Cisco Firepower バージョン 6.2.3.1、6.2.3.2、6.2.3.3、6.2.3.4、6.2.3.5、6.2.3.6、6.2.3.7、6.2.3.9、6.2.3.10、6.2.3.11、6.2.3.12、6.2.3.13、6.2.3.14、6.2.3.15、および 6.2.3.16 リリースノート

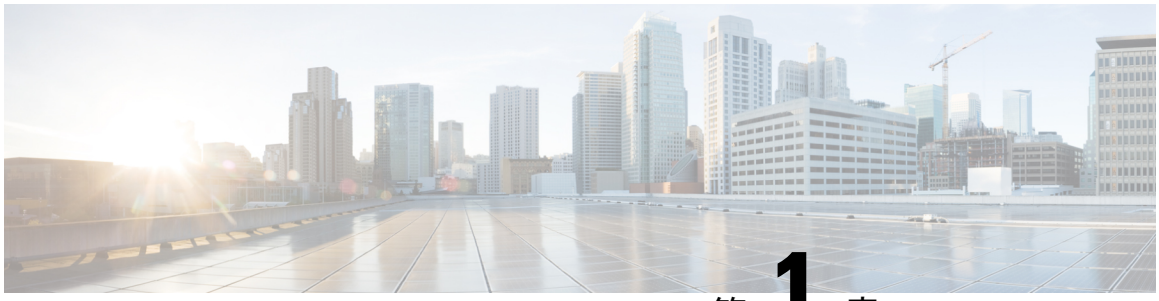
初版：2018 年 5 月 2 日

最終更新：2020 年 12 月 7 日

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

【注意】シスコ製品をご使用になる前に、安全上の注意（**www.cisco.com/jp/go/safety_warning/**）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

目 次



第 1 章

Version6.2.3.x の概要

Firepower をお選びいただき、ありがとうございます。

リリース ノートについて

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

アップグレードとインストールの手順については、次のリンクを参照してください。

リリース日

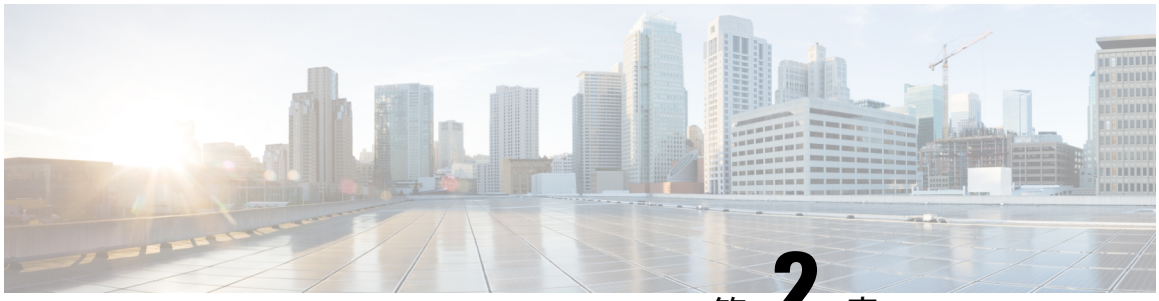
このバージョンで使用可能なすべてのプラットフォームのリストについては、互換性 （5 ページ）を参照してください。

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 （80 ページ）を参照してください。

表 *1 :* バージョン *6.2.3* のパッチの日付

バージョン	ビルド	日付	プラットフォーム
6.2.3.16	59	2020 年 7 月 13 日	すべて
6.2.3.15	39	2020 年 2 月 5 日	FTD/FTDv
	38	2019 年 9 月 18 日	FMC/FMCv Firepower 7000/8000 ASA FirePOWER NGIPSv
6.2.3.14	41	2019 年 7 月 3 日	すべて
	36	2019 年 6 月 12 日	すべて
6.2.3.13	53	2019 年 5 月 16 日	すべて
6.2.3.12	80	2019 年 4 月 17 日	すべて
6.2.3.11	55	2019 年 3 月 17 日	すべて
	53	2019 年 3 月 13 日	—
6.2.3.10	59	2019 年 2 月 7 日	すべて
6.2.3.9	54	2019 年 1 月 10 日	すべて
6.2.3.8	51	2019 年 1 月 2 日	利用できなくなりました。廃止された機能（16ページ）を参照してください。
6.2.3.7	51	2018 年 11 月 15 日	すべて
6.2.3.6	37	2018 年 10 月 10 日	すべて

バージョン	ビルド	日付	プラットフォーム
6.2.3.5	53	2018 年 11 月 6 日	FTD/FTDv
	52	2018 年 12 月 9 日	FMC/FMCv Firepower 7000/8000 ASA FirePOWER NGIPSv
6.2.3.4	54	2018 年 8 月 13 日	すべて
6.2.3.3	76	2018 年 7 月 11 日	すべて
6.2.3.2	46	2018 年 6 月 27 日	すべて
	54	2018 年 6 月 6 日	—
6.2.3.1	47	2018 年 6 月 28 日	すべて
	45	2018 年 6 月 21 日	—
	43	2018 年 5 月 2 日	—



第 2 章

互換性

廃止されたプラットフォームの販売終了およびサポート終了の通知へのリンクを含む、サポート対象の Firepower のすべてのバージョンの詳細な互換性情報については、『Cisco Firepower Compatibility Guide』を参照してください。

この Firepower バージョンの互換性情報については、次を参照してください。

Firepower Management Centerについて

Firepower Management Center（FMC）は、Firepower 展開の一元的な管理コンソールを提供するフォールトトレラントな専用ネットワークアプライアンスです。Firepower Management Center Virtual （FMCv）は、完全なファイアウォール管理機能を仮想化環境にもたらします。

Firepower Management Center

このリリースでは、次の FMC プラットフォームがサポートされています。

- FMC 1000、2500、4500
- FMC 2000、4000
- FMC 750、1500、3500

BIOS および RAID コントローラのファームウェアを最新の状態に保つことをお勧めします。詳細については、『Cisco Firepower Compatibility Guide』を参照してください。

Firepower Management Center Virtual

このリリースでは、次の FMCv の実装がサポートされています。

- Amazon Web Services（AWS）の FMCv
- カーネルベース仮想マシン（KVM）の FMCv
- VMware vSphere/VMware ESXi 5.5、6.0、または 6.5 の FMCv

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

Firepower デバイス

Cisco Firepower デバイスは、ネットワークトラフィックをモニタし、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。

次の表に、このリリースでサポートされているデバイスプラットフォームと、（個別にアップグレード可能な）OS/ハイパーバイザ要件を示します。バンドルされたオペレーティングシステムのバージョンとビルドについては、『Cisco Firepower Compatibility Guide』の「Bundled Components」の情報を参照してください。

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

Firepower Threat Defense デバイス

これらの FTD デバイスは、このリリースでサポートされています。

表 *2 :* バージョン *6.2.3* の *FTD*

FTD プラットフォーム	OS/ハイパーバイザ	詳細情報
Firepower 2110、2120、2130、2140	—	—

FTD プラットフォーム	OS/ハイパーバイザ	詳細情報
Firepower 4110、4120、4140、4150 Firepower 9300：SM-24、SM-36、SM-44 モジュール	FXOS 2.3.1.73 以降のビルド。 （注） Firepower 6.2.3.16+ には FXOS 2.3.1.157+ が必要です。	最初に FXOS をアップグレードします。 問題を解決するには、FXOS を最新のビルドにアップグレードする必要がある場合があります。判断のヒントについては、『Cisco Firepower 4100/9300 FXOS Release Notes, 2.3(1)』を参照してください。
ASA 5506-X、5506H-X、5506W-X ASA 5508-X、5516-X ASA 5512-X ASA 5515-X ASA 5525-X、5545-X、5555-X ISA 3000	—	FTD 展開では、これらのデバイスの OS を個別にアップグレードすることはありませんが、ISA 3000、ASA 5506-X、5508-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
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 5.5、6.0、または 6.5	サポートされているインスタンスについては、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。

NGIPS/ASA FirePOWER デバイス

これらの NGIPS/ASA FirePOWER デバイスは、このリリースでサポートされています。

表 *3 :* バージョン *6.2.3* の *NGIPS/ASA FirePOWER*

NGIPS プラットフォーム	OS/ハイパーバイザ	詳細情報
ASA 5506-X、5506H-X、5506W-X	ASA 9.6(x) ～ 9.9(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、厳密には ASA のアップグレードが必要でない場合でも、問題解決のために、サポートされた最新のバージョンへのアップグレードが必要になることがあります。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、ASA 5506-X、5508-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 5508-X、5516-X	ASA 9.5(2) ～ 9.15(x)	
ASA 5512-X	ASA 9.5(2) ～ 9.9(x)	
ASA 5515-X	ASA 9.5(2) ～ 9.12(x)	
ASA 5525-X、5545-X、5555-X	ASA 9.5(2) ～ 9.14(x)	
ASA 5585-X-SSP-10、-20、-40、-60	ASA 9.5(2) ～ 9.12(x)	
NGIPSv	VMware vSphere/VMware ESXi 5.5、6.0、または 6.5	サポートされているインスタンスについては、『Cisco Firepower NGIPSv Quick Start Guide for VMware』を参照してください。
Firepower 7010、7020、7030、7050 Firepower 7110、7115、7120、7125 Firepower 8120、8130、8140 Firepower 8250、8260、8270、8290 Firepower 8350、8360、8370、8390 AMP 7150、8050、8150 AMP 8350、8360、8370、8390	—	—

マネージャとデバイスの互換性

Firepower Management Center

すべての Firepower デバイスは、複数のデバイスを管理できる Firepower Management Center（FMC）を使用したリモート管理をサポートします。新しいFMCは、いくつかのメジャーバージョンまでの古いデバイスを管理できます。ただし、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。つまり、FMCは管理対象デバイスと同じバージョンまたは新しいバージョンを実行する必要があります。

このリリースの場合：

- バージョン 6.2.3 の FMC は、バージョン 6.1.0 ～ 6.2.3 のデバイスを管理できます。
- バージョン 6.2.3 デバイスにはバージョン 6.2.3 FMC が必要です。

Firepower Device Manager

Firepower Device Manager（FDM）は、単一の FTD デバイスを管理できます。FDM では、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。FDM は FTD に組み込まれているため、このタイプの展開では、マネージャとデバイスの互換性という概念はありません。

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。

ASA、ASDM、および ASA FirePOWER のバージョンには広範な互換性がありますが、ASDM の新しいバージョンでは、古い ASA デバイス上の ASA FirePOWER モジュールを管理できない場合があります。詳細については、Cisco ASA の互換性を参照してください。

このリリースの場合：

- バージョン 7.9.2 ASDM は、バージョン 6.2.3 以前の ASA FirePOWER モジュールを管理できます。
- バージョン 6.2.3 ASA FirePOWER module には、バージョン 7.9.2 ASDM が必要です。

Web ブラウザの互換性

Firepower Web インターフェイスでテストされたブラウザ

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

- Google Chrome
- Mozilla Firefox
- Microsoft Internet Explorer 10 および 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 Firepower バージョンの広範なテストを実施していません。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 10 または 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（Internet Explorer 11 のみ）。
- Firepower Web インターフェイスの IP アドレス/URL の**互換表示**を有効にします。

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

セキュア通信

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

自己署名証明書の置き換えを開始する手順は、次のとおりです。

- FMC：**[システム（System）]**>**[設定（Configuration）]** を選択し、**[HTTPS 証明書（HTTPS Certificates）]** をクリックします。

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

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

（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 。

Firepower で監視されるネットワークからのブラウジング

多くのブラウザでは、デフォルトで Transport Layer Security（TLS）v1.3 が使用されています。暗号化されたトラフィックを処理するために SSL ポリシーを使用していて、モニタ対象ネットワーク内のユーザが TLS v1.3 を有効にしてブラウザを使用している場合、TLS v1.3 をサポートする Web サイトのロードに失敗します。回避策として、ClientHello ネゴシエーションから拡張機能 43（TLS 1.3）を削除するように管理対象デバイスを設定します。バージョン 6.2.3.7+ では、新しい CLI コマンドを使用して、ダウングレードするタイミングを指定できます。「新機能 （13 ページ）」を参照してください。

詳細については、『*Failures loading websites using TLS 1.3 with SSL inspection enabled*』というタイトルのソフトウェアアドバイザリを参照してください。

画面解像度の要件

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

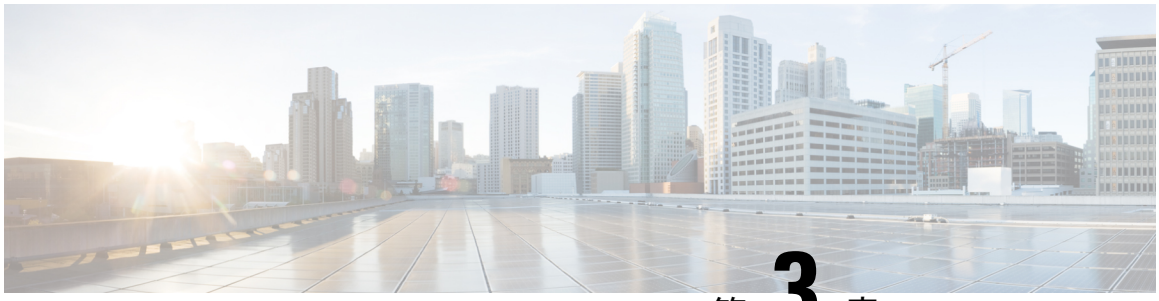
インターフェイス	解像度
Firepower Management Center	1280 X 720
Firepower Device Manager	1024 X 768
を管理している ASDM ASA FirePOWER module	1024 X 768
Firepower Chassis Manager 向け Firepower 9300 シャーシ	1024 X 768

その他の互換性関連のリソース

次の表に、リリースノートとその他の互換性情報へのリンクを示します。ドキュメントの完全なロードマップについては、ドキュメント ロードマップ （77 ページ）を参照してください。

表 *5:* その他の互換性関連のリソース

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



第 3 章

特長と機能

パッチには、新機能、機能、および緊急の問題または解決済みの問題に関連する動作の変更が含まれています。

新機能

次の表に、バージョン 6.2.3.x のパッチの新機能と動作の変更の概要を示します。

表 *6 :* バージョン *6.2.3.x* の新機能

機能	バージョン	説明
FTD NAT ポリシーでのルールの競合の検出	6.2.3.13	**アップグレードの影響。** バージョン 6.2.3.13 以降 にアップグレードすると、競合するルール（「重複」ルールまたは「オーバーラップ」ルールとも呼ばれます）を持つFTD NATポリシーを作成できなくなります。 これは、競合する NAT ルールが順序どおりに適用されていなかった問題を修正するものです。 現在競合しているNATルールがある場合は、アップグレード後に展開することができます。ただし、NAT ルールは引き続き順序どおりに適用されません。 そのため、アップグレード後にFTD NATポリシーを調べることをお勧めします。それには、ポリシーを編集して再保存を試みます（変更は必要ありません）。ルールが競合している場合は保存ができません。問題を修正して保存し、それから展開します。 （注） バージョン 6.3.0 または 6.4.0 にアップグレードすると、この修正が無効になります。この問題は、バージョン 6.3.0.4 および 6.4.0.2 では対処されています。 サポートされるプラットフォーム：FMC を搭載した FTD

機能	バージョン	説明
EMS 拡張機能のサポート	6.2.3.8	**アップグレードの影響。** [復号 - 再署名（Decrypt-Resign）] と [復号 - 既知のキー（Decrypt-Known Key）] の両方の SSL ポリシーアクションが、ClientHello ネゴシエーション時に EMS 拡張機能をサポートし、よりセキュアな通信が可能になりました。EMS 拡張機能は、 RFC 7627 によって定義されています。 バージョン 6.3.0 では EMS 拡張機能のサポートが中止されていることに注意してください。FMC 展開では、この機能は、デバイスのバージョンによって異なります。FMC をバージョン 6.3.0 にアップグレードしてもサポートは中止されませんが、デバイスをアップグレードすると中止されます。 サポートはバージョン 6.3.0.1 で再導入されています。 （注） バージョン 6.2.3.8 は 2019 年 1 月 7 日にシスコサポート & ダウンロードサイトから削除されました。バージョン 6.2.3.9 にアップグレードすると、EMS 拡張機能のサポートも有効になります。 サポートされるプラットフォーム：すべて
TLS v1.3 ダウングレード CLI コマンド	6.2.3.7	新しい CLI コマンドを使用すると、TLS v1.3 接続を TLS v1.2 にダウングレードするタイミングを指定できます。 多くのブラウザでは、デフォルトで TLS v1.3 が使用されています。暗号化されたトラフィックを処理するために SSL ポリシーを使用していて、モニタ対象ネットワーク内のユーザが TLS v1.3 を有効にしてブラウザを使用している場合、TLS v1.3 をサポートする Web サイトのロードに失敗します。 詳細については、『Cisco Threat Defense Command Reference』の「**system support ssl-client-hello-commands**」のセクションを参照してください。これらのコマンドは、Cisco TAC に問い合わせてから使用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
クラスタリングを使用したサイト間 VPN	6.2.3.3	クラスタリングを使用してサイト間 VPN を設定できるようになりました。サイトツーサイト VPN は、中央集中型機能です。マスターユニットだけが VPN 接続をサポートします。 サポートされるプラットフォーム：Firepower 4100/9300

廃止された機能

廃止された機能が原因で、アップグレードができなかったり、アップグレード前またはアップグレード後の設定変更を必要とする場合があります。

（注） バージョン 6.6.0/6.6.x 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。ユーザエージェント設定を使用して FMC をバージョン 6.7.0 以降 にアップグレードすることはできません。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 エージェントで使用できない機能も利用できるようになります。ライセンスを変換するには、販売担当者にお問い合わせください。

詳細については、『Firepower ユーザ ID：ユーザエージェントから Identity Services Engine への移行』の技術メモを参照してください。

これらの機能はバージョン 6.2.3.x で廃止されました。

表 *7:* バージョン *6.2.3.x* で廃止された機能

機能	アップグレードの影響	プラットフォーム	説明
バージョン 6.2.3.8 パッチを削除。	なし。ただしバージョン 6.2.3.8 のままにしないでください。	任意	バージョン 6.2.3.8 は 2019 年 1 月 7 日にシスコ サポートおよびダウンロードサイトから削除されました。このバージョンを実行している場合は、アップグレードすることを強くお勧めします。バージョン 6.2.3.8 を実行しているデバイスは、一定時間後にトラフィックの送受信を停止する可能性があります。 バージョン 6.2.3.8 を以降のパッチにアップグレードしてから、そのパッチをアンインストールすると、バージョン 6.2.3.8 に戻ります。その時点で、ただちにアップグレードするか、バージョン 6.2.3.8 をアンインストールする必要があります。バージョン 6.2.3.8 のままにしないでください。 関連するバグ：CSCvn82378

機能	アップグレードの影響	プラットフォーム	説明
バージョン 6.2.3.1 ～ 6.2.3.3 期限切れの動的分析用のCA証明書	なし。ただし、パッチを適用する必要があります。	ネットワーク向け AMP	2018 年 6 月 15 日、一部の Firepower 展開では、動的分析のためにファイルを送信できなくなりました。「期限切れの動的分析用のCA証明書 （17ページ）」を参照してください。

期限切れの動的分析用の CA 証明書

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

影響を受けるバージョン：バージョン 6.0+

解決：CSCvj07038

2018 年 6 月 15 日、一部の Firepower 展開では、動的分析のためにファイルを送信できなくなりました。これは、AMP Threat Grid クラウドとの通信に必要だった CA 証明書が期限切れになったために発生しました。バージョン6.3.0は、新しい証明書を使用する最初のメジャーバージョンです。

（注） バージョン6.3.0+にアップグレードしない場合は、新しい証明書を取得して動的分析を再度有効にするために、パッチまたはホットフィックスを適用する必要があります。ただし、その後、パッチまたはホットフィックスが適用された展開をバージョン6.2.0またはバージョン6.2.3にアップグレードすると、古い証明書に戻るため、パッチまたはホットフィックスを再度適用する必要があります。

パッチまたはホットフィックスを初めてインストールする場合は、ファイアウォールで、FMCとその管理対象デバイスの両方から `fmc.api.threatgrid.com`（`panacea.threatgrid.com` を置き換える）へのアウトバウンド接続が許可されていることを確認してください。管理対象デバイスは、動的分析のためにファイルをクラウドに送信します。FMC は結果を照会します。

次の表に、メジャー バージョン シーケンスとプラットフォームごとに、古い証明書を使用するバージョンと、新しい証明書を使用するパッチおよびホットフィックスを示します。パッチおよびホットフィックスは、シスコサポートおよびダウンロードサイトで入手できます。

表 *8*：新しい *CA* 証明書を使用するパッチとホットフィックス

古い証明書を使用するバージョン	新しい証明書を使用する最初のパッチ	新しい証明書を使用するホットフィックス	
6.2.3 ～ 6.2.3.3	6.2.3.4	ホットフィックス G	FTD デバイス
		ホットフィックス H	FMC、NGIPS デバイス
6.2.2 ～ 6.2.2.3	6.2.2.4	ホットフィックス BN	すべてのプラットフォーム
6.2.1	なし。アップグレードが必要です。	なし。アップグレードが必要です。	
6.2.0 ～ 6.2.0.5	6.2.0.6	ホットフィックス BX	FTD デバイス
		ホットフィックス BW	FMC、NGIPS デバイス
6.1.0 ～ 6.1.0.6	6.1.0.7	ホットフィックス EM	すべてのプラットフォーム
6.0.x	なし。アップグレードが必要です。	なし。アップグレードが必要です。	

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）すると、更新された新しい侵入ルールおよびプリプロセサルール、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 Firepower バージョンでサポートされていないキーワードが新しい侵入ルールで使用されている場合、SRU を更新しても、そのルールはインポートされません。

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

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

- FMC：[ヘルプ（Help）] > [About（バージョン情報）] を選択します。

- FDM を使用した FTD：**show summary** CLI コマンドを使用します。
- ASDM を使用した ASA FirePOWER：[ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [システム情報（System Information）] を選択します。

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

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

シスコとのデータの共有

一部の機能にシスコとのデータ共有が含まれます。

Cisco Success Network

バージョン 6.2.3 では、 *Cisco Success Network* は、テクニカルサポートを提供するために不可欠な使用状況に関する情報と統計情報をシスコに送信します。

初期設定およびアップグレード中に、参加を承諾するか、辞退するかを尋ねられます。また、いつでもオプトインまたはオプトアウトできます。

Web 分析トラッキング

バージョン 6.2.3 では、 *Web* 分析のトラッキングは、これに限定されませんが、ページでの操作、ブラウザのバージョン、製品のバージョン、ユーザの場所、FMC の管理 IP アドレスまたはホスト名を含む、個人を特定できない使用状況データをシスコに送信します。

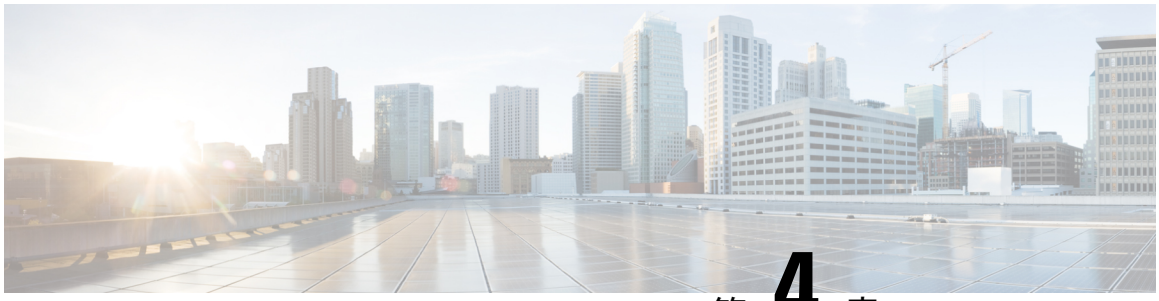
Web 分析トラッキングはデフォルトでオンになっています（バージョン 6.5.0 以降の EULA に承諾すると、Web分析トラッキングに同意したことになります）。ただし、初期設定の完了後にいつでもオプトアウトできます。

