



Management Center 用 Cisco Secure Firewall Threat Defense アップグレードガイド (バージョン 7.2)

初版：2022 年 6 月 6 日

最終更新：2022 年 6 月 30 日

シスコシステムズ合同会社

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

<http://www.cisco.com/jp>

お問い合わせ先：シスコ コンタクトセンター

0120-092-255 (フリーコール、携帯・PHS含む)

電話受付時間：平日 10:00～12:00、13:00～17:00

<http://www.cisco.com/jp/go/contactcenter/>



目次

第 1 章	使用する前に 1
	対象読者 1
	アップグレードの計画 3
	機能の履歴 5
	支援が必要な場合 17

第 2 章	システム要件 19
	Management Center プラットフォーム 19
	Threat Defense プラットフォーム 20
	Threat Defense 管理 22
	ブラウザ要件 24

第 3 章	ソフトウェアのアップグレードガイドライン 27
	アップグレードする最小バージョン 27
	バージョン 7.2 のアップグレードガイドライン 28
	GCP 向け Threat Defense Virtual はバージョン 7.2.0 を飛び越してアップグレードできない 29
	高可用性 Management Center の Cisco Secure Malware Analytics に再接続する 29
	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 30
	バージョン 7.2 パッチのアップグレードガイドライン 30
	応答しないアップグレード 30
	Threat Defense 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 31
	時間とディスク容量のテスト 34
	バージョン 7.2.0.1 の時間とディスク容量 36

バージョン 7.2.0 の時間とディスク容量 37

第 4 章

Management Center のアップグレード 39

Management Center のアップグレードチェックリスト 39

Management Center のアップグレードパス 43

アップグレードパッケージのアップロード 45

Management Center のアップグレード準備状況チェック 46

Management Center のアップグレード：スタンドアロン 47

Management Center のアップグレード：ハイアベイラビリティ 48

第 5 章

Threat Defense のアップグレード 51

Threat Defense のアップグレードチェックリスト 51

Threat Defense のアップグレードパス 55

FXOS を使用する Threat Defense のアップグレードパス 55

FXOS を使用しない Threat Defense のアップグレードパス 58

アップグレードパッケージのアップロード 61

Management Center への Threat Defense アップグレードパッケージのアップロード 61

Threat Defense アップグレードパッケージの内部サーバーへのアップロード 62

Threat Defense アップグレードパッケージのデバイス間のコピー 64

Threat Defense のアップグレード準備状況チェック 66

Threat Defense のアップグレード 67

ウィザードを使用した Threat Defense のアップグレード（復元を無効化） 67

で Threat Defense をアップグレード（復元を有効化） 71

第 6 章

Firepower 4100/9300 の FXOS アップグレード 75

FXOS のアップグレードパッケージ 75

FXOS のアップグレードガイドライン 75

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 77

FXOS のアップグレードパス 78

Threat Defense を使用する FXOS のアップグレードパス 78

Threat Defense および ASA を使用した FXOS のアップグレードパス 81

Chassis Manager を使用した FXOS のアップグレード	83
Firepower Chassis Manager を使用したスタンドアロン FTD 論理デバイスまたは FTD シャーシ内クラスタ用の FXOS のアップグレード	83
Firepower Chassis Manager を使用した FTD シャーシ間クラスタの FXOS のアップグレード	85
Firepower Chassis Manager を使用した FTD ハイアベイラビリティペアの FXOS のアップグレード	88
CLI を使用した FXOS のアップグレード	92
FXOS CLI を使用したスタンドアロン FTD 論理デバイスまたは FTD シャーシ内クラスタ用の FXOS のアップグレード	92
FXOS CLI を使用した FTD シャーシ間クラスタの FXOS のアップグレード	95
FXOS CLI を使用した FTD ハイアベイラビリティペアの FXOS のアップグレード	98

 第 7 章

アップグレードを復元するまたはアンインストールする	105
Threat Defense アップグレードの復元	105
復元ガイドライン	106
Management Center を使用して Threat Defense を復元する	109
パッチのアンインストール	110
アンインストールに対応するパッチ	110
高可用性/拡張性のアンインストール順序	111
Threat Defense パッチのアンインストール	112
スタンドアロン Management Center パッチのアンインストール	114
高可用性 Management Center パッチのアンインストール	115



第 1 章

使用する前に

- [対象読者](#) (1 ページ)
- [アップグレードの計画](#) (3 ページ)
- [機能の履歴](#) (5 ページ)
- [支援が必要な場合](#) (17 ページ)

対象読者

このガイドでは、ハードウェアまたは仮想 **Secure Firewall Management Center** を搭載した **Secure Firewall Threat Defense** のバージョン 7.2 へのアップグレードを準備し、正常に完了する方法について説明します。

関連リソース

別のプラットフォームまたはコンポーネントをアップグレードする場合、または別のバージョンにアップグレードする場合は、これらのリソースのいずれかを参照してください。

表 1: *Management Center* の手順

Version	ガイド
7.2 以降	アップグレードガイド の下にある、お使いのバージョンの『 <i>Management Center</i> 用 <i>Cisco Secure Firewall Threat Defense</i> アップグレードガイド』。
7.1	『 Firepower Management Center 用 <i>Cisco Firepower Threat Defense</i> アップグレードガイド (バージョン 7.1) 』
7.0 以前	Cisco Firepower Management Center Upgrade Guide, Version 6.0–7.0

表 2: *Management Center* を使用した *Threat Defense* の手順

Version	ガイド
7.2 以降	アップグレードガイド の下にある、お使いのバージョンの『 <i>Management Center</i> 用 <i>Cisco Secure Firewall Threat Defense</i> アップグレードガイド』。

Version	ガイド
7.1	『Firepower Management Center 用 Cisco Firepower Threat Defense アップグレードガイド (バージョン 7.1)』
7.0 以前	Cisco Firepower Management Center Upgrade Guide, Version 6.0–7.0

表 3: Device Manager を使用した Threat Defense の手順

Version	ガイド
7.2 以降	アップグレードガイドの下にある、お使いのバージョンの『Device Manager 用 Cisco Secure Firewall Threat Defense アップグレードガイド』内にある「」の章。
7.1	『Firepower Device Manager 用 Cisco Firepower Threat Defense アップグレードガイド (バージョン 7.1)』
7.0*	『Firepower Device Manager 用 Cisco Firepower Threat Defense 設定ガイド (バージョン 7.0)』内の「システム管理」
6.7*	『Firepower Device Manager 用 Cisco Firepower Threat Defense 設定ガイド (バージョン 6.7)』内の「システム管理」
6.6*	『Firepower Device Manager 用 Cisco Firepower Threat Defense 設定ガイド (バージョン 6.6)』内の「システム管理」
6.5*	『Firepower Device Manager 用 Cisco Firepower Threat Defense 設定ガイド (バージョン 6.5)』内の「システム管理」
6.4	『Firepower Device Manager 用 Cisco Firepower Threat Defense 設定ガイド (バージョン 6.4)』内の「システム管理」
6.3	『Firepower Device Manager 用 Cisco Firepower Threat Defense 設定ガイド (バージョン 6.3)』内の「システム管理」
6.2.3	『Firepower Device Manager 用 Cisco Firepower Threat Defense 設定ガイド (バージョン 6.2.3)』内の「システム管理」
6.2.2	『Firepower Device Manager 用 Cisco Firepower Threat Defense 設定ガイド (バージョン 6.2.2)』内の「システム管理」
6.2	『Firepower Device Manager 用 Cisco Firepower Threat Defense 設定ガイド (バージョン 6.2)』内の「システム管理」
6.1	『Firepower Device Manager 用 Cisco Firepower Threat Defense 設定ガイド (バージョン 6.1)』内の「システム管理」

* FDM を使用して Firepower 4100/9300 でバージョン 6.5 ~ 7.0 の FTD 論理デバイスを管理している場合、FXOS のアップグレード手順については、『Cisco Firepower 4100/9300 アップグレー

ドガイド、*FXOS 1.1.1 ~ 2.10.1* を使用した *Firepower 6.0.1 ~ 7.0.x* または *ASA 9.4 (1) ~ 9.16 (x)* の「[FTD 論理デバイスを搭載した Firepower 4100/9300 のアップグレード](#)」も参照してください。

表 4: NGIPS デバイスの手順

Version	プラットフォーム	ガイド
任意	Firepower 7000/8000 シリーズ	Cisco Firepower Management Center Upgrade Guide, Version 6.0-7.0
任意	FMC を搭載した ASA FirePOWER	Cisco Firepower Management Center Upgrade Guide, Version 6.0-7.0
任意	ASDM を使用した ASA FirePOWER	Cisco Secure Firewall ASA アップグレードガイド

表 5: その他のアップグレード可能なコンポーネントの手順

Version	コンポーネント	ガイド
任意	Firepower 4100/9300 上の ASA 論理デバイス	Cisco Secure Firewall ASA アップグレードガイド
Latest	Management Center 用の BIOS およびファームウェア	Cisco Secure Firewall Threat Defense/Firepower ホットフィックスリリース ノート
Latest	ISA 3000 の ROMMON イメージ	Cisco Secure Firewall ASA および Secure Firewall Threat Defense 再イメージ化ガイド

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、アップグレードの章を参照してください。

表 6: 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	<p>展開を評価します。</p> <p>アップグレードパスを計画します。</p> <p>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。</p> <p>アプライアンスへのアクセスを確認します。</p> <p>帯域幅を確認します。</p> <p>メンテナンス時間帯をスケジュールします。</p>
バックアップ	<p>ソフトウェアをバックアップします。</p> <p>Firepower 4100/9300 の FXOS をバックアップします。</p>
アップグレードパッケージ	<p>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。</p> <p>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。</p>
関連するアップグレード	<p>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。</p> <p>Firepower 4100/9300 の FXOS をアップグレードします。</p>
最終チェック	<p>設定を確認します。</p> <p>NTP 同期を確認します。</p> <p>ディスク容量を確認します。</p> <p>設定を展開します。</p> <p>準備状況チェックを実行します。</p> <p>実行中のタスクを確認します。</p> <p>展開の正常性と通信を確認します。</p>

機能の履歴

表 7:バージョン 7.2.0の機能

機能	説明
<p>デバイス間のアップグレードパッケージのコピー（「ピアツーピア同期」）。</p>	<p>Management Center や内部 Web サーバーから各デバイスにアップグレードパッケージをコピーする代わりに、Threat Defense CLI を使用してデバイス間でアップグレードパッケージをコピーできます（「ピアツーピア同期」）。この安全で信頼性の高いリソース共有は、管理ネットワークを経由しますが、Management Center には依存しません。各デバイスは、5 つのパッケージの同時転送に対応できます。</p> <p>この機能は、同じスタンドアロン Management Center によって管理されるバージョン 7.2 以降のスタンドアロンデバイスでサポートされています。次の場合はサポートされていません。</p> <ul style="list-style-type: none"> • コンテナインスタンス。 • デバイスの高可用性ペアとクラスタ。 <p>バージョン 7.1 以降のグループメンバーは通常の同期プロセスの一部として、相互にパッケージを取得できます。アップグレードパッケージを 1 つのグループメンバーにコピーすると、自動的にすべてのグループメンバーと同期されます。</p> <ul style="list-style-type: none"> • 高可用性 Management Center によって管理されるデバイス。 • クラウド提供型の管理センターによって管理されているが、分析モードでお客様が導入した Management Center に追加されたデバイス。 • 異なるドメインのデバイス、または NAT ゲートウェイによって分離されたデバイス。 • Management Center のバージョンに関係なく、バージョン 7.1 以前からアップグレードするデバイス。 <p>新規/変更された CLI コマンド：configure p2psync enable、configure p2psync disable、show peers、show peer details、sync-from-peer、show p2p-sync-status</p>

機能	説明
<p>Threat Defense のアップグレード完了後の Snort 3 への自動アップグレード。</p>	<p>バージョン 7.2 以降の Management Center を使用して Threat Defense をアップグレードする場合、Snort 2 から Snort 3 へのアップグレードを実行するかどうかを選択できるようになりました。</p> <p>ソフトウェアのアップグレード後、設定を展開すると、対象のデバイスが Snort 2 から Snort 3 にアップグレードされます。カスタム侵入ポリシーやネットワーク分析ポリシーを使用しているためにデバイスがアップグレード対象外になる場合は、検出とパフォーマンスを向上させるために、手動で Snort 3 にアップグレードすることを強く推奨します。移行のサポートについては、お使いのバージョンの Cisco Secure Firewall Management Center Snort 3 Configuration Guide を参照してください。</p> <p>このオプションは、バージョン 7.2 以降への Threat Defense のメジャーアップグレードおよびメンテナンスアップグレードでサポートされています。バージョン 7.0 または 7.1 への Threat Defense のアップグレード、または任意のバージョン向けのパッチではサポートされていません。</p>
<p>単一ノードクラスタのアップグレード。</p>	<p>デバイスのアップグレードページ ([デバイス (Devices)] > [デバイスのアップグレード (Device Upgrade)]) を使用して、アクティブノードが 1 つだけのクラスタをアップグレードできるようになりました。非アクティブ化されたノードもアップグレードされます。以前は、このタイプのアップグレードは失敗していました。この機能は、システムの更新ページ ([システム (System)] > [更新 (Updates)]) ではサポートされていません。</p> <p>この場合、ヒットレスアップグレードもサポートされません。トラフィックフローと検査の中断は、スタンドアロンデバイスと同様に、アクティブユニットのインターフェイス設定に依存します。</p> <p>サポートされるプラットフォーム : Firepower 4100/9300、Secure Firewall 3100</p>

機能	説明
<p>CLI からの Threat Defense アップグレードの復元。</p>	<p>Management Center とデバイス間の通信が中断された場合、デバイスの CLI から Threat Defense のアップグレードを元に戻すことができるようになりました。高可用性や拡張性の展開では、すべて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。CLI を使用して復元する場合は、すべてのユニットでセッションを開き、それぞれで復元が可能であることを確認してから、プロセスを同時に開始します。</p> <p>注意 CLI から復元すると、アップグレード後に行った変更によっては、デバイスと Management Center 間で設定が同期されないことがあります。これにより、後に通信と展開の問題が発生する可能性があります。</p> <p>新規/変更された CLI コマンド：upgrade revert、show upgrade revert-info。</p> <p>詳細については、Management Center アップグレードガイドの「Revert the Upgrade」を参照してください。</p>
<p>アップグレードを行っても、トラブルシューティング ファイルは自動的に生成されません。</p>	<p>時間とディスク容量を節約するために、管理センターのアップグレードプロセスでは、アップグレードの開始前にトラブルシューティング ファイルを自動的に生成しなくなりました。デバイスのアップグレードは影響を受けず、引き続きトラブルシューティング ファイルが生成される点に注意してください。</p> <p>管理センターのトラブルシューティング ファイルを手動で生成するには、システム (⚙) > [正常性 (Health)] > [モニター (Monitor)] を選択し、左側のパネルで [Firewall Management Center] をクリックし、[View System & Troubleshoot Details]、[Generate Troubleshooting Files] を選択します。</p>

表 8:バージョン 7.1.0の機能

機能	説明
<p>正常なデバイスアップグレードを元に戻します。</p>	<p>メジャーおよびメンテナンスアップグレードをFTDに戻ることができるようになりました。復元すると、ソフトウェアは、最後のアップグレードの直前の状態に戻ります（スナップショットとも呼ばれます）。パッチのインストール後にアップグレードを元に戻すと、パッチだけでなく、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も元に戻されます。</p> <p>重要 元に戻す必要がある可能性があると思われる場合は、[システム (System)] > [更新 (Updates)] ページを使用してFTDをアップグレードする必要があります。[システムの更新 (System Updates)] ページは、[アップグレード後の復元を有効にする (Enable revert after successful upgrade)] オプションを有効にできる唯一の場所です。このオプションでは、アップグレードの開始時に復元スナップショットを保存するようにシステムが設定されます。これは、[デバイス (Devices)] > [デバイスのアップグレード (Device Upgrade)] ページでウィザードを使用する通常の推奨とは対照的です。</p> <p>この機能は、Firepower 4100/9300 のコンテナインスタンスではサポートされません。</p>
<p>クラスタ化された高可用性デバイスのアップグレードワークフローの改善。</p>	<p>クラスタ化された高可用性デバイスのアップグレードワークフローが次のように改善されました。</p> <ul style="list-style-type: none"> • アップグレードウィザードは、個々のデバイスとしてではなく、グループとして、クラスタ化された高可用性ユニットを正しく表示するようになりました。システムは、発生する可能性のあるグループ関連の問題を特定し、報告し、事前に修正を要求できます。たとえば、Firepower Chassis Manager で非同期の変更を行った場合は、Firepower 4100/9300 のクラスタをアップグレードできません。 • アップグレードパッケージをクラスタおよび高可用性ペアにコピーする速度と効率が向上しました。以前は、FMC はパッケージを各グループメンバーに順番にコピーしていました。これで、グループメンバーは通常の同期プロセスの一部として、相互にパッケージを取得できるようになりました。 • クラスタ内のデータユニットのアップグレード順序を指定できるようになりました。コントロールユニットは常に最後にアップグレードされます。

表 9:バージョン 7.0.0の機能

機能	説明
FTD のアップグレードパフォーマンスとステータスレポートの改善。	FTDのアップグレードがより簡単かつ確実に、より少ないディスク容量で実行できるようになりました。メッセージセンターの新しい[アップグレード (Upgrades)] タブでは、アップグレードステータスとエラーレポートがさらに強化されています。

機能	説明
FTD デバイスのわかりやすいアップグレードワークフロー。	

機能	説明
	<p>FMC の新しいデバイス アップグレード ページ ([デバイス (Devices)]>[アップグレード (Upgrade)]) には、バージョン 6.4 以降の FTD デバイスをアップグレードするためのわかりやすいウィザードがあります。アップグレードするデバイスの選択、アップグレードパッケージのデバイスへのコピー、互換性と準備状況の確認など、アップグレード前の重要な段階を順を追って説明します。</p> <p>開始するには、[デバイス管理 (Device Management)] ページ ([デバイス (Devices)]>[デバイス管理 (Device Management)]>[アクションの選択 (Select Action)]) で新しい [Firepower ソフトウェアのアップグレード (Upgrade Firepower Software)] アクションを使用します。</p> <p>続行すると、選択したデバイスに関する基本情報と、現在のアップグレード関連のステータスが表示されます。表示内容には、アップグレードできない理由が含まれます。あるデバイスがウィザードの1つの段階に「合格」しない場合、そのデバイスは次の段階には表示されません。</p> <p>ウィザードから移動しても、進行状況は保持されます。ただし、管理者アクセス権を持つ他のユーザーはウィザードをリセット、変更、または続行できます。</p> <p>(注) FTD のアップグレードパッケージの場所をアップロードまたは指定するには、引き続き [システム更新 (System Updates)] ページ ([システム (System)]>[更新 (Updates)]) を使用する必要があります。また、[システム更新 (System Updates)] ページを使用して、FMC 自体、およびすべての非 FTD 管理対象デバイスをアップグレードする必要があります。</p> <p>(注) バージョン 7.0 では、ウィザードにクラスタまたは高可用性ペアのデバイスが正しく表示されません。これらのデバイスは1つのユニットとして選択してアップグレードする必要がありますが、ウィザードにはスタンドアロンデバイスとして表示されます。デバイスのステータスとアップグレードの準備状況は、個別に評価および報告されます。つまり、1つのユニットが「合格」して次の段階に進んでいるように見えても、他のユニットは合格していない可能性があります。ただし、それらのデバイスはグループ化されたままです。1つのユニットで準備状況チェックを実行すると、すべてのユニットで実行されます。1つユニットでアップグレードを開始すると、すべてのユニットで開始されます。</p>

機能	説明
	<p>時間がかかるアップグレードの失敗を回避するには、[次へ (Next)]をクリックする前に、すべてのグループメンバーがウィザードの次のステップに進む準備ができていることを手動で確認します。</p>
<p>多くの FTD デバイスを一度にアップグレードします。</p>	<p>FTD アップグレードウィザードでは、次の制限が解除されません。</p> <ul style="list-style-type: none"> • デバイスの同時アップグレード。 <p>一度にアップグレードできるデバイスの数は、同時アップグレードを管理するシステムの機能ではなく、管理ネットワークの帯域幅によって制限されます。以前は、一度に 5 台を上回るデバイスをアップグレードしないことを推奨していました。</p> <p>重要 この改善は、FTD バージョン 6.7 以降へのアップグレードでのみ確認できます。デバイスを古い FTD リリースにアップグレードする場合は、新しいアップグレードウィザードを使用している場合でも、一度に 5 台のデバイスに制限することをお勧めします。</p> • デバイスモデルによるアップグレードのグループ化。 <p>システムが適切なアップグレードパッケージにアクセスできる限り、すべての FTD モデルのアップグレードを同時にキューに入れて呼び出すことができます。</p> <p>以前は、アップグレードパッケージを選択し、そのパッケージを使用してアップグレードするデバイスを選択していました。つまり、アップグレードパッケージを共有している場合にのみ、複数のデバイスを同時にアップグレードできました。たとえば、2 台の Firepower 2100 シリーズ デバイスは同時にアップグレードできますが、Firepower 2100 シリーズと Firepower 1000 シリーズはアップグレードできません。</p>

表 10:バージョン 6.7.0の機能

機能	説明
Threat Defense アップグレードステータス レポートとキャンセル/再試行オプションの改善。	

機能	説明
	<p>[デバイス管理 (Device Management)] ページで、進行中の Threat Defense デバイスアップグレードと準備状況チェックのステータス、およびアップグレードの成功/失敗の7日間の履歴を表示できるようになりました。メッセージセンターでは、拡張ステータスとエラーメッセージも提供されます。</p> <p>デバイス管理とメッセージセンターの両方からワンクリックでアクセスできる新しい [Upgrade Status] ポップアップに、残りのパーセンテージ/時間、特定のアップグレード段階、成功/失敗データ、アップグレードログなどの詳細なアップグレード情報が表示されます。</p> <p>また、このポップアップで、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 ([Cancel Upgrade]) することも、失敗したアップグレードを再試行 ([Retry Upgrade]) することもできます。アップグレードをキャンセルすると、デバイスはアップグレード前の状態に戻ります。</p> <p>(注) 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、アップグレード時に表示される新しい自動キャンセルオプションを無効にする必要があります ([アップグレードに失敗すると自動的にキャンセルされ、前のバージョンにロールバックする (Automatically cancel on upgrade failure and roll back to the previous version)])。オプションを有効にすると、アップグレードが失敗した場合、デバイスは自動的にアップグレード前の状態に戻ります。</p> <p>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。</p> <p>新規/変更された画面：</p> <ul style="list-style-type: none"> • Threat Defense アップグレードパッケージの[システム (System)]> [更新 (Update)]> [製品アップデート (Product Updates)]> [利用可能なアップデート (Available Updates)]> [インストール (Install)] アイコン • [Devices] > [Device Management] > [Upgrade] • [Message Center] > [Tasks]

