



# Firepower Management Center のアップグレード

- [アップグレード チェックリスト : Firepower Management Center \(1 ページ\)](#)
- [スタンドアロンの Firepower Management Center のアップグレード \(6 ページ\)](#)
- [ハイ アベイラビリティ Firepower Management Center のアップグレード \(7 ページ\)](#)

## アップグレード チェックリスト : Firepower Management Center

FMC (FMCvを含む) のアップグレードを行う前にこのチェックリストを完了します。ハイアベイラビリティペアをアップグレードする場合は、チェックリストをペアごとに完了します。



- (注) プロセス中は常に、展開の通信と正常性を維持してください。進行中に FMC 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。

### 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。

表 1:

| ✓ | アクション/チェック                                                                                                                                                                                                                                                                                                                                                                                       |
|---|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|   | <p><b>アップグレードパスを計画します。</b></p> <p>これは、マルチアプライアンス展開、マルチホップアップグレード、または展開の互換性を常に維持しながら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。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常に確認します。</p> <p>(注)<br/>FMC 展開では、通常、FMC をアップグレードしてから、管理対象デバイスをアップグレードします。ただし、場合によっては、最初にデバイスをアップグレードする必要があります。</p> <p><a href="#">アップグレードパス</a>を参照してください。</p>                                                                      |
|   | <p><b>すべてのアップグレードのガイドラインを読み、設定の変更を計画します。</b></p> <p>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。アップグレードの警告、動作の変更、新機能と廃止された機能、および既知の問題など、リリース固有の重要な情報を含むリリースノートから読み始めます。</p>                                                                                                                                                                                                      |
|   | <p><b>帯域幅を確認します。</b></p> <p>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。FMC の展開では、アップグレードパッ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。デバイスのアップグレードを開始する前に、可能な場合は常に、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。</p> <p>『<a href="#">Guidelines for Downloading Data from the Firepower Management Center to Managed Devices</a>』（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。</p> |
|   | <p><b>メンテナンス時間帯をスケジュールします。</b></p> <p>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、ウィンドウ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。たとえば、メンテナンス時間帯で、アプライアンスへのアップグレードパッケージのコピー、準備状況チェックの実行、バックアップの作成などが行われるまで待機しないようにします。</p>                                                                                                                                    |

## 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。

表 2:

| ✓ | アクション/チェック                                                                                                                                                                                                                                                                                          |
|---|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|   | <p><b>アップグレードパッケージをアップロードします。</b></p> <p>FMC の高可用性の展開では、FMC アップグレードパッケージを両方のピアにアップロードし、パッケージをスタンバイに転送する前に同期を一時停止する必要があります。HA 同期の中断を制限するには、アップグレードの準備段階でパッケージをアクティブのピアに転送し、同期を一時停止した後に、実際のアップグレードプロセスの一環としてスタンバイのピアに転送します。</p> <p><a href="#">Firepower Management Center にアップロード</a> を参照してください。</p> |

### バックアップ

災害から回復する能力は、システム保守計画の重要な部分を占めます。

バックアップと復元は、複雑なプロセスになる可能性があります。手順をスキップしたり、セキュリティやライセンスの問題を無視しないでください。バックアップと復元の要件、ガイドライン、制限事項、およびベストプラクティスの詳細については、使用する展開の設定ガイドを参照してください。



**注意** 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。

表 3:

| ✓ | アクション/チェック                                                                                                                                                                                                                                                                                                                                                                                                                      |
|---|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|   | <p><b>バックアップします。</b></p> <p>アップグレードの前後にバックアップします（サポートされている場合）。</p> <ul style="list-style-type: none"> <li>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。</li> <li>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。FMC の展開では、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、新しい FMC バックアップファイルにデバイスがアップグレードされたことを「認識」させることをお勧めします。</li> </ul> |

