Cisco Firepower バージョン 6.5.0.2 および 6.5.0.4 リリースノート

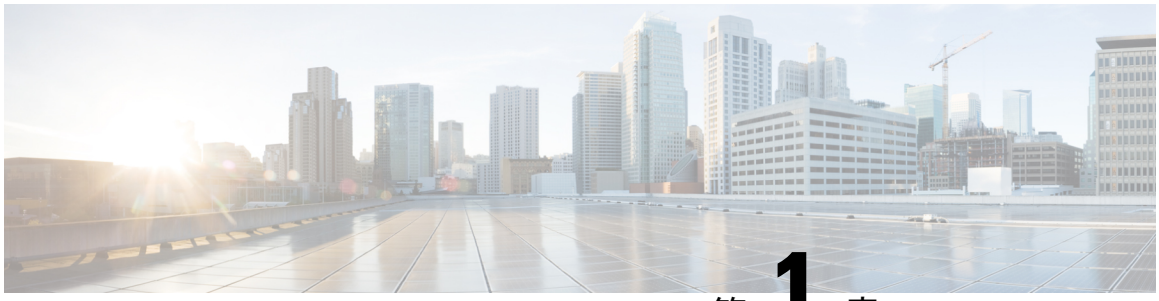
初版：2019 年 11 月 20 日

最終更新：2020 年 3 月 2 日

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

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

目 次



第 1 章

バージョン 6.5.0.x の概要

Firepower をお選びいただき、ありがとうございます。

リリース ノートについて

リリース ノートには、アップグレードの警告や動作の変更など、バージョン 6.5.0.x に関する重要なリリース固有の情報が記載されています。Firepower リリースに精通しており、Firepower 展開をアップグレードした経験がある場合でも、このドキュメントお読みください。

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

- アップグレード手順 （31 ページ）
- 設置手順 （54 ページ）

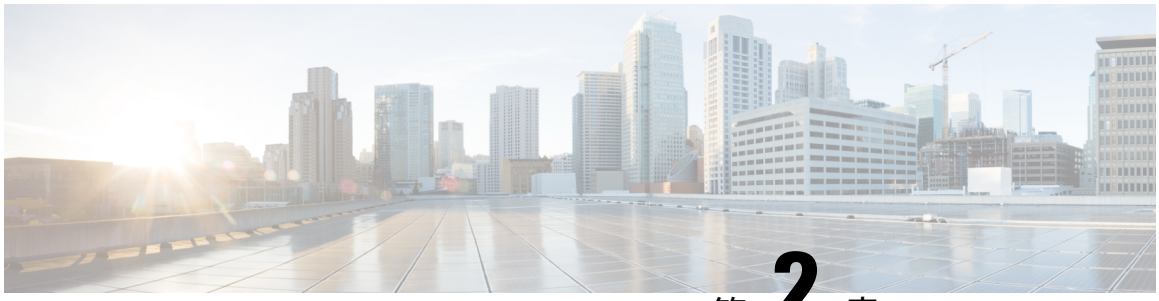
リリース日

バージョン 6.5.0.x で使用可能なすべてのプラットフォームの一覧については、「互換性, on page 3」を参照してください。

Table 1: バージョン ***6.5.0.x*** のリリース日

バージョン（Version）	ビルド（Build）	日付（Date）	プラットフォーム
6.5.0.4	57	2020 年 3 月 2 日	すべて

バージョン（Version）	ビルド（Build）	日付（Date）	プラットフォーム
6.5.0.3	30	2020 年 2 月 3 日	利用できなくなりました。「廃止された機能, on page 11」を参照してください。
6.5.0.2	57	2019 年 12 月 19 日	すべて
6.5.0.1	35	2019 年 11 月 20 日	利用できなくなりました。「廃止された機能, on page 11」を参照してください。



第 2 章

互換性

この章では、Firepower バージョン 6.5.0.xパッチの互換性に関する情報を提供します。

Firepower Management Centerについて

バージョン 6.5.0.x Firepower Management Center ソフトウェアは、物理および仮想プラットフォームでサポートされています。FMC は、混在展開を含めて、FTD または NGIPS を実行する複数のデバイスを管理できます。

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

バージョン 6.5.0.x は、以下をサポートします。

- FMC 1600、2600、4600
- FMC 1000、2500、4500
- FMC 2000、4000

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

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

バージョン 6.5.0.x は、以下をサポートします。

- VMware vSphere/VMware ESXi 6.0、6.5、または 6.7 上の FMCv および FMCv 300
- カーネルベース仮想マシン（KVM）上の FMCv

- Amazon Web Services（AWS）上の FMCv
- Microsoft Azure 上の FMCv

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

Firepower デバイス

バージョン 6.5.0.x Firepower デバイス ソフトウェアは、さまざまな物理および仮想プラットフォームでサポートされています。

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

サポートされている Firepower のデバイス

次の表は、バージョン 6.5.0.x を実行している Firepower デバイスの互換性情報を示しています。ここでも、すべてのデバイスがリモート FMC 管理をサポートしていることに注意してください。

表 2 : バージョン *6.5.0.x* の *Firepower* デバイス

デバイスのプラットフォーム	ソフトウェア	ローカル管理	OS/ハイパーバイザ
Firepower 1010、1120、1140、1150 Firepower 2110、2120、2130、2140	FTD	FDM	—

デバイスのプラットフォーム	ソフトウェア	ローカル管理	OS/ハイパーバイザ
Firepower 4110、4120、4140、4150 Firepower 4115、4125、4145 Firepower 9300 SM-24、SM-36、SM-44 モジュールを搭載 Firepower 9300 SM-40、SM-48、SM-56 モジュールを搭載	FTD	FDM	FXOS 2.7.1.92 + 個別のアップグレード。最初に FXOS をアップグレードします。 問題を解決するには、FXOS を最新のビルドにアップグレードする必要がある場合があります。判断のヒントについては、『Cisco FXOS Release Notes, 2.7(1)』を参照してください。
ISA 3000 ASA 5508-X、5516-X ASA 5525-X、5545-X、5555-X	FTD	FDM	—
	ASA FirePOWER（NGIPS）	ASDM	ASA 9.5(2) ～ 9.14(x) 個別のアップグレード。操作の順序については、『Cisco ASA Upgrade Guide』を参照してください。 ASA と ASA FirePOWER のバージョンには幅広い互換性があります。ただし、厳密にはASA のアップグレードが必要でない場合でも、問題解決のために、サポートされた最新のバージョンへのアップグレードが必要になることがあります。 ASA 5508-X および 5516-X を最新の ROMMON イメージにアップグレードすることをお勧めします。手順については、『Cisco ASA and Firepower Threat Defense Reimage Guide』を参照してください。
FTDv	FTD	FDM（AWS を除く）	次のいずれかです。 • VMware vSphere/VMware ESXi 6.0、6.5、または 6.7 • KVM • AWS • Microsoft Azure サポートされているインスタンスについては、該当する FTDv のスタートアップガイドを参照してください。

デバイスのプラットフォーム	ソフトウェア	ローカル管理	OS/ハイパーバイザ
NGIPSv	NGIPS	—	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

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

Table 3: **バージョン *6.5.0.x* のマネージャとデバイスの互換性**

Firepower Management Center		
バージョン 6.5.0.x FMC	管理可能	バージョン 6.2.3 ～ 6.5.0.x のデバイス。
バージョン 6.5.0.x のデバイス	*require*	バージョン 6.5.0 FMC。
Firepower Device Manager		
バージョン 6.5.0.x FDM	管理可能	FTD デバイス 1 台。
ASDM		
バージョン 7.13.1 の ASDM	管理可能	バージョン 6.5.0.x 以前の ASA FirePOWER モジュール。 ASA、ASDM、および ASA FirePOWER のバージョン間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。
バージョン 6.5.0.x ASA FirePOWER module	*require*	バージョン 7.13.1 の ASDM。

Web ブラウザの互換性

Firepower によってモニタされるネットワークからの Web の参照

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

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

FMC でのセキュア通信

SSL 証明書を使用すると、FMCでアプライアンスとブラウザ間に暗号化チャネルを確立できます。

デフォルトでは、システムに自己署名 HTTPS サーバ証明書が付属しています。この証明書を、グローバルに知られているか、内部で信頼されている認証局（CA）によって署名された証明書に置き換えることをお勧めします。カスタムサーバ証明書要求を生成し、[HTTPS証明書（HTTPS Certificates）] ページでカスタムサーバ証明書をインポートすることができます。**[システム（System）] > [設定（Configuration）]** を選択し、[HTTPS証明書（HTTPS Certificates）] をクリックします。

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

Firepower Web インターフェイスでテストされたブラウザ

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

Note

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

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

ブラウザ	必要な設定と追加の警告
Google Chrome	JavaScript、Cookie Chrome は、画像、CSS、JavaScript などの静的コンテンツを、システムによって提供される自己署名証明書とともにキャッシュしません。これにより、特に低帯域幅環境では、ページの読み込み時間が長くなります。自己署名証明書を置き替えない場合は、代わりに、自己署名証明書をブラウザまたは OS の信頼ストアに追加できます。
Mozilla Firefox	JavaScript、Cookie、TLS v1.2 これらを更新すると、Firefoxは、システムが提供する自己署名証明書を信頼しなくなる場合があります。証明書を置き換えない場合、ログイン ページがロードされないときは Firefox を更新します。Firefox の検索バーに「**`about:support`**」と入力し、[Firefoxをリフレッシュ（Refresh Firefox）] をクリックします。一部の設定が失われます。Refresh Firefox サポートページを参照してください。
Microsoft Internet Explorer 11（Windows のみ）	JavaScript、Cookie、TLS v1.2、128 ビット暗号化 また、次のことを行う必要があります。 • [Check for newer versions of stored pages] 閲覧履歴オプションについては、[Automatically] を選択してください。 • [サーバーにファイルをアップロードするときにローカル ディレクトリのパスを含める] カスタム セキュリティ設定を無効にします。 • Firepower Web インターフェイスの IP アドレス/URL の互換表示を有効にします。 FMC ウォークスルーではテストされていません。

