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

表 *1*: アップグレードパッケージのトラブルシューティング

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。	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/設定していません。
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。
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）（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）。 • 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。

Threat Defense のアップグレードのトラブルシューティング

表 *2: Threat Defense* のアップグレードのトラブルシューティング

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。
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）] > [Threat Defense のアップグレード（Threat Defense 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、Management 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 でのアップグレードパッケージの管理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。
Management 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。 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できます。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、パッケージのある場所へのポインタ（URL）を指定します。「内部サーバーからデバイスへ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。

無応答および失敗した Threat Defense のアップグレード

注意 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*：無応答および失敗した *Threat Defense* のアップグレード

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。
アップグレードが失敗する。	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。 再試行またはキャンセルできない場合、または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 の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。
クラスタ化されたデバイスのアップグレードまたはパッチが失敗し、アップグレードを再試行する代わりに再イメージ化する必要があります。	クラスタノードのアップグレードが失敗し、ノードの再イメージ化を選択した場合は、クラスタに追加する前に、現在のバージョンの制御ノードに再イメージ化します。アップグレードが失敗した時期と方法に応じて、制御ノードの現在のバージョンは古いバージョンまたはターゲットバージョンになります。 アップグレード中の一時的な場合を除き、バージョンが混在するクラスタはサポートされていません。バージョンが混在するクラスタを意図的に作成すると、停止が発生する可能性があります。 **ヒント** 障害が発生したノードをクラスタから削除し、ターゲットバージョンに再イメージ化します。クラスタの残りの部分をターゲットバージョンにアップグレードしてから、再イメージ化されたノードを追加します。
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。 高可用性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。

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。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。「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。

Caution 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 Threat Defense のアップグレード, on page 3」を参照してください。

Table 7: アップグレード時間の考慮事項

考慮事項	詳細（Details）
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

Management Center（/Volume または /var のいずれか）にデバイス 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。アップグレードパッケージをデバイスにコピーすると、準備状況チェックで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。

Table 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 : 20240808*

機能	最小の **Threat Defense**	詳細
Threat Defense のアップグレード		
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	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（*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）]** • 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）]**

機能	最小の Threat Defense	詳細
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。	任意（Any）	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、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）]** 参照：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
廃止：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」）。	7.6.0	Threat Defense CLI を使用して、管理ネットワークを介してデバイス間でアップグレードパッケージをコピーすることはできなくなりました。Management Center とそのデバイス間の帯域幅が限られている場合は、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。 廃止された CLI コマンド：**configure p2psync enable**、**configure p2psync disable**、**show peers**、**show peer details**、**sync-from-peer**、**show p2p-sync-status**

表 *10 : 20240203*

機能	最小の Threat Defense	詳細
Threat Defense のアップグレード		

機能	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。	いずれか	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**（⚙） > **[製品のアップグレード（Product Upgrades）]**では、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（Devices）]** > **[脅威防御のアップグレード（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。 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。 参照：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
Threat Defense のアップグレードウィザードからの復元の有効化。	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 7.2 以降にアップグレードする必要があります。 参照：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

機能	最小の Threat Defense	詳細
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。	任意（Any）	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。 参照：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
推奨リリースの通知。	任意（Any）	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。 参照： Cisco Secure Firewall Management Center の新機能（リリース別）
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。	任意（Any）	**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
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。	任意（Any）	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。 参照：「Internet Access Requirements」

機能	最小の Threat Defense	詳細
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。	任意（Any）	[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。 参照：「Software Update Automation」

表 *11 : 2022* 年 *12* 月 *13* 日

機能	最小の 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。	任意（Any）	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 の無人アップグレード。	任意（Any）	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：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
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。	任意（Any）	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

機能	最小の Threat Defense	詳細
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。	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。 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
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。	いずれか	**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。** Threat Defence をバージョン 7.3 以降にアップグレードする場合、[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、Snort 2 は将来のリリースで非推奨になるため、今すぐ使用を停止することを強く推奨します。 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。

機能	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 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、Secure Firewall 3100 の 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 Threat Defense は問題なくアップグレードできますが、古い Threat Defense および ASA バージョンから 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。 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。 • 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。 • 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 ASA 9.19 以上に再イメージ化してから、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、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 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。 • 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。

機能	最小の Threat Defense	詳細
		『Cisco FXOS トラブルシューティング ガイド（Firepower Threat Defense を実行している Firepower 1000/2100 および Cisco Secure Firewall 3100/4200 向け）』の「Reimage the System with a New Software Version」を参照してください。
コンテンツの更新（Content Updates）		
自動 VDB ダウンロード。	いずれか	Management Center の初期設定では、最新の脆弱性データベース（VDB）を含むようになった、利用可能な最新のソフトウェア更新をダウンロードするための週次タスクがスケジュールされています。この週次タスクを確認し、必要に応じて調整することをお勧めします。必要に応じて、VDB を実際に更新し、構成を展開する新しい週次タスクをスケジュールしてください。 新規/変更された画面：システムで作成された [週次ソフトウェアダウンロード（Weekly Software Download）] のスケジュールされたタスクで、[脆弱性データベース（Vulnerability Database）] チェックボックスがデフォルトで有効になりました。
任意の VDB をインストールします。	いずれか	VDB 357 以降、その Management Center の基準 VDB までさかのぼって任意の VDB をインストールできるようになりました。 VDB を更新したら、構成の変更を展開します。利用できなくなった脆弱性、アプリケーションディテクタ、またはフィンガープリントに基づいて設定を行っている場合は、それらの設定を調べて、トラフィックが期待どおりに処理されていることを確認します。また、VDB を更新するためのスケジュールされたタスクは、ロールバックを取り消すことができることに注意してください。これを回避するには、スケジュールされたタスクを変更するか、新しい VDB パッケージを削除します。 新しい/変更された画面：**システム**（⚙）> **[更新（Updates）]** > **[製品アップデート（Product Updates）]** > **[利用可能なアップデート（Available Updates）]** で、古い VDB をアップロードすると、[インストール（Install）] アイコンの代わりに新しい [ロールバック（Rollback）] アイコンが表示されます。

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。