ソフトウェアのアップグレード

この章では、重要なリリースに固有の情報を提供します。

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、該当するアップグレードまたは設定ガイドのを参照してください：アップグレード手順 （26 ページ）

表 *1:* アップグレードの計画フェーズ

計画フェーズ	Includes
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。

計画フェーズ	Includes
Backups	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。 ASA FirePOWER 用 ASA 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。 ASA FirePOWER 用 ASA 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。

アップグレードする最小バージョン

パッチは4桁目のみを変更できます。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。

Version6.4.0.xパッチのアップグレードガイドライン

このチェックリストには、バージョン 6.4.0 パッチに関するアップグレードガイドラインが含まれています。

表 *2 :* バージョン *6.4.0.x* 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
	アップグレードの失敗：コンテナインスタンスのディスク容量不足（3 ページ）	Firepower 4100/9300	6.3.0 ～ 6.4.0.x	6.3.0.1 ～ 6.5.0
	Firepower 1010 デバイス上の EtherChannel で出力トラフィックがブラックホール化される可能性（3 ページ）	Firepower 1010	6.4.0 のみ	6.4.0.3 ～ 6.4.0.5
	アップグレードの注意：Firepower 7000/8000 シリーズからバージョン 6.4.0.9 ～ 6.4.0.11 へ （4 ページ）	Firepower 7000/8000 シリーズ	6.4.0 ～ 6.4.0.10	6.4.0.9 ～ 6.4.0.11

アップグレードの失敗：コンテナインスタンスのディスク容量不足

展開：FTD を搭載した Firepower 4100/9300

アップグレード元：バージョン 6.3.0 ～ 6.4.0.x

直接アップグレード先：バージョン 6.3.0.1 ～ 6.5.0

多くの場合はメジャーアップグレード時に（場合によってはパッチ適用時に）、コンテナインスタンスを使用して設定されたFTDデバイスが、ディスク容量不足のエラーにより事前チェック段階で失敗することがあります。

この問題が発生した場合には、空きディスク容量を増やしてみてください。それでも解決しない場合は、Cisco TAC にお問い合わせください。

Firepower 1010 デバイス上の EtherChannel で出力トラフィックがブラックホール化される可能性

展開：FTD を搭載した Firepower 1010

影響を受けるバージョン：バージョン 6.4.0 ～ 6.4.0.5

関連するバグ：CSCvq81354

FTD バージョン 6.4.0 ～ 6.4.0.5 を実行している Firepower 1010 デバイスでは EtherChannel を設定しないことを強くお勧めします（バージョン 6.4.0.1 および 6.4.0.2 はこのモデルではサポートされていないことに注意してください）。

内部トラフィックハッシュの問題により、Firepower 1010 デバイス上の EtherChannel では出力トラフィックがブラックホール化されることがあります。ハッシュは送信元 IP アドレスと宛

先 IP アドレスに基づくため、特定の送信元 IP と宛先 IP のペアで一貫性のある動作になります。つまり、一部のトラフィックは常に機能し、一部のトラフィックは常に失敗します。

この問題は、バージョン 6.4.0.6 および 6.5.0 で修正されています。

アップグレードの注意：Firepower 7000/8000 シリーズからバージョン 6.4.0.9 ～ 6.4.0.11 へ

展開：Firepower 7000/8000 シリーズ

アップグレード元：バージョン 6.4.0 ～ 6.4.0.10

宛先：バージョン 6.4.0.9ー6.4.0.11

関連バグ： CSCvw01028

Firepower 7000/8000 シリーズのデバイスでバージョン 6.4.0 よりも古いバージョンを実行した場合は、バージョン 6.4.0.9、6.4.0.10、または 6.4.0.11 にアップグレードしないでください。そうしないと、デバイスが応答しなくなり、再イメージ化が強制されます。代わりに、バージョン 6.4.0.12 以降にアップグレードしてください。

影響を受けるバージョンのいずれかを既に実行していて、この問題に対して脆弱である場合は、Cisco TAC に連絡して修正プログラムを入手し、できるだけ早くバージョン 6.4.0.12 にアップグレードする必要があります。イメージを再作成してアップグレードすることもできます。

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、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。

