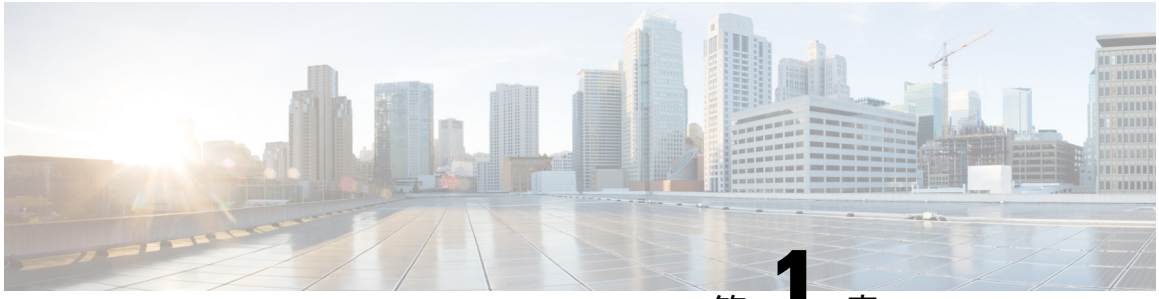
Cisco Firepower バージョン 6.6.x メンテナンス リリース リリースノート

初版：2020 年 9 月 8 日

最終更新：2022 年 5 月 2 日

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

目 次



第 1 章

ようこそ

このドキュメントでは、以下に示す Version6.6 のリリース情報を記載しています。

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

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

リリース日

シスコは、更新版ビルドを適宜リリースしています。ほとんどの場合、各プラットフォームの最新のビルド番号のみが、シスコ サポートおよびダウンロード サイト で入手可能です。最新のビルドを使用することを強くお勧めします。以前のビルドをダウンロードした場合は使用しないでください。詳細については、新しいビルドで解決済みの問題 （89 ページ）を参照してください。

表 *1*：バージョン *6.6* のリリース日

バージョン	ビルド	日付	プラットフォーム
6.6.5.2	14	2022 年 03 月 24 日	すべて

バージョン	ビルド	日付	プラットフォーム
6.6.5.1	15	2021 年 12 月 6 日	すべて
6.6.5	81	2021 年 8 月 3 日	すべて
6.6.4	64	2021 年 4 月 29 日	Firepower 1000 シリーズ
	59	2021 年 4 月 26 日	FMC/FMCv Firepower 1000 シリーズを除くすべてのデバイス
6.6.3	80	2020 年 3 月 11 日	すべて
6.6.1	91	2020 年 9 月 20 日	すべて
	90	2020 年 9 月 8 日	—
6.6.0.1	7	2020 年 7 月 22 日	すべて
6.6.0	90	2020 年 5 月 8 日	Firepower 4112
		2020 年 4 月 6 日	FMC/FMCv Firepower 4112 を除くすべてのデバイス

推奨リリース

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

また、新機能ガイドにも推奨リリースを示します。

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

古いアプライアンスの推奨リリース

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

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

シスコとのデータの共有

次の機能はシスコとデータを共有します。

Cisco Success Network

Cisco Success Network は、テクニカル サポートを提供するために不可欠な使用状況に関する情報と統計情報をシスコに送信します。

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

Cisco Support Diagnostics

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

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

Web 分析トラッキング

Web分析のトラッキングは、これに限定されませんが、ページでの操作、ブラウザのバージョン、製品のバージョン、ユーザーの場所、FMC の管理 IP アドレスまたはホスト名を含む、個人を特定できない使用状況データをシスコに送信します。

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

サポートが必要な場合

オンラインリソース

シスコは、ドキュメント、ソフトウェア、ツールのダウンロードのほか、バグを照会したり、サービスリクエストをオープンしたりするための次のオンラインリソースを提供しています。

これらのリソースは、Cisco ソフトウェアをインストールして設定したり、技術的問題を解決したりするために使用してください。

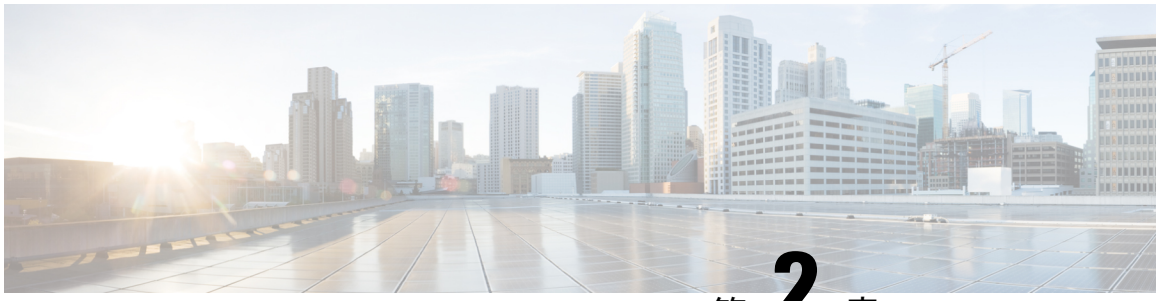
- マニュアル：http://www.cisco.com/jp/go/threatdefense-66-docs
- シスコ サポートおよびダウンロード サイト：https://www.cisco.com/c/en/us/support/index.html
- Cisco Bug Search Tool：https://tools.cisco.com/bugsearch/
- シスコ通知サービス：https://www.cisco.com/cisco/support/notifications.html

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

シスコへのお問い合わせ

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

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



第 2 章

システム要件

このドキュメントでは、Version6.6 のシステム要件を記載します。

デバイスのプラットフォーム

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

（注） これらのリリースノートには、本リリースでサポートされているデバイスが掲載されています。古いデバイスがEOLに達していて、アップグレードできなくなった場合でも、数バージョンの範囲内であれば、より新しいFMCを使用してそのデバイスを管理できます。同様に、より新しいバージョンのASDMでは、より古いバージョンのASA FirePOWERモジュールを管理できます。下位互換性を含む、サポート対象の管理方法については、「マネージャとデバイスの互換性 （8 ページ）」を参照してください。一般的な互換性情報については、Cisco Secure Firewall Threat Defense 互換性ガイド または Cisco Firepower Classic Device 互換性ガイド を参照してください。

表 *2 :* バージョン *6.6.0/6.6.x* の *Firepower Threat Defense*

FTD プラットフォーム	OS/ハイパーバイザ	詳細情報
Firepower 1010、1120、1140、1150 Firepower 2110、2120、2130、2140	—	—
Firepower 4110、4120、4140、4150 Firepower 4112、4115、4125、4145 Firepower 9300：SM-24、SM-36、SM-44 モジュール Firepower 9300：SM-40、SM-48、SM-56 モジュール	FXOS 2.8.1.105 以降のビルド	最初に FXOS をアップグレードします。 問題を解決するには、FXOSを最新のビルドにアップグレードする必要がある場合があります。判断のヒントについては、『Cisco FXOS Release Notes, 2.8(1)』を参照してください。
ASA 5508-X、5516-X ASA 5525-X、5545-X、5555-X ISA 3000	—	FTD 展開では、これらのデバイスのオペレーティングシステムを個別にアップグレードすることはありませんが、ISA 3000、ASA5508-Xおよび 5516-X に最新の ROMMON イメージがあることを確認する必要があります。Cisco ASA and Firepower Threat Defense Reimage Guide

FTD プラットフォーム	OS/ハイパーバイザ	詳細情報
Firepower Threat Defense Virtual（FTDv）	次のいずれかです。 • AWS：Amazon Web Services • Azure：Microsoft Azure • KVM：カーネルベースの仮想マシン • VMware vSphere/VMware ESXi 6.0、6.5、または 6.7	サポートされているインスタンスについては、該当する FTDv のスタートアップガイドを参照してください。

表 *3 :* バージョン *6.6.0/6.6.x* の *NGIPS/ASA FirePOWER*

NGIPS/ASA FirePOWER プラットフォーム	OS/ハイパーバイザ	詳細情報
ASA 5508-X、5516-X ISA 3000	ASA 9.5(2) ～ 9.16(x)	ASA と ASA FirePOWER のバージョンには幅広い互換性があります。ただし、アップグレードすると、新機能を利用でき、問題も解決されます。操作の順序については、『Cisco ASA Upgrade Guide』を参照してください。 また、ISA 3000、ASA5508-X および 5516-X に最新の ROMMON イメージがあることも確認してください。Cisco ASA and Firepower Threat Defense Reimage Guide
ASA 5525-X、5545-X、5555-X	ASA 9.5(2) ～ 9.14(x)	
NGIPSv	VMware vSphere/VMware ESXi 6.0、6.5、または 6.7	サポートされているインスタンスについては、『Cisco Firepower NGIPSv Quick Start Guide for VMware』を参照してください。

FMC プラットフォーム

このドキュメントには、Version6.6 でサポートされている FMC が記載されています。一般的な互換性情報については、Cisco Secure Firewall Management Center 互換性ガイド を参照してください。

FMC ハードウェア

Version6.6 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
- FMC 2000、4000

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

FMCv

FMCv では、2、10、25、または 300 台のデバイスを管理できるライセンスを購入できます。一部のプラットフォームのみが FMCv300 をサポートすることに注意してください。サポートされているインスタンスの詳細については、Cisco Secure Firewall Management Center Virtual 入門ガイド を参照してください。

表 *4 : Version6.6 FMCv* プラットフォーム

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

マネージャとデバイスの互換性

Firepower Management Center

すべてのデバイスが Firepower Management Center を使用した遠隔管理をサポートしており、これにより複数のデバイスを管理することができます。FMC では、その管理対象デバイスと同じまたはより新しいバージョンを実行する必要があります。FMC よりも新しいバージョンのデバイスをアップグレードすることはできません。メンテナンス（3桁）リリースの場合でも、最初に FMC をアップグレードする必要があります。

新しい FMC では、次の表に示されている複数のメジャーバージョンまで遡って古いデバイスを管理できます。ただし、導入環境全体を常に更新することをお勧めします。多くの場合、新

機能の使用や問題解決の適用には、FMC とその管理対象デバイスの両方で最新リリースが必要になります。

表 *5 : FMC*とデバイス間の互換性

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

Firepower Device ManagerおよびCisco Defense Orchestrator

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

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

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

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

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

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

表 *6 : FTD* との *FDM* および *CDO* の互換性

FTDプラットフォーム	FDM 互換	CDO 互換
Firepower 1000 シリーズ	6.4.0 以降	6.4.0 以降
Firepower 2100 シリーズ	6.2.1 以降	6.4.0 以降
Firepower 4100/9300	6.5.0 以降	6.5.0 以降
ASA 5500-X シリーズ	6.1.0 ～ 7.0.x	6.4.0 ～ 7.0.x
ISA 3000	6.2.3 以降	6.4.0 以降

FTDプラットフォーム	FDM 互換	CDO 互換
AWS 用 FTDv	6.6.0 以降	6.6.0 以降
Azure 用 FTDv	6.5.0 以降	6.5.0 以降
KVM 用 FTDv	6.2.3 以降	6.4.0 以降
VMware 用 FTDv	6.2.2 以降	6.4.0 以降

Adaptive Security Device Manager

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

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

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

表 *7: ASDM* と *ASA FirePOWER* の互換性

ASA FirePOWER のバージョン	最小 ASDM バージョン
6.7.x	7.15.1
6.6.x	7.14.1
6.5.0	7.13.1
6.4.0	7.12.1
6.3.0	7.10.1
6.2.3	7.9.2

ブラウザ要件

ブラウザ

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

- Google Chrome
- Mozilla Firefox
- Microsoft Internet Explorer 11（Windows のみ）

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

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

ブラウザの設定と拡張

ブラウザに関係なく、JavaScript、Cookie、および TLS v1.2 が有効なままになっていることを確認する必要があります。

Microsoft Internet Explorer 11 を使用している場合：

- [保存しているページの新しいバージョンの確認（Check for newer versions of stored pages）] 閲覧履歴オプションについては、[自動（Automatically）] を選択してください。
- [サーバーにファイルをアップロードするときにローカル ディレクトリのパスを含める（Include local directory path when uploading files to server）] カスタムセキュリティ設定を無効にします。
- アプライアンスの IP アドレス/URL に対して [Compatibility View] を有効にします。

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

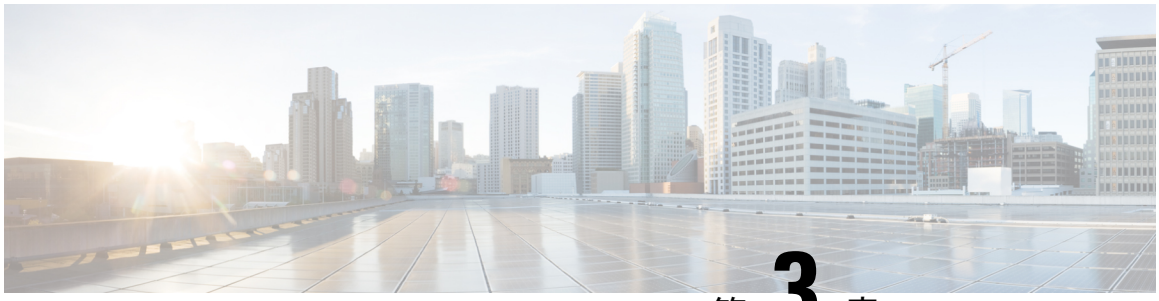
詳しい手順については、オンラインヘルプまたはご使用の製品のコンフィギュレーション ガイドを参照してください。

（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、Version6.6 の新機能と廃止された機能について説明します。また、アップグレードによる影響についても言及します。

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

新機能

FMC バージョン 6.6 の新機能

表 *8 : FMC* バージョン *6.6.3* の新機能

機能	説明
アップグレードがスケジュールされたタスクを延期する	**アップグレードの影響。** アップグレードは、スケジュールされたタスクを延期するようになりました。アップグレード中に開始するようにスケジュールされたタスクは、アップグレード後の再起動の 5 分後に開始されます。 （注） アップグレードを開始する前に、実行中のタスクが完了していることを確認する必要があります。アップグレードの開始時に実行中のタスクは停止し、失敗したタスクとなり、再開できません。 この機能は、バージョン 6.6.3 以降を実行している Firepower アプライアンスでサポートされています。バージョン 6.4.0.10 以降のパッチからアップグレードする場合を除き、バージョン 6.6.3 へのアップグレードはサポートされません。

機能	説明
アプライアンス設定のリソース使用率の正常性モジュール	バージョン 6.7.0 のアップグレードの影響。 バージョン 6.6.3 では、デバイスのメモリ管理が改善され、新しい正常性モジュールであるアプライアンス設定のリソース使用率が導入されています。 モジュールは、展開された設定のサイズに基づき、デバイスのメモリが不足するリスクがある場合にアラートを出します。アラートには、設定に必要なメモリ量と、使用可能なメモリ量を超過した量が示されます。アラートが出た場合は、設定を再評価してください。ほとんどの場合、アクセス制御ルールまたは侵入ポリシーの数または複雑さを軽減できます。詳細については、コンフィギュレーション ガイドの「アクセス制御のベストプラクティス」を参照してください。 アップグレードプロセスにより、すべての正常性ポリシーにこのモジュールが自動的に追加され、有効になります。アップグレード後、正常性ポリシーを管理対象デバイスに適用して、モニタリングを開始します。 （注） このモジュールには、FMC と管理対象デバイスの両方に、バージョン 6.6.3 以降の 6.6.x リリース、またはバージョン 7.0.0 以降が必要です。 バージョン 6.7.0 では、このモジュールのサポートが部分的および一時的に廃止されています。詳細については、バージョン 6.7.0 リリースノートを参照してください。 バージョン 7.0.0 ではフルサポートが提供され、モジュールの名前が構成メモリ割り当てに変更されています。

表 *9 : FMC* バージョン *6.6.0* の新機能

機能	説明
プラットフォーム機能	

機能	説明
クラウドベースの FTDv 展開の自動スケール	バージョン 6.6.0 では、AWS 自動スケール/Azure 自動スケールのサポートが導入されています。 クラウドベースの展開におけるサーバーレス インフラストラクチャでは、キャパシティのニーズに基づいて、自動スケールグループ内の FTDv インスタンスの数が自動的に調整されます。これには、管理側の FMC との自動登録/登録解除が含まれています。 サポートされているプラットフォーム：FTDv for AWS、FTDv for Azure
Firepower Threat Defense：デバイス管理	
DHCP を使用した初期管理インターフェイスの IP アドレスの取得	Firepower 1000/2000 シリーズと ASA-5500-X シリーズのデバイスの場合、管理インターフェイスはデフォルトで DHCP から IP アドレスを取得するようになりました。この変更により、既存のネットワーク上に新しいデバイスを簡単に展開できるようになりました。 この機能は、論理デバイスを展開するときに IP アドレスを設定する Firepower 4100/9300 シャーシではサポートされていません。また、FTDv や ISA 3000 でもサポートされていません。これらについては、引き続きデフォルトで 192.168.45.45 になります。 サポートされているプラットフォーム：Firepower 1000/2000 シリーズ、ASA-5500-X シリーズ
CLI での MTU 値の設定	FTD CLI を使用して、FTD デバイスインターフェイスの MTU（最大伝送単位）値を設定できるようになりました。デフォルト値は 1500 バイトです。MTU の最大値は次のとおりです。 • 管理インターフェイス：1500 バイト • イベントインターフェイス：9000 バイト 新しい FTD CLI コマンド： **configure network mtu** 変更された FTD CLI コマンド：**mtu-event-channel** キーワードと **mtu-management-channel** キーワードが **configure network management-interface** コマンドに追加されました。 サポートされるプラットフォーム：FTD

機能	説明
内部 Web サーバーからのアップグレードパッケージの取得	FTD デバイスは、FMC からではなく、独自の内部 Web サーバーからアップグレードパッケージを取得できるようになりました。これは、FMC とそのデバイスの間の帯域幅が制限されている場合に特に役立ちます。また、FMC 上の領域も節約できます。 （注） この機能は、バージョン 6.6.0+ を実行している FTD デバイスでのみサポートされています。バージョン 6.6.0 へのアップグレードではサポートされておらず、FMC または従来のデバイスでもサポートされていません。 新規/変更されたページ：[システム（System）] > [更新（Updates）] > [更新のアップロード（Upload Update）] ボタン > [ソフトウェア更新ソースの指定（Specify Software Update Source）] オプション サポートされるプラットフォーム：FTD
接続ベースのトラブルシューティングの機能拡張	FTD CLI 接続ベースのトラブルシューティングに次の機能拡張が加えられました（デバッギング）。 • **debug packet-module trace**：モジュールレベルのパケットトレースを有効にするために追加されました。 • **debug packet-condition**：進行中の接続のトラブルシューティングをサポートするように変更されました。 サポートされるプラットフォーム：FTD
Firepower Threat Defense：クラスタリング	

機能	説明
マルチインスタンスクラスタ	コンテナインスタンスを使用してクラスタを作成できるようになりました。Firepower 9300 では、クラスタ内の各モジュールに 1 つのコンテナインスタンスを含める必要があります。セキュリティエンジン/モジュールごとに複数のコンテナインスタンスをクラスタに追加することはできません。 クラスタインスタンスごとに同じセキュリティモジュールまたはシャーシモデルを使用することを推奨します。ただし、必要に応じて、同じクラスタ内に異なる Firepower 9300 セキュリティ モジュール タイプまたは Firepower 4100 モデルのコンテナインスタンスを混在させ、一致させることができます。同じクラスタ内で Firepower 9300 と 4100 のインスタンスを混在させることはできません。 新しい FXOS CLI コマンド： **set port-type cluster** 新規/変更された Chassis Manager ページ： • **[論理デバイス（Logical Devices）] > [クラスタの追加（Add Cluster）]** • **[インターフェイス（Interfaces）] > [すべてのインターフェイス（All Interfaces）] > [新規追加（Add New）]** ドロップダウンメニュー > [サブインターフェイス（Subinterface）] > [タイプ（Type）] フィールド サポートされるプラットフォーム：Firepower 4100/9300
FTD クラスタでのデータユニットへのパラレル設定同期	FTD クラスタの制御ユニットは、デフォルトでスレーブユニットとの設定変更を同時に同期させるようになりました。以前は、同期が順番に行われていました。 サポートされるプラットフォーム：Firepower 4100/9300
クラスタへの参加の失敗または削除のメッセージを次のコマンドに追加。 **show cluster history**	クラスタユニットがクラスタへの参加に失敗するか、クラスタを離脱する場合のために、新しいメッセージが **show cluster history** コマンドに追加されました。 サポートされるプラットフォーム：Firepower 4100/9300
Firepower Threat Defense：ルーティング	

機能	説明
仮想ルータと VRF-Lite	複数の仮想ルータを作成して、インターフェイスグループの個別のルーティングテーブルを管理できるようになりました。各仮想ルータには独自のルーティングテーブルがあるため、デバイスを流れるトラフィックを明確に分離できます。 仮想ルータは、Virtual Routing and Forwarding の「Light」バージョンである VRF-Lite を実装しますが、この VRF-Lite は Multiprotocol Extensions for BGP（MBGP）をサポートしていません。 作成できる仮想ルータの最大数は 5 ~ 100 の範囲で、デバイスのモデルによって異なります。完全なリストについては、『Firepower Management Center Configuration Guide』の「Virtual Routing for Firepower Threat Defense」の章を参照してください。 新規/変更されたページ：[デバイス（Devices）]>[デバイス管理（Device Management）]>[デバイスの編集（edit device）]>[ルーティング（Routing）] タブ 新しい FTD CLI コマンド：**show vrf**。 変更された FTD CLI コマンド：［**vrf** *name* ｜ **all**］キーワードセットを CLI コマンド **clear ospf**、**clear route**、**ping**、**show asp table routing**、**show bgp**、**show ipv6 route**、**show ospf**、**show route**、**show snort counters** に追加し、必要に応じて出力が仮想ルータ情報を表示するように変更しました。 サポートされるプラットフォーム：FTD（Firepower 1010 および ISA 3000 を除く）
Firepower Threat Defense：**VPN**	

機能	説明
リモートアクセス VPN 内の DTLS 1.2	Datagram Transport Layer Security（DTLS）1.2 を使用して、RA VPN 接続を暗号化できるようになりました。 FTD プラットフォーム設定を使用して、FTD デバイスが RA VPN サーバーとして動作するときに使用する最小 TLS プロトコルバージョンを指定します。また、DTLS 1.2 を指定する場合は、最小 TLS バージョンとして TLS 1.2 を選択する必要もあります。 Cisco AnyConnect セキュア モビリティ クライアント バージョン 4.7 以降が必要です。 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）] > [Threat Defense ポリシーの追加/編集（Add/Edit Threat Defense Policy）] > [SSL] > [DTLS バージョン（DTLS Version）] オプション サポートされるプラットフォーム：FTD（ASA 5508-X および ASA 5516-X を除く）
複数のピアに対するサイト間 VPN IKEv2 のサポート	IKEv1 と IKEv2 のポイントツーポイント エクストラネットおよびハブアンドスポークトポロジのために、サイト間 VPN 接続にバックアップピアを追加できるようになりました。これまで設定できたのは、IKEv1 ポイントツーポイント トポロジのバックアップピアのみでした。 新規/変更されたページ：[デバイス（Devices）] > [VPN] > [サイト間（Site To Site）] > [ポイントツーポイントまたはハブアンドスポーク FTD VPN トポロジの追加または編集（Add or Edit a Point to Point or Hub and Spoke FTD VPN Topology）] > [エンドポイントの追加（Add Endpoint）] > [IP アドレス（IP Address）] フィールドで、カンマ区切りのバックアップピアがサポートされるようになりました。 サポートされるプラットフォーム：FTD
セキュリティ ポリシー	

機能	説明
セキュリティポリシーの使いやすさの向上	バージョン 6.6.0 を使用すると、アクセス制御ルールとプレフィルタルールが簡単に使用できるようになります。次の作業に進んでください。 • 1 回の操作（状態、アクション、ロギング、侵入ポリシーなど）で、複数のアクセス制御ルールの特定の属性を編集します。 アクセス コントロール ポリシー エディタで、関連するルールを選択し、右クリックして [編集（Edit）] を選択します。 • 複数のパラメータによってアクセス制御ルールを検索します。 アクセス コントロール ポリシー エディタで、[ルールの検索（Search Rules）] テキストボックスをクリックしてオプションを表示します。 • アクセス制御ルールまたはプレフィルタルール内のオブジェクトの詳細と使用状況を表示します。 アクセス コントロール ポリシー エディタまたはプレフィルタ ポリシー エディタで、ルールを右クリックし、[オブジェクトの詳細（Object Details）] を選択します。 サポートされるプラットフォーム：FMC

機能	説明
アクセス コントロール ポリシーのオブジェクトグループ検索	動作中、FTD デバイスは、アクセスルールで使用されるネットワークオブジェクトの内容に基づいて、アクセス制御ルールを複数のアクセスコントロールリストのエントリに展開します。オブジェクトグループ検索を有効にすることで、アクセス制御ルールの検索に必要なメモリを抑えることができます。 オブジェクトグループ検索を有効にした場合、システムによってネットワークオブジェクトは拡張されませんが、オブジェクトグループの定義に基づいて一致するアクセスルールが検索されます。 オブジェクトグループ検索は、ルールがどのように定義されているかや、FMC にどのように表示されるかには影響しません。アクセス制御ルールと接続を照合するときに、デバイスがアクセス制御ルールを解釈して処理する方法のみに影響します。オブジェクトグループ検索はデフォルトで無効になっています。 新規/変更されたページ：[デバイス（Devices）]>[デバイス管理（Device Management）]>[デバイスの編集（Edit Device）]>[デバイス（Device）]タブ>[詳細設定（Advanced Settings）]>[オブジェクトグループ検索（Object Group Search）]オプション サポートされるプラットフォーム：FTD
アクセス コントロール ポリシーとプレフィルタポリシーの時間ベースのルール	適用するルールの絶対時間または反復時間、あるいは時間範囲を指定できるようになりました。このルールは、トラフィックを処理するデバイスのタイムゾーンに基づいて適用されます。 新規/変更されたページ： • アクセス コントロール ルール エディタまたはプレフィルタルールエディタ • [デバイス（Devices）]>[プラットフォーム設定（Platform Settings）]>[Threat Defenseポリシーの追加/編集（Add/Edit Threat Defense Policy）]>[タイムゾーン（Time Zone ）] • [オブジェクト（Objects）]>[オブジェクト管理（Object Management）]>[時間範囲（Time Range）]と[タイムゾーン（Time Zone）] サポートされるプラットフォーム：FTD

