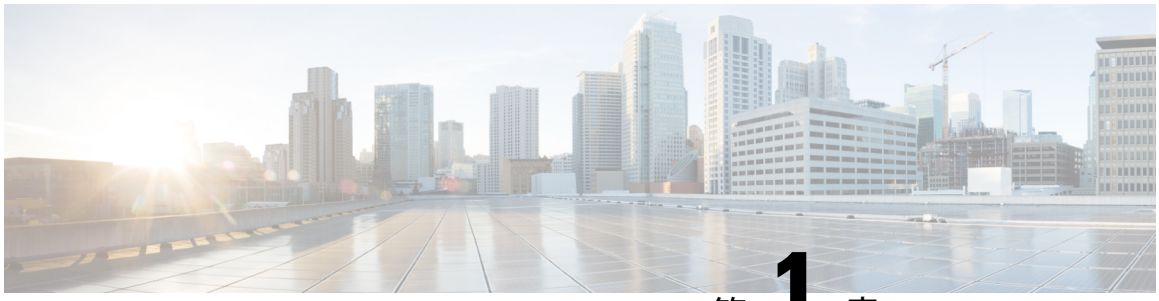
クラウド提供型 Firewall Management Center 用 Cisco Secure Firewall Threat Defense アップグレードガイド

最終更新：2024 年 11 月 21 日

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

目 次



第 1 章

アップグレードの計画

Threat Defense のアップグレードを計画および完了するには、このガイドを使用します。アップグレードには、メジャー（A.x）、メンテナンス（A.x.y）、パッチ（A.x.y.z）リリースがあります。また、特定の緊急の問題に対処するためのマイナーな更新プログラムであるホットフィックスを提供される場合もあります。

互換性

アップグレードまたは再イメージ化する前に、ターゲットバージョンが展開と互換性があることを確認してください。互換性がないためにアップグレードまたは再イメージ化できない場合は、更新情報について、シスコの担当者またはパートナーにお問い合わせください。

互換性情報については、次を参照してください。

- Cisco Secure Firewall Threat Defense 互換性ガイド
- Cisco Firepower 4100/9300 FXOS の互換性

アップグレードのガイドライン

リリース固有のアップグレードの警告とガイドライン、およびアップグレードの影響を受ける機能とバグの情報については、リリースノートを参照してください。アップグレード中の時間/ディスク容量の要件とシステムの動作に関する一般的な情報については、「トラブルシューティングおよび参考資料 （63 ページ）」を参照してください。

ソフトウェアのアップグレードガイドライン

リリース固有のアップグレードの警告とガイドライン、およびアップグレードに影響する機能とバグについては、Threat Defense のリリースノートを参照してください。現在のバージョンと対象バージョンの間にあるすべてのリリースノートを確認してください：http://www.cisco.com/go/ftd-notes。

Firepower 4100/9300 シャーシのアップグレードガイドライン

ほとんどの場合、各メジャーバージョンで最新のFXOSビルドを使用することを推奨します。リリース固有のFXOSアップグレードの警告とガイドライン、およびアップグレードに影響する機能とバグについては、FXOS のリリースノートを参照してください。現在のバージョンと対象バージョンの間にあるすべてのリリースノートを確認してください。http://www.cisco.com/go/firepower9300-rns。

ファームウェア アップグレードのガイドライン（FXOS 2.13 以前へのアップグレード）については、ファームウェア アップグレード ガイド「Cisco Firepower 4100/9300 FXOS ファームウェア アップグレード ガイド」を参照してください。

アップグレードパス

アップグレードパスの計画は、大規模展開やマルチホップアップグレード、およびシャーシ、ホスティング環境またはその他のアップグレードなどを調整する必要がある状況では特に重要です。

シャーシのアップグレードをともなう Threat Defense のアップグレード

一部のデバイスでは、ソフトウェアをアップグレードする前にシャーシのアップグレード（FXOS およびファームウェア）が必要になる場合があります。

- ：どのアップグレードでもシャーシのアップグレードが必要になる可能性があります。シャーシと Threat Defense は個別にアップグレードしますが、1 つのパッケージにシャーシと Threat Defense のアップグレードが含まれており、Management Center から両方のアップグレードを実行します。互換性作業は自動的に行われます。シャーシのみのアップグレードまたは Threat Defense のみのアップグレードを実行できます。
- Firepower 4100/9300：メジャーバージョンにはシャーシのアップグレードが必要です。

最初にシャーシをアップグレードするため、サポートされているが推奨されていない組み合わせを一時的に実行します。オペレーティングシステムはThreat Defenseの「前」にアップグレードします。シャーシのバージョンがすでにデバイスよりも大幅に新しい場合は、以降のシャーシのアップグレードがブロックされる可能性があります。この場合、3 つ（またはそれ以上）の手順のアップグレードを実行します。つまり、最初にデバイス、次にシャーシ、その後に再びデバイスをアップグレードします。または、完全な再イメージ化を実行します。高可用性またはクラスタ展開では、シャーシを一度に 1 つずつアップグレードします。

サポートされる直接アップグレード

次の表に、Threat Defense ソフトウェアでサポートされている直接アップグレードを示します。メジャーリリースとメンテナンスリリースに直接アップグレードできますが、パッチでは4桁目のみが変更されることに注意してください。以前のメジャーリリースまたはメンテナンスリリースからパッチに直接アップグレードすることはできません。

Firepower 4100/9300 の場合、この表には、関連する FXOS バージョンもリストされています。シャーシのアップグレードが必要な場合、Threat Defense のアップグレードはブロックされます。ほとんどの場合、各バージョンで最新のビルドを推奨します。最小ビルドについては、「Cisco Secure Firewall Threat Defense 互換性ガイド」を参照してください。

表 *1:* メジャーおよびメンテナンスリリースでサポートされる直接アップグレード

現在のバージョン	ターゲット Threat Defense バージョン					
	7.6	**7.4**	**7.3**	**7.2**	**7.1**	**7.0**
	Firepower 4100/9300 FXOS バージョン					
	2.16	**2.14**	**2.13**	**2.12**	**2.11**	**2.10**
7.6	**YES**	—	—	—	—	—
7.4	**YES**	○ †	—	—	—	—
7.3	**YES**	**YES**	**YES**	—	—	—
7.2	**YES**	**YES**	**YES**	**YES**	—	—
7.1	—	—	—	—	—	—
7.0	—	**YES**	**YES**	**YES**	—	**YES**

† Threat Defense をバージョン 7.4.0 にアップグレードすることはできません。バージョン 7.4.0 は、Cisco Secure Firewall 4200 でのみ新規インストールとして使用できます。代わりに、デバイスをバージョン 7.4.1 以降にアップグレードします。

高可用性/クラスタ展開でのシャーシのアップグレードをともなう Threat Defense のアップグレード順序

高可用性またはクラスタ展開でシャーシのアップグレードが必要な場合は、シャーシを一度に 1 つずつアップグレードします。

表 *2 : Firepower 4100/9300* のシャーシのアップグレード順序（*Management Center* を使用）

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

表 *3 :* マルチインスタンスモードでの *Secure Firewall 3100* のシャーシのアップグレード順序（*Management Center* を使用）

Threat Defense の導入	アップグレード順序
スタンドアロン	1. シャーシをアップグレードします。 2. Threat Defense をアップグレードします。
ハイ アベイラビリティ	Threat Defense をアップグレードする前に、両方のシャーシをアップグレードします。 1. シャーシをアップグレードします。シャーシのアップグレードウィザードには、次の 3 つのオプションがあります。 • 並行アップグレード：高可用性の環境では推奨されません。 • シリアルアップグレード：アクティブユニットがダウンしたときに自動的にフェイルオーバーします。アップグレード順序の最初にスタンバイユニットを配置することを推奨します。 • 2 つのワークフロー（アップグレードウィザードを 2 回実行）：スタンバイデバイスを搭載したシャーシをアップグレードし、ロールを切り替えて、新しいスタンバイデバイスを搭載したシャーシをアップグレードします。 2. Threat Defense をアップグレードします。

アップグレードパッケージ

Management Center でのアップグレードパッケージの管理

システム（⚙）> **[Product Upgrades]** でアップグレードパッケージを管理します。

このページには、適用されるすべてのアップグレードパッケージが、特にマークされた推奨リリースとともに一覧表示されます。パッケージを選択してシスコから簡単に直接ダウンロードしたり、手動でダウンロードしたパッケージをアップロードしたりできます（Cisco.com のアップグレードパッケージ （11 ページ））。

表 *4 : Management Center* でのアップグレードパッケージの管理

目的	作業
使用可能なアップグレードパッケージのリストを更新します。	ページの左下にある **[更新（Refresh）]**（ ） をクリックします。
アップグレードパッケージをシスコから Management Center にダウンロードします。	必要なアップグレードパッケージまたはバージョンの横にある [ダウンロード（Download）] をクリックしてダウンロードします。 デバイスの各ファミリには独自のアップグレードパッケージがあるため、展開によっては複数のアップグレードパッケージをダウンロードする必要がある場合があります。
アップグレードパッケージを Management Center に手動でアップロードします。	ページの右下にある [アップグレードパッケージの追加（Add Upgrade Package）] をクリックし、[ファイルの選択（Choose File）] をクリックします。
内部サーバーからアップグレードパッケージを取得するように Threat Defense デバイスを設定します。	ページの右下にある [アップグレードパッケージの追加（Add Upgrade Package）] をクリックし、[リモートロケーションの指定（Specify Remote Location）] をクリックします。 内部サーバーからデバイスへのアップグレードパッケージのコピー（8 ページ） を参照してください。
Management Center からアップグレードパッケージを削除します。	削除するパッケージまたはパッケージバージョンの横にある**省略記号（...）**をクリックし、[削除（Delete）] を選択します。 これにより、Management Center からパッケージ（またはパッケージへのポインタ）が削除されます。すでにパッケージをコピーしたデバイスからは、パッケージは削除されません。 ほとんどの場合、アップグレードすると、アップグレードされたアプライアンスから関連するパッケージが削除されます。ただし、 の場合は、シャーシ アップグレード パッケージを手動で削除する必要があります。Secure Firewall 3100 からのシャーシ アップグレード パッケージの削除 （10 ページ） を参照してください。

デバイスへのアップグレードパッケージのコピー

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。

Threat Defense および Secure Firewall 3100 シャーシ アップグレードパッケージのコピー

Threat Defense および Secure Firewall 3100 シャーシのアップグレードの場合、これを実行する最も簡単な方法は、Management Center の [製品のアップグレード（Product Upgrades）] ページ（**システム**（ ） > **[Product Upgrades]**）を使用して、シスコからアップグレードパッケージ

をダウンロードすることです。その後、アップグレードウィザードにより、パッケージのコピーが求められるようになります。

の場合、シャーシ アップグレード パッケージがアプリケーション インスタンスの外部に保存されることに注意してください。これにより、すべてのインスタンスからThreat Defenseのアップグレードにアクセスできる状態を維持したまま、シャーシをアップグレードできます。ただし、これは、不要なシャーシ アップグレード パッケージを手動で削除する必要がある（アップグレードプロセスで自動的に削除されない）ことを意味します。

次の表に、このオプションとその他のオプションの詳細を示します。

表 *5 : Threat Defense* および *Secure Firewall 3100* シャーシ アップグレード パッケージの管理対象デバイスへのコピー

要件	使用するケース
Cisco → Management Center → デバイス 現在デバイスに適用されるメジャー、メンテナンス、またはパッチアップグレード（ホットフィックスは含まれない）。 Management Center は シスコ サポートおよびダウンロード サイトにアクセスできます。 Management Center に十分なディスク容量。 Management Center とデバイスの間の十分な帯域幅。	すべての要件が満たされている場合は、強く推奨されます。 参照：Management Center でのアップグレードパッケージの管理 （5 ページ）
Cisco → 使用しているコンピュータ → Management Center → デバイス Management Center に十分なディスク容量。 Management Center とデバイスの間の十分な帯域幅。	ディスク容量と帯域幅の要件を満たしているものの、Management Center が シスコ サポートおよびダウンロード サイトにアクセスできないか、ホットフィックスを適用しようとしています。 参照：Cisco.com のアップグレードパッケージ（11 ページ）
Cisco → 使用しているコンピュータ → 内部サーバー → デバイス デバイスがアクセスできる内部 Web サーバー。	（サポートサイトのアクセスやアップグレードタイプに関係なく）ディスク容量の要件や帯域幅の要件を満たしていません。クラウド提供型 Firewall Management Center では特に、デバイス アップグレード パッケージ用のディスク容量が限られています。 参照：内部サーバーからデバイスへのアップグレードパッケージのコピー （8 ページ）

Firepower 4100/9300 シャーシ アップグレード パッケージのコピー

Firepower 4100/9300 シャーシ アップグレード パッケージの場合は、シスコからアップグレードパッケージをダウンロードし、シャーシマネージャ または CLI（FTP、SCP、SFTP、または TFTP）を使用してパッケージをデバイスにコピーします。Cisco.com のアップグレードパッケージ （11 ページ）と、現在の展開のアップグレード手順を参照してください。