ブラウザ拡張機能との互換性

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

画面解像度の要件

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

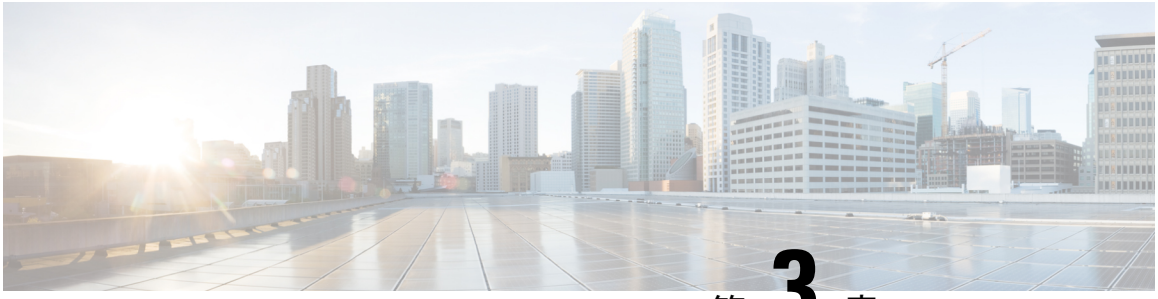
インターフェイス	解像度
Firepower Management Center	1280 X 720
Firepower Device Manager	1024 X 768
を管理している ASDM ASA FirePOWER module	1024 X 768
Firepower Chassis Manager 向け Firepower 4100/9300 シャーシ	1024 X 768

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, on page 57を参照してください。

Table 6: その他の互換性関連のリソース

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



第 3 章

特長と機能

Firepower バージョン 6.5.0.x には以下が含まれます。

新機能

バージョン 6.5.0.x のパッチには新機能は導入されていません。

廃止された機能

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

詳細については、『Cisco Firepower Management Center 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。

これらの機能はバージョン 6.5.0.x のパッチで廃止されました。

表 *7:* バージョン *6.5.0.x* で廃止された機能

機能	バージョン	説明
バージョン 6.5.0.3 は使用できなくなりました。	6.5.0.3	バージョン 6.5.0.3 は、2019 年 2 月 4 日（FMC の場合）および 2020 年 3 月 2 日（デバイスの場合）に シスコ サポートおよびダウンロードサイトから削除されました。このバージョンを実行している場合は、続行しても安全です。 関連するバグ：CSCvs86257 影響を受けるプラットフォーム：すべて
出力最適化	6.5.0.2	FTD デバイスをバージョン 6.5.0.2+ にパッチを適用すると、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） バージョン 6.5.0.2+ にパッチを適用することをお勧めします。バージョン 6.5.0 または 6.5.0.1 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。 関連するバグ：CSCvq34340 影響を受けるプラットフォーム：FTD
バージョン 6.5.0.1 は使用できなくなりました。	6.5.0.1	バージョン 6.5.0.1 は 2019 年 12 月 19 日に シスコ サポートおよびダウンロードサイトから削除されました。このバージョンを実行している場合は、アップグレードすることをお勧めします。 バージョン 6.5.0.1 から、それ以降のパッチにアップグレードした後でそのパッチをアンインストールすると、バージョン 6.5.0.1 に戻ります。その時点で、ただちにアップグレードするか、バージョン 6.5.0.1 をアンインストールする必要があります。バージョン 6.5.0.1 のままにしないでください。 影響を受けるプラットフォーム：すべて

FMC How-To ウォークスルー

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

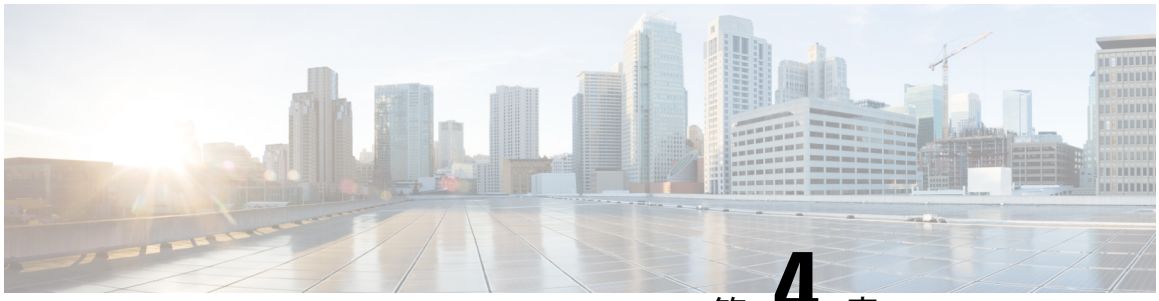
（注） ウォークスルーはFirefoxおよびChromeブラウザでテストされています。別のブラウザで問題が発生した場合は、Firefox または Chrome に切り替えてください。問題が解消されない場合は、Cisco TAC にお問い合わせください。

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

表 *8*：ウォークスルーのトラブルシューティング

問題	解決方法
ウォークスルーを開始するための [How To] リンクが見つからない。	ウォークスルーが有効になっていることを確認します。ユーザ名の下にあるドロップダウンリストから、[ユーザ設定（User Preferences）] を選択し、[設定方法（How-To Settings）] をクリックします。
ウォークスルーが予期しないタイミングで表示される。	ウォークスルーが予期しないタイミングで表示される場合は、ウォークスルーを終了します。
ウォークスルーが突然消えたり終了したりする。	ウォークスルーが消えた場合は、次のようにします。 • ポインタを移動します。 FMC で進行中のウォークスルーが表示されなくなることがあります。たとえば、別のトップレベルメニューをポイントすると表示されなくなります。 • 別のページに移動して、もう一度やり直してください。 ポインタを移動しても表示されない場合は、ウォークスルーが終了している可能性があります。

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。



第 4 章

バージョン 6.5.0.x へのアップグレード

この章では、バージョン 6.5.0.x の重要なリリースに固有の情報を提供します。

に関するガイドラインと警告 バージョン 6.5.0.x

バージョン 6.5.0.x パッチに特に適用される重要なアップグレードガイドラインと警告はありません。ただし、「一般的なガイドラインと警告 （15 ページ）」を確認するようにしてください。

一般的なガイドラインと警告

これらの重要なガイドラインと警告は、すべてのアップグレードに適用されます。ただし、このリストは包括的なものではありません。アップグレードパスの計画、OS のアップグレード、準備状況チェック、バックアップ、メンテナンス期間など、アップグレードプロセスに関するその他の重要な情報へのリンクについては、「アップグレード手順 （31 ページ）」を参照してください。

イベントデータと設定データのバックアップ

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

- アップグレード前：アップグレードが致命的なレベルで失敗した場合は、再イメージ化と復元が必要になることがあります。再イメージ化によって、システムパスワードを含むほとんどの設定が工場出荷時の初期状態に戻ります。最近のバックアップがある場合は、通常の操作にすばやく戻ることができます。

- アップグレード後：これにより、新しくアップグレードされた展開のスナップショットが作成されます。新しい FMC バックアップファイルがデバイスがアップグレードされたことを「認識」するように、管理対象デバイスをアップグレードした後にFMCをバックアップすることをお勧めします。

安全なリモートロケーションにバックアップし、正常に転送が行われることを確認する必要があります。アップグレードによって、ローカルに保存されたバックアップは消去されます。特に、バックアップファイルは暗号化されていないため、不正アクセスを許可しないでください。バックアップ ファイルが変更されていると、復元プロセスは失敗します。

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

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

NTP 同期の確認

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

時刻を確認するには、次の手順を実行します。

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

帯域幅をチェックする

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

FMC の展開では、アップグレードパケージをアップグレード時に管理対象デバイスに転送する場合は、帯域幅が不十分だとアップグレード時間が長くなったり、アップグレードがタイム

アウトする原因となる可能性があります。アップグレードする前に、管理対象デバイスに Firepower アップグレードパッケージを手動でプッシュ（コピー）することをお勧めします。詳細については、『Guidelines for Downloading Data from the Firepower Management Center to Managed Devices』（トラブルシューティング テクニカルノーツ）を参照してください。

アプライアンスアクセス

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

署名付きのアップグレードパッケージ

Firepower では、正しいファイルを使用していることを確認できるようにするために、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、署名付きのパッケージが不要になった後、それらのパッケージを削除します。

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

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

シスコとのデータの共有

一部の機能にシスコとのデータ共有が含まれます。

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

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

6.5.0+ 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 TAC は TAC 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。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。

アップグレードにより侵入ルールをインポートして自動的に有効化できます。

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

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

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

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

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

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

応答しないアップグレード

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

アップグレードする最小バージョン

現在のメジャー バージョン シーケンス内だけで Firepower ソフトウェアにパッチを適用できます。パッチは累積されるため、常に最新のパッチに直接スキップできます。

Table 9: Firepower ソフトウェアをバージョン *6.5.0.x* にアップグレードするための最小バージョン

プラットフォーム	最小バージョン
Firepower Management Center FMC 展開のすべての管理対象デバイス。	6.5.0
FDM を使用した Firepower Threat Defense（すべてのプラットフォーム）	6.5.0
ASDM を使用した ASA FirePOWER	6.5.0

