使用する前に

このガイドの対象読者

本ガイドでは、次のようなFirepowerバージョン**7.0.x 以前**へ正常にアップグレードを準備、および正常に完了する方法について説明します。

- Firepower Management Center（FMC）
- Firepower 4100/9300 用の FXOS を含む、FMC を搭載した Firepower Threat Defense（FTD）デバイス
- FMC を搭載した 7000/8000 シリーズのデバイス
- FMC を搭載した NGIPSv デバイス
- ASA OS を含む、FMC を搭載した ASA FirePOWER デバイス

関連リソース

別のプラットフォームまたはコンポーネントをアップグレードする場合、または別のバージョンにアップグレードする場合は、これらのリソースのいずれかを参照してください。

表 *1 : FMC* のアップグレードガイド

現在の **FMC** のバージョン	ガイド
7.2 以降	お使いのバージョンの『Cisco Secure Firewall Threat Defense Upgrade Guide for Management Center』
7.1	『Cisco Firepower Threat Defense Upgrade Guide for Firepower Management Center, Version 7.1』

現在の FMC のバージョン	ガイド
7.0 以前	『Cisco Firepower Management Center バージョン 6.0 ～ 7.0 アップグレードガイド』

表 *2*：*FTD* を搭載した *FMC* のアップグレードガイド

現在の FMC のバージョン	ガイド
クラウド提供型 Firewall Management Center	クラウド提供型 Firewall Management Center 用 Cisco Secure Firewall Threat Defense アップグレードガイド
7.2 以降	お使いのバージョンの『Cisco Secure Firewall Threat Defense Upgrade Guide for Management Center』
7.1	『Cisco Firepower Threat Defense Upgrade Guide for Firepower Management Center, Version 7.1』
7.0 以前	『Cisco Firepower Management Center バージョン 6.0 ～ 7.0 アップグレードガイド』

表 *3*：*FTD* を搭載した *FDM* のアップグレードガイド

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『Cisco Secure Firewall Threat Defense Upgrade Guide for Device Manager』
7.1	『Cisco Firepower Threat Defense Upgrade Guide for Firepower Device Manager, Version 7.1』
7.0 以前	お使いのバージョンの『Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager』：「System Management」 Firepower 4100/9300 については、『Cisco Firepower 4100/9300 アップグレードガイド、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	Cisco Security Cloud Control を使用した FDM デバイスの管理

表 *4 : NGIPS* のアップグレードガイド

プラットフォーム	現在のマネージャバージョン	ガイド
FMC を搭載した Firepower 7000/8000 シリーズ	6.0.0 ～ 7.0.x	『Cisco Firepower Management Center バージョン 6.0 ～ 7.0 アップグレードガイド』
FMC を搭載した NGIPSv	6.0.0 ～ 7.1.x 7.2.0 ～ 7.2.5 7.3.x 7.4.0	『Cisco Firepower Management Center バージョン 6.0 ～ 7.0 アップグレードガイド』
	7.2.6 ～ 7.2.x 7.4.1 ～ 7.4.x	お使いのバージョンの『Cisco Secure Firewall Threat Defense Upgrade Guide for Management Center』
FMC を搭載した ASA FirePOWER	6.0.0 ～ 7.1.x 7.2.0 ～ 7.2.5 7.3.x 7.4.0	『Cisco Firepower Management Center バージョン 6.0 ～ 7.0 アップグレードガイド』
	7.2.6 ～ 7.2.x 7.4.1 ～ 7.4.x	お使いのバージョンの『Cisco Secure Firewall Threat Defense Upgrade Guide for Management Center』
ASDM を使用した ASA FirePOWER	任意（Any）	『Cisco Secure Firewall ASA アップグレードガイド』

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	Cisco Secure Firewall ASA アップグレードガイド

Version	コンポーネント	ガイド
最新	FMC 用の BIOS およびファームウェア	Cisco Secure Firewall Threat Defense/Firepower ホットフィックス リリース ノート
最新	Firepower 4100/9300 のファームウェア	Cisco Firepower 4100/9300 FXOS ファームウェア アップグレード ガイド
最新	ISA 3000 の ROMMON イメージ	Cisco Secure Firewall ASA および Secure Firewall Threat Defense 再イメージ化ガイド

