



## 使用する前に

- [対象読者](#) (1 ページ)
- [アップグレードの計画](#) (3 ページ)
- [機能の履歴](#) (5 ページ)
- [支援が必要な場合](#) (13 ページ)

## 対象読者

このガイドでは、バージョン 7.1 を搭載した **Firepower Management Center** を使用して、アップグレードを準備し、確実に実行する方法について説明します。

- 現在管理されている FTD デバイスのバージョン 7.1 までのアップグレード。
- バージョン 7.1 以降のリリースへの FMC のアップグレード。

### 関連リソース

別のプラットフォームやコンポーネントをアップグレードする場合、別のバージョンから、または別のバージョンにアップグレードする場合、あるいはクラウドベースのマネージャを使用する場合は、以下に示す関連情報を参照してください。

表 1: FMC のアップグレード

現在の FMC のバージョン	ガイド
クラウド提供型の管理センター (バージョンなし)	なし。更新はシスコが行います。
7.2 以降	お使いのバージョンの『 <a href="#">Cisco Secure Firewall Threat Defense Upgrade Guide for Management Center</a> 』
7.1	『 <a href="#">Cisco Firepower Threat Defense Upgrade Guide for Firepower Management Center, Version 7.1</a> 』

現在のFMCのバージョン	ガイド
7.0 以前	<a href="#">Cisco Firepower Management Center Upgrade Guide, Version 6.0–7.0</a>

表 2: FMC を使用した FTD のアップグレード

現在のFMCのバージョン	ガイド
クラウド提供型の管理センター (バージョンなし)	最新のリリースバージョンの『 <a href="#">Cisco Secure Firewall Threat Defense Upgrade Guide for Management Center</a> 』
7.2 以降	お使いのバージョンの『 <a href="#">Cisco Secure Firewall Threat Defense Upgrade Guide for Management Center</a> 』
7.1	『 <a href="#">Cisco Firepower Threat Defense Upgrade Guide for Firepower Management Center, Version 7.1</a> 』
7.0 以前	<a href="#">Cisco Firepower Management Center Upgrade Guide, Version 6.0–7.0</a>

表 3: FDM を使用した FTD のアップグレード

現在のFTDのバージョン	ガイド
7.2 以降	お使いのバージョンの『 <a href="#">Cisco Secure Firewall Threat Defense Upgrade Guide for Device Manager</a> 』
7.1	『 <a href="#">Cisco Firepower Threat Defense Upgrade Guide for Firepower Device Manager, Version 7.1</a> 』
7.0 以前	『 <a href="#">Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager</a> 』内の「System Management」。  Firepower 4100/9300 については、 <a href="#">Cisco Firepower 4100/9300 アップグレードガイド</a> 、FXOS 1.1.1 ~ 2.10.1 を使用した FTD 6.0.1 ~ 7.0.x または ASA 9.4 (1) ~ 9.16 (x) の FXOS のアップグレード手順も参照してください。
バージョン 6.4 以降、CDO 使用	<a href="#">Cisco Defense Orchestrator</a> での FDM デバイスの管理の「Onboard Devices and Services」。

表 4: NGIPS デバイスのアップグレード

現在のマネージャバージョン	プラットフォーム	ガイド
いずれか	Firepower 7000/8000 シリーズ	<a href="#">Cisco Firepower Management Center Upgrade Guide, Version 6.0-7.0</a>
いずれか	FMC を搭載した ASA FirePOWER	<a href="#">Cisco Firepower Management Center Upgrade Guide, Version 6.0-7.0</a>
いずれか	ASDM を使用した ASA FirePOWER	<a href="#">Cisco Secure Firewall ASA アップグレードガイド</a>

表 5: その他のコンポーネントのアップグレード

Version	コンポーネント	ガイド
いずれか	Firepower 4100/9300 上の ASA 論理デバイス	<a href="#">Cisco Secure Firewall ASA アップグレードガイド</a> 。
最新	FMC 用の BIOS およびファームウェア	<a href="#">Cisco Secure Firewall Threat Defense/Firepower ホットフィックス リリース ノート</a> 。
最新	Firepower 4100/9300 のファームウェア	<a href="#">Cisco Firepower 4100/9300 FXOS ファームウェア アップグレードガイド</a>
最新	ISA 3000 の ROMMON イメージ	<a href="#">Cisco Secure Firewall ASA および Secure Firewall Threat Defense 再イメージ化ガイド</a> 。

