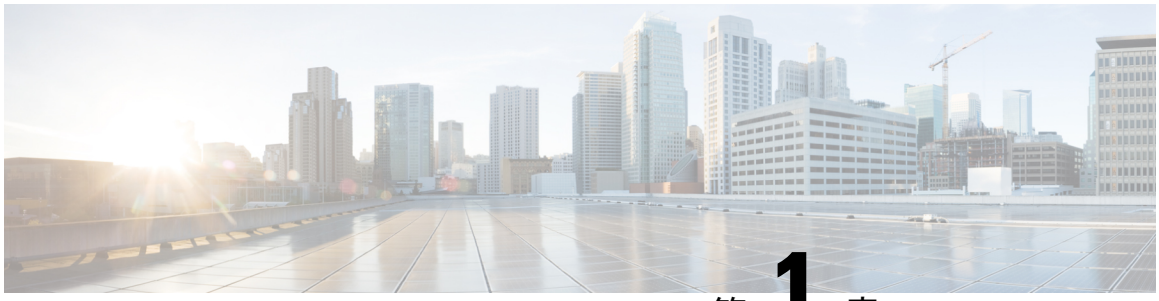
Cisco Firepower Management Center バージョン 6.0 ～ 7.0 アップグレードガイド

初版：2018 年 3 月 29 日

最終更新：2023 年 4 月 20 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

このガイドの対象読者

本ガイドでは、次のようなFirepowerバージョン**7.0.x 以前**へ正常にアップグレードを準備、および正常に完了する方法について説明します。

- Firepower Management Center（FMC）
- Firepower 4100/9300 用の FXOS を含む、FMC を搭載した Firepower Threat Defense（FTD）デバイス
- FMC を搭載した 7000/8000 シリーズのデバイス
- FMC を搭載した NGIPSv デバイス
- ASA OS を含む、FMC を搭載した ASA FirePOWER デバイス

関連リソース

別のプラットフォームまたはコンポーネントをアップグレードする場合、または別のバージョンにアップグレードする場合は、これらのリソースのいずれか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』

現在の FMC のバージョン	ガイド
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 *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。

機能の履歴

表 *6 :* 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 *7*：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 *8* : バージョン *6.6.0* の機能

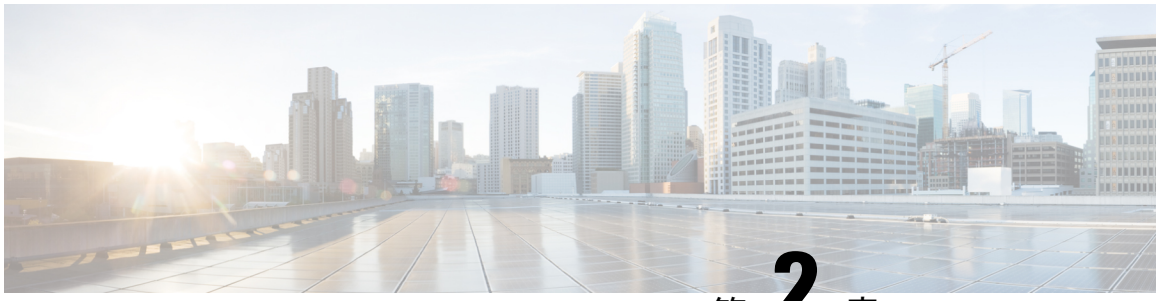
機能	説明
内部 Web サーバーからデバイス アップグレードパッケージを取得します。	デバイスは、FMC からではなく、独自の内部 Web サーバーからアップグレードパッケージを取得できるようになりました。これは、FMC とそのデバイスの間の帯域幅が制限されている場合に特に役立ちます。また、FMC 上の容量も節約できます。 新規/変更された画面：[システム（System）] > [更新（Updates）] > [更新のアップロード（Upload Update）] ボタン > [ソフトウェア更新ソースの指定（Specify Software Update Source）] オプション
アップグ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 *9 :* 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 *10 :* 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）]**



第 2 章

アップグレードの計画

アップグレードの計画フェーズ

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

表 *11* : 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。

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

現在のバージョンおよびモジュールの情報

これらのコマンドを使用して、展開に関する現在のバージョンとモデルの情報を検索します。

表 12：

コンポーネント	情報
Firepower Management Center	FMC で、**[ヘルプ（Help）]** > **[概要（About）]** を選択します。
Firepower 管理対象のデバイス	FMC で、**[デバイス（Devices）]**>**[デバイス管理（Device Management）]** を選択します。
Firepower 4100/9300 用 FXOS	Firepower Chassis Manager：[概要（Overview）] を選択します。 FXOS CLI：バージョンについては、**show version** コマンドを使用します。モデルについては、**scope chassis 1** を入力し、次に **show inventory** を入力します。

コンポーネント	情報
ASA with FirePOWER Services 用 ASA OS	ASA CLI で、**show version** コマンドを使用します。
仮想ホスティング環境	仮想ホスティング環境のドキュメンテーションを参照してください。

アップグレードパス

アップグレードパスは、仮想ホスティング環境やアプライアンスのオペレーティングシステムなどを含め、何をいつアップグレードするかについての詳細な計画です。常に、ハードウェア、ソフトウェア、オペレーティングシステム、およびホスティングの互換性を維持する必要があります。

ヒント　このガイドでは、Firepower 7.0.x 以前について説明します。このガイドの対象読者 （1 ページ）を参照してください

何を持っているのか？

Firepower アプライアンスをアップグレードする前に、展開の現在の状態を判断します。現在のバージョンとモデル情報に加えて、デバイスが高可用性/拡張性を実現するように設定されているかどうか、および IPS、ファイアウォールなどとしてパッシブに展開されているかどうかを確認します。

現在のバージョンおよびモジュールの情報 （12 ページ）を参照してください。

どこへ行くのか？

持っているものがわかったので、行きたい場所に行けることを確認します。

- 展開で対象の Firepower バージョンを実行できるのか？
- アプライアンスでは、対象の Firepower バージョンを実行する前に、個別のオペレーティングシステムのアップグレードが必要となるか？アプライアンスは対象の OS を実行できるのか？
- 仮想アプライアンスでは対象の Firepower バージョンを実行する前に、ホスティング環境のアップグレードが必要となるのか？

これらすべての質問に対する回答については、次のいずれかを参照してください。

- Cisco Secure Firewall Management Center 互換性ガイド
- Cisco Secure Firewall Threat Defense 互換性ガイド
- Cisco Firepower Classic Device 互換性ガイド

アクセス方法は？

アプライアンスが対象のバージョンを実行できることを確認したら、直接アップグレードが可能であることを確認します。

- Firepower ソフトウェアを直接アップグレードできるのか？
- Firepower 4100/9300 では、FXOS を直接アップグレードできるのか？
- FirePOWER サービスを搭載した ASA では、ASA を直接アップグレードできるのか？

これらすべての質問に対する回答については、本ガイドに記載されているアップグレードパスを参照してください。

ヒント　中間バージョンを必要とするアップグレードパスには時間がかかる場合があります。特に、FMC とデバイスのアップグレードを交互に行う必要がある大規模な Firepower の展開では、アップグレードする代わりに古いデバイスのイメージを再作成することを検討してください。まず、FMC からデバイスを削除します。その後、FMC をアップグレードし、デバイスを再イメージ化してから、それらを FMC に再追加します。

展開の互換性を維持できるのか？

常に、ハードウェア、ソフトウェア、オペレーティングシステムの互換性を維持する必要があります。

- FMC とその管理対象デバイス間の Firepower バージョンの互換性を維持できるのか？Cisco Secure Firewall Management Center 互換性ガイド
- Firepower 4100/9300 では、論理デバイスとの FXOS の互換性を維持できるのか？Cisco Firepower 4100/9300 FXOS の互換性
- FirePOWER サービスを搭載した ASA では、ASA FirePOWER モジュールとの ASA の互換性を維持できるのか？Cisco Secure Firewall ASA の互換性

アップグレードパス：Firepower Management Center

次の表に FMC（FMCv を含む）のアップグレードパスを示します。

左側の列で現在のバージョンを確認します。右側の列に記載されているバージョンに直接アップグレードできます。

（注）　現在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 *13 : 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
7.0.0 7.0.x FMC 1000、2500、4500 に対する最後のサポート	→ 7.0.x 以降のメンテナンスリリース
6.7.0 6.7.x	次のいずれかです。 → 7.0.0 または 7.0.x のいずれかのメンテナンスリリース → 6.7.x メンテナンスリリース以降
6.6.0 6.6.x FMC 2000 および 4000 の最後のサポート。	次のいずれかです。 → 7.0.0 または 7.0.x のいずれかのメンテナンスリリース → 6.7.0 または 6.7.x メンテナンスリリース → 6.6.x メンテナンスリリース以降 **注**：データストアの非互換性のため、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 7.0.0 以降に直接アップグレードすることをお勧めします。
6.5.0	次のいずれかです。 → 7.0.0 または 7.0.x のいずれかのメンテナンスリリース → 6.7.0 または 6.7.x メンテナンスリリース → 6.6.0 または 6.6.x メンテナンスリリース
6.4.0 FMC 750、1500、および 3500 の最後のサポート。	次のいずれかです。 → 7.0.0 または 7.0.x のいずれかのメンテナンスリリース → 6.7.0 または 6.7.x メンテナンスリリース → 6.6.0 または 6.6.x メンテナンスリリース → 6.5.0

現在のバージョン	ターゲットバージョン
6.3.0	次のいずれかです。 → 6.7.0 または 6.7.x メンテナンスリリース → 6.6.0 または 6.6.x メンテナンスリリース → 6.5.0 →6.4.0
6.2.3	次のいずれかです。 → 6.6.0 または 6.6.x メンテナンスリリース → 6.5.0 →6.4.0 → 6.3.0
6.2.2	次のいずれかです。 →6.4.0 → 6.3.0 → 6.2.3
6.2.1	次のいずれかです。 →6.4.0 → 6.3.0 → 6.2.3 → 6.2.2
6.2.0	次のいずれかです。 →6.4.0 → 6.3.0 → 6.2.3 → 6.2.2
6.1.0	次のいずれかです。 →6.4.0 → 6.3.0 → 6.2.3 → 6.2.0

現在のバージョン	ターゲットバージョン
6.0.1	次のいずれかです。 → 6.1.0
6.0.0	次のいずれかです。 → 6.0.1 次のプレインストールパッケージが必要です：Firepower System Release Notes Version 6.0.1 Preinstallation。
5.4.1.1	次のいずれかです。 → 6.0.0 次のプレインストールパッケージが必要です：FireSIGHT System Release Notes Version 6.0.0 Preinstallation。

アップグレード パス：FTD 論理デバイス を備えた Firepower 4100/9300

この表は、Firepower Management Center によって管理される FTD 論理デバイスを搭載した Firepower 4100/9300 のアップグレードパスを示しています。

（注） 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 シャーシをアップグレードする場合は、『Cisco Firepower 4100/9300 Upgrade Guide, Firepower 6.0.1–7.0.x or ASA 9.4(1)–9.16(x) with FXOS 1.1.1–2.10.1』を参照してください。

左側の列で現在のバージョンの組み合わせを確認します。右側の列に記載されているバージョンの組み合わせにアップグレードできます。これは複数のステップからなるプロセスであり、最初に FXOS をアップグレードしてから、次に論理デバイスをアップグレードします。

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ることに注意してください。最初にFXOSをアップグレードする必要があるため、サポートされている（ただし推奨されません）組み合わせを簡単に実行します。ここでは、FXOS が論理デバイスの「前」にあります。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 Firepower 4100/9300 FXOS の互換性 』を参照してください。

（注） FXOS の初期バージョンの場合、すべて現在のバージョンと対象バージョンの間の中間バージョンにアップグレードする必要があります。FXOS 2.2.2 になると、アップグレードのオプションが広がります。

表 *14 :* アップグレード パス：*FTD* 論理デバイス を搭載した *Firepower 4100/9300*

現在のバージョン	対象のバージョン
FTD 6.7.0/6.7.x を搭載した FXOS 2.9.1	→ FTD 7.0.0/7.0.x を搭載した FXOS 2.10.1
FTD 6.6.0/6.6.x を搭載した FXOS 2.8.1	次のいずれかです。 → FTD 7.0.0/7.0.x を搭載した FXOS 2.10.1 → FTD 6.7.x を搭載した FXOS 2.9.1
FTD 6.5.0 を搭載した FXOS 2.7.1	次のいずれかです。 → FTD 7.0.0/7.0.x を搭載した FXOS 2.10.1 → FTD 6.7.0/6.7.x を搭載した FXOS 2.9.1 → FTD 6.6.0/6.6.x を搭載した FXOS 2.8.1
FTD 6.4.0 を搭載した FXOS 2.6.1	次のいずれかです。 → FTD 7.0.0/7.0.x を搭載した FXOS 2.10.1 → FTD 6.7.0/6.7.x を搭載した FXOS 2.9.1 → FTD 6.6.0/6.6.x を搭載した FXOS 2.8.1 → FTD 6.5.0 を搭載した FXOS 2.7.1
FTD 6.3.0 を搭載した FXOS 2.4.1	次のいずれかです。 → FTD 6.7.0/6.7.x を搭載した FXOS 2.9.1 → FTD 6.6.0/6.6.x を搭載した FXOS 2.8.1 → FTD 6.5.0 を搭載した FXOS 2.7.1 → FTD 6.4.0 を搭載した FXOS 2.6.1
FTD 6.2.3 を搭載した FXOS 2.3.1	次のいずれかです。 → FTD 6.6.0/6.6.x を搭載した FXOS 2.8.1 → FTD 6.5.0 を搭載した FXOS 2.7.1 → FTD 6.4.0 を搭載した FXOS 2.6.1 → FTD 6.3.0 を搭載した FXOS 2.4.1
FTD 6.2.2 を搭載した FXOS 2.2.2	次のいずれかです。 → FTD 6.4.0 を搭載した FXOS 2.6.1 → FTD 6.3.0 を搭載した FXOS 2.4.1 → FTD 6.2.3 を搭載した FXOS 2.3.1

現在のバージョン	対象のバージョン
FTD 6.2.0 を搭載した FXOS 2.2.2	次のいずれかです。 → FTD 6.4.0 を搭載した FXOS 2.6.1 → FTD 6.3.0 を搭載した FXOS 2.4.1 → FTD 6.2.3 を搭載した FXOS 2.3.1 → FTD 6.2.2 を搭載した FXOS 2.2.2
FTD 6.2.0 を搭載した FXOS 2.2.1	→ FTD 6.2.0 を搭載した FXOS 2.2.2（FXOS のみをアップグレード） もう 1 つのオプションは、推奨される組み合わせである FTD 6.2.2 を搭載した FXOS 2.2.2 にアップグレードすることです。ただし、展開をさらにアップグレードする予定がある場合は、気にしないでください。FXOS 2.2.2 を実行しているので、FTD 6.4.0 を搭載した FXOS 2.6.1 にアップグレードできます。
FTD 6.2.0 を搭載した FXOS 2.1.1	→ FTD 6.2.0 を搭載した FXOS 2.2.1（FXOS のみをアップグレード）
FTD 6.1.0 を搭載した FXOS 2.0.1	→ FTD 6.2.0 を搭載した FXOS 2.1.1
FTD 6.0.1 を搭載した FXOS 1.1.4	→ FTD 6.1.0 を搭載した FXOS 2.0.1

クラスタまたは HA ペアの FTD 論理デバイスを搭載した FXOS のアップグレード

Firepower Management Center の展開では、クラスタ化された高可用性の FTD 論理デバイスを 1 つのユニットとしてアップグレードします。ただし、各シャーシの FXOS を個別にアップグレードします。

表 *15 : FXOS + FTD* のアップグレード順序

展開	アップグレード順序
スタンドアロンデバイス クラスタ、同じシャーシ上のユニット（Firepower 9300 のみ）	**1.** FXOS をアップグレードします。 **2.** FTD のアップグレード。

展開	アップグレード順序
ハイ アベイラビリティ	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.** 新しいスタンバイの FXOS をアップグレードします。 **4.** FTD のアップグレード。
クラスタ、異なるシャーシ上のユニット（6.2+）	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。たとえば、2 つのシャーシがあるクラスタの場合： **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.** 新しい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。 **4.** FTD のアップグレード。

古いバージョンでは、無中断アップグレードにはいくつかの追加要件があります。

表 *16*：古いバージョンでの無中断アップグレード

シナリオ	詳細
高可用性またはクラスタ化されたデバイスのアップグレードで、現在次のいずれかを実行しています。 • FXOS 1.1.4.x ～ 2.2.1.x • FXOS 2.2.2.17 ～ FXOS 2.2.2.68 • FXOS 2.3.1.73 ～ FXOS 2.3.1.111 次の場合： • FTD 6.0.1 ～ 6.2.2.x	フローオフロード機能でのバグ修正により、FXOS と FTD のいくつかの組み合わせはフローオフロードをサポートしていません。『Cisco Firepower Compatibility Guide』を参照してください。無中断アップグレードを実施するには、常に互換性のある組み合わせを実行する必要があります。 アップグレードパスに FXOS の2.2.2.91、2.3.1.130、またはそれ以降のアップグレード（FXOS 2.4.1. x、2.6.1 などを含む）が含まれている場合、次のパスを使用します。 1. FTD を 6.2.2.2 以降にアップグレードします。 2. FXOS を 2.2.2.91、2.3.1.130、またはそれ以降にアップグレードします。 3. FTD を最終バージョンにアップグレードします。 たとえば、FTD 6.2.2.0 を搭載した FXOS 2.2.2.17 を実行していて、FTD 6.4.0 を搭載した FXOS 2.6.1 にアップグレードする場合は、次を実行できます。 1. FTD を 6.2.2.5 にアップグレードします。 2. FXOS を 2.6.1 にアップグレードします。 3. FTD を 6.4.0 にアップグレードします。
高可用性デバイスの FTD バージョン 6.1.0 へのアップグレード	プレインストールパッケージが必要です。詳細については、『Firepower System Release Notes Version 6.1.0 Preinstallation Package』を参照してください。

ダウングレードについての注記

FXOS イメージのダウングレードは公式にはサポートされていません。シスコがサポートする唯一の FXOS のイメージバージョンのダウングレード方法は、デバイスの完全な再イメージ化を実行することです。

アップグレードパス：その他の Firepower Threat Defense デバイス

この表は、オペレーティングシステムを更新する必要がない、FMC によって管理される FTD デバイスのアップグレードパスを示しています Firepower 1000/2100 シリーズ、ASA 5500-X シリーズ、ISA 3000、および Firepower Threat Defense Virtual。

左側の列で現在のバージョンを確認します。右側の列に記載されているバージョンに直接アップグレードできます。

表 *17 :* アップグレードパス：*FMC* を搭載した *Firepower 1000/2100* シリーズ、*ASA 5500-X* シリーズ、*ISA 3000*、および *Firepower Threat Defense Virtual*

