



ASA with FirePOWER サービスのアップグレード

- [アップグレードチェックリスト：FMC を搭載した ASA FirePOWER（1 ページ）](#)
- [ASA のアップグレード（6 ページ）](#)
- [FMC を使用した ASA FirePOWER モジュールのアップグレード（31 ページ）](#)

アップグレード チェックリスト：FMC を搭載した ASA FirePOWER

ASA with FirePOWER Services のアップグレードを行う前にこのチェックリストを完了します。



- (注) プロセス中は常に、展開の通信と正常性を維持してください。進行中に ASA FirePOWER のアップグレードを再開しないでください。事前のチェック中に、アップグレードプロセスが停止しているように見える場合がありますが、これは想定内の動作です。アップグレードに失敗する、アプライアンスが応答しないなど、アップグレードで問題が発生した場合にはCisco TAC にお問い合わせください。
-

計画と実現可能性

誤りを避けるには、注意深い計画と準備が役立ちます。

表 1:

✓	アクション/チェック
	アップグレードパスを計画します。 これは、マルチアプライアンス展開、マルチホップアップグレード、または展開の互換性を常に維持しながらオペレーティングシステムまたはホスティング環境をアップグレードする必要がある状況では特に重要です。実行したアップグレードと次に実行するアップグレードを常に確認します。 (注) FMC 展開では、通常、FMC をアップグレードしてから、管理対象デバイスをアップグレードします。ただし、場合によっては、最初にデバイスをアップグレードする必要があります。 アップグレードパスを参照してください。
	すべてのアップグレードのガイドラインを読み、設定の変更を計画します。 主要なアップグレードでは特に、アップグレードの前または後に、アップグレードにより重要な設定変更が発生することがあります。アップグレードの警告、動作の変更、新機能と廃止された機能、および既知の問題など、リリース固有の重要な情報を含むリリースノートから読み始めます。
	アプライアンスへのアクセスを確認します。 デバイスは、(インターフェイス設定に応じて) アップグレード中、またはアップグレードが失敗した場合に、トラフィックを渡すことを停止できます。アップグレードする前に、ユーザーの位置からのトラフィックがデバイスの管理インターフェイスにアクセスするためにデバイス自体を通過する必要がないことを確認してください。FMC の展開では、デバイスを経由せずに FMC 管理インターフェイスにアクセスできる必要もあります。
	帯域幅を確認します。 管理ネットワークに大量のデータ転送を実行するための帯域幅があることを確認します。FMC の展開では、アップグレードパッケージをアップグレード時に管理対象デバイスに転送する場合は、帯域幅が不十分だとアップグレード時間が長くなったり、アップグレードがタイムアウトする原因となったりする可能性があります。デバイスのアップグレードを開始する前に、可能な場合は常に、アップグレードパッケージを管理対象デバイスにコピーします。 『Guidelines for Downloading Data from the Firepower Management Center to Managed Devices』 (トラブルシューティング テクニカルノート) を参照してください。

✓	アクション/チェック
	メンテナンス時間帯をスケジュールします。 影響が最小限になるメンテナンス時間帯をスケジュールします。トラフィックフローおよびインスペクションへの影響、およびアップグレードにかかる可能性がある時間を考慮してください。また、ウィンドウで実行する必要があるタスクと、事前に実行できるタスクを検討します。たとえば、メンテナンス時間帯で、アプライアンスへのアップグレードパッケージのコピー、準備状況チェックの実行、バックアップの作成などが行われるまで待機しないようにします。

アップグレードパッケージ

アップグレードパッケージは シスコ サポート および ダウンロード サイト で入手できます。

表 2:

✓	アクション/チェック
	アップグレードパッケージを FMC にアップロードします。 Firepower Management Center にアップロード を参照してください。
	アップグレードパッケージをデバイスにコピーします。 FMC がバージョン 6.2.3 以降を実行している場合、デバイスのアップグレードを開始する前に、管理対象デバイスにパッケージをコピー（プッシュ）することをお勧めします。 管理対象デバイスへのコピー を参照してください。

バックアップ

災害から回復する能力は、システム保守計画の重要な部分を占めます。

バックアップと復元は、複雑なプロセスになる可能性があります。手順をスキップしたり、セキュリティやライセンスの問題を無視しないでください。バックアップと復元の要件、ガイドライン、制限事項、およびベストプラクティスの詳細については、使用する展開の設定ガイドを参照してください。



注意 アップグレードの前後に、安全な遠隔地にバックアップし、正常に転送が行われることを確認することを強くお勧めします。

表 3:

✓	アクション/チェック
	ASA をバックアップします。 ASDM または ASA CLI を使用して、アップグレードの前後に設定やその他の重要なファイルをバックアップしてます（特に ASA 設定の移行がある場合）。

関連するアップグレード

オペレーティングシステムとホスティング環境のアップグレードはトラフィックフローとインスペクションに影響を与える可能性があるため、メンテナンス時間帯で実行してください。

表 4:

✓	アクション/チェック
	ASA をアップグレードします。 必要に応じて、ASA をアップグレードします。ASA と ASA FirePOWER のバージョンには幅広い互換性があります。ただし、アップグレードすると、新機能を利用でき、問題も解決されます。 スタンドアロン ASA デバイスの場合、ASA をアップグレードしてリロードした直後に、ASA FirePOWER モジュールをアップグレードします。 ASA クラスタとフェールオーバーペアの場合、トラフィックフローとインスペクションの中断を避けるには、これらのデバイスを一度に 1 台ずつ完全にアップグレードします。各ユニットをリロードして ASA をアップグレードする直前に、ASA FirePOWER モジュールをアップグレードします。 （注） ASA をアップグレードする前に、必ずすべてのアップグレードのガイドラインを読み、設定の変更を計画してください。ASA リリースノート：Cisco ASA リリースノート を使用して開始します。

最終チェック

一連の最終チェックにより、をアップグレードする準備が整います。

表 5:

✓	アクション/チェック
	設定を確認します。 必要なアップグレード前の設定変更を行っていることを確認し、必要なアップグレード後の設定変更を行う準備をします。

✓	アクション/チェック
	NTP 同期を確認します。 時刻の提供に使用している NTP サーバーとすべてのアプライアンスが同期していることを確認します。同期されていないと、アップグレードが失敗する可能性があります。FMC 展開では、時刻のずれが 10 秒を超えている場合、ヘルスマニタからアラートが発行されますが、手動で確認する必要もあります。 時刻を確認するには、次の手順を実行します。 • FMC : [システム (System)] > [設定 (Configuration)] > [時刻 (Time)] を選択します。 • デバイス : show time CLI コマンドを使用します。
	ディスク容量を確認します。 ソフトウェアアップグレードに関するディスク容量チェックを実行します。空きディスク容量が十分でない場合、アップグレードは失敗します。 対象バージョンの Cisco Firepower リリース ノート 内の「ソフトウェアのアップグレード」の章を参照してください。
	設定を展開します。 アップグレードする前に設定を展開すると、失敗する可能性が減少します。一部の展開では、設定が古い場合、アップグレードがブロックされることがあります。FMC における高可用性の展開では、アクティブなピアから展開するだけで済みます。 展開する際にリソースを要求すると、いくつかのパケットがインスペクションなしでドロップされることがあります。さらに、いくつかの設定を展開することで Snort が再起動されます。これにより、トラフィックのインスペクションが中断し、デバイスのトラフィックの処理方法によっては、再起動が完了するまでトラフィックが中断する場合があります。 対象バージョンの Cisco Firepower リリース ノート 内の「ソフトウェアのアップグレード」の章を参照してください。
	古いデバイスで ASA REST API を無効化します。 現在、バージョン 6.3.0 以前を実行している ASA FirePOWER モジュールをアップグレードする前に、ASA REST API を無効にしていることを確認します。無効にしている場合、アップグレードが失敗することがあります。ASA CLI から :no rest api agent。アップグレード後に再度有効できます :rest-api agent。

✓	アクション/チェック
	準備状況チェックを実行します。 FMC がバージョン 6.1.0 以降を実行している場合は、互換性と準備状況のチェックの実施をお勧めします。これらのチェックにより、ソフトウェアをアップグレードするための準備状況を確認できます。 Firepower ソフトウェアの準備状況チェック を参照してください。
	実行中のタスクを確認します。 アップグレードする前に、デバイスの重要なタスク（最終展開を含む）が完了していることを確認します。アップグレードの開始時に実行中のタスクは停止し、失敗したタスクとなり、再開できません。また、アップグレード中に実行するようにスケジュールされたタスクを確認し、それらをキャンセルまたは延期することをお勧めします。