機能	説明
出力最適化の再有効化	**アップグレードの影響。** バージョン 6.6.0 では CSCvs86257 が修正されました。出力最適化が次のような状態だった場合があります。 • 有効になっていたがオフになり、アップグレードするとオンに戻る（機能が有効になっていた場合でも、バージョン 6.4.0 と 6.5.0 の一部のパッチでは出力最適化をオフにしていました）。 • 手動で無効にした場合は、アップグレード後に **asp inspect-dp egress-optimization** を使用して再度有効にすることをお勧めします。 サポートされるプラットフォーム：FTD
イベントロギングおよび分析	
新しいデータストアによるパフォーマンスが向上	**アップグレードの影響。** パフォーマンスを向上させるために、バージョン 6.6.0 では、接続およびセキュリティインテリジェンスイベントに新しいデータストアを使用します。 アップグレードが完了し、FMC がリブートすると、履歴接続イベントとセキュリティインテリジェンスイベントがバックグラウンドで移行され、リソースが制限されます。FMC モデル、システム負荷、および保存したイベント数に応じて、数時間から最大で 1 日かかることがあります。 履歴イベントは、経過時間ごとに、最新のイベントが最初に以降されます。移行されていないイベントは、クエリ結果やダッシュボードに表示されません。移行が完了する前に接続イベントデータベースの制限に達した場合（アップグレード後のイベントの場合など）、最も古い履歴イベントは移行されません。 イベントの移行の進行状況は、メッセージセンターでモニターできます。 サポートされるプラットフォーム：FMC
URL の接続イベントとセキュリティインテリジェンスイベントを検索する場合のワイルドカードのサポート	**`example.com`** のパターンを持つ URL の接続イベントとセキュリティインテリジェンスイベントを検索する場合は、ワイルドカードを含めなければならなくなりました。このような検索の場合、具体的には **`*example.com*`** を使用します。 サポートされるプラットフォーム：FMC

機能	説明
FTD デバイスを使用した最大 30 万の同時ユーザーセッションのモニタリング	バージョン 6.6.0 では、FTD デバイスモデルの一部で、同時ユーザーセッション（ログイン）のモニタリングが新たにサポートされるようになります。 • 30 万セッション：Firepower 4140、4145、4150、9300 • 15 万セッション：Firepower 2140、4112、4115、4120、4125 他のすべてのデバイスは、2,000 に制限されている ASA FirePOWER を除き、以前の 64,000 の制限を引き続きサポートします。 新しい正常性モジュールでは、ユーザー ID 機能のメモリ使用率が設定可能なしきい値に達したときに、アラートを発行します。また、時間の経過に伴うメモリ使用率のグラフも表示できます。 新規/変更されたページ： • [システム（System）] > [正常性（Health）] > [ポリシー（Policy）] > [正常性ポリシーを追加または編集（Add or Edit Health Policy）] > [Snort アイデンティティメモリ使用率（Snort Identity Memory Usage）] • [システム（System）] > [正常性（Health）] > [モニター（Monitor）] > デバイスの選択 > [Snort アイデンティティメモリ使用率（Snort Identity Memory Usage）] モジュールの [グラフ（Graph）] オプション サポートされるプラットフォーム：上記の FTD デバイス
IBM QRadar との統合	IBM QRadar 向けの新しい Cisco Firepower アプリケーションをイベントデータを表示するための代替手段として使用して、ネットワークへの脅威を分析、ハント、および調査をすることができます。eStreamer が必要です。 詳細については、Integration Guide for the Cisco Firepower App for IBM QRadarを参照してください。 サポートされるプラットフォーム：FMC
管理とトラブルシューティング	

機能	説明
設定変更を展開するための新しいオプション	FMC メニューバーの [展開（Deploy）] ボタンが次の機能を追加するオプションが備わったメニューになりました。 • [ステータス（Status）]：デバイスごとに、変更を展開する必要があるかどうか、展開前に解決する必要がある警告またはエラーがあるかどうか、最後の展開が処理中、失敗、正常に完了のうちのどの状態かが表示されます。 • [プレビュー（Preview）]：デバイスに対して最後に展開してから行った、適用可能なすべてのポリシーとオブジェクトの変更が表示されます。 • [展開の選択（Selective Deploy）]：管理対象デバイスに対して展開するポリシーと設定から選択します。 • [展開時間の見積もり（Deploy Time Estimate）]：特定のデバイスに対して展開するためにかかる時間の見積もりが表示されます。すべての展開のみでなく、特定のポリシーや設定の見積もりを表示することができます。 • [履歴（History）]： 以前の展開の詳細が表示されます。 新規/変更されたページ： • **[展開（Deploy）] > [展開（Deployment）]** • **[展開（Deploy）] > [展開履歴（Deployment History）]** サポートされるプラットフォーム：FMC

機能	説明
初期設定による VDB の更新と、SRU の更新のスケジュール設定	新規および再イメージ化された FMC では、セットアッププロセスは次のようになりました。 • 最新の脆弱性データベース（VDB）の更新をダウンロードしてインストールします。 • 毎日の侵入ルール（SRU）のダウンロードを有効にします。これらのダウンロード後は、セットアッププロセスで自動展開が有効にならないことに注意してください。ただし、この設定は変更できます。 アップグレードされた FMC は影響を受けません。 新規/変更されたページ： • [システム（System）] > [更新（Updates）] > [製品の更新（VDB の更新）（Product Updates (VDB updates)）] • [システム（System）] > [更新（Updates）] > [ルールの更新（SRU の更新）（Rule Updates (SRU updates)）] サポートされるプラットフォーム：FMC
FMC を復元するための VDB の一致は不要	バックアップからの FMC の復元に交換用 FMC 上に同じ VDB を使用する必要はなくなりました。ただし、復元すると、既存の VDB がバックアップファイル内の VDB に置き換えられます。 サポートされるプラットフォーム：FMC
サブジェクト代替名（SAN）を使用した HTTPS 証明書	SAN を使用して複数のドメイン名または IP アドレスを保護する HTTPS サーバー証明書を要求できるようになりました。SAN の詳細については、RFC 5280、セクション 4.2.1.6 を参照してください。 新規/変更されたページ：[システム（System）] > [設定（Configuration）] > [HTTPS 証明書（HTTPS Certificate）] > [新しい CSR の生成（Generate New CSR）] > [サブジェクト代替名（Subject Alternative Name）] フィールド サポートされるプラットフォーム：FMC

機能	説明
FMC ユーザーアカウントに関連付けられている実名	FMC ユーザーアカウントを作成または変更するときに、実名を指定できるようになりました。これには、個人名、部署名、またはその他の識別属性を指定できます。 新規/変更されたページ：[システム（System）] > [ユーザー（Users）] > [ユーザー（Users）] > [実名（Real Name）] フィールド サポートされるプラットフォーム：FMC
追加の FTD プラットフォームでの Cisco Support Diagnostics	**アップグレードの影響。** Cisco Support Diagnostics は、すべての FMC および FTD デバイスで完全にサポートされるようになりました。以前は、サポートは FMC、FTD 搭載 Firepower 4100/9300、および Azure 向け FTDv に限定されていました。詳細については、「シスコとのデータの共有 （3 ページ）」を参照してください。 サポートされるプラットフォーム：FMC、FTD
ユーザビリティ	
ライトテーマ	FMC はデフォルトでバージョン 6.5.0 のベータ機能として導入されたライトテーマに設定されます。バージョン 6.6.0 にアップグレードすると、ライトテーマに自動的に切り替わります。これは、ユーザー設定で従来のテーマに戻すことができます。 すべてに返信することはできませんが、ライトテーマについてのフィードバックを歓迎します。[ユーザー設定（User Preferences）] ページのフィードバックリンクを使用するか、fmc-light-theme-feedback@cisco.com からフィードバックをお送りください。 サポートされるプラットフォーム：FMC
アップグレードの残り時間の表示	FMC のメッセージセンターに、アップグレードが完了するまでのおおよその残り時間が表示されるようになりました。これには、リブート時間は含まれません。 新規/変更されたページ：メッセージセンター 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
デフォルトのHTTPSサーバー証明書の更新期限は 800 日	**アップグレードの影響。** 現在のデフォルトの HTTPS サーバー証明書がすでに 800 日である場合を除き、バージョン6.6.0にアップグレードすることで証明書が更新され、有効期限がアップグレード日から 800 日後になりました。今後の更新はすべて、有効期間が 800 日になります。 古い証明書は、生成日に応じて期限切れになるように設定されていました。 サポートされるプラットフォーム：FMC
Firepower Management Center REST API	
新しい REST API 機能	バージョン 6.6.0 の機能をサポートするための次の REST API サービスが追加されました。 • bgp、bgpgeneralsettings、ospfinterface、ospfv2routes、ospfv3interfaces、ospfv3routes、virtualrouters、routemaps、ipv4prefixlists、ipv6prefixlists、aspathlists、communitylists、extendedcommunitylists、standardaccesslists、standardcommunitylists、policylists：ルーティング • virtualrouters、virtualipv4staticroutes、virtualipv6staticroutes、virtualstaticroutes：仮想ルーティング • timeranges、globaltimezones、timezoneobjects：時間ベースのルール • commands：REST API から CLI コマンドの限定的なセットを実行 • pendingchanges：保留中の改善点を展開 古い機能をサポートするために、次の REST API サービスが追加されました。 • intrusionrules、intrusionpolicies：侵入ポリシー サポートされるプラットフォーム：FMC

機能	説明
拡張アクセスリストの REST API サービス名を変更	**アップグレードの影響。** FMC REST API の extendedaccesslist（単数形）サービスは、extendedaccesslists（複数形）になりました。クライアントを更新していることを確認します。古いサービス名を使用すると失敗し、無効な URL エラーが返されます。 要求タイプ：GET 特定の ID に関連付けられている拡張アクセスリストを取得するための URL： • 旧：/api/fmc_config/v1/domain/{domainUUID}/object/extendedaccesslist/{objectId} • 新：/api/fmc_config/v1/domain/{domainUUID}/object/extendedaccesslists/{objectId} すべての拡張アクセスリストを取得するための URL： • 旧：/api/fmc_config/v1/domain/{domainUUID}/object/extendedaccesslist • 新：/api/fmc_config/v1/domain/{domainUUID}/object/extendedaccesslists サポートされるプラットフォーム：FMC

FDM バージョン 6.6 の新機能

表 *10 : FDM* バージョン *6.6.0* の新機能

機能	説明
プラットフォーム機能	
Amazon Web Services（AWS）クラウド用 FTDv における FDM のサポート。	FDM を使用して AWS クラウド用 FTDv で FTD を設定できます。
Firepower 4112 用 FDM	Firepower 4112 用 FTD が導入されました。 （注）　FXOS 2.8.1 が必要です。
ファイアウォールと IPS の機能	

機能	説明
デフォルトでは無効になっている、侵入ルールを有効にする機能。	各システム定義の侵入ポリシーには、デフォルトで無効になっているルールがいくつかあります。以前は、これらのルールのアクションをアラートまたはドロップに変更できませんでした。現在では、デフォルトで無効になっているルールのアクションを変更できるようになりました。 [侵入ポリシー（Intrusion Policy）] ページが変更され、デフォルトで無効になっているルールもすべて表示されるようになりました。また、これらのルールのアクションも編集できます。
侵入ポリシーの侵入検知システム（IDS）モード。	侵入検知システム（IDS）モードで動作するように侵入ポリシーを設定できるようになりました。IDS モードでは、アクティブな侵入ルールは、ルールアクションがドロップであってもアラートのみを発行します。したがって、侵入ポリシーをネットワーク内でアクティブな防御ポリシーにする前に、その侵入ポリシーの動作をモニタリングまたはテストできます。 FDM では、**[ポリシー（Policies）]** > **[侵入（Intrusion）]** ページの各侵入ポリシーに、検査モードの表示が追加されました。また [編集（Edit）] リンクが追加され、モードを変更できるようになりました。 FTD API では、IntrusionPolicy リソースに inspectionMode 属性が追加されました。
脆弱性データベース（VDB）、地理位置情報データベース、および侵入ルールの更新パッケージを手動でアップロードするためのサポート。	VDB、地理位置情報データベース、および侵入ルールの更アップデートパッケージを手動で取得し、FDM を使用してワークステーションから FTD デバイスにアップロードできるようになりました。たとえば、FDM で Cisco Cloud から更新を取得できないエアギャップネットワークがある場合でも、必要な更新パッケージを入手できます。 ワークステーションからファイルを選択してアップロードできるように、**[デバイス（Device）]** > **[更新（Updates）]** ページが更新されました。

機能	説明
FTD 時間に基づいて制限されているアクセス制御ルールの API サポート。	FTD API を使用して、時間範囲オブジェクトを作成できます。このオブジェクトでは、1 回限りの時間範囲または繰り返しの時間範囲を指定します。オブジェクトはアクセス制御ルールに適用します。時間範囲を使用すると、特定の時間帯または一定期間にわたってトラフィックにアクセス制御ルールを適用して、ネットワークを柔軟に使用できます。FDM を使用して時間範囲を作成したり、適用したりはできません。また、アクセス制御ルールに時間範囲が適用されている場合、FDM は表示されません。 TimeRangeObject、Recurrence、TimeZoneObject、DayLightSavingDateRange、および DayLightSavingDayRecurrence リソースが FTD API に追加されました。時間範囲をアクセス制御ルールに適用するために、timeRangeObjects 属性が accessrules リソースに追加されました。さらに、GlobalTimeZone および TimeZone リソースに変更が加えられました。
アクセス コントロール ポリシーのオブジェクトグループ検索。	動作中、FTD デバイスは、アクセスルールで使用されるネットワークオブジェクトの内容に基づいて、アクセス制御ルールを複数のアクセス制御リストのエントリに展開します。オブジェクトグループ検索を有効にすることで、アクセス制御ルールの検索に必要なメモリを抑えることができます。オブジェクトグループ検索を有効にした場合、システムによってネットワークオブジェクトは拡張されませんが、オブジェクトグループの定義に基づいて一致するアクセスルールが検索されます。オブジェクトグループ検索は、アクセスルールがどのように定義されるか、または FDM にどのように表示されるかには影響しません。アクセス制御ルールと接続を照合するときに、デバイスがアクセス制御ルールを解釈して処理する方法のみに影響します。オブジェクトグループ検索はデフォルトで無効になっています。 FDM では、FlexConfig を使用して **object-group-search access-control** コマンドを有効にする必要があります。
VPN 機能	

機能	説明
サイト間 VPN のバックアップピア（FTD API のみ）。	FTD API を使用して、サイト間 VPN 接続にバックアップピアを追加できます。たとえば、2 つの ISP がある場合は、最初の ISP への接続が使用できなくなった場合に、バックアップ ISP にフェールオーバーするように VPN 接続を設定できます。 バックアップピアのもう 1 つの主な用途は、プライマリハブやバックアップハブなど、トンネルのもう一方の端に 2 つの異なるデバイスがある場合です。通常、システムはプライマリハブへのトンネルを確立します。VPN 接続が失敗すると、システムはバックアップハブとの接続を自動的に再確立できます。 SToSConnectionProfile リソースで outsideInterface に対して複数のインターフェイスを指定できるように、FTD API が更新されました。また、BackupPeer リソースと remoteBackupPeers 属性が SToSConnectionProfile リソースに追加されました。 FDM を使用してバックアップピアを設定したり、バックアップピアの存在を FDM に表示したりはできません。
リモートアクセス VPN での Datagram Transport Layer Security（DTLS）1.2 のサポート。	リモートアクセス VPN で DTLS 1.2 を使用できるようになりました。これは、FTD API のみを使用して設定できます。FDM を使用して設定することはできません。ただし、DTLS 1.2 はデフォルトの SSL 暗号グループの一部になったため、グループポリシーの AnyConnect 属性で FDM を使用して DTLS の一般的な使用が可能になりました。DTLS 1.2 は、ASA 5508-X または 5516-X モデルではサポートされていないことに注意してください。 DTLSV1_2 を列挙値として受け入れるように sslcipher リソースの protocolVersion 属性が更新されました。
安全性の低い Diffie-hellman グループ、および暗号化アルゴリズムとハッシュアルゴリズムのサポートを廃止。	次の機能は廃止されており、将来のリリースでは削除されます。VPN で使用するために、IKE プロポーザルまたは IPSec ポリシーでこれらの機能を設定しないでください。これらの機能から移行し、実用可能になったらすぐにより強力なオプションを使用してください。 • Diffie-Hellman グループ：2、5、および 24。 • 強力な暗号化の輸出規制を満たすユーザー向けの暗号化アルゴリズム：DES、3DES、AES-GMAC、AES-GMAC-192、AES-GMAC-256。輸出規制を満たしていないユーザーの場合、DES は引き続きサポートされます（これが唯一のオプションです）。 • ハッシュアルゴリズム：MD5。

機能	説明
ルーティング機能	
仮想ルータと Virtual Routing and Forwarding（VRF）-Lite。	複数の仮想ルータを作成して、インターフェイスグループの個別のルーティングテーブルを管理できます。各仮想ルータには独自のルーティングテーブルがあるため、デバイスを流れるトラフィックを明確に分離できます。 仮想ルータは、Virtual Routing and Forwarding の「Light」バージョンである VRF-Lite を実装しますが、この VRF-Lite は Multiprotocol Extensions for BGP（MBGP）をサポートしていません。 [ルーティング（Routing）] ページが変更され、仮想ルータを有効化できるようになりました。有効にすると、[ルーティング（Routing）]ページに仮想ルータのリストが表示されます。仮想ルータごとに個別のスタティックルートとルーティングプロセスを設定できます。 また、［**vrf** *name* | **all**］キーワードセットを次の CLI コマンドに追加し、必要に応じて出力が仮想ルータ情報を表示するよう変更しました。**clear ospf**、**clear route**、**ping**、**show asp table routing**、**show bgp**、**show ipv6 route**、**show ospf**、**show route**、**show snort counters** **show vrf** コマンドが追加されました。
OSPF および BGP の設定を [Routing] ページに移動しました。	以前のリリースでは、スマート CLI を使用して、[詳細設定（Advanced Configuration）] ページで OSPF と BGP を設定しました。これらのルーティングプロセスは、これまでと同様にスマート CLI を使って設定しますが、そのオブジェクトを [ルーティング（Routing）] ページで直接使用できるようになりました。これにより、仮想ルータごとにプロセスを簡単に設定できます。 OSPF および BGP スマート CLI オブジェクトは、[詳細設定（Advanced Configuration）] ページでは使用できなくなりました。6.6 にアップグレードする前に、これらのオブジェクトを設定した場合は、アップグレード後に [ルーティング（Routing）] ページでそれらのオブジェクトを見つけることができます。
高可用性機能	

機能	説明
高可用性（HA）ペアのスタンバイ装置にログインする外部認証ユーザーの制限を削除。	以前は、外部認証されたユーザーは HA ペアのスタンバイユニットに直接ログインできませんでした。スタンバイユニットへのログインが可能になる前は、ユーザーは最初にアクティブ装置にログインしてから、設定を展開する必要がありました。 この制約は削除されました。外部認証されたユーザーは、有効なユーザー名/パスワードを提供している限り、アクティブ装置にログインしていない場合でも、スタンバイ装置にログインできます。

機能	説明
FTD API の BreakHAStatus リソースによって、インターフェイスがどのように処理されるかが変更。	以前は、**clearIntfs** クエリパラメータを含めて、高可用性（HA）設定を中断するデバイス上のインターフェイスの動作ステータスを制御できました。 バージョン 6.6 以降では、clearIntfs クエリパラメータの代わりに使用する新しい属性 **interfaceOption** があります。この属性は、アクティブノードで使用する場合はオプションですが、非アクティブノードで使用する場合は必須です。次の 2 つのオプションのいずれかを選択できます。 • DISABLE_INTERFACES（デフォルト）：スタンバイデバイス（またはこのデバイス）上のすべてのデータインターフェイスが無効になります。 • ENABLE_WITH_STANDBY_IP：インターフェイスにスタンバイ IP アドレスを設定すると、スタンバイデバイス（またはこのデバイス）上のインターフェイスがスタンバイアドレスを使用するよう再設定されます。スタンバイアドレスを持たないインターフェイスはすべて無効になります。 デバイスが正常なアクティブ/スタンバイ状態になっているときにアクティブノードで [HAの中断（Break HA）] を使用すると、この属性がスタンバイノードのインターフェイスに適用されます。アクティブ/アクティブまたは一時停止などのその他の状態では、この属性が中断を開始するノードに適用されます。 clearIntfs クエリパラメータを使用する場合、clearIntfs=true は interfaceOption = DISABLE_INTERFACES のように動作します。つまり、clearIntfs=true のアクティブ/スタンバイペアを中断すると、両方のデバイスが無効にはならなくなり、スタンバイデバイスのみが無効になります。 FDM を使用して HA を中断すると、インターフェイスオプションには常に DISABLE_INTERFACES が設定されます。スタンバイ IP アドレスを使用してインターフェイスを有効にすることはできません。異なる結果が必要な場合は、API エクスプローラから API コールを使用します。
高可用性の問題の直近の失敗理由を [高可用性（High Availability）] ページに表示。	高可用性（HA）が何らかの理由で失敗した場合（アクティブデバイスが使用できなくなり、スタンバイデバイスにフェールオーバーするなど）、直近の失敗の理由がプライマリデバイスとセカンダリデバイスのステータス情報の下に表示されます。この情報には、イベントの UTC 時刻が含まれます。

機能	説明
インターフェイス機能	
PPPoE のサポート。	ルーテッドインターフェイスの PPPoE を設定できるようになりました。PPPoE は、ハイアベイラビリティ ユニットではサポートされません。 新規/変更された画面：**[デバイス（Device）] > [インターフェイス（Interfaces）] > [編集（Edit）] > [IPv4 アドレス（IPv4 Address）] > [タイプ（Type）] > [PPPoE]** 新規/変更されたコマンド：**show vpdn group、show vpdn username、show vpdn session pppoe state**
デフォルトでは DHCP クライアントとして機能する管理インターフェイス。	管理インターフェイスは、192.168.45.45 IP アドレスを使用する代わりに、デフォルトでは DHCP から IP アドレスを取得するように設定されています。この変更により、既存のネットワークに FTD を簡単に展開できるようになりました。この機能は、Firepower 4100/9300（論理デバイスを展開するときに IP アドレスを設定する）と FTDv および ISA 3000（現在も 192.168.45.45 IP アドレスを使用）を除くすべてのプラットフォームに適用されます。管理インターフェイス上の DHCP サーバーも有効にならなくなりました。 デフォルト（192.168.1.1）では、デフォルトの内部 IP アドレスに引き続き接続できます。
FDM 管理接続の HTTP プロキシサポート。	FDM 接続で使用するために、管理インターフェイスの HTTP プロキシを設定できるようになりました。手動およびスケジュールされたデータベースの更新を含むすべての管理接続は、プロキシを通過します。 設定するための **[システム設定（System Setting）] > [HTTP プロキシ（HTTP Proxy）]** ページが追加されました。さらに、HTTPProxy リソースが FTD API に追加されました。
管理インターフェイスの MTU の設定。	管理インターフェイスの MTU を最大 1500 バイトに設定できるようになりました。デフォルト値は 1500 バイトです。 新規/変更されたコマンド：**configure network mtu、configure network management-interface mtu-management-channel** 変更された画面はありません。
ライセンシング機能	

機能	説明
スマートライセンシングとクラウドサービスの登録は分離され、登録を個別に管理可能	スマートライセンスアカウントではなく、セキュリティアカウントを使用して、クラウドサービスを登録できるようになりました。Cisco Defense Orchestrator を使用してデバイスを管理する場合は、セキュリティアカウントを使用して登録することを推奨します。スマートライセンシングから登録解除せずに、クラウドサービスから登録解除することもできます。 **[システム設定（System Settings）]**>**[クラウドサービス（Cloud Services）]** ページの動作を変更し、クラウドサービスから登録解除する機能を追加しました。さらに、このページからWeb分析機能が削除されました。この機能は、**[システム設定（System Settings）]** > **[Web分析（Web Analytics）]** ページに移動しました。FTD API では、新しい動作を反映するようにCloudServices リソースが変更されました。
パーマネントライセンス予約のサポート。	インターネットへのパスがないエアギャップネットワークがある場合は、スマートライセンスのためにCisco Smart Software Manager（CSSM）に直接登録することはできません。この場合は、ユニバーサル パーマネント ライセンス予約（PLR）モードを使用できるようになりました。このモードでは、CSSM との直接通信を必要としないライセンスを適用できます。エアギャップネットワークがある場合は、アカウント担当者に問い合わせて、CSSM アカウントでユニバーサル PLR モードを使用して必要なライセンスを取得することを許可するように依頼してください。ISA 3000 はユニバーサル PLR をサポートしていません。 **[デバイス（Device）]**>**[スマートライセンス（Smart License）]** ページに、PLR モードに切り替えたり、ユニバーサル PLR ライセンスをキャンセルしたりして登録解除する機能が追加されました。FTD API では、PLRAuthorizationCode、PLRCode、PLRReleaseCode、PLRRequestCode の新しいリソースと、PLRRequestCode、InstallPLRCode、およびCancelReservation のアクションが追加されました。
管理およびトラブルシューティングの機能	

