使用する前に

対象読者

このガイドでは、ハードウェアまたは仮想 **Secure Firewall Management Center** を搭載した **Secure Firewall Threat Defense** の **バージョン 7.2** へのアップグレードを準備し、正常に完了する方法について説明します。

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 : Management Center* の手順

Version	ガイド
7.2 以降	アップグレードガイドの下にある、お使いのバージョンの『*Management Center* 用 *Cisco Secure Firewall Threat Defense* アップグレードガイド』。
7.1	『Firepower Management Center 用 Cisco Firepower Threat Defense アップグレードガイド（バージョン 7.1）』
7.0 以前	Cisco Firepower Management Center Upgrade Guide, Version 6.0–7.0

表 *2 : Management Center* を使用した *Threat Defense* の手順

Version	ガイド
7.2 以降	アップグレードガイドの下にある、お使いのバージョンの『*Management Center* 用 *Cisco Secure Firewall Threat Defense* アップグレードガイド』。

Version	ガイド
7.1	『Firepower Management Center 用 Cisco Firepower Threat Defense アップグレードガイド（バージョン 7.1）』
7.0 以前	Cisco Firepower Management Center Upgrade Guide, Version 6.0–7.0

表 *3 : Device Manager* を使用した *Threat Defense* の手順

Version	ガイド
7.2 以降	アップグレードガイドの下にある、お使いのバージョンの『*Device Manager* 用 *Cisco Secure Firewall Threat Defense* アップグレードガイド』内にある「」の章。
7.1	『Firepower Device Manager 用 Cisco Firepower Threat Defense アップグレードガイド（バージョン 7.1）』
7.0*	『*Firepower Device Manager* 用 *Cisco Firepower Threat Defense* 設定ガイド（バージョン *7.0*）』内の「システム管理」
6.7*	『*Firepower Device Manager* 用 *Cisco Firepower Threat Defense* 設定ガイド（バージョン *6.7*）』内の「システム管理」
6.6*	『*Firepower Device Manager* 用 *Cisco Firepower Threat Defense* 設定ガイド（バージョン *6.6*）』内の「システム管理」
6.5*	『*Firepower Device Manager* 用 *Cisco Firepower Threat Defense* 設定ガイド（バージョン *6.5*）』内の「システム管理」
6.4	『*Firepower Device Manager* 用 *Cisco Firepower Threat Defense* 設定ガイド（バージョン *6.4*）』内の「システム管理」
6.3	『*Firepower Device Manager* 用 *Cisco Firepower Threat Defense* 設定ガイド（バージョン *6.3*）』内の「システム管理」
6.2.3	『*Firepower Device Manager* 用 *Cisco Firepower Threat Defense* 設定ガイド（バージョン *6.2.3*）』内の「システム管理」
6.2.2	『*Firepower Device Manager* 用 *Cisco Firepower Threat Defense* 設定ガイド（バージョン *6.2.2*）』内の「システム管理」
6.2	『*Firepower Device Manager* 用 *Cisco Firepower Threat Defense* 設定ガイド（バージョン *6.2*）』内の「システム管理」
6.1	『*Firepower Device Manager* 用 *Cisco Firepower Threat Defense* 設定ガイド（バージョン *6.1*）』内の「システム管理」

* FDM を使用して Firepower 4100/9300 でバージョン 6.5 ～ 7.0 の FTD 論理デバイスを管理している場合、FXOS のアップグレード手順については、『*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 *Firepower 6.0.1 ～ 7.0.x* または *ASA 9.4 (1) ～ 9.16 (x)*』の「FTD 論理デバイスを搭載した Firepower 4100/9300 のアップグレード」も参照してください。

表 *4* : *NGIPS* デバイスの手順

Version	プラットフォーム	ガイド
任意	Firepower 7000/8000 シリーズ	Cisco Firepower Management Center Upgrade Guide, Version 6.0–7.0
任意	FMC を搭載した ASA FirePOWER	Cisco Firepower Management Center Upgrade Guide, Version 6.0–7.0
任意	ASDM を使用した ASA FirePOWER	Cisco Secure Firewall ASA アップグレードガイド

表 *5* : その他のアップグレード可能なコンポーネントの手順

Version	コンポーネント	ガイド
任意	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
Latest	Management Center 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
Latest	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	展開を評価します。 アップグレードパスを計画します。 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。 アプライアンスへのアクセスを確認します。 帯域幅を確認します。 メンテナンス時間帯をスケジュールします。
バックアップ	ソフトウェアをバックアップします。 Firepower 4100/9300 の FXOS をバックアップします。
アップグレードパッケージ	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。 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。
関連するアップグレード	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。 Firepower 4100/9300 の FXOS をアップグレードします。
最終チェック	設定を確認します。 NTP 同期を確認します。 ディスク容量を確認します。 設定を展開します。 準備状況チェックを実行します。 実行中のタスクを確認します。 展開の正常性と通信を確認します。

