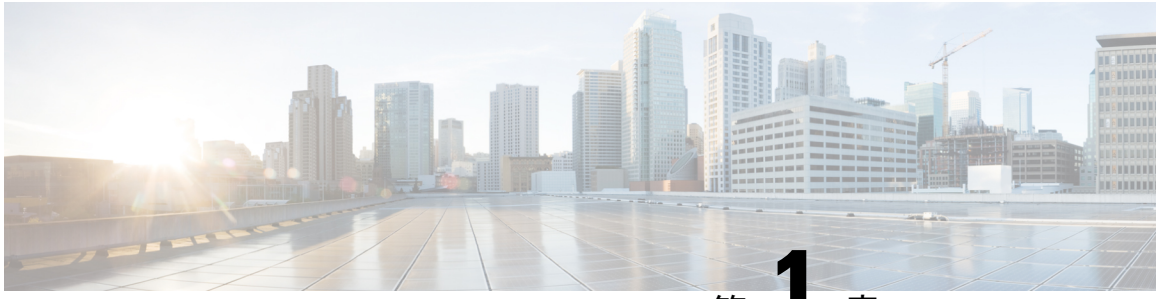
Cisco Firepower バージョン 7.0 リリースノート

初版：2021 年 5 月 26 日

最終更新：2022 年 6 月 30 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

目 次



第 1 章

ようこそ

このドキュメントでは、以下に示す Version7.0 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、お客様が導入した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）、またはクラウド提供型の管理センターで 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

リリース番号：バージョン 7.0 の理由

バージョン 6.7 からバージョン 7.0 へのリリース番号はスキップされます。

これは、複数のパフォーマンスとセキュリティの強化に加えて、過去数回のリリースで導入された主要な新機能による優れた価値を強調しています。バージョン 7.0 へのアップグレードに関して、予期しない非互換性や制限はありません。互換性、アップグレード要件、廃止された機能などの詳細については、以下のリリースノートをお読みください。

バージョン 7.0 は、『Cisco's Next Generation Firewall Product Line Software Release and Sustaining Bulletin』で説明したとおり、長い時間をかけて完成させたリリースです。

FTD と FMC 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。

Snort 3 を使用する利点は次のとおりですが、これに限定されません。

- パフォーマンスの向上。
- SMBv2 インスペクションの改善。
- 新しいスクリプト検出機能。
- HTTP/2 インスペクション。
- カスタムルールグループ。
- カスタム侵入ルールを記述しやすくする構文。
- 侵入イベント内の「would have dropped」インライン結果の理由。
- VDB、SSL ポリシー、カスタム アプリケーション ディテクタ、キャプティブポータル ID ソース、および TLS サーバ ID 検出へ変更を展開するときに Snort が再起動しない。
- Cisco Success Network に送信される Snort 3 固有のテレメトリデータ、およびトラブルシューティングログの改善による、有用性の向上。

Snort 3 侵入ルールの更新は、SRU ではなく LSP（Lightweight Security Package）と呼ばれます。Snort 2 には引き続き SRU が使用されます。シスコからのダウンロードには、最新の LSP と SRU の両方が含まれており、設定に適したルールセットが自動的に使用されます。

FMC は、Snort 2 と Snort 3 の両方のデバイスでの展開を管理でき、各デバイスに正しいポリシーを適用します。ただし、Snort 2 とは異なり、FMC のみをアップグレードしてから展開することで、デバイス上の Snort 3 を更新することはできません。Snort 3 では、新しい機能と解決済みのバグにより、FMC 上のソフトウェアとその管理対象デバイスをアップグレードする必要があります。各ソフトウェアバージョンに含まれている Snort の詳細については、Cisco Firepower Compatibility Guideのバンドルされたコンポーネントのセクションを参照してください。

重要 Snort 3 に切り替える前に、Firepower Management Center Snort 3 Configuration Guideを読んで理解することを強く推奨します。機能の制限と移行手順には特に注意してください。Snort 3 へのアップグレードは影響を最小限に抑えるように設計されていますが、機能は正確にマッピングされません。慎重に計画して準備することで、トラフィックが期待どおりに処理されるようにできます。

Snort 3 の Webサイト（https://snort.org/snort3）にもアクセスできます。https://snort.org/snort3

リリース日

表 *1*：バージョン *7.0* のリリース日

バージョン	ビルド	日付	プラットフォーム
7.0.3	37	2022 年 6 月 30 日	すべて（All）
7.0.2.1	10	2022 年 6 月 27 日	すべて（All）
7.0.2	88	2022 年 5 月 5 日	すべて（All）
7.0.1.1	11	2022-02-17	すべて
7.0.1	84	2021 年 10 月 7 日	すべて
7.0.0.1	15	2021 年 7 月 15 日	すべて
7.0.0	94	2021 年 5 月 26 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 Secure Firewall Management Center の新機能（リリース別）
- Cisco Secure Firewall 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-70-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/

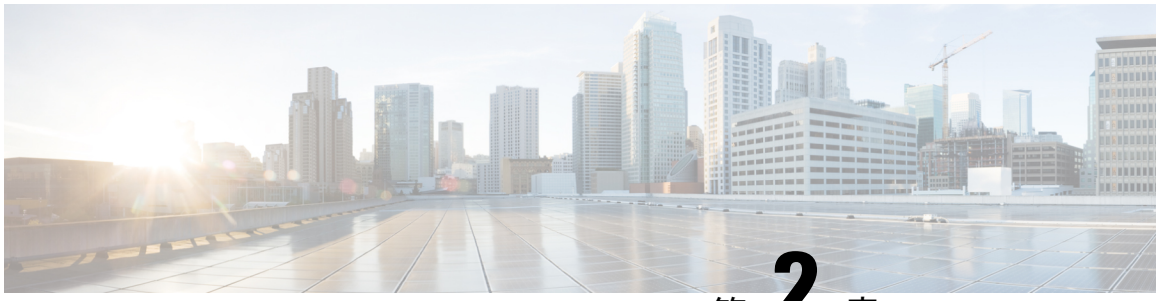
- シスコ通知サービス：https://www.cisco.com/cisco/support/notifications.html

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、Version7.0 のシステム要件を記載します。

デバイスプラットフォーム

このドキュメントでは、Version7.0 でサポートされているデバイスと管理方法を記載します。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。

デバイスの管理方式

次のデバイス管理方法をサポートしています。

- Firepower Management Center：複数のデバイスをリモートで管理します。FMC は、お客様が導入したハードウェアまたは仮想プラットフォームとして、または Cisco Defense Orchestrator（CDO）プラットフォームを使用するシスコが管理するクラウド導入として利用できます。お客様が導入したハードウェアまたは仮想 FMC では、その管理対象デバイスと同じかより新しいバージョンを実行する必要があります。クラウド提供型の管理センターにはバージョンの概念がなく、シスコが機能を更新します。
- Firepower Device Manager：単一の FTD デバイスをローカルで管理します。
- FDM 搭載 Cisco Defense Orchestrator（CDO）：FMC の代わりに、複数の FTD デバイスをリモートで管理します。一部の構成では引き続き FDM が必要ですが、CDO を使用することで、展開したすべての FTD を通して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。
- ASDM：単一の ASAFirePOWER モジュールをローカルで管理します。ASA FirePOWER は、ASA デバイスに個別にインストールされるモジュールです。ASA ファイアウォール

ポリシーが適用された後に、トラフィックがモジュールに送信されます。新しいバージョンの ASDM では、新しいバージョンの ASA FirePOWER モジュールを管理できます。

FTD ハードウェア

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

表 *2 : Version7.0 FTD* ハードウェア

プラットフォーム	FMC 互換		FDM 互換		注記
	お客様が導入	クラウド提供型	FDM のみ	FDM + CDO	
Firepower 1010、1120、1140、1150	**YES**	**YES** 7.0.3 以降のバージョンが必要です。	**YES**	**YES**	—
Firepower 2110、2120、2130、2140	**YES**	**YES** 7.0.3 以降のバージョンが必要です。	**YES**	**YES**	—
Firepower 4110、4120、4140、4150 Firepower 4112、4115、4125、4145	**YES**	**YES** 7.0.3 以降のバージョンが必要です。	**YES**	**YES**	FXOS 2.10.1.159 以降のビルドが必要です。
Firepower 9300 : SM-24、SM-36、SM-44 モジュール Firepower 9300 : SM-40、SM-48、SM-56 モジュール	**YES**	**YES** 7.0.3 以降のバージョンが必要です。	**YES**	**YES**	FXOS 2.10.1.159 以降のビルドが必要です。

プラットフォーム	FMC 互換		FDM 互換		注記
	お客様が導入	クラウド提供型	FDM のみ	FDM + CDO	
ASA 5508-X、5516-X	**YES**	**YES** 7.0.3 以降のバージョンが必要です。	**YES**	**YES**	最新の ROMMON イメージが必要です。Cisco Secure Firewall ASA および Cisco Secure Firewall Threat Defense 再イメージ化ガイドを参照してください。
ISA 3000	**YES**	**YES** 7.0.3 以降のバージョンが必要です。	**YES**	**YES**	最新の ROMMON イメージが必要です。Cisco Secure Firewall ASA および Cisco Secure Firewall Threat Defense 再イメージ化ガイドを参照してください。

FTDv

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

表 *3 : Version7.0 FTDv* パブリック クラウド プラットフォーム

デバイスのプラットフォーム	FMC 互換		FDM 互換	
	お客様が導入	クラウド提供型	FDM のみ	CDO および FDM
Amazon Web Services（AWS）	**YES**	**YES** 7.0.3 以降 のバージョンが必要です。	**YES**	**YES**
Microsoft Azure	**YES**	**YES** 7.0.3 以降 のバージョンが必要です。	**YES**	**YES**

デバイスのプラットフォーム	FMC 互換		FDM 互換	
	お客様が導入	クラウド提供型	FDM のみ	CDO および FDM
Google Cloud Platform（GCP）	**YES**	**YES** 7.0.3 以降のバージョンが必要です。	—	—
Oracle Cloud Infrastrucure（OCI）	**YES**	**YES** 7.0.3 以降のバージョンが必要です。	—	—

表 *4 : Version7.0 FTDv* オンプレミス/プライベート クラウド プラットフォーム

デバイスのプラットフォーム	FMC 互換		FDM 互換	
	お客様が導入	クラウド提供型	FDM のみ	CDO および FDM
Cisco Hyperflex	**YES**	**YES** 7.0.3 以降のバージョンが必要です。	**YES**	**YES**
カーネルベース仮想マシン（KVM）	**YES**	**YES** 7.0.3 以降のバージョンが必要です。	**YES**	**YES**
Nutanix エンタープライズクラウド	**YES**	**YES** 7.0.3 以降のバージョンが必要です。	**YES**	**YES**
OpenStack	**YES**	**YES** 7.0.3 以降のバージョンが必要です。	—	—
VMware vSphere/VMware ESXi 6.5、6.7、または 7.0	**YES**	**YES** 7.0.3 以降のバージョンが必要です。	**YES**	**YES**

ASA FirePOWER および NGIPSv

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（*ASA FirePOWER* モジュール）です。NGIPSv は、仮想環境でソフトウェアを実行します。これらのデバイスは、クラウド提供型の FMC では管理できません。

表 *5 : Version7.0ASA FirePOWER* および *NGIPSv* プラットフォーム

デバイスのプラットフォーム	FMC 互換	ASDM の互換性	注記
ASA 5508-X with FirePOWER Services ASA 5516-X with FirePOWER Services ISA 3000 with FirePOWER Services	**YES**	ASDM 7.16(1) が必要です。	ASA 9.5(2) ～ 9.16(x) が必要です。 最新の ROMMON イメージが必要です。Cisco Secure Firewall ASA および Cisco Secure Firewall Threat Defense 再イメージ化ガイドを参照してください。
NGIPSv	**YES**	—	VMware 6.5、6.7、または 7.0 が必要です。 サポート対象のインスタンスやスループットをはじめとしたホスティング要件については、 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

このセクションでは、Version7.0 でサポートされている、お客様が導入したハードウェアと仮想 FMC を示します。クラウド提供型の管理センターの互換性情報については、『FMC でのデバイス管理（12 ページ）』を参照してください。一般的な互換性情報については、Cisco Secure Firewall Management Center 互換性ガイド を参照してください。

FMC ハードウェア

Version7.0 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

Version7.0 は、次の FMCv プラットフォームをサポートしています。

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 スタートアップガイド を参照してください。

表 *6 : Version7.0 FMCv* パブリック クラウド プラットフォーム

プラットフォーム	FMCv2、10、25	FMCv300
Amazon Web Services（AWS）	**YES**	—
Google Cloud Platform（GCP）	**YES**	—
Microsoft Azure	**YES**	—
Oracle Cloud Infrastrucure（OCI）	**YES**	—

表 *7 : Version7.0 FMCv* オンプレミス/プライベート クラウド プラットフォーム

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

FMC でのデバイス管理

すべての デバイスは、FMC によるリモート管理に対応しています。

お客様が導入した FMC

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

- より新しい FMC でより古いデバイスを管理できます。通常は、メジャーバージョンをいくつか遡ることができます。ただし、導入環境全体を常に更新することをお勧めします。

多くの場合、新機能の使用や問題解決の適用には、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。

- 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。

表 *8 : 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
7.2	6.6
7.1	6.5
7.0	6.4
6.7	6.3
6.6	6.2.3
6.5	6.2.3
6.4	6.1
6.3	6.1
6.2.3	6.1
6.2.2	6.1
6.2.1	6.1
6.2	6.1
6.1	5.4.0.2/5.4.1.1
6.0.1	5.4.0.2/5.4.1.1
6.0	5.4.0.2/5.4.1.1
5.4.1	5.4.1（ASA-5506-X シリーズ、ASA5508-X、および ASA5516-X の ASA FirePOWER）。 5.3.1（ASA5512-X、ASA5515-X、ASA5525-X、ASA5545-X、ASA5555-X、および ASA-5585-X シリーズの ASA FirePOWER）。 5.3.0（Firepower 7000/8000 シリーズおよびレガシーデバイス）。

クラウド提供型の管理センター

クラウド提供型の管理センターは、複数のシスコ セキュリティ ソリューションの管理を統合する Cisco Defense Orchestrator（CDO）プラットフォームを通して提供されます。機能の更新

はシスコが行います。クラウド提供型の管理センターは、以下を実行する Threat Defense デバイスを管理できます。

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

クラウド提供型の管理センターは、バージョン 7.1 を実行している脅威防御デバイス、または任意のバージョンを実行している従来のデバイスを管理できません。クラウド管理を登録解除して無効にしない限り、クラウド提供型の管理センターに登録されている脅威防御デバイスをバージョン 7.0.x からバージョン 7.1 にアップグレードすることはできません。バージョン 7.2 以降に直接アップグレードすることをお勧めします。

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

ブラウザ要件

ブラウザ

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

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

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

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

ブラウザの設定と拡張

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

一部のブラウザ拡張機能では、PKI オブジェクトの証明書やキーなどのフィールドに値を保存できないことに注意してください。これらの拡張機能には Grammarly や Whatfix Editor 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	最小解像度
FMC	1280 X 720
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。

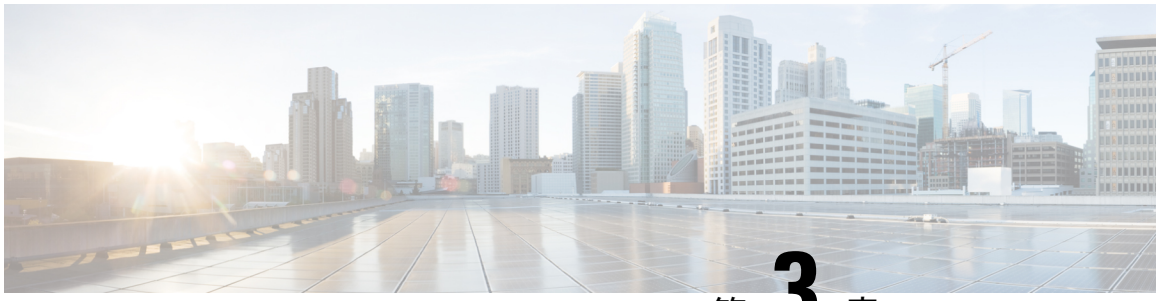
詳しい手順については、オンラインヘルプまたはご使用の製品のコンフィギュレーション ガイドを参照してください。

（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、Version7.0 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 7.0 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 *9 : FMC* バージョン *7.0.3* の新機能

機能	説明
クラウド提供型の管理センターの FTD サポート	

機能	説明
	バージョン 7.0.3 FTD デバイスは、2022 年春に導入されたクラウド提供型の管理センターによる管理をサポートします。このクラウド提供型の管理センターは、Cisco Defense Orchestrator（CDO）プラットフォームを使用して、複数の Cisco セキュリティソリューションの管理を統合します。機能の更新はシスコが行います。 次の場合は、クラウド提供型の管理センターでバージョン 7.0.3 FTD を使用する必要があります。 • 現在、お客様が導入したハードウェアまたは仮想 FMC を使用しています。 • 今すぐクラウド提供型の管理センターに移行したいと考えている。 • デバイスをバージョン 7.2 以降にアップグレードする必要はありません。バージョン 7.2 以降は、クラウド提供型の管理センターによる管理もサポートしています。 この状況に当てはまる場合は、次のことを実行してください。 **1.** 現在の FMC をバージョン 7.2 以降にアップグレードします。 技術的にはバージョン 7.0.3 または 7.1 FMC を使用して FTD をバージョン 7.0.3 にアップグレードできますが、デバイスをクラウド提供型の管理センターに簡単に移行することも、イベントのログ記録と分析の目的でのみ（「分析専用」）、お客様が導入した管理センターにデバイスを登録したままにすることもできません。 **2.** アップグレードされた FMC を使用して、デバイスをバージョン 7.0.3 にアップグレードします。 **3.** デバイスでクラウド管理を有効にします。 バージョン 7.0.x デバイスの場合のみ、デバイスの CLI から **configure manager-cdo enable** を実行してクラウド管理を有効にする必要があります。**show manager-cdo** コマンドは、クラウド管理が有効になっているかどうかを表示します。 **4.** CDO の [FTDをクラウドに移行する（Migrate FTD to cloud）] ウィザードを使用して、クラウド提供型の管理センターにデバイスを移行します。 必要に応じて、お客様が導入した管理センターにデバイスを分析専用デバイスとして登録したままにします。あるいは、シスコのセキュリティ分析とロギング（SaaS） を使用して、Cisco Cloud にセキュリティイベントを送信できます。

機能	説明
	クラウド提供型の管理センターは、バージョン 7.1 を実行している脅威防御デバイス、または任意のバージョンを実行している従来のデバイスを管理できません。クラウド管理を登録解除して無効にしない限り、クラウド提供型の管理センターに登録されている脅威防御デバイスをバージョン 7.0.x からバージョン 7.1 にアップグレードすることはできません。バージョン7.2以降に直接アップグレードすることをお勧めします。 新規/変更された CLI コマンド：**configure manager add**、**configure manager delete**、**configure manager edit**、**show managers** 詳細については、Cisco Defense Orchestrator のクラウド提供型 Firewall Management Center による Firewall Threat Defense の管理を参照してください。

表 *10 : FMC* バージョン *7.0.2* の新機能

機能	説明
ダイナミックオブジェクト名でダッシュ文字を使用できるようになりました。	ダイナミックオブジェクト名でダッシュ文字を使用できるようになりました。これは、ACI エンドポイント更新アプリ（ダッシュ文字が許可されている）を使用して、テナントのエンドポイントグループを表すダイナミックオブジェクトをFMC で作成する場合に特に便利です。 （注） この機能を使用するには、FMC とデバイスの両方にバージョン 7.0.2 が必要です。

機能	説明
SecureX との統合、SecureX とのオーケストレーションの改善	SecureX との統合プロセスが合理化されました。すでに SecureX アカウントを持っている場合は、新しい [統合（Integration）] > [SecureX] ページで該当するクラウドリージョンを選択し、[SecureX の有効化（Enable SecureX）] をクリックして、SecureX に対して認証するだけです。イベントをクラウドに送信するオプション、および Cisco Success Network と Cisco Support Diagnostics を有効にするオプションも、この新しいページに移動されました。 この新しいページで SecureX との統合を有効にすると、システムのクラウド接続のライセンス管理が Cisco Smart Licensing から SecureX に切り替わります。SecureX を「従来の」方法ですでに有効にしている場合、このクラウド接続管理による利点を得るには、無効にしてから再度有効にする必要があります。 Web インターフェースで示されていない場合でも、このページでは対象のクラウドリージョンや、シスコのセキュリティ分析とロギング（SaaS）を使用して Secure Network Analytics（Stealthwatch）クラウドに送信するイベントタイプも管理することを覚えておいてください。以前のバージョンでは、このオプションは、**システム**（⚙）> [統合（Integration）] > [クラウドサービス（Cloud Services）] にありました。SecureX を有効にしても、Secure Network Analytics クラウドとの通信には影響しません。両方にイベントを送信できます。 FMC は SecureX オーケストレーションもサポートするようになりました。これは、セキュリティツール全体のワークフローを自動化するために使用できる強力なドラッグアンドドロップ インターフェイスです。SecureX を有効にすると、オーケストレーションを有効にできます。 （注） これらの変更はバージョン 7.1 で一時的に廃止されましたが、バージョン 7.2 で復活しました。新しい方法で SecureX との統合を有効にした場合は、バージョン 7.1.x にアップグレードする前に、この機能を無効にする必要があります。アップグレードが正常に完了したら、この機能を再度有効にできます。バージョン 7.2 以降へのアップグレードは影響を受けません。

機能	説明
Web インターフェイスの変更：SecureX、脅威インテリジェンス、およびその他の統合。	

機能	説明
	以下の FMC メニューオプションが変更されました。 （注） これらの変更はバージョン 7.1 で一時的に廃止されましたが、バージョン 7.2 で復活しました。 [AMP] > [AMP管理（AMP Management）] は次に変更されました。 [統合（Integration）] > [AMP] > [AMP管理（AMP Management）] [AMP] > [ダイナミック分析接続（Dynamic Analysis Connections）] は次に変更されました。 [統合（Integration）] > [AMP] > [ダイナミック分析接続（Dynamic Analysis Connections）] [インテリジェンス（Intelligence）] > [ソース（Sources）] は次に変更されました。 [統合（Integration）] > [インテリジェンス（Intelligence）] > [ソース（Sources）] [インテリジェンス（Intelligence）] > [要素（Elements）] は次に変更されました。 [統合（Integration）] > [インテリジェンス（Intelligence）] > [要素（Elements）] [インテリジェンス（Intelligence）] > [設定（Settings）] は次に変更されました。 [統合（Integration）] > [インテリジェンス（Intelligence）] > [設定（Settings）] [インテリジェンス（Intelligence）] > [インシデント（Incidents）] は次に変更されました。 [統合（Integration）] > [インテリジェンス（Intelligence）] > [インシデント（Incidents）]

機能	説明		
	システム（⚙） > [統合（Integration）]	は次に変更されました。	[統合（Integration）] > [その他の統合（Other Integrations）]
	システム（⚙） > [ロギング（Logging）] > [セキュリティ分析とロギング（Security Analytics and Logging）]	は次に変更されました。	[統合（Integration）] > [セキュリティ分析とロギング（Security Analytics and Logging）]
	システム（⚙） > [SecureX]	は次に変更されました。	[統合（Integration）] > [SecureX]

表 *11* : *FMC* バージョン *7.0.1* の新機能

機能	説明
Snort 3 の rate_filter インスペクタ。	Snort 3 rate_filter インスペクタが導入されました。 これにより、ルールに対する過剰な一致に対応して侵入ルールのアクションを変更できます。レートベースの攻撃を特定の期間ブロックし、イベントの生成中でも一致するトラフィックを許可するように戻すことができます。詳細については、『Snort 3 Inspector Reference』を参照してください。 （注） この機能を使用するには、FMC とデバイスの両方にバージョン 7.0.1 以降が必要です。また、lsp-rel-20210816-1910 以降を実行している必要があります。**[システム（System）] > [アップデート（Updates）] > [ルールアップデート（Rule Updates）]** で LSP を確認および更新できます。 新規/変更されたページ：カスタムネットワーク分析ポリシーの Snort 3 バージョンを編集して、インスペクタを設定します。 サポートされるプラットフォーム：FTD

機能	説明
ASA FirePOWER サービスを使用する ISA 3000 の新しいデフォルトパスワード	新しいデバイスの場合、admin アカウントのデフォルトパスワードは Adm!n123 になりました。以前は、デフォルトの admin パスワードは Admin123 でした。 バージョン 7.0.1 以降にアップグレードまたは再イメージ化しても、パスワードは変更されません。ただし、すべてのユーザアカウント（特に管理者アクセス権を持つユーザアカウント）に強力なパスワードを設定することを推奨します。 サポートされるプラットフォーム：ASA FirePOWER サービスを使用する ISA 3000

表 *12 : FMC* バージョン *7.0.0* の新機能

機能	説明
プラットフォーム	

機能	説明
FTDvパフォーマンス階層型のスマートライセンス。	**アップグレードの影響。** FTDv は、スループット要件と RA VPN セッションの制限に基づいて、パフォーマンス階層型のスマート ソフトウェア ライセンスをサポートするようになりました。オプションは、FTDv5（100 Mbps/50 セッション）から FTDv100（16 Gbps/10,000 セッション）までです。 新しいデバイスを追加する前に、お使いのアカウントに必要なライセンスが含まれていることを確認してください。追加のライセンスを購入するには、シスコの担当者またはパートナーの担当者にお問い合わせください。 FTDv をバージョン 7.0 にアップグレードすると、デバイスが自動的に FTDv50 階層に割り当てられます。レガシー（非階層型）ライセンスを引き続き使用するには、アップグレード後に階層を [変数（Variable）] に変更します。 サポートされているインスタンス、スループット、およびその他のホスティング要件の詳細については、該当するスタートアップガイドを参照してください。 新規/変更されたページ： • [デバイス（Device）] > [デバイス管理（Device Management）] ページで FTDv デバイスを追加または編集するときに、パフォーマンス階層を指定できるようになりました。 • [システム（System）] > [ライセンス（Licenses）] > [スマートライセンス（Smart Licenses）] ページでパフォーマンス階層を一括編集できます。
高可用性/拡張性	

