



参照先

- [トラフィック フローとインスペクション](#) (1 ページ)
- [時間とディスク容量](#) (5 ページ)
- [アップグレード機能の履歴](#) (7 ページ)

トラフィック フローとインスペクション

アップグレードの影響が最小限になるメンテナンスウィンドウ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を考慮してください。

Firewall Threat Defense アップグレードのトラフィックフローとインスペクション

スタンドアロンデバイスでのソフトウェアのアップグレード

アップグレード中、デバイスはメンテナンスモードで稼働します。アップグレードの開始時にメンテナンスモードを開始すると、トラフィック インスペクションが2〜3秒中断します。インターフェイスの構成により、その時点とアップグレード中の両方のスタンドアロンデバイスによるトラフィックの処理方法が決定されます。

表 1: トラフィックフローとインスペクション : スタンドアロンデバイスでのソフトウェアのアップグレード

インターフェイス コンフィギュレーション		トラフィックの挙動
ファイアウォール インターフェイス	EtherChannel、冗長、サブインターフェイスを含むルーテッドまたはスイッチド。 スイッチドインターフェイスは、ブリッジグループまたはトランスペアレントインターフェイスとしても知られています。	廃棄。 ISA 3000 のブリッジグループ インターフェイスの場合に限り、FlexConfig ポリシーを使用して、停電時のハードウェアバイパスを設定できます。これにより、ソフトウェアのアップグレード中にトラフィックのドロップが発生しますが、デバイスがアップグレード後の再起動中、インスペクションなしでトラフィックが通過します。
	IPS のみのインターフェイス	ハードウェアバイパスを無効にするか、スタンバイモードに戻すまで、インスペクションなしで合格。
	インラインセット、ハードウェアバイパス強制が有効 : [バイパス (Bypass)] : [強制 (Force)]	
	インラインセット、ハードウェアバイパスがスタンバイモード : [バイパス (Bypass)] : [スタンバイ (Standby)]	デバイスがメンテナンスモードの場合、アップグレード中にドロップされます。その後、デバイスがアップグレード後の再起動を完了する間、インスペクションなしで合格します。
	インラインセット、ハードウェアバイパスが無効 : [バイパス (Bypass)] : [無効 (Disabled)]	廃棄。
	インラインセット、ハードウェアバイパス モジュールなし。	廃棄。
	インラインセット、タップモード。	パケットをただちに出力、コピーへのインスペクションなし。
	パッシブ、ERSPAN パッシブ。	中断なし、インスペクションなし。

高可用性デバイスおよびクラスタ化されたデバイスのソフトウェアアップグレード

高可用性デバイスやクラスタ化されたデバイスのアップグレード中に、トラフィックフローや検査が中断されることはありません。高可用性ペアの場合、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。

クラスタの場合、データ セキュリティ モジュールを最初にアップグレードして、その後コントロールモジュールをアップグレードします。コントロール セキュリティ モジュールをアッ

ブグレードする間、通常トラフィックインスペクションと処理は続行しますが、システムはロギングイベントを停止します。ロギングダウンタイム中に処理されるトラフィックのイベントは、アップグレードが完了した後、非同期のタイムスタンプ付きで表示されます。ただし、ロギングダウンタイムが大きい場合、システムはログ記録する前に最も古いイベントをプルーニングすることがあります。

シングルユニットのクラスタでは、ヒットレスアップグレードはサポートされないことに注意してください。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。

ソフトウェアの復元（メジャーおよびメンテナンスリリース）

たとえ高可用性および拡張性を備えた環境でも、復元時のトラフィックフローとインスペクションの中断を予測する必要があります。これは、すべてのユニットを同時に復元させたほうが、復元がより正常に完了するためです。同時復元とは、すべてのデバイスがスタンドアロンであるかのように、トラフィックフローと検査の中断がインターフェイスの設定のみに依存することを意味します。