## アップグレードの計画

誤りを避けるには、注意深い計画と準備が役立ちます。この表はアップグレードの計画プロセスを要約したものです。詳細なチェックリストと手順については、アップグレードの章を参照してください。

表 6: アップグレードの計画フェーズ

計画フェーズ	次を含む
計画と実現可能性	<p>展開を評価します。</p> <p>アップグレードパスを計画します。</p> <p>すべての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。</p> <p>アプライアンスへのアクセスを確認します。</p> <p>帯域幅を確認します。</p> <p>メンテナンス時間帯をスケジュールします。</p>
バックアップ	<p>ソフトウェアをバックアップします。</p> <p>Firepower 4100/9300 の FXOS をバックアップします。</p>
アップグレードパッケージ	<p>アップグレードパッケージをシスコからダウンロードします。</p> <p>システムにアップグレードパッケージをアップロードします。</p>
関連するアップグレード	<p>仮想展開内で仮想ホスティングをアップグレードします。</p> <p>Firepower 4100/9300 のファームウェアをアップグレードします。</p> <p>Firepower 4100/9300 の FXOS をアップグレードします。</p>
最終チェック	<p>設定を確認します。</p> <p>NTP 同期を確認します。</p> <p>設定を展開します。</p> <p>準備状況チェックを実行します。</p> <p>ディスク容量を確認します。</p> <p>実行中のタスクを確認します。</p> <p>展開の正常性と通信を確認します。</p>

# 機能の履歴

表 7:バージョン 7.1.0の機能

機能	説明
<p>正常なデバイスアップグレードを元に戻します。</p>	<p>メジャーおよびメンテナンスアップグレードをFTDに戻すことができるようになりました。復元すると、ソフトウェアは、最後のアップグレードの直前の状態に戻ります（スナップショットとも呼ばれます）。パッチのインストール後にアップグレードを元に戻すと、パッチだけでなく、メジャーアップグレードやメンテナンスアップグレードも元に戻されます。</p> <p><b>重要</b> 元に戻す必要がある可能性があると思われる場合は、システム (⚙️) &gt;[更新 (Updates)] ページを使用してFTDをアップグレードする必要があります。[システムの更新 (System Updates)] ページは、[アップグレード後の復元を有効にする (Enable revert after successful upgrade)] オプションを有効にできる唯一の場所です。このオプションでは、アップグレードの開始時に復元スナップショットを保存するようにシステムが設定されます。これは、[デバイス (Devices)] &gt;[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。</p> <p>この機能は、コンテナインスタンスではサポートされません。</p> <p>必要最低限の Threat Defense、顧客展開の Management Center : 7.1</p> <p>必要最低限の Threat Defense、クラウド提供型 Firewall Management Center : 7.2</p>

機能	説明
<p>クラスタ化された高可用性デバイスのアップグレードワークフローの改善。</p>	<p>クラスタ化された高可用性デバイスのアップグレードワークフローが次のように改善されました。</p> <ul style="list-style-type: none"> <li>• アップグレードウィザードは、個々のデバイスとしてではなく、グループとして、クラスタ化された高可用性ユニットを正しく表示するようになりました。システムは、発生する可能性のあるグループ関連の問題を特定し、報告し、事前に修正を要求できます。たとえば、Firepower Chassis Manager で非同期の変更を行った場合は、Firepower 4100/9300 のクラスタをアップグレードできません。</li> <li>• アップグレードパッケージをクラスタおよび高可用性ペアにコピーする速度と効率が向上しました。以前は、FMC はパッケージを各グループメンバーに順番にコピーしていました。これで、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るようになりました。</li> <li>• クラスタ内のデータユニットのアップグレード順序を指定できるようになりました。コントロールユニットは常に最後にアップグレードされます。</li> </ul>

表 8:バージョン 7.0.0 の機能

機能	説明
<p>FTD のアップグレードパフォーマンスとステータスレポートの改善。</p>	<p>FTD のアップグレードがより簡単かつ確実に、より少ないディスク容量で実行できるようになりました。メッセージセンターの新しい [アップグレード (Upgrades)] タブでは、アップグレードステータスとエラーレポートがさらに強化されています。</p>