### 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。

表 4:

| ✓ | アクション/チェック                                                                                                                       |
|---|----------------------------------------------------------------------------------------------------------------------------------|
|   | <p>仮想ホスティングをアップグレードします。</p> <p>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、FMC の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。</p> |

## 最終チェック

一連の最終チェックにより、 をアップグレードする準備が整います。

表 5:

| ✓ | アクション/チェック                                                                                                                                                                                                                                                                                                                                                                                        |
|---|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|   | <p>設定を確認します。</p> <p>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。</p>                                                                                                                                                                                                                                                                                                                   |
|   | <p><b>NTP 同期を確認します。</b></p> <p>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。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。FMC 展開では、時刻のずれが 10 秒を超えている場合、ヘルスマニタ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。</p> <p>時刻を確認するには、次の手順を実行します。</p> <ul style="list-style-type: none"> <li>• FMC : [システム (System)] &gt; [設定 (Configuration)] &gt; [時刻 (Time)] を選択します。</li> <li>• デバイス : <b>show time</b> CLI コマンドを使用します。</li> </ul> |
|   | <p><b>ディスク容量を確認します。</b></p> <p>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。</p> <p>対象バージョンの <a href="#">Cisco Firepower リリース ノート</a> 内の「ソフトウェアのアップグレード」の章を参照してください。</p>                                                                                                                                                                                                      |

|   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|---|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ✓ | アクション/チェック                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|   | <p>設定を展開します。</p> <p>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。一部の展開では、設定が古い場合、アップグレードがブロックされることがあります。FMC における高可用性の展開では、アクティブなピアから展開するだけで済みます。</p> <p>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。</p> <p>対象バージョンの <a href="#">Cisco Firepower リリース ノート</a> 内の「ソフトウェアのアップグレード」の章を参照してください。</p>                                                                                                                             |
|   | <p>準備状況チェックを実行します。</p> <p>FMC がバージョン 6.1.0 以降を実行している場合は、互換性と準備状況のチェックの実施をお勧めします。これらのチェックにより、ソフトウェアをアップグレードするための準備状況を確認できます。</p> <p><a href="#">Firepower ソフトウェアの準備状況チェック</a> を参照してください。</p>                                                                                                                                                                                                                                                                                                                                                |
|   | <p>実行中のタスクを確認します。</p> <p>アップグレードする前に、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。また、アップグレード中に実行するようにスケジュールされたタスクを確認し、それらをキャンセルまたは延期することをお勧めします。</p> <p>(注)</p> <p>一部の展開では、アップグレードするとスケジュールされたタスクが自動的に延期されるようになりました。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。</p> <p>この機能は現在、バージョン 6.4.0.10 以降のパッチ、バージョン 6.6.3 以降のメンテナンスリリース、およびバージョン 6.7.0 以降を実行している FMC でサポートされています。この機能は、サポートされているバージョンからのすべてのアップグレードでサポートされていることに注意してください。この機能は、サポートされていないバージョンからサポートされているバージョンへのアップグレードではサポートされていません。</p> |

# スタンドアロンの Firepower Management Center のアップグレード

この手順を使用して、Firepower Management Center Virtual を含め、スタンドアロンの Firepower Management Center をアップグレードします。



**注意** 構成の変更の実行または展開、手動による再起動、または FMC のアップグレード中の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

事前アップグレードのチェックリストを完了します。展開したアプライアンスが正常で、きちんと通信していることを確認します。

## 手順

- ステップ 1** [システム (System)] > [更新 (Updates)] を選択します。
- ステップ 2** 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、FMC を選択します。
- ステップ 3** [インストール (Install)] をクリックすると、アップグレードが開始されます。  
アップグレードして再起動することを確認します。
- ステップ 4** ログアウトするまで、事前チェックの進行状況をモニターします。この間、構成の変更を行わないでください。
- ステップ 5** 可能なときに、再度ログインします。
  - マイナーアップグレード（パッチとホットフィックス）：アップグレードと再起動が完了した後にログインできます。
  - 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：アップグレードが完了する前にログインできます。アップグレードの進行状況をモニターし、アップグレードログとエラーメッセージを確認するために使用できるページが表示されます。アップグレードが完了し、システムが再起動すると再度ログアウトされます。リブート後に、再ログインしてください。
- ステップ 6** プロンプトが表示されたら、エンドユーザー ライセンス契約書 (EULA) を確認し、承認します。
- ステップ 7** アップグレードが成功したことを確認します。