機能	説明
ISA 3000 デバイスの高精度時間プロトコル（PTP）設定用 FDM 直接サポート。	FDM を使用して、ISA 3000 デバイスで高精度時間プロトコル（PTP）を設定できます。PTP は、パケットベースネットワーク内のさまざまなデバイスのクロックを同期するために開発された時間同期プロトコルです。このプロトコルは、ネットワーク化された産業用の測定および制御システム向けとして特別に設計されています。以前のリリースでは、PTP を設定するために FlexConfig を使用する必要がありました。 同じ [システム設定（System Settings）] ページの PTP と NTP をグループ化し、**[システム設定（System Settings）] > [NTP]** ページの名前を [タイムサービス（Time Services）] に変更しました。また、PTP リソースが FTD API に追加されました。
FDM 管理 Web サーバー証明書の信頼チェーン検証。	FDM Web サーバーの非自己署名証明書を設定する場合は、すべての中間証明書とルート証明書を信頼チェーンに含める必要があります。システムはチェーン全体を検証します。 **[デバイス（Device）] > [システム設定（System Settings）] > [管理アクセス（Management Access）]** ページの [管理Webサーバー（Management Web Server）] タブに、チェーン内の証明書を選択する機能が追加されました。
バックアップファイルの暗号化のサポート。	パスワードを使用して、バックアップファイルを暗号化できるようになりました。暗号化されたバックアップを復元するには、正しいパスワードを指定する必要があります。 定期的なジョブ、スケジュール済みジョブ、および手動ジョブのバックアップファイルを暗号化するかどうかを選択し、復元時にパスワードを提供する機能が、**[デバイス（Device）] > [バックアップと復元（Backup and Restore）]** ページに追加されました。また、encryptArchive 属性と encryptionKey 属性が BackupImmediate と BackupSchedule リソースに追加され、encryptionKey が FTD API の RestoreImmediate リソースに追加されました。

機能	説明
クラウドサービスで使用するために Cisco Cloud に送信するイベントを選択するサポート。	Cisco Cloud にイベントを送信するようデバイスを設定すると、送信するイベントのタイプ（侵入、ファイル/マルウェア、接続）を選択できるようになりました。接続イベントの場合、すべてのイベントを送信することも、優先順位の高いイベント（侵入、ファイル、またはマルウェアイベントをトリガーする接続に関連するもの、またはセキュリティ インテリジェンスブロッキングポリシーと一致するもの）を送信することもできます。 [Cisco Cloudへのイベントの送信を有効にする（Send Events to the Cisco Cloud Enable）] ボタンが機能するよう変更されました。この機能は、**[システム設定（System Settings）] > [クラウドサービス（Cloud Services）]** ページにあります。
FTD REST API バージョン 5（v5）。	ソフトウェアバージョン 6.6 用の FTD REST API のバージョン番号が 5 になりました。API URL の v1/v2/v3/v4 を v5 に置き換える必要があります。または、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します。 v5 の API には、ソフトウェアバージョン 6.6 で追加されたすべての機能に対応する多数の新しいリソースが含まれています。使用しているリソースモデルに変更が加えられている可能性があるため、既存のすべての呼び出しを再評価してください。リソースを表示できる API エクスプローラを開くには、FDM にログインして、[詳細オプション（More options）] ボタン（⋮）をクリックし、[APIエクスプローラ（API Explorer）] を選択します。

バージョン 6.6 の新しいハードウェアと仮想プラットフォーム

表 *11* : バージョン *6.6.0* 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
Firepower 4112 上の FTD。	Firepower 4112 が導入されました。このプラットフォームでは、ASA 論理デバイスを展開することもできます。FXOS 2.8.1 が必要です。

機能	説明
AWS の展開用の大型のインスタンス。	**アップグレードの影響。** FTDv for AWS により、次の大型のインスタンスのサポートが追加されています。 • C5.xlarge • C 5.2 xlarge • C5.4xlarge FMCv for AWS により、次の大型のインスタンスのサポートが追加されています。 • C3.4xlarge • C4.4xlarge • C5.4xlarge AWS インスタンスタイプ用の既存のすべての FMCv が廃止されました。アップグレードする前に、サイズを変更する必要があります。詳細については、FMCv をアップグレードするには 28 GB の RAM が必要 （52 ページ）を参照してください。

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

（注） バージョン 6.6 は、Cisco Firepower User Agent ソフトウェアをアイデンティティソースとしてサポートする最後のリリースです。ユーザーエージェント設定を使用して FMC をバージョン 6.7 以降 にアップグレードすることはできません。Cisco Identity Services Engine/Passive Identity Connector（ISE/ISE-PIC）に切り替える必要があります。これにより、ユーザー エージェントで使用できない機能も利用できるようになります。ライセンスを変換するには、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。

詳細については、Cisco Firepower User Agent のサポート終了 [英語] 通知、および Firepower ユーザー ID：ユーザーエージェントから Identity Services Engine への移行 [英語] の技術メモを参照してください。

FMC バージョン 6.6 で廃止された機能

表 *12 : FMC* バージョン *6.6.1* で廃止された機能

機能	アップグレードの影響	説明
ルールが競合してもカスタム侵入ルールのインポートが失敗しない。	なし	バージョン 6.6.0 では、ルールの競合があった場合、FMC はカスタム（ローカル）侵入ルールのインポートの完全な拒否を開始しました。バージョン 6.6.1 ではこの機能を廃止し、競合が発生したルールをサイレントでスキップする、バージョン 6.6 より前の動作に戻ります。 既存のルールと同じ SID/リビジョン番号を持つ侵入ルールをインポートしようとすると、競合が発生することに注意してください。カスタムルールの更新バージョンには必ず新しいリビジョン番号を付けてください。FMC コンフィギュレーション ガイドでローカル侵入ルールをインポートするためのベストプラクティスを参考にすることを推奨します。 バージョン 6.7 では、ルールの競合に関する警告が追加されます。

表 *13 : FMC* バージョン *6.6.0* で廃止された機能

機能	アップグレードの影響	説明
VMware 向け FTDv の e1000 インターフェイス。	アップグレードされないようにします。	バージョン 6.6 では、VMware 向け FTDv の e1000 インターフェイスのサポートを終了します。vmxnet3 または ixgbe インターフェイスに切り替えるまで、アップグレードすることはできません。または、新しいデバイスを展開できます。 詳細については、『VMware 向け Cisco Secure Firewall Threat Defense Virtual スタートアップガイド』を参照してください。
安全性の低い Diffie-Hellman グループ、暗号化アルゴリズム、およびハッシュアルゴリズム。	なし。ただし、今すぐ切り替える必要があります。	バージョン 6.6 では、次の FTD セキュリティ機能は廃止されます。 • Diffie-Hellman グループ：2、5、および 24。 • 強力な暗号化の輸出規制を満たすユーザー向けの暗号化アルゴリズム：DES、3DES、AES-GMAC、AES-GMAC-192、AES-GMAC-256。輸出規制を満たしていないユーザーの場合、DES は引き続きサポートされます（これが唯一のオプションです）。 • ハッシュアルゴリズム：MD5。 これらの機能はバージョン 6.7 で廃止されました。VPN で使用するために、IKE プロポーザルまたは IPSec ポリシーでこれらの機能を設定しないでください。できるだけ強力なオプションに変更してください。
接続イベントのカスタムテーブル。	サポートされていないカスタムテーブルは削除する必要があります。	バージョン 6.6 は、接続イベントとセキュリティ インテリジェンス イベントのカスタムテーブルのサポートを終了します。アップグレード後は、これらのイベントの既存のカスタムテーブルは引き続き「利用可能」ですが、結果は返されません。これらのテーブルを削除することをお勧めします。 他のタイプのカスタムテーブルに変更はありません。 廃止されたオプション： • [分析（Analysis）] > [詳細設定（Advanced）] > [カスタムテーブル （Custom Tables）] > [カスタムテーブルの作成（Create Custom Table）] > [テーブル（Tables）] ドロップダウンリスト > [接続イベント（Connection Events）] と、[セキュリティ インテリジェンス イベント（Security Intelligence Events）] のクリック

機能	アップグレードの影響	説明
イベントビューアから接続イベントを削除する機能。	なし。	バージョン6.6は、接続イベントとセキュリティインテリジェンス イベントをイベントビューアから削除するためのサポートを終了しています。データベースを消去するには、**[システム（System）] > [ツール（Tools）] > [データの消去（Data purge）]** を選択します。 廃止されたオプション： • **[分析（Analysis）] > [接続（Connections）] > [イベント（Events）]** > [削除（Delete）] と [すべて削除（Delete All）] • **[分析（Analysis）] > [接続（Connections）] > [セキュリティ インテリジェンス イベント（Security Intelligence Events）]** > [削除（Delete）] と [すべて削除（Delete All）]
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。

FDM バージョン 6.6 で廃止された機能

表 *14 : FDM* バージョン *6.6.0* で廃止された機能

機能	アップグレードの影響	説明
VMware 向け FTDv の e1000 インターフェイス。	アップグレードされないようにします。	バージョン 6.6 では、VMware 向け FTDv の e1000 インターフェイスのサポートを終了します。vmxnet3 または ixgbe インターフェイスに切り替えるまで、アップグレードすることはできません。または、新しいデバイスを展開できます。 詳細については、『VMware 向け Cisco Secure Firewall Threat Defense Virtual スタートアップガイド』を参照してください。
安全性の低い Diffie-Hellman グループ、暗号化アルゴリズム、およびハッシュアルゴリズム。	なし。ただし、今すぐ切り替える必要があります。	バージョン 6.6 では、次の FTD セキュリティ機能は廃止されます。 • Diffie-Hellman グループ：2、5、および 24。 • 強力な暗号化の輸出規制を満たすユーザー向けの暗号化アルゴリズム：DES、3DES、AES-GMAC、AES-GMAC-192、AES-GMAC-256。輸出規制を満たしていないユーザーの場合、DES は引き続きサポートされます（これが唯一のオプションです）。 • ハッシュアルゴリズム：MD5。 これらの機能はバージョン 6.7 で廃止されました。VPN で使用するために、IKE プロポーザルまたは IPSec ポリシーでこれらの機能を設定しないでください。できるだけ強力なオプションに変更してください。

バージョン 6.6 で廃止されたハードウェアと仮想プラットフォーム

表 *15* : バージョン *6.6.0* 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
クラウドベースの FMCv 展開でのメモリ不足のインスタンス。	パフォーマンス上の理由から、次の FMCv インスタンスはサポートされなくなりました。 • AWS での c3.xlarge • AWS での c3.2xlarge • AWS での c4.xlarge • AWS での c4.2xlarge • Azure での Standard_D3_v2 バージョン 6.6.0+ にアップグレードする前に、サイズを変更する必要があります。詳細については、FMCv をアップグレードするには 28 GB の RAM が必要 （52 ページ）を参照してください。 さらに、バージョン 6.6 リリースの時点で、クラウドベースの FMCv の展開におけるメモリ不足のインスタンスタイプが完全に廃止されました。以前の Firepower バージョンであっても、これらを使用して新しい FMCv 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。

廃止された FlexConfig コマンド

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

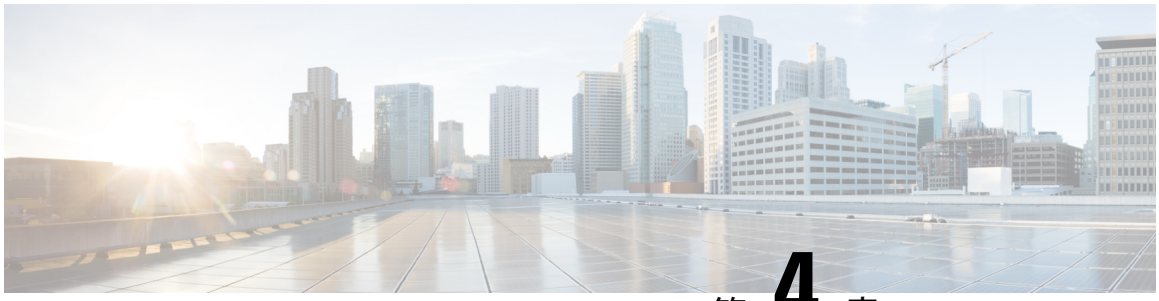
注意 ほとんどの場合、既存の FlexConfig 設定はアップグレード後も引き続き機能し、展開ができます。ただし、廃止されたコマンドを使用すると、展開の問題が発生する場合があります。

FlexConfig について

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

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

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



第 4 章

ソフトウェアのアップグレード

この章では、重要なリリースに固有の情報を提供します。

アップグレードの計画

誤りを避けるには、注意深い計画と準備が役立ちます。この表はアップグレードの計画プロセスを要約したものです。詳細なチェックリストと手順については、該当するアップグレードまたは設定ガイドのを参照してください：アップグレード手順 （79 ページ）

表 *16*：アップグレードの計画フェーズ

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

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

アップグレードする最小バージョン

次のように Version6.6.x に直接アップグレードできます。特定のメンテナンスリリースまたはパッチレベルを実行する必要はありません。

表 *17 :* バージョン *6.6.0/6.6.x* にアップグレードするための最小バージョン

プラットフォーム	最小バージョン
Firepower Management Center	6.2.3
FMC を使用した Firepower デバイス	6.2.3 FXOS 2.8.1.105 以降のビルド （Firepower 4100/9300 に必要）。
FDM を搭載した Firepower デバイス	6.2.3

プラットフォーム	最小バージョン
ASDM を使用した ASA FirePOWER	6.3.0 CSCvu50400 のため、ASDM 搭載の ASA FirePOWER をバージョン 6.2.3.x から 6.6.0 へ直接アップグレードしないでください。アップグレードは成功しますが、重大なパフォーマンスの問題が発生するため、Cisco TAC に連絡して修正を依頼する必要があります。代わりに、中間リリースにアップグレードしてから、バージョン 6.6.0 にアップグレードする必要があります。または、バージョン 6.2.3.x → バージョン 6.6.1 またはその他のバージョン 6.6.x メンテナンスリリースへ直接アップグレードできます。

メンテナンスリリースの新しいアップグレードガイドライン

本チェックリストには、バージョン 6.6.x のメンテナンスリリースの新規または固有のアップグレードガイドラインが含まれています。

表 *18* : バージョン *6.6.x* の新しいガイドライン

✓	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
	アップグレード禁止：FMC バージョン 6.6.5 以降からバージョン 6.7.0 （49 ページ）	FMC	6.6.5 以降 6.6.x リリース	6.7.0 のみ

アップグレード禁止：FMC バージョン 6.6.5 以降からバージョン 6.7.0

展開：FMC

アップグレード元：バージョン 6.6.5 以降のメンテナンスリリース

直接アップグレード先：バージョン 6.7.0 のみ

バージョン 6.6.5 以降の 6.6.x メンテナンスリリースからバージョン 6.7.0 にアップグレードすることはできません。これは、バージョン 6.6.5 のデータストアがバージョン 6.7.0 のデータストアよりも新しいためです。バージョン 6.6.5 以降を実行している場合は、バージョン 7.0.0 以降に直接アップグレードすることをお勧めします。

以前に公開されたアップグレードガイドライン

このチェックリストには、バージョン 6.6.0 の新規または固有のアップグレードガイドラインが含まれています。

表 *19* : バージョン *6.6.0* の新しいガイドライン

✓	ガイドライン	プラットフォーム	アップグレード元	直接アップグレード先
	アップグレードの失敗：侵入イベントに関する電子メールアラート機能を搭載した FMC （51 ページ）	FMC	6.2.3 ～ 6.7.0.x	6.7.0 6.6.0、6.6.1、6.6.3 これらのリリースに対するすべてのパッチ
	FMCv をアップグレードするには 28 GB の RAM が必要 （52 ページ）	FMCv	6.2.3 ～ 6.5.0.x	6.6.0 以降

このチェックリストには、古いアップグレードガイドラインが含まれています。

表 *20* : 以前に公開されたバージョン *6.6.0* のガイドライン

✓	ガイドライン	プラットフォーム	アップグレード元	直接アップグレード先
	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 （53 ページ）	Firepower 1000 シリーズ	6.4.0	6.5.0 以降
	FTD/FDM アップグレード時に削除される履歴データ （54 ページ）	FDM を使用した FTD	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 （54 ページ）	任意（Any）	6.2.3 ～ 6.4.0.x	6.5.0 以降
	TLS 暗号化アクセラレーションの有効化/無効にすることは不可 （62 ページ）	Firepower 2100 シリーズ Firepower 4100/9300	6.2.3 ～ 6.3.0.x	6.4.0 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
	FMC、NGIPSv で準備状況チェックに失敗する可能性 （62 ページ）	FMC NGIPSv	6.1.0 ～ 6.1.0.6 6.2.0 ～ 6.2.0.6 6.2.1 6.2.2 ～ 6.2.2.4 6.2.3 ～ 6.2.3.4	6.3.0 以降
	リモートアクセス VPN のデフォルト設定の変更によって VPN トラフィックがブロックされる可能性（63 ページ）	FMC を使用した FTD	6.2.0 ～ 6.2.3.x	6.3.0 以降
	セキュリティ インテリジェンスによって可能になるアプリケーションの識別 （63 ページ）	FMC の展開	6.1.0 ～ 6.2.3.x	6.3.0 以降
	アップグレード後に VDB を更新して CIP 検出を有効化 （64 ページ）	任意（Any）	6.1.0 ～ 6.2.3.x	6.3.0 以降
	無効な侵入変数セットによって展開に失敗する可能性 （64 ページ）	任意（Any）	6.1.0 ～ 6.2.3.x	6.3.0 以降

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

展開：Firepower Management Center

アップグレード元：バージョン 6.2.3 ～ 6.7.0.x

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

関連するバグ：CSCvw38870、CSCvx86231

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

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

侵入に関する電子メールアラートを完全に無効にするには、次の操作を行います。

1. Firepower Management Center で、**[Policies]** > **[Actions]** > **[Alerts]**を選択し、**[Intrusion Email]** をクリックします。

2. [State] を [off] に設定します。
3. [Rules] の横にある [Email Alerting per Rule Configuration] をクリックし、ルールの選択を解除します。

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

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

4. 設定を保存します。

FMCv をアップグレードするには 28 GB の RAM が必要

展開：FMCv

アップグレード元：バージョン 6.5.0.x

直接アップグレード先：バージョン 6.6.0+

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 6.6.0+ 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。FMCv のメモリ要件の詳細については、Cisco Firepower Management Center Virtual 入門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 Firepower バージョンであっても、これらを使用して新しい FMCv 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 FMCv 展開のアップグレード前の要件を示します。

表 *21* : バージョン *6.6.0+* 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。

FTD/FDM アップグレード時に削除される履歴データ

展開：Firepower Device Manager

アップグレード元：バージョン 6.2.3 ～ 6.4.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+

Cisco Talos Intelligence Group（Talos）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 *22*：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。
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。

変更内容	詳細
「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 *23 :* 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 **[Policies]** > **[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 *24 :* 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（58 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 *25 :* 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 *26 :* 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。

TLS 暗号化アクセラレーションの有効化/無効にすることは不可

展開：Firepower 2100 シリーズ、Firepower 4100/9300 シャーシ

アップグレード元：バージョン 6.1.0 ～ 6.3.x

直接アップグレード先：バージョン 6.4.0 以降

SSL ハードウェア アクセラレーションは、TLS 暗号化アクセラレーションに名前が変更されました。

デバイスによっては、TLS 暗号化アクセラレーションがソフトウェアまたはハードウェアで実行される場合があります。アップグレードでは、この機能を手動で無効にした場合でも、すべての対象デバイスでアクセラレーションが自動的に有効になります。ほとんどの場合、この機能を設定することはできません。この機能は自動的に有効になり、無効にすることはできません。

バージョン 6.4.0 へのアップグレード： Firepower 4100/9300 シャーシのマルチインスタンス機能を使用している場合は、FXOS CLI を使用して、モジュール/セキュリティ エンジンごとに、1 つのコンテナ インスタンスに対して TLS 暗号アクセラレーションを有効にすることができます。他のコンテナインスタンスに対してアクセラレーションは無効になっていますが、ネイティブ インスタンスには有効になっています。

バージョン 6.5.0 以降へのアップグレード：Firepower 4100/9300 シャーシのマルチインスタンス機能を使用している場合は、FXOS CLI を使用して、Firepower 4100/9300 シャーシ上の複数のコンテナ インスタンス（最大 16 個）に対して TLS 暗号アクセラレーションを有効にすることができます。新しいインスタンスでは、この機能がデフォルトで有効になっています。ただし、アップグレードによって既存のインスタンスのアクセラレーションが有効になることはありません。代わりに、 **config hwCrypto enable** CLI コマンドを使用してください。

FMC、NGIPSv で準備状況チェックに失敗する可能性

展開：FMC、NGIPSv

アップグレード元：バージョン 6.1.0 ～ 6.1.0.6、バージョン 6.2.0 ～ 6.2.0.6、バージョン 6.2.1、バージョン 6.2.2 ～ 6.2.2.4、およびバージョン 6.2.3 ～ 6.2.3.4

直接アップグレード先：バージョン 6.3.0+

次に示すバージョンの Firepower のいずれかからアップグレードする場合は、そこに示されているモデルで準備状態チェックを実行できません。これは、準備状況チェック プロセスが新しいアップグレード パッケージに対して互換性を持たないためです。

表 *27 :* バージョン *6.3.0* 以降用の準備状況チェックを備えたパッチ

準備完了チェックがサポートされない	修正された最初のパッチ
6.1.0 ～ 6.1.0.6	6.1.0.7
6.2.0 ～ 6.2.0.6	6.2.0.7

準備完了チェックがサポートされない	修正された最初のパッチ
6.2.1	なし。バージョン 6.2.3.5+ にアップグレードしてください。
6.2.2 ～ 6.2.2.4	6.2.2.5
6.2.3 ～ 6.2.3.4	6.2.3.5

リモート アクセス VPN のデフォルト設定の変更によって VPN トラフィックがブロックされる可能性

展開：リモート アクセス VPN 用に設定された Firepower Threat Defense

アップグレード元：バージョン 6.2.x

直接アップグレード先：バージョン 6.3 +

バージョン6.3では非表示オプションの **sysopt connection permit-vpn** のデフォルト設定が変更されています。アップグレードすると、リモート アクセス VPN がトラフィックを渡さなくなる可能性があります。この場合は、次のいずれかの手法を使用してください。

- **sysopt connection permit-vpn** コマンドを設定する FlexConfig オブジェクトを作成します。このコマンドの新しいデフォルトは **no sysopt connection permit-vpn** です。

  これは、外部ユーザーがリモート アクセス VPN アドレス プール内の IP アドレスになりすますことができないため、VPN でトラフィックを許可するよりも安全な方法です。欠点はVPN トラフィックが検査されないことです。つまり、侵入とファイルの保護、URL フィルタリング、その他の高度な機能がトラフィックに適用されません。

- リモート アクセス VPN アドレス プールからの接続を許可するアクセス制御ルールを作成します。

  この方法では、VPN トラフィックが確実に検査され、高度なサービスを接続に適用できます。欠点は、外部のユーザーが IP アドレスをスプーフィングして、内部ネットワークにアクセスしやすくなることです。

セキュリティインテリジェンスによって可能になるアプリケーションの識別

展開：Firepower Management Center

アップグレード元：バージョン 6.1 ～ 6.2.3.x

直接アップグレード先：バージョン 6.3 +

バージョン 6.3 では、セキュリティ インテリジェンスの設定によりアプリケーションの検出と識別が可能になります。現在の展開で検出を無効にした場合は、アップグレード プロセスに

よって再び検出が有効になる可能性があります。必要がない場合（たとえば、IPS のみの展開など）に検出を無効にするとパフォーマンスが向上する可能性があります。

検出を無効にするには、次の手順を実行する必要があります。

- ネットワーク検出ポリシーからすべてのルールを削除します。
- 単純なネットワークベースの条件（ゾーン、IP アドレス、VLAN タグ、およびポート）のみを使用してアクセス制御を実行します。どんな種類のアプリケーション、ユーザー、URL、または地理位置情報の制御も行わないでください。
- **（新規）**デフォルトのグローバル リストなど、アクセス コントロール ポリシーのセキュリティ インテリジェンス設定からすべてのホワイトリストとブラックリストを削除することで、ネットワークと URL ベースのセキュリティ インテリジェンスを無効にします。
- **（新規）**DNS のデフォルトのグローバル ホワイトリストや DNS ルールのグローバル ブラックリストなど、関連付けられている DNS ポリシー内のすべてのルールを削除または無効にすることで、DNS ベースのセキュリティ インテリジェンスを無効にします。

アップグレード後に VDB を更新して CIP 検出を有効化

展開：すべて

アップグレード元：バージョン 6.1.0 ～ 6.2.3.x、VDB 299+ 搭載

直接アップグレード先：バージョン 6.3.0+

脆弱性データベース（VDB）299 以降を使用しているときにアップグレードする場合、アップグレード プロセスの問題により、アップグレード後の CIP 検出を使用できなくなります。これには、2018 年 6 月から現在までにリリースされたすべての VDB に加えて、最新の VDB も含まれます。

アップグレード後は常に脆弱性データベース（VDB）を最新バージョンに更新することを推奨しますが、この場合は特に重要です。

この問題の影響を受けるかどうかを確認するには、CIP ベース アプリケーションの条件を使用して、アクセス制御ルールを設定してみてください。ルール エディタで CIP アプリケーションが見つからない場合は、手動で VDB を更新します。

無効な侵入変数セットによって展開に失敗する可能性

展開：すべて

アップグレード元：バージョン 6.1 ～ 6.2.3.x

直接アップグレード先：バージョン 6.3.0+

侵入変数セット内のネットワーク変数については、除外する IP アドレスが、含める IP アドレスのサブセットである必要があります。次の表に、有効な設定と無効な設定の例を示します。

有効	無効
含める：10.0.0.0/8 除外する：10.1.0.0/16	含める：10.1.0.0/16 除外する：172.16.0.0/12 除外する：10.0.0.0/8

バージョン 6.3.0 より前のバージョンでは、このタイプの無効な設定でネットワーク変数を正常に保存できました。現在のバージョンでは、これらの設定によって展開がブロックされ、次のエラーが表示されます。`Variable set has invalid excluded values.`

この場合は、正しく設定されていない変数セットを識別して編集してから展開しなおしてください。変数セットによって参照されているネットワーク オブジェクトおよびグループの編集が必要である場合もあることに注意してください。

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。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。

トラフィック フローとインスペクション

次の場合に、トラフィックフローおよび検査の中断が発生することがあります。

- デバイスを再起動する場合。
- デバイスソフトウェア、オペレーティングシステム、または仮想ホスティング環境をアップグレードする場合。
- デバイスソフトウェアをアンインストールまたは場合。
- ドメイン間でデバイスを移動する場合。
- 設定の変更を展開する場合（Snort プロセスが再起動する）。

