Threat Defense のアップグレード

Threat Defense 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。 • Management Center のアップグレードパス • Threat Defense のアップグレードパス （5 ページ） • FXOS のアップグレードパス

✓	アクション/チェック	詳細
	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。リリースノートを使用して開始します。 • Cisco Secure Firewall Threat Defense リリースノート • Cisco Firepower 4100/9300 FXOS リリースノート
	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 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。アップグレードパケージをアップグレード時に管理対象デバイスに転送する場合は、帯域幅が不十分だと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する原因となったりする可能性があります。 『Firepower Management Center から管理対象装置へのデータをダウンロードするためのガイドライン』（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。
	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および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。 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および時間とディスク容量のテストを参照してください。

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。

✓	アクション/チェック	詳細
	Threat Defense をバックアップします。	サポートされている場合は、Management Centerを使用してThreat Defense 構成をバックアップします。Cisco Secure Firewall 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 Threat Defense 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、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。
	Firepower 4100/9300 の FXOS をバックアップします。	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。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
	アップグレードパッケージをアップロードします。	Management Center またはデバイスがアクセスできる内部サーバーにThreat Defense アップグレードパッケージをアップロードします。アップグレードパッケージのアップロード （11 ページ） を参照してください。 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。

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 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。トラフィックフローとインスペクションでの中断を防ぐには、Threat Defense 高可用性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 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。 • Management Center：[システム（System）] > [設定（Configuration）] > [時刻（Time）] を選択します。 • Threat Defense ：**show time** CLI コマンドを使用します。

✓	アクション/チェック	詳細
	ディスク容量を確認します。	ソフトウェアアップグレードに関するディスク容量チェックを実行します。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。 時間とディスク容量のテスト を参照してください。
	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。これは、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。
	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 のアップグレード準備状況チェック （16 ページ）を参照してください。
	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。

Threat Defense 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。

Management Center では、その管理対象デバイスと同じ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。Management Center 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 Management Center をアップグレードする必要があります。

FXOS を使用する Threat Defense のアップグレードパス

次の表に、Firepower 4100/9300 の Threat Defense のアップグレードパスを示します。

現在の Threat Defense /Management Center 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（ただし推奨されていない）組み合わせを短時間実行します。ここでは、FXOS が論理デバイスの「前」になります。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 *1 : Firepower 4100/9300* での *Threat Defense* 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 7.2 を搭載した FXOS 2.12	→ Threat Defense 7.2.x 以降のメンテナンスリリースを搭載した FXOS 2.12
Threat Defense 7.1 を搭載した FXOS 2.11.1	次のいずれかです。 → Threat Defense 7.2 を搭載した FXOS 2.12 → Threat Defense 7.1.x 以降のメンテナンスリリースを搭載した FXOS 2.11.1

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。 → Threat Defense 7.2 を搭載した FXOS 2.12 → Threat Defense 7.1 を搭載した FXOS 2.11.1 → Threat Defense 7.0.x 以降のメンテナンスリリースを搭載した FXOS 2.10.1 （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） クラウド提供型の管理センターは、バージョン 7.1 を実行している脅威防御デバイス、または任意のバージョンを実行しているデバイスを管理できません。クラウド管理を登録解除して無効にしない限り、クラウド提供型の管理センターに登録されている脅威防御デバイスをバージョン 7.0.x からバージョン 7.1 にアップグレードすることはできません。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。 → Threat Defense 7.2 を搭載した FXOS 2.12 → Threat Defense 7.1 を搭載した FXOS 2.11.1 → Threat Defense 7.0 を搭載した FXOS 2.10.1 → Threat Defense 6.7.x 以降のメンテナンスリリースを搭載した FXOS 2.9.1
Threat Defense 6.6 を搭載した FXOS 2.8.1	次のいずれかです。 → Threat Defense 7.2 を搭載した FXOS 2.12 → Threat Defense 7.1 を搭載した FXOS 2.11.1 → Threat Defense 7.0 を搭載した FXOS 2.10.1 → Threat Defense 6.7 を搭載した FXOS 2.9.1 → Threat Defense 6.6.x 以降のメンテナンスリリースを搭載した FXOS 2.8.1