時間テストとディスク容量の要件

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

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

時間テストについて

ここで指定した時間の値は、社内のテストに基づいています。

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

テスト条件

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

- ハイアベイラビリティと拡張性：スタンドアロンデバイスでテストします。

  ハイアベイラビリティの構成またはクラスタ化された構成では、動作の継続性を保持するため、複数のデバイスは1つずつアップグレードされます。アップグレード中は、各デバイスはメンテナンス モードで動作します。そのため、デバイス ペアまたはクラスタ全体のアップグレードには、スタンドアロンデバイスのアップグレードよりも長い時間がかかります。

- 構成：シスコでは、構成およびトラフィック負荷が最小限のアプライアンスでテストを行います。

  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 6.5.0.4 の時間とディスク容量

Table 10: バージョン *6.5.0.4* の時間とディスク容量

プラットフォーム	ボリュームの容量	必要容量	FMC の容量	時間
Firepower 1000 シリーズ	2.6 GB	2.6 GB	500 MB	20 分
Firepower 2100 シリーズ	[2.5 GB]	[2.5 GB]	530 MB	18 分
Firepower 4100 シリーズ	[2.5 GB]	[2.5 GB]	360 MB	13 分
Firepower 9300	[2.5 GB]	[2.5 GB]	360 MB	17 分
ASA 5500-X シリーズ with FTD	1.9 GB	110 MB	310 MB	16 分
FTDv：VMware 6.0	1.9 GB	110 MB	310 MB	9 分
ASA FirePOWER	2.6 GB	20 MB	340 MB	72 分
NGIPSv：VMware 6.0	740 MB	20 MB	230 MB	8 分

バージョン 6.5.0.3 の時間とディスク容量

バージョン 6.5.0.3 は、2019 年 2 月 4 日（FMC の場合）および 2020 年 3 月 2 日（デバイスの場合）に シスコ サポートおよびダウンロード サイト から削除されました。このバージョンを実行している場合は、続行しても安全です。

バージョン 6.5.0.2 の時間とディスク容量

Table 11: バージョン *6.5.0.2* の時間とディスク容量

プラットフォーム	ボリュームの容量	必要容量	FMC の容量	時間
FMC	2.6 GB	20 MB	—	42 分
FMCv：VMware 6.0	2.7 GB	23 MB	—	34 分
Firepower 1000 シリーズ	[2.5 GB]	[2.5 GB]	480 MB	12 分
Firepower 2100 シリーズ	2.3 GB	2.3 GB	500 MB	17 分
Firepower 4100 シリーズ	2.3 GB	2.3 GB	340 MB	13 分
Firepower 9300	2.3 GB	2.3 GB	340 MB	17 分

プラットフォーム	ボリュームの容量	必要容量	FMC の容量	時間
ASA 5500-X シリーズ with FTD	1.9 GB	110 MB	280 MB	22 分
FTDv：VMware 6.0	1.7 GB	110 MB	280 MB	10 分
ASA FirePOWER	[2.5 GB]	20 MB	320 MB	56 分
NGIPSv：VMware 6.0	680 MB	18 MB	210 MB	9 分

バージョン 6.5.0.1 の時間とディスク容量

バージョン 6.5.0.1 は 2019 年 12 月 19 日に シスコ サポートおよびダウンロード サイト から削除されました。このバージョンを実行している場合は、アップグレードすることをお勧めします。

トラフィック フロー、検査、およびデバイス動作

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

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

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

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

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

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

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

表 *12 : FXOS* アップグレード中のトラフィックの動作

展開	方法	トラフィックの動作
スタンドアロン	—	ドロップされる
ハイアベイラビリティ	**ベストプラクティス**：スタンバイで FXOS を更新し、アクティブピアを切り替えて新しいスタンバイをアップグレードします。	影響なし
	スタンバイでアップグレードが終了する前に、アクティブピアで FXOS をアップグレードします。	1 つのピアがオンラインになるまでドロップされる
シャーシ間クラスタ（6.2 以降）	**ベストプラクティス**：少なくとも 1 つのモジュールを常にオンラインにするため、一度に 1 つのシャーシをアップグレードします。	影響なし
	ある時点ですべてのモジュールを停止するため、シャーシを同時にアップグレードします。	少なくとも 1 つのモジュールがオンラインになるまでドロップされる
シャーシ内クラスタ（Firepower 9300 のみ）	Fail-to-wire 有効：[バイパス：スタンバイ（Bypass: Standby）] または [バイパス：強制（Bypass-Force）]（6.1 以降）	インスペクションなしで転送
	Fail-to-wire 無効：[バイパス：無効（Bypass: Disabled）]（6.1 以降）	少なくとも 1 つのモジュールがオンラインになるまでドロップされる
	fail-to-wire モジュールなし。	少なくとも 1 つのモジュールがオンラインになるまでドロップされる

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

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

表 *13 : Firepower* ソフトウェアアップグレード中のトラフィックの動作：スタンドアロン *FTD* デバイス

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

ハイアベイラビリティペア：FirePOWER ソフトウェアアップグレード

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

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

クラスタ：FirePOWER ソフトウェアアップグレード

Firepower Threat Defense クラスタのデバイスで FirePOWER ソフトウェアをアップグレードする間に、トラフィックフローまたはインスペクションが中断されることはありません。継続稼

働できるように、一度に1つずつアップグレードされます。アップグレード中、デバイスはメンテナンスモードで稼働します。

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

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

（注） バージョン6.2.0、6.2.0.1、または6.2.0.2からシャーシ間クラスタをアップグレードすると、各モジュールがクラスタから削除されるときに、トラフィックインスペクションで2～3秒のトラフィック中断が発生します。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、デバイスがトラフィックを処理する方法に応じて異なります。

ハイアベイラビリティとクラスタリング ヒットレス アップグレードの要件

ヒットレスアップグレードの実行には、次の追加要件があります。

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

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

1. FTD を 6.2.2.2 以降にアップグレードします。

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

3. FTD を最終バージョンにアップグレードします。

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

1. FTD を 6.2.2.5 にアップグレードします。

2. FXOS を 2.6.1 にアップグレードします。

3. FTD を 6.4.0 にアップグレードします。

バージョン6.1.0へのアップグレード：FTDハイアベイラビリティペアのバージョン6.1.0へのヒットレスアップグレードを実行するには、プレインストールパッケージが必要です。詳細に

ついては、『Firepower System Release Notes Version 6.1.0 Preinstallation Package』を参照してください。

展開時のトラフィックの動作

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

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

表 *14 : FTD* 展開時のトラフィックの動作

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

FTD アップグレード時の動作：その他のデバイス

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

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

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

表 *15 : Firepower* ソフトウェアアップグレード中のトラフィックの動作：スタンドアロン *FTD* デバイス

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

ハイアベイラビリティペア：FirePOWER ソフトウェアアップグレード

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

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

展開時のトラフィックの動作

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

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

表 *16 : FTD* 展開時のトラフィックの動作

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

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

ASA FirePOWER アップグレード時の動作

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

表 *17 : ASA FirePOWER* アップグレード中のトラフィックの動作

トラフィック リダイレクト ポリシー	トラフィックの動作
フェール オープン（**sfr fail-open**）	インスペクションなしで転送
フェール クローズ（**sfr fail-close**）	ドロップされる
モニタのみ（**sfr {fail-close}|{fail-open} monitor-only**）	パケットをただちに出力、コピーへのインスペクションなし

ASA FirePOWER 展開時のトラフィックの動作

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

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

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

NGIPSv アップグレード時の動作

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

Firepower ソフトウェア アップグレード

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

表 *18 : NGIPSv* アップグレード中のトラフィックの動作

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

展開時のトラフィックの動作

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

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

表 *19 : NGIPSv* 展開時のトラフィックの動作

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

インターフェイスの設定	トラフィックの動作
インライン、タップ モード	すぐにパケットを出力し、バイパス Snort をコピーする
パッシブ	中断なし、インスペクションなし

アップグレード手順

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

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

アップグレードパッケージ

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

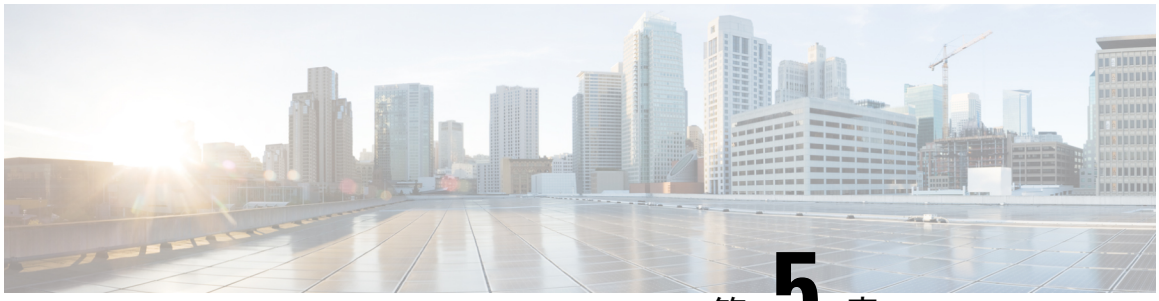
- FMCv を含む Firepower Management Center：https://www.cisco.com/go/firepower-software
- Firepower Threat Defense（ISA 3000）：https://www.cisco.com/go/isa3000-software
- Firepower Threat Defense（FTDv を含む他のすべてのモデル）：https://www.cisco.com/go/ftd-software
- ASA with FirePOWER Services（ASA 5500-X シリーズ）：https://www.cisco.com/go/asa-firepower-sw
- ASA with FirePOWER Services（ISA 3000）：https://www.cisco.com/go/isa3000-software
- NGIPSv：https://www.cisco.com/go/ngipsv-software

