----
```

```
Client certificate import succeed, exiting...
```

bypass

7000 または 8000 シリーズ デバイスで、インライン ペアをフェールオープン（ハードウェア バイパス）モードまたはフェールクローズモードにします。このコマンドは、インラインセットの [バイパス モード（Bypass Mode）] オプションが [バイパス（Bypass）] に設定されている場合にのみ使用できます。

デバイスを再起動するとインライン セットのフェールオープン モードが解除されるということに注意してください。

アクセス

Configuration

構文

```
configure bypass {open | close} {interface}
```

ここで、`interface` はインライン ペアのいずれかのハードウェア ポートの名前です。

例

```
> configure bypass open s1p1
```

high-availability

デバイスで高可用性のバイパスを無効にしたり、設定したりします。このコマンドは、NGIPSv、ASA FirePOWER、またはセカンダリ スタック メンバとして設定されているデバイスでは使用できません。

アクセス

Configuration

構文

```
configure high-availability {disable | bypass}
```

例

```
> configure high-availability disable
```

gui

デバイスの Web インターフェイス（システムのメジャーな更新時に表示される、簡潔なアップグレード Web インターフェイスなど）を有効または無効にします。このコマンドは NGIPSv および ASA FirePOWER では使用できません。

アクセス

Configuration

構文

```
configure gui [enable | disable]
```

例

```
> configure gui disable
```

lcd

デバイスの正面の LCD ディスプレイを有効または無効にします。このコマンドは NGIPSv および ASA FirePOWER では使用できません。

アクセス

Configuration

構文

```
configure lcd {enable | disable}
```

例

```
> configure lcd disable
```

log-ips-connections

記録された侵入イベントに関連付けられている接続イベントのロギングを有効または無効にします。

アクセス（Access）

Configuration

構文

```
configure log-ips-connections {enable | disable}
```

例

```
> configure log-ips-connections disable
```

manager コマンド

`configure manager` コマンドは、管理元の Firepower Management Center へのデバイスの接続を設定します。

アクセス

設定

追加

管理元のFirepower Management Centerからの接続を承認するようデバイスを設定します。このコマンドは、デバイスがアクティブに管理されていない場合のみ機能します。

デバイスをFirepower Management Centerに登録するには、一意の英数字による登録キーが必要です。ほとんどの場合は、登録キーと一緒にホスト名または IP アドレスを指定する必要があります。ただし、デバイスとFirepower Management Centerが NAT デバイスによって分けられている場合は、登録キーと一緒に一意の NAT ID を入力し、ホスト名の代わりに `DONTRESOLVE` を指定します。

構文

```
configure manager add {hostname | IPv4_address | IPv6_address | DONTRESOLVE} regkey
[nat_id]
```

ここで、{hostname | IPv4_address | IPv6_address | `DONTRESOLVE`} は、このデバイスを管理する Firepower Management Center の DNS ホスト名、または IP アドレス（IPv4 または IPv6）を指定します。Firepower Management Center を直接アドレス指定できない場合は、`DONTRESOLVE` を使用します。`DONTRESOLVE` を使用する場合は nat_id が必要です。regkey は、デバイスを Firepower Management Center に登録するために必要な一意の英数字の登録キーです。nat_id は、Firepower Management Center とデバイス間の登録プロセスで使用される任意の英数字の文字列です。hostname が `DONTRESOLVE` に設定されている場合に必要です。

例

```
> configure manager add DONTRESOLVE abc123 efg456
```

削除

Firepower Management Centerの接続情報をデバイスから削除します。このコマンドは、デバイスがアクティブに管理されていない場合のみ機能します。

構文

```
configure manager delete
```

例

```
> configure manager delete
```

mpls-depth

管理インターフェイスでMPLSレイヤの数を設定します。このコマンドはNGIPSvおよびASA FirePOWERでは使用できません。

アクセス

Configuration

構文

```
configure mpls-depth depth
```

ここで *depth* は 0～6 の数値です。

例

```
> configure mpls-depth 3
```

network コマンド

`configure network` コマンドは、デバイスの管理インターフェイスを設定します。

アクセス

設定

dns searchdomains

DNS 検索ドメインの現行のリストを、コマンドで指定されたリストに置き換えます。

構文

```
configure network dns searchdomains {searchlist}
```

searchlist はカンマで区切られたドメインのリストです。

例

```
> configure network dns searchdomains foo.bar.com,bar.com
```

dns servers

DNS サーバの現行のリストを、コマンドで指定されたリストに置き換えます。

構文

```
configure nework dns servers {dnslist}
```

dnslist は、カンマで区切られた DNS サーバのリストです。

例

```
> configure network dns servers 10.123.1.10,10.124.1.10
```

hostname

デバイスのホスト名を設定します。

構文

```
configure network hostname {name}
```

name は新しいホスト名です。

例

```
> configure network hostname sfrocks
```

http-proxy

7000 & 8000 シリーズ および NGIPSv デバイスで、HTTP プロキシを設定します。コマンドを発行した後で、CLI はユーザに対して HTTP プロキシのアドレスとポート、プロキシの認証が必要かどうかを尋ねます。認証が必要な場合はプロキシのユーザ名、プロキシのパスワード、およびプロキシのパスワードの確認を入力するよう要求されます。

NGIPSv 上でこのコマンドを使用して、HTTP プロキシ サーバを設定し、仮想デバイスが動的解析のためにファイルを AMP クラウドへ送信できるようにします。

構文

プロキシのパスワードでは、英数字のみが使用できます。

```
configure network http-proxy
```

例

```
> configure network http-proxy
Manual proxy configuration
Enter HTTP Proxy address:
Enter HTTP Proxy Port:
Use Proxy Authentication? (y/n) [n]:
Enter Proxy Username:
Enter Proxy Password:
Confirm Proxy Password:
```

http-proxy-disable

7000 シリーズ、8000 シリーズ、または NGIPSv デバイスで、任意の HTTP プロキシの設定を削除します。

構文

```
configure network http-proxy-disable
```

例

```
> configure network http-proxy-disable
Are you sure that you wish to delete the current
http-proxy configuration? (y/n):
```

ipv4 delete

デバイスの管理インターフェイスの IPv4 設定を無効にします。

構文

```
configure network ipv4 delete [management_interface]
```

ここで、*management_interface* は管理インターフェイス ID です。インターフェイスを指定しない場合、このコマンドはデフォルトの管理インターフェイスを設定します。このパラメータは、**configure management-interface** コマンドを使って複数の管理インターフェイスを有効にする場合にのみ必要です。複数の管理インターフェイスは、8000 シリーズ デバイスおよび ASA 5585-X with FirePOWER サービスでのみサポートされています。他のプラットフォームではこ

のパラメータを指定しないでください。管理インターフェイスIDは、デフォルト管理インターフェイスでは **eth0**、オプションのイベント インターフェイスでは **eth1** です。

例

