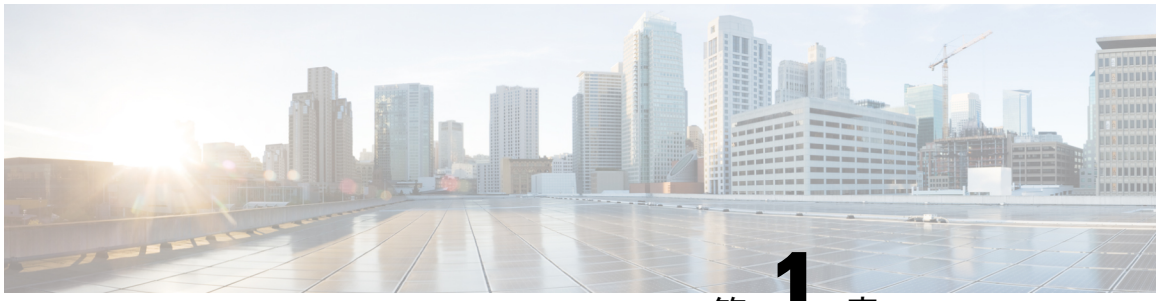
Management Center 用 Cisco Secure Firewall Threat Defense アップグレードガイド（バージョン 7.2.6 ～ 7.2.x）

初版：2024 年 3 月 19 日

最終更新：2024 年 7 月 1 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 および Management Center 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。

このガイドの対象読者

このガイドのアップグレード手順は、次の作業を行うユーザーを対象としています。

- バージョン バージョン 7.2.6 以降のメンテナンスリリースからの Managagement Center のアップグレード。
- バージョン 7.2.6 以降のメンテナンスリリースをすでに実行している Managagement Center を使用した Threat Defense のアップグレード（通常はバージョン 7.2 に）。

つまり、このガイドを使用して Management Center をアップグレードした後に、別のガイドを使用して Threat Defense をアップグレードする必要があります。

互換性

アップグレードする前に、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。

互換性については、次の資料を参照してください。

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

アップグレードのガイドライン

ソフトウェアのアップグレードガイドライン

このガイドには、現在のバージョンの Management Center に関するアップグレード手順が記載されています。リリース固有のアップグレードガイドライン（アップグレードの影響を受ける機能など）については、ターゲットバージョンのリリースノートを参照してください。

表 *1 : Cisco Secure Firewall Threat Defense* リリースノート

ターゲットバージョン	リリースノート
7.2.x	https://cisco.com/go/fmc-ftd-release-notes-72
7.1.x	Cisco Firepower バージョン 7.1.x リリースノート
7.0.x	Cisco Firepower バージョン 7.0.x リリースノート
6.7.x	Cisco Firepower バージョン 6.7.x リリースノート
6.6.x	Cisco Firepower バージョン 6.6.x リリースノート

Firepower 4100/9300 の FXOS アップグレードガイドライン

リリース固有の FXOS アップグレードガイドラインについては、ターゲットバージョンのリリースノートを参照してください。展開に影響を与える可能性のあるバグについては、現在のバージョンとターゲットバージョンの間のリリースノートを確認してください。

表 *2 : Cisco Firepower 4100/9300 FXOS* リリースノート

ターゲット Threat Defense	ターゲット FXOS	リリースノート
7.2	2.12	Cisco Firepower 4100/9300 FXOS 2.12(1) リリースノート
7.1	2.11	Cisco Firepower 4100/9300 FXOS 2.11(1) リリースノート https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/fxos2111/release/notes/fxos2111_rn.html
7.0	2.10	Cisco Firepower 4100/9300 FXOS 2.10(1) リリースノート https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/fxos2101/release/notes/fxos2101_rn.html

ターゲット Threat Defense	ターゲット FXOS	リリースノート
6.7	2.9	Cisco Firepower 4100/9300 FXOS 2.9(1) リリースノート https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/fxos291/release/notes/fxos291_rn.html
6.6	2.8	Cisco Firepower 4100/9300 FXOS 2.8(1) リリースノート https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/fxos281/release/notes/fxos281_rn.html

Firepower 4100/9300 のファームウェア アップグレード ガイドライン

ファームウェア アップグレード ガイドラインについては、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、または関連するアップグレード（オペレーティングシステム、シャーシ、ホスティング環境など）を調整する必要がある状況では特に重要です。

Management Center のアップグレードパス

次の表に、Management Center をアップグレードするための最小バージョンを示します。

Managagement Center では、その管理対象デバイスと同じバージョンか、より新しいバージョンを実行する必要があります。最初に Management Center をターゲットバージョンにアップグレードしてから、デバイスをアップグレードします。Management Center よりも大幅に古いバージョンを実行しているデバイスから開始すると、以降の Management Center 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する必要があります。つまり、最初にデバイス、次に Management Center、その後に再びデバイスをアップグレードします。

表 *3 : Management Center* をアップグレードするための最小バージョン

ターゲットバージョン	アップグレードする最小バージョン	管理可能な最も古いデバイス
7.4	7.0	7.0
7.3	7.0	6.7
7.2	6.6	6.6

Threat Defense のアップグレードパス

次の表に、Threat Defense をアップグレードするための最小バージョンを示します。最小バージョンを実行していない場合は、複数手順のアップグレードを実行する必要があります。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。シャーシのアップグレードをともなう Threat Defense のアップグレードパス （4 ページ）を参照してください。

表 *4 : Threat Defense* をアップグレードするための最小バージョン

ターゲットバージョン	アップグレードする最小バージョン
7.4	7.0
7.3	7.0
7.2	6.6

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

Firepower 4100/9300 の場合、Threat Defense のメジャーアップグレードにはシャーシのアップグレード（FXOS とファームウェア）が必要です。メンテナンスリリースおよびパッチの場合は、ほとんど必要ありません。シャーシの FXOS 2.14.1 以降へのアップグレードにはファームウェアが含まれます。それ以外の場合は、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。

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する必要があります。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。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。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 （5 ページ）を参照してください。

次の表に、シャーシのアップグレードが必要な場合に Threat Defense をアップグレードするための最小バージョンを示します。

表 *5 : Threat Defense* シャーシをアップグレードするための最小バージョン

対象のバージョン	アップグレードする最小バージョン
FXOS 2.14.1.131 以降上の Threat Defense 7.4	FXOS 2.10 上の Threat Defense 7.0
FXOS 2.13.0.198 以降上の Threat Defense 7.3	FXOS 2.10 上の Threat Defense 7.0
FXOS 2.12.0.31 以降上の Threat Defense 7.2	FXOS 2.8 上の Threat Defense 6.6

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 *6 : 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。

アップグレードパッケージ

Management Center へのアップグレードパッケージのアップロードとダウンロード

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 （10 ページ））。

表 *7: 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。

目的	作業
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、Threat Defense をアップグレードすると、関連するアップグレードパッケージがデバイスから削除されます。

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

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 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。

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 *8 : Threat Defense* 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 でのインターネットアクセス。 Managagement Center に十分なディスク容量。 Managagement 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 へのアップグレードパッケージのアップロードとダウンロード （6 ページ）

要件	使用するケース
Cisco → 使用しているコンピュータ → Management Center → デバイス Managagement Center に十分なディスク容量。 Managagement 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 にインターネットアクセスがないか、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（10 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。	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（インターネットアクセスやアップグレードタイプに関係なく）。 参照：内部サーバーからのアップグレードパッケージのコピー （8 ページ）
デバイス → デバイス 同じスタンドアロン Managagement 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。 別の方法でアップグレードパッケージを取得した少なくとも 1 つのデバイス。	転送を仲介する Managagement Center に依存せずにアップグレードパッケージをデバイスにコピーする必要があります。 参照：Threat Defense アップグレードパッケージのデバイス間のコピー （9 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 （10 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 *9 :* 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、同じスタンドアロン 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。
- 高可用性 Management Center によって管理されるデバイス。
- クラウド提供型 Firewall Management Center によって管理されるが、分析モードでオンプレミス Management Center に追加されたデバイス。
- 異なるドメインのデバイス、または NAT ゲートウェイによって分離されたデバイス。
- Management Center のバージョンに関係なく、バージョン 7.1 以前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。この機能に関連するすべての CLI コマンドの詳細については、Cisco Secure Firewall Threat Defense コマンドリファレンス を参照してください。

始める前に

- 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。

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。

Cisco.com のアップグレードパッケージ

システムにインターネットアクセスがない場合、または別の理由（ホットフィックス、ベータリリース）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 サイトで入手できます。

- Management Center： https://www.cisco.com/go/firepower-software
- Threat Defense ：https://www.cisco.com/go/ftd-software
- ASA FirePOWER：https://www.cisco.com/go/asa-firepower-sw

