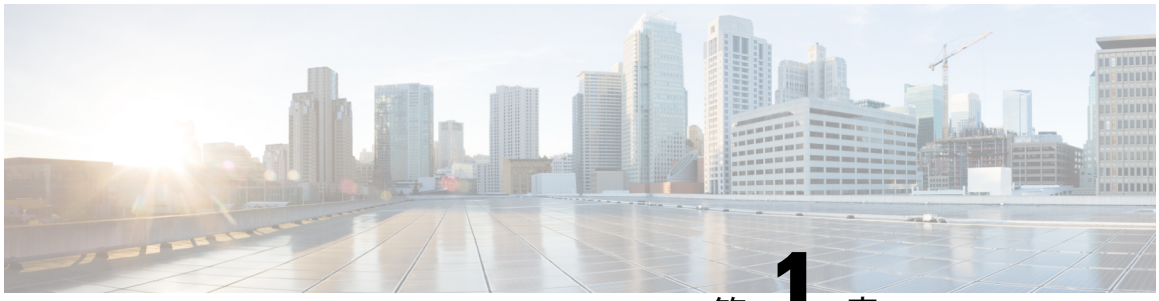
Cisco Firepower 4100/9300 アップグレードガイド、FXOS 1.1.1 ～ 2.10.1 を使用した FTD 6.0.1 ～ 7.0.x または ASA 9.4(1) ～ 9.16(x)

最終更新：2025 年 4 月 28 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/

© 2018–2025 Cisco Systems, Inc. All rights reserved.

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、次のものを使用して Firepower 4100/9300 のシャーシの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)（**バージョン 6.0.1 ～ 7.0.x**）によって管理される Firepower Threat Defense（FTD）の論理デバイス
- 適応型セキュリティアプライアンス（ASA）の論理デバイス（**バージョン 9.4(1) ～ 9.16(x)**）
- Firepower Extensible Operating System（FXOS）（**バージョン 1.1.1 ～ 2.10.1**）

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* のアップグレードガイド

現在の FMC 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 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 *2*：*FTD* を搭載した *FMC* のアップグレードガイド

現在の FMC のバージョン	ガイド
クラウド提供型 Firewall Management Center	クラウド提供型 Firewall Management Center 用 Cisco Secure Firewall Threat Defense アップグレードガイド
7.2 以降	お使いのバージョンの『Cisco Secure Firewall Threat Defense Upgrade Guide for 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』

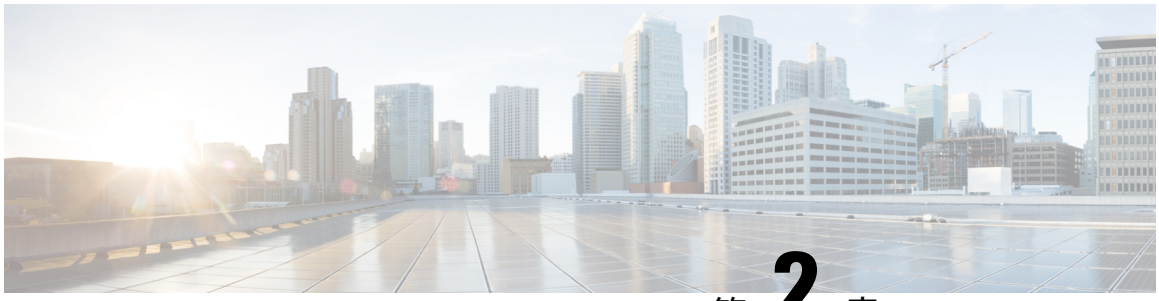
表 *3*：*FTD* を搭載した *FDM* のアップグレードガイド

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	お使いのバージョンの『Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager』：「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 を使用した FDM デバイスの管理

表 *4*：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
ASA 9.17（1）+	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

Version	コンポーネント	ガイド
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



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、「アップグレード」の章を参照してください。

表 *5:* アップグレードの計画フェーズ

計画フェーズ	次を含む
計画と実現可能性	展開を評価します。 アップグレードパスを計画します。 すべてのアップグレードガイドラインを読み、設定の変更を計画します。 アプライアンスへのアクセスを確認します。 帯域幅を確認します。 メンテナンス時間帯をスケジュールします。
バックアップ	ソフトウェアをバックアップします。 Firepower 4100/9300 の FXOS をバックアップします。
アップグレードパッケージ	アップグレードパッケージをシスコからダウンロードします。 システムにアップグレードパッケージをアップロードします。
関連するアップグレード	仮想展開内で仮想ホスティングをアップグレードします。 Firepower 4100/9300 の FXOS をアップグレードします。
最終チェック	設定を確認します。 NTP 同期を確認します。 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 *6:*

コンポーネント	情報
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。
FMC を搭載した Firepower Threat Defense 論理デバイス	FMC で、**[デバイス（Devices）]**>**[デバイス管理（Device Management）]** を選択します。
FDM を搭載した Firepower Threat Defense 論理デバイス	FDM で、[Device] をクリックして [Device Summary] に移動します。
ASA 論理デバイス	ASDM：**[Home]** > **[Device Dashboard]** > **[Device Information]** の順に選択します。 ASA CLI：**show version** コマンドを使用します。
Firepower Management Center	FMC で、**[ヘルプ（Help）]** > **[概要（About）]** を選択します。

アップグレードパス

アップグレードパスは、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 6.0.1 ～ 7.0.x または ASA 9.4(1) ～ 9.16(x) と FXOS 1.1.1 ～ 2.10.1 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 （6 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？
- 展開で対象の ASA 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？

これらすべての質問に対する回答については、Cisco Firepower 4100/9300 FXOS の互換性 を参照してください。

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？
- ASA ソフトウェアを直接アップグレードできるのか？
- FXOS 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
- 、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

アップグレードパス：FXOS のみ

この表は、論理デバイスが設定されていない Firepower 4100/9300 シャーシでの FXOS のアップグレードパスを示しています。

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。 通常、バージョンシーケンスにおける最新の FXOS ビルドが推奨されます。

表 7：アップグレードパス：*Firepower 4100/9300* の *FXOS*

現在の FXOS のバージョン	対象の FXOS のバージョン
2.2.2 以降	他の理由（論理デバイスの互換性、リリース固有の問題）で許可されていない場合を除き、以降の任意のバージョン。
2.2.1	→ 2.2.2 ～ 2.8.1
2.1(1)	→ 2.2.1 ～ 2.8.1
2.0.1	→ 2.1.1 ～ 2.8.1
1.1.4	→ 2.0.1
1.1.3	→ 1.1.4
1.1.2	→ 1.1.3
1.1.1	→ 1.1.2

アップグレードパス：ASA 論理デバイス

- FXOS：FXOS 2.2.2 以降では、上位バージョンに直接アップグレードできます。（FXOS 2.0.1 ～ 2.2.1 は 2.8.1 までアップグレードできます。2.0.1 より前のバージョンについては、各中間バージョンにアップグレードする必要があります。）現在の論理デバイスバージョンをサポートしていないバージョンに FXOS をアップグレードすることはできないことに注意してください。次の手順でアップグレードを行う必要があります。現在の論理デバイスをサポートする最新のバージョンに FXOS をアップグレードします。次に、論理デバイスをその FXOS バージョンでサポートされている最新のバージョンにアップグレードします。たとえば、FXOS 2.2/ASA 9.8 から FXOS 2.13/ASA 9.19 にアップグレードする場合は、次のアップグレードを実行する必要があります。

  1. FXOS 2.2 → FXOS 2.11（9.8 をサポートする最新バージョン）
  2. ASA 9.8 → ASA 9.17（2.11 でサポートされている最新バージョン）
  3. FXOS 2.11 → FXOS 2.13
  4. ASA 9.17 → ASA 9.19

- FTD：上記の FXOS 要件に加えて、FTD に対して中間アップグレードが必要になる場合があります。正確なアップグレードパスについては、ご使用のバージョンの FMC アップグレードガイドを参照してください。

- Cisco ASA：Cisco ASA では、上記の FXOS 要件に注意して、現在のバージョンから任意の上位バージョンに直接アップグレードできます。

表 *8 : Firepower 4100/9300* と *ASA* および *FTD* の互換性

FXOS のバージョン	モデル	ASA のバージョン	FTD バージョン
2.14(1)	Firepower 4112	9.16 9.14	**7.4**（推奨） 7.3 7.2 7.1 7.0 6.6
	Firepower 4145 Firepower 4125 Firepower 4115	9.16 9.14	**7.4**（推奨） 7.3 7.2 7.1 7.0 6.6
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40		
2.13	Firepower 4112	9.16 9.14	**7.3**（推奨） 7.2 7.1 7.0 6.6
	Firepower 4145 Firepower 4125 Firepower 4115	9.16 9.14	**7.3**（推奨） 7.2 7.1 7.0 6.6
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40		

FXOS のバージョン	モデル	**ASA** のバージョン	**FTD** バージョン
2.12	Firepower 4112	9.16 9.14	**7.2**（推奨） 7.1 7.0 6.6
	Firepower 4145 Firepower 4125 Firepower 4115	9.16 9.14 9.12	**7.2**（推奨） 7.1 7.0 6.6 6.4
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40		
	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	9.16 9.14 9.12	**7.2**（推奨） 7.1 7.0 6.6 6.4
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		

FXOS のバージョン	モデル	**ASA** のバージョン	**FTD** バージョン
2.11	Firepower 4112	9.16 9.14	**7.1**（推奨） 7.0 6.6
	Firepower 4145 Firepower 4125 Firepower 4115	9.16 9.14 9.12	**7.1**（推奨） 7.0 6.6 6.4
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40		
	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	9.16 9.14 9.12 9.8	**7.1**（推奨） 7.0 6.6 6.4
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		

FXOS のバージョン	モデル	**ASA** のバージョン	**FTD** バージョン
2.10 （注） 7.0.2+ および 9.16(3.11)+ との互換性を確保するには、FXOS 2.10(1.179)+ が必要です。	Firepower 4112	**9.16**（推奨） 9.14	**7.0**（推奨） 6.6
	Firepower 4145 Firepower 4125 Firepower 4115	**9.16**（推奨） 9.14 9.12	**7.0**（推奨） 6.6 6.4
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40		
	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	**9.16**（推奨） 9.14 9.12 9.8	**7.0**（推奨） 6.6 6.4
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		
2.9	Firepower 4112	9.14	6.6
	Firepower 4145 Firepower 4125 Firepower 4115	9.14 9.12	6.6 6.4
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40		
	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	9.14 9.12 9.8	6.6 6.4
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		