トラフィック フローとインスペクション

次の場合に、トラフィックフローおよび検査の中断が発生することがあります。

- デバイスを再起動する場合。
- デバイスソフトウェア、オペレーティングシステム、または仮想ホスティング環境をアップグレードする場合。
- デバイスソフトウェアをアンインストールまたは場合。
- ドメイン間でデバイスを移動する場合。
- 設定の変更を展開する場合（Snort プロセスが再起動する）。

デバイスタイプ、高可用性または拡張性の設定、およびインターフェイス設定によって、中断の性質が決まります。これらのタスクは、保守期間中に行うか、中断による展開環境への影響が最も小さい時点で行うことを強く推奨します。

FirepowerThreatDefenseのアップグレード時の動作：Firepower4100/9300

FXOS のアップグレード

シャーシ間クラスタリングまたはハイアベイラビリティペアの構成がある場合でも、各シャーシの FXOS を個別にアップグレードします。アップグレードの実行方法により、FXOS のアップグレード時にデバイスがトラフィックを処理する方法が決定されます。

表 *3:* トラフィックの挙動：*FXOS* のアップグレード

展開	メソッド	トラフィックの動作
スタンドアロン	—	廃棄
ハイアベイラビリティ	**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。	影響なし。
	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。	1 つのピアがオンラインになるまでドロップされる。
シャーシ間クラスタ（6.2 以降）	**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。	影響なし。
	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。	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。
シャーシ内クラスタ（Firepower 9300 のみ）	ハードウェアバイパス有効：[Bypass: Standby] または [Bypass-Force]。（6.1 以降）	検査なしで受け渡される。
	ハードウェアバイパス無効：[Bypass: Disabled]。（6.1 以降）	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。	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。

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 *4:* トラフィックの挙動：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		トラフィックの動作
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、ハードウェアバイパス強制が有効：[Bypass: Force]（6.1 以上）。	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 スタンバイ モード：[Bypass: Standby]（6.1 以上）。	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：[Bypass: Disabled]（6.1 以上）。	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。

- FMC を使用した FTD：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。

- FDM を使用した FTD：高可用性ペアの場合、スタンバイをアップグレードし、ロールを手動で切り替えてから、新しいスタンバイをアップグレードします。

（注） バージョン 6.2.0、6.2.0.1、または 6.2.0.2 からシャーシ間クラスタをアップグレードすると、各モジュールがクラスタから削除されるときに、トラフィック インスペクションで 2 ～ 3 秒のトラフィック中断が発生します。 高可用性デバイスまたはクラスタ化されたデバイスをバージョン 6.0.1 から 6.2.2.x にアップグレードするには、追加のアップグレードパス要件が必要になる場合があります。詳しくは、Cisco Firepower Management Center Upgrade Guide, Version 6.0–7.0 の「upgrade path information in the planning」の章を参照してください。

ソフトウェアのアンインストール（パッチ）

バージョン 6.2.3 以降では、パッチをアンインストールすると、アップグレード前のバージョンに戻り、設定は変更されません。

- FMC を使用した FTD：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。

- FDM を使用した FTD：サポートされていません。

設定変更の導入

アップグレード プロセス中には、設定を複数回展開します。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。詳細については、『Firepower Management Center 構成ガイド』の「Configurations that Restart the Snort Process when Deployed or Activated」を参照してください。

展開する際にリソースを要求すると、いくつかのパケットがインスペクションなしでドロップされることがあります。また、Snort プロセスを再起動すると、HA/スケーラビリティ用に設定されたものを含め、すべてのデバイスでトラフィック インスペクションが中断されます。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。

表 *5:* トラフィックの動作：構成変更の展開

インターフェイス コンフィギュレーション		トラフィックの動作
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、[Failsafe] が有効または無効（6.0.1 ～ 6.1）。	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 Fail Open: Down]：無効（6.2 以降）	廃棄
	インラインセット、[Snort Fail Open: Down]：有効（6.2 以降）	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。

Firepower Threat Defense アップグレード時の動作：その他のデバイス

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 *6:* トラフィックの挙動：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		トラフィックの動作
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、ハードウェアバイパス強制が有効：[Bypass: Force]（Firepower 2100 シリーズ、6.3 以上）。	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 スタンバイ モード：[Bypass: Standby]（Firepower 2100 シリーズ、6.3 以上）。	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：[Bypass: Disabled]（Firepower 2100 シリーズ、6.3 以上）。	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。

