FTD のアップグレード

この章では、バージョン 7.1 FMC を使用して Threat Defense をアップグレードする方法について説明します。FMC で別のバージョンを実行している場合、またはクラウド提供型の Management Center を使用している場合は、『対象読者』を参照してください。

FTD のアップグレード チェックリスト

計画と実現可能性

誤りを避けるには、注意深い計画と準備が役立ちます。

✓	アクション/チェック	詳細
	展開を評価します。	状況を理解することにより、目的を達成する方法を決定します。現在のバージョンとモデル情報に加えて、展開が高可用性/拡張性を実現するように設定されているかどうか、デバイスが IPS またはファイアウォールとして展開されているかどうかなどを確認します。

✓	アクション/チェック	詳細
	アップグレードパスを計画します。	これは、大規模展開、マルチホップアップグレード、またはオペレーティングシステムまたはホスティング環境をアップグレードする必要がある状況では特に重要です。次を参照してください。 • FMC のアップグレードパス • FTD のアップグレードパス （7 ページ） • FXOS のアップグレードパス
	アップグレードガイドラインを読み、設定の変更を計画します。	主要なアップグレードでは特に、アップグレードの前または後に、アップグレードにより重要な設定変更が発生することがあります。以下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：重要なリリース固有のアップグレードガイドラインが記載されています。 • Cisco Secure Firewall Management Center の新機能（リリース別）：アップグレードに影響を与える新機能および廃止された機能が記載されています。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バージョンを確認してください。 • Cisco Firepower リリースノート：「*Open and Resolved Bugs*」の章に、アップグレードに影響を与えるバグが記載されています。現在のバージョンと対象バージョン間にあるすべてのバージョンのリリースノートを確認してください。：サポート契約がある場合は、Cisco バグ検索ツールを使用して最新のバグリストを取得できます。 • Cisco Firepower 4100/9300 FXOS 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が記載されています。

✓	アクション/チェック	詳細
	ウィザードまたは [システムの更新（System Updates）] ページのどちらを使用するかを決定します。	一部のチェックリスト項目では、Threat Defense アップグレードウィザードを使用した場合と [システムの更新（System Updates）] ページを使用した場合の比較が示されています。ウィザードでは、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、アップグレードの重要な段階が順を追って説明されます。ウィザードを使用すると、アップグレードをより迅速かつ確実に、より少ないディスク容量で実行できます。 通常、ウィザードを使用してアップグレードすることをお勧めしますFTD。ただし、アップグレード完了後に復元が必要になる可能性がある場合は、**システム**（⚙）>**[更新（Updates）]** を使用します。また、[システムの更新（System Updates）] ページを使用して、パッケージを管理したり、FMC および古い従来型のデバイスをアップグレードする必要があります。
	アプライアンスへのアクセスを確認します。	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 FMC 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。
	帯域幅を確認します。	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。

✓	アクション/チェック	詳細
	メンテナンス時間帯をスケジュールします。	影響が最小限になるようにメンテナンス時間帯をスケジュールします。トラフィックフローやインスペクションへの影響、およびアップグレードにかかる可能性がある時間を考慮してください。また、この時間帯で実行する必要があるタスクと、事前に実行できるタスクを検討します。参照先： • FXOS 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 • 時間とディスク容量のテスト

バックアップ

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 FMC 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 FMC をバックアップしてください。

✓	アクション/チェック	詳細
	FTD をバックアップします。	サポートされている場合は、FMC を使用して FTD 構成をバックアップします。Firepower Management Center アドミニストレーション ガイドの「バックアップ/復元」の章を参照してください。 Firepower 9300 で FTD および ASA 論理デバイスが別のモジュールで実行されている場合、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）。『Cisco ASA Series General Operations Configuration Guide』の「*Software and Configurations*」の章を参照してください。

✓	アクション/チェック	詳細
	Firepower 4100/9300 の FXOS をバックアップします。	Firepower Chassis Manager または FXOS CLI を使用して、論理デバイス設定およびプラットフォーム設定を含むシャーシ設定をエクスポートします。 詳細については、『Cisco Firepower 4100/9300 FXOS コンフィギュレーション ガイド』の「コンフィギュレーションのインポート/エクスポート」を参照してください。