ASA のアップグレード

スタンドアロン、フェールオーバー、またはクラスタリング展開の ASA と ASDM をアップグレードするには、このセクションの手順を使用します。

スタンドアロンユニットのアップグレード

スタンドアロンユニットをアップグレードするには CLI または ASDM を使用します。

CLI を使用したスタンドアロンユニットのアップグレード

ここでは、ASDM イメージおよび ASA イメージをインストールする方法について説明します。また、ASA FirePower モジュールをアップグレードするタイミングについても説明します。

始める前に

この手順では、FTP を使用します。TFTP、HTTP、またはその他のサーバー タイプについては、『[ASA Command Reference](#)』の **copy** コマンドを参照してください。

手順

- ステップ 1** 特権 EXEC モードで、ASA ソフトウェアをフラッシュメモリにコピーします。
- ```
copy ftp://[[user[:password]]@]server[/path/]asa_image_name diskn:/[path/]asa_image_name
```
- 例 :

```
ciscoasa# copy ftp://jcrichton:aeryn@10.1.1.1/asa-9-12-1-smp-k8.bin disk0:/asa-9-12-1-smp-k8.bin
```

**ステップ 2** ASDM イメージをフラッシュメモリにコピーします。

**copy ftp://[[user[:password]]@]server[/path]/asdm\_image\_name diskn:/[path]/asdm\_image\_name**

例 :

```
ciscoasa# copy ftp://jcrichton:aeryn@10.1.1.1/asdm-7121.bin disk0:/asdm-7121.bin
```

**ステップ 3** グローバル コンフィギュレーション モードにアクセスします。

**configure terminal**

例 :

```
ciscoasa# configure terminal
ciscoasa(config)#
```

**ステップ 4** 設定されている現在のブート イメージを表示します (最大 4 個)。

**show running-config boot system**

ASA は、表示された順序でイメージを使用します。最初のイメージが使用できない場合は次のイメージが使用され、以下同様です。新しいイメージ URL をリストの先頭に挿入することはできません。新しいイメージが先頭であることを指定するには、既存のエントリをすべて削除してから、次の手順に従ってイメージの URL を目的の順序で入力します。

例 :

```
ciscoasa(config)# show running-config boot system
boot system disk0:/cdisk.bin
boot system disk0:/asa931-smp-k8.bin
```

**ステップ 5** 既存のブートイメージコンフィギュレーションがある場合は削除します。新しいブートイメージを最初の選択肢として入力できるようにするためです。

**no boot system diskn:/[path]/asa\_image\_name**

例 :

```
ciscoasa(config)# no boot system disk0:/cdisk.bin
ciscoasa(config)# no boot system disk0:/asa931-smp-k8.bin
```

**ステップ 6** ブートする ASA イメージを設定します (先ほどアップロードしたもの)。

**boot system diskn:/[path]/asa\_image\_name**

このイメージが使用できない場合に使用するバックアップ イメージに対して、このコマンドを繰り返します。たとえば、先ほど削除したイメージを再入力できます。

例 :

```
ciscoasa(config)# boot system disk0:/asa-9-12-1-smp-k8.bin
```

**ステップ 7** 使用する ASDM イメージを設定します（先ほどアップロードしたもの）。

**asdm image diskn:[path/]asdm\_image\_name**

使用するように設定できる ASDM イメージは 1 つだけであるため、最初に既存のコンフィギュレーションを削除する必要はありません。

例：

```
ciscoasa(config)# asdm image disk0:/asdm-7121.bin
```

**ステップ 8** 新しい設定をスタートアップ コンフィギュレーションに保存します。

**write memory**

**ステップ 9** ASA をリロードします。

**reload**

**ステップ 10** ASA FirePOWER モジュールをアップグレードする場合は、ASA REST API を無効にします。無効にしない場合アップグレードは失敗します。

**no rest-api agent**

次のコマンドを実行して、アップグレード後に REST API を再度有効にすることができます。

**rest-api agent**

（注）

FirePOWER モジュールのバージョン 6.0 以降を実行している場合、ASA 5506-X シリーズは ASA の REST API をサポートしません。

**ステップ 11** ASA FirePOWER モジュールをアップグレードします。

## ASDM を使用したローカルコンピュータからのスタンドアロンユニットのアップグレード

**Upgrade Software from Local Computer** ツールにより、コンピュータからフラッシュファイルシステムにイメージファイルをアップロードし、ASA をアップグレードできます。

### 手順

**ステップ 1** メイン ASDM アプリケーションウィンドウで、[Tools] > [Upgrade Software from Local Computer] の順に選択します。

[Upgrade Software] ダイアログボックスが表示されます。



- ステップ 2** [アップロードするイメージ (Image to Upload) ] ドロップダウン リストから、[ASDM] を選択します。
- ステップ 3** [Local File Path] フィールドで [Browse Local Files] をクリックして PC 上のファイルを見つけます。
- ステップ 4** [Flash File System Path] フィールドで [Browse Flash] をクリックしてフラッシュ ファイルシステム上のディレクトリまたはファイルを見つけます。
- ステップ 5** [イメージのアップロード (Upload Image) ] をクリックします。  
アップグレード プロセスには数分かかる場合があります。
- ステップ 6** このイメージを ASDM イメージとして設定するように求められます。[Yes] をクリックします。
- ステップ 7** ASDM を終了して、コンフィギュレーションを保存したことを確認します。[OK] をクリックします。  
アップグレード ツールを終了します。注：ASA ソフトウェアをアップグレードした後で、設定を保存し、ASDM を終了して再接続します。
- ステップ 8** これらの手順を繰り返し、[Image to Upload] ドロップダウンリストで [ASA] を選択します。この手順は、その他のタイプのファイルのアップロードでも同じです。
- ステップ 9** [ツール (Tools) ] > [システムリロード (System Reload) ] を選択して、ASA をリロードします。  
リロードの詳細の確認を求める新しいウィンドウが表示されます。
- a) [Save the running configuration at the time of reload] オプション ボタン (デフォルト) をクリックします。
  - b) リロードする時刻を選択します (たとえば、デフォルトの [Now]) 。
  - c) [Schedule Reload] をクリックします。
- リロードが開始されると、[Reload Status] ウィンドウにリロードの進行状況が表示されます。ASDM を終了するオプションも表示されます。
- ステップ 10** ASA のリロード後、ASDM を再起動します。  
コンソールポートでリロードの状況を確認できます。または、数分待った後に ASDM を使用して、接続可能になるまで再試行することもできます。
- ステップ 11** ASA FirePOWER モジュールをアップグレードする場合は、[ツール (Tools) ] > [コマンドラインインターフェイス (Command Line Interface) ] を選択し、**no rest-api agent** を入力して ASA REST API を無効にします。  
  
REST API を無効にしない場合、ASA FirePOWER モジュールのアップグレードは失敗します。次のコマンドを実行して、アップグレード後に REST API を再度有効にすることができます。  
**rest-api agent**  
(注)  
FirePOWER モジュールのバージョン 6.0 以降を実行している場合、ASA 5506-X シリーズは ASA の REST API をサポートしません。
- ステップ 12** ASA FirePOWER モジュールをアップグレードします。

## ASDM Cisco.com ウィザードを使用したスタンドアロンユニットのアップグレード

**Upgrade Software from Cisco.com Wizard** により、ASDM および ASA を最新のバージョンに自動的にアップグレードできます。

このウィザードでは、次の操作を実行できます。

- アップグレード用の ASA イメージファイルまたは ASDM イメージファイルを選択する。



(注) ASDM は最新のイメージバージョンをダウンロードし、そこにはビルド番号が含まれています。たとえば、9.9(1) をダウンロードする場合に、ダウンロードが 9.9(1.2) となる可能性があります。この動作は想定されているため、計画したアップグレードを続行できます。

- 実行したアップグレードの変更点を確認する。
- イメージをダウンロードし、インストールする。
- インストールのステータスを確認する。
- インストールが正常に完了した場合は、ASA をリロードして、コンフィギュレーションを保存し、アップグレードを完了する。

### 始める前に

内部的な変更により、このウィザードでは ASDM 7.10(1) を使用する必要があります。ASDM は ASA の以前のリリースと下位互換性があるため、実行している ASA バージョンを問わず、ASDM をアップグレードすることができます。

