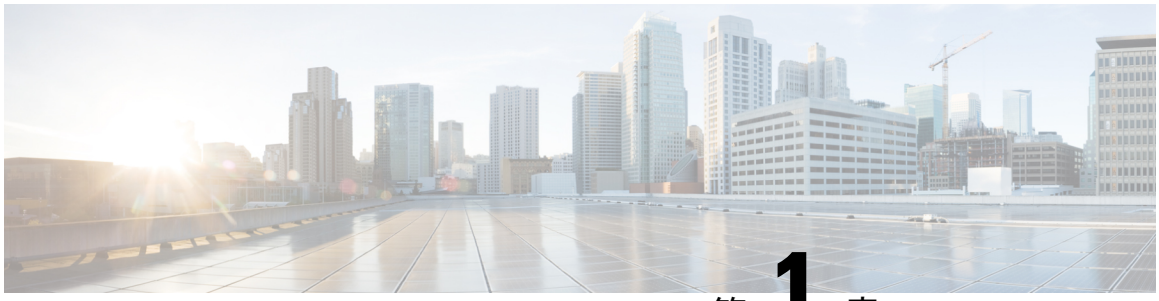
Firepower Management Center 用Cisco Firepower Threat Defense アップグレードガイド（バージョン7.1）

初版：2021 年 12 月 1 日

最終更新：2022 年 6 月 30 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

使用する前に

対象読者

このガイドでは、**バージョン 7.1** を搭載した **Firepower Management Center** を使用して、アップグレードを準備し、確実に実行する方法について説明します。

- 現在管理されている FTD デバイスの バージョン 7.1 までのアップグレード。
- バージョン 7.1 以降のリリースへの FMC のアップグレード。

関連リソース

別のプラットフォームやコンポーネントをアップグレードする場合、別のバージョンから、または別のバージョンにアップグレードする場合、あるいはクラウドベースのマネージャを使用する場合は、以下に示す関連情報を参照してください。

表 *1 : FMC* のアップグレード

現在の FMC のバージョン	ガイド
クラウド提供型の管理センター（バージョンなし）	なし。更新はシスコが行います。
7.2 以降	お使いのバージョンの『Cisco Secure Firewall Threat Defense Upgrade Guide for Management Center』
7.1	『Cisco Firepower Threat Defense Upgrade Guide for Firepower Management Center, Version 7.1』

現在の FMC のバージョン	ガイド
7.0 以前	Cisco Firepower Management Center Upgrade Guide, Version 6.0–7.0

表 *2 : FMC* を使用した *FTD* のアップグレード

現在の FMC のバージョン	ガイド
クラウド提供型の管理センター（バージョンなし）	最新のリリースバージョンの『Cisco Secure Firewall Threat Defense Upgrade Guide for Management Center』
7.2 以降	お使いのバージョンの『Cisco Secure Firewall Threat Defense Upgrade Guide for Management Center』
7.1	『Cisco Firepower Threat Defense Upgrade Guide for Firepower Management Center, Version 7.1』
7.0 以前	Cisco Firepower Management Center Upgrade Guide, Version 6.0–7.0

表 *3 : FDM* を使用した *FTD* のアップグレード

現在の FTD のバージョン	ガイド
7.2 以降	お使いのバージョンの『Cisco Secure Firewall Threat Defense Upgrade Guide for Device Manager』
7.1	『Cisco Firepower Threat Defense Upgrade Guide for Firepower Device Manager, Version 7.1』
7.0 以前	『Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager』内の「System Management」。 Firepower 4100/9300 については、Cisco Firepower 4100/9300 アップグレードガイド、FXOS 1.1.1 ～ 2.10.1 を使用した FTD 6.0.1 ～ 7.0.x または ASA 9.4 (1) ～ 9.16 (x)の FXOS のアップグレード手順も参照してください。
バージョン 6.4 以降、CDO 使用	Cisco Defense Orchestrator での FDM デバイスの管理の「Onboard Devices and Services」。

表 *4 : NGIPS* デバイスのアップグレード

現在のマネージャバージョン	プラットフォーム	ガイド
いずれか	Firepower 7000/8000 シリーズ	Cisco Firepower Management Center Upgrade Guide, Version 6.0–7.0
いずれか	FMC を搭載した ASA FirePOWER	Cisco Firepower Management Center Upgrade Guide, Version 6.0–7.0
いずれか	ASDM を使用した ASA FirePOWER	Cisco Secure Firewall ASA アップグレードガイド

表 *5 :* その他のコンポーネントのアップグレード

Version	コンポーネント	ガイド
いずれか	Firepower 4100/9300 上の ASA 論理デバイス	Cisco Secure Firewall ASA アップグレードガイド。
最新	FMC 用の BIOS およびファームウェア	Cisco Secure Firewall Threat Defense/Firepower ホットフィックス リリース ノート。
最新	Firepower 4100/9300 のファームウェア	Cisco Firepower 4100/9300 FXOS ファームウェア アップグレード ガイド
最新	ISA 3000 の ROMMON イメージ	Cisco Secure Firewall ASA および Secure Firewall Threat Defense 再イメージ化ガイド。

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、アップグレードの章を参照してください。

表 *6:* アップグレードの計画フェーズ

計画フェーズ	次を含む
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。
バックアップ	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。
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 のファームウェア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。
最終チェック	設定を確認します。 NTP 同期を確認します。 設定を展開します。 準備状況チェックを実行します。 ディスク容量を確認します。 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。

機能の履歴

表 *7:* バージョン *7.1.0* の機能

機能	説明
正常なデバイスアップグレードを元に戻します。	メジャーおよびメンテナンスアップグレードを FTD に戻すことができるようになりました。復元すると、ソフトウェアは、最後のアップグレードの直前の状態に戻ります（スナップショットとも呼ばれます）。パッチのインストール後にアップグレードを元に戻すと、パッチだけでなく、メジャーアップグレードやメンテナンスアップグレードも元に戻されます。 **重要** 元に戻す必要がある可能性があると思われる場合は、**システム**（⚙）>**[更新（Updates）]**ページを使用して FTD をアップグレードする必要があります。[システムの更新（System Updates）] ページは、[アップグレード後の復元を有効にする（Enable revert after successful upgrade）] オプションを有効にできる唯一の場所です。このオプションでは、アップグレードの開始時に復元スナップショットを保存するようにシステムが設定されます。これは、[デバイス（Devices）]>[デバイスのアップグレード（Device Upgrade）] ページでウィザードを使用する通常の推奨とは対照的です。 この機能は、コンテナインスタンスではサポートされません。 必要最低限の Threat Defense、顧客展開の Management Center：7.1 必要最低限の Threat Defense、クラウド提供型 Firewall Management Center：7.2

機能	説明
クラスタ化された高可用性デバイスのアップグレードワークフローの改善。	クラスタ化された高可用性デバイスのアップグレードワークフローが次のように改善されました。 • アップグレードウィザードは、個々のデバイスとしてではなく、グループとして、クラスタ化された高可用性ユニットを正しく表示するようになりました。システムは、発生する可能性のあるグループ関連の問題を特定し、報告し、事前に修正を要求できます。たとえば、Firepower Chassis Manager で非同期の変更を行った場合は、Firepower 4100/9300 のクラスタをアップグレードできません。 • アップグレードパッケージをクラスタおよび高可用性ペアにコピーする速度と効率が向上しました。以前は、FMC はパッケージを各グループメンバーに順番にコピーしていました。これで、グループメンバーは通常の同期プロセスの一部として、相互にパッケージを取得できるようになりました。 • クラスタ内のデータユニットのアップグレード順序を指定できるようになりました。コントロールユニットは常に最後にアップグレードされます。

表 *8 :* バージョン *7.0.0* の機能

機能	説明
FTD のアップグレード パフォーマンスとステータスレポートの改善。	FTDのアップグレードがより簡単かつ確実に、より少ないディスク容量で実行できるようになりました。メッセージセンターの新しい [アップグレード（Upgrades）] タブでは、アップグレードステータスとエラーレポートがさらに強化されています。

機能	説明
FTD デバイスのわかりやすいアップグレードワークフロー。	

機能	説明
	FMC の新しいデバイス アップグレード ページ（[デバイス（Devices）]>[デバイスアップグレード（Device Upgrade）]）には、バージョン 6.4 以降の FTD デバイスをアップグレードするためのわかりやすいウィザードがあります。アップグレードするデバイスの選択、アップグレードパッケージのデバイスへのコピー、互換性と準備状況の確認など、アップグレード前の重要な段階を順を追って説明します。 開始するには、[デバイス管理（Device Management）] ページ（[デバイス（Devices）] > [デバイス管理（Device Management）]>[アクションの選択（Select Action）]）で新しい [Firepower ソフトウェアのアップグレード（Upgrade Firepower Software）] アクションを使用します。 続行すると、選択したデバイスに関する基本情報と、現在のアップグレード関連のステータスが表示されます。表示内容には、アップグレードできない理由が含まれます。あるデバイスがウィザードの 1 つの段階に「合格」しない場合、そのデバイスは次の段階には表示されません。 ウィザードから移動しても、進行状況は保持されます。ただし、管理者アクセス権を持つ他のユーザーはウィザードをリセット、変更、または続行できます。 （注） FTD のアップグレードパッケージの場所をアップロードまたは指定するには、引き続き **システム**（⚙）>**[更新（Updates）]**を使用する必要があります。また、[システム更新（System Updates）] ページを使用して、FMC 自体、およびすべての非 FTD 管理対象デバイスをアップグレードする必要があります。 （注） バージョン 7.0 では、ウィザードにクラスタまたは高可用性ペアのデバイスが正しく表示されません。これらのデバイスは 1 つのユニットとして選択してアップグレードする必要がありますが、ウィザードにはスタンドアロンデバイスとして表示されます。デバイスのステータスとアップグレードの準備状況は、個別に評価および報告されます。つまり、1 つのユニットが「合格」して次の段階に進んでいるように見えても、他のユニットは合格していない可能性があります。ただし、それらのデバイスはグループ化されたままです。1 つのユニットで準備状況チェックを実行すると、すべてのユニットで実行されます。1 つユニットでアップグレードを開始すると、すべてのユニッ

機能	説明
	トで開始されます。 時間がかかるアップグレードの失敗を回避するには、[次へ（Next）] をクリックする前に、すべてのグループメンバーがウィザードの次のステップに進む準備ができていることを手動で確認します。
多くの FTD デバイスを一度にアップグレードします。	FTD アップグレードウィザードでは、次の制限が解除されます。 • デバイスの同時アップグレード。 一度にアップグレードできるデバイスの数は、同時アップグレードを管理するシステムの機能ではなく、管理ネットワークの帯域幅によって制限されます。以前は、一度に 5 台を上回るデバイスをアップグレードしないことを推奨していました。 **重要** この改善は、FTD バージョン 6.7 以降へのアップグレードでのみ確認できます。デバイスを古い FTD リリースにアップグレードする場合は、新しいアップグレードウィザードを使用している場合でも、一度に 5 台のデバイスに制限することをお勧めします。 • デバイスモデルによるアップグレードのグループ化。 システムが適切なアップグレードパッケージにアクセスできる限り、すべての FTD モデルのアップグレードを同時にキューに入れて呼び出すことができます。 以前は、アップグレードパッケージを選択し、そのパッケージを使用してアップグレードするデバイスを選択していました。つまり、アップグレードパッケージを共有している場合にのみ、複数のデバイスを同時にアップグレードできました。たとえば、2 台の Firepower 2100 シリーズ デバイスは同時にアップグレードできますが、Firepower 2100 シリーズと Firepower 1000 シリーズはアップグレードできません。

表 *9 :* バージョン *6.7.0* の機能

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

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

機能	説明
	• **show upgrade status detail** • **show upgrade status continuous** • **show upgrade status** • **upgrade cancel** • **upgrade retry**
アップグレードでディスク容量を節約するために PCAP ファイルが削除される。	アップグレードにより、ローカルに保存された PCAP ファイルが削除されるようになりました。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。

表 *10* : バージョン *6.6.0* の機能

機能	説明
内部 Web サーバーからデバイスアップグレードパッケージを取得します。	デバイスは、FMC からではなく、独自の内部 Web サーバーからアップグレードパッケージを取得できるようになりました。これは、FMC とそのデバイスの間の帯域幅が制限されている場合に特に役立ちます。また、FMC 上の容量も節約できます。 新規/変更された画面：[システム（System）] > [更新（Updates）] > [更新のアップロード（Upload Update）] ボタン > [ソフトウェア更新ソースの指定（Specify Software Update Source）] オプション
アップグレードがスケジュールされたタスクを延期する。	FMC のアップグレードプロセスによって、スケジュールされたタスクが延期されるようになりました。アップグレード中に開始するようにスケジュールされたタスクは、アップグレード後の再起動の 5 分後に開始されます。 （注） アップグレードを開始する前に、実行中のタスクが完了していることを確認する必要があります。アップグレードの開始時に実行中のタスクは停止し、失敗したタスクとなり、再開できません。 この機能は、サポートされているバージョンからのすべてのアップグレードでサポートされていることに注意してください。これには、バージョン 6.4.0.10 以降のパッチ、バージョン 6.6.3 以降のメンテナンスリリース、およびバージョン 6.7.0 以降が含まれます。この機能は、サポートされていないバージョンからサポートされているバージョンへのアップグレードではサポートされていません。

表 *11* : バージョン *6.4.0* の機能

機能	説明
アップグレードがスケジュールされたタスクを延期する。	FMCのアップグレードプロセスによって、スケジュールされたタスクが延期されるようになりました。アップグレード中に開始するようにスケジュールされたタスクは、アップグレード後の再起動の 5 分後に開始されます。 （注） アップグレードを開始する前に、実行中のタスクが完了していることを確認する必要があります。アップグレードの開始時に実行中のタスクは停止し、失敗したタスクとなり、再開できません。 この機能は、サポートされているバージョンからのすべてのアップグレードでサポートされていることに注意してください。これには、バージョン 6.4.0.10 以降のパッチ、バージョン 6.6.3 以降のメンテナンスリリース、およびバージョン 6.7.0 以降が含まれます。この機能は、サポートされていないバージョンからサポートされているバージョンへのアップグレードではサポートされていません。

表 *12* : バージョン *6.2.3* の機能

機能	説明
アップグレードの前に、アップグレードパッケージを管理対象デバイスにコピーします。	実際のアップグレードを実行する前に、FMCから管理対象デバイスにアップグレードパッケージをコピー（またはプッシュ）できるようになりました。帯域幅の使用量が少ない時間帯やアップグレードのメンテナンス期間外でプッシュできるため、この機能は便利です。 高可用性デバイス、クラスタデバイス、またはスタック構成デバイスにプッシュすると、アップグレードパッケージは最初にアクティブ/コントロール/プライマリに送信され、次にスタンバイ/データ/セカンダリに送信されます。 新規/変更された画面：**[システム（System）]** > **[更新（Updates）]**

支援が必要な場合

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。

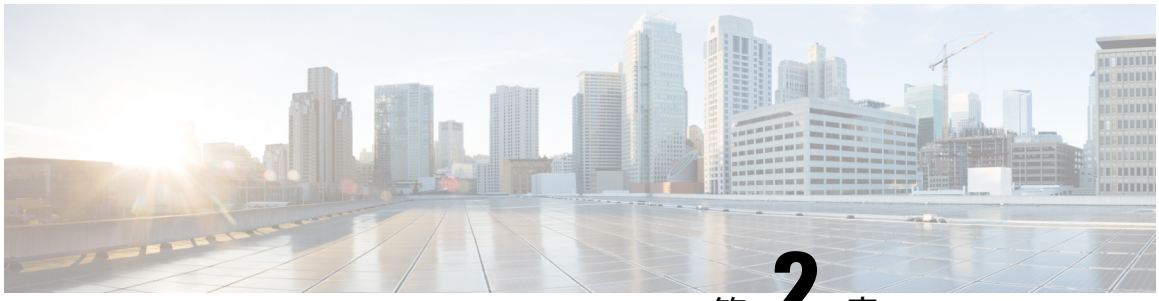
- マニュアル：http://www.cisco.com/go/threatdefense-71-docs
- シスコ サポートおよびダウンロード サイト：https://www.cisco.com/c/en/us/support/index.html
- Cisco Bug Search Tool：https://tools.cisco.com/bugsearch/
- シスコ通知サービス：https://www.cisco.com/cisco/support/notifications.html

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



第 2 章

システム要件

このドキュメントでは、バージョン 7.1 のシステム要件を記載します。

FMC プラットフォーム

FMC 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します。FMC とのデバイスの互換性については、「FTD管理 （19 ページ）」を参照してください。一般的な互換性情報については、Cisco Secure Firewall Management Center 互換性ガイド を参照してください。

FMC ハードウェア

バージョン 7.1 は次の FMC ハードウェアをサポートします。

- FMC 1600
- FMC 2600
- FMC 4600

また、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必要があります（Cisco Secure Firewall Threat Defense/Firepower ホットフィックス リリース ノート を参照）。

FMCv

バージョン 7.1 はパブリッククラウドに加えて、プライベートクラウドやオンプレミスクラウドでの FMCv 導入をサポートします。

FMCv では、2、10、25、または 300 台のデバイスを管理できるライセンスを購入できます。ただし、300 台のデバイスをサポートするのは、一部のプラットフォームのみです。また、2 デバイスの仮想 FMC は高可用性をサポートしていません。 サポートされているインスタンスの詳細については、Cisco Secure Firewall Management Center Virtual 入門ガイド を参照してください。

表 *13* : バージョン *7.1 FMCv* プラットフォーム

プラットフォーム（Platform）	管理対象デバイス		ハイ アベイラビリティ
	2、10、25	300	
パブリック クラウド			
Amazon Web Services（AWS）	対応	対応	対応
Google Cloud Platform（GCP）	対応	—	—
Microsoft Azure	対応	—	—
Oracle Cloud Infrastrucure（OCI）	対応	対応	対応
オンプレミス/プライベートクラウド			
Cisco HyperFlex	対応	—	—
カーネルベース仮想マシン（KVM）	対応	—	—
Nutanix エンタープライズクラウド	対応	—	—
OpenStack	対応	—	—
VMware vSphere/VMware ESXi 6.5、6.7、または 7.0	対応	対応	対応

クラウド提供型の管理センター

Cisco クラウド提供型 Firewall Management Center は、複数のシスコ セキュリティ ソリューションの管理を統合する Cisco Defense Orchestrator（CDO）プラットフォームを通して提供されます。クラウド提供型 Firewall Management Center にはバージョンがないため、機能の更新はシスコが行います。

顧客展開型の管理センターは、仮想プラットフォームの場合でも、オンプレミス FMC と呼ばれることが多いことに注意してください。

アップグレードのガイドラインについては、「クラウド提供型 Firewall Management Center のガイドライン （24 ページ）」を参照してください。

（注） クラウド提供型の Management Center では、バージョン 7.1 のデバイスを管理できません。

FTDプラットフォーム

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。デバイスの管理方法については、「FTD管理 （19 ページ）」を参照してください。一般的な互換性情報については、Cisco Secure Firewall Threat Defense 互換性ガイドを参照してください。

FTD ハードウェア

バージョン 7.1 FTD のハードウェアは、多様なスループット、拡張性、およびフォームファクタに対応します。

表 *14* : バージョン *7.1 FTD* ハードウェア

プラットフォーム	FMC 互換		FDM 互換		注記
	お客様が導入	クラウド提供型	FDM のみ	FDM + CDO	
Firepower1010、1120、1140、1150	対応	—	対応	対応	—
Firepower 2110、2120、2130、2140	対応	—	対応	対応	—
Cisco Secure Firewall3110、3120、3130、3140	対応	—	対応	対応	バージョン 7.1.0 リリースには、これらのデバイスのオンラインヘルプが含まれていません。FMC の場合、新しいオンラインヘルプがバージョン 7.1.0.2 に含まれています。FDM の場合は、Cisco.com に掲載されているドキュメントを参照してください。
Firepower 4110、4120、4140、4150 Firepower 4112、4115、4125、4145	対応	—	対応	対応	FXOS 2.11.1.154 以降のビルドが必要です。 最新のファームウェアを推奨します。Cisco Firepower 4100/9300 FXOS ファームウェアアップグレードガイドを参照してください。

プラットフォーム	FMC 互換		FDM 互換		注記
	お客様が導入	クラウド提供型	FDM のみ	FDM + CDO	
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	対応	—	対応	対応	FXOS 2.11.1.154 以降のビルドが必要です。 最新のファームウェアを推奨します。Cisco Firepower 4100/9300 FXOS ファームウェアアップグレードガイドを参照してください。
ISA 3000	はい	—	対応	対応	最新の ROMMON イメージが必要です。Cisco Secure Firewall ASA および Secure Firewall Threat Defense 再イメージ化ガイドを参照してください。

FTDv

バージョン 7.1 FTDv の導入により、スループット要件とリモートアクセス VPN セッションの制限に基づいて、パフォーマンス階層型のスマート ソフトウェア ライセンスがサポートされます。オプションは、FTDv5（100 Mbps/50 セッション）から FTDv100（16 Gbps/10,000 セッション）までです。サポートされているインスタンス、スループット、およびその他のホスティング要件の詳細については、該当するスタートアップガイドを参照してください。

表 *15 : バージョン 7.1 FTDv* プラットフォーム

デバイスのプラットフォーム	FMC 互換		FDM 互換	
	お客様が導入	クラウド提供型	FDM のみ	FDM + CDO
パブリック クラウド				
Amazon Web Services（AWS）	対応	—	対応	対応
Microsoft Azure	対応	—	対応	対応
Google Cloud Platform（GCP）	対応	—	—	—
Oracle Cloud Infrastrucure（OCI）	対応	—	—	—

デバイスのプラットフォーム	FMC 互換		FDM 互換	
	お客様が導入	クラウド提供型	FDM のみ	FDM + CDO
オンプレミス/プライベートクラウド				
Cisco Hyperflex	対応	—	対応	対応
カーネルベース仮想マシン（KVM）	対応	—	対応	対応
Nutanix エンタープライズクラウド	対応	—	対応	対応
OpenStack	対応	—	—	—
VMware vSphere/VMware ESXi 6.5、6.7、または 7.0	対応	—	対応	対応

FTD管理

デバイスモデルとバージョンに応じて、次のデバイス管理方法をサポートしています。

お客様が導入したFMC

すべてのデバイスは、お客様が導入したFMCによるリモート管理に対応しています。FMCでは管理対象デバイスと同じまたはそれ以降のバージョンを実行する必要があります。これは、以下を意味します。

- より新しいFMCでより古いデバイスを管理できます。通常は、メジャーバージョンをいくつか遡ることができます。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。
- 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。

