Cisco Firepower バージョン 6.4.0 リリースノート

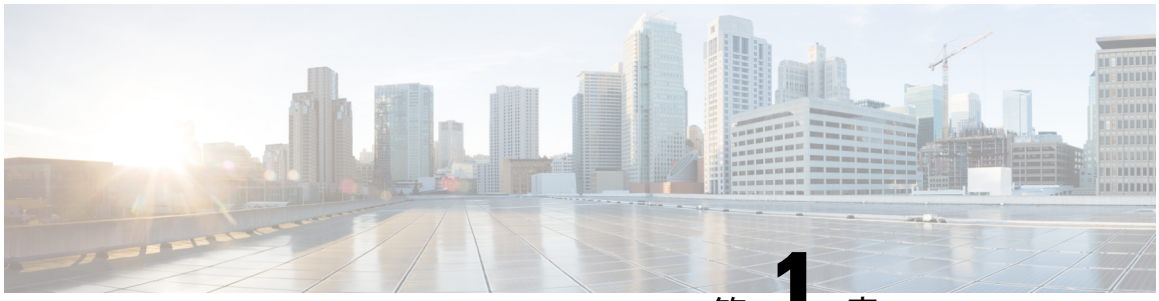
初版：2019 年 4 月 24 日

最終更新：2020 年 4 月 16 日

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

【注意】シスコ製品をご使用になる前に、安全上の注意（ **www.cisco.com/jp/go/safety_warning/** ）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

目 次



第 1 章

バージョン 6.4.0 の概要

Firepower をお選びいただき、ありがとうございます。

リリース ノートについて

リリース ノートには、アップグレードの警告や動作の変更など、バージョン 6.4.0 に関する重要なリリース固有の情報が記載されています。Firepower リリースに精通しており、Firepower 展開をアップグレードした経験がある場合でも、このドキュメントお読みください。

Firepower ソフトウェアのアップグレードまたは新規インストールは、複雑なプロセスになる場合があります。ここで手順を説明する代わりに、リリース ノートでは適切なリソースを示しています。アップグレードとインストールの手順については、次のリンクを参照してください。

- アップグレード手順 （68 ページ）
- 設置手順 （77 ページ）

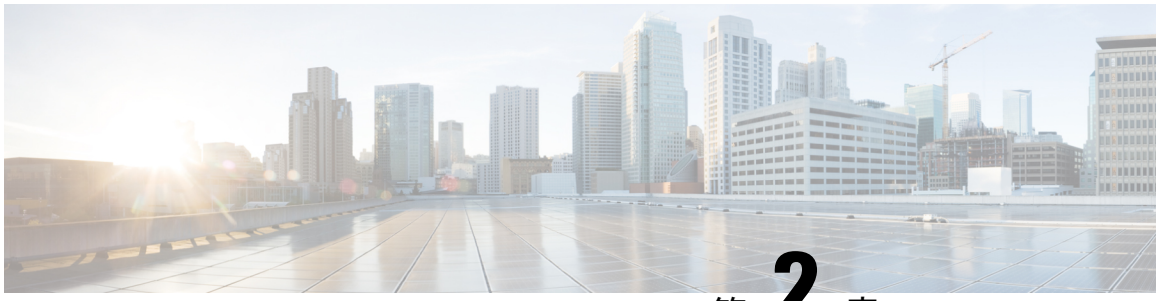
リリース日

バージョン 6.4.0 で使用可能なすべてのプラットフォームの一覧については、「互換性, on page 3」を参照してください。

シスコは、更新版ビルドを適宜リリースしています。ほとんどの場合、各プラットフォームの最新のビルド番号のみが、シスコ サポートおよびダウンロード サイト で入手可能です。最新のビルドを使用することを強くお勧めします。以前のビルドをダウンロードした場合は使用しないでください。詳細については、新しいビルドで解決済みの問題, on page 85を参照してください。

Table 1: バージョン *6.4.0* のリリース日

ビルド（**Build**）	日付（**Date**）	プラットフォーム
113	2020 年 3 月 3 日	FMC/FMCv
102	2019 年 6 月 20 日	Firepower 4115、4125、4145 SM-40、SM-48、およびSM-56モジュールを搭載した Firepower 9300
	2019 年 6 月 13 日	Firepower 1010、1120、1140
	2019 年 4 月 24 日	Firepower 2110、2120、2130、2140 Firepower 4110、4120、4140、4150 SM-24、SM-36、およびSM-44モジュールを搭載した Firepower 9300 ASA 5508-X、5515-X、5516-X、5525-X、5545-X、5555-X ASA 5585-X-SSP-10、-20、-40、-60 ISA 3000 FTDv Firepower 7000/8000 シリーズ NGIPSv



第 2 章

互換性

この章では、Firepower バージョン 6.4.0の互換性に関する情報を提供します。

Firepower Management Centerについて

バージョン 6.4.0 Firepower Management Center ソフトウェアは、物理および仮想プラットフォームでサポートされています。FMC は、混在展開を含めて、FTD または NGIPS を実行する複数のデバイスを管理できます。

Firepower Management Center 物理プラットフォーム

バージョン 6.4.0 は、以下をサポートします。

- FMC 1600、2600、4600
- FMC 1000、2500、4500
- FMC 2000、4000
- FMC 750、1500、3500

BIOS および RAID コントローラのファームウェアを最新の状態に保つことをお勧めします。詳細については、Cisco Firepower Compatibility Guideを参照してください。

Firepower Management Center Virtual （FMCv）プラットフォーム：

バージョン 6.4.0 は、以下をサポートします。

- VMware vSphere/VMware ESXi 6.0 または 6.5 上の FMCv

- カーネルベース仮想マシン（KVM）上の FMCv
- Amazon Web Services（AWS）上の FMCv
- Microsoft Azure 上の FMCv

サポートされている FMCv インスタンスについては、『Cisco Firepower Management Center Virtual 入門ガイド』を参照してください。

Firepower デバイス

バージョン 6.4.0 Firepower デバイス ソフトウェアは、さまざまな物理および仮想プラットフォームでサポートされています。

- **ソフトウェア**：一部の Firepower デバイスは Firepower Threat Defense（FTD）ソフトウェアを実行します。また、一部の Firepower デバイスは NGIPS/ASA FirePOWER ソフトウェアを実行します。一部ではどちらを実行することもできますが、両方を同時に実行することはできません。
- **リモート管理**：すべての Firepower デバイスは、複数のデバイスを管理できる Firepower Management Center（FMC）を使用したリモート管理をサポートします。
- **ローカル管理**：一部の Firepower デバイスは、ローカルの単一デバイス管理をサポートしています。Firepower Device Manager（FDM）で FTD を管理するか、ASDM で ASA FirePOWER を管理できます。一度に 1 つのデバイスに関して使用できる管理方法は 1 つだけです。
- **OS/ハイパーバイザ**：一部の Firepower 実装では、オペレーティングシステムとソフトウェアがバンドルされます。その他の実装では、自分でオペレーティング システムをアップグレードする必要があります。バンドルされたオペレーティングシステムのバージョンとビルドについては、Cisco Firepower Compatibility Guideの「Bundled Components」の情報を参照してください。

サポートされている Firepower のデバイス

次の表は、バージョン 6.4.0 を実行している Firepower デバイスの互換性情報を示しています。ここでも、すべてのデバイスがリモート FMC 管理をサポートしていることに注意してください。

表 *2*：バージョン *6.4.0* の *Firepower* デバイス

デバイスのプラットフォーム	ソフトウェア	ローカル管理	OS/ハイパーバイザ
Firepower 1010、1120、1140 Firepower 2110、2120、2130、2140	FTD	FDM	—

デバイスのプラットフォーム	ソフトウェア	ローカル管理	OS/ハイパーバイザ
Firepower 4110、4120、4140、4150 Firepower 4115、4125、4145 Firepower 9300 SM-24、SM-36、SM-44 モジュールを搭載 Firepower 9300 SM-40、SM-48、SM-56 モジュールを搭載	FTD	—	FXOS 2.6.1.157 以降のビルド。 個別のアップグレード。最初に FXOS をアップグレードします。 問題を解決するには、FXOS を最新のビルドにアップグレードする必要がある場合があります。判断のヒントについては、『Cisco Firepower 4100/9300 FXOS Release Notes, 2.6(1)』を参照してください。
ISA 3000	FTD	FDM	—
ASA 5508-X、5516-X ASA 5515-X、5525-X、5545-X、5555-X	ASA FirePOWER（NGIPS）	ASDM	次のいずれかです。 • ASA 9.5(2)、9.5(3) • ASA 9.6(x) ～ 9.14(x) 例外： • ASA 5515-X デバイスは ASA 9.13(x)+ をサポートしていません。 個別のアップグレード。操作の順序については、『Cisco ASA Upgrade Guide』を参照してください。 ASA と ASA FirePOWER のバージョンには幅広い互換性があります。ただし、厳密には ASA のアップグレードが必要でない場合でも、問題解決のために、サポートされた最新のバージョンへのアップグレードが必要になることがあります。 ASA 5508-x、および 5516-x を最新の ROMMON イメージにアップグレードすることをお勧めします。手順については、『Cisco ASA and Firepower Threat Defense Reimage Guide』を参照してください。

デバイスのプラットフォーム	ソフトウェア	ローカル管理	OS/ハイパーバイザ
ASA 5585-X-SSP-10、-20、-40、-60	ASA FirePOWER（NGIPS）	ASDM	次のいずれかです。 • ASA 9.5(2)、9.5(3) • ASA 9.6(x) ～ 9.12(x) 個別のアップグレード。操作の順序については、『Cisco ASA Upgrade Guide』を参照してください。 ASA と ASA FirePOWER のバージョンには幅広い互換性があります。ただし、厳密にはASA のアップグレードが必要でない場合でも、問題解決のために、サポートされた最新のバージョンへのアップグレードが必要になることがあります。
FTDv	FTD	FDM（VMware および KVM のみ）	次のいずれかです。 • VMware vSphere/VMware ESXi 6.0 または 6.5 • KVM • AWS • Microsoft Azure サポートされているインスタンスについては、該当するFTDv のスタートアップガイドを参照してください。
NGIPSv	NGIPS	—	VMware vSphere/VMware ESXi 6.0 または 6.5 サポートされているインスタンスについては、『Cisco Firepower NGIPSv Quick Start Guide for VMware』を参照してください。
Firepower 7010、7020、7030、7050 Firepower 7110、7115、7120、7125 Firepower 8120、8130、8140 Firepower 8250、8260、8270、8290 Firepower 8350、8360、8370、8390 AMP 7150、8050、8150 AMP 8350、8360、8370、8390	NGIPS	選択した管理機能のためのローカル GUI が制限されています。	—

マネージャとデバイスの互換性

FMC では、管理対象のデバイスと同じメジャーバージョンを実行している必要があります。パッチ未適用の FMC を使用してパッチを適用したデバイスを管理することもできますが、新しい機能と解決済みの問題では、多くの場合 FMC とその管理対象デバイスの「両方」で最新のパッチが必要になります。環境全体をパッチすることを強くお勧めします。

Table 3: バージョン *6.4.0* のマネージャとデバイスの互換性

Firepower Management Center		
バージョン 6.4.0 FMC	管理可能	バージョン 6.1 ～ 6.4.0.x のデバイス。
バージョン 6.4.0 のデバイス	必須	バージョン 6.4.0 FMC。
Firepower Device Manager		
バージョン 6.4.0 FDM	管理可能	FTD デバイス 1 台。
ASDM		
バージョン 7.12.1 の ASDM	管理可能	バージョン 6.4.0.x 以前の ASA FirePOWER モジュール。
バージョン 6.4.0 ASA FirePOWER module	必須	バージョン 7.12.1 の ASDM。

Web ブラウザの互換性

Firepower によってモニタされるネットワークからの Web の参照

多くのブラウザでは、デフォルトで Transport Layer Security（TLS）v1.3 が使用されています。暗号化されたトラフィックを処理するために SSL ポリシーを使用していて、モニタ対象ネットワーク内のユーザが TLS v1.3 を有効にしてブラウザを使用している場合、TLS v1.3 をサポートする Web サイトのロードに失敗することがあります。

詳細については、『*Failures loading websites using TLS 1.3 with SSL inspection enabled*』というタイトルのソフトウェア アドバイザリを参照してください。

FMC でのセキュア通信

SSL 証明書を使用すると、FMC（および 7000/8000 シリーズデバイス）でアプライアンスとブラウザ間に暗号化チャネルを確立できます。

デフォルトでは、システムに自己署名 HTTPS サーバ証明書が付属しています。この証明書を、グローバルに知られているか、内部で信頼されている認証局（CA）によって署名された証明

書に置き換えることをお勧めします。カスタムサーバ証明書要求を生成し、[HTTPS証明書（HTTPS Certificates）] ページでカスタムサーバ証明書をインポートすることができます。**[システム（System）]** > **[設定（Configuration）]** を選択し、[HTTPS証明書（HTTPS Certificates）] をクリックします。

詳細については、オンライン ヘルプまたは『Firepower Management Center Configuration Guide』を参照してください。

Firepower Web インターフェイスでテストされたブラウザ

Firepower Web インターフェイスは、現在サポートされているバージョンの MacOS と Microsoft Windwos を実行している一般的なブラウザ（Google Chrome、Mozilla Firefox、および Microsoft Internet Explorer）の最新バージョンでテストされています。他のブラウザで問題が発生した場合、またはサポートが終了したオペレーティングシステムを実行している場合は、交換またはアップグレードしてください。問題が解消されない場合は、Cisco TAC にお問い合わせください。

Note Apple Safari または Microsoft Edge での広範なテストは実施されていませんが、Cisco TAC では、これらのブラウザの最新バージョンで発生した問題に関するフィードバックを求めています。

***Table 4: Firepower Web* インターフェイスでテストされたブラウザ**

ブラウザ	必要な設定と追加の警告
Google Chrome	JavaScript、Cookie Chrome は、画像、CSS、JavaScript などの静的コンテンツを、システムによって提供される自己署名証明書とともにキャッシュしません。これにより、特に低帯域幅環境では、ページの読み込み時間が長くなります。自己署名証明書を置き替えない場合は、代わりに、自己署名証明書をブラウザまたは OS の信頼ストアに追加できます。
Mozilla Firefox	JavaScript、Cookie、TLS v1.2 これらを更新すると、Firefoxは、システムが提供する自己署名証明書を信頼しなくなる場合があります。証明書を置き換えない場合、ログイン ページがロードされないときは Firefox を更新します。Firefox の検索バーに「`about:support`」と入力し、[Firefoxをリフレッシュ（Refresh Firefox）] をクリックします。一部の設定が失われます。Refresh Firefox サポートページを参照してください。

ブラウザ	必要な設定と追加の警告
Microsoft Internet Explorer 11（Windows のみ）	JavaScript、Cookie、TLS v1.2、128 ビット暗号化 また、次のことを行う必要があります。 • [Check for newer versions of stored pages] 閲覧履歴オプションについては、[Automatically] を選択してください。 • [サーバーにファイルをアップロードするときにローカル ディレクトリのパスを含める] カスタム セキュリティ設定を無効にします。 • Firepower Web インターフェイスの IP アドレス/URL の互換表示を有効にします。 FMC ウォークスルーではテストされていません。

ブラウザ拡張機能との互換性

一部のブラウザ拡張機能（Grammarly や Whatfix Editor など）によって、PKI オブジェクトの証明書やキーなどのフィールドの値が保存されなくなる場合があります。これらの拡張機能は文字（HTML など）をフィールドに挿入するため、FMC で無効として認識されることになります。FMC の使用時はこれらの拡張機能を無効にすることをお勧めします。

画面解像度の要件

***Table 5: Firepower* ユーザ インターフェイスの画面解像度の要件**

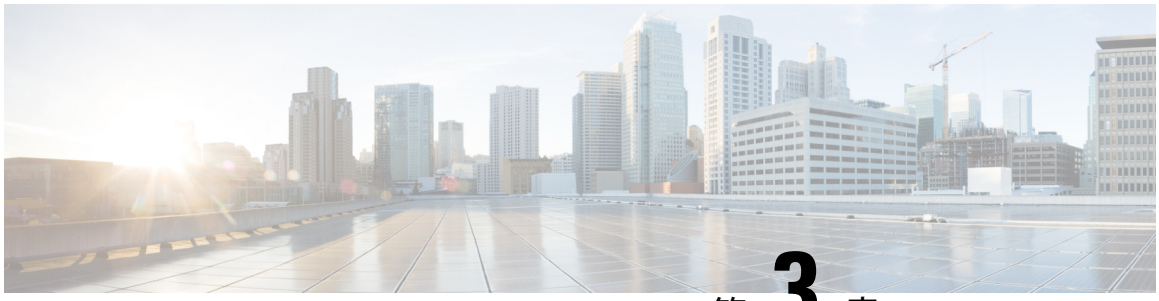
インターフェイス	解像度
Firepower Management Center	1280 X 720
7000/8000 シリーズ デバイス（制限されたローカル インターフェイス）	1280 X 720
Firepower Device Manager	1024 X 768
を管理している ASDM ASA FirePOWER module	1024 X 768
Firepower Chassis Manager 向け Firepower 4100/9300 シャーシ	1024 X 768

その他の互換性関連のリソース

この表には、リリースノートとその他の互換性情報へのリンクがあります。完全なドキュメントロードマップについては、ドキュメントロードマップ, on page 83を参照してください。

Table 6: その他の互換性関連のリソース

説明	Resources
互換性ガイドには、バンドルコンポーネントや統合製品など、サポートされているハードウェアモデルとソフトウェアバージョンに関する詳細な互換性情報が記載されています。	Cisco Firepower Compatibility Guide Cisco ASA の互換性 Cisco Firepower 4100/9300 FXOS の互換性
リリースノートには、アップグレードの警告や動作の変更など、リリース固有の情報が記載されています。	Cisco Firepower リリース ノート Cisco ASA リリースノート Cisco Firepower 4100/9300 FXOS リリースノート
持続性に関する速報には、管理プラットフォームやオペレーティングシステムなど、シスコ□次世代ファイアウォール製品ラインに関するサポートタイムラインが記載されています。	Cisco NGFW 製品ラインのソフトウェアリリースおよび持続性に関する速報



第 3 章

特長と機能

Firepower バージョン 6.4.0 には以下が含まれます。

新機能

次のトピックでは、Firepower バージョン 6.4.0 で使用可能な新機能をリストしています。アップグレード パスが 1 つ以上のメジャー バージョンをスキップする場合は、『Cisco Firepower リリース ノート』で過去の新機能リストを参照してください。

Firepower Management Center/Firepower バージョン 6.4.0 の新機能

次の表に、Firepower Management Center を使用して設定された場合に Firepower バージョン 6.4.0 で使用可能な新機能を示します。

表 *7:* バージョン *6.4.0* の新機能：*FMC* 導入環境

機能	説明
ハードウェアと仮想ハードウェア	
FMC モデル MC1600、2600、および 4600	Firepower Management Center モデル MC1600、2600、および 4600 を導入しました。なお、これらのモデルではバージョン 6.3.x もサポートされています。
FMCv Azure 上	Microsoft Azure 上に Firepower Management Center Virtual を導入しました。

機能	説明
FTD Firepower 1010、1120、1140 上	Firepower 1010、1120、および 1140 を導入しました。
FTD Firepower 4115、4125、および 4145	Firepower 4115、4125、および 4145 が導入されました。
Firepower 9300 SM-40、SM-48、および SM-56 のサポート	新しい 3 つのセキュリティ モジュール（SM-40、SM-48、SM-56）を導入しました。
ASA および FTD（同じ Firepower 9300 上）	ASA および FTD 論理デバイスを同じ Firepower 9300 上で展開できるようになりました。FXOS 2.6.1 が必要です。
ライセンス	
の新しいライセンス機能 ISA 3000	ASA FirePOWER および FTD の導入環境では、 ISA 3000 は URL フィルタリングおよびマルウェアのライセンスとそれらの関連機能をサポートするようになりました。 FTD のみ、ISA 3000 は、承認された顧客向けに特定のライセンスの予約をサポートするようになりました。 サポートされているプラットフォーム： ISA 3000
Firepower Threat Defense ルーティング	

機能	説明
OSPFv2 ルーティングの循環（キーチェーン）認証	OSPFv2 ルーティングを設定すると、循環（キーチェーン）認証を使用できるようになりました。 新規/変更された画面： • **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** > **[キーチェーン（Key Chain）]** オブジェクト • **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > [デバイスの編集（edit device）] > [ルーティング（Routing）] タブ > [OSPF 設定（OSPF settings）] > [インターフェイス（Interface）] タブ > [インターフェイスの追加/編集（add/edit interface）] > [認証（Authentication）] オプション • **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > [デバイスの編集（edit device）] > [ルーティング（Routing）] タブ > [OSPF 設定（OSPF settings）] > [エリア（Area）] タブ > [エリアの追加/編集（add/edit area）] > [仮想リンク（Virtual Link）] サブタブ > [仮想リンクの追加/編集（add/edit virtual link）]> [認証（Authentication）] オプション サポートされているプラットフォーム： FTD
Firepower Threat Defense 暗号化と VPN	
RA VPN：セカンダリ認証	セカンダリ認証（二重認証とも呼ばれる）は、2 つの異なる認証サーバを使用して、RA VPN 接続にさらにもう 1 つのセキュリティのレイヤを追加します。セカンダリ認証が有効になっている場合、AnyConnect VPN のユーザは VPN ゲートウェイにログインするために 2 組のクレデンシャルを提供する必要があります。 RA VPN は、AAA のみのセカンダリ認証と、クライアント証明書認証方式および AAA 認証方式をサポートします。 新規/変更された画面：**[デバイス（Devices）]** > **[VPN]** > **[リモート アクセス（Remote Access）]** > [設定の追加/編集（add/edit configuration）] > [接続プロファイル（Connection Profile）] > [AAA] 領域 サポートされているプラットフォーム： FTD

機能	説明
サイト間 VPN：エクストラネット エンドポイントのダイナミック IP アドレス	エクストラネットエンドポイントにダイナミック IP アドレスを使用するように、サイト間 VPN を設定できるようになりました。ハブアンドスポーク導入環境では、ハブをエクストラネット エンドポイントとして使用できます。 新規/変更された画面：**[デバイス（Devices）]** > **[VPN]** > **[サイト間（Site To Site）]** > [FTD VPN トポロジの追加/編集（add/edit FTD VPN topology）] > [エンドポイント（Endpoints）] タブ > [エンドポイントの追加（add endpoint）] > [IP アドレス（IP Address）] オプション サポートされているプラットフォーム： FTD
サイト間 VPN：ポイントツーポイント トポロジのためのダイナミック暗号マップ	ポイントツーポイントおよびハブアンドスポーク VPN トポロジでは、ダイナミック暗号マップを使用できるようになりました。フルメッシュ トポロジについては、ダイナミック暗号マップはまだサポートされていません。 トポロジを設定するときは、暗号マップ タイプを指定します。トポロジ内のピアの 1 つに対して、ダイナミック IP アドレスも指定する必要があります。 新規/変更された画面：**[デバイス（Devices）]** > **[VPN]** > **[サイト間（Site To Site）]** > [FTD VPN トポロジの追加/編集（add/edit FTD VPN topology）] > [IPsec] タブ > [暗号マップ タイプ（Crypto Map Type）] オプション サポートされているプラットフォーム： FTD

機能	説明
TLS 暗号化アクセラレーション	SSL ハードウェア アクセラレーションは、*TLS* 暗号化アクセラレーションに名前が変更されました。デバイスによっては、TLS 暗号化アクセラレーションがソフトウェアまたはハードウェアで実行される場合があります。バージョン 6.4 のアップグレード プロセスでは、この機能を手動で無効にした場合でも、すべての対象デバイスでアクセラレーションが自動的に有効になります。 ほとんどの場合、この機能を設定することはできません。この機能は自動的に有効になり、無効にすることはできません。ただし、Firepower 4100/9300 シャーシのマルチインスタンス機能を使用している場合は、モジュール/セキュリティ エンジンごとに、*1* つのコンテナ インスタンスに対して TLS 暗号アクセラレーションを有効にすることができます。他のコンテナ インスタンスに対してアクセラレーションは無効になっていますが、ネイティブ インスタンスには有効になっています。 Firepower 4100/9300 シャーシ向けの新しい FXOS CLI コマンド： • **show hwCrypto** • **config hwCrypto** 新しい FTD CLI コマンド： • **show crypto accelerator status**（**system support ssl-hw-status** の代替） 削除された FTD CLI コマンド： • **system support ssl-hw-accel** • **system support ssl-hw-status** サポートされているプラットフォーム：Firepower 2100 シリーズ、Firepower 4100/9300 シャーシ
イベント、ロギング、および分析	

機能	説明
ファイルおよびマルウェア イベントの syslog メッセージの改良	完全修飾ファイルおよびマルウェアのイベントデータが syslog 経由で管理対象デバイスから送信できるようになりました。 新規/変更された画面：**[ポリシー（Policies）]** > **[アクセス制御（Access Control）]** > **[アクセスコントロール（Access Control）]** > [ポリシーの追加/編集（add/edit policy）] > [ロギング（Logging）] タブ > [ファイルおよびマルウェアの設定（File and Malware Settings）] 領域 サポートされているプラットフォーム：すべて
CVE ID による侵入イベントの検索	特定の CVE エクスプロイトの結果として生成された侵入イベントを検索できるようになりました。 新規/変更された画面：**[分析（Analysis）]** > **[検索（Search）]** サポートされているプラットフォーム： FMC
[IntrusionPolicy] フィールドが syslog に含まれるようになりました。	侵入イベントの syslog メッセージは、イベントをトリガーした侵入ポリシーを指定するようになりました。 サポートされているプラットフォーム：すべて
Cisco Threat Response（CTR）の統合	Cisco Threat Response は、脅威の迅速な検出、調査、および対応に役立つ新しい Cisco Cloud を提供しています。CTR を使用すると、Firepower Threat Defense などの複数の製品から集約されたデータを使用してインシデントを分析できます。詳細については、Firepower および Cisco Threat Response の統合ガイドを参照してください。 新規/変更された画面：**[システム（System）]** > **[統合（Integration）]** > **[クラウド サービス（Cloud Services）]** サポートされているプラットフォーム： FTD
Splunk の統合	Splunk のユーザは、新しい個別の Splunk アプリケーションである Cisco Firepower App for Splunk を使用してイベントを分析できます。どの機能を使用できるかは、Firepower のバージョンによって異なります。 サポートされているプラットフォーム： FMC
管理	

