# Cisco Firepower バージョン 6.4.0 パッチリリースノート

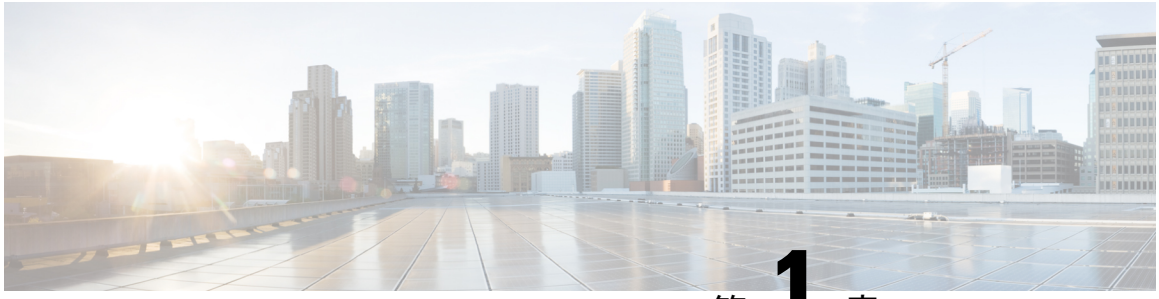
**初版**：2019 年 5 月 15 日

**最終更新**：2022 年 3 月 8 日


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

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

# 目 次



第 1 章

# ようこそ

本マニュアルでは、重要なリリースに固有の情報を記載しています。



## リリース日

シスコは、更新版ビルドを適宜リリースしています。ほとんどの場合、各プラットフォームの最新のビルド番号のみが、シスコ サポートおよびダウンロード サイト で入手可能です。最新のビルドを使用することを強くお勧めします。以前のビルドをダウンロードした場合は使用しないでください。詳細については、新しいビルドで解決済みの問題 （74 ページ）を参照してください。

**表 *1* : バージョン *6.4.0* の日付**

| バージョン | ビルド | 日付 | プラットフォーム |
|---|---|---|---|
| 6.4.0 | 113 | 2020 年 3 月 3 日 | FMC/FMCv |

| バージョン | ビルド | 日付 | プラットフォーム |
|---|---|---|---|
| 6.4.0 | 102 | 2019 年 6 月 20 日 | Firepower 4115、4125、4145<br>SM-40、SM-48、および SM-56 モジュールを搭載した Firepower 9300 |
| | | 2019 年 6 月 13 日 | Firepower 1010、1120、1140 |
| | | 2019 年 4 月 24 日 | Firepower 2110、2120、2130、2140<br>Firepower 4110、4120、4140、4150<br>SM-24、SM-36、および SM-44 モジュールを搭載した Firepower 9300<br>ASA 5508-X、5515-X、5516-X、5525-X、5545-X、5555-X<br>ASA 5585-X-SSP-10、-20、-40、-60<br>ISA 3000<br>FTDv<br>Firepower 7000/8000 シリーズ<br>NGIPSv |

表 *2 :* バージョン *6.4.0* 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 |
|---|---|---|---|
| 6.4.0.14 | 67 | 2022 年 02 月 18 日 | すべて |
| 6.4.0.13 | 57 | 2021 年 12 月 2 日 | すべて |
| 6.4.0.12 | 112 | 2021 年 5 月 12 日 | すべて |
| 6.4.0.11 | 11 | 2021 年 1 月 11 日 | すべて |
| 6.4.0.10 | 95 | 2020 年 10 月 21 日 | すべて |
| 6.4.0.9 | 62 | 2020 年 5 月 26 日 | すべて |

| バージョン | ビルド | 日付 | プラットフォーム |
|---|---|---|---|
| 6.4.0.8 | 28 | 2020 年 1 月 29 日 | すべて |
| 6.4.0.7 | 53 | 2019 年 12 月 19 日 | すべて |
| 6.4.0.6 | 28 | 2019 年 10 月 16 日 | 利用できなくなりました。 |
| 6.4.0.5 | 23 | 2019 年 9 月 18 日 | すべて |
| 6.4.0.4 | 34 | 2019 年 8 月 21 日 | すべて |
| 6.4.0.3 | 29 | 2019 年 7 月 17 日 | すべて |
| 6.4.0.2 | 35 | 2019 年 7 月 3 日 | FMC/FMCv<br>FTD/FTDv（FirePOWER 1000 シリーズ以外） |
| | 34 | 2019 年 6 月 27 日 | — |
| | | 2019 年 6 月 26 日 | Firepower 7000/8000 シリーズ<br>ASA FirePOWER<br>NGIPSv |

| バージョン | ビルド | 日付 | プラットフォーム |
|---|---|---|---|
| 6.4.0.1 | 17 | 2019 年 6 月 27 日 | FMC 1600、2600、4600 |
| | | 2019 年 6 月 20 日 | Firepower 4115、4125、4145<br>SM-40、SM-48、および SM-56 モジュールを搭載した Firepower 9300 |
| | | 2019 年 5 月 15 日 | FMC 750、1000、1500、2000、2500、3500、4000、4500<br>FMCv<br>Firepower 2110、2120、2130、2140<br>Firepower 4110、4120、4140、4150<br>SM-24、SM-36、および SM-44 モジュールを搭載した Firepower 9300<br>ASA 5508-X、5515-X、5516-X、5525-X、5545-X、5555-X<br>ASA 5585-X-SSP-10、-20、-40、-60<br>ISA 3000<br>FTDv<br>Firepower 7000/8000 シリーズ<br>NGIPSv |