機能	説明
	新しい Threat Defense CLI コマンド <ul style="list-style-type: none"> • show upgrade status detail • show upgrade status continuous • show upgrade status • upgrade cancel • upgrade retry
アップグレードでディスク容量を節約するために PCAP ファイルが削除される。	アップグレードにより、ローカルに保存された PCAP ファイルが削除されるようになりました。アップグレードするには、十分な空きディスク容量が必要です。これがない場合、アップグレードは失敗します。

表 11:バージョン 6.6.0の機能

機能	説明
内部 Web サーバーからデバイスアップグレードパッケージを取得します。	デバイスは、Management Center からではなく、独自の内部 Web サーバーからアップグレードパッケージを取得できるようになりました。これは、Management Center とそのデバイスとの間の帯域幅が制限されている場合に特に役立ちます。また、Management Center 上の容量も節約できます。 新規/変更された画面：[システム (System)]>[更新 (Updates)]>[更新のアップロード (Upload Update)]ボタン >[ソフトウェア更新ソースの指定 (Specify Software Update Source)]オプション

機能	説明
アップグレードがスケジュールされたタスクを延期する。	<p>Management Center のアップグレードプロセスによって、スケジュールされたタスクが延期されるようになりました。アップグレード中に開始するようにスケジュールされたタスクは、アップグレード後の再起動の 5 分後に開始されます。</p> <p>(注) アップグレードを開始する前に、実行中のタスクが完了していることを確認する必要があります。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。</p> <p>この機能は、サポートされているバージョンからのすべてのアップグレードでサポートされていることに注意してください。これには、バージョン 6.4.0.10 以降のパッチ、バージョン 6.6.3 以降のメンテナンスリリース、およびバージョン 6.7.0 以降が含まれます。この機能は、サポートされていないバージョンからサポートされているバージョンへのアップグレードではサポートされていません。</p>

表 12:バージョン 6.4.0 の機能

機能	説明
アップグレードがスケジュールされたタスクを延期する。	<p>Management Center のアップグレードプロセスによって、スケジュールされたタスクが延期されるようになりました。アップグレード中に開始するようにスケジュールされたタスクは、アップグレード後の再起動の 5 分後に開始されます。</p> <p>(注) アップグレードを開始する前に、実行中のタスクが完了していることを確認する必要があります。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。</p> <p>この機能は、サポートされているバージョンからのすべてのアップグレードでサポートされていることに注意してください。これには、バージョン 6.4.0.10 以降のパッチ、バージョン 6.6.3 以降のメンテナンスリリース、およびバージョン 6.7.0 以降が含まれます。この機能は、サポートされていないバージョンからサポートされているバージョンへのアップグレードではサポートされていません。</p>

表 13:バージョン 6.2.3 の機能

機能	説明
アップグレードの前に、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。	<p>実際のアップグレードを実行する前に、Management Center から管理対象デバイスにアップグレードパッケージをコピー（またはプッシュ）できるようになりました。帯域幅の使用量が少ない時間帯やアップグレードのメンテナンス期間外でプッシュできるため、この機能は便利です。</p> <p>高可用性デバイス、クラスタデバイス、またはスタック構成デバイスにプッシュすると、アップグレードパッケージは最初にアクティブ/コントロール/プライマリに送信され、次にスタンバイ/データ/セカンダリに送信されます。</p> <p>新規/変更された画面：[システム (System)] > [更新 (Updates)]</p>

支援が必要な場合

オンラインリソース

シスコは、ドキュメント、ソフトウェア、ツールのダウンロードのほか、バグを照会したり、サービスリクエストをオープンしたりするための次のオンラインリソースを提供しています。これらのリソースは、Cisco ソフトウェアをインストールして設定したり、技術的問題を解決したりするために使用してください。

- マニュアル：<http://www.cisco.com/go/threatdefense-72-docs>
- シスコ サポートおよびダウンロード サイト：<https://www.cisco.com/c/en/us/support/index.html>
- Cisco Bug Search Tool：<https://tools.cisco.com/bugsearch/>
- シスコ通知サービス：<https://www.cisco.com/cisco/support/notifications.html>

シスコ サポートおよびダウンロード サイトの大部分のツールにアクセスする際は、Cisco.com のユーザー ID およびパスワードが必要です。

シスコへのお問い合わせ

上記のオンラインリソースを使用して問題を解決できない場合は、Cisco TAC にお問い合わせください。

- Cisco TAC の電子メール アドレス：tac@cisco.com
- Cisco TAC の電話番号（北米）：1.408.526.7209 または 1.800.553.2447
- Cisco TAC の連絡先（世界全域）：[Cisco Worldwide Support の連絡先](#)



第 2 章

システム要件

このドキュメントでは、バージョン 7.2 のシステム要件を記載します。

- [Management Center プラットフォーム](#) (19 ページ)
- [Threat Defense プラットフォーム](#) (20 ページ)
- [Threat Defense 管理](#) (22 ページ)
- [ブラウザ要件](#) (24 ページ)

Management Center プラットフォーム

このセクションでは、バージョン 7.2 でサポートされている、お客様が導入したハードウェアと仮想 Management Center を示します。クラウド提供型の管理センターにはバージョンはありません。

クラウド提供型の管理センターを含む、Management Center とのデバイス互換性については、「[Threat Defense 管理](#) (22 ページ)」を参照してください。一般的な互換性情報については、[Cisco Secure Firewall Management Center 互換性ガイド](#) を参照してください。

Management Center ハードウェア

バージョン 7.2 は次の Management Center ハードウェアをサポートします。

- FMC 1600
- FMC 2600
- FMC 4600

また、BIOS および RAID コントローラのファームウェアを最新の状態に保つ必要があります ([Cisco Secure Firewall Threat Defense/Firepower ホットフィックス リリース ノート](#) を参照)。

Management Center Virtual

バージョン 7.2 は、次の Management Center Virtual プラットフォームをサポートしています。

Management Center Virtual では、2、10、25、または 300 台のデバイスを管理できるライセンスを購入できます。一部のプラットフォームのみが FMCv300 をサポートすることに注意してく

ださい。さらに、FMCv2 は高可用性をサポートしていません。サポートされているインスタンスの詳細については、[Cisco Secure Firewall Management Center Virtual 入門ガイド](#)を参照してください。

表 14: バージョン 7.2 Management Center Virtual パブリック クラウド プラットフォーム

プラットフォーム (Platform)	FMCv2、10、25	FMCv300	ハイ アベイラビリティ
Alibaba	対応	—	—
Amazon Web Services (AWS)	対応	対応	対応
Google Cloud Platform (GCP)	対応	—	—
Microsoft Azure	対応	—	—
Oracle Cloud Infrastructure (OCI)	対応	対応	対応

表 15: バージョン 7.2 Management Center Virtual オンプレミス/プライベートクラウド プラットフォーム

プラットフォーム (Platform)	FMCv2、10、25	FMCv300	ハイ アベイラビリティ
Cisco HyperFlex	対応	—	—
カーネルベース仮想マシン (KVM)	対応	—	—
Nutanix エンタープライズクラウド	対応	—	—
OpenStack	対応	—	—
VMware vSphere/VMware ESXi 6.5、6.7、または 7.0	対応	対応	対応

Threat Defense プラットフォーム

次の表に、このリリースのサポート対象デバイスと管理方式を示します。これらの管理方法の詳細については、[Threat Defense 管理 \(22 ページ\)](#)を参照してください。一般的な互換性情報については、[Cisco Secure Firewall Threat Defense 互換性ガイド](#)を参照してください。

Threat Defense ハードウェア

Threat Defense のハードウェアは、多様なスループット、拡張性、およびフォームファクタに対応します。

表 16:バージョン 7.2 Threat Defense ハードウェア

プラットフォーム (Platform)	Management Center 互換		Device Manager 互換		注記
	お客様が 導入	クラウド 提供型	Device Manager のみ	Device Manager + CDO	
Firepower 1010、 1120、1140、1150	対応	対応	対応	対応	—
Firepower 2110、 2120、2130、2140	対応	対応	対応	対応	—
Secure Firewall 3110、 3120、3130、3140	対応	対応	対応	対応	—
Firepower 4110、 4120、4140、4150 Firepower 4112、 4115、4125、4145	対応	対応	対応	対応	FXOS 2.12.0.31 以降のビルドが必要です。
Firepower 9300 : SM-24、SM-36、 SM-44 モジュール Firepower 9300 : SM-40、SM-48、 SM-56 モジュール	対応	対応	対応	対応	FXOS 2.12.0.31 以降のビルドが必要です。
ISA 3000	対応	対応	対応	対応	最新の ROMMON イメージが必要です。 Cisco Secure Firewall ASA および Secure Firewall Threat Defense 再イメージ化ガイドを参照してください。

Threat Defense Virtual

仮想版 Threat Defense の導入により、スループット要件とリモートアクセス VPN セッションの制限に基づいて、パフォーマンス階層型のスマート ソフトウェア ライセンスがサポートされます。オプションは、FTDv5 (100 Mbps/50 セッション) から FTDv100 (16 Gbps/10,000 セッション) までです。サポートされているインスタンス、スループット、およびその他のホスティング要件の詳細については、該当する [スタートアップガイド](#) を参照してください。

表 17:バージョン 7.2 Threat Defense Virtual パブリック クラウド プラットフォーム

デバイスのプラットフォーム	Management Center 互換		Device Manager 互換	
	お客様が導入	クラウド提供型	Device Manager のみ	CDO および Device Manager
Alibaba	対応	対応	—	—
Amazon Web Services (AWS)	対応	対応	対応	対応
Microsoft Azure	対応	対応	対応	対応
Google Cloud Platform (GCP)	対応	対応	対応	対応
Oracle Cloud Infrastrucure (OCI)	対応	対応	—	—

表 18:バージョン 7.2 Threat Defense Virtual オンプレミス/プライベートクラウドプラットフォーム

デバイスのプラットフォーム	Management Center 互換		Device Manager 互換	
	お客様が導入	クラウド提供型	Device Manager のみ	CDO および Device Manager
Cisco Hyperflex	対応	対応	対応	対応
カーネルベース仮想マシン (KVM)	対応	対応	対応	対応
Nutanix エンタープライズクラウド	対応	対応	対応	対応
OpenStack	対応	対応	—	—
VMware vSphere/VMware ESXi 6.5、6.7、または 7.0	対応	対応	対応	対応

Threat Defense 管理

お客様が導入した Management Center

すべての Firepower および Secure Firewall Threat Defense デバイスは、Management Center によるリモート管理に対応しています。

お客様が導入したハードウェアまたは仮想 Management Center は、管理対象デバイスと同じまたは新しいバージョンを実行する必要があります。これは、以下を意味します。

- より新しい Management Center でより古いデバイスを管理できます。通常は、メジャーバージョンをいくつか遡ることができます。ただし、導入環境全体を常に更新することをお勧めします。多くの場合、新機能の使用や問題解決の適用には、Management Center とその管理対象デバイスの両方で最新リリースが必要になります。
- Management Center よりも新しいバージョンのデバイスをアップグレードすることはできません。メンテナンス（3 桁）リリースの場合でも、最初に Management Center をアップグレードする必要があります。

表 19: Management Center とデバイス間の互換性

Management Center バージョン	管理可能な最も古いデバイスバージョン
クラウド提供型の管理センター（バージョンなし）	7.0.3 次を参照してください。
7.2	6.6
7.1	6.5
7.0	6.4
6.7	6.3
6.6	6.2.3
6.5	6.2.3
6.4	6.1
6.3	6.1
6.2.3	6.1
6.2.2	6.1
6.2.1	6.1
6.2	6.1
6.1	5.4.0.2/5.4.1.1
6.0.1	5.4.0.2/5.4.1.1
6.0	5.4.0.2/5.4.1.1

Management Center バージョン	管理可能な最も古いデバイスバージョン
5.4.1	<p>5.4.1 (ASA-5506-X シリーズ、ASA5508-X、および ASA5516-X の ASA FirePOWER)。</p> <p>5.3.1 (ASA5512-X、ASA5515-X、ASA5525-X、ASA5545-X、ASA5555-X、および ASA-5585-X シリーズの ASA FirePOWER)。</p> <p>5.3.0 (Firepower 7000/8000 シリーズおよびレガシーデバイス)。</p>

クラウド提供型の管理センター

クラウド提供型の管理センターは、複数のシスコ セキュリティ ソリューションの管理を統合する Cisco Defense Orchestrator (CDO) プラットフォームを通して提供されます。更新についてはシスコが行います。クラウド提供型の管理センターは、以下を実行する Threat Defense デバイスを管理できます。

- 7.0.3 以降のメンテナンスリリース
- バージョン 7.2.0 以降

クラウド提供型の管理センターは、バージョン 7.1 を実行している脅威防御デバイス、または任意のバージョンを実行しているデバイスを管理できません。クラウド管理を登録解除して無効にしない限り、クラウド提供型の管理センターに登録されている脅威防御デバイスをバージョン 7.0.x からバージョン 7.1 にアップグレードすることはできません。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。

クラウド管理デバイスは、イベントのログ記録と分析の目的でのみ、バージョン 7.2 以降のお客様導入の管理センターに追加できます。あるいは、シスコのセキュリティ分析とロギング (SaaS) を使用して、Cisco Cloud にセキュリティイベントを送信できます。

ブラウザ要件

ブラウザ

現在サポートされている MacOS と Microsoft Windows 上で稼働する、次の一般的なブラウザの最新バージョンでテストを実施しています。

- Google Chrome
- Mozilla Firefox
- Microsoft Edge (Windows のみ)

他のブラウザで問題が発生した場合、またはサポートが終了したオペレーティングシステムを実行している場合は、交換またはアップグレードしてください。問題が解消されない場合は、Cisco TAC にお問い合わせください。



- (注) Apple Safari を使用した広範なテストを実施していません。また、FMC ウォークスルーを使用した Microsoft Edge の広範なテストも実施していません。ただし、Cisco TAC で発生した問題に関するフィードバックを求めています。

ブラウザの設定と拡張

ブラウザに関係なく、JavaScript、Cookie、および TLS v1.2 が有効なままになっていることを確認する必要があります。Microsoft Edge を使用している場合は、IE モードを有効にしないでください。

一部のブラウザ拡張機能では、PKI オブジェクトの証明書やキーなどのフィールドに値を保存できないことに注意してください。これらの拡張機能には Grammarly や Whatfix Editor がありますが、それに限りません。この問題は、これらの拡張機能によってフィールドに文字（HTML など）が挿入され、システムが無効と見なすために発生します。シスコの製品にログインしている間は、これらの拡張機能を無効にすることをお勧めします。

画面解像度

インターフェイス	最小解像度
Management Center	1280 X 720
Firepower 4100/9300 用 Chassis Manager	1024 X 768

セキュア通信

初めてログインした場合、システムは自己署名デジタル証明書を使用して Web 通信を保護します。ブラウザに信頼されていない機関に関する警告が表示されますが、信頼ストアに証明書を追加することもできます。これにより継続できるようになりますが、自己署名証明書を、世界的に知られている、または内部で信頼されている認証局（CA）によって署名された証明書に置き換えることをお勧めします。

自己署名証明書の置き換えを開始するには、[システム (System) > [設定 (Configuration)] を選択し、[HTTPS証明書 (HTTPS Certificates)] をクリックします。

詳しい手順については、オンラインヘルプまたはのコンフィギュレーションガイドを参照してください。



(注) 自己署名証明書を置き換えない場合は、次の手順を実行します。

- Google Chrome は、画像、CSS、JavaScript などの静的コンテンツをキャッシュしません。これにより、特に低帯域幅環境では、ページの読み込み時間が長くなります。
 - Mozilla Firefox は、ブラウザの更新時に自己署名証明書を信頼しなくなる場合があります。この場合は Firefox を更新できますが、一部の設定が失われることに注意してください。Mozilla の [Firefox 更新サポートページ](#) を参照してください。
-

監視対象ネットワークからの参照

多くのブラウザでは、デフォルトで Transport Layer Security (TLS) v1.3 が使用されています。暗号化されたトラフィックを処理するために SSL ポリシーを使用していて、モニター対象ネットワーク内のユーザーが TLS v1.3 を有効にしてブラウザを使用している場合、TLS v1.3 をサポートする Web サイトのロードに失敗することがあります。詳細については、『[Failures loading websites using TLS 1.3 with SSL inspection enabled](#)』というタイトルのソフトウェアアドバイザリを参照してください。



第 3 章

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、Threat Defense 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います。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 \(75 ページ\)](#) 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 \(27 ページ\)](#)
- [バージョン 7.2 のアップグレードガイドライン \(28 ページ\)](#)
- [バージョン 7.2 パッチのアップグレードガイドライン \(30 ページ\)](#)
- [応答しないアップグレード \(30 ページ\)](#)
- [Threat Defense 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 \(31 ページ\)](#)
- [時間とディスク容量のテスト \(34 ページ\)](#)

アップグレードする最小バージョン

次のようにバージョン 7.2 に直接アップグレードできます。

表 20:バージョン 7.2 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
Management Center	6.6

プラットフォーム	最小バージョン
Threat Defense (GCP 対応 Threat Defense Virtual を除く)	6.6 Firepower 4100/9300 には FXOS 2.12.0.31 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 2.12 リリースノート を参照してください。
GCP 向け Threat Defense Virtual	7.2 バージョン 7.1 以前からバージョン 7.2 以降にアップグレードすることはできないため、新しいインスタンスを展開する必要があります。バージョン 7.2.x メンテナンスリリースにアップグレードするための最小バージョンは、バージョン 7.2.0 です。「 GCP 向け Threat Defense Virtual はバージョン 7.2.0 を飛び越してアップグレードできない (29 ページ) 」を参照してください。

パッチを適用する最小バージョン

バージョン 7.2 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。

バージョン 7.2 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 21: Management Center を使用した Threat Defense のアップグレードガイドラインバージョン 7.2

✓	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 (27 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 (75 ページ)	Firepower 4100/9300	任意 (Any)	任意 (Any)
	GCP 向け Threat Defense Virtual はバージョン 7.2.0 を飛び越してアップグレードできない (29 ページ)	GCP 用 Threat Defense Virtual	6.7.0 ~ 7.1.x	7.2 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
	高可用性 Management Center の Cisco Secure Malware Analytics に再接続する (29 ページ)	Management Center	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 (30 ページ)	Firepower 1010	6.4.0 ~ 6.6.x	6.7 以降

GCP 向け Threat Defense Virtual はバージョン 7.2.0 を飛び越してアップグレードできない

展開対象 : GCP 向け Threat Defense Virtual

アップグレード元 : バージョン 6.7.0 ~ 7.1.x

直接アップグレード先 : バージョン 7.2.0 以降

自動スケーリングのサポートに必要なインターフェースの変更により、GCP 向け Threat Defense Virtual のアップグレードはバージョン 7.2.0 を飛び越すことができません。つまり、バージョン 7.1.x 以前からバージョン 7.2.0 より後にアップグレードすることはできません。新しいインスタンスを展開し、デバイス固有の設定をやり直す必要があります。

高可用性 Management Center 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 Management Center 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 ～ 4047 の範囲にしてスイッチポートを設定した場合、Threat Defense 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。

バージョン 7.2 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 22: Management Center バージョン 7.2 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 (27 ページ)	任意 (Any)	任意 (Any)	任意のパッチ
	アンインストールに対応するパッチ (110 ページ)	任意 (Any)	任意 (Any)	任意のパッチ

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 Management Center

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 Threat Defense 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。Management Center で、[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。Threat Defense CLI を使用することもできます。



- (注) デフォルトでは、Threat Defense 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。

Threat Defense 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 23: 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。
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。

シングルユニットのクラスタでは、ヒットレスアップグレードはサポートされないことに注意してください。トラフィックフローと検査の中断は、スタンドアロンデバイスと同様に、アクティブユニットのインターフェイス設定に依存します。

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 24: 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 packets 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、Management Center 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 (30 ページ)** を参照してください。

表 25: 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、Management Center 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。

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

ディスク容量テスト

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

また、デバイスアップグレードパッケージ用に Management Center（/Volume または /var 内）に必要な容量も報告します。Threat Defense 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 Device Manager 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 26: ディスク容量の確認

プラットフォーム	コマンド
Management Center	[システム (System)] > [モニタリング (Monitoring)] > [統計 (Statistics)] を選択し、Management Center を選択します。[Disk Usage] で、[By Partition] の詳細を展開します。
Threat Defense with Management Center	[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。

バージョン 7.2.0.1 の時間とディスク容量

表 27: バージョン 7.2.0.1 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	Management Center の必要容量	アップグレード時間	リポート時間
Management Center	/ボリューム内で 59 MB	/内で 22 MB	—	7 分	7 分

プラットフォーム	ボリュームの容量	必要容量	Management Center の必要容量	アップグレード時間	リブート時間
Management Center Virtual : VMware	/ボリューム内で 61 MB	/内で 15 MB	—	10 分	4 分
Firepower 1000 シリーズ	—	/ngfw 内 1.2 GB	250 MB	7 分	10 分
Firepower 2100 シリーズ	—	/ngfw 内で 1.2 GB	300 MB	5 分	10 分
Secure Firewall 3100 シリーズ	—	/ngfw 内で 2.1 GB	490 MB	9 分	4 分
Firepower 4100 シリーズ	—	/ngfw 内 1.1 GB	51 MB	5 分	7 分
Firepower 4100 シリーズ コンテナ インスタンス	—	/ngfw 内 1.1 GB	51 MB	5 分	3 分
Firepower 9300	—	/ngfw 内 1.1 GB	51 MB	4 分	9 分
ISA 3000	/ngfw/var 内で 630 MB	/ngfw/bin 内で 180 MB	56 MB	9 分	12 分
Threat Defense Virtual : VMware	/ngfw/var 内で 660 MB	/ngfw/bin 内で 170 MB	56 MB	4 分	4 分

バージョン 7.2.0 の時間とディスク容量

表 28:バージョン 7.2.0 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	Management Center の必要容量	アップグレード時間	リブート時間
Management Center	バージョン 6.6.0 ~ 6.7.0	/var 内で 16.7 GB	/内で 51 MB	—	30 分	9 分
	バージョン 7.0 以降	/Volume 内で 19.1 GB	/内で 45 MB			
Management Center Virtual : VMware	バージョン 6.6.0 ~ 6.7.0	/var 内で 16.7 GB	/内で 50 MB で	—	30 分	5 分
	バージョン 7.0 以降	/Volume 内で 19.2 GB	/内で 45 MB			
Firepower 1000 シリーズ	—	—	/ngfw 内で 7.6 GB	930 MB	15 分	13 分
Firepower 2100 シリーズ	—	—	/ngfw 内で 7.7 GB	1.0 GB	13 分	13 分