機能	説明
VMware の FTDv はデフォルトで vmxnet3 インターフェイスに設定される	VMware 上の FTDv は、仮想デバイスを作成するときにデフォルトで vmxnet3 インターフェイスに設定されるようになりました。以前は、デフォルトは e1000 でした。Vmxnet3 のデバイス ドライバとネットワーク処理は ESXi ハイパーバイザと統合されているため、使用するリソースが少なくなり、ネットワーク パフォーマンスが向上します。 （注） e1000 インターフェイスを使用している場合は、切り替えることを強く推奨します。詳細については、『Cisco Firepower Threat Defense Virtual for VMware Getting Started Guide』の VMware インターフェイスの追加と設定の手順を参照してください。 サポートされているプラットフォーム：VMware 上の FTDv
管理インターフェイスで重複アドレス検出（DAD）を無効にする機能	IPv6 を有効にすると、DAD を無効にすることができます。DAD を使用するとサービス拒否攻撃の可能性が拡大するため、DAD は無効にすることができます。この設定を無効にした場合は、すでに割り当てられているアドレスがこのインターフェイスで使用されていないことを手動で確認する必要があります。 新規/変更された画面：**[システム（System）]** > **[設定（Configuration）]** > **[管理インターフェイス（Management Interfaces）]** > **[インターフェイス（Interfaces）]** 領域 > [インターフェイスの編集（edit interface）] > [IPv6 DAD] チェックボックス サポートされているプラットフォーム：FMC、7000 および 8000 シリーズ

機能	説明
管理インターフェイス上のICMPv6エコー応答と宛先到達不能メッセージを無効にする機能	IPv6 を有効にすると、ICMPv6 エコー応答および宛先到達不能メッセージを無効できるようになりました。これらのパケットを無効にすることで、サービス拒否攻撃の可能性から保護します。エコー応答パケットを無効にすると、デバイスの管理インターフェイスにテスト目的で IPv6 ping を使用できなくなります。 新規/変更された画面： **[システム（System）] > [設定（Configuration）] > [管理インターフェイス（Management Interfaces）] > [ICMPv6]** 新規/変更されたコマンド： • **configure network ipv6 destination-unreachable** • **configure network ipv6 echo-reply** サポートされているプラットフォーム：FMC（Web インターフェイスのみ）、管理対象デバイス（CLI のみ）
RADIUS サーバに定義されている FTD ユーザの Service-Type 属性のサポート	FTD CLI ユーザの RADIUS の認証では、以前は RADIUS 外部認証オブジェクトにユーザ名をあらかじめ定義してから、RADIUS サーバに定義されているユーザ名とリストが一致していることを手動で確認する必要がありました。Service-Type 属性を使用して RADIUS サーバで CLI ユーザを定義できるようになりました。また、Basic と Config の両方のユーザ ロールも定義できます。このメソッドを使用するには、外部認証オブジェクトのシェルアクセスフィルタを空白のままにしてください。 新規/変更された画面：**[システム（System）] > [ユーザ（Users）] > [外部認証（External Authentication）]** タブ > [外部認証オブジェクトの追加/編集（add/edit external authentication object）] > [シェル アクセス フィルタ（Shell Access Filter）] サポートされているプラットフォーム： FTD
オブジェクトの使用状況の表示	オブジェクト マネージャでネットワーク、ポート、VLAN、またはURLオブジェクトが使用されているポリシー、設定、およびその他のオブジェクトを表示できるようになりました。 新規/変更された画面：[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > でオブジェクトのタイプを選択し [使用状況の検索（Find Usage）]（双眼鏡）アイコン サポートされているプラットフォーム： FMC

機能	説明
署名済みの SRU、VDB、および GeoDB の更新（セキュリティの拡張）	Firepowerは正しい更新ファイルを使用していることが確認できるため、バージョン6.4以降では署名済みの更新を侵入ルール（SRU）、脆弱性データベース（VDB）、および地理位置情報データベース（GeoDB）に使用します。以前のバージョンでは、引き続き未署名の更新が使用されます。シスコ サポートおよびダウンロード サイト から手動で更新をダウンロードしない限り（たとえば、エアギャップ導入環境の場合）、機能の違いはわかりません。 ただし、SRU、VDB、および GeoDB の更新を手動でダウンロードしてインストールする場合は、必ず現在のバージョンに対応した正しいパッケージをダウンロードしてください。バージョン 6.4 以降の署名付きの更新ファイルの先頭は「Sourcefire」ではなく「Cisco」で、末尾は .sh ではなく .sh.REL.tar です。 • SRU：Cisco_Firepower_SRU-*date-build*-vrt.sh.REL.tar • VDB：Cisco_VDB_Fingerprint_Database-4.5.0-*version*.sh.REL.tar • GeoDB：Cisco_GEODB_Update-*date-build*.sh.REL.tar バージョン 5.x ～ 6.3 の更新ファイルでは、引き続き古い命名方式が使用されています。 • SRU：Sourcefire_Rule_Update-*date-build*-vrt.sh • VDB：Sourcefire_VDB_Fingerprint_Database-4.5.0-*version*.sh • GeoDB：Sourcefire_Geodb_Update-*date-build*.sh シスコは、署名なしの更新を必要とするバージョンのサポートが終了するまで、署名付きと署名なしの両方の更新を提供します。署名付きの（.tar）パッケージは解凍しないでください。 （注） 古い FMC または ASA FirePOWER デバイスに署名付きの更新を誤ってアップロードした場合は、手動で削除する必要があります。パッケージを残しておくと、ディスク領域が占有されるため、今後のアップグレードで問題が発生する可能性もあります。 サポートされているプラットフォーム：すべて

機能	説明
管理対象デバイスのスケジュールされたリモート バックアップ	FMC を使用して、特定の管理対象デバイスのリモートバックアップをスケジュールできるようになりました。以前、スケジュールされたバックアップをサポートしていたのはFirepower 7000/8000 シリーズのデバイスのみで、デバイスのローカル GUI を使用する必要がありました。 新規/変更された画面：**[システム（System）]** > **[ツール（Tools）]** > **[スケジューリング（Scheduling）]** > [タスクの追加/編集（add/edit task）] > [ジョブ タイプ：バックアップ（Job Type: Backup）] を選択 > [バックアップのタイプ（Backup Type）] を選択 サポートされているプラットフォーム：FTD の物理プラットフォーム、VMware 用 FTDv、Firepower 7000/8000 シリーズ 例外：FTD のクラスタ化されたデバイスまたはコンテナ インスタンスはサポートされていません。
モニタリングおよびトラブルシューティング	
URL フィルタリング モニタの改善	URL フィルタリング モニタ アラートの時間しきい値を設定できるようになりました。 新規/変更された画面：**[システム（System）]** > **[健全性（Health）]** > **[ポリシー（Policy）]** > [ポリシーの追加/編集（add/edit policy）] > [URL フィルタリング モニタ（URL Filtering Monitor）] サポートされているプラットフォーム：すべて

機能	説明
アクセス制御ルールと事前フィルタ ルールのヒット カウント	FTD デバイスのアクセス制御ルールと事前フィルタ ルールのヒット カウントにアクセスできるようになりました。 新規/変更された画面： • **[ポリシー（Policies）] > [アクセス制御（Access Control）] > [アクセス制御（Access Control）]** > [ポリシーの追加/編集（add/edit policy）] > [ヒット カウントの分析（Analyze Hit Counts）] • **[ポリシー（Policies）] > [アクセス制御（Access Control）] > [事前フィルタ（Prefilter）]** > [ポリシーの追加/編集（add/edit policy）] > [ヒット カウントの分析（Analyze Hit Counts）] 新しいコマンド： • **show rule hits** • **clear rule hits** • **cluster exec show rule hits** • **cluster exec clear rule hits** • **show cluster rule hits** 変更されたコマンド： • **show failover** に HA ピア間のヒット カウントの同期に関連するオブジェクトのスタティック カウントが含まれるようになりました。 サポートされているプラットフォーム： FTD
接続ベースのトラブルシューティング	接続ベースのトラブルシューティングまたはデバッグにおいて、モジュール間で一貫したデバッグが提供され、特定の接続について適切なログを収集します。また、レベルベースのデバッグを最大 7 レベルまでサポートし、lina ログと Snort ログで一貫したログ収集メカニズムを使用できます。 新規/変更されたコマンド： • **clear packet debugs** • **debug packet start** • **debug packet stop** • **show packet debugs** サポートされているプラットフォーム： FTD

機能	説明
Cisco Success Network の新しいモニタリング機能	Cisco Success Network の次のモニタリング機能を追加しました。 • CSPA（Cisco Security Packet Analyzer）のクエリ情報 • FMC で有効になっているコンテキスト クロス起動インスタンス • TLS/SSL インスペクション イベント • Snort の再起動 Cisco Success Network は、テクニカル サポートを提供するために不可欠な使用状況に関する情報と統計情報をシスコに送信します。いつでもオプトインまたはオプトアウトできます。 サポートされているプラットフォーム： FMC
Firepower Management Center REST API	
新しい REST API 機能	バージョン 6.4 の機能をサポートするための REST API オブジェクトを追加しました。 • cloudeventsconfigs：Cisco Threat Response の統合を管理します。 • ftddevicecluster：シャーシのクラスタリングを管理します。 • hitcounts：アクセス制御ルールと事前フィルタ ルールのヒット カウント統計情報を管理します。 • keychain：OSPFv2 ルーティングの設定時に、認証のローテーションに使用されるキーチェーン オブジェクトを管理します。 • loggingsettings：アクセス コントロール ポリシーのロギング設定を管理します。 サポートされているプラットフォーム： FMC
OAS に基づく API エクスプローラ	バージョン 6.4 は OpenAPI 仕様（OAS）に基づいて、新しい API エクスプローラを使用します。OAS の一部として、CodeGen を使用してサンプル コードを生成するようになりました。必要に応じて、レガシー API エクスプローラにもアクセスできます。 サポートされているプラットフォーム： FMC
パフォーマンス	

機能	説明
Snort 再起動の改善	バージョン 6.4 より以前では、Snort の再起動中、暗号化された接続のうち、「復号しない」 SSL ルールまたはデフォルト ポリシー アクションに一致したものがシステムによってドロップされていました。現在は、大きなフロー オフロードまたは Snort preserve-connection を無効にしていない限り、ルーテッド/透過トラフィックはドロップされずにインスペクションなしで通過します。 サポートされているプラットフォーム：Firepower 4100/9300
選択された IPS トラフィックのパフォーマンスの向上	出力最適化は、選択された IPS トラフィックを対象としたパフォーマンス機能です。この機能は、すべての FTD プラットフォームでデフォルトで有効になっています。 バージョン 6.4 のアップグレード プロセスでは、対象デバイスでの出力最適化が有効になります。詳細については、『Cisco Firepower Threat Defense コマンド リファレンス（Cisco Firepower Threat Defense Command Reference）』を参照してください。出力最適化に関する問題をトラブルシューティング Cisco TACするには、にお問い合わせください。 サポートされているプラットフォーム： FTD 新規/変更されたコマンド： • **asp inspect-dp egress optimization** • **show asp inspect-dp egress optimization** • **clear asp inspect-dp egress optimization** • **show conn state egress_optimization**
SNMP イベント ロギングの高速化	外部 SNMP トラップ サーバに侵入イベントと接続イベントを送信する際のパフォーマンスが向上しました。 サポートされているプラットフォーム：すべて
展開の高速化	アプライアンスの通信と展開フレームワークが向上しました。 サポートされているプラットフォーム： FTD
アップグレードの高速化	イベント データベースが向上しました。 サポートされているプラットフォーム：すべて

Firepower Device Manager/FTD バージョン 6.4.0 の新機能

リリース日：2019 年 4 月 24 日

次の表に、Firepower Device Manager を使用して設定された場合に FTD 6.4.0 で使用できる新機能を示します。

表 *8*:

機能	説明
Firepower 1000 シリーズ デバイス設定	Firepower Device Manager を使用して、Firepower 1000 シリーズ デバイスで Firepower Threat Defense を設定できます。 Power over Ethernet（PoE）ポートを通常のイーサーネット ポートとして使用することはできますが、PoE に関連するプロパティを有効にしたり設定することはできないことにご注意ください。
ISA 3000 のハードウェア バイパス	ISA 3000 のハードウェアバイパスは、**[デバイス（Device）]** > **[インターフェイス（Interfaces）]** ページで設定できるようになりました。リリース 6.3 では、FlexConfig を使用してハードウェアバイパスを設定する必要がありました。FlexConfig を使用している場合は、[インターフェイス（Interfaces）] ページの設定をやり直し、FlexConfig から hardware bypass コマンドを削除してください。ただし、TCP シーケンス番号のランダム化を無効にするための FlexConfig 部分の使用は引き続き推奨されます。
FDM CLI コンソールからシステムを再起動およびシャットダウンする機能	FDM で CLI コンソールを使用して、**reboot** および **shutdown** コマンドを発行できるようになりました。以前は、システムを再起動またはシャットダウンするために、デバイスに対して個別の SSH セッションを開く必要がありました。これらコマンドを使用するには、管理者権限が必要です。
RADIUS を使用した FTD CLI ユーザの外部認証および認可。	FTD CLI にログインするユーザを、外部 RADIUS サーバを使用して認証および認可できます。外部ユーザに設定（管理者）または基本（読み取り専用）のアクセス権を付与できます。 **[デバイス（Device）]** > **[システム設定（System Settings）]** > **[管理アクセス（Management Access）]** ページの [AAA設定（AAA Configuration）] タブに SSH の設定を追加しました。

機能	説明
ネットワーク範囲オブジェクトとネストされたネットワーク グループ オブジェクトのサポート	IPv4 または IPv6 アドレスの範囲、および他のネットワーク グループ（つまり、ネストされたグループ）を含むネットワーク グループ オブジェクトを指定するネットワーク オブジェクトを作成できるようになりました。 これらの機能を含めるためにネットワーク オブジェクトとネットワーク グループ オブジェクトの [追加/編集（Add/Edit）] ダイアログボックスが変更されました。また、当該タイプのアドレス指定がポリシーのコンテキスト内で妥当かどうかにより、これらのオブジェクトの使用を許可するためにさまざまなセキュリティ ポリシーが変更されました。
オブジェクトとルールの全文検索オプション	オブジェクトおよびルールでは、全文検索を実行できます。多数の項目を含むポリシーまたはオブジェクト リストを検索することで、ルールまたはオブジェクト内の任意の場所で検索文字列を含むすべての項目を検索できます。 ルールを含むすべてのポリシー、および [オブジェクト（Objects）] リストのすべてのページに検索ボックスが追加されました。さらに、API でサポートされているオブジェクトの GET コールで **filter=fts~***search-string* オプションを使用して、全文検索に基づいて項目を取得できます。
FDM 管理対象 FTD デバイスでサポートされている API バージョンのリストの取得	GET/api/versions（ApiVersions）メソッドを使用して、デバイスでサポートされる API バージョンのリストを取得できます。API クライアントを使用すると、サポートされているバージョンで有効なコマンドとシンタックスを使用してデバイスと通信し、デバイスを設定できます。
FTD REST API バージョン 3（v3）	ソフトウェア バージョン 6.4 向けの FTD REST API のバージョン番号が 3 になりました。API URL の v1/v2 は v3 に置き換える必要があります。v3 の API には、ソフトウェア バージョン 6.4 で追加されたすべての機能に対応する多数の新しいリソースが含まれています。使用しているリソース モデルに変更が加えられている可能性があるため、既存のすべての呼び出しを再評価してください。リソースを表示できる API エクスプローラを開くには、ログインした後に、Firepower Device Manager の URL の最後を **/#/api-explorer** に変更します。

機能	説明
アクセス制御ルールのヒットカウント	アクセスコントロールルールのヒットカウントを表示できます。ヒットカウントには、接続がルールに一致した頻度が示されます。 ヒットカウント情報が含まれるようにアクセスコントロールポリシーを更新しました。FTD API では、HitCounts リソースと **includeHitCounts** および **filter=fetchZeroHitCounts** オプションが GET アクセスポリシールールのリソースに追加されました。
ダイナミック アドレス指定と証明書認証のためのサイト間 VPN の強化	ピアの認証に事前共有キーではなく証明書を使用したサイト間 VPN 接続を設定できるようになりました。リモートピアに不明な（ダイナミック）IP アドレスが設定されている接続も設定できます。サイト間 VPN ウィザードと IKEv1 ポリシーオブジェクトにオプションが追加されました。
リモート アクセス VPN での RADIUS サーバと認可変更のサポート	リモートアクセス VPN（RA VPN）ユーザの認証、認可、およびアカウンティングに RADIUS サーバを使用できるようになりました。また、Cisco ISE RADIUS サーバの使用時、認証後にユーザの認証を変更するために、ダイナミック認証とも呼ばれる Change of Authentication（CoA）を設定できます。 RADIUS サーバとサーバ グループ オブジェクトに属性を追加し、RA VPN 接続プロファイル内の RADIUS サーバグループを選択できるようになりました。
リモートアクセス VPN の複数の接続プロファイルとグループ ポリシー	複数の接続プロファイルを設定し、そのプロファイルで使用するグループ ポリシーを作成できます。 接続プロファイルおよびグループ ポリシーが別々のページとなるように **[デバイス（Device）]** > **[リモートアクセス VPN（Remote Access VPN）]** ページを変更し、グループ ポリシーを選択できるように RA VPN 接続ウィザードを更新しました。以前はウィザードで設定していた一部の項目がグループポリシーで設定されるようになりました。
証明書ベースの 2 番目の認証ソース、およびリモート アクセス VPN での二要素認証のサポート	ユーザ認証に証明書を使用し、セカンダリ認証ソースを設定して、接続を確立する前にユーザを 2 回認証させることができます。また、2 つ目の要素として RSA トークンまたは Duo パスコードを使用して二要素認証を設定できます。 これらの追加オプションの設定をサポートするように RA VPN 接続ウィザードを更新しました。

機能	説明
複数のアドレス範囲を持つ IP アドレス プールとリモート アクセス VPN 向けの DHCP アドレス プールのサポート	サブネットを指定する複数のネットワークオブジェクトを選択することで、複数のアドレス範囲を持つアドレスプールを設定できるようになりました。さらに、DHCP サーバでアドレスプールを設定し、そのサーバを使用して RA VPN クライアントにアドレスを提供できます。認証に RADIUS を使用する場合は、代わりに RADIUS サーバでアドレスプールを設定できます。 これらの追加オプションの設定をサポートするように RA VPN 接続ウィザードを更新しました。必要に応じて、接続プロファイルではなくグループポリシーでアドレスプールを設定できます。
Active Directory レルムの強化	1 つのレルムに最大 10 の冗長 Active Directory（AD）サーバを含められるようになりました。また、複数のレルムを作成したり、不要になったレルムを削除したりできます。さらに、レルム内のユーザのダウンロードの制限は、以前のリリースの 2,000 から 50,000 に増えています。 複数のレルムとサーバをサポートするように、**[オブジェクト（Objects）] > [アイデンティティ ソース（Identity Sources）]** ページを更新しました。レルム内のすべてのユーザにルールを適用するため、アクセス制御と SSL 復号化ルールのユーザの基準でレルムを選択することができます。アイデンティティ ルールと RA VPN 接続プロファイルでレルムを選択することもできます。
ISE サーバの冗長性サポート	パッシブ認証向けの ID ソースとして Cisco Identity Services Engine（ISE）を設定する際に、ISE ハイアベイラビリティ設定がある場合は、セカンダリ ISE サーバを設定できるようになりました。 ISE アイデンティティ オブジェクトにセカンダリサーバの属性が追加されました。
ファイル/マルウェア イベントを外部 syslog サーバに送信	アクセスコントロールルールに設定されたファイルポリシーによって生成される、ファイルおよびマルウェアイベントを受信するように外部 syslog サーバを設定できるようになりました。ファイルイベントにはメッセージ ID 430004 を使用し、マルウェアイベントには 430005 を使用します。 **[デバイス（Device）] > [システム設定（System Settings）] > [ログの設定（Logging Settings）]** ページにファイル/マルウェア syslog サーバのオプションが追加されました。

機能	説明
内部バッファのログおよびカスタムイベントのログフィルタのサポート	内部バッファをシステムロギングの宛先として設定できるようになりました。さらに、イベントログフィルタを作成して、syslog サーバおよび内部バッファロギングの宛先に対して生成されるメッセージをカスタマイズできます。 イベント ログ フィルタ オブジェクトを [オブジェクト（Objects）] ページに追加し、このオブジェクトを使用する機能が **[デバイス（Device）] > [システム設定（System Settings）] > [ログの設定（Logging Settings）]** ページに追加されました。内部バッファ オプションも [ログの設定（Logging Settings）] ページに追加しました。
Firepower Device Manager の Web サーバ向けの証明書	Firepower Device Manager の設定インターフェイスへの HTTPS 接続に使用される証明書を設定できるようになりました。Web ブラウザがすでに信頼している証明書をアップロードすることで、デフォルトの内部証明書を使用するときに、Untrusted Authority メッセージを回避できます。**[デバイス（Device）] > [システム設定（System Settings）] > [管理アクセス（Management Access）] > [管理Webサーバ（Management Web Server）]** ページが追加されました。
Cisco Threat Response のサポート	Cisco Threat Response のクラウドベースのアプリケーションに侵入イベントを送信するようにシステムを設定できます。Cisco Threat Response を使用して、侵入を分析できます。 Cisco Threat Response を **[デバイス（Device）] > [システム設定（System Settings）] > [クラウド サービス（Cloud Services）]** ページに追加しました。

廃止された機能

このトピックでは、Firepower バージョンで廃止された機能とプラットフォームを示します。アップグレード パスが 1 つ以上のメジャー バージョンをスキップする場合は、中間リリースの情報を確認する必要があります。

廃止されたプラットフォームの販売終了およびサポート終了の通知へのリンクを含む、サポート対象の Firepower のすべてのバージョンの詳細な互換性情報については、『Cisco Firepower Compatibility Guide』を参照してください。

（注） Cisco Firepower User Agent ソフトウェアとアイデンティティソースについてはサポートの終了が予定されています。今すぐ Cisco Identity Services Engine/Passive Identity Connector（ISE/ISE-PIC）に切り替えてください。これにより、ユーザエージェントで使用できない機能も利用できるようになります。ライセンスを変換するには、販売担当者にお問い合わせください。

詳細については、Cisco Firepower Management Center コンフィギュレーション ガイド [英語] で該当する *Cisco Firepower* ユーザ エージェント コンフィギュレーション ガイドを参照してください。

バージョン 6.4.0 で廃止された機能

これらの機能はバージョン 6.4.0 で廃止されました。

表 *9* : バージョン *6.4.0* で廃止された機能

機能	説明
SSL ハードウェア アクセラレーション FTD CLI コマンド	TLS crypto アクセラレーション機能の一部として、次の FTD CLI コマンドを削除しました。 • **system support ssl-hw-accel enable** • **system support ssl-hw-accel disable** • **system support ssl-hw-status** 代替手段の詳細については、新しい機能のマニュアルを参照してください。 影響を受けるプラットフォーム：FTD

バージョン 6.3.0 で廃止された機能

これらの機能はバージョン 6.3.0 で廃止されました。

表 *10* : バージョン *6.3.0* で廃止された機能

機能	説明
復号化のためのEMS拡張機能のサポート	バージョン 6.3.0 では、バージョン 6.2.3.8/6.2.3.9 で導入された EMS 拡張機能のサポートが中止されます。つまり、[復号 - 再署名（Decrypt-Resign）] と [復号 - 既知のキー（Decrypt-Known Key）] の両方の SSL ポリシーアクションが、ClientHello ネゴシエーション時に EMS 拡張機能をサポート（よりセキュアな通信が可能）しなくなります。EMS 拡張機能は、 RFC 7627 によって定義されています。 FMC展開では、この機能は、デバイスのバージョンによって異なります。FMC をバージョン 6.3.0 にアップグレードしても、サポートされるバージョンがデバイスで実行されていれば、サポートは中止されません。ただし、デバイスをバージョン6.3.0にデバイスをアップグレードすると、サポートは中止されます。 サポートはバージョン 6.3.0.1 で再導入されています。 影響を受けるプラットフォーム：すべて
パッシブおよびインライン タップ インターフェイスの復号化	バージョン6.3.0では、パッシブモードまたはインラインタップモードのインターフェイスでの復号化トラフィックは、GUIを介して設定することはできますが、サポートされなくなりました。暗号化されたトラフィックのインスペクションは必然的に制限されます。
VMware 5.5 のホスティング	バージョン 6.3.0 以降の仮想展開は VMware vSphere/VMware ESXi 5.5 でテストされていません。Firepower ソフトウェアをアップグレードする前に、ホスティング環境をアップグレードすることをお勧めします。 影響を受けるプラットフォーム：FMCv、FTDv、VMware 向けの NGIPSv
Firepower ソフトウェアを搭載した ASA 5506-X シリーズおよび ASA 5512-X デバイス	これらのモデルでは、Firepower ソフトウェア（FTD と ASA FirePOWER の両方）のバージョン6.3.0以降へのアップグレードまたは新規インストールはできません。 • ASA 5506-X、5506H-X、5506W-X • ASA 5512-X ただし、バージョン 6.3.0 の FMC を使用して、古いデバイス（バージョン 6.1.0 ～ 6.2.3.x）を管理できます。

