Cisco Firepower バージョン 6.7.0 リリースノート

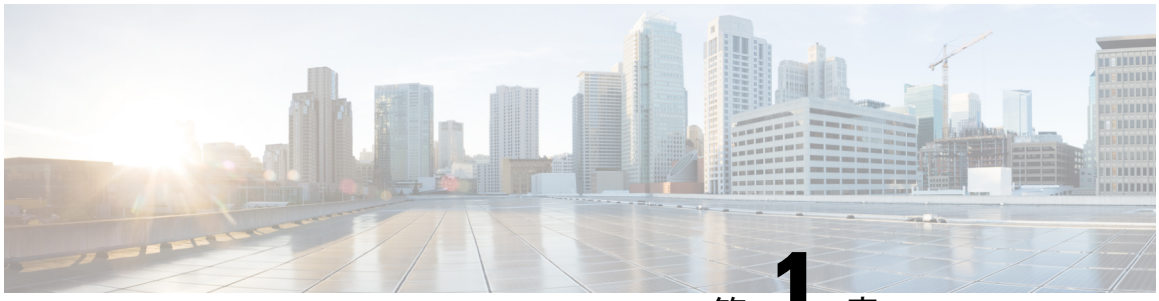
初版：2020 年 11 月 2 日

最終更新：2020 年 12 月 15 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

Version6.7.0 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、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、このドキュメントをお読みください。

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 （94 ページ）
- インストール手順 （110 ページ）

ハイライト

Firepower Device Manager 用 Snort 3.0

Snort 3.0 は、Firepower Device Manager（FDM）で管理する場合の新しいバージョン 6.7.0 以上の Firepower Threat Defense（FTD）展開用のデフォルト検査エンジンになりました。

古いリリースからバージョン 6.7.0 にアップグレードした場合、アクティブな検査エンジンは Snort 2.0 のままですが、切り替えることができます。この機能と FDM を使用した FTD のその他の新機能の詳細については、「FDM バージョン 6.7.0 の新機能 （47 ページ）」を参照してください。

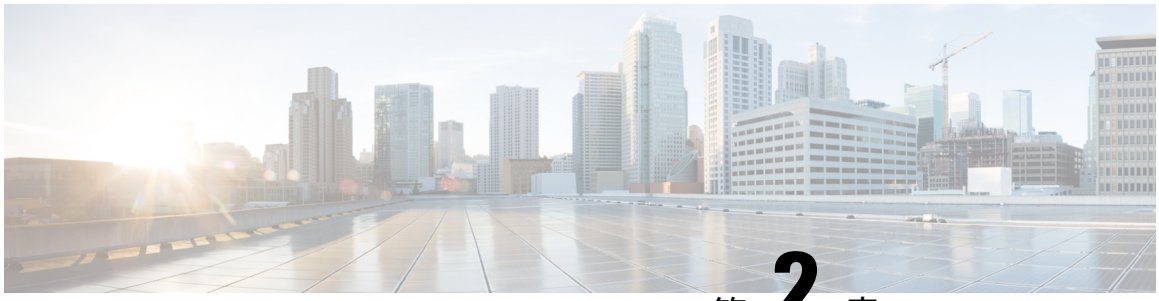
Snort 3.0 の詳細については、https://snort.org/snort3 を参照してください。

リリース日

このバージョンで使用可能なすべてのプラットフォームのリストについては、互換性（3 ページ）を参照してください。

表 *1 :* バージョン *6.7.0* の日付

バージョン	ビルド（Build）	日付	プラットフォーム
6.7.0	65	2020 年 11 月 2 日	すべて



第 2 章

互換性

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。

この Firepower バージョンの互換性情報については、次を参照してください。

Firepower Management Centerについて

Firepower Management Center（FMC）は、Firepower 展開の一元的な管理コンソールを提供するフォールトトレラントな専用ネットワークアプライアンスです。Firepower Management Center Virtual （FMCv）は、完全なファイアウォール管理機能を仮想化環境にもたらします。

Firepower Management Center

このリリースでは、次の FMC プラットフォームがサポートされています。

- FMC 1600、2600、4600
- FMC 1000、2500、4500

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

このリリースでは、次の FMCv の実装がサポートされています。

- Amazon Web Services（AWS）の FMCv

- Microsoft Azure の FMCv
- Google Cloud Platform（GCP）の FMCv ***NEW***
- Oracle Cloud Infrastructure（OCI）の FMCv ***NEW***
- カーネルベース仮想マシン（KVM）の FMCv
- VMware vSphere/VMware ESXi 6.0、6.5、または 6.7 の FMCv および FMCv 300

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

Cisco Firepower デバイスは、ネットワークトラフィックをモニタし、定義された一連のセキュリティルールに基づいて特定のトラフィックを許可するかブロックするかを決定します。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。一部のデバイスはいずれかのソフトウェアを実行できますが、両方を同時に実行することはできません。

次の表に、このリリースでサポートされているデバイスプラットフォームと、（個別にアップグレード可能な）OS/ハイパーバイザ要件を示します（）。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。

（注） これらは、このリリースでサポートされているデバイスです。古いデバイスが EOL に達していて、アップグレードできなくなった場合でも、数バージョンの範囲内であれば、より新しい FMC を使用してそのデバイスを管理できます。 同様に、より新しいバージョンの ASDM では、より古いバージョンの ASA FirePOWER モジュールを管理できます。下位互換性を含む、サポート対象の管理方法については、「マネージャとデバイスの互換性 （6 ページ）」を参照してください。

Firepower Threat Defense デバイス

これらの FTD デバイスは、このリリースでサポートされています。

表 2 : バージョン 6.7.x の FTD

FTD プラットフォーム	OS/ハイパーバイザ	詳細情報
Firepower 1010、1120、1140、1150 Firepower 2110、2120、2130、2140	—	—

FTD プラットフォーム	OS/ハイパーバイザ	詳細情報
Firepower 4110、4120、4140、4150 Firepower 4112、4115、4125、4145 Firepower 9300：SM-24、SM-36、SM-44 モジュール Firepower 9300：SM-40、SM-48、SM-56 モジュール	FXOS 2.9.1.131 以降のビルド	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 FXOS Release Notes, 2.9(1)』を参照してください。
ASA 5508-X、5516-X ISA 3000	—	FTD 展開では、これらのデバイスの OS を個別にアップグレードすることはありませんが、最新の ROMMON イメージがあることを確認する必要があります。Cisco ASA and Firepower Threat Defense Reimage Guide
Firepower Threat Defense Virtual（FTDv）	次のいずれかです。 • AWS：Amazon Web Services • Azure：Microsoft Azure • GCP：Google Cloud Platform **新規** • OCI：Oracle Cloud Infrastructure **新規** • KVM：カーネルベースの仮想マシン • VMware vSphere/VMware ESXi 6.0、6.5、または 6.7	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。

NGIPS/ASA FirePOWER デバイス

これらの NGIPS/ASA FirePOWER デバイスは、このリリースでサポートされています。

表 *3 :* バージョン *6.7.x* の *NGIPS/ASA FirePOWER*

NGIPS プラットフォーム	OS/ハイパーバイザ	詳細情報
ASA 5508-X、5516-X ISA 3000	ASA 9.5(2) ～ 9.15(x)	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。操作の順序については、『Cisco ASA Upgrade Guide』を参照してください。 また、最新の ROMMON イメージがあることも確認してください。Cisco ASA and Firepower Threat Defense Reimage Guide
NGIPSv	VMware vSphere/VMware ESXi 6.0、6.5、または 6.7	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。

マネージャとデバイスの互換性

Firepower Management Center

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。新しいFMCは、いくつかのメジャーバージョンまでの古いデバイスを管理できます。ただし、FMC よりも新しいバージョンのデバイスをアップグレードすることはできません。つまり、FMCは管理対象デバイスと同じバージョンまたは新しいバージョンを実行する必要があります。

このリリースの場合：

- バージョン 6.7.x の FMC は、バージョン 6.3.0 ～ 6.7.x のデバイスを管理できます。
- バージョン 6.7.x デバイスにはバージョン 6.7.x FMC が必要です。

（注） バージョン 6.7.x デバイスを管理するバージョン 6.7.x FMC の場合、FMC はデバイスと同じまたはそれ以降のメンテナンス（3 桁）リリースを実行している必要があることに注意してください。たとえば、バージョン 6.7.1 の FMC では、バージョン 6.7.0 のデバイスを管理できますが、バージョン 6.7.2 のデバイスは管理できません。

Firepower Device Manager と Cisco Defense Orchestrator

FMC の代替として、Firepower Threat Defense デバイスは FDM および CDO の管理をサポートします。

- Firepower Device Manager（FDM）は、単一の FTD デバイスを管理できます。

  FDM では、小規模または中規模ネットワークで最も一般的に使用されるソフトウェアの基本機能を設定できます。

- Cisco Defense Orchestrator（CDO）はクラウドベースで、複数の FTD デバイスを管理できます。

  CDO を使用すると、FMC を使用せずに展開全体で一貫したセキュリティポリシーを確立して維持できます。一部の構成では引き続き FDM が必要ですが、CDO を使用すると、複数の FTD デバイスで一貫したセキュリティポリシーを確立して維持できます。

すべての FTD デバイスは、FDM ローカル管理と同時に CDO をサポートします。FDM は FTD に組み込まれており、CDO はクラウドベースの製品であるため、このタイプの展開にはマネージャとデバイスの互換性という概念はありません。

Adaptive Security Device Manager

ASA with FirePOWER Services は、Firepower NGIPS ソフトウェアを個別のアプリケーションとして実行する ASA ファイアウォールです。Cisco Adaptive Security Device Manager（ASDM）を使用して両方のアプリケーションを管理できます。

ASA、ASDM、および ASA FirePOWER のバージョンには広範な互換性がありますが、ASDM の新しいバージョンでは、古い ASA デバイス上の ASA FirePOWER モジュールを管理できない場合があります。詳細については、Cisco ASA の互換性を参照してください。

このリリースの場合：

- バージョン 7.15.1 ASDM は、バージョン 6.7.x 以前の ASA FirePOWER モジュールを管理できます。
- バージョン 6.7.x ASA FirePOWER module には、バージョン 7.15.1 ASDM が必要です。

Web ブラウザの互換性

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 MacOS および Microsoft Windows で動作する、次の一般的なブラウザの最新バージョンでテストされています。

- Google Chrome
- Mozilla Firefox
- Microsoft Edge（Windows のみ）

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。

（注） Apple Safari を使用した広範なテストを実施していません。また、FMC ウォークスルーを使用した Microsoft Edge の広範なテストも実施していません。ただし、Cisco TAC 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。

ブラウザの設定と拡張

ブラウザに関係なく、JavaScript、Cookie、および TLS v1.2 が有効なままになっていることを確認する必要があります。Microsoft Edge を使用している場合は、IE モードを有効にしないでください。

一部のブラウザ拡張機能では、PKI オブジェクトの証明書やキーなどのフィールドに値を保存できないことに注意してください。これらの拡張機能には Grammarly や Whatfix Editor などがありますが、それに限りません。この問題は、これらの拡張機能によってフィールドに文字（HTML など）が挿入され、システムが無効と見なすために発生します。Firepower アプライアンスにログインしている間は、これらの拡張機能を無効にすることをお勧めします。

セキュア通信

Firepower Web インターフェイスに初めてログインすると、システムは自己署名デジタル証明書を使用して Web 通信を保護します。ブラウザに信頼されていない機関に関する警告が表示されますが、信頼ストアに証明書を追加することもできます。これにより Firepower Web インターフェイスを継続できるようになりますが、自己署名証明書を、世界的に知られている、または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。

自己署名証明書の置き換えを開始する手順は、次のとおりです。

- FMC：**[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。

- FDM：**[デバイス（Device）]**、**[システム設定（System Settings）]** > **[管理アクセス（Management Access）]** リンク、**[管理 Web サーバ（Management Web Server）]** タブの順にクリックします。

手順について詳しくは、オンラインヘルプまたはご使用の Firepower 製品の設定ガイドを参照してください。

（注） 自己署名証明書を置き換えない場合は、次の手順を実行します。

- Google Chrome は、画像、CSS、JavaScript などの静的コンテンツを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。
- Mozilla Firefox は、ブラウザの更新時に自己署名証明書を信頼しなくなる場合があります。この場合は Firefox を更新できますが、一部の設定が失われることに注意してください。Mozilla の Firefox 更新サポートページを参照してください 。

Firepower で監視されるネットワークからのブラウジング

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。

画面解像度の要件

表 *4 : Firepower* ユーザ インターフェイスの画面解像度の要件

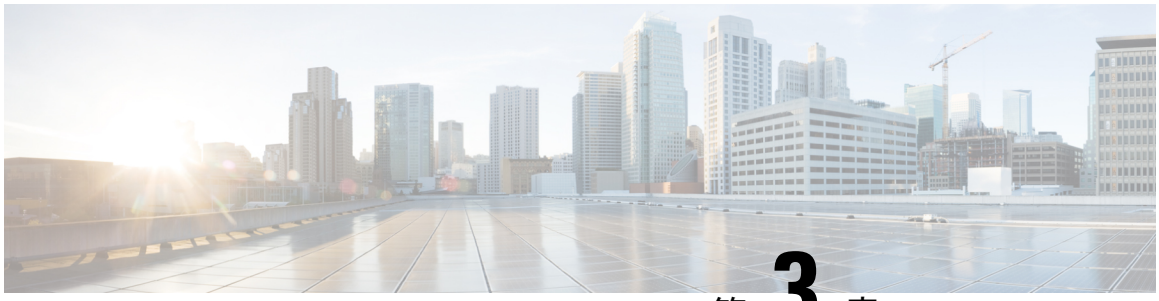
インターフェイス	解像度
Firepower Management Center	1280 X 720
Firepower Device Manager	1024 X 768
を管理している ASDM ASA FirePOWER module	1024 X 768
Firepower Chassis Manager 向け Firepower 4100/9300 シャーシ	1024 X 768

その他の互換性関連のリソース

次の表に、リリースノートとその他の互換性情報へのリンクを示します。ドキュメントの完全なロードマップについては、ドキュメント ロードマップ（115 ページ）を参照してください。

表 *5:* その他の互換性関連のリソース

説明	リソース
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

メジャーリリースは、Firepowerソフトウェアの新機能、機能、および拡張機能を提供します。メジャーバージョンには、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、動作の変更などが含まれることがあります。

廃止された機能は、バージョンをスキップするときにアップグレードの問題を引き起こす可能性が最も高いため、リリースノートには廃止された機能の履歴情報が記載されています。新機能の履歴情報については、スキップするバージョンのリリースノートを参照してください。

Firepower Management Center 展開に関する機能

以下のトピックでは、Version6.7.0 FMC 展開に関する新機能と廃止された機能について説明します。

FMC バージョン 6.7.0 の新機能

これらの Firepower 機能はバージョン 6.7.0 の FMC 展開で導入されました。

表 *6 :* バージョン *6.7.0* の新機能：*FMC* の展開

機能	説明
ハードウェアと仮想ハードウェア	
Oracle Cloud Infrastructure（OCI）仮想導入	Oracle Cloud Infrastructure に FMCv と FTDv を導入しました。

機能	説明
Google Cloud Platform（GCP）仮想導入	Google Cloud Platform に FMCv と FTDv を導入しました。
VMware 向け FMCv でのハイアベイラビリティのサポート	VMware 向け FMCv は、ハイアベイラビリティをサポートするようになりました。 ハードウェアモデルと同様に、FMCv HA を設定します。2 つの同じ FMCv ライセンスが必要です（FMCv300 を 2 つなど）。たとえば、FMCv10 HA ペアで 10 個の FTD デバイスを管理するには、2 個の FMCv10 権限と 10 個の FTD 権限が必要です。FMCv HA に違反すると、「追加」権限が解放されます（これで、スタンドアロンの FMCv10 は 2 つになります）。管理対象クラシック（NGIPS）デバイスの場合、FMCv 権限は必要ありません。 サポートされるプラットフォーム：VMWare で実行される 10、25、および 300 デバイス向けの FMCv のみ（2 デバイス向けの FMCv はサポートされません）
AWS 向け FTDv の自動スケールの改善	バージョン 6.7.0 には、AWS 向け FTDv の次の自動スケールの改善が含まれています。 • カスタム指標パブリッシャ。新しい Lambda 関数は、自動スケールグループ内のすべての FTDv インスタンスのメモリ消費量について FMC を毎秒ポーリングし、その値を CloudWatch メトリックにパブリッシュします。 • メモリ消費に基づく新しいスケーリングポリシーを使用できます。 • FMC への SSH およびセキュアトンネル用の FTDv プライベート IP 接続。 • FMC の設定検証。 • ELB でより多くのリスニングポートを開くためのサポート。 • シングルスタック展開に変更。すべての Lambda 関数と AWS リソースは、合理化された展開のためにシングルスタックから展開されます。 サポートされているプラットフォーム：AWS の FTDv
Azure 向け FTDv の自動スケールの改善	Azure 向け FTDv の自動スケール ソリューションには、CPU だけでなく、CPU とメモリ（RAM）に基づくスケーリングメトリックのサポー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：Azure の FTDv
Firepower Threat Defense：デバイス管理	

機能	説明
データインターフェイスでのFTDの管理	専用の管理インターフェイスではなく、データインターフェイス上の FTD の FMC 管理を設定できるようになりました。 この機能は、本社の FMC からブランチオフィスの FTD を管理し、外部インターフェイスで FTD を管理する必要がある場合に、リモート展開に役立ちます。DHCP を使用して FTD でパブリック IP アドレスを受信する場合は、オプションで Web タイプの更新方式を使用して、インターフェイスのダイナミック DNS（DDNS）を設定できます。DDNS は、FTD の IP アドレスが変更された場合に FMC が完全修飾ドメイン名（FQDN）で FTD に到達できるようにします。 （注） FMCアクセス（データインターフェイス上）は、クラスタリングまたはハイアベイラビリティではサポートされません。 新規/変更された画面： • **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > **[デバイス（Device）]** > **[管理（Management）]** セクション • **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > **[インターフェイス（Interfaces）]** > **[FMCアクセス（FMC Access）]** • **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > **[DHCP]** > **[DDNS]** > **[DDNS更新方式（DDNS Update Methods）]** ページ 新規/変更された FTD CLI コマンド：**configure network management-data-interface**、**configure policy rollback** サポートされるプラットフォーム：FTD
FTD での FMC IP アドレスの更新	FMC の IP アドレスを変更する場合に、FTD CLI を使用してデバイスを更新できるようになりました。 新規/変更された FTD CLI コマンド： **configure manager edit** サポートされるプラットフォーム：FTD

機能	説明
Firepower 4100/9300 の FTD 動作リンク状態と物理リンク状態の同期	Firepower 4100/9300 シャーシでは、FTD 動作リンク状態をデータインターフェイスの物理リンク状態と同期できるようになりました。 現在、FXOS 管理状態がアップで、物理リンク状態がアップである限り、インターフェイスはアップ状態になります。FTD アプリケーション インターフェイスの管理状態は考慮されません。FTD からの同期がない場合は、たとえば、FTD アプリケーションが完全にオンラインになる前に、データインターフェイスが物理的にアップ状態になったり、FTD のシャットダウン開始後からしばらくの間はアップ状態のままになる可能性があります。インラインセットの場合、この状態の不一致によりパケットがドロップされることがあります。これは、FTD が処理できるようになる前に外部ルータが FTD へのトラフィックの送信を開始することがあるためです。 この機能はデフォルトで無効になっており、FXOS の論理デバイスごとに有効にできます。 （注） この機能は、クラスタリング、コンテナインスタンス、または Radware vDP デコレータを使用する FTD ではサポートされません。ASA でもサポートされていません。 新規/変更された [Firepower Chassis Manager] 画面：[論理デバイス（Logical Devices）] > [リンク状態の有効化（Enable Link State）] 新規/変更された FXOS コマンド：**set link-state-sync enabled**、**show interface expand detail** サポートされるプラットフォーム：Firepower 4100/9300
Firepower 1100/2100 シリーズ SFP インターフェイスで、自動ネゴシエーションの無効化がサポートされるようになりました	自動ネゴシエーションを無効にするように Firepower 1100/2100 シリーズ SFP インターフェイスを設定できるようになりました。 10 GB インターフェイスの場合、自動ネゴシエーションなしで速度を 1 GB に設定できます。速度が 10 GB に設定されているインターフェイスの自動ネゴシエーションは無効にできません。 新規/変更された画面：**[Devices]** > **[Device Management]** > **[Interfaces]** > [edit interface] > **[Hardware Configuration]** > **[Speed]** サポートされるプラットフォーム：Firepower 1100/2100 シリーズ
Firepower Threat Defense：クラスタリング	

機能	説明
FMC の新しいクラスタ管理機能	FMC を使用して、以前は CLI を使用する必要のあった次のクラスタ管理タスクを実行できるようになりました。 • クラスタユニットを有効または無効にします。 • [Device Management] ページからクラスタのステータスを表示します（ユニットごとの履歴とサマリーを含む）。 • ロールをコントロールユニットに変更します。 新規/変更された画面： • [Devices] > [Device Management] > [More] メニュー • [Devices] > [Device Management] > [Cluster] > [General] エリア > [Cluster Live Status] リンク > [Cluster Status] サポートされるプラットフォーム：Firepower 4100/9300
クラスタ導入の高速化	クラスタの展開がより迅速に完了するようになりました。また、ほとんどの導入の失敗も、より迅速に失敗します。 サポートされるプラットフォーム：Firepower 4100/9300

機能	説明
クラスタリングでの PAT アドレス割り当ての変更。PAT プールの [フラットなポート範囲（Flat Port Range）] オプションがデフォルトで有効になり、設定できなくなりました。	**アップグレードの影響。** PAT アドレスがクラスタのメンバーに配布される方法が変更されます。 以前は、アドレスはクラスタのメンバーに配布されていたため、PAT プールにはクラスタメンバーごとに少なくとも 1 つのアドレスが必要でした。制御は各 PAT プールアドレスを等しいサイズのポートブロックに分割し、それらをクラスタメンバーに配布するようになりました。各メンバーには、同じ PAT アドレスのポートブロックがあります。したがって、通常 PAT に必要な接続量に応じて、PAT プールのサイズを 1 つの IP アドレスにまで減らすことができます。 ポートブロックは、1024 ～ 65535 の範囲で 512 ポートのブロック単位で割り当てられます。オプションで、PAT プールルールを設定するときに、このブロック割り当てに予約ポート 1 ー 1023 を含めることができます。たとえば、単一ノードでは PAT プール IP アドレスあたり 65535 個の接続すべてを処理するのに対し、4 ノードクラスタでは、各ノードは 32 個のブロックを取得し、PAT プール IP アドレスあたり 16384 個の接続を処理できます。 この変更の一環として、スタンドアロンまたはクラスタ内での動作に関わりなく、すべてのシステムの PAT プールは、フラットなポート範囲 1024 ー 65535 を使用できるようになりました。以前は、[Flat Port Range] オプションを PAT プールルール（FTD NAT の [Pat Pool] タブ）で有効化することで、フラットな範囲を使用できました。[フラットなポート範囲（Flat Port Range）] オプションは無視され、PAT プールは常にフラットになります。必要に応じて [Include Reserved Ports] オプションを選択して、PAT プールに 1 ー 1023 のポート範囲を含めることができます。 ポートブロック割り当てを設定する（[ブロック割り当て（Block Allocation）] PAT プールオプション）と、デフォルトの 512 ポートブロックではなく、独自のブロック割り当てサイズが使用されます。また、クラスタ内のシステムの PAT プールに拡張 PAT を設定することはできません。 この変更は自動的に有効になります。アップグレードの前後に何もする必要はありません。 サポートされるプラットフォーム：FTD
Firepower Threat Defense：暗号化と VPN	