内部サーバーからデバイスへのアップグレードパッケージのコピー

Threat Defense のアップグレードパッケージは、Management Center ではなく内部サーバーに保存できます。これは、Management Center 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、Management Center 上の容量も節約できます。

シスコからパッケージを取得してサーバーをセットアップしたら、それらのパッケージへのポインタを設定します。Management Center で、パッケージをアップロードする場合と同様に開始します。[製品のアップグレード（Product Upgrades）] ページ（**システム**（⚙）> **[Product Upgrades]**）で、[アップグレードパッケージの追加（Add Upgrade Package）] をクリックしてください。ただし、コンピュータ上のファイルを選択する代わりに、[リモートロケーションの指定（Specify Remote Location）] をクリックし、適切な詳細情報を入力します。パッケージを取得する時間になると、デバイスは、内部サーバーからパッケージをコピーします。

表 *6 :* 内部サーバーから *Threat Defense* のアップグレードパッケージをコピーするためのオプション

フィールド	説明
URL	プロトコル（HTTP/HTTPS）およびアップグレードパッケージへのフルパスを含む送信元 URL。次に例を示します。 `https://internal_web_server/upgrade_package.sh.REL.tar`
CA 証明書	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）。 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。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。

Threat Defense アップグレードパッケージのデバイス間のコピー

Management Center や内部 Web サーバーから各デバイスにアップグレードパッケージをコピーする代わりに、Threat Defense CLI を使用してデバイス間でアップグレードパッケージをコピーできます（「ピアツーピア同期」）。この安全で信頼性の高いリソース共有は、管理ネットワークを経由しますが、Management Center には依存しません。各デバイスは、5 つのパッケージの同時転送に対応できます。

この機能は、同じ Management Center によって管理されるバージョン 7.2 以降のスタンドアロンデバイスでサポートされています。次の場合はサポートされていません。

- コンテナインスタンス。
- デバイスの高可用性ペアとクラスタ。これらのデバイスは通常の同期プロセスの一部として、相互にパッケージを取得します。アップグレードパッケージを 1 つのグループメンバーにコピーすると、自動的にすべてのグループメンバーと同期されます。
- 分析モードでオンプレミス Management Center に追加されたデバイス。
- NAT ゲートウェイによって分離されたデバイス。
- バージョン 7.0.x からアップグレードするデバイス。

アップグレードパッケージが必要なすべてのデバイスに対して、次の手順を繰り返します。

Before you begin

- Threat Defense アップグレードパッケージを Management Center または内部 サーバーにアップロードします。
- アップグレードパッケージを 1 つ以上のデバイスにコピーします。

Procedure

ステップ 1 管理者アカウントでアップグレードパッケージが必要なデバイスに SSH 接続します。

ステップ 2 機能を有効にします。

configure p2psync enable

ステップ 3 まだはっきりしない場合は、必要なアップグレードパッケージをどこで入手できるかを確認してください。

show peers：この機能も有効になっている他の適格なデバイスを一覧表示します。

show peer details *ip_address*：指定した IP アドレスのデバイスについて、利用可能なアップグレードパッケージとそのパスを一覧表示します。

ステップ 4 検出した IP アドレスとパスを指定して、必要なパッケージが存在するデバイスからパッケージをコピーします。

sync-from-peer *ip_address package_path*

パッケージのコピー実行を確定すると、パッケージ転送を監視するために使用できる同期ステータス UUID がシステムに表示されます。

ステップ 5 CLI から転送ステータスをモニタリングします。

show p2p-sync-status：このデバイスへの過去 5 回の転送についての同期ステータスを表示します。これには、完了した転送と失敗した転送も含まれます。

show p2p-sync-status *sync_status_UUID*：このデバイスを対象とした特定の転送の同期ステータスを表示します。

Secure Firewall 3100 からのシャーシ アップグレード パッケージの削除

の場合、シャーシ アップグレード パッケージはアプリケーション インスタンスの外部に保存されます。これにより、すべてのインスタンスから Threat Defense のアップグレードにアクセスできる状態を維持したまま、シャーシをアップグレードできます。ただし、これは、不要なシャーシ アップグレード パッケージを手動で削除する必要がある（アップグレードプロセスで自動的に削除されない）ことを意味します。

Note 不要なシャーシ アップグレード パッケージは、シャーシ アップグレード ワークフローのコンテキストで削除する必要があります。これを行う最適なタイミングは、次のバージョンにアップグレードするときです。

シャーシをアクティブにアップグレードしていないときにシャーシ アップグレード パッケージを削除するには、この手順を使用します。

Before you begin

削除するパッケージに対応するもの以外に少なくとも 1 つのシャーシアップグレードパッケージをダウンロード（またはポインタを設定）します。

Procedure

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 不要なパッケージがあるシャーシを選択し、[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）] で、[FXOS とファームウェアのアップグレード（シャーシのみ）（Upgrade FXOS and Firmware (Chassis Only)）] を選択します。

シャーシ アップグレード ウィザードが表示されます。

ステップ 3 [アップグレード先（Upgrade to）] メニューからターゲットバージョンを選択します。

削除するパッケージに対応するバージョン以外のバージョンを選択してください。このバージョンにはアップグレードしないため、どれを選択しても問題ありません。

ステップ 4 [デバイスの選択（Device Selection）] ペインで、「`X devices have packages that might not be needed`」（不要である可能性のあるパッケージが X デバイスにあります）というメッセージをクリックします。

不要なパッケージがあるシャーシが [デバイスの詳細（Device Details）] ペインに一覧表示されます。シャーシが現在実行しているバージョン用のパッケージや、選択した「ターゲットバージョン」用のパッケージ

は削除できないことに注意してください。これら以外のパッケージが搭載されたシャーシのみがカウントされます。

ステップ 5 [デバイスの詳細（Device Details）] ペインでシャーシを選択し、[デバイスのアップグレードパッケージの管理（Manage Upgrade Packages on Device）] をクリックし、削除するパッケージを選択して [削除（Remove）] をクリックします。

クリーンアップするシャーシごとにこの手順を繰り返してください。

ステップ 6 シャーシアップグレードウィザードに戻り、[リセット（Reset）] をクリックしてワークフローをリセットします。

Cisco.com のアップグレードパッケージ

システムが シスコ サポートおよびダウンロード サイト にアクセスできない場合、またはホットフィックスなどの別の理由で直接ダウンロードできない場合は、シスコからアップグレードパッケージを手動でダウンロードします。内部サーバーから取得するようにデバイスを設定する場合も、アップグレードパッケージを手動で取得する必要があります。また、Firepower 4100/9300 のシャーシ アップグレード パッケージは手動で取得する必要があります。

パッケージは、シスコ サポートおよびダウンロード サイト：https://www.cisco.com/go/ftd-software で入手できます。

Threat Defense パッケージ

ファミリまたはシリーズのすべてのモデルに同じアップグレードパッケージを使用します。適切なソフトウェアを見つけるには、使用しているモデルをシスコ サポートおよびダウンロード サイトで選択または検索し、適切なバージョンのソフトウェアのダウンロードページを参照します。使用可能なアップグレードパッケージは、インストールパッケージ、ホットフィックス、およびその他の該当するダウンロードとともに表示されます。アップグレードパッケージのファイル名には、プラットフォーム、、ソフトウェアバージョン、およびビルドが反映されています。アップグレードパッケージは署名されており、ファイル名の最後は .sh.REL.tar です。解凍したり、名前を変更したりしないでください。

表 7: アップグレードパッケージ

プラットフォーム	パッケージ	注記
Threat Defense パッケージ		
Firepower 1000	Cisco_FTD_SSP-FP1K_Upgrade-*Version-build*.sh.REL.tar	—
Firepower 2100	Cisco_FTD_SSP-FP2K_Upgrade-*Version-build*.sh.REL.tar	過去のバージョン7.4.x はアップグレードできません。

プラットフォーム	パッケージ	注記
Cisco Secure Firewall 3100	Cisco_FTD_SSP-FP3K_Upgrade-*Version-build*.sh.REL.tar	—
Cisco Secure Firewall 4200	Cisco_Secure_FW_TD_4200-*Version-build*.sh.REL.tar	—
Firepower 4100/9300	Cisco_FTD_SSP_Upgrade-*Version-build*.sh.REL.tar	—
ASA 5500-X	Cisco_FTD_Upgrade-*Version-build*.sh.REL.tar	過去のバージョン7.0.xはアップグレードできません。
Threat Defense Virtual	Cisco_FTD_Upgrade-*Version-build*.sh.REL.tar	—
FTD を使用した ISA 3000	Cisco_FTD_Upgrade-*Version-build*.sh.REL.tar	—

Secure Firewall 3100 のシャーシパッケージ

の場合、脅威防御とシャーシのアップグレードはパッケージを共有します。

Firepower 4100/9300 用シャーシパッケージ

正しい FXOS パッケージを見つけるには、デバイスモデルを選択または検索し、対象の FXOS バージョンとビルドの *Firepower Extensible Operating System* のダウンロードページを参照します。FXOSパッケージは、リカバリパッケージおよびMIBパッケージとともにリストされています。ファームウェアは、FXOS 2.14.1 以降へのアップグレードに含まれています。

表 *8 : FXOS* パッケージ

プラットフォーム	パッケージ
Firepower 4100/9300	fxos-k9.*fxos_version*.SPA

ファームウェアは、FXOS 2.14.1 以降へのアップグレードに含まれています（Threat Defense 7.4.1 への対応）。古いデバイスをアップグレードする場合は、デバイスモデルを選択または検索し、*Firepower Extensible Operating System* のダウンロードページを参照します。ファームウェアパッケージは、[すべてのリリース（All Releases）] > [ファームウェア（Firmware）] にあります。

表 *9 :* ファームウェアパッケージ

プラットフォーム	パッケージ
Firepower 4100	fxos-k9-fpr4k-firmware.*firmware_version*.SPA
Firepower 9300	fxos-k9-fpr9k-firmware.*firmware_version*.SPA

アップグレードの準備状況

インフラストラクチャとネットワークの確認

アプライアンス アクセス

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

帯域幅

管理ネットワークに大量のデータ転送を実行するための帯域幅があることを確認します。可能な場合は常に、アップグレードパッケージを事前にアップロードしてください。アップグレード時にアップグレードパケージをデバイスに転送する際の帯域幅が不十分な場合、アップグレード時間が長くなったり、アップグレードがタイムアウトしたりする可能性があります。『Guidelines for Downloading Data from the Firepower Management Center to Managed Devices』（トラブルシューティング テクニカルノーツ）を参照してください。

設定と展開の確認

設定

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。変更管理ワークフローを決定します。設定変更を展開します。アップグレード後に再度展開する必要があり、通常は Snort が再起動されることに注意してください。「設定展開時のトラフィックフローとインスペクション （70 ページ）」を参照してください。

展開の正常性

正常に展開され、通信が確立されていることを確認します。正常性モニターによって報告された問題がある場合は、続行する前にそれらを解決します。特に、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する必要があります。時刻のずれが 10 秒を超えている場合、ヘルスモニターからアラートが発行されますが、手動で確認する必要もあります。同期されていないと、アップグレードが失敗する可能性があります。時刻を確認するには、**show time** CLI コマンドを使用します。

バックアップ

ホットフィックスを除き、アップグレードはシステムに保存されているすべてのバックアップを削除します。アップグレードの前後に、安全な遠隔地にバックアップし、正常に転送が行われることを確認することを強くお勧めします。

- アップグレード前：アップグレードが致命的な失敗であった場合は、再イメージ化を実行し、復元する必要がある場合があります。再イメージ化によって、システムパスワードを含むほとんどの設定が工場出荷時の初期状態に戻ります。最近のバックアップがある場合は、通常の操作にすばやく戻ることができます。
- アップグレード後：これにより、新しくアップグレードされた展開のスナップショットが作成されます。

表 *10*：バックアップ

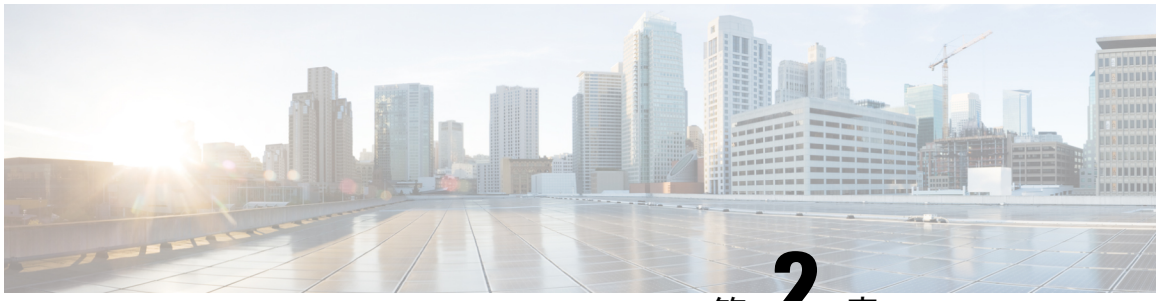
バックアップ	ガイド
Threat Defense	Cisco Defense Orchestrator のクラウド提供型 Firewall Management Center を使用した Firewall Threat Defense の管理：「Backup/Restore」 バックアップは、パブリッククラウドの Threat Defense Virtual など、すべてのケースでサポートされているわけではないことに注意してください。ただし、バックアップできる場合は、バックアップする必要があります。
Secure Firewall 3100 シャーシ	Cisco Defense Orchestrator のクラウド提供型 Firewall Management Center を使用した Firewall Threat Defense の管理：*Secure Firewall 3100* のマルチインスタンスモード
Firepower 4100/9300 シャーシ	『Cisco Firepower 4100/9300 FXOS Configuration Guide』：「*Configuration Import/Export*」
Firepower 9300 シャーシ上の ASA	『Cisco ASA Series General Operations Configuration Guide』：「Software and Configurations」 Threat Defense および ASA 論理デバイスを持つ Firepower 9300 の場合は、ASDM または ASA CLI を使用して、ASA 構成やその他の重要なファイルをバックアップしてください（特に ASA 構成の移行がある場合）。