（注） バージョン 6.2.3 から 6.6.x へのアップグレードでは、Web 分析トラッキングを有効化（または再有効化）できます。これは、現在の設定がオプトアウトであっても発生する可能性があります。このデータの収集を拒否する場合は、アップグレードの後にオプトアウトしてください。

Cisco Support Diagnostics

バージョン 6.5.0 以降では、 *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、参加を承諾するか、辞退するかを尋ねられます。また、いつでもオプトインまたはオプトアウトできます。



第 4 章

Version6.2.3.x へのアップグレード

この章では、重要なリリースに固有の情報を提供します。

Firepowerソフトウェアのアップグレードガイドラインについて

便宜上、このリリースノートでは、過去の Firepower ソフトウェアリリースの廃止機能とバージョン固有のアップグレードガイドラインが重複しています。ただし、対象バージョンのリリースノート、およびスキップするその他のメジャーリリースまたはメンテナンスリリースのリリースノートを必ずお読みください。

重要 アップグレードガイドラインは複数の場所に表示できます。このチェックリストを使用して、すべてを確認してください。

表 *9 : Firepower* ソフトウェアのアップグレードガイドラインのインデックス

✓	リソース	詳細
	Version6.2.3.xパッチのガイドライン （22 ページ）	新規またはこのリリースに固有の重要なアップグレードガイドラインについては、これらを参照してください。

✓	リソース	詳細
	一般的なガイドライン （24 ページ）	ガイドラインが変更されている可能性があるため、アップグレードプロセスに精通している場合でも、これらをお読みください。
	既知の問題 （133 ページ）	パッチの既知の問題はリスト化されていませんが、Cisco バグ検索ツールを使用して、Firepower 製品の未解決のバグの最新リストを取得できます。
	特長と機能 （13 ページ）	パッチには、機能、および緊急の問題または解決済みの問題に関連する動作の変更のみが含まれていますが、この章を確認することをお勧めします。廃止された機能では、特別にアップグレード前の構成変更が必要になる場合があります。

Version6.2.3.xパッチのガイドライン

このチェックリストには、バージョン 6.2.3 パッチに関するアップグレードガイドラインが含まれています。

表 *10* : バージョン *6.2.3.x* 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
	CC モードが有効になっているバージョン 6.2.3.10 FTD にアップグレードすると FSIC 障害が発生 （23 ページ）	FTD	6.2.3 ～ 6.2.3.9	6.2.3.10 のみ
	バージョン 6.2.3.3 FTD デバイスをローカル管理に切り替えることは不可 （23 ページ）	FMC を使用した FTD	6.2.3 ～ 6.2.3.2	6.2.3.3
	アップグレードにより CSSM から FTD/FDM を登録解除することが可能 （23 ページ）	FDM を使用した FTD	6.2.3 ～ 6.2.3.1	6.2.3.2 ～ 6.2.3.5
	バージョン 6.2.3 ～ 88 FMC をアップグレードする前のホットフィックス （24 ページ）	FMC	6.2.3-88	6.2.3.1 ～ 6.2.3.3

CC モードが有効になっているバージョン 6.2.3.10 FTD にアップグレードすると FSIC 障害が発生

展開： Firepower Threat Defense

アップグレード元：バージョン 6.2.3 ～ 6.2.3.9

直接アップグレード先：バージョン 6.2.3.10 のみ

既知の問題：CSCvo39052

CC モードを有効にして FTD デバイスをバージョン6.2.3.10 にアップグレードすると、デバイスの再起動時に FSIC（ファイル システム整合性チェック）が失敗します。

⚠

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

FTD の展開にセキュリティ認定コンプライアンス（CC モード）が必要な場合は、バージョン 6.2.3.13 以降に直接アップグレードすることをお勧めします。Firepower 4100/9300 デバイスの場合は、FXOS 2.3.1.130+ にアップグレードすることも推奨します。

バージョン 6.2.3.3 FTD デバイスをローカル管理に切り替えることは不可

展開：FMC を使用した FTD

アップグレード元：バージョン 6.2.3 ～ 6.2.3.2

直接アップグレード先：バージョン 6.2.3.3 のみ

バージョン 6.2.3.3 では、Firepower Threat Defense デバイスの管理を FMC から FDM に切り替えることはできません。この問題は、バージョン6.2.3.3パッチをアンインストールしても発生します。この時点でローカル管理に切り替える場合は、バージョン 6.2.3 を新しくインストールするか、Cisco TAC にお問い合わせください。

この問題を回避するには、6.2.3.3 のバージョンにアップグレードする前に管理を切り替えます。または、最新パッチにアップグレードします。管理を切り替えると、デバイス構成は失われます。

バージョン 6.2.3.3 では、FDM から FMC への管理の切り替えが可能であることに注意してください。

アップグレードにより CSSM から FTD/FDM を登録解除することが可能

展開：FDM を使用した FTD

アップグレード元：バージョン 6.2.3 または 6.2.3.1

直接アップグレード先：6.2.3.2 ～ 6.2.3.5

Firepower Device Manager によって管理されている Firepower Threat Defense デバイスをアップグレードすると、そのデバイスが Cisco Smart Software Manager から登録解除される場合があります。アップグレードが完了したら、ライセンスのステータスを確認します。

ステップ 1 [デバイス（Device）] をクリックし、[スマートライセンス概要（Smart License summary）] の [設定の表示（View Configuration）] をクリックします。

ステップ 2 デバイスが登録されていない場合は、[デバイスの登録（Register Device）] をクリックします。

バージョン 6.2.3 ～ 88 FMC をアップグレードする前のホットフィックス

展開：FMC

アップグレード元：バージョン 6.2.3 ～ 88

直接アップグレード先：バージョン 6.2.3.1、バージョン 6.2.3.2、またはバージョン 6.2.3.3

シスコは、Firepower のアップグレードパッケージの更新版ビルドを適宜リリースしています。バージョン 6.2.3 ～ 88 は、それ以降のビルドに置き換えられています。バージョン 6.2.3 ～ 88 を実行している FMC をバージョン 6.2.3.1、バージョン 6.2.3.2、またはバージョン 6.2.3.3 にアップグレードすると、SSE クラウド接続が継続的にドロップし、エラーが生成されます。パッチをアンインストールしても、この問題は解決しません。

バージョン 6.2.3 ～ 88 を実行している場合は、アップグレードの前にホットフィックス T をインストールします。

一般的なガイドライン

これらの一般的なガイドラインは、すべてのアップグレードに適用されます。

アプライアンスの正常性と通信

アップグレードプロセスの間、展開環境内のアプライアンスが正常に通信していること、およびヘルスモニタによって報告された問題がないことを確認します。マイナーな問題がメジャーな問題になる前に解決します。

応答しないアップグレード

アップグレードしているアプライアンスとの間での変更の展開、またはアップグレードしているアプライアンスの手動での再起動やシャットダウンは行わないでください。進行中のアップグレードを再開しないでください。事前のチェック中に、アップグレードプロセスが停止して

いるように見える場合がありますが、これは想定内の動作です。アップグレードに失敗する、アプライアンスが応答しないなど、アップグレードで問題が発生した場合には Cisco TAC にお問い合わせください。

アップグレード前のチェックリスト

このチェックリストは、一般的なアップグレード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、該当するアップグレードガイド（「アップグレード手順 （50 ページ）」）を参照してください。

表 *11 : Firepower* ソフトウェアのアップグレード前チェックリスト

✓	アクション	詳細
	導入評価。	FirePOWER アプライアンスをアップグレードする前に、展開の現在の状態を判断します。状況を理解することにより、目的を達成する方法を決定します。 少なくとも次の項目に回答できる必要があります。 • どんなアプライアンスがありますか、またどの FirePOWER バージョンを実行していますか。どのバージョンを実行したいですか、またそのバージョンは実行可能ですか。直接アップグレードできますか。FMC 展開では、FMC デバイスの互換性を維持できますか。 • アプライアンスのいずれかで個別のオペレーティングシステムのアップグレードが必要ですか。ホスティング環境のアップグレードを必要とする仮想アプライアンスはありますか。 • ハイアベイラビリティ/スケーラビリティを実現するように設定されていますか。デバイスは、IPS として、ファイアウォールとして、パッシブに展開されていますか。

✓	アクション	詳細
	管理ネットワークの帯域幅を確認します。	Firepowerアプライアンスをアップグレードする（または準備状況チェックを実行する）には、アップグレードパッケージがアプライアンス上に存在する必要があります。Firepowerアップグレードパッケージには、さまざまなサイズがあります。管理ネットワークに大量のデータ転送を実行するための帯域幅があることを確認します。 FMCの展開では、アップグレードパケージをアップグレード時に管理対象デバイスに転送する場合は、帯域幅が不十分だとアップグレード時間が長くなったり、アップグレードがタイムアウトする原因となったりする可能性があります。アップグレードする前に、管理対象デバイスにFirepowerアップグレードパッケージを手動でプッシュ（コピー）することをお勧めします。 『Guidelines for Downloading Data from the Firepower Management Center to Managed Devices』（トラブルシューティングテクニカルノーツ）を参照してください。
	アプライアンスへのアクセスを確認します。	Firepowerデバイスは、（インターフェイス設定に応じて）アップグレード中、またはアップグレードが失敗した場合に、トラフィックを渡すことを停止できます。Firepowerデバイスをアップグレードする前に、ユーザの位置からのトラフィックがデバイスの管理インターフェイスにアクセスするためにデバイス自体を通過する必要がないことを確認してください。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。
	設定変更を計画します。	主要なアップグレードでは特に、アップグレードの前または後に、アップグレードにより重要な設定変更が発生することがあります。たとえば、廃止されたFlexConfigコマンドは、アップグレード後の展開の問題を引き起こす可能性があります。 「Firepowerソフトウェアのアップグレードガイドラインについて（21ページ）」のチェックリストを使用して、潜在的な問題を特定します。

✓	アクション	詳細
	バックアップを実行します。	アップグレードの前後に Firepower アプライアンスをバックアップします（サポートされている場合）。 • アップグレード前：アップグレードが致命的な失敗であった場合は、再イメージ化を実行し、復元する必要がある場合があります。再イメージ化によって、システムパスワードを含むほとんどの設定が工場出荷時の初期状態に戻ります。最近のバックアップがある場合は、通常の操作にすばやく戻ることができます。 • アップグレード後：これにより、新しくアップグレードされた展開のスナップショットが作成されます。新しいFMCバックアップファイルがデバイスがアップグレードされたことを「認識」するように、管理対象デバイスをアップグレードした後に FMC をバックアップすることをお勧めします。 **注意** Firepower アプライアンスを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。アプライアンスに残っているバックアップは、手動またはアップグレードプロセスによって削除できます（アップグレードプロセスでは、ローカルに保存されたバックアップが消去される）。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。誤りを避けるには、注意深い計画と準備が役立ちます。バックアップと復元の要件、ガイドライン、制限事項、およびベストプラクティスの詳細については、ご使用の Firepower 製品のコンフィギュレーション ガイドを参照してください。
	準備状況チェックを実行します。	FMC展開では、準備状況チェックをお勧めします。このチェックにより、Firepowerをアップグレードするためのアプライアンスの準備状況を評価できます。このチェックにより、データベース整合性、バージョン不一致、デバイス登録などの問題を識別できます。

✓	アクション	詳細
	アップグレードをスケジュール設定します。1007	アップグレードのスケジュール設定は、中断による展開環境への影響が最も小さい時間に行うことを推奨します。 メンテナンスウィンドウをスケジュールするときは、トラフィックフローおよびインスペクションへの影響と、アップグレードにかかる可能性がある時間を考慮します。また、ウィンドウで実行する必要があるタスクと、事前に実行できるタスクを検討します。慎重な計画と準備で中断を最小限に抑えます。メンテナンスウィンドウがアップグレードパッケージの取得およびプッシュ、準備状況チェックの実行、バックアップの作成などを行うまで待機しないようにします。
	NTP 同期を確認します。	時刻の提供に使用している NTP サーバと Firepower アプライアンスが同期していることを確認します。同期されていないと、アップグレードが失敗する可能性があります。FMC 展開では、時刻のずれが 10 秒を超えている場合、[時刻同期化ステータス（Time Synchronization Status）] ヘルスモジュールからアラートが発行されますが、手動で確認する必要もあります。 時刻を確認するには、次の手順を実行します。 • FMC：[システム（System）] > [設定（Configuration）] > [時刻（Time）] を選択します。 • デバイス：**show time** CLI コマンドを使用します。
	ASA FirePOWER デバイスで ASA REST API を無効化します。	ASA FirePOWER モジュールをアップグレードする前に、ASA REST API を無効にしていることを確認します。無効にしていない場合、アップグレードが失敗することがあります。ASA CLI から：`no rest api agent`。アンインストール後に再度有効にすることができます：`rest-api agent`。 ASA FirePOWER モジュール（6.0+）も実行している場合、ASA 5506-X シリーズ デバイスは ASA REST API をサポートしないことに注意してください。
	設定を展開します。	アップグレードする前に古いデバイスに設定を展開すると、失敗する可能性が減少します。 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、いくつかの設定を展開することで Snort が再起動されます。これにより、トラフィックのインスペクションが中断し、デバイスのトラフィックの処理方法によっては、再起動が完了するまでトラフィックが中断する場合があります。詳細については、トラフィック フロー、検査、およびデバイス動作 （41 ページ） を参照してください。

✓	アクション	詳細
	実行中のタスクを確認します。	アップグレードする前に、重要なタスクが完了していることを確認します。アップグレードの開始時に実行中のタスクは停止し、失敗したタスクとなり、再開できません。 また、アップグレード中に実行するようにスケジュールされたタスクを確認し、それらをキャンセルまたは延期することをお勧めします。
	ディスク容量を確認します。	最終的なディスク容量のチェックを実行します。空きディスク容量が十分でない場合、アップグレードは失敗します。詳細については、時間テストとディスク容量の要件 （29 ページ）を参照してください。

アップグレードする最小バージョン

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

したがって、バージョン 6.2.3.x にアップグレードするには、バージョン 6.2.3 以降を実行している必要があります。

（注） FTD を使用する Firepower 4100/9300 シャーシの場合、Firepower 6.2.3.16 以上には FXOS 2.3.1.157 以降のビルドが必要です。最初に FXOS をアップグレードします。

時間テストとディスク容量の要件

Firepower アプライアンスをアップグレードするには、十分な空きディスク容量が必要です。これがない場合、アップグレードは失敗します。Firepower Management Center を使用して管理対象デバイスをアップグレードする場合、デバイスアップグレードパッケージに対して、FMC は /Volume パーティションに追加のディスク容量を必要とします。また、アップグレードを実行するための十分な時間を確保してください。

参考のために、社内の時間とディスク容量のテストに関するレポートを提供しています。

時間テストについて

ここで指定した時間の値は、社内のテストに基づいています。

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

テスト条件

- 展開：値は、Firepower Management Center 展開のテストから取得されています。これは、同様の条件の場合、リモートとローカルで管理されているデバイスの raw アップグレード時間が類似しているためです。
- バージョン：メジャー アップグレードの場合、以前のすべての対象メジャー バージョンからのアップグレードをテストします。パッチについては、ベースバージョンからアップグレードをテストします。
- モデル：ほとんどの場合、各シリーズの最もローエンドのモデルでテストし、場合によってはシリーズの複数のモデルでテストします。
- 仮想設定：メモリおよびリソースのデフォルト設定を使用してテストします。
- ハイアベイラビリティと拡張性：スタンドアロンデバイスでテストします。

  ハイアベイラビリティの構成またはクラスタ化された構成では、動作の継続性を保持するため、複数のデバイスは1つずつアップグレードされます。アップグレード中は、各デバイスはメンテナンス モードで動作します。そのため、デバイス ペアまたはクラスタ全体のアップグレードには、スタンドアロンデバイスのアップグレードよりも長い時間がかかります。
- 構成：構成とトラフィック負荷が最小限のアプライアンスでテストします。

  アップグレード時間は、構成の複雑さ、イベントデータベースのサイズ、また、それらがアップグレードから影響を受けるかどうか、受ける場合はどのような影響を受けるかにより、長くなる場合があります。たとえば多くのアクセス制御ルールを使用している場合、アップグレードはこれらのルールの格納方法をバックエンドで変更する必要があるため、アップグレードにはさらに長い時間がかかります。

時間はアップグレードのみを対象

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

- 管理対象デバイスへのアップグレードパッケージの転送（アップグレード前かアップグレード中かにかかわらない）。
- 準備状況チェック。
- VDB と SRU の更新。
- 設定の展開。

- リブート（値が別途に報告される場合がある）。

ディスク容量の要件について

容量の見積もりは、すべてのアップグレードについて報告された最大のものです。

バージョン 6.2.3.16 の時間とディスク容量

表 *12 :* バージョン *6.2.3.16* の時間とディスク容量

Platform	ボリュームの容量	必要容量	FMC の容量	6.2.3 からのアップグレード時間	リブート時間
FMC	3.6 GB	250 MB	—	40 分	9 分
FMCv：VMware 6.0	3.3 GB	220 MB	—	25 分	4 分
Firepower 2100 シリーズ	2.6 GB	2.6 GB	620 MB	11 分	12 分
Firepower 4100 シリーズ	1.7 GB	1.7 GB	410 MB	5 分	5 分
Firepower 9300	1.8 GB	1.8 GB	410 MB	5 分	9 分
ASA 5500-X シリーズ with FTD	2 GB	200 MB	430 MB	18 分	33 分
FTDv：VMware 6.0	2 GB	190 MB	430 MB	8 分	5 分
Firepower 7000/8000 シリーズ	3.5 GB	200 MB	670 MB	31 分	14 分
ASA FirePOWER	3.8 GB	58 MB	600 MB	74 分	77 分
NGIPSv：VMware 6.0	2.3 GB	180 MB	500 MB	6 分	4 分

バージョン 6.2.3.15 の時間とディスク容量

表 *13 :* バージョン *6.2.3.15* の時間とディスク容量

Platform	ボリュームの容量	必要容量	FMC の容量	6.2.3 からの時間
FMC	4.7 GB	260 MB	—	50 分
FMCv：VMware 6.0	4.7 GB	210 MB	—	ハードウェアによって異なる

Platform	ボリュームの容量	必要容量	FMC の容量	6.2.3 からの時間
Firepower 2100 シリーズ	2.3 GB	2.3 GB	590 MB	27 分
Firepower 4100 シリーズ	1.7 GB	1.7 GB	390 MB	10 分
Firepower 9300	2.4 GB	2.4 GB	390 MB	11 分
ASA 5500-X シリーズ with FTD	2 GB	190 MB	410 MB	38 分
FTDv：VMware 6.0	2.4 GB	190 MB	410 MB	ハードウェアによって異なる
Firepower 7000/8000 シリーズ	3.5 GB	210 MB	640 MB	19 分
ASA FirePOWER	3.9 GB	56 MB	580 MB	100 分
NGIPSv：VMware 6.0	2.7 GB	180 MB	470 MB	ハードウェアによって異なる

バージョン 6.2.3.14 の時間とディスク容量

表 *14 :* バージョン *6.2.3.14* の時間とディスク容量

Platform	ボリュームの容量	必要容量	FMC の容量	6.2.3 からの時間
FMC	4.5 GB	260 MB	—	58 分
FMCv：VMware 6.0	4.7 GB	190 MB	—	ハードウェアによって異なる
Firepower 2100 シリーズ	1.9 GB	1.9 GB	590 MB	23 分
Firepower 4100 シリーズ	1.7 GB	1.7 GB	390 MB	11 分
Firepower 9300	1.7 GB	1.7 GB	390 MB	10 分
ASA 5500-X シリーズ with FTD	2 GB	200 MB	410 MB	32 分
FTDv：VMware 6.0	2.4 GB	190 MB	410 MB	ハードウェアによって異なる
Firepower 7000/8000 シリーズ	3.4GB	200 MB	630 MB	19 分
ASA FirePOWER	3.7 GB	53 MB	560 MB	106 分

Platform	ボリュームの容量	必要容量	FMC の容量	6.2.3 からの時間
NGIPSv：VMware 6.0	2.6 GB	190 MB	470 MB	ハードウェアによって異なる

バージョン 6.2.3.13 の時間とディスク容量

表 *15 :* バージョン *6.2.3.13* の時間とディスク容量

Platform	ボリュームの容量	必要容量	FMC の容量	6.2.3 からの時間
FMC	4.7 GB	290 MB	—	50 分
FMCv：VMware 6.0	4.6 GB	190 MB	—	ハードウェアによって異なる
Firepower 2100 シリーズ	2.6 GB	2.6 GB	590 MB	25 分
Firepower 4100 シリーズ	1.7 GB	1.7 GB	390 MB	11 分
Firepower 9300	1.8 GB	1.8 GB	390 MB	11 分
ASA 5500-X シリーズ with FTD	2.4 GB	190 MB	410 MB	32 分
FTDv：VMware 6.0	2.3 GB	190 MB	410 MB	ハードウェアによって異なる
Firepower 7000/8000 シリーズ	3.8 GB	190 MB	620 MB	18 分
ASA FirePOWER	3.7 GB	51 MB	560 MB	105 分
NGIPSv：VMware 6.0	2.6 GB	180 MB	470 MB	ハードウェアによって異なる

バージョン 6.2.3.12 の時間とディスク容量

表 *16 :* バージョン *6.2.3.12* の時間とディスク容量

Platform	ボリュームの容量	必要容量	FMC の容量	6.2.3 からの時間
FMC	3.9 GB	220 MB	—	49 分
FMCv：VMware 6.0	4.6 GB	160 MB	—	ハードウェアによって異なる

Platform	ボリュームの容量	必要容量	FMC の容量	6.2.3 からの時間
Firepower 2100 シリーズ	1.9 GB	1.9 GB	390 MB	21 分
Firepower 4100 シリーズ	970 MB	970 MB	190 MB	14 分
Firepower 9300	1.7 GB	1.7 GB	190 MB	11 分
ASA 5500-X シリーズ with FTD	1.4 GB	96 MB	210 MB	30 分
FTDv：VMware 6.0	2.4 GB	200 MB	210 MB	ハードウェアによって異なる
Firepower 7000/8000 シリーズ	3.6 GB	160 MB	540 MB	19 分
ASA FirePOWER	3.5 GB	31 MB	480 MB	104 分
NGIPSv：VMware 6.0	2.6 GB	130 MB	400 MB	ハードウェアによって異なる

バージョン 6.2.3.11 の時間とディスク容量

表 *17* : バージョン *6.2.3.11* の時間とディスク容量

Platform	ボリュームの容量	必要容量	FMC の容量	6.2.3 からの時間
FMC	4.5 GB	250 MB	—	39 分
FMCv：VMware 6.0	4.6 GB	35 MB	—	ハードウェアによって異なる
Firepower 2100 シリーズ	2.8 GB	2.8 GB	590 MB	40 分
Firepower 4100 シリーズ	2 GB	2 GB	380 MB	10 分
Firepower 9300	1.6 GB	1.6 GB	380 MB	11 分
ASA 5500-X シリーズ with FTD	1.8 GB	230 MB	410 MB	33 分
FTDv：VMware 6.0	2.2 GB	230 MB	410 MB	ハードウェアによって異なる
Firepower 7000/8000 シリーズ	3.3 GB	170 MB	600 MB	23 分
ASA FirePOWER	3.6 GB	50 MB	530 MB	110 分

Platform	ボリュームの容量	必要容量	FMC の容量	6.2.3 からの時間
NGIPSv：VMware 6.0	2.6 GB	130 MB	450 MB	ハードウェアによって異なる

