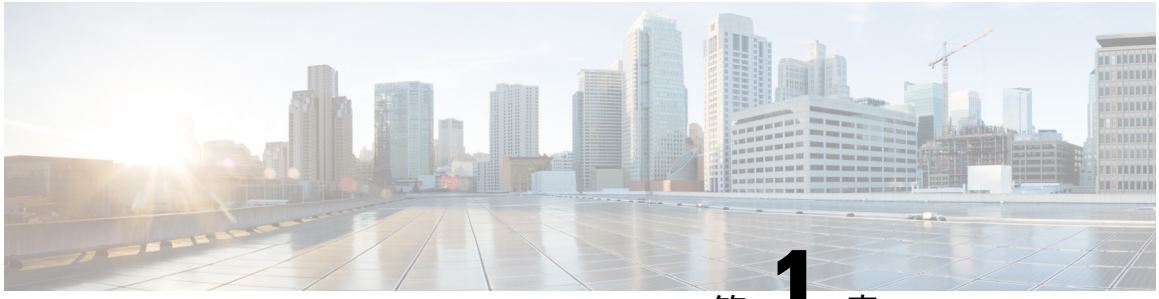
Cisco Firepower バージョン 6.6.x パッチリリースノート

初版：2020 年 7 月 22 日

最終更新：2022 年 3 月 24 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/

目 次



第 1 章

ようこそ

本マニュアルでは、重要なリリースに固有の情報を記載しています。

リリース日

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

表 *1* : バージョン *6.6.x* の日付

バージョン	ビルド	日付	プラットフォーム
6.6.5	81	2021 年 8 月 3 日	すべて
6.6.4	64	2021 年 4 月 29 日	Firepower 1000 シリーズ
	59	2021 年 4 月 26 日	FMC/FMCv Firepower 1000 シリーズを除くすべてのデバイス
6.6.3	80	2020 年 3 月 11 日	すべて
6.6.1	91	2020 年 9 月 20 日	すべて
	90	2020 年 9 月 8 日	—

バージョン	ビルド	日付	プラットフォーム
6.6.0	90	2020 年 5 月 8 日	Firepower 4112
		2020 年 4 月 6 日	FMC/FMCv Firepower 4112 を除くすべてのデバイス

表 *2:* バージョン *6.6.x* のパッチの日付

バージョン	ビルド	日付	プラットフォーム
6.6.5.2	14	2022 年 03 月 24 日	すべて
6.6.5.1	15	2021 年 12 月 6 日	すべて
6.6.0.1	7	2020 年 7 月 22 日	すべて

推奨リリース

新しい機能と解決済みの問題を利用するには、対象となるすべてのアプライアンスを推奨リリース以上にアップグレードすることをお勧めします。シスコ サポートおよびダウンロードサイトでは、推奨リリースに金色の星が付いています。

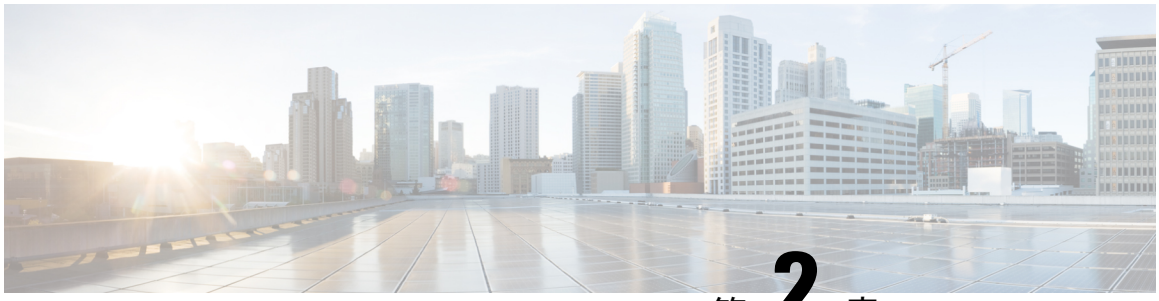
また、新機能ガイドにも推奨リリースを示します。

- Cisco Firepower Management Center の新機能（リリース別）
- Cisco Firepower Device Manager の新機能（リリース別）

古いアプライアンスの推奨リリース

アプライアンスが古すぎて推奨リリースを実行できず、ハードウェアを今すぐ更新しない場合は、メジャーバージョンを選択してから可能な限りパッチを適用します。一部のメジャーバージョンは長期または超長期に指定されているため、いずれかを検討してください。これらの用語の説明については、「Cisco NGFW Product Line Software Release and Sustaining Bulletin」を参照してください。

ハードウェアの更新に関心がある場合は、シスコの担当者またはパートナー担当者にお問い合わせください。



第 2 章

互換性

一般的な互換性情報については、次を参照してください。

- Cisco Firepower Compatibility Guide：バンドルされている OS やその他のコンポーネントのバージョンやビルドを含む、サポート対象のすべてのバージョンの詳細な互換性情報、および廃止されたプラットフォームの販売終了やサポート終了の通知へのリンク。
- 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：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。

本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

Firepower Management Center は、一元化されたファイアウォール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 は、仮想環境に完全なファイアウォール管理機能を提供します。

Firepower Management Center

本リリースでは、次のハードウェア FMC プラットフォームをサポートしています。

- 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

本リリースでは、次の FMCv パブリッククラウドの実装をサポートしています。

- Firepower Management Center VirtualAmazon Web Services（AWS）用
- Firepower Management Center VirtualMicrosoft Azure 用

このリリースでは、次の FMCv オンプレミス/プライベート クラウドの実装がサポートされています。

- Firepower Management Center Virtualカーネルベース仮想マシン（KVM）用
- Firepower Management Center VirtualVMware vSphere および VMware ESXi 6.0、6.5、6.7 用

サポートされている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ーし、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。

（注） これらのリリースノートには、本リリースでサポートされているデバイスが掲載されています。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 （7 ページ）」を参照してください。

表 *3 :* バージョン *6.6.0/6.6.x* の *Firepower Threat Defense*

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 2.8.1.105 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, 2.8(1)』を参照してください。
ASA 5508-X、5516-X ASA 5525-X、5545-X、5555-X ISA 3000	—	FTD 展開では、これらのデバイスのオペレーティングシステムを個別にアップグレードすることはありませんが、ISA 3000、ASA5508-Xおよび 5516-X に最新の 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

FTD プラットフォーム	OS/ハイパーバイザ	詳細情報
Firepower Threat Defense Virtual（FTDv）	次のいずれかです。 • AWS：Amazon Web Services • Azure：Microsoft Azure • 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。

表 *4 :* バージョン *6.6.0/6.6.x* の *NGIPS/ASA FirePOWER*

NGIPS/ASA FirePOWER 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) ～ 9.16(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、アップグレードすると、新機能を利用でき、問題も解決されます。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、ISA 3000、ASA5508-X および 5516-X に最新の 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
ASA 5525-X、5545-X、5555-X	ASA 9.5(2) ～ 9.14(x)	
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

すべてのデバイスが Firepower Management Center を使用した遠隔管理をサポートしており、これにより複数のデバイスを管理することができます。FMC では、その管理対象デバイスと同じまたはより新しいバージョンを実行する必要があります。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。メンテナンス（3桁）リリースの場合でも、最初に FMC をアップグレードする必要があります。

新しい FMC では、次の表に示されている複数のメジャーバージョンまで遡って古いデバイスを管理できます。ただし、導入環境全体を常に更新することをお勧めします。多くの場合、新機能の使用や問題解決の適用には、FMC とその管理対象デバイスの両方で最新リリースが必要になります。

表 *5 : FMC*とデバイス間の互換性

FMC バージョン	管理可能な最も古いデバイスバージョン
6.7.x	6.3.0
6.6.x	6.2.3
6.5.0	6.2.3
6.4.0	6.1.0
6.3.0	6.1.0
6.2.3	6.1.0

Firepower Device ManagerおよびCisco Defense Orchestrator

FMC に代わるものとして、多くの FTD デバイスが Firepower Device Manager および Cisco Defense Orchestrator の管理をサポートします。

- Firepower Device Manager が FTD に内蔵されており、単一のデバイスを管理できます。

  これにより、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あり、複数の FTD デバイスを管理できます。