- NGIPSv： https://www.cisco.com/go/ngipsv-software

ソフトウェア 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、パッケージタイプ（アップグレード、パッチ、ホットフィックス）、ソフトウェアバージョン、およびビルドが反映されています。アップグレードパッケージは署名されており、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 *10 : Management Center* パッケージ

プラットフォーム	パッケージ
Management Center	Cisco_Secure_FW_Mgmt_Center_Upgrade-*Version-build*.sh.REL.tar

表 *11 : Threat Defense* パッケージ

プラットフォーム	パッケージ
Firepower 1000 シリーズ	Cisco_FTD_SSP-FP1K_Upgrade-*Version-build*.sh.REL.tar
Firepower 2100 シリーズ	Cisco_FTD_SSP-FP2K_Upgrade-*Version-build*.sh.REL.tar
Secure Firewall 3100 シリーズ	Cisco_FTD_SSP-FP3K_Upgrade-*Version-build*.sh.REL.tar
Firepower 4100/9300	Cisco_FTD_SSP_Upgrade-*Version-build*.sh.REL.tar
ASA 5500-X シリーズ 最終サポート：バージョン 7.0	Cisco_FTD_Upgrade-*Version-build*.sh.REL.tar
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

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。

表 *12* : *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

FXOS 2.14.1 以降へのアップグレードにはファームウェアが含まれます。FXOS の以前のバージョンに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 *13* : 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。Firepower Management Center から管理対象デバイスへのデータのダウンロードに関するガイドライン [英語]（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。設定変更を展開します。

（注） アップグレード後に再度展開する必要があります。展開により、トラフィックフローとインスペクションが影響を受ける可能性があります。Threat Defense 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、次の手順を実行します。

- Management Center：**システム**（⚙） > **[Configuration]** > **[Time]** を選択します。
- Threat Defense ：**show time** CLI コマンドを使用します。

実行中のタスクとスケジュールされたタスク

重要なタスク（最終展開を含む）が完了していることを確認します。アップグレードの開始時に実行中のタスクは停止し、失敗したタスクとなり、再開できません。

バージョン 6.6.3+ からのアップグレードは、スケジュールされたタスクを自動的に延期します。アップグレード中に開始するようにスケジュールされたタスクは、アップグレード後の再起動の 5 分後に開始されます。スケジュールされたタスクを実行しない場合は（または以前のバージョンからアップグレードする場合）、アップグレード中に実行するようにスケジュールされたタスクを確認し、タスクをキャンセルまたは延期します。

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。新しいManagement Centerバックアップファイルがデバイスがアップグレードされたことを「認識」するように、管理対象デバイスをアップグレードした後にManagement Center をバックアップしてください。

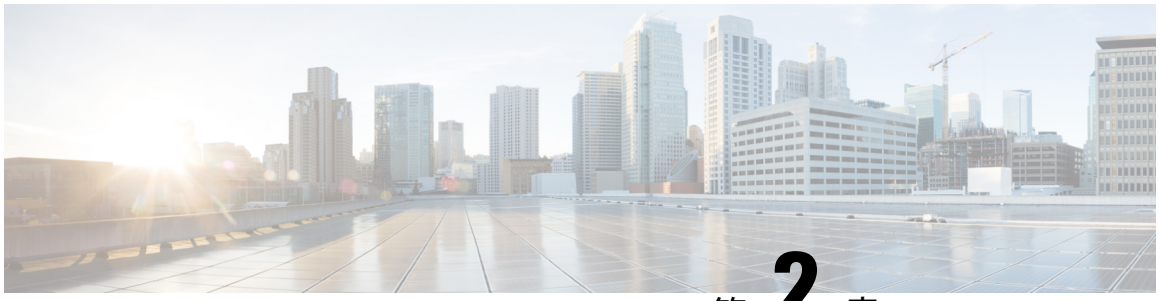
表 *14*：バックアップ

バックアップ	ガイド
Management center	Cisco Secure Firewall Management Center アドミニストレーション ガイド：「Backup/Restore」 設定とイベントをバックアップすることをお勧めします。
Threat Defense	Cisco Secure Firewall Management Center アドミニストレーション ガイド：「Backup/Restore」 バックアップは、KVM デバイスのクラスタ化された Threat Defense Virtual またはパブリッククラウドの Threat Defense Virtual についてはサポートされていません。
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 および Management Center 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。Management Center の場合、準備状況チェックに合格することは必須です。準備状況チェックで不合格になるとアップグレードできません。Threat Defense の場合は、この要件を無効にできますが、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

Management Center のアップグレード

Management Center のアップグレード：スタンドアロン

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

続行すると、Management Center のアップグレードウィザードに、アップグレード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。ウィザードから移動しても進行状況は保持され、他のユーザーは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、**システム**（⚙）> **[Product Upgrades]** を選択し、Management Center のシステム概要で [再開（Resume）] をクリックします。

Management Center 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（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や準備状況チェックの実行など、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、設定展開時のトラフィックフローとインスペクション （74 ページ）を参照してください。古い ASA FirePOWER または NGIPSv デバイスを管理している場合、トラフィック処理については、Cisco Firepower Management Center Upgrade Guide, Version 6.0–7.0を参照ください。

⚠

注意 アップグレード中は、設定の変更の実施または展開を行わないでください。システムが非アクティブに見えても、進行中のアップグレードを手動で再起動、シャットダウン、または再起動しないでください。システムが使用できない状態になり、再イメージ化が必要になる場合があります。アップグレードに失敗する、アプライアンスが応答しないなど、アップグレードで問題が発生した場合には Cisco TAC にお問い合わせください。

始める前に

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 （1 ページ）
- アップグレードパスを計画します：アップグレードパス （3 ページ）
- 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 （2 ページ）
- 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 （12 ページ）
- 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 （13 ページ）
- バックアップを実行します：バックアップ （13 ページ）

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

ステップ 2 アップグレードパッケージを取得します。

[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 へのアップグレードパッケージのアップロードとダウンロード （6 ページ）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 （65 ページ）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、[Management Center] を選択します。

Management Center のアップグレードウィザードが表示されます。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。

ステップ 4 [次へ（Next）] をクリックして準備状況チェックを実行します。

[準備状況チェックの実行（Run Readiness Checks）] をクリックします。準備状況チェックの実行中は、手動で再起動またはシャットダウンしないでください。Management Center の場合、準備状況チェックに合格することは必須です。準備状況チェックで不合格になるとアップグレードできません。

ステップ 5 [次へ（Next）] をクリックし、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 （13 ページ））。

ステップ 6 [アップグレード（Upgrade）] をクリックし、アップグレードして再起動することを確認します。

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

ステップ 7 可能なときに、 に再度ログインします。

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

ステップ 8 アップグレードが成功したことを確認します。

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

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

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

ステップ 10 アップグレード後に必要な構成変更があれば、実行します。

ステップ 11 管理対象デバイスに構成を再展開します。

Management Centerのアップグレード：ハイアベイラビリティ

高可用性 Management Center を一度に 1 つずつアップグレードするには、この手順を使用します。ワークフローもアップグレードパッケージも、高可用性 Management Center 間で同期されません。

同期を一時停止して、スタンバイをアップグレードします。アップグレードが完了すると、Management Center がアクティブに戻って稼働し、他の Management Center をアップグレードできるようになります。この一時的なアクティブ-アクティブ状態のことを「スプリットブレイン」と呼び、アップグレード中（およびパッチのアンインストール中）を除き、サポートされていません。 ペアが split-brain の状況で、構成の変更または展開を行わないでください。同期の再開後は変更内容が失われます。

続行すると、Management Center のアップグレードウィザードに、アップグレード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。ウィザードから移動しても進行状況は保持され、他のユーザーは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、**システム**（⚙）>**[Product Upgrades]** を選択し、Management Center のシステム概要で [再開（Resume）] をクリックします。

Management Center のアップグレードは、ウィザードを完了し、同期を一時停止して、[アップグレード（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や準備状況チェックの実行など、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、設定展開時のトラフィックフローとインスペクション （74 ページ）を参照してください。古い ASA FirePOWER または NGIPSv デバイスを管理している場合、トラフィック処理については、Cisco Firepower Management Center Upgrade Guide, Version 6.0–7.0を参照ください。

（注） ホットフィックス リリース ノートに特に記載されていない、または Cisco TAC から指示されていない限り、高可用性 Management Center にホットフィックスをインストールするために同期を一時停止する必要はありません。

注意 アップグレード中は、設定の変更の実施または展開を行わないでください。システムが非アクティブに見えても、進行中のアップグレードを手動で再起動、シャットダウン、または再起動しないでください。システムが使用できない状態になり、再イメージ化が必要になる場合があります。アップグレードに失敗する、アプライアンスが応答しないなど、アップグレードで問題が発生した場合には Cisco TAC にお問い合わせください。

