



バージョン 6.5.0.x へのアップグレード

この章では、バージョン 6.5.0.x の重要なリリースに固有の情報を提供します。

- [に関するガイドラインと警告 バージョン 6.5.0.x \(1 ページ\)](#)
- [一般的なガイドラインと警告 \(1 ページ\)](#)
- [アップグレードする最小バージョン, on page 4](#)
- [時間テストとディスク容量の要件 \(5 ページ\)](#)
- [トラフィック フロー、検査、およびデバイス動作 \(8 ページ\)](#)
- [アップグレード手順 \(17 ページ\)](#)
- [アップグレードパッケージ, on page 17](#)

に関するガイドラインと警告 バージョン 6.5.0.x

バージョン 6.5.0.x パッチに特に適用される重要なアップグレードガイドラインと警告はありません。ただし、「[一般的なガイドラインと警告 \(1 ページ\)](#)」を確認するようにしてください。

一般的なガイドラインと警告

これらの重要なガイドラインと警告は、すべてのアップグレードに適用されます。ただし、このリストは包括的なものではありません。アップグレードパスの計画、OS のアップグレード、準備状況チェック、バックアップ、メンテナンス期間など、アップグレードプロセスに関するその他の重要な情報へのリンクについては、「[アップグレード手順 \(17 ページ\)](#)」を参照してください。

イベントデータと設定データのバックアップ

サポートされている場合は、アップグレードの前後にバックアップすることをお勧めします。

- **アップグレード前**：アップグレードが致命的なレベルで失敗した場合は、再イメージ化と復元が必要になることがあります。再イメージ化によって、システムパスワードを含むほとんどの設定が工場出荷時の初期状態に戻ります。最近のバックアップがある場合は、通常の操作にすばやく戻ることができます。

- アップグレード後：これにより、新しくアップグレードされた展開のスナップショットが作成されます。新しい FMC バックアップファイルがデバイスがアップグレードされたことを「認識」するように、管理対象デバイスをアップグレードした後に FMC をバックアップすることをお勧めします。

安全なリモートロケーションにバックアップし、正常に転送が行われることを確認する必要があります。アップグレードによって、ローカルに保存されたバックアップは消去されます。特に、バックアップファイルは暗号化されていないため、不正アクセスを許可しないでください。バックアップファイルが変更されていると、復元プロセスは失敗します。

バックアップの最初のステップとして、アプライアンスモデルとバージョンを、パッチレベルを含めて書き留めておいてください。FMC の場合は、VDB のバージョンを書き留めておきます。Firepower 4100/9300 シャーシの場合は、FXOS のバージョンを書き留めておきます。新しいアプライアンスや再イメージ化したアプライアンスにバックアップを復元する必要がある場合は、新しいアプライアンスを最初に更新する必要がある場合があるため、これは重要です。



- (注) バックアップと復元は、複雑なプロセスになる可能性があります。手順をスキップしたり、セキュリティ上の問題を無視しないでください。誤りを避けるには、注意深い計画と準備が役立ちます。バックアップと復元の要件、ガイドライン、制限事項、およびベストプラクティスの詳細については、ご使用の Firepower 製品のコンフィギュレーションガイドを参照してください。

NTP 同期の確認

アップグレードする前に、時刻の提供に使用している NTP サーバと Firepower アプライアンスが同期していることを確認します。同期されていないと、アップグレードが失敗する可能性があります。FMC 展開では、時刻のずれが 10 秒を超えている場合、[時刻同期化ステータス (Time Synchronization Status)] ヘルスマジュールからアラートが発行されますが、手動で確認する必要があります。

時刻を確認するには、次の手順を実行します。

- FMC : [システム (System)] > [設定 (Configuration)] > [時刻 (Time)] を選択します。
- デバイス : **show time** CLI コマンドを使用します。