デバイスタイプ、高可用性または拡張性の設定、およびインターフェイス設定によって、中断の性質が決まります。これらのタスクは、保守期間中に行うか、中断による展開環境への影響が最も小さい時点で行うことを強く推奨します。

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

FXOS のアップグレード

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

表 *28 :* トラフィックの挙動：*FXOS* のアップグレード

展開	メソッド	トラフィックの動作
スタンドアロン	—	廃棄
ハイアベイラビリティ	**ベストプラクティス**：スタンバイで FXOS を更新し、アクティブピアを切り替えて新しいスタンバイをアップグレードします。	影響なし。
	スタンバイでアップグレードが終了する前に、アクティブ ピアで FXOS をアップグレードします。	1 つのピアがオンラインになるまでドロップされる。
シャーシ間クラスタ（6.2 以降）	**ベストプラクティス**：少なくとも 1 つのモジュールを常にオンラインにするため、一度に 1 つのシャーシをアップグレードします。	影響なし。
	ある時点ですべてのモジュールを停止するため、シャーシを同時にアップグレードします。	少なくとも 1 つのモジュールがオンラインになるまでドロップされる。
シャーシ内クラスタ（Firepower 9300 のみ）	ハードウェアバイパス有効：[Bypass: Standby] または [Bypass-Force]。（6.1 以降）	検査なしで受け渡される。
	ハードウェアバイパス無効：[Bypass: Disabled]。（6.1 以降）	少なくとも 1 つのモジュールがオンラインになるまでドロップされる。
	ハードウェア バイパス モジュールなし。	少なくとも 1 つのモジュールがオンラインになるまでドロップされる。

スタンドアロンデバイスでのソフトウェアのアップグレード

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

表 *29*：トラフィックの挙動：スタンドアロンデバイスでのソフトウェアのアップグレード

インターフェイス コンフィギュレーション		トラフィックの動作
ファイアウォール インターフェイス	EtherChannel、冗長、サブインターフェイスを含むルーテッドまたはスイッチド。 スイッチドインターフェイスは、ブリッジグループまたはトランスペアレントインターフェイスとしても知られています。	廃棄
IPS のみのインターフェイス	インラインセット、ハードウェアバイパス強制が有効：[Bypass: Force]（6.1 以上）。	ハードウェアバイパスを無効にするか、スタンバイモードに戻すまで、インスペクションなしで合格。
	インラインセット、ハードウェアバイパス スタンバイ モード：[Bypass: Standby]（6.1 以上）。	デバイスがメンテナンスモードの場合、アップグレード中にドロップされます。その後、デバイスがアップグレード後の再起動を完了する間、インスペクションなしで合格します。
	インラインセット、ハードウェアバイパスが無効：[Bypass: Disabled]（6.1 以上）。	廃棄
	インラインセット、ハードウェアバイパス モジュールなし。	廃棄
	インラインセット、タップモード。	パケットをただちに出力、コピーへのインスペクションなし。
	パッシブ、ERSPAN パッシブ。	中断なし、インスペクションなし。

高可用性および拡張性に関するソフトウェアのアップグレード

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

- FMC を搭載した FTD：高可用性ペアの場合、スタンバイデバイスが最初にアップグレードされます。デバイスの役割が切り替わり、新しくスタンバイになったデバイスがアップグレードされます。

  クラスタの場合、データ セキュリティ モジュールを最初にアップグレードして、その後コントロールモジュールをアップグレードします。コントロール セキュリティ モジュールをアップグレードする間、通常トラフィック インスペクションと処理は続行しますが、システムはロギングイベントを停止します。ロギングダウンタイム中に処理されるトラ

フィックのイベントは、アップグレードが完了した後、非同期のタイムスタンプ付きで表示されます。ただし、ロギングダウンタイムが大きい場合、システムはログ記録する前に最も古いイベントをプルーニングすることがあります。

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

ソフトウェアのアンインストール（パッチ）

バージョン 6.2.3 以降では、パッチをアンインストールすると、アップグレード前のバージョンに戻り、設定は変更されません。

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

設定変更の導入

アップグレード プロセス中には、設定を複数回展開します。Snort は、通常、アップグレード直後の最初の展開時に再起動されます。展開の前に、特定のポリシーまたはデバイス設定を変更しない限り、それ以外の展開時に再起動されることはありません。詳細については、『Firepower Management Center 構成ガイド』の「Configurations that Restart the Snort Process when Deployed or Activated」を参照してください。

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

表 *30*：トラフィックの挙動：設定変更の展開

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

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、[Failsafe] が有効または無効（6.0.1 ～ 6.1）。	検査なしで受け渡される。 [フェールセーフ（Failsafe）] が無効で、Snortがビジーでもダウンしていない場合、いくつかのパケットがドロップすることがあります。
	インラインセット、[Snort Fail Open: Down]：無効（6.2 以降）	廃棄
	インラインセット、[Snort Fail Open: Down]：有効（6.2 以降）	検査なしで受け渡される。
	インラインセット、タップモード。	パケットをただちに出力、コピーへのインスペクションなし。
	パッシブ、ERSPAN パッシブ。	中断なし、インスペクションなし。

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

スタンドアロンデバイスでのソフトウェアのアップグレード

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

表 *31 :* トラフィックの挙動：スタンドアロンデバイスでのソフトウェアのアップグレード

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

インターフェイス コンフィギュレーション		トラフィックの動作
IPS のみのインターフェイス	インラインセット、ハードウェアバイパス強制が有効：[Bypass: Force]（Firepower 2100 シリーズ、6.3 以上）。	ハードウェアバイパスを無効にするか、スタンバイモードに戻すまで、インスペクションなしで合格。
	インラインセット、ハードウェアバイパス スタンバイ モード：[Bypass: Standby]（Firepower 2100 シリーズ、6.3 以上）。	デバイスがメンテナンスモードの場合、アップグレード中にドロップされます。その後、デバイスがアップグレード後の再起動を完了する間、インスペクションなしで合格します。
	インラインセット、ハードウェアバイパスが無効：[Bypass: Disabled]（Firepower 2100 シリーズ、6.3 以上）。	廃棄
	インラインセット、ハードウェアバイパス モジュールなし。	廃棄
	インラインセット、タップモード。	パケットをただちに出力、コピーへのインスペクションなし。
	パッシブ、ERSPAN パッシブ。	中断なし、インスペクションなし。

高可用性および拡張性に関するソフトウェアのアップグレード

高可用性デバイスやデバイスのアップグレード中に、トラフィックフローや検査が中断されることはありません。

- FMC を使用した Firepower Threat Defense：高可用性ペアの場合、スタンバイデバイスが最初にアップグレードされます。デバイスの役割が切り替わり、新しくスタンバイになったデバイスがアップグレードされます。
- FDM を使用した Firepower Threat Defense：高可用性ペアの場合、スタンバイをアップグレードし、ロールを手動で切り替えてから、新しいスタンバイをアップグレードします。

ソフトウェアのアンインストール（パッチ）

バージョン 6.2.3 以降では、パッチをアンインストールすると、アップグレード前のバージョンに戻り、設定は変更されません。

- FMC を搭載した FTD：スタンドアロンデバイスの場合、パッチのアンインストール中のトラフィックフローと検査の中断は、アップグレードの場合と同じになります。高可用性および拡張性の展開では、中断を最小限に抑えるために、アンインストールの順序を明確

に計画する必要があります。これは、ユニットとしてアップグレードしたデバイスであっても、デバイスから個別にパッチをアンインストールするためです。

- FDM を搭載した FTD ：サポートされていません。

設定変更の導入

アップグレードプロセス中には、設定を複数回展開します。Snort は、通常、アップグレード直後の最初の展開時に再起動されます。展開の前に、特定のポリシーまたはデバイス設定を変更しない限り、それ以外の展開時に再起動されることはありません。詳細については、『Firepower Management Center 構成ガイド』の「Configurations that Restart the Snort Process when Deployed or Activated」を参照してください。

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

表 *32*：トラフィックの挙動：設定変更の展開

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

ASA FirePOWER アップグレード時の動作

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

表 *33 : ASA FirePOWER* アップグレード中のトラフィックの動作

トラフィック リダイレクションのポリシー	トラフィックの動作
フェール オープン（**sfr fail-open**）	インスペクションなしで転送
フェール クローズ（**sfr fail-close**）	ドロップされる
モニターのみ（**sfr {fail-close}|{fail-open} monitor-only**）	パケットをただちに出力、コピーへのインスペクションなし

ASA FirePOWER 展開時のトラフィックの動作

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

アップグレード プロセス中には、設定を複数回展開します。Snort は、通常、アップグレード直後の最初の展開時に再起動されます。展開の前に、特定のポリシーまたはデバイス設定を変更しない限り、それ以外の展開時に再起動されることはありません。詳細については、『Firepower Management Center 構成ガイド』の「Configurations that Restart the Snort Process when Deployed or Activated」を参照してください。

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

NGIPSv アップグレード時の動作

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

Firepower ソフトウェア アップグレード

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

表 *34 : NGIPSv* アップグレード中のトラフィックの動作

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

インターフェイス 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、タップ モード	パケットをただちに出力、コピーへのインスペクションなし
パッシブ	中断なし、インスペクションなし

展開時のトラフィックの動作

アップグレード プロセス中には、設定を複数回展開します。Snort は、通常、アップグレード直後の最初の展開時に再起動されます。展開の前に、特定のポリシーまたはデバイス設定を変更しない限り、それ以外の展開時に再起動されることはありません。詳細については、『Firepower Management Center 構成ガイド』の「Configurations that Restart the Snort Process when Deployed or Activated」を参照してください。

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

表 *35 : NGIPSv* 展開時のトラフィックの動作

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

時間とディスク容量のテスト

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

時間テスト

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

注意 アップグレード中は、設定の変更の実施または展開を行わないでください。システムが非アクティブに見えても、進行中のアップグレードを手動で再起動、シャットダウン、または再起動しないでください。システムが使用できない状態になり、再イメージ化が必要になる場合があります。アップグレードに失敗する、アプライアンスが応答しないなど、アップグレードで問題が発生した場合には Cisco TAC にお問い合わせください。

表 *36 :* 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。
高可用性/拡張性	特に断りのない限り、スタンドアロンデバイスでテストします。 高可用性の構成またはクラスタ化された構成では、動作の継続性を保持するため、複数のデバイスは1つずつアップグレードされます。アップグレード中は、各デバイスはメンテナンスモードで動作します。そのため、デバイスペアまたはクラスタ全体のアップグレードには、スタンドアロンデバイスのアップグレードよりも長い時間がかかります。
設定	シスコでは、構成およびトラフィック負荷が最小限のアプライアンスでテストを行います。 アップグレード時間は、構成の複雑さ、イベントデータベースのサイズ、また、それらがアップグレードから影響を受けるかどうか、受ける場合はどのような影響を受けるかにより、長くなる場合があります。たとえば多くのアクセス制御ルールを使用している場合、アップグレードはこれらのルールの格納方法をバックエンドで変更する必要があるため、アップグレードにはさらに長い時間がかかります。

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

ディスク容量テスト

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

また、デバイス アップグレード パッケージ用に 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 *37 :* ディスク容量の確認

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

バージョン 6.6.5 の時間とディスク容量

表 *38 :* バージョン *6.6.5* の時間とディスク容量

プラットフォーム	ローカルの容量	FMC の容量	アップグレード時間	リブート時間
FMC	16.5 GB /var 内 23 MB / 内	—	55 分	14 分

プラットフォーム	ローカルの容量	FMC の容量	アップグレード時間	リブート時間
FMCv：VMware	21 GB /var 内 29 MB / 内	—	51 分	9 分
Firepower 1000 シリーズ	9.7 GB /ngfw/var 内 400 MB /ngfw 内	1.1 GB	20 分	16 分
Firepower 2100 シリーズ	10.2 GB /ngfw/var 内 450 MB /ngfw 内	1.1 GB	17 分	15 分
Firepower 9300	10.2 GB /ngfw/var 内 11 MB /ngfw 内	1.1 GB	12 分	10 分
Firepower 4100 シリーズ	10.1 MB /ngfw/var 内 10 MB /ngfw 内	1.1 GB	10 分	11 分
Firepower 4100 シリーズ コンテナ インスタンス	10.7 GB /ngfw/var 内 11 MB /ngfw 内	1.1 GB	12 分	7 分
FTD を搭載した ASA 5500-X シリーズ	8.6 GB /ngfw/var 内 756 KB /ngfw 内	1.3 GB	22 分	30 分
FTDv：VMware	9.1 GB /ngfw/var 内 756 KB /ngfw 内	1.3 GB	12 分	21 分
ASA FirePOWER	12 GB /var 内 26 MB / 内	1.4 GB	65 分	25 分
NGIPSv	7.4 GB /var 内 21 MB / 内	910 MB	12 分	21 分

バージョン 6.6.4 の時間とディスク容量

表 *39 :* バージョン *6.6.4* の時間とディスク容量

プラットフォーム	ローカルの容量	FMC の容量	アップグレード時間	リブート時間
FMC	15.1 GB /var 内 23 MB / 内	—	60 分	28 分

プラットフォーム	ローカルの容量	FMC の容量	アップグレード時間	リブート時間
FMCv：VMware	23.7 GB /var 内 29 MB / 内	—	43 分	8 分
Firepower 1000 シリーズ	9.7 GB /ngfw/var 内 400 MB /ngfw 内	1 GB	21 分	16 分
Firepower 2100 シリーズ	10.1 GB /ngfw/var 内 450 MB /ngfw 内	1 GB	21 分	13 分
Firepower 9300	10.1 GB /ngfw/var 内 11 MB /ngfw 内	970 MB	14 分	10 分
Firepower 4100 シリーズ	8.9 GB /ngfw/var 内 11 MB /ngfw 内	970 MB	11 分	9 分
Firepower 4100 シリーズ コンテナ インスタンス	10.9 GB /ngfw/var 内 10 MB /ngfw 内	970 MB	10 分	7 分
FTD を搭載した ASA 5500-X シリーズ	8.5 GB /ngfw/var 内 756 KB /ngfw 内	1.2 GB	20 分	19 分
FTDv：VMware	7.7 GB /ngfw/var 内 756 KB /ngfw 内	1.2 GB	19 分	12 分
ASA FirePOWER	11.4 GB /var 内 26 MB / 内	1.3 GB	59 分	16 分
NGIPSv	7.4 GB /var 内 21 MB / 内	870 MB	13 分	8 分

バージョン 6.6.3 の時間とディスク容量

表 *40 :* バージョン *6.6.3* の時間とディスク容量

プラットフォーム	ローカルの容量	FMC の容量	アップグレード時間	リブート時間
FMC	15.1 GB /var 内 23 MB / 内	—	60 分	28 分

プラットフォーム	ローカルの容量	FMC の容量	アップグレード時間	リブート時間
FMCv：VMware	23.7 GB /var 内 29 MB / 内	—	43 分	8 分
Firepower 1000 シリーズ	9.7 GB /ngfw/var 内 400 MB /ngfw 内	1 GB	21 分	16 分
Firepower 2100 シリーズ	10.1 GB /ngfw/var 内 450 MB /ngfw 内	1 GB	21 分	13 分
Firepower 9300	10.1 GB /ngfw/var 内 11 MB /ngfw 内	970 MB	14 分	10 分
Firepower 4100 シリーズ	8.9 GB /ngfw/var 内 11 MB /ngfw 内	970 MB	11 分	9 分
Firepower 4100 シリーズ コンテナ インスタンス	10.9 GB /ngfw/var 内 10 MB /ngfw 内	970 MB	10 分	7 分
FTD を搭載した ASA 5500-X シリーズ	8.5 GB /ngfw/var 内 756 KB /ngfw 内	1.2 GB	20 分	19 分
FTDv：VMware	7.7 GB /ngfw/var 内 756 KB /ngfw 内	1.2 GB	19 分	12 分
ASA FirePOWER	11.4 GB /var 内 26 MB / 内	1.3 GB	59 分	16 分
NGIPSv	7.4 GB /var 内 21 MB / 内	870 MB	13 分	8 分

バージョン 6.6.1 の時間とディスク容量

表 *41 :* バージョン *6.6.1* の時間とディスク容量

プラットフォーム	/var 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	18.6 GB	23 MB	—	54 分	14 分
FMCv：VMware	15.8 GB	58 MB	—	56 分	13 分

プラットフォーム	/var 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 1000 シリーズ	10.8 GB	400 MB	1.1 GB	20 分	17 分
Firepower 2100 シリーズ	10.9 GB	450 MB	1.1 GB	16 分	21 分
Firepower 9300	9.8 GB	11 MB	1 GB	15 分	15 分
Firepower 4100 シリーズ	9.7 GB	10 MB	1 GB	15 分	14 分
Firepower 4100 シリーズ コンテナ インスタンス	11.2 GB	9 MB	1 GB	10 分	13 分
FTD を搭載した ASA 5500-X シリーズ	9.3 GB	1 MB	1.2 GB	21 分	24 分
FTDv：VMware	9.3 GB	1 MB	1.2 GB	18 分	19 分
ASA FirePOWER	12.3 GB	26 MB	1.4 GB	72 分	23 分
NGIPSv	7.1 GB	54 MB	860 MB	14 分	20 分

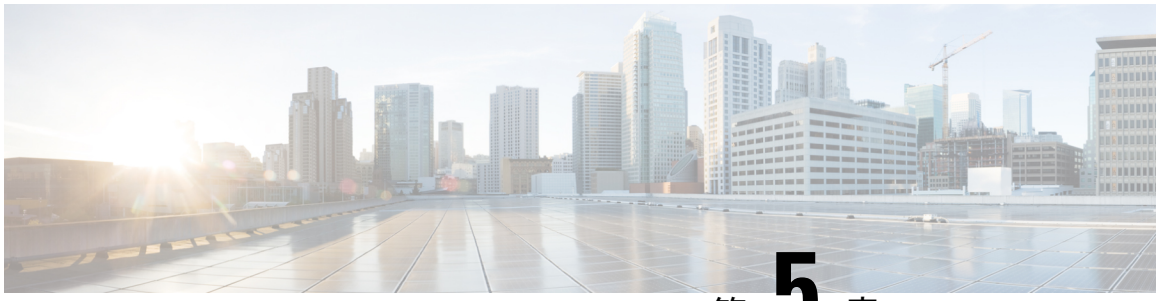
アップグレード手順

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

表 *42 : Firepower* アップグレード手順

タスク	ガイド
Firepower Management Center の展開でアップグレードします。	Cisco Firepower Management Center Upgrade Guide, Version 6.0–7.0
Firepower Device Manager を搭載した Firepower Threat Defense をアップグレードします。	Firepower Device Manager 用 Cisco Firepower Threat Defense 構成ガイド アップグレード先のバージョンではなく、現在実行している Firepower Threat Defense バージョンのガイドの「システム管理」の章を参照してください。

タスク	ガイド
Firepower 4100/9300 シャーシの FXOS をアップグレードします。	Cisco Firepower 4100/9300 アップグレードガイド、Firepower 6.0.1–7.0.x または ASA 9.4(1)–9.16(x) with FXOS 1.1.1–2.10.1
ASDM を使用して ASA FirePOWER モジュールをアップグレードします。	Cisco ASA Upgrade Guide
ISA 3000、ASA 5508-X、ASA 5516-X で ROMMON イメージをアップグレードします。	Cisco ASA and Firepower Threat Defense Reimage Guide 「Upgrade the ROMMON Image」のセクションを参照してください。常に最新のイメージがあることを確認してください。



第 5 章

ソフトウェアのインストール

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

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

インストールにおけるチェックリストおよびガイドライン

再イメージ化によって、システムパスワードを含むほとんどの設定が工場出荷時の初期状態に戻ります。このチェックリストは、一般的な再イメージ化の問題を回避できるアクションを示しています。ただし、このチェックリストは包括的なものではありません。詳細な手順については、該当する設置ガイド『取り付け手順 （85 ページ）』を参照してください。

表 *43 :*

✓	アクション/チェック
	アプライアンスへのアクセスを確認します。 アプライアンスに物理的にアクセスできない場合、再イメージ化プロセスによって管理ネットワークの設定を維持できます。これにより、再イメージ化した後、アプライアンスに接続して、初期設定を実行できます。ネットワーク設定を削除する場合は、アプライアンスに物理的にアクセスできる必要があります。Lights-Out 管理（LOM）を使用することはできません。 （注） 以前のバージョンに再イメージ化すると、ネットワーク設定が自動的に削除されます。このようなまれなケースでは、物理的アクセスが必要です。 デバイスに関して、ユーザーの位置からのトラフィックがデバイスの管理インターフェイスにアクセスするためにデバイス自体を通過する必要がないことを確認してください。FMC の展開では、デバイスを経由せずに FMC 管理インターフェイスにアクセスできる必要もあります。
	バックアップを実行します。 サポートされている場合、再イメージ化の前にバックアップします。 再イメージ化してアップグレードする必要がない場合、バージョンの制約により、バックアップを使用して古い設定をインポートできないことに注意してください。設定は手動で再作成する必要があります。 **注意** 安全なリモートロケーションにバックアップし、正常に転送が行われることを確認することを強くお勧めします。再イメージ化によって、システムパスワードを含むほとんどの設定が工場出荷時の初期状態に戻ります。アプライアンスに残っているすべてのバックアップが削除されます。特に、バックアップファイルは暗号化されていないため、不正アクセスを許可しないでください。バックアップ ファイルが変更されていると、復元プロセスは失敗します。 バックアップと復元は、複雑なプロセスになる可能性があります。手順をスキップしたり、セキュリティやライセンスの問題を無視しないでください。バックアップと復元の要件、ガイドライン、制限事項、およびベストプラクティスの詳細については、使用する展開の設定ガイドを参照してください。

✓	アクション/チェック
	FMC 管理からデバイスを削除する必要があるか判断します。 再イメージ化されたアプライアンスを手動で設定する予定がある場合は、再イメージ化する前に、リモート管理からデバイスを削除します。 • FMC を再イメージ化する場合は、すべてのデバイスを管理から削除します。 • 単一のデバイスを再イメージ化するか、またはリモートからローカルでの管理に切り替える場合は、その単一のデバイスを削除します。 再イメージ化後にバックアップから復元する場合は、デバイスをリモート管理から削除する必要はありません。
	ライセンスの問題に対処します。 アプライアンスを再イメージ化する前に、ライセンスの問題に対処してください。孤立した権限付与の発生を防ぐために、Cisco Smart Software Manager（CSSM）から登録解除することが必要になる場合があります。これで、再登録を防ぐことができます。または、新しいライセンスについてセールス部門に連絡する必要がある場合があります。 詳細については、以下を参照してください。 • ご使用の製品の設定ガイド。 • スマート ライセンスの登録解除 （83 ページ） • Cisco Firepower System Feature Licenses Guide • Frequently Asked Questions (FAQ) about Firepower Licensing

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

Firepower 1000/2100 シリーズデバイスの完全な再イメージ化を実行することを推奨します。消去設定方式を使用すると、Firepower Threat Defense ソフトウェアに加えて、FXOS が復元しない場合があります。この場合、特にハイ アベイラビリティ展開では、障害が発生する可能性があります。

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

スマート ライセンスの登録解除

Firepower Threat Defense は Cisco Smart Licensing を使用します。ライセンス供与された機能を使用するには、Cisco Smart Software Manager（CSSM）で登録します。後で再イメージ化または管理の切り替えを行うことにした場合は、孤立した権限付与を発生させないように登録を解除する必要があります。これらが生じると再登録できない場合があります。

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

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

次の操作を行う前に、CSSM から手動で登録解除します。

- FTD デバイスを管理する Firepower Management Center を再イメージ化する。
- モデルの移行中にソース Firepower Management Center をシャットダウンする。
- FDM によってローカルで管理されている Firepower Threat Defense デバイスを再イメージ化する。
- Firepower Threat Defense デバイスを FDM から FMC 管理に切り替える。

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

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

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

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

取り付け手順

表 *44 : Firepower Management Center* 取り付け手順

FMC	ガイド
FMC 1600、2600、4600	Cisco Firepower Management Center 1600, 2600, and 4600 Getting Started Guide
FMC 1000、2500、4500	Cisco Firepower Management Center 1000, 2500, and 4500 Getting Started Guide
FMC 2000、4000	Cisco Firepower Management Center 750, 1500, 2000, 3500 and 4000 Getting Started Guide
FMCv	Cisco Secure Firewall Management Center Virtual 入門ガイド

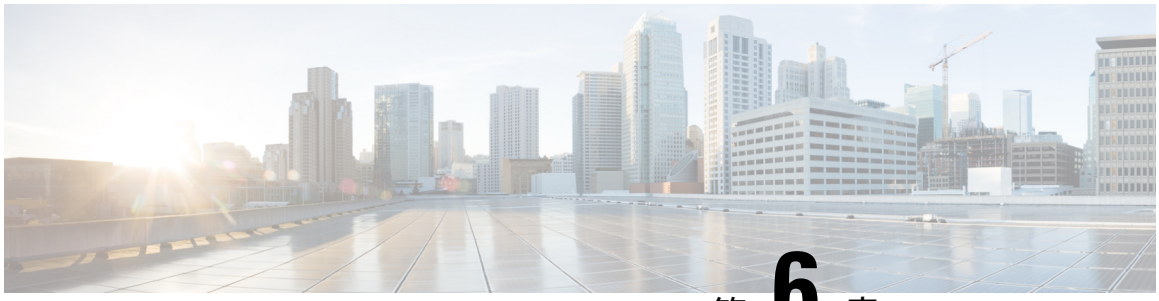
表 *45 : Firepower Threat Defense* 取り付け手順