# 推奨リリース

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

また、新機能ガイドにも推奨リリースを示します。

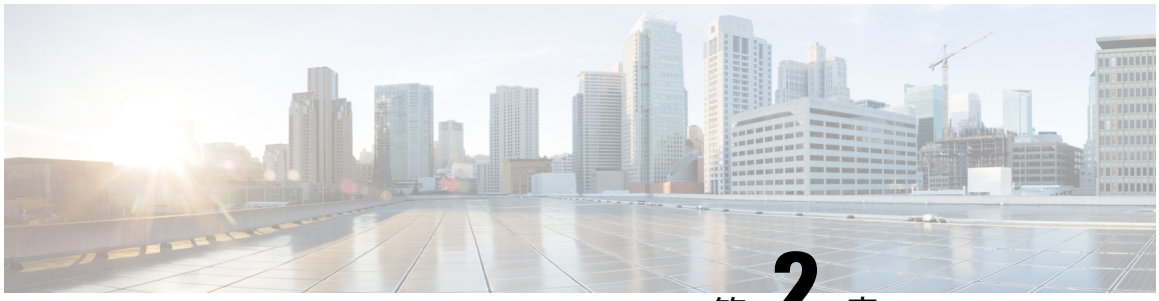
- Cisco Firepower Management Center の新機能（リリース別）
- Cisco Firepower Device Manager の新機能（リリース別）

### 古いアプライアンスの推奨リリース

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

語の説明については、「Cisco NGFW Product Line Software Release and Sustaining Bulletin」を参照してください。

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



第 2 章

# 互換性

一般的な互換性情報については、次を参照してください。

- Cisco Firepower Compatibility Guide：バンドルされている OS やその他のコンポーネントのバージョンやビルドを含む、サポート対象のすべてのバージョンの詳細な互換性情報、および廃止されたプラットフォームの販売終了やサポート終了の通知へのリンク。
- 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：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。

本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

Firepower Management Center は、一元化されたファイアウォール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 は、仮想環境に完全なファイアウォール管理機能を提供します。

### Firepower Management Center

本リリースでは、次のハードウェア FMC プラットフォームをサポートしています。

- FMC 1600、2600、4600
- 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

本リリースでは、次の FMCv パブリッククラウドの実装をサポートしています。

- Firepower Management Center VirtualAmazon Web Services（AWS）用
- Firepower Management Center VirtualMicrosoft Azure 用

このリリースでは、次の FMCv オンプレミス/プライベート クラウドの実装がサポートされています。

- Firepower Management Center Virtualカーネルベース仮想マシン（KVM）用
- Firepower Management Center VirtualVMware vSphere および VMware ESXi 6.0 または 6.5 用

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

（注） これらのリリースノートには、本リリースでサポートされているデバイスが掲載されています。古いデバイスが EOL に達していて、アップグレードできなくなった場合でも、数バージョンの範囲内であれば、より新しい FMC を使用してそのデバイスを管理できます。同様に、より新しいバージョンの ASDM では、より古いバージョンの ASA FirePOWER モジュールを管理できます。下位互換性を含む、サポート対象の管理方法については、「マネージャとデバイスの互換性 （11 ページ）」を参照してください。

**表 *3*: バージョン *6.4.0* の *Firepower Threat Defense***

| FTD プラットフォーム | OS/ハイパーバイザ | 詳細情報 |
|---|---|---|
| Firepower 1010、1120、1140<br>Firepower 2110、2120、2130、2140 | — | Firepower 1000 シリーズ デバイスでは、バージョン 6.4.0.1 および 6.4.0.2 はサポートされていません。 |

| 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<br>Firepower 4115、4125、4145<br>SM-24、SM-36、SM-44 モジュールを搭載した Firepower 9300<br>SM-40、SM-48、SM-56 モジュールを搭載した Firepower 9300 | FXOS 2.6.1.157 以降のビルド。 | 最初に FXOS をアップグレードします。<br>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, 2.6(1)』を参照してください。 |
| ASA 5508-X、5516-X<br>ASA 5515-X<br>ASA 5525-X、5545-X、5555-X<br>ISA 3000 | — | FTD 展開では、これらのデバイスのオペレーティングシステムを個別にアップグレードすることはありませんが、ISA 3000、ASA5508-Xおよび 5516-X に最新の ROMMON イメージがあることを確認する必要があります。Cisco ASA and Firepower Threat Defense Reimage Guide |

| FTD プラットフォーム | OS/ハイパーバイザ | 詳細情報 |
|---|---|---|
| FTDv | 次のいずれかです。<br>• AWS：Amazon Web Services<br>• Azure：Microsoft Azure<br>• KVM：カーネルベースの仮想マシン<br>• VMware vSphere/VMware ESXi 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。 |