プラットフォーム	ボリュームの容量	必要容量	Management Center の必要容量	アップグレード時間	リブート時間	
Secure Firewall 3100 シリーズ	—	使用できません	1.2 GB	使用できません	使用できません	
Firepower 4100 シリーズ	—	/ngfw 内で 7.8 GB	880 MB	12 分	9 分	
Firepower 4100 シリーズ コンテナ インスタンス	—	/ngfw 内で 7.9 GB	880 MB	12 分	8 分	
Firepower 9300	—	/ngfw 内で 11.2 GB	880 MB	11 分	12 分	
ISA 3000	バージョン 6.6.0	/home 内で 9.3 GB	/ngfw 内で 270 KB	1.0 GB	21 分	8 分
	バージョン 6.7.0	/ngfw/Volume 内で 9.3 GB	/ngfw 内で 270 KB			
	バージョン 7.0.0 ~ 7.1.0	/ngfw/var 内で 9.3 GB	/ngfw/bin 内で 270 KB			
Threat Defense Virtual : VMware	バージョン 6.6.0	/home 内で 4.6 GB	/ngfw 内で 350 KB	1.0 GB	11 分	8 分
	バージョン 6.7.0	/ngfw/Volume 内で 4.4 GB	/ngfw 内で 350 KB			
	バージョン 7.0.0 ~ 7.1.0	/ngfw/var 内で 5.4 GB	/ngfw/bin 内で 250 KB			



第 4 章

Management Center のアップグレード

- [Management Center のアップグレードチェックリスト \(39 ページ\)](#)
- [Management Center のアップグレードパス \(43 ページ\)](#)
- [アップグレードパッケージのアップロード \(45 ページ\)](#)
- [Management Center のアップグレード準備状況チェック \(46 ページ\)](#)
- [Management Center のアップグレード：スタンドアロン \(47 ページ\)](#)
- [Management Center のアップグレード：ハイアベイラビリティ \(48 ページ\)](#)

Management Center のアップグレード チェックリスト

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。

✓	アクション/チェック	詳細
	展開を評価します。	状況を理解することにより、目的を達成する方法を決定します。現在のバージョンとモデル情報に加えて、展開が高可用性/拡張性を実現するように設定されているかどうか、デバイスが IPS またはファイアウォールとして展開されているかどうかなどを確認します。
	アップグレードパスを計画します。	これは、大規模展開、マルチホップアップグレード、または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。次を参照してください。 <ul style="list-style-type: none">• Management Center のアップグレードパス (43 ページ)• Threat Defense のアップグレードパス (55 ページ)• FXOS のアップグレードパス (78 ページ)

✓	アクション/チェック	詳細
	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。	<p>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。リリースノートを使用して開始します。</p> <ul style="list-style-type: none"> • Cisco Secure Firewall Threat Defense リリースノート • Cisco Firepower 4100/9300 FXOS リリースノート
	アプライアンスへのアクセスを確認します。	<p>デバイスは、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せん。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。</p> <p>デバイスを經由せずに Management Center の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。</p>
	帯域幅を確認します。	<p>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。可能な場合は常に、アップグレードパッケージを事前にアップロードしてください。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。</p> <p>『Firepower Management Center から管理対象装置へのデータをダウンロードするためのガイドライン』（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。</p>
	メンテナンス時間帯をスケジュールします。	<p>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、この時間帯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。</p> <p>Threat Defense 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 (31 ページ) および 時間とディスク容量のテスト (34 ページ) を参照してください。</p>

バックアップ

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。

- アップグレード前：アップグレードが致命的な失敗であった場合は、再イメージ化を実行し、復元する必要がある場合があります。再イメージ化によって、システムパスワードを

含むほとんどの設定が工場出荷時の初期状態に戻ります。最近のバックアップがある場合は、通常の操作にすばやく戻ることができます。

- アップグレード後：これにより、新しくアップグレードされた展開のスナップショットが作成されます。新しいManagement Centerバックアップファイルがデバイスがアップグレードされたことを「認識」するように、管理対象デバイスをアップグレードした後にManagement Center をバックアップしてください。

✓	アクション/チェック	詳細
	設定およびイベントをバックアップします。	Cisco Secure Firewall Management Center アドミニストレーションガイド の「バックアップ/復元」の章を参照してください。
	Firepower 4100/9300 のFXOS をバックアップします。	Chassis Manager または FXOS CLI を使用して、論理デバイス設定およびプラットフォーム設定を含むシャーシ設定をエクスポートします。 詳細については、『 Cisco Firepower 4100/9300 FXOS コンフィギュレーションガイド 』の「コンフィギュレーションのインポート/エクスポート」を参照してください。

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。アップグレードの前にアップグレードパッケージをシステムにアップロードすると、メンテナンス時間が短縮されます。

✓	アクション/チェック	詳細
	アップグレードパッケージをアップロードします。	Management Center の高可用性では、Management Center アップグレードパッケージを両方のピアにアップロードし、パッケージをスタンバイに転送する前に同期を一時停止する必要があります。同期の中断を制限するには、アップグレードの準備段階でパッケージをアクティブのピアに転送し、同期を一時停止した後に、実際のアップグレードプロセスの一環としてスタンバイのピアに転送します。 アップグレードパッケージのアップロード (45 ページ) を参照してください。

関連するアップグレード

メンテナンス時間帯にホスティング環境のアップグレードを実行することをお勧めします。

✓	アクション/チェック	詳細
	仮想ホスティングをアップグレードします。	必要に応じて、ホスティング環境をアップグレードします。通常、古いバージョンのVMwareを実行していて、メジャーアップグレードを実行している場合、アップグレードが必要です。

最終チェック

一連の最終チェックにより、ソフトウェアをアップグレードする準備が整います。

✓	アクション/チェック	詳細
	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。
	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リケーションが同期していることを確認します。時刻のずれが10秒を超えている場合、ヘルスマニター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。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。 時刻を確認するには、次の手順を実行します。 <ul style="list-style-type: none"> • Management Center : [システム (System)] > [設定 (Configuration)] > [時刻 (Time)] を選択します。 • Threat Defense : 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。 時間とディスク容量のテスト (34 ページ) 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。これは、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ります。 Threat Defense 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 (31 ページ) を参照してください。
	準備状況チェックを実行します。	互換性と準備状況のチェックに合格すると、アップグレードが失敗する可能性が低くなります。 Management Center のアップグレード準備状況チェック (46 ページ) を参照してください。

✓	アクション/チェック	詳細
	実行中のタスクを確認します。	<p>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。</p> <p>バージョン 6.6.3+からのアップグレードは、スケジュールされたタスクを自動的に延期します。アップグレード中に開始するようにスケジュールされたタスクは、アップグレード後の再起動の5分後に開始されます。これが起こらないようにするには（または以前のバージョンからアップグレードする場合）、アップグレード中に実行するようにスケジュールされているタスクを確認し、それらをキャンセルまたは延期します。</p>

Management Center のアップグレードパス

次の表に、Management Center のアップグレードパスを示します。

Management Center では、その管理対象デバイスと同じまたはより新しいバージョンを実行する必要があります。Management Center よりも新しいバージョンのデバイスをアップグレードすることはできません。メンテナンス（3桁）リリースの場合でも、最初に Management Center をアップグレードする必要があります。

現在の Threat Defense /Management Center のバージョンが対象のバージョンより後の日付にリリースされた場合、期待どおりにアップグレードできない可能性があります。このような場合、アップグレードはすぐに失敗し、2つのバージョン間にデータストアの非互換性があることを説明するエラーが表示されます。現在のバージョンと対象のバージョンの両方に関するリリースノートには、特定の制限が掲載されています。

表 29: Management Center の直接アップグレード

現在のバージョン	ターゲットバージョン
7.2	→ 以降の 7.2.x メンテナンスリリース
7.1	<p>次のいずれかです。</p> <p>→ 7.2 または 7.2.x メンテナンスリリース</p> <p>→ 以降の 7.1.x メンテナンスリリース</p>

現在のバージョン	ターゲットバージョン
7.0 FMC 1000、2500、4500 に対する最後のサポート	次のいずれかです。 → 7.2 または 7.2.x メンテナンスリリース → 7.1 または 7.1.x メンテナンスリリース → 7.0.x 以降のメンテナンスリリース (注) 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。
6.7	次のいずれかです。 → 7.2 または 7.2.x メンテナンスリリース → 7.1 または 7.1.x メンテナンスリリース → 7.0 または 7.0.x メンテナンスリリース → 6.7.x メンテナンスリリース以降
6.6 FMC 2000 および 4000 の最後のサポート。	次のいずれかです。 → 7.2 または 7.2.x メンテナンスリリース → 7.1 または 7.1.x メンテナンスリリース → 7.0 または 7.0.x メンテナンスリリース → 6.7 または 6.7.x メンテナンスリリース → 6.6.x メンテナンスリリース以降 (注) データストアの非互換性のため、FMC をバージョン 6.6.5 以降からバージョン 6.7.0 にアップグレードすることができません。バージョン 7.0 以降に直接アップグレードすることをお勧めします。
6.5	次のいずれかです。 → 7.1 または 7.1.x メンテナンスリリース → 7.0 または 7.0.x メンテナンスリリース → 6.7 または 6.7.x メンテナンスリリース → 6.6 または 6.6.x メンテナンスリリース

現在のバージョン	ターゲットバージョン
6.4 FMC 750、1500、および3500の最後のサポート。	次のいずれかです。 → 7.0 または 7.0.x メンテナンスリリース → 6.7 または 6.7.x メンテナンスリリース → 6.6 または 6.6.x メンテナンスリリース → 6.5
6.3	次のいずれかです。 → 6.7 または 6.7.x メンテナンスリリース → 6.6 または 6.6.x メンテナンスリリース → 6.5 → 6.4
6.2.3	次のいずれかです。 → 6.6 または 6.6.x メンテナンスリリース → 6.5 → 6.4 → 6.3

アップグレードパッケージのアップロード

アップグレードパッケージは、署名付きの tar アーカイブ (.tar) です。署名付きのパッケージをアップロードした後、パッケージが確認されるため、Management Center の [システムの更新 (System Updates)] ページのロードに数分かかることがあります。表示を迅速化するには、不要なアップグレードパッケージを削除してください。署名付きのパッケージは解凍しないでください。

始める前に

高可用性ペアのスタンバイの Management Center をアップグレードしている場合は、同期を一時停止します。

Management Center の高可用性では、Management Center アップグレードパッケージを両方のピアにアップロードし、パッケージをスタンバイに転送する前に同期を一時停止する必要があります。同期の中断を制限するには、アップグレードの準備段階でパッケージをアクティブのピアに転送し、同期を一時停止した後に、実際のアップグレードプロセスの一環としてスタンバイのピアに転送します。

- ステップ 1** シスコサポートおよびダウンロードサイトから適切なアップグレードパッケージをダウンロードします。
<https://www.cisco.com/go/firepower-software>
- ファミリまたはシリーズのすべてのモデルに同じソフトウェアアップグレードパッケージを使用します。適切なソフトウェアを見つけるには、使用しているモデルを選択または検索し、適切なバージョンのソフトウェアのダウンロードページを参照します。使用可能なアップグレードパッケージは、インストールパッケージ、ホットフィックス、およびその他の該当するダウンロードとともに表示されます。
- アップグレードパッケージのファイル名には、次のように、プラットフォーム、パッケージタイプ（アップグレード、パッチ、ホットフィックス）、ソフトウェアバージョン、およびビルドが反映されています。
- ```
Cisco_Secure_FW_Mgmt_Center_Upgrade-7.2-999.sh.REL.tar
```
- ステップ 2** Management Center で、[システム (System)] > [更新 (Updates)] を選択します。
- ステップ 3** [更新のアップロード (Upload Update)] をクリックします。
- ヒント** 一部のアップグレードパッケージは、リリースが手動でダウンロードできるようになってからしばらくすると、直接ダウンロードできるようになります。遅延の長さは、リリースの種類、リリースの選択、およびその他の要因によって異なります。Management Center がインターネットにアクセスできる場合は、代わりに [アップデートのダウンロード (Download Updates)] をクリックして、展開の対象となるすべてのパッケージと、必要に応じて最新の VDB をダウンロードできます。
- ステップ 4** [アクション (Action)] については、[ローカル ソフトウェア アップデート パッケージのアップロード (Upload local software update package)] オプションボタンをクリックします。
- ステップ 5** [Choose File] をクリックします。
- ステップ 6** パッケージを参照し、[Upload] をクリックします。

## Management Center のアップグレード準備状況チェック

Management Center 準備状況チェックを実行するには、次の手順を使用します。

準備状況チェックでは、メジャーアップグレードとメンテナンスアップグレードの準備状況进行评估します。準備状況チェックで不合格になると、問題を修正するまでアップグレードできません。準備状況チェックの実行に必要な時間は、モデルとデータベースのサイズによって異なります。準備状況チェックを行っている間は、手動で再起動またはシャットダウンしないでください。

### 始める前に

アップグレードパッケージを Management Center にアップロードします。

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

**ステップ2** [利用可能なアップデート (Available Updates)] で該当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、Management Center を選択します。

**ステップ3** [準備状況の確認 (Check Readiness)] をクリックします。

メッセージセンターで準備状況チェックの進行状況をモニターできます。

### 次のタスク

[システム (System)] > [更新 (Updates)] ページで、[準備状況チェック (Readiness Checks)] をクリックすると、進行中のチェックや不合格のチェックなど、展開全体の準備状況チェックのステータスが表示されます。また、このページを使用して、不合格となった後にチェックを簡単に再実行することもできます。

## Management Center のアップグレード：スタンドアロン

この手順を使用して、スタンドアロンの Management Center をアップグレードします。



**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。

### 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。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** Management Center で、[システム (System)] > [更新 (Updates)] を選択します。

**ステップ2** [利用可能なアップデート (Available Updates)] で該当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、Management Center を選択します。

**ステップ3** [インストール (Install)] をクリックし、アップグレードして再起動することを確認します。

ログアウトするまで、メッセージセンターで事前チェックの進行状況をモニターできます。

**ステップ4** 可能なときに、再度ログインします。

- メジャーアップグレードとメンテナンスアップグレード：アップグレードが完了する前にログインできます。アップグレードの進行状況をモニターし、アップグレードログとエラーメッセージを確認するために使用できるページが表示されます。アップグレードが完了し、システムが再起動すると再度ログアウトされます。リブート後に、再ログインしてください。
- パッチとホットフィックス：アップグレードと再起動が完了した後にログインできます。

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。

ログイン時にアップグレードの成功メッセージが表示されない場合は、[ヘルプ (Help)] > [バージョン情報 (About)] を選択して、現在のソフトウェアのバージョン情報を表示します。

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 アップグレード後に必要な構成変更があれば、実行します。

ステップ8 管理対象デバイスに構成を再展開します。

---

## Management Center のアップグレード：ハイアベイラビリティ

ハイアベイラビリティ Management Center を1つずつアップグレードします。同期を一時停止して、まずスタンバイをアップグレードしてから、アクティブにします。スタンバイのアップグレードが開始されると、ステータスがスタンバイからアクティブに切り替わり、両方のピアがアクティブになります。この一時的な状態のことを「スプリットブレイン」と呼び、アップグレード中（およびパッチのアンインストール中）を除き、サポートされていません。



**注意** ペアが split-brain の状態で、構成の変更または展開を行わないでください。同期の再開後は変更内容が失われます。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、アッ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。

### 始める前に

両方のピアの事前アップグレードチェックリストを完了します。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 アクティブ状態の Management Center で、同期を一時停止します。

- [システム (System)] > [統合 (Integration)] の順に選択します。
- [ハイアベイラビリティ (High Availability)] タブで、[同期の一時停止 (Pause Synchronization)] をクリックします。

**ステップ2** アップグレードパッケージをスタンバイにアップロードします。

Management Center の高可用性では、Management Center アップグレードパッケージを両方のピアにアップロードし、パッケージをスタンバイに転送する前に同期を一時停止する必要があります。同期の中断を制限するには、アップグレードの準備段階でパッケージをアクティブのピアに転送し、同期を一時停止した後に、実際のアップグレードプロセスの一環としてスタンバイのピアに転送します。

**ステップ3** ピアを一度に1つずつアップグレード：最初はスタンバイ、次はアクティブです。

「[Management Center のアップグレード：スタンドアロン \(47 ページ\)](#)」の手順に従います。各ピアで更新が成功したことを確認したら停止します。要約すると、各ピアで次の手順を実行します。

- a) [システム (System)] > [更新 (Updates)] ページで、アップグレードをインストールします。
- b) ログアウトするまで進行状況をモニターし、ログインできる状態になったら再度ログインします（これは2回行われる場合があります）。
- c) アップグレードが成功したことを確認します。

**ステップ4** アクティブピアにする Management Center で、同期を再開します。

- a) [システム (System)] > [統合 (Integration)] の順に選択します。
- b) [ハイアベイラビリティ (High Availability)] タブで、[アクティブにする (Make-Me-Active)] をクリックします。
- c) 同期が再開し、その他の Management Center がスタンバイモードに切り替わるまで待ちます。

**ステップ5** 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6** アップグレード後に必要な構成変更があれば、実行します。

**ステップ7** 管理対象デバイスに構成を再展開します。







## 第 5 章

# Threat Defense のアップグレード

- [Threat Defense のアップグレードチェックリスト \(51 ページ\)](#)
- [Threat Defense のアップグレードパス \(55 ページ\)](#)
- [アップグレードパッケージのアップロード \(61 ページ\)](#)
- [Threat Defense のアップグレード準備状況チェック \(66 ページ\)](#)
- [Threat Defense のアップグレード \(67 ページ\)](#)

## Threat Defense のアップグレードチェックリスト

### 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。

| ✓ | アクション/チェック       | 詳細                                                                                                                                                                                                                                                                                                              |
|---|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|   | 展開を評価します。        | 状況を理解することにより、目的を達成する方法を決定します。現在のバージョンとモデル情報に加えて、展開が高可用性/拡張性を実現するように設定されているかどうか、デバイスが IPS またはファイアウォールとして展開されているかどうかなどを確認します。                                                                                                                                                                                     |
|   | アップグレードパスを計画します。 | これは、大規模展開、マルチホップアップグレード、または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。次を参照してください。 <ul style="list-style-type: none"><li>• <a href="#">Management Center のアップグレードパス (43 ページ)</a></li><li>• <a href="#">Threat Defense のアップグレードパス (55 ページ)</a></li><li>• <a href="#">FXOS のアップグレードパス (78 ページ)</a></li></ul> |

| ✓ | アクション/チェック                    | 詳細                                                                                                                                                                                                                                                                                                           |
|---|-------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|   | 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。 | <p>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。リリースノートを使用して開始します。</p> <ul style="list-style-type: none"> <li>• <a href="#">Cisco Secure Firewall Threat Defense リリースノート</a></li> <li>• <a href="#">Cisco Firepower 4100/9300 FXOS リリースノート</a></li> </ul>                                     |
|   | アプライアンスへのアクセスを確認します。          | <p>デバイスは、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せん。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。</p> <p>デバイスを經由せずに <b>Management Center</b> の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。</p>                                                                                       |
|   | 帯域幅を確認します。                    | <p>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。可能な場合は常に、アップグレードパッケージを事前にアップロードしてください。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。</p> <p>『<a href="#">Firepower Management Center から管理対象装置へのデータをダウンロードするためのガイドライン</a>』（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。</p> |
|   | メンテナンス時間帯をスケジュールします。          | <p>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、この時間帯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。</p> <p><a href="#">Threat Defense 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 (31 ページ)</a> および <a href="#">時間とディスク容量のテスト (34 ページ)</a> を参照してください。</p>                                       |

### バックアップ

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。

- アップグレード前：アップグレードが致命的な失敗であった場合は、再イメージ化を実行し、復元する必要がある場合があります。再イメージ化によって、システムパスワードを

含むほとんどの設定が工場出荷時の初期状態に戻ります。最近のバックアップがある場合は、通常の操作にすばやく戻ることができます。

- アップグレード後：これにより、新しくアップグレードされた展開のスナップショットが作成されます。新しい Management Center バックアップファイルがデバイスがアップグレードされたことを「認識」するように、管理対象デバイスをアップグレードした後に Management Center をバックアップしてください。

| ✓ | アクション/チェック                             | 詳細                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|---|----------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|   | Threat Defense をバックアップします。             | サポートされている場合は、Management Center を使用して Threat Defense 構成をバックアップします。 <a href="#">Cisco Secure Firewall Management Center アドミニストレーションガイド</a> の「バックアップ/復元」の章を参照してください。<br><br>Firepower 9300 で Threat Defense および ASA 論理デバイスが別のモジュールで実行されている場合、ASDM または ASA CLI を使用して、構成やその他の重要なファイルをバックアップしてください（特に ASA 構成の移行がある場合）。『 <a href="#">Cisco ASA Series General Operations Configuration Guide</a> 』の「 <i>Software and Configurations</i> 」の章を参照してください。 |
|   | Firepower 4100/9300 の FXOS をバックアップします。 | Chassis Manager または FXOS CLI を使用して、論理デバイス設定およびプラットフォーム設定を含むシャーシ設定をエクスポートします。<br><br>詳細については、『 <a href="#">Cisco Firepower 4100/9300 FXOS コンフィギュレーションガイド</a> 』の「コンフィギュレーションのインポート/エクスポート」を参照してください。                                                                                                                                                                                                                                             |

### 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。アップグレードの前にアップグレードパッケージをシステムにアップロードすると、メンテナンス時間が短縮されます。

| ✓ | アクション/チェック              | 詳細                                                                                                                                                                                                            |
|---|-------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|   | アップグレードパッケージをアップロードします。 | Management Center またはデバイスがアクセスできる内部サーバーに Threat Defense アップグレードパッケージをアップロードします。 <a href="#">アップグレードパッケージのアップロード (61 ページ)</a> を参照してください。<br><br>Firepower 4100/9300 の場合、FXOS アップロード手順は FXOS アップグレード手順に含まれています。 |

### 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。

| ✓ | アクション/チェック                              | 詳細                                                                                                                                                                                                                                          |
|---|-----------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|   | 仮想ホスティングをアップグレードします。                    | 必要に応じて、ホスティング環境をアップグレードします。通常、古いバージョンの VMware を実行していて、メジャーアップグレードを実行している場合、アップグレードが必要です。                                                                                                                                                    |
|   | Firepower 4100/9300 の FXOS をアップグレードします。 | FXOS のアップグレードは通常、メジャーアップグレードの要件ですが、メンテナンスリリースやパッチの場合は要件になるのは非常にまれです。トラフィックフローとインスペクションでの中断を防ぐには、Threat Defense 高可用性ペアおよびシャーシ間クラスタの FXOS を一度に 1 つずつアップグレードします。<br><br><a href="#">Firepower 4100/9300 の FXOS アップグレード (75 ページ)</a> を参照してください。 |

