Cisco Firepower バージョン 6.2.3 リリースノート

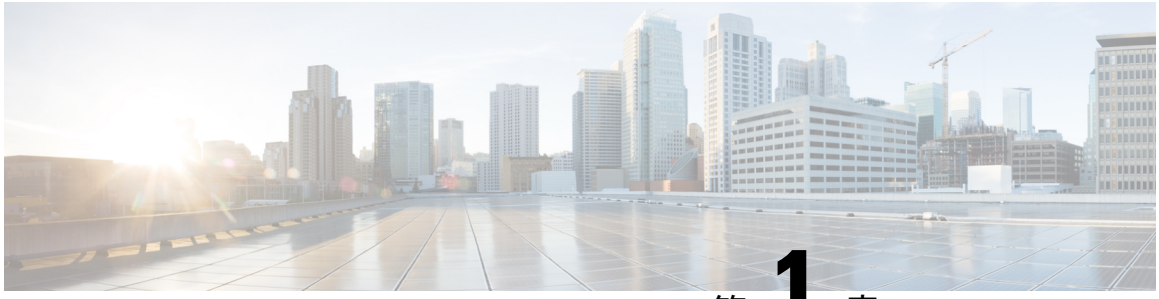
初版：2018 年 3 月 29 日

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 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 （82 ページ）を参照してください。

表 *1:* バージョン *6.2.3* の日付

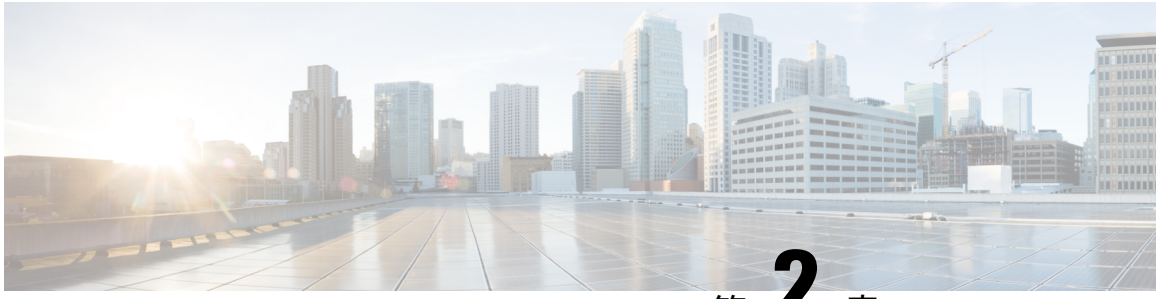
バージョン	ビルド	日付	プラットフォーム：アップグレード	プラットフォーム：再イメージ化
6.2.3	113	2020 年 6 月 1 日	FMC/FMCv	FMC/FMCv
6.2.3	111	2019 年 11 月 25 日	—	FTDv: AWS, Azure
6.2.3	110	2019 年 6 月 14 日	—	—
6.2.3	99	2018 年 9 月 7 日	—	—
6.2.3	96	2018 年 7 月 26 日	—	—
6.2.3	92	2018 年 7 月 5 日	—	—
6.2.3	88	2018 年 6 月 11	—	—
6.2.3	85	2018 年 4 月 9 日	—	—
6.2.3	84	2018 年 4 月 9 日	Firepower 7000/8000 シリーズ NGIPSv	—
6.2.3	83	2018 年 4 月 2 日	FTD/FTDv ASA FirePOWER	FTD：物理プラットフォーム FTDv：VMware、FVM Firepower 7000/8000 ASA FirePOWER NGIPSv
6.2.3	79	2018 年 3 月 29 日	—	—

以下のパッチも利用できます。

表 *2 :* 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（All）
	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。
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 *3 :* 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 *4 :* 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 または 7000/8000 シリーズ：**[システム（System）]** > **[設定（Configuration）]** を選択し、**[HTTPS 証明書（HTTPS Certificates）]** をクリックします。

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

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

（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。

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

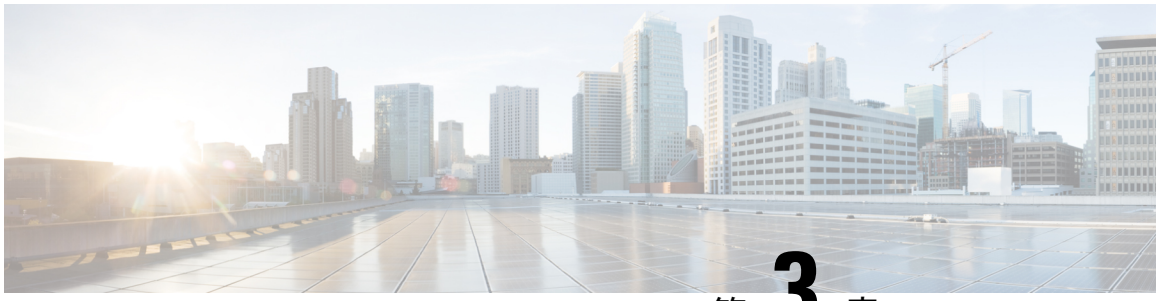
インターフェイス	解像度
Firepower Management Center	1280 X 720
7000/8000 シリーズ デバイス（制限されたローカル インターフェイス）	1280 X 720
Firepower Device Manager	1024 X 768
を管理している ASDM ASA FirePOWER module	1024 X 768
Firepower Chassis Manager 向け Firepower 9300 シャーシ	1024 X 768

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 （79 ページ）を参照してください。

表 *6:* 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

メジャーリリースは、Firepowerソフトウェアの新機能、機能、および拡張機能を提供します。メジャーバージョンには、廃止された機能とプラットフォーム、メニューと用語の変更、動作の変更などが含まれることがあります。

廃止された機能は、バージョンをスキップするときにアップグレードの問題を引き起こす可能性が最も高いため、リリースノートには廃止された機能の履歴情報が記載されています。新機能の履歴情報については、スキップするバージョンのリリースノートを参照してください。

Firepower Management Center/バージョン 6.2.3 の新機能

次の表に、Firepower Management Centerを使用して設定された場合にFirepowerバージョン6.2.3で使用できる新機能を示します。

機能	説明
ハードウェアと仮想ハードウェア	

機能	説明
ISA 3000 の FTD	管理のために Firepower Device Manager または Firepower Management Center を使用して、ISA 3000 シリーズで Firepower Threat Defense を実行できるようになりました。 ISA 3000 は脅威のライセンスのみをサポートしていることに注意してください。URL フィルタリングやマルウェアのライセンスはサポートしていません。したがって、ISA 3000 では URL フィルタリングやマルウェアのライセンスを必要とする機能は設定できません。ハードウェア バイパスやアラーム ポートなど、ASA でサポートされていた ISA 3000 の特別な機能は、このリリースの Firepower Threat Defense ではサポートされていません。
VMware ESXi 6.5 のサポート	Firepower Threat Defense Virtual、Firepower Management Center Virtual、および Firepower NGIPS Virtual が、VMware ESXi 6.5 でサポートされるようになりました。
Firepower Threat Defense：**暗号化と VPN**	
SSL ハードウェア アクセラレーション	特定の FirePOWER 管理対象デバイス モデルでは、パフォーマンスが大幅に向上する、ハードウェアでの SSL 暗号化および復号化のアクセラレーションをサポートしています。SSL ハードウェア アクセラレーションは、サポートするすべてのアプライアンスに対してデフォルトで無効化されています。 サポートされるプラットフォーム：Firepower 4100/9300

機能	説明
Firepower Threat Defense の VPN の改善	証明書の登録操作のノンブロッキング ワーク フローでは、複数の Firepower Threat Defense デバイスで証明書の登録を並行して実行できます。 • 管理者は、[Access & Certificate] ステップで [Enroll the selected certificate object on the target devices] チェックボックスをオンにすることで、ポリシー内のすべてのデバイスに対して、リモート アクセス VPN ポリシー ウィザードで証明書を登録できるようになりました。この操作を選択した場合、ウィザードの終了後に展開のみを実行する必要があります。この設定は、デフォルトでオンになっています。 • 管理者は、デバイスでリモートアクセス VPN 証明書の登録を一度に 1 つずつ開始する必要がなくなりました。各デバイスの登録プロセスは、現在独立しており、並行して実行できます。 • PKS12 証明書の登録に失敗した場合、管理者は、登録を再試行するためにもう一度 PKS12 ファイルを再アップロードする必要はありません。これは、PKS12 ファイルが証明書の登録オブジェクトに保存されるためです。
Firepower Threat Defense：ハイアベイラビリティとクラスタリング	
Firepower Management Center のハイ アベイラビリティ メッセージ	Firepower Management Center のハイ アベイラビリティ ペアでは、UI メッセージが改善されています。UI には、Firepower Management Center のペアが確立されている間に、中間ステータス メッセージが表示されるようになり、書き換えられた UI メッセージがより直感的になりました。
内部エラーの発生後に自動的に Firepower Threat Defense クラスタに再参加	以前は、多くの内部エラー状態によって、クラスタ ユニットがクラスタから削除され、ユーザが問題を解決した後で、手動でクラスタに再参加する必要がありました。現在は、ユニットが自動的に、5 分、10 分、20 分の間隔でクラスタに再参加しようとします。内部エラーには、アプリケーション同期のタイムアウト、一貫性のないアプリケーションステータスなどがあります。 新しい/変更されたコマンド：**show cluster info auto-join** サポートされるプラットフォーム：Firepower 4100/9300

機能	説明

Firepower Threat Defense のハイアベイラビリティ強化	バージョン 6.2.3 では、ハイア ベイラビリティの Firepower Threat Defense デバイスに関する次の機能が導入されています。
	• ハイアベイラビリティペアのアクティブまたはスタンバイ Firepower Threat Defense デバイスが再起動されると、Firepower Management Center は、どちらの管理対象デバイスでも正確なハイアベイラビリティステータスを表示しない場合があります。ただし、Firepower Threat Defense と Firepower Management Center 間の通信が確立されていないために、Firepower Management Center ではステータスがアップグレードされないことがあります。**[Devices]** > **[Device Management]** ページの [Refresh Node Status] オプションを使用すると、ハイアベイラビリティノードのステータスを更新して、ハイアベイラビリティペアのアクティブデバイスとスタンバイデバイスに関する正確な情報を取得できます。
	• Firepower Management Center UI の **[Devices]** > **[Device Management]** ページには、新しい [Switch Active Peer] アイコンがあります。
	• バージョン 6.2.3 には、新しい REST API オブジェクト **Device High Availability Pair Services** が含まれており、次の 4 つの機能を備えています。
	  • **DELETE ftddevicehapairs**
	  • **PUT ftddevicehapairs**
	  • **POST ftddevicehapairs**
	  • **GET ftddevicehapairs**

管理とトラブルシューティング	
Firepower Threat Defense SSH アクセスへの外部認証の追加	LDAP または RADIUS を使用して、Firepower Threat Defense への SSH アクセス用に外部認証を設定できるようになりました。 新規/変更された画面：**[デバイス（Devices）]**>**[プラットフォーム設定（Platform Settings）]** > **[外部認証（External Authentication）]** サポートされるプラットフォーム：FTD

機能	説明
脆弱性データベース（VDB）の強化されたインストール	Firepower Management Center は、VDB をインストールする前に、インストールにより Snort プロセスが再起動し、トラフィック検査が中断され、管理対象デバイスがトラフィックを処理する方法次第でトラフィック フローが中断される可能性があるという警告を表示するようになりました。メンテナンス期間中など、都合の良い期間までインストールをキャンセルすることができます。 次のようなときに警告が表示される可能性があります。 • VDB をダウンロードして手動でインストールした後。 • スケジュールされたタスクを作成して VDB をインストールする場合。 • たとえば、以前にスケジュールされたタスクの実行中に、または Firepower ソフトウェア アップグレードの一部として、VDB がバックグラウンドでインストールされる場合。
アップグレード パッケージのプッシュ	実際のアップグレードを実行する前に、Firepower Management Center から管理対象デバイスにアップグレード パッケージをコピー（またはプッシュ）できるようになりました。帯域幅の使用量が少ない時間帯やアップグレードのメンテナンス期間外でプッシュできるため、この機能は便利です。 ハイア ベイラビリティ デバイス、クラスタ デバイス、またはスタック構成デバイスにプッシュすると、システムは、アップグレード パッケージを最初にアクティブ/マスター/プライマリに送信し、次にスタンバイ/スレーブ/セカンダリに送信します。 新規/変更された画面：**[System]** > **[Updates]**
Firepower Threat Defense の保守性	バージョン 6.2.3 では、 **show fail over** CLI コマンドが改善されています。新しいキーワード **-history** を使用すると、トラブルシューティングに役立つ詳細が表示されます。 • **Show fail over history** は、失敗の理由に加えて、その具体的な詳細を表示します。 • **Show fail over history details** は、ピア ユニットのフェールオーバー履歴を表示します。 （注） このコマンド出力には、フェールオーバーでのピア ユニットの状態変化や、その状態変化の理由が含まれます。