アップグレード機能の履歴

表 *6* : バージョン *7.0.0* の機能

機能	詳細
Threat Defense のアップグレード	
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。	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。

機能	詳細
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。	FMC の新しいデバイス アップグレード ページ（[デバイス（Devices）] > [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。 開始するには、[デバイス管理（Device Management）] ページ（[デバイス（Devices）] > [デバイス管理（Device Management）] > [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。 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。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。 （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 [システム（System）]（⚙）> **[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。 （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、すべてのユニットで開始されます。 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。

機能	詳細
多くのFTDデバイスを一度にアップグレードします。	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。 **重要** この改善点は、FTD アップグレードウィザードを使用した 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。
異なるデバイスモデルをまとめてアップグレードします。	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、FTDアップグレードウィザードを使用してすべての 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せるようになりました。 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。

表 *7: バージョン 6.7.0* の機能

機能	詳細
Threat Defense のアップグレード	
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。

機能	詳細
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。	[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日間の履歴を確認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。 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。 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。 （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、FMCを使用してFTDデバイスをアップグレードするとき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（[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。 パッチの自動キャンセルはサポートされていません。HA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。 新規/変更された画面： • FTDアップグレードパッケージの[システム（System）]（⚙）>**[更新（Updates）]**>**[製品の更新（Product Updates）]**>**[使用可能な更新（Available Updates）]**>**[インストール（Install）]**アイコン • **[Devices]**>**[Device Management]**>**[Upgrade]** • **[Message Center]**>**[Tasks]** 新規/変更されたCLIコマンド：**show upgrade status detail**、**show upgrade status continuous**、**show upgrade status**、**upgrade cancel**、**upgrade retry**
コンテンツの更新（Content Updates）	

機能	詳細
カスタム侵入ルールのインポートでルール競合の際に警告表示。	カスタム（ローカル）侵入ルールをインポートする場合、FMC がルールの競合について警告するようになりました。以前は、システムは競合の原因となるルールをサイレントにスキップしていました。ただし、競合のあるルールのインポートが完全に失敗するバージョン 6.6.0.1 は除きます。 [ルールの更新（Rule Updates）] ページで、ルールのインポートに競合があった場合は、[ステータス（Status）] 列に警告アイコンが表示されます。詳細については、警告アイコンの上にポインタを置いて、ツールチップを参照してください。 既存のルールと同じ SID/リビジョン番号を持つ侵入ルールをインポートしようとすると、競合が発生することに注意してください。カスタムルールの更新バージョンには必ず新しいリビジョン番号を付けてください。 新規/変更された画面：[システム（System）]（⚙）>**[更新（Updates）]**>**[ルールの更新（Rule Updates）]** に警告アイコンが追加されました。

表 *8* : バージョン *6.6.0* の機能

機能	詳細
Threat Defense のアップグレード	
内部 Web サーバーから FTD アップグレードパッケージを取得します。	FTD 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 上の領域も節約できます。 （注） この機能は、バージョン 6.6+ を実行している FTD デバイスでのみサポートされています。バージョン 6.6 へのアップグレードではサポートされておらず、FMC または従来のデバイスでもサポートされていません。 新規/変更された画面：アップグレードパッケージをアップロードするページに、[ソフトウェアアップデートソースの指定（Specify software update source）] オプションを追加しました。
コンテンツの更新（Content Updates）	
初期セットアップ中の自動VDB更新。	新規または再イメージ化された FMC をセットアップすると、システムは自動的に脆弱性データベース（VDB）の更新を試みます。 これは1回限りの操作です。FMCがインターネットにアクセスできる場合は、自動の定期 VDB 更新のダウンロードとインストールを実行するようにタスクをスケジュールしておくことを推奨します。