機能	説明
FTD デバイスのわかりやすいアップグレードワークフロー。	

機能	説明
	<p>FMC の新しいデバイス アップグレード ページ ([デバイス (Devices) ]&gt;[デバイスアップグレード (Device Upgrade) ]) には、バージョン 6.4 以降の FTD デバイスをアップグレードするためのわかりやすいウィザードがあります。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。</p> <p>開始するには、[デバイス管理 (Device Management) ] ページ ([デバイス (Devices) ]&gt;[デバイス管理 (Device Management) ]&gt;[アクションの選択 (Select Action) ]) で新しい [Firepower ソフトウェアのアップグレード (Upgrade Firepower Software) ] アクションを使用します。</p> <p>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。</p> <p>ウィザードから移動しても、進行状況は保持されます。ただし、管理者アクセス権を持つ他のユーザーはウィザードをリセット、変更、または続行できます。</p> <p>(注) FTD の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するには、引き続き <b>システム (⚙)</b> &gt;[更新 (Updates) ]を使用する必要があります。また、[システム更新 (System Updates) ] ページを使用して、FMC 自体、およびすべての非 FTD 管理対象デバイスをアップグレードする必要があります。</p> <p>(注) バージョン 7.0 では、ウィザードにクラスタまたは高可用性ペアのデバイスが正しく表示されません。これらのデバイスは1つのユニットとして選択してアップグレードする必要がありますが、ウィザードにはスタンドアロンデバイスとして表示されます。デバイスのステータスとアップグレードの準備状況は、個別に評価および報告されます。つまり、1つのユニットが「合格」して次の段階に進んでいるように見えても、他のユニットは合格していない可能性があります。ただし、それらのデバイスはグループ化されたままです。1つのユニットで準備状況チェックを実行すると、すべてのユニットで実行されます。1つユニットでアップグレードを開始すると、すべてのユニッ</p>

機能	説明
	<p>トで開始されます。</p> <p>時間がかかるアップグレードの失敗を回避するには、[次へ (Next) ]をクリックする前に、すべてのグループメンバーがウィザードの次のステップに進む準備ができていることを手動で確認します。</p>
<p>多くのFTDデバイスを一度にアップグレードします。</p>	<p>FTD アップグレードウィザードでは、次の制限が解除されません。</p> <ul style="list-style-type: none"> <li>• デバイスの同時アップグレード。                     <p>一度にアップグレードできるデバイスの数は、同時アップグレードを管理するシステムの機能ではなく、管理ネットワークの帯域幅によって制限されます。以前は、一度に5台を上回るデバイスをアップグレードしないことを推奨していました。</p> <p><b>重要</b> この改善は、FTDバージョン6.7以降へのアップグレードでのみ確認できます。デバイスを古いFTDリリースにアップグレードする場合は、新しいアップグレードウィザードを使用している場合でも、一度に5台のデバイスに制限することをお勧めします。</p> </li> <li>• デバイスモデルによるアップグレードのグループ化。                     <p>システムが適切なアップグレードパッケージにアクセスできる限り、すべてのFTDモデルのアップグレードを同時にキューに入れて呼び出すことができます。</p> <p>以前は、アップグレードパッケージを選択し、そのパッケージを使用してアップグレードするデバイスを選択していました。つまり、アップグレードパッケージを共有している場合にのみ、複数のデバイスを同時にアップグレードできました。たとえば、2台のFirepower 2100シリーズデバイスは同時にアップグレードできますが、Firepower 2100シリーズとFirepower 1000シリーズはアップグレードできません。</p> </li> </ul>

表 9:バージョン 6.7.0の機能

機能	説明
FTD アップグレードステータスレポートとキャンセル/再試行オプションの改善。	

機能	説明
	<p>[デバイス管理 (Device Management)] ページで、進行中の FTD デバイスアップグレードと準備状況チェックのステータス、およびアップグレードの成功/失敗の 7 日間の履歴を表示できるようになりました。メッセージセンターでは、拡張ステータスとエラーメッセージも提供されます。</p> <p>デバイス管理とメッセージセンターの両方からワンクリックでアクセスできる新しい [Upgrade Status] ポップアップに、残りのパーセンテージ/時間、特定のアップグレード段階、成功/失敗データ、アップグレードログなどの詳細なアップグレード情報が表示されます。</p> <p>また、このポップアップで、失敗したアップグレードまたは進行中のアップグレードを手動でキャンセル ([Cancel Upgrade]) することも、失敗したアップグレードを再試行 ([Retry Upgrade]) することもできます。アップグレードをキャンセルすると、デバイスはアップグレード前の状態に戻ります。</p> <p>(注) 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には、アップグレード時に表示される新しい自動キャンセルオプションを無効にする必要があります ([アップグレードに失敗すると自動的にキャンセルされ、前のバージョンにロールバックする (Automatically cancel on upgrade failure and roll back to the previous version)] )。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。</p> <p>パッチの自動キャンセルはサポートされていません。高可用性または拡張性の展開では、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。</p> <p>新規/変更された画面：</p> <ul style="list-style-type: none"> <li>• FTD アップグレードパッケージの [システム (System)] &gt; [更新 (Update)] &gt; [製品アップデート (Product Updates)] &gt; [利用可能なアップデート (Available Updates)] &gt; [インストール (Install)] アイコン</li> <li>• [Devices] &gt; [Device Management] &gt; [Upgrade]</li> <li>• [Message Center] &gt; [Tasks]</li> </ul> <p>新しい FTD CLI コマンド</p>

