



## Version6.2.3.x へのアップグレード

この章では、重要なリリースに固有の情報を提供します。

- [Firepower ソフトウェアのアップグレードガイドラインについて \(1 ページ\)](#)
- [Version6.2.3.xパッチのガイドライン \(2 ページ\)](#)
- [一般的なガイドライン \(4 ページ\)](#)
- [アップグレードする最小バージョン \(9 ページ\)](#)
- [時間テストとディスク容量の要件 \(9 ページ\)](#)
- [トラフィック フロー、検査、およびデバイス動作 \(21 ページ\)](#)
- [アップグレード手順 \(30 ページ\)](#)
- [アップグレードパッケージ \(31 ページ\)](#)

## Firepowerソフトウェアのアップグレードガイドラインについて

便宜上、このリリースノートでは、過去の Firepower ソフトウェアリリースの廃止機能とバージョン固有のアップグレードガイドラインが重複しています。ただし、対象バージョンのリリースノート、およびスキップするその他のメジャーリリースまたはメンテナンスリリースのリリースノートを必ずお読みください。



### 重要

アップグレードガイドラインは複数の場所に表示できます。このチェックリストを使用して、すべてを確認してください。

表 1: Firepower ソフトウェアのアップグレードガイドラインのインデックス

✓	リソース	詳細
	<a href="#">Version6.2.3.xパッチのガイドライン (2 ページ)</a>	新規またはこのリリースに固有の重要なアップグレードガイドラインについては、これらを参照してください。

✓	リソース	詳細
	<a href="#">一般的なガイドライン</a> (4 ページ)	ガイドラインが変更されている可能性があるため、アップグレードプロセスに精通している場合でも、これらをお読みください。
	<a href="#">既知の問題</a>	パッチの既知の問題はリスト化されていませんが、 <a href="#">Cisco バグ検索ツール</a> を使用して、Firepower 製品の未解決のバグの最新リストを取得できます。
	<a href="#">特長と機能</a>	パッチには、機能、および緊急の問題または解決済みの問題に関連する動作の変更のみが含まれていますが、この章を確認することをお勧めします。廃止された機能では、特別にアップグレード前の構成変更が必要になる場合があります。

## Version6.2.3.xパッチのガイドライン

このチェックリストには、バージョン 6.2.3 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 6.2.3.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
	<a href="#">CC モードが有効になっているバージョン 6.2.3.10 FTD にアップグレードすると FSIC 障害が発生</a> (3 ページ)	FTD	6.2.3 ~ 6.2.3.9	6.2.3.10 のみ
	<a href="#">バージョン 6.2.3.3 FTD デバイスをローカル管理に切り替えることは不可</a> (3 ページ)	FMC を使用した FTD	6.2.3 ~ 6.2.3.2	6.2.3.3
	<a href="#">アップグレードにより CSSM から FTD/FDM を登録解除することが可能</a> (3 ページ)	FDM を使用した FTD	6.2.3 ~ 6.2.3.1	6.2.3.2 ~ 6.2.3.5
	<a href="#">バージョン 6.2.3 ~ 88 FMC をアップグレードする前のホットフィックス</a> (4 ページ)	FMC	6.2.3-88	6.2.3.1 ~ 6.2.3.3

## CC モードが有効になっているバージョン 6.2.3.10 FTD にアップグレードすると FSIC 障害が発生

展開 : Firepower Threat Defense

アップグレード元 : バージョン 6.2.3 ~ 6.2.3.9

直接アップグレード先 : バージョン 6.2.3.10 のみ

既知の問題 : [CSCvo39052](#)

CC モードを有効にして FTD デバイスをバージョン 6.2.3.10 にアップグレードすると、デバイスの再起動時に FSIC（ファイル システム整合性チェック）が失敗します。



### 注意

セキュリティ認定準拠が有効な場合に FSIC が失敗すると、Firepower ソフトウェアは起動せず、リモート SSH アクセスが無効になり、ローカルコンソールを介してのみアプライアンスにアクセスできます。この問題が発生した場合は、Cisco TAC にお問い合わせください。

FTD の展開にセキュリティ認定コンプライアンス（CC モード）が必要な場合は、バージョン 6.2.3.13 以降に直接アップグレードすることをお勧めします。Firepower 4100/9300 デバイスの場合は、FXOS 2.3.1.130+ にアップグレードすることも推奨します。

