Cisco Firepower バージョン 6.7.x パッチ リリースノート

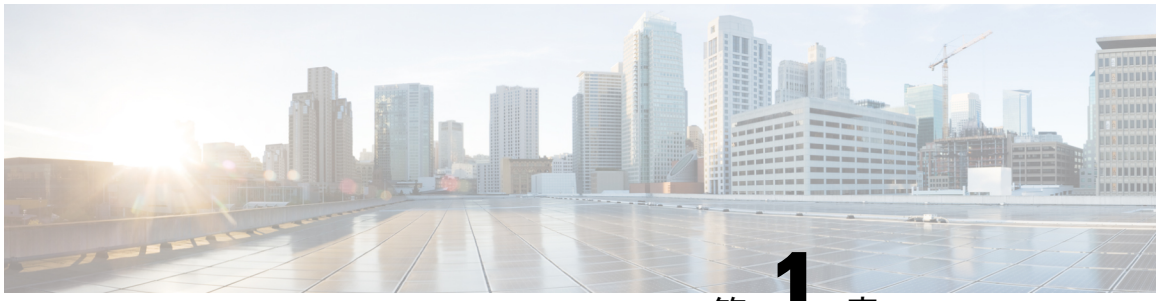
初版：2021 年 3 月 24 日

最終更新：2022 年 5 月 2 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

ようこそ

このドキュメントでは、以下に示す Version6.7 のリリース情報を記載しています。

- Cisco Firepower Threat Defense
- Cisco Firepower Management Center
- Cisco Firepower Device Manager
- Cisco Firepower 従来型デバイス：Firepower 7000/8000 シリーズ、NGIPSv、および ASA with FirePOWER Services

このドキュメントでは、ハードウェアと仮想アプライアンスについて説明します。Cisco Defense Orchestrator（CDO）で Firepower Threat Defense を管理している場合は、Cisco Defense Orchestrator の新機能 も参照してください。

リリースの主なポイント

FDM 展開向け Snort 3

新規に FTD を展開する場合、Snort 3 がデフォルトの検査エンジンになります。アップグレードされた展開では引き続き Snort 2 が使用されますが、いつでも切り替えることができます。詳細については、Snort 3.0 の Web サイト（https://snort.org/snort3）を参照してください。

リリース日

表 *1*: バージョン *6.7* のリリース日

バージョン	ビルド	日付	プラットフォーム
6.7.0.3	105	2022-02-17	すべて
6.7.0.2	24	2021 年 5 月 11 日	すべて
6.7.0.1	13	2021 年 3 月 24 日	すべて
6.7.0	65	2020 年 11 月 2 日	すべて

推奨リリース

新しい機能と解決済みの問題を利用するには、対象となるすべてのアプライアンスを推奨リリース以上にアップグレードすることをお勧めします。シスコ サポートおよびダウンロードサイトでは、推奨リリースに金色の星が付いています。

また、新機能ガイドにも推奨リリースを示します。

- Cisco Firepower Management Center の新機能（リリース別）
- Cisco Firepower Device Manager の新機能（リリース別）

古いアプライアンスの推奨リリース

アプライアンスが古すぎて推奨リリースを実行できず、ハードウェアを今すぐ更新しない場合は、メジャーバージョンを選択してから可能な限りパッチを適用します。一部のメジャーバージョンは長期または超長期に指定されているため、いずれかを検討してください。これらの用語の説明については、「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」を参照してください。

ハードウェアの更新に関心がある場合は、シスコの担当者またはパートナー担当者にお問い合わせください。

シスコとのデータの共有

次の機能はシスコとデータを共有します。

Cisco Success Network

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。

初期設定およびアップグレード中に、登録するか尋ねられます。登録はいつでも変更できます。

Cisco Support Diagnostics

Cisco Support Diagnostics（「シスコのプロアクティブサポート」とも呼ばれる）は、設定および運用上の健全性データをシスコに送信し、自動化された問題検出システムを通じてそのデータを処理して問題をプロアクティブに通知できるようにします。また、この機能により、Cisco TACTAC ケースの過程でデバイスから必要な情報を収集することもできます。

初期設定およびアップグレード中に、登録するか尋ねられます。登録はいつでも変更できます。この機能は FDM で現在サポートされていません。

Web 分析トラッキング

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、ユーザーの場所、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。

デフォルトで登録されていますが、初期設定の完了後にいつでも登録を変更できます。

サポートが必要な場合

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。

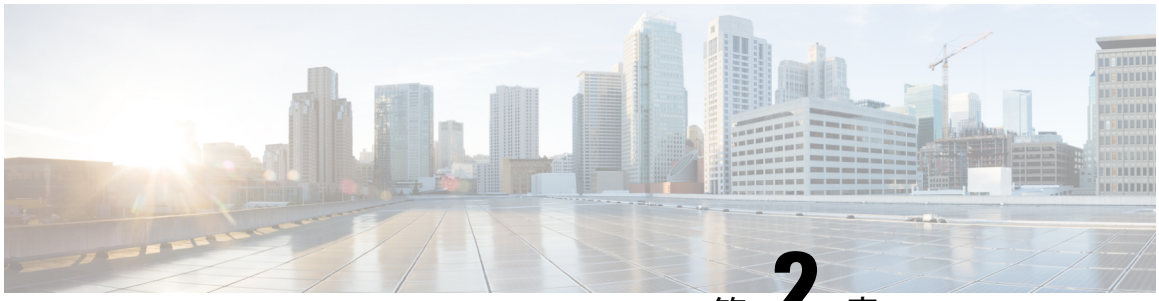
- マニュアル：http://www.cisco.com/jp/go/threatdefense-67-docs
- シスコ サポートおよびダウンロード サイト：https://www.cisco.com/c/en/us/support/index.html
- Cisco Bug Search Tool：https://tools.cisco.com/bugsearch/
- シスコ通知サービス：https://www.cisco.com/cisco/support/notifications.html

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、Version6.7 のシステム要件を記載します。

デバイスのプラットフォーム

Cisco Firepower デバイスは、ネットワークトラフィックをモニターし、定義された一連のセキュリティルールに基づいて特定のトラフィックを許可するかブロックするかを決定します。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。一部のデバイスはいずれかのソフトウェアを実行できますが、両方を同時に実行することはできません。

（注） これらのリリースノートには、本リリースでサポートされているデバイスが掲載されています。古いデバイスがEOLに達していて、アップグレードできなくなった場合でも、数バージョンの範囲内であれば、より新しいFMCを使用してそのデバイスを管理できます。同様に、より新しいバージョンのASDMでは、より古いバージョンのASA FirePOWERモジュールを管理できます。下位互換性を含む、サポート対象の管理方法については、「マネージャとデバイスの互換性 （9 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 または Cisco Firepower Classic Device 互換性ガイド を参照してください。

表 *2 :* バージョン *6.7.0/6.7.x* の *Firepower Threat Defense*

FTD プラットフォーム	OS/ハイパーバイザ	詳細情報
Firepower 1010、1120、1140、1150 Firepower 2110、2120、2130、2140	—	—
Firepower 4110、4120、4140、4150 Firepower 4112、4115、4125、4145 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	FXOS 2.9.1.131 以降のビルド	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 FXOS Release Notes, 2.9(1)』を参照してください。
ASA 5508-X、5516-X ISA 3000	—	FTD 展開では、これらのデバイスのオペレーティングシステムを個別にアップグレードすることはありませんが、 に最新の ROMMON イメージがあることを確認する必要があります。Cisco ASA and Firepower Threat Defense Reimage Guide

FTD プラットフォーム	OS/ハイパーバイザ	詳細情報
Firepower Threat Defense Virtual（FTDv）	次のいずれかです。 • AWS：Amazon Web Services • Azure：Microsoft Azure • GCP：Google Cloud Platform • OCI：Oracle Cloud Infrastructure • KVM：カーネルベースの仮想マシン • VMware vSphere/VMware ESXi 6.0、6.5、または 6.7	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。

表 *3 :* バージョン *6.7.0/6.7.x* の *NGIPS/ASA FirePOWER*

NGIPS/ASA FirePOWER プラットフォーム	OS/ハイパーバイザ	詳細情報
ASA 5508-X、5516-X ISA 3000	ASA 9.5(2) ～ 9.16(x)	ASA と ASA FirePOWER のバージョンには幅広い互換性があります。ただし、アップグレードすると、新機能を利用でき、問題も解決されます。操作の順序については、『Cisco ASA Upgrade Guide』を参照してください。 また、最新の ROMMON イメージがあることも確認してください。Cisco ASA and Firepower Threat Defense Reimage Guide
NGIPSv	VMware vSphere/VMware ESXi 6.0、6.5、または 6.7	サポートされているインスタンスについては、『Cisco Firepower NGIPSv Quick Start Guide for VMware』を参照してください。

FMC プラットフォーム

このドキュメントには、Version6.7 でサポートされている FMC が記載されています。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。

FMC ハードウェア

Version6.7 は次の FMC ハードウェアをサポートします。

- FMC 1600、2600、4600
- FMC 1000、2500、4500

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 Firepower ホットフィックス リリース ノート を参照）。

FMCv

FMCv 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。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 Getting Started Guide を参照してください。

表 *4 : Version6.7 FMCv* プラットフォーム

プラットフォーム（Platform）	FMCv2、10、25	FMCv300
オンプレミス/プライベート プラットフォーム		
カーネルベース仮想マシン（KVM）	**YES**	—
VMware vSphere/VMware ESXi 6.0、6.5、または 6.7	**YES**	**YES**
パブリック クラウド プラットフォーム		
Amazon Web Services（AWS）	**YES**	—
Google Cloud Platform（GCP）	**YES**	—
Microsoft Azure	**YES**	—
Oracle Cloud Infrastrucure（OCI）	**YES**	—

マネージャとデバイスの互換性

Firepower Management Center

すべてのデバイスが Firepower Management Center を使用した遠隔管理をサポートしており、これにより複数のデバイスを管理することができます。FMC 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。FMC 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 FMC をアップグレードする必要があります。

新しい FMC では、次の表に示されている複数のメジャーバージョンまで遡って古いデバイスを管理できます。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、FMC 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。

表 *5 : FMC*とデバイス間の互換性

FMC バージョン	管理可能な最も古いデバイスバージョン
6.7.x	6.3.0
6.6.x	6.2.3
6.5.0	6.2.3
6.4.0	6.1.0
6.3.0	6.1.0
6.2.3	6.1.0

Firepower Device ManagerおよびCisco Defense Orchestrator

FMC に代わるものとして、多くの FTD デバイスが Firepower Device Manager および Cisco Defense Orchestrator の管理をサポートします。

- Firepower Device Manager が FTD に内蔵されており、単一のデバイスを管理できます。

  これにより、小規模または中規模ネットワークで最も一般的に使用されるソフトウェアの基本機能を設定できます。

- Cisco Defense Orchestrator（CDO） はクラウドベースであり、複数の FTD デバイスを管理できます。

  これにより、FMC を使用せずに展開全体で一貫したセキュリティポリシーを確立して維持できます。一部の構成では引き続き FDM が必要ですが、CDO を使用すると、複数の FTD デバイスで一貫したセキュリティポリシーを確立して維持できます。

FDM を使用したローカル管理をサポートするすべての FTD デバイスは、CDO も同時にサポートします。

表 *6 : FTD* との *FDM* および *CDO* の互換性

FTDプラットフォーム	FDM 互換	CDO 互換
Firepower 1000 シリーズ	6.4.0 以降	6.4.0 以降
Firepower 2100 シリーズ	6.2.1 以降	6.4.0 以降
Firepower 4100/9300	6.5.0 以降	6.5.0 以降
ASA 5500-X シリーズ	6.1.0 ～ 7.0.x	6.4.0 ～ 7.0.x
ISA 3000	6.2.3 以降	6.4.0 以降
AWS 用 FTDv	6.6.0 +	6.6.0 +
Azure 用 FTDv	6.5.0 以降	6.5.0 以降
GCP 用 FTDv	—	—
KVM 用 FTDv	6.2.3 以降	6.4.0 以降
OCI 用 FTDv	—	—
FTDv VMware の場合	6.2.2 以降	6.4.0 以降

Adaptive Security Device Manager

ASA with FirePOWER Services は、Firepower NGIPS ソフトウェアを個別のアプリケーションとして実行する ASA ファイアウォールであり、ASA FirePOWER モジュールとも呼ばれています。Cisco Adaptive Security Device Manager（ASDM）を使用して両方のアプリケーションを管理できます。

ほとんどの場合、新しい ASDM のバージョンは以前のすべての ASA のバージョンと下位互換性があります。ただし、いくつか例外があります。たとえば、ASDM 7.13(1) は ASA 9.10(1) で ASA 5516-X を管理できます。ASDM 7.13(1) と 7.14(1) は、ASA 5512-X、5515-X、5585-X、および ASASM をサポートしていませんでした。そのため、ASDM 7.13(1.101) または 7.14(1.48) にアップグレードして ASDM のサポートを復元する必要があります。詳細は、『Cisco ASA の互換性』を参照してください。

新しい ASA FirePOWER モジュールには、次の表に示されている新しいバージョンの ASDM が必要です。

表 *7 : ASDM* と *ASA FirePOWER* の互換性

ASA FirePOWER のバージョン	最小 ASDM バージョン
6.7.x	7.15.1
6.6.x	7.14.1
6.5.0	7.13.1

ASA FirePOWER のバージョン	最小 ASDM バージョン
6.4.0	7.12.1
6.3.0	7.10.1
6.2.3	7.9.2

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 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。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（Interface）	最小解像度
FMC	1280 X 720

インターフェイス（**Interface**）	最小解像度
FDM	1024 X 768
ASA FirePOWER moduleを管理している ASDM	1024 X 768
Firepower 4100/9300 用 Firepower 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手順は、次のとおりです。

- FMC：**[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：[Device] をクリックしてから **[System Settings]** > **[Management Access]** リンクをクリックし、次に [Management Web Server）] タブをクリックします。

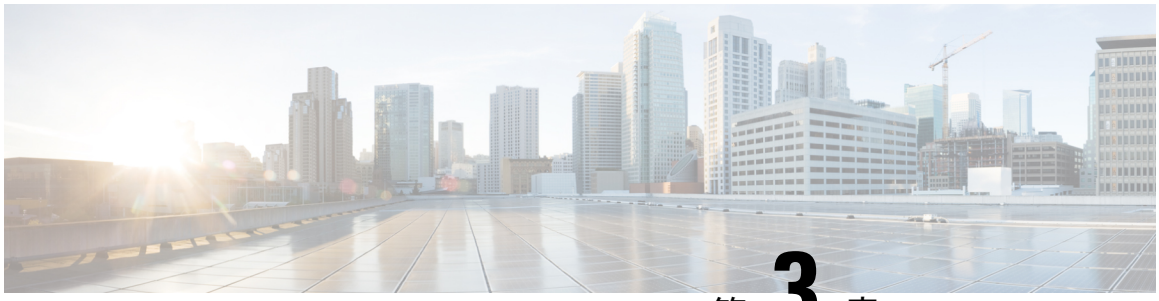
詳しい手順については、オンラインヘルプまたはご使用の製品のコンフィギュレーション ガイドを参照してください。

（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

特長と機能

このドキュメントでは、Version6.7の新機能と廃止された機能について説明します。また、アップグレードによる影響についても言及します。

重要 新規および廃止された機能が原因で、アップグレード前またはアップグレード後の設定変更が必要になったり、アップグレードができなかったりする場合があります。アップグレードでバージョンがスキップされる場合は、リリースノートで履歴情報とアップグレードの影響を確認するか、該当する『New Features by Release』のガイドを参照してください。

新機能

FMC バージョン 6.7 の新機能

新しい FMC で古いデバイスを管理できますが、常に環境全体を更新することを推奨します。新しいトラフィック処理機能では、FMC とデバイスの両方で最新のリリースが前提条件となります。 デバイスが明らかに関与していない機能（Web インターフェイスの外観の変更、クラウド統合）では、FMC の最新バージョンのみを必須条件としているにもかかわらず、それが保証されない場合があります。新機能の説明では、バージョンの要件が標準で想定される条件から逸脱している場合は明示しています。

表 *8 : FMC* バージョン *6.7.0* の新機能

機能	説明
プラットフォーム機能	

機能	説明
VMware 向け FMCv での高可用性のサポート。	VMware 向け FMCv は、高可用性をサポートするようになりました。ハードウェアモデルの場合と同様に、FMCv Web インターフェイスを使用して HA を確立します。 FTD の展開では、2 つの同一ライセンスの FMCv と、各管理対象デバイスに 1 つの FTD 権限が必要です。たとえば、FMCv10 HA ペアで 10 台の FTD デバイスを管理するには、2 つの FMCv10 権限と 10 の FTD 権限が必要です。クラシックデバイス（7000/8000 シリーズ、NGIPSv、ASA FirePOWER）のみを管理している場合は、FMCv 権限は必要ありません。 この機能は、VMware 向け FMCv 2（つまり、2 つのデバイスのみ管理するようにライセンスされた FMCv）ではサポートされていません。 サポートされるプラットフォーム：VMware 向け FMCv 10、25、および 300
AWS 向け FTDv の自動スケールの改善。	バージョン 6.7.0 には、AWS 向け FTDv の次の自動スケールの改善が含まれています。 • カスタム指標パブリッシャ。新しい Lambda 関数は、自動スケールグループ内のすべての FTDv インスタンスのメモリ消費量について FMC を毎秒ポーリングし、その値を CloudWatch メトリックにパブリッシュします。 • メモリ消費に基づく新しいスケーリングポリシーを使用できます。 • FMC への SSH およびセキュアトンネル用の FTDv プライベート IP 接続。 • FMC の設定検証。 • ELB でより多くのリスニングポートを開くためのサポート。 • シングルスタック展開に変更。すべての Lambda 関数と AWS リソースは、合理化された展開のためにシングルスタックから展開されます。 サポートされているプラットフォーム：AWS の FTDv
Azure 向け FTDv の自動スケールの改善。	Azure 向け FTDv の自動スケール ソリューションには、CPU だけでなく、CPU とメモリ（RAM）に基づくスケーリングメトリックのサポートが含まれるようになりました。 サポートされているプラットフォーム：Azure の FTDv

機能	説明
Firepower Threat Defense：デバイス管理	
データインターフェイスでの FTD の管理。	専用の管理インターフェイスではなく、データインターフェイス上の FTD の FMC 管理を設定できるようになりました。 この機能は、本社の FMC からブランチオフィスの FTD を管理し、外部インターフェイスで FTD を管理する必要がある場合に、リモート展開に役立ちます。DHCP を使用して FTD でパブリック IP アドレスを受信する場合は、オプションで Web タイプの更新方式を使用して、インターフェイスのダイナミック DNS（DDNS）を設定できます。DDNS は、FTD の IP アドレスが変更された場合に FMC が完全修飾ドメイン名（FQDN）で FTD に到達できるようにします。 （注） データインターフェイスでの FMC アクセスは、クラスタリングまたはハイアベイラビリティではサポートされません。 新規/変更されたページ： • **[デバイス（Devices）] > [デバイス管理（Device Management）] > [デバイス（Device）] > [管理（Management）]** セクション • **[デバイス（Devices）] > [デバイス管理（Device Management）] > [インターフェイス（Interfaces）] > [FMCアクセス（FMC Access）]** • **[デバイス（Devices）] > [デバイス管理（Device Management）] > [DHCP] > [DDNS] > [DDNS更新方式（DDNS Update Methods）]** ページ 新規/変更された FTD CLI コマンド：**configure network management-data-interface**、**configure policy rollback** サポートされるプラットフォーム：FTD
FTD での FMC IP アドレスの更新。	FMC IP アドレスを変更する場合に、FTD CLI を使用してデバイスを更新できるようになりました。 新規/変更された FTD CLI コマンド： **configure manager edit** サポートされるプラットフォーム：FTD