ほとんどの場合、旧バージョンのデバイスはFMCのメジャーバージョンまたはメンテナンスバージョンに直接アップグレードできます。ただし、対象バージョンがデバイスでサポートされていても、直接アップグレードできない旧バージョンのデバイスを管理している場合があります。リリース固有の要件については、を参照してください。アップグレードする最小バージョン （23 ページ）。

表 *16 :* お客様が導入した *FMC* : デバイスの互換性

FMC バージョン	管理可能な最も古いデバイスバージョン
7.3	6.7
7.2	6.6
7.1	6.5
7.0	6.4
6.7	6.3
6.6	6.2.3
6.5	6.2.3
6.4	6.1
6.3	6.1
6.2.3	6.1
6.2.2	6.1
6.2.1	6.1
6.2	6.1
6.1	5.4.0.2/5.4.1.1
6.0.1	5.4.0.2/5.4.1.1
6.0	5.4.0.2/5.4.1.1
5.4.1	5.4.1（ASA-5506-X シリーズ、ASA5508-X、および ASA5516-X の ASA FirePOWER）。 5.3.1（ASA5512-X、ASA5515-X、ASA5525-X、ASA5545-X、ASA5555-X、および ASA-5585-X シリーズの ASA FirePOWER）。 5.3.0（Firepower 7000/8000 シリーズおよびレガシーデバイス）。

クラウド提供型 Firewall Management Center

クラウド提供型 Firewall Management Center は、次を実行している FTD デバイスを管理できます。

- バージョン 7.2 以降
- 7.0.3 以降のメンテナンスリリース

クラウド提供型 Firewall Management Center は、バージョン 7.1 を実行している FTD デバイス、または任意のバージョンを実行している従来のデバイスを管理できません。クラウド管理の登録を解除するか、または無効にしない限り、クラウド管理対象デバイスはバージョン 7.0.x からバージョン 7.1 にアップグレードできません。バージョン 7.2 以降に直接アップグレードすることをお勧めします。

クラウド管理デバイスは、イベントのログ記録と分析の目的でのみ、バージョン 7.2 以降のお客様導入の管理センターに追加できます。あるいは、シスコのセキュリティ分析とロギング（SaaS） を使用して、Cisco Cloud にセキュリティイベントを送信できます。

ブラウザ要件

ブラウザ

現在サポートされている MacOS と Microsoft Windows 上で稼働する、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 Edge（Windows のみ）

他のブラウザで問題が発生した場合、またはサポートが終了したオペレーティングシステムを実行している場合は、交換またはアップグレードしてください。問題が解消されない場合は、Cisco TAC にお問い合わせください。

（注） Apple Safari を使用した広範なテストを実施していません。また、FMC ウォークスルーを使用した Microsoft Edge の広範なテストも実施していません。ただし、Cisco TAC で発生した問題に関するフィードバックを求めています。

ブラウザの設定と拡張

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

一部のブラウザ拡張機能では、PKI オブジェクトの証明書やキーなどのフィールドに値を保存できないことに注意してください。これらの拡張機能には Grammarly や Whatfix Editor などがありますが、それに限りません。この問題は、これらの拡張機能によってフィールドに文字（HTML など） が挿入され、システムが無効と見なすために発生します。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。

画面解像度

インターフェイス	最小解像度
FMC	1280 X 720
Firepower 4100/9300 用 Firepower Chassis Manager	1024 X 768

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には、**[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。

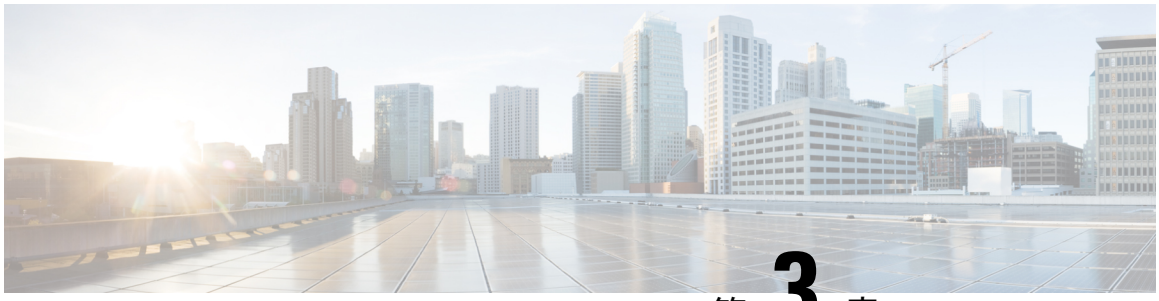
詳しい手順については、オンラインヘルプまたはのコンフィギュレーションガイドを参照してください。

（注） 自己署名証明書を置き換えない場合は、次の手順を実行します。

- Google Chrome は、画像、CSS、JavaScript などの静的コンテンツをキャッシュしません。これにより、特に低帯域幅環境では、ページの読み込み時間が長くなります。
- Mozilla Firefox は、ブラウザの更新時に自己署名証明書を信頼しなくなる場合があります。この場合は Firefox を更新できますが、一部の設定が失われることに注意してください。Mozilla の Firefox 更新サポートページを参照してください。

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。



第 3 章

ソフトウェアのアップグレードガイドライン

利便性を考え、このドキュメントには、FTDリリースノートで公開されている重要なリリース固有のソフトウェアのアップグレードガイドラインを複製したものが記載されてます。Firepower 4100/9300 の FXOS アップグレードガイドラインについては、FXOS のアップグレードガイドライン （74 ページ） を参照してください。

重要 リリースノートにも目を通してください。重要な追加情報やバージョン固有の情報が記載されている場合があります。たとえば、新機能や廃止された機能が原因で、アップグレード前またはアップグレード後に設定の変更が必要になったり、アップグレードができなかったりする場合があります。または、既知の問題（未解決のバグ）がアップグレードに影響することがあります。

アップグレードする最小バージョン

アップグレードする最小バージョン

次のように、メンテナンスリリースを含む バージョン 7.1 に直接アップグレードできます。

表 *17*：バージョン *7.1* 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
FMC	6.5

プラットフォーム	最小バージョン
FTD	6.5 Firepower 4100/9300 には FXOS 2.11.1.154 が必要です。ほとんどの場合、各メジャーバージョンで最新の FXOS ビルドを使用することを推奨します。判断のヒントについては、Cisco Firepower 4100/9300 FXOS Release Notes, 2.11(1）を参照してください。

パッチを適用する最小バージョン

パッチは4桁目のみを変更します。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。

クラウド提供型 Firewall Management Center のガイドライン

クラウド提供型 Firewall Management Center はアップグレード対象外です。 にはバージョンがないため、機能の更新はシスコが行います。

クラウド提供型 Firewall Management Center を使用した FTD のアップグレード

クラウド提供型 Firewall Management Center を使用して FTD をアップグレードするには、Firepower Management Center 用 Cisco Firepower Threat Defense アップグレードガイド の最新リリースバージョンを使用します。

（注） クラウド提供型 Firewall Management Center では FTD バージョン 7.1 を管理できません。クラウド管理の登録を解除して無効にしない限り、クラウド管理型デバイスをバージョン 7.0 からバージョン 7.1 にアップグレードできません。バージョン 7.2 以降に直接アップグレードすることをお勧めします。

共同管理デバイスのアップグレード

お客様が導入した FMC バージョン 7.2 以降を実行しているハードウェアでは、クラウド管理型の FTD デバイスを共同管理できますが、用途はイベントのロギングと分析に限られます。クラウド提供型 Firewall Management Center を使用して、アップグレードを含む FTD のすべての側面を管理および設定する必要があります。

お客様が導入した FMC では、その管理対象デバイスと同じまたはそれ以降のバージョンを実行する必要があります。これには クラウド提供型 Firewall Management Center によって共同管理されるデバイスも含まれます。つまり、クラウド提供型 Firewall Management Center を使用し

て、お客様が導入した FMC より新しいバージョンに共同管理デバイスをアップグレードすることはできません。

たとえば、2 つのマネージャを持つ Threat Defense デバイスがあるとします。

- バージョン A を実行しているデバイスがあります。
- お客様が導入した FMC では、バージョン B を実行しています。
- クラウド提供型 Firewall Management Center にはバージョンがありません。

このシナリオでは、クラウド提供型 Firewall Management Center を使用してデバイスをバージョン B（共同マネージャと同じバージョン）にアップグレードできますが、バージョン C（共同マネージャより新しいバージョン）にはアップグレードできません。

バージョン 7.1 のアップグレードガイドライン

以下のチェックリストでは、該当する可能性のある新規アップグレードガイドラインや以前に公開されたアップグレードガイドラインを提供します。

表 *18 : FMC* を使用した *FTD* のアップグレードガイドラインバージョン *7.1*

✓	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
	Cisco Secure Firewall Management Center の新機能（リリース別）：アップグレードに影響を与える新機能および廃止された機能が記載されています。現在のバージョンと対象バージョンの間にあるすべてのバージョンを確認してください。	任意	任意	任意
	Cisco Firepower リリースノート：「*Open and Resolved Bugs*」の章に、アップグレードに影響を与えるバグが記載されています。現在のバージョンと対象バージョン間にあるすべてのバージョンのリリースノートを確認してください。	任意	任意	任意
	アップグレードする最小バージョン （23 ページ）	任意	任意	任意
	FXOS のアップグレードガイドライン （74 ページ）	Firepower 4100/9300	任意	任意

✓	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
	アップグレード禁止：バージョン 7.0.4 以降から バージョン 7.1.0（26 ページ）	任意（Any）	7.0.4 以降	7.1.0 のみ
	高可用性 FMC の Cisco Secure Malware Analytics に再接続する（26 ページ）	FMC	6.4.0 ～ 6.7.x	7.0 以上
	アップグレードの失敗：Firepower 1010 スイッチポートでの無効な VLAN ID （27 ページ）	Firepower 1010	6.4.0 ～ 6.6.x	6.7 以降
	FMCv には 28 GB の RAM が必要（27 ページ）	FMCv	6.2.3 ～ 6.5.0.x	6.6 以降

アップグレード禁止：バージョン 7.0.4 以降から バージョン 7.1.0

展開：すべて

アップグレード元：バージョン 7.0.4 以降のメンテナンスリリース

直接アップグレード先：バージョン 7.1.0 のみ

データストアの非互換性のため、をバージョン 7.0.4 以降からバージョン 7.1.0 にアップグレードすることができません。バージョン 7.2 以降に直接アップグレードすることをお勧めします。

高可用性 FMC の Cisco Secure Malware Analytics に再接続する

展開：動的分析のためにファイルを送信する高可用性/AMP for Networks（マルウェア検出）展開

アップグレード元：バージョン 6.4.0 ～ 6.7.x

直接アップグレード先：バージョン 7.0.0 以降

関連するバグ： CSCvu35704

バージョン 7.0.0 では、フェールオーバー後にシステムが動的分析用のファイルの送信を停止する高可用性の問題が修正されています。修正を有効にするには、Cisco Secure Malware Analytics パブリッククラウドに再度関連付ける必要があります。

高可用性ペアをアップグレードした後、プライマリ FMC で次の手順を実行します。

1. **[AMP] > [ダイナミック分析接続（Dynamic Analysis Connections）]**を選択します。
2. パブリッククラウドに対応するテーブル行で、 [関連付け（Associate）] をクリックします。

ポータルウィンドウが開きます。サインインする必要はありません。再関連付けは、数分以内にバックグラウンドで行われます。

アップグレードの失敗：Firepower1010スイッチポートでの無効なVLAN ID

展開：Firepower 1010

アップグレード元：バージョン 6.4 ～ 6.6

直接アップグレード先：バージョン 6.7 以降

Firepower 1010 では、VLAN ID を 3968 ー 4047 の範囲にしてスイッチポートを設定した場合、FTD のバージョン 6.7 以降へのアップグレードは失敗します。これらの ID は内部使用専用です。

FMCv には 28 GB の RAM が必要

展開：FMCv

アップグレード元：バージョン 6.2.3 ～ 6.5

直接アップグレード先：バージョン 6.6 以降

すべての FMCv 実装には同じ RAM 要件が適用され、32 GB が推奨、28 GB が必須となりました（FMCv 300 の場合は 64 GB）。仮想アプライアンスに割り当てられたメモリが 28 GB 未満の場合、バージョン 6.6 以降へのアップグレードは失敗します。アップグレード後、メモリ割り当てを引き下げると、正常性モニターがアラートを発行します。

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

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

次の表に、メモリが不足している展開のアップグレード前の要件を示します。

表 *19 :* バージョン *6.6* 以降 にアップグレードする場合の *FMCv* のメモリ要件

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

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、アップグレード中は手動で再起動またはシャットダウンしないでください。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。

応答しない FMC

進行中のアップグレードは再開しないでください。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。

応答しない FTD のアップグレード

メジャーアップグレードやメンテナンスアップグレードでは、失敗したアップグレードまたは進行中のアップグレードを手動でキャンセルし、失敗したアップグレードを再試行できます。FMC で、[デバイス管理（Device Management）] ページの [アップグレード（Upgrade）] タブ、およびメッセージセンターからアクセスできる [アップグレードステータス（Upgrade Status）] ポップアップを使用します。FTD CLI を使用することもできます。

（注） デフォルトでは、FTDはアップグレードが失敗すると自動的にアップグレード前の状態に復元されます（「自動キャンセル」）。失敗したアップグレードを手動でキャンセルまたは再試行できるようにするには、アップグレードを開始するときに自動キャンセルオプションを無効にします。パッチの自動キャンセルはサポートされていません。高可用性またはクラスタ展開では、自動キャンセルは各デバイスに個別に適用されます。つまり、1 つのデバイスでアップグレードが失敗した場合、そのデバイスだけが元に戻ります。

この機能は、パッチまたはバージョン 6.6 以前からのアップグレードではサポートされていません。

FTD アップグレードのトラフィックフローとインスペクション

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 *20 :* トラフィックフローとインスペクション：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		トラフィックの挙動
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 ISA 3000 のブリッジ グループ インターフェイスの場合に限り、FlexConfig ポリシーを使用して、停電時のハードウェアバイパスを設定できます。これにより、ソフトウェアのアップグレード中にトラフィックのドロップが発生しますが、デバイスがアップグレード後の再起動中、インスペクションなしでトラフィックが通過します。
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：[バイパス（Bypass）]：[強制（Force）]	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がスタンバイモード：[バイパス（Bypass）]：[スタンバイ（Standby）]	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：[バイパス（Bypass）]：[無効（Disabled）]	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。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。

ソフトウェアの復元（メジャーおよびメンテナンスリリース）

たとえ高可用性および拡張性を備えた環境でも、復元時のトラフィックフローとインスペクションの中断を予測する必要があります。これは、すべてのユニットを同時に復元させたほうが、復元がより正常に完了するためです。同時復元とは、すべてのデバイスがスタンドアロンであるかのように、トラフィックフローと検査の中断がインターフェイスの設定のみに依存することを意味します。

ソフトウェアのアンインストール（パッチ）

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。

設定変更の導入

Snort プロセスを再起動すると、高可用性/拡張性を備えた構成になっているものを含め、すべてのデバイスでトラフィックフローとインスペクションが一時的に中断されます。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。Snort を再起動せずに展開すると、リソース要求時にいくつかのパケットが検査なしでドロップされることがあります。

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。

表 *21* : トラフィックフローとインスペクション：設定変更の展開

インターフェイス コンフィギュレーション		トラフィックの挙動
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		トラフィックの挙動
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。	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フェールオープン：ダウン（Snort Fail Open: Down）]：無効	廃棄
	インライン、[Snortフェールオープン：ダウン（Snort Fail Open: Down）]：有効	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。

時間とディスク容量のテスト

参考のために、FMC およびソフトウェアのアップグレードにかかる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 アップグレード中は、設定を変更または展開しないでください。システムが非アクティブに見えても、手動で再起動またはシャットダウンしないでください。ほとんどの場合、進行中のアップグレードを再開しないでください。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応答しないアップグレード（28 ページ）を参照してください。

表 *22 :* 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	デバイスアップグレードの時間は、FMC展開でのテストに基づいています。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。 高可用性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。
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（/Volume または /var 内）に必要な容量も報告します。FTD アップグレードパッケージ用の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。

空きディスク容量が十分でない場合、アップグレードは失敗します。

表 *23 :* ディスク容量の確認

プラットフォーム	コマンド
FMC	**[システム（System）]**>**[モニタリング（Monitoring）]**>**[統計（Statistics）]**を選択し、FMC を選択します。[ディスク使用率（Disk Usage）] で、[By Partition] の詳細を展開します。
FTD with FMC	**[システム（System）]**>**[モニタリング（Monitoring）]**>**[統計（Statistics）]**を選択し、確認するデバイスを選択します。[ディスク使用率（Disk Usage）] で、[By Partition] の詳細を展開します。

バージョン 7.1.0.3 の時間とディスク容量

表 *24 :* バージョン *7.1.0.3* 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	/var 内で 2.9 GB	/ 内で 29 MB	—	20 分	7 分
FMCv：VMware	/var 内で 4.0 GB	/ 内で 25 MB	—	23 分	6 分
Firepower 1000 シリーズ	—	/ngfw 内で 3.2 GB	1.0 GB	9 分	13 分
Firepower 2100 シリーズ	—	/ngfw 内で 3.2 GB	1.1 GB	7 分	14 分
Secure Firewall 3100 シリーズ	—	/ngfw 内で 3.5 GB	1.1 GB	4 分	15 分
Firepower 4100 シリーズ	—	/ngfw 内で 2.8 GB	780 MB	5 分	7 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 4100 シリーズ コンテナ インスタンス	—	/ngfw 内で 2.9 GB	780 MB	6 分	5 分
Firepower 9300	—	/ngfw 内で 2.3 GB	780 MB	5 分	10 分
ISA 3000	/ngfw/var 内で 1.7 GB	/ngfw/bin 内で 270 MB	780 MB	11 分	14 分
FTDv：VMware	/ngfw/var 内で 2.1 GB	/ngfw/bin 内で 270 MB	350 MB	5 分	6 分

バージョン 7.1.0.2 の時間とディスク容量

表 *25 :* バージョン *7.1.0.2* 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	アップグレード時間	リブート時間
FMC	/var 内で 2.0 GB	/ 内で 19 MB	—	20 分	4 分
FMCv：VMware	/var 内で 2.5 GB	/ 内で 14 MB	—	21 分	[1 分（1 min）]
Secure Firewall 3100 シリーズ	—	/ngfw 内で 3.2 GB		4 分	46 分

バージョン 7.1.0.1 の時間とディスク容量

表 *26 :* バージョン *7.1.0.1* の時間とディスク容量

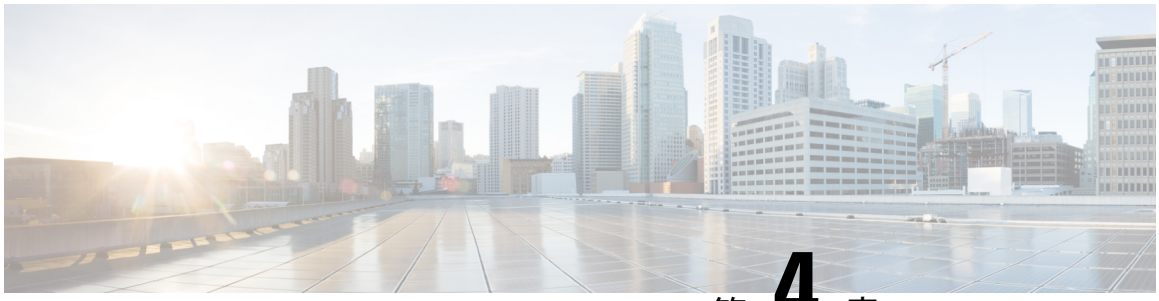
プラットフォーム	ボリュームの容量	必要容量	FMC の容量	アップグレード時間	リブート時間
FMC	/var 内で 2.0 GB	/ 内で 19 MB	—	18 分	8 分
FMCv：VMware	/var 内で 2.2 GB	/ 内で 14 MB	—	21 分	4 分
Firepower 1000 シリーズ	—	/ngfw 内で 5.6 GB	430 MB	10 分	11 分
Firepower 2100 シリーズ	—	/ngfw 内で 5.6 GB	420 MB	10 分	10 分
Firepower 4100 シリーズ	—	/ngfw 内で 5.6 GB	430 MB	7 分	7 分
Firepower 4100 シリーズ コンテナ インスタンス	—	/ngfw 内で 5.6 GB	430 MB	6 分	4 分
Firepower 9300	—	/ngfw 内で 5.1 GB	430 MB	7 分	8 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
ISA 3000	/ngfw/var 内で 2.0 GB	/ngfw/bin 内で 240 MB	430 MB	4 分	13 分
FTDv：VMware	/ngfw/var 内で 1.5 GB	/ngfw/bin 内で 240 MB	430 MB	4 分	4 分

バージョン 7.1.0 の時間とディスク容量

表 *27 :* バージョン *7.1.0* の時間とディスク容量

プラットフォーム		ボリュームの容量	必要容量	FMC の容量	アップグレード時間	リブート時間
FMC		/var 内で 16.9 GB	/ 内で 43 MB	—	33 分	15 分
FMCv：VMware		/var 内で 17 GB	/ 内で 50 MB で	—	34 分	5 分
Firepower 1000 シリーズ		—	/ngfw 内で 8.2 GB	930 MB	16 分	11 分
Firepower 2100 シリーズ		—	/ngfw 内で 8.3 GB	1 GB	13 分	13 分
Firepower 4100 シリーズ		—	/ngfw 内で 8.6 GB	870 MB	15 分	9 分
Firepower 4100 シリーズ コンテナ インスタンス		—	/ngfw 内で 8.6 GB	870 MB	16 分	8 分
Firepower 9300		—	/ngfw 内で 11.2 GB	870 MB	11 分	12 分
ISA 3000	バージョン 6.5 ～ 6.6	/home 内で 9.3 GB	/ngfw 内で 256 KB	1 GB	21 分	8 分
	バージョン 6.7 以降	/ngfw/Volume 内で 9.3 GB	/ngfw 内で 270 KB			
	バージョン 7.0 以降	/ngfw/var 内で 9.2 GB	/ngfw/bin 内で 260 KB			
FTDv：VMware	バージョン 6.5 ～ 6.6	/home 内で 4.6 GB	/ngfw 内で 925 KB	1 GB	11 分	6 分
	バージョン 6.7 以降	/ngfw/Volume 内で 4.4 GB	/ngfw 内で 210 KB			
	バージョン 7.0 以降	/ngfw/var 内で 5.3 GB	/ngfw/bin 内で 220 KB			



