システム設定（System Configuration）

以下のトピックでは、Firepower Management Center および管理対象デバイスでシステム設定を行う方法について説明します。

- システム設定の概要 （2 ページ）
- アプライアンス情報 （5 ページ）
- HTTPS 証明書 （7 ページ）
- 外部データベース アクセスの設定 （13 ページ）
- データベース イベント数の制限 （15 ページ）
- 管理インターフェイス （17 ページ）
- システムのシャットダウンと再起動 （36 ページ）
- リモート ストレージ管理 （38 ページ）
- 変更調整 （43 ページ）
- ポリシー変更のコメント （45 ページ）
- アクセス リスト （46 ページ）
- 監査ログ （48 ページ）
- 監査ログ証明書 （51 ページ）
- ダッシュボード設定 （58 ページ）
- DNS キャッシュ （59 ページ）
- 電子メールの通知 （60 ページ）
- 言語の選択 （62 ページ）
- ログイン バナー （63 ページ）
- SNMP ポーリング （64 ページ）
- セキュリティ認定準拠の （67 ページ）
- 時刻および時刻同期 （71 ページ）
- セッション タイムアウト （76 ページ）
- 脆弱性マッピング （78 ページ）
- リモート コンソールのアクセス管理 （79 ページ）
- REST API 設定 （86 ページ）
- VMware Tools と仮想システム （87 ページ）

システム設定の概要

システム設定の設定値は、Firepower Management Center またはクラシック管理対象デバイス（7000 および 8000 シリーズ、ASA FirePOWER、NGIPSv）のいずれかに適用されます。

- Firepower Management Center では、これらの構成設定は「ローカル」のシステム設定の一部です。Firepower Management Center 上のシステム設定は単一システムに固有のものであり、Management Center のシステム設定への変更はそのシステムのみに影響する点に注意してください。
- クラシック管理対象デバイスでは、プラットフォーム設定ポリシーの一部として Firepower Management Center から設定を適用します。共有ポリシーを作成して、展開全体で同様の設定になっている可能性の高い、管理対象デバイスに最適なシステム設定の設定値のサブセットを設定します。

ヒント　7000 および 8000 シリーズ デバイスでは、ローカル Web インターフェイスからコンソール設定やリモート管理などのシステム設定の制限付きタスクを実行できます。これらは、プラットフォーム設定ポリシーを使用して 7000 または 8000 シリーズ デバイスに適用される設定とは異なります。

Firepower Management Center システム設定のナビゲーション

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	Management Center	グローバルだけ	Admin

システム設定により、Firepower Management Center の基本設定を特定します。

手順

ステップ 1　**[システム（System）] > [設定（Configuration）]**を選択します。

ステップ 2　ナビゲーション ウィンドウを使用して、変更する設定を選択します。詳細については、表 1 : システム設定 （3 ページ）を参照してください。

システム設定

次の表に Firepower Management Center のシステム設定の説明を示します。この表では、7000 および 8000 シリーズ デバイスについて、デバイスのローカル Web インターフェイスから構成する設定、および Firepower Management Center から展開したプラットフォーム設定ポリシーを使用して構成する設定も示します。

表 *1*：システム設定

設定	説明	他の設定元	
		プラットフォーム設定	7000 & 8000 シリーズ
情報	アプライアンスに関する最新情報を表示し、表示名を編集します。アプライアンス情報 （5 ページ）を参照してください。	No	Yes
HTTPS Certificate	必要に応じて、信頼できる認証局の HTTPS サーバ証明書を要求し、システムに証明書をアップロードします。HTTPS 証明書 （7 ページ）を参照してください。	No	Yes
外部データベース アクセス	データベースへの外部読み取り専用アクセスを有効にし、ダウンロードするクライアント ドライバを提供します。外部データベース アクセスの設定 （13 ページ）を参照してください。	No	No
データベース	Firepower Management Center が保存できる各イベントのタイプの最大数を指定します。データベース イベント数の制限 （15 ページ）を参照してください。	No	No
管理インターフェイス	アプライアンスの IP アドレス、ホスト名、プロキシ設定などのオプションを変更します。管理インターフェイス （17 ページ）を参照してください。	No	Yes
プロセス	Firepower システム関連のプロセスをシャットダウン、リブート、または再起動します。システムのシャットダウンと再起動 （36 ページ）を参照してください。	No	Yes
リモート ストレージ デバイス	バックアップとレポート用のリモート ストレージ デバイスを設定します。リモート ストレージ管理 （38 ページ）を参照してください。	No	No
リコンサイルの変更	過去 24 時間にわたるシステムへの変更の詳細なレポートを送信するようにシステムを設定します。変更調整 （43 ページ）を参照してください。	No	Yes
アクセス コントロールの設定	ユーザがアクセス コントロール ポリシーを追加または変更する際にユーザにコメントを要求するようにシステムを設定します。ポリシー変更のコメント （45 ページ）を参照してください。	No	No

設定	説明	他の設定元	
		プラットフォーム設定	7000 & 8000 シリーズ
アクセス リスト	どのコンピュータが特定のポートでシステムにアクセスできるかを制御します。アクセス リスト （46 ページ）を参照してください。	Yes	No
監査ログ	外部ホストに監査ログを送信するようにシステムを設定します。監査ログ （48 ページ）を参照してください。	Yes	No
監査ログ クライアント証明書	監査ログを外部ホストにストリーミングする際にチャネルを保護するようにシステムを設定します。次を参照してください。 監査ログ証明書（51 ページ）	Yes	Yes
ダッシュボード	ダッシュボードのカスタム分析ウィジェットを有効にします。ダッシュボード設定 （58 ページ）を参照してください。	No	No
DNS キャッシュ	イベント表示ページで IP アドレスを自動的に解決するようにシステムを設定します。DNS キャッシュ （59 ページ）を参照してください。	No	No
電子メール通知	メール ホストを設定し、暗号化方式を選択して、電子メールベースの通知とレポートに認証クレデンシャルを提供します。電子メールの通知（60 ページ）を参照してください。	No	No
外部認証（External Authentication）	外部 RADIUS、LDAP、または Microsoft Active Directory のリポジトリによって認証されるユーザのデフォルト ユーザ ロールを設定します。を参照してください。 外部認証の設定	Yes	No
侵入ポリシーの設定	ユーザが侵入ポリシーを変更する際にユーザにコメントを要求するようにシステムを設定します。ポリシー変更のコメント （45 ページ）を参照してください。	No	No
[言語（Language）]	Web インターフェイスに異なる言語を指定します。言語の選択 （62 ページ）を参照してください。	Yes	No
ログイン バナー	ユーザがログインすると表示されるカスタム ログイン バナーを作成します。ログイン バナー （63 ページ）を参照してください。	Yes	No
ネットワーク分析ポリシーの設定	ユーザがネットワーク分析ポリシーを変更する際にユーザにコメントを要求するようにシステムを設定します。ポリシー変更のコメント （45 ページ）を参照してください。	No	No
SNMP	Simple Network Management Protocol （SNMP）のポーリングを有効にします。SNMP ポーリング （64 ページ）を参照してください。	Yes	No

設定	説明	他の設定元	
		プラットフォーム設定	7000 & 8000 シリーズ
UCAPL/CC コンプライアンス	米国国防総省によって設定される特定の要件の順守を有効にします。セキュリティ認定コンプライアンスの有効化 （69 ページ）を参照してください。	Yes	No
時刻（Time）	現在の時刻設定を確認し、現在のシステム設定の時刻同期の設定が[ローカル設定で手動（Manually in Local Configuration）] に設定されている場合は、時間を変更します。時刻および時刻同期 （71 ページ）を参照してください。	No	Yes
時刻の同期	システムの時刻の同期を管理します。時刻および時刻同期 （71 ページ）を参照してください。	Yes	No
シェル タイムアウト	ユーザのログイン セッションが非アクティブによりタイムアウトするまでのアイドル時間の長さを分単位で設定します。セッション タイムアウト （76 ページ）を参照してください。	Yes	No
脆弱性マッピング	ホスト IP アドレスから送受信されるアプリケーション プロトコル トラフィックの脆弱性をそのホストIPアドレスにマップします。脆弱性マッピング （78 ページ）を参照してください。	No	No
コンソール設定	VGA またはシリアル ポート経由、または Lights-Out Management（LOM）経由のコンソール アクセスを設定します。リモート コンソールのアクセス管理 （79 ページ）を参照してください。	No	制限付き
REST API 設定	Firepower REST API 経由の Firepower Management Center へのアクセスを有効または無効にします。REST API 設定 （86 ページ）を参照してください。	No	No
VMware ツール	VMware ツールを有効にして Firepower Management Center Virtual で使用します。VMware Tools と仮想システム （87 ページ）を参照してください。	適用対象外	適用対象外

関連トピック

Firepower プラットフォーム設定の概要

アプライアンス情報

Web インターフェイスの [情報（Information）] ページには、次の表に示す情報が含まれています。別途記載のない限り、フィールドはすべて読み取り専用です。

フィールド	説明
[名前（Name）]	アプライアンスに割り当てられた名前。この名前はFirepowerシステムのコンテキスト内でのみ使用されることに注意してください。ホスト名をアプライアンスの名前として使用できますが、このフィールドに別の名前を入力しても、ホスト名が変更されることはありません。
製品モデル（Product Model）	アプライアンスのモデル名。
シリアル番号（Serial Number）	アプライアンスのシリアル番号。
ソフトウェア バージョン（Software Version）	アプライアンスに現在インストールされているソフトウェアのバージョン。
Firepower Management Centerへのパケット転送の禁止（Prohibit Packet Transfer to the ）	管理対象デバイスがイベントに合わせてパケット データを送信し、Firepower Management Center上にデータを保存するかを指定します。この設定は、7000および8000シリーズ デバイスのローカルWebインターフェイスで使用できます。
オペレーティング システム（Operating System）	アプライアンス上で現在実行されているオペレーティング システム。
オペレーティング システム バージョン（Operating System Version）	アプライアンス上で現在実行されているオペレーティング システムのバージョン。
IPv4 アドレス（IPv4 Address）	デフォルト管理インターフェイス（`eth0`）のIPv4 アドレス。IPv4 の管理が無効になっている場合は、このフィールドにそのことが示されます。
IPv6 アドレス（IPv6 Address）	デフォルト管理インターフェイス（`eth0`）のIPv6 アドレス。IPv6 の管理が無効になっている場合は、このフィールドに表示されます。
現在のポリシー（Current Policies）	現在展開されているシステム レベルのポリシー。ポリシーが最後に適用された後で更新されていると、ポリシー名がイタリック体で表示されます。
モデル番号（Model Number）	内部フラッシュ ドライブに保存されているアプライアンス固有のモデル番号。この番号は、トラブルシューティングで重要になる場合があります。

システム情報の表示および変更

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス
任意（Any）	任意（Any）	Management Center 7000 & 8000 シリーズ	グローバルだけ	Admin

Firepower Management Center の Web インターフェイスまたは 7000 および 8000 シリーズ ローカル Web インターフェイスの情報ページでは、製品名やモデル番号など、読み取り専用の情報を含むシステムについての情報を提供します。このページでは、システムの表示名の変更を変更することもできます。また、7000 および 8000 シリーズ デバイスの場合、パケット転送を禁止する機能もあります。

（注） パケット転送を禁止することは、侵入ポリシー違反をトリガーしたパケットの具体的な内容について気にする必要がない低帯域幅の展開で、効果を発揮する可能性があります。

手順

ステップ 1 **[システム（System）] > [設定（Configuration）]**を選択します。

ステップ 2 オプションで、以下のシステム情報の設定を変更します。

- 名前：表示名を変更するには、[名前（Name）] フィールドに名前を入力します。
- パケット転送の禁止：Firepower Management Center にパケット データを送信しないようにするには、[管理センターへのパケット転送を禁止する（Prohibit Packet Transfer to the Management Center）] チェックボックスをオンにします。このオプションは、7000 または 8000 シリーズ デバイスのローカル Web インターフェイスでのみ使用できます。

ステップ 3 [保存（Save）] をクリックします。

HTTPS 証明書

Firepower Management Center および 7000 および 8000 シリーズ デバイスは、セキュア ソケット レイヤ（SSL）証明書によりシステムと Web ブラウザ間に暗号化チャネルを確立することができます。すべての Firepower デバイスにデフォルト証明書が含まれていますが、これはグローバル レベルで既知の CA から信頼された認証局（CA）によって生成された証明書ではありません。したがって、デフォルト証明書ではなく、グローバル レベルで既知の CA または内部で信頼された CA 署名付きのカスタム証明書の使用を検討してください。

⚠

注意 Firepower Management Center は 4096 ビット HTTPS 証明書をサポートしています。Firepower Management Center で使用する証明書が 4096 ビットを超える公開サーバ キーを使用して生成されている場合、Management Center Web インターフェイスにログインできません。HTTPS 証明書のバージョン 6.0.0 への更新の詳細については、*Firepower System Release Notes, Version 6.0* の「Update Management Center HTTPS Certificates to Version 6.0」を参照してください。HTTPS 証明書を生成またはインポートしても Management Center Web インターフェイスにログインできない場合は、サポート窓口にご連絡ください。

デフォルト HTTPS サーバ証明書

アプライアンスに提供されるデフォルトサーバ証明書を使用する場合、Webインターフェイスのアクセスに有効な HTTPS クライアント証明書が必要になるようにシステムを設定しないでください。これは、デフォルトサーバ証明書が、クライアント証明書に署名する CA によって署名されないためです。

カスタム HTTPS サーバ証明書

Firepower Management Center Web インターフェイスを使用して、システム情報と指定した ID 情報に基づいて、サーバ証明書要求を生成できます。ブラウザによって信頼されている内部認証局（CA）がインストールされている場合は、この要求を使用して証明書に署名することができます。生成された要求を認証局に送信して、サーバ証明書を要求することもできます。認証局（CA）から署名付き証明書を取得すると、その証明書をインポートできます。

HTTP クライアント証明書

クライアント ブラウザの証明書チェック機能を使用して、Firepower システムの Web サーバへのアクセスを制限できます。ユーザ証明書を有効にすると、Web サーバはユーザのブラウザ クライアントで有効なユーザ証明書が選択されていることを確認します。そのユーザ証明書は、サーバ証明書で使用されているのと同じ信頼できる認証局によって生成されている必要があります。以下の状況ではいずれの場合もブラウザは Web インターフェイスをロードできません。

- ユーザがブラウザに無効な証明書を選択する。
- ユーザがブラウザにサーバ証明書に署名した認証局が生成していない証明書を選択する。
- ユーザがブラウザにデバイスの証明書チェーンの認証局が生成していない証明書を選択する。

クライアントブラウザ証明書を確認するには、システムを設定してオンライン証明書ステータス プロトコル（OCSP）を使用するか、1 つ以上の証明書失効リスト（CRL）ファイルをロードします。OCSP を使用する場合、Web サーバは接続要求を受信すると、接続を確立する前に認証局と通信して、クライアント証明書の有効性を確認します。サーバに 1 つ以上の CRL をロー

ドするよう設定する場合、Web サーバはクライアント証明書を CRL の一覧に照らして比較します。ユーザが CRL にある失効した証明書の一覧に含まれる証明書を選択した場合、ブラウザは Web インターフェイスをロードできません。

（注） CRL を使用した証明書の確認を選択すると、システムはクライアント ブラウザ証明書、監査ログ サーバ証明書の両方の検証に同じ CRL を使用します。

現在の HTTPS サーバ証明書の表示

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス
任意（Any）	任意（Any）	Management Center 7000 および 8000 シリーズ	グローバルだけ	Admin

ログインしているアプライアンスのサーバ証明書のみを表示できます。

手順

ステップ 1 **[システム（System）] > [設定（Configuration）]**を選択します。

ステップ 2 [HTTPS Certificate] をクリックします。

HTTPS サーバの証明書署名要求の作成

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
該当なし	任意（Any）	Management Center 7000 および 8000 シリーズ	グローバルだけ	Admin

ローカル構成の [HTTPS 証明書（HTTPS Certificate）] ページから、この手順を使用して証明書要求を生成する場合は、1 つのシステムに対して 1 つの証明書しか生成できません。広く知られている CA または内部的に信頼できる CA によって署名されていない証明書をインストールすると、Webインターフェイスに接続しようとするとブラウザにセキュリティ警告が表示されます。

証明書要求用に生成されるキーは、ベース 64 エンコードの PEM 形式です。

手順

ステップ 1 **[システム（System）] > [設定（Configuration）]**を選択します。

ステップ 2 [HTTPS Certificate] をクリックします。

ステップ 3 [新規 CSR の生成（Generate New CSR）] をクリックします。

ステップ 4 [国名（2 文字のコード）（Country Name (two-letter code)）] フィールドに国番号を入力します。

ステップ 5 [都道府県（State or Province）] フィールドに、都道府県名を入力します。

ステップ 6 [市区町村（Locality or City）] を入力します。

ステップ 7 [組織（Organization）] の名前を入力します。

ステップ 8 [組織単位（部署名）（Organizational Unit (Department)）] の名前を入力します。

ステップ 9 [共通名（Common Name）] フィールドに、証明書を要求するサーバの完全修飾ドメイン名を入力します。

（注） [共通名（Common Name）] フィールドには、証明書に表示されるとおりに、サーバの完全修飾ドメイン名を正確に入力する必要があります。共通名と DNS ホスト名が一致していないと、アプライアンスへの接続時に警告が表示されます。

ステップ 10 [生成（Generate）] をクリックします。

ステップ 11 テキスト エディタを開きます。

ステップ 12 証明書要求のテキストブロック全体（`BEGIN CERTIFICATE REQUEST` 行と `END CERTIFICATE REQUEST` 行を含む）をコピーして、空のテキスト ファイルに貼り付けます。

ステップ 13 このファイルを *servername*`.csr` として保存します。*servername* は証明書を使用するサーバの名前です。

ステップ 14 [閉じる（Close）] をクリックします。

次のタスク

- 証明機関に証明書要求を送信します。
- 署名された証明書を受け取ったら、Firepower Management Center にインポートします。#unique_1203を参照してください。

HTTPS サーバ証明書のインポート

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス
任意（Any）	任意（Any）	Management Center 7000 および 8000 シリーズ	グローバルだけ	Admin

証明書を生成した署名認証局から中間 CA を信頼するように要求された場合は、証明書チェーン（証明書パス）も提供する必要があります。

クライアント証明書が必要な場合、サーバ証明書が次に示すいずれかの条件を満たしていないときに、Web インターフェイス経由でのアプライアンスへのアクセスに失敗します。

- 証明書が、クライアント証明書に署名したものと同じ CA によって署名されている。
- 証明書が、証明書チェーンの中間証明書に署名したものと同じ CA によって署名されている。

注意 Firepower Management Center は 4096 ビット HTTPS 証明書をサポートしています。Firepower Management Center で使用する証明書が 4096 ビットを超える公開サーバ キーを使用して生成されている場合、Management Center Web インターフェイスにログインできません。HTTPS 証明書のバージョン 6.0.0 への更新の詳細については、*Firepower System Release Notes, Version 6.0* の「Update Management Center HTTPS Certificates to Version 6.0」を参照してください。HTTPS 証明書を生成またはインポートしていて、Management Center の Web インターフェイスにログインできない場合は、サポートまでお問い合わせください。

始める前に

- 証明書署名要求を生成します。HTTPS サーバの証明書署名要求の作成 （9 ページ）を参照してください。
- この CSR ファイルを証明書の要求先となる認証局にアップロードするか、この CSR を使用して自己署名証明書を作成します。

手順

ステップ 1 **[システム（System）] > [設定（Configuration）]**を選択します。

ステップ 2 [HTTPS Certificate] をクリックします。

ステップ 3 [HTTPSサーバ証明書のインポート（Import HTTPS Server Certificate）] をクリックします。

ステップ 4 テキスト エディタでサーバ証明書を開いて、`BEGIN CERTIFICATE` の行と `END CERTIFICATE` の行を含むテキストのブロック全体をコピーします。このテキストを [サーバ証明書（Server Certificate）] フィールドに貼り付けます。

ステップ 5 **秘密キー**を指定する必要があるかどうかは、証明書署名要求の生成方法によって異なります。

- Firepower Management Center Web インターフェイスを使用して証明書署名要求を生成した場合（HTTPS サーバの証明書署名要求の作成 （9 ページ）に記載）、システムにはすでに秘密キーがあるため、ここで入力する必要はありません。
- 他の方法を使用して証明書署名要求を生成した場合、ここで秘密キーを指定する必要があります。秘密キー ファイルを開いて、`BEGIN RSA PRIVATE KEY` の行と `END RSA PRIVATE KEY` の行を含むテキストのブロック全体をコピーします。このテキストを [秘密キー（Private Key）] フィールドに貼り付けます。