機能	説明
Firepower 4100/9300 の FTD 動作リンク状態と物理リンク状態の同期。	Firepower 4100/9300 シャーシでは、FTD 動作リンク状態をデータインターフェイスの物理リンク状態と同期できるようになりました。 現在、FXOS 管理状態がアップで、物理リンク状態がアップである限り、インターフェイスはアップ状態になります。FTD アプリケーション インターフェイスの管理状態は考慮されません。FTD からの同期がない場合は、たとえば、FTD アプリケーションが完全にオンラインになる前に、データインターフェイスが物理的にアップ状態になったり、FTD のシャットダウン開始後からしばらくの間はアップ状態のままになる可能性があります。インラインセットの場合、この状態の不一致によりパケットがドロップされることがあります。これは、FTD が処理できるようになる前に外部ルータが FTD へのトラフィックの送信を開始することがあるためです。 この機能はデフォルトで無効になっており、FXOS の論理デバイスごとに有効にできます。 （注） この機能は、クラスタリング、コンテナインスタンス、または Radware vDP デコレータを使用する FTD ではサポートされません。ASA でもサポートされていません。 新規/変更された [Firepower Chassis Manager] ページ：[論理デバイス（Logical Devices）]>[リンク状態の有効化（Enable Link State）] 新規/変更された FXOS コマンド：**set link-state-sync enabled**、**show interface expand detail** サポートされるプラットフォーム：Firepower 4100/9300

機能	説明
Firepower 1100/2100 シリーズの SFP インターフェイスで、自動ネゴシエーションの無効化がサポートされるようになりました。	**アップグレードの影響。** フロー制御とリンク ステータス ネゴシエーションを無効化するように Firepower 1100/2100 シリーズ SFP インターフェイスを設定できるようになりました。 以前は、これらのデバイスで SFP インターフェイス速度（1000 または 10000 Mbps）を設定すると、フロー制御とリンク ステータス ネゴシエーションが自動的に有効になり、無効にはできませんでした。 [ネゴシエーションなし（No Negotiate）] を選択して、フロー制御とリンク ステータス ネゴシエーションを無効化できるようになりました。これにより、1 GB SFP インターフェイスまたは 10 GB SFP+ インターフェイスを設定しているかに関係なく、速度は 1000 Mbps に設定されます。10000 Mbps でネゴシエーションを無効化することはできません。 新規/変更されたページ：[デバイス（Devices）]>[デバイス管理（Device Management）] > [インターフェイス（Interfaces）] > [インターフェイスの編集（edit interface）] > [ハードウェア構成（Hardware Configuration）] > [速度（Speed）] サポートされるプラットフォーム：Firepower 1100/2100 シリーズ
Firepower Threat Defense：クラスタリング	
FMC の新しいクラスタ管理機能。	FMC を使用して、以前は CLI を使用する必要のあった次のクラスタ管理タスクを実行できるようになりました。 • クラスタユニットを有効または無効にします。 • [Device Management] ページからクラスタのステータスを表示します（ユニットごとの履歴とサマリーを含む）。 • ロールをコントロールユニットに変更します。 新規/変更されたページ： • [Devices] > [Device Management] > [More] メニュー • [Devices] > [Device Management] > [Cluster] > [General] エリア > [Cluster Live Status] リンク > [Cluster Status] サポートされるプラットフォーム：Firepower 4100/9300

機能	説明
クラスタ導入の高速化。	クラスタの展開がより迅速に完了するようになりました。また、ほとんどの導入の失敗も、より迅速に失敗します。 サポートされるプラットフォーム：Firepower 4100/9300

機能	説明
クラスタリングでの PAT アドレス割り当ての変更。PAT プールの [フラットなポート範囲（Flat Port Range）] オプションがデフォルトで有効になり、設定できなくなりました。	**アップグレードの影響。** PAT アドレスがクラスタのメンバーに配布される方法が変更されます。 以前は、アドレスはクラスタのメンバーに配布されていたため、PAT プールにはクラスタメンバーごとに少なくとも 1 つのアドレスが必要でした。制御は各 PAT プールアドレスを等しいサイズのポートブロックに分割し、それらをクラスタメンバーに配布するようになりました。各メンバーには、同じ PAT アドレスのポートブロックがあります。したがって、通常 PAT に必要な接続量に応じて、PAT プールのサイズを 1 つの IP アドレスにまで減らすことができます。 ポートブロックは、1024 ～ 65535 の範囲で 512 ポートのブロック単位で割り当てられます。オプションで、PAT プールルールを設定するときに、このブロック割り当てに予約ポート 1 ー 1023 を含めることができます。たとえば、単一ノードでは PAT プール IP アドレスあたり 65535 個の接続すべてを処理するのに対し、4 ノードクラスタでは、各ノードは 32 個のブロックを取得し、PAT プール IP アドレスあたり 16384 個の接続を処理できます。 この変更の一環として、スタンドアロンまたはクラスタ内での動作に関わりなく、すべてのシステムの PAT プールは、フラットなポート範囲 1024 ー 65535 を使用できるようになりました。以前は、[Flat Port Range] オプションを PAT プールルール（FTD NAT の [Pat Pool] タブ）で有効化することで、フラットな範囲を使用できました。[フラットなポート範囲（Flat Port Range）] オプションは無視され、PAT プールは常にフラットになります。必要に応じて [Include Reserved Ports] オプションを選択して、PAT プールに 1 ー 1023 のポート範囲を含めることができます。 ポートブロック割り当てを設定する（[ブロック割り当て（Block Allocation）] PAT プールオプション）と、デフォルトの 512 ポートブロックではなく、独自のブロック割り当てサイズが使用されます。また、クラスタ内のシステムの PAT プールに拡張 PAT を設定することはできません。 この変更は自動的に有効になります。アップグレードの前後に何もする必要はありません。 サポートされるプラットフォーム：FTD
Firepower Threat Defense：暗号化と VPN	

機能	説明
RA VPN の AnyConnect モジュールサポート。	FTD RA VPN で AnyConnect モジュールがサポートされるようになりました。 RA VPN グループポリシーの一部として、ユーザーが Cisco AnyConnect VPN クライアントをダウンロードするときに、さまざまなオプションモジュールをダウンロードしてインストールするように設定できるようになりました。これらのモジュールは、Web セキュリティ、マルウェア保護、オフネットワークローミング保護などのサービスを提供できます。 各モジュールを、AnyConnect プロファイルエディタで作成され、AnyConnect ファイルオブジェクトとして FMC にアップロードされたカスタム設定を含むプロファイルに関連付ける必要があります。 新規/変更されたページ： • モジュールプロファイルのアップロード：新しい [File Type] オプションが [Objects] > [Object Management] > [VPN] > [AnyConnect File] > [Add AnyConnect File] に追加されました • モジュールの設定：[Client Modules] オプションが [Objects] > [Object Management] > [VPN] > [Group Policy] > [add or edit a Group Policy object] > [AnyConnect] 設定に追加されました サポートされるプラットフォーム：FTD
RA VPN の AnyConnect 管理 VPN トンネル。	FTD RA VPN は、エンドユーザーが VPN 接続を確立したときだけでなく、企業のエンドポイントの電源がオンになったときにエンドポイントへの VPN 接続を可能にする AnyConnect 管理 VPN トンネルをサポートするようになりました。 この機能は、オフィスネットワークに VPN を介してユーザーが頻繁に接続しないデバイスに対しては特に、外出中のオフィスのエンドポイントで管理者がパッチ管理を行うのに役立ちます。社内ネットワークの接続を必要とするエンドポイントオペレーティング システム ログイン スクリプトに対するメリットもあります。 サポートされるプラットフォーム：FTD

機能	説明
RA VPN のシングルサインオン。	FTD RA VPN は、 SAML 2.0 準拠のアイデンティティ プロバイダー（IdP）で設定されたリモートアクセス VPN ユーザーのシングルサインオン（SSO）をサポートするようになりました。 新規/変更されたページ： • SSO サーバーへの接続：[Objects] > [Object Management] > [AAA Server] > [Single Sign-on Server] • RA VPN の一部として SSO を設定します。RA VPN 接続プロファイルを設定する際に、認証方式（AAA 設定）として [SAML] を追加しました。 サポートされるプラットフォーム：FTD
RA VPN の LDAP 許可。	FTD RA VPN は、LDAP 属性マップを使用した LDAP 認証をサポートするようになりました。 LDAP 属性マップにより、Active Directory（AD）または LDAP サーバーに存在する属性が、シスコの属性名と同一視されるようになります。その後、リモートアクセス VPN 接続の確立中に AD または LDAP サーバーが FTD デバイスに認証を返すと、FTD デバイスは、その情報を使用して、AnyConnect クライアントが接続を完了する方法を調整できます。 サポートされるプラットフォーム：FTD

機能	説明
仮想トンネルインターフェイス（VTI）とルートベースのサイト間 VPN。	FTD サイト間 VPN は、仮想トンネルインターフェイス（VTI）と呼ばれる論理インターフェイスをサポートするようになりました。 ポリシーベース VPN の代替策として、仮想トンネルインターフェイスが設定されたピア間に VPN トンネルを作成することができます。これは、各トンネルの終端に IPsec プロファイルが付加されたルートベースの VPN をサポートします。これは、動的または静的なルートの使用が可能です。VTI を使用することにより、静的暗号マップのアクセス リストを設定してインターフェイスにマッピングすることが不要になります。トラフィックは、スタティックルートまたは BGP を使用して暗号化されます。ルーテッドセキュリティゾーンを作成し、そこに VTI インターフェイスを追加し、VTI トンネルを介して復号化されたトラフィック制御のアクセス制御ルールを定義できます。 VTI ベースの VPN は、次の間で作成できます。 • 2 つの FTD デバイス • FTD デバイスとパブリッククラウド • FTD デバイスとサービスプロバイダーの冗長性を備えた別の FTD デバイス 新規/変更されたページ： • **[Devices] > [Device Management] > [Interfaces] > [Add Interfaces] > [Virtual Tunnel Interface]** • **[Devices] > [VPN] > [Site To Site] > [Add VPN] > [Firepower Threat Defense Device] > [Route Based (VTI)]** サポートされるプラットフォーム：FTD
サイト間 VPN に対するダイナミック RRI サポート。	FTD サイト間 VPN は、サイト間 VPN 展開で IKEv2 ベースのスタティック暗号マップでサポートされるダイナミック リバース ルート インジェクション（RRI）をサポートするようになりました。これにより、スタティックルートは、リモート トンネルエンドポイントで保護されているネットワークとホストのルーティングプロセスに自動的に挿入されます。 新規/変更されたページ：サイト間 VPN トポロジにエンドポイントを追加するときの [ダイナミック リバース ルート インジェクションの有効化（Enable Dynamic Reverse Route Injection）] 詳細オプションが追加されました。 サポートされるプラットフォーム：FTD

機能	説明
手動証明書登録の拡張機能。	署名済み CA 証明書とアイデンティティ証明書を CA 機関から互いに独立して取得できるようになりました。 証明書署名要求（CSR）を作成し、アイデンティティ証明書を取得するための登録パラメータを保存する PKI 証明書登録オブジェクトに次の変更を行いました。 • PKI 証明書登録オブジェクトの手動登録設定に [CA Only] オプションが追加されました。このオプションを有効にすると、CA 機関から署名済み CA 証明書のみを受け取り、アイデンティティ証明書は受け取りません。 • PKI 証明書登録オブジェクトの手動登録設定で、[CA Certificate] フィールドを空白のままにできるようになりました。これを行うと、署名済み CA 証明書ではなく、CA 機関からアイデンティティ証明書のみを受け取ります。 新規/変更されたページ：[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [PKI] > [証明書の登録（Cert Enrollment）] > [証明書の登録の追加（Add Cert Enrollment）] > [CA 情報（CA Information）] > [登録タイプ（Enrollment Type）] > [手動（Manual）] サポートされるプラットフォーム：FTD
FTD 証明書管理の拡張機能。	FTD 証明書管理に次の機能拡張が行われました。 • 証明書の内容を表示するときに、認証局（CA）のチェーンを表示できるようになりました。 • 証明書をエクスポートできるようになりました。 新規/変更されたページ： • [Devices] > [Certificates] > [Status] 列 > [View] アイコン（虫めがね） • [Devices] > [Certificates] > [Export] アイコン サポートされるプラットフォーム：FTD
アクセス制御：URL フィルタリング、アプリケーション制御、およびセキュリティ インテリジェンス	

機能	説明
TLS 1.3（TLS サーバーアイデンティティ検出）で暗号化されたトラフィックの URL フィルタリングとアプリケーション制御。	サーバー証明書からの情報を使用して、TLS 1.3 で暗号化されたトラフィックの URL フィルタリングとアプリケーション制御を実行できるようになりました。この機能が動作するためにトラフィックを復号化する必要はありません。 （注） 暗号化トラフィックで URL フィルタリングとアプリケーション制御を実行する場合は、この機能を有効にすることを推奨します。ただし、特に低メモリモデルでは、デバイスのパフォーマンスに影響を与える可能性があります。 新規/変更されたページ：アクセス コントロール ポリシーの [詳細（Advanced）] タブに [TLS サーバーアイデンティティ検出（TLS Server Identity Discovery）] の警告とオプションが追加されました。 新規/変更された FTD CLI コマンド：**show conn detail** コマンドの出力に B フラグが追加されました。TLS 1.3 暗号化接続では、このフラグは、アプリケーションおよび URL の検出にサーバー証明書を使用したことを示します。 サポートされるプラットフォーム：FTD
レピュテーションが不明な Web サイトへのトラフィックに対する URL フィルタリング。	レピュテーションが不明な Web サイトに対して URL フィルタリングを実行できるようになりました。 新規/変更されたページ：アクセス制御、QoS、および SSL ルールエディタに [不明なレピュテーションに適用（Apply to unknown reputation）] チェックボックスが追加されました。 サポートされるプラットフォーム：FMC

機能	説明
DNS フィルタリングにより URL フィルタリングを強化します。	**ベータ版。** *DNS*フィルタリングは、暗号化されたトラフィックを含め（ただしトラフィックを復号化せずに）トランザクションの早い段階で要求されたドメインのカテゴリとレピュテーションを決定することで、URL フィルタリングを強化します。アクセス コントロール ポリシーごとに DNS フィルタリングを有効にし、そのポリシーのすべてのカテゴリ/レピュテーション URL ルールに適用します。 （注） DNS フィルタリングはベータ機能であり、期待どおりに動作しない可能性があります。実稼働環境では使用しないでください。 新規/変更されたページ：[全般設定（General Settings）] の下のアクセス コントロール ポリシーの [詳細（Advanced）] タブに [DNS トラフィックへのレピュテーション適用の有効化（Enable reputation enforcement on DNS traffic）] オプションが追加されました。 サポートされるプラットフォーム：FMC
セキュリティ インテリジェンス フィードの更新頻度の短縮。	FMC は、5 分または 15 分ごとにセキュリティ インテリジェンス データを更新できるようになりました。以前は、最短更新頻度は 30 分でした。 カスタムフィードでこれらの短い頻度のいずれかを設定する場合は、md5 チェックサムを使用してフィードにダウンロードする更新があるかどうかを判断するようにシステムを設定する必要もあります。 新規/変更されたページ： [オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [セキュリティ インテリジェンス（Security Intelligence）] > [ネットワークリストとフィード（Network Lists and Feeds）] > [フィードの編集（edit feed）] > [更新頻度（Update Frequency）] に新しいオプションが追加されました。 サポートされるプラットフォーム：FMC
アクセス制御：ユーザー制御	

機能	説明
ISE/ISE-PIC を使用した pxGrid 2.0。	**アップグレードの影響。** FMC を ISE/ISE-PIC アイデンティティソースに接続する場合は、pxGrid 2.0 を使用します。まだ pxGrid 1.0 を使用している場合は、ここで切り替えてください。このバージョンは廃止されました。 pxGrid 2.0 で使用するために、バージョン 6.7.0 では Cisco ISE 適応型ネットワーク制御（ANC）修復が導入され、相関ポリシー違反に関連する ISE 設定 ANC ポリシーが適用またはクリアされます。 pxGrid 1.0 で Cisco ISE エンドポイント保護サービス（EPS）修復を使用した場合は、pxGrid 2.0 で ANC 修復を設定して使用します。「誤った」pxGrid を使用している場合、ISE 修復は起動しません。ISE Connection Status Monitor ヘルスモジュールは、不一致を警告します。 サポートされているすべての Firepower バージョン（統合製品を含む）の詳細な互換性情報については、『Cisco Firepower Compatibility Guide』を参照してください。 新規/変更されたページ： • [Policies] > [Actions] > [Modules] > [Installed Remediation Modules] リスト • [Policies] > [Actions] > [Instances] > [Select a module type] ドロップダウンリスト サポートされるプラットフォーム：FMC
レルムシーケンス。	レルムを順序付けられたレルムシーケンスにグループ化できるようになりました。 単一のレルムを追加するのと同じ方法で、アイデンティティルールにレルムシーケンスを追加します。アイデンティティルールをネットワークトラフィックに適用すると、システムは指定された順序で Active Directory ドメインを検索します。LDAP レルムのレルムシーケンスは作成できません。 新規/変更されたページ：[システム（System）] > [統合（Integration）] > [レルムシーケンス（Realm Sequences）] サポートされるプラットフォーム：FMC

機能	説明
ISE サブネットフィルタリング。	特にメモリの少ないデバイスでは、CLI を使用して、ISE からのユーザーと IP およびセキュリティグループタグ（SGT）と IP のマッピングの受信から、サブネットを除外できるようになりました。 Snort Identity Memory Usage ヘルスモジュールは、メモリ使用率が特定のレベル（デフォルトでは 80%）を超えるとアラートを出します。 新しいデバイス CLI コマンド： **configure identity-subnet-filter** {**add** | **remove**} サポートされるプラットフォーム：FMC 管理対象デバイス
アクセス制御：侵入およびマルウェア防御	
動的分析のためのファイルの事前分類の改善。	**アップグレードの影響。** システムは、静的分析の結果（動的要素のないファイルなど）に基づいて、疑わしいマルウェアファイルを動的分析用に送信しないことを決定できるようになりました。 アップグレード後、[Captured Files] テーブルでは、これらのファイルの動的分析ステータスが [Rejected for Analysis] になります。 サポートされるプラットフォーム：FMC

機能	説明
S7Commplusプリプロセッサ。	新しい S7Commplus プリプロセッサは、広く受け入れられている S7 産業用プロトコルをサポートします。これを使用して、対応する侵入ルールとプリプロセッサルールを適用し、悪意のあるトラフィックをドロップし、侵入イベントを生成できます。 新規/変更されたページ： • プリプロセッサの有効化：ネットワーク分析ポリシーエディタで、[Settings] をクリックし（「Settings」という語をクリックします）、SCADA プリプロセッサで [S7Commplus Configuration] を有効にします。 • プリプロセッサの設定：ネットワーク分析ポリシーエディタの [Settings] で、[S7Commplus Configuration] をクリックします。 • S7Commplus プリプロセッサルールの設定：侵入ポリシーエディタで、[Rules] > [Preprocessors] > [S7 Commplus Configurations] の順にクリックします。 サポートされるプラットフォーム：ISA 3000 を含むすべての FTD デバイス
カスタム侵入ルールのインポートでルール競合の際に警告表示。	カスタム（ローカル）侵入ルールをインポートする場合、FMC がルールの競合について警告するようになりました。以前は、FMC は競合の原因となるルールをサイレントにスキップしていました。ただし、競合のあるルールのインポートが完全に失敗するバージョン 6.6.0.1 は除きます。 [ルールの更新（Rule Updates）] ページで、ルールのインポートに競合があった場合は、[ステータス（Status）] 列に警告アイコンが表示されます。詳細については、警告アイコンの上にポインタを置いて、ツールチップを参照してください。 既存のルールと同じ SID/リビジョン番号を持つ侵入ルールをインポートしようとすると、競合が発生することに注意してください。カスタムルールの更新バージョンには必ず新しいリビジョン番号を付けてください。FMC コンフィギュレーション ガイドでローカル侵入ルールをインポートするためのベストプラクティスを参考にすることを推奨します。 新規/変更されたページ：**[システム（System）] > [更新（Updates）] > [ルールの更新（Rule Updates）]** に警告アイコンが追加されました。 サポートされるプラットフォーム：FMC