### 最終チェック

一連の最終チェックにより、ソフトウェアをアップグレードする準備が整います。

| ✓ | アクション/チェック    | 詳細                                                                                                                                                                                                                                                                                                                                                                                |
|---|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|   | 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。                                                                                                                                                                                                                                                                                                                           |
|   | 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。時刻のずれが 10 秒を超えている場合、ヘルスマニター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。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。<br><br>時刻を確認するには、次の手順を実行します。 <ul style="list-style-type: none"> <li>• Management Center : [システム (System) ] &gt; [設定 (Configuration) ] &gt; [時刻 (Time) ] を選択します。</li> <li>• Threat Defense : <b>show time</b> CLI コマンドを使用します。</li> </ul> |

| ✓ | アクション/チェック      | 詳細                                                                                                                                                                                                                                                                                        |
|---|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|   | 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。<br><br><a href="#">時間とディスク容量のテスト (34 ページ)</a> 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。これは、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ります。 <a href="#">Threat Defense 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 (31 ページ)</a> を参照してください。                                                                                                                                    |
|   | 準備状況チェックを実行します。 | 互換性と準備状況のチェックに合格すると、アップグレードが失敗する可能性が低くなります。<br><br><a href="#">Threat Defense のアップグレード準備状況チェック (66 ページ)</a> を参照してください。                                                                                                                                                                    |
|   | 実行中のタスクを確認します。  | 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。<br><br>バージョン 6.6.3+ からのアップグレードは、スケジュールされたタスクを自動的に延期します。アップグレード中に開始するようにスケジュールされたタスクは、アップグレード後の再起動の 5 分後に開始されます。これが起こらないようにするには（または以前のバージョンからアップグレードする場合）、アップグレード中に実行するようにスケジュールされているタスクを確認し、それらをキャンセルまたは延期します。 |

## Threat Defense のアップグレードパス

展開に一致するアップグレードパスを選択します。

Management Center では、その管理対象デバイスと同じまたはより新しいバージョンを実行する必要があります。Management Center よりも新しいバージョンのデバイスをアップグレードすることはできません。メンテナンス（3 桁）リリースの場合でも、最初に Management Center をアップグレードする必要があります。

## FXOS を使用する Threat Defense のアップグレードパス

次の表に、Firepower 4100/9300 の Threat Defense のアップグレードパスを示します。

現在の Threat Defense /Management Center のバージョンが対象のバージョンより後の日付にリリースされた場合、期待どおりにアップグレードできない可能性があります。このような場合、アップグレードはすぐに失敗し、2つのバージョン間にデータストアの非互換性があることを説明するエラーが表示されます。現在のバージョンと対象のバージョンの両方に関するリリースノートには、特定の制限が掲載されています。

この表には、シスコにより特別に認定されたバージョンの組み合わせのみが掲載されています。最初に FXOS をアップグレードするため、サポートされている（ただし推奨されていない）組み合わせを短時間実行します。ここでは、FXOS が論理デバイスの「前」になります。最小限のビルドおよびその他の詳細な互換性情報については、[Cisco Secure Firewall Threat Defense 互換性ガイド](#) を参照してください。

表 30 : Firepower 4100/9300 での Threat Defense の直接アップグレード

| 現在のバージョン                             | 対象のバージョン                                                                                                   |
|--------------------------------------|------------------------------------------------------------------------------------------------------------|
| Threat Defense 7.2 を搭載した FXOS 2.12   | → Threat Defense 7.2.x 以降のメンテナンスリリースを搭載した FXOS 2.12                                                        |
| Threat Defense 7.1 を搭載した FXOS 2.11.1 | 次のいずれかです。<br>→ Threat Defense 7.2 を搭載した FXOS 2.12<br>→ Threat Defense 7.1.x 以降のメンテナンスリリースを搭載した FXOS 2.11.1 |

| 現在のバージョン                             | 対象のバージョン                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|--------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Threat Defense 7.0 を搭載した FXOS 2.10.1 | <p>次のいずれかです。</p> <ul style="list-style-type: none"> <li>→ Threat Defense 7.2 を搭載した FXOS 2.12</li> <li>→ Threat Defense 7.1 を搭載した FXOS 2.11.1</li> <li>→ Threat Defense 7.0.x 以降のメンテナンスリリースを搭載した FXOS 2.10.1</li> </ul> <p>(注) 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。</p> <p>(注) クラウド提供型の管理センターは、バージョン 7.1 を実行している脅威防御デバイス、または任意のバージョンを実行しているデバイスを管理できません。クラウド管理を登録解除して無効にしない限り、クラウド提供型の管理センターに登録されている脅威防御デバイスをバージョン 7.0.x からバージョン 7.1 にアップグレードすることはできません。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。</p> |
| Threat Defense 6.7 を搭載した FXOS 2.9.1  | <p>次のいずれかです。</p> <ul style="list-style-type: none"> <li>→ Threat Defense 7.2 を搭載した FXOS 2.12</li> <li>→ Threat Defense 7.1 を搭載した FXOS 2.11.1</li> <li>→ Threat Defense 7.0 を搭載した FXOS 2.10.1</li> <li>→ Threat Defense 6.7.x 以降のメンテナンスリリースを搭載した FXOS 2.9.1</li> </ul>                                                                                                                                                                                                                                                                                      |
| Threat Defense 6.6 を搭載した FXOS 2.8.1  | <p>次のいずれかです。</p> <ul style="list-style-type: none"> <li>→ Threat Defense 7.2 を搭載した FXOS 2.12</li> <li>→ Threat Defense 7.1 を搭載した FXOS 2.11.1</li> <li>→ Threat Defense 7.0 を搭載した FXOS 2.10.1</li> <li>→ Threat Defense 6.7 を搭載した FXOS 2.9.1</li> <li>→ Threat Defense 6.6.x 以降のメンテナンスリリースを搭載した FXOS 2.8.1</li> </ul>                                                                                                                                                                                                                                       |

| 現在のバージョン                              | 対象のバージョン                                                                                                                                                                        |
|---------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Threat Defense 6.5 を搭載した FXOS 2.7.1   | 次のいずれかです。<br>→ Threat Defense 7.1 を搭載した FXOS 2.11.1<br>→ Threat Defense 7.0 を搭載した FXOS 2.10.1<br>→ Threat Defense 6.7 を搭載した FXOS 2.9.1<br>→ Threat Defense 6.6 を搭載した FXOS 2.8.1 |
| Threat Defense 6.4 を搭載した FXOS 2.6.1   | 次のいずれかです。<br>→ Threat Defense 7.0 を搭載した FXOS 2.10.1<br>→ Threat Defense 6.7 を搭載した FXOS 2.9.1<br>→ Threat Defense 6.6 を搭載した FXOS 2.8.1<br>→ Threat Defense 6.5 を搭載した FXOS 2.7.1  |
| Threat Defense 6.3 を搭載した FXOS 2.4.1   | 次のいずれかです。<br>→ Threat Defense 6.7 を搭載した FXOS 2.9.1<br>→ Threat Defense 6.6 を搭載した FXOS 2.8.1<br>→ Threat Defense 6.5 を搭載した FXOS 2.7.1<br>→ Threat Defense 6.4 を搭載した FXOS 2.6.1   |
| Threat Defense 6.2.3 を搭載した FXOS 2.3.1 | 次のいずれかです。<br>→ Threat Defense 6.6 を搭載した FXOS 2.8.1<br>→ Threat Defense 6.5 を搭載した FXOS 2.7.1<br>→ Threat Defense 6.4 を搭載した FXOS 2.6.1<br>→ Threat Defense 6.3 を搭載した FXOS 2.4.1   |

## FXOS を使用しない Threat Defense のアップグレードパス

この表は、FXOS をアップグレードする必要がない場合の Threat Defense のアップグレードパスを示しています。

現在の Threat Defense /Management Center のバージョンが対象のバージョンより後の日付にリリースされた場合、期待どおりにアップグレードできない可能性があります。このような場合、アップグレードはすぐに失敗し、2つのバージョン間にデータストアの非互換性があることを説明するエラーが表示されます。現在のバージョンと対象のバージョンの両方に関するリリースノートには、特定の制限が掲載されています。





- (注) 自動スケーリングのサポートに必要なインターフェースの変更により、GCP 向け Threat Defense Virtual のアップグレードはバージョン 7.2.0 を飛び越すことができません。つまり、バージョン 7.1.x 以前からバージョン 7.2.0 より後にアップグレードすることはできません。新しいインスタンスを展開し、デバイス固有の設定をやり直す必要があります。

表 31: Threat Defense の直接アップグレード

| 現在のバージョン                                  | ターゲットバージョン                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 7.2                                       | → 以降の 7.2.x メンテナンスリリース                                                                                                                                                                                                                                                                                                                                                                                                             |
| 7.1                                       | 次のいずれかです。<br>→ 7.2 または 7.2.x メンテナンスリリース<br>→ 以降の 7.1.x メンテナンスリリース                                                                                                                                                                                                                                                                                                                                                                  |
| 7.0<br>ASA 5508-X および 5516-X における最後のサポート。 | 次のいずれかです。<br>→ 7.2 または 7.2.x メンテナンスリリース<br>→ 7.1 または 7.1.x メンテナンスリリース<br>→ 7.0.x 以降のメンテナンスリリース<br><br>(注) 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。<br><br>(注) クラウド提供型の管理センターは、バージョン 7.1 を実行している脅威防御デバイス、または任意のバージョンを実行しているデバイスを管理できません。クラウド管理を登録解除して無効にしない限り、クラウド提供型の管理センターに登録されている脅威防御デバイスをバージョン 7.0.x からバージョン 7.1 にアップグレードすることはできません。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。 |

| 現在のバージョン                                     | ターゲットバージョン                                                                                                                                                |
|----------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
| 6.7                                          | 次のいずれかです。<br>→ 7.2 または 7.2.x メンテナンスリリース<br>→ 7.1 または 7.1.x メンテナンスリリース<br>→ 7.0 または 7.0.x メンテナンスリリース<br>→ 6.7.x メンテナンスリリース以降                               |
| 6.6<br>ASA 5525-X、5545-X、5555-X における最後のサポート。 | 次のいずれかです。<br>→ 7.2 または 7.2.x メンテナンスリリース<br>→ 7.1 または 7.1.x メンテナンスリリース<br>→ 7.0 または 7.0.x メンテナンスリリース<br>→ 6.7 または 6.7.x メンテナンスリリース<br>→ 6.6.x メンテナンスリリース以降 |
| 6.5                                          | 次のいずれかです。<br>→ 7.1 または 7.1.x メンテナンスリリース<br>→ 7.0 または 7.0.x メンテナンスリリース<br>→ 6.7 または 6.7.x メンテナンスリリース<br>→ 6.6 または 6.6.x メンテナンスリリース                         |
| 6.4<br>ASA 5515-X における最後のサポート。               | 次のいずれかです。<br>→ 7.0 または 7.0.x メンテナンスリリース<br>→ 6.7 または 6.7.x メンテナンスリリース<br>→ 6.6 または 6.6.x メンテナンスリリース<br>→ 6.5                                              |
| 6.3                                          | 次のいずれかです。<br>→ 6.7 または 6.7.x メンテナンスリリース<br>→ 6.6 または 6.6.x メンテナンスリリース<br>→ 6.5<br>→ 6.4                                                                   |

| 現在のバージョン                    | ターゲットバージョン                 |
|-----------------------------|----------------------------|
| 6.2.3                       | 次のいずれかです。                  |
| ASA 5506-X シリーズにおける最後のサポート。 | → 6.6 または 6.6.x メンテナンスリリース |
|                             | → 6.5                      |
|                             | → 6.4                      |
|                             | → 6.3                      |

## アップグレードパッケージのアップロード

Threat Defense アップグレードパッケージを Management Center または内部 Web サーバーにアップロードした後、それらをデバイスにコピーできます。

### Management Center への Threat Defense アップグレードパッケージのアップロード

アップグレードパッケージは、署名付きの tar アーカイブ (.tar) です。署名付きのパッケージをアップロードした後、パッケージが確認されるため、Management Center の [システムの更新 (System Updates) ] ページのロードに数分かかることがあります。表示を迅速化するには、不要なアップグレードパッケージを削除してください。署名付きのパッケージは解凍しないでください。

**ステップ 1** シスコ サポートおよびダウンロード サイト : <https://www.cisco.com/go/ftd-software> からのアップグレードパッケージをダウンロードします。

ファミリーまたはシリーズのすべてのモデルに同じソフトウェアアップグレードパッケージを使用します。適切なソフトウェアを見つけるには、使用しているモデルを選択または検索し、適切なバージョンのソフトウェアのダウンロードページを参照します。使用可能なアップグレードパッケージは、インストールパッケージ、ホットフィックス、およびその他の該当するダウンロードとともに表示されます。アップグレードパッケージのファイル名には、プラットフォーム、パッケージタイプ (アップグレード、パッチ、ホットフィックス)、ソフトウェアバージョン、およびビルドが反映されています。

|                           |                                               |
|---------------------------|-----------------------------------------------|
| Firepower 1000 シリーズ       | Cisco_FTD_SSP-FP1K_Upgrade-7.2-999.sh.REL.tar |
| Firepower 2100 シリーズ       | Cisco_FTD_SSP-FP2K_Upgrade-7.2-999.sh.REL.tar |
| Secure Firewall 3100 シリーズ | Cisco_FTD_SSP-FP3K_Upgrade-7.2-999.sh.REL.tar |
| Firepower 4100/9300       | Cisco_FTD_SSP_Upgrade-7.2-999.sh.REL.tar      |
| Threat Defense Virtual    | Cisco_FTD-7.2-999.sh.REL.tar                  |
| ISA 3000                  | Cisco_FTD-7.2-999.sh.REL.tar                  |

ステップ2 Management Center で、[システム (System) ]>[更新 (Updates) ] を選択します。

ステップ3 [更新のアップロード (Upload Update) ] をクリックします。

ヒント 一部のアップグレードパッケージは、リリースが手動でダウンロードできるようになってからしばらくすると、直接ダウンロードできるようになります。遅延の長さは、リリースの種類、リリースの選択、およびその他の要因によって異なります。Management Center がインターネットにアクセスできる場合は、代わりに [アップデートのダウンロード (Download Updates) ] をクリックして、展開の対象となるすべてのパッケージと、必要に応じて最新の VDB をダウンロードできます。

ステップ4 [アクション (Action) ] については、[ローカルソフトウェアアップデートパッケージのアップロード (Upload local software update package) ] オプションボタンをクリックします。

ステップ5 [Choose File] をクリックします。

ステップ6 パッケージを参照し、[Upload] をクリックします。

ステップ7 (オプション) 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。

復元を有効にする必要がなく、Threat Defense アップグレードウィザードを使用する予定の場合、パッケージをコピーするように求められます。復元を有効にするため、[システム (System) ]>[更新 (Updates) ] ページを使用してアップグレードする場合は、次のように、アップグレードパッケージを今すぐにデバイスにコピーすることをお勧めします。

- a) コピーするアップグレードパッケージの横にある [アップデートのプッシュまたはステージ (Push or Stage Update) ] アイコンをクリックします。
- b) 宛先デバイスを選択します。

この時点でパッケージをすべての対象デバイスにコピーするか、サブセットにコピーしてから Threat Defense CLI を使用してデバイス間でアップグレードパッケージをコピーすることができます。 [Threat Defense アップグレードパッケージのデバイス間のコピー \(64 ページ\)](#) を参照してください。

アップグレードパッケージをプッシュ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。

- c) [プッシュ (Push) ] をクリックします。

---

## Threat Defense アップグレードパッケージの内部サーバーへのアップロード

この手順を使用して、Management Center からではなく、独自の内部 Web サーバーからアップグレードパッケージを取得するように Threat Defense デバイスを設定します。これは、Management Center とそのデバイスとの間の帯域幅が制限されている場合に特に役立ちます。また、Management Center 上の容量も節約できます。

この機能を設定するには、Web サーバーのアップグレードパッケージの場所にポインタ (URL) を保存します。アップグレードプロセスでは、Management Center ではなく Web サーバーから

アップグレードパッケージが取得されます。または、アップグレードする前に、Management Center のプッシュ機能を使用してパッケージをコピーすることもできます。

各アップグレードパッケージに対して、この手順を繰り返します。アップグレードパッケージごとに、1つの場所のみを設定できます。

### 始める前に

セキュア Webサーバー (HTTPS) の場合は、サーバーのデジタル証明書 (PEM 形式) を取得します。サーバーの管理者から証明書を取得できるようにする必要があります。また、ブラウザまたは OpenSSL などのツールを使用して、サーバーの証明書の詳細を表示したり、証明書をエクスポートまたはコピーしたりすることもできます。

**ステップ 1** シスコ サポートおよびダウンロード サイト : <https://www.cisco.com/go/ftd-software>からの アップグレードパッケージをダウンロードします。

ファミリまたはシリーズのすべてのモデルに同じソフトウェアアップグレードパッケージを使用します。適切なソフトウェアを見つけるには、使用しているモデルを選択または検索し、適切なバージョンのソフトウェアのダウンロードページを参照します。使用可能なアップグレードパッケージは、インストールパッケージ、ホットフィックス、およびその他の該当するダウンロードとともに表示されます。アップグレードパッケージのファイル名には、プラットフォーム、パッケージタイプ (アップグレード、パッチ、ホットフィックス)、ソフトウェアバージョン、およびビルドが反映されています。

|                           |                                               |
|---------------------------|-----------------------------------------------|
| Firepower 1000 シリーズ       | Cisco_FTD_SSP-FP1K_Upgrade-7.2-999.sh.REL.tar |
| Firepower 2100 シリーズ       | Cisco_FTD_SSP-FP2K_Upgrade-7.2-999.sh.REL.tar |
| Secure Firewall 3100 シリーズ | Cisco_FTD_SSP-FP3K_Upgrade-7.2-999.sh.REL.tar |
| Firepower 4100/9300       | Cisco_FTD_SSP_Upgrade-7.2-999.sh.REL.tar      |
| Threat Defense Virtual    | Cisco_FTD-7.2-999.sh.REL.tar                  |
| ISA 3000                  | Cisco_FTD-7.2-999.sh.REL.tar                  |

**ステップ 2** デバイスがアクセスできる内部 Web サーバーにアップグレードパッケージをコピーします。

**ステップ 3** Management Center で、[システム (System)] > [更新 (Updates)] を選択します。

**ステップ 4** [更新のアップロード (Upload Update)] をクリックします。

何もアップロードしない場合でも、このオプションを選択します。次のページに、URL の入力を求めるプロンプトが表示されます。

**ステップ 5** アクションについては、[Upload local software update package] オプション ボタンをクリックします。

**ステップ 6** アップグレードパッケージの送信元 URL を入力します。

次の例のように、プロトコル (HTTP/HTTPS) とフルパスを提供します。

```
https://internal_web_server/upgrade_package.sh.REL.tar
```

アップグレードパッケージのファイル名には、プラットフォーム、パッケージタイプ（アップグレード、パッチ、ホットフィックス）、およびアップグレードするソフトウェアのバージョンが反映されています。正しいファイル名を入力したことを確認します。

**ステップ 7** HTTPS サーバーの場合は、**CA 証明書**を提供します。

これは、以前取得したサーバーのデジタル証明書です。テキストブロック全体（BEGIN CERTIFICATE 行と END CERTIFICATE 行を含む）をコピーして貼り付けます。

**ステップ 8** **[Save]** をクリックします。

場所が保存されます。アップロードされたアップグレードパッケージとアップグレードパッケージの URL はまとめてリストされますが、明確にラベル付けされます。

**ステップ 9** （オプション）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。

復元を有効にする必要がなく、Threat Defense アップグレードウィザードを使用する予定の場合、パッケージをコピーするように求められます。復元を有効にするため、**[システム (System)] > [更新 (Updates)]** ページを使用してアップグレードする場合は、次のように、アップグレードパッケージを今すぐにデバイスにコピーすることをお勧めします。

- a) コピーするアップグレードパッケージの横にある **[アップデートのプッシュまたはステージ (Push or Stage Update)]** アイコンをクリックします。
- b) 宛先デバイスを選択します。

この時点でパッケージをすべての対象デバイスにコピーするか、サブセットにコピーしてから Threat Defense CLI を使用してデバイス間でアップグレードパッケージをコピーすることができます。[Threat Defense アップグレードパッケージのデバイス間のコピー \(64 ページ\)](#) を参照してください。

アップグレードパッケージをプッシュ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。

- c) **[プッシュ (Push)]** をクリックします。

---

## Threat Defense アップグレードパッケージのデバイス間のコピー

Management Center や内部 Web サーバーから各デバイスにアップグレードパッケージをコピーする代わりに、Threat Defense CLI を使用してデバイス間でアップグレードパッケージをコピーできます（「ピアツーピア同期」）。この安全で信頼性の高いリソース共有は、管理ネットワークを経由しますが、Management Center には依存しません。各デバイスは、5つのパッケージの同時転送に対応できます。

この機能は、同じスタンドアロン Management Center によって管理されるバージョン 7.2 以降のスタンドアロンデバイスでサポートされています。次の場合はサポートされていません。

- コンテナインスタンス。
- デバイスの高可用性ペアとクラスタ。

バージョン 7.1 以降のグループメンバーは通常の同期プロセスの一部として、相互にパッケージを取得できます。アップグレードパッケージを1つのグループメンバーにコピーすると、自動的にすべてのグループメンバーと同期されます。

- 高可用性 Management Center によって管理されるデバイス。
- クラウド提供型の管理センターによって管理されているが、分析モードでお客様が導入した Management Center に追加されたデバイス。
- 異なるドメインのデバイス、または NAT ゲートウェイによって分離されたデバイス。
- Management Center のバージョンに関係なく、バージョン 7.1 以前からアップグレードするデバイス。

アップグレードパッケージが必要なすべてのデバイスに対して、次の手順を繰り返します。この機能に関連するすべての CLI コマンドの詳細については、[Cisco Secure Firewall Threat Defense コマンドリファレンス](#) を参照してください。

#### 始める前に

- Threat Defense アップグレードパッケージを Management Center または内部 サーバーにアップロードします。
- アップグレードパッケージを 1 つ以上のデバイスにコピーします。

---

**ステップ 1** 管理者アカウントでアップグレードパッケージが必要なデバイスに SSH 接続します。

**ステップ 2** 機能を有効にします。

**configure p2psync enable**

**ステップ 3** まだはっきりしない場合は、必要なアップグレードパッケージをどこで入手できるかを確認してください。

**show peers** : この機能も有効になっている他の適格なデバイスを一覧表示します。

**show peer details ip\_address** : 指定した IP アドレスのデバイスについて、利用可能なアップグレードパッケージとそのパスを一覧表示します。

**ステップ 4** 検出した IP アドレスとパスを指定して、必要なパッケージが存在するデバイスからパッケージをコピーします。

**sync-from-peer ip\_address package\_path**

パッケージのコピー実行を確定すると、パッケージ転送を監視するために使用できる同期ステータス UUID がシステムに表示されます。

**ステップ 5** CLI から転送ステータスをモニタリングします。

**show p2p-sync-status** : このデバイスへの過去 5 回の転送についての同期ステータスを表示します。これには、完了した転送と失敗した転送も含まれます。

`show p2p-sync-status sync_status_UUID` : このデバイスを対象とした特定の転送の同期ステータスを表示します。

## Threat Defense のアップグレード準備状況チェック

Threat Defense 準備状況チェックを手動で実行するには、次の手順を使用します。



- (注) デバイスのアップグレードが成功した後に復元を有効にする場合は、次の手順を使用して準備状況を確認します。それ以外の場合は、代わりにアップグレードウィザードを使用することをお勧めします。このウィザードでは、次のチェックを完了するように求められます。 [ウィザードを使用した Threat Defense のアップグレード \(復元を無効化\) \(67 ページ\)](#)

