Cisco Firepower バージョン 6.3.0.1、6.3.0.2、6.3.0.3、6.3.0.4、および 6.3.0.5 リリースノート

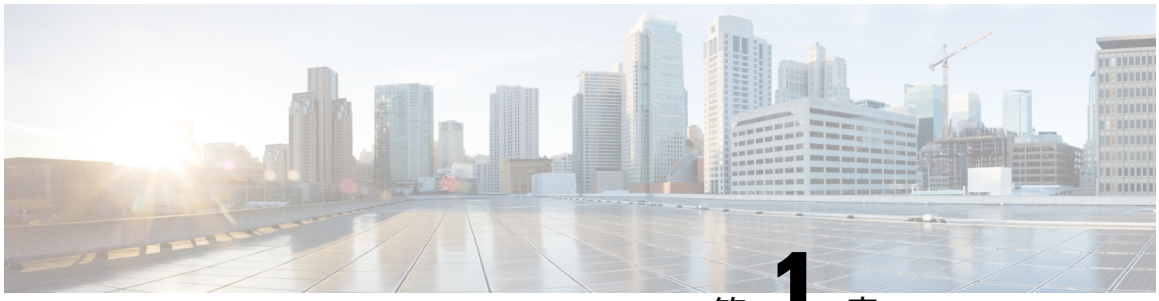
初版：2019 年 2 月 18 日

最終更新：2020 年 5 月 26 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/

【注意】シスコ製品をご使用になる前に、安全上の注意（**www.cisco.com/jp/go/safety_warning/**）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

目 次



第 1 章

バージョン 6.3.0.x の概要

Firepower をお選びいただき、ありがとうございます。

リリース ノートについて

リリース ノートには、アップグレードの警告や動作の変更など、バージョン 6.3.0.x に関する重要なリリース固有の情報が記載されています。Firepower リリースに精通しており、Firepower 展開をアップグレードした経験がある場合でも、このドキュメントお読みください。

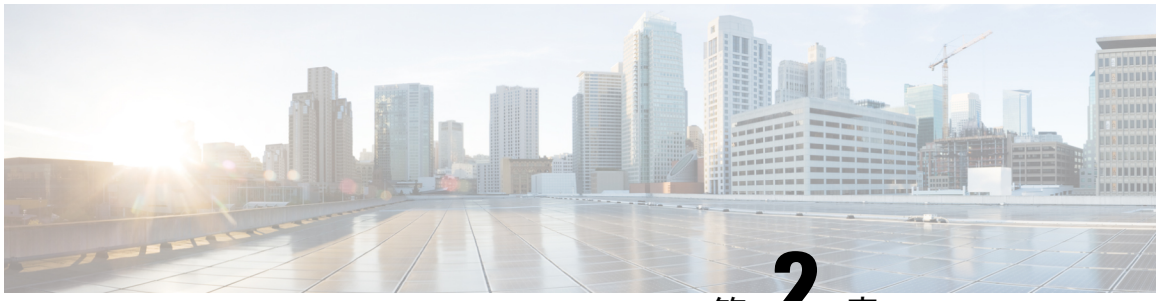
Firepower ソフトウェアのアップグレードまたは新規インストールは、複雑なプロセスになる場合があります。ここで手順を説明する代わりに、リリース ノートでは適切なリソースを示しています。アップグレードとインストールの手順については、次のリンクを参照してください。

リリース日

バージョン 6.3.0.x で使用可能なすべてのプラットフォームの一覧については、「互換性, on page 3」を参照してください。

Table 1: バージョン ***6.3.0.x*** のリリース日

バージョン	ビルド	日付	プラットフォーム
6.3.0.5	35	2019 年 11 月 18 日	Firepower 7000/8000 シリーズ NGIPSv
	34	2019 年 11 月 18 日	FMC/FMCv すべての FTD デバイス ASA FirePOWER
6.3.0.4	44	2019 年 8 月 14 日	すべて（All）
6.3.0.3	77	2019 年 6 月 27 日	FMC 1600、2600、4600
		2019 年 5 月 1 日	FMC 750、1000、1500、2000、2500、3500、4000、4500 FMCv すべてのデバイス
6.3.0.2	67	2019 年 6 月 27 日	FMC 1600、2600、4600
		2019 年 3 月 20 日	FMC 750、1000、1500、2000、2500、3500、4000、4500 FMCv すべてのデバイス
6.3.0.1	85	2019 年 6 月 27 日	FMC 1600、2600、4600
		2019 年 2 月 18 日	FMC 750、1000、1500、2000、2500、3500、4000、4500 FMCv すべてのデバイス



第 2 章

互換性

この章では、Firepower バージョン 6.3.0.xパッチの互換性に関する情報を提供します。

Firepower Management Centerについて

バージョン 6.3.0.x Firepower Management Center ソフトウェアは、物理および仮想プラットフォームでサポートされています。FMC は、混在展開を含めて、FTD または NGIPS を実行する複数のデバイスを管理できます。

Firepower Management Center 物理プラットフォーム

バージョン 6.3.0.x は、以下をサポートします。

- FMC 1600、2600、4600
- FMC 1000、2500、4500
- FMC 2000、4000
- FMC 750、1500、3500

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ことをお勧めします。詳細については、『Cisco Firepower Compatibility Guide』を参照してください。

Firepower Management Center Virtual （FMCv）プラットフォーム：

バージョン 6.3.0.x は、以下をサポートします。

- VMware vSphere/VMware ESXi 6.0 または 6.5 上の FMCv

- カーネルベース仮想マシン（KVM）上の FMCv
- Amazon Web Services（AWS）上の FMCv

サポートされている FMCv インスタンスについては、『Cisco Firepower Management Center Virtual 入門ガイド』を参照してください。

Firepower デバイス

バージョン 6.3.0.x Firepower デバイス ソフトウェアは、さまざまな物理および仮想プラットフォームでサポートされています。

- **ソフトウェア**：一部の Firepower デバイスは Firepower Threat Defense（FTD）ソフトウェアを実行します。また、一部の Firepower デバイスは NGIPS/ASA FirePOWER ソフトウェアを実行します。一部ではどちらを実行することもできますが、両方を同時に実行することはできません。
- **リモート管理**：すべての Firepower デバイスは、複数のデバイスを管理できる Firepower Management Center（FMC）を使用したリモート管理をサポートします。
- **ローカル管理**：一部の Firepower デバイスは、ローカルの単一デバイス管理をサポートしています。Firepower Device Manager（FDM）で FTD を管理するか、ASDM で ASA FirePOWER を管理できます。一度に 1 つのデバイスに関して使用できる管理方法は 1 つだけです。
- **OS/ハイパーバイザ**：一部の Firepower 実装では、オペレーティングシステムとソフトウェアがバンドルされます。その他の実装では、自分でオペレーティング システムをアップグレードする必要があります。バンドルされたオペレーティングシステムのバージョンとビルドについては、『Cisco Firepower Compatibility Guide』の「Bundled Components」の情報を参照してください。

サポートされている Firepower のデバイス

次の表は、バージョン 6.3.0.x を実行している Firepower デバイスの互換性情報を示しています。ここでも、すべてのデバイスがリモート FMC 管理をサポートしていることに注意してください。

表 2 : バージョン *6.3.0.x* の *Firepower* デバイス

デバイスのプラットフォーム	ソフトウェア	ローカル管理	OS/ハイパーバイザ
Firepower 2110、2120、2130、2140	FTD	FDM	—

デバイスのプラットフォーム	ソフトウェア	ローカル管理	OS/ハイパーバイザ
Firepower 4110、4120、4140、4150 Firepower 9300 SM-24、SM-36、SM-44 モジュールを搭載	FTD	—	FXOS 2.4.1.214 以降のビルド。 個別のアップグレード。最初に FXOS をアップグレードします。 問題を解決するには、FXOS を最新のビルドにアップグレードする必要がある場合があります。判断のヒントについては、『Cisco Firepower 4100/9300 FXOS Release Notes, 2.4(1)』を参照してください。
ISA 3000	FTD	FDM	—
ASA 5508-X、5516-X ASA 5515-X、5525-X、5545-X、5555-X	ASA FirePOWER（NGIPS）	ASDM	次のいずれかです。 • ASA 9.5(2)、9.5(3) • ASA 9.6(x) ～ 9.14(x) 例外： • ASA 5515-X デバイスは ASA 9.13(x)+ をサポートしていません。 個別のアップグレード。操作の順序については、『Cisco ASA Upgrade Guide』を参照してください。 ASA と ASA FirePOWER のバージョンには幅広い互換性があります。ただし、厳密には ASA のアップグレードが必要でない場合でも、問題解決のために、サポートされた最新のバージョンへのアップグレードが必要になることがあります。 ASA 5508-x、および 5516-x を最新の ROMMON イメージにアップグレードすることをお勧めします。手順については、『Cisco ASA and Firepower Threat Defense Reimage Guide』を参照してください。

デバイスのプラットフォーム	ソフトウェア	ローカル管理	OS/ハイパーバイザ
ASA 5585-X-SSP-10、-20、-40、-60	ASA FirePOWER（NGIPS）	ASDM	次のいずれかです。 • ASA 9.5(2)、9.5(3) • ASA 9.6(x) ～ 9.12(x) 個別のアップグレード。操作の順序については、『Cisco ASA Upgrade Guide』を参照してください。 ASA と ASA FirePOWER のバージョンには幅広い互換性があります。ただし、厳密にはASA のアップグレードが必要でない場合でも、問題解決のために、サポートされた最新のバージョンへのアップグレードが必要になることがあります。
FTDv	FTD	FDM（VMware および KVM のみ）	次のいずれかです。 • VMware vSphere/VMware ESXi 6.0 または 6.5 • KVM • AWS • Microsoft Azure サポートされているインスタンスについては、該当するFTDv のスタートアップガイドを参照してください。
NGIPSv	NGIPS	—	VMware vSphere/VMware ESXi 6.0 または 6.5 サポートされているインスタンスについては、『Cisco Firepower NGIPSv（VMware 向け）クイックスタート』を参照してください。
Firepower 7010、7020、7030、7050 Firepower 7110、7115、7120、7125 Firepower 8120、8130、8140 Firepower 8250、8260、8270、8290 Firepower 8350、8360、8370、8390 AMP 7150、8050、8150 AMP 8350、8360、8370、8390	NGIPS	選択した管理機能のためのローカル GUI が制限されています。	—

マネージャとデバイスの互換性

FMC では、管理対象のデバイスと同じメジャーバージョンを実行している必要があります。パッチ未適用の FMC を使用してパッチを適用したデバイスを管理することもできますが、新しい機能と解決済みの問題では、多くの場合 FMC とその管理対象デバイスの「両方」で最新のパッチが必要になります。環境全体をパッチすることを強くお勧めします。

Table 3: **バージョン *6.3.0.x* のマネージャとデバイスの互換性**

Firepower Management Center		
バージョン 6.3.0.x FMC	管理可能	バージョン 6.1 ～ 6.3.0.x のデバイス。
バージョン 6.3.0.x のデバイス	必須	バージョン 6.3.0 FMC。
Firepower Device Manager		
バージョン 6.3.0.x FDM	管理可能	FTD デバイス 1 台。
ASDM		
バージョン 7.10.1 の ASDM	管理可能	バージョン 6.3.0.x 以前の ASA FirePOWER モジュール。
バージョン 6.3.0.x ASA FirePOWER モジュール	*require*	バージョン 7.10.1 の ASDM。

Web ブラウザの互換性

Firepower Web インターフェイスでテストされたブラウザ

Firepower Web インターフェイスは、現在サポートされている MacOS および Microsoft Windows で動作する、次の一般的なブラウザの最新バージョンでテストされています。

- Google Chrome
- Mozilla Firefox
- Microsoft Internet Explorer 11（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。

Note Apple Safari または Microsoft Edge 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 Internet Explorer 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 Internet Explorer 11 を使用している場合：

- [保存しているページの新しいバージョンがあるかどうかの確認（Check for newer versions of stored pages）] 閲覧履歴オプションについては、[自動（Automatically）] を選択してください。
- [サーバーにファイルをアップロードするときにローカルディレクトリのパスを含める（Include local directory path when uploading files to server）] カスタム セキュリティ設定を無効にします。
- Firepower Web インターフェイスの IP アドレス/URL の**互換表示**を有効にします。

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 などがありますが、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。Firepower アプライアンス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。

セキュア通信

Firepower Web インターフェイスに初めてログインすると、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 Firepower Web インターフェイスを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手順は、次のとおりです。

- FMC または 7000/8000 シリーズ：**[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。
- FDM：**[デバイス（Device）]**、**[システム設定（System Settings）]** > **[管理アクセス（Management Access）]** リンク、**[管理 Web サーバ（Management Web Server）]** タブの順にクリックします。

手順について詳しくは、オンラインヘルプまたはご使用の Firepower 製品の設定ガイドを参照してください。

Note

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の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。

Firepower で監視されるネットワークからのブラウジング

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、モニタ対象ネットワーク内のユーザが 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。

画面解像度の要件

***Table 4: Firepower* ユーザ インターフェイスの画面解像度の要件**

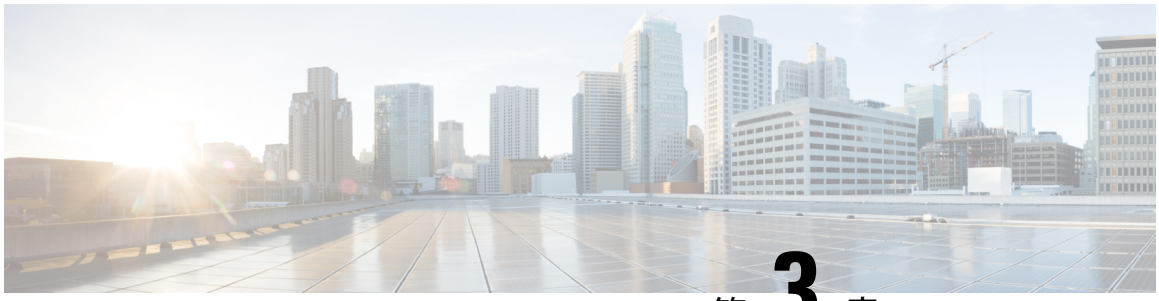
インターフェイス	解像度
Firepower Management Center	1280 X 720
7000/8000 シリーズ デバイス（制限されたローカル インターフェイス）	1280 X 720
Firepower Device Manager	1024 X 768
を管理している ASDM ASA FirePOWER モジュール	1024 X 768
Firepower Chassis Manager 向け Firepower 4100/9300 シャーシ	1024 X 768

その他の互換性関連のリソース

次の表に、リリースノートとその他の互換性情報へのリンクを示します。ドキュメントの完全なロードマップについては、ドキュメントロードマップ, on page 61を参照してください。

Table 5: その他の互換性関連のリソース

説明	リソース
互換性ガイドには、バンドルコンポーネントや統合製品をなど、サポートされているハードウェアモデルとソフトウェアバージョンに関する詳細な互換性情報が記載されています。	Cisco Firepower Compatibility Guide Cisco ASA の互換性 Cisco Firepower 4100/9300 FXOS の互換性
リリースノートには、アップグレードの警告や動作の変更など、リリース固有の情報が記載されています。	Cisco Firepower リリースノート Cisco ASA リリースノート Cisco Firepower 4100/9300 FXOS リリースノート
持続性に関する速報には、管理プラットフォームやオペレーティングシステムなど、シスコ□次世代ファイアウォール製品ラインに関するサポートタイムラインが記載されています。	Cisco NGFW 製品ラインのソフトウェアリリースおよび持続性に関する速報



第 3 章

特長と機能

Firepower バージョン 6.3.0.x には以下が含まれます。

新機能

次の表に、バージョン 6.3.0.x のパッチで使用可能な新機能の概要を示します。

表 *6 :* バージョン *6.3.0.x* の新機能

機能	バージョン	説明
FTD NAT ポリシーでのルールの競合の検出	6.3.0.4	バージョン 6.3.0.4 にアップグレードすると、競合するルール（「重複」ルールまたは「オーバーラップ」ルールとも呼ばれます）を持つFTD NATポリシーを作成できなくなります。これは、競合するNATルールが順序どおりに適用されていなかった問題を修正するものです。 現在競合しているNATルールがある場合は、アップグレード後に展開することができます。ただし、NAT ルールは引き続き順序どおりに適用されません。 そのため、アップグレード後にFTD NATポリシーを調べることをお勧めします。それには、ポリシーを編集して再保存を試みます（変更は必要ありません）。ルールが競合している場合は保存ができません。問題を修正して保存し、それから展開します。 （注） 6.4.0にアップグレードすると、この修正が無効になります。この問題は、バージョン 6.3.0.4 および 6.4.0.2 では対処されています。 サポートされるプラットフォーム：FMC を搭載した FTD
EMS拡張機能のサポート	6.3.0.1	バージョン 6.3.0.1 では EMS 拡張機能のサポートが再導入されます。これは、バージョン 6.2.3.8/6.2.3.9 で導入されましたが、バージョン 6.3.0 には含まれていませんでした。 [復号 - 再署名（Decrypt-Resign）] と [復号 - 既知のキー（Decrypt-Known Key）] の両方の SSL ポリシーアクションが、再びClientHelloネゴシエーション時にEMS拡張機能をサポートし、よりセキュアな通信が可能になります。EMS 拡張機能は、 RFC 7627 によって定義されています。 FMC展開では、この機能は、デバイスのバージョンによって異なります。ベストプラクティスは展開全体をアップグレードすることですが、デバイスにパッチを適用するだけでも、この機能はサポートされます。 影響を受けるプラットフォーム：すべて

機能	バージョン	説明
[ISE接続ステータスのモニタ（ISE Connection Status Monitor）] ヘルスモジュール	6.3.0.4	新しいヘルスモジュール [ISE接続ステータスのモニタ（ISE Connection Status Monitor）] は、Cisco Identity Services Engine（ISE）とFMC間のサーバ接続のステータスをモニタします。 新規/変更された画面：[システム（System）] > [健全性（Health）] > [ポリシー（Policy）] > ポリシーの作成または編集 > [ISE接続ステータスのモニタ（ISE Connection Status Monitor）] （注） バージョン 6.4.0 にアップグレードすると、このモジュールが無効になります。サポートは、バージョン 6.4.0.2 で再開されています。 サポート対象プラットフォーム：FMC