機能	説明
クラスタリング用の PAT ポートブロック割り当ての改善	PAT ポートブロック割り当ての改善により、制御ユニットはノードに参加するためにポートを確保し、未使用のポートを積極的に再利用できるようになります。割り当てを最適化するには、FlexConfig を使用して **cluster-member-limit** コマンドを実行して、予定しているクラスタ内の最大ノード数を設定します。これにより、制御ユニットは計画されたノード数にポートブロックを割り当てることができ、使用する予定のない追加のノード用にポートを予約する必要がなくなります。デフォルトは16ノードです。また、syslog 747046 を監視して、新しいノードに使用できるポートが十分にあることを確認することもできます。 新規/変更されたコマンド：**cluster-member-limit**（FlexConfig）、**show nat pool cluster [summary]**、**show nat pool ip detail** サポートされるプラットフォーム：Firepower 4100/9300
FTD CLI **show cluster history** の改善。	新しいキーワードを指定すると、**show cluster history** コマンドの出力をカスタマイズできます。 新規/変更されたコマンド：**show cluster history** [**brief**] [**latest**] [**reverse**] [**time**] サポートされるプラットフォーム：Firepower 4100/9300
クラスタから永久に削除するための FTD CLI コマンド。	FTD CLI を使用して、ユニットをクラスタから完全に削除し、その設定をスタンドアロンデバイスに変換できるようになりました。 新規/変更されたコマンド： **cluster reset-interface-mode** サポートされるプラットフォーム：Firepower 4100/9300
NAT	
優先順位付けされたシステム定義の NAT ルール。	新しいセクション 0 が NAT ルールテーブルに追加されました。このセクションは、システムの使用に限定されます。システムが正常に機能するために必要なすべての NAT ルールがこのセクションに追加され、これらのルールは作成したルールよりも優先されます。以前は、システム定義のルールがセクション 1 に追加され、ユーザー定義のルールがシステムの適切な機能を妨げる可能性がありました。 セクション 0 のルールを追加、編集、または削除することはできませんが、**show nat detail** コマンド出力に表示されます。 サポートされるプラットフォーム：FTD
仮想ルーティング	

機能	説明
ISA 3000 の仮想ルータサポート。	ISA 3000 デバイスには最大 10 台の仮想ルータを設定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：ISA 3000
サイト間 VPN	
ルートベースのサイト間 VPN 向けバックアップ用仮想トンネルインターフェイス（VTI）。	仮想トンネルインターフェイスを使用するサイト間 VPN を設定する場合、トンネルのバックアップ VTI を選択できます。 バックアップ VTI を指定すると復元力が得られるため、プライマリ接続がダウンした場合でもバックアップ接続は継続して機能します。たとえば、プライマリ VTI をあるサービスプロバイダーのエンドポイントに接続し、バックアップ VTI を別のサービスプロバイダーのエンドポイントに接続できます。 新規/変更されたページ：ポイントツーポイント接続の VPN タイプとして [ルートベース（Route-Based）] を選択した場合に、サイト間 VPN ウィザードにバックアップ VTI を追加する機能が追加されました。 サポートされるプラットフォーム：FTD
Remote Access VPN	
ロード バランシング。	RA VPN ロードバランシングがサポートされるようになりました。システムは、セッション数によってグループ化されたデバイス間でセッションを分散します。トラフィック量やその他の要因は考慮されません。 新規/変更された画面：RA VPN ポリシーの [詳細設定（Advanced Settings）] にロード バランシング 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
ローカル認証。	RA VPN ユーザーのローカル認証がサポートされるようになりました。これは、プライマリまたはセカンダリ認証方式として、または設定されたリモートサーバーに到達できない場合のフォールバックとして使用できます。 **1.** ローカルレルムを作成します。 ローカルユーザー名とパスワードは、ローカルレルムに保存されます。レルムを作成し（**[システム（System）] > [統合（Integration）] > [レルム（Realms）]**）、新しい **[ローカル（LOCAL）]** レルムタイプを選択すると、1つ以上のローカルユーザーを追加するように求められます。 **2.** ローカル認証を使用するように RA VPN を設定します。 RA VPN ポリシーを作成または編集し（**[デバイス（Devices）] > [VPN] > [リモートアクセス（Remote Access）]**）、そのポリシー内に接続プロファイルを作成して、その接続プロファイルでプライマリ、セカンダリ、またはフォールバック認証サーバーとして **[ローカル（LOCAL）]** を指定します。 **3.** 作成したローカルレルムを RA VPN ポリシーに関連付けます。 RA VPN ポリシーエディタで、新しい **[ローカルレルム（Local Realm）]** 設定を使用します。ローカル認証を使用する RA VPN ポリシーのすべての接続プロファイルは、ここで指定したローカルレルムを使用します。 サポートされるプラットフォーム：FTD

機能	説明
ダイナミック アクセス ポリシー。	新しいダイナミック アクセス ポリシーを使用すると、変化する環境に自動的に適応するリモートアクセス VPN 認証を設定できます。 **1.** AnyConnect HostScan パッケージを AnyConnect ファイルとしてアップロードして、HostScan を設定します（**[オブジェクト（Objects）]>[オブジェクト管理（Object Management）]>[VPN]>[AnyConnect ファイル（AnyConnect File）]**）。**[ファイルタイプ（File Type）]** ドロップダウンリストに新しい **[HostScan パッケージ（HostScan Package）]** オプションがあります。 このモジュールはエンドポイントで実行され、ダイナミック アクセス ポリシーが使用するポスチャアセスメントを実行します。 **2.** ダイナミック アクセス ポリシーを作成します（**[デバイス（Devices）] [ダイナミック アクセス ポリシー（Dynamic Access Policy）]**）。 ダイナミック アクセス ポリシーは、ユーザーがセッションを開始するたびに評価するセッション属性（グループメンバーシップやエンドポイントセキュリティなど）を指定します。その後、その評価に基づいてアクセスを拒否または許可できます。 **3.** 作成したダイナミック アクセス ポリシーを RA VPN ポリシーに関連付けます。 リモートアクセス VPN ポリシーエディタで、新しい **[ダイナミック アクセス ポリシー（Dynamic Access Policy）]**設定を使用します。 サポートされるプラットフォーム：FTD
マルチ証明書認証。	リモートアクセス VPN ユーザのマルチ証明書認証をサポートするようになりました。SSL または IKEv2 EAP フェーズで AnyConnect クライアントを使用して VPN アクセスを許可するためにユーザの ID 証明書を認証することに加えて、マシンまたはデバイス証明書を検証して、デバイスが会社支給のデバイスであることを確認できます。 サポートされるプラットフォーム：FTD

機能	説明
AnyConnect カスタム属性。	AnyConnect カスタム属性をサポートし、AnyConnect クライアント機能を設定するためのインフラストラクチャを、これらの機能の明示的なサポートをシステムに追加することなく、提供するようになりました。 サポートされるプラットフォーム：FTD
アクセス制御	

機能	説明
FTD 用 Snort 3。	

機能	説明
	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。 Snort 3 を使用する利点は次のとおりですが、これに限定されません。 • パフォーマンスの向上。 • SMBv2 インスペクションの改善。 • 新しいスクリプト検出機能。 • HTTP/2 インスペクション。 • カスタムルールグループ。 • カスタム侵入ルールを記述しやすくする構文。 • 侵入イベント内の「would have dropped」インライン結果の理由。 • VDB、SSL ポリシー、カスタム アプリケーション ディテクタ、キャプティブポータル ID ソース、および TLS サーバ ID 検出へ変更を展開するときに Snort が再起動しない。 • Cisco Success Network に送信される Snort 3 固有のテレメトリデータ、およびトラブルシューティングログの改善による、有用性の向上。 Snort 3 侵入ルールの更新は、SRU ではなく LSP（Lightweight Security Package）と呼ばれます。Snort 2 には引き続き SRU が使用されます。シスコからのダウンロードには、最新の LSP と SRU の両方が含まれており、設定に適したルールセットが自動的に使用されます。 FMC は、Snort 2 と Snort 3 の両方のデバイスでの展開を管理でき、各デバイスに正しいポリシーを適用します。ただし、Snort 2 とは異なり、FMC のみをアップグレードしてから展開することで、デバイス上の Snort 3 を更新することはできません。Snort 3 では、新しい機能と解決済みのバグにより、FMC 上のソフトウェアとその管理対象デバイスをアップグレードする必要があります。各ソフトウェアバージョンに含まれている Snort の詳細については、Cisco Firepower Compatibility Guide のバンドルされたコンポーネントのセクションを参照してください。 **重要** Snort 3 に切り替える前に、Firepower Management Center Snort 3 Configuration Guide を読んで理解することを強く推奨します。機能の制限と移行手順には特に注意してく

機能	説明
	ださい。Snort 3 へのアップグレードは影響を最小限に抑えるように設計されていますが、機能は正確にマッピングされません。慎重に計画して準備することで、トラフィックが期待どおりに処理されるようにできます。 Snort 3 の Webサイト（https://snort.org/snort3）にもアクセスできます。https://snort.org/snort3 サポートされるプラットフォーム：FTD

機能	説明
ダイナミックオブジェクト。	ダイナミックオブジェクトは、アクセスコントロールルールで使用できます。 ダイナミックオブジェクトは、単に IP アドレスまたはサブネットのリストです（範囲なし、FQDN なし）。ただし、ネットワークオブジェクトとは異なり、ダイナミックオブジェクトへの変更はすぐに有効になり、再展開する必要はありません。これは、IP アドレスがワークロードリソースに動的にマッピングされる仮想環境やクラウド環境で役立ちます。 ダイナミックオブジェクトを作成および管理するには、Cisco Secure 動的属性コネクタを使用することをお勧めします。コネクタは、ワークロードの変更に基づいてファイアウォールポリシーを迅速かつシームレスに更新する別個の軽量アプリケーションです。そのためには、環境内のタグ付きリソースからワークロード属性を取得し、指定した基準に基づいて IP リストをコンパイルします（「動的属性フィルタ」）。次に、FMC でダイナミックオブジェクトを作成し、IP リストを入力します。ワークロードが変更されると、コネクタによってダイナミックオブジェクトが更新され、新しいマッピングに基づいてすぐにトラフィックの処理が開始されます。詳細については、Cisco Secure 動的属性コネクタ コンフィギュレーション ガイドを参照してください。 作成したダイナミックオブジェクトは、アクセス コントロール ルール エディタの新しい [動的属性（Dynamic Attributes）] タブでアクセスコントロールルールに追加できます。このタブは、フォーカスの狭い [SGT/ISE 属性（SGT/ISE Attributes）] タブに代わるものです。ここで、SGT 属性を使用したルールの設定を続行します。 （注） FMC でダイナミックオブジェクトを作成することもできます（**[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [外部属性（External Attributes）] > [ダイナミックオブジェクト（Dynamic Objects）]**）。ただし、この場合はコンテナのみ作成されます。その後、REST API を使用してデータを入力して管理する必要があります。Firepower Management Center REST API バージョン 7.0 クイックスタートガイド [英語] を参照してください。 サポート対象プラットフォーム：FMC Cisco Secure Dynamic Attributes Connector の統合でサポートされる仮想/クラウドワークロード：Microsoft Azure、AWS、VMware

機能	説明
Active Directory ドメインのクロスドメイン信頼。	Microsoft Active Directory フォレスト（相互に信頼する AD ドメインのグループ）のユーザーを使用してユーザー アイデンティティ ルールを設定できるようになりました。 新規/変更されたページ： • レルムとディレクトリを同時に設定するようになりました。 • 新しい [同期結果（Sync Results）] ページ（[システム（System）] > [統合（Integration）] > [レルム（Realms）] > [同期結果（Sync Results）]）に、クロスドメイン信頼関係のユーザーおよびグループのダウンロードに関連するエラーが表示されます。 サポート対象プラットフォーム：FMC
DNS フィルタリング。	バージョン 6.7 でベータ機能として導入された DNS フィルタリングは、完全にサポートされるようになり、新しいアクセス コントロール ポリシーではデフォルトで有効になっています。 サポートされるプラットフォーム：すべて
イベントロギングおよび分析	

機能	説明
Secure Network Analytics オンプレミス展開でのイベント保存プロセスの改善。	新しいシスコのセキュリティ分析とロギング（オンプレミス）アプリと新しいFMCウィザードにより、オンプレミスSecure Network Analyticsソリューションのリモートデータストレージをより簡単に設定できます。 **1.** ハードウェアまたは仮想Stealthwatchアプライアンスを展開します。 Stealthwatch Management Consoleを単独で使用することも、Stealthwatch Management Console、フローコレクタ、およびデータストアを設定することもできます。 **2.** Stealthwatch Management Consoleに新しいCisco Security Analytics and Logging（オンプレミス）アプリをインストールして、Stealthwatchをリモートデータストアとして設定することができます。 **3.** FMCで、**[システム（System）]>[ロギング（Logging）]>[セキュリティ分析とロギング（Security Analytics & Logging）]**ページの新しいウィザードのいずれかを使用して、Stealthwatch展開に接続します。 Stealthwatchのコンテキストクロス起動を設定するために使用したフォーカスの狭いページは、ウィザードによって置き換えられます。現在、これはウィザードのステップの1つです。 syslogを使用してFirepowerイベントをStealthwatchに送信するアップグレードされた展開では、ウィザードを使用する前にこれらの設定を無効にします。そうしないと、二重にイベントが発生します。Stealthwatchへのsyslog接続を削除するには、FTDプラットフォーム設定を使用します（[デバイス（Devices）]>[プラットフォーム設定（Platform Settings）]）。syslogへのイベント送信を無効にするには、アクセス制御ルールを編集します。 Stealthwatchのハードウェア要件およびソフトウェア要件を含む詳細については、オンプレミスにおけるシスコのセキュリティ分析とロギング：Firepowerイベント統合ガイドを参照してください。 サポート対象プラットフォーム：FMC

機能	説明
Secure Network Analytics オンプレミス展開でリモートに保存されたイベントを操作する。	FMC を使用して、Secure Network Analytics オンプレミス展開でリモートに保存された接続イベントを操作できるようになりました。 接続イベントページ（[分析（Analysis）] > [接続（Connections）] > [イベント（Events）]）と統合イベントビューア（[分析（Analysis）] > [統合イベント（Unified Events）]）の新しいデータソースオプションを使用して、処理する接続イベントを選択できます。デフォルトでは、時間範囲に何も存在しない場合、ローカルに保存された接続イベントが表示されます。その場合、システムはリモートに保存されたイベントを表示します。 また、リモートで保存された接続イベントに基づいてレポートを生成できるように、レポートテンプレートにデータソースオプションが追加されました（[概要（Overview）]>[レポート（Reporting）] > [レポートテンプレート（Report Templates）]）。 （注） この機能は、接続イベントでのみサポートされます。クロス起動は、リモートで保存されたセキュリティインテリジェンス、侵入、ファイル、およびマルウェアのイベントを調べる唯一の方法です。統合イベントビューアでも、システムはこれらのタイプのローカルに保存されたイベントのみを表示します。 ただし、すべてのセキュリティ インテリジェンス イベントに同一の接続イベントが存在することに注意してください。これらは「IP ブロック」や「DNS ブロック」などの理由を持つイベントです。これらの重複イベントは、接続イベントページまたは統合イベントビューアで処理できますが、専用のセキュリティインテリジェンス イベント ページでは処理できません。 サポートされるプラットフォーム：FMC。

機能	説明
すべての接続イベントを Secure Network Analytics クラウドに保存する。	Cisco Security Analytics and Logging（SaaS）を使用して、すべての接続イベントを Stealthwatch クラウドに保存できるようになりました。以前は、セキュリティ インテリジェンス、侵入、ファイル、およびマルウェアのイベント、およびそれらに関連する接続イベントに限定されていました。 クラウドに送信するイベントを変更するには、[システム（System）] > [統合（Integration）] を選択します。[クラウドサービス（Cloud Services）] タブで、[シスコクラウドイベントの設定（Cisco Cloud Event Configuration）] を編集します。優先順位の高い接続イベントをクラウドに送信する古いオプションは、[すべて（All）]、[なし（None）]、または [セキュリティイベント（Security Events）] の選択肢に置き換えられました。 （注） これらの設定は、SecureX に送信するイベントも制御します。ただし、すべての接続イベントをクラウドに送信するように選択した場合でも、SecureX はセキュリティ（優先度の高い）接続イベントのみを消費します。また、[分析（Analysis）] > [SecureX] で SecureX 接続自体を設定することにも注意してください。 サポート対象プラットフォーム：FMC
統合イベントビューア。	統合イベントビューア（**[分析（Analysis）] > [統合イベント（Unified Events）]**）では、1 つのテーブルで接続、セキュリティ インテリジェンス、侵入、ファイル、およびマルウェアの各イベントが表示されます。これは、異なるタイプのイベント間の関係を調べるのに役立ちます。 単一の検索フィールドを使用すると、複数の条件に基づいてビューを動的にフィルタリングできます。また、[本番稼働（Go Live）] オプションでは、管理対象デバイスから受信したイベントがリアルタイムで表示されます。 サポート対象プラットフォーム：FMC

機能	説明
SecureX のリボン。	FMC 上の SecureX のリボンは SecureX にピボットされ、シスコのセキュリティ製品全体の脅威の状況を即座に確認できます。 SecureX に接続してリボンを有効にするには、[分析（Analysis）] > [SecureX] を使用します。クラウドリージョンを選択し、SecureX に送信するイベントを指定するには、引き続き [システム（System）] > [統合（Integration）] > [クラウドサービス（Cloud Services）] を使用する必要があります。 詳細については、Cisco Secure Firewall Threat Defense および SecureX 統合ガイドを参照してください。 サポート対象プラットフォーム：FMC
ローカルストレージをオフにすると、すべての接続イベントのレート制限が免除されます。	イベントレート制限は、FMC に送信されるすべてのイベントに適用されます。ただし、セキュリティイベント（セキュリティ インテリジェンス、侵入、ファイル、マルウェアのイベント、およびそれらに関連する接続イベント）は例外です。 ローカル接続イベントストレージを無効にすると、セキュリティイベントだけでなく、すべての接続イベントがレート制限から除外されるようになりました。これを行うには、[システム（System）] > [設定（Configuration）] > [データベース（Database）] ページで [最大接続イベント数（Maximum Connection Events）] を 0 に設定します。 （注） [最大接続イベント数（Maximum Connection Events）] は、0 に設定してオフにすること以外では、接続イベントのレート制限を制御しません。このフィールドに 0 以外の数値を指定すると、優先順位の低い接続イベントがすべてレート制限されます。 ローカルイベントストレージを無効にしても、リモートイベントストレージには影響せず、接続の概要や相関にも影響しないことに注意してください。システムは、引き続き、トラフィックプロファイル、相関ポリシー、ダッシュボード表示などの機能に接続イベント情報を使用します。 サポート対象プラットフォーム：FMC

機能	説明
ファイルおよびマルウェアイベントテーブルに一緒に表示されるポートとプロトコル。	ファイルおよびマルウェアイベントテーブルでは、[ポート（Port）] フィールドにプロトコルが表示されるようになり、[ポート（Port）] フィールドでプロトコルを検索できます。アップグレード前に存在したイベントの場合、プロトコルが不明な場合は「TCP」が使用されます。 新規/変更されたページ： • **[分析（Analysis）] > [ファイル（Files）] > [マルウェアイベント（Malware Events）]** • **[分析（Analysis）] > [ファイル（Files）] > [ファイルイベント（File Events）]** サポートされるプラットフォーム：FMC
のアップグレード	
FTD のアップグレードパフォーマンスとステータスレポートの改善。	FTD のアップグレードがより簡単かつ確実に、より少ないディスク容量で実行できるようになりました。メッセージセンターの新しい **[アップグレード（Upgrades）]** タブでは、アップグレードステータスとエラーレポートがさらに強化されています。 サポートされるプラットフォーム：FTD

機能	説明
FTD の [アップグレード（Upgrade）] ウィザード。	

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

機能	説明
	時間がかかるアップグレードの失敗を回避するには、[次へ（Next）] をクリックする前に、すべてのグループメンバーがウィザードの次のステップに進む準備ができていることを手動で確認します。 サポートされるプラットフォーム：FTD
多くの FTD デバイスを一度にアップグレードします。	FTD アップグレードウィザードでは、次の制限が解除されます。 • デバイスの同時アップグレード。 一度にアップグレードできるデバイスの数は、同時アップグレードを管理するシステムの機能ではなく、管理ネットワークの帯域幅によって制限されます。以前は、一度に 5 台を上回るデバイスをアップグレードしないことを推奨していました。 **重要** この改善は、FTD バージョン 6.7 以降へのアップグレードでのみ確認できます。デバイスを古い FTD リリースにアップグレードする場合は、新しいアップグレードウィザードを使用している場合でも、一度に 5 台のデバイスに制限することをお勧めします。 • デバイスモデルによるアップグレードのグループ化。 システムが適切なアップグレードパッケージにアクセスできる限り、すべての FTD モデルのアップグレードを同時にキューに入れて呼び出すことができます。 以前は、アップグレードパッケージを選択し、そのパッケージを使用してアップグレードするデバイスを選択していました。つまり、アップグレードパッケージを共有している場合にのみ、複数のデバイスを同時にアップグレードできました。たとえば、2 台の Firepower 2100 シリーズ デバイスは同時にアップグレードできますが、Firepower 2100 シリーズと Firepower 1000 シリーズはアップグレードできません。 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	
SD カードを使用した ISA 3000 でのゼロタッチ復元。	ローカルバックアップを実行すると、バックアップファイルが SD カードにコピーされます（カードがある場合）。交換用デバイスの設定を復元するには、新しいデバイスに SD カードを取り付け、デバイスの起動中に [リセット（Reset）] ボタンを 3 ー 15 秒間押します。 サポートされるプラットフォーム：ISA 3000

機能	説明
RA およびサイト間 VPN ポリシーを選択的に展開する。	バージョン 6.6 で導入された選択的ポリシーの展開では、リモートアクセスとサイト間VPNポリシーがサポートされ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）] ページに VPN ポリシー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
新しいヘルス モジュール。	次の正常性モジュールが追加されました。 • AMP 接続ステータス • AMP Threat Grid のステータス • ASP ドロップ • 高度な Snort 統計情報 • シャーシステータス FTD • イベント ストリーム ステータス • FMC アクセス設定の変更 • FMC HA ステータス（古い HA ステータスの交換） • FTD HA ステータス • ファイルシステムの整合性チェック • フロー オフロード • ヒット カウント（Hit Count） • MySQL ステータス • NTP ステータス FTD • Rabbit MQ ステータス • ルーティング統計情報 • SSE 接続ステータス • Sybase ステータス • 未解決グループモニター • VPN 統計情報 • xTLS カウンタ さらに、バージョン 6.6.3 で [アプライアンス設定のリソース使用率（Appliance Configuration Resource Utilization）] モジュールとして導入された [構成メモリ割り当て（Configuration Memory Allocation）] モジュールは、バージョン 6.7 では完全にはサポートされていませんでしたが、完全にサポートされます。 サポートされるプラットフォーム：FMC
セキュリティと強化	

機能	説明
AWS 導入用の新しいデフォルトパスワード。	初期展開時にユーザーデータ（ [高度な詳細（Advanced Details）] > [ユーザーデータ（User Data）]）を使用してデフォルトパスワードを定義していなければ、adminアカウントのデフォルトパスワードは AWS のインスタンス ID です。 以前は、デフォルトの admin パスワードは Admin123 でした。 サポートされているプラットフォーム：FMCv for AWS、FTDv for AWS
証明書の登録用の EST。	証明書の登録用の Enrollment over Secure Transport のサポートが提供されました。 新規/変更されたページ：[オブジェクト（Objects）] > [PKI] > [証明書の登録（Cert Enrollment）] > [CA情報（CA Information）] タブ設定時の新しい登録オプション。 サポート対象プラットフォーム：FMC
EdDSA 証明書タイプのサポート。	新しい証明書キータイプ：EdDSA（キーサイズ 256）が追加されました。 新規/変更されたページ：[オブジェクト（Objects）] > [PKI] > [証明書の登録（Cert Enrollment）] > [キー（Key）] タブの設定時の新しい証明書キーオプション。 サポート対象プラットフォーム：FMC
NTP サーバーの AES-128 CMAC 認証。	AES-128 CMAC キーを使用して、FMC と NTP サーバー間の接続を保護できるようになりました。 新規/変更されたページ：**[システム（System）] > [設定（Configuration）] > [時刻の同期（Time Synchronization）]**。 サポートされるプラットフォーム：FMC
SNMPv3 ユーザーは、SHA-224 または SHA-384 認証アルゴリズムを使用して認証できます。	SNMPv3 ユーザーは、SHA-224 または SHA-384 アルゴリズムを使用して認証できるようになりました。 新規/変更されたページ：[デバイス（Devices）] > [プラットフォーム設定（Platform Settings）] > [SNMP] > [ユーザー（Users）] > [認証アルゴリズムタイプ（Auth Algorithm Type）] サポートされるプラットフォーム：FTD
ユーザビリティとパフォーマンス	

機能	説明
ポリシーとオブジェクトのグローバル検索。	特定のポリシーを名前で検索し、特定のオブジェクトを名前と設定値で検索できるようになりました。この機能は、クラシックテーマでは使用できません。 新規/変更されたページ：[展開（Deploy）] メニューの左側にある [FMC] メニューバーに [検索（Search）] アイコンとフィールドの機能が追加されました。 サポート対象プラットフォーム：FMC
Intel QuickAssist Technology（QAT）を使用した FTDv でのハードウェア暗号化アクセラレーション。	VMware の FTDv および KVM の FTDv でハードウェア暗号化アクセラレーション（CBC 暗号のみ）がサポートされるようになりました。この機能を使用するには、ホスティング プラットフォームに Intel QAT 8970 PCI アダプタ/バージョン 1.7 以降のドライバが必要です。リブートすると、ハードウェア暗号化アクセラレーションが自動的に有効になります。 サポートされるプラットフォーム：VMware の FTDv、KVM の FTDv
多対 1 および 1 対多接続の CPU 使用率とパフォーマンスが向上しました。	ダイナミック NAT / PAT およびスキャン脅威検出とホスト統計情報を含む接続を除き、システムは接続の作成時に、ローカルホストオブジェクトを作成せず、ロックすることもなくなりました。これにより、多数の接続を同じサーバー（ロードバランサや Web サーバーなど）に対して確立する場合や、1 つのエンドポイントが多数のリモートホストに接続する場合に、パフォーマンスと CPU 使用率が向上します。 次のコマンドが変更されました：**clear local-host**（廃止）、 **show local-host** サポートされるプラットフォーム：FTD
FMC REST API：新しいサービスと操作 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。詳細については、Firepower Management Center REST API バージョン 7.0 クイックスタートガイド [英語] を参照してください。	
デバイス	alerts：GET
統合	fmchastatuses：GET securexconfigs：GET および PUT

機能	説明
オブジェクト	anyconnectcustomattributes、anyconnectpackages、anyconnectprofiles：GET anyconnectcustomattributes/overrides：GET applicationfilters：PUT、POST、および DELETE certificatemaps：GET dnsservergroups：GET dnsservergroups/overrides：GET dynamicobjectmappings：POST dynamicobjects：GET、PUT、POST、および DELETE dynamicobjects/mappings：GET および PUT geolocations：PUT、 POST、および DELETE grouppolicies：GET hostscanpackages：GET intrusionrules、intrusionrulegroups：GET、PUT、POST、および DELETE intrusionrulesupload：POST ipv4addresspools、ipv6addresspools：GET ipv4addresspools/overrides、ipv6addresspools/overrides：GET localrealmusers：GET、PUT、POST、DELETE radiusservergroups：GET realms：PUT、POST、および DELETE sidnsfeeds、sidnslists、sinetworkfeeds、sinetworklists：GET sinkholes：GET ssoservers：GET ssoservers/overrides：GET usage：GET