  これにより、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。

FDM を使用したローカル管理をサポートするすべての FTD デバイスは、CDO も同時にサポートします。

表 *6 : FTD* との *FDM* および *CDO* の互換性

FTDプラットフォーム	FDM 互換	CDO 互換
Firepower 1000 シリーズ	6.4.0 以降	6.4.0 以降
Firepower 2100 シリーズ	6.2.1 以降	6.4.0 以降
Firepower 4100/9300	6.5.0 以降	6.5.0 以降
ASA 5500-X シリーズ	6.1.0 ～ 7.0.x	6.4.0 ～ 7.0.x
ISA 3000	6.2.3 以降	6.4.0 以降
AWS 用 FTDv	6.6.0 +	6.6.0 +
Azure 用 FTDv	6.5.0 以降	6.5.0 以降
KVM 用 FTDv	6.2.3 以降	6.4.0 以降
FTDv VMware の場合	6.2.2 以降	6.4.0 以降

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あり、ASA FirePOWER モジュールとも呼ばれています。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。

ほとんどの場合、新しい ASDM のバージョンは以前のすべての ASA のバージョンと下位互換性があります。ただし、いくつか例外があります。たとえば、ASDM 7.13(1) は ASA 9.10(1) で ASA 5516-X を管理できます。ASDM 7.13(1) と 7.14(1) は、ASA 5512-X、5515-X、5585-X、および ASASM をサポートしていませんでした。そのため、ASDM 7.13(1.101) または 7.14(1.48) にアップグレードして ASDM のサポートを復元する必要があります。詳細は、『Cisco ASA Compatibility』を参照してください。

新しい ASA FirePOWER モジュールには、次の表に示されている新しいバージョンの ASDM が必要です。

表 *7 : ASDM* と *ASA FirePOWER* の互換性

ASA FirePOWER のバージョン	最小 ASDM バージョン
6.7.x	7.15.1
6.6.x	7.14.1
6.5.0	7.13.1
6.4.0	7.12.1
6.3.0	7.10.1

ASA FirePOWER のバージョン	最小 ASDM バージョン
6.2.3	7.9.2

Web ブラウザの互換性

ブラウザ

現在サポートされている MacOS と Microsoft Windows で実行する、次の一般的なブラウザの最新バージョンでテストを実施しています。

- Google Chrome
- Mozilla Firefox
- Microsoft Internet Explorer 11（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 または Microsoft Edge 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 Internet Explorer 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 Internet Explorer 11 を使用している場合：

- [保存しているページの新しいバージョンの確認（Check for newer versions of stored pages）] 閲覧履歴オプションについては、[自動（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（Include local directory path when uploading files to server）] カスタムセキュリティ設定を無効にします。
- アプライアンスの IP アドレス/URL に対して [互換表示（Compatibility View）] を有効にします。

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。シスコの製品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

初めてログインした場合、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。

- Firepower Management Center：**[システム（System）]** > **[Configuration]** を選択し、[HTTPS 証明書（HTTPS Certificates）] をクリックします。
- Firepower Device Manager：[デバイス（Device）] をクリックしてから **[システム設定（System Settings）]** > **[管理アクセス（Management Access）]** リンクをクリックし、次に [管理Web サーバ（Management Web Server）] タブをクリックします。

詳しい手順については、オンラインヘルプまたはご使用の製品の構成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『Refresh Firefox』[英語]サポートページを参照してください 。

監視対象ネットワークからの参照

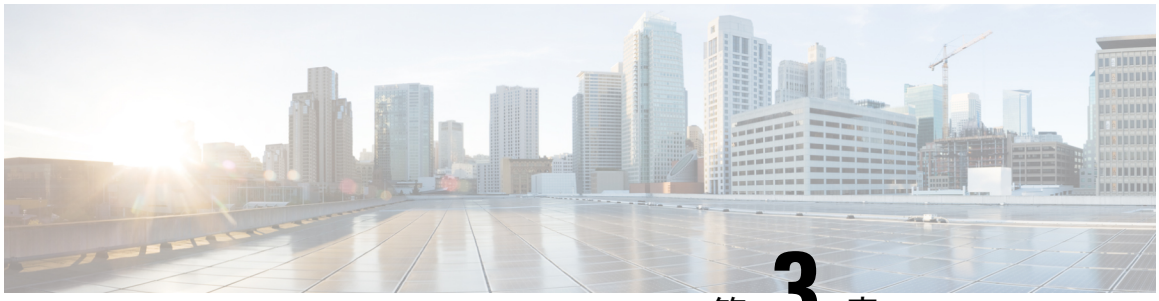
多くのブラウザでは、デフォルトで Transport Layer Security（TLS）v1.3 が使用されています。暗号化されたトラフィックを処理するために SSL ポリシーを使用していて、モニター対象ネットワーク内のユーザーが TLS v1.3 を有効にしてブラウザを使用している場合、TLS v1.3 をサポートする Web サイトのロードに失敗することがあります。

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 *8* : 画面解像度の要件

インターフェイス	解決策
Firepower Management Center	1280 X 720
Firepower Device Manager	1024 X 768
ASA FirePOWER moduleを管理している ASDM	1024 X 768
Firepower 4100/9300 用 Firepower Chassis Manager	1024 X 768



第 3 章

特長と機能

パッチには、新機能、機能、および緊急の問題または解決済みの問題に関連する動作の変更が含まれています。

Firepower Management Center 展開に関する機能

バージョン 6.6.x パッチには Firepower Management Center 展開に関する新機能または廃止された機能はありません。

（注） 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。ユーザーエージェント設定を使用して Firepower Management Center 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。Cisco Identity Services Engine/Passive Identity Connector（ISE/ISE-PIC）に切り替える必要があります。これにより、ユーザー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、シスコの担当者またはパートナーの担当者にお問い合わせください。

詳細については、『End-of-Life and End-of-Support for the Cisco Firepower User Agent』[英語] の通知、および『Firepower User Identity: Migrating from User Agent to Identity Services Engine』[英語] の技術メモを参照してください。

Firepower Device Manager 展開の機能

バージョン 6.6.x パッチには Firepower Device Manager 展開に関する新機能または廃止された機能はありません。

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、新規および更新された侵入ルールとプリプロセッサルール、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。

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、Snort のバージョンによって異なります。

- FMC：[ヘルプ（Help）] > [バージョン情報（About）] 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 *9*: 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。ユーザー名の下にあるドロップダウンリストから、[User Preferences] を選択し、[How-To Settings] をクリックします。
ウォークスルーが予期しないタイミングで表示される。	ウォークスルーが予期しないタイミングで表示される場合は、ウォークスルーを終了します。
ウォークスルーが突然消えたり終了したりする。	ウォークスルーが消えた場合は、次のようにします。 • ポインタを移動します。 FMC で進行中のウォークスルーが表示されなくなることがあります。たとえば、別のトップレベルメニューをポイントすると表示されなくなります。 • 別のページに移動して、もう一度やり直してください。 ポインタを移動しても表示されない場合は、ウォークスルーが終了している可能性があります。
ウォークスルーが FMC と同期していない。 • 誤った手順から開始される。 • 進行が早すぎる。 • 先に進まない。	ウォークスルーが同期していない場合は、次のようにします。 • 続行します。 たとえば、フィールドに無効な値を入力してエラーが表示された場合は、ウォークスルーが先に進行することがあります。戻ってエラーを解決してタスクを完了することが必要になる場合があります。 • ウォークスルーを終了し、別のページに移動してもう一度やり直します。 場合によっては続行できないこともあります。たとえば、手順の完了後に [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

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、ユーザーの場所、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。

デフォルトで Web 分析トラッキングに登録しています（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、初期設定完了後はいつでも登録を変更できます。

（注） バージョン 6.2.3 から 6.6.x にアップグレードすると、Web 分析トラッキングに登録される可能性があります。登録は、意図的に登録解除した場合でも行われ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、アップグレード後に登録解除してください。

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。

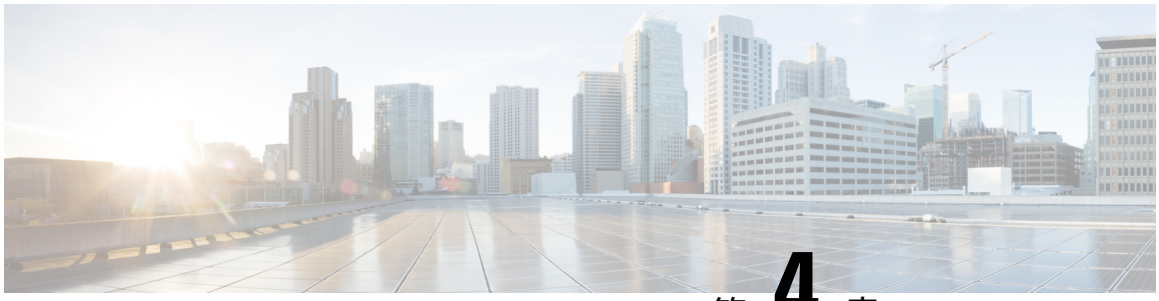
初期設定およびアップグレード中に、登録するか尋ねられます。登録はいつでも変更できます。

