Firepower Threat Defense のアップグレード：その他の FTD デバイス

アップグレードチェックリスト：その他の FTD デバイス

このチェックリストを使用して、Firepower 1000/2100 シリーズ、ASA 5500-X シリーズ、ISA 3000、および FTDv デバイスをアップグレードします。

アップグレードを行うたびにチェックリストを完了します。ステップの実行を省略すると、アップグレードが失敗する場合があります。プロセスの間、展開環境内のアプライアンスが正常に通信していること、およびヘルスモニタによって報告された問題がないことを確認します。

アップグレードの計画

アップグレードパスを正しく計画し、そのパスに従うことによって、常に展開の互換性を保ちます。

✓	アクション/チェック	詳細
	アップグレードパスを確認する アップグレードパスにおける自分の位置を確認します。実行したアップグレードと次に実行するアップグレードを確認します。	アップグレードパス：その他の FTD デバイス （4 ページ）

✓	アクション/チェック	詳細
	バージョンを確認する デバイスの現在のバージョンと対象となるバージョンを確認します。 • Firepower Threat Defense ソフトウェア • 仮想ホスティング環境（FTDv）	Firepower デバイス
	FMC の互換性を確認する デバイスのアップグレード後に FMC がそのデバイスを管理できるかどうか確認します。管理できない場合は、最初に FMC をアップグレードするようアップグレードパスを修正します。	FMC デバイスのバージョン互換性を維持できるか
	リリースノートを読む 次のアップグレード/一連のアップグレードのリリースノートを読み、バージョン固有の警告とガイドラインに特に注意してください。	FirePOWER リリースノート

アップグレード前のアクションおよびチェック

メンテナンスウィンドウ外で事前チェックを実行することによって、中断を最小化します。

✓	アクション/チェック	詳細
	必要な設定変更を行う 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。	FirePOWER リリースノート
	ディスク容量を確認する FirePOWER ソフトウェアアップグレード用の予備のディスク容量を確認します。	時間テストとディスク容量の要件
	アップグレードパッケージを取得する 正しいアップグレードパッケージを取得して、FMC にアップロードします。署名付きの（.tar）パッケージは解凍しないでください。	アップグレードパッケージの取得およびプッシュ

✓	アクション/チェック	詳細
	帯域幅をチェックする FMC からデバイスに大容量のデータを転送するための帯域幅があることを確認します。	Guidelines for Downloading Data from the Firepower Management Center to Managed Deviceshttps://www.cisco.com/c/en/us/support/docs/security/firepower-management-center/212043-Guidelines-for-Downloading-Data-from.html（トラブルシューティング テクニカルノーツ）
	アップグレードパッケージをプッシュする アップグレードパッケージをデバイスにプッシュします。バージョン 6.2.3+ が必要です。	管理対象デバイスへのアップグレード パッケージのプッシュ
	準備状況チェックを実行する 準備状況チェックを実行します。バージョン 6.1+ が必要です。	準備状況チェックの実行
	デバイスをバックアップする FMC を使用して、物理 FTD デバイスおよび FTDv（VMware）の設定データをバックアップします。外部の場所にバックアップして、正常に転送されたことを確認します。その他の FTDv 実装についてはサポートされていません。バージョン 6.3+ が必要です。	Firepower Management Center Configuration Guide
	アプライアンスへのアクセスを確認する お使いのコンピュータが FMC の管理インターフェイスとデバイスの管理インターフェイスに、どちらもデバイス自体を通過せずに接続できることを確認してください。	アップグレード時のアプライアンスへのアクセス
	メンテナンス時間帯をスケジュールする 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。実行する必要がある作業、トラフィックフローおよびインスペクションへのアップグレードの影響、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。	FTD アップグレード時の動作：その他のデバイス および 時間テストとディスク容量の要件

デバイスをアップグレードする

アップグレードによってトラフィックフローまたはインスペクションが中断する可能性があるため、メンテナンスウィンドウでアップグレードを実行します。

✓	アクション/チェック	詳細
	ホスティングをアップグレードする 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（FTDv）。	ホスティング環境のドキュメンテーションを参照してください。
	FirePOWER ソフトウェアのアップグレード FirePOWER ソフトウェアをアップグレードします。	FTD ソフトウェアのアップグレード：その他の FTD デバイス （5 ページ）

アップグレードパス：その他の FTD デバイス

次の表に、Firepower Management Center によって管理される、バンドル オペレーティング システムを搭載した Firepower Theat Defense デバイス（Firepower 1000 シリーズ、Firepower 2100 シリーズ、ASA 5500-X シリーズ、ISA 3000、および FTDv）のアップグレードパスを示します。現在のバージョンから目的のバージョンに直接アップグレードできない場合は、指示に従ってアップグレードパスに中間バージョンを含める必要があります。

（注） FTD ハイアベイラビリティペアのバージョン 6.1.0 へのヒットレスアップグレードを実行するには、プレインストールパッケージが必要です。詳細については、『Firepower System Release Notes Version 6.1.0 Preinstallation Package』を参照してください。

表 *1 :* 推奨されるアップグレードパス：*Firepower 1000/2100* シリーズ、*ASA 5500-X* シリーズ、*ISA 3000*、および *FMC* を搭載した *FTDv*