- FMC を使用した Firepower Threat Defense：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。
- FDM を使用した Firepower Threat Defense：高可用性ペアの場合、スタンバイをアップグレードし、ロールを手動で切り替えてから、新しいスタンバイをアップグレードします。

ソフトウェアのアンインストール（パッチ）

バージョン 6.2.3 以降では、パッチをアンインストールすると、アップグレード前のバージョンに戻り、設定は変更されません。

- FMC を使用した FTD：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。
- FDM を使用した FTD：サポートされていません。

設定変更の導入

アップグレード プロセス中には、設定を複数回展開します。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。詳細については、『Firepower Management Center 構成ガイド』の「Configurations that Restart the Snort Process when Deployed or Activated」を参照してください。

展開する際にリソースを要求すると、いくつかのパケットがインスペクションなしでドロップされることがあります。また、Snort プロセスを再起動すると、HA/スケーラビリティ用に設定されたものを含め、すべてのデバイスでトラフィック インスペクションが中断されます。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。

表 *7:* トラフィックの動作：構成変更の展開

インターフェイス コンフィギュレーション		トラフィックの動作
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

インターフェイス コンフィギュレーション		トラフィックの動作
IPS のみのインターフェイス	インラインセット、[Failsafe] が有効または無効（6.0.1 ～ 6.1）。	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 Fail Open: Down]：無効（6.2 以降）	廃棄
	インラインセット、[Snort Fail Open: Down]：有効（6.2 以降）	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。

FirePOWER 7000/8000 シリーズのアップグレード時の動作

次のセクションでは、Firepower 7000/8000 シリーズデバイスをアップグレードする際のデバイスおよびトラフィックの動作について説明します。

スタンドアロン 7000/8000 シリーズ：Firepower ソフトウェアのアップグレード

インターフェイスの構成により、アップグレード中に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 *8*：アップグレード中のトラフィックの動作：スタンドアロン *7000/8000* シリーズ

インターフェイス コンフィギュレーション	トラフィックの動作
インライン、ハードウェア バイパスが有効（[バイパスモード：バイパス（Bypass Mode: Bypass）]）	インスペクションなしで転送。ただし、トラフィックは、次の 2 つのポイントで一時的に中断します。 • アップグレード プロセスの開始時に、リンクがダウンしてから復旧（フラップ）し、ネットワーク カードがハードウェア バイパスに切り替わるとき。 • アップグレードが完了した後、リンクが復旧し、ネットワーク カードがバイパスから切り替わるとき。インスペクションはエンドポイントの再接続後に再開され、デバイス インターフェイスとのリンクを再確立します。

インターフェイス コンフィギュレーション	トラフィックの動作
インライン、ハードウェア バイパス モジュールなし、またはハードウェア バイパスが無効（[バイパスモード：非バイパス（Bypass Mode: Non-Bypass）]）	切断
インライン、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
Passive	中断なし、インスペクションなし
ルーテッド、スイッチド	切断（Dropped）

7000/8000 シリーズ ハイ アベイラビリティ ペア：Firepower ソフトウェアのアップグレード

ハイ アベイラビリティ ペアのデバイス（またはデバイス スタック）をアップグレードする間に、トラフィック フローまたはインスペクションが中断されることはありません。継続稼働できるように、一度に1つずつアップグレードされます。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。

最初にアップグレードするピアは、展開によって異なります。

- ルーテッドまたはスイッチド：最初にスタンバイが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。アップグレードの完了時には、デバイスの役割は切り替わったままです。アクティブ/スタンバイの役割を維持する場合、アップグレード前に役割を手動で切り替えます。それにより、アップグレード プロセスによって元の役割に切り替わります。
- アクセス制御のみ：最初にアクティブがアップグレードされます。アップグレードの完了時に、アクティブとスタンバイの以前の役割がデバイスで維持されます。

8000 シリーズ スタック：FirePOWER ソフトウェア アップグレード

8000 シリーズ スタックでは、デバイスは同時にアップグレードされます。プライマリ デバイスがアップグレードを完了してスタックが動作を再開するまで、トラフィックはスタックがスタンドアロンデバイスであったかのように影響を受けます。すべてのデバイスがアップグレードを完了するまで、スタックは、制限付きの混合バージョンの状態で動作します。