FXOS のバージョン	モデル	**ASA** のバージョン	**FTD** バージョン
2.8	Firepower 4112	**9.14**	**6.6** （注） 6.6.1+ では FXOS 2.8(1.125)+ が必要です。
	Firepower 4145 Firepower 4125 Firepower 4115	**9.14**（推奨） 9.12 （注） Firepower 9300 SM-56 には ASA 9.12(2)+ が必要	**6.6**（推奨） （注） 6.6.1+ では FXOS 2.8(1.125)+ が必要です。 6.4
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40		
	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	**9.14**（推奨） 9.12 9.8	**6.6**（推奨） （注） 6.6.1+ では FXOS 2.8(1.125)+ が必要です。 6.4 6.2.3
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		
2.6(1.157) （注） ASA 9.12+ および FTD 6.4+ では、同じ Firepower 9300 シャーシ内の別のモジュールで実行できるようになりました。	Firepower 4145 Firepower 4125 Firepower 4115	**9.12** （注） Firepower 9300 SM-56 には ASA 9.12.2+ が必要	**6.4**
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40		
	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	**9.12**（推奨） 9.8	**6.4**（推奨） 6.2.3
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		

FXOS のバージョン	モデル	**ASA** のバージョン	**FTD** バージョン
2.6(1.131)	Firepower 9300 SM-48 Firepower 9300 SM-40	**9.12**	サポート対象外
	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	**9.12**（推奨） 9.8	
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		
2.3(1.73)	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	9.8 （注） FXOS 2.3(1.130)+ を実行している場合、フローオフロードには 9.8(2.12)+ が必要です。	**6.2.3**（推奨） （注） 6.2.3.16+ には FXOS 2.3.1.157+ が必要
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		
2.3(1.66) 2.3(1.58)	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	9.8 （注） FXOS 2.3(1.130)+ を実行している場合、フローオフロードには 9.8(2.12)+ が必要です。	
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		
2.2	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	**9.8**	FTD バージョンはサポートが終了しています
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		

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：FTD 論理デバイスと FMC を備えた

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 を搭載した Firepower 9300 シャーシをアップグレードする場合は、アップグレードパス：Firepower 9300 の FTD および ASA 論理デバイス （22 ページ）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。

表 *9:* 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 FDM および CDO 管理の最初のサポート	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

現在のバージョン	対象のバージョン
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
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

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 2.2.1	→ 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 *10 : 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。
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。

展開	アップグレード順序
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 *11*：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。

シナリオ	詳細
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：FTD 論理デバイスと FDM

この表は、Firepower Device Manager 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 を搭載した Firepower 9300 シャーシをアップグレードする場合は、アップグレードパス：Firepower 9300 の FTD および ASA 論理デバイス （22 ページ）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。

表 *12 :* 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

現在のバージョン	対象のバージョン
FTD 6.5.0 を搭載した FXOS 2.7.1 FDM および CDO 管理の最初のサポート	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

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 Device Manager の展開では、高可用性のペアのメンバーを個別にアップグレードします。この表の事例では、デバイス A が元のアクティブデバイスであり、デバイス B が元のスタンバイです。

表 *13 : 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	**1.** FXOS をアップグレードします。 **2.** FTD 論理デバイスをアップグレードします。
ハイ アベイラビリティ	FTD をアップグレードする前に、両方のシャーシで FXOS をアップグレードします。中断を最小限に抑えるため、次の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 FTD 論理デバイス（B）を搭載したシャーシの FXOS をアップグレードします。 **2.** ロールを切り替えます。 **3.** 新しいスタンバイの論理デバイス（A）を搭載したシャーシの FXOS をアップグレードします。 **4.** 新しいスタンバイの FTD 論理デバイス（A）をアップグレードします。 **5.** ロールを再度切り替えます。 **6.** 元のスタンバイの FTD 論理デバイス（B）をアップグレードします。

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：Firepower 9300 の FTD および ASA 論理デバイス

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

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） このタイプの展開では、FXOS をアップグレードしても、どちらのタイプの論理デバイスとの互換性も失われないことを確認する必要があります。複数のバージョンをスキップする必要がある場合、通常は FTD がリミッタになります。FXOS と ASA は通常、FTD よりも 1 ホップでさらにアップグレードできます。

表 *14 :* アップグレード パス：*FTD* および *ASA* 論理デバイス搭載した *Firepower 9300*

現在のバージョン	対象のバージョン
次を搭載した FXOS 2.9.1： • FTD 6.7.0/6.7.x • ASA 9.15(x)	→ ASA 9.16(x) および FTD 7.0.0/7.0.x を搭載した FXOS 2.10.1
次を搭載した FXOS 2.8.1： • FTD 6.6.0/6.6.x • ASA 9.14(x)	次のいずれかです。 → ASA 9.16(x) および FTD 7.0.07.0.x を搭載した FXOS 2.10.1 → ASA 9.15(x) および FTD 6.7.0/6.7.x を搭載した FXOS 2.9.1
次を搭載した FXOS 2.7.1： • FTD 6.5.0 • ASA 9.13(x)	次のいずれかです。 → ASA 9.16(x) および FTD 7.0.x を搭載した FXOS 2.10.1 → ASA 9.15(x) および FTD 6.7.0/6.7.x を搭載した FXOS 2.9.1 → ASA 9.14(x) および FTD 6.6.0/6.6.x を搭載した FXOS 2.8.1

現在のバージョン	対象のバージョン
次を搭載した FXOS 2.6.1： • FTD 6.4.0 • ASA 9.12(x)	次のいずれかです。 → ASA 9.16(x) および FTD 7.0.x を搭載した FXOS 2.10.1 → ASA 9.15(x) および FTD 6.7.0/6.7.x を搭載した FXOS 2.9.1 → ASA 9.14(x) および FTD 6.6.0/6.6.x を搭載した FXOS 2.8.1 → ASA 9.13(x) および FTD 6.5.0 を搭載した FXOS 2.7.1

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 *15 : 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	次のいずれかです。 → 7.1.0 ～ 7.4.x → 7.0.x 以降のメンテナンスリリース （注） データストアの非互換性のため、 をバージョン 7.0.4 以降からバージョン 7.1.0 にアップグレードすることができません。バージョン 7.2 以降に直接アップグレードすることをお勧めします。
6.7.0 6.7.x	次のいずれかです。 → 7.0.0 ～ 7.2.x → 6.7.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
6.6.0 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。 → 6.7.0 ～ 7.2.x → 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	6.6.0 ～ 7.1.x
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。 → 6.6.0 ～ 7.0.x → 6.5.0
6.3.0	次のいずれかです。 → 6.6.0 ～ 6.7.x → 6.5.0 →6.4.0
6.2.3	次のいずれかです。 → 6.6.x → 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

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 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。

応答しないアップグレード

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

応答しない FMC

進行中のアップグレードは再開しないでください。アップグレードに失敗する、アプライアンスが応答しないなど、アップグレードで問題が発生した場合にはCisco TACにお問い合わせください。

応答しない FTD のアップグレード

メジャーアップグレードやメンテナンスアップグレードでは、失敗したアップグレードまたは進行中のアップグレードを手動でキャンセルし、失敗したアップグレードを再試行できます。

- FMC：[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。
- FDM：[システムアップグレード（System Upgrade）] パネルを使用します。

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。

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。

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 （25 ページ） を参照してください。

表 *16* : 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 *17*: 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。
FTD	**show disk** CLI コマンドを使用します。

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

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 *18*：

プラットフォーム	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 4100/9300	任意（Any）	Cisco_FTD_SSP

ASA パッケージ

Firepower 4100/9300 用の 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 で入手できます。

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

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） FXOS 内の ASA バンドルをアップグレードすると、ASA 上の古い ASDM バンドル イメージがバンドル内の ASDM イメージに置き換えられます。これは、両者の名前が同じ（**asdm.bin**）であるためです。ただし、アップロードした別の ASDM イメージ（たとえば **asdm-782.bin**）を手動で選択すると、バンドルアップグレード後も引き続き同じイメージが使用されます。互換性のある ASDM バージョンを実行していることを確認するには、バンドルをアップグレードする前に ASDM をアップグレードするか、または ASA バンドルをアップグレードする直前に、バンドルされた ASDM イメージ（**asdm.bin**）を使用するように ASA を再設定する必要があります。

表 *19 : Firepower 4100/9300* 用の *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	cisco-asa.*version*.**SPA.csp**
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**

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 *20 : 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**

パッケージ タイプ	パッケージ
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**

FMC を使用した 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。

手順

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。

手順

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） （78 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、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。

手順

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。

FDM を使用した Firepower Threat Defense アップグレードパッケージのアップロード

Firepower Threat Defense ソフトウェア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 パッケージがデバイス上にある必要があります。

FTD デバイスへのアップロード（バージョン 6.2.0 以降、FDM 使用）

手順

ステップ 1 [デバイス（Device）] をクリックし、[更新サマリー（Updates summary）] の [設定の表示（View Configuration）] をクリックします。

[システムアップグレード（System Upgrade）] セクションには、現在実行中のソフトウェア バージョン、およびすでにアップロードされた更新が表示されます。

ステップ 2 アップグレード ファイルをアップロードします。

- アップグレードファイルをまだアップロードしていない場合、[検索（Browse）] をクリックしてファイルを選択します。アップロードが完了したら、[Run Upgrade Immediately on Upload] オプションを選択してインストールを開始できます。
- すでにアップロードされたファイルがあるか、別のファイルをアップロードする場合、[別のファイルをアップロード（Upload Another File）] をクリックします。1 つのファイルのみアップロードできます。新規ファイルをアップロードすると、古いファイルが置き換えられます。
- ファイルを削除するには、[削除（Delete）] アイコン（）をクリックします。

FTD デバイスへのアップロード（バージョン 6.0.1 および 6.1.0、FDM 使用）

手順

ステップ 1 アップグレード イメージを入手し、インストールを準備します。

a) Cisco.com にログインし、アップグレード イメージをダウンロードします。

- ファイル タイプが .sh である適切なアップグレード ファイルを入手したことを確認します。システム ソフトウェア パッケージやブート イメージをダウンロードしないでください。
- アップグレードに必要なベースライン イメージを実行していることを確認します。

b) 管理 IP アドレスからアクセスできる HTTP サーバーにソフトウェアを配置します。

代わりに、SCP または TFTP を使用してファイルをダウンロードできます。これらのいずれかのオプションを選択したら、そのファイル転送プロトコルをサポートするサーバーにファイルを配置します。

ステップ 2 SSH クライアントを使用して、**admin** ユーザー アカウントとパスワードで管理 IP アドレスにログオンします。

代わりに、コンソール ポートに接続することもできます。

ステップ 3 **expert** コマンドを入力してエキスパートモードに移行します。

```
> expert
admin@firepower:~$
```

ステップ 4 作業ディレクトリを /var/sf/updates/ に変更します（**cd** コマンドを使用）。

```
admin@firepower:~$ cd /var/sf/updates/
admin@firepower:/var/sf/updates$
```