署名付きの（.tar）パッケージは解凍しないでください。

Table 20:* のアップグレード パッケージ バージョン *6.5.0.x

プラットフォーム	パッケージ
FMC/FMCv	Cisco_Firepower_Mgmt_Center_Patch-*version-build*.sh.REL.tar
Firepower 1000 シリーズ	Cisco_FTD_SSP_FP1K_Patch-*version-build*.sh.REL.tar

プラットフォーム	パッケージ
Firepower 2100 シリーズ	Cisco_FTD_SSP_FP2K_Patch-*version-build*.sh.REL.tar
Firepower 4100/9300 シャーシ	Cisco_FTD_SSP_Patch-*version-build*.sh.REL.tar
FTD を搭載した ASA 5500-X シリーズ FTD を搭載した ISA 3000 Firepower Threat Defense 仮想	Cisco_FTD_Patch-*version-build*.sh.REL.tar
ASA FirePOWER	Cisco_Network_Sensor_Patch-*version-build*.sh.REL.tar
NGIPSv	Cisco_Firepower_NGIPS_Virtual_Patch-*version-build*.sh.REL.tar



第 5 章

バージョン 6.5.0.x のパッチのアンインストール

Firepower のパッチは次の場所からアンインストールできます。

- FMC とその管理対象デバイス
- ASDM によって管理されている ASA FirePOWER モジュール

パッチをアンインストールすると、アップグレード前のバージョンがアプライアンスで実行されます。

（注） FDM によって管理されている FTD デバイスからパッチをアンインストールすることは「できません」。また、任意のアプライアンスから Firepower ソフトウェアのメジャー バージョンをアンインストールすることもできません。このような場合は、新しくインストールする必要があります。

詳細については、以下を参照してください。

- アンインストールに関する注意事項と制約事項 （33 ページ）
- HA/スケーラビリティ環境でのアンインストール順序 （36 ページ）
- アンインストールの手順 （38 ページ）
- パッケージのアンインストール, on page 44

アンインストールに関する注意事項と制約事項

これらの重要なガイドラインと制限事項は、アンインストールに適用されます。

パッチのアンインストールがサポートされていることを確認します

特定のパッチをアンインストールすると、次のような問題が Firepower アプライアンスで発生する可能性があります。

- アンインストール後に設定変更を展開できない

- オペレーティングシステムと Firepower ソフトウェアの間に互換性がなくなる
- セキュリティ認定コンプライアンスが有効な状態（CC/UCAPL モード）でそのパッチが適用されていた場合、アプライアンスの再起動時に FSIC（ファイル システム整合性チェック）が失敗する

⚠

注意 セキュリティ認定準拠が有効な場合に FSIC が失敗すると、Firepower ソフトウェアは起動せず、リモート SSH アクセスが無効になり、ローカルコンソールを介してのみアプライアンスにアクセスできます。この問題が発生した場合は、Cisco TAC にお問い合わせください。

このような場合に、前のパッチに戻す必要があるときは、再イメージ化してからアップグレードすることをお勧めします。

次の表に、アンインストールしてはならない状況を示します。

表 *21* : アンインストール時に後続の問題が発生したバージョン *6.5.0.x* のパッチ

プラットフォーム	アンインストール元	アップグレード元が次の場合
FMC/FMCv	6.5.0.1	6.5.0

シェルを使用して先にデバイスからアンインストールする

FMC の展開では、先に管理対象デバイスからパッチをアンインストールします。FMC では管理対象デバイスよりも後のバージョンを実行することを推奨します。

デバイス パッチをアンインストールするには、エキスパート モードとも呼ばれる Linux シェルを使用する必要があります。これは、デバイスから「個別に」、かつ「ローカルに」アンインストールすることを意味します。つまり、次のようになります。

- クラスタ化された、スタック構成の、またはハイ アベイラビリティ（HA）の Firepower デバイスから、あるいは FirePOWER Services デバイスのあるクラスタ化 ASA またはフェールオーバー ASA から、パッチを一括でアンインストールすることはできません。中断を最小限に抑えるアンインストール順序を計画するには、「HA/スケーラビリティ環境でのアンインストール順序 （36 ページ）」を参照してください。
- FMC、ASDM、または FDM を使用してデバイスからパッチをアンインストールすることも、7000/8000 シリーズ デバイスのローカル Web インターフェイスを使用することもできません。
- FMC のユーザ アカウントを使用して、いずれかの管理対象デバイスにログインしてデバイスからパッチをアンインストールすることはできません。Firepower アプライアンスでは独自のユーザ アカウントを維持しています。
- デバイスの `admin` ユーザとして、または CLI 設定アクセス権を持つ別のローカル ユーザとして、デバイス シェルにアクセスできる必要があります。シェル アクセスを無効にした場合、デバイス パッチをアンインストールすることはできません。デバイスのロックダウンを元に戻すには、Cisco TAC にご連絡ください。

デバイスより後に FMC からアンインストールする

管理対象デバイスからアンインストールした後に、FMC からパッチをアンインストールします。アップグレードと同様に、ハイアベイラビリティ FMC から一度に1つずつアンインストールする必要があります。「HA/スケーラビリティ環境でのアンインストール順序 （36 ページ）」を参照してください。

FMC パッチのアンインストールには FMC Web インターフェイスを使用することをお勧めします。管理者アクセス権が必要になります。Web インターフェイスを使用できない場合は、Linux シェルを、シェルの `admin` ユーザまたはシェルアクセス権を持つ外部ユーザのどちらかとして使用できます。シェル アクセスを無効にした場合は、FMC のロックダウンを元に戻すために Cisco TAC にご連絡ください。

NTP 同期の確認

アンインストールする前に、時刻の提供に使用している NTP サーバと Firepower アプライアンスが同期していることを確認します。同期されていないと、アンインストール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。

アプライアンス アクセス

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

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

ASA FirePOWER パッチをアンインストールする前に、ASA REST API を無効にしていることを確認してください。無効でない場合、アンインストールが失敗する可能性があります。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`。

無応答のアンインストール

アンインストールしているアプライアンスとの間での変更の展開、またはアンインストール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。進行中のアンインストールを再開しないでください。 アンインストール 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。アンインストールに失敗する、アプライ

アンスが応答しないなど、アンインストール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。

アンインストールに失敗した場合、再イメージ化が必要になることがあります。再イメージ化を行うと、ほとんどの設定が工場出荷時の状態に戻ります。このため、再イメージ化の前にイベント データと設定データを外部の場所にバックアップしておくことを強くお勧めします。

トラフィック フロー、検査、およびデバイス動作

アンインストール時のトラフィック 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。アップグレードは、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お勧めします。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 （22 ページ）を参照してください。

HA/スケーラビリティ環境でのアンインストール順序

Firepower アプライアンスからのパッチのアンインストールは、アプライアンスをユニットとしてアップグレードした場合であっても、個別に行います。特にハイ アベイラビリティ（HA）およびスケーラビリティの展開環境では、中断を最小限に抑えるアンインストール順序を計画する必要があります。アップグレードとは異なり、システムはこの操作を行いません。次の表に、HA/スケーラビリティ環境でのアンインストール順序の概要を示します。

通常は次のことに注意してください。

- 先にセカンダリ/スタンバイ/スレーブ ユニットからアンインストールし、その次にプライマリ/アクティブ/マスターからアンインストールします。
- 一度に 1 つずつアンインストールします。次のユニットに移る前に、パッチが 1 つのユニットから完全にアンインストールされるまで待ちます。

表 *22 : HA* 内の *FMC* の場合におけるアンインストール順序

FMC の環境	アンインストール順序
FMC ハイ アベイラビリティ	同期を一時停止した状態（「スプリットブレイン」と呼びます）で、FMC のピアから一度に 1 つずつアンインストールします。ペアが split-brain の状況で、構成の変更または展開を行わないでください。 **1.** 同期を一時停止します（スプリットブレインに移行します）。 **2.** スタンバイからアンインストールします。 **3.** アクティブからアンインストールします。 **4.** 同期を再開します（スプリットブレインから抜けます）。

表 *23 : HA* またはクラスタ内の *FTD* デバイスの場合におけるアンインストール順序

FTD の環境	アンインストール順序
FTD ハイ アベイラビリティ	ハイ アベイラビリティ用に設定された FTD デバイスからパッチをアンインストールすることはできません。先にハイ アベイラビリティを解除する必要があります。 **1.** ハイ アベイラビリティを解除します。 **2.** 以前のスタンバイからアンインストールします。 **3.** 以前のアクティブからアンインストールします。 **4.** ハイ アベイラビリティを再確立します。
FTD クラスタ	一度に 1 つのユニットからアンインストールし、マスター ユニットを最後に残します。クラスタ化されたユニットは、パッチのアンインストール中はメンテナンス モードで動作します。 **1.** スレーブ モジュールから一度に 1 つずつアンインストールします。 **2.** スレーブ モジュールの 1 つを新しいマスター モジュールに設定します。 **3.** 以前のマスターからアンインストールします。

表 *24 : ASA* フェール オーバーペア/クラスタ内の *ASA with FirePOWER Services* デバイスの場合におけるアンインストール順序

ASA 展開	アンインストール順序
ASA FirePOWER が有効な ASA アクティブ/スタンバイ フェール オーバー ペア	常にスタンバイからアンインストールします。 **1.** スタンバイ ASA デバイスの ASA FirePOWER モジュールからアンインストールします。 **2.** フェールオーバーします。 **3.** 新しいスタンバイ ASA デバイスの ASA FirePOWER モジュールからアンインストールします。