ソフトウェアのアンインストール（パッチ）

スタンドアロンデバイスの場合、パッチのアンインストール中のトラフィックフローと検査の中断は、アップグレードの場合と同じになります。高可用性および拡張性の展開では、中断を最小限に抑えるために、アンインストールの順序を明確に計画する必要があります。これは、ユニットとしてアップグレードしたデバイスであっても、デバイスから個別にパッチをアンインストールするためです。

シャーシのアップグレードでのトラフィックフローとインスペクション

FXOS をアップグレードするとシャーシが再起動します。ファームウェアのアップグレードを含むバージョン 2.14.1 以降への FXOS アップグレードの場合、シャーシは 2 回リブートします。1 回は FXOS 用、1 回はファームウェア用です。対象には、のバージョン 7.4.1 以降のシャーシアップグレードが含まれます。

高可用性またはクラスタ展開の場合でも、各シャーシの FXOS を個別にアップグレードします。中断を最小限に抑えるには、1 つずつシャーシをアップグレードします。「[アップグレード順序](#)」を参照してください。

表 2: トラフィックフローとインスペクション：FXOS のアップグレード

Firewall Threat Defense の導入	トラフィックの挙動	メソッド
スタンドアロン	廃棄。	—

Firewall Threat Defense の導入	トラフィックの挙動	メソッド
高可用性	影響なし。	ベストプラクティス：スタンバイで FXOS を更新し、アクティブピアを切り替えて新しいスタンバイをアップグレードします。
	1 つのピアがオンラインになるまでドロップされる。	スタンバイでアップグレードが終了する前に、アクティブピアで FXOS をアップグレードします。
シャーシ間クラスタ	影響なし。	ベストプラクティス：少なくとも 1 つのモジュールを常にオンラインにするため、一度に 1 つのシャーシをアップグレードします。
	少なくとも 1 つのモジュールがオンラインになるまでドロップされる。	ある時点ですべてのモジュールを停止するため、シャーシを同時にアップグレードします。
シャーシ内クラスタ (FirePOWER 9300 のみ)	検査なしで受け渡される。	ハードウェアバイパス有効：[Bypass: Standby] または [Bypass-Force]。
	少なくとも 1 つのモジュールがオンラインになるまでドロップされる。	ハードウェアバイパス無効：[Bypass: Disabled]。
	少なくとも 1 つのモジュールがオンラインになるまでドロップされる。	ハードウェアバイパス モジュールなし。

設定展開時のトラフィックフローとインスペクション

Snort は、通常、アップグレード直後の最初の展開時に再起動されます。つまり、クラウド提供型 Firewall Management Center のアップグレードの場合、すべての管理対象デバイスで Snort が再起動する可能性があります。後続の展開後は、展開の前に特定のポリシーまたはデバイス設定を変更しない限り、Snort は再起動しません。

Snort プロセスを再起動すると、高可用性/拡張性を備えた構成になっているものを含め、すべてのデバイスでトラフィックフローとインスペクションが一時的に中断されます。インターフェイス設定により、中断中にインスペクションせずにトラフィックをドロップするか受け渡すかが決定されます。Snort を再起動せずに展開すると、リソース要求時にいくつかのパケットが検査なしでドロップされることがあります。

表 3: トラフィックフローとインスペクション：設定変更の展開

インターフェイス コンフィギュレーション		トラフィックの挙動
ファイアウォール インターフェイス	EtherChannel、冗長、サブインターフェイスを含むルーテッドまたはスイッチド。 スイッチドインターフェイスは、ブリッジグループまたはトランスペアレントインターフェイスとしても知られています。	廃棄。
IPS のみのインターフェイス	インラインセット、[フェールセーフ (Failsafe)] が有効または無効。	検査なしで受け渡される。 [フェールセーフ (Failsafe)] が無効で、Snort がビジーでもダウンしていない場合、いくつかのパケットがドロップすることがあります。
	インラインセット、[Snortフェールオープン：ダウン (Snort Fail Open: Down)]：無効	廃棄。
	インライン、[Snortフェールオープン：ダウン (Snort Fail Open: Down)]：有効	検査なしで受け渡される。
	インラインセット、タップモード。	パケットをただちに出力、コピーへのインスペクションなし。
	パッシブ、ERSPAN パッシブ。	中断なし、インスペクションなし。