```
> configure network ipv4 delete eth1
```

ipv4 dhcp

デバイスの管理インターフェイスの IPv4 設定を DHCP に設定します。管理インターフェイスは DHCP サーバと通信して、設定情報を取得します。

構文

```
configure network ipv4 dhcp [management_interface]
```

ここで、*management_interface* は管理インターフェイス ID です。DHCP はデフォルトの管理インターフェイスでのみサポートされているため、この引数を使用する必要はありません。

例

```
> configure network ipv4 dhcp
```

ipv4 manual

デバイスの管理インターフェイスの IPv4 設定を手動で設定します。

構文

```
configure network ipv4 manual ipaddr netmask [gw] [management_interface]
```

ここで *ipaddr* は IP アドレスで、*netmask* はサブネットマスク、*gw* はデフォルト ゲートウェイの IPv4 アドレスです。*management_interface* は管理インターフェイス ID です。インターフェイスを指定しない場合、このコマンドはデフォルトの管理インターフェイスを設定します。このパラメータは、**configure management-interface** コマンドを使って複数の管理インターフェイスを有効にする場合にのみ必要です。複数の管理インターフェイスは、8000 シリーズ デバイスおよび ASA 5585-X with FirePOWER サービスでのみサポートされています。他のプラットフォームではこのパラメータを指定しないでください。管理インターフェイス ID は、デフォルト管理インターフェイスでは**eth0**、オプションのイベントインターフェイスでは**eth1** です。

例

```
> configure network ipv4 manual 10.123.1.10 255.255.0.0 10.123.1.1
```

ipv6 delete

デバイスの管理インターフェイスの IPv6 設定を無効にします。

構文

```
configure network ipv6 delete [management_interface]
```

ここで、*management_interface* は管理インターフェイス ID です。インターフェイスを指定しない場合、このコマンドはデフォルトの管理インターフェイスを設定します。このパラメータは、**configure management-interface** コマンドを使って複数の管理インターフェイスを有効にする場合にのみ必要です。複数の管理インターフェイスは、8000 シリーズ デバイスおよび ASA 5585-X with FirePOWER サービスでのみサポートされています。他のプラットフォームではこのパラメータを指定しないでください。管理インターフェイス ID は、デフォルト管理インターフェイスでは **eth0**、オプションのイベント インターフェイスでは **eth1** です。

例

```
> configure network ipv6 delete
```

ipv6 dhcp

デバイスの管理インターフェイスの IPv6 設定を DHCP に設定します。管理インターフェイスは DHCP サーバと通信して、設定情報を取得します。

構文

```
configure network ipv6 dhcp [management_interface]
```

ここで、*management_interface* は管理インターフェイス ID です。DHCP はデフォルトの管理インターフェイスでのみサポートされているため、この引数を使用する必要はありません。

例

```
> configure network ipv6 dhcp
```

ipv6 manual

デバイスの管理インターフェイスの IPv6 設定を手動で設定します。

構文

```
configure network ipv6 manual ip6addr/ip6prefix [ip6gw] [management_interface]
```

ここで *ip6addr*/*ip6prefix* は IP アドレスとプレフィックス長、*ip6gw* はデフォルト ゲートウェイの IPv6 アドレスを表します。*management_interface* は管理インターフェイス ID です。インターフェイスを指定しない場合、このコマンドはデフォルトの管理インターフェイスを設定しま

す。このパラメータは、**configure management-interface** コマンドを使って複数の管理インターフェイスを有効にする場合にのみ必要です。複数の管理インターフェイスは、8000 シリーズデバイスおよび ASA 5585-X with FirePOWER サービスでのみサポートされています。他のプラットフォームではこのパラメータを指定しないでください。管理インターフェイス ID は、デフォルト管理インターフェイスでは**eth0**、オプションのイベント インターフェイスでは**eth1**です。

例

```
> configure network ipv6 manual 2001:DB8:3ffe:1900:4545:3:200:f8ff:fe21:67cf 64
```

ipv6 router

デバイスの管理インターフェイスの IPv6 設定をルータに設定します。管理インターフェイスは IPv6 ルータと通信して、設定情報を取得します。

構文

```
configure network ipv6 router [management_interface]
```

ここで、*management_interface* は管理インターフェイス ID です。インターフェイスを指定しない場合、このコマンドはデフォルトの管理インターフェイスを設定します。このパラメータは、**configure management-interface** コマンドを使って複数の管理インターフェイスを有効にする場合にのみ必要です。複数の管理インターフェイスは、8000 シリーズ デバイスおよび ASA 5585-X with FirePOWER サービスでのみサポートされています。他のプラットフォームではこのパラメータを指定しないでください。管理インターフェイス ID は、デフォルト管理インターフェイスでは **eth0**、オプションのイベント インターフェイスでは **eth1** です。

例

```
> configure network ipv6 router
```

management-interface disable

管理インターフェイスを無効にします。複数の管理インターフェイスは、8000 シリーズ デバイスおよび ASA 5585-X with FirePOWER サービスでのみサポートされています。

構文

```
configure network management-interface disable ethn
```

ここで、*n* は設定する管理インターフェイスの番号、**eth0** はデフォルトの管理インターフェイス、**eth1** はオプションのイベント インターフェイスです。シスコでは、管理チャネルとイベント チャネルの両方を有効にして、eth0 デフォルト管理インターフェイスを有効のままにすることを推奨しています。Firepower Management Center および管理対象デバイスで個別のイベン

トインターフェイスを使用する方法の詳細については、管理インターフェイス （1266ページ）を参照してください。

例

```
> configure network management-interface disable eth1
```

management-interface disable-event-channel

指定された管理インターフェイスでイベント トラフィック チャネルを無効にします。複数の管理インターフェイスは、8000 シリーズ デバイスおよび ASA 5585-X with FirePOWER サービスでのみサポートされています。

構文

```
configure network management-interface disable-event-channel ethn
```

ここで、*n* は設定する管理インターフェイスの番号、**eth0** はデフォルトの管理インターフェイス、**eth1** はオプションのイベント インターフェイスです。シスコでは、管理チャネルとイベント チャネルの両方を有効にして、eth0デフォルト管理インターフェイスを有効のままにすることを推奨しています。Firepower Management Center および管理対象デバイスで個別のイベント インターフェイスを使用する方法の詳細については、管理インターフェイス （1266ページ）を参照してください。

例

```
> configure network management-interface disable-event-channel eth1
```

management-interface disable-management-channel

指定された管理インターフェイスで管理トラフィック チャネルを無効にします。複数の管理インターフェイスは、8000 シリーズ デバイスおよび ASA 5585-X with FirePOWER サービスでのみサポートされています。

構文