展開時のトラフィックの動作

アップグレード プロセス中には、設定を複数回展開します。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。詳細については、『Firepower Management Center 構成ガイド』の「Configurations that Restart the Snort Process when Deployed or Activated」を参照してください。

展開する際にリソースを要求すると、いくつかのパケットがインスペクションなしでドロップされることがあります。また、Snortプロセスを再起動すると、HA/スケーラビリティ用に設定されたものを含め、すべてのデバイスでトラフィック インスペクションが中断されます。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。

表 *9 :* 展開時のトラフィックの動作：*7000/8000* シリーズ

インターフェイス コンフィギュレーション	トラフィックの動作
インライン、[フェールセーフ（Failsafe）] が有効または無効	インスペクションなしで転送 [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、タップ モード	すぐにパケットを出力し、バイパス Snort をコピーする
Passive	中断なし、インスペクションなし
ルーテッド、スイッチド	切断（Dropped）

ASA FirePOWER アップグレード時の動作

ASA FirePOWER module にトラフィックをリダイレクトする ASA サービス ポリシーは、Firepower ソフトウェア アップグレードの間（Snort プロセスを再起動する特定の設定を導入するときなど）にモジュールがトラフィックを処理する方法を決定します。

表 *10 : ASA FirePOWER* アップグレード中のトラフィックの動作

トラフィック リダイレクションのポリシー	トラフィックの動作
フェール オープン（**sfr fail-open**）	インスペクションなしで転送
フェール クローズ（**sfr fail-close**）	切断
モニターのみ（**sfr {fail-close}|{fail-open} monitor-only**）	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

ASA FirePOWER 展開時のトラフィックの動作

Snort プロセスを再起動している間のトラフィックの動作は、ASA FirePOWER module をアップグレードする場合と同じです。

アップグレード プロセス中には、設定を複数回展開します。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。詳細については、

『Firepower Management Center 構成ガイド』の「Configurations that Restart the Snort Process when Deployed or Activated」を参照してください。

展開する際にリソースを要求すると、いくつかのパケットがインスペクションなしでドロップされることがあります。 さらに、Snort プロセスを再起動すると、トラフィック インスペクションが中断されます。サービスポリシーにより、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通過するかが決定されます。

NGIPSv アップグレード時の動作

このセクションでは、NGIPSvをアップグレードするときのデバイスとトラフィックの動作を説明します。

Firepower ソフトウェア アップグレード

インターフェイスの設定により、アップグレード中にNGIPSv がトラフィックを処理する方法が決定されます。

表 *11 : NGIPSv* アップグレード中のトラフィックの動作

インターフェイス コンフィギュレーション	トラフィックの動作
インライン	切断
インライン、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	中断なし、インスペクションなし

展開時のトラフィックの動作

アップグレード プロセス中には、設定を複数回展開します。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。詳細については、『Firepower Management Center 構成ガイド』の「Configurations that Restart the Snort Process when Deployed or Activated」を参照してください。

展開する際にリソースを要求すると、いくつかのパケットがインスペクションなしでドロップされることがあります。さらに、Snortプロセスを再起動すると、トラフィック インスペクションが中断されます。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。

表 *12 : NGIPSv* 展開時のトラフィックの動作

インターフェイス コンフィギュレーション	トラフィックの動作
インライン、[フェールセーフ（Failsafe）] が有効または無効	インスペクションなしで転送 [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、タップ モード	すぐにパケットを出力し、バイパス Snort をコピーする
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、FTD および FMC ソフトウェアの社内の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 システムが非アクティブに見えても、手動で再起動、シャットダウン、または進行中のアップグレードの再開をしないでください。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。

表 *13 :* 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	FTD のアップグレードの時間は、FMC 展開でのテストでのものです。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。

条件	詳細
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。 ハイ アベイラビリティ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。
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 FMC（/var 内）に必要な容量も報告します。または FDM 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。

表 *14*：ディスク容量の確認

プラットフォーム	コマンド
FMC	**[System]** > **[Monitoring]** > **[Statistics]**を選択し、FMC を選択します。[Disk Usage] で、[By Partition] の詳細を展開します。
FMC を使用した FTD	**[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。
FDM を使用した FTD	**show disk** CLI コマンドを使用します。