現在のバージョン	ターゲットバージョン
7.0.0 7.0.x ASA 5508-X および 5516-X における最後の FTD サポート	→ 7.0.x 以降のメンテナンスリリース
6.7.0 6.7.x	次のいずれかです。 → 7.0.0 または 7.0.x のいずれかのメンテナンスリリース → 6.7.x メンテナンスリリース以降
6.6.0 6.6.x ASA 5525-X、5545-X、5555-X における最後の FTD サポート。	次のいずれかです。 → 7.0.0 または 7.0.x のいずれかのメンテナンスリリース → 6.7.0 または 6.7.x メンテナンスリリース → 6.6.x メンテナンスリリース以降
6.5.0	次のいずれかです。 → 7.0.0 または 7.0.x のいずれかのメンテナンスリリース → 6.7.0 または 6.7.x メンテナンスリリース → 6.6.0 または 6.6.x メンテナンスリリース
6.4.0 ASA 5515-X における最後の FTD サポート	次のいずれかです。 → 7.0.0 または 7.0.x のいずれかのメンテナンスリリース → 6.7.0 または 6.7.x メンテナンスリリース → 6.6.0 または 6.6.x メンテナンスリリース → 6.5.0
6.3.0	次のいずれかです。 → 6.7.0 または 6.7.x メンテナンスリリース → 6.6.0 または 6.6.x メンテナンスリリース → 6.5.0 →6.4.0

現在のバージョン	ターゲットバージョン
6.2.3 ASA 5506-X シリーズにおける最後の FTD サポート	次のいずれかです。 → 6.6.0 または 6.6.x メンテナンスリリース → 6.5.0 →6.4.0 → 6.3.0
6.2.2	次のいずれかです。 →6.4.0 → 6.3.0 → 6.2.3
6.2.1 Firepower 2100 シリーズのみ。	次のいずれかです。 →6.4.0 → 6.3.0 → 6.2.3 → 6.2.2
6.2.0	次のいずれかです。 →6.4.0 → 6.3.0 → 6.2.3 → 6.2.2
6.1.0	次のいずれかです。 →6.4.0 → 6.3.0 → 6.2.3 → 6.2.0
6.0.1	→ 6.1.0

アップグレードパス：Firepower 7000/8000 シリーズ

この表に、FMC によって管理される Firepower 7000/8000 シリーズデバイスのアップグレードパスを示します。

左側の列で現在のバージョンを確認します。右側の列に記載されているバージョンに直接アップグレードできます。

表 *18 :* アップグレードパス：*FMC* を搭載した *Firepower 7000/8000* シリーズ

現在のバージョン	ターゲットバージョン
6.4.0	なし。 バージョン 6.4.0 は、Firepower 7000/8000 シリーズ デバイスの最後のメジャーリリースです。
6.3.0	次のいずれかです。 →6.4.0
6.2.3	次のいずれかです。 →6.4.0 → 6.3.0
6.2.2	次のいずれかです。 →6.4.0 → 6.3.0 → 6.2.3
6.2.1 このプラットフォームではサポートされていません。	—
6.2.0	次のいずれかです。 →6.4.0 → 6.3.0 → 6.2.3 → 6.2.2
6.1.0	次のいずれかです。 →6.4.0 → 6.3.0 → 6.2.3 → 6.2.0
6.0.1	次のいずれかです。 → 6.1.0

現在のバージョン	ターゲットバージョン
6.0.0	次のいずれかです。 → 6.0.1
5.4.0.2	次のいずれかです。 → 6.0.0 次のプレインストールパッケージが必要です：FireSIGHT System Release Notes Version 6.0.0 Preinstallation。

アップグレードパス： ASA FirePOWER

この表に、FMC によって管理される ASA FirePOWER module のアップグレードパスを示します。

左側の列で現在のバージョンを確認します。右側の列に記載されているバージョンに直接アップグレードできます。

必要に応じて、ASA もアップグレードできます。ASA と ASA FirePOWER のバージョンには幅広い互換性があります。ただし、アップグレードすると、新機能を利用でき、問題も解決されます。 ASA のアップグレードパスについては、アップグレードパス：ASA FirePOWER 用 ASA （29 ページ） を参照してください。

表 *19*：アップグレードパス：*FMC* を搭載した *ASA FirePOWER*

現在のバージョン	ターゲットバージョン
7.0.0 7.0.x 任意のプラットフォームにおける最後の ASA FirePOWER のサポート。	→ 7.0.x 以降のメンテナンスリリース
6.7.0 6.7.x	次のいずれかです。 → 7.0.0 または 7.0.x のいずれかのメンテナンスリリース → 6.7.x メンテナンスリリース以降
6.6.0 6.6.x ASA 5525-X、5545-X、5555-X での最後の ASA FirePOWER のサポート。	次のいずれかです。 → 7.0.0 または 7.0.x のいずれかのメンテナンスリリース → 6.7.0 または 6.7.x メンテナンスリリース → 6.6.x メンテナンスリリース以降

現在のバージョン	ターゲットバージョン
6.5.0	次のいずれかです。 → 7.0.0 または 7.0.x のいずれかのメンテナンスリリース → 6.7.0 または 6.7.x メンテナンスリリース → 6.6.0 または 6.6.x メンテナンスリリース
6.4.0 ASA 5585-X シリーズおよび ASA 5515-X での最後の ASA FirePOWER のサポート。	次のいずれかです。 → 7.0.0 または 7.0.x のいずれかのメンテナンスリリース → 6.7.0 または 6.7.x メンテナンスリリース → 6.6.0 または 6.6.x メンテナンスリリース → 6.5.0
6.3.0	次のいずれかです。 → 6.7.0 または 6.7.x メンテナンスリリース → 6.6.0 または 6.6.x メンテナンスリリース → 6.5.0 →6.4.0
6.2.3 ASA 5506-x シリーズおよび ASA 5512-x での最後の ASA FirePOWER のサポート。	次のいずれかです。 → 6.6.0 または 6.6.x メンテナンスリリース → 6.5.0 →6.4.0 → 6.3.0
6.2.2	次のいずれかです。 →6.4.0 → 6.3.0 → 6.2.3
6.2.1 このプラットフォームではサポートされていません。	—

現在のバージョン	ターゲットバージョン
6.2.0	次のいずれかです。 →6.4.0 → 6.3.0 → 6.2.3 → 6.2.2
6.1.0	次のいずれかです。 →6.4.0 → 6.3.0 → 6.2.3 → 6.2.0
6.0.1	次のいずれかです。 → 6.1.0
6.0.0	次のいずれかです。 → 6.0.1
5.4.0.2 または 5.4.1.1	次のいずれかです。 → 6.0.0 次のプレインストールパッケージが必要です：FireSIGHT System Release Notes Version 6.0.0 Preinstallation。

ASA のアップグレード

ASA と ASA FirePOWER のバージョンには幅広い互換性があります。ただし、アップグレードすると、新機能を利用でき、問題も解決されます。詳細な互換性情報については、「Cisco Secure Firewall ASA の互換性」を参照してください。

ASA クラスタリングまたはフェールオーバーペアが設定されていても、デバイスごとに個別に ASA をアップグレードします。ASA FirePOWER モジュールをアップグレードする正確なタイミング（ASA のリロードの前か後か）は、展開によって異なります。次の表に、スタンドアロンおよび HA/スケーラビリティ展開の ASA アップグレード順序の概要を示します。詳細な手順については、「ASA のアップグレード （106 ページ）」を参照してください。

表 ***20 : ASA + ASA FirePOWER*** のアップグレード順序

ASA 展開	アップグレード順序
スタンドアロンデバイス	**1.** ASA をアップグレードします（リロードを含む）。 **2.** ASA FirePOWER をアップグレードします。
ASA フェールオーバー：アクティブ/スタンバイ	スタンバイを常にアップグレードします。 **1.** スタンバイの ASA をアップグレードします（ただし、リロードしません）。 **2.** スタンバイの ASA FirePOWER をアップグレードします。 **3.** スタンバイの ASA をリロードします。 **4.** フェールオーバーします。 **5.** 新しいスタンバイの ASA をアップグレードします。 **6.** 新しいスタンバイの ASA FirePOWER をアップグレードします。 **7.** 新しいスタンバイの ASA をリロードします。
ASA フェールオーバー：アクティブ/スタンバイ	アップグレードしないユニットの両方のフェールオーバーグループをアクティブにします。 **1.** プライマリの両方のフェールオーバーグループをアクティブにします。 **2.** セカンダリの ASA をアップグレードします（ただし、リロードしません）。 **3.** セカンダリの ASA FirePOWER をアップグレードします。 **4.** セカンダリの ASA をリロードします。 **5.** セカンダリの両方のフェールオーバーグループをアクティブにします。 **6.** プライマリの ASA をアップグレードします（ただし、リロードしません）。 **7.** プライマリの ASA FirePOWER をアップグレードします。 **8.** プライマリの ASA をリロードします。

ASA 展開	アップグレード順序
ASA クラスタ	アップグレードの前に、各ユニットでクラスタリングを無効にします。一度に1つのユニットからアップグレードし、制御ユニットを最後に残します。 **1.** データユニットでクラスタリングを無効にします。 **2.** そのデータユニットのASAをアップグレードします（ただし、リロードしません）。 **3.** ユニットの ASA FirePOWER をアップグレードします。 **4.** ASA をリロードします。 **5.** クラスタリングを再び有効にします。ユニットが再びクラスタに参加するのを待ちます。 **6.** 各データユニットに対して手順を繰り返します。 **7.** 制御ユニットでクラスタリングを無効にします。新しい制御ユニットが引き継ぐまで待ちます。 **8.** 前の制御ユニットのASAをアップグレードします（ただし、リロードしません）。 **9.** 前の制御ユニットのASA FirePOWERをアップグレードします。 **10.** クラスタリングを再び有効にします。

アップグレードパス：ASA FirePOWER 用 ASA

この表は、FirePOWER サービスを使用した ASA 上の ASA 用のアップグレード パスを示します。 ASA と ASA FirePOWER のバージョンには幅広い互換性があります。ただし、アップグレードすると、新機能を利用でき、問題も解決されます。

左側の列で現在ASAのバージョンを確認します。記載されている対象のバージョンに直接アップグレードできます。推奨バージョンは**太字**で示されています。

表 *21 :* アップグレードパス：*ASA FirePOWER* 用 *ASA*

現在のバージョン	ターゲットバージョン
9.15(x) Firepower バージョン 7.0.x を搭載した、任意のプラットフォームでの最後の ASA FirePOWER のサポート。	→ **9.16(x)**

現在のバージョン	ターゲットバージョン
9.14(x) Firepower バージョン 6.6.x を搭載した、ASA 5525-X、ASA 5545-X、ASA 5555-X での最後の ASA FirePOWER のサポート。	次のいずれかです。 → **9.16(x)** → **9.15(x)**
9.13(x)	次のいずれかです。 → **9.16(x)** → **9.15(x)** → **9.14(x)** → **9.13(x)**
9.12(x) Firepower バージョン 6.4.0 を搭載した、ASA 5515-X および ASA 5585-X での最後の ASA FirePOWER のサポート。	次のいずれかです。 → **9.16(x)** → **9.15(x)** → **9.14(x)** → **9.13(x)** → **9.12(x)**
9.10(x)	次のいずれかです。 → **9.16(x)** → **9.15(x)** → **9.14(x)** → **9.13(x)** → **9.12(x)** → 9.10(x)
9.9(x) Firepower バージョン 6.2.3 を搭載した、ASA 5506-X シリーズおよび ASA 5512-X での最後の ASA FirePOWER のサポート。	次のいずれかです。 → **9.15(x)** → **9.14(x)** → **9.13(x)** → **9.12(x)** → 9.10(x) → 9.9(x)

現在のバージョン	ターゲットバージョン
9.8(x)	次のいずれかです。 → **9.16(x)** → **9.15(x)** → **9.14(x)** → **9.13(x)** → **9.12(x)** → 9.10(x) → 9.9(x) → **9.8(x)**
9.7(x)	次のいずれかです。 → **9.16(x)** → **9.15(x)** → **9.14(x)** → **9.13(x)** → **9.12(x)** → 9.10(x) → 9.9(x) → **9.8(x)**
9.6(x)	次のいずれかです。 → **9.16(x)** → **9.15(x)** → **9.14(x)** → **9.13(x)** → **9.12(x)** → 9.10(x) → 9.9(x) → **9.8(x)** → 9.6(x)

現在のバージョン	ターゲットバージョン
9.5(x)	次のいずれかです。 → **9.16(x)** → **9.15(x)** → **9.14(x)** → **9.13(x)** → **9.12(x)** → 9.10(x) → 9.9(x) → **9.8(x)** → 9.6(x)
9.4(x)	次のいずれかです。 → **9.16(x)** → **9.15(x)** → **9.14(x)** → **9.12(x)** → 9.10(x) → 9.9(x) → **9.8(x)** → 9.6(x)
9.3(x)	次のいずれかです。 → **9.16(x)** → **9.15(x)** → **9.14(x)** → **9.13(x)** → **9.12(x)** → 9.10(x) → 9.9(x) → **9.8(x)** → 9.6(x)

現在のバージョン	ターゲットバージョン
9.2(x)	次のいずれかです。 → **9.16(x)** → **9.15(x)** → **9.14(x)** → **9.13(x)** → **9.12(x)** → 9.10(x) → 9.9(x) → **9.8(x)** → 9.6(x)

アップグレードパス：**NGIPSv**

この表に、FMC によって管理される NGIPSv のアップグレードパスを示します。

左側の列で現在のバージョンを確認します。右側の列に記載されているバージョンに直接アップグレードできます。

表 *22*：アップグレードパス：*FMC* を搭載した *NGIPSv*

現在のバージョン	ターゲットバージョン
7.0.0 7.0.x 最後の NGIPSv のサポート。	→ 7.0.x 以降のメンテナンスリリース
6.7.0 6.7.x	次のいずれかです。 → 7.0.0 または 7.0.x のいずれかのメンテナンスリリース → 6.7.x メンテナンスリリース以降
6.6.0 6.6.x	次のいずれかです。 → 7.0.0 または 7.0.x のいずれかのメンテナンスリリース → 6.7.0 または 6.7.x メンテナンスリリース → 6.6.x メンテナンスリリース以降

現在のバージョン	ターゲットバージョン
6.5.0	次のいずれかです。 → 7.0.0 または 7.0.x のいずれかのメンテナンスリリース → 6.7.0 または 6.7.x メンテナンスリリース → 6.6.0 または 6.6.x メンテナンスリリース
6.4.0	次のいずれかです。 → 7.0.0 または 7.0.x のいずれかのメンテナンスリリース → 6.7.0 または 6.7.x メンテナンスリリース → 6.6.0 または 6.6.x メンテナンスリリース → 6.5.0
6.3.0	次のいずれかです。 → 6.7.0 または 6.7.x メンテナンスリリース → 6.6.0 または 6.6.x メンテナンスリリース → 6.5.0 →6.4.0
6.2.3	次のいずれかです。 → 6.6.0 または 6.6.x メンテナンスリリース → 6.5.0 →6.4.0 → 6.3.0
6.2.2	次のいずれかです。 →6.4.0 → 6.3.0
6.2.1 このプラットフォームではサポートされていません。	—

現在のバージョン	ターゲットバージョン
6.2.0	次のいずれかです。 →6.4.0 → 6.3.0 → 6.2.3 → 6.2.2
6.1.0	次のいずれかです。 →6.4.0 → 6.3.0 → 6.2.3 → 6.2.0
6.0.1	次のいずれかです。 → 6.1.0
6.0.0	次のいずれかです。 → 6.0.1
5.4.1.1	次のいずれかです。 → 6.0.0 次のプレインストールパッケージが必要です：FireSIGHT System Release Notes Version 6.0.0 Preinstallation。

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 または従来のデバイスのアップグレード

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。

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。実際のレポートについては、対象バージョンのリリースノートを参照してください。

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 （35 ページ） を参照してください。

表 *23 :* 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 *24*：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。

アップグレードパッケージのダウンロード

アップグレードを開始する前に シスコ サポートおよびダウンロード サイト からアップグレードパッケージをダウンロードしてください。特定のアップグレードに応じて、ローカルコンピュータまたはアプライアンスがアクセスできるサーバーにパッケージを配置する必要があります。このガイドの個々のチェックリストと手順では、選択肢について説明します。

（注） ダウンロードには、Cisco.com のログインおよびサービス契約が必要です。

Firepower ソフトウェア パッケージ

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

- Firepower Management Center Virtual を含む Firepower Management Center： https://www.cisco.com/go/firepower-software
- Firepower Threat Defense（ISA 3000）： https://www.cisco.com/go/isa3000-software
- Firepower Threat Defense（Firepower Threat Defense Virtual を含む他のすべてのモデル）： https://www.cisco.com/go/ftd-software
- FirePOWER 7000 シリーズ： https://www.cisco.com/go/7000series-software
- FirePOWER 8000 シリーズ： https://www.cisco.com/go/8000series-software
- ASA with FirePOWER Services（ASA 5500-X シリーズ）： https://www.cisco.com/go/asa-firepower-sw
- ASA with FirePOWER Services（ISA 3000）： https://www.cisco.com/go/isa3000-software
- NGIPSv： https://www.cisco.com/go/ngipsv-software

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

ヒント インターネットにアクセスできる Firepower Management Center では、リリースが手動でダウンロードできるようになった後しばらくしてから、シスコから選択したリリースを直接ダウンロードできます。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。

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。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）、およびソフトウェアバージョンが反映されています。 メンテナンスリリースでは、アップグレード パッケージ タイプが使用されます。

次に例を示します。

- パッケージ：`Cisco_Firepower_Mgmt_Center_Upgrade--999.sh.REL.tar`
- プラットフォーム： Firepower Management Center
- パッケージタイプ：アップグレード
- バージョンとビルド：-999
- ファイル拡張子：sh.REL.tar

システムでは、正しいファイルを使用していることを確認できるようにするために、バージョン 6.2.1 以上からのアップグレードパッケージは、署名付きの tar アーカイブ（.tar）になっています。署名付きの（.tar）パッケージは解凍しないでください。また、アップグレードパッケージを電子メールで転送しないでください。

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

Firepower ソフトウェア アップグレード パッケージ

表 *25 :*

Platform	バージョン	パッケージ
FMC/FMCv	6.3.0 以降	Cisco_Firepower_Mgmt_Center
	5.4.0 ～ 6.2.3	Sourcefire_3D_Defense_Center_S3
Firepower 1000 シリーズ	いずれか	Cisco_FTD_SSP-FP1K
Firepower 2100 シリーズ	いずれか	Cisco_FTD_SSP-FP2K
Firepower 4100/9300	いずれか	Cisco_FTD_SSP
FTD を搭載した ASA 5500-X シリーズ FTD を使用した ISA 3000 FTDv	いずれか	Cisco_FTD
Firepower 7000/8000 シリーズ AMP モデル	6.3.0 ～ 6.4.0	Cisco_Firepower_NGIPS_Appliance
	5.4.0 ～ 6.2.3	Sourcefire_3D_Device_S3
ASA FirePOWER	いずれか	Cisco_Network_Sensor
NGIPSv	6.3.0 以降	Cisco_Firepower_NGIPS_Virtual
	6.2.2 ～ 6.2.3	Sourcefire_3D_Device_VMware
	5.4.0 ～ 6.2.0	Sourcefire_3D_Device_Virtual64_VMware

FXOS パッケージ

Firepower 4100/9300 用の FXOS 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 で利用できます。

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

FXOSパッケージを見つけるには、Firepowerアプライアンスモデルを選択または検索し、対象バージョンの Firepower Extensible Operating System のダウンロードページを参照します。

（注） CLI を使用して FXOS をアップグレードする場合は、Firepower 4100/9300 が SCP、SFTP、TFTP、または FTP を使用してアクセスできるサーバーにアップグレードパッケージをコピーします。

表 *26 : Firepower 4100/9300* 用 *FXOS* パッケージ

パッケージ タイプ	パッケージ
FXOS イメージ	fxos-k9.*version*.**SPA**
リカバリ（キックスタート）	fxos-k9-**kickstart**.*version*.**SPA**
リカバリ（マネージャ）	fxos-k9-**manager**.*version*.**SPA**
リカバリ（システム）	fxos-k9-**system**.*version*.**SPA**
MIB	fxos-**mibs**-fp9k-fp4k.*version*.**zip**
ファームウェア：Firepower 4100 シリーズ	fxos-k9-fpr4k-**firmware**.*version*.**SPA**
ファームウェア：Firepower 9300	fxos-k9-fpr9k-**firmware**.*version*.**SPA**

