ソフトウェアのアップグレード

このドキュメントには、Version7.0 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が、

重要 ここに記載されているガイドラインに加えて、以下の内容も確認する必要があります。

- 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、未解決および解決済みのバグについてのリリースノートを参照するか、Cisco バグ検索ツールを使用してください。
- 特長と機能：新規および廃止された機能が原因で、アップグレード前またはアップグレード後の設定変更が必要になったり、アップグレードができなかったりする場合があります。アップグレードでバージョンがスキップされる場合は、リリースノートで履歴情報とアップグレードの影響を確認するか、該当する『New Features by Release』のガイドを参照してください。

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-70-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。
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 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

次のように Version7.0 に直接アップグレードできます。

Version7.0 にパッチを適用する場合、パッチは4桁目のみを変更することに注意してください。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。

表 *2 : Version7.0* 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	6.4.0
FTD	6.4.0 Firepower 4100/9300 には FXOS 2.10.1.159 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, 2.10(1)』を参照してください。
ASA with FirePOWER サービス	6.4.0 ASA 9.5(2) ～ 9.16(x) が必要です。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	6.4.0

Version7.0 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 *Version7.0*

✓	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
	アップグレードする最小バージョン （2 ページ）	いずれか（Any）	いずれか（Any）	7.0
	FXOS のアップグレードガイドライン （16 ページ）	Firepower 4100/9300	任意（Any）	7.0
	高可用性 FMC の Cisco Threat Grid に再接続する （4 ページ）	FMC	6.4.0 ー 6.7.x	7.0.0 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 1010 スイッチポートでの無効な VLAN ID （5 ページ）	Firepower 1010	6.4.0 ～ 6.6.x	6.7.0 以降
	FMCv には 28 GB の RAM が必要（5 ページ）	FMCv	6.2.3 ～ 6.5.0.x	6.6.0 +
	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 （7 ページ）	Firepower 1000 シリーズ	6.4.0	6.5.0 以降
	新しいURL カテゴリとレピュテーション （7 ページ）	任意（Any）	6.2.3 ～ 6.4.0.x	6.5.0 以降

表 *4 : FDM* を使用した *FTD* のアップグレードガイドライン*Version7.0*

✓	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
	アップグレードする最小バージョン （2 ページ）	いずれか（Any）	いずれか（Any）	7.0
	FXOS のアップグレードガイドライン （16 ページ）	Firepower 4100/9300	いずれか（Any）	7.0
	アップグレードの失敗：Firepower 1010 スイッチポートでの無効な VLAN ID （5 ページ）	Firepower 1010	6.4.0 ～ 6.6.x	6.7.0 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 （7 ページ）	Firepower 1000 シリーズ	6.4.0	6.5.0 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（7 ページ）	任意（Any）	6.2.3 ～ 6.4.0.x	6.5.0 以降
	新しいURL カテゴリとレピュテーション （7 ページ）	任意（Any）	6.2.3 ～ 6.4.0.x	6.5.0 以降

高可用性 FMC の Cisco Threat Grid に再接続する

展開：動的分析のためにファイルを送信する高可用性/AMP for Networks（マルウェア検出）展開

アップグレード元：バージョン 6.4.0 ～ 6.7.x

直接アップグレード先：バージョン 7.0.0 以降

関連するバグ： CSCvu35704

バージョン 7.0.0 では、フェールオーバー後にシステムが動的分析用のファイルの送信を停止する高可用性の問題が修正されています。修正を有効にするには、Cisco Threat Grid パブリッククラウドに再度関連付ける必要があります。

高可用性ペアをアップグレードした後、プライマリ FMC で次の手順を実行します。

1. **[AMP]** > **[ダイナミック分析接続（Dynamic Analysis Connections）]**を選択します。
2. パブリッククラウドに対応するテーブル行で、 [関連付け（Associate）] をクリックします。

   ポータルウィンドウが開きます。サインインする必要はありません。再関連付けは、数分以内にバックグラウンドで行われます。

アップグレードの失敗：Firepower1010スイッチポートでの無効なVLAN ID

展開：Firepower 1010

アップグレード元：バージョン 6.4 ～ 6.6

直接アップグレード先：バージョン 6.7 以降

Firepower 1010 では、VLAN ID を 3968 ー 4047 の範囲にしてスイッチポートを設定した場合、FTD のバージョン 6.7 以降へのアップグレードは失敗します。これらの ID は内部使用専用です。