準備状況チェックでは、メジャーアップグレードとメンテナンスアップグレードの準備状況を評価します。準備状況チェックで不合格になると、問題を修正するまでアップグレードできません。準備状況チェックの実行に必要な時間は、モデルによって異なります。準備状況チェックを行っている間は、手動で再起動またはシャットダウンしないでください。

### 始める前に

チェックするデバイスの Management Center にアップグレードパッケージをアップロードします。または、内部 Web サーバー上の場所を指定します。

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

**ステップ 2** [利用可能なアップデート (Available Updates)] で、チェックするデバイスの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ます。

対象デバイスのリストが、アップグレード前の互換性チェックの結果とともに表示されます。アップグレードの失敗の原因となる明らかな問題がある場合、この事前チェックによってアップグレードが防止されます。

**ステップ 3** チェックするデバイスを選択し、[準備状況の確認 (Check Readiness)] をクリックします。

他の適格なデバイスを選択できない場合は、互換性チェックに合格したことを確認してください。

**ステップ 4** [準備状況の確認 (Check Readiness)] をクリックします。

メッセージセンターで準備状況チェックの進行状況をモニターできます。



### 次のタスク

[システム (System)] > [更新 (Updates)] ページで、[準備状況チェック (Readiness Checks)] をクリックすると、進行中のチェックや不合格のチェックなど、展開全体の準備状況チェックのステータスが表示されます。また、このページを使用して、不合格となった後にチェックを簡単に再実行することもできます。

## Threat Defense のアップグレード

Threat Defense をアップグレードする前に、使用する手順を決定します。

アップグレード完了後に元に戻す必要が生じる可能性がある場合は、システム (⚙️) > [更新 (Updates)] ページを使用し、Management Center で Threat Defense をアップグレードします。これは、「アップグレード成功後の復元を可能にする」オプションを設定する唯一の方法です。



---

**重要** これは、[デバイス (Devices)] > [デバイスのアップグレード (Device Upgrade)] ページでウィザードを使用する通常の推奨とは対照的です。

---

## ウィザードを使用した Threat Defense のアップグレード（復元を無効化）

Management Center には、Threat Defense をアップグレードするためのウィザードが用意されています。

ウィザードでは、アップグレードするデバイスの選択、アップグレードパッケージのデバイスへのコピー、互換性と準備状況の確認など、アップグレード前の重要な段階を順を追って説明します。続行すると、選択したデバイスに関する基本情報と、現在のアップグレード関連のステータスが表示されます。表示内容には、アップグレードできない理由が含まれます。あるデバイスがウィザードの1つの段階に「合格」しない場合、そのデバイスは次の段階には表示されません。

ウィザードから移動しても、進行状況は保持されますが、管理者アクセス権を持つ他のユーザーはワークフローをリセット、変更、または続行できます（CAC でログインした場合を除きます。この場合、進行状況はログアウトしてから 24 時間後にクリアされます）。進行状況は、高可用性 Management Center 間でも同期されます。



**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（30 ページ）](#)を参照してください。

### 始める前に

- この手順を使用するかどうかを決定します。一般的には、アップグレードウィザードを使用することをお勧めします。ただし、アップグレード完了後に復元が必要になる可能性がある場合は、代わりに **[システム (System)] > [更新 (Updates)]** ページを使用する必要があります。また、システム更新ページを使用してアップグレードパッケージをアップロードし、Management Center 自体をアップグレードする必要があります。
- 事前アップグレードのチェックリストを完了します。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。

### アップグレードするデバイスを選択します。

**ステップ 1** **[デバイス (Devices)] > [デバイス管理 (Device Management)]** の順に選択します。

**ステップ 2** アップグレードするデバイスを選択します。

複数のデバイスを同時にアップグレードできます。デバイスクラスとハイアベイラビリティペアのメンバーは、同時にアップグレードする必要があります。

**重要** パフォーマンスの問題により、デバイスをバージョン 6.6.x 以前にアップグレードする場合は（バージョン 6.6.x からのアップグレードではなく）、同時にアップグレードするデバイスは 5 つまでにすることを強くお勧めします。

**ステップ 3** **[アクションの選択 (Select Action)]** または **[一括アクションの選択 (Select Bulk Action)]** メニューから、**[Firepower ソフトウェアのアップグレード (Upgrade Firepower Software)]** を選択します。

**[デバイスアップグレード (Device Upgrade)]** ページが表示され、選択したデバイスの数が示され、ターゲットバージョンを選択するように求められます。このページには、左側の **[デバイスの選択]** と右側の **[デバイスの詳細]** の 2 つのペインがあります。**[デバイスの選択 (Device Selection)]** でデバイスリンク（「4 つのデバイス」など）をクリックして、デバイス詳細を表示します。

進行中のアップグレードワークフローがすでにある場合は、最初にデバイスをマージする（新しく選択したデバイスを以前に選択したデバイスに追加して続行する）か、リセットする（以前の選択を破棄し、新しく選択したデバイスのみを使用する）必要があることに注意してください。

**ステップ 4** デバイスの選択内容を確認します。

追加のデバイスを選択するには、[デバイス管理 (Device Management)] ページに戻ります。進行状況は失われません。デバイスを削除するには、[リセット (Reset)] をクリックしてデバイスの選択をクリアし、最初からやり直します。

アップグレードパッケージをデバイスにコピーします。

**ステップ 5** [アップグレード先 (Upgrade to)] メニューから、対象のバージョンを選択します。

システムは、選択したデバイスのどれをそのバージョンにアップグレードできるかを決定します。対象外のデバイスがある場合は、デバイスのリンクをクリックして理由を確認できます。削除したくなければ、不要なデバイスは削除する必要はありません。それらは次のステップには含まれません。

[アップグレード先 (Upgrade to)] メニューの選択肢は、システムで利用可能なデバイスアップグレードパッケージに対応していることに注意してください。対象のバージョンがリストにない場合は、[システム (System)] > [更新 (Updates)] に移動し、正しいアップグレードパッケージの場所をアップロードまたは指定します。

**ステップ 6** アップグレードパッケージがまだ必要なすべてのデバイスについて、[アップグレードパッケージのコピー] をクリックして、選択を確認します。

Threat Defense をアップグレードするには、アップグレードパッケージがアプライアンスにある必要があります。アップグレードの前にアップグレードパッケージをコピーすると、アップグレードのメンテナンス時間が短縮されます。

**ヒント** Threat Defense CLI を使用して、アップグレードパッケージをデバイス間でコピーすることもできます。資格要件などの詳細については、[Threat Defense アップグレードパッケージのデバイス間のコピー \(64 ページ\)](#) を参照してください。

互換性、準備状況、およびその他の最終チェックを実行します。

**ステップ 7** 準備状況チェックに合格する必要があるすべてのデバイスについて、[準備状況チェックの実行 (Run Readiness Check)] をクリックして、選択を確認します。

[互換性と準備状況のチェックに合格する必要がある (Require passing compatibility and readiness checks option)] オプションを無効にすることでチェックをスキップできますが、お勧めしません。すべてのチェックに合格すると、アップグレードが失敗する可能性が大幅に減少します。準備状況チェックの実行中は、デバイスに変更を展開したり、手動で再起動またはシャットダウンしたりしないでください。デバイスが準備状況チェックに失敗した場合は、問題を修正して、準備状況チェックを再度実行してください。準備状況チェックの結果、解決できない問題が見つかった場合は、アップグレードを開始しないでください。代わりに、Cisco TAC にお問い合わせください。

互換性チェックは自動的に行われることに注意してください。たとえば、Firepower 4100/9300 で FXOS をアップグレードする必要がある場合、または管理対象デバイスに展開する必要がある場合は、システムによってすぐに警告されます。

**ステップ 8** アップグレード前の最終的なチェックを実行します。

アップグレード前のチェックリストを再確認します。関連するすべてのタスク、特に最終チェックを完了していることを確認してください。

**ステップ 9** 必要に応じて、[デバイスのアップグレード (Device Upgrade)] ページに戻ります。

進行状況は保持されています。保持されていない場合は、管理者アクセス権を持つ他の誰かがワークフローをリセット、変更、または完了した可能性があります。

**ステップ 10** [Next] をクリックします。

アップグレードします。

**ステップ 11** デバイスの選択とターゲットバージョンを確認します。

**ステップ 12** （オプション）クラスタ化されたデバイスのアップグレード順序を変更します。

クラスタのデバイスの詳細を表示し、[アップグレード順序の変更（Change Upgrade Order）] をクリックします。制御ユニットは常に最後にアップグレードされます。これを変更することはできません。

**ステップ 13** アップグレードオプションを選択します。

メジャーアップグレードおよびメンテナンスアップグレードでは、次のことを行えます。

- **アップグレードの失敗時に自動的にキャンセルし、前のバージョンにロールバックする**：アップグレードに失敗すると、デバイスは自動的にアップグレード前の状態に戻ります。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場合は、このオプションを無効にします。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。
- **Snort 2 から Snort 3 にアップグレードする**：ソフトウェアのアップグレード後、設定を展開すると、対象のデバイスが Snort 2 から Snort 3 にアップグレードされます。カスタム侵入ポリシーやネットワーク分析ポリシーを使用しているためにデバイスがアップグレード対象外になる場合は、検出とパフォーマンスを向上させるために、手動で Snort 3 にアップグレードすることを強く推奨します。移行のサポートについては、お使いのバージョンの [Cisco Secure Firewall Management Center Snort 3 Configuration Guide](#) を参照してください。

これらのオプションは、パッチではサポートされていません。

**ステップ 14** [アップグレードを開始（Start Upgrade）] 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。

メッセージセンターでアップグレードの進行状況をモニタします。アップグレード中のトラフィック処理については、「[Threat Defense 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（31 ページ）](#)」のを参照してください。

アップグレード中にデバイスが 2 回再起動する場合があります。これは想定されている動作です。

成功を確認し、アップグレード後のタスクを完了します。

**ステップ 15** 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 16** （オプション）高可用性および拡張性の展開では、デバイスのロールを調べます。

アップグレードプロセスは、常にスタンバイユニットまたはデータノードをアップグレードするようにデバイスのロールを切り替えます。デバイスをアップグレード前のロールに戻すことはありません。特定のデバイスに優先するロールがある場合は、それらの変更を今すぐ行ってください。

**ステップ 17** 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 18** アップグレード後に必要な構成変更があれば、実行します。

**ステップ 19** アップグレードしたデバイスに構成を再度展開します。

### 次のタスク

(オプション) [デバイスのアップグレード (Device Upgrade)] ページに戻り、[完了 (Finish)] をクリックして、ウィザードをクリアします。これを行うまで、[デバイスのアップグレード (Device Upgrade)] ページには、実行したばかりのアップグレードに関する詳細が引き続き表示されます。

## で Threat Defense をアップグレード (復元を有効化)

この手順を使用して、Management Center の [システムアップデート (System Updates)] ページから Threat Defense をアップグレードします。



**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 \(30 ページ\)](#) を参照してください。

### 始める前に

- この手順を使用するかどうかを決定します。一般的には、アップグレードウィザードを使用することをお勧めします。ただし、アップグレード完了後に復元が必要になる可能性がある場合は、この手順を使用します。
- 事前アップグレードのチェックリストを完了します。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** Management Center で、[システム (System)] > [更新 (Updates)] を選択します。

**ステップ 2** [利用可能なアップデート (Available Updates)] で該当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。複数のデバイスで同じアップグレードパッケージを使用する場合にのみ、複数のデバイスを

同時にアップグレードできます。デバイス クラスタとハイ アベイラビリティ ペアのメンバーは、同時にアップグレードする必要があります。

**重要** [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 アップグレードオプションを選択します。

メジャーアップグレードおよびメンテナンスアップグレードでは、次のことを行えます。

- **アップグレードの失敗時に自動的にキャンセルし、前のバージョンにロールバックする** : アップグレードに失敗すると、デバイスは自動的にアップグレード前の状態に戻ります。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場合は、このオプションを無効にします。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。
- **アップグレード成功後の復元を可能にする** : アップグレードが成功してから 30 日間、デバイスをアップグレード前の状態に戻すことができます。
- **Snort 2 から Snort 3 にアップグレードする** : ソフトウェアのアップグレード後、設定を展開すると、対象のデバイスが Snort 2 から Snort 3 にアップグレードされます。カスタム侵入ポリシーやネットワーク分析ポリシーを使用しているためにデバイスがアップグレード対象外になる場合は、検出とパフォーマンスを向上させるために、手動で Snort 3 にアップグレードすることを強く推奨します。移行のサポートについては、お使いのバージョンの [Cisco Secure Firewall Management Center Snort 3 Configuration Guide](#) を参照してください。

これらのオプションは、パッチではサポートされていません。

### ステップ 4 [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。

メッセージセンターでアップグレードの進行状況をモニタします。アップグレード中のトラフィック処理については、「[Threat Defense 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 \(31 ページ\)](#)」のを参照してください。

アップグレード中にデバイスが 2 回再起動する場合があります。これは想定されている動作です。

### ステップ 5 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 (オプション) 高可用性および拡張性の展開では、デバイスのロールを調べます。

アップグレードプロセスは、常にスタンバイユニットまたはデータノードをアップグレードするようにデバイスのロールを切り替えます。デバイスをアップグレード前のロールに戻すことはありません。特定のデバイスに優先するロールがある場合は、それらの変更を今すぐ行ってください。

### ステップ 7 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 8** アップグレード後に必要な構成変更があれば、実行します。

**ステップ 9** アップグレードしたデバイスに構成を再度展開します。

---



で Threat Defense をアップグレード (復元を有効化)





## 第 6 章

# Firepower 4100/9300 の FXOS アップグレード

Firepower 4100/9300 の場合、Threat Defense 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。Threat Defense 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。

- [FXOS のアップグレードパッケージ \(75 ページ\)](#)
- [FXOS のアップグレードガイドライン \(75 ページ\)](#)
- [FXOS のアップグレードパス \(78 ページ\)](#)
- [Chassis Manager を使用した FXOS のアップグレード \(83 ページ\)](#)
- [CLI を使用した FXOS のアップグレード \(92 ページ\)](#)

## FXOS のアップグレードパッケージ

FXOS イメージはシスコ サポートおよびダウンロードサイトで入手できます。

- Firepower 4100 シリーズ : <http://www.cisco.com/go/firepower4100-software>
- Firepower 9300 : <http://www.cisco.com/go/firepower9300-software>

正しい FXOS イメージを見つけるには、デバイス モデルを選択または検索し、対象バージョンとビルドの *Firepower Extensible Operating System* のダウンロードページを参照します。FXOS イメージ (fxos-k9.version.SPA) は、リカバリおよび MIB パッケージとともにリストされます。

## FXOS のアップグレードガイドライン

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。

**Threat Defense 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 7.2 を実行するために必要な FXOS の最小バージョンは、FXOS 2.12.0.31 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 \(77 ページ\)](#) を参照してください。

**Threat Defense 高可用性/スケーラビリティを備えた FXOS のアップグレード順序**

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 つずつシャーシの FXOS をアップグレードします。Threat Defense のアップグレードの場合、グループ化されたデバイスが 1 つずつ自動的にアップグレードされます。

表 32: Threat Defense 高可用性/スケーラビリティを備えた FXOS のアップグレード順序

| 展開                       | アップグレード順序                                                                                                                                                                                                                                                                                                  |
|--------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| スタンドアロンデバイス              | <ol style="list-style-type: none"> <li>1. FXOS をアップグレードします。</li> <li>2. Threat Defense をアップグレードします。</li> </ol>                                                                                                                                                                                             |
| ハイ アベイラビリティ              | <p>FTD をアップグレードする前に、両方のシャーシで Threat Defense をアップグレードします。中断を最小限に抑えるため、スタンバイは常にアップグレードします。</p> <ol style="list-style-type: none"> <li>1. スタンバイデバイスを備えたシャーシの FXOS をアップグレードします。</li> <li>2. ロールを切り替えます。</li> <li>3. 新しいスタンバイデバイスを備えたシャーシの FXOS をアップグレードします。</li> <li>4. Threat Defense をアップグレードします。</li> </ol> |
| シャーシ内クラスタ (同じシャーシ上のユニット) | <ol style="list-style-type: none"> <li>1. FXOS をアップグレードします。</li> <li>2. Threat Defense をアップグレードします。</li> </ol>                                                                                                                                                                                             |

| 展開                       | アップグレード順序                                                                                                                                                                                                                                                                                                                  |
|--------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| シャーシ内クラスタ（異なるシャーシ上のユニット） | <p>Threat Defense をアップグレードする前に、すべてのシャーシの FXOS をアップグレードします。中断を最小限に抑えるため、すべてデータユニットのシャーシを常にアップグレードします。</p> <ol style="list-style-type: none"> <li>1. すべてのデータユニットのシャーシの FXOS をアップグレードします。</li> <li>2. 制御モジュールをアップグレードしたシャーシに切り替えます。</li> <li>3. 残りのシャーシの FXOS をアップグレードします。</li> <li>4. Threat Defense をアップグレードします。</li> </ol> |

### FTD および ASA 論理デバイスを搭載した FXOS のアップグレード

Firepower 9300 に Threat Defense および ASA 論理デバイスが設定されている場合は、この章の手順を使用して FXOS と Threat Defense をアップグレードします。FXOS をアップグレードしても、どちらのタイプの論理デバイスとの互換性も失われないことを確認する必要があります（[Threat Defense および ASA を使用した FXOS のアップグレードパス（81 ページ）](#) を参照）。

ASA のアップグレード手順については、[Cisco Secure Firewall ASA アップグレードガイド](#) を参照してください。

### 論理デバイスを搭載していない FXOS のアップグレード

論理デバイスが設定されていない場合は、この章の手順を使用して、スタンドアロン型の Threat Defense デバイスの FXOS をアップグレードします。論理デバイスに関する指示は無視してください。または、必要な FXOS バージョンへのシャーシの完全な再イメージ化を実行します。

## 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 33: 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        | —    |

| 導入                                   | トラフィックの挙動                          | メソッド                                                                    |
|--------------------------------------|------------------------------------|-------------------------------------------------------------------------|
| 高可用性                                 | 影響なし。                              | <b>ベストプラクティス</b> ：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<br>タ                        | 影響なし。                              | <b>ベストプラクティス</b> ：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<br>タ (FirePOWER<br>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。                                                      |

## FXOS のアップグレードパス

展開に一致するアップグレードパスを選択します。

### Threat Defense を使用する FXOS のアップグレードパス

次の表に、Firepower 4100/9300 の Threat Defense のアップグレードパスを示します。

現在の Threat Defense /Management Center のバージョンが対象のバージョンより後の日付にリリースされた場合、期待どおりにアップグレードできない可能性があります。このような場合、アップグレードはすぐに失敗し、2 つのバージョン間にデータストアの非互換性があることを説明するエラーが表示されます。現在のバージョンと対象のバージョンの両方に関するリリースノートには、特定の制限が掲載されています。

この表には、シスコにより特別に認定されたバージョンの組み合わせのみが掲載されています。最初に FXOS をアップグレードするため、サポートされている（ただし推奨されていない）組み合わせを短時間実行します。ここでは、FXOS が論理デバイスの「前」になります。

最小限のビルドおよびその他の詳細な互換性情報については、[Cisco Secure Firewall Threat Defense 互換性ガイド](#) を参照してください。

表 34: Firepower 4100/9300 での Threat Defense の直接アップグレード

| 現在のバージョン                             | 対象のバージョン                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|--------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Threat Defense 7.2 を搭載した FXOS 2.12   | → Threat Defense 7.2.x 以降のメンテナンスリリースを搭載した FXOS 2.12                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Threat Defense 7.1 を搭載した FXOS 2.11.1 | 次のいずれかです。<br>→ Threat Defense 7.2 を搭載した FXOS 2.12<br>→ Threat Defense 7.1.x 以降のメンテナンスリリースを搭載した FXOS 2.11.1                                                                                                                                                                                                                                                                                                                                                                               |
| Threat Defense 7.0 を搭載した FXOS 2.10.1 | 次のいずれかです。<br>→ Threat Defense 7.2 を搭載した FXOS 2.12<br>→ Threat Defense 7.1 を搭載した FXOS 2.11.1<br>→ Threat Defense 7.0.x 以降のメンテナンスリリースを搭載した FXOS 2.10.1<br><br>(注) 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。<br><br>(注) クラウド提供型の管理センターは、バージョン 7.1 を実行している脅威防御デバイス、または任意のバージョンを実行しているデバイスを管理できません。クラウド管理を登録解除して無効にしない限り、クラウド提供型の管理センターに登録されている脅威防御デバイスをバージョン 7.0.x からバージョン 7.1 にアップグレードすることはできません。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。 |

| 現在のバージョン                            | 対象のバージョン                                                                                                                                                                                                                               |
|-------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Threat Defense 6.7 を搭載した FXOS 2.9.1 | 次のいずれかです。<br>→ Threat Defense 7.2 を搭載した FXOS 2.12<br>→ Threat Defense 7.1 を搭載した FXOS 2.11.1<br>→ Threat Defense 7.0 を搭載した FXOS 2.10.1<br>→ Threat Defense 6.7.x 以降のメンテナンスリリースを搭載した FXOS 2.9.1                                          |
| Threat Defense 6.6 を搭載した FXOS 2.8.1 | 次のいずれかです。<br>→ Threat Defense 7.2 を搭載した FXOS 2.12<br>→ Threat Defense 7.1 を搭載した FXOS 2.11.1<br>→ Threat Defense 7.0 を搭載した FXOS 2.10.1<br>→ Threat Defense 6.7 を搭載した FXOS 2.9.1<br>→ Threat Defense 6.6.x 以降のメンテナンスリリースを搭載した FXOS 2.8.1 |
| Threat Defense 6.5 を搭載した FXOS 2.7.1 | 次のいずれかです。<br>→ Threat Defense 7.1 を搭載した FXOS 2.11.1<br>→ Threat Defense 7.0 を搭載した FXOS 2.10.1<br>→ Threat Defense 6.7 を搭載した FXOS 2.9.1<br>→ Threat Defense 6.6 を搭載した FXOS 2.8.1                                                        |
| Threat Defense 6.4 を搭載した FXOS 2.6.1 | 次のいずれかです。<br>→ Threat Defense 7.0 を搭載した FXOS 2.10.1<br>→ Threat Defense 6.7 を搭載した FXOS 2.9.1<br>→ Threat Defense 6.6 を搭載した FXOS 2.8.1<br>→ Threat Defense 6.5 を搭載した FXOS 2.7.1                                                         |
| Threat Defense 6.3 を搭載した FXOS 2.4.1 | 次のいずれかです。<br>→ Threat Defense 6.7 を搭載した FXOS 2.9.1<br>→ Threat Defense 6.6 を搭載した FXOS 2.8.1<br>→ Threat Defense 6.5 を搭載した FXOS 2.7.1<br>→ Threat Defense 6.4 を搭載した FXOS 2.6.1                                                          |

| 現在のバージョン                              | 対象のバージョン                                                                                                                                                                      |
|---------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Threat Defense 6.2.3 を搭載した FXOS 2.3.1 | 次のいずれかです。<br>→ Threat Defense 6.6 を搭載した FXOS 2.8.1<br>→ Threat Defense 6.5 を搭載した FXOS 2.7.1<br>→ Threat Defense 6.4 を搭載した FXOS 2.6.1<br>→ Threat Defense 6.3 を搭載した FXOS 2.4.1 |