アップグレードパッケージ

アップグレードの前にアップグレードパッケージをシステムにアップロードすると、メンテナンス時間が短縮されます。

✓	アクション/チェック	詳細
	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て、FMC または内部 Web 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は シスコ サポートおよびダウンロードサイト（FTD のアップグレードパッケージのアップロード （14 ページ））で入手できます。 FMC を使用して直接ダウンロードを実行することもできます（）。 デバイスのアップグレードパッケージを FMC にアップロードするか、内部サーバーから取得するようにデバイスを設定します。 • [システム（System）] > [更新（Updates）] メニューを使用して FTD アップグレードパッケージを FMC にアップロードする （15 ページ） • [システム（System）] > [更新（Updates）] メニューを使用して FTD アップグレードパッケージを内部サーバーにアップロードする （16 ページ） Firepower 4100/9300 の場合、FXOS アップロード手順は FXOS アップグレード手順に含まれています。
	アップグレードパッケージをデバイスにコピーします。	FTD を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存在している必要があります。アップグレードの前にアップグレードパッケージをコピーすると、アップグレードのメンテナンス時間が短縮されます。 Threat Defense のアップグレードウィザードでは、アップグレードパッケージを必要なデバイスにコピーするように求められます。または、[システムの更新（System Updates）] ページを使用できます。

関連するアップグレード

オペレーティングシステムとホスティング環境のアップグレードはトラフィックフローとインスペクションに影響を与える可能性があるため、メンテナンス時間帯で実行してください。

✓	アクション/チェック	詳細
	仮想ホスティングをアップグレードします。	必要に応じて、ホスティング環境をアップグレードします。通常、古いバージョンの VMware を実行していて、メジャーアップグレードを実行している場合、アップグレードが必要です。
	Firepower 4100/9300 のファームウェアをアップグレードします。	最新のファームウェアを推奨します。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。
	Firepower 4100/9300 の FXOS をアップグレードします。	FXOS のアップグレードは通常、メジャーアップグレードの要件ですが、メンテナンスリリースやパッチの場合は要件になるのは非常にまれです。中断を最小限に抑えるには、FTD のハイアベイラビリティペアおよびシャーシ間クラスタの FXOS を一度に 1 つずつアップグレードします。 Firepower 4100/9300 の FXOS のアップグレード を参照してください。

最終チェック

一連の最終チェックにより、ソフトウェアをアップグレードする準備が整います。

✓	アクション/チェック	詳細
	設定を確認します。	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。
	NTP 同期を確認します。	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します。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。 • FMC：[システム（System）] > [設定（Configuration）] > [時刻（Time）] を選択します。 • FTD：**show time** CLI コマンドを使用します。

✓	アクション/チェック	詳細
	設定を展開します。	アップグレードする前に設定を展開すると、失敗する可能性が減少します。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。FTD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。
	準備状況チェックを実行します。	互換性と準備状況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低くなります。 Threat Defense のアップグレードウィザードにより、準備状況チェックを実行するように求められます。または、[システムの更新（System Updates）]ページを使用できます[システム（System）] > [更新（Updates）] メニューを使用して FTD の準備状況チェックを実行する。
	のディスク容量を確認します。	準備状況チェックには、ディスク容量チェックが含まれます。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。 デバイスで使用可能なディスク容量を確認するには、**システム（⚙） > [モニタリング（Monitoring）] > [統計（Statistics）]**を選択してから、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。
	実行中のタスクを確認します。	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。これが起こらないようにするには（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ているタスクを確認し、それらをキャンセルまたは延期します。

FTD のアップグレードパス

展開に一致するアップグレードパスを選択します。

顧客が展開した FMC はその管理対象デバイスと同じかまたはより新しいバージョンを実行する必要があります。FMC よりも新しいバージョンのデバイスをアップグレードすることはで