時間とディスク容量

アップグレードまでの時間

将来のベンチマークとして使用できるように、独自のアップグレード時間を追跡および記録することをお勧めします。次の表に、アップグレード時間に影響を与える可能性のあるいくつかの事項を示します。



注意 アップグレード中は、設定を変更または展開しないでください。システムが非アクティブに見えても、手動で再起動またはシャットダウンしないでください。ほとんどの場合、進行中のアップグレードを再開しないでください。システムが使用できない状態になり、再イメージ化が必要になる場合があります。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、「[無応答および失敗した Firewall Threat Defense のアップグレード](#)」を参照してください。

表 4: アップグレード時間の考慮事項

考慮事項	詳細
バージョン	アップグレードでバージョンがスキップされると、通常、アップグレード時間は長くなります。
モデル	通常、ローエンドモデルではアップグレード時間が長くなります。
仮想アプライアンス	仮想展開でのアップグレード時間はハードウェアに大きく依存します。
高可用性とクラスタリング	高可用性の構成またはクラスタ化された構成では、動作の継続性を保持するため、複数のデバイスは1つずつアップグレードされます。アップグレード中は、各デバイスはメンテナンスモードで動作します。そのため、デバイスペアまたはクラスタ全体のアップグレードには、スタンドアロンデバイスのアップグレードよりも長い時間がかかります。
設定	アップグレード時間は、構成の複雑さ
コンポーネント	オペレーティングシステムまたは仮想ホスティングのアップグレード、アップグレードパッケージの転送、準備状況チェック、VDB と侵入ルール（SRU/LSP）の更新、設定の展開、およびその他の関連タスクを実行するために、追加の時間が必要になる場合があります。

アップグレードするディスク容量

アップグレードするには、アップグレードパッケージがデバイスにある必要があります。デバイスがインターネットにアクセスできないデバイスアップグレードの場合は、クラウド提供型 Firewall Management Center（/Volume または /var のいずれか）にもデバイス アップグレードパッケージ用の十分な容量が必要です。または、内部サーバーを使用して保存することもできます。準備状況チェックでは、アップグレードを実行するのに十分なディスク容量があるかどうかを示されます。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。詳細については、「[設定と展開の確認](#)」を参照してください。

アップグレード機能の履歴

表 5: デバイスアップグレード機能の履歴

機能	最小の Management Center	最小の Threat Defense	詳細
新しいデバイスと シャーシのアップグ レードウィザード	20251121	任意	新しい合理化されたアップグレードウィザードにより、アップグレードするデバイスの選択と準備、およびアップグレードを妨げる問題の特定が容易になります。 Firewall Threat Defense ウィザードでは、無人モードで新しい準備専用オプションを利用することに注意してください。つまり、ウィザードがパッケージのコピーと準備状況の確認をしている間、明示的に開始していない場合でも、無人モードの実行に関するメッセージが表示されることがあります。
無人 Firewall Threat Defense アップグレー ドの準備専用オプショ ンとスキップチェック オプション	20251121	任意	無人 Firewall Threat Defense アップグレード : - アップグレードの準備のみを行います。パッケージをコピーして準備状況を確認しますが、実際のアップグレードは実行しないでください。 - すでに合格したデバイスの準備状況チェックをスキップします。 これらの新しいオプションは、無人モードを開始すると使用できます。
アップグレードパッ ケージのダウンロード に関する新しいオプ ション	20251121	任意	次の作業に進んでください。 - デバイスがインターネットからアップグレードパッケージをダウンロードできないようにします。つまり、デバイスがインターネットにアクセスできる場合でも、デバイスがクラウド提供型 Firewall Management Center または内部サーバーからアップグレードパッケージを取得するように要求できるようになりました。 - デバイスが内部サーバーまたはインターネットから失敗したダウンロードを再試行する時間を指定します。この設定は、クラウド提供型 Firewall Management Center とデバイス間の転送には適用されません。 新規/変更された画面 : [管理 (Administration)] > [製品アップグレード (Product Upgrades)] > [グローバルアップグレード設定 (Global upgrade settings)]