## バージョン 6.2.3.3 FTD デバイスをローカル管理に切り替えることは不可

展開 : FMC を使用した FTD

アップグレード元 : バージョン 6.2.3 ~ 6.2.3.2

直接アップグレード先 : バージョン 6.2.3.3 のみ

バージョン 6.2.3.3 では、Firepower Threat Defense デバイスの管理を FMC から FDM に切り替えることはできません。この問題は、バージョン 6.2.3.3 パッチをアンインストールしても発生します。この時点でローカル管理に切り替える場合は、バージョン 6.2.3 を新しくインストールするか、Cisco TAC にお問い合わせください。

この問題を回避するには、6.2.3.3 のバージョンにアップグレードする前に管理を切り替えます。または、最新パッチにアップグレードします。管理を切り替えると、デバイス構成は失われます。

バージョン 6.2.3.3 では、FDM から FMC への管理の切り替えが可能であることに注意してください。

## アップグレードにより CSSM から FTD/FDM を登録解除することが可能

展開 : FDM を使用した FTD

アップグレード元 : バージョン 6.2.3 または 6.2.3.1

直接アップグレード先 : 6.2.3.2 ~ 6.2.3.5

Firepower Device Manager によって管理されている Firepower Threat Defense デバイスをアップグレードすると、そのデバイスが Cisco Smart Software Manager から登録解除される場合があります。アップグレードが完了したら、ライセンスのステータスを確認します。

**ステップ 1** [デバイス (Device)] をクリックし、[スマートライセンス概要 (Smart License summary)] の [設定の表示 (View Configuration)] をクリックします。

**ステップ 2** デバイスが登録されていない場合は、[デバイスの登録 (Register Device)] をクリックします。

## バージョン 6.2.3 ~ 88 FMC をアップグレードする前のホットフィックス

展開 : FMC

アップグレード元 : バージョン 6.2.3 ~ 88

直接アップグレード先 : バージョン 6.2.3.1、バージョン 6.2.3.2、またはバージョン 6.2.3.3

シスコは、Firepower のアップグレードパッケージの更新版ビルドを適宜リリースしています。バージョン 6.2.3 ~ 88 は、それ以降のビルドに置き換えられています。バージョン 6.2.3 ~ 88 を実行している FMC をバージョン 6.2.3.1、バージョン 6.2.3.2、またはバージョン 6.2.3.3 にアップグレードすると、SSE クラウド接続が継続的にドロップし、エラーが生成されます。パッチをアンインストールしても、この問題は解決しません。

バージョン 6.2.3 ~ 88 を実行している場合は、アップグレードの前に [ホットフィックス T](#) をインストールします。

## 一般的なガイドライン

これらの一般的なガイドラインは、すべてのアップグレードに適用されます。

### アプライアンスの正常性と通信

アップグレードプロセスの間、展開環境内のアプライアンスが正常に通信していること、およびヘルスマニタによって報告された問題がないことを確認します。マイナーな問題がメジャーな問題になる前に解決します。

### 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。

### アップグレード前のチェックリスト

このチェックリストは、一般的なアップグレードの問題を回避できるアクションを示しています。ただし、このリストは包括的なものではありません。詳細な手順については、該当するアップグレードガイド（「[アップグレード手順（30 ページ）](#)」）を参照してください。

表 3: Firepower ソフトウェアのアップグレード前チェックリスト

✓	アクション	詳細
	導入評価。	<p>FirePOWER アプライアンスをアップグレードする前に、展開の現在の状態を判断します。状況を理解することにより、目的を達成する方法を決定します。</p> <p>少なくとも次の項目に回答できる必要があります。</p> <ul style="list-style-type: none"> <li>• どんなアプライアンスがありますか、またどの FirePOWER バージョンを実行していますか。どのバージョンを実行したいですか、またそのバージョンは実行可能ですか。直接アップグレードできますか。FMC 展開では、FMC デバイスの互換性を維持できますか。</li> <li>• アプライアンスのいずれかで個別のオペレーティングシステムのアップグレードが必要ですか。ホスティング環境のアップグレードを必要とする仮想アプライアンスはありますか。</li> <li>• ハイアベイラビリティ/スケーラビリティを実現するように設定されていますか。デバイスは、IPS として、ファイアウォールとして、パッシブに展開されていますか。</li> </ul>