ステップ 6 必要な中間証明書をすべて開いて、それぞれのテキストのブロック全体をコピーして、[証明書チェーン（Certificate Chain）] フィールドに貼り付けます。

ステップ 7 [保存（Save）] をクリックします。

有効な HTTPS クライアント証明書の強制

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス
任意（Any）	任意（Any）	Management Center 7000 および 8000 シリーズ	グローバルだけ	Admin

システムは、OCSP または PEM（Privacy-enhanced Electronic Mail）形式でインポートされた CRL を使用した HTTPS クライアント証明書の検証をサポートしています。

CRL を使用する場合は、失効した証明書のリストを最新の状態に保つために、CRL を更新するスケジュールタスクを作成してください。システムは、最後に更新した CRL を表示します。

（注） クライアント認証を有効にした後で Web インターフェイスにアクセスするには、ブラウザに有効なクライアント証明書が存在している（またはリーダーに CAC が挿入されている）**必要があります**。

始める前に

- 接続に使用するクライアント証明書に署名したものと同じ認証局で署名されたサーバ証明書をインポートします。HTTPS サーバ証明書のインポート （10 ページ）を参照してください。
- サーバ証明書チェーンをインポートします（必要な場合）。#unique_1203を参照してください。

手順

ステップ 1 **[システム（System）] > [設定（Configuration）]**を選択します。

ステップ 2 [HTTPS Certificate] をクリックします。

ステップ 3 [クライアント証明書の有効化（Enable Client Certificates）] を選択します。プロンプトが表示されたら、ドロップダウンリストから該当する証明書を選択します。

ステップ 4 次の 3 つのオプションがあります。

- 1 つ以上の CRL を使用してクライアント証明書を検証する場合は、[CRL のフェッチの有効化（Enable Fetching of CRL）] を選択して、手順 5 に進みます。
- OCSP を使用してクライアント証明書を検証する場合は、[OCSPの有効化（Enable OCSP）] を選択して、手順 7 に進みます。
- 失効の確認なしでクライアント証明書を承認する場合は、手順 8 に進みます。

ステップ 5 既存の CRL ファイルへの有効な URL を入力して、[CRL の追加（Add CRL）] をクリックします。最大 25 個まで CRL の追加を繰り返します。

ステップ 6 [CRL の更新（Refresh CRL）] をクリックして現在の CRL をロードするか、指定した URL から CRL をロードします。

（注） CRL のフェッチを有効にすると、定期的に CRL を更新するスケジュール タスクが作成されます。このタスクを編集して、更新の頻度を設定します。

ステップ 7 クライアント証明書がアプライアンスにロードされた認証局によって署名されていることと、サーバ証明書がブラウザの証明書ストアにロードされている認証局によって署名されていることを確認します。（これらは同じ認証局であることが必要です）。

注意 有効化したクライアント証明書で設定を保存している場合、ブラウザの証明書ストアに有効なクライアント証明書がないと、アプライアンスへの Web サーバ アクセスがすべて無効になります。設定を保存する前に、有効なクライアント証明書がインストールされていることを確認してください。

ステップ 8 **[保存]** をクリックします。

関連トピック

証明書失効リストのダウンロードの設定

外部データベース アクセスの設定

サードパーティ製クライアントによるデータベースへの読み取り専用アクセスを許可するように、Firepower Management Center を設定できます。これによって、次のいずれかを使用して SQL でデータベースを照会できるようになります。

- 業界標準のレポート作成ツール（Actuate BIRT、JasperSoft iReport、Crystal Reports など）
- JDBC SSL 接続をサポートするその他のレポート作成アプリケーション（カスタム アプリケーションを含む）
- シスコが提供する RunQuery と呼ばれるコマンドライン型 Java アプリケーション（インタラクティブに実行することも、1 つのクエリの結果をカンマ区切り形式で取得することもできる）

Firepower Management Center のシステム設定を使用して、データベース アクセスを有効にして、選択したホストにデータベースの照会を許可するアクセス リストを作成します。このアクセス リストは、アプライアンスのアクセスは制御しません。

次のツールを含むパッケージをダウンロードすることもできます。

- RunQuery（シスコが提供するデータベース クエリ ツール）
- InstallCert（アクセスしたい Firepower Management Center から SSL 証明書を取得して受け入れるために使用できるツール）
- データベースへの接続時に使用する必要がある JDBC ドライバ

データベースアクセスを構成するためにダウンロードしたパッケージ内のツールの使用方法については、『*Firepower System Database Access Guide*』を参照してください。

データベースへの外部アクセスの有効化

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス
任意（Any）	任意（Any）	Management Center	グローバルだけ	Admin

手順

ステップ 1 **[システム（System）] > [設定（Configuration）]**を選択します。

ステップ 2 [外部データベース アクセス（External Database Access）] をクリックします。

ステップ 3 [外部データベース アクセスの許可（Allow External Database Access）] チェックボックスをオンにします。

ステップ 4 [サーバホスト名（Server Hostname）] フィールドに、適切な値を入力します。サードパーティ アプリケーションの要件に応じて、この値は、Firepower Management Center の完全修飾ドメイン名（FQDN）、IPv4 アドレス、または IPv6 アドレスにできます。

ステップ 5 [クライアント JDBC ドライバ（Client JDBC Driver）] の横にある [ダウンロード（Download）] をクリックし、ブラウザのプロンプトに従って `client.zip` パッケージをダウンロードします。

ステップ 6 1 つ以上の IP アドレスからのデータベース アクセスを追加するには、[ホストの追加（Add Hosts）] をクリックします。[アクセス リスト（Access List）] フィールドに [IP アドレス（IP Address）] フィールドが表示されます。

ステップ 7 [IP アドレス（IP Address）] フィールドに、IP アドレスまたはアドレスの範囲を入力するか、`any` を入力します。

ステップ 8 [追加（Add）] をクリックします。

ステップ 9 [保存（Save）] をクリックします。

ヒント 最後に保存されたデータベース設定に戻すには、[更新（Refresh）] をクリックします。

関連トピック

Firepower システムの IP アドレス表記法

データベース イベント数の制限

Firepower Management Center が保存できる各イベント タイプの最大数を指定できます。パフォーマンスを向上させるには、定期的に処理するイベント数に合わせてイベント数の制限を調整する必要があります。一部のイベント タイプでは、ストレージを無効にすることができます。

システムは侵入イベント、ディスカバリ イベント、監査レコード、セキュリティ インテリジェンス データ、URL フィルタリング データをアプライアンスのデータベースから自動的にプルーニングします。イベントが自動的にプルーニングされると自動で電子メール通知を生成するようにシステムを設定できます。また、手動でディスカバリ データベースやユーザ データベースをプルーニングし、Firepower Management Center データベースからディスカバリ データや接続データを消去することもできます。

データベース イベント数の制限の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス
任意（Any）	任意（Any）	Management Center	グローバルだけ	Admin

始める前に

- Firepower Management Center のデータベースからイベントがプルーニングされた場合に電子メール通知を受信するには、電子メール サーバを設定する必要があります。メール リレー ホストおよび通知アドレスの設定 （61 ページ）を参照してください。

手順

ステップ 1 **[システム（System）] > [設定（Configuration）]**を選択します。

ステップ 2 [データベース（Database）] を選択します。

ステップ 3 各データベースについて、保存するレコードの数を入力します。

各データベースが保持できるレコード数の詳細については、データベース イベント数の制限（16 ページ）を参照してください。

ステップ 4 必要に応じて、[データ プルーニング通知のアドレス（Data Pruning Notification Address）] フィールドに、プルーニング通知を受信する電子メール アドレスを入力します。

ステップ 5 [保存（Save）] をクリックします。

データベース イベント数の制限

次の表に、Firepower Management Center に保存可能な各イベント タイプのレコードの最小数と最大数を示します。

表 *2:* データベース イベント数の制限

イベント タイプ（Event Type）	上限	下限
侵入イベント	1,000 万（Management Center Virtual） 2,000 万（MC750） 3,000 万（MC1000 および MC1500） 6,000 万（MC2000 および MC2500） 1 億 5,000 万（MC3500） 3 億（MC4000 および MC4500）	10,000
検出イベント	1,000 万 2,000 万（MC2000、MC2500、MC4000、および MC4500）	0（ストレージを無効化）
接続イベント セキュリティ インテリジェンス イベント	5,000 万（Management Center 仮想） 5,000 万（MC750） 1 億（MC1000 および MC1500） 3 億（MC2000 および MC2500） 5 億（MC3500） 10 億（MC4000 および MC4500） 制限は接続イベントとセキュリティ インテリジェンス イベントの間で共有されます。設定済みの最大数の合計がこの制限を超えることはできません。	0（ストレージを無効化）
接続の要約（集約された接続イベント）	5,000 万（Management Center 仮想） 5,000 万（MC750） 1 億（MC1000 および MC1500） 3 億（MC2000 および MC2500） 5 億（MC3500） 10 億（MC4000 および MC4500）	0（ストレージを無効化）

イベントタイプ（Event Type）	上限	下限
相関イベントおよびコンプライアンスのホワイトリストイベント	100 万 200 万（MC2000、MC2500、MC4000、および MC4500）	1 つ
マルウェア イベント	1,000 万 2,000 万（MC2000、MC2500、MC4000、および MC4500）	10,000
ファイル イベント	1,000 万 2,000 万（MC2000、MC2500、MC4000、および MC4500）	0（ストレージを無効化）
ヘルス イベント	100 万	0（ストレージを無効化）
監査レコード	100,000	1 つ
修復ステータス イベント	1,000 万	1 つ
ホワイトリスト違反履歴	30 日間の違反履歴	1 日の履歴
ユーザ アクティビティ（ユーザ イベント）	1,000 万	1 つ
ユーザ ログイン（ユーザ履歴）	1,000 万	1 つ
侵入ルール更新のインポート ログ レコード	100 万	1 つ

管理インターフェイス

セットアップの完了後、管理ネットワーク設定を変更することができます。これには、Management Center と管理対象デバイスの両方での管理インターフェイス、ホスト名、検索ドメイン、DNS サーバ、HTTP プロキシの追加が含まれます。

管理インターフェイスについて

デフォルトでは、Firepower Management Center はすべてのデバイスを 1 つの管理インターフェイス上で制御します。各デバイスには Management Center と通信するための管理インターフェイスが 1 つ含まれています。

また、初期設定（Management Center および管理対象デバイスの両方）や、管理者として Management Center にログインする際にも管理インターフェイスで行います。

管理インターフェイスは、スマートライセンスサーバとの通信、更新プログラムのダウンロード、その他の管理機能の実行にも使用します。

Firepower Management Center 上の管理インターフェイス

Firepower Management Center では、初期セットアップ、管理者の HTTP アクセス、デバイスの管理、ならびにその他の管理機能（ライセンス管理や更新など）に、eth0 インターフェイスが使用されます。

同じネットワーク上、あるいは別のネットワーク上に、追加の管理インターフェイスを設定することもできます。Management Center が管理するデバイスの数が多い場合、管理インターフェイスをさらに追加することで、スループットとパフォーマンスの向上につながります。これらの管理インターフェイスをその他すべての管理機能に使用することもできます。管理インターフェイスごとに、対応する機能を限定することをお勧めします。たとえば、ある特定の管理インターフェイスを HTTP 管理者アクセス用に使用し、別の管理インターフェイスをデバイスの管理に使用するなどです。

デバイス管理用に、管理インターフェイスには 2 つの別個のトラフィック チャネルがあります。管理トラフィック チャネルはすべての内部トラフィック（デバイス管理に固有のデバイス間トラフィックなど）を伝送し、イベント トラフィック チャネルはすべてイベント トラフィック（Web イベントなど）を伝送します。オプションで、Management Center 上にイベントを処理するためのイベント専用インターフェイスを別個に設定することもできます。設定できるイベント専用インターフェイスは 1 つだけです。イベント トラフィックは大量の帯域幅を使用する可能性があるので、管理トラフィックからイベント トラフィックを分離することで、Management Center のパフォーマンスを向上させることができます。たとえば、10 GigabitEthernet インターフェイスをイベント インターフェイスとして割り当て、可能なら、1 GigabitEthernet インターフェイスを管理用に使用します。たとえば、イベント専用インターフェイスは完全にセキュアなプライベート ネットワーク上に設定し、通常の管理インターフェイスはインターネットにアクセスできるネットワーク上で使用することをお勧めします。目的がスループットの向上だけである場合は、管理インターフェイスとイベント インターフェイスを同じネットワーク上で使用することもできます。

（注） すべての管理インターフェイスが、アクセス リスト設定（システムのアクセス リストの設定（47 ページ））によって制御される HTTP 管理者アクセスをサポートします。逆に、インターフェイスを HTTP アクセスのみに制限することはできません。管理インターフェイスでは、常にデバイス管理がサポートされます（管理トラフィック、イベント トラフィック、またはその両方）。

以下の機能は、デフォルトの管理インターフェイス（eth0）でのみサポートされます。

- DHCP IP アドレッシング。他の管理インターフェイスでは静的 IP アドレスを使用する必要があります。
- 新しいデバイスを登録する際の NAT ID の使用。

- Lights-Out Management

管理対象デバイス上の管理インターフェイス

一部のモデルでは、イベントトラフィック専用として設定できる追加管理インターフェイスがあり、Management Center との通信中に管理トラフィックとイベント トラフィックを分離できます。

デバイスをセットアップするときに、接続先とする Management Center の IP アドレスを指定します。初期登録時は、管理トラフィックとイベントトラフィックの両方がこのアドレスに送信されます。注：場合によっては、Management Center が別の管理インターフェイスで初期接続を確立することがあります。その場合、以降の接続では指定した IP アドレスの管理インターフェイスを使用する必要があります。

デバイスと Management Center の両方に別個のイベント インターフェイスが設定されている場合は、デバイスと Management Center が互いのイベント インターフェイスを管理通信中に学習した後、ネットワークで許可されていれば、後続のイベントトラフィックがそれらのインターフェイス間で送られます。イベントネットワークがダウンすると、イベントトラフィックは、通常の管理インターフェイスに戻ります。デバイスは、可能な場合に別個のイベントインターフェイスを使用しますが、管理インターフェイスは常にバックアップです。管理対象デバイス上で 1 つの管理インターフェイスだけを使用している場合、管理トラフィックを Management Center管理インターフェイスに送信できませんし、イベント トラフィックを別個の Management Center イベント インターフェイスに送信することもできません。Management Center と管理対象デバイスの両方で別個のイベント インターフェイスを使用する必要があります。

管理インターフェイスのサポート

管理インターフェイスの場所については、ご使用のモデルのハードウェアインストレーションガイドを参照してください。

（注） Firepower 4100/9300 シャーシ（Firepower 4100 および 9300）の場合、MGMT インターフェイスは Firepower Threat Defense の論理デバイスを管理するためではなく、シャーシを管理するために使用します。mgmt タイプ（または firepower-eventing タイプあるいはその両方）の別個の NIC インターフェイスを設定してから、そのインターフェイスを Firepower Threat Defense 論理デバイスに割り当てる必要があります。

（注） シャーシ上の Firepower Threat Defense の場合、物理管理インターフェイスは、診断論理インターフェイス（SNMP または syslog に利用できて、Management Center でデータ インターフェイスと併せて設定されます）と、Management Center 通信用の管理論理インターフェイスの間で共有されます。詳細については、管理/診断インターフェイスとネットワーク配置を参照してください。

Firepower Management Centerおよび管理対象デバイスの各モデルでサポートされる管理インターフェイスについては、以下の表を参照してください。

表 *3 : Firepower Management Center* でサポートされる管理インターフェイス

モデル	管理インターフェイス
MC750、MC1500、MC3500	eth0（デフォルト） eth1
MC2000、MC4000	eth0（デフォルト） eth1 eth2 eth3
MC1000	eth0（デフォルト） eth1
MC2500、MC4500	eth0（デフォルト） eth1 eth2 eth3
Firepower Management Center Virtual	eth0（デフォルト）

表 *4 :* 管理対象デバイスでサポートされる管理インターフェイス

モデル	管理インターフェイス	オプションのイベント インターフェイス
7000 シリーズ	eth0	サポートなし
8000 シリーズ	eth0	eth1
NGIPSv	eth0	サポートなし
ASA 5585-X 上の ASA FirePOWER サービス モジュール	eth0 （注） eth0 は、管理 1/0 インターフェイスの内部名です。	eth1 （注） eth1 は、管理 1/1 インターフェイスの内部名です。
ASA 5506-X、5508-X、5516-X 上の ASA FirePOWER サービス モジュール	eth0 （注） eth0 は、管理 1/1 インターフェイスの内部名です。	サポートなし

モデル	管理インターフェイス	オプションのイベント インターフェイス
ASA 5512-X-X から 5555-X 上の ASA FirePOWER サービス モジュール	eth0 （注） eth0 は、管理 0/0 インターフェイスの内部名です。	サポートなし
ASA 5506-X、5508-X、5516-X 上の Firepower Threat Defense	br1 （注） br1 は、管理 1/1 インターフェイスの内部名です。	サポートなし
5512-X ～ 5555-X 上の Firepower Threat Defense	br1 （注） br1 は、管理 0/0 インターフェイスの内部名です。	サポートなし
Firepower 4100 および 9300 上の Firepower Threat Defense	management0 （注） management0 は、物理インターフェイス ID に関わらず、このインターフェイスの内部名です。	management1 （注） management1 は、物理インターフェイス ID に関わらず、このインターフェイスの内部名です。
Firepower Threat Defense Virtual	br1	サポートなし

管理インターフェイス上のネットワーク ルート

管理インターフェイス（イベント専用インターフェイスを含む）は、リモート ネットワークに到達するためのスタティック ルートのみをサポートしています。Management Center または管理対象デバイスをセットアップすると、セットアップ プロセスにより、指定したゲートウェイ IP アドレスへのデフォルト ルートが作成されます。このルートを削除することはできません。また、このルートで変更できるのはゲートウェイ アドレスのみです。

デフォルト ルートでは、常に最も番号の小さい管理インターフェイス（eth0 など）が使用されます。

複数のインターフェイスが同じネットワーク上にある場合を含めて、リモート ネットワークにアクセスするには、管理インターフェイスごとに 1 つ以上のスタティック ルートを使用することをお勧めします。

たとえば、Management Center で、eth0 と eth1 が同じネットワーク上にありますが、各インターフェイスで異なるデバイス グループを管理するとします。デフォルト ゲートウェイは 192.168.45.1 です。eth1 でリモート 10.6.6.0/24 宛先ネットワーク上のデバイスを管理する場合

は、同じ 192.168.45.1 のゲートウェイを使用して eth1 経由で 10.6.6.0/24 用のスタティック ルートを作成できます。10.6.6.0/24 へのトラフィックは、デフォルト ルートの前にこのルートに到達するため、eth1 が想定どおりに使用されます。

2 つの Management Center インターフェイスを使用して同じネットワーク上のリモート デバイスを管理する場合は、デバイス IP アドレスごとに別のスタティック ルートが必要なため、Management Center のスタティック ルーティングが適切に拡張できないことがあります。

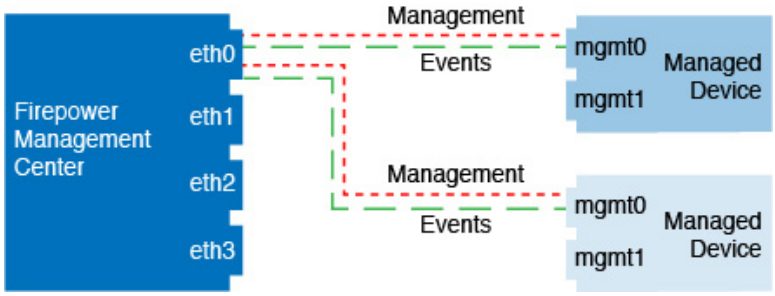
別の例には、Management Center と管理対象デバイスの両方に個別の管理インターフェイスとイベント専用インターフェイスが含まれています。イベント専用インターフェイスは、管理インターフェイスとは別のネットワーク上にあります。この場合は、リモートイベント専用ネットワーク宛てのトラフィック用にイベント専用インターフェイスを介してスタティック ルートを追加します。その逆も同様です。