ASA パッケージ

ASA ソフトウェアは シスコ サポートおよびダウンロード サイト で利用できます。

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

ASA ソフトウェアを見つけるには、使用している Firepower アプライアンスモデルを選択または検索し、適切なダウンロードページを参照して、バージョンを選択します。

（注） ASDMアップグレードウィザードを使用している場合は、事前にダウンロードする必要はありません。それ以外の場合は、ローカルコンピュータにダウンロードします。CLIアップグレードの場合、HTTP、FTP、SCP など、ASA **copy** コマンドでサポートされているプロトコルを介してデバイスがアクセスできるサーバーにソフトウェアをコピーする必要があります。

表 *27 : ASA* ソフトウェア

ダウンロードページ	ソフトウェアタイプ	パッケージ
適応型セキュリティアプライアンス（ASA）ソフトウェア	ASA および ASDM のアップグレード	asa*version*-**lfbff-k8.SPA** ASA 5506-X、ASA 5508-X、ASA 5516-X、および ISA 3000 用
		asa*version*-**smp-k8.bin** ASA 5512-X、ASA 5515-X、ASA 5525-X、ASA 5545-X、ASA 5555-X および ASA 5585-X 用
適応型セキュリティアプライアンス（ASA）デバイスマネージャ	ASDM のアップグレードのみ	asdm-*version*.**bin**
適応型セキュリティアプライアンス REST API プラグイン	ASA REST API	asa-restapi-*version*-**lfbff-k8.SPA**

Firepowerソフトウェアアップグレードパッケージのアップロード

Firepower ソフトウェア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アプライアンスにある必要があります。

Firepower Management Center にアップロード

次の手順を使用して、FMC 自体と FMC が管理するデバイス用に、手動でFirepower ソフトウェアのアップグレードパッケージを Firepower Management Center にアップロードします。

始める前に

高可用性ペアのスタンバイの Firepower Management Center 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の高可用性の展開では、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。HA 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 Firepower Management Center Web インターフェイスで **[システム（System）]** > **[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。

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、Firepower Management Center によって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。 Firepower Management Center がインターネットにアクセスできる場合は、代わりに [アップデートのダウンロード（Download updates）] をクリックして、展開の対象となるすべてのパッケージと、必要に応じて最新の VDB をダウンロードできます。

ステップ 3 （バージョン 6.6.0+）**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 [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。

内部サーバへのアップロード（FMC を使用したバージョン 6.6.0 以降の FTD）

バージョン 6.6.0 以降では、Firepower Threat Defense デバイスは、FMC からではなく内部 Web サーバからアップグレードパッケージを取得できます。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 上の領域も節約できます。

（注） この機能は、バージョン 6.6.0+ を実行している FTD デバイスでのみサポートされています。バージョン 6.6.0 へのアップグレードではサポートされておらず、FMC または従来のデバイスでもサポートされていません。

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 FTD 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

- 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、FTD デバイスがアクセスできる内部 Web サーバーにコピーします。
- 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 Web インターフェイスで、**[System]** > **[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 Firepower 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。

[製品アップデート（Product Updates）]ページに戻ります。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。

管理対象デバイスへのコピー

Firepower ソフトウェア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ある必要があります。サポートされている場合、デバイスのアップグレードを開始する前に、この手順を使用して管理対象デバイスにパッケージをコピー（プッシュ）することをお勧めします。

（注） Firepower 4100/9300 では、必要な付属の FXOS アップグレードを開始する前に、Firepower Threat Defense アップグレードパッケージをコピーすることを推奨（場合によっては必須）しています。

サポートは Firepower のバージョンによって異なります。

- バージョン 6.2.2 以前は、アップグレード前のコピーをサポートしていません。

  デバイスのアップグレードを開始すると、システムは最初のタスクとしてアップグレードパッケージを Firepower Management Center からデバイスにコピーします。

- バージョン 6.2.3 では、アップグレードパッケージを Firepower Management Center からデバイスに手動でコピーする機能が追加されています。

  これにより、アップグレードのメンテナンス時間を短縮できます。

- バージョン 6.6.0 では、アップグレードパッケージを内部 Web サーバーから Firepower Threat Defense デバイスに手動でコピーする機能が追加されています。

  これは、Firepower Management Center とその Firepower Threat Defense デバイスの間の帯域幅が制限されている場合に役立ちます。また、Firepower Management Center 上の容量も節約できます。

- バージョン 7.0.0 では、アップグレードパッケージを Firepower Threat Defense デバイスにコピーするように即す新しい Firepower Threat Defense アップグレードワークフローが導入されています。

  Firepower Management Center がバージョン 7.0.0 以降を実行している場合は、[Device Upgrade] ページを使用して、アップグレードパッケージを FTD デバイスにコピーすることをお勧めします。詳しくは、FMC を使用した Firepower Threat Defense のアップグレード（バージョン 7.0.0） （86 ページ） を参照してください。古い展開環境にあるアップグレードパッケージをクラシックデバイス（Firepower 7000/8000 シリーズ、ASA FirePOWER、NGIPSv）にコピーするには、引き続きこの手順を使用する必要があります。

手動でコピーする場合、各デバイスはソースからアップグレードパッケージを取得することに注意してください。システムは、クラスタ、スタック、または HA メンバーユニット間でアップグレードパッケージをコピーしません。

始める前に

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。『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。

ステップ 1 Firepower Management Center Web インターフェイスで **[システム（System）]** > **[更新（Updates）]** を選択します。

ステップ 2 デバイスが取得できる場所にアップグレードパッケージを配置します。

- Firepower Management Center：手動でパッケージをアップロードするか、または FMC に直接取得します。
- 内部 Web サーバー（Firepower Threat Defense バージョン 6.6.0 以降）：内部 Web サーバーにアップロードし、そのサーバーからパッケージを取得するように Firepower Threat Defense デバイスを設定します。

ステップ 3 プッシュするアップグレードパッケージの横にある [Push]（バージョン 6.5.0 以前）アイコンまたは [アップデートのプッシュまたはステージ（Push or Stage update）]（バージョン 6.6.0 以降）アイコンをクリックして、接続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。

ステップ 4 パッケージをプッシュします

- Firepower Management Center：[Push] をクリックします。
- 内部 Web サーバー：[送信元からデバイスへの更新のダウンロード（Download Update to Device from Source）] をクリックします。

Firepower ソフトウェアの準備状況チェック

準備状況チェックにより、ソフトウェアをアップグレードするための Firepower アプライアンスの準備状況を評価できます。アプライアン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ようお勧めします。

準備状況チェックの実行に必要な時間は、アプライアンスのモデルとデータベースのサイズによって異なります。それ以降のリリースでは、準備状況チェックもより高速化されています。

FMCを使用した準備状況チェックの実行（バージョン7.0.0およびFTD）

FMC がバージョン 7.0.0 以降を実行している場合は、[デバイスのアップグレード（Device Upgrade）]ページを使用して、FTD デバイスで準備チェックを実行することをお勧めします。詳しくは、FMC を使用した Firepower Threat Defense のアップグレード（バージョン 7.0.0）（86 ページ）を参照してください。

以下の場合は、次のトピックを参照してください。

- FMC 自体での準備状況チェックの実行。
- 管理対象デバイスでの準備チェックの実行、および FMC がバージョン 6.7.x を実行している。
- 管理対象デバイスでの準備チェックの実行、および FMC がバージョン 6.6.x 以前を実行している。

FMC を使用した準備状況チェックの実行（バージョン 6.7.0 以降）

この手順は、現在バージョン 6.7.0 以降を実行している FMC、およびそれらの管理対象デバイス（古いバージョン（6.3.0 ～ 6.6.x）を実行しているデバイスを含む）、および高可用性およびスケーラビリティ展開の FTD デバイスに有効です。

重要 FMC がバージョン 7.0.0 以降を実行している場合は、[Device Upgrade] ページを使用して、FTD デバイスで準備チェックを実行することをお勧めします。詳しくは、FMC を使用した Firepower Threat Defense のアップグレード（バージョン 7.0.0）（86 ページ）を参照してください。FMC およびクラシックデバイスで準備状況チェックを実行するには、引き続きこの手順を使用する必要があります。

始める前に

- FMC をバージョン 6.7.0 以降にアップグレードします。FMC が現在古いバージョンを実行している場合は、FMC を使用した準備状況チェックの実行（バージョン 6.0.1 ～ 6.6.x）（48 ページ）を参照してください。
- チェックするアプライアンスの FMC にアップグレードパッケージをアップロードします。バージョン 6.6.0 以降の FTD デバイスを確認する場合は、内部 Web サーバー上のアップグレードパッケージの場所を指定することもできます。準備状況チェックはアップグレードパッケージに含まれるので、これが必要です。
- （オプション）クラシックデバイスを任意のバージョンにアップグレードする場合、または FTD デバイスをバージョン 6.3.0.1 ～ 6.6.x にアップグレードする場合は、アップグレードパッケージをデバイスにコピーします。これにより、準備状況チェックの実行に必要な時間を短縮できます。FTD デバイスをバージョン 6.7.0 以降にアップグレードする場合は、この手順をスキップできます。アップグレード自体を開始する前に、アップグレードパッケージをデバイスにプッシュすることをお勧めしますが、準備状況チェックを実行する前に行う必要はありません。

ステップ 1 FMC Web インターフェイスで、**[System]** > **[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。

対象アプライアンスのリストが、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。バージョン 6.7.0 以降、より複雑な準備状況チェックを実行する前に、FTD デバイスは特定の基本チェックに合格する必要があります。この事前チェックは、アップグレードが失敗する原因となる問題を検出します。これらをより早期に検出し、続行をブロックするようになりました。

ステップ 3 チェックするアプライアンスを選択し、[準備状況の確認（Check Readiness）] をクリックします。

他の適格なアプライアン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。オペレーティングシステムをアップグレードするか、構成の変更を展開する必要がある場合があります。

ステップ 4 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します。

チェックが失敗した場合、メッセージセンターは失敗ログを提供します。

次のタスク

[システム（System）] > **[更新（Updates）]**ページで、[準備状況チェック（Readiness Checks）] をクリックすると、進行中のチェックや不合格のチェックなど、FTD 展開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 を使用した準備状況チェックの実行（バージョン 6.0.1 ～ 6.6.x）

この手順は、現在バージョン 6.0.1 ～ 6.6.x を実行している FMC とそのスタンドアロン管理対象デバイスに有効です。

（注） クラスタ化されたデバイス、スタック構成のデバイス、および高可用性ペアのデバイスについては、Linux シェル（エクスパートモードとも呼ばれます）から準備状況チェックを実行してください。チェックを実行するには、最初にアップグレードパッケージを各デバイスの正しい場所にプッシュまたはコピーしてから、コマンド `sudo install_update.pl --detach --readiness-check /var/sf/updates/`*`upgrade_package_name`* を使用します。詳細な手順については、Cisco TAC にお問い合わせください。

始める前に

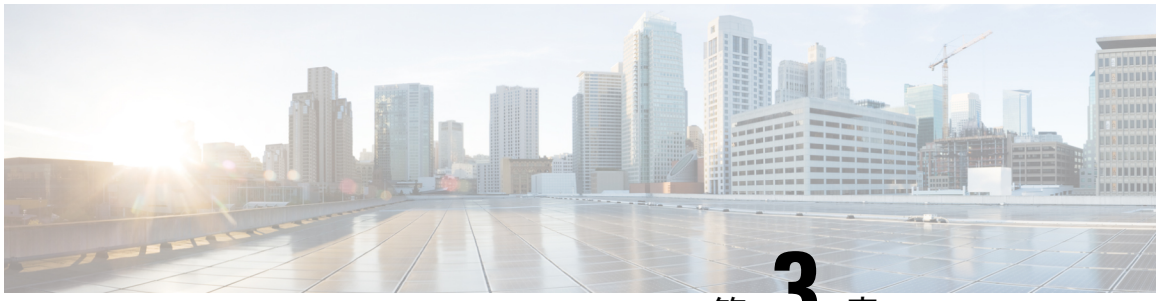
- （バージョン 6.0.1）バージョン 6.0.1 → 6.1.0 のアップグレードで準備状況チェックを実行する場合は、最初にバージョン 6.1 のプレインストールパッケージをインストールします。これは、FMC および管理対象デバイスに対して行う必要があります。『Firepower System Release Notes Version 6.1.0 Pre-Installation Package』を参照してください。
- チェックするアプライアンスの FMC にアップグレードパッケージをアップロードします。バージョン 6.6.x FTD デバイスを確認する場合は、内部 Web サーバー上のアップグレードパッケージの場所を指定することもできます。準備状況チェックはアップグレードパッケージに含まれるので、これが必要です。
- （オプション、バージョン 6.2.3 以降）管理対象デバイスにアップグレードパッケージをプッシュします。これにより、チェックの実行に必要な時間を短縮できます。
- 構成を、構成が古い管理対象デバイスに展開します。そうしない場合、準備状況チェックは失敗することがあります。

ステップ 1 FMC Web インターフェイスで、**[システム（System）]** > **[更新（Updates）]** を選択します。

ステップ 2 適切な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。

ステップ 3 チェックするアプライアンスを選択し、[準備状況チェックの開始（Launch Readiness Check）] をクリックします。

ステップ 4 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します。



第 3 章

Firepower Management Center のアップグレード

アップグレード チェックリスト：Firepower Management Center

FMC（FMCv を含む）のアップグレードを行う前にこのチェックリストを完了します。ハイアベイラビリティペアをアップグレードする場合は、チェックリストをピアごとに完了します。

（注） プロセス中は常に、展開の通信と正常性を維持してください。進行中に FMC のアップグレードを再開しないでください。事前のチェック中に、アップグレードプロセスが停止しているように見える場合がありますが、これは想定内の動作です。アップグレードに失敗する、アプライアンスが応答しないなど、アップグレードで問題が発生した場合にはCisco TACにお問い合わせください。

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。

表 *28 :*

✓	アクション/チェック
	アップグレードパスを計画します。 これは、マルチアプライアンス展開、マルチホップアップグレード、または展開の互換性を常に維持しながら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。実行したアップグレードと次に実行するアップグレードを常に確認します。 （注） FMC 展開では、通常、FMC をアップグレードしてから、管理対象デバイスをアップグレードします。ただし、場合によっては、最初にデバイスをアップグレードする必要があります。 アップグレードパス （13 ページ）を参照してください。
	すべてのアップグレードの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。アップグレードの警告、動作の変更、新機能と廃止された機能、および既知の問題など、リリース固有の重要な情報を含むリリースノートから読み始めます。
	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。FMC の展開では、アップグレードパケージをアップグレード時に管理対象デバイスに転送する場合は、帯域幅が不十分だとアップグレード時間が長くなったり、アップグレードがタイムアウトする原因となったりする可能性があります。デバイスのアップグレードを開始する前に、可能な場合は常に、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。 『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。
	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および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、ウィンドウで実行する必要があるタスクと、事前に実行できるタスクを検討します。 たとえば、メンテナンス時間帯で、アプライアンスへのアップグレードパッケージのコピー、準備状況チェックの実行、バックアップの作成などが行われるまで待機しないようにします。

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。

表 29：

✓	アクション/チェック
	アップグレードパッケージをアップロードします。 FMC の高可用性の展開では、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。HA 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。 Firepower Management Center にアップロード （42 ページ） を参照してください。

バックアップ

災害から回復する能力は、システム保守計画の重要な部分を占めます。

バックアップと復元は、複雑なプロセスになる可能性があります。手順をスキップしたり、セキュリティやライセンスの問題を無視しないでください。バックアップと復元の要件、ガイドライン、制限事項、およびベストプラクティスの詳細については、使用する展開の設定ガイドを参照してください。

⚠

注意 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。

表 30：

✓	アクション/チェック
	バックアップします。 アップグレードの前後にバックアップします（サポートされている場合）。 • アップグレード前：アップグレードが致命的な失敗であった場合は、再イメージ化を実行し、復元する必要がある場合があります。再イメージ化によって、システムパスワードを含むほとんどの設定が工場出荷時の初期状態に戻ります。最近のバックアップがある場合は、通常の操作にすばやく戻ることができます。 • アップグレード後：これにより、新しくアップグレードされた展開のスナップショットが作成されます。FMC の展開では、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、新しい FMC バックアップファイルにデバイスがアップグレードされたことを「認識」させることをお勧めします。

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。

表 *31 :*

✓	アクション/チェック
	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、FMC の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、 をアップグレードする準備が整います。

表 *32 :*

✓	アクション/チェック
	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。同期されていないと、アップグレードが失敗する可能性があります。FMC 展開では、時刻のずれが 10 秒を超えている場合、ヘルスモニタからアラートが発行されますが、手動で確認する必要もあります。 時刻を確認するには、次の手順を実行します。 • FMC：[システム（System）] > [設定（Configuration）] > [時刻（Time）] を選択します。 • デバイス：**show time** CLI コマンドを使用します。
	ディスク容量を確認します。 ソフトウェアアップグレードに関するディスク容量チェックを実行します。空きディスク容量が十分でない場合、アップグレードは失敗します。 対象バージョンの Cisco Firepower リリース ノート 内の「ソフトウェアのアップグレード」の章を参照してください。

✓	アクション/チェック
	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。 一部の展開では、設定が古い場合、アップグレードがブロックされることがあります。FMC における高可用性の展開では、アクティブなピアから展開するだけで済みます。 展開する際にリソースを要求すると、いくつかのパケットがインスペクションなしでドロップされることがあります。 さらに、いくつかの設定を展開することで Snort が再起動されます。これにより、トラフィックのインスペクションが中断し、デバイスのトラフィックの処理方法によっては、再起動が完了するまでトラフィックが中断する場合があります。 対象バージョンの Cisco Firepower リリース ノート 内の「ソフトウェアのアップグレード」の章を参照してください。
	準備状況チェックを実行します。 FMC がバージョン 6.1.0 以降を実行している場合は、互換性と準備状況のチェックの実施をお勧めします。これらのチェックにより、ソフトウェアをアップグレードするための準備状況を確認できます。 Firepower ソフトウェアの準備状況チェック （46 ページ）を参照してください。
	実行中のタスクを確認します。 アップグレードする前に、重要なタスク（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。また、アップグレード中に実行するようにスケジュールされたタスクを確認し、それらをキャンセルまたは延期することをお勧めします。 （注） 一部の展開では、アップグレードするとスケジュールされたタスクが自動的に延期されるようになりました。アップグレード中に開始するようにスケジュールされたタスクは、アップグレード後の再起動の 5 分後に開始されます。 この機能は現在、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 以降を実行している FMC でサポートされています。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。

スタンドアロンの Firepower Management Center のアップグレード

この手順を使用して、Firepower Management Center Virtual を含め、スタンドアロンの Firepower Management Center をアップグレードします。

⚠

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

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。展開したアプライアンスが正常で、きちんと通信していることを確認します。

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

ステップ 2 使用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）] をクリックすると、アップグレードが開始されます。

アップグレードして再起動することを確認します。

ステップ 4 ログアウトするまで、事前チェックの進行状況をモニターします。この間、構成の変更を行わないでください。

ステップ 5 可能なときに、再度ログインします。

- マイナーアップグレード（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。
- 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。