✓	アクション	詳細
	管理ネットワークの帯域幅を確認します。	<p>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。</p> <p>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ったりす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。</p> <p>『<a href="#">Guidelines for Downloading Data from the Firepower Management Center to Managed Devices</a>』（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。</p>
	アプライアンスへのアクセスを確認します。	<p>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。FMC の展開では、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。</p>
	設定変更を計画します。	<p>主要なアップグレードでは特に、アップグレードの前または後に、アップグレードにより重要な設定変更が発生することがあります。たとえば、廃止された FlexConfig コマンドは、アップグレード後の展開の問題を引き起こす可能性があります。</p> <p>「<a href="#">Firepower ソフトウェアのアップグレードガイドラインについて (1 ページ)</a>」のチェックリストを使用して、潜在的な問題を特定します。</p>

✓	アクション	詳細
	バックアップを実行します。	<p>アップグレードの前後に Firepower アプライアンスをバックアップします（サポートされている場合）。</p> <ul style="list-style-type: none"> <li>• アップグレード前：アップグレードが致命的な失敗であった場合は、再イメージ化を実行し、復元する必要がある場合があります。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。</li> <li>• 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。</li> </ul> <p><b>注意</b> Firepower アプライアンスを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ことを強くお勧めします。アプライアンスに残っているバックアップは、手動またはアップグレードプロセスによって削除できます（アップグレードプロセスでは、ローカルに保存されたバックアップが消去される）。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。</p> <p>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、セキュリティやライセンス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。</p>
	準備状況チェックを実行します。	FMC 展開では、準備状況チェックをお勧めします。このチェックにより、Firepower をアップグレードするためのアプライアンスの準備状況を評価できます。このチェックにより、データベース整合性、バージョン不一致、デバイス登録などの問題を識別できます。

✓	アクション	詳細
	アップグレードをスケジュール設定します。1007	<p>アップグレードのスケジュール設定は、中断による展開環境への影響が最も小さい時間に行うことを推奨します。</p> <p>メンテナンスウィンドウをスケジュールするときは、トラフィックフローおよびインスペクションへの影響と、アップグレードにかかる可能性がある時間を考慮します。また、ウィンドウで実行する必要があるタスクと、事前に実行できるタスクを検討します。慎重な計画と準備で中断を最小限に抑えます。メンテナンスウィンドウがアップグレードパッケージの取得およびプッシュ、準備状況チェックの実行、バックアップの作成などを行うまで待機しないようにします。</p>
	NTP 同期を確認します。	<p>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もあります。</p> <p>時刻を確認するには、次の手順を実行します。</p> <ul style="list-style-type: none"> <li>• FMC : [システム (System)] &gt; [設定 (Configuration)] &gt; [時刻 (Time)] を選択します。</li> <li>• デバイス : <b>show time</b> CLI コマンドを使用します。</li> </ul>
	ASA FirePOWER デバイスで ASA REST API を無効化します。	<p>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。</p> <p>ASA FirePOWER モジュール (6.0+) も実行している場合、ASA 5506-X シリーズデバイスは ASA REST API をサポートしないことに注意してください。</p>
	設定を展開します。	<p>アップグレードする前に古いデバイスに設定を展開すると、失敗する可能性が減少します。</p> <p>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、いくつかの設定を展開することで Snort が再起動されます。これにより、トラフィックのインスペクションが中断し、デバイスのトラフィックの処理方法によっては、再起動が完了するまでトラフィックが中断する場合があります。詳細については、<a href="#">トラフィックフロー、検査、およびデバイス動作 (21 ページ)</a> を参照してください。</p>



✓	アクション	詳細
	実行中のタスクを確認します。	アップグレードする前に、重要なタスクが完了していることを確認します。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。  また、アップグレード中に実行するようにスケジュールされたタスクを確認し、それらをキャンセルまたは延期することをお勧めします。
	ディスク容量を確認します。	最終的なディスク容量のチェックを実行します。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。詳細については、 <a href="#">時間テストとディスク容量の要件</a> （9 ページ）を参照してください。

## 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。

したがって、バージョン 6.2.3.x にアップグレードするには、バージョン 6.2.3 以降を実行している必要があります。



(注) FTD を使用する Firepower 4100/9300 シャーシの場合、Firepower 6.2.3.16 以上には FXOS 2.3.1.157 以降のビルドが必要です。最初に FXOS をアップグレードします。