機能	最小の Management Center	最小の Threat Defense	詳細
廃止：メッセージセンターでのデバイスの復元の監視	20251121	任意	メッセージセンターからデバイスの復元を監視できなくなりました。代わりに、[デバイス管理 (Device Management)] ページ ([デバイス (Devices)] > [デバイス管理 (Device Management)]) を使用します。[アップグレード (Upgrade)] タブで、復元するデバイスの横にある [詳細の表示 (View Details)] をクリックします。
手動の準備状況チェックを行わずに Firewall Threat Defense または シャーシをアップグレードします。	20250219	7.7.0	Firewall Threat Defense または シャーシのアップグレードのために、時間のかかるアップグレード前の準備状況チェックを実行する必要がなくなりました。代わりに、これらのチェックがシステムによって定期的に行われ、正常性モニターで報告されるようになりました。これにより、アップグレードを妨げる問題を事前に修正できます。 • デバイス用の新しいデータベースモジュールは、データベーススキーマと構成データ (EO) の整合性を管理します。 • デバイス用に新しく追加された FXOS 正常性モジュールは、FXOS ベースのデバイスで FXOS httpd サービスをモニターします。 • ディスク ステータス モジュールがより堅牢になり、smartctl (信頼性の監視、障害の予測、およびその他のセルフテストを実行するための Linux ユーティリティ) の毎日の実行から報告されたディスク正常性の問題に関するアラートを生成するようになりました。 バージョンの制限：この機能は、バージョン 7.7 以降からのアップグレードでサポートされています。それ以前のバージョンを実行しているデバイスでは、アップグレード時の準備状況チェックが必要です。

機能	最小の Management Center	最小の Threat Defense	詳細
インターネットにアクセスできるデバイスは、インターネットからアップグレードパッケージをダウンロードします。	20250219	任意	アップグレードパッケージを使用せずにデバイスとシャーシのアップグレードを開始できるようになりました。適切なタイミングで、デバイスがインターネットからパッケージを直接取得します。これにより、時間とクラウド提供型 Firewall Management Center のディスク容量を節約できます。 インターネットにアクセスできないデバイスでは、引き続きクラウド提供型 Firewall Management Center または内部サーバーからパッケージを取得できます。デバイスは、インターネットまたはクラウド提供型 Firewall Management Center の前に、内部サーバー（設定されている場合）を試行することに注意してください。内部サーバーからのダウンロードが失敗した場合、インターネットにアクセスできる新しいデバイスは、インターネット、クラウド提供型 Firewall Management Center の順に試行しますが、古いデバイスやインターネットにアクセスできないデバイスは、クラウド提供型 Firewall Management Center のみを試行します。（この文脈での「新しい」とは、Firewall Threat Defense 7.6 以降またはシャーシ 7.4.1 以降を意味します）。 制限事項：クラウド提供型 Firewall Management Center およびデバイスは、インターネットにアクセスする必要があります。インターネットにアクセスできるデバイスに、インターネットを試行する前に強制的にクラウド提供型 Firewall Management Center を試行させる方法はありません。ホットフィックスではサポートされていません。 ダウンロードの場所：https://cdo-ftd-images.s3-us-west-2.amazonaws.com/
Firewall Threat Defense およびシャーシアップグレードウィザードからアップグレード後の設定変更レポートを生成およびダウンロードします。	20240808	任意	アップグレードワークフローをクリアしていない場合でも、Firewall Threat Defense ウィザードおよびシャーシアップグレードウィザードからアップグレード後の設定変更レポートを生成およびダウンロードできるようになりました。 以前は、[高度な展開（Advanced Deploy）]画面を使用してレポートを生成し、メッセージセンターを使用してレポートをダウンロードしていました。このメソッドは引き続き使用できます。これは、複数のデバイスの変更レポートをすばやく生成する場合、またはワークフローをクリアした場合に役立ちます。 新規/変更された画面： • [デバイス（Devices）]> [Threat Defenseアップグレード（Threat Defense Upgrade）]> [設定の変更（Configuration Changes）] • [デバイス（Devices）]> [シャーシアップグレード（Chassis Upgrade）]> [設定の変更（Configuration Changes）]