ステップ 6 プロンプトが表示されたら、エンド ユーザー ライセンス契約書（EULA）を確認し、承認します。

ステップ 7 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 8 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 9 リリース ノートに記載されているアップグレード後の構成の変更をすべて完了します。

ステップ 10 構成を再展開します。

すべての管理対象デバイスに再展開します。 デバイスに構成を展開しない場合、最終的なアップグレードが失敗し、イメージの再作成が必要になることがあります。

ハイ アベイラビリティ Firepower Management Center のアップグレード

この手順を使用して、ハイアベイラビリティペアに含まれる FMC の Firepower ソフトウェアをアップグレードします。

一度に 1 つのピアを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。スタンバイで事前チェックが開始されると、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。この一時的な状態は *split-brain* と呼ばれていて、アップグレード中を除き、サポートされていません。ペアが split-brain の状況で、構成の変更または展開を行わないでください。同期の再開後は変更内容が失われます。

⚠

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

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。展開したアプライアンスが正常で、きちんと通信していることを確認します。

ステップ 1 同期を一時停止します。

a) **[システム（System）]** > **[統合（Integration）]**を選択します。

b) [ハイ アベイラビリティ（High Availability）] タブで、[同期の一時停止（Pause Synchronization）] をクリックします。

ステップ 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 の高可用性の展開では、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。HA 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。

「スタンドアロンの Firepower Management Center のアップグレード （56 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、可能な場合な再度ログインします（これは主なアップグレードで 2 回行われます）。
c) アップグレードが成功したことを確認します。

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

ステップ 4 同期を再開します。

a) アクティブピアにする FMC にログインします。
b) **[システム（System）]** > **[統合（Integration）]** の順に選択します。
c) [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。
d) 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。

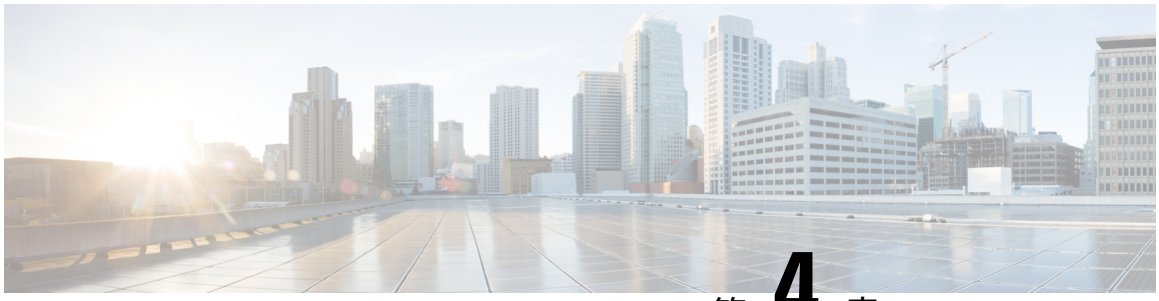
ステップ 5 侵入ルール（SRU/LSP）および脆弱性データベース（VDB）を更新します。

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 リリース ノートに記載されているアップグレード後の構成の変更をすべて完了します。

ステップ 7 構成を再展開します。

すべての管理対象デバイスに再展開します。 デバイスに構成を展開しない場合、最終的なアップグレードが失敗し、イメージの再作成が必要になることがあります。



第 4 章

Firepower Threat Defense 論理デバイスのアップグレード

アップグレード チェックリスト：FMC を搭載した Firepower Threat Defense

Firepower Threat Defense のアップグレードを行う前にこのチェックリストを完了します。

（注） プロセス中は常に、展開の通信と正常性を維持してください。

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。ただし、バージョン6.7.0からのメジャーおよびメンテナンス FTD アップグレードを行った後は、失敗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。[Device Management] ページおよびメッセージセンターからアクセスできる [Upgrade Status] ポップアップを使用するか、FTD CLI を使用してください。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戻ります（「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。すべてのオプションを使い切った場合、または展開でキャンセルや再試行がサポートされていない場合は、Cisco TAC にお問い合わせください。

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。

表 *33*：

✓	アクション/チェック
	アップグレードパスを計画します。 これは、マルチアプライアンス展開、マルチホップアップグレード、または展開の互換性を常に維持しながら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。実行したアップグレードと次に実行するアップグレードを常に確認します。 （注） FMC 展開では、通常、FMC をアップグレードしてから、管理対象デバイスをアップグレードします。ただし、場合によっては、最初にデバイスをアップグレードする必要があります。 アップグレードパス （13 ページ）を参照してください。
	すべてのアップグレードの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。アップグレードの警告、動作の変更、新機能と廃止された機能、および既知の問題など、リリース固有の重要な情報を含むリリースノートから読み始めます。
	アプライアンスへのアクセスを確認します。 デバイスは、（インターフェイス設定に応じて）アップグレード中、またはアップグレードが失敗した場合に、トラフィックを渡すことを停止できます。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。FMC の展開では、デバイスを経由せずに FMC 管理インターフェイスにアクセスできる必要もあります。
	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。FMC の展開では、アップグレードパケージをアップグレード時に管理対象デバイスに転送する場合は、帯域幅が不十分だとアップグレード時間が長くなったり、アップグレードがタイムアウトする原因となったりする可能性があります。デバイスのアップグレードを開始する前に、可能な場合は常に、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。 『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
	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および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、ウィンドウで実行する必要があるタスクと、事前に実行できるタスクを検討します。 たとえば、メンテナンス時間帯で、アプライアンスへのアップグレードパッケージのコピー、準備状況チェックの実行、バックアップの作成などが行われるまで待機しないようにします。

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。

表 *34*：

✓	アクション/チェック
	アップグレードパッケージを FMC または内部 Web サーバーにアップロードします。 バージョン 6.6.0 以降では、FTD アップグレードパッケージのソースとして FMC の代わりに内部 Web サーバーを設定できます。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役立ち、FMC の容量を節約することができます。 内部サーバへのアップロード（FMC を使用したバージョン 6.6.0 以降の FTD） （43 ページ）を参照してください。
	アップグレードパッケージをデバイスにコピーします。 サポートされている場合、デバイスのアップグレードを開始する前に、管理対象デバイスにパッケージをコピー（プッシュ）することをお勧めします。 • バージョン 6.2.2 以前は、アップグレード前のコピーをサポートしていません。 • バージョン 6.2.3 では、FMC からアップグレードパッケージを手動でコピーできます。 • バージョン 6.6.0 では、アップグレードパッケージを内部 Web サーバーから手動でコピーする機能が追加されています。 • バージョン 7.0.0 では、アップグレードパッケージをコピーするように求める FTD アップグレードのワークフローが追加されています。 （注） Firepower 4100/9300 では、必要な付属の FXOS アップグレードを開始する前に、 アップグレードパッケージをコピーすることを推奨（場合によっては必須）しています。 管理対象デバイスへのコピー （44 ページ）を参照してください。

バックアップ

災害から回復する能力は、システム保守計画の重要な部分を占めます。

バックアップと復元は、複雑なプロセスになる可能性があります。手順をスキップしたり、セキュリティやライセンスの問題を無視しないでください。バックアップと復元の要件、ガイドライン、制限事項、およびベストプラクティスの詳細については、使用する展開の設定ガイドを参照してください。

⚠

注意 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。

表 *35：*

✓	アクション/チェック
	FTD をバックアップします。 FMC を使用してデバイスをバックアップします。すべての FTD プラットフォームおよび設定でバックアップがサポートされているわけではありません。バージョン 6.3.0 以降が必要です。 アップグレードの前後にバックアップします（サポートされている場合）。 • アップグレード前：アップグレードが致命的な失敗であった場合は、再イメージ化を実行し、復元する必要がある場合があります。再イメージ化によって、システムパスワードを含むほとんどの設定が工場出荷時の初期状態に戻ります。最近のバックアップがある場合は、通常の操作にすばやく戻ることができます。 • アップグレード後：これにより、新しくアップグレードされた展開のスナップショットが作成されます。FMC の展開では、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、新しい FMC バックアップファイルにデバイスがアップグレードされたことを「認識」させることをお勧めします。
	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、アップグレードの前後に、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。

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。

表 *36*：

✓	アクション/チェック
	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、任意の仮想アプライアンスの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、デバイスの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 FXOS をアップグレードします。 必要に応じて、FTD をアップグレードする前に、FXOS をアップグレードします。これは通常、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。トラフィックフローとインスペクションでの中断を防ぐには、FTD 高可用性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。 （注） FXOS をアップグレードする前に、必ずすべてのアップグレードのガイドラインを読み、設定の変更を計画してください。FXOS リリースノート：Cisco Firepower 4100/9300 FXOS リリースノート を使用して開始します。

最終チェック

一連の最終チェックにより、 をアップグレードする準備が整います。

表 *37*：

✓	アクション/チェック
	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。同期されていないと、アップグレードが失敗する可能性があります。FMC 展開では、時刻のずれが 10 秒を超えている場合、ヘルスモニタからアラートが発行されますが、手動で確認する必要もあります。 時刻を確認するには、次の手順を実行します。 • FMC：[システム（System）] > [設定（Configuration）] > [時刻（Time）] を選択します。 • デバイス：**show time** CLI コマンドを使用します。

✓	アクション/チェック
	ディスク容量を確認します。 ソフトウェアアップグレードに関するディスク容量チェックを実行します。空きディスク容量が十分でない場合、アップグレードは失敗します。 対象バージョンの Cisco Firepower リリース ノート 内の「ソフトウェアのアップグレード」の章を参照してください。
	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。 一部の展開では、設定が古い場合、アップグレードがブロックされることがあります。FMC における高可用性の展開では、アクティブなピアから展開するだけで済みます。 展開する際にリソースを要求すると、いくつかのパケットがインスペクションなしでドロップされることがあります。 さらに、いくつかの設定を展開することで Snort が再起動されます。これにより、トラフィックのインスペクションが中断し、デバイスのトラフィックの処理方法によっては、再起動が完了するまでトラフィックが中断する場合があります。 対象バージョンの Cisco Firepower リリース ノート 内の「ソフトウェアのアップグレード」の章を参照してください。
	準備状況チェックを実行します。 FMC がバージョン 6.1.0 以降を実行している場合は、互換性と準備状況のチェックの実施をお勧めします。これらのチェックにより、ソフトウェアをアップグレードするための準備状況を確認できます。バージョン 7.0.0 では、これらのチェックを完了するように求める新しい FTD アップグレードのワークフローが導入されています。 Firepower ソフトウェアの準備状況チェック （46 ページ）を参照してください。
	実行中のタスクを確認します。 アップグレードする前に、デバイスの重要なタスク（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。また、アップグレード中に実行するようにスケジュールされたタスクを確認し、それらをキャンセルまたは延期することをお勧めします。

Firepower Threat Defense 論理デバイスを持つ Firepower 4100/9300 上の FXOS のアップグレード

Firepower 4100/9300 で、シャーシ間クラスタリングの Firepower またはハイアベイラビリティペアの構成がある場合でも、各シャーシの FXOS を個別にアップグレードします。FXOS CLI または Firepower Chassis Manager を使用できます。

FXOS をアップグレードするとシャーシが再起動します。導入によっては、トラフィックがドロップしたり、インスペクションなしにネットワークを通過する可能性があります。お使いのバージョンのCiscoFirepower リリースノートを参照してください。

FXOSのアップグレード：FTDスタンドアロンデバイスとシャーシ間クラスタ

スタンドアロンの Firepower Threat Defense 論理デバイスの場合、または FTD シャーシ内クラスタ（同じシャーシ上のユニット）の場合は、最初にFXOSプラットフォームバンドルをアップグレードしてから、FTD論理デバイスをアップグレードします。Firepower Management Center を使用して、クラスタ化されたデバイスを 1 つのユニットとしてアップグレードします。

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。

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 のアップグレード：FTD 高可用性ペア

Firepower Threat Defense の高可用性展開では、どちらかの FTD 論理デバイスをアップグレードする前に、両方のシャーシで FXOS プラットフォームバンドル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。

Firepower Management Center の展開では、論理デバイスを 1 つのユニットとしてアップグレードします。

1. スタンバイの FXOS をアップグレードします。
2. ロールを切り替えます。
3. 新しいスタンバイの FXOS をアップグレードします。
4. FTD 論理デバイスをアップグレードします。

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。

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。

FXOS のアップグレード：FTD シャーシ間クラスタ

Firepower Threat Defense シャーシ間クラスタ（異なるシャーシのユニット）の場合、FTD 論理デバイスをアップグレードする前に、すべてのシャーシでFXOSプラットフォームバンドル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上の FXOS を常にアップグレードします。次に、Firepower Management Center を使用して、論理デバイスを 1 つのユニットとしてアップグレードします。

たとえば、2 つのシャーシがあるクラスタの場合：

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. 新しい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。
4. FTD 論理デバイスをアップグレードします。

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。

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。

FMC を使用した Firepower Threat Defense のアップグレード（バージョン 7.0.0）

FMC には、FTD をアップグレードするためのウィザードが用意されています。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 [システムの更新（System Updates）] ページ（**[システム（System）] > [更新（Updates）]**）を使用する必要があります。また、[システムの更新（System Updates）] ページを使用して、FMC 自体、および古い従来型デバイスをアップグレードする必要があります。

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、アップグレード前の重要な段階を順を追って説明します。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が、管理者アクセス権を持つ他のユーザーはワークフローをリセット、変更、または続行できます（CAC でログインした場合を除きます。この場合、進行状況はログアウトしてから 24 時間後にクリアされます）。進行状況は、高可用性 FMC 間でも同期されます。

（注） バージョン 7.0.x では、[デバイスのアップグレード（Device Upgrade）] ページ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、ワークフロー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、[Next] をクリックする前に、すべてのグループメンバーがワークフロー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。

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。ただし、バージョン 6.7.0 からの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、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。 [デバイス管理（Device Management）] ページ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するか、FTD CLI を使用します。

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戻ります（「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。すべてのオプションを使い切った場合、または展開でキャンセルや再試行がサポートされていない場合は、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。展開したアプライアンスが正常で、きちんと通信していることを確認します。

アップグレードするデバイスを選択します。

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

ステップ 2 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、デバイスをアップグレードする場合は（バージョン 6.4.0.x から 6.6.x 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 3 [アクションの選択（Select Action）] または [一括アクションの選択（Select Bulk Action）] メニューから、[Firepower ソフトウェアをアップグレードする（Upgrade Firepower Software）] を選択します。

[デバイスのアップグレード（Device Upgrade）] ページが表示され、選択したデバイスの数が示され、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）] でデバイスリンク（「4 つのデバイス」 など）をクリックして、デバイス詳細を表示します。

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 4 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。

アップグレードパッケージをデバイスにコピーします。

ステップ 5 [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。削除したくなければ、不要なデバイスは削除する必要はありません。それらは次のステップには含まれません。

[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リストにない場合は、[System] > [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。

ステップ 6 アップグレードパッケージがまだ必要なすべてのデバイスについて、[Copy Upgrade Packages] をクリックして、選択を確認します。

FTD をアップグレードするには、ソフトウェアアップグレードパッケージがアプライアンスにある必要があります。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。

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 7 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。

[Require passing compatibility and readiness checks option] オプションを無効にすることでチェックをスキップできますが、お勧めしません。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、Firepower 4100/9300 で FXOS をアップグレードする必要がある場合、または管理対象デバイスに展開する必要がある場合、システムはすぐに警告します。

ステップ 8 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 9 必要に応じて、[Device Upgrade] ページに戻ります。

進行状況は保持されています。保持されていない場合は、管理者アクセス権を持つ他の誰かがワークフローをリセット、変更、または完了した可能性があります。

ステップ 10 [Next] をクリックします。

アップグレードします。

ステップ 11 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 12 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 13 [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、リリースノートの「ソフトウェアのアップグレード」の章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 14 アップグレードが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、**[Devices]** > **[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 15 （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、常にスタンバイデバイスまたはデータユニット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 16 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 17 リリース ノートに記載されているアップグレード後の構成の変更をすべて完了します。

ステップ 18 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）[Device Upgrade] ページに戻り、[Finish] 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、[Device Upgrade] 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。

FMC を使用した Firepower Threat Defense のアップグレード（バージョン 6.0.1 ～ 6.7.0）

この手順を使用して、FMC の [システムアップデート（System Updates）] ページから FTD をアップグレードします。このページで、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。

始める前に

- この手順を使用するかどうかを決定します。バージョン 7.0.x への FTD アップグレードについては、代わりにアップグレードウィザードを使用することをお勧めします。FMC を使用した Firepower Threat Defense のアップグレード（バージョン 7.0.0） （86 ページ）を参照してください。
- 事前アップグレードのチェックリストを完了します。展開したアプライアンスが正常で、きちんと通信していることを確認します。
- （任意）高可用性デバイスのペアのアクティブ/スタンバイの役割を切り替えます。**[Devices]** > **[Device Management]** を選択し、ペアの横にある [Switch Active Peer] アイコンをクリックして、選択内容を確認します。

  ハイ アベイラビリティ ペアのスタンバイ 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。アップグレードの完了時には、デバイスの役割は切り替わったままです。アクティブ/スタンバイの役割を維持する場合、アップグレード前に役割を手動で切り替えます。それにより、アップグレードプロセスによって元の役割に切り替わります。

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

ステップ 2 使用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、アップグレードするデバイスを選択します。

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。

（注） [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 3 （バージョン 6.7.0 以降）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。 パッチの自動キャンセルはサポートされていません。

ステップ 4 [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。

一部のデバイスは、アップグレード時に 2 回再起動することがありますが、これは想定内の動作です。トラフィックは、デバイスの設定および展開方法に応じて、アップグレードの間ドロップするか、検査なしでネットワークを通過します。 詳細については、対象バージョンの Cisco Firepower リリース ノート 内の「ソフトウェアのアップグレード」の章を参照してください。

ステップ 5 アップグレードの進捗状況 をモニタします。

注意 アップグレード中のデバイスへの変更の展開、手動での再起動、シャットダウンは行わないでください。

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。ただし、バージョン 6.7.0 からのメジャーおよびメンテナンス FTD アップグレードを行った後は、失敗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。[Device Management] ページおよびメッセージセンターからアクセスできる [Upgrade Status] ポップアップを使用するか、FTD CLI を使用してください。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戻ります（「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。すべてのオプションを使い切った場合、または展開でキャンセルや再試行がサポートされていない場合は、Cisco TAC にお問い合わせください。

ステップ 6 アップグレードが成功したことを確認します。

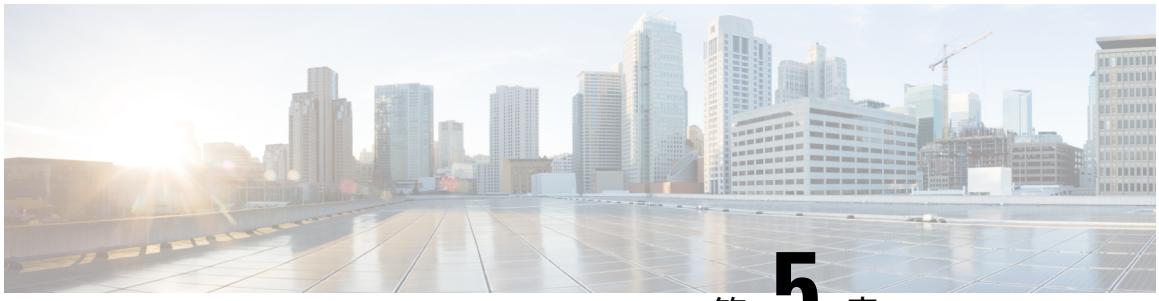
アップグレードが完了したら、**[Devices]** > **[Device Management]** を選択し、アップグレードしたデバイスのソフトウェアバージョンが正しいことを確認します。