```
configure network management-interface disable-management-channel ethn
```

ここで、*n* は設定する管理インターフェイスの番号、**eth0** はデフォルトの管理インターフェイス、**eth1** はオプションのイベント インターフェイスです。シスコでは、管理チャネルとイベント チャネルの両方を有効にして、eth0デフォルト管理インターフェイスを有効のままにすることを推奨しています。Firepower Management Center および管理対象デバイスで個別のイベント インターフェイスを使用する方法の詳細については、管理インターフェイス （1266ページ）を参照してください。

例

```
> configure network management-interface disable-management-channel eth1
```

management-interface enable

指定した管理インターフェイスを有効にします。複数の管理インターフェイスは、8000 シリーズ デバイスおよび ASA 5585-X with FirePOWER サービスでのみサポートされています。

構文

```
configure network management-interface enable eth<i>n</i>
```

ここで、*n* は有効にする管理インターフェイスの番号、**eth0** はデフォルトの管理インターフェイス、**eth1** はオプションのイベント インターフェイスです。

デバイスを管理する場合、Firepower Management Center 管理インターフェイスには 2 つの別個のトラフィック チャネルがあります。管理トラフィック チャネルはすべての内部トラフィック（デバイスの管理に固有のデバイス間トラフィックなど）を伝送し、イベント トラフィック チャネルはすべてイベント トラフィック（Web イベントなど）を伝送します。必要に応じて、Management Center で個別のイベント専用インターフェイスを設定し、イベント トラフィックを処理することもできます（Firepower Management Center Web インタ フェースで、この設定が実行されていることを確認してください）。イベント専用インターフェイスは 1 つだけ設定できます。イベント トラフィックは大量の帯域幅を使用する可能性があるので、管理トラフィックからイベント トラフィックを分離することで、Management Center のパフォーマンスを向上させることができます。

デフォルトの eth0 インターフェイスには、デフォルトで管理とイベント チャンネルの両方が含まれています。必要に応じて、イベント専用インターフェイスとして eth0 インターフェイスを有効にできます。可能であれば、デバイス イベント インターフェイスと Firepower Management Center イベント インターフェイスの間で、イベント トラフィックが送信されます。イベント ネットワークがダウンすると、イベント トラフィックは、デフォルトの管理インターフェイスに戻ります。可能な場合には別個のイベント インターフェイスが使用されますが、管理インターフェイスが常にバックアップとなります。

管理インターフェイスを有効にすると、管理とイベント チャンネルの両方がデフォルトで有効にされます。管理チャネルとイベント チャネルの両方にデフォルト管理インターフェイスを使用することをお勧めします。その後、別個のイベント専用インターフェイスを有効にします。Firepower Management Center イベント専用インターフェイスは管理チャネルのトラフィックを受け入れることができないので、デバイス イベント インターフェイスで管理チャネルを単に無効にしてください。

configure network {**ipv4** | **ipv6**} **manual** コマンドを使用して管理インターフェイスのアドレスを設定します。

例

```
> configure network management-interface enable eth1
> configure network management-interface disable-management-channel eth1
```

management-interface enable-event-channel

指定された管理インターフェイスでイベント トラフィック チャネルを有効にします。複数の管理インターフェイスは、8000 シリーズ デバイスおよび ASA 5585-X with FirePOWER サービスでのみサポートされています。

構文

```
configure network management-interface enable-event-channel ethn
```

ここで、*n* は設定する管理インターフェイスの番号、**eth0** はデフォルトの管理インターフェイス、**eth1** はオプションのイベント インターフェイスです。シスコでは、管理チャネルとイベント チャネルの両方を有効にして、eth0デフォルト管理インターフェイスを有効のままにすることを推奨しています。Firepower Management Center および管理対象デバイスで個別のイベント インターフェイスを使用する方法の詳細については、管理インターフェイス （1266ページ）を参照してください。

例

```
> configure network management-interface enable-event-channel eth1
```

management-interface enable-management-channel

指定された管理インターフェイスで管理トラフィック チャネルを有効にします。 複数の管理インターフェイスは、8000 シリーズ デバイスおよび ASA 5585-X with FirePOWER サービスでのみサポートされています。

構文

```
configure network management-interface enable-management-channel ethn
```

ここで、*n* は設定する管理インターフェイスの番号、**eth0** はデフォルトの管理インターフェイス、**eth1** はオプションのイベント インターフェイスです。シスコでは、管理チャネルとイベント チャネルの両方を有効にして、eth0デフォルト管理インターフェイスを有効のままにすることを推奨しています。Firepower Management Center および管理対象デバイスで個別のイベント インターフェイスを使用する方法の詳細については、管理インターフェイス （1266ページ）を参照してください。

例

```
> configure network management-interface enable-management-channel eth1
```

management-interface tcpport

管理用の TCP ポートの値を変更します。

構文

```
configure network management-interface tcpport port
```

port は設定する管理ポートの値です。

例

```
> configure network management-interface tcpport 8500
```

management-port

デバイスの TCP 管理ポートの値を設定します。

構文

```
configure network management-port number
```

number は設定する管理ポートの値を表します。

例

```
> configure network management-port 8500
```

static-routes ipv4 add

指定した管理インターフェイスの IPv4 スタティック ルートを追加します。

構文

```
configure network static-routes ipv4
add interface destination netmask gateway
```

interface は管理インターフェイス、destination は宛先 IP アドレス、netmask はネットワーク マスク アドレス、gateway は追加するゲートウェイ アドレスです。

例

```
> configure network static-routes ipv4
add eth1 10.115.24.0 255.255.255.0 10.115.9.2
```

static-routes ipv4 delete

指定した管理インターフェイスの IPv4 スタティック ルートを削除します。

構文

```
configure network static-routes ipv4
delete interface destination netmask gateway
```

interface は管理インターフェイス、destination は宛先 IP アドレス、netmask はネットワーク マスク アドレス、gateway は削除するゲートウェイ アドレスです。

例

```
> configure network static-routes ipv4
delete eth1 10.115.24.0 255.255.255.0 10.115.9.2
```

static-routes ipv6 add

指定した管理インターフェイスの IPv6 スタティック ルートを追加します。

構文

```
configure network static-routes ipv6
add interface destination prefix gateway
```

interface は管理インターフェイス、destination は宛先 IP アドレス、prefix は IPv6 プレフィックス長、gateway は追加するゲートウェイ アドレスです。

例

```
> configure network static-routes ipv6
add eth1 2001:DB8:3ffe:1900:4545:3:200: f8ff:fe21:67cf 64
```

static-routes ipv6 delete

指定した管理インターフェイスの IPv6 スタティック ルートを削除します。

構文

```
configure network static-routes ipv6
delete interface destination prefix gateway
```

interface は管理インターフェイス、destination は宛先 IP アドレス、prefix は IPv6 プレフィックス長、gateway は削除するゲートウェイ アドレスです。

例

