ソフトウェアのアップグレードガイドライン

利便性を考え、このドキュメントには、Threat Defense リリースノートで公開されている重要なリリース固有のソフトウェアのアップグレードガイドラインを複製したものが記載されてます。Firepower 4100/9300 の FXOS アップグレードガイドラインについては、FXOS のアップグレードガイドライン を参照してください。

重要 リリースノートにも目を通してください。重要な追加情報やバージョン固有の情報が記載されている場合があります。たとえば、新機能や廃止された機能が原因で、アップグレード前またはアップグレード後に設定の変更が必要になったり、アップグレードができなかったりする場合があります。または、既知の問題（未解決のバグ）がアップグレードに影響することがあります。

アップグレードする最小バージョン

次のように バージョン 7.2 に直接アップグレードできます。

表 *1*：バージョン *7.2* にアップグレードするための最小バージョン

プラットフォーム	最小バージョン
Management Center	6.6

プラットフォーム	最小バージョン
Threat Defense （GCP 対応 Threat Defense Virtual を除く）	6.6 Firepower 4100/9300 には FXOS 2.12.0.31 が必要です。ほとんどの場合、各メジャーバージョンで最新の FXOS ビルドを使用することを推奨します。判断のヒントについては、Cisco Firepower 4100/9300 FXOS 2.12 リリースノートを参照してください。
GCP 向け Threat Defense Virtual	7.2 バージョン 7.1 以前からバージョン 7.2 以降にアップグレードすることはできないため、新しいインスタンスを展開する必要があります。バージョン 7.2.x メンテナンスリリースにアップグレードするための最小バージョンは、バージョン 7.2.0 です。「GCP 向け Threat Defense Virtual はバージョン 7.2.0 を飛び越してアップグレードできない （3 ページ）」を参照してください。

パッチを適用する最小バージョン

バージョン 7.2 にパッチを適用する場合、パッチは 4 桁目のみを変更することに注意してください。以前のメジャーリリースまたはメンテナンスリリースからパッチに直接アップグレードすることはできません。

バージョン 7.2 のアップグレードガイドライン

以下のチェックリストでは、該当する可能性のある新規アップグレードガイドラインや以前に公開されたアップグレードガイドラインを提供します。

表 *2 : Management Center* を使用した *Threat Defense* のアップグレードガイドラインバージョン *7.2*

✓	ガイドライン	プラットフォーム	アップグレード元	直接アップグレード先
	アップグレードする最小バージョン （1 ページ）	任意（Any）	任意（Any）	任意（Any）
	FXOS のアップグレードガイドライン	Firepower 4100/9300	任意（Any）	任意（Any）
	GCP 向け Threat Defense Virtual はバージョン 7.2.0 を飛び越してアップグレードできない （3 ページ）	GCP 用 Threat Defense Virtual	6.7.0 ～ 7.1.x	7.2 以降

✓	ガイドライン	プラットフォーム	アップグレード元	直接アップグレード先
	高可用性 Management Center の Cisco Secure Malware Analytics に再接続する （3 ページ）	Management Center	6.4.0 ～ 6.7.x	7.0 以上
	アップグレードの失敗：Firepower 1010 スイッチポートでの無効な VLAN ID （4 ページ）	Firepower 1010	6.4.0 ～ 6.6.x	6.7 以降

GCP 向け Threat Defense Virtual はバージョン 7.2.0 を飛び越してアップグレードできない

展開対象：GCP 向け Threat Defense Virtual

アップグレード元：バージョン 6.7.0 ～ 7.1.x

直接アップグレード先：バージョン 7.2.0 以降

自動スケーリングのサポートに必要なインターフェースの変更により、GCP 向け Threat Defense Virtual のアップグレードはバージョン 7.2.0 を飛び越すことができません。つまり、バージョン 7.1.x 以前からバージョン 7.2.0 より後にアップグレードすることはできません。新しいインスタンスを展開し、デバイス固有の設定をやり直す必要があります。

高可用性 Management Center の Cisco Secure Malware Analytics に再接続する

展開：動的分析のためにファイルを送信する高可用性/AMP for Networks（マルウェア検出）展開

アップグレード元：バージョン 6.4.0 ～ 6.7.x

直接アップグレード先：バージョン 7.0.0 以降

関連するバグ： CSCvu35704

バージョン 7.0.0 では、フェールオーバー後にシステムが動的分析用のファイルの送信を停止する高可用性の問題が修正されています。修正を有効にするには、Cisco Secure Malware Analytics パブリッククラウドに再度関連付ける必要があります。