帯域幅をチェックする

Firepower アプライアンスをアップグレードする (または準備状況チェックを実行する) には、アップグレードパッケージがアプライアンス上に存在する必要があります。Firepower アップグレードパッケージには、さまざまなサイズがあります。管理ネットワークに大量のデータ転送を実行するための帯域幅があることを確認します。

FMC の展開では、アップグレードパッケージをアップグレード時に管理対象デバイスに転送する場合は、帯域幅が不十分だとアップグレード時間が長くなったり、アップグレードがタイム

アウトする原因となる可能性があります。アップグレードする前に、管理対象デバイスに Firepower アップグレードパッケージを手動でプッシュ（コピー）することをお勧めします。詳細については、『[Guidelines for Downloading Data from the Firepower Management Center to Managed Devices](#)』（トラブルシューティング テクニカルノート）を参照してください。

アプライアンスアクセス

Firepower デバイスは、（インターフェイス設定に応じて）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。Firepower デバイスをアップグレードする前に、ユーザ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。Firepower Management Center 展開では、デバイスを経由せずに FMC 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。

署名付きのアップグレードパッケージ

Firepower では、正しいファイルを使用していることを確認できるようにするために、アップグレードパッケージとホットフィックスパッケージは「署名付き」のアーカイブになっています。署名付きの（.tar）パッケージは解凍しないでください。



- (注) 署名付きのアップグレードパッケージをアップロードした後、システムがパッケージを確認する際に、GUIのロードに数分かかることがあります。表示を高速化するには、署名付きのパッケージが不要になった後、それらのパッケージを削除します。

ASA FirePOWER デバイスでの ASA REST API の無効化

ASA FirePOWER モジュールをアップグレードする前に、ASA REST API を無効にしていることを確認します。無効にしていない場合、アップグレードが失敗することがあります。ASA CLI から :no rest api agent。アンインストール後に再度有効にすることができます :rest-api agent。

シスコとのデータの共有

一部の機能にシスコとのデータ共有が含まれます。

6.2.3+ では、*Cisco Success Network* は、テクニカルサポートを提供するために不可欠な使用状況に関する情報と統計情報をシスコに送信します。アップグレード中に、参加を承諾するか、辞退するかを尋ねられます。また、いつでもオプトインまたはオプトアウトできます。

バージョン 6.2.3+ では、Web 分析のトラッキングは、これに限定されませんが、ページでの操作、ブラウザのバージョン、製品のバージョン、ユーザの場所、FMC の管理 IP アドレスまたはホスト名を含む、個人を特定できない使用状況データをシスコに送信します。現在の設定でオプトアウトが選択されている場合でも、メジャーアップグレードによって Web 分析トラッキングが有効になります。このデータの収集を拒否する場合は、各メジャーアップグレードの後にオプトアウトしてください。

6.5.0+ では、*Cisco Support Diagnostics*（「シスコのプロアクティブサポート」とも呼ばれる）は、設定および運用上の健全性データをシスコに送信し、自動化された問題検出システムを通じてそのデータを処理して問題をプロアクティブに通知できるようにします。また、この機能により、Cisco TAC は TAC ケースの過程でデバイスから必要な情報を収集することもできます。アップグレード中に、参加を承諾するか、辞退するかを尋ねられます。また、いつでもオプトインまたはオプトアウトできます。

アップグレードにより侵入ルールをインポートして自動的に有効化できます。

現在の Firepower バージョンでサポートされていないキーワードが新しい侵入ルールで使用されている場合、侵入ルールデータベース（SRU）を更新しても、そのルールはインポートされません。

Firepower ソフトウェアをアップグレードし、これらのキーワードがサポートされると、新しい侵入ルールがインポートされ、IPS の設定に応じて自動的に有効化できるため、イベントの生成とトラフィックフローへの影響を開始できます。