機能	説明
アクセス制御：TLS/SSL 暗号解読	
復号の既知キー TLS/SSL ルールのための ClientHello の変更。	**アップグレードの影響。** TLS/SSL 復号化を設定した場合、管理対象デバイスが ClientHello メッセージを受信すると、システムはそのメッセージを復号の既知キーアクションを含む TLS/SSL ルールと照合しようとします。以前は、システムは ClientHello メッセージと復号 - 再署名ルールのみを照合していました。 照合は ClientHello メッセージからのデータとキャッシュされたサーバー証明書データからのデータに依存します。メッセージが一致すると、ClientHello メッセージが特定の方法で変更されます。FMC コンフィギュレーション ガイドの「*ClientHello* メッセージ処理」のトピックを参照してください。 この動作の変更は、アップグレード後に自動的に行われます。復号の既知キー TLS/SSL ルールを使用する場合は、暗号化されたトラフィックが期待どおりに処理されていることを確認します。 サポートされているプラットフォーム：すべてのデバイス
イベントロギングおよび分析	
オンプレミスの Stealthwatch ソリューションによるリモートデータストレージと相互起動。	オンプレミスの Stealthwatch ソリューションである Cisco Security Analytics and Logging（On Premises）を使用して、大量の Firepower イベントデータを FMC 以外に保存できるようになりました。 FMC でイベントを表示する場合、リモートデータストレージの場所にあるイベントをすばやく相互起動して表示できます。FMC は syslog を使用して、接続、セキュリティ インテリジェンス、侵入、ファイル、およびマルウェアイベントを送信します。 （注） このオンプレミスソリューションは、バージョン 6.4.0 以上を実行している FMC でサポートされます。ただし、コンテキスト相互起動には Firepower バージョン 6.7.0 以上が必要です。このソリューションは、Stealthwatch Enterprise（SWE）バージョン 7.3 を実行する必要がある Stealthwatch Management Console（SMC）用の Security Analytics and Logging On Prem アプリケーションの可用性にも依存します。 サポートされるプラットフォーム：FMC

機能	説明
Stealthwatch コンテキスト相互起動リソースを迅速に追加する。	FMC の新しいページを使用すると、Stealthwatch アプライアンスのコンテキスト相互起動リソースをすばやく追加できます。 Stealthwatch リソースを追加した後は、一般的なコンテキスト相互起動ページで管理します。ここで、Stealthwatch 以外の相互起動リソースを手動で作成および管理します。 新規/変更されたページ： • Stealthwatch リソースを追加します。[System] > [Logging] > [Security Analytics and Logging] • リソースを管理します。[Analysis] > [Advanced] > [Contextual Cross-Launch] サポート対象プラットフォーム：FMC
新しい相互起動オプションフィールドタイプ。	次のイベントデータの追加タイプを使用して、外部リソースに相互起動できるようになりました。 • アクセス コントロール ポリシー • 侵入ポリシー • アプリケーションプロトコル • クライアント アプリケーション • Web アプリケーション • ユーザー名（レルムを含む） 新規/変更されたページ： • 相互起動クエリリンクを作成または編集する際の新しい変数：[Analysis] > [Advanced] > [Contextual Cross-Launch]。 • ダッシュボードとイベントビューアの新しいデータタイプで、右クリックで相互起動が可能になりました。 サポートされるプラットフォーム：FMC

機能	説明
National Vulnerability Database（NVD）が Bugtraq に代わって使用されるようになりました。	**アップグレードの影響。** Bugtraq 脆弱性データは使用できなくなりました。現在、ほとんどの脆弱性データはNVDから取得されています。この変更をサポートするために、次の変更を行いました。 • [CVE ID] および [Severity] フィールドが [Vulnerabilities] テーブルに追加されました。テーブルビューで CVE ID を右クリックすると、NVDの脆弱性に関する詳細を表示できます。 • [Vulnerability Impact] フィールドが [Impact] に名前変更されました（テーブルビューのみ）。 • 使用されていない/冗長な [Bugtraq ID]、[Title, Available Exploits]、[Technical Description]、[Solution] フィールドが削除されました。 • ホストネットワークマップから [Bugtraq ID] フィルタリングオプションが削除されました。 脆弱性データをエクスポートする場合は、アップグレード後に統合が期待どおりに機能していることを確認します。 サポートされるプラットフォーム：FMC
のアップグレード	

機能	説明
アップグレード前の互換性チェック。	

機能	説明
	アップグレードの影響。 FMC展開では、より複雑な準備状況チェックを実行したり、アップグレードを試行したりする前に、Firepowerアプライアンスがアップグレード前の互換性チェックに合格することが必要になりました。このチェックは、アップグレードが失敗する原因となる問題を検出します。これらをより早期に検出し、続行をブロックするようになりました。 検出は次のとおりです。 • FXOS を新しいリリースの付属する FXOS バージョンにアップグレードするまで、FMC を使用して Firepower 4100/9300 シャーシをバージョン6.7.0以降にアップグレードすることはできません。 デバイスをバージョン6.7.0以降にアップグレードしている限り、アップグレードはブロックされます。たとえば、Firepower バージョン 6.6.x に対して古いバージョンの FXOS がデバイスで実行されている場合でも、Firepower 4100/9300 の 6.3 → 6.6.x のアップグレードはブロックされません。 • デバイスの設定が古い場合、FMC を使用してデバイスをアップグレードすることはできません。 FMC がバージョン 6.7.0 以降を実行しており、管理対象デバイスを有効なターゲットにアップグレードしている限り、アップグレードはブロックされます。たとえば、デバイスの設定が古い場合、デバイスを 6.3.0 → 6.6.x にアップグレードするとブロックされます。 • デバイスの設定が古い場合、FMC をバージョン 6.7.0 以上からアップグレードすることはできません。 FMC がバージョン 6.7.0 以降を実行している限り、アップグレードはブロックされます。以前のバージョン（バージョン 6.7.0 へのアップグレードを含む）からアップグレードする場合は、必ず自分で展開する必要があります。 インストールするアップグレードパッケージを選択すると、FMCはすべての対象アプライアンスの互換性チェック結果を表示します。新しい [Readiness Check] ページにもこの情報が表示されます。示された問題を修正するまでアップグレードできません。 新規/変更されたページ： • アップグレードパッケージの**[System]** > **[Update]** > **[Product**

機能	説明
	Updates] > **[Available Updates]** > **[Install]**アイコン • **[System]** > **[Update]** > **[Product Updates]** > **[Readiness Checks]** サポートされるプラットフォーム：FMC、FTD

機能	説明
準備状況チェックの改善。	

機能	説明
	アップグレードの影響。 準備状況チェックにより、ソフトウェアをアップグレードするための Firepower アプライアンスの準備状況を評価できます。これらのチェックには、データベースの整合性、ファイルシステムの整合性、設定の整合性、ディスク容量などが含まれます。 FMC をバージョン 6.7.0 にアップグレードすると、FTD のアップグレード準備状況チェックが次のように改善されます。 • 準備状況チェックが高速になります。 • デバイス CLI にログインすることなく、ハイアベイラビリティおよびクラスタ化された FTD デバイスで準備状況チェックがサポートされるようになりました。 • FTD デバイスをバージョン 6.7.0 以上にアップグレードするための準備状況チェックで、デバイスにアップグレードパッケージが存在する必要はなくなりました。アップグレード自体を開始する前に、アップグレードパッケージをデバイスにプッシュすることをお勧めしますが、準備状況チェックを実行する前に行う必要はありません。 • インストールするアップグレードパッケージを選択すると、該当するすべての FTD デバイスの準備状況が FMC に表示されるようになりました。新しい [Readiness Checks] ページでは、展開内の FTD デバイスの準備状況チェックの結果を表示できます。このページから準備状況チェックを再実行することもできます。 • 準備状況チェックの結果には、推定アップグレード時間が含まれます（ただし、リブート時間は含まれません）。 • エラーメッセージの方が優れています。FMC のメッセージセンターから成功/失敗ログをダウンロードすることもできます。 FMC がバージョン 6.7.0 以上を実行している限り、これらの改善はバージョン 6.3.0 以上からの FTD アップグレードでサポートされます。 新規/変更されたページ： • アップグレードパッケージの **[System]** > **[Update]** > **[Product Updates]** > **[Available Updates]** > **[Install]** アイコン • **[System]** > **[Update]** > **[Product Updates]** > **[Readiness Checks]**

機能	説明
	• **[Message Center] > [Tasks]** サポートされるプラットフォーム：FTD

機能	説明
FTD 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
	アップグレードの影響。 [Device Management] ページで、進行中の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。 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。 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。 （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、FMC を使用して FTD デバイスをアップグレードするとき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（[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。 パッチの自動キャンセルはサポートされていません。HA 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。 新規/変更されたページ： • FTD アップグレードパッケージの**[System]** > **[Update]** > **[Product Updates]** > **[Available Updates]** > **[Install]**アイコン • **[Devices]** > **[Device Management]** > **[Upgrade]** • **[Message Center] > [Tasks]** 新しい FTD CLI コマンド： • **show upgrade status detail**

機能	説明
	• **show upgrade status continuous** • **show upgrade status** • **upgrade cancel** • **upgrade retry** サポートされるプラットフォーム：FTD
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。	**アップグレードの影響。** FMCアップグレードは、スケジュールされたタスクを延期す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。 （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。 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。 サポートされるプラットフォーム：FMC
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。	**アップグレードの影響。** 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。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。 サポートされるプラットフォーム：すべて
展開とポリシー管理	

機能	説明
設定のロール バック。	**ベータ版。** FTD デバイスの設定を「ロールバック」して、以前に展開した設定に置き換えることができるようになりました。 （注） ロールバックはベータ機能であり、すべての展開タイプとシナリオでサポートされているわけではありません。これは中断を伴う操作でもあります。FMC コンフィギュレーション ガイドの「ポリシー管理」の章に記載されているガイドラインと制限事項を必ず読んで理解してください。 新規/変更されたページ：[Deploy] > [Deployment History] > [Rollback] 列とアイコン。 サポートされるプラットフォーム：FTD
侵入およびファイルポリシーを（アクセス コントロール ポリシーとは無関係に）展開する。	依存する変更がない限り、アクセス コントロール ポリシーとは無関係に侵入ポリシーとファイルポリシーを選択して展開できるようになりました。 新規/変更されたページ：[展開（Deploy）] > [展開（Deployment）] サポートされるプラットフォーム：FMC
アクセス制御ルールのコメントの検索。	アクセス制御ルールのコメント内で検索できるようになりました。 新規/変更されたページ：アクセス コントロール ポリシー エディタで、[検索ルール（Search Rules）] ドロップダウンダイアログに[コメント（Comments）]フィールドが追加されました。 サポートされるプラットフォーム：FMC
FTD NAT ルールの検索とフィルタリング。	FTD NAT ポリシーでルールを検索して、IP アドレス、ポート、オブジェクト名などに基づいてルールを検索できるようになりました。検索結果には部分一致が含まれます。条件で検索すると、ルールテーブルがフィルタリングされ、一致するルールのみが表示されます。 新規/変更されたページ：FTD NAT ポリシーを編集するときに、ルールテーブルの上に検索フィールドが追加されました。 サポートされるプラットフォーム：FTD

機能	説明
アクセス コントロール ポリシーとプレフィルタポリシー間のルールのコピーおよび移動。	あるアクセス コントロール ポリシーから別のアクセス コントロール ポリシーにアクセス制御ルールをコピーできます。アクセス コントロール ポリシーとそれに関連付けられたプレフィルタポリシーの間でルールを移動することもできます。 新規/変更されたページ：アクセス コントロール ポリシー エディタおよびプレフィルタ ポリシー エディタで、各ルールの右クリック メニューに [Copy] および [Move] オプションが追加されました。 サポートされるプラットフォーム：FMC
オブジェクト一括インポート。	カンマ区切り値（CSV）ファイルを使用して、ネットワーク、ポート、URL、VLAN タグ、および識別名オブジェクトを FMC に一括インポートできるようになりました。 制限事項および特定のフォーマット手順については、FMC コンフィギュレーション ガイドの「再利用可能なオブジェクト」の章を参照してください。 新規/変更されたページ：[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [オブジェクトタイプの選択（choose an object type）] > [オブジェクトタイプの追加（Add Object Type）] > [オブジェクトのインポート（Import Object）] サポートされるプラットフォーム：FMC

機能	説明
アクセス制御およびプレフィルタポリシーのインターフェイス オブジェクトの最適化。	特定のFTDデバイスでインターフェイス オブジェクトの最適化を有効にできるようになりました。 展開時に、アクセス制御とプレフィルタポリシーで使用されるインターフェイスグループとセキュリティゾーンは、送信元/宛先インターフェイスペアごとに個別のルールを生成します。インターフェイス オブジェクトの最適化を有効にすると、システムはアクセス制御/プレフィルタルールごとに 1 つのルールを展開します。これにより、デバイス設定の簡素化および展開のパフォーマンス向上が可能になります。 インターフェイス オブジェクトの最適化はデフォルトで無効になっています。これを有効にする場合は、[Object Group Search] も有効にする必要があります。これは、ネットワークオブジェクトに加えてインターフェイス オブジェクトにも適用されるようになり、デバイスのメモリ使用量を削減できます。 新規/変更されたページ：**[デバイス（Devices）]**>**[デバイス管理（Device Management）]**>**[デバイス（Device）**>**[詳細設定（Advanced Settings）]** セクション > [インターフェイス オブジェクトの最適化（Interface Object Optimization）] チェックボックス サポートされるプラットフォーム：FTD
管理とトラブルシューティング	
FMC シングルサインオン。	FMC は、サードパーティの SAML 2.0 準拠アイデンティティプロバイダー（IdP）で設定された外部ユーザーのシングルサインオン（SSO）をサポートするようになりました。IdP のユーザーまたはグループロールをFMCユーザーロールにマッピングできます。 新規/変更されたページ： • **[Login]** > **[Single Sign-On]** • **[System]** > **[Users]** > **[SSO]** サポートされるプラットフォーム：FMC
FMC ログアウトの遅延。	FMC からログアウトする場合、自動的に 5 秒間のカウントダウンが行われます。[ログアウト（Log Out）] を再度クリックすると、すぐにログアウトできます。 サポートされるプラットフォーム：FMC

機能	説明
FTD コンテナインスタンスのバックアップと復元。	FMC を使用してバージョン 6.7.0 以降の FTD コンテナインスタンスをバックアップおよび復元できるようになりました。 サポートされるプラットフォーム：Firepower 4100/9300
ヘルスモニタリングの強化。	ヘルスモニタリングが次のように拡張されました。 • [Health Status] サマリーページでは Firepower Management Center と FMC が管理するすべてのデバイスの正常性を一目で確認できます。 • [Monitoring] ナビゲーションペインでは、デバイス階層を移動できます。 • 管理対象デバイスは、個別に一覧表示されるか、該当する場合は地理位置情報、高可用性、またはクラスタステータスに基づいてグループ化されます。 • ナビゲーションペインから個々のデバイスのヘルスモニターを表示できます。 • 相互に関連するメトリックを相互に関連付けるカスタムダッシュボード。CPU や Snort などの事前定義された相関グループから選択します。または、使用可能なメトリックグループから独自の変数セットを作成して、カスタム相関ダッシュボードを作成します。 サポートされるプラットフォーム：FMC

機能	説明
ヘルスモジュールの更新。	CPU 使用率ヘルスモジュールが 4 つの新しいモジュールに置き換わりました。 • CPU使用率（コアごと）：すべてのコアのCPU使用率をモニターします。 • CPU 使用率データプレーン：デバイス上のすべてのデータプレーンプロセスの平均 CPU 使用率をモニターします。 • CPU 使用率 Snort：デバイス上の Snort プロセスの平均 CPU 使用率をモニターします。 • CPU 使用率システム：デバイス上のすべてのシステムプロセスの平均 CPU 使用率をモニターします。 メモリ使用量を追跡するために、次のヘルスモジュールが追加されました。 • メモリ使用率データプレーン：データプレーンプロセスで使用される割り当て済みメモリの割合をモニターします。 • メモリ使用率 Snort：Snort プロセスによって使用される割り当て済みメモリの割合をモニターします。 統計情報を追跡するために、次のヘルスモジュールが追加されました。 • 接続統計情報：接続統計情報と NAT 変換カウントをモニターします。 • クリティカルプロセス統計情報：クリティカルプロセスの状態、リソース消費量、再起動回数をモニターします。 • 展開された設定の統計情報：展開された設定に関する統計情報（ACEの数やIPSルールなど）をモニターします。 • Snort 統計情報：イベント、フロー、およびパケットの Snort 統計情報をモニターします。 サポートされるプラットフォーム：FMC

機能	説明
メッセージセンターの検索。	メッセージセンターで現在のビューをフィルタリングできるようになりました。 新規/変更されたページ：メッセージセンターの [Show Notifications] スライダに [Filter] アイコンとフィールドが追加されました。 サポートされるプラットフォーム：FMC
ユーザビリティとパフォーマンス	
Dusk テーマ。	**ベータ版。** FMC Web インターフェイスのデフォルトは Light テーマですが、新しい Dusk テーマを選択することもできます。 （注） Dusk テーマはベータ機能です。ページまたは機能を使用できない問題が発生した場合は、別のテーマに切り替えてください。すべてに対応することはできませんが、フィードバックもお寄せください。[ユーザー設定 (User Preferences)] ページのフィードバックリンクを使用するか、fmc-light-theme-feedback@cisco.com までお問い合わせください。 新規/変更されたページ：ユーザー名の下にあるドロップダウンリストの [ユーザー設定（User Preferences）] サポートされるプラットフォーム：FMC
FMC メニューの検索。	FMC メニューを検索できるようになりました。 新規/変更されたページ：[Deploy] メニューの左側にある [FMC] メニューバーに [Search] アイコンとフィールドが追加されました。 サポートされるプラットフォーム：FMC
Firepower Management Center REST API	

機能	説明
新しい REST API サービス。	

機能	説明
	新機能と既存の機能をサポートするために、次の FMC REST API サービス/操作が追加されました。 認可サービス： • ssoconfig：FMC シングルサインオンを取得および変更するための GET および PUT 操作。 ヘルスサービス： • メトリック：ヘルスモニターのメトリックを取得する GET 操作。 • アラート：ヘルスアラートを取得する GET 操作。 • deploymentdetails：展開の正常性の詳細を取得する GET 操作。 展開サービス： • jobhistories：展開履歴を取得する GET 操作。 • rollbackrequests：設定ロールバックを要求する POST 操作。 デバイスサービス： • メトリック：デバイスメトリックを取得する GET 操作。 • virtualtunnelinterfaces：仮想トンネルインターフェイスを取得および変更するための GET、PUT、POST、および DELETE 操作。 統合サービス： • externalstorage：外部イベントストレージ設定を取得および変更するための GET、ID による GET、および PUT 操作。 ポリシーサービス： • intrusionpolicies：侵入ポリシーを変更するための POST および DELETE 操作。 サービスの更新： • cancelupgrades：失敗したアップグレードをキャンセルする POST 操作。 • retryupgrades：失敗したアップグレードを再試行する POST 操作。

機能	説明
	サポートされるプラットフォーム：FMC

FDM バージョン 6.7 の新機能

表 *9 : FDM* バージョン *6.7.0* の新機能

機能	説明
プラットフォーム機能	
ASA 5525-X、5545-X、5555-X でのサポートが終了します。最後にサポートされていたリリースは FTD 6.6 です。	FTD 6.7 を ASA 5525-X、5545-X、5555-X にインストールすることはできません。これらのモデルで最後にサポートされていたリリースは FTD 6.6 です。
ファイアウォールと IPS の機能	
アクセス制御ルールの照合のための TLS サーバーアイデンティティ検出	TLS 1.3 証明書は暗号化されます。TLS 1.3 で暗号化されたトラフィックで、アプリケーションまたはURL フィルタリングを使用するアクセスルールに対応するには、システムが TLS 1.3 証明書を復号する必要があります。暗号化された接続が適切なアクセス制御ルールに適合していることを確認するため、[TLS Server Identity Discovery] を有効にすることを推奨します。この設定では、証明書のみが復号されます。接続は暗号化されたままになります。 [Access Control Settings]（⚙）ボタンとダイアログボックスが **[Policy]** > **[Access Control]**ページに追加されました。
外部の信頼できる CA 証明書のグループ	SSL 復号ポリシーで使用される信頼できる CA 証明書のリストをカスタマイズできるようになりました。デフォルトでは、ポリシーはすべてのシステム定義の信頼できる CA 証明書を使用しますが、カスタムグループを作成して証明書を追加したり、デフォルトグループを独自のより制限されたグループに置き換えることができます。 **[Objects]** > **[Certificates]** ページに証明書グループが追加され、SSL 復号ポリシー設定を変更して証明書グループを選択できるようにしました。