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。 → Threat Defense 7.1 を搭載した FXOS 2.11.1 → Threat Defense 7.0 を搭載した FXOS 2.10.1 → Threat Defense 6.7 を搭載した FXOS 2.9.1 → Threat Defense 6.6 を搭載した FXOS 2.8.1
Threat Defense 6.4 を搭載した FXOS 2.6.1	次のいずれかです。 → Threat Defense 7.0 を搭載した FXOS 2.10.1 → Threat Defense 6.7 を搭載した FXOS 2.9.1 → Threat Defense 6.6 を搭載した FXOS 2.8.1 → 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。 → Threat Defense 6.7 を搭載した FXOS 2.9.1 → Threat Defense 6.6 を搭載した FXOS 2.8.1 → 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。 → Threat Defense 6.6 を搭載した FXOS 2.8.1 → 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

FXOS を使用しない Threat Defense のアップグレードパス

この表は、FXOS をアップグレードする必要がない場合の Threat Defense のアップグレードパスを示しています。

現在の Threat Defense /Management Center 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。

（注） 自動スケーリングのサポートに必要なインターフェースの変更により、GCP 向け Threat Defense Virtual のアップグレードはバージョン 7.2.0 を飛び越すことができません。つまり、バージョン 7.1.x 以前からバージョン 7.2.0 より後にアップグレードすることはできません。新しいインスタンスを展開し、デバイス固有の設定をやり直す必要があります。

表 *2 : Threat Defense* 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
7.2	→ 以降の 7.2.x メンテナンスリリース
7.1	次のいずれかです。 → 7.2 または 7.2.x メンテナンスリリース → 以降の 7.1.x メンテナンスリリース
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。 → 7.2 または 7.2.x メンテナンスリリース → 7.1 または 7.1.x メンテナンスリリース → 7.0.x 以降のメンテナンスリリース （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） クラウド提供型の管理センターは、バージョン 7.1 を実行している脅威防御デバイス、または任意のバージョンを実行しているデバイスを管理できません。クラウド管理を登録解除して無効にしない限り、クラウド提供型の管理センターに登録されている脅威防御デバイスをバージョン 7.0.x からバージョン 7.1 にアップグレードすることはできません。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。

現在のバージョン	ターゲットバージョン
6.7	次のいずれかです。 → 7.2 または 7.2.x メンテナンスリリース → 7.1 または 7.1.x メンテナンスリリース → 7.0 または 7.0.x メンテナンスリリース → 6.7.x メンテナンスリリース以降
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 または 7.2.x メンテナンスリリース → 7.1 または 7.1.x メンテナンスリリース → 7.0 または 7.0.x メンテナンスリリース → 6.7 または 6.7.x メンテナンスリリース → 6.6.x メンテナンスリリース以降
6.5	次のいずれかです。 → 7.1 または 7.1.x メンテナンスリリース → 7.0 または 7.0.x メンテナンスリリース → 6.7 または 6.7.x メンテナンスリリース → 6.6 または 6.6.x メンテナンスリリース
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 または 7.0.x メンテナンスリリース → 6.7 または 6.7.x メンテナンスリリース → 6.6 または 6.6.x メンテナンスリリース → 6.5
6.3	次のいずれかです。 → 6.7 または 6.7.x メンテナンスリリース → 6.6 または 6.6.x メンテナンスリリース → 6.5 → 6.4

現在のバージョン	ターゲットバージョン
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 または 6.6.x メンテナンスリリース → 6.5 → 6.4 → 6.3

アップグレードパッケージのアップロード

Threat Defense アップグレードパッケージを Management Center または内部 Web サーバーにアップロードした後、それらをデバイスにコピーできます。

Management Center への Threat Defense 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、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、パッケージが確認されるため、Management Center 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 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から のアップグレードパッケージをダウンロードします。

ファミリまたはシリーズのすべてのモデルに同じソフトウェア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、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。