ASA 展開	アンインストール順序
ASA FirePOWER が有効な ASA アクティブ/アクティブ フェールオーバー ペア	アンインストールしないユニットの両方のフェールオーバー グループをアクティブにします。 1. プライマリ ASA デバイスの両方のフェールオーバー グループをアクティブにします。 2. セカンダリ ASA デバイスの ASA FirePOWER モジュールからアンインストールします。 3. セカンダリ ASA デバイスの両方のフェールオーバー グループをアクティブにします。 4. プライマリ ASA デバイスの ASA FirePOWER モジュールからアンインストールします。
ASA FirePOWER が有効な ASA クラスタ	アンインストールの前に、各ユニットでクラスタリングを無効にします。一度に 1 つのユニットからアンインストールし、マスターユニットを最後に残します。 1. スレーブ ユニットでクラスタリングを無効にします。 2. そのユニットの ASA FirePOWER モジュールからアンインストールします。 3. クラスタリングを再び有効にします。ユニットが再びクラスタに参加するのを待ちます。 4. 各スレーブユニットに対して手順を繰り返します。 5. マスターユニットでクラスタリングを無効にします。新しいマスターが引き継がれるまで待ちます。 6. 以前のマスターの ASA FirePOWER モジュールからアンインストールします。 7. クラスタリングを再び有効にします。

アンインストールの手順

ここでは、対象となるアプライアンスから Firepower パッチをアンインストールする方法について説明します。

スタンドアロン FMC からのアンインストール

次の手順を実行して、Firepower Management Center Virtual を含むスタンドアロンの Firepower Management Center からパッチをアンインストールします。

始める前に

管理対象デバイスからパッチをアンインストールします。FMC では管理対象デバイスよりも後のバージョンを実行することを推奨します。

ステップ 1 構成が古い管理対象デバイスに展開します。

アンインストールする前に展開すると、失敗する可能性が減少します。

ステップ 2 事前チェックを実行します。

- 正常性のチェック：FMC のメッセージ センターを使用します（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ます）。導入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。
- タスクの実行：また、メッセージ センターで、必須タスクが完了していることを確認します。アンインストールの開始時に実行中だったタスクは停止され、失敗したタスクとなって再開できなくなります。後で失敗ステータス メッセージを手動で削除できます。

ステップ 3 **[システム（System）] > [更新（Updates）]** を選択します。

ステップ 4 FMC のアンインストール パッケージの横にある [インストール（Install）] アイコンをクリックし、FMC を選択します。

正しいアンインストール パッケージがない場合は、Cisco TAC にお問い合わせください。

ステップ 5 [インストール（Install）] をクリックして、アンインストールを開始します。

アンインストールすることを確認し、FMC を再起動します。

ステップ 6 ログアウトするまで、メッセージ センターで進行状況を確認します。

パッチのアンインストール中は、設定の変更やデバイスへの展開をしないでください。メッセージ センターに進行状況が数分間表示されない場合や、アンインストールの失敗が示された場合でも、アンインストールを再開したり、FMC を再起動したりしないでください。代わりに、Cisco TAC にお問い合わせください。

ステップ 7 パッチをアンインストールして FMC が再起動したら、再び FMC にログインします。

ステップ 8 成功したことを確認します。

[ヘルプ（Help）] > [バージョン情報（About）] を選択し、現在のソフトウェア バージョン情報を表示します。

ステップ 9 メッセージ センターを使用して、導入環境に問題がないことを再度確認します。

ステップ 10 構成を再展開します。

ハイ アベイラビリティ FMC からのアンインストール

次の手順を実行して、ハイ アベイラビリティ ペアの Firepower Management Center からパッチをアンインストールします。

ピアから一度に1つずつアンインストールします。同期を一時停止した状態で、先にスタンバイからアンインストールし、次にアクティブからアンインストールします。スタンバイのFMCでアンインストールが開始されると、ステータスがスタンバイからアクティブに切り替わり、両方のピアがアクティブになります。この一時的な状態のことを「スプリットブレイン」と呼び、アップグレード中とアンインストール中を除き、サポートされていません。ペアがsplit-brainの状況で、構成の変更または展開を行わないでください。同期の再開後は変更内容が失われます。

始める前に

管理対象デバイスからパッチをアンインストールします。FMC では管理対象デバイスよりも後のバージョンを実行することを推奨します。

ステップ 1 アクティブな FMC で、構成が古い管理対象デバイスに展開します。

アンインストールする前に展開すると、失敗する可能性が減少します。

ステップ 2 同期を一時停止する前に、メッセージ センターを使用して導入環境に問題がないことを確認します。

FMC メニュー バーで、[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 センターを表示します。導入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。

ステップ 3 同期を一時停止します。

a) **[システム（System）] > [統合（[Integration）]**を選択します。
b) [ハイ アベイラビリティ（High Availability）] タブで、[同期の一時停止（Pause Synchronization）] をクリックします。

ステップ 4 FMC からパッチを一度に 1 つずつアンインストールします。先にスタンバイで行い、次はアクティブで行います。

「スタンドアロン FMC からのアンインストール （38 ページ）」の手順に従います。ただし、初期の展開は省略し、各 FMC で更新が成功したことを確認したら停止します。要約すると、それぞれの FMC で以下の手順を実行します。

a) 事前チェック（ヘルス、実行中のタスク）を実行します。
b) **[システム（System）] > [更新（Updates）]** ページで、パッチをアンインストールします。
c) ログアウトするまで進行状況を確認し、ログインできる状態になったら再びログインします。
d) アンインストールが成功したことを確認します。

ペアが split-brain の状況で、構成の変更または展開を行わないでください。

ステップ 5 アクティブ ピアにする FMC で、同期を再開します。

a) **[システム（System）] > [統合（Integration）]** の順に選択します。
b) [ハイ アベイラビリティ（High Availability）] タブで、[アクティブにする（Make-Me-Active）] をクリックします。
c) 同期が再開し、その他の FMC がスタンバイ モードに切り替わるまで待ちます。

ステップ 6 メッセージ センターを使用して、導入環境に問題がないことを再度確認します。

ステップ 7 構成を再展開します。

任意のデバイスからのアンインストール（FMC マネージド）

次の手順を実行して、Firepower Management Center 環境内の「1 台」の管理対象デバイスからパッチをアンインストールします。これには、物理および仮想デバイス、セキュリティ モジュール、および ASA FirePOWER モジュールが含まれます。

始める前に

- 特に HA/スケーラビリティの環境において、正しいデバイスからアンインストールしようとしていることを確認してください。「HA/スケーラビリティ環境でのアンインストール順序 （36 ページ）」を参照してください。
- ASA FirePOWER モジュールの場合は、ASA REST API を無効にしていることを確認してください。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`。

ステップ 1 デバイスの設定が古い場合は、この時点で FMC から展開します。

アンインストールする前に展開すると、失敗する可能性が減少します。

例外：混合バージョンのスタック、クラスタ、または HA ペアには展開しないでください。HA/スケーラビリティ環境では、最初のデバイスからアンインストールする前に展開しますが、すべてのメンバからパッチのアンインストールを終えるまでは再度展開しないでください。

ステップ 2 事前チェックを実行します。

- 正常性のチェック：FMC のメッセージ センターを使用します（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ます）。導入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。
- タスクの実行：また、メッセージ センターで、必須タスクが完了していることを確認します。アンインストールの開始時に実行中だったタスクは停止され、失敗したタスクとなって再開できなくなります。後で失敗ステータス メッセージを手動で削除できます。

ステップ 3 デバイスの Firepower CLI にアクセスします。`admin` として、または設定アクセス権を持つ別の Firepower CLI ユーザとしてログインします。

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

コンソールを使用する場合、一部のデバイスではデフォルトでオペレーティング システムの CLI に設定されており、Firepower CLI にアクセスする場合は追加の手順が必要になります。

Firepower 1000/2100 シリーズ	`connect ftd`

Firepower 4100/9300 シャーシ	`connect module slot_number console`、次に `connect ftd`（最初のログインのみ）
ASA FirePOWER	`session sfr`

ステップ 4 Firepower CLI プロンプトで、`expert`コマンドを使用して Linux シェルにアクセスします。

ステップ 5 uninstall コマンドを実行し、プロンプトが表示されたらパスワードを入力します。

```
sudo install_update.pl --detach /var/sf/updates/uninstall_package_name
```

パッケージ名はプラットフォームによって異なります。「パッケージのアンインストール（44 ページ）」を参照してください。 署名付きの（.tar）パッケージは解凍しないでください。

アンインストールをコンソールから実行している場合を除き、`--detach` オプションを使用して、ユーザ セッションがタイムアウトした場合にアンインストールが停止しないようにします。これを行わないと、アンインストールはユーザ シェルの子プロセスとして実行されます。接続が終了した場合は、プロセスが強制終了し、チェックが中断してアプライアンスが不安定な状態のままになることがあります。

注意 システムから、アンインストールの確認メッセージが表示されることはありません。このコマンドを入力すると、デバイスの再起動を含むアンインストールが開始されます。アンインストール時のトラフィック 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。準備が整っていることを確認してください。

ステップ 6 アンインストールをモニタします。

アンインストールを解除しなければ、コンソールまたは端末に進行状況が表示されます。解除した場合は、`tail` または `tailf` を使用してログを表示できます。

- FTD デバイス：`tail /ngfw/var/log/sf/update.status`
- その他のすべてのデバイス：`tail /var/log/sf/update.status`

ステップ 7 成功したことを確認します。

パッチをアンインストールしてデバイスを再起動した後、デバイスのソフトウェア バージョンが正しいことを確認します。FMC で、**[デバイス（Devices）]**>**[デバイス管理（Device Management）]** を選択します。