ソフトウェアアップグレード準備状況チェック

ユーザーが自分で実行するチェックに加えて、システムも、独自のアップグレード準備状況チェックを実行できます。Threat Defense アップグレードウィザードでは、適切なタイミングでチェックを実行するように求められます。準備状況チェックは無効にできますが、推奨されません。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。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。

準備状況チェックは、メンテナンスウィンドウ外に実行できます。準備状況チェックの実行に必要な時間は、モデルとデータベースのサイズによって異なります。準備状況チェックを行っている間は、手動で再起動またはシャットダウンしないでください。



第 2 章

Threat Defense のアップグレード

Threat Defense のアップグレード

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

アップグレードウィザードから移動しても進行状況は保持されます。他のユーザーは、すでに選択されているデバイスの新しいアップグレードワークフローを開始できません。（例外：CAC でログインしている場合、ログアウトしてから 24 時間後に進行状況がクリアされます）。ワークフローに戻るには、**[デバイス（Devices）] > [Threat Defense のアップグレード（Threat Defense Upgrade）]**を選択します。

アップグレードは、アップグレードウィザードを完了して [アップグレードの開始（Start Upgrade）] をクリックするまで開始されません。アップグレードパッケージのダウンロード、それらのデバイスへのコピー、準備状況チェックの実行、アップグレードオプションの選択など、その時点までのすべての手順は、メンテナンスウィンドウ外で実行できます。アップグレード中およびアップグレード後の最初の展開時におけるトラフィック処理については（通常は Snort が再起動されます）、トラフィック フローとインスペクション, on page 67を参照してください。

⚠

Caution アップグレード中は、設定の変更を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。アップグレード中にデバイスが複数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。アップグレードに失敗する、デバイ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 無応答および失敗した Threat Defense のアップグレード, on page 65 を参照してください。

Before you begin

アップグレードの準備が整っていることを確認します。

- ターゲットバージョンを実行できるかどうかを確認します：互換性, on page 1
- アップグレードパスを計画します：アップグレードパス, on page 2
- アップグレードのガイドラインを確認します：アップグレードのガイドライン, on page 1
- インフラストラクチャとネットワークを確認します：インフラストラクチャとネットワークの確認, on page 13
- 設定、タスク、および展開全体の正常性を確認します：設定と展開の確認, on page 13
- バックアップを実行します：バックアップ, on page 14
- 必要に応じてシャーシをアップグレードします：Secure Firewall 3100 または Firepower 4100/9300 シャーシのアップグレード, on page 25

Procedure

ステップ 1 Management Center で、**システム**（⚙）> **[Product Upgrades]** を選択します。

[製品のアップグレード（Product Upgrades）] ページには、アップグレードを中心とした展開の概要（デバイスの数、それらが最後にアップグレードされた日時、進行中のアップグレードの有無など）が表示されます。

ステップ 2 デバイス アップグレード パッケージを Management Center に取得します。

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する前に、パッケージを Management Center またはデバイスがアクセスできる内部サーバーにアップロードする必要があります。

[製品のアップグレード（Product Upgrades）]ページには、現在の展開に適用されるすべてのアップグレードパッケージが、特にマークされた推奨リリースとともに一覧表示されます。ほとんどの場合、必要なアップグレードパッケージまたはバージョンの横にある [ダウンロード（Download）] をクリックするだけで取得できます。

詳細については、Management Center でのアップグレードパッケージの管理, on page 5およびアップグレードパッケージのトラブルシューティング, on page 63を参照してください。

ステップ 3 アップグレードウィザードを起動します。

ターゲットバージョンの横にある [アップグレード（Upgrade）] をクリックします。ドロップダウンメニューが表示されたら、[Threat Defense] を選択します。

Threat Defense アップグレードウィザードが表示されます。これには、左側の [デバイスの選択（Device Selection）] と右側の [デバイスの詳細（Device Details）] の 2 つのペインがあります。[デバイスの選択（Device Selection）] ペインでデバイスリンク（「`4 つのデバイス（4 devices）`」 など）をクリックして、[デバイスの詳細（Device Details）] を表示します。ターゲットバージョンは、[アップグレード先

（Upgrade to）] メニューで事前に選択されています。システムは、どのデバイスをそのバージョンにアップグレードできるかを判断し、[デバイスの詳細（Device Details）] ペインに表示します。

ステップ 4 アップグレードするデバイスを選択します。

[デバイスの詳細（Device Details）] ペインで、アップグレードするデバイスを選択し、[選択に追加（Add to Selection）] をクリックします。

[デバイスの選択（Device Selection）] ペインのデバイスリンクを使用すると、選択したデバイス、残りのアップグレード候補、不適格なデバイス（理由付き）、アップグレードパッケージが必要なデバイスなどの間で [デバイスの詳細（Device Details）] ペインを切り替えることができます。選択からデバイスを削除したり、[リセット（Reset）] をクリックしてデバイスの選択をクリアし、最初からやり直すことができます。不適格なデバイスを削除する必要はありません。それらはアップグレードから自動的に除外されます。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。

Tip
アップグレードするデバイスを選択したら、無人モード（**[無人モード（Unattended Mode）]** > **[開始（Start）]**）でアップグレードを開始できます。いくつかのオプションを指定すると、システムは自動的に必要なアップグレードパッケージをデバイスにコピーし、互換性チェックと準備状況チェックを実行してアップグレードを開始します。アップグレードが完了したら、検証とアップグレード後のタスクを開始します。詳細については、「無人モードでの Threat Defense のアップグレード, on page 23」を参照してください。

ステップ 5 アップグレードパッケージをデバイスにコピーします。

[アップグレードパッケージのコピー（Copy Upgrade Package）] をクリックし、転送が完了するまで待ちます。 の場合、シャーシをアップグレードしていると、アップグレードパッケージは、通常、すでにデバイス上に存在しています（削除していない場合）。

ステップ 6 [次へ（Next）] をクリックして互換性および準備状況チェックを実行します。

互換性やその他のクイック事前チェックは自動的に実行されます。たとえば、設定を展開する必要がある場合、すぐにアラートが表示されます。他のチェックには、より長い時間がかかります。これらを開始するには、[準備状況チェックの実行（Run Readiness Check）] をクリックします。

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。[互換性と準備状況のチェックに合格することを必須にする（Require passing compatibility and readiness checks option）] オプションを無効にするとチェックをスキップできますが、推奨しません。すべてのチェックに合格すると、アップグレードが失敗する可能性が大幅に減少します。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。

ステップ 7 [次へ（Next）] をクリックしてアップグレードオプションを選択します。

これらのオプションを使用すると、成功したアップグレードと失敗したアップグレードの両方から元に戻し、トラブルシューティングファイルを生成し、Snort をアップグレードすることができます。これらのオプションを無効にできる理由については、Threat Defense のアップグレードオプション, on page 21を参照してください。

ステップ 8 アップグレードの準備ができていることを再確認します。

以前に実行した設定と展開の正常性チェックを再確認することをお勧めします（設定と展開の確認, on page 13）。

ステップ 9 [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。

ウィザードにアップグレードの全体的な進行状況が表示されます。メッセージセンターでもアップグレードの進行状況をモニターできます。詳細なステータスについては、確認するデバイスの横にある **[詳細の表示（View Details）][詳細ステータス（Detailed Status）]** をクリックしてください。この詳細なステータスは、[デバイス管理（Device Management）] ページの [アップグレード（Upgrade）] タブでも確認できます。

高可用性デバイスの場合、[アップグレードの開始（Start Upgrade）] をクリックすると、メッセージセンターとアップグレードウィザードによってユニットが高可用性状態と関連付けられることに注意してください。つまり、フェールオーバーが発生し、スタンバイのみをアップグレードしている場合でも、「スタンバイ」、次に「アクティブ」のアップグレードがレポートされます。[デバイス管理（Device Management）] ページには、ユニットの現在の正しい高可用性状態が常に表示されます。この状態は、メッセージセンターまたはウィザードで表示される元の状態とは異なる場合があります。

Caution
高可用性デバイスの場合、メッセージセンターは、個別のタスクで各ユニットのアップグレードの成功を報告します。メッセージセンターの表示に関係なく、両方のデバイスのアップグレードが完了するまで、高可用性ペアに設定を再展開しないでください。

Tip
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キャンセルする必要がある場合や、失敗したアップグレードを再試行する必要がある場合は、詳細なステータスのポップアップから実行します。ワークフローをクリアしていない場合は、ウィザードに戻って詳細なステータスを表示できます。クリア済みの場合は、[デバイス管理（Device Management）] ページの [アップグレード（Upgrade）] タブを使用してください。Threat Defense CLI を使用することもできます。

ステップ 10 成功したことを確認します。

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

ステップ 11 （オプション）高可用性展開またはクラスタ化された展開では、デバイスのロールを調べます。

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

ステップ 12 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。

アップグレードによってこれらのコンポーネントが更新されることがよくありますが、より新しいコンポーネントが利用できる可能性があります。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 13 アップグレード後に必要な構成変更があれば、実行します。

ステップ 14 アップグレードしたデバイスに構成を再度展開します。

展開する前に、アップグレードによって加えられた変更（およびアップグレード後に加えた変更）を確認できます。

- ワークフローをクリアしていない場合は、ウィザードに戻ることができます。**[デバイス（Devices）]**>**[Threat Defense のアップグレード（Threat Defense Upgrade）]** を選択し、各デバイスの横にある [構成変更（Configuration Changes）] をクリックします。
- ワークフローをクリアした場合、または複数のデバイスの変更レポートをすばやく生成する場合は、[高度な展開（Advanced Deploy）] ページを使用します。**[展開（Deploy）]**>**[高度な展開（Advanced Deploy）]**を選択し、アップグレードしたデバイスを選択して、[保留中の変更レポート（Pending Changes Reports）] をクリックします。レポートの生成が完了したら、メッセージセンターの [タスク（Tasks）] タブからレポートをダウンロードできます。

What to do next

- （オプション）[アップグレード情報のクリア（Clear Upgrade Information）] をクリックして、ウィザードをクリアします。これを行うまで、ページには、実行したばかりのアップグレードに関する詳細が引き続き表示されます。ウィザードをクリアしたら、[デバイス管理（Device Management）] ページの [アップグレード（Upgrade）] タブを使用して、管理対象デバイスに関する最後のアップグレードの情報を確認し、[高度な展開（Advanced Deploy）] 画面で設定の変更を確認します。
- 再度バックアップします：バックアップ, on page 14

Threat Defense のアップグレードオプション

表 *11 : Threat Defense* のアップグレードオプション

オプション	無効にする場合	詳細
互換性と準備状況のチェックに合格する必要があります。	Cisco TAC の指示があった場合。	このオプションを無効にすると、互換性と準備状況のチェックに合格せずにアップグレードを開始できます。ただし、推奨されません。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。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。
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。	失敗したアップグレードを手動で（自動ではなく）キャンセルし、再試行する場合。	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。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。

オプション	無効にする場合	詳細
アップグレードを開始する前にトラブルシューティング ファイルを生成します。	時間とディスク容量を節約する場合。	バージョン 7.3 以降へのアップグレードでは、アップグレード前のトラブルシューティング ファイルの自動生成をスキップできます。 脅威防御デバイスのトラブルシューティング ファイルを手動で生成するには、**システム**（⚙）>**[正常性（Health）]**>**[モニタ（Monitor）]** を選択し、左側のパネルでデバイスをクリックし、[システムおよびトラブルシューティングの詳細を表示（View System & Troubleshoot Details）]、[トラブルシューティング ファイルの生成（Generate Troubleshooting Files）] をクリックします。
Snort 2 を Snort 3 にアップグレードします。	Snort 3 のアップグレードを防ぐ場合。	バージョン 7.2 ～ 7.6 へのアップグレードでは、設定を展開すると、対象のデバイスが Snort 2 から Snort 3 にアップグレードされます。 バージョン 7.3 以降へのアップグレードでは、このオプションを無効にすることはできません。個々のデバイスを元に戻すことはできますが、Snort 2 は将来のリリースで非推奨になるため、今すぐ使用を停止することを強く推奨します。 カスタム侵入ポリシーやネットワーク分析ポリシーを使用しているためにデバイスがアップグレード対象外になる場合は、手動で Snort 3 にアップグレードすることを強く推奨します。移行のサポートについては、お使いのバージョンの Cisco Secure Firewall Management Center Snort 3 Configuration Guide を参照してください。
アップグレード成功後の復元を可能にします。	時間とディスク容量を節約する場合。	7.1 以降へのアップグレードでは、Threat Defense のアップグレードを元に戻す期間が 30 日間あります。 復元すると、ソフトウェアは、最後のアップグレードの直前の状態に戻ります（スナップショットとも呼ばれます）。パッチのインストール後にアップグレードを元に戻すと、パッチだけでなくアップグレードも元に戻されます。 コンテナインスタンス、パッチ、またはホットフィックスではサポートされていません。