FTDプラットフォーム	ガイド
Firepower 1000/2100 シリーズ	Cisco Secure Firewall ASA および Threat Defense 再イメージ化ガイド Cisco FXOS トラブルシューティングガイド（Firepower Threat Defense を実行している Firepower 1000/2100 シリーズ向け）
Firepower 4100/9300	Cisco Firepower 4100/9300 FXOS Configuration Guides：イメージ管理に関する章 Cisco Firepower 4100 スタートアップガイド Cisco Firepower 9300 スタートアップ ガイド
ASA 5500-X シリーズ	Cisco Secure Firewall ASA および Threat Defense 再イメージ化ガイド
ISA 3000	Cisco Secure Firewall ASA および Threat Defense 再イメージ化ガイド
FTDv：AWS	AWS クラウド向け Cisco Secure Firewall Threat Defense Virtual スタートアップガイド
FTDv：Azure	Microsoft Azure クラウド向け Cisco Secure Firewall Threat Defense Virtual クイックスタートガイド
FTDv：KVM	KVM 向け Cisco Secure Firewall Threat Defense Virtual スタートアップガイド

FTDプラットフォーム	ガイド
FTDv：VMware	VMware 向け Cisco Secure Firewall Threat Defense Virtual スタートアップガイド

表 *46 : NGIPSv* および *ASA FirePOWER* のインストール手順

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



第 6 章

資料

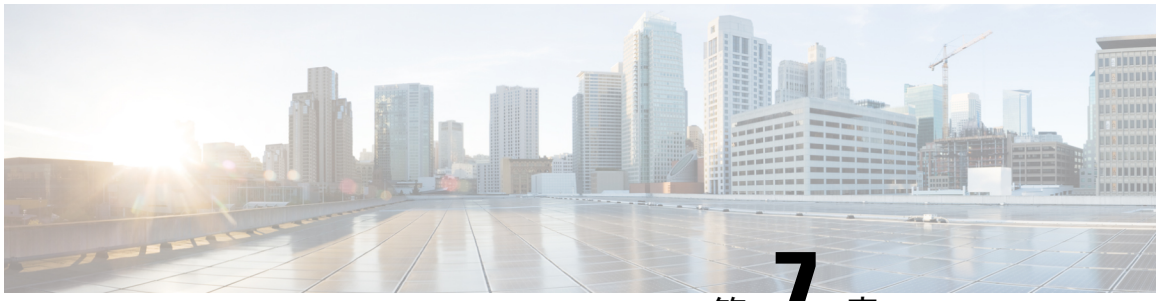
メンテナンスリリースで必要な場合は、Firepower のマニュアルを更新します。

- ドキュメント ロードマップ （87 ページ）

ドキュメント ロードマップ

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

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



第 7 章

解決済みの問題

便宜上、リリースノートには、各メンテナンスリリースの解決済みの問題が記載されています。

サポート契約がある場合は、Cisco Bug Search Tool を使用して最新のバグリストを取得できます。検索では、特定のプラットフォームとバージョンに影響するバグに絞り込むことができます。バグのステータス、バグ ID ごとに検索したり、特定のキーワードを検索することもできます。

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

新しいビルドで解決済みの問題

シスコは、更新版ビルドを適宜リリースしています。ほとんどの場合、各プラットフォームの最新のビルド番号のみが、シスコ サポートおよびダウンロード サイト で入手可能です。最新のビルドを使用することを強くお勧めします。以前のビルドをダウンロードした場合は使用しないでください。

同じソフトウェアバージョンに対して、1つのビルドから別のビルドにアップグレードすることはできません。新しいビルドで問題が解決する場合は、代わりに、アップグレードまたはホットフィックスが機能するかどうかを確認します。それ以外の場合は、Cisco TAC にご連絡ください。公的に利用可能なホットフィックスへのクイックリンクについては、Cisco Firepower ホットフィックス リリース ノート を参照してください。

表 *47* : バージョン *6.6* の新しいビルド

バージョン	新しいビルド	リリース日	パッケージ	プラットフォーム	解決済み
6.6.1	91	2020-09-16	アップグレード 再イメージ化	すべて	CSCvv69991：FTD が 6.6.1 へのアップグレード後にメンテナンスモードでスタックする すでにこの問題が発生している場合は、Cisco TAC にお問い合わせください。 バージョン 6.6.1-90 への FTD デバイスのアップグレードまたは再イメージ化が正常に行われた場合は、ホットフィックス 6.6.1-A を適用してください。ホットフィックスを適用するまで、デバイスを NetFlow エクスポータとして設定しないでください。 すべての FMC、ASA FirePOWER モジュール、および NGIPSv でバージョン 6.6.1-90 を引き続き実行できます。 詳細については、「Software Advisory: Inoperable FTD Device/NetFlow Exporter after Reboot」を参照してください。

バージョン 6.6.5 で解決済みの問題

表 *48* : バージョン *6.6.5* で解決済みの問題

不具合 ID	タイトル
CSCvf88062	CTM：Nitrox S/G の長さを検証する必要がある
CSCvg69380	ASA：まれに発生した CP 処理での破損によってコンソールロックが発生する
CSCvh19737	FTD データインターフェイス（オフボックス管理）での HTTPS アクセスが失敗する
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
CSCvj08826	FMC ibdata1 ファイルのサイズが大きくなることがある
CSCvm82290	IRB/TFW 設定でホストが到達不能な場合に ASA コアブロックが枯渇する

不具合 ID	タイトル
CSCvo34210	スレッド名 Unicorn Proxy Thread で ASA が 9.6.4.20 トレースバックを実行する
CSCvp13352	VPN セッションがタイムアウトした後でも、ASA はクライアント側接続に対する TCP キープアライブを実行し続ける
CSCvp15559	設定同期中にセカンダリ ASA でトレースバックが発生する
CSCvp28713	パケットトレーサーの RESULT の入出力インターフェイスが「UNKNOWN」と表示される
CSCvp69936	ASA：tcp_intercept スレッド名 thread detection でのトレースバック
CSCvq98396	ASA：暗号化セッションがスタンバイユニットでリークを処理する
CSCvr11958	AWS FTD：「ERROR: failed to set interface to promiscuous mode」により展開が失敗する
CSCvr33428	FMC が SYN フラッド攻撃から接続イベントを生成する
CSCvr77005	インターフェイスが使用可能になると、トラフィックが暗号マップからプライマリインターフェイスにフォールバックしない
CSCvr85295	Cisco Adaptive Security Appliance と Firepower Threat Defense ソフトウェア リモート
CSCvs13204	SR-IOV インターフェイス上の ASAv フェールオーバー トラフィックが、インターフェイスのダウンによりドロップされることがある
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
CSCvs72390	Cisco Firepower Management Center のクロスサイト スクリプティングの脆弱性
CSCvs72450	FXOS：サービスモジュールの hwclock を同時書き込みコリジョンによる破損から修復
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
CSCvs82926	ASA「Chassis 0 Cooling Fan OK」SCH メッセージを使用した FRP 1000 および FPR2100 シリーズの重大な RPMアラート
CSCvs84542	スレッド idfw_proc での ASA のトレースバック
CSCvs95188	異なるインスタンス間で共有される FXOS FTD マルチインスタンス CPU コア

不具合 ID	タイトル
CSCvt10944	VTI トンネル経由で EMIX トラフィックを送信しているときに CTM がクラッシュした
CSCvt11885	移行スクリプトの実行がメモリ不足エラーで終了する
CSCvt37303	プレフィルタールールゾーンの検証（アクティビティの検証）が、UI の HW レイヤーでバイパスされる
CSCvt39977	PSNG_TCP_PORTSCAN [122:1:1] ルールアラートの場合の無効なパケットデータ
CSCvt48260	スタンバイユニットがアクティブユニットを検出すると、fover_parse でトレースバックしてブートループする
CSCvt52604	FMC の [Objects] セクションから [Interfaces] ページがロードされない（ドメインページも影響を受けることがある）
CSCvt55927	6.4.0.9-34 FDM で HA を解除できない
CSCvt71529	SSL ハンドシェイク中の ASA のトレースバックとリロード
CSCvt74194	unified2 レコード取得中のエラー：ファイルの破損
CSCvt75760	HTTP クリーンアップによるクライアントレス WebVPN のトレースバックまたはページ障害
CSCvt92077	ASAv での ping の失敗：9.13（CAT9k の再起動後）
CSCvt97205	ASA 9.14.1 上で SNMPPOLL/SNMPTRAP からリモートエンド（サイト間 VPN）ASA インターフェイスが失敗する
CSCvu02594	非同期セッションが多すぎるため、Snort の終了に時間がかかる
CSCvu09496	多くの ACP で同じ DNS ポリシーが参照されると、DNS データが繰り返し収集されエクスポートされる
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
CSCvu30704	サイズ「0」のクラッシュ情報により ASA がトレースバックする
CSCvu33992	トレースバック：ASA が lina_sigcrash+1394 をリロードした
CSCvu44472	FMC システムプロセスが起動する
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

不具合 ID	タイトル
CSCvu82680	パフォーマンスファイルの一部が、本来は含まれないはずの FTD バックアップの一部として含まれている
CSCvu84127	明確な理由なしに Firepower がリブートすることがある
CSCvu87906	バックアップファイルが 6.6.0 ～ 90 で増大し続ける（統合イベントファイルが誤ってバックアップに含まれる）
CSCvu89110	ASA：「logging permit-hostdown」が設定され、TCP syslog がダウンしている場合も新しい接続をブロクする
CSCvu94878	OpenSSH 5.7 ～ 8.3 のクライアント側に、Observable Discrepan がある
CSCvu97112	SNMP ポーリングが HA のアクティブデバイスで動作を停止した
CSCvu97242	2100：クラッシュが発生すると、コアファイルとクラッシュ情報の両方が切り捨てられ、不完全になる可能性がある
CSCvu98222	SSL 復号ポリシーを有効にした後、FTD Lina エンジンがデータパスでトレースバックすることがある
CSCvv00719	時間範囲オブジェクトを含むアクセス コントロール ポリシーがヒットしない
CSCvv02925	OSPF ネイバーシップが確立されていない
CSCvv07917	ASA が新しいルートを学習すると、フローティングスタティックによって作成された ASP ルートテーブルが削除される
CSCvv10778	9.12.4 へのアップグレード後のスレッド名 DATAPATH（5585）または Lina（2100）のトレースバック
CSCvv15572	新しいコンテキストの作成中に「config-url」を入力すると、ASA のトレースバックが発生する
CSCvv17585	特定の状況下で Netflow テンプレートが送信されない
CSCvv19230	ASAv AnyConnect ユーザがアイドルタイムアウトで予期せず切断される
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
CSCvv24647	FP2100-SNMP：不正な値がイーサネット統計ポーリングに返される
CSCvv24976	RRI ルートインターフェイスをシャットダウンした後、静的デフォルトルートがリブにインストールされない
CSCvv25394	アップグレード後、ASA がディスクの名前を交換して disk0 が disk1になり、disk1 が disk0 になった

不具合 ID	タイトル
CSCvv30172	リブート後に ADI が断続的に KCD に参加できなくなる
CSCvv31755	更新の失敗により、アプリケーションとシャーシ間でインターフェイスのステータスが一致しないことがある
CSCvv32333	ASA は現在もマルチモードでの SNMP を介した internal-data0/0 カウンタのポーリングを許可しない
CSCvv36788	MsgLayer[PID]：エラー：Msglyr::ZMQWrapper::registerSender()：ZeroMQ ソケットのバインドに失敗した
CSCvv37629	不正な SIP パケットにより SIP 接続タイムアウトまで 4k ブロックのホールドアップが発生し、トラフィックの問題を引き起こす可能性がある
CSCvv40406	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（lina 変更）。
CSCvv41453	管理専用ルートテーブルからスタティック IPv6 ルートを削除すると、データトラフィックに影響する
CSCvv44863	URL フィルタリング設定ファイルからデフォルトの脅威カテゴリ設定を読み込めない
CSCvv49698	ASA Anyconnect url-redirect が IPv6 で機能しない
CSCvv49800	ASA/FTD：HA スイッチオーバーが Firepower シャーシのグレースフル再起動で発生しない
CSCvv50338	snpi_nat_xlate_destroy+2508 でのトレースバック クラスタ ユニット
CSCvv52349	2100/1000 シリーズ Firepower デバイスに XFS 破損を処理するユーティリティがない
CSCvv52591	ctm_hw_malloc_from_pool で DMA メモリリークが発生し、管理接続と VPN 接続が失敗する
CSCvv53696	Anyconnect ユーザーの AAA または CoA タスク中の ASA/FTD トレースバックおよびリロード
CSCvv55248	ACL トランザクションコミット用に生成された Syslog が一貫した形式でなく、利用できない場合がある
CSCvv55291	HA の中断後、HA の再参加後に Snmp ユーザーがスタンバイデバイスで失敗する。
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

不具合 ID	タイトル
CSCvv58332	ASA/FTD が BGP MP_REACH_NLRI 属性のネクストホップバイトを逆順で読み取る
CSCvv62305	フェールオーバーペアに参加しようとした場合の fover_parse での ASA トレースバックとリロード
CSCvv63412	tmatch のコンパイルが進行中のとき、ASA がすべてのトラフィックを理由「No route to host」でドロップする
CSCvv64068	ネットワーク/サービスオブジェクト名の変更後、syslog の ACL のハッシュ値で不一致が発生する
CSCvv65184	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
CSCvv66005	inspect esmtp での ASA のトレースバックとリロード
CSCvv66561	ssh pubkey-chain サーバーでのキー文字列のサポートが意図したとおりに機能しない。
CSCvv66920	内部フロー：U ターン GRE フローが不正な接続フローの作成をトリガーする
CSCvv67196	FTD が crl ファイルを取得するためにすべての crl URL を試行しない
CSCvv67398	SNMP が無効な場合、Inspect-snmp で thru-the-box snmp paks がドロップされる
CSCvv67500	DATAPATH での ASA 9.12 のランダムトレースバックおよびリロード
CSCvv68669	分類の失敗により、マスター ASA のシステムコンテキストで仮想 IP アドレスへのトラフィックがドロップされる
CSCvv69991	FTD が 6.6.1 へのアップグレード後にメンテナンスモードでスタックする
CSCvv70984	ブックマーク SSL 暗号設定の変更中の ASA トレースバック
CSCvv71097	トレースバック：ASA が snp_fdb_destroy_fh_callback + 104 をリロードする
CSCvv72466	ASA のアップグレード後、startup-config で OSPF ネットワークコマンドが欠落する
CSCvv73017	fover および SSH スレッドによるトレースバック
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））
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

不具合 ID	タイトル
CSCvv80782	トレースバックにより purg_process となる
CSCvv85029	スレッド名 ace_work で ASA5555 がトレースバックし、リロードする
CSCvv86861	SNMP トラフィックのテスト中にトレースバックする
CSCvv86926	コアファイルを作成する FTD での予期しないトレースバックとリロード
CSCvv87232	ASA：igb_saleen_io_sfp_mod_poll_thread プロセスで CPU 専有の値が高くなる
CSCvv87496	「VPN packet redirect on peer」による ASA クラスタメンバー 2048 ブロックの枯渇
CSCvv88017	ASA：EasyVPN HW クライアントが重複したフェーズ 2 のキー再生成をトリガーし、トンネル経由で切断される
CSCvv89355	フェールオーバー後に DHCP プロキシ更新タイマーが起動しない
CSCvv89400	AES 256 を使用すると ASA SNMPv3 ポーリングが失敗する
CSCvv89708	ASA/FTD がスレッド名 fover_FSM_thread でトレースバックし、リロードすることがある
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
CSCvv90181	展開中に「show running-config」が実行されている場合、トランスクリプトに展開失敗の理由が表示されない
CSCvv90720	ASA/FTD：HA スイッチオーバー後に接続されたスイッチで MAC アドレステーブルのフラッピングが表示される
CSCvv90753	SLA が原因で同期プロセスがハングする
CSCvv94165	FTD 6.6：snmpd プロセスの CPU がスパイクする
CSCvv94701	ASA が「octnic_hm_thread」でリロードし続け、リロード後は回復するまでに非常に長い時間がかかる
CSCvv96193	プロポーザルが選択されていない場合、ASA または FTD のデバッグで明確な失敗理由が出力されない
CSCvv97527	asa config timeout コマンドが snort の DAQ 設定を壊す
CSCvv97877	セカンダリユニットがクラスタに参加できない

不具合 ID	タイトル
CSCvw00161	Firepower 2140 での VPNス レッドによる ASA のトレースバックとリロード
CSCvw01767	階層によっては、CRL フェールオープンオプションが機能しない場合がある
CSCvw03628	RFC822Name が空に設定された名前制約により、ASA が CA 証明書をインポートしない
CSCvw05392	diagnostic-cli に常に表示されるメッセージ
CSCvw06195	ASA のトレースバック cp_midpath_process_thread
CSCvw06298	異なるコンテキストの共有インターフェイスで ASA が MAC アドレスを複製して、トラフィックに影響を与える
CSCvw07000	PDTS Tx キューがスタックしたまま Snort がビジー状態でドロップする
CSCvw12008	「show tech-support」コマンドの実行中の ASA トレースバックとリロード
CSCvw12040	証明書チェーンの検証に失敗したため、ヒープキャッシュメモリが急激に枯渇している
CSCvw12100	サイト間セッションおよび AnyConnect セッションで ASA の古い VPN コンテキストが表示される
CSCvw13348	CCM レイヤ（スプリント 98、シーケンス 2）における WR6、WR8 および LTS18 コミット ID の更新
CSCvw15359	KP fxos snmp に、EPM インデックスの entPhysicalSerialNum,entPhysicalAssetID に初期化されていない文字列がある
CSCvw16165	ポートチャネルのメンバーがダウンすると、Firepower 1010 シリーズがトラフィックの通過を停止する
CSCvw16619	オフロードされたトラフィックが ECMP セットアップでセカンダリルートにフェールオーバーされない
CSCvw18614	LINA プロセスでの ASA トレースバック
CSCvw19227	使用されていないプレフィックスリストのオブジェクトを削除できない
CSCvw19907	agx 通信の snmpd の再起動が snmp-sa に対して失敗する
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）

不具合 ID	タイトル
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）
CSCvw21844	カプセル化されたフローを処理する際の DATAPATH スレッドでの FTD トレースバックとリロード
CSCvw22576	スタンバイ時のみ state fover インターフェースで「no mfib forwarding」コマンドが実行される
CSCvw22881	radius_rcv_auth により、コントロールプレーンの CPU 使用率が 100% になることがある
CSCvw22986	プライマリユニットのインターフェイスが init 状態のままであるため、セカンダリユニットがバルク同期状態で無限にスタックする
CSCvw23199	スレッド名 Logger での ASA/FTD のトレースバックとリロード
CSCvw24556	フローオフロードが有効になっている場合、TCP ファイル転送（ビッグファイル）が正しく閉じない
CSCvw26171	strncpy NULL 文字列が SSL ライブラリから渡されている間の ASA syslog トレースバック
CSCvw26331	スレッド名 ci/console での ASA のトレースバックとリロード
CSCvw26544	Cisco ASA および FTD ソフトウェアの SIP で確認されたサービス拒否攻撃に対する脆弱性
CSCvw27301	EAP を使用した IKEv2 で、MOBIKE ステータスが処理されない
CSCvw28814	SNMP プロセスがクラッシュし、Lina のトレースバックが発生した
CSCvw30252	ASA/FTD が SNMP のメモリ破損によりトレースバックおよびリロードすることがある
CSCvw31569	ディレクタ/バックアップフローは残され、このフローに関連するトラフィックがブラックホール化される
CSCvw32518	9.12(4)4 以降にアップグレード後の ASASM トレースバックおよびリロード
CSCvw36662	TACACS+ ASCII パスワード変更要求が正しく処理されない
CSCvw37259	デバイスがハング状態になるまで 600/秒のレートで VPN syslog が生成される
CSCvw37340	Oracle MySQL の MySQL サーバー製品の脆弱性（コンポーネント：
CSCvw37807	NTP 認証が有効な場合に IPsec 送信エラーが増加する

不具合 ID	タイトル
CSCvw42091	FTD/HA：「no shutdown」コマンドがスタンバイの実行コンフィギュレーションに表示されない
CSCvw42999	FPR2110 上の 9.10.1.11 ASA がランダムにトレースバックおよびリロードする
CSCvw43486	PBR 設定変更時の ASA/FTD トレースバックとリロード
CSCvw43489	inflate.c の inflate_dynamic 関数の NEEDBITS マクロが..
CSCvw43508	Info-ZIP UnZ の CRC32 検証でのヒープベースのバッファオーバーフロー...
CSCvw43510	Info-ZIP の test_compr_eb 関数でのヒープベースのバッファオーバーフロー...
CSCvw43529	1.25 より前の BusyBox の DHCP クライアント（udhcpc）での整数オーバーフロー。...
CSCvw43534	Mozilla Network S に Null ポインタの逆参照の脆弱性が存在する...
CSCvw43537	バス内の networking/ntpd.c の recv_and_process_client_pkt 関数...
CSCvw43541	zlib 1.2.8 の inftrees.c により、コンテキスト依存の攻撃者が...
CSCvw43543	zlib 1.2.8 の inflate.c の inflateMark 関数は、継続を許可する場合がある...
CSCvw43544	zlib 1.2.8 内の crc32.c の crc32_big 関数が、コンテキスト...
CSCvw43546	1.2 までの BusyBox 内の libbb/lineedit.c の add_match 関数で...
CSCvw43555	Info-Zip UnZip バージョン ← 6.0... にヒープベースのバッファオーバーフローが存在する...
CSCvw43559	8e2174e9bd836e5 をコミットする前の BusyBox プロジェクトの BusyBox wget バージョン...
CSCvw43567	1.20.1 以前の GNU Wget 内の xattr.c にある set_file_metadata がファイルを保存する...
CSCvw43571	1.30.0 以前の BusyBox で問題が発見された。範囲外の...
CSCvw43586	3.5.8 から 3.6.7 のバージョンの gnutls に脆弱性が見つかった...
CSCvw43615	3.6.15 以前の GnuTLS で問題が発見された。サーバーはトリガーできる...
CSCvw44122	ASA：非 DNS トラフィックを DNS 検査エンジンにリダイレクトする「class-default」クラスマップ
CSCvw45863	リロード時の ASAv SNMP トレースバック

不具合 ID	タイトル
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
CSCvw46702	アプリケーション設定の同期のタイムアウトが原因で FTD クラスタのセカンダリユニットがクラスタに参加できない
CSCvw47321	一部の FPR プラットフォームのインバウンドトラフィックの IPSec トランスポート モード トラフィックの破損
CSCvw48517	ASA を 9.13(1)13 にアップグレードすると、DAP が動作しなくなる
CSCvw48829	「show clock」のタイムゾーンが「show run clock」のタイムゾーンと異なる
CSCvw50679	アップグレード中に ASA/FTD がトレースバックおよびリロードすることがある
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
CSCvw51462	IPv4 デフォルトトンネルルートが拒否される
CSCvw51745	ルーティングテーブルに再追加された SLA 監視対象の静的ルートが RIP データベースに入力されていない。
CSCvw51950	手動フェールオーバー後に新しいアクティブの ASA から FPR SSL トラストポイントが削除される
CSCvw51985	ASA：IPv6 DACL 障害により、AnyConnect セッションを再開できない
CSCvw52083	FXOS logrotate がすべてのログファイルを正しくローテーションしない
CSCvw52609	Cisco ASA と FTD ソフトウェアの Web サービスバッファオーバーフローによるサービス拒否の脆弱性
CSCvw53255	FTD/ASA HA：トレースバックによるフェールオーバー後でも、スタンバイユニット FXOS がトラフィックを転送できる
CSCvw53427	ASA が複数のクエリパラメータを含む SAML アサーションで HTTP POST を処理できない
CSCvw53796	Cisco ASA および FTD Web サービスインターフェイスで確認されたクロスサイト スクリプティングの脆弱性
CSCvw54640	FPR-4150：スレッド名 DATAPATH での ASA トレースバックおよびリロード
CSCvw56703	ifc タイプの管理のみを変更すると、IPv6 静的ルートがインストールされない

不具合 ID	タイトル
CSCvw58414	タイプ dynamic-split-exclude-domains の AnyConnect カスタム属性の名前がリロード後に変更される
CSCvw59035	FTD BVI アドレスから直接接続された IP への接続の問題
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
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
CSCvw62528	ASA が IPv6 NTP サーバーとの同期に失敗する
CSCvw63862	ASA：ランダムな L2TP ユーザが古い ACL フィルタエントリが原因でリソースにアクセスできない
CSCvw64623	アクティブ IP アドレスを持つスタンバイインターフェイスから送信されたスタンバイ ASA リンクダウン SNMPTRAP
CSCvw68593	Linux カーネル f の応答 ICMP パケットが制限される方法に欠陥がある
CSCvw71766	IKev 2 Daemon スレッドでの ASA トレースバックおよびリロード
CSCvw72260	ASA のアップグレードが「CSP directory does not exist - STOP_FAILED Application_Not_Found」で失敗する
CSCvw72608	アクティブで受信したスタンバイの失敗イベントにより、スタンバイでの将来の展開がスキップされる
CSCvw73402	リモートFTPへのクラスタコピーのキャプチャの失敗により、FTDのLINA CLI が応答しなくなる
CSCvw74940	IKE デーモンでの ASA トレースバックおよびリロード
CSCvw75104	ポートチャネルメンバーのインターフェイスの変更に対する FDM-HA での展開の失敗
CSCvw75605	ドメイン、カウント、およびその他のフィールドが選択されていると、接続イベントの表に関する表示レポートが失敗する。
CSCvw77930	トンネルグループ名に「.」が含まれている場合、ASAがSAMLアサーションの処理に失敗する
CSCvw79208	入力文字列の後半に「http://」サブストリングがある場合、URL の正規化が正しく行われない
CSCvw79294	sftunnel が大量のログをメッセージファイルに記録する

