



アップグレードの計画

このガイドを使用して、Firewall Threat Defense のアップグレードを計画して完了します。アップグレードには、マイナー (A.x) 、メンテナンス (A.x.y) 、脆弱性 (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](#) (1 ページ)
- [アップグレードのガイドライン](#) (1 ページ)
- [アップグレードパス](#) (2 ページ)
- [アップグレード順序](#) (4 ページ)
- [アップグレードパッケージ](#) (7 ページ)
- [アップグレードの準備状況](#) (16 ページ)

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、「[Cisco Secure Firewall Threat Defense 互換性ガイド](#)」を参照してください。

アップグレードのガイドライン

以下のトピックでのガイドラインとリソースリンクに加えて、時間とディスク容量の要件に関する一般的な情報、およびトラフィックフローや検査の中断を含むアップグレード中のシステム動作の詳細については、「[参照先](#)」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

Firewall Threat Defense の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、<http://www.cisco.com/go/ftd-notes> で、現在のバージョンからターゲットバージョンまでのすべてのリリースノートを確認してください。

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、FXOS のメジャーバージョンの最新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、現在のバージョンと対象バージョン間の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。

Firewall Threat Defense Virtual のアップグレードガイドライン

アップグレードしても、Firewall Threat Defense Virtual インスタンスのシリアル番号や UUID は変更されません。

クラスターをアップグレードする前に、ベースイメージとテンプレートイメージ ID を更新します。

パブリッククラウドでクラスターをアップグレードする前に、ターゲットバージョンのイメージをクラウドイメージリポジトリにコピーし、クラスター展開テンプレートのイメージ ID を更新します (実際には、既存のテンプレートを変更したコピーで置き換えることを推奨します)。これにより、アップグレード後に新しいインスタンス (クラスタースケリング中に起動されたインスタンスなど) が正しいバージョンを使用ようになります。クラスターにパッチが適用されている場合など、必要なイメージがマーケットプレイスにない場合は、インスタンス固有 (Day 0) の設定がなく、正しいバージョンを実行しているスタンドアロンの Firewall Threat Defense Virtual インスタンスのスナップショットからカスタムイメージを作成します。

自動スケリングされたクラスターをアップグレードする前に、正常性チェックを一時停止します。

AWS 向け Firewall Threat Defense Virtual の場合、自動スケリングされたクラスターのアップグレードの前に HealthCheck プロセスと ReplaceUnhealthy プロセスを一時停止します。これにより、アップグレード後の再起動中に Auto Scaling グループによってインスタンスが終了されなくなります。一時停止したプロセスは、後で再開できます。手順については、Amazon EC2 Auto Scaling のユーザーガイドの「[Suspend and resume Amazon EC2 Auto Scaling processes](#)」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と発注は、大規模展開、高可用性/クラスターリング、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。

アップグレードターゲットの選択

可能な限り最新のリリースに直接移行することで、アップグレードなどの影響を最小限に抑えます。機能、拡張機能、および重要な修正は、リリース日ではなくバージョンで先行する「今後」のリリースをスキップできるためです。たとえば、メジャーバージョン A 内で最新の場合、ドットゼロバージョン B にアップグレードすると、機能や修正が廃止される可能性があります。

最新のリリースに移行できない場合、少なくとも現在のバージョンがターゲットバージョンより前の日付でリリースされたことを確認してください。ターゲットバージョンについては、[Cisco Secure Firewall Threat Defense リリースノート](#)を参照してください。

パッチが適用された展開のアップグレード

パッチ/脆弱性（4桁）リリースに含まれる重要な修正は、今後のリリースをスキップすることもできます。これらの重要な修正に依存している場合は、ターゲットバージョンにそれらが含まれていることを確認してください。リリース日の完全なリストについては、[Cisco Secure Firewall Management Center の新機能（リリース別）](#)を参照してください。

サポートされているアップグレードおよびダウングレード

このセクションでは、アップグレードおよびダウングレード機能の概要について説明します。

サポートされるアップグレード

次の表に、Firewall 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。



（注） パッチは4桁目のみを変更できます。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。

表 1: サポート対象の直接アップグレード

現在のバージョン	ターゲット Firewall Threat Defense バージョン					
	10.x へ	7.7 へ	7.6 へ	7.4 へ	7.3 へ	7.2 へ
10.x から	対応	—	—	—	—	—
7.7 から	対応	対応	—	—	—	—
7.6 から	対応	対応	対応	—	—	—
7.4 から	対応	対応	対応	対応 *	—	—