機能	説明
RA VPN の AnyConnect モジュールサポート	FTD RA VPN で AnyConnect モジュールがサポートされるようになりました。 RA VPN グループポリシーの一部として、ユーザが Cisco AnyConnect VPN クライアントをダウンロードするときに、さまざまなオプションモジュールをダウンロードしてインストールするように設定できるようになりました。これらのモジュールは、Web セキュリティ、マルウェア保護、オフネットワークローミング保護などのサービスを提供できます。 各モジュールを、AnyConnect プロファイルエディタで作成され、AnyConnect ファイルオブジェクトとして FMC にアップロードされたカスタム設定を含むプロファイルに関連付ける必要があります。 新規/変更された画面： • モジュールプロファイルのアップロード：新しい [File Type] オプションが [Objects] > [Object Management] > [VPN] > [AnyConnect File] > [Add AnyConnect File] に追加されました • モジュールの設定：[Client Modules] オプションが [Objects] > [Object Management] > [VPN] > [Group Policy] > [add or edit a Group Policy object] > [AnyConnect] 設定に追加されました サポートされるプラットフォーム：FTD
RA VPN の AnyConnect 管理 VPN トンネル	FTD RA VPN は、エンドユーザが VPN 接続を確立したときだけでなく、企業のエンドポイントの電源がオンになったときにエンドポイントへの VPN 接続を可能にする AnyConnect 管理 VPN トンネルをサポートするようになりました。 この機能は、オフィスネットワークに VPN を介してユーザが頻繁に接続しないデバイスに対しては特に、外出中のオフィスのエンドポイントで管理者がパッチ管理を行うのに役立ちます。社内ネットワークの接続を必要とするエンドポイントオペレーティングシステムログインスクリプトに対するメリットもあります。 サポートされるプラットフォーム：FTD
RA VPN のシングルサインオン	FTD RA VPN は、 SAML 2.0 準拠のアイデンティティ プロバイダー（IdP）で設定されたリモートアクセス VPN ユーザのシングルサインオン（SSO）をサポートするようになりました。 新規/変更された画面： • SSO サーバへの接続：[Objects] > [Object Management] > [AAA Server] > [Single Sign-on Server] • RA VPN の一部として SSO を設定します。RA VPN 接続プロファイルを設定する際に、認証方式（AAA 設定）として [SAML] を追加しました。 サポートされるプラットフォーム：FTD

機能	説明
RA VPN の LDAP 許可	FTD RA VPN は、LDAP 属性マップを使用した LDAP 認証をサポートするようになりました。 LDAP 属性マップにより、Active Directory（AD）または LDAP サーバに存在する属性が、シスコの属性名と同一視されるようになります。その後、リモートアクセス VPN 接続の確立中に AD または LDAP サーバが FTD デバイスに認証を返すと、FTD デバイスは、その情報を使用して、AnyConnect クライアントが接続を完了する方法を調整できます。 サポートされるプラットフォーム：FTD
仮想トンネルインターフェイス（VTI）とルートベースのサイト間 VPN	FTD サイト間 VPN は、仮想トンネルインターフェイス（VTI）と呼ばれる論理インターフェイスをサポートするようになりました。 ポリシーベース VPN の代替策として、仮想トンネルインターフェイスが設定されたピア間に VPN トンネルを作成することができます。これは、各トンネルの終端に IPsec プロファイルが付加されたルートベースの VPN をサポートします。これは、動的または静的なルートの使用が可能です。VTI を使用することにより、静的暗号マップのアクセス リストを設定してインターフェイスにマッピングすることが不要になります。トラフィックは、スタティックルートまたは BGP を使用して暗号化されます。ルーテッド セキュリティ ゾーンを作成し、そこに VTI インターフェイスを追加し、VTI トンネルを介して復号化されたトラフィック制御のアクセス制御ルールを定義できます。 VTI ベースの VPN は、次の間で作成できます。 • 2 つの FTD デバイス • FTD デバイスとパブリッククラウド • FTD デバイスとサービスプロバイダーの冗長性を備えた別の FTD デバイス 新規/変更された画面： • **[Devices] > [Device Management] > [Interfaces] > [Add Interfaces] > [Virtual Tunnel Interface]** • **[Devices] > [VPN] > [Site To Site] > [Add VPN] > [Firepower Threat Defense Device] > [Route Based (VTI)]** サポートされるプラットフォーム：FTD

機能	説明
サイト間 VPN に対するダイナミック RRI サポート	FTD サイト間 VPN は、サイト間 VPN 展開で IKEv2 ベースのスタティック暗号マップでサポートされるダイナミック リバース ルート インジェクション（RRI）をサポートするようになりました。これにより、スタティックルートは、リモート トンネル エンドポイントで保護されているネットワークとホストのルーティングプロセスに自動的に挿入されます。 新規/変更された画面：サイト間 VPN トポロジにエンドポイントを追加するときの [Enable Dynamic Reverse Route Injection] 詳細オプションが追加されました。 サポートされるプラットフォーム：FTD
手動証明書登録の拡張機能	署名済み CA 証明書とアイデンティティ証明書を CA 機関から互いに独立して取得できるようになりました。 証明書署名要求（CSR）を作成し、アイデンティティ証明書を取得するための登録パラメータを保存する PKI 証明書登録オブジェクトに次の変更を行いました。 • PKI 証明書登録オブジェクトの手動登録設定に [CA Only] オプションが追加されました。このオプションを有効にすると、CA 機関から署名済み CA 証明書のみを受け取り、アイデンティティ証明書は受け取りません。 • PKI 証明書登録オブジェクトの手動登録設定で、[CA Certificate] フィールドを空白のままにできるようになりました。これを行うと、署名済み CA 証明書ではなく、CA 機関からアイデンティティ証明書のみを受け取ります。 新規/変更された画面：[Objects] > [Object Management] > [PKI] > [Cert Enrollment] > [Add Cert Enrollment] > [CA Information] > [Enrollment Type] > [Manual] サポートされるプラットフォーム：FTD
FTD 証明書管理の拡張機能	FTD 証明書管理に次の機能拡張が行われました。 • 証明書の内容を表示するときに、認証局（CA）のチェーンを表示できるようになりました。 • 証明書をエクスポートできるようになりました。 新規/変更された画面： • [Devices] > [Certificates] > [Status] 列 > [View] アイコン（虫めがね） • [Devices] > [Certificates] > [Export] アイコン サポートされるプラットフォーム：FTD
アクセス制御：URL フィルタリング、アプリケーション制御、およびセキュリティ インテリジェンス	

機能	説明
TLS 1.3（TLS サーバアイデンティティ検出）で暗号化されたトラフィックの URL フィルタリングとアプリケーション制御	サーバ証明書からの情報を使用して、TLS 1.3 で暗号化されたトラフィックの URL フィルタリングとアプリケーション制御を実行できるようになりました。この機能が動作するためにトラフィックを復号化する必要はありません。 （注） 暗号化トラフィックで URL フィルタリングとアプリケーション制御を実行する場合は、この機能を有効にすることを推奨します。ただし、特に低メモリモデルでは、デバイスのパフォーマンスに影響を与える可能性があります。 新規/変更された画面：アクセス コントロール ポリシーの [Advanced] タブに [TLS Server Identity Discovery] の警告とオプションが追加されました。 新規/変更された FTD CLI コマンド：**show conn detail** コマンドの出力に B フラグが追加されました。TLS 1.3 暗号化接続では、このフラグは、アプリケーションおよび URL の検出にサーバ証明書を使用したことを示します。 サポートされるプラットフォーム：FTD
レピュテーションが不明な Web サイトへのトラフィックに対する URL フィルタリング	レピュテーションが不明な Web サイトに対して URL フィルタリングを実行できるようになりました。 新規/変更された画面：アクセス制御、QoS、および SSL ルールエディタに [Apply to unknown reputation] チェックボックスが追加されました。 サポートされるプラットフォーム FMC
DNS フィルタリングにより URL フィルタリングを強化します	**ベータ版。** *DNS* フィルタリングは、暗号化されたトラフィックを含め（ただしトラフィックを復号化せずに）トランザクションの早い段階で要求されたドメインのカテゴリとレピュテーションを決定することで、URL フィルタリングを強化します。アクセス コントロール ポリシーごとに DNS フィルタリングを有効にし、そのポリシーのすべてのカテゴリ/レピュテーション URL ルールに適用します。 （注） DNS フィルタリングはベータ機能であり、期待どおりに動作しない可能性があります。実稼働環境では使用しないでください。 新規/変更された画面：[General Settings] の下のアクセス コントロール ポリシーの [Advanced] タブに [Enable reputation enforcement on DNS traffic] オプションが追加されました。 サポートされるプラットフォーム FMC

機能	説明
セキュリティインテリジェンスフィードの更新頻度の短縮	FMC は、5 分または 15 分ごとにセキュリティ インテリジェンス データを更新できるようになりました。以前は、最短更新頻度は 30 分でした。 カスタムフィードでこれらの短い頻度のいずれかを設定する場合は、md5 チェックサムを使用してフィードにダウンロードする更新があるかどうかを判断するようにシステムを設定する必要もあります。 新規/変更された画面：新しいオプションが [Objects] > [Object Management] > [Security Intelligence] > [Network Lists and Feeds] > [edit feed] > [Update Frequency] に追加されました サポートされるプラットフォーム FMC
アクセス制御：ユーザ制御	
ISE/ISE-PIC を使用した pxGrid 2.0	**アップグレードの影響。** FMC を ISE/ISE-PIC アイデンティティソースに接続する場合は、pxGrid 2.0 を使用します。まだ pxGrid 1.0 を使用している場合は、ここで切り替えてください。このバージョンは廃止されました。 pxGrid 2.0 で使用するために、バージョン 6.7.0 では Cisco ISE 適応型ネットワーク制御（ANC）修復が導入され、相関ポリシー違反に関連する ISE 設定 ANC ポリシーが適用またはクリアされます。 pxGrid 1.0 で Cisco ISE エンドポイント保護サービス（EPS）修復を使用した場合は、pxGrid 2.0 で ANC 修復を設定して使用します。「誤った」pxGrid を使用している場合、ISE 修復は起動しません。ISE Connection Status Monitor ヘルスモジュールは、不一致を警告します。 サポートされているすべての Firepower バージョン（統合製品を含む）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。 新規/変更された画面： • [Policies] > [Actions] > [Modules] > [Installed Remediation Modules] リスト • [Policies] > [Actions] > [Instances] > [Select a module type] ドロップダウンリスト サポートされるプラットフォーム FMC

機能	説明
レルムシーケンス	レルムを順序付けられたレルムシーケンスにグループ化できるようになりました。 単一のレルムを追加するのと同じ方法で、アイデンティティルールにレルムシーケンスを追加します。アイデンティティルールをネットワークトラフィックに適用すると、システムは指定された順序で Active Directory ドメインを検索します。LDAP レルムのレルムシーケンスは作成できません。 新規/変更された画面：[System] > [Integration] > [Realm Sequences] サポートされるプラットフォーム FMC
ISE サブネットフィルタリング	特にメモリの少ないデバイスでは、CLI を使用して、ISE からのユーザと IP およびセキュリティグループタグ（SGT）と IP のマッピングの受信から、サブネットを除外できるようになりました。 Snort Identity Memory Usage ヘルスモジュールは、メモリ使用率が特定のレベル（デフォルトでは 80%）を超えるとアラートを出します。 新しいデバイス CLI コマンド：**configure identity-subnet-filter** {**add** | **remove**} サポートされるプラットフォーム：FMC 管理対象デバイス
アクセス制御：侵入およびマルウェア防御	
動的分析のためのファイルの事前分類の改善	**アップグレードの影響。** システムは、静的分析の結果（動的要素のないファイルなど）に基づいて、疑わしいマルウェアファイルを動的分析用に送信しないことを決定できるようになりました。 アップグレード後、[Captured Files] テーブルでは、これらのファイルの動的分析ステータスが [Rejected for Analysis] になります。 サポートされるプラットフォーム FMC

機能	説明
S7Commplus プリプロセッサ	新しい S7Commplus プリプロセッサは、広く受け入れられている S7 産業用プロトコルをサポートします。これを使用して、対応する侵入ルールとプリプロセッサルールを適用し、悪意のあるトラフィックをドロップし、侵入イベントを生成できます。 新規/変更された画面： • プリプロセッサの有効化：ネットワーク分析ポリシーエディタで、[Settings] をクリックし（「Settings」という語をクリックします）、SCADA プリプロセッサで [S7Commplus Configuration] を有効にします。 • プリプロセッサの設定：ネットワーク分析ポリシーエディタの [Settings] で、[S7Commplus Configuration] をクリックします。 • S7Commplus プリプロセッサルールの設定：侵入ポリシーエディタで、[Rules] > [Preprocessors] > [S7 Commplus Configurations] の順にクリックします。 サポートされるプラットフォーム：ISA 3000 を含むすべての FTD デバイス
カスタム侵入ルールのインポートでルール競合の際に警告表示	カスタム（ローカル）侵入ルールをインポートする場合、FMC がルールの競合について警告するようになりました。以前は、FMC は競合の原因となるルールをサイレントにスキップしていました。ただし、競合のあるルールのインポートが完全に失敗するバージョン 6.6.0.1 は除きます。 [ルールの更新（Rule Updates）] ページで、ルールのインポートに競合があった場合は、[ステータス（Status）] 列に警告アイコンが表示されます。詳細については、警告アイコンの上にポインタを置いて、ツールチップを参照してください。 既存のルールと同じ SID/リビジョン番号を持つ侵入ルールをインポートしようとすると、競合が発生することに注意してください。カスタムルールの更新バージョンには必ず新しいリビジョン番号を付けてください。Firepower Management Center 構成ガイド のローカル侵入ルールをインポートするためのベストプラクティスを読むことを推奨します。 新規/変更された画面：**[System]** > **[Updates]** > **[Rule Updates]** に警告アイコンが追加されました。 サポートされるプラットフォーム FMC
アクセス制御：TLS/SSL 暗号解読	

機能	説明
復号の既知キー TLS/SSL ルールのための ClientHello の変更	**アップグレードの影響。** TLS/SSL 復号化を設定した場合、管理対象デバイスが ClientHello メッセージを受信すると、システムはそのメッセージを復号の既知キーアクションを含む TLS/SSL ルールと照合しようとします。以前は、システムは ClientHello メッセージと復号 - 再署名ルールのみを照合していました。 照合は ClientHello メッセージからのデータとキャッシュされたサーバ証明書データからのデータに依存します。メッセージが一致すると、デバイスは ClientHello メッセージを特定の方法で変更します。『Firepower Management Center 構成ガイド』の「ClientHello Message Handling」のトピックを参照してください。 この動作の変更は、アップグレード後に自動的に行われます。復号の既知キー TLS/SSL ルールを使用する場合は、暗号化されたトラフィックが期待どおりに処理されていることを確認します。 サポートされているプラットフォーム：すべてのデバイス
イベントロギングおよび分析	
オンプレミスの Stealthwatch ソリューションによるリモートデータストレージと相互起動	オンプレミスの Stealthwatch ソリューションである Cisco Security Analytics and Logging（On Premises）を使用して、大量の Firepower イベントデータを FMC 以外に保存できるようになりました。 FMC でイベントを表示する場合、リモートデータストレージの場所にあるイベントをすばやく相互起動して表示できます。FMC は syslog を使用して、接続、セキュリティ インテリジェンス、侵入、ファイル、およびマルウェアイベントを送信します。 （注） このオンプレミスソリューションは、バージョン 6.4.0 以上を実行している FMC でサポートされます。ただし、コンテキスト相互起動には Firepower バージョン 6.7.0 以上が必要です。このソリューションは、Stealthwatch Enterprise（SWE）バージョン 7.3 を実行する必要がある Stealthwatch Management Console（SMC）用の Security Analytics and Logging On Prem アプリケーションの可用性にも依存します。 サポートされるプラットフォーム：FMC

機能	説明
Stealthwatch コンテキスト相互起動リソースを迅速に追加する	FMC の新しいページを使用すると、Stealthwatch アプライアンスのコンテキスト相互起動リソースをすばやく追加できます。 Stealthwatch リソースを追加した後は、一般的なコンテキスト相互起動ページで管理します。ここで、Stealthwatch 以外の相互起動リソースを手動で作成および管理します。 新規/変更された画面： • Stealthwatch リソースを追加します。[System] > [Logging] > [Security Analytics and Logging] • リソースを管理します。[Analysis] > [Advanced] > [Contextual Cross-Launch] サポート対象プラットフォーム：FMC
新しい相互起動オプションフィールドタイプ	次のイベントデータの追加タイプを使用して、外部リソースに相互起動できるようになりました。 • アクセス コントロール ポリシー • 侵入ポリシー • アプリケーションプロトコル • クライアント アプリケーション • Web アプリケーション • ユーザ名（レルムを含む） 新規/変更された画面： • 相互起動クエリリンクを作成または編集する際の新しい変数：[Analysis] > [Advanced] > [Contextual Cross-Launch]。 • ダッシュボードとイベントビューアの新しいデータタイプで、右クリックで相互起動が可能になりました。 サポートされるプラットフォーム：FMC

機能	説明
National Vulnerability Database（NVD）によって Bugtraq が置き換わりました	**アップグレードの影響。** Bugtraq 脆弱性データは使用できなくなりました。現在、ほとんどの脆弱性データはNVDから取得されています。この変更をサポートするために、次の変更を行いました。 • [CVE ID] および [Severity] フィールドが [Vulnerabilities] テーブルに追加されました。テーブルビューで CVE ID を右クリックすると、NVD の脆弱性に関する詳細を表示できます。 • [Vulnerability Impact] フィールドが [Impact] に名前変更されました（テーブルビューのみ）。 • 使用されていない/冗長な [Bugtraq ID]、[Title, Available Exploits]、[Technical Description]、[Solution] フィールドが削除されました。 • ホストネットワークマップから [Bugtraq ID] フィルタリングオプションが削除されました。 脆弱性データをエクスポートする場合は、アップグレード後に統合が期待どおりに機能していることを確認します。 サポートされるプラットフォーム FMC
のアップグレード	

機能	説明
アップグレード前の互換性チェック	

機能	説明
	アップグレードの影響。 FMC 展開では、より複雑な準備状況チェックを実行したり、アップグレードを試行したりする前に、Firepower アプライアンスがアップグレード前の互換性チェックに合格することが必要になりました。このチェックは、アップグレードが失敗する原因となる問題を検出します。これらをより早期に検出し、続行をブロックするようになりました。 検出は次のとおりです。 • FXOS を新しいリリースのコンパニオン FXOS バージョンにアップグレードするまで、FMC を使用して Firepower 4100/9300 シャーシをバージョン 6.7.0 以上にアップグレードすることはできません。「Firepower デバイス（4 ページ）」を参照してください。 デバイスをバージョン 6.7.0 以降にアップグレードしている限り、アップグレードはブロックされます。たとえば、Firepower バージョン 6.6.x に対して古いバージョンの FXOS がデバイスで実行されている場合でも、Firepower 4100/9300 の 6.3 → 6.6.x のアップグレードはブロックされません。 • デバイスの設定が古い場合、FMC を使用してデバイスをアップグレードすることはできません。 FMC がバージョン 6.7.0 以降を実行しており、管理対象デバイスを有効なターゲットにアップグレードしている限り、アップグレードはブロックされます。たとえば、デバイスの設定が古い場合、デバイスを 6.3.0 → 6.6.x にアップグレードするとブロックされます。 • デバイスの設定が古い場合、FMC をバージョン 6.7.0 以上からアップグレードすることはできません。 FMC がバージョン 6.7.0 以降を実行している限り、アップグレードはブロックされます。以前のバージョン（バージョン 6.7.0 へのアップグレードを含む）からアップグレードする場合は、必ず自分で展開する必要があります。 インストールするアップグレードパッケージを選択すると、FMC はすべての対象アプライアンスの互換性チェック結果を表示します。新しい [Readiness Check]ページにもこの情報が表示されます。示された問題を修正するまでアップグレードできません。 新規/変更された画面： • アップグレードパッケージの**[System]** > **[Update]** > **[Product Updates]** > **[Available Updates]** > **[Install]**アイコン • **[System]** > **[Update]** > **[Product Updates]** > **[Readiness Checks]**

機能	説明
	サポートされるプラットフォーム：FMC、FTD
準備状況チェックの改善	**アップグレードの影響。** 準備状況チェックにより、ソフトウェアをアップグレードするためのFirepowerアプライアンスの準備状況を評価できます。これらのチェックには、データベースの整合性、ファイルシステムの整合性、設定の整合性、ディスク容量などが含まれます。 FMC をバージョン 6.7.0 にアップグレードすると、FTD のアップグレード準備状況チェックが次のように改善されます。 • 準備状況チェックが高速になります。 • デバイス CLI にログインすることなく、ハイアベイラビリティおよびクラスタ化された FTD デバイスで準備状況チェックがサポートされるようになりました。 • FTD デバイスをバージョン 6.7.0 以上にアップグレードするための準備状況チェックで、デバイスにアップグレードパッケージが存在する必要はなくなりました。アップグレード自体を開始する前に、アップグレードパッケージをデバイスにプッシュすることをお勧めしますが、準備状況チェックを実行する前に行う必要はありません。 • インストールするアップグレードパッケージを選択すると、該当するすべてのFTDデバイスの準備状況がFMCに表示されるようになりました。新しい [Readiness Checks] ページでは、展開内の FTD デバイスの準備状況チェックの結果を表示できます。このページから準備状況チェックを再実行することもできます。 • 準備状況チェックの結果には、推定アップグレード時間が含まれます（ただし、リブート時間は含まれません）。 • エラーメッセージの方が優れています。FMC のメッセージセンターから成功/失敗ログをダウンロードすることもできます。 FMCがバージョン6.7.0以上を実行している限り、これらの改善はバージョン 6.3.0 以上からの FTD アップグレードでサポートされます。 新規/変更された画面： • アップグレードパッケージの**[System]** > **[Update]** > **[Product Updates]** > **[Available Updates]** > **[Install]**アイコン • **[System]** > **[Update]** > **[Product Updates]** > **[Readiness Checks]** • **[Message Center] > [Tasks]** サポートされるプラットフォーム：FTD

機能	説明
FTDアップグレードステータス レポートとキャンセル/再試行オプションの改善	

機能	説明
	アップグレードの影響。 [Device Management] ページで、進行中のデバイスアップグレードと準備状況チェックのステータス、およびアップグレードの成功/失敗の 7 日間の履歴を表示できるようになりました。メッセージセンターでは、拡張ステータスとエラーメッセージも提供されます。 デバイス管理とメッセージセンターの両方からワンクリックでアクセスできる新しい [Upgrade Status] ポップアップに、残りのパーセンテージ/時間、特定のアップグレード段階、成功/失敗データ、アップグレードログなどの詳細なアップグレード情報が表示されます。 また、このポップアップで、失敗したアップグレードまたは進行中のアップグレードを手動でキャンセル（[Cancel Upgrade]）することも、失敗したアップグレードを再試行（[Retry Upgrade]）することもできます。アップグレードをキャンセルすると、デバイスはアップグレード前の状態に戻ります。 （注） 失敗したアップグレードを手動でキャンセルまたは再試行できるようにするには、FMC を使用して FTD デバイスをアップグレードするときに表示される新しい自動キャンセルオプションを無効にする必要があります（[Automatically cancel on upgrade failure and roll back to the previous version]）。オプションを有効にすると、アップグレードが失敗した場合、デバイスは自動的にアップグレード前の状態に戻ります。 パッチの自動キャンセルはサポートされていません。HA またはクラスタ展開では、自動キャンセルは各デバイスに個別に適用されます。つまり、1 つのデバイスでアップグレードが失敗した場合、そのデバイスだけが元に戻ります。 新規/変更された画面： • FTD アップグレードパッケージの**[System]** > **[Update]** > **[Product Updates]** > **[Available Updates]** > **[Install]**アイコン • **[Devices]** > **[Device Management]** > **[Upgrade]** • **[Message Center] > [Tasks]** 新しい FTD CLI コマンド： • **show upgrade status detail** • **show upgrade status continuous** • **show upgrade status** • **upgrade cancel** • **upgrade retry**