不具合 ID	タイトル
CSCvw81322	マルチインスタンスモードを実行している FTD が、SRU のインストールと展開後に snort GID 3 ルールを無効にする
CSCvw81897	ASA：OpenSSL の脆弱性 CVE-2020-1971
CSCvw82577	Monet DB の一部として多数の小さなファイルがあると、FMC のバックアップ tar ファイルのサイズが肥大化する
CSCvw82629	ACL に関する「設定セッション」の変更時に ASA トレースバックが発生する。
CSCvw83572	バージョン 9.14.1.30 以降で BVI HTTP/SSH アクセスが機能しない
CSCvw83665	アップグレード後、FDM によって管理される FTD での変更を展開できない
CSCvw83780	ACL の変更時に FTD ファイアウォールがトレースバックおよびリロードすることがある
CSCvw84339	ホスト名が 30 文字を超えると、FTD の管理対象デバイスのバックアップが失敗する
CSCvw84786	スレッド名 snmp_alarm_thread での ASA トレースバックおよびリロード
CSCvw87788	ASA トレースバックとリロードの WebVPN スレッド
CSCvw88176	MonetDB のイベントデータベースのクラッシュにより、FMC 6.6.1 の接続イベントが失われる
CSCvw89365	証明書の変更中に ASA/FTD がトレースバックおよびリロードすることがある。
CSCvw90151	PPPOE - ASA が設定されていないプロトコルに対して CONFACK を送信する
CSCvw90634	FP2100 ASA：9.15.1.1 へのアップグレード後にネットワークモジュールがダウン/ダウンの 1 Gbps SFP
CSCvw91757	6.6.1 へのアップグレード後に FTDv を通過する SNMPv3 トラフィックを NAP がドロップする
CSCvw93139	Cisco ASA および FP 1000/2100 シリーズ コマンドインジェクションの FTD ソフトウェアの脆弱性
CSCvw94988	プライマリのクラスタユニットが無効になった後、V ルートが見つからないために S2S トラフィックが失敗する

不具合 ID	タイトル
CSCvw95301	キャプチャが削除されたときに ASA がトレースバックを実行し、スレッド名：ssh でリロードされる
CSCvw96129	[IMS_7_0_0] Lina Write Memory を使用したセカンダリでの HA 解除の失敗後に、展開が失敗する
CSCvw96488	inspect_h323_ras+1810 のトレースバック
CSCvw97256	リンク状態 API の読み取りが失敗した場合にリンク状態の更新を無視するには、rmu 読み取りエラーの処理が必要
CSCvw97267	スイッチポートのフラップがあると、DHCP クライアントの新しい IP アドレスの取得が失敗する
CSCvw97821	ASA：CoA で dACL が提供されない場合、VPN トラフィックが渡されない
CSCvw98315	FXOS は 6.7.0 への FTD アップグレード後に古い FTD バージョンを報告する
CSCvw98603	SQlite における複数の脆弱性
CSCvw98840	ASA：CoA 後の v6 トラフィックに IPv6 エントリのない dACL が適用されない
CSCvw99916	ASAv：9.14 へのアップグレード後に使用されたメモリ値の SNMP 結果が正しくない
CSCvx00655	PM から CriticalStatus を取得する際のタイムアウトによる ASA または SFR のサービスカードの障害
CSCvx01805	Firepower 2100 で設定の同期中にハートビートエラーが発生し、AppAgent が登録解除される
CSCvx02869	スレッド名のトレースバック：Lic TMR
CSCvx03764	アイデンティティ NAT トラフィックおよびクラスタリング環境では、オフロード書き換えデータを修正する必要がある
CSCvx04057	SGT 名が未解決のまま ACE で使用されている場合、回線が無視または非アクティブ状態にならない
CSCvx04643	ASA のリロードで「content-security-policy」設定が削除される
CSCvx05381	Cisco ASA および FTD ソフトウェアのコマンドインジェクションの脆弱性
CSCvx05385	ASA が HA の設定同期中にロガースレッドでトレースバックを生成することがある

不具合 ID	タイトル
CSCvx05956	navl 属性のコピー中に snort CPU 使用率が高くなる
CSCvx06385	6.6.1 へのアップグレード後に FPR 2100 の Fail-to-wire ポートがフラッピングする
CSCvx08734	ASA：デフォルトの IPv6/IPv4 ルートトンネリングが機能しない
CSCvx09147	sftunnel fsync が空のファイルを処理せず、メモリリークを示す
CSCvx09248	v2 および v3 の SNMP ウォークが失敗し、この OID でこのエージェントで使用可能なオブジェクトがありませんと表示される
CSCvx09535	ASA トレースバック：失効した証明書でリロードがトリガーされる AnyConnect クライアントの CRL チェック
CSCvx10110	アクティブな LDAP AAA サーバーの最後のトランザクションでのタイムスタンプのステータスが「不明」になる
CSCvx10502	5.10 以前の Linux カーネルの drivers/target/target_core_xcopy.c 内。
CSCvx10514	p11-kit 0.21.1 ～ 0.23.21 で問題が発見された。内で複数
CSCvx10519	curl 7.62.0 ～ 7.70.0 が情報漏えいに対して脆弱である
CSCvx10520	curl 7.20.0 ～ 7.70.0 が na の不適切な制限に対して脆弱である
CSCvx10555	MagickCore/statistic.c 内の ImageMagick で欠陥が見つかった。攻撃者
CSCvx10841	EIGRP を使用して VXLAN または VNI インターフェイスのサブネットをアドバタイズもしくは再配布できない
CSCvx11295	スレッド Crypto CA で ASA がトレースバックおよびリロードする
CSCvx11460	リモートエンドで TFC が有効になっている状態で Firepower 2110 がトラフィックをサイレントにドロップする
CSCvx13694	スレッド名 PTHREAD-4432 で ASA/FTD トレースバックする
CSCvx13835	バインドにおける複数の脆弱性
CSCvx14031	IKEv2 セッションの CoA の後に DACL が削除されると、IPv4 DACL がアクティブデバイスでスタックする（トラフィックは影響を受けない）
CSCvx15040	ASA/FTD で DHCP プロキシオファーがドロップされる
CSCvx16202	FMC からプッシュされた自己参照オブジェクトにより、エラーで lina がクラッシュする（GRP 階層でループする）

不具合 ID	タイトル
CSCvx16317	管理のコンテキストが変更されると、マルチコンテキスト ASA から connect fxos admin で FXOS にアクセスできない
CSCvx16592	VRF が設定されている場合、FTD はパケットを WCCP Web キャッシュエンジンにリダイレクトしない
CSCvx16700	「MIO が強制時刻同期に応答しない（MIO DID NOT RESPOND TO FORCED TIME SYNC）」ために、ブレードの起動中に FXOS クロック同期の問題が発生する
CSCvx17664	ASA がスレッド名「webvpn_task」でトレースバックおよびリロードすることがある
CSCvx17780	FPR-2100-ASA：最新バージョンの ASA インターフェイスで ifType の SNMP ウォークに「other」が表示される
CSCvx17785	ACL を追加または削除し、ルートマップコマンド（pbr_route_map_update）に入力すると、トレースバックが発生する
CSCvx17842	FMC から送信されたオブジェクトループによる lina のトレースバックを防ぎます。代わりに展開を失敗させます。
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
CSCvx20692	すべてのオブジェクトのタイプが同じ場合、Smart CLI で 10 個のオブジェクトのみが表示される
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
CSCvx21782	lina モニタが原因で Firepower プラットフォームが破損したコアダンプを生成する
CSCvx22695	OCSP 応答データのクリーンアップ中のに ASA がトレースバックおよびリロードする
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
CSCvx23907	CVE-2021-1405 に対する NGFW の影響を評価する
CSCvx24537	SAML：同じサブジェクト名を持つ 2 つ以上の IDP 証明書がある場合、SAML 認証が失敗する可能性がある

不具合 ID	タイトル
CSCvx25406	パケットの MTU のサイズが出力インターフェイスの MTU のサイズより大きい場合、LINA はパケットを何の警告を出すことなくドロップする
CSCvx25719	X-Frame-Options ヘッダーが webvpn 応答ページで設定されていない
CSCvx25836	「show crashinfo」による新しい出力ログの追加で ASA がトレースバックおよびリロードする
CSCvx26221	handle_agentx_packet / snmp で SNMP にトレースバックすると、FP1k および 5508 での起動に時間がかかる
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
CSCvx26525	FMC が 6.6.1 にアップグレードされた後、FTD デバイスで SNMP の設定が無くなっていることが判明した
CSCvx26808	FPR2100 シリーズのプロセス lina での FTD のトレースバックおよびリロード
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
CSCvx27077	SAML：トンネルグループで参照されているときに、webvpn saml IDP 設定が削除されないようにする
CSCvx27430	ASA：FIPS が有効な場合、PAC ファイルをインポートできない
CSCvx27914	地理位置情報ウィジェット FMC でイベントを表示できない
CSCvx28520	DKK の顧客 SSL ルールを使用した SSL の復号化が失敗する
CSCvx29429	CSCvx07389 の修正にもかかわらず、FPR4100/FPR9300 で ma_ctx*.log が大きなディスク領域を消費する
CSCvx29448	FTD：管理 int をポーリングできる診断 int で SNMP ホストが設定される
CSCvx29771	フローオフロードによる一括ルーティング更新後にファイアウォール CPU が増加することがある
CSCvx29814	DHCP GIADDR フィールドの IP アドレスが DHCP DECLINE を DHCP サーバに送信した後に反転する
CSCvx29832	フローオフロードを有効にした状態で大量のルートを更新すると、CPU のパフォーマンスが低下する
CSCvx30314	SSL 中間パスで ASA がトレースバックおよびリロードする
CSCvx33822	4GB RAM と 2 つの CPU を搭載した ASAv を展開するオプションがない

不具合 ID	タイトル
CSCvx33904	1.9.5p2 より前の sudo には、ヒープベースのバッファオーバーフローがあり、権限を使用できる
CSCvx34237	FIPS 障害による ASA のリロード
CSCvx34335	AAA LDAP サーバー：平均ラウンドトリップ時間が常に 0 ミリ秒になる
CSCvx37737	HA 中断および 6.6.0 または 6.6.1 へのアップグレード後に OSPF NSF による HA の障害が発生する
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
CSCvx41171	ACL 設定を同時に変更すると、「show running-config」の出力が完全に中断される
CSCvx41440	Talos クラウドとローカル DB 間で URL レピュテーションの不一致が発生する。
CSCvx42081	FPR4150 ASA Standby Ready ユニットのループが失敗し、設定を削除してインストールし直す必要がある
CSCvx42197	ASA EIGRP ルートがネイバーの切断後にスタックする
CSCvx44117	新しい net-snmp パッチの追加と未使用の net-snmp レシピのクリーンアップ
CSCvx44401	スレッド名 Unicorn Proxy Thread で FTD/ASA がトレースバックする
CSCvx45976	スレッド名：vnet-proxy（rip：socks_proxy_datarelay）で ASA および FTD のウォッチドッグが強制的にトレースバックとリロードを実行する
CSCvx47230	IE および Windows プラットフォームの古いバージョンの X-Frame-Options ヘッダーのサポート
CSCvx47628	2.4.57 および 2.5.x ～ 2.5.1 alpha の OpenLDAP では、アサーション
CSCvx47634	GNU C ライブラリ（別名 glibc または libc6）2.32 の iconv 関数
CSCvx47642	2.4.57 より前の OpenLDAP で整数アンダーフローが発見された
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
CSCvx49715	EVP_CipherUpdate、EVP_EncryptUpdate、EVP_DecryptUpdate への呼び出しは、
CSCvx49716	2.66.7 および 2.67.x より前の GNOME GLib で問題が発見された

不具合 ID	タイトル
CSCvx49720	BIND サーバーは、影響を受けるバージョンを実行している場合、脆弱となる
CSCvx50366	スレッド名 fover_health_monitoring_thread でのトレースバック
CSCvx52122	トランスペアレントコンテキストの削除中の SNMP 通知スレッドでの ASA トレースバックとリロード
CSCvx54235	ASP キャプチャの dispatch-queue-limit にパケットがないと表示される
CSCvx54396	マルチキャストルーティングが有効になっていると、断続的にポリシー展開が失敗する
CSCvx54606	FTD 6.6.1/6.7.0 が SNMP Ifspeed OID （1.3.6.1.2.1.2.2.1.5）応答値＝0 を送信している
CSCvx54934	グラフ形式でインライン結果を使用すると、侵入イベントレポートの生成が失敗する
CSCvx56323	S2S VPN の編集がエラー「ノードが見つかりません：12884908935（Node not found: 12884908935）」で失敗する
CSCvx57417	スマートトンネルコード署名証明書の更新
CSCvx59120	データトンネルが起動する前に COA を受信すると、親セッションが切断される
CSCvx61200	参照リークが原因で TID フィードがスタックする
CSCvx62239	VPN ロードバランシングのクラスタの形成を妨げているものについて、ログに包括的な詳細を記録する必要がある
CSCvx63256	6.2.3 から 6.6.3 へのアップグレード後に FTD または 4110 でエキスパートモードに入るときにエラーが発生する
CSCvx63647	スレッド名 CTM Daemon での ASA トレースバックおよびリロード
CSCvx64478	SAML トランザクション中に不要なコンソールが出力される
CSCvx65467	設定変更後に 663 FDM が syslog イベントを送信しない
CSCvx65745	FPR2100：UE イベントがクラッシュをトリガーするために、octeon でカーネルパニックを有効にします。
CSCvx67996	FMC RAVPN：IPv6 DNS がグループ ポリシーで設定されている場合、展開が失敗する
CSCvx68128	ASA 内部デッドロックにより、機能（syslog、リロード、ASDM、anyconnect）が失われる

不具合 ID	タイトル
CSCvx68355	ASA：countryName が UTF8 としてエンコードされている場合、CA 証明書をインポートできない
CSCvx68490	SSL URL カテゴリが削除されたため、100_ftd_onbox_data_import.sh で FDM のアップグレードが失敗する
CSCvx68951	SNMP を使用してインターフェイスの物理アドレスをポーリングすると、ASA が「00 00 00 00 00 00」で応答する
CSCvx69405	スレッド名 SNMP ContextThread での ASA トレースバックおよびリロード
CSCvx71434	asa_run_ttyS0 スクリプトによるスレッド名 pix_startup_thread での ASA/FTD トレースバックおよびリロード
CSCvx71571	ASA：CSM で「エラー：ハッシュテーブルからエントリを削除できません」
CSCvx72904	ifmibポーリングの最適化
CSCvx73164	シスコ製品に影響を及ぼす Lasso SAML 実装の脆弱性：2021 年 6 月
CSCvx74035	複数の ACL とオブジェクトが設定された状態で「clear configure all」を実行すると、ASA がトレースバックおよびリロードする
CSCvx75503	再送信された SYN が検査エンジンで検査されない
CSCvx75963	キャプチャ取得中に ASA がトレースバックする
CSCvx76703	ルールがインターフェイスグループによるトラフィックに一致している場合、FMC がプレフィルタのポリシー変更を保存しない
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
CSCvx80835	手動登録が、証明書をインポートした後、LINA でスタック保留中のトラストポイントのエントリを作成する
CSCvx81405	既知のキールールに一致すると予想される接続が復号化されない場合がある
CSCvx85534	データインターフェイスからの予期しない IP を持つ SNMP トラップが送信される

不具合 ID	タイトル
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
CSCvx86177	FMC データベースを外部からポーリングするために使用される inet6_ntoa と unix_timestamp 関数がエラーを返す
CSCvx87679	フェールオーバーライセンスの数がスタンバイのファイアウォールに同期されない。
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
CSCvx87790	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
CSCvx88683	ASA が BGP パスワードをスタンバイユニットに正しく複製しない
CSCvx89827	FPR 2110 でバンコクタイムゾーンを設定できない
CSCvx91341	2.66.8 より前の GNOME GLib で問題が発見された。g_file_repla の場合
CSCvx94326	VPN ロードバランシングがスタックし、グループから切断されることがある
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
CSCvx95255	既存の ASDM コンテキストスイッチから新しい ASDM 接続を区別するための ASA のサポート変更
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
CSCvx98041	FTD-API：ruleId の重複するシーケンス番号により、無効な snort ngfw.rules が展開される
CSCvx99373	FMC：「beakerd」プロセスのコアファイルがデバッグシンボルをアーカイブしていないため、使用できない
CSCvy01752	スレッド Lic HA クラスタでのトレースバック
CSCvy02448	FPFPR2100 シリーズ プラットフォームの ASA で時刻同期が正しく機能しない
CSCvy02703	CTM Message Handler による ASA および FTD のトレースバック
CSCvy03006	uauth のデバッグ機能の改善

不具合 ID	タイトル
CSCvy03045	管理のコンテキストが変更されると、マルチコンテキスト ASA から connect fxos admin で FXOS にアクセスできない
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
CSCvy04869	ユーザー証明書のキーサイズが 8192 ビットの場合、AnyConnect 証明書認証が失敗する
CSCvy04965	WM スタンバイが HA への再参加に失敗し、「CD App Sync エラーがスタンバイで SSP 設定を適用できませんでした」というメッセージが表示される
CSCvy05807	FO 同期の操作後に SNMPWalk 失敗が確認された。
CSCvy05966	Snort 2.9.16.3-3033 トレースバック（FTD 6.6.3）
CSCvy07491	access-list の再設定時の ASA トレースバック
CSCvy07654	FTD：ndclientd の後にハートビートが見つからないため、TS ファイルを生成する際にフェールオーバーロールの変更が発生する
CSCvy08908	Java によってポート転送アプリケーションがブロックされる
CSCvy09217	暗号の不一致が原因で HA がアクティブ/アクティブ状態になる
CSCvy09252	Syncd が FMC HA のセカンダリの FMC 部分で繰り返し終了する
CSCvy10665	Firepower 9000 シリーズ SM-56 で、ディスクマネージャの YYYY-MM-DD ファイルの filespec エントリがない
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）
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の ASA トレースバックとリロード。
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
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
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
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

不具合 ID	タイトル
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
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
CSCvy40482	9.14MR3：snmpwalk が [Errno 146] の接続拒否エラーで失敗した
CSCvy61008	Lina と FXOS 間の同期外れの時間
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

バージョン 6.6.4 で解決済みの問題

表 *49*：バージョン *6.6.4* で解決済みの問題

不具合 ID	タイトル
CSCvu84127	明確な理由なしに Firepower FTD がリブートする
CSCvx86231	999_finish/935_change_reconciliation_baseline.pl での 6.6.3 への FMC アップグレードの失敗

バージョン 6.6.3 で解決済みの問題

表 *50*：バージョン *6.6.3* で解決済みの問題

不具合 ID	タイトル
CSCvm82290	IRB/TFW 設定でホストが到達不能な場合に ASA コアブロックが枯渇する
CSCvs50274	ASA5506 からボックスへ icmp 要求パケットが断続的にドロップされる
CSCuw51499	ACE の追加/削除、ACL オブジェクト/オブジェクトグループの編集で TCM が機能しない
CSCvs85595	ユニットの同期中に awk:fatal メッセージが表示される
CSCvt09940	Cisco Firepower 4110 の ICMP ソフトウェアの TCP フラッド DoS 攻撃に対する脆弱性

不具合 ID	タイトル
CSCvt48260	スタンバイユニットがアクティブユニットを検出すると、fover_parse でトレースバックしてブートループする
CSCvt64952	「Show crypto accelerator load-balance detail」が欠落しており、出力が未定義
CSCvt75760	HTTP クリーンアップによるクライアントレス WebVPN のトレースバックまたはページ障害
CSCvt92077	ASAv での ping の失敗：9.13（CAT9k の再起動後）
CSCvu23539	内部フロー：LU flag3 オーバーラップ
CSCvu27868	ASA：ASA のアップグレード後、外部 IPv6 ロギングサーバーへの特定の syslog メッセージの欠如
CSCvu33992	トレースバック：ASA が lina_sigcrash+1394 をリロードした
CSCvu36302	vpn-addr-assign local reuse-delay が設定されている場合、%ASA-3-737403 が誤って使用される
CSCvv02925	OSPF ネイバーシップが確立されていない
CSCvv17585	特定の状況下で Netflow テンプレートが送信されない
CSCvv43484	システムアップグレード後に ASA が RIP パケットの処理を停止する
CSCvv48594	メモリリーク：脅威の検出での snp_tcp_intercept_stat_top_n_integrate() による
CSCvv49800	ASA/FTD：HA スイッチオーバーが Firepower シャーシのグレースフル再起動で発生しない
CSCvv58605	スレッドでの ASA トレースバックおよびリロード：暗号化 CA、MTX 内の非仮想化 pki グローバルテーブルによるメモリ破損
CSCvv63412	tmatch のコンパイルが進行中のとき、ASA がすべてのトラフィックを理由「No route to host」でドロップする
CSCvv72466	ASA のアップグレード後、startup-config で OSPF ネットワークコマンドが欠落する
CSCvv89400	AES 256 を使用すると ASA SNMPv3 ポーリングが失敗する
CSCvw22986	プライマリユニットのインターフェイスが init 状態のままであるため、セカンダリユニットがバルク同期状態で無限にスタックする
CSCvw24556	フローオフロードが有効になっている場合、TCP ファイル転送（ビッグファイル）が正しく閉じない

不具合 ID	タイトル
CSCvw32518	9.12(4)4 以降にアップグレード後の ASASM トレースバックおよびリロード
CSCvw53884	ASA5506 上の M500IT モデルのソリッドステートドライブが 3 年 2 ヵ月のサービス期間後に応答しなくなることがある
CSCvs68576	二重否定が原因で、自動 NAT ルールの削除時に展開に失敗する
CSCvu95109	6.6 から 6.7.0 への KVM/KP FDM のアップグレードがディスク容量が原因で失敗する/ngfw/var/cisco/deploy/fdm
CSCvv20450	FMC 6.4 から 6.7 へのアップグレードが失敗する「Error running script 500_rpms/110_generate_dbaccess.sh」
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
CSCvv87495	FMC がランダムに応答しなくなる（SSH または GUI なし）：エラー 500
CSCvv91486	リロード中のストリームでメモリリークが発生
CSCvw03229	6.4 から 6.6.1 にアップグレードすると、デバイスがマルウェアおよび接続イベントを送信しなくなる
CSCvw37369	Python 3 ～ 3.9.0 の Lib/test/multibytecodec_support.py CJK
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
CSCvs13204	SR-IOV インターフェイス上の ASAv フェールオーバー トラフィックが、インターフェイスのダウンによりドロップされることがある
CSCvs79606	「dns server-group DefaultDNS」CLI が無効にならない
CSCvt13822	ASA：一致する暗号マップエントリがないため、VTI が IPSec トンネルを拒否する
CSCvt17912	lina_free_exec_st で segfault/reload を引き起こすプラットフォームの制限をプッシュするストレス
CSCvt61196	マルチコンテキストモードの ASA で、コンテキストを削除しても SSH キーが削除されない。
CSCvt95176	2.1.0 より前の expat の readfilemap.c で、コンテキスト依存の攻撃者が許可される
CSCvu06767	マルチインスタンス上の Lina コアにより両方の論理デバイスでブートループが発生する
CSCvu16423	ASA 9.12(2)：ユニコーンプロキシスレッドによる複数のトレースバック

不具合 ID	タイトル
CSCvu17852	MPF で接続制限が設定されている場合、「show service policy」で現在の接続数が負になる
CSCvu43355	二重解放によるデータパスでの FTD Lina トレースバック
CSCvu44135	SSH 管理接続制限を超えた場合に syslog 710004 が生成されない
CSCvu70931	「no key config-key」を入力した後でクラスタ/AAA サーバーキーが欠如する
CSCvu89110	ASA：「logging permit-hostdown」が設定され、TCP syslog がダウンしている場合も新しい接続をブロクする
CSCvv09396	セッション終了後に、L2TP の VPN ルートが陳腐化する
CSCvv12857	暗号化エンジンの障害後に ASA がフリーズする
CSCvv15572	新しいコンテキストの作成中に「config-url」を入力すると、ASA のトレースバックが発生する
CSCvv32425	show asp table classify domain permit を実行した場合の ASA トレースバック
CSCvv40195	Syslog トラップにログ内容が含まれていない
CSCvv66005	inspect esmtp での ASA のトレースバックとリロード
CSCvv66920	内部フロー：U ターン GRE フローが不正な接続フローの作成をトリガーする
CSCvw07000	PDTS Tx キューがスタックしたまま Snort がビジー状態でドロップする
CSCvw12100	サイト間セッションおよび AnyConnect セッションで ASA の古い VPN コンテキストが表示される
CSCvw27301	EAP を使用した IKEv2 で、MOBIKE ステータスが処理されない
CSCvw44122	ASA：非 DNS トラフィックを DNS 検査エンジンにリダイレクトする「class-default」クラスマップ
CSCvw59035	FTD BVI アドレスから直接接続された IP への接続の問題
CSCvw64623	アクティブ IP アドレスを持つスタンバイインターフェイスから送信されたスタンバイ ASA リンクダウン SNMPTRAP
CSCvw87788	ASA トレースバックとリロードの WebVPN スレッド
CSCvw98840	ASA：CoA 後の v6 トラフィックに IPv6 エントリのない dACL が適用されない

不具合 ID	タイトル
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
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
CSCvt48601	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
CSCvt69260	接続イベントに古いデバイス名が表示される
CSCvt70854	6.6.0-90： [Firepower 1010] メモリ不足のため、SRU の更新中に tomcat が再起動する
CSCvt99020	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
CSCvv26683	CLI から「configure high-availability disable」コマンドを実行すると、次の HAJoin で例外が発生する
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
CSCvv55271	FMC から監査ログを取得する REST API で、startIndex の有無にかかわらず最初の 25 エントリのみ返される
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
CSCvv58604	トラフィックが、ブロック/リセットおよび SSL インスペクションで設定された AC ポリシーと一致する場合、リセットが送信されない
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
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
CSCvv98534	アップグレードに失敗しても、syslog に監査メッセージが作成されない
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
CSCvw05415	FDM：オブジェクトの S2S VPN 一致基準バージョンでオブジェクトグループの編集が更新されない
CSCvg73237	ENH：VPN の総容量の単なる割合ではなく、絶対値として CAC が設定される