```
> configure network static-routes ipv6
delete eth1 2001:DB8:3ffe:1900:4545:3:200:f8ff: fe21:67cf 64
```

password

現行のユーザは、自身のパスワードを変更することができます。コマンドを発行すると、CLI は現在の（古い）パスワードを入力するようユーザに要求し、その後で新しいパスワードを 2 回入力するよう要求します。

アクセス

Basic

構文

```
configure password
```

例

```
> configure password
Enter current password:
Enter new password:
Confirm new password:
```

スタッキングの無効化

7000 および 8000 シリーズ のデバイスでは、次のデバイスに存在するスタック構成はすべて削除されます。

- プライマリとして設定されているデバイスでは、スタックは完全に削除されます。
- セカンダリとして設定されているデバイスでは、そのデバイスはスタックから削除されます。

このコマンドは、NGIPSv または ASA FirePOWER モジュールでは使用できません。また、これを使用してデバイスの高可用性ペアを解除することはできません。

スタッキング階層の上位アプライアンスとの通信を確立できない場合は、このコマンドを使用します。Firepower Management Centerを通信で使用できる場合は、代わりにFirepower Management CenterWeb インターフェイスを使用するよう伝えるメッセージが表示されます。同様に、プライマリ デバイスを使用できる場合に、セカンダリとして設定されているデバイス上で `stacking disable` を入力すると、プライマリ デバイスからコマンドを入力するよう伝えるメッセージが表示されます。

アクセス

Configuration

構文

```
configure stacking disable
```

例

```
> configure stacking disable
```

user コマンド

NGIPSv でのみ使用できます。`configure user` コマンドは、デバイスのローカル ユーザ データベースを管理します。

アクセス

設定

アクセス

指定したユーザのアクセス レベルを変更します。このコマンドは、指定されたユーザが次にログインするときに有効になります。

構文

```
configure user access username [basic | config]
```

username は、アクセスを変更するユーザの名前を表します。`basic` はbasic アクセスを、`config` は configuration アクセスを表します。

例

```
> configure user access jdoe basic
```

追加

指定された名前とアクセス レベルで新しいユーザを作成します。このコマンドでは、ユーザのパスワードを入力するよう要求されます。

構文

```
configure user add username [basic | config]
```

ここで、username は新しいユーザの名前を指定します。`basic` は基本アクセス、`config` は設定アクセスを表します。

例

```
> configure user add jdoe basic
Enter new password for user jdoe:
Confirm new password for user jdoe:
```

aging

ユーザ パスワードに有効期限を設定します。

構文

```
configure user aging username max_days warn_days
```

ここで、`username` はユーザの名前、`max_days` はパスワードが有効な最大日数、`warn_days` は有効期限が切れる前にユーザがパスワードを変更するために確保されている日数を表します。

例

```
> configure user aging jdoe 100 3
```

削除

ユーザとユーザのホーム ディレクトリを削除します。

構文

```
configure user delete username
```

`username` はユーザの名前を表します。

例

```
> configure user delete jdoe
```

disable

ユーザを無効にします。無効なユーザはログインできません。

構文

```
configure user disable username
```

username はユーザの名前を表します。

例

```
> configure user disable jdoe
```

enable

ユーザを有効にします。

構文

```
configure user enable username
```

username はユーザの名前を指定します。

例

```
> configure user enable jdoe
```

forcereset

ユーザが次にログインするときに、パスワードの変更を要求します。ユーザがログインしてパスワードを変更すると、強度のチェックが自動的に有効になります。

構文

```
configure user forcereset username
```

username はユーザの名前を表します。

例

```
> configure user forcereset jdoe
```

maxfailedlogins

指定したユーザが、ログインで失敗できる最大回数を設定します。

構文

```
configure user maxfailedlogins username number
```

username はユーザの名前、*number* は、ログインで失敗できる最大回数を表します。

例

```
> configure user maxfailedlogins jdoe 3
```

minpasswdlen

ユーザ パスワードに含める必要がある最小文字数を設定します。

構文

```
configure user minpasswdlen username number
```

ここで、*username* はユーザ アカウントの名前を指定し、*number* はそのアカウントに含める必要がある最小文字数（1 ～ 127）を指定します。

例

```
> configure user minpasswdlen jdoe 13
```

password

ユーザのパスワードを設定します。このコマンドでは、ユーザのパスワードを入力するよう要求されます。

構文

```
configure user password username
```

username はユーザの名前を表します。

例

```
> configure user pasword jdoe
Enter new password for user jdoe:
Confirm new password for user jdoe:
```

strengthcheck

ユーザのパスワードに対する強度の要件を有効または無効にします。ユーザパスワードの有効期限が切れた場合、または configure user forcereset コマンドを使用している場合は、ユーザが次にログインしたときにこの要件が自動的に有効になります。

構文

```
configure user strengthcheck username {enable | disable}
```

username はユーザの名前を表します。`enable` は指定されたユーザのパスワードの要件を設定し、`disable` は、指定されたユーザのパスワードの要件を削除します。

例

```
> configure user strengthcheck jdoe enable
```

unlock

ログイン失敗の最大数を超過したユーザをロック解除します。

構文

```
configure user unlock username
```

username はユーザの名前を表します。

例

```
> configure user unlock jdoe
```

vmware-tools

NGIPSv での VMware Tools の機能を有効または無効にします。このコマンドは、NGIPSv のみで使用できます。

VMware ツールは、仮想マシンのパフォーマンスを向上させるためのユーティリティ スイートです。これらのユーティリティを使用すると、VMware 製品の便利な機能をすべて活用できます。このシステムは、すべての仮想アプライアンスで次のプラグインをサポートします。

- guestInfo
- powerOps
- timeSync
- vmbackup

VMware ツールおよびサポートされるプラグインの詳細については、VMware の Web サイト（http://www.vmware.com）を参照してください。

アクセス

Basic

構文

```
configure vmware-tools [enable | disable]
```

例

```
> configure vmware-tools enable
```

クラシック デバイス CLI system コマンド

system コマンドを使用して、システム全体のファイルおよびアクセス コントロールの設定を管理することができます。Configuration CLI アクセス権を持つユーザのみが、システム モードでコマンドを発行できます。

アクセス制御コマンド

`system access-control` コマンドは、ユーザがデバイス上でアクセス制御設定を管理できるようにします。

アクセス

設定

archive

現在展開されているアクセス コントロール ポリシーをテキスト ファイルとして `/var/common` に保存します。

構文

```
system access-control archive
```

例

```
> system access-control archive
```

clear-rule-counts

アクセス コントロール ルールのヒット数を 0 にリセットします。

構文