第 4 章

FMCのアップグレード

この章では、お客様が導入した FMC を バージョン 7.1 から新しいバージョンにアップグレードする方法について説明します。

クラウド提供型の Management Center を使用している場合、この章は必要ありません。その場合は、シスコが Management Center の機能更新を担当します。ユーザーは Firepower Management Center 用 Cisco Firepower Threat Defense アップグレードガイド の最新のリリースバージョンを使用してデバイスをアップグレードできます。

FMC のアップグレード チェックリスト

計画と実現可能性

誤りを避けるには、注意深い計画と準備が役立ちます。

✓	アクション/チェック	詳細
	展開を評価します。	状況を理解することにより、目的を達成する方法を決定します。現在のバージョンとモデル情報に加えて、展開が高可用性/拡張性を実現するように設定されているかどうか、デバイスが IPS またはファイアウォールとして展開されているかどうかなどを確認します。

✓	アクション/チェック	詳細
	アップグレードパスを計画します。	これは、大規模展開、マルチホップアップグレード、またはオペレーティングシステムまたはホスティング環境をアップグレードする必要がある状況では特に重要です。次を参照してください。 • FMC のアップグレードパス （41 ページ） • FTD のアップグレードパス （55 ページ） • FXOS のアップグレードパス （76 ページ）
	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。	主要なアップグレードでは特に、アップグレードの前または後に、アップグレードにより重要な設定変更が発生することがあります。以下を参照してください。 • ソフトウェアのアップグレードガイドライン （23ページ）：重要なリリース固有のアップグレードガイドラインが記載されています。 • Cisco Secure Firewall Management Center の新機能（リリース別）：アップグレードに影響を与える新機能および廃止された機能が記載されています。現在のバージョンと対象バージョンの間にあるすべてのバージョンを確認してください。 • Cisco Firepower リリースノート：「*Open and Resolved Bugs*」の章に、アップグレードに影響を与えるバグが記載されています。現在のバージョンと対象バージョン間にあるすべてのバージョンのリリースノートを確認してください。：サポート契約がある場合は、Cisco バグ検索ツールを使用して最新のバグリストを取得できます。 • Cisco Firepower 4100/9300 FXOS リリースノート：Firepower 4100/9300 の FXOS アップグレードガイドラインが記載されています。
	帯域幅を確認します。	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。可能な場合は常に、アップグレードパッケージを事前にアップロードしてください。
	メンテナンス時間帯をスケジュールします。	影響が最小限になるようにメンテナンス時間帯をスケジュールします。特にアップグレードにかかる可能性がある時間を考慮してください。また、この時間帯で実行する必要があるタスクと、事前に実行できるタスクを検討します。 時間とディスク容量のテスト （32 ページ）を参照。

バックアップ

アップグレードの前後に、安全な遠隔地にバックアップし、正常に転送が行われることを確認することを強くお勧めします。

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

✓	アクション/チェック	詳細
	設定およびイベントをバックアップします。	Firepower Management Center アドミニストレーション ガイドの「バックアップ/復元」の章を参照してください。
	Firepower 4100/9300 の FXOS をバックアップします。	Firepower Chassis Manager または FXOS CLI を使用して、論理デバイス設定およびプラットフォーム設定を含むシャーシ設定をエクスポートします。 詳細については、『Cisco Firepower 4100/9300 FXOS コンフィギュレーション ガイド』の「コンフィギュレーションのインポート/エクスポート」を参照してください。

アップグレードパッケージ

アップグレードの前にアップグレードパッケージをシステムにアップロードすると、メンテナンス時間が短縮されます。

✓	アクション/チェック	詳細
	シスコからアップグレードパッケージをダウンロードして、FMC にアップロードします。	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。FMC を使用して直接ダウンロードを実行することもできます。 FMC の高可用性では、FMC アップグレードパッケージを両方のピアにアップロードし、パッケージをスタンバイに転送する前に同期を一時停止する必要があります。同期の中断を制限するには、アップグレードの準備段階でパッケージをアクティブのピアに転送し、同期を一時停止した後に、実際のアップグレードプロセスの一環としてスタンバイのピアに転送します。 FMC のアップグレードパッケージのアップロード （44 ページ） を参照してください。

関連するアップグレード

メンテナンス時間帯にホスティング環境のアップグレードを実行することをお勧めします。

✓	アクション/チェック	詳細
	仮想ホスティングをアップグレードします。	必要に応じて、ホスティング環境をアップグレードします。通常、古いバージョンの VMware を実行していて、メジャーアップグレードを実行している場合、アップグレードが必要です。

最終チェック

一連の最終チェックにより、ソフトウェアをアップグレードする準備が整います。

✓	アクション/チェック	詳細
	設定を確認します。	必要なアップグレード前の設定変更を行っていることを確認し、必要なアップグレード後の設定変更を行う準備をします。
	NTP 同期を確認します。	時刻の提供に使用している NTP サーバーとすべてのアプライアンスが同期していることを確認します。時刻のずれが 10 秒を超えている場合、ヘルスモニター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。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。 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。 • FTD：**show time** CLI コマンドを使用します。
	設定を展開します。	アップグレードする前に設定を展開すると、失敗する可能性が減少します。展開により、トラフィックフローとインスペクションが影響を受ける可能性があります。FTD アップグレードのトラフィックフローとインスペクション（29 ページ）を参照してください。
	準備状況チェックを実行します。	互換性と準備状況のチェックに合格すると、アップグレードが失敗する可能性が低くなります。 FMC で準備状況チェックを実行します。（45 ページ）を参照してください。

✓	アクション/チェック	詳細
	のディスク容量を確認します。	準備状況チェックには、ディスク容量チェックが含まれます。空きディスク容量が十分でない場合、アップグレードは失敗します。 Management Center で使用可能なディスク容量を確認するには、**システム**（⚙）>**[モニタリング（Monitoring）]**>**[統計（Statistics）]**を選択してから FMC を選択します。[ディスク使用率（Disk Usage）] で、[By Partition] の詳細を展開します。
	実行中のタスクを確認します。	重要なタスク（最終展開を含む）が完了していることを確認します。アップグレードの開始時に実行中のタスクは停止し、失敗したタスクとなり、再開できません。 バージョン 6.6.3+ からのアップグレードは、スケジュールされたタスクを自動的に延期します。アップグレード中に開始するようにスケジュールされたタスクは、アップグレード後の再起動の 5 分後に開始されます。これが起こらないようにするには（または以前のバージョンからアップグレードする場合）、アップグレード中に実行するようにスケジュールされているタスクを確認し、それらをキャンセルまたは延期します。

FMC のアップグレードパス

お客様が導入した FMC のアップグレードパスを次の表に示します。

顧客が展開した FMC はその管理対象デバイスと同じか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。

現在の FTD/FMC のバージョンが対象のバージョンより後の日付にリリースされた場合、期待どおりにアップグレードできない可能性があります。このような場合、アップグレードはすぐに失敗し、2 つのバージョン間にデータストアの非互換性があることを説明するエラーが表示されます。現在のバージョンと対象のバージョンの両方のに関するリリースノートには、特定の制限が掲載されています。

表 *28 : FMC* の直接アップグレード

現在のバージョン	ターゲットバージョン
7.3	→ 任意の後続リリース 7.3.x

現在のバージョン	ターゲットバージョン
7.2	次のいずれかです。 → 7.3.x → 任意の後続リリース 7.2.x
7.1	次のいずれかです。 → 7.3.x → 7.2.x → 任意の後続リリース 7.1.x
7.0 FMC 1000、2500、4500 に対する最後のサポート	次のいずれかです。 → 7.3.x → 7.2.x → 7.1.x → 任意の後続リリース 7.0.x （注） データストアの非互換性のため、 をバージョン 7.0.4 以降からバージョン 7.1.0 にアップグレードすることができません。バージョン 7.2 以降に直接アップグレードすることをお勧めします。
6.7	次のいずれかです。 → 7.2.x → 7.1.x → 7.0.x → 任意の後続リリース 6.7.x

現在のバージョン	ターゲットバージョン
6.6 FMC 2000 および 4000 の最後のサポート。	次のいずれかです。 → 7.2.x → 7.1.x → 7.0.x → 6.7.x → 任意の後続リリース 6.6.x （注） データストアの非互換性のため、FMC をバージョン 6.6.5 以降からバージョン 6.7.0 にアップグレードすることができません。バージョン 7.0 以降に直接アップグレードすることをお勧めします。
6.5	次のいずれかです。 → 7.1.x → 7.0.x → 6.7.x → 6.6.x
6.4 FMC 750、1500、および 3500 の最後のサポート。	次のいずれかです。 → 7.0.x → 6.7.x → 6.6.x → 6.5
6.3	次のいずれかです。 → 6.7.x → 6.6.x → 6.5 → 6.4

現在のバージョン	ターゲットバージョン
6.2.3	次のいずれかです。 → 6.6.x → 6.5 → 6.4 → 6.3

FMC のアップグレードパッケージのアップロード

この手順を使用すると、アップグレードパッケージを FMC に手動でアップロードできます。

ヒント　一部のアップグレードパッケージは、リリースが手動でダウンロードできるようになってからしばらくすると、直接ダウンロードできるようになります。遅延の長さは、リリースの種類、リリースの選択、およびその他の要因によって異なります。FMC がインターネットにアクセスできる場合は、[アップデートのダウンロード（Download Updates）] ボタンをクリックして、FMC とすべての管理対象デバイス向けの最新の VDB、最新のメンテナンスリリース、および最新の重要パッチをすぐにダウンロードできます。

アップグレードパッケージは、署名付きの tar アーカイブ（.tar）です。署名付きのパッケージをアップロードした後、パッケージが確認されるため、FMC の [システムの更新（System Updates）] ページのロードに数分かかることがあります。表示を迅速化するには、不要なアップグレードパッケージを削除してください。署名付きのパッケージは解凍しないでください。

始める前に

高可用性ペアのスタンバイの FMC をアップグレードしている場合は、同期を一時停止します。

FMC の高可用性では、FMC アップグレードパッケージを両方のピアにアップロードし、パッケージをスタンバイに転送する前に同期を一時停止する必要があります。同期の中断を制限するには、アップグレードの準備段階でパッケージをアクティブのピアに転送し、同期を一時停止した後に、実際のアップグレードプロセスの一環としてスタンバイのピアに転送します。

ステップ 1　シスコサポートおよびダウンロードサイトから適切なアップグレードパッケージをダウンロードします。
https://www.cisco.com/go/firepower-software

ファミリまたはシリーズのすべてのモデルに同じソフトウェアアップグレードパッケージを使用します。適切なソフトウェアを見つけるには、使用しているモデルを選択または検索し、適切なバージョンのソフトウェアのダウンロードページを参照します。使用可能なアップグレードパッケージは、インストールパッケージ、ホットフィックス、およびその他の該当するダウンロードとともに表示されます。

アップグレードパッケージのファイル名には、次のように、プラットフォーム、パッケージタイプ（アップグレード、パッチ、ホットフィックス）、ソフトウェアバージョン、およびビルドが反映されています。

```
Cisco_Firepower_Mgmt_Center_Upgrade-7.1-999.sh.REL.tar
```

ステップ 2 FMC で、**システム**（⚙）>**[更新（Updates）]** を選択します。

ステップ 3 [更新のアップロード（Upload Update）] をクリックします。

ステップ 4 [アクション（Action）] については、[ローカル ソフトウェア アップデート パッケージのアップロード（Upload local software update package）] オプションボタンをクリックします。

ステップ 5 [ファイルの選択（Choose File）] をクリックします。

ステップ 6 パッケージを参照し、[アップロード（Upload）] をクリックします。

FMC で準備状況チェックを実行します。

FMC 準備状況チェックを実行するには、次の手順を使用します。

準備状況チェックでは、メジャーアップグレードとメンテナンスアップグレードの準備状況を評価します。準備状況チェックで不合格になると、問題を修正するまでアップグレードできません。準備状況チェックの実行に必要な時間は、モデルとデータベースのサイズによって異なります。準備状況チェックを行っている間は、手動で再起動またはシャットダウンしないでください。

始める前に

アップグレードパッケージを FMC にアップロードします。

ステップ 1 FMC で、**システム**（⚙）>**[更新（Updates）]** を選択します。

ステップ 2 [利用可能なアップデート（Available Updates）] で該当するアップグレード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て、FMC を選択します。

ステップ 3 [準備状況の確認（Check Readiness）] をクリックします。

メッセージセンターで準備状況チェックの進行状況をモニターできます。

次のタスク

システム（⚙）>**[更新（Updates）]** で [準備状況チェック（Readiness Checks）] をクリックすると、チェック進行中やチェック不合格など、アップグレード環境全体の準備状況チェックのステータスが表示されます。また、このページを使用して、不合格となった後にチェックを簡単に再実行することもできます。

FMC のアップグレード：スタンドアロン

この手順を使用して、スタンドアロンの FMC をアップグレードします。

⚠

注意 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。

始める前に

事前アップグレードのチェックリストを完了します。正常に展開され、通信が確立されていることを確認します。

ステップ 1 FMC で、**システム**（⚙）>**[更新（Updates）]** を選択します。

ステップ 2 [利用可能なアップデート（Available Updates）] で該当するアップグレード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て、FMC を選択します。

ステップ 3 [インストール（Install）] をクリックし、アップグレードして再起動することを確認します。

ログアウトするまで、メッセージセンターで事前チェックの進行状況をモニターできます。

ステップ 4 可能なときに、再度ログインします。

- メジャーアップグレードとメンテナンスアップグレード：アップグレードが完了する前にログインできます。アップグレードの進行状況をモニターし、アップグレードログとエラーメッセージを確認するために使用できるページが表示されます。アップグレードが完了し、システムが再起動すると再度ログアウトされます。リブート後に、再ログインしてください。
- パッチとホットフィックス：アップグレードと再起動が完了した後にログインできます。

ステップ 5 アップグレードが成功したことを確認します。

ログイン時にアップグレードの成功メッセージが表示されない場合は、**[ヘルプ（Help）]** > **[バージョン情報（About）]** を選択して、現在のソフトウェアのバージョン情報を表示します。

ステップ 6 侵入ルール（SRU/LSP）および脆弱性データベース（VDB）を更新します。

シスコ サポートおよびダウンロード サイト で利用可能なコンポーネントが現在実行中のバージョンより新しい場合は、新しいバージョンをインストールします。侵入ルールを更新する場合、ポリシーを自動的に再適用する必要はありません。後で適用します。

ステップ 7 アップグレード後に必要な構成変更があれば、実行します。

ステップ 8 管理対象デバイスに構成を再展開します。

FMC のアップグレード：ハイアベイラビリティ

ハイアベイラビリティ FMC を 1 つずつアップグレードします。同期を一時停止して、まずスタンバイをアップグレードしてから、アクティブにします。スタンバイのアップグレードが開始されると、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（およびパッチのアンインストール中）を除き、サポートされていません。

⚠

注意 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。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。

始める前に

両方のピアの事前アップグレードチェックリストを完了します。正常に展開され、通信が確立されていることを確認します。

ステップ 1 アクティブ状態の FMC で、同期を一時停止します。

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、[同期の一時停止（Pause Synchronization）] をクリックします。

ステップ 2 アップグレードパッケージをスタンバイにアップロードします。

FMC の高可用性では、FMC アップグレードパッケージを両方のピアにアップロードし、パッケージをスタンバイに転送する前に同期を一時停止する必要があります。同期の中断を制限するには、アップグレードの準備段階でパッケージをアクティブのピアに転送し、同期を一時停止した後に、実際のアップグレードプロセスの一環としてスタンバイのピアに転送します。

ステップ 3 ピアを一度に 1 つずつアップグレード：最初はスタンバイ、次はアクティブです。

「FMC のアップグレード：スタンドアロン （46 ページ）」の手順に従います。各ピア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、各ピアで次の手順を実行します。

a) **[システム（System）]** > **[更新（Updates）]** ページで、アップグレードをインストールします。
b) ログアウトするまで進行状況をモニターし、ログインできる状態になったら再度ログインします（これは 2 回行われる場合があります）。
c) アップグレードが成功したことを確認します。

ステップ 4 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。

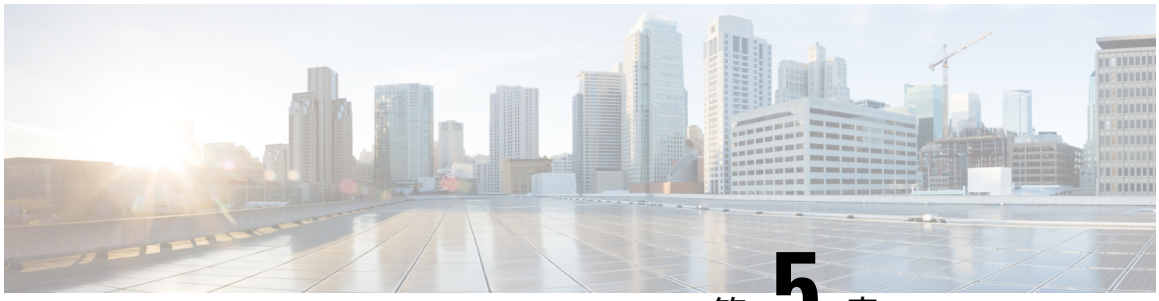
b) [ハイ アベイラビリティ（High Availability）] タブで、[アクティブにする（Make-Me-Active）] をクリックします。
c) 同期が再開し、その他の FMC がスタンバイ モードに切り替わるまで待ちます。

ステップ 5 侵入ルール（SRU/LSP）および脆弱性データベース（VDB）を更新します。

シスコ サポートおよびダウンロード サイト で利用可能なコンポーネントが現在実行中のバージョンより新しい場合は、新しいバージョンをインストールします。侵入ルールを更新する場合、ポリシーを自動的に再適用する必要はありません。後で適用します。

ステップ 6 アップグレード後に必要な構成変更があれば、実行します。

ステップ 7 管理対象デバイスに構成を再展開します。



第 5 章

FTD のアップグレード

この章では、バージョン 7.1 FMC を使用して Threat Defense をアップグレードする方法について説明します。FMC で別のバージョンを実行している場合、またはクラウド提供型の Management Center を使用している場合は、『対象読者 （1 ページ）』を参照してください。

FTD のアップグレード チェックリスト

計画と実現可能性

誤りを避けるには、注意深い計画と準備が役立ちます。

✓	アクション/チェック	詳細
	展開を評価します。	状況を理解することにより、目的を達成する方法を決定します。現在のバージョンとモデル情報に加えて、展開が高可用性/拡張性を実現するように設定されているかどうか、デバイスが IPS またはファイアウォールとして展開されているかどうかなどを確認します。

✓	アクション/チェック	詳細
	アップグレードパスを計画します。	これは、大規模展開、マルチホップアップグレード、またはオペレーティングシステムまたはホスティング環境をアップグレードする必要がある状況では特に重要です。次を参照してください。 • FMC のアップグレードパス （41 ページ） • FTD のアップグレードパス （55 ページ） • FXOS のアップグレードパス （76 ページ）
	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。	主要なアップグレードでは特に、アップグレードの前または後に、アップグレードにより重要な設定変更が発生することがあります。以下を参照してください。 • ソフトウェアのアップグレードガイドライン （23ページ）：重要なリリース固有のアップグレードガイドラインが記載されています。 • Cisco Secure Firewall Management Center の新機能（リリース別）：アップグレードに影響を与える新機能および廃止された機能が記載されています。現在のバージョンと対象バージョンの間にあるすべてのバージョンを確認してください。 • Cisco Firepower リリースノート：「*Open and Resolved Bugs*」の章に、アップグレードに影響を与えるバグが記載されています。現在のバージョンと対象バージョン間にあるすべてのバージョンのリリースノートを確認してください。：サポート契約がある場合は、Cisco バグ検索ツールを使用して最新のバグリストを取得できます。 • Cisco Firepower 4100/9300 FXOS リリースノート：Firepower 4100/9300 の FXOS アップグレードガイドラインが記載されています。

✓	アクション/チェック	詳細
	ウィザードまたは [システムの更新（System Updates）] ページのどちらを使用するかを決定します。	一部のチェックリスト項目では、Threat Defense アップグレードウィザードを使用した場合と [システムの更新（System Updates）] ページを使用した場合の比較が示されています。ウィザードでは、アップグレードするデバイスの選択、アップグレードパッケージのデバイスへのコピー、互換性と準備状況の確認など、アップグレードの重要な段階が順を追って説明されます。ウィザードを使用すると、アップグレードをより迅速かつ確実に、より少ないディスク容量で実行できます。 通常、ウィザードを使用してアップグレードすることをお勧めしますFTD。ただし、アップグレード完了後に復元が必要になる可能性がある場合は、**システム**（⚙）>**[更新（Updates）]** を使用します。また、[システムの更新（System Updates）] ページを使用して、パッケージを管理したり、FMC および古い従来型のデバイスをアップグレードする必要があります。
	アプライアンスへのアクセスを確認します。	デバイスは、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。アップグレードする前に、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。 デバイスを経由せずに FMC の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。
	帯域幅を確認します。	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。可能な場合は常に、アップグレードパッケージを事前にアップロードしてください。アップグレード時にアップグレードパケージをデバイスに転送する際の帯域幅が不十分な場合、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したりする可能性があります。 『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。

✓	アクション/チェック	詳細
	メンテナンス時間帯をスケジュールします。	影響が最小限になるようにメンテナンス時間帯をスケジュールします。トラフィックフローやインスペクションへの影響、およびアップグレードにかかる可能性がある時間を考慮してください。また、この時間帯で実行する必要があるタスクと、事前に実行できるタスクを検討します。参照先： • FXOS のアップグレードでのトラフィックフローとインスペクション （75 ページ） • 時間とディスク容量のテスト （32 ページ）

バックアップ

アップグレードの前後に、安全な遠隔地にバックアップし、正常に転送が行われることを確認することを強くお勧めします。

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

✓	アクション/チェック	詳細
	FTD をバックアップします。	サポートされている場合は、FMC を使用して FTD 構成をバックアップします。Firepower Management Center アドミニストレーション ガイドの「バックアップ/復元」の章を参照してください。 Firepower 9300 で FTD および ASA 論理デバイスが別のモジュールで実行されている場合、ASDM または ASA CLI を使用して、ASA 構成やその他の重要なファイルをバックアップしてください（特に ASA 構成の移行がある場合）。『Cisco ASA Series General Operations Configuration Guide』の「*Software and Configurations*」の章を参照してください。

✓	アクション/チェック	詳細
	Firepower 4100/9300 の FXOS をバックアップします。	Firepower Chassis Manager または FXOS CLI を使用して、論理デバイス設定およびプラットフォーム設定を含むシャーシ設定をエクスポートします。 詳細については、『Cisco Firepower 4100/9300 FXOS コンフィギュレーションガイド』の「コンフィギュレーションのインポート/エクスポート」を参照してください。