ステップ 7 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 8 リリース ノートに記載されているアップグレード後の構成の変更をすべて完了します。

ステップ 9 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 5 章

FirePOWER 7000/8000 シリーズと NGIPSv のアップグレード

アップグレード チェックリスト：FMC を搭載した Firepower 7000/8000 シリーズと NGIPSv

Firepower 7000/8000 シリーズおよび NGIPSv デバイスをアップグレードする前に、このチェックリストを完了します。

（注） プロセス中は常に、展開の通信と正常性を維持してください。進行中のデバイスのアップグレードは再開しないでください。事前のチェック中に、アップグレードプロセスが停止しているように見える場合がありますが、これは想定内の動作です。アップグレードに失敗する、アプライアンスが応答しないなど、アップグレードで問題が発生した場合にはCisco TACにお問い合わせください。

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。

表 *38 :*

✓	アクション/チェック
	アップグレードパスを計画します。 これは、マルチアプライアンス展開、マルチホップアップグレード、または展開の互換性を常に維持しながら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。実行したアップグレードと次に実行するアップグレードを常に確認します。 （注） FMC 展開では、通常、FMC をアップグレードしてから、管理対象デバイスをアップグレードします。ただし、場合によっては、最初にデバイスをアップグレードする必要があります。 アップグレードパス （13 ページ）を参照してください。
	すべてのアップグレードの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。アップグレードの警告、動作の変更、新機能と廃止された機能、および既知の問題など、リリース固有の重要な情報を含むリリースノートから読み始めます。
	アプライアンスへのアクセスを確認します。 デバイスは、（インターフェイス設定に応じて）アップグレード中、またはアップグレードが失敗した場合に、トラフィックを渡すことを停止できます。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。FMC の展開では、デバイスを経由せずに FMC 管理インターフェイスにアクセスできる必要もあります。
	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。FMC の展開では、アップグレードパケージをアップグレード時に管理対象デバイスに転送する場合は、帯域幅が不十分だとアップグレード時間が長くなったり、アップグレードがタイムアウトする原因となったりする可能性があります。デバイスのアップグレードを開始する前に、可能な場合は常に、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。 『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
	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および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、ウィンドウで実行する必要があるタスクと、事前に実行できるタスクを検討します。 たとえば、メンテナンス時間帯で、アプライアンスへのアップグレードパッケージのコピー、準備状況チェックの実行、バックアップの作成などが行われるまで待機しないようにします。

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。

表 *39*：

✓	アクション/チェック
	アップグレードパッケージを FMC にアップロードします。 Firepower Management Center にアップロード （42 ページ） を参照してください。
	アップグレードパッケージをデバイスにコピーします。 FMC がバージョン 6.2.3 以降を実行している場合、デバイスのアップグレードを開始する前に、管理対象デバイスにパッケージをコピー（プッシュ）することをお勧めします。 管理対象デバイスへのコピー （44 ページ）を参照してください。

バックアップ

災害から回復する能力は、システム保守計画の重要な部分を占めます。

バックアップと復元は、複雑なプロセスになる可能性があります。手順をスキップしたり、セキュリティやライセンスの問題を無視しないでください。バックアップと復元の要件、ガイドライン、制限事項、およびベストプラクティスの詳細については、使用する展開の設定ガイドを参照してください。

注意 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。

表 *40 :*

✓	アクション/チェック
	7000/8000 シリーズ デバイスをバックアップします。 FMC を使用して 7000/8000 シリーズ デバイスをバックアップします。バックアップは、NGIPSv についてはサポートされていません。 アップグレードの前後にバックアップします（サポートされている場合）。 • アップグレード前：アップグレードが致命的な失敗であった場合は、再イメージ化を実行し、復元する必要がある場合があります。再イメージ化によって、システムパスワードを含むほとんどの設定が工場出荷時の初期状態に戻ります。最近のバックアップがある場合は、通常の操作にすばやく戻ることができます。 • アップグレード後：これにより、新しくアップグレードされた展開のスナップショットが作成されます。FMC の展開では、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、新しい FMC バックアップファイルにデバイスがアップグレードされたことを「認識」させることをお勧めします。

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。

表 *41 :*

✓	アクション/チェック
	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、任意の仮想アプライアンスの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、デバイスの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、 をアップグレードする準備が整います。

表 *42 :*

✓	アクション/チェック
	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。

✓	アクション/チェック
	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。同期されていないと、アップグレードが失敗する可能性があります。FMC 展開では、時刻のずれが 10 秒を超えている場合、ヘルスモニタからアラートが発行されますが、手動で確認する必要もあります。 時刻を確認するには、次の手順を実行します。 • FMC：[システム（System）] > [設定（Configuration）] > [時刻（Time）] を選択します。 • デバイス：**show time** CLI コマンドを使用します。
	ディスク容量を確認します。 ソフトウェアアップグレードに関するディスク容量チェックを実行します。空きディスク容量が十分でない場合、アップグレードは失敗します。 対象バージョンの Cisco Firepower リリース ノート 内の「ソフトウェアのアップグレード」の章を参照してください。
	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。 一部の展開では、設定が古い場合、アップグレードがブロックされることがあります。FMC における高可用性の展開では、アクティブなピアから展開するだけで済みます。 展開する際にリソースを要求すると、いくつかのパケットがインスペクションなしでドロップされることがあります。 さらに、いくつかの設定を展開することで Snort が再起動されます。これにより、トラフィックのインスペクションが中断し、デバイスのトラフィックの処理方法によっては、再起動が完了するまでトラフィックが中断する場合があります。 対象バージョンの Cisco Firepower リリース ノート 内の「ソフトウェアのアップグレード」の章を参照してください。
	準備状況チェックを実行します。 FMC がバージョン 6.1.0 以降を実行している場合は、互換性と準備状況のチェックの実施をお勧めします。これらのチェックにより、ソフトウェアをアップグレードするための準備状況を確認できます。 Firepower ソフトウェアの準備状況チェック （46 ページ）を参照してください。

✓	アクション/チェック
	実行中のタスクを確認します。 アップグレードする前に、デバイスの重要なタスク（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。また、アップグレード中に実行するようにスケジュールされたタスクを確認し、それらをキャンセルまたは延期することをお勧めします。

FMC を搭載した FirePOWER 7000/8000 と NGIPSv のアップグレード

FirePOWER 7000/8000 シリーズおよび NGIPSv デバイスをアップグレードするには、この手順を使用します。複数のデバイスで同じアップグレードパッケージが使用されている場合、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 スタックとハイ 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。

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。展開したアプライアンスが正常で、きちんと通信していることを確認します。

ステップ 1 （任意）スイッチングとルーティングを実行する高可用性デバイスのペアのアクティブ/スタンバイの役割を切り替えます。

ハイ アベイラビリティ ペアがアクセス制御のみを実行するために展開されている場合、アクティブ デバイスが最初にアップグレードされます。アップグレードの完了時に、アクティブとスタンバイの以前の役割がデバイスで維持されます。

ただし、ルーテッド展開またはスイッチド展開の場合、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。アップグレードの完了時には、デバイスの役割は切り替わったままです。アクティブ/スタンバイの役割を維持する場合、アップグレード前に役割を手動で切り替えます。それにより、アップグレードプロセスによって元の役割に切り替わります。

[Devices] > **[Device Management]** を選択し、ペアの横にある [Switch Active Peer] アイコンをクリックして、選択内容を確認します。

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

ステップ 3 使用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、アップグレードするデバイスを選択します。

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。

（注） [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 4 [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。

トラフィックは、デバイスの設定および展開方法に応じて、アップグレードの間ドロップするか、検査なしでネットワークを通過します。 詳細については、対象バージョンの Cisco Firepower リリース ノート 内の「ソフトウェアのアップグレード」の章を参照してください。

ステップ 5 アップグレードの進捗状況 をモニタします。

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

ステップ 6 アップグレードが成功したことを確認します。

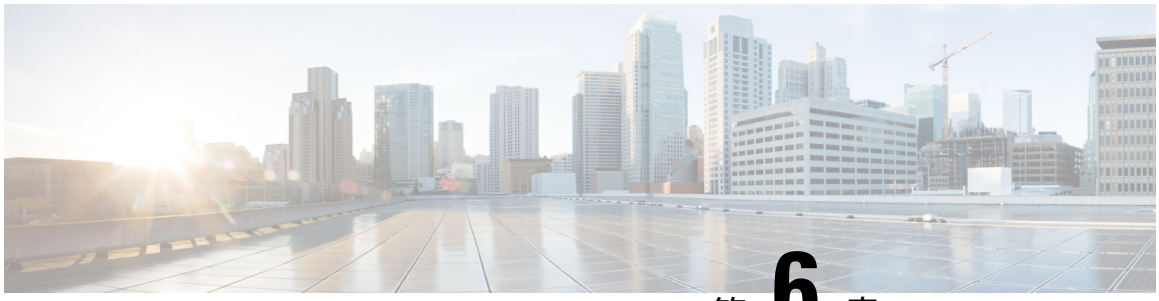
アップグレードが完了したら、**[Devices]** > **[Device Management]** を選択し、アップグレードしたデバイスのソフトウェアバージョンが正しいことを確認します。

ステップ 7 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 8 リリース ノートに記載されているアップグレード後の構成の変更をすべて完了します。

ステップ 9 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

ASA with FirePOWER サービスのアップグレード

アップグレード チェックリスト：FMC を搭載した ASA FirePOWER

ASA with FirePOWER Services のアップグレードを行う前にこのチェックリストを完了します。

（注） プロセス中は常に、展開の通信と正常性を維持してください。進行中に ASA FirePOWER のアップグレードを再開しないでください。事前のチェック中に、アップグレードプロセスが停止しているように見える場合がありますが、これは想定内の動作です。アップグレードに失敗する、アプライアンスが応答しないなど、アップグレードで問題が発生した場合にはCisco TACにお問い合わせください。

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。

表 *43 :*

✓	アクション/チェック
	アップグレードパスを計画します。 これは、マルチアプライアンス展開、マルチホップアップグレード、または展開の互換性を常に維持しながら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。実行したアップグレードと次に実行するアップグレードを常に確認します。 （注） FMC 展開では、通常、FMC をアップグレードしてから、管理対象デバイスをアップグレードします。ただし、場合によっては、最初にデバイスをアップグレードする必要があります。 アップグレードパス （13 ページ）を参照してください。
	すべてのアップグレードの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。アップグレードの警告、動作の変更、新機能と廃止された機能、および既知の問題など、リリース固有の重要な情報を含むリリースノートから読み始めます。
	アプライアンスへのアクセスを確認します。 デバイスは、（インターフェイス設定に応じて）アップグレード中、またはアップグレードが失敗した場合に、トラフィックを渡すことを停止できます。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。FMC の展開では、デバイスを経由せずに FMC 管理インターフェイスにアクセスできる必要もあります。
	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。FMC の展開では、アップグレードパケージをアップグレード時に管理対象デバイスに転送する場合は、帯域幅が不十分だとアップグレード時間が長くなったり、アップグレードがタイムアウトする原因となったりする可能性があります。デバイスのアップグレードを開始する前に、可能な場合は常に、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。 『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
	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および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、ウィンドウで実行する必要があるタスクと、事前に実行できるタスクを検討します。 たとえば、メンテナンス時間帯で、アプライアンスへのアップグレードパッケージのコピー、準備状況チェックの実行、バックアップの作成などが行われるまで待機しないようにします。

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。

表 *44*：

✓	アクション/チェック
	アップグレードパッケージを FMC にアップロードします。 Firepower Management Center にアップロード （42 ページ） を参照してください。
	アップグレードパッケージをデバイスにコピーします。 FMC がバージョン 6.2.3 以降を実行している場合、デバイスのアップグレードを開始する前に、管理対象デバイスにパッケージをコピー（プッシュ）することをお勧めします。 管理対象デバイスへのコピー （44 ページ）を参照してください。

バックアップ

災害から回復する能力は、システム保守計画の重要な部分を占めます。

バックアップと復元は、複雑なプロセスになる可能性があります。手順をスキップしたり、セキュリティやライセンスの問題を無視しないでください。バックアップと復元の要件、ガイドライン、制限事項、およびベストプラクティスの詳細については、使用する展開の設定ガイドを参照してください。

⚠

注意 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。

表 *45：*

✓	アクション/チェック
	ASA をバックアップします。 ASDM または ASA CLI を使用して、アップグレードの前後に設定やその他の重要なファイルをバックアップしてます（特に ASA 設定の移行がある場合）。

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。

表 *46：*

✓	アクション/チェック
	ASA をアップグレードします。 必要に応じて、ASAをアップグレードします。 ASA と ASA FirePOWER のバージョンには幅広い互換性があります。ただし、アップグレードすると、新機能を利用でき、問題も解決されます。 スタンドアロンASAデバイスの場合、ASAをアップグレードしてリロードした直後に、ASA FirePOWER モジュールをアップグレードします。 ASA クラスタとフェールオーバペアの場合、トラフィックフローとインスペクションの中断を避けるには、これらのデバイスを一度に 1 台ずつ完全にアップグレードします。各ユニットをリロードして ASA をアップグレードする直前に、ASA FirePOWER モジュールをアップグレードします。 （注） ASAをアップグレードする前に、必ずすべてのアップグレードのガイドラインを読み、設定の変更を計画してください。ASAリリースノート：Cisco ASA リリースノート を使用して開始します。

最終チェック

一連の最終チェックにより、 をアップグレードする準備が整います。

表 *47：*

✓	アクション/チェック
	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。

✓	アクション/チェック
	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。同期されていないと、アップグレードが失敗する可能性があります。FMC 展開では、時刻のずれが 10 秒を超えている場合、ヘルスモニタからアラートが発行されますが、手動で確認する必要もあります。 時刻を確認するには、次の手順を実行します。 • FMC：[システム（System）] > [設定（Configuration）] > [時刻（Time）] を選択します。 • デバイス：**show time** CLI コマンドを使用します。
	ディスク容量を確認します。 ソフトウェアアップグレードに関するディスク容量チェックを実行します。空きディスク容量が十分でない場合、アップグレードは失敗します。 対象バージョンの Cisco Firepower リリース ノート 内の「ソフトウェアのアップグレード」の章を参照してください。
	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。 一部の展開では、設定が古い場合、アップグレードがブロックされることがあります。FMC における高可用性の展開では、アクティブなピアから展開するだけで済みます。 展開する際にリソースを要求すると、いくつかのパケットがインスペクションなしでドロップされることがあります。 さらに、いくつかの設定を展開することで Snort が再起動されます。これにより、トラフィックのインスペクションが中断し、デバイスのトラフィックの処理方法によっては、再起動が完了するまでトラフィックが中断する場合があります。 対象バージョンの Cisco Firepower リリース ノート 内の「ソフトウェアのアップグレード」の章を参照してください。
	古いデバイスで ASA REST API を無効化します。 現在、バージョン 6.3.0 以前を実行している ASA FirePOWER モジュールをアップグレードする前に、ASA REST API を無効にしていることを確認します。無効にしていない場合、アップグレードが失敗することがあります。ASA CLI から：`no rest api agent`。アップグレード後に再度有効できます：`rest-api agent`。

✓	アクション/チェック
	準備状況チェックを実行します。 FMC がバージョン 6.1.0 以降を実行している場合は、互換性と準備状況のチェックの実施をお勧めします。これらのチェックにより、ソフトウェアをアップグレードするための準備状況を確認できます。 Firepower ソフトウェアの準備状況チェック （46 ページ）を参照してください。
	実行中のタスクを確認します。 アップグレードする前に、デバイスの重要なタスク（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。また、アップグレード中に実行するようにスケジュールされたタスクを確認し、それらをキャンセルまたは延期することをお勧めします。

ASA のアップグレード

スタンドアロン、フェールオーバー、またはクラスタリング展開の ASA と ASDM をアップグレードするには、このセクションの手順を使用します。

スタンドアロンユニットのアップグレード

スタンドアロンユニットをアップグレードするには CLI または ASDM を使用します。

CLI を使用したスタンドアロンユニットのアップグレード

ここでは、ASDMイメージおよびASAイメージをインストールする方法について説明します。また、ASA FirePower モジュールをアップグレードするタイミングについても説明します。

始める前に

この手順では、FTP を使用します。TFTP、HTTP、またはその他のサーバー タイプについては、『ASA Command Reference』の **copy** コマンドを参照してください。

ステップ 1 特権 EXEC モードで、ASA ソフトウェアをフラッシュメモリにコピーします。

copy ftp://[[*user*[**:***password*]**@**]*server*[*/path*]*/asa_image_name* **disk***n***:/**[*path/*]*asa_image_name*

例：

```
ciscoasa# copy ftp://jcrichton:aeryn@10.1.1.1/asa-9-12-1-smp-k8.bin disk0:/asa-9-12-1-smp-k8.bin
```

ステップ 2 ASDM イメージをフラッシュメモリにコピーします。

copy ftp://[[*user*[**:***password*]**@**]*server*[*/path*]*/asdm_image_name* **disk***n***:/**[*path/*]*asdm_image_name*

例：

```
ciscoasa# copy ftp://jcrichton:aeryn@10.1.1.1/asdm-7121.bin disk0:/asdm-7121.bin
```

ステップ 3 グローバル コンフィギュレーション モードにアクセスします。

configure terminal

例：

```
ciscoasa# configure terminal
ciscoasa(config)#
```

ステップ 4 設定されている現在のブート イメージを表示します（最大 4 個）。

show running-config boot system

ASA は、表示された順序でイメージを使用します。最初のイメージが使用できない場合は次のイメージが使用され、以下同様です。新しいイメージURLをリストの先頭に挿入することはできません。新しいイメージが先頭であることを指定するには、既存のエントリをすべて削除してから、次の手順に従ってイメージの URL を目的の順序で入力します。

例：

```
ciscoasa(config)# show running-config boot system
boot system disk0:/cdisk.bin
boot system disk0:/asa931-smp-k8.bin
```

ステップ 5 既存のブートイメージコンフィギュレーションがある場合は削除します。新しいブートイメージを最初の選択肢として入力できるようにするためです。

no boot system disk*n***:/**[*path/*]*asa_image_name*

例：

```
ciscoasa(config)# no boot system disk0:/cdisk.bin
ciscoasa(config)# no boot system disk0:/asa931-smp-k8.bin
```

ステップ 6 ブートする ASA イメージを設定します（先ほどアップロードしたもの）。

boot system disk*n***:/**[*path/*]*asa_image_name*

このイメージが使用できない場合に使用するバックアップ イメージに対して、このコマンドを繰り返します。たとえば、先ほど削除したイメージを再入力できます。

例：

```
ciscoasa(config)# boot system disk0:/asa-9-12-1-smp-k8.bin
```

ステップ 7 使用する ASDM イメージを設定します（先ほどアップロードしたもの）。

asdm image disk*n*:/[*path*/]*asdm_image_name*

使用するように設定できる ASDM イメージは 1 つだけであるため、最初に既存のコンフィギュレーションを削除する必要はありません。

例：

```
ciscoasa(config)# asdm image disk0:/asdm-7121.bin
```

ステップ 8 新しい設定をスタートアップ コンフィギュレーションに保存します。

write memory

ステップ 9 ASA をリロードします。

reload

ステップ 10 ASA FirePOWER モジュールをアップグレードする場合は、ASA REST API を無効にします。無効にしない場合アップグレードは失敗します。

no rest-api agent

次のコマンドを実行して、アップグレード後に REST API を再度有効にすることができます。

rest-api agent

（注） FirePOWER モジュールのバージョン 6.0 以降を実行している場合、ASA 5506-X シリーズは ASA の REST API をサポートしません。

