



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](#) (1 ページ)
- [アップグレードする最小バージョン](#) (2 ページ)
- [Version6.6.x.xパッチのアップグレードガイドライン](#) (2 ページ)
- [応答しないアップグレード](#) (5 ページ)
- [トラフィック フローとインスペクション](#) (5 ページ)
- [時間とディスク容量のテスト](#) (13 ページ)
- [アップグレード手順](#) (17 ページ)

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](#) (17 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。

Version 6.6.x.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 6.6.x 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 6.6.x.x 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：侵入イベントに関する電子メールアラート機能を搭載した FMC (3 ページ)	FMC	6.2.3 ~ 6.7.0.x	6.7.0 6.6.0、6.6.1、または 6.6.3 これらのリリースに対するすべてのパッチ
	FDM を使用したバージョン 6.6.0.1 FTD アップグレードによる HA の一時停止 (4 ページ)	FDM を使用した FTD	6.6.0	6.6.0.1

アップグレードの失敗：侵入イベントに関する電子メールアラート機能を搭載した FMC

展開：Firepower Management Center

アップグレード元：バージョン 6.2.3 ~ 6.7.0.x

アップグレード先（直接）：バージョン 6.6.0、6.6.1、6.6.3、6.7.0、およびこれらのリリースへのパッチ

関連するバグ：CSCvw38870、CSCvx86231

個々の侵入イベントに対して電子メールアラートを設定した場合は、Firepower Management Center を上記のいずれかのバージョンにアップグレードする前に、その設定を完全に無効にします。そうならないと、アップグレードは失敗します。

この機能は、アップグレード後に再度有効にすることができます。この問題のためにすでにアップグレードに失敗した場合は、Cisco TAC に連絡してください。

侵入に関する電子メールアラートを完全に無効にするには、次の操作を行います。

1. Firepower Management Center で、[Policies] > [Actions] > [Alerts] を選択し、[Intrusion Email] をクリックします。
2. [State] を [off] に設定します。
3. [Rules] の横にある [Email Alerting per Rule Configuration] をクリックし、ルールを選択を解除します。

アップグレード後に再選択できるように、選択を解除したルールを書き留めておきます。



ヒント ルールの再選択に時間がかかりすぎる場合は、アップグレードする前に Cisco TAC に連絡してください。選択した内容を保存しておくことで、アップグレード後にすぐに再実装できるようにご案内いたします。

4. 設定を保存します。

FDM を使用したバージョン 6.6.0.1 FTD アップグレードによる HA の一時停止

展開 : FTD と FDM をハイアベイラビリティペアとして設定

アップグレード元 : バージョン 6.6.0

直接アップグレード先 : バージョン 6.6.0.1

関連バグ : [CSCvv45500](#)

ハイアベイラビリティ (HA) の FDM 管理 FTD デバイスをバージョン 6.6.0.1 にアップグレードすると、アップグレード後の再起動後にデバイスが一時停止モードになります。HA を手動で再開する必要があります。

FMC 展開は影響を受けません。

FDM 管理 FTD HA ペアをバージョン 6.6.0.1 にアップグレードするには、次の手順を実行します。

1. スタンバイデバイスをアップグレードします。
2. アップグレードが完了してデバイスがリブートしたら、手動で HA を再開します。FDM または CLI を使用できます。
 - FDM : **[Device] > [High Availability]** をクリックし、ギアメニュー (⚙️) から **[Resume HA]** を選択します。
 - CLI : **configure high-availability resume**

新しくアップグレードされたデバイスの HA ステータスは、スタンバイ装置として、装置がピアとネゴシエートした後に正常に戻ります。

3. 新しくアップグレードしたデバイスがアクティブピアになるように、アクティブピアとスタンバイピアを切り替えます (強制フェールオーバー)。
4. 新しいスタンバイピアに対してこの手順を繰り返します。

FDM でのハイアベイラビリティの設定と管理の詳細については、『[Firepower Device Manager 用 Cisco Firepower Threat Defense 構成ガイド](#)』を参照してください。

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

展開	メソッド	トラフィックの動作
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ー (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ー (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。

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

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 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2〜3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

