



のアップグレードガイドライン

このドキュメントには、バージョン 6.6 の重要なリリース固有のアップグレードガイドラインが記載されています。

- [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 \(2 ページ\)](#)
- [バージョン 6.6 のアップグレードガイドライン \(3 ページ\)](#)
- [FXOS のアップグレードガイドライン \(23 ページ\)](#)
- [応答しないアップグレード \(24 ページ\)](#)
- [パッチをアンインストールする \(24 ページ\)](#)
- [トラフィック フローとインスペクション \(27 ページ\)](#)
- [時間とディスク容量のテスト \(33 ページ\)](#)

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ガイドとコンフィギュレーションガイド (<http://www.cisco.com/jp/go/threatdefense-66-docs>) を参照してください。

表 1: アップグレードの計画フェーズ

計画フェーズ	次を含む
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	次を含む
バックアップ	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 のファームウェア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。 設定を展開します。 準備状況チェックを実行します。 ディスク容量を確認します。 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

アップグレードする最小バージョン

次のように、メンテナンスリリースを含むバージョン 6.6 に直接アップグレードできます。

表 2:バージョン 6.6 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
FMC	6.2.3

プラットフォーム	最小バージョン
FTD	6.2.3 Firepower 4100/9300 には FXOS 2.8.1.15 が必要です。ほとんどの場合、各メジャーバージョンで最新の FXOS ビルドを使用することを推奨します。判断のヒントについては、 Cisco Firepower 4100/9300 FXOS Release Notes, 2.8(1) を参照してください。
ASA with FirePOWER サービス	6.2.3 モデルの ASA 要件については、 デバイスプラットフォーム を参照してください。ASA と ASA FirePOWER のバージョン間には広い互換性がありますが、アップグレードすることで、新機能と解決された問題を活用できます。判断のヒントについては、 Cisco Secure Firewall ASA リリースノート を参照してください。
NGIPSv	6.2.3

パッチを適用する最小バージョン

パッチは4桁目のみを変更します。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。

バージョン 6.6 のアップグレードガイドライン

以下のチェックリストでは、該当する可能性のある新規アップグレードガイドラインや以前に公開されたアップグレードガイドラインを提供します。

表 3: FMC を使用した FTD のアップグレードガイドラインバージョン 6.6

✓	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
	Cisco Secure Firewall Management Center の新機能 (リリース別) : アップグレードに影響を与える新機能および廃止された機能が記載されています。現在のバージョンと対象バージョンの間にあるすべてのバージョンを確認してください。	任意 (Any)	任意 (Any)	任意 (Any)

✓	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
	未解決のバグおよび解決されたバグ：アップグレードに影響を与えるバグが記載されています。現在のバージョンと対象バージョン間にあるすべてのバージョンのリリースノートを確認してください。	任意 (Any)	任意 (Any)	任意 (Any)
	アップグレードする最小バージョン (2 ページ)	任意 (Any)	任意 (Any)	任意 (Any)
	FXOS のアップグレードガイドライン (23 ページ)	Firepower 4100/9300	任意 (Any)	任意 (Any)
	アップグレード禁止：FMC バージョン 6.6.5 以降からバージョン 6.7.0 (7 ページ)	FMC	6.6.5 以降 6.6.x リリース	6.7.0 のみ
	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 (8 ページ)	FMC	6.2.3 ~ 6.7.0.x	6.7.0 6.6.0、6.6.1、6.6.3 これらのリリースに対するすべてのパッチ
	FMCv には 28 GB の RAM が必要 (8 ページ)	FMCv	6.2.3 ~ 6.5.0.x	6.6 以降
	Firepower 1000 シリーズ デバイスではアップグレード後に電源の再投入が必要 (10 ページ)	Firepower 1000 シリーズ	6.4.0	6.5 以降
	新しい URL カテゴリとレピュテーション (10 ページ)	いずれか	6.2.3 ~ 6.4.0.x	6.5 以降
	TLS 暗号化アクセラレーションの有効化/無効にすることは不可 (19 ページ)	Firepower 2100 シリーズ Firepower 4100/9300	6.2.3 ~ 6.3.0.x	6.4 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
	名前が変更されたアップグレードとインストールパッケージ (19 ページ)	FMC Firepower 7000/8000 シリーズ NGIPSv	いずれか	6.3+
	FMC、NGIPSv で準備状況チェックに失敗する可能性 (20 ページ)	FMC Firepower 7000/8000 シリーズ NGIPSv	6.1.0 ~ 6.1.0.6 6.2.0 ~ 6.2.0.6 6.2.1 6.2.2 ~ 6.2.2.4 6.2.3 ~ 6.2.3.4	6.3+
	リモートアクセス VPN のデフォルト設定の変更によって VPN トラフィックがブロックされる可能性 (21 ページ)	FTD	6.2.0 ~ 6.2.3.x	6.3+
	セキュリティ インテリジェンスによって可能になるアプリケーションの識別 (21 ページ)	FMC の展開	6.1.0 ~ 6.2.3.x	6.3+
	アップグレード後に VDB を更新して CIP 検出を有効化 (22 ページ)	いずれか	6.1.0 ~ 6.2.3.x	6.3+
	無効な侵入変数セットによって展開に失敗する可能性 (22 ページ)	いずれか	6.1.0 ~ 6.2.3.x	6.3+

表 4: FDM を使用した FTD のアップグレードガイドラインバージョン 6.6

✓	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
	Cisco Secure Firewall Device Manager の新機能 (リリース別) : アップグレードに影響を与える新機能および廃止された機能が記載されています。現在のバージョンと対象バージョンの間にあるすべてのバージョンを確認してください。	任意 (Any)	任意 (Any)	任意 (Any)

✓	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
	未解決のバグおよび解決されたバグ：アップグレードに影響を与えるバグが記載されています。現在のバージョンと対象バージョン間にあるすべてのバージョンのリリースノートを確認してください。	任意 (Any)	任意 (Any)	任意 (Any)
	アップグレードする最小バージョン (2 ページ)	任意 (Any)	任意 (Any)	任意 (Any)
	FXOS のアップグレードガイドライン (23 ページ)	Firepower 4100/9300	任意 (Any)	任意 (Any)
	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 (6 ページ)	任意 (Any)	6.6.0	6.6.0.1
	Firepower 1000 シリーズ デバイスではアップグレード後に電源の再投入が必要 (10 ページ)	Firepower 1000 シリーズ	6.4.0	6.5 以降
	FDM を使用した FTD のアップグレード時に削除される履歴データ (10 ページ)	いずれか	6.2.3 ~ 6.4.0.x	6.5 以降
	新しい URL カテゴリとレピュテーション (10 ページ)	いずれか	6.2.3 ~ 6.4.0.x	6.5 以降
	TLS 暗号化アクセラレーションの有効化/無効にすることは不可 (19 ページ)	Firepower 2100 シリーズ Firepower 4100/9300	6.2.3 ~ 6.3.0.x	6.4 以降
	アップグレード後に VDB を更新して CIP 検出を有効化 (22 ページ)	いずれか	6.1.0 ~ 6.2.3.x	6.3+
	無効な侵入変数セットによって展開に失敗する可能性 (22 ページ)	いずれか	6.1.0 ~ 6.2.3.x	6.3+

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、『[Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager](#)』を参照してください。

アップグレード禁止：FMC バージョン 6.6.5 以降からバージョン 6.7.0

展開：FMC

アップグレード元：バージョン 6.6.5 以降のメンテナンスリリース

直接アップグレード先：バージョン 6.7.0 のみ

バージョン 6.6.5 以降の 6.6.x メンテナンスリリースからバージョン 6.7.0 にアップグレードすることはできません。これは、バージョン 6.6.5 のデータストアがバージョン 6.7.0 のデータストアよりも新しいためです。バージョン 6.6.5 以降を実行している場合は、バージョン 7.0.0 以降に直接アップグレードすることをお勧めします。

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。そうになっていなければ、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。

FMCv には 28 GB の RAM が必要

展開：FMCv

アップグレード元：バージョン 6.2.3 ～ 6.5

直接アップグレード先：バージョン 6.6 以降

すべての FMCv 実装には同じ RAM 要件が適用され、32 GB が推奨、28 GB が必須となりました（FMCv 300 の場合は 64 GB）。仮想アプライアンスに割り当てられたメモリが 28 GB 未満の場合、バージョン 6.6 以降へのアップグレードは失敗します。アップグレード後、メモリ割り当てを引き下げると、正常性モニターがアラートを発行します。