サポートされているキーワードは、Firepower ソフトウェアに含まれている Snort のバージョンによって異なります。

- FMC : [ヘルプ (Help)] > [About (バージョン情報)] を選択します。
- FDM を使用した FTD : **show summary** CLI コマンドを使用します。
- ASDM を使用した ASA FirePOWER : [ASA FirePOWER 設定 (ASA FirePOWER Configuration)] > [システム情報 (System Information)] を選択します。

また、[Cisco Firepower Compatibility Guide](#)の「*Bundled Components*」の項で Snort バージョンを確認することもできます。

Snort リリースノートには、新しいキーワードの詳細が含まれています。<https://www.snort.org/downloads> で Snort ダウンロードページのリリースノートを参照できます。

応答しないアップグレード

アップグレードしているアプライアンスとの間での変更の展開、またはアップグレードしているアプライアンスの手動での再起動やシャットダウンは行わないでください。進行中のアップグレードを再開しないでください。事前のチェック中に、アップグレードプロセスが停止しているように見える場合がありますが、これは想定内の動作です。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。

アップグレードする最小バージョン

現在のメジャーバージョンシーケンス内だけで Firepower ソフトウェアにパッチを適用できます。パッチは累積されるため、常に最新のパッチに直接スキップできます。

Table 1: Firepower ソフトウェアをバージョン 6.5.0.x 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
Firepower Management Center FMC 展開のすべての管理対象デバイス。	6.5.0
FDM を使用した Firepower Threat Defense (すべてのプラットフォーム)	6.5.0
ASDM を使用した ASA FirePOWER	6.5.0

時間テストとディスク容量の要件

Firepower アプライアンスを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。Firepower Management Center を使用して管理対象デバイスをアップグレードする場合、デバイスアップグレードパッケージに対して、FMC は /Volume パーティションに追加のディスク容量を必要とします。また、アップグレードを実行するための十分な時間を確保してください。

参考のために、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。

時間テストについて

ここで指定した時間の値は、社内のテストに基づいています。



- (注) 特定のプラットフォーム/シリーズについてテストされたすべてのアップグレードの最も遅い時間を報告していますが、複数の理由により（以下を参照）、報告された時間よりも、アップグレードにかかる時間が長くなることがあります。

テスト条件

- 展開：値は、Firepower Management Center 展開のテストから取得されています。これは、同様の条件の場合、リモートとローカルで管理されているデバイスの raw アップグレード時間が類似しているためです。
- バージョン：メジャーアップグレードの場合、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。
- 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。
- 仮想設定：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。

- **ハイアベイラビリティと拡張性**：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。

- **構成**：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。

時間はアップグレードのみを対象

値は、各プラットフォーム上で Firepower アップグレードスクリプトの実行にかかる時間のみを表しています。これらには、次の時間は含まれていません。

- 管理対象デバイスへのアップグレードパッケージの転送（アップグレード前かアップグレード中かにかかわらず）。
- 準備状況チェック。
- VDB と SRU の更新。
- 設定の展開。
- リポート（値が別途に報告される場合がある）。

ディスク容量の要件について

容量の見積もりは、すべてのアップグレードについて報告された最大のものです。2020年前半以降のリリースでは、次のようになります。

- 切り上げなし（1 MB 未満）。
- 次の 1 MB に切り上げ（1 MB ～ 100 MB）。
- 次の 10 MB に切り上げ（100 MB ～ 1 GB）。
- 次の 100 MB に切り上げ（1 GB を超える容量）。

バージョン 6.5.0.4 の時間とディスク容量

Table 2: バージョン 6.5.0.4 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	時間
Firepower 1000 シリーズ	2.6 GB	2.6 GB	500 MB	20 分
Firepower 2100 シリーズ	[2.5 GB]	[2.5 GB]	530 MB	18 分
Firepower 4100 シリーズ	[2.5 GB]	[2.5 GB]	360 MB	13 分
Firepower 9300	[2.5 GB]	[2.5 GB]	360 MB	17 分
ASA 5500-X シリーズ with FTD	1.9 GB	110 MB	310 MB	16 分
FTDv : VMware 6.0	1.9 GB	110 MB	310 MB	9 分
ASA FirePOWER	2.6 GB	20 MB	340 MB	72 分
NGIPSv : VMware 6.0	740 MB	20 MB	230 MB	8 分