機能	説明
	サポートされるプラットフォーム：FTD
アップグレードがスケジュールされたタスクを延期する	**アップグレードの影響。** FMC アップグレードは、スケジュールされたタスクを延期するようになりました。アップグレード中に開始するようにスケジュールされたタスクは、アップグレード後の再起動の 5 分後に開始されます。 （注） アップグレードを開始する前に、実行中のタスクが完了していることを確認する必要があります。アップグレードの開始時に実行中のタスクは停止し、失敗したタスクとなり、再開できません。 この機能は、サポートされているバージョンからのすべてのアップグレードでサポートされていることに注意してください。2020 年 11 月現在、これにはバージョン 6.4.0.10 以降のパッチと、およびバージョン 6.7.0 以上が含まれています。この機能は、サポートされていないバージョンからサポートされているバージョンへのアップグレードではサポートされていません。 サポートされるプラットフォーム FMC
アップグレードでディスク容量を節約するために PCAP ファイルが削除される	**アップグレードの影響。** 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。アップグレードにより、ローカルに保存された PCAP ファイルが削除さ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：すべて
展開とポリシー管理	
コンフィギュレーション ロールバック	**ベータ版。** FTD デバイスの設定を「ロールバック」して、以前に展開した設定に置き換えることができるようになりました。 （注） ロールバックはベータ機能であり、すべての展開タイプとシナリオでサポートされているわけではありません。これは中断を伴う操作でもあります。『Firepower Management Center 構成ガイド』の「Policy Management」の章のガイドラインと制限事項を必ず読んで理解してください。 新規/変更されたページ：[Deploy] > [Deployment History] > [Rollback] 列とアイコン。 サポートされるプラットフォーム：FTD

機能	説明
FTD コンテナインスタンスのバックアップと復元	FMC を使用して FTD コンテナインスタンスをバックアップ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）]>[ツール（Tools）]>[バックアップ/復元（Backup/Restore）] > [管理対象デバイスのバックアップ（Managed Device Backup）] 新規/変更された FTD CLI コマンド： **restore** サポートされているプラットフォーム：Firepower 4100/9300
侵入およびファイルポリシーを（アクセス コントロール ポリシーとは無関係に）展開する	依存する変更がない限り、アクセス コントロール ポリシーとは無関係に侵入ポリシーとファイルポリシーを選択して展開できるようになりました。 新規/変更された画面：[Deploy] > [Deployment] サポートされるプラットフォーム FMC
アクセス制御ルールのコメントの検索	アクセス制御ルールのコメント内で検索できるようになりました。 新規/変更された画面：アクセス コントロール ポリシー エディタで、[Search Rules] ドロップダウンダイアログに [Comments] フィールドが追加されました。 サポートされるプラットフォーム FMC
FTD NAT ルールの検索とフィルタリング	FTD NAT ポリシーでルールを検索して、IP アドレス、ポート、オブジェクト名などに基づいてルールを検索できるようになりました。検索結果には部分一致が含まれます。条件で検索すると、ルールテーブルがフィルタリングされ、一致するルールのみが表示されます。 新規/変更された画面：FTD NAT ポリシーを編集するときに、ルールテーブルの上に検索フィールドが追加されました。 サポートされるプラットフォーム：FTD
アクセス コントロール ポリシーとプレフィルタポリシー間のルールのコピーおよび移動	あるアクセス コントロール ポリシーから別のアクセス コントロール ポリシーにアクセス制御ルールをコピーできます。アクセス コントロール ポリシーとそれに関連付けられたプレフィルタポリシーの間でルールを移動することもできます。 新規/変更されたページ：アクセス コントロール ポリシー エディタおよびプレフィルタ ポリシー エディタで、各ルールの右クリック メニューに [Copy] および [Move] オプションが追加されました。 サポートされるプラットフォーム FMC

機能	説明
オブジェクト一括インポート	カンマ区切り値（CSV）ファイルを使用して、ネットワーク、ポート、URL、VLAN タグ、および識別名オブジェクトを FMC に一括インポートできるようになりました。 制限事項および特定のフォーマット手順については、『Firepower Management Center 構成ガイド』の「*Reusable Objects*」の章を参照してください。 新規/変更された画面：[Objects] > [Object Management] > [choose an object type] > [Add [Object Type]] > [Import Object] サポートされるプラットフォーム FMC
アクセス制御およびプレフィルタポリシーのインターフェイスオブジェクトの最適化	特定の FTD デバイスでインターフェイス オブジェクトの最適化を有効にできるようになりました。 展開時に、アクセス制御とプレフィルタポリシーで使用されるインターフェイスグループとセキュリティゾーンは、送信元/宛先インターフェイスペアごとに個別のルールを生成します。インターフェイス オブジェクトの最適化を有効にすると、システムはアクセス制御/プレフィルタルールごとに 1 つのルールを展開します。これにより、デバイス設定の簡素化および展開のパフォーマンス向上が可能になります。 インターフェイス オブジェクトの最適化はデフォルトで無効になっています。これを有効にする場合は、[Object Group Search] も有効にする必要があります。これは、ネットワークオブジェクトに加えてインターフェイス オブジェクトにも適用されるようになり、デバイスのメモリ使用量を削減できます。 新規/変更された画面：**[Devices]** > **[Device Management]** > **[Device]** > **[Advanced Settings]**セクション > [Interface Object Optimization] チェックボックス サポートされるプラットフォーム：FTD
管理とトラブルシューティング	
FMC シングルサインオン	FMC は、サードパーティの SAML 2.0 準拠アイデンティティ プロバイダー（IdP）で設定された外部ユーザのシングルサインオン（SSO）をサポートするようになりました。IdP のユーザまたはグループロールを FMC ユーザロールにマッピングできます。 新規/変更された画面： • **[Login]** > **[Single Sign-On]** • **[System]** > **[Users]** > **[SSO]** サポートされるプラットフォーム FMC

機能	説明
FMC ログアウトの遅延	FMC からログアウトする場合、自動的に 5 秒間遅延しカウントダウンが行われます。[ログアウト（Log Out）] を再度クリックすると、すぐにログアウトできます。 サポートされるプラットフォーム FMC
ヘルスモニタリングの強化	ヘルスモニタリングが次のように拡張されました。 • [Health Status] サマリーページでは Firepower Management Center と FMC が管理するすべてのデバイスの正常性を一目で確認できます。 • [Monitoring] ナビゲーションペインでは、デバイス階層を移動できます。 • 管理対象デバイスは、個別に一覧表示されるか、該当する場合は地理位置情報、高可用性、またはクラスタステータスに基づいてグループ化されます。 • ナビゲーションペインから個々のデバイスのヘルスモニタを表示できます。 • 相互に関連するメトリックを相互に関連付けるカスタムダッシュボード。CPU や Snort などの事前定義された相関グループから選択します。または、使用可能なメトリックグループから独自の変数セットを作成して、カスタム相関ダッシュボードを作成します。 サポートされるプラットフォーム FMC

機能	説明
ヘルスモジュールの更新	CPU使用率ヘルスモジュールが4つの新しいモジュールに置き換わりました。 • CPU 使用率（コアごと）：すべてのコアの CPU 使用率をモニタします。 • CPU 使用率データプレーン：デバイス上のすべてのデータプレーンプロセスの平均 CPU 使用率をモニタします。 • CPU 使用率 Snort：デバイス上の Snort プロセスの平均 CPU 使用率をモニタします。 • CPU使用率システム：デバイス上のすべてのシステムプロセスの平均CPU使用率をモニタします。 メモリ使用量を追跡するために、次のヘルスモジュールが追加されました。 • メモリ使用率データプレーン：データプレーンプロセスで使用される割り当て済みメモリの割合をモニタします。 • メモリ使用率Snort：Snortプロセスによって使用される割り当て済みメモリの割合をモニタします。 統計情報を追跡するために、次のヘルスモジュールが追加されました。 • 接続統計情報：接続統計情報と NAT 変換カウントをモニタします。 • クリティカルプロセス統計情報：クリティカルプロセスの状態、リソース消費量、再起動回数をモニタします。 • 展開された設定の統計情報：展開された設定に関する統計情報（ACE の数や IPS ルールなど）をモニタします。 • Snort 統計情報：イベント、フロー、およびパケットの Snort 統計情報をモニタします。 サポートされるプラットフォーム FMC
メッセージセンターの検索	メッセージセンターで現在のビューをフィルタリングできるようになりました。 新規/変更されたページ：メッセージセンターの [Show Notifications] スライダに [Filter] アイコンとフィールドが追加されました。 サポートされているプラットフォーム： FMC
ユーザビリティとパフォーマンス	

機能	説明
Dusk テーマ	**ベータ版。** FMC Web インターフェイスのデフォルトは Light テーマですが、新しい Dusk テーマを選択することもできます。 （注） Dusk テーマはベータ機能です。ページまたは機能を使用できない問題が発生した場合は、別のテーマに切り替えてください。すべてに対応することはできませんが、フィードバックもお寄せください。[ユーザ設定 (User Preferences)] ページのフィードバックリンクを使用するか、fmc-light-theme-feedback@cisco.com までお問い合わせください。 新規/変更された画面：ユーザ名の下にあるドロップダウンリストの [ユーザ設定（User Preferences）] サポートされるプラットフォーム FMC
FMC メニューの検索	FMC メニューを検索できるようになりました。 新規/変更されたページ：[Deploy] メニューの左側にある [FMC] メニューバーに [Search] アイコンとフィールドが追加されました。 サポートされているプラットフォーム： FMC
Firepower Management Center REST API	

機能	説明
新しい REST API サービス	新機能と既存の機能をサポートするために、次の FMC REST API サービス/操作が追加されました。 認可サービス： • ssoconfig：FMC シングルサインオンを取得および変更するための GET および PUT 操作。 ヘルスサービス： • メトリック：ヘルスモニタのメトリックを取得する GET 操作。 • アラート：ヘルスアラートを取得する GET 操作。 • deploymentdetails：展開の正常性の詳細を取得する GET 操作。 展開サービス： • jobhistories：展開履歴を取得する GET 操作。 • rollbackrequests：設定ロールバックを要求する POST 操作。 デバイスサービス： • メトリック：デバイスメトリックを取得する GET 操作。 • virtualtunnelinterfaces：仮想トンネルインターフェイスを取得および変更するための GET、PUT、POST、および DELETE 操作。 統合サービス： • externalstorage：外部イベントストレージ設定を取得および変更するための GET、ID による GET、および PUT 操作。 ポリシーサービス： • intrusionpolicies：侵入ポリシーを変更するための POST および DELETE 操作。 サービスの更新： • cancelupgrades：失敗したアップグレードをキャンセルする POST 操作。 • retryupgrades：失敗したアップグレードを再試行する POST 操作。 サポートされているプラットフォーム： FMC

FMC バージョン 6.7.0 で廃止された機能

これらの機能はバージョン 6.7.0 の FMC 展開で廃止されました。

表 *7:* バージョン *6.7.0* で廃止された機能：*FMC* 展開

機能	アップグレードの影響	説明
Cisco Firepower User Agent software ソフトウェアと ID ソース	FMC がアップグレードされないようにします。	ユーザエージェント設定を使用して FMC をバージョン 6.7.0 以降 にアップグレードすることはできません。 バージョン 6.6.0/6.6.x は、Cisco Firepower User Agent ソフトウェアをアイデンティティソースとしてサポートする最後のリリースです。Cisco Identity Services Engine/Passive Identity Connector（ISE/ISE-PIC）に切り替える必要があります。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。 廃止された FTD CLI コマンド：**configure user agent** 詳細については、『Cisco Firepower Management Center Configuration Guide』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。
Cisco ISE エンドポイント保護サービス（EPS）の修復	ISE 修復が機能しなくなることがあります。	Cisco ISE エンドポイント保護サービス（EPS）の修復は、pxGrid 2.0 では機能しません。代わりに、新しい Cisco ISE Adaptive Network Control（ANC）修復を設定して使用します。 「不正な」pxGrid を使用して FMC を ISE/ISE-PIC アイデンティティソースに接続している場合、ISE 修復は起動しません。ISE Connection Status Monitor ヘルスモジュールは、不一致を警告します。

機能	アップグレードの影響	説明
安全性の低い Diffie-Hellman グループ、暗号化アルゴリズム、およびハッシュアルゴリズム	FMC がアップグレードされないようにします。	次のいずれかの FTD 機能を使用している場合、FMC をアップグレードできないことがあります。 • Diffie-Hellman グループ：2、5、および 24。 グループ 5 は、IKEv1 の FMC 展開で引き続きサポートされますが、より強力なオプションに変更することをお勧めします。 • 強力な暗号化の輸出規制を満たすユーザ向けの暗号化アルゴリズム：DES、3DES、AES-GMAC、AES-GMAC-192、AES-GMAC-256。輸出規制を満たしていないユーザの場合、DES は引き続きサポートされます（これが唯一のオプションです）。 • NULL の「暗号化アルゴリズム」（暗号化なしの認証、テスト目的）は、IKEv1 と IKEv2 の両方の IPsec プロポーザルの FMC 展開で引き続きサポートされます。ただし、IKEv2 ポリシーではサポートされなくなりました。 • ハッシュアルゴリズム：MD5。 IKE プロポーザルまたは IPsec ポリシーでこれらの機能を使用している場合は、アップグレードする前に VPN 設定を変更して確認します。
ヘルスモジュール	なし	バージョン 6.7.0 では、次のヘルスモジュールが廃止されています。 • CPU 使用率：4 つの新しいモジュールに置き換えられました。「FMC バージョン 6.7.0 の新機能 （11 ページ）」を参照してください。 • ローカルマルウェア分析：このモジュールは、バージョン 6.3.0 のデバイス上の脅威データの更新モジュールに置き換えられました。バージョン 6.7.0 以降の FMC は、古いモジュールが適用されるデバイスを管理できなくなります。 • ユーザ エージェント ステータス モニタ：Cisco Firepower ユーザエージェントはサポートされなくなりました。

機能	アップグレードの影響	説明
FMC のクラシックテーマを使用したウォークスルー	なし	バージョン 6.7.0 では、クラシックテーマの FMC ウォークスルー（使用方法）が廃止されました。ユーザ設定でテーマを切り替えることができます。
Bugtraq	脆弱性データをエクスポートする場合は、アップグレード後に統合が期待どおりに機能していることを確認します。	バージョン 6.7.0 では Bugtraq のデータベースフィールドとオプションが削除されます。Bugtraq 脆弱性データは使用できなくなりました。現在、ほとんどの脆弱性データは National Vulnerability Database（NVD）から取得されています。 詳細については、FMC バージョン 6.7.0 の新機能 （11 ページ）を参照してください。
Microsoft Internet Explorer	ブラウザを切り替える必要があります。	Microsoft Internet Explorer を使用して Firepower Web インターフェイスをテストすることはなくなりました。Google Chrome、Mozilla Firefox、または Microsoft Edge に切り替えることをお勧めします。 詳細については、Web ブラウザの互換性 （8 ページ）を参照してください。
Firepower ソフトウェアを使用した ASA 5525-X、5545-X、および 5555-X デバイス	アップグレードは禁止されています。	ASA 5525-X、5545-X、および 5555-X のデバイスでは、Firepower ソフトウェア（FTD と ASA FirePOWER の両方）のバージョン 6.7.0+ にアップグレードしたり、このバージョンを新規インストールすることはできません。

以前に廃止された FMC 機能

アップグレードパスでバージョンをスキップする場合は、中間リリースの廃止された機能を確認してください。

FMC バージョン 6.6.0 で廃止された機能

これらの機能はバージョン 6.6.0 の FMC 展開で廃止されました。

表 *8 :* バージョン *6.6.0* で廃止された機能：*FMC* 展開

機能	アップグレードの影響	説明
クラウドベースの FMCv 展開でのメモリ不足のインスタンス	アップグレードは禁止されています。	パフォーマンス上の理由から、次の FMCv インスタンスはサポートされなくなりました。 • AWS での c3.xlarge • AWS での c3.2xlarge • AWS での c4.xlarge • AWS での c4.2xlarge • Azure での Standard_D3_v2 バージョン 6.6.0+ にアップグレードする前に、サイズを変更する必要があります。詳細については、FMCv をアップグレードするには 28 GB の RAM が必要 （68 ページ）を参照してください。 さらに、バージョン 6.6.0 リリースの時点で、クラウドベースの FMCv の展開におけるメモリ不足のインスタンスタイプが完全に廃止されました。以前の Firepower バージョンであっても、これらを使用して新しい FMCv インスタンスを作成することはできません。既存のインスタンスは引き続き実行できます。
VMware 向け FTDv の e1000 インターフェイス	アップグレードされないようにします。	バージョン 6.6.0 では、VMware 向け FTDv の e1000 インターフェイスのサポートを終了します。vmxnet3 または ixgbe インターフェイスに切り替えるまで、アップグレードすることはできません。または、新しいデバイスを展開できます。 詳細については、『Cisco Firepower Threat Defense Virtual for VMware Getting Started Guide』を参照してください。

機能	アップグレードの影響	説明
安全性の低い Diffie-Hellman グループ、暗号化アルゴリズム、およびハッシュアルゴリズム	なし。ただし、今すぐ切り替える必要があります。	バージョン6.6.0では、次のFTD機能は廃止されます。 • Diffie-Hellman グループ：2、5、および 24。 • 強力な暗号化の輸出規制を満たすユーザ向けの暗号化アルゴリズム：DES、3DES、AES-GMAC、AES-GMAC-192、AES-GMAC-256。輸出規制を満たしていないユーザの場合、DESは引き続きサポートされます（これが唯一のオプションです）。 • ハッシュアルゴリズム：MD5。 これらの機能はバージョン 6.7.0 で廃止されました。VPNで使用するために、IKEプロポーザルまたはIPSecポリシーでこれらの機能を設定しないでください。できるだけ強力なオプションに変更してください。
接続イベントのカスタムテーブル	サポートされていないカスタムテーブルは削除する必要があります。	バージョン6.6.0は、接続イベントとセキュリティインテリジェンス イベントのカスタムテーブルのサポートを終了します。アップグレード後は、これらのイベントの既存のカスタムテーブルは引き続き「利用可能」ですが、結果は返されません。これらのテーブルを削除することをお勧めします。 他のタイプのカスタムテーブルに変更はありません。 廃止されたオプション： • [分析（Analysis）] > [詳細設定（Advanced）] > [カスタムテーブル（Custom Tables）] > [カスタムテーブルの作成（Create Custom Table）] > [テーブル（Tables）] ドロップダウンリスト > [接続イベント（Connection Events）] と、[セキュリティインテリジェンス イベント（Security Intelligence Events）] のクリック

機能	アップグレードの影響	説明
イベントビューアから接続イベントを削除する機能	なし	バージョン 6.6.0 は、接続イベントとセキュリティ インテリジェンス イベントをイベントビューアから削除するためのサポートを終了しています。データベースを消去するには、**[システム（System）]** > **[ツール（Tools）]** > **[データの消去（Data purge）]** を選択します。 廃止されたオプション： • **[分析（Analysis）]** > **[接続（Connections）]** > **[イベント（Events）]** > [削除（Delete）] と [すべて削除（Delete All）] • **[分析（Analysis）]** > **[接続（Connections）]** > **[セキュリティ インテリジェンス イベント（Security Intelligence Events）]** > [削除（Delete）] と [すべて削除（Delete All）]

FMC バージョン 6.5.0 で廃止された機能

これらの機能はバージョン 6.5.0 の FMC 展開で廃止されました。

表 *9 :* バージョン *6.5.0* で廃止された機能：*FMC* 展開

機能	アップグレードの影響	説明
FMC CLI を無効にする機能	なし	バージョン 6.3.0 では、明示的に有効にする必要がある FMC CLI が導入されました。バージョン 6.5.0 では、新しい展開とアップグレードされた展開の両方に対して、FMC CLI が自動的に有効になります。Linux シェル（エキスパート モードとも呼ばれる）にアクセスする場合は、CLI にログインしてから、**expert** コマンドを使用する必要があります。 **注意** Cisco TAC の指示がない限り、シェルを使用して Firepower アプライアンスにアクセスしないことをお勧めします。 廃止されたオプション：**[システム（System）]** > **[設定（Configuration）]** > **[コンソール設定（Console Configuration）]** > **[CLI アクセスの有効化（Enable CLI Access）]** チェックボックス

機能	アップグレードの影響	説明
TLS 1.0 および 1.1	クライアントがアップグレードされたアプライアンスとの接続に失敗することがあります。	セキュリティ強化対策： • キャプティブポータル（アクティブ認証）では、TLS 1.0 のサポートが廃止されました。 • ホスト入力で TLS 1.0 および TLS 1.1 のサポートが廃止されました。 クライアントが Firepower アプライアンスとの接続に失敗した場合は、TLS 1.2 をサポートするようにクライアントをアップグレードすることをお勧めします。
Firepower 4100/9300 用の TLS crypto アクセラレーション FXOS CLI コマンド	なし	Firepower 4100/9300 の複数のコンテナ インスタンスに対して TLS crypto アクセラレーションを許可する一環として、次の FXOS CLI コマンドを削除しました。 • **show hwCrypto** • **config hwCrypto** 次の FTD CLI コマンドも同様です： • **show crypto accelerator 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。
Cisco Security Packet Analyzer の統合	なし。ただし、統合はサポートされていません。	バージョン 6.5.0 では、FMC と Cisco Security Packet Analyzer の統合のサポートを終了します。 廃止された画面/オプション： • **[システム（System）] > [統合（Integration）] > [パケットアナライザ（Packet Analyzer）]** • **[分析（Analysis）] > [詳細（Advanced）] > [パケットアナライザのクエリ（Packet Analyzer Queries）]** • ダッシュボードまたはイベント ビューアでイベントを右クリックしたときの [クエリパケットアナライザ（Query Packet Analyzer）]

機能	アップグレードの影響	説明
デフォルトの HTTPS サーバ証明書	なし	バージョン 6.4.0.9 以降からアップグレードする場合、デフォルトの HTTPS サーバ証明書の lifespan-on-renew は 3 年に戻りますが、バージョン 6.6.0 以降で再び 800 日に更新されます。 現在のデフォルトの HTTPS サーバ証明書は、いつ生成されたかに応じて、次のように期限切れになるように設定されています。 • 6.4.0.9 以降のパッチ：800 日 • 6.4.0 ～ 6.4.0.8：3 年 • 6.3.0 およびすべてのパッチ：3 年 • 6.2.3：20 年
Firepower Management Center モデル FMC 750、1500、3500	アップグレードは禁止されています。	FMC 750、FMC 1500、および FMC 3500 では、Firepower Management Center ソフトウェアをバージョン 6.5.0 以降にアップグレードしたり、このバージョンの新規インストールはできません。これらの FMC を使用してバージョン 6.5.0 以降のデバイスを管理することはできません。
Firepower ソフトウェアを搭載した ASA 5515-X および ASA 5585-X シリーズ デバイス	アップグレードは禁止されています。	ASA 5515-X および ASA 5585-X シリーズのデバイス（SSP-10、-20、-40、および -60）では、Firepower ソフトウェア（FTD と ASA FirePOWER の両方）のバージョン 6.5.0 以降にアップグレードしたり、このバージョンを新規インストールすることはできません。
Firepower 7000/8000 シリーズ デバイス	アップグレードは禁止されています。	AMP モデルを含む、Firepower 7000/8000 シリーズ デバイスでは、Firepower ソフトウェアをバージョン 6.5.0 以降にアップグレードしたり、このバージョンを新規インストールしたりできません。

FMC 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 の FMC 展開で廃止されました。

表 *10* : バージョン *6.4.0* で廃止された機能：*FMC* 展開

機能	アップグレードの影響	説明
SSL ハードウェアアクセラレーション FTD CLI コマンド	なし	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。
FMC メニューの変更	なし	バージョン 6.4.0 では、次の FMC ページの場所が変更されています。 **[システム（System）]> [統合（Integration）]> [クラウドサービス（Cloud Services）]** は次に変更されました。 **[システム（System）]> [統合（Integration）]> [Cisco CSI]**