高可用性ペアをアップグレードした後、プライマリ Management Center で次の手順を実行します。

1. **[AMP] > [ダイナミック分析接続（Dynamic Analysis Connections）]**を選択します。
2. パブリッククラウドに対応するテーブル行で、[関連付け（Associate）] をクリックします。

ポータルウィンドウが開きます。サインインする必要はありません。再関連付けは、数分以内にバックグラウンドで行われます。

アップグレードの失敗：Firepower1010スイッチポートでの無効なVLAN ID

展開：Firepower 1010

アップグレード元：バージョン 6.4 ～ 6.6

直接アップグレード先：バージョン 6.7 以降

Firepower 1010 では、VLAN ID を 3968 ー 4047 の範囲にしてスイッチポートを設定した場合、Threat Defense のバージョン 6.7 以降へのアップグレードは失敗します。これらの ID は内部使用専用です。

バージョン 7.2 パッチのアップグレードガイドライン

以下のチェックリストでは、該当する可能性のあるパッチのアップグレードガイドラインを提供します。

表 *3 : Management Center* バージョン *7.2* パッチのアップグレードガイドライン

✓	ガイドライン	プラットフォーム	アップグレード元	直接アップグレード先
	アップグレードする最小バージョン （1 ページ）	任意（Any）	任意（Any）	任意のパッチ
	アンインストールに対応するパッチ	任意（Any）	任意（Any）	任意のパッチ

応答しないアップグレード

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、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。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。

応答しない Management Center

進行中のアップグレードは再開しないでください。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。

応答しない Threat Defense のアップグレード

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では、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し、失敗したアップグレードを再試行できます。Management Center で、[デバイス管理（Device Management）] ページおよびメッセージセンターからアクセスできる [アップグレードステータス（Upgrade Status）] ポップアップを使用します。Threat Defense CLI を使用することもできます。

（注） デフォルトでは、Threat Defense はアップグレードが失敗すると自動的にアップグレード前の状態に復元されます（「自動キャンセル」）。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、アップグレードを開始するときに自動キャンセルオプションを無効にします。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。

この機能は、パッチまたはバージョン6.6以前からのアップグレードではサポートされていません。

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。

高可用性および拡張性に関するソフトウェアのアップグレード

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。

設定変更の導入

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。

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。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、それ以外の展開時に再起動されることはありません。

表 *5:* 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のテスト

参考のために、Management Center およびソフトウェアのアップグレードにかかる時間とディスク容量のテストに関するレポートを提供しています。

時間テスト

特定のプラットフォームおよびシリーズでテストされたすべてのソフトウェアアップグレードの中で最長のテスト時間を報告します。次の表で説明するように、アップグレードには、複数の理由により、指定された時間よりも時間がかかる可能性があります。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。

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応答しないアップグレード （4 ページ） を参照してください。

表 *6*: ソフトウェアアップグレードの時間テストの条件

条件	詳細
配置	デバイスアップグレードの時間は、Management Center 展開でのテストに基づいています。同様の条件の場合、リモートとローカルの管理対象デバイスの raw アップグレード時間は類似しています。
バージョン	メジャーリリースおよびメンテナンスリリースでは、以前のすべての対象メジャーバージョンからのアップグレードをテストします。パッチについては、ベースバージョンからアップグレードをテストします。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	ほとんどの場合、各シリーズの最もローエンドのモデルでテストし、場合によってはシリーズの複数のモデルでテストします。
仮想アプライアンス	メモリおよびリソースのデフォルト設定を使用してテストします。ただし、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することに注意してください。
高可用性/拡張性	特に断りのない限り、スタンドアロンデバイスでテストします。 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	シスコでは、構成およびトラフィック負荷が最小限のアプライアンスでテストを行います。 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、また、それらがアップグレードから影響を受けるかどうか、受ける場合はどのような影響を受けるかにより、長くなる場合があります。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、アップグレードはこ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、アップグレードにはさらに長い時間がかかります。

条件	詳細
コンポーネント	ソフトウェアアップグレード自体とその後の再起動のみの時間を報告します。これには、オペレーティングシステムのアップグレード、アップグレードパッケージの転送、準備状況チェック、VDB および侵入ルール （SRU/LSP）の更新、または設定の展開のための時間は含まれません。

ディスク容量テスト

特定のプラットフォーム/シリーズでテストされたすべてのソフトウェアアップグレードの中で最も多く使用されているディスク容量を報告します。これには、アップグレードパッケージをデバイスにコピーするために必要な容量が含まれます。

また、デバイス アップグレード パッケージ用に Management Center（/Volume または /var 内）に必要な容量も報告します。Threat Defense アップグレードパッケージ用の内部サーバーがある場合、または Device Manager を使用している場合は、それらの値を無視してください。