バージョン 6.5.0.3 の時間とディスク容量

バージョン 6.5.0.3 は、2019 年 2 月 4 日（FMC の場合）および 2020 年 3 月 2 日（デバイスの場合）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、続行しても安全です。

バージョン 6.5.0.2 の時間とディスク容量

Table 3: バージョン 6.5.0.2 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	時間
FMC	2.6 GB	20 MB	—	42 分
FMCv : VMware 6.0	2.7 GB	23 MB	—	34 分
Firepower 1000 シリーズ	[2.5 GB]	[2.5 GB]	480 MB	12 分
Firepower 2100 シリーズ	2.3 GB	2.3 GB	500 MB	17 分
Firepower 4100 シリーズ	2.3 GB	2.3 GB	340 MB	13 分
Firepower 9300	2.3 GB	2.3 GB	340 MB	17 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	時間
ASA 5500-X シリーズ with FTD	1.9 GB	110 MB	280 MB	22 分
FTDv : VMware 6.0	1.7 GB	110 MB	280 MB	10 分
ASA FirePOWER	[2.5 GB]	20 MB	320 MB	56 分
NGIPSv : VMware 6.0	680 MB	18 MB	210 MB	9 分

バージョン 6.5.0.1 の時間とディスク容量

バージョン 6.5.0.1 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。

トラフィック フロー、検査、およびデバイス動作

アップグレード中に発生するトラフィックフローおよびインスペクションでの潜在的な中断を特定する必要があります。これは、次の場合に発生する可能性があります。

- デバイスが再起動された場合。
- デバイス上で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。
- デバイス上で Firepower ソフトウェアをアップグレードするか、パッチをアンインストールする場合。
- アップグレードまたはアンインストール プロセスの一部として設定変更を展開する場合 (Snort プロセスが再開します)。

デバイスのタイプ、展開のタイプ (スタンドアロン、ハイアベイラビリティ、クラスタ化)、およびインターフェイスの設定 (パッシブ、IPS、ファイアウォールなど) によって中断の性質が決まります。アップグレードまたはアンインストールは、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。

FTD アップグレード時の動作 : Firepower 4100/9300 Chassis

このセクションでは、FTD を搭載した Firepower 4100/9300 シャーシ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 4100/9300 Chassis : 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 4: FXOS アップグレード中のトラフィックの動作

展開	方法	トラフィックの動作
スタンドアロン	—	ドロップされる
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)	Fail-to-wire 有効 : [バイパス : スタンバイ (Bypass: Standby)] または [バイパス : 強制 (Bypass-Force)] (6.1 以降)	インスペクションなしで転送
	Fail-to-wire 無効 : [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
	fail-to-wire 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 FTD デバイス : Firepower ソフトウェアのアップグレード

インターフェイスの設定により、アップグレード中にスタンドアロン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 5: Firepower ソフトウェア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 FTD デバイス

インターフェイスの設定		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。	ドロップされる
IPS のみのインターフェイス	インラインセット、fail-to-wire が有効 : [バイパス : スタンバイ (Bypass: Standby)] または [バイパス : 強制 (Bypass-Force)] (6.1 以降)	次のいずれかを行います。 <ul style="list-style-type: none"> • ドロップ (6.1 から 6.2.2.x) • インスペクションなしで転送 (6.2.3 以降)
	インラインセット、fail-to-wire が無効 : [バイパス : 無効 (Bypass: Disabled)] (6.1 以降)	ドロップされる
	インラインセット、fail-to-wire モジュールなし	ドロップされる
	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

ハイアベイラビリティペア : FirePOWER ソフトウェアアップグレード

ハイアベイラビリティペアのデバイスの FirePOWER ソフトウェア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。