アップグレードパッケージ

アップグレードの前にアップグレードパッケージをシステムにアップロードすると、メンテナンス時間が短縮されます。

✓	アクション/チェック	詳細
	シスコからアップグレードパッケージをダウンロードして、FMC または内部 Web サーバーにアップロードします。	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（FTD のアップグレードパッケージのアップロード （62 ページ））で入手できます。 FMC を使用して直接ダウンロードを実行することもできます（）。 デバイスのアップグレードパッケージを FMC にアップロードするか、内部サーバーから取得するようにデバイスを設定します。 • [システム（System）] > [更新（Updates）] メニューを使用して FTD アップグレードパッケージを FMC にアップロードする （63 ページ） • [システム（System）] > [更新（Updates）] メニューを使用して FTD アップグレードパッケージを内部サーバーにアップロードする （64 ページ） Firepower 4100/9300 の場合、FXOS アップロード手順は FXOS アップグレード手順に含まれています。
	アップグレードパッケージをデバイスにコピーします。	FTD をアップグレードするには、アップグレードパッケージがデバイスに存在している必要があります。アップグレードの前にアップグレードパッケージをコピーすると、アップグレードのメンテナンス時間が短縮されます。 Threat Defense のアップグレードウィザードでは、アップグレードパッケージを必要なデバイスにコピーするように求められます。または、[システムの更新（System Updates）] ページを使用できます。

関連するアップグレード

オペレーティングシステムとホスティング環境のアップグレードはトラフィックフローとインスペクションに影響を与える可能性があるため、メンテナンス時間帯で実行してください。

✓	アクション/チェック	詳細
	仮想ホスティングをアップグレードします。	必要に応じて、ホスティング環境をアップグレードします。通常、古いバージョンの VMware を実行していて、メジャーアップグレードを実行している場合、アップグレードが必要です。
	Firepower 4100/9300 のファームウェアをアップグレードします。	最新のファームウェアを推奨します。Cisco Firepower 4100/9300 FXOS ファームウェア アップグレード ガイドを参照してください。
	Firepower 4100/9300 の FXOS をアップグレードします。	FXOS のアップグレードは通常、メジャーアップグレードの要件ですが、メンテナンスリリースやパッチの場合は要件になるのは非常にまれです。中断を最小限に抑えるには、FTD のハイアベイラビリティペアおよびシャーシ間クラスタの FXOS を一度に 1 つずつアップグレードします。 Firepower 4100/9300 の FXOS のアップグレード （73 ページ） を参照してください。

最終チェック

一連の最終チェックにより、ソフトウェアをアップグレードする準備が整います。

✓	アクション/チェック	詳細
	設定を確認します。	必要なアップグレード前の設定変更を行っていることを確認し、必要なアップグレード後の設定変更を行う準備をします。
	NTP 同期を確認します。	時刻の提供に使用している NTP サーバーとすべてのアプライアンスが同期していることを確認します。時刻のずれが 10 秒を超えている場合、ヘルスモニター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。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。 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。 • FTD：**show time** CLI コマンドを使用します。

✓	アクション/チェック	詳細
	設定を展開します。	アップグレードする前に設定を展開すると、失敗する可能性が減少します。展開により、トラフィックフローとインスペクションが影響を受ける可能性があります。FTDアップグレードのトラフィックフローとインスペクション（29ページ）を参照してください。
	準備状況チェックを実行します。	互換性と準備状況のチェックに合格すると、アップグレードが失敗する可能性が低くなります。 Threat Defense のアップグレードウィザードにより、準備状況チェックを実行するように求められます。または、[システムの更新（System Updates）]ページを使用できます[システム（System）] > [更新（Updates）] メニューを使用して FTD の準備状況チェックを実行する。
	のディスク容量を確認します。	準備状況チェックには、ディスク容量チェックが含まれます。空きディスク容量が十分でない場合、アップグレードは失敗します。 デバイスで使用可能なディスク容量を確認するには、**システム**（⚙） > **[モニタリング（Monitoring）]** > **[統計（Statistics）]**を選択してから、確認するデバイスを選択します。[ディスク使用率（Disk Usage）] で、[By Partition] の詳細を展開します。
	実行中のタスクを確認します。	重要なタスク（最終展開を含む）が完了していることを確認します。アップグレードの開始時に実行中のタスクは停止し、失敗したタスクとなり、再開できません。 バージョン 6.6.3+ からのアップグレードは、スケジュールされたタスクを自動的に延期します。アップグレード中に開始するようにスケジュールされたタスクは、アップグレード後の再起動の 5 分後に開始されます。これが起こらないようにするには（または以前のバージョンからアップグレードする場合）、アップグレード中に実行するようにスケジュールされているタスクを確認し、それらをキャンセルまたは延期します。

FTD のアップグレードパス

展開に一致するアップグレードパスを選択します。

顧客が展開した FMC はその管理対象デバイスと同じか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。

FXOS を使用しない FTD のアップグレードパス

この表は、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ない場合の FTD のアップグレードパスを示しています。これには、アプライアンスモードの Firepower 1000/2100 シリーズ、ASA-5500-X シリーズ、および ISA 3000 が含まれます。

現在の FTD/FMC のバージョンが対象のバージョンより後の日付にリリースされた場合、期待どおりにアップグレードできない可能性があります。このような場合、アップグレードはすぐに失敗し、2 つのバージョン間にデータストアの非互換性があることを説明するエラーが表示されます。現在のバージョンと対象のバージョンの両方のに関するリリースノートには、特定の制限が掲載されています。

表 *29 : FTD* の直接アップグレード

現在のバージョン	ターゲットバージョン
7.3	→ 以降の 7.3.x リリース
7.2	次のいずれかです。 → 7.3.x → 以降の 7.2.x リリース （注） バージョン 7.2.3 で導入された Firepower 1010E は、バージョン 7.3 ではサポートされません。サポートは今後のリリースで復帰予定です。
7.1	次のいずれかです。 → 7.3.x → 7.2.x → 以降の 7.1.x リリース

現在のバージョン	ターゲットバージョン
7.0 ASA 5508-X および 5516-X における最後のサポート。	次のいずれかです。 → 7.3.x → 7.2.x → 7.1.x → 以降の 7.0.x リリース （注） データストアの非互換性のため、 をバージョン 7.0.4 以降からバージョン 7.1.0 にアップグレードすることができません。バージョン 7.2 以降に直接アップグレードすることをお勧めします。 （注） クラウド提供型 Firewall Management Center は、バージョン 7.1 を実行している FTD デバイス、または任意のバージョンを実行している従来のデバイスを管理できません。クラウド管理の登録を解除するか、または無効にしない限り、クラウド管理対象デバイスはバージョン 7.0.x からバージョン 7.1 にアップグレードできません。バージョン 7.2 以降に直接アップグレードすることをお勧めします。
6.7	次のいずれかです。 → 7.2.x → 7.1.x → 7.0.x → 以降の 6.7.x リリース
6.6 ASA 5525-X、5545-X、5555-X における最後のサポート。	次のいずれかです。 → 7.2.x → 7.1.x → 7.0.x → 6.7.x → 任意の後続リリース 6.6.x

現在のバージョン	ターゲットバージョン
6.5	次のいずれかです。 → 7.1.x → 7.0.x → 6.7.x → 6.6.x
6.4 ASA 5515-X における最後のサポート。	次のいずれかです。 → 7.0.x → 6.7.x → 6.6.x → 6.5
6.3	次のいずれかです。 → 6.7.x → 6.6.x → 6.5 → 6.4
6.2.3 ASA 5506-X シリーズにおける最後のサポート。	次のいずれかです。 → 6.6.x → 6.5 → 6.4 → 6.3

FXOS を使用する FTD のアップグレードパス

Firepower 4100/9300 に搭載されている FTD のアップグレードパスを次の表に示します。

現在の FTD/FMC のバージョンが対象のバージョンより後の日付にリリースされた場合、期待どおりにアップグレードできない可能性があります。このような場合、アップグレードはすぐに失敗し、2 つのバージョン間にデータストアの非互換性があることを説明するエラーが表示されます。現在のバージョンと対象のバージョンの両方のに関するリリースノートには、特定の制限が掲載されています。

この表には、シスコにより特別に認定されたバージョンの組み合わせのみが掲載されています。最初にFXOSをアップグレードするため、サポートされているが推奨されていない組み合わせを一時的に実行します。オペレーティングシステムはデバイスソフトウェアの「前」に

アップグレードします。FXOSをアップグレードしても、論理デバイスやアプリケーションインスタンスとの互換性ガ失われないようにしてください。 最小限のビルドおよびその他の詳細な互換性情報については、Cisco Secure Firewall Threat Defense 互換性ガイド を参照してください。

表 *30 : Firepower 4100/9300* における *FTD* の直接アップグレード

現在のバージョン	対象のバージョン
Threat Defense 7.3 を搭載した FXOS 2.13	→ FXOS 2.13 と任意の後続リリース Threat Defense 7.3.x
Threat Defense 7.2 を搭載した FXOS 2.12 Firepower 4110、4120、4140、4150 の最後のサポート。 SM-24、SM-36、SM-44 モジュールを搭載した Firepower 9300 の最後のサポート。	次のいずれかです。 → FXOS 2.13 と Threat Defense 7.3.x → FXOS 2.12 と任意の後続リリース Threat Defense 7.2.x
Threat Defense 7.1 を搭載した FXOS 2.11.1	次のいずれかです。 → FXOS 2.13 と Threat Defense 7.3.x → FXOS 2.12 と Threat Defense 7.2.x → FXOS 2.11.1 と任意の後続リリース Threat Defense 7.1.x

現在のバージョン	対象のバージョン
Threat Defense 7.0 を搭載した FXOS 2.10.1	次のいずれかです。 → FXOS 2.13 と Threat Defense 7.3.x → FXOS 2.12 と Threat Defense 7.2.x → FXOS 2.11.1 と Threat Defense 7.1.x → FXOS 2.10.1 と任意の後続リリース Threat Defense 7.0.x （注） データストアの非互換性のため、をバージョン 7.0.4 以降からバージョン 7.1.0 にアップグレードすることができません。バージョン 7.2 以降に直接アップグレードすることをお勧めします。 （注） クラウド提供型 Firewall Management Center は、バージョン 7.1 を実行している FTD デバイス、または任意のバージョンを実行している従来のデバイスを管理できません。クラウド管理の登録を解除するか、または無効にしない限り、クラウド管理対象デバイスはバージョン 7.0.x からバージョン 7.1 にアップグレードできません。バージョン 7.2 以降に直接アップグレードすることをお勧めします。
Threat Defense 6.7 を搭載した FXOS 2.9.1	次のいずれかです。 → FXOS 2.12 と Threat Defense 7.2.x → FXOS 2.11.1 と Threat Defense 7.1.x → FXOS 2.10.1 と Threat Defense 7.0.x → FXOS 2.9.1 と任意の後続リリース Threat Defense 6.7.x
Threat Defense 6.6 を搭載した FXOS 2.8.1	次のいずれかです。 → FXOS 2.12 と Threat Defense 7.2.x → FXOS 2.11.1 と Threat Defense 7.1.x → FXOS 2.10.1 と Threat Defense 7.0.x → FXOS 2.9.1 と Threat Defense 6.7.x → FXOS 2.8.1 と任意の後続リリース Threat Defense 6.6.x

現在のバージョン	対象のバージョン
Threat Defense 6.5 を搭載した FXOS 2.7.1	次のいずれかです。 → FXOS 2.11.1 と Threat Defense 7.1.x → FXOS 2.10.1 と Threat Defense 7.0.x → FXOS 2.9.1 と Threat Defense 6.7.x → FXOS 2.8.1 と Threat Defense 6.6.x
Threat Defense 6.4 を搭載した FXOS 2.6.1	次のいずれかです。 → FXOS 2.10.1 と Threat Defense 7.0.x → FXOS 2.9.1 と Threat Defense 6.7.x → FXOS 2.8.1 と Threat Defense 6.6.x → Threat Defense 6.5 を搭載した FXOS 2.7.1
Threat Defense 6.3 を搭載した FXOS 2.4.1	次のいずれかです。 → FXOS 2.9.1 と Threat Defense 6.7.x → FXOS 2.8.1 と Threat Defense 6.6.x → Threat Defense 6.5 を搭載した FXOS 2.7.1 → Threat Defense 6.4 を搭載した FXOS 2.6.1
Threat Defense 6.2.3 を搭載した FXOS 2.3.1	次のいずれかです。 → FXOS 2.8.1 と Threat Defense 6.6.x → Threat Defense 6.5 を搭載した FXOS 2.7.1 → Threat Defense 6.4 を搭載した FXOS 2.6.1 → Threat Defense 6.3 を搭載した FXOS 2.4.1

FTD ハイアベイラビリティ/スケーラビリティ と FXOS のアップグレード順序

高可用性や拡張性を導入する場合でも、各シャーシのFXOSを個別にアップグレードします。中断を最小限に抑えるには、1 つずつシャーシの FXOS をアップグレードします。FTD のアップグレードの場合、グループ化されたデバイスが 1 つずつ自動的にアップグレードされます。

表 *31 : Firepower 4100/9300* に搭載された *FXOS* と *Threat Defense* のアップグレード順序

FTD の導入	アップグレード順序
スタンドアロン	1. FXOS をアップグレードします。 2. FTD をアップグレードします。
ハイ アベイラビリティ	FTD をアップグレードする前に、両方のシャーシで FTD をアップグレードします。中断を最小限に抑えるため、スタンバイは常にアップグレードします。 1. スタンバイデバイスを備えたシャーシの FXOS をアップグレードします。 2. ロールを切り替えます。 3. 新しいスタンバイデバイスを備えたシャーシの FXOS をアップグレードします。 4. FTD をアップグレードします。
シャーシ内クラスタ（同じシャーシ上のユニット）	1. FXOS をアップグレードします。 2. FTD をアップグレードします。
シャーシ内クラスタ（異なるシャーシ上のユニット）	FTD をアップグレードする前に、すべてのシャーシの FXOS をアップグレードします。中断を最小限に抑えるため、すべてデータユニットのシャーシを常にアップグレードします。 1. すべてデータユニットのシャーシの FXOS をアップグレードします。 2. 制御モジュールをアップグレードしたシャーシに切り替えます。 3. 残りのシャーシの FXOS をアップグレードします。 4. FTD をアップグレードします。

FTD のアップグレードパッケージのアップロード

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（https://www.cisco.com/go/ftd-software）で入手できます。

ファミリまたはシリーズのすべてのモデルに同じアップグレードパッケージを使用します。適切なソフトウェアを見つけるには、使用しているモデルを シスコ サポートおよびダウンロード サイト で選択または検索し、適切なバージョンのソフトウェアのダウンロードページを参

照します。使用可能なアップグレードパッケージは、インストールパッケージ、ホットフィックス、およびその他の該当するダウンロードとともに表示されます。アップグレードパッケージのファイル名には、プラットフォーム、パッケージタイプ（アップグレード、パッチ、ホットフィックス）、ソフトウェアバージョン、およびビルドが反映されています。

アップグレードパッケージは署名付きで、次の表に示すように末尾が .sh.REL.tar。署名付きのアップグレード パッケージは解凍しないでください。

表 *32*：ソフトウェア アップ グレード パッケージ

プラットフォーム（**Platform**）	アップグレードパッケージ
Firepower 1000 シリーズ	Cisco_FTD_SSP-FP1K_Upgrade-7.1-999.sh.REL.tar
Firepower 2100 シリーズ	Cisco_FTD_SSP-FP2K_Upgrade-7.1-999.sh.REL.tar
Secure Firewall 3100 シリーズ	Cisco_FTD_SSP-FP3K_Upgrade-7.1-999.sh.REL.tar
Firepower 4100/9300	Cisco_FTD_SSP_Upgrade-7.1-999.sh.REL.tar
FTDv	Cisco_FTD_Upgrade-7.1-999.sh.REL.tar
FTD を使用した ISA 3000	Cisco_FTD_Upgrade-7.1-999.sh.REL.tar

ヒント　一部のアップグレードパッケージは、リリースが手動でダウンロードできるようになってからしばらくすると、直接ダウンロードできるようになります。遅延の長さは、リリースの種類、リリースの選択、およびその他の要因によって異なります。FMC がインターネットにアクセスできる場合は、**システム**（⚙） > **[更新（Updates）]** で [アップデートのダウンロード（Download Updates）] をクリックして、FMC とすべての管理対象デバイス向けの最新の VDB、最新のメンテナンスリリース、および最新の重要パッチをすぐにダウンロードできます。

[システム（System）]>[更新（Updates）] メニューを使用して FTD アップグレードパッケージを FMC にアップロードする

アップグレードパッケージは、署名付きの tar アーカイブ（.tar）です。署名付きのパッケージをアップロードした後、パッケージを検証するための [システムの更新（System Updates）] ページのロードに数分かかることがあります。表示を迅速化するには、不要なアップグレードパッケージを削除してください。署名付きのパッケージは解凍しないでください。

ステップ 1　FMC で、**システム**（⚙） > **[更新（Updates）]** を選択します。

ステップ 2　[更新のアップロード（Upload Update）] をクリックします。

ステップ 3 [アクション（Action）] については、[ローカル ソフトウェア アップデート パッケージのアップロード（Upload local software update package）] オプションボタンをクリックします。

ステップ 4 [ファイルの選択（Choose File）] をクリックします。

ステップ 5 パッケージを参照し、[アップロード（Upload）] をクリックします。

ステップ 6 （オプション）アップグレードパッケージを管理対象デバイスにコピーします。

復元を有効にする必要がなく、FTDアップグレードウィザードを使用する予定の場合、パッケージをコピーするように求められます。復元を有効にするため、[システムの更新（System Updates）] ページを使用してアップグレードする場合は、次のように、アップグレードパッケージを今すぐにデバイスにコピーすることを推奨します。

a) コピーするアップグレードパッケージの横にある [アップデートのプッシュまたはステージ（Push or Stage Update）] アイコンをクリックします。

b) 宛先デバイスを選択します。

アップグレード パッケージをプッシュするデバイスがリストに表示されない場合は、間違ったアップグレード パッケージを選択しています。

c) [プッシュ（Push）] をクリックします。

[システム（System）]>[更新（Updates）]メニューを使用してFTDアップグレードパッケージを内部サーバーにアップロードする

この手順を使用して、FMC からではなく、独自の内部 Web サーバーからアップグレードパッケージを取得するように FTD デバイスを設定します。これは、FMC とそのデバイスの間の帯域幅が制限されている場合に特に役立ちます。また、FMC 上の容量も節約できます。

この機能を設定するには、Webサーバーのアップグレードパッケージの場所にポインタ（URL）を保存します。アップグレードプロセスでは、FMC ではなく Web サーバーからアップグレードパッケージが取得されます。または、アップグレードする前に、FMC のプッシュ機能を使用してパッケージをコピーすることもできます。

各アップグレードパッケージに対して、この手順を繰り返します。アップグレードパッケージごとに、1 つの場所のみを設定できます。

始める前に

デバイスがアクセスできる内部 Web サーバーにアップグレードパッケージをコピーします。セキュア Webサーバー（HTTPS）の場合は、サーバーのデジタル証明書（PEM 形式）を取得します。サーバーの管理者から証明書を取得できるようにする必要があります。また、ブラウザまたは OpenSSL などのツールを使用して、サーバーの証明書の詳細を表示したり、証明書をエクスポートまたはコピーしたりすることもできます。

ステップ 1 FMC で、**システム**（⚙）> **[更新（Updates）]** を選択します。

ステップ 2 [更新のアップロード（Upload Update）] をクリックします。

何もアップロードしない場合でも、このオプションを選択します。次のページに、URL の入力を求めるプロンプトが表示されます。

ステップ 3 **アクション**については、**[ローカルソフトウェアアップデートパッケージのアップロード（Upload local software update package）]** オプション ボタンをクリックします。

ステップ 4 アップグレードパッケージの**送信元 URL** を入力します。

次の例のように、プロトコル（HTTP/HTTPS）とフルパスを提供します。

```
https://internal_web_server/upgrade_package.sh.REL.tar
```

アップグレードパッケージのファイル名には、プラットフォーム、パッケージタイプ（アップグレード、パッチ、ホットフィックス）、およびアップグレードするソフトウェアのバージョンが反映されています。正しいファイル名を入力したことを確認します。

ステップ 5 HTTPS サーバーの場合は、**CA 証明書**を提供します。

これは、以前取得したサーバーのデジタル証明書です。テキストブロック全体（BEGIN CERTIFICATE 行と END CERTIFICATE行を含む）をコピーして貼り付けます。

ステップ 6 **[保存（Save）]** をクリックします。

場所が保存されます。アップロードされたアップグレードパッケージとアップグレードパッケージの URL はまとめてリストされますが、明確にラベル付けされます。

ステップ 7 （オプション）アップグレードパッケージを管理対象デバイスにコピーします。

復元を有効にする必要がなく、FTDアップグレードウィザードを使用する予定の場合、パッケージをコピーするように求められます。復元を有効にするため、[システムの更新（System Updates）]ページを使用してアップグレードする場合は、次のように、アップグレードパッケージを今すぐにデバイスにコピーすることを推奨します。

a) コピーするアップグレードパッケージの横にある [アップデートのプッシュまたはステージ（Push or Stage Update）] アイコンをクリックします。

b) 宛先デバイスを選択します。

アップグレード パッケージをプッシュするデバイスがリストに表示されない場合は、間違ったアップグレード パッケージを選択しています。

c) [プッシュ（Push）] をクリックします。

ウィザードを使用した FTD のアップグレード（復元を無効化）

この手順を使用すると、ウィザードを使用して FTD をアップグレードできます。

続行すると、選択したデバイスに関する基本情報と、現在のアップグレード関連のステータスが表示されます。表示内容には、アップグレードできない理由が含まれます。あるデバイスが

ウィザードの 1 つの段階に「合格」しない場合、そのデバイスは次の段階には表示されません。

ウィザードから移動しても進行状況は保持されます。他のユーザーは、の新しいアップグレードワークフローを開始できません（例外：CAC でログインしている場合、ログアウトしてから 24 時間後に進行状況がクリアされます）。他のユーザーのワークフローをリセットする必要がある場合は、管理者アクセス権が必要です。ユーザーを削除または非アクティブ化するか、ユーザーロールを更新して、ユーザーに付与された権限を無効にできます**[デバイス（Devices）] > [デバイスのアップグレード（Device Upgrade）]**。