ステップ 5 HTTP サーバからアップグレード ファイルをダウンロードします。

sudo wget *url*

たとえば、次のコマンドでは、Cisco_FTD_Upgrade-6.2.0-181.sh という架空のアップグレード ファイルを files.example.com HTTP サーバーの ftd フォルダからダウンロードします。**sudo** コマンドは root ユーザーの下で機能するため、警告が表示されます。コマンドを実行する前に **admin** パスワードを再入力する必要があります。ダウンロードが完了するまで待ちます。

```
admin@firepower:/var/sf/updates$ sudo wget
http://files.example.com/ftd/Cisco_FTD_Upgrade-6.2.0-181.sh
```

```
We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

Password: (enter admin password)
Connecting to files.example.com
|************************************************
************************************************
************************************************
************************************************
*********************************|

...(remaining output omitted)
```

HTTP サーバーを使用しない場合は、代わりに **tftp** または **scp** コマンドを使用します。

FMC を使用した 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）（78 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）（78 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）（40 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）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。

手順

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。

手順

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。

FDM を使用した 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、Firepower Threat Defense ソフトウェアをアップグレードするための準備状況を評価できます。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ようお勧めします。

準備状況チェックを行っているアプライアンスを手動で再起動またはシャットダウンしないでください。

準備状況チェックは、Firepower Device Manager バージョン 7.0.0 以降でサポートされています。

準備状況チェックの実行（FDM を使用したバージョン 7.0.0 以降）

アップグレードパッケージがインストールされる前に、準備状況チェックが実行されて、システムに有効なアップグレードであるか確認されます。また、他にもアップグレードの成功を妨げる可能性のある項目がないかチェックされます。準備状況チェックに失敗した場合は、インストールを再試行する前に問題を修正する必要があります。チェックに失敗した場合、次回インストールを試みると、チェック失敗についてのプロンプトが表示され、強制的にインストールを実行するオプションが与えられます。

次の手順の説明に従って、アップグレードを開始する前に手動で準備状況チェックを実行することもできます。

始める前に

チェックするアップグレードパッケージをアップロードします。

手順

ステップ 1 [デバイス（Device）] をクリックし、[更新サマリー（Updates summary）] の [設定の表示（View Configuration）] をクリックします。

[システムアップグレード（System Upgrade）] セクションには、現在実行中のソフトウェアバージョン、およびすでにアップロードされた更新が表示されます。

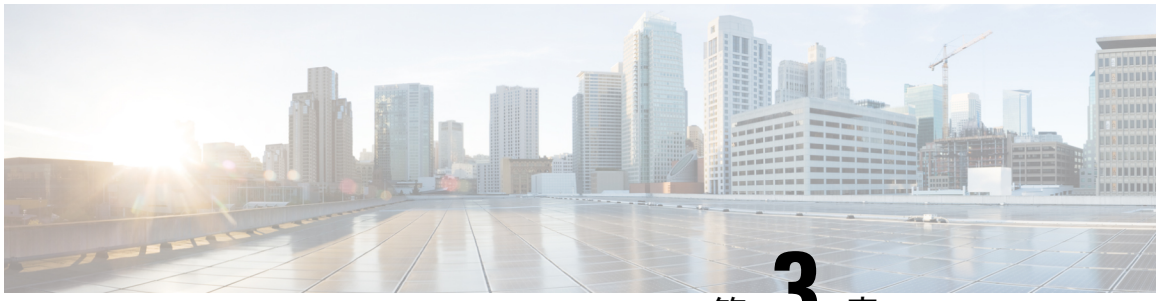
ステップ 2 [Readiness Check] セクションを確認します。

- アップグレードチェックがまだ実行されていない場合は、[Run Upgrade Readiness Check] リンクをクリックします。チェックの進行状況がこの領域に表示されます。プロセスの完了には、20 秒程度かかります。
- アップグレードチェックがすでに実行されている場合、このセクションにはチェックが成功か失敗かが示されます。チェックに失敗した場合は、[See Details] をクリックして、準備状況チェックの詳細を表示します。問題を修正した後、チェックを再度実行します。

ステップ 3 準備状況チェックに失敗した場合は、アップグレードパッケージをインストールする前に問題を解決する必要があります。詳細情報には、指摘された問題の修正方法に関するヘルプが含まれています。失敗したスクリプトについては、[Show Recovery Message] リンクをクリックすると情報が表示されます。

一般的な問題のいくつかを以下に示します。

- FXOS バージョンに互換性がない：FXOS アップグレードを個別にインストールする Firepower 4100/9300 などのシステムでは、現行の FTD ソフトウェアバージョンとは異なる FXOS の最小バージョンが必要になる場合があります。この場合、FTD ソフトウェアをアップグレードする前に、まず FXOS をアップグレードする必要があります。
- デバイスモデルがサポートされていない：アップグレードパッケージは、サポートされていないデバイスにはインストールできません。誤ったパッケージをアップロードしたか、デバイスが旧モデルのため、新しい FTD ソフトウェアバージョンではサポートされていない可能性があります。デバイスの互換性を確認し、サポートされているパッケージがあればアップロードしてください。
- ディスク容量が不十分：十分な空き容量がない場合は、システムバックアップなどの不要なファイルを削除してください。作成したファイルのみを削除します。



第 3 章

Firepower 4100/9300 の FXOS アップグレード

論理デバイスが構成されていない Firepower 4100/9300 シャーシの FXOS をアップグレードするには、次の手順を使用します。

- Firepower Chassis Manager を使用した Firepower 4100/9300 シャーシの FXOS のアップグレード （43 ページ）
- CLI を使用した Firepower 4100/9300 シャーシの FXOS のアップグレード （45 ページ）

Firepower Chassis Manager を使用した Firepower 4100/9300 シャーシの FXOS のアップグレード

この項では、Firepower Chassis Manager を使用して、論理デバイスでまだ構成されていない 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について説明します。

（注） Firepower Threat Defense または ASA の論理デバイスで構成された Firepower 4100/9300 シャーシの FXOS プラットフォームバンドル、アプリケーション ソフトウェア、またはその両方をアップグレードする必要がある場合は、「FTD 論理デバイスを搭載した Firepower 4100/9300 のアップグレード （49 ページ）」または「ASA 論理デバイスを搭載した Firepower 4100/9300 のアップグレード （85 ページ）」を参照してください。

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。

- アップグレードを計画します。
- 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 の構成をバックアップします。

（注） アップグレード プロセスには通常 20 ～ 30 分かかります。

手順

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 Firepower eXtensible オペレーティングシステム 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。

Firepower eXtensible オペレーティング 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 5 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。

CLI を使用した Firepower 4100/9300 シャーシの FXOS のアップグレード

この項では、FXOS CLI を使用して、論理デバイスでまだ構成されていない 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について説明します。

（注） Firepower Threat Defense または ASA の論理デバイスで構成された Firepower 4100/9300 シャーシの FXOS プラットフォームバンドル、アプリケーション ソフトウェア、またはその両方をアップグレードする必要がある場合は、「FTD 論理デバイスを搭載した Firepower 4100/9300 のアップグレード （49 ページ）」または「ASA 論理デバイスを搭載した Firepower 4100/9300 のアップグレード （85 ページ）」を参照してください。

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。

- アップグレードを計画します。
- 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 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。

（注） アップグレード プロセスには通常 20 ～ 30 分かかります。

手順

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。

Firepower eXtensible オペレーティング 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。

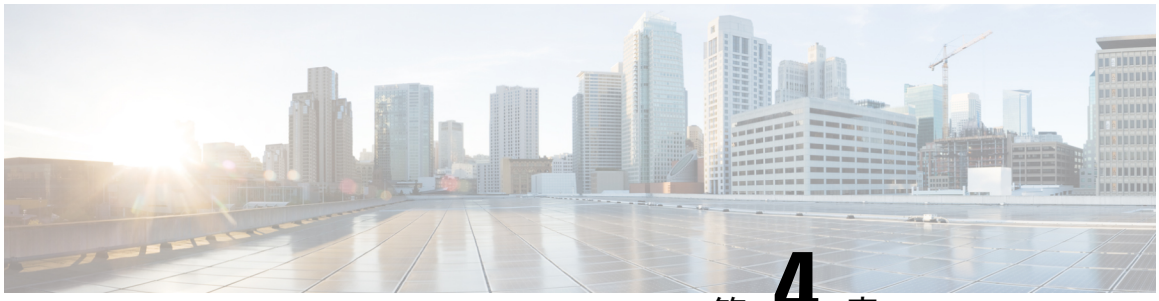
（注）
FPRM コンポーネントをアップグレードすると、システムが再起動し、その他のコンポーネントのアップグレードを続行します。

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。



第 4 章

FTD 論理デバイスを搭載した Firepower 4100/9300 のアップグレード

Firepower Threat Defense 論理デバイスを使用して構成された Firepower 4100/9300 シャーシをアップグレードするには、この項の手順を使用します。

主要な FirePOWER バージョンには、付随する FXOS バージョンがあります。論理デバイスをアップグレードする前に、FXOS の付随するバージョンを実行している必要があります。Firepower のシャーシ間クラスタリングまたは高可用性ペアの構成がある場合でも、各シャーシの FXOS プラットフォームバンドルを個別にアップグレードします。

（注） このガイドには、Firepower Device Manager/Cloud Defense Orchestrator 展開での Firepower Threat Defense 論理デバイスのアップグレード手順は含まれていません。このガイドを使用して FXOS をアップグレードしてから、次のいずれかを参照してください。

- 『『Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager』』：アップグレード先のバージョンではなく、現在実行している FTD バージョンのガイドの「System Management」の章を参照してください。
- 『Cisco Defense Orchestrator を使用した FTD の管理』：「Device Upgrade」の項を参照してください。

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Cisco Firepower 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。

手順

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。

手順

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。次の事例では、デバイス A が元のアクティブデバイスであり、デバイス B が元のスタンバイです。

Firepower Management Center

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（B）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（A）の FXOS をアップグレードします。
4. FTD 論理デバイス（A+B）をアップグレードします。

Firepower Device Manager

Firepower Device Manager の展開では、論理デバイスを個別にアップグレードします。

1. スタンバイの FTD 論理デバイス（B）を搭載したシャーシの FXOS をアップグレードします。

2. ロールを切り替えます。
3. 新しいスタンバイの論理デバイス（A）を搭載したシャーシの FXOS をアップグレードします。

   両方のシャーシにアップグレードされた FXOS が搭載されました。
4. 新しいスタンバイの FTD 論理デバイス（A）をアップグレードします。
5. ロールを再度切り替えます。
6. 元のスタンバイの FTD 論理デバイス（B）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。

手順

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。

手順

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。

手順

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。

手順

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。

Firepower Management Center を使用した Firepower Threat Defense 論理デバイスのアップグレード

Firepower Management Center 展開では、最初に Firepower Management Center をアップグレードしてから、新しくアップグレードされた FMC を使用して管理対象デバイスをアップグレードします。計画を参照してください。FMC 自体のアップグレード、および Firepower 4100/9300