```
system access-control clear-rule-counts
```

例

```
> system access-control clear-rule-counts
```

rollback

これまでに導入されたアクセス制御設定に対して、システムの復帰を行います。このコマンドをスタックまたは高可用性ペアのデバイスで使用することはできません。

構文

```
system access-control rollback
```

例

```
> system access-control rollback
```

コンプライアンス コマンド

コンプライアンス（compliance）コマンドは、デバイスのセキュリティ認定コンプライアンスモードの表示、設定を行います。

⚠

注意 この設定を有効にした後は、無効にすることはできません。無効にする必要がある場合は、サポートにお問い合わせください。

アクセス

設定

enable cc

デバイスのセキュリティ認定準拠をコモン クライテリア（CC）モードに設定します。

⚠

注意 この設定を有効にした後は、無効にすることはできません。無効にする必要がある場合は、サポートにお問い合わせください。

構文

```
system compliance enable cc
```

例

```
> system compliance enable cc
```

enable ucapl

デバイスのセキュリティ認定準拠を統合機能承認取得済み製品リスト（UCAPL）モードに設定します。

注意 この設定を有効にした後は、無効にすることはできません。無効にする必要がある場合は、サポートにお問い合わせください。

構文

```
system compliance enable ucapl
```

例

```
> system compliance enable ucapl
```

show

デバイスの現在のセキュリティ認定のコンプライアンス モードを表示します。

構文

```
system compliance show
```

例

```
> system compliance show
```

disable-http-user-cert

ブラウザに有効なクライアント証明書を提示させる要求事項を無効にします。

アクセス

Configuration

構文

```
system disable-http-user-cert
```

例

```
> system disable-http-user-cert
```

file コマンド

`system file` コマンドを使用すると、ユーザは、デバイス上の common ディレクトリにあるファイルを管理することができます。

アクセス

設定

copy

FTP を使用して、ログイン ユーザ名を使用しているホスト上のリモート ロケーションへファイルを転送します。ローカル ファイルは common ディレクトリに配置する必要があります。

構文

```
system file copy hostname username path filenames filenames ...
```

`hostname` はターゲットのリモート ホストの名前または IP アドレスを表します。`username` はリモート ホスト上のユーザの名前、`path` はリモート ホスト上の宛先パス、`filenames` は転送するローカル ファイルを表します。複数のファイル名はスペースで区切って指定します。

例

```
> system file copy sfrocks jdoe /pub *
```

削除

common ディレクトリから、指定したファイルを削除します。

構文

```
system file delete filenames filenames ...
```

`filenames` は削除するファイルを指定します。複数のファイル名はスペースで区切って指定します。

例

```
> system file delete *
```

list

ファイル名が指定されていない場合は、common ディレクトリ内のすべてのファイルについて変更の時刻、サイズ、およびファイル名が表示されます。ファイル名が指定されている場合は、指定されたファイル名と一致したファイルで、変更の時刻、サイズ、およびファイル名が表示されます。

構文

```
system file list filenames
```

filenames は表示するファイルを表します。複数のファイル名はスペースで区切って指定します。

例

```
> system file list
```

secure-copy

SCP を使用して、ログイン ユーザ名を使用しているホスト上のリモート ロケーションへファイルを転送します。ローカル ファイルは /var/common ディレクトリに配置する必要があります。

構文

```
system file secure-copy hostname username path filenames filenames ...
```

hostname はターゲットのリモート ホストの名前または IP アドレスを表します。*username* はリモート ホスト上のユーザの名前、*path* はリモート ホスト上の宛先パス、*filenames* は転送するローカル ファイルを表します。複数のファイル名はスペースで区切って指定します。

例

```
> system file secure-copy 10.123.31.1 jdoe /tmp *
```

generate-troubleshoot

シスコが解析に使用するトラブルシューティング データを生成します。

従来型デバイスのコマンド ライン リファレンス

注意 低メモリ デバイス用のトラブルシューティング ファイルを生成すると、自動アプリケーション バイパス（AAB）が有効になっている場合は AAB をトリガーすることができます。少なくとも、AAB をトリガーすると Snort プロセスを再開すると、一時的にトラフィック検査が中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、ターゲットデバイスがトラフィックを処理する方法に応じて異なります。詳細はSnort® の再起動によるトラフィックの動作（451 ページ）を参照してください。。そのような場合、AAB のトリガーによって、デバイスが一時的に動作不能な状態になることがあります。動作不能な状態が続く場合は Cisco Technical Assistance Center（TAC） に連絡してください。展開に適したソリューションをご提案します。影響を受けやすいデバイスは、Firepower 7010、7020、および 7030、ASA 5508-X、5515-X、5516-X および 5525-X、NGIPSv などです。

アクセス

Configuration

構文

```
system generate-troubleshoot option1 optionN
```

オプションが次の 1 つまたは複数の場合は、スペースで区切ります。

- `ALL`：次のすべてのオプションを実行します。
- `SNT`：Snort のパフォーマンスと設定
- `PER`: ハードウェアのパフォーマンスとログ
- `SYS`：システム設定、ポリシー、およびログ
- `DES`：検出設定、ポリシー、およびログ
- `NET`：インターフェイスとネットワーク関連データ
- `VDB`：検出、認知、VDB データ、およびログ
- `UPG`：データとログのアップグレード
- `DBO`：すべてのデータベース データ
- `LOG`：すべてのログ データ
- `NMP`：ネットワーク マップ情報

例

```
> system generate-troubleshoot VDB NMP
starting /usr/local/sf/bin/sf_troubleshoot.pl…
Please, be patient. This may take several minutes.
```

```
The troubleshoot options codes specified are VDB,NMP.
Getting filenames from [usr/local/sf/etc/db_updates/index]
Getting filenames from [usr/local/sf/etc/db_updates/base-6.2.3]
Troubleshooting information successfully created at
/var/common/results-06-14-2018—222027.tar.gz
```

ldapsearch

ユーザが、指定されたLDAPサーバのクエリを実行できるようにします。すべてのパラメータが必須であることに注意してください。

アクセス

Configuration

構文

```
system ldapsearch host port baseDN userDN basefilter
```

host は LDAP サーバのドメイン、port は LDAP サーバのポート、baseDN は検索する DN（識別名）、userDN は LDAP ディレクトリへバンドするユーザの DN、basefilter は検索するレコードを表します。

例

```
> system ldapsearch ldap.example.com 389 cn=users,

dc=example,dc=com cn=user1,cn=users,dc=example,dc=com, cn=user2
```

ロックダウン

`expert` コマンドを削除し、デバイス上の Linux シェルへアクセスします。

⚠

注意 このコマンドは、サポートからのホットフィックスがない場合は取り消すことはできません。使用には注意が必要です。

アクセス

Configuration

構文