廃止された機能

（注） Cisco Firepower User Agent ソフトウェアとアイデンティティソースについてはサポートの終了が予定されています。今すぐ Cisco Identity Services Engine/Passive Identity Connector（ISE/ISE-PIC）に切り替えてください。これにより、ユーザエージェントで使用できない機能も利用できるようになります。ライセンスを変換するには、販売担当者にお問い合わせください。

詳細については、「Cisco Firepower Management Center Configuration Guides」ページで該当する *Cisco Firepower* ユーザ エージェント コンフィギュレーション ガイドを参照してください。

バージョン 6.3.0 のパッチで廃止された機能はありません。

FMC How-To ウォークスルー

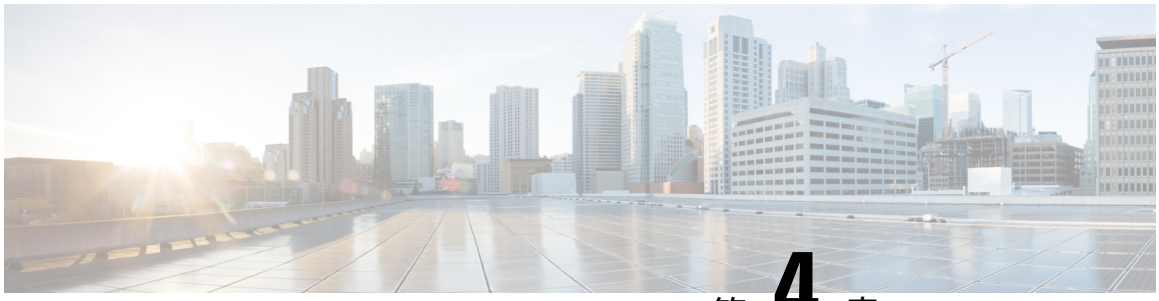
バージョン 6.3.0 では、デバイスのセットアップやポリシー設定などのさまざまな基本タスクについて順を追って説明する、FMC に関するウォークスルー（How-To とも呼ばれる）が導入されています。ブラウザウィンドウの下部にある [How To] をクリックし、ウォークスルーを選択して、手順ごとの説明に従って操作します。

（注） ウォークスルーはFirefoxおよびChromeブラウザでテストされています。別のブラウザで問題が発生した場合は、Firefox または Chrome に切り替えてください。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。

次の表に、一般的な問題点と解決策をいくつか示します。ウォークスルーは、右上隅の [x] をクリックするといつでも終了できます。

表 7: ウォークスルーのトラブルシューティング

問題	解決方法
ウォークスルーを開始するための [How To] リンクが見つからない。	ウォークスルーが有効になっていることを確認します。ユーザ名の下にあるドロップダウンリストから、[ユーザ設定（User Preferences）] を選択し、[設定方法（How-To Settings）] をクリックします。
ウォークスルーが予期しないタイミングで表示される。	ウォークスルーが予期しないタイミングで表示される場合は、ウォークスルーを終了します。
ウォークスルーが突然消えたり終了したりする。	ウォークスルーが消えた場合は、次のようにします。 • ポインタを移動します。 FMC で進行中のウォークスルーが表示されなくなることがあります。たとえば、別のトップレベルメニューをポイントすると表示されなくなります。 • 別のページに移動して、もう一度やり直してください。 ポインタを移動しても表示されない場合は、ウォークスルーが終了している可能性があります。
ウォークスルーが FMC と同期していない。 • 誤った手順から開始される。 • 進行が早すぎる。 • 先に進まない。	ウォークスルーが同期していない場合は、次のようにします。 • 続行します。 たとえば、フィールドに無効な値を入力してエラーが表示された場合は、ウォークスルーが先に進行することがあります。戻ってエラーを解決してタスクを完了することが必要になる場合があります。 • ウォークスルーを終了し、別のページに移動してもう一度やり直します。 場合によっては続行できないこともあります。たとえば、手順の完了後に [次へ（Next）] をクリックしないと、ウォークスルーの終了が必要になる場合があります。



第 4 章

バージョン 6.3.0.x へのアップグレード

この章では、バージョン 6.3.0.x の重要なリリースに固有の情報を提供します。

また、新機能、変更された機能、または廃止された機能に関する情報について「特長と機能（11 ページ）」をご確認ください。

に関するガイドラインと警告 バージョン 6.3.0.x

このチェックリストには、バージョン 6.3.0.x パッチに適用される重要なアップグレードガイドラインと警告が含まれています。また、「一般的なガイドラインと警告 （16 ページ）」も確認してください。

表 *8 :* バージョン *6.3.0.x* のガイドライン

✓	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
	アップグレードの失敗：コンテナインスタンスのディスク容量不足（15 ページ）	Firepower 4100/9300	6.3.0.x	以降のパッチ 6.4.0 および 6.5.0

アップグレードの失敗：コンテナインスタンスのディスク容量不足

展開：FTD を搭載した Firepower 4100/9300

アップグレード元：バージョン 6.3.0 ～ 6.4.0.x

直接アップグレード先：バージョン 6.3.0.1 ～ 6.5.0

多くの場合はメジャーアップグレード時に（場合によってはパッチ適用時に）、コンテナインスタンスを使用して設定されたFTDデバイスが、ディスク容量不足のエラーにより事前チェック段階で失敗することがあります。

この問題が発生した場合には、空きディスク容量を増やしてみてください。それでも解決しない場合は、Cisco TAC にお問い合わせください。

一般的なガイドラインと警告

これらの重要なガイドラインと警告は、すべてのアップグレードに適用されます。ただし、このリストは包括的なものではありません。アップグレードパスの計画、OSのアップグレード、準備状況チェック、バックアップ、メンテナンス期間など、アップグレードプロセスに関するその他の重要な情報へのリンクについては、「アップグレード手順 （35 ページ）」を参照してください。

イベントデータと設定データのバックアップ

サポートされている場合は、アップグレードの前後にバックアップすることをお勧めします。

- アップグレード前：アップグレードが致命的なレベルで失敗した場合は、再イメージ化と復元が必要になることがあります。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 FMC 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FMCをバックアップすることをお勧めします。

安全なリモートロケーションにバックアップし、正常に転送が行われることを確認する必要があります。アップグレードによって、ローカルに保存されたバックアップは消去されます。特に、バックアップファイルは暗号化されていないため、不正アクセスを許可しないでください。バックアップ ファイルが変更されていると、復元プロセスは失敗します。

バックアップの最初のステップとして、アプライアンスモデルとバージョンを、パッチレベルを含めて書き留めておいてください。 FMC の場合は、VDB のバージョンを書き留めておきます。 Firepower 4100/9300 シャーシの場合は、FXOS のバージョンを書き留めておきます。。新しいアプライアンスや再イメージ化したアプライアンスにバックアップを復元する必要がある場合は、新しいアプライアンスを最初に更新する必要がある場合があるため、これは重要です。

（注） バックアップと復元は、複雑なプロセスになる可能性があります。手順をスキップしたり、セキュリティ上の問題を無視しないでください。誤りを避けるには、注意深い計画と準備が役立ちます。バックアップと復元の要件、ガイドライン、制限事項、およびベストプラクティスの詳細については、ご使用の Firepower 製品のコンフィギュレーション ガイドを参照してください。

NTP 同期の確認

アップグレードする前に、時刻の提供に使用している NTP サーバと Firepower アプライアンスが同期していることを確認します。同期されていないと、アップグレードが失敗する可能性があります。FMC展開では、時刻のずれが10秒を超えている場合、[時刻同期化ステータス（Time Synchronization Status）] ヘルスモジュールからアラートが発行されますが、手動で確認する必要もあります。

時刻を確認するには、次の手順を実行します。

- FMC：[システム（System）] > [設定（Configuration）] > [時刻（Time）] を選択します。
- デバイス：**show time** CLI コマンドを使用します。

帯域幅の確認

Firepowerアプライアンスをアップグレードする（または準備状況チェックを実行する）には、アップグレードパッケージがアプライアンス上に存在する必要があります。Firepower アップグレードパッケージには、さまざまなサイズがあります。管理ネットワークに大量のデータ転送を実行するための帯域幅があることを確認します。

FMC の展開では、アップグレードパ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る可能性があります。アップグレードする前に、管理対象デバイスに Firepower アップグレードパッケージを手動でプッシュ（コピー）することをお勧めします。詳細については、『Guidelines for Downloading Data from the Firepower Management Center to Managed Devices』（トラブルシューティングのテクニカルノート）を参照してください。

アプライアンスアクセス

Firepower デバイスは、（インターフェイス設定に応じて）アップグレード中、またはアップグレードが失敗した場合に、トラフィックを渡すことを停止できます。Firepower デバイスをアップグレードする前に、ユーザ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。Firepower Management Center 展開では、デバイスを経由せずに FMC 管理インターフェイスにアクセスできる必要もあります。

署名付きのアップグレードパッケージ

Firepowerでは、正しいファイルを使用していることを確認できるようにするために、バージョン6.2.1+からのアップグレードパッケージ（およびバージョン6.2.1+へのホットフィックス）は、署名付きのtarアーカイブ（.tar）になっています。以前のバージョンからのアップグレードでは、引き続き未署名のパッケージが使用されます。

シスコサポートおよびダウンロードサイトからアップグレードパッケージを手動でダウンロードする場合（たとえば、メジャーアップグレードやエアギャップ展開のために）、正しいパッケージをダウンロードしていることを確認してください。 署名付きの（.tar）パッケージは解凍しないでください。

（注） 署名付きのアップグレードパッケージをアップロードした後、システムがパッケージを確認する際に、GUIのロードに数分かかることがあります。表示を高速化するには、署名付きのパッケージが不要になった後、それらのパッケージを削除します。

ASA FirePOWER デバイスでの ASA REST API の無効化

ASA FirePOWER モジュールをアップグレードする前に、ASA REST API を無効にしていることを確認します。無効にしていない場合、アップグレードが失敗することがあります。ASA CLIから：`no rest api agent`。アンインストール後に再度有効にすることができます：`rest-api agent`。

シスコとのデータの共有

一部の機能にシスコとのデータ共有が含まれます。

6.2.3+では、*Cisco Success Network* は、テクニカルサポートを提供するために不可欠な使用状況に関する情報と統計情報をシスコに送信します。アップグレード中に、参加を承諾するか、辞退するかを尋ねられます。また、いつでもオプトインまたはオプトアウトできます。

バージョン6.2.3+では、Web分析のトラッキングは、これに限定されませんが、ページでの操作、ブラウザのバージョン、製品のバージョン、ユーザの場所、FMC の管理 IP アドレスまたはホスト名を含む、個人を特定できない使用状況データをシスコに送信します。現在の設定でオプトアウトが選択されている場合でも、メジャーアップグレードによってWeb分析トラッキングが有効になります。このデータの収集を拒否する場合は、各メジャーアップグレードの後にオプトアウトしてください。

アップグレードにより侵入ルールをインポートして自動的に有効化できます。

現在の Firepower バージョンでサポートされていないキーワードが新しい侵入ルールで使用されている場合、侵入ルールデータベース（SRU）を更新しても、そのルールはインポートされません。

Firepower ソフトウェアをアップグレードし、これらのキーワードがサポートされると、新しい侵入ルールがインポートされ、IPS の設定に応じて自動的に有効化できるため、イベントの生成とトラフィックフローへの影響を開始できます。

サポートされているキーワードは、Firepower ソフトウェアに含まれている Snort のバージョンによって異なります。

- FMC：[ヘルプ（Help）] > [About（バージョン情報）] を選択します。
- FDM を使用した FTD：**show summary** CLI コマンドを使用します。
- ASDM を使用した ASA FirePOWER：[ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [システム情報（System Information）] を選択します。

また、『Cisco Firepower Compatibility Guide』の「*Bundled Components*」の項で Snort バージョンを確認することもできます。

Snort リリースノートには、新しいキーワードの詳細が含まれています。https://www.snort.org/downloads でSnort ダウンロードページのリリースノートを参照できます。

応答しないアップグレード

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

アップグレードする最小バージョン

現在のメジャー バージョン シーケンス内だけで Firepower ソフトウェアにパッチを適用できます。パッチは累積されるため、常に最新のパッチに直接スキップできます。

***Table 9: Firepower* ソフトウェアをバージョン *6.3.0.x* 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
Firepower Management Center FMC 展開のすべての管理対象デバイス。	6.3.0
FDM を使用した Firepower Threat Defense（すべてのプラットフォーム）	6.3.0
ASDM を使用した ASA FirePOWER	6.3.0

時間テストとディスク容量の要件

Firepower アプライアンスを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。Firepower Management Center を使用して管理

対象デバイスをアップグレードする場合、デバイスアップグレードパッケージに対して、FMC は /Volume パーティションに追加のディスク容量を必要とします。また、アップグレードを実行するための十分な時間を確保してください。

参考のために、社内の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。

時間テストについて

ここで指定した時間の値は、社内のテストに基づいています。

（注） 特定のプラットフォーム/シリーズについてテストされたすべてのアップグレードの最も遅い時間を報告していますが、複数の理由により（以下を参照）、報告された時間よりも、アップグレードにかかる時間が長くなることがあります。

テスト条件

- 展開：値は、Firepower Management Center 展開のテストから取得されています。これは、同様の条件の場合、リモートとローカルで管理されているデバイスの raw アップグレード時間が類似しているためです。
- バージョン：メジャー アップグレードの場合、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。
- 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。
- 仮想設定：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。
- ハイアベイラビリティと拡張性：スタンドアロンデバイスでテストします。

  ハイアベイラビリティ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。 スタック構成の 8000 シリーズ デバイスは同時にアップグレードされ、スタックは、すべてのデバイスのアップグレードが完了するまで、限定的なバージョン混在の状態で動作することに注意してください。これには、スタンドアロンデバイスのアップグレードと比べて大幅に長い時間がかかるということはありません。
- 構成：構成とトラフィック負荷が最小限のアプライアンスでテストします。

  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。

時間はアップグレードのみを対象

値は、各プラットフォーム上で Firepower アップグレードスクリプトの実行にかかる時間のみを表しています。これらには、次の時間は含まれていません。

- 管理対象デバイスへのアップグレードパッケージの転送（アップグレード前かアップグレード中かにかかわらない）。
- 準備状況チェック。
- VDB と SRU の更新。
- 設定の展開。
- リブート（値が別途に報告される場合がある）。

ディスク容量の要件について

容量の見積もりは、すべてのアップグレードについて報告された最大のものです。2020 年前半以降のリリースでは、次のようになります。

- 切り上げなし（1 MB 未満）。
- 次の 1 MB に切り上げ（1 MB ～ 100 MB）。
- 次の 10 MB に切り上げ（100 MB ～ 1 GB）。
- 次の 100 MB に切り上げ（1 GB を超える容量）。

バージョン 6.3.0.5 の時間とディスク容量

Table 10: バージョン *6.3.0.5* の時間とディスク容量

プラットフォーム	ボリュームの容量	必要容量	FMC の容量	6.3.0 からの時間
FMC	4.9 GB	200 MB	—	46 分
FMCv：VMware 6.0	4.5 GB	180 MB	—	41 分
Firepower 2100 シリーズ	2.3 GB	2.3 GB	480 MB	21 分
Firepower 4100 シリーズ	1.6 GB	1.6 GB	280 MB	13 分
Firepower 9300	1.6 GB	1.6 GB	280 MB	17 分
ASA 5500-X シリーズ with FTD	1.7 GB	110 MB	270 MB	26 分
FTDv：VMware 6.0	1.7 GB	110 MB	270 MB	17 分

プラットフォーム	ボリュームの容量	必要容量	FMC の容量	6.3.0 からの時間
Firepower 7000/8000 シリーズ	2.6 GB	210 MB	600 MB	23 分
ASA FirePOWER	3.6 GB	47 MB	540 MB	74 分
NGIPSv：VMware 6.0	2.1 GB	160 MB	440 MB	17 分

バージョン 6.3.0.4 の時間とディスク容量

Table 11: バージョン ***6.3.0.4*** の時間とディスク容量

プラットフォーム	ボリュームの容量	必要容量	FMC の容量	6.3.0 からの時間
FMC	3.4GB	180 MB	—	34 分
FMCv：VMware 6.0	4.4 GB	180 MB	—	38 分
Firepower 2100 シリーズ	2.3 GB	2.3 GB	480 MB	17 分
Firepower 4100 シリーズ	1.6 GB	1.6 GB	280 MB	12 分
Firepower 9300	1.8 GB	1.8 GB	280 MB	12 分
ASA 5500-X シリーズ with FTD	1.7 GB	110 MB	270 MB	23 分
FTDv：VMware 6.0	1.7 GB	110 MB	270 MB	18 分
Firepower 7000/8000 シリーズ	3.3 GB	170 MB	600 MB	21 分
ASA FirePOWER	3.5 GB	31 MB	530 MB	48 分
NGIPSv：VMware 6.0	2.1 GB	160 MB	430 MB	16 分

バージョン 6.3.0.3 の時間とディスク容量

Table 12: バージョン ***6.3.0.3*** の時間とディスク容量

プラットフォーム	ボリュームの容量	必要容量	FMC の容量	6.3.0 からの時間
FMC	3.7 GB	180 MB	—	33 分
FMCv：VMware 6.0	3.2 GB	180 MB	—	24 分
Firepower 2100 シリーズ	1.2 GB	1.2 GB	290 MB	18 分

プラットフォーム	ボリュームの容量	必要容量	FMC の容量	6.3.0 からの時間
Firepower 4100 シリーズ	990 MB	990 MB	99 MB	11 分
Firepower 9300	990 MB	990 MB	99 MB	12 分
ASA 5500-X シリーズ with FTD	620 MB	110 MB	79 MB	18 分
FTDv：VMware 6.0	240 MB	110 MB	79 MB	7 分
Firepower 7000/8000 シリーズ	2.6 GB	170 MB	400 MB	20 分
ASA FirePOWER	2.9 GB	30 MB	340 MB	45 分
NGIPSv：VMware 6.0	1.5 GB	160 MB	250 MB	4 分