## 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：構成とトラフィック負荷が最小限のアプライアンスでテストします。

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。

- リブート（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。

## バージョン 6.2.3.16 の時間とディスク容量

表 4: バージョン 6.2.3.16 の時間とディスク容量

Platform	ボリュームの容量	必要容量	FMC の容量	6.2.3からのアップグレード時間	リブート時間
FMC	3.6 GB	250 MB	—	40 分	9 分
FMCv : VMware 6.0	3.3 GB	220 MB	—	25 分	4 分
Firepower 2100 シリーズ	2.6 GB	2.6 GB	620 MB	11 分	12 分
Firepower 4100 シリーズ	1.7 GB	1.7 GB	410 MB	5 分	5 分
Firepower 9300	1.8 GB	1.8 GB	410 MB	5 分	9 分
ASA 5500-X シリーズ with FTD	2 GB	200 MB	430 MB	18 分	33 分
FTDv : VMware 6.0	2 GB	190 MB	430 MB	8 分	5 分
Firepower 7000/8000 シリーズ	3.5 GB	200 MB	670 MB	31 分	14 分
ASA FirePOWER	3.8 GB	58 MB	600 MB	74 分	77 分
NGIPSv : VMware 6.0	2.3 GB	180 MB	500 MB	6 分	4 分

## バージョン 6.2.3.15 の時間とディスク容量

表 5: バージョン 6.2.3.15 の時間とディスク容量

Platform	ボリュームの容量	必要容量	FMC の容量	6.2.3からの時間
FMC	4.7 GB	260 MB	—	50 分
FMCv : VMware 6.0	4.7 GB	210 MB	—	ハードウェアによって異なる

Platform	ボリュームの容量	必要容量	FMC の容量	6.2.3 からの時間
Firepower 2100 シリーズ	2.3 GB	2.3 GB	590 MB	27 分
Firepower 4100 シリーズ	1.7 GB	1.7 GB	390 MB	10 分
Firepower 9300	2.4 GB	2.4 GB	390 MB	11 分
ASA 5500-X シリーズ with FTD	2 GB	190 MB	410 MB	38 分
FTDv : VMware 6.0	2.4 GB	190 MB	410 MB	ハードウェアによって異なる
Firepower 7000/8000 シリーズ	3.5 GB	210 MB	640 MB	19 分
ASA FirePOWER	3.9 GB	56 MB	580 MB	100 分
NGIPSv : VMware 6.0	2.7 GB	180 MB	470 MB	ハードウェアによって異なる

## バージョン 6.2.3.14 の時間とディスク容量

表 6: バージョン 6.2.3.14 の時間とディスク容量

Platform	ボリュームの容量	必要容量	FMC の容量	6.2.3 からの時間
FMC	4.5 GB	260 MB	—	58 分
FMCv : VMware 6.0	4.7 GB	190 MB	—	ハードウェアによって異なる
Firepower 2100 シリーズ	1.9 GB	1.9 GB	590 MB	23 分
Firepower 4100 シリーズ	1.7 GB	1.7 GB	390 MB	11 分
Firepower 9300	1.7 GB	1.7 GB	390 MB	10 分
ASA 5500-X シリーズ with FTD	2 GB	200 MB	410 MB	32 分
FTDv : VMware 6.0	2.4 GB	190 MB	410 MB	ハードウェアによって異なる
Firepower 7000/8000 シリーズ	3.4GB	200 MB	630 MB	19 分
ASA FirePOWER	3.7 GB	53 MB	560 MB	106 分

Platform	ボリュームの容量	必要容量	FMC の容量	6.2.3 からの時間
NGIPSv : VMware 6.0	2.6 GB	190 MB	470 MB	ハードウェアによって異なる