これらの新しいメモリ要件は、すべての仮想環境にわたって一貫した要件を適用し、パフォーマンスを向上させ、新しい機能を利用できるようにします。デフォルト設定を引き下げないことをお勧めします。使用可能なリソースによっては、パフォーマンスを向上させるために仮想アプライアンスのメモリとCPUの数を増やすことができます。詳細については、[Cisco Secure Firewall Management Center Virtual 入門ガイド](#)を参照してください。



- (注) バージョン 6.6.0 リリースの時点で、クラウドベースの FMCv の展開 (AWS、Azure) でのメモリ不足インスタンスのタイプが完全に廃止されました。以前のバージョンであっても、これらを使用して新しいインスタンスを作成することはできません。既存のインスタンスは引き続き実行できます。

次の表に、メモリが不足している展開のアップグレード前の要件を示します。

表 5:バージョン 6.6以降にアップグレードする場合の FMCvのメモリ要件

プラットフォーム	アップグレード前のアクション	詳細
VMware	28 GB 以上 (推奨 32 GB) を割り当てます。	最初に仮想マシンの電源をオフにします。 手順については、VMware のマニュアルを参照してください。
KVM	28 GB 以上 (推奨 32 GB) を割り当てます。	手順については、ご使用の KVM 環境のマニュアルを参照してください。
AWS	インスタンスのサイズを変更します。 <ul style="list-style-type: none"> • c3.xlarge から c3.4xlarge へ。 • c3.2.xlarge から c3.4xlarge へ。 • c4.xlarge から c4.4xlarge へ。 • c4.2xlarge から c4.4xlarge へ。 また、新規展開用に c5.4xlarge インスタンスも用意しています。	サイズを変更する前にインスタンスを停止します。これを行うと、インスタンスストアのボリューム上のデータが失われるため、最初にインスタンスストアによってバックアップされたインスタンスを最初に移行してください。さらに、管理インターフェイスに復元力のある IP アドレスがない場合は、そのパブリック IP アドレスが解放されます。 手順については、Linux インスタンスの AWS ユーザーガイドのインスタンスタイプの変更に関するマニュアルを参照してください。

プラットフォーム	アップグレード前のアクション	詳細
Azure	<p>インスタンスのサイズを変更します。</p> <ul style="list-style-type: none"> Standard_D3_v2 から Standard_D4_v2 へ。 	<p>Azure ポータルまたは PowerShell を使用します。サイズを変更する前にインスタンスを停止する必要はありませんが、停止すると追加のサイズが表示される場合があります。サイズ変更により、実行中の仮想マシンが再起動されます。</p> <p>手順については、Windows VM のサイズ変更に関する Azure のマニュアルを参照してください。</p>

Firepower 1000 シリーズ デバイスではアップグレード後に電源の再投入が必要

展開 : Firepower 1000 シリーズ デバイス

アップグレード元 : バージョン 6.4.0.x

直接アップグレード先 : バージョン 6.5.0+

バージョン 6.5.0 では、Firepower 1000/2100 および Firepower 4100/9300 シリーズ デバイス向けの FXOS CLI の「安全に消去する」機能が導入されています。

Firepower 1000 シリーズ デバイスでは、この機能を適切に動作させるには、バージョン 6.5.0+ にアップグレードした後にデバイスの電源を再投入する必要があります。自動リブートでは十分ではありません。サポートされているその他のデバイスでは、電源の再投入は必要ありません。

FDM を使用した FTD のアップグレード時に削除される履歴データ

展開 : FTD (FDM を使用)

アップグレード元 : バージョン 6.2.3 ~ 6.4.0.x

直接アップグレード先 : バージョン 6.5.0 以降

データベーススキーマの変更により、すべての履歴レポート データがアップグレード中に削除されます。アップグレード後、履歴データをクエリしたり、履歴データをダッシュボードに表示したりすることはできません。

新しい URL カテゴリとレピュテーション

展開 : すべて

アップグレード元 : バージョン 6.2.3 ~ 6.4.0.x

直接アップグレード先：バージョン 6.5.0+

Talos インテリジェンスグループは、URL の分類およびフィルタ処理のために、新しいカテゴリを導入し、レピュテーションの名前を変更しました。カテゴリの変更に関する詳細なリストについては、『[Cisco Firepower Release Notes, Version 6.5.0](#)』を参照してください。新しい URL カテゴリの説明については、Talos の「[Intelligence Categories](#)」サイトを参照してください。

また、ルール設定オプションは同じままですが、未分類およびレピュテーションのない URL の概念が新しくなっています。

- 未分類の URL は、疑わしい (Questionable)、ニュートラル (Neutral)、好ましい (Favorable)、信頼されている (Trusted) というレピュテーションのいずれかになります。

[未分類 (Uncategorized)] の URL はフィルタ処理できますが、レピュテーションによりさらに制約を追加することはできません。これらのルールは、レピュテーションに関係なく、すべての未分類 URL と一致します。

カテゴリのない信頼されていない (Untrusted) ルールのような設定は存在しないことに注意してください。それ以外の場合、信頼されていない (Untrusted) レピュテーションの未分類 URL は、「悪意のあるサイト (Malicious Sites)」という新しい脅威カテゴリに自動的に割り当てられます。

- レピュテーションのない URL は任意のカテゴリに属することができます。

レピュテーションのない URL をフィルタ処理することはできません。「レピュテーションなし」に対応するオプションはルールエディタにありません。ただし、レピュテーションに [すべて (Any)] を指定して URL をフィルタ処理することは可能で、その場合はレピュテーションのない URL が含まれます。これらの URL もカテゴリで制約する必要があります。Any/Any ルールに対するユーティリティはありません。

次の表に、アップグレードでの変更点の概要を示します。これらの変更は、ほとんどのお客様にとって最小限の影響で済むように設計されており、アップグレード後の展開を妨げることもありませんが、これらのリリースノートおよび現在の URL フィルタリングの設定を確認することを強くお勧めします。慎重な計画と準備は、誤った手順を回避することに加えて、アップグレード後のトラブルシューティングにかかる時間を短縮するのに役立ちます。

表 6: アップグレード時の展開の変更

変更内容	詳細
URL ルールのカテゴリが変更されます。	<p>アップグレードにより、次のポリシーで、新しいカテゴリセットのほぼ同等のルールが使用されるように URL ルールが変更されます。</p> <ul style="list-style-type: none"> • アクセス コントロール • SSL • QoS (FMC のみ) • 相関 (FMC のみ) <p>これらの変更により、余分なルールや無効になったルールが生じ、パフォーマンスが低下する可能性があります。マージされたカテゴリが設定に含まれている場合、許可またはブロックされる URL が若干変更されることがあります。</p>
URL ルールのレピュテーションの名前が変更されます。	<p>アップグレードにより、新しいレピュテーション名を使用するように URL ルールが変更されます。</p> <ol style="list-style-type: none"> 1. 信頼されていない (「高リスク」だった) 2. 疑わしい (「疑わしいサイト」だった) 3. ニュートラル (「セキュリティリスクのある無害なサイト」だった) 4. 好ましい (「無害なサイト」だった) 5. 信頼されている (「十分に既知」だった)
URL キャッシュをクリアします。	<p>アップグレードによって URL キャッシュがクリアされます。このキャッシュには、システムが以前にクラウドで検索した結果が含まれています。ローカル データ セットに含まれていない URL については、アクセス時間が一時的に少し長くなることがあります。</p>
「レガシー」イベントにラベルを付けます。	<p>すでにログに記録されているイベントの場合、アップグレードにより、関連する URL のカテゴリおよびレピュテーション情報が「レガシー」としてラベル付けされます。これらのレガシー イベントは時間の経過とともにデータベースからエージアウトします。</p>

URL カテゴリおよびレピュテーションのアップグレード前のアクション

アップグレードする前に、次のアクションを実行します。

表 7: アップグレード前のアクション

アクション	詳細
<p>アプライアンスが Talos のリソースにアクセスできることを確認します。</p>	<p>アップグレード後、システムは次のシスコのリソースと通信する必要があります。</p> <ul style="list-style-type: none"> • https://regsvc.sco.cisco.com/ - 登録 • https://est.sco.cisco.com/ - セキュア通信のための証明書を取得 • https://updates-talos.sco.cisco.com/ - クライアント/サーバーマニフェストを取得 • http://updates.ironport.com/ - データベースのダウンロード（注：ポート 80 を使用） • https://v3.sds.cisco.com/ - クラウドクエリ <p>クラウドクエリサービスは、次の IP アドレスブロックも使用します。</p> <ul style="list-style-type: none"> • IPv4 クラウドクエリ : <ul style="list-style-type: none"> • 146.112.62.0/24 • 146.112.63.0/24 • 146.112.255.0/24 • 146.112.59.0/24 • IPv6 クラウドクエリ : <ul style="list-style-type: none"> • 2a04:e4c7:ffff::/48 • 2a04: e4c7: fffe::/48