バージョン 6.4.0.14 の時間とディスク容量

表 *15*：バージョン *6.4.0.14* 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	FMC の容量	アップグレード時間	リブート時間
FMC	/var 内 4.5 GB	/ 内 170 MB	—	42 分	18 分
FMCv：VMware	/var 内 5.2 GB	/ 内 170 MB	—	25 分	2 分
Firepower 1000 シリーズ	—	/ngfw 内 2.4 GB		11 分	11 分
Firepower 2100 シリーズ	—	/ngfw 内 1.9 GB		8 分	10 分
Firepower 4100 シリーズ	—	/ngfw 内 2.5 GB		4 分	9 分
Firepower 9300	—	/ngfw 内 2.5 GB		4 分	8 分
FTD を搭載した ASA 5500-X シリーズ	/home 内 2.0 GB	/ngfw 内 110 MB		12 分	42 分
FTDv：VMware	/home 内 1.9 GB	/ngfw 内 110 MB		6 分	2 分
Firepower 7000/8000 シリーズ	3.7 GB	/ 内 170 MB		10 分	2 分
ASA FirePOWER	/var 内 4.2 GB	/ 内 38 MB		43 分	51 分
NGIPSv	/var 内 2.2 GB	/ 内 170 MB		6 分	4 分

バージョン 6.4.0.13 の時間とディスク容量

表 *16 :* バージョン *6.4.0.13* 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	FMC の容量	アップグレード時間	リブート時間
FMC	/var 内 3.8 GB	/ 内 170 MB	—	34 分	8 分
FMCv：VMware	/var 内 3.9 GB	/ 内 170 MB	—	21 分	4 分
Firepower 1000 シリーズ	—	/ngfw 内 3.0 GB	540 MB	11 分	13 分
Firepower 2100 シリーズ	—	/ngfw 内 2.6 GB	510 MB	8 分	12 分
Firepower 4100 シリーズ	—	/ngfw 内 2.5 GB	450 MB	4 分	9 分
Firepower 9300	—	/ngfw 内 2.5 GB	450 MB	4 分	9 分
FTD を搭載した ASA 5500-X シリーズ	/home 内 2.0 GB	/ngfw 内 110 MB	295 MB	12 分	9 分
FTDv：VMware	/home 内 1.9 GB	/ngfw 内 110 MB	295 MB	7 分	5 分
Firepower 7000/8000 シリーズ	/var 内 3.7 GB	/ 内 170 MB	670 MB	11 分	14 分
ASA FirePOWER	/var 内 4.2 GB	/ 内 38 MB	660 MB	43 分	8 分
NGIPSv	/var 内 2.2 GB	/ 内 170 MB	460 MB	6 分	4 分

バージョン 6.4.0.12 の時間とディスク容量

表 *17 :* バージョン *6.4.0.12* 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	FMC の容量	アップグレード時間	リブート時間
FMC	/var 内 3.8 GB	/ 内 170 MB	—	25 分	8 分
FMCv：VMware	/var 内 3.8 GB	/ 内 170 MB	—	27 分	4 分
Firepower 1000 シリーズ		/ngfw 内 2.9 GB	530 MB	10 分	13 分
Firepower 2100 シリーズ		/ngfw 内 2.5 GB	510 MB	8 分	32 分
Firepower 4100 シリーズ		/ngfw 内 2.5 GB	440 MB	4 分	9 分
Firepower 9300		/ngfw 内 2.5 GB	440 MB	4 分	8 分

プラットフォーム	ボリュームの容量	必要容量	FMC の容量	アップグレード時間	リブート時間
FTD を搭載した ASA 5500-X シリーズ	/home 内 1.9 GB	/ngfw 内 110 MB	290 MB	12 分	40 分
FTDv：VMware	/home 内 1.9 GB	/ngfw 内 110 MB	290 MB	7 分	5 分
Firepower 7000/8000 シリーズ	/var 内 3.7 GB	/ 内 170 MB	660 MB	10 分	15 分
ASA FirePOWER	/var 内 4.2 GB	/ 内 37 MB	600 MB	47 分	51 分
NGIPSv	/var 内 2.2 GB	/ 内 150 MB	460 MB	7 分	5 分