ハイアベイラビリティ対応の FMC の間では、ワークフローも Threat Defense のアップグレードパッケージも同期されないので注意してください。フェールオーバーが発生した場合は、新しいアクティブな FMC でワークフローを再作成する必要があります。これには、FMC へのアップグレードパッケージのアップロードと準備状況チェックの実行が含まれます（デバイスにコピー済みのアップグレードパッケージは削除されませんが、 FMC にアップロードパッケージまたはパッケージの格納場所へのポインタが必要です）。

注意 アップグレード中は、設定を変更または展開しないでください。システムが非アクティブに見えても、手動で再起動またはシャットダウンしないでください。ほとんどの場合、進行中のアップグレードを再開しないでください。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応答しないアップグレード （28 ページ） を参照してください。

始める前に

- この手順を使用するかどうかを決定します。

  通常、ウィザードを使用してアップグレードすることをお勧めしますFTD。ただし、アップグレード完了後に復元が必要になる可能性がある場合は、**システム**（⚙） > **[更新（Updates）]** を使用します。また、[システムの更新（System Updates）] ページを使用して、パッケージを管理したり、FMC および古い従来型のデバイスをアップグレードする必要があります。

- 事前アップグレードのチェックリストを完了します。正常に展開され、通信が確立されていることを確認します。

ワークフローを開始します。

ステップ 1 **[デバイス（Devices）] > [デバイス管理（Device Management）]** を選択します。

アップグレード対象のデバイスを選択して、アップグレードパッケージをコピーします。

ステップ 2 デバイスの選択内容を確認します。

追加のデバイスを選択するには、[デバイス管理（Device Management）] ページに戻ります。進行状況は失われません。デバイスを削除するには、[リセット（Reset）] をクリックしてデバイスの選択をクリアし、最初からやり直します。

ステップ 3 アップグレードするデバイスを選択します。

複数のデバイスを同時にアップグレードできます。デバイスクラスタとハイアベイラビリティペアのメンバーは、同時にアップグレードする必要があります。

重要 パフォーマンスの問題により、デバイスをバージョン 6.6.x 以前にアップグレードする場合は（バージョン 6.6.x からのアップグレードではなく）、同時にアップグレードするデバイスは 5 つまでにすることを強くお勧めします。

ステップ 4 [Select Action] または [Select Bulk Action] メニューから、[Upgrade Firepower Software] を選択します。

デバイスのアップグレードウィザードが表示され、選択したデバイスの数が示されます。また、対象のバージョンを選択するように求められます。このページには、左側の [デバイスの選択（Device Selection）] と右側の [デバイスの詳細（Device Details）] の 2 つのペインがあります。[デバイスの選択（Device Selection）] ペインでデバイスリンク（「4 つのデバイス（4 devices）」など）をクリックして、[デバイスの詳細（Device Details）] を表示します。

進行中のアップグレードワークフローがすでにある場合は、最初にデバイスをマージする（新しく選択したデバイスを以前に選択したデバイスに追加して続行する）か、リセットする（以前の選択を破棄し、新しく選択したデバイスのみを使用する）必要があることに注意してください。

ステップ 5 デバイスの選択内容を確認します。

追加のデバイスを選択するには、[デバイス管理（Device Management）] ページに戻ります。進行状況は失われません。デバイスを削除するには、[リセット（Reset）] をクリックしてデバイスの選択をクリアし、最初からやり直します。

ステップ 6 [アップグレード先（Upgrade to）] メニューから、対象のバージョンを選択します。

システムは、選択したデバイスのどれをそのバージョンにアップグレードできるかを決定します。対象外のデバイスがある場合は、デバイスのリンクをクリックして理由を確認できます。不適格なデバイスを削除する必要はありません。自動的にアップグレードの対象から除外されます。

[Upgrade to] メニューの選択肢は、システムで利用可能なデバイスのアップグレードパッケージに対応していることに注意してください。対象のバージョンが表示されない場合は、**システム**（⚙）> **[更新（Updates）]** に移動し、正しいアップグレードパッケージの場所をアップロードまたは指定します。異なるデバイスモデルをアップグレードするために複数のアップグレードパッケージが必要な場合は、次の手順に進む前に、必要なすべてのアップグレードパッケージについてこれを行います。

ステップ 7 アップグレードパッケージが必要なすべてのデバイスについて、[アップグレードパッケージのコピー（Copy Upgrade Packages）] をクリックして、選択内容を確認します。

FTD をアップグレードするには、アップグレードパッケージがデバイスに存在している必要があります。アップグレードの前にアップグレードパッケージをコピーすると、アップグレードのメンテナンス時間が短縮されます。

ステップ 8 [次へ（Next）] をクリックします。

互換性、準備状況、およびその他の最終チェックを実行します。

ステップ 9 準備状況チェックに合格する必要があるすべてのデバイスについて、[Run Readiness Check] をクリックして、選択を確認します。

[互換性と準備状況のチェックに合格することを必須にする（Require passing compatibility and readiness checks option）] オプションを無効にするとチェックをスキップできますが、推奨しません。すべてのチェックに合格すると、アップグレードが失敗する可能性が大幅に減少します。準備状況チェックの実行中は、デバイスに変更を展開したり、手動で再起動またはシャットダウンしたりしないでください。デバイスが準備状況チェックに失敗した場合は、問題を修正して、準備状況チェックを再度実行してください。準備状況チェックの結果、解決できない問題が見つかった場合は、アップグレードを開始しないでください。代わりに、Cisco TAC にお問い合わせください。

互換性チェックは自動的に行われることに注意してください。たとえば、FXOS をアップグレードする必要がある場合や、管理対象デバイスに展開する必要がある場合は、ただちにシステムアラートが表示されます。

ステップ 10 アップグレード前の最終的なチェックを実行します。

アップグレード前のチェックリストを再確認します。関連するすべてのタスク、特に最終チェックを完了していることを確認してください。

ステップ 11 必要に応じて、**[デバイス（Devices）] > [デバイスのアップグレード（Device Upgrade）]** に戻ります。

ステップ 12 [次へ（Next）] をクリックします。

デバイスをアップグレードします。

ステップ 13 デバイスの選択と対象のバージョンを確認します。

ステップ 14 （オプション）クラスタ化されたデバイスのアップグレード順序を変更します。

クラスタのデバイスの詳細を表示し、[アップグレード順序の変更（Change Upgrade Order）] をクリックします。制御ユニットは常に最後にアップグレードされます。これを変更することはできません。

ステップ 15 ロールバックオプションを選択します。

メジャーおよびメンテナンスアップグレードの場合、**アップグレードに失敗すると自動的にキャンセルされ、1つ前のバージョンにロールバックされます。**オプションを有効にすると、アップグレードが失敗した場合、デバイスは自動的にアップグレード前の状態に戻ります。失敗したアップグレードを手動でキャンセルまたは再試行できるようにする場合は、このオプションを無効にします。高可用性またはクラスタ展開では、自動キャンセルは各デバイスに個別に適用されます。つまり、1つのデバイスでアップグレードが失敗した場合、そのデバイスだけが元に戻ります。

このオプションは、パッチではサポートされていません。

ステップ 16 [Start Upgrade] をクリックし、アップグレードして、デバイスを再起動することを確認します。

メッセージセンターでアップグレードの進行状況をモニターできます。進行状況の詳細を確認するには、[デバイス管理（Device Management）] ページの [アップグレード（Upgrade）] タブ、およびメッセージセンターからアクセスできる [アップグレードステータス（Upgrade Status）] ポップアップを使用します。アップグレード中のトラフィック処理については、「FTD アップグレードのトラフィックフローとインスペクション （29 ページ）」のを参照してください。。

アップグレード中にデバイスが 2 回再起動する場合があります。これは想定されている動作です。

成功を確認し、アップグレード後のタスクを完了します。

ステップ 17 成功したことを確認します。

アップグレードが完了したら、**[デバイス（Devices）] > [デバイス管理（Device Management）]** を選択し、アップグレードした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。

ステップ 18 （オプション）高可用性および拡張性の展開では、デバイスのロールを調べます。

アップグレードプロセスは、常にスタンバイユニットまたはデータノードをアップグレードするようにデバイスのロールを切り替えます。デバイスをアップグレード前のロールに戻すことはありません。特定のデバイスに優先するロールがある場合は、それらの変更を今すぐ行ってください。

ステップ 19 侵入ルール（SRU/LSP）および脆弱性データベース（VDB）を更新します。

シスコサポートおよびダウンロードサイトで利用可能なコンポーネントが現在実行中のバージョンより新しい場合は、新しいバージョンをインストールします。侵入ルールを更新する場合、ポリシーを自動的に再適用する必要はありません。後で適用します。

ステップ 20 アップグレード後に必要な構成変更があれば、実行します。

ステップ 21 アップグレードしたデバイスに構成を再度展開します。

次のタスク

（オプション）**[完了（Finish）]**[アップグレード情報のクリア（Clear Upgrade Information）] をクリックして、ウィザードをクリアします。これを行うまで、ページには、実行したばかりのアップグレードに関する詳細が引き続き表示されます。

[システム（System）] > [更新（Updates）] メニューを使用した FTD のアップグレード（復元を有効化）

この手順を使用すると、[システムの更新（System Updates）] ページから FTD をアップグレードできます。

⚠

注意 アップグレード中は、設定を変更または展開しないでください。システムが非アクティブに見えても、手動で再起動またはシャットダウンしないでください。ほとんどの場合、進行中のアップグレードを再開しないでください。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応答しないアップグレード （28 ページ） を参照してください。

始める前に

- この手順を使用するかどうかを決定します。

  アップグレード完了後に元に戻す必要が生じる可能性がある場合は、**システム**（⚙）**>[更新（Updates）]** を使用して FTD をアップグレードします。これは、[アップグレードの成

功後に復元を有効にする（Enable revert after successful upgrade）] オプション（）を設定する唯一の方法であり、Threat Defense のアップグレードウィザードを使用するという通常の推奨事項とは対照的です。

- 事前アップグレードのチェックリストを完了します。正常に展開され、通信が確立されていることを確認します。

ステップ 1 FMC で、**システム**（⚙）> **[更新（Updates）]** を選択します。

ステップ 2 [利用可能なアップデート（Available Updates）] で該当するアップグレード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ます。

アップグレードするデバイスがリストに表示されない場合は、間違ったアップグレード パッケージを選択しています。

対象デバイスのリストが、アップグレード前の互換性チェックの結果とともに表示されます。アップグレードの失敗の原因となる明らかな問題がある場合、この事前チェックによってアップグレードが防止されます。

ステップ 3 チェックするデバイスを選択し、[準備状況の確認（Check Readiness）] をクリックします。

準備状況チェックでは、メジャーアップグレードとメンテナンスアップグレードの準備状況を評価します。 準備状況チェックの実行に必要な時間は、モデルによって異なります。 準備状況チェックを行っている間は、手動で再起動またはシャットダウンしないでください。

このページの [準備状況チェック（Readiness Checks）] では、チェック進行中やチェック不合格など、アップグレード環境全体のチェックステータスを確認できます。また、このページを使用して、不合格となった後にチェックを簡単に再実行することもできます。メッセージセンターで準備状況チェックの進行状況をモニターすることもできます。

他の適格なデバイスを選択できない場合は、互換性チェックに合格したことを確認してください。デバイスが準備チェックで不合格になった場合は、アップグレードする前に問題を修正してください。

ステップ 4 アップグレードするデバイスを選択します。

複数のデバイスで同じアップグレードパッケージを使用する場合にのみ、複数のデバイスを同時にアップグレードできます。デバイス クラスタとハイ アベイラビリティ ペアのメンバーは、同時にアップグレードする必要があります。

重要 [システムの更新（System Update）] ページから同時にアップグレードするデバイスは 5 台までにすることを強く推奨します。選択したすべてのデバイスがそのプロセスを完了するまで、アップグレードを停止することはできません。いずれかのデバイスのアップグレードに問題がある場合、問題を解決する前に、すべてのデバイスのアップグレードを完了する必要があります。

ステップ 5 アップグレードオプションを選択します。

メジャーアップグレードおよびメンテナンスアップグレードでは、次のことを行えます。

- **アップグレードの失敗時に自動的にキャンセルし、前のバージョンにロールバックする**：アップグレードに失敗すると、デバイスは自動的にアップグレード前の状態に戻ります。失敗したアップグ

レードを手動でキャンセルまたは再試行できるようにする場合は、このオプションを無効にします。高可用性またはクラスタ展開では、自動キャンセルは各デバイスに個別に適用されます。つまり、1つのデバイスでアップグレードが失敗した場合、そのデバイスだけが元に戻ります。

- **アップグレード成功後の復元を可能にする**：アップグレードが成功してから 30 日間、デバイスをアップグレード前の状態に戻すことができます。

これらのオプションは、パッチではサポートされていません。

ステップ 6 [Install] をクリックし、アップグレードして、デバイスを再起動することを確認します。

メッセージセンターでアップグレードの進行状況をモニタします。アップグレード中のトラフィック処理については、「FTD アップグレードのトラフィックフローとインスペクション （29 ページ）」のを参照してください。。

アップグレード中にデバイスが 2 回再起動する場合があります。これは想定されている動作です。

ステップ 7 成功したことを確認します。

アップグレードが完了したら、**[デバイス（Devices）] > [デバイス管理（Device Management）]** を選択し、アップグレードした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。

ステップ 8 （オプション）高可用性および拡張性の展開では、デバイスのロールを調べます。

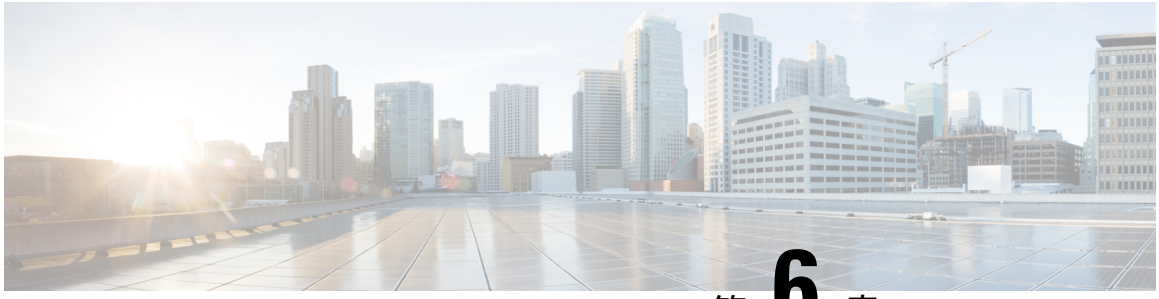
アップグレードプロセスは、常にスタンバイユニットまたはデータノードをアップグレードするようにデバイスのロールを切り替えます。デバイスをアップグレード前のロールに戻すことはありません。特定のデバイスに優先するロールがある場合は、それらの変更を今すぐ行ってください。

ステップ 9 侵入ルール（SRU/LSP）および脆弱性データベース（VDB）を更新します。

シスコ サポートおよびダウンロードサイトで利用可能なコンポーネントが現在実行中のバージョンより新しい場合は、新しいバージョンをインストールします。侵入ルールを更新する場合、ポリシーを自動的に再適用する必要はありません。後で適用します。

ステップ 10 アップグレード後に必要な構成変更があれば、実行します。

ステップ 11 アップグレードしたデバイスに構成を再度展開します。



第 6 章

Firepower 4100/9300 の FXOS のアップグレード

Firepower 4100/9300 の場合、FTD のメジャーアップグレードには FXOS のアップグレードも必要です。

FTD のメジャーバージョンには特別に認定および推奨されている付随の FXOS バージョンがあります。シスコではこれらの組み合わせの拡張テストを実施するため、可能な限りこれらの組み合わせを使用してください。メンテナンスリリースとパッチで FXOS のアップグレードが必要になることはほとんどありませんが、最新の FXOS ビルドにアップグレードして、解決済みの問題を有効に活用できます。

また、最新のファームウェアを推奨します（『Cisco Firepower 4100/9300 FXOS ファームウェア アップグレード ガイド』を参照）。

FXOS のアップグレードパッケージ

FXOS イメージとファームウェアのアップデート版は 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。

- Firepower 4100 シリーズ：http://www.cisco.com/go/firepower4100-software
- Firepower 9300：http://www.cisco.com/go/firepower9300-software

正しい FXOS イメージを見つけるには、デバイスモデルを選択または検索し、対象の FXOS バージョンとビルドの *Firepower Extensible Operating System* のダウンロードページを参照します。FXOSイメージは、リカバリパッケージおよびMIBパッケージとともにリストされていま

す。ファームウェアをアップグレードする必要がある場合、[すべてのリリース（All Releases）] > [ファームウェア（Firmware）] を選択すると、アップグレードパッケージが表示されます。

パッケージの種類は次のとおりです。

- Firepower 4100/9300 FXOS イメージ：fxos-k9.*fxos_version*.SPA
- Firepower 4100 シリーズ ファームウェア：fxos-k9-fpr4k-firmware.*firmware_version*.SPA
- Firepower 9300 ファームウェア：fxos-k9-fpr9k-firmware.*firmware_version*.SPA

FXOS のアップグレードガイドライン

重要なリリース固有のアップグレードガイドライン、新機能および廃止された機能、未解決のバグおよび解決済みのバグについては、Cisco Firepower 4100/9300 FXOS リリースノート を参照してください。

FTD をアップグレードするために必要な FXOS の最小バージョン

バージョン 7.1 を実行するために必要な FXOS の最小バージョンは、FXOS 2.11.1.154 です。

FXOS をアップグレードするために必要な FXOS の最小バージョン

FXOS 2.2.2 から、それ以降の任意の FXOS バージョンにアップグレードできます。

FXOS アップグレードの所要時間

FXOS のアップグレードには最長 45 分かかることがあり、トラフィックフローやインスペクションに影響を与える場合があります。詳細については、FXOS のアップグレードでのトラフィックフローとインスペクション （75 ページ）を参照してください。

FXOS と FTD ハイアベイラビリティ/スケーラビリティのアップグレード順序

高可用性や拡張性を導入する場合でも、各シャーシの FXOS を個別にアップグレードします。中断を最小限に抑えるには、1 つずつシャーシの FXOS をアップグレードします。FTD のアップグレードの場合、グループ化されたデバイスが 1 つずつ自動的にアップグレードされます。詳細については、FXOS と FTD ハイアベイラビリティ/スケーラビリティのアップグレード順序 （81 ページ）を参照してください。

FXOS ならびに FTD と ASA 論理デバイスのアップグレード

Firepower 9300 に FTD および ASA 論理デバイスが設定されている場合は、この章の手順を使用して FXOS と FTD をアップグレードします。FXOS をアップグレードしても、どちらのタイプの論理デバイスとの互換性も失われないことを確認する必要があります（FXOS ならびに FTD と ASA のアップグレードパス （78 ページ） を参照）。

ASA のアップグレード手順については、Cisco Secure Firewall ASA アップグレードガイド を参照してください。

論理デバイスを搭載していない FXOS のアップグレード

論理デバイスやコンテナインスタンスが設定されていない場合は、この章の手順を使用して、スタンドアロン型の FTD デバイスの FXOS をアップグレードします。論理デバイスに関する指示は無視してください。または、必要なFXOSバージョンへのシャーシの完全な再イメージ化を実行します。

FXOS のアップグレードでのトラフィックフローとインスペクション

FXOS をアップグレードするとシャーシが再起動します。ハイアベイラビリティやスケーラビリティ環境でも、各シャーシのFXOSを個別にアップグレードします。中断を最小限に抑えるには、1 つずつシャーシをアップグレードします。詳細については、「FXOS と FTD ハイアベイラビリティ/スケーラビリティのアップグレード順序 （81 ページ）」を参照してください。

表 *33 :* トラフィックフローとインスペクション：*FXOS* のアップグレード

FTD の導入	トラフィックの挙動	メソッド
スタンドアロン	廃棄	—
高可用性	影響なし。	**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。
	1 つのピアがオンラインになるまでドロップされる。	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。
シャーシ間クラスタ	影響なし。	**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。
	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。	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。
シャーシ内クラスタ（FirePOWER 9300 のみ）	検査なしで受け渡される。	ハードウェアバイパス有効：[Bypass: Standby] または [Bypass-Force]。
	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無効：[Bypass: Disabled]。
	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。

FXOS のアップグレードパス

展開に一致するアップグレードパスを選択します。

FTD を使用する FXOS のアップグレードパス

Firepower 4100/9300 に搭載されている FTD のアップグレードパスを次の表に示します。

現在の FTD/FMC のバージョンが対象のバージョンより後の日付にリリースされた場合、期待どおりにアップグレードできない可能性があります。このような場合、アップグレードはすぐに失敗し、2 つのバージョン間にデータストアの非互換性があることを説明するエラーが表示されます。現在のバージョンと対象のバージョンの両方のに関するリリースノートには、特定の制限が掲載されています。

この表には、シスコにより特別に認定されたバージョンの組み合わせのみが掲載されています。最初にFXOSをアップグレードするため、サポートされているが推奨されていない組み合わせを一時的に実行します。オペレーティングシステムはデバイスソフトウェアの「前」にアップグレードします。FXOSをアップグレードしても、論理デバイスやアプリケーションインスタンスとの互換性ガ失われないようにしてください。 最小限のビルドおよびその他の詳細な互換性情報については、Cisco Secure Firewall Threat Defense 互換性ガイド を参照してください。

表 *34 : Firepower 4100/9300* における *FTD* の直接アップグレード

現在のバージョン	対象のバージョン
Threat Defense 7.3 を搭載した FXOS 2.13	→ FXOS 2.13 と任意の後続リリース Threat Defense 7.3.x
Threat Defense 7.2 を搭載した FXOS 2.12 Firepower 4110、4120、4140、4150 の最後のサポート。 SM-24、SM-36、SM-44 モジュールを搭載した Firepower 9300 の最後のサポート。	次のいずれかです。 → FXOS 2.13 と Threat Defense 7.3.x → FXOS 2.12 と任意の後続リリース Threat Defense 7.2.x
Threat Defense 7.1 を搭載した FXOS 2.11.1	次のいずれかです。 → FXOS 2.13 と Threat Defense 7.3.x → FXOS 2.12 と Threat Defense 7.2.x → FXOS 2.11.1 と任意の後続リリース Threat Defense 7.1.x