機能	説明
パッシブ ID ルールの Active Directory レルムシーケンス	Active Directory（AD）サーバーとそのドメインの番号付きリストであるレルムシーケンスを作成し、パッシブ認証 ID ルールで使用できます。レルムシーケンスは、複数の AD ドメインをサポートしている状況で、ユーザーベースのアクセス制御を実行するときに役立ちます。各 AD ドメインの個別のルールを記述する代わりに、すべてのドメインを対象とする単一のルールを作成できます。シーケンス内の AD レルムの順序は、ID の競合が発生した場合に、その競合を解決するために使用されます。 **[Objects]** > **[Identity Sources]** ページに AD レルム シーケンス オブジェクトが追加され、そのオブジェクトをパッシブ認証アイデンティティルールのレルムとして選択できるようになりました。FTD API に **RealmSequence** リソースが追加されました。また **IdentityRule** リソースには、アクションとしてパッシブ認証を使用するルールのレルムとしてレルム シーケンス オブジェクトを選択する機能が追加されました。
TrustSec セキュリティグループタグ（SGT）グループオブジェクトの FDM サポートと、アクセス制御ルールでのそれらの使用	FTD 6.5 では、SGT グループオブジェクトを設定し、それらをアクセス制御ルールの一致基準として使用するためのサポートが FTD API に追加されました。さらに、ISE によってパブリッシュされた SXP トピックをリッスンするように ISE アイデンティティ オブジェクトを変更できます。これらの機能を FDM で直接設定できるようになりました。 新しいオブジェクトである SGT グループが追加され、それらを選択および表示できるようにアクセス制御ポリシーが更新されました。また、サブスクライブするトピックの明示的な選択を含むように ISE オブジェクトを変更しました。

機能	説明
Snort 3.0 のサポート	新しいシステムでは、Snort 3.0 がデフォルトの検査エンジンです。古いリリースから 6.7 にアップグレードした場合、アクティブな検査エンジンは Snort 2.0 のままですが、Snort 3.0 に切り替えることができます。このリリースでは、Snort 3.0 は、仮想ルータ、時間ベースのアクセス制御ルール、または TLS 1.1 以下の接続の復号化をサポートしていません。これらの機能が必要ない場合にのみ Snort 3.0 を有効にしてください。Snort 2.0 と Snort 3.0 の間を自由に切り替えることができるため、必要に応じて、変更を元に戻すことができます。バージョンを切り替えるたびにトラフィックが中断されます。 **[デバイス（Device）] > [更新（Updates）]** ページの [侵入ルール（Intrusion Rules）] グループに Snort のバージョンを切り替える機能が追加されました。FTD API では、IntrusionPolicy リソースアクション/toggleinspectionengine が追加されました。 さらに、Snort 3 ルールパッケージの更新で追加、削除、または変更された侵入ルールを示す新しい監査イベント、ルール更新イベントがあります。
Snort 3 のカスタム侵入ポリシー	Snort 3 を検査エンジンとして使用している場合は、カスタム侵入ポリシーを作成できます。これに対し、Snort 2 を使用する場合にのみ、事前定義されたポリシーを使用できます。カスタム侵入ポリシーを使用すると、ルールのグループを追加または削除し、グループレベルでセキュリティレベルを変更して、グループ内のルールのデフォルトアクション（無効化、アラート、またはドロップ）を効率的に変更できます。Snort 3 の侵入ポリシーを使用すると、Cisco Talos 提供の基本ポリシーを編集することなく、IPS/IDS システムの動作をより詳細に制御できます。 侵入ポリシーを一覧表示するように **[Policies] > [Intrusion]** ページが変更されました。新しいポリシーを作成したり、既存のポリシーを表示または編集（グループの追加/削除、セキュリティレベルの割り当て、ルールのアクションの変更など）することができます。複数のルールを選択し、それらのアクションを変更することもできます。さらに、アクセス制御ルールでカスタム侵入ポリシーを選択できます。
侵入イベント用の複数の syslog サーバー	侵入ポリシー用に複数の syslog サーバーを設定できます。侵入イベントは各 syslog サーバーに送信されます。 侵入ポリシー設定ダイアログボックスに、複数の syslog サーバーオブジェクトを選択する機能が追加されました。

機能	説明
URL レピュテーション照合にレピュテーションが不明なサイトを含めることが可能です	URL カテゴリのトラフィック一致基準を設定し、レピュテーション範囲を選択する場合に、レピュテーションが不明な URL をレピュテーション照合に含めることができます。 アクセス制御ルールと SSL 復号ルールの URL レピュテーション基準に [レピュテーションが不明なサイトを含める（Include Sites with Unknown Reputation）] チェックボックスが追加されました。
VPN 機能	
仮想トンネルインターフェイス（VTI）とルートベースのサイト間 VPN	VPN 接続プロファイルのローカルインターフェイスとして仮想トンネルインターフェイスを使用して、ルートベースのサイト間 VPN を作成できるようになりました。ルートベースのサイト間 VPN を使用すると、VPN 接続プロファイルを一切変更することなく、ルーティングテーブルを変更するだけで、特定の VPN 接続で保護されたネットワークを管理できます。リモートネットワークの追跡を継続し、前述の変更に対応して VPN 接続プロファイルを更新する必要はありません。その結果、クラウド サービス プロバイダーや大企業の VPN 管理が簡素化されます。 インターフェイスのリストのページに [仮想トンネルインターフェイス（Virtual Tunnel Interfaces）] タブが追加され、VTI をローカルインターフェイスとして使用できるように、サイト間 VPN ウィザードが更新されました。
FTD リモート アクセス VPN 接続を行うための Hostscan およびダイナミック アクセス ポリシー（DAP）の API サポート	Hostscan パッケージとダイナミック アクセス ポリシー（DAP）ルール XML ファイルをアップロードし、XML ファイルを作成するよう DAP ルールを設定することで、接続中のエンドポイントのステータスに関連する属性に基づいてグループポリシーをリモートユーザーに割り当てる方法を制御することができます。Cisco Identity Services Engine（ISE）がない場合は、これらの機能を使用して認可変更を実行できます。Hostscan のアップロードと DAP の設定は FTD API を使用してのみ行えます。FDM を使用して設定することはできません。Hostscan および DAP の使用方法の詳細については、AnyConnect のマニュアルを参照してください。 dapxml、hostscanpackagefiles、hostscanxmlconfigs、ravpns の各 FTD API オブジェクトモデルを追加または変更しました。

機能	説明
外部 CA 証明書の証明書失効チェックの有効化	FTD API を使用して、特定の外部 CA 証明書の証明書失効チェックを有効にすることができます。失効チェックは、リモートアクセス VPN で使用される証明書に特に役立ちます。FDM を使用して証明書の失効チェックを設定することはできません。FTD API を使用する必要があります。 ExternalCACertificate リソースに revocationCheck、crlCacheTime、および oscpDisableNonce 属性が追加されました。
安全性の低い Diffie-Hellman グループ、および暗号化アルゴリズムとハッシュアルゴリズムのサポートがなくなりました	6.6 で廃止されていた以下の機能が削除されました。それらを IKE プロポーザルまたは IPsec ポリシーで引き続き使用している場合は、アップグレード後にそれらを置き換えないと、設定変更を展開できません。VPN が正しく機能するように、サポートされる DH および暗号化アルゴリズムにアップグレードする前に VPN 設定を変更することをお勧めします。 • Diffie-Hellman グループ：2、5、および 24。 • 強力な暗号化の輸出規制を満たすユーザー向けの暗号化アルゴリズム：DES、3DES、AES-GMAC、AES-GMAC-192、AES-GMAC-256。輸出規制を満たしていないユーザーの場合、DES は引き続きサポートされます（これが唯一のオプションです）。 • ハッシュアルゴリズム：MD5。
リモートアクセス VPN 用のカスタムポート	リモートアクセス VPN（RA VPN）接続に使用するポートを設定できます。RA VPN に使用されているインターフェイスで FDM に接続する必要がある場合は、RA VPN 接続のポート番号を変更できます。FDM が使用するポート 443 は、デフォルトの RA VPN ポートでもあります。 RA VPN ウィザードのグローバル設定ステップが更新され、ポート設定が追加されました。
リモートアクセス VPN を認証するための SAML サーバーのサポート	SAML 2.0 サーバーをリモートアクセス VPN の認証ソースとして設定できます。サポートされている SAML サーバーは次のとおりです：Duo。 **[Objects]** > **[Identity Sources]** ページでのアイデンティティソースとして SAML サーバーが追加され、それを使用できるようにリモートアクセス VPN 接続プロファイルが更新されました。

機能	説明
AnyConnect モジュールプロファイルの FTD API サポート	FTD API を使用して、AMP イネーブラ、ISE ポスチャ、Umbrella といった AnyConnect で使用されるモジュールプロファイルをアップロードできます。これらのプロファイルは、AnyConnect プロファイル エディタ パッケージからインストールできるオフライン プロファイル エディタを使用して作成する必要があります。 AnyConnectClientProfile モデルに anyConnectModuleType 属性が追加されました。最初はモジュールプロファイルを使用する AnyConnect クライアント プロファイル オブジェクトを作成できますが、FDM で作成されたオブジェクトを変更して正しいモジュールタイプを指定するには、依然として API を使用する必要があります。
ルーティング機能	
スマート CLI による EIGRP のサポート	以前のリリースでは、FlexConfig を使用して、[Advanced Configuration] ページで EIGRP を設定しました。今回、[Routing] ページでスマート CLI を直接使用して EIGRP を設定するようになりました。 FlexConfig を使用して EIGRP を設定した場合は、リリース 6.7 にアップグレードするときに、FlexConfig ポリシーから FlexConfig オブジェクトを削除してから、スマート CLI オブジェクトで設定を再作成する必要があります。スマート CLI の更新が完了するまでは、参照用に EIGRP FlexConfig オブジェクトを保持できます。設定は自動的に変換されません。 [Routing] ページに EIGRP スマート CLI オブジェクトが追加されました。
インターフェイス機能	
ISA 3000 ハードウェアバイパスの持続性	永続化オプションを使用して、ISA 3000 インターフェイスペアのハードウェアバイパスを有効にできるようになりました。電源が回復した後、ハードウェアバイパスは手動で無効にするまで有効のままになります。持続性のないハードウェアバイパスを有効にすると、電源が回復した後にハードウェアバイパスが自動的に無効になります。ハードウェアバイパスが無効になっていると、短時間のトラフィック中断が発生する可能性があります。永続化オプションを使用すると、トラフィックの短時間の中断が発生するタイミングを制御できます。 新規/変更された画面：**[Device]** > **[Interfaces]** > **[Hardware Bypass]** > **[Hardware Bypass Configuration]**

機能	説明
Firepower 4100/9300 における FTD 動作リンク状態と物理リンク状態の同期	Firepower 4100/9300 シャーシでは、FTD 動作リンク状態をデータインターフェイスの物理リンク状態と同期できるようになりました。現在、FXOS 管理状態がアップで、物理リンク状態がアップである限り、インターフェイスはアップ状態になります。FTD アプリケーション インターフェイスの管理状態は考慮されません。FTD からの同期がない場合は、たとえば、FTD アプリケーションが完全にオンラインになる前に、データインターフェイスが物理的にアップ状態になったり、FTD のシャットダウン開始後からしばらくの間はアップ状態のままになる可能性があります。この機能はデフォルトで無効になっており、FXOS の論理デバイスごとに有効にできます。 （注） この機能は、Radware vDP デコレータを使用する FTD ではサポートされません。 新規/変更された Firepower Chassis Manager 画面：[論理デバイス（Logical Devices）] > [リンク状態の有効化（Enable Link State）] 新規/変更された FXOS コマンド：**set link-state-sync enabled**、**show interface expand detail** サポートされているプラットフォーム： Firepower 4100/9300
Firepower 1100 および 2100 SFP インターフェイスで、自動ネゴシエーションの無効化がサポートされるようになりました	自動ネゴシエーションを無効にするように Firepower 1100 および 2100 SFP インターフェイスを設定できるようになりました。10GB インターフェイスの場合、自動ネゴシエーションなしで速度を 1GB に設定できます。速度が 10GB に設定されているインターフェイスの自動ネゴシエーションは無効にできません。 新規/変更画面：[Device] > [Interfaces] > [Edit Interface] > [Advanced Options] > [Speed] サポートされるプラットフォーム：Firepower 1100 および 2100
管理およびトラブルシューティングの機能	

機能	説明
失敗した FTD ソフトウェアのアップグレードをキャンセルし、以前のリリースに戻す機能	FTD のメジャー ソフトウェア アップグレードが失敗するか、正常に機能しない場合は、アップグレードインストールの実行時の状態にデバイスを戻すことができます。 FDM の [System Upgrade] パネルにアップグレードを元に戻す機能が追加されました。アップグレード時に、FDM ログイン画面にアップグレードステータスが表示され、アップグレードが失敗した場合にキャンセルしたり元に戻すためのオプションが表示されます。FTD API に CancelUpgrade、RevertUpgrade、RetryUpgrade、および UpgradeRevertInfo リソースが追加されました。 FTD CLI に **show last-upgrade status**、**show upgrade status**、**show upgrade revert-info**、**upgrade cancel**、**upgrade revert**、**upgrade cleanup-revert**、および **upgrade retry** コマンドが追加されました。
データインターフェイス上の FDM/FTD API アクセス用のカスタム HTTPS ポート	データインターフェイスで FDM または FTD API アクセスに使用する HTTPS ポートを変更できます。ポートをデフォルトの 443 から変更することにより、管理アクセスと同じデータインターフェイスで設定されているその他の機能（リモートアクセス VPN など）の競合を回避できます。管理インターフェイスの管理アクセス HTTPS ポートは変更できないことに注意してください。 **[Device]** > **[System Settings]** > **[Management Access]** > **[Data Interfaces]** ページにポートを変更する機能が追加されました。
Firepower 1000 および 2100 シリーズ デバイス上の Cisco Defense Orchestrator のロータッチプロビジョニング	Cisco Defense Orchestrator（CDO）を使用して新しい FTD デバイスを管理する予定がある場合、デバイスセットアップ ウィザードを完了することなく、または FDM にログインすることさえなく、デバイスを追加できるようになりました。 新しい Firepower 1000 および 2100 シリーズ デバイスは、最初に Cisco Cloud に登録され、CDO で簡単に要求できます。CDO に入ると、CDO からデバイスをすぐに管理できます。このロータッチプロビジョニングでは、物理デバイスと直接やりとりする必要性が最小限に抑えられ、ネットワクデバイスに関する経験が浅い従業員が勤務するリモートオフィスなどの場所にとって理想的です。 Firepower 1000 および 2100 シリーズ デバイスの初期プロビジョニング方法が変更されました。また、**[System Settings]** > **[Cloud Services]** ページに自動登録が追加されました。これにより、FDM を使用して以前に管理していたアップグレード済みデバイスおよびその他のデバイスのプロセスを手動で開始できます。

機能	説明
SNMP 設定の FTD API サポート	FTD API を使用して FDM または CDO 管理対象 FTD デバイスで SNMP バージョン 2c または 3 を設定できます。 API リソースの SNMPAuthentication、SNMPHost、SNMPSecurityConfiguration、SNMPServer、SNMPUser、SNMPUserGroup、SNMPv2cSecurityConfiguration、および SNMPv3SecurityConfiguration が追加されました。 （注） FlexConfig を使用して SNMP を設定した場合は、FTD API SNMP リソースを使用して設定をやり直す必要があります。SNMP を設定するためのコマンドは、FlexConfig では使用できなくなりました。FlexConfig ポリシーから SNMP FlexConfig オブジェクトを削除するだけで、変更を展開できます。その後、API を使用して機能を再設定するときに、それらのオブジェクトを参照として使用できます。
システムに保持されるバックアップファイルの最大数が 10 から 3 に減少	システムでは、10 個ではなく最大 3 個のバックアップファイルがシステムに保持されます。新しいバックアップが作成されると、最も古いバックアップファイルが削除されます。必要な場合にシステムを回復するために必要なバージョンを入手できるように、バックアップファイルは異なるシステムにダウンロードしてください。
FTD API バージョンの後方互換性	FTD バージョン 6.7 以降、ある機能の API リソースモデルがリリース間で変更されない場合、FTD API は古い API バージョンに基づくコールを受け入れることができます。機能モデルが変更された場合でも、古いモデルを新しいモデルに変換する論理的な方法があれば、古いコールが機能します。たとえば、v4 コールを v5 システムで受け入れることができます。コールのバージョン番号として「latest（最新）」を使用する場合、「古い」コールは、このシナリオでは v5 コールとして解釈されるため、下位互換性を利用するかどうかは、API コールの構築方法によって決まります。

機能	説明
FTD REST API バージョン 6（v6）	ソフトウェアバージョン 6.7 用の FTD REST API はバージョン 6 です。API URL の v6 を使用するか、優先的に /latest/ を使用して、デバイスでサポートされている最新の API バージョンを使用していることを示せます。 使用しているリソースモデルに変更が加えられている可能性があるため、既存のすべての呼び出しを再評価してください。リソースを表示できる API エクスプローラを開くには、FDM にログインして、[詳細オプション（More options）] ボタン（⋮）をクリックし、[APIエクスプローラ（API Explorer）] を選択します。

バージョン 6.7 の新しいハードウェアと仮想プラットフォーム

表 *10* : バージョン *6.7.0* の新しいハードウェアと仮想プラットフォーム

機能	説明
新しい仮想環境。	次の環境に FMCv および FTDv が導入されました。 • Oracle Cloud Infrastrucure（OCI） • Google Cloud Platform（GCP）

新しい侵入ルールとキーワード

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が可能です。

侵入ルールを更新（SRU/LSP）すると、新規および更新された侵入ルールとプリプロセッサルール、既存のルールに対して変更された状態、および変更されたデフォルトの侵入ポリシーの設定が提供されます。現在の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、SRU/LSP を更新しても、そのルールはインポートされません。

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。

Snort のバージョンを確認するには、互換性ガイドの「バンドルされたコンポーネント」の項を参照するか、次のコマンドのいずれかを使用します。

- FMC：**[ヘルプ（Help）]** > **[概要（About）]**を選択します。
- FDM：**show summary** CLI コマンドを使用します。

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。

廃止された機能

FMC バージョン 6.7 で廃止された機能

表 *11 : FMC* バージョン *6.7.0* で廃止された機能

機能	アップグレードの影響	説明
Cisco Firepower User Agent software ソフトウェアとアイデンティティソース。	FMC がアップグレードされないようにします。	ユーザーエージェント設定を使用して FMC をバージョン 6.7 以降 にアップグレードすることはできません。 バージョン 6.6 は、Cisco Firepower User Agent ソフトウェアをアイデンティティソースとしてサポートする最後のリリースです。Cisco Identity Services Engine/Passive Identity Connector（ISE/ISE-PIC）に切り替える必要があります。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 User Agent のサポート終了 [英語] 通知、およびFirepower ユーザー ID：ユーザーエージェントから Identity Services Engine への移行 [英語] の技術メモを参照してください。 廃止された FTD CLI コマンド： **configure user agent**
Cisco ISE エンドポイント保護サービス（EPS）の修復。	ISE 修復が機能しなくなることがあります。	Cisco ISE エンドポイント保護サービス（EPS）の修復は、pxGrid 2.0 では機能しません。代わりに、新しい Cisco ISE Adaptive Network Control（ANC）修復を設定して使用します。 「不正な」pxGrid を使用して FMC を ISE/ISE-PIC アイデンティティソースに接続している場合、ISE 修復は起動しません。ISE Connection Status Monitor ヘルスモジュールは、不一致を警告します。

機能	アップグレードの影響	説明
安全性の低い Diffie-Hellman グループ、暗号化アルゴリズム、およびハッシュアルゴリズム。	FMC がアップグレードされないようにします。	次の FTD 機能のいずれかを使用している場合、FMC をアップグレードできないことがあります。 • Diffie-Hellman グループ：2、5、および 24。 グループ 5 は、IKEv1 の FMC 展開で引き続きサポートされますが、より強力なオプションに変更することをお勧めします。 • 強力な暗号化の輸出規制を満たすユーザー向けの暗号化アルゴリズム：DES、3DES、AES-GMAC、AES-GMAC-192、AES-GMAC-256。輸出規制を満たしていないユーザーの場合、DES は引き続きサポートされます（これが唯一のオプションです）。 • NULL の「暗号化アルゴリズム」（暗号化なしの認証、テスト目的）は、IKEv1 と IKEv2 の両方の IPsec プロポーザルの FMC 展開で引き続きサポートされます。ただし、IKEv2 ポリシーではサポートされなくなりました。 • ハッシュアルゴリズム：MD5。 IKE プロポーザルまたは IPsec ポリシーでこれらの機能を使用している場合は、アップグレードする前に VPN 設定を変更して確認します。