現在のバージョン	ターゲット Firewall Threat Defense バージョン					
	10.x へ	7.7 へ	7.6 へ	7.4 へ	7.3 へ	7.2 へ
7.3 から	対応	対応	対応	対応	対応	—
7.2 から	—	対応	対応	対応	対応	対応

Firepower 4100/9300 アップグレードでサポートされている FXOS バージョン

Firepower 4100/9300 の場合、この表には、対応する FXOS バージョンが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、Firewall 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 2: Firepower 4100/9300 アップグレードでサポートされている FXOS バージョン

ターゲット Firewall Threat Defense バージョン	FXOS の最小バージョン
10.x	2.18.0
7.7	2.17.0
7.6	2.16.0
7.4.1 ~ 7.4.x	2.14.1
7.4.0	—
7.3	2.13.0
7.2	2.12.0

サポートされるダウングレード

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、以前のバージョンに戻せることがあります。「[Firewall Threat Defense の復元](#)」を参照してください。

アップグレード順序

Firewall Threat Defense の前にシャーシ

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 Firewall 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 Firewall Threat Defense のアップグレードが含まれており、クラウド提供型 Firewall 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 Firewall Threat Defense のみのアップグレードを実行することが可能です。

- 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Firewall 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。

高可用性/クラスタ化シャーシ Firewall Threat Defense

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。高可用性を確保するには、常にスタンバイをアップグレードすることがベストプラクティスですが、シャーシには、スタンバイインスタンスとアクティブインスタンスの両方（異なる高可用性ペアに属する）を設定することができます。この場合、アップグレード中のシャーシ上のアクティブなユニットが自動的にフェールオーバーします。クラスタリングの場合も同様です。データ専用ユニットのシャーシをアップグレードすることが常に最適です。

アップグレードする前に、高可用性ペアおよびクラスタは、スプリットブレインなどではなく、同期している必要があります。このような問題があると、ほとんどの場合に Firewall Threat Defense のアップグレードは続行されませんが、シャーシは自身のインスタンスのステータスを認識しません。つまり、シャーシを一度にアップグレードする場合でも、各シャーシのアップグレードの前に展開が正常であることを確認しなければ、中断が発生する可能性があります。

表 3: Firepower 4100/9300 シャーシのアップグレード順序

Firewall 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. Firewall Threat Defense をアップグレードします。

Firewall Threat Defense の導入	アップグレード順序
ハイ アベイラビリティ	Firewall 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. Firewall 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. Firewall 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）	Firewall 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. すべての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. Firewall Threat Defense をアップグレードします。

表 4: マルチインスタンスモードでの *Secure Firewall 3100/4200* のシャーシのアップグレード順序

Firewall 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. Firewall Threat Defense をアップグレードします。

Firewall Threat Defense の導入	アップグレード順序
ハイ アベイラビリティ	Firewall 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。 • 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） ベストプラクティス：スタンバイ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、ヘルスを確認し、新しいスタンバイを搭載したシャーシをアップグレードします。この方法は中断のリスクが最も低いです。 • シリアルアップグレード 条件付きで推奨。アクティブユニットがダウンすると自動的にフェールオーバーします。シリアルアップグレードを使用する場合は、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します。これにより、並行アップグレードの完全な中断は回避されますが、最初のシャーシが復旧した後、高可用性が再同期される前にセカンダリシャーシがアップグレードを開始すると、問題が発生する可能性があります。 • 並行アップグレード 高可用性環境には推奨されません。 2. Firewall 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

クラウド提供型 Firewall Management Center によるアップグレードパッケージの管理

[管理 (Administration)] > [アップグレードと更新 (Upgrades & updates)] > [製品アップグレード (Product Upgrades)] には利用可能なすべてのアップグレードが一覧表示されます（推奨リリースには特別なマークが付いています）。簡単にパッケージを選択してインターネットから直接クラウド提供型 Firewall Management Center に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。詳細については、次の表を参照してください

い。一般的な問題の解決策については、「[アップグレードパッケージのトラブルシューティング \(14 ページ\)](#)」を参照してください。



- (注) インターネットにアクセスできるデバイスは、クラウド提供型 Firewall Management Center のパッケージなしでアップグレードできます。デバイスは適切な時期にパッケージを取得します。「[デバイスへのアップグレードパッケージのコピー \(9 ページ\)](#)」を参照してください。