```
system lockdown
```

例

```
> system lockdown
```

nat rollback

以前に適用していたNATの設定に、システムを戻します。このコマンドはNGIPSvまたはASA FirePOWER では使用できません。このコマンドをスタックまたは高可用性ペアのデバイスで使用することはできません。

アクセス

Configuration

構文

```
system nat rollback
```

例

```
> system nat rollback
```

renew-http-cert

必要に応じて新しいキーを使用して、システムで提供されるデフォルト HTTPS サーバ証明書を更新します。更新された証明書は 3 年間有効です。このコマンドは NGIPSv および ASA FirePOWER デバイスでは使用できません。

アクセス

Configuration

構文

```
system renew-http-cert [newkey]
```

例

```
> system renew-http-cert newkey
```

reboot

デバイスをリブートします。

アクセス

Configuration

構文

```
system reboot
```

例

```
> system reboot
```

restart

デバイスのアプリケーションを再起動します。

アクセス

Configuration

構文

```
system restart
```

例

```
> system restart
```

support コマンド

`system support` コマンドを使用することで、デバイス上の特殊な SSL ClientHello 処理を管理できます。

アクセス

設定

ssl-client-hello-display

SSL ハンドシェイク時に ClientHello メッセージを処理するための現在の設定を表示します。これらの設定の説明については、`ssl-client-hello-enabled` および `ssl-client-hello-tuning` コマンドを参照してください。

アクセス

Basic

構文

```
system support ssl-client-hello-display
```

例

```
> system support ssl-client-hello-display
```

ssl-client-hello-enabled

SSL ハンドシェイク時に ClientHello メッセージの特殊な処理を制御します。

⚠

注意 サポートからの指示がない限り、このコマンドは使用**しないで**ください。

アクセス

Configuration

構文

```
system support ssl-client-hello-enabled setting {true | false}
```

Setting に指定できる値は次のとおりです。

feature
ClientHello メッセージのすべての特殊な処理を制御します。

curves
Firepower システムでサポートされていない楕円曲線の削除を制御します。

- `true`（有効）：サポートされていないすべての楕円曲線を ClientHello メッセージから削除し、トラフィックの復号の確率が向上します。`extensions` 設定を有効にする必要もあります。
- `false`（無効）：ClientHello メッセージ内のサポートされていない楕円曲線を保持し、トラフィックの復号の確率が低下します。

ciphers
Firepower システムでサポートされていない暗号スイートの削除を制御します。

- `true`（有効）：サポートされていない暗号スイートを ClientHello メッセージから削除し、トラフィックの復号の確率が向上します。
- `false`（無効）：ClientHello メッセージ内のサポートされていない暗号スイートを保持します。これによりトラフィックの復号の確率が低下し、関連する接続イベントの SSL Flow Error フィールドで多数の `Unsupported` エラーや `Unknown Cipher` エラーが発生する可能性があります。

内線番号

復号を妨げる TLS 拡張の削除を制御します。

従来型デバイスのコマンド ライン リファレンス

- `true`（有効）：復号を妨げるTLS拡張を特定し、ClientHelloメッセージから削除します。**curves**、**session_ticket**、および**alpn**を有効にする場合、この値を指定する必要があります。
- `false`（無効）：ClientHelloメッセージ内のすべてのTLS拡張を保持します。これによりトラフィックの復号の確率が低下し、関連する接続イベントのSSL Flow Errorフィールドで`Unknown Session`エラーが発生する可能性があります。

session_ticket

ClientHelloメッセージのSessionTicket拡張の処理を制御します。システムが着信ClientHelloメッセージ内のSessionTicket値をキャッシュされたセッションデータと照合できる場合、クライアントとサーバで完全なSSLハンドシェイクが実行されなくてもセッションを再開できます。

- `true`（有効）：認識されないSessionTicket値をClientHelloメッセージから削除します。これにより、再開されたセッションでトラフィックの復号の確率が向上します。`extensions`設定を有効にする必要もあります。
- `false`（無効）：ClientHelloメッセージ内のすべてのSessionTicket値を保持します。これによりトラフィックの復号の確率が低下し、関連する接続イベントのSSL Flow Errorフィールドで`Uncached Session`エラーが発生する可能性があります。

session_id

ClientHelloメッセージのセッション識別子要素の処理を制御します。システムが着信ClientHelloメッセージ内のセッション識別子をキャッシュされたセッションデータと照合できる場合、クライアントとサーバで完全なSSLハンドシェイクが実行されなくてもセッションを再開できます。

- `true`（有効）：認識されないセッション識別子値をClientHelloメッセージから削除します。これにより、再開されたセッションでトラフィックの復号の確率が向上します。
- `false`（無効）：ClientHelloメッセージ内のすべてのセッション識別子値を保持します。これによりトラフィックの復号の確率が低下し、関連する接続イベントのSSL Flow Errorフィールドで`Uncached Session`エラーが発生する可能性があります。

alpn

復号できないALPNプロトコル値、特にSPDYおよびHTTP2プロトコルの削除を制御します。

- `true`（有効）：クライアントがSPDYまたはHTTP2セッションを確立することを禁止し、トラフィックの復号および検査の確率が向上します。`extensions`設定を有効にする必要もあります。
- `false`（無効）：クライアントがサーバとSPDYまたはHTTP2セッションを確立することを許可し、トラフィックの復号および検査の確率が低下します。

compression

ClientHelloメッセージからのTLS圧縮要求の削除を制御します。

- `true`（有効）：クライアントがサーバと TLS 圧縮セッションを確立することを禁止します。
- `false`（無効）：クライアントがサーバと TLS 圧縮セッションを確立することを許可します。これによりセッションのトラフィックの復号が妨げられ、関連する接続イベントの SSL Flow Error フィールドで `Compression Used` エラーが発生する可能性があります。

例

```
> system support ssl-client-hello-enabled feature false
```

ssl-client-hello-force-reset

デフォルト値に処理する ClientHello メッセージの設定可能な設定をリセットします。システムはユーザの確認を必要とせず続行します。

⚠

注意 サポートからの指示がない限り、このコマンドは使用**しないで**ください。

アクセス

Configuration

構文

```
system support ssl-client-hello-force-reset
```

例

```
> system support ssl-client-hello-force-reset
```

ssl-client-hello-reset

デフォルト値に処理する ClientHello メッセージの設定可能な設定をリセットします。システムは、続行する前にユーザの確認を必要とします。

⚠

注意 サポートからの指示がない限り、このコマンドは使用**しないで**ください。

アクセス

Configuration

構文