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、登録するか尋ねられます。登録はいつでも変更できます。

（注） この機能は、Firepower Management Center およびそこで管理される Firepower Threat Defense デバイスでサポートされます。バージョン 6.5.0 でのみ、FTD サポートは、FTD 搭載 Firepower 4100/9300 および Azure 向け FTDv に制限されます。この機能は、Firepower Device Manager ではサポートされていません。



第 4 章

ソフトウェアのアップグレード

この章では、重要なリリースに固有の情報を提供します。

アップグレードの計画

誤りを避けるには、注意深い計画と準備が役立ちます。この表はアップグレードの計画プロセスを要約したものです。詳細なチェックリストと手順については、該当するアップグレードまたは設定ガイドのを参照してください：アップグレード手順 （33 ページ）

表 *10*：アップグレードの計画フェーズ

計画フェーズ	Includes
計画と実現可能性	展開を評価します。 アップグレードパスを計画します。 すべてのアップグレードガイドラインを読み、設定の変更を計画します。 アプライアンスへのアクセスを確認します。 帯域幅を確認します。 メンテナンス時間帯をスケジュールします。

計画フェーズ	Includes
Backups	ソフトウェアをバックアップします。 Firepower 4100/9300 の FXOS をバックアップします。 ASA FirePOWER 用 ASA をバックアップします。
アップグレードパッケージ	アップグレードパッケージをシスコからダウンロードします。 システムにアップグレードパッケージをアップロードします。
関連するアップグレード	仮想展開内で仮想ホスティングをアップグレードします。 Firepower 4100/9300 の FXOS をアップグレードします。 ASA FirePOWER 用 ASA をアップグレードします。
最終チェック	設定を確認します。 NTP 同期を確認します。 ディスク容量を確認します。 設定を展開します。 準備状況チェックを実行します。 実行中のタスクを確認します。 展開の正常性と通信を確認します。

アップグレードする最小バージョン

パッチは4桁目のみを変更できます。以前のメジャーリリースまたはメンテナンスリリースからパッチに直接アップグレードすることはできません。

Version6.6.x.xパッチのアップグレードガイドライン

このチェックリストには、バージョン 6.6.x パッチに関するアップグレードガイドラインが含まれています。

表 *11* : バージョン *6.6.x.x* 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
	アップグレードの失敗：侵入イベントに関する電子メールアラート機能を搭載した FMC （19 ページ）	FMC	6.2.3 ～ 6.7.0.x	6.7.0 6.6.0、6.6.1、または 6.6.3 これらのリリースに対するすべてのパッチ
	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 （20 ページ）	FDM を使用した FTD	6.6.0	6.6.0.1

アップグレードの失敗：侵入イベントに関する電子メールアラート機能を搭載した FMC

展開：Firepower Management Center

アップグレード元：バージョン 6.2.3 ～ 6.7.0.x

アップグレード先（直接）：バージョン 6.6.0、6.6.1、6.6.3、6.7.0、およびこれらのリリースへのパッチ

関連するバグ：CSCvw38870、CSCvx86231

個々の侵入イベントに対して電子メールアラートを設定した場合は、Firepower Management Center を上記のいずれかのバージョンにアップグレードする前に、その設定を完全に無効にします。そうなっていなければ、アップグレードは失敗します。

この機能は、アップグレード後に再度有効にすることができます。この問題のためにすでにアップグレードに失敗した場合は、Cisco TAC に連絡してください。

侵入に関する電子メールアラートを完全に無効にするには、次の操作を行います。

1. Firepower Management Center で、**[Policies]** > **[Actions]** > **[Alerts]**を選択し、**[Intrusion Email]** をクリックします。
2. [State] を [off] に設定します。
3. [Rules] の横にある [Email Alerting per Rule Configuration] をクリックし、ルールの選択を解除します。

   アップグレード後に再選択できるように、選択を解除したルールを書き留めておきます。

ヒント　ルールの再選択に時間がかかりすぎる場合は、アップグレードする前に Cisco TAC に連絡してください。選択した内容を保存しておくことで、アップグレード後にすぐに再実装できるようにご案内いたします。

4. 設定を保存します。

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

展開：FTD と FDM をハイアベイラビリティペアとして設定

アップグレード元：バージョン 6.6.0

直接アップグレード先：バージョン 6.6.0.1

関連バグ：CSCvv45500

ハイアベイラビリティ（HA）の FDM 管理 FTD デバイスをバージョン 6.6.0.1 にアップグレードすると、アップグレード後の再起動後にデバイスが一時停止モードになります。HA を手動で再開する必要があります。

FMC 展開は影響を受けません。

FDM 管理 FTD HA ペアをバージョン 6.6.0.1 にアップグレードするには、次の手順を実行します。

1. スタンバイデバイスをアップグレードします。
2. アップグレードが完了してデバイスがリブートしたら、手動で HA を再開します。FDM または CLI を使用できます。
   - FDM：**[Device]** > **[High Availability]**をクリックし、ギアメニュー（⚙）から [Resume HA] を選択します。
   - CLI： **configure high-availability resume**

   新しくアップグレードされたデバイスの HA ステータスは、スタンバイ装置として、装置がピアとネゴシエートした後に正常に戻ります。
3. 新しくアップグレードしたデバイスがアクティブピアになるように、アクティブピアとスタンバイピアを切り替えます（強制フェールオーバー）。
4. 新しいスタンバイピアに対してこの手順を繰り返します。

FDM でのハイアベイラビリティの設定と管理の詳細については、『Firepower Device Manager 用 Cisco Firepower Threat Defense 構成ガイド』を参照してください。

応答しないアップグレード

アップグレード中は、設定の変更の実施または展開を行わないでください。システムが非アクティブに見えても、進行中のアップグレードを手動で再起動、シャットダウン、または再起動しないでください。システムが使用できない状態になり、再イメージ化が必要になる場合があります。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。

トラフィック フローとインスペクション

次の場合に、トラフィックフローおよび検査の中断が発生することがあります。

- デバイスを再起動する場合。
- デバイスソフトウェア、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。
- デバイスソフトウェアをアンインストールまたは場合。
- ドメイン間でデバイスを移動する場合。
- 設定の変更を展開する場合（Snort プロセスが再起動する）。

デバイスタイプ、高可用性または拡張性の設定、およびインターフェイス設定によって、中断の性質が決まります。これらのタスクは、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。

FirepowerThreatDefenseのアップグレード時の動作：Firepower4100/9300

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*：トラフィックの挙動：*FXOS* のアップグレード

展開	メソッド	トラフィックの動作
スタンドアロン	—	廃棄

展開	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。

スタンドアロンデバイスでのソフトウェアのアップグレード

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。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 *13*：トラフィックの挙動：スタンドアロンデバイスでのソフトウェアのアップグレード

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]（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。

高可用性および拡張性に関するソフトウェアのアップグレード

高可用性デバイスやクラスタ化されたデバイスのアップグレード中に、トラフィックフローや検査が中断されることはありません。

- FMC を使用した FTD：高可用性ペアの場合、スタンバイ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。

  クラスタの場合、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。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。

- FDM を使用した FTD：高可用性ペアの場合、スタンバイをアップグレードし、ロールを手動で切り替えてから、新しいスタンバイをアップグレードします。

ソフトウェアのアンインストール（パッチ）

バージョン 6.2.3 以降では、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に戻り、設定は変更されません。

- FMC を使用した FTD：スタンドアロンデバイスの場合、パッチのアンインストール中のトラフィックフローと検査の中断は、アップグレードの場合と同じになります。高可用性および拡張性の展開では、中断を最小限に抑えるために、アンインストールの順序を明確に計画する必要があります。これは、ユニットとしてアップグレードしたデバイスであっても、デバイスから個別にパッチをアンインストールするためです。
- FDM を使用した FTD：サポートされていません。

設定変更の導入

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*：トラフィックの動作：構成変更の展開

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、[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。

Firepower Threat Defense アップグレード時の動作：その他のデバイス

スタンドアロンデバイスでのソフトウェアのアップグレード

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。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 *15：*トラフィックの挙動：スタンドアロンデバイスでのソフトウェアのアップグレード

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]（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。

