# ソフトウェアのアップグレードガイドライン

利便性を考え、このドキュメントには、FTDリリースノートで公開されている重要なリリース固有のソフトウェアのアップグレードガイドラインを複製したものが記載されてます。Firepower 4100/9300 の FXOS アップグレードガイドラインについては、FXOS のアップグレードガイドライン を参照してください。

**重要** リリースノートにも目を通してください。重要な追加情報やバージョン固有の情報が記載されている場合があります。たとえば、新機能や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に設定の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。または、既知の問題（未解決のバグ）がアップグレードに影響することがあります。



# 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 7.1 に直接アップグレードできます。

**表 *1*: バージョン *7.1* 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 | 6.5 |

| プラットフォーム | 最小バージョン |
|---|---|
| FTD | 6.5<br><br>Firepower 4100/9300 には FXOS 2.11.1.154 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, 2.11(1）を参照してください。 |

### 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。

# クラウド提供型 Firewall Management Center のガイドライン

クラウド提供型 Firewall Management Center はアップグレード対象外です。 にはバージョンがないため、機能の更新はシスコが行います。

### クラウド提供型 Firewall Management Center を使用した FTD のアップグレード

クラウド提供型 Firewall Management Center を使用して FTD をアップグレードするには、Firepower Management Center 用 Cisco Firepower Threat Defense アップグレードガイド の最新リリースバージョンを使用します。

（注） クラウド提供型 Firewall Management Center では FTD バージョン 7.1 を管理できません。クラウド管理の登録を解除して無効にしない限り、クラウド管理型デバイスをバージョン 7.0 からバージョン 7.1 にアップグレードできません。バージョン 7.2 以降に直接アップグレードすることをお勧めします。

### 共同管理デバイスのアップグレード

お客様が導入した FMC バージョン 7.2 以降を実行しているハードウェアでは、クラウド管理型の FTD デバイスを共同管理できますが、用途はイベントのロギングと分析に限られます。クラウド提供型 Firewall Management Center を使用して、アップグレードを含む FTD のすべての側面を管理および設定する必要があります。

お客様が導入した FMC では、その管理対象デバイスと同じまたはそれ以降のバージョンを実行する必要があります。これには クラウド提供型 Firewall Management Center によって共同管理されるデバイスも含まれます。つまり、クラウド提供型 Firewall Management Center を使用し

て、お客様が導入した FMC より新しいバージョンに共同管理デバイスをアップグレードすることはできません。

たとえば、2 つのマネージャを持つ Threat Defense デバイスがあるとします。

- バージョン A を実行しているデバイスがあります。
- お客様が導入した FMC では、バージョン B を実行しています。
- クラウド提供型 Firewall Management Center にはバージョンがありません。

このシナリオでは、クラウド提供型 Firewall Management Center を使用してデバイスをバージョン B（共同マネージャと同じバージョン）にアップグレードできますが、バージョン C（共同マネージャより新しいバージョン）にはアップグレードできません。

# バージョン 7.1 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 *2 : 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 *7.1***

| ✓ | 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 | 任意 | 任意 |
| | Cisco Firepower リリースノート：「*Open and Resolved Bugs*」の章に、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 | 任意 | 任意 |
| | アップグレードする最小バージョン （1 ページ） | 任意 | 任意 | 任意 |
| | FXOS のアップグレードガイドライン | Firepower 4100/9300 | 任意 | 任意 |

| ✓ | 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 |
|---|---|---|---|---|
| | アップグレード禁止：バージョン 7.0.4 以降から バージョン 7.1.0（4 ページ） | 任意（Any） | 7.0.4 以降 | 7.1.0 のみ |
| | 高可用性 FMC の Cisco Secure Malware Analytics に再接続する（4 ページ） | FMC | 6.4.0 ～ 6.7.x | 7.0 以上 |
| | 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 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 以降 |

# アップグレード禁止：バージョン 7.0.4 以降から バージョン 7.1.0

**展開**：すべて

**アップグレード元**：バージョン 7.0.4 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 7.1.0 のみ

データストアの非互換性のため、をバージョン 7.0.4 以降からバージョン 7.1.0 にアップグレードすることができません。バージョン 7.2 以降に直接アップグレードすることをお勧めします。

# 高可用性 FMC の Cisco Secure Malware Analytics 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 Secure Malware Analytics 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 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 *3:* 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。<br>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。<br>• c3.xlarge から c3.4xlarge へ。<br>• c3.2.xlarge から c3.4xlarge へ。<br>• c4.xlarge から c4.4xlarge へ。<br>• c4.2xlarge から c4.4xlarge へ。<br>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。<br>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。<br>• 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。<br>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。 |

# 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。

### 応答しない FMC

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 で、[デバイス管理（Device Management）] ページの [アップグレード（Upgrade）] タブ、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。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。高可用性またはクラスタ展開では、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。

# 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 *4:* 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。<br>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<br>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。

### ソフトウェアの復元（メジャーおよびメンテナンスリリース）

たとえ高可用性および拡張性を備えた環境でも、復元時のトラフィックフローとインスペクションの中断を予測する必要があります。これは、すべてのユニットを同時に復元させたほうが、復元がより正常に完了するためです。同時復元とは、すべてのデバイスがスタンドアロンであるかのように、トラフィックフローと検査の中断がインターフェイスの設定のみに依存することを意味します。