不具合 ID	タイトル
CSCvn12453	フローがハッシュされる RX リング番号を表示する debug menu コマンドが実装される
CSCvq81410	ASA：Safari ブラウザを使用して HTTP 経由で ASA コマンドを実行できない
CSCvs84542	スレッド idfw_proc での ASA のトレースバック
CSCvs99356	Snort2：SSP プラットフォームで SSL ポリシーが設定されていると、大きなファイルのダウンロードに時間がかかる
CSCvt11302	FIPS デバイスで FIPS が有効になっている場合、Webtype ACL を作成できない
CSCvt22356	ASA のリブート後、ASA クラスタの Health-check monitor-interface debounce-time が 9000ms にリセットされる
CSCvt33785	ランダム VPN ピアの IPSec SA が作成されない
CSCvt41357	syslog ホストにアクセスできない場合、「no logging permit-hostdown」コマンドで接続がブロックされない
CSCvt42610	SNMP ポーリング中に確認されたメモリリーク
CSCvt71529	SSL ハンドシェイク中の ASA のトレースバックとリロード
CSCvt80134	WebVPN リライタが SAP Netweaver からのデータを解析できない
CSCvu08339	タップモードがオフで FTD インラインセット ブリッジ グループ ID が 0 に設定される
CSCvu27287	スケジュールバックアップが EEM を介した SCP で失敗する
CSCvu55469	FTD：接続アイドルタイムアウトがリセットされない
CSCvu98505	PLR 経由でライセンスされた ASA に「export-controlled functionality enabled」フラグが正しく設定されていない
CSCvv20405	WEBVPN：ERROR：マルチコンテキスト ASA の無効なトンネルグループ名
CSCvv50338	snpi_nat_xlate_destroy+2508 でのトレースバック クラスタ ユニット
CSCvv63208	ASA 5506/5508：再起動後に SNMP ポーリングが失敗するが、しばらくすると復元される
CSCvv67398	SNMP が無効な場合、Inspect-snmp で thru-the-box snmp paks がドロップされる

不具合 ID	タイトル
CSCvw54640	FPR-4150：スレッド名 DATAPATH での ASA トレースバックおよびリロード
CSCvw58414	タイプ dynamic-split-exclude-domains の AnyConnect カスタム属性の名前がリロード後に変更される
CSCvx09535	ASA トレースバック：失効した証明書でリロードがトリガーされる AnyConnect クライアントの CRL チェック
CSCvt00255	カーネルを cpe:2.3:o:linux:linux_kernel:4.14.187: にアップグレード
CSCvu98780	FTD-API：CDO テンプレートの適用によってルール削除のバグがトリガーされる
CSCvv22208	onbox モードで、展開が失敗したときに、zones.conf がロールバックしない
CSCvv36915	「Show NTP」コマンドがマルチインスタンス FTD で機能しない
CSCvv63227	アップグレードされたセットアップで SLA が動作を停止する
CSCvv67754	メモリの計算結果が正しくないため、Snort のメモリ使用率が高くなる
CSCvw88467	eStreamer が Sybase の代わりに MySQL から ids_event_msg_map をクエリする
CSCvq47743	AnyConnect と管理セッションが数週間後に接続に失敗する
CSCvf88062	CTM：Nitrox S/G の長さを検証する必要がある
CSCvs85196	ASA SIP 接続が連続した複数回のフェールオーバー後にドロップする：ピンホールタイムアウト/インスペクションによるクローズ
CSCvt76688	syslog メッセージ 201008 に、TCP サーバーがダウンした場合のドロップの理由が含まれている必要がある
CSCvt88454	クライアントレスポータルを使用すると、設定された言語と一致しない文字列がある
CSCvv07864	マルチキャスト EIGRP トラフィックが内部 FTD インターフェイスで表示されない
CSCvv10778	9.12.4 へのアップグレード後のスレッド名 DATAPATH（5585）または Lina（2100）のトレースバック
CSCvv19230	ASAv AnyConnect ユーザがアイドルタイムアウトで予期せず切断される
CSCvv41453	管理専用ルートテーブルからスタティック IPv6 ルートを削除すると、データトラフィックに影響する

不具合 ID	タイトル
CSCvv57590	ASA：スタンバイでの ACL のコンパイルに時間がかかる
CSCvv73017	fover および SSH スレッドによるトレースバック
CSCvv86861	夜間に VPN、EMIX、および SNMP トラフィックを実行中に、タイマーで KP のクラッシュが確認される
CSCvv90181	展開中に「show running-config」が実行されている場合、トランスクリプトに展開失敗の理由が表示されない
CSCvw28814	QP を v9.14.1.109 にアップグレード中に SNMP プロセスがクラッシュした
CSCvw42999	FPR2110 上の 9.10.1.11 ASA がランダムにトレースバックおよびリロードする
CSCvw51985	ASA：IPv6 DACL 障害により、AnyConnect セッションを再開できない
CSCvw53255	FTD/ASA HA：トレースバックによるフェールオーバー後でも、スタンバイユニット FXOS がトラフィックを転送できる
CSCvw74940	IKE デーモンでの ASA トレースバックおよびリロード
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
CSCvp10079	FMC HA スイッチで DB スイッチロールが失敗する
CSCvr02310	TLS1.3 が DND ルールで唯一許可されている TLS バージョンである場合、Server Hello がドロップされる
CSCvs47365	FXOS 2.9.1 アップデートを使用すると、FMC で発生するイベントレートが低下するか、デバイスからイベントレートが来なくなる
CSCvt34973	SFNotificationd によって「メッセージ」ファイルに過剰なロギングが発生することがある
CSCvt61370	通信のデッドロックが原因で、デバイスからのイベントが停止することがある
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
CSCvu33591	FPWR 4100 ：/var/sf/fwcfg/ にある破損ファイルが原因で Snort がダウンする
CSCvu35768	FMC を 6409-59 から 6.6.0-90 にアップグレードした後、サブドメイン内の Radius 外部ユーザーを使用して UI をログに記録できない

不具合 ID	タイトル
CSCvv04441	アップグレード前に RA-VPN が設定されている場合、ngfw.rules がプライマリ FTD HA とセカンダリ FTD HA の間で一致しない
CSCvv19573	インターフェイスが管理専用のスタティックルートの更新に関連付けられている場合、展開が失敗する
CSCvv21045	データベースが新しい接続の受け入れを停止することがあり、イベント処理が停止する
CSCvv40961	http-proxy 設定が原因でアップグレードが失敗する
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
CSCvu71324	ASA：dhcp-network-scope の使用により、自動 DENY ルールが複数のコンテキストに適用される
CSCvv14621	クラスタでコマンド レプリケーション タイムアウトが発生した場合に表示されるエラーメッセージの修正
CSCvv29687	ASA でのデフォルトの syslog 780001/780002 のレート制限
CSCvv43885	キャリアライセンスが準拠していない場合、「show sctp」コマンドは使用できない
CSCvv49698	ASA Anyconnect url-redirect が IPv6 で機能しない
CSCvv62305	フェールオーバーペアに参加しようとした場合の fover_parse での ASA トレースバックとリロード
CSCvv80782	トレースバックにより purg_process となる
CSCvv86926	コアファイルを作成する FTD での予期しないトレースバックとリロード
CSCvv88017	ASA：EasyVPN HW クライアントが重複したフェーズ 2 のキー再生成をトリガーし、トンネル経由で切断される
CSCvv94165	FTD 6.6：snmpd プロセスの CPU がスパイクする
CSCvw26171	strncpy NULL 文字列が SSL ライブラリから渡されている間の ASA syslog トレースバック
CSCvw63862	ASA：ランダムな L2TP ユーザが古い ACL フィルタエントリが原因でリソースにアクセスできない
CSCvw97821	ASA：CoA で dACL が提供されない場合、VPN トラフィックが渡されない
CSCvt01938	show ntp を実行すると、出力を得るためのパスワードを求められる

不具合 ID	タイトル
CSCvt66875	AppId は UltraSurf にトンネリングされた IP ではなく、プロキシ IP をキャッシュする
CSCvt72683	FP 8130 での NAT ポリシーの展開後の NAT ポリシーの設定が表示されない
CSCvt87074	libxslt 1 の前に xsltNumberFormatGetMultipleLevel で Type Confusion が生じる
CSCvu93834	FDM/FTD-API：スタンバイ状態で管理ユーザーのパスワードを変更できない
CSCvv40916	展開中に、AbstractBaseDeploymentValidationHandler.validatePreApply に 3 分の遅延が発生する
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
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
CSCvw22546	ローカル管理 FTD で API を使用して DH グループを変更できない
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
CSCvw83498	FTD-API：LDAP 属性マップで、ldapValue（スペースを含む）が処理されない
CSCvo11165	WebVPN の言語変換表を更新する必要がある
CSCvr35872	ASA トレースバックスレッド名：DATAPATH-0-1388 PBR 9.10(1)22
CSCvr85295	Cisco Adaptive Security Appliance と Firepower Threat Defense ソフトウェア リモート
CSCvs72450	FXOS：サービスモジュールの hwclock を同時書き込みコリジョンによる破損から修復
CSCvs72378	異なるコンテキスト間で切り替えると、ASDMセッションが突然終了する
CSCvt18199	スタンドアロン ASA の「overlaps with inside standby interface address」エラーで IPv6 NAT が拒否される
CSCvu82738	インラインセットの show interface のドロップレートが正しくない
CSCvu83389	ASA がヌル TEID の GTPV1 転送再配置要求メッセージをドロップする
CSCvu84066	/32 マスクの BFD マップ送信元アドレスが機能しない

不具合 ID	タイトル
CSCvv34140	ASA IKEv2 VTI：レスポンダとして CTM から SPI を要求できない
CSCvv89708	ASA/FTD がスレッド名 fover_FSM_thread でトレースバックし、リロードすることがある
CSCvw26331	スレッド名 ci/console での ASA のトレースバックとリロード
CSCvw36662	TACACS+ ASCII パスワード変更要求が正しく処理されない
CSCvw48517	ASA を 9.13(1)13 にアップグレードすると、DAP が動作しなくなる
CSCvw50679	アップグレード中に ASA/FTD がトレースバックおよびリロードすることがある
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
CSCvh75756	重複するプリプロセッサキーワード：ssl（Duplicate preprocessor keyword: ssl）
CSCvs91270	インスペクションの中断：展開ページでエラーが発生
CSCvt26530	「Snort の障害により他のユニットのインスペクションエンジンに障害が発生しました（Inspection engine in other unit has failed due to snort failure）」が原因で FTD がフェールオーバーした
CSCvv04023	FDM（オンボックスマネージャ）：インターフェイスが zones.conf から削除されたため、トラフィックが適切なルールでヒットしない
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
CSCvv69015	6.6.X のトラブルシューティング要求に CSD が応答しない
CSCvv73540	特定の制限を超えるとファイルキャッシュをドロップするモニターを作成
CSCvw38810	AWS の FTD：6.6.1 へのアップグレード後にディスクマネージャプロセスが開始されない
CSCvw41728	FTD で CLI を使用して syslog を設定できない
CSCvu68529	Embryonic 接続制限が一貫して機能しない
CSCvv31629	トラフィックが非対称的に通過すると、断続的に埋め込まれた GRE 経由の ping 応答が FTD クラスタでドロップする
CSCvv69991	FTD が 6.6.1 へのアップグレード後にメンテナンスモードでスタックする
CSCvp47536	FTD での AAA 要求が RRI から学習した V ルートをたどらない

不具合 ID	タイトル
CSCvs91389	FTD トレースバック Lina プロセス
CSCvt04560	クラスタ展開でのファイアウォールで SCTP ハートビートが失敗する
CSCvt27585	スタンバイからのフェールオーバー切り替え実行中に 2100 でのトレースバックが発生する
CSCvt40306	ASA：リロード後にスタンバイユニットの BVI インターフェイスが応答を停止する
CSCvu58153	RADIUS ポートの表現がビッグエンディアンではなくリトルエンディアンとして表示される
CSCvv87232	ASA：igb_saleen_io_sfp_mod_poll_thread プロセスで CPU 専有の値が高くなる
CSCvv90720	ASA/FTD：HA スイッチオーバー後に接続されたスイッチで MAC アドレステーブルのフラッピングが表示される
CSCvv94701	ASA が「octnic_hm_thread」でリロードし続け、リロード後は回復するまでに非常に長い時間がかかる
CSCvw00161	Firepower 2140 での VPNス レッドによる ASA のトレースバックとリロード
CSCvw12008	「show tech-support」コマンドの実行中の ASA トレースバックとリロード
CSCvw21844	カプセル化されたフローを処理する際の DATAPATH スレッドでの FTD トレースバックとリロード
CSCvw37259	デバイスがハング状態になるまで 600/秒のレートで VPN syslog が生成される
CSCvx09248	v2 および v3 の SNMP ウォークが失敗し、この OID でこのエージェントで使用可能なオブジェクトがありませんと表示される
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
CSCvt89183	FDM が管理 Web サーバー経由で CA 署名付き証明書をロードできない
CSCvu75315	6.6.0 へのアップグレード後、レポートに棒グラフと円グラフで侵入イベントが表示されない
CSCvu79102	FTD-API/FDM：HA 同期ステータスがスタンバイで失敗する
CSCvv40316	FDM：スマート CLI ルーティングオブジェクトを使用して BGP の 11 番目のネイバーを追加できない

不具合 ID	タイトル
CSCvx09324	名前のない EtherChannel インターフェイス内の名前付き/名前のないサブインターフェイスの場合、設定のインポートが失敗する
CSCvu45822	ASA でトレースバックが発生し、リロードされた
CSCvv04584	resson no-mcast-intrf でマルチキャストトラフィックがドロップされている
CSCvg69380	ASA：まれに発生した CP 処理での破損によってコンソールロックが発生する
CSCvt73407	ASA デバイスの ユーザー名 enable_15 に対する TACACS フォールバック認証が失敗する
CSCvu29660	使用可能なブロックがゼロになっても、ブロック枯渇スナップショットが作成されない
CSCvu97764	TAP モードの FTD が出力インターフェイスでキャプチャされない
CSCvv36518	ASA：CSCuw51499 修正後のリロード後のダウンタイムが延長される
CSCvv36725	ASA logging rate-limit 1 5 message ... 5 秒ではなく 10 秒内に 1 メッセージに制限
CSCvv37108	ネイバーからの OSPF LS アップデートメッセージを ASA がサイレントにドロップする
CSCvv52591	ctm_hw_malloc_from_pool で DMA メモリリークが発生し、管理接続と VPN 接続が失敗する
CSCvv67500	DATAPATH での ASA 9.12 のランダムトレースバックおよびリロード
CSCvw45863	リロード時の ASAv SNMP トレースバック
CSCvw47321	一部の FPR プラットフォームのインバウンドトラフィックの IPSec トランスポート モード トラフィックの破損
CSCvw51462	IPv4 デフォルトトンネルルートが拒否される
CSCvw53427	ASA が複数のクエリパラメータを含む SAML アサーションで HTTP POST を処理できない
CSCvw84786	スレッド名 snmp_alarm_thread での ASA トレースバックおよびリロード
CSCvr55741	展開に成功した後、FMC に旧ポリシーが表示される
CSCvt31292	FTD デバイスが SSE にイベントを送信しない場合がある
CSCvu63397	整数オーバーフロー（FileExtract 正常性アラート内）により、ログスパム「file capture perf stats」が発生する

不具合 ID	タイトル
CSCvu82272	管理対象デバイスの非アクティブな古いエントリが原因で、Firepower Management Center でのアップグレードが失敗することがある
CSCvu85421	次のメッセージで展開が失敗する：「クリプトマップ s2sCryptoMap がインターフェイス内にありません（no crypto map s2sCryptoMap interface inside）」
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
CSCvv79705	POE の NPE が原因で 800_post/100_ftd_onbox_data_import.sh で 6.6.0 または 6.6.1 へのアップグレードが失敗する
CSCvw49531	VDB のアップグレード後にアプリケーションが誤って分類される
CSCvw60741	6.6.1 へのアップグレード後に「show version」で出力が表示されない
CSCvv23370	webVPN、SNMP 関連トラフィックの実行中に FPR2130 でトレースバックが発生した
CSCvv28997	スレッド名 Crypto CA での ASA トレースバックおよびリロード
CSCvv44051	GRE/IPiniP パッセンジャフローによる snp_cluster_forward_and_free_packet でのクラスタ ユニット トレースバック
CSCvv44270	ASAv5 がトレースバックなしでリロードする
CSCvv54831	パケットトレーサコマンドの実行時の ASA トレースバックおよびリロード
CSCvo34210	スレッド名 Unicorn Proxy Thread で ASA が 9.6.4.20 トレースバックを実行する
CSCvt15163	Cisco ASA および FTD ソフトウェアの Web サービスに関する情報漏洩の脆弱性
CSCvu48886	デフォルト以外の「crypto ikev2 limit max-in-negotiation-sa」を削除すると FTD の展開が失敗する
CSCvu93278	AnyConnect-IKEv2 スケーリング接続で作業中に KP でクラッシュが確認される
CSCvv16082	stress/low memory: assert: mh->mh_mem_pool > MEMPOOL_UNDEFINED && mh->mh_mem_pool < MEMPOOL_MAX_TYPE
CSCvv25394	アップグレード後、ASA がディスクの名前を交換して disk0 が disk1になり、disk1 が disk0 になった

不具合 ID	タイトル
CSCvv58332	ASA/FTD が BGP MP_REACH_NLRI 属性のネクストホップバイトを逆順で読み取る
CSCvw16619	オフロードされたトラフィックが ECMP セットアップでセカンダリルートにフェールオーバーされない
CSCvw19907	agx 通信の snmpd の再起動が snmp-sa に対して失敗する
CSCvw31569	ディレクタ/バックアップフローは残され、このフローに関連するトラフィックがブラックホール化される
CSCvw43486	PBR 設定変更時の ASA/FTD トレースバックとリロード
CSCvt39292	LDAPS 外部ユーザーが Firepower 4110 で「sudo su」を実行できない
CSCvt86467	c3p0 0.9.5.2 では、com/mcha の extractXmlConfigFromInputStream で XXE が許可される
CSCvu85381	スタンバイでのポリシー展開の失敗に続いて HA の再構成が失敗する
CSCvv09477	Oracle MySQL の MySQL サーバー製品の脆弱性（コンポーネント：
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
CSCvv43864	ポリシーを変更すると、変更ログのプレビューが空白になる
CSCvv51623	Manual-NAT-rule が、展開後、Lina の実行コンフィギュレーションの before-auto-nat-section に移動される
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
CSCvw23286	データベースオプティマイザが途中で終了するため、FMC で MySQL の CPU 使用率が高くなる
CSCvw38870	800_post/1027_ldap_external_auth_fix.pl で、6.7.0 への FMC のアップグレードが失敗する
CSCvw66953	URL カテゴリを Beaker に変換するときにアップグレードが失敗する
CSCvx01381	手動時刻設定用の FMC GUI の [Year] ドロップダウンリストに 2020年 までしか表示されない
CSCvu43827	スレッド名「cluster config sync」または「fover_FSM_thread」での ASA および FTD クラスタ ユニット トレースバック
CSCvu48285	TACACS REST API：/cli api を使用して設定された ASA が「Command authorization failed」メッセージで失敗する

不具合 ID	タイトル
CSCvv02245	ASA「session sfr」コマンドが初期設定のために FirePOWER モジュールから切断する
CSCvv08684	クラスタサイト固有の MAC アドレスが、フローオフロードによって書き換えられない
CSCvv34003	ISA 3000 で OID 1.3.6.1.2.1.47.1.1.1.1.5 の snmpwalk が、.16 および .17 に対して値 0 を返す
CSCvv57842	WebSSL クライアントレス ユーザー アカウントが最初の不正なパスワードでロックアウトされている
CSCvr33428	FMC が SYN フラッド攻撃から接続イベントを生成する
CSCvs07922	アクティブ ASA で、IPv6 を使用した WebVPN に対して不正な IP を含むロギングメッセージが生成される
CSCvs81763	vFTD が VLAN タグ付きトラフィックを渡すことができない（トランクモード）
CSCvt56923	FTD の手動による証明書の登録が、組織の件名フィールドの "&"（アンパサンド）が原因で失敗する
CSCvt70664	ASA：AnyConnect の Radius Acct-Requests に acct-session-time アカウンティング属性がない
CSCvt70879	vpn-filter に使用される ACL での「clear configure access-list」がリソースにアクセスできない
CSCvt89790	「snmp-server location」を設定すると、ASA 9.14.1 の「snmp-server contact」にも同じ値が設定される
CSCvt97205	ASA 9.14.1 上で SNMPPOLL/SNMPTRAP からリモートエンド（サイト間 VPN）ASA インターフェイスが失敗する
CSCvt99137	クラスタに大量の FTP トラフィックがあると、SEC_FLOW メッセージが再送信ループ状態になる
CSCvu40834	ネイティブ SSP プラットフォームでのカレンダー更新のマージの損傷を修正
CSCvu59573	「admin」で始まるグループ URL が正しく機能しない
CSCvu98222	SSL 復号ポリシーを有効にした後、FTD Lina エンジンがデータパスでトレースバックすることがある
CSCvu98468	SDI：新しいデバイスがフェールオーバーに参加すると、SDI ファイルがスタンバイに同期されない

不具合 ID	タイトル
CSCvv37629	不正な SIP パケットにより SIP 接続タイムアウトまで 4k ブロックのホールドアップが発生し、トラフィックの問題を引き起こす可能性がある
CSCvv53696	Anyconnect ユーザーの AAA または CoA タスク中の ASA/FTD トレースバックおよびリロード
CSCvv87496	「VPN packet redirect on peer」による ASA クラスタメンバー 2048 ブロックの枯渇
CSCvw22881	radius_rcv_auth により、コントロールプレーンの CPU 使用率が 100% になることがある
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
CSCvw83572	バージョン 9.14.1.30 以降で BVI HTTP/SSH アクセスが機能しない
CSCvw83780	プロセス名：lina におけるスタンバイ FTD 6.6.1 コア
CSCvx09123	ISA3000 上の M500IT モデルのソリッドステートドライブが 3 年 2 ヵ月のサービス期間後に応答しなくなることがある
CSCvx17785	ACL を追加または削除し、route-map コマンドに入力すると、クラッシュが絶えず発生する
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
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
CSCvt15056	ASDM によって管理される SFR：システムポリシーが適用されない
CSCvt80172	CVE-2017-11610 に対処するには、スーパーバイザソフトウェアをアップグレードする必要がある
CSCvu17819	vFTD での SSH RBAC の 6.7.0 へのアップグレードが失敗する
CSCvu32449	FDM：AnyConnect「名前が重複しているため、検証に失敗しました：（Validation failed due to duplicate name:）」
CSCvv25839	SSl 復号が有効な場合、reCAPTCHA が機能しない
CSCvv46490	SnortAttribConfig のエラーにより FMC でポリシーの展開が失敗する
CSCvw62820	Memcached 1.5.6 以降の更新

バージョン 6.6.1 で解決済みの問題

表 *51* : バージョン *6.6.1* で解決済みの問題

問題 ID 番号	説明
CSCtb41710	CDP が使用できない場合にのみ none にフォールバックする ASA 失効チェック
CSCvb92169	ASA が、より適切なフラグメント関連のログと ASP ドロップの理由を提供する必要がある
CSCvh19161	スレッド名：SXP CORE での ASA/FTD トレースバックおよびリロード
CSCvk51778	ASA 5515/5525/5545/5555 での「show inventory」（または）「show environment」でドライバ/ioctl エラーログが表示される
CSCvn64647	tcp_retrans_timeout 内部スレッド処理による ASA トレースバックおよびリロード
CSCvn82441	[SXP] FPR-2110 の ASA とスイッチ間での SXP 接続の確立に関する問題
CSCvn93683	ASA：cluster exec show コマンドですべての出力が表示されない
CSCvn95731	スレッド名 SSH での ASA トレースバックおよびリロード
CSCvq87625	ENH：「show tech」出力への「show run all sysopt」の追加
CSCvq93836	ENH：「show tech」出力への「show logging setting」の追加
CSCvr02080	多数のエントリを含む CRL のデコード中に、CERT API プロセスで CPU 占有が観察される
CSCvr15503	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
CSCvr57051	ポリシーの展開にエラー「HASH 参照としての未定義の値を使用できません（Can't use an undefined value as a HASH reference）」で失敗しました。
CSCvr58411	新しいスタティックスポークを追加または変更した場合、新しいスタティックハブ/スポーク設定の RRI がハブで動作しない
CSCvr60195	ASA/FTD がスレッド名「HTTP Cli Exec」でトレースバックおよびリロードすることがある
CSCvr98881	トレースバック：FTD ZeroMQ メモリアサーション
CSCvr99642	トレース「webvpn_periodic_signal」を使用した複数回の ASA トレースバックおよびリロード

問題 ID 番号	説明
CSCvs09533	FP2100：3 つ以上のインラインセットを介したトラフィックの処理時のトレースバックおよびリロード
CSCvs21705	admin ユーザーは、ドメイン内のデバイスルーティング設定にアクセスする権限がない
CSCvs33852	バージョン 9.6.4.34 へのアップグレード後、アクセスグループを追加できない
CSCvs38785	syslog のタイムスタンプ形式が一貫していない
CSCvs39253	バージョン 6.4 で Firepower 7000 および 8000 が電子メールを送信できない
CSCvs41883	ND ポリシー参照が見つからない場合、6.4.0.x へのアップグレード後に展開が失敗する
CSCvs45111	CCM レイヤ（スプリント 75）での WR6 および WR8 コミット ID の更新
CSCvs52108	Umbrella インスペクションによる ASA トレースバック
CSCvs55603	ACL で一致した場合に ICMP 応答がドロップされた
CSCvs59056	Float-Conn が有効になっている場合、ASA/FTD トンネルスタティックルートが準最適なルックアップによって無視される
CSCvs64510	メッセージ（「Can't call method "binip" on unblessed reference」）が表示されて展開が失敗する
CSCvs72393	FPR1010 温度しきい値を変更する必要がある
CSCvs73754	ASA/FTD：BVI の ARP が物理インターフェイスに割り当てられていないために発生するブロック 256 サイズの枯渇
CSCvs79023	スレッド名での ASA/FTD のトレースバック：DNS インスペクションによる DATAPATH
CSCvs82829	Anyconnect 設定がサイト間 VPN トンネルに追加されるとコールが失敗する
CSCvs88413	バージョン 9.8 へのアップグレードにポートチャネルのバンドルに失敗する
CSCvs90100	ASA/FTD がスレッド名「License Thread」でトレースバックおよびリロードすることがある
CSCvs94061	クロックのずれとトラフィックの中断を引き起こすNTP スクリプトエラー
CSCvs97863	フラッシュファイルシステムでのクローズ時の fsync コールの数を減らす