スタンバイ側の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。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。

クラスタ : FirePOWER ソフトウェアアップグレード

Firepower Threat Defense クラスタのデバイスで FirePOWER ソフトウェア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。

スレーブセキュリティ モジュールを最初にアップグレードして、その後マスターをアップグレードします。アップグレード中、セキュリティモジュールはメンテナンスモードで稼働しません。

マスター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спек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ブルーニングすることがあります。



- (注) バージョン 6.2.0、6.2.0.1、または 6.2.0.2 からシャーン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たびに、トラフィック インспекションで 2~3 秒のトラフィック 中断が発生します。この中断中にトラフィックがドロップされるか、それ以上インспекションが行われずに受け渡されるかは、デバイスがトラフィックを処理する方法に応じて異なります。

ハイアベイラビリティとクラスタリング ヒットレス アップグレードの要件

ヒットレスアップグレードの実行には、次の追加要件があります。

フローオフロード : フローオフロード機能でのバグ修正により、FXOS と FTD のいくつかの組み合わせはフローオフロードをサポートしていません。『[Cisco Firepower Compatibility Guide](#)』を参照してください。ハイアベイラビリティまたはクラスタ化された展開でヒットレスアップグレードを実行するには、常に互換性のある組み合わせを実行していることを確認する必要があります。

アップグレードパスに FXOS の 2.2.2.91、2.3.1.130、またはそれ以降のアップグレード (FXOS 2.4.1.x、2.6.1 などを含む) が含まれている場合、次のパスを使用します。

1. FTD を 6.2.2.2 以降にアップグレードします。
2. FXOS を 2.2.2.91、2.3.1.130、またはそれ以降にアップグレードします。
3. FTD を最終バージョンにアップグレードします。

たとえば、FXOS 2.2.2.17/FTD 6.2.2.0 を実行していて、FXOS 2.6.1/FTD 6.4.0 にアップグレードする場合は、次を実行できます。

1. FTD を 6.2.2.5 にアップグレードします。
2. FXOS を 2.6.1 にアップグレードします。
3. FTD を 6.4.0 にアップグレードします。

バージョン 6.1.0 へのアップグレード : FTD ハイアベイラビリティペアのバージョン 6.1.0 へのヒットレスアップグレードを実行するには、プレインストールパッケージが必要です。詳細に

については、『[Firepower System Release Notes Version 6.1.0 Preinstallation Package](#)』を参照してください。

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 Configuration Guide](#)』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 Firepower 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 6: FTD 展開時のトラフィックの動作

インターフェイスの設定		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。	ドロップされる
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 (6.0.1 ~ 6.1.0.x)	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。
	インラインセット、[Snort フェールオープン : ダウン (Snort Fail Open: Down)] : 無効 (6.2 以降)	ドロップされる
	インラインセット、[Snort フェールオープン : ダウン (Snort Fail Open: Down)] : 有効 (6.2+)	インスペクションなしで転送
	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

FTD アップグレード時の動作：その他のデバイス

このセクションでは、Firepower 1000/2100 シリーズ、ASA 5500-X シリーズ、ISA 3000、および FTDv で Firepower Threat Defense 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。

スタンドアロン FTD デバイス：Firepower ソフトウェアのアップグレード

インターフェイスの設定により、アップグレード中にスタンドアロン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 7: Firepower ソフトウェア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 FTD デバイス

インターフェイスの設定		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。	ドロップされる
IPS のみのインターフェイス	インラインセット、fail-to-wire が有効：[バイパス：スタンバイ (Bypass: Standby)] または [バイパス：強制 (Bypass-Force)] (6.1 以降)	次のいずれかを行います。 <ul style="list-style-type: none"> • ドロップ (6.1 から 6.2.2.x) • インスペクションなしで転送 (6.2.3 以降)
	インラインセット、fail-to-wire が無効：[バイパス：無効 (Bypass: Disabled)] (6.1 以降)	ドロップされる
	インラインセット、fail-to-wire モジュールなし	ドロップされる
	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

