Version6.2.3 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

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
	Version6.2.3のガイドライン （2 ページ）	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。
	以前に公開されたガイドライン （6 ページ）	アップグレードでバージョンがスキップされる場合は、これらを参照してください。
	一般的なガイドライン （9 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。
	既知の問題	これらを読み、アップグレードに影響するバグを回避する準備を整えます。 アップグレードでバージョンがスキップされる場合は、スキップするメジャーバージョンの既知の問題も参照してください。「Cisco Firepower リリース ノート」を参照してください。
	特長と機能	アップグレードに影響する可能性のあるその他の項目については、これらをお読みください。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。 アップグレードでバージョンがスキップされる場合は、スキップしたバージョンの新機能に関するドキュメントもお読みください。「Cisco Firepower リリース ノート」を参照してください。

Version6.2.3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 の新規または固有のアップグレードガイドラインが含まれています。現在**バージョン 6.1.0 ～ 6.2.2** を実行している場合は、次のガイドラインを確認してください。

表 *2 :* バージョン *6.2.3* の新しいガイドライン

✓	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
	シスコとのデータの共有 （3 ページ）	いずれか（Any）	いずれか（Any）	6.2.3 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
	アップグレードの失敗：Firepower 2100 シリーズのバージョン 6.2.2.5 から （4 ページ）	FDM を使用した Firepower 2100 シリーズ	6.2.2.5	6.2.3 のみ
	FTD/FDM のアップグレード後にレルムを編集/再保存 （4 ページ）	FDM を使用した FTD	6.2.0 ～ 6.2.2.x	6.2.3 のみ
	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 （5 ページ）	FDM を使用した FTD	6.2.0 ～ 6.2.2.x	6.2.3 ～ 6.4.0
	アップグレード後にアクセス コントロール ポリシーを編集/再保存する （5 ページ）	任意	6.1.0 ～ 6.2.2.x	6.2.3 のみ
	レポートの結果の制限の変更 （5 ページ）	FMC	6.1.0 ～ 6.2.2.x	6.2.3 ～ 6.4.0
	アップグレードの前にバージョン 6.1.x FTD クラスタからサイト ID を削除 （6 ページ）	FTD クラスタ	6.1.0.x	6.2.3 ～ 6.4.0

シスコとのデータの共有

展開：すべて

アップグレード元：バージョン 6.1.0+

直接アップグレード先：バージョン 6.2.3+

一部の機能にシスコとのデータ共有が含まれます。

Cisco Success Network

バージョン 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。

初期設定および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。

Web 分析トラッキング

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。

Web 分析トラッキングはデフォルトでオンになっています（バージョン 6.5.0 以降の EULA に承諾すると、Web 分析トラッキングに同意したことになります）。ただし、初期設定の完了後にいつでもオプトアウトできます。

（注） バージョン 6.2.3 から 6.6.x へのアップグレードでは、Web 分析トラッキングを有効化（または再有効化）できます。これは、現在の設定がオプトアウトであっても発生する可能性があります。このデータの収集を拒否する場合は、アップグレードの後にオプトアウトしてください。

Cisco Support Diagnostics

バージョン 6.5.0 以降では、 *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 TACTAC 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。

初期設定および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。

アップグレードの失敗：Firepower 2100 シリーズのバージョン 6.2.2.5 から

展開：FDM によって管理される、FTD を使用した Firepower 2100 シリーズ

アップグレード元：バージョン 6.2.2.5

直接アップグレード先：バージョン 6.2.3 のみ

バージョン 6.2.2.5 を実行している Firepower 2100 シリーズ デバイスで DNS 設定を変更した後に、中間展開なしでバージョン 6.2.3 にアップグレードすると、アップグレードに失敗します。デバイスをアップグレードする前に、展開するか、展開をトリガーするアクション（SRU アップデートなど）を実行する必要があります。

FTD/FDM のアップグレード後にレルムを編集/再保存

展開：FDM を使用した FTD

アップグレード元：バージョン 6.2.0 ～ バージョン 6.2.2.x

直接アップグレード先：バージョン 6.2.3 のみ

バージョン 6.2.3 以前では、ユーザは非アクティブ状態で 24 時間後に自動的にログアウトされませんでした。Firepower Device Manager を使用していて Firepower Threat Defense をバージョン 6.2.3 にアップグレードした後、アクティブ認証でアイデンティティ ポリシーを使用している場合、設定を展開する前にレルムを更新します。**[オブジェクト（Objects）]** > **[アイデンティ**