始める前に

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 （1 ページ）
- アップグレードパスを計画します：アップグレードパス （3 ページ）
- 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 （2 ページ）
- 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 （12 ページ）
- 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 （13 ページ）
- バックアップを実行します：バックアップ （13 ページ）

両方の Management Center のアップグレードを準備します。

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

ステップ 2 アップグレードパッケージを取得します。

[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 へのアップグレードパッケージのアップロードとダウンロード （6 ページ）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 （65 ページ）を参照してください。

これは両方の Management Center で実行する必要があります。アップグレードパッケージは同期されません。

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、[Management Center] を選択します。

Management Center のアップグレードウィザードが表示されます。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。

ステップ 4 [次へ（Next）] をクリックして準備状況チェックを実行します。

[準備状況チェックの実行（Run Readiness Checks）] をクリックします。準備状況チェックの実行中は、手動で再起動またはシャットダウンしないでください。Management Center の場合、準備状況チェックに合格することは必須です。準備状況チェックで不合格になるとアップグレードできません。

ステップ 5 [次へ（Next）] をクリックし、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 （13 ページ））。

ステップ 6 他の Management Center について、手順 1 ～ 5 を繰り返します。

同期を一時停止します。

ステップ 7 アクティブ状態の Managagement Center で、同期を一時停止します。

アクティブから一時停止した場合は、どちらからでも再開できます。スタンバイから一時停止した場合は、スタンバイから再開する必要があります。

a) **[統合（Integration）] > [その他の統合（Other Integrations）]** を選択します。
b) [ハイ アベイラビリティ（High Availability）] タブで、[同期の一時停止（Pause Synchronization）] をクリックします。

スタンバイをアップグレードしてから、アクティブをアップグレードします。

ステップ 8 スタンバイ状態の Managagement Center で、[アップグレード（Upgrade）] をクリックし、アップグレードして再起動することを確認します。

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

ステップ 9 可能なときに、 に再度ログインします。

- メジャーアップグレードとメンテナンスアップグレード：アップグレードが完了する前にログインできます。アップグレードの進行状況をモニターし、アップグレードログとエラーメッセージを確

認するために使用できるページが表示されます。アップグレードが完了し、システムが再起動すると再度ログアウトされます。リブート後に、再ログインしてください。

- パッチとホットフィックス：アップグレードと再起動が完了した後にログインできます。

ステップ 10 アップグレードが成功したことを確認します。

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

ステップ 11 他の Management Center について、手順 8 ～ 10 を繰り返します。

同期を再開し、アップグレード後のタスクを完了します。

ステップ 12 引き続き、古いアクティブ状態の Managagement Center（アップグレードしたばかりの Managagement Center）で、同期を再開します。

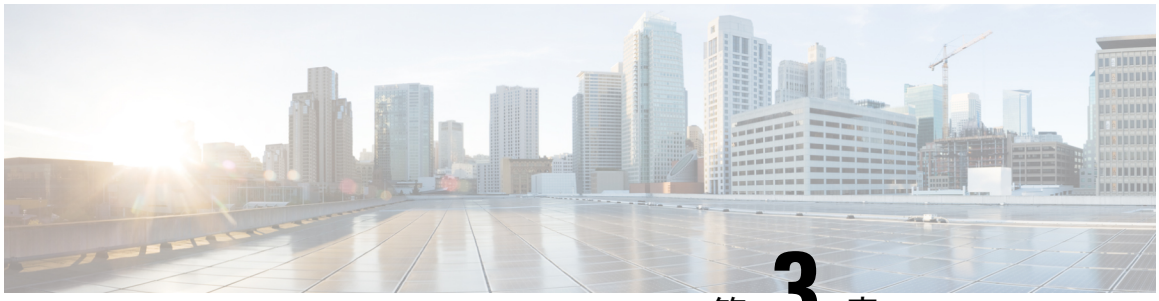
a) **[統合（Integration）]** > **[その他の統合（Other Integrations）]** を選択します。
b) [ハイ アベイラビリティ（High Availability）] タブで、[同期の再開（Resume Synchronization）] をクリックします。

ステップ 13 侵入ルール（SRU/LSP）および脆弱性データベース（VDB）を更新します。

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

ステップ 14 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 15 管理対象デバイスに構成を再展開します。



第 3 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、Threat Defense ウィザードに、選択したデバイスに関する基本情報と、現在のアップグレード関連のステータスが表示されます。表示内容には、アップグレードできない理由が含まれます。あるデバイスがウィザードの 1 つの段階に「合格」しない場合、そのデバイスは次の段階には表示されません。

ウィザードから移動しても進行状況は保持されます。他のユーザーは、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）] > [デバイスのアップグレード（Device Upgrade）]**を選択します。

デバイス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、トラフィック フローとインスペクション （71 ページ）を参照してください。

⚠

注意 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 （69 ページ） を参照してください。

始める前に

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 （1 ページ）
- アップグレードパスを計画します：アップグレードパス （3 ページ）
- 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 （2 ページ）
- 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 （12 ページ）
- 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 （13 ページ）
- バックアップを実行します：バックアップ （13 ページ）
- 必要に応じてシャーシをアップグレードします：Firepower 4100/9300 シャーシのアップグレード （31 ページ）

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 へのアップグレードパッケージのアップロードとダウンロード （6 ページ）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 （65 ページ）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。

ヒント 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 （26 ページ）」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。

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 （25 ページ）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 （13 ページ））。

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）] 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。

ヒント 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）高可用性および拡張性の展開では、デバイスのロールを調べます。

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

ステップ 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。

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。**[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）] タブから変更レポートをダウンロードできます。

次のタスク

- （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、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ます。
- 再度バックアップします：バックアップ （13 ページ）

Threat Defense のアップグレードオプション

表 *15 : 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。
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 以降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。 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。

オプション	無効にする場合	詳細
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 16：

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。

目的	操作手順
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

古い ASA FirePOWER および NGIPSv デバイスのアップグレード

バージョン 7.0 で最後にサポートされていた古い ASA FirePOWER または NGIPSv デバイスをアップグレードするには、この手順を使用します。

（注） [インストール（Install）]をクリックするまで、デバイスのアップグレードは開始されません。その時点までの手順（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など）はすべて、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、ターゲットバージョンのリリースノート（Cisco Secure Firewall Threat Defense リリースノート）を参照してください。

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

始める前に

アップグレードの準備が整っていることを確認します。このガイドには、これらのデバイスの詳細なチェックリスト、計画情報、または ASA アップグレード手順が含まれていないことに注意してください。アップグレード手順については、Cisco Firepower Management Center Upgrade Guide, Version 6.0–7.0 を参照してください。

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

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 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 へのアップグレードパッケージのアップロードとダウンロード（6 ページ）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（65 ページ）を参照してください。

ステップ 3 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、アップグレードするデバイスのタイプ（[ASA FirePOWER] または [NGIPSv]）を選択します。

従来型デバイスのアップグレードページが表示されます。

ステップ 4 アップグレードするデバイスを選択します。

一度に 5 台を上回るデバイスをアップグレードしないことをお勧めします。選択したすべてのデバイスがそのプロセスを完了するまで、アップグレードを停止することはできません。いずれかのデバイスのアップグレードに問題がある場合、問題を解決する前に、すべてのデバイスのアップグレードを完了する必要があります。

ステップ 5 [Install] をクリックし、アップグレードして、デバイスを再起動することを確認します。

メッセージセンターでアップグレードの進行状況をモニタします。

ステップ 6 成功したことを確認します。

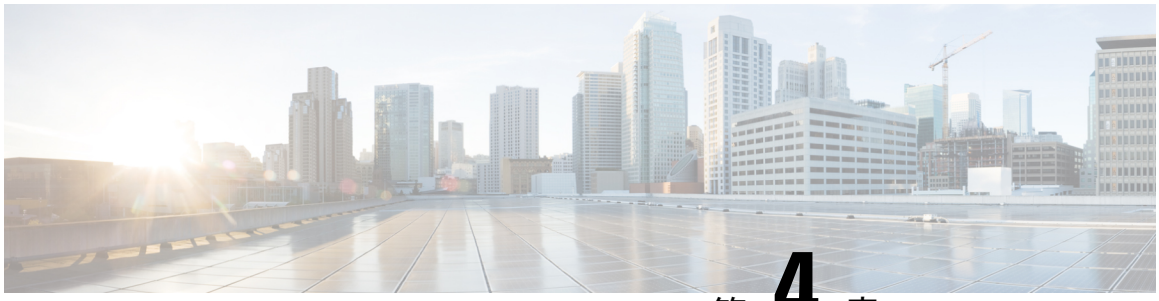
アップグレードが完了したら、**[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択し、アップグレードしたデバイスのソフトウェアバージョンが正しいことを確認します。

