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。

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。