### 手順

**ステップ 1** [ツール (Tools)] > [ASA/ASDM 更新の確認 (Check for ASA/ASDM Updates)] を選択します。

マルチコンテキストモードでは、システムからこのメニューにアクセスします。

[Cisco.com Authentication] ダイアログボックスが表示されます。

**ステップ 2** Cisco.com のユーザー ID とパスワードを入力して、[Login] をクリックします。

[Cisco.com Upgrade Wizard] が表示されます。

(注)

利用可能なアップグレードがない場合は、ダイアログボックスが表示されます。ウィザードを終了するには、[OK] をクリックします。

**ステップ 3** [Next] をクリックして [Select Software] 画面を表示します。

現在の ASA バージョンおよび ASDM バージョンが表示されます。

**ステップ 4** ASA バージョンおよび ASDM バージョンをアップグレードするには、次の手順を実行します。

- a) [ASA] 領域で、[Upgrade to] チェックボックスをオンにしてから、アップグレードする ASA バージョンをドロップダウン リストから選択します。
- b) [ASDM] 領域で、[Upgrade to] チェックボックスをオンにしてから、アップグレードする ASDM バージョンをドロップダウン リストから選択します。

**ステップ 5** [Next] をクリックして [Review Changes] 画面を表示します。

**ステップ 6** 次の項目を確認します。

- ダウンロードした ASA イメージ ファイルや ASDM イメージ ファイルが正しいファイルであること。
- アップロードする ASA イメージ ファイルや ASDM イメージ ファイルが正しいファイルであること。
- 正しい ASA ブート イメージが選択されていること。

**ステップ 7** [Next] をクリックして、アップグレード インストールを開始します。

アップグレード インストールの進行状況を示すステータスを表示できます。

[Results] 画面が表示され、アップグレード インストール ステータス（成功または失敗）など、追加の詳細が示されます。

**ステップ 8** アップグレード インストールが成功した場合に、アップグレード バージョンを有効にするには、[Save configuration and reload device now] チェックボックスをオンにして、ASA を再起動し、ASDM を再起動します。

**ステップ 9** [Finish] をクリックして、ウィザードを終了し、コンフィギュレーションに対して行った変更を保存します。

（注）

次に高いバージョン（存在する場合）にアップグレードするには、ウィザードを再起動する必要があります。

**ステップ 10** ASA のリロード後、ASDM を再起動します。

コンソールポートでリロードの状況を確認できます。または、数分待った後に ASDM を使用して、接続可能になるまで再試行することもできます。

**ステップ 11** ASA FirePOWER モジュールをアップグレードする場合は、[ツール (Tools)] > [コマンドライン インターフェイス (Command Line Interface)] を選択し、**no rest-api agent** を入力して ASA REST API を無効にします。

REST API を無効にしない場合、ASA FirePOWER モジュールのアップグレードは失敗します。次のコマンドを実行して、アップグレード後に REST API を再度有効にすることができます。

**rest-api agent**

（注）

FirePOWER モジュールのバージョン 6.0 以降を実行している場合、ASA 5506-X シリーズは ASA の REST API をサポートしません。

**ステップ 12** ASA FirePOWER モジュールをアップグレードします。

## アクティブ/スタンバイ フェールオーバー ペアのアップグレード

アクティブ/スタンバイ フェールオーバー ペアをアップグレードしてゼロ ダウンタイム アップグレードを実現するには、CLI または ASDM を使用します。

### CLI を使用したアクティブ/スタンバイ フェールオーバー ペアのアップグレード

アクティブ/スタンバイ フェールオーバー ペアをアップグレードするには、次の手順を実行します。

#### 始める前に

- アクティブ装置で次の手順を実行します。SSH アクセスの場合、アクティブな IP アドレスに接続します。アクティブ装置は常にこの IP アドレスを保有しています。CLI に接続する場合は、ASA プロンプトを調べてフェールオーバー ステータスを確認します。フェールオーバー ステータスと優先順位（プライマリまたはセカンダリ）を表示するように ASA プロンプトを設定できます。これは、接続しているユニットを特定するのに役立ちます。[prompt](#) コマンドを参照してください。代わりに、**show failover** コマンドを入力して、このユニットのステータスと優先順位（プライマリまたはセカンダリ）を表示します。
- この手順では、FTP を使用します。TFTP、HTTP、またはその他のサーバータイプについては、『[ASA Command Reference](#)』の **copy** コマンドを参照してください。

#### 手順

**ステップ 1** 特権 EXEC モード時にアクティブ装置で、ASA ソフトウェアをアクティブ装置のフラッシュメモリにコピーします。

```
copy ftp://[[user[:password]]@]server[/path]/asa_image_name diskn: [/path]/asa_image_name
```

例 :

```
asa/act# copy ftp://jcrichton:aeryn@10.1.1.1/asa941-smp-k8.bin disk0:/asa941-smp-k8.bin
```

**ステップ 2** ソフトウェアをスタンバイ装置にコピーします。アクティブ装置で指定したのと同じパスを指定してください。

```
failover exec mate copy /noconfirm ftp://[[user[:password]]@]server[/path]/asa_image_name diskn: [/path]/asa_image_name
```

例 :

```
asa/act# failover exec mate copy /noconfirm ftp://jcrichon:aeryn@10.1.1.1/asa941-smp-k8.bin
disk0:/asa941-smp-k8.bin
```

**ステップ 3** ASDM イメージをアクティブ装置のフラッシュ メモリにコピーします。

**copy ftp://[[user[:password]]@]server[/path]/asdm\_image\_name diskn:[/path]/asdm\_image\_name**

例 :

```
asa/act# copy ftp://jcrichon:aeryn@10.1.1.1/asdm-741.bin disk0:/asdm-741.bin
```

**ステップ 4** ASDM イメージをスタンバイ装置にコピーします。アクティブ装置で指定したのと同じパスを指定してください。

**failover exec mate copy /noconfirm ftp://[[user[:password]]@]server[/path]/asdm\_image\_name  
diskn:[/path]/asdm\_image\_name**

例 :

```
asa/act# failover exec mate copy /noconfirm ftp://jcrichon:aeryn@10.1.1.1/asdm-741.bin
disk0:/asdm-741.bin
```

**ステップ 5** まだグローバルコンフィギュレーションモードを開始していない場合は、グローバルコンフィギュレーション モードを開始します。

**configure terminal**

**ステップ 6** 設定されている現在のブート イメージを表示します (最大 4 個)。

**show running-config boot system**

例 :

```
asa/act(config)# show running-config boot system
boot system disk0:/cdisk.bin
boot system disk0:/asa931-smp-k8.bin
```

ASA は、表示された順序でイメージを使用します。最初のイメージが使用できない場合は次のイメージが使用され、以下同様です。新しいイメージ URL をリストの先頭に挿入することはできません。新しいイメージが先頭であることを指定するには、既存のエントリをすべて削除してから、次の手順に従ってイメージの URL を目的の順序で入力します。

**ステップ 7** 既存のブートイメージコンフィギュレーションがある場合は削除します。新しいブートイメージを最初の選択肢として入力できるようにするためです。

**no boot system diskn:[/path]/asa\_image\_name**

例 :

```
asa/act(config)# no boot system disk0:/cdisk.bin
asa/act(config)# no boot system disk0:/asa931-smp-k8.bin
```

**ステップ 8** ブートする ASA イメージを設定します（先ほどアップロードしたもの）。

**boot system diskn:[path/]asa\_image\_name**

例：

```
asa/act(config)# boot system disk0://asa941-smp-k8.bin
```

このイメージが使用できない場合に使用するバックアップ イメージに対して、このコマンドを繰り返します。たとえば、先ほど削除したイメージを再入力できます。

**ステップ 9** 使用する ASDM イメージを設定します（先ほどアップロードしたもの）。

**asdm image diskn:[path/]asdm\_image\_name**

例：

```
asa/act(config)# asdm image disk0:/asdm-741.bin
```

使用するよう設定できる ASDM イメージは 1 つだけであるため、最初に既存のコンフィギュレーションを削除する必要はありません。

**ステップ 10** 新しい設定をスタートアップ コンフィギュレーションに保存します。

**write memory**

これらの設定変更は、スタンバイ ユニットに自動的に保存されます。

**ステップ 11** ASA FirePOWER モジュールをアップグレードする場合は、ASA REST API を無効にします。無効にしない場合アップグレードは失敗します。

**no rest-api agent**

**ステップ 12** スタンバイ装置の ASA FirePOWER モジュールをアップグレードします。

ASDM によって管理される ASA FirePOWER モジュールの場合、ASDM をスタンバイ管理 IP アドレスに接続します。アップグレードが完了するまで待ちます。