ティレルム（**Identity Realm**）**]** を選択し、レルムを編集して（変更は不要）、保存します。その後、展開します。

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 ～ 6.2.2.x

直接アップグレード先：バージョン 6.2.3 ～ 6.4.0

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。

アップグレード後にアクセス コントロール ポリシーを編集/再保存する

展開：すべて

アップグレード元：バージョン 6.1 ～ 6.2.2.x

直接アップグレード先：バージョン 6.2.3 のみ

侵入ポリシーの変数セットでのみ使用されるネットワークまたはポート オブジェクトを設定している場合、アップグレード後にアクセス コントロール ポリシーに関連付けられている展開が失敗します。これが発生する場合、アクセス コントロール ポリシーを編集し、（説明の編集などの）変更、保存、および再展開を行います。

レポートの結果の制限の変更

展開：Firepower Management Center

アップグレード元：バージョン 6.1.0 ～ 6.2.2.x

直接アップグレード先：バージョン 6.2.3 ～ 6.4.0

バージョン 6.2.3 では、次のように、使用できる結果の数、またはレポートのセクションに含めることができる結果の数が制限されています。テーブルおよび詳細ビューでは、PDF レポートに HTML または CSV レポートよりも少ないレコードを含めることができます。

表 *3:* レポートの結果の新しい制限

レポート セクション タイプ	最大レコード数：HTML または CSV レポート セクション	最大レコード数：PDF レポート セクション
棒グラフ 円グラフ	100（上位または下位）	100（上位または下位）
テーブル ビュー	400,000	100,000
詳細ビュー	1,000	500

Firepower Management Center をアップグレードする前に、レポート テンプレート内のセクションで最大 HTML または CSV よりも大きい結果数を指定する場合は、アップグレード プロセスが設定を新しい最大値に下げます。

PDF レポートを生成するレポート テンプレートの場合、テンプレート セクションの PDF の制限を超えると、アップグレード プロセスは出力形式を HTML に変更します。PDF の生成を続行するには、結果数を PDF の最大に下げます。アップグレード後にこれを行った場合、出力形式の設定を PDF に戻します。

アップグレードの前にバージョン6.1.xFTDクラスタからサイトIDを削除

展開： Firepower Threat Defenseクラスタ

アップグレード元：バージョン 6.1.x

直接アップグレード先：バージョン 6.2.3 ～ 6.4.0

Firepower Threat Defense バージョン 6.1.x クラスタは、サイト間クラスタリングをサポートしていません（バージョン 6.2.0 以降では FlexConfig を使用してサイト間機能を設定できます）。

FXOS 2.1.1 でバージョン 6.1.x クラスタを展開または再展開している場合、（サポートされていない）サイト ID の値を入力しているときは、アップグレードする前に、FXOS の各ユニットでサイト ID を削除（0 に設定）する必要があります。そうしないと、アップグレード後、ユニットがクラスタに再度参加できなくなります。

すでにアップグレード済みの場合は、サイト ID を各ユニットから削除してからクラスタを再確立します。サイト ID を表示または変更するには、『Cisco FXOS CLI Configuration Guide』を参照してください。

以前に公開されたガイドライン

このチェックリストには、中間リリースに適用されるアップグレードガイドラインが含まれています。現在**バージョン 6.1 ～ 6.2.1** を実行している場合は、次のガイドラインを確認してください。

表 *4 :* 以前に公開されたバージョン *6.2.3* のガイドライン

✓	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：FDM を実行する ASA 5500-X シリーズのバージョン 6.2.2.5 から （7 ページ）	FDM を使用した FTD	6.2.0 のみ	6.2.2 ～ 6.4.0
	アクセス コントロールではSRUから遅延ベースのパフォーマンス設定を取得可能 （7 ページ）	FMC	6.1.0.x	6.2.0 ～ 6.4.0
	FTD での「フェールセーフ」から「Snort フェール オープン」への置き換え （8 ページ）	FMC を使用した FTD	6.1.0.x	6.2.0 ～ 6.4.0

アップグレードの失敗：FDM を実行する ASA 5500-X シリーズのバージョン 6.2.2.5 から

展開：FDM を使用した FTD（メモリが少ない ASA 5500-X シリーズ デバイスで実行）

アップグレード元：バージョン 6.2.0

直接アップグレード先：バージョン 6.2.2 ～ 6.4.0

バージョン6.2.0からアップグレードする場合、アップグレードに失敗し、「`Uploaded file is not a valid system upgrade file`」というエラーが表示される可能性があります。これは、正しいファイルを使用している場合でも発生する可能性があります。

この場合は、次の回避策を試してください。

- 再度お試しください。
- CLI を使用してアップグレードする。
- まず 6.2.0.1 にアップグレードする。

アクセスコントロールではSRUから遅延ベースのパフォーマンス設定を取得可能

展開：FMC

アップグレード元：6.1.x

直接アップグレード先：6.2.0+

バージョン 6.2.0+ の新しいアクセス コントロール ポリシーでは、デフォルトで、最新の侵入ルール更新（SRU）から遅延ベースのパフォーマンス設定が取得されます。この動作は、新し