バージョン 6.2.0 で廃止された機能

これらの機能はバージョン 6.2.0 で廃止されました。

表 *11* : バージョン *6.2.0* で廃止された機能

機能	説明
ネストされた相関ルール	

機能	説明
	バージョン 6.2.0 では、ネストされた相関ルールのサポートが終了します。ある相関ルールが別の相関ルールのトリガーとなっている場合、その相関ルールはネストされています。 たとえば、どちらも侵入イベントのトリガーであるルール A とルール B を作成する場合、「ルール A は true」をルール B の制約として使用できます。この設定では、ルール A はルール B 内にネストされています。 **自動設定の変更** アップグレードプロセスは、ネストされたルール（ルール A）からネストされたルール（ルール B）へ設定をコピーしてネストされたルールを削除することで、特定のネストされた相関ルールを「フラット化」します。また、アップグレードは、ホストプロファイル/ユーザ資格とスヌーズ/非アクティブ期間を、ネストされたルールからネスト ルールへコピーします。 非アクティブ期間を除いて、これらのすべての設定について、設定がネスト ルールに存在しない場合にのみ、システムはネストされたルールからネストルールへ設定をコピーできます。システムがネストされたルールからネストルールへ非アクティブ期間をコピーするときは、結果として生じるルールがネスト構成にもともと含まれる両方のルールの設定を使用するように、ネスト ルールの非アクティブ期間を保持します。 **アップグレードの失敗の回避** アップグレードする前に、ネストされた相関ルールを「フラット化」できることを確認してください。そうなっていなければ、アップグレードは失敗します。ネストされたルールとネスト ルールに特定の競合がある場合は、アップグレードによりネストされたルールをフラット化できないことに注意してください。アップグレードの失敗を回避するには、アップグレードの前に、以下のように相関ルールを変更します。 • ネストされた構成内で 1 つのルールだけがこれらの設定を指定するように、ホスト プロファイル資格、ユーザ資格、スヌーズ期間の設定をネストされたルールまたはネスト ルールから削除します。 • 接続トラッカーを任意のネストされたルールから削除します。 • ホスト プロファイル資格、ユーザ資格、スヌーズ期間、非アクティブ期間を、true にする必要がないネストされたルールから削除します。つまり、ネスト ルール内の OR 演算子を使用して他のルールの条件にリンクされているネストされたルールから、これらの要素を削除します。

機能	説明
	影響を受けるプラットフォーム：FMC

廃止された FlexConfig コマンド

いくつかの Firepower Threat Defense の機能は、ASA 設定コマンドを使用して設定されます。バージョン 6.2（FMC 展開）またはバージョン 6.2.3（FDM 展開）以降では、Smart CLI または FlexConfig を使用して、他の方法では Web インターフェイスでサポートされないさまざまな ASA 機能を手動で設定できます。

FTD アップグレードにより、以前に FlexConfig を使用して設定した機能について、GUI またはスマート CLI のサポートが追加されることがあります。これにより、現在使用している FlexConfig コマンドが廃止される可能性があります。既存の設定は引き続き動作し、展開も可能ですが、新しく廃止されたコマンドを使用して FlexConfig オブジェクトを割り当てたり作成したりすることはできなくなります。

アップグレード後、FlexConfig ポリシーおよび FlexConfig オブジェクトを確認してください。廃止されたコマンドが含まれている場合、メッセージは問題を示します。設定をやり直すことをお勧めします。新しい設定を確認したら、問題のある FlexConfig オブジェクトまたは FlexConfig コマンドを削除できます。

Firepower Management Center を使用した FTD

次の表に、廃止された FlexConfig オブジェクトとそれらに関連付けられているテキスト オブジェクトを示します。事前定義されたオブジェクトの完全なリストについては、『Firepower Management Center Configuration Guide』を参照してください。

表 *12 : FMC* を使用した *FTD*：廃止された *FlexConfig* オブジェクト

非推奨メソッド	オブジェクト	詳細	新しいロケーション
6.3.0 以降	FlexConfig オブジェクト： • Default_DNS_Configure 関連するテキスト オブジェクト： • defaultDNSNameServerList • defaultDNSParameters	デフォルト DNS グループを設定します。デフォルト DNS グループでは、データインターフェイスの完全修飾ドメイン名を解決する際に使用できる DNS サーバを定義します。これにより、IP アドレスではなくホスト名を使用して、CLI で **ping** などのコマンドを使用することができます。	FTD プラットフォーム設定ポリシーで、データインターフェイスの DNS を設定します。

非推奨メソッド	オブジェクト	詳細	新しいロケーション
6.3.0 以降	FlexConfig オブジェクト： • TCP_Embryonic_Conn_Limit • TCP_Embryonic_Conn_Timeout 関連するテキスト オブジェクト： • tcp_conn_misc • tcp_conn_limit • tcp_conn_timeout	初期接続制限およびタイムアウトを設定して SYN フラッド サービス妨害（DoS）攻撃から保護します。	これらの機能は、FTD サービス ポリシーで設定します。ポリシーは、デバイスに割り当てられているアクセス制御ポリシーの [詳細設定（Advanced）] タブで確認できます。

次の表に、バージョン 6.2.3+ で、FDM を使用した FTD で新たに廃止された CLI コマンドの一覧を示します。機能がバージョン 6.2.0 に導入されたときに廃止されたコマンドを含む、廃止されたコマンドの完全なリストについては、『Firepower Management Center Configuration Guide』を参照してください。

表 *13 : FMC* を使用した *FTD* : 廃止された *CLI* コマンド

非推奨メソッド	コマンド	詳細
6.2.3 以降	**pager**	設定がブロックされます。

Firepower Device Manager を使用した FTD

次の表に、バージョン 6.3.0+ で、FDM を使用した FTD で新たに廃止された CLI コマンドの一覧を示します。機能がバージョン 6.2.3 に導入されたときに廃止されたコマンドを含む、廃止されたコマンドの完全なリストについては、『『Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager』』を参照してください。

表 *14 : FDM* を使用した *FTD* : 廃止された *CLI* コマンド

非推奨メソッド	コマンド（Command）	詳細（Details）
6.3.0 以降	**access-list**	**extended** および **standard** アクセス リストは作成できなくなりました。Smart CLI 拡張アクセス リストまたは標準アクセス リスト オブジェクトを使用してこれらの ACL を作成します。その後、それらは、サービス ポリシー トラフィック クラス用の拡張 ACL により、オブジェクト名によって ACL を参照する FlexConfig サポート コマンド（**match access-list** など）で使用できます。

非推奨メソッド	コマンド（Command）	詳細（Details）
6.3.0 以降	**as-path**	スマート CLI AS パス オブジェクトを作成し、それらをスマート CLI BGP オブジェクトで使用して、自律システム パス フィルタを設定します。
6.3.0 以降	**community-list**	スマート CLI 拡張コミュニティ リスト オブジェクトまたは標準コミュニティ リスト オブジェクトを作成し、それらをスマート CLI BGP オブジェクトで使用して、コミュニティ リスト フィルタを設定します。
6.3.0 以降	**dns-group**	**[オブジェクト（Objects）]** > **[DNSグループ（DNS Groups）]** を使用して DNS グループを設定し、**[デバイス（Device）]** > **[システム設定（System Settings）]** > **[DNSサーバ（DNS Server）]** を使用してグループを割り当てます。
6.3.0 以降	**policy-list**	スマート CLI ポリシー リスト オブジェクトを作成し、それらをスマート CLI BGP オブジェクトで使用して、ポリシー リストを設定します。
6.3.0 以降	**prefix-list**	スマート CLI IPv4 プレフィックス リスト オブジェクトを作成し、それらをスマート CLI OSPF オブジェクトまたはスマート CLI BGP オブジェクトで使用して、IPv4 用のプレフィックス リスト フィルタリングを設定します。
6.3.0 以降	**route-map**	スマート CLI ルート マップ オブジェクトを作成し、それらをスマート CLI OSPF オブジェクトまたはスマート CLI BGP オブジェクトで使用して、ルート マップを設定します。
6.3.0 以降	**router bgp**	BGP には Smart CLI テンプレートを使用します。

FMC メニューの変更

次の表に、変更された Firepower Management Center メニュー（移動されたページ）を示します。新規および削除されたメニュー オプションについては、新機能および廃止された機能のマニュアルを参照してください。

表 *15 : Firepower Management Center* メニューの変更

バージョン	新しいメニュー パス	古いメニュー パス
6.4.0	**[システム（System）]** > **[統合（Integration）]** > **[クラウド サービス（Cloud Services）]**	**[システム（System）]** > **[統合（Integration）]** > **[Cisco CSI]**

バージョン	新しいメニュー パス	古いメニュー パス
6.3.0	**[分析（Analysis）] > [検索（Lookup）] > [Whois]**	**[分析（Analysis）] > [詳細（Advanced）] > [Whois]**
6.3.0	**[分析（Analysis）] > [検索（Lookup）] > [位置情報（Geolocation）]**	**[分析（Analysis）] > [詳細（Advanced）] > [位置情報（Geolocation）]**
6.3.0	**[分析（Analysis）] > [検索（Lookup）] > [URL]**	**[分析（Analysis）] > [詳細（Advanced）] > [URL]**
6.3.0	**[分析（Analysis）] > [カスタム（Custom）] > [カスタムワークフロー（Custom Workflows）]**	**[分析（Analysis）] > [詳細（Advanced）] > [カスタムワークフロー（Custom Workflows）]**
6.3.0	**[分析（Analysis）] > [カスタム（Custom）] > [カスタムテーブル（Custom Tables）]**	**[分析（Analysis）] > [詳細（Advanced）] > [カスタムテーブル（Custom Tables）]**
6.3.0	**[分析（Analysis）] > [脆弱性（Vulnerabilities）] > [脆弱性（Vulnerabilities）]**	**[分析（Analysis）] > [ホスト（Hosts）] > [脆弱性（Vulnerabilities）]**
6.3.0	**[分析（Analysis）] > [脆弱性（Vulnerabilities）] > [サードパーティの脆弱性（Third Party Vulnerabilities）]**	**[分析（Analysis）] > [ホスト（Hosts）] > [サードパーティの脆弱性（Third-Party Vulnerabilities）]**

FMC How-To ウォークスルー

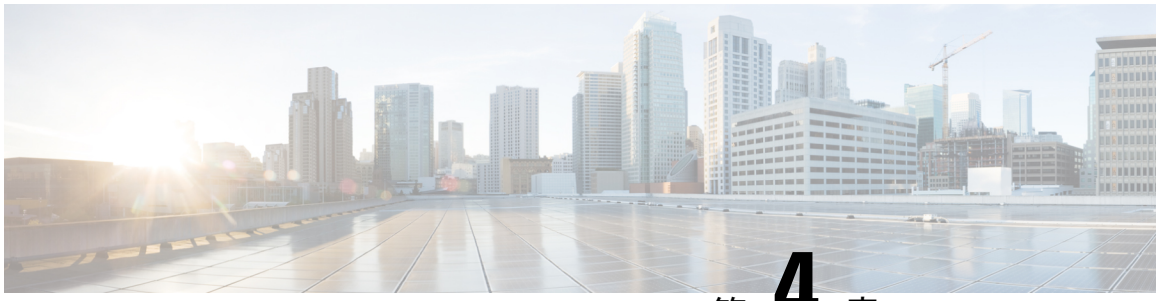
バージョン 6.3.0 では、デバイスのセットアップやポリシー設定などのさまざまな基本タスクについて順を追って説明する、FMC に関するウォークスルー（How-To とも呼ばれる）が導入されています。ブラウザウィンドウの下部にある [How To] をクリックし、ウォークスルーを選択して、手順ごとの説明に従って操作します。

（注） ウォークスルーはFirefoxおよびChromeブラウザでテストされています。別のブラウザで問題が発生した場合は、Firefox または Chrome に切り替えてください。問題が解消されない場合は、Cisco TAC にお問い合わせください。

次の表に、一般的な問題点と解決策をいくつか示します。ウォークスルーは、右上隅の [x] をクリックするといつでも終了できます。

表 *16 :* ウォークスルーのトラブルシューティング

問題	解決方法
ウォークスルーを開始するための [How To] リンクが見つからない。	ウォークスルーが有効になっていることを確認します。ユーザ名の下にあるドロップダウンリストから、[ユーザ設定（User Preferences）] を選択し、[設定方法（How-To Settings）] をクリックします。
ウォークスルーが予期しないタイミングで表示される。	ウォークスルーが予期しないタイミングで表示される場合は、ウォークスルーを終了します。
ウォークスルーが突然消えたり終了したりする。	ウォークスルーが消えた場合は、次のようにします。 • ポインタを移動します。 FMC で進行中のウォークスルーが表示されなくなることがあります。たとえば、別のトップレベルメニューをポイントすると表示されなくなります。 • 別のページに移動して、もう一度やり直してください。 ポインタを移動しても表示されない場合は、ウォークスルーが終了している可能性があります。
ウォークスルーが FMC と同期していない。 • 誤った手順から開始される。 • 進行が早すぎる。 • 先に進まない。	ウォークスルーが同期していない場合は、次のようにします。 • 続行します。 たとえば、フィールドに無効な値を入力してエラーが表示された場合は、ウォークスルーが先に進行することがあります。戻ってエラーを解決してタスクを完了することが必要になる場合があります。 • ウォークスルーを終了し、別のページに移動してもう一度やり直します。 場合によっては続行できないこともあります。たとえば、手順の完了後に [次へ（Next）] をクリックしないと、ウォークスルーの終了が必要になる場合があります。



第 4 章

バージョン 6.4.0 へのアップグレード

この章では、バージョン 6.4.0 の重要なリリースに固有の情報を提供します。

また、新機能、廃止された機能とプラットフォーム、メニューと用語の変更、ブラックリストに登録された FlexConfig コマンドなどの情報に関して「特長と機能 （11 ページ）」に目を通す必要があります。

に関するガイドラインと警告 バージョン 6.4.0

このチェックリストには、バージョン 6.4.0 に関する新しい重要なアップグレード ガイドラインと警告が含まれています。「以前に公開されたガイドラインと警告 （42 ページ）」および「一般的なガイドラインと警告 （51 ページ）」も確認する必要があります。

表 *17* : バージョン *6.4.0* の新しいガイドライン

✓	ガイドライン	プラットフォーム	アップグレード元	直接アップグレード先
	Firepower 1010 デバイス上の EtherChannel で出力トラフィックがブラックホール化される場合がある （40 ページ）	Firepower 1010	6.4.0	6.4.0.3 ～ 6.4.0.5

✓	ガイドライン	プラットフォーム	アップグレード元	直接アップグレード先
	アップグレードの失敗：コンテナインスタンスのディスク容量不足（40 ページ）	Firepower 4100/9300	6.3.0 ～ 6.4.0.x	6.3.0.1 ～ 6.5.0
	アップグレードの失敗：以前のバージョンが 6.2.3.12 の NGIPS デバイス （41 ページ）	Firepower 7000/8000 シリーズ ASA FirePOWER NGIPSv	6.2.3 ～ 6.3.0.x	6.4.0 のみ
	TLS 暗号化アクセラレーションの有効化/無効にすることは不可（41 ページ）	Firepower 2100 シリーズ Firepower 4100/9300	6.1.0 ～ 6.3.0.x	6.4.0 以降
	Firepower 4100/9300 のアップグレードにはバージョン 6.2.0 が必要 （42 ページ）	Firepower 4100/9300	6.1.0.x	6.4.0 のみ

Firepower 1010 デバイス上の EtherChannel で出力トラフィックがブラックホール化される場合がある

展開：FTD を搭載した Firepower 1010

影響を受けるバージョン：バージョン 6.4.0 ～ 6.4.0.5

関連するバグ：CSCvq81354

FTD バージョン 6.4.0 ～ 6.4.0.5 を実行している Firepower 1010 デバイスでは EtherChannel を設定しないことを強くお勧めします（バージョン 6.4.0.1 および 6.4.0.2 はこのモデルではサポートされていないことに注意してください）。

内部トラフィックハッシュの問題により、Firepower 1010 デバイス上の EtherChannel では出力トラフィックがブラックホール化されることがあります。ハッシュは送信元 IP アドレスと宛先 IP アドレスに基づくため、特定の送信元 IP と宛先 IP のペアで一貫性のある動作になります。つまり、一部のトラフィックは常に機能し、一部のトラフィックは常に失敗します。

この問題は、次回の 6.4.0.x パッチで修正される予定です。また、バージョン 6.5.0 でも修正されます。

アップグレードの失敗：コンテナインスタンスのディスク容量不足

展開：FTD を搭載した Firepower 4100/9300

アップグレード元：バージョン 6.3.0 ～ 6.4.0.x

直接アップグレード先：バージョン 6.3.0.1 ～ 6.5.0

多くの場合はメジャーアップグレード時に（場合によってはパッチ適用時に）、コンテナインスタンスを使用して設定されたFTDデバイスが、ディスク容量不足のエラーにより事前チェック段階で失敗することがあります。

この問題が発生した場合には、空きディスク容量を増やしてみてください。それでも解決しない場合は、Cisco TAC にお問い合わせください。

アップグレードの失敗：以前のバージョンが 6.2.3.12 の NGIPS デバイス

展開：7000/8000 シリーズ、ASA FirePOWER、NGIPSv

関連するバグ：CSCvp42398

アップグレード元：バージョン 6.2.3 ～ 6.3.0.x

直接アップグレード先：バージョン 6.4.0 のみ

次の場合、NGIPS デバイスをバージョン 6.4.0 にアップグレードすることはできません。

- デバイスが以前にバージョン 6.2.3.12 を実行していて、その後、次を実行した。
- バージョン 6.2.3.12 パッチをアンインストールしたか、バージョン 6.3.0.x にアップグレードした。

  これには、バージョン 6.2.3.12 パッチをアンインストールしてから、バージョン 6.3.0.x にアップグレードしたシナリオも含まれています。

上記が現在の状況である場合は、Cisco TAC にお問い合わせください。

TLS 暗号化アクセラレーションの有効化/無効にすることは不可

展開：Firepower 2100 シリーズ、Firepower 4100/9300 シャーシ

アップグレード元：バージョン 6.1.0 ～ 6.3.x

直接アップグレード先：バージョン 6.4.0 以降

SSL ハードウェアアクセラレーションは、*TLS* 暗号化アクセラレーションに名前が変更されました。

デバイスによっては、TLS 暗号化アクセラレーションがソフトウェアまたはハードウェアで実行される場合があります。アップグレードでは、この機能を手動で無効にした場合でも、すべての対象デバイスでアクセラレーションが自動的に有効になります。ほとんどの場合、この機能を設定することはできません。この機能は自動的に有効になり、無効にすることはできません。

バージョン *6.4.0* へのアップグレード： Firepower 4100/9300 シャーシのマルチインスタンス機能を使用している場合は、FXOS CLI を使用して、モジュール/セキュリティエンジンごとに、*1* つのコンテナ インスタンスに対して TLS 暗号アクセラレーションを有効にすることができます。他のコンテナインスタンスに対してアクセラレーションは無効になっていますが、ネイティブ インスタンスには有効になっています。

バージョン *6.5.0* 以降へのアップグレード：Firepower 4100/9300 シャーシのマルチインスタンス機能を使用している場合は、FXOS CLI を使用して、Firepower 4100/9300 シャーシ上の複数のコンテナ インスタンス（最大 16 個）に対して TLS 暗号アクセラレーションを有効にすることができます。新しいインスタンスでは、この機能がデフォルトで有効になっています。ただし、アップグレードによって既存のインスタンスのアクセラレーションが有効になることは「ありません」。代わりに、 **config hwCrypto enable** CLI コマンドを使用してください。

Firepower 4100/9300 のアップグレードにはバージョン 6.2.0 が必要

展開：FTD を搭載した Firepower 4100/9300

アップグレード元：バージョン 6.1.x

直接アップグレード先：バージョン 6.4.0 のみ

他の FMC 管理対象デバイスとは異なり、Firepower 4100/9300 シリーズデバイスでは、Firepower Threat Defense ソフトウェアをバージョン 6.1 から 6.4 に直接アップグレードすることはできません。これは、FXOS 2.6.1 は FTD バージョン 6.1 と互換性がないが、バージョン 6.4 では必要であるからです。

FXOS 2.3.1 では中間バージョンとしてバージョン 6.2.3 を使用することを推奨します。FXOS を最初にアップグレードする必要があることに注意してください。バージョン6.3 を中間リリースとして使用しないでください。『Firepower ReleaseNotes, Version 6.3.0』のガイドラインと警告を参照してください。

以前に公開されたガイドラインと警告

アップグレード パスでメジャー バージョンがスキップされる場合は、このチェックリストを確認してください。いくつかの以前のメジャーバージョンからバージョン6.4.0 にアップグレードできます。アップグレードする最小バージョン （54 ページ）を参照してください。

表 *18 :* 以前に公開されたバージョン *6.4.0* のガイドライン

✓	ガイドライン	プラットフォーム	アップグレード元	直接アップグレード先
	URL フィルタリング キャッシュのタイムアウトが変更される可能性 （44 ページ）	任意（Any）	6.2.3.x	6.3.0 以降

✓	ガイドライン	プラットフォーム	アップグレード元	直接アップグレード先
	FMC、7000/8000 シリーズ、NGIPSv で準備状況チェックに失敗する可能性 （44 ページ）	FMC Firepower 7000/8000 シリーズ NGIPSv	6.1.0 ～ 6.1.0.6 6.2.0 ～ 6.2.0.6 6.2.1 6.2.2 ～ 6.2.2.4 6.2.3 ～ 6.2.3.4	6.3.0 以降
	リモートアクセス VPN のデフォルト設定の変更によって VPN トラフィックがブロックされる可能性 （45 ページ）	FMC を使用した FTD	6.2.0 ～ 6.2.3.x	6.3.0 以降
	アプライアンスへのアクセスの更新されたセキュリティ （45 ページ）	任意（Any）	6.1.0 ～ 6.2.3.x	6.3.0 以降
	セキュリティ インテリジェンスによって可能になるアプリケーションの識別 （46 ページ）	FMC の展開	6.1.0 ～ 6.2.3.x	6.3.0 以降
	アップグレード後に VDB を更新して CIP 検出を有効化 （46 ページ）	任意（Any）	6.1.0 ～ 6.2.3.x	6.3.0 以降
	無効な侵入変数セットによって展開に失敗する可能性 （47 ページ）	任意（Any）	6.1.0 ～ 6.2.3.x	6.3.0 以降
	接続イベントと侵入イベントに関する Syslog の動作の変更 （47 ページ）	FMC	6.1.0 ～ 6.2.3.x	6.3.0 以降
	アップグレードにより CSSM から FTD/FDM を登録解除することが可能 （48 ページ）	FDM を使用した FTD	6.2.0 ～ 6.2.2.x	6.2.3 ～ 6.4.0
	レポートの結果の制限の変更 （48 ページ）	FMC	6.1.0 ～ 6.2.2.x	6.2.3 ～ 6.4.0
	アップグレードの前にバージョン 6.1.x FTD クラスタからサイト ID を削除 （49 ページ）	FTD クラスタ	6.1.0.x	6.2.3 ～ 6.4.0
	アップグレードの失敗：FDM を実行する ASA 5500-X シリーズのバージョン 6.2.2.5 から （49 ページ）	FDM を使用した FTD	6.2.0 のみ	6.2.2 ～ 6.4.0

✓	ガイドライン	プラットフォーム	アップグレード元	直接アップグレード先
	アクセス コントロールではSRUから遅延ベースのパフォーマンス設定を取得可能 （50 ページ）	FMC	6.1.0.x	6.2.0 ～ 6.4.0
	FTD での「フェールセーフ」から「Snort フェール オープン」への置き換え （50 ページ）	FMC を使用した FTD	6.1.0.x	6.2.0 ～ 6.4.0

URL フィルタリング キャッシュのタイムアウトが変更される可能性

展開：すべて

アップグレード元：バージョン 6.2.3.x

直接アップグレード先：バージョン 6.3.0+

バージョン 6.3.0 の新機能として、GUI で URL フィルタリング キャッシュのタイムアウト値を設定できます。古いデータと一致する URL のインスタンスを最小限に抑えるため、キャッシュ内の URL を期限切れに設定できます。Cisco TAC と連携して URL フィルタリング キャッシュのタイムアウト値を変更している場合、アップグレードによってその値が変更される可能性があります。

アップグレード完了後、

- FMC：**[システム（System）] > [統合（Integration）]** を選択し、[Cisco CSI] タブをクリックして、[キャッシュされたURLの期限切れ（Cached URLs Expire）] 設定を確認します。
- FDM：**[システム設定（System Settings）] > [トラフィック設定（Traffic Settings）] > [URL フィルタリングの設定（URL Filtering Preferences）]** を選択し、[URL存続可能時間（URL Time to Live）] 設定を確認します。

FMC、7000/8000シリーズ、NGIPSvで準備状況チェックに失敗する可能性

展開：FMC、7000/8000 シリーズ デバイス、NGIPSv

アップグレード元：バージョン 6.1.0 ～ 6.1.0.6、バージョン 6.2.0 ～ 6.2.0.6、バージョン 6.2.1、バージョン 6.2.2 ～ 6.2.2.4、およびバージョン 6.2.3 ～ 6.2.3.4

直接アップグレード先：バージョン 6.3.0+

次に示すバージョンの Firepower のいずれかからアップグレードする場合は、そこに示されているモデルで準備状態チェックを実行できません。これは、準備状況チェック プロセスが新しいアップグレード パッケージに対して互換性を持たないためです。