（注） 管理インターフェイスのルーティングは、データ インターフェイスに対して設定するルーティングとは完全に別のものです。

管理およびイベント トラフィック チャネルの例

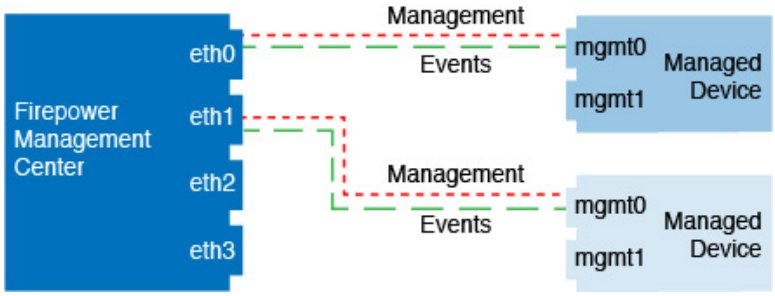
以下に、Firepower Management Center と管理対象デバイスでデフォルト管理インターフェイスのみを使用する例を示します。

図 *1 : Firepower Management Center* 上で単一の管理インターフェイスを使用する場合



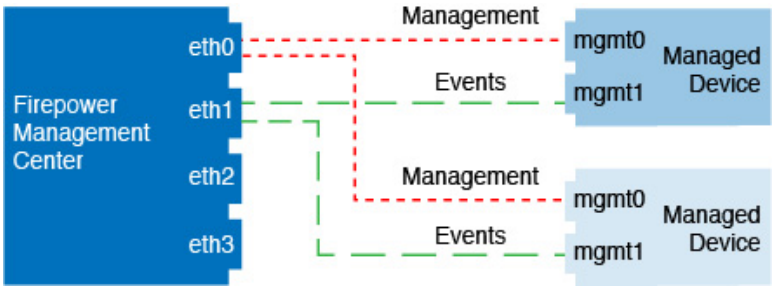
以下に、Firepower Management Center でデバイスごとに別個の管理インターフェイスを使用する例を示します。この場合、各管理対象デバイスが 1 つの管理インターフェイスを使用します。

図 *2 : Firepower Management Center* 上の複数の管理インターフェイスを使用する場合



以下に、個別のイベントインターフェイスを使用するFirepower Management Centerと管理対象デバイスの例を示します。

図 3 : *Firepower Management Center*上の個別のイベント インターフェイスと管理対象デバイスを使用する場合



以下に、Firepower Management Center上で複数の管理インターフェイスと個別のイベントインターフェイスが混在し、個別のイベントインターフェイスを使用する管理対象デバイスと単一の管理インターフェイスを使用する管理対象デバイスが混在する例を示します。

図 4 : 管理インターフェイスとイベント インターフェイスを混在させて使用する場合

管理インターフェイスの設定

Firepowerアプライアンスの管理インターフェイス設定を変更できます。

- Firepower Management Center：Webインターフェイスを使用します。（Firepower Management Centerは、Cisco TACの監督下にある場合に限り、Linuxシェル アクセスをサポートします。）
- Firepower Threat Defenseデバイス、NGIPSv、ASA FirePOWER：CLIを使用します。
- 7000 & 8000シリーズ デバイス：制限されたWebインターフェイスまたはCLIを使用します。

次の項を参照してください。

関連トピック

通信ポートの要件

Firepower Management Center 管理インターフェイスの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス
任意（Any）	任意（Any）	Management Center	グローバルだけ	Admin

Firepower Management Center で管理インターフェイスの設定を変更します。オプションとして追加の管理インターフェイスを有効にしたり、イベントのみのインターフェイスを設定したりできます。

⚠

注意 接続されている管理インターフェイスを変更する場合は十分にご注意ください。設定エラーのために再接続できない場合は、Management Center コンソール ポートにアクセスして、Linux シェルでネットワーク設定を再設定する必要があります。この操作では、Cisco TAC に連絡する必要があります。

手順

ステップ 1 **[システム（System）] > [設定（Configuration）]** を選択し、次に [管理インターフェイス（Management Interfaces）] を選択します。

ステップ 2 [インターフェイス（Interfaces）]エリアで、設定するインターフェイスの横にある [編集（Edit）] をクリックします。

このセクションでは、利用可能なすべてのインターフェイスがリストされます。インターフェイスをさらに追加することはできません。

それぞれの管理インターフェイスに対して、以下のオプションを設定できます。

- [有効にする（Enabled）] : 管理インターフェイスを有効にします。デフォルト eth0 管理インターフェイスを無効に**しないでください**。eth0 インターフェイスを必要とするプロセスもあります。
- [チャネル（Channels）] : イベントのみのインターフェイスを設定します。Management Center では 1 つのイベント インターフェイスしか設定できません。これを設定するには、[管理トラフィック（Management Traffic）] チェックボックスをオフにして、[イベント トラフィック（Event Traffic）] チェックボックスをオンのままにしておきます。必要に応じて、管理インターフェイスの [イベント トラフィック（Event Traffic）] を無効にすることができます。いずれの場合も、デバイスは、イベントのみのインターフェイスにイベントを送信しようとします。そのインターフェイスがダウンしていた場合は、イベント チャネルが無効になっていても、管理インターフェイス上でイベントを送信します。インターフェイス上でイベント チャネルと管理チャンネルの両方を無効にすることはできません。
- [モード（Mode）] : リンク モードを指定します。GigabitEthernet インターフェイスでは、自動ネゴシエーションの値を変更しても反映されないことに注意してください。

- [MTU]：最大伝送ユニット（MTU）を設定します。デフォルトは 1500 です。設定可能な MTU の範囲は、モデルとインターフェイスのタイプによって異なる場合があります。

  システムは、設定された MTU 値から自動的に 18 バイトを削減するため、IPv6 の場合、1298 未満の値は MTU の最小値である 1280 に準拠しません。IPv4 の場合は、594 未満の値は MTU の最小値 576 に準拠しません。たとえば、構成値 576 は自動的に 558 に削減されます。

- [MDI/MDIX]：[自動-MDIX（Auto-MDIX）] を設定します。
- [IPv4 設定（IPv4 Configuration）]：IPv4 IP アドレスを設定します。次のどちらかを選択します。
  - [スタティック（Static）]：IPv4 の管理 IP アドレスとネットマスクを手動で入力します。
  - [DHCP]：DHCP を使用するインターフェイスを設定します（eth0 のみ）。
  - [無効（Disabled）]：無効 IPv4。IPv4 と IPv6 の両方を無効にしないでください。
- [IPv6 設定（IPv6 Configuration）]：IPv6 IP アドレスを設定します。次のどちらかを選択します。
  - [スタティック（Static）]：IPv6 の管理 IP アドレスとプレフィックス長を手動で入力します。
  - [DHCP]：DHCPv6 を使用するインターフェイスを設定します（eth0 のみ）。
  - [ルータ割当て（Router Assigned）]：ステートレス自動設定を有効にします。
  - [無効（Disabled）]：IPv6 を無効にします。IPv4 と IPv6 の両方を無効にしないでください。

ステップ 3 [ルート（Routes）]エリアで、スタティック ルートを編集アイコン（）をクリックして編集するか、またはルートを追加アイコン（  ）をクリックして追加します。表示アイコン（  ）をクリックして、ルートの統計を表示します。

追加の各インターフェイスがリモート ネットワークに到達するには、スタティック ルートが必要です。新しいルートが必要になるケースの詳細については、管理インターフェイス上のネットワーク ルート （21 ページ）を参照してください。

（注） デフォルト ルートでは、ゲートウェイ IP アドレスのみを変更できます。デフォルト ルートでは常に eth0 インターフェイスが使用されます。

次の設定をスタティック ルートに対して設定できます。

- [宛先（Destination）]：ルートを作成する宛先ネットワークのアドレスを設定します。
- [ネットマスク（Netmask）] または [プレフィックス長（Prefix Length）]：ネットワークのネットマスク（IPv4）またはプレフィックス長（IPv6）を設定します。
- [インターフェイス（Interface）]：出力管理インターフェイスを設定します。

- [ゲートウェイ（Gateway）]：ゲートウェイ IP アドレスを設定します。

ステップ 4 [共有設定（Shared Settings）] エリアで、すべてのインターフェイスで共有されているネットワーク パラメータを設定します。

（注） eth0 インターフェイスで [DHCP] を選択すると、DHCP サーバから取得する共有設定の一部を手動で指定することができなくなります。

次の共有設定を行うことができます。

- [ホスト名（Hostname）]：Management Center ホスト名を設定します。ホスト名を変更する場合、syslog メッセージに反映される新しいホスト名を使用するには、Management Center を再起動します。再起動するまでは、新しいホスト名が Syslog メッセージに反映されません。
- [ドメイン（Domains）]：カンマで区切られた、Management Center の検索ドメインを設定します。これらのドメインは、**ping system**など、コマンドで完全修飾ドメイン名を指定しない場合にホスト名に追加されます。ドメインは、管理インターフェイスまたは管理インターフェイスを経由するコマンドでのみ、使用されます。
- [プライマリ DNS サーバ（Primary DNS Serve）]、[セカンダリ DNS サーバ（Secondary DNS Server）]、[ターシャリ DNS サーバ（Tertiary DNS Server）]：優先度順に使用される DNS サーバを設定します。
- [リモート管理ポート（Remote Management Port）]：管理対象デバイスとの通信用のリモート管理ポートを設定します。Management Center および管理対象デバイスは、双方向の SSL 暗号化通信チャネル（デフォルトではポート 8305）を使用して通信します。

  （注） シスコは、リモート管理ポートをデフォルト設定のままにしておくことを**強く**推奨していますが、管理ポートがネットワーク上の他の通信と競合する場合は、別のポートを選択できます。管理ポートを変更する場合は、展開内の相互に通信する必要がある**すべての**デバイスの管理ポートを変更する必要があります。

ステップ 5 [プロキシ（Proxy）] 領域で、HTTP プロキシを設定します。

Management Center は、ポート TCP/443（HTTPS）および TCP/80（HTTP）でインターネットに直接接続するように構成されています。HTTP ダイジェスト経由で認証できるプロキシサーバを使用できます。

（注） NT LAN Manager（NTLM）認証を使用するプロキシはサポートされません。

a) [有効（Enabled）] チェックボックスをオンにします。
b) [HTTP プロキシ（HTTP Proxy）] フィールドに、プロキシ サーバの IP アドレスまたは完全修飾ドメイン名を入力します。
c) [ポート（Port）] フィールドに、ポート番号を入力します。
d) [プロキシ認証の使用（Use Proxy Authentication）] を選択してから [ユーザ名（User Name）] と [パスワード（Password）] を入力して、認証資格情報を設定します。

ステップ 6 [保存（Save）] をクリックします。

ステップ 7 管理 IP アドレスを変更すると、Management Center と管理対象デバイスの間の通信に影響を与える可能性があります。

IP アドレスを変更しても、現在の接続には影響を与えません。ただし、デバイスまたは Management Center をリロードした場合は、接続を再確立する必要があります。ピアの正しい IP アドレスを持つために、少なくとも 1 つのデバイス（Management Center または管理対象デバイス）が必要です。たとえば、Management Center でデバイスを追加し、（IP アドレスの代わりに）NAT ID を指定した場合は、設定時にデバイスに定義した Management Center IP アドレスが正しくなくなるため、デバイスは通信を再確立できなくなります。また、デバイスで Management Center IP アドレスを更新することはできません。IP アドレスを置き換えて、新しいデバイスとして再登録することのみができます（**configure manager add**）。一方で、Management Center で管理対象デバイスの正しい IP アドレスが認識されている場合は、管理対象デバイスが持つ Management Center 用の IP アドレスが正しくない場合でも、Management Center は正常に接続を確立できます。

Web インターフェイスでのクラシック デバイス管理インターフェイスの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス
該当なし	任意（Any）	7000 & 8000 シリーズ	グローバルだけ	Admin

Webインターフェイスを使用して、管理対象デバイスの管理インターフェイスの設定を変更します。モデルでサポートされている場合に、オプションでイベントインターフェイスを有効にすることができます。

⚠

注意 慎重に管理インターフェイスに変更を加えてください。構成エラーで再接続できなくなると、デバイスのコンソール ポートへのアクセスおよび CLI での再設定が必要になります。

手順

ステップ 1 **[システム（System）] > [設定（Configuration）]** を選択して、[管理インターフェイス（Management Interfaces）] を選択します。

ステップ 2 [インターフェイス（Interfaces）]エリアで、設定するインターフェイスの横にある [編集（Edit）] をクリックします。

このセクションでは、利用可能なすべてのインターフェイスがリストされます。インターフェイスをさらに追加することはできません。

それぞれの管理インターフェイスに対して、以下のオプションを設定できます。

- [有効にする（Enabled）]：管理インターフェイスを有効にします。デフォルト eth0 管理インターフェイスを無効にしないでください。eth0 インターフェイスを必要とするプロセスもあります。
- [チャネル（Channels）]：（8000 シリーズのみ）イベント オンリーのインターフェイスを設定します。8000 シリーズのデバイスで eth1 管理インターフェイスを有効にして、イベント インターフェイスとして機能させることができます。これを設定するには、[管理トラフィック（Management Traffic）] チェックボックスをオフにして、[イベント トラフィック（Event Traffic）] チェックボックスをオンのままにしておきます。eth0 管理インターフェイスを入力するには、両方のチェックボックスをオンのままにしておきます。

  Firepower Management Center イベント専用インターフェイスは管理チャネルのトラフィックを受け入れることができないので、デバイス イベント インターフェイスで管理チャネルを単に無効にしてください。

  必要に応じて、管理インターフェイスの [イベント トラフィック（Event Traffic）] を無効にすることができます。いずれの場合も、デバイスは、イベントのみのインターフェイス上でイベントを送信しようとします。そのインターフェイスがダウンしていた場合は、イベント チャネルが無効になっていても、管理インターフェイス上でイベントを送信します。

  インターフェイス上でイベント チャネルと管理チャンネルの両方を無効にすることはできません。
- [モード（Mode）]：リンク モードを指定します。GigabitEthernet インターフェイスでは、自動ネゴシエーションの値を変更しても反映されないことに注意してください。
- [MTU]：最大伝送ユニット（MTU）を設定します。デフォルトは 1500 です。設定可能な MTU の範囲は、モデルとインターフェイスのタイプによって異なる場合があります。

  システムは、設定された MTU 値から自動的に 18 バイトを削減するため、IPv6 の場合、1298 未満の値は MTU の最小値である 1280 に準拠しません。IPv4 の場合は、594 未満の値は MTU の最小値 576 に準拠しません。たとえば、構成値 576 は自動的に 558 に削減されます。
- [MDI/MDIX]：[自動-MDIX（Auto-MDIX）] を設定します。
- [IPv4 設定（IPv4 Configuration）]：IPv4 IP アドレスを設定します。次のどちらかを選択します。
  - [スタティック（Static）]：IPv4 の管理 IP アドレスとネットマスクを手動で入力します。
  - [DHCP]：DHCP を使用するインターフェイスを設定します（eth0 のみ）。
  - [無効（Disabled）]：無効 IPv4。IPv4 と IPv6 の両方を無効にしないでください。
- [IPv6 設定（IPv6 Configuration）]：IPv6 IP アドレスを設定します。次のどちらかを選択します。
  - [スタティック（Static）]：IPv6 の管理 IP アドレスとプレフィックス長を手動で入力します。

- [DHCP]：DHCPv6 を使用するインターフェイスを設定します（eth0 のみ）。
- [ルータ割当て（Router Assigned）]：ステートレス自動設定を有効にします。
- [無効（Disabled）]：IPv6 を無効にします。IPv4 と IPv6 の両方を無効に**しないでください**。

ステップ 3 [ルート（Routes）]エリアで、スタティック ルートを編集アイコン（）をクリックして編集するか、またはルートを追加アイコン（）をクリックして追加します。表示アイコン（）をクリックして、ルートの統計を表示します。

（注） Firepower Management Center がリモート ネットワーク上にある場合は、イベント専用インターフェイスのスタティック ルートを追加する必要があります。追加しないと、すべてのトラフィックが管理インターフェイスを通じてデフォルト ルートと一致します。デフォルト ルートでは、ゲートウェイ IP アドレスのみを変更できます。デフォルト ルートでは常に eth0 インターフェイスが使用されます。ルーティングの詳細については、管理インターフェイス上のネットワーク ルート （21 ページ）を参照してください。

次の設定をスタティック ルートに対して設定できます。

- [宛先（Destination）]：ルートを作成する宛先ネットワークのアドレスを設定します。
- [ネットマスク（Netmask）] または [プレフィックス長（Prefix Length）]：ネットワークのネットマスク（IPv4）またはプレフィックス長（IPv6）を設定します。
- [インターフェイス（Interface）]：出力管理インターフェイスを設定します。
- [ゲートウェイ（Gateway）]：ゲートウェイ IP アドレスを設定します。

ステップ 4 [共有設定（Shared Settings）] エリアで、すべてのインターフェイスで共有されているネットワーク パラメータを設定します。

（注） eth0 インターフェイスで [DHCP] を選択すると、DHCP サーバから取得する共有設定の一部を手動で指定することができなくなります。

以下の共有設定を行うことができます。

- [ホスト名（Hostname）]：デバイスのホスト名を設定します。ホスト名を変更する場合、Syslog メッセージに新しいホスト名を反映させるには、デバイスをリブートします。再起動するまでは、新しいホスト名が Syslog メッセージに反映されません。
- [ドメイン（Domains）]：カンマで区切ったデバイスの検索ドメインを設定します。これらのドメインは、コマンドで完全修飾ドメイン名を指定しないときに、ホスト名に ping system などとして加えられます。**ping system** ドメインは、管理インターフェイスまたは管理インターフェイスを経由するコマンドでのみ、使用されます。
- [プライマリ DNS サーバ（Primary DNS Server）]、[セカンダリ DNS サーバ（Secondary DNS Server）]、[テリタリ DNS サーバ（Tertiary DNS Server）]：DNS サーバが優先順で使用されるよう設定します。

- [リモート管理ポート（Remote Management Port）]：Management Center で通信のリモート管理ポートを設定します。Management Center および管理対象デバイスは、双方向の SSL 暗号化通信チャネル（デフォルトではポート 8305）を使用して通信します。

  （注） シスコは、リモート管理ポートをデフォルト設定のままにしておくことを**強く**推奨していますが、管理ポートがネットワーク上の他の通信と競合する場合は、別のポートを選択できます。管理ポートを変更する場合は、導入内の相互に通信する必要がある**すべての**デバイスの管理ポートを変更する必要があります。

ステップ 5 [LCD パネル（LCD Panel）]エリアで、[ネットワーク設定の再設定を許可（Allow reconfiguration of network settings）] チェックボックスをオンにして、デバイスの LCD パネルを使用したネットワーク設定の変更を有効にします。

LCD パネルを使用して、デバイスの IP アドレスを編集できます。変更が管理 Firepower Management Centerに反映されていることを確認します。状況によっては、Firepower Management Center でデータを手動で更新することが必要になります。

注意 LCD パネルを使用した再構成を許可すると、セキュリティ リスクが発生する可能性があります。LCDパネルを使用してネットワーク設定を構成する場合は、物理アクセスだけが必要で、認証は必要ありません。このオプションを有効にするとセキュリティ上の問題が発生する可能性があることを示す警告が Web インターフェイスに表示されます。

ステップ 6 [プロキシ（Proxy）] エリアで、HTTP プロキシ設定をします。

デバイスは、ポート TCP/443（HTTPS）および TCP/80（HTTP）でインターネットに直接接続するように設定されています。HTTP ダイジェスト経由で認証できるプロキシサーバを使用できます。

（注） NT LAN Manager（NTLM）認証を使用するプロキシはサポートされません。

a) [有効（Enabled）] チェックボックスをオンにします。
b) [HTTP プロキシ（HTTP Proxy）] フィールドに、プロキシ サーバの IP アドレスまたは完全修飾ドメイン名を入力します。
c) [ポート（Port）] フィールドに、ポート番号を入力します。
d) [プロキシ認証の使用（Use Proxy Authentication）] を選択してから [ユーザ名（User Name）] と [パスワード（Password）] を入力して、認証資格情報を設定します。