バージョン 6.2.3.10 の時間とディスク容量

表 *18 :* バージョン *6.2.3.10* の時間とディスク容量

Platform	ボリュームの容量	必要容量	FMC の容量	6.2.3 からの時間
FMC	4.2 GB	200 MB	—	40 分
FMCv	4.5 GB	230 MB	—	ハードウェアによって異なる
Firepower 2100 シリーズ	1.8 GB	1.8 GB	390 MB	21 分
Firepower 4100/9300 シャーシ	1.3 GB	1.3 GB	190 MB	11 分
ASA 5500-X シリーズ with FTD	1.3 GB	140 MB	210 MB	25 分
FTDv	1.6 GB	140 MB	210 MB	ハードウェアによって異なる
Firepower 7000/8000 シリーズ	3.2 GB	190 MB	560 MB	25 分
ASA FirePOWER	3.4GB	31 MB	480 MB	100 分
NGIPSv	2.1 GB	160 MB	400 MB	ハードウェアによって異なる

バージョン 6.2.3.9 の時間とディスク容量

表 *19 :* バージョン *6.2.3.9* の時間とディスク容量

Platform	ボリュームの容量	必要容量	FMC の容量	6.2.3 からの時間
FMC	3630 MB	190 MB	—	35 分
FMCv	3596 MB	172 MB	—	ハードウェアによって異なる

Platform	ボリュームの容量	必要容量	FMC の容量	6.2.3 からの時間
Firepower 2100 シリーズ	1677 MB	1677 MB	385 MB	21 分
Firepower 4100/9300 シャーシ	779 MB	779 MB	184 MB	9 分
ASA 5500-X シリーズ with FTD	1105 MB	130 MB	206 MB	12 分
ISA 3000 with FTD	1071 MB	130 MB	206 MB	25 分
FTDv	1094 MB	130 MB	206 MB	ハードウェアによって異なる
Firepower 7000/8000 シリーズ	2975 MB	161 MB	538 MB	30 分
ASA FirePOWER	3211 MB	27 MB	462 MB	38 分
NGIPSv	1883 MB	146 MB	378 MB	ハードウェアによって異なる

バージョン 6.2.3.8 の時間とディスク容量

バージョン 6.2.3.8 は 2019 年 1 月 7 日にシスコサポートおよびダウンロードサイトから削除されました。このバージョンを実行している場合は、アップグレードすることをお勧めします。

バージョン 6.2.3.7 の時間とディスク容量

表 *20 :* バージョン *6.2.3.7* の時間とディスク容量

Platform	ボリュームの容量	必要容量	FMC の容量	6.2.3 からの時間
FMC	2909 MB	137 MB	—	25 分
FMCv	3972 MB	211 MB	—	ハードウェアによって異なる
Firepower 2100 シリーズ	1668 MB	1668 MB	384 MB	19 分
Firepower 4100/9300 シャーシ	795 MB	795 MB	183 MB	8 分
ASA 5500-X シリーズ with FTD	1067 MB	130 MB	205 MB	9 分
ISA 3000 with FTD	1080 MB	130 MB	205 MB	20 分

Platform	ボリュームの容量	必要容量	FMC の容量	6.2.3 からの時間
FTDv	1146 MB	130 MB	205 MB	ハードウェアによって異なる
Firepower 7000/8000 シリーズ	3300 MB	136 MB	477 MB	20 分
ASA FirePOWER	2291 MB	26 MB	411 MB	80 分
NGIPSv	1588 MB	121 MB	327 MB	ハードウェアによって異なる

バージョン 6.2.3.6 の時間とディスク容量

表 *21 :* バージョン *6.2.3.6* の時間とディスク容量

Platform	ボリュームの容量	必要容量	FMC の容量	6.2.3 からの時間
FMC	2524 MB	47 MB	—	30 分
FMCv	2315 MB	101 MB	—	ハードウェアによって異なる
Firepower 2100 シリーズ	1673 MB	1673 MB	383 MB	10 分
Firepower 4100/9300 シャーシ	790 MB	790 MB	182 MB	17 分
ASA 5500-X シリーズ with FTD	1220 MB	130 MB	205 MB	21 分
ISA 3000 with FTD	1087 MB	130 MB	205 MB	21 分
FTDv	1133 MB	130 MB	205 MB	ハードウェアによって異なる
Firepower 7000/8000 シリーズ	1196 MB	17 MB	204 MB	30 分
ASA FirePOWER	1844 MB	16 MB	226 MB	106 分
NGIPSv	364 MB	17 MB	142 MB	ハードウェアによって異なる

バージョン 6.2.3.5 の時間とディスク容量

表 *22 :* バージョン *6.2.3.5* の時間とディスク容量

Platform	ボリュームの容量	必要容量	FMC の容量	6.2.3 からの時間
FMC	1566 MB	24 MB	—	28 分
FMCv	2266 MB	80 MB	—	ハードウェアによって異なる
Firepower 2100 シリーズ	1001 MB	1001 MB	257 MB	20 分
Firepower 4100/9300 シャーシ	370 MB	370 MB	56 MB	7 分
ASA 5500-X シリーズ with FTD	587 MB	130 MB	78 MB	20 分
ISA 3000 with FTD	379 MB	130 MB	78 MB	20 分
Firepower 7000/8000 シリーズ	806 MB	17 MB	78 MB	22 分
ASA FirePOWER	1465 MB	15 MB	100 MB	70 分
NGIPSv	120 MB	17 MB	16 MB	ハードウェアによって異なる

バージョン 6.2.3.4 の時間とディスク容量

表 *23 :* バージョン *6.2.3.4* の時間とディスク容量

Platform	ボリュームの容量	必要容量	FMC の容量	6.2.3 からの時間
FMC	2191 MB	107 MB	—	80 分
FMCv	1760 MB	35 MB	—	ハードウェアによって異なる
Firepower 2100 シリーズ	1014 MB	1014 MB	261 MB	17 分
Firepower 4100/9300 シャーシ	334 MB	334 MB	59 MB	7 分
ASA 5500-X シリーズ with FTD	411 MB	128 MB	82 MB	20 分

Platform	ボリュームの容量	必要容量	FMC の容量	6.2.3 からの時間
ISA 3000 with FTD	393 MB	128 MB	82 MB	20 分
FTDv	411 MB	128 MB	82 MB	ハードウェアによって異なる
Firepower 7000/8000 シリーズ	800 MB	17 MB	82 MB	23 分
ASA FirePOWER	1385 MB	15 MB	103 MB	25 分
NGIPSv	191 MB	17 MB	20 MB	ハードウェアによって異なる

バージョン 6.2.3.3 の時間とディスク容量

表 *24 :* バージョン *6.2.3.3* の時間とディスク容量

Platform	ボリュームの容量	必要容量	FMC の容量	6.2.3 からの時間
FMC	1879 MB	88 MB	—	26 分
FMCv	2093 MB	90 MB	—	ハードウェアによって異なる
Firepower 2100 シリーズ	987 MB	987 MB	255 MB	15 分
Firepower 4100/9300 シャーシ	313 MB	313 MB	54 MB	5 分
ASA 5500-X シリーズ with FTD	553 MB	128 MB	77 MB	16 分
ISA 3000 with FTD	307 MB	90 MB	77 MB	15 分
FTDv	307 MB	90 MB	77 MB	ハードウェアによって異なる
Firepower 7000/8000 シリーズ	825 MB	17 MB	77 MB	15 分
ASA FirePOWER	634 MB	16 MB	98 MB	40 分
NGIPSv	102 MB	17 MB	77 MB	ハードウェアによって異なる

バージョン 6.2.3.2 の時間とディスク容量

表 *25 :* バージョン *6.2.3.2* の時間とディスク容量

Platform	ボリュームの容量	必要容量	FMC の容量	6.2.3 からの時間
FMC	1743 MB	27 MB	—	24 分
FMCv	1976 MB	70 MB	—	ハードウェアによって異なる
Firepower 2100 シリーズ	977 MB	977 MB	252 MB	17 分
Firepower 4100/9300 シャーシ	374 MB	374 MB	51 MB	4 分
ASA 5500-X シリーズ with FTD	585 MB	126 MB	73 MB	16 分
ISA 3000 with FTD	676 MB	126 MB	73 MB	17 分
FTDv	585 MB	126 MB	73 MB	ハードウェアによって異なる
Firepower 7000/8000 シリーズ	688 MB	11 MB	76 MB	13 分
ASA FirePOWER	1440 MB	15 MB	98 MB	40 分
NGIPSv	96 MB	17 MB	14 MB	ハードウェアによって異なる

バージョン 6.2.3.1 の時間とディスク容量

表 *26 :* バージョン *6.2.3.1* の時間とディスク容量

Platform	ボリュームの容量	必要容量	FMC の容量	6.2.3 からの時間
FMC	1361.8 MB	59.67 MB	—	25 分
FMCv	1240.8 MB	40.8 MB	—	ハードウェアによって異なる
Firepower 2100 シリーズ	948.3 MB	948.3 MB	246 MB	81 分
Firepower 4100/9300 シャーシ	278 MB	278 MB	45 MB	8 分

Platform	ボリュームの容量	必要容量	FMC の容量	6.2.3 からの時間
ASA 5500-X シリーズ with FTD	275.5 MB	89.9 MB	68 MB	16 分
ISA 3000 with FTD	343.4 MB	127.5 MB	68 MB	15 分
FTDv	275.5 MB	89.9 MB	67 MB	ハードウェアによって異なる
Firepower 7000/8000 シリーズ	99.8 MB	36 MB	10 MB	19 分
ASA FirePOWER	867.9 MB	15.45 MB	32 MB	60 分
NGIPSv	101.9 MB	17.18 MB	9 MB	ハードウェアによって異なる

トラフィック フロー、検査、およびデバイス動作

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

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

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

FTD アップグレード時の動作： Firepower 9300 シャーシ

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

Firepower 9300 シャーシ：FXOS のアップグレード

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

表 *27 : FXOS* アップグレード中のトラフィックの動作

導入	方法	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 FTD デバイス：Firepower ソフトウェアのアップグレード

アップグレード中、Firepower デバイス/セキュリティモジュールはメンテナンスモードで稼働します。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 *28 : Firepower* ソフトウェアアップグレード中のトラフィックの動作：スタンドアロン *FTD* デバイス

インターフェイス 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。

ハイアベイラビリティペア：FirePOWER ソフトウェアアップグレード

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

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

クラスタ：FirePOWER ソフトウェア アップグレード

Firepower Threat Defense クラスタのデバイスで FirePOWER ソフトウェアをアップグレードする間に、トラフィック フローまたはインスペクションが中断されることはありません。継続稼働できるように、一度に 1 つずつアップグレードされます。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。アップグレード中、セキュリティモジュールはメンテナンスモードで稼働します。

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。

（注） バージョン 6.2.0、6.2.0.1、または 6.2.0.2 からシャーシ間クラスタをアップグレードすると、各モジュールがクラスタから削除されるときに、トラフィック インスペクションで 2 ～ 3 秒のトラフィック中断が発生します。

ハイアベイラビリティとクラスタリング ヒットレス アップグレードの要件

ヒットレスアップグレードの実行には、次の追加要件があります。

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

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

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

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

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

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

展開時のトラフィックの動作

アップグレード プロセス中には、設定を複数回展開します。Snort は、通常、アップグレード直後の最初の展開時に再起動されます。展開の前に、特定のポリシーまたはデバイス設定を変更しない限り、それ以外の展開時に再起動されることはありません。詳細については、『Firepower Management Center 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 Firepower デバイスでトラフィック インスペクションが中断されます。インターフェイス設定により、中断中にインスペクションせずにトラフィックをドロップするか受け渡すかが決定されます。

表 *29 : FTD* 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
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。

FTD アップグレード時の動作：その他のデバイス

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

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

アップグレード中、Firepower 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 *30 : Firepower* ソフトウェアアップグレード中のトラフィックの動作：スタンドアロン *FTD* デバイス

インターフェイス 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。

ハイアベイラビリティペア：FirePOWER ソフトウェアアップグレード

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

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

展開時のトラフィックの動作

アップグレード プロセス中には、設定を複数回展開します。Snort は、通常、アップグレード直後の最初の展開時に再起動されます。展開の前に、特定のポリシーまたはデバイス設定を変更しない限り、それ以外の展開時に再起動されることはありません。詳細については、『Firepower Management Center 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Firepowerデバイスでトラフィック インスペクションが中断されます。インターフェイス設定により、中断中にインスペクションせずにトラフィックをドロップするか受け渡すかが決定されます。

表 *31 : FTD* 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
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 *32 : 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

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 クローズ（**sfr fail-close**）	ドロップされる
モニタのみ（**sfr {fail-close}|{fail-open} monitor-only**）	パケットをただちに出力、コピーへのインスペクションなし

ASA FirePOWER 展開時のトラフィックの動作

Snort プロセス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 *33 : NGIPSv* アップグレード中のトラフィックの動作

インターフェイス コンフィギュレーション	トラフィックの動作
インライン	切断
インライン、タップ モード	パケットをただちに出力、コピーへのインスペクションなし
パッシブ	中断なし、インスペクションなし

展開時のトラフィックの動作

アップグレード プロセス中には、設定を複数回展開します。Snort は、通常、アップグレード直後の最初の展開時に再起動されます。展開の前に、特定のポリシーまたはデバイス設定を変更しない限り、それ以外の展開時に再起動されることはありません。詳細については、

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

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

表 *34 : 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

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 *35 : Firepower* アップグレード手順

タスク	ガイド
FMC 展開のアップグレード。	Cisco Firepower Management Center Upgrade Guide
FDM を使用した Firepower Threat Defense ソフトウェアのアップグレード。	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 FTD バージョンのガイドの「システム管理」の章を参照してください。
Firepower 4100/9300 シャーシの FXOS のアップグレード。	Cisco Firepower 4100/9300 Upgrade Guide
ASDM を使用した ASA FirePOWER モジュールのアップグレード。	Cisco ASA Upgrade Guide

タスク	ガイド
ISA 3000、ASA 5506-X、5508-X、および 5516-X での ROMMON イメージのアップグレード。	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。

アップグレードパッケージ

アップグレード パッケージは、 シスコサポートおよびダウンロードサイトで入手できます。

- FMCv を含む Firepower Management Center：https://www.cisco.com/go/firepower-software
- Firepower Threat Defense（ISA 3000）： https://www.cisco.com/go/isa3000-software
- Firepower Threat Defense（FTDv を含む他のすべてのモデル）：https://www.cisco.com/go/ftd-software
- ASA with FirePOWER Services（ASA 5500-X シリーズ）： https://www.cisco.com/go/asa-firepower-sw
- NGIPSv： https://www.cisco.com/go/ngipsv-software

Firepower ソフトウェア アップグレード パッケージを検索するには、Firepower アプライアンス モデルを選択または検索し、現在のバージョンの Firepower ソフトウェアのダウンロード ページを参照します。使用可能なアップグレード パッケージは、インストール パッケージ、ホットフィックス、およびその他の該当するダウンロードとともに表示されます。

ヒント インターネットにアクセスできる FMC は、手動でダウンロードできるようになってから約 2 週間後に、シスコからバージョン 6.2.3.x ～ 6.5.0.x Firepower パッチを直接ダウンロードできます。次の場合、シスコからの直接ダウンロードはサポートされていません。

- メジャーリリース。
- バージョン 6.6 以降へのほとんどのパッチ。
- FDM または ASDM 展開。

ファミリまたはシリーズのすべての Firepower モデルに同じアップグレード パッケージを使用します。アップグレード パッケージのファイル名には、プラットフォーム、パッケージ タイプ（アップグレード、パッチ、ホットフィックス）、および Firepower のバージョンが反映されています。

次に例を示します。

- パッケージ：`Cisco_Firepower_Mgmt_Center_Patch-6.6.0.1-7.sh.REL.tar`

- プラットフォーム： Firepower Management Center
- パッケージタイプ：パッチ
- バージョンおよびビルド：6.6.0.1 ～ 7
- ファイル拡張子：sh.REL.tar

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

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

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

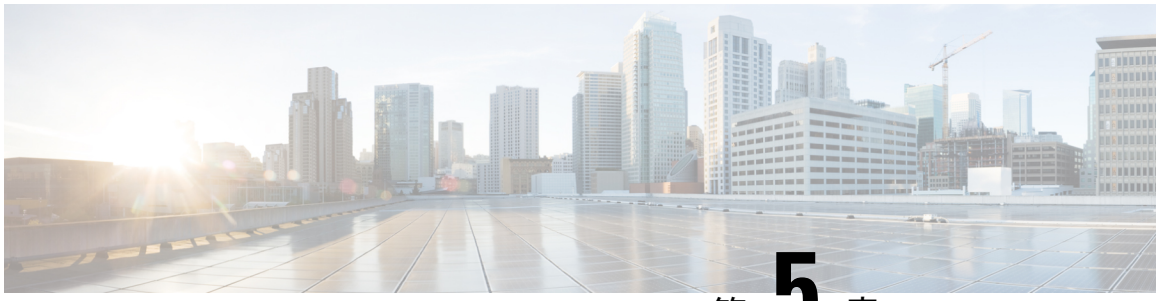
表 *36 : Firepower* ソフトウェア アップグレード パッケージ

プラットフォーム	パッケージ
FMC/FMCv	Sourcefire_3D_Defense_Center_S3
Firepower 2100 シリーズ	Cisco_FTD_SSP-FP2K
Firepower 4100/9300 シャーシ	Cisco_FTD_SSP
FTD を搭載した ASA 5500-X シリーズ FTD を搭載した ISA 3000 FTDv	Cisco_FTD
ASA FirePOWER	Cisco_Network_Sensor
NGIPSv	Sourcefire_3D_Device_VMware

オペレーティングシステムのアップグレードパッケージ

オペレーティングシステムのアップグレードパッケージの詳細については、次のガイドの「アップグレードの計画」の章を参照してください。

- Cisco ASA Upgrade Guide（ASA OS の場合）
- Cisco Firepower 4100/9300 Upgrade Guide（FXOSの場合）



第 5 章

更新プログラムのアンインストール

Firepower のパッチは次の場所からアンインストールできます。

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

パッチをアンインストールすると、アップグレード前のバージョンがアプライアンスで実行されます。

（注） FDM によって管理されている FTD デバイスからは、パッチのアンインストールやはできません。また、任意のアプライアンスから Firepower ソフトウェアのメジャー バージョンをアンインストールすることもできません。このような場合は、イメージを再作成する必要があります。

詳細については、以下を参照してください。

- アンインストールに関する注意事項と制約事項 （53 ページ）
- HA/スケーラビリティ環境でのアンインストール順序 （56 ページ）
- アンインストールの手順 （59 ページ）
- パッケージのアンインストール （65 ページ）

アンインストールに関する注意事項と制約事項

これらの重要なガイドラインと制限事項は、アンインストールに適用されます。

アンインストールがサポートされる状況は限られています。

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

- アンインストール後に設定変更を展開できない
- オペレーティングシステムと Firepower ソフトウェアの間に互換性がなくなる

- セキュリティ認定コンプライアンスが有効な状態（CC/UCAPL モード）でそのパッチが適用されていた場合、アプライアンスの再起動時に FSIC（ファイル システム整合性チェック）が失敗する

⚠

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

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

次の表に、アンインストールしてはならない状況を示します。

表 *37* : アンインストール時に後続の問題が発生したバージョン *6.2.3.x* のパッチ

プラットフォーム	アンインストール元	アップグレード元が次の場合
FMC/FMCv Firepower 7000/8000 シリーズ ASA FirePOWER NGIPSv	6.2.3.7 以降	6.2.3 ～ 6.2.3.6
FMC/FMCv Firepower 7000/8000 シリーズ ASA FirePOWER NGIPSv	6.2.3.11 以降	6.2.3 ～ 6.2.3.10
任意（Any）	6.2.3.15+	6.2.3 ～ 6.2.3.14

シェルを使用して先にデバイスからアンインストールする

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

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

- クラスタ化された、スタック構成の、またはハイ アベイラビリティ（HA）の Firepower デバイスから、あるいは FirePOWER Services デバイスのあるクラスタ化 ASA またはフェールオーバー ASA から、パッチを一括でアンインストールすることはできません。中断を最小限に抑えるアンインストール順序を計画するには、「HA/スケーラビリティ環境でのアンインストール順序 （56 ページ）」を参照してください。

- FMC、ASDM、または FDM を使用してデバイスからパッチをアンインストールすることも、7000/8000 シリーズデバイスのローカル Web インターフェイスを使用することもできません。
- FMC のユーザ アカウントを使用して、いずれかの管理対象デバイスにログインしてデバイスからパッチをアンインストールすることはできません。Firepower アプライアンスでは独自のユーザ アカウントを維持しています。
- デバイスの `admin` ユーザとして、または CLI 設定アクセス権を持つ別のローカル ユーザとして、デバイス シェルにアクセスできる必要があります。シェル アクセスを無効にした場合、デバイスパッチをアンインストールすることはできません。デバイスのロックダウンを元に戻すには、Cisco TAC にご連絡ください。

デバイスより後に FMC からアンインストールする

管理対象デバイスからアンインストールした後に、FMC からパッチをアンインストールします。アップグレードと同様に、ハイ アベイラビリティ FMC から一度に1つずつアンインストールする必要があります。「HA/スケーラビリティ環境でのアンインストール順序 （56 ページ）」を参照してください。

FMC パッチのアンインストールには FMC Web インターフェイスを使用することをお勧めします。管理者アクセス権が必要になります。Web インターフェイスを使用できない場合は、Linux シェルを、シェルの `admin` ユーザまたはシェル アクセス権を持つ外部ユーザのどちらかとして使用できます。

NTP 同期の確認

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

時刻を確認するには、次の手順を実行します。

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

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

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

アプライアンスへのアクセス、通信、正常性

Firepower デバイスは、（インターフェイス設定に応じて）アンインストール中、またはアンインストールが失敗した場合に、トラフィックを渡すことを停止できます。Firepower デバイスからパッチをアンインストールする前に、ユーザの位置からのトラフィックがデバイスの管理インターフェイスにアクセスするためにデバイス自体を通過する必要がないことを確認してください。Firepower Management Center 展開では、デバイスを経由せずに FMC 管理インターフェイスにアクセスできる必要もあります。

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

アンインストールに失敗した場合、再イメージ化が必要になることがあります。再イメージ化を行うと、ほとんどの設定が工場出荷時の状態に戻ります。このため、再イメージ化の前にイベント データと設定データを外部の場所にバックアップしておくことを強くお勧めします。

トラフィック フロー、検査、およびデバイス動作

アンインストール時のトラフィック フローとインスペクションの中断は、アップグレード時に発生する中断と同じです。アップグレードは、保守期間中に行うか、中断による展開環境への影響が最も小さい時点で行うことを強くお勧めします。詳細については、トラフィック フロー、検査、およびデバイス動作 （41 ページ）を参照してください。

HA/スケーラビリティ環境でのアンインストール順序

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

通常は次のことに注意してください。

- 先にセカンダリ/スタンバイ/データユニットをアンインストールしてから、次にプライマリ/アクティブコントロールからアンインストールします。
- 一度に 1 つずつアンインストールします。次のユニットに移る前に、パッチが 1 つのユニットから完全にアンインストールされるまで待ちます。

表 *38 : HA* 内の *FMC* の場合におけるアンインストール順序

FMC の環境	アンインストール順序
FMC ハイ アベイラビリティ	同期を一時停止した状態（「スプリットブレイン」と呼びます）で、FMC のピアから一度に 1 つずつアンインストールします。ペアが split-brain の状況で、構成の変更または展開を行わないでください。 **1.** 同期を一時停止します（スプリットブレインに移行します）。 **2.** スタンバイからアンインストールします。 **3.** アクティブからアンインストールします。 **4.** 同期を再開します（スプリットブレインから抜けます）。