バージョン 6.3.0.2 の時間とディスク容量

Table 13: バージョン *6.3.0.2* の時間とディスク容量

プラットフォーム	ボリュームの容量	必要容量	FMC の容量	6.3.0 からの時間
FMC	3.5 GB	180 MB	—	53 分
FMCv：VMware 6.0	3.2 GB	180 MB	—	28 分
Firepower 2100 シリーズ	1.2 GB	1.2 GB	100 MB	17 分
Firepower 4100 シリーズ	970 MB	970 MB	100 MB	12 分
Firepower 9300	970 MB	970 MB	100 MB	11 分
ASA 5500-X シリーズ with FTD	570 MB	110 MB	80 MB	12 分
FTDv：VMware 6.0	600 MB	110 MB	80 MB	10 分
Firepower 7000/8000 シリーズ	[2.5 GB]	170 MB	400 MB	20 分
ASA FirePOWER	3 GB	30 MB	340 MB	45 分
NGIPSv：VMware 6.0	1.5 GB	160 MB	250 MB	10 分

バージョン 6.3.0.1 の時間とディスク容量

Table 14: バージョン *6.3.0.1* の時間とディスク容量

プラットフォーム	ボリュームの容量	必要容量	FMC の容量	6.3.0 からの時間
FMC	3 GB	170 MB	—	31 分
FMCv：VMware 6.0	2.4 GB	170 MB	—	25 分
Firepower 2100 シリーズ	1.2 GB	1.2 GB	290 MB	18 分
Firepower 4100 シリーズ	740 MB	740 MB	100 MB	12 分
Firepower 9300	740 MB	740 MB	100 MB	12 分
ASA 5500-X シリーズ with FTD	400 MB	150 MB	72 MB	17 分
FTDv：VMware 6.0	400 MB	150 MB	72 MB	10 分
Firepower 7000/8000 シリーズ	2.1 GB	170 MB	350 MB	20 分
ASA FirePOWER	2.4 GB	28 MB	270 MB	44 分
NGIPSv：VMware 6.0	1.5 GB	150 MB	350 MB	10 分

トラフィック フロー、検査、およびデバイス動作

アップグレード中に発生するトラフィック フローおよびインスペクションでの潜在的な中断を特定する必要があります。これは、次の場合に発生する可能性があります。

- デバイスが再起動された場合。
- デバイス上でオペレーティング システムまたは仮想ホスティング環境をアップグレードする場合。
- デバイス上で Firepower ソフトウェアをアップグレードするか、パッチをアンインストールする場合。
- アップグレードまたはアンインストール プロセスの一部として設定変更を展開する場合（Snort プロセスが再開します）。

デバイスのタイプ、展開のタイプ（スタンドアロン、ハイ アベイラビリティ、クラスタ化）、およびインターフェイスの設定（パッシブ、IPS、ファイアウォールなど）によって中断の性質が決まります。アップグレードまたはアンインストールは、保守期間中に行うか、中断による展開環境への影響が最も小さい時点で行うことを強く推奨します。

FTD アップグレード時の動作： Firepower 4100/9300 シャーシ

このセクションでは、FTD を搭載した Firepower 4100/9300 シャーシをアップグレードするときのデバイスとトラフィックの動作を説明します。

Firepower 4100/9300 シャーシ：FXOS のアップグレード

シャーシ間クラスタリングまたはハイアベイラビリティペアの構成がある場合でも、各シャーシの FXOS を個別にアップグレードします。アップグレードの実行方法により、FXOS のアップグレード時にデバイスがトラフィックを処理する方法が決定されます。

表 *15 : FXOS* アップグレード中のトラフィックの動作

展開	方法	トラフィックの動作
スタンドアロン	—	ドロップされる
ハイアベイラビリティ	**ベストプラクティス**：スタンバイで FXOS を更新し、アクティブピアを切り替えて新しいスタンバイをアップグレードします。	影響なし
	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。	1 つのピアがオンラインになるまでドロップされる
シャーシ間クラスタ（6.2 以降）	**ベストプラクティス**：少なくとも 1 つのモジュールを常にオンラインにするため、一度に 1 つのシャーシをアップグレードします。	影響なし
	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。	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
シャーシ内クラスタ（Firepower 9300 のみ）	Fail-to-wire 有効：[バイパス：スタンバイ（Bypass: Standby）] または [バイパス：強制（Bypass-Force）]（6.1 以降）	インスペクションなしで転送
	Fail-to-wire 無効：[バイパス：無効（Bypass: Disabled）]（6.1 以降）	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
	fail-to-wire モジュールなし。	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

スタンドアロン FTD デバイス：Firepower ソフトウェアのアップグレード

インターフェイスの設定により、アップグレード中にスタンドアロンデバイスがトラフィックを処理する方法が決定されます。

表 *16 : Firepower* ソフトウェアアップグレード中のトラフィックの動作：スタンドアロン *FTD* デバイス

インターフェイスの設定		トラフィックの動作
ファイアウォールインターフェイス	EtherChannel、冗長、サブインターフェイスを含むルーテッドまたはスイッチド スイッチドインターフェイスは、ブリッジグループまたはトランスペアレントインターフェイスとしても知られています。	ドロップされる
IPS のみのインターフェイス	インラインセット、fail-to-wire が有効：[バイパス：スタンバイ（Bypass: Standby）] または [バイパス：強制（Bypass-Force）]（6.1 以降）	次のいずれかを行います。 • ドロップ（6.1 から 6.2.2.x） • インスペクションなしで転送（6.2.3 以降）
	インラインセット、fail-to-wire が無効：[バイパス：無効（Bypass: Disabled）]（6.1 以降）	ドロップされる
	インラインセット、fail-to-wire モジュールなし	ドロップされる
	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

ハイアベイラビリティペア：FirePOWER ソフトウェアアップグレード

ハイアベイラビリティペアのデバイスの FirePOWER ソフトウェアをアップグレードする間に、トラフィックフローまたはインスペクションが中断されることはありません。継続稼働できるように、一度に 1 つずつアップグレードされます。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。

スタンバイ側の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。アップグレードの完了時には、デバイスの役割は切り替わったままです。アクティブ/スタンバイの役割を維持する場合、アップグレード前に役割を手動で切り替えます。それにより、アップグレードプロセスによって元の役割に切り替わります。

クラスタ：FirePOWER ソフトウェアアップグレード

Firepower Threat Defense クラスタのデバイスで FirePOWER ソフトウェアをアップグレードする間に、トラフィックフローまたはインスペクションが中断されることはありません。継続稼働できるように、一度に1つずつアップグレードされます。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。

スレーブ セキュリティ モジュールを最初にアップグレードして、その後マスターをアップグレードします。アップグレード中、セキュリティモジュールはメンテナンスモードで稼働します。

マスター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。

（注） バージョン6.2.0、6.2.0.1、または6.2.0.2からシャーシ間クラスタをアップグレードすると、各モジュールがクラスタから削除されるときに、トラフィック インスペクションで2～3秒のトラフィック中断が発生します。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、デバイスがトラフィックを処理する方法に応じて異なります。

ハイアベイラビリティとクラスタリング ヒットレス アップグレードの要件

ヒットレスアップグレードの実行には、次の追加要件があります。

フローオフロード：フローオフロード機能でのバグ修正により、FXOSとFTDのいくつかの組み合わせはフローオフロードをサポートしていません。『Cisco Firepower Compatibility Guide』を参照してください。ハイアベイラビリティまたはクラスタ化された展開でヒットレスアップグレードを実行するには、常に互換性のある組み合わせを実行していることを確認する必要があります。

アップグレードパスに FXOS の2.2.2.91、2.3.1.130、またはそれ以降のアップグレード（FXOS 2.4.1. x、2.6.1 などを含む）が含まれている場合、次のパスを使用します。

1. FTD を 6.2.2.2 以降にアップグレードします。
2. FXOS を 2.2.2.91、2.3.1.130、またはそれ以降にアップグレードします。
3. FTD を最終バージョンにアップグレードします。

たとえば、FXOS 2.2.2.17/FTD 6.2.2.0 を実行していて、FXOS 2.6.1/FTD 6.4.0 にアップグレードする場合は、次を実行できます。

1. FTD を 6.2.2.5 にアップグレードします。
2. FXOS を 2.6.1 にアップグレードします。
3. FTD を 6.4.0 にアップグレードします。

バージョン 6.1.0 へのアップグレード：FTD ハイアベイラビリティペアのバージョン 6.1.0 へのヒットレスアップグレードを実行するには、プレインストールパッケージが必要です。詳細については、『Firepower System Release Notes Version 6.1.0 Preinstallation Package』を参照してください。

展開時のトラフィックの動作

アップグレード プロセス中には、設定を複数回展開します。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。詳細については、『Firepower Management Center Configuration Guide』の「Configurations that Restart the Snort Process when Deployed or Activated」を参照してください。

展開する際にリソースを要求すると、いくつかのパケットがインスペクションなしでドロップされることがあります。また、Snort プロセスを再起動すると、HA/スケーラビリティ用に設定されたものを含め、すべての Firepower デバイスでトラフィック インスペクションが中断されます。インターフェイス設定により、中断中にインスペクションせずにトラフィックをドロップするか受け渡すかが決定されます。

表 *17 : FTD* 展開時のトラフィックの動作

インターフェイスの設定		トラフィックの動作
ファイアウォール インターフェイス	EtherChannel、冗長、サブインターフェイスを含むルーテッドまたはスイッチド スイッチドインターフェイスは、ブリッジグループまたはトランスペアレントインターフェイスとしても知られています。	ドロップされる

インターフェイスの設定		トラフィックの動作
IPS のみのインターフェイス	インラインセット、[フェールセーフ（Failsafe）]が有効または無効（6.0.1 ～ 6.1.0.x）	インスペクションなしで転送 [フェールセーフ（Failsafe）] が無効で、Snortがビジーでもダウンしていない場合、いくつかのパケットがドロップすることがあります。
	インラインセット、[Snortフェールオープン：ダウン（Snort Fail Open: Down）]：無効（6.2 以降）	ドロップされる
	インラインセット、[Snortフェールオープン：ダウン（Snort Fail Open: Down）]：有効（6.2+）	インスペクションなしで転送
	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

FTD アップグレード時の動作：その他のデバイス

このセクションでは、Firepower 1000/2100 シリーズ、ASA 5500-X シリーズ、ISA 3000、および FTDv で Firepower Threat Defense をアップグレードするときのデバイスとトラフィックの動作を説明します。

スタンドアロン FTD デバイス：Firepower ソフトウェアのアップグレード

インターフェイスの設定により、アップグレード中にスタンドアロンデバイスがトラフィックを処理する方法が決定されます。

表 *18 : Firepower* ソフトウェアアップグレード中のトラフィックの動作：スタンドアロン *FTD* デバイス

インターフェイスの設定		トラフィックの動作
ファイアウォールインターフェイス	EtherChannel、冗長、サブインターフェイスを含むルーテッドまたはスイッチド スイッチドインターフェイスは、ブリッジグループまたはトランスペアレントインターフェイスとしても知られています。	ドロップされる

インターフェイスの設定		トラフィックの動作
IPS のみのインターフェイス	インラインセット、fail-to-wire が有効：[バイパス：スタンバイ（Bypass: Standby）] または [バイパス：強制（Bypass-Force）]（6.1 以降）	次のいずれかを行います。 • ドロップ（6.1 から 6.2.2.x） • インスペクションなしで転送（6.2.3 以降）
	インラインセット、fail-to-wire が無効：[バイパス：無効（Bypass: Disabled）]（6.1 以降）	ドロップされる
	インラインセット、fail-to-wire モジュールなし	ドロップされる
	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

ハイアベイラビリティペア：FirePOWER ソフトウェアアップグレード

ハイアベイラビリティペアのデバイスの FirePOWER ソフトウェアをアップグレードする間に、トラフィックフローまたはインスペクションが中断されることはありません。継続稼働できるように、一度に 1 つずつアップグレードされます。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。

スタンバイ側の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。アップグレードの完了時には、デバイスの役割は切り替わったままです。アクティブ/スタンバイの役割を維持する場合、アップグレード前に役割を手動で切り替えます。それにより、アップグレードプロセスによって元の役割に切り替わります。

展開時のトラフィックの動作

アップグレード プロセス中には、設定を複数回展開します。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。詳細については、『Firepower Management Center Configuration Guide』の「Configurations that Restart the Snort Process when Deployed or Activated」を参照してください。

展開する際にリソースを要求すると、いくつかのパケットがインスペクションなしでドロップされることがあります。また、Snort プロセスを再起動すると、HA/スケーラビリティ用に設定されたものを含め、すべての Firepower デバイスでトラフィック インスペクションが中断されます。インターフェイス設定により、中断中にインスペクションせずにトラフィックをドロップするか受け渡すかが決定されます。

表 *19 : FTD* 展開時のトラフィックの動作

インターフェイスの設定		トラフィックの動作
ファイアウォールインターフェイス	EtherChannel、冗長、サブインターフェイスを含むルーテッドまたはスイッチド スイッチドインターフェイスは、ブリッジグループまたはトランスペアレントインターフェイスとしても知られています。	ドロップされる
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（6.0.1 ～ 6.1.0.x）	インスペクションなしで転送 [フェールセーフ（Failsafe）] が無効で、Snortがビジーでもダウンしていない場合、いくつかのパケットがドロップすることがあります。
	インラインセット、[Snortフェールオープン：ダウン（Snort Fail Open: Down）]：無効（6.2 以降）	ドロップされる
	インラインセット、[Snortフェールオープン：ダウン（Snort Fail Open: Down）]：有効（6.2+）	インスペクションなしで転送
	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

FirePOWER 7000/8000 シリーズのアップグレード時の動作

次のセクションでは、Firepower 7000/8000 シリーズデバイスをアップグレードする際のデバイスおよびトラフィックの動作について説明します。

スタンドアロン 7000/8000 シリーズ：Firepower ソフトウェアのアップグレード

インターフェイスの設定により、アップグレード中にスタンドアロンデバイスがトラフィックを処理する方法が決定されます。

表 *20 :* アップグレード中のトラフィックの動作：スタンドアロン *7000/8000* シリーズ

インターフェイスの設定	トラフィックの動作
インライン、ハードウェア バイパスが有効（[バイパスモード：バイパス（Bypass Mode: Bypass）]）	インスペクションなしで転送。ただし、トラフィックは、次の 2 つのポイントで一時的に中断します。 • アップグレード プロセスの開始時に、リンクがダウンしてから復旧（フラップ）し、ネットワーク カードがハードウェア バイパスに切り替わるとき。 • アップグレードが完了した後、リンクが復旧し、ネットワーク カードがバイパスから切り替わるとき。インスペクションはエンドポイントの再接続後に再開され、デバイス インターフェイスとのリンクを再確立します。
インライン、ハードウェア バイパス モジュールなし、またはハードウェア バイパスが無効（[バイパスモード：非バイパス（Bypass Mode: Non-Bypass）]）	ドロップされる
インライン、タップ モード	パケットをただちに出力、コピーへのインスペクションなし
パッシブ	中断なし、インスペクションなし
ルーテッド、スイッチド	ドロップされる

7000/8000 シリーズ ハイ アベイラビリティ ペア：Firepower ソフトウェアのアップグレード

ハイ アベイラビリティ ペアのデバイス（またはデバイス スタック）をアップグレードする間に、トラフィック フローまたはインスペクションが中断されることはありません。継続稼働できるように、一度に1つずつアップグレードされます。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。

最初にアップグレードするピアは、展開によって異なります。

- ルーテッドまたはスイッチド：最初にスタンバイが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。アップグレードの完了時には、デバイスの役割は切り替わったままです。アクティブ/スタンバイの役割を維持する場合、アップグレード前に役割を手動で切り替えます。それにより、アップグレードプロセスによって元の役割に切り替わります。
- アクセス制御のみ：最初にアクティブがアップグレードされます。アップグレードの完了時に、アクティブとスタンバイの以前の役割がデバイスで維持されます。

8000 シリーズ スタック：FirePOWER ソフトウェア アップグレード

8000 シリーズ スタックでは、デバイスは同時にアップグレードされます。プライマリ デバイスがアップグレードを完了してスタックが動作を再開するまで、トラフィックはスタックがスタンドアロンデバイスであったかのように影響を受けます。すべてのデバイスがアップグレードを完了するまで、スタックは、制限付きの混合バージョンの状態で動作します。

展開時のトラフィックの動作

アップグレード プロセス中には、設定を複数回展開します。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。詳細については、『Firepower Management Center Configuration Guide』の「Configurations that Restart the Snort Process when Deployed or Activated」を参照してください。

展開する際にリソースを要求すると、いくつかのパケットがインスペクションなしでドロップされることがあります。また、Snortプロセスを再起動すると、HA/スケーラビリティ用に設定されたものを含め、すべての Firepower デバイスでトラフィック インスペクションが中断されます。インターフェイス設定により、中断中にインスペクションせずにトラフィックをドロップするか受け渡すかが決定されます。

表 *21 :* 展開時のトラフィックの動作：*7000/8000* シリーズ

インターフェイスの設定	トラフィックの動作
インライン、[フェールセーフ（Failsafe）]が有効または無効	インスペクションなしで転送 [フェールセーフ（Failsafe）]が無効で、Snort がビジーでもダウンしていない場合、いくつかのパケットがドロップすることがあります。
インライン、タップ モード	すぐにパケットを出力し、バイパス Snort をコピーする
パッシブ	中断なし、インスペクションなし
ルーテッド、スイッチド	ドロップされる

ASA FirePOWER アップグレード時の動作

Snortプロセスを再起動する特定の設定を展開する場合を含め、モジュールが FirePOWER ソフトウェア アップグレード中にトラフィックを処理する方法を決定する、ASA FirePOWER モジュールへのトラフィック リダイレクトに関する ASA サービス ポリシーです。

表 *22 : ASA FirePOWER* アップグレード中のトラフィックの動作

トラフィック リダイレクト ポリシー	トラフィックの動作
フェール オープン（**sfr fail-open**）	インスペクションなしで転送
フェール クローズ（**sfr fail-close**）	ドロップされる