ステップ 8 メッセージ センターを使用して、導入環境に問題がないことを再度確認します。

ステップ 9 構成を再展開します。

例外：HA/スケーラビリティ環境では、混合バージョンのスタック、クラスタ、または HA ペアには展開しないでください。展開は、すべてのメンバーについてこの手順を繰り返した後にのみ行います。

次のタスク

- HA/スケーラビリティ環境の場合は、各デバイスについて計画した順序でこの手順を繰り返します。その後、最終的な調整を行います。たとえば、FTD HA 環境では、両方のピアからアンインストールした後に HA を再確立します。

- ASA FirePOWER モジュールでは、先に ASA REST API を無効にしていた場合は再度有効にします。ASA CLI から、`rest-api agent` を実行します。

ASA FirePOWER からのアンインストール（ASDM マネージド）

次の手順を実行して、ローカル管理されている ASA FirePOWER モジュールからパッチをアンインストールします。FMC を使用して ASA FirePOWER を管理している場合は、「任意のデバイスからのアンインストール（FMC マネージド） （41 ページ）」を参照してください。

始める前に

- 特に ASA のフェールオーバー/クラスタ環境において、正しいデバイスからアンインストールしようとしていることを確認してください。「HA/スケーラビリティ環境でのアンインストール順序 （36 ページ）」を参照してください。
- ASA REST API が無効になっていることを確認します。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`。

ステップ 1 デバイスの設定が古い場合は、この時点で ASDM から展開します。

アンインストールする前に展開すると、失敗する可能性が減少します。

ステップ 2 事前チェックを実行します。

- システム ステータス：**[モニタリング（Monitoring）] > [ASA FirePOWER のモニタリング（ASA FirePOWER Monitoring）] > [統計情報（Statistics）]** を選択し、すべてが想定どおりであることを確認します。
- 実行中のタスク：**[モニタリング（Monitoring）] > [ASA FirePOWER のモニタリング（ASA FirePOWER Monitoring）] > [タスク（Task）]** を選択し、必須タスクが完了していることを確認します。アンインストールの開始時に実行中だったタスクは停止され、失敗したタスクとなって再開できなくなります。後で失敗ステータス メッセージを手動で削除できます。

ステップ 3 ASA FirePOWER モジュールの Firepower CLI にアクセスします。`admin` として、または設定アクセス権を持つ別の Firepower CLI ユーザとしてログインします。

モジュールの管理インターフェイスに SSH 接続するか（ホスト名または IP アドレス）、コンソールを使用できます。コンソールを使用する場合、ASA 5585-X シリーズ デバイスは専用の ASA FirePOWER コンソール ポートを備えています。他の ASA モデルでは、コンソール ポートはデフォルトで ASA CLI に設定されており、Firepower CLI にアクセスするには `session sfr` コマンドを使用する必要があります。

ステップ 4 Firepower CLI プロンプトで、`expert`コマンドを使用して Linux シェルにアクセスします。

ステップ 5 uninstall コマンドを実行し、プロンプトが表示されたらパスワードを入力します。

```
sudo install_update.pl --detach
/var/sf/updates/Cisco_Network_Sensor_Patch_Uninstaller-version-build.sh.REL.tar
```

署名付きの（.tar）パッケージは解凍しないでください。

アンインストールをコンソールから実行している場合を除き、`--detach` オプションを使用して、ユーザセッションがタイムアウトした場合にアンインストールが停止しないようにします。これを行わないと、アンインストールはユーザ シェルの子プロセスとして実行されます。接続が終了した場合は、プロセスが強制終了し、チェックが中断してアプライアンスが不安定な状態のままになることがあります。

注意 システムから、アンインストールの確認メッセージが表示されることはありません。このコマンドを入力すると、デバイスの再起動を含むアンインストールが開始されます。アンインストール時のトラフィック 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。準備が整っていることを確認してください。

ステップ 6 アンインストールをモニタします。

アンインストールを解除しなければ、コンソールまたは端末に進行状況が表示されます。解除した場合は、`tail` または `tailf` を使用してログを表示できます。

```
tail /var/log/sf/update.status
```

パッチのアンインストール中は、デバイスに設定を展開しないでください。メッセージセンターに進行状況が数分間表示されない場合や、アンインストールの失敗が示された場合でも、アンインストールを再開したり、デバイスを再起動したりしないでください。代わりに、Cisco TAC にお問い合わせください。

ステップ 7 成功したことを確認します。

パッチをアンインストールしてモジュールを再起動した後、モジュールのソフトウェア バージョンが正しいことを確認します。**[設定（Configuration）] > [ASA FirePOWER の設定（ASA FirePOWER Configuration）] > [デバイス管理（Device Management）] > [デバイス（Device）]** を選択します。

ステップ 8 構成を再展開します。

次のタスク

- ASA フェールオーバー/クラスタ環境の場合は、各デバイスについて計画した順序でこの手順を繰り返します。
- ASA FirePOWER モジュールでは、先に ASA REST API を無効にしていた場合は再度有効にします。ASA CLI から、`rest-api agent` を実行します。

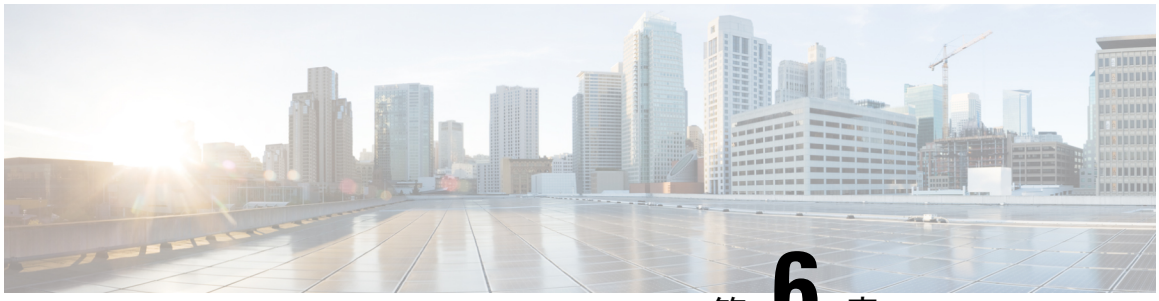
パッケージのアンインストール

Firepower アプライアンスにパッチを適用すると、そのパッチ用のアンインストーラーがアップグレード ディレクトリに自動的に作成されます。

- `/ngfw/var/sf/updates`（FTD デバイスの場合）
- `/var/sf/updates`（FMC および他のすべてのデバイス（7000/8000 シリーズ、ASA FirePOWER、NGIPSv）の場合）

パッケージがアップグレード ディレクトリにない場合（手動で削除した場合など）は、Cisco TAC にお問い合わせください。 署名付きの（.tar）パッケージは解凍しないでください。

プラットフォーム	パッケージ
FMC/FMCv	Cisco_Firepower_Mgmt_Center_Patch_Uninstaller-*version-build*.sh.REL.tar
Firepower 1000 シリーズ	Cisco_FTD_SSP_FP1K_Patch_Uninstaller-*version-build*.sh.REL.tar
Firepower 2100 シリーズ	Cisco_FTD_SSP_FP2K_Patch_Uninstaller-*version-build*.sh.REL.tar
Firepower 4100/9300 シャーシ	Cisco_FTD_SSP_Patch_Uninstaller-*version-build*.sh.REL.tar
FTD を搭載した ASA 5500-X シリーズ FTD を搭載した ISA 3000 FTDv	Cisco_FTD_Patch_Uninstaller-*version-build*.sh.REL.tar
Firepower 7000/8000 シリーズ	Cisco_Firepower_NGIPS_Appliance_Patch_Uninstaller-*version-build*.sh.REL.tar
NGIPSv	Cisco_Firepower_NGIPS_Virtual_Patch_Uninstaller-*version-build*.sh.REL.tar
ASA FirePOWER	Cisco_Network_Sensor_Patch_Uninstaller-*version-build*.sh.REL.tar



第 6 章

新規インストール バージョン 6.5.0

Firepower アプライアンスをアップグレードできない（または必要なアップグレード パスを実行したくない）場合は、Firepower のメジャー リリースを新規インストールできます。特定のパッチを実行するには、バージョン 6.5.0 をインストールしてからアップグレードしてください。

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。これらのすべてのシナリオ（ローカルとリモート間のデバイス管理の切り替えを含む）では、デバイス設定が失われます。

（注） 管理の再イメージ化または切り替えを行う前に、ライセンスの問題に対処してください。Cisco Smart Licensing を使用している場合は、孤立した権限付与の発生を防ぐために、Cisco Smart Software Manager（CSSM）から手動で登録解除する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 *25 :* シナリオ：新規インストールが必要ですか。

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

シナリオ	ソリューション	ライセンシング
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。
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

誤りを避けるには、注意深い計画と準備が役立ちます。Firepower リリースに精通していて、Firepower アプライアンスを再イメージ化したことがある場合でも、これらのガイドラインと制限事項に加えて、「設置手順 （54 ページ）」にリンクされている手順を必ず参照してください。

イベント データと設定データのバックアップ

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

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

安全なリモートロケーションにバックアップし、正常に転送が行われることを確認する必要があります。再イメージ化によって、システムパスワードを含むほとんどの設定が工場出荷時の初期状態に戻ります。アプライアンスに残っているすべてのバックアップが削除されます。特

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

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

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

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

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

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

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

ライセンスの問題の対処

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

ライセンスの詳細については、次を参照してください。

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

アプライアンス アクセス

再イメージ化により、ほとんどの設定が工場出荷時の初期状態に戻ります。

アプライアンスに物理的にアクセスできない場合、再イメージ化プロセスによって管理ネットワークの設定を維持できます。これにより、再イメージ化した後、アプライアンスに接続し