機能	説明
デバイス一覧のソート	**[Devices]** > **[Devices Management]** ページで、[View by] ドロップダウンリストを使用して、グループ、ライセンス、モデル、またはアクセスコントロールポリシーのいずれかのカテゴリでデバイス一覧をソートして表示できます。マルチドメイン導入では、ドメイン（その導入のデフォルトの表示カテゴリ）を基準にソートして表示することもできます。デバイスはリーフ ドメインに属している必要があります。
監査ログの改善	監査ログは、Firepower Threat Defense Platform 設定の **[Devices]** > **[Platform Settings]** ページでポリシーが変更されたかどうかを示します。
FTD CLI コマンドの更新	Firepower Threat Defense デバイスの CLI コマンドの **asa_mgmt_plane** オプションと **asa_dataplane** オプションは、**management-plane** と **data-plane** にそれぞれ名前が変更されています。
Cisco Success Network	**アップグレードの影響。** *Cisco Success Network* は、テクニカルサポートを提供するために不可欠な使用状況に関する情報と統計情報をシスコに送信します。 アップグレード中に、参加を承諾するか、辞退するかを尋ねられます。また、いつでもオプトインまたはオプトアウトできます。
Web 分析トラッキング	**アップグレードの影響。** *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。 バージョン 6.2.3 にアップグレードすると、Web 分析トラッキングが有効になります。このデータの収集を拒否する場合は、アップグレード後にオプトアウトできます。
Performance	

機能	説明
ポリシー展開の再起動の改善	バージョン 6.2.3 の機能強化として、Snort プロセスを再起動する設定が削減されました。Firepower Threat Defense デバイスでは、設定の展開により Snort プロセスが再起動し、トラフィック検査が中断され、管理対象デバイスがトラフィックを処理する方法次第でトラフィック フローが中断される可能性がある場合、展開の前に、管理 UI が警告を出すようになりました。 再起動の動作は、Firepower Device Manager を使用して管理されているデバイスでは異なることに注意してください。詳細については、Firepower Device Manager/FTD バージョン 6.2.3 の新機能 （20 ページ） を参照してください。
ポリシー適用時のトラフィック ドロップ	バージョン 6.2.3 では、**configure snort preserve-connection {enable | disable}** コマンドが Firepower Threat Defense CLI に追加されています。このコマンドは、Snort プロセスがダウンした場合に、ルーテッド インターフェイスとトランスペアレント インターフェイスで既存の接続を維持するかどうかを決定します。コマンドを無効にすると、Snort がダウンして、Snort が再開するまでドロップされたままになると、新規または既存のすべての接続がドロップされます。コマンドを有効にした場合、すでに許可されている接続は確立されたままですが、Snort が再び使用可能になるまで新しい接続を確立できません。 Firepower Device Manager で管理されている Firepower Threat Defense デバイスでは、このコマンドを永続的に無効にできないことに注意してください。次の設定の展開時に設定がデフォルトに戻ると、既存の接続がドロップされることがあります。
ローエンド アプライアンスのメモリ容量の増加	バージョン 6.1.0.7、6.2.0.5、6.2.2.2、および 6.2.3 では、Firepower ローエンド アプライアンスのメモリ容量が増加しています。これにより、ヘルス アラートの数が削減されます。
ISE pxGrid ディスカバリの高速化	ハイ アベイラビリティの ISE pxGrid に障害が発生した場合、または到達不能になった場合、Firepower Management Center は、新しいアクティブ pxGrid をより迅速に検出できるようになりました。
FMC REST API	

機能	説明
Firepower Management Center REST API の改善	新しい Firepower Management Center REST API は、ASA FirePOWER から Firepower Threat Defense への移行時に、NAT ルール、スタティック ルーティング設定、および対応するオブジェクトに対する CRUD（作成、取得、アップグレード、削除）操作の使用をサポートしています。 NAT 用に新しく導入された API • NAT ルール • Firepower Threat Defense NAT ポリシー • 自動 NAT ルール • 手動 NAT ルール Cisco ACI に Firepower Threat Defense デバイスを展開する場合、API を使用すると、APIC コントローラを介して、適切なスタティック ルートを適切に追加できるほか、特定のサービス グラフに必要なその他の設定も追加できます。また、API により、Firepower Threat Defense を ACI に挿入する最も柔軟性の高い方法である、PBR サービス グラフの挿入も可能になります。 スタティック ルート用に新しく導入された API • IPv4 スタティック ルート • IPv6 スタティック ルート • SLA モニタ

Firepower Device Manager/FTD バージョン 6.2.3 の新機能

リリース：2018年3月29日

次の表に、Firepower Device Manager を使用して設定された場合に FTD 6.2.3 で使用できる新機能を示します。

機能	説明
SSL/TLS の復号	接続の内容を調べることができるように、SSL/TLS 接続を復号できます。復号しないと、暗号化された接続は、侵入およびマルウェアの脅威を識別したり、URL およびアプリケーション使用状況ポリシーへの準拠を強制したりするための効果的な検査が行えません。**[Policies]** > **[SSL Decryption]** ページおよび **[Monitoring]** > **[SSL Decryption]** ダッシュボードが追加されました。 **注目** アクティブな認証を実装するアイデンティティポリシーは、SSL 復号ルールを自動的に生成します。SSL 復号をサポートしていないリリースからアップグレードする場合、SSL 復号ポリシーは、この種類のルールがある場合、自動的に有効になります。ただし、アップグレードの完了後、再署名の復号ルールで使用する証明書を指定する必要があります。アップグレード後すぐに SSL 復号設定を編集してください。
セキュリティ インテリジェンスのブラックリスト登録	新しい **[ポリシー（Policies）]** > **[セキュリティインテリジェンス（Security Intelligence）]** ページから設定できるセキュリティ インテリジェンス ポリシーにより、送信元/宛先の IP アドレスまたは宛先 URL に基づいて、望ましくないトラフィックを早い段階でドロップできます。許可された接続もすべてアクセス コントロール ポリシーによって引き続き評価され、最終的にドロップされる可能性があります。セキュリティ インテリジェンスを使用するには、脅威ライセンスを有効にする必要があります。 また、[ポリシー（Policies）] ダッシュボードの名前を [アクセスおよびSIルール（Access And SI Rules）] に変更し、セキュリティ インテリジェンス同等のルールがアクセス ルールとともにダッシュボードに含まれるようになりました。
侵入ルールの調整	アクセス制御ルールを適用する事前に定義された侵入ポリシー内の侵入ルールのアクションを変更できます。トラフィックに一致するイベント（警告）をドロップまたは生成する各ルールを設定したり、ルールを無効にしたりできます。有効になっているルールのアクション（ドロップまたは警告に設定）のみ変更できます。デフォルトで無効になっているルールを有効にはできません。侵入ルールを調整するには、**[Policies]** > **[Intrusion]** を選択します。

機能	説明
侵入ポリシーに基づく自動ネットワーク分析ポリシー（NAP）割り当て	以前のリリースでは、[Balanced Security and Connectivity] ネットワーク分析ポリシーが、特定の送信元/送信先のセキュリティゾーンとネットワークオブジェクトの組み合わせに割り当てられた侵入ポリシーに関係なく、プリプロセッサ設定で常に使用されました。システムは自動的に NAP ルールを生成し、同じ名前の NAP と侵入ポリシーをそれらの基準に基づいてトラフィックに割り当てるようになりました。レイヤ 4 または 7 の基準を使用して異なる侵入ポリシーをトラフィック（それ以外は同じ送信元/送信先のセキュリティ ゾーンおよびネットワーク オブジェクトと一致する）に割り当てる場合、完全に一致する NAP および侵入ポリシーは取得されないことに注意してください。カスタム ネットワーク分析ポリシーは作成できません。
脅威、攻撃、およびターゲットのダッシュボード用のドリル ダウン レポート	脅威、攻撃、およびターゲットのダッシュボードに移動して、報告された項目についての詳細を表示できるようになりました。これらのダッシュボードは [Monitoring] ページで使用できます。 これらの新しいレポートのため、6.2.3 より前のリリースからアップグレードする場合は、これらのダッシュボードのレポートデータが失われます。
[Web Applications] ダッシュボード	新しい [Web Applications] ダッシュボードは、Google など、ネットワークで使用されている上位の Web アプリケーションを示します。このダッシュボードはアプリケーションのダッシュボードを強化し、HTTP の使用率などのプロトコル指向の情報を提供します。
新しいゾーンのダッシュボードが入力ゾーンと出力ゾーンのダッシュボードを置き換え	新しいゾーンのダッシュボードは、デバイスに入ってから出るトラフィックに対する上位セキュリティゾーンのペアを示します。このダッシュボードは、入力および出力ゾーンに対する個別のダッシュボードを置き換えます。
新しいマルウェア ダッシュボード	新しいマルウェアダッシュボードは、上位のマルウェアのアクションと判定結果の組み合わせを示します。ドリルダウンして、関連付けられているファイル タイプの情報を参照できます。この情報を表示するには、アクセス ルールにファイル ポリシーを設定する必要があります。
自己署名入りの内部証明書、および内部 CA 証明書	自己署名入りの内部アイデンティティ証明書を生成できるようになりました。また、SSL 復号ポリシーで使用するための、自己署名付きの内部 CA 証明書を生成したり、アップロードできるようになりました。これらの機能を、**[Objects]** > **[Certificates]** ページで設定します。

機能	説明
インターフェイスのプロパティ編集時に DHCP サーバの設定を編集する機能	インターフェイスのプロパティを編集すると同時に、インターフェイスに設定されている DHCP サーバの設定を編集できるようになりました。これにより、インターフェイスの IP アドレスを別のサブネットに変更する必要がある場合に、DHCP アドレス プールを簡単に再定義できます。
製品を改善し、効果的な技術サポートを提供するための、Cisco Success Network によるシスコへの利用状況や統計データの送信	Cisco Success Network に接続し、シスコにデータを送信できます。Cisco Success Network を有効にすることで、テクニカル サポートを提供するために不可欠な、使用状況の情報と統計情報をシスコに提供します。またこの情報により、シスコは製品を向上させ、未使用の使用可能な機能を認識させるため、ネットワーク内にある製品の価値を最大限に生かすことができます。Cisco Smart Software Manager でデバイスを登録するとき、または後から好きなときに、接続を有効にできます。接続はいつでも無効にできます。 Cisco Success Network はクラウド サービスです。**[Device]** > **[System Settings]** > **[Cloud Management]** ページの名前が [Cloud Services] に変更されました。同じページから、Cisco Defense Orchestrator を設定できます。
Firepower Threat Defense 仮想 カーネルベースの仮想マシン（KVM）のハイパーバイザデバイス用の設定	Firepower Device Manager を使用して、Firepower Threat Defense 仮想 for KVM デバイス上の FTD を設定できます。以前は、VMware のみがサポートされていました。 （注） Firepower Device Manager のサポートを得るには、新しい 6.2.3 イメージをインストールする必要があります。既存の仮想マシンを古いバージョンからアップグレードして Firepower Device Manager に切り替えることはできません。
ISA 3000（Cisco 3000 シリーズ産業用セキュリティアプライアンス）デバイスの設定	Firepower Device Manager を使用して ISA 3000 デバイス上の FTD を設定できます。ISA 3000 は脅威のライセンスのみをサポートしていることに注意してください。URL フィルタリングやマルウェアのライセンスはサポートしていません。したがって、ISA 3000 では URL フィルタリングやマルウェアのライセンスを必要とする機能は設定できません。

機能	説明
ルール データベースまたは VDB の更新でのオプションの展開	侵入ルール データベースまたは VDB を更新する、または更新スケジュールを設定する際に、更新が即時展開しないようにすることができます。更新プログラムは検査エンジンを再起動するため、展開時に瞬間的なトラフィックのドロップが発生します。自動的に展開しないことにより、トラフィックのドロップの影響が最小になる場合に展開を開始できます。 （注） VDB ダウンロードは、単独で Snort を再起動することもできますが、展開時に再起動が発生します。ダウンロード時の再起動を止めることはできません。
展開が Snort を再起動するかどうかを示す、改善されたメッセージ。さらに、展開時の Snort を再起動する必要性の低下	展開を開始する前に、Firepower Device Manager により、設定の更新で Snort の再起動が必要かどうかが示されます。Snort の再起動は、トラフィックの瞬間的なドロップを発生させます。したがって、展開がトラフィックに影響を与えず、すぐに実行できるかどうかがわかるようになったため、混乱が少ないときに展開できます。 さらに、以前のリリースでは展開の実行の度に Snort が再起動されていました。Snort は、次の理由でのみ再起動されるようになりました。 • ユーザが SSL 復号ポリシーを有効または無効にする • 更新されたルール データベースまたは VDB がダウンロードされた • ユーザが 1 つまたは複数の物理インターフェイス（ただしサブインターフェイスではない）で MTU を変更した
Firepower Device Manager の CLI コンソール	Firepower Device Manager から CLI コンソールを開くことができるようになりました。CLI コンソールは SSH またはコンソール セッションを模倣していますが、コマンドのサブセットのみ（**show**、**ping**、**traceroute**、および **packet-tracer**）を許可します。トラブルシューティングとデバイスのモニタリングに CLI コンソールを使用します。

機能	説明
管理アドレスへのアクセスのブロックのサポート	管理IPアドレスにアクセスできないようにするため、プロトコルのすべての管理アクセスリストのエントリを削除できるようになりました。以前は、すべてのエントリを削除すると、すべてのクライアントIPアドレスからのアクセスを許可するようにシステムのデフォルトが設定されていました。6.2.3へのアップグレードでは、以前からのプロトコル（HTTPSまたはSSH）用の空の管理アクセス リストがあった場合、システムはすべての IP アドレス用のデフォルトの許可ルールを作成します。必要に応じて、これらのルールを削除できます。 また、SSH または HTTPS アクセスを無効にする場合を含み、Firepower Device Manager は CLI から管理アクセスリストに加えた変更を認識します。 少なくとも 1 つのインターフェイスに対する HTTPS アクセスを有効にしてください。そうしないとデバイスを設定および管理することができません。