表 *4 :* バージョン *6.4.0* の *NGIPS/ASA FirePOWER*

| NGIPS/ASA FirePOWER プラットフォーム | OS/ハイパーバイザ | 詳細情報 |
|---|---|---|
| ASA 5508-X、5516-X<br>ISA 3000 | ASA 9.5(2) ～ 9.16(x) | ASA と ASA FirePOWER のバージョンには幅広い互換性があります。ただし、アップグレードすると、新機能を利用でき、問題も解決されます。操作の順序については、『Cisco ASA Upgrade Guide』を参照してください。<br>また、ISA 3000、ASA5508-X および 5516-X に最新の ROMMON イメージがあることも確認してください。Cisco ASA and Firepower Threat Defense Reimage Guide |
| ASA 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 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。 |

| NGIPS/ASA FirePOWER プラットフォーム | OS/ハイパーバイザ | 詳細情報 |
|---|---|---|
| Firepower 7010、7020、7030、7050<br>Firepower 7110、7115、7120、7125<br>Firepower 8120、8130、8140<br>Firepower 8250、8260、8270、8290<br>Firepower 8350、8360、8370、8390<br>AMP 7150、8050、8150<br>AMP 8350、8360、8370、8390 | — | — |

# マネージャとデバイスの互換性

### Firepower Management Center

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

新しい FMC では、次の表に示されている複数のメジャーバージョンまで遡って古いデバイスを管理できます。ただし、導入環境全体を常に更新することをお勧めします。多くの場合、新機能の使用や問題解決の適用には、FMC とその管理対象デバイスの両方で最新リリースが必要になります。

**表 *5 : FMC*とデバイス間の互換性**

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

### Firepower Device ManagerおよびCisco Defense Orchestrator

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

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

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

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

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

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

**表 *6 : FTD* との *FDM* および *CDO* の互換性**

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

### Adaptive Security Device Manager

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

ほとんどの場合、新しい ASDM のバージョンは以前のすべての ASA のバージョンと下位互換性があります。ただし、いくつか例外があります。たとえば、ASDM 7.13(1) は ASA 9.10(1) で ASA 5516-X を管理できます。ASDM 7.13(1) と 7.14(1) は、ASA 5512-X、5515-X、5585-X、お

よび ASASM をサポートしていませんでした。そのため、ASDM 7.13(1.101) または 7.14(1.48) にアップグレードして ASDM のサポートを復元する必要があります。詳細は、『Cisco ASA Compatibility』を参照してください。

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

**表 *7 : ASDM* と *ASA FirePOWER* の互換性**

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

# Web ブラウザの互換性

### ブラウザ

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

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

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

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

### ブラウザの設定と拡張

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

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

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

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

### セキュア通信

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

自己署名証明書の置き換えを開始する手順は、次のとおりです。

- Firepower Management Center または 7000/8000 シリーズ：**[システム（System）]** > **[Configuration]** を選択し、[HTTPS 証明書（HTTPS Certificates）] をクリックします。
- Firepower Device Manager：[デバイス（Device）] をクリックしてから **[システム設定（System Settings）]** > **[管理アクセス（Management Access）]** リンクをクリックし、次に [管理Web サーバ（Management Web Server）] タブをクリックします。

詳しい手順については、オンラインヘルプまたはご使用の製品の構成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『Refresh Firefox』[英語]サポートページを参照してください。

### 監視対象ネットワークからの参照

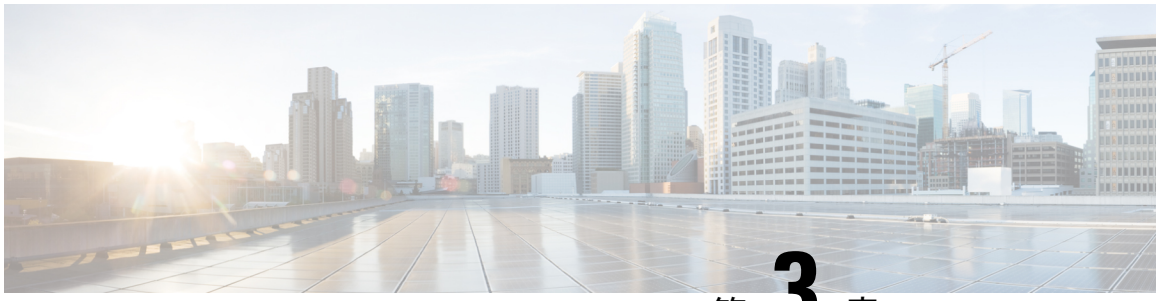
多くのブラウザでは、デフォルトで Transport Layer Security（TLS）v1.3 が使用されています。暗号化されたトラフィックを処理するために SSL ポリシーを使用していて、モニター対象ネットワーク内のユーザーが TLS v1.3 を有効にしてブラウザを使用している場合、TLS v1.3 をサポートする Web サイトのロードに失敗することがあります。

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

# 画面解像度の要件

**表 *8* : 画面解像度の要件**

| インターフェイス | 解決策 |
|---|---|
| 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 |
| ASA FirePOWER moduleを管理している ASDM | 1024 X 768 |
| Firepower 4100/9300 用 Firepower Chassis Manager | 1024 X 768 |



第 3 章

# 特長と機能

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



# Firepower Management Center 展開に関する機能

（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。ユーザーエージェント設定を使用して Firepower Management Center 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、ユーザーエージェントで使用できない機能も利用できるようになります。ライセンスを変換するには、シスコの担当者またはパートナーの担当者にお問い合わせください。

詳細については、『End-of-Life and End-of-Support for the Cisco Firepower User Agent』[英語] の通知、および『Firepower User Identity: Migrating from User Agent to Identity Services Engine』[英語] の技術メモを参照してください。