### 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 *5:* 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。<br>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 | | トラフィックの挙動 |
|---|---|---|
| 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。<br>[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。 |

# 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 （6 ページ） を参照してください。

表 *6:* 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。<br>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。<br>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 *7:* 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。 |

# バージョン 7.1.0.3 の時間とディスク容量

**表 *8:* バージョン *7.1.0.3* 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 2.9 GB | / 内で 29 MB | — | 20 分 | 7 分 |
| FMCv：VMware | /var 内で 4.0 GB | / 内で 25 MB | — | 23 分 | 6 分 |
| Firepower 1000 シリーズ | — | /ngfw 内で 3.2 GB | 1.0 GB | 9 分 | 13 分 |
| Firepower 2100 シリーズ | — | /ngfw 内で 3.2 GB | 1.1 GB | 7 分 | 14 分 |
| Secure Firewall 3100 シリーズ | — | /ngfw 内で 3.5 GB | 1.1 GB | 4 分 | 15 分 |
| Firepower 4100 シリーズ | — | /ngfw 内で 2.8 GB | 780 MB | 5 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 4100 シリーズ コンテナ インスタンス | — | /ngfw 内で 2.9 GB | 780 MB | 6 分 | 5 分 |
| Firepower 9300 | — | /ngfw 内で 2.3 GB | 780 MB | 5 分 | 10 分 |
| ISA 3000 | /ngfw/var 内で 1.7 GB | /ngfw/bin 内で 270 MB | 780 MB | 11 分 | 14 分 |
| FTDv：VMware | /ngfw/var 内で 2.1 GB | /ngfw/bin 内で 270 MB | 350 MB | 5 分 | 6 分 |

# バージョン 7.1.0.2 の時間とディスク容量

**表 *9*：バージョン *7.1.0.2* 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 2.0 GB | / 内で 19 MB | — | 20 分 | 4 分 |
| FMCv：VMware | /var 内で 2.5 GB | / 内で 14 MB | — | 21 分 | [1 分（1 min）] |
| Secure Firewall 3100 シリーズ | — | /ngfw 内で 3.2 GB | | 4 分 | 46 分 |

# バージョン 7.1.0.1 の時間とディスク容量

**表 *10*：バージョン *7.1.0.1* 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 2.0 GB | / 内で 19 MB | — | 18 分 | 8 分 |
| FMCv：VMware | /var 内で 2.2 GB | / 内で 14 MB | — | 21 分 | 4 分 |
| Firepower 1000 シリーズ | — | /ngfw 内で 5.6 GB | 430 MB | 10 分 | 11 分 |
| Firepower 2100 シリーズ | — | /ngfw 内で 5.6 GB | 420 MB | 10 分 | 10 分 |
| Firepower 4100 シリーズ | — | /ngfw 内で 5.6 GB | 430 MB | 7 分 | 7 分 |
| Firepower 4100 シリーズ コンテナ インスタンス | — | /ngfw 内で 5.6 GB | 430 MB | 6 分 | 4 分 |
| Firepower 9300 | — | /ngfw 内で 5.1 GB | 430 MB | 7 分 | 8 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 |
|---|---|---|---|---|---|
| ISA 3000 | /ngfw/var 内で 2.0 GB | /ngfw/bin 内で 240 MB | 430 MB | 4 分 | 13 分 |
| FTDv：VMware | /ngfw/var 内で 1.5 GB | /ngfw/bin 内で 240 MB | 430 MB | 4 分 | 4 分 |

# バージョン 7.1.0 の時間とディスク容量

**表 *11* : バージョン *7.1.0* 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 16.9 GB | / 内で 43 MB | — | 33 分 | 15 分 |
| FMCv：VMware | | /var 内で 17 GB | / 内で 50 MB で | — | 34 分 | 5 分 |
| Firepower 1000 シリーズ | | — | /ngfw 内で 8.2 GB | 930 MB | 16 分 | 11 分 |
| Firepower 2100 シリーズ | | — | /ngfw 内で 8.3 GB | 1 GB | 13 分 | 13 分 |
| Firepower 4100 シリーズ | | — | /ngfw 内で 8.6 GB | 870 MB | 15 分 | 9 分 |
| Firepower 4100 シリーズ コンテナ インスタンス | | — | /ngfw 内で 8.6 GB | 870 MB | 16 分 | 8 分 |
| Firepower 9300 | | — | /ngfw 内で 11.2 GB | 870 MB | 11 分 | 12 分 |
| ISA 3000 | バージョン 6.5 ～ 6.6 | /home 内で 9.3 GB | /ngfw 内で 256 KB | 1 GB | 21 分 | 8 分 |
| | バージョン 6.7 以降 | /ngfw/Volume 内で 9.3 GB | /ngfw 内で 270 KB | | | |
| | バージョン 7.0 以降 | /ngfw/var 内で 9.2 GB | /ngfw/bin 内で 260 KB | | | |
| FTDv：VMware | バージョン 6.5 ～ 6.6 | /home 内で 4.6 GB | /ngfw 内で 925 KB | 1 GB | 11 分 | 6 分 |
| | バージョン 6.7 以降 | /ngfw/Volume 内で 4.4 GB | /ngfw 内で 210 KB | | | |
| | バージョン 7.0 以降 | /ngfw/var 内で 5.3 GB | /ngfw/bin 内で 220 KB | | | |

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。