## バージョン 6.2.3.13 の時間とディスク容量

表 7: バージョン 6.2.3.13 の時間とディスク容量

Platform	ボリュームの容量	必要容量	FMC の容量	6.2.3 からの時間
FMC	4.7 GB	290 MB	—	50 分
FMCv : VMware 6.0	4.6 GB	190 MB	—	ハードウェアによって異なる
Firepower 2100 シリーズ	2.6 GB	2.6 GB	590 MB	25 分
Firepower 4100 シリーズ	1.7 GB	1.7 GB	390 MB	11 分
Firepower 9300	1.8 GB	1.8 GB	390 MB	11 分
ASA 5500-X シリーズ with FTD	2.4 GB	190 MB	410 MB	32 分
FTDv : VMware 6.0	2.3 GB	190 MB	410 MB	ハードウェアによって異なる
Firepower 7000/8000 シリーズ	3.8 GB	190 MB	620 MB	18 分
ASA FirePOWER	3.7 GB	51 MB	560 MB	105 分
NGIPSv : VMware 6.0	2.6 GB	180 MB	470 MB	ハードウェアによって異なる

## バージョン 6.2.3.12 の時間とディスク容量

表 8: バージョン 6.2.3.12 の時間とディスク容量

Platform	ボリュームの容量	必要容量	FMC の容量	6.2.3 からの時間
FMC	3.9 GB	220 MB	—	49 分
FMCv : VMware 6.0	4.6 GB	160 MB	—	ハードウェアによって異なる

Platform	ボリュームの容量	必要容量	FMC の容量	6.2.3 からの時間
Firepower 2100 シリーズ	1.9 GB	1.9 GB	390 MB	21 分
Firepower 4100 シリーズ	970 MB	970 MB	190 MB	14 分
Firepower 9300	1.7 GB	1.7 GB	190 MB	11 分
ASA 5500-X シリーズ with FTD	1.4 GB	96 MB	210 MB	30 分
FTDv : VMware 6.0	2.4 GB	200 MB	210 MB	ハードウェアによって異なる
Firepower 7000/8000 シリーズ	3.6 GB	160 MB	540 MB	19 分
ASA FirePOWER	3.5 GB	31 MB	480 MB	104 分
NGIPSv : VMware 6.0	2.6 GB	130 MB	400 MB	ハードウェアによって異なる

## バージョン 6.2.3.11 の時間とディスク容量

表 9: バージョン 6.2.3.11 の時間とディスク容量

Platform	ボリュームの容量	必要容量	FMC の容量	6.2.3 からの時間
FMC	4.5 GB	250 MB	—	39 分
FMCv : VMware 6.0	4.6 GB	35 MB	—	ハードウェアによって異なる
Firepower 2100 シリーズ	2.8 GB	2.8 GB	590 MB	40 分
Firepower 4100 シリーズ	2 GB	2 GB	380 MB	10 分
Firepower 9300	1.6 GB	1.6 GB	380 MB	11 分
ASA 5500-X シリーズ with FTD	1.8 GB	230 MB	410 MB	33 分
FTDv : VMware 6.0	2.2 GB	230 MB	410 MB	ハードウェアによって異なる
Firepower 7000/8000 シリーズ	3.3 GB	170 MB	600 MB	23 分
ASA FirePOWER	3.6 GB	50 MB	530 MB	110 分

Platform	ボリュームの容量	必要容量	FMC の容量	6.2.3 からの時間
NGIPSv : VMware 6.0	2.6 GB	130 MB	450 MB	ハードウェアによって異なる

## バージョン 6.2.3.10 の時間とディスク容量

表 10: バージョン 6.2.3.10 の時間とディスク容量

Platform	ボリュームの容量	必要容量	FMC の容量	6.2.3 からの時間
FMC	4.2 GB	200 MB	—	40 分
FMCv	4.5 GB	230 MB	—	ハードウェアによって異なる
Firepower 2100 シリーズ	1.8 GB	1.8 GB	390 MB	21 分
Firepower 4100/9300 シャーシ	1.3 GB	1.3 GB	190 MB	11 分
ASA 5500-X シリーズ with FTD	1.3 GB	140 MB	210 MB	25 分
FTDv	1.6 GB	140 MB	210 MB	ハードウェアによって異なる
Firepower 7000/8000 シリーズ	3.2 GB	190 MB	560 MB	25 分
ASA FirePOWER	3.4GB	31 MB	480 MB	100 分
NGIPSv	2.1 GB	160 MB	400 MB	ハードウェアによって異なる

## バージョン 6.2.3.9 の時間とディスク容量

表 11: バージョン 6.2.3.9 の時間とディスク容量

Platform	ボリュームの容量	必要容量	FMC の容量	6.2.3 からの時間
FMC	3630 MB	190 MB	—	35 分
FMCv	3596 MB	172 MB	—	ハードウェアによって異なる