アクション	詳細
<p>潜在的なルールの問題を特定します。</p>	<p>今後の変更点を理解します。現在の URL フィルタリング設定を調べて、アップグレード後に実行する必要があるアクションを特定します（次の項を参照）。</p> <p>(注) 廃止されたカテゴリを使用する URL ルールをこの時点で変更することができます。そうしない場合、それらを使用するルールによってアップグレード後の展開が妨げられます。</p> <p>FMC 展開では、アクセスコントロールのルールや下位ポリシー（SSL など）のルールを含む、ポリシーの現在の保存されている設定に関する詳細情報を提供する、アクセスコントロール ポリシー レポートを生成することを推奨します。URL ルールごとに、現在のカテゴリ、レピュテーション、関連付けられているルールアクションが表示されます。FMC で[ポリシー (Policies)] > [アクセス制御 (Access Control)]を選択し、該当するポリシーの横にあるレポートアイコン (📄) をクリックします。</p>

URL カテゴリおよびレピュテーションのアップグレード後のアクション

アップグレード後に URL フィルタリング設定を再確認し、できるだけ早く次のアクションを実行する必要があります。展開のタイプとアップグレードによって行われた変更に応じて、一部（すべてではない）の問題が GUI でマークされることがあります。たとえば、FMC/FDM のアクセス コントロール ポリシーでは、[警告の表示 (Show Warnings)] (FMC) または [問題ルールの表示 (Show Problem Rules)] (FDM) をクリックできます。

表 8: アップグレード後の操作

アクション	詳細
<p>廃止されたカテゴリをルールから削除します。必須。</p>	<p>アップグレードでは、廃止されたカテゴリを使用する URL ルールは変更されません。これらを使用するルールは展開を阻止します。</p> <p>FMC では、これらのルールがマークされます。</p>
<p>新しいカテゴリを含めるルールを作成または変更します。</p>	<p>ほとんどの新しいカテゴリは脅威を特定します。これらのカテゴリを使用することを強くお勧めします。</p> <p>FMC では、この新しいカテゴリはこのアップグレード後にマークされませんが、今後、Talos によってカテゴリが追加される場合があります。この場合は新しいカテゴリがマークされます。</p>

アクション	詳細
<p>マージされたカテゴリの結果として変更されたルールを評価します。</p>	<p>影響を受けたカテゴリのいずれかが含まれている各ルールに影響を受けたすべてのルールが含まれるようになります。元のカテゴリが異なるレピュテーションに関連付けられていた場合、新しいルールはさらに広い、より包含的なレピュテーションに関連付けられます。以前と同様に URL をフィルタリングするには、いくつかの設定を変更する必要があります。 「マージされた URL カテゴリを持つルールのガイドライン (15 ページ)」 を参照してください。</p> <p>変更内容とプラットフォームがルールの警告を処理する方法に応じて、変更がマークされることがあります。たとえば、FMC は完全に冗長および完全にプリエンブション処理されたルールをマークしますが、部分的に重複したルールはマークしません。</p>
<p>分割されたカテゴリの結果として変更されたルールを評価します。</p>	<p>アップグレードにより、URL ルール内の古い単一のカテゴリが新しいカテゴリすべてに置き換えられ、新しいカテゴリは古いカテゴリにマッピングされます。これにより URL のフィルタリング方法は変更されませんが、影響を受けるルールを変更して、新しい精度を活用することができます。</p> <p>これらの変更はマークされません。</p>
<p>名前が変更されたカテゴリまたは変更されていないカテゴリを把握します。</p>	<p>特に対処の必要はありませんが、これらの変更には注意する必要があります。</p> <p>これらの変更はマークされません。</p>
<p>未分類およびレピュテーションのない URL の処理方法を評価します。</p>	<p>未分類の URL とレピュテーションのない URL を使用できるようになりましたが、未分類の URL をレピュテーションでフィルタ処理することも、レピュテーションのない URL をフィルタ処理することもできません。</p> <p>[未分類 (Uncategorized)]カテゴリまたは[すべて (Any)]のレピュテーションでフィルタ処理されるルールが、期待どおりに動作することを確認してください。</p>

マージされた URL カテゴリを持つルールのガイドライン

アップグレード前に URL フィルタリング設定を確認する場合は、次のシナリオとガイドラインのどちらが適用されるかを決定します。これにより、アップグレード後の設定が予想どおりに実行され、問題を解決するためのクイックアクションを実行できるようになります。

表 9: マージされた URL カテゴリを持つルールのガイドライン

ガイドライン	詳細
ルールの順序によってトラフィックに一致するルールを決定	同じカテゴリを含むルールを検討する場合は、トラフィックが、その条件を含むリスト内の最初のルールと一致することに注意してください。
同じルール内のカテゴリと異なるルール内のカテゴリ	<p>単一のルール内でカテゴリをマージすると、ルール内の単一のカテゴリにマージされます。たとえば、カテゴリ A とカテゴリ B がマージされてカテゴリ AB になり、カテゴリ A とカテゴリ B を持つルールがある場合、マージ後にルールは単一のカテゴリ AB を保持します。</p> <p>異なるルールのカテゴリをマージすると、マージ後に各ルールで同じカテゴリを持つルールが個別に生成されます。たとえば、カテゴリ A とカテゴリ B がマージされてカテゴリ AB になり、カテゴリ A を持つルール 1 とカテゴリ B を持つルール 2 がある場合、マージ後にルール 1 とルール 2 にはカテゴリ AB がそれぞれ含まれます。この状況を解決する方法は、ルールの順序、ルールに関連付けられたアクションとレピュテーションレベル、ルールに含まれる他の URL カテゴリ、およびルールに含まれる非 URL 条件によって異なります。</p>
関連付けられたアクション	異なるルールのマージされたカテゴリが異なるアクションに関連付けられている場合、マージ後に、同じカテゴリに対して異なるアクションを持つ 2 つ以上のルールが生成される場合があります。
関連付けられているレピュテーションレベル	マージの前に異なるレピュテーションレベルに関連付けられたカテゴリが単一のルールに含まれている場合、マージされたカテゴリは、より包括的なレピュテーションレベルに関連付けられます。たとえば、カテゴリ A が特定のルールで [すべてのレピュテーション (Any reputation)] に関連付けられており、カテゴリ B が同じルールでレピュテーションレベル [3 - セキュリティリスクのある無害なサイト (3 - Benign sites with security risks)] に関連付けられている場合、マージ後に、そのルール内のカテゴリ AB は [すべてのレピュテーション (Any reputation)] に関連付けられます。

ガイドライン	詳細
重複および冗長カテゴリとルール	<p>マージ後、異なるルールには、異なるアクションとレピュテーションレベルに関連付けられている同じカテゴリが含まれる場合があります。</p> <p>冗長ルールは完全に重複しているとは限りませんが、ルール順序が前にある別のルールが一致する場合、トラフィックに一致しなくなる可能性があります。たとえば、ルール 1 とカテゴリ A ([すべてのレピュテーション (Any Reputation)])に適用される) を事前マージし、ルール 2 とカテゴリ B (レピュテーション 1-3 のみに適用される) を事前マージする場合、マージ後に、ルール 1 とルール 2 の両方にカテゴリ AB が含まれるようになるが、ルール順序でルール 1 の順序が前にあると、ルール 2 が一致することはありません。</p> <p>FMC において、同一のカテゴリとレピュテーションを持つルールでは警告が表示されます。ただし、これらの警告は、含まれているカテゴリが同じですが、レピュテーションが異なるルールを示すことはありません。</p> <p>注意：重複または冗長カテゴリを解決する方法を決定する際には、ルールのすべての条件を考慮してください。</p>
ルール内の他の URL カテゴリ	<p>マージされた URL を含むルールには、他の URL カテゴリも含まれている場合があります。したがって、マージ後に特定のカテゴリが複製された場合は、これらのルールを削除するのではなく、変更する必要があることがあります。</p>
ルール内の非 URL 条件	<p>マージされた URL カテゴリを含むルールには、アプリケーション条件などの他のルール条件も含まれている場合があります。したがって、マージ後に特定のカテゴリが複製された場合は、これらのルールを削除するのではなく、変更する必要があることがあります。</p>