きません。メンテナンス（3 桁）リリースの場合でも、最初に FMC をアップグレードする必要があります。

FXOS を使用しない FTD のアップグレードパス

この表は、オペレーティングシステムをアップグレードする必要がない場合の FTD のアップグレードパスを示しています。これには、アプライアンスモードの Firepower 1000/2100 シリーズ、ASA-5500-X シリーズ、および ISA 3000 が含まれます。

現在の FTD/FMC のバージョンが対象のバージョンより後の日付にリリースされた場合、期待どおりにアップグレードできない可能性があります。このような場合、アップグレードはすぐに失敗し、2 つのバージョン間にデータストアの非互換性があることを説明するエラーが表示されます。現在のバージョンと対象のバージョンの両方のに関するリリースノートには、特定の制限が掲載されています。

表 *1: FTD* の直接アップグレード

現在のバージョン	ターゲットバージョン
7.3	→ 以降の 7.3.x リリース
7.2	次のいずれかです。 → 7.3.x → 以降の 7.2.x リリース （注） バージョン 7.2.3 で導入された Firepower 1010E は、バージョン 7.3 ではサポートされません。サポートは今後のリリースで復帰予定です。
7.1	次のいずれかです。 → 7.3.x → 7.2.x → 以降の 7.1.x リリース

現在のバージョン	ターゲットバージョン
7.0 ASA 5508-X および 5516-X における最後のサポート。	次のいずれかです。 → 7.3.x → 7.2.x → 7.1.x → 以降の 7.0.x リリース （注） データストアの非互換性のため、 をバージョン 7.0.4 以降からバージョン 7.1.0 にアップグレードすることができません。バージョン 7.2 以降に直接アップグレードすることをお勧めします。 （注） クラウド提供型 Firewall Management Center は、バージョン 7.1 を実行している FTD デバイス、または任意のバージョンを実行している従来のデバイスを管理できません。クラウド管理の登録を解除するか、または無効にしない限り、クラウド管理対象デバイスはバージョン 7.0.x からバージョン 7.1 にアップグレードできません。バージョン 7.2 以降に直接アップグレードすることをお勧めします。
6.7	次のいずれかです。 → 7.2.x → 7.1.x → 7.0.x → 以降の 6.7.x リリース
6.6 ASA 5525-X、5545-X、5555-X における最後のサポート。	次のいずれかです。 → 7.2.x → 7.1.x → 7.0.x → 6.7.x → 任意の後続リリース 6.6.x

現在のバージョン	ターゲットバージョン
6.5	次のいずれかです。 → 7.1.x → 7.0.x → 6.7.x → 6.6.x
6.4 ASA 5515-X における最後のサポート。	次のいずれかです。 → 7.0.x → 6.7.x → 6.6.x → 6.5
6.3	次のいずれかです。 → 6.7.x → 6.6.x → 6.5 → 6.4
6.2.3 ASA 5506-X シリーズにおける最後のサポート。	次のいずれかです。 → 6.6.x → 6.5 → 6.4 → 6.3

FXOS を使用する FTD のアップグレードパス

Firepower 4100/9300 に搭載されている FTD のアップグレードパスを次の表に示します。

現在の FTD/FMC のバージョンが対象のバージョンより後の日付にリリースされた場合、期待どおりにアップグレードできない可能性があります。このような場合、アップグレードはすぐに失敗し、2 つのバージョン間にデータストアの非互換性があることを説明するエラーが表示されます。現在のバージョンと対象のバージョンの両方のに関するリリースノートには、特定の制限が掲載されています。

この表には、シスコにより特別に認定されたバージョンの組み合わせのみが掲載されています。最初にFXOS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デバイスソフトウェアの「前」に

アップグレードします。FXOSをアップグレードしても、論理デバイスやアプリケーションインスタンスとの互換性ガ失われないようにしてください。 最小限のビルドおよびその他の詳細な互換性情報については、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* における *FTD* の直接アップグレード