Firepower Device Manager 展開に関する機能

FDM バージョン 6.7.0 の新機能

これらの FTD 機能はバージョン 6.7.0 の FDM 展開で導入されました。

機能	説明
プラットフォーム機能	
ASA 5525-X、5545-X、5555-X でのサポートが終了します。最後にサポートされていたリリースは FTD 6.6 です。	FTD 6.7 を ASA 5525-X、5545-X、5555-X にインストールすることはできません。これらのモデルで最後にサポートされていたリリースは FTD 6.6 です。
ファイアウォールと IPS の機能	

機能	説明
アクセス制御ルールの照合のための TLS サーバアイデンティティ検出。	TLS 1.3 証明書は暗号化されます。TLS 1.3 で暗号化されたトラフィックで、アプリケーションまたは URL フィルタリングを使用するアクセスルールに対応するには、システムが TLS 1.3 証明書を復号する必要があります。暗号化された接続が適切なアクセス制御ルールに適合していることを確認するため、[TLSサーバアイデンティティ検出（TLS Server Identity Discovery）] を有効にすることを推奨します。この設定では、証明書のみが復号されます。接続は暗号化されたままになります。 [アクセス制御の設定（Access Control Settings）]（⚙）ボタンとダイアログボックスが **[ポリシー（Policy）]** > **[アクセス制御（Access Control）]**ページに追加されました。
外部の信頼できる CA 証明書のグループ。	SSL 復号ポリシーで使用される信頼できる CA 証明書のリストをカスタマイズできるようになりました。デフォルトでは、ポリシーはすべてのシステム定義の信頼できる CA 証明書を使用しますが、カスタムグループを作成して証明書を追加したり、デフォルトグループを独自のより制限されたグループに置き換えることができます。 **[オブジェクト（Objects）]** > **[証明書（Certificates）]** ページに証明書グループが追加され、SSL 復号ポリシー設定を変更して証明書グループを選択できるようにしました。
パッシブ ID ルールの Active Directory レルムシーケンス。	Active Directory（AD）サーバとそのドメインの番号付きリストであるレルムシーケンスを作成し、パッシブ認証 ID ルールで使用できます。レルムシーケンスは、複数の AD ドメインをサポートしている状況で、ユーザベースのアクセス制御を実行するときに役立ちます。各 AD ドメインの個別のルールを記述する代わりに、すべてのドメインを対象とする単一のルールを作成できます。シーケンス内の AD レルムの順序は、ID の競合が発生した場合に、その競合を解決するために使用されます。 **[オブジェクト（Objects）]** > **[アイデンティティソース（Identity Sources）]** ページに AD レルム シーケンス オブジェクトが追加され、そのオブジェクトをパッシブ認証アイデンティティルールのレルムとして選択できるようになりました。FTD API に **RealmSequence** リソースが追加されました。また **IdentityRule** リソースには、アクションとしてパッシブ認証を使用するルールのレルムとしてレルム シーケンス オブジェクトを選択する機能が追加されました。

機能	説明
TrustSec セキュリティグループタグ（SGT）グループオブジェクトの FDM サポートと、アクセス制御ルールでのそれらの使用。	FTD 6.5 では、SGT グループオブジェクトを設定し、それらをアクセス制御ルールの一致基準として使用するためのサポートが FTD API に追加されました。さらに、ISE によってパブリッシュされた SXP トピックをリッスンするように ISE アイデンティティ オブジェクトを変更できます。これらの機能を FDM で直接設定できるようになりました。 新しいオブジェクトである SGT グループが追加され、それらを選択および表示できるようにアクセス制御ポリシーが更新されました。また、サブスクライブするトピックの明示的な選択を含むように ISE オブジェクトを変更しました。
Snort 3.0 のサポート。	新しいシステムでは、Snort 3.0 がデフォルトの検査エンジンです。古いリリースから 6.7 にアップグレードした場合、アクティブな検査エンジンは Snort 2.0 のままですが、Snort 3.0 に切り替えることができます。このリリースでは、Snort 3.0 は、仮想ルータ、時間ベースのアクセス制御ルール、または TLS 1.1 以下の接続の復号化をサポートしていません。これらの機能が必要ない場合にのみ Snort 3.0 を有効にしてください。Snort 2.0 と Snort 3.0 の間を自由に切り替えることができるため、必要に応じて、変更を元に戻すことができます。バージョンを切り替えるたびにトラフィックが中断されます。 **[デバイス（Device）] > [更新（Updates）]**ページの [侵入ルール（Intrusion Rules）] グループに Snort のバージョンを切り替える機能が追加されました。FTD API では、IntrusionPolicy リソースアクション/toggleinspectionengine が追加されました。 さらに、Snort 3 ルールパッケージの更新で追加、削除、または変更された侵入ルールを示す新しい監査イベント、ルール更新イベントがあります。
Snort 3 のカスタム侵入ポリシー。	Snort 3 を検査エンジンとして使用している場合は、カスタム侵入ポリシーを作成できます。これに対し、Snort 2 を使用する場合にのみ、事前定義されたポリシーを使用できます。カスタム侵入ポリシーを使用すると、ルールのグループを追加または削除し、グループレベルでセキュリティレベルを変更して、グループ内のルールのデフォルトアクション（無効化、アラート、またはドロップ）を効率的に変更できます。Snort 3 の侵入ポリシーを使用すると、Cisco Talos 提供の基本ポリシーを編集することなく、IPS/IDS システムの動作をより詳細に制御できます。 侵入ポリシーを一覧表示するように**[ポリシー（Policies）] > [侵入（Intrusion）]**ページが変更されました。新しいポリシーを作成したり、既存のポリシーを表示または編集（グループの追加/削除、セキュリティレベルの割り当て、ルールのアクションの変更など）することができます。複数のルールを選択し、それらのアクションを変更することもできます。さらに、アクセス制御ルールでカスタム侵入ポリシーを選択できます。

機能	説明
侵入イベント用の複数の syslog サーバ。	侵入ポリシー用に複数の syslog サーバを設定できます。侵入イベントは各 syslog サーバに送信されます。 侵入ポリシー設定ダイアログボックスに、複数の syslog サーバオブジェクトを選択する機能が追加されました。
URL レピュテーション照合にレピュテーションが不明なサイトを含めることが可能です。	URL カテゴリのトラフィック一致基準を設定し、レピュテーション範囲を選択する場合に、レピュテーションが不明な URL をレピュテーション照合に含めることができます。 アクセス制御ルールと SSL 復号ルールの URL レピュテーション基準に [レピュテーションが不明なサイトを含める（Include Sites with Unknown Reputation）] チェックボックスが追加されました。
VPN 機能	
仮想トンネルインターフェイス（VTI）とルートベースのサイト間 VPN。	VPN 接続プロファイルのローカルインターフェイスとして仮想トンネルインターフェイスを使用して、ルートベースのサイト間 VPN を作成できるようになりました。ルートベースのサイト間 VPN を使用すると、VPN 接続プロファイルを一切変更することなく、ルーティングテーブルを変更するだけで、特定の VPN 接続で保護されたネットワークを管理できます。リモートネットワークの追跡を継続し、前述の変更に対応して VPN 接続プロファイルを更新する必要はありません。その結果、クラウド サービス プロバイダーや大企業の VPN 管理が簡素化されます。 インターフェイスのリストのページに [仮想トンネルインターフェイス（Virtual Tunnel Interfaces）] タブが追加され、VTI をローカルインターフェイスとして使用できるように、サイト間 VPN ウィザードが更新されました。
FTD リモート アクセス VPN 接続を行うための Hostscan およびダイナミック アクセス ポリシー（DAP）の API サポート。	Hostscan パッケージとダイナミック アクセス ポリシー（DAP）ルール XML ファイルをアップロードし、XML ファイルを作成するよう DAP ルールを設定することで、接続中のエンドポイントのステータスに関連する属性に基づいてグループポリシーをリモートユーザに割り当てる方法を制御することができます。Cisco Identity Services Engine（ISE）がない場合は、これらの機能を使用して認可変更を実行できます。Hostscan のアップロードと DAP の設定は FTD API を使用してのみ行えます。FDM を使用して設定することはできません。Hostscan および DAP の使用方法の詳細については、AnyConnect のマニュアルを参照してください。 dapxml、hostscanpackagefiles、hostscanxmlconfigs、ravpns の各 FTD API オブジェクトモデルを追加または変更しました。

機能	説明
外部 CA 証明書の証明書失効チェックの有効化。	FTD API を使用して、特定の外部 CA 証明書の証明書失効チェックを有効にすることができます。失効チェックは、リモートアクセス VPN で使用される証明書に特に役立ちます。FDM を使用して証明書の失効チェックを設定することはできません。FTD API を使用する必要があります。 ExternalCACertificate リソースに revocationCheck、crlCacheTime、および oscpDisableNonce 属性が追加されました。
安全性の低い Diffie-Hellman グループ、および暗号化アルゴリズムとハッシュアルゴリズムのサポートがなくなりました。	6.6 で廃止されていた以下の機能が削除されました。それらを IKE プロポーザルまたは IPsec ポリシーで引き続き使用している場合は、アップグレード後にそれらを置き換えないと、設定変更を展開できません。VPN が正しく機能するように、サポートされる DH および暗号化アルゴリズムにアップグレードする前に VPN 設定を変更することをお勧めします。 • Diffie-Hellman グループ：2、5、および 24。 • 強力な暗号化の輸出規制を満たすユーザ向けの暗号化アルゴリズム：DES、3DES、AES-GMAC、AES-GMAC-192、AES-GMAC-256。輸出規制を満たしていないユーザの場合、DES は引き続きサポートされます（これが唯一のオプションです）。 • ハッシュアルゴリズム：MD5。
リモートアクセス VPN 用のカスタムポート。	リモートアクセス VPN（RA VPN）接続に使用するポートを設定できます。RA VPN に使用されているインターフェイスで FDM に接続する必要がある場合は、RA VPN 接続のポート番号を変更できます。FDM が使用するポート 443 は、デフォルトの RA VPN ポートでもあります。 RA VPN ウィザードのグローバル設定ステップが更新され、ポート設定が追加されました。
リモートアクセス VPN を認証するための SAML サーバのサポート。	SAML 2.0 サーバをリモートアクセス VPN の認証ソースとして設定できます。サポートされている SAML サーバは次のとおりです：Duo。 **[オブジェクト（Objects）] > [アイデンティティソース（Identity Sources）]** ページでのアイデンティティソースとして SAML サーバが追加され、それを使用できるようにリモートアクセス VPN 接続プロファイルが更新されました。

機能	説明
AnyConnect モジュールプロファイルの FTD API サポート。	FTD API を使用して、AMP イネーブラ、ISE ポスチャ、Umbrella といった AnyConnect で使用されるモジュールプロファイルをアップロードできます。これらのプロファイルは、AnyConnect プロファイルエディタ パッケージからインストールできるオフライン プロファイル エディタを使用して作成する必要があります。 AnyConnectClientProfile モデルに anyConnectModuleType 属性が追加されました。最初はモジュールプロファイルを使用する AnyConnect クライアントプロファイル オブジェクトを作成できますが、FDM で作成されたオブジェクトを変更して正しいモジュールタイプを指定するには、依然として API を使用する必要があります。
ルーティング機能	
スマート CLI による EIGRP のサポート。	以前のリリースでは、FlexConfig を使用して、[詳細設定（Advanced Configuration）] ページで EIGRP を設定しました。今回、[ルーティング（Routing）] ページでスマート CLI を直接使用して EIGRP を設定するようになりました。 FlexConfig を使用して EIGRP を設定した場合は、リリース 6.7 にアップグレードするときに、FlexConfig ポリシーから FlexConfig オブジェクトを削除してから、スマート CLI オブジェクトで設定を再作成する必要があります。スマート CLI の更新が完了するまでは、参照用に EIGRP FlexConfig オブジェクトを保持できます。設定は自動的に変換されません。 [ルーティング（Routing）] ページに EIGRP スマート CLI オブジェクトが追加されました。
インターフェイス機能	
ISA 3000 ハードウェアバイパスの持続性	永続化オプションを使用して、ISA 3000 インターフェイスペアのハードウェアバイパスを有効にできるようになりました。電源が回復した後、ハードウェアバイパスは手動で無効にするまで有効のままになります。持続性のないハードウェアバイパスを有効にすると、電源が回復した後にハードウェアバイパスが自動的に無効になります。ハードウェアバイパスが無効になっていると、短時間のトラフィック中断が発生する可能性があります。永続化オプションを使用すると、トラフィックの短時間の中断が発生するタイミングを制御できます。 新規/変更された画面：**[デバイス（Device）]** > **[インターフェイス（Interfaces）]** > **[ハードウェアバイパス（Hardware Bypass）]** > **[ハードウェアバイパスの設定（Hardware Bypass Configuration）]**

機能	説明
Firepower 4100/9300 の FTD 動作リンク状態と物理リンク状態の同期	Firepower 4100/9300 シャーシでは、FTD 動作リンク状態をデータインターフェイスの物理リンク状態と同期できるようになりました。現在、FXOS 管理状態がアップで、物理リンク状態がアップである限り、インターフェイスはアップ状態になります。FTD アプリケーション インターフェイスの管理状態は考慮されません。FTD からの同期がない場合は、たとえば、FTD アプリケーションが完全にオンラインになる前に、データインターフェイスが物理的にアップ状態になったり、FTD のシャットダウン開始後からしばらくの間はアップ状態のままになる可能性があります。この機能はデフォルトで無効になっており、FXOS の論理デバイスごとに有効にできます。 （注） この機能は、Radware vDP デコレータを使用する FTD ではサポートされません。 新規/変更された [Firepower Chassis Manager] 画面：[論理デバイス（Logical Devices）] > [リンク状態の有効化（Enable Link State）] 新規/変更された FXOS コマンド：**set link-state-sync enabled**、**show interface expand detail** サポートされるプラットフォーム：Firepower 4100/9300
Firepower 1100 および 2100 SFP インターフェイスで、自動ネゴシエーションの無効化がサポートされるようになりました	自動ネゴシエーションを無効にするように Firepower 1100 および 2100 SFP インターフェイスを設定できるようになりました。10GB インターフェイスの場合、自動ネゴシエーションなしで速度を 1GB に設定できます。速度が 10GB に設定されているインターフェイスの自動ネゴシエーションは無効にできません。 新規/変更画面：[Device] > [Interfaces] > [Edit Interface] > [Advanced Options] > [Speed] サポートされるプラットフォーム：Firepower 1100 および 2100
管理およびトラブルシューティングの機能	
失敗した FTD ソフトウェアのアップグレードをキャンセルし、以前のリリースに戻す機能。	FTD のメジャー ソフトウェア アップグレードが失敗するか、正常に機能しない場合は、アップグレードインストールの実行時の状態にデバイスを戻すことができます。 FDM の [システムのアップグレード（System Upgrade）] パネルにアップグレードを元に戻す機能が追加されました。アップグレード時に、FDM ログイン画面にアップグレードステータスが表示され、アップグレードが失敗した場合にキャンセルしたり元に戻すためのオプションが表示されます。FTD API に CancelUpgrade、RevertUpgrade、RetryUpgrade、および UpgradeRevertInfo リソースが追加されました。 FTD CLI に **show last-upgrade status**、**show upgrade status**、**show upgrade revert-info**、**upgrade cancel**、**upgrade revert**、**upgrade cleanup-revert**、および **upgrade retry** コマンドが追加されました。

機能	説明
データインターフェイス上のFDM/FTD APIアクセス用のカスタムHTTPSポート。	データインターフェイスで FDM または FTD API アクセスに使用する HTTPS ポートを変更できます。ポートをデフォルトの443から変更することにより、管理アクセスと同じデータインターフェイスで設定されているその他の機能（リモートアクセス VPN など）の競合を回避できます。管理インターフェイスの管理アクセス HTTPS ポートは変更できないことに注意してください。 **[デバイス（Device）]** > **[システム設定（System Settings）]** > **[管理アクセス（Management Access）]** > **[データインターフェイス（Data Interfaces）]** ページにポートを変更する機能が追加されました。
Firepower 1000および2100シリーズデバイス上の Cisco Defense Orchestrator のロータッチプロビジョニング。	Cisco Defense Orchestrator（CDO）を使用して新しい Firepower Threat Defense デバイスを管理する予定がある場合、デバイス セットアップ ウィザードを完了することなく、またはFDMにログインすることさえなく、デバイスを追加できるようになりました。 新しい Firepower 1000 および 2100 シリーズ デバイスは、最初に Cisco Cloud に登録され、CDO で簡単に要求できます。CDO に入ると、CDO からデバイスをすぐに管理できます。このロータッチプロビジョニングでは、物理デバイスと直接やりとりする必要性が最小限に抑えられ、ネットワクデバイスに関する経験が浅い従業員が勤務するリモートオフィスなどの場所にとって理想的です。 Firepower 1000 および 2100 シリーズ デバイスの初期プロビジョニング方法が変更されました。また、**[システム設定（System Settings）]**>**[クラウドサービス（Cloud Services）]**ページに自動登録が追加されました。これにより、FDM を使用して以前に管理していたアップグレード済みデバイスおよびその他のデバイスのプロセスを手動で開始できます。
SNMP 設定の FTD API サポート。	FTD API を使用して FDM または CDO 管理対象 FTD デバイスで SNMP バージョン 2c または 3 を設定できます。 API リソースの SNMPAuthentication、SNMPHost、SNMPSecurityConfiguration、SNMPServer、SNMPUser、SNMPUserGroup、SNMPv2cSecurityConfiguration、および SNMPv3SecurityConfiguration が追加されました。 （注） FlexConfig を使用して SNMP を設定した場合は、FTD API SNMP リソースを使用して設定をやり直す必要があります。SNMP を設定するためのコマンドは、FlexConfig では使用できなくなりました。FlexConfig ポリシーから SNMP FlexConfig オブジェクトを削除するだけで、変更を展開できます。その後、API を使用して機能を再設定するときに、それらのオブジェクトを参照として使用できます。

機能	説明
システムに保持されるバックアップファイルの最大数が 10 から 3 に減少。	システムでは、10 個ではなく最大 3 個のバックアップファイルがシステムに保持されます。新しいバックアップが作成されると、最も古いバックアップファイルが削除されます。必要な場合にシステムを回復するために必要なバージョンを入手できるように、バックアップファイルは異なるシステムにダウンロードしてください。
FTD API バージョンの下位互換性。	FTD バージョン 6.7 以降、ある機能の API リソースモデルがリリース間で変更されない場合、FTD API は古い API バージョンに基づくコールを受け入れることができます。機能モデルが変更された場合でも、古いモデルを新しいモデルに変換する論理的な方法があれば、古いコールが機能します。たとえば、v4 コールを v5 システムで受け入れることができます。コールのバージョン番号として「latest（最新）」を使用する場合、「古い」コールは、このシナリオでは v5 コールとして解釈されるため、下位互換性を利用するかどうかは、API コールの構築方法によって決まります。
FTD REST API バージョン 6（v6）。	ソフトウェアバージョン 6.7 用の FTD REST API はバージョン 6 です。API URL の v6 を使用するか、優先的に /latest/ を使用して、デバイスでサポートされている最新の API バージョンを使用していることを示せます。 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、FDM にログインして、[詳細オプション（More options）] ボタン（⋮）をクリックし、[APIエクスプローラ（API Explorer）] を選択します。

FDM バージョン 6.7.0 で廃止された機能

これらの FTD 機能はバージョン 6.7.0 の FDM 展開で廃止されました。

表 *11* : バージョン *6.7.0* で廃止された機能：*FDM* 展開

機能	アップグレードの影響	説明
安全性の低い Diffie-Hellman グループ、暗号化アルゴリズム、およびハッシュアルゴリズム	アップグレード後に展開ができないようにします。	次の FTD 機能のいずれかを使用している場合、アップグレード後の展開ができないことがあります。 • Diffie-Hellman グループ：2、5、および 24。 • 強力な暗号化の輸出規制を満たすユーザ向けの暗号化アルゴリズム：DES、3DES、AES-GMAC、AES-GMAC-192、AES-GMAC-256。輸出規制を満たしていないユーザの場合、DESは引き続きサポートされます（これが唯一のオプションです）。 • ハッシュアルゴリズム：MD5。 IKE プロポーザルまたは IPsec ポリシーでこれらの機能を使用している場合は、アップグレードする前に VPN 設定を変更して確認します。
FlexConfig コマンド	アップグレード後に展開ができないようにします。 アップグレード後に設定をやり直す必要があります。	バージョン 6.7.0 では、FDM を使用する FTD の次の FlexConfig CLI コマンドは廃止されます。 • **router eigrp**：[ルーティング（Routing）] ページの **[デバイス（Device）]**>**[ルーティング（Routing）]**>**[EIGRP]** で直接スマート CLI EIGRP オブジェクトを作成して、使用できます。 • **snmp-server**：FTD API を使用して SNMP バージョン 2c または 3 を設定できるようになりました。 関連付けられている FlexConfig オブジェクトを削除するまで、アップグレード後に展開することはできません。
次でのバックアップファイルの保持： FTD	なし。アップグレードによって、ローカルのバックアップは常に消去されます。	バージョン 6.7.0 では、FDM 管理の FTD デバイスが保存するバックアップファイルの数を 10 から 3 に減らします。 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ことをお勧めします。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。

機能	アップグレードの影響	説明
Microsoft Internet Explorer	ブラウザを切り替える必要があります。	Microsoft Internet Explorer を使用して Firepower Web インターフェイスをテストすることはなくなりました。Google Chrome、Mozilla Firefox、または Microsoft Edge に切り替えることをお勧めします。 詳細については、Web ブラウザの互換性 （8 ページ）を参照してください。
Firepower ソフトウェアを使用した ASA 5525-X、5545-X、および 5555-X デバイス	アップグレードは禁止されています。	ASA 5525-X、5545-X、および 5555-X のデバイスでは、FTD ソフトウェアのバージョン 6.7.0 以降にアップグレードしたり、このバージョンを新規インストールすることはできません。

以前に廃止された FDM 機能

アップグレードパスでバージョンをスキップする場合は、中間リリースの廃止された機能を確認してください。

FDM バージョン 6.6.0 で廃止された機能

これらの FTD 機能はバージョン 6.6.0 の FDM 展開で廃止されました。

表 *12*：バージョン *6.6.0* で廃止された機能：*FDM* 展開

機能	アップグレードの影響	説明
VMware 向け FTDv の e1000 インターフェイス	アップグレードされないようにします。	バージョン 6.6.0 では、VMware 向け FTDv の e1000 インターフェイスのサポートを終了します。vmxnet3 または ixgbe インターフェイスに切り替えるまで、アップグレードすることはできません。または、新しいデバイスを展開できます。 詳細については、『Cisco Firepower Threat Defense Virtual for VMware Getting Started Guide』を参照してください。

機能	アップグレードの影響	説明
安全性の低い Diffie-Hellman グループ、暗号化アルゴリズム、およびハッシュアルゴリズム	なし。ただし、今すぐ切り替える必要があります。	バージョン 6.6.0 では、次の FTD 機能は廃止されます。 • Diffie-Hellman グループ：2、5、および 24。 • 強力な暗号化の輸出規制を満たすユーザ向けの暗号化アルゴリズム：DES、3DES、AES-GMAC、AES-GMAC-192、AES-GMAC-256。輸出規制を満たしていないユーザの場合、DES は引き続きサポートされます（これが唯一のオプションです）。 • ハッシュアルゴリズム：MD5。 これらの機能はバージョン 6.7.0 で廃止されました。VPN で使用するために、IKE プロポーザルまたは IPSec ポリシーでこれらの機能を設定しないでください。できるだけ強力なオプションに変更してください。

FDM バージョン 6.5.0 で廃止された機能

これらの FTD 機能はバージョン 6.5.0 の FDM 展開で廃止されました。

表 *13 :* バージョン *6.5.0* で廃止された機能：*FDM* 展開

機能	アップグレードの影響	説明
デフォルトの HTTPS サーバ証明書	なし	バージョン 6.4.0.9 以降からアップグレードする場合、デフォルトの HTTPS サーバ証明書の lifespan-on-renew は 3 年に戻りますが、バージョン 6.6.0 以降で再び 800 日に更新されます。 現在のデフォルトの HTTPS サーバ証明書は、いつ生成されたかに応じて、次のように期限切れになるように設定されています。 • 6.4.0.9 以降のパッチ：800 日 • 6.4.0 ～ 6.4.0.8：3 年 • 6.3.0 およびすべてのパッチ：3 年 • 6.2.3：20 年