高可用性および拡張性に関するソフトウェアのアップグレード

高可用性デバイスやデバイスのアップグレード中に、トラフィックフローや検査が中断されることはありません。

- FMC を使用した Firepower Threat Defense：高可用性ペアの場合、スタンバイ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。
- FDM を使用した Firepower Threat Defense：高可用性ペアの場合、スタンバイをアップグレードし、ロールを手動で切り替えてから、新しいスタンバイをアップグレードします。

ソフトウェアのアンインストール（パッチ）

バージョン 6.2.3 以降では、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に戻り、設定は変更されません。

- FMC を使用した FTD：スタンドアロンデバイスの場合、パッチのアンインストール中のトラフィックフローと検査の中断は、アップグレードの場合と同じになります。高可用性および拡張性の展開では、中断を最小限に抑えるために、アンインストールの順序を明確

に計画する必要があります。これは、ユニットとしてアップグレードしたデバイスであっても、デバイスから個別にパッチをアンインストールするためです。

- FDM を使用した FTD：サポートされていません。

設定変更の導入

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*：トラフィックの動作：構成変更の展開

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 *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**）	切断
モニターのみ（**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 *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 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
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 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 *19 : 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
パッシブ	中断なし、インスペクションなし

時間とディスク容量のテスト

参考のために、FTD および FMC ソフトウェアの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

特定のプラットフォームおよびシリーズでテストされたすべてのソフトウェアアップグレードの中で最長のテスト時間を報告します。次の表で説明するように、アップグレードには、複数の理由により、指定された時間よりも時間がかかる可能性があります。将来のベンチマークとして使用できるように、独自のアップグレード時間を追跡および記録することをお勧めします。

⚠

注意 システムが非アクティブに見えても、手動で再起動、シャットダウン、または進行中のアップグレードの再開をしないでください。システムが使用できない状態になり、再イメージ化が必要になる場合があります。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。

表 *20 :* ソフトウェアアップグレードの時間テストの条件

条件	詳細
配置	FTDのアップグレードの時間は、FMC展開でのテストでのものです。同様の条件の場合、リモートとローカルの管理対象デバイスのrawアップグレード時間は類似しています。
バージョン	メジャーリリースおよびメンテナンスリリースでは、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。アップグレードでバージョンがスキップされると、通常、アップグレード時間は長くなります。
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。
仮想アプライアンス	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。ただし、仮想展開でのアップグレード時間はハードウェアに大きく依存することに注意してください。
高可用性/拡張性	特に断りのない限り、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。
設定	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。

条件	詳細
コンポーネント	ソフトウェアアップグレード自体とその後の再起動のみの時間を報告します。これには、オペレーティングシステムのアップグレード、アップグレードパッケージの転送、準備状況チェック、VDB および侵入ルール （SRU/LSP）の更新、または設定の展開のための時間は含まれません。

ディスク容量テスト

特定のプラットフォーム/シリーズでテストされたすべてのソフトウェアアップグレードの中で最も多く使用されているディスク容量を報告します。これには、アップグレードパッケージをデバイスにコピーするために必要な容量が含まれます。

また、デバイス アップグレード パッケージ用に FMC（/var 内）に必要な容量も報告します。FTD デバイスがアップグレードパッケージを取得する内部サーバーがある場合、または FDM を使用している場合は、それらの値を無視してください。

特定の場所（/var や /ngfw など）のディスク容量の見積もりを報告する場合、その場所にマウントされているパーティションのディスク容量の見積もりを報告しています。一部のプラットフォームでは、これらの場所が同じパーティション上にある場合があります。

表 *21* : ディスク容量の確認

プラットフォーム	コマンド
FMC	**[System]** > **[Monitoring]** > **[Statistics]**を選択し、FMC を選択します。[Disk Usage] で、[By Partition] の詳細を展開します。
FMC を使用した FTD	**[System]** > **[Monitoring]** > **[Statistics]**を選択し、確認するデバイスを選択します。[Disk Usage] で、[By Partition] の詳細を展開します。
FDM を使用した FTD	**show disk** CLI コマンドを使用します。

バージョン 6.6.5.2 の時間とディスク容量

表 *22* : バージョン *6.6.5.2* 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	アップグレード時間	リブート時間
FMC	2.8 GB /var 内	20 MB / 内	—	39 分	8 分
FMCv：VMware	3.4GB /var 内	23 MB / 内	—	26 分	8 分
Firepower 1000 シリーズ	—	3.0 GB /ngfw 内	630 MB	8 分	12 分
Firepower 2100 シリーズ	—	2.9 GB /ngfw 内	660 MB	7 分	12 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	アップグレード時間	リブート時間
Firepower 9300	—	2.4 GB /ngfw 内	430 MB	5 分	8 分
Firepower 4100 シリーズ	—	2.9 GB /ngfw 内	430 MB	6 分	8 分
Firepower 4100 シリーズ コンテナ インスタンス	—	2.5 GB /ngfw 内	430 MB	5 分	6 分
FTD を搭載した ASA 5500-X シリーズ	2.2 GB /home 内	120 MB /ngfw 内	380 MB	10 分	15 分
FTDv：VMware	1.8 GB /home 内	120 MB /ngfw 内	380 MB	5 分	6 分
ASA FirePOWER	2.9 GB /var 内	21 MB / 内	450 MB	68 分	22 分
NGIPSv	920 MB /var 内	19 MB / 内	310 MB	6 分	5 分

バージョン 6.6.5.1 の時間とディスク容量

表 *23 :* バージョン *6.6.5.1* 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	アップグレード時間	リブート時間
FMC	2.2 GB /var 内	20 MB / 内	—	34 分	8 分
FMCv：VMware	2.2 GB /var 内	23 MB / 内	—	28 分	6 分
Firepower 1000 シリーズ	—	1.5 GB /ngfw 内	340 MB	8 分	12 分
Firepower 2100 シリーズ	—	1.4 GB /ngfw 内	370 MB	6 分	11 分
Firepower 9300	—	770 MB /ngfw 内	140 MB	5 分	8 分
Firepower 4100 シリーズ	—	790 MB /ngfw 内	140 MB	5 分	8 分
Firepower 4100 シリーズ コンテナ インスタンス	—	730 MB /ngfw 内	140 MB	6 分	5 分
FTD を搭載した ASA 5500-X シリーズ	590 MB /home 内	120 MB /ngfw 内	85 MB	9 分	9 分
FTDv：VMware	590 MB /home 内	120 MB /ngfw 内	85 MB	6 分	5 分
ASA FirePOWER	1.7 GB /var 内	21 MB / 内	130 MB	69 分	7 分
NGIPSv	78 MB /var 内	19 MB / 内	16 MB	6 分	5 分

バージョン 6.6.0.1 の時間とディスク容量

この表で、アップグレード時間には再起動が含まれます。

表 *24 :* バージョン *6.6.0.1* の時間とディスク容量

プラットフォーム	/var の容量	必要容量	FMC の容量	アップグレード時間
FMC	31 MB	20 MB	—	22 分
FMCv：VMware	1.1 GB	23 MB	—	17 分
Firepower 1000 シリーズ	450 MB	450 MB	240 MB	21 分
Firepower 2100 シリーズ	260 MB	260 MB	270 MB	17 分
Firepower 9300	460 MB	460 MB	46 MB	33 分
Firepower 4100 シリーズ	470 MB	470 MB	46 MB	11 分
FTD を搭載した ASA 5500-X シリーズ	440 MB	120 MB	46 MB	17 分
FTD を使用した ISA 3000	440 MB	120 MB	46 MB	21 分
FTDv：VMware	430 MB	120 MB	46 MB	11 分
ASA FirePOWER	80 MB	20 MB	15 MB	18 分
NGIPSv	64 MB	28 MB	15 MB	9 分

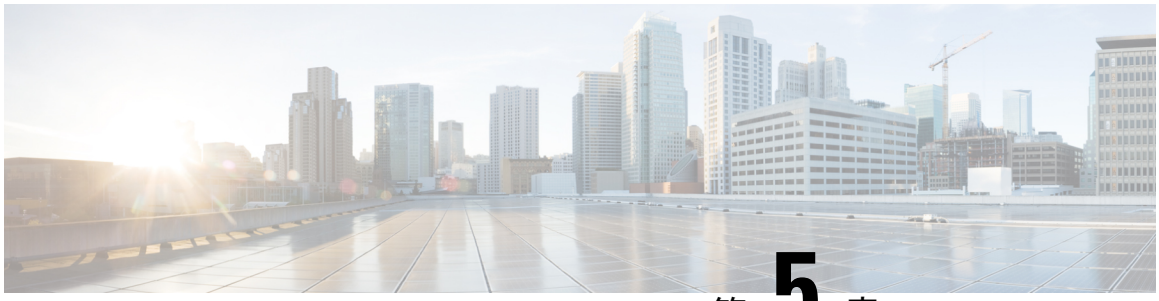
アップグレード手順

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 *25 : Firepower* アップグレード手順

タスク	ガイド
Firepower Management Center の展開でアップグレードします。	Cisco Firepower Management Center Upgrade Guide, Version 6.0–7.0