機能	アップグレードの影響	説明
アプライアンス設定のリソース使用率の正常性モジュール（一時的に廃止）。	ヘルスモニターでのアップグレード後のエラーの可能性	バージョン 6.7 では、バージョン 6.6.3 で導入され、後続のすべての 6.6.x リリースでサポートされるアプライアンス設定のリソース使用率の正常性モジュールに関するサポートが部分的かつ一時的に廃止されています。 バージョン 6.7 のサポートは次のとおりです。 • バージョン 6.6.3 以降からバージョン 6.7 への FMC のアップグレード デバイスがバージョン 6.6.x のままである場合にのみ、モジュールのサポートが継続されます。デバイスをバージョン 6.7 にアップグレードすると、モジュールは動作を停止し、正常性モニターにエラーが表示されます。エラーを解決するには、FMC を使用してモジュールを無効にし、ポリシーを再適用します。 • バージョン 6.3 ー 6.6.1 からバージョン 6.7.0 への FMC のアップグレード、または FMC バージョン 6.7 の新規インストール。 このモジュールはサポートされていません。 モジュールがサポートされていない FMC にモジュールが有効になっているバージョン 6.6.x デバイスを追加するまれなケースでは、解決できないエラーがヘルスモニターに表示されます。このエラーは無視しても問題ありません。 バージョン 7.0 ではフルサポートが提供され、モジュールの名前が 構成メモリ割り当てに変更されています。
その他の正常性モジュール（永久的に廃止）。	なし。	バージョン 6.7 では、次のヘルスモジュールが廃止されています。 • CPU 使用率：4 つの新しいモジュールに置き換えられました。FMC バージョン 6.7 の新機能 （13 ページ）を参照してください。 • ローカルマルウェア分析：このモジュールは、バージョン 6.3 のデバイス上の脅威データの更新モジュールに置き換えられました。バージョン 6.7 以降の FMC は、古いモジュールが適用されるデバイスを管理できなくなります。 • ユーザー エージェント ステータス モニター：Cisco Firepower ユーザーエージェントはサポートされなくなりました。

機能	アップグレードの影響	説明
クラシックテーマを使用したウォークスルー。	なし。	バージョン 6.7 では、クラシックテーマの FMC ウォークスルー（使用方法）が廃止されました。ユーザー設定でテーマを切り替えることができます。
Bugtraq	脆弱性データをエクスポートする場合は、アップグレード後に統合が期待どおりに機能していることを確認します。	バージョン 6.7 では Bugtraq のデータベースフィールドとオプションが削除されます。Bugtraq 脆弱性データは使用できなくなりました。現在、ほとんどの脆弱性データは National Vulnerability Database（NVD）から取得されています。 詳細については、FMC バージョン 6.7 の新機能 （13 ページ）を参照してください。
Microsoft Internet Explorer	ブラウザを切り替える必要があります。	Microsoft Internet Explorer を使用して Firepower Web インターフェイスをテストすることはなくなりました。Google Chrome、Mozilla Firefox、または Microsoft Edge に切り替えることをお勧めします。

FDM バージョン 6.7 で廃止された機能

表 *12 : FDM* バージョン *6.7.0* で廃止された機能

機能	アップグレードの影響	説明
安全性の低い Diffie-Hellman グループ、暗号化アルゴリズム、およびハッシュアルゴリズム。	アップグレード後に展開ができないようにします。	次の FTD 機能のいずれかを使用している場合、アップグレード後の展開ができないことがあります。 • Diffie-Hellman グループ：2、5、および 24。 • 強力な暗号化の輸出規制を満たすユーザー向けの暗号化アルゴリズム：DES、3DES、AES-GMAC、AES-GMAC-192、AES-GMAC-256。輸出規制を満たしていないユーザーの場合、DES は引き続きサポートされます（これが唯一のオプションです）。 • ハッシュアルゴリズム：MD5。 IKE プロポーザルまたは IPsec ポリシーでこれらの機能を使用している場合は、アップグレードする前に VPN 設定を変更して確認します。

機能	アップグレードの影響	説明
FlexConfig コマンド。	アップグレード後に展開ができないようにします。 アップグレード後に設定をやり直す必要があります。	バージョン 6.7 では、FDM を使用する FTD の次の FlexConfig CLI コマンドは廃止されます。 • **router eigrp**：[ルーティング（Routing）] ページの **[デバイス（Device）] > [ルーティング（Routing）] > [EIGRP]** で直接スマート CLI EIGRP オブジェクトを作成して、使用できます。 • **snmp-server**：FTD API を使用して SNMP バージョン 2c または 3 を設定できるようになりました。 関連付けられている FlexConfig オブジェクトを削除するまで、アップグレード後に展開することはできません。
バックアップファイルの保持。	なし。アップグレードによって、ローカルのバックアップは常に消去されます。	バージョン 6.7 では、保存されるバックアップファイルの数が 10 から 3 に減ります。 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ことをお勧めします。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。
Microsoft Internet Explorer	ブラウザを切り替える必要があります。	Microsoft Internet Explorer を使用して Firepower Web インターフェイスをテストすることはなくなりました。Google Chrome、Mozilla Firefox、または Microsoft Edge に切り替えることをお勧めします。

バージョン 6.7 で廃止されたハードウェアと仮想プラットフォーム

表 *13*：バージョン *6.7.0* で廃止されたハードウェアと仮想プラットフォーム

機能	説明
Firepower ソフトウェアを使用した ASA 5525-X、5545-X、および 5555-X デバイス。	ASA 5525-X、5545-X、および 5555-X でバージョン 6.7 以降は実行できません。

廃止された FlexConfig コマンド

このドキュメントでは、今回のリリースで廃止された FlexConfig のオブジェクトおよびコマンドと、その他の廃止された機能が記載されています。FlexConfig が導入されたときに禁止されたコマンドを含む、禁止されたコマンドと以前のリリースで廃止になった機能の完全なリストについては、コンフィギュレーション ガイドを参照してください。

⚠

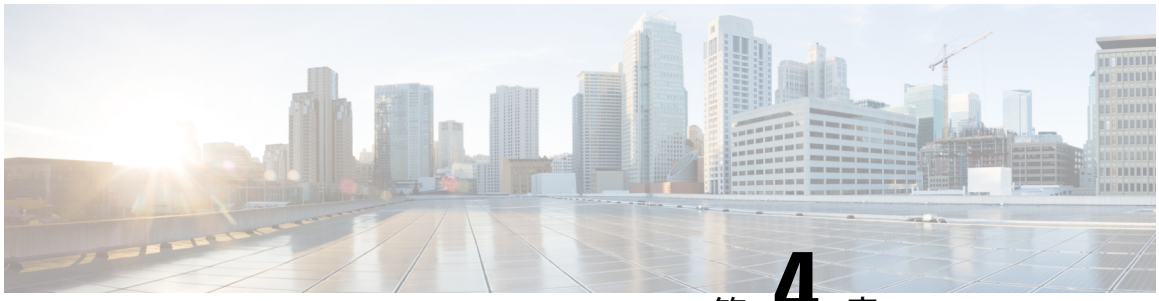
注意 ほとんどの場合、既存の FlexConfig 設定はアップグレード後も引き続き機能し、展開ができます。ただし、廃止されたコマンドを使用すると、展開の問題が発生する場合があります。

FlexConfig について

いくつかの FTD の機能は、ASA 設定コマンドを使用して設定されます。Smart CLI または FlexConfig を使用して、他の方法では Web インターフェイスでサポートされないさまざまな ASA 機能を手動で設定できます。

アップグレードにより、以前に FlexConfig を使用して設定した機能について、GUI またはスマート CLI のサポートが追加されることがあります。これにより、現在使用している FlexConfig コマンドが廃止される可能性があります。ご使用の構成は自動的に変換されません。アップグレード後は、新しく廃止されたコマンドを使用して FlexConfig オブジェクトを割り当てたり作成したりすることはできません。

アップグレード後、FlexConfig ポリシーおよび FlexConfig オブジェクトを確認してください。廃止されたコマンドが含まれている場合、メッセージは問題を示します。設定をやり直すことをお勧めします。新しい設定を確認したら、問題のある FlexConfig オブジェクトまたは FlexConfig コマンドを削除できます。



第 4 章

ソフトウェアのアップグレード

この章では、重要なリリースに固有の情報を提供します。

アップグレードの計画

誤りを避けるには、注意深い計画と準備が役立ちます。この表はアップグレードの計画プロセスを要約したものです。詳細なチェックリストと手順については、該当するアップグレードまたは設定ガイドのを参照してください：アップグレード手順 （82 ページ）

表 *14*：アップグレードの計画フェーズ

計画フェーズ	次を含む
計画と実現可能性	展開を評価します。 アップグレードパスを計画します。 すべてのアップグレードガイドラインを読み、設定の変更を計画します。 アプライアンスへのアクセスを確認します。 帯域幅を確認します。 メンテナンス時間帯をスケジュールします。

計画フェーズ	次を含む
バックアップ	ソフトウェアをバックアップします。 Firepower 4100/9300 の FXOS をバックアップします。 ASA FirePOWER 用 ASA をバックアップします。
アップグレードパッケージ	アップグレードパッケージをシスコからダウンロードします。 システムにアップグレードパッケージをアップロードします。
関連するアップグレード	仮想展開内で仮想ホスティングをアップグレードします。 Firepower 4100/9300 の FXOS をアップグレードします。 ASA FirePOWER 用 ASA をアップグレードします。
最終チェック	設定を確認します。 NTP 同期を確認します。 ディスク容量を確認します。 設定を展開します。 準備状況チェックを実行します。 実行中のタスクを確認します。 展開の正常性と通信を確認します。

アップグレードする最小バージョン

パッチは4桁目のみを変更できます。以前のメジャーリリースまたはメンテナンスリリースからパッチに直接アップグレードすることはできません。

パッチのアップグレードガイドライン

このチェックリストには、バージョン 6.7.x パッチに関するアップグレードガイドラインが含まれています。

表 *15* : バージョン *6.7.x.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：侵入イベントに関する電子メールアラート機能を搭載した FMC （67 ページ）	FMC	6.2.3 ～ 6.7.0.x	6.7.0 6.6.0、6.6.1、6.6.3 これらのリリースに対するすべてのパッチ

アップグレードの失敗：侵入イベントに関する電子メールアラート機能を搭載した FMC

展開：Firepower Management Center

アップグレード元：バージョン 6.2.3 ～ 6.7.0.x

アップグレード先（直接）：バージョン 6.6.0、6.6.1、6.6.3、6.7.0、およびこれらのリリースへのパッチ

関連するバグ：CSCvw38870、CSCvx86231

個々の侵入イベントに対して電子メールアラートを設定した場合は、Firepower Management Center を上記のいずれかのバージョンにアップグレードする前に、その設定を完全に無効にします。そうなっていなければ、アップグレードは失敗します。

この機能は、アップグレード後に再度有効にすることができます。この問題のためにすでにアップグレードに失敗した場合は、Cisco TAC に連絡してください。

侵入に関する電子メールアラートを完全に無効にするには、次の操作を行います。

1. Firepower Management Center で、**[Policies]** > **[Actions]** > **[Alerts]**を選択し、**[Intrusion Email]** をクリックします。
2. [State] を [off] に設定します。
3. [Rules] の横にある [Email Alerting per Rule Configuration] をクリックし、ルールの選択を解除します。

   アップグレード後に再選択できるように、選択を解除したルールを書き留めておきます。

ヒント　ルールの再選択に時間がかかりすぎる場合は、アップグレードする前に Cisco TAC に連絡してください。選択した内容を保存しておくことで、アップグレード後にすぐに再実装できるようにご案内いたします。

4. 設定を保存します。

応答しないアップグレード

アップグレード中は、設定を変更または展開しないでください。システムが非アクティブに見えても、アップグレード中は手動で再起動またはシャットダウンしないでください。システムが使用できない状態になり、再イメージ化が必要になる場合があります。

応答しない FMC または従来のデバイスのアップグレード

進行中のアップグレードは再開しないでください。アップグレードに失敗する、アプライアンスが応答しないなど、アップグレードで問題が発生した場合にはCisco TACにお問い合わせください。

応答しない FTD のアップグレード

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

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

FTD CLI を使用することもできます。

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

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

トラフィック フローとインスペクション

次の場合に、トラフィックフローおよび検査の中断が発生することがあります。

- デバイスを再起動する場合。
- デバイスソフトウェア、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。
- デバイスソフトウェアをアンインストールまたは復元する場合。

- ドメイン間でデバイスを移動する場合。
- 設定の変更を展開する場合（Snort プロセスが再起動する）。

デバイスタイプ、高可用性または拡張性の設定、およびインターフェイス設定によって、中断の性質が決まります。これらのタスクは、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。

FirepowerThreatDefenseのアップグレード時の動作：Firepower4100/9300

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 *16*：トラフィックの挙動：*FXOS* のアップグレード

展開	メソッド	トラフィックの動作
スタンドアロン	—	廃棄
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。

展開	メソッド	トラフィックの動作
シャーシ内クラスタ（Firepower 9300 のみ）	ハードウェアバイパス有効：[Bypass: Standby] または [Bypass-Force]。（6.1 以降）	検査なしで受け渡される。
	ハードウェアバイパス無効：[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。
	ハードウェア バイパス 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。

スタンドアロンデバイスでのソフトウェアのアップグレード

アップグレード中、デバイスはメンテナンスモードで稼働します。アップグレードの開始時にメンテナンスモードを開始すると、トラフィック インスペクションが 2 ー 3 秒中断します。インターフェイスの構成により、その時点とアップグレード中の両方のスタンドアロンデバイスによるトラフィックの処理方法が決定されます。

表 *17:* トラフィックの挙動：スタンドアロンデバイスでのソフトウェアのアップグレード

インターフェイス コンフィギュレーション	トラフィックの動作
ファイアウォール インターフェイス	EtherChannel、冗長、サブインターフェイスを含むルーテッドまたはスイッチド。 スイッチドインターフェイスは、ブリッジグループまたはトランスペアレントインターフェイスとしても知られています。	廃棄

インターフェイス コンフィギュレーション		トラフィックの動作
IPS のみのインターフェイス	インラインセット、ハードウェアバイパス強制が有効：[Bypass: Force]（6.1 以上）。	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 スタンバイ モード：[Bypass: Standby]（6.1 以上）。	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：[Bypass: Disabled]（6.1 以上）。	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。

- FMC を搭載した FTD：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。

- FDM を搭載した FTD：高可用性ペアの場合、スタンバイをアップグレードし、ロールを手動で切り替えてから、新しいスタンバイをアップグレードします。

ソフトウェアのアンインストール（パッチ）

バージョン 6.2.3 以降では、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。

- FMC を搭載した FTD：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。
- FDM を搭載した FTD ：サポートされていません。

ソフトウェアの復元（メジャーおよびメンテナンスリリース）

復元すると、FTD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の直前の状態に戻ります。展開に関係なく（たとえ高可用性および拡張性に関する場合でも）、トラフィックフローと検査の中断が起こること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。

復元に関するサポートは、FDM を搭載した FTD のバージョン 6.7.0 で開始されます。FMC を搭載した FTD ではサポートされません。

設定変更の導入

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 構成ガイド』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 *18*：トラフィックの挙動：設定変更の展開

インターフェイス コンフィギュレーション		トラフィックの動作
ファイアウォール インターフェイス	EtherChannel、冗長、サブインターフェイスを含むルーテッドまたはスイッチド。 スイッチドインターフェイスは、ブリッジグループまたはトランスペアレントインターフェイスとしても知られています。	廃棄
IPS のみのインターフェイス	インラインセット、[Failsafe] が有効または無効（6.0.1 ～ 6.1）。	検査なしで受け渡される。 [フェールセーフ（Failsafe）] が無効で、Snort がビジーでもダウンしていない場合、いくつかのパケットがドロップすることがあります。
	インラインセット、[Snort Fail Open: Down]：無効（6.2 以降）	廃棄
	インラインセット、[Snort Fail Open: Down]：有効（6.2 以降）	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。

Firepower Threat Defense アップグレード時の動作：その他のデバイス

スタンドアロンデバイスでのソフトウェアのアップグレード

アップグレード中、デバイスはメンテナンスモードで稼働します。アップグレードの開始時にメンテナンスモードを開始すると、トラフィック インスペクションが 2 ー 3 秒中断します。インターフェイスの構成により、その時点とアップグレード中の両方のスタンドアロンデバイスによるトラフィックの処理方法が決定されます。

表 *19:* トラフィックの挙動：スタンドアロンデバイスでのソフトウェアのアップグレード

インターフェイス コンフィギュレーション		トラフィックの動作
ファイアウォール インターフェイス	EtherChannel、冗長、サブインターフェイスを含むルーテッドまたはスイッチド。 スイッチドインターフェイスは、ブリッジグループまたはトランスペアレントインターフェイスとしても知られています。	廃棄
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：[Bypass: Force]（Firepower 2100 シリーズ、6.3 以上）。	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 スタンバイ モード：[Bypass: Standby]（Firepower 2100 シリーズ、6.3 以上）。	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：[Bypass: Disabled]（Firepower 2100 シリーズ、6.3 以上）。	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。

- FMC を使用した Firepower Threat Defense：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。
- FDM を使用した Firepower Threat Defense：高可用性ペアの場合、スタンバイをアップグレードし、ロールを手動で切り替えてから、新しいスタンバイをアップグレードします。

ソフトウェアのアンインストール（パッチ）

バージョン 6.2.3 以降では、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。

- FMC を搭載した FTD：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。
- FDM を搭載した FTD ：サポートされていません。

ソフトウェアの復元（メジャーおよびメンテナンスリリース）

復元すると、FTD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の直前の状態に戻ります。展開に関係なく（たとえ高可用性および拡張性に関する場合でも）、トラフィックフローと検査の中断が起こること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。

復元に関するサポートは、FDM を搭載した FTD のバージョン 6.7.0 で開始されます。FMC を搭載した FTD ではサポートされません。

設定変更の導入

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 構成ガイド』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 *20 :* トラフィックの挙動：設定変更の展開

インターフェイス コンフィギュレーション		トラフィックの動作
ファイアウォール インターフェイス	EtherChannel、冗長、サブインターフェイスを含むルーテッドまたはスイッチド。 スイッチドインターフェイスは、ブリッジグループまたはトランスペアレントインターフェイスとしても知られています。	廃棄
IPS のみのインターフェイス	インラインセット、[Failsafe] が有効または無効（6.0.1 ～ 6.1）。	検査なしで受け渡される。 [フェールセーフ（Failsafe）] が無効で、Snortがビジーでもダウンしていない場合、いくつかのパケットがドロップすることがあります。
	インラインセット、[Snort Fail Open: Down]：無効（6.2 以降）	廃棄
	インラインセット、[Snort Fail Open: Down]：有効（6.2 以降）	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。

ASA FirePOWER アップグレード時の動作

ASA FirePOWER module にトラフィックをリダイレクトする ASA サービス ポリシーは、Firepower ソフトウェア アップグレードの間（Snort プロセスを再起動する特定の設定を導入するときなど）にモジュールがトラフィックを処理する方法を決定します。

表 *21 : 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 リダイレクションのポリシー	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
モニターのみ（**sfr {fail-close}|{fail-open} monitor-only**）	パケットをただちに出力、コピーへのインスペクションなし

ASA FirePOWER 展開時のトラフィックの動作

Snort プロセスを再起動している間のトラフィックの動作は、ASA FirePOWER module 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 構成ガイド』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 *22 : 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 コンフィギュレーション	トラフィックの動作
インライン	切断
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 構成ガイド』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 *23 : NGIPSv* 展開時のトラフィックの動作

インターフェイス コンフィギュレーション	トラフィックの動作
インライン、[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

時間とディスク容量のテスト

参考のために、FMC およびソフトウェアのアップグレードにかかる時間とディスク容量のテストに関するレポートを提供しています。

時間テスト

特定のプラットフォームおよびシリーズでテストされたすべてのソフトウェアアップグレードの中で最長のテスト時間を報告します。次の表で説明するように、アップグレードには、複数の理由により、指定された時間よりも時間がかかる可能性があります。将来のベンチマークとして使用できるように、独自のアップグレード時間を追跡および記録することをお勧めします。