Firepower 1000 シリーズ	Cisco_FTD_SSP-FP1K_Upgrade-7.2-999.sh.REL.tar
Firepower 2100 シリーズ	Cisco_FTD_SSP-FP2K_Upgrade-7.2-999.sh.REL.tar
Secure Firewall 3100 シリーズ	Cisco_FTD_SSP-FP3K_Upgrade-7.2-999.sh.REL.tar
Firepower 4100/9300	Cisco_FTD_SSP_Upgrade-7.2-999.sh.REL.tar
Threat Defense Virtual	Cisco_FTD-7.2-999.sh.REL.tar
ISA 3000	Cisco_FTD-7.2-999.sh.REL.tar

ステップ 2 Management Center で、**[システム（System）] > [更新（Updates）]** を選択します。

ステップ 3 [更新のアップロード（Upload Update）] をクリックします。

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。Management Center がインターネットにアクセスできる場合は、代わりに [アップデートのダウンロード（Download Updates）] をクリックして、展開の対象となるすべてのパッケージと、必要に応じて最新の VDB をダウンロードできます。

ステップ 4 [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 5 [Choose File] をクリックします。

ステップ 6 パッケージを参照し、[Upload] をクリックします。

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、Threat Defense 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（System）] > [更新（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お勧めします。

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。

この時点でパッケージをすべての対象デバイスにコピーするか、サブセットにコピーしてから 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することができます。Threat Defense アップグレードパッケージのデバイス間のコピー （14 ページ） を参照してください。

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。

Threat Defense アップグレードパッケージの内部サーバーへのアップロード

この手順を使用して、Management Center 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 Threat Defense デバイスを設定します。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。

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、Management Center 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、Management Center 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

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 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から のアップグレードパッケージをダウンロードします。

ファミリまたはシリーズのすべてのモデルに同じソフトウェア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、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。

Firepower 1000 シリーズ	Cisco_FTD_SSP-FP1K_Upgrade-7.2-999.sh.REL.tar
Firepower 2100 シリーズ	Cisco_FTD_SSP-FP2K_Upgrade-7.2-999.sh.REL.tar
Secure Firewall 3100 シリーズ	Cisco_FTD_SSP-FP3K_Upgrade-7.2-999.sh.REL.tar
Firepower 4100/9300	Cisco_FTD_SSP_Upgrade-7.2-999.sh.REL.tar
Threat Defense Virtual	Cisco_FTD-7.2-999.sh.REL.tar
ISA 3000	Cisco_FTD-7.2-999.sh.REL.tar

ステップ 2 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。

ステップ 3 Management Center で、**[システム（System）]** > **[更新（Updates）]** を選択します。

ステップ 4 [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 5 **アクション**については、**[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 6 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 7 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 8 **[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 9 （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、Threat Defense 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（System）]** > **[更新（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お勧めします。

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。

この時点でパッケージをすべての対象デバイスにコピーするか、サブセットにコピーしてから 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することができます。Threat Defense アップグレードパッケージのデバイス間のコピー （14 ページ） を参照してください。

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。

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。

バージョン 7.1 以降の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。
- クラウド提供型の管理センターによって管理されているが、分析モードでお客様が導入した 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。

Threat Defense のアップグレード準備状況チェック

Threat Defense 準備状況チェックを手動で実行するには、次の手順を使用します。

（注） デバイスのアップグレードが成功した後に復元を有効にする場合は、次の手順を使用して準備状況を確認します。それ以外の場合は、代わりにアップグレードウィザードを使用することをお勧めします。このウィザードでは、次のチェックを完了するように求められます。ウィザードを使用した Threat Defense のアップグレード（復元を無効化） （17 ページ）

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。準備状況チェックで不合格になると、問題を修正するまでアップグレードできません。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。

始める前に

チェックするデバイスの Management Center にアップグレードパッケージをアップロードします。または、内部 Web サーバー上の場所を指定します。

ステップ 1 Management Center で、**[システム（System）] > [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、チェックするデバイスの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。

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。

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。

ステップ 4 [準備状況の確認（Check Readiness）] をクリックします。

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できます。

次のタスク

[システム（System）] > **[更新（Updates）]**ページで、[準備状況チェック（Readiness Checks）]をクリックすると、進行中のチェックや不合格のチェックなど、展開全体の準備状況チェックのステータスが表示されます。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。