# FMC バージョン 6.4.0 パッチの新機能

表 *9:*

| 機能 | 説明 |
|---|---|
| **バージョン 6.4.0.10**<br>アップグレードがスケジュールされたタスクを延期する | **アップグレードの影響。**<br>アップグレードは、スケジュールされたタスクを延期するようになりました。アップグレード中に開始するようにスケジュールされたタスクは、アップグレード後の再起動の 5 分後に開始されます。<br>（注） アップグレードを開始する前に、実行中のタスクが完了していることを確認する必要があります。アップグレードの開始時に実行中のタスクは停止し、失敗したタスクとなり、再開できません。<br>この機能は、バージョン 6.4.0.10 以降のパッチを実行している Firepower アプライアンスでサポートされています。バージョン 6.4.0.10 へのアップグレード、またはバージョン 6.4.0.10 をスキップするアップグレードではサポートされません。<br>この機能は、バージョン 6.5.0、6.6.0、または 6.6.1 でもサポートされていません。バージョン 6.6.3 および 6.7.0 では再導入されています。 |
| **バージョン 6.4.0.9**<br>デフォルトの HTTPS サーバー証明書 | **アップグレードの影響。**<br>FMC または 7000/8000 シリーズのデバイスをバージョン 6.4.0 ～ 6.4.0.8 から以降のバージョン 6.4.0.x のパッチに（または FMC をバージョン 6.6.0+ に）アップグレードすると、デフォルトの HTTPS サーバー証明書が更新されます。この証明書は、アップグレードの日から 800 日後に期限切れになります。今後の更新はすべて、有効期間が 800 日になります。<br>古い証明書には、生成日に応じて、次の期限が設定されています。<br>• 6.4.0 ～ 6.4.0.8：3 年<br>• 6.3.0 およびすべてのパッチ：3 年<br>• 6.2.3 以前：20 年<br>バージョン 6.5.0 ～ 6.5.0.4 では、更新時の有効期限が 3 年に戻ることに注意してください。ただし、バージョン 6.5.0.5 および 6.6.0 では 800 日に更新されます。 |

| 機能 | 説明 |
| --- | --- |
| **バージョン 6.4.0.4**<br>新しい syslog フィールド | 次の新しい syslog フィールドは、一意の接続イベントをまとめて識別します。<br>• センサー UUID<br>• 最初のパケット時間<br>• 接続インスタンス ID<br>• 接続数カウンタ<br>これらのフィールドは、侵入、ファイル、およびマルウェアイベントの syslog にも表示され、接続イベントをこれらのイベントに関連付けることができます。 |
| **バージョン 6.4.0.2**<br>FTD NAT ポリシーでのルールの競合の検出 | **アップグレードの影響。**<br>バージョン 6.4.0.2 以降のパッチにアップグレードすると、競合するルール（「重複」ルールまたは「オーバーラップ」ルールとも呼ばれます）を持つ FTD NAT ポリシーを作成できなくなります。これは、競合する NAT ルールが順序どおりに適用されていなかった問題を修正するものです。<br>現在競合している NAT ルールがある場合は、アップグレード後に展開することができます。ただし、NAT ルールは引き続き順序どおりに適用されません。<br>そのため、アップグレード後に FTD NAT ポリシーを調べることをお勧めします。それには、ポリシーを編集して再保存を試みます（変更は必要ありません）。ルールが競合している場合は保存ができません。問題を修正して保存し、それから展開します。 |
| **バージョン 6.4.0.2**<br>[ISE接続ステータスのモニター（ISE Connection Status Monitor）] ヘルスモジュール | 新しいヘルスモジュール [ISE接続ステータスのモニター（ISE Connection Status Monitor）] は、Cisco Identity Services Engine（ISE）と FMC 間のサーバー接続のステータスをモニターします。 |

# FMC バージョン 6.4.0 パッチで廃止された機能

表 *10*：

| 機能 | アップグレードの影響 | 説明 |
|---|---|---|
| **バージョン 6.4.0.7**<br>出力最適化 | パッチを適用すると、出力最適化処理がオフになります。 | CSCvq34340 を軽減するため、Firepower Threat Defense をバージョン 6.4.0.7 以降にパッチすると、出力最適化処理がオフになります。これは、出力最適化機能が有効になっているか、無効になっているかに関係なく発生します。<br>（注） この問題が修正されているバージョン 6.6.0+ にアップグレードすることをお勧めします。機能を「有効」のままにすると、出力最適化がオンに戻ります。<br>バージョン 6.4.0 ～ 6.4.0.6 のままの場合は、FTD CLI から **no asp inspect-dp egress-optimization** を実行して出力最適化を手動で無効にする必要があります。<br>詳細については、ソフトウェアアドバイザリ『FTD traffic outage due to 9344 block size depletion caused by the egress optimization feature』を参照してください。 |