現在のバージョン	対象のバージョン
Threat Defense 7.3 を搭載した FXOS 2.13	→ FXOS 2.13 と任意の後続リリース Threat Defense 7.3.x
Threat Defense 7.2 を搭載した FXOS 2.12 Firepower 4110、4120、4140、4150 の最後のサポート。 SM-24、SM-36、SM-44 モジュールを搭載した Firepower 9300 の最後のサポート。	次のいずれかです。 → FXOS 2.13 と Threat Defense 7.3.x → FXOS 2.12 と任意の後続リリース Threat Defense 7.2.x
Threat Defense 7.1 を搭載した FXOS 2.11.1	次のいずれかです。 → FXOS 2.13 と Threat Defense 7.3.x → FXOS 2.12 と Threat Defense 7.2.x → FXOS 2.11.1 と任意の後続リリース Threat Defense 7.1.x

現在のバージョン	対象のバージョン
Threat Defense 7.0 を搭載した FXOS 2.10.1	次のいずれかです。 → FXOS 2.13 と Threat Defense 7.3.x → FXOS 2.12 と Threat Defense 7.2.x → FXOS 2.11.1 と Threat Defense 7.1.x → FXOS 2.10.1 と任意の後続リリース Threat Defense 7.0.x （注） データストアの非互換性のため、をバージョン 7.0.4 以降からバージョン 7.1.0 にアップグレードすることができません。バージョン 7.2 以降に直接アップグレードすることをお勧めします。 （注） クラウド提供型 Firewall Management Center は、バージョン 7.1 を実行している FTD デバイス、または任意のバージョンを実行している従来のデバイスを管理できません。クラウド管理の登録を解除するか、または無効にしない限り、クラウド管理対象デバイスはバージョン 7.0.x からバージョン 7.1 にアップグレードできません。バージョン 7.2 以降に直接アップグレードすることをお勧めします。
Threat Defense 6.7 を搭載した FXOS 2.9.1	次のいずれかです。 → FXOS 2.12 と Threat Defense 7.2.x → FXOS 2.11.1 と Threat Defense 7.1.x → FXOS 2.10.1 と Threat Defense 7.0.x → FXOS 2.9.1 と任意の後続リリース Threat Defense 6.7.x
Threat Defense 6.6 を搭載した FXOS 2.8.1	次のいずれかです。 → FXOS 2.12 と Threat Defense 7.2.x → FXOS 2.11.1 と Threat Defense 7.1.x → FXOS 2.10.1 と Threat Defense 7.0.x → FXOS 2.9.1 と Threat Defense 6.7.x → FXOS 2.8.1 と任意の後続リリース Threat Defense 6.6.x

現在のバージョン	対象のバージョン
Threat Defense 6.5 を搭載した FXOS 2.7.1	次のいずれかです。 → FXOS 2.11.1 と Threat Defense 7.1.x → FXOS 2.10.1 と Threat Defense 7.0.x → FXOS 2.9.1 と Threat Defense 6.7.x → FXOS 2.8.1 と Threat Defense 6.6.x
Threat Defense 6.4 を搭載した FXOS 2.6.1	次のいずれかです。 → FXOS 2.10.1 と Threat Defense 7.0.x → FXOS 2.9.1 と Threat Defense 6.7.x → FXOS 2.8.1 と Threat Defense 6.6.x → Threat Defense 6.5 を搭載した FXOS 2.7.1
Threat Defense 6.3 を搭載した FXOS 2.4.1	次のいずれかです。 → FXOS 2.9.1 と Threat Defense 6.7.x → FXOS 2.8.1 と Threat Defense 6.6.x → Threat Defense 6.5 を搭載した FXOS 2.7.1 → Threat Defense 6.4 を搭載した FXOS 2.6.1
Threat Defense 6.2.3 を搭載した FXOS 2.3.1	次のいずれかです。 → FXOS 2.8.1 と Threat Defense 6.6.x → Threat Defense 6.5 を搭載した FXOS 2.7.1 → Threat Defense 6.4 を搭載した FXOS 2.6.1 → Threat Defense 6.3 を搭載した FXOS 2.4.1