## Threat Defense および ASA を使用した FXOS のアップグレードパス

この表では、別のモジュールで実行されている Threat Defense および ASA 論理デバイスを搭載した Firepower 9300 シャーシのアップグレードパスを示します。



- (注) このドキュメントには、ASA 論理デバイスのアップグレード手順は記載されていません。アップグレード手順については、[Cisco Secure Firewall ASA アップグレードガイド](#)を参照してください。

現在の Threat Defense /Management Center のバージョンが対象のバージョンより後の日付にリリースされた場合、期待どおりにアップグレードできない可能性があります。このような場合、アップグレードはすぐに失敗し、2つのバージョン間にデータストアの非互換性があることを説明するエラーが表示されます。現在のバージョンと対象のバージョンの両方に関するリリースノートには、特定の制限が掲載されています。

この表には、シスコにより特別に認定されたバージョンの組み合わせのみが掲載されています。最初に FXOS をアップグレードするため、サポートされている（ただし推奨されていない）組み合わせを短時間実行します。ここでは、FXOS が論理デバイスの「前」になります。最小限のビルドおよびその他の詳細な互換性情報については、[Cisco Secure Firewall Threat Defense 互換性ガイド](#)を参照してください。

このタイプの展開では、FXOS をアップグレードしても、どちらのタイプの論理デバイスとの互換性も失われないことを確認する必要があります。複数のバージョンをスキップする必要がある場合、通常は Threat Defense がリミッタになります。FXOS と ASA は通常、1 ホップでさらにアップグレードできます。ターゲットの FXOS バージョンに達したら、どのタイプの論理デバイスからでもアップグレードを開始できます。

表 35: Firepower 9300 での Threat Defense および ASA の直接アップグレード

| 現在のバージョン                                                    | 対象のバージョン                                             |
|-------------------------------------------------------------|------------------------------------------------------|
| 次を搭載した FXOS 2.11.1<br>• Threat Defense 7.1<br>• ASA 9.17(x) | → ASA 9.18(x) および Threat Defense 7.2 を搭載した FXOS 2.12 |

| 現在のバージョン                                                                                                          | 対象のバージョン                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 次を搭載した FXOS 2.10.1 <ul style="list-style-type: none"> <li>• Threat Defense 7.0</li> <li>• ASA 9.16(x)</li> </ul>  | 次のいずれかです。 <ul style="list-style-type: none"> <li>→ ASA 9.18(x) および Threat Defense 7.2 を搭載した FXOS 2.12</li> <li>→ ASA 9.17(x) および Threat Defense 7.1 を搭載した FXOS 2.11.1</li> </ul> (注) 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。<br>(注) クラウド提供型の管理センターは、バージョン 7.1 を実行している脅威防御デバイス、または任意のバージョンを実行しているデバイスを管理できません。クラウド管理を登録解除して無効にしない限り、クラウド提供型の管理センターに登録されている脅威防御デバイスをバージョン 7.0.x からバージョン 7.1 にアップグレードすることはできません。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。 |
| 次を搭載した FXOS 2.9.1 : <ul style="list-style-type: none"> <li>• Threat Defense 6.7</li> <li>• ASA 9.15(x)</li> </ul> | 次のいずれかです。 <ul style="list-style-type: none"> <li>→ ASA 9.18(x) および Threat Defense 7.2 を搭載した FXOS 2.12</li> <li>→ ASA 9.17(x) および Threat Defense 7.1 を搭載した FXOS 2.11.1</li> <li>→ ASA 9.16(x) および Threat Defense 7.0 を搭載した FXOS 2.10.1</li> </ul>                                                                                                                                                                                                                                                          |
| 次を搭載した FXOS 2.8.1 : <ul style="list-style-type: none"> <li>• Threat Defense 6.6</li> <li>• ASA 9.14(x)</li> </ul> | 次のいずれかです。 <ul style="list-style-type: none"> <li>→ ASA 9.18(x) および Threat Defense 7.2 を搭載した FXOS 2.12</li> <li>→ ASA 9.17(x) および Threat Defense 7.1 を搭載した FXOS 2.11.1</li> <li>→ ASA 9.16(x) および Threat Defense 7.0 を搭載した FXOS 2.10.1</li> <li>→ ASA 9.15(x) および Threat Defense 6.7 を搭載した FXOS 2.9.1</li> </ul>                                                                                                                                                                                           |



| 現在のバージョン                                                                                                          | 対象のバージョン                                                                                                                                                                                                                                                                                                         |
|-------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 次を搭載した FXOS 2.7.1 : <ul style="list-style-type: none"> <li>• Threat Defense 6.5</li> <li>• ASA 9.13(x)</li> </ul> | 次のいずれかです。 <ul style="list-style-type: none"> <li>→ ASA 9.17(x) および Threat Defense 7.1 を搭載した FXOS 2.11.1</li> <li>→ ASA 9.16(x) および Threat Defense 7.0 を搭載した FXOS 2.10.1</li> <li>→ ASA 9.15(x) および Threat Defense 6.7 を搭載した FXOS 2.9.1</li> <li>→ ASA 9.14(x) および Threat Defense 6.6 を搭載した FXOS 2.8.1</li> </ul> |
| 次を搭載した FXOS 2.6.1 : <ul style="list-style-type: none"> <li>• Threat Defense 6.4</li> <li>• ASA 9.12(x)</li> </ul> | 次のいずれかです。 <ul style="list-style-type: none"> <li>→ ASA 9.16(x) および Threat Defense 7.0 を搭載した FXOS 2.10.1</li> <li>→ ASA 9.15(x) および Threat Defense 6.7 を搭載した FXOS 2.9.1</li> <li>→ ASA 9.14(x) および Threat Defense 6.6 を搭載した FXOS 2.8.1</li> <li>→ ASA 9.13(x) および Threat Defense 6.5 を搭載した FXOS 2.7.1</li> </ul>  |

## Chassis Manager を使用した FXOS のアップグレード

### Firepower Chassis Manager を使用したスタンドアロン FTD 論理デバイスまたは FTD シャーシ内クラスタ用の FXOS のアップグレード

このセクションでは、スタンドアロン Firepower 4100/9300 シャーシの FXOS プラットフォームバンドルをアップグレードする方法を説明します。

このセクションでは、次のタイプのデバイスのアップグレードプロセスについて説明します。

- FTD 論理デバイスで構成されており、フェールオーバーペアまたはシャーシ間クラスタの一部ではない Firepower 4100 シリーズ シャーシ。
- フェールオーバーペアまたはシャーシ間クラスタの一部ではない 1 つまたは複数のスタンドアロン FTD 論理デバイスで構成されている Firepower 9300 シャーシ。
- シャーシ内クラスタ内の FTD 論理デバイスで構成されている Firepower 9300 シャーシ。

## 始める前に

アップグレードを開始する前に、以下が完了していることを確認します。

- アップグレード先の FXOS プラットフォーム バンドル ソフトウェア パッケージをダウンロードします。
- FXOS と FTD の構成をバックアップします。

- 
- ステップ 1** Firepower Chassis Manager で、[システム (System)] > [更新 (Updates)] を選択します。  
[使用可能な更新 (Available Updates)] ページに、シャーシで使用可能な FXOS プラットフォームバンドルのイメージやアプリケーションのイメージのリストが表示されます。
- ステップ 2** 新しいプラットフォーム バンドル イメージをアップロードします。
- a) [イメージのアップロード (Upload Image)] をクリックして、[イメージのアップロード (Upload Image)] ダイアログ ボックスを開きます。
  - b) [ファイルを選択 (Choose File)] をクリックして対象のファイルに移動し、アップロードするイメージを選択します。
  - c) [Upload] をクリックします。  
選択したイメージが Firepower 4100/9300 シャーシにアップロードされます。
  - d) 特定のソフトウェアイメージについては、イメージをアップロードした後にエンドユーザライセンス契約書が表示されます。システムのプロンプトに従ってエンドユーザ契約書に同意します。
- ステップ 3** 新しいプラットフォーム バンドル イメージが正常にアップロードされたら、アップグレードする FXOS プラットフォーム バンドルの [アップグレード (Upgrade)] をクリックします。
- システムは、まずインストールするソフトウェア パッケージを確認します。そして現在インストールされているアプリケーションと指定した FXOS プラットフォーム ソフトウェア パッケージの間の非互換性を通知します。また既存のセッションを終了することやアップグレードの一部としてシステムをリポートする必要があることが警告されます。
- ステップ 4** インストールの続行を確定するには [はい (Yes)] を、インストールをキャンセルするには [いいえ (No)] をクリックします。
- システムがバンドルを解凍し、コンポーネントをアップグレードまたはリロードします。
- ステップ 5** Firepower Chassis Manager は、アップグレード中は使用できません。FXOS CLI を使用してアップグレードプロセスをモニターできます。
- a) **scope system** を入力します。
  - b) **show firmware monitor** を入力します。
  - c) すべてのコンポーネント (FPRM、ファブリック インターコネクト、およびシャーシ) で「Upgrade-Status: Ready」と表示されるのを待ちます。
- (注) FPRM コンポーネントをアップグレードすると、システムが再起動し、その他のコンポーネントのアップグレードを続行します。

例 :

```
FP9300-A# scope system
FP9300-A /system # show firmware monitor
FPRM:
 Package-Vers: 2.3(1.58)
 Upgrade-Status: Ready

Fabric Interconnect A:
 Package-Vers: 2.3(1.58)
 Upgrade-Status: Ready

Chassis 1:
 Server 1:
 Package-Vers: 2.3(1.58)
 Upgrade-Status: Ready
 Server 2:
 Package-Vers: 2.3(1.58)
 Upgrade-Status: Ready
```

- ステップ 6** すべてのコンポーネントが正常にアップグレードされたら、次のコマンドを入力して、セキュリティモジュール/セキュリティエンジンおよびインストールされているアプリケーションの状態を確認します。
- top** を入力します。
  - scope ssa** を入力します。
  - show slot** を入力します。
  - Firepower 4100 シリーズ アプライアンスのセキュリティエンジン、または Firepower 9300 appliance のインストールされている任意のセキュリティモジュールについて、管理状態が「Ok」、操作の状態が「Online」であることを確認します。
  - show app-instance** を入力します。
  - シャーシにインストールされているすべての論理デバイスについて、操作の状態が「Online」であることを確認します。

## Firepower Chassis Manager を使用した FTD シャーシ間クラスタの FXOS のアップグレード

シャーシ間クラスタとして構成されている FTD 論理デバイスを備えた FirePOWER 9300 または FirePOWER 4100 シリーズのセキュリティアプライアンスがある場合、次の手順を使用して FirePOWER 9300 または FirePOWER 4100 シリーズのセキュリティアプライアンスの FXOS プラットフォームバンドルを更新します。

### 始める前に

アップグレードを開始する前に、以下が完了していることを確認します。

- アップグレード先の FXOS プラットフォームバンドルソフトウェアパッケージをダウンロードします。
- FXOS と FTD の構成をバックアップします。

- ステップ 1** 次のコマンドを入力して、セキュリティ モジュール/セキュリティ エンジンおよびインストールされているアプリケーションの状態を確認します。
- シャーシ #2 の FXOS CLI に接続します（これは制御ユニットを持たないシャーシである必要があります）。
  - top** を入力します。
  - scope ssa** を入力します。
  - show slot** を入力します。
  - Firepower 4100 シリーズ アプライアンスのセキュリティ エンジン、または Firepower 9300 appliance のインストールされている任意のセキュリティ モジュールについて、管理状態が「Ok」、操作の状態が「Online」であることを確認します。
  - show app-instance** を入力します。
  - シャーシにインストールされているすべての論理デバイスについて、操作の状態が「Online」、クラスタの状態が「In Cluster」であることを確認します。また、稼働バージョンとして表示されている FTD ソフトウェアのバージョンが正しいことを確認します。
- 重要** 制御ユニットがこのシャーシ上にないことを確認します。「Master」に設定されているクラスタのロールを持つ Firepower Threat Defense インスタンスがあってはけません。
- Firepower 9300 appliance にインストールされているすべてのセキュリティ モジュール、または Firepower 4100 シリーズ アプライアンス上のセキュリティ エンジンについて、FXOS バージョンが正しいことを確認してください。
- scope server 1/slot\_id** で、Firepower 4100 シリーズ セキュリティ エンジンの場合、*slot\_id* は 1 です。
- show version** を使用して無効にすることができます。
- ステップ 2** シャーシ #2 の Firepower Chassis Manager に接続します（これは制御ユニットを持たないシャーシである必要があります）。
- ステップ 3** Firepower Chassis Manager で、[システム (System)] > [更新 (Updates)] を選択します。  
[使用可能な更新 (Available Updates)] ページに、シャーシで使用可能な FXOS プラットフォームバンドルのイメージやアプリケーションのイメージのリストが表示されます。
- ステップ 4** 新しいプラットフォーム バンドル イメージをアップロードします。
- [イメージのアップロード (Upload Image)] をクリックして、[イメージのアップロード (Upload Image)] ダイアログ ボックスを開きます。
  - [ファイルを選択 (Choose File)] をクリックして対象のファイルに移動し、アップロードするイメージを選択します。
  - [Upload] をクリックします。  
選択したイメージが Firepower 4100/9300 シャーシにアップロードされます。
  - 特定のソフトウェア イメージについては、イメージをアップロードした後にエンドユーザ ライセンス契約書が表示されます。システムのプロンプトに従ってエンドユーザ契約書に同意します。
- ステップ 5** 新しいプラットフォーム バンドル イメージが正常にアップロードされたら、アップグレードする FXOS プラットフォーム バンドルの [アップグレード (Upgrade)] をクリックします。

システムは、まずインストールするソフトウェア パッケージを確認します。そして現在インストールされているアプリケーションと指定した FXOS プラットフォーム ソフトウェア パッケージの間の非互換性を通知します。また既存のセッションを終了することやアップグレードの一部としてシステムをリブートする必要があることが警告されます。

**ステップ 6** インストールの続行を確定するには[はい (Yes) ]を、インストールをキャンセルするには[いいえ (No) ]をクリックします。

システムがバンドルを解凍し、コンポーネントをアップグレードまたはリロードします。

**ステップ 7** Firepower Chassis Manager は、アップグレード中は使用できません。FXOS CLI を使用してアップグレードプロセスをモニターできます。

- a) **scope system** を入力します。
- b) **show firmware monitor** を入力します。
- c) すべてのコンポーネント (FPRM、ファブリック インターコネクト、およびシャーシ) で「Upgrade-Status: Ready」と表示されるのを待ちます。  
(注) FPRM コンポーネントをアップグレードすると、システムが再起動し、その他のコンポーネントのアップグレードを続行します。
- d) **top** を入力します。
- e) **scope ssa** を入力します。
- f) **show slot** を入力します。
- g) Firepower 4100 シリーズ アプライアンスのセキュリティ エンジン、または Firepower 9300 appliance のインストールされている任意のセキュリティ モジュールについて、管理状態が「Ok」、操作の状態が「Online」であることを確認します。
- h) **show app-instance** を入力します。
- i) シャーシにインストールされているすべての論理デバイスについて、操作の状態が「Online」、クラスタの状態が「In Cluster」、クラスタのロールが「Slave」であることを確認します。

例 :

```
FP9300-A# scope system
FP9300-A /system # show firmware monitor
FPRM:
 Package-Vers: 2.3(1.58)
 Upgrade-Status: Ready

Fabric Interconnect A:
 Package-Vers: 2.3(1.58)
 Upgrade-Status: Ready

Chassis 1:
 Server 1:
 Package-Vers: 2.3(1.58)
 Upgrade-Status: Ready
 Server 2:
 Package-Vers: 2.3(1.58)
 Upgrade-Status: Ready

FP9300-A /system #
FP9300-A /system # top
FP9300-A# scope ssa
FP9300-A /ssa # show slot
```

```

Slot:
 Slot ID Log Level Admin State Oper State

 1 Info Ok Online
 2 Info Ok Online
 3 Info Ok Not Available
FP9300-A /ssa #

FP9300-A /ssa # show app-instance
App Name Slot ID Admin State Oper State Running Version Startup Version Profile Name
Cluster State Cluster Role

ftd 1 Enabled Online 6.2.2.81 6.2.2.81
In Cluster Slave
ftd 2 Enabled Online 6.2.2.81 6.2.2.81
In Cluster Slave
ftd 3 Disabled Not Available 6.2.2.81
Not Applicable None
FP9300-A /ssa #

```

- ステップ 8** シャーシ #2 のセキュリティモジュールの 1 つを制御用として設定します。
- シャーシ #2 のセキュリティモジュールの 1 つを制御用として設定すると、シャーシ #1 には制御ユニットが含まれなくなり、すぐにアップグレードすることができます。
- ステップ 9** クラスタ内の他のすべてのシャーシに対して手順 1 ~ 7 を繰り返します。
- ステップ 10** 制御ロールをシャーシ #1 に戻すには、シャーシ #1 のセキュリティモジュールの 1 つを制御用として設定します。

## Firepower Chassis Manager を使用した FTD ハイアベイラビリティペアの FXOS のアップグレード

ハイアベイラビリティペアとして構成されている FTD 論理デバイスを備えた FirePOWER 9300 または FirePOWER 4100 シリーズのセキュリティアプライアンスがある場合、次の手順を使用して FirePOWER 9300 または FirePOWER 4100 シリーズのセキュリティアプライアンスの FXOS プラットフォームバンドルを更新します。

### 始める前に

アップグレードを開始する前に、以下が完了していることを確認します。

- アップグレード先の FXOS プラットフォーム バンドル ソフトウェア パッケージをダウンロードします。
- FXOS と FTD の構成をバックアップします。

- ステップ 1** スタンバイの Firepower Threat Defense 論理デバイスを含む Firepower セキュリティアプライアンス上の Firepower Chassis Manager に接続します。

- ステップ 2** Firepower Chassis Manager で、[システム (System)] > [更新 (Updates)] を選択します。  
[使用可能な更新 (Available Updates)] ページに、シャーシで使用可能な FXOS プラットフォームバンドルのイメージやアプリケーションのイメージのリストが表示されます。
- ステップ 3** 新しいプラットフォーム バンドル イメージをアップロードします。
- [イメージのアップロード (Upload Image)] をクリックして、[イメージのアップロード (Upload Image)] ダイアログ ボックスを開きます。
  - [ファイルを選択 (Choose File)] をクリックして対象のファイルに移動し、アップロードするイメージを選択します。
  - [Upload] をクリックします。  
選択したイメージが Firepower 4100/9300 シャーシにアップロードされます。
  - 特定のソフトウェア イメージについては、イメージをアップロードした後にエンドユーザライセンス契約書が表示されます。システムのプロンプトに従ってエンドユーザ契約書に同意します。
- ステップ 4** 新しいプラットフォーム バンドル イメージが正常にアップロードされたら、アップグレードする FXOS プラットフォーム バンドルの [アップグレード (Upgrade)] をクリックします。
- システムは、まずインストールするソフトウェア パッケージを確認します。そして現在インストールされているアプリケーションと指定した FXOS プラットフォーム ソフトウェア パッケージの間の非互換性を通知します。また既存のセッションを終了することやアップグレードの一部としてシステムをリブートする必要があることが警告されます。
- ステップ 5** インストールの続行を確定するには[はい (Yes)] を、インストールをキャンセルするには[いいえ (No)] をクリックします。
- システムがバンドルを解凍し、コンポーネントをアップグレードまたはリロードします。
- ステップ 6** Firepower Chassis Manager は、アップグレード中は使用できません。FXOS CLI を使用してアップグレードプロセスをモニターできます。
- scope system** を入力します。
  - show firmware monitor** を入力します。
  - すべてのコンポーネント (FPRM、ファブリック インターコネクト、およびシャーシ) で「Upgrade-Status: Ready」と表示されるのを待ちます。
- (注) FPRM コンポーネントをアップグレードすると、システムが再起動し、その他のコンポーネントのアップグレードを続行します。

**例 :**

```

FP9300-A# scope system
FP9300-A /system # show firmware monitor
FPRM:
 Package-Vers: 2.3(1.58)
 Upgrade-Status: Ready

Fabric Interconnect A:
 Package-Vers: 2.3(1.58)
 Upgrade-Status: Ready

Chassis 1:
 Server 1:
 Package-Vers: 2.3(1.58)

```

```
Upgrade-Status: Ready
Server 2:
Package-Vers: 2.3 (1.58)
Upgrade-Status: Ready
```

- ステップ 7** すべてのコンポーネントが正常にアップグレードされたら、次のコマンドを入力して、セキュリティ モジュール/セキュリティ エンジンおよびインストールされているアプリケーションの状態を確認します。
- top** を入力します。
  - scope ssa** を入力します。
  - show slot** を入力します。
  - Firepower 4100 シリーズ アプライアンスのセキュリティ エンジン、または Firepower 9300 appliance のインストールされている任意のセキュリティ モジュールについて、管理状態が「Ok」、操作の状態が「Online」であることを確認します。
  - show app-instance** を入力します。
  - シャーシにインストールされているすべての論理デバイスについて、操作の状態が「Online」であることを確認します。
- ステップ 8** アップグレードしたユニットをアクティブユニットにして、アップグレード済みのユニットにトラフィックが流れるようにします。
- Firepower Management Center に接続します。
  - [**デバイス (Devices)**] > [**デバイス管理 (Device Management)**] を選択します。
  - アクティブ ピアを変更するハイアベイラビリティペアの横にあるアクティブピア切り替えアイコン (🔄) をクリックします。
  - ハイアベイラビリティペアでスタンバイデバイスをアクティブデバイスにすぐに切り替える場合は、[はい (Yes)] をクリックします。
- ステップ 9** 新しいスタンバイの Firepower Threat Defense 論理デバイスを含む Firepower セキュリティアプライアンス上の Firepower Chassis Manager に接続します。
- ステップ 10** Firepower Chassis Manager で、[**システム (System)**] > [**更新 (Updates)**] を選択します。[使用可能な更新 (Available Updates)] ページに、シャーシで使用可能な FXOS プラットフォームバンドルのイメージやアプリケーションのイメージのリストが表示されます。
- ステップ 11** 新しいプラットフォームバンドルイメージをアップロードします。
- [**イメージのアップロード (Upload Image)**] をクリックして、[**イメージのアップロード (Upload Image)**] ダイアログボックスを開きます。
  - [**ファイルを選択 (Choose File)**] をクリックして対象のファイルに移動し、アップロードするイメージを選択します。
  - [**Upload**] をクリックします。  
選択したイメージが Firepower 4100/9300 シャーシにアップロードされます。
  - 特定のソフトウェアイメージについては、イメージをアップロードした後にエンドユーザーライセンス契約書が表示されます。システムのプロンプトに従ってエンドユーザー契約書に同意します。
- ステップ 12** 新しいプラットフォームバンドルイメージが正常にアップロードされたら、アップグレードする FXOS プラットフォームバンドルの [**アップグレード (Upgrade)**] をクリックします。