機能	説明
ポリシー	accesspolicies/securityintelligencepolicies：GET dnspolicies：GET dnspolicies/allowdnsrules、dnspolicies/blockdnsrules：GET dynamicaccesspolicies：GET、PUT、POST、および DELETE identitypolicies：GET intrusionpolicies：PUT、POST、および DELETE intrusionpolicies/intrusionrulegroups、intrusionpolicies/intrusionrules：GET および PUT networkanalysispolicies：GET、PUT、POST、および DELETE networkanalysispolicies/inspectorconfigs：GET networkanalysispolicies/inspectoroverrideconfigs：GET および PUT ravpns：GET ravpns/addressassignmentsettings、ravpns/certificatemapsettings、ravpns/connectionprofiles：GET
検索（Search）	globalsearch：GET

FDM バージョン 7.0 の新機能

表 *13 : FDM* バージョン *7.0.0* の新機能

機能	説明
プラットフォーム機能	
ISA 3000 の仮想ルータサポート	ISA 3000 デバイスには最大 10 の仮想ルータを設定できます。
AWS における FTDv の新しいデフォルトパスワード	AWS では、初期展開時にユーザーデータを使用してデフォルトのパスワードを定義（**[Advanced Details]** > **[User Data]**）していなければ、FTDv のデフォルトの管理者パスワードは AWS のインスタンス ID です。
ファイアウォールと IPS の機能	

機能	説明
システム定義の NAT ルールの新しいセクション 0	新しいセクション 0 が NAT ルールテーブルに追加されました。このセクションは、システムの使用に限定されます。システムが正常に機能するために必要なすべての NAT ルールがこのセクションに追加され、これらのルールは作成したルールよりも優先されます。以前は、システム定義のルールがセクション 1 に追加され、ユーザー定義のルールがシステムの適切な機能を妨げる可能性がありました。セクション 0 のルールを追加、編集、または削除することはできませんが、**show nat detail** コマンド出力に表示されます。
Snort 3 のカスタム侵入ルール	オフラインツールを使用して、Snort 3 で使用するカスタム侵入ルールを作成し、侵入ポリシーにアップロードできます。独自のカスタムルールグループにカスタムルールを編成して、必要に応じて簡単に更新できます。FDM で直接ルールを作成することもできますが、ルールの形式はアップロードされたルールと同じです。FDM には、ルール作成のガイダンスはありません。新しい侵入ルールの基礎として、システム定義のルールを含む既存のルールを複製できます。 侵入ポリシーの編集時に、**[Policies]** > **[Intrusion]** ページにカスタムグループとルールのサポートが追加されました。
FDM 管理対象システムの Snort 3 の新機能	FDM 管理対象システムで Snort 3 を検査エンジンとして使用する場合、次の追加機能を設定できるようになりました。 • 時間ベースのアクセス制御ルール（FTD API のみ）。 • 複数の仮想ルータ。 • SSL 復号ポリシーを使用した TLS 1.1 以下の接続の復号化。 • SSL 復号ポリシーを使用したプロトコル FTPS、SMTPS、IMAPS、POP3S の復号化。
URL カテゴリとレピュテーションに基づく DNS 要求のフィルタリング	URL フィルタリングカテゴリとレピュテーションルールを DNS ルックアップ要求に適用できます。ルックアップ要求の完全修飾ドメイン名（FQDN）にブロックしているカテゴリやレピュテーションがある場合、システムは DNS 応答をブロックします。ユーザーは DNS 解決を受信しないため、ユーザーは接続を完了できません。非 Web トラフィックに URL カテゴリおよびレピュテーション フィルタリングを適用するには、このオプションを使用します。この機能を使用するには、URL フィルタリングライセンスが必要です。 アクセス コントロール ポリシーの設定に [Reputation Enforcement on DNS Traffic] オプションが追加されました。

機能	説明
VPN 機能	
リモートアクセス VPN の FDM SSL 暗号設定	FDM でリモートアクセス VPN 接続に使用する TLS バージョンと暗号化の暗号を定義できます。以前は、FTD API を使用して SSL を設定する必要がありました。 次のページが追加されました：**[Objects]** > **[SSL Ciphers]**、**[Device]** > **[System Settings]** > **[SSL Settings]**。
Diffie-Hellman グループ 31 のサポート	IKEv2 プロポーザルおよびポリシーで Diffie-Hellman（DH）グループ 31 を使用できるようになりました。
デバイス上の仮想トンネルインターフェイスの最大数は 1024 です	作成できる仮想トンネルインターフェイス（VTI）の最大数は 1024 です。以前のバージョンでは、送信元インターフェイスあたりの最大数は 100 でした。
サイト間 VPN セキュリティ アソシエーションの IPsec ライフタイム設定	セキュリティ アソシエーションが再ネゴシエートされるまでに維持する期間のデフォルト設定を変更できます。 サイト間 VPN ウィザードに [Lifetime Duration] オプションと [Lifetime Size] オプションが追加されました。
ルーティング機能	
等コストマルチパス（ECMP）ルーティング	複数のインターフェイスを含むように ECMP トラフィックゾーンを設定できます。これにより、ゾーン内の任意のインターフェイスで、既存の接続のトラフィックが FTD デバイスに出入りできるようになります。この機能により、FTD デバイス上での等コストマルチパス（ECMP）のルーティングや、FTD デバイスへのトラフィックの複数のインターフェイスにわたる外部ロードバランシングが可能になります。 ECMP トラフィックゾーンはルーティングにのみ使用されます。これらはセキュリティゾーンとは異なります。 [Routing] ページに [ECMP Traffic Zones] タブが追加されました。FTD API に ECMPZones リソースが追加されました。
インターフェイス機能	
新しいデフォルトの内部 IP アドレス	192.168.1.0/24 のアドレスが DHCP を使用して外部インターフェイスに割り当てられている場合、IP アドレスの競合を避けるために、内部インターフェイスのデフォルト IP アドレスが 192.168.1.1 から **192.168.95.1** に変更されています。

機能	説明
デフォルトの外部 IP アドレスで IPv6 自動設定が有効になりました。管理用の新しいデフォルト IPv6 DNS サーバーについて	外部インターフェイスのデフォルト設定には、IPv4 DHCP クライアントに加えて、IPv6 自動設定が含まれています。デフォルトの管理 DNS サーバーには、IPv6 サーバー：2620:119:35::35 も含まれるようになりました。
ISA 3000 の EtherChannel サポート	FDM を使用して ISA 3000 で EtherChannel を設定できるようになりました。 新規/変更された画面：**[Devices]** > **[Interfaces]** > **[EtherChannels]**
ライセンシング機能	
FTDv のパフォーマンス階層型ライセンス	FTDv は、スループット要件と RA VPN セッションの制限に基づいて、パフォーマンス階層型のスマートライセンスをサポートするようになりました。使用可能なパフォーマンスライセンスのいずれかで FTDv のライセンスを取得すると、2 つのことが発生します。まず、デバイスのスループットを指定されたレベルに制限するレートリミッタがインストールされます。次に、VPN セッションの数は、ライセンスで指定されたレベルに制限されます。
管理およびトラブルシューティングの機能	
FTD API を使用した DHCP リレー設定。	FTD API を使用して DHCP リレーを設定できます。インターフェイスで DHCP リレーを使用すると、他のインターフェイスを介してアクセス可能な DHCP サーバーに DHCP 要求を送信できます。物理インターフェイス、サブインターフェイス、EtherChannel、および VLAN インターフェイスで DHCP リレーを設定できます。いずれかのインターフェイス上に DHCP サーバーを設定している場合、DHCP リレーは設定できません。 以前のリリースで FlexConfig を使用して DHCP リレーを設定した場合は（**dhcprelay** コマンド）、アップグレード後に API を使用して設定を再実行し、FlexConfig オブジェクトを削除する必要があります。 FTD API に次のモデルを追加しました：dhcprelayservices
ブートストラップ処理の高速化と FDM への早期ログイン	FDM 管理対象システムを最初にブートストラップするプロセスが改善され、より高速になりました。したがって、デバイスを起動してから FDM にログインするまで待機する必要はありません。また、ブートストラップの進行中にログインできるようになりました。ブートストラップが完了していない場合は、プロセスのステータス情報が表示されるため、デバイスで何が発生しているかがわかります。

機能	説明
多対 1 および 1 対多接続の CPU 使用率とパフォーマンスが向上しました。	ダイナミック NAT / PAT およびスキャン脅威検出とホスト統計情報を含む接続を除き、システムは接続の作成時に、ローカルホストオブジェクトを作成せず、ロックすることもなくなりました。これにより、多数の接続を同じサーバー（ロードバランサや Web サーバーなど）に対して確立する場合や、1 つのエンドポイントが多数のリモートホストに接続する場合に、パフォーマンスと CPU 使用率が向上します。 次のコマンドが変更されました：**clear local-host**（廃止）、**show local-host**
FDM管理対象デバイスのアップグレード準備状況チェック。	アップロードしたFTD ソフトウェア アップグレードパッケージをインストールする前に、アップグレード準備状況チェックを実行できます。準備状況チェックでは、システムに対してアップグレードが有効であり、システムがパッケージのインストールに必要な他の要件を満たしていることを確認します。アップグレードの準備状況チェックを実行すると、インストールの失敗を回避できます。 **[Device]** > **[Updates]**ページの **[System Upgrade]** セクションに、アップグレードの準備状況チェックを実行するリンクが追加されました。
FTD REST API バージョン 6.1（v6）	ソフトウェアバージョン 7.0 の FTD REST API はバージョン 6.1 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。6.1 の URL バージョンパス要素は、6.0：v6 と同じであることに注意してください。 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 7.0 の新しいハードウェアと仮想プラットフォーム

表 *14 :* バージョン *7.0.0* 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
VMware vSphere/VMware ESXi 7.0 のサポート。	VMware vSphere/VMware ESXi 7.0 に FMCv、FTDv、および NGIPSv 仮想アプライアンスを展開できるようになりました。 バージョン 7.0 でも VMware 6.0 のサポートは終了します。Firepower ソフトウェアをアップグレードする前に、ホスティング環境をサポートされているバージョンにアップグレードします。
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。 • Cisco HyperFlex • Nutanix エンタープライズクラウド • OpenStack (FDM 管理のサポートなし)

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 7.0 で廃止された機能

表 *15 : FMC* バージョン *7.0.2* で廃止された機能

機能	アップグレードの影響	説明
REST API で SecureX との統合を設定。	なし。	SecureX 統合の改善の一環として（FMC バージョン 7.0 の新機能 （17 ページ） を参照）、REST API を使用して SecureX との統合を設定できなくなりました。FMC の Web インターフェイスを使用する必要があります。

表 *16 : FMC* バージョン *7.0.0* で廃止された機能

機能	アップグレードの影響	説明
キーが 2048 ビット未満の RSA 証明書、または署名アルゴリズムで SHA-1 を使用する RSA 証明書。	FTD デバイスを介したアップグレード後の VPN 接続を防止します。	バージョン 7.0 では、キーが 2048 ビット未満の RSA 証明書、または署名アルゴリズムで SHA-1 を使用する RSA 証明書のサポートが削除されています。 アップグレードする前に、オブジェクトマネージャを使用し、より強力なオプションを使用して PKI 証明書の登録を更新します（[オブジェクト（Objects）]>[PKI]>[証明書の登録（Cert Enrollment）]）。更新しない場合、アップグレードしても現在の設定は保持されますが、デバイスを介した VPN 接続は失敗します。 弱いオプションを使用して古い FTD デバイス（バージョン 6.4 ー 6.7.x）のみを管理し続けるには、[デバイス（Devices）] > [証明書（Certificates）] ページで各デバイスの新しい [弱暗号化の有効化（Enable Weak-Crypto）] オプションを選択します。

機能	アップグレードの影響	説明
SNMPv3 ユーザー向けの MD5 認証アルゴリズムと DES 暗号化（削除）。	アップグレード後に展開ができないようにします。	バージョン 7.0 では、FTD デバイスにおける SNMPv3 ユーザー向けの MD5 認証アルゴリズムと DES 暗号化のサポートが削除されています。 FTD をバージョン 7.0 にアップグレードすると、FMC の設定に関係なく、該当ユーザーがデバイスから削除されます。プラットフォーム設定ポリシーでこれらのオプションを使用している場合は、FTD をアップグレードする前に構成を変更して確認してください。 これらのオプションは、Threat Defense プラットフォーム設定ポリシー（[デバイス（Devices）] > [プラットフォーム設定（Platform Settings）]）で SNMPv3 ユーザーを作成または編集する際の [認証アルゴリズムタイプ（Auth Algorithm Type）] および [暗号化タイプ（Encryption Type）] ドロップダウンにあります。
AMP クラウドとのポート 32137 通信。	FMC がアップグレードされないようにします。	バージョン 7.0 では、パブリックおよびプライベート AMP クラウドからファイル配置データを取得するためにポート 32137 を使用する FMC オプションが廃止されています。プロキシを設定しない限り、FMC はポート 443/HTTPS を使用するようになりました。 アップグレードする前に、[システム（System）] > [統合（Integration）] > [クラウドサービス（Cloud Services）] ページで [ネットワーク用 AMP にレガシーポート 32137 を使用（Use Legacy Port 32137 for AMP for Networks）] オプションを無効にします。AMP for Networks の展開が期待どおりに機能するまで、アップグレードを続行しないでください。
HA ステータス正常性モジュール。	なし。	バージョン 7.0 では、[HA ステータス（HA Status）] 正常性モジュールの名前が変更されています。これからは、[FMC HA ステータス（FMC HA Status）] 正常性モジュールです。これは、新しい [FTD HA ステータス（FTD HA Status）] モジュールと区別するためです。
レガシー API エクスプローラ。	なし。	バージョン 7.0 では、FMC REST API レガシー API Explorer のサポートが削除されています。

機能	アップグレードの影響	説明
地理位置情報の詳細。	なし。これは日付ベースで廃止予定です。	2022 年 5 月、GeoDB が 2 つのパッケージに分割されました。IP アドレスを国/大陸にマッピングする国コードパッケージと、ルーティング可能な IP アドレスに関連付けられた追加のコンテキストデータを含む IP パッケージです。IP パッケージのコンテキストデータには、追加のロケーションの詳細に加えて、ISP、接続タイプ、プロキシタイプ、ドメイン名などの接続情報を含めることができます。 新しい国コードパッケージのファイル名は、古いオールインワンパッケージと同じ（Cisco_GEODB_Update-*date-build*）です。これにより、バージョン 7.1 以前を実行している環境では、引き続き GeoDB の更新プログラムを取得できます。GeoDB 更新プログラムを手動でダウンロードする場合（エアギャップ展開など）、IP パッケージではなく、必ず国コードパッケージを取得してください。 **重要** この分割による地理位置情報ルールやトラフィック処理への影響はありません。これらのルールは、国コードパッケージのデータのみに依存しています。ただし、オールインワンパッケージは原則的に国コードパッケージに置き換えられるため、コンテキストデータは更新されなくなり、陳腐化されます。最新のデータを取得するには、FMC をバージョン 7.2 以降にアップグレードするか再イメージ化して、GeoDB を更新します。
Web インターフェイスの変更。	なし	バージョン 7.0 では、次の点が変更されています。 • アクセス コントロール ルール エディタでは、[動的属性（Dynamic Attributes）] タブが、フォーカスの狭い [SGT/ISE 属性（SGT/ISE Attributes）] タブに置き換わります。ここで、SGT 属性を使用したルールの設定を続行します。 • **[システム（System）]** > **[SecureX]** で、SecureX 統合を設定するようになりました以前は、これらの設定は**[システム（System）]** > **[統合（Integration）]** > **[クラウドサービス（Cloud Services）]** で行っていました。 • **[ヘルプ（Help）]** > **[使用方法（How-Tos）]** でウォークスルーが呼び出されるようになりました。以前は、ブラウザウィンドウの下部にある [使用方法（How-Tos）] をクリックしていました。

FDM バージョン 7.0 で廃止された機能

表 *17 : FDM* バージョン *7.0.0* で廃止された機能

機能	アップグレードの影響	説明
dhcprelay 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 7.0 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。 • **dhcprelay**FTD API を使用して DHCP リレーを設定できるようになりました。インターフェイスで DHCP リレーを使用すると、デバイス上の別のインターフェイスで実行されている DHCP サーバー、または他のインターフェイスを介してアクセス可能な DHCP サーバーに DHCP 要求を送信できます。物理インターフェイス、サブインターフェイス、EtherChannel、および VLAN インターフェイスで DHCP リレーを設定できます。 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。

バージョン 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

表 *18 :* バージョン *7.0.0* 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
VMware vSphere/VMware ESXi 6.0 のサポート。	バージョン 7.0 では、VMware vSphere/VMware ESXi 6.0 での仮想展開のサポートが廃止されています。Firepower ソフトウェアをアップグレードする前に、ホスティング環境をサポートされているバージョンにアップグレードします。

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。

⚠

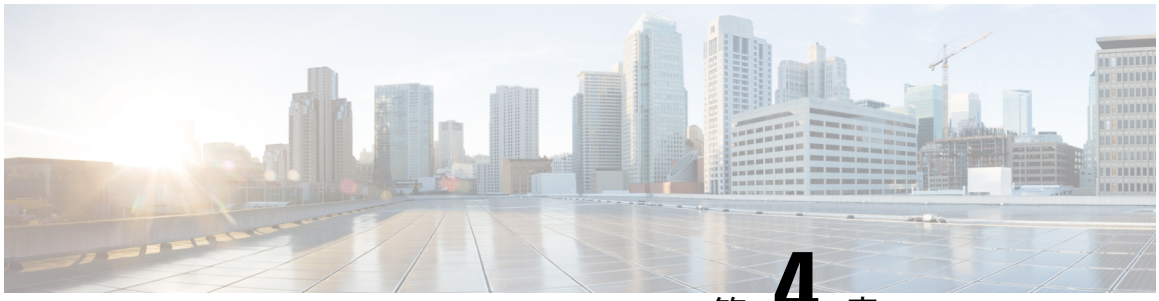
注意 ほとんどの場合、既存の FlexConfig 設定はアップグレード後も引き続き機能し、展開ができます。ただし、廃止されたコマンドを使用すると、展開の問題が発生する場合があります。

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

このドキュメントには、Version7.0 の重要なリリース固有のアップグレードガイドラインが記載されていますが、

重要 ここに記載されているガイドラインに加えて、以下の内容も確認する必要があります。

- 未解決のバグおよび解決されたバグ （107 ページ）：アップグレードに影響するバグを回避する準備を整えます。アップグレードでバージョンがスキップされる場合は、未解決および解決済みのバグについてのリリースノートを参照するか、Cisco バグ検索ツールを使用してください。
- 特長と機能 （17 ページ）：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。

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ガ

イドとコンフィギュレーション ガイド（http://www.cisco.com/jp/go/threatdefense-70-docs）を参照してください。

表 *19*：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。
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

次のように Version7.0 に直接アップグレードできます。

Version7.0 にパッチを適用する場合、パッチは4桁目のみを変更することに注意してください。以前のメジャーリリースまたはメンテナンスリリースからパッチに直接アップグレードすることはできません。

表 *20 : Version7.0* にアップグレードするための最小バージョン

プラットフォーム	最小バージョン
FMC	6.4.0
FTD	6.4.0 Firepower 4100/9300 には FXOS 2.10.1.159 が必要です。ほとんどの場合、各メジャーバージョンで最新の FXOS ビルドを使用することを推奨します。判断のヒントについては、『Cisco Firepower 4100/9300 FXOS Release Notes, 2.10(1)』を参照してください。
ASA with FirePOWER サービス	6.4.0 ASA 9.5(2) ～ 9.16(x) が必要です。ASA と ASA FirePOWER のバージョン間には広い互換性がありますが、アップグレードすることで、新機能と解決された問題を活用できます。判断のヒントについては、Cisco Secure Firewall ASA リリースノートを参照してください。
NGIPSv	6.4.0

Version7.0 のアップグレードガイドライン

以下のチェックリストでは、該当する可能性のある新規アップグレードガイドラインや以前に公開されたアップグレードガイドラインを提供します。

表 *21 : FMC* を使用した *FTD* のアップグレードガイドライン *Version7.0*

✓	ガイドライン	プラットフォーム	アップグレード元	直接アップグレード先
	アップグレードする最小バージョン （62 ページ）	いずれか（Any）	いずれか（Any）	7.0
	FXOS のアップグレードガイドライン （76 ページ）	Firepower 4100/9300	任意（Any）	7.0
	高可用性 FMC の Cisco Threat Grid に再接続する （64 ページ）	FMC	6.4.0 ー 6.7.x	7.0.0 以降

✓	ガイドライン	プラットフォーム	アップグレード元	直接アップグレード先
	アップグレードの失敗：Firepower 1010 スイッチポートでの無効な VLAN ID （65 ページ）	Firepower 1010	6.4.0 ～ 6.6.x	6.7.0 以降
	FMCv には 28 GB の RAM が必要（65 ページ）	FMCv	6.2.3 ～ 6.5.0.x	6.6.0 +
	Firepower 1000 シリーズ デバイスではアップグレード後に電源の再投入が必要 （67 ページ）	Firepower 1000 シリーズ	6.4.0	6.5.0 以降
	新しいURL カテゴリとレピュテーション （67 ページ）	任意（Any）	6.2.3 ～ 6.4.0.x	6.5.0 以降

表 *22 : FDM* を使用した *FTD* のアップグレードガイドライン *Version7.0*

✓	ガイドライン	プラットフォーム	アップグレード元	直接アップグレード先
	アップグレードする最小バージョン （62 ページ）	いずれか（Any）	いずれか（Any）	7.0
	FXOS のアップグレードガイドライン （76 ページ）	Firepower 4100/9300	いずれか（Any）	7.0
	アップグレードの失敗：Firepower 1010 スイッチポートでの無効な VLAN ID （65 ページ）	Firepower 1010	6.4.0 ～ 6.6.x	6.7.0 以降
	Firepower 1000 シリーズ デバイスではアップグレード後に電源の再投入が必要 （67 ページ）	Firepower 1000 シリーズ	6.4.0	6.5.0 以降
	FDM を使用した FTD のアップグレード時に削除される履歴データ（67 ページ）	任意（Any）	6.2.3 ～ 6.4.0.x	6.5.0 以降
	新しいURL カテゴリとレピュテーション （67 ページ）	任意（Any）	6.2.3 ～ 6.4.0.x	6.5.0 以降

高可用性 FMC の Cisco Threat Grid に再接続する

展開：動的分析のためにファイルを送信する高可用性/AMP for Networks（マルウェア検出）展開

アップグレード元：バージョン 6.4.0 ～ 6.7.x

直接アップグレード先：バージョン 7.0.0 以降

関連するバグ： CSCvu35704

バージョン 7.0.0 では、フェールオーバー後にシステムが動的分析用のファイルの送信を停止する高可用性の問題が修正されています。修正を有効にするには、Cisco Threat Grid パブリッククラウドに再度関連付ける必要があります。

高可用性ペアをアップグレードした後、プライマリ FMC で次の手順を実行します。

1. **[AMP]** > **[ダイナミック分析接続（Dynamic Analysis Connections）]**を選択します。
2. パブリッククラウドに対応するテーブル行で、 [関連付け（Associate）] をクリックします。

   ポータルウィンドウが開きます。サインインする必要はありません。再関連付けは、数分以内にバックグラウンドで行われます。

アップグレードの失敗：Firepower1010スイッチポートでの無効なVLAN ID

展開：Firepower 1010

アップグレード元：バージョン 6.4 ～ 6.6

直接アップグレード先：バージョン 6.7 以降

Firepower 1010 では、VLAN ID を 3968 ー 4047 の範囲にしてスイッチポートを設定した場合、FTD のバージョン 6.7 以降へのアップグレードは失敗します。これらの ID は内部使用専用です。

FMCv には 28 GB の RAM が必要

展開：FMCv

アップグレード元：バージョン 6.2.3 ～ 6.5

直接アップグレード先：バージョン 6.6 以降

すべての FMCv 実装には同じ RAM 要件が適用され、32 GB が推奨、28 GB が必須となりました（FMCv 300 の場合は 64 GB）。仮想アプライアンスに割り当てられたメモリが 28 GB 未満の場合、バージョン 6.6 以降へのアップグレードは失敗します。アップグレード後、メモリ割り当てを引き下げると、正常性モニターがアラートを発行します。

これらの新しいメモリ要件は、すべての仮想環境にわたって一貫した要件を適用し、パフォーマンスを向上させ、新しい機能を利用できるようにします。デフォルト設定を引き下げないことをお勧めします。使用可能なリソースによっては、パフォーマンスを向上させるために仮想アプライアンスのメモリと CPU の数を増やすことができます。詳細については、Cisco Secure Firewall Management Center Virtual スタートアップガイドを参照してください。

（注） バージョン 6.6.0 リリースの時点で、クラウドベースの FMCv の展開（AWS、Azure）でのメモリ不足インスタンスのタイプが完全に廃止されました。以前のバージョンであっても、これらを使用して新しいインスタンスを作成することはできません。既存のインスタンスは引き続き実行できます。

次の表に、メモリが不足している展開のアップグレード前の要件を示します。

表 *23 :* バージョン *6.6* 以降 にアップグレードする場合の *FMCv* のメモリ要件

プラットフォーム	アップグレード前のアクション	詳細
VMware	28 GB 以上（推奨 32 GB）を割り当てます。	最初に仮想マシンの電源をオフにします。 手順については、VMware のマニュアルを参照してください。
KVM	28 GB 以上（推奨 32 GB）を割り当てます。	手順については、ご使用の KVM 環境のマニュアルを参照してください。
AWS	インスタンスのサイズを変更します。 • c3.xlarge から c3.4xlarge へ。 • c3.2.xlarge から c3.4xlarge へ。 • c4.xlarge から c4.4xlarge へ。 • c4.2xlarge から c4.4xlarge へ。 また、新規展開用に c5.4xlarge インスタンスも用意しています。	サイズを変更する前にインスタンスを停止します。これを行うと、インスタンスストアのボリューム上のデータが失われるため、最初にインスタンスストアによってバックアップされたインスタンスを最初に移行してください。さらに、管理インターフェイスに復元力のある IP アドレスがない場合は、そのパブリック IP アドレスが解放されます。 手順については、Linux インスタンスの AWS ユーザーガイドのインスタンスタイプの変更に関するマニュアルを参照してください。
Azure	インスタンスのサイズを変更します。 • Standard_D3_v2 から Standard_D4_v2 へ。	Azure ポータルまたは PowerShell を使用します。サイズを変更する前にインスタンスを停止する必要はありませんが、停止すると追加のサイズが表示される場合があります。サイズ変更により、実行中の仮想マシンが再起動されます。 手順については、Windows VM のサイズ変更に関する Azure のマニュアルを参照してください。

Firepower 1000 シリーズ デバイスではアップグレード後に電源の再投入が必要

展開：Firepower 1000 シリーズ デバイス

アップグレード元：バージョン 6.4.0.x

直接アップグレード先：バージョン 6.5.0+

バージョン 6.5.0 では、Firepower 1000/2100 および Firepower 4100/9300 シリーズ デバイス向けの FXOS CLI の「安全に消去する」機能が導入されています。