タスク	ガイド
Firepower Device Manager を搭載した Firepower Threat Defense をアップグレードします。	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 Firepower Threat Defense バージョンのガイドの「*System Management*」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, Firepower 6.0.1–7.0.x or ASA 9.4(1)–9.16(x) with FXOS 1.1.1–2.10.1
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
ISA 3000、ASA 5508-X、ASA 5516-X で ROMMON イメージをアップグレードします。	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。



第 5 章

パッチのアンインストール

Firepower Management Center および ASDM の展開では、ほとんどのパッチをアンインストールすることができます。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に戻り、設定は変更されません。

アンインストールは、Firepower Device Manager ではサポートされていません。ホットフィックスをアンインストールしようとしないでください。代わりに、Cisco TAC にお問い合わせください。

アンインストールに対応するパッチ

特定のパッチをアンインストールすると、アンインストールが成功した場合でも、問題が発生する可能性があります。次のような問題があります。

- 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 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 セキュリティ認定の遵守が有効な場合に FSIC が失敗すると、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るため、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。

アンインストールに対応したバージョン 6.6.0/6.6.x のパッチ

現在、すべての 6.6.0/6.6.x のパッチでアンインストールがサポートされています。

アンインストールパッチのガイドライン

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

Firepower Management Center では、その管理対象デバイスと同じまたはより新しいバージョンを実行する必要があります。これは FMC 展開で、最初に管理対象デバイスからパッチをアンインストールすることを意味します。

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。

- 高可用性および拡張性展開のデバイス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 （37 ページ）」を参照してください。
- FMC または ASDM 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。
- FMC のユーザー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。デバイスでは、独自のユーザーアカウントが維持されます。
- デバイスの `admin` ユーザーとして、または CLI 設定アクセス権を持つ別のローカル ユーザーとして、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。

デバイスの後に 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、高可用性 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。詳しくは、「HA/スケーラビリティ環境でのアンインストール順序 （37 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` ユーザーまたはシェル アクセス権を持つ外部ユーザーのどちらかとして 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。

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/データユニットをアンインストールしてから、次にプライマリ/アクティブコントロール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 *26 : HA* 内の *FMC* の場合におけるアンインストール順序

展開	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、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 *27 : 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

展開	アンインストール順序
デバイスの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。

展開	アンインストール順序
デバイス 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、制御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.** データ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.** データモジュールの 1 つを新しい制御モジュールに設定します。 **3.** 以前のコントロールからアンインストールします。

表 *28 : 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 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 展開	アンインストール順序
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、制御ユニットを最後に残します。 **1.** データ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.** 各データユニットに対して手順を繰り返します。 **5.** 制御ユニットでクラスタリングを無効にします。新しい制御ユニットが引き継ぐまで待ちます。 **6.** 以前の制御ユニットの ASA FirePOWER モジュールからアンインストールします。 **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

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 モニター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 （39 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（37ページ）」を参照してください。