表 *9* : バージョン *6.5.0* の機能

機能	詳細
コンテンツの更新（Content Updates）	
ソフトウェアの自動ダウンロードとGeoDB の更新。	新規または再イメージ化されたFMC を設定すると、システムは自動的に次のスケジュールを設定します。 • FMC とその管理対象デバイスのソフトウェアアップデートをダウンロードする週次タスク。 • GeoDB の週次更新。 タスクはUTC でスケジュールされるため、いつ現地で実行されるかは、日付と場所によって異なります。また、タスクはUTC でスケジュールされるため、サマータイムなど、所在地で実施される場合がある季節調整に合わせて調節されることもありません。このような影響を受ける場合、スケジュールされたタスクは、現地時間を基準とすると、夏期では冬期の場合よりも 1 時間「遅れて」実行されることになります。自動スケジュール設定を確認し、必要に応じて調整することをお勧めします。

表 *10* : バージョン *6.4.0* の機能

機能	詳細
Management Center のアップグレード	
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。	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。 （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。 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。
コンテンツの更新（Content Updates）	

機能	詳細
署名済みのSRU、VDB、およびGeoDBの更新。	正しい更新ファイルを使用していることが確認できるため、バージョン6.4以降では署名済みの更新を侵入ルール（SRU）、脆弱性データベース（VDB）、および地理位置情報データベース（GeoDB）が使用されます。以前のバージョンでは、引き続き未署名の更新が使用されます。 シスコ サポートおよびダウンロード サイトから手動で更新をダウンロードしない限り（たとえば、エアギャップ導入環境の場合）、機能の違いはわかりません。ただし、SRU、VDB、およびGeoDBの更新を手動でダウンロードしてインストールする場合は、必ず現在のバージョンに対応した正しいパッケージをダウンロードしてください。 署名付きの更新ファイルの先頭は、以下のように「Sourcefire」ではなく「Cisco」で、末尾は .sh ではなく .sh.REL.tar です。 • SRU：Cisco_Firepower_SRU-*date-build*-vrt.sh.REL.tar • VDB：Cisco_VDB_Fingerprint_Database-4.5.0-*version*.sh.REL.tar • GeoDB：Cisco_GEODB_Update-*date-build*.sh.REL.tar シスコは、署名なしの更新を必要とするバージョンのサポートが終了するまで、署名付きと署名なしの両方の更新を提供します。署名付きの（.tar）パッケージは解凍しないでください。古い FMC または ASA FirePOWER デバイスに署名付きの更新を誤ってアップロードした場合は、手動で削除する必要があります。パッケージを残しておくと、ディスク領域が占有されるため、今後のアップグレードで問題が発生する可能性もあります。

表 *11 :* バージョン *6.2.3* の機能

機能	詳細
デバイスのアップグレード	
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。	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。 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。 新規/変更された画面：[システム（System）]（⚙）>**[更新（Updates）]**。
コンテンツの更新（Content Updates）	

機能	詳細
VDB の更新前に、Snort の再起動について FMC から警告されます。	脆弱性データベース（VDB）の更新で Snort プロセスが再起動することが、FMC から警告されるようになりました。これにより、トラフィック インスペクションが中断され、管理対象デバイスによるトラフィックの処理方法によっては、トラフィックフローが中断される可能性があります。メンテナンス期間中など、都合の良い期間までインストールをキャンセルすることができます。 次のようなときに警告が表示される可能性があります。 • VDB をダウンロードして手動でインストールした後。 • スケジュールされたタスクを作成して VDB をインストールする場合。 • たとえば、以前にスケジュールされたタスクの実行中に、またはソフトウェアアップグレードの一部として、VDB がバックグラウンドでインストールされる場合。
廃止：地理位置情報の詳細	2022 年 5 月、GeoDB が 2 つのパッケージに分割されました。IP アドレスを国/大陸にマッピングする国コードパッケージと、ルーティング可能な IP アドレスに関連付けられた追加のコンテキストデータを含む IP パッケージです。2024 年 1 月に、IP パッケージの提供を停止しました。この措置によりディスク容量が節約されますが、地理位置情報ルールやトラフィック処理には影響しません。コンテキストデータはすべて古くなっており、最新のバージョンにアップグレードすると IP パッケージが削除されます。 コンテキストデータを表示したりするオプションは効果がなく、以降のバージョンでは削除されます。

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。