表 *39 : HA* またはクラスタ内の *FTD* デバイスの場合におけるアンインストール順序

FTD の環境	アンインストール順序
FTD ハイ アベイラビリティ	ハイ アベイラビリティ用に設定された FTD デバイスからパッチをアンインストールすることはできません。先にハイ アベイラビリティを解除する必要があります。 **1.** ハイ アベイラビリティを解除します。 **2.** 以前のスタンバイからアンインストールします。 **3.** 以前のアクティブからアンインストールします。 **4.** ハイ アベイラビリティを再確立します。
FTD クラスタ	一度に1つのユニットからアンインストールし、制御ユニットを最後に残します。クラスタ化されたユニットは、パッチのアンインストール中はメンテナンス モードで動作します。 **1.** データモジュールから一度に 1 つずつアンインストールします。 **2.** データモジュールの 1 つを新しい制御モジュールに設定します。 **3.** 以前のコントロールからアンインストールします。

表 *40 : ASA* フェール オーバーペア/クラスタ内の *ASA with FirePOWER Services* デバイスの場合におけるアンインストール順序

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

アンインストールの手順

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

スタンドアロン FMC からのアンインストール

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

始める前に

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

ステップ 1 構成が古い管理対象デバイスに展開します。

アンインストールする前に展開すると、失敗する可能性が減少します。

ステップ 2 事前チェックを実行します。

- 正常性のチェック：FMC のメッセージ センターを使用します（メニュー バーの [システムステータス（System Status）] アイコンをクリックします）。導入環境内のアプライアンスが正常に通信していること、およびヘルス モニタによって報告された問題がないことを確認します。
- タスクの実行：また、メッセージ センターで、必須タスクが完了していることを確認します。アンインストールの開始時に実行中だったタスクは停止され、失敗したタスクとなって再開できなくなります。後で失敗ステータス メッセージを手動で削除できます。

ステップ 3 **[System]** > **[Updates]** を選択します。

ステップ 4 FMC のアンインストール パッケージの横にある [インストール（Install）] アイコンをクリックし、FMC を選択します。

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

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

アンインストールすることを確認し、FMC を再起動します。

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

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

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

ステップ 8 成功したことを確認します。

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

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

ステップ 10 構成を再展開します。

ハイ アベイラビリティ FMC からのアンインストール

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

ピアから一度に 1 つずつアンインストールします。同期を一時停止した状態で、先にスタンバイからアンインストールし、次にアクティブからアンインストールします。スタンバイの FMC でアンインストールが開始されると、ステータスがスタンバイからアクティブに切り替わり、両方のピアがアクティブになります。この一時的な状態のことを「スプリットブレイン」と呼び、アップグレード中とアンインストール中を除き、サポートされていません。ペアが split-brain の状況で、構成の変更または展開を行わないでください。同期の再開後は変更内容が失われます。

始める前に

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

ステップ 1 アクティブな FMC で、構成が古い管理対象デバイスに展開します。

アンインストールする前に展開すると、失敗する可能性が減少します。

ステップ 2 同期を一時停止する前に、メッセージ センターを使用して導入環境に問題がないことを確認します。

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

ステップ 3 同期を一時停止します。

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

b) [ハイ アベイラビリティ（High Availability）] タブで、[同期の一時停止（Pause Synchronization）] をクリックします。

ステップ 4 FMC からパッチを一度に 1 つずつアンインストールします。先にスタンバイで行い、次はアクティブで行います。

「スタンドアロン FMC からのアンインストール （59 ページ）」 の手順に従います。ただし、初期の展開は省略し、各 FMC で更新が成功したことを確認したら停止します。要約すると、それぞれの FMC で以下の手順を実行します。

a) 事前チェック（ヘルス、実行中のタスク）を実行します。

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

ペアが split-brain の状況で、構成の変更または展開を行わないでください。

ステップ 5 アクティブ ピアにする FMC で、同期を再開します。

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

ステップ 6 メッセージ センターを使用して、導入環境に問題がないことを再度確認します。

ステップ 7 構成を再展開します。

任意のデバイスからのアンインストール（FMC マネージド）

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

始める前に

- 特に HA/スケーラビリティの環境において、正しいデバイスからアンインストールしようとしていることを確認してください。「HA/スケーラビリティ環境でのアンインストール順序 （56 ページ）」を参照してください。
- ASA FirePOWER モジュールの場合は、ASA REST API を無効にしていることを確認してください。ASA CLI から：`no rest api agent`。アンインストール後に再度有効にすることができます：`rest-api agent`。

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

アンインストールする前に展開すると、失敗する可能性が減少します。

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

ステップ 2 事前チェックを実行します。

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

- タスクの実行：また、メッセージセンターで、必須タスクが完了していることを確認します。アンインストールの開始時に実行中だったタスクは停止され、失敗したタスクとなって再開できなくなります。後で失敗ステータス メッセージを手動で削除できます。

ステップ 3 デバイスの Firepower CLI にアクセスします。`admin` として、または設定アクセス権を持つ別の Firepower CLI ユーザとしてログインします。

デバイスの管理インターフェイスに SSH 接続するか（ホスト名または IP アドレス）、コンソールを使用できます。 ASA 5585-X シリーズ デバイスは専用の ASA FirePOWER コンソール ポートを備えています。

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

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

ステップ 4 Firepower CLI プロンプトで、`expert`コマンドを使用して Linux シェルにアクセスします。

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

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

Firepowerアプライアンスにパッチを適用すると、そのパッチを簡単に識別できるアンインストーラーが、アップグレードディレクトリに自動的に作成されます。パッケージのアンインストール （65 ページ）を参照してください。

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

注意 システムから、アンインストールの確認メッセージが表示されることはありません。このコマンドを入力すると、デバイスの再起動を含むアンインストールが開始されます。アンインストール時のトラフィック フローとインスペクションの中断は、アップグレード時に発生する中断と同じです。準備が整っていることを確認してください。

ステップ 6 アンインストールをモニタします。

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

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

ステップ 7 成功したことを確認します。

パッチをアンインストールしてデバイスを再起動した後、デバイスのソフトウェア バージョンが正しいことを確認します。FMC で、**[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択します。

ステップ 8 メッセージ センターを使用して、導入環境に問題がないことを再度確認します。

ステップ 9 構成を再展開します。

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

次のタスク

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

ASA FirePOWER からのアンインストール（ASDM マネージド）

次の手順を実行して、ローカル管理されている ASA FirePOWER モジュールからパッチをアンインストールします。FMC を使用して ASA FirePOWER を管理している場合は、「任意のデバイスからのアンインストール（FMC マネージド） （61 ページ）」を参照してください。

始める前に

- 特に ASA のフェールオーバー/クラスタ環境において、正しいデバイスからアンインストールしようとしていることを確認してください。「HA/スケーラビリティ環境でのアンインストール順序 （56 ページ）」を参照してください。
- ASA REST API が無効になっていることを確認します。ASA CLI から：`no rest api agent`。アンインストール後に再度有効にすることができます：`rest-api agent`。

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

アンインストールする前に展開すると、失敗する可能性が減少します。

ステップ 2 事前チェックを実行します。

- システム ステータス：**[モニタリング（Monitoring）]** > **[ASA FirePOWER のモニタリング（ASA FirePOWER Monitoring）]** > **[統計情報（Statistics）]** を選択し、すべてが想定どおりであることを確認します。
- 実行中のタスク：**[モニタリング（Monitoring）]** > **[ASA FirePOWER のモニタリング（ASA FirePOWER Monitoring）]** > **[タスク（Task）]** を選択し、必須タスクが完了していることを確認します。アンイン

ストールの開始時に実行中だったタスクは停止され、失敗したタスクとなって再開できなくなります。後で失敗ステータス メッセージを手動で削除できます。

ステップ 3 ASA FirePOWER モジュールの Firepower CLI にアクセスします。`admin` として、または設定アクセス権を持つ別の Firepower CLI ユーザとしてログインします。

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

ステップ 4 Firepower CLI プロンプトで、`expert`コマンドを使用して Linux シェルにアクセスします。

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

```
sudo install_update.pl --detach
/var/sf/updates/Cisco_Network_Sensor_Patch_Uninstaller-version-build.sh.REL.tar
```

署名付きの（.tar）パッケージは解凍しないでください。

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

注意 システムから、アンインストールの確認メッセージが表示されることはありません。このコマンドを入力すると、デバイスの再起動を含むアンインストールが開始されます。アンインストール時のトラフィック フローとインスペクションの中断は、アップグレード時に発生する中断と同じです。準備が整っていることを確認してください。

ステップ 6 アンインストールをモニタします。

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

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

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

ステップ 7 成功したことを確認します。

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

ステップ 8 構成を再展開します。

次のタスク

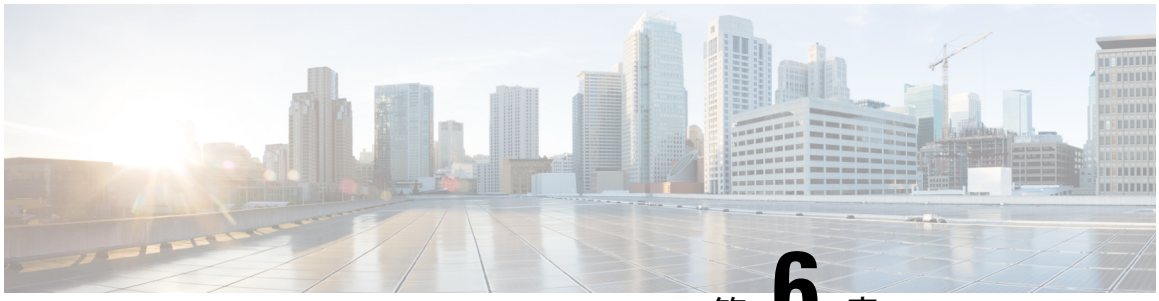
- ASA フェールオーバー/クラスタ環境の場合は、各デバイスについて計画した順序でこの手順を繰り返します。
- ASA FirePOWER モジュールでは、先に ASA REST API を無効にしていた場合は再度有効にします。ASA CLI から、`rest-api agent` を実行します。

パッケージのアンインストール

パッチのアンインストーラーは、アップグレードパッケージと同様に名前が付けられていますが、ファイル名には「Patch」ではなく「Patch_Uninstaller」が含まれます。Firepower アプライアンスにパッチを適用すると、そのパッチ用のアンインストーラーがアップグレードディレクトリに自動的に作成されます。

- `/ngfw/var/sf/updates`（FTD デバイスの場合）
- `/var/sf/updates`（FMC および従来型デバイス（ASA FirePOWER、NGIPSv）の場合）

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



第 6 章

ソフトウェアの新規インストール

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をインストールしてからパッチを適用してください。

新規インストールの決定

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

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

表 *41 :* シナリオ：新規インストールが必要ですか。

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

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

新規インストールに関するガイドラインと制約事項

これらの一般的なガイドラインと警告は、再イメージ化に適用されます。

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

Firepower2100 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。

再イメージ化チェックリスト

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（「インストール手順 （74 ページ）」）を参照してください。

表 *42 : Firepower* 再イメージ化チェックリスト

✓	アクション	詳細
	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、アプライアンスへの物理的アクセスまたはLights-Out管理（LOM）アクセスが必要です。LOM は限定されたアプライアンスのみでサポートされており、すでに設定されている必要があることに注意してください。 （注） 以前のメジャーバージョンに再イメージ化すると、ネットワーク設定が自動的に削除されます。このようなまれなケースでは、物理的アクセスまたはLOMアクセスが必要です。 デバイスに関して、ユーザの位置からのトラフィックがデバイスの管理インターフェイスにアクセスするためにデバイス自体を通過する必要がないことを確認してください。FMC展開では、デバイスを経由せずに FMC 管理インターフェイスにアクセスできる必要もあります。

✓	アクション	詳細
	バックアップを実行します。	再イメージ化の前に Firepower アプライアンスをバックアップします（サポートされている場合）。 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** Firepower アプライアンスを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。誤りを避けるには、注意深い計画と準備が役立ちます。バックアップと復元の要件、ガイドライン、制限事項、およびベストプラクティスの詳細については、ご使用の Firepower 製品のコンフィギュレーション ガイドを参照してください。
	FMC 管理からデバイスを削除します。	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。 FMC または FTD デバイスの再イメージ化後にバックアップから復元する場合は、デバイスをリモート管理から削除する必要はありません。

✓	アクション	詳細
	ライセンスの問題に対処します。	Firepowerアプライアンスを再イメージ化する前に、ライセンスの問題に対処してください。 状況により、Cisco Smart Software Manager からの登録解除が必要になります。また場合によっては、新しいライセンスについてセールス担当者に問い合わせる必要があります。シナリオに応じて必要な操作を決定するには、「新規インストールの決定」を参照してください。 ライセンスの詳細については、次を参照してください。 • Cisco Firepower System Feature Licenses Guide • Frequently Asked Questions (FAQ) about Firepower Licensing • 設定ガイドのライセンスの章

スマート ライセンスの登録解除

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

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

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

次の操作を行う前に、CSSM から手動で登録解除します。

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

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

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

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

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

の登録解除 Firepower Management Center

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

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

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

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

ステップ 3 [Smart License Status] の横の **停止記号**（ ） をクリックします。

ステップ 4 警告し、登録を解除することを確認します。

を使用した FTD デバイスの登録解除 FDM

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

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

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

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

ステップ 4 警告し、登録を解除することを確認します。

インストール手順

リリース ノートにはインストール手順は含まれていません。代わりに、次のドキュメントのいずれかを参照してください。インストールパッケージはシスコサポートおよびダウンロードサイト から入手できます。

表 *43 : Firepower Management Center* のインストール手順

FMC プラットフォーム	ガイド
FMC 1000、2500、4500	Cisco Firepower Management Center 1000, 2500, and 4500 Getting Started Guide
FMC 750、1500、3500 FMC 2000、4000	Cisco Firepower Management Center 750, 1500, 2000, 3500 and 4000 Getting Started Guide
FMCv	Cisco Firepower Management Center Virtual 入門ガイド

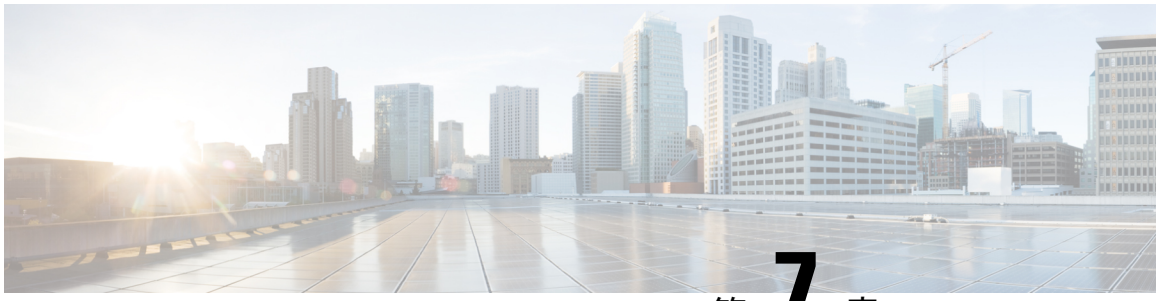
表 *44 : Firepower Threat Defense* のインストール手順

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

FTD プラットフォーム	ガイド
FTDv：Azure	Cisco Firepower Threat Defense Virtual クイック スタート ガイド（Microsoft Azure クラウド向け）

表 *45 : 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 ASA and Firepower Threat Defense Reimage Guide ASDM Book 2: Cisco ASA Series Firewall ASDM Configuration Guide：Managing the ASA FirePOWER Module



第 7 章

資料

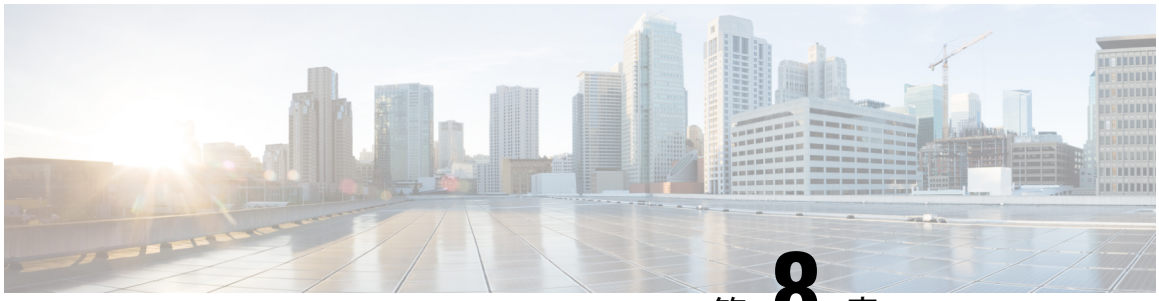
パッチで必要な場合は、Firepower のマニュアルを更新します。

- ドキュメント ロードマップ （77 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
- Navigating the Cisco FXOS Documentation



第 8 章

解決済みの問題

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

（注） 各リストは1度だけ自動生成され、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 バグ検索ツール を「信頼できる情報源」と考えてください。

解決された問題については、次を参照してください。

解決済みの問題の検索

サポート契約がある場合は、Cisco Bug Search Tool を使用して Firepower 製品の最新の解決済みバグリストを取得することができます。 検索では、特定の Firepower プラットフォームとバージョンに影響するバグに絞り込むことができます。バグ ID ごとに検索したり、特定のキーワードを検索したりすることもできます。

これらの一般的なクエリには、バージョン 6.2.3 パッチを実行している Firepower 製品の解決済みのバグが表示されます。

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

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 Firepower 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 Firepower の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。

この表を使用して、プラットフォームで新しい ビルドが使用可能かどうかを確認します。

表 *46* : 新しいビルドを使用したバージョン *6.2.3.x* パッチ

バージョン	新しいビルド	リリース日	プラットフォーム	解決済み
6.2.3.15	39	2020 年 1 月 5 日	FTD/FTDv	CSCvs84578：4100/9300 プラットフォーム上の FTD を 6.2.3.15 break SSHD にアップグレードし、FTD インスタンスが起動しないようにする CSCvs84713：ASA55XX 上の FTD を 6.2.3.15 にアップグレードした後、デバイスに SSH 接続できない CSCvs95725：6.2.3.15 で実行されている仮想 FTD が SSH 要求をブロックし、FMC との接続を失う FTD デバイスをバージョン 6.2.3.15-38 にすでにアップグレードしている場合は、ホットフィックス DW をデバイスに適用します。詳細については、「CSCvs84578 および CSCvs84713 のソフトウェアアドバイザリ」を参照してください。
6.2.3.14	41	2019 年 7 月 3 日	すべて	CSCvq34224：マネージャをアップグレードすると、Firepower プライマリ検出エンジンプロセスが終了する。 すでにバージョン 6.2.3.14-36 にアップグレードしていて、ハイアベイラビリティ用に FTD デバイスが設定されている場合は、FMC にホットフィックス CY を適用します。
6.2.3.11	55	2019 年 3 月 17 日	すべて	Cisco Firepower システムのユーザ エージェントの問題。 バージョン 6.2.3.11 ～ 53 をすでにダウンロードしてインストールしている場合は、Cisco TAC に連絡してホットフィックスを取得してください。

バージョン	新しいビルド	リリース日	プラットフォーム	解決済み
6.2.3.5	53	2018 年 11 月 6 日	FTD/FTDv	CSCvk67239：ASA ファイアウォールおよび Firepower Threat Defense デバイスは、フェールオーバーペアまたはマルチユニットクラスタ内のユニットの状態が変化したときに、トレースバックおよびリロードを行う場合があります。これは、バージョン 6.2.3.5 からバージョン 6.2.3.6 にアップグレードするときにも発生します。 詳細については、CSCck67239 のソフトウェアアドバイザリを参照してください。
6.2.3.2	46	2017 年 6 月 27 日	すべて	CSCvj25386：デバイスでバージョン 6.0 が実行されたことがあると、バージョン 6.2.2.3 よりも前のバージョンへのアップグレードに失敗する場合がありました。 CSCvk06176：この新しいビルドでも、FMC でバージョン 6.2.3 ～ 88 が実行されたことがあると、SSE クラウド接続がドロップされ、テレメトリはアップグレード後にデータを送信できません。FMC が影響を受けている場合は、ホットフィックス T を適用します。
6.2.3.1	47	2017 年 6 月 28 日	すべて	CSCvj25386：デバイスでバージョン 6.0 が実行されたことがあると、バージョン 6.2.2.3 よりも前のバージョンへのアップグレードに失敗する場合がありました。 CSCvk06176：この新しいビルドでも、FMC でバージョン 6.2.3 ～ 88 が実行されたことがあると、SSE クラウド接続がドロップされ、テレメトリはアップグレード後にデータを送信できません。FMC が影響を受けている場合は、ホットフィックス T を適用します。
	45 および 46	2017 年 6 月 21 日	すべて	コンポーネントの問題。

バージョン 6.2.3.16 で解決済みの問題

表 *47* : バージョン *6.2.3.16* で解決済みの問題

不具合 ID	タイトル
CSCvg84794	KP ASA イメージの起動後にすべてのインターフェイスが起動しない
CSCvj49994	IPv6 アドレスがないため、アップグレード中に FXOS パッケージのダウンロードに失敗した
CSCvm48451	4100 および 9300 で侵入イベントパフォーマンスのグラフが空白になる
CSCvm84994	Firepower 4100 および Firepower 9300 の FTD で SSH アイドルタイムアウトが動作しない
CSCvm85823	SSH、ssh_exec を実行できない：コンソールでの open(pager) エラー
CSCvn93683	ASA：cluster exec show コマンドですべての出力が表示されない
CSCvo62077	Cisco Firepower Threat Defense ソフトウェアの VPN システムロギングにおけるサービス拒否攻撃に対する脆弱性
CSCvo78789	Cisco 適応型セキュリティアプライアンスのスマートトンネルに関する脆弱性
CSCvo80853	Cisco Firepower Threat Defense ソフトウェアのパケットにおけるサービス拒否攻撃に対する脆弱性
CSCvp04134	9.12.1 へのアップグレード時に HTTP CLI Exec でトレースバックする
CSCvp16945	Cisco ASA ソフトウェアと FTD ソフトウェアの MGCP におけるサービス拒否攻撃に対する脆弱性
CSCvp16949	Cisco ASA ソフトウェアと FTD ソフトウェアの MGCP におけるサービス拒否攻撃に対する脆弱性
CSCvp45149	プライマリシステムをアクティブとして戻すときのトレースバック
CSCvp49481	Cisco ASA ソフトウェアと Cisco FTD ソフトウェアの SSL VPN におけるサービス拒否攻撃に対する脆弱性
CSCvp55941	ファイル復帰ブロックがランダムにスローされて、SMB 共有からのファイルへのアクセスに関する問題が発生する
CSCvp87623	CAC（HTTPS クライアント証明書）の使用時に更新をアップロードすると「更新要求エンティティが大きすぎます（update request entity too large）」というエラーが発生する

不具合 ID	タイトル
CSCvp90847	FTD/FMC での再署名に SSL が使用するルート CA の更新
CSCvp93468	Cisco ASA ソフトウェアと Cisco FTD ソフトウェアの SSL VPN におけるサービス拒否攻撃に対する脆弱性
CSCvq12070	2 つ以上の同時 ASDM セッションを確立できない
CSCvq13442	コンテキストを削除すると、ssh key-exchange がグローバルにデフォルトになる
CSCvq20910	Cisco Firepower 2100 シリーズのセキュリティアプライアンスの ARP におけるサービス拒否攻撃に対する脆弱性
CSCvq35440	Anyconnect のストラップ検証へのアップグレードの機能拡張：Cisco VPN セッションリプレイの脆弱性
CSCvq36042	ハートビートが失われてリロードが発生する
CSCvq54034	CCM レイヤで WRL6 と WRL8 のコミット ID が更新される（Sprint 65）
CSCvq56257	キャッシュされたマルウェアの処置が想定どおりに期限切れにならないことがある
CSCvq66092	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 BGP DoS の脆弱性
CSCvq70485	「securityzones」REST API が低速になる
CSCvq70775	FPR2100 FTD スタンバイユニットで 9K ブロックがリークする
CSCvq71217	CSCvn30118 の後、mysql-server.err によりローテーションが失敗して、ディスク使用率が高くなる
CSCvq73534	Cisco ASA ソフトウェアのケルベロス認証バイパスの脆弱性
CSCvq73599	Cisco VPN セッションリプレイの脆弱性：ASA for SSL（OpenSSL 1.0.2）および SCEP プロキシのストラップ修正
CSCvq93640	CCM レイヤで WRL6 と WRL8 のコミット ID が更新される（Sprint 67）
CSCvr07419	Cisco ASA および FTD ソフトウェアの IPv6 DNS におけるサービス拒否攻撃に対する脆弱性
CSCvr09748	Cisco FXOS および FTD ソフトウェアのコマンドライン インターフェイスで任意のファイルが読み取り/書き込みされる脆弱性
CSCvr11395	スケジュール済みの展開時にデバイスグループから展開された一部のデバイスのみ