ステップ 11 ASA FirePOWER モジュールをアップグレードします。

ASDM を使用したローカルコンピュータからのスタンドアロンユニットのアップグレード

Upgrade Software from Local Computer ツールにより、コンピュータからフラッシュファイルシステムにイメージファイルをアップロードし、ASA をアップグレードできます。

ステップ 1 メイン ASDM アプリケーション ウィンドウで、**[Tools]** > **[Upgrade Software from Local Computer]** の順に選択します。

[Upgrade Software] ダイアログボックスが表示されます。

ステップ 2 [アップロードするイメージ（Image to Upload）] ドロップダウン リストから、[ASDM] を選択します。

ステップ 3 [Local File Path] フィールドで [Browse Local Files] をクリックして PC 上のファイルを見つけます。

ステップ 4 [Flash File System Path] フィールドで [Browse Flash] をクリックしてフラッシュ ファイル システム上のディレクトリまたはファイルを見つけます。

ステップ 5 [イメージのアップロード（Upload Image）] をクリックします。

アップグレード プロセスには数分かかる場合があります。

ステップ 6 このイメージを ASDM イメージとして設定するように求められます。[Yes] をクリックします。

ステップ 7 ASDM を終了して、コンフィギュレーションを保存したことを確認します。[OK] をクリックします。

アップグレード ツールを終了します。**注**：ASA ソフトウェアをアップグレードした後で、設定を保存し、ASDM を終了して再接続します。

ステップ 8 これらの手順を繰り返し、[Image to Upload] ドロップダウンリストで [ASA] を選択します。この手順は、その他のタイプのファイルのアップロードでも同じです。

ステップ 9 **[Tools]** > **[System Reload]** を選択して、ASA をリロードします。

リロードの詳細の確認を求める新しいウィンドウが表示されます。

a) [Save the running configuration at the time of reload] オプション ボタン（デフォルト）をクリックします。
b) リロードする時刻を選択します（たとえば、デフォルトの [Now]）。
c) [Schedule Reload] をクリックします。

リロードが開始されると、[Reload Status] ウィンドウにリロードの進行状況が表示されます。ASDM を終了するオプションも表示されます。

ステップ 10 ASA のリロード後、ASDM を再起動します。

コンソール ポートでリロードの状況を確認できます。または、数分待った後に ASDM を使用して、接続可能になるまで再試行することもできます。

ステップ 11 ASA FirePOWER モジュールをアップグレードする場合は、**[ツール（Tools）]** > **[コマンドラインインターフェイス（Command Line Interface）]** を選択し、 **no rest-api agent** を入力して ASA REST API を無効にします。

REST API を無効にしない場合、ASA FirePOWER モジュールのアップグレードは失敗します。次のコマンドを実行して、アップグレード後に REST API を再度有効にすることができます。

rest-api agent

（注） FirePOWER モジュールのバージョン 6.0 以降を実行している場合、ASA 5506-X シリーズは ASA の REST API をサポートしません。

ステップ 12 ASA FirePOWER モジュールをアップグレードします。

ASDM Cisco.com ウィザードを使用したスタンドアロンユニットのアップグレード

Upgrade Software from Cisco.com Wizard により、ASDM および ASA を最新のバージョンに自動的にアップグレードできます。

このウィザードでは、次の操作を実行できます。

- アップグレード用の ASA イメージ ファイルまたは ASDM イメージ ファイルを選択する。

（注） ASDM は最新のイメージバージョンをダウンロードし、そこにはビルド番号が含まれています。たとえば、9.9(1) をダウンロードする場合に、ダウンロードが 9.9(1.2) となる可能性があります。この動作は想定されているため、計画したアップグレードを続行できます。

- 実行したアップグレードの変更点を確認する。
- イメージをダウンロードし、インストールする。
- インストールのステータスを確認する。
- インストールが正常に完了した場合は、ASA をリロードして、コンフィギュレーションを保存し、アップグレードを完了する。

始める前に

内部的な変更により、このウィザードでは ASDM 7.10(1) 以降の使用のみがサポートされています。また、イメージの命名が変更されたため、ASA 9.10(1) 以降にアップグレードするには、ASDM 7.12(1) 以降を使用する必要があります。ASDM は ASA の以前のリリースと下位互換性があるため、実行している ASA バージョンを問わず、ASDM をアップグレードすることができます。

ステップ 1 **[Tools]** > **[Check for ASA/ASDM Updates]** を選択します。

マルチコンテキストモードでは、システムからこのメニューにアクセスします。

[Cisco.com Authentication] ダイアログボックスが表示されます。

ステップ 2 Cisco.com のユーザー ID とパスワードを入力して、[Login] をクリックします。

[Cisco.com Upgrade Wizard] が表示されます。

（注） 利用可能なアップグレードがない場合は、ダイアログボックスが表示されます。ウィザードを終了するには、[OK] をクリックします。

ステップ 3 [Next] をクリックして [Select Software] 画面を表示します。

現在の ASA バージョンおよび ASDM バージョンが表示されます。

ステップ 4 ASA バージョンおよび ASDM バージョンをアップグレードするには、次の手順を実行します。

a) [ASA] 領域で、[Upgrade to] チェックボックスをオンにしてから、アップグレードする ASA バージョンをドロップダウン リストから選択します。

b) [ASDM] 領域で、[Upgrade to] チェックボックスをオンにしてから、アップグレードする ASDM バージョンをドロップダウン リストから選択します。

ステップ 5 [Next] をクリックして [Review Changes] 画面を表示します。

ステップ 6 次の項目を確認します。

- ダウンロードした ASA イメージ ファイルや ASDM イメージ ファイルが正しいファイルであること。
- アップロードする ASA イメージ ファイルや ASDM イメージ ファイルが正しいファイルであること。
- 正しい ASA ブート イメージが選択されていること。

ステップ 7 [Next] をクリックして、アップグレード インストールを開始します。

アップグレード インストールの進行状況を示すステータスを表示できます。

[Results] 画面が表示され、アップグレード インストール ステータス（成功または失敗）など、追加の詳細が示されます。

ステップ 8 アップグレード インストールが成功した場合に、アップグレード バージョンを有効にするには、[Save configuration and reload device now] チェックボックスをオンにして、ASA を再起動し、ASDM を再起動します。

ステップ 9 [Finish] をクリックして、ウィザードを終了し、コンフィギュレーションに対して行った変更を保存します。

（注） 次に高いバージョン（存在する場合）にアップグレードするには、ウィザードを再起動する必要があります。

ステップ 10 ASA のリロード後、ASDM を再起動します。

コンソール ポートでリロードの状況を確認できます。または、数分待った後に ASDM を使用して、接続可能になるまで再試行することもできます。

ステップ 11 ASA FirePOWER モジュールをアップグレードする場合は、**[ツール（Tools）]** > **[コマンドラインインターフェイス（Command Line Interface）]** を選択し、 **no rest-api agent** を入力して ASA REST API を無効にします。

REST API を無効にしない場合、ASA FirePOWER モジュールのアップグレードは失敗します。次のコマンドを実行して、アップグレード後に REST API を再度有効にすることができます。

rest-api agent

（注） FirePOWER モジュールのバージョン 6.0 以降を実行している場合、ASA 5506-X シリーズは ASA の REST API をサポートしません。

ステップ 12 ASA FirePOWER モジュールをアップグレードします。

アクティブ/スタンバイ フェールオーバー ペアのアップグレード

アクティブ/スタンバイ フェールオーバー ペアをアップグレードしてゼロ ダウンタイム アップグレードを実現するには、CLI または ASDM を使用します。

CLI を使用したアクティブ/スタンバイ フェールオーバー ペアのアップグレード

アクティブ/スタンバイ フェールオーバー ペアをアップグレードするには、次の手順を実行します。

始める前に

- アクティブ装置で次の手順を実行します。SSH アクセスの場合、アクティブな IP アドレスに接続します。アクティブ装置は常にこの IP アドレスを保有しています。CLI に接続する場合は、ASA プロンプトを調べてフェールオーバー ステータスを確認します。フェールオーバー ステータスと優先順位（プライマリまたはセカンダリ）を表示するように ASA プロンプトを設定できます。これは、接続しているユニットを特定するのに役立ちます。prompt コマンドを参照してください。代わりに、**show failover** コマンドを入力して、このユニットのステータスと優先順位（プライマリまたはセカンダリ）を表示します。
- この手順では、FTP を使用します。TFTP、HTTP、またはその他のサーバー タイプについては、『ASA Command Reference』の **copy** コマンドを参照してください。

ステップ 1 特権 EXEC モード時にアクティブ装置で、ASA ソフトウェアをアクティブ装置のフラッシュ メモリにコピーします。

copy ftp://[[*user*[**:***password*]**@**]*server*[*/path*]*/asa_image_name* **disk***n***:/**[*path/*]*asa_image_name*

例：

```
asa/act# copy ftp://jcrichton:aeryn@10.1.1.1/asa9829-15-1-smp-k8.bin disk0:/asa9829-15-1-smp-k8.bin
```

ステップ 2 ソフトウェアをスタンバイ装置にコピーします。アクティブ装置で指定したのと同じパスを指定してください。

failover exec mate copy /noconfirm ftp://[[*user*[**:***password*]**@**]*server*[*/path*]*/asa_image_name*
disk*n***:/**[*path/*]*asa_image_name*

例：

```
asa/act# failover exec mate copy /noconfirm ftp://jcrichton:aeryn@10.1.1.1/asa9829-15-1-smp-k8.bin
 disk0:/asa9829-15-1-smp-k8.bin
```

ステップ 3 ASDM イメージをアクティブ装置のフラッシュ メモリにコピーします。

copy ftp://[[*user*[**:***password*]**@**]*server*[*/path*]*/asdm_image_name* **disk***n***:/**[*path/*]*asdm_image_name*

例：

```
asa/act# copy ftp://jcrichton:aeryn@10.1.1.1/asdm-77178271417151.bin disk0:/asdm-77178271417151.bin
```

ステップ 4 ASDM イメージをスタンバイ装置にコピーします。アクティブ装置で指定したのと同じパスを指定してください。

failover exec mate copy /noconfirm ftp://[[*user*[**:***password*]**@**]*server*[*/path*]/*asdm_image_name*
disk*n***:/**[*path/*]*asdm_image_name*

例：

```
asa/act# failover exec mate copy /noconfirm ftp://jcrichton:aeryn@10.1.1.1/asdm-77178271417151.bin
 disk0:/asdm-77178271417151.bin
```

ステップ 5 まだグローバル コンフィギュレーション モードを開始していない場合は、グローバル コンフィギュレーション モードを開始します。

configure terminal

ステップ 6 設定されている現在のブート イメージを表示します（最大 4 個）。

show running-config boot system

例：

```
asa/act(config)# show running-config boot system
boot system disk0:/cdisk.bin
boot system disk0:/asa931-smp-k8.bin
```

ASA は、表示された順序でイメージを使用します。最初のイメージが使用できない場合は次のイメージが使用され、以下同様です。新しいイメージ URL をリストの先頭に挿入することはできません。新しいイメージが先頭であることを指定するには、既存のエントリをすべて削除してから、次の手順に従ってイメージの URL を目的の順序で入力します。

ステップ 7 既存のブートイメージコンフィギュレーションがある場合は削除します。新しいブートイメージを最初の選択肢として入力できるようにするためです。

no boot system disk*n***:/**[*path/*]*asa_image_name*

例：

```
asa/act(config)# no boot system disk0:/cdisk.bin
asa/act(config)# no boot system disk0:/asa931-smp-k8.bin
```

ステップ 8 ブートする ASA イメージを設定します（先ほどアップロードしたもの）。

boot system disk*n***:/**[*path/*]*asa_image_name*

例：

```
asa/act(config)# boot system disk0://asa9829-15-1-smp-k8.bin
```

このイメージが使用できない場合に使用するバックアップ イメージに対して、このコマンドを繰り返します。たとえば、先ほど削除したイメージを再入力できます。

ステップ 9 使用する ASDM イメージを設定します（先ほどアップロードしたもの）。

asdm image disk*n***:/**[*path/*]*asdm_image_name*

例：

```
asa/act(config)# asdm image disk0:/asdm-77178271417151.bin
```

使用するように設定できる ASDM イメージは 1 つだけであるため、最初に既存のコンフィギュレーションを削除する必要はありません。

ステップ 10 新しい設定をスタートアップ コンフィギュレーションに保存します。

write memory

これらの設定変更は、スタンバイ ユニットに自動的に保存されます。

ステップ 11 ASA FirePOWER モジュールをアップグレードする場合は、ASA REST API を無効にします。無効にしない場合アップグレードは失敗します。

no rest-api agent

ステップ 12 スタンバイ装置の ASA FirePOWER モジュールをアップグレードします。

ASDM によって管理される ASA FirePOWER モジュールの場合、ASDM をスタンバイ管理 IP アドレスに接続します。アップグレードが完了するまで待ちます。

ステップ 13 スタンバイ装置をリロードして新しいイメージを起動します。

failover reload-standby

スタンバイ装置のロードが完了するまで待ちます。**show failover** コマンドを使用して、スタンバイ ユニットが Standby Ready 状態かどうかを検証します。

ステップ 14 強制的にアクティブ装置からスタンバイ装置へのフェールオーバーを行います。

no failover active

SSH セッションから切断されている場合は、新しいアクティブ/元のスタンバイ ユニット上に現在あるメイン IP アドレスに再接続します。

ステップ 15 以前のアクティブ装置の ASA FirePOWER モジュールをアップグレードします。

ASDM によって管理される ASA FirePOWER モジュールの場合、ASDM をスタンバイ管理 IP アドレスに接続します。アップグレードが完了するまで待ちます。

ステップ 16 新しいアクティブ装置から、元のアクティブ装置（今の新しいスタンバイ装置）をリロードします。

failover reload-standby

例：

```
asa/act# failover reload-standby
```

（注） 元のアクティブ ユニットのコンソール ポートに接続されている場合は、代わりに **reload** コマンドを入力して、元のアクティブ ユニットをリロードする必要があります。

ASDM を使用したアクティブ/スタンバイ フェールオーバー ペアのアップグレード

アクティブ/スタンバイ フェールオーバー ペアをアップグレードするには、次の手順を実行します。

始める前に

ローカル管理コンピュータに ASA と ASDM のイメージを配置します。

ステップ 1 スタンバイ IP アドレスに接続して、*standby* ユニット上で ASDM を起動します。

ステップ 2 メイン ASDM アプリケーション ウィンドウで、**[Tools]** > **[Upgrade Software from Local Computer]** の順に選択します。

[Upgrade Software] ダイアログボックスが表示されます。

ステップ 3 [アップロードするイメージ（Image to Upload）] ドロップダウン リストから、[ASDM] を選択します。

ステップ 4 [Local File Path] フィールドにコンピュータ上のファイルへのローカル パスを入力するか、[Browse Local Files] をクリックして PC 上のファイルを見つけます。

ステップ 5 [Flash File System Path] フィールドにフラッシュファイルシステムへのパスを入力するか、[Browse Flash] をクリックしてフラッシュファイルシステム上のディレクトリまたはファイルを検索します。

ステップ 6 [イメージのアップロード（Upload Image）] をクリックします。アップグレード プロセスには数分かかる場合があります。

このイメージを ASA イメージとして設定するように求められる場合は、[No] をクリックします。アップグレード ツールを終了します。

ステップ 7 これらの手順を繰り返し、[Image to Upload] ドロップダウン リストで [ASA] を選択します。

このイメージを ASA イメージとして設定するように求められる場合は、[No] をクリックします。アップグレード ツールを終了します。

ステップ 8 メイン IP アドレスに接続して ASDM をアクティブなユニットに接続し、スタンバイ ユニットで使用したのと同じファイルの場所を使用して、ASDM ソフトウェアをアップロードします。

ステップ 9 このイメージを ASDM イメージとして設定するように求められたら、[Yes] をクリックします。

ASDM を終了して、コンフィギュレーションを保存したことを確認します。[OK] をクリックします。アップグレード ツールを終了します。**注**：ASA ソフトウェアをアップグレードした後で、設定を保存し、ASDM をリロードします。

ステップ 10 スタンバイ ユニットで使用したのと同じファイルの場所を使用して、ASA ソフトウェアをアップロードします。

ステップ 11 このイメージを ASA イメージとして設定するように求められたら、[Yes] をクリックします。

新しいイメージを使用するために、ASA をリロードするよう求められます。[OK] をクリックします。アップグレード ツールを終了します。

ステップ 12 コンフィギュレーションの変更を保存するには、ツールバーの [Save] アイコンをクリックします。

これらの設定変更は、スタンバイ ユニットに自動的に保存されます。

ステップ 13 ASA FirePOWER モジュールをアップグレードする場合は、**[ツール（Tools）]** > **[コマンドラインインターフェイス（Command Line Interface）]** を選択し、**no rest-api enable** を入力して ASA REST API を無効にします。

REST API を無効にしない場合、ASA FirePOWER モジュールのアップグレードは失敗します。

ステップ 14 スタンバイ装置の ASA FirePOWER モジュールをアップグレードします。

ASDM によって管理される ASA FirePOWER モジュールの場合、ASDM をスタンバイ管理 IP アドレスに接続します。アップグレードの完了を待ってから、ASDM をアクティブ装置に接続します。

ステップ 15 **[モニタリング（Monitoring）]** > **[プロパティ（Properties）]** > **[フェールオーバー（Failover）]** > **[ステータス（Status）]** の順に選択し、[スタンバイのリロード（Reload Standby）] をクリックして、スタンバイ装置をリロードします。

[システム（System）] ペインを開いたまま、スタンバイ ユニットがリロードされるのを確認します。

ステップ 16 スタンバイ ユニットがリロードしたら、**[Monitoring]** > **[Properties]** > **[Failover]** > **[Status]** の順に選択し、[Make Standby] をクリックして、アクティブなユニットをスタンバイ ユニットにフェールオーバーします。

ASDM は新しいアクティブ ユニットに自動的に再接続されます。

ステップ 17 以前のアクティブ装置の ASA FirePOWER モジュールをアップグレードします。

ASDM によって管理される ASA FirePOWER モジュールの場合、ASDM をスタンバイ管理 IP アドレスに接続します。アップグレードの完了を待ってから、ASDM をアクティブ装置に接続します。

ステップ 18 **[モニタリング（Monitoring）]** > **[プロパティ（Properties）]** > **[フェールオーバー（Failover）]** > **[ステータス（Status）]** の順に選択し、[スタンバイのリロード（Reload Standby）] をクリックして、（新しい）スタンバイユニットをリロードします。

アクティブ/アクティブ フェールオーバー ペアのアップグレード

アクティブ/アクティブ フェールオーバー ペアをアップグレードしてゼロ ダウンタイム アップグレードを実現するには、CLI または ASDM を使用します。

CLI を使用したアクティブ/アクティブ フェールオーバー ペアのアップグレード

アクティブ/アクティブ フェールオーバー コンフィギュレーションの 2 つの装置をアップグレードするには、次の手順を実行します。

始める前に

- 標準出荷単位で次の手順を実行します。
- これらの手順をシステム実行スペースで実行します。
- この手順では、FTP を使用します。TFTP、HTTP、またはその他のサーバー タイプについては、『ASA Command Reference』の **copy** コマンドを参照してください。

ステップ 1 特権EXECモード時にプライマリ ユニットで、ASA ソフトウェアをフラッシュ メモリにコピーします。

copy ftp://[[*user*[**:***password*]**@**]*server*[*/path*]*/asa_image_name* **disk***n***:/**[*path/*]*asa_image_name*