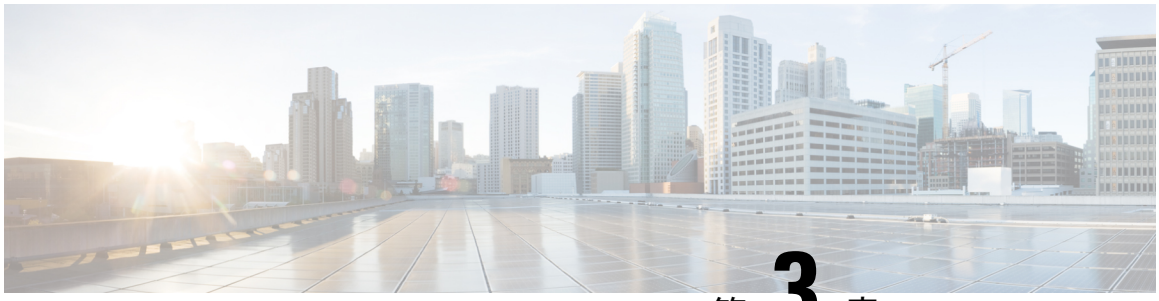
無人モードでの Threat Defense のアップグレード

Threat Defense アップグレードウィザードには、オプションの無人モードがあります。アップグレードするターゲットバージョンとデバイスを選択し、いくつかのアップグレードオプションを指定して、その場から離れるだけです。ログアウトしたり、ブラウザを閉じたりすることもできます。

無人アップグレードを使用すると、システムは自動的に必要なアップグレードパッケージをデバイスにコピーし、互換性チェックと準備状況チェックを実行してアップグレードを開始します。ウィザードを手動でステップ実行する場合と同様に、アップグレードのステージに「合格」しなかったデバイス（たとえば、チェックの失敗）は、次のステージに含まれません。アップグレードが完了したら、検証とアップグレード後のタスクを開始します。

表 *12*：

目的	操作手順
無人アップグレードを開始します。	Threat Defense アップグレードウィザードで、アップグレードするターゲットバージョンとデバイスを選択します。**[無人モード（Unattended Mode）] > [開始（Start）]** を選択し、アップグレードオプションを選択して、もう一度 [開始（Start）] をクリックします。
コピーフェーズとチェックフェーズの間に無人アップグレードを一時停止します。	Threat Defense アップグレードウィザードで、**[無人モード（Unattended Mode）] > [停止（Stop）]** を選択します。 コピーフェーズとチェックフェーズの間に無人モードを一時停止して再開できます。ただし、無人モードを一時停止しても、進行中のタスクは停止しません。開始されたコピーとチェックは完了するまで実行されます。手動アップグレードアクションを実行するには、無人モードを一時停止する必要があります。 実際のデバイスのアップグレードが開始されると、無人モードを停止してキャンセルすることはできません。代わりに、[デバイス管理（Device Management）] ページの [アップグレード（Upgrade）] タブ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。
無人アップグレードをモニターします。	無人アップグレードをモニターする方法は、次のとおりです。 • コピーおよび確認ステータス：**[無人モード（Unattended Mode）] > [ステータスの表示（View Status）]** • 全体的なアップグレードステータス：メッセージセンター • 詳細なアップグレードステータス：[デバイス管理（Device Management）] ページの [アップグレード（Upgrade）] タブ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



第 3 章

Secure Firewall 3100 または Firepower 4100/9300 シャーシのアップグレード

一部のデバイスでは、ソフトウェアをアップグレードする前にシャーシのアップグレード（FXOS およびファームウェア）が必要になる場合があります。

- ：どのアップグレードでもシャーシのアップグレードが必要になる可能性があります。シャーシと Threat Defense は個別にアップグレードしますが、1 つのパッケージにシャーシと Threat Defense のアップグレードが含まれており、Management Center から両方のアップグレードを実行します。互換性作業は自動的に行われます。シャーシのみのアップグレードまたは Threat Defense のみのアップグレードを実行できます。
- Firepower 4100/9300：メジャーバージョンにはシャーシのアップグレードが必要です。

最初にシャーシをアップグレードするため、サポートされているが推奨されていない組み合わせを一時的に実行します。オペレーティングシステムはThreat Defenseの「前」にアップグレードします。シャーシのバージョンがすでにデバイスよりも大幅に新しい場合は、以降のシャーシのアップグレードがブロックされる可能性があります。この場合、3 つ（またはそれ以上）の手順のアップグレードを実行します。つまり、最初にデバイス、次にシャーシ、その後に再びデバイスをアップグレードします。または、完全な再イメージ化を実行します。高可用性またはクラスタ展開では、シャーシを一度に 1 つずつアップグレードします。

- Secure Firewall 3100 シャーシのアップグレード, on page 25
- Chassis Manager を使用した Firepower 4100/9300 上の FXOS のアップグレード （29 ページ）
- CLI を使用した Firepower 4100/9300 上の FXOS のアップグレード （38 ページ）
- Firepower 4100/9300 のファームウェアのアップグレード （50 ページ）

Secure Firewall 3100 シャーシのアップグレード

上のシャーシをアップグレードするには、この手順を使用します。

続行すると、シャーシアップグレードウィザードに、選択したシャーシ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。あるシャーシがウィザードの1つの段階に「合格」しない場合、そのデバイスは次の段階には表示されません。

ウィザードから移動しても進行状況は保持されます。他のユーザーは、すでに選択されているシャーシの新しいアップグレードワークフローを開始できません（例外：CAC でログインしている場合、ログアウトしてから 24 時間後に進行状況がクリアされます）。ワークフローに戻るには、**[デバイス（Devices）]** > **[シャーシのアップグレード（Chassis Upgrade）]**を選択します。

シャーシのアップグレードは、ウィザードを完了して[アップグレードの開始（Start Upgrade）]をクリックするまで開始されません。アップグレードパッケージのダウンロード、それらのシャーシへのコピー、アップグレードオプションの選択など、その時点までのすべての手順は、メンテナンスウィンドウ外で実行できます。アップグレード時におけるトラフィック処理については、シャーシのアップグレードでのトラフィックフローとインスペクション, on page 69を参照してください。

Caution アップグレード中は、設定変更を行ったり、それらをシャーシまたは Threat Defense インスタンスに展開したりしないでください。システムが非アクティブに見えても、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。アップグレード中にシャーシが複数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。アップグレードに失敗する、シャーシが応答しないなど、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。

Before you begin

アップグレードの準備が整っていることを確認します。

- ターゲットバージョンを実行できるかどうかを確認します：互換性, on page 1
- アップグレードパスを計画します：アップグレードパス, on page 2
- アップグレードのガイドラインを確認します：アップグレードのガイドライン, on page 1
- インフラストラクチャとネットワークを確認します：インフラストラクチャとネットワークの確認, on page 13
- 設定、タスク、および展開全体の正常性を確認します：設定と展開の確認, on page 13
- バックアップを実行します：バックアップ, on page 14

Procedure

ステップ 1 Management Center で、**システム**（⚙）> **[Product Upgrades]** を選択します。

[製品のアップグレード（Product Upgrades）] ページには、アップグレードを中心とした展開の概要（デバイスの数、それらが最後にアップグレードされた日時、進行中のアップグレードの有無など）が表示されます。

ステップ 2 Management Center にシャーシ アップグレード パッケージを取得します。

アップグレードパッケージを管理対象シャーシにコピーする前に、パッケージを Management Center（またはシャーシがアクセスできる内部サーバー）にアップロードする必要があります。[製品のアップグレード（Product Upgrades）] ページには、現在の展開に適用されるすべてのアップグレードパッケージが、特にマークされた推奨リリースとともに一覧表示されます。ほとんどの場合、必要なアップグレードパッケージまたはバージョンの横にある [ダウンロード（Download）] をクリックするだけで取得できます。シャーシと Threat Defense ソフトウェアのアップグレードには同じパッケージを使用することに注意してください。

詳細については、Management Center でのアップグレードパッケージの管理, on page 5およびアップグレードパッケージのトラブルシューティング, on page 63を参照してください。

ステップ 3 アップグレードウィザードを起動します。

ターゲットバージョンの横にある [アップグレード（Upgrade）] をクリックします。ドロップダウンメニューが表示されたら、[シャーシ（Chassis）] を選択します。

シャーシ アップグレード ウィザードが表示されます。これには、左側の [デバイスの選択（Device Selection）] と右側の [デバイスの詳細（Device Details）] の 2 つのペインがあります。[デバイスの選択（Device Selection）] ペインでデバイスリンク（「`4 つのデバイス（4 devices）`」 など）をクリックして、それらのシャーシの [デバイスの詳細（Device Details）] を表示します。ターゲットバージョンは、[アップグレード先（Upgrade to）] メニューで事前に選択されています。システムは、どのシャーシをそのバージョンにアップグレードできるかを判断し、[デバイスの詳細（Device Details）] ペインに表示します。[デバイスの選択（Device Selection）] ペインには、アップグレードパッケージに含まれる FXOS とファームウェアのバージョンも表示されます。

ステップ 4 アップグレードするシャーシを選択します。

[デバイスの詳細（Device Details）] ペインで、アップグレードするシャーシを選択し、[選択に追加（Add to Selection）] をクリックします。

[デバイスの選択（Device Selection）] ペインのデバイスリンクを使用すると、選択したシャーシ、残りのアップグレード候補、不適格なシャーシ（理由付き）、アップグレードパッケージが必要なシャーシなどの間で [デバイスの詳細（Device Details）] ペインを切り替えることができます。選択のシャーシを追加/削除したり、[リセット（Reset）] をクリックしてシャーシの選択をクリアし、最初からやり直すことができます。不適格なシャーシを削除する必要はありません。それらはアップグレードから自動的に除外されます。

ステップ 5 （オプション）選択したシャーシから不要なアップグレードパッケージを削除します。

シャーシアップグレードパッケージは手動で管理する必要があります。この時点がクリーンアップの最適なタイミングです。

a) [デバイスの選択（Device Selection）] ペインで、「`X devices have packages that might not be needed`」（不要である可能性のあるパッケージがXデバイスにあります）というメッセージをクリックします。

b) [デバイスの詳細（Device Details）]ペインでシャーシを選択し、[デバイスのアップグレードパッケージの管理（Manage Upgrade Packages on Device）] をクリックし、削除するパッケージを選択して [削除（Remove）] をクリックします。

クリーンアップするシャーシごとにこの手順を繰り返してください。

ステップ 6 新しいアップグレードパッケージをシャーシにコピーします。

[アップグレードパッケージのコピー（Copy Upgrade Package）] をクリックし、転送が完了するまで待ちます。

ステップ 7 [次へ（Next）] をクリックしてアップグレードオプションを選択します。

デフォルトでは、シャーシのアップグレードは並行して実行されます。

高可用性インスタンスを持つシャーシの場合は、シリアルアップグレード順序をお勧めします。[デバイスの詳細（Device Details）] ペインで適切なシャーシを選択し、[シリアルアップグレードに移行（Move to Serial Upgrade）]をクリックします。アップグレード順序の最初にスタンバイユニットを持つシャーシを配置することもお勧めします。シリアルアップグレード順序を変更するには、[アップグレード順序の変更（Change Upgrade Order）]をクリックします。詳細については、「高可用性/クラスタ展開でのシャーシのアップグレードをともなう Threat Defense のアップグレード順序, on page 4」を参照してください。

ステップ 8 アップグレードの準備ができていることを再確認します。

以前に実行した設定と展開の正常性チェックを再確認することをお勧めします（設定と展開の確認, on page 13）。

ステップ 9 [アップグレードの開始（Start Upgrade）]をクリックし、アップグレードして、シャーシを再起動することを確認します。

ウィザードにアップグレードの全体的な進行状況が表示されます。メッセージセンターでもアップグレードの進行状況をモニターできます。詳細なステータスについては、確認するシャーシの横にある **[詳細の表示（View Details）][詳細ステータス（Detailed Status）]** をクリックしてください。この詳細なステータスは、[デバイス管理（Device Management）] ページの [アップグレード（Upgrade）] タブでも確認できます。

ステップ 10 成功したことを確認します。

アップグレードが完了したら、**[デバイス（Devices）] > [デバイス管理（Device Management）]** を選択し、アップグレードしたシャーシのシャーシバージョンが正しいことを確認します。