トラフィック リダイレクト ポリシー	トラフィックの動作
モニタのみ（**sfr {fail-close}|{fail-open} monitor-only**）	パケットをただちに出力、コピーへのインスペクションなし

ASA FirePOWER 展開時のトラフィックの動作

Snort プロセスが再起動している間のトラフィックの動作は、ASA FirePOWER モジュールをアップグレードする場合と同じです。

アップグレード プロセス中には、設定を複数回展開します。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。詳細については、『Firepower Management Center Configuration Guide』の「Configurations that Restart the Snort Process when Deployed or Activated」を参照してください。

展開する際にリソースを要求すると、いくつかのパケットがインスペクションなしでドロップされることがあります。 さらに、Snort プロセスを再起動すると、トラフィック インスペクションが中断されます。サービスポリシーにより、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通過するかが決定されます。

NGIPSv アップグレード時の動作

このセクションでは、NGIPSvをアップグレードするときのデバイスとトラフィックの動作を説明します。

Firepower ソフトウェア アップグレード

インターフェイスの設定により、アップグレード中にNGIPSv がトラフィックを処理する方法が決定されます。

表 *23 : NGIPSv* アップグレード中のトラフィックの動作

インターフェイスの設定	トラフィックの動作
インライン	ドロップされる
インライン、タップ モード	パケットをただちに出力、コピーへのインスペクションなし
パッシブ	中断なし、インスペクションなし

展開時のトラフィックの動作

アップグレード プロセス中には、設定を複数回展開します。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。詳細については、

『Firepower Management Center Configuration Guide』の「Configurations that Restart the Snort Process when Deployed or Activated」を参照してください。

展開する際にリソースを要求すると、いくつかのパケットがインスペクションなしでドロップされることがあります。さらに、Snortプロセスを再起動すると、トラフィックインスペクションが中断されます。インターフェイス設定により、中断中にインスペクションせずにトラフィックをドロップするか受け渡すかが決定されます。

表 *24 : NGIPSv* 展開時のトラフィックの動作

インターフェイスの設定	トラフィックの動作
インライン、[フェールセーフ（Failsafe）] が有効または無効	インスペクションなしで転送 [フェールセーフ（Failsafe）] が無効で、Snort がビジーでもダウンしていない場合、いくつかのパケットがドロップすることがあります。
インライン、タップ モード	すぐにパケットを出力し、バイパス Snort をコピーする
パッシブ	中断なし、インスペクションなし

アップグレード手順

リリース ノートにはアップグレード手順は含まれていません。これらのリリース ノートに記載されているガイドラインと警告を読んだ後、次のいずれかを参照してください。

- Cisco Firepower Management Center Upgrade Guide：管理対象デバイスや付随するオペレーティング システムを含む、FMC 展開のアップグレード
- Cisco ASA Upgrade Guide：ASDM を使用した ASA FirePOWER モジュールのアップグレード
- Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager：FDM を使用した FTD のアップグレード

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。

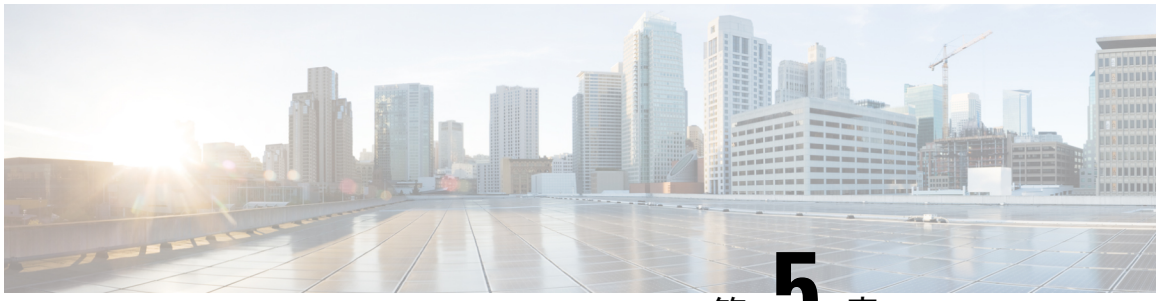
- FMCv を含む Firepower Management Center：https://www.cisco.com/go/firepower-software
- Firepower Threat Defense（ISA 3000）：https://www.cisco.com/go/isa3000-software
- Firepower Threat Defense（FTDv を含む他のすべてのモデル）：https://www.cisco.com/go/ftd-software

- FirePOWER 7000 シリーズ： https://www.cisco.com/go/7000series-software
- FirePOWER 8000 シリーズ： https://www.cisco.com/go/8000series-software
- ASA with FirePOWER Services（ASA 5500-X シリーズ）： https://www.cisco.com/go/asa-firepower-sw
- ASA with FirePOWER Services（ISA 3000）： https://www.cisco.com/go/isa3000-software
- NGIPSv： https://www.cisco.com/go/ngipsv-software

署名付きの（.tar）パッケージは解凍しないでください。

Table 25: のアップグレード パッケージ バージョン ***6.3.0.x***

プラットフォーム	パッケージ
FMC/FMCv	Cisco_Firepower_Mgmt_Center_Patch-*version-build*.sh.REL.tar
Firepower 2100 シリーズ	Cisco_FTD_SSP_FP2K_Patch-*version-build*.sh.REL.tar
Firepower 4100/9300 シャーシ	Cisco_FTD_SSP_Patch-*version-build*.sh.REL.tar
FTD を搭載した ASA 5500-X シリーズ FTD を搭載した ISA 3000 Firepower Threat Defense 仮想	Cisco_FTD_Patch-*version-build*.sh.REL.tar
Firepower 7000/8000 シリーズ	Cisco_Firepower_NGIPS_Appliance_Patch-*version-build*.sh.REL.tar
ASA FirePOWER	Cisco_Network_Sensor_Patch-*version-build*.sh.REL.tar
NGIPSv	Cisco_Firepower_NGIPS_Virtual_Patch-*version-build*.sh.REL.tar



第 5 章

バージョン 6.3.0.x のパッチのアンインストール

Firepower のパッチは次の場所からアンインストールできます。

- FMC とその管理対象デバイス
- ASDM によって管理されている ASA FirePOWER モジュール

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がアプライアンスで実行されます。

（注） FDM によって管理されている FTD 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」。また、任意のアプライアンスから Firepower ソフトウェアのメジャー バージョンをアンインストールすることもできません。このような場合は、新しくインストールする必要があります。

詳細については、以下を参照してください。

- アンインストールに関する注意事項と制約事項 （37 ページ）
- HA/スケーラビリティ環境でのアンインストール順序 （40 ページ）
- アンインストールの手順 （43 ページ）
- パッケージのアンインストール, on page 49

アンインストールに関する注意事項と制約事項

これらの重要なガイドラインと制限事項は、アンインストールに適用されます。

パッチのアンインストールがサポートされていることを確認します

特定のパッチをアンインストールすると、次のような問題が Firepower アプライアンスで発生する可能性があります。

- 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 Firepower 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 セキュリティ認定準拠が有効な場合に FSIC が失敗すると、Firepower 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り、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。

このような場合に、前のパッチに戻す必要があるときは、再イメージ化してからアップグレードすることをお勧めします。

次の表に、アンインストールしてはならない状況を示します。

表 *26* : アンインストール時に後続の問題が発生したバージョン *6.3.0.x* のパッチ

プラットフォーム	アンインストール元	アップグレード元が次の場合
任意	6.3.0.5+	6.3.0 ～ 6.3.0.4

シェルを使用して先にデバイスからアンインストールする

FMC の展開では、先に管理対象デバイスからパッチをアンインストールします。FMC では管理対象デバイスよりも後のバージョンを実行することを推奨します。

デバイス パッチをアンインストールするには、エキスパート モードとも呼ばれる Linux シェルを使用する必要があります。これは、デバイスから「個別に」、かつ「ローカルに」アンインストールすることを意味します。つまり、次のようになります。

- クラスタ化された、スタック構成の、またはハイ アベイラビリティ（HA）の Firepower デバイスから、あるいは FirePOWER Services デバイスのあるクラスタ化 ASA またはフェールオーバー ASA から、パッチを一括でアンインストールすることはできません。中断を最小限に抑えるアンインストール順序を計画するには、「HA/スケーラビリティ環境でのアンインストール順序 （40 ページ）」を参照してください。
- FMC、ASDM、または FDM を使用してデバイスからパッチをアンインストールすることも、7000/8000 シリーズ デバイスのローカル Web インターフェイスを使用することもできません。
- FMC のユーザ アカウントを使用して、いずれかの管理対象デバイスにログインして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。Firepower アプライアンスでは独自のユーザ アカウントを維持しています。
- デバイスの `admin` ユーザとして、または CLI 設定アクセス権を持つ別のローカル ユーザとして、デバイス シェルにアクセスできる必要があります。シェル アクセスを無効にした場合、デバイス パッチをアンインストールすることはできません。デバイスのロックダウンを元に戻すには、Cisco TAC にご連絡ください。

デバイスより後に FMC からアンインストールする

管理対象デバイスからアンインストールした後に、FMC からパッチをアンインストールします。アップグレードと同様に、ハイアベイラビリティ FMC から一度に1つずつアンインストールする必要があります。「HA/スケーラビリティ環境でのアンインストール順序 （40 ページ）」を参照してください。

FMC パッチのアンインストールには FMC Web インターフェイスを使用することをお勧めします。管理者アクセス権が必要になります。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` ユーザまたはシェルアクセス権を持つ外部ユーザ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、FMC のロックダウンを元に戻すために Cisco TAC にご連絡ください。

NTP 同期の確認

アンインストールする前に、時刻の提供に使用している NTP サーバと Firepower アプライアンスが同期していることを確認します。同期されていないと、アンインストールが失敗する可能性があります。FMC 展開では、時刻のずれが 10 秒を超えている場合、[時刻同期化ステータス（Time Synchronization Status）] ヘルスモジュールからアラートが発行されますが、手動で確認する必要もあります。

時刻を確認するには、次の手順を実行します。

- FMC：[システム（System）] > [設定（Configuration）] > [時刻（Time）] を選択します。
- デバイス：**show time** CLI コマンドを使用します。

アプライアンス アクセス

Firepower デバイスは、（インターフェイス設定に応じて）アンインストール中、またはアンインストールが失敗した場合に、トラフィックを渡すことを停止できます。Firepower デバイスからパッチをアンインストールする前に、ユーザ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。Firepower Management Center 展開では、デバイスを経由せずに FMC 管理インターフェイスにアクセスできる必要もあります。

ASA FirePOWER デバイスでの ASA REST API の無効化

ASA FirePOWER パッチをアンインストールする前に、ASA REST API を無効にしていることを確認してください。無効でない場合、アンインストールが失敗する可能性があります。ASA CLI から：`no rest api agent`。アンインストール後に再度有効にすることができます：`rest-api agent`。

無応答のアンインストール

アンインストールしているアプライアンスとの間での変更の展開、またはアンインストールしているアプライアンスの手動での再起動やシャットダウンは行わないでください。進行中のアンインストールを再開しないでください。 アンインストール プロセスが停止しているように見える場合がありますが、これは想定内の動作です。ア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。

アンインストールに失敗した場合、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。このため、再イメージ化の前にイベント データと設定データを外部の場所にバックアップしておくことを強くお勧めします。

トラフィック フロー、検査、およびデバイス動作

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。アップグレードは、保守期間中に行うか、中断による展開環境への影響が最も小さい時点で行うことを強くお勧めします。詳細については、トラフィック フロー、検査、およびデバイス動作 （24 ページ）を参照してください。

HA/スケーラビリティ環境でのアンインストール順序

Firepower アプライアンスからのパッチのアンインストールは、アプライアンスをユニットとしてアップグレードした場合であっても、個別に行います。特にハイ アベイラビリティ（HA）およびスケーラビリティの展開環境では、中断を最小限に抑えるアンインストール順序を計画する必要があります。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。次の表に、HA/スケーラビリティ環境でのアンインストール順序の概要を示します。

通常は次のことに注意してください。

- 先にセカンダリ/スタンバイ/スレーブ ユニットからアンインストールし、その次にプライマリ/アクティブ/マスターからアンインストールします。
- 一度に 1 つずつアンインストールします。次のユニットに移る前に、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 *27 : HA* 内の *FMC* の場合におけるアンインストール順序

FMC の環境	アンインストール順序
FMC ハイ 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、FMC のピアから一度に 1 つずつアンインストールします。ペアが 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。 **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）。 **2.** スタンバイからアンインストールします。 **3.** アクティブからアンインストールします。 **4.** 同期を再開します（スプリットブレインから抜けます）。

表 *28 : HA* またはクラスタ内の *FTD* デバイスの場合におけるアンインストール順序

FTD の環境	アンインストール順序
FTD ハイ 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 FTD 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。 **1.** ハイ アベイラビリティを解除します。 **2.** 以前のスタンバイからアンインストールします。 **3.** 以前のアクティブからアンインストールします。 **4.** ハイ アベイラビリティを再確立します。
FTD クラスタ	一度に 1 つのユニットからアンインストールし、マスター 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。 **1.** スレーブ 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。 **2.** スレーブ モジュールの 1 つを新しいマスター モジュールに設定します。 **3.** 以前のマスターからアンインストールします。

表 *29 : HA* またはスタック内の *7000/8000* シリーズ デバイスの場合におけるアンインストール順序

7000/8000 シリーズの環境	アンインストール順序
7000/8000 シリーズ ハイ アベイラビリティ	常にスタンバイからアンインストールします。HA ペア内の 7000/8000 シリーズ デバイスは、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。 **1.** スタンバイからアンインストールします。 **2.** ロールを切り替えます。 **3.** 新しいスタンバイからアンインストールします。
8000 シリーズ スタック	スタック内のすべてのデバイスから同時にアンインストールします。すべてのデバイスからパッチをアンインストールするまで、スタックは制限付きの混合バージョンの状態で動作します。

表 *30 : ASA* フェール オーバーペア/クラスタ内の *ASA with FirePOWER Services* デバイスの場合におけるアンインストール順序

ASA 展開	アンインストール順序
ASA FirePOWER が有効な ASA アクティブ/スタンバイ フェールオーバー ペア	常にスタンバイからアンインストールします。 1. スタンバイ ASA デバイスの ASA FirePOWER モジュールからアンインストールします。 2. フェールオーバーします。 3. 新しいスタンバイ ASA デバイスの ASA FirePOWER モジュールからアンインストールします。
ASA FirePOWER が有効な ASA アクティブ/アクティブ フェールオーバー ペア	アンインストールしないユニットの両方のフェールオーバー グループをアクティブにします。 1. プライマリ ASA デバイスの両方のフェールオーバー グループをアクティブにします。 2. セカンダリ ASA デバイスの ASA FirePOWER モジュールからアンインストールします。 3. セカンダリ ASA デバイスの両方のフェールオーバー グループをアクティブにします。 4. プライマリ ASA デバイスの ASA FirePOWER モジュールからアンインストールします。
ASA FirePOWER が有効な ASA クラスタ	アンインストールの前に、各ユニットでクラスタリングを無効にします。一度に 1 つのユニットからアンインストールし、マスターユニットを最後に残します。 1. スレーブ ユニットでクラスタリングを無効にします。 2. そのユニットの ASA FirePOWER モジュールからアンインストールします。 3. クラスタリングを再び有効にします。ユニットが再びクラスタに参加するのを待ちます。 4. 各スレーブユニットに対して手順を繰り返します。 5. マスターユニットでクラスタリングを無効にします。新しいマスターが引き継がれるまで待ちます。 6. 以前のマスターの ASA FirePOWER モジュールからアンインストールします。 7. クラスタリングを再び有効にします。

アンインストールの手順

ここでは、対象となるアプライアンスから Firepower パッチをアンインストールする方法について説明します。

スタンドアロン FMC からのアンインストール

次の手順を実行して、Firepower Management Center Virtual を含むスタンドアロンの Firepower Management Center からパッチをアンインストールします。

始める前に

管理対象デバイスからパッチをアンインストールします。FMC では管理対象デバイスよりも後のバージョンを実行することを推奨します。

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 事前チェックを実行します。

- 正常性のチェック：FMC のメッセージ センターを使用します（メニュー バーの [システムステータス（System Status）] アイコンをクリックします）。導入環境内のアプライアンスが正常に通信していること、およびヘルス モニタによって報告された問題がないことを確認します。
- タスクの実行：また、メッセージ センターで、必須タスクが完了していることを確認します。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 3 **[システム（System）] > [更新（Updates）]** を選択します。

ステップ 4 FMC のアンインストール 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、FMC を選択します。

正しいアンインストール パッケージがない場合は、Cisco TAC にお問い合わせください。

ステップ 5 [インストール（Install）] をクリックして、アンインストールを開始します。

アンインストールすることを確認し、FMC を再起動します。

ステップ 6 ログアウトするまで、メッセージ センターで進行状況を確認します。

パッチのアンインストール中は、設定の変更やデバイスへの展開をしないでください。メッセージ センターに進行状況が数分間表示されない場合や、アンインストールの失敗が示された場合でも、アンインストールを再開したり、FMC を再起動したりしないでください。代わりに、Cisco TAC にお問い合わせください。

ステップ 7 パッチをアンインストールして FMC が再起動したら、再び FMC にログインします。

ステップ 8 成功したことを確認します。

[ヘルプ（Help）] > **[バージョン情報（About）]** を選択し、現在のソフトウェア バージョン情報を表示します。

ステップ 9 メッセージ センターを使用して、導入環境に問題がないことを再度確認します。

ステップ 10 構成を再展開します。

ハイ アベイラビリティ FMC からのアンインストール

次の手順を実行して、ハイ アベイラビリティ ペアの Firepower Management Center からパッチをアンインストールします。

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。スタンバイの FMC 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。ペアが 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。

始める前に

管理対象デバイスからパッチをアンインストールします。FMC では管理対象デバイスよりも後のバージョンを実行することを推奨します。

ステップ 1 アクティブな FMC 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 同期を一時停止する前に、メッセージ センターを使用して導入環境に問題がないことを確認します。