ステップ 7 侵入ルール（SRU/LSP）および脆弱性データベース（VDB）を更新します。

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

ステップ 8 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 9 アップグレードしたデバイスに構成を再度展開します。



第 4 章

Firepower 4100/9300 シャーシのアップグレード

Firepower 4100/9300 の場合、Threat Defense のメジャーアップグレードにはシャーシのアップグレード（FXOS とファームウェア）が必要です。メンテナンスリリースおよびパッチの場合は、ほとんど必要ありません。シャーシの FXOS 2.14.1 以降へのアップグレードにはファームウェアが含まれます。それ以外の場合は、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。

- Chassis Manager を使用した 上の FXOS のアップグレード （31 ページ）
- CLI を使用した 上の FXOS のアップグレード （40 ページ）

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

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

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

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

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

始める前に

アップグレードを開始する前に、以下が完了していることを確認します。

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

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

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

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

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

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

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

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

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

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

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

例：

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

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

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

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

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

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

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

始める前に

アップグレードを開始する前に、以下が完了していることを確認します。

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

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

a) シャーシ #2 の FXOS CLI に接続します（これは制御ユニットを持たないシャーシである必要があります）。
b) **top** を入力します。
c) **scope ssa** を入力します。
d) **show slot** を入力します。
e) Firepower 4100 シリーズ アプライアンスのセキュリティ エンジン、または Firepower 9300 applianceのインストールされている任意のセキュリティ モジュールについて、管理状態が「Ok」、操作の状態が「Online」であることを確認します。
f) **show app-instance** を入力します。
g) シャーシにインストールされているすべての論理デバイスについて、操作の状態が「Online」、クラスタの状態が「In Cluster」であることを確認します。また、稼働バージョンとして表示されている FTD ソフトウェアのバージョンが正しいことを確認します。

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

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

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

show versionを使用して無効にすることができます。

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

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

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

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

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

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

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

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

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

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

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

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

例：

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

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

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

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

Slot:
    Slot ID    Log Level Admin State  Oper State
    ---------- --------- ------------ ----------
    1          Info      Ok           Online
    2          Info      Ok           Online
```

```
    3          Info      Ok           Not Available
FP9300-A /ssa #

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

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

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

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

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

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

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

始める前に

アップグレードを開始する前に、以下が完了していることを確認します。

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

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

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

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

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

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

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

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

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

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

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

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

例：

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

例：

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

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

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

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

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

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

a) Firepower Management Center に接続します。

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

CLI を使用した 上の FXOS のアップグレード

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

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

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

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

始める前に

アップグレードを開始する前に、以下が完了していることを確認します。

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

ステップ 1 FXOS CLI に接続します。
ステップ 2 新しいプラットフォーム バンドル イメージを Firepower 4100/9300 シャーシにダウンロードします。

a) ファームウェア モードに入ります。

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

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

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

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

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

c) ダウンロード プロセスをモニタする場合：

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

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

例：

次の例では、SCP プロトコルを使用してイメージをコピーします。

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

ステップ 3 必要に応じて、ファームウェア モードに戻ります。

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

ステップ 4 auto-install モードにします。

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

ステップ 5 FXOS プラットフォーム バンドルをインストールします。

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

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

ステップ 6 システムは、まずインストールするソフトウェア パッケージを確認します。そして現在インストールされているアプリケーションと指定した FXOS プラットフォーム ソフトウェア パッケージの間の非互換性を通

知します。また既存のセッションを終了することやアップグレードの一部としてシステムをリブートする必要があることが警告されます。

yes を入力して、検証に進むことを確認します。

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

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

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

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

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

例：

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

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

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

FP9300-A /system #
```

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

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

f) シャーシにインストールされているすべての論理デバイスについて、操作の状態が「Online」であることを確認します。

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

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

始める前に

アップグレードを開始する前に、以下が完了していることを確認します。

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

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

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

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

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

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

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

show versionを使用して無効にすることができます。

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

a) **top** を入力します。

b) ファームウェア モードに入ります。

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

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

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

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

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

d) ダウンロード プロセスをモニタする場合：

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

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

例：

次の例では、SCP プロトコルを使用してイメージをコピーします。

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

ステップ 4 必要に応じて、ファームウェア モードに戻ります。

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

ステップ 5 auto-install モードにします。

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

ステップ 6 FXOS プラットフォーム バンドルをインストールします。

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

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

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

yes を入力して、検証に進むことを確認します。

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

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

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

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

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

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

例：

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

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

```
    Upgrade-Status: Ready

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

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

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

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

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

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

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

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

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

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

始める前に

アップグレードを開始する前に、以下が完了していることを確認します。

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

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

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

a) ファームウェア モードに入ります。

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

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

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

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

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

c) ダウンロード プロセスをモニタする場合：

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

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

例：

次の例では、SCP プロトコルを使用してイメージをコピーします。

```
Firepower-chassis-a # scope firmware
Firepower-chassis-a /firmware # download image scp://user@192.168.1.1/images/fxos-k9.2.3.1.58.SPA
Firepower-chassis-a /firmware # scope download-task fxos-k9.2.3.1.58.SPA
Firepower-chassis-a /firmware/download-task # show detail
Download task:
    File Name: fxos-k9.2.3.1.58.SPA
    Protocol: scp
    Server: 192.168.1.1
    Userid:
```

```
    Path:
    Downloaded Image Size (KB): 853688
    State: Downloading
    Current Task: downloading image fxos-k9.2.3.1.58.SPA from
192.168.1.1(FSM-STAGE:sam:dme:FirmwareDownloaderDownload:Local)
```

ステップ 3 必要に応じて、ファームウェア モードに戻ります。

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

ステップ 4 auto-install モードにします。

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

ステップ 5 FXOS プラットフォーム バンドルをインストールします。

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

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

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

yes を入力して、検証に進むことを確認します。

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

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

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

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

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

例：

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

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

Chassis 1:
    Server 1:
        Package-Vers: 2.3(1.58)
```

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

FP9300-A /system #
```

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

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

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

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

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

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

a) ファームウェア モードに入ります。

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

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

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

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

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

c) ダウンロード プロセスをモニタする場合：

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

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

例：

次の例では、SCP プロトコルを使用してイメージをコピーします。

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

ステップ 13 必要に応じて、ファームウェア モードに戻ります。

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

ステップ 14 auto-install モードにします。

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

ステップ 15 FXOS プラットフォーム バンドルをインストールします。

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

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

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

yes を入力して、検証に進むことを確認します。

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

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

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

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

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

例：

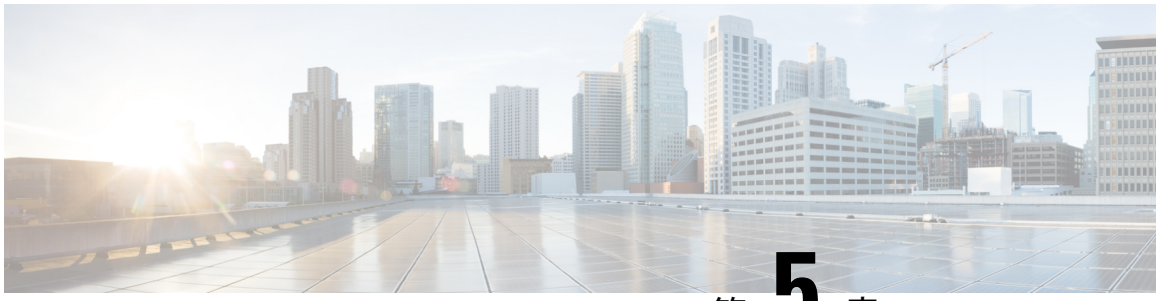
```
FP9300-A# scope system
FP9300-A /system # show firmware monitor
FPRM:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

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

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

FP9300-A /system #
```

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

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

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

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



第 5 章

アップグレードを元に戻すまたはアンインストールする

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

- メジャーおよびメンテナンスアップグレードの Threat Defense バージョン 7.1 以降への復元がサポートされています。
- アンインストールは、Threat Defense へのパッチと Management Center へのパッチでサポートされています。

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

- Threat Defense の復元 （53 ページ）
- パッチのアンインストール （58 ページ）

Threat Defense の復元

Threat Defense の復元について

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

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。Threat Defense 復元のガイドライン （54 ページ）を参照してください。