ステップ 7 [保存（Save）] をクリックします。

ステップ 8 管理 IP アドレスを変更すると、Management Center と管理対象デバイスの間の通信に影響を与える可能性があります。

IP アドレスを変更しても、現在の接続には影響を与えません。ただし、デバイスまたは Management Center をリロードした場合は、接続を再確立する必要があります。ピアの正しい IP アドレスを持つために、少なくとも 1 つのデバイス（Management Center または管理対象デバイス）が必要です。たとえば、デバイス設定中に（IP アドレスの代わりに）Management Center の NAT ID を指定した場合は、デバイスを追加したときに Management Center で定義したデバイス IP アドレスが正しくなくなるため、Management Center は通信を再確立できなくな

ります。この場合は、Management Center でデバイスの管理 IP アドレスを変更する必要があります。デバイス管理設定の編集を参照してください。

CLI での Firepower Threat Defense またはクラシック デバイス管理インターフェイスの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス
任意（Any）	任意（Any）	Firepower Threat Defense 従来型	グローバルだけ	Admin

CLI を使用して、管理対象デバイスの管理インターフェイスの設定を変更します。これらの設定の多くは、初期セットアップ時に設定されたものです。この手順に従うことで、それらの設定を変更でき、さらに設定を追加できます（例：モデルでサポートされる場合にイベント インターフェイスを有効化する、スタティック ルートを追加する）。Firepower Threat Defense CLI については、『*Command Reference for Firepower Threat Defense*』を参照してください。クラシック デバイス CLI の詳細については、このガイドの従来型デバイスのコマンド ライン リファレンスを参照してください。Firepower Threat Defense およびクラシック デバイスは、管理インターフェイス設定に同じコマンドを使用します。その他のコマンドは、プラットフォーム間で異なる可能性があります。

⚠

注意 SSH を使用する際は、慎重に管理インターフェイスに変更を加えてください。構成エラーで再接続できなくなると、デバイスのコンソール ポートへのアクセスが必要になります。

始める前に

- Firepower Threat Defense では、**configure user add** コマンドを使用して CLI にログイン可能なユーザ アカウントを作成できます。Firepower Threat Defense の CLI ユーザ アカウントの作成を参照してください。
- 7000 & 8000 シリーズ デバイスでは、ユーザ アカウントの作成の説明に従って、Web インターフェイスでユーザ アカウントを作成できます。

手順

ステップ 1 コンソール ポートから、または SSH を使用して、デバイス CLI に接続します。

Firepower Threat Defense デバイスのコマンドライン インターフェイスへのログインまたは従来型デバイスでのコマンドライン インターフェイスへのログインを参照してください。

ステップ 2 管理者のユーザ名とパスワードでログインします。

ステップ 3 イベント オンリーのインターフェイスを有効にします（サポート モデルについては、管理インターフェイスのサポート （19 ページ）参照）。

configure network management-interface enable *management_interface*

configure network management-interface disable-management-channel *management_interface*

例：

これは Firepower 4100 または 9300 デバイスの例です。有効なインターフェイス名はデバイス タイプによって異なります。

```
> configure network management-interface enable management1
Configuration updated successfully

> configure network management-interface disable-management-channel management1
Preserve existing configuration- currently no IP addresses on eth1 to update (bootproto
 IPv4:,bootproto IPv6:
at /usr/local/sf/lib/perl/5.10.1/SF/NetworkConf/NetworkSettings.pm line 821.
Configuration updated successfully

>
```

Firepower Management Center イベント専用インターフェイスは管理チャネルのトラフィックを受け入れることができないので、デバイス イベント インターフェイスで管理チャネルを単に無効にしてください。

オプションで、**configure network management-interface disable-events-channel** コマンドを使用して、管理インターフェイスのイベントを無効にすることができます。いずれの場合も、デバイスは、イベントのみのインターフェイス上でイベントを送信しようとします。そのインターフェイスがダウンしていた場合は、イベント チャネルが無効になっていても、管理インターフェイス上でイベントを送信します。

インターフェイス上でイベントチャネルと管理チャンネルの両方を無効にすることはできません。

ステップ 4 管理インターフェイスまたはイベント インターフェイスのネットワーク設定をします。

management_interface 引数を指定しない場合は、デフォルト管理インターフェイスのネットワーク設定を変更します。イベント インターフェイスを設定する際には、必ず *management_interface* 引数を指定してください。イベントインターフェイスは、管理インターフェイスの個別のネットワーク、または同じネットワークに配置できます。自分で設定するインターフェイスに接続すると、切断されます。新しい IP アドレスに再接続できます。

a) IPv4 アドレスを設定します。

- 手動設定

  configure network ipv4 manual *ip_address netmask gateway_ip* [*management_interface*]

  このコマンド内の *gateway_ip* は、プライマリ管理インターフェイスのデフォルト ルートを作成するためにしか使用されないことに注意してください。イベントのみのインターフェイスのゲートウェイを設定する場合、このコマンドは、ゲートウェイを無視して、それ用のデフォルト ルートまたはスタティック ルートを作成しません。

configure network static-routes コマンドを使用することによって、別にスタティックルートを作成する必要があります。

例：

```
> configure network ipv4 manual 10.10.10.45 255.255.255.0 management1
Setting IPv4 network configuration.
Network settings changed.

>
```

- DHCP（デフォルト管理インターフェイスのみでサポート）。

  configure network ipv4 dhcp

b) IPv6 アドレスを設定します。

- ステートレス自動設定

  configure network ipv6 router [*management_interface*]

  例：

```
> configure network ipv6 router management0
Setting IPv6 network configuration.
Network settings changed.

>
```

- 手動設定

  configure network ipv6 manual *ip6_address ip6_prefix_length* [*ip6_gateway_ip*] [*management_interface*]

  このコマンド内の *ipv6_gateway_ip* は、プライマリ管理インターフェイスのデフォルトルートを作成するためにしか使用されないことに注意してください。イベントのみのインターフェイスのゲートウェイを設定する場合、このコマンドは、ゲートウェイを無視して、それ用のデフォルトルートまたはスタティックルートを作成しません。**configure network static-routes** コマンドを使用することによって、別にスタティックルートを作成する必要があります。

  例：

```
> configure network ipv6 manual 2001:0DB8:BA98::3210 64 management1
Setting IPv6 network configuration.
Network settings changed.

>
```

- DHCPv6（デフォルト管理インターフェイスのみでサポート）。

  configure network ipv6 dhcp

ステップ 5 （Firepower Threat Defense のみ）デフォルト管理インターフェイスの DHCP サーバが、接続されているホストに IP アドレスを提供することを可能にします。

configure network ipv4 dhcp-server-enable *start_ip_address end_ip_address*

例：

```
> configure network ipv4 dhcp-server-enable 10.10.10.200 10.10.10.254
DHCP Server Enabled

>
```

管理インターフェイスの IP アドレスを手動で設定するときにのみ、DHCP サーバを設定できます。このコマンドは、Firepower Threat Defense Virtual ではサポートされません。DHCP サーバのステータスを表示するには **show network-dhcp-server** と入力します。

```
> show network-dhcp-server
DHCP Server Enabled
10.10.10.200-10.10.10.254
```

ステップ 6 Firepower Management Center がリモート ネットワーク上にある場合は、イベント専用インターフェイスのスタティック ルートを追加します。追加しないと、すべてのトラフィックが管理インターフェイスを通じてデフォルト ルートと一致します。

configure network static-routes {**ipv4** | **ipv6**} **add** *management_interface destination_ip netmask_or_prefix gateway_ip*

デフォルト ルートの場合は、このコマンドを使用しないでください。デフォルト ルートのゲートウェイ IP アドレスの変更は、デフォルト管理インターフェイスのための **configure network ipv4** コマンドまたは **ipv6** コマンドを使用する場合にのみ可能です（手順 4 を参照）。

ルーティングの詳細については、管理インターフェイス上のネットワーク ルート （21 ページ）を参照してください。

例：

```
> configure network static-routes ipv4 add management1 192.168.6.0 255.255.255.0 10.10.10.1
Configuration updated successfully

> configure network static-routes ipv6 add management1 2001:0DB8:AA89::5110 64
2001:0DB8:BA98::3211
Configuration updated successfully

>
```

スタティック ルートを表示するには、**show network-static-routes** と入力します（デフォルト ルートは表示されません）。

```
> show network-static-routes
---------------[ IPv4 Static Routes ]---------------
Interface                : management1
Destination              : 192.168.6.0
Gateway                  : 10.10.10.1
Netmask                  : 255.255.255.0
```

```
[…]
```

ステップ 7 ホスト名の設定

configure network hostname 名前

例：

```
> configure network hostname farscape1
```

再起動するまでは、新しいホスト名が Syslog メッセージに反映されません。

ステップ 8 検索ドメインを設定します。

configure network dns searchdomains *domain_list*

例：

```
> configure network dns searchdomains example.com,cisco.com
```

カンマで区切ったデバイスの検索ドメインを設定します。これらのドメインは、コマンドで完全修飾ドメイン名を指定しないときに、ホスト名に ping system などとして加えられます。**ping system** ドメインは、管理インターフェイスまたは管理インターフェイスを経由するコマンドでのみ、使用されます。

ステップ 9 カンマで区切った 3 つの DNS サーバを設定します。

configure network dns servers *dns_ip_list*

例：

```
> configure network dns servers 10.10.6.5,10.20.89.2,10.80.54.3
```

ステップ 10 Management Center で通信のリモート管理ポートを設定します。

configure network management-interface tcpport *number*

例：

```
> configure network management-interface tcpport 8555
```

Management Center および管理対象デバイスは、双方向の SSL 暗号化通信チャネル（デフォルトではポート 8305）を使用して通信します。

（注） シスコは、リモート管理ポートをデフォルト設定のままにしておくことを**強く**推奨していますが、管理ポートがネットワーク上の他の通信と競合する場合は、別のポートを選択できます。管理ポートを変更する場合は、導入内の相互に通信する必要がある**すべての**デバイスの管理ポートを変更する必要があります。

ステップ 11 HTTP プロキシを設定します。デバイスは、ポート TCP/443（HTTPS）および TCP/80（HTTP）でインターネットに直接接続するように設定されています。HTTP ダイジェスト経由で認証で

きるプロキシ サーバを使用できます。コマンド発行後に、HTTP プロキシのアドレスとポート、プロキシの認証が必要かどうかをユーザは尋ねられます。認証が必要な場合はプロキシのユーザ名、プロキシのパスワード、およびプロキシのパスワードの確認を入力するよう要求されます。

configure network http-proxy

例：

```
> configure network http-proxy
Manual proxy configuration
Enter HTTP Proxy address: 10.100.10.10
Enter HTTP Proxy Port: 80
Use Proxy Authentication? (y/n) [n]: Y
Enter Proxy Username: proxyuser
Enter Proxy Password: proxypassword
Confirm Proxy Password: proxypassword
```

ステップ 12 管理 IP アドレスを変更すると、Management Center と管理対象デバイスの間の通信に影響を与える可能性があります。

IP アドレスを変更しても、現在の接続には影響を与えません。ただし、デバイスまたは Management Center をリロードした場合は、接続を再確立する必要があります。ピアの正しい IP アドレスを持つために、少なくとも 1 つのデバイス（Management Center または管理対象デバイス）が必要です。たとえば、デバイス設定中に（IP アドレスの代わりに）Management Center の NAT ID を指定した場合は、デバイスを追加したときに Management Center で定義したデバイス IP アドレスが正しくなくなるため、Management Center は通信を再確立できなくなります。この場合は、Management Center でデバイスの管理 IP アドレスを変更する必要があります。デバイス管理設定の編集を参照してください。

システムのシャットダウンと再起動

アプライアンス上のプロセスのシャットダウンおよび再起動を制御するには、Firepower システムの Web インターフェイスを使用します。アプライアンスのシャットダウンは、設定データを失うことなく、安全にシステムの電源を切って再起動する準備をします。

Firepower Management Center 上のプロセスを制御できる、以下のオプションがあります。

- システムのシャットダウン：Firepower システムのグレースフル シャットダウンを開始します。
- システムの再起動：システムを通常の方法でシャット ダウンして再起動します。
- コンソールの再起動：通信、データベース、HTTP サーバのプロセスを再起動します。これは通常、トラブルシューティングの際に使用されます。

以上のオプションは、7000 および 8000 シリーズ 管理対象デバイスすべてで共通に使用できます。これらのデバイス上で Snort プロセスを再起動することもできます。

注意 電源ボタンを使用してアプライアンスを停止**しないでください**。データが失われる可能性があります。Webインターフェイスを使用して完全にアプライアンスをシャットダウンする必要があります。

注意 Snortプロセスを再起動すると、一時的にトラフィック インスペクションが中断されます。 この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、ターゲットデバイスがトラフィックを処理する方法に応じて異なります。詳細については、Snort® の再起動によるトラフィックの動作を参照してください。

Firepower仮想管理対象デバイスの場合、VMwareなどの仮想インフラストラクチャーには一般的に、仮想マシンのシャットダウン方法、再起動方法、中断方法を定義する設定可能な電源オプションが用意されています。これらのオプションをどのように設定するかについては、使用している仮想プラットフォームのドキュメンテーションを参照してください。

（注） VMware上で稼働するFirepower仮想管理対象デバイスの場合、VMwareツールにカスタム電源オプションが含まれています。したがって、グレースフルシャットダウンを設定するには、仮想マシンにVMwareツールがインストールされている必要があります。

システムのシャット ダウンと再起動

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス
任意（Any）	任意（Any）	Management Center 7000 & 8000 シリーズ	グローバルだけ	Admin

手順

ステップ 1 **[システム（System）] > [設定（Configuration）]**を選択します。

ステップ 2 [プロセス（Process）] を選択します。

ステップ 3 アプライアンスをシャットダウンするには、以下を実行します。

- Management Center：[管理センターのシャットダウン（Shutdown Management Center）] の横にある [コマンドの実行（Run Command）] をクリックします。
- 管理対象デバイス：[アプライアンスのシャットダウン（Shutdown Appliance）] の横にある [コマンドの実行（Run Command）] をクリックします。

ステップ 4 アプライアンスを再起動するには、以下を実行します。

- Management Center：[管理センターの再起動（Reboot Management Center）] の横にある [コマンドの実行（Run Command）] をクリックします。
- 管理対象デバイス：[アプライアンスの再起動（Reboot Appliance）] の横にある [コマンドの実行（Run Command）] をクリックします。

（注） Firepower Management Center または管理対象デバイスを再起動すると、アプライアンスからログアウトされます。システムはデータベース チェックを実行しますが、これは完了するのに 1 時間かかります。

ステップ 5 アプライアンスを再起動するには、以下を実行します。

- Management Center：[管理センターの再起動（Restart Management Center）] の横にある [コマンドの実行（Run Command）] をクリックします。
- 管理対象デバイス：[アプライアンス コンソールの再起動（Restart Appliance Console）] の横にある [コマンドの実行（Run Command）] をクリックします。

（注） Firepower Management Center を再起動すると、ネットワーク マップ内に削除されたホストが再表示されることがあります。

ステップ 6 管理対象デバイスで Snort プロセスを再起動するには、[Snort の再起動（Restart Snort）] の横にある [コマンドの実行（Run Command）] をクリックします。

（注） このコマンドは、7000 および 8000 シリーズ デバイスのローカル Web インターフェイスでのみ使用できます。

注意 Snort プロセスを再開すると、一時的にトラフィック検査が中断されます。この中断中にトラフィックがドロップするか、検査なしで通過するかどうかは、デバイスの設定方法によって異なります。詳細については、Snort® の再起動によるトラフィックの動作を参照してください。

関連トピック

Snort® の再起動シナリオ

リモート ストレージ管理

Firepower Management Center では、バックアップおよびレポートのローカル ストレージまたはリモート ストレージとして、以下を使用することができます。

- ネットワーク ファイル システム（NFS）
- サーバ メッセージ ブロック（SMB）/Common Internet File System（CIFS）
- セキュア シェル（SSH）

（注） システムがサポートするバックアップおよびリモート ストレージのサーバ メッセージ ブロック プロトコルはバージョン 1 のみです。

1 つのリモート システムにバックアップを送信し、別のリモート システムにレポートを送信することはできませんが、どちらかをリモート システムに送信し、もう一方を Firepower Management Center に格納することは可能です。

ヒント リモート ストレージを構成して選択した後は、接続データベースの制限を**増やさなかった**場合に**のみ**、ローカル ストレージに戻すことができます。

ローカル ストレージの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	Management Center	グローバルだけ	Admin

手順

ステップ 1 **[システム（System）] > [設定（Configuration）]**を選択します。

ステップ 2 [リモート ストレージ デバイス（Remote Storage Device）] を選択します。

ステップ 3 [ストレージ タイプ（Storage Type）] ドロップダウン リストから [ローカル（リモート ストレージなし）（Local (No Remote Storage)）] を選択します。

ステップ 4 [保存（Save）] をクリックします。

リモート ストレージの NFS の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス
任意（Any）	任意（Any）	Management Center	グローバルだけ	Admin

始める前に

- 外部リモート ストレージ システムが機能しており、Management Center からアクセスできることを確認します。

手順

ステップ 1 **[システム（System）] > [設定（Configuration）]**を選択します。

ステップ 2 [リモート ストレージ デバイス（Remote Storage Device）] をクリックします。

ステップ 3 [ストレージ タイプ（Storage Type）] ドロップダウン リストから [NFS] を選択します。

ステップ 4 接続情報を追加します。

- [ホスト（Host）] フィールドに、ストレージ システムの IPv4 アドレスまたはホスト名を入力します。
- [ディレクトリ（Directory）] フィールドに、ストレージ領域へのパスを入力します。

ステップ 5 必要に応じて、[詳細オプションの使用（Use Advanced Options）] チェックボックスをオンにして、必要なコマンドライン オプションを入力します。リモート ストレージ管理の詳細オプション（42 ページ）を参照してください。

ステップ 6 [システムの使用方法（System Usage）] で、次の手順を実行します。

- 指定したホストにバックアップを格納するには、[バックアップに使用（Use for Backups）] を選択します。
- 指定したホストにレポートを格納するには、[レポートに使用（Use for Reports）] を選択します。
- リモート ストレージへのバックアップに関する [ディスク容量のしきい値（Disk Space Threshold）] を入力します。デフォルトは 90% です。

ステップ 7 設定をテストするには、[テスト（Test）] をクリックします。

ステップ 8 [保存（Save）] をクリックします。

リモート ストレージの SMB の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス
任意（Any）	任意（Any）	Management Center	グローバルだけ	Admin

始める前に

- 外部リモート ストレージ システムが機能しており、Management Center からアクセスできることを確認します。

手順

ステップ 1 **[システム（System）] > [設定（Configuration）]**を選択します。

ステップ 2 [リモート ストレージ デバイス（Remote Storage Device）] をクリックします。

ステップ 3 [ストレージ タイプ（Storage Type）] ドロップダウン リストから [SMB] を選択します。

ステップ 4 接続情報を追加します。

- [ホスト（Host）] フィールドに、ストレージ システムの IPv4 アドレスまたはホスト名を入力します。
- [共有（Share）] フィールドに、ストレージ領域の共有を入力します。システムに認識されるのは、ファイルのフル パスではなく、最上位の共有だけであることに注意してください。指定した共有ディレクトリをリモート バックアップ先として使用するには、それを Windows システムで共有する必要があります。
- 必要に応じて、[ドメイン（Domain）] フィールドにリモート ストレージ システムのドメイン名を入力します。
- [ユーザ名（Username）] フィールドにストレージ システムのユーザ名を入力し、[パスワード（Password）] フィールドにそのユーザのパスワードを入力します。

ステップ 5 必要に応じて、[詳細オプションの使用（Use Advanced Options）] チェックボックスをオンにして、必要なコマンドライン オプションを入力します。リモート ストレージ管理の詳細オプション （42 ページ）を参照してください。

ステップ 6 [システムの使用方法（System Usage）] で、次の手順を実行します。

- 指定したホストにバックアップを格納するには、[バックアップに使用（Use for Backups）] を選択します。
- 指定したホストにレポートを格納するには、[レポートに使用（Use for Reports）] を選択します。

ステップ 7 設定をテストするには、[テスト（Test）] をクリックします。

ステップ 8 [保存（Save）] をクリックします。

リモート ストレージの SSH の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス
任意（Any）	任意（Any）	Management Center	グローバルだけ	Admin