FMC メニュー バーで、[システム ステータス（System Status）] アイコンをクリックして、メッセージ センターを表示します。導入環境内のアプライアンスが正常に通信していること、およびヘルス モニタによって報告された問題がないことを確認します。

ステップ 3 同期を一時停止します。

a) **[システム（System）]** > **[統合（Integration）]** を選択します。

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 4 FMC 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 FMC からのアンインストール （43 ページ）」の手順に従います。ただし、初期の展開は省略し、各 FMC 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、それぞれの FMC で以下の手順を実行します。

a) 事前チェック（ヘルス、実行中のタスク）を実行します。

b) **[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。
c) 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。
d) アンインストールが成功したことを確認します。

ペアが 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。

ステップ 5 アクティブ ピアにする FMC 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 FMC 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 6 メッセージ センターを使用して、導入環境に問題がないことを再度確認します。

ステップ 7 構成を再展開します。

任意のデバイスからのアンインストール（FMC マネージド）

次の手順を実行して、Firepower Management Center 環境内の「1 台」の管理対象デバイスからパッチをアンインストールします。これには、物理および仮想デバイス、セキュリティ モジュール、および ASA FirePOWER モジュールが含まれます。

始める前に

- 特に HA/スケーラビリティの環境において、正しいデバイスからアンインストールしようとしていることを確認してください。「HA/スケーラビリティ環境でのアンインストール順序 （40 ページ）」を参照してください。
- ASA FirePOWER モジュールの場合は、ASA REST API を無効にしていることを確認してください。ASA CLI から：`no rest api agent`。アンインストール後に再度有効にすることができます：`rest-api agent`。

ステップ 1 デバイスの設定が古い場合は、この時点で FMC 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。

例外：混合バージョンのスタック、クラスタ、または HA ペアには展開しないでください。HA/スケーラビリティ環境では、最初のデバイスからアンインストールする前に展開しますが、すべての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。

ステップ 2 事前チェックを実行します。

- 正常性のチェック：FMC のメッセージ センターを使用します（メニュー バーの [システム ステータス（System Status）] アイコンをクリックします）。導入環境内のアプライアンスが正常に通信していること、およびヘルス モニタによって報告された問題がないことを確認します。

- タスクの実行：また、メッセージセンターで、必須タスクが完了していることを確認します。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 3 デバイスの Firepower CLI にアクセスします。`admin` として、または設定アクセス権を持つ別の Firepower CLI ユーザ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。 ASA 5585-X シリーズ デバイスは専用の ASA FirePOWER コンソール ポートを備えています。

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、Firepower 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 2100 シリーズ	`connect ftd`
Firepower 4100/9300 シャーシ	`connect module` *slot_number* `console`、次に `connect ftd`（最初のログインのみ）
ASA FirePOWER（ASA 5585-X シリーズを除く）	`session sfr`

ステップ 4 Firepower CLI プロンプトで、`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 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/uninstall_package_name
```

パッケージ名はプラットフォームによって異なります。「パッケージのアンインストール（49ページ）」を参照してください。 署名付きの（.tar）パッケージは解凍しないでください。

アンインストールをコンソールから実行している場合を除き、`--detach` オプションを使用して、ユーザ 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が停止しないようにします。これを行わないと、アンインストールはユーザ シェルの子プロセスとして実行されます。接続が終了した場合は、プロセスが強制終了し、チェックが中断してアプライアンスが不安定な状態のままになることがあります。

注意 システムから、アンインストールの確認メッセージが表示さ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。

ステップ 6 アンインストールをモニタします。

アンインストールを解除しなければ、コンソールまたは端末に進行状況が表示されます。解除した場合は、`tail` または `tailf` を使用してログを表示できます。

- FTD デバイス：`tail /ngfw/var/log/sf/update.status`
- その他のすべてのデバイス：`tail /var/log/sf/update.status`

ステップ 7 成功したことを確認します。

パッチをアンインストールしてデバイスを再起動した後、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。FMC 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 メッセージ センターを使用して、導入環境に問題がないことを再度確認します。

ステップ 9 構成を再展開します。

例外：HA/スケーラビリティ環境では、混合バージョンのスタック、クラスタ、または HA ペアには展開しないでください。展開は、すべてのメンバーについてこの手順を繰り返した後にのみ行います。

次のタスク

- HA/スケーラビリティ環境の場合は、各デバイスについて計画した順序でこの手順を繰り返します。その後、最終的な調整を行います。たとえば、FTD HA 環境では、両方のピアからアンインストールした後に HA を再確立します。
- ASA FirePOWER モジュールでは、先に ASA REST API を無効にしていた場合は再度有効にします。ASA CLI から、`rest-api agent` を実行します。

ASA FirePOWER からのアンインストール（ASDM マネージド）

次の手順を実行して、ローカル管理されている ASA FirePOWER モジュールからパッチをアンインストールします。FMC を使用して ASA FirePOWER を管理している場合は、「任意のデバイスからのアンインストール（FMC マネージド） （45 ページ）」を参照してください。

始める前に

- 特に ASA のフェールオーバー/クラスタ環境において、正しいデバイスからアンインストールしようとしていることを確認してください。「HA/スケーラビリティ環境でのアンインストール順序 （40 ページ）」を参照してください。
- ASA REST API が無効になっていることを確認します。ASA CLI から：`no rest api agent`。アンインストール後に再度有効にすることができます：`rest-api agent`。

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

アンインストールする前に展開すると、失敗する可能性が減少します。

ステップ 2 事前チェックを実行します。

- システム ステータス：**[モニタリング（Monitoring）]** > **[ASA FirePOWER のモニタリング（ASA FirePOWER Monitoring）]** > **[統計情報（Statistics）]** を選択し、すべてが想定どおりであることを確認します。
- 実行中のタスク：**[モニタリング（Monitoring）]** > **[ASA FirePOWER のモニタリング（ASA FirePOWER Monitoring）]** > **[タスク（Task）]** を選択し、必須タスクが完了していることを確認します。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 3 ASA FirePOWER モジュールの Firepower CLI にアクセスします。`admin` として、または設定アクセス権を持つ別の Firepower CLI ユーザとしてログインします。

モジュールの管理インターフェイスに SSH 接続するか（ホスト名または IP アドレス）、コンソールを使用できます。コンソールを使用する場合、ASA 5585-X シリーズ デバイスは専用の ASA FirePOWER コンソール ポートを備えています。他の ASA モデルでは、コンソール ポートはデフォルトで ASA CLI に設定されており、Firepower CLI にアクセスするには `session sfr` コマンドを使用する必要があります。

ステップ 4 Firepower CLI プロンプトで、`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 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/Cisco_Network_Sensor_Patch_Uninstaller-version-build.sh.REL.tar
```

署名付きの（.tar）パッケージは解凍しないでください。

アンインストールをコンソールから実行している場合を除き、`--detach` オプションを使用して、ユーザ 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が停止しないようにします。これを行わないと、アンインストールはユーザ シェルの子プロセスとして実行されます。接続が終了した場合は、プロセスが強制終了し、チェックが中断してアプライアンスが不安定な状態のままになることがあります。

注意 システムから、アンインストールの確認メッセージが表示さ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。

ステップ 6 アンインストールをモニタします。

アンインストールを解除しなければ、コンソールまたは端末に進行状況が表示されます。解除した場合は、`tail` または `tailf` を使用してログを表示できます。

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

パッチのアンインストール中は、デバイスに設定を展開しないでください。メッセージセンターに進行状況が数分間表示されない場合や、アンインストールの失敗が示された場合でも、アンインストールを再開したり、デバイスを再起動したりしないでください。代わりに、Cisco TAC にお問い合わせください。

ステップ 7 成功したことを確認します。

パッチをアンインストールしてモジュールを再起動した後、モジュールのソフトウェア バージョンが正しいことを確認します。**[設定（Configuration）] > [ASA FirePOWER の設定（ASA FirePOWER Configuration）] > [デバイス管理（Device Management）] > [デバイス（Device）]** を選択します。

ステップ 8 構成を再展開します。

次のタスク

- ASA フェールオーバー/クラスタ環境の場合は、各デバイスについて計画した順序でこの手順を繰り返します。
- ASA FirePOWER モジュールでは、先に ASA REST API を無効にしていた場合は再度有効にします。ASA CLI から、`rest-api agent` を実行します。

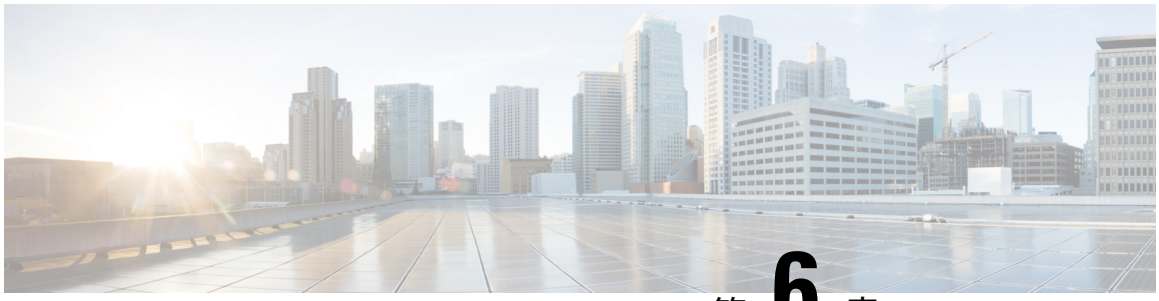
パッケージのアンインストール

Firepower アプライアン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ーがアップグレード ディレクトリに自動的に作成されます。

- `/ngfw/var/sf/updates`（FTD デバイスの場合）
- `/var/sf/updates`（FMC および他のすべてのデバイス（7000/8000 シリーズ、ASA FirePOWER、NGIPSv）の場合）

パッケージがアップグレード ディレクトリにない場合（手動で削除した場合など）は、Cisco TAC にお問い合わせください。 署名付きの（.tar）パッケージは解凍しないでください。

プラットフォーム	パッケージ
FMC/FMCv	Cisco_Firepower_Mgmt_Center_Patch_Uninstaller-*version-build*.sh.REL.tar
Firepower 2100 シリーズ	Cisco_FTD_SSP_FP2K_Patch_Uninstaller-*version-build*.sh.REL.tar
Firepower 4100/9300 シャーシ	Cisco_FTD_SSP_Patch_Uninstaller-*version-build*.sh.REL.tar
FTD を搭載した ASA 5500-X シリーズ FTD を搭載した ISA 3000 FTDv	Cisco_FTD_Patch_Uninstaller-*version-build*.sh.REL.tar
Firepower 7000/8000 シリーズ	Cisco_Firepower_NGIPS_Appliance_Patch_Uninstaller-*version-build*.sh.REL.tar
NGIPSv	Cisco_Firepower_NGIPS_Virtual_Patch_Uninstaller-*version-build*.sh.REL.tar
ASA FirePOWER	Cisco_Network_Sensor_Patch_Uninstaller-*version-build*.sh.REL.tar



第 6 章

新規インストール バージョン 6.3.0

Firepower アプライアンスをアップグレードできない（または必要なアップグレード パスを実行したくない）場合は、Firepower のメジャー リリースを新規インストールできます。特定のパッチを実行するには、バージョン 6.3.0 をインストールしてからアップグレードしてください。

新規インストールの決定

次の表を使用して、新規インストール（再イメージ化とも呼ばれます）する必要がある場合のシナリオを特定します。これらのすべてのシナリオ（ローカルとリモート間のデバイス管理の切り替えを含む）では、デバイス設定が失われます。

（注） 管理の再イメージ化または切り替えを行う前に、ライセンスの問題に対処してください。Cisco Smart Licensing を使用している場合は、孤立した権限付与の発生を防ぐために、Cisco Smart Software Manager（CSSM）から手動で登録解除することが必要になる場合があります。これらが生じると再登録できない場合があります。

表 *31* : シナリオ：新規インストールが必要ですか。

シナリオ	ソリューション	ライセンシング
FMC で管理されているデバイスをより古い Firepower バージョンからアップグレードします。	古いバージョンからのアップグレード パスには中間バージョンが含まれる場合があります。特に、FMC とデバイスのアップグレードを交互に行う必要がある大規模展開の環境では、この複数の手順のプロセスを完了するために時間がかかる場合があります。 この時間を短縮するために、アップグレードする代わりに、古いデバイスを再イメージ化することができます。 **1.** FMC からデバイスを削除します。 **2.** FMC のみをターゲット バージョンにアップグレードします。 **3.** デバイスを再イメージ化します。 バージョン 5.x を実行している 7000/8000 シリーズデバイスのイメージを再作成する必要がある場合は、「新規インストールに関するガイドラインと制約事項 （53 ページ）」を参照してください。 **4.** デバイスを FMC に再度追加します。	FMC からデバイスを削除すると、デバイスが登録解除されます。デバイスを再度追加した後、ライセンスを再割り当てします。
FTD 管理を FDM から FMC（ローカルからリモート）に変更します。	**configure manager** CLI コマンドを使用します。『Command Reference for Firepower Threat Defense』を参照してください。	管理を切り替える前に、デバイスを登録解除します。デバイスを FMC に追加した後、ライセンスを再割り当てします。
FTD 管理を FMC から FDM（リモートからローカル）に変更します。	**configure manager** CLI コマンドを使用します。『Command Reference for Firepower Threat Defense』を参照してください。 **例外**：デバイスが実行中であるか、バージョン6.0.1からアップグレードされています。この場合は、再イメージ化します。	FMC からデバイスを削除し、デバイスを登録解除します。FDM を使用して再登録します。
ASDM と FMC 間の ASA FirePOWER 管理を変更します。	他の管理方法の使用を開始します。	クラシック ライセンスについては、セールス担当者にお問い合わせください。ASA FirePOWER ライセンスは、特定のマネージャに関連付けられています。

シナリオ	ソリューション	ライセンシング
ASA FirePOWER を同じ物理デバイス上の FTD に置き替えます。	再イメージ化します。	クラシック ライセンスをスマート ライセンスに変換します。『Firepower Management Center Configuration Guide』を参照してください。
NGIPSv を FTDv に置き換えます。	再イメージ化します。	新しいスマート ライセンスについては、セールス担当者にお問い合わせください。
FDM を使用した FTD パッチをアンインストールします。	再イメージ化します。 FDM 展開環境では、パッチをアンインストールすることはできません。	再イメージ化する前に、デバイスを登録解除します。その後、再登録します。
障害が発生した FMC または FTD デバイスをバックアップから復元します。	RMA のシナリオでは、工場出荷時の初期状態の設定での交換になります。ただし、交換がすでに設定されている場合は、復元する前に再イメージ化することをお勧めします。	再イメージ化を行う前に登録を解除しないでください。また、FMC からデバイスを削除しないでください。これを行った場合は、復元後に再度登録を解除してから再登録する必要があります。 代わりに、バックアップを実行した後に行われたライセンス変更を元に戻します。復元が完了したら、ライセンスを再設定します。ライセンスの競合や孤立した権限付与に気付いた場合は、Cisco TAC にお問い合わせください。

新規インストールに関するガイドラインと制約事項

誤りを避けるには、注意深い計画と準備が役立ちます。Firepower リリースに精通していて、Firepower アプライアンスを再イメージ化したことがある場合でも、これらのガイドラインと制限事項に加えて、「インストール手順 （58 ページ）」にリンクされている手順を必ず参照してください。

イベント データと設定データのバックアップ

サポートされている場合は、再イメージ化の前にバックアップすることを強くお勧めします。

（注） 再イメージ化してアップグレードする必要がない場合、バージョンの制約により、バックアップを使用して古い設定をインポートすることはできません。設定は手動で再作成する必要があります。

安全なリモートロケーションにバックアップし、正常に転送が行われることを確認する必要があります。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。アプライアンスに残っているすべてのバックアップが削除されます。特に、バックアップファイルは暗号化されていないため、不正アクセスを許可しないでください。バックアップ ファイルが変更されていると、復元プロセスは失敗します。

バックアップの最初のステップとして、アプライアンスモデルとバージョンを、パッチレベルを含めて書き留めておいてください。FMC の場合は、VDB のバージョンを書き留めておきます。 Firepower 4100/9300 シャーシの場合は、FXOS のバージョンを書き留めておきます。新しいアプライアンスや再イメージ化したアプライアンスにバックアップを復元する必要がある場合は、新しいアプライアンスを最初に更新する必要がある場合があるため、これは重要です。

（注） バックアップと復元は、複雑なプロセスになる可能性があります。手順をスキップしたり、セキュリティ上の問題を無視しないでください。誤りを避けるには、注意深い計画と準備が役立ちます。バックアップと復元の要件、ガイドライン、制限事項、およびベストプラクティスの詳細については、ご使用の Firepower 製品のコンフィギュレーション ガイドを参照してください。

からのデバイスの削除 Firepower Management Center

再イメージ化されたアプライアンスを手動で設定する予定がある場合は、再イメージ化する前に、リモート管理からデバイスを削除します。

- FMC を再イメージ化する場合は、すべてのデバイスを管理から削除します。
- 単一のデバイスを再イメージ化するか、またはリモートからローカルでの管理に切り替える場合は、その単一のデバイスを削除します。

FMC または FTD デバイスの再イメージ化後にバックアップから復元する場合は、デバイスをリモート管理から削除する必要はありません。

ライセンスの問題の対処

Firepower アプライアンスを再イメージ化する前に、ライセンスの問題に対処してください。状況により、Cisco Smart Software Manager からの登録解除が必要になります。また場合によっては、新しいライセンスについてセールス担当者に問い合わせる必要があります。シナリオに応じて必要な操作を決定するには、「新規インストールの決定」を参照してください。

ライセンスの詳細については、次を参照してください。

- Cisco Firepower System Feature Licenses Guide
- Frequently Asked Questions (FAQ) about Firepower Licensing
- 設定ガイドのライセンスの章

アプライアンス アクセス

再イメージ化により、ほとんどの設定が工場出荷時の初期状態に戻ります。

アプライアンスに物理的にアクセスできない場合、再イメージ化プロセスによって管理ネットワークの設定を維持できます。これにより、再イメージ化した後、アプライアンスに接続して、初期設定を実行できます。ネットワーク設定を削除する場合は、アプライアンスに物理的にアクセスできる必要があります。Lights-Out 管理（LOM）を使用することはできません。