機能	アップグレードの影響	説明
VDB、GeoDB、および SRU 更新の手動アップロード	なし。ただし、バージョン 6.6.0 以降にアップグレードするまでこの機能は廃止されます。	バージョン 6.5.0 では、VDB、GeoDB、および SRU の更新を手動でデバイスにアップロードすることはできません。 この機能は、バージョン 6.4.0.10 以降のパッチ、およびバージョン 6.6.0 以降でサポートされています。バージョン 6.4.0.10 以降のパッチを実行している場合は、バージョン 6.5.0 を中間バージョンとして使用せずに、直接バージョン 6.6.0 以上にアップグレードすることをお勧めします。
ユニバーサル永久ライセンス予約（PLR）モード	なし。ただし、バージョン 6.6.0 以降にアップグレードするまでこの機能は廃止されます。	バージョン 6.5.0 は、ユニバーサル永久ライセンス予約（PLR）モードをサポートしていません。このモードでは、Cisco Smart Software Manager（CSSM）との直接通信を必要としないライセンスを適用できます。 この機能は、バージョン 6.4.0.10 以降のパッチ、およびバージョン 6.6.0 以降でサポートされています。バージョン 6.4.0.10 以降のパッチを実行している場合は、バージョン 6.5.0 を中間バージョンとして使用せずに、直接バージョン 6.6.0 以上にアップグレードすることをお勧めします。
次を搭載した ASA 5515-X：FTD	アップグレードは禁止されています。	ASA 5515-X デバイスでは、FTD バージョン 6.5.0 以降にアップグレードしたり、このバージョンを新規インストールすることはできません。

FDM バージョン 6.4.0 で廃止された機能

これらの FTD 機能はバージョン 6.4.0.x パッチの FDM 展開で廃止されました。

表 *14 :* バージョン *6.4.0.x* で廃止された機能：*FDM* 展開

機能	アップグレードの影響	説明
バージョン 6.4.0.7 出力最適化	パッチを適用すると、出力最適化処理がオフになります。	CSCvq34340 を軽減するため、FTD デバイスをバージョン 6.4.0.7+ にパッチすると、出力最適化処理がオフになります。これは、出力最適化機能が有効になっているか、無効になっているかに関係なく発生します。 （注） この問題が修正されているバージョン 6.6.0+ にアップグレードすることをお勧めします。機能を「有効」のままにすると、出力最適化がオンに戻ります。 バージョン 6.4.0 ～ 6.4.0.6 のままの場合は、FTD CLI から **no asp inspect-dp egress-optimization** を実行して出力最適化を手動で無効にする必要があります。 詳細については、ソフトウェアアドバイザリ『FTD traffic outage due to 9344 block size depletion caused by the egress optimization feature』を参照してください。

廃止された FlexConfig コマンドについて

このドキュメントでは、各バージョンの廃止された FlexConfig のオブジェクトおよびコマンドと、その他の廃止された機能が記載されています。FlexConfig が導入されたときに禁止されたコマンドを含む、禁止されたコマンドの完全なリストについては、コンフィギュレーションガイドを参照してください。

⚠

注意 ほとんどの場合、既存の FlexConfig 設定はアップグレード後も引き続き機能し、展開ができます。ただし、廃止されたコマンドを使用すると、展開の問題が発生する場合があります。

FlexConfig について

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 6.2.0（FMC 展開）またはバージョン 6.2.3（FDM 展開）以降では、スマート 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。ご使用の構成は自動的に変換されませ

ん。アップグレード後は、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ません。

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。

侵入ルールとキーワード

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が可能です。

侵入ルールを更新（SRU）すると、更新された新しい侵入ルールおよびプリプロッセサルール、既存のルールに対して変更された状態、および変更されたデフォルトの侵入ポリシーの設定が提供されます。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、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。

FMCのHow-Toウォークスルー

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） FMC 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 *15 :* 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。 バージョン 6.7.0 では、クラシックテーマのウォークスルーが廃止されたことに注意してください。ユーザ設定でテーマを切り替えることができます。
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。

問題	解決方法
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。

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。

Cisco Success Network

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。

初期設定および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。

Web 分析トラッキング

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。

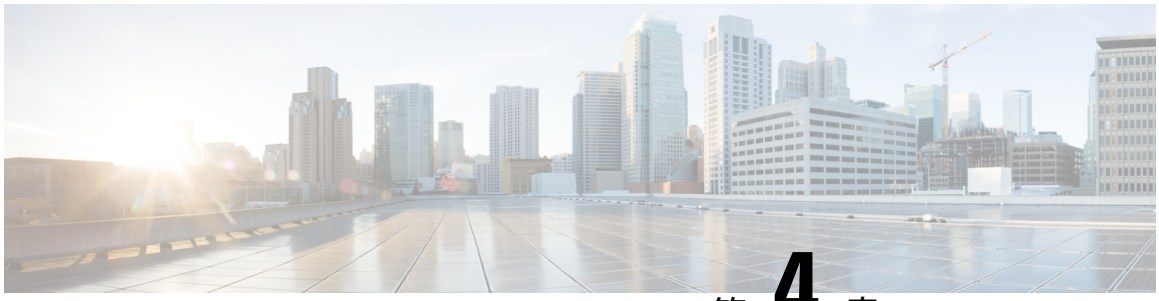
Web 分析トラッキングはデフォルトでオンになっています（バージョン 6.5.0 以降の EULA に承諾すると、Web分析トラッキングに同意したことになります）。ただし、初期設定の完了後にいつでもオプトアウトできます。

（注） バージョン 6.2.3 から 6.6.x へのアップグレードでは、Web 分析トラッキングを有効化（または再有効化）できます。これは、現在の設定がオプトアウトであっても発生する可能性があります。このデータの収集を拒否する場合は、アップグレードの後にオプトアウトしてください。6.7.0 以降へのアップグレードでは、現在の設定が適用されます。

Cisco Support Diagnostics

バージョン 6.5.0 以降では、 *Cisco Support Diagnostics*（「シスコのプロアクティブサポート」とも呼ばれる）は、設定および運用上の健全性データをシスコに送信し、自動化された問題検出システムを通じてそのデータを処理して問題をプロアクティブに通知できるようにします。また、この機能により、Cisco TACTAC ケースの過程でデバイスから必要な情報を収集することもできます。

初期設定および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。



第 4 章

Version6.7.0 へのアップグレード

この章では、重要なリリースに固有の情報を提供します。

Firepowerソフトウェアのアップグレードガイドラインについて

便宜上、このリリースノートでは、過去の Firepower ソフトウェアリリースの廃止機能とバージョン固有のアップグレードガイドラインが重複しています。ただし、対象バージョンのリリースノート、およびスキップするその他のメジャーリリースまたはメンテナンスリリースのリリースノートを必ずお読みください。

重要 アップグレードガイドラインは複数の場所に表示できます。このチェックリストを使用して、すべてを確認してください。

表 *16 : Firepower* ソフトウェアのアップグレードガイドラインのインデックス

✓	リソース	詳細
	Version6.7.0のガイドライン （66 ページ）	新規またはこのリリースに固有の重要なアップグレードガイドラインについては、これらを参照してください。
	以前に公開されたガイドライン （67 ページ）	アップグレードでバージョンがスキップされる場合は、これらを参照してください。
	一般的なガイドライン （78 ページ）	ガイドラインが変更されている可能性があるため、アップグレードプロセスに精通している場合でも、これらをお読みください。
	既知の問題 （135 ページ）	これらを読み、アップグレードに影響するバグを回避する準備を整えます。 アップグレードでバージョンがスキップされる場合は、スキップするメジャーバージョンの既知の問題も参照してください。「Cisco Firepower リリース ノート」を参照してください。
	特長と機能 （11 ページ）	アップグレードに影響する可能性のあるその他の項目については、これらをお読みください。廃止された機能では、特別にアップグレード前の構成変更が必要になる場合があります。 アップグレードでバージョンがスキップされる場合は、スキップしたバージョンの新機能に関するドキュメントもお読みください。「Cisco Firepower リリース ノート」を参照してください。

Version6.7.0のガイドライン

このチェックリストには、バージョン 6.7.0 の新規または固有のアップグレードガイドラインが含まれています。現在**バージョン 6.3.0 ～ 6.6.x** を実行している場合は、次のガイドラインを確認してください。

表 *17* : バージョン *6.7.0* 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 スイッチポートでの無効な VLAN ID によるアップグレードの失敗 （67 ページ）	Firepower 1010	6.4.0 ー 6.6.x	6.7.0 以降

Firepower 1010 スイッチポートでの無効な VLAN ID によるアップグレードの失敗

展開：Firepower 1010

アップグレード元：バージョン 6.4.0 ～ 6.6.x

直接アップグレード先：バージョン 6.7.0 以上

Firepower 1010 では、VLAN ID を 3968 ー 4047 の範囲にしてスイッチポートを設定した場合、FTD のバージョン 6.7.0 以上へのアップグレードは失敗します。これらの ID は内部使用専用です。

以前に公開されたガイドライン

このチェックリストには、中間リリースに適用されるアップグレードガイドラインが含まれています。現在バージョン **6.3.0 ー 6.5.0** を実行している場合は、次のガイドラインを確認してください。

表 *18* : 以前に公開されたバージョン *6.7.0* 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
	FMCv をアップグレードするには 28 GB の RAM が必要 （68 ページ）	FMCv	6.2.3 ～ 6.5.0.x	6.6.0 +
	FMC のアップグレード後にイベントが一時的に使用できない （69 ページ）	FMC	6.2.3 ～ 6.5.0.x	6.6.0 +
	Firepower 1000 シリーズ デバイスではアップグレード後に電源の再投入が必要 （70 ページ）	Firepower 1000 シリーズ	6.4.0	6.5.0 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
	FTD/FDM アップグレード時に削除される履歴データ （70 ページ）	FDM を使用した FTD	6.2.3 ～ 6.4.0.x	6.5.0 以降
	新しい URL カテゴリとレピュテーション （71 ページ）	任意（Any）	6.2.3 ～ 6.4.0.x	6.5.0 以降
	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（78 ページ）	Firepower 2100 シリーズ Firepower 4100/9300	6.2.3 ～ 6.3.0.x	6.4.0 以降

FMCv をアップグレードするには 28 GB の RAM が必要

展開：FMCv

アップグレード元：バージョン 6.5.0.x

直接アップグレード先：バージョン 6.6.0+

すべての FMCv 実装には同じ RAM 要件が適用され、32 GB が推奨、28 GB が必須となりました（FMCv 300 の場合は 64 GB）。仮想アプライアンスに割り当てられたメモリが 28 GB 未満の場合、バージョン 6.6.0+ へのアップグレードは失敗します。アップグレード後、メモリ割り当てを引き下げると、正常性モニタがアラートを発行します。

これらの新しいメモリ要件は、すべての仮想環境にわたって一貫した要件を適用し、パフォーマンスを向上させ、新しい機能を利用できるようにします。デフォルト設定を引き下げないことをお勧めします。使用可能なリソースによっては、パフォーマンスを向上させるために仮想アプライアンスのメモリと CPU の数を増やすことができます。FMCv のメモリ要件の詳細については、Cisco Firepower Management Center Virtual 入門ガイドを参照してください。

（注） バージョン 6.6.0 リリースの時点で、クラウドベースの FMCv の展開（AWS、Azure）でのメモリ不足インスタンスのタイプが完全に廃止されました。以前の Firepower バージョンであっても、これらを使用して新しい FMCv インスタンスを作成することはできません。既存のインスタンスは引き続き実行できます。

次の表に、メモリが不足している FMCv 展開のアップグレード前の要件を示します。

表 *19 :* バージョン *6.6.0+* にアップグレードする場合の *FMCv* のメモリ要件

プラットフォーム	アップグレード前のアクション	詳細
VMware	28 GB 以上（推奨 32 GB）を割り当てます。	最初に仮想マシンの電源をオフにします。 手順については、VMware のマニュアルを参照してください。
KVM	28 GB 以上（推奨 32 GB）を割り当てます。	手順については、ご使用の KVM 環境のマニュアルを参照してください。
AWS	インスタンスのサイズを変更します。 • c3.xlarge から c3.4xlarge へ。 • c3.2.xlarge から c3.4xlarge へ。 • c4.xlarge から c4.4xlarge へ。 • c4.2xlarge から c4.4xlarge へ。 また、新規展開用に c5.4xlarge インスタンスも用意しています。	サイズを変更する前にインスタンスを停止します。これを行うと、インスタンスストアのボリューム上のデータが失われるため、最初にインスタンスストアによってバックアップされたインスタンスを最初に移行してください。さらに、管理インターフェイスに復元力のある IP アドレスがない場合は、そのパブリック IP アドレスが解放されます。 手順については、Linux インスタンスの AWS ユーザガイドのインスタンスタイプの変更に関するマニュアルを参照してください。
Azure	インスタンスのサイズを変更します。 • Standard_D3_v2 から Standard_D4_v2 へ。	Azure ポータルまたは PowerShell を使用します。サイズを変更する前にインスタンスを停止する必要はありませんが、停止すると追加のサイズが表示される場合があります。サイズ変更により、実行中の仮想マシンが再起動されます。 手順については、Windows VM のサイズ変更に関する Azure のマニュアルを参照してください。

FMC のアップグレード後にイベントが一時的に使用できない

展開：FMC

アップグレード元：バージョン 6.5.0.x

直接アップグレード先：バージョン 6.6.0+

バージョン 6.6.0 では、接続およびセキュリティ インテリジェンス イベントに新しいデータストアを使用します。

アップグレードが完了し、FMC がリブートすると、履歴接続イベントとセキュリティ インテリジェンスイベントがバックグラウンドで移行され、リソースが制限されます。FMC モデル、システム負荷、および保存したイベント数に応じて、数時間から最大で 1 日かかることがあります。

履歴イベントは、経過時間ごとに、最新のイベントが最初に以降されます。移行されていないイベントは、クエリ結果やダッシュボードに表示されません。移行が完了する前に接続イベントデータベースの制限に達した場合（アップグレード後のイベントの場合など）、最も古い履歴イベントは移行されません。

ヒント　メニューバーの [システムステータス（System Status）] アイコンをクリックして、メッセージセンターでイベントの移行の進行状況をモニタします。

Firepower 1000 シリーズ デバイスではアップグレード後に電源の再投入が必要

展開：Firepower 1000 シリーズ デバイス

アップグレード元：バージョン 6.4.0.x

直接アップグレード先：バージョン 6.5.0+

バージョン 6.5.0 では、Firepower 1000/2100 および Firepower 4100/9300 シリーズ デバイス向けの FXOS CLI の「安全に消去する」機能が導入されています。

Firepower 1000 シリーズ デバイスでは、この機能を適切に動作させるには、バージョン 6.5.0+ にアップグレードした後にデバイスの電源を再投入する必要があります。自動リブートでは十分ではありません。サポートされているその他のデバイスでは、電源の再投入は必要ありません。

FTD/FDM アップグレード時に削除される履歴データ

展開：Firepower Device Manager

アップグレード元：バージョン 6.2.3 ～ 6.4.x

直接アップグレード先：バージョン 6.5.0 以降

データベース スキーマの変更により、すべての履歴レポート データがアップグレード中に削除されます。アップグレード後、履歴データをクエリしたり、履歴データをダッシュボードに表示したりすることはできません。

新しい URL カテゴリとレピュテーション

展開：すべて

アップグレード元：バージョン 6.2.3 ～ 6.4.0.x

直接アップグレード先：バージョン 6.5.0+

Cisco Talos Intelligence Group（Talos）は、URL の分類およびフィルタ処理のために、新しいカテゴリを導入し、レピュテーションの名前を変更しました。カテゴリの変更に関する詳細なリストについては、『Cisco Firepower Release Notes, Version 6.5.0』を参照してください。新しい URL カテゴリの説明については、Talos の「Intelligence Categories」サイトを参照してください。

また、ルール設定オプションは同じままですが、未分類およびレピュテーションのない URL の概念が新しくなっています。

- 未分類の URL は、疑わしい（Questionable）、ニュートラル（Neutral）、好ましい（Favorable）、信頼されている（Trusted）というレピュテーションのいずれかになります。

  [未分類（Uncategorized）] の URL はフィルタ処理できますが、レピュテーションによりさらに制約を追加することはできません。これらのルールは、レピュテーションに関係なく、すべての未分類 URL と一致します。

  カテゴリのない信頼されていない（Untrusted）ルールのような設定は存在しないことに注意してください。それ以外の場合、信頼されていない（Untrusted）レピュテーションの未分類 URL は、「悪意のあるサイト（Malicious Sites）」という新しい脅威カテゴリに自動的に割り当てられます。

- レピュテーションのない URL は任意のカテゴリに属することができます。

  レピュテーションのない URL をフィルタ処理することはできません。「レピュテーションなし」に対応するオプションはルールエディタにありません。ただし、レピュテーションに [すべて（Any）] を指定して URL をフィルタ処理することは可能で、その場合はレピュテーションのない URL が含まれます。これらの URL もカテゴリで制約する必要があります。Any/Any ルールに対するユーティリティはありません。

次の表に、アップグレードでの変更点の概要を示します。これらの変更は、ほとんどのお客様にとって最小限の影響で済むように設計されており、アップグレード後の展開を妨げることもありませんが、これらのリリースノートおよび現在の URL フィルタリングの設定を確認することを強くお勧めします。慎重な計画と準備は、誤った手順を回避することに加えて、アップグレード後のトラブルシューティングにかかる時間を短縮するのに役立ちます。

表 *20 :* アップグレード時の展開の変更

変更内容	詳細
URL ルールのカテゴリが変更されます。	アップグレードにより、次のポリシーで、新しいカテゴリセットのほぼ同等のルールが使用されるように URL ルールが変更されます。 • アクセス コントロール • SSL • QoS（FMC のみ） • 相関（FMC のみ） これらの変更により、余分なルールや無効になったルールが生じ、パフォーマンスが低下する可能性があります。マージされたカテゴリが設定に含まれている場合、許可またはブロックされる URL が若干変更されることがあります。
URL ルールのレピュテーションの名前が変更されます。	アップグレードにより、新しいレピュテーション名を使用するように URL ルールが変更されます。 **1.** 信頼されていない（「高リスク」だった） **2.** 疑わしい（「疑わしいサイト」だった） **3.** ニュートラル（「セキュリティ リスクのある無害なサイト」だった） **4.** 好ましい（「無害なサイト」だった） **5.** 信頼されている（「十分に既知」だった）
URL キャッシュをクリアします。	アップグレードによって URL キャッシュがクリアされます。このキャッシュには、システムが以前にクラウドで検索した結果が含まれています。ローカル データ セットに含まれていない URL については、アクセス時間が一時的に少し長くなることがあります。
「レガシー」イベントにラベルを付けます。	すでにログに記録されているイベントの場合、アップグレードにより、関連する URL のカテゴリおよびレピュテーション情報が「レガシー」としてラベル付けされます。これらのレガシー イベントは時間の経過とともにデータベースからエージ アウトします。

URL カテゴリおよびレピュテーションのアップグレード前のアクション

アップグレードする前に、次のアクションを実行します。

表 *21* : アップグレード前のアクション

アクション	詳細
アプライアンスが Talos のリソースにアクセスできることを確認します。	アップグレード後、システムは次のシスコのリソースと通信できる必要があります。 • https://regsvc.sco.cisco.com/ - 登録 • https://est.sco.cisco.com/ - セキュア通信のための証明書を取得 • https://updates-talos.sco.cisco.com/ - クライアント/サーバマニフェストを取得 • http://updates.ironport.com/ - データベースのダウンロード（注：ポート 80 を使用） • https://v3.sds.cisco.com/ - クラウドクエリ クラウドクエリサービスは、次の IP アドレスブロックも使用します。 • IPv4 クラウドクエリ： • 146.112.62.0/24 • 146.112.63.0/24 • 146.112.255.0/24 • 146.112.59.0/24 • IPv6 クラウドクエリ： • 2a04:e4c7:ffff::/48 • 2a04: e4c7: fffe::/48
潜在的なルールの問題を特定します。	今後の変更点を理解します。現在の URL フィルタリング設定を調べて、アップグレード後に実行する必要があるアクションを特定します（次の項を参照）。 （注） 廃止されたカテゴリを使用する URL ルールをこの時点で変更することができます。そうしない場合、それらを使用するルールによってアップグレード後の展開が妨げられます。 FMC 展開では、アクセスコントロールのルールや下位ポリシー（SSL など）のルールを含む、ポリシーの現在の保存されている設定に関する詳細情報を提供する、アクセスコントロール ポリシー レポートを生成することを推奨します。URL ルールごとに、現在のカテゴリ、レピュテーション、関連付けられているルール アクションが表示されます。FMC で **[Policies]** > **[Access Control]** を選択し、該当するポリシーの横にあるレポート アイコン（  ）をクリックします。

URL カテゴリおよびレピュテーションのアップグレード後のアクション

アップグレード後に URL フィルタリング設定を再確認し、できるだけ早く次のアクションを実行する必要があります。展開のタイプとアップグレードによって行われた変更に応じて、一部（すべてではない）の問題が GUI でマークされることがあります。たとえば、FMC/FDM のアクセス コントロール ポリシーでは、[警告の表示（Show Warnings）]（FMC）または [問題ルールの表示（Show Problem Rules）] (FDM) をクリックできます。

表 *22*：アップグレード後の操作

アクション	詳細
廃止されたカテゴリをルールから削除します。必須。	アップグレードでは、廃止されたカテゴリを使用する URL ルールは変更されません。これらを使用するルールは展開を阻止します。 FMC では、これらのルールがマークされます。
新しいカテゴリを含めるルールを作成または変更します。	ほとんどの新しいカテゴリは脅威を特定します。これらのカテゴリを使用することを強くお勧めします。 FMC では、この新しいカテゴリはこのアップグレード後にマークされませんが、今後、Talos によってカテゴリが追加される場合があります。この場合は新しいカテゴリがマークされます。
マージされたカテゴリの結果として変更されたルールを評価します。	影響を受けたカテゴリのいずれかが含まれている各ルールに影響を受けたすべてのルールが含まれるようになります。元のカテゴリが異なるレピュテーションに関連付けられていた場合、新しいルールはさらに広い、より包含的なレピュテーションに関連付けられます。以前と同様に URL をフィルタリングするには、いくつかの設定を変更する必要があります。「マージされた URL カテゴリを持つルールのガイドライン（75 ページ）」を参照してください。 変更内容とプラットフォームがルールの警告を処理する方法に応じて、変更がマークされることがあります。たとえば、FMC は完全に冗長および完全にプリエンプション処理されたルールをマークしますが、部分的に重複したルールはマークしません。
分割されたカテゴリの結果として変更されたルールを評価します。	アップグレードにより、URL ルール内の古い単一のカテゴリが新しいカテゴリすべてに置き換えられ、新しいカテゴリは古いカテゴリにマッピングされます。これにより URL のフィルタリング方法は変更されませんが、影響を受けるルールを変更して、新しい精度を活用することができます。 これらの変更はマークされません。

アクション	詳細
名前が変更されたカテゴリまたは**変更されていない**カテゴリを把握します。	特に対処の必要はありませんが、これらの変更に注意する必要があります。 これらの変更はマークされません。
未分類および**レピュテーションのない**URL の処理方法を評価します。	未分類の URL とレピュテーションのない URL を使用できるようになりましたが、未分類の URL をレピュテーションでフィルタ処理することも、レピュテーションのない URL をフィルタ処理することもできません。 [未分類（Uncategorized）] カテゴリまたは [すべて（Any）] のレピュテーションでフィルタ処理されるルールが、期待どおりに動作することを確認してください。