表 *19 :* バージョン *6.3.0* 以降用の準備状況チェックを備えたパッチ

準備完了チェックがサポートされない	修正された最初のパッチ
6.1.0 ～ 6.1.0.6	6.1.0.7
6.2.0 ～ 6.2.0.6	6.2.0.7
6.2.1	なし。バージョン 6.2.3.5+ にアップグレードしてください。
6.2.2 ～ 6.2.2.4	6.2.2.5
6.2.3 ～ 6.2.3.4	6.2.3.5

リモート アクセス VPN のデフォルト設定の変更によって VPN トラフィックがブロックされる可能性

展開：**リモート アクセス VPN 用に設定された** Firepower Threat Defense

アップグレード元：バージョン 6.2.x

直接アップグレード先：バージョン 6.3 +

バージョン6.3では非表示オプションの **sysopt connection permit-vpn** のデフォルト設定が変更されています。アップグレードすると、リモート アクセス VPN がトラフィックを渡さなくなる可能性があります。この場合は、次のいずれかの手法を使用してください。

- **sysopt connection permit-vpn** コマンドを設定する FlexConfig オブジェクトを作成します。このコマンドの新しいデフォルトは **no sysopt connection permit-vpn** です。

  これは、外部ユーザがリモート アクセス VPN アドレス プール内の IP アドレスになりすますことができないため、VPN でトラフィックを許可するよりも安全な方法です。欠点は VPN トラフィックが検査されないことです。つまり、侵入とファイルの保護、URL フィルタリング、その他の高度な機能がトラフィックに適用されません。

- リモート アクセス VPN アドレス プールからの接続を許可するアクセス制御ルールを作成します。

  この方法では、VPN トラフィックが確実に検査され、高度なサービスを接続に適用できます。欠点は、外部のユーザが IP アドレスをスプーフィングして、内部ネットワークにアクセスしやすくなることです。

アプライアンスへのアクセスの更新されたセキュリティ

展開：すべて

アップグレード元：バージョン 6.1 ～ 6.2.3.x

直接アップグレード先：バージョン 6.3 +

セキュリティを強化するために、バージョン 6.3 では、セキュア SSH アクセスのためにサポートされる暗号と暗号化アルゴリズムのリストが更新されました。暗号エラーのために SSH クライアントが Firepower アプライアンスとの接続に失敗する場合は、クライアントを最新バージョンに更新してください。

セキュリティインテリジェンスによって可能になるアプリケーションの識別

展開：Firepower Management Center

アップグレード元：バージョン 6.1 ～ 6.2.3.x

直接アップグレード先：バージョン 6.3 +

バージョン 6.3 では、セキュリティ インテリジェンスの設定によりアプリケーションの検出と識別が可能になります。現在の展開で検出を無効にした場合は、アップグレード プロセスによって再び検出が有効になる可能性があります。必要がない場合（たとえば、IPS のみの展開など）に検出を無効にするとパフォーマンスが向上する可能性があります。

検出を無効にするには、次の手順を実行する必要があります。

- ネットワーク検出ポリシーからすべてのルールを削除します。
- 単純なネットワークベースの条件（ゾーン、IP アドレス、VLAN タグ、およびポート）のみを使用してアクセス制御を実行します。どんな種類のアプリケーション、ユーザ、URL、または地理位置情報の制御も行わないでください。
- **（新規）**デフォルトのグローバル リストなど、アクセス コントロール ポリシーのセキュリティ インテリジェンス設定からすべてのホワイトリストとブラックリストを削除することで、ネットワークと URL ベースのセキュリティ インテリジェンスを無効にします。
- **（新規）**DNS のデフォルトのグローバル ホワイトリストや DNS ルールのグローバル ブラックリストなど、関連付けられている DNS ポリシー内のすべてのルールを削除または無効にすることで、DNS ベースのセキュリティ インテリジェンスを無効にします。

アップグレード後に VDB を更新して CIP 検出を有効化

展開：すべて

アップグレード元：バージョン 6.1.0 ～ 6.2.3.x、VDB 299+ 搭載

直接アップグレード先：バージョン 6.3.0+

脆弱性データベース（VDB）299 以降を使用しているときにアップグレードする場合、アップグレード プロセスの問題により、アップグレード後の CIP 検出を使用できなくなります。これには、2018 年 6 月から現在までにリリースされたすべての VDB に加えて、最新の VDB も含まれます。

アップグレード後は常に脆弱性データベース（VDB）を最新バージョンに更新することを推奨しますが、この場合は特に重要です。

この問題の影響を受けるかどうかを確認するには、CIPベースアプリケーションの条件を使用して、アクセス制御ルールを設定してみてください。ルール エディタで CIP アプリケーションが見つからない場合は、手動で VDB を更新します。

無効な侵入変数セットによって展開に失敗する可能性

展開：すべて

アップグレード元：バージョン 6.1 ～ 6.2.3.x

直接アップグレード先：バージョン 6.3.0+

侵入変数セット内のネットワーク変数については、除外する IP アドレスが、含める IP アドレスのサブセットである必要があります。次の表に、有効な設定と無効な設定の例を示します。

有効	無効
含める：10.0.0.0/8 除外する：10.1.0.0/16	含める：10.1.0.0/16 除外する：172.16.0.0/12 除外する：10.0.0.0/8

バージョン 6.3.0 より前のバージョンでは、このタイプの無効な設定でネットワーク変数を正常に保存できました。現在のバージョンでは、これらの設定によって展開がブロックされ、次のエラーが表示されます。`Variable set has invalid excluded values.`

この場合は、正しく設定されていない変数セットを識別して編集してから展開しなおしてください。変数セットによって参照されているネットワーク オブジェクトおよびグループの編集が必要である場合もあることに注意してください。

接続イベントと侵入イベントに関する Syslog の動作の変更

展開：Firepower Management Center

アップグレード元：バージョン 6.1.0 ～ 6.2.3.x

直接アップグレード先：バージョン 6.3.0+

バージョン 6.3.0 では、システムが Syslog を介して接続イベントと侵入イベントをログに記録する方法が変更され、一元化されています。アクセス コントロール ポリシーの新しい [ロギング（Logging）] タブでこれらの設定にアクセスできます。

アップグレードによって接続イベント ログの既存の設定が変更されることはありません。ただし、Syslog 経由では「期待されなかった」侵入イベントの受信が突然開始される可能性があります。これは、バージョン 6.3.0+ にアップグレードすると、侵入ポリシーによって、Syslog イベントが新しい [Logging] タブ上の宛先に送信されるためです（バージョン 6.3.0 以前では、外部ホストではなく、管理対象デバイス自体の Syslog にイベントを送信するように侵入ポリシーで Syslog アラートを設定できました）。

また、NGIPS デバイス（7000/8000 シリーズ、ASA FirePOWER、NGIPSv）から送信されるメッセージで、RFC 5425 で指定されている ISO 8601 タイムスタンプ形式が使用されるようになりました。

アップグレードにより CSSM から FTD/FDM を登録解除することが可能

導入：FDM を使用した FTD

アップグレード元：バージョン 6.2 ～ 6.2.2.x

直接アップグレード先：バージョン 6.2.3 ～ 6.4.0

Firepower Device Manager によって管理されている Firepower Threat Defense デバイスをアップグレードすると、そのデバイスが Cisco Smart Software Manager から登録解除される場合があります。アップグレードが完了したら、ライセンスのステータスを確認します。

ステップ 1 [デバイス（Device）] をクリックし、[スマートライセンス概要（Smart License summary）] の [設定の表示（View Configuration）] をクリックします。

ステップ 2 デバイスが登録されていない場合は、[Register Device] をクリックします。

レポートの結果の制限の変更

展開：Firepower Management Center

アップグレード元：バージョン 6.1.0 ～ 6.2.2.x

直接アップグレード先：バージョン 6.2.3 ～ 6.4.0

バージョン 6.2.3 では、次のように、使用できる結果の数、またはレポートのセクションに含めることができる結果の数が制限されています。テーブルおよび詳細ビューでは、PDF レポートに HTML または CSV レポートよりも少ないレコードを含めることができます。

表 *20 :* レポートの結果の新しい制限

レポート セクション タイプ	最大レコード数：**HTML** または **CSV** レポート セクション	最大レコード数：**PDF** レポート セクション
棒グラフ 円グラフ	100（上位または下位）	100（上位または下位）
テーブル ビュー	400,000	100,000
詳細ビュー	1,000	500

Firepower Management Center をアップグレードする前に、レポート テンプレート内のセクションで最大 HTML または CSV よりも大きい結果数を指定する場合は、アップグレード プロセスが設定を新しい最大値に下げます。

PDF レポートを生成するレポート テンプレートの場合、テンプレート セクションの PDF の制限を超えると、アップグレード プロセスは出力形式を HTML に変更します。PDF の生成を続行するには、結果数を PDF の最大に下げます。アップグレード後にこれを行った場合、出力形式の設定を PDF に戻します。

アップグレードの前にバージョン6.1.xFTDクラスタからサイトIDを削除

展開： Firepower Threat Defenseクラスタ

アップグレード元：バージョン 6.1.x

直接アップグレード先：バージョン 6.2.3 ～ 6.4.0

Firepower Threat Defense バージョン 6.1.x クラスタは、サイト間クラスタリングをサポートしていません（バージョン 6.2.0 以降では FlexConfig を使用してサイト間機能を設定できます）。

FXOS 2.1.1 でバージョン 6.1.x クラスタを展開または再展開している場合、（サポートされていない）サイト ID の値を入力しているときは、アップグレードする前に、FXOS の各ユニットでサイト ID を削除（**0** に設定）する必要があります。そうしないと、アップグレード後、ユニットがクラスタに再度参加できなくなります。

すでにアップグレード済みの場合は、サイト ID を各ユニットから削除してからクラスタを再確立します。サイト ID を表示または変更するには、『Cisco FXOS CLI Configuration Guide』を参照してください。

アップグレードの失敗：FDM を実行する ASA 5500-X シリーズのバージョン 6.2.2.5 から

展開：FDM を使用した FTD（メモリが少ない ASA 5500-X シリーズ デバイスで実行）

アップグレード元：バージョン 6.2.0

直接アップグレード先：バージョン 6.2.2 ～ 6.4.0

バージョン 6.2.0 からアップグレードする場合、アップグレードに失敗し、「`Uploaded file is not a valid system upgrade file`」というエラーが表示される可能性があります。これは、正しいファイルを使用している場合でも発生する可能性があります。

この場合は、次の回避策を試してください。

- 再度お試しください。（Try again.）
- CLI を使用してアップグレードする
- まず 6.2.0.1 にアップグレードする

アクセスコントロールではSRUから遅延ベースのパフォーマンス設定を取得可能

展開：FMC

アップグレード元：6.1.x

直接アップグレード先：6.2.0+

バージョン 6.2.0+ の新しいアクセス コントロール ポリシーでは、デフォルトで、最新の侵入ルール更新（SRU）から遅延ベースのパフォーマンス設定が取得されます。この動作は、新しい [Apply Settings From] オプションによって制御されます。このオプションを設定するには、アクセス コントロール ポリシーを編集または作成して、[Advanced] をクリックし、遅延ベースのパフォーマンス設定を編集します。

バージョン 6.2.0+ にアップグレードすると、現在（バージョン 6.1.x）の設定に従って新しいオプションが設定されます。現在の設定が次の場合、新しいオプションは次のように設定されます。

- [Default]：新しいオプションは、[Installed Rule Update] に設定されます。アップグレードしてから展開すると、最新の SRU からの遅延ベースのパフォーマンス設定が使用されます。最新の SRU が指定する内容によって、トラフィックの処理が変更される可能性があります。
- [Custom]：新しいオプションは、[Custom] に設定されます。システムは現在のパフォーマンス設定を保持します。このオプションによって動作が変更されることはありません。

アップグレードする前に設定を確認することをお勧めします。前述したように、バージョン 6.1.x の FMC Web インターフェイスから、ポリシーの遅延ベースのパフォーマンス設定を表示し、[Revert To Defaults] ボタンがグレー表示されているかどうかを確認します。ボタンがグレー表示されている場合は、デフォルト設定が使用されています。ボタンがアクティブになっている場合は、カスタム設定が設定されています。

FTDでの「フェールセーフ」から「Snortフェールオープン」への置き換え

展開：FMC を使用した FTD

アップグレード元：バージョン 6.1.x

直接アップグレード先：バージョン 6.2+

バージョン 6.2 では、Snort フェール オープン設定により、FMC によって管理される Firepower Threat Defense デバイスのフェールセーフ オプションが置き換えられます。フェールセーフでは、Snort がビジー状態のときにトラフィックをドロップすることができますが、Snort がダウンしている場合、トラフィックはインスペクションなしで自動的に通過します。Snort フェール オープンでは、このトラフィックをドロップすることができます。

FTD デバイスをアップグレードすると、その新しい Snort フェール オープン設定は、以下のように、古いフェールセーフ設定に依存します。新しい設定ではトラフィックの処理が変更されることはありませんが、アップグレードの前にフェールセーフを有効または無効にするかどうかを検討してください。

表 *21 :* フェールセーフの *Snort* フェール オープンへの移行

バージョン 6.1 のフェールセーフ	バージョン 6.2 の Snort フェール オープン	動作
無効（デフォルトの動作）	[Busy]：無効 [Down]：有効	Snort プロセスがビジー状態の場合は、新規および既存の接続をドロップし、Snort プロセスがダウンしている場合は、接続をインスペクションなしで通過します。
有効（Enabled）	[Busy]：有効 [Down]：有効	Snort プロセスがビジー状態またはダウンしている場合、新規または既存の接続をインスペクションなしで通過します。

Snort フェール オープンでは、デバイスにバージョン 6.2 が必要であることに注意してください。バージョン 6.1.x のデバイスを管理している場合、FMC Web インターフェイスにフェールセーフ オプションが表示されます。

一般的なガイドラインと警告

これらの重要なガイドラインと警告は、すべてのアップグレードに適用されます。ただし、このリストは包括的なものではありません。アップグレードパスの計画、OS のアップグレード、準備状況チェック、バックアップ、メンテナンス期間など、アップグレードプロセスに関するその他の重要な情報へのリンクについては、「アップグレード手順 （68 ページ）」を参照してください。

イベントデータと設定データのバックアップ

サポートされている場合は、アップグレードの前後にバックアップすることをお勧めします。

- アップグレード前：アップグレードが致命的な失敗であった場合は、再イメージ化を実行し、復元する必要がある場合があります。再イメージ化によって、システムパスワードを含むほとんどの設定が工場出荷時の初期状態に戻ります。最近のバックアップがある場合は、通常の操作にすばやく戻ることができます。
- アップグレード後：これにより、新しくアップグレードされた展開のスナップショットが作成されます。新しい FMC バックアップファイルがデバイスがアップグレードされたことを「認識」するように、管理対象デバイスをアップグレードした後に FMC をバックアップすることをお勧めします。

安全なリモートロケーションにバックアップし、正常に転送が行われることを確認する必要があります。アップグレードによって、ローカルに保存されたバックアップは消去されます。特

に、バックアップファイルは暗号化されていないため、不正アクセスを許可しないでください。バックアップ ファイルが変更されていると、復元プロセスは失敗します。

バックアップの最初のステップとして、アプライアンスモデルとバージョンを、パッチレベルを含めて書き留めておいてください。 FMC の場合は、VDB のバージョンを書き留めておきます。 Firepower 4100/9300 シャーシの場合は、FXOS のバージョンを書き留めておきます。. 新しいアプライアンスや再イメージ化したアプライアンスにバックアップを復元する必要がある場合は、新しいアプライアンスを最初に更新する必要がある場合があるため、これは重要です。

（注） バックアップと復元は、複雑なプロセスになる可能性があります。手順をスキップしたり、セキュリティ上の問題を無視しないでください。誤りを避けるには、注意深い計画と準備が役立ちます。バックアップと復元の要件、ガイドライン、制限事項、およびベストプラクティスの詳細については、ご使用の Firepower 製品のコンフィギュレーション ガイドを参照してください。

NTP 同期の確認

アップグレードする前に、時刻の提供に使用している NTP サーバと Firepower アプライアンスが同期していることを確認します。同期されていないと、アップグレードが失敗する可能性があります。FMC展開では、時刻のずれが10秒を超えている場合、[時刻同期化ステータス（Time Synchronization Status）] ヘルスモジュールからアラートが発行されますが、手動で確認する必要もあります。

時刻を確認するには、次の手順を実行します。

- FMC：[システム（System）] > [設定（Configuration）] > [時刻（Time）] を選択します。
- デバイス：**show time** CLI コマンドを使用します。

帯域幅をチェックする

Firepowerアプライアンスをアップグレードする（または準備状況チェックを実行する）には、アップグレードパッケージがアプライアンス上に存在する必要があります。Firepower アップグレードパッケージには、さまざまなサイズがあります。管理ネットワークに大量のデータ転送を実行するための帯域幅があることを確認します。

FMC の展開では、アップグレードパケージをアップグレード時に管理対象デバイスに転送する場合は、帯域幅が不十分だとアップグレード時間が長くなったり、アップグレードがタイムアウトする原因となる可能性があります。アップグレードする前に、管理対象デバイスに Firepower アップグレードパッケージを手動でプッシュ（コピー）することをお勧めします。詳細については、『Guidelines for Downloading Data from the Firepower Management Center to Managed Devices』（トラブルシューティング テクニカルノーツ）を参照してください。

アプライアンスアクセス

Firepowerデバイスは、（インターフェイス設定に応じて）アップグレード中、またはアップグレードが失敗した場合に、トラフィックを渡すことを停止できます。Firepowerデバイスをアップグレードする前に、ユーザの位置からのトラフィックがデバイスの管理インターフェイスにアクセスするためにデバイス自体を通過する必要がないことを確認してください。Firepower Management Center展開では、デバイスを経由せずにFMC管理インターフェイスにアクセスできる必要もあります。

署名付きのアップグレードパッケージ

Firepowerでは、正しいファイルを使用していることを確認できるようにするために、バージョン6.2.1+からのアップグレードパッケージ（およびバージョン6.2.1+へのホットフィックス）は、署名付きのtarアーカイブ（.tar）になっています。以前のバージョンからのアップグレードでは、引き続き未署名のパッケージが使用されます。

シスコサポートおよびダウンロードサイトからアップグレードパッケージを手動でダウンロードする場合（たとえば、メジャーアップグレードやエアギャップ展開のために）、正しいパッケージをダウンロードしていることを確認してください。 署名付きの（.tar）パッケージは解凍しないでください。

（注） 署名付きのアップグレードパッケージをアップロードした後、システムがパッケージを確認する際に、GUIのロードに数分かかることがあります。表示を高速化するには、署名付きのパッケージが不要になった後、それらのパッケージを削除します。

ASA FirePOWER デバイスでの ASA REST API の無効化

ASA FirePOWER モジュールをアップグレードする前に、ASA REST API を無効にしていることを確認します。無効にしていない場合、アップグレードが失敗することがあります。ASA CLIから：`no rest api agent`。アンインストール後に再度有効にすることができます：`rest-api agent`。

シスコとのデータの共有

一部の機能にシスコとのデータ共有が含まれます。

6.2.3+では、*Cisco Success Network*は、テクニカルサポートを提供するために不可欠な使用状況に関する情報と統計情報をシスコに送信します。アップグレード中に、参加を承諾するか、辞退するかを尋ねられます。また、いつでもオプトインまたはオプトアウトできます。

バージョン6.2.3+では、Web分析のトラッキングは、これに限定されませんが、ページでの操作、ブラウザのバージョン、製品のバージョン、ユーザの場所、FMC の管理 IP アドレスまたはホスト名を含む、個人を特定できない使用状況データをシスコに送信します。現在の設定でオプトアウトが選択されている場合でも、メジャーアップグレードによってWeb分析トラッキングが有効になります。このデータの収集を拒否する場合は、各メジャーアップグレードの後にオプトアウトしてください。

アップグレードにより侵入ルールをインポートして自動的に有効化できます。

現在の Firepower バージョンでサポートされていないキーワードが新しい侵入ルールで使用されている場合、侵入ルールデータベース（SRU）を更新しても、そのルールはインポートされません。

Firepower ソフトウェアをアップグレードし、これらのキーワードがサポートされると、新しい侵入ルールがインポートされ、IPS の設定に応じて自動的に有効化できるため、イベントの生成とトラフィックフローへの影響を開始できます。

サポートされているキーワードは、Firepower ソフトウェアに含まれている Snort のバージョンによって異なります。

- FMC：[ヘルプ（Help）] > [About（バージョン情報）] を選択します。
- FDM を使用した FTD：**show summary** CLI コマンドを使用します。
- ASDM を使用した ASA FirePOWER：[ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [システム情報（System Information）] を選択します。

また、Cisco Firepower Compatibility Guideの「*Bundled Components*」の項で Snort バージョンを確認することもできます。

Snort リリースノートには、新しいキーワードの詳細が含まれています。https://www.snort.org/downloads でSnort ダウンロードページのリリースノートを参照できます。

応答しないアップグレード

アップグレードしているアプライアンスとの間での変更の展開、またはアップグレードしているアプライアンスの手動での再起動やシャットダウンは行わないでください。進行中のアップグレードを再開しないでください。事前のチェック中に、アップグレードプロセスが停止しているように見える場合がありますが、これは想定内の動作です。アップグレードに失敗する、アプライアンスが応答しないなど、アップグレードで問題が発生した場合には Cisco TAC にお問い合わせください。

アップグレードする最小バージョン

いくつかの以前のメジャー バージョン シーケンスからバージョン 6.4.0 に直接アップグレードできます。アップグレードするために、以前のバージョンの最新のパッチを実行する必要はありません。

***Table 22: Firepower* ソフトウェアをバージョン *6.4.0* にアップグレードするための最小バージョン**

プラットフォーム	最小バージョン
Firepower Management Center Firepower 4100/9300 シリーズを除く、FMC 展開のすべての管理対象デバイス。	6.1.0

プラットフォーム	最小バージョン
FMC を使用した Firepower 4100/9300 上の Firepower Threat Defense	FXOS 2.6.1.157+ を搭載した 6.2.0 FMC で管理されている Firepower 4100/9300 シリーズ デバイスでは、FTD をバージョン 6.1 から 6.4 に直接アップグレードすることはできません。FXOS 2.3.1 では中間バージョンとしてバージョン 6.2.3 を使用することを推奨します。Firepower 4100/9300 のアップグレードにはバージョン 6.2.0 が必要, on page 42を参照してください。 ハイアベイラビリティまたはクラスタ化された展開をバージョン6.2.0.x、6.2.2.0、または6.2.2.1からアップグレードする際にヒットレスアップグレードが必要な場合は、「FTD アップグレード時の動作：Firepower 4100/9300 Chassis, on page 58」を参照してください。
FDM を使用した Firepower Threat Defense（すべてのプラットフォーム）	6.2.0
ASDM を使用した ASA FirePOWER	6.2.0

時間テストとディスク容量の要件

Firepower アプライアンスをアップグレードするには、十分な空きディスク容量が必要です。これがない場合、アップグレードは失敗します。Firepower Management Center を使用して管理対象デバイスをアップグレードする場合、デバイスアップグレードパッケージに対して、FMC は /Volume パーティションに追加のディスク容量を必要とします。また、アップグレードを実行するための十分な時間を確保してください。

参考のために、社内の時間とディスク容量のテストに関するレポートを提供しています。

時間テストについて

ここで指定した時間の値は、社内のテストに基づいています。

（注） 特定のプラットフォーム/シリーズについてテストされたすべてのアップグレードの最も遅い時間を報告していますが、複数の理由により（以下を参照）、報告された時間よりも、アップグレードにかかる時間が長くなることがあります。

テスト条件

- 展開：値は、Firepower Management Center 展開のテストから取得されています。これは、同様の条件の場合、リモートとローカルで管理されているデバイスの raw アップグレード時間が類似しているためです。
- バージョン：メジャー アップグレードの場合、以前のすべての対象メジャー バージョンからのアップグレードをテストします。パッチについては、ベースバージョンからアップグレードをテストします。
- モデル：ほとんどの場合、各シリーズの最もローエンドのモデルでテストし、場合によってはシリーズの複数のモデルでテストします。
- 仮想設定：メモリおよびリソースのデフォルト設定を使用してテストします。
- ハイアベイラビリティと拡張性: スタンドアロンデバイスでテストします。

  ハイアベイラビリティの構成またはクラスタ化された構成では、動作の継続性を保持するため、複数のデバイスは1つずつアップグレードされます。アップグレード中は、各デバイスはメンテナンス モードで動作します。そのため、デバイス ペアまたはクラスタ全体のアップグレードには、スタンドアロンデバイスのアップグレードよりも長い時間がかかります。 スタック構成の 8000 シリーズ デバイスは同時にアップグレードされ、スタックは、すべてのデバイスのアップグレードが完了するまで、限定的なバージョン混在の状態で動作することに注意してください。これには、スタンドアロンデバイスのアップグレードと比べて大幅に長い時間がかかるということはありません。
- 構成：構成とトラフィック負荷が最小限のアプライアンスでテストします。

  アップグレード時間は、構成の複雑さ、イベントデータベースのサイズ、また、それらがアップグレードから影響を受けるかどうか、受ける場合はどのような影響を受けるかにより、長くなる場合があります。たとえば多くのアクセス制御ルールを使用している場合、アップグレードはこれらのルールの格納方法をバックエンドで変更する必要があるため、アップグレードにはさらに長い時間がかかります。

時間はアップグレードのみを対象

値は、各プラットフォーム上で Firepower アップグレードスクリプトの実行にかかる時間のみを表しています。これらには、次の時間は含まれていません。

- 管理対象デバイスへのアップグレードパッケージの転送（アップグレード前またはアップグレード中）。
- 準備状況チェック。
- VDB と SRU の更新。
- 設定の展開。
- リブート（値が個別に報告される場合がある）。