# Firepower Device Manager 展開の機能

## FDM バージョン 6.4.0 パッチの新機能

表 *11 :*

| 機能 | 説明 |
|---|---|
| **バージョン 6.4.0.10**<br>VDB、GeoDB、および SRU 更新の手動アップロード | VDB、地理位置情報データベース、および侵入ルールの更新パッケージを手動で取得し、FDM を使用してワークステーションから FTD デバイスにアップロードできるようになりました。たとえば、FDM で Cisco Cloud から更新を取得できないエアギャップネットワークがある場合でも、必要な更新パッケージを入手できます。<br>ワークステーションからファイルを選択してアップロードできるように、[Device] > [Updates] ページが更新されました。<br>この機能はバージョン 6.5.0 ではサポートされていないことに注意してください。バージョン 6.6.0 では再導入されています。バージョン 6.4.0.10 以降のパッチを実行している場合は、バージョン 6.5.0 を中間バージョンとして使用せずに、直接バージョン 6.6.0 以上にアップグレードすることをお勧めします。 |
| **バージョン 6.4.0.10**<br>ユニバーサル永久ライセンス予約（PLR）モード | インターネットへのパスがないエアギャップネットワークがある場合は、スマートライセンスのために Cisco Smart Software Manager（CSSM）に直接登録することはできません。この場合は、ユニバーサル パーマネント ライセンス予約（PLR）モードを使用できるようになりました。このモードでは、CSSM との直接通信を必要としないライセンスを適用できます。エアギャップネットワークがある場合は、アカウント担当者に問い合わせて、CSSM アカウントでユニバーサル PLR モードを使用して必要なライセンスを取得することを許可するように依頼してください。<br>[Device] > [Smart License] ページに、PLR モードに切り替えたり、ユニバーサル PLR ライセンスをキャンセルしたりして登録解除する機能が追加されました。FTD API では、PLRAuthorizationCode、PLRCode、PLRReleaseCode、PLRRequestCode の新しいリソースと、PLRRequestCode、InstallPLRCode、および CancelReservation のアクションが追加されました。<br>この機能はバージョン 6.5.0 ではサポートされていないことに注意してください。バージョン 6.6.0 では再導入されています。バージョン 6.4.0.10 以降のパッチを実行している場合は、バージョン 6.5.0 を中間バージョンとして使用せずに、直接バージョン 6.6.0 以上にアップグレードすることをお勧めします。 |

| 機能 | 説明 |
| --- | --- |
| **バージョン 6.4.0.9**<br>デフォルトの HTTPS サーバー証明書 | **アップグレードの影響。**<br>FDM をバージョン 6.4.0 ～ 6.4.0.8 から以降のバージョン 6.4.0.x のパッチに（または6.6.0+に）アップグレードすると、デフォルトの HTTPS サーバー証明書が更新されます。この証明書は、アップグレードの日から800日後に期限切れになります。今後の更新はすべて、有効期間が 800 日になります。<br>古い証明書には、生成日に応じて、次の期限が設定されています。<br>• 6.4.0 ～ 6.4.0.8：3 年<br>• 6.3.0 およびすべてのパッチ：3 年<br>• 6.2.3 以前：20 年<br>バージョン 6.5.0 ～ 6.5.0.4 では、更新時の有効期限が 3 年に戻ることに注意してください。ただし、バージョン 6.5.0.5 および 6.6.0 では 800 日に更新されます。 |
| **バージョン 6.4.0.4**<br>新しい syslog フィールド | 次の新しい syslog フィールドは、一意の接続イベントをまとめて識別します。<br>• センサー UUID<br>• 最初のパケット時間<br>• 接続インスタンス ID<br>• 接続数カウンタ<br>これらのフィールドは、侵入、ファイル、およびマルウェアイベントの syslog にも表示され、接続イベントをこれらのイベントに関連付けることができます。 |

# FDM バージョン 6.4.0 パッチで廃止された機能

表 *12*：

| 機能 | アップグレードの影響 | 説明 |
|---|---|---|
| **バージョン 6.4.0.7**<br>出力最適化 | パッチを適用すると、出力最適化処理がオフになります。 | CSCvq34340 を軽減するため、Firepower Threat Defense をバージョン 6.4.0.7 以降にパッチすると、出力最適化処理がオフになります。これは、出力最適化機能が有効になっているか、無効になっているかに関係なく発生します。<br>（注） この問題が修正されているバージョン 6.6.0+ にアップグレードすることをお勧めします。機能を「有効」のままにすると、出力最適化がオンに戻ります。<br>バージョン 6.4.0 ～ 6.4.0.6 のままの場合は、FTD CLI から **no asp inspect-dp egress-optimization** を実行して出力最適化を手動で無効にする必要があります。<br>詳細については、ソフトウェアアドバイザリ『FTD traffic outage due to 9344 block size depletion caused by the egress optimization feature』を参照してください。 |

# 侵入ルールとキーワード

アップグレードにより侵入ルールをインポートして自動的に有効化が可能です。

侵入ルールを更新（SRU）すると、新規および更新された侵入ルールとプリプロセッサルール、既存のルールに対して変更された状態、および変更されたデフォルトの侵入ポリシーの設定が提供されます。現在のバージョンでサポートされていないキーワードが新しい侵入ルールで使用されている場合、SRU を更新しても、そのルールはインポートされません。

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

サポートされているキーワードは、Snort のバージョンによって異なります。

- FMC：[ヘルプ（Help）] > [バージョン情報（About）] 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。

# FMC の How-To ウォークスルー

デバイスのセットアップやポリシー設定などのさまざまな基本タスクについて順を追って説明する、FMC に関するウォークスルー（How-To とも呼ばれる）が導入されています。ブラウザウィンドウの下部にある [How To] をクリックし、ウォークスルーを選択して、手順ごとの説明に従って操作します。

