トラブルシューティングおよび参考資料

- アップグレードパッケージのトラブルシューティング （1 ページ）
- Threat Defense のアップグレードのトラブルシューティング （2 ページ）
- 無応答および失敗したアップグレード （4 ページ）
- トラフィック フローとインスペクション （7 ページ）
- 時間とディスク容量 （11 ページ）
- アップグレード機能の履歴 （13 ページ）

アップグレードパッケージのトラブルシューティング

表 *1*:

問題	解決方法
更新しても使用可能なアップグレードがありません。	アップグレードパッケージを直接ダウンロードするには、Management Center でインターネットにアクセスできる必要があります。現在の展開で使用可能な最新バージョンをすでに実行しており、かつ、アップグレードパッケージをロード/設定していない場合も、空白のリストが表示されます。
推奨リリースがマークされていません。	推奨リリースは、対象となる場合にのみ一覧表示されます。推奨リリース以降をすでに実行している場合、またはそこまでアップグレードできない場合は、一覧表示されません。推奨リリースへのパッチは、推奨としてマークされませんが、適用することをお勧めします。

問題	解決方法
必要なパッケージが表示されません。	現在の展開に適用されるメジャーアップグレード、メンテナンスアップグレード、およびパッチアップグレードのみが一覧表示され、直接ダウンロードできます。手動でアップロードしない限り、次のものは一覧表示されません。 • 特定バージョンへのデバイスアップグレード（メジャーおよびメンテナンス）（Management Center がそのバージョン以降を実行しており、かつ、そのバージョンをサポートしているデバイスがある場合を除く）。 • デバイスパッチ（該当するメンテナンスリリースのデバイスが 1 つ以上ある場合を除く）。これは、Management Center パッチにも適用されます。 • ホットフィックス。これらは手動でアップロードする必要があります。
デバイスに適用されない、使用可能な、未ダウンロードのパッケージが表示されます。	この Management Center によって管理されるすべてのデバイスに適用されるダウンロード可能なアップグレードが一覧表示されます。マルチドメイン展開では、これに、現在アクセスできないデバイスが含まれる可能性があります。

Threat Defense のアップグレードのトラブルシューティング

表 *2:*

問題	解決方法
ターゲットバージョンの [アップグレード（Upgrade）] ボタンがない。	次のいずれかです。 • 依然として、アップグレードパッケージが必要です。 • 現在、そのバージョンにアップグレードできるものがありません。

問題	解決方法
アップグレードウィザードにデバイスが一覧表示されない。	**[デバイス（Devices）] > [デバイスのアップグレード（Device Upgrade）]**からウィザードに直接アクセスした場合は、ワークフローが空白になることがあります。 開始するには、[アップグレード先（Upgrade to）] メニューからターゲットバージョンを選択します。システムは、どのデバイスをそのバージョンにアップグレードできるかを判断し、[デバイスの詳細（Device Details）] ペインに表示します。[アップグレード先（Upgrade to）] メニューの選択肢は、Managagement Center 上のデバイス アップグレード パッケージに対応していることに注意してください。ターゲットバージョンが一覧表示されていない場合は、[アップグレードパッケージの管理（Manage Upgrade Packages）] をクリックしてアップロードします。Management Center へのアップグレードパッケージのアップロードとダウンロードを参照してください。 ターゲットバージョンがあるにもかかわらず、ウィザードにデバイスが一覧表示されない場合は、そのバージョンにアップグレードできるデバイスがありません。それでもデバイスがここに表示される必要があると思われる場合は、ユーザーロールによって、デバイスの管理が（そのため、アップグレードも）禁止されている可能性があります。マルチドメイン展開では、間違ったドメインにログインしている可能性があります。
デバイスが、他のユーザーのアップグレードワークフローにロックされる。	他のユーザーのワークフローをリセットする必要がある場合は、管理者アクセス権が必要です。次のいずれかの操作を実行できます。 • ユーザーを削除または非アクティブ化します。 • **システム**（⚙） > **[Product Upgrades]** を使用する権限がなくなるように、ユーザーのロールを更新します。