始める前に

- 外部リモート ストレージ システムが機能しており、Firepower Management Center からアクセスできることを確認します。

手順

ステップ 1 **[システム（System）] > [設定（Configuration）]**を選択します。

ステップ 2 [リモート ストレージ デバイス（Remote Storage Device）] をクリックします。

ステップ 3 [ストレージ タイプ（Storage Type）] ドロップダウン リストから [SSH] を選択します。

ステップ 4 接続情報を追加します。

- [ホスト（Host）] フィールドに、ストレージ システムの IP アドレスまたはホスト名を入力します。
- [ディレクトリ（Directory）] フィールドに、ストレージ領域へのパスを入力します。
- [ユーザ名（Username）] フィールドにストレージ システムのユーザ名を入力し、[パスワード（Password）] フィールドにそのユーザのパスワードを入力します。接続ユーザ名の一部としてネットワーク ドメインを指定するには、ユーザ名の前にドメインを入力し、スラッシュ（/）で区切ります。
- SSH キーを使用するには、[SSH 公開キー（SSH Public Key）] フィールドの内容をコピーして authorized_keys ファイルに貼り付けます。

ステップ 5 必要に応じて、[詳細オプションの使用（Use Advanced Options）] チェックボックスをオンにして、必要なコマンドライン オプションを入力します。リモート ストレージ管理の詳細オプション （42 ページ）を参照してください。

ステップ 6 [システムの使用方法（System Usage）] で、次の手順を実行します。

- 指定したホストにバックアップを格納するには、[バックアップに使用（Use for Backups）] を選択します。
- 指定したホストにレポートを格納するには、[レポートに使用（Use for Reports）] を選択します。

ステップ 7 設定をテストする場合は、[テスト（Test）] をクリックする必要があります。

ステップ 8 [保存（Save）] をクリックします。

リモート ストレージ管理の詳細オプション

Secure File Transfer Protocol（SFTP）を使用してレポートとバックアップを保存するために、ネットワーク ファイル システム（NFS）プロトコル、サーバ メッセージ ブロック（SMB）プロトコル、または SSH を選択すると、NFS、SMB、SSH マウントのマニュアル ページに記載さ

れているいずれかのマウント バイナリ オプションを使用するために、[詳細設定オプションの使用（Use Advanced Options）] チェック ボックスを選択できます。

SMB を選択すると、次の形式で [コマンド ライン オプション（Command Line Options）] フィールドにセキュリティ モードを入力します。

```
sec=mode
```

`mode` は、リモート ストレージで使用するセキュリティ モードです。

表 *5 : SMB* セキュリティ モードの設定

[モード（Mode）]	説明
<なし>	NULLユーザ（名前なし）として接続します。
`krb5`	Kerberos バージョン 5 認証を使用します。
`krb5i`	Kerberos 認証とパケット署名を使用します。
`ntlm`	NTLM パスワード ハッシュを使用します。（デフォルト）。
`ntlmi`	署名付きのNTLMパスワードハッシュを使用します（`/proc/fs/cifs/PacketSigningEnabled` がオンになっている場合またはサーバが署名を要求する場合はデフォルト）。
`ntlmv2`	NTLMv2 パスワード ハッシュを使用します。
`ntlmv2i`	パケット署名付きのNTLMv2パスワードハッシュを使用します。

変更調整

ユーザが行う変更をモニタし、変更が部門の推奨する標準に従っていることを確認するため、過去 24 時間に行われたシステム変更の詳細なレポートを電子メールで送信するようにシステムを構成できます。ユーザが変更をシステム構成に保存するたびに、変更のスナップショットが取得されます。変更調整レポートは、これらのスナップショットによる情報を組み合わせて、最近のシステム変更の概要を提供します。

次の図は、変更調整レポートの[ユーザ（User）]セクションの例を示しています。ここには、各構成の変更前の値と変更後の値の両方が一覧表示されています。ユーザが同じ構成に対して複数の変更を行った場合は、個々の変更の概要が最新のものから順に時系列でレポートに一覧表示されます。

過去 24 時間に行われた変更を参照できます。

変更調整の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス
任意（Any）	任意（Any）	Management Center 7000 & 8000 シリーズ	グローバルだけ	Admin

始める前に

- 24時間にシステムに行われた変更のメール送信されるレポートを受信する電子メール サーバを設定します。詳細については、メール リレー ホストおよび通知アドレスの設定 （61ページ）を参照してください。

手順

ステップ 1 **[システム（System）] > [設定（Configuration）]**を選択します。

ステップ 2 [変更調整（Change Reconciliation）] をクリックします。

ステップ 3 **[有効（Enable）]** チェックボックスをオンにします。

ステップ 4 [実行する時間（Time to Run）] ドロップダウン リストから、システムが変更調整レポートを送信する時刻を選択します。

ステップ 5 [メール宛先（Email to）] フィールドにメール アドレスを入力します。

ヒント 電子メール アドレスを追加したら、いつでも [最新のレポートの再送信（Resend Last Report）] をクリックして、最新の変更調整レポートのコピーを受信者に再送信できます。

ステップ 6 ポリシーの変更を追加する場合は、[ポリシー設定を含める（Include Policy Configuration）] チェックボックスをオンにします。

ステップ 7 過去 24 時間のすべての変更を含める場合は、[全変更履歴を表示（Show Full Change History）] チェックボックスをオンにします。

ステップ 8 [保存（Save）] をクリックします。

関連トピック

監査ログを使って変更を調査する

変更調整オプション

[ポリシー設定を含める（Include Policy Configuration）] オプションは、ポリシーの変更のレコードを変更調整レポートに含めるかどうかを制御します。これには、アクセス制御、侵入、シス

テム、ヘルス、およびネットワーク検出の各ポリシーの変更が含まれます。このオプションを選択しなかった場合は、ポリシーの変更はどれもレポートに表示されません。このオプションは Firepower Management Center のみで使用できます。

[すべての変更履歴を表示する（Show Full Change History）] オプションは、過去 24 時間のすべての変更のレコードを変更調整レポートに含めるかどうかを制御します。このオプションを選択しなかった場合は、変更がカテゴリごとに統合された形でレポートに表示されます。

ポリシー変更のコメント

ユーザがアクセス コントロール ポリシー、侵入ポリシー、またはネットワーク分析ポリシーを変更した場合、それらのポリシー関連の変更をコメント機能を使用してトラッキングするように Firepower システムを設定することができます。

ポリシー変更のコメントが有効にされていると、管理者はコメントにアクセスして、導入で重要なポリシーが変更された理由を素早く評価できます。オプションで、侵入ポリシーおよびネットワーク分析ポリシーに対する変更を監査ログに書き込むこともできます。

ポリシーの変更を追跡するコメントの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス
任意（Any）	任意（Any）	Management Center	グローバルだけ	Admin

ユーザがアクセス コントロール ポリシー、侵入ポリシー、またはネットワーク分析ポリシーを変更する場合に、コメントの入力を要求するように Firepower システムを設定できます。コメントを使用して、ユーザのポリシーの変更の理由を追跡できます。ポリシーの変更に関するコメントを有効にした場合、コメントをオプションまたは必須に設定できます。システムは、ポリシーに対する新しい変更が保存されるたびに、ユーザにコメントを入力するようプロンプトを出します。

手順

ステップ 1 **[システム（System）] > [設定（Configuration）]**を選択します。

システム設定オプションは、左側のナビゲーション パネルに表示されます。

ステップ 2 次のいずれかのポリシー コメントの設定を行います。

- アクセス コントロール ポリシーのコメント設定には、[アクセス コントロールの設定（Access Control Preferences）] をクリックします。
- 侵入ポリシーのコメント設定には、[侵入ポリシー設定（Intrusion Policy Preferences）] をクリックします。

- ネットワーク分析ポリシーのコメント設定には、[ネットワーク分析ポリシー設定（Network Analysis Policy Preferences）] をクリックします。

ステップ 3 各ポリシー タイプに次の選択肢があります。

- [無効化（Disabled）]：変更のコメントを無効にします。
- [オプション（Optional）]：コメントの変更について記述するオプションをユーザに提供します。
- [必須（Required）]：保存する前にコメントで変更について説明するようにユーザに要求します。

ステップ 4 侵入ポリシーまたはネットワーク分析ポリシーのコメントには、次のオプションがあります。

- 侵入ポリシーのすべての変更を監査ログに書き込むには、[侵入ポリシーの変更を監査ログに書き込む（Write changes in Intrusion Policy to audit log）] をオンにします。
- ネットワーク分析ポリシーのすべての変更を監査ログに書き込むには、[ネットワーク分析ポリシーの変更を監査ログに書き込む（Write changes in Network Analysis Policy to audit log）] をオンにします。

ステップ 5 [保存（Save）] をクリックします。

アクセス リスト

Firepower Management Center およびクラシック管理対象デバイスでは、アクセス リストを使用して、IPアドレスとポートを基準にシステムへのアクセスを制限できます。デフォルトでは、任意の IP アドレスに対して以下のポートが有効化されています。

- 443（HTTPS）：Web インターフェイス アクセスに使用されます。
- 22（SSH）：コマンド ライン アクセスに使用されます。

さらに、ポート 161 で SNMP 情報をポーリングするためのアクセスも追加できます。

⚠

注意 デフォルトでは、アクセスは制限されていません。よりセキュアな環境で運用するために、特定の IP アドレスに対するアクセスを追加してから、デフォルトの **any** オプションを削除することを検討してください。

システムのアクセス リストの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	Management Center 従来型	任意（Any）	Admin

この構成は、Firepower Management Center または従来の管理対象デバイス（7000 および 8000 シリーズ、ASA FirePOWER、および NGIPSv）に適用されます。

- Firepower Management Center では、この構成はシステム構成の一部です。
- 従来の管理対象デバイスでは、この構成をプラットフォーム設定ポリシーの一部として Firepower Management Center から適用します。

いずれの場合も、構成は、システム構成変更を保存するか、共有プラットフォーム設定ポリシーを展開するまで有効になりません。

このアクセス リストは、外部データベース アクセスを制御しないので注意してください。

手順

ステップ 1 Firepower Management Center を構成するか従来の管理対象デバイスを構成するかに応じて、次の操作を実行します。

- Management Center：**[システム（System）] > [設定（Configuration）]** を選択します。
- 管理対象デバイス：**[デバイス（Devices）] > [プラットフォーム設定（Platform Settings）]** を選択し、Firepower ポリシーを作成または編集します。

ステップ 2 [アクセス リスト（Access List）] をクリックします。

ステップ 3 現在の設定の 1 つを削除するために、削除アイコン（  ）をクリックすることもできます。

注意 アプライアンスのインターフェイスへの接続に現在使用されている IP アドレスへのアクセスを削除し、`IP=any port=443` のエントリが存在しない場合、ポリシーを展開した時点でシステムへのアクセスは失われます。

ステップ 4 1 つ以上の IP アドレスへのアクセスを追加するには、[ルールの追加（Add Rules）] をクリックします。

ステップ 5 [IP アドレス（IP Address）] フィールドに、IP アドレスまたはアドレスの範囲を入力するか、`any` を入力します。

ステップ 6 [SSH]、[HTTPS]、[SNMP]、またはこれらのオプションの組み合わせを選択して、これらの IP アドレスで有効にするポートを指定します。

ステップ 7 [追加（Add）] をクリックします。

ステップ 8 [保存（Save）] をクリックします。

次のタスク

- 設定変更を展開します。設定変更の展開を参照してください。

関連トピック

Firepower システムの IP アドレス表記法

監査ログ

Firepower Management Center は、管理センター ユーザのアクティビティを読み取り専用監査ログに記録します。

従来型デバイスも監査ログを保持します。従来型デバイスの監査ログを参照してください。

監査ログのデータは、いくつかの方法で確認できます。

- 監査ログは、Web インターフェイスの標準イベント ビューに表示されます。標準イベント ビューでは、監査ビューの任意の項目に基づいて監査ログ メッセージの表示、並べ替え、フィルタ処理ができます。監査情報を簡単に削除したり、それに関するレポートを作成したりすることができ、ユーザが行った変更に関する詳細なレポートを表示することもできます。システムの監査を参照してください。
- 監査ログ メッセージを syslog に送信するよう、Firepower Management Center を設定することができます。syslog への監査ログ メッセージの送信 （49 ページ）を参照してください。
- 監査ログ メッセージを HTTP サーバにストリーミングするよう、Firepower Management Center を設定することができます。監査ログ メッセージを HTTP サーバに送信する （50 ページ）を参照してください。

監査ログ データを外部 syslog または HTTP サーバにストリーミングすると、ローカル アプライアンスの容量を節約できます。

監査ログ ストリーミングのチャネルを保護するには、TLS 証明書を使用して TLS および相互認証を有効にします。詳細については、監査ログ証明書 （51 ページ）を参照してください。

注意 外部URLに監査情報を送信すると、システムパフォーマンスに影響を与える場合があります。

syslog への監査ログ メッセージの送信

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス
任意（Any）	任意（Any）	Management Center	任意（Any）	Admin

（注） 従来型デバイスからsyslogサーバへ監査ログ メッセージを送信する場合は、監査ログ メッセージを従来型デバイスから Syslog に送信するを参照してください。

この機能を有効にすると、監査ログ レコードは、syslog に次の形式で表示されます。

```
Date Time Host [Tag] Sender: User_Name@User_IP, Subsystem, Action
```

現地の日付、時刻、および発信元ホスト名の後に、角括弧で囲まれたオプション タグが続き、送信側デバイス名の後に監査ログ メッセージが続きます。

たとえば、FROMMC のタグを指定した場合は、監査ログメッセージ例は次のように表示されます。

```
Mar 01 14:45:24 localhost [FROMMC] Dev-MC7000: admin@10.1.1.2, Operations > Monitoring,
Page View
```

メッセージに関連付ける重大度、ファシリティ、およびオプション タグを指定できます。タグは、syslogの監査ログ メッセージと一緒に表示されます。ファシリティはメッセージを作成するサブシステムを示し、重大度はメッセージの重大度を定義します。syslog メッセージにはファシリティおよび重大度は含まれません。これらの値はsyslogメッセージを受信するシステムにメッセージの分類方法を示す値です。

始める前に

- syslog サーバが機能しており、監査ログを送信するシステムからアクセスできることを確認します。
- TLS証明書を使用してTLSおよび相互認証を有効にすることによって、監査ログ ストリーミングのチャネルを保護できます。詳細については、監査ログ証明書 （51 ページ）を参照してください。

手順

ステップ 1 **[システム（System）] > [設定（Configuration）]**を選択します。

ステップ 2 [監査ログ（Audit Log）] をクリックします。

ステップ 3 [監査ログを Syslog に送信（Send Audit Log to Syslog）] ドロップダウン メニューから、[有効（Enabled）] を選択します。

ステップ 4 [ホスト（Host）] フィールドにある syslog サーバの IP アドレスまたは完全修飾名を使用して、監査情報の宛先ホストを指定します。デフォルト ポート（6514）が使用されます。

注意 監査ログを受け入れるように設定しているコンピュータが、リモート メッセージを受け入れるようにセットアップされていない場合、ホストは監査ログを受け入れません。

（注） このフィールドに無効な IPv4 アドレス（192.168.1.456 など）を入力した場合でも、システムは警告を表示しません。代わりに、システムは無効なアドレスをホスト名として扱います。

ステップ 5 Syslog アラート ファシリティで説明されているとおりに、[ファシリティ（Facility）] リストからファシリティを選択します。

ステップ 6 syslog 重大度レベルで説明されているとおりに、[重大度（Severity）] リストから重大度を選択します。

ステップ 7 オプションで、[タグ（Tag）] フィールドに、syslog メッセージとともに表示するタグ名を入力します。たとえば、syslog に送信されるすべての監査ログ レコードの先頭に「FROMMC」を付加したい場合に、このフィールドに「FROMMC」と入力します。

ステップ 8 [保存（Save）] をクリックします。

監査ログ メッセージを HTTP サーバに送信する

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	Management Center	任意（Any）	Admin

（注） 従来型デバイスから HTTP サーバへ監査ログ メッセージを送信する場合は、監査ログ メッセージを従来型デバイスから HTTP サーバに送信するを参照してください。

この機能を有効にすると、アプライアンスまたはデバイスは、HTTP サーバに次の形式で監査ログ レコードを送信します。

Date Time Host [Tag] Sender: User_Name@User_IP, Subsystem, Action

ローカルの日付、時刻、および発信元ホスト名の後に、角括弧で囲まれたオプション タグが続き、送信側アプライアンスまたはデバイス名の後に監査ログ メッセージが続きます。

たとえば、FROMMC のタグを指定した場合は、監査ログメッセージ例は次のように表示されます。

```
Mar 01 14:45:24 localhost [FROMMC] Dev-MC7000: admin@10.1.1.2, Operations > Monitoring,
Page View
```

始める前に

- 外部ホストが機能していることと、監査ログを送信するアプライアンスまたはデバイスからアクセスできることを確認します。
- このストリームのチャネルは、SSL 証明書を使用して TLS と相互認証を有効にすることで保護できます。詳細については、監査ログ証明書 （51 ページ）を参照してください。

手順

ステップ 1 **[システム（System）] > [設定（Configuration）]**を選択します。

ステップ 2 [監査ログ（Audit Log）] をクリックします。

ステップ 3 必要に応じて、[タグ（Tag）] フィールドに、メッセージとともに表示するタグ名を入力します。たとえば、すべての監査ログ レコードの前に `FROMMC` を付けるには、このフィールドに `FROMMC` を入力します。

ステップ 4 [HTTP サーバへの監査ログの送信（Send Audit Log to HTTP Server）] ドロップダウン リストから、[有効（Enabled）] を選択します。

ステップ 5 [監査情報を送信する URL（URL to Post Audit）] フィールドに、監査情報の送信先 URL を指定します。次にリストした HTTP POST 変数を要求するリスナー プログラムに対応する URL を入力します。

- `subsystem`
- `actor`
- `event_type`
- `message`
- `action_source_ip`
- `action_destination_ip`
- 結果
- 時刻
- `tag`（定義されている場合。手順 3 を参照）

注意 暗号化されたポストを許可するには、HTTPS URL を使用します。外部 URL に監査情報を送信すると、システム パフォーマンスに影響を与える場合があります。

ステップ 6 [保存（Save）] をクリックします。

監査ログ証明書

クライアント証明書

クライアント証明書を使用して、監査ログ サーバと次の間の通信を保護するには：

- Firepower Management Center：Management Center から監査ログを安全にストリーミングする方法 （52 ページ）を参照してください。
- 従来型デバイス：NGIPS デバイスから監査ログをセキュアにストリームする方法を参照してください。

（注） 管理対象デバイスの証明書を操作するために Management Center を使用することはできません。管理対象デバイスの証明書を操作するには、ローカル Web インターフェイスを使用して各デバイスに直接ログインする必要があります。

サーバ証明書（Server Certificate）

必要に応じて、監査ログ サーバに署名付き証明書の提供を要求できます。

（注） サーバに署名付き証明書の提供を要求する場合、クライアント証明書はサーバ証明書と同じ認証局によって署名される必要があります。

サーバ証明書を確認するため、1 つ以上の証明書失効リスト（CRL）をロードするようにアプライアンスを設定します。アプライアンスは、サーバ証明書を CRL に記載されている証明書に照らして比較します。サーバが提供した証明書が失効した証明書として CRL に記載されている場合、そのサーバには監査ログをストリーミングできません。監査ログ サーバと Management Center 間にセキュアな接続が必要な場合 （56 ページ）を参照してください。

（注） CRL を使用して証明書を確認する場合、システムは、監査ログ サーバ証明書の検証と、アプライアンスと Web ブラウザの間の HTTP 接続を保護する証明書の検証の両方に、同じ CRL を使用します。

Management Center から監査ログを安全にストリーミングする方法

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	Management Center	任意（Any）	Admin

信頼できる HTTP サーバまたは syslog サーバに監査ログをストリーミングする場合、Transport Layer Security（TLS）証明書を使用してアプライアンスとサーバ間のチャネルを保護できます。

各クライアント証明書は、アプライアンスやデバイスごとに異なります。複数のアプライアンスやデバイスがある場合、各アプライアンスについて次の手順をすべて実行します。

管理対象従来型デバイスから外部サーバへ、監査ログを安全にストリーミングするには、NGIPS デバイスから監査ログをセキュアにストリームする方法を参照してください。