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：混合したバージョンのクラスタまたは 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 モニター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 ユーザー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 シリーズ	`connect ftd`
Firepower 2100 シリーズ	`connect ftd`
Firepower 4100/9300	`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/uninstaller_name
```

Firepowerアプライアンスにパッチを適用すると、そのパッチを簡単に識別できる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。「パッケージのアンインストール（45ページ）」を参照してください。

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、ユーザー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ー 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ーします。

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 または 拡張性の展開では、混合したバージョンのクラスタ、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 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 （37 ページ）」を参照してください。

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：**[モニターリング（Monitoring）] > [ASA FirePOWER のモニターリング（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：**[モニターリング（Monitoring）] > [ASA FirePOWER のモニターリング（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 ユーザー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ることにご注意ください。

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、ユーザー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ー 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ーします。

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

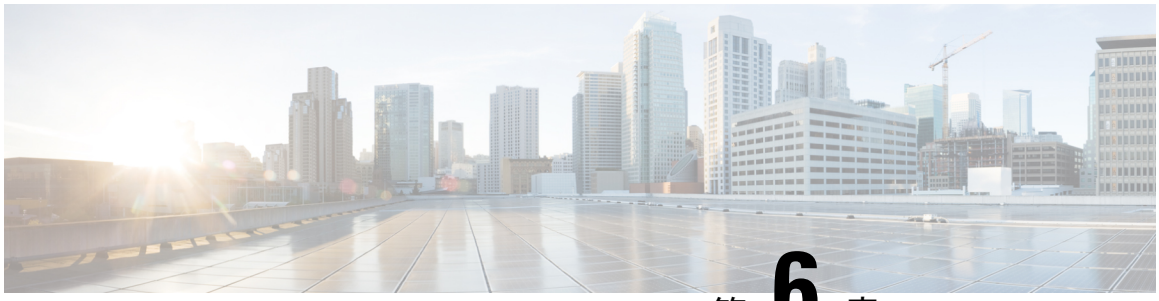
ASA フェールオーバー/クラスタ環境の場合は、各デバイスについて計画した順序でこの手順を繰り返します。

パッケージのアンインストール

パッチのアンインストーラーは、アップグレードパッケージと同様に名前が付けられていますが、ファイル名には「Patch」ではなく「Patch_Uninstaller」が含まれます。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`（Firepower Threat Defense デバイスの場合）
- `/var/sf/updates`（Firepower Management Center および NGIPS デバイス（ASA FirePOWER、NGIPSv）の場合）

アンインストーラー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。



第 6 章

ソフトウェアのインストール

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。

インストールにおけるチェックリストおよびガイドライン

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、このチェック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『取り付け手順 （51 ページ）』を参照してください。

表 *29 :*

✓	アクション/チェック
	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、ユーザー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。
	バックアップを実行します。 サポートされている場合、再イメージ化の前にバックアップします。 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** 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。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、使用する展開の設定ガイドを参照してください。

✓	アクション/チェック
	FMC 管理からデバイスを削除する必要があるか判断します。 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。 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。 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。孤立した権限付与の発生を防ぐために、Cisco Smart Software Manager（CSSM）から登録解除することが必要になる場合があります。これで、再登録を防ぐことができます。または、新しいライセンスについてセールス部門に連絡する必要がある場合があります。 詳細については、以下を参照してください。 • ご使用の製品の設定ガイド。 • スマート ライセンスの登録解除 （49 ページ） • Cisco Firepower System Feature Licenses Guide • Frequently Asked Questions (FAQ) about Firepower Licensing

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。

スマート ライセンスの登録解除

Firepower Threat Defense は 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）で登録します。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。

取り付け手順

表 *30 : Firepower Management Center* 取り付け手順

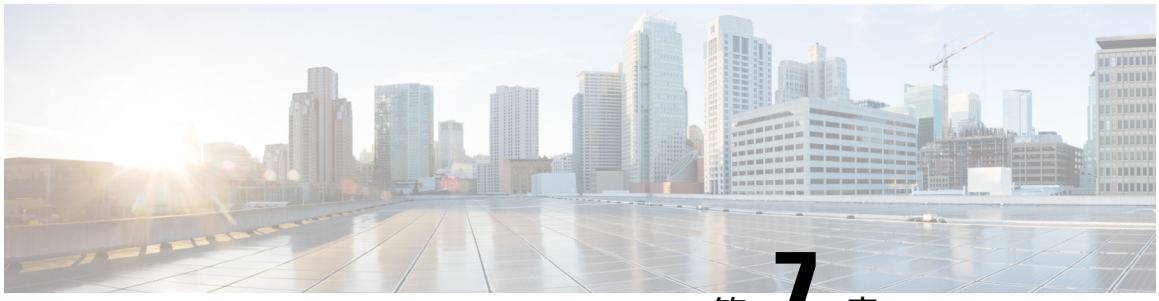
FMC	ガイド
FMC 1600、2600、4600	Cisco Firepower Management Center 1600, 2600, and 4600 Getting Started Guide
FMC 1000、2500、4500	Cisco Firepower Management Center 1000, 2500, and 4500 Getting Started Guide
FMC 2000、4000	Cisco Firepower Management Center 750, 1500, 2000, 3500 and 4000 Getting Started Guide
FMCv	Cisco Firepower Management Center Virtual Getting Started Guide

表 *31 : Firepower Threat Defense* 取り付け手順

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 Troubleshooting Guide for the Firepower 1000/2100 Series Running Firepower Threat Defense
Firepower 4100/9300	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：AWS	Cisco Firepower Threat Defense Virtual for the AWS Cloud Getting Started Guide
FTDv：Azure	Cisco Firepower Threat Defense Virtual for the Microsoft Azure Cloud Quick Start Guide
FTDv：KVM	Cisco Firepower Threat Defense Virtual for KVM Getting Started Guide
FTDv：VMware	Cisco Firepower Threat Defense Virtual for VMware Getting Started Guide

表 *32 : 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

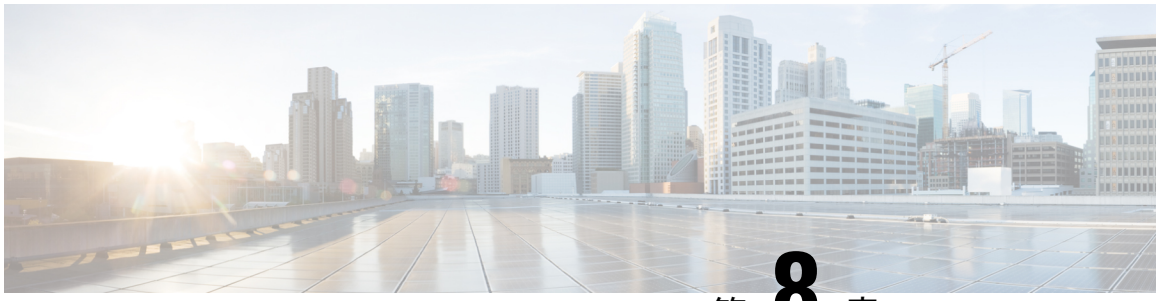
パッチで必要な場合は、Firepower のマニュアルを更新します。

- ドキュメント ロードマップ （53 ページ）

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、リリースノートには、各パッチの解決済みの問題が記載されています。

サポート契約がある場合は、Cisco Bug Search Tool を使用して最新のバグリストを取得できます。検索では、特定の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。バグのステータス、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。

重要 バグリストは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。

バージョン 6.6.5.2 で解決済みの問題

表 *33* : バージョン *6.6.5.2* で解決済みの問題

不具合 ID	タイトル
CSCvz66795	コマンド「show access-list」実行時の SSH プロセスでの ASA のトレースバックとリロード
CSCvy60831	ASA および FTD メモリブロックの位置がデータパスでの断片化されたパケットに対して更新されない
CSCwa46963	セキュリティ：CVE-2021-44228 -> Log4j 2 の脆弱性
CSCwa08262	マッピングされたグループポリシーを持つ AnyConnect ユーザーは、トンネルグループの下にあるデフォルト GP から属性を取得します

不具合 ID	タイトル
CSCvz89327	OSPFv2 フローにクラスター集中型「c」フラグがない
CSCwa02929	FTD が SSL フローエラーの CORRUPT_MESSAGE でトラフィックをブロックする
CSCvz89545	アップグレード後の SSL VPN のパフォーマンスの低下と重大な安定性に関する問題
CSCvz53993	SSL フローでの Snort によるランダムなパケットのブロック
CSCwa28895	FTD SSL プロキシは、設定可能または動的な最大 TCP ウィンドウサイズを許可する必要があります
CSCvz02076	Snort のリロードがタイムアウトして再起動する
CSCwa67882	オフロードされた GRE トンネルは、気づかない内にオフロードを解除し、CPU にパントされる場合があります。
CSCwa20516	FMC ポリシーの展開に 14 分以上かかる
CSCvx76665	2100 および 1010 で表示される「インターフェイスのアップデートに失敗しました」というエラーメッセージ