ステップ 11 （任意）設定の変更を確認します。

Threat Defense をアップグレードする前に、シャーシのアップグレードによって行われた変更を確認することをお勧めします。

- ワークフローをクリアしていない場合は、ウィザードに戻ることができます。**[デバイス（Devices）]> [シャーシのアップグレード（Chassis Upgrade）]** を選択し、各シャーシの横にある [構成変更（Configuration Changes）] をクリックします。
- ワークフローをクリアした場合、または複数のシャーシの変更レポートをすばやく生成する場合は、[高度な展開（Advanced Deploy）] ページを使用します。**[展開（Deploy）] > [高度な展開（Advanced**

Deploy）]を選択し、アップグレードしたシャーシを選択して、[保留中の変更レポート（Pending Changes Reports）] をクリックします。レポートの生成が完了したら、メッセージセンターの [タスク（Tasks）] タブからレポートをダウンロードできます。

ステップ 12 （オプション）高可用性展開では、デバイスのロールを調べます。

アップグレードの実行方法によっては、高可用性インスタンスのロールが切り替わる場合があります。後続の Threat Defense のアップグレードでもデバイスロールが切り替わることに注意し、必要な変更を加えてください。

What to do next

- （オプション）[アップグレード情報のクリア（Clear Upgrade Information）] をクリックして、ウィザードをクリアします。これを行うまで、ページには、実行したばかりのアップグレードに関する詳細が引き続き表示されます。ウィザードをクリアしたら、[デバイス管理（Device Management）] ページの [アップグレード（Upgrade）] タブを使用して、シャーシに関する最後のアップグレードの情報を確認し、[高度な展開（Advanced Deploy）] 画面で設定の変更を確認します。
- 再度バックアップします：バックアップ, on page 14

Chassis Manager を使用した Firepower 4100/9300 上の FXOS のアップグレード

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

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

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

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

Before you begin

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。

Procedure

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。

Note
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。

Example:

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

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

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

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

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

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

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

Before you begin

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。

Procedure

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。

Important
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。

Note
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。

Example:

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

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

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

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

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

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

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

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

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

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

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

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

Before you begin

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。

Procedure

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。

Note
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。

Example:

```
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。

Note
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。

Example:

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

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

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

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

a) **top** を入力します。
b) **scope ssa** を入力します。

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

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

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

CLI を使用した Firepower 4100/9300 上の FXOS のアップグレード

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

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

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

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

Before you begin

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。

Procedure

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**

Example:

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。

Note
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。

Example:

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

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

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

```
FP9300-A /system #
```

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

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

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

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

Before you begin

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。

Procedure

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。

Important
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**

Example:

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。

Note
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。

Example:

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

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

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

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

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

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

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

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

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

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

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

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

Before you begin

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。

Procedure

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**

Example:

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。

Note
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。

Example:

```
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**

Example:

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。

Note
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。

Example:

```
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。

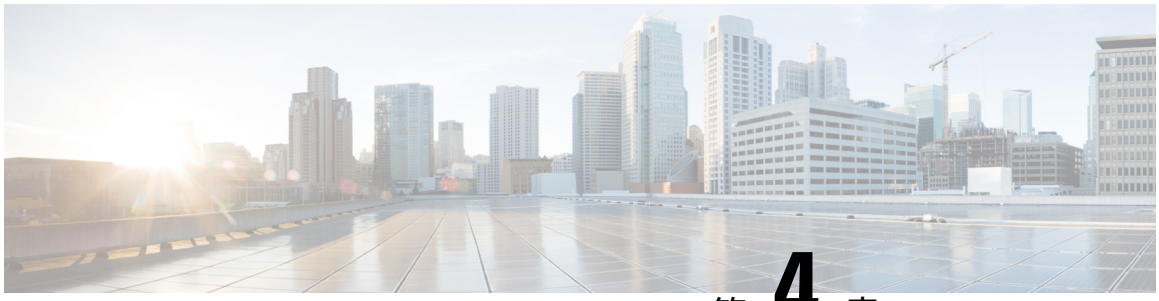
d) Firepower 4100 シリーズ アプライアンスのセキュリティ エンジン、または Firepower 9300 applianceのインストールされている任意のセキュリティ モジュールについて、管理状態が「Ok」、操作の状態が「Online」であることを確認します。
e) **show app-instance** を入力します。
f) シャーシにインストールされているすべての論理デバイスについて、操作の状態が「Online」であることを確認します。

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。

Firepower 4100/9300 のファームウェアのアップグレード

シャーシの FXOS 2.14.1 以降へのアップグレード（Threat Defense 7.4 の関連リリース）にはファームウェアが含まれます。古いデバイスをアップグレードする場合は、「Cisco Firepower 4100/9300 FXOS ファームウェア アップグレード ガイド」を参照してください。



第 4 章

復元またはアンインストール

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

復元とアンインストール

復元するかアンインストールするかは、リリースタイプによって異なります。

表 *13*：復元とアンインストール

	[元に戻す（Revert）]	アンインストール
リリース	バージョン 7.2 以降へのメジャーおよびメンテナンスアップグレード。	パッチ。
詳細	ソフトウェアは、最後のメジャーアップグレードまたはメンテナンスアップグレード（スナップショット）の直前の状態に戻ります。詳細については、元に戻る設定 （54 ページ）を参照してください。	ソフトウェアをパッチを適用したバージョンに戻します。設定は変更されません。
制約事項	コンテナインスタンスではサポートされていません。復元を妨げるその他のシナリオについては、「復元ガイドライン （52 ページ）」を参照してください。	アンインストールがサポートされていない、または推奨されていないシナリオについては、「アンインストールのガイドライン （57 ページ）」を参照してください。

	[元に戻す（Revert）]	アンインストール
復元/アンインストール元	[デバイス（Devices）] > [デバイス管理（Device Management）] を使用して Threat Defense アップグレードを元に戻します。	デバイスでエキスパートモード（CLI）を使用して Threat Defense パッチをアンインストールします。

例：復元とアンインストール

パッチ適用後に元に戻すと、パッチも削除されます。次に例を示します。

1. Threat Defense をバージョン 7.2.0 から 7.2.5 にアップグレードします。
2. バージョン 7.2.5 → 7.2.5.2 にパッチを適用します。
3. 次のいずれかを実行できます。
   - パッチをアンインストールして、バージョン 7.2.5 に戻します。

     これにより、パッチのみが削除されます。
   - アップグレードを元に戻して、バージョン 7.2.0 に戻します。

     これにより、パッチとメンテナンスリリースが削除されます。

Threat Defense アップグレードの復元

復元ガイドライン

このセクションでは、復元の一般的なガイドラインについて説明します。バージョン固有の復元の問題を確認するには、リリースノート「https://cisco.com/go/fmc-ftd-release-notes-74」のアップグレードガイドラインを参照してください。

高可用性またはクラスタ化デバイスの復元

Management Center Web インターフェイスを使用して Threat Defense を復元する場合、個々の高可用性ユニットまたはクラスタ化されたノードを選択することはできません。

すべてのユニットやノードを同時に復元させたほうが、復元が成功する可能性が高くなります。Management Center から復元を開始すると、システムは自動的にこれを実行します。デバイス CLI を使用する必要がある場合は、これを手動で行います。すべてのユニットとノードでセッションを開き、それぞれで復元が可能であることを確認してから、プロセスを同時に開始します。同時復元とは、すべてのデバイスがスタンドアロンであるかのように、トラフィックフローと検査の中断がインターフェイスの設定のみに依存することを意味します。

完全または部分的にアップグレードされたグループで復元がサポートされていることに注意してください。部分的にアップグレードされたグループの場合、システムはアップグレードされ

たユニットとノードからのみアップグレードを削除します。元に戻しても高可用性やクラスタが壊れることはありませんが、グループを分解してその新しいスタンドアロンデバイスを復元することができます。

Firepower 4100/9300 の復元

復元しても FXOS はダウングレードされません。

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

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

復元を妨げるシナリオ

次のいずれかの状況で復元を試みると、システムはエラーを表示します。

表 *14*：復元を妨げるシナリオ

シナリオ	解決方法
次の理由により、スナップショットを復元することはできません。 • デバイスをアップグレードしたときに、復元を有効にしていませんでした。 • Management Center またはデバイスからスナップショットを削除したか、スナップショットの期限が切れました。 • 別の Management Center でデバイスをアップグレードしました。 • 現在実行しているバージョンに戻しました（連続して複数の復元を実行しようとしています）。	なし。 復元スナップショットは、Management Center とデバイスに 30 日間保存され、その後自動的に削除され、復元できなくなります。ディスク容量を節約するためにどのアプライアンスからでもスナップショットを手動で削除できますが、復元の機能が失われます。 システムは1つのスナップショットのみを保存します。複数回復元することはできません。つまり、次のとおりです。 • サポート対象：A → B → C → B • サポート対象外：A → B → C → B → A

シナリオ	解決方法
最後のアップグレードに失敗しました。	アップグレードをキャンセルして、デバイスをアップグレード前の状態に戻します。または、問題を修正して再試行してください。 復元は、アップグレードは成功したものの、アップグレードされたデバイスが期待どおりに機能しない場合に使用します。復元は、失敗または進行中のアップグレードをキャンセルすることとは異なります。元に戻すこともキャンセルすることもできない場合は、イメージを再作成する必要があります。
アップグレード以降に、管理アクセスインターフェイスが変更されています。	元に戻して、もう一度お試しください。
クラスタのユニットが異なるバージョンからアップグレードされました。	すべて一致するまでユニットを削除し、クラスタメンバーを調整してから、小さなクラスタを復元します。新しくスタンドアロンユニットを復元することもできます。
クラスタでのアップグレード後に 1 つ以上のユニットがクラスタに追加されました。	新しいユニットを削除し、クラスタメンバーを調整してから、小さなクラスタを復元します。新しくスタンドアロンユニットを復元することもできます。
クラスタで Management Center と FXOS が異なる数のクラスタユニットを識別しています。	クラスタメンバーを調整して再試行しますが、すべてのユニットを復元することはできない場合があります。

元に戻る設定

元に戻る設定

次の設定が元に戻ります。

- Snort バージョン。
- デバイス固有の設定。

  一般的なデバイス設定、ルーティング、インターフェース、インラインセット、DHCP、SNMPなど、**[デバイス（Devices）]**>**[デバイス管理（Device Management）]**ページで設定するものすべて。
- デバイス固有の設定で使用されるオブジェクト。

  アクセスリスト、AS パス、キーチェーン、インターフェイス、ネットワーク、ポート、ルートマップ、SLA モニターオブジェクトなどが含まれます。デバイスのアップグレード後にこれらのオブジェクトを編集した場合、システムは新しいオブジェクトを作成する

か、元に戻されたデバイスが使用するオブジェクトのオーバーライドを設定します。これにより、他のデバイスは現在の設定に従ってトラフィックを処理し続けることができます。

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

元に戻されない設定

次の設定は元に戻りません。

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

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

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

  復元に成功した後にインターフェイスの変更を同期します。

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

  推奨される FXOS と Threat Defense の組み合わせを実行する必要がある場合は、完全な再イメージ化が必要になる場合があります。復元ガイドライン （52 ページ）を参照してください。

Threat Defense アップグレードの復元

Management Center とデバイス間の通信が中断されない限り、Management Center を使用してデバイスを復元する必要があります。通信が中断された場合は、デバイスで **upgrade revert** CLI コマンドを使用できます。システムがどのバージョンに戻るのかを確認するには、**show upgrade revert-info** コマンドを使用します。

Caution CLI から復元すると、アップグレード後に行った変更によっては、デバイスと Management Center 間で設定が同期されないことがあります。これにより、後に通信と展開の問題が発生する可能性があります。

Before you begin

- 復元がサポートされていることを確認してください。ガイドラインを読んで理解してください。
- 「アップグレードの計画, on page 1」の章に戻ります。一般に、インストールの準備をしたのと同じ方法で、アップグレードを元に戻す準備をします。安全な外部の場所にバック

アップすることが特に重要です。復元に失敗した場合、再イメージ化が必要になることがあります。再イメージ化を行うと、ほとんどの設定が工場出荷時の状態に戻ります。

Procedure

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

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

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

ステップ 3 復元して再起動することを確認します。

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

ステップ 4 復元の進行状況を監視します。

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

ステップ 5 復元が成功したことを確認します。

復元が完了したら、**[デバイス（Devices）] > [デバイス管理（Device Management）]** を選択し、復元したデバイスのソフトウェアバージョンが正しいことを確認します。

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

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

ステップ 7 その他に必要となる復元後の構成変更を完了します。

たとえば、デバイスのアップグレード後にデバイス固有の設定で使用されるオブジェクトを編集した場合、システムは新しいオブジェクトを作成するか、復元されたデバイスが使用するオブジェクトのオーバーライドを設定します。復元したデバイスで使用されるオブジェクトを調べ、必要な調整を行うことをお勧めします。

ステップ 8 復元したデバイスに構成を再度展開します。

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

Threat Defense パッチのアンインストール

アンインストールのガイドライン

このトピックでは、アンインストールの一般的なガイドラインについて説明します。バージョン固有のアンインストールの問題を確認するには、リリースノート「https://cisco.com/go/fmc-ftd-release-notes-74」のアップグレードガイドラインを参照してください。

高可用性またはクラスタ化デバイスからのアンインストール

一度に1つのデバイスからアンインストールすることで、中断を最小限に抑えます。アップグレードとは異なり、システムはこの操作を行いません。次に移る前に、パッチが1つのユニットから完全にアンインストールされるまで待ちます。

高可用性：高可用性用に設定されたデバイスからパッチをアンインストールすることはできません。先にハイ アベイラビリティを解除する必要があります。

1. ハイ アベイラビリティを解除します。
2. 以前のスタンバイからアンインストールします。
3. 以前のアクティブからアンインストールします。
4. ハイ アベイラビリティを再確立します。

クラスタ：一度に1つのユニットからアンインストールし、制御ユニットを最後に残します。クラスタ化されたユニットは、パッチのアンインストール中はメンテナンス モードで動作します。

1. データモジュールから一度に 1 つずつアンインストールします。
2. データモジュールの 1 つを新しい制御モジュールに設定します。
3. 以前のコントロールからアンインストールします。

アンインストールの防止または制限のシナリオ

これらの状況のいずれかでアンインストールしようとすると、重大な問題が発生する可能性があります。

表 *15:* アンインストールの防止または制限のシナリオ

シナリオ	解決方法
リリースノートには、特定のパッチがアンインストールをサポートしていない、または推奨していないと記載されています。	パッチのアンインストールは、ソフトウェアにのみ適用されます。オペレーティングシステムを更新するパッチや、アンインストールによって元に戻されないその他のコンポーネントをアンインストールすると、設定の変更を展開できなかったり、新しいコンポーネントと古いソフトウェアの間でその他の非互換性が発生する可能性があります。このような場合は、アンインストールしないことをお勧めします。 パッチは累積的であり、パッチをアンインストールするとソフトウェアが開始時のバージョンに戻るため、影響を受けるパッチよりも前のバージョンに戻る場合は、それ以降のパッチをアンインストールしないことを推奨します。たとえば、パッチ5でオペレーティングシステムを更新する場合は、パッチ 5 をアンインストールしないでください。また、パッチ 4 以前（基本バージョンを含む）で起動した場合は、パッチ 6 以降もアンインストールしないでください。 これまたはその他の理由によりインストールすべきではない特定のパッチは、リリースノートに記載されています。これらのパッチのいずれかをアンインストールする必要がある場合は、Cisco TAC にお問い合わせください。
セキュリティ認定コンプライアンス（CC/UCAPL）モードになっています。	パッチによってオペレーティングシステムが更新され、セキュリティ認定コンプライアンスが有効になっている場合、アプライアンスのリブート時にFSIC（ファイルシステム完全性チェック）が失敗します。ソフトウェアは起動せず、リモートSSHアクセスが無効になり、ローカルコンソールを介してのみアプライアンスにアクセスできます。アンインストールは、セキュリティ認定コンプライアンスモードでは推奨されません。これを行う必要がある場合は、Cisco TAC にお問い合わせください。

シナリオ	解決方法
ホットフィックスまたはホットフィックスパッチをアンインストールする必要があります。	ホットフィックスとパッチは、インストールとまったく逆の順序（最後にインストールしたものを最初に削除）でアンインストールする必要があります。次に例を示します。 • インストール：パッチ A → ホットフィックス B → ホットフィックス C → パッチ D → ホットフィックス E • アンインストール：ホットフィックス E → パッチ D → ホットフィックス C → ホットフィックス B → パッチ A 更新履歴を表示するには、エキスパートモードを使用します（**cat /etc/sf/patch_history**）。 ホットフィックスおよびホットフィックスパッチのアンインストールは推奨されません。これを行う必要がある場合は、Cisco TAC にお問い合わせください。
現在実行中のバージョンに戻りました。	なし。 メジャーリリースまたはメンテナンスリリースにアップグレードすると、新しいバージョンに適用されないアップグレードパッケージとアンインストーラが削除されます。

Threat Defense のパッチのアンインストール

Linux シェル（エキスパートモード）を使用してパッチをアンインストールします。デバイスの `admin` ユーザーとして、または CLI 設定アクセス権を持つ別のローカルユーザーとして、デバイス シェルにアクセスできる必要があります。Management Center ユーザーアカウントは使用できません。シェルアクセスを無効にした場合は、 ロックダウンを元に戻すために Cisco TAC にご連絡ください。

Caution アンインストール中に設定の変更を行ったり、展開したりしないでください。システムが非アクティブに見えても、進行中のアンインストールを手動で再起動、シャットダウン、または再起動しないでください。システムが使用できない状態になり、再イメージ化が必要になる場合があります。アンインストールに失敗する、アプライアンスが応答しないなど、アンインストールで問題が発生した場合には、Cisco TAC にお問い合わせください。

Before you begin

- アンインストールがサポートされていることを確認します。ガイドラインを読んで理解してください。
- 「アップグレードの計画, on page 1」の章に戻ります。一般に、パッチのアンインストールは、インストールの準備と同じ方法で準備する必要があります。

- 高可用性ペアを解除します。

Procedure

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

アンインストールする前に展開すると、失敗する可能性が減少します。展開とその他の必須のタスクが完了していることを確認してください。アンインストールの開始時に実行中だったタスクは停止され、失敗したタスクとなって再開できなくなります。後で失敗ステータス メッセージを手動で削除できます。

ステップ 2 デバイスの Threat Defense CLI にアクセスします。`admin` として、または設定アクセス権を持つ別の CLI ユーザーとしてログインします。

デバイスの管理インターフェイスに SSH 接続するか（ホスト名または IP アドレス）、コンソールを使用できます。コンソールを使用する場合、一部のデバイスではデフォルトでオペレーティング システムの CLI に設定されており、次のように Threat Defense CLI にアクセスする場合は追加の手順が必要になります。

Firepower 1000 Firepower 2100 Cisco Secure Firewall 3100 Cisco Secure Firewall 4200	`connect ftd`
Firepower 4100/9300	`connect module` *slot_number* `console`、次に `connect ftd`（最初のログインのみ）
ASA 5500-X シリーズ ISA 3000	—
Threat Defense Virtual	—

ステップ 3 `expert` コマンドを使用して Linux シェルにアクセスします。

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