ディスク容量の要件について

容量の見積もりは、すべてのアップグレードについて報告された最大のものです。2020 年前半以降のリリースでは、次のようになります。

- 切り上げなし（1 MB 未満）。
- 次の 1 MB に切り上げ（1 MB ～ 100 MB）。
- 次の 10 MB に切り上げ（100 MB ～ 1 GB）。
- 次の 100 MB に切り上げ（1 GB を超える容量）。

バージョン 6.4.0 の時間とディスク容量

Table 23: バージョン *6.4.0* の時間とディスク容量

プラットフォーム	ボリュームの容量	必要容量	FMC の容量	時間
FMC	13.3 GB	26 MB	—	41 分
FMCv：VMware 6.0	13.6 GB	29 MB	—	30 分
Firepower 2100 シリーズ	12 MB	8.9 GB	950 MB	20 分
Firepower 4100 シリーズ	10 MB	7.5 GB	920 MB	6 分
Firepower 9300	10 MB	7.7 GB	920 MB	7 分
ASA 5500-X シリーズ with FTD	9 GB	110 KB	1.1 GB	24 分
FTDv：VMware 6.0	7.5 GB	100 KB	1.1 GB	12 分
Firepower 7000/8000 シリーズ	7.7 GB	19 MB	980 MB	34 分
ASA FirePOWER	11.5 GB	22 MB	1.3 GB	66 分
NGIPSv：VMware 6.0	6.5 GB	19 MB	840 MB	16 分

トラフィック フロー、検査、およびデバイス動作

アップグレード中に発生するトラフィック フローおよびインスペクションでの潜在的な中断を特定する必要があります。これは、次の場合に発生する可能性があります。

- デバイスが再起動された場合。

- デバイス上でオペレーティングシステムまたは仮想ホスティング環境をアップグレードする場合。
- デバイス上で Firepower ソフトウェアをアップグレードするか、パッチをアンインストールする場合。
- アップグレードまたはアンインストール プロセスの一部として設定変更を展開する場合（Snort プロセスが再開します）。

デバイスのタイプ、展開のタイプ（スタンドアロン、ハイアベイラビリティ、クラスタ化）、およびインターフェイスの設定（パッシブ、IPS、ファイアウォールなど）によって中断の性質が決まります。アップグレードまたはアンインストールは、保守期間中に行うか、中断による展開環境への影響が最も小さい時点で行うことを強く推奨します。

FTD アップグレード時の動作： Firepower 4100/9300 Chassis

このセクションでは、FTD を搭載した Firepower 4100/9300 シャーシをアップグレードするときのデバイスとトラフィックの動作を説明します。

Firepower 4100/9300 Chassis：FXOS のアップグレード

シャーシ間クラスタリングまたはハイアベイラビリティペアの構成がある場合でも、各シャーシの FXOS を個別にアップグレードします。アップグレードの実行方法により、FXOS のアップグレード時にデバイスがトラフィックを処理する方法が決定されます。

表 *24 : FXOS* アップグレード中のトラフィックの動作

展開	方法	トラフィックの動作
スタンドアロン	—	ドロップされる
ハイアベイラビリティ	**ベストプラクティス**：スタンバイで FXOS を更新し、アクティブピアを切り替えて新しいスタンバイをアップグレードします。	影響なし
	スタンバイでアップグレードが終了する前に、アクティブピアで FXOS をアップグレードします。	1 つのピアがオンラインになるまでドロップされる
シャーシ間クラスタ（6.2 以降）	**ベストプラクティス**：少なくとも 1 つのモジュールを常にオンラインにするため、一度に 1 つのシャーシをアップグレードします。	影響なし
	ある時点ですべてのモジュールを停止するため、シャーシを同時にアップグレードします。	少なくとも 1 つのモジュールがオンラインになるまでドロップされる

展開	方法	トラフィックの動作
シャーシ内クラスタ（Firepower 9300 のみ）	Fail-to-wire 有効：[バイパス：スタンバイ（Bypass: Standby）] または [バイパス：強制（Bypass-Force）]（6.1 以降）	インスペクションなしで転送
	Fail-to-wire 無効：[バイパス：無効（Bypass: Disabled）]（6.1 以降）	少なくとも 1 つのモジュールがオンラインになるまでドロップされる
	fail-to-wire モジュールなし。	少なくとも 1 つのモジュールがオンラインになるまでドロップされる

スタンドアロン FTD デバイス：Firepower ソフトウェアのアップグレード

インターフェイスの設定により、アップグレード中にスタンドアロンデバイスがトラフィックを処理する方法が決定されます。

表 *25 : Firepower* ソフトウェアアップグレード中のトラフィックの動作：スタンドアロン *FTD* デバイス

インターフェイスの設定		トラフィックの動作
ファイアウォールインターフェイス	EtherChannel、冗長、サブインターフェイスを含むルーテッドまたはスイッチド スイッチドインターフェイスは、ブリッジグループまたはトランスペアレントインターフェイスとしても知られています。	ドロップされる
IPS のみのインターフェイス	インラインセット、fail-to-wire が有効：[バイパス：スタンバイ（Bypass: Standby）] または [バイパス：強制（Bypass-Force）]（6.1 以降）	次のいずれかを行います。 • ドロップ（6.1 から 6.2.2.x） • インスペクションなしで転送（6.2.3 以降）
	インラインセット、fail-to-wire が無効：[バイパス：無効（Bypass: Disabled）]（6.1 以降）	ドロップされる
	インラインセット、fail-to-wire モジュールなし	ドロップされる
	インラインセット、タップモード	パケットをただちに出力、コピーへのインスペクションなし
	パッシブ、ERSPAN パッシブ	中断なし、インスペクションなし

ハイアベイラビリティペア：FirePOWER ソフトウェアアップグレード

ハイアベイラビリティペアのデバイスのFirePOWERソフトウェアをアップグレードする間に、トラフィックフローまたはインスペクションが中断されることはありません。継続稼働できるように、一度に1つずつアップグレードされます。アップグレード中、デバイスはメンテナンスモードで稼働します。

スタンバイ側のデバイスが最初にアップグレードされます。デバイスの役割が切り替わり、新しくスタンバイになったデバイスがアップグレードされます。アップグレードの完了時には、デバイスの役割は切り替わったままです。アクティブ/スタンバイの役割を維持する場合、アップグレード前に役割を手動で切り替えます。それにより、アップグレードプロセスによって元の役割に切り替わります。

クラスタ：FirePOWER ソフトウェアアップグレード

Firepower Threat Defense クラスタのデバイスで FirePOWER ソフトウェアをアップグレードする間に、トラフィックフローまたはインスペクションが中断されることはありません。継続稼働できるように、一度に1つずつアップグレードされます。アップグレード中、デバイスはメンテナンスモードで稼働します。

スレーブ セキュリティ モジュールを最初にアップグレードして、その後マスターをアップグレードします。アップグレード中、セキュリティモジュールはメンテナンスモードで稼働します。

マスターセキュリティモジュールをアップグレードする間、通常トラフィックインスペクションと処理は続行しますが、システムはロギングイベントを停止します。ロギングダウンタイム中に処理されるトラフィックのイベントは、アップグレードが完了した後、非同期のタイムスタンプ付きで表示されます。ただし、ロギングダウンタイムが大きい場合、システムはログ記録する前に最も古いイベントをプルーニングすることがあります。

（注） バージョン6.2.0、6.2.0.1、または6.2.0.2からシャーシ間クラスタをアップグレードすると、各モジュールがクラスタから削除されるときに、トラフィック インスペクションで2～3秒のトラフィック中断が発生します。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、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。

ハイアベイラビリティとクラスタリング ヒットレス アップグレードの要件

ヒットレスアップグレードの実行には、次の追加要件があります。

フローオフロード：フローオフロード機能でのバグ修正により、FXOSとFTDのいくつかの組み合わせはフローオフロードをサポートしていません。『Cisco Firepower Compatibility Guide』を参照してください。ハイアベイラビリティまたはクラスタ化された展開でヒットレスアップグレードを実行するには、常に互換性のある組み合わせを実行していることを確認する必要があります。

アップグレードパスに FXOS の2.2.2.91、2.3.1.130、またはそれ以降のアップグレード（FXOS 2.4.1. x、2.6.1 などを含む）が含まれている場合、次のパスを使用します。

1. FTD を 6.2.2.2 以降にアップグレードします。

2. FXOS を 2.2.2.91、2.3.1.130、またはそれ以降にアップグレードします。

3. FTD を最終バージョンにアップグレードします。

たとえば、FXOS 2.2.2.17/FTD 6.2.2.0 を実行していて、FXOS 2.6.1/FTD 6.4.0 にアップグレードする場合は、次を実行できます。

1. FTD を 6.2.2.5 にアップグレードします。

2. FXOS を 2.6.1 にアップグレードします。

3. FTD を 6.4.0 にアップグレードします。

バージョン 6.1.0 へのアップグレード：FTD ハイアベイラビリティペアのバージョン 6.1.0 へのヒットレスアップグレードを実行するには、プレインストールパッケージが必要です。詳細については、『Firepower System Release Notes Version 6.1.0 Preinstallation Package』を参照してください。

展開時のトラフィックの動作

アップグレード プロセス中には、設定を複数回展開します。Snort は、通常、アップグレード直後の最初の展開時に再起動されます。展開の前に、特定のポリシーまたはデバイス設定を変更しない限り、それ以外の展開時に再起動されることはありません。詳細については、『Firepower Management Center Configuration Guide』の「Configurations that Restart the Snort Process when Deployed or Activated」を参照してください。

展開する際にリソースを要求すると、いくつかのパケットがインスペクションなしでドロップされることがあります。また、Snortプロセスを再起動すると、HA/スケーラビリティ用に設定されたものを含め、すべての Firepower デバイスでトラフィック インスペクションが中断されます。インターフェイス設定により、中断中にインスペクションせずにトラフィックをドロップするか受け渡すかが決定されます。

表 *26 : FTD* 展開時のトラフィックの動作

インターフェイスの設定		トラフィックの動作
ファイアウォール インターフェイス	EtherChannel、冗長、サブインターフェイスを含むルーテッドまたはスイッチド スイッチドインターフェイスは、ブリッジグループまたはトランスペアレントインターフェイスとしても知られています。	ドロップされる

インターフェイスの設定		トラフィックの動作
IPS のみのインターフェイス	インラインセット、[フェールセーフ（Failsafe）]が有効または無効（6.0.1 ～ 6.1.0.x）	インスペクションなしで転送 [フェールセーフ（Failsafe）] が無効で、Snortがビジーでもダウンしていない場合、いくつかのパケットがドロップすることがあります。
	インラインセット、[Snortフェールオープン：ダウン（Snort Fail Open: Down）]：無効（6.2 以降）	ドロップされる
	インラインセット、[Snortフェールオープン：ダウン（Snort Fail Open: Down）]：有効（6.2+）	インスペクションなしで転送
	インラインセット、タップモード	パケットをただちに出力、コピーへのインスペクションなし
	パッシブ、ERSPAN パッシブ	中断なし、インスペクションなし

FTD アップグレード時の動作：その他のデバイス

このセクションでは、Firepower 1000/2100 シリーズ、ASA 5500-X シリーズ、ISA 3000、および FTDv で Firepower Threat Defense をアップグレードするときのデバイスとトラフィックの動作を説明します。

スタンドアロン FTD デバイス：Firepower ソフトウェアのアップグレード

インターフェイスの設定により、アップグレード中にスタンドアロンデバイスがトラフィックを処理する方法が決定されます。

表 *27 : Firepower* ソフトウェアアップグレード中のトラフィックの動作：スタンドアロン *FTD* デバイス

インターフェイスの設定		トラフィックの動作
ファイアウォールインターフェイス	EtherChannel、冗長、サブインターフェイスを含むルーテッドまたはスイッチド スイッチドインターフェイスは、ブリッジグループまたはトランスペアレントインターフェイスとしても知られています。	ドロップされる

インターフェイスの設定		トラフィックの動作
IPS のみのインターフェイス	インラインセット、fail-to-wire が有効：[バイパス：スタンバイ（Bypass: Standby）] または [バイパス：強制（Bypass-Force）]（6.1 以降）	次のいずれかを行います。 • ドロップ（6.1 から 6.2.2.x） • インスペクションなしで転送（6.2.3 以降）
	インラインセット、fail-to-wire が無効：[バイパス：無効（Bypass: Disabled）]（6.1 以降）	ドロップされる
	インラインセット、fail-to-wire モジュールなし	ドロップされる
	インラインセット、タップモード	パケットをただちに出力、コピーへのインスペクションなし
	パッシブ、ERSPAN パッシブ	中断なし、インスペクションなし

ハイアベイラビリティペア：FirePOWER ソフトウェアアップグレード

ハイアベイラビリティペアのデバイスの FirePOWER ソフトウェアをアップグレードする間に、トラフィックフローまたはインスペクションが中断されることはありません。継続稼働できるように、一度に 1 つずつアップグレードされます。アップグレード中、デバイスはメンテナンスモードで稼働します。

スタンバイ側のデバイスが最初にアップグレードされます。デバイスの役割が切り替わり、新しくスタンバイになったデバイスがアップグレードされます。アップグレードの完了時には、デバイスの役割は切り替わったままです。アクティブ/スタンバイの役割を維持する場合、アップグレード前に役割を手動で切り替えます。それにより、アップグレードプロセスによって元の役割に切り替わります。

展開時のトラフィックの動作

アップグレード プロセス中には、設定を複数回展開します。Snort は、通常、アップグレード直後の最初の展開時に再起動されます。展開の前に、特定のポリシーまたはデバイス設定を変更しない限り、それ以外の展開時に再起動されることはありません。詳細については、『Firepower Management Center Configuration Guide』の「Configurations that Restart the Snort Process when Deployed or Activated」を参照してください。

展開する際にリソースを要求すると、いくつかのパケットがインスペクションなしでドロップされることがあります。また、Snort プロセスを再起動すると、HA/スケーラビリティ用に設定されたものを含め、すべての Firepower デバイスでトラフィック インスペクションが中断されます。インターフェイス設定により、中断中にインスペクションせずにトラフィックをドロップするか受け渡すかが決定されます。

表 *28 : FTD* 展開時のトラフィックの動作

インターフェイスの設定		トラフィックの動作
ファイアウォールインターフェイス	EtherChannel、冗長、サブインターフェイスを含むルーテッドまたはスイッチド スイッチドインターフェイスは、ブリッジグループまたはトランスペアレントインターフェイスとしても知られています。	ドロップされる
IPS のみのインターフェイス	インラインセット、[フェールセーフ（Failsafe）]が有効または無効（6.0.1 ～ 6.1.0.x）	インスペクションなしで転送 [フェールセーフ（Failsafe）] が無効で、Snortがビジーでもダウンしていない場合、いくつかのパケットがドロップすることがあります。
	インラインセット、[Snortフェールオープン：ダウン（Snort Fail Open: Down）]：無効（6.2 以降）	ドロップされる
	インラインセット、[Snortフェールオープン：ダウン（Snort Fail Open: Down）]：有効（6.2+）	インスペクションなしで転送
	インラインセット、タップモード	パケットをただちに出力、コピーへのインスペクションなし
	パッシブ、ERSPAN パッシブ	中断なし、インスペクションなし

FirePOWER 7000/8000 シリーズのアップグレード時の動作

次のセクションでは、Firepower 7000/8000 シリーズデバイスをアップグレードする際のデバイスおよびトラフィックの動作について説明します。

スタンドアロン 7000/8000 シリーズ：Firepower ソフトウェアのアップグレード

インターフェイスの設定により、アップグレード中にスタンドアロンデバイスがトラフィックを処理する方法が決定されます。

表 *29 :* アップグレード中のトラフィックの動作：スタンドアロン *7000/8000* シリーズ

インターフェイスの設定	トラフィックの動作
インライン、ハードウェア バイパスが有効（[バイパスモード：バイパス（Bypass Mode: Bypass）]）	インスペクションなしで転送。ただし、トラフィックは、次の 2 つのポイントで一時的に中断します。 • アップグレード プロセスの開始時に、リンクがダウンしてから復旧（フラップ）し、ネットワーク カードがハードウェア バイパスに切り替わるとき。 • アップグレードが完了した後、リンクが復旧し、ネットワーク カードがバイパスから切り替わるとき。インスペクションはエンドポイントの再接続後に再開され、デバイス インターフェイスとのリンクを再確立します。
インライン、ハードウェア バイパス モジュールなし、またはハードウェア バイパスが無効（[バイパスモード：非バイパス（Bypass Mode: Non-Bypass）]）	ドロップされる
インライン、タップ モード	パケットをただちに出力、コピーへのインスペクションなし
パッシブ	中断なし、インスペクションなし
ルーテッド、スイッチド	ドロップされる

7000/8000 シリーズ ハイ アベイラビリティ ペア：Firepower ソフトウェアのアップグレード

ハイ アベイラビリティ ペアのデバイス（またはデバイス スタック）をアップグレードする間に、トラフィック フローまたはインスペクションが中断されることはありません。継続稼働できるように、一度に1つずつアップグレードされます。アップグレード中、デバイスはメンテナンスモードで稼働します。

最初にアップグレードするピアは、展開によって異なります。

- ルーテッドまたはスイッチド：最初にスタンバイがアップグレードされます。デバイスの役割が切り替わり、新しくスタンバイになったデバイスがアップグレードされます。アップグレードの完了時には、デバイスの役割は切り替わったままです。アクティブ/スタンバイの役割を維持する場合、アップグレード前に役割を手動で切り替えます。それにより、アップグレードプロセスによって元の役割に切り替わります。
- アクセス制御のみ：最初にアクティブがアップグレードされます。アップグレードの完了時に、アクティブとスタンバイの以前の役割がデバイスで維持されます。

8000 シリーズ スタック：FirePOWER ソフトウェア アップグレード

8000 シリーズ スタックでは、デバイスは同時にアップグレードされます。プライマリ デバイスがアップグレードを完了してスタックが動作を再開するまで、トラフィックはスタックがスタンドアロンデバイスであったかのように影響を受けます。すべてのデバイスがアップグレードを完了するまで、スタックは、制限付きの混合バージョンの状態で動作します。

展開時のトラフィックの動作

アップグレード プロセス中には、設定を複数回展開します。Snort は、通常、アップグレード直後の最初の展開時に再起動されます。展開の前に、特定のポリシーまたはデバイス設定を変更しない限り、それ以外の展開時に再起動されることはありません。詳細については、『Firepower Management Center Configuration Guide』の「Configurations that Restart the Snort Process when Deployed or Activated」を参照してください。

展開する際にリソースを要求すると、いくつかのパケットがインスペクションなしでドロップされることがあります。また、Snort プロセスを再起動すると、HA/スケーラビリティ用に設定されたものを含め、すべての Firepower デバイスでトラフィック インスペクションが中断されます。インターフェイス設定により、中断中にインスペクションせずにトラフィックをドロップするか受け渡すかが決定されます。

表 *30 :* 展開時のトラフィックの動作：*7000/8000* シリーズ

インターフェイスの設定	トラフィックの動作
インライン、[フェールセーフ（Failsafe）]が有効または無効	インスペクションなしで転送 [フェールセーフ（Failsafe）]が無効で、Snort がビジーでもダウンしていない場合、いくつかのパケットがドロップすることがあります。
インライン、タップ モード	すぐにパケットを出力し、バイパス Snort をコピーする
パッシブ	中断なし、インスペクションなし
ルーテッド、スイッチド	ドロップされる

ASA FirePOWER アップグレード時の動作

Snort プロセスを再起動する特定の設定を展開する場合を含め、モジュールが FirePOWER ソフトウェア アップグレード中にトラフィックを処理する方法を決定する、ASA FirePOWER module へのトラフィック リダイレクトに関する ASA サービス ポリシーです。

表 *31 : ASA FirePOWER* アップグレード中のトラフィックの動作

トラフィック リダイレクト ポリシー	トラフィックの動作
フェール オープン（**sfr fail-open**）	インスペクションなしで転送
フェール クローズ（**sfr fail-close**）	ドロップされる

トラフィック リダイレクト ポリシー	トラフィックの動作
モニタのみ（**sfr {fail-close}|{fail-open} monitor-only**）	パケットをただちに出力、コピーへのインスペクションなし

ASA FirePOWER 展開時のトラフィックの動作

Snort プロセスが再起動している間のトラフィックの動作は、ASA FirePOWER moduleをアップグレードする場合と同じです。

アップグレード プロセス中には、設定を複数回展開します。Snort は、通常、アップグレード直後の最初の展開時に再起動されます。展開の前に、特定のポリシーまたはデバイス設定を変更しない限り、それ以外の展開時に再起動されることはありません。詳細については、『Firepower Management Center Configuration Guide』の「Configurations that Restart the Snort Process when Deployed or Activated」を参照してください。

展開する際にリソースを要求すると、いくつかのパケットがインスペクションなしでドロップされることがあります。 さらに、Snort プロセスを再起動すると、トラフィック インスペクションが中断されます。サービスポリシーにより、中断中にインスペクションせずにトラフィックをドロップするか通過するかが決定されます。

NGIPSv アップグレード時の動作

このセクションでは、NGIPSvをアップグレードするときのデバイスとトラフィックの動作を説明します。

Firepower ソフトウェア アップグレード

インターフェイスの設定により、アップグレード中に NGIPSv がトラフィックを処理する方法が決定されます。

表 *32 : NGIPSv* アップグレード中のトラフィックの動作

インターフェイスの設定	トラフィックの動作
インライン	ドロップされる
インライン、タップ モード	パケットをただちに出力、コピーへのインスペクションなし
パッシブ	中断なし、インスペクションなし

展開時のトラフィックの動作

アップグレード プロセス中には、設定を複数回展開します。Snort は、通常、アップグレード直後の最初の展開時に再起動されます。展開の前に、特定のポリシーまたはデバイス設定を変更しない限り、それ以外の展開時に再起動されることはありません。詳細については、

『Firepower Management Center Configuration Guide』の「Configurations that Restart the Snort Process when Deployed or Activated」を参照してください。

展開する際にリソースを要求すると、いくつかのパケットがインスペクションなしでドロップされることがあります。さらに、Snortプロセスを再起動すると、トラフィック インスペクションが中断されます。インターフェイス設定により、中断中にインスペクションせずにトラフィックをドロップするか受け渡すかが決定されます。

表 *33 : NGIPSv* 展開時のトラフィックの動作

インターフェイスの設定	トラフィックの動作
インライン、[フェールセーフ（Failsafe）] が有効または無効	インスペクションなしで転送 [フェールセーフ（Failsafe）] が無効で、Snort がビジーでもダウンしていない場合、いくつかのパケットがドロップすることがあります。
インライン、タップ モード	すぐにパケットを出力し、バイパス Snort をコピーする
パッシブ	中断なし、インスペクションなし

アップグレード手順

リリース ノートにはアップグレード手順は含まれていません。これらのリリース ノートに記載されているガイドラインと警告を読んだ後、次のいずれかを参照してください。

- Cisco Firepower Management Center Upgrade Guide：管理対象デバイスや付随するオペレーティング システムを含む、FMC 展開のアップグレード
- Cisco ASA Upgrade Guide：ASDM を使用した ASA FirePOWER moduleのアップグレード
- Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager：FDM を使用した FTD のアップグレード

アップグレードパッケージ

アップグレードパッケージは、シスコ サポートおよびダウンロード サイトで入手できます。

- FMCv を含む Firepower Management Center：https://www.cisco.com/go/firepower-software
- Firepower Threat Defense（ISA 3000）：https://www.cisco.com/go/isa3000-software
- Firepower Threat Defense（FTDv を含む他のすべてのモデル）：https://www.cisco.com/go/ftd-software
- FirePOWER 7000 シリーズ：https://www.cisco.com/go/7000series-software

- FirePOWER 8000 シリーズ： https://www.cisco.com/go/8000series-software
- ASA with FirePOWER Services（ASA 5500-X シリーズ）： https://www.cisco.com/go/asa-firepower-sw
- ASA with FirePOWER Services（ISA 3000）： https://www.cisco.com/go/isa3000-software
- NGIPSv： https://www.cisco.com/go/ngipsv-software

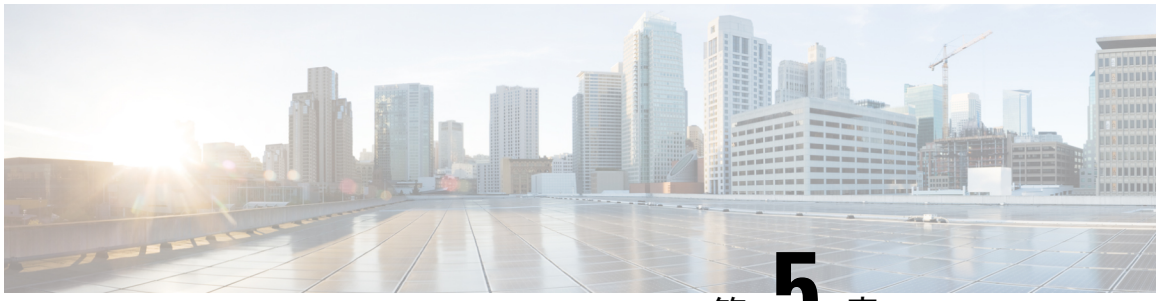
バージョン 6.2.1+ からのアップグレード パッケージは、署名付きの tar アーカイブ（.tar）です。解凍しないでください。