次の表の例ではカテゴリ A とカテゴリ B を使用しています。現在はカテゴリ AB にマージされています。2 つのルールの例では、ルール 1 はルール 2 よりも前に表示されます。

表 10: マージされた URL カテゴリを持つルールの例

シナリオ	アップグレード前	アップグレード後
同じルール内のマージされたカテゴリ	ルール 1 にはカテゴリ A とカテゴリ B が含まれる。	ルール 1 にはカテゴリ AB が含まれる。

シナリオ	アップグレード前	アップグレード後
異なるルール内でマージされたカテゴリ	<p>ルール 1 にはカテゴリ A が含まれる。</p> <p>ルール 2 にはカテゴリ B が含まれる。</p>	<p>ルール 1 にはカテゴリ AB が含まれる。</p> <p>ルール 2 にはカテゴリ AB が含まれる。</p> <p>具体的な結果は、リスト内のルールの順序、レピュテーションレベル、および関連付けられたアクションによって異なります。また、冗長性を解決する方法を決定する際に、ルール内の他のすべての条件も考慮する必要があります。</p>
異なるルール内でマージされたカテゴリには異なるアクションが含まれる (レピュテーションは同じ)	<p>ルール 1 には [許可 (Allow)] に設定されたカテゴリ A が含まれる。</p> <p>ルール 2 には [ブロック (Block)] に設定されたカテゴリ B が含まれる。 (レピュテーションは同じ)</p>	<p>ルール 1 には [許可 (Allow)] に設定されたカテゴリ AB が含まれる。</p> <p>ルール 2 には [ブロック (Block)] に設定されたカテゴリ AB が含まれる。</p> <p>ルール 1 は、このカテゴリのすべてのトラフィックに一致します。</p> <p>ルール 2 がトラフィックに一致することはなく、カテゴリとレピュテーションの両方が同じであるため、マージ後に警告を表示した場合は、警告インジケータが表示されます。</p>
同じルール内でマージされたカテゴリには異なるレピュテーションレベルが含まれる	<p>ルール 1 には次が含まれます。</p> <p>レピュテーション Any のカテゴリ A</p> <p>レピュテーション 1-3 のカテゴリ B</p>	<p>ルール 1 にはレピュテーション Any のカテゴリ AB が含まれる。</p>
異なるルール内でマージされたカテゴリには異なるレピュテーションレベルが含まれる	<p>ルール 1 にはレピュテーション Any のカテゴリ A が含まれる。</p> <p>ルール 2 にはレピュテーション 1-3 のカテゴリ B が含まれる。</p>	<p>ルール 1 にはレピュテーション Any のカテゴリ AB が含まれる。</p> <p>ルール 2 にはレピュテーション 1-3 のカテゴリ AB が含まれる。</p> <p>ルール 1 は、このカテゴリのすべてのトラフィックに一致します。</p> <p>ルール 2 がトラフィックに一致することはありませんが、レピュテーションが同一でないため、警告インジケータは表示されません。</p>

TLS 暗号化アクセラレーションの有効化/無効にすることは不可

展開：Firepower 2100 シリーズ、Firepower 4100/9300 シャーシ

アップグレード元：バージョン 6.1.0 ～ 6.3.x

直接アップグレード先：バージョン 6.4.0 以降

SSL ハードウェアアクセラレーションは、TLS 暗号化アクセラレーションに名前が変更されました。

デバイスによっては、TLS 暗号化アクセラレーションがソフトウェアまたはハードウェアで実行される場合があります。アップグレードでは、この機能を手動で無効にした場合でも、すべての対象デバイスでアクセラレーションが自動的に有効になります。ほとんどの場合、この機能を設定することはできません。この機能は自動的に有効になり、無効にすることはできません。

バージョン 6.4.0 へのアップグレード：Firepower 4100/9300 シャーシのマルチインスタンス機能を使用している場合は、FXOS CLI を使用して、モジュール/セキュリティエンジンごとに、1 つのコンテナインスタンスに対して TLS 暗号化アクセラレーションを有効にすることができます。他のコンテナインスタンスに対してアクセラレーションは無効になっていますが、ネイティブインスタンスには有効になっています。

バージョン 6.5.0 以降へのアップグレード：Firepower 4100/9300 シャーシのマルチインスタンス機能を使用している場合は、FXOS CLI を使用して、Firepower 4100/9300 シャーシ上の複数のコンテナインスタンス（最大 16 個）に対して TLS 暗号化アクセラレーションを有効にすることができます。新しいインスタンスでは、この機能がデフォルトで有効になっています。ただし、アップグレードによって既存のインスタンスのアクセラレーションが有効になることはありません。代わりに、**config hwCrypto enable** CLI コマンドを使用してください。

名前が変更されたアップグレードとインストールパッケージ

展開：FMC、7000/8000 シリーズ、NGIPSv

アップグレード元：バージョン 6.1.0 ～ 6.2.3.x

直接アップグレード先：バージョン 6.3+

アップグレード、パッチ、ホットフィックス、およびインストールパッケージの命名スキーム（名前の最初の部分）は、当該プラットフォーム上で「Version 6.3.0」で始まるように変更されました。



- (注) この変更により、古い物理アプライアンス（DC750、1500、2000、3500、4000 のほか、7000/8000 シリーズ デバイスと AMP モデル）の再イメージ化に関する問題が発生します。バージョン 5.x を現在実行していて、これらのアプライアンスのいずれかにバージョン 6.3.0 または 6.4.0 を新規インストールする必要がある場合は、シスコ サポート および ダウンロード サイト から インストール パッケージをダウンロードした後、その名前を「古い」名前に変更します。これらのアプライアンスをバージョン 6.5+ に再イメージ化することはできません。

表 11: 命名スキーム : アップグレード、パッチ、およびホットフィックス パッケージ

プラットフォーム	命名方式
FMC	新 : Cisco_Firepower_Mgmt_Center 旧 : Sourcefire_3D_Defense_Center_S3
NGIPSv	新 : Cisco_Firepower_NGIPS_Virtual 旧 : Sourcefire_3D_Device_VMware 旧 : Sourcefire_3D_Device_Virtual64_VMware

表 12: 命名スキーム : インストールパッケージ

プラットフォーム	命名方式
FMC (物理)	新 : Cisco_Firepower_Mgmt_Center 旧 : Sourcefire_Defense_Center_M4 旧 : Sourcefire_Defense_Center_S3
FMCv: VMware	新 : Cisco_Firepower_Mgmt_Center_Virtual_VMware 旧 : Cisco_Firepower_Management_Center_Virtual_VMware
FMCv: KVM	新 : Cisco_Firepower_Mgmt_Center_Virtual_KVM 旧 : Cisco_Firepower_Management_Center_Virtual
Firepower 7000/8000 シリーズ	新 : Cisco_Firepower_NGIPS_Appliance 旧 : Sourcefire_3D_Device_S3
NGIPSv	新 : Cisco_Firepower_NGIPSv_VMware 旧 : Cisco_Firepower_NGIPS_VMware

FMC、NGIPSv で準備状況チェックに失敗する可能性

展開 : FMC、NGIPSv

アップグレード元 : バージョン 6.1.0 ~ 6.1.0.6、バージョン 6.2.0 ~ 6.2.0.6、バージョン 6.2.1、バージョン 6.2.2 ~ 6.2.2.4、およびバージョン 6.2.3 ~ 6.2.3.4

直接アップグレード先 : バージョン 6.3.0+

次に示すバージョンの Firepower のいずれかからアップグレードする場合は、そこに示されているモデルで準備状態チェックを実行できません。これは、準備状況チェックプロセスが新しいアップグレードパッケージに対して互換性を持たないためです。

表 13:バージョン 6.3.0以降用の準備状況チェックを備えたパッチ

準備完了チェックがサポートされない	修正された最初のパッチ
6.1.0 ~ 6.1.0.6	6.1.0.7
6.2.0 ~ 6.2.0.6	6.2.0.7
6.2.1	なし。バージョン 6.2.3.5+ にアップグレードしてください。
6.2.2 ~ 6.2.2.4	6.2.2.5
6.2.3 ~ 6.2.3.4	6.2.3.5

リモート アクセス VPN のデフォルト設定の変更によって VPN トラフィックがブロックされる可能性

展開：リモート アクセス VPN 用に設定された Firepower Threat Defense

アップグレード元：バージョン 6.2.x

直接アップグレード先：バージョン 6.3+

バージョン6.3では非表示オプションの **sysopt connection permit-vpn** のデフォルト設定が変更されています。アップグレードすると、リモート アクセス VPN がトラフィックを渡さなくなる可能性があります。この場合は、次のいずれかの手法を使用してください。