不具合 ID	タイトル
CSCvr17735	SI 更新時の SFDataCorrelator で CPU の使用率が高くなる
CSCvr37502	libexpat 不適切な解析によるサービス拒否の脆弱性
CSCvr39556	libclamav.so のセグメンテーション違反（SFDataCorrelator のコンテキスト内）
CSCvr49734	Cisco FXOS および UCS Manager ソフトウェアにおける CLI コマンドインジェクションの脆弱性
CSCvr55825	Cisco ASA および FTD ソフトウェアのパストラバーサルの脆弱性
CSCvr63941	KP ASA 診断 CLI チャネルが機能しなくなる
CSCvr85295	Cisco Adaptive Security Appliance と Firepower Threat Defense ソフトウェアリモート
CSCvr86213	CD は、クラスタノードリリースの Lina の状態の Cluster-Msg-Delivery-Confirmation を無視する必要がある
CSCvr90768	FTD：低速リンクを通じた展開は失敗する場合がある
CSCvr92327	ASA/FTD がスレッド名「PTHREAD-1533」でトレースバックおよびリロードすることがある
CSCvs12288	SSL ポリシーが有効になっている状態で debug_policy_all が設定されていると Snort が予期せず終了する
CSCvs19968	スタックし、HA FTD ポリシー展開エラーが発生しないようにコンソールを修正する
CSCvs33416	カーネルの 4.14.158 へのアップグレード
CSCvs34844	ハードウェアと通信すると、pm プロセスがランダムにデッドロック状態になる
CSCvs50459	Cisco ASA および Cisco FTD の不正な OSPF パケット処理によるサービス拒否攻撃に対する脆弱性
CSCvs59487	99.14.1.64 イメージへのアップグレード中に KP デバイスでクラッシュが確認された
CSCvs60254	libxml2 xmlParseBalancedChunkMemoryRecover メモリリークの脆弱性
CSCvs61701	Firepower 2100 のメモリリークが原因で DME のプロセスがクラッシュする

不具合 ID	タイトル
CSCvs77334	「別のユニットのインスペクションエンジンが Snort とディスクの障害により失敗しました（Inspection engine in other unit has failed due to snort and disk failure）」というエラーにより FTD がフェールオーバーする
CSCvs84578	4100/9300 プラットフォーム上で FTD を 6.2.3.15 にアップグレードすると、FTD インスタンスが起動しなくなる
CSCvs84713	ASA55XX/ISA 3000/FTDv 上の FTD を 6.2.3.15 ビルド 38 にアップグレードした後、デバイスに SSH 接続できない
CSCvs87168	範囲外のインターフェイス ID による Snort の致命的なエラー
CSCvs94486	CSCvs59487 を解決するには追加の修正が必要
CSCvs98311	CC モードで 6.2.3.15-38 から 6.2.3.16-29 にアップグレードすると、FSIC で障害が発生する
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
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
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
CSCvt39299	シリーズ 3 センサーの 6.2.3.15 から 6.4.0 へのアップグレードが失敗する
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
CSCvu30830	sshd_config ファイルの不正な CiscoSSH キーワークが原因で NGIPS センサーの SSH 接続が切断される

バージョン 6.2.3.15 で解決済みの問題

表 *48 :* バージョン *6.2.3.15* で解決済みの問題

不具合 ID	タイトル
CSCve24102	GUI で、DHCP プールごとに最大 256 個のアドレスを設定できる必要がある
CSCvg49225	スケジュールされた FXOS アップグレードをキャンセルしてもイベントがクリアされない

不具合 ID	タイトル
CSCvg85687	FXOS の起動時にコンソールにエラー メッセージが表示される
CSCvk43854	Cisco Firepower Threat Defense 検出エンジン ポリシーのバイパスの脆弱性
CSCvm64400	IKEv2：IKEv2-PROTO-2：「プラットフォームからの PSH の割り当てに失敗しました（IKEv2-PROTO-2: Failed to allocate PSH from platform）」
CSCvm68648	Firepower ソフトウェアでの CVE-2016-8858（OpenSSH）の確認
CSCvm82966	Linux カーネル 4.14 の脆弱性
CSCvn46390	Lina msglayer パフォーマンスの改善：ポートホットフィックス BO
CSCvn77125	FXOS：copy コマンドでワイルドカードを使用して複数のファイルを転送できる必要がある
CSCvo29989	Cisco FirePower Threat Defense に関する情報漏えいの脆弱性
CSCvo47390	スレッド SSH での ASA トレースバック
CSCvo48838	長すぎる設定行のエラーを Lina が適切に報告しない
CSCvo68184	セカンダリ FTD の診断 I/F の管理専用が表示されなくなる
CSCvo68448	5585 プラットフォームで ASA モジュールをリロードした後、ASA が SFR モジュールを「応答なし」として報告する
CSCvo85861	リンクステートの伝達が FTD CLI に表示されない
CSCvo86485	不正な HTML <base>文法ベースのパーサーによるタグ処理
CSCvo88762	FTD インライン/トランスペアレントでパケットが入力インターフェイスを介して送り返される
CSCvo89224	展開用のデバイス リストの取得で 10 分後に FMC がタイムアウトになる
CSCvo90998	インラインセット インターフェイスの snort に LACPDU を送信すべきでない
CSCvp07616	[ciam] Python urllib セキュリティがバイパスされる脆弱性
CSCvp15176	Firepower デバイスにインストールされた FTD/ASA が通信障害を報告し、それ自体をアクティブ/マスターと見なす場合がある
CSCvp16536	SIP インスペクションによりデータパスで ASA のトレースバックとリロードが確認される
CSCvp16618	HTML ベースタグ内の URL が、GBP で処理された後も書き換えられなない

不具合 ID	タイトル
CSCvp27263	6.5.0 より以前の Cisco Firepower Management Center における ClamAV の複数の脆弱性
CSCvp35141	ASA が POST 要求に対して無効なリダイレクト応答を送信する
CSCvp35769	[ciam] Apache HTTP Server の URL 正規化に関する DoS 攻撃の脆弱性
CSCvp37779	FTD のトラブルシューティング ファイルからの show tech が不完全である
CSCvp46150	[ciam] GNU Wget のバッファオーバーフローの脆弱性
CSCvp48273	[ciam] Linux カーネル cipso_v4_validate のサービス拒否攻撃に対する脆弱性
CSCvp49576	他のユニットがクラスタから離脱する際に FTD クラスタのトレースバックが発生する
CSCvp53637	インラインセットでフローがオフロードされる
CSCvp54261	SFR モジュール/7000/8000 デバイスの監査 syslog で UDP ではなく TCP が syslog 通信に使用される
CSCvp55880	Snort プロセスのダウン時にフェールクローズされた FTD でパケットがパススルーされる
CSCvp55901	HA アクティブユニットの ASA で LINA が繰り返しトレースバックする
CSCvp58028	nfm_exceptiond の natd スレッドで約 90 ～ 100% の CPU 時間が使用される
CSCvp66559	大規模な XML 応答の解析時に例外により FTD HA で展開が失敗する
CSCvp67257	カーネルアップグレード（3.10 ～ 4.14）による USGv6 障害
CSCvp67392	リバースパスチェックにより ASA/FTD HA データインターフェイスのハートビートがドロップされる
CSCvp70699	Firepower シャーシの再起動後における ASA フェールオーバーでのスプリットブレイン（両方のユニットがアクティブ）
CSCvp72244	CVE-2019-11815 の Cisco 8000 シリーズの評価
CSCvp72488	Firepower：6.3.0.2 以降へのアップグレード後のネットワーク接続障害に対する AMP
CSCvp83437	ローカル アカウントを使用したシリアル コンソール/SSH ログインが成功しても、すぐにログイン プロンプトに戻る
CSCvp97061	URL フィルタリングですべての URL が未分類として表示される

不具合 ID	タイトル
CSCvp97799	SSL ポリシーのエクスポート時に openSSL コールで CC モードにして 6.5.0-1148 にアップグレードした後、ポリシーの展開に失敗する
CSCvp97916	アクティブユニットで「フェールオーバー」を 2 回実行すると、スタンバイユニットのインターフェイス設定がクリアされる
CSCvp98066	CD のリセット時にフラグ [parseFailoverReqIssued] をクリアしないと、ノードを結合できない
CSCvq00675	Linux カーネル sas_expander.c が競合状態で任意のコードを実行...
CSCvq06790	シリーズ 3 デバイスで Snort プロセスがメモリ破損でコアをダンプする
CSCvq13917	ADI が VPN ユーザのログインを学習しなくなる
CSCvq19525	TCP_SACK の sfims の評価
CSCvq19641	TCP_SACK に対する Firepower 4K/9K スーパバイザの評価
CSCvq27010	ASA-SFR データプレーンの通信でフラッピングが発生した際にメモリリークが起こる
CSCvq32681	FTD のアップグレード時に複数のインターフェイスペアのインラインセットに対して Fail to Wire 設定が無効になる
CSCvq33916	FP 4100 とスイッチとの間（40Gb BiDi から 40/100Gb BiDi への場合）のリンクダウン
CSCvq39083	SSL ポリシーが有効になっている場合にブラックリストに登録された URL への HTTPS 接続がセキュリティ インテリジェンスでドロップされない
CSCvq44665	FTD/ASA：アサート snp_tcp_intercept_assert_disabled によるデータパスでのトレースバック
CSCvq54242	SSL ポリシーでの警告「送信元ネットワークで、空のグループがあります（There is an empty group in the source networks）」
CSCvq56462	ファイルポリシーが一部のマルウェアドキュメント（.doc）および Adobe Flash（.swf）ファイルを検査しない
CSCvq57710	マネージャをアップグレードすると、Firepower プライマリ検出エンジンプロセスが終了することがある
CSCvq61651	FMC での URL DB ダウンロード失敗アラート：FMC/FDM で新しい URL DB の更新が有効にならない
CSCvq65092	デバイス関連の REST API コールが低速になる
CSCvq98171	最新の r241 イメージを使用してリカバリを実行できない

バージョン 6.2.3.14 で解決済みの問題

表 *49* : バージョン *6.2.3.14* で解決済みの問題

不具合 ID	タイトル
CSCvb15074	削除されたかアウトオブバンドで追加されたインターフェイスの FMC ヘルス通知がスタックする
CSCvi63474	6.2.2 へのアップグレード後に ASDM を介した SFR モジュールのシステム ポリシーの編集ができない
CSCvk69823	FMC または FTD のいずれでも変更を加えていないにもかかわらず、FlexConfig オブジェクトがデバイスにプッシュされる
CSCvm70274	tcp プロキシ：データパスでの ASA のトレースバック
CSCvn86777	メモリが不足している FTD で展開を行うとインターフェイス名が削除される
CSCvo24145	大きな firewall_rule_cache テーブルによる ids_event_alerter の高メモリ使用率
CSCvo33348	非標準ポートの Mysql トラフィックが正しく分類されない
CSCvo33851	ngfw.properties が空の場合に ngfwManager が開始されない
CSCvo43679	FTD Lina のトレースバック（Normaliser によるシステムでのパケット ループが原因）
CSCvo50168	監査ログの設定の失敗によりシステム設定が編集できなくなる
CSCvo60580	「show inventory」コマンド発行時の ASA のトレースバックとリロード
CSCvo60862	アクセス コントロール ポリシー編集時の内部エラー
CSCvo74745	多数の連続 URL ルックアップ（30M 超）生成後のクラウド エージェントのコア化
CSCvo90805	Cisco Firepower Management Center RSS のクロスサイト スクリプティングの脆弱性
CSCvp16979	ssl および daq デバッグ ログを動的に有効化/無効化できない
CSCvp18878	ASA：データパスでのウォッチドッグのトレースバック
CSCvp19549	FTD lina がスレッド名 cli_xml_server でコア化する
CSCvp24728	FTD によってランダムな SGT タグが追加される

不具合 ID	タイトル
CSCvp24787	（snort）HTTPS 経由時にファイルが検出されなくなる（SSL 再署名）
CSCvp25583	FMC GUI を介して BGP に OSPF を再配布すると FTD によって自動的にメトリックが 0 に設定される
CSCvp29692	ポリシー展開失敗後からのロールバック後に FIPS モードが無効になる
CSCvp33052	処理されていないリソースが一時的に使用できないという問題により Firepower 8000 インターフェイスがフラップする場合がある
CSCvp43536	アップグレードした FMC デバイスで、正常に展開された後も FXOS デバイスがダーティとして表示される
CSCvp54634	不明瞭な DND を使用しているときに正しくないルールが一致する
CSCvp78197	ポリシーの展開による ospf ネイバーの削除および追加
CSCvp81967	管理対象デバイスが 500 以上ある場合に FMC のデバイス管理ページのロードが遅くなる
CSCvp82945	NAT ポリシーの適用がエラーの重複で失敗する
CSCvp96934	重複する NAT を含むエラー メッセージがクリアされ実行可能であることを確認する
CSCvq13917	6.2.3.13 ADI が VPN ユーザのログインを学習しなくなる
CSCvq34224	マネージャをアップグレードすると、Firepower プライマリ検出エンジン プロセスが終了する

バージョン 6.2.3.13 で解決済みの問題

表 *50* : バージョン *6.2.3.13* で解決済みの問題

不具合 ID	タイトル
CSCve13816	いくつかのセキュリティ脆弱性に対処するために MEMCACHED ソフトウェアのアップグレードが必要
CSCvf83160	スレッド名 DATAPATH-2-1785 でのトレースバック
CSCvg01007	https pdf 添付ファイルの問題
CSCvg74603	eStreamer アーカイブ イベントが diskmanager によって正しくプルーニングされない

不具合 ID	タイトル
CSCvi16224	NFVIS（KVM）システムに ASAv VM を展開するときに SNMPv3 の snmp-server ホスト コマンドが正しく適用されない
CSCvi32569	mysql-server.err ログに過剰なロギングが発生すると FTD に大きなログ ファイルが生成される
CSCvi59887	フェールオーバーイベント後にOSPFルートが古くなりルーティングテーブルにスタックする場合がある
CSCvj49623	Smart Licensing のメモリ リーク
CSCvk14242	FTD の sfstunnel プロセスにすでに削除されている大規模なクラウド db ファイルが保持されている
CSCvk26612	「デフォルトのキーリング証明書が無効です。理由：期限切れ（default Keyring's certificate is invalid, reason: expired）」 ヘルスアラート
CSCvk29263	設定セッション内で変更をコミットした後に SSH セッションがスタックする
CSCvk30739	ASA CP コアのピン接続によりコアローカル ブロックが枯渇する
CSCvk44166	Cisco ASA および FTD TCP プロキシのサービス妨害（DoS）脆弱性
CSCvk72958	インターフェイスに適用されている QoS が機能しない
CSCvm00066	ASA が「フラッシュからの読み取り中」に数時間にわたってスタックする
CSCvm08769	アクティブ ユニットの IP を使用してスタンバイ ユニットが BFD パケットを送信すると BGP のネイバーシップが障害を起こす
CSCvm17985	BVI インターフェイスの管理アクセスを使用した write net コマンドの開始が成功しない
CSCvm27111	OSPF 設定を削除する際の FTD Lina のトレースバック
CSCvm36362	ルート トラッキング エラー
CSCvm80779	ASA が H323 H225 を検査しない
CSCvm82290	IRB 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
CSCvm85257	トラフィックを使用してvpnモードを変更するとスピンロックがトレースバックする
CSCvm86008	ポリシーの展開：デルタ設定が実行コンフィギュレーションにコピーされないため LINA 設定が変更されないままになる

不具合 ID	タイトル
CSCvm88294	パーティション強制ドレインが発生していないためディスク使用率が高くなる
CSCvn22833	Firepower 4100 の ASA で ADI プロセスの開始に失敗する
CSCvn30108	ASAv での「show memory」 CLI 出力が正しくない
CSCvn30393	AnyConnect の認証/DAP アセスメントの実行中に ASA が emweb/https でトレースバックする
CSCvn31347	ACL：アクセスグループの設定エラー後に ACL を設定できない
CSCvn32620	IKEv2 が他の VPN ライセンスの取得に失敗した
CSCvn34246	AC ポリシー エディタのロードに時間がかかりすぎるためロード インジケータが必要になる
CSCvn38453	ASA：FIPS が有効な場合に Quovadis ルート証明書をトラストポイントとしてロードできない
CSCvn45750	3D デバイスへの展開時に FMC 監査ログに管理者とシステムのみがオーナーとして表示される（GUI/SYSLOG）
CSCvn50320	Firepower MySQL サーバ：Oracle MySQL の 2018 年 10 月の重要なパッチ更新
CSCvn55007	キー再生成後に DTLS が失敗する
CSCvn57284	FTD でサポートされていない EC カーブ x25519
CSCvn66248	ファイルがオフボックスで変更されて再度コピーされた場合に「boot config」を設定しても効果がない
CSCvn67137	NetFlow の使用時に ASA5506 が徐々にメモリ リークを起こすことがある
CSCvn68527	FPR21xx：AnyConnect で割り当てたアドレスが、スタンバイで割り当て済みと見なされない
CSCvn71592	FMC の再起動後、Snort によって生成された侵入イベントが FMC に送信されず、webGUI に表示される
CSCvn73962	IPSec を使用したデータパスでの ASA 5585 9.8.3.14 のトレースバック
CSCvn76829	SSL クライアントとしての ASA がハンドシェイク エラー パスでメモリ リークを起こす
CSCvn77248	シスコ セキュアブート ハードウェアにおける改ざんの脆弱性

不具合 ID	タイトル
CSCvn78597	プロキシが有効になっている場合、HTTPS ブロック サイトでは Firepower ブロック ページが MS IE11 および Edge に表示されない
CSCvn78674	シスコ適応型セキュリティ アプライアンスのクライアントレス SSL VPN におけるクロスサイト スクリプティングの脆弱性
CSCvn78870	範囲外の allocate-interface コマンドによる ASA マルチコンテキストのトレースバックとリロード
CSCvn94100	「Process Name: lina」| Netflow による ASA のトレースバック
CSCvn95711	スレッド名のトレースバック：IKEV2 ipsec-proposal にプロトコルを追加した後の Unicorn Admin ハンドラ
CSCvn96898	SCP のダウンロードにより DMA_Pool で発生するバイナリ サイズ 1024 のメモリ リーク
CSCvn97591	パケット トレーサが「ERROR: TRACER: NP failed tracing packet」で失敗し、循環 ASP でキャプチャをドロップする
CSCvo04444	Ikev2 トンネルの作成に失敗する
CSCvo06216	CSCuz22961 の hanover におけるスプリット DNS コミットの問題に対する 255 文字以上のサポート
CSCvo11406	シスコ適応型セキュリティ アプライアンスのクライアントレス SSL VPN におけるクロスサイト スクリプティングの脆弱性
CSCvo11416	シスコ適応型セキュリティ アプライアンスのクライアントレス SSL VPN におけるクロスサイト スクリプティングの脆弱性
CSCvo13497	「log default」キーワードのあるアクセスリストを削除できない
CSCvo15484	ユーザ情報が mysql と sybase 間で一致しない場合、ユーザ IOC を削除できない（部分的に修正）
CSCvo17033	シスコ適応型セキュリティ アプライアンスのクライアントレス SSL VPN におけるクロスサイト スクリプティングの脆弱性
CSCvo23222	マルチコンテキスト展開でのリソースの問題により AnyConnect セッションが拒否される
CSCvo27109	9.6(4)6 から 9.6(4)20 へのアップグレード時にスタンバイがリブート ループに陥ることがある
CSCvo42174	ASA IPSec VPN EAP が PKI の有効な証明書をロードできない

不具合 ID	タイトル
CSCvo45093	異なる名前の 2 つのオブジェクトがあるが、ECMP なしのルートで同じネットワークが使用されている場合の検証チェック
CSCvo45209	FTD - クラスタ：クラスタに新しいユニットを追加するとトラフィックのドロップが発生する場合がある
CSCvo51265	SCP のボックスへの大規模なファイル転送によりトレースバックが発生する
CSCvo55151	VTI が存在する場合に crypto ipsec inner-routing-lookup の設定を許可しないようにする必要がある
CSCvo56616	展開がタイムアウトする場合があり非終端 AQ が発生する
CSCvo56836	スケール：500 以上のデバイスを使用すると UMS によって UI がハングする（特に展開時）
CSCvo58847	トンネル置き換えシナリオが原因で発生した高 IKE CPU に対処するための機能強化
CSCvo60627	新しいクラスタ ユニットをセットアップに追加した後でポリシーの展開が失敗する
CSCvo62060	FMC が大量のデバイスを管理しているときにテレメトリが送信されない
CSCvo66534	影響を受けるスレッドとしてデータパスを示すトレースバックとリロード
CSCvo70866	任意の値の SGT タグを持つすべてのクライアント パケットに対するサーバ パケットで SGT タグがタグなしと表示される
CSCvo72179	SMB ではリモート ストレージ設定でドット（.）を使ったバージョン文字列の設定を許可する必要がある
CSCvo72232	ブラウザの ERR_SSL_BAD_RECORD_MAC_ALERT または SSL_ERROR_BAD_MAC_ALERT
CSCvo74350	ASA がトレースバックしリロードすることがある。WebVPN トラフィックに関連する可能性がある
CSCvo76727	ルートに複数のオブジェクトであるとポリシーの展開に失敗する可能性について警告が表示されない
CSCvo81073	NGFWHA EO がないため [Device Management] ページをロードできないか、FMC をアップグレードできない
CSCvo83574	インライン セットをタップ モードから切り替えるとデバイスが不良状態になる
CSCvo87930	w3m を使用した ipv6 の HTTP が失敗する

不具合 ID	タイトル
CSCvo88188	App-ID 条件を持つ SSL ルールが復号機能を制限する可能性がある
CSCvo88306	重複するルールがあると NAT ルールが誤った順序で適用される可能性がある
CSCvo93872	GTP トラフィックの検査中のメモリ リーク
CSCvo94486	セキュリティ インテリジェンスの処理中に Snort プロセスが終了する
CSCvp21837	FMC を経由する必要なしに FTD が URL ルックアップを直接実行できるようにする
CSCvp42398	シリーズ 3 8250：999_finish/989_flip_mbr.sh で 6.4.0 ～ 87 へのアップグレードに失敗した
CSCvp54634	不明瞭な DND を使用しているときに正しくないルールが一致する

バージョン 6.2.3.12 で解決済みの問題

表 *51* : バージョン *6.2.3.12* で解決済みの問題

不具合 ID	タイトル
CSCvh26064	7000/8000 センサーで「変更調整」を使用できない
CSCvj82652	disk0 が読み取り専用にマウントされているため展開の変更がデバイスにプッシュされない
CSCvk56988	Cisco ClamAV MEW アンパッカーの Denial of Service（DoS）脆弱性
CSCvm16724	FXOS ASA/FTD には内部データ インターフェイス カウンタをポーリングするための手段が必要
CSCvm24210	同じタイムスタンプで実行されている 2 つのスケジュール タスクが同じファイルにアクセスするとスケジュール タスクの 1 つが失敗する
CSCvm35373	設定が原因でプルーニング プロセスの開始に失敗する
CSCvm40545	FTD を 2 回連続してダウングレードすると（2 回のダウングレード間で更新せずに）誤った lina バージョンになる
CSCvn07452	インライン セットをタップからインラインに切り替えると 712x デバイスが不安定になる
CSCvn09383	「www.」の部分なしで同じ URL が 2 回目に入力されると手動 URL ルックアップで Uncategorized が返される