現在のバージョン	対象のバージョン
Threat Defense 7.0 を搭載した FXOS 2.10.1	次のいずれかです。 → FXOS 2.13 と Threat Defense 7.3.x → FXOS 2.12 と Threat Defense 7.2.x → FXOS 2.11.1 と Threat Defense 7.1.x → FXOS 2.10.1 と任意の後続リリース Threat Defense 7.0.x （注） データストアの非互換性のため、をバージョン 7.0.4 以降からバージョン 7.1.0 にアップグレードすることができません。バージョン 7.2 以降に直接アップグレードすることをお勧めします。 （注） クラウド提供型 Firewall Management Center は、バージョン 7.1 を実行している FTD デバイス、または任意のバージョンを実行している従来のデバイスを管理できません。クラウド管理の登録を解除するか、または無効にしない限り、クラウド管理対象デバイスはバージョン 7.0.x からバージョン 7.1 にアップグレードできません。バージョン 7.2 以降に直接アップグレードすることをお勧めします。
Threat Defense 6.7 を搭載した FXOS 2.9.1	次のいずれかです。 → FXOS 2.12 と Threat Defense 7.2.x → FXOS 2.11.1 と Threat Defense 7.1.x → FXOS 2.10.1 と Threat Defense 7.0.x → FXOS 2.9.1 と任意の後続リリース Threat Defense 6.7.x
Threat Defense 6.6 を搭載した FXOS 2.8.1	次のいずれかです。 → FXOS 2.12 と Threat Defense 7.2.x → FXOS 2.11.1 と Threat Defense 7.1.x → FXOS 2.10.1 と Threat Defense 7.0.x → FXOS 2.9.1 と Threat Defense 6.7.x → FXOS 2.8.1 と任意の後続リリース Threat Defense 6.6.x

現在のバージョン	対象のバージョン
Threat Defense 6.5 を搭載した FXOS 2.7.1	次のいずれかです。 → FXOS 2.11.1 と Threat Defense 7.1.x → FXOS 2.10.1 と Threat Defense 7.0.x → FXOS 2.9.1 と Threat Defense 6.7.x → FXOS 2.8.1 と Threat Defense 6.6.x
Threat Defense 6.4 を搭載した FXOS 2.6.1	次のいずれかです。 → FXOS 2.10.1 と Threat Defense 7.0.x → FXOS 2.9.1 と Threat Defense 6.7.x → FXOS 2.8.1 と Threat Defense 6.6.x → Threat Defense 6.5 を搭載した FXOS 2.7.1
Threat Defense 6.3 を搭載した FXOS 2.4.1	次のいずれかです。 → FXOS 2.9.1 と Threat Defense 6.7.x → FXOS 2.8.1 と Threat Defense 6.6.x → Threat Defense 6.5 を搭載した FXOS 2.7.1 → Threat Defense 6.4 を搭載した FXOS 2.6.1
Threat Defense 6.2.3 を搭載した FXOS 2.3.1	次のいずれかです。 → FXOS 2.8.1 と Threat Defense 6.6.x → Threat Defense 6.5 を搭載した FXOS 2.7.1 → Threat Defense 6.4 を搭載した FXOS 2.6.1 → Threat Defense 6.3 を搭載した FXOS 2.4.1

FXOS ならびに FTD と ASA のアップグレードパス

この表では、別のモジュールで実行されている FTD および ASA 論理デバイスを搭載した Firepower 9300 シャーシのアップグレードパスを示します。

（注） このドキュメントには、ASA 論理デバイスのアップグレード手順は記載されていません。アップグレード手順については、Cisco Secure Firewall ASA アップグレードガイド を参照してください。

現在の FTD/FMC のバージョンが対象のバージョンより後の日付にリリースされた場合、期待どおりにアップグレードできない可能性があります。このような場合、アップグレードはすぐ

に失敗し、2 つのバージョン間にデータストアの非互換性があることを説明するエラーが表示されます。現在のバージョンと対象のバージョンの両方のに関するリリースノートには、特定の制限が掲載されています。

この表には、シスコにより特別に認定されたバージョンの組み合わせのみが掲載されています。最初にFXOSをアップグレードするため、サポートされているが推奨されていない組み合わせを一時的に実行します。オペレーティングシステムはデバイスソフトウェアの「前」にアップグレードします。FXOS をアップグレードしても、論理デバイス（ASA デバイスを含む）や FTD アプリケーション インスタンスとの互換性が失われないようにしてください。複数のバージョンをスキップする必要がある場合、通常はFTDがリミッタになります。FXOS と ASA は通常、1 ホップでさらにアップグレードできます。ターゲットの FXOS バージョンに達したら、どのタイプの論理デバイスからでもアップグレードを開始できます。最小限のビルドおよびその他の詳細な互換性情報については、『Cisco Secure Firewall Threat Defense 互換性ガイド』を参照してください。

表 *35 : Firepower 9300* での *FTD* および *ASA* の直接アップグレード

現在のバージョン	対象のバージョン
FXOS 2.13 と以下の組み合わせ： • Threat Defense 7.3 • ASA 9.19(x)	→ FXOS 2.13、ASA 9.19(x)、および任意の後続リリース Threat Defense 7.3.x
FXOS 2.12： • Threat Defense 7.2 • ASA 9.18(x) SM-24、SM-36、SM-44 モジュールを搭載した Firepower 9300 の最後のサポート。	次のいずれかです。 → FXOS 2.13、ASA 9.19(x)、および Threat Defense 7.3.x → FXOS 2.12、ASA 9.18(x)、および任意の後続リリース Threat Defense 7.2.x
次を搭載した FXOS 2.11.1 • Threat Defense 7.1 • ASA 9.17(x)	→ FXOS 2.13、ASA 9.19(x)、および Threat Defense 7.3.x → FXOS 2.12、ASA 9.18(x)、および Threat Defense 7.2.x → FXOS 2.11.1、ASA 9.17(x)、および任意の後続リリース Threat Defense 7.1.x

現在のバージョン	対象のバージョン
次を搭載した FXOS 2.10.1 • Threat Defense 7.0 • ASA 9.16(x)	次のいずれかです。 → FXOS 2.13、ASA 9.19(x)、および Threat Defense 7.3.x → FXOS 2.12、ASA 9.18(x)、および Threat Defense 7.2.x → FXOS 2.11.1、ASA 9.17(x)、および Threat Defense 7.1.x → FXOS 2.10.1、ASA 9.16(x)、および任意の後続リリース Threat Defense 7.0.x （注） データストアの非互換性のため、をバージョン 7.0.4 以降からバージョン 7.1.0 にアップグレードすることができません。バージョン 7.2 以降に直接アップグレードすることをお勧めします。 （注） クラウド提供型 Firewall Management Center は、バージョン 7.1 を実行している FTD デバイス、または任意のバージョンを実行している従来のデバイスを管理できません。クラウド管理の登録を解除するか、または無効にしない限り、クラウド管理対象デバイスはバージョン 7.0.x からバージョン 7.1 にアップグレードできません。バージョン 7.2 以降に直接アップグレードすることをお勧めします。
次を搭載した FXOS 2.9.1： • Threat Defense 6.7 • ASA 9.15(x)	次のいずれかです。 → FXOS 2.12、ASA 9.18(x)、および Threat Defense 7.2.x → FXOS 2.11.1、ASA 9.17(x)、および Threat Defense 7.1.x → FXOS 2.10.1、ASA 9.16(x)、および Threat Defense 7.0.x → FXOS 2.9.1、ASA 9.15(x)、および任意の後続リリース Threat Defense 6.7.x
次を搭載した FXOS 2.8.1： • Threat Defense 6.6 • ASA 9.14(x)	次のいずれかです。 → FXOS 2.12、ASA 9.18(x)、および Threat Defense 7.2.x → FXOS 2.11.1、ASA 9.17(x)、および Threat Defense 7.1.x → FXOS 2.10.1、ASA 9.16(x)、および Threat Defense 7.0.x → FXOS 2.9.1、ASA 9.15(x)、および Threat Defense 6.7.x → FXOS 2.8.1、ASA 9.14(x)、および任意の後続リリース Threat Defense 6.6.x

現在のバージョン	対象のバージョン
次を搭載した FXOS 2.7.1： • Threat Defense 6.5 • ASA 9.13(x)	次のいずれかです。 → FXOS 2.11.1、ASA 9.17(x)、および Threat Defense 7.1.x → FXOS 2.10.1、ASA 9.16(x)、および Threat Defense 7.0.x → FXOS 2.9.1、ASA 9.15(x)、および Threat Defense 6.7.x → FXOS 2.8.1、ASA 9.14(x)、および Threat Defense 6.6.x
次を搭載した FXOS 2.6.1： • Threat Defense 6.4 • ASA 9.12(x)	次のいずれかです。 → FXOS 2.10.1、ASA 9.16(x)、および Threat Defense 7.0.x → FXOS 2.9.1、ASA 9.15(x)、および Threat Defense 6.7.x → FXOS 2.8.1、ASA 9.14(x)、および Threat Defense 6.6.x → FXOS 2.7.1、ASA 9.13(x)、および Threat Defense 6.5

FXOS と FTD ハイアベイラビリティ/スケーラビリティのアップグレード順序

高可用性や拡張性を導入する場合でも、各シャーシのFXOSを個別にアップグレードします。中断を最小限に抑えるには、1 つずつシャーシの FXOS をアップグレードします。FTD のアップグレードの場合、グループ化されたデバイスが 1 つずつ自動的にアップグレードされます。

表 *36 : Firepower 4100/9300* に搭載された *FXOS* と *Threat Defense* のアップグレード順序

FTD の導入	アップグレード順序
スタンドアロン	**1.** FXOS をアップグレードします。 **2.** FTD をアップグレードします。
ハイ アベイラビリティ	FTD をアップグレードする前に、両方のシャーシで FTD をアップグレードします。中断を最小限に抑えるため、スタンバイは常にアップグレードします。 **1.** スタンバイデバイスを備えたシャーシの FXOS をアップグレードします。 **2.** ロールを切り替えます。 **3.** 新しいスタンバイデバイスを備えたシャーシの FXOS をアップグレードします。 **4.** FTD をアップグレードします。

FTD の導入	アップグレード順序
シャーシ内クラスタ（同じシャーシ上のユニット）	1. FXOS をアップグレードします。 2. FTD をアップグレードします。
シャーシ内クラスタ（異なるシャーシ上のユニット）	FTD をアップグレードする前に、すべてのシャーシの FXOS をアップグレードします。中断を最小限に抑えるため、すべてデータユニットのシャーシを常にアップグレードします。 1. すべてデータユニットのシャーシの FXOS をアップグレードします。 2. 制御モジュールをアップグレードしたシャーシに切り替えます。 3. 残りのシャーシの FXOS をアップグレードします。 4. FTD をアップグレードします。

Firepower Chassis Manager を使用した 上の FXOS のアップグレード

Firepower Chassis Manager を使用したスタンドアロン FTD 論理デバイスまたは FTD シャーシ内クラスタ用の FXOS のアップグレード

このセクションでは、スタンドアロン Firepower 4100/9300 シャーシの FXOS プラットフォームバンドルをアップグレードする方法を説明します。

このセクションでは、次のタイプのデバイスのアップグレードプロセスについて説明します。

- FTD 論理デバイスで構成されており、フェールオーバーペアまたはシャーシ間クラスタの一部ではない Firepower 4100 シリーズ シャーシ。
- フェールオーバーペアまたはシャーシ間クラスタの一部ではない 1 つまたは複数のスタンドアロン FTD 論理デバイスで構成されている Firepower 9300 シャーシ。
- シャーシ内クラスタ内の FTD 論理デバイスで構成されている Firepower 9300 シャーシ。

始める前に

アップグレードを開始する前に、以下が完了していることを確認します。

- アップグレード先の FXOS プラットフォーム バンドル ソフトウェア パッケージをダウンロードします。

• FXOS と FTD の構成をバックアップします。

ステップ 1 Firepower Chassis Manager で、**[システム（System）] > [更新（Updates）]** を選択します。
[使用可能な更新（Available Updates）] ページに、シャーシで使用可能な FXOS プラットフォームバンドルのイメージやアプリケーションのイメージのリストが表示されます。

ステップ 2 新しいプラットフォーム バンドル イメージをアップロードします。

a) [イメージのアップロード（Upload Image）] をクリックして、[イメージのアップロード（Upload Image）] ダイアログ ボックスを開きます。
b) [ファイルを選択（Choose File）] をクリックして対象のファイルに移動し、アップロードするイメージを選択します。
c) [Upload] をクリックします。
選択したイメージが Firepower 4100/9300 シャーシにアップロードされます。
d) 特定のソフトウェア イメージについては、イメージをアップロードした後にエンドユーザ ライセンス契約書が表示されます。システムのプロンプトに従ってエンドユーザ契約書に同意します。

ステップ 3 新しいプラットフォーム バンドル イメージが正常にアップロードされたら、アップグレードする FXOS プラットフォーム バンドルの [アップグレード（Upgrade）] をクリックします。

システムは、まずインストールするソフトウェア パッケージを確認します。そして現在インストールされているアプリケーションと指定した FXOS プラットフォーム ソフトウェア パッケージの間の非互換性を通知します。また既存のセッションを終了することやアップグレードの一部としてシステムをリブートする必要があることが警告されます。

ステップ 4 インストールの続行を確定するには [はい（Yes）] を、インストールをキャンセルするには [いいえ（No）] をクリックします。

システムがバンドルを解凍し、コンポーネントをアップグレードまたはリロードします。

ステップ 5 Firepower Chassis Manager は、アップグレード中は使用できません。FXOS CLI を使用してアップグレード プロセスをモニターできます。

a) **scope system** を入力します。
b) **show firmware monitor** を入力します。
c) すべてのコンポーネント（FPRM、ファブリック インターコネクト、およびシャーシ）で「`Upgrade-Status: Ready`」と表示されるのを待ちます。

（注） FPRM コンポーネントをアップグレードすると、システムが再起動し、その他のコンポーネントのアップグレードを続行します。

例：

```
FP9300-A# scope system
FP9300-A /system # show firmware monitor
FPRM:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Fabric Interconnect A:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready
```

```
Chassis 1:
    Server 1:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready
    Server 2:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready
```

ステップ 6 すべてのコンポーネントが正常にアップグレードされたら、次のコマンドを入力して、セキュリティ モジュール/セキュリティ エンジンおよびインストールされているアプリケーションの状態を確認します。

a) **top** を入力します。
b) **scope ssa** を入力します。
c) **show slot** を入力します。
d) Firepower 4100 シリーズ アプライアンスのセキュリティ エンジン、または Firepower 9300 applianceのインストールされている任意のセキュリティ モジュールについて、管理状態が「Ok」、操作の状態が「Online」であることを確認します。
e) **show app-instance** を入力します。
f) シャーシにインストールされているすべての論理デバイスについて、操作の状態が「Online」であることを確認します。

Firepower Chassis Manager を使用した FTD シャーシ間クラスタの FXOS のアップグレード

シャーシ間クラスタとして構成されている FTD 論理デバイスを備えた FirePOWER 9300 または FirePOWER 4100 シリーズのセキュリティアプライアンスがある場合、次の手順を使用して FirePOWER 9300 または FirePOWER 4100 シリーズのセキュリティアプライアンスの FXOS プラットフォームバンドルを更新します。

始める前に

アップグレードを開始する前に、以下が完了していることを確認します。

- アップグレード先の FXOS プラットフォーム バンドル ソフトウェア パッケージをダウンロードします。
- FXOS と FTD の構成をバックアップします。

ステップ 1 次のコマンドを入力して、セキュリティ モジュール/セキュリティ エンジンおよびインストールされているアプリケーションの状態を確認します。

a) シャーシ #2 の FXOS CLI に接続します（これは制御ユニットを持たないシャーシである必要があります）。
b) **top** を入力します。
c) **scope ssa** を入力します。

d) **show slot** を入力します。
e) Firepower 4100 シリーズ アプライアンスのセキュリティ エンジン、または Firepower 9300 applianceのインストールされている任意のセキュリティ モジュールについて、管理状態が「Ok」、操作の状態が「Online」であることを確認します。
f) **show app-instance** を入力します。
g) シャーシにインストールされているすべての論理デバイスについて、操作の状態が「Online」、クラスタの状態が「In Cluster」であることを確認します。また、稼働バージョンとして表示されている FTD ソフトウェアのバージョンが正しいことを確認します。

重要 制御ユニットがこのシャーシ上にないことを確認します。「Master」に設定されているクラスタのロールを持つ Firepower Threat Defense インスタンスがあってはいけません。

h) Firepower 9300 appliance にインストールされているすべてのセキュリティ モジュール、または Firepower 4100 シリーズ アプライアンス上のセキュリティ エンジンについて、FXOS バージョンが正しいことを確認してください。

scope server 1/*slot_id* で、Firepower 4100 シリーズ セキュリティ エンジンの場合、*slot_id* は 1 です。

show versionを使用して無効にすることができます。

ステップ 2 シャーシ #2 の Firepower Chassis Manager に接続します（これは制御ユニットを持たないシャーシである必要があります）。

ステップ 3 Firepower Chassis Manager で、**[システム（System）] > [更新（Updates）]** を選択します。
[使用可能な更新（Available Updates）] ページに、シャーシで使用可能な FXOS プラットフォーム バンドルのイメージやアプリケーションのイメージのリストが表示されます。

ステップ 4 新しいプラットフォーム バンドル イメージをアップロードします。

a) [イメージのアップロード（Upload Image）] をクリックして、[イメージのアップロード（Upload Image）] ダイアログ ボックスを開きます。
b) [ファイルを選択（Choose File）] をクリックして対象のファイルに移動し、アップロードするイメージを選択します。
c) [Upload] をクリックします。
選択したイメージが Firepower 4100/9300 シャーシにアップロードされます。
d) 特定のソフトウェア イメージについては、イメージをアップロードした後にエンドユーザ ライセンス契約書が表示されます。システムのプロンプトに従ってエンドユーザ契約書に同意します。

ステップ 5 新しいプラットフォーム バンドル イメージが正常にアップロードされたら、アップグレードする FXOS プラットフォーム バンドルの [アップグレード（Upgrade）] をクリックします。

システムは、まずインストールするソフトウェア パッケージを確認します。そして現在インストールされているアプリケーションと指定した FXOS プラットフォーム ソフトウェア パッケージの間の非互換性を通知します。また既存のセッションを終了することやアップグレードの一部としてシステムをリブートする必要があることが警告されます。

ステップ 6 インストールの続行を確定するには [はい（Yes）] を、インストールをキャンセルするには [いいえ（No）] をクリックします。

システムがバンドルを解凍し、コンポーネントをアップグレードまたはリロードします。

ステップ 7 Firepower Chassis Manager は、アップグレード中は使用できません。FXOS CLI を使用してアップグレード プロセスをモニターできます。

a) **scope system** を入力します。
b) **show firmware monitor** を入力します。
c) すべてのコンポーネント（FPRM、ファブリック インターコネクト、およびシャーシ）で「`Upgrade-Status: Ready`」と表示されるのを待ちます。

（注） FPRM コンポーネントをアップグレードすると、システムが再起動し、その他のコンポーネントのアップグレードを続行します。

d) **top** を入力します。
e) **scope ssa** を入力します。
f) **show slot** を入力します。
g) Firepower 4100 シリーズ アプライアンスのセキュリティ エンジン、または Firepower 9300 appliance のインストールされている任意のセキュリティ モジュールについて、管理状態が「`Ok`」、操作の状態が「`Online`」であることを確認します。
h) **show app-instance** を入力します。
i) シャーシにインストールされているすべての論理デバイスについて、操作の状態が「`Online`」、クラスタの状態が「`In Cluster`」、クラスタのロールが「`Slave`」であることを確認します。

例：

```
FP9300-A# scope system
FP9300-A /system # show firmware monitor
FPRM:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Fabric Interconnect A:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Chassis 1:
    Server 1:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready
    Server 2:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready

FP9300-A /system #
FP9300-A /system # top
FP9300-A# scope ssa
FP9300-A /ssa # show slot

Slot:
    Slot ID    Log Level Admin State  Oper State
    ---------- --------- ------------ ----------
    1          Info      Ok           Online
    2          Info      Ok           Online
    3          Info      Ok           Not Available
FP9300-A /ssa #

FP9300-A /ssa # show app-instance
App Name   Slot ID    Admin State Oper State       Running Version Startup Version Profile Name
Cluster State   Cluster Role
```

```
---------- ---------- ---------- ---------------- --------------- --------------- ------------
-------------- ------------
ftd        1          Enabled    Online           6.2.2.81        6.2.2.81
In Cluster     Slave
ftd        2          Enabled    Online           6.2.2.81        6.2.2.81
In Cluster     Slave
ftd        3          Disabled   Not Available                    6.2.2.81
Not Applicable  None
FP9300-A /ssa #
```

ステップ 8 シャーシ #2 のセキュリティモジュールの 1 つを制御用として設定します。

シャーシ #2 のセキュリティモジュールの 1 つを制御用として設定すると、シャーシ #1 には制御ユニットが含まれなくなり、すぐにアップグレードすることができます。

ステップ 9 クラスタ内の他のすべてのシャーシに対して手順 1 ～ 7 を繰り返します。

ステップ 10 制御ロールをシャーシ #1 に戻すには、シャーシ #1 のセキュリティモジュールの 1 つを制御用として設定します。

Firepower Chassis Manager を使用した FTD ハイアベイラビリティペアの FXOS のアップグレード

ハイアベイラビリティペアとして構成されている FTD 論理デバイスを備えた FirePOWER 9300 または FirePOWER 4100 シリーズのセキュリティアプライアンスがある場合、次の手順を使用して FirePOWER 9300 または FirePOWER 4100 シリーズのセキュリティアプライアンスの FXOS プラットフォームバンドルを更新します。

始める前に

アップグレードを開始する前に、以下が完了していることを確認します。

- アップグレード先の FXOS プラットフォーム バンドル ソフトウェア パッケージをダウンロードします。
- FXOS と FTD の構成をバックアップします。

ステップ 1 スタンバイの Firepower Threat Defense 論理デバイスを含む Firepower セキュリティアプライアンス上の Firepower Chassis Manager に接続します。

ステップ 2 Firepower Chassis Manager で、**[システム（System）]** > **[更新（Updates）]** を選択します。
[使用可能な更新（Available Updates）] ページに、シャーシで使用可能な FXOS プラットフォームバンドルのイメージやアプリケーションのイメージのリストが表示されます。

ステップ 3 新しいプラットフォーム バンドル イメージをアップロードします。

a) [イメージのアップロード（Upload Image）] をクリックして、[イメージのアップロード（Upload Image）] ダイアログ ボックスを開きます。

b) [ファイルを選択（Choose File）] をクリックして対象のファイルに移動し、アップロードするイメージを選択します。
c) [Upload] をクリックします。
選択したイメージが Firepower 4100/9300 シャーシにアップロードされます。
d) 特定のソフトウェア イメージについては、イメージをアップロードした後にエンドユーザ ライセンス契約書が表示されます。システムのプロンプトに従ってエンドユーザ契約書に同意します。