問題 ID 番号	説明
CSCvt00113	SNMP コミュニティストリングのメモリリークによる ASA/FTD トレースバックおよびリロード
CSCvt01282	CCM レイヤ（スプリント 79）での WR6 および WR8 コミット ID の更新
CSCvt01397	LINA 設定がプッシュされなかったにもかかわらず、展開は正常としてマークされる
CSCvt02409	FPR9300 3 ノードクラスタのネストされた VLAN トラフィックで 9.12.2.151 snp_cluster_ingress がトレースバックする
CSCvt03598	Cisco ASA ソフトウェアおよび FTD ソフトウェア Web サービスの読み取り専用パストラバーサルの脆弱性
CSCvt05862	サーバーが管理インターフェイスを介して到達可能な場合、IPv6 DNS サーバーの解決が失敗する
CSCvt06606	フローオフロードが FTD 6.2(3.10) と FXOS 2.6(1.169) の組み合わせで機能しない
CSCvt06841	ASA でのキャプチャを使用して設定すると、誤ったアクセスリストのヒットカウントが表示される
CSCvt11742	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
CSCvt12463	ASA：Unicorn Admin Handler スレッドでのトレースバック
CSCvt13730	FP1010/2100 - FTD：リリース 6.6.0 への FTD アップグレード後の管理ポートのダウン/ダウン
CSCvt15062	FTD 2100：デバイスのリブート時に BYPASS から NON-BYPASS への移行中にパケットがドロップする
CSCvt16642	FMC がリモートの syslog サーバーに対して一部の監査メッセージを送信していない
CSCvt18337	アップグレード後に HA ノードでフェールオーバーが無効になった
CSCvt20709	SSL を挿入した RESET での方向が誤っていたため、誤ったインターフェイスから出力され、MAC フラップが発生する
CSCvt21041	スレッド「ctm_ipsec_display_msg」での FTD のトレースバック
CSCvt23643	データを復旧するための、VPN フェールオーバーリカバリに約 30 秒かかる
CSCvt24328	FTD：lina_host_file_open_raw 関数に関連するトレースバックとリロード

問題 ID 番号	説明
CSCvt26031	ASAv が IPv6 を使用してスマートライセンスを登録できない
CSCvt26067	セカンダリインターフェイスが FTD で使用されている場合、アクティブ FTP が失敗する
CSCvt28182	sctp-state-bypass がインライン FTD に対して呼び出されない
CSCvt29049	FPR2100：アプライアンスモードでの ASA の SNMP 遅延
CSCvt30731	CCM レイヤ（スプリント 80）での WR6、WR8 および LTS18 コミット ID の更新
CSCvt34894	Snort が過剰なメモリを消費し、パフォーマンスの問題を引き起こす。
CSCvt35233	DAQ モジュール process_snort_verdict 判定ブラックリストからの過剰なロギング
CSCvt35945	9.8 トレインで SSH バージョン2を有効にする場合に Encryption-3DES-AES が必要であってはならない
CSCvt36542	FPR 上のマルチコンテキスト ASA/LINA が DHCP リリースメッセージを送信しない
CSCvt37881	https のブロックページが機能しない
CSCvt38279	ISA3000 で disk0 を消去すると、ファイルシステムがサポートされなくなる
CSCvt39135	SSL ポリシーが適用された状態で、SSL 以外のトラフィックが少ないときに Snort インスタンスにより CPU が 90% を超えてスパイクする
CSCvt39349	展開ステータスが [DEPLOYED] または [FAILED] である限り、デバイスの登録を許可する必要がある
CSCvt41333	IKEv2 トンネルのダウン時にダイナミック RRI ルートが破棄されない
CSCvt43967	ゼロを含む長さが 46 バイト以下のパディングパケットを RA トンネルから受信した
CSCvt45206	アップグレード前に存在していたイベントを検索すると、イベント検索が失敗することがある
CSCvt45863	IP ヘッダーの長さがパケット長と一致しない場合に暗号リングが停止する
CSCvt46289	Firepower 1000 シリーズで ASA LDAPS 接続が失敗する
CSCvt46830	FPR2100 「show crypto accelerator statistics」 カウンタは対称暗号を追跡しない

問題 ID 番号	説明
CSCvt50528	ASA/FTD - CLI での証明書のインストールに関するデフォルト設定の警告メッセージ
CSCvt50946	CSCvi42008 の修正にもかかわらず stuck uauth エントリが AnyConnect ユーザー接続を拒否する
CSCvt51346	PKI-CRL：ダウンロード時のメモリリークおよび大きな CRL のクリア
CSCvt51348	PKI-CRL：ループ内の大きな CRL をクリアせずにダウンロードした時のメモリリーク
CSCvt51349	フラグメント所有者に転送されたフラグメント化されたパケットが、データ インターフェイス キャプチャで表示されない
CSCvt51987	ASA FPR9300 SM56 での 80 サイズのブロックの枯渇によりトラフィックが停止する
CSCvt52607	SSL HW モードのフローテーブルメモリの使用率を引き下げて Snort が D 状態になる確率を低減する
CSCvt52782	ASA トレースバックスレッド名：webvpn_task
CSCvt53640	SFR を 6.4.0 から 6.4.0.9-34 にアップグレードした後の ASA5585 トレースバックおよびリロード
CSCvt54182	FTD が SSL 複合を実行するように設定されている場合に LINA コアが生成される
CSCvt59015	KP IOQ ドライバ。防御パラメータと状態チェックを追加する。
CSCvt59770	FTD：SCEP を介した証明書の取得の失敗により停止する
CSCvt61370	通信のデッドロックが原因で、デバイスからのイベントが停止することがある
CSCvt63484	igb_saleen_io_sfp_mod_poll_thre プロセスにより ASA の CPU 使用率が高くなる
CSCvt64035	remote acess mib：ラップアラウンド前に SNMP 64 ビットのみが 4Gb を報告する
CSCvt64270	ASA が、誤った宛先 MAC アドレスを持つフェールオーバー インターフェイス チェック制御パケットを送信している
CSCvt64822	ASA が SSL ハンドシェイク後にトレースバックし予期せずリロードすることがある

問題 ID 番号	説明
CSCvt65982	RRI ルートの削除時にスレーブユニットでルートフォールバックが発生しない
CSCvt66351	NetFlow のレポートのフローのバイト数が非常に大きい
CSCvt68131	スレッド「IKEv2 Mgd Timer Thread」で FTD がトレースバックし、リロードする
CSCvt68294	Firepower 4120 の最大 VPN セッション制限を 20,000 に調整する
CSCvt68819	アップグレード前に存在していたイベントをコピーすると、クリップボードへのコピーが失敗することがある
CSCvt73806	FP2120 LINA アクティブボックスでの FTD のトレースバックとリロード。[VPN]
CSCvt75241	FPR2100 で FTD をリロードした後、VPN でアドバタイズされたスタティックルートの再配布が失敗する
CSCvt75741	netsnmp-5.8 を AES 192/256 サポートでコンパイルする
CSCvt79777	sfipproxy.conf で IP アドレスが重複している
CSCvt79988	FMC を 6.6 にアップグレードした後、SNMP 設定が原因でポリシー展開が失敗する
CSCvt80126	CLI の「show asp table socket 18421590 det」で ASA がトレースバックし、リロードする
CSCvt83133	group-url を使用して Google Chrome から anyconnect webvpn ポータルにアクセスできない
CSCvt85815	「機密データの検出」を有効にすると、ポリシーの展開が失敗する
CSCvt86188	診断インターフェイスを介して SNMP トラップを生成できない
CSCvt90330	スレッド名 coa_task での ASA トレースバックおよびリロード
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
CSCvt91521	暗号化アクセラレータバイアス設定を show tech に含める必要がある
CSCvt92647	ASA のアップグレード後に、IPv6 アドレスで設定されたステートリンクを介した接続が失われる
CSCvt93142	ASA は、クライアント認証の証明書にヌルシーケンスのエンコーディングを許可する必要がある

問題 ID 番号	説明
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
CSCvt95517	FTD 上の AnyConnect の証明書マッピングが機能しない
CSCvt97917	AWS 9.13.1.7 BYOL イメージ上の ASAv を PLR に対して有効にできない
CSCvt98599	IKEv2 コールアドミッション統計情報の「Active SAs」カウンタが実際のセッション数と同期していない
CSCvu00112	ssh クォータ制限が ci_cons_shell でヒットしたときに tsd0 がリセットされない
CSCvu01039	トレースバック：アクティブなトラフィックでの FTD インラインセットタップモード設定の変更
CSCvu03107	AnyConnect 統計情報が %ASA-4-113019 と RADIUS アカウンティングの両方で二重になる
CSCvu03562	ユーザー名とパスワードを入力すると、デバイスの SSH 接続が失われる
CSCvu03675	FPR2100：メモリ不足の状態で ASA コンソールがハングして応答しなくなることがある
CSCvu04279	ASAv/AWS：AWS で C5 ASAv コードをアップグレードまたはダウングレードできない
CSCvu05180	リモートアクセス VPN ポリシーの展開後、FTD で AAA サーバー設定が欠落している
CSCvu05216	CRL CDP オーバーライドを指定する証明書マップでバックアップエントリが許可されない
CSCvu05336	ASAv：SNMP プロセスでのトレースバックおよびリロード
CSCvu05821	タイムスタンプ形式が常に UTC で表示される
CSCvu07602	FPR-41x5：「clear crypto accelerator load-balance」によりトレースバックおよびリロードが発生する
CSCvu07880	QP プラットフォーム上の ASA で誤ったコアダンプファイルシステム領域（50 GB）が表示される
CSCvu08013	DTLS v1.2 および AES-GCM 暗号を使用すると、特定のサイズのパケットが頻繁にドロップされる
CSCvu09199	6.7.0 FMC で 6.6.0 ftd イメージのプッシュ アップグレード イメージに 30 分かかる

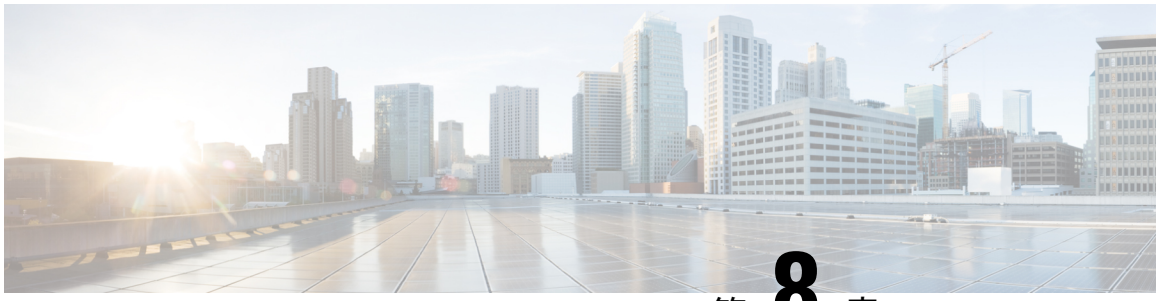
問題 ID 番号	説明
CSCvu10053	ASA トレースバックおよび関数 snmp_master_callback_thread のリロード
CSCvu10900	大量の ssl-certs-unified.log ファイルが、トラブルシューティングで 9GB に寄与
CSCvu12039	起動後にスレーブユニットがクラスタマスターからの SCTP 設定の同期に失敗することがある
CSCvu12248	ユーザーが AnyConnect VPN を使用して接続する場合の ASA-FPWR 1010 トレースバックおよびリロード
CSCvu12307	FTD-HA：「ERROR：指定された AnyConnect クライアントイメージは存在しません。」
CSCvu12684	HKT：9.8.4.15 へのアップグレードでフェールオーバー時間が増加する
CSCvu13287	FDM がサブジェクトまたは発行元のない証明書をインポートできず、アップグレードも失敗する
CSCvu15611	FTD-HA：スタンバイが HA に参加できない「CD アプリ同期エラーはアプリ構成の適用に失敗しました」
CSCvu17924	DATAPATH での FTD フェールオーバーユニットのトレースバックおよびリロード
CSCvu17965	手動 NAT ルールのポート値を変更すると、ASA でトレースバックが生成され、リロードされる
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 の接続イベントが失われる
CSCvu20007	LINA からの Config_XML_Response の形式が正しくない。Lina が使用可能なメモリがないと報告している。
CSCvu20257	CCM レイヤ（スプリント 85）での WR6、WR8 および LTS18 コミット ID の更新
CSCvu23289	多数の neostore.transaction.db.* ファイルによってディスクがいっぱいになり、neo4j の問題が発生する
CSCvu25030	スレッド名：CP processing での FTD 6.4.0.8 トレースバックおよびリロード
CSCvu26296	ASA インターフェイス ACL が ASA からの snmp コントロールプレーン トラフィックをドロップしている
CSCvu26561	Kerberos と統合すると、WebVPN SSO が予期しない結果になる

問題 ID 番号	説明
CSCvu26658	SFDataCorrelator がバックアップ操作中にイベントをドロップすることがある
CSCvu29145	Snort フロー IP プロファイリングでは、「system support flow-ip-profiling start」コマンドを使用して有効にできない
CSCvu29395	アクティブな IGMP join でマスターロールの変更を実行中にトレースバックが発生した
CSCvu30512	PKI-CRL：メモリトラッキングが有効になっている CRL のクリア中にトレースバックが発生した
CSCvu32698	「key config-key password-encryption」が存在する場合、クラスタに参加する際に ASA が SNMP でクラッシュする
CSCvu34413	リロード後に ASA で SSH キーが失われる
CSCvu36539	スマートライセンスデバイスが 6.2.2 -> 6.4.0 -> 6.6.0 にアップグレードされた場合、アップグレードが失敗する。
CSCvu37547	メモリリーク：リソース制限 MIB ハンドラが原因で、最終的にリロードが発生する
CSCvu38795	無効なインターフェイスの GOID エントリが原因で、トレースバック後に FTD ファイアウォールユニットがクラスタに参加できない
CSCvu40213	スレッド名 kerberos_recv での ASA トレースバック
CSCvu40324	フロールックアップ呼び出しトレースバックによる ASA トレースバックおよびリロード
CSCvu40398	FIPS を有効にした後の FIPS SELF-TEST FAILURE による ASAv のリロード
CSCvu40531	pktmgr.out および lacp.out への FXOS LACP パケットロギングにより /opt/cisco/platform/logs が 100% になる
CSCvu42434	ASA：実行中の SSH セッションがスタックしているため CPU 使用率が高い/ASA に SSH できない
CSCvu43924	DHCP 検出パケットの GIADDR が dhcp-network-scope の IP アドレスに変更される
CSCvu45748	スレッド名「ppp_timer_thread」での ASA トレースバック
CSCvu49625	[PKI] 標準ベースの IKEv2 証明書認証セッションが 2 番目の userfromcert ルックアップを不必要に実行する

問題 ID 番号	説明
CSCvu53258	FMC が証明書マップを誤って lina にプッシュする
CSCvu53585	6.6.0 へのアップグレード後に Elektra onbox ポリシーの展開が失敗する
CSCvu55843	TACACS 承認ユーザーによる設定変更後の ASA トレースバック
CSCvu57834	100% CPU を使用する syslog-ng プロセス
CSCvu60011	FTD：障害状態の HA に展開された Snort ポリシーの変更が完全に同期されない
CSCvu61704	ASA の intel_82576_check_link_thread を使用した高い CPU 使用率がユニット全体のパフォーマンスに影響する
CSCvu63458	FPR2100：show tech でクラッシュ出力を表示すると、最新のトレースバックからの出力が表示されない
CSCvu65070	Lina 9.14：デバッグ snmp フレームワークを改善して agentx を使用し SIGHUP を回避する
CSCvu65688	CSCvt98599 にもかかわらず、IKEv2 CAC の「Active SAs」カウンタが実際のセッション数と同期していない
CSCvu65843	FP2100：6.6.0 での自動ネゴシエーションの変更によるファイバ SFP インターフェイスのダウン
CSCvu65936	FDM 6.6.0 のアップグレード（または）configImport が EtherChannelInterface でフェールオーバーリンク検証の失敗として失敗する
CSCvu66119	シリーズ 3 で URL ルールが誤って昇格されると、トラフィックが誤ったルールに一致する
CSCvu70529	snort のリロード時にバイナリルール（SO ルール）がロードされない
CSCvu72094	スレッド名 DATAPATH での ASA トレースバックおよびリロード
CSCvu72278	バージョン 1.41.0 より前の nghttp2 で、非常に大きな HTTP/2 SETTINGS fra
CSCvu72280	PCR の pcre_jit_compile.c の compile_bracket_matchingpath 関数
CSCvu72658	AnyConnect 接続クライアント IP が断続的に OSPF にアドバタイズされない
CSCvu73207	AnyConnect ユーザーへの DTLS パケットで保持されない DSCP 値
CSCvu75594	FTD：すでに適用されているキャプチャでキャプチャ バッファ オプションを変更する場合のトレースバックとリロード

問題 ID 番号	説明
CSCvu75930	SMA リソースが枯渇すると、サービスモジュールがスーパーバイザにエラーを返さない
CSCvu75993	トランスペアレント トラフィックが KVM で展開された FTDv を通過しない（ルーテッドモード）
CSCvu77095	ASA がリマーク付きの ACE を削除できず、「指定されたリマークが存在しません」というエラーが表示される
CSCvu78721	アップグレード後にインターフェイス速度を変更（修正）できない
CSCvu79125	高度なマルウェアリスクレポートの生成に失敗する
CSCvu80143	9.14.1.12 でトレースバック後に snmpd が戻らない
CSCvu82918	HA 同期がスタンバイで予期しないエラーで失敗する
CSCvu83178	EIGRP サマリールートがスタンバイに複製されず、スイッチオーバー後に停止する
CSCvu83599	ASA がスレッド snmp_alarm_thread でトレースバックし、予期せずリロードすることがある
CSCvu90727	EAP-TLS 認証を使用するネイティブ VPN クライアントが ASA に接続できない
CSCvu91105	process_stdout.log ファイルが大きいため、/ngfw で管理対象外ディスクの使用率が高くなる
CSCvu98197	「復号しない」SSL 復号ルールに一致する HTTPS 接続がブロックされることがある
CSCvu98708	ASA：HA：IPv6 インターフェイスのスタンバイで SNMP ポーリングが失敗する
CSCvv03130	FTD clish で「show banner」コマンドを実行しても出力が返されない
CSCvv04092	イベントを表示しようとすると、誤った sql が生成される
CSCvv09944	WCCP 設定がプッシュされているときに FTD 展開時に LINA がトレースバックする
CSCvv10948	FDM アップグレード：UI で保留中の変更が表示されない（ただし、アップグレードは開始されていない）
CSCvv12273	hardwareStatus MIB で複数の OID を持つ snmpget を使用した SNMP get-response が noSuchObject を返す

問題 ID 番号	説明
CSCvv12943	脅威データに FDM 6.5 以上のバージョンで、6.4 には存在していた GID：SID フィールドがない（CDO に影響）
CSCvv12988	バックアップ中に tomcat が強制終了された後、正常に回復しない
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
CSCvv17434	Kenton5508 の 6.2.3 -> 6.6.1-50 アップグレードが失敗した
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
CSCvv26786	「プロセス名：lina」で ASA がトレースバックし、予期せずリロードする
CSCvv26845	ASA：SNMP 機能でウォッチドッグのトレースバックとリロード
CSCvv27750	ログがローテーションしないため、/ngfw で管理対象外ディスクの使用率が高くなる
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
CSCvv30371	SNMP：VPN ポーリングのメモリリーク
CSCvv31334	6.6.1 ー 63 の KP HA でピアを切り替えようとすると、Lina のトレースバックとリロードが発生する（ネストされたクラッシュがロックされる）
CSCvv33013	FDM：文字 ^ @ _ で秘密鍵を追加できない
CSCvv33621	vftd：diskmanager のモニターリングがアップグレード時に正しく機能しない
CSCvv69991	FTD が 6.6.1 へのアップグレード後にメンテナンスモードでスタックする



第 8 章

既知の問題

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

サポート契約がある場合は、Cisco Bug Search Tool を使用して最新のバグリストを取得できます。検索では、特定のプラットフォームとバージョンに影響するバグに絞り込むことができます。バグのステータス、バグ ID ごとに検索したり、特定のキーワードを検索することもできます。

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

• バージョン 6.6.0 で未解決のバグ （141 ページ）

バージョン 6.6.0 で未解決のバグ

表 *52* : バージョン *6.6.0* で未解決のバグ

不具合 ID	タイトル
CSCvr90564	ユーザー VRF のエリア間 OSPF 設定を無効にすると、展開が失敗する
CSCvt14898	RAVPN を使用したアップグレード後に展開に失敗する（no split-tunnel-network-list value RA-VPN-policy|splitAcl）
CSCvt29546	同じボックスにバックアップを復元した後に、ライセンスの登録が解除される
CSCvt37753	MI クラスタでポリシーの展開が失敗する
CSCvt39442	管理者ユーザーが原因でダッシュボードウィジェットが表示されない

不具合 ID	タイトル
CSCvt43431	CLI の管理インターフェイス設定の変更後、UI では CLI の変更が更新されていなかったOOB の同期の問題
CSCvt61370	通信のデッドロックが原因で、デバイスからのイベントが停止することがある
CSCvt66906	セッションでアプリケーションが検出された場合でも、Appid はダイナミックキャッシュを検索する
CSCvt68316	インポートの失敗後に展開が絶えず失敗し、変更を破棄できない
CSCvt68819	アップグレード前に存在していたイベントをコピーすると、クリップボードへのコピーが失敗することがある
CSCvt69260	接続イベントに古いデバイス名が表示される
CSCvt70854	6.6.0-90： [Firepower 1010] メモリ不足のため、SRU の更新中に tomcat が再起動する
CSCvt77143	Apache Commons FileUpload の HTTP リクエストヘッダーの値の処理の拒否
CSCvt77210	1.2.2 よりも前の minimist では正しく追加または変更されているように見える場合がある
CSCvt78634	アサーションドメイン ID を使用したポリシー展開時に FTD lina がトレースバックする
CSCvt79988	FMC を 6.6 にアップグレードした後、SNMP 設定が原因でポリシー展開が失敗する
CSCvt86467	c3p0 0.9.5.2 では、com/mcha の extractXmlConfigFromInputStream で XXE が許可される
CSCvt87117	libexpat 不適切な解析によるサービス拒否の脆弱性
CSCvt87123	Expat libexpat XML パーサーに関するサービス拒否の脆弱性
CSCvt89042	dom4j XML インジェクションの脆弱性
CSCvt89045	Redis redis-cli バッファオーバーフローの脆弱性
CSCvt89378	ログイン時に「データベースに重大なエラーが発生しました。再起動する必要があります（The database has encountered a critical error, and needs to be restarted.）」という UI エラーが表示される
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

不具合 ID	タイトル
CSCvt97205	ASA 9.14.1 上で SNMPPOLL/SNMPTRAP からリモートエンド（サイト間 VPN）ASA インターフェイスが失敗する
CSCvt99082	Rest API：拡張アクセスリストの URL が extendedaccesslist から extendedaccesslist に変更された
CSCvu06882	KVM ASAv からの virtio インターフェイスのホットプラグ削除によりクラッシュが発生する
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
CSCvu13287	FDM のアップグレードが 800_post/100_ftd_onbox_data_import.sh で失敗する
CSCvu16826	リリース6.6へのアップグレード後に snort ルールが破損しているため、FTD snort インスタンスがダウンする
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 の接続イベントが失われる
CSCvu20690	2.1.3 より前の dom4j で、外部 DTD および外部エンティティがデフォルトで許可される
CSCvu29145	Snort フロー IP プロファイリングでは、「system support flow-ip-profiling start」コマンドを使用して有効にできない
CSCvu30441	FMC 6.6 REST API GUI では、新しいアクセスルールを PUT または POST しようとする際に応答がない
CSCvu30748	PTHREAD-1859 でバージョン 9.14.1 にアップグレードした後の ASAv のトレースバックおよびリロード
CSCvu35426	リーフドメインのスケジュール展開では、1 つのデバイスのみがポリシーを展開する
CSCvu35768	FMC を 6409-59 から 6.6.0-90 にアップグレードした後、サブドメイン内の Radius 外部ユーザーを使用して UI をログに記録できない
CSCvu38869	jQuery フレームワークが JavaScript Object Notation（使用できないソリューション）を使用してデータを交換する
CSCvu50400	Firepower 6.2.3.x から 6.6.0 にアップグレードした後、ASDM を使用する ASA FirePOWER の CPU 使用率が高くなる
CSCvu62018	SSL 復号を使用して最大検出 IPS を使用すると、ルール 129:12 によりトラフィックがブロックされる：Snort2
CSCvu65890	サポートされていないにも関わらず、FMC が SNMP3 設定で MD5 および DES から切り替えることができない

不具合 ID	タイトル
CSCvu70622	リロード後に CTS SGT 伝播が有効になる
CSCvu74702	ポリシーの展開後に検出エンジンが予期せず終了し、コアファイルが生成される
CSCvu75315	6.6.0 へのアップグレード後、レポートに棒グラフと円グラフで侵入イベントが表示されない
CSCvu79125	高度なマルウェアリスクレポートの生成に失敗する
CSCvu82272	管理対象デバイスの非アクティブな古いエントリが原因で、Firepower Management Center でのアップグレードが失敗することがある
CSCvu82578	ライトテーマ UI FMC：SFR モジュールでインターフェイスページのロード時に長い遅延が発生する
CSCvu84127	Firepower 2100：明確な理由なしに FTD がリブートする
CSCvu84556	サイト間ダイナミッククリプトマップが RA VPN ダイナミッククリプトマップの下に展開される
CSCvu96559	トレースバック：ASA で予期しないトレースバックが発生し、不完全なコアが生成される
CSCvv01558	6.6.0-90 を実行している ASA/ Elektra-HA デバイスで、sfhassd から「認識できないインスタンス（unrecognized instance）」のエラーが発生する
CSCvv04023	FDM（オンボックスマネージャ）：インターフェイスが zones.conf から削除されたため、トラフィックが適切なルールでヒットしない
CSCvw38870	800_post/1027_ldap_external_auth_fix.pl で、6.6.0、6.6.1、6.6.3、6.7.0 への FMC のアップグレードが失敗する