機能	最小の Management Center	最小の Threat Defense	詳細
マルチインスタンス モードでの Secure Firewall 3100 のシャー シのアップグレード	20240808	7.4.1	マルチインスタンスモードの Cisco Secure Firewall 3100 では、コンテナインスタンスのアップグレード（Firewall Threat Defense のアップグレード）とは別に、オペレーティングシステムとファームウェアがアップグレードの対象（シャーシのアップグレード）になります。 新規/変更された画面： • シャーシのアップグレード：[デバイス（Devices）]>[シャーシのアップグレード（Chassis Upgrade）] • Firewall Threat Defense のアップグレード：[デバイス（Devices）]>[Threat Defenseのアップグレード（Threat Defense Upgrade）]
FXOS アップグレード に含まれるファーム ウェアのアップグレー ド。	20240203	任意	シャーシ/FXOS アップグレードの影響。ファームウェアのアップグレードにより、余分な再起動が発生します。 Firepower 4100/9300 の場合、バージョン 2.14.1 への FXOS アップグレードにファームウェアのアップグレードが含まれるようになりました。マルチインスタンスモードの Cisco Secure Firewall 3100（バージョン 7.4.1 の新機能）には、FXOS とファームウェアのアップグレードもバンドルされています。デバイス上のいずれかのファームウェアコンポーネントが FXOS バンドルに含まれているコンポーネントよりも古い場合、FXOS アップグレードによってファームウェアも更新されます。ファームウェアがアップグレードされると、デバイスは 2 回リブートします。1 回は FXOS 用、1 回はファームウェア用です。 ソフトウェアおよびオペレーティングシステムのアップグレードと同様に、ファームウェアのアップグレード中に設定変更を行ったり、展開したりしないでください。システムが非アクティブに見えても、ファームウェアのアップグレード中は手動で再起動またはシャットダウンしないでください。 参照：Cisco Firepower 4100/9300 FXOS ファームウェア アップグレードガイド
アップグレードパッ ケージを選択してクラ ウド提供型 Firewall Management Center に直 接ダウンロードしま す。		任意	クラウド提供型 Firewall Management Center に直接ダウンロードする Firewall Threat Defense アップグレードパッケージを選択できるようになりました。>[更新（Updates）]>[製品の更新（Product Updates）]の新しい[の更新のダウンロード（Download Threat Defense Updates）]サブタブを使用します。 バージョンの制限：バージョン 20240203 では、この機能は改善されたパッケージ管理システムに置き換えられています。

機能	最小の Management Center	最小の Threat Defense	詳細
Firewall Threat Defense のアップグレード完了 後の Snort 3 への自動 アップグレードはオプ ションではなくなりま した。		任意	アップグレードの影響。展開すると、対象となるすべてのデバイスが Snort 3 にアップグレードされます。 Firewall Threat Defense をバージョン 7.3 以降にアップグレードすると、[Snort 2 から Snort 3 にアップグレードする (Upgrade Snort 2 to Snort 3)] オプションは無効化できなくなります。 ソフトウェアのアップグレード後、設定を展開すると、対象となるすべてのデバイスが Snort 2 から Snort 3 にアップグレードされます。個々のデバイスを元に戻すことはできますが、Firewall Threat Defense 7.7 以降では Snort 2 はサポートされていません。すぐに使用を停止する必要があります。 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自動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 Custom Snort 3 Intrusion Policies for Access Control を参照してください。