```
system support ssl-client-hello-reset
```

例

```
> system support ssl-client-hello-reset
```

ssl-client-hello-tuning

SSL ハンドシェイク時に管理対象デバイスが ClientHello メッセージをどのように変更するか調整できます。このコマンドは、ClientHello メッセージで許可される暗号スイート、楕円曲線、および拡張のデフォルト リストを調整します。このコマンドは、許可される値のデフォルト リストにエントリを追加するか、許可される値のデフォルト リストからエントリを削除するだけです。デフォルト リストは上書きされません。

⚠

注意 サポートからの指示がない限り、このコマンドは使用**しないで**ください。

アクセス

Configuration

構文

```
system support ssl-client-hello-tuning setting value
```

value 要素は値のカンマ区切りのリストをサポートします。*setting* および *value* 要素の設定可能な値には次が含まれます。

設定	システムのアクション	値
`ciphers_allow`	ClientHello メッセージで指定された暗号スイートを許可します。このコマンドを使用すると、システムは変更するすべての ClientHello メッセージで指定された暗号スイートを保持します。	IANA の Web サイトから個々の暗号スイートの数を取得します。 https://www.iana.org/assignments/tls-parameters/tls-parameters.xhtml#tls-parameters-4 IANA は 16 進数の値を提供します。このコマンドを使用してそれらを 10 進数に変換します。
`ciphers_remove`	ClientHello メッセージで指定された暗号スイートを拒否します。このコマンドを使用すると、システムは変更するすべての ClientHello メッセージから指定された暗号スイートを削除します。	

設定	システムのアクション	値
curves_allow	ClientHello メッセージで指定された楕円曲線を許可します。このコマンドを使用すると、システムは変更するすべての ClientHello メッセージで指定された楕円曲線を保持します。	IANA の Web サイトから曲線の数を取得します。https://www.iana.org/assignments/tls-parameters/tls-parameters.xhtml#tls-parameters-8
curves_remove	ClientHello メッセージで指定された楕円曲線を拒否します。このコマンドを使用すると、システムは変更するすべての ClientHello メッセージから指定された楕円曲線を削除します。	
extensions_allow	ClientHello メッセージで指定された拡張を許可します。このコマンドを使用すると、システムは変更するすべての ClientHello メッセージで指定された拡張を保持します。	IANA の Web サイトから拡張の数を取得します。https://www.iana.org/assignments/tls-extensiontype-values/tls-extensiontype-values.xhtml
extensions_remove	ClientHello メッセージで指定された楕円曲線を拒否します。システムは変更するすべての ClientHello メッセージから指定された拡張を削除します。デフォルトでは、システムは拡張 22、23、および 30032 を拒否します。	

例

```
> system support ssl-client-hello-tuning ciphers_allow 4,7,16,22
```

shutdown

デバイスをシャットダウンします。このコマンドは ASA FirePOWER モジュールでは使用できません。

アクセス

Configuration

構文

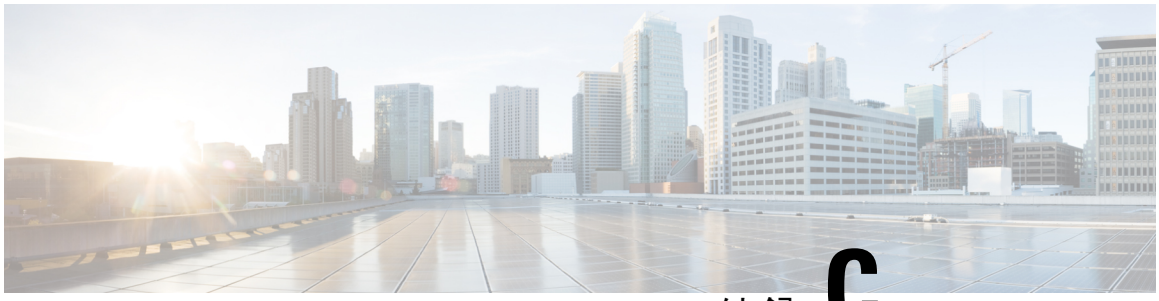
```
system shutdown
```

例

```
> system shutdown
```

クラッシク デバイスの CLI の履歴

機能	バージョン	詳細
HTTPS 証明書	6.3	現在、システムとともに提供されるデフォルトの HTTPS サーバ クレデンシャルは 3 年で期限が切れます。バージョン 6.3 にアップグレードする前に生成されたデフォルト証明書をアプライアンスが使用している場合、証明書は最初に生成されたときから 20 年後に期限切れとなります。デフォルトの HTTPS サーバ証明書を使用している場合、システムはその証明書を更新する機能を提供しています。 新しいクラシック CLI コマンド：**show http-cert-expire date**、**system renew-http-cert** サポートされるプラットフォーム：物理 FMC、7000 および 8000 シリーズ デバイス
クラシック CLI コマンドの `system lockdown-sensor` シンタックス。	6.3	クラシック CLI の **system lockown-sensor** コマンドは、**system lockdown** に変更されました。



付録 C

Firepower Management Center のコマンド ライン リファレンス

このリファレンスでは、Firepower Management Center のコマンドライン インターフェイス（CLI）について説明します。

（注） 従来型デバイス（7000 および 8000 シリーズ、ASA FirePOWER、NGIPSv）の場合は、従来型デバイスのコマンド ライン リファレンス （3289 ページ）を参照してください。

（注） Firepower Threat Defense については、Cisco Firepower Threat Defense コマンド リファレンスを参照してください。

Firepower Management Center CLI について

`admin` ユーザ ロールを持つユーザによって有効にされた場合にのみ、Firepower Management Center CLI が使用できます。

- デフォルトでは CLI は有効になっておらず、CLI/シェル アカウントを使用して Firepower Management Center にログインしたユーザは Linux シェルに直接アクセスできます。
- CLI が有効になっている場合、シェル/CLI アカウントを使用して Firepower Management Center にログインしたユーザは CLI にアクセスでき、Linux シェルにアクセスするには `expert` コマンドを使用する必要があります。

⚠

注意 Cisco TAC または Firepower ユーザ マニュアルの明示的な手順による指示がない限り、Linux シェルにアクセスしないことを強くお勧めします。

⚠

注意 Linux シェルへのアクセス権があるユーザはルート権限を取得できるため、セキュリティ上のリスクが生じる可能性があります。システム セキュリティ上の理由から、次の点を強くお勧めします。

- 外部認証を確立した場合は、Linux シェル アクセスが付与されるユーザのリストを適切に制限してください。
- 事前定義された `admin` ユーザに加えて、Linux シェル ユーザを確立しないでください。

CLI が有効になっている場合、この付録で説明されているコマンドを使用して Firepower Management Center を表示してトラブルシューティングを行うとともに、限定された設定操作を実行できます。

Firepower Management Center CLI モード

CLI には 4 つのモードが含まれています。デフォルト モードである CLI 管理には、CLI 自体の内部を移動するためのコマンドが含まれています。残りのモードには、Firepower Management Center の機能の 3 つの異なる領域に対処するコマンドが含まれています。これらのモード内のコマンドは、モード名の`system`ム、`show`、または `configure` で始まります。

モードを入力すると、CLI は、現在のモードを反映するように変更を求められます。たとえば、システム コンポーネントのバージョン情報を表示するには、標準 CLI プロンプトに完全なコマンドを入力します。