- **sysopt connection permit-vpn** コマンドを設定する FlexConfig オブジェクトを作成します。このコマンドの新しいデフォルトは **no sysopt connection permit-vpn** です。

これは、外部ユーザーがリモート アクセス VPN アドレス プール内の IP アドレスになりすますことができないため、VPN でトラフィックを許可するよりも安全な方法です。欠点は VPN トラフィックが検査されないことです。つまり、侵入とファイルの保護、URL フィルタリング、その他の高度な機能がトラフィックに適用されません。

- リモート アクセス VPN アドレス プールからの接続を許可するアクセス制御ルールを作成します。

この方法では、VPN トラフィックが確実に検査され、高度なサービスを接続に適用できます。欠点は、外部のユーザーが IP アドレスをスプーフィングして、内部ネットワークにアクセスしやすくなることです。

セキュリティインテリジェンスによって可能になるアプリケーションの識別

展開：Firepower Management Center

アップグレード元：バージョン 6.1 ～ 6.2.3.x

直接アップグレード先：バージョン 6.3+

バージョン 6.3 では、セキュリティインテリジェンスの設定によりアプリケーションの検出と識別が可能になります。現在の展開で検出を無効にした場合は、アップグレードプロセスによって再び検出が有効になる可能性があります。必要がない場合（たとえば、IPS のみの展開など）に検出を無効にするとパフォーマンスが向上する可能性があります。

検出を無効にするには、次の手順を実行する必要があります。

- ネットワーク検出ポリシーからすべてのルールを削除します。
- 単純なネットワークベースの条件（ゾーン、IP アドレス、VLAN タグ、およびポート）のみを使用してアクセス制御を実行します。どんな種類のアプリケーション、ユーザー、URL、または地理位置情報の制御も行わないでください。
- **(新規)** デフォルトのグローバルリストなど、アクセスコントロールポリシーのセキュリティインテリジェンス設定からすべてのホワイトリストとブラックリストを削除することで、ネットワークと URL ベースのセキュリティインテリジェンスを無効にします。
- **(新規)** DNS のデフォルトのグローバルホワイトリストや DNS ルールのグローバルブラックリストなど、関連付けられている DNS ポリシー内のすべてのルールを削除または無効にすることで、DNS ベースのセキュリティインテリジェンスを無効にします。

アップグレード後に VDB を更新して CIP 検出を有効化

展開：すべて

アップグレード元：バージョン 6.1.0 ～ 6.2.3.x、VDB 299+ 搭載

直接アップグレード先：バージョン 6.3.0+

脆弱性データベース（VDB）299 以降を使用しているときにアップグレードする場合、アップグレードプロセスの問題により、アップグレード後の CIP 検出を使用できなくなります。これには、2018 年 6 月から現在までにリリースされたすべての VDB に加えて、最新の VDB も含まれます。

アップグレード後は常に脆弱性データベース（VDB）を最新バージョンに更新することを推奨しますが、この場合は特に重要です。

この問題の影響を受けるかどうかを確認するには、CIP ベースアプリケーションの条件を使用して、アクセス制御ルールを設定してみてください。ルールエディタで CIP アプリケーションが見つからない場合は、手動で VDB を更新します。

無効な侵入変数セットによって展開に失敗する可能性

展開：すべて

アップグレード元：バージョン 6.1 ～ 6.2.3.x

直接アップグレード先：バージョン 6.3.0+

侵入変数セット内のネットワーク変数については、除外する IP アドレスが、含める IP アドレスのサブセットである必要があります。次の表に、有効な設定と無効な設定の例を示します。

有効	無効
含める：10.0.0.0/8 除外する：10.1.0.0/16	含める：10.1.0.0/16 除外する：172.16.0.0/12 除外する：10.0.0.0/8

バージョン 6.3.0 より前のバージョンでは、このタイプの無効な設定でネットワーク変数を正常に保存できました。現在のバージョンでは、これらの設定によって展開がブロックされ、次のエラーが表示されます。Variable set has invalid excluded values.

この場合は、正しく設定されていない変数セットを識別して編集してから展開しなおしてください。変数セットによって参照されているネットワークオブジェクトおよびグループの編集が必要である場合もあることに注意してください。

FXOS のアップグレードガイドライン

Firepower 4100/9300 の場合、FTD のメジャーアップグレードには FXOS のアップグレードも必要です。

FTD のメジャーバージョンには特別に認定および推奨されている付随の FXOS バージョンがあります。シスコではこれらの組み合わせの拡張テストを実施するため、可能な限りこれらの組み合わせを使用してください。メンテナンスリリースとパッチで FXOS のアップグレードが必要になることはほとんどありませんが、最新の FXOS ビルドにアップグレードして、解決済みの問題を有効に活用できます。

また、最新のファームウェアを推奨します（『[Cisco Firepower 4100/9300 FXOS ファームウェアアップグレードガイド](#)』を参照）。

重要なリリース固有のアップグレードガイドライン、新機能および廃止された機能、未解決のバグおよび解決済みのバグについては、[Cisco Firepower 4100/9300 FXOS リリースノート](#) を参照してください。

FTD をアップグレードするために必要な FXOS の最小バージョン

バージョン 6.6 を実行するために必要な FXOS の最小バージョンは、FXOS 2.8.1.15 です。

FXOS をアップグレードするために必要な FXOS の最小バージョン

FXOS 2.2.2 から、それ以降の任意の FXOS バージョンにアップグレードできます。

FXOS アップグレードの所要時間

FXOS のアップグレードには最長 45 分かかることがあり、トラフィックフローやインスペクションに影響を与える場合があります。詳細については、[FXOS のアップグレードでのトラフィックフローとインスペクション \(27 ページ\)](#) 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、アップグレード中は手動で再起動またはシャットダウンしないでください。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。

パッチをアンインストールする

FMC および ASDM の展開では、ほとんどのパッチをアンインストールすることができます。以前のメジャーリリースまたはメンテナンスリリースに戻す必要がある場合は、イメージを再作成する必要があります。ガイドライン、制限、および手順については、FMC アップグレードガイドの「[Uninstall a Patch](#)」またはこれらのリリースノート「[ASDM による ASA FirePOWER パッチのアンインストール \(24 ページ\)](#)」を参照してください。

ASDM による ASA FirePOWER パッチのアンインストール

Linux シェル (エキスパートモード) を使用してデバイスパッチをアンインストールします。デバイスの admin ユーザーとして、または CLI 設定アクセス権を持つ別のローカルユーザーとして、デバイス シェルにアクセスできる必要があります。シェルアクセスを無効にした場合は、ロックダウンを元に戻すために Cisco TAC にご連絡ください。

ASA フェールオーバーペアおよびクラスタの場合、一度に1つのアプライアンスからアンインストールすることにより、中断を最小限に抑えます。次に移る前に、パッチが1つのユニットから完全にアンインストールされるまで待ちます。

表 14: ASA フェールオーバーペア/クラスタ内の ASA with FirePOWER Services のアンインストール順序

設定	アンインストール順序
ASA FirePOWER が有効な ASA アクティブ/スタンバイ フェールオーバー ペア	<p>常にスタンバイからアンインストールします。</p> <ol style="list-style-type: none"> 1. スタンバイ ASA デバイスの ASA FirePOWER モジュールからアンインストールします。 2. フェールオーバーします。 3. 新しいスタンバイ ASA デバイスの ASA FirePOWER モジュールからアンインストールします。
ASA FirePOWER が有効な ASA アクティブ/アクティブ フェールオーバー ペア	<p>アンインストールしないユニットの両方のフェールオーバー グループをアクティブにします。</p> <ol style="list-style-type: none"> 1. プライマリ ASA デバイスの両方のフェールオーバー グループをアクティブにします。 2. セカンダリ ASA デバイスの ASA FirePOWER モジュールからアンインストールします。 3. セカンダリ ASA デバイスの両方のフェールオーバー グループをアクティブにします。 4. プライマリ ASA デバイスの ASA FirePOWER モジュールからアンインストールします。
ASA FirePOWER が有効な ASA クラスタ	<p>アンインストールの前に、各ユニットでクラスタリングを無効にします。一度に1つのユニットからアンインストールし、制御ユニットを最後に残します。</p> <ol style="list-style-type: none"> 1. データユニットでクラスタリングを無効にします。 2. そのユニットの ASA FirePOWER モジュールからアンインストールします。 3. クラスタリングを再び有効にします。ユニットが再びクラスタに参加するのを待ちます。 4. 各データユニットに対して手順を繰り返します。 5. 制御ユニットでクラスタリングを無効にします。新しい制御ユニットが引き継ぐまで待ちます。 6. 以前の制御ユニットの ASA FirePOWER モジュールからアンインストールします。 7. クラスタリングを再び有効にします。