不具合 ID	タイトル
CSCvn38189	バックアップ スクリプトの終了後に SFDataCorrelator が再起動されない
CSCvn46358	VPN ステータス メッセージの送信による lina msglyr インフラの過負荷
CSCvn49854	後続の HTTP 要求が URL と XFF を取得しない
CSCvn67570	amp-stunnel.conf が FMC のアップグレード後に正しい amp クラウド サーバを指さない
CSCvn67888	REST API を使用してオブジェクトを追加するとポリシーの展開に失敗する
CSCvn72570	Cisco ASA ソフトウェアおよび FTD ソフトウェア VPN SAML 認証バイパスの脆弱性
CSCvn73848	設定されたアイドル タイムアウトよりも前に Snort セッションがタイムアウトする
CSCvn74112	FTDv には vmxnet3 と ixgbevf インターフェイスが混在した初期起動の設定がない
CSCvn75368	FPR プラットフォームの IPsec VPN が断続的にダウンする
CSCvn78593	FTD でコントロールプレーン ACL が正しく機能しない
CSCvn82895	Diskmanager がすべてのイベント ファイルを追跡しない場合がある
CSCvn87965	FMC を TG アカウントに関連付ける際に FMC がユーザを TG コンソールにリダイレクトすることはできない
CSCvn99712	Cisco Firepower Management Center のクロスサイト スクリプティングの永続的な脆弱性
CSCvo02097	ASA クラスタを 9.10.1.7 にアップグレードするとトレースバックが発生する
CSCvo12057	DHCPRelay がユニキャスト フラグ付きの DHCP Offer パケットを消費しない
CSCvo15545	nfm-burnin.sh システム検証テストが最新の NFM リリースで失敗する
CSCvo17775	新しいサブインターフェイスが追加され、「ac-address auto」が有効になると EIGRP が中断する
CSCvo20847	同期時に xlate の割り当ての破損が原因でアクティブ FTP がクラスタを介して失敗する
CSCvo23150	ユーザ ID に対する過剰な DB クエリによりユーザ セッションの処理が遅くなる

不具合 ID	タイトル
CSCvo27164	SFDataCorrelator が不適切な「Resuming storage of old events」メッセージをログに記録する
CSCvo29973	暗号スイート条件がある ssl ルールにより不要な tls 1.3 ダウングレードが発生する可能性がある
CSCvo31353	URL カテゴリが使用され、証明書の共通名が一致しない場合、SSL 接続が失敗する可能性がある
CSCvo31953	SFDataCorelator プロセスのメモリ リーク
CSCvo32329	削除されたレルムが原因で多くの user_id が user_identities キャッシュにロードされる
CSCvo38051	ctm_ipsec_pfkey_parse_msg における ctm_ipsec_pfkey.c:602 での segfault
CSCvo39052	CC モードを有効にした後の FSIC エラー
CSCvo39094	展開するデバイスを選択した後、ポリシー展開タスクを挿入するための処理時間が遅延する/長くなる
CSCvo40210	ダッシュボード ウィジェットでの Talos RSS フィードの更新
CSCvo43693	複数のファイル modules*.tgz および vdb*.tgz が FMC から転送されるため FTD HA の作成が失敗する
CSCvo44064	sni がないため url ルックアップが保留中の際にアグレッシブ ダウングレード アクションが実行される
CSCvo47562	キー再生成中に PKI ハンドルが解放されないため、VPN セッションが失敗する
CSCvo50230	未分類の URL への SSL 接続が繰り返し失敗する場合がある
CSCvo54799	fstab の devpts エントリが破損しているためデバイスへの ssh が失敗する
CSCvo55203	登録済みデバイスが [Device Management] ページに表示されない
CSCvo55282	ユーザが AC ルールに無効なインライン ポート範囲を誤って入力できるとポリシーの展開が失敗する
CSCvo56675	フェールオーバー状態の変更または xlate のクリアを原因とする ASA または FTD のトレースバックとリロード
CSCvo56895	コンテキスト エクスプローラの一部のドーナツ グラフのロードに失敗する
CSCvo61091	NAP ポリシー メタデータを送信する際の eStreamer メモリおよび CPU 使用率の増大

不具合 ID	タイトル
CSCvo62031	IKE デバッグ実行中の ASA のトレースバックとリロード
CSCvo63240	アップグレード後にスマートトンネルのブックマークが機能せず、証明書エラーとなる
CSCvo66920	機能強化：重複するリモート プロキシのカウンタを追加
CSCvo67454	無効なポート範囲オブジェクトにより AC ポリシーの展開が失敗する
CSCvo72462	ルールを復号しないとトラフィックが中断する

バージョン 6.2.3.11 で解決済みの問題

表 *52* : バージョン *6.2.3.11* で解決済みの問題

不具合 ID	タイトル
CSCuz28594	Diskmanager：Diskmanager が 99 % までプルーニングしないため /var/storage で重大なアラートが発生する
CSCvi54162	ピアが存在しない場合に「ha-replace」アクションが動作しない
CSCvi55841	ブラックリスト設定ファイルの保存エラーが検出されない
CSCvi62112	FTD トランスペアレントで FlexConfig を介して BPDU をブロックすると展開と登録の問題が発生する
CSCvk06386	ファイル ポリシー判定にかかわらず、FTD ファイルが複数の既存の接続を介して許可される
CSCvm14875	多数の古い cloudconfig EO がパフォーマンスの問題を引き起こす
CSCvm58799	展開中に複数の Snort が応答しない場合、リカバリに時間がかかりすぎる
CSCvm60039	カスタム DNS セキュリティ インテリジェンス フィードのダウンロードに断続的に失敗する
CSCvm96339	archive_cache_seed.sensor ファイルが原因で /dev/root パーティションが 100 % になる
CSCvn10634	順序が正しくない（実際のデータの前に ACK がある）場合、HTTP フローでファイルが検出されない
CSCvn16102	Diskmanager のファイル キャプチャ データが数時間にわたって同時に増加しない
CSCvn17347	CPU プロファイリング結果表示時のトレースバックとリロード

不具合 ID	タイトル
CSCvn38082	FMC は mongo の破損を特定して回復する必要がある
CSCvn41903	dce2-mem-reloader のメモリ調整に時間がかかりすぎるため Snort のリロードが失敗して再起動が発生する
CSCvn47788	Firepower プラットフォーム設定ポリシーの監査ログ ホストの有効なホスト名 IP で UI 検証が失敗する
CSCvn48739	CLISH モードおよびトラブルシューティングで取得された FTD show tech は省略されている場合がある
CSCvn53145	ポリシーの展開で「Variable set has invalid execulded values」がスローされた
CSCvn69019	単一引用符で囲まれたユーザ名は user_ip_map ファイルに書き込まれない
CSCvn72683	FMC webGUI の [Device Management] ページのロード時間が長すぎる（約 45 秒、ライセンスの取得に 25 秒）
CSCvn73848	設定されたアイドル タイムアウトよりも前に Snort セッションがタイムアウトする
CSCvo00887	「Do Not Decrypt」ルールが可能な唯一の判定である場合、ssl クライアント hello を変更することはできない
CSCvo03186	Firepower Management Center の [Domain] ページのロードに時間がかかりすぎる
CSCvo03808	OOM が原因で FMC からの展開が失敗し、理由が示されない
CSCvo11077	新しい IKEv1 トンネルを確立して終了すると IPSec でメモリ リークが検出される
CSCvo39052	CC モードを有効にした後の FSIC エラー

バージョン 6.2.3.10 で解決済みの問題

表 *53* : バージョン *6.2.3.10* で解決済みの問題

不具合 ID	タイトル
CSCuu67159	ASA：DATAPATH-2-1157 でのトレースバック
CSCva62256	500 台のセンサーがある場合、アプライアンス ステータス ウィジェットでのロードに時間がかかりすぎる

不具合 ID	タイトル
CSCvf81672	EtherChannel に障害が発生した場合のフェールオーバー後に ASA ルートがフラッシュされる
CSCvg40735	GTP インスペクションが CPU 使用率をスパイクさせることがある
CSCvg56122	SSL ハンドシェイクが大規模な証明書チェーンで失敗する
CSCvi09811	DATAPATH のトレースバック、assertion "0" failed: file"./snp_cluster_transport.h", line 480
CSCvi28763	FTD プラットフォーム設定：SSL カスタム設定のデフォルト DH グループを 2 に変更する
CSCvi34533	SNMPv3 ユーザが定義されていない場合、アクセス リストで変更を保存できない
CSCvi71622	スタンバイ FTD の DATAPATH でのトレースバック
CSCvi97028	到達不能な syslog サーバを設定すると fmc GUI が低速になる
CSCvj01704	SFR モジュールのシャットダウン後に ASA が ASA 5585-X のみでリブートによりトレースバック状態になる
CSCvj65154	プロキシ パスワードに @ 文字が含まれている場合、FMC が SSM との通信に失敗する
CSCvj74643	AD で CAC 認証および認可の使用を有効にすると RADIUS が変更時に切断される
CSCvj87287	FMC に対する REST-API 要求の同時フラッドによりアクセス不能になる
CSCvj89445	GUI で展開ステータスが一致してない
CSCvj97229	FMC の CAC の外部認証オブジェクトには「ユーザ名テンプレート」が必要
CSCvk18330	アクティブな FTP データ転送が FTP インスペクションと NAT で失敗する
CSCvk19946	キャッシュ アーカイブ データのフラッディングにより Sftunnel サービスが停止する
CSCvk39339	日本語の FMC でスケジューリング レポートの生成を実行できない
CSCvk40964	空のインターフェイス設定をデバイスに展開するとトラフィックが停止する
CSCvk46038	エラー：権限付与が設定のキャッシュ中にすでに取得されている
CSCvk50815	GTP インスペクションが TCP パケットを処理してはならない

不具合 ID	タイトル
CSCvk55634	ポリシー展開の通知がスタックしているためランダムなポリシー展開に失敗する
CSCvm24706	GTP 削除ベアラー要求がドロップされている
CSCvm28730	CPU プロファイリング情報の取得中に ASA/FTD-LINA トレースバックが確認される
CSCvm33553	クロック ドリフトにより ndclientd からのハートビートの失敗が発生する
CSCvm46014	FTD HA でスタンバイ デバイスが破損している場合、設定のコピーに失敗できない
CSCvm55091	FP プラットフォームで「No Switchover」のステータスのままで HA 障害を起こしたプライマリ ユニットがアクティブと表示される
CSCvm59983	ファイルサイズ ディレクティブが無効な入力エラーを返し、clish からのキャプチャを中断する
CSCvm67273	ASA：PC alloc_fo_ipsec_info_buffer_ver_1+136 によるメモリ リーク
CSCvm87315	RegistrationTR::addToLamplighter の TID が原因で FTD 登録が失敗する可能性がある
CSCvm88004	ASA 上の SSH サービスが入力された文字や貼り付けられた各文字を自身のパケットにエコー バックする
CSCvn05797	Cisco Firepower Management Center のクロスサイト スクリプティングの脆弱性
CSCvn06618	LINA 設定のロールバックではスタートアップ コンフィギュレーションがデフォルトの実行とマージされる
CSCvn09322	FTD デバイスがアクティブ状態になった後に 5 分以内にリブートされる
CSCvn09367	管理者が ASA 5500-X に CXSC モジュールを取り付けられないようにする
CSCvn15757	NULL チェックなしの SCTP トラフィック インスペクションにより ASA がトレースバックすることがある
CSCvn16489	AMP 動的分析のクラウドを送信レートに対して個別に追跡する必要がある
CSCvn19823	ASA：失敗した SSL 接続が削除されず、DMA メモリが枯渇する
CSCvn20411	エラー メッセージの後、[Device Management] ページがロードされず、タイムアウトする
CSCvn21899	Firepower：SFTunnel 通信のために TLS 1.0 を永続的に無効にする

不具合 ID	タイトル
CSCvn23224	設定済みの SNMP で FTD-HA の形成に失敗する
CSCvn23254	Nameif がインターフェイスで設定されている場合に SNMPv2 が空の ifHCInOctets 値をプルする
CSCvn23701	ftp_telnet.conf(4) => Invalid keyword 'memcap' for 'global' configuration により展開に失敗する
CSCvn24756	セキュリティ インテリジェンス機能によって IP アドレスが誤ってブロック（URL ブロック）される可能性がある
CSCvn30118	mysql-server.err ファイルが完全に削除されず、Firepower のディスク容量を消費し続ける
CSCvn32657	call-home で使用したインターフェイス設定を削除すると ASA がトレースバックする
CSCvn33943	HA 設定の同期を使用した wccp_int_statechange() でのスタンバイ ノードのトレースバック
CSCvn36393	stunnel 設定ファイルで tls1.0 および tls1.1 を除外する
CSCvn37829	プライマリ DMA プールが枯渇すると、ASA は GCM（SSL）接続を許可して DMA_ALT1 を使用する必要がある
CSCvn38010	remove_peers.pl スクリプトが FTD で実行されている場合、このスクリプトを終了する
CSCvn43798	ドメインを削除しても、レルムがそのドメイン内にある場合、一部のオブジェクトの削除に失敗する
CSCvn44201	IOS XE 16.5.1 以降で実行されているネイバーから送信された LLS TLV を持つ OSPF hello パケットが ASA によって破棄される
CSCvn46474	FP2120 FTD が停電後に応答しなくなった
CSCvn47599	RA VPN + SAML 認証により RADIUS サーバに対して 2 つの許可要求が発生する
CSCvn47800	ファイバの枯渇により ASA が新しい AnyConnect 接続の認証を停止する
CSCvn48790	ポリシーの適用中に SI タスクが実行されている場合、スレーブノードがクラスタから退出する
CSCvn49561	CA パスを使用するための FireAMP curl コールの更新
CSCvn53732	復号されていない SSL 接続を変更した場合、この接続を閉じる必要がある

不具合 ID	タイトル
CSCvn54347	fp2100/1000 KP/WM でのフェールオーバー スイッチオーバーまたはフェールオーバー解消における権限付与のリリース エラー
CSCvn56095	SSL 暗号化ハードウェア オフロードで選択的な ack が発生しない
CSCvn61662	CXSC モジュールが継続的にリロードされるために ASA 5500-X が crashinfo を書き込まずにリロードすることがある
CSCvn62787	フロー テーブル設定の更新中に devcmd 障害時における CRUZ への複数回の再試行をサポートする方法
CSCvn63549	Python pop3lib apop() メソッドの Denial of Service（DoS）脆弱性
CSCvn64418	Nokia 7705 ルータでの ISA3000 interop の問題
CSCvn65575	アクティブ認証が有効になっていて、SSL ポリシーが有効になっていない場合、Snort が終了する可能性がある
CSCvn68145	SSL 復号化を使用しているときに Snort が予期せず終了する
CSCvn69213	複数のスレッドが同じロックを待機しているために発生する ASA のトレースバックとリロード ：ウォッチドッグ
CSCvn76763	FTD の messages-X-SNAPSHOT.jar の 2 つのバージョンが展開の失敗を引き起こす
CSCvn77636	ASA/webvpn：FF および Chrome：文法ベースのパーサーでブックマークがレンダリングされない
CSCvn93499	Snort/データ コリレータは Firepower 4100/9300 デバイスで終了するときにクラッシュする可能性がある

バージョン 6.2.3.9 で解決済みの問題

（注） バージョン 6.2.3.9 はバージョン 6.2.3.8（2019 年 1 月 7 日にシスコサポートおよびダウンロードサイトから削除された）を置き換えます。「バージョン 6.2.3.8 で解決済みの問題（105 ページ）」に記載されている問題は、バージョン 6.2.3.9 でも修正されています。

表 *54* : バージョン *6.2.3.9* で解決済みの問題

不具合 ID	タイトル
CSCvn82378	FMC を 6.2.3.8 ～ 51 にアップグレードすると、ASA/FTD を経由するトラフィックの送受信が停止する場合がある

バージョン 6.2.3.8 で解決済みの問題

（注） バージョン 6.2.3.8 は 2019 年 1 月 7 日にシスコサポートおよびダウンロードサイトから削除されました。このバージョンは、バージョン 6.2.3.9 に置き換えられます。ここに記載されている問題は、バージョン 6.2.3.9 でも修正されています。

表 *55* : バージョン *6.2.3.8* で解決済みの問題

不具合 ID	タイトル
CSCuy90400	SSL で Extended Master Secret をサポートするための機能強化
CSCvd03903	Firepower は TCP ダンプの脆弱性の影響を受ける
CSCvd12834	成功および失敗した SSH 認証試行が FP 監査ログに記録されない
CSCve29930	HA ペアのセカンダリ FMC で LOM を設定できない
CSCvf20266	Firepower Management Center システム設定の電子メール通知のパスワードの長さが短すぎる
CSCvf57596	ポリシーの展開が失敗した後、ActionQueueScrape プロセスが終了しなかった
CSCvg10718	トラフィック プロファイルとの相関ポリシーが機能しない
CSCvg36254	FTD 診断インターフェイスが br1 管理サブネットの ARP をプロキシする
CSCvh13022	クライアント hello ペイロードが 6 バイト未満の場合、SSL 復号がバイパスされる
CSCvh14743	NAT 検出ペイロードを使用した DPD により Strongswan/サードパーティ製クライアントとの IKEv2 MOBIKE セッションが失敗する。
CSCvi82404	800_post/755_reapply_sensor_policy.pl でデバイスの更新に失敗する可能性がある
CSCvj67258	2 タプルおよび 4 タプルのハッシュ テーブルをロックレスに変更する
CSCvj97213	ASA IKEv2 キャプチャ タイプ isakmp が破損したパケットを保存しているか、またはパケットが欠落している
CSCvk20292	HA モードの FMC では、アクティブな FMC に障害が発生したときに、スタンバイ FMC からの正常性ポリシーが欠落する
CSCvk30775	ENH：「show tech」出力への「show fragment」の追加

不具合 ID	タイトル
CSCvk30779	ENH：「show tech」出力への「show ipv6 interface」の追加
CSCvk30783	ENH：「show tech」出力への「show aaa-server」の追加
CSCvk33923	FMC から管理対象の FTD デバイスを削除した後のディスク使用率が高い
CSCvk51181	インターフェイスの編集と展開後に FTD IPV6 トラフィックが停止する：パート 1/2
CSCvk62871	パッシブ モードの Firepower 2100 FTP クライアントがサーバとのデータ チャネルを確立できない
CSCvk72192	オーバーヘッドによるメモリ使用率が含まれているために「show memory」の「free memory」が正しく出力されない
CSCvm10968	CVE-2018-5391 不適切な IP フラグメント処理を通じたリモート Denial of Service（DoS）
CSCvm43975	SIP インスペクションの脆弱性による Cisco ASA および FTD のサービス拒否または高 CPU
CSCvm47713	Chrome ブラウザが使用されている場合、SSL ポリシーは *.lightning.force.com での PDF の表示を許可しない
CSCvm49283	オブジェクト グループの検索しきい値の作成がデフォルトで無効になっており、設定可能である。機能停止の原因となる。
CSCvm53531	Cisco 適応型セキュリティ アプライアンス ソフトウェアの特権昇格の脆弱性
CSCvm56371	同じ dACL が接続されているすべての AnyConnect クライアントの dACL を ASA が誤って削除する
CSCvm56719	スレッド名 vpnfol_thread_msg での高可用性スタンバイ ユニットのトレースバック
CSCvm60361	5500 の FTD で SSH 公開キー認証が機能しない
CSCvm62708	NPN ネゴシエーションの SSL 接続は、[Do Not Decrypt] SSL ポリシーに一致すると失敗する可能性がある
CSCvm64230	verify_firmwareRunning() 戻りコードがチェックされない
CSCvm65725	サーバの応答が大きすぎた場合に（ERR_RESPONSE_TOO_BIG）ASA Kerberos 認証で TCP への切り替えが失敗する
CSCvm67704	KRB_ERR_RESPONSE_TOO_BIG を処理するときのメモリ リーク（krb5_extract_ticket でのリーク）

不具合 ID	タイトル
CSCvm76760	FMC - 外部 RADIUS 認証 - [Shell Access Filter] フィールドのテキストが検証されない
CSCvm78449	log default コマンドでアクセス コントロール ライセンス エントリを変更できない
CSCvm80933	サーバがワイルドカードの共通名を持つ証明書を使用する場合、SSL ポリシーが誤ったルールと一致する可能性がある
CSCvm81052	無効な証明書チェーンが原因で、ローカル マルウェア検出の更新が FMC にダウンロードされない
CSCvm82966	Linux カーネル 3.10.107 の脆弱性
CSCvm91280	侵入イベント レポートの日付、時間、曜日が UTC で、時刻がローカル タイムゾーンになる
CSCvm95669	ASA 5506 における http://x.x.x.x/asasfr-5500x-boot-6.2.3-4.img コピー中のエラー（デバイスにスペースが残っていない）
CSCvn03507	次の展開でルートマップ設定から「set ip next-hop verify-availability」が削除される
CSCvn03966	FTD：「object-group-search」が flexconfig を介してプッシュされるとすべての ACL が削除されて機能停止が発生する
CSCvn08146	x509 証明書およびキーへの変更に関する監査の詳細が欠落している
CSCvn09640	FTD：パーサーからの ethertype ACL を信頼する機能が必要である。BPDU の通過を許可する必要がある
CSCvn09808	ソケットの権限エラーによりキャプティブ ポータルの bltd プロセスが起動時に失敗する
CSCvn11219	「Not a directory」というエラー メッセージが表示され、ポリシーの展開に失敗した
CSCvn31753	SSL インスペクション ポリシーによって SEC_ERROR_REUSED_ISSUER_AND_SERIAL ブラウザ エラーが発生する場合がある

バージョン 6.2.3.7 で解決済みの問題

表 *56* : バージョン *6.2.3.7* で解決済みの問題

不具合 ID	タイトル
CSCve34221	CC モードを有効にすると内部サーバ エラーが UI に表示される
CSCvf54682	sudo：CVE-2017-1000368：Sudo 解析された tty 情報の特権昇格の脆弱性
CSCvh14743	NAT 検出ペイロードを使用した DPD により Strongswan/サードパーティ製クライアントとの IKEv2 MOBIKE セッションが失敗する。
CSCvi97500	Firepower Management Center の AMP クラウド イベントが異なるファイル タイプで認識される
CSCvj14631	mgmt インターフェイスが eth0 でない場合、Appliance Information ウィジェットは無効な IPv4 アドレスを表示する
CSCvj58342	セキュリティ コンテキストの削除後にマルチキャストがドロップされる
CSCvj65064	Firepower 2100：ポートチャネルのダウン通知の遅延
CSCvj67258	2 タプルおよび 4 タプルのハッシュ テーブルをロックレスに変更する
CSCvj76858	ポリシーの展開に時間がかかる（最長で 4 時間）
CSCvj91795	URL カテゴリ ルックアップが保留中の場合、SSL デフォルト ポリシー アクションが実行される
CSCvj97213	ASA IKEv2 キャプチャ タイプ isakmp が破損したパケットを保存しているか、またはパケットが欠落している
CSCvj98662	linux ホットフィックス レイヤ ディレクトリの再編成
CSCvk18330	アクティブな FTP データ転送が FTP インスペクションと NAT で失敗する
CSCvk30779	ENH：`show tech` 出力への `show ipv6 interface` の追加
CSCvk31035	KVM（FTD）：外部からの Web サーバのマッピングが他のプラットフォームと一貫した動作をしない
CSCvk33023	クラスタまたはフェールオーバーの Firepower モジュールでのポリシー展開の失敗
CSCvk48389	アップグレードを試行したときの [`Error: Timed out communicating with DME`]
CSCvk56513	トラフィックがプロキシを通過するとき Tor がブロックされない