以外の管理対象デバイスのアップグレードについては、Cisco Firepower Management Center Upgrade Guide, Version 6.0–7.0を参照してください。

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、FTDCLI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 *21 :*

✓	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 （7 ページ）を参照してください。

✓	アクション/チェック
	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。
	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 *22*：

✓	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） （33 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 （34 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 *23：*

✓	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。
	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 *24：*

✓	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。

✓	アクション/チェック
	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 25：

✓	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。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。 FMC を使用した Firepower ソフトウェアの準備状況チェック （38 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。

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。

手順

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） （78 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。

手順

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。

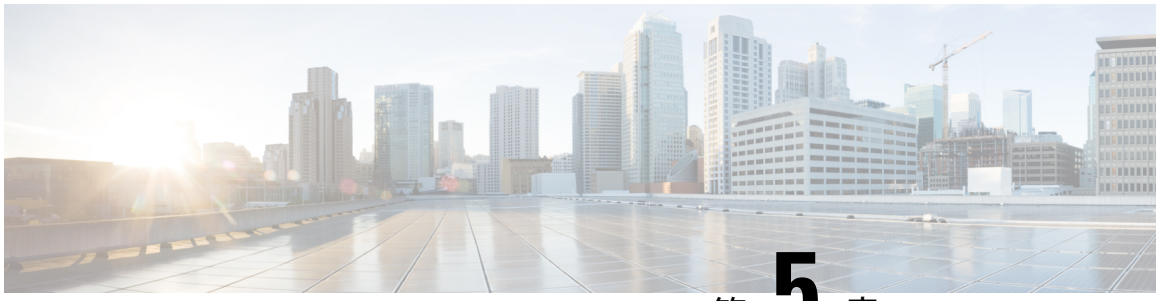
アップグレードが完了したら、**[Devices]** > **[Device Management]** を選択し、アップグレードしたデバイスのソフトウェアバージョンが正しいことを確認します。

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

ASA 論理デバイスを搭載した Firepower 4100/9300 のアップグレード

このセクションの手順を使用して、Firepower 9300/4100 シリーズ セキュリティ アプライアンスの FXOS プラットフォーム バンドルと、アプライアンスにインストールされている論理デバイス上の ASA ソフトウェアをアップグレードします。

チェックリスト：ASA を搭載した Firepower 4100/9300 のアップグレード

アップグレードを計画する際は、次のチェックリストを使用してください。

1. 現在の FXOS のバージョン（現在のバージョンおよびモジュールの情報 （6 ページ））：_____

   現在の ASA のバージョン：_____

2. ASA/Firepower 4100 および 9300 の互換性をチェックします（Cisco Firepower 4100/9300 FXOS の互換性）。

   FXOS のターゲット バージョン：_____

   ターゲット ASA のバージョン：_____

3. FXOS のアップグレード パスをチェックします（アップグレードパス：FXOS のみ （8 ページ））。必要な中間バージョンはありますか。はい _____ いいえ _____

「はい」の場合、FXOS の中間バージョン：

互換性を維持するために、必ず、FXOS のアップグレードに合わせた ASA のアップグレードを計画してください。

アップグレード時に互換性を維持するために必要な ASA の中間バージョン：

4. ターゲットバージョンおよび中間バージョンの FXOS をダウンロードします（FXOS パッケージ （31 ページ））。
5. ターゲットバージョンおよび中間バージョンの ASA をダウンロードします（ASA パッケージ （30 ページ））。

（注） ASDM は ASA for FXOS パッケージに含まれています。

6. Radware DefensePro デコレータ アプリケーションを使用しますか。はい _____ いいえ _____

   「はい」の場合：

   1. 現在の DefensePro のバージョン：_____
   2. ASA/FXOS/DefensePro の互換性をチェックします（Cisco Firepower 4100/9300 FXOS の互換性）。

      DefensePro のターゲット バージョン：_____
   3. ターゲット バージョンの DefensePro をダウンロードします。

7. 各オペレーティング システムのアップグレード ガイドラインをチェックします。
   - FXOS ガイドライン：各中間およびターゲット バージョンの『FXOS リリース ノート』を参照してください。
   - ASA ガイドライン：『Cisco Secure Firewall ASA アップグレードガイド』の「Planning Your Upgrade」を参照してください。
8. 設定をバックアップします。バックアップの方法については、各オペレーティングシステムの設定ガイドを参照してください。

FXOS および ASA スタンドアロン デバイスまたはシャーシ内クラスタのアップグレード

FXOS CLI または Firepower Chassis Manager を使用して、Firepower 9300 上のFXOS およびスタンドアロン ASA デバイスまたは ASA シャーシ内クラスタをアップグレードします。

Firepower Chassis Manager を使用した FXOS および ASA スタンドアロンデバイスまたはシャーシ内クラスタのアップグレード

アップグレード プロセスは最大 45 分かかることがあります。アップグレード中、トラフィックはデバイスを通過しません。適切なアップグレード活動の計画を行ってください。

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 および ASA ソフトウェアパッケージをダウンロードします（アップグレードパッケージのダウンロード （28 ページ））。
- FXOS と ASA の構成をバックアップします。

手順

ステップ 1 Firepower Chassis Manager で、**[System]** > **[Updates]** を選択します。
[Available Updates] の画面に、シャーシで使用可能なパッケージのリストが表示されます。

ステップ 2 新しい FXOS プラットフォーム バンドルのイメージと ASA ソフトウェア イメージのアップロード：：

a) [Upload Image] をクリックします。
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シャーシにアップロードされます。

ステップ 3 新しい FXOS 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 [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。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。ASA バージョンが互換性テーブルにアップグレード可能としてリストされている限り、これらの警告を無視できます。

ステップ 4 [はい（Yes）] をクリックして、インストールを続行することを確認します。

FXOS 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（アップグレード進行のモニター （125 ページ） を参照してください）。

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、続行する前に、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（インストールの確認 （126 ページ） を参照してください）。

ステップ 7 [論理デバイス（Logical Devices）] を選択します。
[Logical Devices] ページに、シャーシに設定された論理デバイスのリストが表示されます。

ステップ 8 アップグレードする各 ASA 論理デバイスごとに、以下を実行います。

a) 更新する論理デバイスの [Set Version] アイコンをクリックして、[Update Image Version] ダイアログボックスを開きます。

b) [New Version] では、アップグレードしたいソフトウェア バージョンを選択します。

c) [OK] をクリックします。

ステップ 9 アップグレードプロセスが完了したら、アプリケーションがオンラインであり、正常にアップグレードされたことを確認します。

a) [論理デバイス（Logical Devices）] を選択します。

b) アプリケーションのバージョンと動作ステータスを確認します。

FXOS CLI を使用した FXOS および ASA スタンドアロン デバイスまたはシャーシ内クラスタのアップグレード

アップグレード プロセスは最大 45 分かかることがあります。アップグレード中、トラフィックはデバイスを通過しません。適切なアップグレード活動の計画を行ってください。

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 および ASA ソフトウェアパッケージをダウンロードします（アップグレードパッケージのダウンロード （28 ページ））。
- FXOS と ASA の構成をバックアップします。
- 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。

手順

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 モードを開始します。

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。

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

c) ダウンロード プロセスをモニターする場合：

scope download-task *image_name*

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 # scope firmware
Firepower-chassis /firmware # download image
scp://user@192.168.1.1/images/fxos-k9.2.3.1.58.SPA
Firepower-chassis /firmware # scope download-task fxos-k9.2.3.1.58.SPA
Firepower-chassis /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 新しいFXOSプラットフォーム バンドルのイメージが正常にダウンロードされたら、FXOS バンドルをアップグレードします。

a) 必要に応じて、ファームウェア モードに戻ります。

up

b) 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をメモします。

show package

c) auto-install モードにします。

scope auto-install

d) FXOS プラットフォーム バンドルをインストールします。

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)）。

e) 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。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。ASA バージョンが互換性テーブルにアップグレード可能としてリストされている限り、これらの警告を無視できます。

yes を入力して、検証に進むことを確認します。

f) 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。

FXOS 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。

g) アップグレードプロセスをモニターするには、アップグレード進行のモニター （125 ページ） を参照してください。

ステップ 4 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、続行する前に、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（インストールの確認 （126 ページ） を参照してください）。

ステップ 5 シャーシに新しい ASA ソフトウェア イメージをダウンロードします。

a) セキュリティ サービス モードを開始します。

top

scope ssa

b) アプリケーション ソフトウェア モードを開始します。

scope app-software

c) 論理デバイス ソフトウェア イメージをダウンロードします。

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@server/path*
- **scp**://*username@server/path*
- **sftp**://*username@server/path*
- **tftp**://*server:port-num/path*

d) ダウンロード プロセスをモニターする場合：

show download-task

e) ダウンロードしたアプリケーションを表示する場合：

up

show app

ダウンロードしたソフトウェアパッケージの ASA のバージョンをメモします。後の手順でアプリケーションを有効にするために、正確なバージョン文字列を使用する必要があります。

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 # scope ssa
Firepower-chassis /ssa # scope app-software
Firepower-chassis /ssa/app-software # download image
scp://user@192.168.1.1/images/cisco-asa.9.4.1.65.csp
Firepower-chassis /ssa/app-software # show download-task

Downloads for Application Software:
    File Name                     Protocol   Server               Userid          State