Firepower 1000 シリーズ デバイスでは、この機能を適切に動作させるには、バージョン 6.5.0+ にアップグレードした後にデバイスの電源を再投入する必要があります。自動リブートでは十分ではありません。サポートされているその他のデバイスでは、電源の再投入は必要ありません。

FDM を使用した FTD のアップグレード時に削除される履歴データ

展開：FTD（FDM を使用）

アップグレード元：バージョン 6.2.3 ～ 6.4.0.x

直接アップグレード先：バージョン 6.5.0 以降

データベース スキーマの変更により、すべての履歴レポート データがアップグレード中に削除されます。アップグレード後、履歴データをクエリしたり、履歴データをダッシュボードに表示したりすることはできません。

新しい URL カテゴリとレピュテーション

展開：すべて

アップグレード元：バージョン 6.2.3 ～ 6.4.0.x

直接アップグレード先：バージョン 6.5.0+

Talos インテリジェンスグループ は、URL の分類およびフィルタ処理のために、新しいカテゴリを導入し、レピュテーションの名前を変更しました。カテゴリの変更に関する詳細なリストについては、『Cisco Firepower Release Notes, Version 6.5.0』を参照してください。新しい URL カテゴリの説明については、Talos の「Intelligence Categories」サイトを参照してください。

また、ルール設定オプションは同じままですが、未分類およびレピュテーションのない URL の概念が新しくなっています。

- 未分類の URL は、疑わしい（Questionable）、ニュートラル（Neutral）、好ましい（Favorable）、信頼されている（Trusted）というレピュテーションのいずれかになります。

[未分類（Uncategorized）]の URL はフィルタ処理できますが、レピュテーションによりさらに制約を追加することはできません。これらのルールは、レピュテーションに関係なく、すべての未分類 URL と一致します。

カテゴリのない信頼されていない（Untrusted）ルールのような設定は存在しないことに注意してください。それ以外の場合、信頼されていない（Untrusted）レピュテーションの未分類 URL は、「悪意のあるサイト（Malicious Sites）」という新しい脅威カテゴリに自動的に割り当てられます。

- レピュテーションのない URL は任意のカテゴリに属することができます。

  レピュテーションのない URL をフィルタ処理することはできません。「レピュテーションなし」に対応するオプションはルールエディタにありません。ただし、レピュテーションに [すべて（Any）] を指定して URL をフィルタ処理することは可能で、その場合はレピュテーションのない URL が含まれます。これらの URL もカテゴリで制約する必要があります。Any/Any ルールに対するユーティリティはありません。

次の表に、アップグレードでの変更点の概要を示します。これらの変更は、ほとんどのお客様にとって最小限の影響で済むように設計されており、アップグレード後の展開を妨げることもありませんが、これらのリリースノートおよび現在の URL フィルタリングの設定を確認することを強くお勧めします。慎重な計画と準備は、誤った手順を回避することに加えて、アップグレード後のトラブルシューティングにかかる時間を短縮するのに役立ちます。

表 *24* : アップグレード時の展開の変更

変更内容	詳細
URL ルールのカテゴリが変更されます。	アップグレードにより、次のポリシーで、新しいカテゴリセットのほぼ同等のルールが使用されるように URL ルールが変更されます。 • アクセス コントロール • SSL • QoS（FMC のみ） • 相関（FMC のみ） これらの変更により、余分なルールや無効になったルールが生じ、パフォーマンスが低下する可能性があります。マージされたカテゴリが設定に含まれている場合、許可またはブロックされる URL が若干変更されることがあります。

変更内容	詳細
URL ルールのレピュテーションの名前が変更されます。	アップグレードにより、新しいレピュテーション名を使用するように URL ルールが変更されます。 **1.** 信頼されていない（「高リスク」だった） **2.** 疑わしい（「疑わしいサイト」だった） **3.** ニュートラル（「セキュリティ リスクのある無害なサイト」だった） **4.** 好ましい（「無害なサイト」だった） **5.** 信頼されている（「十分に既知」だった）
URL キャッシュをクリアします。	アップグレードによって URL キャッシュがクリアされます。このキャッシュには、システムが以前にクラウドで検索した結果が含まれています。ローカル データ セットに含まれていない URL については、アクセス時間が一時的に少し長くなることがあります。
「レガシー」イベントにラベルを付けます。	すでにログに記録されているイベントの場合、アップグレードにより、関連する URL のカテゴリおよびレピュテーション情報が「レガシー」としてラベル付けされます。これらのレガシー イベントは時間の経過とともにデータベースからエージ アウトします。

URL カテゴリおよびレピュテーションのアップグレード前のアクション

アップグレードする前に、次のアクションを実行します。

表 *25:* アップグレード前のアクション

アクション	詳細
アプライアンスが Talos のリソースにアクセスできることを確認します。	アップグレード後、システムは次のシスコのリソースと通信できる必要があります。 • https://regsvc.sco.cisco.com/ - 登録 • https://est.sco.cisco.com/ - セキュア通信のための証明書を取得 • https://updates-talos.sco.cisco.com/ - クライアント/サーバーマニフェストを取得 • http://updates.ironport.com/ - データベースのダウンロード（注：ポート 80 を使用） • https://v3.sds.cisco.com/ - クラウドクエリ クラウドクエリサービスは、次の IP アドレスブロックも使用します。 • IPv4 クラウドクエリ： • 146.112.62.0/24 • 146.112.63.0/24 • 146.112.255.0/24 • 146.112.59.0/24 • IPv6 クラウドクエリ： • 2a04:e4c7:ffff::/48 • 2a04: e4c7: fffe::/48

アクション	詳細
潜在的なルールの問題を特定します。	今後の変更点を理解します。現在の URL フィルタリング設定を調べて、アップグレード後に実行する必要があるアクションを特定します（次の項を参照）。 （注） 廃止されたカテゴリを使用する URL ルールをこの時点で変更することができます。そうしない場合、それらを使用するルールによってアップグレード後の展開が妨げられます。 FMC展開では、アクセスコントロールのルールや下位ポリシー（SSLなど）のルールを含む、ポリシーの現在の保存されている設定に関する詳細情報を提供する、アクセスコントロール ポリシー レポートを生成することを推奨します。URL ルールごとに、現在のカテゴリ、レピュテーション、関連付けられているルール アクションが表示されます。FMC で**[ポリシー（Policies）] > [アクセス制御（Access Control）]**を選択し、該当するポリシーの横にあるレポートアイコン（  ）をクリックします。

URL カテゴリおよびレピュテーションのアップグレード後のアクション

アップグレード後に URL フィルタリング設定を再確認し、できるだけ早く次のアクションを実行する必要があります。展開のタイプとアップグレードによって行われた変更に応じて、一部（すべてではない）の問題が GUI でマークされることがあります。たとえば、FMC/FDM のアクセス コントロール ポリシーでは、[警告の表示（Show Warnings）]（FMC）または [問題ルールの表示（Show Problem Rules）] (FDM) をクリックできます。

表 *26*：アップグレード後の操作

アクション	詳細
廃止されたカテゴリをルールから削除します。必須。	アップグレードでは、廃止されたカテゴリを使用する URL ルールは変更されません。これらを使用するルールは展開を阻止します。 FMC では、これらのルールがマークされます。
新しいカテゴリを含めるルールを作成または変更します。	ほとんどの新しいカテゴリは脅威を特定します。これらのカテゴリを使用することを強くお勧めします。 FMC では、この新しいカテゴリはこのアップグレード後にマークされませんが、今後、Talos によってカテゴリが追加される場合があります。この場合は新しいカテゴリがマークされます。

アクション	詳細
マージされたカテゴリの結果として変更されたルールを評価します。	影響を受けたカテゴリのいずれかが含まれている各ルールに影響を受けたすべてのルールが含まれるようになります。元のカテゴリが異なるレピュテーションに関連付けられていた場合、新しいルールはさらに広い、より包含的なレピュテーションに関連付けられます。以前と同様にURLをフィルタリングするには、いくつかの設定を変更する必要があります。「マージされた URL カテゴリを持つルールのガイドライン（72 ページ）」を参照してください。 変更内容とプラットフォームがルールの警告を処理する方法に応じて、変更がマークされることがあります。たとえば、FMCは完全に冗長および完全にプリエンプション処理されたルールをマークしますが、部分的に重複したルールはマークしません。
分割されたカテゴリの結果として変更されたルールを評価します。	アップグレードにより、URL ルール内の古い単一のカテゴリが新しいカテゴリすべてに置き換えられ、新しいカテゴリは古いカテゴリにマッピングされます。これによりURLのフィルタリング方法は変更されませんが、影響を受けるルールを変更して、新しい精度を活用することができます。 これらの変更はマークされません。
名前が変更されたカテゴリまたは**変更されていない**カテゴリを把握します。	特に対処の必要はありませんが、これらの変更に注意する必要があります。 これらの変更はマークされません。
未分類および**レピュテーションのない**URLの処理方法を評価します。	未分類の URL とレピュテーションのない URL を使用できるようになりましたが、未分類の URL をレピュテーションでフィルタ処理することも、レピュテーションのない URL をフィルタ処理することもできません。 [未分類（Uncategorized）] カテゴリまたは [すべて（Any）] のレピュテーションでフィルタ処理されるルールが、期待どおりに動作することを確認してください。

マージされた URL カテゴリを持つルールのガイドライン

アップグレード前に URL フィルタリング設定を確認する場合は、次のシナリオとガイドラインのどちらが適用されるかを決定します。これにより、アップグレード後の設定が予想どおりに実行され、問題を解決するためのクイックアクションを実行できるようになります。

表 *27 :* マージされた *URL* カテゴリを持つルールのガイドライン

ガイドライン	詳細
ルールの順序によってトラフィックに一致するルールを決定	同じカテゴリを含むルールを検討する場合は、トラフィックが、その条件を含むリスト内の最初のルールと一致することに注意してください。
同じルール内のカテゴリと異なるルール内のカテゴリ	単一のルール内でカテゴリをマージすると、ルール内の単一のカテゴリにマージされます。たとえば、カテゴリ A とカテゴリ B がマージされてカテゴリ AB になり、カテゴリ A とカテゴリ B を持つルールがある場合、マージ後にルールは単一のカテゴリ AB を保持します。 異なるルールのカテゴリをマージすると、マージ後に各ルールで同じカテゴリを持つルールが個別に生成されます。たとえば、カテゴリ A とカテゴリ B がマージされてカテゴリ AB になり、カテゴリ A を持つルール 1 とカテゴリ B を持つルール 2 がある場合、マージ後にルール 1 とルール 2 にはカテゴリ AB がそれぞれ含まれます。この状況を解決する方法は、ルールの順序、ルールに関連付けられたアクションとレピュテーションレベル、ルールに含まれる他の URL カテゴリ、およびルールに含まれる非 URL 条件によって異なります。
関連付けられたアクション	異なるルールのマージされたカテゴリが異なるアクションに関連付けられている場合、マージ後に、同じカテゴリに対して異なるアクションを持つ 2 つ以上のルールが生成される場合があります。
関連付けられているレピュテーションレベル	マージの前に異なるレピュテーションレベルに関連付けられたカテゴリが単一のルールに含まれている場合、マージされたカテゴリは、より包括的なレピュテーションレベルに関連付けられます。たとえば、カテゴリ A が特定のルールで [すべてのレピュテーション（Any reputation）] に関連付けられており、カテゴリ B が同じルールでレピュテーションレベル [3 - セキュリティリスクのある無害なサイト（3 - Benign sites with security risks）] に関連付けられている場合、マージ後に、そのルール内のカテゴリ AB は [すべてのレピュテーション（Any reputation）] に関連付けられます。

ガイドライン	詳細
重複および冗長カテゴリとルール	マージ後、異なるルールには、異なるアクションとレピュテーションレベルに関連付けられている同じカテゴリが含まれる場合があります。 冗長ルールは完全に重複しているとは限りませんが、ルール順序が前にある別のルールが一致する場合、トラフィックに一致しなくなる可能性があります。たとえば、ルール 1 とカテゴリ A（[すべてのレピュテーション（Any Reputation）] に適用される）を事前マージし、ルール 2 とカテゴリ B（レピュテーション 1-3 のみに適用される）を事前マージする場合、マージ後に、ルール 1 とルール 2 の両方にカテゴリ AB が含まれるようになるが、ルール順序でルール 1 の順序が前にあると、ルール 2 が一致することはありません。 FMC において、同一のカテゴリとレピュテーションを持つルールでは警告が表示されます。ただし、これらの警告は、含まれているカテゴリが同じですが、レピュテーションが異なるルールを示すことはありません。 注意：重複または冗長カテゴリを解決する方法を決定する際には、ルールのすべての条件を考慮してください。
ルール内の他の URL カテゴリ	マージされた URL を含むルールには、他の URL カテゴリも含まれている場合があります。したがって、マージ後に特定のカテゴリが複製された場合は、これらのルールを削除するのではなく、変更する必要があることがあります。
ルール内の非 URL 条件	マージされた URL カテゴリを含むルールには、アプリケーション条件などの他のルール条件も含まれている場合があります。したがって、マージ後に特定のカテゴリが複製された場合は、これらのルールを削除するのではなく、変更する必要があることがあります。

次の表の例ではカテゴリ A とカテゴリ B を使用しています。現在はカテゴリ AB にマージされています。2 つのルールの例では、ルール 1 はルール 2 よりも前に表示されます。

表 *28*：マージされた *URL* カテゴリを持つルールの例

シナリオ	アップグレード前	アップグレード後
同じルール内のマージされたカテゴリ	ルール 1 にはカテゴリ A とカテゴリ B が含まれる。	ルール 1 にはカテゴリ AB が含まれる。

シナリオ	アップグレード前	アップグレード後
異なるルール内でマージされたカテゴリ	ルール 1 にはカテゴリ A が含まれる。 ルール 2 にはカテゴリ B が含まれる。	ルール 1 にはカテゴリ AB が含まれる。 ルール 2 にはカテゴリ AB が含まれる。 具体的な結果は、リスト内のルールの順序、レピュテーションレベル、および関連付けられたアクションによって異なります。また、冗長性を解決する方法を決定する際に、ルール内の他のすべての条件も考慮する必要があります。
異なるルール内でマージされたカテゴリには異なるアクションが含まれる （レピュテーションは同じ）	ルール 1 には [許可（Allow）] に設定されたカテゴリ A が含まれる。 ルール 2 には [ブロック（Block）] に設定されたカテゴリ B が含まれる。 （レピュテーションは同じ）	ルール 1 には [許可（Allow）] に設定されたカテゴリ AB が含まれる。 ルール 2 には [ブロック（Block）] に設定されたカテゴリ AB が含まれる。 ルール 1 は、このカテゴリのすべてのトラフィックに一致します。 ルール 2 がトラフィックに一致することはなく、カテゴリとレピュテーションの両方が同じであるため、マージ後に警告を表示した場合は、警告インジケータが表示されます。
同じルール内でマージされたカテゴリには異なるレピュテーションレベルが含まれる	ルール 1 には次が含まれます。 レピュテーション Any のカテゴリ A レピュテーション 1-3 のカテゴリ B	ルール 1 にはレピュテーション Any のカテゴリ AB が含まれる。
異なるルール内でマージされたカテゴリには異なるレピュテーションレベルが含まれる	ルール 1 にはレピュテーション Any のカテゴリ A が含まれる。 ルール 2 にはレピュテーション 1-3 のカテゴリ B が含まれる。	ルール 1 にはレピュテーション Any のカテゴリ AB が含まれる。 ルール 2 にはレピュテーション 1-3 のカテゴリ AB が含まれる。 ルール 1 は、このカテゴリのすべてのトラフィックに一致します。 ルール 2 がトラフィックに一致することはありませんが、レピュテーションが同一でないため、警告インジケータは表示されません。

Version7.0 パッチのアップグレードガイドライン

以下のチェックリストでは、該当する可能性のあるパッチのアップグレードガイドラインを提供します。

表 *29 : FMC Version7.0* パッチのアップグレードガイドライン

✓	ガイドライン	プラットフォーム	アップグレード元	直接アップグレード先
	アップグレードする最小バージョン （62 ページ）	いずれか（Any）	いずれか（Any）	任意のパッチ
	アンインストールに対応するパッチ （78 ページ）	いずれか（Any）	いずれか（Any）	任意のパッチ

表 *30 : FDM Version7.0* パッチのアップグレードガイドライン

✓	ガイドライン	プラットフォーム	アップグレード元	直接アップグレード先
	アップグレードする最小バージョン （62 ページ）	いずれか（Any）	いずれか（Any）	任意のパッチ

FXOS のアップグレードガイドライン

Firepower 4100/9300 の場合、FTD のメジャーアップグレードには FXOS のアップグレードも必要です。FTD のメジャーバージョンには特別に認定および推奨されている付随の FXOS バージョンがあります。シスコではこれらの組み合わせの拡張テストを実施するため、可能な限りこれらの組み合わせを使用してください。メンテナンスリリースとパッチで FXOS のアップグレードが必要になることはほとんどありませんが、最新の FXOS ビルドにアップグレードして、解決済みの問題を有効に活用することもできます。

重要なリリース固有のアップグレードガイドライン、新機能および廃止された機能、未解決のバグおよび解決済みのバグについては、Cisco Firepower 4100/9300 FXOS リリースノート を参照してください。

FTD をアップグレードするために必要な FXOS の最小バージョン

Version7.0 を実行するために必要な FXOS の最小バージョンは、FXOS 2.10.1.159 です。

FXOS をアップグレードするために必要な FXOS の最小バージョン

FXOS 2.2.2 から、それ以降の任意の FXOS バージョンにアップグレードできます。

FXOS アップグレードの所要時間

FXOS のアップグレードには最長 45 分かかることがあり、トラフィックフローやインスペクションに影響を与える場合があります。詳細については、FXOS のアップグレードでのトラフィックフローとインスペクション （79 ページ）を参照してください。

応答しないアップグレード

アップグレード中は、設定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。

アップグレードを元に戻すまたはアンインストールする

アップグレードに成功したにもかかわらず、システムが期待どおりに機能しない場合は、復元またはアンインストールが可能な場合があります。

- メジャーおよびメンテナンスアップグレードを FTD に復元することができます。
- アンインストールは、FMC を搭載した FTD へのパッチが対象です。FMC パッチをアンインストールすることもできます。

これらの方法のいずれも機能しない場合、以前のバージョンに戻すには、イメージを再作成する必要があります。ホットフィックスでは、復元もアンインストールもサポートされていないことに注意してください。 手順については、復元先のバージョンではなく、現在実行しているバージョンのアップグレードガイドを参照してください。

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 7.0 のパッチ

現在、すべてのバージョン 7.0 パッチがアンインストールに対応しています。

トラフィック フローとインスペクション

デバイスのアップグレードにより、トラフィックフローとインスペクションが影響を受けます。影響が最も少ない時間帯にメンテナンス期間をスケジュールします。

FXOS のアップグレードでのトラフィックフローとインスペクション

FXOS をアップグレードするとシャーシが再起動します。高可用性や拡張性を導入する場合でも、各シャーシの FXOS を個別にアップグレードします。中断を最小限に抑えるには、1 つずつシャーシをアップグレードします。

表 *31 :* トラフィックフローとインスペクション：*FXOS* のアップグレード

導入	トラフィックの挙動	メソッド
スタンドアロン	廃棄	—
高可用性	影響なし。	**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。
	1 つのピアがオンラインになるまでドロップされる。	スタンバイでアップグレードが終了する前に、アクティブ ピアで FXOS をアップグレードします。
シャーシ間クラスタ	影響なし。	**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。
	少なくとも 1 つのモジュールがオンラインになるまでドロップされる。	ある時点ですべてのモジュールを停止するため、シャーシを同時にアップグレードします。
シャーシ内クラスタ（FirePOWER 9300 のみ）	検査なしで受け渡される。	ハードウェアバイパス有効：[Bypass: Standby] または [Bypass-Force]。
	少なくとも 1 つのモジュールがオンラインになるまでドロップされる。	ハードウェアバイパス無効：[Bypass: Disabled]。
	少なくとも 1 つのモジュールがオンラインになるまでドロップされる。	ハードウェア バイパス モジュールなし。

FMC を使用した FTD アップグレードのトラフィックフローとインスペクション

スタンドアロンデバイスでのソフトウェアのアップグレード

アップグレード中、デバイスはメンテナンスモードで稼働します。アップグレードの開始時にメンテナンスモードを開始すると、トラフィック インスペクションが 2 ー 3 秒中断します。イ

ンターフェイスの構成により、その時点とアップグレード中の両方のスタンドアロンデバイスによるトラフィックの処理方法が決定されます。

表 *32:* トラフィックフローとインスペクション：スタンドアロンデバイスでのソフトウェアのアップグレード

インターフェイス コンフィギュレーション		トラフィックの動作
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 ISA 3000 のブリッジ グループ インターフェイスの場合に限り、FlexConfig ポリシーを使用して、停電時のハードウェアバイパスを設定できます。これにより、ソフトウェアのアップグレード中にトラフィックのドロップが発生しますが、デバイスがアップグレード後の再起動中、インスペクションなしでトラフィックが通過します。
IPS のみのインターフェイス	インラインセット、ハードウェアバイパス強制が有効：[バイパス（Bypass）]：[強制（Force）]	ハードウェアバイパスを無効にするか、スタンバイモードに戻すまで、インスペクションなしで合格。
	インラインセット、ハードウェアバイパスがスタンバイモード：[バイパス（Bypass）]：[スタンバイ（Standby）]	デバイスがメンテナンスモードの場合、アップグレード中にドロップされます。その後、デバイスがアップグレード後の再起動を完了する間、インスペクションなしで合格します。
	インラインセット、ハードウェアバイパスが無効：[バイパス（Bypass）]：[無効（Disabled）]	廃棄
	インラインセット、ハードウェアバイパス モジュールなし。	廃棄
	インラインセット、タップモード。	パケットをただちに出力、コピーへのインスペクションなし。
	パッシブ、ERSPAN パッシブ。	中断なし、インスペクションなし。

高可用性および拡張性に関するソフトウェアのアップグレード

高可用性デバイスやクラスタ化されたデバイスのアップグレード中に、トラフィックフローや検査が中断されることはありません。高可用性ペアの場合、スタンバイデバイスが最初にアッ

プグレードされます。デバイスの役割が切り替わり、新しくスタンバイになったデバイスがアップグレードされます。

クラスタの場合、データ セキュリティ モジュールを最初にアップグレードして、その後コントロールモジュールをアップグレードします。コントロール セキュリティ モジュールをアップグレードする間、通常トラフィックインスペクションと処理は続行しますが、システムはロギングイベントを停止します。ロギングダウンタイム中に処理されるトラフィックのイベントは、アップグレードが完了した後、非同期のタイムスタンプ付きで表示されます。ただし、ロギングダウンタイムが大きい場合、システムはログ記録する前に最も古いイベントをプルーニングすることがあります。

ソフトウェアのアンインストール（パッチ）

スタンドアロンデバイスの場合、パッチのアンインストール中のトラフィックフローと検査の中断は、アップグレードの場合と同じになります。高可用性および拡張性の展開では、中断を最小限に抑えるために、アンインストールの順序を明確に計画する必要があります。これは、ユニットとしてアップグレードしたデバイスであっても、デバイスから個別にパッチをアンインストールするためです。

設定変更の導入

Snort プロセスを再起動すると、高可用性/拡張性を備えた構成になっているものを含め、すべてのデバイスでトラフィックフローとインスペクションが一時的に中断されます。インターフェイス設定により、中断中にインスペクションせずにトラフィックをドロップするか受け渡すかが決定されます。Snort を再起動せずに展開すると、リソース要求時にいくつかのパケットが検査なしでドロップされることがあります。

Snort は、通常、アップグレード直後の最初の展開時に再起動されます。展開の前に、特定のポリシーまたはデバイス設定を変更しない限り、それ以外の展開時に再起動されることはありません。

表 *33*：トラフィックフローとインスペクション：設定変更の展開

インターフェイス コンフィギュレーション		トラフィックの動作
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、[フェールセーフ（Failsafe）] が有効または無効。	検査なしで受け渡される。 [フェールセーフ（Failsafe）] が無効で、Snortがビジーでもダウンしていない場合、いくつかのパケットがドロップすることがあります。
	インラインセット、[Snortフェールオープン：ダウン（Snort Fail Open: Down）]：無効	廃棄
	インライン、[Snortフェールオープン：ダウン（Snort Fail Open: Down）]：有効	検査なしで受け渡される。
	インラインセット、タップモード。	パケットをただちに出力、コピーへのインスペクションなし。
	パッシブ、ERSPAN パッシブ。	中断なし、インスペクションなし。

FDM を使用した FTD アップグレードのトラフィックフローとインスペクション

ソフトウェアのアップグレード

アップグレード中にトラフィックがドロップされます。高可用性の展開では、デバイスを1つずつアップグレードすることで、中断を最小限に抑えることができます。

ISA 3000 の場合にのみ、電源障害に対するハードウェアバイパスを設定すると、トラフィックはアップグレード中にドロップされますが、デバイスのアップグレード後の再起動中に検査なしでトラフィックが渡されます。

ソフトウェアの復元（メジャーおよびメンテナンスリリース）

復元中にトラフィックがドロップされます。高可用性の展開では、両方のユニットを同時に復元すると、復元が成功する可能性が高くなります。最初のユニットがオンラインに戻ると、トラフィックフローとインスペクションが再開されます。

設定変更の導入

Snort プロセスを再起動すると、高可用性を備えた構成になっているものを含め、すべてのデバイスでトラフィックフローとインスペクションが一時的に中断されます。Snort を再起動せずに展開すると、リソース要求時にいくつかのパケットが検査なしでドロップされることがあります。

Snort は、通常、アップグレード直後の最初の展開時に再起動されます。展開の前に、特定のポリシーまたはデバイス設定を変更しない限り、それ以外の展開時に再起動されることはありません。

FMC を使用した ASA FirePOWER のアップグレードでのトラフィックフローとインスペクション

ソフトウェアのアップグレード

ASA FirePOWER モジュールへのトラフィックリダイレクトに関する ASA サービスポリシーによって、モジュールがソフトウェアアップグレード中にトラフィックを処理する方法が決定されます。

表 *34 :* トラフィックフローとインスペクション：*ASA FirePOWER* のアップグレード

トラフィック リダイレクト ポリシー	トラフィックの挙動
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

ソフトウェアのアンインストール（パッチ）

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。ASA フェールオーバーおよびクラスタの展開では、中断を最小限に抑えるために、アンインストールの順序を明確に計画する必要があります。これは、ユニットとしてアップグレードしたデバイスであっても、デバイスから個別にパッチをアンインストールするためです。

設定変更の導入

Snort プロセスを再開すると、一時的にトラフィックフローと検査が中断されます。Snort プロセスが再起動している間のトラフィックの挙動は、ASA FirePOWER をアップグレードする場合と同じです。Snort を再起動せずに展開すると、リソース要求時にいくつかのパケットが検査なしでドロップされることがあります。