注意 アップグレード中は、設定を変更または展開しないでください。システムが非アクティブに見えても、手動で再起動またはシャットダウンしないでください。ほとんどの場合、進行中のアップグレードを再開しないでください。システムが使用できない状態になり、再イメージ化が必要になる場合があります。アップグレードに失敗する、アプライアンスが応答しないなど、アップグレードで問題が発生した場合には応答しないアップグレード（68 ページ）を参照してください。

表 *24 :* ソフトウェアアップグレードの時間テストの条件

条件	詳細
展開	デバイスアップグレードの時間は、FMC展開でのテストに基づいています。同様の条件の場合、リモートとローカルの管理対象デバイスの raw アップグレード時間は類似しています。

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

ディスク容量テスト

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

また、デバイス アップグレード パッケージ用に FMC（/Volume または /var 内）に必要な容量も報告します。FTD アップグレードパッケージ用の内部サーバーがある場合、または FDM を使用している場合は、それらの値を無視してください。

特定の場所（/var や /ngfw など）のディスク容量の見積もりを報告する場合、その場所にマウントされているパーティションのディスク容量の見積もりを報告しています。一部のプラットフォームでは、これらの場所が同じパーティション上にある場合があります。

空きディスク容量が十分でない場合、アップグレードは失敗します。

表 *25 :* ディスク容量の確認

プラットフォーム	コマンド
FMC	**[システム（System）]**>**[モニタリング（Monitoring）]**>**[統計（Statistics）]**を選択し、FMC を選択します。[Disk Usage] で、[By Partition] の詳細を展開します。
FTD with FMC	**[System]**>**[Monitoring]**>**[Statistics]**を選択し、確認するデバイスを選択します。[Disk Usage] で、[By Partition] の詳細を展開します。
FTD with FDM	**show disk** CLI コマンドを使用します。

バージョン 6.7.0.3 の時間とディスク容量

表 *26 :* バージョン *6.7.0.3* の時間とディスク容量

プラットフォーム	ボリュームの容量	必要容量	FMC の容量	アップグレード時間	リブート時間
FMC	/var 内で 2.9 GB	/ 内で 34 MB	—	38 分	7 分
FMCv：VMware	/var 内で 2.6 GB	/ 内で 39 MB	—	30 分	5 分
Firepower 1000 シリーズ	—	/ngfw 内で 3.3 GB	650 MB	9 分	13 分
Firepower 2100 シリーズ	—	/ngfw 内で 3.2 GB	700 MB	7 分	14 分
Firepower 4100 シリーズ	—	/ngfw 内で 2.5 GB	450 MB	5 分	7 分
Firepower 4100 シリーズ コンテナ インスタンス	—	/ngfw 内で 2.4 GB	450 MB	6 分	4 分
Firepower 9300	—	/ngfw 内で 3.1 GB	450 MB	4 分	8 分
FTD を搭載した ASA 5500-X シリーズ	/ngfw/Volume 内で 2.3 GB	/ngfw 内で 110 MB	380 MB	13 分	9 分
FTD を使用した ISA 3000	/ngfw/Volume 内で 2.2 GB	/ngfw 内で 110 MB	380 MB	19 分	8 分
FTDv：VMware	/ngfw/Volume 内で 2.3 GB	/ngfw 内で 110 MB	380 MB	6 分	5 分

プラットフォーム	ボリュームの容量	必要容量	FMC の容量	アップグレード時間	リブート時間
FTDv：KVM	/ngfw/Volume 内で 2.3 GB	/ngfw 内で 110 MB	380 MB	8 分	5 分
ASA FirePOWER	/var 内で 3.1 GB	/ 内で 36 MB	450 MB	64 分	6 分
NGIPSv	/var 内で 970 MB	/ 内で 34 MB	300 MB	5 分	4 分

バージョン 6.7.0.2 の時間とディスク容量

表 *27* : バージョン *6.7.0.2* の時間とディスク容量

プラットフォーム	ボリュームの容量	必要容量	FMC の容量	アップグレード時間	リブート時間
FMC	/var 内で 2.3 GB	/ 内で 20 MB	—	35 分	7 分
FMCv：VMware	/var 内で 2.4 GB	/ 内で 23 MB	—	28 分	/ngfw に 2.5 GB
Firepower 1000 シリーズ	—	/ngfw 内で 3.0 GB	610 MB	8 分	13 分
Firepower 2100 シリーズ	—	/ngfw 内で 3.0 GB	660 MB	6 分	14 分
Firepower 9300	—	/ngfw 内で 2.6 GB	410 MB	5 分	7 分
Firepower 4100 シリーズ	—	2.4 GB /ngfw 内	410 MB	4 分	7 分
Firepower 4100 シリーズ コンテナ インスタンス	—	/ngfw 内で 2.3 GB	410 MB	5 分	4 分
FTD を搭載した ASA 5500-X シリーズ	/ngfw/Volume 内で 2.2 GB	/ngfw 内で 110 MB	370 MB	10 分	7 分
FTD を使用した ISA 3000	/ngfw/Volume 内で 2.3 GB	/ngfw 内で 110 MB	370 MB	17 分	9 分
FTDv：VMware	/ngfw/Volume 内で 2.2 GB	/ngfw 内で 110 MB	370 MB	6 分	4 分
FTDv：KVM	/ngfw/Volume 内で 2.2 GB	/ngfw 内で 110 MB	370 MB	6 分	8 分
ASA FirePOWER	/var 内で 3.0 GB	/ 内で 21 MB	430 MB	73 分	4 分
NGIPSv	/var 内で 930 MB	/ 内で 19 MB	290 MB	5 分	3 分

バージョン 6.7.0.1 の時間とディスク容量

表 *28 :* バージョン *6.7.0.1* の時間とディスク容量

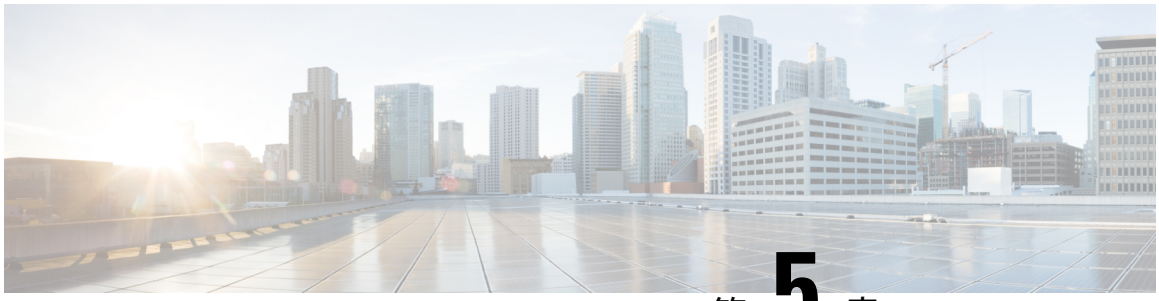
プラットフォーム	ボリュームの容量	必要容量	FMC の容量	アップグレード時間	リブート時間
FMC	/var 内で 1.8 GB	/ 内で 20 MB	—	32 分	7 分
FMCv：VMware	/var 内で 1.4 GB	/ 内で 23 MB	—	28 分	5 分
Firepower 1000 シリーズ	—	/ngfw 内で 1.4 GB	340 MB	7 分	12 分
Firepower 2100 シリーズ	—	/ngfw 内で 1.4 GB	400 MB	7 分	12 分
Firepower 9300	—	/ngfw 内で 710 MB	130 MB	5 分	7 分
Firepower 4100 シリーズ	—	/ngfw 内で 700 MB	130 MB	4 分	5 分
Firepower 4100 シリーズ コンテナ インスタンス	—	/ngfw 内で 480 MB	130 MB	5 分	/ngfw に 2.5 GB
FTD を搭載した ASA 5500-X シリーズ	/ngfw/Volume 内で 540 MB	/ngfw 内で 110 MB	88 MB	10 分	12 分
FTD を使用した ISA 3000	/ngfw/Volume 内で 540 MB	/ngfw 内で 110 MB	88 MB	13 分	7 分
FTDv：VMware	/ngfw/Volume 内で 530 MB	/ngfw 内で 110 MB	88 MB	6 分	4 分
FTDv：KVM	/ngfw/Volume 内で 550 MB	/ngfw 内で 110 MB	88 MB	7 分	3 分
ASA FirePOWER	/var 内で 1.2 GB	/ 内で 21 MB	41 MB	66 分	/ngfw に 2.5 GB
NGIPSv	/var 内で 82 MB	/ 内で 18 MB	9 MB	6 分	3 分

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、次のいずれかのドキュメントを参照してください。

表 *29 : Firepower* アップグレード手順

タスク	ガイド
Firepower Management Center の展開でアップグレードします。	Cisco Firepower Management Center Upgrade Guide, Version 6.0–7.0
Firepower Device Manager を搭載した Firepower Threat Defense をアップグレードします。	Firepower Device Manager 用 Cisco Firepower Threat Defense 構成ガイド アップグレード先のバージョンではなく、現在実行している Firepower Threat Defense バージョンのガイドの「システム管理」の章を参照してください。
Firepower 4100/9300 シャーシの FXOS をアップグレードします。	Cisco Firepower 4100/9300 アップグレードガイド、Firepower 6.0.1–7.0.x または ASA 9.4(1)–9.16(x) with FXOS 1.1.1–2.10.1
ASDM を使用して ASA FirePOWER モジュールをアップグレードします。	Cisco ASA Upgrade Guide
ISA 3000、ASA 5508-X、ASA 5516-X で ROMMON イメージをアップグレードします。	Cisco ASA and Firepower Threat Defense Reimage Guide 「Upgrade the ROMMON Image」のセクションを参照してください。常に最新のイメージがあることを確認してください。



第 5 章

パッチのアンインストール

Firepower Management Center および ASDM の展開では、ほとんどのパッチをアンインストールすることができます。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。

アンインストールは、Firepower Device Manager ではサポートされていません。ホットフィックスをアンインストールしようとしないでください。代わりに、Cisco TAC にお問い合わせください。

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 6.7.0/6.7.x のパッチ

現在、すべての 6.7.0/6.7.x のパッチでアンインストールがサポートされています。

アンインストールパッチのガイドライン

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

Firepower 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。これは FMC 展開で、最初に管理対象デバイスからパッチをアンインストールすることを意味します。

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。

- 高可用性および拡張性展開のデバイス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 （87 ページ）」を参照してください。
- FMC または ASDM 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。
- FMC のユーザー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。デバイスでは、独自のユーザーアカウントが維持されます。
- 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。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。

デバイスの後に 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、高可用性 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。詳しくは、「HA/スケーラビリティ環境でのアンインストール順序 （87 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、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。

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/データユニットをアンインストールしてから、次にプライマリ/アクティブコントロール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 *30 : HA* 内の *FMC* の場合におけるアンインストール順序

展開	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、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 *31 : 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

展開	アンインストール順序
デバイスの高可用性	高可用性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。 **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。

展開	アンインストール順序
デバイス 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、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。 **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。 **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。 **3.** 以前のコントロールからアンインストールします。

表 *32 : 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 展開	アンインストール順序
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、制御ユニットを最後に残します。 **1.** データ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.** 各データユニットに対して手順を繰り返します。 **5.** 制御ユニットでクラスタリングを無効にします。新しい制御ユニットが引き継ぐまで待ちます。 **6.** 以前の制御ユニットの ASA FirePOWER モジュールからアンインストールします。 **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

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 モニター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 **[System]** > **[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 [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。

[Help] > **[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 （89 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（87ページ）」を参照してください。