マージされた URL カテゴリを持つルールのガイドライン

アップグレード前に URL フィルタリング設定を確認する場合は、次のシナリオとガイドラインのどちらが適用されるかを決定します。これにより、アップグレード後の設定が予想どおりに実行され、問題を解決するためのクイックアクションを実行できるようになります。

表 *23 :* マージされた *URL* カテゴリを持つルールのガイドライン

ガイドライン	詳細
ルールの順序によってトラフィックに一致するルールを決定	同じカテゴリを含むルールを検討する場合は、トラフィックが、その条件を含むリスト内の最初のルールと一致することに注意してください。
同じルール内のカテゴリと異なるルール内のカテゴリ	単一のルール内でカテゴリをマージすると、ルール内の単一のカテゴリにマージされます。たとえば、カテゴリ A とカテゴリ B がマージされてカテゴリ AB になり、カテゴリ A とカテゴリ B を持つルールがある場合、マージ後にルールは単一のカテゴリ AB を保持します。 異なるルールのカテゴリをマージすると、マージ後に各ルールで同じカテゴリを持つルールが個別に生成されます。たとえば、カテゴリ A とカテゴリ B がマージされてカテゴリ AB になり、カテゴリ A を持つルール 1 とカテゴリ B を持つルール 2 がある場合、マージ後にルール 1 とルール 2 にはカテゴリ AB がそれぞれ含まれます。この状況を解決する方法は、ルールの順序、ルールに関連付けられたアクションとレピュテーションレベル、ルールに含まれる他の URL カテゴリ、およびルールに含まれる非 URL 条件によって異なります。
関連付けられたアクション	異なるルールのマージされたカテゴリが異なるアクションに関連付けられている場合、マージ後に、同じカテゴリに対して異なるアクションを持つ 2 つ以上のルールが生成される場合があります。

ガイドライン	詳細
関連付けられているレピュテーションレベル	マージの前に異なるレピュテーションレベルに関連付けられたカテゴリが単一のルールに含まれている場合、マージされたカテゴリは、より包括的なレピュテーションレベルに関連付けられます。たとえば、カテゴリ A が特定のルールで [すべてのレピュテーション（Any reputation）] に関連付けられており、カテゴリ B が同じルールでレピュテーションレベル [3 - セキュリティリスクのある無害なサイト（3 - Benign sites with security risks）] に関連付けられている場合、マージ後に、そのルール内のカテゴリ AB は [すべてのレピュテーション（Any reputation）] に関連付けられます。
重複および冗長カテゴリとルール	マージ後、異なるルールには、異なるアクションとレピュテーションレベルに関連付けられている同じカテゴリが含まれる場合があります。 冗長ルールは完全に重複しているとは限りませんが、ルール順序が前にある別のルールが一致する場合、トラフィックに一致しなくなる可能性があります。たとえば、ルール 1 とカテゴリ A（[すべてのレピュテーション（Any Reputation）] に適用される）を事前マージし、ルール 2 とカテゴリ B（レピュテーション 1-3 のみに適用される）を事前マージする場合、マージ後に、ルール 1 とルール 2 の両方にカテゴリ AB が含まれるようになるが、ルール順序でルール 1 の順序が前にあると、ルール 2 が一致することはありません。 FMC において、同一のカテゴリとレピュテーションを持つルールでは警告が表示されます。ただし、これらの警告は、含まれているカテゴリが同じですが、レピュテーションが異なるルールを示すことはありません。 注意：重複または冗長カテゴリを解決する方法を決定する際には、ルールのすべての条件を考慮してください。
ルール内の他の URL カテゴリ	マージされた URL を含むルールには、他の URL カテゴリも含まれている場合があります。したがって、マージ後に特定のカテゴリが複製された場合は、これらのルールを削除するのではなく、変更する必要があることがあります。
ルール内の非 URL 条件	マージされた URL カテゴリを含むルールには、アプリケーション条件などの他のルール条件も含まれている場合があります。したがって、マージ後に特定のカテゴリが複製された場合は、これらのルールを削除するのではなく、変更する必要があることがあります。

次の表の例ではカテゴリ A とカテゴリ B を使用しています。現在はカテゴリ AB にマージされています。2 つのルールの例では、ルール 1 はルール 2 よりも前に表示されます。

表 *24 :* マージされた *URL* カテゴリを持つルールの例

シナリオ	アップグレード前	アップグレード後
同じルール内のマージされたカテゴリ	ルール 1 にはカテゴリ A とカテゴリ B が含まれる。	ルール 1 にはカテゴリ AB が含まれる。
異なるルール内でマージされたカテゴリ	ルール 1 にはカテゴリ A が含まれる。 ルール 2 にはカテゴリ B が含まれる。	ルール 1 にはカテゴリ AB が含まれる。 ルール 2 にはカテゴリ AB が含まれる。 具体的な結果は、リスト内のルールの順序、レピュテーションレベル、および関連付けられたアクションによって異なります。また、冗長性を解決する方法を決定する際に、ルール内の他のすべての条件も考慮する必要があります。
異なるルール内でマージされたカテゴリには異なるアクションが含まれる （レピュテーションは同じ）	ルール 1 には [許可（Allow）] に設定されたカテゴリ A が含まれる。 ルール 2 には [ブロック（Block）] に設定されたカテゴリ B が含まれる。 （レピュテーションは同じ）	ルール 1 には [許可（Allow）] に設定されたカテゴリ AB が含まれる。 ルール 2 には [ブロック（Block）] に設定されたカテゴリ AB が含まれる。 ルール 1 は、このカテゴリのすべてのトラフィックに一致します。 ルール 2 がトラフィックに一致することはなく、カテゴリとレピュテーションの両方が同じであるため、マージ後に警告を表示した場合は、警告インジケータが表示されます。
同じルール内でマージされたカテゴリには異なるレピュテーションレベルが含まれる	ルール 1 には次が含まれます。 レピュテーション Any のカテゴリ A レピュテーション 1-3 のカテゴリ B	ルール 1 にはレピュテーション Any のカテゴリ AB が含まれる。

シナリオ	アップグレード前	アップグレード後
異なるルール内でマージされたカテゴリには異なるレピュテーションレベルが含まれる	ルール 1 にはレピュテーション Any のカテゴリ A が含まれる。 ルール 2 にはレピュテーション 1-3 のカテゴリ B が含まれる。	ルール 1 にはレピュテーション Any のカテゴリ AB が含まれる。 ルール 2 にはレピュテーション 1-3 のカテゴリ AB が含まれる。 ルール 1 は、このカテゴリのすべてのトラフィックに一致します。 ルール 2 がトラフィックに一致することはありませんが、レピュテーションが同一でないため、警告インジケータは表示されません。

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。

一般的なガイドライン

これらの一般的なガイドラインは、すべてのアップグレードに適用されます。

アプライアンスの正常性と通信

アップグレードプロセスの間、展開環境内のアプライアンスが正常に通信していること、およびヘルスモニタによって報告された問題がないことを確認します。マイナーな問題がメジャーな問題になる前に解決します。

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。

アップグレード前のチェックリスト

このチェックリストは、一般的なアップグレードの問題を回避できるアクションを示しています。 ただし、このリストは包括的なものではありません。詳細な手順については、該当するアップグレードガイド（「アップグレード手順 （94 ページ）」）を参照してください。

表 *25 : Firepower* ソフトウェアのアップグレード前チェックリスト

✓	アクション	詳細
	導入評価。	FirePOWER アプライアンスをアップグレードする前に、展開の現在の状態を判断します。状況を理解することにより、目的を達成する方法を決定します。 少なくとも次の項目に回答できる必要があります。 • どんなアプライアンスがありますか、またどの FirePOWER バージョンを実行していますか。どのバージョンを実行したいですか、またそのバージョンは実行可能ですか。直接アップグレードできますか。FMC 展開では、FMC デバイスの互換性を維持できますか。 • アプライアンスのいずれかで個別のオペレーティングシステムのアップグレードが必要ですか。ホスティング環境のアップグレードを必要とする仮想アプライアンスはありますか。 • ハイアベイラビリティ/スケーラビリティを実現するように設定されていますか。デバイスは、IPS として、ファイアウォールとして、パッシブに展開されていますか。

✓	アクション	詳細
	管理ネットワークの帯域幅を確認します。	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ったりする可能性があります。アップグレードする前に、FMC、またはFTDデバイスの場合は独自の内部Webサーバのいずれかから、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。 『Firepower Management Centerから管理対象装置へのデータをダウンロードするためのガイドライン』（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。
	アプライアンスへのアクセスを確認します。	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。FMCの展開では、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。
	設定変更を計画します。	主要なアップグレードでは特に、アップグレードの前または後に、アップグレードにより重要な設定変更が発生することがあります。たとえば、廃止されたFlexConfigコマンドは、アップグレード後の展開の問題を引き起こす可能性があります。 「Firepowerソフトウェアのアップグレードガイドラインについて（65ページ）」のチェックリストを使用して、潜在的な問題を特定します。

✓	アクション	詳細
	バックアップを実行します。	アップグレードの前後に Firepower アプライアンスをバックアップします（サポートされている場合）。 • 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。 **注意** Firepower アプライアンスを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ことを強くお勧めします。アプライアンスに残っているバックアップは、手動またはアップグレードプロセスによって削除できます（アップグレードプロセスでは、ローカルに保存されたバックアップが消去される）。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、セキュリティやライセンス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。
	準備状況チェックを実行します。	FMC展開では、準備状況チェックをお勧めします。このチェックにより、Firepowerをアップグレードするためのアプライアンスの準備状況を評価できます。このチェックにより、データベース整合性、バージョン不一致、デバイス登録などの問題を識別できます。

✓	アクション	詳細
	アップグレードをスケジュール設定します。1007	アップグレードのスケジュール設定は、中断による展開環境への影響が最も小さい時間に行うことを推奨します。 メンテナンスウィンドウをスケジュールするときは、トラフィックフローおよびインスペクションへの影響と、アップグレードにかかる可能性がある時間を考慮します。また、ウィンドウで実行する必要があるタスクと、事前に実行できるタスクを検討します。慎重な計画と準備で中断を最小限に抑えます。メンテナンスウィンドウがアップグレードパッケージの取得およびプッシュ、準備状況チェックの実行、バックアップの作成などを行うまで待機しないようにします。
	NTP 同期を確認します。	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。
	ASA FirePOWER デバイスで ASA REST API を無効化します。	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`。
	設定を展開します。	アップグレードする前に古いデバイスに設定を展開すると、失敗する可能性が減少します。 一部の展開では、設定が古い場合、アップグレードがブロックされることがあります。 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、いくつかの設定を展開することで Snort が再起動されます。これにより、トラフィックのインスペクションが中断し、デバイスのトラフィックの処理方法によっては、再起動が完了するまでトラフィックが中断する場合があります。詳細については、トラフィック フロー、検査、およびデバイス動作 （86 ページ） を参照してください。

✓	アクション	詳細
	実行中のタスクを確認します。	アップグレードする前に、重要なタスクが完了していることを確認します。アップグレードの開始時に実行中のタスクは停止し、失敗したタスクとなり、再開できません。 また、アップグレード中に実行するようにスケジュールされたタスクを確認し、それらをキャンセルまたは延期することをお勧めします。バージョン 6.7.0 以降の FMC 展開では、アップグレードでスケジュールされたタスクが自動的に延期されるようになりました。アップグレード中に開始するようにスケジュールされたタスクは、アップグレード後の再起動の 5 分後に開始されます。
	ディスク容量を確認します。	最終的なディスク容量のチェックを実行します。空きディスク容量が十分でない場合、アップグレードは失敗します。詳細については、時間テストとディスク容量の要件 （83 ページ）を参照してください。

アップグレードする最小バージョン

次のように Version6.7.0 に直接アップグレードできます。特定のメンテナンスリリースまたはパッチレベルを実行する必要はありません。

表 *26 : Firepower* ソフトウェアをバージョン *6.7* にアップグレードするための最小バージョン。*0*

Platform	最小バージョン
Firepower Management Center	6.3.0
Firepower デバイス	6.3.0 FXOS 2.9.1.131 以降のビルド （Firepower 4100/9300 に必要）。

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。
- 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（アップグレード前かアップグレード中かにかかわらない）。
- 準備状況チェック。

- VDB と SRU の更新。
- 設定の展開。
- リブート（値が別途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 6.7.0 の時間とディスク容量

表 *27 :* バージョン *6.7.0* の時間とディスク容量

[Platform]	ボリュームの容量	必要容量	FMC の容量	アップグレード時間	リブート時間
FMC	13.6 GB	70 MB	—	46 分	9 分
FMCv：VMware 6.0	15.5 GB	64 MB	—	35 分	8 分
Firepower 1000 シリーズ	430 MB	11 GB	2 GB	17 分	16 分
Firepower 2100 シリーズ	500 MB	11 GB	1.1 GB	15 分	16 分
Firepower 4100 シリーズ	10 MB	10 GB	1.1 GB	10 分	12 分
Firepower 4100 シリーズコンテナインスタンス	8 MB	9.5 GB	1.1 GB	10 分	9 分
Firepower 9300	64 MB	11.1 GB	1.1 GB	13 分	12 分
ASA 5500-X シリーズ with FTD	8.7 GB	96 KB	1.1 GB	26 分	13 分

[Platform]	ボリュームの容量	必要容量	FMC の容量	アップグレード時間	リブート時間
FTDv：VMware 6.0	8.1 GB	26 KB	1.1 GB	14 分	18 分
ASA FirePOWER	10.3 GB	64 MB	1.3 GB	62 分	11 分
NGIPSv：VMware 6.0	5.5 GB	54 MB	840 MB	10 分	6 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 シャーシ

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 シャーシ：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 *28 : FXOS* アップグレード中のトラフィックの動作

導入	メソッド	トラフィックの動作
スタンドアロン	—	廃棄

導入	メソッド	トラフィックの動作
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。
シャーシ内クラスタ（Firepower 9300 のみ）	ハードウェアバイパス有効：[Bypass: Standby] または [Bypass-Force]。（6.1 以降）	検査なしで受け渡される。
	ハードウェアバイパス無効：[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。
	ハードウェアバイパスモジュールなし。	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

アップグレード中、Firepower デバイス/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。アップグレードの開始時にメンテナンスモードを開始すると、トラフィックインスペクションが 2 ー 3 秒中断します。インターフェイスの構成により、その時点とアップグレード中の両方のスタンドアロンデバイスによるトラフィックの処理方法が決定されます。

表 *29 : 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 コンフィギュレーション		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。	廃棄

インターフェイス コンフィギュレーション		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、ハードウェアバイパス強制が有効：[Bypass: Force]（6.1 以上）。	ハードウェアバイパスを無効にするか、スタンバイモードに戻すまで、インスペクションなしで合格。
	インラインセット、ハードウェアバイパス スタンバイ モード：[Bypass: Standby]（6.1 以上）。	デバイスがメンテナンスモードの場合、アップグレード中にドロップされます。その後、デバイスがアップグレード後の再起動を完了する間、インスペクションなしで合格します。
	インラインセット、ハードウェアバイパスが無効：[Bypass: Disabled]（6.1 以上）。	廃棄
	インラインセット、ハードウェアバイパス モジュールなし。	廃棄
	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。データ セキュリティ モジュールを最初にアップグレードして、その後コントロールモジュール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。

コントロール 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。

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 構成ガイド』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 : FTD* 展開時のトラフィックの動作

インターフェイス コンフィギュレーション		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。	廃棄
IPS のみのインターフェイス	インラインセット、[Failsafe] が有効または無効（6.0.1 ～ 6.1）。	検査なしで受け渡される。 [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 Fail Open: Down]：無効（6.2 以降）	廃棄
	インラインセット、[Snort Fail Open: Down]：有効（6.2 以降）	検査なしで受け渡される。
	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。

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

アップグレード中、Firepower デバイスはメンテナンスモードで稼働します。アップグレードの開始時にメンテナンスモードを開始すると、トラフィック インスペクションが 2 ー 3 秒中断

します。インターフェイスの構成により、その時点とアップグレード中の両方のスタンドアロンデバイスによるトラフィックの処理方法が決定されます。

表 *31 : 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 コンフィギュレーション		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。	廃棄
IPS のみのインターフェイス	インラインセット、ハードウェアバイパス強制が有効：[Bypass: Force]（Firepower 2100 シリーズ、6.3 以上）。	ハードウェアバイパスを無効にするか、スタンバイモードに戻すまで、インスペクションなしで合格。
	インラインセット、ハードウェアバイパス スタンバイ モード：[Bypass: Standby]（Firepower 2100 シリーズ、6.3 以上）。	デバイスがメンテナンスモードの場合、アップグレード中にドロップされます。その後、デバイスがアップグレード後の再起動を完了する間、インスペクションなしで合格します。
	インラインセット、ハードウェアバイパスが無効：[Bypass: Disabled]（Firepower 2100 シリーズ、6.3 以上）。	廃棄
	インラインセット、ハードウェアバイパス モジュールなし。	廃棄
	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 構成ガイド』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 *32 : FTD* 展開時のトラフィックの動作

インターフェイス コンフィギュレーション		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。	廃棄
IPS のみのインターフェイス	インラインセット、[Failsafe] が有効または無効（6.0.1 ～ 6.1）。	検査なしで受け渡される。 [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 Fail Open: Down]：無効（6.2 以降）	廃棄
	インラインセット、[Snort Fail Open: Down]：有効（6.2 以降）	検査なしで受け渡される。
	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。

ASA FirePOWER アップグレード時の動作

ASA FirePOWER module にトラフィックをリダイレクトする ASA サービス ポリシーは、Firepower ソフトウェア アップグレードの間（Snort プロセスを再起動する特定の設定を導入するときなど）にモジュールがトラフィックを処理する方法を決定します。

表 *33 : 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 リダイレクションのポリシー	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
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 プロセスを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 構成ガイド』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 *34 : 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 コンフィギュレーション	トラフィックの動作
インライン	切断

インターフェイス コンフィギュレーション	トラフィックの動作
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
Passive	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 構成ガイド』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 *35 : NGIPSv* 展開時のトラフィックの動作

インターフェイス コンフィギュレーション	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
Passive	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、次のいずれかのドキュメントを参照してください。

表 *36 : Firepower* アップグレード手順

タスク	ガイド
FMC 展開のアップグレード。	Cisco Firepower Management Center Upgrade Guide

タスク	ガイド
FDM を使用した Firepower Threat Defense ソフトウェアのアップグレード。	Firepower Device Manager 用 Cisco Firepower Threat Defense 構成ガイド アップグレード先のバージョンではなく、現在実行している FTD バージョンのガイドの「システム管理」の章を参照してください。
Firepower 4100/9300 シャーシの FXOS のアップグレード。	Cisco Firepower 4100/9300 Upgrade Guide
ASDM を使用した ASA FirePOWER モジュールのアップグレード。	Cisco ASA Upgrade Guide
での ROMMON イメージのアップグレード。	Cisco ASA and Firepower Threat Defense Reimage Guide 「*Upgrade the ROMMON Image*」のセクションを参照してください。常に最新のイメージがあることを確認してください。

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
- 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

Firepower ソフトウェア アップグレード パッケージを検索するには、Firepower アプライアンス モデルを選択または検索し、現在のバージョンの Firepower ソフトウェアのダウンロード ページを参照します。使用可能なアップグレード パッケージは、インストール パッケージ、ホットフィックス、およびその他の該当するダウンロードとともに表示されます。

ヒント インターネットにアクセスできる FMC は、手動でダウンロードできるようになってから約 2 週間後に、シスコから Firepower メンテナンスリリース（Version6.7.x3 桁番号のアップグレード）を直接ダウンロードできます。次の場合、シスコからの直接ダウンロードはサポートされていません。

- メジャーリリース。
- バージョン 6.6 以降へのほとんどのパッチ。
- FDM または ASDM 展開。

ファミリまたはシリーズのすべての Firepower モデルに同じアップグレードパッケージを使用します。アップグレードパッケージのファイル名には、プラットフォーム、パッケージタイプ（アップグレード、パッチ、ホットフィックス）、および Firepower のバージョンが反映されています。 メンテナンスリリースでは、アップグレード パッケージ タイプが使用されることに注意してください。

次に例を示します。

- パッケージ：`Cisco_Firepower_Mgmt_Center_Upgrade-6.6.0-90.sh.REL.tar`
- プラットフォーム： Firepower Management Center
- パッケージタイプ：アップグレード
- バージョンおよびビルド：6.6.0-90
- ファイル拡張子：sh.REL.tar

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、アップグレードパッケージとホットフィックスパッケージは署名付きのアーカイブになっています。署名付きの（.tar）パッケージは解凍しないでください。

（注） 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、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。

表 *37 : Firepower* ソフトウェア アップグレード パッケージ

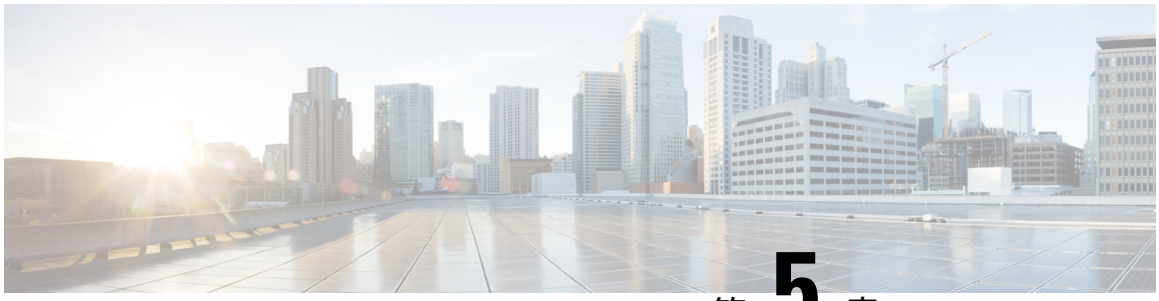
Platform	パッケージ
FMC/FMCv	Cisco_Firepower_Mgmt_Center
Firepower 1000 シリーズ	Cisco_FTD_SSP-FP1K
Firepower 2100 シリーズ	Cisco_FTD_SSP-FP2K

Platform	パッケージ
Firepower 4100/9300 シャーシ	Cisco_FTD_SSP
FTD を搭載した ASA 5500-X シリーズ FTD を搭載した ISA 3000 FTDv	Cisco_FTD
ASA FirePOWER	Cisco_Network_Sensor
NGIPSv	Cisco_Firepower_NGIPS_Virtual

オペレーティングシステムのアップグレードパッケージ

オペレーティングシステムのアップグレードパッケージの詳細については、次のガイドの「アップグレードの計画」の章を参照してください。

- Cisco ASA Upgrade Guide（ASA OS の場合）
- Cisco Firepower 4100/9300 Upgrade Guide（FXOSの場合）



第 5 章

更新プログラムのアンインストール

FDM 展開では、メジャーリリースとメンテナンスリリースを復元できます。これにより、Firepower Threat Defense がアップグレード前の状態に戻ります。

（注） 復元は、FMC または ASDM の展開ではサポートされていません。パッチでは復元もサポートされていません。ただし、FMC や ASDM の展開でパッチをアンインストールできます。手順については、パッチのリリースノートを参照してください。

詳細については、以下を参照してください。

- アンインストール、復元、再イメージ化の選択 （99 ページ）
- 復元についての注意事項と制約事項 （100 ページ）
- メジャーアップグレードまたはメンテナンスアップグレードの復元 （102 ページ）

アンインストール、復元、再イメージ化の選択

次の表では、以前のリリースに戻すためのオプションを、一般的な方法から順に説明します。これらのオプションは、展開のタイプや削除するアップグレードのタイプによって異なります。ホットフィックスをアンインストールしないように注意してください。代わりに、Cisco TAC にお問い合わせください。