ステップ 4 新しいプラットフォーム バンドル イメージが正常にアップロードされたら、アップグレードする FXOS プラットフォーム バンドルの [アップグレード（Upgrade）] をクリックします。

システムは、まずインストールするソフトウェア パッケージを確認します。そして現在インストールされているアプリケーションと指定した FXOS プラットフォーム ソフトウェア パッケージの間の非互換性を通知します。また既存のセッションを終了することやアップグレードの一部としてシステムをリブートする必要があることが警告されます。

ステップ 5 インストールの続行を確定するには [はい（Yes）] を、インストールをキャンセルするには [いいえ（No）] をクリックします。

システムがバンドルを解凍し、コンポーネントをアップグレードまたはリロードします。

ステップ 6 Firepower Chassis Manager は、アップグレード中は使用できません。FXOS CLI を使用してアップグレード プロセスをモニターできます。

a) **scope system** を入力します。
b) **show firmware monitor** を入力します。
c) すべてのコンポーネント（FPRM、ファブリック インターコネクト、およびシャーシ）で「`Upgrade-Status: Ready`」と表示されるのを待ちます。

（注） FPRM コンポーネントをアップグレードすると、システムが再起動し、その他のコンポーネントのアップグレードを続行します。

例：

```
FP9300-A# scope system
FP9300-A /system # show firmware monitor
FPRM:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Fabric Interconnect A:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Chassis 1:
    Server 1:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready
    Server 2:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready
```

ステップ 7 すべてのコンポーネントが正常にアップグレードされたら、次のコマンドを入力して、セキュリティ モジュール/セキュリティ エンジンおよびインストールされているアプリケーションの状態を確認します。

a) **top** を入力します。
b) **scope ssa** を入力します。
c) **show slot** を入力します。
d) Firepower 4100 シリーズ アプライアンスのセキュリティ エンジン、または Firepower 9300 applianceのインストールされている任意のセキュリティ モジュールについて、管理状態が「Ok」、操作の状態が「Online」であることを確認します。
e) **show app-instance** を入力します。
f) シャーシにインストールされているすべての論理デバイスについて、操作の状態が「Online」であることを確認します。

ステップ 8 アップグレードしたユニットをアクティブユニットにして、アップグレード済みのユニットにトラフィックが流れるようにします。

a) Firepower Management Center に接続します。
b) **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択します。
c) アクティブ ピアを変更するハイ アベイラビリティ ペアの横にあるアクティブ ピア切り替えアイコン（  ）をクリックします。
d) ハイ アベイラビリティ ペアでスタンバイ デバイスをアクティブ デバイスにすぐに切り替える場合は、[はい（Yes）] をクリックします。

ステップ 9 新しいスタンバイの Firepower Threat Defense 論理デバイスを含む Firepower セキュリティアプライアンス上の Firepower Chassis Manager に接続します。

ステップ 10 Firepower Chassis Manager で、**[システム（System）]** > **[更新（Updates）]** を選択します。
[使用可能な更新（Available Updates）] ページに、シャーシで使用可能な FXOS プラットフォームバンドルのイメージやアプリケーションのイメージのリストが表示されます。

ステップ 11 新しいプラットフォーム バンドル イメージをアップロードします。

a) [イメージのアップロード（Upload Image）] をクリックして、[イメージのアップロード（Upload Image）] ダイアログ ボックスを開きます。
b) [ファイルを選択（Choose File）] をクリックして対象のファイルに移動し、アップロードするイメージを選択します。
c) [Upload] をクリックします。
選択したイメージが Firepower 4100/9300 シャーシにアップロードされます。
d) 特定のソフトウェア イメージについては、イメージをアップロードした後にエンドユーザ ライセンス契約書が表示されます。システムのプロンプトに従ってエンドユーザ契約書に同意します。

ステップ 12 新しいプラットフォーム バンドル イメージが正常にアップロードされたら、アップグレードする FXOS プラットフォーム バンドルの [アップグレード（Upgrade）] をクリックします。

システムは、まずインストールするソフトウェア パッケージを確認します。そして現在インストールされているアプリケーションと指定した FXOS プラットフォーム ソフトウェア パッケージの間の非互換性を通知します。また既存のセッションを終了することやアップグレードの一部としてシステムをリブートする必要があることが警告されます。

ステップ 13 インストールの続行を確定するには [はい（Yes）] を、インストールをキャンセルするには [いいえ（No）] をクリックします。

システムがバンドルを解凍し、コンポーネントをアップグレードまたはリロードします。アップグレード プロセスは、完了までに最大 30 分かかることがあります。

ステップ 14 Firepower Chassis Manager は、アップグレード中は使用できません。FXOS CLI を使用してアップグレード プロセスをモニターできます。

a) **scope system** を入力します。
b) **show firmware monitor** を入力します。
c) すべてのコンポーネント（FPRM、ファブリック インターコネクト、およびシャーシ）で「Upgrade-Status: Ready」と表示されるのを待ちます。

（注） FPRM コンポーネントをアップグレードすると、システムが再起動し、その他のコンポーネントのアップグレードを続行します。

例：

```
FP9300-A# scope system
FP9300-A /system # show firmware monitor
FPRM:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Fabric Interconnect A:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Chassis 1:
    Server 1:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready
    Server 2:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready
```

ステップ 15 すべてのコンポーネントが正常にアップグレードされたら、次のコマンドを入力して、セキュリティ モジュール/セキュリティ エンジンおよびインストールされているアプリケーションの状態を確認します。

a) **top** を入力します。
b) **scope ssa** を入力します。
c) **show slot** を入力します。
d) Firepower 4100 シリーズ アプライアンスのセキュリティ エンジン、または Firepower 9300 applianceのインストールされている任意のセキュリティ モジュールについて、管理状態が「Ok」、操作の状態が「Online」であることを確認します。
e) **show app-instance** を入力します。
f) シャーシにインストールされているすべての論理デバイスについて、操作の状態が「Online」であることを確認します。

ステップ 16 アップグレードしたユニットを、アップグレード前のようにアクティブ ユニットにします。

a) Firepower Management Center に接続します。
b) **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択します。
c) アクティブ ピアを変更するハイ アベイラビリティ ペアの横にあるアクティブ ピア切り替えアイコン（  ）をクリックします。

d) ハイ アベイラビリティ ペアでスタンバイ デバイスをアクティブ デバイスにすぐに切り替える場合は、[はい（Yes）] をクリックします。

CLI を使用した 上の FXOS のアップグレード

FXOS CLIを使用したスタンドアロンFTD論理デバイスまたはFTDシャーシ内クラスタ用の FXOS のアップグレード

このセクションでは、スタンドアロン Firepower 4100/9300 シャーシの FXOS プラットフォーム バンドルをアップグレードする方法を説明します。

このセクションでは、次のタイプのデバイスの FXOS のアップグレード プロセスについて説明します。

- FTD論理デバイスで構成されており、フェールオーバーペアまたはシャーシ間クラスタの一部ではない Firepower 4100 シリーズ シャーシ。
- フェールオーバーペアまたはシャーシ間クラスタの一部ではない1つまたは複数のスタンドアロン FTD デバイスで構成されている Firepower 9300 シャーシ。
- シャーシ内クラスタ内の FTD 論理デバイスで構成されている Firepower 9300 シャーシ。

始める前に

アップグレードを開始する前に、以下が完了していることを確認します。

- アップグレード先の FXOS プラットフォーム バンドル ソフトウェア パッケージをダウンロードします。
- FXOS と FTD の構成をバックアップします。
- Firepower 4100/9300 シャーシにソフトウェア イメージをダウンロードするために必要な次の情報を収集します。
  - イメージのコピー元のサーバーの IP アドレスおよび認証クレデンシャル。
  - イメージ ファイルの完全修飾名。

ステップ 1 FXOS CLI に接続します。

ステップ 2 新しいプラットフォーム バンドル イメージを Firepower 4100/9300 シャーシにダウンロードします。

a) ファームウェア モードに入ります。

```
Firepower-chassis-a # scope firmware
```

b) FXOS プラットフォーム バンドル ソフトウェア イメージをダウンロードします。

Firepower-chassis-a /firmware # **download image** *URL*

次のいずれかの構文を使用してインポートされるファイルの URL を指定します。

- **ftp**://*username@hostname*/*path*/*image_name*
- **scp**://*username@hostname*/*path*/*image_name*
- **sftp**://*username@hostname*/*path*/*image_name*
- **tftp**://*hostname***:***port-num*/*path*/*image_name*

c) ダウンロード プロセスをモニタする場合：

Firepower-chassis-a /firmware # **scope download-task** *image_name*

Firepower-chassis-a /firmware/download-task # **show detail**

例：

次の例では、SCP プロトコルを使用してイメージをコピーします。

```
Firepower-chassis-a # scope firmware
Firepower-chassis-a /firmware # download image scp://user@192.168.1.1/images/fxos-k9.2.3.1.58.SPA
Firepower-chassis-a /firmware # scope download-task fxos-k9.2.3.1.58.SPA
Firepower-chassis-a /firmware/download-task # show detail
Download task:
    File Name: fxos-k9.2.3.1.58.SPA
    Protocol: scp
    Server: 192.168.1.1
    Userid:
    Path:
    Downloaded Image Size (KB): 853688
    State: Downloading
    Current Task: downloading image fxos-k9.2.3.1.58.SPA from
192.168.1.1(FSM-STAGE:sam:dme:FirmwareDownloaderDownload:Local)
```

ステップ 3 必要に応じて、ファームウェア モードに戻ります。

Firepower-chassis-a /firmware/download-task # **up**

ステップ 4 auto-install モードにします。

Firepower-chassis-a /firmware # **scope auto-install**

ステップ 5 FXOS プラットフォーム バンドルをインストールします。

Firepower-chassis-a /firmware/auto-install # **install platform platform-vers** *version_number*

version_number は、インストールする FXOS プラットフォーム バンドルのバージョン番号です（たとえば、2.3(1.58)）。

ステップ 6 システムは、まずインストールするソフトウェア パッケージを確認します。そして現在インストールされているアプリケーションと指定した FXOS プラットフォーム ソフトウェア パッケージの間の非互換性を通知します。また既存のセッションを終了することやアップグレードの一部としてシステムをリブートする必要があることが警告されます。

yes を入力して、検証に進むことを確認します。

ステップ 7 インストールの続行を確定するには **yes** を、インストールをキャンセルするには **no** を入力します。

システムがバンドルを解凍し、コンポーネントをアップグレードまたはリロードします。

ステップ 8 アップグレード プロセスをモニタするには、次の手順を実行します。

a) **scope system** を入力します。
b) **show firmware monitor** を入力します。
c) すべてのコンポーネント（FPRM、ファブリック インターコネクト、およびシャーシ）で「Upgrade-Status: Ready」と表示されるのを待ちます。

（注） FPRM コンポーネントをアップグレードすると、システムが再起動し、その他のコンポーネントのアップグレードを続行します。

例：

```
FP9300-A# scope system
FP9300-A /system # show firmware monitor
FPRM:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Fabric Interconnect A:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Chassis 1:
    Server 1:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready
    Server 2:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready

FP9300-A /system #
```

ステップ 9 すべてのコンポーネントが正常にアップグレードされたら、次のコマンドを入力して、セキュリティ モジュール/セキュリティ エンジンおよびインストールされているアプリケーションの状態を確認します。

a) **top** を入力します。
b) **scope ssa** を入力します。
c) **show slot** を入力します。
d) Firepower 4100 シリーズ アプライアンスのセキュリティ エンジン、または Firepower 9300 applianceのインストールされている任意のセキュリティ モジュールについて、管理状態が「Ok」、操作の状態が「Online」であることを確認します。
e) **show app-instance** を入力します。
f) シャーシにインストールされているすべての論理デバイスについて、操作の状態が「Online」であることを確認します。

FXOS CLI を使用した FTD シャーシ間クラスタの FXOS のアップグレード

シャーシ間クラスタとして構成されている FTD 論理デバイスを備えた FirePOWER 9300 または FirePOWER 4100 シリーズのセキュリティアプライアンスがある場合、次の手順を使用して FirePOWER 9300 または FirePOWER 4100 シリーズのセキュリティアプライアンスの FXOS プラットフォームバンドルを更新します。

始める前に

アップグレードを開始する前に、以下が完了していることを確認します。

- アップグレード先の FXOS プラットフォーム バンドル ソフトウェア パッケージをダウンロードします。
- FXOS と FTD の構成をバックアップします。
- Firepower 4100/9300 シャーシにソフトウェアイメージをダウンロードするために必要な次の情報を収集します。
  - イメージのコピー元のサーバーの IP アドレスおよび認証クレデンシャル。
  - イメージ ファイルの完全修飾名。

ステップ 1 シャーシ #2 の FXOS CLI に接続します（これは制御ユニットを持たないシャーシである必要があります）。

ステップ 2 次のコマンドを入力して、セキュリティ モジュール/セキュリティ エンジンおよびインストールされているアプリケーションの状態を確認します。

a) **top** を入力します。
b) **scope ssa** を入力します。
c) **show slot** を入力します。
d) Firepower 4100 シリーズ アプライアンスのセキュリティ エンジン、または Firepower 9300 appliance のインストールされている任意のセキュリティ モジュールについて、管理状態が「Ok」、操作の状態が「Online」であることを確認します。
e) **show app-instance** を入力します。
f) シャーシにインストールされているすべての論理デバイスについて、操作の状態が「Online」、クラスタの状態が「In Cluster」であることを確認します。また、稼働バージョンとして表示されている FTD ソフトウェアのバージョンが正しいことを確認します。

重要 制御ユニットがこのシャーシ上にないことを確認します。「Master」に設定されているクラスタのロールを持つ Firepower Threat Defense インスタンスがあってはいけません。

g) Firepower 9300 appliance にインストールされているすべてのセキュリティ モジュール、または Firepower 4100 シリーズ アプライアンス上のセキュリティ エンジンについて、FXOS バージョンが正しいことを確認してください。

scope server 1/*slot_id* で、Firepower 4100 シリーズ セキュリティ エンジンの場合、*slot_id* は 1 です。

show versionを使用して無効にすることができます。

ステップ 3 新しいプラットフォーム バンドル イメージを Firepower 4100/9300 シャーシにダウンロードします。

a) **top** を入力します。

b) ファームウェア モードに入ります。

Firepower-chassis-a # **scope firmware**

c) FXOS プラットフォーム バンドル ソフトウェア イメージをダウンロードします。

Firepower-chassis-a /firmware # **download image** *URL*

次のいずれかの構文を使用してインポートされるファイルの URL を指定します。

- **ftp**://*username@hostname*/*path*/*image_name*
- **scp**://*username@hostname*/*path*/*image_name*
- **sftp**://*username@hostname*/*path*/*image_name*
- **tftp**://*hostname***:***port-num*/*path*/*image_name*

d) ダウンロード プロセスをモニタする場合：

Firepower-chassis-a /firmware # **scope download-task** *image_name*

Firepower-chassis-a /firmware/download-task # **show detail**

例：

次の例では、SCP プロトコルを使用してイメージをコピーします。

```
Firepower-chassis-a # scope firmware
Firepower-chassis-a /firmware # download image scp://user@192.168.1.1/images/fxos-k9.2.3.1.58.SPA
Firepower-chassis-a /firmware # scope download-task fxos-k9.2.3.1.58.SPA
Firepower-chassis-a /firmware/download-task # show detail
Download task:
    File Name: fxos-k9.2.3.1.58.SPA
    Protocol: scp
    Server: 192.168.1.1
    Userid:
    Path:
    Downloaded Image Size (KB): 853688
    State: Downloading
    Current Task: downloading image fxos-k9.2.3.1.58.SPA from
192.168.1.1(FSM-STAGE:sam:dme:FirmwareDownloaderDownload:Local)
```

ステップ 4 必要に応じて、ファームウェア モードに戻ります。

Firepower-chassis-a /firmware/download-task # **up**

ステップ 5 auto-install モードにします。

Firepower-chassis /firmware # **scope auto-install**

ステップ 6 FXOS プラットフォーム バンドルをインストールします。

Firepower-chassis /firmware/auto-install # **install platform platform-vers** *version_number*

version_number は、インストールする FXOS プラットフォーム バンドルのバージョン番号です（たとえば、2.3(1.58)）。

ステップ 7 システムは、まずインストールするソフトウェア パッケージを確認します。そして現在インストールされているアプリケーションと指定した FXOS プラットフォーム ソフトウェア パッケージの間の非互換性を通知します。また既存のセッションを終了することやアップグレードの一部としてシステムをリブートする必要があることが警告されます。

yes を入力して、検証に進むことを確認します。

ステップ 8 インストールの続行を確定するには **yes** を、インストールをキャンセルするには **no** を入力します。

システムがバンドルを解凍し、コンポーネントをアップグレードまたはリロードします。

ステップ 9 アップグレード プロセスをモニタするには、次の手順を実行します。

a) **scope system** を入力します。
b) **show firmware monitor** を入力します。
c) すべてのコンポーネント（FPRM、ファブリック インターコネクト、およびシャーシ）で「`Upgrade-Status: Ready`」と表示されるのを待ちます。

（注） FPRM コンポーネントをアップグレードすると、システムが再起動し、その他のコンポーネントのアップグレードを続行します。

d) **top** を入力します。
e) **scope ssa** を入力します。
f) **show slot** を入力します。
g) Firepower 4100 シリーズ アプライアンスのセキュリティ エンジン、または Firepower 9300 applianceのインストールされている任意のセキュリティ モジュールについて、管理状態が「`Ok`」、操作の状態が「`Online`」であることを確認します。
h) **show app-instance** を入力します。
i) シャーシにインストールされているすべての論理デバイスについて、操作の状態が「`Online`」、クラスタの状態が「`In Cluster`」、クラスタのロールが「`Slave`」であることを確認します。

例：

```
FP9300-A# scope system
FP9300-A /system # show firmware monitor
FPRM:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Fabric Interconnect A:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Chassis 1:
    Server 1:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready
    Server 2:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready
```

```
FP9300-A /system #
FP9300-A /system # top
FP9300-A# scope ssa
FP9300-A /ssa # show slot

Slot:
    Slot ID    Log Level Admin State  Oper State
    ---------- --------- ------------ ----------
    1          Info      Ok           Online
    2          Info      Ok           Online
    3          Info      Ok           Not Available
FP9300-A /ssa #

FP9300-A /ssa # show app-instance
App Name   Slot ID    Admin State Oper State       Running Version Startup Version Profile Name
Cluster State   Cluster Role
---------- ---------- ----------- ---------------- --------------- --------------- ------------
--------------- ------------
ftd        1          Enabled     Online           6.2.2.81        6.2.2.81
In Cluster      Slave
ftd        2          Enabled     Online           6.2.2.81        6.2.2.81
In Cluster      Slave
ftd        3          Disabled    Not Available                    6.2.2.81
Not Applicable  None
FP9300-A /ssa #
```

ステップ 10 シャーシ #2 のセキュリティモジュールの 1 つを制御用として設定します。

シャーシ #2 のセキュリティモジュールの 1 つを制御用として設定すると、シャーシ #1 には制御ユニットが含まれなくなり、すぐにアップグレードすることができます。

ステップ 11 クラスタ内の他のすべてのシャーシに対して手順 1 ～ 9 を繰り返します。

ステップ 12 制御ロールをシャーシ #1 に戻すには、シャーシ #1 のセキュリティモジュールの 1 つを制御用として設定します。

FXOS CLI を使用した FTD ハイアベイラビリティペアの FXOS のアップグレード

ハイアベイラビリティペアとして構成されている FTD 論理デバイスを備えた FirePOWER 9300 または FirePOWER 4100 シリーズのセキュリティアプライアンスがある場合、次の手順を使用して FirePOWER 9300 または FirePOWER 4100 シリーズのセキュリティアプライアンスの FXOS プラットフォームバンドルを更新します。

始める前に

アップグレードを開始する前に、以下が完了していることを確認します。

- アップグレード先の FXOS プラットフォーム バンドル ソフトウェア パッケージをダウンロードします。
- FXOS と FTD の構成をバックアップします。

- Firepower 4100/9300 シャーシにソフトウェア イメージをダウンロードするために必要な次の情報を収集します。
  - イメージのコピー元のサーバーの IP アドレスおよび認証クレデンシャル。
  - イメージ ファイルの完全修飾名。

ステップ 1 スタンバイの Firepower Threat Defense 論理デバイスを含む Firepower セキュリティ アプライアンス上の FXOS CLI に接続します。

ステップ 2 新しいプラットフォーム バンドル イメージを Firepower 4100/9300 シャーシにダウンロードします。

a) ファームウェア モードに入ります。

Firepower-chassis-a # **scope firmware**

b) FXOS プラットフォーム バンドル ソフトウェア イメージをダウンロードします。

Firepower-chassis-a /firmware # **download image** *URL*

次のいずれかの構文を使用してインポートされるファイルの URL を指定します。

- **ftp**://*username@hostname*/*path*/*image_name*
- **scp**://*username@hostname*/*path*/*image_name*
- **sftp**://*username@hostname*/*path*/*image_name*
- **tftp**://*hostname***:***port-num*/*path*/*image_name*

c) ダウンロード プロセスをモニタする場合：

Firepower-chassis-a /firmware # **scope download-task** *image_name*

Firepower-chassis-a /firmware/download-task # **show detail**

例：

次の例では、SCP プロトコルを使用してイメージをコピーします。

```
Firepower-chassis-a # scope firmware
Firepower-chassis-a /firmware # download image scp://user@192.168.1.1/images/fxos-k9.2.3.1.58.SPA
Firepower-chassis-a /firmware # scope download-task fxos-k9.2.3.1.58.SPA
Firepower-chassis-a /firmware/download-task # show detail
Download task:
    File Name: fxos-k9.2.3.1.58.SPA
    Protocol: scp
    Server: 192.168.1.1
    Userid:
    Path:
    Downloaded Image Size (KB): 853688
    State: Downloading
    Current Task: downloading image fxos-k9.2.3.1.58.SPA from
192.168.1.1(FSM-STAGE:sam:dme:FirmwareDownloaderDownload:Local)
```