**ステップ 13** スタンバイ装置をリロードして新しいイメージを起動します。

**failover reload-standby**

スタンバイ装置のロードが完了するまで待ちます。**show failover** コマンドを使用して、スタンバイユニットが Standby Ready 状態かどうかを検証します。

**ステップ 14** 強制的にアクティブ装置からスタンバイ装置へのフェールオーバーを行います。

**no failover active**

SSH セッションから切断されている場合は、新しいアクティブ/元のスタンバイ ユニット上に現在あるメイン IP アドレスに再接続します。

**ステップ 15** 以前のアクティブ装置の ASA FirePOWER モジュールをアップグレードします。

ASDM によって管理される ASA FirePOWER モジュールの場合、ASDM をスタンバイ管理 IP アドレスに接続します。アップグレードが完了するまで待ちます。

**ステップ 16** 新しいアクティブ装置から、元のアクティブ装置（今の新しいスタンバイ装置）をリロードします。

**failover reload-standby**

例：

```
asa/act# failover reload-standby
```

（注）

元のアクティブユニットのコンソールポートに接続されている場合は、代わりに **reload** コマンドを入力して、元のアクティブ ユニットのリロードする必要があります。

---

## ASDM を使用したアクティブ/スタンバイ フェールオーバー ペアのアップグレード

アクティブ/スタンバイ フェールオーバー ペアをアップグレードするには、次の手順を実行します。

始める前に

ローカル管理コンピュータに ASA と ASDM のイメージを配置します。

### 手順

---

**ステップ 1** スタンバイ IP アドレスに接続して、*standby* ユニット上で ASDM を起動します。

**ステップ 2** メイン ASDM アプリケーション ウィンドウで、[Tools] > [Upgrade Software from Local Computer] の順に選択します。

[Upgrade Software] ダイアログボックスが表示されます。

**ステップ 3** [アップロードするイメージ (Image to Upload)] ドロップダウン リストから、[ASDM] を選択します。

**ステップ 4** [Local File Path] フィールドにコンピュータ上のファイルへのローカル パスを入力するか、[Browse Local Files] をクリックして PC 上のファイルを見つけます。

**ステップ 5** [Flash File System Path] フィールドにフラッシュファイルシステムへのパスを入力するか、[Browse Flash] をクリックしてフラッシュファイルシステム上のディレクトリまたはファイルを検索します。

**ステップ 6** [イメージのアップロード (Upload Image)] をクリックします。アップグレードプロセスには数分かかる場合があります。

このイメージを ASA イメージとして設定するように求められる場合は、[No] をクリックします。アップグレード ツールを終了します。

**ステップ 7** これらの手順を繰り返し、[Image to Upload] ドロップダウン リストで [ASA] を選択します。

このイメージを ASA イメージとして設定するように求められる場合は、[No] をクリックします。アップグレード ツールを終了します。

- ステップ 8**   メイン IP アドレスに接続して ASDM をアクティブなユニットに接続し、スタンバイ ユニットで使用したのと同じファイルの場所を使用して、ASDM ソフトウェアをアップロードします。
- ステップ 9**   このイメージを ASDM イメージとして設定するように求められたら、[Yes] をクリックします。
- ASDM を終了して、コンフィギュレーションを保存したことを確認します。[OK] をクリックします。アップグレード ツールを終了します。注：ASA ソフトウェアをアップグレードした後で、設定を保存し、ASDM をリロードします。
- ステップ 10**   スタンバイ ユニットで使用したのと同じファイルの場所を使用して、ASA ソフトウェアをアップロードします。
- ステップ 11**   このイメージを ASA イメージとして設定するように求められたら、[Yes] をクリックします。
- 新しいイメージを使用するために、ASA をリロードするよう求められます。[OK] をクリックします。アップグレード ツールを終了します。
- ステップ 12**   コンフィギュレーションの変更を保存するには、ツールバーの [Save] アイコンをクリックします。
- これらの設定変更は、スタンバイ ユニットに自動的に保存されます。
- ステップ 13**   ASA FirePOWER モジュールをアップグレードする場合は、[ツール (Tools)] > [コマンドラインインターフェイス (Command Line Interface)] を選択し、no rest-api enable を入力して ASA REST API を無効にします。
- REST API を無効にしない場合、ASA FirePOWER モジュールのアップグレードは失敗します。
- ステップ 14**   スタンバイ装置の ASA FirePOWER モジュールをアップグレードします。
- ASDM によって管理される ASA FirePOWER モジュールの場合、ASDM をスタンバイ管理 IP アドレスに接続します。アップグレードの完了を待ってから、ASDM をアクティブ装置に接続します。
- ステップ 15**   [モニタリング (Monitoring)] > [プロパティ (Properties)] > [フェールオーバー (Failover)] > [ステータス (Status)] の順に選択し、[スタンバイのリロード (Reload Standby)] をクリックして、スタンバイ装置をリロードします。
- [システム (System)] ペインを開いたまま、スタンバイ ユニットがリロードされるのを確認します。
- ステップ 16**   スタンバイ ユニットがリロードしたら、[Monitoring] > [Properties] > [Failover] > [Status] の順に選択し、[Make Standby] をクリックして、アクティブなユニットをスタンバイ ユニットにフェールオーバーします。
- ASDM は新しいアクティブ ユニットに自動的に再接続されます。
- ステップ 17**   以前のアクティブ装置の ASA FirePOWER モジュールをアップグレードします。
- ASDM によって管理される ASA FirePOWER モジュールの場合、ASDM をスタンバイ管理 IP アドレスに接続します。アップグレードの完了を待ってから、ASDM をアクティブ装置に接続します。
- ステップ 18**   [モニタリング (Monitoring)] > [プロパティ (Properties)] > [フェールオーバー (Failover)] > [ステータス (Status)] の順に選択し、[スタンバイのリロード (Reload Standby)] をクリックして、(新しい) スタンバイユニットをリロードします。
-



## アクティブ/アクティブ フェールオーバー ペアのアップグレード

アクティブ/アクティブ フェールオーバー ペアをアップグレードしてゼロ ダウンタイム アップグレードを実現するには、CLI または ASDM を使用します。

### CLI を使用したアクティブ/アクティブ フェールオーバー ペアのアップグレード

アクティブ/アクティブ フェールオーバー コンフィギュレーションの 2 つの装置をアップグレードするには、次の手順を実行します。

#### 始める前に

- 標準出荷単位で次の手順を実行します。
- これらの手順をシステム実行スペースで実行します。
- この手順では、FTP を使用します。TFTP、HTTP、またはその他のサーバータイプについては、『[ASA Command Reference](#)』の **copy** コマンドを参照してください。

#### 手順

**ステップ 1** 特権 EXEC モード時にプライマリ ユニットで、ASA ソフトウェアをフラッシュ メモリにコピーします。

**copy ftp://[[user[:password]]@]server[/path]/asa\_image\_name diskn:[/path]/asa\_image\_name**

例 :

```
asa/act/pri# copy ftp://jcrichon:aeryn@10.1.1.1/asa941-smp-k8.bin disk0:/asa941-smp-k8.bin
```

**ステップ 2** ソフトウェアをセカンダリ装置にコピーします。プライマリ装置で指定したのと同じパスを指定してください。

**failover exec mate copy /noconfirm ftp://[[user[:password]]@]server[/path]/asa\_image\_name diskn:[/path]/asa\_image\_name**

例 :

```
asa/act/pri# failover exec mate copy /noconfirm ftp://jcrichon:aeryn@10.1.1.1/asa941-smp-k8.bin disk0:/asa941-smp-k8.bin
```

**ステップ 3** ASDM イメージをプライマリ装置のフラッシュ メモリにコピーします。

**copy ftp://[[user[:password]]@]server[/path]/asdm\_image\_name diskn:[/path]/asdm\_image\_name**

例 :

```
asa/act/pri# ciscoasa# copy ftp://jcrichon:aeryn@10.1.1.1/asdm-741.bin disk0:/asdm-741.bin
```