（注） 以前のメジャーバージョンに再イメージ化すると、ネットワーク設定が自動的に削除されます。このようなまれなケースでは、物理的アクセスが必要です。

デバイスに関して、ユーザの位置からのトラフィックがデバイスの管理インターフェイスにアクセスするためにデバイス自体を通過する必要がないことを確認してください。FMC 展開では、デバイスを経由せずに FMC 管理インターフェイスにアクセスできる必要もあります。

シスコとのデータの共有

一部の機能にシスコとのデータ共有が含まれます。

バージョン 6.2.3+ では、*Cisco Success Network* は、テクニカルサポートを提供するために不可欠な使用状況に関する情報と統計情報をシスコに送信します。初期設定中に、参加を承諾するか、辞退するかを尋ねられます。また、いつでもオプトインまたはオプトアウトできます。

バージョン 6.2.3+ では、Web 分析のトラッキングは、これに限定されませんが、ページでの操作、ブラウザのバージョン、製品のバージョン、ユーザの場所、FMC の管理 IP アドレスまたはホスト名を含む、個人を特定できない使用状況データをシスコに送信します。Web 分析トラッキングはデフォルトでオンになっていますただし、初期設定の完了後にいつでもオプトアウトできます。また、この機能を再度有効にする可能性があるメジャーアップグレード後は、もう一度オプトアウトする必要があります。

以前のメジャー バージョンへの Firepower 2100 シリーズ デバイスの再イメージ化

Firepower 2100 シリーズ デバイスを以前のメジャーバージョンに戻す必要がある場合は、完全な再イメージ化を実行することをお勧めします。消去設定方式を使用すると、Firepower Threat Defense ソフトウェアに加えて、FXOS が復元しない場合があります。この場合、特にハイ アベイラビリティ展開では、障害が発生する可能性があります。

詳細については、Cisco FXOS トラブルシューティング ガイド（Firepower Threat Defense を実行している Firepower 1000/2100 シリーズ向け）に記載されている再イメージ化の手順を参照してください。

バージョン 6.3.0 以降へのバージョン 5.x ハードウェアの再イメージ化

バージョン 6.3+ のインストールパッケージの名前が変更されていると、古い物理アプライアンス（FMC 750、1500、2000、3500、4000 のほか、7000/8000 シリーズ デバイスと AMP モデル）の再イメージ化に関する問題が発生します。バージョン 5.x を現在実行していて、バージョン 6.3.0 を新規にインストールする必要がある場合は、インストールパッケージをダウンロー

ドした後、その名前を「古い」名前に変更します。『Cisco Firepower Release Notes, Version 6.3.0』の「Renamed Upgrade and Installation Packages」の情報を参照してください。

FMC（Defense Center）をバージョン 5.x からより新しいバージョンに再イメージ化した後、古いデバイスを管理することはできません。また、これらのデバイスを再イメージ化してから、FMC に再度追加する必要があります。シリーズ 2 デバイスは EOL であり、Firepower ソフトウェアの過去バージョン 5.4.0.x を実行できないことに注意してください。それらのデバイスを置き換える必要があります。

スマート ライセンスの登録解除

Firepower Threat Defense デバイスは、ローカル（Firepower Device Manager）またはリモート（Firepower Management Center）で管理されているかどうかに関係なく、Cisco Smart Licensing を使用します。ライセンス供与された機能を使用するには、Cisco Smart Software Manager（CSSM）で登録する必要があります。後で再イメージ化または管理の切り替えを行うことにした場合は、孤立した権限付与を発生させないように登録を解除する必要があります。これらが生じると再登録できない場合があります。

（注） FMC または FTD デバイスをバックアップから復元する必要がある場合は、再イメージ化の前に登録を解除しないでください。また、FMC からデバイスを削除しないでください。代わりに、バックアップを実行した後に行われたライセンス変更を元に戻します。復元が完了したら、ライセンスを再設定します。ライセンスの競合や孤立した権限付与に気付いた場合は、Cisco TAC にお問い合わせください。

登録を解除すると、仮想アカウントからアプライアンスが削除され、関連付けられたライセンスが解放されるため、ライセンスを再割り当てできるようになります。アプライアンスを登録解除すると、適用モードになります。アプライアンスの現在の設定とポリシーはそのまま機能しますが、変更を加えたり展開したりすることはできません。

次の操作を行う前に、CSSM から手動で登録解除します。

- FTD デバイスを管理する Firepower Management Center を再イメージ化する。
- FDM によってローカルで管理されている Firepower Threat Defense デバイスを再イメージ化する。
- Firepower Threat Defense デバイスを FDM から FMC 管理に切り替える。

FMC からデバイスを削除すると、CSSM から自動的に登録解除されます。これにより、次のことが可能になります。

- FMC によって管理されている Firepower Threat Defense デバイスを再イメージ化する。
- Firepower Threat Defense デバイスを FMC から FDM 管理に切り替える。

上記の 2 つのケースでは、FMC からデバイスを削除すると、デバイスが自動的に登録解除されます。FMC からデバイスを削除すれば、手動で登録解除する必要はありません。

ヒント NGIPS デバイスのクラシック ライセンスは、特定のマネージャ（ASDM/FMC）に関連付けられており、CSSM を使用して制御されません。クラシック デバイスの管理を切り替える場合、または NGIPS 展開から FTD 展開に移行する場合は、セールス担当者にお問い合わせください。

の登録解除 Firepower Management Center

バックアップから復元する予定がない限り、再イメージ化する前に CSSM から Firepower Management Center の登録を解除してください。これは、管理対象の Firepower Threat Defense デバイスの登録も解除します。

FMC が高可用性に設定されている場合、ライセンスの変更が自動的に同期されます。他の FMC の登録を解除する必要はありません。

ステップ 1 Firepower Management Center にログインします。

ステップ 2 **[システム（System）] > [ライセンス（Licenses）] > [スマートライセンス（Smart Licenses）]**を選択します。

ステップ 3 [スマートライセンスのステータス（Smart License Status）] の横の停止記号 をクリックします。

ステップ 4 警告を読み、登録解除することを確認します。

を使用した FTD デバイスの登録解除 FDM

再イメージ化するか、またはリモート（FMC）管理に切り替える前に、ローカルの管理対象 Firepower Threat Defense デバイスの登録を Cisco Smart Software Manager から解除します。

高可用性のために設定されているデバイスの場合は、その装置を登録解除するために、高可用性ペアにあるその他の装置にログインする必要があります。

ステップ 1 Firepower Device Manager にログインします。

ステップ 2 [デバイス（Device）] をクリックし、[スマートライセンス（Smart License）] のサマリーで [設定の表示（View Configuration）] をクリックします。

ステップ 3 歯車ドロップダウンリストから [デバイスの登録解除（Unregister Device）] を選択します。

ステップ 4 警告し、登録を解除することを確認します。

インストール手順

リリース ノートとアップグレード ガイドにはインストール手順は含まれていません。代わりに、次のドキュメントのいずれかを参照してください。インストール 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 から入手できます。

***Table 32: Firepower Management Center* のインストール手順**

FMC プラットフォーム	ガイド
FMC 1600、2600、4600	Cisco Firepower Management Center 1600, 2600, and 4600 Hardware Installation Guide：Restoring a Firepower Management Center to Factory Defaults
FMC 1000、2500、4500	Cisco Firepower Management Center 1000, 2500, and 4500 Getting Started Guide：Restoring a Firepower Management Center to Factory Defaults
FMC 750、1500、3500 FMC 2000、4000	Cisco Firepower Management Center 750, 1500, 2000, 3500 and 4000 Getting Started Guide：Restoring a Firepower Management Center to Factory Defaults
FMCv	『Cisco Firepower Management Center Virtual 入門ガイド』

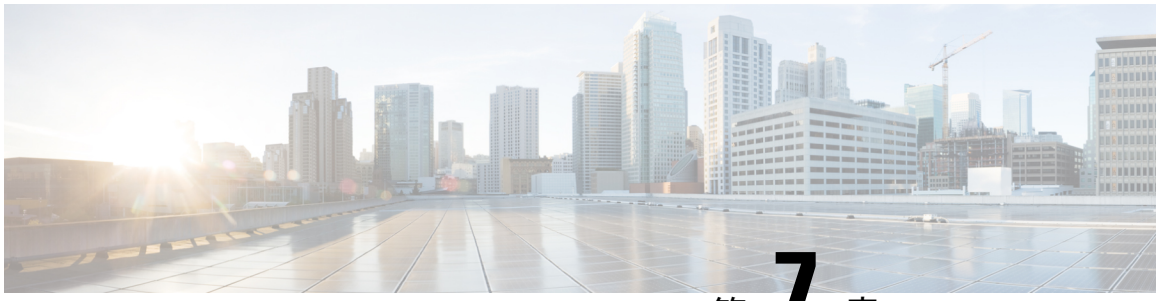
***Table 33: Firepower Threat Defense* のインストール手順**

FTD プラットフォーム	ガイド
Firepower 2100 シリーズ	Cisco ASA and Firepower Threat Defense Reimage Guide Cisco FXOS トラブルシューティング ガイド（Firepower Threat Defense を実行している Firepower 1000/2100 シリーズ向け）
Firepower 4100/9300 シャーシ	Cisco Firepower 4100/9300 FXOS Configuration Guides：イメージ管理に関する章 Cisco Firepower 4100 スタートアップガイド Cisco Firepower 9300 Getting Started Guide
ASA 5500-X シリーズ	Cisco ASA and Firepower Threat Defense Reimage Guide
ISA 3000	Cisco ASA and Firepower Threat Defense Reimage Guide
FTDv: VMware	VMware 向け Cisco Firepower Threat Defense Virtual スタートアップガイド
FTDv: KVM	Cisco Firepower Threat Defense Virtual for KVM スタートアップガイド

FTD プラットフォーム	ガイド
FTDv：AWS	Cisco Firepower Threat Defense Virtual for the AWS Cloud スタートアップガイド
FTDv：Azure	Cisco Firepower Threat Defense Virtual for the Microsoft Azure Cloud Quick Start Guide

Table 34: FirePOWER 7000/8000 シリーズ、***NGIPSv*** および ***ASA FirePOWER*** インストール手順

NGIPS プラットフォーム	ガイド
Firepower 7000 シリーズ	Cisco Firepower 7000 Series Getting Started Guide：*Restoring a Device to Factory Defaults*
Firepower 8000 シリーズ	Cisco Firepower 8000 Series Getting Started Guide：*Restoring a Device to Factory Defaults*
NGIPSv	Cisco Firepower NGIPSv（VMware 向け）クイックスタート
ASA FirePOWER	Cisco ASA and Firepower Threat Defense Reimage Guide ASDM Book 2: Cisco ASA Series Firewall ASDM Configuration Guide：Managing the ASA FirePOWER Module



第 7 章

資料

次のトピックでは、Firepower のドキュメントへのリンクを記載しています。

更新されたドキュメント： バージョン 6.3.0.x

少なくとも 1 つの バージョン 6.3.0.x パッチのために、次の Firepower のドキュメントが更新されました。

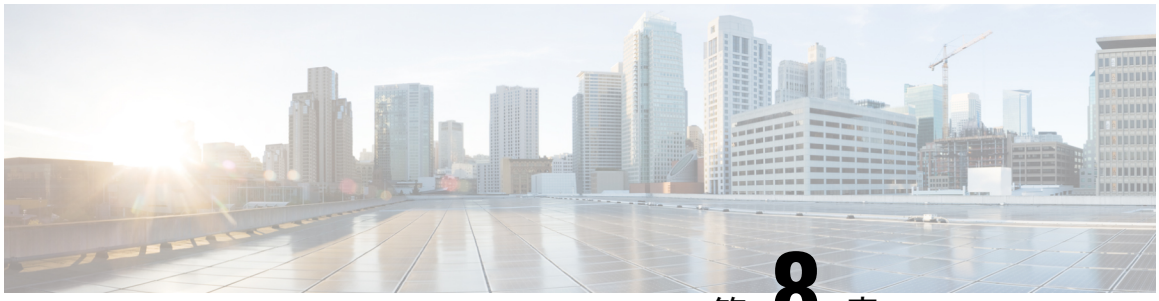
- Cisco Firepower Compatibility Guide
- Cisco Firepower Management Center Upgrade Guide
- 『Firepower Management Center Configuration Guide, Version 6.3』

更新されていない、またはこのリリースで新しく使用可能になったドキュメントへのリンクについては、「ドキュメントロードマップ, on page 61」を参照してください。

ドキュメントロードマップ

ドキュメントロードマップでは、現在使用可能なドキュメントおよび従来のドキュメントへのリンクを示します。

- Cisco Firepower ドキュメント一覧
- Cisco ASA シリーズ ドキュメント一覧
- Cisco FXOS ドキュメント一覧



第 8 章

解決済みの問題

便宜上、これらのリリースノートには、各パッチの解決済みのバグが記載されています。

各リストは1回自動生成され、その後は更新されません。特定の解決済みの問題がシステムでどのように分類または更新されたかとその時期によっては、リリースノートに記載されない場合があります。Cisco Bug Search Tool を「信頼できる情報源」と考えてください。

解決済みの問題の検索

サポート契約がある場合は、Cisco Bug Search Tool を使用して Firepower 製品の最新の解決済みバグリストを取得することができます。これらの一般的なクエリには、バージョン6.3.0.xパッチを実行している Firepower 製品の解決済みのバグが表示されます。

- Firepower Management Center
- Firepower Management Center Virtual
- Firepower Threat Defense
- ASA with FirePOWER サービス
- NGIPSv

検索では、特定の Firepower プラットフォームとバージョンに影響するバグに絞り込むことができます。バグ ID ごとに検索したり、特定のキーワードを検索することもできます。

バージョン 6.3.0.5 で解決済みの問題

Table 35: バージョン *6.3.0.5* で解決済みの問題

不具合 ID	タイトル
CSCve24102	GUI で、DHCP プールごとに最大 256 個のアドレスを設定できる必要がある
CSCvh73096	使用可能な場合に ISE から sAMAccountUserName を読み取る
CSCvk26612	「デフォルトのキーリング証明書が無効です。理由：期限切れ（default Keyring's certificate is invalid, reason: expired）」 ヘルスアラート
CSCvk43854	Cisco Firepower Threat Defense 検出エンジン ポリシーのバイパスの脆弱性
CSCvm40288	HA リンクでのポートチャネルの問題
CSCvm48451	4100 および 9300 で侵入イベントパフォーマンスのグラフが空白になる
CSCvm68648	Firepower ソフトウェアでの CVE-2016-8858（OpenSSH）の確認
CSCvm76266	スレッド名：cli_xml_server での Lina のトレースバック
CSCvm82966	Linux カーネル 4.14 の脆弱性
CSCvn24594	NTPD を開始する前に、ブレード sysclock の NTPDATE update をスーパーバイザから追加する
CSCvn77388	SDI - 一時停止されたサーバにより、正常なサーバでの認証の完了に 15 秒の遅延が発生する
CSCvn81898	接続イベントに関する syslog アラートが設定されている場合に、syslog メッセージにデバイス名が含まれていない
CSCvn83385	Cisco FTD、FMC、および FXOS ソフトウェア PAM のサービス拒否攻撃に対する脆弱性
CSCvo11280	ASA 機能拡張：SDI クラスタのメンバーで状態が変更されたら、syslog メッセージを生成する
CSCvo14961	「dns_cache_timer」プロセスの終了を待機している間に ASA がトレースバックし、リロードすることがある。
CSCvo28118	メンバーがクラスタに参加しようとすると VPN クラスタリング HA のタイマースレッドでトレースバックが発生する
CSCvo29989	Cisco FirePower Threat Defense に関する情報漏えいの脆弱性

不具合 ID	タイトル
CSCvo43795	OSPF プロセス のクリア後でも OSPF プロセス ID が変更されない
CSCvo66546	SFDataCorrelator プロセスで Firepower が頻繁にトレースバックおよび再起動する
CSCvo68448	5585 プラットフォームで ASA モジュールをリロードした後、ASA が SFR モジュールを「応答なし」として報告する
CSCvo73250	ENH：警告「重複する要素が見つかりました（found duplicate element）」の ACE の詳細
CSCvo74397	ENH：「コマンドは無視されました。設定中です...（Command Ignored, configuration in progress...）」にプロセス情報を追加
CSCvo83169	Cisco ASA ソフトウェアと FTD ソフトウェアの FTP のインスペクション サービス拒否攻撃に対する脆弱性
CSCvo86038	flow-offloaded フローでの同時 FIN が接続の失効につながる
CSCvo86940	ブレードで enic、vfio-pci、igb_uio を設定しようとするとパスワードの入力が求められる
CSCvo90998	インラインセット インターフェイスの snort に LACPDU を送信すべきでない
CSCvp04186	cts import-pac tftp：構文が機能しない
CSCvp12582	ASA のウェルノウンポート名ではなくポート番号をアクセスリストで表示するオプション
CSCvp19910	ヘッダー TEID : 0 の gtpv1 identification req メッセージを処理できない
CSCvp19998	ASA がヘッダー TEID:0 の GTPV1 SGSN Context Req メッセージをドロップする
CSCvp23579	[ネットワークファイルトラジェクトリ（Network File Trajectory）] ページのロードに毎回 90 秒かかる
CSCvp33052	処理されていないリソースが一時的に使用できないという問題により Firepower 8000 インターフェイスがフラップする場合がある
CSCvp33341	Cisco ASA および Firepower Threat Defense ソフトウェア WebVPN クロスサイト スクリプティングの脆弱性
CSCvp46173	サブドメイン内のインターフェイスグループまたはインターフェイスゾーンの変更によってグローバルドメインが上書きされる
CSCvp49576	xlate_detach のウォッチドッグによる FTD のトレースバック