Snort は、通常、アップグレード直後の最初の展開時に再起動されます。展開の前に、特定のポリシーまたはデバイス設定を変更しない限り、それ以外の展開時に再起動されることはありません。

FMC を使用した NGIPSv のアップグレードでのトラフィックフローとインスペクション

ソフトウェアのアップグレード

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

表 *35 :* トラフィックフローとインスペクション：*NGIPSv* 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
インライン	廃棄
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。

ソフトウェアのアンインストール（パッチ）

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。

設定変更の導入

Snort プロセスを再開すると、一時的にトラフィックフローと検査が中断されます。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。Snort を再起動せずに展開すると、リソース要求時にいくつかのパケットが検査なしでドロップされることがあります。

Snort は、通常、アップグレード直後の最初の展開時に再起動されます。展開の前に、特定のポリシーまたはデバイス設定を変更しない限り、それ以外の展開時に再起動されることはありません。

表 *36 :* トラフィックフローとインスペクション：設定変更の展開

インターフェイス コンフィギュレーション	トラフィックの挙動
インライン、[フェールセーフ（Failsafe）] が有効または無効	検査なしで受け渡される。 [フェールセーフ（Failsafe）] が無効で、Snort がビジーでもダウンしていない場合、いくつかの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（77 ページ）を参照してください。

表 *37* : 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。
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。

条件	詳細
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 *38*：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。

プラットフォーム	コマンド
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 7.0.3 の時間とディスク容量

表 *39 :* バージョン *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 15.1 GB	/ 内で 20 MB	—	52 分	7 分
FMCv：VMware		/var 内で 20.1 GB	/ 内で 29 MB	—	40 分	5 分
Firepower 1000 シリーズ		—	/ngfw 内で 6.7 GB	860 MB	16 分	16 分
Firepower 2100 シリーズ		—	/ngfw 内で 6.7 GB	910 MB	11 分	16 分
Firepower 4100 シリーズ		—	/ngfw 内で 6.9 GB	810 MB	12 分	10 分
Firepower 4100 シリーズ コンテナ インスタンス		—	/ngfw 内で 8.9 GB	810 MB	12 分	8 分
Firepower 9300		—	/ngfw 内で 7.0 GB	810 MB	15 分	11 分
FTD を搭載した ASA 5500-X シリーズ	バージョン 6.4.0 ～ 6.6.0	/home 内で 5.3 GB	/ngfw 内で 944 KB	1.0 GB	20 分	19 分
	バージョン 6.7.0	/ngfw/Volume 内で 5.3 GB	/ngfw 内で 200 KB			
	バージョン 7.0.0	/ngfw/var 内で 5.3 GB	/ngfw/bin 内で 300 MB			
FTDv：VMware	バージョン 6.4.0 ～ 6.6.0	/home 内で 5.3 GB	/ngfw 内で 936 KB	1.0 GB	12 分	9 分
	バージョン 6.7.0	/ngfw/Volume 内で 5.6 GB	/ngfw 内で 200 KB			
	バージョン 7.0.0	/ngfw/var 内で 5.7 GB	/ngfw/bin 内で 180 MB			
ASA FirePOWER		/var 内で 8.6 GB	/ 内で 26 MB	1.2 GB	58 分	7 分
NGIPSv		/var 内で 5.7 GB	/ 内で 21 MB	730 MB	10 分	7 分

バージョン 7.0.2.1 の時間とディスク容量

表 *40 :* バージョン *7.0.2.1* の時間とディスク容量

プラットフォーム	ボリュームの容量	必要容量	FMC の容量	アップグレード時間	リブート時間
FMC	/var 内で 2 GB	/ 内で 19 MB	—	30 分	4 分
FMCv：VMware	/var 内で 1.9 GB	/ 内で 13 MB	—	26 分	3 分
Firepower 1000 シリーズ	—	/ngfw 内で 1.4 GB	180 MB	7 分	9 分
Firepower 2100 シリーズ	—	/ngfw 内で 1.3 GB	180 MB	6 分	10 分
Firepower 4100 シリーズ	—	/ngfw 内で 1.4 GB	180 MB	5 分	7 分
Firepower 9300	—	/ngfw 内で 1.3 GB	180 MB	4 分	8 分
FTD を搭載した ASA 5500-X シリーズ	/ngfw/var 内で 900 MB	/ngfw/bin 内で 190 MB	190 MB	7 分	12 分
FTDv：VMware	/ngfw/var 内で 900 MB	/ngfw/bin 内で 190 MB	190 MB	4 分	5 分
ASA FirePOWER	/var 内で 950 MB	/ 内で 13 MB	55 MB	57 分	6 分
NGIPSv	/var 内で 42 MB	/ 内で 13 MB	9 MB	5 分	3 分

バージョン 7.0.2 の時間とディスク容量

表 *41 :* バージョン *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 17.2 GB	/ 内で 20 MB	—	53 分	7 分
FMCv：VMware	/var 内で 17.2 GB	/ 内で 29 MB	—	40 分	5 分
Firepower 1000 シリーズ	—	/ngfw 内で 7.0 GB	560 MB	16 分	17 分
Firepower 2100 シリーズ	—	/ngfw 内で 6.7 GB	910 MB	11 分	16 分
Firepower 4100 シリーズ	—	/ngfw 内で 6.9 GB	810 MB	13 分	10 分
Firepower 4100 シリーズ コンテナ インスタンス	—	/ngfw 内で 8.2 GB	810 MB	12 分	6 分
Firepower 9300	—	/ngfw 内で 6.9 GB	810 MB	12 分	11 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
FTD を搭載した ASA 5500-X シリーズ	バージョン 6.4.0 ～ 6.6.0	/home 内で 5.7 GB	/ngfw 内で 944 KB	1.0 GB	18 分	19 分
	バージョン 6.7.0	/ngfw/Volume 内で 5.5 GB	/ngfw 内で 300 KB			
	バージョン 7.0.0	/ngfw/var 内で 5.3 GB	/ngfw/bin 内で 3.4 GB			
FTDv：VMware	バージョン 6.4.0 ～ 6.6.0	/home 内で 5.3 GB	/ngfw 内で 936 KB	1.0 GB	10 分	8 分
	バージョン 6.7.0	/ngfw/Volume 内で 5.5 GB	/ngfw 内で 200 KB			
	バージョン 7.0.0	/ngfw/var 内で 5.5 GB	/ngfw/bin 内で 180 MB			
ASA FirePOWER		/var 内で 8.0 GB	/ 内で 26 MB	1.2 GB	70 分	14 分
NGIPSv		/var 内で 5.8 GB	/ 内で 21 MB	730 MB	12 分	7 分

バージョン 7.0.1.1 の時間とディスク容量

表 *42 :* バージョン *7.0.1.1* 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 650 MB	/ 内で 29 MB	—	9 分	/ngfw に 2.5 GB
FMCv：VMware	/var 内で 770 MB	/ 内で 13 MB	—	9 分	/ngfw に 2.5 GB
Firepower 1000 シリーズ	—	/ngfw 内で 2.1 GB	300 MB	8 分	14 分
Firepower 2100 シリーズ	—	/ngfw 内で 2.1 GB	300 MB	7 分	使用できません
Firepower 4100 シリーズ	—	/ngfw 内で 1.4 GB	300 MB	5 分	8 分
Firepower 9300	—	/ngfw 内で 1.7 GB	300 MB	4 分	8 分
FTD を搭載した ASA 5500-X シリーズ	/ngfw/var 内で 1.3 GB	/ngfw/bin 内で 180 MB	310 MB	7 分	11 分
FTDv：VMware	/ngfw/var 内で 1.4 GB	/ngfw/bin 内で 180 MB	310 MB	4 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
ASA FirePOWER	/var 内で 760 MB	/ 内で 13 MB	250 MB	36 分	[1 分（1 min）]
NGIPSv	/var 内で 810 MB	/ 内で 13 MB	250 MB	5 分	3 分

バージョン 7.0.1 の時間とディスク容量

表 *43 :* バージョン *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 17 GB	/ 内で 20 MB	—	51 分	8 分
FMCv：VMware		/var 内で 19.5 GB	/ 内で 29 MB	—	41 分	6 分
Firepower 1000 シリーズ		—	/ngfw 内で 7 GB	850 MB	17 分	25 分
Firepower 2100 シリーズ		—	/ngfw 内で 6.6 GB	900 MB	12 分	16 分
Firepower 4100 シリーズ		—	/ngfw 内で 6.9 GB	800 MB	12 分	11 分
Firepower 4100 シリーズ コンテナ インスタンス		—	/ngfw 内で 9.3 GB	800 MB	12 分	9 分
Firepower 9300		—	/ngfw 内で 6.8 GB	800 MB	16 分	10 分
FTD を搭載した ASA 5500-X シリーズ	バージョン 6.4.0 ～ 6.6.0	/home 内で 6 GB	/ngfw 内で 944 KB	1GB	17 分	18 分
	バージョン 6.7.0	/ngfw/Volume 内で 4 GB	/ngfw 内で 208 KB			
	バージョン 7.0.0	/ngfw/var 内で 5.4 GB	/ngfw/bin 内で 320 MB			
FTDv：VMware	バージョン 6.4.0 ～ 6.6.0	/home 内で 5.3 GB	/ngfw 内で 944 KB	1 GB	18 分	18 分
	バージョン 6.7.0	/ngfw/Volume 内で 4.7 GB	/ngfw 内で 200 KB			
	バージョン 7.0.0	/ngfw/var 内で 4.2 GB	/ngfw/bin 内で 175 MB			
ASA FirePOWER		/var 内で 8.6 GB	/ 内で 26 MB	1.1 GB	65 分	7 分
NGIPSv		/var 内で 4.5 GB	/ 内で 21 MB	720 MB	10 分	5 分

バージョン 7.0.0.1 の時間とディスク容量

表 *44 :* バージョン *7.0.0.1* の時間とディスク容量

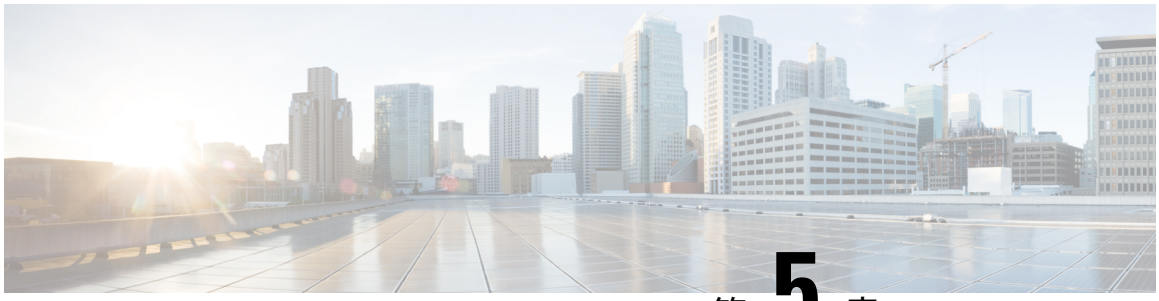
プラットフォーム	ボリュームの容量	必要容量	FMC の容量	アップグレード時間	リブート時間
FMC	/var 内で 350 MB	/ 内で 19 MB	—	8 分	8 分
FMCv：VMware	/var 内で 66 MB	/ 内で 13 MB	—	9 分	/ngfw に 2.5 GB
Firepower 1000 シリーズ	—	/ngfw 内で 720 MB	47 MB	8 分	9 分
Firepower 2100 シリーズ	—	/ngfw 内で 710 MB	42 MB	6 分	10 分
Firepower 4100 シリーズ	—	/ngfw 内で 800 MB	47 MB	4 分	6 分
Firepower 9300	—	/ngfw 内で 860 MB	47 MB	4 分	32 分
FTD を搭載した ASA 5500-X シリーズ	/ngfw/var 内で 470 MB	/ngfw/bin 内で 170 MB	54 MB	6 分	10 分
FTDv：VMware	/ngfw/var 内で 490 MB	/ngfw/bin 内で 160 MB	54 MB	4 分	4 分
ASA FirePOWER	/var 内で 54 MB	/ 内で 13 MB	8 MB	39 分	4 分
NGIPSv	/var 内で 66 MB	/ 内で 13 MB	8 MB	5 分	3 分

バージョン 7.0.0 の時間とディスク容量

表 *45 :* バージョン *7.0.0* の時間とディスク容量

プラットフォーム	ボリュームの容量	必要容量	FMC の容量	アップグレード時間	リブート時間
FMC	/var 内で 14 GB	/ 内で 70 MB	—	41 分	7 分
FMCv：VMware	/var 内で 16 GB	/ 内で 72 MB で	—	28 分	4 分
Firepower 1000 シリーズ	/ngfw/var 内で 420 MB	/ngfw 内で 7.6 GB	890 MB	12 分	14 分
Firepower 2100 シリーズ	/ngfw/var 内で 480 MB	/ngfw 内で 7.7 GB	950 MB	11 分	13 分
Firepower 4100 シリーズ	/ngfw/var 内で 40 MB	/ngfw 内で 8.4 GB	830 MB	8 分	9 分
Firepower 4100 シリーズ コンテナ インスタンス	/ngfw/var 内で 36 MB	/ngfw 内で 9.7 GB	830 MB	8 分	7 分

プラットフォーム	ボリュームの容量	必要容量	FMC の容量	アップグレード時間	リブート時間
Firepower 9300	/ngfw/var 内で 45 MB	/ngfw 内で 11.1 GB	830 MB	11 分	11 分
FTD を搭載した ASA 5500-X シリーズ	/ngfw/var 内で 5.3 GB	/ngfw 内で 95 KB	1.1 GB	25 分	12 分
FTDv：VMware	/ngfw/var 内で 6.6 GB	/ngfw 内で 23 KB	1.1 GB	11 分	6 分
ASA FirePOWER	/var 内で 9.5 GB	/ 内で 64 MB	1.1 GB	69 分	8 分
NGIPSv	/var 内で 5 GB	/ 内で 54 MB	720 MB	8 分	4 分



第 5 章

ソフトウェアのインストール

Version7.0 に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。これは再イメージ化とも呼ばれます。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。

設置に関するガイドライン

以下のガイドラインにより再イメージ化の一般的な問題を防ぐことができますが、包括的な解決策ではありません。詳細なチェックリストと手順については、該当するインストールガイドを参照してください。

バックアップ

再イメージ化の前に、安全なリモートロケーションにバックアップし、正常に転送されたことを確認することを強く推奨します。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。

（注） アップグレードを不要にするため再イメージ化したい場合、バージョンの制約によっては、バックアップを使用して古い設定をインポートすることはできません。設定は手動で再作成する必要があります。

アプライアンス アクセス

アプライアンスに物理的にアクセスできない場合、現在のメジャーリリースまたはメンテナンスリリースへの再イメージ化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

定を削除する場合や以前のリリースに再イメージ化する場合は、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。

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。

Smart Software Manager からのの登録解除

アプライアンスまたはスイッチデバイス管理のイメージを再作成する前に、Cisco Smart Software Manager（CSSM） での登録解除が必要になる場合があります。これは、再登録を妨げる可能性のある孤立した権限付与の発生を避けるためです。

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。

バックアップから復元する予定がある場合は、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手動で元に戻します。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。

表 *46 : CSSM* からの登録解除シナリオ（バックアップから復元しない）

シナリオ	アクション
FMC を再イメージ化します。	手動で登録解除します。
FMC のモデルを移行します。	ソースのFMCをシャットダウンする前に、手動で登録を解除します。
FMC で FTD を再イメージ化します。	FMCからデバイスを削除すると、自動的に登録が解除されます。
FDM で FTD を再イメージ化します。	手動で登録解除します。
FMCからデバイスマネージャーにFTDを切り替えます。	FMCからデバイスを削除すると、自動的に登録が解除されます。
デバイスマネージャーから FMC に FTD を切り替えます。	手動で登録解除します。

管理からデバイスを削除します。

FMC の展開で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、FMC からデバイスを削除します。バックアップからの復元を予定している場合は、これを行う必要はありません。

表 *47*：管理からデバイスを削除するシナリオ（バックアップから復元しない）

シナリオ	アクション
FMC を再イメージ化します。	管理からデバイスを削除します。
FTD を再イメージ化します。	管理から任意のデバイスを削除します。
デバイスマネージャーから FMC に FTD を切り替えます。	管理から任意のデバイスを削除します。

FXOS をダウングレードするための FTD ハードウェアの完全な再イメージ化

FXOS オペレーティングシステムを使用する FTD ハードウェアモデルの場合、以前のソフトウェアバージョンに再イメージ化するには、FXOS がソフトウェアにバンドルされているか、個別にアップグレードされているかに関係なく、完全な再イメージ化が必要になる場合があります。

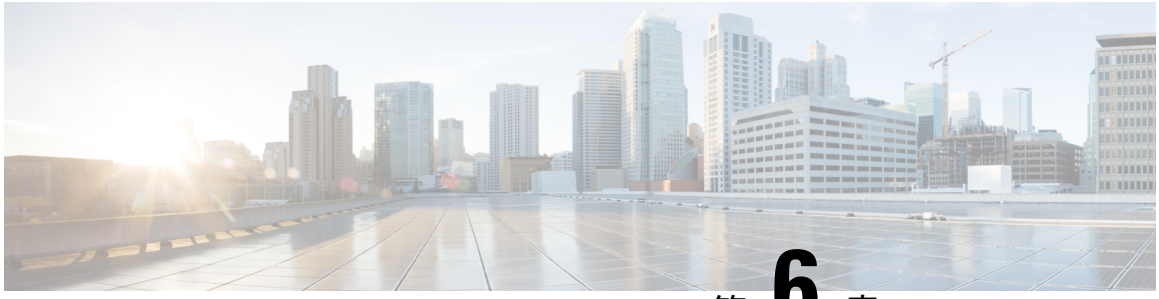
表 *48*：完全な再イメージ化のシナリオ

モデル	詳細
Firepower 1000 シリーズ Firepower 2100 シリーズ	**erase configuration** メソッドを使用してイメージを再作成すると、FXOS がソフトウェアとともにダウングレードされ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。これらの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。
Firepower 4100/9300	FTD を復元しても FXOS はダウングレードされません。 Firepower 4100/9300 の場合、FTD のメジャーバージョンには特別に認定および推奨されている付随の FXOS バージョンがあります。FTD の以前のバージョンに戻った後、推奨されていないバージョンの FXOS（新しすぎる）を実行している可能性があります。 新しいバージョンの FXOS は旧バージョンの FTD と下位互換性がありますが、シスコでは推奨の組み合わせについて拡張テストを実施しています。FXOS を手動ではダウングレードできないため、このような状況下で推奨の組み合わせを稼働するには、完全な再イメージ化が必要になります。

設置ガイド

表 *49*：設置ガイド

プラットフォーム	ガイド
FMC	
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 スタートアップガイド
FTD	
Firepower 1000/2100	Cisco Secure Firewall ASA および Cisco Secure Firewall 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 および Cisco Secure Firewall 3100 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 Cisco Secure Firewall Threat Defense 再イメージ化ガイド
ISA 3000	Cisco Secure Firewall ASA および Cisco Secure Firewall Threat Defense 再イメージ化ガイド
FTDv	Cisco Secure Firewall Threat Defense Virtual スタートアップガイド
ASA FirePOWER/NGIPSv	
ASA FirePOWER	Cisco Secure Firewall ASA および Cisco Secure Firewall Threat Defense 再イメージ化ガイド ASDM ブック 2：Cisco ASA シリーズ ファイアウォール ASDM 7.16 コンフィギュレーション ガイド
NGIPSv	Cisco Firepower NGIPSv Quick Start Guide for VMware



第 6 章

ソフトウェアの復元またはアンインストール

アップグレードに成功したにもかかわらず、システムが期待どおりに機能しない場合は、以前のバージョンに戻せることがあります。

- メジャーおよびメンテナンスアップグレードを FDM を使用する FDM に戻します。
- FMC および ASDM 展開のパッチをアンインストールします。

これらの方法のいずれも機能しない場合、以前のバージョンに戻すには、イメージを再作成する必要があります。ホットフィックスでは、復元もアンインストールもサポートされていないことに注意してください。アップグレードが失敗した場合は、「応答しないアップグレード（77 ページ）」を参照してください。

FDM を使用する FTD の復元

メジャーまたはメンテナンスアップグレードを復元すると、ソフトウェアは（スナップショットとも呼ばれる）アップグレードの直線の状態に戻ります。パッチ適用後に復元すると、パッチも必然的に削除されます。FDM を使用して FTD アップグレードを正常に復元するには、『Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager, Version 7.0』の「System Management」の章を参照してください。

パッチのアンインストール

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

アンインストールに対応するパッチ

特定のパッチをアンインストールすると、アンインストールが成功した場合でも、問題が発生する可能性があります。次のような問題があります。

- アンインストール後に設定変更を展開できない
- オペレーティングシステムと ソフトウェアの間に互換性がなくなる
- セキュリティ認定コンプライアンスが有効な状態（CC/UCAPLモード）でそのパッチが適用されていた場合、アプライアンスの再起動時に FSIC（ファイル システム整合性チェック）が失敗する

⚠

注意 セキュリティ認定の遵守が有効な場合にFSICが失敗すると、ソフトウェアは起動せず、リモート SSH アクセスが無効になるため、ローカルコンソールを介してのみアプライアンスにアクセスできます。この問題が発生した場合は、Cisco TACにお問い合わせください。

アンインストールに対応したバージョン 7.0 のパッチ

現在、すべてのバージョン 7.0 パッチがアンインストールに対応しています。

高可用性/拡張性のアンインストール順序

高可用性/拡張性の展開では、一度に 1 つのアプライアンスからアンインストールすることで中断を最小限に抑えます。アップグレードとは異なり、システムはこの操作を行いません。次に移る前に、パッチが 1 つのユニットから完全にアンインストールされるまで待ちます。

表 *50 : FMC* 高可用性のアンインストール順序

設定	アンインストール順序
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 *51 : FTD* 高可用性およびクラスタのアンインストール順序

設定	アンインストール順序
FTD ハイ アベイラビリティ	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。
FTD クラスタ	一度に1つのユニットからアンインストールし、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 *52 : ASA* フェールオーバーペア/クラスタ内の *ASA with FirePOWER Services* のアンインストール順序

設定	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。

設定	アンインストール順序
ASA FirePOWER が有効な ASA アクティブ/アクティブ フェールオーバー ペア	アンインストールしないユニットの両方のフェールオーバー グループをアクティブにします。 **1.** プライマリ ASA デバイスの両方のフェールオーバー グループをアクティブにします。 **2.** セカンダリ ASA デバイスの ASA FirePOWER モジュールからアンインストールします。 **3.** セカンダリ ASA デバイスの両方のフェールオーバー グループをアクティブにします。 **4.** プライマリ ASA デバイスの ASA FirePOWER モジュールからアンインストールします。
ASA FirePOWER が有効な ASA クラスタ	アンインストールの前に、各ユニットでクラスタリングを無効にします。一度に1つのユニットからアンインストールし、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。

スタンドアロン FMC パッチのアンインストール

FMC パッチのアンインストールには Web インターフェイスを使用することをお勧めします。Web インターフェイスを使用できない場合は、Linux シェルを、シェルの `admin` ユーザーまたはシェル アクセス権を持つ外部ユーザーのどちらかとして 使用できます。シェルアクセスを無効にした場合は、 ロックダウンを元に戻すために Cisco TAC にご連絡ください。

⚠

注意 アンインストール中に設定の変更を行ったり、展開したりしないでください。システムが非アクティブに見えても、進行中のアンインストールを手動で再起動、シャットダウン、または再起動しないでください。システムが使用できない状態になり、再イメージ化が必要になる場合があります。アンインストールに失敗する、アプライアンスが応答しないなど、アンインストールで問題が発生した場合には、Cisco TAC にお問い合わせください。

始める前に

- アンインストールによってFMCのパッチレベルが管理対象デバイスより低くなる場合は、最初にデバイスからパッチをアンインストールします。
- 正常に展開され、通信が確立されていることを確認します。

ステップ 1 構成が古い管理対象デバイスに展開します。

アンインストールする前に展開すると、失敗する可能性が減少します。

ステップ 2 [利用可能なアップデート（Available Updates）] で該当するアンインストールパッケージの横にある [インストール（Install）] アイコンをクリックして、FMC を選択します。

パッチのアンインストーラには、アップグレードパッケージと同様に名前が付けられていますが、ファイル名には `Patch` ではなく `Patch_Uninstaller` が含まれています。FMC にパッチを適用すると、そのパッチ用のアンインストーラが自動的に作成されます。アンインストーラがない場合は、Cisco TAC までお問い合わせください。

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

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

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

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

ステップ 5 管理対象デバイスに構成を再展開します。

高可用性 FMC パッチのアンインストール

FMC パッチのアンインストールには Web インターフェイスを使用することをお勧めします。Web インターフェイスを使用できない場合は、Linux シェルを、シェルの `admin` ユーザーまたはシェル アクセス権を持つ外部ユーザーのどちらかとして 使用できます。シェルアクセスを無効にした場合は、 ロックダウンを元に戻すために Cisco TAC にご連絡ください。

高可用性ピアから一度に1つずつアンインストールします。同期を一時停止した状態で、先にスタンバイからアンインストールし、次にアクティブからアンインストールします。スタンバ

イでアンインストールが開始されると、ステータスがスタンバイからアクティブに切り替わり、両方のピアがアクティブになります。この一時的な状態のことを「スプリットブレイン」と呼び、アップグレード中とアンインストール中を除き、サポートされていません。

注意 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。アンインストール中に設定の変更を行ったり、展開したりしないでください。システムが非アクティブに見えても、進行中のアンインストールを手動で再起動、シャットダウン、または再起動しないでください。システムが使用できない状態になり、再イメージ化が必要になる場合があります。アンインストールに失敗する、アプライアンスが応答しないなど、アンインストールで問題が発生した場合には、Cisco TAC にお問い合わせください。

始める前に

- アンインストールによってFMCのパッチレベルが管理対象デバイスより低くなる場合は、最初にデバイスからパッチをアンインストールします。
- 正常に展開され、通信が確立されていることを確認します。

ステップ 1 アクティブな 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 アクティブ状態の FMC で、同期を一時停止します。

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

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

「スタンドアロンFMCパッチのアンインストール （100ページ）」の手順に従います。ただし、初期の展開は省略し、各ピアでアンインストールが成功したことを確認したら停止します。要約すると、各ピアで次の手順を実行します。

a) [システム（System）] > [更新（Updates）] ページで、パッチをアンインストールします。
b) ログアウトするまで進行状況を確認し、ログインできる状態になったら再びログインします。
c) アンインストールが成功したことを確認します。

ステップ 4 アクティブ ピアにする 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 5 管理対象デバイスに構成を再展開します。

FMC によるデバイスパッチのアンインストール

Linux シェル（エキスパートモード）を使用してデバイスパッチをアンインストールします。デバイスの admin ユーザーとして、またはCLI設定アクセス権を持つ別のローカル ユーザーとして、デバイス シェルにアクセスできる必要があります。FMC ユーザーアカウントは使用できません。シェルアクセスを無効にした場合は、 ロックダウンを元に戻すために Cisco TAC にご連絡ください。