    ---------------------------- ---------- -------------------- --------------- -----

    cisco-asa.9.4.1.65.csp         Scp        192.168.1.1          user
Downloaded

Firepower-chassis /ssa/app-software # up

Firepower-chassis /ssa # show app

Application:
    Name       Version    Description Author     Deploy Type CSP Type    Is Default App
    ---------- ---------- ----------- ---------- ----------- ----------- --------------
    asa        9.4.1.41   N/A                    Native      Application No
    asa        9.4.1.65   N/A                    Native      Application Yes
```

ステップ 6 アップグレードする各 ASA 論理デバイスごとに、以下を実行います。

a) セキュリティ サービス モードを開始します。

top

scope ssa

b) スコープを更新するセキュリティ モジュールに設定します。

scope slot*slot_number*

c) スコープを更新する ASA アプリケーションに設定します。

scope app-instance asa *instance_name*

d) スタートアップ バージョンを新しい ASA ソフトウェアのバージョンに設定します。

set startup-version *version_number*

ステップ 7 設定を確定します。

commit-buffer

トランザクションをシステム設定にコミットします。アプリケーションイメージが更新され、アプリケーションが再起動します。

ステップ 8 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するには、インストールの確認 （126 ページ） を参照してください。

FXOS および ASA 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

FXOS CLI または Firepower Chassis Manager を使用して、FXOS および ASA 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ます。

Firepower Chassis Manager を使用した FXOS および ASA 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

アップグレード プロセスはシャーシごとに最大 45 分かかることがあります。適切なアップグレード活動の計画を行ってください。

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。

- アクティブになっているユニットとスタンバイになっているユニットを確認する必要があります。ASDM をアクティブな ASA の IP アドレスに接続します。アクティブ装置は、常にアクティブな IP アドレスを保有しています。次に、**[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）]** の順に選択して、このユニットの優先順位（プライマリまたはセカンダリ）を表示し、接続先のユニットを確認できるようにします。
- アップグレード先の FXOS および ASA ソフトウェアパッケージをダウンロードします（アップグレードパッケージのダウンロード （28 ページ））。
- FXOS と ASA の構成をバックアップします。

手順

ステップ 1 スタンバイ ASA 論理デバイスが含まれているシャーシでは、新しい FXOS プラットフォーム バンドル イメージと ASA ソフトウェアイメージをアップロードします。

a) Firepower Chassis Manager で、**[System]** > **[Updates]** を選択します。
[Available Updates] の画面に、シャーシで使用可能なパッケージのリストが表示されます。
b) [Upload Image] をクリックします。
c) [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。

d) [Upload] をクリックします。
選択したイメージがシャーシにアップロードされます。

ステップ 2 新しい FXOS 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後に、スタンバイ ASA 論理デバイスが含まれているシャーシの FXOS バンドルをアップグレードします。

a) アップグレードする FXOS プラットフォーム バンドルの [Upgrade] アイコンをクリックします。

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。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。ASA バージョンが互換性テーブルにアップグレード可能としてリストされている限り、これらの警告を無視できます。

b) [はい（Yes）] をクリックして、インストールを続行することを確認します。

FXOS 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 3 アップグレード中は Firepower Chassis Manager を使用できません。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（アップグレード進行のモニター （125 ページ） を参照してください）。

ステップ 4 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、続行する前に、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（インストールの確認 （126 ページ） を参照してください）。

ステップ 5 ASA 論理デバイス イメージのアップグレード：

a) [Logical Devices] を選択して [Logical Devices] ページを開きます。
[Logical Devices] ページに、シャーシに設定された論理デバイスのリストが表示されます。

b) 更新する論理デバイスの [Set Version] アイコンをクリックして、[Update Image Version] ダイアログボックスを開きます。

c) [New Version] では、更新後のソフトウェア バージョンを選択します。

d) [OK] をクリックします。

ステップ 6 アップグレードプロセスが完了したら、アプリケーションがオンラインであり、正常にアップグレードされたことを確認します。

a) [論理デバイス（Logical Devices）] を選択します。

b) アプリケーションのバージョンと動作ステータスを確認します。

ステップ 7 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) スタンバイ ASA IP アドレスに接続して、スタンバイ装置で ASDM を起動します。

b) **[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、[アクティブにする（Make Active）] をクリックして、スタンバイ装置を強制的にアクティブにします。

ステップ 8 新しいスタンバイ ASA 論理デバイスが含まれているシャーシでは、新しい FXOS プラットフォーム バンドル イメージと ASA ソフトウェアイメージをアップロードします。

a) Firepower Chassis Manager で、**[System]** > **[Updates]** を選択します。
[Available Updates] の画面に、シャーシで使用可能なパッケージのリストが表示されます。
b) [Upload Image] をクリックします。
c) [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。
d) [Upload] をクリックします。
選択したイメージがシャーシにアップロードされます。

ステップ 9 新しい FXOS 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後に、新しいスタンバイ ASA 論理デバイスが含まれているシャーシの FXOS バンドルをアップグレードします。

a) アップグレードする FXOS プラットフォーム バンドルの [Upgrade] アイコンをクリックします。

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。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。ASA バージョンが互換性テーブルにアップグレード可能としてリストされている限り、これらの警告を無視できます。

b) [はい（Yes）] をクリックして、インストールを続行することを確認します。

FXOS 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 10 アップグレード中は Firepower Chassis Manager を使用できません。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（アップグレード進行のモニター （125 ページ） を参照してください）。

ステップ 11 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、続行する前に、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（インストールの確認 （126 ページ） を参照してください）。

ステップ 12 ASA 論理デバイス イメージのアップグレード：

a) [論理デバイス（Logical Devices）] を選択します。
[Logical Devices] ページに、シャーシに設定された論理デバイスのリストが表示されます。論理デバイスが設定されていない場合は、これを通知するメッセージが代わりに表示されます。
b) 更新する論理デバイスの [Set Version] アイコンをクリックして、[Update Image Version] ダイアログボックスを開きます。
c) [New Version] では、更新後のソフトウェア バージョンを選択します。
d) [OK] をクリックします。

ステップ 13 アップグレードプロセスが完了したら、アプリケーションがオンラインであり、正常にアップグレードされたことを確認します。

a) [論理デバイス（Logical Devices）] を選択します。
b) アプリケーションのバージョンと動作ステータスを確認します。

ステップ 14 （オプション）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) スタンバイ ASA IP アドレスに接続して、スタンバイ装置で ASDM を起動します。
b) **[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、[アクティブにする（Make Active）] をクリックして、スタンバイ装置を強制的にアクティブにします。

FXOS CLI を使用した FXOS および ASA 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

アップグレード プロセスはシャーシごとに最大 45 分かかることがあります。適切なアップグレード活動の計画を行ってください。

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。

- どのユニットがアクティブで、どのユニットがスタンバイかを特定する必要があります。シャーシで ASA コンソールに接続し、**show failover** コマンドを入力してユニットのアクティブ/スタンバイステータスを表示します。
- アップグレード先の FXOS および ASA ソフトウェアパッケージをダウンロードします（アップグレードパッケージのダウンロード （28 ページ））。
- FXOS と ASA の構成をバックアップします。
- 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。

手順

ステップ 1 スタンバイ ASA 論理デバイスが含まれているシャーシでは、新しい FXOS プラットフォーム バンドル イメージをダウンロードします。

a) FXOS CLI に接続します。
b) ファームウェア モードを開始します。

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。

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

d) ダウンロード プロセスをモニターする場合：

scope download-task *image_name*

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 # scope firmware
Firepower-chassis /firmware # download image
scp://user@192.168.1.1/images/fxos-k9.2.3.1.58.SPA
Firepower-chassis /firmware # scope download-task fxos-k9.2.3.1.58.SPA
Firepower-chassis /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 2 新しいFXOSプラットフォーム バンドルのイメージが正常にダウンロードされたら、FXOSバンドルをアップグレードします。

a) 必要に応じて、ファームウェア モードに戻ります。

up

b) 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をメモします。

show package

c) auto-install モードにします。

scope auto-install

d) FXOS プラットフォーム バンドルをインストールします。

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)）。

e) 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。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。ASA バージョンが互換性テーブルにアップグレード可能としてリストされている限り、これらの警告を無視できます。

yes を入力して、検証に進むことを確認します。

f) 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。

FXOS 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。

g) アップグレードプロセスをモニターするには、アップグレード進行のモニター（125 ページ） を参照してください。

ステップ 3 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、続行する前に、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（インストールの確認 （126 ページ） を参照してください）。

ステップ 4 シャーシに新しい ASA ソフトウェア イメージをダウンロードします。

a) セキュリティ サービス モードを開始します。

top

scope ssa

b) アプリケーション ソフトウェア モードを開始します。

scope app-software

c) 論理デバイス ソフトウェア イメージをダウンロードします。

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@server*/*path*
- **scp**://*username@server*/*path*
- **sftp**://*username@server*/*path*
- **tftp**://*server*:*port-num*/*path*

d) ダウンロード プロセスをモニターする場合：

show download-task

e) ダウンロードしたアプリケーションを表示する場合：

up

show app

ダウンロードしたソフトウェアパッケージの ASA のバージョンをメモします。後の手順でアプリケーションを有効にするために、正確なバージョン文字列を使用する必要があります。

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 # scope ssa
Firepower-chassis /ssa # scope app-software
Firepower-chassis /ssa/app-software # download image
scp://user@192.168.1.1/images/cisco-asa.9.4.1.65.csp
Firepower-chassis /ssa/app-software # show download-task

Downloads for Application Software:
    File Name                     Protocol   Server               Userid          State

    ----------------------------- ---------- -------------------- --------------- -----

    cisco-asa.9.4.1.65.csp         Scp        192.168.1.1          user
Downloaded

Firepower-chassis /ssa/app-software # up

Firepower-chassis /ssa # show app

Application:
    Name       Version    Description Author     Deploy Type CSP Type    Is Default App
    ---------- ---------- ----------- ---------- ----------- ----------- --------------
    asa        9.4.1.41   N/A                    Native      Application No
    asa        9.4.1.65   N/A                    Native      Application Yes
```

ステップ 5 ASA 論理デバイス イメージのアップグレード：

a) セキュリティ サービス モードを開始します。

top

scope ssa

b) スコープを更新するセキュリティ モジュールに設定します。

scope slot*slot_number*

c) スコープを更新する ASA アプリケーションに設定します。

scope app-instance asa *instance_name*

d) スタートアップ バージョンを更新するバージョンに設定します。

set startup-version *version_number*

e) 設定を確定します。

commit-buffer

トランザクションをシステム設定にコミットします。アプリケーション イメージが更新され、アプリケーションが再起動します。

ステップ 6 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するには、インストールの確認 （126 ページ） を参照してください。

ステップ 7 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) スタンバイ ASA 論理デバイスが含まれるシャーシで、コンソール接続または Telnet 接続を使用してモジュール CLI に接続します。

connect module *slot_number* {**console** | **telnet**}

複数のセキュリティ モジュールをサポートしないデバイスのセキュリティ エンジンに接続するには、*slot_number* として **1** を使用します。

例：

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>
```

b) アプリケーションのコンソールに接続します。

connect asa

例：