FTD ハイアベイラビリティ/スケーラビリティ と FXOS のアップグレード順序

高可用性や拡張性を導入する場合でも、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 つずつシャーシの FXOS をアップグレードします。FTD のアップグレードの場合、グループ化されたデバイスが 1 つずつ自動的にアップグレードされます。

表 *3 : Firepower 4100/9300* に搭載された *FXOS* と *Threat Defense* のアップグレード順序

FTD の導入	アップグレード順序
スタンドアロン	1. FXOS をアップグレードします。 2. FTD をアップグレードします。
ハイ アベイラビリティ	FTD をアップグレードする前に、両方のシャーシで FTD 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の FXOS 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の FXOS をアップグレードします。 4. FTD 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. FXOS をアップグレードします。 2. FTD 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）	FTD をアップグレードする前に、すべてのシャーシの FXOS 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の FXOS 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. 残りのシャーシの FXOS をアップグレードします。 4. FTD をアップグレードします。

FTD のアップグレードパッケージのアップロード

アップグレード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。

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付きで、次の表に示すように末尾が .sh.REL.tar。署名付きのアップグレード パッケージは解凍しないでください。

表 *4:* ソフトウェア アップ グレード パッケージ

プラットフォーム（**Platform**）	アップグレードパッケージ
Firepower 1000 シリーズ	Cisco_FTD_SSP-FP1K_Upgrade-7.1-999.sh.REL.tar
Firepower 2100 シリーズ	Cisco_FTD_SSP-FP2K_Upgrade-7.1-999.sh.REL.tar
Secure Firewall 3100 シリーズ	Cisco_FTD_SSP-FP3K_Upgrade-7.1-999.sh.REL.tar
Firepower 4100/9300	Cisco_FTD_SSP_Upgrade-7.1-999.sh.REL.tar
FTDv	Cisco_FTD_Upgrade-7.1-999.sh.REL.tar
FTD を使用した ISA 3000	Cisco_FTD_Upgrade-7.1-999.sh.REL.tar

ヒント 一部のアップグレードパッケージは、リリースが手動でダウンロードできるようになってからしばらくすると、直接ダウンロードできるようになります。遅延の長さは、リリースの種類、リリースの選択、およびその他の要因によって異なります。FMC がインターネットにアクセスできる場合は、**システム**（⚙） > **[更新（Updates）]** で [アップデートのダウンロード（Download Updates）] をクリックして、FMC とすべての管理対象デバイス向けの最新の VDB、最新のメンテナンスリリース、および最新の重要パッチをすぐにダウンロードできます。

[システム（System）]>[更新（Updates）] メニューを使用して FTD アップグレードパッケージを FMC にアップロードする

アップグレードパッケージは、署名付きの tar アーカイブ（.tar）です。署名付きのパッケージをアップロードした後、パッケージを検証するための [システムの更新（System Updates）] ページのロードに数分かかることがあります。表示を迅速化するには、不要なアップグレードパッケージを削除してください。署名付きのパッケージは解凍しないでください。

ステップ 1 FMC で、**システム**（⚙） > **[更新（Updates）]** を選択します。
ステップ 2 [更新のアップロード（Upload Update）] をクリックします。

ステップ 3 [アクション（Action）] については、[ローカル ソフトウェア アップデート パッケージのアップロード（Upload local software update package）] オプションボタンをクリックします。

ステップ 4 [ファイルの選択（Choose File）] をクリックします。

ステップ 5 パッケージを参照し、[アップロード（Upload）] をクリックします。

ステップ 6 （オプション）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。

復元を有効にする必要がなく、FTDアップグレードウィザードを使用する予定の場合、パッケージをコピーするように求められます。復元を有効にするため、[システムの更新（System Updates）] ページを使用してアップグレードする場合は、次のように、アップグレードパッケージを今すぐにデバイスにコピーすることを推奨します。

a) コピーするアップグレードパッケージの横にある [アップデートのプッシュまたはステージ（Push or Stage Update）] アイコンをクリックします。

b) 宛先デバイスを選択します。

アップグレード パッケージをプッシュするデバイスがリストに表示されない場合は、間違ったアップグレード パッケージを選択しています。

c) [プッシュ（Push）] をクリックします。

[システム（System）]>[更新（Updates）]メニューを使用してFTDアップグレードパッケージを内部サーバーにアップロードする

この手順を使用して、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するように FTD デバイスを設定します。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 上の容量も節約できます。