機能	最小の Management Center	最小の Threat Defense	詳細
Cisco Secure Firewall 3100 の統合アップグレードおよびインストールパッケージ。		7.3.0	

機能	最小の Management Center	最小の Threat Defense	詳細
			再イメージ化の影響。 バージョン 7.3 では、次のように、Cisco Secure Firewall 3100 の Firewall Threat Defense のインストールおよびアップグレードパッケージを組み合わせてみました。 - バージョン 7.1 ～ 7.2 インストールパッケージ： isco-ftd-fp3k.version.SPA - バージョン 7.1 ～ 7.2 アップグレードパッケージ： Cisco_FTD_SSP_FP3K_Upgrade-version-build.sh.REL.tar - バージョン 7.3 以降の統合パッケージ： Cisco_FTD_SSP_FP3K_Upgrade-version-build.sh.REL.tar Firewall Threat Defense は問題なくアップグレードできますが、古い Firewall Threat Defense および Cisco ASA バージョンから Firewall Threat Defense バージョン 7.3 以上に直接再イメージ化することはできません。これは、新しいイメージタイプに必要な ROMMON アップデートが原因です。これらの古いバージョンから再イメージ化するには、古い ROMMON でサポートされているだけでなく新しい ROMMON への更新も行う、ASA 9.19 以上を「通過」する必要があります。個別の ROMMON アップデータはありません。 Firewall Threat Defense バージョン 7.3 以上にするには、次のオプションがあります。 - Firewall Threat Defense バージョン 7.1 または 7.2 からのアップグレード — 通常のアップグレードプロセスを使用します。 該当するアップグレードガイドを参照してください。 - Firewall Threat Defense バージョン 7.1 または 7.2 からの再イメージ化 — 最初に Cisco ASA 9.19 以上に再イメージ化してから、Firewall Threat Defense バージョン 7.3 以上に再イメージ化します。 『Cisco Secure Firewall ASA および Secure Firewall Threat Defense 再イメージ化ガイド』の「Threat Defense→ASA: Firepower 1000, 2100; Secure Firewall 3100」、次に「ASA→Threat Defense: Firepower 1000, 2100 Appliance Mode; Secure Firewall 3100」を参照してください。 - ASA 9.17 または 9.18 からの再イメージ化 — 最初に ASA 9.19 以上にアップグレードしてから、Firewall Threat Defense バージョン 7.3 以上に再イメージ化します。 『Cisco Secure Firewall ASA アップグレードガイド』を参照し、次に『Cisco Secure Firewall ASA および Secure Firewall Threat Defense』