機能	説明
デバイス CLI を使用した、機能の設定のための Smart CLI および FlexConfig	Smart CLI と FlexConfig により、まだ Firepower Device Manager ポリシーおよび設定では直接サポートされていない機能を設定できます。Firepower Threat Defense は、ASA 設定コマンドを使用していくつかの機能を実装します。ASA 設定コマンドの知識があり、専門家ユーザの場合、次の方法を使用して、デバイスでこれらの機能を設定できます。 • Smart CLI：（推奨される方法です。）Smart CLI テンプレートは、特定の機能の定義済みテンプレートです。機能に必要なすべてのコマンドが提供されているため、変数の値を選択するだけで済みます。システムにより選択が検証されるため、機能を正しく設定できる可能性が高まります。目的の機能の Smart CLI テンプレートが存在する場合は、この方法を使用する必要があります。このリリースでは、Smart CLI を使用して、OSPFv2 を設定できます。 • FlexConfig：FlexConfig ポリシーは、FlexConfig オブジェクトのコレクションです。FlexConfig オブジェクトは Smart CLI テンプレートより自由な形式であり、システムに CLI、変数はなく、データ検証も行われません。有効な一連のコマンドを作成するには、ASA 設定コマンドを知り、ASA 設定ガイドに従う必要があります。 **注意** Smart CLI と FlexConfig の利用は、ASA の強力なバックグラウンドを持つ上級者が自身のリスクで行う場合にかぎることをシスコは強く推奨します。ブラックリストに登録されていない任意のコマンドも設定できます。Smart CLI または FlexConfig を介して機能を有効にすると、その他の設定済みの機能に予期しない結果が発生する可能性があります。
Firepower Threat Defense REST API、および API エクスプローラ	REST API を使用して、Firepower Device Manager を介してローカルで管理している Firepower Threat Defense デバイスをプログラムで操作できます。オブジェクトモデルを表示し、クライアントプログラムから作成できるさまざまな呼び出しのテストに使用できる API エクスプローラがあります。API エクスプローラを開くには、Firepower Device Manager にログインし、URL のパスを /#/api-explorer（https://ftd.example.com/#/api-explorer など）に変更します。

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。 アップグレードパスでバージョンをスキップする場合は、中間リリースの廃止された機能を確認してください。

（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。

バージョン 6.2.3 で廃止された機能

以下の機能はバージョン 6.2.3 で廃止されました。

表 7: バージョン *6.2.3* 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
pager FlexConfig コマンド	アップグレード後に設定をやり直す必要があります。	FDM を使用した FTD	バージョン 6.2.3 では、FDM を使用した FTD の場合、**pager** FlexConfig CLI コマンドがブロックされます。
期限切れの動的分析用のCA証明書	なし。ただし、パッチまたはアップグレードが必要です。	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 （30ページ）」を参照してください。

バージョン 6.2.0 で廃止された機能

これらの機能はバージョン 6.2.0 で廃止されました。

表 *8 :* バージョン *6.2.0* 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
ネストされた相関ルール	アップグレードが失敗する可能性があります。	FMC	

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 6.2.0 では、ネストされた相関ルールのサポートが終了します。ある相関ルールが別の相関ルールのトリガーとなっている場合、その相関ルールはネストされています。たとえば、どちらも侵入イベントのトリガーであるルール A とルール B を作成する場合、「ルール A は true」をルール B の制約として使用できます。この設定では、ルールAはルール B 内にネストされています。 **自動設定の変更** アップグレードプロセスは、ネストされたルール（ルールA）からネストされたルール（ルール B）へ設定をコピーしてネストされたルールを削除することで、特定のネストされた相関ルールを「フラット化」します。また、アップグレードは、ホストプロファイル/ユーザ資格とスヌーズ/非アクティブ期間を、ネストされたルールからネストルールへコピーします。 非アクティブ期間を除いて、これらのすべての設定について、設定がネスト ルールに存在しない場合にのみ、システムはネストされたルールからネスト ルールへ設定をコピーできます。システムがネストされたルールからネスト ルールへ非アクティブ期間をコピーするときは、結果として生じるルールがネスト構成にもともと含まれる両方のルールの設定を使用するように、ネスト ルールの非アクティブ期間を保持します。 **アップグレードの失敗の回避** アップグレードする前に、ネストされた相関ルールを「フラット化」できることを確認してください。そうなっていなければ、アップグレードは失敗します。ネストされたルールとネスト ルールに特定の競合がある場合は、アップグレードによりネストされたルールをフラット化できないことに注意してください。アップグレードの失敗を回避するには、アップグレードの前に、以下のように相関ルールを変更します。 • ネストされた構成内で 1 つのルールだけ

機能	アップグレードの影響	プラットフォーム	説明
			がこれらの設定を指定するように、ホスト プロファイル資格、ユーザ資格、スヌーズ期間の設定をネストされたルールまたはネスト ルールから削除します。 • 接続トラッカーを任意のネストされたルールから削除します。 • ホスト プロファイル資格、ユーザ資格、スヌーズ期間、非アクティブ期間を、true にする必要がないネストされたルールから削除します。つまり、ネスト ルール内の OR 演算子を使用して他のルールの条件にリンクされているネストされたルールから、これらの要素を削除します。

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 *9*：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。	

廃止された FlexConfig コマンド

このリリースノートでは、廃止された機能 （27 ページ）に、各バージョンの廃止された FlexConfig のオブジェクトおよびコマンドと、その他の廃止された機能が記載されています。

FlexConfig が導入されたときに禁止されたコマンドを含む、禁止されたコマンドの完全なリストについては、コンフィギュレーション ガイドを参照してください。

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

FlexConfig について

いくつかの Firepower Threat Defense の機能は、ASA 設定コマンドを使用して設定されます。バージョン 6.2.0（FMC 展開）またはバージョン 6.2.3（FDM 展開）以降では、スマート CLI

または FlexConfig を使用して、他の方法では Web インターフェイスでサポートされないさまざまな ASA 機能を手動で設定できます。

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

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

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ッセサルール、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。

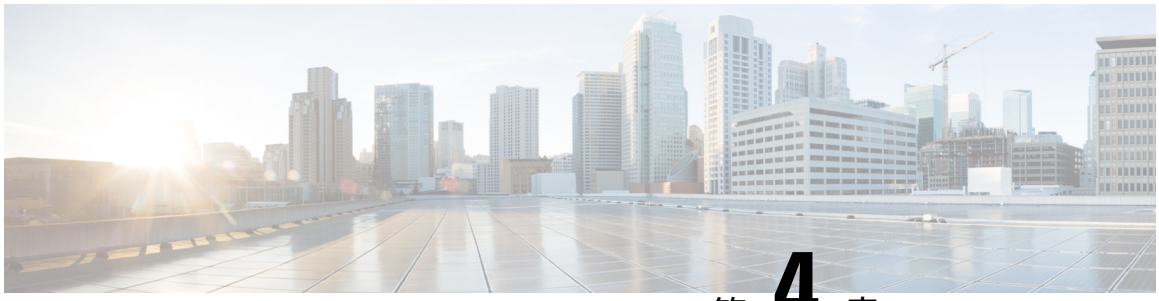
Web 分析トラッキングはデフォルトでオンになっています（バージョン 6.5.0 以降の EULA に承諾すると、Web分析トラッキングに同意したことになります）。ただし、初期設定の完了後にいつでもオプトアウトできます。

（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 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 *10* : *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のガイドライン （36 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。
	以前に公開されたガイドライン （40 ページ）	アップグレードでバージョンがスキップされる場合は、これらを参照してください。
	一般的なガイドライン （43 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 （105 ページ）	これらを読み、アップグレードに影響するバグを回避する準備を整えます。 アップグレードでバージョンがスキップされる場合は、スキップするメジャーバージョンの既知の問題も参照してください。「Cisco Firepower リリース ノート」を参照してください。
	特長と機能 （13 ページ）	アップグレードに影響する可能性のあるその他の項目については、これらをお読みください。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。 アップグレードでバージョンがスキップされる場合は、スキップしたバージョンの新機能に関するドキュメントもお読みください。「Cisco Firepower リリース ノート」を参照してください。

Version6.2.3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 の新規または固有のアップグレードガイドラインが含まれています。現在**バージョン 6.1.0 ～ 6.2.2** を実行している場合は、次のガイドラインを確認してください。

表 *11* : バージョン *6.2.3* の新しいガイドライン

✓	ガイドライン	プラットフォーム	アップグレード元	直接アップグレード先
	シスコとのデータの共有 （37 ページ）	いずれか（Any）	いずれか（Any）	6.2.3 以降

✓	ガイドライン	プラットフォーム	アップグレード元	直接アップグレード先
	アップグレードの失敗：Firepower 2100 シリーズのバージョン 6.2.2.5 から （38 ページ）	FDM を使用した Firepower 2100 シリーズ	6.2.2.5	6.2.3 のみ
	FTD/FDM のアップグレード後にレルムを編集/再保存 （38 ページ）	FDM を使用した FTD	6.2.0 ～ 6.2.2.x	6.2.3 のみ
	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 （39 ページ）	FDM を使用した FTD	6.2.0 ～ 6.2.2.x	6.2.3 ～ 6.4.0
	アップグレード後にアクセス コントロール ポリシーを編集/再保存する （39 ページ）	任意	6.1.0 ～ 6.2.2.x	6.2.3 のみ
	レポートの結果の制限の変更 （39 ページ）	FMC	6.1.0 ～ 6.2.2.x	6.2.3 ～ 6.4.0
	アップグレードの前にバージョン 6.1.x FTD クラスタからサイト ID を削除 （40 ページ）	FTD クラスタ	6.1.0.x	6.2.3 ～ 6.4.0

シスコとのデータの共有

展開：すべて

アップグレード元：バージョン 6.1.0+

直接アップグレード先：バージョン 6.2.3+

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。

アップグレードの失敗：Firepower 2100 シリーズのバージョン 6.2.2.5 から

展開：FDM によって管理される、FTD を使用した Firepower 2100 シリーズ

アップグレード元：バージョン 6.2.2.5

直接アップグレード先：バージョン 6.2.3 のみ

バージョン 6.2.2.5 を実行している Firepower 2100 シリーズ デバイスで DNS 設定を変更した後に、中間展開なしでバージョン 6.2.3 にアップグレードすると、アップグレードに失敗します。デバイスをアップグレードする前に、展開するか、展開をトリガーするアクション（SRU アップデートなど）を実行する必要があります。

FTD/FDM のアップグレード後にレルムを編集/再保存

展開：FDM を使用した FTD

アップグレード元：バージョン 6.2.0 ～ バージョン 6.2.2.x

直接アップグレード先：バージョン 6.2.3 のみ

バージョン 6.2.3 以前では、ユーザは非アクティブ状態で 24 時間後に自動的にログアウトされませんでした。Firepower Device Manager を使用していて Firepower Threat Defense をバージョン 6.2.3 にアップグレードした後、アクティブ認証でアイデンティティ ポリシーを使用している場合、設定を展開する前にレルムを更新します。**[オブジェクト（Objects）]** > **[アイデンティ**

ティレルム（Identity Realm）] を選択し、レルムを編集して（変更は不要）、保存します。その後、展開します。

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 ～ 6.2.2.x

直接アップグレード先：バージョン 6.2.3 ～ 6.4.0

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。

アップグレード後にアクセス コントロール ポリシーを編集/再保存する

展開：すべて

アップグレード元：バージョン 6.1 ～ 6.2.2.x

直接アップグレード先：バージョン 6.2.3 のみ

侵入ポリシーの変数セットでのみ使用されるネットワークまたはポート オブジェクトを設定している場合、アップグレード後にアクセス コントロール ポリシーに関連付けられている展開が失敗します。これが発生する場合、アクセス コントロール ポリシーを編集し、（説明の編集などの）変更、保存、および再展開を行います。

レポートの結果の制限の変更

展開：Firepower Management Center

アップグレード元：バージョン 6.1.0 ～ 6.2.2.x

直接アップグレード先：バージョン 6.2.3 ～ 6.4.0

バージョン 6.2.3 では、次のように、使用できる結果の数、またはレポートのセクションに含めることができる結果の数が制限されています。テーブルおよび詳細ビューでは、PDF レポートに HTML または CSV レポートよりも少ないレコードを含めることができます。

表 *12 :* レポートの結果の新しい制限

レポート セクション タイプ	最大レコード数：HTML または CSV レポート セクション	最大レコード数：PDF レポート セクション
棒グラフ 円グラフ	100（上位または下位）	100（上位または下位）
テーブル ビュー	400,000	100,000
詳細ビュー	1,000	500

Firepower Management Center をアップグレードする前に、レポート テンプレート内のセクションで最大 HTML または CSV よりも大きい結果数を指定する場合は、アップグレード プロセスが設定を新しい最大値に下げます。