ハイアベイラビリティペア：FirePOWER ソフトウェアアップグレード

ハイアベイラビリティペアのデバイスの FirePOWER ソフトウェア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。

スタンバイ側の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。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。

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 Configuration Guide](#)』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 packets 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 Firepower 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 8: FTD 展開時のトラフィックの動作

インターフェイスの設定		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。	ドロップされる

インターフェイスの設定		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、[フェールセーフ (Failsafe)] が有効または無効 (6.0.1 ~ 6.1.0.x)	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。
	インラインセット、[Snortフェールオープン：ダウン (Snort Fail Open: Down)]：無効 (6.2 以降)	ドロップされる
	インラインセット、[Snortフェールオープン：ダウン (Snort Fail Open: Down)]：有効 (6.2+)	インスペクションなしで転送
	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

ASA FirePOWER アップグレード時の動作

Snort プロセスを再起動する特定の設定を展開する場合を含め、モジュールが FirePOWER ソフトウェアアップグレード中にトラフィックを処理する方法を決定する、ASA FirePOWER module へのトラフィック リダイレクトに関する ASA サービス ポリシーです。

表 9: 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 リダイレクト 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)	ドロップされる
モニタのみ (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 プロセスが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 Configuration Guide](#)』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 10: NGIPSv アップグレード中のトラフィックの動作

インターフェイスの設定	トラフィックの動作
インライン	ドロップされる
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 Configuration Guide](#)』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 11: NGIPSv 展開時のトラフィックの動作

インターフェイスの設定	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。

インターフェイスの設定	トラフィックの動作
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

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、次のいずれかを参照してください。

- [Cisco Firepower Management Center Upgrade Guide](#) : 管理対象デバイスや付随するオペレーティング システムを含む、FMC 展開のアップグレード
- [Cisco ASA Upgrade Guide](#) : ASDM を使用した ASA FirePOWER module のアップグレード
- [Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager](#) : FDM を使用した FTD のアップグレード

アップグレードパッケージ

アップグレードパッケージは、シスコ サポートおよびダウンロードサイトで入手できます。

- FMCv を含む Firepower Management Center : <https://www.cisco.com/go/firepower-software>
- Firepower Threat Defense (ISA 3000) : <https://www.cisco.com/go/isa3000-software>
- Firepower Threat Defense (FTDv を含む他のすべてのモデル) : <https://www.cisco.com/go/ftd-software>
- ASA with FirePOWER Services (ASA 5500-X シリーズ) : <https://www.cisco.com/go/asa-firepower-sw>
- ASA with FirePOWER Services (ISA 3000) : <https://www.cisco.com/go/isa3000-software>
- NGIPSv : <https://www.cisco.com/go/ngipsv-software>

署名付きの (.tar) パッケージは解凍しないでください。

Table 12: のアップグレード パッケージ バージョン 6.5.0.x

プラットフォーム	パッケージ
FMC/FMCv	Cisco_Firepower_Mgmt_Center_Patch-version-build.sh.REL.tar
Firepower 1000 シリーズ	Cisco_FTD_SSP_FP1K_Patch-version-build.sh.REL.tar

プラットフォーム	パッケージ
Firepower 2100 シリーズ	Cisco_FTD_SSP_FP2K_Patch-version-build.sh.REL.tar
Firepower 4100/9300 シャーシ	Cisco_FTD_SSP_Patch-version-build.sh.REL.tar
FTD を搭載した ASA 5500-X シリーズ	Cisco_FTD_Patch-version-build.sh.REL.tar
FTD を搭載した ISA 3000	
Firepower Threat Defense 仮想	
ASA FirePOWER	Cisco_Network_Sensor_Patch-version-build.sh.REL.tar
NGIPSv	Cisco_Firepower_NGIPS_Virtual_Patch-version-build.sh.REL.tar