この機能を設定するには、Webサーバーのアップグレードパッケージの場所にポインタ（URL）を保存します。アップグレードプロセスでは、FMC ではなく Web サーバーからアップグレードパッケージが取得されます。または、アップグレードする前に、FMC のプッシュ機能を使用してパッケージをコピーすることもできます。

各アップグレードパッケージに対して、この手順を繰り返します。アップグレードパッケージごとに、1 つの場所のみを設定できます。

始める前に

デバイスがアクセスできる内部 Web サーバーにアップグレードパッケージをコピーします。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）を取得します。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。

ステップ 1 FMC で、**システム**（⚙）>**[更新（Updates）]** を選択します。

ステップ 2 [更新のアップロード（Upload Update）] をクリックします。

何もアップロードしない場合でも、このオプションを選択します。次のページに、URL の入力を求めるプロンプトが表示されます。

ステップ 3 **アクション**については、**[ローカルソフトウェアアップデートパッケージのアップロード（Upload local software update package）]** オプション ボタンをクリックします。

ステップ 4 アップグレードパッケージの**送信元 URL** を入力します。

次の例のように、プロトコル（HTTP/HTTPS）とフルパスを提供します。

```
https://internal_web_server/upgrade_package.sh.REL.tar
```

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）、およびアップグレードするソフトウェアのバージョンが反映されています。正しいファイル名を入力したことを確認します。

ステップ 5 HTTPS サーバーの場合は、**CA 証明書**を提供します。

これは、以前取得したサーバーのデジタル証明書です。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。

ステップ 6 **[保存（Save）]** をクリックします。

場所が保存されます。アップロードされたアップグレードパッケージとアップグレードパッケージの URL はまとめてリストされますが、明確にラベル付けされます。

ステップ 7 （オプション）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。

復元を有効にする必要がなく、FTDアップグレードウィザードを使用する予定の場合、パッケージをコピーするように求められます。復元を有効にするため、[システムの更新（System Updates）]ページを使用してアップグレードする場合は、次のように、アップグレードパッケージを今すぐにデバイスにコピーすることを推奨します。

a) コピーするアップグレードパッケージの横にある [アップデートのプッシュまたはステージ（Push or Stage Update）] アイコンをクリックします。

b) 宛先デバイスを選択します。

アップグレード パッケージをプッシュするデバイスがリストに表示されない場合は、間違ったアップグレード パッケージを選択しています。

c) [プッシュ（Push）] をクリックします。

ウィザードを使用した FTD のアップグレード（復元を無効化）

この手順を使用すると、ウィザードを使用して FTD をアップグレードできます。

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。他のユーザーは、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）。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。ユーザーを削除または非アクティブ化するか、ユーザーロールを更新して、ユーザーに付与された権限を無効にできます**[デバイス（Devices）]** > **[デバイスのアップグレード（Device Upgrade）]**。

ハイアベイラビリティ対応の FMC の間では、ワークフローも Threat Defense のアップグレードパッケージも同期されないので注意してください。フェールオーバーが発生した場合は、新しいアクティブな FMC でワークフローを再作成する必要があります。これには、FMC へのアップグレードパッケージのアップロードと準備状況チェックの実行が含まれます（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、 FMC 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）。

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 応答しないアップグレード を参照してください。

始める前に

- この手順を使用するかどうかを決定します。

  通常、ウィザードを使用してアップグレードすることをお勧めしますFTD。ただし、アップグレード完了後に復元が必要になる可能性がある場合は、**システム**（⚙） > **[更新（Updates）]** を使用します。また、[システムの更新（System Updates）] ページを使用して、パッケージを管理したり、FMC および古い従来型のデバイスをアップグレードする必要があります。

