アップグレードの計画

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

互換性

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

互換性情報については、次を参照してください。

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

アップグレードのガイドライン

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

ソフトウェアのアップグレードガイドライン

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

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

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

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

アップグレードパス

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

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

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

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

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

サポートされる直接アップグレード

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

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

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

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

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

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

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

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

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

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

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

アップグレードパッケージ

Management Center でのアップグレードパッケージの管理

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

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

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

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

デバイスへのアップグレードパッケージのコピー

アップグレードするには、アップグレードパッケージがデバイスにある必要があります。

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

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

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

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

次の表に、このオプションとその他のオプションの詳細を示します。

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

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

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

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

内部サーバーからデバイスへのアップグレードパッケージのコピー

Threat Defense のアップグレードパッケージは、Management Center ではなく内部サーバーに保存できます。これは、Management Center とそのデバイスの間の帯域幅が制限されている場合に特に役立ちます。また、Management Center 上の容量も節約できます。

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

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

フィールド	説明
URL	プロトコル（HTTP/HTTPS）およびアップグレードパッケージへのフルパスを含む送信元 URL。次に例を示します。 `https://internal_web_server/upgrade_package.sh.REL.tar`
CA 証明書	セキュア Web サーバー（HTTPS）の場合は、サーバーのデジタル証明書（PEM 形式）。 テキストブロック全体（BEGIN CERTIFICATE 行と END CERTIFICATE 行を含む）をコピーして貼り付けます。サーバーの管理者から証明書を取得できるようにする必要があります。また、ブラウザまたは OpenSSL などのツールを使用して、サーバーの証明書の詳細を表示したり、証明書をエクスポートまたはコピーしたりすることもできます。

Threat Defense アップグレードパッケージのデバイス間のコピー

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

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

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

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

Before you begin

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

Procedure

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

ステップ 2 機能を有効にします。

configure p2psync enable

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

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

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

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

sync-from-peer *ip_address package_path*

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

ステップ 5 CLI から転送ステータスをモニタリングします。

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

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

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

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

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

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

Before you begin

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

Procedure

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

ステップ 2 不要なパッケージがあるシャーシを選択し、[アクションの選択（Select Action）] または [一括アクションの選択（Select Bulk Action）] で、[FXOS とファームウェアのアップグレード（シャーシのみ）（Upgrade FXOS and Firmware (Chassis Only)）] を選択します。

シャーシ アップグレード ウィザードが表示されます。

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

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

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

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

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

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

クリーンアップするシャーシごとにこの手順を繰り返してください。

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

Cisco.com のアップグレードパッケージ

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

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

Threat Defense パッケージ

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

表 7: アップグレードパッケージ

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

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

Secure Firewall 3100 のシャーシパッケージ

の場合、脅威防御とシャーシのアップグレードはパッケージを共有します。

Firepower 4100/9300 用シャーシパッケージ

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

表 *8 : FXOS* パッケージ

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

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

表 *9 :* ファームウェアパッケージ

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

アップグレードの準備状況

インフラストラクチャとネットワークの確認

アプライアンス アクセス

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

帯域幅

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

設定と展開の確認

設定

必要なアップグレード前の設定変更を行っていることを確認し、必要なアップグレード後の設定変更を行う準備をします。変更管理ワークフローを決定します。設定変更を展開します。アップグレード後に再度展開する必要があり、通常は Snort が再起動されることに注意してください。「設定展開時のトラフィックフローとインスペクション」を参照してください。

展開の正常性

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

バックアップ

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

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

表 *10*：バックアップ

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

ソフトウェアアップグレード準備状況チェック

ユーザーが自分で実行するチェックに加えて、システムも、独自のアップグレード準備状況チェックを実行できます。Threat Defense アップグレードウィザードでは、適切なタイミングでチェックを実行するように求められます。準備状況チェックは無効にできますが、推奨されません。すべてのチェックに合格すると、アップグレードが失敗する可能性が大幅に減少しま

す。チェックの結果、解決できない問題が見つかった場合は、アップグレードを開始しないでください。

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

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。