Table 34: バージョン ***6.2.1+*** からのアップグレード パッケージ

プラットフォーム	パッケージ
FMC/FMCv	Cisco_Firepower_Mgmt_Center_Upgrade-*version-build*.sh.REL.tar
Firepower 2100 シリーズ	Cisco_FTD_SSP_FP2K_Upgrade-*version-build*.sh.REL.tar
Firepower 4100/9300 シャーシ	Cisco_FTD_SSP_Upgrade-*version-build*.sh.REL.tar
FTD を搭載した ASA 5500-X シリーズ FTD を搭載した ISA 3000 Firepower Threat Defense 仮想	Cisco_FTD_Upgrade-*version-build*.sh.REL.tar
Firepower 7000/8000 シリーズ	Cisco_Firepower_NGIPS_Appliance_Upgrade-*version-build*.sh.REL.tar
ASA FirePOWER	Cisco_Network_Sensor_Upgrade-*version-build*.sh.REL.tar
NGIPSv	Cisco_Firepower_NGIPS_Virtual_Upgrade-*version-build*.sh.REL.tar

Table 35: バージョン ***6.1.x*** または ***6.2.0.x*** からのアップグレード パッケージ

プラットフォーム	パッケージ
FMC/FMCv	Cisco_Firepower_Mgmt_Center_Upgrade-*version-build*.sh
Firepower 4100/9300 シャーシ	Cisco_FTD_SSP_Upgrade-*version-build*.sh
FTD を搭載した ASA 5500-X シリーズ Firepower Threat Defense 仮想	Cisco_FTD_Upgrade-*version-build*.sh
Firepower 7000/8000 シリーズ	Cisco_Firepower_NGIPS_Appliance_Upgrade-*version-build*.sh
ASA FirePOWER	Cisco_Network_Sensor_Upgrade-*version-build*.sh
NGIPSv	Cisco_Firepower_NGIPS_Virtual_Upgrade-*version-build*.sh



第 5 章

新規インストール バージョン 6.4.0

Firepower アプライアンスをアップグレードできない（または必要なアップグレード パスを実行したくない）場合は、Firepower のメジャー リリースを新規インストールできます。

新規インストールの決定

次の表を使用して、新規インストール（再イメージ化とも呼ばれます）する必要がある場合のシナリオを特定します。これらのすべてのシナリオ（ローカルとリモート間のデバイス管理の切り替えを含む）では、デバイス設定が失われます。

（注） 管理の再イメージ化または切り替えを行う前に、ライセンスの問題に対処してください。Cisco Smart Licensing を使用している場合は、孤立した権限付与の発生を防ぐために、Cisco Smart Software Manager（CSSM）から手動で登録解除する必要がある場合があります。これらが生じると再登録できない場合があります。

表 *36 :* シナリオ：新規インストールが必要ですか。

シナリオ	ソリューション	ライセンシング
FMC で管理されているデバイスをより古い Firepower バージョンからアップグレードします。	古いバージョンからのアップグレード パスには中間バージョンが含まれる場合があります。特に、FMC とデバイスのアップグレードを交互に行う必要がある大規模展開の環境では、この複数の手順のプロセスを完了するために時間がかかる場合があります。 この時間を短縮するために、アップグレードする代わりに、古いデバイスを再イメージ化することができます。 **1.** FMC からデバイスを削除します。 **2.** FMC のみをターゲット バージョンにアップグレードします。 **3.** デバイスを再イメージ化します。 バージョン 5.x を実行している 7000/8000 シリーズデバイスのイメージを再作成する必要がある場合は、「新規インストールに関するガイドラインと制約事項 （73 ページ）」を参照してください。 **4.** デバイスを FMC に再度追加します。	FMC からデバイスを削除すると、デバイスが登録解除されます。デバイスを再度追加した後、ライセンスを再割り当てします。
FTD 管理を FDM から FMC（ローカルからリモート）に変更します。	**configure manager** CLI コマンドを使用します。『Command Reference for Firepower Threat Defense』を参照してください。	管理を切り替える前に、デバイスを登録解除します。デバイスを FMC に追加した後、ライセンスを再割り当てします。
FTD 管理を FMC から FDM（リモートからローカル）に変更します。	**configure manager** CLI コマンドを使用します。『Command Reference for Firepower Threat Defense』を参照してください。 **例外**：デバイスが実行中であるか、バージョン6.0.1からアップグレードされています。この場合は、再イメージ化します。	FMC からデバイスを削除し、デバイスを登録解除します。FDM を使用して再登録します。
ASDM と FMC 間の ASA FirePOWER 管理を変更します。	他の管理方法の使用を開始します。	クラシック ライセンスについては、セールス担当者にお問い合わせください。ASA FirePOWER ライセンスは、特定のマネージャに関連付けられています。

シナリオ	ソリューション	ライセンシング
ASA FirePOWER を同じ物理デバイス上の FTD に置き替えます。	再イメージ化します。	クラシック ライセンスをスマート ライセンスに変換します。『Firepower Management Center Configuration Guide』を参照してください。
NGIPSv を FTDv に置き換えます。	再イメージ化します。	新しいスマート ライセンスについては、セールス担当者にお問い合わせください。
障害が発生した FMC または FTD デバイスをバックアップから復元します。	RMA のシナリオでは、交換品は工場出荷時の初期状態の設定で届きます。ただし、交換品がすでに設定されている場合は、復元する前に再イメージ化することをお勧めします。	再イメージ化する前に登録を解除したり、FMC からデバイスを削除したりしないでください。これらの操作を行った場合、復元後に再度登録を解除してから再登録する必要があります。 代わりに、バックアップを実行した後に行われたライセンス変更を元に戻します。復元が完了したら、ライセンスを再設定します。ライセンスの競合や孤立した権限付与に気付いた場合は、Cisco TAC にお問い合わせください。

新規インストールに関するガイドラインと制約事項

誤りを避けるには、注意深い計画と準備が役立ちます。Firepower リリースに精通していて、Firepower アプライアンスを再イメージ化したことがある場合でも、これらのガイドラインと制限事項に加えて、「設置手順 （77 ページ）」にリンクされている手順を必ず参照してください。

イベント データと設定データのバックアップ

サポートされている場合は、再イメージ化の前にバックアップすることを強くお勧めします。

（注） 再イメージ化してアップグレードする必要がない場合、バージョンの制約により、バックアップを使用して古い設定をインポートすることはできません。設定は手動で再作成する必要があります。

安全なリモートロケーションにバックアップし、正常に転送が行われることを確認する必要があります。再イメージ化によって、システムパスワードを含むほとんどの設定が工場出荷時の初期状態に戻ります。アプライアンスに残っているすべてのバックアップが削除されます。特に、バックアップファイルは暗号化されていないため、不正アクセスを許可しないでください。バックアップ ファイルが変更されていると、復元プロセスは失敗します。

バックアップの最初のステップとして、アプライアンスモデルとバージョンを、パッチレベルを含めて書き留めておいてください。 FMC の場合は、VDB のバージョンを書き留めておきます。 Firepower 4100/9300 シャーシの場合は、FXOS のバージョンを書き留めておきます。新しいアプライアンスや再イメージ化したアプライアンスにバックアップを復元する必要がある場合は、新しいアプライアンスを最初に更新する必要がある場合があるため、これは重要です。

（注） バックアップと復元は、複雑なプロセスになる可能性があります。手順をスキップしたり、セキュリティ上の問題を無視しないでください。誤りを避けるには、注意深い計画と準備が役立ちます。バックアップと復元の要件、ガイドライン、制限事項、およびベストプラクティスの詳細については、ご使用の Firepower 製品のコンフィギュレーション ガイドを参照してください。

からのデバイスの削除 Firepower Management Center

再イメージ化されたアプライアンスを手動で設定する予定がある場合は、再イメージ化する前に、リモート管理からデバイスを削除します。

- FMC を再イメージ化する場合は、すべてのデバイスを管理から削除します。
- 単一のデバイスを再イメージ化するか、またはリモートからローカルでの管理に切り替える場合は、その単一のデバイスを削除します。

FMC または FTD デバイスの再イメージ化後にバックアップから復元する場合は、デバイスをリモート管理から削除する必要はありません。

ライセンスの問題の対処

Firepower アプライアンスを再イメージ化する前に、ライセンスの問題に対処してください。状況により、Cisco Smart Software Manager からの登録解除が必要になります。また場合によっては、新しいライセンスについてセールス担当者に問い合わせる必要があります。シナリオに応じて必要な操作を決定するには、「新規インストールの決定」を参照してください。

ライセンスの詳細については、次を参照してください。

- Cisco Firepower System Feature Licenses Guide
- Frequently Asked Questions (FAQ) about Firepower Licensing
- 設定ガイドのライセンスの章

アプライアンス アクセス

再イメージ化により、ほとんどの設定が工場出荷時の初期状態に戻ります。

アプライアンスに物理的にアクセスできない場合、再イメージ化プロセスによって管理ネットワークの設定を維持できます。これにより、再イメージ化した後、アプライアンスに接続して、初期設定を実行できます。ネットワーク設定を削除する場合は、アプライアンスに物理的にアクセスできる必要があります。Lights-Out 管理（LOM）を使用することはできません。

（注） 以前のメジャーバージョンに再イメージ化すると、ネットワーク設定が自動的に削除されます。このようなまれなケースでは、物理的アクセスが必要です。

デバイスに関して、ユーザの位置からのトラフィックがデバイスの管理インターフェイスにアクセスするためにデバイス自体を通過する必要がないことを確認してください。FMC 展開では、デバイスを経由せずに FMC 管理インターフェイスにアクセスできる必要もあります。

シスコとのデータの共有

一部の機能にシスコとのデータ共有が含まれます。

バージョン 6.2.3+ では、*Cisco Success Network* は、テクニカルサポートを提供するために不可欠な使用状況に関する情報と統計情報をシスコに送信します。初期設定中に、参加を承諾するか、辞退するかを尋ねられます。また、いつでもオプトインまたはオプトアウトできます。

バージョン 6.2.3+ では、Web 分析のトラッキングは、これに限定されませんが、ページでの操作、ブラウザのバージョン、製品のバージョン、ユーザの場所、FMC の管理 IP アドレスまたはホスト名を含む、個人を特定できない使用状況データをシスコに送信します。Web 分析トラッキングはデフォルトでオンになっていますただし、初期設定の完了後にいつでもオプトアウトできます。また、この機能を再度有効にする可能性があるメジャーアップグレード後は、もう一度オプトアウトする必要があります。

以前のメジャー バージョンへの Firepower 1000/2100 シリーズ デバイスの再イメージ化

Firepower 1000/2100 シリーズデバイスを以前のメジャーバージョンに戻す必要がある場合は、完全な再イメージ化を実行することをお勧めします。消去設定方式を使用すると、Firepower Threat Defense ソフトウェアに加えて、FXOS が復元しない場合があります。この場合、特にハイ アベイラビリティ展開では、障害が発生する可能性があります。

詳細については、Cisco FXOS トラブルシューティングガイド（Firepower Threat Defense を実行している Firepower 1000/2100 シリーズ向け）に記載されている再イメージ化の手順を参照してください。

バージョン 6.3.0 以降へのバージョン 5.x ハードウェアの再イメージ化

バージョン 6.3+ のインストールパッケージの名前が変更されていると、古い物理アプライアンス（FMC 750、1500、2000、3500、4000 のほか、7000/8000 シリーズ デバイスと AMP モデル）の再イメージ化に関する問題が発生します。現在バージョン 5.x を実行していて、バージョン 6.4.0 を新規にインストールする必要がある場合は、インストールパッケージをダウンロードした後、その名前を「古い」名前に変更します。『Cisco Firepower Release Notes, Version 6.3.0』の「Renamed Upgrade and Installation Packages」の情報を参照してください。

FMC（Defense Center）をバージョン 5.x からより新しいバージョンに再イメージ化した後、古いデバイスを管理することはできません。また、これらのデバイスを再イメージ化してから、FMC に再度追加する必要があります。シリーズ 2 デバイスは EOL であり、Firepower ソフトウェアの過去バージョン 5.4.0.x を実行できないことに注意してください。それらのデバイスを置き換える必要があります。

スマート ライセンスの登録解除

Firepower Threat Defense デバイスは、ローカル（Firepower Device Manager）またはリモート（Firepower Management Center）で管理されているかどうかに関係なく、Cisco Smart Licensing を使用します。ライセンス供与された機能を使用するには、Cisco Smart Software Manager（CSSM）で登録する必要があります。後で再イメージ化または管理の切り替えを行うことにした場合は、孤立した権限付与を発生させないように登録を解除する必要があります。これらが生じると再登録できない場合があります。

（注） FMC または FTD デバイスをバックアップから復元する必要がある場合は、再イメージ化の前に登録を解除しないでください。また、FMC からデバイスを削除しないでください。代わりに、バックアップを実行した後に行われたライセンス変更を元に戻します。復元が完了したら、ライセンスを再設定します。ライセンスの競合や孤立した権限付与に気付いた場合は、Cisco TAC にお問い合わせください。

登録を解除すると、仮想アカウントからアプライアンスが削除され、関連付けられたライセンスが解放されるため、ライセンスを再割り当てできるようになります。アプライアンスを登録解除すると、適用モードになります。アプライアンスの現在の設定とポリシーはそのまま機能しますが、変更を加えたり展開したりすることはできません。

次の操作を行う前に、CSSM から手動で登録解除します。

- FTD デバイスを管理する Firepower Management Center を再イメージ化する。
- FDM によってローカルで管理されている Firepower Threat Defense デバイスを再イメージ化する。
- Firepower Threat Defense デバイスを FDM から FMC 管理に切り替える。

FMC からデバイスを削除すると、CSSM から自動的に登録解除されます。これにより、次のことが可能になります。

- FMC によって管理されている Firepower Threat Defense デバイスを再イメージ化する。
- Firepower Threat Defense デバイスを FMC から FDM 管理に切り替える。

上記の 2 つのケースでは、FMC からデバイスを削除すると、デバイスが自動的に登録解除されます。FMC からデバイスを削除すれば、手動で登録解除する必要はありません。

ヒント NGIPS デバイスのクラシック ライセンスは、特定のマネージャ（ASDM/FMC）に関連付けられており、CSSM を使用して制御されません。クラシック デバイスの管理を切り替える場合、または NGIPS 展開から FTD 展開に移行する場合は、セールス担当者にお問い合わせください。

の登録解除 Firepower Management Center

バックアップから復元する予定がない限り、再イメージ化する前に、CSSM から Firepower Management Center の登録を解除してください。これは、管理対象の Firepower Threat Defense デバイスの登録も解除します。

FMCが高可用性に設定されている場合、ライセンスの変更が自動的に同期されます。他のFMCの登録を解除する必要はありません。

ステップ 1 Firepower Management Center にログインします。

ステップ 2 **[システム（System）] > [ライセンス（Licenses）] > [スマートライセンス（Smart Licenses）]**を選択します。

ステップ 3 [スマートライセンスのステータス（Smart License Status）] の横の停止記号アイコン をクリックします。

ステップ 4 警告を読み、登録解除することを確認します。

を使用した FTD デバイスの登録解除 FDM

再イメージ化するか、またはリモート（FMC）管理に切り替える前に、ローカルの管理対象 Firepower Threat Defense デバイスの登録を Cisco Smart Software Manager から解除します。

高可用性のために設定されているデバイスの場合は、その装置を登録解除するために、高可用性ペアにあるその他の装置にログインする必要があります。

ステップ 1 Firepower Device Manager にログインします。

ステップ 2 [デバイス（Device）] をクリックし、[スマートライセンス（Smart License）] のサマリーで [設定の表示（View Configuration）] をクリックします。

ステップ 3 歯車ドロップダウンリストから [デバイスの登録解除（Unregister Device）] を選択します。

ステップ 4 警告し、登録を解除することを確認します。

設置手順

リリース ノートとアップグレード ガイドにはインストール手順は含まれていません。代わりに、次のドキュメントのいずれかを参照してください。インストール パッケージは シスコ サポートおよびダウンロード サイト から入手できます。

Table 37: Firepower Management Center のインストール手順

FMC プラットフォーム	ガイド
FMC 1600、2600、4600	Cisco Firepower Management Center 1600, 2600, and 4600 Hardware Installation Guide：Restoring a Firepower Management Center to Factory Defaults
FMC 750、1500、3500 FMC 2000、4000	Cisco Firepower Management Center 750, 1500, 2000, 3500 and 4000 Getting Started Guide：Restoring a Firepower Management Center to Factory Defaults
FMCv	『Cisco Firepower Management Center Virtual 入門ガイド』

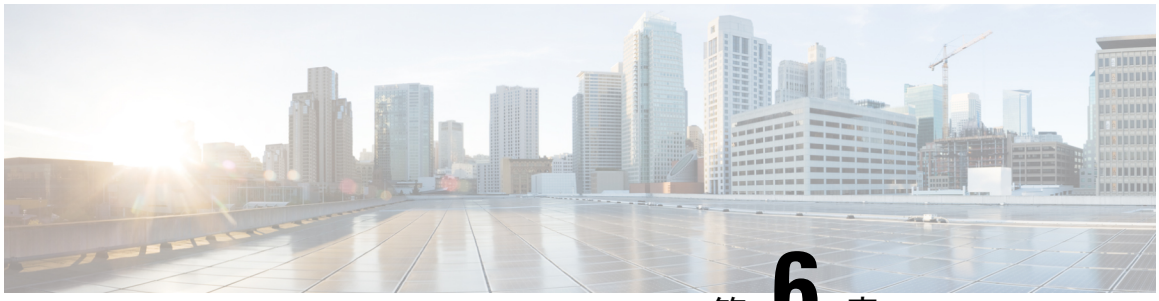
Table 38: Firepower Threat Defense のインストール手順

FTD プラットフォーム	ガイド
Firepower 1000/2100 シリーズ	Cisco ASA and Firepower Threat Defense Reimage Guide Cisco FXOS トラブルシューティングガイド（Firepower Threat Defense を実行している Firepower 1000/2100 シリーズ向け）
Firepower 4100/9300 シャーシ	Cisco Firepower 4100/9300 FXOS Configuration Guides：イメージ管理に関する章 Cisco Firepower 4100 スタートアップガイド Cisco Firepower 9300 Getting Started Guide
ASA 5500-X シリーズ	Cisco ASA and Firepower Threat Defense Reimage Guide
ISA 3000	Cisco ASA and Firepower Threat Defense Reimage Guide
FTDv: VMware	Cisco Firepower Threat Defense Virtual for VMware Getting Started Guide
FTDv: KVM	Cisco Firepower Threat Defense Virtual for KVM スタートアップガイド
FTDv：AWS	Cisco Firepower Threat Defense Virtual for the AWS Cloud スタートアップガイド
FTDv：Azure	Cisco Firepower Threat Defense Virtual for the Microsoft Azure Cloud Quick Start Guide

Table 39: FirePOWER 7000/8000 シリーズ、*NGIPSv* および *ASA FirePOWER* インストール手順

NGIPS プラットフォーム	ガイド
Firepower 7000 シリーズ	Cisco Firepower 7000 Series Getting Started Guide：*Restoring a Device to Factory Defaults*

NGIPS プラットフォーム	ガイド
Firepower 8000 シリーズ	Cisco Firepower 8000 Series Getting Started Guide：*Restoring a Device to Factory Defaults*
NGIPSv	Cisco Firepower NGIPSv Quick Start Guide for VMware
ASA FirePOWER	Cisco ASA and Firepower Threat Defense Reimage Guide ASDM Book 2: Cisco ASA Series Firewall ASDM Configuration Guide：Managing the ASA FirePOWER Module



第 6 章

資料

次のトピックでは、Firepower のドキュメントへのリンクを記載しています。

新規および更新されたドキュメント

次の Firepower ドキュメントが更新されたか、バージョン 6.4.0 で新たに利用可能になっています。更新されていない、またはこのリリースで新しく使用可能になったドキュメントへのリンクについては、「ドキュメントロードマップ, on page 83」を参照してください。

Firepower コンフィギュレーション ガイドとオンライン ヘルプ

- Firepower Management Center Configuration Guide, Version 6.4 とオンラインヘルプ
- Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager, Version 6.4.0 とオンラインヘルプ
- Cisco ASA with FirePOWER Services Local Management Configuration Guide, Version 6.4 とオンラインヘルプ
- Cisco Firepower Threat Defense Command Reference

FXOS コンフィギュレーション ガイドとリリース ノート

- Cisco Firepower 4100/9300 FXOS Firepower Chassis Manager Configuration Guide, 2.6(1)
- Cisco Firepower 4100/9300 FXOS CLI Configuration Guide, 2.6(1)
- Cisco Firepower 4100/9300 FXOS Command Reference
- Cisco Firepower 4100/9300 FXOS Release Notes, 2.6(1)

強化ガイド

- Cisco Firepower Management Center Hardening Guide, Version 6.4（新規）

- Cisco Firepower Threat Defense Hardening Guide, Version 6.4（新規）
- Cisco Firepower 4100/9300 FXOS Hardening Guide （新規）

アップグレード ガイド

- Cisco Firepower Management Center Upgrade Guide
- Cisco Firepower 4100/9300 Upgrade Guide
- Cisco ASA Upgrade Guide

ハードウェア設置ガイド

- Cisco Firepower Management Center 1600, 2600, and 4600 Hardware Installation Guide （新規）
- Cisco Firepower 1010 ハードウェア設置ガイド （新規）
- Cisco Firepower 1100 シリーズ ハードウェア設置ガイド （新規）
- Cisco Firepower 4115、4125、および 4145 ハードウェア設置ガイド （新規）
- Cisco Firepower 9300 ハードウェア設置ガイド

スタートアップ ガイド

- Cisco Firepower Management Center 1600, 2600, and 4600 Getting Started Guide （新規）
- 『Cisco Firepower Management Center Virtual 入門ガイド』
- Cisco Firepower Threat Defense Virtual for VMware Getting Started Guide
- Cisco Firepower Threat Defense Virtual for KVM スタートアップガイド
- Cisco Firepower 1010 スタートアップガイド （新規）
- Cisco Firepower 1100 シリーズ スタートアップガイド （新規）
- Cisco Firepower 4100 スタートアップガイド （新規）
- Cisco Firepower 9300 Getting Started Guide （新規）

API および統合ガイド

- Firepower Management Center REST API Quick Start Guide, Version 6.4.0
- Cisco Firepower Threat Defense REST API ガイド （Cisco Firepower Threat Defense REST API Guide）
- Cisco Firepower App for Splunk User Guide（新規）
- Firepower および Cisco Threat Response の統合ガイド （新規）

互換性ガイド

- Cisco Firepower Compatibility Guide
- Cisco ASA の互換性
- Cisco Firepower 4100/9300 FXOS の互換性

ライセンス

- Cisco Firepower システム機能ライセンス
- 『Frequently Asked Questions (FAQ) about Firepower Licensing』

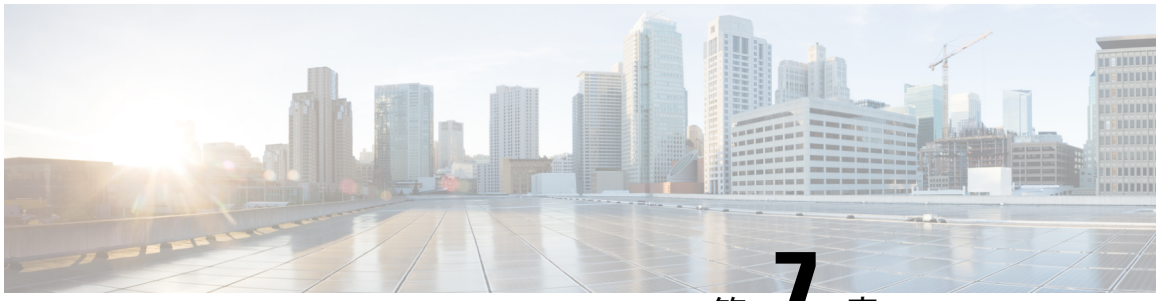
トラブルシューティングおよび設定の例

- Cisco Firepower Threat Defense Syslog メッセージ
- Deploy a Cluster for Firepower Threat Defense for Scalability and High Availability
- Cisco FXOS トラブルシューティングガイド（Firepower Threat Defense を実行している Firepower 1000/2100 シリーズ向け）

ドキュメントロードマップ

ドキュメントロードマップでは、現在使用可能なドキュメントおよび従来のドキュメントへのリンクを示します。

- Cisco Firepower ドキュメント一覧
- Cisco ASA シリーズ ドキュメント一覧
- Cisco FXOS ドキュメント一覧



第 7 章

解決済みの問題

便宜上、これらのリリースノートには、このバージョンの解決済みのバグが記載されています。

このリストは1回自動生成され、その後は更新されません。特定の解決済みの問題がシステムでどのように分類または更新されたかとその時期によっては、リリースノートに記載されない場合があります。Cisco バグ検索ツール を「信頼できる情報源」と考えてください。

- 解決済みの問題の検索 （85 ページ）
- 新しいビルドで解決済みの問題 （85 ページ）
- バージョン 6.4.0 で解決済みの問題, on page 86

解決済みの問題の検索

サポート契約がある場合は、Cisco Bug Search Tool を使用して Firepower 製品の最新の解決済みバグリストを取得することができます。これらの一般的なクエリには、バージョン6.4.0を実行している Firepower 製品の解決済みのバグが表示されます。

- Firepower Management Center
- Firepower Management Center Virtual
- ASA with FirePOWER サービス
- NGIPSv

検索では、特定の Firepower プラットフォームとバージョンに影響するバグに絞り込むことができます。バグ ID ごとに検索したり、特定のキーワードを検索することもできます。

新しいビルドで解決済みの問題

シスコは、更新版ビルドを適宜リリースしています。ほとんどの場合、各プラットフォームの最新のビルド番号のみが、シスコ サポートおよびダウンロード サイト で入手可能です。最新のビルドを使用することを強くお勧めします。以前のビルドをダウンロードした場合は使用しないでください。

同じ Firepower バージョンに対して、1 つのビルドから別のビルドにアップグレードすることはできません。新しいビルドで問題が解決する場合は、代わりに、アップグレードまたはホットフィックスが機能するかどうかを確認します。それ以外の場合は、Cisco TAC にご連絡ください。公的に利用可能な Firepower のホットフィックスへのクイックリンクについては、Cisco Firepower ホットフィックス リリース ノートを参照してください。