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 スタートアップ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。 • 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。
Azure	インスタンスのサイズを変更します。 • Standard_D3_v2 から Standard_D4_v2 へ。	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。 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。

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。	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。 • アクセス コントロール • SSL • QoS（FMC のみ） • 相関（FMC のみ） 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。

変更内容	詳細
URL ルールのレピュテーションの名前が変更されます。	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。 **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。	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。
「レガシー」イベントにラベルを付けます。	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。

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
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。	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できる必要があります。 • 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 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。 • IPv4 クラウドクエリ： • 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： • 2a04:e4c7:ffff::/48 • 2a04: e4c7: fffe::/48

アクション	詳細
潜在的なルールの問題を特定します。	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）。 （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。 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。

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
廃止されたカテゴリをルールから削除します。必須。	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。 FMC では、これらのルールがマークされます。
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。	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。 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。

アクション	詳細
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。	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（12 ページ）」を参照してください。 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プ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。
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。	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。 これらの変更はマークされません。
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。	特に対処の必要はありませんが、これらの変更に注意する必要があります。 これらの変更はマークされません。
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。	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。 [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。

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	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。 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。
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	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。 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。 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。 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。
ルール内の他の URL カテゴリ	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。
ルール内の非 URL 条件	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。

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	ルール 1 にはカテゴリ A が含まれる。 ルール 2 にはカテゴリ B が含まれる。	ルール 1 にはカテゴリ AB が含まれる。 ルール 2 にはカテゴリ AB が含まれる。 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。
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）	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。 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）	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。 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。 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。 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。
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	ルール 1 には次が含まれます。 レピュテーション Any のカテゴリ A レピュテーション 1-3 のカテゴリ B	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。
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	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。 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。	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。 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。 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。 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。

Version7.0 パッチ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パッチのアップグレードガイドラインを提供します。

表 *11 : FMC Version7.0* パッチのアップグレードガイドライン

✓	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
	アップグレードする最小バージョン （2 ページ）	いずれか（Any）	いずれか（Any）	任意のパッチ
	アンインストールに対応するパッチ （18 ページ）	いずれか（Any）	いずれか（Any）	任意のパッチ

表 *12 : FDM Version7.0* パッチのアップグレードガイドライン

✓	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
	アップグレードする最小バージョン （2 ページ）	いずれか（Any）	いずれか（Any）	任意のパッチ

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することもできます。

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

Version7.0 を実行するために必要な FXOS の最小バージョンは、FXOS 2.10.1.159 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 （19 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、設定を変更または展開しないでください。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。

応答しない FMC または従来のデバイスのアップグレード

進行中のアップグレードは再開しないでください。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。

応答しない FTD のアップグレード

メジャーアップグレードやメンテナンスアップグレードでは、失敗したアップグレードまたは進行中のアップグレードを手動でキャンセルし、失敗したアップグレードを再試行できます。

- FMC：[デバイス管理（Device Management）] ページおよびメッセージセンターからアクセスできる [アップグレードステータス（Upgrade Status）] ポップアップを使用します。
- FDM：[システムアップグレード（System Upgrade）] パネルを使用します。

FTD CLI を使用することもできます。

（注） デフォルトでは、FTDはアップグレードが失敗すると自動的にアップグレード前の状態に復元されます（「自動キャンセル」）。失敗したアップグレードを手動でキャンセルまたは再試行できるようにするには、アップグレードを開始するときに自動キャンセルオプションを無効にします。パッチの自動キャンセルはサポートされていません。高可用性または拡張性の展開では、自動キャンセルは各デバイスに個別に適用されます。つまり、1 つのデバイスでアップグレードが失敗した場合、そのデバイスだけが元に戻ります。

この機能は、パッチまたはバージョン 6.6 以前からのアップグレードではサポートされていません。

アップグレードを元に戻すまたはアンインストールする

アップグレードに成功したにもかかわらず、システムが期待どおりに機能しない場合は、復元またはアンインストールが可能な場合があります。

- メジャーおよびメンテナンスアップグレードを FTD に復元することができます。
- アンインストールは、FMC を搭載した FTD へのパッチが対象です。FMC パッチをアンインストールすることもできます。

これらの方法のいずれも機能しない場合、以前のバージョンに戻すには、イメージを再作成する必要があります。ホットフィックスでは、復元もアンインストールもサポートされていないことに注意してください。 手順については、復元先のバージョンではなく、現在実行しているバージョンのアップグレードガイドを参照してください。