Platform	ボリュームの容量	必要容量	FMC の容量	6.2.3 からの時間
Firepower 2100 シリーズ	1677 MB	1677 MB	385 MB	21 分
Firepower 4100/9300 シャーシ	779 MB	779 MB	184 MB	9 分
ASA 5500-X シリーズ with FTD	1105 MB	130 MB	206 MB	12 分
ISA 3000 with FTD	1071 MB	130 MB	206 MB	25 分
FTDv	1094 MB	130 MB	206 MB	ハードウェアによって異なる
Firepower 7000/8000 シリーズ	2975 MB	161 MB	538 MB	30 分
ASA FirePOWER	3211 MB	27 MB	462 MB	38 分
NGIPSv	1883 MB	146 MB	378 MB	ハードウェアによって異なる

## バージョン 6.2.3.8 の時間とディスク容量

バージョン 6.2.3.8 は 2019 年 1 月 7 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 6.2.3.7 の時間とディスク容量

表 12: バージョン 6.2.3.7 の時間とディスク容量

Platform	ボリュームの容量	必要容量	FMC の容量	6.2.3 からの時間
FMC	2909 MB	137 MB	—	25 分
FMCv	3972 MB	211 MB	—	ハードウェアによって異なる
Firepower 2100 シリーズ	1668 MB	1668 MB	384 MB	19 分
Firepower 4100/9300 シャーシ	795 MB	795 MB	183 MB	8 分
ASA 5500-X シリーズ with FTD	1067 MB	130 MB	205 MB	9 分
ISA 3000 with FTD	1080 MB	130 MB	205 MB	20 分



Platform	ボリュームの容量	必要容量	FMC の容量	6.2.3 からの時間
FTDv	1146 MB	130 MB	205 MB	ハードウェアによって異なる
Firepower 7000/8000 シリーズ	3300 MB	136 MB	477 MB	20 分
ASA FirePOWER	2291 MB	26 MB	411 MB	80 分
NGIPSv	1588 MB	121 MB	327 MB	ハードウェアによって異なる

## バージョン 6.2.3.6 の時間とディスク容量

表 13: バージョン 6.2.3.6 の時間とディスク容量

Platform	ボリュームの容量	必要容量	FMC の容量	6.2.3 からの時間
FMC	2524 MB	47 MB	—	30 分
FMCv	2315 MB	101 MB	—	ハードウェアによって異なる
Firepower 2100 シリーズ	1673 MB	1673 MB	383 MB	10 分
Firepower 4100/9300 シャーシ	790 MB	790 MB	182 MB	17 分
ASA 5500-X シリーズ with FTD	1220 MB	130 MB	205 MB	21 分
ISA 3000 with FTD	1087 MB	130 MB	205 MB	21 分
FTDv	1133 MB	130 MB	205 MB	ハードウェアによって異なる
Firepower 7000/8000 シリーズ	1196 MB	17 MB	204 MB	30 分
ASA FirePOWER	1844 MB	16 MB	226 MB	106 分
NGIPSv	364 MB	17 MB	142 MB	ハードウェアによって異なる

## バージョン 6.2.3.5 の時間とディスク容量

表 14: バージョン 6.2.3.5 の時間とディスク容量

Platform	ボリュームの容量	必要容量	FMC の容量	6.2.3 からの時間
FMC	1566 MB	24 MB	—	28 分
FMCv	2266 MB	80 MB	—	ハードウェアによって異なる
Firepower 2100 シリーズ	1001 MB	1001 MB	257 MB	20 分
Firepower 4100/9300 シャーシ	370 MB	370 MB	56 MB	7 分
ASA 5500-X シリーズ with FTD	587 MB	130 MB	78 MB	20 分
ISA 3000 with FTD	379 MB	130 MB	78 MB	20 分
Firepower 7000/8000 シリーズ	806 MB	17 MB	78 MB	22 分
ASA FirePOWER	1465 MB	15 MB	100 MB	70 分
NGIPSv	120 MB	17 MB	16 MB	ハードウェアによって異なる