```
Firepower-module1> connect asa
Connecting to asa(asa1) console... hit Ctrl + A + D  to return to bootCLI
[...]
asa>
```

c) この装置をアクティブにします。

failover active

d) 設定を保存します。

write memory

e) ユニットがアクティブであることを確認します。

show failover

ステップ 8 アプリケーション コンソールを終了して FXOS モジュール CLI に移動します。

Ctrl-a, d と入力します。

ステップ 9 FXOS CLI のスーパバイザ レベルに戻ります。

コンソールを終了します。

a) **~** と入力

Telnet アプリケーションに切り替わります。

b) Telnet アプリケーションを終了するには、次を入力します。

telnet>**quit**

Telnet セッションを終了します。

a) **Ctrl-], .** と入力

ステップ 10 新しいスタンバイ ASA 論理デバイスが含まれているシャーシでは、新しい FXOS プラットフォーム バンドル イメージをダウンロードします。

a) FXOS CLI に接続します。

b) ファームウェア モードを開始します。

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。

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

d) ダウンロード プロセスをモニターする場合：

scope download-task *image_name*

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 # scope firmware
Firepower-chassis /firmware # download image
scp://user@192.168.1.1/images/fxos-k9.2.3.1.58.SPA
Firepower-chassis /firmware # scope download-task fxos-k9.2.3.1.58.SPA
Firepower-chassis /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 11 新しいFXOSプラットフォーム バンドルのイメージが正常にダウンロードされたら、FXOSバンドルをアップグレードします。

a) 必要に応じて、ファームウェア モードに戻ります。

up

b) 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をメモします。

show package

c) auto-install モードにします。

scope auto-install

d) FXOS プラットフォーム バンドルをインストールします。

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)）。

e) 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。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。ASA バージョンが互換性テーブルにアップグレード可能としてリストされている限り、これらの警告を無視できます。

yes を入力して、検証に進むことを確認します。

f) 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。

FXOS 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。

g) アップグレードプロセスをモニターするには、アップグレード進行のモニター（125 ページ） を参照してください。

ステップ 12 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、続行する前に、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（インストールの確認 （126 ページ） を参照してください）。

ステップ 13 シャーシに新しい ASA ソフトウェア イメージをダウンロードします。

a) セキュリティ サービス モードを開始します。

top

scope ssa

b) アプリケーション ソフトウェア モードを開始します。

scope app-software

c) 論理デバイス ソフトウェア イメージをダウンロードします。

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@server/path*
- **scp**://*username@server/path*
- **sftp**://*username@server/path*
- **tftp**://*server*:*port-num*/*path*

d) ダウンロード プロセスをモニターする場合：

show download-task

e) ダウンロードしたアプリケーションを表示する場合：

up

show app

ダウンロードしたソフトウェアパッケージの ASA のバージョンをメモします。後の手順でアプリケーションを有効にするために、正確なバージョン文字列を使用する必要があります。

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 # scope ssa
Firepower-chassis /ssa # scope app-software
Firepower-chassis /ssa/app-software # download image
scp://user@192.168.1.1/images/cisco-asa.9.4.1.65.csp
Firepower-chassis /ssa/app-software # show download-task

Downloads for Application Software:
    File Name                     Protocol   Server               Userid          State

    ----------------------------- ---------- -------------------- --------------- -----

    cisco-asa.9.4.1.65.csp         Scp        192.168.1.1          user
Downloaded

Firepower-chassis /ssa/app-software # up

Firepower-chassis /ssa # show app

Application:
    Name       Version    Description Author     Deploy Type CSP Type    Is Default App
    ---------- ---------- ----------- ---------- ----------- ----------- --------------
    asa        9.4.1.41   N/A                    Native      Application No
    asa        9.4.1.65   N/A                    Native      Application Yes
```

ステップ 14 ASA 論理デバイス イメージのアップグレード：

a) セキュリティ サービス モードを開始します。

top

scope ssa

b) スコープを更新するセキュリティ モジュールに設定します。

scope slot*slot_number*

c) スコープを更新する ASA アプリケーションに設定します。

scope app-instance asa *instance_name*

d) スタートアップ バージョンを更新するバージョンに設定します。

set startup-version *version_number*

e) 設定を確定します。

commit-buffer

トランザクションをシステム設定にコミットします。アプリケーションイメージが更新され、アプリケーションが再起動します。

ステップ 15 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するには、インストールの確認 （126 ページ） を参照してください。

ステップ 16 （オプション）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) スタンバイ ASA 論理デバイスが含まれるシャーシで、コンソール接続または Telnet 接続を使用してモジュール CLI に接続します。

connect module *slot_number* {**console** | **telnet**}

複数のセキュリティ モジュールをサポートしないデバイスのセキュリティ エンジンに接続するには、*slot_number* として **1** を使用します。

例：

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>
```

b) アプリケーションのコンソールに接続します。

connect asa

例：

```
Firepower-module1> connect asa
Connecting to asa(asa1) console... hit Ctrl + A + D  to return to bootCLI
[...]
asa>
```

c) この装置をアクティブにします。

failover active

d) 設定を保存します。

write memory

e) ユニットがアクティブであることを確認します。

show failover

FXOS および ASA 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

FXOS CLI または Firepower Chassis Manager を使用して、FXOS および ASA 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ます。

Firepower Chassis Manager を使用した FXOS および ASA 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

アップグレード プロセスはシャーシごとに最大 45 分かかることがあります。適切なアップグレード活動の計画を行ってください。

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。

- どのユニットがプライマリ ユニットか特定する必要があります。ASDM に接続し、**[Monitoring]** > **[Properties]** > **[Failover]** > **[Status]** の順に選択して、このユニットの優先順位（プライマリまたはセカンダリ）を表示し、接続先のユニットを確認できるようにします。
- アップグレード先の FXOS および ASA ソフトウェアパッケージをダウンロードします。
- FXOS と ASA の構成をバックアップします。

手順

ステップ 1 プライマリ 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。

a) フェールオーバー グループ 1 の管理アドレスに接続して、プライマリ ユニット（またはフェールオーバー グループ 1 がアクティブに設定されているユニット）で ASDM を起動します。

b) **[モニタリング（Monitoring）]** > **[フェールオーバー（Failover）]** > **[フェールオーバー グループ 2（Failover Group 2）]** の順に選択して、[アクティブにする（Make Active）] をクリックします。

c) 後続の手順のために、このユニットの ASDM に接続したままにします。

ステップ 2 セカンダリ ASA 論理デバイスが含まれているシャーシでは、新しい FXOS プラットフォーム バンドル イメージと ASA ソフトウェアイメージをアップロードします。

a) セカンダリユニットの Firepower Chassis Manager に接続します。

b) **[システム（System）]** > **[更新（Updates）]** を選択します。
[Available Updates] の画面に、シャーシで使用可能なパッケージのリストが表示されます。

c) [Upload Image] をクリックします。
d) [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。
e) [Upload] をクリックします。
選択したイメージがシャーシにアップロードされます。

ステップ 3 新しい FXOS 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後に、セカンダリ ASA 論理デバイスが含まれているシャーシの FXOS バンドルをアップグレードします。

a) アップグレードする FXOS プラットフォーム バンドルの [Upgrade] アイコンをクリックします。

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。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。ASA バージョンが互換性テーブルにアップグレード可能としてリストされている限り、これらの警告を無視できます。

b) [はい（Yes）] をクリックして、インストールを続行することを確認します。

FXOS 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 4 アップグレード中は Firepower Chassis Manager を使用できません。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（アップグレード進行のモニター （125 ページ） を参照してください）。

ステップ 5 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、続行する前に、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（インストールの確認 （126 ページ） を参照してください）。

ステップ 6 ASA 論理デバイス イメージのアップグレード：

a) [論理デバイス（Logical Devices）] を選択します。
[Logical Devices] ページに、シャーシに設定された論理デバイスのリストが表示されます。
b) 更新する論理デバイスの [Set Version] アイコンをクリックして、[Update Image Version] ダイアログボックスを開きます。
c) [New Version] では、更新後のソフトウェア バージョンを選択します。
d) [OK] をクリックします。

ステップ 7 アップグレードプロセスが完了したら、アプリケーションがオンラインであり、正常にアップグレードされたことを確認します。

a) [論理デバイス（Logical Devices）] を選択します。
b) アプリケーションのバージョンと動作ステータスを確認します。

ステップ 8 セカンダリ 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。

a) フェールオーバー グループ 1 の管理アドレスに接続して、プライマリ ユニット（またはフェールオーバー グループ 1 がアクティブに設定されているユニット）で ASDM を起動します。

b) **[Monitoring]** > **[Failover]** > **[Failover Group 1]** の順に選択して、[Make Standby] をクリックします。

c) **[Monitoring]** > **[Failover]** > **[Failover Group 2]** の順に選択して、[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 9 プライマリ ASA 論理デバイスが含まれているシャーシでは、新しい FXOS プラットフォーム バンドル イメージと ASA ソフトウェアイメージをアップロードします。

a) プライマリユニットの Firepower Chassis Manager に接続します。

b) **[システム（System）]** > **[更新（Updates）]** を選択します。
[Available Updates] の画面に、シャーシで使用可能なパッケージのリストが表示されます。

c) [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。

d) [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。

e) [Upload] をクリックします。
選択したパッケージがシャーシにアップロードされます。

f) 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 10 新しい FXOS 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後に、プライマリ ASA 論理デバイスが含まれているシャーシの FXOS バンドルをアップグレードします。

a) アップグレードする FXOS プラットフォーム バンドルの [Upgrade] アイコンをクリックします。

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。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。ASA バージョンが互換性テーブルにアップグレード可能としてリストされている限り、これらの警告を無視できます。

b) [はい（Yes）] をクリックして、インストールを続行することを確認します。

FXOS 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 11 アップグレード中は Firepower Chassis Manager を使用できません。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（アップグレード進行のモニター （125 ページ） を参照してください）。

ステップ 12 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、続行する前に、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（インストールの確認 （126 ページ） を参照してください）。

ステップ 13 ASA 論理デバイス イメージのアップグレード：

a) [論理デバイス（Logical Devices）] を選択します。
[Logical Devices] ページに、シャーシに設定された論理デバイスのリストが表示されます。
b) 更新する論理デバイスの [Set Version] アイコンをクリックして、[Update Image Version] ダイアログボックスを開きます。
c) [New Version] では、更新後のソフトウェア バージョンを選択します。
d) [OK] をクリックします。

ステップ 14 アップグレードプロセスが完了したら、アプリケーションがオンラインであり、正常にアップグレードされたことを確認します。

a) [論理デバイス（Logical Devices）] を選択します。
b) アプリケーションのバージョンと動作ステータスを確認します。

ステップ 15 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。[Preempt Enabled] でフェールオーバー グループが設定されていない場合は、[Monitoring] > [Failover] > [Failover Group #] ペインを使用して、指定された装置上でアクティブ ステータスに戻すことができます。

FXOS CLI を使用した FXOS および ASA 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

アップグレード プロセスはシャーシごとに最大 45 分かかることがあります。適切なアップグレード活動の計画を行ってください。

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。

- どのユニットがプライマリかを特定する必要があります。シャーシで ASA コンソールに接続し、**show failover** コマンドを入力してユニットの状態と優先順位（プライマリまたはセカンダリ）を表示します。
- アップグレード先の FXOS および ASA ソフトウェアパッケージをダウンロードします。
- FXOS と ASA の構成をバックアップします。
- 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。

手順

ステップ 1 コンソール ポート（推奨）または SSH を使用して、セカンダリ ユニットの FXOS CLI に接続します。

ステップ 2 プライマリ 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。

a) コンソール接続または Telnet 接続を使用して、モジュール CLI に接続します。

connect module *slot_number* {**console** | **telnet**}

複数のセキュリティ モジュールをサポートしないデバイスのセキュリティ エンジンに接続するには、*slot_number* として **1** を使用します。

例：

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>
```

b) アプリケーションのコンソールに接続します。

connect asa

例：

```
Firepower-module1> connect asa
Connecting to asa(asa1) console... hit Ctrl + A + D  to return to bootCLI
[...]
asa>
```

c) プライマリ 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。

enable

デフォルトで、イネーブル パスワードは空白です。

no failover active group 1

no failover active group 2

例：

```
asa> enable
Password: <blank>
asa# no failover active group 1
asa# no failover active group 2
```