- ステップ 4** ASDM イメージをセカンダリ装置にコピーします。標準出荷単位で指定したのと同じパスを指定してください。

**failover exec mate copy /noconfirm ftp://[[user[:password]]@]server[/path]/asdm\_image\_name  
diskn:/[path]/asdm\_image\_name**

例：

```
asa/act/pri# failover exec mate copy /noconfirm ftp://jcrichon:aeryn@10.1.1.1/asdm-741.bin
disk0:/asdm-741.bin
```

- ステップ 5** まだグローバルコンフィギュレーションモードを開始していない場合は、グローバルコンフィギュレーションモードを開始します。

**configure terminal**

- ステップ 6** 設定されている現在のブート イメージを表示します（最大 4 個）。

**show running-config boot system**

例：

```
asa/act/pri(config)# show running-config boot system
boot system disk0:/cdisk.bin
boot system disk0:/asa931-smp-k8.bin
```

ASA は、表示された順序でイメージを使用します。最初のイメージが使用できない場合は次のイメージが使用され、以下同様です。新しいイメージ URL をリストの先頭に挿入することはできません。新しいイメージが先頭であることを指定するには、既存のエントリをすべて削除してから、次の手順に従ってイメージの URL を目的の順序で入力します。

- ステップ 7** 既存のブートイメージコンフィギュレーションがある場合は削除します。新しいブートイメージを最初の選択肢として入力できるようにするためです。

**no boot system diskn:/[path]/asa\_image\_name**

例：

```
asa/act/pri(config)# no boot system disk0:/cdisk.bin
asa/act/pri(config)# no boot system disk0:/asa931-smp-k8.bin
```

- ステップ 8** ブートする ASA イメージを設定します（先ほどアップロードしたもの）。

**boot system diskn:/[path]/asa\_image\_name**

例：

```
asa/act/pri(config)# boot system disk0://asa941-smp-k8.bin
```

このイメージが使用できない場合に使用するバックアップ イメージに対して、このコマンドを繰り返します。たとえば、先ほど削除したイメージを再入力できます。

- ステップ 9** 使用する ASDM イメージを設定します（先ほどアップロードしたもの）。

**asdm image diskn: [/path/]asdm\_image\_name**

例 :

```
asa/act/pri(config)# asdm image disk0:/asdm-741.bin
```

使用するよう設定できる ASDM イメージは 1 つだけであるため、最初に既存のコンフィギュレーションを削除する必要はありません。

**ステップ 10** 新しい設定をスタートアップ コンフィギュレーションに保存します。

**write memory**

これらの設定変更は、セカンダリ ユニットに自動的に保存されます。

**ステップ 11** ASA FirePOWER モジュールをアップグレードする場合は、ASA REST API を無効にします。無効にしない場合アップグレードは失敗します。

**no rest-api agent**

**ステップ 12** プライマリ装置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。

**failover active group 1**

**failover active group 2**

例 :

```
asa/act/pri(config)# failover active group 1
asa/act/pri(config)# failover active group 2
```

**ステップ 13** セカンダリ ユニットの ASA FirePOWER モジュールをアップグレードします。

ASDM によって管理される ASA FirePOWER モジュールの場合、ASDM をフェールオーバー グループ 1 または 2 のスタンバイ管理 IP アドレスに接続します。アップグレードが完了するまで待ちます。

**ステップ 14** セカンダリ装置をリロードして新しいイメージを起動します。

**failover reload-standby**

セカンダリ装置のロードが完了するまで待ちます。**show failover** コマンドを使用して、両方のフェールオーバー グループが Standby Ready 状態であることを確認します。

**ステップ 15** セカンダリ装置で、両方のフェールオーバー グループを強制的にアクティブにします。

**no failover active group 1**

**no failover active group 2**

例 :

```
asa/act/pri(config)# no failover active group 1
asa/act/pri(config)# no failover active group 2
asa/stby/pri(config)#
```

SSHセッションから切断されている場合は、セカンダリユニット上に現在あるフェールオーバー グループ 1 の IP アドレスに再接続します。

**ステップ 16** プライマリ ユニットの ASA FirePOWER モジュールをアップグレードします。

ASDM によって管理される ASA FirePOWER モジュールの場合、ASDM をフェールオーバー グループ 1 または 2 のスタンバイ管理 IP アドレスに接続します。アップグレードが完了するまで待ちます。

**ステップ 17** プライマリ装置をリロードします。

**failover reload-standby**

例：

```
asa/act/sec# failover reload-standby
```

(注)

プライマリ ユニットのコンソール ポートに接続されている場合は、代わりに **reload** コマンドを入力して、プライマリ ユニットのリロードする必要があります。

SSH セッションから切断される場合があります。

**ステップ 18** フェールオーバー グループは、**preempt** コマンドを使用して設定されている場合、プリエンプト遅延の経過後、指定された装置で自動的にアクティブになります。

## ASDM を使用したアクティブ/アクティブ フェールオーバー ペアのアップグレード

アクティブ/アクティブ フェールオーバー コンフィギュレーションの 2 つの装置をアップグレードするには、次の手順を実行します。

### 始める前に

- これらの手順をシステム実行スペースで実行します。
- ローカル管理コンピュータに ASA と ASDM のイメージを配置します。

### 手順

- ステップ 1** フェールオーバー グループ 2 の管理アドレスに接続して、セカンダリ ユニットの ASDM を起動します。
- ステップ 2** メイン ASDM アプリケーション ウィンドウで、**[Tools] > [Upgrade Software from Local Computer]** の順に選択します。
- [Upgrade Software] ダイアログボックスが表示されます。
- ステップ 3** [アップロードするイメージ (Image to Upload)] ドロップダウン リストから、[ASDM] を選択します。
- ステップ 4** [Local File Path] フィールドにコンピュータ上のファイルへのローカル パスを入力するか、[Browse Local Files] をクリックして PC 上のファイルを見つけます。

- ステップ 5** [Flash File System Path] フィールドにフラッシュファイルシステムへのパスを入力するか、[Browse Flash] をクリックしてフラッシュファイルシステム上のディレクトリまたはファイルを検索します。
- ステップ 6** [イメージのアップロード (Upload Image) ] をクリックします。アップグレードプロセスには数分かかる場合があります。
- このイメージを ASA イメージとして設定するように求められる場合は、[No] をクリックします。アップグレード ツールを終了します。
- ステップ 7** これらの手順を繰り返し、[Image to Upload] ドロップダウン リストで [ASA] を選択します。
- このイメージを ASA イメージとして設定するように求められる場合は、[No] をクリックします。アップグレード ツールを終了します。
- ステップ 8** フェールオーバー グループ 1 の管理 IP アドレスに接続して ASDM をプライマリ ユニットに接続し、セカンダリ ユニットで使ったのと同じファイルの場所を使用して、ASDM ソフトウェアをアップロードします。
- ステップ 9** このイメージを ASDM イメージとして設定するように求められたら、[Yes] をクリックします。
- ASDM を終了して、コンフィギュレーションを保存したことを確認します。[OK] をクリックします。アップグレード ツールを終了します。注：ASA ソフトウェアをアップグレードした後で、設定を保存し、ASDM をリロードします。
- ステップ 10** セカンダリ ユニットで使ったのと同じファイルの場所を使用して、ASA ソフトウェアをアップロードします。
- ステップ 11** このイメージを ASA イメージとして設定するように求められたら、[Yes] をクリックします。
- 新しいイメージを使用するために、ASA をリロードするよう求められます。[OK] をクリックします。アップグレード ツールを終了します。
- ステップ 12** コンフィギュレーションの変更を保存するには、ツールバーの [Save] アイコンをクリックします。
- これらの設定変更は、セカンダリ ユニットに自動的に保存されます。
- ステップ 13** ASA FirePOWER モジュールをアップグレードする場合は、[ツール (Tools) ] > [コマンドラインインターフェイス (Command Line Interface) ] を選択し、no rest-api enable を入力して ASA REST API を無効にします。
- REST API を無効にしない場合、ASA FirePOWER モジュールのアップグレードは失敗します。
- ステップ 14** [Monitoring] > [Failover] > [Failover Group #] の順に選択して、プライマリ ユニット上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。ここで # は、プライマリ ユニットに移動するフェールオーバー グループの数です。[Make Active] をクリックします。
- ステップ 15** セカンダリ ユニットの ASA FirePOWER モジュールをアップグレードします。
- ASDM によって管理される ASA FirePOWER モジュールの場合、ASDM をフェールオーバー グループ 1 または 2 のスタンバイ管理 IP アドレスに接続します。アップグレードの完了を待ってから、ASDM をプライマリ ユニットに接続します。
- ステップ 16** [Monitoring] > [Failover] > [System] の順に選択し、[Reload Standby] をクリックして、セカンダリ ユニットをリロードします。