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：混合したバージョンのクラスタまたは 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 モニター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、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 1000 シリーズ	`connect ftd`
Firepower 2100 シリーズ	`connect ftd`
Firepower 4100/9300	`connect module` *slot_number* `console`、次に `connect ftd`（最初のログインのみ）
ASA FirePOWER	`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/uninstaller_name
```

Firepowerアプライアンスにパッチを適用すると、そのパッチを簡単に識別できる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。「パッケージのアンインストール（95ページ）」を参照してください。

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、ユーザー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ー 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ーします。

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 または 拡張性の展開では、混合したバージョンのクラスタ、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 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） （91 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 （87 ページ）」を参照してください。

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：**[Monitoring]** > **[ASA FirePOWER Monitoring]** > **[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：**[Monitoring]** > **[ASA FirePOWER Monitoring]** > **[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 ユーザー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ることにご注意ください。

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、ユーザー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ー 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ーします。

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。**[Configuration]** > **[ASA FirePOWER Configuration]** > **[Device Management]** > **[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

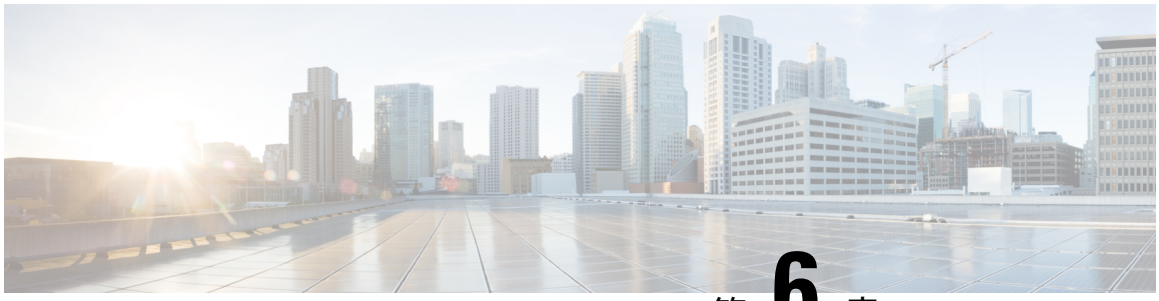
ASA フェールオーバー/クラスタ環境の場合は、各デバイスについて計画した順序でこの手順を繰り返します。

パッケージのアンインストール

パッチのアンインストーラーは、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」が含まれます。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`（Firepower Threat Defense デバイスの場合）
- `/var/sf/updates`（Firepower Management Center および NGIPS デバイス（ASA FirePOWER、NGIPSv）の場合）

アンインストーラー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。



第 6 章

ソフトウェアのインストール

アップグレードできない場合、またはアップグレードしない場合は、メジャーリリースおよびメンテナンスリリースを新規インストールできます。

パッチ用のインストールパッケージは提供していません。特定のパッチを実行するには、適切なメジャーリリースまたはメンテナンスリリースをインストールしてからパッチを適用してください。

インストールにおけるチェックリストおよびガイドライン

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。このチェックリストは、一般的な再イメージ化の問題を回避できるアクションを示しています。ただし、このチェックリストは包括的なものではありません。詳細な手順については、該当する設置ガイド『取り付け手順 （101 ページ）』を参照してください。

表 *33*:

✓	アクション/チェック
	アプライアンスへのアクセスを確認します。 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、ユーザーの位置からのトラフィックがデバイスの管理インターフェイスにアクセスするためにデバイス自体を通過する必要がないことを確認してください。FMC の展開では、デバイスを経由せずに FMC 管理インターフェイスにアクセスできる必要もあります。
	バックアップを実行します。 サポートされている場合、再イメージ化の前にバックアップします。 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できないことに注意してください。設定は手動で再作成する必要があります。 **注意** 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ことを強くお勧めします。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。 バックアップと復元は、複雑なプロセスになる可能性があります。手順をスキップしたり、セキュリティやライセンスの問題を無視しないでください。バックアップと復元の要件、ガイドライン、制限事項、およびベストプラクティスの詳細については、使用する展開の設定ガイドを参照してください。

✓	アクション/チェック
	FMC 管理からデバイスを削除する必要があるか判断します。 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。 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。
	ライセンスの問題に対処します。 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。孤立した権限付与の発生を防ぐために、Cisco Smart Software Manager（CSSM）から登録解除することが必要になる場合があります。これで、再登録を防ぐことができます。または、新しいライセンスについてセールス部門に連絡する必要がある場合があります。 詳細については、以下を参照してください。 • ご使用の製品の設定ガイド。 • スマート ライセンスの登録解除 （99 ページ） • Cisco Firepower System Feature Licenses Guide • Frequently Asked Questions (FAQ) about Firepower Licensing

以前のメジャー バージョンへの Firepower 1000/2100 シリーズ デバイスの再イメージ化

Firepower 1000/2100 シリーズデバイスの完全な再イメージ化を実行することを推奨します。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。

スマート ライセンスの登録解除

Firepower Threat Defense は 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）で登録します。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、クラウドおよびクラウドサービスからアプライアンスが登録解除され、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。
- モデルの移行中にソース Firepower Management Center をシャットダウンする。
- 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。

取り付け手順

表 *34 : Firepower Management Center* 取り付け手順

FMC	ガイド
FMC 1600、2600、4600	Cisco Firepower Management Center 1600, 2600, and 4600 Getting Started Guide
FMC 1000、2500、4500	Cisco Firepower Management Center 1000, 2500, and 4500 Getting Started Guide
FMCv	Cisco Secure Firewall Management Center Virtual Getting Started Guide

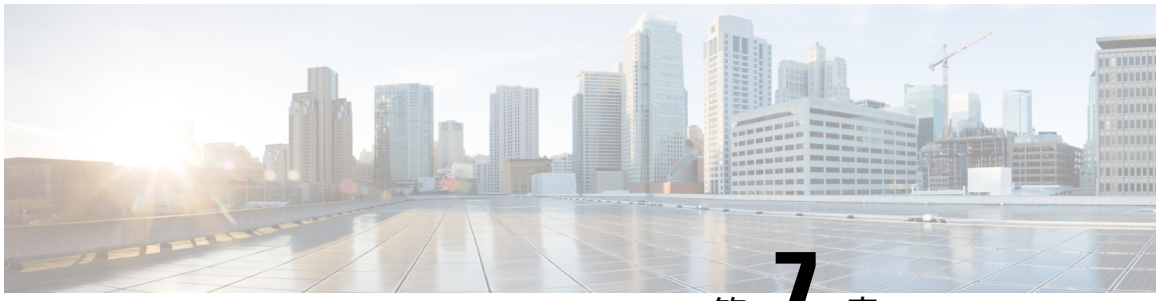
表 *35 : Firepower Threat Defense* 取り付け手順

FTDプラットフォーム	ガイド
Firepower 1000/2100 シリーズ	Cisco Secure Firewall ASA および Threat Defense 再イメージ化ガイド 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	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 スタートアップ ガイド
ASA 5500-X シリーズ	Cisco Secure Firewall ASA および Threat Defense 再イメージ化ガイド
ISA 3000	Cisco Secure Firewall ASA および Threat Defense 再イメージ化ガイド
FTDv：AWS	AWS クラウド向け Cisco Secure Firewall Threat Defense Virtual スタートアップガイド
FTDv：Azure	Microsoft Azure クラウド向け Cisco Secure Firewall Threat Defense Virtual クイックスタートガイド
FTDv：GCP	Google クラウドプラットフォーム向け Cisco Secure Firewall Threat Defense Virtual スタートアップガイド
FTDv：KVM	KVM 向け Cisco Secure Firewall Threat Defense Virtual スタートアップガイド

FTDプラットフォーム	ガイド
FTDv：OCI	Oracle クラウド インフラストラクチャ向け Cisco Secure Firewall Threat Defense Virtual スタートアップガイド
FTDv：VMware	VMware 向け Cisco Secure Firewall Threat Defense Virtual スタートアップガイド

表 *36 : NGIPSv* および *ASA FirePOWER* のインストール手順

NGIPS プラットフォーム	ガイド
NGIPSv	Cisco Firepower NGIPSv Quick Start Guide for VMware
ASA FirePOWER	Cisco Secure Firewall ASA および Threat Defense 再イメージ化ガイド ASDM Book 2: Cisco ASA Series Firewall ASDM Configuration Guide：Managing the ASA FirePOWER Module



第 7 章

資料

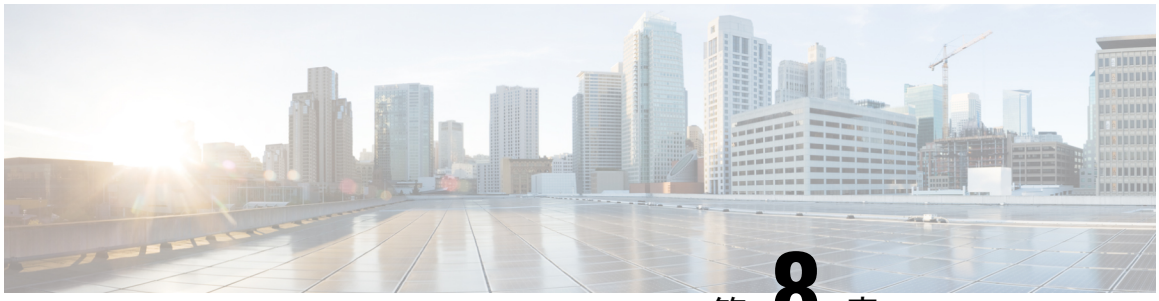
パッチで必要な場合は、Firepower のマニュアルを更新します。

- ドキュメント ロードマップ （103 ページ）

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、リリースノートには、各パッチの解決済みの問題が記載されています。

サポート契約がある場合は、Cisco Bug Search Tool を使用して最新のバグリストを取得できます。検索では、特定の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。バグのステータス、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。

重要 バグリストは1回自動生成され、その後は更新されません。バグ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。

バージョン 6.7.0.3 で解決済みの問題

表 *37* : バージョン *6.7.0.3* で解決済みの問題

不具合 ID	タイトル
CSCvr11958	AWS FTD：「ERROR: failed to set interface to promiscuous mode」により展開が失敗する
CSCvr94911	FXOS：一部のインターフェイス移行ログに理由がない
CSCvt62869	SPLIT-BRAIN：フェイルオーバー制御メッセージのブロックの事前割り当て
CSCvt68055	snmpd が FP21xx デバイスの FXOS で頻繁に再生成される
CSCvu44472	FMC システムプロセスが起動する

不具合 ID	タイトル
CSCvu53810	TD2 がバックプレーン インターフェイス間で MPLS のロードバランシングを行わず、すべてを最初のインターフェイスに送信する
CSCvu84127	明確な理由なしに Firepower がリブートすることがある
CSCvv21602	FP2K MIB に cfprApSmMonitorTable がありません
CSCvv24647	FTD 2100 - SNMP：不正な値がイーサネット統計ポーリングに返される
CSCvv36788	MsgLayer[PID]：エラー：Msglyr::ZMQWrapper::registerSender()：ZeroMQ ソケットのバインドに失敗した
CSCvv41811	CIAM：net-snmp 5.1 CVE-2019-20892
CSCvv43771	スケジュールされたバックアップに対して複数のデバイスを選択できない
CSCvv46490	SnortAttribConfig のエラーにより FMC でポリシーの展開が失敗する
CSCvv59036	ユーザーが削除していないのに、FMC から静的ルートが削除される。
CSCvv67196	FTD が crl ファイルを取得するためにすべての crl URL を試行しない
CSCvv89715	Firepower 8000 シリーズスタックの Fastpath ルールが FMC からランダムに消える
CSCvv90079	9300 シャーシ内クラスタで変更を行った後、ルータ BGP がプッシュされない
CSCvv90753	SLA が原因で同期プロセスがハングする
CSCvv92897	バージョン 6.6.0 にアップグレードすると、システムが以前欠落していた memcap 制限に達することがある
CSCvw05392	diagnostic-cli に常に表示されるメッセージ
CSCvw15359	KP fxos snmp に、EPM インデックスの entPhysicalSerialNum,entPhysicalAssetID に初期化されていない文字列がある
CSCvw33536	4100/9300：ポートチャネル/インターフェイスをアプリケーションに関連付けることができない
CSCvw38870	800_post/1027_ldap_external_auth_fix.pl で、6.6.0、6.6.1、6.6.3、6.7.0 への FMC のアップグレードが失敗する
CSCvw51436	Cisco ASA ソフトウェアおよび FTD ソフトウェアの SNMP アクセスの脆弱性
CSCvw55788	VTI インターフェイスからのトラフィックが間違ったルールにヒットする

不具合 ID	タイトル
CSCvw62255	Firepower 4100 で WSP-Q40GLR4L トランシーバと Arista スイッチを使用すると、「リンクが接続されていない（Link not connected）」エラーが発生する
CSCvw67974	FXOS のアップグレード後に公開キー認証を使用した SSH アクセスが失敗する
CSCvw72260	ASA のアップグレードが「CSP directory does not exist - STOP_FAILED Application_Not_Found」で失敗する
CSCvw72608	アクティブで受信したスタンバイの失敗イベントにより、スタンバイでの将来の展開がスキップされる
CSCvw74231	CIAM：linux-kernel 3.14.39 CVE-2020-14305 など
CSCvw74660	Syslog-ng パッチに問題がある可能性があるため、CC モードで Syslog-ng が起動しない
CSCvw77924	シャーシのリロード後に ASCII 文字「"」が設定された RADIUS キーが FXOS で機能しない
CSCvw79465	FXOS アップグレードが FTD イメージに対して適切な互換性チェックを実行しない
CSCvw81322	マルチインスタンスモードを実行している FTD が、SRU のインストールと展開後に snort GID 3 ルールを無効にする
CSCvw81976	ENH：fail-to-wire インラインペアのステータスを BYPASS-FAIL に変更
CSCvw83498	FTD-API：LDAP 属性マップで、ldapValue（スペースを含む）が処理されない
CSCvw83810	CIAM：curl 7.66.0 CVE-2020-8286 など
CSCvw85377	アクセスポリシーの URL フィルタリングルールで URL が更新されていない
CSCvw90634	FP2100 ASA：9.15.1.1 へのアップグレード後にネットワークモジュールがダウン/ダウンの 1 Gbps SFP
CSCvw90923	CCM レイヤ（スプリント 101、シーケンス 4）における WR6、WR8 および LTS18 コミット ID の更新
CSCvw93159	Firepower 2100：ASA および FTD が「Local disk 2 missing on server 1/1」というメッセージを生成する
CSCvw95181	FXOS のアップグレードが、「does not support application instances of deployment type container」というエラーで失敗する

不具合 ID	タイトル
CSCvw97201	ClamAV が原因で FTD が 6.7 にアップグレードされた後、SFDataCorrelator が終了する
CSCvw97256	リンク状態 API の読み取りが失敗した場合にリンク状態の更新を無視するには、rmu 読み取りエラーの処理が必要
CSCvw98315	FXOS は 6.7.0 への FTD アップグレード後に古い FTD バージョンを報告する
CSCvx05956	navl 属性のコピー中に snort CPU 使用率が高くなる
CSCvx06920	CCM レイヤ（スプリント 103、シーケンス 5）における WR6、WR8 および LTS18 コミット ID の更新
CSCvx14602	svc_sam_dcosAG の Firepower メモリリーク
CSCvx16700	「MIO が強制時刻同期に応答しない（MIO DID NOT RESPOND TO FORCED TIME SYNC）」ために、ブレードの起動中に FXOS クロック同期の問題が発生する
CSCvx19563	FDM：STO Certificate Trust Bundle を使用するには、さまざまなアイテムを更新する必要がある（QuoVadis ルート CA の問題）
CSCvx19934	6.6.3 で snmpv1 を削除し、snmpv3 を一度に追加すると、snmp 設定の展開が失敗する
CSCvx23907	CVE-2021-1405 に対する NGFW の影響を評価する
CSCvx25336	ENH：FQDN チェックを無効にする方法を追加
CSCvx27992	CIAM：open-ldap 2.4.48 CVE-2020-36230 など
CSCvx28070	廃止予定のため、スマートライセンスの QuoVadis ルート CA を更新する
CSCvx29429	CSCvx07389 の修正にもかかわらず、FPR4100/FPR9300 で ma_ctx*.log が大きなディスク領域を消費する
CSCvx29448	FTD：管理 int をポーリングできる診断 int で SNMP ホストが設定される
CSCvx32283	Cisco Firepower Management Center のオープンリダイレクトの脆弱性
CSCvx33904	1.9.5p2 より前の sudo には、ヒープベースのバッファオーバーフローがあり、特権昇格を使用できる
CSCvx38047	FXOS が障害警告コード F4526902 を表示する
CSCvx45976	スレッド名：vnet-proxy（rip：socks_proxy_datarelay）で ASA および FTD のウォッチドッグが強制的にトレースバックとリロードを実行する

不具合 ID	タイトル
CSCvx47550	CCM レイヤ（スプリント 105、シーケンス 6）での WR6、WR8 および LTS18 コミット ID の更新
CSCvx47634	GNU C ライブラリ（別名 glibc または libc6）2.32 の iconv 関数
CSCvx47895	Cisco ASA ソフトウェアおよび FTD ソフトウェアにおけるアイデンティティベースのルールバイパスの脆弱性
CSCvx49005	CIAM：openssl 1.1.1g
CSCvx50636	TLS1.3 フローが原因で Snort プロセスがトレースバックして再起動することがある
CSCvx50980	ASA CP の誤った計算により、パーセンテージが高くなる（CP CPU 100%）
CSCvx52541	SSEConnector 設定を更新して、CA バンドル /etc/ssl/certs.pem を使用できるようにする
CSCvx55664	Cisco Firepower Management Center のクロスサイト スクリプティングの脆弱性
CSCvx66329	FTD ホットフィックス Cisco_FTD_SSP_FP2K_Hotfix_O のインストールがスクリプト 000_start/125_verify_bundle.sh で失敗する
CSCvx66494	MIO での CIMC ウォッチドッグリセットの処理
CSCvx67468	CCM レイヤ（スプリント 107、シーケンス 6）での WR6、WR8 および LTS18 コミット ID の更新
CSCvx67996	FMC RAVPN：IPv6 DNS がグループ ポリシーで設定されている場合、展開が失敗する
CSCvx71156	アクセスリストが 6.7 で機能していない
CSCvx79526	Cisco ASA および FTD ソフトウェアのリソースの枯渇で確認されたサービス拒否攻撃に対する脆弱性
CSCvx79793	SSL ポリシーを使用したファイル転送またはファイルアップロードが低速で、復号化の再署名アクションが適用される
CSCvx82705	OpenSSL の 2021 年 3 月の脆弱性に対する SSP の評価
CSCvx86231	999_finish/935_change_reconciliation_baseline.pl での 6.6.3 への FMC アップグレードの失敗
CSCvx86283	Cisco Firepower Threat Defense ソフトウェアのコマンドインジェクションの脆弱性
CSCvx89827	FPR 2110 でバンコクタイムゾーンを設定できない

不具合 ID	タイトル
CSCvx95255	既存の ASDM コンテキストスイッチから新しい ASDM 接続を区別するための ASA のサポート変更
CSCvx95652	ASAv Azure：一定期間の実行後、一部またはすべてのインターフェイスがトラフィックの通過を停止する場合がある
CSCvx98041	FTD-API：ruleId の重複するシーケンス番号により、無効な snort ngfw.rules が展開される
CSCvx98807	CCM レイヤ（スプリント 109、シーケンス 9）での WR6、WR8 および LTS18 コミット ID の更新
CSCvy02240	Cisco Firepower Threat Defense イーサネット産業用プロトコルのポリシーバイパスの脆弱性
CSCvy02247	Cisco Firepower システム ソフトウェア ルール エディタの影響のないバッファオーバーフローの脆弱性
CSCvy03045	管理のコンテキストが変更されると、マルチコンテキスト ASA から connect fxos admin で FXOS にアクセスできない
CSCvy04959	FXOS：「メモリリーク」が appAG プロセスのトレースバックとリロードを引き起こす場合がある
CSCvy04965	WM スタンバイが HA への再参加に失敗し、「CD App Sync エラーがスタンバイで SSP 設定を適用できませんでした」というメッセージが表示される
CSCvy05966	Snort 2.9.16.3-3033 トレースバック（FTD 6.6.3）
CSCvy08798	CCM レイヤ（スプリント 110、シーケンス 10）での WR6、WR8 および LTS18 コミット ID の更新
CSCvy09217	暗号の不一致が原因で HA がアクティブ/アクティブ状態になる
CSCvy09252	Syncd が FMC HA のセカンダリの FMC 部分で繰り返し終了する
CSCvy10789	LDAP パスワードで FTD 2110 ASCII 文字を使用できない
CSCvy13229	FDM - GUI にアクセスできない（tomcat が開いているファイル記述子が多すぎる）
CSCvy13543	Cisco Firepower Threat Defense ソフトウェアの SSH 接続で確認されたサービス拒否攻撃に対する脆弱性
CSCvy16559	Cisco Firepower Threat Defense ソフトウェアのコマンドインジェクションの脆弱性

不具合 ID	タイトル
CSCvy16573	Cisco Firepower Threat Defense のコマンドインジェクションの脆弱性
CSCvy19136	証明書認証が使用される場合に Web ポータルで永続的なリダイレクトが発生する
CSCvy19225	Cisco Firepower Threat Defense のコマンドインジェクションの脆弱性
CSCvy20504	Cisco ASA および FTD ソフトウェア Web サービスインターフェイスで確認されたクロスサイト スクリプティングの脆弱性
CSCvy23349	FTD がインラインペア展開で TCP フローを不必要に ACK する
CSCvy31400	FPR1K：速度の自動ネゴシエーションが無効になっているため、ファイバー SFP インターフェイスがダウンする
CSCvy31424	QP FTD アプリケーションが、FXOS/FTD アップグレード後に古い affinity.conf が原因で起動に失敗する
CSCvy34333	ASA のアップグレードに失敗した場合、プラットフォームとアプリケーションの間でバージョンステータスの同期が解除される
CSCvy35948	CCM レイヤ（スプリント 111、シーケンス 11）での WR6、WR8 および LTS18 コミット ID の更新
CSCvy36910	Cisco 適応型セキュリティアプライアンスと Firepower Threat Defense ソフトウェアの DoS の脆弱性
CSCvy39791	Lina のトレースバックとコアファイルサイズが 40G を超えており、圧縮に失敗する
CSCvy40482	9.14MR3：snmpwalk が [Errno 146] の接続拒否エラーで失敗した
CSCvy41757	Cisco Firepower Threat Defense ソフトウェアにおける CLI 任意ファイルの書き込みの脆弱性
CSCvy41771	Cisco Firepower Management Center ソフトウェアの認証されたディレクトリトラバーサルの脆弱性
CSCvy43187	Cisco 適応型セキュリティアプライアンスと Firepower Threat Defense ソフトウェアの DoS の脆弱性
CSCvy51814	Firepower フローオフロードが、すべての既存およびおよび新しいフローのオフロードを停止させる
CSCvy55054	Cisco 適応型セキュリティアプライアンスと Firepower Threat Defense ソフトウェアの DoS の脆弱性
CSCvy58278	config-request リクエストを処理するサービス拒否の脆弱性

不具合 ID	タイトル