表 5: クラウド提供型 Firewall Management Center によるアップグレードパッケージの管理

目的	作業
利用可能なアップグレード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。
インターネットからクラウド提供型 Firewall Management Center にアップグレードパッケージを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クラウド提供型 Firewall 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。 参照: アップグレードパッケージの手動ダウンロード (13 ページ)
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。 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 (11 ページ)
デバイスがインターネットではなくクラウド提供型 Firewall Management Center からアップグレードパッケージを取得するように設定します。	[グローバルアップグレード設定 (Global upgrade settings)] をクリックし、[デバイスにサポートサイトからのダウンロードを許可 (Allow devices to download from the support site)] オプションを無効にします。 デフォルトでは、インターネットにアクセスできるデバイスは、内部サーバーからのダウンロードが失敗した場合のフォールバックを含め、クラウド提供型 Firewall Management Center の前にインターネットからアップグレードパッケージをダウンロードします。 参照: デバイスへのアップグレードパッケージのコピー (9 ページ)

目的	作業
部分的なダウンロードの再試行時間を設定します。	[グローバルアップグレード設定 (Global upgrade settings)] をクリックし、[失敗したダウンロードの再試行 (Retry failed downloads for)] ドロップダウンリストからオプションを選択します。 インターネット (クラウド提供型 Firewall Management Center とデバイス) または内部サーバー (デバイスのみ) からの部分的なダウンロードは保存され、指定した間隔で再試行されます。デフォルトは 24 時間です。 この設定は、管理ネットワークを介したクラウド提供型 Firewall Management Center からのデバイスダウンロードには適用されません。 デバイスダウンロードの場合、再試行するにはバージョン 7.4.3、7.6.1、または 7.7.0 以降が必要です。
クラウド提供型 Firewall 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、クラウド提供型 Firewall 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 3100/4200 からのシャーシアップグレードパッケージの削除 (12 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。

Firewall Threat Defense 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デバイスを選択すると、アップグレードウィザードからアップグレードパッケージをコピーするよう求められます。デバイスは、次のソースを順番に試します。いずれかが失敗すると、通常、デバイスは次のソースを試します。

内部サーバー。

設定されている場合、内部サーバーが優先されます。インターネットまたはクラウド提供型 Firewall Management Center からアップグレードパッケージを取得することが不可能または現実的ではない場合に推奨されます。たとえば、デバイスがインターネットにアクセスできない場合、クラウド提供型 Firewall Management Center に十分なディスク容量がない場合、またはデバイスとダウンロード場所間の帯域幅が不足している場合などです。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。

内部サーバーからのダウンロードに失敗した場合は、インターネットにアクセスできる新しいデバイス（Firewall Threat Defense 7.6 以降またはシャーシ 7.4.1 以降）で次に試してください。古いデバイスやインターネットにアクセスできないデバイスでは、クラウド提供型 Firewall Management Center を試してください。

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](#)（11 ページ）

インターネット。ほとんどのケースで推奨。

デバイスがインターネットにアクセスでき、デバイスとダウンロード場所の間に十分な帯域幅がある場合に推奨されます。インターネットアクセスは毎週テストされます。ホットフィックスではサポートされていません。

デフォルトでは、インターネットにアクセスできるデバイスはクラウド提供型 Firewall Management Center の前にインターネットを試します。ただし、デバイスのインターネットアクセスが低速または不安定な場合は、グローバルアップグレード設定を使用して、デバイスにクラウド提供型 Firewall Management Center からアップグレードパッケージを取得させることができます。インターネットからのダウンロードが失敗すると、デバイスはクラウド提供型 Firewall Management Center を試します。

参照：[クラウド提供型 Firewall Management Center によるアップグレードパッケージの管理](#)（7 ページ）

クラウド提供型 Firewall Management Center。

デバイスがインターネットに到達できないか、インターネットアクセスが低速または不安定であるが、クラウド提供型 Firewall Management Center に十分なディスク容量があり、クラウド提供型 Firewall Management Center とデバイスの間に十分な帯域幅がある場合に推奨されます。内部サーバーからのダウンロードまたは直接ダウンロードが失敗した場合のフォールバックとして、デバイス アップグレード パッケージをクラウド提供型 Firewall Management Center に保存することもできます。

クラウド提供型 Firewall Management Center は、ほとんどのデバイスアップグレードパッケージをインターネットから直接取得できます。ホットフィックスを適用している場合は、アップグレードパッケージを手動でアップロードします。

参照：[クラウド提供型 Firewall Management Center によるアップグレードパッケージの管理](#)（7 ページ）

シャーシ アップグレード パッケージのコピー

については、前述の Firewall Threat Defense の方法を使用します。これらのシャーシ 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 Firewall 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。

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 サポートおよびダウンロード サイト からアップグレードパッケージを手動でダウンロードし、Firewall Chassis Manager 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。[アップグレードパッケージの手動ダウンロード（13 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