問題	解決方法
Managagement Center から管理対象デバイスへのアップグレードパッケージのコピーがタイムアウトになる。	これは、多くの場合、Management Center とそのデバイスの間の帯域幅が制限されているときに発生します。 次のいずれかを試みることができます。 • 内部 Web サーバーからアップグレードパッケージを直接取得するようにデバイスを設定します。 これを実行するには、Management Center からアップグレードパッケージを削除し（これはオプションですが、ディスク容量を節約できます）、アップグレードパッケージを再度追加します。ただし、その際、代わりにその場所へのポインタ（URL）を指定します。内部サーバーからのアップグレードパッケージのコピー を参照してください。 • 別のデバイスからアップグレードパッケージをコピーします。 少なくとも 1 つのスタンドアロンデバイスにアップグレードパッケージを取得できる場合は、Threat Defense CLI（「peer to peer sync」）を使用して、同じスタンドアロン Managagement Center によって管理されている他のスタンドアロンデバイスにアップグレードパッケージをコピーできます。Threat Defense アップグレードパッケージのデバイス間のコピー を参照してください。
アップグレードのセットアップ中に高可用性 Managagement Center がフェールオーバーする。	ワークフローも Threat Defense アップグレードパッケージも、高可用性 Management Center 間で同期されません。 フェールオーバーの場合は、新しいアクティブ Management Center でワークフローを再作成する必要があります。これには、アップグレードパッケージのダウンロードと、それらのデバイスへのコピーが含まれます（デバイスにコピー済みのアップグレードパッケージは削除されませんが、Management Center にアップロードパッケージまたはパッケージの格納場所へのポインタが必要です）。

無応答および失敗したアップグレード

無応答および失敗した Management Center のアップグレード

アップグレード中は、設定の変更の実施または展開を行わないでください。システムが非アクティブに見えても、進行中のアップグレードを手動で再起動、シャットダウン、または再起動しないでください。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 Cisco TAC にお問い合わせください。

無応答および失敗した Threat Defense のアップグレード

（注） システムが非アクティブに見えても、アップグレード中のどの時点でも再起動またはシャットダウンしないでください。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。

表 *3:*

問題	解決方法
デバイスに到達できない。	デバイスは、アップグレード中、またはアップグレードが失敗した場合に、トラフィックを渡すことを停止できます。アップグレードする前に、ユーザーの位置からのトラフィックがデバイスの管理インターフェイスにアクセスするためにデバイス自体を通過する必要がないことを確認してください。 デバイスを経由せずに Management Center の管理インターフェイスにアクセスできる必要もあります。
アップグレードまたはパッチがハングアップしているように見える/デバイスが非アクティブになっているように見える。	Management Center でのデバイス アップグレード ステータスの更新が停止しているものの、アップグレードの失敗のレポートがない場合は、アップグレードのキャンセルを試みることができます。以下を参照してください。キャンセルできない場合やキャンセルが機能しない場合は、Cisco TAC にお問い合わせください。 **ヒント**：エキスパートモードおよび tail または tailf（`tail /ngfw/var/log/sf/update.status`）を使用して、デバイス自体のアップグレードログをモニターできます。
Upgrade failed.	アップグレードが失敗する場合は、次の手順を実行してください。 • デバイスがアップグレード前の状態に戻っている（自動キャンセルが有効になっている）場合は、問題を修正して最初から再試行します。 • デバイスが引き続きメンテナンスモードである場合は、問題を修正してアップグレードを再開します。または、キャンセルし、後で再試行します。 問題が解消されない場合は、Cisco TAC にお問い合わせください。

問題	解決方法
パッチが失敗する。	進行中のパッチまたは失敗したパッチはキャンセルできません。ただし、パッチが早い段階（検証段階など）で失敗した場合は、デバイスが正常に稼働しつづける可能性があります。単純に、問題を修正し、再試行してください。 デバイスがメンテナンスモードになった後にパッチが失敗した場合は、アンインストーラが存在するか確認します。存在する場合は、それを実行して失敗したパッチを削除することを試行できます。Threat Defense パッチのアンインストールを参照してください。アンインストールが完了したら、問題を修正して再試行できます。 アンインストーラが存在しない場合、アンインストールが失敗する場合、または問題が解決しない場合は、Cisco TAC にお問い合わせください。
アップグレードをキャンセルしたい。	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。失敗したアップグレードや進行中のアップグレードは、[デバイス管理（Device Management）] ページの [アップグレード（Upgrade）] タブからアクセスできる [アップグレードステータス（Upgrade Status）] ポップアップでキャンセルできます。パッチはキャンセルできません。 キャンセルできない場合やキャンセルが機能しない場合は、Cisco TAC にお問い合わせください。
失敗したアップグレードを再試行（再開）したい。	[デバイス管理（Device Management）] ページの [アップグレード（Upgrade）] タブからアクセスできる [アップグレードステータス（Upgrade Status）] ポップアップでアップグレードを再開できます。 問題が解消されない場合は、Cisco TAC にお問い合わせください。