## バージョン 6.2.3.4 の時間とディスク容量

表 15: バージョン 6.2.3.4 の時間とディスク容量

Platform	ボリュームの容量	必要容量	FMC の容量	6.2.3 からの時間
FMC	2191 MB	107 MB	—	80 分
FMCv	1760 MB	35 MB	—	ハードウェアによって異なる
Firepower 2100 シリーズ	1014 MB	1014 MB	261 MB	17 分
Firepower 4100/9300 シャーシ	334 MB	334 MB	59 MB	7 分
ASA 5500-X シリーズ with FTD	411 MB	128 MB	82 MB	20 分

Platform	ボリュームの容量	必要容量	FMC の容量	6.2.3 からの時間
ISA 3000 with FTD	393 MB	128 MB	82 MB	20 分
FTDv	411 MB	128 MB	82 MB	ハードウェアによって異なる
Firepower 7000/8000 シリーズ	800 MB	17 MB	82 MB	23 分
ASA FirePOWER	1385 MB	15 MB	103 MB	25 分
NGIPSv	191 MB	17 MB	20 MB	ハードウェアによって異なる

## バージョン 6.2.3.3 の時間とディスク容量

表 16: バージョン 6.2.3.3 の時間とディスク容量

Platform	ボリュームの容量	必要容量	FMC の容量	6.2.3 からの時間
FMC	1879 MB	88 MB	—	26 分
FMCv	2093 MB	90 MB	—	ハードウェアによって異なる
Firepower 2100 シリーズ	987 MB	987 MB	255 MB	15 分
Firepower 4100/9300 シャーシ	313 MB	313 MB	54 MB	5 分
ASA 5500-X シリーズ with FTD	553 MB	128 MB	77 MB	16 分
ISA 3000 with FTD	307 MB	90 MB	77 MB	15 分
FTDv	307 MB	90 MB	77 MB	ハードウェアによって異なる
Firepower 7000/8000 シリーズ	825 MB	17 MB	77 MB	15 分
ASA FirePOWER	634 MB	16 MB	98 MB	40 分
NGIPSv	102 MB	17 MB	77 MB	ハードウェアによって異なる

## バージョン 6.2.3.2 の時間とディスク容量

表 17: バージョン 6.2.3.2 の時間とディスク容量

Platform	ボリュームの容量	必要容量	FMC の容量	6.2.3 からの時間
FMC	1743 MB	27 MB	—	24 分
FMCv	1976 MB	70 MB	—	ハードウェアによって異なる
Firepower 2100 シリーズ	977 MB	977 MB	252 MB	17 分
Firepower 4100/9300 シャーシ	374 MB	374 MB	51 MB	4 分
ASA 5500-X シリーズ with FTD	585 MB	126 MB	73 MB	16 分
ISA 3000 with FTD	676 MB	126 MB	73 MB	17 分
FTDv	585 MB	126 MB	73 MB	ハードウェアによって異なる
Firepower 7000/8000 シリーズ	688 MB	11 MB	76 MB	13 分
ASA FirePOWER	1440 MB	15 MB	98 MB	40 分
NGIPSv	96 MB	17 MB	14 MB	ハードウェアによって異なる

## バージョン 6.2.3.1 の時間とディスク容量

表 18: バージョン 6.2.3.1 の時間とディスク容量

Platform	ボリュームの容量	必要容量	FMC の容量	6.2.3 からの時間
FMC	1361.8 MB	59.67 MB	—	25 分
FMCv	1240.8 MB	40.8 MB	—	ハードウェアによって異なる
Firepower 2100 シリーズ	948.3 MB	948.3 MB	246 MB	81 分
Firepower 4100/9300 シャーシ	278 MB	278 MB	45 MB	8 分

Platform	ボリュームの容量	必要容量	FMC の容量	6.2.3 からの時間
ASA 5500-X シリーズ with FTD	275.5 MB	89.9 MB	68 MB	16 分
ISA 3000 with FTD	343.4 MB	127.5 MB	68 MB	15 分
FTDv	275.5 MB	89.9 MB	67 MB	ハードウェアによって異なる
Firepower 7000/8000 シリーズ	99.8 MB	36 MB	10 MB	19 分
ASA FirePOWER	867.9 MB	15.45 MB	32 MB	60 分
NGIPSv	101.9 MB	17.18 MB	9 MB	ハードウェアによって異なる

## 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 9300 シャーシ

このセクションでは、FTD を搭載した Firepower 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 9300 シャーシ : 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 19: FXOS アップグレード中のトラフィックの動作