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

パッチのアンインストーラには、アップグレードパッケージと同様に名前が付けられていますが、ファイル名には `Patch` ではなく `Patch_Uninstaller` が含まれています。デバイスにパッチを適用すると、そのパッチ用のアンインストーラがアップグレードディレクトリに自動的に作成されます。アンインストーラがない場合は、Cisco TAC までお問い合わせください。

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

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

Caution
確認を求められることはありません。このコマンドを入力すると、デバイスの再起動を含むアンインストールが開始されます。アンインストール時のトラフィック フローとインスペクションの中断は、アップグ

レード時に発生する中断と同じです。準備が整っていることを確認してください。`--detach` オプションを使用すると、SSH セッションがタイムアウトした場合にアンインストールプロセスが強制終了されなくなり、デバイスが不安定な状態になる可能性があることに注意してください。

ステップ 6 ログアウトするまでアンインストールを監視します。

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

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

それ以外の場合は、コンソールか端末で進行状況を監視します。

ステップ 7 アンインストールが成功したことを確認します。

アンインストールが完了したら、デバイスのソフトウェアバージョンが正しいことを確認します。Management Center で、**[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択します。

ステップ 8 高可用性でクラスタ化されている展開では、ユニットごとに手順 2 から 7 を繰り返します。

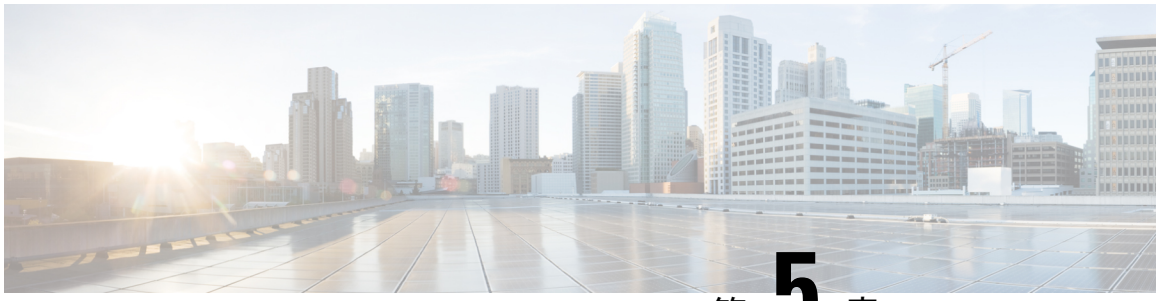
クラスタの場合、制御ユニットからアンインストールしないでください。すべてのデータユニットからアンインストールしたら、そのうちの 1 つを新しい制御ユニットに設定し、以前の制御ユニットからアンインストールします。

ステップ 9 構成を再展開します。

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

What to do next

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



第 5 章

トラブルシューティングおよび参考資料

アップグレードパッケージのトラブルシューティング

表 *16 :* アップグレードパッケージのトラブルシューティング

問題	解決方法
更新しても使用可能なアップグレードがありません。	現在の展開で使用可能な最新バージョンをすでに実行しており、かつ、アップグレードパッケージをロード/設定していません。
推奨リリースがマークされていません。	推奨リリースは、対象となる場合にのみ一覧表示されます。推奨リリース以降をすでに実行している場合、またはそこまでアップグレードできない場合は、一覧表示されません。推奨リリースへのパッチは、推奨としてマークされませんが、適用することをお勧めします。
必要なパッケージが表示されません。	現在の展開に適用されるメジャーアップグレード、メンテナンスアップグレード、およびパッチアップグレードのみが一覧表示され、直接ダウンロードできます。手動でアップロードしない限り、次のものは一覧表示されません。 • 特定バージョンへのデバイスアップグレード（メジャーおよびメンテナンス）（そのバージョンをサポートしているデバイスがある場合を除く）。 • デバイスパッチ（該当するメンテナンスリリースのデバイスが 1 つ以上ある場合を除く）。 • ホットフィックス。これらは手動でアップロードする必要があります。

Threat Defense のアップグレードのトラブルシューティング

表 *17 : Threat Defense* のアップグレードのトラブルシューティング

問題	解決方法
ターゲットバージョンの [アップグレード（Upgrade）] ボタンがない。	次のいずれかです。 • 依然として、アップグレードパッケージが必要です。 • 現在、そのバージョンにアップグレードできるものがありません。
アップグレードウィザードにデバイスが一覧表示されない。	**[デバイス（Devices）] > [Threat Defense のアップグレード（Threat Defense Upgrade）]** からウィザードに直接アクセスした場合は、ワークフローが空白になることがあります。 開始するには、[アップグレード先（Upgrade to）] メニューからターゲットバージョンを選択します。システムは、どのデバイスをそのバージョンにアップグレードできるかを判断し、[デバイスの詳細（Device Details）] ペインに表示します。[アップグレード先（Upgrade to）] メニューの選択肢は、Management Center 上のデバイス 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。ターゲットバージョンが一覧表示されていない場合は、[アップグレードパッケージの管理（Manage Upgrade Packages）] をクリックしてアップロードします。Management Center でのアップグレードパッケージの管理（5 ページ）を参照してください。 ターゲットバージョンがあるにもかかわらず、ウィザードにデバイスが一覧表示されない場合は、そのバージョンにアップグレードできるデバイスがありません。それでもデバイスがここに表示される必要があると思われる場合は、ユーザーロールによって、デバイスの管理が（そのため、アップグレードも）禁止されている可能性があります。
Management Center から管理対象デバイスへのアップグレードパッケージのコピーがタイムアウトになる。	これは、多くの場合、Management Center とそのデバイスの間の帯域幅が制限されているときに発生します。 内部 Web サーバーからアップグレードパッケージを直接取得するようにデバイスを設定できます。Management Center からアップグレードパッケージを削除し（これはオプションですが、ディスク容量を節約できます）、アップグレードパッケージを再度追加します。ただし、その際、パッケージのある場所へのポインタ（URL）を指定します。「内部サーバーからデバイスへのアップグレードパッケージのコピー （8 ページ）」を参照してください。

無応答および失敗した Threat Defense のアップグレード

⚠

注意 システムが非アクティブに見えても、アップグレード中のどの時点でも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。

表 *18 :* 無応答および失敗した *Threat Defense* のアップグレード

問題	解決方法
デバイスに到達できない。	デバイスは、アップグレード中、またはアップグレードが失敗した場合に、トラフィックを渡すことを停止できます。アップグレードする前に、ユーザーの位置からのトラフィックがデバイスの管理インターフェイスにアクセスするためにデバイス自体を通過する必要がないことを確認してください。 デバイスを経由せずに Management Center の管理インターフェイスにアクセスできる必要もあります。
アップグレードまたはパッチがハングアップしているように見える/デバイスが非アクティブになっているように見える。	Management Center でのデバイス アップグレード ステータスの更新が停止しているものの、アップグレードの失敗のレポートがない場合は、アップグレードのキャンセルを試みることができます。以下を参照してください。キャンセルできない場合やキャンセルが機能しない場合は、Cisco TAC にお問い合わせください。 **ヒント**：エキスパートモードおよび tail または tailf（`tail /ngfw/var/log/sf/update.status`）を使用して、デバイス自体のアップグレードログをモニターできます。
アップグレードが失敗する。	アップグレードが失敗する場合は、次の手順を実行してください。 • デバイスがアップグレード前の状態に戻っている（自動キャンセルが有効になっている）場合は、問題を修正して最初から再試行します。 • デバイスが引き続きメンテナンスモードである場合は、問題を修正してアップグレードを再開します。または、キャンセルし、後で再試行します。 再試行またはキャンセルできない場合、または問題が解消されない場合は、Cisco TAC にお問い合わせください。

問題	解決方法
パッチが失敗する。	進行中のパッチまたは失敗したパッチはキャンセルできません。ただし、パッチが早い段階（検証段階など）で失敗した場合は、デバイスが正常に稼働しつづける可能性があります。単純に、問題を修正し、再試行してください。 デバイスがメンテナンスモードになった後にパッチが失敗した場合は、アンインストーラが存在するか確認します。存在する場合は、それを実行して失敗したパッチを削除することを試行できます。Threat Defense のパッチのアンインストール （59 ページ）を参照してください。アンインストールが完了したら、問題を修正して再試行できます。 アンインストーラが存在しない場合、アンインストールが失敗する場合、または問題が解決しない場合は、Cisco TAC にお問い合わせください。
クラスタ化されたデバイスのアップグレードまたはパッチが失敗し、アップグレードを再試行する代わりに再イメージ化する必要があります。	クラスタノードのアップグレードが失敗し、ノードの再イメージ化を選択した場合は、クラスタに追加する前に、現在のバージョンの制御ノードに再イメージ化します。アップグレードが失敗した時期と方法に応じて、制御ノードの現在のバージョンは古いバージョンまたはターゲットバージョンになります。 アップグレード中の一時的な場合を除き、バージョンが混在するクラスタはサポートされていません。バージョンが混在するクラスタを意図的に作成すると、停止が発生する可能性があります。 **ヒント** 障害が発生したノードをクラスタから削除し、ターゲットバージョンに再イメージ化します。クラスタの残りの部分をターゲットバージョンにアップグレードしてから、再イメージ化されたノードを追加します。
アップグレードをキャンセルしたい。	キャンセルすると、デバイスはアップグレード前の状態に戻ります。失敗したアップグレードや進行中のアップグレードは、[デバイス管理（Device Management）] ページの [アップグレード（Upgrade）] タブからアクセスできる [アップグレードステータス（Upgrade Status）] ポップアップでキャンセルできます。パッチはキャンセルできません。 キャンセルできない場合やキャンセルが機能しない場合は、Cisco TAC にお問い合わせください。
失敗したアップグレードを再試行（再開）したい。	[デバイス管理（Device Management）] ページの [アップグレード（Upgrade）] タブからアクセスできる [アップグレードステータス（Upgrade Status）] ポップアップでアップグレードを再開できます。 問題が解消されない場合は、Cisco TAC にお問い合わせください。

問題	解決方法
アップグレードが失敗した場合の動作を変更したい。	アップグレードプロセスの一部は、失敗した場合の動作の選択です。これは、[アップグレードに失敗すると自動的にキャンセルされる...（Automatically cancel on upgrade failure...）]（自動キャンセル）オプションで実行されます。 • [自動キャンセルが有効（Auto-cancel enabled）]（デフォルト）：アップグレードが失敗すると、アップグレードがキャンセルされ、デバイスは自動的にアップグレード前の状態に復元されます。これにより、再グループ化して再試行しながら、可能なかぎり迅速に通常の操作に戻ります。 • [自動キャンセルが無効（Auto-cancel disabled）]：アップグレードが失敗した場合、デバイスはそのままになります。これにより、問題を修正し、アップグレードを再開することができます。 高可用性およびクラスタデバイスでは、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。

トラフィック フローとインスペクション

アップグレードの影響が最小限になるメンテナンスウィンドウ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を考慮してください。

ThreatDefenseアップグレードのトラフィックフローとインスペクション

スタンドアロンデバイスでのソフトウェアのアップグレード

アップグレード中、デバイスはメンテナンスモードで稼働します。アップグレードの開始時にメンテナンスモードを開始すると、トラフィックインスペクションが2ー3秒中断します。インターフェイスの構成により、その時点とアップグレード中の両方のスタンドアロンデバイスによるトラフィックの処理方法が決定されます。

表 *19:* トラフィックフローとインスペクション：スタンドアロンデバイスでのソフトウェアのアップグレード

インターフェイス コンフィギュレーション		トラフィックの挙動
ファイアウォール インターフェイス	EtherChannel、冗長、サブインターフェイスを含むルーテッドまたはスイッチド。 スイッチドインターフェイスは、ブリッジグループまたはトランスペアレントインターフェイスとしても知られています。	廃棄。 ISA 3000 のブリッジ グループ インターフェイスの場合に限り、FlexConfig ポリシーを使用して、停電時のハードウェアバイパスを設定できます。これにより、ソフトウェアのアップグレード中にトラフィックのドロップが発生しますが、デバイスがアップグレード後の再起動中、インスペクションなしでトラフィックが通過します。
IPS のみのインターフェイス	インラインセット、ハードウェアバイパス強制が有効：[バイパス（Bypass）]：[強制（Force）]	ハードウェアバイパスを無効にするか、スタンバイモードに戻すまで、インスペクションなしで合格。
	インラインセット、ハードウェアバイパスがスタンバイモード：[バイパス（Bypass）]：[スタンバイ（Standby）]	デバイスがメンテナンスモードの場合、アップグレード中にドロップされます。その後、デバイスがアップグレード後の再起動を完了する間、インスペクションなしで合格します。
	インラインセット、ハードウェアバイパスが無効：[バイパス（Bypass）]：[無効（Disabled）]	廃棄。
	インラインセット、ハードウェアバイパス モジュールなし。	廃棄。
	インラインセット、タップモード。	パケットをただちに出力、コピーへのインスペクションなし。
	パッシブ、ERSPAN パッシブ。	中断なし、インスペクションなし。

高可用性デバイスおよびクラスタ化されたデバイスのソフトウェアアップグレード

高可用性デバイスやクラスタ化されたデバイスのアップグレード中に、トラフィックフローや検査が中断されることはありません。高可用性ペアの場合、スタンバイデバイスが最初にアップグレードされます。デバイスの役割が切り替わり、新しくスタンバイになったデバイスがアップグレードされます。

クラスタの場合、データ セキュリティ モジュールを最初にアップグレードして、その後コントロールモジュールをアップグレードします。コントロール セキュリティ モジュールをアッ

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

シングルユニットのクラスタでは、ヒットレスアップグレードはサポートされないことに注意してください。トラフィックフローと検査の中断は、スタンドアロンデバイスと同様に、アクティブユニットのインターフェイス設定に依存します。

ソフトウェアの復元（メジャーおよびメンテナンスリリース）

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

ソフトウェアのアンインストール（パッチ）

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

シャーシのアップグレードでのトラフィックフローとインスペクション

FXOS をアップグレードするとシャーシが再起動します。ファームウェアのアップグレードを含むバージョン 2.14.1 以降への FXOS アップグレードの場合、デバイスは 2 回リブートします。1 回は FXOS 用、1 回はファームウェア用です。対象には、 のバージョン 7.4.1 以降のシャーシアップグレードが含まれます。

高可用性またはクラスタ展開の場合でも、各シャーシの FXOS を個別にアップグレードします。中断を最小限に抑えるには、1 つずつシャーシをアップグレードします。「高可用性/クラスタ展開でのシャーシのアップグレードをともなう Threat Defense のアップグレード順序 （4 ページ）」を参照してください。

表 *20*：トラフィックフローとインスペクション：*FXOS* のアップグレード

Threat Defense の導入	トラフィックの挙動	メソッド
スタンドアロン	廃棄。	—

Threat Defense の導入	トラフィックの挙動	メソッド
高可用性	影響なし。	**ベストプラクティス**：スタンバイで FXOS を更新し、アクティブピアを切り替えて新しいスタンバイをアップグレードします。
	1 つのピアがオンラインになるまでドロップされる。	スタンバイでアップグレードが終了する前に、アクティブ ピアで FXOS をアップグレードします。
シャーシ間クラスタ	影響なし。	**ベストプラクティス**：少なくとも 1 つのモジュールを常にオンラインにするため、一度に 1 つのシャーシをアップグレードします。
	少なくとも 1 つのモジュールがオンラインになるまでドロップされる。	ある時点ですべてのモジュールを停止するため、シャーシを同時にアップグレードします。
シャーシ内クラスタ（FirePOWER 9300 のみ）	検査なしで受け渡される。	ハードウェアバイパス有効：[Bypass: Standby] または [Bypass-Force]。
	少なくとも 1 つのモジュールがオンラインになるまでドロップされる。	ハードウェアバイパス無効：[Bypass: Disabled]。
	少なくとも 1 つのモジュールがオンラインになるまでドロップされる。	ハードウェア バイパス モジュールなし。

設定展開時のトラフィックフローとインスペクション

Snort は、通常、アップグレード直後の最初の展開時に再起動されます。つまり、Management Center のアップグレードの場合、すべての管理対象デバイスで Snort が再起動する可能性があります。後続の展開後は、展開の前に特定のポリシーまたはデバイス設定を変更しない限り、Snort は再起動しません。

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

表 *21* : トラフィックフローとインスペクション：設定変更の展開

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

時間とディスク容量

アップグレードまでの時間

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。次の表に、アップグレード時間に影響を与える可能性のあるいくつかの事項を示します。

Caution 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、にお問い合わせください「無応答および失敗した Threat Defense のアップグレード, on page 65」を参照してください。

Table 22: アップグレード時間の考慮事項

考慮事項	詳細（Details）
バージョン	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	通常、ローエンドモデルではアップグレード時間が長くなります。
仮想アプライアンス	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します。
高可用性とクラスタリング	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	アップグレード時間は、構成の複雑さ
コンポーネント	オペレーティングシステムまたは仮想ホスティングのアップグレード、アップグレードパッケージの転送、準備状況チェック、VDB と侵入ルール（SRU/LSP）の更新、設定の展開、およびその他の関連タスクを実行するために、追加の時間が必要になる場合があります。

アップグレードするディスク容量