⚠

注意 アンインストール中に設定の変更を行ったり、展開したりしないでください。システムが非アクティブに見えても、進行中のアンインストールを手動で再起動、シャットダウン、または再起動しないでください。システムが使用できない状態になり、再イメージ化が必要になる場合があります。アンインストールに失敗する、アプライアンスが応答しないなど、アンインストールで問題が発生した場合には、Cisco TAC にお問い合わせください。

始める前に

- FTD高可用性ペアを解除します。その他の高可用性や拡張性の展開では、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（「高可用性/拡張性のアンインストール順序 （98 ページ）」を参照）。
- 正常に展開され、通信が確立されていることを確認します。

ステップ 1 デバイスの設定が古い場合は、この時点で 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。展開とその他の必須のタスクが完了していることを確認してください。アンインストールの開始時に実行中だったタスクは停止され、失敗したタスクとなって再開できなくなります。後で失敗ステータス メッセージを手動で削除できます。

例外：複数のバージョンが構成されているクラスタや高可用性ペアには展開しないでください。高可用性や拡張性の展開では、最初のユニットからアンインストールする前に展開しますが、すべてのユニットからパッチをアンインストールするまでは再度展開しないでください。

ステップ 2 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 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 3 `expert` コマンドを使用して Linux シェルにアクセスします。

ステップ 4 アップグレードディレクトリにアンインストールパッケージがあることを確認します。

```
ls /var/sf/updates
```

パッチのアンインストーラには、アップグレードパッケージと同様に名前が付けられていますが、ファイル名には `Patch` ではなく `Patch_Uninstaller` が含まれています。デバイスにパッチを適用すると、そのパッチ用のアンインストーラがアップグレードディレクトリに自動的に作成されます。アンインストーラがない場合は、Cisco TAC までお問い合わせください。

ステップ 5 uninstall コマンドを実行し、プロンプトが表示されたらパスワードを入力します。

```
sudo install_update.pl --detach /var/sf/updates/uninstaller_name
```

注意 確認を求められることはありません。このコマンドを入力すると、デバイスの再起動を含むアンインストールが開始されます。アンインストール時のトラフィック フローとインスペクションの中断は、アップグレード時に発生する中断と同じです。準備が整っていることを確認してください。`--detach` オプションを使用すると、SSH セッションがタイムアウトした場合にアンインストールプロセスが強制終了されなくなり、デバイスが不安定な状態になる可能性があることに注意してください。

ステップ 6 ログアウトするまでアンインストールを監視します。

個別のアンインストールの場合は、`tail` か `tailf` を使用してログを表示します。

- FTD：`tail /ngfw/var/log/sf/update.status`
- ASA FirePOWER および NGIPSv：`tail /var/log/sf/update.status`

それ以外の場合は、コンソールか端末で進行状況を監視します。

ステップ 7 アンインストールが成功したことを確認します。

アンインストールが完了したら、デバイスのソフトウェアバージョンが正しいことを確認します。FMC で、[デバイス（Devices）] > [デバイス管理（Device Management）] の順に選択します。

ステップ 8 構成を再展開します。

例外：複数のバージョンが構成されているクラスタや高可用性ペアには展開しないでください。展開は、すべてのユニットでこの手順を繰り返した後にのみ行います。

次のタスク

高可用性や拡張性の展開では、各ユニットに対し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。次に例を示します。

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

ASDM による ASA FirePOWER パッチのアンインストール

Linux シェル（エキスパートモード）を使用してデバイスパッチをアンインストールします。デバイスの `admin` ユーザーとして、または CLI 設定アクセス権を持つ別のローカル ユーザーとして、デバイス シェルにアクセスできる必要があります。シェルアクセスを無効にした場合は、 ロックダウンを元に戻すために Cisco TAC にご連絡ください。

注意 アンインストール中に設定の変更を行ったり、展開したりしないでください。システムが非アクティブに見えても、進行中のアンインストールを手動で再起動、シャットダウン、または再起動しないでください。システムが使用できない状態になり、再イメージ化が必要になる場合があります。アンインストールに失敗する、アプライアンスが応答しないなど、アンインストールで問題が発生した場合には、Cisco TAC にお問い合わせください。

始める前に

- ASA のフェールオーバーやクラスタの展開では、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（「高可用性/拡張性のアンインストール順序（98 ページ）」を参照）。
- 正常に展開され、通信が確立されていることを確認します。

ステップ 1 デバイスの設定が古い場合は、この時点で 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。展開とその他の必須のタスクが完了していることを確認してください。アンインストールの開始時に実行中だったタスクは停止され、失敗したタスクとなって再開できなくなります。後で失敗ステータス メッセージを手動で削除できます。

ステップ 2 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 3 `expert` コマンドを使用して Linux シェルにアクセスします。

ステップ 4 アップグレードディレクトリにアンインストールパッケージがあることを確認します。

```
ls /var/sf/updates
```

パッチのアンインストーラには、アップグレードパッケージと同様に名前が付けられていますが、ファイル名には `Patch` ではなく `Patch_Uninstaller` が含まれています。デバイスにパッチを適用すると、そ

のパッチ用のアンインストーラがアップグレードディレクトリに自動的に作成されます。アンインストーラがない場合は、Cisco TAC までお問い合わせください。

ステップ 5 uninstall コマンドを実行し、プロンプトが表示されたらパスワードを入力します。

```
sudo install_update.pl --detach /var/sf/updates/uninstaller_name
```

注意 確認を求められることはありません。このコマンドを入力すると、デバイスの再起動を含むアンインストールが開始されます。アンインストール時のトラフィック フローとインスペクションの中断は、アップグレード時に発生する中断と同じです。準備が整っていることを確認してください。`--detach` オプションを使用すると、SSH セッションがタイムアウトした場合にアンインストールプロセスが強制終了されなくなり、デバイスが不安定な状態になる可能性があることに注意してください。

ステップ 6 ログアウトするまでアンインストールを監視します。

個別のアンインストールの場合は、`tail` か `tailf` を使用してログを表示します。

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

それ以外の場合は、コンソールか端末で進行状況を監視します。

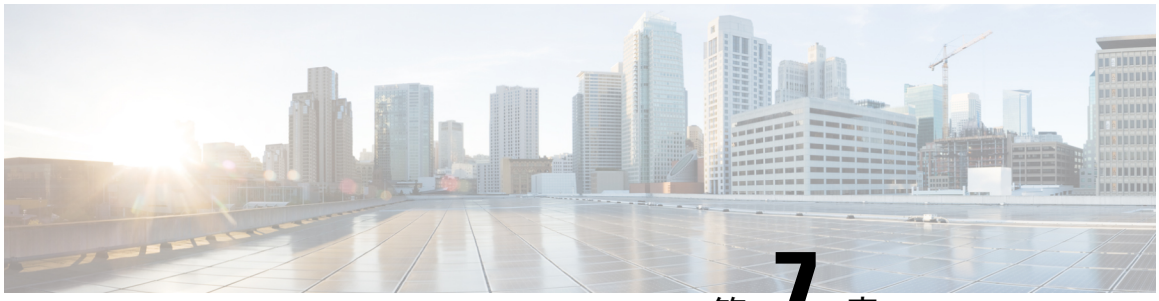
ステップ 7 アンインストールが成功したことを確認します。

アンインストールが完了したら、モジュールのソフトウェアバージョンが正しいことを確認します。[設定（Configuration）] > [ASA FirePOWERの設定（ASA FirePOWER Configuration）] > [デバイス管理（Device Management）] > [デバイス（Device）] の順に選択します。

ステップ 8 構成を再展開します。

次のタスク

ASA のフェールオーバーやクラスタの展開では、各ユニットに対して計画した順序でこの手順を繰り返します。



第 7 章

未解決のバグおよび解決されたバグ

利便性を考え、このドキュメントには未解決のバグと解決済みのバグの一覧を記載しています。

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。メンテナンスリリースまたはパッチの未解決のバグも記載していません。サポート契約がある場合は、Cisco バグ検索ツールを使用して最新のバグリストを取得できます。

Version7.0 で未解決のバグ

メンテナンスリリースまたはパッチの未解決のバグは記載していません。最新のバグリストについては、Cisco バグ検索ツールを使用してください。

バージョン 7.0.0 で未解決のバグ

表 *53* : バージョン *7.0.0* で未解決のバグ

不具合 ID	タイトル
CSCvr74863	CIP-Multiservice が間違ったサービス属性を表示する
CSCvx21050	Snort3 UDP のパフォーマンスが Snort2 と比較して最大 50% 低下する
CSCvx25425	Snort3 SSL：復号化されていないセッションからのチケットが、後続ポリシー決定のためにキャッシュされない
CSCvx30175	Snort3：TCP フラグを閉じている SMTP が正しく伝搬されない

不具合 ID	タイトル
CSCvx63788	AC ポリシーのデフォルトアクションの新しいウィンドウでポリシーを編集すると、IPS ポリシーにエラーのポップアップが表示される
CSCvx64252	イニシエータの FQDN オブジェクト検索を使用すると、イベント検索エラーが発生する
CSCvx67856	FTD7.0：システムでアングレースフルリブートが発生すると、Prometheus プロセスが起動しない
CSCvx89720	7.0.0 へのアップグレード後に、RA VPN ユーザーを対象にしたユーザーベースのアクセス制御ルールが期待どおりに適用されない場合がある
CSCvx96452	ペイロード伝送の完了後、一部の HTTP2 TLS トラフィックが TCP FIN ではなく TCP RST で終了する
CSCvx96452	Snort3：リセットしてブロックの SSL ルールに一致するトラフィックに対して、接続イベントに許可アクションが散発的に表示される
CSCvx99179	FDM-VMware：6.5 以降から 7.0/7.1 へのアップグレード中の nikita-incremen コア
CSCvy00329	特定の FTP フローでホスト属性テーブルが正しく更新されない
CSCvy02879	FDM ISA 3000 の HA がアクティブ-アクティブ状態になる
CSCvy07113	7.0.0-1459：QP プラットフォームに固有のファイルポリシー設定で FTP トラフィック（マルウェアファイル）がブロックされない
CSCvy13572	7.0：6.7 で使用されている LSP バージョンにダウングレードすると、展開に失敗する
CSCvy19415	FTD HA を切り替えると（セカンダリ、アクティブ）、syslog メッセージでプライマリデバイス名が送信される
CSCvy26742	7.0.0-62 KVM vFTD に 1K ルールをアップロードすると展開に失敗する
CSCvy27261	Snort2 および Snort3 のイベントビューには、より明確化するための機能拡張が必要
CSCvy31096	Snort 設定がリロードされた場合にホストが再検出される
CSCvy32550	ルールが GID 2000 で構築されていないため、Snort3 カスタムルールメッセージの相関フィルタリングに失敗する
CSCvy33696	スタンバイ インスペクション エンジンの Snort 障害が原因で FDM KVM-HA の解除に失敗する
CSCvy35352	特定の条件下で抑制設定のエラー処理が必要になる

不具合 ID	タイトル
CSCvy38070	テーブルチャートの日付がX軸で、件数がY軸の場合、ファイル/マルウェアイベントのレポートで障害が発生する
CSCvy39840	SI TALOS フィードの更新がルールファイルと同期されない
CSCvy43483	Snort 切り替えで、Snort 2 に切り替えるのに時間がかかることがある
CSCvy43740	vFDM ISA HA セキュリティ インテリジェンス フィードの更新で java.lang.NullPoin がスローされる
CSCvy44701	Snort 3 HTTP/2 インスペクタのバージョン 7.0 FMC オンラインヘルプに、誤ったコンテンツが含まれる
CSCvy48764	公開キー認証による SSH アクセスにはユーザーパスワードが必要
CSCwa16654	Firepower リリース 7.0.x が Snort 3 の ssl_state や ssl_version キーワードをサポートしていない

解決済みのバグ Version7.0

バージョン 7.0.3 で解決済みのバグ

表 *54* : バージョン *7.0.3* で解決済みのバグ

不具合 ID	タイトル
CSCwa65014	7.2 FMC イベンティングに対するクラウド管理型の 7.0.3 デバイスのサポート
CSCwa75204	どの SSL ルールでも SNORT3 Certsize 16k トラフィックが 2100 で失敗する
CSCwa98690	AWS FTDv AutoScale_layer.zip ファイルで脆弱な pycrypto 2.x ツールキットが使用されている
CSCwb93932	タイマー サービス アサーションによる ASA/FTD のトレースバックとリロード

バージョン 7.0.2.1 で解決済みのバグ

表 *55* : バージョン *7.0.2.1* で解決済みのバグ

不具合 ID	タイトル
CSCwb93932	タイマー サービス アサーションによる ASA/FTD のトレースバックとリロード

バージョン 7.0.2 で解決済みのバグ

表 *56* : バージョン *7.0.2* で解決済みのバグ

不具合 ID	タイトル
CSCvt68055	snmpd が FP21xx デバイスの FXOS で頻繁に再生成される
CSCvy82668	SSH セッションが解放されません
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
CSCvt15348	マルチコアプラットフォームで ASA show processes cpu-usage output が誤解を招く
CSCvy72841	Firepower 1K FTD が eth2 インターフェイスの内部 MAC アドレスを使用して LLDP パケットを送信する
CSCvz80981	バージョン 7.0 を実行している SFR モジュールで SNMPv3 が機能しない
CSCvy08351	侵入および相関の電子メールアラートがメールサーバーに送信されなくなる
CSCvz66474	snmpd コアファイルが FTD で生成される
CSCvx75683	「show cluster info trace」の出力が「タグが存在しません」というメッセージにより負担がかかっています
CSCvz25434	BVI が DHCP クライアントとして設定されている場合、1550 ブロックの枯渇が原因で ASA および FTD がトラフィックをブラックホールする
CSCwa45799	bcm_usd プロセスが原因で FXOS の CPU 使用率が高くなる
CSCwa18889	マルチインスタンスで Lina と FXOS 間でクロックドリフトが観察された
CSCvy99217	IKEv2: SA エラーコードは、ユーザーにわかりやすいように理由を変換する必要があります
CSCvz00961	ASA の切り捨てられた/破損した設定に関連する AnyConnect 接続の障害

不具合 ID	タイトル
CSCvz36905	V ルートと同じ v6 ルートを追加すると、重複したエントリが作成される
CSCwa58060	updates-talos.sco.cisco.com から ICMP 応答が受信されない場合、LSP のダウンロードが失敗する
CSCvz03524	sha1 ではなく sha256 リクエストが原因で PKI の「OCSP 失効チェック」が失敗する
CSCwa74900	debug webvpn cifs 255 を有効にした後トレースバックとリロードが発生
CSCvz29233	ASA：システムコンテキストでインターフェイスのフラップが発生したときに、カスタムコンテキストからの ARP エントリが削除されない
CSCvy35416	並列展開が異なる子ドメインに対してトリガーされると、グローバルドメインからの展開に失敗する
CSCvy99218	更新に失敗した場合、VDB バージョンが更新されてはいけない
CSCvz81888	asa-9.14.3 から asa-9.15.1/9.16.1.28 にアップグレードした後、NTP が *（同期）ステータスに変更されない
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
CSCvz75988	RFC5424 が有効な場合、一貫性のないロギングタイムスタンプが起こる
CSCvz52199	ASA VPN ロードバランシング アルゴリズムの精度が上がる
CSCvz48407	スレッド名 DATAPATH-15-18621 でのトレースバックおよびリロード
CSCvz05687	DND フローのフラグメント化された証明書の要求に失敗
CSCwa96759	Lina は tcpmod_proxy_handle_mixed_mode でトレースバックしてリロードする場合がある
CSCvz90722	暗号 ACL のオブジェクトグループでは、hitcnt の合計が個々の要素と一致しない
CSCvz59950	KP-FPR2130 のスケーリングの長時間テストで IKEv2 がクラッシュする
CSCvz38332	FTD または ASA - 9.14.2.15 から 9.14.3 へのアップグレード後にブートループでスタックする
CSCvz55140	CCM レイヤ（スプリント 117、シーケンス 17）での WR6、WR8 および LTS18 コミット ID の更新
CSCwa58686	OGS コンパイル動作における ASA および FTD の変更によりブートループが発生する

不具合 ID	タイトル
CSCvz43455	hostscan のアップグレード中に ASAv がトレースバックを確認する
CSCvz20679	FTDv - Lina のトレースバックおよびリロード
CSCvz60578	MASTER_POST_CONFIG 状態のクラスタユニットは、一定期間後に無効状態に移行する必要がある
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
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
CSCvz79930	Snort3.dmp および crashinfo ファイルがディスクマネージャによって管理されない
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
CSCwa19713	asp ドロップタイプ「no-adjacency」の原因により BVI インターフェイスで設定された ASA によってトラフィックがドロップした
CSCvz70958	dhcpp_add_ipl_stby によるスタンバイの高いコントロールプレーン CPU
CSCvz61689	ソフトウェアのアップグレード後にポートチャネルメンバーインターフェイスが失われ、ダウン状態になる
CSCvz92016	Cisco ASA および FTD ソフトウェアの Web サービスインターフェイスにおける権限昇格の脆弱性
CSCvz34831	ASA が DACL のダウンロードに失敗した場合、試行を停止しない
CSCvz90375	起動時の ASA 9.14 の使用可能な DMA メモリが不足し、サポートされる AnyConnect セッションが減少
CSCvy40401	ipsec 構成で NULL 暗号化を使用すると、L2L VPN セッションの起動が失敗する
CSCwa76822	syslog-ng 宛先のスロットリングフロー制御が調整される
CSCvz33468	ASA/FTD：手動 NAT ルールでオブジェクトグループを変更した後、NAT は送信元アドレスの変換を停止
CSCwa11186	AAA LDAP デバッグで機密情報がマスクされる
CSCvz00383	スレッド名 Checkheaps で FTD lina トレースバックとリロードが発生する
CSCvy17030	FMC の接続イベントページに「エラー：このクエリを処理できません。サポートに問い合わせてください。」と表示される

不具合 ID	タイトル
CSCvx97053	異なるコンテキストで同じインターフェイスとネットワークに ipv6 アドレス/プレフィックスを設定できません
CSCvx24470	FTD/FDM：RA VPN のカスタム ポートが設定されている場合、展開のたびに RA VPN セッションが切断される
CSCwa05385	CCM レイヤ（スプリント 124、シーケンス 19）での WR6、WR8 および LTS18 コミット ID の更新
CSCvz96440	FMC で NGIPS デバイスのアーカイブが作成されないようにする必要がある
CSCwa68660	ASA を 9.12.4.x にアップグレードした後、FTP インスペクションが正しく機能しなくなる
CSCvy98027	FXOS で物理インターフェイスが動作しているのにアプリケーションインターフェイスがダウンする
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
CSCvz73146	FTD：スレッド名 DATAPATH でのトレースバック
CSCwa87597	ASA/FTD フェールオーバー：アクティブメイトから設定レプリケーションを受信すると、スタンバイリブートする
CSCwb01919	FP2140 ASA 9.16.2 HA ユニットが lua_getinfo（getfuncname）でトレースバックおよびリロードする
CSCvy96895	フェールオーバー後、ASA がアクティブ IP アドレスとスタンバイ MAC アドレスを使用して VTY セッションを切断します
CSCwa55878	FTD サービスモジュールの障害：「ND がダウンした可能性があります」という誤ったアラーム
CSCwa14725	IKE デーモンスレッドでの ASA および FTD のトレースバックとリロード
CSCvy35737	Anyconnect パッケージの検証中に FTD のトレースバックとリロードが発生する
CSCvz91218	高速トラフィックでのインターフェイスリングのドロップにより、スタンバイユニットで Statelink hello メッセージがドロップした
CSCwa20758	CCM レイヤ（スプリント 124、シーケンス 20）での WR6、WR8 および LTS18 コミット ID の更新
CSCwa67882	オフロードされた GRE トンネルは、サイレントにオフロードを解除し、CPU にパントされる場合がある

不具合 ID	タイトル
CSCwa67884	条件付きフローオフロードデバッグで出力が生成されない
CSCwa97784	ASA：ジャンボサイズのパケットが L2TP トンネル上でフラグメント化されない
CSCwa29956	FTD のアップグレード後に「デバイスでインターフェイスの設定が変更されました」というメッセージが表示される場合がある
CSCwa60574	snp_ha_trans_alloc_msg_muxbuf_space 関数での ASA のトレースバックとリロード
CSCwa89243	9.15.1.17 にアップグレードした後、SNMP はポーリングに応答しなくなった
CSCvz30582	Cisco Firepower Management Center のクロスサイト スクリプティングの脆弱性
CSCwa04461	Cisco ASA ソフトウェアおよび FTD ソフトウェアリモートアクセスの SSL VPN サービス拒否
CSCwa30114	オブジェクトサービスでポートの範囲を使用する場合「NAT がポートを予約できません」というエラーが発生
CSCvy80030	ENH：「show tech」出力に「show coredump filesystem」を追加
CSCwa39680	SSL 復号のデバッグを有効にすると、Snort がパケット処理を停止する（Snort2）
CSCvy96803	プロセス名「lina」または「snmp_alarm_thread」で ASA/FTD のトレースバックとリロードが発生する
CSCvz34149	/opt/cisco/platfom/logs/var/log/messages の新しい保存先の更新
CSCvo77184	VMware ASAv は、e1000 ではなく vmxnet3 にデフォルト設定する必要があります
CSCvx92932	SFDataCorrelator プロセス終了が原因で、FMC にイベントがない
CSCwa79980	FPR の SNMP get コマンドは、インターフェイスインデックスを表示しない
CSCvz38976	7.1/Firepower Threat Defense デバイスが大規模なパケットを転送できないことがある/フラグメント化の失敗
CSCvz64470	ICMP 到達不能メッセージ生成時のメモリ破損による ASA および FTD のトレースバックとリロード
CSCwb34035	SNMP の設定中に ASA CLI がランダムにハングする

不具合 ID	タイトル
CSCvz00032	Cisco Firepower Threat Defense ソフトウェアの TCP Proxy DoS 攻撃に対する脆弱性
CSCvu23149	データベーステーブル rule_opts の SID_GID_ORD インデックスの破損が原因で、FMC でバックアップの生成に失敗する
CSCwa57115	オブジェクトで存在しない ACL を削除した後、新しいアクセスリストが有効にならない
CSCvz37306	既存のユーザーで複数のコンテキストスイッチを実行した後、ASDM セッションが新しいユーザーに提供されない
CSCwa53489	ハッシュテーブルへのアクセス中に無効なメモリアクセスにより Lina トレースバックとリロードが発生
CSCvy98458	FP21xx のトレースバック「Panic:DATAPATH-10-xxxx -remove_mem_from_head: Error - found a bad header」
CSCvy52924	FTD がリブート時にすべての VRF インスタンスの OSPF ネットワークステートメント設定を失う
CSCvz92932	ASA show tech の実行により、CPU でスパイクが発生し、IKEv2 セッションに影響を与える
CSCvz44339	FTD：ngfw-interface および host-group を使用して SNMP ホストを削除しようとすると、展開が失敗する
CSCwa40223	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
CSCvy47108	UAuth エントリがスタックしているため、リモートアクセス IKEv2 VPN セッションを確立できない
CSCvy86780	エラーにより LSP のインストールを完了できない再度実行してください。（Please try again.）」
CSCvz57710	conf t が、context-config モードで disk0:/t に変換される
CSCvz14377	MySQL DB と EO から管理者とその他のユーザーが失われる
CSCvz89126	マルチ コンテキスト スイッチオーバーが ASDM から実行される場合の ASA での ASDM セッション/クォータカウントが不一致である
CSCvy78209	Snort が高 CPU 使用率アラートを示すが、top.log には高 CPU 使用率が示されない
CSCwa19443	フローオフロード - 比較状態の値が長期間エラー状態のままになる

不具合 ID	タイトル
CSCvy91668	スティッキネストラフィックによる PAT プールの枯渇は、新しい接続のドロップにつながる可能性があります。
CSCwa70008	期限切れの証明書により、セキュリティインテリジェンスの更新が失敗する
CSCvz81480	IPsec で GCM が 使用されている場合、アウトバウンドパケットの IV が Nitrox V プラットフォームで更新されない
CSCvx70480	ポリシーにアクセスすると 403 エラーが発生 -> FMC（4600）から FMCv にユーザーロールをエクスポートした後のアクセス制御
CSCwa18795	Scaled AC-SSL TVM プロファイルテストの「スレッド：Unicorn Proxy Thread CPU：7 watchdog_cycles」でクラッシュする
CSCvz67816	FTD で変更される IPV6 DNS PTR クエリ
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
CSCvs85607	ログパーティションが一杯になると FXOS ログインが中断する
CSCwb18252	FTD/ASA：BFD 機能のトレースバックにより予期しないリブートを引き起こす
CSCvz02076	Snort のリロードがタイムアウトして再起動する
CSCvz44645	FTDは、スレッド名 'lina' でトレースバックおよびリロードする場合がある
CSCwa79676	HA 印刷の FPR1010 で複数のインターフェイスのブロードキャスト ストーム アラートが発生する
CSCvy24921	SNMPv3：構成が変更されるたびに SNMP EngineID が変更される
CSCvz36933	ポリシーの展開時にセンサーの SNMP プロセスが再起動することがある
CSCvz86796	CMPV2 登録時にスレッド CMP でクラッシュする
CSCvz70316	LINA はトレースバックとリロードを生成する可能性がある
CSCwa60300	axios 0.21.1
CSCvy30392	テーブル ids_event_msg_map の破損した int_id インデックスが原因で、FMC でのバックアップ生成に失敗する
CSCvz55849	LINA プロセスでの FTD のトレースバックとリロード
CSCvz61160	ICMP エラーメッセージを処理する際、DATAPATH で ASA がトレースバックする

不具合 ID	タイトル
CSCvx43150	FMC で、RMA 後のメンバーデバイスの登録プロセスが失敗する
CSCwa91090	AnyConnect TLSv1.2 セッション確立中に SSL ハンドシェイクログから不明なセッションが表示される
CSCvz43848	TID ソースが解析状態でスタックする
CSCvz61767	SNMPv2 または SNMPv1 が設定されたポリシーが展開されない
CSCvz69571	anyconnect セッションが終了した後、ASA ログに転送されたデータの間違った値が表示される
CSCwa51862	プロキシを使用すると LSP ダウンロードが実行されない
CSCwa31373	ルールをコピーすると、FMC 6.6.5 で重複する ACP ルールが生成される
CSCwa65389	ASDM を介してインターフェイス設定を変更する場合は、Unicorn Admin Handler で ASA トレースバックおよびリロードが発生
CSCwa32286	CCM レイヤ（スプリント 125、シーケンス 21）での WR6、WR8 および LTS18 コミット ID の更新
CSCwa08262	マッピングされたグループポリシーを持つ AnyConnect ユーザーは、トンネルグループの下にあるデフォルト GP から属性を取得します
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
CSCwa36678	FMC からの展開中にトレースバックを使用してランダム FTD がリロードされる
CSCvz50712	TLS サーバー検出は、AnyConnect 展開のプローブに誤った送信元 IP アドレスを使用
CSCwa41918	SSL インスペクションで、証明書を削除するときに予期しない動作が発生する場合がある
CSCwa36672	ASDM を使用してキャプチャを実行するとき ASA on FPR4100 のトレースバックとリロード
CSCvz64548	デバイス上の SFTunnel がイベントメッセージを処理しない
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
CSCvy43002	SNMPWalk + S2S-IKEv2 および AnyConnect TVM プロファイルの実行中にクラッシュを検出
CSCwa46963	セキュリティ：CVE-2021-44228 → Log4j 2 における脆弱性