次の手順を使用して、Firepower Management Center から外部サーバへ監査ログを安全にストリーミングします。

始める前に

クライアントおよびサーバ証明書を必須とする場合の影響については、監査ログ証明書 （51 ページ）を参照してください。

手順

ステップ 1 次の手順を実行して、署名付きクライアント証明書を入手し、アプライアンスにインストールします。

a) Management Center の署名付き監査ログ クライアント証明書の取得 （54 ページ）：

システム情報と指定した ID 情報に基づいて、アプライアンスで証明書署名要求（CSR）を生成します。

CSR を認識済みの信頼できる認証局（CA）に送信して、署名付きクライアント証明書を要求します。

アプライアンスと監査ログ サーバ間の相互認証が必要な場合、接続に使用するサーバ証明書に署名したのと同じ CA がクライアント証明書に署名する必要があります。

b) 認証局から署名付き証明書を受信した後は、その証明書をアプライアンスにインポートします。Management Center への監査ログ クライアント証明書のインポート （55 ページ）を参照してください。

ステップ 2 Transport Layer Security（TLS）を使用するサーバとの通信チャネルを設定し、相互認証を有効にします。

監査ログ サーバと Management Center 間にセキュアな接続が必要な場合 （56 ページ）を参照してください。

ステップ 3 まだ行っていない場合は、監査ログ ストリーミングを設定します。次を参照してください。

- syslog への監査ログ メッセージの送信 （49 ページ）
- 監査ログ メッセージを HTTP サーバに送信する （50 ページ）

Management Center の署名付き監査ログ クライアント証明書の取得

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス
該当なし	任意（Any）	Management Center	グローバルだけ	Admin

管理対象の従来型デバイスの証明書を取得するには、従来型デバイスの署名付き監査ログ クライアント証明書の取得を参照してください。

重要 ハイ アベイラビリティ設定のスタンバイ Firepower Management Center では [監査ログ証明書（Audit Log Certificate）] ページを使用できません。スタンバイ Firepower Management Center からこのタスクを実行することはできません。

システムは、ベース 64 エンコードの PEM 形式で証明書要求のキーを生成します。

始める前に

次の点を考慮してください。

- 証明書をインストールするデバイスまたはアプライアンスで、証明書署名要求（CSR）を生成する必要があります。（たとえば、アプライアンス A でデバイス B の証明書署名要求は生成できません。）各デバイスおよびアプライアンスで固有の証明書署名要求を生成する必要があります。
- セキュリティを確保するには、グローバルに認識された信頼できる認証局（CA）を使用して、証明書に署名します。
- アプライアンスと監査ログ サーバ間で相互認証が必要な場合は、同じ認証局によってクライアント証明書とサーバ証明書の両方が署名される必要があります。

手順

ステップ 1 **[システム（System）] > [設定（Configuration）]**を選択します。
ステップ 2 [監査ログ証明書（Audit Log Certificate）] をクリックします。
ステップ 3 [新規 CSR の生成（Generate New CSR）] をクリックします。
ステップ 4 [国名（2 文字のコード）（Country Name (two-letter code)）] フィールドに国番号を入力します。
ステップ 5 [都道府県（State or Province）] フィールドに、都道府県名を入力します。
ステップ 6 [市区町村（Locality or City）] を入力します。
ステップ 7 [組織（Organization）] の名前を入力します。
ステップ 8 [組織単位（部署名）（Organizational Unit (Department)）] の名前を入力します。

ステップ 9 [共通名（Common Name）] フィールドに、証明書を要求するサーバの完全修飾ドメイン名を入力します。

（注） 共通名と DNS ホスト名が一致しないと、監査ログのストリーミングは失敗します。

ステップ 10 [生成（Generate）] をクリックします。

ステップ 11 テキスト エディタで、新しい空のファイルを開きます。

ステップ 12 証明書要求のテキスト ブロック全体（`BEGIN CERTIFICATE REQUEST` 行と `END CERTIFICATE REQUEST` 行を含む）をコピーして、空のテキスト ファイルに貼り付けます。

ステップ 13 このファイルを *clientname*`.csr` として保存します。*clientname* は、証明書を使用する予定のアプライアンスの名前にします。

ステップ 14 [閉じる（Close）] をクリックします。

次のタスク

- この手順の「はじめる前に」セクションのガイドラインを使用して選択した認証局に、証明書署名要求を送信します。
- 署名された証明書を受け取ったら、アプライアンスにインポートします。Management Center への監査ログ クライアント証明書のインポート （55 ページ）を参照してください。

Management Center への監査ログ クライアント証明書のインポート

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス
任意（Any）	任意（Any）	Management Center	グローバルだけ	Admin

重要 ハイ アベイラビリティ設定のスタンバイ Firepower Management Center では [監査ログ証明書（Audit Log Certificate）] ページを使用できません。スタンバイ Firepower Management Center からこのタスクを実行することはできません。

（注） 監査ログ クライアント証明書を従来型管理対象デバイスにインポートする場合は、従来型デバイスへの監査ログ クライアント証明書のインポートを参照してください。

始める前に

- Management Center の署名付き監査ログ クライアント証明書の取得 （54 ページ）.

- 正しいアプライアンスの署名付き証明書をインポートしていることを確認します。各証明書は、アプライアンスやデバイスごとに異なります。
- 証明書を生成した署名認証局から中間 CA を信頼するように要求された場合は、必要な証明書チェーン（証明書パスとも呼ばれる）を提供します。クライアント証明書に署名した CA は、証明書チェーンのいずれの中間証明書に署名した CA と同じである必要があります。

手順

ステップ 1 Management Center で、**[システム（System）] > [設定（Configuration）]** を選択します。

ステップ 2 [監査ログ証明書（Audit Log Certificate）] をクリックします。

ステップ 3 [監査クライアント証明書のインポート（Import Audit Client Certificate）] をクリックします。

ステップ 4 テキスト エディタでクライアント証明書を開いて、`BEGIN CERTIFICATE` の行と `END CERTIFICATE` の行を含むテキストのブロック全体をコピーします。このテキストを [クライアント証明書（Client Certificate）] フィールドに貼り付けます。

ステップ 5 秘密キーをアップロードするには、秘密キー ファイルを開いて、`BEGIN RSA PRIVATE KEY` の行と `END RSA PRIVATE KEY` の行を含むテキストのブロック全体をコピーします。このテキストを [秘密キー（Private Key）] フィールドに貼り付けます。

ステップ 6 必要な中間証明書をすべて開いて、それぞれのテキストのブロック全体をコピーして、[証明書チェーン（Certificate Chain）] フィールドに貼り付けます。

ステップ 7 [保存（Save）] をクリックします。

監査ログ サーバと Management Center 間にセキュアな接続が必要な場合

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス
任意（Any）	任意（Any）	Management Center	グローバルだけ	Admin

システムは、識別符号化規則（DER）形式でインポートされている CRL を使用した、監査ログ サーバ証明書の検証をサポートしています。

（注） CRL を使用して証明書を確認する場合、システムは、監査ログ サーバ証明書の検証と、アプライアンスと Web ブラウザの間の HTTP 接続を保護する証明書の検証の両方に、同じ CRL を使用します。

重要　ハイ アベイラビリティ設定のスタンバイ Firepower Management Center では [監査ログ証明書（Audit Log Certificate）] ページを使用できません。スタンバイ Firepower Management Center からこのタスクを実行することはできません。

従来型管理対象デバイスの証明書を要求するには、監査ログ サーバと 7000 および 8000 シリーズ デバイスとの間にセキュアな接続が必要な場合を参照します。

始める前に

- 相互認証を必須とし、証明書失効リスト（CRL）を使用して証明書の有効性を保持する場合の影響について説明します。監査ログ証明書 （51 ページ）を参照してください。
- Management Center から監査ログを安全にストリーミングする方法 （52 ページ）に記載されている手順およびその手順で参照されているトピックに従って、クライアント証明書を取得してインポートします。

手順

ステップ 1　Management Center で、**[システム（System）]** > **[設定（Configuration）]** を選択します。

ステップ 2　[監査ログ証明書（Audit Log Certificate）] をクリックします。

ステップ 3　Transport Layer Security を使用して監査ログを安全に外部サーバへストリーミングするには、[TLSの有効化（Enable TLS）] 選択します。

ステップ 4　検証せずにサーバ証明書を受け入れる場合（非推奨）、次を実行します。

a)　[相互認証の有効化（Enable Mutual Authentication）] をオフにします。

b)　[保存（Save）] をクリックして、残りの手順をスキップします。

ステップ 5　監査ログ サーバの証明書を検証するには、[相互認証の有効化（Enable Mutual Authentication）] をオンにします。

ステップ 6　（相互認証を有効にした場合）無効な証明書を自動的に認識するには、次を実行します。

a)　[CRLの取得の有効化（Enable Fetching of CRL）] をオンにします。

（注）　CRL のフェッチを有効にすると、定期的に CRL を更新するスケジュール タスクが作成されます。

b)　既存の CRL ファイルへの有効な URL を入力して、[CRL の追加（Add CRL）] をクリックします。

最大 25 個まで CRL の追加を繰り返します。

c)　[CRL の更新（Refresh CRL）] をクリックして現在の CRL をロードするか、指定した URL から CRL をロードします。

ステップ 7　クライアント証明書を作成したものと同じ認証局によって生成された有効なクライアント証明書があることを確認します。

ステップ 8 [保存（Save）] をクリックします。

次のタスク

（オプション）CRL 更新の頻度を設定する場合は、証明書失効リストのダウンロードの設定を参照してください。

Management Center での監査ログ クライアント証明書の表示

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス
任意（Any）	任意（Any）	Management Center	グローバルだけ	Admin

ログインしているアプライアンスまたはデバイスの監査ログ クライアント証明書のみ表示できます。

（注） ハードウェア 7000 または 8000 シリーズまたは ASA FirePOWER 管理対象デバイスの監査ログ証明書を表示する場合は、従来型デバイスでの監査ログ クライアント証明書の表示を参照してください。

重要 ハイ アベイラビリティ設定のスタンバイ Firepower Management Center では [監査ログ証明書（Audit Log Certificate）] ページを使用できません。スタンバイ Firepower Management Center からこのタスクを実行することはできません。

Management Center で現在の監査ログ証明書を表示するには、次を実行します。

手順

ステップ 1 **[システム（System）] > [設定（Configuration）]**を選択します。

ステップ 2 [監査ログ証明書（Audit Log Certificate）] をクリックします。

ダッシュボード設定

ダッシュボードでは、ウィジェットを使用することにより、現在のシステム ステータスが一目でわかります。ウィジェットは小さな自己完結型コンポーネントであり、Firepower システム

のさまざまな側面に関するインサイトを提供します。Firepower システムには、事前定義された複数のダッシュボード ウィジェットが付属しています。

[カスタム分析（Custom Analysis）] ウィジェットがダッシュボードで有効になるように、Firepower Management Center を設定できます。

関連トピック

ダッシュボードについて

ダッシュボードのカスタム分析ウィジェットの有効化

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス
任意（Any）	任意（Any）	Management Center	グローバルだけ	Admin

[カスタム分析（Custom Analysis）] ダッシュボード ウィジェットを使用して、柔軟でユーザによる構成が可能なクエリに基づいてイベントのビジュアル表現を作成します。

手順

ステップ 1 **[システム（System）] > [設定（Configuration）]**を選択します。

ステップ 2 [ダッシュボード（Dashboard）] をクリックします。

ステップ 3 ユーザが [カスタム分析（Custom Analysis）] ウィジェットをダッシュボードに追加できるようにするには、[カスタム分析ウィジェットの有効化（Enable Custom Analysis Widgets）] チェックボックスをオンにします。

ステップ 4 [保存（Save）] をクリックします。

DNS キャッシュ

イベント表示ページで、IP アドレスを自動的に解決するようにシステムを設定できます。また、アプライアンスによって実行される DNS キャッシュの基本的なプロパティを設定できます。DNS キャッシングを設定すると、追加のルックアップを実行せずに、以前に解決した IP アドレスを識別できます。これにより、IP アドレスの解決が有効になっている場合に、ネットワーク上のトラフィックの量を減らし、イベント ページの表示速度を速めることができます。

DNS キャッシュ プロパティの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	Management Center	グローバルだけ	Admin

DNS 解決のキャッシングは、以前に解決された DNS ルックアップのキャッシングを許可するシステム全体の設定です。

手順

ステップ 1 **[システム（System）] > [設定（Configuration）]**を選択します。

ステップ 2 [DNS キャッシュ（DNS Cache）] を選択します。

ステップ 3 [DNS 解決のキャッシング（DNS Resolution Caching）] ドロップダウン リストから、次のいずれかを選択します。

- [有効化（Enabled）]：キャッシングを有効にします。
- [無効化（Disabled）]：キャッシングを無効にします。

ステップ 4 [DNS キャッシュ タイムアウト（分）（DNS Cache Timeout（in minutes））] フィールドで、非アクティブのために削除されるまで DNS エントリがメモリ内にキャッシュされる時間（分単位）を入力します。

デフォルトは 300 分（5 時間）です。

ステップ 5 [保存（Save）] をクリックします。

関連トピック

イベント ビュー設定の設定
管理インターフェイス （17 ページ）

電子メールの通知

次の処理を行う場合は、メール ホストを設定します。

- イベントベースのレポートの電子メール送信
- スケジュールされたタスクのステータス レポートの電子メール送信
- 変更調整レポートの電子メール送信
- データプルーニング通知の電子メール送信

- 検出イベント、インパクト フラグ、相関イベント アラート、侵入イベント アラート、およびヘルス イベント アラートでの電子メールの使用

電子メール通知を設定する場合、システムとメール リレー ホスト間の通信に使用する暗号化方式を選択し、必要に応じて、メール サーバの認証クレデンシャルを指定できます。設定した後、接続をテストできます。

メール リレー ホストおよび通知アドレスの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス
任意（Any）	任意（Any）	Management Center	グローバルだけ	Admin

手順

ステップ 1 **[システム（System）] > [設定（Configuration）]**を選択します。

ステップ 2 [電子メール通知（Email Notification）] をクリックします。

ステップ 3 [メール リレー ホスト（Mail Relay Host）] フィールドで、使用するメール サーバのホスト名または IP アドレスを入力します。入力したメール ホストはアプライアンスからのアクセスを許可している**必要があります**。

ステップ 4 [ポート番号（Port Number）] フィールドに、電子メール サーバで使用するポート番号を入力します。

一般的なポートには次のものがあります。

- 25。暗号化を使用しない場合
- 465。SSLv3 を使用する場合
- 587。TLS を使用する場合

ステップ 5 [暗号化方式（Encryption Method）] を選択します。

- [TLS]：Transport Layer Security を使用して通信を暗号化します。
- [SSLv3]：セキュア ソケット レイヤを使用して通信を暗号化します。
- [なし（None）]：暗号化されていない通信を許可します。

（注） アプライアンスとメール サーバとの間の暗号化された通信では、証明書の検証は不要です。

ステップ 6 [送信元アドレス（From Address）] フィールドに、アプライアンスから送信されるメッセージの送信元電子メール アドレスとして使用する有効な電子メール アドレスを入力します。

ステップ 7 必要に応じて、メール サーバに接続する際にユーザ名とパスワードを指定するには、[認証を使用（Use Authentication）] を選択します。[ユーザ名（Username）] フィールドにユーザ名を入力します。パスワードを [パスワード（Password）] フィールドに入力します。

ステップ 8 設定したメール サーバを使用してテスト メールを送信するには、[テスト メールのサーバ設定（Test Mail Server Settings）] をクリックします。
テストの成功または失敗を示すメッセージがボタンの横に表示されます。

ステップ 9 [保存（Save）] をクリックします。

言語の選択

[言語（Language）] ページを使用して、Web インターフェイス用に異なる言語を指定できます。

別の言語の指定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス
任意（Any）	任意（Any）	Management Center 7000 & 8000 シリーズ	任意（Any）	Admin

この設定は、Firepower Management Center または 7000 および 8000 シリーズ 管理対象デバイスに適用されます。

- Firepower Management Center では、この設定はシステム設定の一部になります。
- 7000 および 8000 シリーズ 管理対象デバイスでは、この設定をプラットフォーム設定ポリシーの一部として Firepower Management Center から適用します。

いずれの場合も、システム設定変更を保存するか、共有プラットフォーム設定ポリシーを展開するまで、設定は有効にはなりません。

注意 ここで指定した言語は、アプライアンスにログインしたすべてのユーザの Web インターフェイスに使用されます。

手順

ステップ 1 Firepower Management Center または従来型の管理対象デバイスのどちらを設定しているかに応じて、次の操作を実行します。

- Management Center：**[システム（System）] > [設定（Configuration）]** を選択します。
- 管理対象デバイス：**[デバイス（Devices）] > [プラットフォーム設定（Platform Settings）]** を選択し、Firepower ポリシーを作成または編集します。

ステップ 2 [言語（Language）] をクリックします。

ステップ 3 使用する言語を選択します。

ステップ 4 [保存（Save）] をクリックします。

次のタスク

- 設定変更を展開します。設定変更の展開を参照してください。

ログイン バナー

[ログイン バナー（Login Banner）] ページを使用して、セキュリティ アプライアンスまたは共有ポリシーのセッション バナー、ログイン バナー、カスタム メッセージ バナーを指定できます。

バナーのテキストにはスペースを使用できますが、タブは使用できません。バナーには複数行のテキストを指定できます。テキストに空の行が含まれている場合、バナーでは、その行が改行（CR）として表示されます。使用できるのは、改行（Enter キーを押す）を含む ASCII 文字だけです。改行は 2 文字としてカウントされます。

Telnet または SSH を介してセキュリティ アプライアンスにアクセスしたときに、バナー メッセージを処理するのに十分なシステム メモリがなかった場合や、バナー メッセージの表示を試行して TCP 書き込みエラーが発生した場合には、セッションが閉じます。

カスタム ログイン バナーの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス
任意（Any）	任意（Any）	Management Center 従来型	任意（Any）	Admin

SSH または Web インターフェイスからログインするユーザに向けて表示するカスタム ログイン バナーを作成できます。

この設定は、Firepower Management Center または従来型の管理対象デバイス（7000 および 8000 シリーズ、ASA FirePOWER および NGIPSv）に適用されます。

- Firepower Management Center では、この構成はシステム構成の一部です。
- 従来の管理対象デバイスでは、この構成をプラットフォーム設定ポリシーの一部として Firepower Management Center から適用します。

いずれの場合でも、システム設定の変更を保存するか、共有プラットフォーム設定ポリシーを展開するまで設定は有効になりません。

手順

ステップ 1 Firepower Management Center または Classic 管理対象デバイスのいずれを設定しているかに応じて、以下を実行します。

- Management Center：**[システム（System）]** > **[設定（Configuration）]** を選択します。
- 管理対象デバイスの場合：**[デバイス（Devices）]** > **[プラットフォーム設定（Platform Settings）]**を選択するか、ファイアウォール ポリシーを作成、または編集します。

ステップ 2 [ログイン バナー（Login Banner）] を選択します。

ステップ 3 [カスタム ログイン バナー（Custom Login Banner）] フィールドに、使用するログイン バナー テキストを入力します。

ステップ 4 [保存（Save）] をクリックします。

次のタスク

- 設定変更を展開します。設定変更の展開を参照してください。

SNMP ポーリング

Firepower Management Center およびクラシック管理対象デバイスには、Simple Network Management Protocol（SNMP）ポーリングを有効にすることができます。SNMP 機能は、SNMP プロトコルのバージョン 1、2、3 をサポートします。

この機能を使用して、次の要素にアクセスできます。

- 標準 Management Information Base（MIB）。これには、連絡先、管理、場所、サービス情報、IP アドレッシングやルーティングの情報、トランスミッション プロトコルの使用状況の統計などのシステムの詳細が含まれます。
- 7000 および 8000 シリーズ管理対象デバイスの追加の MIB。これには、物理インターフェイス、論理インターフェイス、仮想インターフェイス、ARP、NDP、仮想ブリッジ、仮想ルータを通して渡されるトラフィックの統計が含まれます。

（注） SNMP プロトコルの SNMP バージョンを選択する際は、SNMPv2 では読み取り専用コミュニティのみをサポートし、SNMPv3 では読み取り専用ユーザのみをサポートすることに注意してください。SNMPv3 は AES128 による暗号化もサポートします。

SNMP 機能を有効にすると、システムで SNMP トラップを送信できなくなり、MIB の情報はネットワーク管理システムによるポーリングでのみ使用可能になることに注意してください。

SNMP ポーリングの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス
任意（Any）	任意（Any）	Management Center 従来型	任意（Any）	Admin

この構成は、Firepower Management Center または従来の管理対象デバイス（7000 および 8000 シリーズ、ASA FirePOWER、および NGIPSv）に適用されます。