インターネットにアクセスできない管理対象デバイスは、クラウド提供型 Firewall Management Center または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必要があります。内部サーバーは、クラウド提供型 Firewall Management Center とそのデバイス間（またはデバイスとインターネット ダウンロード ロケーション間）で帯域幅が制限されている場合に特に役立ちます。また、クラウド提供型 Firewall Management Center 上の容量も節約できます。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。

アップグレードパッケージ（[アップグレードパッケージの手動ダウンロード（13 ページ）](#)）を取得してサーバーをセットアップしたら、ポインタを設定します。クラウド提供型 Firewall 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（[管理（Administration）]>[アップグレードと更新（Upgrades & updates）]>[製品アップグレード（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、コンピューター上のファイルを選択するのではなく、[リモートロケーションの指定（Specify Remote Location）]をクリックして、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。



- (注) 設定すると、内部サーバーが優先されます。内部サーバーからのコピーが失敗した場合は、インターネットにアクセスできる新しいデバイス（Firewall Threat Defense 7.6 以降またはシャーシ 7.4.1 以降）で、インターネットに接続してからクラウド提供型 Firewall Management Center を試してください。ただし、グローバルアップグレード設定でサポートサイトからのダウンロードを無効にしている場合を除きます。古いデバイスやインターネットにアクセスできないデバイスでは、クラウド提供型 Firewall Management Center を試してください。

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

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。 <code>https://internal_web_server/upgrade_package.sh.REL.tar</code>

フィールド	説明
CA certificates	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。

Secure Firewall 3100/4200 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 Firewall 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。



- (注) 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。

始める前に

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。

手順

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。[詳細 (Details)] 列には、不要な可能性のあるパッケージを含むシャーシが表示されます。

ステップ4 影響を受けるシャーシを表示するには、[警告 (Warning)] フィルタを使用します。

ステップ5 フィルタ処理されたビューで、シャーシの横にある [パッケージの表示とクリーンアップ (View and clean up packages)] をクリックし、削除するパッケージを選択してから、[選択したパッケージの削除 (Delete selected packages)] 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。

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。

アップグレードパッケージの手動ダウンロード

別の理由（たとえば、ホットフィックス、Firepower 4100/9300 シャーシのアップグレード、または内部サーバーの使用など）により直接ダウンロードできない場合、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。

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
Firepower 1000	Cisco_FTD_SSP-FP1K_Upgrade-Version-build.sh.REL.tar

プラットフォーム	パッケージ
Firepower 2100 最終サポート：バージョン 7.4.x	Cisco_FTD_SSP-FP2K_Upgrade-Version-build.sh.REL.tar
Firepower 4100/9300	Cisco_FTD_SSP_Upgrade-Version-build.sh.REL.tar
Cisco Secure Firewall 200	Cisco_Secure_FW_TD_200-Version-build.sh.REL.tar
Cisco Secure Firewall 1200	Cisco_Secure_FW_TD_1200-Version-build.sh.REL.tar
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
Cisco Secure Firewall 6100	Cisco_Secure_FW_TD_6100-Version-build.sh.REL.tar
FTD を使用した ISA 3000	Cisco_FTD_Upgrade-Version-build.sh.REL.tar
Threat Defense Virtual	Cisco_FTD_Upgrade-Version-build.sh.REL.tar

Secure Firewall 3100/4200 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

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 9: アップグレードパッケージのトラブルシューティング

問題	解決方法
更新しても使用可能なアップグレードがありません。	現在の展開で使用可能な最新バージョンをすでに実行しており、かつ、アップグレードパッケージをロード/設定していません。

問題	解決方法
推奨リリースがマークされていません。	推奨リリースは、対象となる場合にのみ一覧表示されます。推奨リリース以降をすでに実行している場合、またはそこまでアップグレードできない場合は、一覧表示されません。推奨リリースへのパッチは推奨としてマークされませんが、適用することをお勧めします。
必要なパッケージが表示されません。	現在の展開に適用されるメジャー、メンテナンス、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。これらは、手動でアップロードしない限り表示されません。 - 特定の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）は、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き、表示されません。 - デバイスパッチは、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き、表示されません。 - 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。
パッケージがページから削除されました。	クラウド提供型 Firewall Management Center のインスタンスがアップグレードされると、ローカルに保存されているアップグレードパッケージは削除されます。これには、直接再度ダウンロードできないパッケージが含まれます。たとえば、廃止されたリリース、展開に適用されなくなったリリース、管理対象デバイスに引き続き適用する必要があるホットフィックスなどです。引き続き必要なサポートされているパッケージをアップロードします。インスタンスがアップグレードされたかどうかを確認するには、 Security Cloud Control の新機能 をチェックしてください。
クラウド提供型 Firewall Management Center から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します。	これは、多くの場合、クラウド提供型 Firewall 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、クラウド提供型 Firewall Management Center からアップグレードパッケージを削除し（これは任意ですが、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。内部サーバーからデバイスへのアップグレードパッケージのコピー（11 ページ） を参照してください。 - デバイスがインターネットからアップグレードパッケージをダウンロードできるようにします。 インターネットにアクセスできるデバイスは、まずインターネットからのダウンロードを自動的に試行し、失敗した場合にのみクラウド提供型 Firewall Management Center でフォールバックします。