不具合 ID	タイトル
CSCvy74984	デフォルトの外部ルートが使用されると、Azure 上の ASAv がメタデータサーバーへの接続を失う
CSCvv36788	MsgLayer[PID]：エラー：Msglyr::ZMQWrapper::registerSender()：ZeroMQ ソケットのバインドに失敗した
CSCvy97080	SMB トラフィックの処理中に Snort3 が予期せず再起動する
CSCwa67145	AD でグループの 1 つが削除されると、レルムのダウンロードが実行されない
CSCvz77744	OSPFv3：FTD の間違った「転送アドレス」が ospfv3 データベースに追加される
CSCvz17923	ディスパッチャは、特定の条件下で保留中の非同期ロックを考慮しないため、CPU ユーティリティが低下
CSCvx67851	ISA3000 の FDM 上の PLR
CSCwa56449	HTTP cli EXEC コードでの ASA トレースバック
CSCvz77662	スケーリングされた AC-SSL TVM プロファイルテストのデータパスでクラッシュする
CSCwb09219	ASA/FTD：「署名者証明書が見つかりません」が原因で、アップグレード後に OCSP が機能しない場合がある
CSCvz84850	「タイマーサービス」機能により、ASA および FTD のトレースバックとリロードが発生する
CSCwa42594	ASA：GTP ヘッダーに SEQ および EXT フィールドがある場合、IP ヘッダーチェックの検証に失敗する
CSCwa40312	スタンバイ ASA ユニットで間違った IPv6 メッセージが表示される
CSCwa88571	スマートポータルを使用して FMC を登録できない
CSCvk62945	ASA：「Syslog 317007 が見つからない」というエラーを受信
CSCvz38692	snmp_master_callback_thread での ASAv のトレースバックとリロード
CSCwa50145	FPR8000 センサーの UI ログインにより、基本的な権限を持つシェルユーザーが作成される
CSCvz08387	ASP ドロップキャプチャ出力に誤ったドロップ理由が表示される場合がある
CSCvy35352	特定の条件下で抑制設定のエラー処理が必要になる

不具合 ID	タイトル
CSCvy69453	WM スタンバイデバイスは、再起動後にコールドスタートトラップを送信しません
CSCwa02929	FTD が SSL フローエラーの CORRUPT_MESSAGE でトラフィックをブロックする
CSCvz89545	アップグレード後の SSL VPN のパフォーマンスの低下と重大な安定性に関する問題
CSCvz24765	snmpd コアで再起動したデバイス
CSCvz07614	ASA：孤立した SSH セッションでは、CLI からポリシーマップを削除できない
CSCvy40482	9.14MR3：snmpwalk が [Errno 146] の接続拒否エラーで失敗した
CSCvz02425	ポリシー名の読み取り中に NPE が原因で展開に失敗する
CSCvz28103	FDM で DHCP リレー設定を保存すると、flex-config/smart CLI エラーが発生する
CSCvz01604	CSCvx82503 で修正プログラムが導入されたにもかかわらず、100K CPS レートで DDoS をテストすると、ASA が高い CPU 使用率（100%）になる
CSCvu96436	特定のロックが長時間競合した場合のマスターと 1 つのスレーブのトレースバック
CSCvy79952	ダウングレード後の ASA/FTD トレースバックとリロード
CSCvx80830	Radius サーバーが dACL を送信し、vpn-simultaneous-logins が 1 に設定されていると、同じユーザーからの VPN 接続が失敗する
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
CSCvy64911	デバッグ：crasLocalAddress の SNMP MIB 値に IP アドレスが表示されない
CSCwa68805	HA 作成中に FTD のトレースバックとリロードが発生
CSCvz71064	ikev2 トンネルで約 2 分かかる ASA からのコンテキストを削除します
CSCvz40352	アクセスリストに明確なルールが存在するにもかかわらず、暗黙の ACL によって ASA トラフィックがドロップする
CSCvz86256	プライマリ ASA は、スプリットブレインが検出され、ピアがコールドスタンバイになるとすぐに GARP を送信する必要がある
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

不具合 ID	タイトル
CSCvz72771	ASA/FTD が、スタックトレースの「c_assert_cond_terminate」でトレースバックおよびリロードする場合がある
CSCvw37191	再起動後に FXOS SNMPv3 エンジンの ID が変更される
CSCwa34287	ASA：アップグレード後のリロード後に NTP 同期が失われる
CSCvz83432	CCM レイヤ（スプリント 121、シーケンス 18）での WR6、WR8 および LTS18 コミット ID の更新
CSCwa31508	QW-4145 デバイスで継続的に展開に失敗する
CSCvz81342	Diskmanager が AMP ファイルのキャプチャファイルをプルーニングしない
CSCvy60831	ASA および FTD メモリブロックの位置がデータパスでの断片化されたパケットに対して更新されない
CSCvz67003	ASDM セッション数とクォータ管理の数が一致しない ASDM の「ロスト接続ファイアウォール」メッセージ
CSCvz67001	リモート SSH ストレージターゲットへの FMC イベントバックアップが失敗する
CSCvz47709	[IMS_7_1_0] アップグレード FMC 7.1.0 での DeployACPolicyPostUpgrade（2022）
CSCvz23157	show コマンドが発行されると SNMP エージェントが再起動する
CSCwa96327	ポートチャネルメンバーであるインターフェイスの ifHighSpeed 値が正しくない
CSCvw29647	FTD：NAS-IP-Address:0.0.0.0 が Radius 要求パケットで aaa-server のネットワークインターフェイスとして定義されていない
CSCvz61658	update_mem_reference の CPU ホグ
CSCvy78525	TCP ping の VRF ルートルックアップがない
CSCvz82562	ASA/FTD：サイト間 VPN：トラフィックが正しく断片化されていない
CSCvy56395	キー設定が存在する場合の SNMP 暗号化コミュニティストリングによる ASA トレースバックとリロード
CSCwa79494	スポークフラップからの IPSec トンネルの場合、トラフィックはハブで失敗し続ける
CSCvz88149	ブロック解放中に Lina のトレースバックとリロードにより、FTD ブートループが発生する

不具合 ID	タイトル
CSCvy89658	CCM レイヤ（スプリント 114、シーケンス 13）での WR6、WR8 および LTS18 コミット ID の更新
CSCvz38361	直接接続されていないネイバーのために BGP パケットがドロップされる
CSCvx14489	フェイルオーバー後に ipv6 インターフェイスで snmpwalk が失敗します
CSCwa90408	長時間のテストで SSH SCP でクラッシュが発生。
CSCvz58710	SCTP トラフィックにより ASA がトレースバックする。
CSCvy55439	頻繁な PDTS 読み取り/書き込みによる FTDv スループットの低下
CSCvy08972	イベントデータベースで utf8 エラーが発生し、イベントの処理が一時停止する
CSCwa35200	AnyConnect SSL の一部の syslog が、ユーザーコンテキストではなく管理コンテキストで生成される
CSCvi58484	クラスタ：別のクラスタユニットに応答が着信する場合は、外部 IP への FTD/ASA を送信元とする ping が失敗することがある
CSCvz30558	Cisco Firepower Management Center のクロスサイト スクリプティングの脆弱性
CSCwa69303	SSP プラットフォームで実行されている ASA で、重大なエラー「[FSM:FAILED]: sam:dme:MgmtIfSwMgmtOobIfConfig」が生成される
CSCwb42846	Snort インスタンスで CPU 使用率が 100% になりスタックする
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
CSCvz95108	デバイスでのメジャーバージョンの変更によるアップグレード後の FTD 展開の失敗
CSCwa38277	プールとして範囲が広い ASA NAT66 が IPv6 で機能しない
CSCvy33501	FDM フェールオーバーペア：新しく設定された sVTI IPSEC SA はスタンバイに同期されない。FDM は HA が同期していないことを示しています
CSCvy21334	「スイッチオーバーなし」の場合、アクティブは CoA アップデートをスタンバイに送信しようとする
CSCvz20544	Anyconnect プロファイルのループ処理で、ASA および FTD がトレースバックおよびリロードする場合がある
CSCvz61431	クラスタ構成の同期中に表示される「Netsnmp_update_ma_config: ERROR Failed to build req」メッセージ

不具合 ID	タイトル
CSCvv43190	GREヘッダープロトコルフィールドが内部IPヘッダーのプロトコルフィールドと一致しない場合の暗号エンジンエラー
CSCvy04430	管理セッションが数週間後に接続に失敗
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
CSCvy04343	PLR モードの ASA で「ライセンスのスマート予約」が失敗する。
CSCwa25033	セグメンテーション違反を引き起こす予期しない HTTP/2 データフレーム
CSCvz53884	SNMP OID HOST-RESOURCES-MIB（1.3.6.1.2.1.25）が FMC に存在しない
CSCwb01700	ASA：SSH と ASDM セッションが CLOSE_WAIT でスタックし、ASA の MGMT が不足する
CSCvz55395	トラフィックが存在する場合でも、設定されたアイドルタイムアウト後に TCP 接続がクリアされる
CSCvx36885	DATAPATH での ASA のリロードとトレースバック
CSCvz05468	最初の機能の有効化/展開としてプラットフォーム設定に複数の SSH ホストエントリがあると、LINA で SSH が切断される
CSCvz95949	FP1120 9.14.3：アクティブなデバイスの再起動後に一時的なスプリットブレインが発生
CSCvz65181	Cisco Firepower Threat Defense ソフトウェアの セキュリティインテリジェンスにおける DNS フィードバイパスの脆弱性
CSCwa98684	ポリシーの展開中にコンソールに過度の警告が発生
CSCvy10789	LDAP パスワードで FTD 2110 ASCII 文字を使用できない
CSCvz12494	FPR2100 では、電源オフ/オン後、FXOS のバージョンが ASA のバージョンと一致しない
CSCvz62578	ASDM の管理者ルールセクションで SFR モジュールの AC ルールを編集または移動できない
CSCwa26353	Snort3：LSP の更新後にポリシーがダーティにならない（カスタム侵入ポリシーのみが使用されている場合）
CSCvz55302	メモリ不足の状態での SSL null チェックによる FTD/ASA のトレースバックとリロード
CSCwa85043	トレースバッグ：ASA/FTD がスレッド名「Logger」でトレースバックおよびリロードする場合がある

不具合 ID	タイトル
CSCvz39646	ASA または AnyConnect - 古い RADIUS セッション
CSCwa13873	「failover active」コマンドの実行後に、状態遷移における遅延が原因により ASA フェールオーバー スプリット ブレインが発生
CSCvz85437	FXOS および FTD を 2.10.1.159 および 6.6.4 にアップグレードした後に FTD 25G、40G、および 100G のインターフェイスがダウンする
CSCvv48942	Snmpwalk がフェールオーバーインターフェイスのトラフィックカウンターを 0 として表示する
CSCvy74781	スタンバイデバイスが、フェールオーバー後に SSL トラフィックのキープアライブメッセージを送信する
CSCwa36661	ASP テーブル内にルートがないため、トラフィックがユーザー VRF の一部の出力インターフェイスにヒットしない
CSCvz69699	PxGrid を使用して ISE と統合された FMC の UI にアクセスできない
CSCwa33364	MR ブランチで見られる中間フローの問題について、FTD で誤解を招く OVER_SUBSCRIBED フローフラグが付けられる
CSCwa11052	バージョン 9.14(2)15 へのアップグレード後に SNMP が応答しなくなる
CSCwa48849	再開されたセッションでの SSL の予期しない動作
CSCwa56975	コントロールプレーンで DHCP オファーが表示されない
CSCvy78573	cloudagent は、ルックアップのために長さゼロの URL を Beaker に送信してはいけない
CSCvz58376	ポリシーの展開後に Snort ダウンする
CSCvz36862	FMC ポリシーの展開で、フェーズ 3 にかかる時間が 15 分を超える
CSCvw65324	マージテーブルの同時クエリにより、FMC 構築で mserver コアが引き起こされる
CSCvy58268	ブロック 80 および 256 の枯渇スナップショットが作成されない
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
CSCvz93407	IPS ポリシー名にスペースが含まれる場合、アップグレード後に使用できなくなる
CSCwa36889	FTD 管理インターフェイスのプログラムが FXOS で破損している

不具合 ID	タイトル
CSCvu18510	MonetDB のイベントデータベースのクラッシュにより、FMC の接続イベントが失われる
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
CSCvz53142	ASA が、name-server コマンドで指定されたインターフェイスを使用して IPv6 DNS サーバーに到達しない
CSCvz00934	トンネルの送信元を（FMC アクセス）データインターフェイスとして使用して VTI を設定できない
CSCwa40719	トレースバック: セカンダリファイアウォールをスレッド名でリロード: fover_parse
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
CSCwa17918	OSPF のデフォルトルートを常にアドバタイズするオプションをオフにできない
CSCwa55418	アップグレード前に AnyConnect パッケージを使用して展開すると、複数の DB フォルダ current-policy-bundle が生成される
CSCvz35787	中間フローについて、FTD で誤解を招く OVER_SUBSCRIBED フローフラグが付けられる
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
CSCvz70595	SAML ハンドラの処理中に ASA でトレースバックが観察される
CSCvy90836	スレッド名 SNMP ContextThread での ASA トレースバックおよびリロード
CSCvz78816	ASA では、FO 後にアクティブ IP アドレスとスタンバイ MAC アドレスを使用して ssh、https セッションが切断される
CSCvz30933	clear configure snmp-server コマンドが発行されると ASA のトレースバックとリロードが発生する
CSCvz96462	VPN セッションはないが、IP アドレスが「使用中」
CSCvz94573	遅延によるハートビートの低下が原因で MIO ハートビート障害が発生する
CSCwa14485	Cisco Firepower Threat Defense ソフトウェアで確認されたサービス拒否攻撃に対する脆弱性

不具合 ID	タイトル
CSCwa33898	Cisco 適応型セキュリティ アプライアンスのソフトウェアクライアントレス SSL VPN ヒープオーバーフローの脆弱性
CSCvy19170	SAML：AnyConnect IKEv2 でメモリリークを検出
CSCwa99932	クラッシュおよび再起動後に ASA/FTD がスタックする
CSCvz89327	OSPFv2 フローにクラスター集中型「c」フラグがない
CSCwa03347	IPv6 PIM パケットが、無効な IP の長さによるドロップが原因となり ASP でドロップする
CSCvz05541	ASA55XX：ソフトウェアアップグレード後に拡張モジュールインターフェイスが起動しない
CSCwa34110	FMC は南半球の DST 設定をサポートする必要がある
CSCvy90162	スケーリングされた AC-SSL-SAML 認証 TVM プロファイルのユニコーンプロキシスレッドでウォッチドッグバーキングに関連するクラッシュを検出
CSCvz71569	プロセス ZeroMQ のメモリ不足状態が原因で FTD のトレースバックとリロードが発生
CSCvz25454	ASA：129 行の asp-drop キャプチャにドロップ理由がありません
CSCvz68336	複数のインラインペアでの単一接続が原因で SSL 復号化が機能しない
CSCvy37484	device_policy_ref のエントリが大きいため、デバイス管理ページを開くときにパフォーマンスが低下する
CSCvz41761	FMC では、$ 文字を使用した EIGRP 認証秘密鍵の作成は許可されない
CSCvq29993	FPR2100 のみ：サイズが 80、256、1550 のメモリブロックで永続的なブロックリークとブラックホールトラフィックが発生
CSCwa76564	フェールオーバーの前後にマルチコンテキストが切り替わるとき、ASA で ASDM セッション/クォータ件数の不一致が発生する
CSCvz05189	クラスタでの xlate の複製中に Lina トレースバックによる FTD のリロードが発生する
CSCwa87315	ASA/FTD は、スレッド名「IP アドレス割り当て」でトレースバックおよびリロードする場合がある
CSCvc57575	ISIS：コンテキストの削除中に無効な ISIS デバッグが表示される
CSCvy32366	ASA を 9.15(1)10 にアップグレードした後、ASDM 7.15(1)150 ワンタイムパスワード（OTP）フィールドが表示されない

不具合 ID	タイトル
CSCvw62288	ASA：syslog レートが高い場合の 256 バイトのブロック枯渇
CSCvy60574	ポート dcosAG リークの修正を CSCvx14602 から KP/WM へ
CSCvz00699	ASA のアップグレード後、webvpn でトレースバックとリロードが定期的に発生する
CSCvz66795	コマンド「show access-list」実行時の SSH プロセスでの ASA のトレースバックとリロード
CSCvz09109	ヘッダーのみが設定されているにもかかわらず、クラスタ CCL インターフェイスキャプチャには完全なパケットが表示されない
CSCwa28822	FTD が UI 管理を FDM から FMC に移動すると、トラフィックが失敗する
CSCvz51258	show tech-support の出力は、crashinfo がある場合に混乱を招く可能性があり、クリーンアップするまたは直感的にする必要があります
CSCwa26038	ICMPインスペクションにより、適切にログに記録されないパケットドロップが発生する
CSCwb15795	監査メッセージが生成されない：ASAv9.12 からのロギングが有効化されない
CSCvz09106	Cisco ASA ソフトウェアと Cisco FTD ソフトウェアの SSL VPN におけるサービス拒否攻撃に対する脆弱性
CSCvy41763	Cisco Firepower Threat Defense ソフトウェアの XML インジェクションの脆弱性
CSCwa41834	pix_startup_thread による ASA/FTD トレースバックおよびリロード
CSCvy89648	CSCvx29429 の回避策を適用した後、ma_ctx ファイルが拡張子「.backup」で表示される
CSCvz02398	7.0 での SE リングタイムアウトで生成された暗号アーカイブ
CSCvz76746	管理トンネルを実装している間、ユーザーはオープン接続を使用して AnyConnect をバイパスできる
CSCvz76745	クラウドベースのマルウェアイベントによる SFDataCorrelator メモリの増加
CSCvz91618	KP：SNMP ホストグループの追加および削除時のトレースバックを検出
CSCvz99222	インラインセットの show コマンドと clear コマンドが機能しない
CSCvy53461	RSA キーと証明書が ASA コード 9.12.x を使用した WS-SVC-ASA-SM1-K7 でリロード後に削除される

不具合 ID	タイトル
CSCvy75724	ローエンドプラットフォームでの Msglyr プールメモリの減少による ZMQ OOM
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
CSCwa28895	FTD SSL プロキシは、設定可能または動的な最大 TCP ウィンドウサイズを許可する必要がある
CSCvz06652	SNMP の有効期間設定で snmpd コアファイルが検出される
CSCvz50922	FPR2100：ESP-Null 暗号化を使用すると、L2L VPN トンネルを形成できない
CSCvz95743	アップグレード後の NTP 同期の喪失
CSCvz77037	mojo-server の SSL エラーで FMC ユーザーインターフェイスのアクセスに失敗することがある
CSCvy96325	FTD/ASA：ACP に新しい ACE エントリを追加すると、LINA の ACE 要素が削除および再追加される
CSCwa69376	負荷が高い場合に snmp_logging.c:1303 でバスエラーが発生する
CSCwa53088	snort 2 ssl-debug ファイルが書き込まれない場合がある
CSCvx81447	dnsproxy ログメッセージが ASA に継続的に表示される
CSCwa39683	SSL デバッグが有効になっている場合、ssl_policy log_error メッセージによってログファイルがあふれる
CSCvy58697	SSL 共有キャッシュプロセスでメモリリークが発生する可能性がある
CSCvz24238	Cisco Firepower Management Center のクロスサイト スクリプティングの脆弱性
CSCwa15185	ASA/FTD：LUA から不要なプロセス呼び出しを削除
CSCvw56551	インターフェイス設定を変更すると、ASA で NAT の表面的な警告メッセージが表示される
CSCvz76848	RA トンネルで DTLS1.2 を使用する場合の FTD トレースバックとリロード
CSCvz76966	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 DNS DoS の脆弱性
CSCvz15529	スレッド名 Datapath での ASA のトレースバックおよびリロード

不具合 ID	タイトル
CSCvy57905	VTI トンネルインターフェイスが、HA の KP および WM プラットフォームでリロード後もダウンしたままになる
CSCwa27822	6.7 または 7.0 への FTD のメジャーアップグレード後、Lina プロセスが開始状態のままになる
CSCvy33676	以前の動的 xlate が作成されると、FTD で UN-NAT が作成される
CSCvz30333	「show capture」コマンドが実行されると、FTD または Lina がトレースバックすることがある
CSCwa21016	Cisco Firepower Threat Defense ソフトウェアの DNS 適用で確認されたサービス拒否攻撃に対する脆弱性
CSCvy82655	REST API：一括 AC ルールの作成が処理不可能なエンティティ（422）で失敗する
CSCwb00595	Mempool_DMA 割り当ての問題/メモリリークが発生
CSCwa85138	トランザクションコミット診断に関する複数の問題が発生
CSCwa51241	スイッチで FPR1140 管理インターフェイスからの不明な MAC アドレスを検出
CSCwa03275	BGP ルートが未解決と表示され、「ホストへのルートがありません」という ASP のドロップが原因となりパケットをドロップする
CSCvz73709	ASA および FTD のスタンバイユニットが HA に参加できない
CSCvz21886	nat が IP ではなくポート番号に一致する pbr ACL に一致した場合、nat の un-nat が 2 回発生しない
CSCvy63464	FTD 1100/2100 シリーズがクロックを 2033 に設定してリブートする
CSCvz19634	FTD ソフトウェアのアップグレードが 200_pre/505_revert_prep.sh で失敗することがある
CSCwa94894	ASA/FTD は、スレッド名「DATAPATH-4-9608」でトレースバックおよびリロードする場合がある
CSCvx89451	ISA3000：shutdown コマンドがシステムをシャットダウンする代わりに再起動する
CSCwa61218	OID「1.3.6.1.4.1.9.9.171.1.3.2.1.2」をポーリングすると、関連するトンネルの負のインデックス値が得られる
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

不具合 ID	タイトル
CSCvy99348	shutdown コマンドが、FP1k デバイスをシャットダウンする代わりに再起動する
CSCvz71825	Firepower 2K デバイスの MAC アルゴリズムが CC および UCAPL モードに対して正しくない
CSCwa18858	ASA が、「ラベル長 164 バイトがプロトコルの制限である 63 バイトを超えている」という理由で非 DNS トラフィックをドロップする
CSCvz54471	ASA：「HA 状態の進行に失敗した」後、HA ペアで失敗した ASA が自動的に回復されない
CSCvs27336	Smart Call Home プロセスにより ASA がトレースバックする
CSCwa67209	FTD のアップグレード後、FMC で 1 Gbps SFP ファイバーメンバーのポートチャネルの自動ネゴシエーションが無効になることがある
CSCwb33334	ASA：RAVPN トンネル経由で一部のトラフィックを送信した後にクラッシュする
CSCwa75077	プレフィルタルールに時間範囲オブジェクトが誤って入力される
CSCwa40237	Cisco Firepower Management Center で確認されたファイル アップロード セキュリティがバイパスされる脆弱性
CSCvz94153	IPV4 アドレスが設定されていない場合、IPV6 での NTP 同期が失敗する
CSCwa55562	同じ送信元 IP に割り当てられた異なる CG-NAT ポートのブロックにより、ホストごとの PAT ポートブロックが枯渇する
CSCvz31880	スケーリングストレステストを停止した後、「ユニコーンプロキシスレッド CPU：9 watchdog_cycles」で ASA がクラッシュする。
CSCwb20940	FMC：検出モードでの SSL/Snort3/NAP の組み合わせの検証チェックを追加
CSCwa77073	SNMP が予期しないオーダーにより snmpgetbulk に応答している
CSCwa11088	ページの更新/読み込み前に編集しようとすると、制御ルールの順序が自動的に変更される
CSCvz43414	HA のフェイルオーバー後に内部 LDAP 属性マッピングが失敗する
CSCvz46879	Sourcefire モジュールの mojo_server 設定の微調整
CSCvy90821	「debug snmp ?」のオートコンプリートが ASA で動作していない

バージョン 7.0.1.1 で解決済みのバグ

表 *57* : バージョン *7.0.1.1* で解決済みのバグ

不具合 ID	タイトル
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
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 7.0.1 で解決済みのバグ

表 *58* : バージョン *7.0.1* で解決済みのバグ

不具合 ID	タイトル
CSCum03297	ENH：ASA は MAXHOG のタイムスタンプを「show proc cpu-hog」に保存する必要がある
CSCvf89237	CVE-2017-9233 についてのユニコーン企業の評価
CSCvg66052	Firepower アプライアンスで 2 つの CPU コアが継続的にスパイクする
CSCvr11958	AWS FTD：「ERROR: failed to set interface to promiscuous mode」により展開が失敗する
CSCvs50538	SSL エンジンが判定を返さない場合、ファイアウォールエンジンは SSL ハンドシェイクからの情報にフォールバックする必要がある
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
CSCvv21602	FP2K MIB に cfprApSmMonitorTable がありません
CSCvv36788	MsgLayer[PID]：エラー：Msglyr::ZMQWrapper::registerSender()：ZeroMQ ソケットのバインドに失敗した
CSCvv43190	GRE ヘッダープロトコルフィールドが内部 IP ヘッダーのプロトコルフィールドと一致しない場合の暗号エンジンエラー
CSCvv48942	Snmpwalk がフェールオーバーインターフェイスのトラフィックカウンターを 0 として表示する
CSCvv59676	Snort2：TLS の証明書キャッシュのアグレッシブプルーニングを実装してメモリを解放する

不具合 ID	タイトル
CSCvv71097	トレースバック：ASA が snp_fdb_destroy_fh_callback＋104 をリロードする
CSCvv89715	8000 シリーズのスタックの Fastpath ルールが FMC からランダムに消える
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
CSCvw62526	エンジニアリング ASA Build での ASAトレースバックとリロード：9.12.3.237
CSCvw71405	暗号化プロセスで FPR1120 が ASA トレースバックとリロードを実行している
CSCvx11917	FTD アクティブユニットが host-move-pkt drop reason でインターフェイスフェールオーバー メッセージをドロップすることがある
CSCvx20872	netflow リフレッシュタイマーによる ASA/FTD トレースバックとリロード
CSCvx21050	Snort3 UDP のパフォーマンスが Snort2 と比較して最大 40% 低下しており、CPU 使用率の適切な修正が必要
CSCvx23833	IKEv2キー の再生成：Create_Child_SA 応答の直後に受信した新しい SPI を使用した ESP パケットの SPI が無効になる
CSCvx26308	chastrcpy_s: source の文字列が着信側に対して長すぎるため ASA がトレースバックおよびリロードする
CSCvx26927	CH をセグメント化して再送信した際に TLS サイトがロードされない
CSCvx38124	CP がピン接続されているコアでのコアローカルブロック割り当ての失敗によりドロップが発生する
CSCvx48490	「Initiator/Responder」パケットを 0 として示す SSL 復号化された https フローの EOF イベント
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%）
CSCvx51123	FMC UI エラー：ドメインの保存中にエラーが発生
CSCvx63788	AC ポリシーのデフォルトアクションの新しいウィンドウでポリシーを編集すると、IPS ポリシーにエラーのポップアップが表示される
CSCvx65178	ファイアウォール MIB 内の特定の OID に対して SNMP 一括取得が機能せず、デバイスのパフォーマンスが低下する
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