- 事前アップグレードのチェックリストを完了します。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。

ワークフローを開始します。

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

アップグレード対象のデバイスを選択して、アップグレードパッケージをコピーします。

ステップ 2 デバイスの選択内容を確認します。

追加のデバイスを選択するには、[デバイス管理（Device Management）] ページに戻ります。進行状況は失われません。デバイスを削除するには、[リセット（Reset）] をクリックしてデバイスの選択をクリアし、最初からやり直します。

ステップ 3 アップグレードするデバイスを選択します。

複数のデバイスを同時にアップグレードできます。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。

重要 パフォーマンスの問題により、デバイスをバージョン 6.6.x 以前にアップグレードする場合は（バージョン 6.6.x からのアップグレードではなく）、同時にアップグレードするデバイスは 5 つまでにすることを強くお勧めします。

ステップ 4 [Select Action] または [Select Bulk Action] メニューから、[Upgrade Firepower Software] を選択します。

デバイスのアップグレードウィザードが表示され、選択したデバイスの数が示されます。また、対象のバージョンを選択するように求められます。このページには、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。

進行中のアップグレードワークフローがすでにある場合は、最初にデバイスをマージする（新しく選択したデバイスを以前に選択したデバイスに追加して続行する）か、リセットする（以前の選択を破棄し、新しく選択したデバイスのみを使用する）必要があることに注意してください。

ステップ 5 デバイスの選択内容を確認します。

追加のデバイスを選択するには、[デバイス管理（Device Management）] ページに戻ります。進行状況は失われません。デバイスを削除するには、[リセット（Reset）] をクリックしてデバイスの選択をクリアし、最初からやり直します。

ステップ 6 [アップグレード先（Upgrade to）] メニューから、対象のバージョンを選択します。

システムは、選択したデバイスのどれをそのバージョンにアップグレードできるかを決定します。対象外のデバイスがある場合は、デバイスのリンクをクリックして理由を確認できます。不適格なデバイスを削除する必要はありません。自動的にアップグレードの対象から除外されます。

[Upgrade to] メニューの選択肢は、システムで利用可能なデバイスの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。対象のバージョンが表示されない場合は、**システム**（⚙）> **[更新（Updates）]** に移動し、正しい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します。異なるデバイスモデルをアップグレードするために複数のアップグレードパッケージが必要な場合は、次の手順に進む前に、必要なすべてのアップグレードパッケージについてこれを行います。

ステップ 7 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ついて、[アップグレードパッケージのコピー（Copy Upgrade Packages）] をクリックして、選択内容を確認します。

FTD を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存在している必要があります。アップグレードの前にアップグレードパッケージをコピーすると、アップグレードのメンテナンス時間が短縮されます。

ステップ 8 [次へ（Next）] をクリックします。

互換性、準備状況、およびその他の最終チェックを実行します。

ステップ 9 準備状況チェックに合格する必要があるすべてのデバイスについて、[Run Readiness Check] をクリックして、選択を確認します。

[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。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。デバイスが準備状況チェックに失敗した場合は、問題を修正して、準備状況チェックを再度実行してください。準備状況チェックの結果、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。代わりに、Cisco TAC にお問い合わせください。

互換性チェックは自動的に行われることに注意してください。たとえば、FXOS をアップグレードする必要がある場合や、管理対象デバイスに展開する必要がある場合は、ただちにシステムアラートが表示されます。

ステップ 10 アップグレード前の最終的なチェックを実行します。

アップグレード前のチェックリストを再確認します。関連するすべてのタスク、特に最終チェックを完了していることを確認してください。

ステップ 11 必要に応じて、**[デバイス（Devices）] > [デバイスのアップグレード（Device Upgrade）]** に戻ります。

ステップ 12 [次へ（Next）] をクリックします。

デバイスをアップグレードします。

ステップ 13 デバイスの選択と対象のバージョンを確認します。

ステップ 14 （オプション）クラスタ化されたデバイスのアップグレード順序を変更します。

クラスタのデバイスの詳細を表示し、[アップグレード順序の変更（Change Upgrade Order）] をクリックします。制御ユニットは常に最後にアップグレードされます。これを変更することはできません。