アンインストールに対応するパッチ

特定のパッチをアンインストールすると、アンインストールが成功した場合でも、問題が発生する可能性があります。次のような問題があります。

- アンインストール後に設定変更を展開できない
- オペレーティングシステムと ソフトウェアの間に互換性がなくなる
- セキュリティ認定コンプライアンスが有効な状態（CC/UCAPL モード）でそのパッチが適用されていた場合、アプライアンスの再起動時に FSIC（ファイル システム整合性チェック）が失敗する

⚠

注意 セキュリティ認定の遵守が有効な場合にFSICが失敗すると、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るため、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。

アンインストールに対応したバージョン 7.0 のパッチ

現在、すべてのバージョン 7.0 パッチがアンインストールに対応しています。

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。高可用性や拡張性を導入する場合でも、各シャーシの FXOS を個別にアップグレードします。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 *13 :* 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

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。
シャーシ間クラスタ	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 つのシャーシ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、シャーシを同時にアップグレードします。
シャーシ内クラスタ（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 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 *14:* 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 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。
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：[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。
	インラインセット、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。
	インラインセット、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。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。

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 *15*：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、[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。
	インラインセット、[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。

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。

ソフトウェアの復元（メジャーおよびメンテナンスリリース）

復元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、両方のユニットを同時に復元すると、復元が成功する可能性が高くなります。最初のユニットがオンラインに戻ると、トラフィックフローとインスペクションが再開されます。

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 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 *16* : 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 *17:* 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	トラフィックの動作
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 *18:* 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、設定を変更または展開しないでください。システムが非アクティブに見えても、手動で再起動またはシャットダウンしないでください。ほとんどの場合、進行中のアップグレードを再開しないでください。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応答しないアップグレード（17ページ）を参照してください。

表 *19*：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
展開	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。

条件	詳細
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 *20*：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。[Disk Usage] で、[By Partition] の詳細を展開します。

プラットフォーム	コマンド
FTD with FMC	**[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。
FTD with FDM	**show disk** CLI コマンドを使用します。

バージョン 7.0.3 の時間とディスク容量

表 *21 :* バージョン *7.0.3* 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 20 MB	—	52 分	7 分
FMCv：VMware		/var 内で 20.1 GB	/ 内で 29 MB	—	40 分	5 分
Firepower 1000 シリーズ		—	/ngfw 内で 6.7 GB	860 MB	16 分	16 分
Firepower 2100 シリーズ		—	/ngfw 内で 6.7 GB	910 MB	11 分	16 分
Firepower 4100 シリーズ		—	/ngfw 内で 6.9 GB	810 MB	12 分	10 分
Firepower 4100 シリーズ コンテナ インスタンス		—	/ngfw 内で 8.9 GB	810 MB	12 分	8 分
Firepower 9300		—	/ngfw 内で 7.0 GB	810 MB	15 分	11 分
FTD を搭載した ASA 5500-X シリーズ	バージョン 6.4.0 ～ 6.6.0	/home 内で 5.3 GB	/ngfw 内で 944 KB	1.0 GB	20 分	19 分
	バージョン 6.7.0	/ngfw/Volume 内で 5.3 GB	/ngfw 内で 200 KB			
	バージョン 7.0.0	/ngfw/var 内で 5.3 GB	/ngfw/bin 内で 300 MB			
FTDv：VMware	バージョン 6.4.0 ～ 6.6.0	/home 内で 5.3 GB	/ngfw 内で 936 KB	1.0 GB	12 分	9 分
	バージョン 6.7.0	/ngfw/Volume 内で 5.6 GB	/ngfw 内で 200 KB			
	バージョン 7.0.0	/ngfw/var 内で 5.7 GB	/ngfw/bin 内で 180 MB			
ASA FirePOWER		/var 内で 8.6 GB	/ 内で 26 MB	1.2 GB	58 分	7 分
NGIPSv		/var 内で 5.7 GB	/ 内で 21 MB	730 MB	10 分	7 分