例：

```
asa/act/pri# copy ftp://jcrichton:aeryn@10.1.1.1/asa9829-15-1-smp-k8.bin
disk0:/asa9829-15-1-smp-k8.bin
```

ステップ 2 ソフトウェアをセカンダリ装置にコピーします。プライマリ装置で指定したのと同じパスを指定してください。

failover exec mate copy /noconfirm ftp://[[*user*[**:***password*]**@**]*server*[*/path*]*/asa_image_name* **disk***n***:/**[*path/*]*asa_image_name*

例：

```
asa/act/pri# failover exec mate copy /noconfirm
ftp://jcrichton:aeryn@10.1.1.1/asa9829-15-1-smp-k8.bin disk0:/asa9829-15-1-smp-k8.bin
```

ステップ 3 ASDM イメージをプライマリ装置のフラッシュ メモリにコピーします。

copy ftp://[[*user*[**:***password*]**@**]*server*[*/path*]*/asdm_image_name* **disk***n***:/**[*path/*]*asdm_image_name*

例：

```
asa/act/pri# ciscoasa# copy ftp://jcrichton:aeryn@10.1.1.1/asdm-77178271417151.bin
disk0:/asdm-77178271417151.bin
```

ステップ 4 ASDM イメージをセカンダリ装置にコピーします。標準出荷単位で指定したのと同じパスを指定してください。

failover exec mate copy /noconfirm ftp://[[*user*[**:***password*]**@**]*server*[*/path*]*/asdm_image_name* **disk***n***:/**[*path/*]*asdm_image_name*

例：

```
asa/act/pri# failover exec mate copy /noconfirm
ftp://jcrichton:aeryn@10.1.1.1/asdm-77178271417151.bin disk0:/asdm-77178271417151.bin
```

ステップ 5 まだグローバル コンフィギュレーション モードを開始していない場合は、グローバル コンフィギュレーション モードを開始します。

configure terminal

ステップ 6 設定されている現在のブート イメージを表示します（最大 4 個）。

show running-config boot system

例：

```
asa/act/pri(config)# show running-config boot system
boot system disk0:/cdisk.bin
```

```
boot system disk0:/asa931-smp-k8.bin
```

ASA は、表示された順序でイメージを使用します。最初のイメージが使用できない場合は次のイメージが使用され、以下同様です。新しいイメージURLをリストの先頭に挿入することはできません。新しいイメージが先頭であることを指定するには、既存のエントリをすべて削除してから、次の手順に従ってイメージの URL を目的の順序で入力します。

ステップ 7 既存のブートイメージコンフィギュレーションがある場合は削除します。新しいブートイメージを最初の選択肢として入力できるようにするためです。

no boot system disk*n***:/**[*path*/]*asa_image_name*

例：

```
asa/act/pri(config)# no boot system disk0:/cdisk.bin
asa/act/pri(config)# no boot system disk0:/asa931-smp-k8.bin
```

ステップ 8 ブートする ASA イメージを設定します（先ほどアップロードしたもの）。

boot system disk*n***:/**[*path*/]*asa_image_name*

例：

```
asa/act/pri(config)# boot system disk0://asa9829-15-1-smp-k8.bin
```

このイメージが使用できない場合に使用するバックアップ イメージに対して、このコマンドを繰り返します。たとえば、先ほど削除したイメージを再入力できます。

ステップ 9 使用する ASDM イメージを設定します（先ほどアップロードしたもの）。

asdm image disk*n***:/**[*path*/]*asdm_image_name*

例：

```
asa/act/pri(config)# asdm image disk0:/asdm-77178271417151.bin
```

使用するように設定できる ASDM イメージは 1 つだけであるため、最初に既存のコンフィギュレーションを削除する必要はありません。

ステップ 10 新しい設定をスタートアップ コンフィギュレーションに保存します。

write memory

これらの設定変更は、セカンダリ ユニットに自動的に保存されます。

ステップ 11 ASA FirePOWER モジュールをアップグレードする場合は、ASA REST API を無効にします。無効にしない場合アップグレードは失敗します。

no rest-api agent

ステップ 12 プライマリ装置の両方のフェールオーバー グループをアクティブにします。

failover active group 1

failover active group 2

例：

```
asa/act/pri(config)# failover active group 1
asa/act/pri(config)# failover active group 2
```

ステップ 13 セカンダリ ユニットの ASA FirePOWER モジュールをアップグレードします。

ASDM によって管理される ASA FirePOWER モジュールの場合、ASDM をフェールオーバー グループ 1 または 2 のスタンバイ管理 IP アドレスに接続します。アップグレードが完了するまで待ちます。

ステップ 14 セカンダリ装置をリロードして新しいイメージを起動します。

failover reload-standby

セカンダリ装置のロードが完了するまで待ちます。**show failover** コマンドを使用して、両方のフェールオーバー グループが Standby Ready 状態であることを確認します。

ステップ 15 セカンダリ装置で、両方のフェールオーバー グループを強制的にアクティブにします。

no failover active group 1

no failover active group 2

例：

```
asa/act/pri(config)# no failover active group 1
asa/act/pri(config)# no failover active group 2
asa/stby/pri(config)#
```

SSH セッションから切断されている場合は、セカンダリ ユニット上に現在あるフェールオーバー グループ 1 の IP アドレスに再接続します。

ステップ 16 プライマリ ユニットの ASA FirePOWER モジュールをアップグレードします。

ASDM によって管理される ASA FirePOWER モジュールの場合、ASDM をフェールオーバー グループ 1 または 2 のスタンバイ管理 IP アドレスに接続します。アップグレードが完了するまで待ちます。

ステップ 17 プライマリ装置をリロードします。

failover reload-standby

例：

```
asa/act/sec# failover reload-standby
```

（注） プライマリ ユニットのコンソール ポートに接続されている場合は、代わりに **reload** コマンドを入力して、プライマリ ユニットをリロードする必要があります。

SSH セッションから切断される場合があります。

ステップ 18 フェールオーバー グループは、**preempt** コマンドを使用して設定されている場合、プリエンプト遅延の経過後、指定された装置で自動的にアクティブになります。

ASDM を使用したアクティブ/アクティブ フェールオーバー ペアのアップグレード

アクティブ/アクティブ フェールオーバー コンフィギュレーションの 2 つの装置をアップグレードするには、次の手順を実行します。

始める前に

- これらの手順をシステム実行スペースで実行します。
- ローカル管理コンピュータに ASA と ASDM のイメージを配置します。

ステップ 1 フェールオーバー グループ 2 の管理アドレスに接続して、セカンダリ ユニットで ASDM を起動します。

ステップ 2 メイン ASDM アプリケーション ウィンドウで、**[Tools] > [Upgrade Software from Local Computer]** の順に選択します。

[Upgrade Software] ダイアログボックスが表示されます。

ステップ 3 [アップロードするイメージ（Image to Upload）] ドロップダウン リストから、[ASDM] を選択します。

ステップ 4 [Local File Path] フィールドにコンピュータ上のファイルへのローカル パスを入力するか、[Browse Local Files] をクリックして PC 上のファイルを見つけます。

ステップ 5 [Flash File System Path] フィールドにフラッシュファイルシステムへのパスを入力するか、[Browse Flash] をクリックしてフラッシュファイルシステム上のディレクトリまたはファイルを検索します。

ステップ 6 [イメージのアップロード（Upload Image）] をクリックします。アップグレード プロセスには数分かかる場合があります。

このイメージを ASA イメージとして設定するように求められる場合は、[No] をクリックします。アップグレード ツールを終了します。

ステップ 7 これらの手順を繰り返し、[Image to Upload] ドロップダウン リストで [ASA] を選択します。

このイメージを ASA イメージとして設定するように求められる場合は、[No] をクリックします。アップグレード ツールを終了します。

ステップ 8 フェールオーバー グループ 1 の管理 IP アドレスに接続して ASDM をプライマリ ユニットに接続し、セカンダリ ユニットで使用したのと同じファイルの場所を使用して、ASDM ソフトウェアをアップロードします。

ステップ 9 このイメージを ASDM イメージとして設定するように求められたら、[Yes] をクリックします。

ASDM を終了して、コンフィギュレーションを保存したことを確認します。[OK] をクリックします。アップグレード ツールを終了します。**注**：ASA ソフトウェアをアップグレードした後で、設定を保存し、ASDM をリロードします。

ステップ 10 セカンダリ ユニットで使用したのと同じファイルの場所を使用して、ASA ソフトウェアをアップロードします。

ステップ 11 このイメージを ASA イメージとして設定するように求められたら、[Yes] をクリックします。

新しいイメージを使用するために、ASA をリロードするよう求められます。[OK] をクリックします。アップグレード ツールを終了します。

ステップ 12 コンフィギュレーションの変更を保存するには、ツールバーの [Save] アイコンをクリックします。

これらの設定変更は、セカンダリ ユニットに自動的に保存されます。

ステップ 13 ASA FirePOWER モジュールをアップグレードする場合は、**[ツール（Tools）]** > **[コマンドラインインターフェイス（Command Line Interface）]** を選択し、**no rest-api enable** を入力して ASA REST API を無効にします。

REST API を無効にしない場合、ASA FirePOWER モジュールのアップグレードは失敗します。

ステップ 14 **[Monitoring]** > **[Failover]** > **[Failover Group #]** の順に選択して、プライマリ ユニット上の両方のフェールオーバー グループをアクティブにします。ここで # は、プライマリ ユニットに移動するフェールオーバー グループの数です。[Make Active] をクリックします。

ステップ 15 セカンダリ ユニットの ASA FirePOWER モジュールをアップグレードします。

ASDM によって管理される ASA FirePOWER モジュールの場合、ASDM をフェールオーバー グループ 1 または 2 のスタンバイ管理 IP アドレスに接続します。アップグレードの完了を待ってから、ASDM をプライマリ ユニットに接続します。

ステップ 16 **[Monitoring]** > **[Failover]** > **[System]** の順に選択し、[Reload Standby] をクリックして、セカンダリユニットをリロードします。

[System] ペインを開いたまま、セカンダリユニットがリロードされるのを確認します。

ステップ 17 セカンダリ ユニットが起動したら、**[Monitoring]** > **[Failover]** > **[Failover Group #]** の順に選択して、セカンダリ ユニット上の両方のフェールオーバー グループをアクティブにします。ここで # は、セカンダリユニットに移動するフェールオーバー グループの数です。[Make Standby] をクリックします。

ASDM は、セカンダリ ユニット上のフェールオーバー グループ 1 の IP アドレスに自動的に再接続されます。

ステップ 18 プライマリ ユニットの ASA FirePOWER モジュールをアップグレードします。

ASDM によって管理される ASA FirePOWER モジュールの場合、ASDM をフェールオーバー グループ 1 または 2 のスタンバイ管理 IP アドレスに接続します。アップグレードの完了を待ってから、ASDM をセカンダリ ユニットに接続します。

ステップ 19 **[Monitoring]** > **[Failover]** > **[System]** の順に選択し、[Reload Standby] をクリックして、プライマリユニットをリロードします。

ステップ 20 フェールオーバーグループは、[Preempt Enabled] を使用して設定されると、プリエンプト遅延の経過後、指定された装置で自動的にアクティブになります。ASDM は、プライマリ ユニット上のフェールオーバー グループ 1 の IP アドレスに自動的に再接続されます。

ASA クラスタのアップグレード

ASA クラスタをアップグレードしてゼロ ダウンタイム アップグレードを実現するには、CLI または ASDM を使用します。

CLI を使用した ASA クラスタのアップグレード

ASA クラスタ内のすべての装置をアップグレードするには、次の手順を実行します。この手順では、FTP を使用します。TFTP、HTTP、またはその他のサーバー タイプについては、『ASA Command Reference』の **copy** コマンドを参照してください。

始める前に

- 制御ユニットで次の手順を実行します。ASA FirePOWER モジュールもアップグレードしている場合は、各データユニットへのコンソールアクセスまたは ASDM アクセスが必要です。クラスタ ユニットと状態（制御またはデータ）を表示するように ASA プロンプトを設定できます。これは、接続しているユニットを特定するのに役立ちます。prompt コマンドを参照してください。代わりに、**show cluster info** コマンドを入力して、各ユニットの役割を表示します。
- コンソール ポートを使用する必要があります。クラスタリングのイネーブルまたはディセーブルを、リモート CLI 接続から行うことはできません。
- マルチ コンテキスト モードでは、システム実行スペースで後続の手順を実行します。

ステップ 1 特権 EXEC モード時に制御ユニットで、ASA ソフトウェアをクラスタ内のすべてのユニットにコピーします。

cluster exec copy /noconfirm ftp://[[*user*[**:***password*]**@**]*server*[*/path*]*/asa_image_name* **disk***n***:/**[*path/*]*asa_image_name*

例：

```
asa/unit1/master# cluster exec copy /noconfirm
ftp://jcrichton:aeryn@10.1.1.1/asa9829-15-1-smp-k8.bin disk0:/asa9829-15-1-smp-k8.bin
```

ステップ 2 ASDM イメージをクラスタ内のすべての装置にコピーします。

cluster exec copy /noconfirm ftp://[[*user*[**:***password*]**@**]*server*[*/path*]*/asdm_image_name*
disk*n***:/**[*path/*]*asdm_image_name*

例：

```
asa/unit1/master# cluster exec copy /noconfirm ftp://jcrichton:aeryn@10.1.1.1/asdm-77178271417151.bin
 disk0:/asdm-77178271417151.bin
```

ステップ 3 まだグローバル コンフィギュレーション モードを開始していない場合は、ここで開始します。

configure terminal

例：

```
asa/unit1/master# configure terminal
asa/unit1/master(config)#
```

ステップ 4 設定されている現在のブート イメージを表示します（最大 4 個）。

show running-config boot system

例：

```
asa/unit1/master(config)# show running-config boot system
boot system disk0:/cdisk.bin
boot system disk0:/asa931-smp-k8.bin
```

ASA は、表示された順序でイメージを使用します。最初のイメージが使用できない場合は次のイメージが使用され、以下同様です。新しいイメージURLをリストの先頭に挿入することはできません。新しいイメージが先頭であることを指定するには、既存のエントリをすべて削除してから、次の手順に従ってイメージの URL を目的の順序で入力します。

ステップ 5 既存のブートイメージコンフィギュレーションがある場合は削除します。新しいブートイメージを最初の選択肢として入力できるようにするためです。

no boot system disk*n***:/**[*path*/]*asa_image_name*

例：

```
asa/unit1/master(config)# no boot system disk0:/cdisk.bin
asa/unit1/master(config)# no boot system disk0:/asa931-smp-k8.bin
```

ステップ 6 ブートする ASA イメージを設定します（先ほどアップロードしたもの）。

boot system disk*n***:/**[*path*/]*asa_image_name*

例：

```
asa/unit1/master(config)# boot system disk0://asa9829-15-1-smp-k8.bin
```

このイメージが使用できない場合に使用するバックアップ イメージに対して、このコマンドを繰り返します。たとえば、先ほど削除したイメージを再入力できます。

ステップ 7 使用する ASDM イメージを設定します（先ほどアップロードしたもの）。

asdm image disk*n***:/**[*path*/]*asdm_image_name*

例：

```
asa/unit1/master(config)# asdm image disk0:/asdm-77178271417151.bin
```

使用するように設定できる ASDM イメージは 1 つだけであるため、最初に既存のコンフィギュレーションを削除する必要はありません。

ステップ 8 新しい設定をスタートアップ コンフィギュレーションに保存します。

write memory

これらの設定変更は、データユニットに自動的に保存されます。

ステップ 9 ASA FirePOWER モジュールをアップグレードする場合は、ASA REST API を無効にします。無効にしない場合、ASA FirePOWER モジュールのアップグレードは失敗します。

no rest-api agent

ステップ 10 ASDM によって管理されている ASA FirePOWER モジュールをアップグレードする場合、ASDM を個別の管理 IP アドレスに接続する必要があります。このため、各ユニットの IP アドレスをメモしておく必要があります。

show running-config interface *management_interface_id*

使用されている **cluster-pool** プール名をメモします。

show ip[**v6**] **local pool** *poolname*

クラスタ ユニットの IP アドレスをメモします。

例：

```
asa/unit2/slave# show running-config interface gigabitethernet0/0
!
interface GigabitEthernet0/0
 management-only
 nameif inside
 security-level 100
 ip address 10.86.118.1 255.255.252.0 cluster-pool inside-pool
asa/unit2/slave# show ip local pool inside-pool
Begin           End             Mask            Free     Held     In use
10.86.118.16    10.86.118.17    255.255.252.0       0        0        2

Cluster Unit                    IP Address Allocated
unit2                           10.86.118.16
unit1                           10.86.118.17
asa1/unit2/slave#
```

ステップ 11 データユニットをアップグレードします。

ASA FirePOWER モジュールもアップグレードするかどうかによって、以下の手順を選択します。ASA FirePOWER モジュールもアップグレードする場合、ASA FirePOWER プロシージャは ASA のリロードの回数を最小化します。以下の手順では、データコンソールまたは ASDM を使用するよう選択できます。すべてのコンソール ポートへのアクセスは準備できていないが、ASDM にネットワーク経由でアクセスできる場合は、コンソールではなく ASDM を使用することを推奨します。

（注） アップグレードプロセス中は、**cluster master unit** コマンドを使用して強制的にデータユニットを制御に変更しないでください。ネットワークの接続性とクラスタの安定性に関連した障害が発生する恐れがあります。最初にすべてのデータユニットをアップグレードしてリロードし、次にこの手順を実行すると、現在の制御ユニットから新しい制御ユニットへの移行をスムーズに行うことができます。

ASA FirePOWER モジュールをアップグレードしない場合：

a) 制御ユニットでメンバー名を表示するには、**cluster exec unit ?** または **show cluster info** コマンドを入力します。

b) データユニットをリロードします。

cluster exec unit *data-unit* **reload noconfirm**

例：

```
asa/unit1/master# cluster exec unit unit2 reload noconfirm
```

c) 各データユニットに対して手順を繰り返します。

接続損失を回避し、トラフィックを安定させるために、各装置が起動しクラスタに再接続するのを待ち（約 5 分）、次の装置にこれらの手順を繰り返します。装置がクラスタに再接続したことを確認するには、**show cluster info** を入力します。

ASA FirePOWER モジュールもアップグレードする場合（データコンソールを使用）：

a) データユニットのコンソールポートに接続し、グローバル コンフィギュレーション モードに入ります。

enable

configure terminal

例：

```
asa/unit2/slave> enable
Password:
asa/unit2/slave# configure terminal
asa/unit2/slave(config)#
```

b) クラスタリングを無効にします。

cluster group *name*

no enable

リロード時にクラスタリングを有効にするために、この構成を保存しないでください。複数の障害やアップグレード処理中の再参加を避けるために、クラスタリングを無効にする必要があります。このユニットでは、すべてのアップグレードとリロードが完了した後に再参加のみする必要があります。

例：

```
asa/unit2/slave(config)# cluster group cluster1
asa/unit2/slave(cfg-cluster)# no enable
Cluster disable is performing cleanup..done.
All data interfaces have been shutdown due to clustering being disabled. To recover either
enable clustering or remove cluster group configuration.

Cluster unit unit2 transitioned from SLAVE to DISABLED
asa/unit2/ClusterDisabled(cfg-cluster)#
```

c) このデータユニットの ASA FirePOWER モジュールをアップグレードします。

ASDM によって管理される ASA FirePOWER モジュールの場合、事前にメモした個別の管理 IP アドレスに ASDM を接続します。アップグレードが完了するまで待ちます。

d) データユニットをリロードします。

reload noconfirm

e) 各データユニットに対して手順を繰り返します。

接続損失を回避し、トラフィックを安定させるために、各装置が起動しクラスタに再接続するのを待ち（約 5 分）、次の装置にこれらの手順を繰り返します。装置がクラスタに再接続したことを確認するには、**show cluster info** を入力します。