問題	解決方法
アップグレードが失敗した場合の動作を変更したい。	アップグレードプロセスの一部は、失敗した場合の動作の選択です。これは、[アップグレードに失敗すると自動的にキャンセルされる...（Automatically cancel on upgrade failure...）]（自動キャンセル）オプションで実行されます。 • [自動キャンセルが有効（Auto-cancel enabled）]（デフォルト）：アップグレードが失敗すると、アップグレードがキャンセルされ、デバイスは自動的にアップグレード前の状態に復元されます。これにより、再グループ化して再試行しながら、可能なかぎり迅速に通常の操作に戻ります。 • [自動キャンセルが無効（Auto-cancel disabled）]：アップグレードが失敗した場合、デバイスはそのままになります。これにより、問題を修正し、アップグレードを再開することができます。 ハイアベイラビリティおよびクラスタデバイスでは、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。自動キャンセルは、バージョン 6.6 からのアップグレードではサポートされていません。

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。

ThreatDefense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ー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 *4:* 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	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）]	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

プグレードする間、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、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。

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。詳細については、「高可用性/クラスタ展開でのシャーシのアップグレードをともなう Threat Defense のアップグレード順序」を参照してください。

表 *5:* 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

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。	—

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、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 *6:* 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、にお問い合わせください「無応答および失敗したアップグレード （4 ページ）」を参照してください。

表 7: 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、イベントデータベースのサイズ、それらがアップグレードから影響を受けるかどうか、どのような影響を受けるかによって長くなります。たとえば、多くのアクセス制御ルールを使用している場合、アップグレードではそれらのルールの格納方法をバックエンドで変更する必要があるため、さらに長い時間がかかります。
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アプライアンスにある必要があります。Management Center を使用するデバイスのアップグレードの場合は、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が示されます。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。

表 *8*：ディスク容量の確認

プラットフォーム	コマンド
Management center	**システム**（⚙）> **[モニタリング（Monitoring）]** > **[統計（Statistics）]** を選択し、Management Center を選択します。 [ディスク使用率（Disk Usage）] で、[By Partition] の詳細を展開します。
脅威防御	**システム**（⚙）> **[モニタリング（Monitoring）]** > **[統計（Statistics）]** を選択し、確認するデバイスを選択します。 [ディスク使用率（Disk Usage）] で、[By Partition] の詳細を展開します。

アップグレード機能の履歴

表 *9*：バージョン *7.2.6* の機能

機能	最小 Management Center	最小 Threat Defense	詳細
アップグレード			

機能	最小 Management Center	最小 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。	7.2.6 7.4.1	いずれか	

機能	最小 Management Center	最小 Threat Defense	詳細
			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。これには、Management Center、Threat Defense デバイス、およびすべての古いNGIPSv/ASA FirePOWER デバイスが含まれます。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。 リスト/直接ダウンロードアップグレードパッケージを取得するには、インターネットアクセスが必要です。インターネットアクセスがない場合は、手動管理に限定されます。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**（⚙）> **製品のアップグレード**では、Management Center とすべての管理対象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**（⚙）> **[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。 • **[デバイスの脅威防御のアップグレード**>（**Devices Threat Defense Upgrade**）**]** を選択すると、脅威防御のアップグレードウィザードに直接移動します。 • **システム**（⚙）> **[ユーザー（Users）]** > **[ユーザーロール（User Role）]** > **[ユーザーロールの作成（Create User Role）]** > **[メニューベースの権限（Menu-Based Permissions）]**を使用すると、[製品のアップグレード（Product Upgrades）]（システムソフトウェア）へのアクセスを許可せずに、[コンテンツの更新（Content Updates）]（VDB、GeoDB、侵入ルール ）へのアクセスを許可できます。 廃止された画面/オプション： • **システム**（⚙）> **[更新（Updates）]**は廃止されました。脅威防御アップグレードはすべてウィザードを使用するようになりました。 • 脅威防御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。