PDF レポートを生成するレポート テンプレートの場合、テンプレート セクションの PDF の制限を超えると、アップグレード プロセスは出力形式を HTML に変更します。PDF の生成を続行するには、結果数を PDF の最大に下げます。アップグレード後にこれを行った場合、出力形式の設定を PDF に戻します。

アップグレードの前にバージョン6.1.xFTDクラスタからサイトIDを削除

展開： Firepower Threat Defenseクラスタ

アップグレード元：バージョン 6.1.x

直接アップグレード先：バージョン 6.2.3 ～ 6.4.0

Firepower Threat Defense バージョン 6.1.x クラスタは、サイト間クラスタリングをサポートしていません（バージョン 6.2.0 以降では FlexConfig を使用してサイト間機能を設定できます）。

FXOS 2.1.1 でバージョン 6.1.x クラスタを展開または再展開している場合、（サポートされていない）サイト ID の値を入力しているときは、アップグレードする前に、FXOS の各ユニットでサイト ID を削除（0 に設定）する必要があります。そうしないと、アップグレード後、ユニットがクラスタに再度参加できなくなります。

すでにアップグレード済みの場合は、サイト ID を各ユニットから削除してからクラスタを再確立します。サイト ID を表示または変更するには、『Cisco FXOS CLI Configuration Guide』を参照してください。

以前に公開されたガイドライン

このチェックリストには、中間リリースに適用されるアップグレードガイドラインが含まれています。現在**バージョン 6.1 ～ 6.2.1** を実行している場合は、次のガイドラインを確認してください。

表 *13 :* 以前に公開されたバージョン *6.2.3* のガイドライン

✓	ガイドライン	プラットフォーム	アップグレード元	直接アップグレード先
	アップグレードの失敗：FDM を実行する ASA 5500-X シリーズのバージョン 6.2.2.5 から （41 ページ）	FDM を使用した FTD	6.2.0 のみ	6.2.2 ～ 6.4.0
	アクセス コントロールでは SRU から遅延ベースのパフォーマンス設定を取得可能 （41 ページ）	FMC	6.1.0.x	6.2.0 ～ 6.4.0
	FTD での「フェールセーフ」から「Snort フェール オープン」への置き換え （42 ページ）	FMC を使用した FTD	6.1.0.x	6.2.0 ～ 6.4.0

アップグレードの失敗：FDM を実行する ASA 5500-X シリーズのバージョン 6.2.2.5 から

展開：FDM を使用した FTD（メモリが少ない ASA 5500-X シリーズ デバイスで実行）

アップグレード元：バージョン 6.2.0

直接アップグレード先：バージョン 6.2.2 ～ 6.4.0

バージョン 6.2.0 からアップグレードする場合、アップグレードに失敗し、「`Uploaded file is not a valid system upgrade file`」というエラーが表示される可能性があります。これは、正しいファイルを使用している場合でも発生する可能性があります。

この場合は、次の回避策を試してください。

- 再度お試しください。
- CLI を使用してアップグレードする。
- まず 6.2.0.1 にアップグレードする。

アクセスコントロールではSRUから遅延ベースのパフォーマンス設定を取得可能

展開：FMC

アップグレード元：6.1.x

直接アップグレード先：6.2.0+

バージョン 6.2.0+ の新しいアクセス コントロール ポリシーでは、デフォルトで、最新の侵入ルール更新（SRU）から遅延ベースのパフォーマンス設定が取得されます。この動作は、新し

い [設定の適用元（Apply Settings From）] オプションによって制御されます。このオプションを設定するには、アクセス コントロール ポリシーを編集または作成して、[詳細設定（Advanced）] をクリックし、遅延ベースのパフォーマンス設定を編集します。

バージョン 6.2.0+ にアップグレードすると、現在（バージョン 6.1.x）の設定に従って新しいオプションが設定されます。現在の設定が次の場合、新しいオプションは次のように設定されます。

- [デフォルト（Default）]：新しいオプションは、[インストールされたルールの更新（Installed Rule Update）] に設定されます。アップグレードしてから展開すると、最新の SRU からの遅延ベースのパフォーマンス設定が使用されます。最新の SRU が指定する内容によって、トラフィックの処理が変更される可能性があります。
- [カスタム（Custom）]：新しいオプションは、[カスタム（Custom）] に設定されます。システムは現在のパフォーマンス設定を保持します。このオプションによって動作が変更されることはありません。

アップグレードする前に設定を確認することをお勧めします。前述したように、バージョン 6.1.x の FMC Web インターフェイスから、ポリシーの遅延ベースのパフォーマンス設定を表示し、[Revert To Defaults] ボタンがグレー表示されているかどうかを確認します。ボタンがグレー表示されている場合は、デフォルト設定が使用されています。ボタンがアクティブになっている場合は、カスタム設定が設定されています。

FTDでの「フェールセーフ」から「Snortフェールオープン」への置き換え

展開：FMC を使用した FTD

アップグレード元：バージョン 6.1.x

直接アップグレード先：バージョン 6.2 以降

バージョン 6.2 では、Snort フェール オープン設定により、FMC によって管理される Firepower Threat Defense デバイスのフェールセーフ オプションが置き換えられます。フェールセーフでは、Snort がビジー状態のときにトラフィックをドロップすることができますが、Snort がダウンしている場合、トラフィックはインスペクションなしで自動的に通過します。Snort フェール オープンでは、このトラフィックをドロップすることができます。

FTD デバイスをアップグレードすると、その新しい Snort フェール オープン設定は、以下のように、古いフェールセーフ設定に依存します。新しい設定ではトラフィックの処理が変更されることはありませんが、アップグレードの前にフェールセーフを有効または無効にするかどうかを検討してください。

表 *14 :* フェールセーフの *Snort* フェール オープンへの移行

バージョン 6.1 のフェールセーフ	バージョン 6.2 の Snort フェール オープン	動作
無効（デフォルトの動作）	[Busy]：無効 [Down]：有効	Snort プロセスがビジー状態の場合は、新規および既存の接続をドロップし、Snort プロセスがダウンしている場合は、接続をインスペクションなしで通過します。
有効	[Busy]：有効 [Down]：有効	Snort プロセスがビジー状態またはダウンしている場合、新規または既存の接続をインスペクションなしで通過します。

Snort フェール オープンでは、デバイスにバージョン 6.2 が必要であることに注意してください。バージョン 6.1.x のデバイスを管理している場合、FMC Web インターフェイスにフェールセーフ オプションが表示されます。

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 （62 ページ）」）を参照してください。

表 *15 : 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。
	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。	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（35 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 （51 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 （48 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

次のように Version6.2.3 に直接アップグレードできます。特定のパッチレベルを実行する必要はありません。

表 *16 : Firepower* ソフトウェアをバージョン *6.2.3* にアップグレードするための最小バージョン

プラットフォーム	最小バージョン
Firepower Management Center	6.1.0
FMC を使用した Firepower デバイス	6.1.0 FXOS 2.3.1.73 以降のビルド（Firepower 4100/9300 に必要）。
FDM を搭載した Firepower デバイス	6.2.0
ASDM を使用した ASA FirePOWER	6.2.0

時間テストとディスク容量の要件

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

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

時間テストについて

ここで指定した時間の値は、社内のテストに基づいています。

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

テスト条件

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

  ハイアベイラビリティの構成またはクラスタ化された構成では、動作の継続性を保持するため、複数のデバイスは 1 つずつアップグレードされます。アップグレード中は、各デバイスはメンテナンス モードで動作します。そのため、デバイス ペアまたはクラスタ全体のアップグレードには、スタンドアロンデバイスのアップグレードよりも長い時間がかかります。 スタック構成の 8000 シリーズ デバイスは同時にアップグレードされ、スタックは、すべてのデバイスのアップグレードが完了するまで、限定的なバージョン混在の状態で動作することに注意してください。これには、スタンドアロンデバイスのアップグレードと比べて大幅に長い時間がかかるということはありません。
- 構成：構成とトラフィック負荷が最小限のアプライアンスでテストします。

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

時間はアップグレードのみを対象

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

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

ディスク容量の要件について

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

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

バージョン 6.2.3 の時間とディスク容量

表 *17 :* バージョン *6.2.3* 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	時間
FMC	6.1.0 から：7415 MB 6.2.0 から：8863 MB 6.2.1 から：8263 MB 6.2.2 から：11860 MB	6.1.0 から：17 MB 6.2.0 から：24 MB 6.2.1 から：23 MB 6.2.2 から：24 MB	—	6.1.0 から：38 分 6.2.0 から：43 分 6.2.1 から：37 分 6.2.2 から：37 分
FMCv	6.1.0 から：7993 MB 6.2.0 から：9320 MB 6.2.1 から：11571 MB 6.2.2 から：11487 MB	6.1.0 から：23 MB 6.2.0 から：28 MB 6.2.1 から：24 MB 6.2.2 から：24 MB	—	ハードウェアによって異なる
Firepower 2100 シリーズ	6.2.1 から：7356 MB 6.2.2 から：11356 MB	6.2.1 から：7356 MB 6.2.2 から：11356 MB	1000 MB	6.2.1 から：15 分 6.2.2 から：15 分

Platform	ボリュームの容量	必要容量	FMC の容量	時間
Firepower 4100/9300 シャーシ	6.1.0 から：5593 MB 6.2.0 から：5122 MB 6.2.2 から：7498 MB	6.1.0 から：5593 MB 6.2.0 から：5122 MB 6.2.2 から：7498 MB	795 MB	6.1.0 から：10 分 6.2.0 から：12 分 6.2.2 から：15 分
FTD を搭載した ASA 5500-X シリーズ	6.1.0 から：4322 MB 6.2.0 から：6421 MB 6.2.2 から：6450 MB	6.1.0 から：.088 MB 6.2.0 から：.092 MB 6.2.2 から：.088 MB	1000 MB	6.1.0 から：54 分 6.2.0 から：53 分 6.2.2 から：50 分
FTDv	6.1.0 から：4225 MB 6.2.0 から：5179 MB 6.2.2 から：6450 MB	6.1.0 から：.076 MB 6.2.0 から：.092 MB 6.2.2 から：.092 MB	1000 MB	ハードウェアによって異なる
Firepower 7000/8000 シリーズ	6.1.0 から：5145 MB 6.2.0 から：5732 MB 6.2.2 から：6752 MB	6.1.0 から：18 MB 6.2.0 から：18 MB 6.2.2 から：18 MB	840 MB	6.1.0 から：29 分 6.2.0 から：31 分 6.2.2 から：31 分
ASA FirePOWER	6.1.0 から：7286 MB 6.2.0 から：7286 MB 6.2.2 から：10748 MB	6.1.0 から：16 MB 6.2.0 から：16 MB 6.2.2 から：16 MB	6.1.0 から：1200 MB 6.2.0 から：1200 MB	6.1.0 から：94 分 6.2.0 から：104 分 6.2.2 から：96 分
NGIPSv	6.1.0 から：4115 MB 6.2.0 から：5505 MB 6.2.2 から：5871 MB	6.1.0 から：18 MB 6.2.0 から：19 MB 6.2.2 から：19 MB	741 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 *18 : 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。

導入	方法	トラフィックの動作
シャーシ内クラスタ（Firepower 9300 のみ）	ハードウェアバイパス有効：[Bypass: Standby] または [Bypass-Force]。（6.1 以降）	検査なしで受け渡される。
	ハードウェアバイパス無効：[Bypass: Disabled]。（6.1 以降）	少なくとも 1 つのモジュールがオンラインになるまでドロップされる。
	ハードウェア バイパス モジュールなし。	少なくとも 1 つのモジュールがオンラインになるまでドロップされる。

スタンドアロン 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 *19 : 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]（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 *20 : 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 *21 : 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]（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 *22 : 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。

FirePOWER 7000/8000 シリーズのアップグレード時の動作

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

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

インターフェイスの構成により、アップグレード中に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 *23 :* アップグレード中のトラフィックの動作：スタンドアロン *7000/8000* シリーズ

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

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

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

最初にアップグレードするピアは、展開によって異なります。

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

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

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

展開時のトラフィックの動作

アップグレード プロセス中には、設定を複数回展開します。Snort は、通常、アップグレード直後の最初の展開時に再起動されます。展開の前に、特定のポリシーまたはデバイス設定を変更しない限り、それ以外の展開時に再起動されることはありません。詳細については、『Firepower Management Center 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 *24 :* 展開時のトラフィックの動作：*7000/8000* シリーズ

インターフェイス 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
ルーテッド、スイッチド	切断

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

トラフィック リダイレクションのポリシー	トラフィックの動作
フェール オープン（**sfr fail-open**）	インスペクションなしで転送
フェール クローズ（**sfr fail-close**）	ドロップされる
モニタのみ（**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 *26 : NGIPSv* アップグレード中のトラフィックの動作

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

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

展開時のトラフィックの動作

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

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

表 *27 : 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 *28 : 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

タスク	ガイド
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
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
- FirePOWER 7000 シリーズ：https://www.cisco.com/go/7000series-software
- FirePOWER 8000 シリーズ：https://www.cisco.com/go/8000series-software
- ASA with FirePOWER Services（ASA 5500-X シリーズ）：https://www.cisco.com/go/asa-firepower-sw
- 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_Upgrade-6.6.0-90.sh.REL.tar`
- プラットフォーム： Firepower Management Center
- パッケージタイプ：アップグレード
- バージョンおよびビルド：6.6.0-90
- 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 *29 : Firepower* ソフトウェア アップグレード パッケージ