この表を使用して、プラットフォームで新しい バージョン 6.4.0 ビルドが使用可能かどうかを確認します。

表 *40* : バージョン *6.4.0* の新しいビルド

新しいビルド	[解放（Released）]	パッケージ	プラットフォーム	解決済み
113	2020 年 3 月 3 日	アップグレード 再イメージ化	FMC/FMCv	CSCvr95287：Cisco Firepower Management Center LDAP 認証バイパスの脆弱性 以前のビルドを実行している場合は、最新バージョンの 6.4.0.x パッチを適用します。パッチを適用できない場合、または適用しない場合は、ホットフィックス T またはホットフィックス U を適用します。

バージョン 6.4.0 で解決済みの問題

***Table 41:* バージョン *6.4.0* で解決済みの問題**

不具合 ID	タイトル
CSCuz85967	新たに追加された管理インターフェイスに「管理専用」設定がない
CSCvc56570	ポリシーの展開に失敗すると、瞬間的なトラフィックのドロップと確立された接続の障害が発生する
CSCve24102	GUI で、DHCP プールごとに最大 256 個のアドレスを設定できる必要がある
CSCvf83504	SYS_FW_INTERFACE_NAME_LIST と SYS_FW_NON_INLINE_INTERFACE_NAME_LIST がサブインターフェイスを認識しない
CSCvg11366	File::Temp が MOJO、Syncd.pl などによって使用された場合に File::Temp への呼び出し後にクリーンアップが発生することを確認する
CSCvg29468	一般的なマイクロエンジン障害が誤検出される可能性の減少
CSCvg74603	eStreamer アーカイブ イベントが diskmanager によって正しくプルーニングされない

不具合 ID	タイトル
CSCvh75756	重複するプリプロセッサキーワード：ssl（Duplicate preprocessor keyword: ssl）
CSCvh93045	異なる ip の同じデバイス（同じ NS）を登録しようとすると FMC がデータベース自体をクリーンにする
CSCvi01404	ssl インスペクションポリシーが原因で ECDSA 署名付き証明書を使用しているサイトで障害が発生する場合がある
CSCvi16039	Firepower Management Center が SNMPv3 パスワードのさまざまな文字を受け付けない
CSCvi16074	SNMPv3 パスワードの入力時に Firepower Management Center がエラーを誤認する
CSCvi25965	Sybase のアップグレード：SRU のインストール後、ゾンビの非アクティブプロセスによってポリシーの展開が失敗する
CSCvi28409	FTP プロトコルを使用する一部のファイルについて、キャプチャされたファイルのダウンロードが FMC 上で機能していない
CSCvi32569	mysql-server.err ログに過剰なロギングが発生すると FTD に大きなログ ファイルが生成される
CSCvi34123	拡張機能：リストの先頭に _ が含まれている DNS リストを追加できない
CSCvi49522	アプリケーション タグ、検索、またはカテゴリフィルタを使用した POST または PUT ルールが ACP ルール GUI にアクセスできない
CSCvi63474	6.2.2 へのアップグレード後に ASDM を介した SFR モジュールのシステム ポリシーの編集ができない
CSCvi71622	スタンバイ FTD での DATAPATH のトレースバック
CSCvi81022	isco Firepower Threat Defense SSL/TLS ポリシー バイパスの脆弱性
CSCvi89202	アップグレードの再開時にディスク領域のチェックが省略される
CSCvi93680	初回起動の失敗をユーザに警告する必要がある
CSCvj08826	FMC：ibdata1 ファイルのサイズが大きくなっていく（300 GB から 2.4 TB 以上と表示）
CSCvj13960	SNMP が有効なときの高 CPU の表示
CSCvj27949	FMC が夏時間オフセットを正しく使用しない
CSCvj39253	アーカイブの検査オプションが有効になっている場合に、ファイルポリシーによって xlsm がブロックされる

不具合 ID	タイトル
CSCvj50451	FMC でネットワーク オブジェクト 0.0.0.0/32 を追加できない
CSCvj57511	ASDM：レイヤ ポリシーの無効にされたルール状態が、変更をコミットした後に継承するように戻される
CSCvj70886	API エクスプローラは 4096 ビット証明書をサポートする必要がある
CSCvj81798	10 の送信元/10 の宛先 N/W、10 の送信元/10 の宛先ポート、10 のサブインターフェイスを持つアクセスルールをゾーンに展開した場合の OOM
CSCvk14242	FTD の sfstunnel プロセスにすでに削除されている大規模なクラウド db ファイルが保持されている
CSCvk20209	FMC の外部認証が ISE を介した RADIUS オブジェクトに対して機能しない
CSCvk20381	新しい ASAv Azure、KVM、および VMWare の導入でトレースバック ループが確認される
CSCvk23653	ip プールがグループ ポリシーから参照除外される前に否定される
CSCvk26612	「デフォルトのキーリング証明書が無効です。理由：期限切れ（default Keyring's certificate is invalid, reason: expired）」 ヘルスアラート
CSCvk29558	FTD VPN：S2S オプション [証明書 OU フィールドでトンネルを決定（Certificate OU field to determine the tunnel）] を無効にしても効果がない
CSCvk33503	Flexconfig ethertype コマンドが解析されず、展開が失敗する
CSCvk34648	高スループットの IPsec VPN トラフィックによりデータのキー再生成で Firepower 2100 トンネルがフラップする
CSCvk43854	Cisco Firepower Threat Defense 検出エンジン ポリシーのバイパスの脆弱性
CSCvk45941	展開失敗の場合にロギングの向上が必要：VPN ポリシーの不正な文字
CSCvk55766	デバイスをプラットフォーム設定ポリシーに割り当てようとすると、デバイスのリストがランダムにポリシーから消える
CSCvk56984	tomcat の複数の脆弱性
CSCvm04150	最初のブート スクリプトが 2 回実行された後、すべてのヘルス モジュールがヘルス モジュール テーブルで削除済みとしてマークされた
CSCvm05768	Https サーバ証明書の必須フィールド
CSCvm41983	[ポリシーの展開（Policy Deployment）] ページの最後の [展開（deploy）] をクリックすると [展開（Deploy）] ウィンドウに戻る

不具合 ID	タイトル
CSCvm48451	4100 および 9300 で侵入イベントパフォーマンスのグラフが空白になる
CSCvm50153	FMC：手動入力の ip 範囲を使用した VPN スプリットトンネル拡張 ACL による展開の失敗
CSCvm54029	6.4.0：無効な IPV6 RA_VPN セッションが、ADI によって処理され、user_ip_map ファイルに記録される
CSCvm54062	アクティブからスタンバイへのファイルのコピー後にアクションキュータスクがスタックした
CSCvm60056	カスタムの DNS セキュリティ インテリジェンス フィードをダウンロードした後、webGUI タイムスタンプが更新されない
CSCvm62846	TID の復元 | 設定のみのバックアップに失敗しました
CSCvm63199	新たに設定されたインターフェイスが、capture コマンドに表示されない
CSCvm68648	Firepower ソフトウェアの CVE-2016-8858（OpenSSH）に必要な更新
CSCvm68999	KP での展開の失敗：検出の再設定に失敗しました
CSCvm70274	tcp プロキシ：データパスでの ASA のトレースバック
CSCvm72980	FDM：-FTD が SSL ハンドシェイクで完全なチェーンを送信しない
CSCvm78028	RIP 設定で「トラフィック方向」と「ルート タイプのフィルタ」が同じ 2 つのフィルタを追加できない
CSCvm84459	不正な call_home_ca ファイルによってスマート ライセンスの登録が阻止される
CSCvm85453	FMC HA：フェールオーバー後に新しいアクティブ FMC から SNMP トラップが送信されない
CSCvm86008	ポリシーの展開：デルタ設定が実行コンフィギュレーションにコピーされないため LINA 設定が変更されないままになる
CSCvm88294	パーティション強制ドレインが発生していないためディスク使用率が高くなる
CSCvm90290	Firepower ソフトウェアの ImageMagick パッケージが古くなっている可能性がある
CSCvm92210	ユーザ定義のポート番号が含まれている場合に anyconnect グループ Url を FTD に展開できない
CSCvm96642	DSA 証明書は現時点ではアクティブ認証ではサポートされていない

不具合 ID	タイトル
CSCvn00312	エラーや警告を表示しようとするときに展開がスタックする
CSCvn12373	FMC HA の rna_attribute 重複キーでポリシーの展開が失敗する
CSCvn13880	マルチキャスト ルーティングが有効な場合にタイマー イベントが原因でユニットがスレッド PIM IPv4 または IGMP IPv4 でトレースバックする
CSCvn14276	「arp permit-nonconnected」は FlexConfig ではサポートされない
CSCvn14511	FMC は SNMP ユーザ認証設定で中カッコ（「{」など）を受け付けない
CSCvn19609	Flex オブジェクト エディタで予期しない改行が発生している可能性があり、その結果ポリシーの展開に失敗する
CSCvn23926	OSPFv3 インターフェイス認証 SPI はデバイスのインターフェイスごとに一意である必要がある
CSCvn24920	スタンバイデバイスが 9.12 イメージにアップグレードされている場合に、VPN セッションがスタンバイユニットに複製されない
CSCvn29101	Cisco Firepower Management Center MySQL Unix Millennium 2028 Date の脆弱性
CSCvn31882	展開モードが「常時」に設定されている場合、Flex 設定ステートメントが重複する
CSCvn34246	AC ポリシー エディタのロードに時間がかかりすぎるためロード インジケータが必要になる
CSCvn36022	指定されたオブジェクトを使用するすべての ACP/デバイスに関する情報を提供する FMC オブジェクト管理
CSCvn38101	スタンバイ アドレスとの nat オーバーラップで ui がチェックされない
CSCvn39960	FMC でハブアンドスポーク VPN に対して保護されたネットワークを設定しても lina CLI には効果がない
CSCvn44222	6.3.0-79：HA のアップグレードまたはセカンダリの RAVPN diskfiles の欠落により展開が失敗する
CSCvn46358	VPN ステータス メッセージの送信による lina msglyr インフラの過負荷
CSCvn47504	6.x では VMware のバルーン ドライバを無効にする必要がある
CSCvn48907	Cisco Firepower Management Center のクロスサイト スクリプティングの永続的な脆弱性
CSCvn57284	FTD でサポートされていない EC カーブ x25519

不具合 ID	タイトル
CSCvn58125	レポートのダッシュボードで空のフィルタリングが生成される
CSCvn67084	マネージャとして FMC を追加する際に、ローカルマネージャの削除に失敗する
CSCvn71592	FMC の再起動後、Snort によって生成された侵入イベントが FMC に送信されず、webGUI に表示される
CSCvn75713	FMC 上の CVE Nmap のバージョン
CSCvn75722	FMC 上の CVE Nmap のバージョン
CSCvn75729	FMC 上の CVE Nmap のバージョン
CSCvn81898	接続イベントに関する syslog アラートが設定されている場合に、syslog メッセージにデバイス名が含まれていない
CSCvn82823	インターフェイス nameif で大文字と小文字が区別されている場合に FTD HA インターフェイス モニタリングの変更が有効にならない
CSCvn82891	Httpd の複数の脆弱性
CSCvn85761	FMC ではオブジェクト名に特殊文字を使用した秘密キーの作成はできない
CSCvn91775	FMC GUI において [オブジェクト（Objects）] > [VPN] > [証明書マップ（Cert Maps）] で数値名を使用した証明書マップの作成を許可してはならない
CSCvo04444	Ikev2 トンネルの作成に失敗する
CSCvo06383	データベースがダウンしているため、バージョン 6.0.1 から 6.1.0 への FMC のアップグレードが失敗する
CSCvo19433	Flexconfig ドキュメントで、影響の範囲を誤った設定から指定している
CSCvo19666	28 コア インスタンスで達成しているパフォーマンスが予測より 20% 低い
CSCvo20847	同期時に xlate の割り当ての破損が原因でアクティブ FTP がクラスタを介して失敗する
CSCvo23366	適応型プロファイリングの設定ファイルが破損しているため展開に失敗した
CSCvo24145	大きな firewall_rule_cache テーブルによる ids_event_alerter の高メモリ使用率
CSCvo24624	6.3.0 から 6.4.0-1299 へのアップグレードの失敗

不具合 ID	タイトル
CSCvo29989	Cisco FirePower Threat Defense に関する情報漏えいの脆弱性
CSCvo31831	ベース ポリシーを削除しても子ポリシーの EO は削除されない
CSCvo33348	非標準ポートの Mysql トラフィックが正しく分類されない
CSCvo33851	ngfw.properties が空の場合に ngfwManager が開始されない
CSCvo35129	epol_wait イベント処理の修正が必要
CSCvo35283	GRE を介した HTTP/POP3 トラフィックに対するユニットの追加または削除のためにクラスタユニットがクラッシュする
CSCvo38051	ctm_ipsec_pfkey_parse_msg における ctm_ipsec_pfkey.c:602 での segfault
CSCvo42884	6.3 へのアップグレード後に、FTD でサイト間 VPN を変更できない
CSCvo45209	FTD - クラスタ：クラスタに新しいユニットを追加するとトラフィックのドロップが発生する場合がある
CSCvo45675	FMC アップグレード プロセスでは、アップグレード後に無効になる設定を確認する必要がある
CSCvo50168	監査ログの設定の失敗によりシステム設定が編集できなくなる
CSCvo56836	スケール：500 以上のデバイスを使用すると UMS によって UI がハングする（特に展開時）
CSCvo59683	EOAttributes テーブル内の古いオブジェクトの数が多いと、高 CPU 使用率/バックアップ障害が発生する
CSCvo60862	アクセス コントロール ポリシー編集時の内部エラー
CSCvo62060	FMC が大量のデバイスを管理しているときにテレメトリが送信されない
CSCvo63168	Sybase 接続に障害が発生した場合の temp_id リーク
CSCvo63232	UIMP が、子ドメインに存在するレルムからユーザを更新しない
CSCvo65521	TID ディレクトリが正しくないためバックアップの復元に失敗する
CSCvo66546	SFDataCorrelator プロセスで Firepower が頻繁にトレースバックおよび再起動する
CSCvo66575	ISE 2.6、ISE 2.4p6、および ISE 2.3p6 との pxGrid 接続が切断される
CSCvo68448	5585 プラットフォームで ASA モジュールをリロードした後、ASA が SFR モジュールを「応答なし」として報告する

不具合 ID	タイトル
CSCvo70545	Cisco Firepower Detection Engine の RTF/RAR マルウェアおよびファイルポリシーバイパスの脆弱性
CSCvo70866	任意の値の SGT タグを持つすべてのクライアント パケットに対するサーバ パケットで SGT タグがタグなしと表示される
CSCvo72179	SMB ではリモート ストレージ設定でドット（.）を使ったバージョン文字列の設定を許可する必要がある
CSCvo72232	ブラウザの ERR_SSL_BAD_RECORD_MAC_ALERT または SSL_ERROR_BAD_MAC_ALERT
CSCvo72238	FTD クラスタがドメインで管理され、サブドメインの AC ポリシーが割り当てられると、FMC バックアップが失敗する
CSCvo72659	既存の相関ルールに対する編集が有効にならない
CSCvo74397	ENH：「コマンドは無視されました。設定中です...（Command Ignored, configuration in progress...）」にプロセス情報を追加
CSCvo74745	多数の連続 URL ルックアップ（30M 超）生成後のクラウド エージェントのコア化
CSCvo74765	Lina 応答が 10,000 ミリ秒後にタイムアウトするために FDM ポリシーの展開に失敗する
CSCvo74833	追跡されていないファイルが原因で、Firepower デバイスの管理対象外ディスク容量が多くなる
CSCvo76866	2100 でのトレースバック：ウォッチドッグ
CSCvo77796	グローバルなスナップショットの作成における IntrusionPolicy の手順が遅いために、導入が遅くなる
CSCvo80725	「エラー：ip_multicast_ctl によるチャネルの取得に失敗（ERROR: ip_multicast_ctl failed to get channel）」により vFTD 6.4 が OSPF 隣接関係を確立できない
CSCvo81073	NGFWHA EO がないため [Device Management] ページをロードできないか、FMC をアップグレードできない
CSCvo83574	インライン セットをタップ モードから切り替えるとデバイスが不良状態になる
CSCvo86038	flow-offloaded フローでの同時 FIN が接続の失効につながる
CSCvo88188	App-ID 条件を持つ SSL ルールが復号機能を制限する可能性がある

不具合 ID	タイトル
CSCvo88306	重複するルールがあると NAT ルールが誤った順序で適用される可能性がある
CSCvo89224	展開用のデバイス リストの取得で 10 分後に FMC がタイムアウトになる
CSCvo90550	Firepower の推奨事項では GID 3 の IPS ルールが有効にならない
CSCvo90805	Cisco Firepower Management Center RSS のクロスサイト スクリプティングの脆弱性
CSCvo94486	セキュリティ インテリジェンスの処理中に Snort プロセスが終了する
CSCvp01542	証明書の場所が原因で、FMC 6.3 マルチテナンシー/ドメイン LDAPS ユーザ/グループのダウンロードに失敗する
CSCvp04134	9.12.1 へのアップグレード時に HTTP CLI Exec でトレースバックする
CSCvp06526	短い CPU アフィニティに一致するように sfhassd スレッド CPU アフィニティを管理する
CSCvp12239	KP：パッチ 6.3.0.3-58 へのアップグレード後にアクティブになるセカンダリ/スタンバイデバイス
CSCvp23579	[ネットワークファイルトラジェクトリ（Network File Trajectory）] ページのロードに毎回 90 秒かかる
CSCvp24787	（snort）HTTPS 経由時にファイルが検出されなくなる（SSL 再署名）
CSCvp25570	グループポリシー属性と FQDN が同じウィザード フローで編集されている場合、RAVPN 接続プロファイルを作成できない
CSCvp25581	FMC-HA user_group_map エントリがスプリットブレインで消去されている
CSCvp25583	FMC GUI を介して BGP に OSPF を再配布すると FTD によって自動的にメトリックが 0 に設定される
CSCvp25782	メタデータキャッシュのプルーニング中の EventHandler コア
CSCvp30447	侵入ポリシーでグローバルルールしきい値が無効になっている場合に syslog アラートがサーバに送信されない
CSCvp33052	処理されていないリソースが一時的に使用できないという問題により Firepower 8000 インターフェイスがフラップする場合がある
CSCvp35359	明示的な UPN と暗黙的な UPN が一致しないと FMC-ISE 統合が機能しない
CSCvp37779	FTD のトラブルシューティング ファイルからの show tech が不完全である

不具合 ID	タイトル
CSCvp39970	/var/opt/CSCOpx/MDC/tomcat/log/stdout.logs によって過剰なログメッセージが書き込まれ、ディスクがいっぱいになる場合がある
CSCvp43474	REST API クエリ /api/fmc_config/v1/domain/UUID/devices/devicerecords が失敗する
CSCvp43536	アップグレードした FMC デバイスで、正常に展開された後も FXOS デバイスがダーティとして表示される
CSCvp45149	プライマリシステムをアクティブとして戻すときのトレースバック
CSCvp46173	サブドメイン内のインターフェイスグループまたはインターフェイスゾーンの変更によってグローバルドメインが上書きされる
CSCvp48453	[DOC] バックアップからバージョン 6.x+ Firepower 7000/8000 デバイスを復元しても、管理 IP がリセットされない
CSCvp54261	SFR モジュール/7000/8000 デバイスの監査 syslog で UDP ではなく TCP が syslog 通信に使用される
CSCvp55941	ファイル復帰ブロックがランダムにスローされて、SMB 共有からのファイルへのアクセスに関する問題が発生する
CSCvp58028	nfm_exceptiond の natd スレッドで約 90 ～ 100% の CPU 時間が使用される
CSCvp58310	pxgrid 機能の統合、接続のハング、curl のハングの問題
CSCvp59960	リテラル（ユーザまたはシスコが作成したもの）を含むネットワーク グループでネットワーク検出が機能しない
CSCvp66222	Cisco Firepower Detection Engine の RTF/RAR マルウェアおよびファイルポリシーバイパスの脆弱性
CSCvp66488	Firepower が Snort ルールに基づかずに予期しない SNMP トラップを送信する
CSCvp67392	リバース パス チェックにより ASA/FTD HA データ インターフェイスのハートビートがドロップされる
CSCvp70833	ASA/FTD：同じサービスの NAT ルールがエラー「エラー：NAT がポートを予約できません（ERROR: NAT unable to reserve ports）」を 2 回表示する
CSCvp72244	CVE-2019-11815 の Cisco 8000 シリーズの評価
CSCvp72601	FMC UI：VPN ハブアンドスポークトポロジのロードに時間がかかる
CSCvp72770	vFTD が Azure プラットフォームで実行されている場合に、FMC から vFTD にコピーされた BCDB ファイルが切り捨てられる

不具合 ID	タイトル
CSCvp73555	ネットワーク検出の展開後に rna_networks が空になる
CSCvp75594	FTD を実行している ASA5500-X で 6.4 にアップグレードした後に展開に失敗する
CSCvp78197	ポリシーの展開による ospf ネイバーの削除および追加
CSCvp79157	多数のデバイスへの同時展開の実行時に FTD/Firepower ポリシーの展開が失敗する
CSCvp81967	管理対象デバイスが 500 以上ある場合に FMC のデバイス管理ページのロードが遅くなる
CSCvp82945	NAT ポリシーの適用がエラーの重複で失敗する
CSCvp83687	Firepower：ネットワークファイルのトラジェクトリグラフがロードされない
CSCvp87623	CAC（HTTPS クライアント証明書）の使用時に更新をアップロードすると「更新要求エンティティが大きすぎます（update request entity too large）」というエラーが発生する
CSCvp95663	IPS イベント（「ブロックした場合（Would have blocked）」）の InlineResult でメタデータが欠落する
CSCvp96934	重複する NAT を含むエラー メッセージがクリアされ実行可能であることを確認する
CSCvp97061	URL フィルタリングですべての URL が未分類として表示される
CSCvp97799	SSL ポリシーのエクスポート時に openSSL コールで CC モードにして 6.5.0-1148 にアップグレードした後、ポリシーの展開に失敗する
CSCvp98066	CD のリセット時にフラグ [parseFailoverReqIssued] をクリアしないと、ノードを結合できない
CSCvp99327	スマートサテライトにスマートライセンスを登録しようとした後に FMC UI が応答しなくなる
CSCvp99930	プライマリがアクティブの間に sftunnel の例外で展開が失敗する
CSCvq00675	Linux カーネル sas_expander.c が競合状態で任意のコードを実行...
CSCvq06790	シリーズ 3 デバイスで Snort プロセスがメモリ破損でコアをダンプする
CSCvq07573	6.4 へのアップグレード後、FMC のグローバルな事前展開フェーズに時間がかかる

不具合 ID	タイトル
CSCvq07914	FMC 6.4.0 - ポリシー展開の失敗 - domains.conf のドメインエントリが重複している
CSCvq08684	特殊文字および符号化によるポリシー展開の失敗
CSCvq08767	snort 検証での展開の失敗 - 「SMTP：SMTP mime mempool を割り当てることができませんでした（SMTP: Could not allocate SMTP mime mempool）」
CSCvq09093	VPN 事前展開の検証がデバイスごとに約 20 秒かかる
CSCvq09209	ポリシーの展開が snort 検証失敗のエラーで失敗した（memcap に指定された値が正しくない）
CSCvq12070	2 つ以上の同時 ASDM セッションを確立できない
CSCvq14586	データベースの更新が失敗した場合に 600_schema/100_update_database.sh はエラーを返す必要がある
CSCvq16123	Firepower ダイナミック Snort ルールが、Snort のリロードが関係する展開後に無効になる
CSCvq19525	TCP_SACK の sfims の評価
CSCvq24258	大規模なアプライアンスで Mojo サーバのワーカー数が増加する
CSCvq24494	FP2100 - FP2100 プラットフォームでリング/CPU コアをオーバーサブスクライブするフローによって動作中フローの中断が発生する
CSCvq25912	6.4.0 では相関ルールアラートが動作しない
CSCvq29969	再生成されていない場合でも、Firepower 推奨ルール数が変更される
CSCvq32250	HA アクティブ/スタンバイペアで誤ってプログラムされた BGP ネクストホップ
CSCvq32678	アップグレードの異常によりポリシーの展開が失敗する：NGFW_UPGRADE がマップファイルで見つかりません（NGFW_UPGRADE is missing in map file）
CSCvq32681	FTD のアップグレード時に複数のインターフェイスペアのインラインセットに対して Fail to Wire 設定が無効になる
CSCvq34224	マネージャをアップグレードすると、Firepower プライマリ検出エンジンプロセスが終了する
CSCvq36042	ハートビートが失われてリロードが発生する
CSCvq37902	TID が URL としてのソースの追加に失敗する - フラットファイル