不具合 ID	タイトル
CSCvk59260	低速ネットワークでは、**リソースが一時的に使用できなくなる**例外により、展開に失敗する可能性がある
CSCvk66529	FPR 9300 の FTD で事前フィルタが有効になっている状態で TCP ヘッダーが破損する
CSCvk66771	CPU プロファイラがしきい値に達しないままサンプルを収集せずに実行を停止する
CSCvk72192	show memory の出力に誤ったメモリが表示される
CSCvk76146	41xx 上の一部のデバイスの /ngfw パーティションには 39 GB が表示され、その他のデバイスでは 100 GB が表示される
CSCvm03931	新しい CA 証明書が存在しないため、Firepower によるソフトウェア アップデートのダウンロードが失敗する
CSCvm04237	BusyBox `huft_build` 関数の Denial of Service（DoS）脆弱性
CSCvm05464	CVE-2018-5391 不適切な IP フラグメント処理を通じたリモート Denial of Service（DoS）
CSCvm08500	NAT ルールの説明（チェコ/スロバキア文字を含む）を削除すると ASA cmd の検証が失敗する
CSCvm09040	チケットと既知キーのアクションを使用したセッションの再開試行で完全なハンドシェイクが使用される
CSCvm19948	SNI を使用しない SSL 接続が誤った SSL ルールにヒットする可能性がある
CSCvm32256	スレーブ ユニットが無効状態になっている場合、FTD クラスタに参加できない
CSCvm32613	FMC 6.2.3.3 から 6.2.3.4 にアップグレードした後、syslog メッセージの形式が変更された
CSCvm43975	SIP インスペクションの脆弱性による Cisco ASA および FTD のサービス拒否または高 CPU
CSCvm47595	SSL ポリシーを使用していない場合、FMC は不正なアクセス コントロール ポリシーに一致する接続を表示する
CSCvm49283	オブジェクト グループの検索しきい値の作成がデフォルトで無効になっており、設定可能である。機能停止の原因となる。
CSCvm51395	メモリ制限のため、fwrulechecker でアクセス コントロール ポリシーの展開に失敗する

不具合 ID	タイトル
CSCvm56371	同じ dACL が接続されているすべての AnyConnect クライアントの dACL を ASA が誤って削除する
CSCvm56719	スレッド名 vpnfol_thread_msg での高可用性スタンバイ ユニットのトレースバック
CSCvm56851	ファイル イベントまたは FireAMP イベントを逆シリアル化するエラーの後、eStreamer が繰り返し終了する
CSCvm58672	SSL ハードウェア オフロード機能が有効になっているときに SSL ポリシーを展開できない
CSCvm60468	Linux カーネル yurex_read の特権昇格の脆弱性
CSCvm60548	セキュリティ インテリジェンスの同期タスクが失敗する
CSCvm60791	Linux カーネル alarm_timer_nsleep () 関数の整数オーバーフローの脆弱性
CSCvm64255	SFNotificationd の停止に失敗する
CSCvm65725	サーバの応答が大きすぎた場合に（ERR_RESPONSE_TOO_BIG）ASA Kerberos 認証で TCP への切り替えが失敗する
CSCvm67184	監査 Syslog メッセージがユーザ情報なしで送信される
CSCvm67316	ASA：CSCvm70848 の IKEv2/IPSec デバッグを追加
CSCvm67704	KRB_ERR_RESPONSE_TOO_BIG を処理するときのメモリ リーク（krb5_extract_ticket でのリーク）
CSCvm68467	イベント アラート プロセスの CPU 使用率により、ビジー状態の Firepower 2100 での展開が遅れる
CSCvm71378	NAT ルールが原因でポリシーの展開が失敗する
CSCvm78449	log default コマンドでアクセス コントロール ライセンス エントリを変更できない
CSCvm80874	ASAv/FP2100 スマート ライセンス：ライセンスを登録/更新できない
CSCvm82492	Snort プロセスでは、影響を与えるトラフィックの終了に時間がかかる
CSCvm82930	FTD：重複する NAT ステートメントが設定されている場合に SSH から ASA へのデータ インターフェイスが失敗する
CSCvm96634	ポリシー展開の最終段階は、現在のユーザではなく **admin** で監査ログに記録される

不具合 ID	タイトル
CSCvm96916	FMC が ASA に **strong-encryption-disable** をランダムに送信する

バージョン 6.2.3.6 で解決済みの問題

表 *57* : バージョン *6.2.3.6* で解決済みの問題

不具合 ID	タイトル
CSCux69220	DHCP での WebVPN 「enable intf」、ASA ブート時の CLI の欠落
CSCve95403	FIPS ブート テスト後に送信されたログが原因で ASA がブートループする
CSCvf85831	イメージのアップロード中に ASDM がエラーを表示する
CSCvh16414	ヘルス モニタリングが FTD の CPU を 100 % または 150 % として誤って表示する可能性がある
CSCvh69117	SFDataCorrelator ログ スパム「Received an unknown event type」
CSCvh98781	ASA/FTD 導入エラー「Management interface is not allowed as Data is in use by this instance」
CSCvi13054	「Attempted to store stale object」が表示され、スケジュールされたルール推奨更新が失敗する
CSCvi48170	ASA 9.4.4.8、SNMP により低速なメモリ リークが発生する
CSCvi71761	Firepower 9300 で FTD cli プロンプトがスタックしている
CSCvi77340	競合状態の結果、ユーザ id REST API が機能しない
CSCvi90633	ASDM AC のダウンロード時に GUI 言語を編集しても FPR-21XX の変更が無視される
CSCvi98909	RTP パケットが AC ポリシーのルールと一致しない
CSCvj42269	システム メモリが 101% と報告する syslog 321006 を ASA 9.8.2 が受信する
CSCvj44032	TCP 4 ウェイ ティアダウンの際に早期の Snort 接続が終了する
CSCvj47256	後続のフェールオーバーが 2 回実行されと ASA SIP セッションと Skinny セッションがドロップされる
CSCvj67776	clear crypto ipsec ikev2 のコマンドがスタンバイに複製されない
CSCvj72309	FTD が BGP のグレースフル リスタート後に End-of-RIB のマーカーを送信しない

不具合 ID	タイトル
CSCvk04592	ハーフクローズ状態の lina conn テーブルでフローがスタックする
CSCvk12076	AnyConnect クライアント プロファイルが接続プロファイルで割り当てられていない場合、グループ ポリシーの下に表示されない
CSCvk14768	スレッド名 DATAPATH-1-2325 での ASA のトレースバック
CSCvk23483	柔軟なタイムアウトが適用されず、600 秒のタイムアウトが適用される
CSCvk24297	Windows 10 バージョン 1803 の IKEv2 フラグメンテーション機能が有効になっているため EAP を使用した IKEv2 RA が失敗する
CSCvk34648	高スループットの LAN 間 VPN トラフィックによりデータ キー再生成で Firepower 2100 トンネルがフラップする
CSCvk36087	ASDM を介して ASA にログインすると syslog 611101 に 0.0.0.0 の IP がリモート IP として表示される
CSCvk36733	huasan 製スイッチで ASA の EtherChannel をアクティブ モードで設定すると MAC アドレスがフラッピングする
CSCvk38176	GTP インスペクションおよびフェールオーバーによるトレースバックとリロード
CSCvk42473	QoS ルールの評価でアプリケーションの変更時にフローが再評価されない
CSCvk43865	トレースバック：mutex ロック実行中の ASA 9.8.2.28
CSCvk52667	FDM：6.2.3 ～ 83 ビルドで最新の SRU に更新した後、展開が失敗する
CSCvk62896	SA の削除中に生じる ASA IKEv2 のクラッシュ
CSCvk66722	DHCP オプション「false」を設定すると、GUI に DHCP 設定が表示されなくなる
CSCvk67239	「Thread Name: Logger Page fault: Address not mapped」での ASA のトレースバックとリロード
CSCvk68772	クライアント証明書を有効にしてからアップグレードすると、FMC UI にアクセスできない
CSCvk68809	FMC を 5.4.0 からアップグレードする場合、ca-cert.pem ファイルのソフトリンクがない
CSCvk70676	ASA がメッセージ本文として HTTP を送信するとクライアントレス WebVPN が失敗する
CSCvk72652	アグレッシブ モードを無効にする場合、FMC が「crypto ikev1 am-disable」を展開しない

不具合 ID	タイトル
CSCvk74461	LDAP グループはダウンロードされるが、GUI で使用できない
CSCvk76160	FDM を使用して KP 6.2.2.2 で復元できない
CSCvk76547	TCP ハンドシェイク パケットの再送信時にフローが確立されている IPS ルールがブロックしない
CSCvm01396	プロキシ設定を使用しているブラウザに Firepower ブロック ページが表示されない
CSCvm05821	SRU の更新中に自動的に有効にされる機密データの検出
CSCvm07458	EEM を使用して VPN 接続イベントを追跡するとトレースバックとリロードが発生することがある
CSCvm07643	FTD 6.2：侵入イベントが送信元ポートと宛先ポートを表示しない
CSCvm09624	IPS ルールを適用するときに、AppID に基づいてプロトコルが更新されない
CSCvm11389	ごく一部の ECDHE 接続が失敗する
CSCvm11714	特殊文字「&」を使用する場合の EIGRP 認証キーの問題
CSCvm15880	FPR 9k ASA クラスタのマルチコンテキスト モード/vpn モードの配信が原因で設定がトランスペアレント モードの場合にリブート ループが生じる
CSCvm19585	6.2.3.5 へのアップグレード後にスマート ライセンスが登録解除される
CSCvm23370	ASA：PC cssls_get_crypto_ctxt によるメモリ リーク
CSCvm25972	ASA トレースバック：スレッド名 NIC Status Poll
CSCvm26004	ASA での AAB の計算が正しくないと、ランダムな AAB 呼び出しが発生する
CSCvm29973	DNS SI イベントの誤検出
CSCvm44905	SSL インスペクションがフロー情報なしでフローの処理を続行する場合がある
CSCvm56019	Cisco 適応型セキュリティ アプライアンスの WebVPN：VPN がブラウザを介して接続しない

バージョン 6.2.3.5 で解決済みの問題

表 *58* : バージョン *6.2.3.5* で解決済みの問題

不具合 ID	タイトル
CSCvb19750	Cisco Firepower Management Center のクロスサイト リクエスト偽造の脆弱性
CSCve39071	ThreatGRID クラウドへの接続試行を無効にするオプション
CSCve85565	syslog が VPN トンネルを介して送信されるとトレースバックする
CSCvg33300	整数ホスト属性を作成した後、変更できない
CSCvg51412	管理対象デバイスと estreamer クライアント間で estreamer sftunnel を確立できない
CSCvg54724	Firepower 動的分析アソシエーションが US アドレスのみにリダイレクトされる
CSCvg75144	フィルタと一致するすべてのアプリケーションがすべてのオブジェクトを削除する
CSCvg91631	URL レピュテーションに Encore の高リスクまたは不明が表示される
CSCvg94363	Firepower Threat Defense でプレフィックス リスト「le 32」が機能しない
CSCvh21219	次の展開で PBR 設定から「set ip next-hop verify-availability」が削除される
CSCvh89017	configure user add コマンドが数値ユーザを受け入れない
CSCvi01312	WebVPN：Confluence アプリケーションと Jira アプリケーションでの複数のレンダリングの問題
CSCvi31540	ペイロード暗号化なし（NPE）の ASA での「show tech」を使用したトレースバックとリロード
CSCvi34164	ASA が TCP/UDP syslog に 104001 メッセージおよび 104002 メッセージを送信しない
CSCvi37644	PKI：ASA が「Add CA req to pool failed. Pool full.」というエラーで CRL の処理に失敗する
CSCvi45989	ASDM で管理される ASA によって [Query Cisco CSI for Unknown URLs] オプションがリセットされる（回帰）
CSCvi51370	競合状態のために、ルール メッセージなしで syslog アラートが発生する可能性がある

不具合 ID	タイトル
CSCvi53708	CLI と REST-API の間の ASA NAT の位置の不一致が原因で REST が誤った設定を削除する
CSCvi69343	通信のリセット時に ids_event_processor がメモリをリークする
CSCvi69356	SFDataCorrelator が「Invalid column value name」エラーをレポートし、管理対象デバイスで eStreamer が機能しない
CSCvi76808	[Decrypt - Known Key] SSL ルール アクションによる、暗号化された SMTP TLS のファイルの検出に失敗する
CSCvi79691	LDAP over SSL 暗号化エンジン エラー
CSCvi79999	VTI 使用時の ARP トラフィックにより 256 バイトのブロック リークが確認される
CSCvi85382	ASA-IC-6GE-SFP-A モジュールが取り付けられている場合の ASA5515 の DMA のメモリ不足
CSCvi93500	複数のプロキシがある場合、snort による x-forward-for-like ヘッダーの処理が正しくない
CSCvi94239	IDSEventAlerter ログ スパム「Unable to get SSL certificatefingerprint」
CSCvi96442	スレーブ ユニットが S2S の UDP/500 および IPSec パケットをマスターにリダイレクトせずにドロップする
CSCvi97894	キャプチャ トラフィックの実行時にいくつかのハードウェア ルールが切り捨てられる
CSCvi98424	ファイル読み取りエラーの後、IDSEventAlerter と IDSEventProcessor が機能を停止し、スパムがログに記録される
CSCvi99743	Telnet アクセスを使用して「failover active」を実行した後に生じるスレッド「Logger」でのスタンバイ トレースバック
CSCvj07038	Firepower デバイスは Threat Grid 証明書を信頼する必要がある
CSCvj11442	Firepower Threat Defense：ネイバーの展開操作の BGP 順序が原因で障害が発生する
CSCvj19835	アプリケーション データ フェーズで ECDHE-RSA-RC4-SHA 暗号を使用した復号化された接続が失敗する
CSCvj38002	SNMPv3 ユーザ engineID がアクティブな engineID と一致しないため、SNMP 要求で「user not found」エラーが発生する
CSCvj44517	SSL ポリシーの複製における信頼できる CA のリスト

不具合 ID	タイトル
CSCvj49452	脆弱な SSL/TLS バージョンと暗号を使用した sftunnel
CSCvj54840	コンテキスト ストレス テストの作成/削除により nameif_install_arp_punt_service でトレースバックが発生する
CSCvj65581	2100 シリーズ アプライアンスでの ftdrpcd プロセスからの過剰なロギング
CSCvj67504	SSL ポリシーにユーザまたはグループを追加するときにポリシーの展開が失敗する
CSCvj67740	スタティック IPv6 ルート プレフィックスが ASA 設定から削除される
CSCvj75793	2100/4100/9300：Management Center からキャプチャを停止/一時停止しても CPU 使用率が低下しない
CSCvj85516	Firepower Threat Defense で「management」という名前のインターフェイスのパケット キャプチャが失敗する
CSCvj88514	IP ローカル プールが同じ名前で設定されている
CSCvj91449	各リブート後に IPv6 に対して logging host コマンドが有効になっている場合の ASA のトレースバック
CSCvj92040	TLS クライアントにより、CC で許可されていない、CC モードの CipherSuite がいくつか提供される
CSCvj95451	webvpn-l7-rewriter：IE でブックマークのログアウトが失敗する
CSCvj96173	6.2.3 にアップグレードした後、FMC が eStreamer クライアントの sha1 証明書を引き続き生成する
CSCvj97326	Firepower サービスで SSL ポリシーを作成できない
CSCvj98964	SCTP トラフィックにより ASA がトレースバックすることがある
CSCvk01577	FTD 6.2.3 の CLISH モードからのピグテールが許可されない
CSCvk01981	ユーザの消去後にユーザが不明と表示される
CSCvk06249	si_uuid が firewall_rule_cache にない場合、SFDataCorrelator アラートがデッドロック再起動を引き起こす可能性がある
CSCvk06336	FMC が不正なアクセス コントロール ポリシー ルールに一致する接続を表示し、パケット カウントがゼロになる
CSCvk06368	FMC カーネルの脆弱性の評価
CSCvk08377	9.8.2.20 を実行している ASA 5525 でメモリが枯渇する。

不具合 ID	タイトル
CSCvk10252	SI カテゴリがアラートまたは eStreamer に対して正しくない可能性があり、パフォーマンスとメモリの問題もある
CSCvk11898	v2 ハンドオフの処理中に GTP ソフト トレースバックが確認される
CSCvk14910	エージェント uuid なしで FireAMP イベントを処理すると、SFDataCorrelator が終了したままになる
CSCvk16568	アプリケーション ID が検出された場合、AppID がトラフィックの処理を停止する
CSCvk17382	ルールの評価の処理中に Snort が予期せず終了する
CSCvk18378	show process（rip：inet_ntop6）実行時の ASA のトレースバックとリロード
CSCvk18578	ASA SSLVPN ログイン ページのカスタマイズをロードするために必要な圧縮の有効化
CSCvk18846	sfdccsm のロギング レベルのために Firepower Management Center WebUI のパフォーマンスが低下する
CSCvk19435	GTP APN 制限の解析時に不要な IE が存在するエラー
CSCvk26887	無効なコンテンツ エンコーディングによりローカル CA からの証明書のインポートが失敗する
CSCvk27686	ASDM/Telnet/SSHを介して QoS メトリックにアクセスするときに ASA のトレースバックとリロードが発生することがある
CSCvk28023	WebVPN：文法ベースのパーサーがメタタグを処理できない
CSCvk30212	ネイバー IPv6 アドレスが先行する 0 をグループに含んでいる場合、FMC は BGPv6 コマンドを否定する
CSCvk30665	ASA の「snmp-server enable traps memory-threshold」で CPU が占有され、「no buffer」でドロップする
CSCvk33947	センシティブ データのしきい値設定が正しくない
CSCvk35323	オーバーライドが設定されているオブジェクトでは、設定のコピーが行われなかった
CSCvk35761	1 つのセッションで複数のパターンを処理する場合、センシティブ データが想定どおりに動作しない
CSCvk37890	Firepower 2110、webvpn の条件付きデバッグが原因で Threat Defense がトレースバックする
CSCvk40332	ゾーン情報のない UDP トラフィックが誤った AC ルールと一致する

不具合 ID	タイトル
CSCvk49527	switchprimarynode API コールのアプリケーション レベル タイムアウトを追加する
CSCvk50364	インラインセットに対して NGIPSV「system support capture-traffic」が機能しない
CSCvk50732	MAC で Safari 11.1.x ブラウザを使用した AnyConnect 4.6 の Web 展開が失敗する
CSCvk52305	DAQ の segfault で Snort プロセスが終了した
CSCvk54078	VPN 設定を使用した Firepower Threat Defense のハイ アベイラビリティの作成に失敗する
CSCvk54491	競合状態処理の評価により Snort プロセスが終了する
CSCvk54779	フラグメント化したパケットに関する非同期キューの問題によりブロックが枯渇する：9344
CSCvk55355	同じ共通名を持つ 2 つのグループに少なくとも 1 人のユーザが属しているため、ユーザ/グループのダウンロードが失敗する
CSCvk57516	Firepower Threat Defense：暗号マップが正しくないために DMA メモリが不足して VPN 障害が発生する
CSCvk58188	max_sessions に指定された値が範囲外であるため Snort 設定の検証に失敗した
CSCvk66012	FMC でクラスタのメンバーがシャットダウン/無効化されている場合、ポリシーの展開が失敗する
CSCvk71511	イベント ストレージが大きく、デバイス数が多い場合、SFDataCorrelator イベントのバックログが増加する
CSCvk72602	誤った TCP チェックサムが snort の再試行を引き起こす
CSCvk73990	変更調整レポート：ルール削除イベントをシンプルにする
CSCvm01497	別のドメインのレポートテンプレートを使用すると、スケジュールされたレポートが正しいドメインに保存されない
CSCvm06114	RDP ブックマーク プラグインが起動しない
CSCvm16686	冗長インターフェイスを使用したハイ アベイラビリティの作成中に Threat Defense のインターフェイスがダウンする

バージョン 6.2.3.4 で解決済みの問題

表 *59* : バージョン *6.2.3.4* で解決済みの問題

不具合 ID	タイトル
CSCuy01269	`rna_client_app_map` の最後のエントリが重複している場合、SFDataCorrelator が失敗する
CSCvd28906	十分な LCMB メモリを割り当てることができないため、5506 での最初のブート時に ASA がトレースバックする
CSCvd92210	IPV6 アドレスが syslog で受け入れられない
CSCvf61852	Threat Intelligence Director（TID）の起動によって遅延が発生し、Tomcat の起動が停止する
CSCvg28901	Firepower Management Center に証明書をインポートするときに証明書メッセージをインストールできない
CSCvg96103	ブロック応答の非常に大きな HTML ページを含めると、復号化されたすべてのサイトでロードが失敗する
CSCvh25088	MySQL テーブル `secondary_login` が無制限に増大する
CSCvh91483	URL フィルタリング ライセンスが期限切れになるか、削除されると、CloudAgent が 1 分ごとに再起動する
CSCvi03103	BGP ASN によってポリシーの展開が失敗する
CSCvi30280	`UserIdentity [ERROR] UserLoginInfo` メッセージの処理中のエラー：`[1] Invalid Argument`
CSCvi34210	Snort が、トランスペアレント Threat Defense の異なる BVI に対する U ターン トラフィックの同じ接続に一致する
CSCvi44713	**show memory binsize** および **show memory top-usage** で正しい情報が表示されない（すべてが PC 0x0 を表示する）
CSCvi45807	ASA：再起動後に dns **expire-entry-timer** 設定が表示されなくなる
CSCvi59968	Firepower 2100 での SNMP Get 要求に対する不適切な応答 `1.3.6.1.2.1.1.2.0`
CSCvi65512	FTD：システムの負荷が比較的低い状態で AAB が snort を強制的に再起動することがある
CSCvi97729	フェールオーバーが「新規アクティブ」に移行しているときに to-the-box トラフィックがデータ インターフェイスの外にルーティングされる

不具合 ID	タイトル
CSCvj15572	インターフェイスの MAC アドレスの変更時にフローオフロードのリライト ルールが更新されない
CSCvj25386	デフォルトのアイデンティティ レルム EOs が欠落しているためアップグレードに失敗する
CSCvj44531	ファントム SSL オブジェクトとセンサーへの空の展開
CSCvj49502	下位のデバッグ レベルでクライアントの hello 送信情報が必要
CSCvj74210	`show service-policy inspect gtp pdp-context detail` 実行時の **SSH** でのトレースバック
CSCvj75655	外部データベースが Firepower Management Center からの接続イベントをクエリできない
CSCvj76748	`cloud-sa.amp.sourcefire.com` から `cloud-sa.amp.cisco.com` に移行する必要がある
CSCvj79729	（2/2）SFDataCorrelator（センサー上）の `user_id/user_group` ブロードキャストの高メモリ使用率
CSCvj91418	appid が NetBIOS トラフィックを処理するときに Snort が大量のメモリを使用する
CSCvj91965	Firepower Management Center の変更調整レポートで特定のフィールドに空白がある
CSCvj93913	SSL インスペクション TLS 1.3 のダウングレードでは、クライアント/サーバのランダム値を RFC 準拠に変更する必要がある
CSCvj94024	Firepower デバイスが完全なリカバリに入ると、ネットワーク カードから定期的にビジーが返される
CSCvk02250	**show memory binsize** および **show memory top-usage** で正しい情報が表示されない（修正完了）
CSCvk06160	OS 脆弱性マップの初期化中に SFDC が繰り返し終了する
CSCvk06176	不正な実行ファイルのため SSEConnector が起動しない
CSCvk06677	HTTPS セッションが HW SSL でロードされずにタイムアウトする場合がある
CSCvk12841	Internet Explorer または Edge を使用しているときに SSL ページがロードされない