機能	最小 Management Center	最小 Threat Defense	詳細
			その他のバージョンの制限：Management Center バージョン 7.3.x または 7.4.0 ではサポートされていません。 参照：Management Center 用 Cisco Secure Firewall Threat Defense アップグレードガイド
推奨リリースの通知。	7.2.6 7.4.1	いずれか	新しい推奨リリースが利用可能になると、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。 その他のバージョンの制限：Management Center バージョン 7.3.x または 7.4.0 ではサポートされていません。 参照： Cisco Secure Firewall Management Center の新機能（リリース別）
ソフトウェアアップグレードの直接ダウンロードに関するインターネットアクセス要件を更新しました。	7.2.6 7.4.1	いずれか	**アップグレードの影響。システムは新しいリソースに接続します。** Management Center では、ソフトウェア アップグレード パッケージの直接ダウンロードの場所が sourcefire.com から amazonaws.com に変更されています。 その他のバージョンの制限：Management Center バージョン 7.3.x または 7.4.0 ではサポートされていません。 参照：「Internet Access Requirements」
Threat Defense のアップグレード			
Threat Defense のアップグレードウィザードからの復元の有効化。	7.2.6 7.4.1	任意（7.1 以降にアップグレードする場合）	脅威防御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。 その他のバージョンの制限：Threat Defense をバージョン 7.1 以降にアップグレードする必要があります。Management Center バージョン 7.3.x または 7.4.0 ではサポートされていません。 参照：Management Center 用 Cisco Secure Firewall Threat Defense アップグレードガイド

機能	最小 Management Center	最小 Threat Defense	詳細
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。	7.2.6	いずれか	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。 脅威防御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。 参照：Management Center 用 Cisco Secure Firewall Threat Defense アップグレードガイド
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。	7.2.6 7.4.1	いずれか	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。 その他のバージョンの制限：Management Center バージョン 7.3.x または 7.4.0 ではサポートされていません。 参照：Management Center 用 Cisco Secure Firewall Threat Defense アップグレードガイド
Threat Defense の無人アップグレード。	7.2.6	いずれか	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す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。 参照：Management Center 用 Cisco Secure Firewall Threat Defense アップグレードガイド

機能	最小 Management Center	最小 Threat Defense	詳細
さまざまなユーザーによる同時 Threat Defense アップグレードワークフロー。	7.2.6	いずれか	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。 参照：Management Center 用 Cisco Secure Firewall Threat Defense アップグレードガイド
アップグレード前のトラブルシューティング生成をスキップします。	7.2.6	いずれか	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。 脅威防御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**（⚙）>**[正常性（Health）]**>**[モニタ（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。 参照：Management Center 用 Cisco Secure Firewall Threat Defense アップグレードガイド
Management Center のアップグレード			
Management Center の新しいアップグレードウィザード。	7.2.6 7.4.1	いずれか	新しいアップグレード開始ページとウィザードにより、Management Center のアップグレードを簡単に実行できます。**システム**（⚙）>**[製品のアップグレード（Product Upgrades）]** を使用して、Management Center で適切なアップグレードパッケージを入手したら、[アップグレード（Upgrade）] をクリックして開始します。 その他のバージョンの制限：バージョン 7.2.6 以降/7.4.1 以降からの Management Center のアップグレードでのみサポートされます。バージョン 7.3.x または 7.4.0 からのアップグレードではサポートされていません。 Management Center を任意のバージョンにアップグレードするには、Management Center で現在実行しているバージョンのアップグレードガイドを参照してください。：Management Center 用 Cisco Secure Firewall Threat Defense アップグレードガイド。バージョン 7.4.0 を実行している場合は、バージョン 7.3.x のガイドを使用できます。

機能	最小 Management Center	最小 Threat Defense	詳細
同期を一時停止することなく、高可用性管理センターでホットフィックスを利用できます。	7.2.6 7.4.1	いずれか	ホットフィックス リリース ノートに特に記載されていない、または Cisco TAC から指示されていない限り、高可用性 Management Center にホットフィックスをインストールするために同期を一時停止する必要はありません。 その他のバージョンの制限：Management Center バージョン 7.3.x または 7.4.0 ではサポートされていません。 参照：Management Center 用 Cisco Secure Firewall Threat Defense アップグレードガイド
コンテンツの更新（Content Updates）			
スケジュール済みタスクでは、パッチおよび VDB 更新のみダウンロードされます。	7.2.6 7.4.1	いずれか	**アップグレードの影響。スケジュールされたダウンロードタスクは、メンテナンスリリースの取得を停止します。** [最新の更新のダウンロード（Download Latest Update）] スケジュール済みタスクでは、メンテナンスリリースはダウンロードされなくなり、適用可能な最新のパッチと VDB の更新のみがダウンロードされるようになりました。メンテナンス（およびメジャー）リリースを Management Center に直接ダウンロードするには、**システム**（⚙）> **[製品のアップグレード（Product Upgrades）]**を使用します。 その他のバージョンの制限：Management Center バージョン 7.3.x または 7.4.0 ではサポートされていません。 参照：「Software Update Automation」