ASA FirePOWER モジュールのアップグレードもある場合（ASDM を使用）：

a) 事前にメモしたこのデータユニットの「個別」の管理 IP アドレスに ASDM を接続します。
b) **[Configuration]** > **[Device Management]** > **[High Availability and Scalability]** > **[ASA Cluster]** > **[Cluster Configuration]** の順に選択します。
c) [ASAクラスタに参加（Participate in ASA cluster）] チェックボックスをオフにします。

複数の障害やアップグレード処理中の再参加を避けるために、クラスタリングを無効にする必要があります。このユニットでは、すべてのアップグレードとリロードが完了した後に再参加のみする必要があります。

[Configure ASA cluster settings] チェックボックスをオフにしないでください。オフにすると、すべてのクラスタ コンフィギュレーションがクリアされ、ASDM が接続されている管理インターフェイスを含むすべてのインターフェイスもシャットダウンします。この場合、接続を復元するには、コンソール ポートで CLI にアクセスする必要があります。

（注） ASDM の以前のバージョンは、この画面でのクラスタの無効化をサポートしていません。この場合、**[Tools]** > **[Command Line Interface]** ツールを使用します。[Multiple Line] ラジオボタンをクリックして、**cluster group** *name* と **no enable** を入力します。クラスタグループ名は、**[Home]** > **[Device Dashboard]** > **[Device Information]** > **[ASA Cluster]** エリアで確認できます。

d) [適用（Apply）] をクリックします。
e) ASDM から出るように促されます。同じ IP アドレスに ASDM を再接続します。
f) ASA FirePOWER モジュールをアップグレードします。

アップグレードが完了するまで待ちます。

g) ASDM で、**[Tools]** > **[System Reload]** を選択します。
h) [実行コンフィギュレーションを保存しないでリロードする（Reload without saving the running configuration）] オプション ボタンをクリックします。

この装置のリロード時にクラスタリングを有効にするために、この構成を保存しないようにします。

i) [Schedule Reload] をクリックします。
j) [Yes] をクリックしてリロードを続行します。
k) 各データユニットに対して手順を繰り返します。

接続損失を回避し、トラフィックを安定させるために、各装置が起動しクラスタに再接続するのを待ち（約5分）、次の装置にこれらの手順を繰り返します。装置がクラスタに再接続したことを確認するには、制御ユニットの **[Monitoring]** > **[ASA Cluster]** > **[Cluster Summary]** ペインを確認します。

ステップ 12 制御ユニットをアップグレードします。

a) クラスタリングを無効にします。

cluster group *name*

no enable

新しい制御ユニットが選択され、トラフィックが安定するまで 5 分間待ちます。

リロード時にクラスタリングを有効にするために、この構成を保存しないでください。

可能であれば、制御ユニットのクラスタを手動で無効にすることを推奨します。これにより、新しい制御ユニットを迅速かつできるだけクリーンな状態で選定できます。

例：

```
asa/unit1/master(config)# cluster group cluster1
asa/unit1/master(cfg-cluster)# no enable
Cluster disable is performing cleanup..done.
All data interfaces have been shutdown due to clustering being disabled. To recover either
enable clustering or remove cluster group configuration.

Cluster unit unit1 transitioned from MASTER to DISABLED
asa/unit1/ClusterDisabled(cfg-cluster)#
```

b) このユニットの ASA FirePOWER モジュールをアップグレードします。

ASDM によって管理される ASA FirePOWER モジュールの場合、事前にメモした個別の管理 IP アドレスに ASDM を接続します。この時点で、メインクラスタ IP アドレスは新しい制御ユニットに属しています。元の制御ユニットは、その個別の管理 IP アドレスに引き続きアクセスできます。

アップグレードが完了するまで待ちます。

c) このユニットをリロードします。

reload noconfirm

元の制御ユニットがクラスタに再接続すると、そのユニットはデータユニットになります。

ASDM を使用した ASA クラスタのアップグレード

ASA クラスタ内のすべての装置をアップグレードするには、次の手順を実行します。

始める前に

- 制御ユニットで次の手順を実行します。ASA FirePOWER モジュールもアップグレードしている場合は、各データユニットへの ASDM アクセスが必要です。
- マルチ コンテキスト モードでは、システム実行スペースで後続の手順を実行します。
- ローカル管理コンピュータに ASA と ASDM のイメージを配置します。

ステップ 1 メインクラスタ IP アドレスに接続して、「制御」ユニットで ASDM を起動します。

この IP アドレスは、常に制御ユニットに保持されます。

ステップ 2 メイン ASDM アプリケーションウィンドウで、**[Tools]** > **[Upgrade Software from Local Computer]** の順に選択します。

[Upgrade Software from Local Computer] ダイアログボックスが表示されます。

ステップ 3 [クラスタ内のすべてのデバイス（All devices in the cluster）] オプション ボタンをクリックします。

[ソフトウェアのアップグレード（Upgrade Software）] ダイアログボックスが表示されます。

ステップ 4 [アップロードするイメージ（Image to Upload）] ドロップダウン リストから、[ASDM] を選択します。

ステップ 5 [ローカル ファイル パス（Local File Path）] フィールドで [ローカル ファイルの参照（Browse Local Files）] をクリックして、コンピュータ上のファイルを見つけます。

ステップ 6 （任意）[フラッシュファイルシステムのパス（Flash File System Path）] フィールドにフラッシュファイルシステムへのパスを入力するか、[フラッシュの参照（Browse Flash）] をクリックしてフラッシュファイルシステム上のディレクトリまたはファイルを検索します。

デフォルトでは、このフィールドにはパス（**disk0:/***filename*）が入力されています。

ステップ 7 [イメージのアップロード（Upload Image）] をクリックします。アップグレード プロセスには数分かかる場合があります。

ステップ 8 このイメージを ASDM イメージとして設定するように求められます。[Yes] をクリックします。

ステップ 9 ASDM を終了して、コンフィギュレーションを保存したことを確認します。[OK] をクリックします。

アップグレード ツールを終了します。**注**：ASA ソフトウェアをアップグレードした後で、設定を保存し、ASDM をリロードします。

ステップ 10 これらの手順を繰り返し、[アップロードするイメージ（Image to Upload）] ドロップダウン リストから [ASA] を選択します。

ステップ 11 コンフィギュレーションの変更を保存するには、ツールバーの [Save] アイコンをクリックします。

これらの設定変更は、データユニットに自動的に保存されます。

ステップ 12 **[Configuration]** > **[Device Management]** > **[High Availability and Scalability]** > **[ASA Cluster]** > **[Cluster Members]** で、各ユニットの個別の管理 IP アドレスをメモして、後で ASDM をデータユニットに直接接続できるようにします。

ステップ 13 ASA FirePOWER モジュールをアップグレードする場合は、**[ツール（Tools）]**>**[コマンドラインインターフェイス（Command Line Interface）]** を選択し、**no rest-api enable** を入力して ASA REST API を無効にします。

REST API を無効にしない場合、ASA FirePOWER モジュールのアップグレードは失敗します。

ステップ 14 データユニットをアップグレードします。

ASA FirePOWER モジュールもアップグレードするかどうかによって、以下の手順を選択します。ASA FirePOWER モジュールもアップグレードする場合、ASA FirePOWER プロシージャは ASA のリロードの回数を最小化します。

（注） アップグレードプロセス中は、強制的にデータユニットを制御に変更するために **[Monitoring]** > **[ASA Cluster]** > **[Cluster Summary]** ページを使用して制御ユニットを変更しないでください。ネットワークの接続性とクラスタの安定性に関連した障害が発生する可能性があります。最初にすべてのデータユニットをリロードし、次にこの手順を実行すると、現在の制御ユニットから新しい制御ユニットへの移行をスムーズに行うことができます。

ASA FirePOWER モジュールをアップグレードしない場合：

a) 制御ユニットで、**[Tools]** > **[System Reload]** を選択します。
b) [Device] ドロップダウンリストからデータユニット名を選択します。
c) [Schedule Reload] をクリックします。
d) [Yes] をクリックしてリロードを続行します。
e) 各データユニットに対して手順を繰り返します。

接続損失を回避し、トラフィックを安定させるために、各装置が起動しクラスタに再接続するのを待ち（約 5 分）、次の装置にこれらの手順を繰り返します。ユニットがクラスタに再接続したことを確認するには、**[Monitoring]** > **[ASA Cluster]** > **[Cluster Summary]** ペインを表示します。

ASA FirePOWER モジュールのアップグレードもある場合：

a) 制御ユニットで、**[Configuration]** > **[Device Management]** > **[High Availability and Scalability]** > **[ASA Cluster]** > **[Cluster Members]** を選択します。
b) アップグレードするデータユニットを選択して [Delete] をクリックします。
c) [適用（Apply）] をクリックします。
d) ASDM を終了し、事前にメモした「個別」の管理 IP アドレスに接続して、ASDM をデータユニットに接続します。
e) ASA FirePOWER モジュールをアップグレードします。

アップグレードが完了するまで待ちます。

f) ASDM で、**[Tools]** > **[System Reload]** を選択します。
g) [実行コンフィギュレーションを保存しないでリロードする（Reload without saving the running configuration）] オプション ボタンをクリックします。

この装置のリロード時にクラスタリングを有効にするために、この構成を保存しないようにします。

h) [Schedule Reload] をクリックします。
i) [Yes] をクリックしてリロードを続行します。
j) 各データユニットに対して手順を繰り返します。

接続損失を回避し、トラフィックを安定させるために、各装置が起動しクラスタに再接続するのを待ち（約5分）、次の装置にこれらの手順を繰り返します。ユニットがクラスタに再接続したことを確認するには、**[Monitoring]** > **[ASA Cluster]** > **[Cluster Summary]** ペインを表示します。

ステップ 15 制御ユニットをアップグレードします。

a) 制御ユニットの ASDM で、**[Configuration]** > **[Device Management]** > **[High Availability and Scalability]** > **[ASA Cluster]** > **[Cluster Configuration]** ペインを選択します。

b) [ASAクラスタに参加（Participate in ASA cluster）] チェックボックスをオフにして、[適用（Apply）] をクリックします。

ASDM から出るように促されます。

c) 新しい制御ユニットが選択され、トラフィックが安定するまで最大 5 分間待機します。

元の制御ユニットがクラスタに再接続すると、そのユニットはデータユニットになります。

d) 事前にメモした「個別」の管理 IP アドレスに接続して、ASDM を元の制御ユニットに再接続します。

この時点で、メインクラスタ IP アドレスは新しい制御ユニットに属しています。元の制御ユニットは、その個別の管理 IP アドレスに引き続きアクセスできます。

e) ASA FirePOWER モジュールをアップグレードします。

アップグレードが完了するまで待ちます。

f) **[Tools]** > **[System Reload]** を選択します。

g) [実行コンフィギュレーションを保存しないでリロードする（Reload without saving the running configuration）] オプション ボタンをクリックします。

この装置のリロード時にクラスタリングを有効にするために、この構成を保存しないようにします。

h) [Schedule Reload] をクリックします。

i) [Yes] をクリックしてリロードを続行します。

ASDM から出るように促されます。メインクラスタ IP アドレスで ASDM を再起動すると、新しい制御ユニットに再接続されます。

FMC を使用した ASA FirePOWER モジュールのアップグレード

この手順を使用して、FMC によって管理される ASA FirePOWER module をアップグレードします。モジュールをいつアップグレードするかは、ASAをアップグレードするかどうか、およびASAの展開によって異なります。

- スタンドアロン ASA デバイス：ASA もアップグレードする場合は、ASA をアップグレードしてリロードした直後に、ASA FirePOWER module をアップグレードします。
- ASA クラスタとフェールオーバーペア：トラフィックフローとインスペクションの中断を避けるには、これらのデバイスを一度に 1 台ずつ完全にアップグレードします。ASA を

アップグレードする場合、各ユニットをリロードしてASAをアップグレードする直前に、ASA FirePOWER module をアップグレードします。

詳細については、アップグレードパス： ASA FirePOWER （25 ページ）と ASA アップグレード手順を参照してください。

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。展開したアプライアンスが正常で、きちんと通信していることを確認します。

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

ステップ 2 使用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、アップグレードするデバイスを選択します。

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。

（注） [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 3 [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。

トラフィックは、デバイスの設定および展開方法に応じて、アップグレードの間ドロップするか、検査なしでネットワークを通過します。 詳細については、対象バージョンの Cisco Firepower リリース ノート 内の「ソフトウェアのアップグレード」の章を参照してください。

ステップ 4 アップグレードの進捗状況 をモニタします。

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

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。

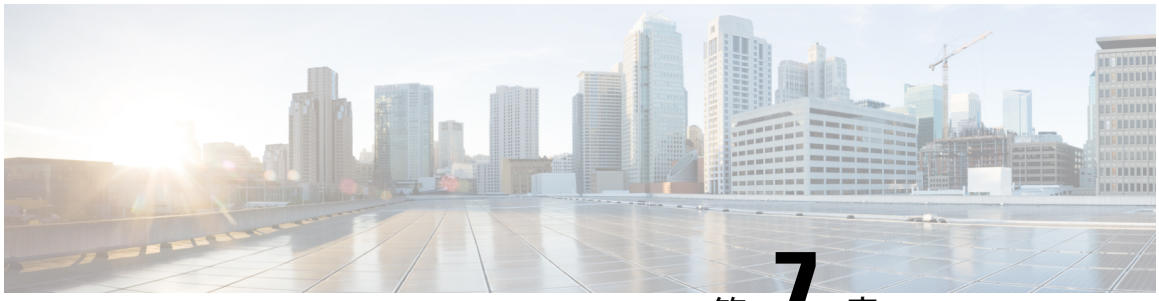
アップグレードが完了したら、**[Devices] > [Device Management]** を選択し、アップグレードしたデバイスのソフトウェアバージョンが正しいことを確認します。

ステップ 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 リリース ノートに記載されているアップグレード後の構成の変更をすべて完了します。

ステップ 8 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 7 章

パッチをアンインストールする

ほとんどのパッチをアンインストールすることができます。以前のメジャーリリースまたはメンテナンスリリースに戻す必要がある場合は、イメージを再作成する必要があります。

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 7.0 のパッチ

現在、すべてのバージョン 7.0 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。

アンインストールに対応したバージョン 6.6 のパッチ

現在、すべてのバージョン 6.6 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 6.5 のパッチ

この表は、バージョン 6.5 のパッチでサポートされているアンインストールのシナリオを示しています。アンインストールすると、アップグレード前のパッチレベルに戻ります。アンインストールによってサポートされているよりも前に戻る場合は、イメージを再作成してから、目的のパッチレベルにアップグレードすることをお勧めします。

表 *48 :* アンインストールに対応したバージョン *6.5.0* のパッチ

現在のバージョン	アンインストールすべき最も古いバージョン		
	FTD/FTDv	**ASA FirePOWER** **NGIPSv**	**FMC/FMCv**
6.5.0.2 以降	6.5.0	6.5.0	6.5.0.1
6.5.0.1	6.5.0	6.5.0	—

アンインストールに対応したバージョン 6.4 のパッチ

この表は、バージョン 6.4 のパッチでサポートされているアンインストールのシナリオを示しています。アンインストールすると、アップグレード前のパッチレベルに戻ります。アンインストールによってサポートされているよりも前に戻る場合は、イメージを再作成してから、目的のパッチレベルにアップグレードすることをお勧めします。

表 *49 :* アンインストールに対応したバージョン *6.4.0* のパッチ

現在のバージョン	アンインストールすべき最も古いバージョン		
	FTD/FTDv	**Firepower 7000/8000** **ASA FirePOWER** **NGIPSv**	**FMC/FMCv**
6.4.0.5 以降	6.4.0.4	6.4.0.4	6.4.0.4
6.4.0.4	—	—	—
6.4.0.3	6.4.0	—	—

現在のバージョン	アンインストールすべき最も古いバージョン		
	FTD/FTDv	**Firepower 7000/8000 ASA FirePOWER NGIPSv**	**FMC/FMCv**
6.4.0.2	6.4.0	—	—
6.4.0.1	6.4.0	6.4.0	6.4.0

アンインストールに対応したバージョン 6.3 のパッチ

この表は、バージョン 6.3 のパッチでサポートされているアンインストールのシナリオを示しています。アンインストールすると、アップグレード前のパッチレベルに戻ります。アンインストールによってサポートされているよりも前に戻る場合は、イメージを再作成してから、目的のパッチレベルにアップグレードすることをお勧めします。

表 *50*：アンインストールに対応したバージョン *6.3.0* のパッチ

現在のバージョン	アンインストールすべき最も古いバージョン
6.3.0.5	—
6.3.0.1 ～ 6.3.0.4	6.3.0

アンインストールに対応したバージョン 6.2.3 のパッチ

この表は、バージョン 6.2.3 のパッチでサポートされているアンインストールのシナリオを示しています。アンインストールすると、アップグレード前のパッチレベルに戻ります。アンインストールによってサポートされているよりも前に戻る場合は、イメージを再作成してから、目的のパッチレベルにアップグレードすることをお勧めします。

表 *51*：アンインストールに対応したバージョン *6.2.3* のパッチ

現在のバージョン	アンインストールすべき最も古いバージョン		
	FTD/FTDv	**Firepower 7000/8000 ASA FirePOWER NGIPSv**	**FMC/FMCv**
6.2.3.16 以降	6.2.3.15	6.2.3.15	6.2.3.15
6.2.3.15	—	—	—
6.2.3.12 ～ 6.2.3.14	6.2.3	6.2.3.11	6.2.3.11
6.2.3.11	6.2.3	—	—
6.2.3.8 ～ 6.2.3.10	6.2.3	6.2.3.7	6.2.3.7

現在のバージョン	アンインストールすべき最も古いバージョン		
	FTD/FTDv	**Firepower 7000/8000** **ASA FirePOWER** **NGIPSv**	**FMC/FMCv**
6.2.3.7	6.2.3	—	—
6.2.3.1 ～ 6.2.3.6	6.2.3	6.2.3	6.2.3

アンインストールに対応したバージョン 6.2.2 のパッチ

この表は、バージョン 6.2.2 のパッチでサポートされているアンインストールのシナリオを示しています。以前のパッチからアップグレードした場合でも、アンインストールすると直前のパッチに戻ります。アンインストールによってサポートされているよりも前に戻る場合は、イメージを再作成してから、目的のパッチレベルにアップグレードすることをお勧めします。

表 *52 :* アンインストールに対応したバージョン *6.2.2* のパッチ

現在のバージョン	アンインストールすべき最も古いバージョン
6.2.2.3 ～ 6.2.2.5	6.2.2.2
6.2.2.2	—
6.2.2.1	6.2.2

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 *53 : 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 *54 : 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。

表 *55 : ASA* フェールオーバーペア/クラスタ内の *ASA with FirePOWER Services* のアンインストール順序

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

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

FMC を使用した デバイス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 （136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 Firepower CLI にアクセスします。`admin` として、または設定アクセス権を持つ別の 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、Firepower CLI 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`
Firepower 4100/9300	`connect module` *slot_number* `console`、次に `connect ftd`（最初のログインのみ）
ASA FirePOWER	`session sfr`

ステップ 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。

- FTD：`tail /ngfw/var/log/sf/update.status`
- ASA FirePOWER および NGIPSv：`tail /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 （140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。