- Firepower Management Center では、この構成はシステム構成の一部です。
- 従来の管理対象デバイスでは、この構成をプラットフォーム設定ポリシーの一部として Firepower Management Center から適用します。

いずれの場合も、構成は、システム構成変更を保存するか、共有プラットフォーム設定ポリシーを展開するまで有効になりません。

（注） システムをポーリングするには、使用する任意のコンピュータで SNMP アクセスを追加する必要があります。SNMP MIB には展開の攻撃に使用される可能性がある情報も含まれているので注意してください。SNMP アクセスのアクセス リストを MIB のポーリングに使用される特定のホストに制限することをお勧めします。SNMPv3 を使用し、ネットワーク管理アクセスには強力なパスワードを使用することもお勧めします。

SNMPv3 は、読み取り専用ユーザと AES128 による暗号化のみをサポートしています。

始める前に

- システムのアクセス リストの設定 （47 ページ）の説明に従って、使用するコンピュータごとに SNMP アクセスを追加し、システムをポーリングします。

手順

ステップ 1 Firepower Management Center を構成するか従来の管理対象デバイスを構成するかに応じて、次の操作を実行します。

- Management Center：**[システム（System）]** > **[設定（Configuration）]** を選択します。
- 管理対象デバイス：**[デバイス（Devices）]** > **[プラットフォーム設定（Platform Settings）]** を選択し、Firepower ポリシーを作成または編集します。

ステップ 2 [SNMP] をクリックします。

ステップ 3 [SNMP バージョン（SNMP Version）] ドロップダウン リストから、使用する SNMP バージョンを選択します。

ステップ 4 次の選択肢があります。

- [バージョン 1（Version 1）] または [バージョン 2（Version 2）] を選択した場合は、[コミュニティ ストリング（Community String）] フィールドに SNMP コミュニティ名を入力します。手順 13 に進みます。

  （注） SNMPv2 は、読み取り専用コミュニティのみをサポートしています。

- [バージョン 3（Version 3）] を選択した場合、[ユーザを追加（Add User）] をクリックするとユーザ定義ページが表示されます。

  （注） SNMPv3 は、読み取り専用ユーザと AES128 による暗号化のみをサポートしています。

ステップ 5 ユーザ名を入力します。

ステップ 6 [認証プロトコル（Authentication Protocol）] ドロップダウン リストから、認証に使用するプロトコルを選択します。

ステップ 7 [認証パスワード（Authentication Password）] フィールドに SNMP サーバの認証に必要なパスワードを入力します。

ステップ 8 [パスワードの確認（Verify Password）] フィールドに、認証パスワードを再度入力します。

ステップ 9 使用するプライバシー プロトコルを [プライバシー プロトコル（Privacy Protocol）] リストから選択するか、プライバシー プロトコルを使用しない場合は [なし（None）] を選択します。

ステップ 10 [プライバシー パスワード（Privacy Password）] フィールドに SNMP サーバで必要な SNMP プライバシー キーを入力します。

ステップ 11 [パスワードの確認（Verify Password）] フィールドに、プライバシー パスワードを再度入力します。

ステップ 12 [追加（Add）] をクリックします。

ステップ 13 [保存（Save）] をクリックします。

次のタスク

- 設定変更を展開します。設定変更の展開を参照してください。

セキュリティ認定準拠の

お客様の組織が、米国防総省およびグローバル認定組織によって確立されたセキュリティ基準に従う機器とソフトウェアだけを使用することを求められる場合があります。Firepower システムでは、以下のセキュリティ認定標準規格へのコンプライアンスをサポートします。

- コモン クライテリア（CC）：国際コモン クライテリア承認アレンジメントによって確立された、セキュリティ製品のプロパティを定義するグローバル標準規格
- Unified Capabilities Approved Products List（UCAPL）：米国国防情報システム局（DISA）によって確立された、セキュリティ要件を満たす製品のリスト

（注） 米国政府は、Unified Capabilities Approved Products List（UCAPL）の名称を Defense Information Network Approved Products List（DODIN APL）に変更しました。このドキュメントおよび Firepower Management Center Web インターフェイスでの UCAPL の参照は、DODIN APL への参照として解釈できます。

- 連邦情報処理標準（FIPS）140：暗号化モジュールの要件に関する規定

セキュリティ認定コンプライアンスは、CC モードまたは UCAPL モードで有効にすることができます。セキュリティ認定コンプライアンスを有効にしても、選択したセキュリティ モードのすべての要件との厳密なコンプライアンスが保証されるわけではありません。強化手順についての詳細は、認定機関から提供されている本製品に関するガイドラインを参照してください。

注意 この設定を有効にした場合、無効にすることはできません。アプライアンスを CC モードまたは UCAPL モードでなくす必要がある場合は、アプライアンスを再イメージ化する必要があります。

セキュリティ認定準拠特性

次の表は、CC または UCAPL モードを有効にしたときの動作の変更を示しています。（ログイン アカウントの制約は、Web インターフェイス アクセスではなくコマンドラインまたはシェル アクセスを指します。）

システムの変更	CC モード	UCAPL モード
FIPS コンプライアンスは有効です。	○	○
バックアップまたはレポートについては、リモート ストレージは利用できません。	○	○
追加のシステム監査デーモンが開始されます。	なし	○
システム ブートローダは固定されています。	なし	○
追加のセキュリティがログイン アカウントに適用されます。	なし	○
ログインアカウントセッションの自動ログアウトを実行します。	なし	○
再起動キー シーケンスの Ctrl-Alt-Del を無効にします。	なし	○
最大 10 の同時ログイン セッションを実行します。	なし	○
バージョン 6.2.0.3 またはそれ以降の 6.2.0.x パッチでのみ、eStreamer を使用したイベント データのエクスポートがサポートされています。	○	○
ログイン アカウントの厳密なセーフガードを適用します。 • パスワードは、大文字および小文字を組み合わせて最大 15 の英数字として、1 つ以上の数字を含む必要があります。 • パスワードは、辞書に出現する単語であったり、連続する繰り返し文字を含んでいたりすることができません。 • 3 回連続ログインに失敗した場合、そのユーザはロックアウトされます。この場合は、管理者がパスワードをリセットする必要があります。 • パスワード履歴を保存しています。 • ログインが成功した場合は、失敗したログインの履歴を表示します。	なし	○

セキュリティ認定準拠の推奨事項

セキュリティ認定コンプライアンスの使用が有効のときに、次のベストプラクティスを確認することをお勧めします。

- 展開時にセキュリティ認定準拠を有効にするには、最初に Firepower Management Center で有効にし、次に、管理対象のすべてのデバイスの同じモードで有効にします。

注意 両方が同じセキュリティ認定準拠モードで動作していない限り、Firepower Management Center は管理対象デバイスからイベント データを受信しません。

- 高可用性設定で Firepower Management Center を使用すると、双方の設定を行い、同じセキュリティ認定準拠モードを使用します。
- 次の機能を使用するようにシステムを設定できません。
  - 電子メールレポート、アラート、データのプルーニング通知。
  - Nmap Scan、Cisco IOS Null Route、Set Attribute Value、ISE EPS の修復。
  - バックアップまたはレポート用のリモート ストレージ。
  - サードパーティ クライアントのシステム データベースへのアクセス。
  - 電子メール、SNMP トラップ、syslog から送信される外部通知、アラート。
  - アプライアンスとサーバの間のチャネルを保護するために、SSL 証明書を使用せずに、HTTP サーバまたは syslog サーバに送信された監査ログ メッセージ。
- バージョン 6.2.0.3 およびそれ以降の 6.2.0.x パッチの場合のみ、eStreamer を使用してイベント データを外部クライアントにエクスポートするようにシステムを設定できます。
- CC モードを使用して展開中に SSO を有効にできません。
- CC モードを使用して展開中に CAC を有効にできません。
- CC または UCAPL モードを使用した展開では、Firepower REST API 経由で Firepower Management Center および管理対象デバイスへのアクセスを無効にします。
- UCAPL モードを使用して展開中に CAC を有効にします。

（注） FirePOWER システムは、次の CC または UCAPL モードをサポートしていませんスタックまたはハイ アベイラビリティ ペアの従来型デバイス

セキュリティ認定コンプライアンスの有効化

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス
該当なし	任意（Any）	Management Center 従来型	任意（Any）	Admin

この構成は、Firepower Management Center または従来型の管理対象デバイス（7000 および 8000 シリーズ、ASA FirePOWER、NGIPSv）に適用されます。

- Firepower Management Center では、この構成はシステム構成の一部です。
- 従来型の管理対象デバイスでは、この構成をプラットフォーム設定ポリシーの一部として Firepower Management Center から適用します。

いずれの場合も、システム構成変更を保存するか、共有プラットフォーム設定ポリシーを展開するまでは、構成が有効になりません。

注意 この設定を有効にした後は、無効にすることはできません。アプライアンスを CC モードまたは UCAPL モードでなくす必要がある場合は、アプライアンスを再イメージ化する必要があります。

始める前に

- アプライアンスでセキュリティ認定コンプライアンスを有効にする前に、展開に組み込む予定のあるすべてのデバイスを Firepower Management Center に登録することをお勧めします。

手順

ステップ 1 設定するアプライアンスの種類に応じて、次のようにします。

- Management Center：**[システム（System）]** > **[設定（Configuration）]** を選択します。
- 従来型管理対象デバイス：**[デバイス（Devices）]** > **[プラットフォーム設定（Platform Settings）]** を選択し、Firepower ポリシーを作成または編集します。

ステップ 2 [UCAPL/CC コンプライアンス（UCAPL/CC Compliance）] をクリックします。

（注） UCAPL または CC コンプライアンスを有効にすると、アプライアンスがリブートします。Firepower Management Center は、システム設定を保存するとリブートし、管理対象デバイスは、設定の変更を展開するとリブートします。

ステップ 3 アプライアンスのセキュリティ認定コンプライアンスを永続的に有効にするには、2 つの選択肢があります。

- [コモン クライテリア（Common Criteria）] モードでセキュリティ認定コンプライアンスを有効にするには、ドロップダウン リストから [CC] を選択します。
- [Unified 機能承認製品リスト（Unified Capabilities Approved Products List）] モードでセキュリティ認定コンプライアンスを有効にするには、ドロップダウン リストから [UCAPL] を選択します。

ステップ 4 [保存（Save）] をクリックします。

次のタスク

- まだ適用していない場合は、制御と防御のライセンスを、展開内のすべての従来型アプライアンスに適用します。
- アプライアンスがバージョン 5.2.0 より前のバージョンから更新された場合は、セキュリティ認定コンプライアンスを有効にすると、アプライアンス証明書が再生成されます。展開全体でセキュリティ認定コンプライアンスを同じモードで有効にした後、管理対象デバイスを Firepower Management Center に再登録します。
- 設定変更を展開します。設定変更の展開を参照してください。

時刻および時刻同期

FirePOWER システムを正常に動作させるには、Firepower Management Center とその管理対象デバイスのシステム時刻を同期させることが不可欠です。

Management Center とすべてのデバイスのシステム時刻を同期させるには、Network Time Protocol（NTP）サーバを使用します。

⚠

注意 Firepower Management Center と管理対象デバイスの時刻が同期していないと、意図しない結果になることがあります。

ネットワーク NTP サーバを使用した時刻の同期

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス
任意（Any）	任意（Any）	Management Center	グローバルだけ	Admin

Firepower Management Center とすべての管理対象デバイス間で適切な同期を維持する最適な方法は、ネットワークで NTP サーバを使用することです。

始める前に

次の点に注意してください。

- リモート NTP サーバを指定する場合、アプライアンスおよびデバイスはそれに対するネットワーク アクセス権限を持っている必要があります。
- 信頼できない NTP サーバを指定しないでください。

- NTP サーバへの接続では、構成されたプロキシ設定は使用されません。

注意 Firepower Management Center が再起動され、ここで指定したものとは異なる NTP サーバ レコードを DHCP サーバが設定した場合、DHCP 提供の NTP サーバが代わりに使用されます。この状況を回避するには、同じ NTP サーバを設定するように DHCP サーバを設定します。

手順

ステップ 1 **[システム（System）] > [設定（Configuration）]**を選択します。

ステップ 2 [時間同期（Time Synchronization）] をクリックします。

ステップ 3 [NTP を使用して時間を提供（Serve Time via NTP）] が [有効（Enabled）] の場合、[無効（Disable）] を選択します。

ステップ 4 [マイクロックの設定（Set My Clock）] オプションには、[NTPの接続元（Via NTP from）] を選択して、NTP サーバのホスト名または IP アドレスを入力します。

組織内に連携する NTP サーバがある場合は、複数の NTP サーバをカンマ区切りのリストで入力します。

ステップ 5 [保存（Save）] をクリックします。

ステップ 6 管理対象デバイスでは同じ NTP サーバを使用して同期するように設定します。

管理対象デバイスに割り当てられたプラットフォーム設定ポリシーの [時刻同期（Time Synchronization）] 設定で、[NTPの接続元（Via NTP from）] に同期するようにクロックを設定して、上で指定したのと同じ NTP サーバを指定し、この変更をデバイスに展開します。手順については、次を参照してください。

- Firepower Threat Defense デバイスの場合は、次を参照してください。 脅威に対する防御のための NTP 時刻同期の設定
- その他すべてのデバイスについては、次を参照してください。 従来型デバイスでの時刻同期

ネットワーク NTP サーバにアクセスせずに時刻を同期

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス
任意（Any）	任意（Any）	Management Center	グローバルだけ	Admin

デバイスがネットワーク NTP サーバに直接アクセスできない、または組織内に Management Center および管理対象デバイスで時刻を同期するネットワーク NTP サーバがない場合は、物理ハードウェア Firepower Management Center を NTP サーバとして使用できます。

重要 仮想 Firepower Management Center を NTP サーバとして使用しません。

手順

ステップ 1 Firepower Management Center でシステム時刻を手動で設定するには、次の手順を実行します。

a) **[システム（System）] > [設定（Configuration）]**を選択します。
b) [時間同期（Time Synchronization）] をクリックします。
c) [NTP を使用して時間を提供（Serve Time via NTP）] が [有効（Enabled）] の場合、[無効（Disable）] を選択します。
d) [保存（Save）] をクリックします。
e) [マイクロックの設定（Set My Clock）] で、[ローカル設定で手動（Manually in Local Configuration）] を選択します。
f) [保存（Save）] をクリックします。
g) 画面の左側のナビゲーション パネルで [時間（Time）] をクリックします。
h) [時間の設定（Set Time）] ドロップダウン リストを使用して時間を設定します。
i) 表示されるタイムゾーンが UTC ではない場合、クリックして、タイムゾーンを [UTC] に設定します。
j) [保存（Save）] をクリックします。
k) [完了（Done）] をクリックします。
l) [適用（Apply）] をクリックします。

ステップ 2 Firepower Management Center を NTP サーバとして機能するように設定します。

a) 画面の左側のナビゲーション パネルで [時刻同期（Time Synchronization）] をクリックします。
b) [NTPを使用して時間を提供（Serve Time via NTP）] で、[有効（Enabled）] を選択します。
c) [保存（Save）] をクリックします。

ステップ 3 管理対象デバイスでは Firepower Management Center NTP サーバを使用して同期するように設定します。

管理対象デバイスに割り当てられたプラットフォーム設定ポリシーの [時刻同期（Time Synchronization）] 設定で、[Management CenterのNTPを使用（Via NTP from Management Center）] に同期するようにクロックを設定して、この変更を管理対象デバイスに展開します。手順については、次を参照してください。

- Firepower Threat Defense デバイスの場合は、次を参照してください。 脅威に対する防御のための NTP 時刻同期の設定

- その他すべてのデバイスについては、次を参照してください。 従来型デバイスでの時刻同期

時刻同期の設定の変更について

- NTP を使用して時刻を提供するように Management Center を設定してから、後でそれを無効にした場合、管理対象デバイスの NTP サービスは引き続き Management Center と時刻を同期しようとします。新しい時刻ソースを確立するには、すべての該当するプラットフォーム設定ポリシーを更新および再展開する必要があります。
- Firepower Management Center を NTP サーバとして設定してから時刻を変更する必要がある場合、NTP オプションを無効にして、時間を手動で変更してから NTP オプションを再度有効にする必要があります。

現在のシステム時刻、ソース、およびNTPサーバ接続ステータスの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス
任意（Any）	任意（Any）	Management Center	グローバルだけ	Admin

[ユーザ設定（User Preferences）] の [タイムゾーン（Time Zone）] ページで設定したタイムゾーン（デフォルトでは America/New York）を使用すると、ほとんどのページでローカル時刻で時刻設定が表示されますが、アプライアンスには UTC 時間を使用して格納されます。

さらに、現在の時刻は [時刻の同期（Time Synchronization）] ページの上部に UTC で表示されます（ローカル時刻は手動時計設定オプションで表示されます（有効になっている場合））。

（注） タイムゾーン機能（[ユーザ設定（User Preferences）]）は、デフォルトのシステム クロックが UTC 時間に設定されていることを前提としています。ローカル タイムゾーンを使用するようにアプライアンスのシステム クロックを変更した場合は、正確なローカル時刻が表示されるように、それを変更して UTC 時間に戻す必要があります。

（注） NGIPS ハードウェア デバイスで時刻および時刻源情報を表示する場合は、NGIPS デバイスの現在のシステム時刻、ソース、およびNTPサーバ接続ステータスの表示を参照してください。

手順

ステップ 1 **[システム（System）] > [設定（Configuration）]**を選択します。

ステップ 2 [時間（Time）] をクリックします。

アプライアンスで NTP サーバを使用する場合、テーブル エントリについては、NTP サーバのステータス （75 ページ）を参照してください。

NTP サーバのステータス

システムが NTP から時間を同期する場合、Firepower Management Center の [時間（Time）] ページ（[システム（System）] > [設定（Configuration）] メニューの下）と 7000 および 8000 シリーズ デバイスのローカル Web インターフェイスから NTP ステータスを表示できます。

表 *6 : NTP* ステータス

カラム	説明
NTP サーバ	構成済みの NTP サーバの IP アドレスと名前。
ステータス	NTP サーバの時間同期のステータス。 • [使用中（Being Used）] は、アプライアンスが NTP サーバと同期していることを示します。 • [使用可能（Available）] は、NTP サーバが使用可能であるものの、時間がまだ同期していないことを示します。 • [使用不能（Not Available）] は、NTP サーバが構成に含まれているものの、NTP デーモンがその NTP サーバを使用できないことを示します。 • [保留（Pending）] は、NTP サーバが新しいか、または NTP デーモンが最近再起動されたことを示します。この値は、時間の経過とともに [使用中（Being Used）]、[使用可能（Available）]、または [使用不能（Not Available）] に変わるはずです。 • [不明（Unknown）] は、NTP サーバのステータスが不明であることを示します。

カラム	説明
オフセット	アプライアンスと構成済みの NTP サーバ間の時間の差（ミリ秒）。負の値はアプライアンスの時間が NTP サーバより遅れていることを示し、正の値は進んでいることを示します。
Last Update	NTP サーバと最後に時間を同期してから経過した時間（秒数）。NTP デーモンは、いくつかの条件に基づいて自動的に同期時間を調整します。たとえば、更新時間が大きい（300秒など）場合、それは時間が比較的安定しており、NTP デーモンが小さい更新増分値を使用する必要がないと判断したことを示します。

セッション タイムアウト

Firepower システムの Web インターフェイスまたは補助コマンドライン インターフェイスの無人ログインセッションは、セキュリティ上のリスクを生じさせる場合があります。ユーザのログインセッションが非アクティブなったためにタイムアウトするまでのアイドル時間を分単位で設定できます。シェル（コマンドライン）セッションでも同様のタイムアウトを設定できます。

長期にわたり Web インターフェイスをパッシブかつセキュアにモニタする予定のユーザが、導入内に存在する可能性があります。ユーザ設定オプションで Web インターフェイスのセッション タイムアウトからユーザを除外することができます。メニュー オプションへの完全なアクセス権がある管理者ロールのユーザは、侵害が生じる場合、余分のリスクを生じさせますが、セッション タイムアウトから除外することはできません。

セッション タイムアウトの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	Management Center 従来型	任意（Any）	Admin

この構成は、Firepower Management Center または従来の管理対象デバイス（7000 および 8000 シリーズ、ASA FirePOWER、および NGIPSv）に適用されます。

- Firepower Management Center では、この構成はシステム構成の一部です。
- 従来の管理対象デバイスでは、この構成をプラットフォーム設定ポリシーの一部として Firepower Management Center から適用します。