バージョン 6.4.0.11 の時間とディスク容量

表 *18 :* バージョン *6.4.0.11* 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	FMC の容量	アップグレード時間	リブート時間
FMC	3.8 GB	170 MB	—	30 分	8 分
FMCv：VMware	4.1 GB	170 MB	—	27 分	7 分
Firepower 1000 シリーズ	3.0 GB	3.0 GB	530 MB	14 分	9 分
Firepower 2100 シリーズ	2.5 GB	2.5 GB	510 MB	9 分	6 分
Firepower 4100 シリーズ	1.8 GB	1.8 GB	310 MB	8 分	7 分
Firepower 9300	1.8 GB	1.8 GB	310 MB	9 分	9 分
FTD を搭載した ASA 5500-X シリーズ	1.6 GB	110 MB	290 MB	12 分	12 分
FTDv：VMware	4.4 GB	170 MB	290 MB	28 分	4 分
Firepower 7000/8000 シリーズ	3.6 GB	170 MB	680 MB	11 分	97 分
ASA FirePOWER	4.2 GB	36 MB	630 MB	54 分	51 分
NGIPSv	2.4 GB	150 MB	470 MB	11 分	15 分

バージョン 6.4.0.10 の時間とディスク容量

表 *19 :* バージョン *6.4.0.10* 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	FMC の容量	アップグレード時間	リブート時間
FMC	3.8 GB	170 MB	—	30 分	8 分
FMCv：VMware	4.1 GB	170 MB	—	27 分	7 分
Firepower 1000 シリーズ	2.9 GB	2.9 GB	560 MB	11 分	14 分
Firepower 2100 シリーズ	2.5 GB	2.5 GB	530 MB	8 分	13 分
Firepower 4100 シリーズ	1.8 GB	1.8 GB	330 MB	5 分	11 分
Firepower 9300	1.8 GB	1.8 GB	330 MB	5 分	17 分
FTD を搭載した ASA 5500-X シリーズ	1.9 GB	110 MB	310 MB	12 分	31 分
FTDv：VMware	2.0 GB	110 MB	310 MB	8 分	8 分
Firepower 7000/8000 シリーズ	3.6 GB	170 MB	680 MB	11 分	97 分
ASA FirePOWER	4.2 GB	36 MB	630 MB	54 分	51 分
NGIPSv	2.4 GB	150 MB	470 MB	11 分	15 分

バージョン 6.4.0.9 の時間とディスク容量

表 *20 :* バージョン *6.4.0.9* 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	FMC の容量	アップグレード時間	リブート時間
FMC	3.7 GB	170 MB	—	41 分	10 分
FMCv：VMware	3.7 GB	170 MB	—	28 分	6 分
Firepower 1000 シリーズ	2.9 GB	2.9 GB	530 MB	11 分	14 分

プラットフォーム	ボリュームの容量	必要容量	FMC の容量	アップグレード時間	リブート時間
Firepower 2100 シリーズ	2.6 GB	2.6 GB	510 MB	10 分	13 分
Firepower 4100 シリーズ	1.8 GB	1.8 GB	310 MB	4 分	10 分
Firepower 9300	1.8 GB	1.8 GB	310 MB	4 分	10 分
FTD を搭載した ASA 5500-X シリーズ	1.9 GB	290 MB	290 MB	12 分	42 分
FTDv：VMware	1.9 GB	290 MB	290 MB	7 分	9 分
Firepower 7000/8000 シリーズ	3.7 GB	170 MB	650 MB	20 分	6 分
ASA FirePOWER	4.2 GB	36 MB	600 MB	48 分	48 分
NGIPSv	2.1 GB	150 MB	450 MB	6 分	4 分

バージョン 6.4.0.8 の時間とディスク容量

表 *21 :* バージョン *6.4.0.8* 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	FMC の容量	アップグレード時間
FMC	5.0 GB	170 MB	—	44 分
FMCv：VMware	5.1 GB	170 MB	—	32 分
Firepower 1000 シリーズ	3.0 GB	3.0 GB	530 MB	18 分
Firepower 2100 シリーズ	2.5 GB	2.5 GB	510 MB	18 分
Firepower 4100 シリーズ	1.8 GB	1.8 GB	310 MB	14 分
Firepower 9300	2.0 GB	2.0 GB	310 MB	11 分
FTD を搭載した ASA 5500-X シリーズ	1.8 GB	110 MB	290 MB	17 分
FTDv：VMware	1.9 GB	110 MB	290 MB	12 分
Firepower 7000/8000 シリーズ	3.7 GB	190 MB	650 MB	25 分