Threat Defense のアップグレード

Threat Defense をアップグレードする前に、使用する手順を決定します。

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）]**ページを使用し、Management Center で Threat Defense をアップグレードします。これは、「**アップグレード成功後の復元を可能にする**」オプションを設定する唯一の方法です。

重要 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。

ウィザードを使用した Threat Defense のアップグレード（復元を無効化）

Management Center には、Threat Defense をアップグレードするためのウィザードが用意されています。

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、アップグレード前の重要な段階を順を追って説明します。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が、管理者アクセス権を持つ他のユーザーはワークフローをリセット、変更、または続行できます（CAC でログインした場合を除きます。この場合、進行状況はログアウトしてから 24 時間後にクリアされます）。進行状況は、高可用性 Management Center 間でも同期されます。

⚠

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。一般的には、アップグレードウィザードを使用することをお勧めします。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、代わりに **[システム（System）]** > **[更新（Updates）]** ページを使用する必要があります。また、システム更新ページを使用してアップグレードパッケージをアップロードし、Management Center 自体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。

アップグレードするデバイスを選択します。

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

ステップ 2 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 3 [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）] メニューから、[Firepower ソフトウェアのアップグレード（Upgrade Firepower Software）] を選択します。

[デバイスアップグレード（Device Upgrade）] ページが表示され、選択したデバイスの数が示され、ターゲット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] と右側の [デバイスの詳細] の 2 つのペインがあります。[デバイスの選択（Device Selection）] でデバイスリンク（「4 つのデバイス」 など）をクリックして、デバイス詳細を表示します。

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 4 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。

アップグレードパッケージをデバイスにコピーします。

ステップ 5 [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。削除したくなければ、不要なデバイスは削除する必要はありません。それらは次のステップには含まれません。

[アップグレード先（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リストにない場合は、[システム（System）] > [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。

ステップ 6 アップグレードパッケージがまだ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] をクリックして、選択を確認します。

Threat Defense 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アプライアンスにある必要があります。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。

ヒント Threat Defense CLI を使用して、アップグレードパッケージをデバイス間でコピーすることもできます。資格要件などの詳細については、Threat Defense アップグレードパッケージのデバイス間のコピー （14 ページ）を参照してください。

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 7 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、[準備状況チェックの実行（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必要がある（Require passing compatibility and readiness checks option）] オプションを無効にすることでチェックをスキップできますが、お勧めしません。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、Firepower 4100/9300 で FXOS をアップグレードする必要がある場合、または管理対象デバイスに展開する必要がある場合は、システムによってすぐに警告されます。

ステップ 8 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 9 必要に応じて、[デバイスのアップグレード（Device Upgrade）] ページに戻ります。

進行状況は保持されています。保持されていない場合は、管理者アクセス権を持つ他の誰かがワークフローをリセット、変更、または完了した可能性があります。

ステップ 10 [Next] をクリックします。

アップグレードします。

ステップ 11 デバイスの選択とターゲットバージョンを確認します。

ステップ 12 （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 13 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。
- **Snort 2 から Snort 3 にアップグレードする**：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。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。

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 14 [アップグレードを開始（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、「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」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 15 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、**[Devices]** > **[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 16 （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 17 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 18 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 19 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）[デバイスのアップグレード（Device Upgrade）]ページに戻り、[完了（Finish）]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、[デバイスのアップグレード（Device Upgrade）]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。

で Threat Defense をアップグレード（復元を有効化）

この手順を使用して、Management Center の [システムアップデート（System Updates）] ページから Threat Defense をアップグレードします。

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。一般的には、アップグレードウィザードを使用することをお勧めします。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、この手順を使用します。
- 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。

ステップ 1 Management Center で、**[システム（System）] > [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て、アップグレードするデバイスを選択します。

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。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 3 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。
- **Snort 2 から Snort 3 にアップグレードする**：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。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。

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 4 [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、「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」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 5 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、**[Devices]** > **[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 6 （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 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。

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。