ステップ 3 アプリケーション コンソールを終了して FXOS モジュール CLI に移動します。

Ctrl-a, d と入力します。

ステップ 4 FXOS CLI のスーパバイザ レベルに戻ります。

コンソールを終了します。

a) ~ と入力

Telnet アプリケーションに切り替わります。

b) Telnet アプリケーションを終了するには、次を入力します。

telnet>**quit**

Telnet セッションを終了します。

a) **Ctrl-], .** と入力

ステップ 5 セカンダリ ASA 論理デバイスが含まれているシャーシでは、新しい FXOS プラットフォーム バンドル イメージと ASA ソフトウェアイメージをダウンロードします。

a) FXOS CLI に接続します。

b) ファームウェア モードを開始します。

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。

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

d) ダウンロード プロセスをモニターする場合：

scope download-task *image_name*

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 # scope firmware
Firepower-chassis /firmware # download image
scp://user@192.168.1.1/images/fxos-k9.2.3.1.58.SPA
Firepower-chassis /firmware # scope download-task fxos-k9.2.3.1.58.SPA
Firepower-chassis /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 6 新しいFXOSプラットフォーム バンドルのイメージが正常にダウンロードされたら、FXOSバンドルをアップグレードします。

a) 必要に応じて、ファームウェア モードに戻ります。

top

scope firmware

b) 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をメモします。

show package

c) auto-install モードにします。

scope auto-install

d) FXOS プラットフォーム バンドルをインストールします。

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)）。

e) 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。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。ASA バージョンが互換性テーブルにアップグレード可能としてリストされている限り、これらの警告を無視できます。

yes を入力して、検証に進むことを確認します。

f) 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。

FXOS 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。

g) アップグレードプロセスをモニターするには、アップグレード進行のモニター （125 ページ） を参照してください。

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、続行する前に、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（インストールの確認 （126 ページ） を参照してください）。

ステップ 8 シャーシに新しい ASA ソフトウェア イメージをダウンロードします。

a) セキュリティ サービス モードを開始します。

top

scope ssa

b) アプリケーション ソフトウェア モードを開始します。

scope app-software

c) 論理デバイス ソフトウェア イメージをダウンロードします。

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@server*/*path*
- **scp**://*username@server*/*path*
- **sftp**://*username@server*/*path*
- tftp://*server*:*port-num*/*path*

d) ダウンロード プロセスをモニターする場合：

show download-task

e) ダウンロードしたアプリケーションを表示する場合：

up

show app

ダウンロードしたソフトウェアパッケージの ASA のバージョンをメモします。後の手順でアプリケーションを有効にするために、正確なバージョン文字列を使用する必要があります。

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 # scope ssa
Firepower-chassis /ssa # scope app-software
Firepower-chassis /ssa/app-software # download image
scp://user@192.168.1.1/images/cisco-asa.9.4.1.65.csp
Firepower-chassis /ssa/app-software # show download-task

Downloads for Application Software:
    File Name                     Protocol   Server              Userid          State

   ----------------------------- ---------- ------------------- --------------- -----

    cisco-asa.9.4.1.65.csp         Scp        192.168.1.1          user
Downloaded

Firepower-chassis /ssa/app-software # up

Firepower-chassis /ssa # show app

Application:
    Name       Version    Description Author     Deploy Type CSP Type    Is Default App
    ---------- ---------- ----------- ---------- ----------- ----------- --------------
    asa        9.4.1.41   N/A                    Native      Application No
    asa        9.4.1.65   N/A                    Native      Application Yes
```

ステップ 9 ASA 論理デバイス イメージのアップグレード：

a) セキュリティ サービス モードを開始します。

top

scope ssa

b) スコープを更新するセキュリティ モジュールに設定します。

scope slot*slot_number*

c) スコープを更新する ASA アプリケーションに設定します。

scope app-instance asa *instance_name*

d) スタートアップ バージョンを更新するバージョンに設定します。

set startup-version *version_number*

e) 設定を確定します。

commit-buffer

トランザクションをシステム設定にコミットします。アプリケーション イメージが更新され、アプリケーションが再起動します。

ステップ 10 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するには、インストールの確認 （126 ページ） を参照してください。

ステップ 11 セカンダリ 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。

a) コンソール接続または Telnet 接続を使用して、モジュール CLI に接続します。

connect module *slot_number* {**console** | **telnet**}

複数のセキュリティ モジュールをサポートしないデバイスのセキュリティ エンジンに接続するには、*slot_number* として **1** を使用します。

例：

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>
```

b) アプリケーションのコンソールに接続します。

connect asa

例：

```
Firepower-module1> connect asa
Connecting to asa(asa1) console... hit Ctrl + A + D  to return to bootCLI
[...]
```

```
asa>
```

c) セカンダリ 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。

enable

デフォルトで、イネーブル パスワードは空白です。

failover active group 1

failover active group 2

例：

```
asa> enable
Password: <blank>
asa# failover active group 1
asa# failover active group 2
```

ステップ 12 アプリケーション コンソールを終了して FXOS モジュール CLI に移動します。

Ctrl-a, d と入力します。

ステップ 13 FXOS CLI のスーパバイザ レベルに戻ります。

コンソールを終了します。

a) ~ と入力

Telnet アプリケーションに切り替わります。

b) Telnet アプリケーションを終了するには、次を入力します。

telnet>**quit**

Telnet セッションを終了します。

a) **Ctrl-], .** と入力

ステップ 14 プライマリ ASA 論理デバイスが含まれているシャーシでは、新しい FXOS プラットフォーム バンドル イメージと ASA ソフトウェアイメージをダウンロードします。

a) FXOS CLI に接続します。

b) ファームウェア モードを開始します。

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。

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

d) ダウンロード プロセスをモニターする場合：

scope download-task *image_name*

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 # scope firmware
Firepower-chassis /firmware # download image
scp://user@192.168.1.1/images/fxos-k9.2.3.1.58.SPA
Firepower-chassis /firmware # scope download-task fxos-k9.2.3.1.58.SPA
Firepower-chassis /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 15 新しいFXOSプラットフォーム バンドルのイメージが正常にダウンロードされたら、FXOSバンドルをアップグレードします。

a) 必要に応じて、ファームウェア モードに戻ります。

up

b) 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をメモします。

show package

c) auto-install モードにします。

scope auto-install

d) FXOS プラットフォーム バンドルをインストールします。

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)）。

e) 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。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。ASA バージョンが互換性テーブルにアップグレード可能としてリストされている限り、これらの警告を無視できます。

yes を入力して、検証に進むことを確認します。

f) 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。

FXOS 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。

g) アップグレードプロセスをモニターするには、アップグレード進行のモニター（125 ページ） を参照してください。

ステップ 16 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、続行する前に、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（インストールの確認 （126 ページ） を参照してください）。

ステップ 17 シャーシに新しい ASA ソフトウェア イメージをダウンロードします。

a) セキュリティ サービス モードを開始します。

top

scope ssa

b) アプリケーション ソフトウェア モードを開始します。

scope app-software

c) 論理デバイス ソフトウェア イメージをダウンロードします。

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@server*/*path*
- **scp**://*username@server*/*path*
- **sftp**://*username@server*/*path*
- **tftp**://*server*:*port-num*/*path*

d) ダウンロード プロセスをモニターする場合：

show download-task

e) ダウンロードしたアプリケーションを表示する場合：

up

show app

ダウンロードしたソフトウェアパッケージの ASA のバージョンをメモします。後の手順でアプリケーションを有効にするために、正確なバージョン文字列を使用する必要があります。

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 # scope ssa
Firepower-chassis /ssa # scope app-software
Firepower-chassis /ssa/app-software # download image
scp://user@192.168.1.1/images/cisco-asa.9.4.1.65.csp
Firepower-chassis /ssa/app-software # show download-task

Downloads for Application Software:
    File Name                     Protocol   Server              Userid          State
```

```
    ------------------------------ ---------- ------------------- --------------- -----