プラットフォーム	ボリュームの容量	必要容量	FMC の容量	アップグレード時間
ASA FirePOWER	2.2 GB	110 MB	590 MB	16 分
NGIPSv	2.1 GB	150 MB	450 MB	9 分

バージョン 6.4.0.7 の時間とディスク容量

表 *22 :* バージョン *6.4.0.7* 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	FMC の容量	アップグレード時間
FMC	4.9 GB	170 MB	—	41 分
FMCv：VMware	5.1 GB	170 MB	—	32 分
Firepower 1000 シリーズ	2.9 GB	2.9 GB	530 MB	17 分
Firepower 2100 シリーズ	2.4 GB	2.4 GB	500 MB	17 分
Firepower 4100 シリーズ	1.7 GB	1.7 GB	310 MB	15 分
Firepower 9300	2.4 GB	2.4 GB	310 MB	12 分
FTD を搭載した ASA 5500-X シリーズ	1.9 GB	110 MB	290 MB	18 分
FTDv：VMware	1.8 GB	110 MB	290 MB	9 分
Firepower 7000/8000 シリーズ	3.7 GB	190 MB	650 MB	28 分
ASA FirePOWER	4.2 GB	36 MB	590 MB	54 分
NGIPSv	2.3 GB	150 MB	450 MB	9 分

バージョン 6.4.0.6 の時間とディスク容量

バージョン 6.4.0.6 は 2019 年 12 月 19 日に シスコ サポートおよびダウンロード サイト から削除されました。このバージョンを実行している場合は、アップグレードすることをお勧めします。

バージョン 6.4.0.5 の時間とディスク容量

表 *23 :* バージョン *6.4.0.5* 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	FMC の容量	アップグレード時間
FMC	5.0 GB	170 MB	—	39 分
FMCv：VMware	3.7 GB	170 MB	—	27 分
Firepower 1000 シリーズ	2.9 GB	2.9 GB	530 MB	26 分
Firepower 2100 シリーズ	2.5 GB	2.5 GB	500 MB	16 分
Firepower 4100 シリーズ	1.8 GB	1.8 GB	310 MB	12 分
Firepower 9300	1.8 GB	1.8 GB	310 MB	11 分
FTD を搭載した ASA 5500-X シリーズ	1.8 GB	110 MB	290 MB	20 分
FTDv：VMware	1.8 GB	110 MB	290 MB	10 分
Firepower 7000/8000 シリーズ	3.6 GB	170 MB	650 MB	26 分
ASA FirePOWER	4.1 GB	36 MB	590 MB	45 分
NGIPSv	2.1 GB	150 MB	450 MB	10 分

バージョン 6.4.0.4 の時間とディスク容量

表 *24 :* バージョン *6.4.0.4* 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	FMC の容量	アップグレード時間
FMC	4.4 GB	170 MB	—	35 分
FMCv：VMware	4.8 GB	170 MB	—	31 分
Firepower 1000 シリーズ	2.9 GB	2.9 GB	520 MB	28 分
Firepower 2100 シリーズ	2.4 GB	2.4 GB	500 MB	10 分
Firepower 4100 シリーズ	2.0 GB	2.0 GB	310 MB	12 分
Firepower 9300	1.7 GB	1.7 GB	310 MB	10 分

プラットフォーム	ボリュームの容量	必要容量	FMC の容量	アップグレード時間
FTD を搭載した ASA 5500-X シリーズ	1.8 GB	110 MB	290 MB	29 分
FTDv：VMware	1.8 GB	110 MB	290 MB	8 分
Firepower 7000/8000 シリーズ	3.6 GB	170 MB	650 MB	24 分
ASA FirePOWER	4.2 GB	36 MB	600 MB	55 分
NGIPSv	2.1 GB	150 MB	550 MB	10 分