特定の場所（/var や /ngfw など）のディスク容量の見積もりを報告する場合、その場所にマウントされているパーティションのディスク容量の見積もりを報告しています。一部のプラットフォームでは、これらの場所が同じパーティション上にある場合があります。

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 *7:* 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（System）]**>**[モニタリング（Monitoring）]**>**[統計（Statistics）]**を選択し、Management Center を選択します。[Disk Usage] で、[By Partition] の詳細を展開します。
Threat Defense with Management Center	**[System]** > **[Monitoring]** > **[Statistics]**を選択し、確認するデバイスを選択します。[Disk Usage] で、[By Partition] の詳細を展開します。

バージョン 7.2.0.1 の時間とディスク容量

表 *8:* バージョン *7.2.0.1* の時間とディスク容量

プラットフォーム	ボリュームの容量	必要容量	Management Center の必要容量	アップグレード時間	リブート時間
Management Center	/ボリューム内で 59 MB	/内で 22 MB	—	7 分	7 分

プラットフォーム	ボリュームの容量	必要容量	Management Center の必要容量	アップグレード時間	リブート時間
Management Center Virtual：VMware	/ボリューム内で 61 MB	/内で 15 MB	—	10 分	4 分
Firepower 1000 シリーズ	—	/ngfw 内 1.2 GB	250 MB	7 分	10 分
Firepower 2100 シリーズ	—	/ngfw 内で 1.2 GB	300 MB	5 分	10 分
Secure Firewall 3100 シリーズ	—	/ngfw 内で 2.1 GB	490 MB	9 分	4 分
Firepower 4100 シリーズ	—	/ngfw 内 1.1 GB	51 MB	5 分	7 分
Firepower 4100 シリーズ コンテナ インスタンス	—	/ngfw 内 1.1 GB	51 MB	5 分	3 分
Firepower 9300	—	/ngfw 内 1.1 GB	51 MB	4 分	9 分
ISA 3000	/ngfw/var 内で 630 MB	/ngfw/bin 内で 180 MB	56 MB	9 分	12 分
Threat Defense Virtual：VMware	/ngfw/var 内で 660 MB	/ngfw/bin 内で 170 MB	56 MB	4 分	4 分

バージョン 7.2.0 の時間とディスク容量

表 *9*：バージョン *7.2.0* の時間とディスク容量

プラットフォーム		ボリュームの容量	必要容量	Management Center の必要容量	アップグレード時間	リブート時間
Management Center	バージョン 6.6.0 ～ 6.7.0	/var 内で 16.7 GB	/ 内で 51 MB	—	30 分	9 分
	バージョン 7.0 以降	/Volume 内で 19.1 GB	/ 内で 45 MB			
Management Center Virtual：VMware	バージョン 6.6.0 ～ 6.7.0	/var 内で 16.7 GB	/ 内で 50 MB で	—	30 分	5 分
	バージョン 7.0 以降	/Volume 内で 19.2 GB	/ 内で 45 MB			
Firepower 1000 シリーズ		—	/ngfw 内で 7.6 GB	930 MB	15 分	13 分
Firepower 2100 シリーズ		—	/ngfw 内で 7.7 GB	1.0 GB	13 分	13 分

プラットフォーム		ボリュームの容量	必要容量	Management Center の必要容量	アップグレード時間	リブート時間
Secure Firewall 3100 シリーズ		—	使用できません	1.2 GB	使用できません	使用できません
Firepower 4100 シリーズ		—	/ngfw 内で 7.8 GB	880 MB	12 分	9 分
Firepower 4100 シリーズ コンテナ インスタンス		—	/ngfw 内で 7.9 GB	880 MB	12 分	8 分
Firepower 9300		—	/ngfw 内で 11.2 GB	880 MB	11 分	12 分
ISA 3000	バージョン 6.6.0	/home 内で 9.3 GB	/ngfw 内で 270 KB	1.0 GB	21 分	8 分
	バージョン 6.7.0	/ngfw/Volume 内で 9.3 GB	/ngfw 内で 270 KB			
	バージョン 7.0.0 ～ 7.1.0	/ngfw/var 内で 9.3 GB	/ngfw/bin 内で 270 KB			
Threat Defense Virtual：VMware	バージョン 6.6.0	/home 内で 4.6 GB	/ngfw 内で 350 KB	1.0 GB	11 分	8 分
	バージョン 6.7.0	/ngfw/Volume 内で 4.4 GB	/ngfw 内で 350 KB			
	バージョン 7.0.0 ～ 7.1.0	/ngfw/var 内で 5.4 GB	/ngfw/bin 内で 250 KB			

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。