CSCvy61008	Lina と FXOS 間の同期外れの時間
CSCvy64145	CCM レイヤ（スプリント 113、シーケンス 12）での WR6、WR8 コミット ID の更新
CSCvy65802	AppAgent のハートビートの強化
CSCvy66942	9300/4100 スーパーバイザで REST API LTP を使用して FPR4100/9300 IPv6 設定を適用することができない
CSCvy69730	Cisco FMC ソフトウェア設定情報開示の脆弱性
CSCvy72118	navl 属性のコピー中に snort CPU 使用率が高くなる（断片化されたメタデータ）
CSCvy72194	Cisco FMC ソフトウェアにおける設定情報開示の脆弱性
CSCvy73585	FMC は、FPR1010 で 8 を超えるポートチャネル ID の設定を許可できない
CSCvy80325	ios pem ファイルを vFTD のパッチ アップグレード パッケージに含める
CSCvy83116	FTD 1000 スタンバイが HA への再参加に失敗し、「CD App Sync エラーは SSP 設定の生成に失敗しました」というメッセージが表示される
CSCvy83657	FXOS プロセスコアがシステムファイルからプルーニングされたか、または削除された（検証なし）
CSCvy89144	Cisco ASA および FTD の Web サービスで確認されたサービス拒否攻撃に対する脆弱性
CSCvy89440	s2sCryptoMap 設定の損失
CSCvy93480	Cisco ASA および FTD ソフトウェアの IKEv2 サイト間 VPN で確認されたサービス拒否攻撃に対する脆弱性
CSCvy95329	AC ルールエントリが見つからないため、アクセスルールが正しく一致しない
CSCvy96625	CSCvr33428 および CSCvy39659 によって導入された変更をロールバックする
CSCvy96698	FXOS portmgr で速度値を 2 回チェックするスプリアス ステータス アクションを解決する
CSCvz05767	FP-1010 HA リンクがダウンするか、新しいホストがデバイスに接続できない
CSCvz14616	SFDataCor プロセスがスタックしているため、接続イベントがない

不具合 ID	タイトル
CSCvz15676	Firepower 1010 デバイスで、ASA アプリをアップグレードした後、デバイスがフェイルセーフモードになる
CSCvz27235	複数のシスコ製品の Snort Modbus におけるサービス妨害の脆弱性
CSCvz32386	FMC が同じ暗号マップのエントリに PFS21 および IKEv1 設定をプッシュするときの FTD 展開エラー
CSCvz38811	削除されたファイルが Java プロセスでディスク容量を保持している
CSCvz53993	SSL フローでの Snort によるランダムなパケットのブロック
CSCvz59464	IPReputation フィードエラー メッセージ：メソッドが許可されていません
CSCwa46963	セキュリティ：CVE-2021-44228 → Log4j 2 における脆弱性
CSCwa70008	期限切れの証明書がセキュリティ Intel を引き起こし、マルウェアファイルの事前分類署名の更新が失敗する
CSCwa87714	6.7.0.3: SRU 更新時にピア証明書を既知の CA 証明書で認証できない
CSCwa88571	スマートポータルを使用して FMC を登録できない

バージョン 6.7.0.2 で解決済みの問題

表 *38* : バージョン *6.7.0.2* で解決済みの問題

不具合 ID	タイトル
CSCvh19737	FTD データインターフェイス（オフボックス管理）での HTTPS アクセスが失敗する
CSCvm82290	IRB/TFW 設定でホストが到達不能な場合に ASA コアブロックが枯渇する
CSCvp69936	ASA：tcp_intercept スレッド名 thread detection でのトレースバック
CSCvs72450	FXOS：サービスモジュールの hwclock を同時書き込みコリジョンによる破損から修復
CSCvs82926	ASA「Chassis 0 Cooling Fan OK」SCH メッセージを使用した FPR2100 シリーズの重大な RPM アラート
CSCvu91097	Cisco Firepower Management Center ソフトウェアにおけるポリシーの脆弱性
CSCvv19230	ASAv AnyConnect ユーザがアイドルタイムアウトで予期せず切断される
CSCvv70984	ブックマーク SSL 暗号設定の変更中の ASA トレースバック

不具合 ID	タイトル
CSCvv85029	スレッド名 ace_work で ASA5555 がトレースバックし、リロードする
CSCvv86861	夜間に VPN、EMIX、および SNMP トラフィックを実行中に、タイマーで KP をトレースバックする
CSCvv89708	ASA/FTD がスレッド名 fover_FSM_thread でトレースバックし、リロードすることがある
CSCvv97877	セカンダリユニットがクラスタに参加できない
CSCvw16165	ポートチャネルのメンバーがダウンすると、Firepower 1000 シリーズがトラフィックの通過を停止する
CSCvw16619	オフロードされたトラフィックが ECMP セットアップでセカンダリルートにフェールオーバーされない
CSCvw18614	LINA プロセスでの ASA トレースバック
CSCvw19272	複数のシスコ製品での Snort HTTP 検出エンジンのファイルポリシーバイパスの脆弱性
CSCvw23199	スレッド名 Logger での ASA/FTD のトレースバックとリロード
CSCvw24084	snmp/snmp_config_utils.c で Rip Netsnmp_config_req_dequeue_and_send+269 を使用すると、SNMP で FTD がクラッシュすることがある
CSCvw26544	Cisco ASA および FTD ソフトウェアの SIP で確認されたサービス拒否攻撃に対する脆弱性
CSCvw38614	リブート時に AZURE ASA/FTD NIC MAC アドレスが並べ替えられることがある
CSCvw43486	PBR 設定変更時の ASA/FTD トレースバックとリロード
CSCvw46630	FTD：NLP パスでリターン ICMP 接続先到達不能メッセージがドロップされている
CSCvw51307	プロセス名「Lina」で ASA/FTD がトレースバックおよびリロードする
CSCvw51950	FPR 4K：手動フェールオーバー後に新しいアクティブ ASA から SSL トラストポイントが削除される
CSCvw51985	ASA：IPv6 DACL 障害により、AnyConnect セッションを再開できない
CSCvw53596	FPR4120：cli_xmlserver_thread の Lina ウォッチドッグ トレースバック
CSCvw53796	Cisco ASA および FTD Web サービスインターフェイスで確認されたクロスサイト スクリプティングの脆弱性

不具合 ID	タイトル
CSCvw59035	FTD BVI アドレスから直接接続された IP への接続の問題
CSCvw71766	IKev 2 Daemon スレッドでの ASA トレースバックおよびリロード
CSCvw76572	FMC を 6.7 にアップグレードした後、ポリシーマップテーブルに 1000 を超えるエントリがある場合、展開に失敗する
CSCvw79542	「証明書eoが定義されていません」が原因でポリシーの展開が失敗する。
CSCvw81897	ASA：OpenSSL の脆弱性 CVE-2020-1971
CSCvw82629	ACL に関する「設定セッション」の変更時に ASA トレースバックが発生する。
CSCvw83572	バージョン 9.14.1.30 以降で BVI HTTP/SSH アクセスが機能しない
CSCvw84339	ホスト名が 30 文字を超えると、FTD の管理対象デバイスのバックアップが失敗する
CSCvw87788	ASA トレースバックとリロードの WebVPN スレッド
CSCvw89365	証明書の変更中に ASA/FTD がトレースバックおよびリロードすることがある。
CSCvw93139	Cisco ASA および FP 1000/2100 シリーズ コマンド インジェクションの FTD ソフトウェアの脆弱性
CSCvw93272	Cisco Firepower Management Center ソフトウェアのクロスサイト スクリプティングに対する脆弱性
CSCvw93276	Cisco Firepower Management Center ソフトウェアのクロスサイト スクリプティングに対する脆弱性
CSCvw93282	Cisco Firepower Management Center ソフトウェアのクロスサイト スクリプティングに対する脆弱性
CSCvw93513	Cisco Firepower Management Center ソフトウェアのクロスサイト スクリプティングに対する脆弱性
CSCvw95301	キャプチャが削除されたときに ASA がトレースバックを実行し、スレッド名：ssh でリロードされる
CSCvw95368	ASA： Remote Access VPN が有効な場合、emweb/https でトレースバックを実行し、リロードされる
CSCvw96488	inspect_h323_ras+1810 のトレースバック
CSCvw97256	リンク状態APIの読み取りが失敗した場合にリンク状態の更新を無視するには、rmu 読み取りエラーの処理が必要

不具合 ID	タイトル
CSCvw97821	ASA：CoA で dACL が提供されない場合、VPN トラフィックが渡されない
CSCvw98840	ASA：CoA 後の v6 トラフィックに IPv6 エントリのない dACL が適用されない
CSCvw99916	ASAv：9.14 へのアップグレード後に使用されたメモリ値の SNMP 結果が正しくない
CSCvx01381	手動時刻設定用の FMC GUI の [Year] ドロップダウンリストに 2020年 までしか表示されない
CSCvx01786	FCM WebUI にログイン前バナーが表示されない
CSCvx02869	スレッド名のトレースバック：Lic TMR
CSCvx03764	アイデンティティ NAT トラフィックおよびクラスタリング環境では、オフロード書き換えデータを修正する必要がある
CSCvx04057	SGT 名が未解決のまま ACE で使用されている場合、回線が無視または非アクティブ状態にならない
CSCvx04643	ASA のリロードで「content-security-policy」設定が削除される
CSCvx05381	Cisco ASA および FTD ソフトウェアのコマンドインジェクションの脆弱性
CSCvx05385	ASA が HA の設定同期中にロガースレッドでトレースバックを生成することがある
CSCvx06385	6.6.1 へのアップグレード後に FPR 2100 の Fail-to-wire ポートがフラッピングする
CSCvx08734	ASA：デフォルトの IPv6/IPv4 ルートトンネリングが機能しない
CSCvx09164	FDM v6.6 から v6.7 へのアップグレードにより、snort3 の呼び出しが失敗する
CSCvx09535	ASA トレースバック：失効した証明書でリロードがトリガーされる AnyConnect クライアントの CRL チェック
CSCvx11295	スレッド Crypto CA で ASA がトレースバックおよびリロードする
CSCvx11460	リモートエンドで TFC が有効になっている状態で Firepower 2110 がトラフィックをサイレントにドロップする
CSCvx13694	スレッド名 PTHREAD-4432 で ASA/FTD トレースバックする
CSCvx14564	CD アプリの同期エラーで無効状態となっている 1000 シリーズ FTD - スタンバイ状態で SSP 設定の適用に失敗する

不具合 ID	タイトル
CSCvx15040	ASA/FTD で DHCP プロキシオファーがドロップされる
CSCvx17664	ASA がスレッド名「webvpn_task」でトレースバックおよびリロードすることがある
CSCvx17780	FPR-2100-ASA：最新バージョンの ASA インターフェイスで ifType の SNMP ウォークに「other」が表示される
CSCvx17785	ACL を追加または削除し、route-map コマンドに入力すると、クラッシュが絶えず発生する
CSCvx17842	FMC から送信されたオブジェクトループによる lina のトレースバックを防ぎます。代わりに展開を失敗させます。
CSCvx20303	ASA/FTD が SNMP ホストグループオブジェクトの変更後にトレースバックすることがある
CSCvx22695	OCSP 応答データのクリーンアップ中のに ASA がトレースバックおよびリロードする
CSCvx25719	X-Frame-Options ヘッダーが webvpn 応答ページで設定されていない
CSCvx25836	「show crashinfo」による新しい出力ログの追加で ASA がトレースバックおよびリロードする
CSCvx26221	handle_agentx_packet / snmp で SNMP にトレースバックすると、FP1k および 5508 での起動に時間がかかる
CSCvx26808	FPR2100 シリーズのプロセス lina での FTD のトレースバックおよびリロード
CSCvx27430	ASA：FIPS が有効な場合、PAC ファイルをインポートできない
CSCvx29771	フローオフロードによる一括ルーティング更新後にファイアウォール CPU が増加することがある
CSCvx29814	DHCP GIADDR フィールドの IP アドレスが DHCP DECLINE を DHCP サーバに送信した後に反転する
CSCvx30735	Cisco Firepower Device Manager ソフトウェアにおけるファイルシステム容量の枯渇によるサービス拒否の脆弱性
CSCvx34237	FIPS 障害による ASA のリロード
CSCvx41171	ACL 設定を同時に変更すると、「show running-config」の出力が完全に中断される

不具合 ID	タイトル
CSCvx42081	FPR4150 ASA Standby Ready ユニットのループが失敗し、設定を削除してインストールし直す必要がある
CSCvx42197	ASA EIGRP ルートがネイバーの切断後にスタックする
CSCvx44401	スレッド名 Unicorn Proxy Thread で FTD/ASA がトレースバックする
CSCvx47230	IE および Windows プラットフォームの古いバージョンの X-Frame-Options ヘッダーのサポート
CSCvx50366	スレッド名 fover_health_monitoring_thread でのトレースバック
CSCvx52122	トランスペアレントコンテキストの削除中の SNMP 通知スレッドでの ASA トレースバックとリロード
CSCvx54235	ASP キャプチャの dispatch-queue-limit にパケットがないと表示される
CSCvx54396	マルチキャストが有効な場合、FTD での展開が失敗する
CSCvx54606	FTD 6.6.1/6.7.0 が SNMP Ifspeed OID （1.3.6.1.2.1.2.2.1.5）応答値＝0 を送信している
CSCvx57417	スマートトンネルコード署名証明書の更新
CSCvx59120	データトンネルが起動する前に COA を受信すると、親セッションが切断される
CSCvx63647	スレッド名 CTM Daemon での ASA トレースバックおよびリロード
CSCvx68128	ASA 内部デッドロックにより、機能（syslog、リロード、ASDM、anyconnect）が失われる
CSCvx68785	FTD-API：展開 API によりレコードをシリアル化できない
CSCvx69405	スレッド名 SNMP ContextThread での ASA トレースバックおよびリロード
CSCvx71434	asa_run_ttyS0 スクリプトによるスレッド名 pix_startup_thread での ASA/FTD トレースバックおよびリロード
CSCvx72904	ifmibポーリングの最適化
CSCvx74035	複数の ACL とオブジェクトが設定された状態で「clear configure all」を実行すると、ASA がトレースバックおよびリロードする
CSCvx76233	システムイメージをフラッシュにコピーするときのスレッド ci/console での ASA トレースバックおよびリロード

バージョン 6.7.0.1 で解決済みの問題

表 *39* : バージョン *6.7.0.1* で解決済みの問題

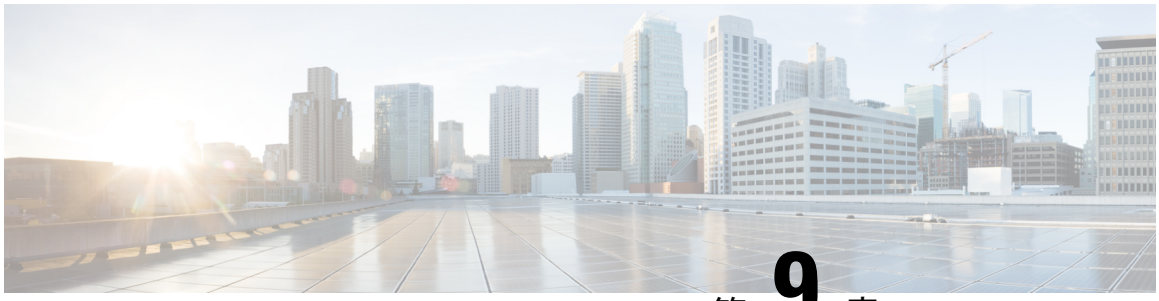
不具合 ID	タイトル
CSCvg69380	ASA：まれに発生した CP 処理での破損によってコンソールロックが発生する
CSCvo34210	スレッド名 Unicorn Proxy Thread で ASA が 9.6.4.20 トレースバックを実行する
CSCvr33428	FMC が SYN フラッド攻撃から接続イベントを生成する
CSCvr85295	Cisco Adaptive Security Appliance と Firepower Threat Defense ソフトウェア リモート
CSCvs13204	SR-IOV インターフェイス上の ASAv フェールオーバー トラフィックが、インターフェイスのダウンによりドロップされることがある
CSCvs84542	スレッド idfw_proc での ASA のトレースバック
CSCvt71529	SSL ハンドシェイク中の ASA のトレースバックとリロード
CSCvt75760	HTTP クリーンアップによるクライアントレス WebVPN のトレースバックまたはページ障害
CSCvt77665	[ciam] GNU readline _rl_tropen 機能の安全でない一時ファイルの脆弱性
CSCvu64784	CIAM：linux-kernel 3.14.39 で脆弱性を調査する必要がある（2015 年以前）
CSCvu64884	CIAM：linux-kernel 3.14.39 の脆弱性（2017 ～ 2020 年、SIR：Medium）
CSCvu70493	FXOS：AAA/RADIUS：NAS-IP フィールドを 127.0.01 に設定
CSCvu96592	CIAM：pcre 8.35 および 8.38
CSCvu98222	SSL 復号ポリシーを有効にした後、FTD Lina エンジンがデータパスでトレースバックすることがある
CSCvv15572	新しいコンテキストの作成中に「config-url」を入力すると、ASA のトレースバックが発生する
CSCvv17585	特定の状況下で Netflow テンプレートが送信されない
CSCvv36393	statsAG メモリリーク
CSCvv52349	2100/1000 シリーズ Firepower デバイスに XFS 破損を処理するユーティリティがない

不具合 ID	タイトル
CSCvv58480	FXOS：DC PSU の電圧が「ステータスの表示（show stats）」の誤った値で表示される
CSCvv66005	inspect esmtp での ASA のトレースバックとリロード
CSCvv67500	DATAPATH での ASA 9.12 のランダムトレースバックおよびリロード
CSCvv72466	ASA のアップグレード後、startup-config で OSPF ネットワークコマンドが欠落する
CSCvv73017	fover および SSH スレッドによるトレースバック
CSCvv80782	トレースバックにより purg_process となる
CSCvv84358	起動時の VIC アダプタカーネルクラッシュ
CSCvv85742	アップグレード：アップグレード後に FSM ステータスに不正な値が表示されることがある
CSCvv86926	コアファイルを作成する FTD での予期しないトレースバックとリロード
CSCvv87232	ASA：igb_saleen_io_sfp_mod_poll_thread プロセスで CPU 専有の値が高くなる
CSCvv88017	ASA：EasyVPN HW クライアントが重複したフェーズ 2 のキー再生成をトリガーし、トンネル経由で切断される
CSCvv90720	ASA/FTD：HA スイッチオーバー後に接続されたスイッチで MAC アドレステーブルのフラッピングが表示される
CSCvv94165	FTD 6.6：snmpd プロセスの CPU がスパイクする
CSCvv94701	ASA が「octnic_hm_thread」でリロードし続け、リロード後は回復するまでに非常に長い時間がかかる
CSCvv95277	FPR2100 httpd ログファイルの増加により、パーティション /opt/cisco/platform/logs のディスク使用率が高い
CSCvv96092	Cisco FXOS および NX-OS ソフトウェアの UDLD DoS と任意のコード実行の脆弱性
CSCvv98751	CIAM：linux-kernel 3.14.39 CVE-2020-14386 など
CSCvv98764	CIAM：libproxy 0.4.11 CVE-2020-25219
CSCvv98773	CIAM：gnutls 3.3.5 CVE-2020-24659
CSCvv98959	[ciam] GNOME プロジェクト libxml2 v2.9.10 以前で、グローバル バッファ オーバーフローが発生する

不具合 ID	タイトル
CSCvw00161	Firepower 2140 での VPNス レッドによる ASA のトレースバックとリロード
CSCvw07000	PDTS Tx キューがスタックしたまま Snort がビジー状態でドロップする
CSCvw12008	「show tech-support」コマンドの実行中の ASA トレースバックとリロード
CSCvw12100	サイト間セッションおよび AnyConnect セッションで ASA の古い VPN コンテキストが表示される
CSCvw13348	CCM レイヤ（スプリント 98、シーケンス 2）における WR6、WR8 および LTS18 コミット ID の更新
CSCvw19401	メモリリーク：DME プロセスが Firepower 4100/9300（M5 シリーズのみ）で生成されるコアをトレースバックする場合がある
CSCvw19907	agx 通信の snmpd の再起動が snmp-sa に対して失敗する
CSCvw21844	カプセル化されたフローを処理する際の DATAPATH スレッドでの FTD トレースバックとリロード
CSCvw22435	FXOS 2.8.1 で「copy ftp: wrokspace:」を使用するとエラー「該当するファイルまたはディレクトリがありません（No such file or directory）」が発生する
CSCvw22881	radius_rcv_auth により、コントロールプレーンの CPU 使用率が 100% になることがある
CSCvw22986	プライマリユニットのインターフェイスが init 状態のままであるため、セカンダリユニットがバルク同期状態で無限にスタックする
CSCvw24556	フローオフロードが有効になっている場合、TCP ファイル転送（ビッグファイル）が正しく閉じない
CSCvw24642	CIAM：linux-kernel 3.14.39 CVE-2020-25645 など
CSCvw26171	strncpy NULL 文字列が SSL ライブラリから渡されている間の ASA syslog トレースバック
CSCvw26331	スレッド名 ci/console での ASA のトレースバックとリロード
CSCvw27072	セカンダリノードで SNMP V3 ウォークが認証エラーで失敗する
CSCvw27301	EAP を使用した IKEv2 で、MOBIKE ステータスが処理されない
CSCvw28814	QP を v9.14.1.109 にアップグレード中に SNMP プロセスがクラッシュした
CSCvw30252	ASA/FTD が SNMP のメモリ破損によりトレースバックおよびリロードすることがある

不具合 ID	タイトル
CSCvw31569	ディレクタ/バックアップフローは残され、このフローに関連するトラフィックがブラックホール化される
CSCvw32518	9.12(4)4 以降にアップグレード後の ASASM トレースバックおよびリロード
CSCvw36662	TACACS+ ASCII パスワード変更要求が正しく処理されない
CSCvw37259	デバイスがハング状態になるまで 600/秒のレートで VPN syslog が生成される
CSCvw38984	Cisco FXOS および NX-OS ソフトウェアの UDLD DoS と任意のコード実行の脆弱性
CSCvw42999	FPR2110 上の 9.10.1.11 ASA がランダムにトレースバックおよびリロードする
CSCvw44122	ASA：非 DNS トラフィックを DNS 検査エンジンにリダイレクトする「class-default」クラスマップ
CSCvw44182	CIAM：tcp-dump 4.9.3 CVE-2020-8037
CSCvw45863	リロード時の ASAv SNMP トレースバック
CSCvw46885	SNMP および管理アクセス設定に関連する ASA/FTD トレースバックおよびリロード
CSCvw47321	一部の FPR プラットフォームのインバウンドトラフィックの IPSec トランスポート モード トラフィックの破損
CSCvw48517	ASA を 9.13(1)13 にアップグレードすると、DAP が動作しなくなる
CSCvw48829	「show clock」のタイムゾーンが「show run clock」のタイムゾーンと異なる
CSCvw51462	IPv4 デフォルトトンネルルートが拒否される
CSCvw53427	ASA が複数のクエリパラメータを含む SAML アサーションで HTTP POST を処理できない
CSCvw53494	リリースビルドで CRUZ paloview にアクセスできない
CSCvw53884	ASA5506 上の M500IT モデルのソリッドステートドライブが 3 年 2 ヵ月のサービス期間後に応答しなくなることがある
CSCvw54640	FPR-4150：スレッド名 DATAPATH での ASA トレースバックおよびリロード

不具合 ID	タイトル
CSCvw58414	タイプ dynamic-split-exclude-domains の AnyConnect カスタム属性の名前がリロード後に変更される
CSCvw63862	ASA：ランダムな L2TP ユーザが古い ACL フィルタエントリが原因でリソースにアクセスできない
CSCvw74940	IKE デーモンでの ASA トレースバックおよびリロード
CSCvw83780	プロセス名：lina におけるスタンバイ FTD 6.6.1 コア
CSCvw84786	スレッド名 snmp_alarm_thread での ASA トレースバックおよびリロード
CSCvx09123	ISA3000 上の M500IT モデルのソリッドステートドライブが 3 年 2 ヵ月のサービス期間後に応答しなくなることがある
CSCvx09248	v2 および v3 の SNMP ウォークが失敗し、この OID でこのエージェントで使用可能なオブジェクトがありませんと表示される
CSCvx30314	スレッド名 DATAPATH での ASA 9.15.1.7 トレースバックおよびリロード



第 9 章

既知の問題

便宜上、リリースノートには、メジャーリリースの既知の問題が記載しています。メンテナンスリリースまたはパッチの既知の問題は記載していません。

サポート契約がある場合は、Cisco Bug Search Tool を使用して最新のバグリストを取得できます。検索では、特定の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。バグのステータス、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。

重要 バグリストは1回自動生成され、その後は更新されません。バグ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。

• バージョン 6.7.0 で未解決のバグ （125 ページ）

バージョン 6.7.0 で未解決のバグ

表 *40* : バージョン *6.7.0* で未解決のバグ

不具合 ID	タイトル
CSCvv59527	pxGridv2 エンドポイントのダウンロードが応答せず ADI、SFDataCorrelator を切断する
CSCvv95130	FTD デバイス（ASA 5500-X および Firepower 1000/2100 シリーズ）がバックアップからの復元後に応答しない
CSCvv99419	[6.7.0] FDM Snort 3 SSL ポリシーの追加/削除により、Snort が UI 警告なしで再起動する
CSCvw20092	レトロスペクティブイベントによって作成されたマルウェアイベントの eStreamer イベントでファイルポリシーが設定されていない

不具合 ID	タイトル
CSCvw41726	FMC モニターリング、手動の Syslog 設定によりページが不規則に動作する
CSCvw46630	FTD：NLP パスでリターン ICMP 接続先到達不能メッセージがドロップされている
CSCvw48743	接続ベースのデバッグでパフォーマンスが低下する
CSCvw51105	IPv6 が設定されている場合、ISE 3.0 への 6.7.0 FMC pxGrid 接続が機能しない
CSCvx71029	SFP リンクを使用して FPR デバイスに接続されたスイッチでは、速度の自動ネゴシエーションの無効化が必要になる場合があります。