機能	最小の Management Center	最小の Threat Defense	詳細
			再イメージ化ガイド』の「ASA→Threat Defense: Firepower 1000, 2100 Appliance Mode; Secure Firewall 3100」を参照してください。 • Firewall Threat Defense バージョン 7.3 以上からの再イメージ化 — 通常の再イメージ化プロセスを使用します。 『Cisco FXOS 障害対応ガイド (Firepower Threat Defense 向け)』の「Reimage the System with a New Software Version」を参照してください。
低解像度の画面用に最適化された Firewall Threat Defense およびシャーシアップグレードウィザード。		任意	Firewall Threat Defense とシャーシアップグレードウィザードを、低解像度の画面（および小さなブラウザウィンドウ）用に最適化しました。テキストが小さく表示され、特定の画面要素が非表示になります。セッションの途中で解像度またはウィンドウサイズを変更した場合は、Web インターフェイスを調整するためにページを更新することが必要になる場合があります。クラウド提供型 Firewall Management Center を使用するための最小画面の解像度は 1,280 X 720 であることに注意してください。 新規/変更された画面： • [デバイス (Devices)] > [Threat Defense のアップグレード (Threat Defense Upgrade)] • [デバイス (Devices)] > [シャーシのアップグレード (Chassis Upgrade)]
Firewall Threat Defense アップグレードウィザードからの復元の有効化。	20240203	任意（7.1 以降にアップグレードする場合）	Firewall Threat Defense アップグレードウィザードからの復元を有効化できます。 バージョンの制限：Firewall Threat Defense をバージョン 7.2 以降にアップグレードする必要があります。
Firewall Threat Defense アップグレードウィザードから詳細なアップグレードステータスを表示します。	20240203	任意	Firewall Threat Defense アップグレードウィザードの最終ページで、アップグレードの進行状況をモニターできるようになりました。この機能は、[デバイス管理 (Device Management)] ページの [アップグレード (Upgrade)] タブおよび Management Center の既存のモニタリング機能に追加されます。新しいアップグレードフローを開始していない限り、[デバイス (Devices)] > [Threat Defense アップグレード (Threat Defense Upgrade)] によってこのウィザードの最後のページに戻り、現在の（または最後に完了した）デバイスのアップグレードの詳細なステータスを確認できます。

機能	最小の Management Center	最小の Threat Defense	詳細
アップグレードの開始 ページとパッケージ管 理が改善されました。	20240203	任意	新しいアップグレードページでは、アップグレードの選択、ダウンロード、管理、および展開全体への適用が容易になります。このページには、現在の展開に適用されるすべてのアップグレードパッケージが、特にマークされた推奨リリースとともに一覧表示されます。パッケージを選択してシスコから簡単に直接ダウンロードしたり、パッケージを手動でアップロードおよび削除したりできます。 適切なメンテナンスリリースのアプライアンスが少なくとも1つある（またはパッチを手動でアップロードした）場合を除き、パッチは表示されません。ホットフィックスは手動でアップロードする必要があります。 新規/変更された画面： • [システム (System)] (⚙️) > [製品のアップグレード (Product Upgrades)] では、デバイスをアップグレードし、アップグレードパッケージを管理します。 • [システム (System)] (⚙️) > [コンテンツの更新 (Content Updates)] で、侵入ルール、VDB、および GeoDB を更新できるようになりました。 • [デバイス (Devices)] > [脅威防御のアップグレード (Threat Defense Upgrade)] を選択すると、Firewall Threat Defense アップグレードウィザードに直接移動します。 廃止された画面/オプション： • [システム (System)] (⚙️) > [更新 (Updates)] は廃止されました。Firewall Threat Defense のすべてのアップグレードでウィザードが使用されるようになりました。 • Firewall Threat Defense アップグレードウィザードの [アップグレードパッケージの追加 (Add Upgrade Package)] ボタンは、新しいアップグレードページへの [アップグレードパッケージの管理 (Manage Upgrade Packages)] リンクに置き換えられました。
推奨リリースの通知。	20240203	任意	新しい推奨リリースが利用可能になると、クラウド提供型 Firewall Management Center から通知されるようになりました。今すぐアップグレードしない場合は、後でシステムに通知するか、次の推奨リリースまでリマインダを延期できます。新しいアップグレードページには、推奨リリースも示されます。 参照：Cisco Secure Firewall Management Center の新機能（リリース別）