（注） FMC ウォークスルーは Firefox および Chrome ブラウザでテストされています。別のブラウザで問題が発生した場合は、Firefox または Chrome に切り替えてください。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。

次の表に、一般的な問題点と解決策をいくつか示します。ウォークスルーは、右上隅の [x] をクリックするといつでも終了できます。

**表 *13 :* ウォークスルーのトラブルシューティング**

| 問題 | 解決方法 |
|---|---|
| ウォークスルーを開始するための [How To] リンクが見つからない。 | ウォークスルーが有効になっていることを確認します。ユーザー名の下にあるドロップダウンリストから、[User Preferences] を選択し、[How-To Settings] をクリックします。 |
| ウォークスルーが予期しないタイミングで表示される。 | ウォークスルーが予期しないタイミングで表示される場合は、ウォークスルーを終了します。 |
| ウォークスルーが突然消えたり終了したりする。 | ウォークスルーが消えた場合は、次のようにします。<br>• ポインタを移動します。<br>FMC で進行中のウォークスルーが表示されなくなることがあります。たとえば、別のトップレベルメニューをポイントすると表示されなくなります。<br>• 別のページに移動して、もう一度やり直してください。<br>ポインタを移動しても表示されない場合は、ウォークスルーが終了している可能性があります。 |

| 問題 | 解決方法 |
| --- | --- |
| ウォークスルーがFMCと同期していない。<br>• 誤った手順から開始される。<br>• 進行が早すぎる。<br>• 先に進まない。 | ウォークスルーが同期していない場合は、次のようにします。<br>• 続行します。<br>たとえば、フィールドに無効な値を入力してエラーが表示された場合は、ウォークスルーが先に進行することがあります。戻ってエラーを解決してタスクを完了することが必要になる場合があります。<br>• ウォークスルーを終了し、別のページに移動してもう一度やり直します。<br>場合によっては続行できないこともあります。たとえば、手順の完了後に [Next] をクリックしないと、ウォークスルーの終了が必要になる場合があります。 |

# シスコとのデータの共有

### 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、ユーザーの場所、FMC の管理 IP アドレスまたはホスト名を含む、個人を特定できない使用状況データをシスコに送信します。

デフォルトで Web 分析トラッキングに登録しています（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、初期設定完了後はいつでも登録を変更できます。

（注） バージョン 6.2.3 から 6.6.x にアップグレードすると、Web 分析トラッキングに登録される可能性があります。登録は、意図的に登録解除した場合でも行われ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、アップグレード後に登録解除してください。

### 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。

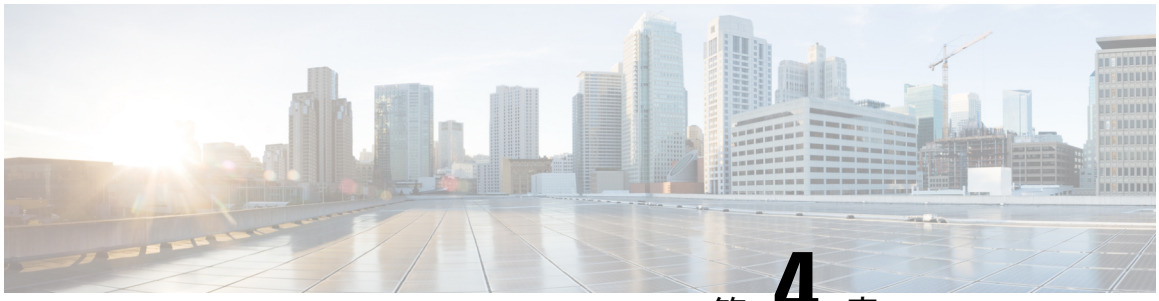
初期設定およびアップグレード中に、登録するか尋ねられます。登録はいつでも変更できます。

### Cisco Support Diagnostics

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、登録するか尋ねられます。登録はいつでも変更できます。

（注） この機能は、Firepower Management Center およびそこで管理される Firepower Threat Defense デバイスでサポートされます。バージョン 6.5.0 でのみ、FTD サポートは、FTD 搭載 Firepower 4100/9300 および Azure 向け FTDv に制限されます。この機能は、Firepower Device Manager ではサポートされていません。



第 4 章

# ソフトウェアのアップグレード

この章では、重要なリリースに固有の情報を提供します。



## アップグレードの計画

誤りを避けるには、注意深い計画と準備が役立ちます。この表はアップグレードの計画プロセスを要約したものです。詳細なチェックリストと手順については、該当するアップグレードまたは設定ガイドのを参照してください：アップグレード手順 （52 ページ）

**表 *14*：アップグレードの計画フェーズ**

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

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

# アップグレードする最小バージョン

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

# Version6.4.0.xパッチのアップグレードガイドライン

このチェックリストには、バージョン 6.4.0 パッチに関するアップグレードガイドラインが含まれています。

表 *15*：バージョン *6.4.0.x* ガイドライン

| ✓ | ガイドライン | プラットフォーム | アップグレード元 | 直接アップグレード先 |
|---|---|---|---|---|
| | アップグレードの失敗：コンテナインスタンスのディスク容量不足（29 ページ） | Firepower 4100/9300 | 6.3.0 ～ 6.4.0.x | 6.3.0.1 ～ 6.5.0 |
| | Firepower 1010 デバイス上の EtherChannel で出力トラフィックがブラックホール化される可能性（29 ページ） | Firepower 1010 | 6.4.0 のみ | 6.4.0.3 ～ 6.4.0.5 |
| | アップグレードの注意：Firepower 7000/8000 シリーズからバージョン 6.4.0.9 ～ 6.4.0.11 へ （30 ページ） | Firepower 7000/8000 シリーズ | 6.4.0 ～ 6.4.0.10 | 6.4.0.9 ～ 6.4.0.11 |