Threat Defense 復元のガイドライン

システム要件

メジャーおよびメンテナンスアップグレードの Threat Defense バージョン 7.1 以降への復元がサポートされています。

以下では復元機能はサポートされていません。

- 以前のバージョンへのアップグレード
- パッチとホットフィックス
- コンテナインスタンス

- Management Center のアップグレード

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。

復元しても FXOS はダウングレードされない

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 *17*：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。	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。
最後のアップグレードに失敗しました。	アップグレードをキャンセルして、デバイスをアップグレード前の状態に戻します。または、問題を修正して再試行してください。 復元は、アップグレードは成功したものの、アップグレードされたシステムが期待どおりに機能しない場合に使用します。復元は、失敗または進行中のアップグレードをキャンセルすることとは異なります。元に戻すこともキャンセルすることもできない場合は、イメージを再作成する必要があります。
アップグレード以降に、管理アクセスインターフェイスが変更されています。	元に戻して、もう一度お試しください。
クラスタのユニットが異なるバージョンからアップグレードされました。	すべて一致するまでユニットを削除し、クラスタメンバーを調整してから、小さなクラスタを復元します。新しくスタンドアロンユニットを復元することもできます。
クラスタでのアップグレード後に 1 つ以上のユニットがクラスタに追加されました。	新しいユニットを削除し、クラスタメンバーを調整してから、小さなクラスタを復元します。新しくスタンドアロンユニットを復元することもできます。
クラスタで 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。

Management Center を使用して Threat Defense を復元する

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。

⚠

注意 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。

Threat Defense の履歴：

- 7.1：初期サポート。

始める前に

- 復元がサポートされていることを確認してください。ガイドラインを読んで理解してください。
- 安全な外部の場所にバックアップします。復元に失敗した場合、再イメージ化が必要になることがあります。再イメージ化を行うと、ほとんどの設定が工場出荷時の状態に戻ります。

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

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

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

ステップ 3 復元して再起動することを確認します。

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

ステップ 4 復元の進行状況を監視します。

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

ステップ 5 復元が成功したことを確認します。

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

ステップ 6 （Firepower 4100/9300）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。

パッチのアンインストール

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

（注） このガイドでは、Management Center および Threat Defense パッチのアンインストールの方法について説明します。古い ASA FirePOWER または NGIPSv デバイスからパッチをアンインストールするには、Cisco Firepower Management Center Upgrade Guide, Version 6.0–7.0を参照してください。

高可用性/拡張性のアンインストール順序

高可用性/拡張性の展開では、一度に 1 つのアプライアンスからアンインストールすることで中断を最小限に抑えます。アップグレードとは異なり、システムはこの操作を行いません。次に移る前に、パッチが 1 つのユニットから完全にアンインストールされるまで待ちます。

表 *18 : Management Center* 高可用性のアンインストール順序

設定	アンインストール順序
Management Center ハイ アベイラビリティ	同期を一時停止した状態（「スプリットブレイン」と呼びます）で、ピアから一度に 1 つずつアンインストールします。ペアが split-brain の状況で、構成の変更または展開を行わないでください。 **1.** 同期を一時停止します（スプリットブレインに移行します）。 **2.** スタンバイからアンインストールします。 **3.** アクティブからアンインストールします。 **4.** 同期を再開します（スプリットブレインから抜けます）。

表 *19 : Threat Defense* 高可用性およびクラスタのアンインストール順序

設定	アンインストール順序
Threat Defense ハイ アベイラビリティ	ハイ アベイラビリティ用に設定されたデバイスからパッチをアンインストールすることはできません。先にハイ アベイラビリティを解除する必要があります。 **1.** ハイ アベイラビリティを解除します。 **2.** 以前のスタンバイからアンインストールします。 **3.** 以前のアクティブからアンインストールします。 **4.** ハイ アベイラビリティを再確立します。
Threat Defense クラスタ	一度に1つのユニットからアンインストールし、制御ユニットを最後に残します。クラスタ化されたユニットは、パッチのアンインストール中はメンテナンス モードで動作します。 **1.** データモジュールから一度に 1 つずつアンインストールします。 **2.** データモジュールの 1 つを新しい制御モジュールに設定します。 **3.** 以前のコントロールからアンインストールします。

Threat Defense パッチのアンインストール

Linux シェル（エキスパートモード）を使用してパッチをアンインストールします。デバイスの `admin` ユーザーとして、またはCLI設定アクセス権を持つ別のローカルユーザーとして、デバイス シェルにアクセスできる必要があります。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。

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

始める前に

- Threat Defense 高可用性ペアを解除します。高可用性/拡張性のアンインストール順序（58 ページ）を参照してください。
- 正常に展開され、通信が確立されていることを確認します。

ステップ 1 デバイスの設定が古い場合は、この時点で 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 に設定されていて、Threat Defense CLI にアクセスする場合は、次の表に示すような、追加の手順が必要になります。

Firepower 1000 シリーズ	`connect ftd`
Firepower 2100 シリーズ	`connect ftd`
Secure Firewall 3100 シリーズ	`connect ftd`
Firepower 4100/9300	`connect module` *slot_number* `console`、次に `connect ftd`（最初のログインのみ）

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

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

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

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

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

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

注意 確認を求められることはありません。このコマンドを入力すると、デバイスの再起動を含むアンインストールが開始されます。アンインストール時のトラフィック フローとインスペクションの中断は、アップグレード時に発生する中断と同じです。準備が整っていることを確認してください。`--detach` オプションを使用すると、SSH セッションがタイムアウトした場合にアンインストールプロセスが強制終了されなくなり、デバイスが不安定な状態になる可能性があることに注意してください。

ステップ 6 ログアウトするまでアンインストールを監視します。

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

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

それ以外の場合は、コンソールか端末で進行状況を監視します。

ステップ 7 アンインストールが成功したことを確認します。

アンインストールが完了したら、デバイスのソフトウェアバージョンが正しいことを確認します。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/スケーラビリティの展開では、ユニットごとに手順 2 から 6 を繰り返します。

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

ステップ 9 構成を再展開します。

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

次のタスク

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

スタンドアロン Management Center パッチのアンインストール

Management Center パッチのアンインストールには Web インターフェイスを使用することをお勧めします。Web インターフェイスを使用できない場合は、Linux シェルを、シェルの `admin` ユーザーまたはシェル アクセス権を持つ外部ユーザーのどちらかとして 使用できます。シェ

ルアクセスを無効にした場合は、 ロックダウンを元に戻すために Cisco TAC にご連絡ください。

⚠

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

始める前に

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

ステップ 1 構成が古い管理対象デバイスに展開します。

アンインストールする前に展開すると、失敗する可能性が減少します。

ステップ 2 [利用可能なアップデート（Available Updates）] で該当するアンインストールパッケージの横にある [インストール（Install）] アイコンをクリックして、Management Center を選択します。

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

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

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

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

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

ステップ 5 管理対象デバイスに構成を再展開します。

高可用性 Management Center パッチのアンインストール

Management Center パッチのアンインストールには Web インターフェイスを使用することをお勧めします。Web インターフェイスを使用できない場合は、Linux シェルを、シェルの `admin` ユーザーまたはシェル アクセス権を持つ外部ユーザーのどちらかとして 使用できます。シェ

ルアクセスを無効にした場合は、 ロックダウンを元に戻すために Cisco TAC にご連絡ください。

高可用性ピアから一度に1つずつアンインストールします。同期を一時停止した状態で、先にスタンバイからアンインストールし、次にアクティブからアンインストールします。スタンバイでアンインストールが開始されると、ステータスがスタンバイからアクティブに切り替わり、両方のピアがアクティブになります。この一時的な状態のことを「スプリットブレイン」と呼び、アップグレード中とアンインストール中を除き、サポートされていません。

⚠

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

始める前に

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

ステップ 1 アクティブな Management Center で、構成が古い管理対象デバイスに展開します。

アンインストールする前に展開すると、失敗する可能性が減少します。

ステップ 2 アクティブ状態の Management Center で、同期を一時停止します。

a) **[統合（Integration）] > [その他の統合（Other Integrations）]**を選択します。
b) [ハイ アベイラビリティ（High Availability）] タブで、[同期の一時停止（Pause Synchronization）] をクリックします。

ステップ 3 ピアからパッチを一度に 1 つずつアンインストールします。先にスタンバイで行い、次はアクティブで行います。

「スタンドアロン Management Center パッチのアンインストール （61 ページ）」の手順に従います。ただし、初期の展開は省略し、各ピアでアンインストールが成功したことを確認したら停止します。要約すると、各ピアで次の手順を実行します。