CSCwa88571	スマートポータルを使用して FMC を登録できない
CSCvz33468	FQDN_NAT で object-group/ nat のヒットカウントの変更が更新されないと、NAT が動作しなくなる。
CSCvx78968	スレッド名での ASA および FTD のトレースバックとリロード：VTI が設定された IKEv2 デーモン
CSCwa19443	フローオフロード - 比較状態の値が長期間エラー状態のままになる
CSCvz76746	管理トンネルを実装している間、ユーザーはオープン接続を使用して AnyConnect をバイパスできます。
CSCwa14725	IKE デーモンスレッドでの ASA および FTD のトレースバックとリロード
CSCvz32386	FMC が同じクリプトマップエントリに PFS21 および IKEv1 設定をプッシュする際に FTD 展開エラーが発生する
CSCvz55849	LINA プロセスでの FTD のトレースバックとリロード
CSCvz85437	FXOS および FTD を 2.10.1.159 および 6.6.4 にアップグレードした後に FTD 100G のインターフェイスがダウンする
CSCwa70008	期限切れの証明書により、セキュリティインテリジェンスの更新が失敗する

不具合 ID	タイトル
CSCvz92932	ASA show tech の実行により CPU のスパイクが発生し、IKEv2 セッションに影響を与える
CSCvz95108	デバイスでのメジャーバージョンの変更によるアップグレード後の FTD 展開の失敗
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
CSCwa55878	FTD サービスモジュールの障害：「ND がダウンした可能性があります」という誤ったアラーム
CSCvz40352	アクセスリストに明確なルールが存在するにもかかわらず、暗黙の ACL によって ASA トラフィックがドロップする
CSCwa03275	BGP ルートが未解決と表示され、「ホストへのルートがありません」という ASP のドロップが原因となりパケットをドロップする
CSCvz94153	IPV4 アドレスが設定されていない場合、IPV6 での NTP 同期が失敗する
CSCvy89440	s2sCryptoMap 設定の損失
CSCwa58686	OGS コンパイル動作における ASA および FTD の変更によりブートループが発生する
CSCwa11052	バージョン 9.14(2)15 へのアップグレード後に SNMP が応答しなくなる
CSCvz02398	7.0 での SE リングタイムアウトで生成された暗号アーカイブ
CSCvz03524	sha1 ではなく sha256 リクエストが原因で PKI の「OCSP 失効チェック」が失敗する
CSCwa03347	IPv6 PIM パケットが、無効な IP の長さによるドロップが原因となり ASP でドロップする

バージョン 6.6.5.1 で解決済みの問題

表 *34* : バージョン *6.6.5.1* で解決済みの問題

不具合 ID	タイトル
CSCvg66052	Firepower アプライアンスで 2 つの CPU コアが継続的にスパイクする
CSCvq43454	ENH：SAML 認証を使用しているときに、「NotValidBefore」タイムスタンプの許容時間をサポートする

不具合 ID	タイトル
CSCvs27336	Smart Call Home プロセスによる ASA のトレースバック
CSCvs61701	Firepower 2100 のメモリリークが原因で DME のプロセスがクラッシュする
CSCvv43190	GRE ヘッダープロトコルフィールドが内部 IP ヘッダーのプロトコルフィールドと一致しない場合の暗号エンジンエラー
CSCvv48942	Snmpwalk がフェールオーバーインターフェイスのトラフィックカウンターを 0 として表示する
CSCvw71405	暗号化プロセスで FPR1120 が ASA トレースバックとリロードを実行している
CSCvx16134	マルチコアを使用しているにもかかわらず、「show processes cpu-usage」で見られる一部のプロセスで CPU の使用率が 100% になる
CSCvx50980	ASA CP の誤った計算により、パーセンテージが高くなる（CP CPU 100%）
CSCvx65178	ファイアウォール MIB 内の特定の OID に対して SNMP 一括取得が機能せず、デバイスのパフォーマンスが低下する
CSCvx80830	Radius サーバーが dACL を送信し、vpn-simultaneous-logins が 1 に設定されていると、同じユーザーからの VPN 接続が失敗する
CSCvx90486	ifXTable の snmpwalk がデータインターフェイスを返さないことがある
CSCvx95884	HA バルク同期中および通常の conn 同期中に CPU 使用率が高くなり、大量の「バッファなし」がドロップする
CSCvy02247	Cisco Firepower システム ソフトウェア ルール エディタの影響のないバッファオーバーフローの脆弱性
CSCvy04343	PLR モードの ASA で「ライセンスのスマート予約」が失敗する。
CSCvy09436	DHCP 予約で一部のデバイスに予約済みアドレスを適用できない
CSCvy10583	スレッド名 DATAPATH での ASA トレースバックおよびリロード
CSCvy12782	FTD/ASA：HA の ixgbe-vf SRIOV インターフェイスで設定すると、PAT されたトラフィックが影響を受ける
CSCvy16179	CSCuz67596 の修正を実行中でも、スレッド名 Unicorn Admin Handler で ASA クラスタがトレースバックする
CSCvy17078	トレースバック：LINA プロセスで FPR 2110 の ASA がトレースバックおよびリロードする

不具合 ID	タイトル
CSCvy21334	「スイッチオーバーなし」の場合、アクティブは CoA アップデートをスタンバイに送信しようとする
CSCvy27283	プライバシーアルゴリズムの AES192 または AES256 を使用した場合、ASA または FTD の SNMPv3 ポーリングが失敗することがある
CSCvy31229	/ngfwに空き領域がない
CSCvy33105	DNS ルックアップが有効な場合、「show route bgp」または「show route isis」であいまいなコマンドエラーが表示される
CSCvy33676	以前の動的 xlate が作成されると、FTD で UN-NAT が作成される
CSCvy35737	Anyconnect パッケージの検証中に FTD のトレースバックとリロードが発生する
CSCvy39621	ASA/FTDは、最大再試行回数に達した後も連続的な RADIUS アクセス要求を送信する
CSCvy43447	マルチインスタンス FTD の Lic TMR スレッドでの FTDトレースバックとリロード
CSCvy47108	UAuth エントリがスタックしているため、リモートアクセス IKEv2 VPN セッションを確立できない
CSCvy48159	メモリヘッダー検証によるプロセス名 lina での ASA トレースバックとリロード
CSCvy49732	ASA/FTD がスレッド名「ssh」でトレースバックし、リロードすることがある
CSCvy50011	IKE デーモンプロセスでの ASA トレースバックおよびリロード
CSCvy51659	OCSP タイムアウトが長い場合、AnyConnect 認証が失敗することがある
CSCvy51814	Firepower フローオフロードが、すべての既存のフローおよび新しいフローのオフロードを停止させる
CSCvy52074	ASA/FTD がスレッド名「webvpn_task」でトレースバックおよびリロードすることがある
CSCvy52924	FTD がリブート時にすべての VRF インスタンスの OSPF ネットワークステートメント設定を失う
CSCvy53461	RSA キーと証明書が ASA コード 9.12.x を使用した WS-SVC-ASA-SM1-K7 でリロード後に削除される
CSCvy55356	ドキュメントに反して、10 ミリ秒未満の CPU 占有が発生する

不具合 ID	タイトル
CSCvy56395	キー設定が存在する場合の SNMP 暗号化コミュニティストリングによる ASA トレースバックとリロード
CSCvy57905	VTI トンネルインターフェイスが、HA の KP および WM プラットフォームでリロード後もダウンしたままになる
CSCvy58268	ブロック 80 および 256 の枯渇スナップショットが作成されない
CSCvy60100	HA の再起動後に SNMP v3 設定が失われる
CSCvy64492	ASAv が MAC テーブルの自身のアドレスに非アイデンティティ L2 エントリを追加し、HA hello をドロップする
CSCvy64911	デバッグ：crasLocalAddress の SNMP MIB 値に IP アドレスが表示されない
CSCvy69189	vpnfol_sync/Bulk-sync keytab がスタックしているため、FTD HA がバルク状態のままになる
CSCvy72194	Cisco FMC ソフトウェアにおける設定情報開示の脆弱性
CSCvy72846	ASA アカウンティングが誤った Acct-Session-Time を報告する
CSCvy74781	スタンバイデバイスが、フェールオーバー後に SSL トラフィックのキープアライブメッセージを送信する
CSCvy74984	デフォルトの外部ルートが使用されると、Azure 上の ASAv がメタデータサーバーへの接続を失う
CSCvy82794	snmp コマンドを無効にする場合の ASA/FTD トレースバックとリロード
CSCvy90836	スレッド名 SNMP ContextThread での ASA トレースバックおよびリロード
CSCvy91668	スティッキネストラフィックによる PAT プールの枯渇は、新しい接続のドロップにつながる可能性がある
CSCvy92990	7.0 へのアップグレード後の SSL に関連する FTD トレースバックとリロード
CSCvy96625	CSCvr33428 および CSCvy39659 で導入された「修正」を元に戻す
CSCvy96803	SNMP 機能に関連するプロセス名 lina の FTD トレースバックとリロード
CSCvy98458	FP21xx のトレースバック「Panic:DATAPATH-10-xxxx -remove_mem_from_head: Error - found a bad header」
CSCvz00383	スレッド名 Checkheaps で FTD lina トレースバックとリロードが発生する
CSCvz00699	ASA のアップグレード後、webvpn でトレースバックとリロードが定期的に発生する

不具合 ID	タイトル
CSCvz05189	クラスタでの xlate の複製中に Lina トレースバックによる FTD のリロードが発生する
CSCvz07614	ASA：孤立した SSH セッションでは、CLI からポリシーマップを削除できない
CSCvz15529	スレッド名 Datapath での ASA のトレースバックおよびリロード
CSCvz20544	Anyconnect プロファイルのループ処理で、ASA および FTD がトレースバックおよびリロードする場合がある
CSCvz20679	FTDv - Lina のトレースバックおよびリロード
CSCvz21886	nat が IP ではなくポート番号に一致する pbr ACL に一致した場合、nat の un-nat が 2 回発生しない
CSCvz23157	show コマンドが発行されると SNMP エージェントが再起動する
CSCvz25434	BVI が DHCP クライアントとして設定されている場合、1550 ブロックの枯渇が原因で ASA および FTD がトラフィックをブラックホールする
CSCvz27235	複数のシスコ製品の Snort Modbus におけるサービス妨害の脆弱性
CSCvz29233	ASA：システムコンテキストでインターフェイスのフラップが発生したときに、カスタムコンテキストからの ARP エントリが削除されない
CSCvz30333	「show capture」コマンドが実行されると、FTD または Lina がトレースバックすることがある