システムは、まずインストールするソフトウェア パッケージを確認します。そして現在インストールされているアプリケーションと指定した FXOS プラットフォーム ソフトウェア パッケージの間の非互換性を通知します。また既存のセッションを終了することやアップグレードの一部としてシステムをリブートする必要があることが警告されます。

**ステップ 13** インストールの続行を確定するには[はい (Yes) ]を、インストールをキャンセルするには[いいえ (No) ]をクリックします。

システムがバンドルを解凍し、コンポーネントをアップグレードまたはリロードします。アップグレードプロセスは、完了までに最大 30 分かかることがあります。

**ステップ 14** Firepower Chassis Manager は、アップグレード中は使用できません。FXOS CLI を使用してアップグレードプロセスをモニターできます。

- a) **scope system** を入力します。
- b) **show firmware monitor** を入力します。
- c) すべてのコンポーネント (FPRM、ファブリック インターコネクト、およびシャーシ) で「Upgrade-Status: Ready」と表示されるのを待ちます。

(注) FPRM コンポーネントをアップグレードすると、システムが再起動し、その他のコンポーネントのアップグレードを続行します。

例 :

```
FP9300-A# scope system
FP9300-A /system # show firmware monitor
FPRM:
 Package-Vers: 2.3(1.58)
 Upgrade-Status: Ready

Fabric Interconnect A:
 Package-Vers: 2.3(1.58)
 Upgrade-Status: Ready

Chassis 1:
 Server 1:
 Package-Vers: 2.3(1.58)
 Upgrade-Status: Ready
 Server 2:
 Package-Vers: 2.3(1.58)
 Upgrade-Status: Ready
```

**ステップ 15** すべてのコンポーネントが正常にアップグレードされたら、次のコマンドを入力して、セキュリティ モジュール/セキュリティ エンジンおよびインストールされているアプリケーションの状態を確認します。

- a) **top** を入力します。
- b) **scope ssa** を入力します。
- c) **show slot** を入力します。
- d) Firepower 4100 シリーズ アプライアンスのセキュリティ エンジン、または Firepower 9300 appliance のインストールされている任意のセキュリティ モジュールについて、管理状態が「Ok」、操作の状態が「Online」であることを確認します。
- e) **show app-instance** を入力します。

- f) シャーシにインストールされているすべての論理デバイスについて、操作の状態が「Online」であることを確認します。

**ステップ 16** アップグレードしたユニットを、アップグレード前のようにアクティブ ユニットにします。

- a) Firepower Management Center に接続します。
- b) [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択します。
- c) アクティブ ピアを変更するハイ アベイラビリティ ペアの横にあるアクティブ ピア切り替えアイコン (🔄) をクリックします。
- d) ハイ アベイラビリティ ペアでスタンバイ デバイスをアクティブ デバイスにすぐに切り替える場合は、[はい (Yes)] をクリックします。

## CLI を使用した FXOS のアップグレード

### FXOS CLI を使用したスタンドアロン FTD 論理デバイスまたは FTD シャーシ内クラスタ用の FXOS のアップグレード

このセクションでは、スタンドアロン Firepower 4100/9300 シャーシの FXOS プラットフォームバンドルをアップグレードする方法を説明します。

このセクションでは、次のタイプのデバイスの FXOS のアップグレードプロセスについて説明します。

- FTD 論理デバイスで構成されており、フェールオーバーペアまたはシャーシ間クラスタの一部ではない Firepower 4100 シリーズ シャーシ。
- フェールオーバーペアまたはシャーシ間クラスタの一部ではない 1 つまたは複数のスタンドアロン FTD デバイスで構成されている Firepower 9300 シャーシ。
- シャーシ内クラスタ内の FTD 論理デバイスで構成されている Firepower 9300 シャーシ。

#### 始める前に

アップグレードを開始する前に、以下が完了していることを確認します。

- アップグレード先の FXOS プラットフォーム バンドル ソフトウェア パッケージをダウンロードします。
- FXOS と FTD の構成をバックアップします。
- Firepower 4100/9300 シャーシにソフトウェアイメージをダウンロードするために必要な次の情報を収集します。
  - イメージのコピー元のサーバーの IP アドレスおよび認証クレデンシャル。
  - イメージ ファイルの完全修飾名。

**ステップ 1** FXOS CLI に接続します。

**ステップ 2** 新しいプラットフォーム バンドル イメージを Firepower 4100/9300 シャーシにダウンロードします。

a) ファームウェア モードに入ります。

```
Firepower-chassis-a # scope firmware
```

b) FXOS プラットフォーム バンドル ソフトウェア イメージをダウンロードします。

```
Firepower-chassis-a /firmware # download image URL
```

次のいずれかの構文を使用してインポートされるファイルの URL を指定します。

- `ftp://username@hostname/path/image_name`
- `scp://username@hostname/path/image_name`
- `sftp://username@hostname/path/image_name`
- `tftp://hostname:port-num/path/image_name`

c) ダウンロード プロセスをモニタする場合 :

```
Firepower-chassis-a /firmware # scope download-task image_name
```

```
Firepower-chassis-a /firmware/download-task # show detail
```

例 :

次の例では、SCP プロトコルを使用してイメージをコピーします。

```
Firepower-chassis-a # scope firmware
Firepower-chassis-a /firmware # download image scp://user@192.168.1.1/images/fxos-k9.2.3.1.58.SPA
Firepower-chassis-a /firmware # scope download-task fxos-k9.2.3.1.58.SPA
Firepower-chassis-a /firmware/download-task # show detail
Download task:
 File Name: fxos-k9.2.3.1.58.SPA
 Protocol: scp
 Server: 192.168.1.1
 Userid:
 Path:
 Downloaded Image Size (KB): 853688
 State: Downloading
 Current Task: downloading image fxos-k9.2.3.1.58.SPA from
192.168.1.1 (FSM-STAGE:sam:dme:FirmwareDownloaderDownload:Local)
```

**ステップ 3** 必要に応じて、ファームウェア モードに戻ります。

```
Firepower-chassis-a /firmware/download-task # up
```

**ステップ 4** auto-install モードにします。

```
Firepower-chassis-a /firmware # scope auto-install
```

**ステップ 5** FXOS プラットフォーム バンドルをインストールします。

```
Firepower-chassis-a /firmware/auto-install # install platform platform-vers version_number
```

`version_number` は、インストールする FXOS プラットフォームバンドルのバージョン番号です（たとえば、2.3(1.58)）。

**ステップ 6** システムは、まずインストールするソフトウェアパッケージを確認します。そして現在インストールされているアプリケーションと指定した FXOS プラットフォームソフトウェアパッケージの間の非互換性を通知します。また既存のセッションを終了することやアップグレードの一部としてシステムをリブートする必要があることが警告されます。

**yes** を入力して、検証に進むことを確認します。

**ステップ 7** インストールの続行を確定するには **yes** を、インストールをキャンセルするには **no** を入力します。

システムがバンドルを解凍し、コンポーネントをアップグレードまたはリロードします。

**ステップ 8** アップグレードプロセスをモニタするには、次の手順を実行します。

- a) **scope system** を入力します。
- b) **show firmware monitor** を入力します。
- c) すべてのコンポーネント（FPRM、ファブリック インターコネクト、およびシャーシ）で「Upgrade-Status: Ready」と表示されるのを待ちます。

(注) FPRM コンポーネントをアップグレードすると、システムが再起動し、その他のコンポーネントのアップグレードを続行します。

例：

```
FP9300-A# scope system
FP9300-A /system # show firmware monitor
FPRM:
 Package-Vers: 2.3(1.58)
 Upgrade-Status: Ready

Fabric Interconnect A:
 Package-Vers: 2.3(1.58)
 Upgrade-Status: Ready

Chassis 1:
 Server 1:
 Package-Vers: 2.3(1.58)
 Upgrade-Status: Ready
 Server 2:
 Package-Vers: 2.3(1.58)
 Upgrade-Status: Ready

FP9300-A /system #
```

**ステップ 9** すべてのコンポーネントが正常にアップグレードされたら、次のコマンドを入力して、セキュリティ モジュール/セキュリティ エンジンおよびインストールされているアプリケーションの状態を確認します。

- a) **top** を入力します。
- b) **scope ssa** を入力します。
- c) **show slot** を入力します。

- d) Firepower 4100 シリーズ アプライアンスのセキュリティ エンジン、または Firepower 9300 appliance のインストールされている任意のセキュリティ モジュールについて、管理状態が「Ok」、操作の状態が「Online」であることを確認します。
- e) **show app-instance** を入力します。
- f) シャーシにインストールされているすべての論理デバイスについて、操作の状態が「Online」であることを確認します。

---

## FXOS CLI を使用した FTD シャーシ間クラスタの FXOS のアップグレード

シャーシ間クラスタとして構成されている FTD 論理デバイスを備えた FirePOWER 9300 または FirePOWER 4100 シリーズのセキュリティアプライアンスがある場合、次の手順を使用して FirePOWER 9300 または FirePOWER 4100 シリーズのセキュリティアプライアンスの FXOS プラットフォームバンドルを更新します。

### 始める前に

アップグレードを開始する前に、以下が完了していることを確認します。

- アップグレード先の FXOS プラットフォーム バンドル ソフトウェア パッケージをダウンロードします。
- FXOS と FTD の構成をバックアップします。
- Firepower 4100/9300 シャーシにソフトウェアイメージをダウンロードするために必要な次の情報を収集します。
  - イメージのコピー元のサーバーの IP アドレスおよび認証クレデンシャル。
  - イメージファイルの完全修飾名。

- 
- ステップ 1** シャーシ #2 の FXOS CLI に接続します（これは制御ユニットを持たないシャーシである必要があります）。
- ステップ 2** 次のコマンドを入力して、セキュリティ モジュール/セキュリティ エンジンおよびインストールされているアプリケーションの状態を確認します。
- a) **top** を入力します。
  - b) **scope ssa** を入力します。
  - c) **show slot** を入力します。
  - d) Firepower 4100 シリーズ アプライアンスのセキュリティ エンジン、または Firepower 9300 appliance のインストールされている任意のセキュリティ モジュールについて、管理状態が「Ok」、操作の状態が「Online」であることを確認します。
  - e) **show app-instance** を入力します。

- f) シャーシにインストールされているすべての論理デバイスについて、操作の状態が「Online」、クラスタの状態が「In Cluster」であることを確認します。また、稼働バージョンとして表示されている FTD ソフトウェアのバージョンが正しいことを確認します。

**重要** 制御ユニットがこのシャーシ上にないことを確認します。「Master」に設定されているクラスタのロールを持つ Firepower Threat Defense インスタンスがあってはけません。

- g) Firepower 9300 appliance にインストールされているすべてのセキュリティ モジュール、または Firepower 4100 シリーズ アプライアンス上のセキュリティ エンジンについて、FXOS バージョンが正しいことを確認してください。

**scope server 1/slot\_id** で、Firepower 4100 シリーズ セキュリティ エンジンの場合、*slot\_id* は 1 です。

**show version** を使用して無効にすることができます。

**ステップ 3** 新しいプラットフォーム バンドル イメージを Firepower 4100/9300 シャーシにダウンロードします。

- a) **top** を入力します。  
b) ファームウェア モードに入ります。

Firepower-chassis-a # **scope firmware**

- c) FXOS プラットフォーム バンドル ソフトウェア イメージをダウンロードします。

Firepower-chassis-a /firmware # **download image URL**

次のいずれかの構文を使用してインポートされるファイルの URL を指定します。

- **ftp://username@hostname/path/image\_name**
- **scp://username@hostname/path/image\_name**
- **sftp://username@hostname/path/image\_name**
- **tftp://hostname:port-num/path/image\_name**

- d) ダウンロード プロセスをモニタする場合 :

Firepower-chassis-a /firmware # **scope download-task image\_name**

Firepower-chassis-a /firmware/download-task # **show detail**

例 :

次の例では、SCP プロトコルを使用してイメージをコピーします。

```
Firepower-chassis-a # scope firmware
Firepower-chassis-a /firmware # download image scp://user@192.168.1.1/images/fxos-k9.2.3.1.58.SPA
Firepower-chassis-a /firmware # scope download-task fxos-k9.2.3.1.58.SPA
Firepower-chassis-a /firmware/download-task # show detail
Download task:
 File Name: fxos-k9.2.3.1.58.SPA
 Protocol: scp
 Server: 192.168.1.1
 Userid:
 Path:
 Downloaded Image Size (KB): 853688
 State: Downloading
 Current Task: downloading image fxos-k9.2.3.1.58.SPA from
```

```
192.168.1.1 (FSM-STAGE:sam:dme:FirmwareDownloaderDownload:Local)
```

**ステップ 4** 必要に応じて、ファームウェア モードに戻ります。

```
Firepower-chassis-a /firmware/download-task # up
```

**ステップ 5** auto-install モードにします。

```
Firepower-chassis /firmware # scope auto-install
```

**ステップ 6** FXOS プラットフォーム バンドルをインストールします。

```
Firepower-chassis /firmware/auto-install # install platform platform-vers version_number
```

*version\_number* は、インストールする FXOS プラットフォーム バンドルのバージョン番号です（たとえば、2.3(1.58)）。

**ステップ 7** システムは、まずインストールするソフトウェア パッケージを確認します。そして現在インストールされているアプリケーションと指定した FXOS プラットフォーム ソフトウェア パッケージの間の非互換性を通知します。また既存のセッションを終了することやアップグレードの一部としてシステムをリブートする必要があることが警告されます。

**yes** を入力して、検証に進むことを確認します。

**ステップ 8** インストールの続行を確定するには **yes** を、インストールをキャンセルするには **no** を入力します。

システムがバンドルを解凍し、コンポーネントをアップグレードまたはリロードします。

**ステップ 9** アップグレードプロセスをモニタするには、次の手順を実行します。

a) **scope system** を入力します。

b) **show firmware monitor** を入力します。

c) すべてのコンポーネント（FPRM、ファブリック インターコネクト、およびシャーシ）で「Upgrade-Status: Ready」と表示されるのを待ちます。

（注） FPRM コンポーネントをアップグレードすると、システムが再起動し、その他のコンポーネントのアップグレードを続行します。

d) **top** を入力します。

e) **scope ssa** を入力します。

f) **show slot** を入力します。

g) Firepower 4100 シリーズ アプライアンスのセキュリティ エンジン、または Firepower 9300 appliance のインストールされている任意のセキュリティ モジュールについて、管理状態が「Ok」、操作の状態が「Online」であることを確認します。

h) **show app-instance** を入力します。

i) シャーシにインストールされているすべての論理デバイスについて、操作の状態が「Online」、クラスタの状態が「In Cluster」、クラスタのロールが「Slave」であることを確認します。

例：

```
FP9300-A# scope system
FP9300-A /system # show firmware monitor
FPRM:
```

## FXOS CLI を使用した FTD ハイアベイラビリティペアの FXOS のアップグレード

```

Package-Vers: 2.3(1.58)
Upgrade-Status: Ready

Fabric Interconnect A:
Package-Vers: 2.3(1.58)
Upgrade-Status: Ready

Chassis 1:
Server 1:
Package-Vers: 2.3(1.58)
Upgrade-Status: Ready
Server 2:
Package-Vers: 2.3(1.58)
Upgrade-Status: Ready

FP9300-A /system #
FP9300-A /system # top
FP9300-A# scope ssa
FP9300-A /ssa # show slot

Slot:
Slot ID Log Level Admin State Oper State

1 Info Ok Online
2 Info Ok Online
3 Info Ok Not Available
FP9300-A /ssa #

FP9300-A /ssa # show app-instance
App Name Slot ID Admin State Oper State Running Version Startup Version Profile Name
Cluster State Cluster Role

ftd 1 Enabled Online 6.2.2.81 6.2.2.81
In Cluster Slave
ftd 2 Enabled Online 6.2.2.81 6.2.2.81
In Cluster Slave
ftd 3 Disabled Not Available 6.2.2.81
Not Applicable None
FP9300-A /ssa #

```

**ステップ 10** シャーシ #2 のセキュリティモジュールの 1 つを制御用として設定します。

シャーシ #2 のセキュリティモジュールの 1 つを制御用として設定すると、シャーシ #1 には制御ユニットが含まれなくなり、すぐにアップグレードすることができます。

**ステップ 11** クラスタ内の他のすべてのシャーシに対して手順 1 ~ 9 を繰り返します。

**ステップ 12** 制御ロールをシャーシ #1 に戻すには、シャーシ #1 のセキュリティモジュールの 1 つを制御用として設定します。

## FXOS CLI を使用した FTD ハイアベイラビリティペアの FXOS のアップグレード

ハイアベイラビリティペアとして構成されている FTD 論理デバイスを備えた FirePOWER 9300 または FirePOWER 4100 シリーズのセキュリティアプライアンスがある場合、次の手順を使用



して FirePOWER 9300 または FirePOWER 4100 シリーズのセキュリティアプライアンスの FXOS プラットフォームバンドルを更新します。

### 始める前に

アップグレードを開始する前に、以下が完了していることを確認します。

- アップグレード先の FXOS プラットフォーム バンドル ソフトウェア パッケージをダウンロードします。
- FXOS と FTD の構成をバックアップします。
- Firepower 4100/9300 シャーシにソフトウェアイメージをダウンロードするために必要な次の情報を収集します。
  - イメージのコピー元のサーバーの IP アドレスおよび認証クレデンシャル。
  - イメージ ファイルの完全修飾名。

**ステップ 1** スタンバイの Firepower Threat Defense 論理デバイスを含む Firepower セキュリティ アプライアンス上の FXOS CLI に接続します。

**ステップ 2** 新しいプラットフォーム バンドル イメージを Firepower 4100/9300 シャーシにダウンロードします。

a) ファームウェア モードに入ります。

```
Firepower-chassis-a # scope firmware
```

b) FXOS プラットフォーム バンドル ソフトウェア イメージをダウンロードします。

```
Firepower-chassis-a /firmware # download image URL
```

次のいずれかの構文を使用してインポートされるファイルの URL を指定します。

- `ftp://username@hostname/path/image_name`
- `scp://username@hostname/path/image_name`
- `sftp://username@hostname/path/image_name`
- `tftp://hostname:port-num/path/image_name`

c) ダウンロードプロセスをモニタする場合 :

```
Firepower-chassis-a /firmware # scope download-task image_name
```

```
Firepower-chassis-a /firmware/download-task # show detail
```

例 :

次の例では、SCP プロトコルを使用してイメージをコピーします。

```
Firepower-chassis-a # scope firmware
Firepower-chassis-a /firmware # download image scp://user@192.168.1.1/images/fxos-k9.2.3.1.58.SPA
Firepower-chassis-a /firmware # scope download-task fxos-k9.2.3.1.58.SPA
Firepower-chassis-a /firmware/download-task # show detail
Download task:
```

```

File Name: fxos-k9.2.3.1.58.SPA
Protocol: scp
Server: 192.168.1.1
Userid:
Path:
Downloaded Image Size (KB): 853688
State: Downloading
Current Task: downloading image fxos-k9.2.3.1.58.SPA from
192.168.1.1 (FSM-STAGE:sam:dme:FirmwareDownloaderDownload:Local)

```

**ステップ 3** 必要に応じて、ファームウェア モードに戻ります。

```
Firepower-chassis-a /firmware/download-task # up
```

**ステップ 4** auto-install モードにします。

```
Firepower-chassis-a /firmware # scope auto-install
```

**ステップ 5** FXOS プラットフォーム バンドルをインストールします。

```
Firepower-chassis-a /firmware/auto-install # install platform platform-vers version_number
```

*version\_number* は、インストールする FXOS プラットフォームバンドルのバージョン番号です (たとえば、2.3(1.58))。

**ステップ 6** システムは、まずインストールするソフトウェア パッケージを確認します。そして現在インストールされているアプリケーションと指定した FXOS プラットフォーム ソフトウェア パッケージの間の非互換性を通知します。また既存のセッションを終了することやアップグレードの一部としてシステムをリブートする必要があることが警告されます。

**yes** を入力して、検証に進むことを確認します。

**ステップ 7** インストールの続行を確定するには **yes** を、インストールをキャンセルするには **no** を入力します。

システムがバンドルを解凍し、コンポーネントをアップグレードまたはリロードします。

**ステップ 8** アップグレードプロセスをモニタするには、次の手順を実行します。

- a) **scope system** を入力します。
- b) **show firmware monitor** を入力します。
- c) すべてのコンポーネント (FPRM、ファブリック インターコネクト、およびシャーシ) で「Upgrade-Status: Ready」と表示されるのを待ちます。

(注) FPRM コンポーネントをアップグレードすると、システムが再起動し、その他のコンポーネントのアップグレードを続行します。

例 :

```

FP9300-A# scope system
FP9300-A /system # show firmware monitor
FPRM:
 Package-Vers: 2.3(1.58)
 Upgrade-Status: Ready

Fabric Interconnect A:
 Package-Vers: 2.3(1.58)
 Upgrade-Status: Ready

```

```
Chassis 1:
 Server 1:
 Package-Vers: 2.3(1.58)
 Upgrade-Status: Ready
 Server 2:
 Package-Vers: 2.3(1.58)
 Upgrade-Status: Ready
```

```
FP9300-A /system #
```

- ステップ 9** すべてのコンポーネントが正常にアップグレードされたら、次のコマンドを入力して、セキュリティ モジュール/セキュリティ エンジンおよびインストールされているアプリケーションの状態を確認します。
- top** を入力します。
  - scope ssa** を入力します。
  - show slot** を入力します。
  - Firepower 4100 シリーズ アプライアンスのセキュリティ エンジン、または Firepower 9300 appliance のインストールされている任意のセキュリティ モジュールについて、管理状態が「Ok」、操作の状態が「Online」であることを確認します。
  - show app-instance** を入力します。
  - シャーシにインストールされているすべての論理デバイスについて、操作の状態が「Online」であることを確認します。
- ステップ 10** アップグレードしたユニットをアクティブユニットにして、アップグレード済みのユニットにトラフィックが流れるようにします。
- Firepower Management Center に接続します。
  - [**デバイス (Devices)**] > [**デバイス管理 (Device Management)**] を選択します。
  - アクティブ ピアを変更するハイ アベイラビリティ ペアの横にあるアクティブ ピア切り替えアイコン (🔄) をクリックします。
  - ハイ アベイラビリティ ペアでスタンバイ デバイスをアクティブ デバイスにすぐに切り替える場合は、[はい (Yes)] をクリックします。
- ステップ 11** 新しいスタンバイの Firepower Threat Defense 論理デバイスを含む Firepower セキュリティ アプライアンス上の FXOS CLI に接続します。
- ステップ 12** 新しいプラットフォーム バンドル イメージを Firepower 4100/9300 シャーシにダウンロードします。
- ファームウェア モードに入ります。  
Firepower-chassis-a # **scope firmware**
  - FXOS プラットフォーム バンドル ソフトウェア イメージをダウンロードします。  
Firepower-chassis-a /firmware # **download image URL**  
次のいずれかの構文を使用してインポートされるファイルの URL を指定します。
    - **ftp://username@hostname/path/image\_name**
    - **scp://username@hostname/path/image\_name**
    - **sftp://username@hostname/path/image\_name**