いずれの場合も、構成は、システム構成変更を保存するか、共有プラットフォーム設定ポリシーを展開するまで有効になりません。

システムへのシェルアクセスを制限する必要がある場合、追加オプションによって補助コマンドライン インターフェイスの `expert` コマンドを永続的に無効にすることができます。アプライアンスでエキスパートモードを無効にすると、構成シェルアクセスを持つユーザでも、シェルのエキスパート モードに入ることができなくなります。ユーザが補助コマンドライン インターフェイスのエキスパートモードに入ると、ユーザはシェルに応じた任意のLinuxコマンドを実行できます。エキスパート モードに入っていない場合は、コマンドライン ユーザはコマンドライン インターフェイスが提供するコマンドだけを実行できます。

手順

ステップ 1 Firepower Management Center を構成するか従来の管理対象デバイスを構成するかに応じて、次の操作を実行します。

- Management Center：**[システム（System）] > [設定（Configuration）]** を選択します。
- 管理対象デバイス：**[デバイス（Devices）] > [プラットフォーム設定（Platform Settings）]** を選択し、Firepower ポリシーを作成または編集します。

ステップ 2 [シェル タイムアウト（Shell Timeout）] をクリックします。

ステップ 3 次の選択肢があります。

- Web インターフェイスのセッション タイムアウトを設定するには、[ブラウザ セッション タイムアウト（分）（Browser Session Timeout (Minutes)）] フィールドに数値（分数）を入力します。デフォルト値は `60` で、最大値は `1440`（24 時間）です。このセッション タイムアウトからユーザを除外する方法については、ユーザ アカウント ログイン オプションを参照してください。
- コマンドライン インターフェイスのセッション タイムアウトを設定するには、[シェル タイムアウト（分）（Shell Timeout (Minutes)）] フィールドに数値（分数）を入力します。デフォルト値は `0` で、最大値は `1440`（24 時間）です。
- 補助コマンドライン インターフェイスで `expert` コマンドを永続的に無効にするには、[expert コマンドを永続的に無効化（Permanently Disable Expert Access）] チェックボックスを選択します。

注意 エキスパート モードが無効になった状態でポリシーをアプライアンスに展開した場合、Web インターフェイスまたは補助コマンドライン インターフェイスを介してエキスパート モードにアクセスする機能を復元することはできません。エキスパート モード機能を復元するには、サポートに問い合わせる必要があります。

ステップ 4 [保存（Save）] をクリックします。

次のタスク

- 設定変更を展開します。設定変更の展開を参照してください。

脆弱性マッピング

サーバのディスカバリ イベント データベースにアプリケーション ID が含まれており、トラフィックのパケット ヘッダにベンダーおよびバージョンが含まれる場合、Firepower システムは、そのアドレスから送受信されるすべてのアプリケーション プロトコル トラフィックについて、脆弱性をホスト IP アドレスに自動的にマップします。

パケットにベンダー情報もバージョン情報も含まれないサーバすべてに対して、システムでこれらのベンダーとバージョンレスのサーバのサーバ トラフィックと脆弱性を関連付けるかどうかを設定できます。

たとえば、ホストがヘッダーにベンダーまたはバージョンが含まれていないSMTP トラフィックを提供しているとします。システム設定の [脆弱性マッピング（Vulnerability Mapping）] ページでSMTP サーバを有効にしてから、そのトラフィックを検出するデバイスを管理するFirepower Management Center にその設定を保存した場合、SMTP サーバと関連付けられているすべての脆弱性がそのホストのホスト プロファイルに追加されます。

ディテクタがサーバ情報を収集して、それをホストプロファイルに追加しますが、アプリケーション プロトコル ディテクタは脆弱性のマッピングに使用されません。これは、カスタム アプリケーション プロトコル ディテクタにベンダーまたはバージョンを指定できず、また脆弱性マッピング用のサーバを選択できないためです。

サーバの脆弱性のマッピング

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス
任意（Any）	保護	Management Center	グローバルだけ	Admin

手順

ステップ 1 **[システム（System）] > [設定（Configuration）]**を選択します。

ステップ 2 [脆弱性マッピング（Vulnerability Mapping）] を選択します。

ステップ 3 次の選択肢があります。

- ベンダーまたはバージョンの情報が含まれていないアプリケーション プロトコル トラフィックを受信するホストに、サーバの脆弱性がマップされないようにするには、そのサーバのチェックボックスをオフにします。
- ベンダーまたはバージョンの情報が含まれていないアプリケーション プロトコル トラフィックを受信するホストに、サーバの脆弱性がマップされるようにするには、そのサーバのチェックボックスをオフにします。

ヒント [有効（Enabled）]の横にあるチェックボックスを使用すると、すべてのチェックボックスを一度にオンまたはオフにできます。

ステップ 4 [保存（Save）] をクリックします。

リモート コンソールのアクセス管理

サポート対象システム上でリモート アクセスを行うため、VGA ポート（デフォルト）または物理アプライアンス上のシリアル ポートを介して Linux システムのコンソールを使用できます。組織の Cisco 導入の物理レイアウトに最も適したオプションを選択してください。

サポートされている物理ハードウェア ベースの Firepower システムでは、Serial Over LAN（SOL）接続のデフォルト管理インターフェイス（`eth0`）で Lights-Out 管理（LOM）を使用すると、システムの管理インターフェイスにログインすることなく、リモートでシステムをモニタまたは管理できます。アウトオブバンド管理接続のコマンドライン インターフェイスを使用すると、シャーシのシリアル番号の表示や状態（ファン速度や温度など）のモニタなどの、限定タスクを実行できます。

LOM は、システムとシステムを管理するユーザの両方で有効にする必要があります。システムとユーザを有効にした後、サードパーティ製の Intelligent Platform Management Interface（IPMI）ユーティリティを使用し、システムにアクセスして管理します。

システム上のリモート コンソール設定の構成

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス
任意（Any）	任意（Any）	Management Centerおよび7000 & 8000 シリーズ	グローバルだけ	LOM アクセス権限のある Admin

始める前に

- デバイスの管理インターフェイスに接続されたサードパーティ スイッチング装置で、スパニング ツリー プロトコル（STP）を無効にします。

手順

ステップ 1 **[システム（System）] > [設定（Configuration）]**を選択します。

ステップ 2 [コンソール構成（Console Configuration）] をクリックします。

ステップ 3 リモート コンソール アクセスのオプションを選択します。

- アプライアンスの VGA ポートを使用するには、[VGA] を選択します。

- アプライアンスのシリアル ポートを使用するか、Firepower Management Center、Firepower 7050、または 8000 シリーズ デバイス上で LOM/SOL を使用する場合には、[物理シリアル ポート（Physical Serial Port）] を選択します。
- 7000 シリーズ デバイス（Firepower 7050 以外）で LOM/SOL を使用する場合は、[Lights-Out Management] を選択します。これらのデバイスでは、SOL と通常のシリアル接続を同時に使用することはできません。

（注） リモート コンソールを [物理シリアル ポート（Physical Serial Port）] から [Lights-Out Management] に変更した場合や、70xx ファミリのデバイス（Firepower 7050 以外）で [Lights-Out Management] から [物理シリアル ポート（Physical Serial Port）] に変更した場合は、アプライアンスを 2 回リブートしないと、期待どおりのブート プロンプトが表示されないことがあります。

ステップ 4 SOL 経由で LOM を設定するには、必要な IPv4 設定を入力します。

- システムのアドレス構成（[DHCP] または [Manual（手動）]）を選択します。
- LOM に使用する IP アドレスを入力します。

（注） LOM IP アドレスは、システムの管理インターフェイスの IP アドレスとは異なる必要があります。

- システムのネットマスクを入力します。
- システムのデフォルト ゲートウェイを入力します。

ステップ 5 [保存（Save）] をクリックします。

次のタスク

- Lights-Out Management を設定した場合は、Lights-Out Management ユーザを有効にします。Lights-Out 管理のユーザ アクセス設定 （80 ページ）を参照してください。

Lights-Out 管理のユーザ アクセス設定

Lights-Out 管理機能を使用するユーザに対して、この機能の権限を明示的に付与する必要があります。LOM ユーザには、次のような制約もあります。

- ユーザに Administrator ロールを割り当てる必要があります。
- ユーザ名に使用できるのは英数字 16 文字までです。LOM ユーザに対し、ハイフンやそれより長いユーザ名はサポートされていません。
- 71xx ファミリ デバイスへの設定を除き、パスワードには最大 20 文字の英数字を使用できます。Firepower 7110、7115、7120、または 7125 デバイスで LOM が有効になっている場合、パスワードには最大 16 文字の英数字を使用できます。20 または 16 文字よりも長いパスワードは、LOM ユーザに対してサポートされません。ユーザの LOM パスワードは、そ

のユーザのシステムパスワードと同じです。辞書に載っていない複雑な最大長のパスワードをアプライアンスに対して使用し、それを 3 か月ごとに変更することを推奨します。

- 物理 Firepower Management Center および 8000 シリーズ デバイスには、最大 13 人の LOM ユーザを設定できます。8000 シリーズ デバイスには、最大 8 人の LOM ユーザを設定できます。

あるロールを持つユーザのログイン中に LOM でそのロールを非アクティブ化してから再アクティブ化した場合や、ユーザのログインセッション中にそのユーザまたはユーザ ロールをバックアップから復元した場合、そのユーザは IPMItool コマンドへのアクセスを回復するために Web インターフェイスにログインし直す必要があります。

Lights-Out 管理ユーザ アクセスの有効化

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	Management Centerおよび7000 & 8000 シリーズ	グローバルだけ	LOM アクセス権限のある Admin

各システムのローカル Web インターフェイスを使用して、システムごとに LOM と LOM ユーザを設定します。つまり、Firepower Management Center を使用して管理対象デバイスで LOM を設定することはできません。同様に、ユーザはアプライアンスごとに個別に管理されるため、Firepower Management Center で LOM 対応ユーザを有効化または作成しても、管理対象デバイスのユーザにはその機能は転送されません。

手順

ステップ 1 **[システム（System）] > [設定（Configuration）]**を選択します。

ステップ 2 [コンソール構成（Console Configuration）] をクリックします。

ステップ 3 [Lights Out 管理（Lights Out Management）] をクリックします。

ステップ 4 次の選択肢があります。

- 既存のユーザに LOM ユーザ アクセスを許可するには、リスト内のユーザ名の横にある編集アイコン（  ）をクリックします。
- 新しいユーザに LOM ユーザ アクセスを許可するには、[ユーザの作成（Create User）] をクリックします。

ステップ 5 [ユーザの設定（User Configuration）] で、Administrator ロールを有効にします。

ステップ 6 [Lights-Out 管理アクセスの許可（Allow Lights-Out Management Access）] チェックボックスをオンにします。

ステップ 7 [保存（Save）] をクリックします。

Serial over LAN 接続の設定

アプライアンスへの Serial over LAN 接続を作成するには、コンピュータ上でサードパーティ製の IPMI ユーティリティを使用します。Linux 系環境または Mac 環境を使用するコンピュータでは IPMItool を使用し、Windows 環境では IPMIutil を使用します。

（注） シスコでは、IPMItool バージョン 1.8.12 以降の使用を推奨しています。

Linux

多くのディストリビューションで IPMItool が標準となっており、使用可能です。

Mac

Mac では、IPMItool をインストールする必要があります。最初に、Mac に Apple の XCode Apple Developer Tools がインストールされていることを確認します。これにより、コマンドライン開発用のオプション コンポーネント（新しいバージョンでは UNIX Development and System Tools、古いバージョンでは Command Line Support）がインストールされていることを確認できます。次に、MacPorts と IPMItool をインストールします。詳細については、好みの検索エンジンを使用するか、次のサイトを参照してください。

```
https://developer.apple.com/technologies/tools/
http://www.macports.org/
```

Windows

Windows では、IPMIutil をコンパイルする必要があります。コンパイラにアクセスできない場合は、IPMIutil 自体を使用してコンパイルできます。詳細については、好みの検索エンジンを使用するか、次のサイトを参照してください。

```
http://ipmiutil.sourceforge.net/
```

IPMI ユーティリティのコマンドについて

IPMI ユーティリティで使用するコマンドは、次の IPMItool の例に示したセグメントで構成されます。

```
ipmitool -I lanplus -H IP_address -U user_name command
```

引数の説明

- `ipmitool` はユーティリティを起動します
- `-I lanplus` はセッションの暗号化を有効にします
- `-H` IP_address はアクセスするアプライアンスの IP アドレスを示します
- `-U` user_name は権限を持つユーザの名前です

- - command は指定するコマンドの名前です

（注） シスコでは、IPMItool バージョン 1.8.12 以降の使用を推奨しています。

Windows 用の同等のコマンドは次のとおりです。

```
ipmiutil command -V 4 -J 3 -N IP_address -Uuser_name
```

このコマンドは、アプライアンスのコマンドラインにユーザを接続します。これによって、ユーザは物理的にそのアプライアンスの近くにいるときと同じようにログインできます。場合によっては、パスワードの入力を求められます。

IPMItool を使用した Serial Over LAN の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス
任意（Any）	任意（Any）	Management Centerおよび7000 & 8000 シリーズ	任意（Any）	LOM アクセス権限のある Admin

手順

IPMItool を使用して、次のコマンドと、プロンプトが表示されたらパスワードを入力します:

```
ipmitool -I lanplus -H IP_address -U user_name sol activate
```

IPMIutil を使用した Serial Over LAN の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス
任意（Any）	任意（Any）	Management Centerおよび7000 & 8000 シリーズ	任意（Any）	LOM アクセス権限のある Admin

手順

IPMIutil を使用して、次のコマンドと、プロンプトが表示されたらパスワードを入力します。

```
ipmiutil -J 3 -H IP_address -U username sol -a
```

Lights-Out 管理の概要

Lights-Out 管理（LOM）では、システムにログインすることなく、デフォルトの管理インターフェイス（eth0）から SOL 接続を介して一連の限定操作を実行できます。SOL 接続を作成するコマンドに続いて、次のいずれかの LOM コマンドを使用します。コマンドが完了すると、接続は終了します。電源制御コマンドの中には、70xx Family デバイスに対して有効でないものもあります。

（注） Firepower 71xx、Firepower 82xx、または Firepower 83xx デバイスのベースボード管理コントローラ（BMC）は、ホストの電源がオンのときにのみ 1 Gbps のリンク速度でアクセスできます。デバイスの電源がオフの場合、BMC は 10/100 Mbps でのみイーサネット リンクを確立できます。したがって、デバイスにリモートから電源供給するために LOM を使用している場合は、10/100 Mbps のリンク速度だけを使用してデバイスをネットワークに接続してください。

注意 まれに、コンピュータがシステムの管理インターフェイスとは異なるサブネットにあり、そのシステムに DHCP が構成されている場合は、LOM 機能にアクセスしようとすると失敗することがあります。この場合は、システムの LOM を無効にして再び有効にするか、または同じサブネット上のコンピュータをシステムとして使用して、その管理インターフェイスを ping することができます。その後、LOM を使用できるようになるはずです。

注意 シスコでは、Intelligent Platform Management Interface（IPMI）標準（CVE-2013-4786）に内在する脆弱性を認識しています。システムの Lights-Out 管理（LOM）を有効にすると、この脆弱性にさらされます。この脆弱性を軽減するために、信頼済みユーザだけがアクセス可能なセキュアな管理ネットワークにシステムを展開し、辞書に載っていない複雑な最大長のパスワードをシステムに対して使用し、それを 3 か月ごとに変更してください。この脆弱性のリスクを回避するには、LOM を有効にしないでください。

システムへのアクセス試行がすべて失敗した場合は、LOM を使用してリモートでシステムを再起動できます。SOL 接続がアクティブなときにシステムが再起動すると、LOM セッションが切断されるか、またはタイムアウトする可能性があります。

注意 システムが別の再起動の試行に応答している間は、システムを再起動**しないでください**。リモートでシステムを再起動すると、通常の方法でシステムがリブートしないため、データが失われる可能性があります。

表 *7 : Lights-Out* 管理のコマンド

IPMItool	IPMIutil	説明
（適用なし）	`-V 4`	IPMI セッションの管理者権限を有効にします。
`-I lanplus`	`-J 3`	IPMI セッションの暗号化を有効にします。
`-H`	`-N`	リモート アプライアンスの IP アドレスを指定します。
`-U`	`-U`	認可された LOM アカウントのユーザ名を指定します。
`sol activate`	`sol -a`	SOL セッションを開始します。
`sol deactivate`	`sol -d`	SOL セッションを終了します。
`chassis power cycle`	`power -c`	アプライアンスを再起動します（70xx Family デバイスでは無効）。
`chassis power on`	`power -u`	アプライアンスの電源を投入します。
`chassis power off`	`power -d`	アプライアンスの電源をオフにします（70xx Family デバイスでは無効）。
`sdr`	`sensor`	アプライアンスの情報（ファン速度や温度など）を表示します。

たとえば、アプライアンスの情報のリストを表示する IPMItool のコマンドは、次のとおりです。

```
ipmitool -I lanplus -H IP_address -U user_name sdr
```

（注） シスコでは、IPMItool バージョン 1.8.12 以降の使用を推奨しています。

IPMIutil ユーティリティの同等のコマンドは次のとおりです。

```
ipmiutil sensor -V 4 -J 3 -N IP_address -U user_name
```

IPMItool による Lights-Out Management の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス
任意（Any）	任意（Any）	Management Centerおよび7000 & 8000 シリーズ	任意（Any）	LOM アクセス権限のある Admin

手順

プロンプトが表示されたら、IPMItool の次のコマンドとパスワードを入力します。

```
ipmitool -I lanplus -H IP_address -U user_name command
```

IPMIutil による Lights-Out Management の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス
任意（Any）	任意（Any）	Management Centerおよび7000 & 8000 シリーズ	任意（Any）	LOM アクセス権限のある Admin

手順

プロンプトが表示されたら、IPMIutil の次のコマンドとパスワードを入力します。

```
ipmiutil -J 3 -H IP_address -U username command
```

REST API 設定

Firepower の REST API は、サードパーティ アプリケーションで REST クライアントおよび標準HTTP メソッドを使用してアプライアンス設定を表示および管理するための軽量のインターフェイスを提供します。Firepower の REST API の詳細については、『*Firepower REST API Quick Start Guide*』を参照してください。

デフォルトでは、Firepower Management Center はアプリケーションからの REST API を使用した要求を許可します。このアクセスをブロックするように Firepower Management Center を設定できます。

REST API アクセスの有効化

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス
任意（Any）	任意（Any）	Management Center	任意（Any）	Admin

（注） Firepower Management Center ハイ アベイラビリティを使用する展開では、この機能は、アクティブな Firepower Management Center でだけ使用できます。

手順

ステップ 1 **[システム（System）] > [設定（Configuration）]** を選択します。

ステップ 2 [REST API 設定（REST API Preferences）] をクリックします。

ステップ 3 Firepower Management Center への REST API アクセスを有効または無効にするには、[REST API の有効化（Enable REST API）] チェックボックスをオンまたはオフにします。

ステップ 4 [保存（Save）] をクリックします。

VMware Tools と仮想システム

VMware Tools は、仮想マシン向けのパフォーマンスを向上させるためのユーティリティ スイートです。これらのユーティリティを使用すると、VMware 製品の便利な機能をフルに活用できます。VMware で実行されている Firepower 仮想アプライアンスは、次のプラグインをサポートします。

- guestInfo
- powerOps
- timeSync
- vmbackup

サポートされるすべてのバージョンの ESXi で VMware Tools を有効にすることもできます。サポートされているバージョンの一覧については、『*Cisco Firepower NGIPSv for VMware* クイック スタート ガイド』を参照してください。VMware Tools のすべての機能については、VMware の Web サイト（http://www.vmware.com/）を参照してください。

VMware 向け Firepower Management Center での VMware ツールの有効化

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス
任意（Any）	任意（Any）	Firepower Management Center	グローバルだけ	Admin

NGIPSv には Web インターフェイスがないため、そのプラットフォームで VMware ツールを有効にするには CLI を使用する必要があります（*Cisco Firepower NGIPSv for VMware* クイック スタート ガイドを参照）。

手順

ステップ 1 **[システム（System）] > [設定（Configuration）]**を選択します。

ステップ 2 [VMware ツール（VMware Tools）] をクリックします。

ステップ 3 [VMware ツールの有効化（Enable VMware Tools）] をクリックします。

ステップ 4 [保存（Save）] をクリックします。