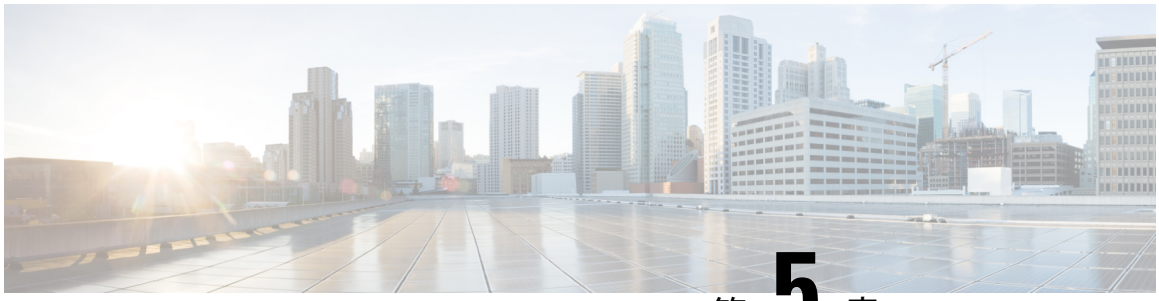
プラットフォーム	パッケージ
FMC/FMCv	Sourcefire_3D_Defense_Center_S3

プラットフォーム	パッケージ
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
Firepower 7000/8000 シリーズ AMP モデル	Sourcefire_3D_Device_S3
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

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 *30 :* 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 *31 : 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 *32 : Firepower Management Center* のインストール手順

FMC プラットフォーム	ガイド
FMC 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

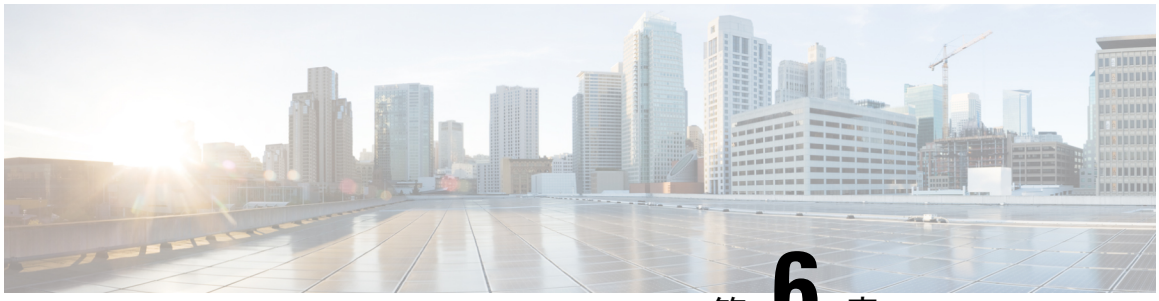
表 *33 : Firepower Threat Defense* のインストール手順

FTD プラットフォーム	ガイド
Firepower 2100 シリーズ	Cisco ASA and Firepower Threat Defense Reimage Guide Cisco FXOS トラブルシューティングガイド（Firepower Threat Defense を実行している Firepower 1000/2100 シリーズ向け）
Firepower 4100/9300 シャーシ	Cisco Firepower 4100/9300 FXOS Configuration Guides：イメージ管理に関する章 Cisco Firepower 4100 スタートアップガイド Cisco Firepower 9300 Getting Started Guide
ASA 5500-X シリーズ	Cisco ASA and Firepower Threat Defense Reimage Guide
ISA 3000	Cisco ASA and Firepower Threat Defense Reimage Guide
FTDv: VMware	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 *34 : FirePOWER 7000/8000* シリーズ、*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
Firepower 7000 シリーズ	Cisco Firepower 7000 Series Getting Started Guide：*Restoring a Device to Factory Defaults*
Firepower 8000 シリーズ	Cisco Firepower 8000 Series Getting Started Guide：*Restoring a Device to Factory Defaults*
NGIPSv	Cisco Firepower NGIPSv 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 6 章

資料

Firepower のマニュアルについては、次を参照してください。

- 新規および更新されたドキュメント （77 ページ）
- ドキュメント ロードマップ （79 ページ）

新規および更新されたドキュメント

次の Firepower ドキュメントが更新されたか、 今回のリリースで新たに利用可能になっています。 他の Firepower マニュアルへのリンクについては、ドキュメント ロードマップ （79 ページ） を参照してください。

コンフィギュレーション ガイド

- Firepower Management Center Configuration Guide, Version 6.2.3とオンライン ヘルプ
- Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager, Version 6.2.3 とオンライン ヘルプ
- ASA with FirePOWER Services Local Management Configuration Guide, Version 6.2.3
- Cisco Firepower Threat Defense コマンド リファレンス

FXOS Configuration Guides and Release Notes

- Cisco Firepower 4100/9300 FXOS Firepower Chassis Manager 2.3(1) コンフィギュレーション ガイド
- Cisco Firepower 4100/9300 FXOS 2.3(1) CLI コンフィギュレーション ガイド
- Cisco Firepower 4100/9300 FXOS Release Notes, 2.3(1)

アップグレード ガイド

- Cisco Firepower Management Center Upgrade Guide
- Cisco ASA Upgrade Guide

ハードウェア設置ガイド

- Cisco Firepower 2100 シリーズ ハードウェア設置ガイド
- Cisco ISA 3000 Industrial Security Appliances Hardware Installation Guide

Quick Start/Getting Started Guides

- **Firepower 2100**

  Cisco Firepower Threat Defense for the Firepower 2100 Series Using Firepower Management Center Quick Start Guide

  Cisco Firepower Threat Defense for the Firepower 2100 Series Using Firepower Device Manager Quick Start Guide

- **ISA 3000**

  Cisco ASA for the ISA 3000 Series Quick Start Guide

  Cisco Firepower Threat Defense for the ISA 3000 Using Firepower Management Center Quick Start Guide

  Cisco Firepower Threat Defense for the ISA 3000 Using Firepower Device Manager Quick Start Guide

- **Firepower Threat Defense Virtual**

  Cisco Firepower Threat Defense Virtual for VMware Getting Started Guide

  Cisco Firepower Threat Defense Virtual for KVM スタートアップガイド

移行ガイド

- Cisco ASA to Firepower Threat Defense Migration Guide, Version 6.2.2

API および統合ガイド

- Firepower Management Center REST API Quick Start Guide, Version 6.2.3
- Cisco Firepower Threat Defense REST API Guide
- Firepower System Event Streamer Integration Guide, Version 6.2.3

互換性ガイド

- Cisco Firepower Compatibility Guide
- Cisco ASA Compatibility Guide
- Cisco FXOS Compatibility Guide

ライセンスおよびオープン ソース

- 『Cisco Firepower System Feature Licenses」』

- Frequently Asked Questions (FAQ) about Firepower Licensing
- Open Source Used in Firepower System Version 6.2.3

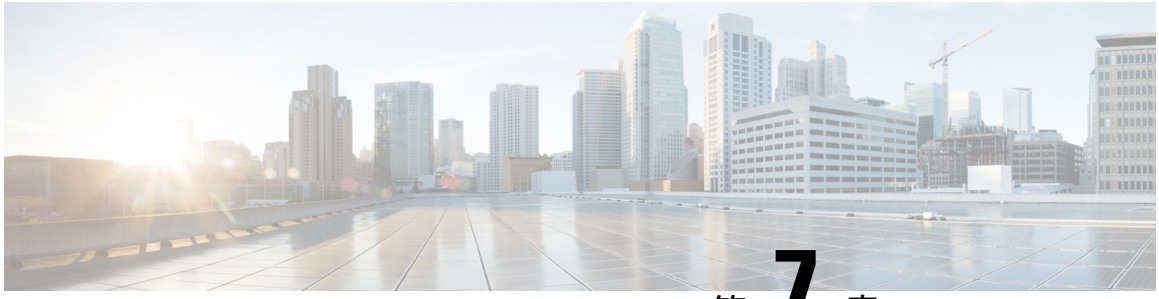
トラブルシューティングおよび設定の例

- Cisco Firepower Threat Defense Syslog メッセージ
- 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）

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 7 章

解決済みの問題

便宜上、これらのリリースノートには、このバージョンの解決済みのバグが記載されています。

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

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 （81 ページ）
- 新しいビルドで解決済みの問題 （82 ページ）
- バージョン 6.2.3 で解決済みの問題 （83 ページ）

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 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 *35* : バージョン *6.2.3* の新しいビルド

新しいビルド	リリース日	プラットフォーム：アップグレード	プラットフォーム：再イメージ化	解決済み
113	2020 年 6 月 1 日	FMC/FMCv	FMC/FMCv	CSCvr95287：Cisco Firepower Management Center LDAP 認証バイパスの脆弱性 以前のビルドを実行している場合は、 ホットフィックス DO を適用します。
111	2019 年 11 月 25 日	—	FTDv: AWS, Azure	Cisco TAC にお問い合わせください。
110	2019 年 6 月 14 日	—	—	CSCvn78174：Cisco ASA ソフトウェアおよび Cisco FTD ソフトウェア TCP タイマー処理におけるサービス妨害の脆弱性
99	2018 年 9 月 7 日	—	—	Cisco TAC にお問い合わせください。
96	2018 年 7 月 26 日	—	—	Cisco TAC にお問い合わせください。
92	2018 年 7 月 5 日	—	—	CSCvk06176：実行ファイルが誤っているため SSEConnector が起動しない

新しいビルド	リリース日	プラットフォーム：アップグレード	プラットフォーム：再イメージ化	解決済み
88	2018 年 6 月 11	—	—	CSCvj13327：6.2.3 へのアップグレードが 600_schema/100_update_database.sh で失敗し、oom killer が呼び出された
85	2018 年 4 月 9 日	—	—	Cisco TAC にお問い合わせください。
84	2018 年 4 月 9 日	Firepower 7000/8000 NGIPSv	—	CSCvi74560：6.2.3 が変数セットに変数を正しく展開せず、展開が失敗する CSCvi74623：6.2.3 アップグレードによって home_net 変数がデフォルトの「any」にリセットされる CSCvi77527：インストール後のデータベース整合性チェックエラーで 6.2.3 へのアップグレードが失敗する
83	2018 年 4 月 2 日	FTD/FTDv ASA FirePOWER	FTD：物理プラットフォーム FTDv：VMware、FVM Firepower 7000/8000 ASA FirePOWER NGIPSv	Cisco TAC にお問い合わせください。

バージョン 6.2.3 で解決済みの問題

表 *36 :* バージョン *6.2.3* で解決済みの問題

不具合 ID	タイトル
CSCuw57184	キャッシュ内の URL エントリが無期限に保持されない
CSCuw73747	ヨーロッパ/イスタンブールのタイム ゾーンの DST が異なる日付に適用されている

不具合 ID	タイトル
CSCux17501	SSL インスペクションでは、3072 ビット キーの RSA 証明書を持つサイトの復号化エラーがあるトラフィックがブロックされる
CSCux42313	Cisco ASA モジュールのキャプティブ ポータルのリダイレクトがスタックしている
CSCux61395	センサーへのストリーミング中にエラーが発生するとユーザ ID が失われる
CSCuy10223	アクティブ認証アイデンティティ ルールで ASA セキュリティ ゾーンを使用できない
CSCuy18154	SFDataCorrelator でセッションを受信する前に、ADISubscriber がシャットダウンする
CSCuy21943	バックアップの復元後、Firepower Threat Defense を展開できない
CSCuy56306	SCP ではリモート サーバへのバックアップ中にタイム アウトして失敗することが予期される
CSCuy57310	Cisco 適応型セキュリティ アプライアンスのトラフィック フローの機密性におけるサービス拒否攻撃に対する脆弱性
CSCuz09515	アクティブ/パッシブ認証が事前定義済みオブジェクトで機能しない
CSCuz85967	新たに追加された管理インターフェイスに「管理専用」設定がない
CSCuz92983	Lag インターフェイスのモード 10 ギガビット全二重でポリシーの展開が失敗する
CSCva21702	トラフィック キャプチャの BPF 検証
CSCva34909	DNS ブラックリストには 81 文字の制限がある
CSCva36446	SSL ハンドシェイクの成功直後に ASA が Anyconnect セッションの受け入れを停止するか、または接続を終了する
CSCva44278	孤立したデータベース オブジェクトが原因でポリシーの適用が失敗する
CSCvb13949	VDB の更新では、準備状況チェック オプションを有効にしてはならない
CSCvb28202	PlatformSettings オブジェクトの DB 整合性チェックにおける誤警告
CSCvc03899	Management Center によって管理される Firepower Threat Defense：/ngfw での管理対象外ディスクの使用率が高い
CSCvc37876	バックエンドのプライマリ Threat Defense デバイス ペアの不整合が原因でポリシーの展開が失敗する