```
> show version
```

これまでに `show` モードに入ったことがある場合は、show モードの CLI プロンプトで `show` キーワードを使用せずにコマンドを入力できます。

```
show> version
```

Firepower Management Center CLI の有効化

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
該当なし	いずれか（Any）	FMC	いずれか（Any）	`admin`

Firepower Management Center の CLI をいったん有効にすると、管理インターフェイスにログインしているユーザのアプライアンスへの初回アクセスは CLI 経由となります。Linux シェルには `expert` コマンドを使用してのみアクセスできます。

（注） 管理者が `system lockdown` コマンドを使用してデバイス シェルへのアクセスを無効にした場合は、[CLI アクセスの有効化（Enable CLI Access）] チェック ボックスがオンになり、グレー表示されます。

ステップ 1 **[System]** > **[Configuration]**を選択します。

ステップ 2 [コンソール構成（Console Configuration）] をクリックします。

ステップ 3 Firepower Management Center CLI を有効または無効にするには、[CLI アクセスの有効化（Enable CLI Access）] チェックボックスをオンまたはオフにします。

ステップ 4 **[保存（Save）]** をクリックします。

Firepower Management Center CLI 管理コマンド

CLI 管理コマンドを使用して、CLI とやりとりすることができます。これらのコマンドはデバイスの処理に影響しません。

exit

CLI コンテキストを、次に高い CLI コンテキスト レベルへ移動します。デフォルト モードからこのコマンドを発行すると、ユーザは現行の CLI セッションからログアウトします。

構文

```
exit
```

例

```
system> exit
>
```

expert

Linux シェルを起動します。

構文

```
expert
```

例

```
> expert
```

? （疑問符）

CLI コマンドおよびパラメータの状況依存ヘルプを表示します。次のように、疑問符（?）のコマンドを使用します。

- 現在の CLI コンテキスト内で使用できるコマンドのヘルプを表示するには、コマンド プロンプトで疑問符（?）を入力します。
- 特定文字セットから始まる使用可能なコマンドのリストを表示するには、疑問符（?）に続けて短縮されたコマンドを入力します。
- コマンドの正式な引数のヘルプを表示するには、コマンドプロンプトの引数の代わりに疑問符（?）を入力します。

疑問符（?）は、コンソールにエコーバックされないことに注意してください。

構文

```
?
abbreviated_command ?
command [arguments] ?
```

例

```
> ?
```

Firepower Management Center CLI の show コマンド

Show コマンドは、アプライアンスの状態に関する情報を提供します。これらのコマンドはアプライアンスの動作モードを変更しません。また、これらのコマンドを実行しても、システムの動作に対する影響は最小限になります。

version

製品のバージョンとビルドを表示します。

構文

```
show version
```

例

```
> show version
```

Firepower Management Center CLI 設定コマンド

コンフィギュレーション コマンドを使用して、システムを設定および管理することができます。これらのコマンドはシステムの動作に影響を与えます。

password

現在の CLI/シェル ユーザは自身のパスワードを変更できます。

⚠

注意 システム セキュリティ上の理由により、いかなるアプライアンスでも、事前定義された **admin** に加えて、Linux シェル ユーザを確立しないことをお勧めします。

コマンドを発行すると、CLI は現在の（古い）パスワードを入力するようユーザに要求し、その後で新しいパスワードを 2 回入力するよう要求します。

構文

```
configure password
```

例

```
> configure password
Changing password for admin.
(current) UNIX password:
New UNIX password:
Retype new UNIX password:
passwd: password updated successfully
```

Firepower Management Center CLI システム コマンド

system コマンドを使用して、システム全体のファイルおよびアクセス コントロールの設定を管理することができます。

generate-troubleshoot

シスコが解析に使用するトラブルシューティング データを生成します。

構文

```
system generate-troubleshoot option1 optionN
```

オプションが次の 1 つまたは複数の場合は、スペースで区切ります。

- ALL：次のすべてのオプションを実行します。
- SNT：Snort のパフォーマンスと設定
- PER: ハードウェアのパフォーマンスとログ
- SYS：システム設定、ポリシー、およびログ
- DES：検出設定、ポリシー、およびログ
- NET：インターフェイスとネットワーク関連データ
- VDB：検出、認知、VDB データ、およびログ
- UPG：データとログのアップグレード
- DBO：すべてのデータベース データ
- LOG：すべてのログ データ
- NMP：ネットワーク マップ情報

例

```
> system generate-troubleshoot VDB NMP
starting /usr/local/sf/bin/sf_troubleshoot.pl…
Please, be patient. This may take several minutes.
The troubleshoot options codes specified are VDB,NMP.
Getting filenames from [usr/local/sf/etc/db_updates/index]
Getting filenames from [usr/local/sf/etc/db_updates/base-6.2.3]
Troubleshooting information successfully created at
/var/common/results-06-14-2018—222027.tar.gz
```

lockdown

expert コマンドを削除し、デバイス上の Linux シェルへアクセスします。

⚠

注意 このコマンドは、サポートからのホットフィックスがない場合は取り消すことはできません。使用には注意が必要です。

構文

```
system lockdown
```

例

```
> system lockdown
```

reboot

アプライアンスのリブート。

構文

```
system reboot
```

例

```
> system reboot
```

restart

アプライアンス アプリケーションを再起動します。

構文

```
system restart
```

例

```
> system restart
```

shutdown

アプライアンスをシャット ダウンします。

構文

```
system shutdown
```

例

```
> system shutdown
```

Firepower Management Center CLI の履歴

機能	バージョン	詳細
のCLIアクセスを有効化および無効化する機能 FMC	6.3	新しい/変更された画面： FMC の Web インターフェイスで管理者が使用可能な新しいチェックボックス：**[System]** > **[Configuration]** の [CLI アクセスの有効化（Enable CLI Access）] > [コンソール設定（Console Configuration）] ページ。 • オン： SSH を使用して FMC にログインすると CLI にアクセスします。 • オフ：SSH を使用して FMC にログインすると Linux シェルにアクセスします。これは、バージョン 6.3 の新規インストールと、以前のリリースからバージョン 6.3 にアップグレードした場合のデフォルトの状態です。 サポートされるプラットフォーム FMC
FMC CLI	6.3	導入された機能。 最初にサポートされているコマンドは次のとおりです。 • `exit` • `expert` • `?` • `show version` • `configure password` • `system generate-troubleshoot` • `system lockdown` • `system reboot` • `system restart` • `system shutdown` サポートされるプラットフォーム FMC