機能	最小 Management Center	最小 Threat Defense	詳細
国コードの地理位置情報パッケージのみをダウンロードします。	7.2.6 7.4.0	いずれか	**アップグレードの影響。アップグレードすると、IP パッケージが削除される可能性があります。** バージョン 7.2.6 以降/7.4.0 以降では、IP アドレスを国や大陸にマッピングする地理位置情報データベース（GeoDB）の国コードパッケージのみをダウンロードするようにシステムを設定できます。コンテキストデータを含む大規模な IP パッケージはオプションになりました。 IP パッケージのダウンロードは次のとおりです。 • バージョン 7.2.0 ～ 7.2.5：常に有効。 • バージョン 7.2.6 ～ 7.2.x：デフォルトでは無効になっていますが、有効にすることができます。 • バージョン 7.3.x：常に有効。 • バージョン 7.4.0 ～ 7.4.1：デフォルトで有効になっていますが、無効にすることもできます。 ダウンロードがデフォルトで無効になっているバージョンに初めてアップグレードすると、システムはダウンロードを無効にし、既存の IP パッケージを削除します。IP パッケージがないと、オプションを手動で有効にして GeoDB を更新するまで、IP アドレスのコンテキスト地理位置情報データを表示できません。 新規/変更された画面： • バージョン 7.2.6/7.4.1：**システム**（⚙）**>[コンテンツの更新（Content Updates）] > [地理位置情報の更新（Geolocation Updates）]** • バージョン 7.4.0：**システム**（⚙）**> [更新（Updates）] > [地理位置情報の更新（Geolocation Updates）]** 参照：「Update the Geolocation Database」

表 *10*：バージョン *7.2.0* の機能

機能	詳細
Threat Defense のアップグレード	

機能	詳細
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。これらのデバイス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します。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 Firewall Management Center によって管理されるが、分析モードでオンプレミス 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**
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 Cisco Secure Firewall Management Center Snort 3 Configuration Guide を参照してください。 バージョンの制限：Threat Defense のバージョン 7.0.x または 7.1.x へのアップグレードはサポートされていません。

機能	詳細
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**（⚙）**[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
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**。
Management Center のアップグレード	
Management Centerのアップグレードでは、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。
コンテンツの更新（Content Updates）	

機能	詳細
GeoDB を 2 つのパッケージに分割。	2022 年 5 月、バージョン 7.2 リリースの直前に、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。IP パッケージのコンテキストデータには、追加のロケーションの詳細に加えて、ISP、接続タイプ、プロキシタイプ、ドメイン名などの接続情報を含めることができます。 バージョン 7.2.0 から 7.2.5 までの Management Center にインターネットアクセスがあり、定期的な更新を有効にしている場合、または シスコ サポートおよびダウンロード サイト から 1 回限りの更新を手動で開始した場合、両方のパッケージが自動的に取得されます。バージョン 7.2.6 以降または 7.4.0 以降では、システムに IP パッケージを取得させるかどうかを設定できます。 エアギャップ展開などで更新を手動でダウンロードする場合、パッケージを個別にインポートする必要があります。 • 国コードパッケージ：Cisco_GEODB_Update-*date-build*.sh.REL.tar • IP パッケージ：Cisco_IP_GEODB_Update-*date-build*.sh.REL.tar **[ヘルプ（Help）]**（?）>**[バージョン情報（About）]** には、システムで現在使用されているパッケージのバージョンが一覧表示されます。

表 *11 :* バージョン *7.1.0* の機能

機能	詳細
Threat Defense のアップグレード	

機能	詳細
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**（⚙）> **[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、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。	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 *12 :* 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	

機能	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。	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**（⚙）> **[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。	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 *13 :* 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**（⚙） > **[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**（⚙） > **[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 *14 :* 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 *15* : 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 *16* : 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。	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。
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 *17 :* 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**（⚙）>**[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。

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。