不具合 ID	タイトル
CSCvx76665	2100 で「インターフェイスのアップデートに失敗しました」というエラーメッセージが表示される
CSCvx77768	Umbrella によるトレースバックとリロード
CSCvx78238	ASA のトラフィックでのマルチコンテキストの Firepower サービスが不適切なインターフェイスに移動する
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
CSCvx80830	Radius サーバーが dACL を送信し、vpn-simultaneous-logins が 1 に設定されていると、同じユーザーからの VPN 接続が失敗する
CSCvx85922	ASA/FTDは、設定をメモリに保存/書き込みするときにトレースバックおよびリロードすることがある
CSCvx87709	HAで FPR 2100 が ASA を実行するフェールオーバー中のウォッチドッグでのトレースバックとリロード
CSCvx90486	ifXTable の snmpwalk がデータインターフェイスを返さないことがある
CSCvx91317	MariaDB 10.2 でバージョン 10 より前のリモートコード実行の問題を発見
CSCvx93254	DHCP リレーサーバーで「無効なヘルパーアドレス」のエラーが発生
CSCvx94398	セカンダリ ASA がスタートアップ コンフィギュレーションを取得できない
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
CSCvx95884	HA バルク同期中および通常の conn 同期中に CPU 使用率が高くなり、大量の「バッファなし」がドロップする
CSCvx96452	ペイロード伝送の完了後、一部の HTTP2 TLS トラフィックが TCP FIN ではなく TCP RST で終了する
CSCvx97632	クラスタコマンドを使用して長い宛先ファイル名を持つファイルをコピーする場合にASA がトレースバックおよびリロードする
CSCvy01482	アップグレード後にレルムの同期結果ページがフリーズする
CSCvy01752	スレッド Lic HA クラスタでのトレースバック
CSCvy03006	uauth のデバッグ機能の改善
CSCvy03907	アクセス コントロール ポリシーの作成および編集が「ルール名は既に存在します」というエラーで失敗する

不具合 ID	タイトル
CSCvy04343	PLR モードの ASA で「ライセンスのスマート予約」が失敗する。
CSCvy05966	Snort 2.9.16.3-3033 トレースバック（FTD 6.6.3）
CSCvy07113	7.0.0-1459：QP プラットフォームに固有のファイルポリシー設定で FTP トラフィック（マルウェアファイル）がブロックされない
CSCvy07491	access-list の再設定時の ASA トレースバック
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
CSCvy09436	DHCP 予約で一部のデバイスに予約済みアドレスを適用できない
CSCvy10583	スレッド名 DATAPATH での ASA トレースバックおよびリロード
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）
CSCvy14721	CH パケットの宛先ポートが送信元ポート以下であるときに FTD によって SSL トラフィックがドロップされる
CSCvy16179	CSCuz67596 の修正を実行中でも、スレッド名 Unicorn Admin Handler で ASA クラスタがトレースバックする
CSCvy17078	トレースバック：LINA プロセスで FPR 2110 の ASA がトレースバックおよびリロードする
CSCvy17365	REST API ログインページの問題
CSCvy17470	IKEv2 の A/S フェールオーバーペアで ASA トレースバックとリロードが発生する
CSCvy18138	登録フラグ付きのカプセル化されたパケットが RP に送信されたときに、PIM Register Sent カウンタが増加しない
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
CSCvy19453	MAC アドレスのみを持つ冗長な新しいホストイベントを含む SFDataCorrelator のパフォーマンスの問題
CSCvy21334	「スイッチオーバーなし」の場合、アクティブは CoA アップデートをスタンバイに送信しようとする
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
CSCvy27261	Snort2 および Snort3 のイベントビューの不整合

不具合 ID	タイトル
CSCvy29815	NTP AES-CMAC の入力が IOS-XE と整合性がない
CSCvy30016	「最大証明書キャッシュエントリ」プルーニングでは、SSL キャッシュをロックする必要がある
CSCvy30101	SSL 復号を使用すると、Snort2 のメモリ使用量が予想される制限を超えて増加する可能性がある
CSCvy31096	Snort 設定がリロードされた場合にホストが再検出される
CSCvy31229	/ngfwに空き領域がない
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
CSCvy31521	syslog-ng モニターを FMC に追加する
CSCvy32154	ポリシーマップでオフロードCLIを無効にした後、フローがオフロードされる
CSCvy32366	ASA を 9.15(1)10 にアップグレードした後、ASDM 7.15(1)150 ワンタイムパスワード（OTP）フィールドが表示されない
CSCvy33105	DNS ルックアップが有効な場合、「show route bgp」または「show route isis」であいまいなコマンドエラーが表示される
CSCvy33676	以前の動的 xlate が作成されると、FTD で UN-NAT が作成される
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
CSCvy36694	Azure の FTDv 6.7 が GigabitEthernet インターフェイスで 1000 の速度を設定できない
CSCvy37835	ssl置換キーのみのアクションにより、検出エンジンのメモリ使用量が無制限になる場合がある
CSCvy39191	FMC への API 呼び出しを実行すると、T-ufin で内部サーバーエラー 500 が発生する
CSCvy39621	ASA/FTDは、最大再試行回数に達した後も連続的な RADIUS アクセス要求を送信する
CSCvy39659	ASA/FTD がスレッド名「DATAPATH-15-14815」でトレースバックし、リロードすることがある
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

不具合 ID	タイトル
CSCvy40482	9.14MR3：snmpwalk が [Errno 146] の接続拒否エラーで失敗した
CSCvy41157	復元後に HA 構成に失敗する
CSCvy43447	マルチインスタンス FTD の Lic TMR スレッドでの FTDトレースバックとリロード
CSCvy47108	UAuth エントリがスタックしているため、リモートアクセス IKEv2 VPN セッションを確立できない
CSCvy48159	メモリヘッダー検証によるプロセス名 lina での ASA トレースバックとリロード
CSCvy48730	ASA/FTD がスレッド名「Unicorn Proxy Thread」でトレースバックおよびリロードすることがある
CSCvy49732	ASA/FTD がスレッド名「ssh」でトレースバックし、リロードすることがある
CSCvy50011	IKE デーモンプロセスでの ASA トレースバックおよびリロード
CSCvy51659	OCSP タイムアウトが長い場合、AnyConnect 認証が失敗することがある
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
CSCvy52074	ASA/FTD 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
CSCvy52924	FTD がリブート時にすべての VRF インスタンスの OSPF ネットワークステートメント設定を失う
CSCvy53301	「展開中の内部エラー」により FDM で HA 構成に失敗する
CSCvy53461	RSA キーと証明書が ASA コード 9.12.x を使用した WS-SVC-ASA-SM1-K7 でリロード後に削除される
CSCvy53798	x25519 曲線を使用してフローを復号化するときにメモリリークが発生
CSCvy55356	ドキュメントに反して、10 ミリ秒未満の CPU 占有が発生する
CSCvy56395	キー設定が存在する場合の SNMP 暗号化コミュニティストリングによる ASA トレースバックとリロード
CSCvy58268	ブロック 80 および 256 の枯渇スナップショットが作成されない
CSCvy60100	HA の再起動後に SNMP v3 設定が失われる
CSCvy60574	ポート dcosAG リークの修正を CSCvx14602 から KP/WM へ

不具合 ID	タイトル
CSCvy61008	Lina と FXOS 間の同期外れの時間
CSCvy63949	直接認証トラフィックが ASA を通過している場合でも ASA 直接認証がタイムアウトする
CSCvy64492	ASAv が MAC テーブルの自身のアドレスに非アイデンティティ L2 エントリを追加し、HA hello をドロップする
CSCvy64911	デバッグ：crasLocalAddress の SNMP MIB 値に IP アドレスが表示されない
CSCvy66711	Cisco ASA 9.16.1 と FTD 7.0.0 の IPsec に関するサービス妨害（DoS）の脆弱性
CSCvy67756	Firepower サービスの HTTPS トラフィックは、SSL ポリシーでルールを復号化しない（Do not decript）ルールと一致すると動作を停止する
CSCvy68859	侵入ルールの LSP およびカテゴリフィルタで DB 接続が解放されない
CSCvy69189	vpnfol_sync/Bulk-sync keytab がスタックしているため、FTD HA がバルク状態のままになる
CSCvy69787	AWS TenGigabit インターフェイス上の ASAv が 10000Mbps ではなく 1000mbps を学習している
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）
CSCvy72321	パケットトレーサーが、NAT フェーズでManual/Twice NAT に一致するときに「自動後」オプションを追加する
CSCvy72846	ASA アカウンティングが誤った Acct-Session-Time を報告する
CSCvy73554	ASA：暗号 ACL の「deny ip any any」エントリにより、IKEv2 リモート AnyConnect アクセス接続が阻止される
CSCvy74781	スタンバイデバイスが、フェールオーバー後に SSL トラフィックのキープアライブメッセージを送信する
CSCvy74984	デフォルトの外部ルートが使用されると、Azure 上の ASAv がメタデータサーバーへの接続を失う
CSCvy79023	idhttpsd アクセスログファイルのサイズ超過とログローテーションの失敗により、デバイス UI が停止する
CSCvy79952	ダウングレード後の ASA/FTD トレースバックとリロード
CSCvy82794	snmp コマンドを無効にする場合の ASA/FTD トレースバックとリロード

不具合 ID	タイトル
CSCvy83116	WM スタンバイが HA への再参加に失敗し、「CD アプリの同期エラーは、SSP 設定の生成における失敗です（CD App Sync error is SSP Config Generation Failure）」というメッセージが表示される
CSCvy84733	SFR 6.7 から 7.0 へのアップグレード：Syslog の機能が停止
CSCvy89440	s2sCryptoMap 設定の損失
CSCvy89648	CSCvx29429 の回避策を適用した後、ma_ctx ファイルが拡張子「.backup」で表示される
CSCvy89658	CCM レイヤ（スプリント 114、シーケンス 13）での WR6、WR8 および LTS18 コミット ID の更新
CSCvy92990	7.0 へのアップグレード後の SSL に関連する FTD トレースバックとリロード
CSCvy95554	group_fsp_reference テーブルのデータベースのマージで障害が発生したため、LDAP をダウンロードできない
CSCvy96625	CSCvr33428 および CSCvy39659 で導入された「修正」を復元する
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
CSCvy96803	SNMP 機能に関連するプロセス名 lina の FTD トレースバックとリロード
CSCvy99373	AD で adSamAccountName を解決するときにADI セッション処理が遅延する
CSCvz00032	スレッド名 Lina での FTD のトレースバックおよびリロード
CSCvz00254	アップグレードのインポート中にサイト間 VPN が無効な状態になり、FDM 6.7.0 から 7.0.0 へのアップグレードに失敗する
CSCvz00383	スレッド名 Checkheaps で FTD lina トレースバックとリロードが発生する
CSCvz00699	ASA のアップグレード後、webvpn でトレースバックとリロードが定期的に発生する
CSCvz05189	クラスタでの xlate の複製中に Lina トレースバックによる FTD のリロードが発生する
CSCvz05197	IE 11 でイベントページが機能しない
CSCvz05468	最初の機能の有効化/展開としてプラットフォーム設定に複数の SSH ホストエントリがあると、LINA で SSH が切断される

不具合 ID	タイトル
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
CSCvz06652	SNMP の有効期間設定で snmpd コアファイルが検出される
CSCvz06848	snmp-server community 検証でエラーが発生し、FTD/FDM のアップグレードに失敗する
CSCvz07614	ASA：孤立した SSH セッションでは、CLI からポリシーマップを削除できない
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
CSCvz15529	スレッド名 Datapath での ASA のトレースバックおよびリロード
CSCvz17534	FTD のバックアップ復元 CLI で VPN 設定が復元されない
CSCvz20544	Anyconnect プロファイルのループ処理で、ASA および FTD がトレースバックおよびリロードする場合がある
CSCvz21886	nat が IP ではなくポート番号に一致する pbr ACL に一致した場合、nat の un-nat が 2 回発生しない
CSCvz23157	show コマンドが発行されると SNMP エージェントが再起動する
CSCvz25434	BVI が DHCP クライアントとして設定されている場合、1550 ブロックの枯渇が原因で ASA および FTD がトラフィックをブラックホールする
CSCvz25663	snmp-server host のコミュニティストリング検証の失敗による FTD/FDM アップグレードエラー
CSCvz26950	[DOC] FMC ドキュメント内のアプライアンス情報ウィジェットに高可用性の情報がない
CSCvz29233	ASA：システムコンテキストでインターフェイスのフラップが発生したときに、カスタムコンテキストからの ARP エントリが削除されない
CSCvz30333	「show capture」コマンドが実行されると、FTD または Lina がトレースバックすることがある
CSCvz30933	clear configure snmp-server コマンドが発行されると ASA のトレースバックとリロードが発生する
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
CSCvz34831	ASA が DACL のダウンロードに失敗した場合、試行を停止しない

不具合 ID	タイトル
CSCvz35201	アップグレードの失敗/999_finish/989_update_ngfw_conf_aquila_ssp.sh でフリーズ
CSCvz38361	直接接続されていないネイバーのために BGP パケットがドロップされる
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
CSCvz46333	内部ソケット接続の損失による FTD ポリシー展開の失敗
CSCvz66506	FMC HA に登録されている 7.0 にアップグレードした後、FPR2100 で継続的な ADI クラッシュが発生する

バージョン 7.0.0.1 で解決済みのバグ

表 *59* : バージョン *7.0.0.1* で解決済みのバグ

不具合 ID	タイトル
CSCvy66711	Cisco ASA 9.16.1 と FTD 7.0.0 の IPsec に関するサービス妨害（DoS）の脆弱性

バージョン 7.0.0 で解決済みのバグ

表 *60* : バージョン *7.0.0* で解決済みのバグ

不具合 ID	タイトル
CSCvi96835	ルーティングポリシーで使用されるグループオブジェクトの一部であるホストを範囲に変更しても検証エラーが発生しない
CSCvk22190	時刻同期の問題の後、FMC で接続/侵入イベントを受信しない
CSCvm69294	スタンバイ FMC が大量の SNMP トラップを送信している
CSCvm99989	SystemUpTime の SNMP OID に誤った値が表示される
CSCvo57004	[Analyze Hit Counts）] で、設定されたユーザータイムゾーンではなく UTC でタイムスタンプが表示される
CSCvp54996	GNU Wget のバッファオーバーフローの脆弱性
CSCvp58886	SNMP FXOS（FPR2100）のロケーション内の特殊文字により、ポリシー展開が失敗する

不具合 ID	タイトル
CSCvq55919	Cisco Firepower Management Center ソフトウェアに蓄積されたクロスサイト スクリプティングの脆弱性
CSCvq89604	Cisco_Firepower_Mgmt_Center_Patch_Uninstaller-6.4.0.3-29.sh.REL.tar の実行が失敗する
CSCvr03127	Apache HTTP Server mod_proxy クロスサイト スクリプティングの脆弱性
CSCvr13762	FMC 上の NGFWHA に EO UUID がない
CSCvr46901	分析接続イベントで、UI にすべてのイベントは表示および報告されない
CSCvr74896	クラウドフィードが無効になっている状態で AC ポリシーを FMC にインポートすると、セキュリティ インテリジェンスを更新できない
CSCvs02229	Network Time Protocol 認証モード 6 のパケット処理ヌルポイント
CSCvs05066	Snort ファイルのメモリプールの破損によりパフォーマンスが低下し、プロセスが失敗する
CSCvs06043	ngfwManager の CSM_CCMservice 用の TunnelClient が FMC の CSM_CCM サービスから送信された ACK を読み取らない
CSCvs71034	Beaker の登録がエラー 400 で失敗：不正な要求
CSCvs71969	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
CSCvs74802	AnyConnect または S2S IKEv2 暗号化ポリシーがデバイスに展開されないことがある
CSCvs79606	「dns server-group DefaultDNS」CLI が無効にならない
CSCvs84242	自動 NAT および相関ネットワークオブジェクトを削除するとき、FMC の展開に失敗する
CSCvt29771	[Object Management] ページからセキュリティゾーンを変更した場合の無効な応答メッセージ
CSCvt31292	FTD デバイスが SSE にイベントを送信しない場合がある
CSCvt43136	複数のシスコ製品 Snort TCP 高速オープン ファイル ポリシー バイパスの脆弱性
CSCvt49334	4120 センサーで、タスクの削除によって cron.d ディレクトリから「task_xx」ファイルが削除されない
CSCvt74194	unified2 レコード取得中のエラー：ファイルの破損

不具合 ID	タイトル
CSCvt74893	FMCv イーサネットドライバが vmxnet3 TCP のパフォーマンス侵害を示している
CSCvt91258	FDM：管理ゲートウェイとしてデータインターフェイスを使用して、どの NTP サーバーにも到達しない
CSCvt93177	デフォルトでフルプロキシを無効化してライトウェイトプロキシにする。（FP2LWP）FTD デバイス
CSCvt93999	アップグレードが進行中の場合、FMC は同じデバイスで 2 回目のアップグレードを許可すべきではない
CSCvu12608	ASA5506/5508/5516 デバイスが正しく起動しない/ブートループが発生する
CSCvu18510	MonetDB のイベントデータベースのクラッシュにより、FMC 6.6.0 および 6.6.1 の接続イベントが失われる
CSCvu21953	FMC 6.4.0 が FTD に「strong-encryption-disable」をランダムに送信する
CSCvu22293	リモートストレージを持つ複数の管理対象デバイスの FMC でスケジュールされたバックアップが失敗する
CSCvu29508	FMC を手動で削除して FTD クラスタメンバーを追加すると、古いインターフェイスをダングリングする
CSCvu30756	ユーザー ID が、異なるネットマップの同一セッションを正しく処理しない
CSCvu34228	FTD LINA トレースバック & リロード処理中の Snort リターン判定
CSCvu35704	FMC、センサー、ThreatGrid 間の APIKEY の不一致により、ファイル送信が大幅に低下する
CSCvu44472	FMC システムプロセスが起動する
CSCvu54706	Cisco Firepower Management Center CWE-772：低速 HTTP POST の脆弱性
CSCvu75855	有効になるべきではないときに、管理対象デバイスで stunnel プロセスが有効になる
CSCvu77689	FileZilla への FTP が SMTP に誤って分類される
CSCvu88005	GET taskstatus の FMC REST API ユーザー権限
CSCvu88886	アップグレード後に、管理対象 FTD への脅威データの展開が失敗する場合がある
CSCvv00155	インターフェイスまたはサブインターフェイスを削除すると、フェールオーバー MAC アドレス設定も削除される必要がある

不具合 ID	タイトル
CSCvv08244	Firepower モジュールによって「復号しない」SSL 復号ルールに一致する信頼できる HTTPS 接続がブロックされることがある
CSCvv12491	6.4 にアップグレードした後も cloudagent_urllookup_health ファイルが古い形式のままになる
CSCvv14109	バックアップファイルから復元された新しい FMC が、ユーザー IP とユーザーグループのマッピングをデバイスに送信しない
CSCvv14442	将来のタイムスタンプを持つファイル/ディレクトリが含まれている場合、FMC バックアップの復元が失敗する
CSCvv17893	uip スナップショットとログファイルが不正なため、FTD がキャッチアップを繰り返し要求し、ファイルハンドラを使い果たす
CSCvv20780	ポリシーの展開が「展開トランザクションを保持できませんでした」エラーで失敗する
CSCvv21782	6.6.1：ASA SFR プラットフォームのすべてのトラフィックに対して無効な ID として表示されるプレフィルタポリシー値
CSCvv27084	loggerd を介した EventHandler Syslog が宛先ホスト名をサポートしていない
CSCvv27867	FMC クラシックテーマ：複数のアイテムを持つグループのオブジェクト詳細にスクロールバーがない
CSCvv29275	FMC OSPF エリアが 49 エントリまで制限される。50 番目のエントリを追加すると、プロセスは自動的に無効になる
CSCvv34523	firewall_target_cache テーブルが想定どおりにプルーニングされないため、データベースのサイズが大きくなる
CSCvv34851	6.7.0-1992：重複した接続イベントの 1 つに空の SSL 情報がある
CSCvv36915	「Show NTP」コマンドがマルチインスタンス FTD で機能しない
CSCvv38869	データベースエラーが原因で FMC が FTD を 6.3 から 6.7 にアップグレードできない
CSCvv40961	http-proxy 設定が原因でアップグレードが失敗する
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
CSCvv45106	csd-service.json ファイルが見つからないため、2100 で CSD が起動しない
CSCvv46490	SnortAttribConfig のエラーにより FMC でポリシーの展開が失敗する

不具合 ID	タイトル
CSCvv50298	FTD 管理インターフェースが TLS プードル攻撃に対して脆弱になる（CVE-2014-3566）
CSCvv53042	DBCheck.pl の出力にアップグレード失敗の原因となる致命的なエラーが含まれる
CSCvv55066	FPR1010：SMBファイル転送中に Internal-Data0/0 およびデータインターフェイスがフラッピングする
CSCvv56644	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 Web DoS の脆弱性
CSCvv57476	Chrome 85、IE、および Edge ブラウザで CSS スタイルをロードすると問題が発生する
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。
CSCvv60849	Snort D-state を回避するために、メモリ cgroup の制限を調整する必要がある
CSCvv62931	src.port=dst.port の場合、FTD が Server Hello およびサーバー証明書をクライアントに送信しない
CSCvv68000	FDM UI によって作成された RA VPN グループポリシーを取得すると、bravado エラーが発生する
CSCvv68078	セカンダリ FMC で Sybase データベースが破損しているため同期できない
CSCvv69862	リーフで 45 分の FTDHA 後に「長時間実行のバックアップを終了する」のメッセージと共に FMC バックアップエラーが発生
CSCvv70096	Snort 2：SSL 復号化および再署名プロセスでのメモリリーク
CSCvv70683	[タスク（Task）] タブに新しい通知が表示されない
CSCvv73054	Snort ライブラリが展開中に削除される
CSCvv74658	FTD/ASA は、ファイル名に「!」の文字を含むコアダンプファイルを作成する（CSCvv40406 の zmq 変更（fxos））
CSCvv74795	syslog-ng には、ASA5525-X で実行中の追加のインスタンスがある
CSCvv74816	NAT 免除が適用されている間は、FDM でローカルアドレスプールの削除を許可してはいけない
CSCvv74951	システムのアップグレードスクリプトの実行中、メモリの cgroup を無効化
CSCvv75148	VPN イベントの RabbitMQ キューには、*.idx ファイルの蓄積を避けるためのサイズ制限がない

不具合 ID	タイトル
CSCvv76581	Cisco Firepower 製品ラインの Racoon 攻撃の評価（CVE-2020-1968）
CSCvv79459	CCM レイヤ（スプリント 94、シーケンス 1）における WR6、WR8 および LTS18 コミット ID の更新
CSCvv79897	Lina のクラッシュとシステムの再起動イベントの発生を防ぐために、FTD ユニットの「sensor restart」コマンドをブロックする
CSCvv83841	アップグレード：600_schema/100_update_database.sh に十分なルートディスク容量がない
CSCvv84172	登録失敗時のクラスタ化されたテーブルと EO のダングリング参照
CSCvv84385	ディスクマネージャーが、FMC eStreamer によって使用される統合ファイルを誤ってプルーニングする
CSCvv89715	8000 シリーズのスタックの 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
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
CSCvv94165	FTD 6.6：snmpd プロセスの CPU がスパイクする
CSCvv97527	asa config timeout コマンドが snort の DAQ 設定を壊す
CSCvv97902	policy_deployment.db に deployment_info がないため、展開の消去が実行されない
CSCvw03256	[Message] フィールドが選択されている場合、FMC ダッシュボードに侵入テーブルの「No Data」と表示される
CSCvw04171	読み取り専用ユーザーの場合、[デバイスの概要（Device Summary）] タブに forbidden エラーページが返される
CSCvw07352	Sybase 接続ステータスが 0 になると、SFDataCorrerator のログスパム、メタデータで障害が発生する
CSCvw10877	/var/sf/user_identity は、トラブルシューティングでアーカイブを一緒に取得してはいけない
CSCvw13395	FMC 6.6.0 の UI のライトテーマ内に [タイムアウト時に接続をリセットする（Reset Connection Upon Timeout）] チェックボックスがない
CSCvw16565	DCE/RPC の設定で [SMB 自動検出ポート（SMB Auto-Detect Ports）] を有効にすると、ポリシーの展開に失敗する

不具合 ID	タイトル
CSCvw21145	ポリシーを保存する際に起こる重複 NAT ルールエラー（重複する自動 NAT ルールが原因）
CSCvw21161	ポリシー保存時に起こる重複 NAT ルールエラー（異なるルールが重複として検出される）
CSCvw21628	6.6.x より前から 6.6.x 以降にアップグレードすると、侵入イベントのパケットドリルダウンが機能しなくなる
CSCvw27966	オブジェクト名が「any」で始まる場合、ポリシーの展開に失敗する
CSCvw28894	vuln テーブルのエントリが重複しているため、SFDataCorrerator の起動が遅くなり、vuln の再マッピングが発生する
CSCvw28946	VxLan 構成を展開すると、コマンド mtu の送信順番が乱れるため、展開に失敗する
CSCvw29561	「スマートライセンスクラウドとの継続的なスマートエージェント通信を示しています」という FMC SLR ライセンスのアラートが表示される
CSCvw29563	repair_users.pl スクリプトが機能しなくなった
CSCvw29581	mysql ユーザーテーブルが破損している場合、 VDB のアップグレードは機能しない
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
CSCvw33939	IPv6 オブジェクトを含むネットワークグループを使用した VPN スプリットトンネルの標準 ACL が原因で FMC の展開に失敗
CSCvw34692	BGP ネイバーの TTL ホップを初めて変更した後は変更できなくなる
CSCvw38708	AC ポリシーが構成要素のキャッシュを使用せずにアクティビティを保存および検証する
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
CSCvw41901	FMC の REST API を介してシステム定義オブジェクトを削除すると、HTTP 500 エラーコードが返される
CSCvw42497	ポリシー検証で AC ポリシーのナビゲート中にエラーが発生
CSCvw45125	セカンダリノードが構成中または一括同期中に展開がブロックされる
CSCvw47943	Firepower 推奨事項であるスキャン結果のクエリの最適化
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

不具合 ID	タイトル
CSCvw60177	スタンバイまたはセカンダリのクラスタユニットがスレッド名 fover_parse および「cluster config sync」でクラッシュすることがある
CSCvw79294	sftunnel が大量のログをメッセージファイルに記録する
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
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
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
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
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

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。

リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。

あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。