不具合 ID	タイトル
CSCvp54261	SFR モジュール/7000/8000 デバイスの監査 syslog で UDP ではなく TCP が syslog 通信に使用される
CSCvp55901	HA アクティブユニットの ASA で LINA が繰り返しトレースバックする
CSCvp55941	ファイル復帰ブロックがランダムにスローされて、SMB 共有からのファイルへのアクセスに関する問題が発生する
CSCvp58028	nfm_exceptiond の natd スレッドで約 90 ～ 100% の CPU 時間が使用される
CSCvp67257	カーネルアップグレード（3.10 ～ 4.14）による USGv6 障害
CSCvp67626	ゲートウェイ IP が正しく設定されていない場合、000_start/125_verify_bundle.sh で 2100 アップグレードが失敗する
CSCvp72244	CVE-2019-11815 の Cisco 8000 シリーズの評価
CSCvp76944	Cisco ASA および FTD ソフトウェア WebVPN CPU のサービス妨害（DoS）脆弱性
CSCvp84546	ASA 9.9.2 クライアントレス WebVPN - HTML の処理時に HTML エンティティが誤って復号化される
CSCvp87623	CAC（HTTPS クライアント証明書）の使用時に更新をアップロードすると「更新要求エンティティが大きすぎます（update request entity too large）」というエラーが発生する
CSCvp97061	URL フィルタリングですべての URL が未分類として表示される
CSCvp97799	SSL ポリシーのエクスポート時に openSSL コールで CC モードにして 6.5.0-1148 にアップグレードした後、ポリシーの展開に失敗する
CSCvp98066	CD のリセット時にフラグ [parseFailoverReqIssued] をクリアしないと、ノードを結合できない
CSCvp99137	Firepower 2100 上の ASA：管理インターフェイス上の過剰な数の DNS クエリ
CSCvq00675	Linux カーネル sas_expander.c が競合状態で任意のコードを実行...
CSCvq01459	9.12.2.1 へのアップグレード後の LINA トレースバック
CSCvq05113	設定の最初の 10 個のインターフェイスで ASA フェールオーバー LANTEST メッセージが送信される
CSCvq06790	シリーズ 3 デバイスで Snort プロセスがメモリ破損でコアをダンプする
CSCvq08684	特殊文字および符号化によるポリシー展開の失敗

不具合 ID	タイトル
CSCvq09093	VPN 事前展開の検証がデバイスごとに約 20 秒かかる
CSCvq11513	トレースバック：「saml identity-provider」コマンドでマルチコンテキスト ASA がクラッシュする
CSCvq12411	CSCvj98964 の修正があるにも関わらず、SCTP トラフィックにより ASA がトレースバックすることがある
CSCvq13442	コンテキストを削除すると、ssh key-exchange がグローバルにデフォルトになる
CSCvq16123	Firepower ダイナミック Snort ルールが、Snort のリロードが関係する展開後に無効になる
CSCvq17263	DATAPATH-8-15821 での FTD LINA のトレースバック
CSCvq19525	TCP_SACK の sfims の評価
CSCvq21607	CLI を使用してバックアップを復元すると、「ssl trust-point」コマンドが削除される
CSCvq24134	ASA IKEv2 - フェーズ 2 のキー再生成の開始後に ASA が追加の削除メッセージを送信する
CSCvq25626	バッファへのロギング時の ASAv のウォッチドッグ
CSCvq25775	FTD Firepower 2100：バインドユーザのパスワードに特殊文字が含まれている場合、外部認証が失敗する
CSCvq26794	存在しない原因を含む GTP 応答メッセージがドロップされて、TID が 0 のエラーメッセージが発行される
CSCvq27010	ASA-SFR データプレーンの通信でフラッピングが発生した際にメモリリークが起こる
CSCvq28250	ENH：syn cookie の問題に関する ASA クラスタのデバッグ
CSCvq32681	FTD のアップグレード時に複数のインターフェイスペアのインラインセットに対して Fail to Wire 設定が無効になる
CSCvq36042	ハートビートが失われてリロードが発生する
CSCvq39083	SSL ポリシーが有効になっている場合にブラックリストに登録された URL への HTTPS 接続がセキュリティ インテリジェンスでドロップされない
CSCvq39317	ASA がファイルの整合性を確認できない
CSCvq40943	6K スポークでの FTD 4150 VPN s2s 展開の失敗

不具合 ID	タイトル
CSCvq44665	FTD/ASA：アサート snp_tcp_intercept_assert_disabled によるデータパスでのトレースバック
CSCvq46918	アップグレード後に SNMPv3 ユーザが削除される
CSCvq50314	失敗した SSH ログイン試行が syslog 経由でエクスポートされない
CSCvq54242	SSL ポリシーでの警告「送信元ネットワークで、空のグループがあります（There is an empty group in the source networks）」
CSCvq54667	SSL ネゴシエーションの問題により、SSL VPN が確立できない場合がある
CSCvq56138	パスワードの文字列にスペースが含まれている場合に LDAP ユーザの FMC GUI へのユーザログインが失敗する
CSCvq56462	ファイルポリシーが一部のマルウェアドキュメント（.doc）および Adobe Flash（.swf）ファイルを検査しない
CSCvq60131	デバイスへの EZVPN スポークの移動時に ASA のトレースバックが発生する
CSCvq63024	デュアルスタック ASAv の手動フェールオーバーの問題
CSCvq64742	スレッド名 ssh での ASA5515-K9 スタンバイトレースバック
CSCvq65092	デバイス関連の REST API コールが低速になる
CSCvq65241	スレッド名での Saleen の ASA トレースバック：IPv6 IDB
CSCvq65542	すべてのバグが修正されるまで、fp2100 から asp load-balance per-packet 機能を無効にする
CSCvq69111	トレースバック：スレッド名でのクラスタユニット lina のアサーション：クラスタコントローラ
CSCvq70468	ASA クラスタが OSPF ルートをフラッシュしない
CSCvq70485	「securityzones」REST API が低速になる
CSCvq75743	ASA：3 ホップ離れた宛先に対する BGP の再帰ルートルックアップが失敗する
CSCvq76533	MC4000 の F_RNA_EVENT_LIMIT は 2000 万である必要がある
CSCvq77547	ポートチャネルでのフェールオーバー記述子の不一致により、フェールオーバーで接続の複製が失敗する
CSCvq80318	Internal-Data0/1 の列挙時に ASA が PCI cfg 領域に関する誤ったエラーメッセージを生成する

不具合 ID	タイトル
CSCvq80735	ネイバーが 1 つのインターフェイスと同じサブネット上にある場合、BGP にネイバーを追加できない
CSCvq81516	FMC で 12 時～午後 1 時（UTC）の間の VPN イベントが表示されない
CSCvq91645	フローオフロードハッシュの動作変更

バージョン6.3.0.4 で解決済みの問題

Table 36: バージョン*6.3.0.4* で解決済みの問題

不具合 ID	タイトル
CSCvf83160	スレッド名でのトレースバック：DATAPATH-2-1785
CSCvg01007	https pdf 添付ファイルの問題
CSCvg74603	eStreamer アーカイブ イベントが diskmanager によって正しくプルーニングされない
CSCvi63474	6.2.2 へのアップグレード後に ASDM を介した SFR モジュールのシステム ポリシーの編集ができない
CSCvk14242	FTD の sfstunnel プロセスにすでに削除されている大規模なクラウド db ファイルが保持されている
CSCvm27111	OSPF 設定を削除する際の FTD Lina のトレースバック
CSCvm36362	ルート トラッキング エラー
CSCvm50421	ACE での OSPF/EIGRP と IPv6 の同時使用が原因で ASA が同期設定中にスレーブ/スタンバイでトレースバックする
CSCvm70274	tcp プロキシ：データパスでの ASA のトレースバック
CSCvm88294	パーティション強制ドレインが発生していないためディスク使用率が高くなる
CSCvn25605	FTW：センサーが完全に回復した後でも、バイパス LED がオレンジ色に点灯したままになる
CSCvn34246	AC ポリシー エディタのロードに時間がかかりすぎるためロード インジケータが必要になる
CSCvn45750	3D デバイスへの展開時に FMC 監査ログに管理者とシステムのみがオーナーとして表示される（GUI/SYSLOG）

不具合 ID	タイトル
CSCvn57284	FTD でサポートされていない EC カーブ x25519
CSCvn66248	ファイルがオフボックスで変更されて再度コピーされた場合に「boot config」を設定しても効果がない
CSCvn76875	BGP のグレースフルリスタートが断続的に動作しなくなる
CSCvn78597	プロキシが有効になっている場合、HTTPS ブロック サイトでは Firepower ブロック ページが MS IE11 および Edge に表示されない
CSCvo03700	クラスタがスレーブユニットで有効になっている場合にスレッドロガーで ASA がトレースバックすることがある
CSCvo24145	大きな firewall_rule_cache テーブルによる ids_event_alerter の高メモリ使用率
CSCvo31695	メモリブロックの解放時におけるスレッド名 DATAPATH-0-1668 でのトレースバック
CSCvo33348	非標準ポートの Mysql トラフィックが正しく分類されない
CSCvo33851	ngfw.properties が空の場合に ngfwManager が開始されない
CSCvo43679	FTD Lina のトレースバック（Normaliser によるシステムでのパケット ループが原因）
CSCvo48838	長すぎる設定行のエラーを Lina が適切に報告しない
CSCvo50168	監査ログの設定の失敗によりシステム設定が編集できなくなる
CSCvo51265	SCP のボックスへの大規模なファイル転送によりトレースバックが発生する
CSCvo54799	fstab の devpts エントリが破損しているためデバイスへの ssh が失敗する
CSCvo56836	スケール：500 以上のデバイスを使用すると UMS によって UI がハングする（特に展開時）
CSCvo60862	アクセス コントロール ポリシー編集時の内部エラー
CSCvo62060	FMC が大量のデバイスを管理しているときにテレメトリが送信されない
CSCvo65464	FPR2100：ポート チャネル インターフェイスを介して学習された EIGRP ルートが無限 FD になります
CSCvo66534	影響を受けるスレッドとしてデータパスを示すトレースバックとリロード
CSCvo70866	任意の値の SGT タグを持つすべてのクライアント パケットに対するサーバ パケットで SGT タグがタグなしと表示される

不具合 ID	タイトル
CSCvo72179	SMB ではリモート ストレージ設定でドット（.）を使ったバージョン文字列の設定を許可する必要がある
CSCvo72232	ブラウザの ERR_SSL_BAD_RECORD_MAC_ALERT または SSL_ERROR_BAD_MAC_ALERT
CSCvo74350	ASA がトレースバックしリロードすることがある。WebVPN トラフィックに関連する可能性がある
CSCvo74625	管理ゲートウェイがデータインターフェイスとして設定されている場合、6.4.0 - IPv6 ルーティングが WM および KP で機能しない
CSCvo74745	多数の連続 URL ルックアップ（30M 超）生成後のクラウド エージェントのコア化
CSCvo78789	Cisco 適応型セキュリティアプライアンスのスマートトンネルに関する脆弱性
CSCvo80501	手動フェールオーバーの実行時にスタンバイファイアウォールがトレースバックしてリロードする
CSCvo81073	NGFWHA EO がないため [Device Management] ページをロードできないか、FMC をアップグレードできない
CSCvo81260	API を介して FMC の「FQDN」を使用すると、ネットワーク属性内のすべてのオブジェクトが「ANY」になる
CSCvo83574	インライン セットをタップ モードから切り替えるとデバイスが不良状態になる
CSCvo87930	w3m を使用した ipv6 の HTTP が失敗する
CSCvo88188	App-ID 条件を持つ SSL ルールが復号機能を制限する可能性がある
CSCvo88306	重複するルールがあると NAT ルールが誤った順序で適用される可能性がある
CSCvo89224	展開用のデバイス リストの取得で 10 分後に FMC がタイムアウトになる
CSCvo90153	ASA が特殊文字を含むユーザを https 経由で認証できない
CSCvo90550	Firepower の推奨事項では GID 3 の IPS ルールが有効にならない
CSCvo90805	Cisco Firepower Management Center RSS のクロスサイト スクリプティングの脆弱性
CSCvo93872	GTP トラフィックの検査中のメモリ リーク
CSCvo94486	セキュリティ インテリジェンスの処理中に Snort プロセスが終了する

不具合 ID	タイトル
CSCvp03498	FMC のユーザ アイデンティティ機能のヘルス モニタリング オプション。
CSCvp07143	DTLS 1.2 および AnyConnect oMTU
CSCvp09150	Cisco ASA ソフトウェアの Web ベース管理インターフェイスの権限昇格における脆弱性
CSCvp12052	ASA がトレースバックおよびリロードすることがある。webvpn に関連する可能性がある
CSCvp16979	ssl および daq デバッグ ログを動的に有効化/無効化できない
CSCvp18878	ASA：データパスでのウォッチドッグのトレースバック
CSCvp21837	FMC（6.5.0 より前）を経由することなく、FTD が URL ルックアップを直接実行できるようにする
CSCvp23137	SSD 2 が見つからない場合に ASA/FTD が syslog を生成する：/dev/sdb が存在する。ステータス：操作不能（/dev/sdb is present. Status: Inoperable）
CSCvp24787	（snort）HTTPS 経由時にファイルが検出されなくなる（SSL 再署名）
CSCvp25581	FMC-HA user_group_map エントリがスプリットブレインで消去されている
CSCvp25583	FMC GUI を介して BGP に OSPF を再配布すると FTD によって自動的にメトリックが 0 に設定される
CSCvp25782	メタデータキャッシュのプルーニング中の EventHandler コア
CSCvp27263	6.5.0 より以前の Cisco Firepower Management Center における ClamAV の複数の脆弱性
CSCvp29245	過剰なイベントログによりディスク容量が使い果たされたため、FTD と FDM の操作が失敗する
CSCvp32617	9.6.2 以降で「確立済み TCP」が機能しない
CSCvp35359	明示的な UPN と暗黙的な UPN が一致しないと FMC-ISE 統合が機能しない
CSCvp36425	Cisco ASA および FTD ソフトウェアの暗号化 TLS および SSL ドライバにおけるサービス拒否（DoS）攻撃に対する脆弱性
CSCvp37779	FTD のトラブルシューティング ファイルからの show tech が不完全である
CSCvp38808	FP2100：「パスワード暗号キーが設定されていません（The password encryption key has not been set.）」という障害の除去

不具合 ID	タイトル
CSCvp43474	REST API クエリ /api/fmc_config/v1/domain/UUID/devices/devicerecords が失敗する
CSCvp43536	アップグレードした FMC デバイスで、正常に展開された後も FXOS デバイスがダーティとして表示される
CSCvp46341	2100 Firepower プラットフォームで Fail-to-Wire（FTW）ポートが回復に失敗する
CSCvp54634	不明瞭な DND を使用しているときに正しくないルールが一致する
CSCvp58310	pxgrid 機能の統合、接続のハング、curl のハングの問題
CSCvp72488	Firepower：6.3.0.2 以降へのアップグレード後のネットワーク接続障害に対する AMP
CSCvp72601	FMC UI：VPN ハブアンドスポークトポロジのロードに時間がかかる
CSCvp72770	vFTD が Azure プラットフォームで実行されている場合に、FMC から vFTD にコピーされた BCDB ファイルが切り捨てられる
CSCvp78197	ポリシーの展開による ospf ネイバーの削除および追加
CSCvp81967	管理対象デバイスが 500 以上ある場合に FMC のデバイス管理ページのロードが遅くなる
CSCvp82945	NAT ポリシーの適用がエラーの重複で失敗する
CSCvp96934	重複する NAT を含むエラー メッセージがクリアされ実行可能であることを確認する
CSCvq08684	特殊文字および符号化によるポリシー展開の失敗
CSCvq34224	マネージャをアップグレードすると、Firepower プライマリ検出エンジン プロセスが終了する
CSCvq61651	FMC での URL DB ダウンロード失敗アラート：FMC/FDM で新しい URL DB の更新が有効にならない

バージョン 6.3.0.3 で解決済みの問題

Table 37: バージョン *6.3.0.3* で解決済みの問題

不具合 ID	タイトル
CSCvi16224	NFVIS（KVM）システムに ASAv VM を展開するときに SNMPv3 の snmp-server ホスト コマンドが正しく適用されない
CSCvi62112	FTD トランスペアレントで FlexConfig を介して BPDU をブロックすると展開と登録の問題が発生する
CSCvj06993	NSF による ASA の HA：ASA の HA でインターフェイス障害が発生した場合に NSF が正しくトリガーされない
CSCvj82652	disk0 が読み取り専用にマウントされているため展開の変更がデバイスにプッシュされない
CSCvk06386	ファイル ポリシー判定にかかわらず、FTD ファイルが複数の既存の接続を介して許可される
CSCvm00066	ASA が「フラッシュからの読み取り中」に数時間にわたってスタックする
CSCvm16724	FXOS ASA/FTD には内部データ インターフェイス カウンタをポーリングするための手段が必要
CSCvm35373	設定が原因でプルーニング プロセスの開始に失敗する
CSCvm62846	TID の復元 | 設定のみのバックアップに失敗しました
CSCvm86008	ポリシーの展開：デルタ設定が実行コンフィギュレーションにコピーされないため LINA 設定が変更されないままになる
CSCvn07452	インライン セットをタップからインラインに切り替えると 712x デバイスが不安定になる
CSCvn09383	「www.」の部分なしで同じ URL が 2 回目に入力されると手動 URL ルックアップで Uncategorized が返される
CSCvn25949	ASA への REST API イメージのアップロード中にデジタル署名の検証に失敗した
CSCvn30108	ASAv での「show memory」 CLI 出力が正しくない
CSCvn31347	ACL：アクセスグループの設定エラー後に ACL を設定できない
CSCvn38453	ASA：FIPS が有効な場合に Quovadis ルート証明書をトラストポイントとしてロードできない