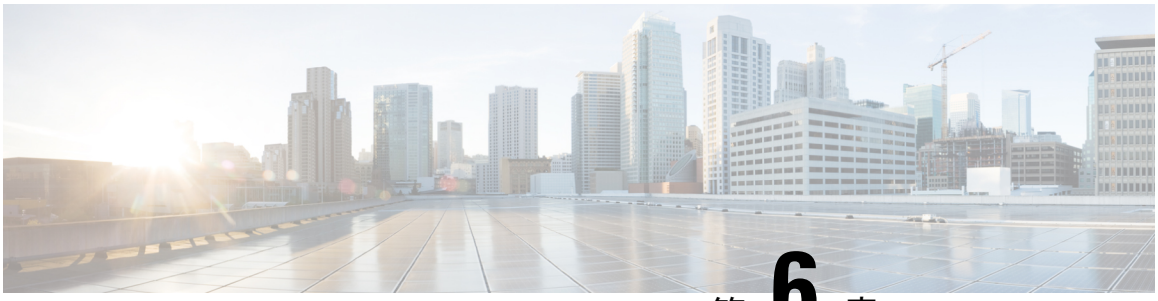
a) [システム（System）] > [更新（Updates）] ページで、パッチをアンインストールします。
b) ログアウトするまで進行状況を確認し、ログインできる状態になったら再びログインします。
c) アンインストールが成功したことを確認します。

ステップ 4 アクティブ ピアにする Management Center で、同期を再開します。

a) **[統合（Integration）] > [その他の統合（Other Integrations）]**を選択します。

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

ステップ 5 管理対象デバイスに構成を再展開します。



第 6 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 *20 :*

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。	アップグレードパッケージを直接ダウンロードするには、Management Center でインターネットにアクセスできる必要があります。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/設定していない場合も、空白のリストが表示されます。
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。

問題	解決方法
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）（Management Center がそのバージョン以降を実行しており、かつ、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）。これは、Management Center パッチにも適用されます。 • 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。
デバイスに適用されない、使用可能な、未ダウンロードのパッケージが表示されます。	この Management Center によって管理されるすべてのデバイスに適用されるダウンロード可能なアップグレードが一覧表示されます。マルチドメイン展開では、これに、現在アクセスできないデバイスが含まれる可能性があります。

Threat Defense のアップグレードのトラブルシューティング

表 *21 :*

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。

問題	解決方法
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）] > [デバイスのアップグレード（Device 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、Managagement 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 へのアップグレードパッケージのアップロードとダウンロード （6 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。マルチドメイン展開では、間違ったドメインにログインしている可能性があります。
デバイスが、他のユーザーのアップグレードワークフローにロックされる。	他のユーザーのワークフローをリセットする必要がある場合は、管理者アクセス権が必要です。次のいずれかの操作を実行できます。 • ユーザーを削除または非アクティブ化します。 • **システム**（⚙） > **[Product Upgrades]** を使用する権限がなくなるように、ユーザーのロールを更新します。

問題	解決方法
Managagement 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。 次のいずれかを試みることができます。 • 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します。 これを実行するには、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、代わりにその場所へのポインタ（URL）を指定します。内部サーバーから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。 • 別のデバイスからアップグレードパッケージをコピーします。 少なくとも 1 つのスタンドアロンデバイスにアップグレードパッケージを取得できる場合は、Threat Defense CLI（「peer to peer sync」）を使用して、同じスタンドアロン Managagement Center によって管理されている他のスタンドアロンデバイスにアップグレードパッケージをコピーできます。Threat Defense アップグレードパッケージのデバイス間のコピー （9 ページ） を参照してください。
アップグレードのセットアップ中に高可用性 Managagement Center がフェールオーバーする。	ワークフローも Threat Defense アップグレードパッケージも、高可用性 Management Center 間で同期されません。 フェールオーバーの場合は、新しいアクティブ Management Center でワークフローを再作成する必要があります。これには、アップグレードパッケージのダウンロードと、それらのデバイスへのコピーが含まれます（デバイスにコピー済みのアップグレードパッケージは削除されませんが、Management Center にアップロードパッケージまたはパッケージの格納場所へのポインタが必要です）。

無応答および失敗したアップグレード

無応答および失敗した Management Center のアップグレード

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

答しないなど、アップグレードで問題が発生した場合には Cisco TAC にお問い合わせください。

無応答および失敗した Threat Defense のアップグレード

（注） 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 *22：*

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。
Upgrade failed.	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。 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 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。
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。 ハイアベイラビリティ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。自動キャンセルは、バージョン 6.6 からのアップグレードではサポートされていません。

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 *23 :* 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。

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。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 （5 ページ）」を参照してください。

表 *24*：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 *25*：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。

注意 アップグレード中は、設定を変更または展開しないでください。システムが非アクティブに見えても、手動で再起動またはシャットダウンしないでください。ほとんどの場合、進行中のアップグレードを再開しないでください。システムが使用できない状態になり、再イメージ化が必要になる場合があります。アップグレードに失敗する、アプライアンスが応答しないなど、アップグレードで問題が発生した場合には、にお問い合わせください「無応答および失敗したアップグレード （68 ページ）」を参照してください。

表 *26*：アップグレード時間の考慮事項

考慮事項	詳細
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、イベントデータベースのサイズ、それらがアップグレードから影響を受けるかどうか、どのような影響を受けるかによって長くなります。たとえば、多くのアクセス制御ルールを使用している場合、アップグレードではそれらのルールの格納方法をバックエンドで変更する必要があるため、さらに長い時間がかかります。
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

アップグレードするには、アップグレードパッケージがアプライアンスにある必要があります。Management Center を使用するデバイスのアップグレードの場合は、Management Center（/Volume または /var のいずれか）にもデバイス 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。準備状況チェックで

は、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。

表 *27* : 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 *28* : バージョン *7.2.6* の機能

機能	最小 Management Center	最小 Threat Defense	詳細
アップグレード			

機能	最小 Management Center	最小 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。	7.2.6 7.4.1	いずれか	

機能	最小 Management Center	最小 Threat Defense	詳細
			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。これには、Management Center、Threat Defense デバイス、およびすべての古いNGIPSv/ASA FirePOWER デバイスが含まれます。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。 リスト/直接ダウンロードアップグレードパッケージを取得するには、インターネットアクセスが必要です。インターネットアクセスがない場合は、手動管理に限定されます。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**では、Management Center とすべての管理対象デバイス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。 • **[デバイスの脅威防御のアップグレード**>（**Devices 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。 • **システム**（⚙）> **[ユーザー（Users）]** > **[ユーザーロール（User Role）]** > **[ユーザーロールの作成（Create User Role）]** > **[メニューベースの権限（Menu-Based Permissions）]**を使用すると、[製品のアップグレード（Product Upgrades）]（システムソフトウェア）へのアクセスを許可せずに、[コンテンツの更新（Content Updates）]（VDB、GeoDB、侵入ルール ）へのアクセスを許可できます。 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。

機能	最小 Management Center	最小 Threat Defense	詳細
			その他のバージョンの制限：Management Center バージョン 7.3.x または 7.4.0 ではサポートされていません。 参照：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。	7.2.6 7.4.1	いずれか	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。 その他のバージョンの制限：Management Center バージョン 7.3.x または 7.4.0 ではサポートされていません。 参照： Cisco Secure Firewall Management Center の新機能（リリース別）
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。	7.2.6 7.4.1	いずれか	**アップグレードの影響。システムは新しいリソースに接続します。** 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。 その他のバージョンの制限：Management Center バージョン 7.3.x または 7.4.0 ではサポートされていません。 参照：「Internet Access Requirements」
Threat Defense のアップグレード			
Threat Defense のアップグレードウィザードからの復元の有効化。	7.2.6 7.4.1	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 7.1 以降にアップグレードする必要があります。Management Center バージョン 7.3.x または 7.4.0 ではサポートされていません。 参照：Management Center 用 Cisco Secure Firewall Threat Defense アップグレードガイド

機能	最小 Management Center	最小 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。	7.2.6	いずれか	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 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。	7.2.6 7.4.1	いずれか	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。 その他のバージョンの制限：Management Center バージョン 7.3.x または 7.4.0 ではサポートされていません。 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。	7.2.6	いずれか	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：Management Center 用 Cisco Secure Firewall Threat Defense アップグレードガイド

機能	最小 Management Center	最小 Threat Defense	詳細
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。	7.2.6	いずれか	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
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。	7.2.6	いずれか	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
Management Center のアップグレード			
Management Center の新しいアップグレードウィザード。	7.2.6 7.4.1	いずれか	新しいアップグレード開始ページとウィザードにより、Management Center のアップグレードを簡単に実行できます。**システム**（⚙）>**[製品のアップグレード（Product Upgrades）]** を使用して、Management Center で適切なアップグレードパッケージを入手したら、[アップグレード（Upgrade）] をクリックして開始します。 その他のバージョンの制限：バージョン 7.2.6 以降/7.4.1 以降からの Management Center のアップグレードでのみサポートされます。バージョン 7.3.x または 7.4.0 からのアップグレードではサポートされていません。 Management Center を任意のバージョンにアップグレードするには、Management Center で現在実行しているバージョンのアップグレードガイドを参照してください。：Management Center 用 Cisco Secure Firewall Threat Defense アップグレードガイド。バージョン 7.4.0 を実行している場合は、バージョン 7.3.x のガイドを使用できます。