ログイン時にアップグレードの成功メッセージが表示されない場合は、[ヘルプ (Help)] > [バージョン情報 (About)] を選択して、現在のソフトウェアのバージョン情報を表示します。

**ステップ 8** 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 9** 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 10** 構成を再展開します。

すべての管理対象デバイスに再展開します。デバイスに構成を展開しない場合、最終的なアップグレードが失敗し、イメージの再作成が必要になることがあります。

## ハイ アベイラビリティ Firepower Management Center のアップグレード

この手順を使用して、ハイアベイラビリティペアに含まれる FMC の Firepower ソフトウェアをアップグレードします。

一度に1つのピアをアップグレードします。同期を一時停止して、まずスタンバイをアップグレードしてから、アクティブにします。スタンバイで事前チェックが開始されると、ステータスがスタンバイからアクティブに切り替わり、両方のピアがアクティブになります。この一時的な状態は *split-brain* と呼ばれていて、アップグレード中を除き、サポートされていません。ペアが *split-brain* の状態で、構成の変更または展開を行わないでください。同期の再開後は変更内容が失われます。



**注意** 構成の変更の実行または展開、手動による再起動、または FMC のアップグレード中の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

両方のピアの事前アップグレードチェックリストを完了します。展開したアプライアンスが正常で、きちんと通信していることを確認します。

## 手順

**ステップ 1** 同期を一時停止します。

- a) **[システム (System)] > [統合 (Integration)]** を選択します。
- b) **[ハイ アベイラビリティ (High Availability)]** タブで、**[同期の一時停止 (Pause Synchronization)]** をクリックします。

**ステップ 2** アップグレードパッケージをスタンバイにアップロードします。

FMC の高可用性の展開では、FMC アップグレードパッケージを両方のピアにアップロードし、パッケージをスタンバイに転送する前に同期を一時停止する必要があります。HA 同期の中断を制限するには、アップグレードの準備段階でパッケージをアクティブのピアに転送し、同期を一時停止した後に、実際のアップグレードプロセスの一環としてスタンバイのピアに転送します。

**ステップ 3** ピアを一度に 1 つずつアップグレード：最初はスタンバイ、次はアクティブです。

「[スタンドアロンの Firepower Management Center のアップグレード \(6 ページ\)](#)」の手順に従います。各ピアで更新が成功したことを確認したら停止します。要約すると、各ピアで次の手順を実行します。

- a) **[システム (System)] > [更新 (Updates)]** ページで、アップグレードをインストールします。
- b) ログアウトするまで進行状況をモニターし、可能な場合な再度ログインします（これは主なアップグレードで 2 回行われます）。
- c) アップグレードが成功したことを確認します。

ペアが split-brain の状態で、構成の変更または展開を行わないでください。

**ステップ 4** 同期を再開します。

- a) アクティブピアにする FMC にログインします。
- b) **[システム (System)] > [統合 (Integration)]** の順に選択します。
- c) **[ハイ アベイラビリティ (High Availability)]** タブで、**[アクティブにする (Make-Me-Active)]** をクリックします。
- d) 同期が再開し、その他の FMC がスタンバイモードに切り替わるまで待ちます。

**ステップ 5** 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 6** 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 7** 構成を再展開します。

すべての管理対象デバイスに再展開します。デバイスに構成を展開しない場合、最終的なアップグレードが失敗し、イメージの再作成が必要になることがあります。



## 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。