注意 アンインストール中に設定の変更を行ったり、展開したりしないでください。システムが非アクティブに見えても、進行中のアンインストールを手動で再起動、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。アンインストールに失敗する、アプライアンスが応答しないなど、アンインストール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。

始める前に

- ASA のフェールオーバーやクラスタの展開では、正しいデバイスからアンインストールしようとしていることを確認してください。
- 正常に展開され、通信が確立されていることを確認します。

ステップ 1 デバイスの設定が古い場合は、この時点で ASDM から展開します。

アンインストールする前に展開すると、失敗する可能性が減少します。展開とその他の必須のタスクが完了していることを確認してください。アンインストールの開始時に実行中だったタスクは停止され、失敗したタスクとなって再開できなくなります。後で失敗ステータス メッセージを手動で削除できます。

ステップ 2 ASA FirePOWER モジュールの Firepower CLI にアクセスします。admin として、または設定アクセス権を持つ別の Firepower CLI ユーザーとしてログインします。

モジュールの管理インターフェイスに SSH 接続するか（ホスト名または IP アドレス）、コンソールを使用できます。コンソールポートはデフォルトで ASA CLI に設定されており、Firepower CLI にアクセスするには `session sfr` コマンドを使用する必要があることにご注意ください。

ステップ 3 `expert` コマンドを使用して Linux シェルにアクセスします。

ステップ 4 アップグレードディレクトリにアンインストールパッケージがあることを確認します。

```
ls /var/sf/updates
```

パッチのアンインストーラには、アップグレードパッケージと同様に名前が付けられていますが、ファイル名には Patch ではなく Patch_Uninstaller が含まれています。デバイスにパッチを適用すると、そのパッチ用のアンインストーラがアップグレードディレクトリに自動的に作成されます。アンインストーラがない場合は、Cisco TAC までお問い合わせください。

ステップ 5 `uninstall` コマンドを実行し、プロンプトが表示されたらパスワードを入力します。

```
sudo install_update.pl --detach /var/sf/updates/uninstaller_name
```

注意 確認を求められることはありません。このコマンドを入力すると、デバイスの再起動を含むアンインストールが開始されます。アンインストール時のトラフィックフローとインスペクションの中断は、アップグレード時に発生する中断と同じです。準備が整っていることを確認してください。--detach オプションを使用すると、SSH セッションがタイムアウトした場合にアンインストールプロセスが強制終了されなくなり、デバイスが不安定な状態になる可能性があることに注意してください。

ステップ6 ログアウトするまでアンインストールを監視します。

個別のアンインストールの場合は、tail か tailf を使用してログを表示します。

```
tail /ngfw/var/log/sf/update.status
```

それ以外の場合は、コンソールか端末で進行状況を監視します。

ステップ7 アンインストールが成功したことを確認します。

アンインストールが完了したら、モジュールのソフトウェアバージョンが正しいことを確認します。[設定 (Configuration)] > [ASA FirePOWERの設定 (ASA FirePOWER Configuration)] > [デバイス管理 (Device Management)] > [デバイス (Device)] の順に選択します。

ステップ8 構成を再展開します。

次のタスク

ASAのフェールオーバーやクラスタの展開では、各ユニットに対して計画した順序でこの手順を繰り返します。

トラフィックフローとインスペクション

デバイスのアップグレード（ソフトウェアおよびオペレーティングシステム）により、トラフィックフローとインスペクションが影響を受けます。影響が最も少ない時間帯にメンテナンス期間をスケジュールします。

FXOSのアップグレードでのトラフィックフローとインスペクション

FXOSをアップグレードするとシャーシが再起動します。ハイアベイラビリティやスケーラビリティ環境でも、各シャーシのFXOSを個別にアップグレードします。中断を最小限に抑えるには、1つずつシャーシをアップグレードします。

表 15: トラフィックフローとインスペクション: FXOSのアップグレード

FTDの導入	トラフィックの挙動	メソッド
スタンドアロン	廃棄	—
高可用性	影響なし。	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。
	1つのピアがオンラインになるまでドロップされる。	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。

FTD の導入	トラフィックの挙動	メソッド
シャーン間クラス タ	影響なし。	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 つのシャーンを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。	ある時点ですべてのモジュールを停止するため、シャーンを同時にアップグレードします。
シャーン内クラス タ (FirePOWER 9300 のみ)	検査なしで受け渡される。	ハードウェアバイパス有効：[Bypass: Standby] または [Bypass-Force]。
	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無効：[Bypass: Disabled]。
	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。

FMC を使用した FTD アップグレードのトラフィックフローとインスペクション

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 16: トラフィックフローとインスペクション：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	トラフィックの挙動
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 ISA 3000 のブリッジグループインターフェイスの場合に限り、FlexConfig ポリシーを使用して、停電時のハードウェアバイパスを設定できます。これにより、ソフトウェアのアップグレード中にトラフィックのドロップが発生しますが、デバイスがアップグレード後の再起動中、インスペクションなしでトラフィックが通過します。

インターフェイス コンフィギュレーション	トラフィックの挙動	
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：[バイパス (Bypass)]：[強制 (Force)]	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します。
	インラインセッ、ハードウェアバイパスがスタンバイモード：[バイパス (Bypass)]：[スタンバイ (Standby)]	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：[バイパス (Bypass)]：[無効 (Disabled)]	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。

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。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ブルーニングすることがあります。

ソフトウェアのアンインストール（パッチ）

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。

設定変更の導入

Snort プロセスを再起動すると、高可用性/拡張性を備えた構成になっているものを含め、すべてのデバイスでトラフィックフローとインスペクションが一時的に中断されます。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。Snort を再起動せずに展開すると、リソース要求時にいくつかのパケットが検査なしでドロップされることがあります。

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。

表 17: トラフィックフローとインスペクション：設定変更の展開

インターフェイス コンフィギュレーション		トラフィックの挙動
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、[フェールセーフ (Failsafe)] が有効または無効。	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、[Snortフェールオープン：ダウン (Snort Fail Open: Down)]：無効	廃棄
	インライン、[Snortフェールオープン：ダウン (Snort Fail Open: Down)]：有効	検査なしで受け渡される。
	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。

FDM を使用した FTD アップグレードのトラフィックフローとインスペクション

ソフトウェアのアップグレード

アップグレード中にトラフィックがドロップされます。高可用性の展開では、デバイスを1つずつアップグレードすることで、中断を最小限に抑えることができます。

ISA 3000 の場合にのみ、電源障害に対するハードウェアバイパスを設定すると、トラフィックはアップグレード中にドロップされますが、デバイスのアップグレード後の再起動中に検査なしでトラフィックが渡されます。

設定変更の導入

Snort プロセスを再起動すると、高可用性を備えた構成になっているものを含め、すべてのデバイスでトラフィックフローとインスペクションが一時的に中断されます。Snort を再起動せずに展開すると、リソース要求時にいくつかの packets が検査なしでドロップされることがあります。

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。

ASA FirePOWER のアップグレードでのトラフィックフローとインスペクション

ソフトウェアのアップグレード

ASA FirePOWER モジュールへのトラフィックリダイレクトに関する ASA サービスポリシーによって、モジュールが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が決定されます。

表 18: トラフィックフローとインスペクション : ASA FirePOWER のアップグレード

トラフィック リダイレクト ポリシー	トラフィックの挙動
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

ソフトウェアのアンインストール（パッチ）

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。ASA フェールオーバーおよびクラスタの展開では、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。

設定変更の導入

Snort プロセスを再開すると、一時的にトラフィックフローと検査が中断されます。Snort プロセスが再起動している間のトラフィックの挙動は、ASA FirePOWER をアップグレードする場合と同じです。Snort を再起動せずに展開すると、リソース要求時にいくつかのパケットが検査なしでドロップされることがあります。

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。

FMC を使用した NGIPSv のアップグレードでのトラフィックフローとインスペクション

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 NGIPSv がトラフィックを処理する方法が決定されます。

表 19: トラフィックフローとインスペクション: NGIPSv 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	トラフィックの挙動
インライン	廃棄
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。