導入	方法	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 FTD デバイス : Firepower ソフトウェアのアップグレード

アップグレード中、Firepower デバイス/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 20: 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 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、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、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、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、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、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。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。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プ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спекションで 2～3 秒のトラフィック中断が発生します。

## 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 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 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 21: FTD 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
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）。
	インラインセット、[Snort Fail Open: Down]：無効（6.2 以降）	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]：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。

## 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

アップグレード中、Firepower 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спек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 22: 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 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	<p>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。</p> <p>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。</p>	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、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。

### 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 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 23: FTD 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
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。

## 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 24: 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

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 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 25: 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 26: 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

## 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 27: Firepower アップグレード手順

タスク	ガイド
FMC 展開のアップグレード。	<a href="#">Cisco Firepower Management Center Upgrade Guide</a>
FDM を使用した Firepower Threat Defense ソフトウェアのアップグレード。	<a href="#">Firepower Device Manager 用 Cisco Firepower Threat Defense 構成ガイド</a> 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 FTD バージョンのガイドの「システム管理」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。	<a href="#">Cisco Firepower 4100/9300 Upgrade Guide</a>
ASDM を使用した ASA FirePOWER モジュールのアップグレード。	<a href="#">Cisco ASA Upgrade Guide</a>

タスク	ガイド
ISA 3000、ASA 5506-X、5508-X、および 5516-X での ROMMON イメージのアップグレード。	<a href="#">Cisco ASA and Firepower Threat Defense Reimage Guide</a> 「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。

## 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>
- NGIPSv : <https://www.cisco.com/go/ngipsv-software>

Firepower ソフトウェアアップグレードパッケージを検索するには、Firepower アプライアンスモデルを選択または検索し、現在のバージョンの Firepower ソフトウェアのダウンロードページを参照します。使用可能なアップグレードパッケージは、インストールパッケージ、ホットフィックス、およびその他の該当するダウンロードとともに表示されます。



**ヒント** インターネットにアクセスできる FMC は、手動でダウンロードできるようになってから約 2 週間後に、シスコからバージョン 6.2.3.x ~ 6.5.0.x Firepower パッチを直接ダウンロードできます。次の場合、シスコからの直接ダウンロードはサポートされていません。

- メジャーリリース。
- バージョン 6.6 以降へのほとんどのパッチ。
- FDM または ASDM 展開。

ファミリまたはシリーズのすべての Firepower モデルに同じアップグレードパッケージを使用します。アップグレードパッケージのファイル名には、プラットフォーム、パッケージタイプ（アップグレード、パッチ、ホットフィックス）、および Firepower のバージョンが反映されています。

次に例を示します。

- パッケージ : Cisco\_Firepower\_Mgmt\_Center\_Patch-6.6.0.1-7.sh.REL.tar

- プラットフォーム：Firepower Management Center
- パッケージタイプ：パッチ
- バージョンおよびビルド：6.6.0.1 ～ 7
- ファイル拡張子：sh.REL.tar

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、バージョン 6.2.1 以上からのアップグレードパッケージは、署名付きの tar アーカイブ（.tar）になっています。以前のバージョンからのアップグレードでは、引き続き未署名のパッケージが使用されます。

シスコサポートおよびダウンロードサイトからアップグレードパッケージを手動でダウンロードする場合（たとえば、メジャーアップグレードやエアギャップ展開のために）、正しいパッケージをダウンロードしていることを確認してください。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。

表 28: Firepower ソフトウェア アップグレードパッケージ

プラットフォーム	パッケージ
FMC/FMCv	Sourcefire_3D_Defense_Center_S3
Firepower 2100 シリーズ	Cisco_FTD_SSP-FP2K
Firepower 4100/9300 シャーシ	Cisco_FTD_SSP
FTD を搭載した ASA 5500-X シリーズ	Cisco_FTD
FTD を搭載した ISA 3000	
FTDv	
ASA FirePOWER	Cisco_Network_Sensor
NGIPSv	Sourcefire_3D_Device_VMware

### オペレーティングシステムのアップグレードパッケージ

オペレーティングシステムのアップグレードパッケージの詳細については、次のガイドの「アップグレードの計画」の章を参照してください。

- [Cisco ASA Upgrade Guide](#)（ASA OS の場合）
- [Cisco Firepower 4100/9300 Upgrade Guide](#)（FXOS の場合）