不具合 ID	タイトル
CSCvn44222	6.3.0-79：HA のアップグレードまたはセカンダリの RAVPN diskfiles の欠落により展開が失敗する
CSCvn49854	後続の HTTP 要求が URL と XFF を取得しない
CSCvn67137	NetFlow の使用時に ASA5506 が徐々にメモリ リークを起こすことがある
CSCvn67570	amp-stunnel.conf が FMC のアップグレード後に正しい amp クラウド サーバを指さない
CSCvn68527	KP：AnyConnect がプールから使用している IP が使用可能と表示される
CSCvn71592	FMC の再起動後、Snort によって生成された侵入イベントが FMC に送信されず、webGUI に表示される
CSCvn74112	FTDv には vmxnet3 と ixgbevf インターフェイスが混在した初期起動の設定がない
CSCvn75368	FPR プラットフォームの IPsec VPN が断続的にダウンする
CSCvn78593	FTD でコントロール プレーン ACL が正しく機能しない
CSCvn78870	範囲外の allocate-interface コマンドによるASA マルチコンテキストのトレースバックとリロード
CSCvn82895	Diskmanager がすべてのイベント ファイルを追跡しない場合がある
CSCvn87965	FMC を TG アカウントに関連付ける際に FMC がユーザを TG コンソールにリダイレクトすることはできない
CSCvn95711	スレッド名のトレースバック：IKEV2 ipsec-proposal にプロトコルを追加した後の Unicorn Admin ハンドラ
CSCvn96898	SCP のダウンロードに伴って DMA_Pool で生じるバイナリ サイズ 1024 のメモリ リーク
CSCvn99712	Cisco Firepower Management Center のクロスサイト スクリプティングの永続的な脆弱性
CSCvo02097	ASA クラスタを 9.10.1.7 にアップグレードするとトレースバックが生じる
CSCvo04444	Ikev2 トンネルの作成に失敗する
CSCvo06216	CSCuz22961 の hanover におけるスプリット DNS-コミットの問題に対する 255 文字以上のサポート
CSCvo09046	ASA クラスタを 9.10.1.7 にアップグレードするとメモリ不足が生じる
CSCvo13497	「log default」キーワードのあるアクセスリストを削除できない

不具合 ID	タイトル
CSCvo19247	アウトバウンド SSL パケットの処理中のトレースバック
CSCvo21210	PDTS の numa ノード情報が正しくないためロード バランシングが正しく行われない
CSCvo23222	マルチコンテキスト展開でのリソースの問題により AnyConnect セッションが拒否される
CSCvo23366	適応型プロファイリングの設定ファイルが破損しているため展開に失敗した
CSCvo27109	9.6(4)6 から 9.6(4)20 へのアップグレード時にスタンバイがリブート ループに陥ることがある
CSCvo29973	暗号スイート条件がある ssl ルールにより不要な tls 1.3 ダウングレードが発生する可能性がある
CSCvo31353	URL カテゴリが使用され、証明書の共通名が一致しない場合、SSL 接続が失敗する可能性がある
CSCvo39094	展開するデバイスを選択した後、ポリシー展開タスクを挿入するための処理時間が遅延する/長くなる
CSCvo40210	ダッシュボード ウィジェットでの Talos RSS フィードの更新
CSCvo42174	ASA IPSec VPN EAP が PKI の有効な証明書をロードできない
CSCvo42884	6.3 へのアップグレード後に、FTD でサイト間 VPN を変更できない
CSCvo43693	複数のファイル modules*.tgz および vdb*.tgz が FMC から転送されるため FTD HA の作成が失敗する
CSCvo44064	sni がないため url ルックアップが保留中の際にアグレッシブ ダウングレード アクションが実行される
CSCvo45209	FTD - クラスタ：クラスタに新しいユニットを追加するとトラフィックのドロップが発生する場合がある
CSCvo45675	FMC アップグレード プロセスでは、アップグレード後に無効になる設定を確認する必要がある
CSCvo50230	未分類の URL への SSL 接続が繰り返し失敗する場合がある
CSCvo55151	VTI が存在する場合に crypto ipsec inner-routing-lookup の設定を許可しないようにする必要がある
CSCvo55282	ユーザが AC ルールに無効なインライン ポート範囲を誤って入力できるとポリシーの展開が失敗する

不具合 ID	タイトル
CSCvo56675	フェールオーバー状態の変更または xlate のクリアを原因とする ASA または FTD のトレースバックとリロード
CSCvo56895	コンテキスト エクスプローラの一部のドーナツ グラフのロードに失敗する
CSCvo61091	NAP ポリシー メタデータを送信する際の eStreamer メモリおよび CPU 使用率の増大
CSCvo63168	Sybase 接続に障害が発生した場合の temp_id リーク
CSCvo63232	UIMP が、子ドメインに存在するレルムからユーザを更新しない
CSCvo63240	アップグレード後にスマート トンネルのブックマークが機能せず証明書エラーとなる
CSCvo67454	無効なポート範囲オブジェクトにより AC ポリシーの展開が失敗する
CSCvo72238	FTD クラスタがドメインで管理され、サブドメインの AC ポリシーが割り当てられると、FMC バックアップが失敗する
CSCvo74743	プライマリの子ドメインに対する FMC-HA の変更がセカンダリの ADI.conf に反映されない

バージョン 6.3.0.2 で解決済みの問題

Table 38: バージョン *6.3.0.2* で解決済みの問題

不具合 ID	タイトル
CSCuz28594	Diskmanager：Diskmanager が 99 % までプルーニングしないため /var/storage で重大なアラートが発生する
CSCvh26064	7000/8000 センサーで「変更調整」を使用できない
CSCvi28763	FTD プラットフォーム設定：SSL カスタム設定のデフォルト DH グループを 2 に変更する
CSCvi34533	SNMPv3 ユーザが定義されていない場合、アクセス リストで変更を保存できない
CSCvi55841	ブラックリスト設定ファイルの保存エラーが検出されない
CSCvk16876	トラフィックが誤ったアクセスコントロールルールに一致する

不具合 ID	タイトル
CSCvk31472	スマートライセンスロギングで syslog が汚染され、ログの高速ローテーションが発生する
CSCvk40964	空のインターフェイス設定をデバイスに展開するとトラフィックが停止する
CSCvm14875	多数の古い cloudconfig EO がパフォーマンスの問題を引き起こす
CSCvm24210	同じタイムスタンプで実行されている 2 つのスケジュール タスクが同じファイルにアクセスするとスケジュール タスクの 1 つが失敗する
CSCvm40545	FTD を 2 回連続してダウングレードすると（2 回のダウングレード間で更新せずに）誤った lina バージョンになる
CSCvm58799	展開中に複数の Snort が応答しない場合、リカバリに時間がかかりすぎる
CSCvm60039	カスタム DNS セキュリティ インテリジェンス フィードのダウンロードに断続的に失敗する
CSCvm60548	セキュリティ インテリジェンスの同期タスクが失敗する
CSCvm66743	[ドメイン（Domain）] ページでスケール設定をロードするのに時間がかかる
CSCvm87892	夜間にトラフィックがソーキングすると、snort の sftls クラッシュが検出される
CSCvn10634	順序が正しくない（実際のデータの前に ACK がある）場合、HTTP フローでファイルが検出されない
CSCvn16102	Diskmanager のファイル キャプチャ データが数時間にわたって同時に増加しない
CSCvn17347	CPU プロファイリング結果表示時のトレースバックとリロード
CSCvn19074	MSP：CIP Write アプリケーションのリセットでブロックするアクセス制御ルールがブロックしない
CSCvn38010	remove_peers.pl スクリプトが FTD で実行されている場合、このスクリプトを終了する
CSCvn38082	FMC は mongo の破損を特定して回復する必要がある
CSCvn38189	バックアップ スクリプトの終了後に SFDataCorrelator が再起動されない
CSCvn41903	dce2-mem-reloader のメモリ調整に時間がかかりすぎるため Snort のリロードが失敗して再起動が発生する

不具合 ID	タイトル
CSCvn43798	ドメインを削除しても、レルムがそのドメイン内にある場合、一部のオブジェクトの削除に失敗する
CSCvn46474	FP2120 FTD が停電後に応答しなくなった
CSCvn47788	Firepower プラットフォーム設定ポリシーの監査ログ ホストの有効なホスト名 IP で UI 検証が失敗する
CSCvn48739	CLISH モードおよびトラブルシューティングで取得された FTD show tech は省略されている場合がある
CSCvn48790	ポリシーの適用中に SI タスクが実行されている場合、スレーブノードがクラスタから退出する
CSCvn49561	CA パスを使用するための FireAMP curl コールの更新
CSCvn53145	ポリシーの展開で「Variable set has invalid execulded values」がスローされた
CSCvn65575	アクティブ認証が有効になっていて、SSL ポリシーが有効になっていない場合、Snort が終了する可能性がある
CSCvn67888	REST API を使用してオブジェクトを追加するとポリシーの展開に失敗する
CSCvn68145	SSL 復号化を使用しているときに Snort が予期せず終了する
CSCvn69019	単一引用符で囲まれたユーザ名は user_ip_map ファイルに書き込まれない
CSCvn72650	6.3.0 リリースでの FTD アドレスがマッピングされないトレースバック
CSCvn72683	FMC webGUI の [Device Management] ページのロード時間が長すぎる（約 45 秒、ライセンスの取得に 25 秒）
CSCvn73244	6.3 へのアップグレード後、anyconnect-custom-attr のために RA VPN ポリシーを展開できない
CSCvn76046	6.3 へのアップグレード後、「"」文字を含む事前共有キーが展開されない
CSCvn76783	syslog サーバへのロギングが有効になっているモニタ ルールが、サーバへの接続イベントをレポートしない
CSCvn77285	6.3 へのアップグレード後、SI ヘルス アラートが不正確になる
CSCvn93499	Snort/データ コリレータは Firepower 4100/9300 デバイスで終了するときにクラッシュする可能性がある
CSCvo00887	「Do Not Decrypt」ルールが可能な唯一の判定である場合、ssl クライアント hello を変更することはできない

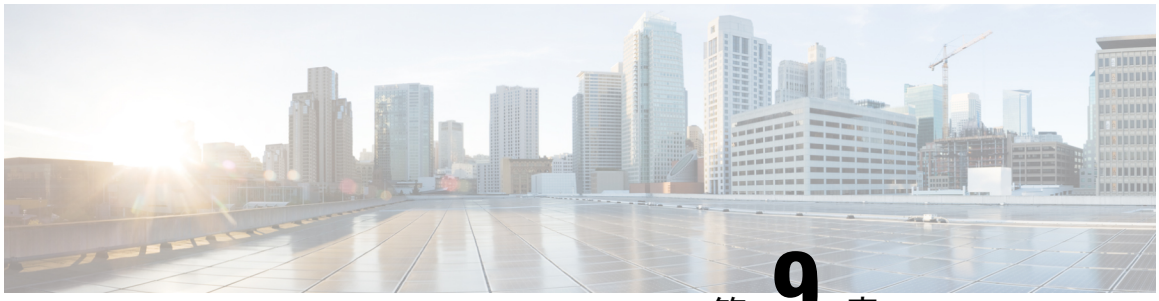
不具合 ID	タイトル
CSCvo03186	Firepower Management Center の [Domain] ページのロードに時間がかかりすぎる
CSCvo03808	OOM が原因で FMC からの展開が失敗し、理由が示されない
CSCvo11077	新しい IKEv1 トンネルを確立して終了すると IPsec でメモリ リークが検出される
CSCvo15484	ユーザ情報が mysql と sybase 間で一致しない場合、ユーザ IOC を削除できない（部分的に修正）
CSCvo23150	ユーザ ID に対する過剰な DB クエリによりユーザ セッションの処理が遅くなる
CSCvo27164	SFDataCorrelator が不適切な「Resuming storage of old events」メッセージをログに記録する
CSCvo32329	削除されたレルムが原因で多くの user_id が user_identities キャッシュにロードされる
CSCvo56616	展開がタイムアウトする場合があり非終端 AQ が発生する

バージョン 6.3.0.1 で解決済みの問題

不具合 ID	タイトル
CSCuy90400	SSL で Extended Master Secret をサポートするための機能強化
CSCva62256	500 台のセンサーがある場合、アプライアンス ステータス ウィジェットでのロードに時間がかかりすぎる
CSCvd03903	Firepower は TCP ダンプの脆弱性の影響を受ける
CSCvd12834	成功および失敗した SSH 認証試行が FP 監査ログに記録されない
CSCve29930	HA ペアのセカンダリ FMC で LOM を設定できない
CSCvf20266	Firepower Management Center システム設定の電子メール通知のパスワードの長さが短すぎる
CSCvh13022	クライアント hello ペイロードが 6 バイト未満の場合、SSL 復号がバイパスされる
CSCvi97028	到達不能な syslog サーバを設定すると fmc GUI が低速になる
CSCvi97500	Firepower Management Center の AMP クラウド イベントが異なるファイル タイプで認識される

不具合 ID	タイトル
CSCvj65154	プロキシ パスワードに @ 文字が含まれている場合、FMC が SSM との通信に失敗する
CSCvj74643	AD で CAC 認証および認可の使用を有効にすると RADIUS が変更時に切断される
CSCvj87287	FMC に対する REST-API 要求の同時フラッドによりアクセス不能になる
CSCvj97229	FMC の CAC の外部認証オブジェクトには「ユーザ名テンプレート」が必要
CSCvk19946	キャッシュ アーカイブ データのフラッディングにより Sftunnel サービスが停止する
CSCvk39339	日本語の FMC でスケジューリング レポートの生成を実行できない
CSCvk55634	ポリシー展開の通知がスタックしているためランダムなポリシー展開に失敗する
CSCvk56988	Cisco ClamAV MEW アンパッカーの Denial of Service（DoS）脆弱性
CSCvm46014	FTD HA でスタンバイ デバイスが破損している場合、設定のコピーに失敗できない
CSCvm47713	Chrome ブラウザが使用されている場合、SSL ポリシーは *.lightning.force.com での PDF の表示を許可しない
CSCvm59983	ファイルサイズ ディレクティブが無効な入力エラーを返し、clish からのキャプチャを中断する
CSCvm64230	verify_firmwareRunning() 戻りコードがチェックされない
CSCvm76760	FMC - 外部 RADIUS 認証 - [Shell Access Filter] フィールドのテキストが検証されない
CSCvm80933	サーバがワイルドカードの共通名を持つ証明書を使用する場合、SSL ポリシーが誤ったルールと一致する可能性がある
CSCvm87315	RegistrationTR::addToLamplighter の TID が原因で FTD 登録が失敗する可能性がある
CSCvm91280	侵入イベント レポートの日付、時間、曜日が UTC で、時刻がローカル タイムゾーンになる
CSCvm96339	archive_cache_seed.sensor ファイルが原因で /dev/root パーティションが 100 % になる
CSCvn03507	後続の展開で「set ip next-hop verify-availability」が正しく適用されない

不具合 ID	タイトル
CSCvn05797	Cisco Firepower Management Center のクロスサイト スクリプティングの脆弱性
CSCvn06618	LINA 設定のロールバックではスタートアップ コンフィギュレーションがデフォルトの実行とマージされる
CSCvn08146	x509 証明書およびキーへの変更に関する監査の詳細が欠落している
CSCvn14650	Linux カーネルの解放済みメモリ使用競合状態の脆弱性
CSCvn16489	AMP 動的分析のクラウドを送信レートに対して個別に追跡する必要がある
CSCvn19289	curl の複数の脆弱性
CSCvn20411	エラー メッセージの後、[Device Management] ページがロードされず、タイムアウトする
CSCvn21899	Firepower：SFTunnel 通信のために TLS 1.0 を永続的に無効にする
CSCvn23701	ftp_telnet.conf(4) => Invalid keyword 'memcap' for 'global' configuration により展開に失敗する
CSCvn30118	mysql-server.err ファイルが完全に削除されず、Firepower のディスク容量を消費し続ける
CSCvn31753	SSL インスペクション ポリシーによって SEC_ERROR_REUSED_ISSUER_AND_SERIAL ブラウザ エラーが発生する場合がある
CSCvn31793	FMC 接続イベントで 1.2 としてレポートされた TLS 1.3 接続
CSCvn36393	stunnel 設定ファイルで tls1.0 および tls1.1 を除外する
CSCvn46121	デフォルト アクションが syslog に記録される場合、セキュリティ インテリジェンス IP モニタ イベントが syslog に送信されない
CSCvn53131	FMC アップグレード後のポリシー適用中の snort 検証エラー
CSCvn53732	復号されていない SSL 接続を変更した場合、この接続を閉じる必要がある
CSCvo02577	SSL HW 復号化によるバッファ枯渇
CSCvo11743	最後のバッチが完全に 100% の場合、fpreplication スナップショット ストリーミングがループする



第 9 章

既知の問題

既知の問題については、次を参照してください。

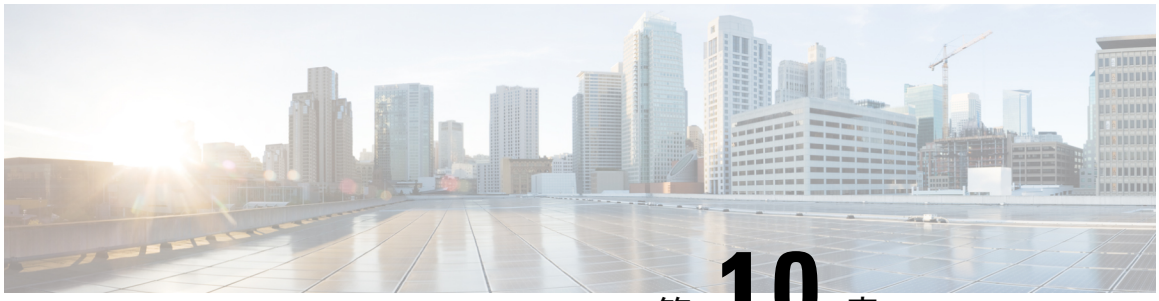
- 既知の問題の検索 （83 ページ）

既知の問題の検索

サポート契約がある場合は、Cisco Bug Search Tool を使用して Firepower 製品の最新のオープンバグリストを取得することができます。これらの一般的なクエリには、バージョン 6.3.0.x パッチを実行している Firepower 製品の未解決のバグが表示されます。

- Firepower Management Center
- Firepower Management Center Virtual
- ASA with FirePOWER サービス
- NGIPSv

検索では、特定の Firepower プラットフォームとバージョンに影響するバグに絞り込むことができます。バグ ID ごとに検索したり、特定のキーワードを検索することもできます。



第 10 章

支援が必要な場合

Firepower をお選びいただき、ありがとうございます。

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、Firepower 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。

- 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 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