バージョン 7.0.2.1 の時間とディスク容量

表 *22 :* バージョン *7.0.2.1* 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 GB	/ 内で 19 MB	—	30 分	4 分
FMCv：VMware	/var 内で 1.9 GB	/ 内で 13 MB	—	26 分	3 分
Firepower 1000 シリーズ	—	/ngfw 内で 1.4 GB	180 MB	7 分	9 分
Firepower 2100 シリーズ	—	/ngfw 内で 1.3 GB	180 MB	6 分	10 分
Firepower 4100 シリーズ	—	/ngfw 内で 1.4 GB	180 MB	5 分	7 分
Firepower 9300	—	/ngfw 内で 1.3 GB	180 MB	4 分	8 分
FTD を搭載した ASA 5500-X シリーズ	/ngfw/var 内で 900 MB	/ngfw/bin 内で 190 MB	190 MB	7 分	12 分
FTDv：VMware	/ngfw/var 内で 900 MB	/ngfw/bin 内で 190 MB	190 MB	4 分	5 分
ASA FirePOWER	/var 内で 950 MB	/ 内で 13 MB	55 MB	57 分	6 分
NGIPSv	/var 内で 42 MB	/ 内で 13 MB	9 MB	5 分	3 分

バージョン 7.0.2 の時間とディスク容量

表 *23 :* バージョン *7.0.2* の時間とディスク容量

プラットフォーム	ボリュームの容量	必要容量	FMC の容量	アップグレード時間	リブート時間
FMC	/var 内で 17.2 GB	/ 内で 20 MB	—	53 分	7 分
FMCv：VMware	/var 内で 17.2 GB	/ 内で 29 MB	—	40 分	5 分
Firepower 1000 シリーズ	—	/ngfw 内で 7.0 GB	560 MB	16 分	17 分
Firepower 2100 シリーズ	—	/ngfw 内で 6.7 GB	910 MB	11 分	16 分
Firepower 4100 シリーズ	—	/ngfw 内で 6.9 GB	810 MB	13 分	10 分
Firepower 4100 シリーズ コンテナ インスタンス	—	/ngfw 内で 8.2 GB	810 MB	12 分	6 分
Firepower 9300	—	/ngfw 内で 6.9 GB	810 MB	12 分	11 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
FTD を搭載した ASA 5500-X シリーズ	バージョン 6.4.0 ～ 6.6.0	/home 内で 5.7 GB	/ngfw 内で 944 KB	1.0 GB	18 分	19 分
	バージョン 6.7.0	/ngfw/Volume 内で 5.5 GB	/ngfw 内で 300 KB			
	バージョン 7.0.0	/ngfw/var 内で 5.3 GB	/ngfw/bin 内で 3.4 GB			
FTDv：VMware	バージョン 6.4.0 ～ 6.6.0	/home 内で 5.3 GB	/ngfw 内で 936 KB	1.0 GB	10 分	8 分
	バージョン 6.7.0	/ngfw/Volume 内で 5.5 GB	/ngfw 内で 200 KB			
	バージョン 7.0.0	/ngfw/var 内で 5.5 GB	/ngfw/bin 内で 180 MB			
ASA FirePOWER		/var 内で 8.0 GB	/ 内で 26 MB	1.2 GB	70 分	14 分
NGIPSv		/var 内で 5.8 GB	/ 内で 21 MB	730 MB	12 分	7 分

バージョン 7.0.1.1 の時間とディスク容量

表 *24 :* バージョン *7.0.1.1* 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 650 MB	/ 内で 29 MB	—	9 分	/ngfw に 2.5 GB
FMCv：VMware	/var 内で 770 MB	/ 内で 13 MB	—	9 分	/ngfw に 2.5 GB
Firepower 1000 シリーズ	—	/ngfw 内で 2.1 GB	300 MB	8 分	14 分
Firepower 2100 シリーズ	—	/ngfw 内で 2.1 GB	300 MB	7 分	使用できません
Firepower 4100 シリーズ	—	/ngfw 内で 1.4 GB	300 MB	5 分	8 分
Firepower 9300	—	/ngfw 内で 1.7 GB	300 MB	4 分	8 分
FTD を搭載した ASA 5500-X シリーズ	/ngfw/var 内で 1.3 GB	/ngfw/bin 内で 180 MB	310 MB	7 分	11 分
FTDv：VMware	/ngfw/var 内で 1.4 GB	/ngfw/bin 内で 180 MB	310 MB	4 分	5 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
ASA FirePOWER	/var 内で 760 MB	/ 内で 13 MB	250 MB	36 分	[1 分（1 min）]
NGIPSv	/var 内で 810 MB	/ 内で 13 MB	250 MB	5 分	3 分