不具合 ID	タイトル
CSCvk17163	6.2.2 Firepower Threat Defense デバイスにハイ アベイラビリティの中断を強制すると、エラーが発生して展開が失敗する
CSCvk17813	ペア環境でデバイスの実行コンフィギュレーションを取得できなかったため、ポリシーの展開が失敗する可能性がある
CSCvk19750	多数のローカル ルールがある .sfo ファイルのインポートに 170 時間以上かかる
CSCvk21405	シェル アプリケーションがサーバから新しい接続のピンホールを開かない
CSCvk25729	大きな ACL のブート時のコンパイルに時間がかかり機能停止が生じる
CSCvk27787	Management Center のペア： Manage_procs.pl により管理対象デバイス上の cluster.conf ファイルが破損する
CSCvk30228	ASAv や FTDv の展開が Microsoft Azure で失敗したりコンソールの応答が遅くなったりする
CSCvk30778	レイヤ 3 および 4 のクライアント hello ダイジェストが 2 回処理され、メモリ リークが発生する
CSCvk30865	破損したレコードであるとレポートされたネゴシエーション済みのバージョンとは異なる TLS バージョンの SSL アラート
CSCvk32718	多くのファイル イベントを含むファイル マルウェア攻撃中にイベント処理が遅くなる
CSCvk45443	ASA クラスタ：NAT と高トラフィックによる CCL でのトラフィック ループ
CSCvk59795	OpenLDAP レルム/サーバを使用したリモート アクセス VPN で正しいネーミング属性が使用されない

バージョン 6.2.3.3 で解決済みの問題

表 *60* : バージョン *6.2.3.3* で解決済みの問題

不具合 ID	タイトル
CSCuz96856	キャッシュの不一致によりブロックされたセッションの新しいクライアント hello フラグ
CSCvd13180	AVT：ASA 9.5.2 の Content-Security-Policy ヘッダーの欠落
CSCvd76939	ASA ポリシーマップ設定がクラスタのスレーブに複製されない

不具合 ID	タイトル
CSCve17484	Firepower Threat Defense でインテリジェント アプリケーション バイパスのドロップ率が機能しない
CSCve53415	キャプチャ実行中に DATAPATH スレッドで ASA がトレースバックする
CSCvg42033	vms.db の eoattributes テーブル内の未使用データをクリーンアップしてバックアップ ファイルのサイズを削減するためにプルーニングを使用する
CSCvg76652	ポートチャネルのサブ インターフェイス不一致のデフォルト DLY 値
CSCvg90365	トランスペアレント ASA で IPv6 アドレスにより ICMP/Telnet トラフィックが失敗する
CSCvh53276	L2FW を通過する IPv6 プロトコルの 112 個のパケットが無効な IP 長メッセージでドロップされている
CSCvh55035	Firepower Threat Defense デバイスが Nexus 9000 を使用して ERSPAN を確立できない
CSCvh55340	REST API の完全バックアップを介して設定を実行している ASA に指定されたコンテキスト設定が含まれていない
CSCvh71738	アクセスグループ設定の削除後に FQDN オブジェクトが解決される
CSCvh75060	REST-API が特定のクエリに対して空の応答を返す
CSCvh83849	デュアル ISP とバックアップ IPSEC トンネルを使用した DHCP リレーによりフラップが発生する
CSCvh95960	capture コマンドで **match** キーワードを使用すると、キャプチャで IPv6 トラフィックが無視される
CSCvi07974	レイヤ 2 トラフィックはインスペクションのために Snort に送信するようにハードコーディングされてはならない
CSCvi15830	アイデンティティ ポリシーでネットワーク グループ オブジェクトが使用されている場合の Threat Defense デバイスの誤った設定
CSCvi16024	サーバの IP アドレスが変更されるとセッションが再開する場合の SSL エラー
CSCvi19220	IPv6 から IPv4 への NAT 変換の実行後に ASA が暗号化に失敗する
CSCvi36434	Cisco Firepower Threat Defense ソフトウェアの SSL Denial of Service（DoS）脆弱性
CSCvi37374	単一のインライン セットを複数回通過すると SSL 接続の完了に失敗する

不具合 ID	タイトル
CSCvi38151	ASA ペア：IPv6 スタティック/接続済みルートがアクティブ/スタンバイ ペア間で同期/複製されない
CSCvi42008	stuck uauth エントリが AnyConnect ユーザ接続を拒否する
CSCvi51515	REST-API：`500 Internal Server Error`
CSCvi53420	同じユーザが複数のグループの一部で、その共通名にコンマ（,）が含まれている場合、ユーザ/グループのダウンロードが失敗する
CSCvi58032	Management Center の内部エラーにより、ポリシー展開の失敗を引き起こす自動 NAT ルールが作成される
CSCvi58183	Firepower Management Center でのカスタム SI フィードの更新が管理対象デバイスに伝搬されない
CSCvi59000	SecGW：ASR 中のデータ損失
CSCvi59148	セッションが同じ IP アドレスから確立されているが、レルムが異なる場合、セッションは管理対象デバイスでアクティブなままになる可能性がある
CSCvi62671	多くのユーザ/グループ マッピングがある場合、6.2.2.1 でユーザ/グループをダウンロードするのに時間がかかる
CSCvi63968	「`Internal Error is preventing Policy Validation`」のため、アクセス コントロール ポリシーを保存できない
CSCvi70606	ASA 9.6(4)：WebVPN ページが正しくロードされていない
CSCvi73414	ユーザ情報が mysql と sybase 間で一致しない場合、ユーザ侵害の兆候を削除できない
CSCvi80928	HW モード：再開されたセッションが復号されない場合、SSL エラーが発生する可能性がある
CSCvi89194	pki ハンドル：増加し、減少しない
CSCvi97479	アクセス コントロール ポリシーの変更を展開する際に Snort が再起動する
CSCvi97721	合計メモリが 4 GB のデバイスでセキュリティ インテリジェンス URL フィード向けのメモリ容量を増やす必要がある
CSCvi98251	SMTP：SMTP mempool を割り当てられなかったため、ポリシーの適用に失敗し、Snort が停止した
CSCvj00918	（1/2）SFDataCorrelator（センサー上）の `user_id/user_group` ブロードキャストの高メモリ使用率

不具合 ID	タイトル
CSCvj06418	カスタム SI DNS フィードがセカンダリ Firepower Management Center に同期されない
CSCvj09571	クラシック ライセンスを使用して多数のデバイスを管理する場合の Firepower Management Center UI の遅延
CSCvj10011	Management Center：IGMP が設定されているが有効になっていないインターフェイスで、IGMP が有効になる
CSCvj17609	ファイルが空の場合、アクション キュー内のエントリで同期に失敗する（ファイルを開くことができない）
CSCvj22491	クラスタ：インターフェイスのダウンからアップへのシナリオにおける ifc monitor debounce-time の拡張
CSCvj24036	RAVPN が必要とするポートを通知する Firepower Management Center UI でのメッセージング
CSCvj25386	デフォルトのアイデンティティ レルム EOs が欠落しているためアップグレードに失敗する
CSCvj25817	ASA は MOBIKE に応答するが、DPD が原因で SA をクリアする。
CSCvj26819	`ssl_debug` 設定を変更するには、検出エンジンを再起動する必要がある
CSCvj32264	ASA：zonelabs-integrity：`Process Integrity FW task` によるトレースバックと高 CPU
CSCvj33202	Firepower の推奨事項と共有ポリシー レイヤを使用して侵入ポリシーを保存できない
CSCvj37448	ASA：リロード後にデバイスが SSL サーバ証明書パケットで ID 証明書のみを送信する
CSCvj37858	`action_queue` クエリに起因するパフォーマンスへの影響
CSCvj37924	CWE-20：不適切な入力検証
CSCvj39858	トレースバック：スレッド名：IPsec message handler
CSCvj42450	スレッド名 DATAPATH-14-17303 での ASA のトレースバック
CSCvj40636	従来の集中型 VPN クラスタリング向けの Firepower Threat Defense クラスタの S2S VPN サポート
CSCvj42680	Firepower Management Center ペアでデバイス登録クエリが頻繁に発生するため、速度が遅くなる
CSCvj44262	portal-access-rule が **deny** から **permit** に変更される

不具合 ID	タイトル
CSCvj45594	低速の Firepower Management Center で古いホスト情報をタイムアウトするときの SFDataCorrelator コア
CSCvj46777	Firepower Threat Defense 2100 ASA の原因不明のトレースバック
CSCvj48168	`show memory` コマンドが返す使用中のメモリ量が少ない
CSCvj48340	ASA のメモリ リーク：snp_svc_insert_dtls_session
CSCvj48931	Firepower 推奨アップデート タスクが実行されない
CSCvj49883	Firepower Threat Defense での ASA のトレースバック 2130-ASA-K9
CSCvj50024	ASA portchannel lacp max-bundle 1 hot-sby ポートがリンク障害後にアップ状態にならない
CSCvj56008	ScanSafe 機能が HTTPS トラフィックに対してまったく機能しない
CSCvj56909	ASA モジュールによって生成される SACK パケットの SLE 値と SRE 値を ASA が非ランダム化しない
CSCvj56963	5 番目のルートを追加する際の、8 つの等価コスト ルートのみが許可されることに関する Management Center エラー
CSCvj61367	送信元ポートがすぐに再利用されると、sslインスペクションが中断する可能性がある
CSCvj67132	bgp ネイバー CLI の順序が間違っているため、ポリシーの展開が失敗する
CSCvj73581	`cli_xml_server` スレッドでのトレースバック
CSCvj74210	`show service-policy inspect gtp pdp-context detail` 実行時の **SSH** でのトレースバック
CSCvj79765	アクティブ ASA での NetFlow 設定がスタンバイ ユニットで逆順に複製される
CSCvj81287	EKU の無効な目的が原因で、Firepower Threat Defens が syslog サーバの TLS-X509 証明書を拒否する
CSCvj83316	XFF データのクリア中に Snort プロセスが終了する
CSCvj91619	1550 ブロックの枯渇による ASA のリロード
CSCvj97157	JS ファイルでのクライアント リライターの問題により Web ページがロードされない
CSCvk00579	[Deploy] タブにデバイス リストが入力されるのが遅い

不具合 ID	タイトル
CSCvk06176	不正な実行ファイルのため SSEConnector が起動しない
CSCvk07522	webvpn：Firefox と Chrome でブックマークのレンダリングが失敗する。IE では問題なし

バージョン 6.2.3.2 で解決済みの問題

表 *61* : バージョン *6.2.3.2* で解決済みの問題

不具合 ID	タイトル
CSCuv68725	ASA が **log disable** オプションを使用して ACE を削除できない
CSCvd13182	AVT：ASA 9.5.2 での X-Content-Type-Options の欠落
CSCvd44525	ASA **show tech** の一部のコマンドが 2 回実行され、running-config/ak47 detailed/startup-config エラーが表示される
CSCve94917	CSCvb29688 に対する修正にもかかわらず、9.1 コードで古い VPN コンテキストに関する問題が確認された
CSCvf18160	WebVPNと共有 storage-url config でのフェールオーバー同期時の ASA のトレースバック
CSCvf39539	送受信したバイト数と IP アドレス スイッチに NetFlow が大きな値を返す
CSCvf40179	エラー：暗号マップを作成できない：エントリを追加するときに上限に到達する
CSCvf82832	ASA：962 へのアップグレード後の ICMPv6 syslog メッセージ
CSCvf96773	PAT プールの範囲が非常に大きいことによるスタンバイ ASA の 高い CPU 使用率
CSCvg05442	DATAPATH プロセスと WebVPN プロセス間でのデッドロックによる ASA のトレースバック
CSCvg43389	1550 ブロックの枯渇による ASA のトレースバック
CSCvg72879	9.9.1/SecGW：Firepower 4100 の 1 秒未満のフェールオーバーにより、10 ～ 20 % のパケット損失が数分間発生する場合がある
CSCvh14743	NAT 検出ペイロードを使用した DPD により Strongswan/サードパーティ製クライアントとの IKEv2 MOBIKE セッションが失敗する。
CSCvh23531	ソフトウェア DHE で ASA TLS クライアントの接続が失敗する

不具合 ID	タイトル
CSCvh30261	コンテキスト変更/設定の同期時に ASA のウォッチドッグがトレースバックする
CSCvh47057	ASA：インスペクションが有効になっているときにゾーン内に設定されたインターフェイスで ICMP フローが `no-adjacency` によりドロップする
CSCvh65500	FTP アクティブ モードの Firepower 2100 クライアントがサーバとのコントロール チャネルを確立できない
CSCvh81142	6.2.3 の実行中に生成された Snort コア
CSCvh83934	SNORT の User-ID コンポーネントのメモリ使用率が、10 M の予約済み制限を超えている
CSCvh91053	DHCP 送信中の ASA が DHCP を介して AC クライアントへのアドレスの割り当てを拒否するか、または割り当てない
CSCvh91399	ASA5500 シリーズのファイアウォールのアップグレードによりブートループが発生する（ROMMON を通過できない）
CSCvh92381	9.6.3.1 上で ASA がトレースバックし、ブート ループの状態になる
CSCvi01376	デフォルト以外の SSL コマンドがリブート時に Firepower 4100 から削除される
CSCvi07636	ASA：スレッド名 UserFromCert でのトレースバック
CSCvi08450	ASA での CWS リダイレクションが特定の状況で SSL Client Hello の再送信を適切に処理しない
CSCvi09305	**Do-Not-Decrypt** SSL ポリシー アクションで一部の SSL 接続が低速になるか、失敗する
CSCvi16264	DATAPATH がコンパイル中の ACL 構造体にアクセスするとウォッチドッグのタイムアウトにより ASA がトレースバックし、リロードする
CSCvi19263	VPN コンテキストのスピン ロックの解放中に ASA 9.7.1.15 がトレースバックする
CSCvi22507	IKEv1 RRI：応答専用のリバース ルートがフェーズ 1 のキー再生成中に削除される
CSCvi23615	Sourcefire.agent_messages テーブルが大きくなり、エージェント メッセージが消費されなくなる
CSCvi33962	WebVPN リライター：BMC Remedy でドロップダウン メニューが機能しない

不具合 ID	タイトル
CSCvi35805	ASA カットスルー プロキシでユーザは Web サイトにアクセスできるが「authentication failed」が表示される
CSCvi42965	ASA が show memory 出力の下に正確な空きメモリを報告しない
CSCvi45567	snmpv1&2c ホスト グループが設定されていると snmpwalk を実行できない
CSCvi47847	シェル アプリケーションがデータ転送用の新しい tcp ポートのピンホールを適切に開かない
CSCvi48523	[static route] ページから SLA モニタを作成できない
CSCvi49383	Azure：クラウド ハイ アベイラビリティを実行している ASAv がウォッチドッグ クラッシュ ループになる
CSCvi55070	IKEv1 RRI：発信専用のリバース ルートがフェーズ 1 のキー再生成中に削除される
CSCvi57808	sfdatacorrelator プロセスが継続的に予期せず終了する
CSCvi58089	webvpn でのメモリ リーク
CSCvi58865	復号を指定する URL カテゴリ ルールがある SSL ポリシーによってブラウザ エラーが発生する可能性がある
CSCvi63864	ハードウェア モードの SSL インスペクションとマルウェア防御で、安全なファイル転送が失敗することがある
CSCvi63888	再開されたセッションが復号されない場合、SSL エラーが発生する可能性がある
CSCvi64007	フェールオーバー後のゼロ化 RSA キーにより REST API がシステム コンテキストへの変更に失敗する
CSCvi66905	PIM 自動 RP パケットがクラスタ マスターのスイッチオーバー後にドロップされる
CSCvi70680	異なる AD の同じグループがダウンロードされない
CSCvi71039	Firepower Management Center：変更調整レポートが断続的に失敗する
CSCvi76577	ASA：netsnmp:Snmpwalk がホストグループの一部の IP グループで失敗する。
CSCvi77352	デバイスがそれ自体をクラスタから削除すると不正な更新が実行される
CSCvi82779	ASA が DATAPATH スレッドでトレースバックを生成する
CSCvi84315	Firepower 2100 シリーズ デバイスでの予期しないエラー

不具合 ID	タイトル
CSCvi86799	多数のインターフェイスと QoS により `show service-policy` の出力時に ASA がトレースバックする
CSCvi87921	FIPS モードの TLS では、ASA 自己署名 RSA 証明書が許可されない
CSCvi95544	ASA が **any** キーワードが設定されている ACL で IPv6 トラフィックを正しく照合しない
CSCvj05140	関連付けられたネットワーク オブジェクトでオブジェクトの説明が展開されない
CSCvj07038	Firepower デバイスは Threat Grid 証明書を信頼する必要がある
CSCvj07571	一部の相関ポリシー ルールを保存するときの `Error 500`
CSCvj07843	eStreamer による CPU 使用率が 100 % の場合 、ファイル/FireAMP イベントが有効化されているとイベント処理が遅くなる
CSCvj22491	クラスタ：インターフェイスのダウンからアップへのシナリオにおける ifc monitor debounce-time の拡張
CSCvj26450	ASA PKI OCSP 障害：CRYPTO_PKI：OCSP 応答データの復号化に失敗した
CSCvj47633	非 SSL トラフィックが原因で SSL インスペクションが失敗する
CSCvj56008	ScanSafe 機能が HTTPS トラフィックに対してまったく機能しない
CSCvj63196	Sybase の問題の回避策：snort エンジンの更新後、ポリシーの展開が突然失敗する

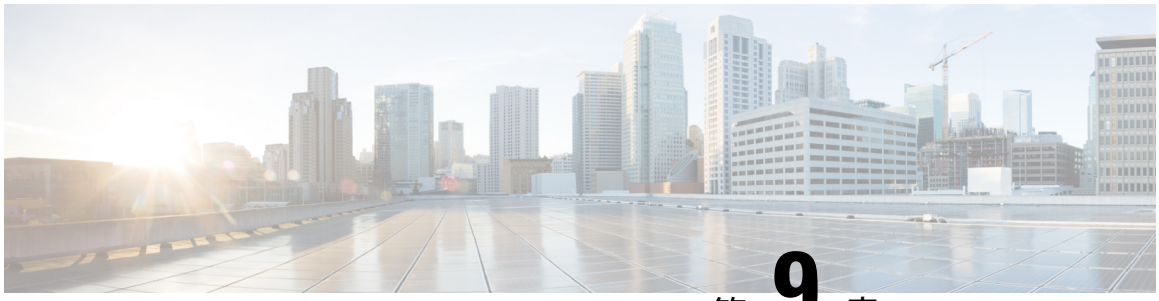
バージョン 6.2.3.1 で解決済みの問題

表 *62 :* バージョン *6.2.3.1* で解決済みの問題

不具合 ID	タイトル
CSCvf97979	ルールのセキュリティ ゾーンを変更した後、デルタ設定の生成中に NAT ポリシーの展開が失敗した
CSCvg00565	`debug menu` セルフ テストの実行時に **glib/g_slice** で ASA がクラッシュする
CSCvg36672	アクション キューでユーザ主導型展開タスクの優先順位を付ける方法が必要

不具合 ID	タイトル
CSCvg65072	Cisco ASA SW、FTD SW、および AnyConnect セキュア モビリティ クライアント SAML 認証のセッション固定攻撃に対する脆弱性
CSCvg78418	Apache/Struts 関連の脆弱性に対する FireSIGHT / FirePOWER の評価
CSCvg84495	OpenLDAP レルム/サーバを使用したリモート アクセス VPN で正しいネーミング属性が使用されない
CSCvh05081	ASA モジュールによって生成される SACK パケットの SLE 値と SRE 値を ASA が非ランダム化しない
CSCvh22181	SSL インスペクションが有効になっている TLS 1.3 を使用した Web サイト（メール サイトなど）のロードが失敗する
CSCvh25433	AC を使用するエンド ポイントで外部ブラウザによるレガシー方式 SAML 認証をサポートするための新しい CLI
CSCvh46202	VPN 経由のフラグメント化されたトラフィックにより 2048 バイト ブロックのリークが遅くなる
CSCvh53616	SSL により Firepower Threat Defense デバイス上の ASA がトレースバックする
CSCvh63903	8000 シリーズ ペア デバイスでの IPv6 アドレスのフェールオーバーが成功しない場合がある
CSCvh79732	Cisco 適応型セキュリティ アプライアンスにおけるサービス拒否攻撃に対する脆弱性
CSCvh81474	[Deploy] ボタンと通知のレンダリングを許可するには、不正な形式の JSON を捕捉する必要がある
CSCvh81737	Cisco 適応型セキュリティ アプライアンスにおけるサービス妨害の脆弱性
CSCvh81870	Cisco 適応型セキュリティ アプライアンスにおけるサービス拒否攻撃に対する脆弱性
CSCvh83012	SFDataCorrelator は重複フローのレートを制限してはならない
CSCvh99414	NFE に障害が発生すると Snort が常に再起動する
CSCvi03546	現在のマップの更新中にエラーが発生したため、管理対象デバイスでユーザ - IP マッピングが更新されない
CSCvi18602	ASA FirePOWER モジュール（5585-x）を 6.2.2.2 から 6.2.2.1 にダウングレードする際に FSIC が失敗した

不具合 ID	タイトル
CSCvi34137	SSL 復号化が有効になっていて、HTTP 要求が TCP セグメント化されている場合、Snort が URI を正しくキャプチャしない
CSCvi44365	アップグレード後、Firepower 4100 のホスト名が SFCLI のホスト名と異なる
CSCvi49752	`sfipproxy` がハイ アベイラビリティ ペアに登録されていると、センサーに正しく書き込まれない場合がある
CSCvi55280	デルタの最後の CLI でエラーが発生した場合、展開トランスクリプトで失敗したコマンドが示されない
CSCvi80849	Cisco Firepower 2100 シリーズ POODLE TLS セキュリティスキャナのアラート



第 9 章

既知の問題

パッチの既知の問題は記載されていません。

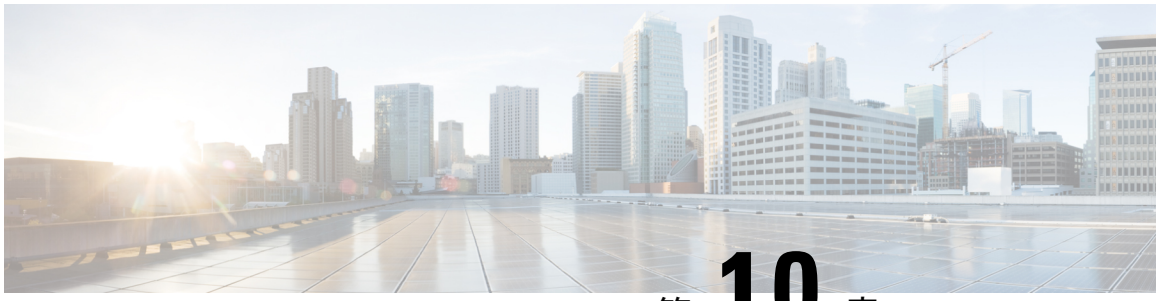
- 既知の問題の検索 （133 ページ）

既知の問題の検索

サポート契約がある場合は、Cisco Bug Search Tool を使用して Firepower 製品の最新のオープンバグリストを取得することができます。 検索では、特定の Firepower プラットフォームとバージョンに影響するバグに絞り込むことができます。バグ ID ごとに検索したり、特定のキーワードを検索したりすることもできます。

これらの一般的なクエリには、Version6.2.3.x パッチを実行している Firepower 製品の未解決のバグが表示されます。

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



第 10 章

支援が必要な場合

Firepower をお選びいただき、ありがとうございます。

オンラインリソース

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

- シスコサポートおよびダウンロードサイト：https://www.cisco.com/c/en/us/support/index.html
- Cisco Bug Search Tool：https://tools.cisco.com/bugsearch/
- シスコ通知サービス：https://www.cisco.com/cisco/support/notifications.html

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

シスコへのお問い合わせ

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

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