バージョン 6.4.0.3 の時間とディスク容量

表 *25 :* バージョン *6.4.0.3* 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	FMC の容量	アップグレード時間
FMC	3.2 GB	24 MB	—	34 分
FMCv：VMware	2.5 GB	23 MB	—	25 分
Firepower 1000 シリーズ	2.9 GB	2.9 GB	520 MB	22 分
Firepower 2100 シリーズ	2.4 GB	2.4 GB	500 MB	19 分
Firepower 4100 シリーズ	1.7 GB	1.7 GB	310 MB	12 分
Firepower 9300	1.7 GB	1.7 GB	310 MB	14 分
FTD を搭載した ASA 5500-X シリーズ	1.8 GB	110 MB	290 MB	18 分
FTDv：VMware	1.8 GB	110 MB	290 MB	12 分
Firepower 7000/8000 シリーズ	1.9 GB	21 MB	370 MB	20 分
ASA FirePOWER	2.5 GB	2.5 GB	320 MB	28 分
NGIPSv	690 MB	21 MB	210 MB	8 分

バージョン 6.4.0.2 の時間とディスク容量

表 *26 :* バージョン *6.4.0.2* 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	FMC の容量	アップグレード時間
FMC	3.1 GB	24 MB	—	39 分
FMCv：VMware	2.5 GB	23 MB	—	24 分
Firepower 2100 シリーズ	1.9 GB	1.9 GB	480 MB	19 分
Firepower 4100 シリーズ	2.3 GB	2.3 GB	290 MB	11 分
Firepower 9300	1.7 GB	1.7 GB	290 MB	11 分
FTD を搭載した ASA 5500-X シリーズ	1.8 GB	110 MB	270 MB	21 分
FTDv：VMware	1.2 GB	110 MB	270 MB	10 分
Firepower 7000/8000 シリーズ	1.9 GB	36 MB	350 MB	20 分
ASA FirePOWER	2.0 GB	21 MB	300 MB	34 分
NGIPSv	630 MB	21 MB	190 MB	10 分

バージョン 6.4.0.1 の時間とディスク容量

表 *27 :* バージョン *6.4.0.1* 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	FMC の容量	アップグレード時間
FMC	1.8 GB	24 MB	—	50 分
FMCv：VMware	1.8 GB	23 MB	—	20 分
Firepower 2100 シリーズ	1.4 GB	1.4 GB	300 MB	17 分
Firepower 4100 シリーズ	1.1 GB	1.1 GB	95 MB	9 分
Firepower 9300	1.1 GB	1.1 GB	95 MB	10 分
FTD を搭載した ASA 5500-X シリーズ	550 MB	110 MB	76 MB	16 分
FTDv：VMware	550 MB	110 MB	76 MB	15 分

プラットフォーム	ボリュームの容量	必要容量	FMC の容量	アップグレード時間
Firepower 7000/8000 シリーズ	59 MB	21 MB	2 MB	14 分
ASA FirePOWER	85 MB	20 MB	2 MB	30 分
NGIPSv	45 MB	21 MB	2 MB	10 分

アップグレード手順

リリースノートにはアップグレード手順は含まれていません。これらのリリースノートに記載されているガイドラインと警告を読んだ後、次のいずれかのドキュメントを参照してください。

表 *28 : Firepower* アップグレード手順

タスク	ガイド
Firepower Management Center の展開でアップグレードします。	Cisco Firepower Management Center Upgrade Guide, Version 6.0–7.0
Firepower Device Manager を搭載した Firepower Threat Defense をアップグレードします。	Firepower Device Manager 用 Cisco Firepower Threat Defense 構成ガイド アップグレード先のバージョンではなく、現在実行している Firepower Threat Defense バージョンのガイドの「*System Management*」の章を参照してください。
Firepower 4100/9300 シャーシの FXOS のアップグレード。	Cisco Firepower 4100/9300 Upgrade Guide, Firepower 6.0.1–7.0.x or ASA 9.4(1)–9.16(x) with FXOS 1.1.1–2.10.1
ASDM を使用した ASA FirePOWER モジュールのアップグレード。	Cisco ASA Upgrade Guide
ISA 3000、ASA 5508-X、ASA 5516-X で ROMMON イメージをアップグレードします。	Cisco ASA and Firepower Threat Defense Reimage Guide 「*Upgrade the ROMMON Image*」のセクションを参照してください。常に最新のイメージがあることを確認してください。