    cisco-asa.9.4.1.65.csp         Scp        192.168.1.1         user
Downloaded

Firepower-chassis /ssa/app-software # up

Firepower-chassis /ssa # show app

Application:
    Name       Version    Description Author     Deploy Type CSP Type    Is Default App
    ---------- ---------- ----------- ---------- ----------- ----------- --------------
    asa        9.4.1.41   N/A                    Native      Application No
    asa        9.4.1.65   N/A                    Native      Application Yes
```

ステップ 18 ASA 論理デバイス イメージのアップグレード：

a) セキュリティ サービス モードを開始します。

top

scope ssa

b) スコープを更新するセキュリティ モジュールに設定します。

scope slot*slot_number*

c) スコープを更新する ASA アプリケーションに設定します。

scope app-instance asa *instance_name*

d) スタートアップ バージョンを更新するバージョンに設定します。

set startup-version *version_number*

e) 設定を確定します。

commit-buffer

トランザクションをシステム設定にコミットします。アプリケーション イメージが更新され、アプリケーションが再起動します。

ステップ 19 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するには、インストールの確認 （126 ページ） を参照してください。

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。[Preempt Enabled] でフェールオーバー グループが設定されていない場合は、[Monitoring] > [Failover] > [Failover Group #] ペインを使用して、指定された装置上でアクティブ ステータスに戻すことができます。

FXOS および ASA シャーシ間クラスタのアップグレード

FXOS CLI または Firepower Chassis Manager を使用して、シャーシ間クラスタ内のすべてのシャーシの FXOS と ASA をアップグレードします。

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

アップグレード プロセスはシャーシごとに最大 45 分かかることがあります。適切なアップグレード活動の計画を行ってください。

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 および ASA ソフトウェアパッケージをダウンロードします。
- FXOS と ASA の構成をバックアップします。

手順

ステップ 1 どのシャーシに制御ノードがあるかを決定します。このシャーシは最後にアップグレードします。

a) Firepower Chassis Manager に接続します。
b) [論理デバイス（Logical Devices）] を選択します。
c) クラスタに含まれるセキュリティ モジュールの属性を表示するには、プラス記号（+）をクリックします。
d) 制御ノードがこのシャーシ上にあることを確認します。**CLUSTER-ROLE** が "Control" に設定されている ASA インスタンスがあるはずです。

ステップ 2 **制御ノードがない**クラスタ内のシャーシの Firepower Chassis Manager に接続します。

ステップ 3 新しい FXOS プラットフォーム バンドルのイメージと ASA ソフトウェア イメージのアップロード：

a) Firepower Chassis Manager で、**[システム（System）] > [更新（Updates）]** を選択します。[Available Updates] の画面に、シャーシで使用可能なパッケージのリストが表示されます。
b) [Upload Image] をクリックします。
c) [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。
d) [Upload] をクリックします。
選択したイメージがシャーシにアップロードされます。
e) 続行する前に、イメージが正常にアップロードされるまで待ちます。

ステップ 4 FXOS バンドルのアップグレード：

a) [System] > [Updates] を選択します。
b) アップグレードする FXOS プラットフォーム バンドルの [Upgrade] アイコンをクリックします。

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。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。ASA バージョンが互換性テーブルにアップグレード可能としてリストされている限り、これらの警告を無視できます。

c) [はい（Yes）] をクリックして、インストールを続行することを確認します。

FXOS 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 アップグレード中は Firepower Chassis Manager を使用できません。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（アップグレード進行のモニター （125 ページ） を参照してください）。

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、続行する前に、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（インストールの確認 （126 ページ） を参照してください）。

ステップ 7 各セキュリティモジュールでの ASA 論理デバイス イメージのアップグレード：

a) [論理デバイス（Logical Devices）] を選択します。
[Logical Devices] ページに、シャーシに設定された論理デバイスのリストが表示されます。

b) 更新する論理デバイスの [Set Version] アイコンをクリックして、[Update Image Version] ダイアログボックスを開きます。

c) [New Version] では、更新後のソフトウェア バージョンを選択します。

d) [OK] をクリックします。

ステップ 8 アップグレードプロセスが完了したら、アプリケーションがオンラインであり、正常にアップグレードされたことを確認します。

a) [論理デバイス（Logical Devices）] を選択します。

b) アプリケーションのバージョンと動作ステータスを確認します。

ステップ 9 制御ノードがないクラスタ内の残りのすべてのシャーシで、手順 ステップ 2 （117 ページ） ～ ステップ 8 （118 ページ） を繰り返します。

ステップ 10 制御ノードがないクラスタ内のすべてのシャーシをアップグレードしたら、**制御ノードがある**シャーシで手順 ステップ 2 （117 ページ） ～ ステップ 8 （118 ページ） を繰り返します。
新しい制御ノードが、以前にアップグレードされたシャーシのいずれかから選択されます。

ステップ 11 分散型 VPN クラスタリングモードでは、クラスタが安定したら、制御ノードで ASA コンソールを使用して、クラスタ内のすべてのモジュール間でアクティブセッションを再配布することができます。

cluster redistribute vpn-sessiondb

次のタスク

シャーシのサイト ID を設定します。シャーシのサイト ID を設定する方法の詳細については、Cisco.com で『Deploying a Cluster for ASA for the Firepower 4100/9300 for Scalability and High Availability』の「Inter-Site Clustering」トピックを参照してください。

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

アップグレード プロセスはシャーシごとに最大 45 分かかることがあります。適切なアップグレード活動の計画を行ってください。

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 および ASA ソフトウェアパッケージをダウンロードします（アップグレードパッケージのダウンロード （28 ページ））。
- FXOS と ASA の構成をバックアップします。
- 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。

手順

ステップ 1 どのシャーシに制御ノードがあるかを決定します。このシャーシは最後にアップグレードします。

a) FXOS CLI に接続します。

b) 制御ノードがこのシャーシ上にあることを確認します。Cluster Role が "Control" に設定されている ASA インスタンスがあるはずです。

scope ssa

show app-instance

ステップ 2 **制御ノードがない**クラスタ内のシャーシの FXOS CLI に接続します。

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

a) ファームウェア モードを開始します。

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。

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@server*/*path*/*image_name*
- **scp**://*username@server*/*path*/*image_name*

- **sftp**://*username@server*/*path*/*image_name*
- **tftp**://*server*:*port-num*/*path*/*image_name*

c) ダウンロード プロセスをモニターする場合：

scope download-task *image_name*

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 # scope firmware
Firepower-chassis /firmware # download image
scp://user@192.168.1.1/images/fxos-k9.2.3.1.58.SPA
Firepower-chassis /firmware # scope download-task fxos-k9.2.3.1.58.SPA
Firepower-chassis /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 FXOS バンドルをアップグレードします。

a) 必要に応じて、ファームウェア モードに戻ります。

top

scope firmware

b) 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をメモします。

show package

c) auto-install モードにします。

scope auto-install

d) FXOS プラットフォーム バンドルをインストールします。

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)）。

e) 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。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。ASA バージョンが互換性テーブルにアップグレード可能としてリストされている限り、これらの警告を無視できます。

yes を入力して、検証に進むことを確認します。

f) 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。

FXOS 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。

g) アップグレードプロセスをモニターするには、アップグレード進行のモニター（125 ページ） を参照してください。

ステップ 5 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、続行する前に、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（インストールの確認 （126 ページ） を参照してください）。

ステップ 6 シャーシに新しい ASA ソフトウェア イメージをダウンロードします。

a) セキュリティ サービス モードを開始します。

top

scope ssa

b) アプリケーション ソフトウェア モードを開始します。

scope app-software

c) 論理デバイス ソフトウェア イメージをダウンロードします。

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@server*/*path*
- **scp**://*username@server*/*path*
- **sftp**://*username@server*/*path*
- **tftp**://*server*:*port-num*/*path*

d) ダウンロード プロセスをモニターする場合：

show download-task

e) ダウンロードしたアプリケーションを表示する場合：

up

show app

ダウンロードしたソフトウェアパッケージの ASA のバージョンをメモします。後の手順でアプリケーションを有効にするために、正確なバージョン文字列を使用する必要があります。

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 # scope ssa
Firepower-chassis /ssa # scope app-software
```

```
Firepower-chassis /ssa/app-software # download image
scp://user@192.168.1.1/images/cisco-asa.9.4.1.65.csp
Firepower-chassis /ssa/app-software # show download-task

Downloads for Application Software:
    File Name                     Protocol   Server               Userid          State

    ----------------------------- ---------- -------------------- --------------- -----

    cisco-asa.9.4.1.65.csp         Scp        192.168.1.1          user
Downloaded

Firepower-chassis /ssa/app-software # up

Firepower-chassis /ssa # show app

Application:
    Name       Version    Description Author     Deploy Type CSP Type    Is Default App
    ---------- ---------- ----------- ---------- ----------- ----------- --------------
    asa        9.4.1.41   N/A                    Native      Application No
    asa        9.4.1.65   N/A                    Native      Application Yes
```

ステップ 7 ASA 論理デバイス イメージのアップグレード：

a) セキュリティ サービス モードを開始します。

top

scope ssa

b) スコープを更新するセキュリティ モジュールに設定します。

scope slot*slot_number*

c) スコープを更新する ASA アプリケーションに設定します。

scope app-instance asa *instance_name*

d) スタートアップ バージョンを更新するバージョンに設定します。

set startup-version *version_number*

e) 設定を確定します。

commit-buffer

トランザクションをシステム設定にコミットします。アプリケーション イメージが更新され、アプリケーションが再起動します。

ステップ 8 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するには、インストールの確認 （126 ページ） を参照してください。

ステップ 9 制御ノードがないクラスタ内の残りのすべてのシャーシで、手順ステップ 2 （119 ページ） ～ ステップ 8 （122 ページ） を繰り返します。

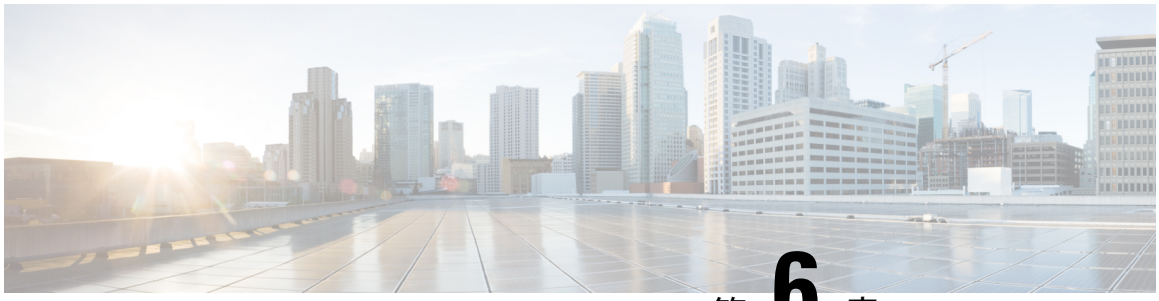
ステップ 10 制御ノードがないクラスタ内のすべてのシャーシをアップグレードしたら、**制御ノードがある**シャーシで手順ステップ 2 （119 ページ） ～ ステップ 8 （122 ページ） を繰り返します。新しい制御ノードが、以前にアップグレードされたシャーシのいずれかから選択されます。

ステップ 11 分散型 VPN クラスタリングモードでは、クラスタが安定したら、制御ノードで ASA コンソールを使用して、クラスタ内のすべてのモジュール間でアクティブセッションを再配布することができます。

cluster redistribute vpn-sessiondb

次のタスク

シャーシのサイト ID を設定します。シャーシのサイト ID を設定する方法の詳細については、Cisco.com で『Deploying a Cluster for ASA for the Firepower 4100/9300 for Scalability and High Availability』の「Inter-Site Clustering」トピックを参照してください。



第 6 章

アップグレードの進行状況のモニターとインストールの確認

アップグレード進行のモニター

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。

手順

ステップ 1 FXOS CLI に接続します。

ステップ 2 **scope system** を入力します。

ステップ 3 **show firmware monitor** を入力します。

ステップ 4 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

```
Firepower-chassis# scope system
Firepower-chassis /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
```

インストールの確認

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。

手順

ステップ 1 FXOS CLI に接続します。

ステップ 2 **top** を入力します。

ステップ 3 **scope ssa** を入力します。

ステップ 4 **show slot** を入力します。

ステップ 5 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。

例：

ステップ 6 **show app-instance** を入力します。

ステップ 7 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」であり、正しいバージョンがリストされていることを確認します。

このシャーシがクラスタの一部である場合、シャーシにインストールされているすべてのセキュリティ モジュールで、クラスタ動作状態が「In-Cluster」であることを確認します。また、制御ユニットがアップグレードするシャーシ上にないことを確認します。Cluster Role が「Master」に設定されているインスタンスがあってはいけません。

例

```
Firepower-chassis# scope ssa
Firepower-chassis /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
Firepower-chassis /ssa #
Firepower-chassis /ssa # show app-instance
App Name   Identifier Slot ID    Admin State Oper State       Running Version Startup
Version Cluster State   Cluster Role
---------- ---------- ---------- ----------- ---------------- ---------------
--------------- --------------- ------------
asa        asa1       1          Enabled     Online           9.10.0.85       9.10.0.85
       Not Applicable  None
asa        asa2       2          Enabled     Online           9.10.0.85       9.10.0.85
       Not Applicable  None
Firepower-chassis /ssa #
```

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。