CSCvz30933	clear configure snmp-server コマンドが発行されると ASA のトレースバックとリロードが発生する
CSCvz34831	ASA が DACL のダウンロードに失敗した場合、試行を停止しない
CSCvz37306	既存のユーザーで複数のコンテキストスイッチを実行した後、ASDM セッションが新しいユーザーに提供されない
CSCvz38332	FTD または ASA - 9.14.2.15 から 9.14.3 へのアップグレード後にブートループでスタックする
CSCvz38361	直接接続されていないネイバーのために BGP パケットがドロップされる
CSCvz38692	snmp_master_callback_thread での ASAv のトレースバックとリロード
CSCvz39565	バルク VPN セッション接続中の ASA または FTD のトレースバックとリロード
CSCvz39646	ASA および AnyConnect - 古い RADIUS セッション

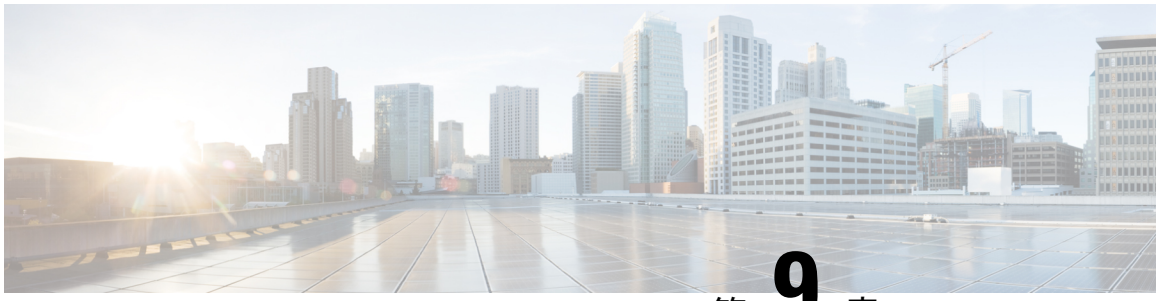
不具合 ID	タイトル
CSCvz43414	HA のフェールオーバー後に内部 LDAP 属性マッピングが失敗する
CSCvz43455	hostscan のアップグレード中に ASAv がトレースバックを確認する
CSCvz48407	スレッド名 DATAPATH-15-18621 でのトレースバックおよびリロード
CSCvz53142	ASA が、name-server コマンドで指定されたインターフェイスを使用して IPv6 DNS サーバーに到達しない
CSCvz57710	conf t が、context-config モードで disk0:/t に変換される
CSCvz58710	SCTP トラフィックにより ASA がトレースバックする。
CSCvz60970	LU を スターリンクに送信する際、enic_put / FREEB 内のスレッド名 DATAPATH-4-23199 で ASA がトレースバックする
CSCvz61160	ICMP エラーメッセージを処理する際、DATAPATH で ASA がトレースバックする
CSCvz64470	ICMP 到達不能メッセージ生成時のメモリ破損による ASA および FTD のトレースバックとリロード
CSCvz69571	anyconnect セッションが終了した後、ASA ログに転送されたデータの間違った値が表示される
CSCvz73146	FTD：スレッド名 DATAPATH でのトレースバック
CSCvz73709	ASA および FTD のスタンバイユニットが HA に参加できない
CSCvz75988	RFC5424 が有効な場合、一貫性のないロギングタイムスタンプが起こる
CSCvz77744	OSPFv3：FTD の間違った「転送アドレス」が ospfv3 データベースに追加される
CSCvz84850	「タイマーサービス」機能により、ASA および FTD のトレースバックとリロードが行われる

バージョン 6.6.0.1 で解決済みの問題

表 *35 :* バージョン *6.6.0.1* で解決済みの問題

不具合 ID	タイトル
CSCvt03598	Cisco ASA ソフトウェアおよび FTD ソフトウェア Web サービスの読み取り専用パストラバーサルの脆弱性

不具合 ID	タイトル
CSCvu65843	FP2100：6.6.0 での自動ネゴシエーションの変更によるファイバ SFP インターフェイスのダウン



第 9 章

既知の問題

便宜上、リリースノートには、メジャーリリースの既知の問題が記載されています。メンテナンスリリースまたはパッチの既知の問題は記載されていません。

サポート契約がある場合は、Cisco Bug Search Tool を使用して最新のバグリストを取得できます。検索では、特定の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。バグの状態、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。

重要 バグリストは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。

• バージョン 6.6.0 の既知の問題 （65 ページ）

バージョン 6.6.0 の既知の問題

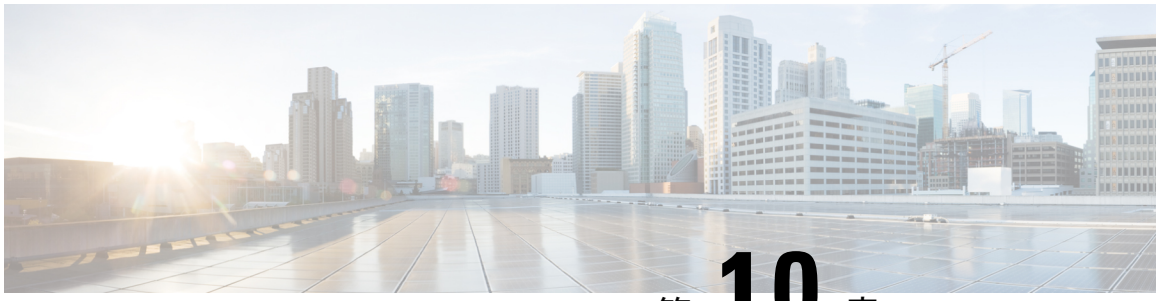
表 *36* : バージョン *6.6.0* の既知の問題

不具合 ID	タイトル
CSCvr90564	ユーザー VRF のエリア間 OSPF 設定を無効にすると、展開が失敗する
CSCvt14898	RAVPN を使用したアップグレード後に展開に失敗する（no split-tunnel-network-list value RA-VPN-policy|splitAcl）
CSCvt29546	同じボックスにバックアップを復元した後に、ライセンスの登録が解除される
CSCvt37753	MI クラスタでポリシーの展開が失敗する
CSCvt39442	管理者ユーザーが原因でダッシュボードウィジェットが表示されない
CSCvt43431	CLI の管理インターフェイス設定の変更後、UI では CLI の変更が更新されていなかったOOB の同期の問題

不具合 ID	タイトル
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
CSCvt66906	セッションでアプリケーションが検出された場合でも、Appidはダイナミックキャッシュを検索する
CSCvt68316	インポートの失敗後に展開が絶えず失敗し、変更を破棄できない
CSCvt68819	アップグレード前に存在していたイベントをコピーすると、クリップボードへのコピーが失敗することがある
CSCvt69260	接続イベントに古いデバイス名が表示される
CSCvt70854	6.6.0-90： [Firepower 1010] メモリ不足のため、SRU の更新中に tomcat が再起動する
CSCvt77143	Apache Commons FileUpload の HTTP リクエストヘッダーの値の処理の拒否
CSCvt77210	1.2.2 よりも前の minimist では正しく追加または変更されているように見える場合がある
CSCvt78634	アサーションドメイン ID を使用したポリシー展開時に FTD lina がトレースバックする
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
CSCvt86467	c3p0 0.9.5.2 では、com/mcha の extractXmlConfigFromInputStream で XXE が許可される
CSCvt87117	libexpat 不適切な解析によるサービス拒否の脆弱性
CSCvt87123	Expat libexpat XML パーサーに関するサービス拒否の脆弱性
CSCvt89042	dom4j XML インジェクションの脆弱性
CSCvt89045	Redis redis-cli バッファオーバーフローの脆弱性
CSCvt89378	ログイン時に「データベースに重大なエラーが発生しました。再起動する必要があります（The database has encountered a critical error, and needs to be restarted.）」という UI エラーが表示される
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 サーバーにも到達しない
CSCvt97205	ASA 9.14.1 上で SNMPPOLL/SNMPTRAP からリモートエンド（サイト間 VPN）ASA インターフェイスが失敗する

不具合 ID	タイトル
CSCvt99082	Rest API：拡張アクセスリストの URL が extendedaccesslist から extendedaccesslist に変更された
CSCvu06882	KVM ASAv からの virtio インターフェイスのホットプラグ削除によりクラッシュが発生する
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 のアップグレードが 800_post/100_ftd_onbox_data_import.sh で失敗する
CSCvu16826	リリース6.6へのアップグレード後に snort ルールが破損しているため、FTD snort インスタンスがダウンする
CSCvu18510	MonetDB のイベントデータベースのクラッシュにより、FMC 6.6.0 の接続イベントが失われる
CSCvu20690	2.1.3 より前の dom4j で、外部 DTD および外部エンティティがデフォルトで許可される
CSCvu29145	Snort フロー IP プロファイリングでは、「system support flow-ip-profiling start」コマンドを使用して有効にできない
CSCvu30441	FMC 6.6 REST API GUI では、新しいアクセスルールを PUT または POST しようとする際に応答がない
CSCvu30748	PTHREAD-1859 でバージョン 9.14.1 にアップグレードした後の ASAv のトレースバックおよびリロード
CSCvu35426	リーフドメインのスケジュール展開では、1 つのデバイスのみがポリシーを展開する
CSCvu35768	FMC を 6409-59 から 6.6.0-90 にアップグレードした後、サブドメイン内の Radius 外部ユーザーを使用して UI をログに記録できない
CSCvu38869	jQuery フレームワークが JavaScript Object Notation（使用できないソリューション）を使用してデータを交換する
CSCvu50400	Firepower 6.2.3.x から 6.6.0 にアップグレードした後、ASDM を使用する ASA FirePOWER の CPU 使用率が高くなる
CSCvu62018	SSL 復号を使用して最大検出 IPS を使用すると、ルール 129:12 によりトラフィックがブロックされる：Snort2
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
CSCvu70622	リロード後に CTS SGT 伝播が有効になる

不具合 ID	タイトル
CSCvu74702	ポリシーの展開後に検出エンジンが予期せず終了し、コアファイルが生成される
CSCvu75315	6.6.0 へのアップグレード後、レポートに棒グラフと円グラフで侵入イベントが表示されない
CSCvu79125	高度なマルウェアリスクレポートの生成に失敗する
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
CSCvu84127	Firepower 2100：明確な理由なしに FTD がリブートする
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
CSCvu96559	トレースバック：ASA で予期しないトレースバックが発生し、不完全なコアが生成される
CSCvv01558	6.6.0-90 を実行している ASA/ Elektra-HA デバイスで、sfhassd から「認識できないインスタンス（unrecognized instance）」のエラーが発生する
CSCvv04023	FDM（オンボックスマネージャ）：インターフェイスが zones.conf から削除されたため、トラフィックが適切なルールでヒットしない
CSCvw38870	800_post/1027_ldap_external_auth_fix.pl で、6.6.0、6.6.1、6.6.3、6.7.0 への FMC のアップグレードが失敗する



第 10 章

サポートが必要な場合

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次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、Cisco 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。

- マニュアル http://www.cisco.com/go/threatdefense-66-docs
- 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 のユーザー 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