# アップグレードの失敗：コンテナインスタンスのディスク容量不足

**展開**：FTD を搭載した Firepower 4100/9300

**アップグレード元**：バージョン 6.3.0 ～ 6.4.0.x

**直接アップグレード先**：バージョン 6.3.0.1 ～ 6.5.0

多くの場合はメジャーアップグレード時に（場合によってはパッチ適用時に）、コンテナインスタンスを使用して設定されたFTDデバイスが、ディスク容量不足のエラーにより事前チェック段階で失敗することがあります。

この問題が発生した場合には、空きディスク容量を増やしてみてください。それでも解決しない場合は、Cisco TAC にお問い合わせください。

# Firepower 1010 デバイス上の EtherChannel で出力トラフィックがブラックホール化される可能性

**展開**：FTD を搭載した Firepower 1010

**影響を受けるバージョン**：バージョン 6.4.0 ～ 6.4.0.5

**関連するバグ**：CSCvq81354

FTD バージョン 6.4.0 ～ 6.4.0.5 を実行している Firepower 1010 デバイスでは EtherChannel を設定しないことを強くお勧めします（バージョン 6.4.0.1 および 6.4.0.2 はこのモデルではサポートされていないことに注意してください）。

内部トラフィックハッシュの問題により、Firepower 1010 デバイス上の EtherChannel では出力トラフィックがブラックホール化されることがあります。ハッシュは送信元 IP アドレスと宛

先 IP アドレスに基づくため、特定の送信元 IP と宛先 IP のペアで一貫性のある動作になります。つまり、一部のトラフィックは常に機能し、一部のトラフィックは常に失敗します。

この問題は、バージョン 6.4.0.6 および 6.5.0 で修正されています。

## アップグレードの注意：Firepower 7000/8000 シリーズからバージョン 6.4.0.9 ～ 6.4.0.11 へ

**展開**：Firepower 7000/8000 シリーズ

**アップグレード元**：バージョン 6.4.0 ～ 6.4.0.10

**宛先**：バージョン 6.4.0.9ー6.4.0.11

**関連バグ**： CSCvw01028

Firepower 7000/8000 シリーズのデバイスでバージョン 6.4.0 よりも古いバージョンを実行した場合は、バージョン 6.4.0.9、6.4.0.10、または 6.4.0.11 にアップグレードしないでください。そうしないと、デバイスが応答しなくなり、再イメージ化が強制されます。代わりに、バージョン 6.4.0.12 以降にアップグレードしてください。

影響を受けるバージョンのいずれかを既に実行していて、この問題に対して脆弱である場合は、Cisco TAC に連絡して修正プログラムを入手し、できるだけ早くバージョン 6.4.0.12 にアップグレードする必要があります。イメージを再作成してアップグレードすることもできます。

# 応答しないアップグレード

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

# トラフィック フローとインスペクション

次の場合に、トラフィックフローおよび検査の中断が発生することがあります。

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

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

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

### FXOS のアップグレード

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

**表 *16*：トラフィックの挙動：*FXOS* のアップグレード**

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

### スタンドアロンデバイスでのソフトウェアのアップグレード

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

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

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

### 高可用性および拡張性に関するソフトウェアのアップグレード

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

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

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

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

（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。 高可用性デバイスまたはクラスタ化されたデバイスをバージョン 6.0.1 から 6.2.2.x にアップグレードするには、追加のアップグレードパス要件が必要になる場合があります。詳しくは、Cisco Firepower Management Center Upgrade Guide, Version 6.0–7.0 の「upgrade path information in the planning」の章を参照してください。

### ソフトウェアのアンインストール（パッチ）

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

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

- FDM を使用した FTD：サポートされていません。

### 設定変更の導入

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

展開する際にリソースを要求すると、いくつかのパケットがインスペクションなしでドロップされることがあります。また、Snort プロセスを再起動すると、HA/スケーラビリティ用に設定されたものを含め、すべてのデバイスでトラフィック インスペクションが中断されます。イン

ターフェイス設定により、中断中にインスペクションせずにトラフィックをドロップするか受け渡すかが決定されます。

**表 *18：*トラフィックの動作：構成変更の展開**

| インターフェイス コンフィギュレーション | | トラフィックの動作 |
|---|---|---|
| ファイアウォール インターフェイス | EtherChannel、冗長、サブインターフェイスを含むルーテッドまたはスイッチド。<br>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。<br>[フェールセーフ（Failsafe）] が無効で、Snort がビジーでもダウンしていない場合、いくつかのパケットがドロップすることがあります。 |
| | インラインセット、[Snort Fail Open: Down]：無効（6.2 以降） | 廃棄 |
| | インラインセット、[Snort Fail Open: Down]：有効（6.2 以降） | 検査なしで受け渡される。 |
| | インラインセット、タップモード。 | パケットをただちに出力、コピーへのインスペクションなし。 |
| | パッシブ、ERSPAN パッシブ。 | 中断なし、インスペクションなし。 |