[System] ペインを開いたまま、セカンダリユニットがリロードされるのを確認します。

**ステップ 17** セカンダリ ユニットが起動したら、[Monitoring] > [Failover] > [Failover Group #] の順に選択して、セカンダリ ユニット上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。ここで#は、セカンダリ ユニットに移動するフェールオーバー グループの数です。[Make Standby] をクリックします。

ASDM は、セカンダリ ユニット上のフェールオーバー グループ 1 の IP アドレスに自動的に再接続されます。

**ステップ 18** プライマリ ユニットの ASA FirePOWER モジュールをアップグレードします。

ASDM によって管理される ASA FirePOWER モジュールの場合、ASDM をフェールオーバー グループ 1 または 2 のスタンバイ管理 IP アドレスに接続します。アップグレードの完了を待ってから、ASDM をセカンダリ ユニットに接続します。

**ステップ 19** [Monitoring] > [Failover] > [System] の順に選択し、[Reload Standby] をクリックして、プライマリユニットをリロードします。

**ステップ 20** フェールオーバーグループは、[Preempt Enabled] を使用して設定されると、プリエンプト遅延の経過後、指定された装置で自動的にアクティブになります。ASDM は、プライマリ ユニット上のフェールオーバー グループ 1 の IP アドレスに自動的に再接続されます。

## ASA クラスタのアップグレード

ASA クラスタをアップグレードしてゼロ ダウンタイム アップグレードを実現するには、CLI または ASDM を使用します。

### CLI を使用した ASA クラスタのアップグレード

ASA クラスタ内のすべての装置をアップグレードするには、次の手順を実行します。この手順では、FTP を使用します。TFTP、HTTP、またはその他のサーバータイプについては、『[ASA Command Reference](#)』の **copy** コマンドを参照してください。

#### 始める前に

- 制御ユニットで次の手順を実行します。ASA FirePOWER モジュールもアップグレードしている場合は、各データユニットへのコンソールアクセスまたは ASDM アクセスが必要です。クラスタ ユニットと状態（制御またはデータ）を表示するように ASA プロンプトを設定できます。これは、接続しているユニットを特定するのに役立ちます。[prompt](#) コマンドを参照してください。代わりに、**show cluster info** コマンドを入力して、各ユニットの役割を表示します。
- コンソール ポートを使用する必要があります。クラスタリングのイネーブルまたはディセーブルを、リモート CLI 接続から行うことはできません。
- マルチ コンテキスト モードでは、システム実行スペースで後続の手順を実行します。

## 手順

- ステップ 1** 特権 EXEC モード時に制御ユニットで、ASA ソフトウェアをクラスタ内のすべてのユニットにコピーします。

**cluster exec copy /noconfirm ftp://[[user[:password]]@]server[/path]/asa\_image\_name diskn:/[path/]asa\_image\_name**

例 :

```
asa/unit1/master# cluster exec copy /noconfirm
ftp://jcrichon:aeryn@10.1.1.1/asa941-smp-k8.bin disk0:/asa941-smp-k8.bin
```

- ステップ 2** ASDM イメージをクラスタ内のすべての装置にコピーします。

**cluster exec copy /noconfirm ftp://[[user[:password]]@]server[/path]/asdm\_image\_name diskn:/[path/]asdm\_image\_name**

例 :

```
asa/unit1/master# cluster exec copy /noconfirm ftp://jcrichon:aeryn@10.1.1.1/asdm-741.bin
disk0:/asdm-741.bin
```

- ステップ 3** まだグローバル コンフィギュレーション モードを開始していない場合は、ここで開始します。

**configure terminal**

例 :

```
asa/unit1/master# configure terminal
asa/unit1/master(config)#
```

- ステップ 4** 設定されている現在のブート イメージを表示します（最大 4 個）。

**show running-config boot system**

例 :

```
asa/unit1/master(config)# show running-config boot system
boot system disk0:/cdisk.bin
boot system disk0:/asa931-smp-k8.bin
```

ASA は、表示された順序でイメージを使用します。最初のイメージが使用できない場合は次のイメージが使用され、以下同様です。新しいイメージ URL をリストの先頭に挿入することはできません。新しいイメージが先頭であることを指定するには、既存のエントリをすべて削除してから、次の手順に従ってイメージの URL を目的の順序で入力します。

- ステップ 5** 既存のブートイメージコンフィギュレーションがある場合は削除します。新しいブートイメージを最初の選択肢として入力できるようにするためです。

**no boot system diskn:/[path/]asa\_image\_name**

例 :

```
asa/unit1/master(config)# no boot system disk0:/cdisk.bin
asa/unit1/master(config)# no boot system disk0:/asa931-smp-k8.bin
```

**ステップ 6** ブートする ASA イメージを設定します (先ほどアップロードしたもの)。

**boot system diskn:[path/]asa\_image\_name**

例 :

```
asa/unit1/master(config)# boot system disk0://asa941-smp-k8.bin
```

このイメージが使用できない場合に使用するバックアップ イメージに対して、このコマンドを繰り返します。たとえば、先ほど削除したイメージを再入力できます。

**ステップ 7** 使用する ASDM イメージを設定します (先ほどアップロードしたもの)。

**asdm image diskn:[path/]asdm\_image\_name**

例 :

```
asa/unit1/master(config)# asdm image disk0:/asdm-741.bin
```

使用するように設定できる ASDM イメージは 1 つだけであるため、最初に既存のコンフィギュレーションを削除する必要はありません。

**ステップ 8** 新しい設定をスタートアップ コンフィギュレーションに保存します。

**write memory**

これらの設定変更は、データユニットに自動的に保存されます。

**ステップ 9** ASA FirePOWER モジュールをアップグレードする場合は、ASA REST API を無効にします。無効にしない場合、ASA FirePOWER モジュールのアップグレードは失敗します。

**no rest-api agent**

**ステップ 10** ASDM によって管理されている ASA FirePOWER モジュールをアップグレードする場合、ASDM を個別の管理 IP アドレスに接続する必要があります。このため、各ユニットの IP アドレスをメモしておく必要があります。

**show running-config interface management\_interface\_id**

使用されている **cluster-pool** プール名をメモします。

**show ip[v6] local pool poolname**

クラスタ ユニットの IP アドレスをメモします。

例 :

```
asa/unit2/slave# show running-config interface gigabitethernet0/0
!
interface GigabitEthernet0/0
 management-only
```



```

nameif inside
security-level 100
ip address 10.86.118.1 255.255.252.0 cluster-pool inside-pool
asa/unit2/slave# show ip local pool inside-pool
Begin End Mask Free Held In use
10.86.118.16 10.86.118.17 255.255.252.0 0 0 2

Cluster Unit IP Address Allocated
unit2 10.86.118.16
unit1 10.86.118.17
asa1/unit2/slave#

```

## ステップ 11 データユニットをアップグレードします。

ASA FirePOWER モジュールもアップグレードするかどうかによって、以下の手順を選択します。ASA FirePOWER モジュールもアップグレードする場合、ASA FirePOWER プロシージャは ASA のリロードの回数を最小化します。以下の手順では、データコンソールまたは ASDM を使用するよう選択できます。すべてのコンソールポートへのアクセスは準備できていないが、ASDM にネットワーク経由でアクセスできる場合は、コンソールではなく ASDM を使用することを推奨します。

### (注)

アップグレードプロセス中は、**cluster master unit** コマンドを使用して強制的にデータユニットを制御に変更しないでください。ネットワークの接続性とクラスタの安定性に関連した障害が発生する恐れがあります。最初にすべてのデータユニットをアップグレードしてリロードし、次にこの手順を実行すると、現在の制御ユニットから新しい制御ユニットへの移行をスムーズに行うことができます。

### ASA FirePOWER モジュールをアップグレードしない場合：

- 制御ユニットでメンバー名を表示するには、**cluster exec unit ?** または **show cluster info** コマンドを入力します。
- データユニットをリロードします。