機能の履歴

表 *7:* バージョン *7.2.0* の機能

機能	説明
デバイス間のアップグレードパッケージのコピー（「ピアツーピア同期」）。	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。 新規/変更された CLI コマンド：**configure p2psync enable**、**configure p2psync disable**、**show peers**、**show peer details**、**sync-from-peer**、**show p2p-sync-status**

機能	説明
Threat Defense のアップグレード完了後の Snort 3 への自動アップグレード。	バージョン 7.2 以降の Management Center を使用して Threat Defense をアップグレードする場合、**Snort 2 から Snort 3 へのアップグレード**を実行するかどうかを選択できるようになりました。 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。 このオプションは、バージョン 7.2 以降への Threat Defense の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サポートされています。バージョン 7.0 または 7.1 への Threat Defense のアップグレード、または任意のバージョン向けのパッチではサポートされていません。
単一ノードクラスタのアップグレード。	デバイスのアップグレードページ（**[デバイス（Devices）]** > **[デバイスのアップグレード（Device Upgrade）]**）を使用して、アクティブノードが 1 つだけのクラスタをアップグレードできるようになりました。非アクティブ化されたノードもアップグレードされます。以前は、このタイプのアップグレードは失敗していました。この機能は、システムの更新ページ（**[システム（System）]** > **[更新（Updates）]**）ではサポートされていません。 この場合、ヒットレスアップグレードもサポートされません。トラフィックフローと検査の中断は、スタンドアロンデバイスと同様に、アクティブユニットのインターフェイス設定に依存します。 サポートされるプラットフォーム：Firepower 4100/9300、Secure Firewall 3100

機能	説明
CLI からの Threat Defense アップグレードの復元。	Management Center とデバイス間の通信が中断された場合、デバイスの CLI から Threat Defense のアップグレードを元に戻すことができるようになりました。高可用性や拡張性の展開では、すべてのユニットを同時に復元すると、復元が成功する可能性が高くなります。CLI を使用して復元する場合は、すべてのユニットでセッションを開き、それぞれで復元が可能であることを確認してから、プロセスを同時に開始します。 **注意** CLI から復元すると、アップグレード後に行った変更によっては、デバイスと Management Center 間で設定が同期されないことがあります。これにより、後に通信と展開の問題が発生する可能性があります。 新規/変更された CLI コマンド：**upgrade revert**、**show upgrade revert-info**。 詳細については、Management Center アップグレードガイドの「Revert the Upgrade」を参照してください。
アップグレードを行っても、トラブルシューティング ファイルは自動的に生成されません。	時間とディスク容量を節約するために、管理センターのアップグレードプロセスでは、アップグレードの開始前にトラブルシューティング ファイルを自動的に生成しなくなりました。デバイスのアップグレードは影響を受けず、引き続きトラブルシューティング ファイルが生成される点に注意してください。 管理センターのトラブルシューティング ファイルを手動で生成するには、**システム**（⚙）>**[正常性（Health）]**>**[モニタ（Monitor）]** を選択し、左側のパネルで [Firewall Management Center] をクリックし、[View System & Troubleshoot Details]、[Generate Troubleshooting Files] を選択します。

表 *8 :* バージョン *7.1.0* の機能

機能	説明
正常なデバイスアップグレードを元に戻します。	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。 **重要** 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（System）] > [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）] > [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。 この機能は、Firepower 4100/9300 のコンテナインスタンスではサポートされません。
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。	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。 • 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。 • 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。 • 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。

表 *9* : バージョン *7.0.0* の機能

機能	説明
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	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
	FMC の新しいデバイス アップグレード ページ（[デバイス（Devices）]>[アップグレード（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 [システム更新（System Updates）] ページ（**[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。

機能	説明
	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。
多くの FTD デバイスを一度にアップグレードします。	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す。 • デバイスの同時アップグレード。 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。 • デバイスモデルによるアップグレードのグループ化。 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。 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 *10* : バージョン *6.7.0* の機能

機能	説明
Threat Defense 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
	[デバイス管理（Device Management）] ページで、進行中の Threat Defense 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。 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、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。 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。 新規/変更された画面： • Threat Defense アップグレードパッケージの**[システム（System）] > [更新（Update）] > [製品アップデート（Product Updates）] > [利用可能なアップデート（Available Updates）] > [インストール（Install）]**アイコン • **[Devices] > [Device Management] > [Upgrade]** • **[Message Center] > [Tasks]**

機能	説明
	新しい Threat Defense CLI コマンド • **show upgrade status detail** • **show upgrade status continuous** • **show upgrade status** • **upgrade cancel** • **upgrade retry**
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 *11* : 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。	デバイスは、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できるようになりました。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。 新規/変更された画面：[システム（System）] > [更新（Updates）] > [更新のアップロード（Upload Update）] ボタン > [ソフトウェア更新ソースの指定（Specify Software Update Source）] オプション

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。	Management Center 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。

表 *12* : 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。	Management Center 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。

表 *13* : 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。	実際のアップグレードを実行する前に、Management Center 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）]**

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-72-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
- 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。