現在のバージョン	ターゲットバージョン						
	6.5.0	**6.4.0**	**6.3.0**	**6.2.3**	**6.2.2**	**6.2.0**	**6.1.0**
6.4.0	直接	—	—	—	—	—	—
6.3.0	直接	直接	—	—	—	—	—
6.2.3	直接	直接	直接	—	—	—	—
6.2.2	→6.4.0 → 6.5.0	直接	直接	直接	—	—	—
6.2.1	→6.4.0 → 6.5.0	直接	直接	直接	直接	—	—
6.2.0	→6.4.0 → 6.5.0	直接	直接	直接	直接	—	—

現在のバージョン	ターゲットバージョン						
	6.5.0	**6.4.0**	**6.3.0**	**6.2.3**	**6.2.2**	**6.2.0**	**6.1.0**
6.1.0	→6.4.0 → 6.5.0	直接	直接	直接	→ 6.2.0 → 6.2.2	直接	—
6.0.1	→ 6.1.0 →6.4.0 → 6.5.0	→ 6.1.0 →6.4.0	→ 6.1.0 → 6.3.0	→ 6.1.0 → 6.2.3	→ 6.1.0 → 6.2.0 → 6.2.2	→ 6.1.0 → 6.2.0	直接

FTD ソフトウェアのアップグレード：その他の FTD デバイス

この手順を使用して、Firepower 1000/2100 シリーズ、ASA 5500-X シリーズ、ISA 3000、およびFTDvデバイスをアップグレードします。複数のデバイスで同じアップグレードパッケージが使用されている場合、複数のデバイスを同時にアップグレードできます。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。

注意 アップグレードしているアプライアンスとの間での変更の展開、またはアップグレードしているアプライアンスの手動での再起動やシャットダウンは行わないでください。進行中のアップグレードを再開しないでください。事前のチェック中に、アップグレードプロセスが停止しているように見える場合がありますが、これは想定内の動作です。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 Cisco TAC にお問い合わせください。

始める前に

仮想ホスティング環境と FMC のアップグレードを含め、アップグレード パス内の場所を確認します。この手順を完全に計画して準備していることを確認します。

ステップ 1 アップグレード対象デバイスに構成を展開します。

メニューバーで、[展開（Deploy）] をクリックします。FMCデバイスを選択し、[展開（Deploy）] をもう一度クリックします。アップグレードする前に展開すると、失敗する可能性が減少します。

展開する際にリソースを要求すると、いくつかのパケットがインスペクションなしでドロップされることがあります。 さらに、いくつかの設定を展開することで Snort が再起動されます。これにより、トラフィックのインスペクションが中断し、デバイスのトラフィックの処理方法によっては、再起動が完了するまでトラフィックが中断する場合があります。詳細については、FTD アップグレード時の動作：その他のデバイス を参照してください。

ステップ 2 アップグレード前の最終的なチェックを実行します。

- 正常性のチェック：メッセージセンターを使用します（メニューバーの[システムステータス（System Status）] アイコンをクリックします）。導入環境内のアプライアンスが正常に通信していること、およびヘルス モニタによって報告された問題がないことを確認します。
- タスクの実行：また、メッセージセンターで、必須タスク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。後で失敗ステータスメッセージを手動で削除できます。
- ディスク容量のチェック：最終的なディスク容量の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。ディスク容量の要件については、「時間テストとディスク容量の要件」を参照してください。

ステップ 3 （オプション、ハイ アベイラビリティのみ）ハイ アベイラビリティ デバイス ペアのアクティブ/スタンバイの役割を切り替えます。

ハイ アベイラビリティ ペアのスタンバイ デバイスが最初にアップグレードされます。デバイスの役割が切り替わり、新しくスタンバイになったデバイスがアップグレードされます。アップグレードの完了時には、デバイスの役割は切り替わったままです。アクティブ/スタンバイの役割を維持する場合、アップグレード前に役割を手動で切り替えます。それにより、アップグレード プロセスによって元の役割に切り替わります。

[デバイス（Devices）] > [デバイス管理（Device Management）] を選択し、ペアの横にある [アクティブ ピアの切り替え（Switch Active Peer）] アイコンをクリックして、選択内容を確認します。

ステップ 4 **[システム（System）] > [更新（Updates）]** を選択します。

ステップ 5 使用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。

（注） 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。FMC では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 6 [インストール（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。

一部のデバイスは、アップグレード時に 2 回再起動することがありますが、これは想定内の動作です。

トラフィックは、デバイスの設定および展開方法に応じて、アップグレードの間ドロップするか、検査なしでネットワークを通過します。詳細については、FTD アップグレード時の動作：その他のデバイスを参照してください。

ステップ 7 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。

デバイスのアップグレード中は、構成をそのデバイスに展開しないでください。メッセージ センターに進行状況が数分間表示されない、またはアップグレードが失敗したことが示されている場合でも、アッ

プグレードを再開したり、デバイスを再起動したりしないでください。代わりに、Cisco TAC にお問い合わせください。

ステップ 8 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 9 メッセージ センターを使用して、導入環境に問題がないことを再度確認します。

ステップ 10 侵入ルール（SRU）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 & ダウンロード サイトで利用可能な SRU や VDB 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。詳細については、Firepower Management Center Configuration Guideを参照してください。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 11 リリース ノートに記載されているアップグレード後の構成の変更をすべて完了します。

ステップ 12 アップグレードしたデバイスに構成を再度展開します。