アップグレードの準備状況

互換性を確認し、アップグレードパスと順序を計画し、アップグレードのガイドラインを確認した後、アップグレードの準備状況を評価する必要があります。システムはこれらのチェックの一部を行いますが、設定変更の展開やバックアップの作成など、追加のチェック（およびアクション）をご自身で実行する必要があります。

次のセクションを活用して直前のタスクを実行し、アップグレードの準備状況を確認します。

インフラストラクチャとネットワークの確認

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あることを確認してください。デバイスを経由せずに クラウド提供型 Firewall 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ッ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 テクニカルノート）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うとともに、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ます。通常、展開すると Snort が再起動されますが、これによって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。「[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。正常性モニターまたは [デバイス管理 (Device Management)] ページで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。

正常性テストに失敗すると、アップグレードできなかったり、アップグレードが失敗したりする可能性があります。ご自身で解決できる NTP の問題を除き、展開で次のいずれかのテストに失敗した場合は、Cisco TAC にお問い合わせください。結果は、正常性モニターの [正常性ステータス (Health Status)] (ホーム) ページ ([トラブルシューティング (Troubleshooting)] > [ヘルス (Health)] > [モニター (Monitor)]) で報告されます。



- (注) これらの定期的な正常性テストを無効にしても、アップグレードの前にシステムでそれらのテストが実施されなくなることはありません。既存の結果がない場合、アップグレードの一部として準備状況チェックが実行されるため、アップグレードの時間が長くなります。

表 10: アップグレード関連の正常性テスト

正常性テスト	説明
データベース	データベースのスキーマと設定データ (EO) の完全性を監視します。
ディスク ステータス	ハードウェアデバイスのディスクおよびRAID コントローラの正常性を監視します。
ディスク使用量	デバイスのディスク使用量を監視します。アップグレードでは必要なディスク容量が計算され、十分なディスク容量がなければアップグレードは行われません。このモジュールがアップグレードを開始する前にアラートを発出している場合は、十分なディスク容量がない可能性があります。 デバイスの正常性ダッシュボードのディスク使用量ウィジェットには、古いバックアップ、コンテンツ更新、障害対応ファイルなどの不要なファイルを安全に削除する [ディスク容量のクリア (Clear disk space)] ボタンがあります。
Firewall Threat Defense HA (クラウド提供型 Firewall Management Center およびデバイス) クラスター/HA 障害ステータス (デバイス)	高可用性ペアおよびクラスターは、スプリットブレインなどではなく、同期している必要があります。このような問題があると、ほとんどの場合に Firewall Threat Defense のアップグレードは続行されません。ただし、Firepower 4100/9300 および では、シャーシはそのインスタンスのステータスを認識しません。つまり、シャーシを一度にアップグレードする場合でも、各シャーシのアップグレードの前に展開が正常であることを確認しなければ、中断が発生する可能性があります。
FXOS の正常性	FXOS ベースのデバイスで FXOS httpd サービスを監視します。このサービスが実行されていなければ、アップグレードは失敗します。

正常性テスト	説明
時刻同期ステータス	デバイスの NTP 同期を監視します。同期されていないと、アップグレードが失敗する可能性があります。システムは、10 秒を超えてオフセットしている場合にのみアラートを発出するため、オフセットが小さい場合は手動で確認することを推奨します（テスト結果の横にある [詳細を表示 (see more)] をクリックします）。

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 11: バックアップ

バックアップ	ガイド
Firewall Threat Defense	Cisco Security Cloud Control : Firewall Threat Defense 向けクラウド提供型ファイアウォール管理センター : 「Backup/Restore」 パブリッククラウドの Firewall Threat Defense Virtual など、バックアップがサポートされていないケースもあります。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 3100/4200 シャーシ	Cisco Security Cloud Control : Firewall Threat Defense 向けクラウド提供型ファイアウォール管理センター : Secure Firewall 3100/4200 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」 Firewall 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）。

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。