て、初期設定を実行できます。ネットワーク設定を削除する場合は、アプライアンスに物理的にアクセスできる必要があります。Lights-Out 管理（LOM）を使用することはできません。

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

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

シスコとのデータの共有

一部の機能にシスコとのデータ共有が含まれます。

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

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

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

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

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

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

バージョン 6.3 以降のインストールパッケージの名前が変更されていると、古い「物理」アプライアンス（FMC 2000 および 4000）の再イメージ化に関する問題が発生します。現在バージョン 5.x を実行していて、バージョン 6.5.0 を新規にインストールする必要がある場合は、インストールパッケージをダウンロードした後、その名前を「古い」名前に変更します。『Cisco Firepower Release Notes, Version 6.3.0』の「Renamed Upgrade and Installation Packages」の情報を参照してください。

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

スマート ライセンスの登録解除

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

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

登録を解除すると、仮想アカウントからアプライアンスが削除され、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 [スマートライセンスのステータス（Smart License Status）] の横の停止記号 をクリックします。

ステップ 4 警告を読み、登録解除することを確認します。

を使用した FTD デバイスの登録解除 FDM

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

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

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

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

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

ステップ 4 警告し、登録を解除することを確認します。

設置手順

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

***Table 26: Firepower Management Center* のインストール手順**

FMC プラットフォーム	ガイド
FMC 1600、2600、4600	Cisco Firepower Management Center 1600, 2600, and 4600 Hardware Installation Guide：Restoring a Firepower Management Center to Factory Defaults
FMC 1000、2500、4500	Cisco Firepower Management Center 1000, 2500, and 4500 Getting Started Guide：Restoring a Firepower Management Center to Factory Defaults
FMC 750、1500、3500 FMC 2000、4000	Cisco Firepower Management Center 750, 1500, 2000, 3500 and 4000 Getting Started Guide：Restoring a Firepower Management Center to Factory Defaults
FMCv および FMCv 300	『Cisco Firepower Management Center Virtual 入門ガイド』

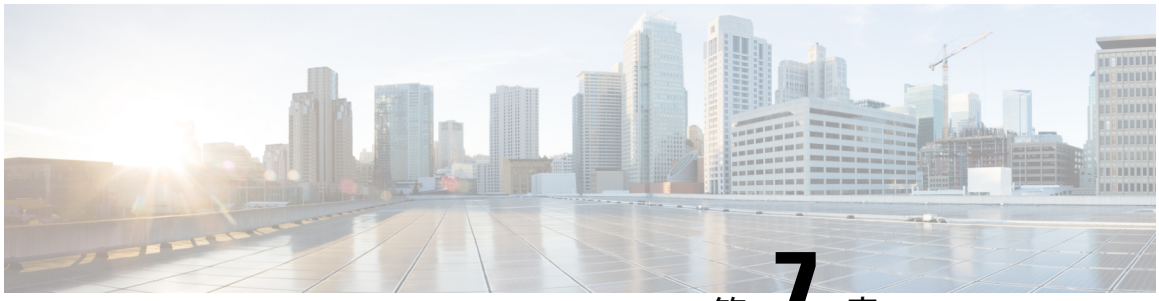
***Table 27: Firepower Threat Defense* のインストール手順**

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

FTD プラットフォーム	ガイド
FTDv：Azure	Cisco Firepower Threat Defense Virtual for the Microsoft Azure Cloud Quick Start Guide

Table 28: NGIPSv および ASA FirePOWER インストール手順

NGIPS プラットフォーム	ガイド
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

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

更新されたドキュメント： バージョン 6.5.0.x

少なくとも 1 つのバージョン 6.5.0.x パッチのために、次の Firepower のドキュメントが更新されました。

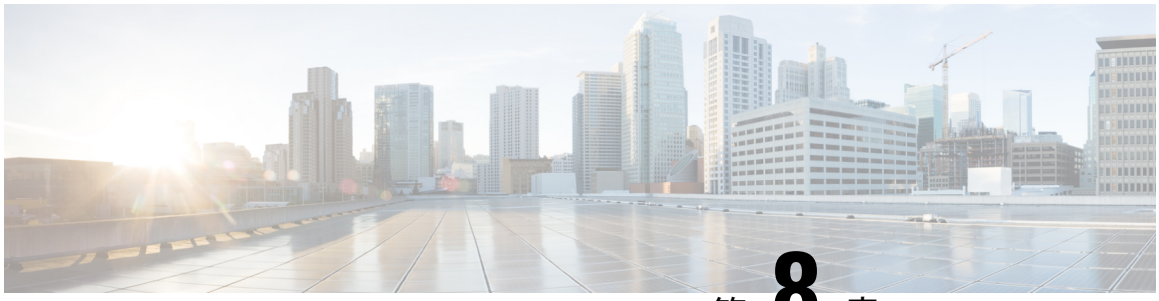
- Cisco Firepower Compatibility Guide

更新されていない、またはこのリリースで新しく使用可能になったドキュメントへのリンクについては、「ドキュメントロードマップ, on page 57」を参照してください。

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、各パッチの解決済みのバグが記載されています。

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

解決済みの問題の検索

サポート契約がある場合は、Cisco Bug Search Tool を使用して Firepower 製品の最新の解決済みバグリストを取得することができます。これらの一般的なクエリには、バージョン6.5.0.xパッチを実行している Firepower 製品の解決済みのバグが表示されます。

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

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

バージョン 6.5.0.4 で解決済みの問題

Table 29: バージョン *6.5.0.4* で解決済みの問題

不具合 ID	タイトル
CSCvq35440	Anyconnect のストラップ検証へのアップグレードの機能拡張：Cisco VPN セッションリプレイの脆弱性
CSCvs55990	ローカル/FDM で管理されている FTD 上に設定された SI DNS を使用した展開が失敗する
CSCvs86257	FMC のアップグレードが 800_post/1025_vrf_policy_upgrade.pl で失敗する

バージョン 6.5.0.3 で解決済みの問題

バージョン 6.5.0.3 は、2019 年 2 月 4 日（FMC の場合）および 2020 年 3 月 2 日（デバイスの場合）にシスコ サポートおよびダウンロード サイトから削除されました。このバージョンを実行している場合は、続行しても安全です。ここに記載されているバグは、バージョン 6.5.0.4 でも修正されています。

Table 30: バージョン *6.5.0.3* で解決済みの問題

不具合 ID	タイトル
CSCvd33448	バックアップ復元後、fireamp.pl が CPU を 100% 使用する
CSCvk55766	デバイスをプラットフォーム設定ポリシーに割り当てようとすると、一連のデバイスがランダムにポリシーから消える
CSCvm85823	SSH、ssh_exec を実行できない：コンソールでの open(pager) エラー
CSCvo76866	2100 でのトレースバック：ウォッチドッグ
CSCvp04134	9.12.1 へのアップグレード時に HTTP CLI Exec でトレースバックする
CSCvp06526	短い CPU アフィニティに一致するように sfhassd スレッド CPU アフィニティを管理する
CSCvp70833	ASA/FTD：同じサービスの NAT ルールがエラー「エラー：NAT がポートを予約できません（ERROR: NAT unable to reserve ports）」を 2 回表示する
CSCvq29167	ブートアップ中にインターフェイスを無効にしたにもかかわらず、物理インターフェイスがリンク稼働状態になる
CSCvq46587	フェールオーバー後、アクティブユニットの TCP セッションがタイムアウトに達しても削除されない

不具合 ID	タイトル
CSCvq50587	ASA/FTD がスレッド名「BGP Router」でトレースバックし、リロードすることがある
CSCvq51284	FPR 2100、low block 9472 がデバイスを介してパケット損失を発生させる
CSCvq76198	FreeBSD システムのトラフィックの中断
CSCvq81516	FMC で 12 時～午後 1 時（UTC）の間の VPN イベントが表示されない
CSCvq87797	マルチコンテキスト 5585 ASA、透過的コンテキストで管理インターフェイス設定が失われる
CSCvq88644	tcp-proxy でのトレースバック
CSCvq93572	外部認証を使用して FTD にユーザを追加することができません。
CSCvq96495	FPR2100 のコンソール接続が約 20 分間ランダムに切断される
CSCvr13278	リロード後に PPPoE セッションが起動しない
CSCvr20486	FTD 1010 パッシブインターフェイスがユニキャストパケットを受信しない
CSCvr21803	入力 FTD インターフェイスに挿入された誤ったパケットによりスイッチ上で Mac アドレスがフラップする
CSCvr25768	ASA が display_hole_og でトレースバックすることがある
CSCvr29978	ルールを変更してすぐに保存すると、設定が削除されることがある
CSCvr38379	FPR2100 の「自動インストール」機能を使用すると、アップグレードした FTD がベース FTD バージョンに再イメージ化されない
CSCvr50266	リロードの問題によってデュアルスタック ASAv フェールオーバーがトリガーされる
CSCvr53058	tcp-intercept と AC ポリシーのモニタを設定すると、AC ポリシーのルックアップが SYN+ACK パケットに対して実行される
CSCvr54054	ID NAT トラフィックに対して Mac の書き換えが実行される
CSCvr54980	FPR2100：シャーシの背面にある電源ボタンをオフにしても、電源がオフにならない
CSCvr55400	スレッド名「cli_xml_server」で FTD/LINA がトレースバックし、リロードされる
CSCvr55678	6.5.0.2 以降での ClamAV zip-bomb 移行の脆弱性