- `tftp://hostname:port-num/path/image_name`

c) ダウンロードプロセスをモニタする場合：

```
Firepower-chassis-a /firmware # scope download-task image_name
```

```
Firepower-chassis-a /firmware/download-task # show detail
```

例：

次の例では、SCP プロトコルを使用してイメージをコピーします。

```
Firepower-chassis-a # scope firmware
Firepower-chassis-a /firmware # download image scp://user@192.168.1.1/images/fxos-k9.2.3.1.58.SPA
Firepower-chassis-a /firmware # scope download-task fxos-k9.2.3.1.58.SPA
Firepower-chassis-a /firmware/download-task # show detail
Download task:
 File Name: fxos-k9.2.3.1.58.SPA
 Protocol: scp
 Server: 192.168.1.1
 Userid:
 Path:
 Downloaded Image Size (KB): 853688
 State: Downloading
 Current Task: downloading image fxos-k9.2.3.1.58.SPA from
 192.168.1.1 (FSM-STAGE:sam:dme:FirmwareDownloaderDownload:Local)
```

**ステップ 13** 必要に応じて、ファームウェア モードに戻ります。

```
Firepower-chassis-a /firmware/download-task # up
```

**ステップ 14** auto-install モードにします。

```
Firepower-chassis-a /firmware # scope auto-install
```

**ステップ 15** FXOS プラットフォーム バンドルをインストールします。

```
Firepower-chassis-a /firmware/auto-install # install platform platform-vers version_number
```

`version_number` は、インストールする FXOS プラットフォームバンドルのバージョン番号です（たとえば、2.3(1.58)）。

**ステップ 16** システムは、まずインストールするソフトウェア パッケージを確認します。そして現在インストールされているアプリケーションと指定した FXOS プラットフォーム ソフトウェア パッケージの間の非互換性を通知します。また既存のセッションを終了することやアップグレードの一部としてシステムをリブートする必要があることが警告されます。

**yes** を入力して、検証に進むことを確認します。

**ステップ 17** インストールの続行を確定するには **yes** を、インストールをキャンセルするには **no** を入力します。

システムがバンドルを解凍し、コンポーネントをアップグレードまたはリロードします。

**ステップ 18** アップグレードプロセスをモニタするには、次の手順を実行します。

a) **scope system** を入力します。

b) **show firmware monitor** を入力します。

- c) すべてのコンポーネント (FPRM、ファブリック インターコネクト、およびシャーシ) で「Upgrade-Status: Ready」と表示されるのを待ちます。

(注) FPRM コンポーネントをアップグレードすると、システムが再起動し、その他のコンポーネントのアップグレードを続行します。

例 :

```
FP9300-A# scope system
FP9300-A /system # show firmware monitor
FPRM:
 Package-Vers: 2.3(1.58)
 Upgrade-Status: Ready

Fabric Interconnect A:
 Package-Vers: 2.3(1.58)
 Upgrade-Status: Ready

Chassis 1:
 Server 1:
 Package-Vers: 2.3(1.58)
 Upgrade-Status: Ready
 Server 2:
 Package-Vers: 2.3(1.58)
 Upgrade-Status: Ready

FP9300-A /system #
```

**ステップ 19** すべてのコンポーネントが正常にアップグレードされたら、次のコマンドを入力して、セキュリティ モジュール/セキュリティ エンジンおよびインストールされているアプリケーションの状態を確認します。

- top** を入力します。
- scope ssa** を入力します。
- show slot** を入力します。
- Firepower 4100 シリーズ アプライアンスのセキュリティ エンジン、または Firepower 9300 appliance のインストールされている任意のセキュリティ モジュールについて、管理状態が「Ok」、操作の状態が「Online」であることを確認します。
- show app-instance** を入力します。
- シャーシにインストールされているすべての論理デバイスについて、操作の状態が「Online」であることを確認します。

**ステップ 20** アップグレードしたユニットを、アップグレード前のようにアクティブ ユニットにします。

- Firepower Management Center に接続します。
- [**デバイス (Devices)**] > [**デバイス管理 (Device Management)**] を選択します。
- アクティブ ピアを変更するハイ アベイラビリティ ペアの横にあるアクティブ ピア切り替えアイコン (🔄) をクリックします。
- ハイ アベイラビリティ ペアでスタンバイ デバイスをアクティブ デバイスにすぐに切り替える場合は、[はい (Yes)] をクリックします。





## 第 7 章

# アップグレードを復元する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 Threat Defense に復元することができます。
- アンインストールは、Management Center を搭載した Threat Defense へのパッチが対象です。Management Center 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。

- [Threat Defense アップグレードの復元 \(105 ページ\)](#)
- [パッチのアンインストール \(110 ページ\)](#)

## Threat Defense アップグレードの復元

Management Center を使用して、メジャーおよびメンテナンスアップグレードを Threat Defense に復元することができます。復元すると、ソフトウェアは、最後のメジャーアップグレードまたはメンテナンスアップグレード（スナップショットとも呼ばれます）の直前の状態に戻ります。パッチ適用後に復元すると、パッチも必然的に削除されます。

### 元に戻る設定

次の設定が元に戻ります。

- Snort バージョン。
- デバイス固有の設定。

一般的なデバイス設定、ルーティング、インターフェース、インラインセット、DHCP、SNMPなど、[デバイス (Devices)] > [デバイス管理 (Device Management)] ページで設定するものすべて。

- デバイス固有の設定で使用されるオブジェクト。

アクセスリスト、AS パス、キーチェーン、インターフェース、ネットワーク、ポート、ルートマップ、SLA モニターオブジェクトなどが含まれます。デバイスのアップグレード後にこれらのオブジェクトを編集した場合、システムは新しいオブジェクトを作成するか、元に戻されたデバイスが使用するオブジェクトのオーバーライドを設定します。これにより、他のデバイスは現在の設定に従ってトラフィックを処理し続けることができます。

復元に成功したら、復元したデバイスで使用されているオブジェクトを調べ、必要な調整を行うことをお勧めします。

### 元に戻されない設定

次の設定は元に戻りません。

- 複数のデバイスで使用できる共有ポリシー。たとえば、プラットフォーム設定やアクセスコントロールポリシーなどです。

正常に元に戻されたデバイスは期限切れとしてマークされているため、設定を再展開する必要があります。

- Firepower 4100/9300 で、Secure Firewall Chassis Manager または FXOS CLI を使用して Threat Defense 論理デバイスに加えたインターフェースの変更。

Firepower 4100/9300 では、復元に成功した後にインターフェースの変更を同期します。

## 復元ガイドライン

### システム要件

復元を行うには、Threat Defense および Management Center 両方でバージョン 7.1.0 以降が必要です。

たとえば、バージョン 7.1.0 の Management Center はデバイスをバージョン 6.5.0 までさかのぼって管理でき、そのバージョン 7.1.0 の Management Center を使用してデバイスを中間バージョン (6.6.x、6.7.x、7.0.x) までアップグレードできる場合であっても、デバイスをバージョン 7.1.0 にアップグレードするまで、復元はサポートされません。

復元は、Firepower 4100/9300 のコンテナインスタンスではサポートされません。

### 高可用性/スケーラビリティデバイスの復元

Management Center Web インターフェースを使用してデバイスを復元する場合、個々の高可用性またはクラスタ化されたユニットを選択することはできません。



すべてのユニットを同時に復元させたほうが、復元が成功する可能性が高くなります。**Management Center** から復元を開始すると、システムは自動的にすべてのユニットを同時に復元させます。デバイス CLI を使用する必要がある場合は、手動で行います。すべてのユニットでセッションを開き、それぞれで復元が可能であることを確認してから、プロセスを同時に開始します。同時復元とは、すべてのデバイスがスタンダ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。

完全または部分的にアップグレードされたグループで復元がサポートされていることに注意してください。部分的にアップグレードされたグループの場合、システムはアップグレードされたユニットからのみアップグレードを削除します。元に戻しても高可用性やクラスタが壊れることはありませんが、グループを分解してその新しいスタンダロンユニットを復元することができます。

### 復元しても FXOS はダウングレードされない

Firepower 4100/9300 の場合、**Threat Defense** 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。**Threat Defense** の以前のバージョンに戻った後、推奨されていないバージョンの FXOS（新しすぎる）を実行している可能性があります。

新しいバージョンの FXOS は旧バージョンの **Threat Defense** と下位互換性がありますが、シスコでは推奨の組み合わせについて拡張テストを実施しています。FXOS を手動ではダウングレードできないため、このような状況下で推奨の組み合わせを稼働するには、完全な再イメージ化が必要になります。

### 復元を妨げるシナリオ

次のいずれかの状況で復元を試みると、システムはエラーを表示します。

表 36: 復元を妨げるシナリオ

| シナリオ                                                                                                                                                                                                                                                    | 解決方法                                                                                                                                                                                                                                                                                                                                                                                                                             |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>次の理由により、スナップショットを復元することはできません。</p> <ul style="list-style-type: none"> <li>• デバイスをアップグレードしたときに、復元を有効にしていませんでした。</li> <li>• Management Center またはデバイスからスナップショットを削除したか、スナップショットの期限が切れました。</li> <li>• 別の Management Center でデバイスをアップグレードしました。</li> </ul> | <p>なし。</p> <p>アップグレード完了後に元に戻す必要がある可能性がある場合は、システム (⚙️) &gt; [更新 (Updates)] ページを使用し、Management Center で Threat Defense をアップグレードします。これは、「アップグレード成功後の復元を可能にする」オプションを設定する唯一の方法です。</p> <p><b>重要</b> これは、[デバイス (Devices)] &gt; [デバイスのアップグレード (Device Upgrade)] ページでウィザードを使用する通常の推奨とは対照的です。</p> <p>復元スナップショットは、Management Center とデバイスに 30 日間保存され、その後自動的に削除され、復元できなくなります。ディスク容量を節約するためにどのアプライアンスからでもスナップショットを手動で削除できますが、復元の機能が失われます。</p> |
| <p>最後のアップグレードに失敗しました。</p>                                                                                                                                                                                                                               | <p>アップグレードをキャンセルして、デバイスをアップグレード前の状態に戻します。または、問題を修正して再試行してください。</p> <p>復元は、アップグレードは成功したものの、アップグレードされたシステムが期待どおりに機能しない場合に使用します。復元は、失敗または進行中のアップグレードをキャンセルすることとは異なります。元に戻すこともキャンセルすることもできない場合は、イメージを再作成する必要があります。</p>                                                                                                                                                                                                               |
| <p>アップグレード以降に、管理アクセスインターフェイスが変更されています。</p>                                                                                                                                                                                                              | <p>元に戻して、もう一度お試しください。</p>                                                                                                                                                                                                                                                                                                                                                                                                        |
| <p>クラスタのユニットが異なるバージョンからアップグレードされました。</p>                                                                                                                                                                                                                | <p>すべて一致するまでユニットを削除し、クラスタメンバーを調整してから、小さなクラスタを復元します。新しくスタンドアロンユニットを復元することもできます。</p>                                                                                                                                                                                                                                                                                                                                               |
| <p>クラスタでのアップグレード後に 1 つ以上のユニットがクラスタに追加されました。</p>                                                                                                                                                                                                         | <p>新しいユニットを削除し、クラスタメンバーを調整してから、小さなクラスタを復元します。新しくスタンドアロンユニットを復元することもできます。</p>                                                                                                                                                                                                                                                                                                                                                     |

| シナリオ                                                   | 解決方法                                              |
|--------------------------------------------------------|---------------------------------------------------|
| クラスタで Management Center と FXOS が異なる数のクラスタユニットを識別しています。 | クラスタメンバーを調整して再試行しますが、すべてのユニットを復元することはできない場合があります。 |

## Management Center を使用して Threat Defense を復元する

Management Center とデバイス間の通信が中断されない限り、Management Center を使用してデバイスを復元する必要があります。通信が中断された場合は、デバイスで **upgrade revert CLI** コマンドを使用できます。システムがどのバージョンに戻るのかを確認するには、**show upgrade revert-info** コマンドを使用します。



**注意** CLIから復元すると、アップグレード後に行った変更によっては、デバイスと Management Center間で設定が同期されないことがあります。これにより、後に通信と展開の問題が発生する可能性があります。

### 始める前に

- 復元がサポートされていることを確認してください。ガイドラインを読んで理解してください。
- 安全な外部の場所にバックアップします。復元に失敗した場合、再イメージ化が必要になることがあります。再イメージ化を行うと、ほとんどの設定が工場出荷時の状態に戻ります。

**ステップ 1** [デバイス (Devices) ] > [デバイス管理 (Device Management) ] を選択します。

**ステップ 2** 復元するデバイスの横にある **その他** (⋮) をクリックして、[アップグレードの復元 (Revert Upgrade) ] を選択します。

ハイ アベイラビリティペアとクラスタを除き、複数のデバイスを選択して復元することはできません。

**ステップ 3** 復元して再起動することを確認します。

復元中のトラフィックフローとインスペクションの中断は、すべてのデバイスがスタンドアロンであるかのように、インターフェイス設定に依存します。これは、高可用性/スケーラビリティ展開であっても、システムがすべてのユニットを同時に復元するためです。

**ステップ 4** 復元の進行状況を監視します。

高可用性/スケーラビリティ展開では、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。数分間にわたり進展がない場合、または復元が失敗したことを示している場合は、Cisco TAC にお問い合わせください。

**ステップ 5** 復元が成功したことを確認します。

復元が完了したら、[デバイス (Devices)] > [デバイス管理 (Device Management)] を選択し、復元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** (Firepower 4100/9300) Chassis Manager または FXOS CLI を使用して、Threat Defense 論理デバイスに加えたインターフェイスの変更を同期します。

Management Center で [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択し、デバイスを編集して [同期 (Sync)] をクリックします。

**ステップ 7** その他に必要な復元後の構成変更を完了します。

たとえば、デバイスのアップグレード後にデバイス固有の設定で使用するオブジェクトを編集した場合、システムは新しいオブジェクトを作成するか、復元されたデバイスが使用するオブジェクトのオーバーライドを設定します。復元したデバイスで使用されるオブジェクトを調べ、必要な調整を行うことをお勧めします。

**ステップ 8** 復元したデバイスに構成を再度展開します。

正常に復元されたデバイスは期限切れとしてマークされます。デバイスは古いバージョンを実行することになるため、展開が成功した後でも、新しい構成がサポートされない場合があります。

## パッチのアンインストール

パッチをアンインストールするとアップグレード前のバージョンに戻り、設定は変更されません。Management Center では、管理対象デバイスと同じかより新しいバージョンを実行する必要があるため、最初にデバイスからパッチをアンインストールします。

## 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 7.2 のパッチ

現在、すべてのバージョン 7.2 パッチがアンインストールに対応しています。

## 高可用性/拡張性のアンインストール順序

高可用性/拡張性の展開では、一度に 1 つのプライアンスからアンインストールすることで中断を最小限に抑えます。アップグレードとは異なり、システムはこの操作を行いません。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 37: *Management Center* 高可用性のアンインストール順序

| 設定                               | アンインストール順序                                                                                                                                                                                                                                                                                         |
|----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Management Center ハイ<br>アベイラビリティ | 同期を一時停止した状態（「スプリットブレイン」と呼びます）で、ピアから一度に 1 つずつアンインストールします。ペアが <b>split-brain</b> の状況で、構成の変更または展開を行わないでください。 <ol style="list-style-type: none"> <li>1. 同期を一時停止します（スプリットブレインに移行します）。</li> <li>2. スタンバイからアンインストールします。</li> <li>3. アクティブからアンインストールします。</li> <li>4. 同期を再開します（スプリットブレインから抜けます）。</li> </ol> |

表 38: *Threat Defense* 高可用性およびクラスタのアンインストール順序

| 設定                            | アンインストール順序                                                                                                                                                                                                                                                |
|-------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Threat Defense ハイ<br>アベイラビリティ | ハイ アベイラビリティ用に設定されたデバイスからパッチをアンインストールすることはできません。先にハイ アベイラビリティを解除する必要があります。 <ol style="list-style-type: none"> <li>1. ハイ アベイラビリティを解除します。</li> <li>2. 以前のスタンバイからアンインストールします。</li> <li>3. 以前のアクティブからアンインストールします。</li> <li>4. ハイ アベイラビリティを再確立します。</li> </ol>   |
| Threat Defense クラス<br>タ       | 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。クラスタ化されたユニットは、パッチのアンインストール中はメンテナンス モードで動作します。 <ol style="list-style-type: none"> <li>1. データモジュールから一度に 1 つずつアンインストールします。</li> <li>2. データモジュールの 1 つを新しい制御モジュールに設定します。</li> <li>3. 以前のコントロールからアンインストールします。</li> </ol> |

## Threat Defense 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 Threat Defense 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。Management Center ユーザーアカウントは使用できません。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。



**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

- 高可用性ペアを解除します。「[高可用性/拡張性のアンインストール順序 \(111 ページ\)](#)」を参照してください。
- 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 Management Center 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** デバイスの Threat Defense 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 CLI ユーザーとしてログインします。

デバイス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。コンソールを使用する場合、一部のデバイスではデフォルトでオペレーティングシステムの CLI に設定されており、Threat Defense CLI にアクセスする場合は追加の手順が必要になります。

|                     |                                                                                          |
|---------------------|------------------------------------------------------------------------------------------|
| Firepower 1000 シリーズ | <code>connect ftd</code>                                                                 |
| Firepower 2100 シリーズ | <code>connect ftd</code>                                                                 |
| Firepower 3100 シリーズ | <code>connect ftd</code>                                                                 |
| Firepower 4100/9300 | <code>connect module slot_number console</code> 、次に <code>connect ftd</code> (最初のログインのみ) |

**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、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。Management Center で、[ **デバイス (Devices)** ] > [ **デバイス管理 (Device Management)** ] を選択します。

**ステップ8** 高可用性/スケーラビリティの展開では、ユニットごとに手順 2 から 6 を繰り返します。

クラスタの場合、制御ユニットからアンインストールしないでください。すべてのデータユニットからアンインストールしたら、そのうちの 1 つを新しい制御ユニットに設定し、以前の制御ユニットからアンインストールします。

**ステップ9** 構成を再展開します。

**例外：**複数のバージョンが構成されている高可用性ペアまたはデバイスクラスタには展開しないでください。展開は最初のデバイスからアンインストールする前に行いますが、すべてのグループメンバからパッチのアンインストールを終えるまでは再度展開しないでください。

---

### 次のタスク

- 高可用性については、高可用性を再確立します。
- クラスタについては、特定のデバイスに優先するロールがある場合は、それらの変更をすぐに行います。

## スタンドアロン Management Center パッチのアンインストール

Management Center パッチのアンインストールには Web インターフェイスを使用することを勧めます。Web インターフェイスを使用できない場合は、Linux シェルを、シェルの admin ユーザーまたはシェル アクセス権を持つ外部ユーザーのどちらかとして使用できます。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。



**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

- アンインストールによって Management Center のパッチレベルが管理対象デバイスより低くなる場合は、最初にデバイスからパッチをアンインストールします。
- 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** 構成が古い管理対象デバイスに展開します。

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。

**ステップ 2** [利用可能なアップデート (Available Updates)] で該当するアンインストール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、Management Center を選択します。

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。Management Center 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 3** [インストール (Install)] をクリックしてから、アンインストールすることを確認して再起動します。

ログアウトするまで、メッセージセンターでアンインストールの進行状況を確認します。

**ステップ 4** 可能なときに再度ログインし、アンインストールが成功したことを確認します。

ログイン時にアンインストールの成功メッセージが表示されない場合は、[ヘルプ (Help)] > [バージョン情報 (About)] の順に選択して、現在のソフトウェアのバージョン情報を表示します。

**ステップ 5** 管理対象デバイスに構成を再展開します。



## 高可用性 Management Center パッチのアンインストール

Management Center パッチのアンインストールには Web インターフェイスを使用することをお勧めします。Web インターフェイスを使用できない場合は、Linux シェルを、シェルの admin ユーザーまたはシェルアクセス権を持つ外部ユーザーのどちらかとして使用できます。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。

高可用性ピアから一度に1つずつアンインストールします。同期を一時停止した状態で、先にスタンバイからアンインストールし、次にアクティブからアンインストールします。スタンバイでアンインストールが開始されると、ステータスがスタンバイからアクティブに切り替わり、両方のピアがアクティブになります。この一時的な状態のことを「スプリットブレイン」と呼び、アップグレード中とアンインストール中を除き、サポートされていません。



**注意** ピアが split-brain の状況で、構成の変更または展開を行わないでください。同期の再開後は変更内容が失われます。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

- アンインストールによって Management Center のパッチレベルが管理対象デバイスより低くなる場合は、最初にデバイスからパッチをアンインストールします。
- 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** アクティブな Management Center で、構成が古い管理対象デバイスに展開します。

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。

**ステップ 2** アクティブ状態の Management Center で、同期を一時停止します。

- a) [システム (System)] > [統合 (Integration)] の順に選択します。
- b) [ハイアベイラビリティ (High Availability)] タブで、[同期の一時停止 (Pause Synchronization)] をクリックします。

**ステップ 3** ピアからパッチを一度に1つずつアンインストールします。先にスタンバイで行い、次はアクティブで行います。

「[スタンドアロン Management Center パッチのアンインストール \(114 ページ\)](#)」の手順に従います。ただし、初期の展開は省略し、各ピアでアンインストールが成功したことを確認したら停止します。要約すると、各ピアで次の手順を実行します。

- a) [システム (System)] > [更新 (Updates)] ページで、パッチをアンインストールします。

- b) ログアウトするまで進行状況を確認し、ログインできる状態になったら再びログインします。
- c) アンインストールが成功したことを確認します。

**ステップ 4** アクティブ ピアにする Management Center で、同期を再開します。

- a) [システム (System)] > [統合 (Integration)] の順に選択します。
- b) [ハイアベイラビリティ (High Availability)] タブで、[アクティブにする (Make-Me-Active)] をクリックします。
- c) 同期が再開し、その他の Management Center がスタンバイ モードに切り替わるまで待ちます。

**ステップ 5** 管理対象デバイスに構成を再展開します。

---

## 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。