い [設定の適用元（Apply Settings From）] オプションによって制御されます。このオプションを設定するには、アクセス コントロール ポリシーを編集または作成して、[詳細設定（Advanced）] をクリックし、遅延ベースのパフォーマンス設定を編集します。

バージョン 6.2.0+ にアップグレードすると、現在（バージョン 6.1.x）の設定に従って新しいオプションが設定されます。現在の設定が次の場合、新しいオプションは次のように設定されます。

- [デフォルト（Default）]：新しいオプションは、[インストールされたルールの更新（Installed Rule Update）] に設定されます。アップグレードしてから展開すると、最新の SRU からの遅延ベースのパフォーマンス設定が使用されます。最新の SRU が指定する内容によって、トラフィックの処理が変更される可能性があります。
- [カスタム（Custom）]：新しいオプションは、[カスタム（Custom）] に設定されます。システムは現在のパフォーマンス設定を保持します。このオプションによって動作が変更されることはありません。

アップグレードする前に設定を確認することをお勧めします。前述したように、バージョン 6.1.x の FMC Web インターフェイスから、ポリシーの遅延ベースのパフォーマンス設定を表示し、[Revert To Defaults] ボタンがグレー表示されているかどうかを確認します。ボタンがグレー表示されている場合は、デフォルト設定が使用されています。ボタンがアクティブになっている場合は、カスタム設定が設定されています。

FTDでの「フェールセーフ」から「Snortフェールオープン」への置き換え

展開：FMC を使用した FTD

アップグレード元：バージョン 6.1.x

直接アップグレード先：バージョン 6.2 以降

バージョン 6.2 では、Snort フェール オープン設定により、FMC によって管理される Firepower Threat Defense デバイスのフェールセーフ オプションが置き換えられます。フェールセーフでは、Snort がビジー状態のときにトラフィックをドロップすることができますが、Snort がダウンしている場合、トラフィックはインスペクションなしで自動的に通過します。Snort フェール オープンでは、このトラフィックをドロップすることができます。

FTD デバイスをアップグレードすると、その新しい Snort フェール オープン設定は、以下のように、古いフェールセーフ設定に依存します。新しい設定ではトラフィックの処理が変更されることはありませんが、アップグレードの前にフェールセーフを有効または無効にするかどうかを検討してください。

表 *5:* フェールセーフの *Snort* フェール オープンへの移行

バージョン 6.1 のフェールセーフ	バージョン 6.2 の Snort フェール オープン	動作
無効（デフォルトの動作）	[Busy]：無効 [Down]：有効	Snort プロセスがビジー状態の場合は、新規および既存の接続をドロップし、Snort プロセスがダウンしている場合は、接続をインスペクションなしで通過します。
有効	[Busy]：有効 [Down]：有効	Snort プロセスがビジー状態またはダウンしている場合、新規または既存の接続をインスペクションなしで通過します。

Snort フェール オープンでは、デバイスにバージョン 6.2 が必要であることに注意してください。バージョン 6.1.x のデバイスを管理している場合、FMC Web インターフェイスにフェールセーフ オプションが表示されます。

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、およびヘルスモ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 （28 ページ）」）を参照してください。

表 *6 : 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。	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。 少なくとも次の項目に回答できる必要があります。 • 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。 • 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。 • 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。
	管理ネットワークの帯域幅を確認します。	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。 『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 ノーツ）を参照してください。

✓	アクション	詳細
	アプライアンスへのアクセスを確認します。	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。
	設定変更を計画します。	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。 「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）」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。

✓	アクション	詳細
	バックアップを実行します。	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）。 • 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。 • 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。 **注意** 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。 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。
	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	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。 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。
	NTP 同期を確認します。	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）] ヘルスモ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。 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。
	ASA FirePOWER デバイスで ASA REST API を無効化します。	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`。 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。
	設定を展開します。	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。 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、トラフィック フロー、検査、およびデバイス動作 （17 ページ） を参照してください。

✓	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、時間テストとディスク容量の要件 （14 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

次のように Version6.2.3 に直接アップグレードできます。特定のパッチレベルを実行する必要はありません。

表 *7: Firepower* ソフトウェアをバージョン *6.2.3* 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	6.1.0
FMC を使用した Firepower デバイス	6.1.0 FXOS 2.3.1.73 以降のビルド（Firepower 4100/9300 に必要）。
FDM を搭載した Firepower デバイス	6.2.0
ASDM を使用した ASA FirePOWER	6.2.0