バージョン 7.0.1 の時間とディスク容量

表 *25 :* バージョン *7.0.1* 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
FMC		/var 内で 17 GB	/ 内で 20 MB	—	51 分	8 分
FMCv：VMware		/var 内で 19.5 GB	/ 内で 29 MB	—	41 分	6 分
Firepower 1000 シリーズ		—	/ngfw 内で 7 GB	850 MB	17 分	25 分
Firepower 2100 シリーズ		—	/ngfw 内で 6.6 GB	900 MB	12 分	16 分
Firepower 4100 シリーズ		—	/ngfw 内で 6.9 GB	800 MB	12 分	11 分
Firepower 4100 シリーズ コンテナ インスタンス		—	/ngfw 内で 9.3 GB	800 MB	12 分	9 分
Firepower 9300		—	/ngfw 内で 6.8 GB	800 MB	16 分	10 分
FTD を搭載した ASA 5500-X シリーズ	バージョン 6.4.0 ～ 6.6.0	/home 内で 6 GB	/ngfw 内で 944 KB	1GB	17 分	18 分
	バージョン 6.7.0	/ngfw/Volume 内で 4 GB	/ngfw 内で 208 KB			
	バージョン 7.0.0	/ngfw/var 内で 5.4 GB	/ngfw/bin 内で 320 MB			
FTDv：VMware	バージョン 6.4.0 ～ 6.6.0	/home 内で 5.3 GB	/ngfw 内で 944 KB	1 GB	18 分	18 分
	バージョン 6.7.0	/ngfw/Volume 内で 4.7 GB	/ngfw 内で 200 KB			
	バージョン 7.0.0	/ngfw/var 内で 4.2 GB	/ngfw/bin 内で 175 MB			
ASA FirePOWER		/var 内で 8.6 GB	/ 内で 26 MB	1.1 GB	65 分	7 分
NGIPSv		/var 内で 4.5 GB	/ 内で 21 MB	720 MB	10 分	5 分

バージョン 7.0.0.1 の時間とディスク容量

表 *26 :* バージョン *7.0.0.1* 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
FMC	/var 内で 350 MB	/ 内で 19 MB	—	8 分	8 分
FMCv：VMware	/var 内で 66 MB	/ 内で 13 MB	—	9 分	/ngfw に 2.5 GB
Firepower 1000 シリーズ	—	/ngfw 内で 720 MB	47 MB	8 分	9 分
Firepower 2100 シリーズ	—	/ngfw 内で 710 MB	42 MB	6 分	10 分
Firepower 4100 シリーズ	—	/ngfw 内で 800 MB	47 MB	4 分	6 分
Firepower 9300	—	/ngfw 内で 860 MB	47 MB	4 分	32 分
FTD を搭載した ASA 5500-X シリーズ	/ngfw/var 内で 470 MB	/ngfw/bin 内で 170 MB	54 MB	6 分	10 分
FTDv：VMware	/ngfw/var 内で 490 MB	/ngfw/bin 内で 160 MB	54 MB	4 分	4 分
ASA FirePOWER	/var 内で 54 MB	/ 内で 13 MB	8 MB	39 分	4 分
NGIPSv	/var 内で 66 MB	/ 内で 13 MB	8 MB	5 分	3 分

バージョン 7.0.0 の時間とディスク容量

表 *27 :* バージョン *7.0.0* 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 14 GB	/ 内で 70 MB	—	41 分	7 分
FMCv：VMware	/var 内で 16 GB	/ 内で 72 MB で	—	28 分	4 分
Firepower 1000 シリーズ	/ngfw/var 内で 420 MB	/ngfw 内で 7.6 GB	890 MB	12 分	14 分
Firepower 2100 シリーズ	/ngfw/var 内で 480 MB	/ngfw 内で 7.7 GB	950 MB	11 分	13 分
Firepower 4100 シリーズ	/ngfw/var 内で 40 MB	/ngfw 内で 8.4 GB	830 MB	8 分	9 分
Firepower 4100 シリーズ コンテナ インスタンス	/ngfw/var 内で 36 MB	/ngfw 内で 9.7 GB	830 MB	8 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 45 MB	/ngfw 内で 11.1 GB	830 MB	11 分	11 分
FTD を搭載した ASA 5500-X シリーズ	/ngfw/var 内で 5.3 GB	/ngfw 内で 95 KB	1.1 GB	25 分	12 分
FTDv：VMware	/ngfw/var 内で 6.6 GB	/ngfw 内で 23 KB	1.1 GB	11 分	6 分
ASA FirePOWER	/var 内で 9.5 GB	/ 内で 64 MB	1.1 GB	69 分	8 分
NGIPSv	/var 内で 5 GB	/ 内で 54 MB	720 MB	8 分	4 分