不具合 ID	タイトル
CSCvc44535	まれな状況下では、キャプティブ ポータルが非常に遅くなり、応答しないことがある
CSCvc48180	バージョン 6.1 または 6.2.1 ではアプリケーション カテゴリとタグが欠落している
CSCvc48768	[Search] オプションが NAP エディタのネットワーク オブジェクトに対して機能しない
CSCvc50598	2 つのリビジョン間の侵入ポリシーの比較レポートが正しく機能していない
CSCvc55341	パケット ビューからイベントを確認しようとしたときの断続的なエラー 500
CSCvc56921	syslog を無効にするなど、ロギング設定を変更すると、IPS およびファイル ポリシーが無効になる
CSCvc65909	ASDM：アクセス コントロール ポリシーをインポートすると、オブジェクトの重複が発生する
CSCvc77913	更新時に SFDataCorrelator のカスタム設定をチェックする必要があり、そうしないと、SFDataCorrelator がダウンしたままになる可能性がある
CSCvc84585	Firepower センサーが EAP チェーンを使用して ISE からユーザを取り込まない
CSCvc91092	Cisco FireSIGHT システム ソフトウェアにおける任意のコード実行の脆弱性
CSCvc92934	SSL 復号が有効になっている場合、アクセス コントロール ポリシーの URL 制約が正しく適用されない
CSCvd19749	000_start/113_EO_integrity_check で 6.1.0 から6.1.0.1 にアップグレードすることに失敗した
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
CSCvd29303	仮想 ASA 5500-X シリーズでは、ディスク ステータス ヘルス モニタリングを無効にする必要がある
CSCvd32767	IPS ルール内のオブジェクトを使用できない
CSCvd35049	QueryEngine およびレポート生成の失敗を防ぐために、ハードコードされたクエリの制限が必要

不具合 ID	タイトル
CSCvd39729	Firepower エンタープライズ オブジェクトの参照先がないため複数の問題が発生する
CSCvd51066	URL クラウド ルックアップに未分類の URL カテゴリがある
CSCvd59044	アクセス コントロール ポリシーが HTTPS トラフィックの URL SI リストの条件に一致しない
CSCvd59268	cli_firstboot ウィザードからデータ インターフェイスと Firepower Management Center を使用できる
CSCvd61462	DNS フィードまたは DNS リストに単一の単語のエントリが含まれている場合の DNS クエリの部分一致
CSCvd72150	削除されたオブジェクトが、Management Center UI の変数セットに追加できると表示され続ける
CSCvd83845	Firepower Management Center で SafeSearch ルールが無効になっている場合でも、SafeSearch 固有のコードがヒットする
CSCvd84471	メモリの問題が原因で、セキュリティ インテリジェンスによって接続がブラックリストに載せられない
CSCvd91889	インターフェイスの論理名を変更したり、サブインターフェイスを追加したりできない
CSCve00330	ハイ アベイラビリティの Firepower Management Center 間で実行される同期の詳細を文書化する
CSCve03600	SMTP トラフィックが早期に SafeSearch ルールに到達する
CSCve11879	ハイ アベイラビリティのスイッチオーバー中に Ping トラフィックが 1 分間ドロップされる
CSCve12096	手動 NAT ルールで使用されるポートオブジェクトの削除中に障害が発生する
CSCve17433	AWS Firepower Management Center でのポリシー展開の失敗
CSCve23827	復元デバイスでクロックの時間が遅れていると、バックアップからの復元が失敗する
CSCve31929	Firepower Management Center では、セキュリティ ゾーンの使用時にネットワーク検出データが表示されない
CSCve42340	URL データベースの更新では HTTP ヘッダーでプロキシ接続用の IP が使用される

不具合 ID	タイトル
CSCve42379	スケール：同様の保留中のタスクがすでに存在する場合、Sync Sybase to MySQL タスクのキューイングを回避する
CSCve42542	ハイ アベイラビリティの作成中にセカンダリ ピアとして Firepower Threat Defense を選択することはできない
CSCve45573	日本語環境でのアクセス コントロール ポリシーのロード中に内部エラー メッセージが表示される
CSCve48087	[Deploy policy] タブでは、Firepower Management Center からデバイス リストを入力できない
CSCve49433	Threat Defense プラットフォーム設定ポリシーで NTP 入力値が正しくチェックされない
CSCve49546	「FINALIZE」でポリシー適用が失敗すると、以降のポリシー適用が成功することはない
CSCve49643	ダブル バイト文字を使用したユーザ ログインが Firepower Management Center に正しく記録されない
CSCve49722	侵入ポリシーが親ドメインから侵入レイヤを継承している場合、エクスポートできない
CSCve49778	Threat Defense ICMP プラットフォーム設定の複数のインターフェイスがあるセキュリティ ゾーンが適切に処理されない
CSCve55618	すでに生成された応答に対して DNS ポリシーが DNS 応答を生成する（応答が回線上で検出された場合）
CSCve56743	Firepower Threat Defense ペア：信頼ルールがあるにもかかわらず、Snort がトラフィックをドロップする
CSCve57521	NGFW ルールの処理では、フローの最初のパケットを常に使用してイニシエータの方向が決定される
CSCve57858	[Do not decrypt] アクションが適用されている場合でも、大きな証明書を持つサイトがロードされない（SSL ポリシーがオンの状態で）
CSCve60167	アップグレードフレームワークで、オンボックススクリプト NEVER_SKIP の確認が必要
CSCve61540	Cisco 適応型セキュリティ アプライアンスのアプリケーション レイヤ プロトコルのインスペクションにおける DoS に対する脆弱性
CSCve73129	6.2.1 へのアップグレードが失敗すると DB クエリが終了しない
CSCve77286	侵入ポリシー ルール フィルタが正常に動作していない

不具合 ID	タイトル
CSCve79555	キャプチャをクリアするときの ASA/Threat Defense のトレースバック（assertion 0 failed: mps_hash_table_debug ファイル）
CSCve84791	asp-drop をキャプチャすると、予期しない ASA 障害が発生する
CSCve87945	新しい https 証明書をインストールできない
CSCve88764	プライマリ Firepower Management Center のバックアップをセカンダリに復元しない
CSCve90384	セカンダリプラットフォームがアクティブのとき、2100プラットフォームでハイアベイラビリティの中断/設定の展開が失敗する
CSCve98443	ユーザ アイデンティティ カウントのトラッキングが正しくない可能性がある
CSCve98877	ダッシュボード ドリルダウンがトップ レベル レポートと一致しない
CSCve99511	ユニットがアクティブロールを引き継ぐとき、スレッド名：sfr-vpn-status-watcher でトレースバックとリロードが発生する
CSCve99818	接続イベントの時間枠設定が、異なる範囲にリセットされる
CSCvf01839	アイドル時間の経過後、「不正なアクションが検出されました」として vFMC がログアウトされる
CSCvf04102	[Vulnerabilities] セクションのレポートプレビューの生成中にエラーが発生する
CSCvf06031	セカンダリ Firepower Threat Defense をクラスタに追加すると、展開が失敗する可能性がある
CSCvf12392	相関ポリシーからのアラート応答でセキュリティインテリジェンスのカテゴリが正しくない可能性がある
CSCvf12828	QP FTD HA ペアのアプリケーション同期の問題が原因で、デバイスが HA 状態でスタックしてプロセスが失敗する
CSCvf15067	デバイスが Firepower Management Center（マネージャなしで）によって管理されている場合の ASA へのホスト名の同期
CSCvf18641	ND ルールのモニタ対象外ホストに対して接続イベントが生成されない
CSCvf18966	拡張アクセス コントロール エントリにポート グループ オブジェクトを追加すると、ERROR: Invalid Protocol が発生する
CSCvf25032	FMC：sydb.out の所有権が root に変更され、vmsDbEngine/dbsrv16 が起動しなくなる

不具合 ID	タイトル
CSCvf25058	Firepower Threat Defense セキュリティ インテリジェンスの DNS メモリ容量がヘルス アラートを超過した
CSCvf25444	SSL ポリシー条件でレルムをコピーしてユーザを置き替えると、ポリシーが破損する
CSCvf27979	「終了値が開始値より小さい」というエラーが表示され、アクセス コントロール ポリシーを表示できない
CSCvf34791	ASA with Firepower Services での 6.2.2 ～ 1290 のインストール：ASA が予期せず失敗する
CSCvf35266	接続プロファイルからグループポリシーの割り当てを解除し、[Advanced] タブで削除すると、展開に失敗する
CSCvf41793	threshold. conf ファイルがプルーニングされていないときの、ids_event_processor/ids_event_alerter の高メモリ使用率
CSCvf42199	snort 再起動の自動回帰スイートの実行中にコアが 14 時間以上表示される。
CSCvf45952	アプリケーション同期の失敗によりペアが再起動されたときに、セカンダリのハイ アベイラビリティの進行に失敗した
CSCvf46168	「no capture < name > stop」でキャプチャ ステータスが Stopped から変更されない
CSCvf46886	セキュリティ アナリストのユーザ ロールでマルウェア イベントからファイルをダウンロードできない
CSCvf49737	H323 ポリシー インスペクション マップで state-checking オプションを追加する
CSCvf53734	Firepower Management Center UI でのアクセス コントロール ルールとカテゴリの重複
CSCvf55897	[Access Policy] ページの [Default action] で侵入ポリシー コントロールを無効にする
CSCvf56476	Firepower 2120 デバイスで LDAPS を有効にした後、DNS Flexconfig が削除される
CSCvf56533	Firepower 9300 クラスタを別の Firepower Management Center に再登録できない
CSCvf57862	Snort のインストールがサイレントに失敗し、Snort がインストールされた後の自動展開がスキップされる
CSCvf60738	RPC コールの失敗が原因で Elektra の登録に失敗する

不具合 ID	タイトル
CSCvf61157	Firepower Management Center DB が破損した場合の名前の不一致
CSCvf64643	Firepower Threat Defense デバイスでのエラー：キャプティブポータル ポートが使用できない。もう一度やり直してください
CSCvf64882	クラスタ保留要求が ASA によってタイム アウトされたため、ハイ アベイラビリティ ペアで展開が失敗する
CSCvf64914	ローカル URL フィルタリング データベースおよび/またはクラウドの性質の更新では、キャッシュされたデータを置き換える必要がある
CSCvf65014	[Intrusion Events] 分析のカスタム [End Time] を使用すると、イベントがない空白ページが返される
CSCvf65226	Firepower Threat Defense デバイスで OSPF Redistribution コマンドが削除されない
CSCvf65245	モニタ ルールが大きなセッション（ファイル転送など）をログに記録しない
CSCvf68502	証明書署名要求でホスト名の FQDN を割り当てることができない
CSCvf71365	空の VDB テーブルが原因で起動中に SFDataCorrelator が終了する場合、適切なメッセージがログに記録される
CSCvf73465	デバイスの削除後に ID_MAPPING テーブルに古いエントリがあるため、再登録に失敗した
CSCvf74023	Management Center でプロキシ認証が設定されている場合、スマート ライセンスの登録が失敗する
CSCvf74113	ルールのしきい値の秒数が 00、08、09 に設定されている場合、Firepower 侵入ルールの UI ポリシーの展開が失敗する
CSCvf75062	展開が「エラー：トラストポイントが登録されていない」で失敗した
CSCvf77836	FTD HA：HA 中断が実行されると、両方のデバイスが不明な状態になる
CSCvf78629	カスタムフィンガープリント GUI で、[Firepower Management Center] オプションではなく、[Defense Center] オプションが表示される
CSCvf81725	syncd のメモリ使用量が多いため、firewall_rule_cache テーブルをロードすると終了する
CSCvf82315	GUI から 10G インターフェイスの IP アドレスを変更できない。
CSCvf91371	SSL 復号・再署名ルールに内部 CA を使用すると、無効な証明書のエラーが発生する

不具合 ID	タイトル
CSCvf95633	Management Center：インターフェイスの「mac-address-table」コマンドが Firepower Threat Defense に送信されない
CSCvf98386	アップグレード後に FDM 事前共有キーがランダムな値に変更された
CSCvg02051	グループ名が ASCII でない場合のエントリ重複による大きなユーザ/グループ テーブル
CSCvg03671	Snort による SI データのロード試行が複数回失敗したことが原因で、FMC ポリシーの展開が遅くなる
CSCvg04309	TCAM が原因のマイクロエンジンの障害は、自動トラブルシューティングを生成しない bb-health につながる
CSCvg06811	captive_portal.log を logrotate.d に追加する
CSCvg09316	Cisco Firepower Threat Defense ソフトウェアのポリシーバイパスの脆弱性
CSCvg20782	Oracle MySQL パッチの更新から CVE に関連付けられた脆弱性が特定された
CSCvg21939	Firepower Management Center GUI の一部が Firefox 56 でロードされない
CSCvg23945	ASA panic/crash spin_lock_fair_mode_enqueue：ロック（mps_shash_bucket_t）が長期間にわたって保持されている
CSCvg24416	Firepower 4100 シリーズでは、FTW インライン インターフェイスがハードウェア バイパスに移行しない
CSCvg24892	6.2.3 エラー：SMTP：Could not allocate SMTP mempool。
CSCvg27431	AWS 6.2.2.1 で大規模なアクセス コントロール ポリシーの適用に失敗する
CSCvg27511	ネットワークオブジェクト：既存のオブジェクトを削除しようとすると「エントリが見つかりません」というエラーが表示される
CSCvg27590	日別変更調整レポートに Firepower 6.2.2 の詳細とユーザがない
CSCvg29442	IPSec が有効になっている場合、高可用性が Active-Failed の状態になる。
CSCvg29791	FlexConfig：システム変数にサブインターフェイス ID を含める必要がある
CSCvg30947	同じメトリックを持つ複数のデフォルト ルートが、Threat Defense デバイスのルーティング テーブルで許可される
CSCvg32590	6.1 から 6.2.3 へのアップグレード：FTD のアップグレードが、アクセスエラーにより /ngfw/var/lib/mysql/sfsnort で失敗した