不具合 ID	タイトル
CSCvr60111	設定がスタンバイから削除され、アクティブ時に展開が失敗する
CSCvr61492	REST API コールに関連し、デバイスのロードが低速になる
CSCvr66768	PBR 設定がプッシュされているときに FTD 展開時に LINA がトレースバックする
CSCvr72665	FMC の 6.3/6.4 へのアップグレードで、既存の廃止済み flexconfig を削除しないようにする必要がある
CSCvr73115	ポリシーインポート後の初期 FTD の展開によって未使用オブジェクトが発生し、ポリシーサイズが膨張する
CSCvr78166	「実行コンフィギュレーションの取得に失敗しました（failed to retrieve running configuration）」という理由で、展開が FTD 上で失敗した
CSCvr78832	SSH：デバイスをローカルで管理している場合は、新しく作成したローカルユーザがログインできない
CSCvr81457	TLS トラッカー（tls_trk_sniff_for_tls）がブロックを解放しようとすると、FTD がトレースバックする
CSCvr82133	FMC を 6.5 にアップグレードした後、ルートを追加できず、また、[デバイス管理（Device Management）] ページからインターフェイスを選択できない
CSCvr84572	FMC 6.5：FMC でのユーザのログインの失敗が監査ログのエントリに記録されない
CSCvr85295	Cisco Adaptive Security Appliance と Firepower Threat Defense ソフトウェア リモート
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
CSCvr90768	FTD：低速リンクを通じた展開は失敗する場合がある
CSCvs10443	6.5 CloudEvent コードが、6.4 コードが理解しない方法で config ファイルを書き込む
CSCvs10526	FTD での SSE 試行のスロットル
CSCvs15276	エラー：IPv6 ICMP の設定時に ::/0 のエントリが存在する
CSCvs32023	デフォルトでは、出力最適化が無効になっている
CSCvs39589	データチャネルがネゴシエートされていない場合は ASA が SSH タイムアウトを実行しない

不具合 ID	タイトル
CSCvs40531	AnyConnect 4.8 が FPR1000 シリーズで動作していない
CSCvs53705	Anyconnect セッションが誤って制限されている
CSCvs61555	Snort の不適切な削除によりポリシー展開が失敗し、侵入ポリシーエディタがハングする

バージョン 6.5.0.2 で解決済みの問題

Table 31: バージョン *6.5.0.2* で解決済みの問題

不具合 ID	タイトル
CSCvr52109	複数のデバイスへの展開後、FTD が正しいアクセスコントロールルールに一致しないことがある
CSCvr88123	マルチ展開により、侵入イベントが突然ドロップする
CSCvs28768	Cisco Firepower ソフトウェアの WhatFix ウォークスルーのデータの問題

バージョン 6.5.0.1 で解決済みの問題

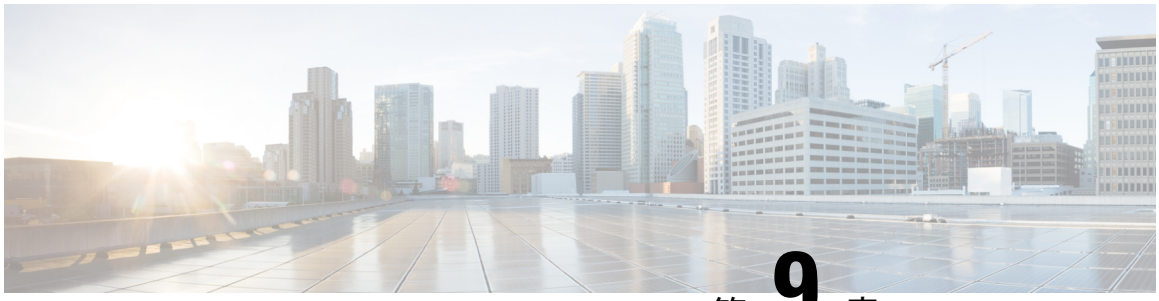
バージョン 6.5.0.1 は 2019 年 12 月 19 日に シスコ サポートおよびダウンロード サイト から削除されました。このバージョンを実行している場合は、アップグレードすることをお勧めします。ここに記載されているバグは、バージョン 6.5.0.2 でも修正されています。

Table 32: バージョン *6.5.0.1* で解決済みの問題

不具合 ID	タイトル
CSCva36446	SSL ハンドシェイクの成功直後に ASA が Anyconnect セッションの受け入れを停止するか、または接続を終了する
CSCvo88762	FTD インライン/トランスペアレントでパケットが入力インターフェイスを介して送り返される
CSCvp29554	lina_host_file_stat コールが原因でウォッチドッグがトレースバックする
CSCvp69229	OpenSSL 0 バイトレコードパディング Oracle の情報漏えいの脆弱性
CSCvp81083	TLS/VPN に関連する ASA/Lina のトレースバック
CSCvq09093	VPN 事前展開の検証がデバイスごとに約 20 秒かかる
CSCvq29969	再生成されていない場合でも、Firepower 推奨ルール数が変更される

不具合 ID	タイトル
CSCvq40943	6K スポークでの FTD 4150 VPN s2s 展開の失敗
CSCvq43453	サブドメインの変数セットで使用されている場合、ポートオブジェクトにオーバーライドを追加できない
CSCvq45000	NAT が設定されている場合に FP 8000 センサーへのポリシーの展開が失敗する
CSCvq53915	Cisco Firepower Management Center のクロスサイト スクリプティングの複数の脆弱性
CSCvq56257	キャッシュされたマルウェアの処置が想定どおりに期限切れにならないことがある
CSCvq63024	デュアルスタック ASAv の手動フェールオーバーの問題
CSCvq67271	子アクセスポリシーの ID によって特定ルールを取得すると、「404：見つかりませんでした（404: Not Found）」ステータスが返される
CSCvq70485	「securityzones」REST API が低速になる
CSCvq70775	FPR2100 FTD スタンバイユニットで 9K ブロックがリークする
CSCvq83019	ACPolicy に多数のアプリケーション フィルタ オブジェクトが使用されている場合に、ポリシー展開タスクの挿入の処理に長時間かかる
CSCvq83168	FMC ではサーバアドレスの後にインターフェイスを使用できないため、管理 VRF を使用した DNS ルックアップを実行できない
CSCvq92126	スレッド IPsec Message Handler での ASA のトレースバック
CSCvq93640	CCM レイヤで WRL6 と WRL8 のコミット ID が更新される（Sprint 67）
CSCvq94729	デルタ CLI の LINA ONLY セクションでのエラー時に展開のロールバックによってトラフィックの瞬間的なドロップが発生する
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
CSCvr00892	外部データベースアクセスで where 句が機能しない
CSCvr04954	FMC 6.4.0：別のドメインのスタックユニットでアップグレード後の展開が失敗する
CSCvr07421	セキュリティゾーン内にインターフェイスが 400 以上あると、deployDB の不適切な形成により、ポリシーの展開が失敗する
CSCvr10777	Ikev2 デーモンでの ASA トレースバック

不具合 ID	タイトル
CSCvr11395	スケジュール済みの展開時にデバイスグループから展開された一部のデバイスのみ
CSCvr12018	ASA：デフォルトルートが BGP を介して学習されている場合は、VPN トラフィックがトンネルルートを取得できない
CSCvr23580	2 つ以上の IP アドレスプールを削除できない
CSCvr25954	FTD/LINA スタンバイが、アクティブからのロギングコマンドの複製中にトレースバックし、リロードすることがある
CSCvr27445	ポリシーの展開中にユニットが HA に参加しようとすると、アプリケーションの同期が失敗する
CSCvr29638	FMC から ACP を展開した後、FPR2110 で HA FTD がクラッシュする
CSCvr35956	ServerKeyExchange と ClientKeyExchange の組み合わせが失敗する --> lina がクラッシュする
CSCvr36687	サブドメインの変数セットで使用されている場合、ネットワークオブジェクトにオーバーライドを追加できない
CSCvr37486	ASP テーブルで確立されているルールが、設定の削除時にアンインストールされない
CSCvr44123	セッションタイムアウトがデフォルトでない場合、FPR2100 の Chassis Manager または REST API を介してログインできない
CSCvr95287	Cisco Firepower Management Center LDAP 認証バイパスの脆弱性



第 9 章

既知の問題

既知の問題については、次を参照してください。

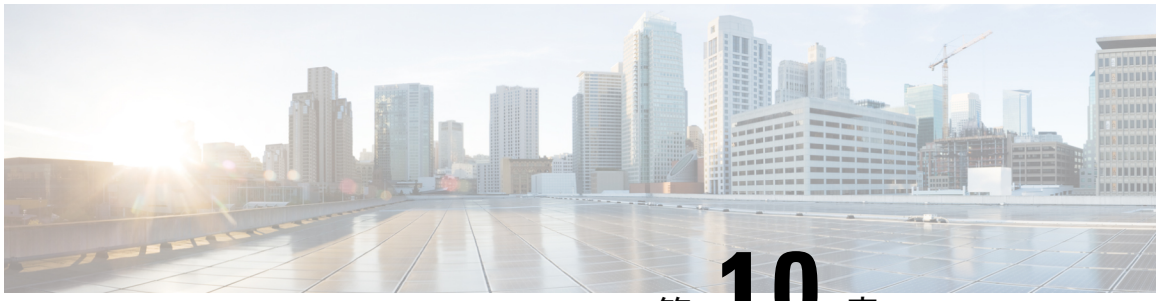
- 既知の問題の検索 （67 ページ）

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。これらの一般的なクエリには、バージョン 6.5.0.x パッチを実行している Firepower 製品の未解決のバグが表示されます。

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

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



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