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。 スタック構成の 8000 シリーズ デバイスは同時にアップグレードされ、スタックは、すべてのデバイスのアップグレードが完了するまで、限定的なバージョン混在の状態で動作することに注意してください。これには、スタンドアロンデバイスのアップグレードと比べて大幅に長い時間がかかるということはありません。
- 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ない）。
- 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。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 6.2.3 の時間とディスク容量

表 *8*: バージョン *6.2.3* 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	時間
FMC	6.1.0 から：7415 MB 6.2.0 から：8863 MB 6.2.1 から：8263 MB 6.2.2 から：11860 MB	6.1.0 から：17 MB 6.2.0 から：24 MB 6.2.1 から：23 MB 6.2.2 から：24 MB	—	6.1.0 から：38 分 6.2.0 から：43 分 6.2.1 から：37 分 6.2.2 から：37 分
FMCv	6.1.0 から：7993 MB 6.2.0 から：9320 MB 6.2.1 から：11571 MB 6.2.2 から：11487 MB	6.1.0 から：23 MB 6.2.0 から：28 MB 6.2.1 から：24 MB 6.2.2 から：24 MB	—	ハードウェアによって異なる
Firepower 2100 シリーズ	6.2.1 から：7356 MB 6.2.2 から：11356 MB	6.2.1 から：7356 MB 6.2.2 から：11356 MB	1000 MB	6.2.1 から：15 分 6.2.2 から：15 分

Platform	ボリュームの容量	必要容量	FMC の容量	時間
Firepower 4100/9300 シャーシ	6.1.0 から：5593 MB 6.2.0 から：5122 MB 6.2.2 から：7498 MB	6.1.0 から：5593 MB 6.2.0 から：5122 MB 6.2.2 から：7498 MB	795 MB	6.1.0 から：10 分 6.2.0 から：12 分 6.2.2 から：15 分
FTD を搭載した ASA 5500-X シリーズ	6.1.0 から：4322 MB 6.2.0 から：6421 MB 6.2.2 から：6450 MB	6.1.0 から：.088 MB 6.2.0 から：.092 MB 6.2.2 から：.088 MB	1000 MB	6.1.0 から：54 分 6.2.0 から：53 分 6.2.2 から：50 分
FTDv	6.1.0 から：4225 MB 6.2.0 から：5179 MB 6.2.2 から：6450 MB	6.1.0 から：.076 MB 6.2.0 から：.092 MB 6.2.2 から：.092 MB	1000 MB	ハードウェアによって異なる
Firepower 7000/8000 シリーズ	6.1.0 から：5145 MB 6.2.0 から：5732 MB 6.2.2 から：6752 MB	6.1.0 から：18 MB 6.2.0 から：18 MB 6.2.2 から：18 MB	840 MB	6.1.0 から：29 分 6.2.0 から：31 分 6.2.2 から：31 分
ASA FirePOWER	6.1.0 から：7286 MB 6.2.0 から：7286 MB 6.2.2 から：10748 MB	6.1.0 から：16 MB 6.2.0 から：16 MB 6.2.2 から：16 MB	6.1.0 から：1200 MB 6.2.0 から：1200 MB	6.1.0 から：94 分 6.2.0 から：104 分 6.2.2 から：96 分
NGIPSv	6.1.0 から：4115 MB 6.2.0 から：5505 MB 6.2.2 から：5871 MB	6.1.0 から：18 MB 6.2.0 から：19 MB 6.2.2 から：19 MB	741 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 *9: 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。

導入	方法	トラフィックの動作
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 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 *10 : 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

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]（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。

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。

（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。

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 *11 : 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。

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 *12 : 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 *13 : 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。

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 *14*：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
パッシブ	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

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 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 *15 :* 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
パッシブ	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

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 *16 : 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**）	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 *17 : 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、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 *18 : 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 *19 : 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。	Cisco Firepower Management Center Upgrade Guide

タスク	ガイド
FDM を使用した Firepower Threat Defense ソフトウェアのアップグレード。	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 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。	Cisco Firepower 4100/9300 Upgrade Guide
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 5506-X、5508-X、および 5516-X での ROMMON イメージのアップグレード。	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。

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
- FirePOWER 7000 シリーズ：https://www.cisco.com/go/7000series-software
- FirePOWER 8000 シリーズ：https://www.cisco.com/go/8000series-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_Upgrade-6.6.0-90.sh.REL.tar`
- プラットフォーム： Firepower Management Center
- パッケージタイプ：アップグレード
- バージョンおよびビルド：6.6.0-90
- 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 *20 : 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

プラットフォーム	パッケージ
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 FTD を搭載した ISA 3000 FTDv	Cisco_FTD
Firepower 7000/8000 シリーズ AMP モデル	Sourcefire_3D_Device_S3
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）