機能	最小 Management Center	最小 Threat Defense	詳細
同期を一時停止することなく、高可用性管理センターでホットフィックスを利用できます。	7.2.6 7.4.1	いずれか	ホットフィックス リリース ノートに特に記載されていない、または Cisco TAC から指示されていない限り、高可用性 Management Center にホットフィックスをインストールするために同期を一時停止する必要はありません。 その他のバージョンの制限：Management Center バージョン 7.3.x または 7.4.0 ではサポートされていません。 参照：Management Center 用 Cisco Secure Firewall Threat Defense アップグレードガイド
コンテンツの更新（Content Updates）			
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。	7.2.6 7.4.1	いずれか	**アップグレードの影響。スケジュールされたダウンロードタスクは、メンテナンスリリースの取得を停止します。** [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。 その他のバージョンの制限：Management Center バージョン 7.3.x または 7.4.0 ではサポートされていません。 参照：「Software Update Automation」

機能	最小 Management Center	最小 Threat Defense	詳細
国コードの地理位置情報パッケージのみをダウンロードします。	7.2.6 7.4.0	いずれか	**アップグレードの影響。アップグレードすると、IP パッケージが削除される可能性があります。** バージョン 7.2.6 以降/7.4.0 以降では、IP アドレスを国や大陸にマッピングする地理位置情報データベース（GeoDB）の国コードパッケージのみをダウンロードするようにシステムを設定できます。コンテキストデータを含む大規模な IP パッケージはオプションになりました。 IP パッケージのダウンロードは次のとおりです。 • バージョン 7.2.0 ～ 7.2.5：常に有効。 • バージョン 7.2.6 ～ 7.2.x：デフォルトでは無効になっていますが、有効にすることができます。 • バージョン 7.3.x：常に有効。 • バージョン 7.4.0 ～ 7.4.1：デフォルトで有効になっていますが、無効にすることもできます。 ダウンロードがデフォルトで無効になっているバージョンに初めてアップグレードすると、システムはダウンロードを無効にし、既存の IP パッケージを削除します。IP パッケージがないと、オプションを手動で有効にして GeoDB を更新するまで、IP アドレスのコンテキスト地理位置情報データを表示できません。 新規/変更された画面： • バージョン 7.2.6/7.4.1：**システム**（⚙）**>[コンテンツの更新（Content Updates）] > [地理位置情報の更新（Geolocation Updates）]** • バージョン 7.4.0：**システム**（⚙）**> [更新（Updates）] > [地理位置情報の更新（Geolocation Updates）]** 参照：「Update the Geolocation Database」

表 *29 :* バージョン *7.2.0* の機能

機能	詳細
Threat Defense のアップグレード	

機能	詳細
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」）。	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、同じスタンドアロン 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。 • 高可用性 Management Center によって管理されるデバイス。 • クラウド提供型 Firewall Management Center によって管理されるが、分析モードでオンプレミス Management Center に追加されたデバイス。 • 異なるドメインのデバイス、または NAT ゲートウェイによって分離されたデバイス。 • Management Center のバージョンに関係なく、バージョン 7.1 以前からアップグレードするデバイス。 新規/変更された CLI コマンド：**configure p2psync enable**、**configure p2psync disable**、**show peers**、**show peer details**、**sync-from-peer**、**show p2p-sync-status**
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。	バージョン 7.2 以降の Management Center を使用して Threat Defense をバージョン 7.2 以降にアップグレードする場合、**Snort 2 から Snort 3 へのアップグレード**を実行するかどうかを選択できるようになりました。 ソフトウェアのアップグレード後、設定を展開すると、対象のデバイスが Snort 2 から Snort 3 にアップグレードされます。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、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。ヘルプについては、ご使用のバージョンの Cisco Secure Firewall Management Center Snort 3 Configuration Guide を参照してください。 バージョンの制限：Threat Defense のバージョン 7.0.x または 7.1.x へのアップグレードはサポートされていません。

機能	詳細
単一ノードクラスタのアップグレード。	デバイスのアップグレードページ（[デバイス（Devices）] > [デバイスのアップグレード（Device Upgrade）]）を使用して、アクティブノードが1つだけのクラスタをアップグレードできるようになりました。非アクティブ化されたノードもアップグレードされます。以前は、このタイプのアップグレードは失敗していました。この機能は、システムの更新ページ（**システム**（⚙）**[更新（Updates）]**）ではサポートされていません。 この場合、ヒットレスアップグレードもサポートされません。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。 サポートされるプラットフォーム：Firepower 4100/9300、Secure Firewall 3100
CLIからの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た場合、デバイスの CLI から Threat Defense のアップグレードを元に戻すことができるようになりました。高可用性や拡張性の展開では、すべてのユニットを同時に復元すると、復元が成功する可能性が高くなります。CLIを使用して復元する場合は、すべてのユニット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。 **注意** 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。 新規/変更された CLI コマンド：**upgrade revert**、**show upgrade revert-info**。
Management Center のアップグレード	
Management Centerのアップグレードでは、トラブルシューティングファイルは自動的に生成されません。	時間とディスク容量を節約するために、管理センターのアップグレードプロセスでは、アップグレードの開始前にトラブルシューティング ファイルを自動的に生成しなくなりました。デバイスのアップグレードは影響を受けず、引き続きトラブルシューティング ファイルが生成される点に注意してください。 管理センター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 [Firewall Management Center] をクリックし、[View System & Troubleshoot Details]、[Generate Troubleshooting Files] を選択します。
コンテンツの更新（Content Updates）	

機能	詳細
GeoDB を 2 つのパッケージに分割。	2022 年 5 月、バージョン 7.2 リリースの直前に、GeoDB が 2 つのパッケージに分割されました。IP アドレスを国/大陸にマッピングする国コードパッケージと、ルーティング可能な IP アドレスに関連付けられた追加のコンテキストデータを含む IP パッケージです。IP パッケージのコンテキストデータには、追加のロケーションの詳細に加えて、ISP、接続タイプ、プロキシタイプ、ドメイン名などの接続情報を含めることができます。 バージョン 7.2.0 から 7.2.5 までの Management Center にインターネットアクセスがあり、定期的な更新を有効にしている場合、または シスコ サポートおよびダウンロード サイト から 1 回限りの更新を手動で開始した場合、両方のパッケージが自動的に取得されます。バージョン 7.2.6 以降または 7.4.0 以降では、システムに IP パッケージを取得させるかどうかを設定できます。 エアギャップ展開などで更新を手動でダウンロードする場合、パッケージを個別にインポートする必要があります。 • 国コードパッケージ：Cisco_GEODB_Update-*date-build*.sh.REL.tar • IP パッケージ：Cisco_IP_GEODB_Update-*date-build*.sh.REL.tar **[ヘルプ（Help）]**（?）>**[バージョン情報（About）]** には、システムで現在使用されているパッケージのバージョンが一覧表示されます。

表 ***30 :*** バージョン ***7.1.0*** の機能

機能	詳細
Threat Defense のアップグレード	

機能	詳細
正常なデバイスアップグレードを元に戻します。	メジャーおよびメンテナンスアップグレードを FTD に戻すことができるようになりました。復元すると、ソフトウェアは、最後のアップグレードの直前の状態に戻ります（スナップショットとも呼ばれます）。パッチのインストール後にアップグレードを元に戻すと、パッチだけでなく、メジャーアップグレードやメンテナンスアップグレードも元に戻されます。 **重要** 元に戻す必要がある可能性があると思われる場合は、**システム**（⚙）> **[更新（Updates）]** ページを使用して FTD をアップグレードする必要があります。[システムの更新（System Updates）] ページは、[アップグレード後の復元を有効にする（Enable revert after successful upgrade）] オプションを有効にできる唯一の場所です。このオプションでは、アップグレードの開始時に復元スナップショットを保存するようにシステムが設定されます。これは、[デバイス（Devices）]>[デバイスのアップグレード（Device Upgrade）] ページでウィザードを使用する通常の推奨とは対照的です。 この機能は、コンテナインスタンスではサポートされません。 必要最低限の FTD：7.1
クラスタ化された高可用性デバイスのアップグレードワークフローの改善。	クラスタ化された高可用性デバイスのアップグレードワークフローが次のように改善されました。 • アップグレードウィザードは、個々のデバイスとしてではなく、グループとして、クラスタ化された高可用性ユニットを正しく表示するようになりました。システムは、発生する可能性のあるグループ関連の問題を特定し、報告し、事前に修正を要求できます。たとえば、Firepower Chassis Manager で非同期の変更を行った場合は、Firepower 4100/9300 のクラスタをアップグレードできません。 • アップグレードパッケージをクラスタおよび高可用性ペアにコピーする速度と効率が向上しました。以前は、FMC はパッケージを各グループメンバーに順番にコピーしていました。これで、グループメンバーは通常の同期プロセスの一部として、相互にパッケージを取得できるようになりました。 • クラスタ内のデータユニットのアップグレード順序を指定できるようになりました。コントロールユニットは常に最後にアップグレードされます。