機能	説明
	<ul style="list-style-type: none"> <li>• <b>show upgrade status detail</b></li> <li>• <b>show upgrade status continuous</b></li> <li>• <b>show upgrade status</b></li> <li>• <b>upgrade cancel</b></li> <li>• <b>upgrade retry</b></li> </ul>
アップグレードでディスク容量を節約するために PCAP ファイルが削除される。	アップグレードにより、ローカルに保存された PCAP ファイルが削除されるようになりました。アップグレードするには、十分な空きディスク容量が必要です。これがない場合、アップグレードは失敗します。

表 10:バージョン 6.6.0の機能

機能	説明
内部 Web サーバーからデバイスアップグレードパッケージを取得します。	<p>デバイスは、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できるようになりました。これは、FMC とそのデバイスと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。</p> <p>新規/変更された画面 : [システム (System) ] &gt; [更新 (Updates) ] &gt; [更新のアップロード (Upload Update) ] ボタン &gt; [ソフトウェア更新ソースの指定 (Specify Software Update Source) ] オプション</p>
アップグレードがスケジュールされたタスクを延期する。	<p>FMC のアップグレードプロセスによって、スケジュールされたタスクが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>(注) アップグレードを開始する前に、実行中のタスクが完了していることを確認する必要があります。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。</p> <p>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。これには、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 以降が含まれます。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>

表 11:バージョン 6.4.0の機能

機能	説明
アップグレードがスケジュールされたタスクを延期する。	<p>FMCのアップグレードプロセスによって、スケジュールされたタスクが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>(注) アップグレードを開始する前に、実行中のタスクが完了していることを確認する必要があります。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。</p> <p>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。これには、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以降が含まれます。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>

表 12:バージョン 6.2.3の機能

機能	説明
アップグレードの前に、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>実際のアップグレードを実行する前に、FMCから管理対象デバイスにアップグレードパッケージをコピー（またはプッシュ）できるようになりました。帯域幅の使用量が少ない時間帯やアップグレードのメンテナンス期間外でプッシュできるため、この機能は便利です。</p> <p>高可用性デバイス、クラスタデバイス、またはスタック構成デバイスにプッシュすると、アップグレードパッケージは最初にアクティブ/コントロール/プライマリに送信され、次にスタンバイ/データ/セカンダリに送信されます。</p> <p>新規/変更された画面：[システム (System)] &gt; [更新 (Updates)]</p>

## 支援が必要な場合

### オンラインリソース

シスコは、ドキュメント、ソフトウェア、ツールのダウンロードのほか、バグを照会したり、サービスリクエストをオープンしたりするための次のオンラインリソースを提供しています。

これらのリソースは、Cisco ソフトウェアをインストールして設定したり、技術的問題を解決したりするために使用してください。

- マニュアル : <http://www.cisco.com/go/threatdefense-71-docs>
- シスコサポートおよびダウンロードサイト : <https://www.cisco.com/c/en/us/support/index.html>
- Cisco Bug Search Tool : <https://tools.cisco.com/bugsearch/>
- シスコ通知サービス : <https://www.cisco.com/cisco/support/notifications.html>

シスコ サポートおよびダウンロードサイトの大部分のツールにアクセスする際は、Cisco.com のユーザー ID およびパスワードが必要です。

### シスコへのお問い合わせ

上記のオンラインリソースを使用して問題を解決できない場合は、Cisco TAC にお問い合わせください。

- Cisco TAC の電子メール アドレス : [tac@cisco.com](mailto:tac@cisco.com)
- Cisco TAC の電話番号 (北米) : 1.408.526.7209 または 1.800.553.2447
- Cisco TAC の連絡先 (世界全域) : [Cisco Worldwide Support の連絡先](#)

## 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。