機能	最小の Management Center	最小の Threat Defense	詳細
Firewall Threat Defense アップグレードウィ ザードからアップグ レードするデバイス を選択します。		任意	ウィザードを使用して、アップグレードするデバイスを選択します。 Firewall Threat Defense アップグレードウィザードを使用して、アップグレードするデバイスを選択できるようになりました。ウィザード上で、選択したデバイス、残りのアップグレード候補、対象外のデバイス（および理由）、アップグレードパッケージが必要なデバイスなどの間でビューを切り替えることができます。以前は、[デバイス管理（Device Management）] ページしか使用できず、プロセスの柔軟性が大幅に低くなっていました。
無人の Firewall Threat Defense アップグレー ド。		任意	Firewall Threat Defense アップグレードウィザードは、新しい[無人モード（Unattended Mode）] メニューを使用して無人アップグレードをサポートできるようになりました。アップグレードするターゲットバージョンとデバイスを選択し、いくつかのアップグレードオプションを指定して、その場から離れるだけです。ログアウトしたり、ブラウザを閉じたりすることもできます。
さまざまなユーザーに よる同時の Firewall Threat Defense アップ グレードワークフロー。		任意	異なるデバイスをアップグレードする限り、異なるユーザーによる同時アップグレードワークフローが可能になりました。このシステムにより、すでに他の誰かのワークフローにあるデバイスをアップグレードすることはできません。以前は、すべてのユーザーで一度に1つのアップグレードワークフローのみが許可されていました。
アップグレード前の Firewall Threat Defense のトラブルシューティ ング生成をスキップし ます。		任意 (Any)	新しい[アップグレード開始前にトラブルシューティングファイルを生成する（Generate troubleshooting files before upgrade begins）] オプションを無効にすることで、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の前にトラブルシューティングファイルを自動生成することをスキップできるようになりました。これにより、時間とディスク容量を節約できます。 Firewall Threat Defense デバイス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（System）]（⚙️）>[正常性（Health）]>[モニター（Monitor）]を選択し、左側のパネルでデバイスをクリックし、[システムおよびトラブルシューティングの詳細を表示（View System & Troubleshoot Details）]、[トラブルシューティングファイルの生成（Generate Troubleshooting Files）]をクリックします。

機能	最小の Management Center	最小の Threat Defense	詳細
Firewall Threat Defense のアップグレードが正 常に完了した後の、 Snort 3 への自動アップ グレード。	任意 (Any)	任意	バージョン 7.2 以降の クラウド提供型 Firewall Management Center を使用して Firewall Threat Defense をバージョン 7.2 以降に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。ヘルプについては、ご使用のバージョンの Custom Snort 3 Intrusion Policies for Access Control を参照してください。 バージョンの制限：Firewall Threat Defense のバージョン 7.0.x へのアップグレード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。	任意 (Any)	任意 (Any)	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	最小の Management Center	最小の Threat Defense	詳細
正常なデバイスアップグレードを元に戻します。	任意	7.2.0	メジャーおよびメンテナンスアップグレードをFTDに戻すことができますようになりました。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）]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、コンテナインスタンスではサポートされません。 必要最低限の FTD : 7.1
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。	任意 (Any)	任意 (Any)	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。

機能	最小の Management Center	最小の Threat Defense	詳細
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。	任意	任意	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	最小の Management Center	最小の Threat Defense	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。	任意 (Any)	任意 (Any)	

機能	最小の Management Center	最小の Threat Defense	詳細
			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)] > [選択 (Selection)]) 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をアップロードする、またはその場所を指定するには、引き続き [システム (Systems)] > [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

機能	最小の Management Center	最小の Threat Defense	詳細
			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。	任意	任意	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。	任意 (Any)	任意 (Any)	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。
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。	任意	任意	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	最小の Management Center	最小の Threat Defense	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。	任意	任意	[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 (Update)] > [製品の更新 (Product Updates)] > [利用可能な更新 (Available Updates)] > [インストール (Install)] アイコン • [Devices] > [Device Management] > [Upgrade] • [メッセージセンター (Message Center)] > [タスク (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

機能	最小の Management Center	最小の Threat Defense	詳細
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。	任意 (Any)	任意 (Any)	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。
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。	任意 (Any)	任意 (Any)	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ます。次に、パッケージをスタンバイ/データ/セカンダリに送信します。 新規/変更された画面：[システム (System)] > [更新 (Updates)]

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。