不具合 ID	タイトル
CSCvg37391	移行したアクセス コントロール ポリシーの展開は、FQDN オブジェクトがあるため失敗する
CSCvg37456	アクティブ ユニットでハイ アベイラビリティ ペアへの展開が成功し、スタンバイ ユニットが更新されますというメッセージ
CSCvg38612	FDM で 6.2.0 から 6.2.3-10646 へのアップグレードに失敗する
CSCvg38789	オブジェクトの展開時にネストされたエンティティが削除されない
CSCvg39981	Firepower Management Center で Firepower Threat Defense のクラスタ名が正しく表示されない
CSCvg43759	URL フィルタの照合に失敗する：2 つの SSL 証明書 CN が連結される
CSCvg45236	高速パス事前フィルタ SSL ポリシーを使用した、予想よりも少ない 256 バイト ブロック数
CSCvg46466	Cisco FMC および Firepower システムソフトウェアの SF トンネル制御チャネルにおけるコマンド実行の脆弱性
CSCvg47696	DfltGrpPolicy の削除後に RA VPN を作成できない
CSCvg48363	冗長 SSL ロギングを有効にすると、ログが使用可能なすべてのディスク領域を消費する可能性がある
CSCvg50707	複数の NGFW ポリシーが検出されたため、Firepower Threat Defense のハイ アベイラビリティ ポリシーの展開が失敗する
CSCvg52545	inlineIPS モードの 9300 ペア の NGFW が SNAP パケットの更新を適切な VLAN タグでトリガーしない
CSCvg58777	Apache tomcat の複数の脆弱性
CSCvg58825	サブドメインのオブジェクト グループを使用してアクセス コントロール ポリシーから生成したレポートが空白/0 バイトである
CSCvg61624	セカンダリがアクティブでプライマリが無効になっている場合（デバイスで一時停止操作を実行することにより）、展開が失敗する
CSCvg61737	「ルールファイル snort.conf を開くことができないため、Snort の検証に失敗」が原因で、展開に失敗した
CSCvg61760	Firepower Threat Defense のすべての syslog メッセージが編集に使用できるわけではない
CSCvg61799	Sysopt permit-vpn の動作が意図していないクリアテキスト トラフィックを阻止するように変更される

不具合 ID	タイトル
CSCvg62337	Firepower Threat Defense デバイスでの Snort のメモリ計算が正しくない
CSCvg66727	jumboframe の削除後に sysopt connection tcpmss 0 が削除されない
CSCvg67377	マルウェア相関ルールにデバイス条件がない
CSCvg71501	輸出規制による機能限定を使用して基本ライセンスを追加した後、ASA/FTD デバイスを再起動する必要がある
CSCvg73042	SSL キャッシュにセッション情報がないため、SSL Web サイトにアクセスするとブラウザに ERR_SSL_PROTOCOL_ERROR が表示される
CSCvg76789	一部の Web サイトに DND がある場合に FMC で MASTER_KEY_INVALID フローエラーが表示される
CSCvg76907	current_user_ip_map が無効なレルムを参照する場合、SFDaco が繰り返しクラッシュする。RA-VPN が何らかの原因になっている?
CSCvg78622	ポリシーおよびオブジェクトの収集で展開に失敗した
CSCvg80346	FMCv/FTDv/NGIPSv で初期化プロセスが再生成される
CSCvg83924	廃止されたアプリケーションが含まれているアクセス コントロール ルールにトラフィックがヒットしない
CSCvg85613	認証がオンになっている場合、Smart Call Home が HTTP プロキシで正しく機能しない
CSCvg86139	Firepower Threat Defense のハイ アベイラビリティ ペアが破損した後、ポリシーの展開が失敗する
CSCvg86366	アップグレード後に変更調整レポートが生成されない
CSCvg87754	Management Center から特定の VPN 関連の Syslog ID（402114 や 402119 など）を無効にできない
CSCvg90403	IRB がマルチキャスト トラフィックとともに使用されている場合にサイズ 80 のブロックのリークが観察される
CSCvg93202	ダッシュボードのカスタム分析 flow_chunk クエリがイベント処理を数時間にわたってブロックする
CSCvg93556	正常な KP HA ペアでの展開が失敗し、「ssp_ha_state_improper」というメッセージが表示される
CSCvg94796	セキュリティ インテリジェンス接続イベントで、イニシエータユーザが「0」と表示される

不具合 ID	タイトル
CSCvg95046	ハイアベイラビリティ Firepower Management Center のアップグレード後に Customer Success Network で障害が発生する
CSCvg98609	Management Center REST API：Threat Defense ペアが、GET policyassignments でターゲットとしてレポートされない
CSCvg98640	ポリシー展開中に Cluster-Hold-Abort と Cluster-Hold-Timeout が正しく処理されない
CSCvg99285	[ERROR] octeon の初期化に失敗 -- 致命的なエラー：DAQ oct_ssl (-1) を初期化できない
CSCvh01213	トラフィックの処理時に ASA がトレースバックし、リロードすることがある
CSCvh03962	Cisco Firepower Management Center のコマンド注入攻撃の脆弱性
CSCvh05658	デバイスを別のグループに移動した後、デバイス グループごとに NAT ポリシーを割り当てても UI は更新されない
CSCvh05897	Firepower Threat Defense クラスタをグループに登録することに失敗する場合がある
CSCvh07577	flexconfig を使用して「management-access」設定を削除できない
CSCvh12923	クラスタ モードの Firepower Threat Defense がリモート アクセス VPN をサポートしていないことを示すために、ドキュメントを更新する必要がある
CSCvh14447	Snort 更新中に 602_log_package.pl.log でルール解析エラーが無視された
CSCvh14478	ファイアウォール ルールチェッカーで、QoS ポリシーによるポリシー展開が失敗する
CSCvh15228	Firepower Threat Defense のトラフィックゾーンメンバーによるトラフィックの中断
CSCvh16252	接続複製時に ASA がスレッド名 fover_rep でトレースバックし、リロードすることがある
CSCvh19991	追加されたグループが AD サーバから欠落している場合、ユーザ/グループのダウンロードが失敗する
CSCvh20742	Cisco 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
CSCvh23085	Cisco 適応型セキュリティ アプライアンスのアプリケーション レイヤ プロトコルのインスペクションにおける DoS に対する脆弱性

不具合 ID	タイトル
CSCvh25000	「health」権限が有効になっていない場合、カスタムユーザロールで CSV レポートを生成できない
CSCvh25562	アクセス コントロール ルールを変更できない/「An internal error occurred」エラー
CSCvh25977	デバイス名の末尾の空白を削除する必要がある：イベントが見つからない
CSCvh26084	破損したフロー イベントの逆シリアル化での SFDataCorrelator コア
CSCvh28733	Firepower Management Center では、ポリシーをスタティックからダイナミックに切り替えるときに、誤った NAT ルールが許可される
CSCvh31939	Firepower Management Center が、SLA モニタオブジェクトで使用中のインターフェイスオブジェクトの削除を許可する
CSCvh47069	Firepower Management Center のデータ消去により、管理対象センサーが再起動時にユーザ セッションを消去する
CSCvh49388	Cisco FireSIGHT システムの VPN ポリシーバイパスの脆弱性
CSCvh49748	不明な app-id のために、ファイル検出をバイパスする最初の試行で、Malware.exe がダウンロードされる
CSCvh53414	オブジェクトの説明に「?」文字が含まれている場合、アクセス コントロール ポリシーの展開が失敗する
CSCvh53597	SSL ポリシーで AppDetector が廃止された場合、ポリシーの展開が失敗する
CSCvh53901	データベースから無効なフィンガープリント タイプを読み取る場合の SFDataCorrelator コア
CSCvh59772	いくつかの編集とテストの後、S2S/RA VPN が削除/割り当て解除されると、展開が失敗する
CSCvh59884	プルーニングされたイベントに関する通知に無効な日付/時刻が含まれている（Thu Jan 1 00:00:01 1970）
CSCvh62164	ASA スタンバイがアクティブ時に高 CPS トラフィックにより一括同期状態でスタックする
CSCvh63896	スレッド名 CP Processing での ASA/FTD のトレースバック
CSCvh67237	展開パッケージの不完全なコピーが原因でポリシーの展開が失敗する
CSCvh67930	Management Center は、保護された IPv4 および IPv6 ネットワークでサイト間トンネルを許可しない

不具合 ID	タイトル
CSCvh68253	同じエンドポイント（ノード）で2つの S2S VPN トポロジを作成すると、予測不可能な結果が発生する
CSCvh68311	Cisco Firepower システムソフトウェアの Cross-Origin 保護の脆弱性
CSCvh68521	8000 シリーズ スタックでは、「Maint on sec fail」設定が有効になっている場合、スタックヘルスが侵害状態になる
CSCvh70474	多数のホストが期限切れになった後の SFDataCorrelator/SFDCNotificationd 接続のログ スパム
CSCvh73463	ドキュメントとログでは、SSH を介した Firepower リモート ストレージが SCP を使用すると指定されているが、実際には SFTP を使用している
CSCvh77456	Cisco Firepower Threat Defense ソフトウェアの FTP インスペクションにおけるサービス妨害の脆弱性
CSCvh77845	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
CSCvh78133	Firepower 2100 の process_stderr.log がエラーでフラッディングし、/ngfw のディスク使用率が高くなる
CSCvh79172	ASA ポリシー適用ロールバックトラッキング中の一時的なトラフィックドロップ向けのフェーズ 1 ソリューション（CSCvc56570）
CSCvh83145	ASA インターフェイス IP とサブネット マスクが 0.0.0.0 0.0.0.0 に変更されるため、インターフェイス上のサービスが停止する
CSCvh84511	Cisco FireSIGHT システムの URL ベースのアクセス コントロール ポリシー バイパスの脆弱性
CSCvh85246	1 つ以上の共通名を指定する「do not decrypt」ルールによって ssl インスペクションが制限される
CSCvh85580	接続イベントの処理中の ids_event_alerter コア
CSCvh89340	Cisco Firepower Threat Defense の SSL エンジンで確認された高 CPU 使用率によるサービス拒否攻撃の脆弱性
CSCvh90092	グループの数が多いと、AQ タスクの選択で少数のグループが無視され、展開が 8 時間遅延する
CSCvh92840	REST API から URL リテラルを追加した後、展開に失敗する
CSCvh95396	プリプロセッサの normalize_tcp オプション「ftp」が無効なため、ポリシーの展開が失敗する

不具合 ID	タイトル
CSCvh95456	Cisco 適応型セキュリティ アプライアンスのアプリケーション レイヤ プロトコルのインスペクションにおける DoS に対する脆弱性
CSCvh95807	ECDSA 署名付き Web サイトへのアクセス時に SSL フローエラーが報告される
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
CSCvh97258	どのブラウザでもモニタリング画面をレンダリングできない
CSCvh97594	ssl インスペクション キャッシュがアンバランスになる可能性があり、最近使用された項目が活用されないまま削除される
CSCvh97782	ベンダーのべき剰余の実装内で KP が不正なメモリ アクセスをトレースバックする
CSCvh98781	ASA/FTD 導入エラー「Management interface is not allowed as Data is in use by this instance」
CSCvh98897	Firepower デバイス上のデータ インターフェイスがアップグレードの失敗時にシャットダウンし、管理の中断が発生する
CSCvi02989	バージョン 6.2.2.1 へのアップグレード後に、アクセス コントロール ポリシーを編集または展開できない
CSCvi09340	ポリシー展開 DB のサイズが大きいため、複数のデバイスでポリシー展開が失敗した
CSCvi31174	FTD：クラスタ内のノードがダウンしていたり FMC から到達できない場合、展開に時間がかかる
CSCvi39938	多数のユーザとグループのダウンロード中にトラフィックが停止する
CSCvi43661	スタティック ルート：ルートの設定中に適切なインターフェイスが割り当てられないため、問題が発生する
CSCvi44246	ポートチャネルのサブインターフェイスでは、Threat Defense ペアの両方のユニットで同じ MAC アドレスが共有される
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
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
CSCvi58729	KP-Onbox の 200_pre/600_ftd_onbox_data_export.sh で、6.2.3 のアップグレード再開が失敗する

不具合 ID	タイトル
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
CSCvi74560	6.2.3 が変数セットに変数を正しく展開せず、展開が失敗する
CSCvi74623	6.2.3 アップグレードによって home_net 変数がデフォルトの「any」にリセットされる
CSCvi77527	インストール後のデータベース整合性チェックエラーで 6.2.3 へのアップグレードが失敗する
CSCvi79043	設定マネージャの削除/追加コマンドに警告を追加
CSCvi80012	アクティブな FTD で Snort ポリシーの適用中にフェールオーバーが発生すると、CD が不正な状態になる
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
CSCvj00363	パケットトレーサとキャプチャの組み合わせで ASA がトレースバックとリロードを起こすことがある
CSCvj05640	SNMP サーバが有効になっていない場合、SNMP アドレスでのトレースバックがマッピングされない
CSCvj13327	6.2.3 へのアップグレードが 600_schema/100_update_database.sh で失敗し、oom killer が呼び出された
CSCvj18111	FTD：N1 フラグのフロー保持を IPS インターフェイスで適用してはならない
CSCvj42450	スレッド名 DATAPATH-14-17303 での ASA のトレースバック
CSCvj47119	「clear capture /all」がクラッシュすることがある
CSCvj50373	Doc：表 1 に、コンフィギュレーション ガイド バージョン 6.2.3 に関する誤った情報が記載されている
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
CSCvj62504	Cisco Firepower 2100 シリーズのセキュリティアプライアンスのサービス拒否攻撃に対する脆弱性
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
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
CSCvj74210	「show service-policy inspect gtp pdp-context detail」実行時の「SSH」でのトレースバック