ソフトウェアのアンインストール（パッチ）

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。

設定変更の導入

Snort プロセスを再開すると、一時的にトラフィックフローと検査が中断されます。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。Snort を再起動せずに展開すると、リソース要求時にいくつかのパケットが検査なしでドロップされることがあります。

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。

表 20: トラフィックフローとインスペクション：設定変更の展開

インターフェイス コンフィギュレーション	トラフィックの挙動
インライン、[フェールセーフ (Failsafe)] が有効または無効	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、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、FMC およびソフトウェアのアップグレードにかかる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 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。

表 21: 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	デバイスアップグレードの時間は、FMC展開でのテストに基づいています。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。 高可用性の構成またはクラスタ化された構成では、動作の継続性を保持するため、複数のデバイスは1つずつアップグレードされます。アップグレード中は、各デバイスはメンテナンスモードで動作します。そのため、デバイスペアまたはクラスタ全体のアップグレードには、スタンドアロンデバイスのアップグレードよりも長い時間がかかります。
設定	シスコでは、構成およびトラフィック負荷が最小限のアプライアンスでテストを行います。 アップグレード時間は、構成の複雑さ、イベントデータベースのサイズ、また、それらがアップグレードから影響を受けるかどうか、受ける場合はどのような影響を受けるかにより、長くなる場合があります。たとえば多くのアクセス制御ルールを使用している場合、アップグレードはこれらのルールの格納方法をバックエンドで変更する必要があるため、アップグレードにはさらに長い時間がかかります。
コンポーネント	ソフトウェアアップグレード自体とその後の再起動のみの時間を報告します。これには、オペレーティングシステムのアップグレード、アップグレードパッケージの転送、準備状況チェック、VDB および侵入ルール (SRU/LSP) の更新、または設定の展開のための時間は含まれません。

ディスク容量テスト

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

また、デバイスアップグレードパッケージ用に FMC (Volume または /var 内) に必要な容量も報告します。FTD アップグレードパッケージ用の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。

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。

表 22: ディスク容量の確認

プラットフォーム	コマンド
FMC	[システム (System)] > [モニタリング (Monitoring)] > [統計 (Statistics)] を選択し、FMC を選択します。[ディスク使用率 (Disk Usage)] で、[By Partition] の詳細を展開します。
FTD with FMC	[システム (System)] > [モニタリング (Monitoring)] > [統計 (Statistics)] を選択し、確認するデバイスを選択します。[ディスク使用率 (Disk Usage)] で、[By Partition] の詳細を展開します。
FTD with FDM	show disk CLI コマンドを使用します。

バージョン 6.6.7.1 の時間とディスク容量

表 23: バージョン 6.6.7.1 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	/var 内で 2.8 GB	/ 内で 20 MB	—	37 分	9 分
FMCv : VMware	/var 内で 3.4 GB	/ 内で 23 MB	—	35 分	7 分
Firepower 1000 シリーズ	—	/ngfw 内で 3.8 GB	870 MB	9 分	7 分
Firepower 2100 シリーズ	—	/ngfw 内で 2.9 GB	900 MB	7 分	13 分

バージョン 6.6.7 の時間とディスク容量

プラットフォーム	ボリュームの容量	必要容量	FMC の容量	アップグレード時間	リブート時間
Firepower 4100 シリーズ	—	/ngfw 内で 3.1 GB	680 MB	6 分	8 分
Firepower 4100 シリーズ コンテナインスタンス	—	/ngfw 内で 2.3 GB	680 MB	6 分	5 分
Firepower 9300	—	/ngfw 内で 3.2 GB	680 MB	5 分	10 分
FTD を搭載した ASA 5500-X シリーズ	/home 内で 3.1 GB	/ngfw 内で 120 MB	630 MB	10 分	16 分
FTDv : VMware	/home 内で 2.5 GB	/ngfw 内で 120 MB	630 MB	7 分	6 分
ASA FirePOWER	/var 内で 2.9 GB	/ 内で 21 MB	430 MB	22 分	6 分
NGIPSv	/var 内で 940 MB	/ 内で 19 MB	290 MB	6 分	6 分

バージョン 6.6.7 の時間とディスク容量

表 24: バージョン 6.6.7 の時間とディスク容量

プラットフォーム	ボリュームの容量	必要容量	FMC の容量	アップグレード時間	リブート時間
FMC	/var 内で 17.0 GB	/ 内で 23 MB	—	49 分	14 分
FMCv : VMware	/var 内で 20.1 GB	/ 内で 29 MB	—	48 分	7 分
Firepower 1000 シリーズ	—	/ngfw 内で 10.4 GB	1.0 GB	19 分	18 分
Firepower 2100 シリーズ	—	/ngfw 内で 10.3 GB	1.0 GB	17 分	15 分
Firepower 4100 シリーズ	—	/ngfw 内で 10.1 GB	970 MB	10 分	11 分
Firepower 4100 シリーズ コンテナインスタンス	—	/ngfw 内で 10.4 GB	970 MB	10 分	8 分
Firepower 9300	—	/ngfw 内で 10.2 GB	970 MB	14 分	10 分

プラットフォーム	ボリュームの容量	必要容量	FMC の容量	アップグレード時間	リポート時間
FTD を搭載した ASA 5500-X シリーズ	/home 内で 8.6 GB	/ngfw 内で 752 KB	1.2 GB	22 分	22 分
FTDv : VMware	/home 内で 9.3 GB	/ngfw 内で 752 KB	1.2 GB	13 分	20 分
ASA FirePOWER	/var 内で 12 GB	/ 内で 26 MB	1.3 GB	73 分	16 分
NGIPSv	/var 内で 7.4 GB	/ 内で 21 MB	870 MB	12 分	7 分

バージョン 6.6.5.2 の時間とディスク容量

表 25: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	リポート時間
FMC	/var 内で 2.8 GB	/ 内で 20 MB	—	39 分	8 分
FMCv : VMware	/var 内で 3.4 GB	/ 内で 23 MB	—	26 分	8 分
Firepower 1000 シリーズ	—	/ngfw 内で 3.0 GB	630 MB	8 分	12 分
Firepower 2100 シリーズ	—	/ngfw 内で 2.9 GB	660 MB	7 分	12 分
Firepower 9300	—	/ngfw 内で 2.4 GB	430 MB	5 分	8 分
Firepower 4100 シリーズ	—	/ngfw 内で 2.9 GB	430 MB	6 分	8 分
Firepower 4100 シリーズ コンテナインスタンス	—	/ngfw 内で 2.5 GB	430 MB	5 分	6 分
FTD を搭載した ASA 5500-X シリーズ	/home 内で 2.2 GB	/ngfw 内で 120 MB	380 MB	10 分	15 分
FTDv : VMware	/home 内で 1.8 GB	/ngfw 内で 120 MB	380 MB	5 分	6 分
ASA FirePOWER	/var 内で 2.9 GB	/ 内で 21 MB	450 MB	68 分	22 分
NGIPSv	/var 内で 920 MB	/ 内で 19 MB	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 26: 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	/var 内で 2.2 GB	/ 内で 20 MB	—	34 分	8 分
FMCv : VMware	/var 内で 2.2 GB	23 MB	—	28 分	6 分
Firepower 1000 シリーズ	—	/ngfw 内で 1.5 GB	340 MB	8 分	12 分
Firepower 2100 シリーズ	—	/ngfw 内で 1.4 GB	370 MB	6 分	11 分
Firepower 9300	—	/ngfw 内で 770 MB	140 MB	5 分	8 分
Firepower 4100 シリーズ	—	/ngfw 内で 790 MB	140 MB	5 分	8 分
Firepower 4100 シリーズ コンテナインスタンス	—	/ngfw 内で 730 MB	140 MB	6 分	5 分
FTD を搭載した ASA 5500-X シリーズ	/home 内で 590 MB	/ngfw 内で 120 MB	85 MB	9 分	9 分
FTDv : VMware	/home 内で 590 MB	/ngfw 内で 120 MB	85 MB	6 分	5 分
ASA FirePOWER	/var 内で 1.7 GB	/ 内で 21 MB	130 MB	69 分	7 分
NGIPSv	/var 内で 78 MB	/ 内で 19 MB	16 MB	6 分	5 分

バージョン 6.6.5 の時間とディスク容量

表 27: バージョン 6.6.5 の時間とディスク容量

プラットフォーム	ボリュームの容量	必要容量	FMC の容量	アップグレード時間	リブート時間
FMC	/var 内で 16.5 GB	/ 内で 23 MB	—	55 分	14 分
FMCv : VMware	/var 内で 21 GB	/ 内で 29 MB	—	51 分	9 分