表 *38 :* 以前のリリースに戻すためのオプション

導入	メソッド	Removes	説明
任意（Any）	再イメージ化	任意のレベルのソフトウェア	わずかな例外を除き、アプライアンスを工場出荷時のデフォルトに戻します。パッチレベルに再イメージ化することはできません。 再イメージ化した後は、設定を最初からやり直す必要があります。以前にエクスポートした設定をインポートしたり、バックアップから復元したりできます。 詳細については、ソフトウェアの新規インストール （103 ページ）を参照してください。
FTD with FDM	[元に戻す（Revert）]	メジャーおよびメンテナンスアップグレード	アプライアンスを最後のメジャーアップグレードまたはメンテナンスアップグレードの直前の状態に戻します（スナップショットとも呼ばれます）。パッチ適用後に復元すると、パッチも必然的に削除されます。 復元の後、アップグレードと復元の間に行った設定変更があればやり直す必要があります。
FMC および管理対象デバイス ASDM を使用した ASA FirePOWER	アンインストール	パッチのみ	アップグレード前に実行していたパッチレベルにアプライアンスを戻します。設定は変更されません。 パッチのアンインストールの詳細については、パッチのリリースノートを参照してください。

復元についての注意事項と制約事項

復元に適用される重要なガイドラインと制限事項は、次のとおりです。

復元がサポートされる状況は限られている

メジャーアップグレードとメンテナンスアップグレードは、FDM 展開でのみ復元できます。アンインストール、復元、再イメージ化の選択 （99 ページ）を参照してください。

スナップショット復元

復元すると、Firepower ソフトウェアは、最後のメジャーアップグレードまたはメンテナンスアップグレード（スナップショットとも呼ばれます）の直前の状態に戻ります。パッチ適用後に復元すると、パッチも必然的に削除されます。復元の後、アップグレードと復元の間に行った設定変更があればやり直す必要があります。

ディスク領域を節約するために復元スナップショットを削除できますが、復元の機能が失われます。

復元しても FXOS はダウングレードされない

Firepower 4100/9300 シャーシの場合、Firepower のメジャーバージョンには特別に認定および推奨されている付随の FXOS バージョンがあります。つまり、Firepower ソフトウェアを復元すると、推奨されていないバージョンの FXOS（新しすぎる）を稼働する可能性があります。

新しいバージョンの FXOS は旧バージョンの Firepower と下位互換性がありますが、シスコでは推奨の組み合わせについて拡張テストを実施しています。FXOS をダウングレードすることはできないため、このような状況下で推奨の組み合わせを稼働するには、完全な再イメージ化が必要になります。

詳細については、Cisco Firepower Compatibility Guideを参照してください。

ハイア ベイラビリティ ユニットの同時復元

FTD ハイアベイラビリティペアの両方のユニットを復元する必要がある場合は、両方のユニットで同時に復元を開始することを推奨します。両方のユニットでセッションを開き、それぞれで復元が可能であることを確認してから、プロセスを開始します。

NTP 同期の確認

復元する前に、時刻の設定で使用している 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、アンインストールが失敗する可能性があります。時刻を確認するには、**show time** CLI コマンドを使用します。

アプライアンスへのアクセス、通信、正常性

Firepower デバイスは、（インターフェイス設定に応じて）復元中、または復元が失敗した場合に、トラフィックを渡すことを停止できます。Firepower デバイスを復元する前に、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。

復元中のアプライアンスに対して変更の展開、手動での再起動、またはシャットダウンは行わないでください。進行中の復元を再起動しないでください。復元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。復元に失敗する、アプライアンスが応答しないなど、復元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。

トラフィック フロー、検査、およびデバイス動作

復元時のトラフィックフローとインスペクションの中断は、アップグレード時に発生する中断と同じです。復元は、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。詳細については、トラフィック フロー、検査、およびデバイス動作 （86 ページ）を参照してください。

メジャーアップグレードまたはメンテナンスアップグレードの復元

FDM から復元を実行するには、次の手順を使用します。FDM を使用できない場合は、**upgrade revert** FTD CLI コマンドを使用します。**show upgrade revert-info** コマンドを使用すると、システムがどのバージョンに戻るのかを確認できます。

始める前に

復元についての注意事項と制約事項 （100 ページ）を読み、理解します。

ステップ 1 [Device] を選択し、次に [Updates summary] の [View Configuration] をクリックします。

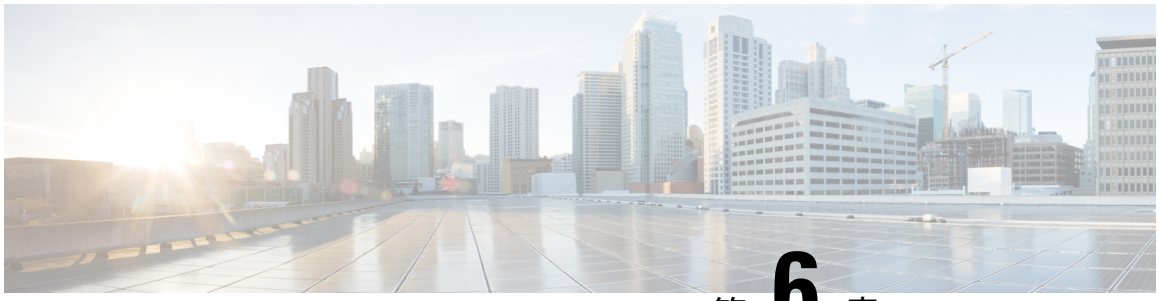
ステップ 2 [System Upgrade] セクションで、[Revert Upgrade] リンクをクリックします。

現在のバージョンと復元されるバージョンを示す確認ダイアログボックスが表示されます。復元できるバージョンがない場合、[Revert Upgrade] リンクは表示されません。

ステップ 3 ターゲットバージョンが許容できるバージョンである場合（かつ使用可能な場合）、[Revert] をクリックします。

次のタスク

アップグレードと復元の間に行った設定変更をやり直します。



第 6 章

ソフトウェアの新規インストール

アップグレードできない場合、またはアップグレードしない場合は、メジャーリリースおよびメンテナンスリリースを新規インストールできます。

パッチ用のインストールパッケージは提供していません。特定のパッチを実行するには、適切なメジャーリリースまたはメンテナンスリリースをインストールしてからパッチを適用してください。

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。Firepower デバイスでは、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ることに注意してください。

（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ことが必要になる場合があります。これらが生じると再登録できない場合があります。

表 *39 :* 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	Cisco Smart Licensing
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。 **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。『Cisco Firepower Threat Defense コマンド リファレンス』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。『Cisco Firepower Threat Defense コマンド リファレンス』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。
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 構成ガイド』を参照してください。

シナリオ	ソリューション	Cisco Smart Licensing
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。
FDM を使用した FTD パッチをアンインストールします。	再イメージ化します。 FDM 展開環境では、パッチをアンインストールすることはできません。	再イメージ化する前に、デバイスを登録解除します。その後、再登録します。
FMC または FMC 管理対象デバイスを以前のメジャーリリースまたはメンテナンスリリースに戻します。	再イメージ化します。 FMC またはその管理対象デバイスからメジャーアップグレードまたはメンテナンスアップグレードをアンインストールすることはできません。可能であれば、バックアップから復元します。	再イメージ化を行う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。これを行った場合は、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。
FDM 管理対象デバイスを以前のメジャーリリースまたはメンテナンスリリースに戻します。	元に戻す。 メジャーアップグレードまたはメンテナンスアップグレードが期待どおりに機能していないと判断した場合は、アップグレードの直前の状態にデバイスを戻すことができます。FXOS のバージョンをダウングレードする必要がある場合もあります。 FDM または CLI を使用できます。 • FDM：[アップグレードの復元（Revert Upgrade）] 機能を使用します。『Firepower Device Manager 用 Cisco Firepower Threat Defense 構成ガイド』を参照してください。 • CLI：**upgrade revert** コマンドを使用します。『Cisco Firepower Threat Defense コマンド リファレンス』を参照してください。	対処は不要です。

シナリオ	ソリューション	Cisco Smart Licensing
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、工場出荷時の初期状態の設定での交換になります。ただし、交換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。	再イメージ化を行う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。これを行った場合は、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

これらの一般的なガイドラインと警告は、再イメージ化に適用されます。

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 シリーズデバイスの完全な再イメージ化を実行することを推奨します。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。

再イメージ化チェックリスト

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。このチェックリストは、一般的な再イメージ化の問題を回避できるアクションを示しています。ただし、このリストは包括的なものではありません。詳細な手順については、該当する設置ガイド（「インストール手順 （110 ページ）」）を参照してください。

表 *40 : Firepower* 再イメージ化チェックリスト

✓	アクション	詳細
	アプライアンスへのアクセスを確認します。	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。
	バックアップを実行します。	再イメージ化の前に Firepower アプライアンスをバックアップします（サポートされている場合）。 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できないことに注意してください。設定は手動で再作成する必要があります。 **注意** Firepower アプライアンスを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ことを強くお勧めします。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、セキュリティやライセンス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。

✓	アクション	詳細
	FMC 管理からデバイスを削除します。	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。
	ライセンスの問題に対処します。	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

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、クラウドおよびクラウドサービスからアプライアンスが登録解除され、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。
- モデルの移行中にソース Firepower Management Center をシャットダウンする。
- 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 [Smart License Status] の横の **停止記号**（ ） をクリックします。

ステップ 4 警告し、登録を解除することを確認します。

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。

インストール手順

リリースノート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。

表 *41 : Firepower Management Center* のインストール手順

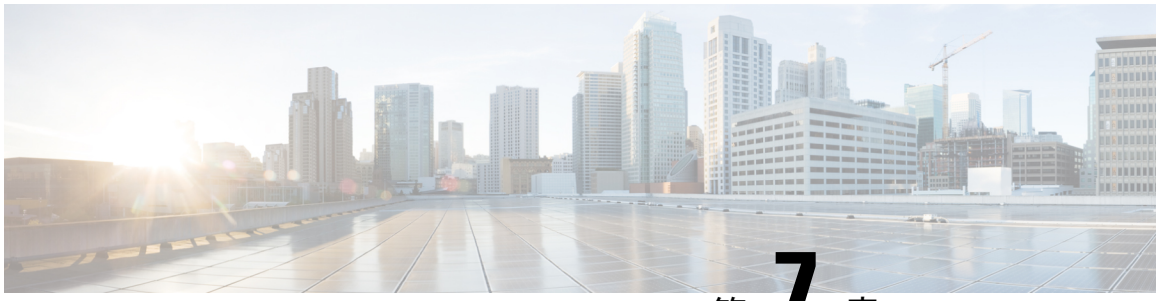
FMC プラットフォーム	ガイド
FMC 1600、2600、4600	Cisco Firepower Management Center 1600, 2600, and 4600 Getting Started Guide
FMC 1000、2500、4500	Cisco Firepower Management Center 1000, 2500, and 4500 Getting Started Guide
FMCv および FMCv 300	Cisco Firepower Management Center Virtual 入門ガイド

表 *42 : 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：GCP	Google クラウドプラットフォーム向け Cisco Firepower Threat Defense Virtual スタートアップガイド
FTDv：OCI	Oracle クラウドインフラストラクチャ向け Cisco Firepower Threat Defense Virtual スタートアップガイド
FTDv：Azure	Cisco Firepower Threat Defense Virtual クイック スタート ガイド（Microsoft Azure クラウド向け）

表 *43 : NGIPSv* および *ASA FirePOWER* のインストール手順

NGIPS プラットフォーム	ガイド
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 7 章

資料

Firepower のマニュアルについては、次を参照してください。

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、 今回のリリースで新たに利用可能になっています。 他の Firepower マニュアルへのリンクについては、ドキュメント ロードマップ （115 ページ） 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 バージョン 6.7 コンフィギュレーション ガイドおよびオンラインヘルプ
- Cisco Firepower Threat Defense バージョン 6.7.0 コンフィギュレーション ガイド（Firepower Device Manager 向け）およびオンラインヘルプ
- FirePOWER Services ローカル管理を搭載した Cisco ASA バージョン 6.7 コンフィギュレーション ガイドおよびオンラインヘルプ
- Cisco Firepower Threat Defense コマンド リファレンス

FXOS コンフィギュレーション ガイドおよびリリース ノート

- Cisco Firepower 4100/9300 FXOS Firepower Chassis Manager 2.9(1) コンフィギュレーション ガイド
- Cisco Firepower 4100/9300 FXOS 2.9(1) CLI コンフィギュレーション ガイド
- Cisco Firepower 4100/9300 FXOS コマンド リファレンス
- Cisco Firepower 4100/9300 FXOS 2.9(1) リリースノート

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 1010 ハードウェア設置ガイド
- Cisco Firepower 1100 シリーズ ハードウェア設置ガイド
- Cisco Firepower 2100 シリーズ 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 Virtual 入門ガイド
- Cisco Firepower 1010 スタートアップガイド
- Cisco Firepower 1100 シリーズ スタートアップガイド
- Cisco Firepower 2100 シリーズ スタートアップ ガイド
- Cisco Firepower 4100 スタートアップガイド
- Cisco Firepower 9300 Getting Started Guide
- Cisco ISA 3000 スタートアップガイド
- Cisco ASA 5508-X and 5516-X Getting Started Guide
- Cisco Firepower Threat Defense Virtual for the AWS Cloud スタートアップガイド
- Google クラウドプラットフォーム向け Cisco Firepower Threat Defense Virtual スタートアップガイド （**新規**）
- Oracle クラウド インフラストラクチャ向け Cisco Firepower Threat Defense Virtual スタートアップガイド （**新規**）
- Cisco Firepower Threat Defense Virtual クイック スタート ガイド（Microsoft Azure クラウド向け）

API および統合ガイド

- Firepower Management Center REST API バージョン 6.7.0 クイックスタートガイド
- Cisco Firepower Threat Defense REST API ガイド （Cisco Firepower Threat Defense REST API Guide）
- Firepower システム データベース アクセス ガイド v6.7

- オンプレミスにおけるシスコのセキュリティ分析とロギング：Firepower Event Integration Guide （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 System Feature Licenses
- Frequently Asked Questions (FAQ) about Firepower Licensing

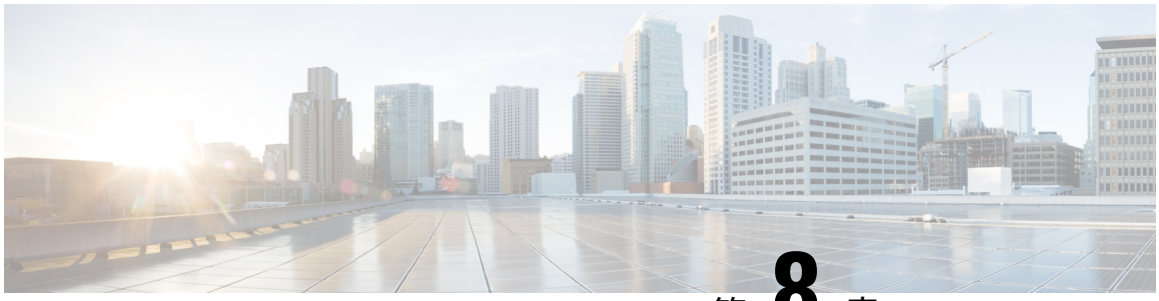
トラブルシューティングおよび設定の例

- Cisco Firepower Threat Defense Syslog メッセージ
- FMC および FTD 管理ネットワークの管理 ***NEW***
- Deploy a Cluster for Firepower Threat Defense for Scalability and High Availability
- FMC によるリモートブランチオフィスでの FTD の展開 ***NEW***

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 8 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。

（注） 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。バグ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 Bug Search Tool を「信頼できる情報源」と考えてください。

解決された問題については、次を参照してください。

- 解決済みの問題の検索 （117 ページ）
- バージョン 6.7.0 で解決済みの問題 （118 ページ）

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。 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したりすることもできます。

これらの一般的なクエリには、バージョン 6.7.0 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
- Firepower Threat Defense
- Firepower Threat Defense Virtual
- ASA with FirePOWER サービス
- NGIPSv

バージョン 6.7.0 で解決済みの問題

表 *44* : バージョン *6.7.0* で解決済みの問題

不具合 ID	タイトル
CSCuq33233	クラスタリング：NAT ルールで PAT IP が重複すると、xlate が複製されない
CSCvd09106	SNMP/Syslog/電子メールアラート設定を編集すると、使用カウントが増加する
CSCvf34107	ボリューム上の管理されていないディスクの使用率が高いとの誤検出アラートが発生する
CSCvg01007	https pdf 添付ファイルの問題
CSCvg74990	アーカイブ検査機能の制限に関するオンラインドキュメントを更新する必要がある
CSCvh65500	FTP アクティブ モードの Firepower 2100 クライアントがサーバとのコントロール チャネルを確立できない
CSCvi47847	Firepower を介してシェルアプリケーションが検出されない
CSCvi51189	ENH：FDM で webvpn/AnyConnect の非 UDP/TCP 443 カスタムポートを許可する必要がある
CSCvi92162	ドキュメント：各 Firepower バージョンごとに、HTTPS トラフィックのアプリケーション検査と URL 検査についての説明が必要
CSCvi96835	ルーティングポリシーで使用されるグループオブジェクトの一部であるホストを範囲に変更しても検証エラーが発生しない
CSCvj87597	Flex Config にセキュリティゾーンが含まれていると、インポートが失敗する
CSCvj91418	Cisco FTD ソフトウェア SMB プロトコルプロセッサ検出エンジンのシステムメモリの不足、DoS 脆弱性
CSCvk16568	アプリケーション ID が検出された場合、AppID がトラフィックの処理を停止する
CSCvk21405	シェルアプリケーションがサーバから新しい接続のピンホールを開かない
CSCvk40714	リモートストレージの SSH オプションを設定できない
CSCvk56513	トラフィックがプロキシを通過するとき Tor がブロックされない

不具合 ID	タイトル
CSCvk62871	パッシブ モードの Firepower 2100 FTP クライアントがサーバとのデータ チャネルを確立できない
CSCvm69294	スタンバイ FMC が大量の SNMP トラップを送信している
CSCvm99989	SystemUpTime の SNMP OID に誤った値が表示される
CSCvn08417	ENH：FlexConfig で crypto コマンドがブラックリストに登録されるべきではない
CSCvn49854	後続の HTTP 要求が URL と XFF を取得しない
CSCvn73530	KP デバイスでスケジュールされている展開タスクが 50 時間以上にわたってスタックした
CSCvn78597	プロキシが有効になっている場合、HTTPS ブロック サイトでは Firepower ブロック ページが MS IE11 および Edge に表示されない
CSCvn94888	FMC に登録された FTD が「サービスを利用できません（Service Unavailable）」を返す
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
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
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）
CSCvp80474	SFOS における OpenSSL の脆弱性（CVE-2019-1559）
CSCvq23896	AppID の保留中、SSL プリプロセッサによって TLS 1.3 トラフィックがホワイトリストに登録された
CSCvq39888	Cisco Firepower Threat Defense ソフトウェアの非標準プロトコル検出バイパスの脆弱性
CSCvq39955	Cisco Firepower Threat Defense ソフトウェアのストリーム再構成バイパスの脆弱性
CSCvq54551	CAC ユーザ向け FMC のインテリジェンスページでロードエラーに失敗した
CSCvq67965	ENH：SFP-Fp2k で自動ネゴシエーションを無効にする機能が必要
CSCvq76964	異常なモジュール FlexFlash コントローラ 1 の古いファームウェアに関連する障害

不具合 ID	タイトル
CSCvq95058	IPSEC SA が、リンクダウンによって発生したフェールオーバーにより削除される
CSCvr01675	複数のシスコ製品での Snort HTTP 検出エンジンのファイルポリシーバイパスの脆弱性
CSCvr09399	動的フローオフロードを無効にできない
CSCvr09468	CLI 「Show nat pool」の ASA トレースバックとリロード
CSCvr13762	FMC 上の NGFWHA に EO UUID がない
CSCvr39217	リブート後、FXOS SNMP ユーザが永続されない
CSCvr49729	FPR2100 に対して Fail-to-Wire ポートダウンが表示され、FTW コンフィギュレーション API の終了に時間がかかる
CSCvr49833	Cisco Firepower 2100 シリーズのセキュリティアプライアンスの ARP におけるサービス拒否攻撃に対する脆弱性
CSCvr55535	ポリシー展開のフェーズ 3 では、一度に 10 個のパッケージしか処理されないため、時間がかかる
CSCvr57051	ポリシーの展開にエラー「Can't use an undefined value as a HASH reference」で失敗しました。
CSCvr66067	ハイアベイラビリティ展開モードでの FMC のバックアップおよび復元手順の提供
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
CSCvr68885	FXOS fault F0479 仮想インターフェイスのリンクの状態はダウンしています。
CSCvr74896	クラウドフィードが無効になっている状態で AC ポリシーを FMC にインポートすると、セキュリティ インテリジェンスを更新できない
CSCvr74901	FXOS 論理デバイスブートストラップの AppAG エンコーディング
CSCvr86077	re_multi_match_ascii によるデータパスでの ASA のトレースバック/ページフォルト
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
CSCvr98881	トレースバック：FTD ZeroMQ メモリアサーション

不具合 ID	タイトル
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。
CSCvs06043	ngfwManager の CSM_CCMservice 用の TunnelClient が FMC の CSM_CCM サービスから送信された ACK を読み取らない
CSCvs13950	REST API ネットワークオブジェクトの検証
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
CSCvs21705	admin ユーザは、ドメイン内のデバイスルーティング設定にアクセスする権限がありません。
CSCvs29494	ハブアンドスポーク VPN、ダイナミック暗号マップ、自動生成 PSK が、静的ピアと動的ピアで同じである
CSCvs31114	FTD 6.5 以降のバイパス失効チェックをサポートしていないことに関する警告
CSCvs33392	サーバがサポートされていない TLS オプションを使用している場合、既知のキー SSL 復号および接続が失敗することがある
CSCvs34851	継続的なリンクフラッピングにより、snm_log コアファイルが生成される
CSCvs37266	サブドメインに属するレビュー済み侵入イベントで、レビュー担当者が不明と表示される
CSCvs39253	バージョン 6.4 で Firepower 7000 および 8000 が電子メールを送信できない
CSCvs39368	Firepower 4100/9300 のメモリリークが原因で DME のプロセスがトレースバックする可能性がある
CSCvs39388	FTD が CC モードでシステム syslog メッセージを送信しない
CSCvs41883	ND ポリシー参照が見つからない場合、6.4.0.x へのアップグレード後に展開が失敗する
CSCvs42203	ホスト名の送信：ホスト名が Null のとき、デバイスがホスト名を「none」にして SA に送信する
CSCvs42388	文字列の Gratuitous ロギング：「プリプロセッサのメモリ統計情報が Null」と表示される
CSCvs42577	パスワードが送信されていないため、ユーザのダウンロードが失敗する可能性がある

不具合 ID	タイトル
CSCvs42799	FXOS のアップグレード後、アプリケーションインスタンスがチェックサム検証に失敗して起動できない
CSCvs44109	FMC：PPPoE パスワードの制限が厳しすぎる。基盤となるコードと一致している必要がある
CSCvs44149	大規模なオブジェクトグループを追加すると、調整レポートにすべてのネットワークが表示されない
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
CSCvs59866	サポートされていない高速モードの lacppolicy 設定を Firepower 2100 の FXOS から削除
CSCvs64510	メッセージ（「Can't call method "binip" on unblessed reference」）が表示されて展開が失敗する
CSCvs68576	二重否定が原因で、自動 NAT ルールの削除時に展開に失敗する
CSCvs71578	6.2.3.10 から 6.4.0 への FMC アップグレードが 400_run_troubleshoot.sh で停止し、アップグレードがハングした
CSCvs72390	Cisco Firepower Management Center のクロスサイト スクリプティングの脆弱性
CSCvs74586	Firepower FTD トランスペアレントが非 IP パケットを復号化しない
CSCvs74747	バックアップの復元後に FTD 登録状態が「pending」と表示される
CSCvs76604	6.6.0-1430 の管理インターフェイスで SNMP が機能しない
CSCvs81871	データインターフェイスの編集時の CCL MTU ポップアップ警告の削除
CSCvs85348	オブジェクト検証で、別のデバイスのインターフェイスが検証される
CSCvs85640	FMC で監査ログを抑制できない
CSCvs86765	単一のルールエラーの発生時にルール影響フラグの再生成を終了すべきではない
CSCvs90447	FXOS 8x1G FTW の継続的なリンクフラッピング
CSCvs91270	検査の中断：展開ページでエラーが発生
CSCvs92044	ポートチャネル メンバー インターフェイスのフラップによる FXOS L3 出力オブジェクトのリソースリーク
CSCvs92077	影響フラグが赤でないローカルルールに対して、誤った影響フラグが付く