不具合 ID	タイトル
CSCvq39083	SSL ポリシーが有効になっている場合にブラックリストに登録された URL への HTTPS 接続がセキュリティ インテリジェンスでドロップされない
CSCvq39828	6.4.0 へのアップグレード後、packet_log テーブルへの挿入時に SFDC がクラッシュする
CSCvq41936	新しいユーザを追加した後に FMC UI で SNMP を無効にしてから再度有効にする必要がある
CSCvq43453	サブドメインの変数セットで使用されている場合、ポートオブジェクトにオーバーライドを追加できない
CSCvq44594	「不明な HPQ ルールキー（Unknown HPQ rule key）」というメッセージがログに大量に出力される
CSCvq45000	NAT が設定されている場合に FP 8000 センサーへのポリシーの展開が失敗する
CSCvq46443	Cisco Firepower Management Center に蓄積されたクロスサイトクリプティングの脆弱性
CSCvq46804	大文字の RADIUS を含む AD ユーザ名でログインできない
CSCvq46918	アップグレード後に SNMPv3 ユーザが削除される
CSCvq50314	失敗した SSH ログイン試行が syslog 経由でエクスポートされない
CSCvq53902	Cisco Firepower Management Center のクロスサイト スクリプティングの複数の脆弱性
CSCvq53915	Cisco Firepower Management Center のクロスサイト スクリプティングの複数の脆弱性
CSCvq54242	SSL ポリシーでの警告「送信元ネットワークで、空のグループがあります（There is an empty group in the source networks）」
CSCvq56138	パスワードの文字列にスペースが含まれている場合に LDAP ユーザの FMC GUI へのユーザログインが失敗する
CSCvq56257	キャッシュされたマルウェアの処置が想定どおりに期限切れにならないことがある
CSCvq56462	ファイルポリシーが一部のマルウェアドキュメント（.doc）および Adobe Flash（.swf）ファイルを検査しない
CSCvq57710	マネージャをアップグレードすると、Firepower プライマリ検出エンジン プロセスが終了することがある

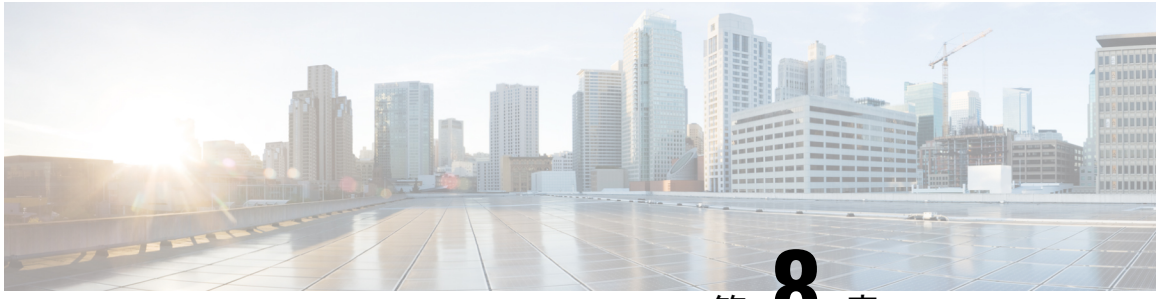
不具合 ID	タイトル
CSCvq59702	ハンドシェイクメッセージの喪失後にデバイスからの接続イベントが停止する
CSCvq61651	FMC での URL DB ダウンロード失敗アラート：FMC/FDM で新しい URL DB の更新が有効にならない
CSCvq65092	デバイス関連の REST API コールが低速になる
CSCvq66217	FMT | MTU 値が許容範囲内にない
CSCvq67271	子アクセスポリシーの ID によって特定ルールを取得すると、「404：見つかりませんでした（404: Not Found）」ステータスが返される
CSCvq70485	「securityzones」REST API が低速になる
CSCvq71217	CSCvn30118 の後、mysql-server.err によりローテーションが失敗して、ディスク使用率が高くなる
CSCvq76533	MC4000 の F_RNA_EVENT_LIMIT は 2000 万である必要がある
CSCvq81516	FMC で 12 時～午後 1 時（UTC）の間の VPN イベントが表示されない
CSCvq83019	ACPolicy に多数のアプリケーション フィルタ オブジェクトが使用されている場合に、ポリシー展開タスクの挿入処理に時間がかかる
CSCvq83168	FMC ではサーバアドレスの後にインターフェイスを使用できないため、管理 VRF を使用した DNS ルックアップを実行できない
CSCvq86553	6.4.0 への更新後、トラフィックが期待される ACP ルールと一致しない
CSCvq88644	tcp-proxy でのトレースバック
CSCvq89794	FDM：ユーザダウンロードが LDAPS で機能しない
CSCvq94729	デルタ CLI の LINA ONLY セクションでのエラー時に展開のロールバックによってトラフィックの瞬間的なドロップが発生する
CSCvq97346	UI で NAT ルールを移動し、展開すると、FDM バックエンドから NAT ルールが削除される
CSCvr00892	外部データベースアクセスで where 句が機能しない
CSCvr04954	スタックユニット：NDPolicy obj err をロードできない別のドメインでのアップグレード後に展開が失敗する
CSCvr06515	Access-control-config ヒットカウンタが増加しない
CSCvr07421	セキュリティゾーン内にインターフェイスが 400 以上あると、deployDB の不適切な形成により、ポリシーの展開が失敗する

不具合 ID	タイトル
CSCvr10777	Ikev2 デーモンでの ASA トレースバック
CSCvr11395	スケジュール済みの展開時にデバイスグループから展開された一部のデバイスのみ
CSCvr13762	FMC 上の NGFWHA に EO UUID がない
CSCvr17735	SI 更新時の SFDataCorrelator で CPU の使用率が高くなる
CSCvr20893	ポリシーの展開後に ids_event_proce プロセスで HA ペアの FTD がクラッシュする
CSCvr23858	domain_snapshot_timeout（20m）により、FMC から FTD へのポリシーの展開が失敗する（または時間がかかる）
CSCvr28532	Snort 検証の失敗が原因でポリシーの展開が失敗する
CSCvr29978	ルールを変更してすぐに保存すると、設定が削除されることがある
CSCvr30694	FMC：FMC が HA 同期の失敗を検出する
CSCvr35956	ServerKeyExchange と ClientKeyExchange の組み合わせに失敗した場合のダブルフリーのブロックによって lina トレースバックが発生する
CSCvr39556	libclamav.so のセグメンテーション違反（SFDataCorrelator のコンテキスト内）
CSCvr45752	FTD HA：いずれかのユニットが正常でない場合に展開が失敗する（FDM）
CSCvr51955	eStreamer は、ACK を長時間受信しない場合に接続を終了する必要がある
CSCvr51998	BGP 経由でデフォルトルートを学習後、ASA スタティックルートが ASP テーブルから消える
CSCvr52109	複数のデバイスへの展開後、FTD が正しいアクセスコントロールルールに一致しないことがある
CSCvr52410	新しい FTD の登録後、後続のポリシーの展開が失敗する
CSCvr53058	TCP の代行受信と AC ポリシーのモニタを設定すると、AC ポリシーのルックアップが SYN+ACK パケットに対して実行される
CSCvr54250	レルムが設定されていない場合でも user_ip_map ファイルの数が多い
CSCvr55400	スレッド名「cli_xml_server」で FTD/LINA がトレースバックし、リロードされる
CSCvr59927	SRU インストールが進行中の場合、展開が失敗する

不具合 ID	タイトル
CSCvr60111	設定がスタンバイから削除され、アクティブ時に展開が失敗する
CSCvr61241	ファイルアップロード機能を実装する情報システムでは、ファイルサイズを検証する必要がある
CSCvr61492	REST API コールに関連し、デバイスのロードが低速になる
CSCvr63851	外部認証経由で NGIPS への SSH 接続が成功しても、すぐに終了する
CSCvr66798	DNS アプリケーションディテクタが DNS トラフィックを検出できないことがある
CSCvr72665	FMC の 6.3/6.4 への アップグレードでは、既存の廃止済み flexconfig を削除しない必要がある
CSCvr73115	ポリシーインポート後の初期 FTD の展開によって未使用オブジェクトが発生し、ポリシーサイズが膨張する
CSCvr78166	「実行コンフィギュレーションの取得に失敗しました」という理由で、展開が FTD 上で失敗した
CSCvr79008	不正なユーザ名の正規化を実行しているすべてのディレクトリサーバを FMC が非効率的にクエリするため、セッション処理が遅延する
CSCvr86016	v3.sds.cisco.com への FMC 接続がプロキシをバイパスしている
CSCvr86213	CD は、クラスタノードリリースの Lina の状態の Cluster-Msg-Delivery-Confirmation を無視する必要がある
CSCvr88123	マルチ展開により、侵入イベントが突然ドロップする
CSCvr90768	FTD：低速リンク経由の展開が失敗することがある
CSCvr92327	ASA/FTD がスレッド名「PTHREAD-1533」でトレースバックおよびリロードすることがある
CSCvr92617	SecurityIntelligenceEoConvertor の NPE によって、Lucene のインデックスの作成が失敗する
CSCvr96527	新しいルールの追加中に FMC の既存ルールがエラーになる
CSCvs00023	CLISH CLI からの「shutdown」コマンドでポートマネージャがクラッシュする
CSCvs04067	Catalina へのアップグレード後、Mac 上の Chrome で FMC デバイスにアクセスできない
CSCvs10114	ネストされたネットワーク オブジェクト グループが NAP ルールに対して展開されていないため、導入が失敗する

不具合 ID	タイトル
CSCvs10443	6.5 CloudEvent コードが、6.4 コードが理解しない方法で設定ファイルを書き込む
CSCvs10526	FTD での SSE 試行のスロットル
CSCvs12288	SSL ポリシーが有効になっている状態で debug_policy_all が設定されていると Snort が予期せず終了する
CSCvs15972	SSL ポリシーが有効な場合にネットワークパフォーマンスが低下する
CSCvs19968	スタックし、HA FTD ポリシー展開エラーが発生しないようにコンソールを修正する
CSCvs22503	「ポリシーイベントの逆シリアル化に失敗しました（Failed to deserialize policy event）」の後に eStreamer が繰り返し終了する
CSCvs23750	6.4.0.4 FMC WebUI でシリーズ 3 スタックを作成できない
CSCvs25607	制約事項に netmap_num を追加するとパフォーマンスが低下する
CSCvs28094	FP8000 センサーのユーザ設定を編集するとエラー 403 が表示される
CSCvs29405	CMD フィールドがフレーム内に存在しない場合、Snort がトラフィックをタグ付きとして処理する
CSCvs32023	出力最適化処理をオフにする
CSCvs34854	FMC がアクセスリスト CLI の差分の後ろに参照インターフェイス CLI の差分を生成する
CSCvs37013	octeon_init がスタックし、HA FTD ポリシー展開エラーを発生させないようにする
CSCvs47201	デバイスレコードに対して GET ALL を実行すると、「isPartOfContainer」が返される。HA とクラスタの一部であるデバイスでは偽
CSCvs52227	実際にデバッグを有効にしなくても、syslog にファイアウォールエンジンのデバッグログが生成される
CSCvs55937	neo4j エラーが原因で FDM の展開が失敗する
CSCvs59056	Float-Conn が有効になっている場合、ASA/FTD トンネルスタティックルートが準最適なルックアップによって無視される
CSCvs61392	Firepower デバイスで、ポリシーが正常に展開された後、ハードウェアルールが更新されない
CSCvs74452	マルウェアシードファイルのロード中に SFDatacorrelator と Snort がコアを繰り返し処理する

不具合 ID	タイトル
CSCvs77334	「別のユニットのインスペクションエンジンが Snort とディスクの障害により失敗しました（Inspection engine in other unit has failed due to snort and disk failure）」というエラーにより FTD がフェールオーバーする
CSCvs81763	vFTD が VLAN タグ付きトラフィックを渡すことができない（トランクモード）
CSCvs91389	FTD トレースバック Lina プロセス
CSCvs91869	FPR-1000 シリーズのランダム番号生成エラー
CSCvt10097	セキュリティゾーンにインターフェイスがある場合でも、SF_Egress_Zone/SF_Ingress_Zone に関するログが空になる
CSCvt23643	データを復旧するための、VPN フェールオーバーリカバリに約 30 秒かかる



第 8 章

既知の問題

便宜上、これらのリリースノートには、このバージョンの既知のバグが記載されています。

このリストは1回自動生成され、その後は更新されません。特定の既知の問題がシステムでどのように分類または更新されたかとその時期によっては、リリースノートに記載されない場合があります。Cisco バグ検索ツール を「信頼できる情報源」と考えてください。

- 既知の問題の検索 （105 ページ）
- バージョン 6.4.0 既知の問題, on page 105

既知の問題の検索

サポート契約がある場合は、Cisco Bug Search Tool を使用して Firepower 製品の最新のオープンバグリストを取得することができます。これらの一般的なクエリには、バージョン6.4.0を実行している Firepower 製品の未解決のバグが表示されます。

- Firepower Management Center
- Firepower Management Center Virtual
- ASA with FirePOWER サービス
- NGIPSv

検索では、特定の Firepower プラットフォームとバージョンに影響するバグに絞り込むことができます。バグ ID ごとに検索したり、特定のキーワードを検索することもできます。

バージョン 6.4.0 既知の問題

Table 42: バージョン *6.4.0* の既知の問題

不具合 ID	タイトル
CSCvo00852	FTDv ESXi 12 コアおよび FTDv KVM 12 コア プラットフォームで Lina CPU が低くトラフィックが失われる

不具合 ID	タイトル
CSCvo03589	アプリケーション エージェントのハートビートが、MI のシナリオで失われる可能性がある
CSCvo40478	FMC ダッシュボードに FMC の最新の製品更新として誤った値が表示される
CSCvo80725	「エラー：ip_multicast_ctl によるチャネルの取得に失敗（ERROR: ip_multicast_ctl failed to get channel）」により vFTD 6.4 が OSPF 隣接関係を確立できない
CSCvp06568	6.4 FMC によって管理されている 6.3 FTD の syslog で NAP ポリシー/SSL ポリシー名が不明
CSCvp14864	ポート 3 とともにポート 4 の poe が有効になっている場合、3504 wlc が到達不能になる
CSCvp19669	FDM イベントにユーザが正しく表示されない
CSCvp21403	検証：データ プレーン：管理アクセスが RA-VPN ポート コリジョンを処理しない
CSCvp23703	FTD で最初のブート スクリプト S97compress-client-resources が無応答で失敗した
CSCvp25570	グループポリシー属性と FQDN が同じウィザード フローで編集されている場合、RAVPN 接続プロファイルを作成できない
CSCvp29817	TempID を RealID に変換するときにログイン履歴の更新に失敗する（ID ごとに 1 個のログ、履歴が失われる）
CSCvp30194	ASA SFR：IPS を使用して ACP をインポートしようとすると「SFO インポート中のエラー：コンテナをロードできません（Error importing SFO: Unable to load container）」が表示される
CSCvp33797	FMC 上でセッションのあるユーザが、ユーザ情報を AD からダウンロードした後に正常に更新されない
CSCvp34148	シスコワイヤレス LAN コントローラのサービス拒否（DoS）攻撃に対する脆弱性
CSCvp37229	ポリシー レイヤの「マイ チェンジ（My Changes）」レイヤから有効にした場合、一部のプロセッサが有効にならない
CSCvp45752	カスタム アプリケーションをサブドメインに追加した場合、古いバージョンの登録済みデバイスで snort が再起動しない
CSCvp47260	日本語版でトラブルシューティング ファイルの生成が停止する

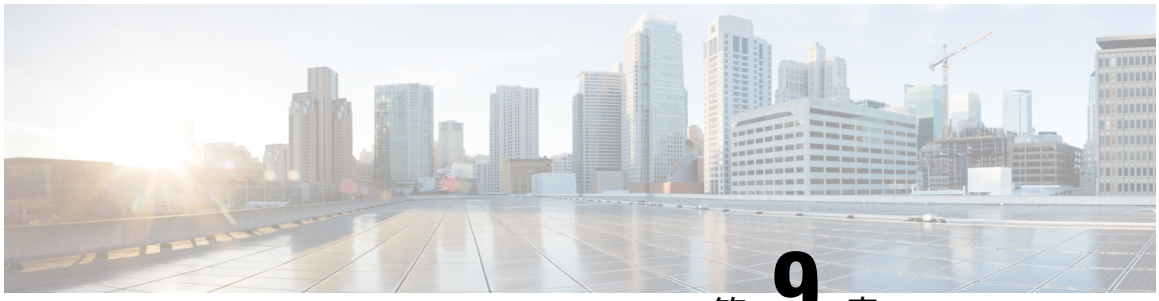
不具合 ID	タイトル
CSCvp47535	新しく追加したアプリケーション プロトコルを [ホスト（Hosts）] に表示できない
CSCvp48523	変更されたユーザがアクセス ポリシーに正しく反映されない
CSCvp48525	[タスクの詳細（Task details）] でスケジュールしたタスクを編集できない
CSCvp48534	侵入ルールにカテゴリを追加できない
CSCvp48545	日本語名のアラートを作成できない
CSCvp48565	VPN トラブルシューティング ログのセットアップに異常に長い時間がかかる
CSCvp48583	[IPv6 DAD] チェックボックスがデフォルトでオンになっている
CSCvp53608	WLC が特定のホストからの HTTP/HTTPS/SSH に応答しない
CSCvp56916	S2S VPN ウィザードに、事前設定された使用可能な証明書がないことが示される
CSCvp56951	FDM/FTDvirtual が「ignore-ipsec-keyusage」 flexconfig オブジェクトをサポート/展開できない
CSCvp57096	メッセージ フィールドに NULL エントリがある ids_event_msg_map テーブルが原因で 6.4.0 へのアップグレードが失敗する場合がある
CSCvp59960	リテラル（ユーザまたはシスコが作成したもの）を含むネットワーク グループでネットワーク検出が機能しない
CSCvp67132	emWeb での WLC のクラッシュ
CSCvq33956	展開プロセス（AQS サブグループ）のメモリ割り当てを最適化して大規模なポリシー展開を可能にする
CSCvq78471	BVI とその DHCP プールを同時に削除するとポリシーの展開が失敗する
CSCvq89604	Cisco_Firepower_Mgmt_Center_Patch_Uninstaller-6.4.0.3-29.sh.REL.tar の実行が失敗する
CSCvr08243	DHCP トラフィックがホスト上で確立されない
CSCvr09620	展開後であっても、プラットフォーム設定ポリシーが展開に利用できる
CSCvr19755	FP2100 ASA：タイムアウトが原因のダウングレードの失敗後のポートチャネルとインターフェイスの設定
CSCvr31594	FLTOOL で FMC のライセンス予約が動作していない

不具合 ID	タイトル
CSCvr35854	Apache HTTP サーバの URL 正規化のサービス拒否（DoS）攻撃攻撃に対する脆弱性
CSCvr35855	Apache HTTP サーバの mod_http2 Use-After-Free のサービス拒否（DoS）攻撃に対する脆弱性
CSCvr35856	Apache HTTP サーバの mod_auth_digest 競合状態のアクセス制御バイパス
CSCvr52736	HTTP サーバフロー深度を若干変更した場合の大幅な劣化
CSCvr57468	RunQuery は Java 開発キット 13 との互換性がない
CSCvr69664	アップグレード後、デバイスビューに誤った管理 IP が表示される
CSCvr93454	サテライトとの統合を設定するときの「インターネット接続が必要です（Internet connection is required）」が誤解を招く
CSCvr94406	HTTP または HTTPS のインテリジェンスソース v6.2.3 ～ v6.4.0.4 で TAXII フィードをダウンロードできない
CSCvs05066	Snort ファイルのメモリプールの破損によりパフォーマンスが低下し、プロセスが失敗する
CSCvs37065	/ngfw/var/sf/fwcfg/interface_info.conf ファイルにデータがないため、Snort がクラッシュする
CSCvs50931	SRU の後でポリシーの展開が失敗する
CSCvs56923	SQL クライアントが外部データベースアクセスを使用して FMC にクエリを実行できない
CSCvs61881	FTD 上の AnyConnect の証明書マッピングが機能しなくなった
CSCvs74667	FMC を 6.4.0.4 にアップグレード後、ホスト情報（ネットワークマップ、ホストなど）がなくなっている
CSCvs81697	外部認証オブジェクトリストの最初のオブジェクトのみを使用して FTD ユーザが認証できる
CSCvs82829	AnyConnect 設定がサイト間 VPN トンネルに追加されるとコールが失敗する
CSCvt02487	送信元または宛先でセキュリティグループタグ SGT を使用しているブロックルールが、ブロックせずに許可する
CSCvt03557	GUI 上に設定された時間/タイムゾーンが仮想 Firepower Management Center 上で矛盾している

不具合 ID	タイトル
CSCvt04377	過剰なロギングが原因でsyslogメッセージファイルがディスク容量を枯渇させる
CSCvt06666	6.3.0.4 から 6.4 へのアップグレードが失敗した後で SFR httpsd プロセスがダウンする
CSCvt16642	FMC がリモートの syslog サーバに対して一部の監査メッセージを送信していない
CSCvt16723	ngfw-onbox ログのログローテーションが想定しているログサイズで実行されていない
CSCvt18051	dets ファイルが破損している場合、RabbitMQ がクラッシュし続ける
CSCvt20235	すべての FTW インターフェイスが不定期にリンクフラップする
CSCvt21986	インスタンス間の Snort と Lina のコアの割り当てに一貫性がない
CSCvt26530	「Snort の障害により他のユニットのインスペクションエンジンに障害が発生した（Inspection engine in other unit has failed due to snort failure）」ことが原因で FTD がフェールオーバーした
CSCvt30212	FDM：CSSM イベント通知が停止しない
CSCvt34894	D 状態になる Snort によりブロックが枯渇する
CSCvt35233	DAQ モジュール process_snort_verdict 判定ブラックリストからの過剰なロギング
CSCvt35366	Lua ディテクタの無効な LUA（null）による過剰なロギング
CSCvt37745	アクティブからスタンバイへセカンダリが復帰する間のトレースバック
CSCvt37913	有用性：FMC HA の EO の権限に違反すると以前のプライマリのままになる
CSCvt39977	PSNG_TCP_PORTSCAN [122:1:1] ルールアラートの場合の無効なパケットデータ
CSCvt42428	FTD：ゼロ除算エラーによりポリシー展開が失敗する
CSCvt42955	SID 26932 誤検出 が NTP ではなく QUIC トラフィックでトリガーされる
CSCvt49028	重複する LDAP ユーザアカウントが存在する場合、VPN ACP と一致するユーザ ID が正しくない
CSCvt50263	FMC が WM モデルデバイスから VPN トラブルシューティングログを取得できない

不具合 ID	タイトル
CSCvt52607	SSL HW モードのフローテーブルメモリの使用率を下げて Snort が D 状態になる確率を低減する
CSCvt56923	FMC の手動による証明書の登録が、組織の件名フィールドの「&」（アンパサンド）が原因で失敗する
CSCvt59770	FTD：SCEP を介した証明書の取得の失敗により停止する
CSCvt60297	Geo ブロックルールを有効にすると、お客様に不適切なアクセスコントロールルールの処理が表示される
CSCvt61229	ルールコメントの特殊文字のために展開を失敗させる必要はない
CSCvt62052	FMC DBCheck.pl の致命的なエラー：[vpn_client_country_code SMALLINT(5) UNSIGNED NOT NULL DEFAULT "0"]
CSCvt62147	プロセス名 LINA で ASA がトレースバックし、リロードする
CSCvt63407	FTD 6.4.0.7 を実行している FP 2000 がプロセス名 LINA でトレースバックし、リロードする
CSCvt64696	AAA RADIUS サーバの接続障害
CSCvt66136	CC モードを使用した 6.4.0 から 6.4.0.9 へのアップロードが原因で httpsd.conf に正しくない設定が含まれる
CSCvt66875	AppId が UltraSurf にトンネリングされた IP ではなく、プロキシ IP をキャッシュする
CSCvt67282	FMC：正常性の通知が run_hm のダウンが原因でスタックする
CSCvt67832	ロックの競合が原因で、Lina スレッドで FTD がトレースバックし、リロードする
CSCvt68131	スレッド「IKEv2 Mgd Timer Thread」で FTD がトレースバックし、リロードする
CSCvt70866	sfipproxy がセカンダリ FMC のリスナーのバインドに失敗することがある
CSCvt72683	FP 8130 での NAT ポリシー展開後、NAT ポリシーの設定が表示されない
CSCvt74194	unified2 レコード取得中のエラー：ファイルの破損
CSCvt75600	アップグレード中に 800_post/021_reinstall_sru.sh で SRU のインストールが失敗する可能性がある
CSCvt75611	FMC のアップグレード中に、展開が実行中か、または開始時にハングしたかのチェックが行われない

不具合 ID	タイトル
CSCvt75677	インターフェイスで論理名を TRUE または FALSE に設定すると、FMC UI からのすべてのスタティックルートが消去される
CSCvt80104	Memcached ソフトウェアを CVE-2018-1000115 に対応するようにアップグレードする必要がある
CSCvt80126	CLI の「show asp table socket 18421590 det」で ASA がトレースバックし、リロードする
CSCvt80138	OpenSSH ソフトウェアを CVE-2018-15473 に対応するようにアップグレードする必要がある
CSCvt80172	CVE-2017-11610 に対処するには、スーパーバイザソフトウェアをアップグレードする必要がある
CSCvt81127	ホットフィックスのアンインストールスクリプトが FMC からエクスポータパッケージを削除しない



第 9 章

支援が必要な場合

Firepower をお選びいただき、ありがとうございます。

オンラインリソース

シスコは、ドキュメント、ソフトウェア、ツールのダウンロードのほか、バグを照会したり、サービス リクエストをオープンしたりするためのオンライン リソースを提供しています。これらのリソースは、Firepower ソフトウェアをインストールして設定したり、技術的問題を解決したりするために使用してください。

- シスコ サポートおよびダウンロード サイト：https://www.cisco.com/c/en/us/support/index.html
- Cisco Bug Search Tool：https://tools.cisco.com/bugsearch/
- シスコ通知サービス：https://www.cisco.com/cisco/support/notifications.html

シスコ サポートおよびダウンロード サイトの大部分のツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。

シスコへのお問い合わせ

上記のオンライン リソースを使用して問題を解決できない場合は、Cisco TAC にお問い合わせください。

- Cisco TAC の電子メール アドレス：tac@cisco.com
- Cisco TAC の電話番号（北米）：1.408.526.7209 または 1.800.553.2447
- Cisco TAC の連絡先（世界全域）：Cisco Worldwide Support の連絡先