不具合 ID	タイトル
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
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
CSCvj89470	Cisco 適応型セキュリティ アプライアンスのダイレクト メモリ アクセスにおけるサービス拒否攻撃に対する脆弱性
CSCvj98499	Linux カーネル cdrom_ioctl_media_changed 関数のカーネルによるメモリの読み取りに関する脆弱性
CSCvj98512	Doc：FTD 管理 IP アドレスの変更手順を修正する必要がある。
CSCvj99658	レンダリング制御チャネルをテストしている ASA/Lina HA フェールオーバー インターフェイスが応答しない
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）
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
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
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
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
CSCvk20381	新しい ASAv Azure、KVM、および VMWare の導入でトレースバック ループが確認される
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
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
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
CSCvk44166	Cisco ASA および FTD TCP プロキシのサービス妨害（DoS）脆弱性
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
CSCvk47253	UDP/TCP トラフィックのフローオフロードが機能しない

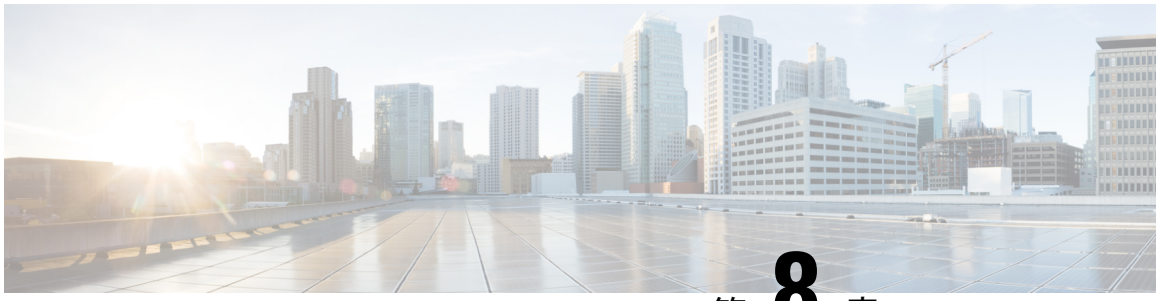
不具合 ID	タイトル
CSCvk50732	MAC で Safari 11.1.x ブラウザを使用した AnyConnect 4.6 の Web 展開が失敗する
CSCvk51181	インターフェイスの編集と展開後に FTD IPV6 トラフィックが停止する：パート 1/2
CSCvk57516	暗号マップが正しくないために DMA メモリが不足して VPN 障害が発生する
CSCvk66732	Cisco 適応型セキュリティ アプライアンス ソフトウェアの IPsec のサービス拒否（DoS）攻撃に対する脆弱性
CSCvk67239	「Thread Name: Logger Page fault: Address not mapped」での FTD または ASA のトレースバックとリロード
CSCvm06114	RDP ブックマーク プラグインが起動しない
CSCvm23370	ASA：PC cssls_get_crypto_ctxt によるメモリ リーク
CSCvm27111	OSPF 設定を削除する際の FTD Lina のトレースバック
CSCvm31905	OpenSSH Bailout によるユーザの列挙の遅延の脆弱性
CSCvm32267	SSL ポリシーを使用した HTTPS 接続で EICAR ファイルがブロックされない
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
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）」
CSCvm70274	tcp プロキシ：データパスでの ASA のトレースバック
CSCvm72145	Cisco ASA ソフトウェアと FTD ソフトウェアの MOBIKE サービス拒否攻撃に対する脆弱性
CSCvm80011	トランスペアレントモードの FTD クラスタ、インラインセット：FTP/SCP フローが停止し、回復しない。
CSCvm86658	snap_get_retaddr_mips の snap.h:285 での FTD トレースバックおよびリロード
CSCvm91893	イベント分析にスライディング時間枠オプションを使用すると、FMC で時刻が更新されず、イベントが表示されない
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

不具合 ID	タイトル
CSCvn09612	非アクティブなオフロードセッションで ASA/FTD 接続アイドル タイマーが増加しない
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
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
CSCvn31390	コンピューティング プロセッサ PortSmash サイドチャネル情報開示の脆弱性
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
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
CSCvn55563	拡張アクセスリストの作成中にポートグループオブジェクトが一覧表示されない（FMC GUI）
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
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
CSCvn69270	VPN クライアント割り当てのトラブルシューティングを追加
CSCvn75368	キー再生成中に IPsec VPN が断続的にダウンする
CSCvn76023	Firepower：ポリシーを展開すると、デバイスリストが空になり、「デバイスリストの取得に失敗」というエラーメッセージが表示される
CSCvn78174	Cisco ASA ソフトウェアおよび Cisco FTD ソフトウェア TCP タイマー処理におけるサービス妨害の脆弱性
CSCvn78593	FTD でコントロールプレーン ACL が正しく機能しない
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 nameif が削除される：finetune mmap thresh
CSCvo11077	Cisco ASA ソフトウェアと FTD ソフトウェアの IKEv1 サービス拒否攻撃に対する脆弱性
CSCvo12985	ASA：Hello パケットの送信の遅延により、フェールオーバー後に EIGRP ネイバーシップの形成が遅延する
CSCvo39356	スレッド名でのトレースバック：IP アドレスの割り当て
CSCvo41572	FMC において接続イベントのパケット カウントが 0 と表示される

不具合 ID	タイトル
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）
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
CSCvo48838	長すぎる設定行のエラーを Lina が適切に報告しない
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
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
CSCvo62031	IKE デバッグ実行中の ASA のトレースバックとリロード
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
CSCvo72462	ルールを復号しないとトラフィックが中断する
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
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
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
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
CSCvp25236	FTD Lina トレースバック：スレッド名：cli_xml_server
CSCvp30505	FDM エラー：アーカイブ済みバックアップのロード中に一部の接続で問題が発生。
CSCvp36425	Cisco ASA および FTD ソフトウェアの暗号化 TLS および SSL ドライバにおけるサービス拒否（DoS）攻撃に対する脆弱性
CSCvp43150	FP9300 クラスタ：マスターユニットがスレーブへのすべてのルート変更を更新しない
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

不具合 ID	タイトル
CSCvp47525	FMC からセンサーへの帯域幅が低いため、1 時間後にアップグレードがタイムアウトする
CSCvp49576	xlate_detach のウォッチドッグによる FTD のトレースバック
CSCvp53637	インラインセットでフローがオフロードされる
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
CSCvp57643	FP9300 クラスタ：マスターユニットがスレーブへのすべてのルート変更を更新しない
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）
CSCvp81083	TLS/VPN に関連する ASA/Lina のトレースバック
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
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
CSCvq54034	CCM レイヤで WRL6 と WRL8 のコミット ID が更新される（Sprint 65）
CSCvq70775	FPR2100 FTD スタンバイユニットで 9K ブロックがリークする
CSCvq75634	管理インターフェイスの設定により、即時トレースバックとリロードが発生する
CSCvq79042	サーバからの DNS 応答が大きく、切り捨てられているため、FQDN ACL エントリが不完全になる
CSCvq80735	ネイバーが 1 つのインターフェイスと同じサブネット上にある場合、BGP にネイバーを追加できない
CSCvq93640	CCM レイヤで WRL6 と WRL8 のコミット ID が更新される（Sprint 67）
CSCvr21803	入力 FTD インターフェイスに挿入された誤ったパケットによりスイッチ上で Mac アドレスがフラップする
CSCvr23986	メモリが不足しており、MIB ウォークが頻繁に実行される状態では、Cisco ASA & FTD デバイスがリロードする場合がある

不具合 ID	タイトル
CSCvr25954	FTD/LINA スタンバイが、アクティブからのロギングコマンドの複製中にトレースバックし、リロードすることがある
CSCvr27445	ポリシーの展開中にユニットが HA に参加しようとすると、アプリケーションの同期が失敗する
CSCvr68146	FTD クラスタを自動で再参加させることができない
CSCvs01422	FTD のデバイスモードの変更時に Lina がトレースバックする
CSCvs03023	クラスタリングモジュールは、タイムアウトエラーとクロックジャンプを回避するために、ハードウェアクロックの更新をスキップする必要がある
CSCvs26402	NAT ポリシー設定範囲の制限が非サービス CMDS にも適用される
CSCvs59056	Float-Conn が有効になっている場合、ASA/FTD トンネルスタティックルートが準最適なルックアップによって無視される
CSCvs80536	ASA キャプチャで FP41xx の不正なインターフェイスが適用される
CSCvs81504	WR6 と WR8 のコミット ID が CCM レイヤで更新される（Sprint 77）
CSCvt06606	フローオフロードが FTD 6.2(3.10) と FXOS 2.6(1.169) の組み合わせで機能しない
CSCvt28182	sctp-state-bypass がインライン FTD に対して呼び出されない



第 8 章

既知の問題

便宜上、このリリースノートには、このバージョンの既知のバグが記載されています。

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

アップグレードでバージョンがスキップされる場合は、スキップするメジャーバージョンの既知の問題も参照してください。「Cisco Firepower リリース ノート」を参照してください。

- 既知の問題の検索 （105 ページ）
- バージョン 6.2.3 の既知の問題 （106 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。

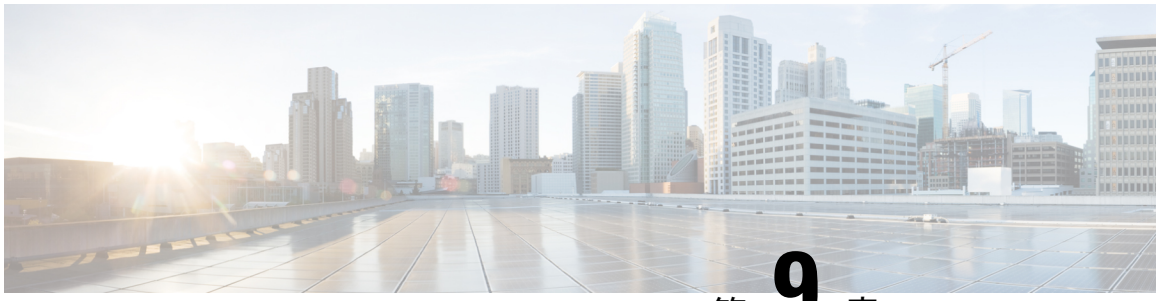
- Firepower Management Center
- Firepower Management Center Virtual
- Firepower Threat Defense
- Firepower Threat Defense Virtual
- ASA with FirePOWER サービス
- NGIPSv

バージョン 6.2.3 の既知の問題

表 *37* : バージョン *6.2.3* の既知の問題

不具合 ID	タイトル
CSCvf16001	SF Cli：「inside」または「outside」インターフェイス キャプチャではすべてのオプションが提供されない
CSCvh73096	Firepower Management Center は、ISE 2.2+ を使用したログインで userPrincipalName 属性をサポートしない
CSCvh89068	Firepower Management Center Perl のコア
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
CSCvi07656	ハードウェア モードの TLS インスペクションが過負荷になると、少数の TLS 接続が失敗する可能性がある
CSCvi10758	ソフトウェア モードの SSL インスペクションを使用すると、いくつかの TLS 接続が適切なタイミングで終了しない
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（HW モード）
CSCvi18123	2100 で CLISH CLI からの Firepower Threat Defense **show tech-support** コマンドの出力が破損する
CSCvi19862	SSL インスペクションを有効にすると、TLS トラフィックのスループットにより、後続のハイ アベイラビリティ フェールオーバーがドロップされる可能性がある
CSCvi35176	展開の失敗：Snort の再起動に失敗する：**APPLY_APP_CONFIG_APPLICATION_FAILURE** SignalAppConfigFailed
CSCvi35588	「**Snort failed to restart** PDTS Handle was NULL」が原因で展開が失敗する
CSCvi42539	SSLv2 がサポートされているが、より高いバージョンがネゴシエートされる場合、復号化された接続が失敗する
CSCvi47264	TAXII フィードを並行して使用すると、一部のインジケータが保留状態のままになる場合がある
CSCvi49538	2100で Firepower デバイス管理が失敗する（6.2.3 ～ 51（PortChannel））
CSCvi50731	以前に ISE で使用された証明書オブジェクトがあり、削除された場合でも、証明書オブジェクトを削除できない

不具合 ID	タイトル
CSCvi61411	ルーティングされた Threat Defense では透過的な設定が可能であるが、KVM でのみでトラフィックが失敗する（6.2.3 ～ 66）
CSCvi62982	ESXi Firstboot config の Firepower Threat Defense Virtual では、ホスト名が FQHN と適切に同期されない
CSCvi63157	Firepower 2110 が接続をドロップする
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
CSCvi66189	ライセンスのためにサテライト サーバを使用している Firepower Management Center で CNP が有効にされている
CSCvi70680	異なる AD の同じグループがダウンロードされない
CSCvv14442	将来のタイムスタンプを持つファイル/ディレクトリが含まれている場合、FMC バックアップの復元が失敗する



第 9 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