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。

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
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 8: 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 9: 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 10: 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 11: 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。
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。

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

ディスク容量テスト

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

また、デバイス アップグレード パッケージ用に FMC (/var 内) に必要な容量も報告します。FTD デバイスがアップグレードパッケージを取得する内部サーバーがある場合、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 12: 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 6.6.5.2 の時間とディスク容量

表 13: バージョン 6.6.5.2 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	レポート時間
FMC	2.8 GB /var 内	20 MB / 内	—	39 分	8 分
FMCv : VMware	3.4GB /var 内	23 MB / 内	—	26 分	8 分
Firepower 1000 シリーズ	—	3.0 GB /ngfw 内	630 MB	8 分	12 分
Firepower 2100 シリーズ	—	2.9 GB /ngfw 内	660 MB	7 分	12 分

バージョン 6.6.5.1 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	リブート時間
Firepower 9300	—	2.4 GB /ngfw 内	430 MB	5 分	8 分
Firepower 4100 シリーズ	—	2.9 GB /ngfw 内	430 MB	6 分	8 分
Firepower 4100 シリーズ コンテナ インスタンス	—	2.5 GB /ngfw 内	430 MB	5 分	6 分
FTD を搭載した ASA 5500-X シリーズ	2.2 GB /home 内	120 MB /ngfw 内	380 MB	10 分	15 分
FTDv : VMware	1.8 GB /home 内	120 MB /ngfw 内	380 MB	5 分	6 分
ASA FirePOWER	2.9 GB /var 内	21 MB /内	450 MB	68 分	22 分
NGIPSv	920 MB /var 内	19 MB /内	310 MB	6 分	5 分

バージョン 6.6.5.1 の時間とディスク容量

表 14: バージョン 6.6.5.1 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	リブート時間
FMC	2.2 GB /var 内	20 MB /内	—	34 分	8 分
FMCv : VMware	2.2 GB /var 内	23 MB /内	—	28 分	6 分
Firepower 1000 シリーズ	—	1.5 GB /ngfw 内	340 MB	8 分	12 分
Firepower 2100 シリーズ	—	1.4 GB /ngfw 内	370 MB	6 分	11 分
Firepower 9300	—	770 MB /ngfw 内	140 MB	5 分	8 分
Firepower 4100 シリーズ	—	790 MB /ngfw 内	140 MB	5 分	8 分
Firepower 4100 シリーズ コンテナ インスタンス	—	730 MB /ngfw 内	140 MB	6 分	5 分
FTD を搭載した ASA 5500-X シリーズ	590 MB /home 内	120 MB /ngfw 内	85 MB	9 分	9 分
FTDv : VMware	590 MB /home 内	120 MB /ngfw 内	85 MB	6 分	5 分
ASA FirePOWER	1.7 GB /var 内	21 MB /内	130 MB	69 分	7 分
NGIPSv	78 MB /var 内	19 MB /内	16 MB	6 分	5 分

バージョン 6.6.0.1 の時間とディスク容量

この表で、アップグレード時間には再起動が含まれます。

表 15: バージョン 6.6.0.1 の時間とディスク容量

プラットフォーム	/var の容量	必要容量	FMC の容量	アップグレード時間
FMC	31 MB	20 MB	—	22 分
FMCv : VMware	1.1 GB	23 MB	—	17 分
Firepower 1000 シリーズ	450 MB	450 MB	240 MB	21 分
Firepower 2100 シリーズ	260 MB	260 MB	270 MB	17 分
Firepower 9300	460 MB	460 MB	46 MB	33 分
Firepower 4100 シリーズ	470 MB	470 MB	46 MB	11 分
FTD を搭載した ASA 5500-X シリーズ	440 MB	120 MB	46 MB	17 分
FTD を使用した ISA 3000	440 MB	120 MB	46 MB	21 分
FTDv : VMware	430 MB	120 MB	46 MB	11 分
ASA FirePOWER	80 MB	20 MB	15 MB	18 分
NGIPSv	64 MB	28 MB	15 MB	9 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 16: 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

タスク	ガイド
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「 <i>System Management</i> 」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 「 <i>Upgrade the ROMMON Image</i> 」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。