ステップ 3 必要に応じて、ファームウェア モードに戻ります。

Firepower-chassis-a /firmware/download-task # **up**

ステップ 4 auto-install モードにします。

Firepower-chassis-a /firmware # **scope auto-install**

ステップ 5 FXOS プラットフォーム バンドルをインストールします。

Firepower-chassis-a /firmware/auto-install # **install platform platform-vers** *version_number*

version_number は、インストールする FXOS プラットフォームバンドルのバージョン番号です（たとえば、2.3(1.58)）。

ステップ 6 システムは、まずインストールするソフトウェア パッケージを確認します。そして現在インストールされているアプリケーションと指定した FXOS プラットフォーム ソフトウェア パッケージの間の非互換性を通知します。また既存のセッションを終了することやアップグレードの一部としてシステムをリブートする必要があることが警告されます。

yes を入力して、検証に進むことを確認します。

ステップ 7 インストールの続行を確定するには **yes** を、インストールをキャンセルするには **no** を入力します。

システムがバンドルを解凍し、コンポーネントをアップグレードまたはリロードします。

ステップ 8 アップグレード プロセスをモニタするには、次の手順を実行します。

a) **scope system** を入力します。
b) **show firmware monitor** を入力します。
c) すべてのコンポーネント（FPRM、ファブリック インターコネクト、およびシャーシ）で「`Upgrade-Status: Ready`」と表示されるのを待ちます。

（注） FPRM コンポーネントをアップグレードすると、システムが再起動し、その他のコンポーネントのアップグレードを続行します。

例：

```
FP9300-A# scope system
FP9300-A /system # show firmware monitor
FPRM:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Fabric Interconnect A:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Chassis 1:
    Server 1:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready
    Server 2:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready

FP9300-A /system #
```

ステップ 9 すべてのコンポーネントが正常にアップグレードされたら、次のコマンドを入力して、セキュリティ モジュール/セキュリティ エンジンおよびインストールされているアプリケーションの状態を確認します。

a) **top** を入力します。
b) **scope ssa** を入力します。
c) **show slot** を入力します。
d) Firepower 4100 シリーズ アプライアンスのセキュリティ エンジン、または Firepower 9300 applianceのインストールされている任意のセキュリティ モジュールについて、管理状態が「Ok」、操作の状態が「Online」であることを確認します。
e) **show app-instance** を入力します。
f) シャーシにインストールされているすべての論理デバイスについて、操作の状態が「Online」であることを確認します。

ステップ 10 アップグレードしたユニットをアクティブユニットにして、アップグレード済みのユニットにトラフィックが流れるようにします。

a) Firepower Management Center に接続します。
b) **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択します。
c) アクティブ ピアを変更するハイ アベイラビリティ ペアの横にあるアクティブ ピア切り替えアイコン（  ）をクリックします。
d) ハイ アベイラビリティ ペアでスタンバイ デバイスをアクティブ デバイスにすぐに切り替える場合は、[はい（Yes）] をクリックします。

ステップ 11 新しいスタンバイの Firepower Threat Defense 論理デバイスを含む Firepower セキュリティ アプライアンス上の FXOS CLI に接続します。

ステップ 12 新しいプラットフォーム バンドル イメージを Firepower 4100/9300 シャーシにダウンロードします。

a) ファームウェア モードに入ります。

Firepower-chassis-a # **scope firmware**

b) FXOS プラットフォーム バンドル ソフトウェア イメージをダウンロードします。

Firepower-chassis-a /firmware # **download image** *URL*

次のいずれかの構文を使用してインポートされるファイルの URL を指定します。

- **ftp**://*username@hostname*/*path*/*image_name*
- **scp**://*username@hostname*/*path*/*image_name*
- **sftp**://*username@hostname*/*path*/*image_name*
- **tftp**://*hostname***:***port-num*/*path*/*image_name*

c) ダウンロード プロセスをモニタする場合：

Firepower-chassis-a /firmware # **scope download-task** *image_name*

Firepower-chassis-a /firmware/download-task # **show detail**

例：

次の例では、SCP プロトコルを使用してイメージをコピーします。

```
Firepower-chassis-a # scope firmware
Firepower-chassis-a /firmware # download image scp://user@192.168.1.1/images/fxos-k9.2.3.1.58.SPA
Firepower-chassis-a /firmware # scope download-task fxos-k9.2.3.1.58.SPA
```

```
Firepower-chassis-a /firmware/download-task # show detail
Download task:
    File Name: fxos-k9.2.3.1.58.SPA
    Protocol: scp
    Server: 192.168.1.1
    Userid:
    Path:
    Downloaded Image Size (KB): 853688
    State: Downloading
    Current Task: downloading image fxos-k9.2.3.1.58.SPA from
192.168.1.1(FSM-STAGE:sam:dme:FirmwareDownloaderDownload:Local)
```

ステップ 13 必要に応じて、ファームウェア モードに戻ります。

Firepower-chassis-a /firmware/download-task # **up**

ステップ 14 auto-install モードにします。

Firepower-chassis-a /firmware # **scope auto-install**

ステップ 15 FXOS プラットフォーム バンドルをインストールします。

Firepower-chassis-a /firmware/auto-install # **install platform platform-vers** *version_number*

version_number は、インストールする FXOS プラットフォームバンドルのバージョン番号です（たとえば、2.3(1.58)）。

ステップ 16 システムは、まずインストールするソフトウェア パッケージを確認します。そして現在インストールされているアプリケーションと指定した FXOS プラットフォーム ソフトウェア パッケージの間の非互換性を通知します。また既存のセッションを終了することやアップグレードの一部としてシステムをリブートする必要があることが警告されます。

yes を入力して、検証に進むことを確認します。

ステップ 17 インストールの続行を確定するには **yes** を、インストールをキャンセルするには **no** を入力します。

システムがバンドルを解凍し、コンポーネントをアップグレードまたはリロードします。

ステップ 18 アップグレード プロセスをモニタするには、次の手順を実行します。

a) **scope system** を入力します。
b) **show firmware monitor** を入力します。
c) すべてのコンポーネント（FPRM、ファブリック インターコネクト、およびシャーシ）で「Upgrade-Status: Ready」と表示されるのを待ちます。

（注） FPRM コンポーネントをアップグレードすると、システムが再起動し、その他のコンポーネントのアップグレードを続行します。

例：

```
FP9300-A# scope system
FP9300-A /system # show firmware monitor
FPRM:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Fabric Interconnect A:
```

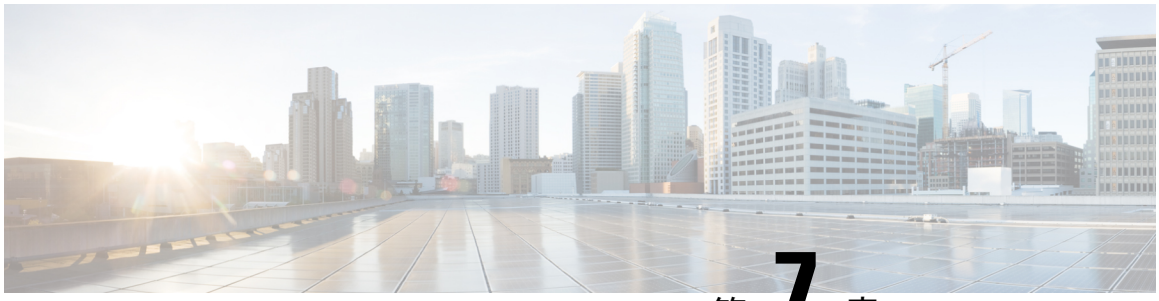
```
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Chassis 1:
    Server 1:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready
    Server 2:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready

FP9300-A /system #
```

ステップ 19 すべてのコンポーネントが正常にアップグレードされたら、次のコマンドを入力して、セキュリティ モジュール/セキュリティ エンジンおよびインストールされているアプリケーションの状態を確認します。

a) **top** を入力します。
b) **scope ssa** を入力します。
c) **show slot** を入力します。
d) Firepower 4100 シリーズ アプライアンスのセキュリティ エンジン、または Firepower 9300 applianceのインストールされている任意のセキュリティ モジュールについて、管理状態が「Ok」、操作の状態が「Online」であることを確認します。
e) **show app-instance** を入力します。
f) シャーシにインストールされているすべての論理デバイスについて、操作の状態が「Online」であることを確認します。

ステップ 20 アップグレードしたユニットを、アップグレード前のようにアクティブ ユニットにします。

a) Firepower Management Center に接続します。
b) **[デバイス（Devices）] > [デバイス管理（Device Management）]** を選択します。
c) アクティブ ピアを変更するハイ アベイラビリティ ペアの横にあるアクティブ ピア切り替えアイコン（  ）をクリックします。
d) ハイ アベイラビリティ ペアでスタンバイ デバイスをアクティブ デバイスにすぐに切り替える場合は、[はい（Yes）] をクリックします。



第 7 章

アップグレードを元に戻すまたはアンインストールする

アップグレードに成功したにもかかわらず、システムが期待どおりに機能しない場合は、復元またはアンインストールが可能な場合があります。

- メジャーおよびメンテナンスアップグレードの FTD への復元がサポートされています。
- アンインストールは、FTD へのパッチと FMC へのパッチでサポートされています。

これが機能せず、以前のバージョンに戻す必要がある場合、イメージを再作成する必要があります。

- Threat Defense の復元 （103 ページ）
- パッチのアンインストール （108 ページ）

Threat Defense の復元

FTD を復元すると、ソフトウェアは、最後のメジャーアップグレードまたはメンテナンスアップグレードの直前の状態に戻ります。パッチ適用後に復元すると、パッチも必然的に削除されます。システムが復元スナップショットを保存できるように、デバイスをアップグレードするときに復元を有効にする必要があります。

FTD の復元について

元に戻る設定

次の設定が元に戻ります。

- Snort バージョン。
- デバイス固有の設定。

一般的なデバイス設定、ルーティング、インターフェース、インラインセット、DHCP、SNMPなど、**[デバイス（Devices）]**>**[デバイス管理（Device Management）]**ページで設定するものすべて。

- デバイス固有の設定で使用されるオブジェクト。

  アクセスリスト、AS パス、キーチェーン、インターフェイス、ネットワーク、ポート、ルートマップ、SLA モニターオブジェクトなどが含まれます。デバイスのアップグレード後にこれらのオブジェクトを編集した場合、システムは新しいオブジェクトを作成するか、元に戻されたデバイスが使用するオブジェクトのオーバーライドを設定します。これにより、他のデバイスは現在の設定に従ってトラフィックを処理し続けることができます。

  復元に成功したら、復元したデバイスで使用されているオブジェクトを調べ、必要な調整を行うことをお勧めします。

元に戻されない設定

次の設定は元に戻りません。

- 複数のデバイスで使用できる共有ポリシー。たとえば、プラットフォーム設定やアクセスコントロール ポリシーなどです。

  正常に元に戻されたデバイスは期限切れとしてマークされているため、設定を再展開する必要があります。

- Firepower 4100/9300 の場合、Firepower Chassis Manager または FXOS CLI を使用して行ったインターフェイスの変更。

  復元に成功した後にインターフェイスの変更を同期します。

- Firepower 4100/9300 の場合、FXOS およびファームウェア。

  推奨される FXOS と FTD の組み合わせを実行する必要がある場合は、完全な再イメージ化が必要になる場合があります。FTD の復元ガイドライン（104 ページ）を参照してください。

FTD の復元ガイドライン

システム要件

FTD を復元するには、デバイスと FMC にバージョン 7.1 以降が必要です。たとえば、バージョン 7.1 の FMC はデバイスをバージョン 6.5 までさかのぼって管理でき、そのバージョン 7.1 の FMC を使用してデバイスを中間バージョン（6.6、6.7、7.0）までアップグレードできる場合であっても、デバイスをバージョン 7.1 にアップグレードするまで、復元はサポートされません。

以下では復元機能はサポートされていません。

- パッチとホットフィックス
- FTD コンテナインスタンス

- FMC

高可用性またはクラスタ化デバイスの復元

FMC Web インターフェイスを使用して FTD を復元する場合、個々の高可用性ユニットまたはクラスタ化されたノードを選択することはできません。システムは、それらを自動的に同時に復元します。つまり、復元中のトラフィックフローとインスペクションの中断は、すべてのデバイスがスタンドアロンであるかのように、インターフェイス設定に依存します。

完全または部分的にアップグレードされたグループで復元がサポートされていることに注意してください。部分的にアップグレードされたグループの場合、システムはアップグレードされたユニットとノードからのみアップグレードを削除します。元に戻しても高可用性やクラスタが壊れることはありませんが、グループを分解してその新しいスタンドアロンデバイスを復元することができます。

復元しても FXOS はダウングレードされない

Firepower 4100/9300 の場合、FTD のメジャーバージョンには特別に認定および推奨されている付随の FXOS バージョンがあります。FTD の以前のバージョンに戻った後、推奨されていないバージョンの FXOS（新しすぎる）を実行している可能性があります。

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

復元を妨げるシナリオ

次のいずれかの状況で復元を試みると、システムはエラーを表示します。

表 *37*：復元を妨げるシナリオ

シナリオ	解決方法
FMC とデバイス間の通信が中断されます。	FTD を復元するには FMC を使用する必要があります。デバイス CLI は使用できません。

シナリオ	解決方法
次の理由により、スナップショットを復元することはできません。 • デバイスをアップグレードしたときに、復元を有効にしていませんでした。 • FMC またはデバイスからスナップショットを削除したか、スナップショットの期限が切れました。 • 別の FMC でデバイスをアップグレードしました。	なし。 アップグレード完了後に元に戻す必要が生じる可能性がある場合は、**システム**（⚙）>**[更新（Updates）]** を使用してFTDをアップグレードします。これは、[アップグレードの成功後に復元を有効にする（Enable revert after successful upgrade）] オプション（）を設定する唯一の方法であり、Threat Defense のアップグレードウィザードを使用するという通常の推奨事項とは対照的です。 復元スナップショットは、FMC とデバイスに30日間保存され、その後自動的に削除され、復元できなくなります。ディスク容量を節約するためにどのアプライアンスからでもスナップショットを手動で削除できますが、復元の機能が失われます。
最後のアップグレードに失敗しました。	アップグレードをキャンセルして、デバイスをアップグレード前の状態に戻します。または、問題を修正して再試行してください。 復元は、アップグレードは成功したものの、アップグレードされたシステムが期待どおりに機能しない場合に使用します。復元は、失敗または進行中のアップグレードをキャンセルすることとは異なります。元に戻すこともキャンセルすることもできない場合は、イメージを再作成する必要があります。
アップグレード以降に、管理アクセスインターフェイスが変更されています。	元に戻して、もう一度お試しください。
クラスタのユニットが異なるバージョンからアップグレードされました。	すべて一致するまでユニットを削除し、クラスタメンバーを調整してから、小さなクラスタを復元します。新しくスタンドアロンユニットを復元することもできます。
クラスタでのアップグレード後に 1 つ以上のユニットがクラスタに追加されました。	新しいユニットを削除し、クラスタメンバーを調整してから、小さなクラスタを復元します。新しくスタンドアロンユニットを復元することもできます。
クラスタで FMC と FXOS が異なる数のクラスタユニットを識別しています。	クラスタメンバーを調整して再試行しますが、すべてのユニットを復元することはできない場合があります。

FMC を使用して FTD を復元する

FTD を復元するには FMC を使用する必要があります。デバイス CLI は使用できません。

Threat Defense の履歴：

- 7.1：初期サポート。

始める前に

- 復元がサポートされていることを確認してください。ガイドラインを読んで理解してください。
- 安全な外部の場所にバックアップします。復元に失敗した場合、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。

ステップ 1 **[デバイス（Devices）] > [デバイス管理（Device Management）]**を選択します。

ステップ 2 復元するデバイスの横にある **その他**（⋮） をクリックして、[アップグレードの復元（Revert Upgrade）] を選択します。

ハイ アベイラビリティペアとクラスタを除き、複数のデバイスを選択して復元することはできません。

ステップ 3 復元して再起動することを確認します。

復元中のトラフィックフローとインスペクションの中断は、すべてのデバイスがスタンドアロンであるかのように、インターフェイス設定に依存します。 これは、高可用性/スケーラビリティ展開であっても、システムがすべてのユニットを同時に復元するためです。

ステップ 4 復元の進行状況を監視します。

高可用性/スケーラビリティ展開では、最初のユニットがオンラインに戻ると、トラフィックフローとインスペクションが再開されます。数分間にわたり進展がない場合、または復元が失敗したことを示している場合は、Cisco TAC にお問い合わせください。

ステップ 5 復元が成功したことを確認します。

復元が完了したら、**[デバイス（Devices）] > [デバイス管理（Device Management）]** を選択し、復元した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。

ステップ 6 （Firepower 4100/9300）Firepower Chassis Manager または FXOS CLI を使用して、FTD 論理デバイスに加えたインターフェイスの変更を同期します。

FMC で **[デバイス（Devices）] > [デバイス管理（Device Management）]** を選択し、デバイスを編集して [同期（Sync）] をクリックします。

ステップ 7 その他に必要となる復元後の構成変更を完了します。

たとえば、デバイスのアップグレード後にデバイス固有の設定で使用されるオブジェクトを編集した場合、システムは新しいオブジェクトを作成するか、復元されたデバイスが使用するオブジェクトのオーバーラ

イドを設定します。復元したデバイスで使用されるオブジェクトを調べ、必要な調整を行うことをお勧めします。

ステップ 8 復元したデバイスに構成を再度展開します。

正常に復元されたデバイスは期限切れとしてマークされます。デバイスは古いバージョンを実行することになるため、展開が成功した後でも、新しい構成がサポートされない場合があります。

パッチのアンインストール

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に戻り、設定は変更されません。FMCでは、管理対象デバイスと同じかより新しいバージョンを実行する必要があるため、最初にデバイスからパッチをアンインストールします。アンインストールは、ホットフィックスではサポートされていません。

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7.1のパッチ

現在、すべてのバージョン7.1パッチがアンインストールに対応しています。

アンインストールに対応したバージョン6.7のパッチ

現在、すべてのバージョン6.7パッチがアンインストールに対応しています。

高可用性/拡張性のアンインストール順序

高可用性/拡張性の展開では、一度に 1 つのアプライアンスからアンインストールすることで中断を最小限に抑えます。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 *38 : FMC* 高可用性のアンインストール順序

設定	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 *39 : FTD* 高可用性およびクラスタのアンインストール順序

設定	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、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。

Threat Defense パッチのアンインストール

Linux シェル（エキスパートモード）を使用してパッチをアンインストールします。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。FMCユーザーアカウントは使用できません。シェルアクセスを無効にした場合は、 ロックダウンを元に戻すために Cisco TAC にご連絡ください。

⚠

注意 アンインストール中に設定の変更を行ったり、展開したりしないでください。システムが非アクティブに見えても、進行中のアンインストールを手動で再起動、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。

始める前に

- FTD 高可用性ペアを解除します。高可用性/拡張性のアンインストール順序 （109 ページ）を参照してください。
- 正常に展開され、通信が確立されていることを確認します。

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。展開とその他の必須のタスクが完了していることを確認してください。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 2 デバイスの FTD 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 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に設定されていて、FTDCLIにアクセスする場合は、次の表に示すような、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`
Secure Firewall 3100 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）

ステップ 3 `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 4 アップグレードディレクトリにアンインストールパッケージがあることを確認します。

```
ls /var/sf/updates
```

パッチのアンインストーラには、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 が含まれています。デバイ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。アンインストーラがない場合は、Cisco TAC までお問い合わせください。

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
```

注意 確認を求めら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。--detach オプションを使用すると、SSH 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プロセスが強制終了されなくなり、デバイスが不安定な状態になる可能性があることに注意してください。

ステップ 6 ログアウトするまでアンインストールを監視します。

個別のアンインストールの場合は、tail か tailf を使用してログを表示します。

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

それ以外の場合は、コンソールか端末で進行状況を監視します。

ステップ 7 アンインストールが成功したことを確認します。

アンインストールが完了したら、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 高可用性/スケーラビリティの展開では、ユニットごとに手順 2 から 6 を繰り返します。

クラスタの場合、制御ユニットからアンインストールしないでください。すべてのデータユニットからアンインストールしたら、そのうちの 1 つを新しい制御ユニットに設定し、以前の制御ユニットからアンインストールします。

ステップ 9 構成を再展開します。

例外：複数のバージョンが構成されている高可用性ペアまたはデバイスクラスタには展開しないでください。展開は最初のデバイスからアンインストールする前に行いますが、すべてのグループメンバー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。

次のタスク

- 高可用性については、高可用性を再確立します。
- クラスタについては、特定のデバイスに優先するロールがある場合は、それらの変更をすぐに行います。

スタンドアロン FMC パッチのアンインストール

FMC パッチのアンインストールには Web インターフェイスを使用することをお勧めします。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、 ロックダウンを元に戻すために Cisco TAC にご連絡ください。

⚠

注意 アンインストール中に設定の変更を行ったり、展開したりしないでください。システムが非アクティブに見えても、進行中のアンインストールを手動で再起動、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。

始める前に

- アンインストールによってFMCのパッチレベルが管理対象デバイスより低くなる場合は、最初にデバイスからパッチをアンインストールします。
- 正常に展開され、通信が確立されていることを確認します。

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 [利用可能なアップデート（Available Updates）] で該当する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て、FMC を選択します。

パッチのアンインストーラには、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` が含まれています。FMC 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が自動的に作成されます。アンインストーラがない場合は、Cisco TAC までお問い合わせください。

ステップ 3 [インストール（Install）] をクリックしてから、アンインストールすることを確認して再起動します。

ログアウトするまで、メッセージセンターでアンインストールの進行状況を確認します。

ステップ 4 可能なときに再度ログインし、アンインストールが成功したことを確認します。

ログイン時にアンインストールの成功メッセージが表示されない場合は、[ヘルプ（Help）] > [バージョン情報（About）] の順に選択して、現在のソフトウェアのバージョン情報を表示します。

ステップ 5 管理対象デバイスに構成を再展開します。

高可用性 FMC パッチのアンインストール

FMC パッチのアンインストールには Web インターフェイスを使用することをお勧めします。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、 ロックダウンを元に戻すために Cisco TAC にご連絡ください。

高可用性ピアから一度に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。

注意 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。 アンインストール中に設定の変更を行ったり、展開したりしないでください。システムが非アクティブに見えても、進行中のアンインストールを手動で再起動、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。

始める前に

- アンインストールによってFMCのパッチレベルが管理対象デバイスより低くなる場合は、最初にデバイスからパッチをアンインストールします。
- 正常に展開され、通信が確立されていることを確認します。

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 アクティブ状態の FMC で、同期を一時停止します。

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、[同期の一時停止（Pause Synchronization）] をクリックします。

ステップ 3 ピア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パッチのアンインストール （112ページ）」の手順に従います。ただし、初期の展開は省略し、各ピアでアンインストールが成功したことを確認したら停止します。要約すると、各ピアで次の手順を実行します。

a) [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。
b) 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。
c) アンインストールが成功したことを確認します。

ステップ 4 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 5 管理対象デバイスに構成を再展開します。

翻訳について
このドキュメントは、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。