プラットフォーム	ボリュームの容量	必要容量	FMC の容量	アップグレード時間	リポート時間
Firepower 1000 シリーズ	/ngfw/var 内で 9.7 GB	/ngfw 内で 400 MB	1.1 GB	20 分	16 分
Firepower 2100 シリーズ	/ngfw/var 内で 10.2 GB	/ngfw 内で 450 MB	1.1 GB	17 分	15 分
Firepower 9300	10.2 GB /ngfw/var 内で 11	/ngfw 内で MB	1.1 GB	12 分	10 分
Firepower 4100 シリーズ	/ngfw/var 内で 10.1 MB	/ngfw 内で 10 MB	1.1 GB	10 分	11 分
Firepower 4100 シリーズコンテナインスタンス	/ngfw/var 内で 10.7 GB	/ngfw 内で 11 MB	1.1 GB	12 分	7 分
FTD を搭載した ASA 5500-X シリーズ	/ngfw/var 内で 8.6 GB	/ngfw 内で 756 KB	1.3 GB	22 分	30 分
FTDv : VMware	/ngfw/var 内で 9.1 GB	/ngfw 内で 756 KB	1.3 GB	12 分	21 分
ASA FirePOWER	/var 内で 12 GB	/ 内で 26 MB	1.4 GB	65 分	25 分
NGIPSv	7.4 GB /var 内で 21	MB/内	910 MB	12 分	21 分

バージョン 6.6.4 の時間とディスク容量

表 28:バージョン 6.6.4 の時間とディスク容量

プラットフォーム	ボリュームの容量	必要容量	FMC の容量	アップグレード時間	リポート時間
FMC	/var 内で 15.1 GB	/ 内で 23 MB	—	60 分	28 分
FMCv : VMware	/var 内で 23.7 GB	/ 内で 29 MB	—	43 分	8 分
Firepower 1000 シリーズ	/ngfw/var 内で 9.7 GB	/ngfw 内で 400 MB	1 GB	21 分	16 分
Firepower 2100 シリーズ	/ngfw/var 内で 10.1 GB	/ngfw 内で 450 MB	1 GB	21 分	13 分

バージョン 6.6.3 の時間とディスク容量

プラットフォーム	ボリュームの容量	必要容量	FMC の容量	アップグレード時間	リブート時間
Firepower 9300	/ngfw/var 内で 10.1 GB	/ngfw 内で 11 MB	970 MB	14 分	10 分
Firepower 4100 シリーズ	/ngfw/var 内で 8.9 GB	/ngfw 内で 11 MB	970 MB	11 分	9 分
Firepower 4100 シリーズ コンテナインスタンス	/ngfw/var 内で 10.9 GB	/ngfw 内で 10 MB	970 MB	10 分	7 分
FTD を搭載した ASA 5500-X シリーズ	/ngfw/var 内で 8.5 GB	/ngfw 内で 756 KB	1.2 GB	20 分	19 分
FTDv : VMware	/ngfw/var 内で 7.7 GB	/ngfw 内で 756 KB	1.2 GB	19 分	12 分
ASA FirePOWER	/var 内で 11.4 GB	/ 内で 26 MB	1.3 GB	59 分	16 分
NGIPSv	/var 内で 7.4 GB	/ 内で 21 MB	870 MB	13 分	8 分

バージョン 6.6.3 の時間とディスク容量

表 29: バージョン 6.6.3 の時間とディスク容量

プラットフォーム	ボリュームの容量	必要容量	FMC の容量	アップグレード時間	リブート時間
FMC	/var 内で 15.1 GB	/ 内で 23 MB	—	60 分	28 分
FMCv : VMware	/var 内で 23.7 GB	/ 内で 29 MB	—	43 分	8 分
Firepower 1000 シリーズ	/ngfw/var 内で 9.7 GB	/ngfw 内で 400 MB	1 GB	21 分	16 分
Firepower 2100 シリーズ	/ngfw/var 内で 10.1 GB	/ngfw 内で 450 MB	1 GB	21 分	13 分
Firepower 4100 シリーズ	/ngfw/var 内で 8.9 GB	/ngfw 内で 11 MB	970 MB	11 分	9 分
Firepower 4100 シリーズ コンテナインスタンス	/ngfw/var 内で 10.9 GB	/ngfw 内で 10 MB	970 MB	10 分	7 分

プラットフォーム	ボリュームの容量	必要容量	FMC の容量	アップグレード時間	リブート時間
Firepower 9300	/ngfw/var 内で 10.1 GB	/ngfw 内で 11 MB	970 MB	14 分	10 分
FTD を搭載した ASA 5500-X シリーズ	/ngfw/var 内で 8.5 GB	/ngfw 内で 756 KB	1.2 GB	20 分	19 分
FTDv : VMware	/ngfw/var 内で 7.7 GB	/ngfw 内で 756 KB	1.2 GB	19 分	12 分
ASA FirePOWER	/var 内で 11.4 GB	/内で 26 MB	1.3 GB	59 分	16 分
NGIPSv	/var 内で 7.4 GB	/内で 21 MB	870 MB	13 分	8 分

バージョン 6.6.1 の時間とディスク容量

表 30:バージョン 6.6.1 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	18.6 GB	23 MB	—	54 分	14 分
FMCv : VMware	15.8 GB	58 MB	—	56 分	13 分
Firepower 1000 シリーズ	10.8 GB	400 MB	1.1 GB	20 分	17 分
Firepower 2100 シリーズ	10.9 GB	450 MB	1.1 GB	16 分	21 分
Firepower 4100 シリーズ	9.7 GB	10 MB	1 GB	15 分	14 分
Firepower 4100 シリーズ コンテナインスタンス	11.2 GB	9 MB	1 GB	10 分	13 分
Firepower 9300	9.8 GB	11 MB	1 GB	15 分	15 分
FTD を搭載した ASA 5500-X シリーズ	9.3 GB	1 MB	1.2 GB	21 分	24 分
FTDv : VMware	9.3 GB	1 MB	1.2 GB	18 分	19 分

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	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
ASA FirePOWER	12.3 GB	26 MB	1.4 GB	72 分	23 分
NGIPSv	7.1 GB	54 MB	860 MB	14 分	20 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 31: 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	ボリュームの容量	必要容量	FMC の容量	アップグレードおよび再起動時間
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 4100 シリーズ	470 MB	470 MB	46 MB	11 分
Firepower 9300	460 MB	460 MB	46 MB	33 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

バージョン 6.6.0 の時間とディスク容量



(注) ASA 5545-X with FirePOWER Services では、デバイス上の SRU がバージョン 6.6.0 アップグレードパッケージ (2020-01-16-001-vrt) と同じか、またはそれよりも新しい場合は、想定よりもアップグレードに時間がかかる場合があります (1 時間以上)。これによる影響があるかどうかを判断するには、デバイス上の Firepower CLI にログインし、**show version** コマンドを使用してルールの更新バージョンを表示します。

表 32:バージョン 6.6.0 の時間とディスク容量

プラットフォーム	ボリュームの容量	必要容量	FMC の容量	アップグレード時間	リブート時間
FMC	/var 内で 16.5 GB	71 MB/内	—	46 分	15 分
FMCv : VMware	/var 内で 16.7 GB	57 MB/内	—	36 分	7 分
Firepower 1000 シリーズ	/ngfw/var 内で 410 MB	/ngfw 内で 11.5 GB	1.1 GB	20 分	17 分
Firepower 2100 シリーズ	/ngfw/var 内で 470 MB	/ngfw 内で 10.3 GB	1 GB	14 分	14 分
Firepower 4100 シリーズ	/ngfw/var 内で 61 MB	/ngfw 内で 9.3 GB	980 MB	11 分	9 分
Firepower 4100 シリーズコンテナインスタンス	/ngfw/var 内で 46 MB	/ngfw 内で 11.3 GB	980 MB	11 分	6 分
Firepower 9300	/ngfw/var 内で 64 MB	/ngfw 内で 8.7 GB	980 MB	15 分	12 分
FTD を搭載した ASA 5500-X シリーズ	/ngfw/var 内で 8.7 GB	/ngfw 内で 70 KB	1.2 GB	23 分	26 分
FTDv : VMware	/ngfw/var 内で 8.7 GB	/ngfw 内で 70 KB	1.2 GB	14 分	17 分
ASA FirePOWER	/var 内で 11.4 GB	63 MB/内	1.4 GB	93 分	10 分
NGIPSv	/var 内で 6.1 GB	53 MB/内	860 MB	10 分	5 分

翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。