**cluster exec unit data-unit reload noconfirm**

例：

```
asa/unit1/master# cluster exec unit unit2 reload noconfirm
```

- 各データユニットに対して手順を繰り返します。

接続損失を回避し、トラフィックを安定させるために、各装置が起動しクラスタに再接続するのを待ち（約 5 分）、次の装置にこれらの手順を繰り返します。装置がクラスタに再接続したことを確認するには、**show cluster info** を入力します。

### ASA FirePOWER モジュールもアップグレードする場合（データコンソールを使用）：

- データユニットのコンソールポートに接続し、グローバル コンフィギュレーション モードに入ります。

**enable**

**configure terminal**

例：

```
asa/unit2/slave> enable
Password:
asa/unit2/slave# configure terminal
asa/unit2/slave(config)#
```

- b) クラスタリングを無効にします。

**cluster group name**

**no enable**

リロード時にクラスタリングを有効にするために、この構成を保存しないでください。複数の障害やアップグレード処理中の再参加を避けるために、クラスタリングを無効にする必要があります。このユニットでは、すべてのアップグレードとリロードが完了した後に再参加のみする必要があります。

例：

```
asa/unit2/slave(config)# cluster group cluster1
asa/unit2/slave(cfg-cluster)# no enable
Cluster disable is performing cleanup..done.
All data interfaces have been shutdown due to clustering being disabled. To recover either
enable clustering or remove cluster group configuration.

Cluster unit unit2 transitioned from SLAVE to DISABLED
asa/unit2/ClusterDisabled(cfg-cluster)#
```

- c) このデータユニットの ASA FirePOWER モジュールをアップグレードします。

ASDM によって管理される ASA FirePOWER モジュールの場合、事前にメモした個別の管理 IP アドレスに ASDM を接続します。アップグレードが完了するまで待ちます。

- d) データユニットをリロードします。

**reload noconfirm**

- e) 各データユニットに対して手順を繰り返します。

接続損失を回避し、トラフィックを安定させるために、各装置が起動しクラスタに再接続するのを待ち（約 5 分）、次の装置にこれらの手順を繰り返します。装置がクラスタに再接続したことを確認するには、**show cluster info** を入力します。

**ASA FirePOWER モジュールのアップグレードもある場合（ASDM を使用）：**

- 事前にメモしたこのデータユニットの「個別」の管理 IP アドレスに ASDM を接続します。
- [Configuration] > [Device Management] > [High Availability and Scalability] > [ASA Cluster] > [Cluster Configuration]** の順に選択します。
- [ASA クラスタに参加 (Participate in ASA cluster)]** チェックボックスをオフにします。

複数の障害やアップグレード処理中の再参加を避けるために、クラスタリングを無効にする必要があります。このユニットでは、すべてのアップグレードとリロードが完了した後に再参加のみする必要があります。

[Configure ASA cluster settings] チェックボックスをオフにしないでください。オフにすると、すべてのクラスタ コンフィギュレーションがクリアされ、ASDM が接続されている管理インターフェイスを含むすべてのインターフェイスもシャットダウンします。この場合、接続を復元するには、コンソール ポートで CLI にアクセスする必要があります。

(注)

ASDM の以前のバージョンは、この画面でのクラスタの無効化をサポートしていません。この場合、[Tools] > [Command Line Interface] ツールを使用します。[Multiple Line] ラジオボタンをクリックして、**cluster group name** と **no enable** を入力します。クラスタ グループ名は、[Home] > [Device Dashboard] > [Device Information] > [ASA Cluster] エリアで確認できます。

- d) [適用 (Apply)] をクリックします。
  - e) ASDM から出るように促されます。同じ IP アドレスに ASDM を再接続します。
  - f) ASA FirePOWER モジュールをアップグレードします。
- アップグレードが完了するまで待ちます。
- g) ASDM で、[Tools] > [System Reload] を選択します。
  - h) [実行コンフィギュレーションを保存しないでリロードする (Reload without saving the running configuration)] オプション ボタンをクリックします。

この装置のリロード時にクラスタリングを有効にするために、この構成を保存しないようにします。

- i) [Schedule Reload] をクリックします。
- j) [Yes] をクリックしてリロードを続行します。
- k) 各データユニットに対して手順を繰り返します。

接続損失を回避し、トラフィックを安定させるために、各装置が起動しクラスタに再接続するのを待ち (約5分)、次の装置にこれらの手順を繰り返します。装置がクラスタに再接続したことを確認するには、制御ユニットの [Monitoring] > [ASA Cluster] > [Cluster Summary] ペインを確認します。

## ステップ 12 制御ユニットをアップグレードします。

- a) クラスタリングを無効にします。

**cluster group name**

**no enable**

新しい制御ユニットが選択され、トラフィックが安定するまで 5 分間待ちます。

リロード時にクラスタリングを有効にするために、この構成を保存しないでください。

可能であれば、制御ユニットのクラスタを手動で無効にすることを推奨します。これにより、新しい制御ユニットを迅速かつできるだけクリーンな状態で選定できます。

例 :

```
asa/unit1/master(config)# cluster group cluster1
asa/unit1/master(cfg-cluster)# no enable
Cluster disable is performing cleanup..done.
```

```
All data interfaces have been shutdown due to clustering being disabled. To recover either
enable clustering or remove cluster group configuration.
```

```
Cluster unit unit1 transitioned from MASTER to DISABLED
asa/unit1/ClusterDisabled(cfg-cluster)#
```

- b) このユニットの ASA FirePOWER モジュールをアップグレードします。

ASDM によって管理される ASA FirePOWER モジュールの場合、事前にメモした個別の管理 IP アドレスに ASDM を接続します。この時点で、メインクラスタ IP アドレスは新しい制御ユニットに属しています。元の制御ユニットは、その個別の管理 IP アドレスに引き続きアクセスできます。

アップグレードが完了するまで待ちます。

- c) このユニットをリロードします。

**reload noconfirm**

元の制御ユニットがクラスタに再接続すると、そのユニットはデータユニットになります。

## ASDM を使用した ASA クラスタのアップグレード

ASA クラスタ内のすべての装置をアップグレードするには、次の手順を実行します。

### 始める前に

- 制御ユニットで次の手順を実行します。ASA FirePOWER モジュールもアップグレードしている場合は、各データユニットへの ASDM アクセスが必要です。
- マルチ コンテキスト モードでは、システム実行スペースで後続の手順を実行します。
- ローカル管理コンピュータに ASA と ASDM のイメージを配置します。

### 手順

- ステップ 1** メインクラスタ IP アドレスに接続して、「制御」ユニットで ASDM を起動します。  
この IP アドレスは、常に制御ユニットに保持されます。
- ステップ 2** メイン ASDM アプリケーションウィンドウで、**[Tools] > [Upgrade Software from Local Computer]** の順に選択します。  
[Upgrade Software from Local Computer] ダイアログボックスが表示されます。
- ステップ 3** [クラスタ内のすべてのデバイス (All devices in the cluster)] オプション ボタンをクリックします。  
[ソフトウェアのアップグレード (Upgrade Software)] ダイアログボックスが表示されます。
- ステップ 4** [アップロードするイメージ (Image to Upload)] ドロップダウン リストから、[ASDM] を選択します。

- ステップ 5** [ローカルファイルパス (Local File Path)] フィールドで [ローカルファイルの参照 (Browse Local Files)] をクリックして、コンピュータ上のファイルを見つけます。
- ステップ 6** (任意) [フラッシュファイルシステムのパス (Flash File System Path)] フィールドにフラッシュファイルシステムへのパスを入力するか、[フラッシュの参照 (Browse Flash)] をクリックしてフラッシュファイルシステム上のディレクトリまたはファイルを検索します。
- デフォルトでは、このフィールドにはパス (**disk0:/filename**) が入力されています。
- ステップ 7** [イメージのアップロード (Upload Image)] をクリックします。アップグレードプロセスには数分かかる場合があります。
- ステップ 8** このイメージを ASDM イメージとして設定するように求められます。[Yes] をクリックします。
- ステップ 9** ASDM を終了して、コンフィギュレーションを保存したことを確認します。[OK] をクリックします。
- アップグレードツールを終了します。注：ASA ソフトウェアをアップグレードした後で、設定を保存し、ASDM をリロードします。
- ステップ 10** これらの手順を繰り返し、[アップロードするイメージ (Image to Upload)] ドロップダウン リストから [ASA] を選択します。
- ステップ 11** コンフィギュレーションの変更を保存するには、ツールバーの [Save] アイコンをクリックします。
- これらの設定変更は、データユニットに自動的に保存されます。
- ステップ 12** [Configuration] > [Device Management] > [High Availability and Scalability] > [ASA Cluster] > [Cluster Members] で、各ユニットの個別の管理 IP アドレスをメモして、後で ASDM をデータユニットに直接接続できるようにします。
- ステップ 13** ASA FirePOWER モジュールをアップグレードする場合は、[ツール (Tools)] > [コマンドラインインターフェイス (Command Line Interface)] を選択し、**no rest-api enable** を入力して ASA REST API を無効にします。
- REST API を無効にしない場合、ASA FirePOWER モジュールのアップグレードは失敗します。
- ステップ 14** データユニットをアップグレードします。
- ASA FirePOWER モジュールもアップグレードするかどうかによって、以下の手順を選択します。ASA FirePOWER モジュールもアップグレードする場合、ASA FirePOWER プロシージャは ASA のリロードの回数を最小化します。