Management Center（/Volume または /var のいずれか）にデバイス アップグレード パッケージ用の十分な容量が必要です。または、内部サーバーを使用して保存することもできます。アップグレードパッケージをデバイスにコピーすると、準備状況チェックでアップグレードを実行するのに十分なディスク容量があるかどうかが示されます。空きディスク容量が十分でない場合、アップグレードは失敗します。

Table 23: ディスク容量の確認

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

アップグレード機能の履歴

表 *24 : 20240808*

機能	最小の **Threat Defense**	詳細
Threat Defense のアップグレード		
マルチインスタンスモードでの Secure Firewall 3100 のシャーシのアップグレード	7.4.1	マルチインスタンスモードの Cisco Secure Firewall 3100 では、コンテナインスタンスのアップグレード（*Threat Defense* のアップグレード）とは別に、オペレーティングシステムとファームウェアがアップグレードの対象（シャーシのアップグレード）になります。 新規/変更された画面： • シャーシのアップグレード：**[デバイス（Devices）]** > **[シャーシのアップグレード（Chassis Upgrade）]** • Threat Defense のアップグレード：**[デバイス（Devices）]** > **[Threat Defense のアップグレード（Threat Defense Upgrade）]**

機能	最小の Threat Defense	詳細
Threat Defense およびシャーシアップグレードウィザードからアップグレード後の設定変更レポートを生成およびダウンロードします。	任意（Any）	アップグレードワークフローをクリアしていない場合でも、Threat Defense ウィザードおよびシャーシ アップグレード ウィザードからアップグレード後の設定変更レポートを生成およびダウンロードできるようになりました。 以前は、[高度な展開（Advanced Deploy）] 画面を使用してレポートを生成し、メッセージセンターを使用してレポートをダウンロードしていました。このメソッドは引き続き使用できます。これは、複数のデバイスの変更レポートをすばやく生成する場合、またはワークフローをクリアした場合に役立ちます。 新規/変更された画面： • **[デバイス（Devices）] > [Threat Defenseアップグレード（Threat Defense Upgrade）] > [設定の変更（Configuration Changes）]** • **[デバイス（Devices）] > [シャーシアップグレード（Chassis Upgrade）] > [設定の変更（Configuration Changes）]** 参照：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
廃止：デバイス間のアップグレードパッケージのコピー（「ピアツーピア同期」）。	7.6.0	Threat Defense CLI を使用して、管理ネットワークを介してデバイス間でアップグレードパッケージをコピーすることはできなくなりました。Management Center とそのデバイス間の帯域幅が限られている場合は、内部 Web サーバーからアップグレードパッケージを直接取得するようにデバイスを設定します。 廃止された CLI コマンド：**configure p2psync enable**、**configure p2psync disable**、**show peers**、**show peer details**、**sync-from-peer**、**show p2p-sync-status**

表 *25 : 20240203*

機能	最小の Threat Defense	詳細
Threat Defense のアップグレード		

機能	最小の Threat Defense	詳細
アップグレードの開始ページとパッケージ管理が改善されました。	いずれか	新しいアップグレードページでは、アップグレードの選択、ダウンロード、管理、および展開全体への適用が容易になります。このページには、現在の展開に適用されるすべてのアップグレードパッケージが、特にマークされた推奨リリースとともに一覧表示されます。パッケージを選択してシスコから簡単に直接ダウンロードしたり、パッケージを手動でアップロードおよび削除したりできます。 適切なメンテナンスリリースのアプライアンスが少なくとも 1 つある（またはパッチを手動でアップロードした）場合を除き、パッチは表示されません。ホットフィックスは手動でアップロードする必要があります。 新規/変更された画面： • **システム**（⚙）> **[製品のアップグレード（Product Upgrades）]**では、をアップグレードし、アップグレードパッケージを管理します。 • **システム**（⚙）> **[コンテンツの更新（Content Updates）]**で、侵入ルール、VDB、および GeoDB を更新できるようになりました。 • **[デバイス（Devices）]** > **[脅威防御のアップグレード（Threat Defense Upgrade）]** を選択すると、脅威防御のアップグレードウィザードに直接移動します。 廃止された画面/オプション： • **システム**（⚙）> **[更新（Updates）]**は廃止されました。脅威防御アップグレードはすべてウィザードを使用するようになりました。 • 脅威防御アップグレードウィザードの[アップグレードパッケージの追加（Add Upgrade Package）] ボタンは、新しいアップグレードページへの[アップグレードパッケージの管理（Manage Upgrade Packages）] リンクに置き換えられました。 参照：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
Threat Defense のアップグレードウィザードからの復元の有効化。	任意（7.1 以降にアップグレードする場合）	脅威防御アップグレードウィザードからの復元を有効化できます。 その他のバージョンの制限：Threat Defense をバージョン 7.2 以降にアップグレードする必要があります。 参照：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

機能	最小の Threat Defense	詳細
Threat Defense アップグレードウィザードから詳細なアップグレードステータスを表示します。	任意（Any）	Threat Defense アップグレードウィザードの最終ページで、アップグレードの進行状況をモニターできるようになりました。この機能は、[デバイス管理（Device Management）] ページの [アップグレード（Upgrade）] タブおよび Management Center の既存のモニタリング機能に追加されます。新しいアップグレードフローを開始していない限り、**[デバイス（Devices）]** > **[Threat Defense アップグレード（Threat Defense Upgrade）]**によってこのウィザードの最後のページに戻り、現在の（または最後に完了した）デバイスのアップグレードの詳細なステータスを確認できます。 参照：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
推奨リリースの通知。	任意（Any）	新しい推奨リリースが利用可能になると、Management Center から通知されるようになりました。今すぐアップグレードしない場合は、後でシステムに通知するか、次の推奨リリースまでリマインダを延期できます。新しいアップグレードページには、推奨リリースも示されます。 参照： Cisco Secure Firewall Management Center の新機能（リリース別）
FXOS アップグレードに含まれるファームウェアのアップグレード。	任意（Any）	**シャーシ/FXOS アップグレードの影響。ファームウェアのアップグレードにより、余分な再起動が発生します。** Firepower 4100/9300 の場合、バージョン 2.14.1 への FXOS アップグレードにファームウェアのアップグレードが含まれるようになりました。マルチインスタンスモードの Cisco Secure Firewall 3100（バージョン 7.4.1 の新機能）には、FXOS とファームウェアのアップグレードもバンドルされています。デバイス上のいずれかのファームウェア コンポーネントが FXOS バンドルに含まれているコンポーネントよりも古い場合、FXOS アップグレードによってファームウェアも更新されます。ファームウェアがアップグレードされると、デバイスは 2 回リブートします。1 回は FXOS 用、1 回はファームウェア用です。 ソフトウェアおよびオペレーティングシステムのアップグレードと同様に、ファームウェアのアップグレード中に設定変更を行ったり、展開したりしないでください。システムが非アクティブに見えても、ファームウェアの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。 参照：Cisco Firepower 4100/9300 FXOS ファームウェア アップグレード ガイド
ソフトウェアアップグレードの直接ダウンロードに関するインターネットアクセス要件を更新しました。	任意（Any）	Management Center では、ソフトウェア アップグレードパッケージの直接ダウンロードの場所が sourcefire.com から amazonaws.com に変更されています。 参照：「Internet Access Requirements」

機能	最小の Threat Defense	詳細
スケジュール済みタスクでは、パッチおよびVDB更新のみダウンロードされます。	任意（Any）	[最新の更新のダウンロード（Download Latest Update）] スケジュール済みタスクでは、メンテナンスリリースはダウンロードされなくなり、適用可能な最新のパッチと VDB の更新のみがダウンロードされるようになりました。メンテナンス（およびメジャー）リリースを Management Center に直接ダウンロードするには、**システム**（⚙）>**[製品のアップグレード（Product Upgrades）]** を使用します。 参照：「Software Update Automation」

表 *26 : 2022* 年 *12* 月 *13* 日

機能	最小の Threat Defense	詳細
Threat Defense アップグレードウィザードからアップグレードするデバイスを選択します。	任意（Any）	ウィザードを使用して、アップグレードするデバイスを選択します。 脅威防御アップグレードウィザードを使用して、アップグレードするデバイスを選択できるようになりました。ウィザード上で、選択したデバイス、残りのアップグレード候補、対象外のデバイス（および理由）、アップグレードパッケージが必要なデバイスなどの間でビューを切り替えることができます。以前は、[デバイス管理（Device Management）] ページしか使用できず、プロセスの柔軟性が大幅に低くなっていました。 参照：Management Center 用 Cisco Secure Firewall Threat Defense アップグレードガイド
Threat Defense の無人アップグレード。	任意（Any）	Threat Defense アップグレードウィザードは、新しい [無人モード（Unattended Mode）] メニューを使用して無人アップグレードをサポートするようになりました。アップグレードするターゲットバージョンとデバイスを選択し、いくつかのアップグレードオプションを指定して、その場から離れるだけです。ログアウトしたり、ブラウザを閉じたりすることもできます。 参照：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
さまざまなユーザーによる同時 Threat Defense アップグレードワークフロー。	任意（Any）	異なるデバイスをアップグレードする限り、異なるユーザーによる同時アップグレードワークフローが可能になりました。このシステムにより、すでに他の誰かのワークフローにあるデバイスをアップグレードすることはできません。以前は、すべてのユーザーで一度に1つのアップグレードワークフローのみが許可されていました。 参照：Management Center 用 Cisco Secure Firewall Threat Defense アップグレードガイド

機能	最小の Threat Defense	詳細
アップグレード前のトラブルシューティング生成をスキップします。	任意（Any）	新しい[アップグレード開始前にトラブルシューティングファイルを生成する（Generate troubleshooting files before upgrade begins）] オプションを無効にすることで、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の前にトラブルシューティング ファイルを自動生成することをスキップできるようになりました。これにより、時間とディスク容量を節約できます。 脅威防御デバイスのトラブルシューティング ファイルを手動で生成するには、**システム**（⚙）>**[正常性（Health）]**>**[モニタ（Monitor）]** を選択し、左側のパネルでデバイスをクリックし、[システムおよびトラブルシューティングの詳細を表示（View System & Troubleshoot Details）]、[トラブルシューティング ファイルの生成（Generate Troubleshooting Files）] をクリックします。 参照：Management Center 用 Cisco Secure Firewall Threat Defense アップグレードガイド
Threat Defense のアップグレード完了後の Snort 3 への自動アップグレードはオプションではなくなりました。	いずれか	**アップグレードの影響。展開すると、対象となるすべてのデバイスが Snort 3 にアップグレードされます。** Threat Defence をバージョン 7.3 以降にアップグレードする場合、[Snort 2から Snort 3にアップグレードする（Upgrade Snort 2 to Snort 3）] オプションは無効化できなくなりました。 ソフトウェアのアップグレード後、設定を展開すると、対象となるすべてのデバイスが Snort 2 から Snort 3 にアップグレードされます。個々のデバイスを元に戻すことはできますが、Snort 2 は将来のリリースで非推奨になるため、今すぐ使用を停止することを強く推奨します。 カスタム侵入ポリシーやネットワーク分析ポリシーを使用しているためにデバイスが自動アップグレード対象外になる場合は、検出とパフォーマンスを向上させるために、手動で Snort 3 にアップグレードすることを強く推奨します。移行のサポートについては、お使いのバージョンの Cisco Secure Firewall Management Center Snort 3 Configuration Guide を参照してください。

機能	最小の Threat Defense	詳細
Cisco Secure Firewall 3100 の統合アップグレードおよびインストールパッケージ。	7.3.0	

機能	最小の Threat Defense	詳細
		再イメージ化の影響。 バージョン 7.3 では、次のように、Secure Firewall 3100 の Threat Defense のインストールおよびアップグレードパッケージを組み合わせました。 • バージョン 7.1 ～ 7.2 インストールパッケージ：isco-ftd-fp3k.*version*.SPA • バージョン 7.1 ～ 7.2 アップグレードパッケージ：Cisco_FTD_SSP_FP3K_Upgrade-*version-build*.sh.REL.tar • バージョン 7.3 以降の統合パッケージ：Cisco_FTD_SSP_FP3K_Upgrade-*version-build*.sh.REL.tar Threat Defense は問題なくアップグレードできますが、古い Threat Defense および ASA バージョンから Threat Defense バージョン 7.3 以上に直接再イメージ化することはできません。これは、新しいイメージタイプに必要な ROMMON アップデートが原因です。これらの古いバージョンから再イメージ化するには、古い ROMMON でサポートされているだけでなく新しい ROMMON への更新も行う、ASA 9.19 以上を「通過」する必要があります。個別の ROMMON アップデータはありません。 Threat Defense バージョン 7.3 以上にするには、次のオプションがあります。 • Threat Defense バージョン 7.1 または 7.2 からのアップグレード — 通常のアップグレードプロセスを使用します。 該当するアップグレードガイドを参照してください。 • Threat Defense バージョン 7.1 または 7.2 からの再イメージ化 — 最初に ASA 9.19 以上に再イメージ化してから、Threat Defense バージョン 7.3 以上に再イメージ化します。 『Cisco Secure Firewall ASA および Secure Firewall Threat Defense 再イメージ化ガイド』の「Threat Defense→ASA: Firepower 1000, 2100; Secure Firewall 3100」、次に「ASA→Threat Defense: Firepower 1000, 2100 Appliance Mode; Secure Firewall 3100」を参照してください。 • ASA 9.17 または 9.18 からの再イメージ化 — 最初に ASA 9.19 以上にアップグレードしてから、Threat Defense バージョン 7.3 以上に再イメージ化します。 『Cisco Secure Firewall ASA アップグレードガイド』を参照し、次に『Cisco Secure Firewall ASA および Secure Firewall Threat Defense 再イメージ化ガイド』の「ASA→Threat Defense: Firepower 1000, 2100 Appliance Mode; Secure Firewall 3100」を参照してください。 • Threat Defense バージョン 7.3 以上からの再イメージ化 — 通常の再イメージ化プロセスを使用します。

機能	最小の Threat Defense	詳細
		『Cisco FXOS トラブルシューティング ガイド（Firepower Threat Defense を実行している Firepower 1000/2100 および Cisco Secure Firewall 3100/4200 向け）』の「Reimage the System with a New Software Version」を参照してください。
コンテンツの更新（Content Updates）		
自動 VDB ダウンロード。	いずれか	Management Center の初期設定では、最新の脆弱性データベース（VDB）を含むようになった、利用可能な最新のソフトウェア更新をダウンロードするための週次タスクがスケジュールされています。この週次タスクを確認し、必要に応じて調整することをお勧めします。必要に応じて、VDB を実際に更新し、構成を展開する新しい週次タスクをスケジュールしてください。 新規/変更された画面：システムで作成された [週次ソフトウェアダウンロード（Weekly Software Download）] のスケジュールされたタスクで、[脆弱性データベース（Vulnerability Database）] チェックボックスがデフォルトで有効になりました。
任意の VDB をインストールします。	いずれか	VDB 357 以降、その Management Center の基準 VDB までさかのぼって任意の VDB をインストールできるようになりました。 VDB を更新したら、構成の変更を展開します。利用できなくなった脆弱性、アプリケーションディテクタ、またはフィンガープリントに基づいて設定を行っている場合は、それらの設定を調べて、トラフィックが期待どおりに処理されていることを確認します。また、VDB を更新するためのスケジュールされたタスクは、ロールバックを取り消すことができることに注意してください。これを回避するには、スケジュールされたタスクを変更するか、新しい VDB パッケージを削除します。 新しい/変更された画面：**システム**（⚙）> **[更新（Updates）]** > **[製品アップデート（Product Updates）]** > **[利用可能なアップデート（Available Updates）]** で、古い VDB をアップロードすると、[インストール（Install）] アイコンの代わりに新しい [ロールバック（Rollback）] アイコンが表示されます。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。