不具合 ID	タイトル
CSCvs94061	クロックのずれとトラフィックの中断を引き起こすNTPスクリプトエラー
CSCvs98373	FMC がクラシックライセンスを断続的に検出できない
CSCvt01397	LINA設定がプッシュされなかったにもかかわらず、展開は正常としてマークされる
CSCvt03320	VLAN インターフェイスで、FMC の DHCP 関連の設定をできるようにする必要がある
CSCvt04377	VLANカプセル化が超過すると、デコードエラーによりディスク領域が枯渇する
CSCvt06091	FXOS が show interface から WSP-Q40GLR4L トランシーバをタイプ QSFP-40G-LR4 として表示する
CSCvt06743	FTW ウォッチドッグのキック遅延により、インラインセットがダウン/バイパス失敗する可能性がある
CSCvt08514	SFDataCorrerator：sfipproxy が再起動せず FPReplicationCommunicationRabbit が接続できない
CSCvt10420	DomainSearchNameValidator クラスでは、更新済みの DOMAIN_NAME_PATTERN の正規表現が必要
CSCvt10604	マスクが異なる 2 つのオブジェクトが、ECMP なしのルートで同じネットワークを使用する場合の検証チェック
CSCvt11885	移行スクリプトの実行がメモリ不足エラーで終了する
CSCvt15062	FTD 2100：デバイスのリブート時に BYPASS から NON-BYPASS への移行中にパケットがドロップする
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
CSCvt17448	OSPF マルチキャスト MAC が l2-table から削除され、OSPF が失敗する
CSCvt18337	アップグレード後に HA ノードでフェールオーバーが無効になった
CSCvt20235	Firepower 4100 シリーズのすべての FTW インターフェイスが同時にリンクフラップするが、まれにしか発生しない
CSCvt20709	SSL を挿入した RESET での方向が誤っていたため、誤ったインターフェイスから出力され、MAC フラップが発生する

不具合 ID	タイトル
CSCvt21986	インスタンス間での Snort と Lina のコアの割り当てに一貫性がない
CSCvt22254	FDM が更新サーバに到達できない場合、復元後に自動展開が失敗する
CSCvt25599	廃止された Flexconfig は、警告だけでなく展開をブロックする必要がある
CSCvt25647	RabbitMQ デバイスアカウントの欠落により、SRU と TID の更新が失敗する
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ました（Inspection engine in other unit has failed due to snort failure）」が原因で FTD がフェールオーバーした
CSCvt34160	FPR9K-NM-4X40G で WSP-Q40GLR4L トランシーバを使用すると、再起動後に「リンクが接続されていない（Link not connected）」というエラーが発生する
CSCvt34894	Snort が過剰なメモリを消費し、パフォーマンスの問題を引き起こす。
CSCvt34973	SFNotificationd によって「メッセージ」ファイルに過剰なロギングが発生することがある
CSCvt35053	Cisco Firepower Management Center ソフトウェアのクロスサイト スクリプティングに対する脆弱性
CSCvt35134	FPR4100/9300：デバイスのリブート時、BYPASS から NON-BYPASS への移行中にパケットがドロップする
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
CSCvt35730	2 番目のトンネルに重複する暗号 ACL がある場合の FDM 展開エラー
CSCvt35897	Cisco 適応型セキュリティ アプライアンス ソフトウェアと Firepower Threat Defense ソフトウェアの DoS 攻撃に対する脆弱性
CSCvt37881	https のブロックページが機能しない
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
CSCvt38279	ISA3000 で disk0 を消去すると、ファイルシステムがサポートされなくなる
CSCvt39292	LDAPS 外部ユーザが Firepower 4110 で「sudo su」を実行できない

不具合 ID	タイトル
CSCvt39349	展開ステータスが [展開済み（DEPLOYED）] または [失敗（FAILED）] である限り、デバイスの登録を許可する必要がある
CSCvt39897	FP 4120 svc_sam_dcosAG がクラッシュタイプ 139 でクラッシュする
CSCvt40306	ASA：リロード後にスタンバイユニットの BVI インターフェイスが応答を停止する
CSCvt45206	アップグレード前に存在していたイベントを検索すると、イベント検索が失敗することがある
CSCvt46784	iptables が破損している場合、clish configure ssh-accesslist コマンドがサイレントに失敗する
CSCvt46999	RAM ディスクを有効または無効にする CLI コマンドの後に EventHandler が接続イベントを処理しない
CSCvt48260	スタンバイユニットがアクティブユニットを検出すると、fover_parse でトレースバックしてブートループする
CSCvt50528	ASA/FTD - CLI での証明書のインストールに関するデフォルト設定の警告メッセージ
CSCvt51039	ライセンスのクリーンアップの処理
CSCvt52604	FMC の [オブジェクト（Objects）] セクションから [インターフェイス（Interfaces）] ページがロードされない（ドメインページも影響を受けることがある）
CSCvt52607	SSL HW モードのフローテーブルメモリの使用率を引き下げて Snort が D 状態になる確率を低減する
CSCvt52844	アップグレードされた FDM 6.6.0-1621 で、レガシーポートを使用して AMP クラウドのルックアップが実行される
CSCvt54267	Cisco Firepower Management Center ソフトウェアのサービス拒否攻撃（DoS）に対する脆弱性
CSCvt54279	FDM：オブジェクトのライセンス名がないために展開が失敗する。Sensitive_data には URLFILTERING ライセンスが必要
CSCvt54943	FPR9300 に余分な「Local Disk 3」が表示される（改善されたソリューション）
CSCvt59770	FTD：SCEP を介した証明書の取得の失敗により停止する
CSCvt61196	マルチコンテキストモードの ASA で、コンテキストを削除しても SSH キーが削除されない。

不具合 ID	タイトル
CSCvt61229	ルールコメント内の特殊文字のために展開を失敗させる必要はない
CSCvt61370	通信のデッドロックが原因で、デバイスからのイベントが停止することがある
CSCvt63293	ハードドライブを 2 台搭載していないアプライアンスでは、ディスク使用率のヘルスモニタが機能しない
CSCvt64642	FMC：証明書を照合するために Anyconnect の「証明書マップ」が「DC（ドメインコンポーネント）」を使用中、展開エラーが発生
CSCvt64822	Cisco 適応型セキュリティ アプライアンス ソフトウェアの SSL/TLS のサービス拒否（DoS）攻撃に対する脆弱性
CSCvt67638	メタデータを抽出できないエラーにより復元が失敗する
CSCvt68486	FXOS：FirePower 4100/9300 で svc_sam_dcosAG プロセスがクラッシュする
CSCvt69260	接続イベントに古いデバイス名が表示される
CSCvt70879	vpn-filter に使用される ACL での「clear configure access-list」がリソースにアクセスできない
CSCvt72683	FP 8130 での NAT ポリシーの展開後の NAT ポリシーの設定が表示されない
CSCvt73808	DAQ から Oct ドライバに送られるヘッダーが長いメッセージの対処
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
CSCvt78809	VNIC の設定エラーが原因でインスタンスの起動に失敗した
CSCvt79471	6.2.3.13 FMC での 500 内部エラーにより、../deployment/deployabledevices に到達できない
CSCvt79777	sfipproxy.conf で IP アドレスが重複している
CSCvt79863	IO エラーが原因で、FTD アップグレードが失敗したにもかかわらず、成功と宣言された
CSCvt79988	FMC を 6.6 にアップグレードした後、SNMP 設定が原因でポリシー展開が失敗する
CSCvt80104	Memcached ソフトウェアを CVE-2018-1000115 アドレス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

不具合 ID	タイトル
CSCvt83121	Cisco ASA および FTD ソフトウェアの OSPFv2 リンクローカルシグナリングで確認されたサービス拒否攻撃に対する脆弱性
CSCvt83133	group-url を使用して Google Chrome から anyconnect webvpn ポータルにアクセスできない
CSCvt85815	「機密データの検出」を有効にすると、ポリシーの展開が失敗する
CSCvt86807	メジャーアップグレード後に Web 分析（Google Analytics）が再度有効になる
CSCvt89587	エラーにより展開失敗：入力ラインのサイズが使用可能なバッファを超過
CSCvt91258	FDM：管理ゲートウェイとしてデータインターフェイスを使用して、どの NTP サーバにも到達しない
CSCvt93177	デフォルトでフルプロキシを無効化してライトウェイトプロキシにする。（FP2LWP）FTD デバイス
CSCvt93999	アップグレードが進行中の場合、FMC は同じデバイスで 2 回目のアップグレードを許可すべきではない
CSCvt94383	無効な GID 権限により、HA 同期とデバイス登録で問題が発生する
CSCvu01083	プロセスの再起動を回避するために、RabbitMQ ログ消去の例外を追加
CSCvu02594	非同期セッションが多すぎるため、Snort の終了に時間がかかる
CSCvu05216	CRL CDP オーバーライドを指定する証明書マップでバックアップエントリが許可されない
CSCvu08802	FMC を 6.4.0.7 から 6.5.0.4 にアップグレードすると、FMC で FTD HA の設定が失われる
CSCvu09379	パスワードが設定されていない FTP 転送を実行すると、イメージの再作成中に FMC がループする
CSCvu09496	多くの ACP で同じ DNS ポリシーが参照されると、DNS データが繰り返し収集されエクスポートされる
CSCvu09723	FDM：デフォルトアクションのロギングが LINA 側に反映されない
CSCvu10900	大量の ssl-certs-unified.log ファイルが、トラブルシューティングで 9GB に寄与
CSCvu11868	FPR9K-NM-4X40G で QSFP-40G-LR4 トランシーバを使用すると、再起動後に「リンクが接続されていない（Link not connected）」というエラーが発生する

不具合 ID	タイトル
CSCvu12307	FTD-HA：「ERROR：指定された AnyConnect クライアントイメージは存在しません。」
CSCvu12608	ASA5506/5508/5516 デバイスが正しく起動しない/ブートループが発生する
CSCvu13287	FDM がサブジェクトまたは発行元のない証明書をインポートできず、アップグレードも失敗する
CSCvu14647	FMC HA 同期中にコンフィギュレーション データベース エラーを停止できない
CSCvu14772	jQuery のバージョンが 1.0.3 ～ 3.5.0 の場合、pa
CSCvu15611	FTD-HA：スタンバイが HA に参加できない「CD アプリ同期エラーはアプリ構成の適用に失敗しました」
CSCvu16201	CheckClientAppVulnerability の実行中に FMC でデータコリレータが予期せず終了した
CSCvu22377	FTD のクラスタグループ名に余分な空白があると、スレーブがキックアウトされる
CSCvu23289	多数の neostore.transaction.db.* ファイルによってディスクがいっぱいになり、neo4j の問題が発生する
CSCvu26658	SFDataCorrelator がバックアップ操作中にイベントをドロップすることがある
CSCvu29660	使用可能なブロックがゼロになっても、ブロック枯渇スナップショットが作成されない
CSCvu30549	「手動 URL フィルタリング」の 3 つの URL エントリオプションすべてのドキュメント化
CSCvu30572	[Add Rule] の [Enter URL] テキストボックスを使用する場合の URL の構文とセマンティクスのドキュメント化
CSCvu30585	「URL オブジェクト」のフォーマットと機能動作のドキュメント化
CSCvu30588	「URL リストとフィードオブジェクト」のフォーマットおよび「セキュリティ インテリジェンス」の機能動作のドキュメント化
CSCvu30756	ユーザ ID が、異なるネットマップの同一セッションを正しく処理しない
CSCvu31167	DOC：ファイルポリシーが [Normalize TCP Payload] オプションを使用したインライン正規化を自動的に有効にする

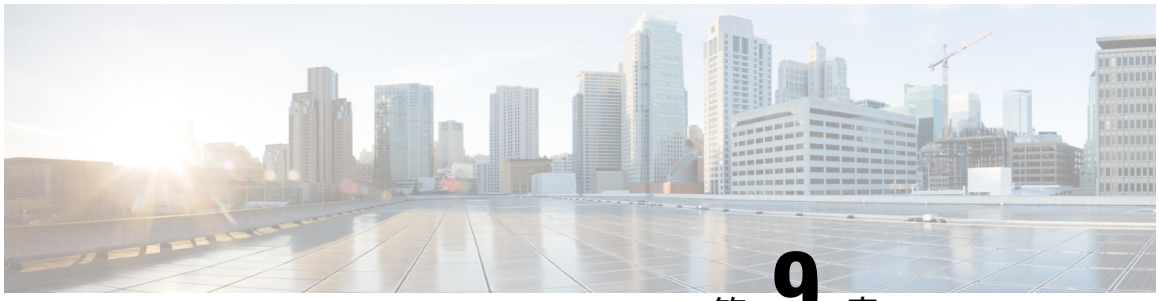
不具合 ID	タイトル
CSCvu32449	FDM：AnyConnect「名前が重複しているため、検証に失敗しました：（Validation failed due to duplicate name:）」
CSCvu36539	スマートライセンスデバイスが 6.2.2 -> 6.4.0 -> 6.6.0 にアップグレードされた場合、アップグレードが失敗する。
CSCvu40531	pktmgr.out および lacp.out への FXOS LACP パケットロギングにより /opt/cisco/platform/logs が 100% になる
CSCvu43827	スレッド名「cluster config sync」または「fover_FSM_thread」での ASA および FTD クラスタ ユニット トレースバック
CSCvu53585	6.6.0 へのアップグレード後に Elektra onbox ポリシーの展開が失敗する
CSCvu54000	EPSV パッシブモードの Firepower 4100 FTP クライアントが、サーバとのデータチャネルを確立できない
CSCvu54221	FMC HA のハードウェア要件の追加
CSCvu54706	Cisco Firepower Management Center CWE-772：低速 HTTP POST の脆弱性
CSCvu55469	FTD：接続アイドルタイムアウトがリセットされない
CSCvu57825	Snort 停止：検出の再設定エラー
CSCvu57834	100% CPU を使用する syslog-ng プロセス
CSCvu58153	RADIUS ポートの表現がビッグエンディアンではなくリトルエンディアンとして表示される
CSCvu60923	Radius サーバグループオブジェクトの IP を編集すると、IP アドレスの値が意図しないものになる
CSCvu65085	[DOC] ルートマップオブジェクトの Set 句に EIGRP の k 値が含まれていない
CSCvu65890	サポートされていないにも関わらず、FMC が SNMP3 設定で MD5 および DES から切り替えることができない
CSCvu65936	FDM 6.6.0 のアップグレード（または）configImport が EtherChannelInterface でフェールオーバーリンク検証の失敗として失敗する
CSCvu66119	シリーズ 3 で URL ルールが誤って昇格されると、トラフィックが誤ったルールに一致する。
CSCvu70529	snort のリロード時にバイナリルール（SO ルール）がロードされない
CSCvu75581	Cisco ASA および FTD Web サービスインターフェイスで確認されたクロスサイト スクリプティングの脆弱性

不具合 ID	タイトル
CSCvu77689	FileZilla への FTP が SMTP に誤って分類される
CSCvu79129	FTD-API/FDM：スマートランセンスの基本ライセンスが失われる
CSCvu82272	管理対象デバイスの非アクティブな古いエントリが原因で、Firepower Management Center でのアップグレードが失敗することがある
CSCvu82578	ライトテーマ UI FMC：SFR モジュールでインターフェイスページのロード時に長い遅延が発生する
CSCvu82743	エンコードされたルールプラグイン SID 値、GID 3 が正しく登録されいない。このルールを無効にする
CSCvu82918	HA 同期がスタンバイで予期しないエラーで失敗する
CSCvu83389	ASA がヌル TEID の GTPV1 転送再配置要求メッセージをドロップする
CSCvu83629	URL リストファイルのセキュリティ インテリジェンスの URL 数が、新しい UI（Ligth テーマ）に表示されない場合がある
CSCvu84556	サイト間ダイナミッククリプトマップが RA VPN ダイナミッククリプトマップの下に展開される
CSCvu85127	同じ UUID のデバイスが接続しようとしている場合、展開できない
CSCvu85381	スタンバイでのポリシー展開の失敗に続いて HA の再構成が失敗する
CSCvu87879	インターフェイス モニタリングが原因で HA の状態が継続的に変化すると、展開が停止する
CSCvu88005	GET taskstatus の FMC REST API ユーザ権限
CSCvu91292	nmap を使用して新しいカスタムアプリケーションが識別されると、Snort が繰り返し再起動する
CSCvu96927	FQDN オブジェクトが NAT グループ内で割り当てられると削除できなくなる
CSCvu98197	「復号しない」SSL 復号ルールに一致する HTTPS 接続がブロックされることがある
CSCvv02925	OSPF ネイバーシップが確立されていない
CSCvv09180	複数の NTP サーバが設定されている場合、Firepower Chassis Manager で NTP の [Server Status] が空白になる
CSCvv10901	VMware ドキュメントの vFTD で、ハイパースレッディングの無効化を推奨する必要がある

不具合 ID	タイトル
CSCvv10948	FDM アップグレード：UI で保留中の変更が表示されない（ただし、アップグレードは開始されていない）
CSCvv11981	統合ロギングのバグ CSCvr98881 で、Lina 側の変更が必要
CSCvv12988	バックアップ中に tomcat が強制終了された後、正常に回復しない
CSCvv13672	長い期間を選択すると、CPU 負荷グラフに不完全な CPU データが表示されることがある
CSCvv14442	将来のタイムスタンプを持つファイル/ディレクトリが含まれている場合、FMC バックアップの復元が失敗する
CSCvv15013	FXOS が追加の内部 VLAN タグを送信すると、デバイスで ARP 更新が失敗する
CSCvv16245	Cisco Firepower Management Center ソフトウェアの共通アクセスカード認証バイパスの脆弱性
CSCvv17893	uip スナップショットとログファイルが不正なため、FTD がキャッチアップを繰り返し要求し、ファイルハンドラを使い果たす
CSCvv18936	セッションタイムアウト後、CAC ログインボタンが新しい UI に表示されない
CSCvv21045	データベースが新しい接続を受け入れないため、イベント処理が停止する
CSCvv21782	6.6.1：ASA SFR プラットフォームのすべてのトラフィックに対して無効な ID として表示されるプレフィルタポリシー値
CSCvv23370	webVPN、SNMP 関連トラフィックの実行中に FPR2130 でトレースバックが発生した。
CSCvv26683	CLI から「configure high-availability disable」コマンドを実行すると、次の HAJoin で例外が発生する
CSCvv27113	侵入イベントの ProcessMetadata が間違った local_sid 制約を使用してエントリをルックアップする
CSCvv29851	FMC：仮想デバイスから物理デバイスへの移行後にハイアベイラビリティページがロードされない
CSCvv31197	復号化された SSL トラフィックのファイルイベントで、ファイル名が正しく表示されない
CSCvv33013	FDM：文字 ^ @ _ で秘密鍵を追加できない

不具合 ID	タイトル
CSCvv34888	CCM レイヤ（スプリント 80）における WR6、WR8 および LTS18 コミット ID の更新
CSCvv36915	「Show NTP」コマンドがマルチインスタンス FTD で機能しない
CSCvv38482	アップグレード後に FDM UI がロードに失敗する
CSCvv40316	FDM：スマート CLI ルーティングオブジェクトを使用して BGP の 11 番目のネイバーを追加できない
CSCvv43864	ポリシーを変更すると、変更ログのプレビューが空白になる
CSCvv45500	FDM を使用したバージョン 6.6.0.1 FTD アップグレードによる HA の一時停止
CSCvv46984	データインターフェイスを通して管理される HA スタンバイデバイスで、660 へのアップグレードが失敗する
CSCvv52591	ctm_hw_malloc_from_pool で DMA メモリリークが発生し、管理接続と VPN 接続が失敗する
CSCvv55066	FPR1010：SMBファイル転送中に Internal-Data0/0 およびデータインターフェイスがフラッピングする
CSCvv57476	Chrome 85、IE、および Edge ブラウザで CSS スタイルをロードすると問題が発生する
CSCvv58604	トラフィックが、ブロック/リセットおよび SSL インスペクションで設定された AC ポリシーと一致する場合、リセットが送信されない
CSCvv64302	DOC：RAM ディスクへのイベントのロギングが、ローエンドデバイスで有効になっていないとドキュメントに誤って記載されている
CSCvv69708	DOC：FTD でプラットフォーム設定を改善（DNS 解決コンフィギュレーション ガイド）
CSCvv70096	Snort 2：SSL 復号化および再署名プロセスでのメモリリーク
CSCvv73540	特定の制限を超えるとファイルキャッシュをドロップするモニタを作成
CSCvv74951	システムのアップグレードスクリプトの実行中、メモリの cgroup を無効化
CSCvv79705	800_post/100_ftd_onbox_data_import.sh で 6.6.0 または 6.6.1 へのアップグレードが失敗した
CSCvv91486	リロード中のストリームでメモリリークが発生
CSCvv99517	FMC：「要求の処理中に内部エラーが発生」というメッセージが表示され、インターフェイス設定を保存できない

不具合 ID	タイトル
CSCvw07003	リーフドメイン管理者ユーザが、サイト間の VPN 設定を編集できない
CSCvw07352	Sybase 接続ステータスが 0 になると、SFDataCorrerator のログスパム、メタデータで障害が発生する
CSCvw17084	Firepower モジュール 6.3 で、復元後にアプリのステータスがダウンする



第 9 章

既知の問題

便宜上、こ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。

（注） 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。バグ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 Bug Search Tool を「信頼できる情報源」と考えてください。

アップグレードでバージョンがスキップされる場合は、スキップするメジャーバージョンの既知の問題も参照してください。「Cisco Firepower リリース ノート」を参照してください。

- 既知の問題の検索 （135 ページ）
- バージョン 6.7.0 の既知の問題 （136 ページ）

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。 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したりすることもできます。

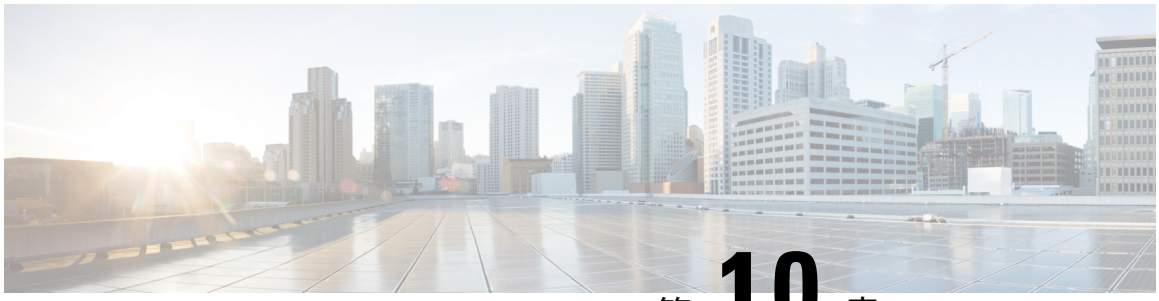
これらの一般的なクエリには、Version6.7.0を実行している Firepower 製品の未解決のバグが表示されます。

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

バージョン 6.7.0 の既知の問題

表 *45* : バージョン *6.7.0* の既知の問題

不具合 ID	タイトル
CSCvv59527	pxGridv2 エンドポイントのダウンロードが応答せず ADI、SFDataCorrelator を切断する
CSCvv95130	FTD を使用した ASA 5500-X シリーズ デバイスがバックアップからの復元後に応答しない
CSCvv99419	[6.7.0] FDM Snort 3 SSL ポリシーの追加/削除により、Snort が UI 警告なしで再起動する
CSCvw20092	レトロスペクティブイベントによって作成されたマルウェアイベントの eStreamer イベントでファイルポリシーが設定されていない



第 10 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