(注)

アップグレードプロセス中は、強制的にデータユニットを制御に変更するために [Monitoring] > [ASA Cluster] > [Cluster Summary] ページを使用して制御ユニットを変更しないでください。ネットワークの接続性とクラスタの安定性に関連した障害が発生する可能性があります。最初にすべてのデータユニットをリロードし、次にこの手順を実行すると、現在の制御ユニットから新しい制御ユニットへの移行をスムーズに行うことができます。

**ASA FirePOWER モジュールをアップグレードしない場合：**

- 制御ユニットで、[Tools] > [System Reload] を選択します。
- [Device] ドロップダウンリストからデータユニット名を選択します。
- [Schedule Reload] をクリックします。

- d) [Yes] をクリックしてリロードを続行します。
- e) 各データユニットに対して手順を繰り返します。

接続損失を回避し、トラフィックを安定させるために、各装置が起動しクラスタに再接続するのを待ち（約 5 分）、次の装置にこれらの手順を繰り返します。ユニットがクラスタに再接続したことを確認するには、**[Monitoring] > [ASA Cluster] > [Cluster Summary]** ペインを表示します。

#### ASA FirePOWER モジュールのアップグレードもある場合：

- a) 制御ユニットで、**[Configuration] > [Device Management] > [High Availability and Scalability] > [ASA Cluster] > [Cluster Members]** を選択します。
- b) アップグレードするデータユニットを選択して **[Delete]** をクリックします。
- c) **[適用 (Apply)]** をクリックします。
- d) ASDM を終了し、事前にメモした「個別」の管理 IP アドレスに接続して、ASDM をデータユニットに接続します。
- e) ASA FirePOWER モジュールをアップグレードします。

アップグレードが完了するまで待ちます。

- f) ASDM で、**[Tools] > [System Reload]** を選択します。
- g) **[実行コンフィギュレーションを保存しないでリロードする (Reload without saving the running configuration)]** オプション ボタンをクリックします。
- この装置のリロード時にクラスタリングを有効にするために、この構成を保存しないようにします。
- h) **[Schedule Reload]** をクリックします。
- i) **[Yes]** をクリックしてリロードを続行します。
- j) 各データユニットに対して手順を繰り返します。

接続損失を回避し、トラフィックを安定させるために、各装置が起動しクラスタに再接続するのを待ち（約 5 分）、次の装置にこれらの手順を繰り返します。ユニットがクラスタに再接続したことを確認するには、**[Monitoring] > [ASA Cluster] > [Cluster Summary]** ペインを表示します。

#### ステップ 15 制御ユニットをアップグレードします。

- a) 制御ユニットの ASDM で、**[Configuration] > [Device Management] > [High Availability and Scalability] > [ASA Cluster] > [Cluster Configuration]** ペインを選択します。
- b) **[ASA クラスタに参加 (Participate in ASA cluster)]** チェックボックスをオフにして、**[適用 (Apply)]** をクリックします。

ASDM から出るように促されます。

- c) 新しい制御ユニットが選択され、トラフィックが安定するまで最大 5 分間待機します。
- 元の制御ユニットがクラスタに再接続すると、そのユニットはデータユニットになります。
- d) 事前にメモした「個別」の管理 IP アドレスに接続して、ASDM を元の制御ユニットに再接続します。

この時点で、メインクラスタ IP アドレスは新しい制御ユニットに属しています。元の制御ユニットは、その個別の管理 IP アドレスに引き続きアクセスできます。

- e) ASA FirePOWER モジュールをアップグレードします。

アップグレードが完了するまで待ちます。

- f) **[Tools] > [System Reload]** を選択します。

- g) [実行コンフィギュレーションを保存しないでリロードする (Reload without saving the running configuration) ] オプション ボタンをクリックします。

この装置のリロード時にクラスタリングを有効にするために、この構成を保存しないようにします。

- h) [Schedule Reload] をクリックします。

- i) [Yes] をクリックしてリロードを続行します。

ASDM から出るように促されます。メインクラスタ IP アドレスで ASDM を再起動すると、新しい制御ユニットに再接続されます。

---

## FMC を使用した ASA FirePOWER モジュールのアップグレード

この手順を使用して、FMC によって管理される ASA FirePOWER module をアップグレードします。モジュールをいつアップグレードするかは、ASA をアップグレードするかどうか、および ASA の展開によって異なります。

- スタンドアロン ASA デバイス : ASA もアップグレードする場合は、ASA をアップグレードしてリロードした直後に、ASA FirePOWER module をアップグレードします。
- ASA クラスタとフェールオーバーペア : トラフィックフローとインスペクションの中断を避けるには、これらのデバイスを一度に 1 台ずつ完全にアップグレードします。ASA をアップグレードする場合、各ユニットをリロードして ASA をアップグレードする直前に、ASA FirePOWER module をアップグレードします。

詳細については、[アップグレードパス : ASA FirePOWER](#) と ASA アップグレード手順を参照してください。

### 始める前に

事前アップグレードのチェックリストを完了します。展開したアプライアンスが正常で、きちんと通信していることを確認します。

## 手順

**ステップ 1** [システム (System)] > [更新 (Updates)] を選択します。

**ステップ 2** 使用するアップグレード パッケージの横にある [インストール (Install)] アイコンをクリックして、アップグレードするデバイスを選択します。

アップグレードするデバイスがリストに表示されない場合は、間違ったアップグレードパッケージを選択しています。

(注)

[システムの更新 (System Update)] ページから同時にアップグレードするデバイスは 5 台までにすることを強く推奨します。選択したすべてのデバイスがそのプロセスを完了するまで、アップグレードを停止することはできません。いずれかのデバイスのアップグレードに問題がある場合、問題を解決する前に、すべてのデバイスのアップグレードを完了する必要があります。

**ステップ 3** [Install] をクリックし、アップグレードして、デバイスを再起動することを確認します。

トラフィックは、デバイスの設定および展開方法に応じて、アップグレードの間ドロップするか、検査なしでネットワークを通過します。詳細については、対象バージョンの [Cisco Firepower リリース ノート](#) 内の「ソフトウェアのアップグレード」の章を参照してください。

**ステップ 4** アップグレードの進捗状況をモニタします。

**注意**

アップグレード中のデバイスへの変更の展開、手動での再起動、シャットダウンは行わないでください。進行中のデバイスのアップグレードは再開しないでください。事前のチェック中に、アップグレードプロセスが停止しているように見える場合がありますが、これは想定内の動作です。アップグレードに失敗する、アプライアンスが応答しないなど、アップグレードで問題が発生した場合にはCisco TACにお問い合わせください。

**ステップ 5** アップグレードが成功したことを確認します。

アップグレードが完了したら、[Devices] > [Device Management] を選択し、アップグレードしたデバイスのソフトウェアバージョンが正しいことを確認します。

**ステップ 6** 侵入ルール (SRU/LSP) および脆弱性データベース (VDB) を更新します。

シスコ サポートおよびダウンロード サイト で利用可能なコンポーネントが現在実行中のバージョンより新しい場合は、新しいバージョンをインストールします。侵入ルールを更新する場合、ポリシーを自動的に再適用する必要はありません。後で適用します。

**ステップ 7** リリース ノートに記載されているアップグレード後の構成の変更をすべて完了します。

**ステップ 8** アップグレードしたデバイスに構成を再度展開します。



## 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。