表 *31* : バージョン *7.0.0* の機能

機能	詳細
Threat Defense のアップグレード	

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

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

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

表 *32* : バージョン *6.7.0* の機能

機能	詳細
Threat Defense のアップグレード	
アップグレードでディスク容量を節約するためにPCAPファイルが削除される。	アップグレードにより、ローカルに保存された PCAP ファイルが削除されるようになりました。アップグレードするには、十分な空きディスク容量が必要です。これがない場合、アップグレードは失敗します。

機能	詳細
FTDアップグレードステータス レポートとキャンセル/再試行オプションの改善。	[デバイス管理（Device Management）] ページで、進行中の FTD デバイスアップグレードと準備状況チェックのステータス、およびアップグレードの成功/失敗の 7 日間の履歴を確認できるようになりました。メッセージセンターでは、拡張ステータスとエラーメッセージも提供されます。 デバイス管理とメッセージセンターの両方からワンクリックでアクセスできる新しい [Upgrade Status] ポップアップに、残りのパーセンテージ/時間、特定のアップグレード段階、成功/失敗データ、アップグレードログなどの詳細なアップグレード情報が表示されます。 また、このポップアップで、失敗したアップグレードまたは進行中のアップグレードを手動でキャンセル（[Cancel Upgrade]）することも、失敗したアップグレードを再試行（[Retry Upgrade]）することもできます。アップグレードをキャンセルすると、デバイスはアップグレード前の状態に戻ります。 （注） 失敗したアップグレードを手動でキャンセルまたは再試行できるようにするには、FMC を使用して FTD デバイスをアップグレードするときに表示される新しい自動キャンセルオプションを無効にする必要があります（[Automatically cancel on upgrade failure and roll back to the previous version]）。オプションを有効にすると、アップグレードが失敗した場合、デバイスは自動的にアップグレード前の状態に戻ります。 パッチの自動キャンセルはサポートされていません。HA 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。 新規/変更された画面： • FTD アップグレードパッケージの **システム**（⚙） > **[更新（Updates）]** > **[製品の更新（Product Updates）]** > **[使用可能な更新（Available Updates）]** > **[インストール（Install）]** アイコン • **[Devices]** > **[Device Management]** > **[Upgrade]** • **[Message Center] > [Tasks]** 新規/変更された CLI コマンド：**show upgrade status detail**、**show upgrade status continuous**、**show upgrade status**、**upgrade cancel**、**upgrade retry**
コンテンツの更新（Content Updates）	

機能	詳細
カスタム侵入ルールのインポートでルール競合の際に警告表示。	カスタム（ローカル）侵入ルールをインポートする場合、FMC がルールの競合について警告するようになりました。以前は、システムは競合の原因となるルールをサイレントにスキップしていました。ただし、競合のあるルールのインポートが完全に失敗するバージョン 6.6.0.1 は除きます。 [ルールの更新（Rule Updates）] ページで、ルールのインポートに競合があった場合は、[ステータス（Status）] 列に警告アイコンが表示されます。詳細については、警告アイコンの上にポインタを置いて、ツールチップを参照してください。 既存のルールと同じ SID/リビジョン番号を持つ侵入ルールをインポートしようとすると、競合が発生することに注意してください。カスタムルールの更新バージョンには必ず新しいリビジョン番号を付けてください。 新規/変更された画面：**システム**（⚙） > **[更新（Updates）]** > **[ルールの更新（Rule Updates）]**に警告アイコンが追加されました。

表 ***33 :*** バージョン ***6.6.0*** の機能

機能	詳細
Threat Defense のアップグレード	
内部 Web サーバーから FTD アップグレードパッケージを取得します。	FTD デバイスは、FMC からではなく、独自の内部 Web サーバーからアップグレードパッケージを取得できるようになりました。これは、FMC とそのデバイスの間の帯域幅が制限されている場合に特に役立ちます。また、FMC 上の領域も節約できます。 （注） この機能は、バージョン 6.6+ を実行している FTD デバイスでのみサポートされています。バージョン 6.6 へのアップグレードではサポートされておらず、FMC または従来のデバイスでもサポートされていません。 新規/変更された画面：アップグレードパッケージをアップロードするページに、[ソフトウェアアップデートソースの指定（Specify software update source）] オプションを追加しました。
コンテンツの更新（Content Updates）	
初期セットアップ中の自動VDB更新。	新規または再イメージ化された FMC をセットアップすると、システムは自動的に脆弱性データベース（VDB）の更新を試みます。 これは1回限りの操作です。FMCがインターネットにアクセスできる場合は、自動の定期 VDB 更新のダウンロードとインストールを実行するようにタスクをスケジュールしておくことを推奨します。

表 *34* : バージョン *6.5.0* の機能

機能	詳細
コンテンツの更新（Content Updates）	
ソフトウェアの自動ダウンロードと GeoDB の更新。	新規または再イメージ化された FMC を設定すると、システムは自動的に次のスケジュールを設定します。 • FMC とその管理対象デバイスのソフトウェアアップデートをダウンロードする週次タスク。 • GeoDB の週次更新。 タスクは UTC でスケジュールされるため、いつ現地で実行されるかは、日付と場所によって異なります。また、タスクは UTC でスケジュールされるため、サマータイムなど、所在地で実施される場合がある季節調整に合わせて調節されることもありません。このような影響を受ける場合、スケジュールされたタスクは、現地時間を基準とすると、夏期では冬期の場合よりも 1 時間「遅れて」実行されることになります。自動スケジュール設定を確認し、必要に応じて調整することをお勧めします。

表 *35* : バージョン *6.4.0* の機能

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

機能	詳細
署名済みのSRU、VDB、およびGeoDBの更新。	正しい更新ファイルを使用していることが確認できるため、バージョン6.4以降では署名済みの更新を侵入ルール（SRU）、脆弱性データベース（VDB）、および地理位置情報データベース（GeoDB）が使用されます。以前のバージョンでは、引き続き未署名の更新が使用されます。 シスコ サポートおよびダウンロードサイトから手動で更新をダウンロードしない限り（たとえば、エアギャップ導入環境の場合）、機能の違いはわかりません。ただし、SRU、VDB、およびGeoDBの更新を手動でダウンロードしてインストールする場合は、必ず現在のバージョンに対応した正しいパッケージをダウンロードしてください。 署名付きの更新ファイルの先頭は、以下のように「Sourcefire」ではなく「Cisco」で、末尾は .sh ではなく .sh.REL.tar です。 • SRU：Cisco_Firepower_SRU-*date-build*-vrt.sh.REL.tar • VDB：Cisco_VDB_Fingerprint_Database-4.5.0-*version*.sh.REL.tar • GeoDB：Cisco_GEODB_Update-*date-build*.sh.REL.tar シスコは、署名なしの更新を必要とするバージョンのサポートが終了するまで、署名付きと署名なしの両方の更新を提供します。署名付きの（.tar）パッケージは解凍しないでください。古い FMC または ASA FirePOWER デバイスに署名付きの更新を誤ってアップロードした場合は、手動で削除する必要があります。パッケージを残しておくと、ディスク領域が占有されるため、今後のアップグレードで問題が発生する可能性もあります。

表 *36 :* バージョン *6.2.3* の機能

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

機能	詳細
VDB の更新前に、Snort の再起動について FMC から警告されます。	脆弱性データベース（VDB）の更新で Snort プロセスが再起動することが、FMC から警告されるようになりました。これにより、トラフィック インスペクションが中断され、管理対象デバイスによるトラフィックの処理方法によっては、トラフィックフローが中断される可能性があります。メンテナンス期間中など、都合の良い期間までインストールをキャンセルすることができます。 次のようなときに警告が表示される可能性があります。 • VDB をダウンロードして手動でインストールした後。 • スケジュールされたタスクを作成して VDB をインストールする場合。 • たとえば、以前にスケジュールされたタスクの実行中に、またはソフトウェアアップグレードの一部として、VDB がバックグラウンドでインストールされる場合。

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。