ステップ 15 ロールバックオプションを選択します。

メジャーおよびメンテナンスアップグレードの場合、**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**。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。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場合は、このオプションを無効にします。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。

このオプションは、パッチではサポートされていません。

ステップ 16 [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。

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ーできます。進行状況の詳細を確認するには、[デバイス管理（Device Management）] ページの [アップグレード（Upgrade）] タブ、およびメッセージセンター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。アップグレード中のトラフィック処理については、「FTD 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」のを参照してください。。

アップグレード中にデバイスが 2 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。

成功を確認し、アップグレード後のタスクを完了します。

ステップ 17 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 18 （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 19 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 20 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 21 アップグレードしたデバイスに構成を再度展開します。

次のタスク

（オプション）**[完了（Finish）]**[アップグレード情報のクリア（Clear Upgrade Information）] をクリックして、ウィザードをクリアします。これを行うまで、ページには、実行したばかりのアップグレードに関する詳細が引き続き表示されます。

[システム（System）] > [更新（Updates）] メニューを使用した FTD のアップグレード（復元を有効化）

この手順を使用すると、[システムの更新（System Updates）] ページから FTD をアップグレードできます。

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 応答しないアップグレード を参照してください。

始める前に

- この手順を使用するかどうかを決定します。

  アップグレード完了後に元に戻す必要が生じる可能性がある場合は、**システム**（⚙）**>[更新（Updates）]** を使用して FTD をアップグレードします。これは、[アップグレードの成

功後に復元を有効にする（Enable revert after successful upgrade）] オプション（）を設定する唯一の方法であり、Threat Defense のアップグレードウィザードを使用するという通常の推奨事項とは対照的です。

- 事前アップグレードのチェックリストを完了します。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 FMC で、**システム**（⚙） > **[更新（Updates）]** を選択します。

ステップ 2 [利用可能なアップデート（Available Updates）] で該当するアップグレード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ます。

アップグレードするデバイスがリストに表示されない場合は、間違ったアップグレード パッケージを選択しています。

対象デバイスのリストが、アップグレード前の互換性チェックの結果とともに表示されます。アップグレードの失敗の原因となる明らかな問題がある場合、この事前チェックによってアップグレードが防止されます。

ステップ 3 チェックするデバイスを選択し、[準備状況の確認（Check Readiness）] をクリックします。

準備状況チェックでは、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の準備状況を評価します。 準備状況チェックの実行に必要な時間は、モデル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。

このページの [準備状況チェック（Readiness Checks）] では、チェック進行中やチェック不合格など、アップグレード環境全体のチェックステータスを確認できます。また、このページを使用して、不合格となった後にチェックを簡単に再実行することもできます。メッセージセンターで準備状況チェックの進行状況をモニターすることもできます。

他の適格なデバイスを選択できない場合は、互換性チェックに合格したことを確認してください。デバイスが準備チェックで不合格になった場合は、アップグレードする前に問題を修正してください。

ステップ 4 アップグレードするデバイスを選択します。

複数のデバイスで同じアップグレードパッケージを使用する場合にのみ、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。

重要 [システムの更新（System Update）] ページから同時にアップグレードするデバイスは 5 台までにすることを強く推奨します。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 アップグレードオプションを選択します。

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では、次のことを行えます。

- **アップグレードの失敗時に自動的にキャンセルし、前のバージョンにロールバックする**：アップグレードに失敗すると、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。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場合は、このオプションを無効にします。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。

- **アップグレード成功後の復元を可能にする**：アップグレードが成功してから 30 日間、デバイスをアップグレード前の状態に戻すことができます。

これらのオプションは、パッチではサポートされていません。

ステップ 6 [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。アップグレード中のトラフィック処理については、「FTD 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」のを参照してください。。

アップグレード中にデバイスが 2 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。

ステップ 7 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 8 （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 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 アップグレードしたデバイスに構成を再度展開します。

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