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

### スタンドアロンデバイスでのソフトウェアのアップグレード

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

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

| インターフェイス コンフィギュレーション | | トラフィックの動作 |
|---|---|---|
| ファイアウォール インターフェイス | EtherChannel、冗長、サブインターフェイスを含むルーテッドまたはスイッチド。<br>スイッチドインターフェイスは、ブリッジグループまたはトランスペアレントインターフェイスとしても知られています。 | 廃棄 |
| IPS のみのインターフェイス | インラインセット、ハードウェアバイパス強制が有効：[Bypass: Force]（Firepower 2100 シリーズ、6.3 以上）。 | ハードウェアバイパスを無効にするか、スタンバイモードに戻すまで、インスペクションなしで合格。 |
| | インラインセット、ハードウェアバイパス スタンバイ モード：[Bypass: Standby]（Firepower 2100 シリーズ、6.3 以上）。 | デバイスがメンテナンスモードの場合、アップグレード中にドロップされます。その後、デバイスがアップグレード後の再起動を完了する間、インスペクションなしで合格します。 |
| | インラインセット、ハードウェアバイパスが無効：[Bypass: Disabled]（Firepower 2100 シリーズ、6.3 以上）。 | 廃棄 |
| | インラインセット、ハードウェアバイパス モジュールなし。 | 廃棄 |
| | インラインセット、タップモード。 | パケットをただちに出力、コピーへのインスペクションなし。 |
| | パッシブ、ERSPAN パッシブ。 | 中断なし、インスペクションなし。 |

### 高可用性および拡張性に関するソフトウェアのアップグレード

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

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

### ソフトウェアのアンインストール（パッチ）

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

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

### 設定変更の導入

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

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

**表 *20*：トラフィックの動作：構成変更の展開**

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

| インターフェイス コンフィギュレーション | | トラフィックの動作 |
|---|---|---|
| IPS のみのインターフェイス | インラインセット、[Failsafe] が有効または無効（6.0.1 ～ 6.1）。 | 検査なしで受け渡される。<br>[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 *21*：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。<br>• 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。<br>• 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 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 |
| Passive | 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（Dropped） |

### 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 :* 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<br>[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 |
| Passive | 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（Dropped） |

# 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 *23 : 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**） | 切断 |
| モニターのみ（**sfr {fail-close}\|{fail-open} monitor-only**） | パケットをただちに出力、コピーへのインスペクションなし |

### ASA FirePOWER 展開時のトラフィックの動作

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

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

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

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

# NGIPSv アップグレード時の動作

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

### Firepower ソフトウェア アップグレード

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

**表 *24 : NGIPSv* アップグレード中のトラフィックの動作**

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

### 展開時のトラフィックの動作

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

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

表 *25 : 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<br>[フェールセーフ（Failsafe）] が無効で、Snort がビジーでもダウンしていない場合、いくつかのパケットがドロップすることがあります。 |
| インライン、タップ モード | すぐにパケットを出力し、バイパス Snort をコピーする |
| パッシブ | 中断なし、インスペクションなし |

# 時間とディスク容量のテスト

参考のために、FTD および FMC ソフトウェアの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

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

⚠

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

表 *26 :* ソフトウェアアップグレードの時間テストの条件

| 条件 | 詳細 |
|---|---|
| 配置 | FTD のアップグレードの時間は、FMC 展開でのテストでのものです。同様の条件の場合、リモートとローカルの管理対象デバイスの raw アップグレード時間は類似しています。 |

| 条件 | 詳細 |
|---|---|
| バージョン | メジャーリリースおよびメンテナンスリリースでは、以前のすべての対象メジャーバージョンからのアップグレードをテストします。パッチについては、ベースバージョンからアップグレードをテストします。アップグレードでバージョンがスキップされると、通常、アップグレード時間は長くなります。 |
| モデル | ほとんどの場合、各シリーズの最もローエンドのモデルでテストし、場合によってはシリーズの複数のモデルでテストします。 |
| 仮想アプライアンス | メモリおよびリソースのデフォルト設定を使用してテストします。ただし、仮想展開でのアップグレード時間はハードウェアに大きく依存することに注意してください。 |
| 高可用性/拡張性 | 特に断りのない限り、スタンドアロンデバイスでテストします。<br>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。 |
| 設定 | シスコでは、構成およびトラフィック負荷が最小限のアプライアンスでテストを行います。<br>アップグレード時間は、構成の複雑さ、イベント データベースのサイズ、また、それらがアップグレードから影響を受けるかどうか、受ける場合はどのような影響を受けるかにより、長くなる場合があります。たとえば多くのアクセス制御ルールを使用している場合、アップグレードはこれらのルールの格納方法をバックエンドで変更する必要があるため、アップグレードにはさらに長い時間がかかります。 |
| コンポーネント | ソフトウェアアップグレード自体とその後の再起動のみの時間を報告します。これには、オペレーティングシステムのアップグレード、アップグレードパッケージの転送、準備状況チェック、VDB および侵入ルール （SRU/LSP）の更新、または設定の展開のための時間は含まれません。 |

### ディスク容量テスト

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

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

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

**表 *27* : ディスク容量の確認**

| プラットフォーム | コマンド |
|---|---|
| FMC | **[System]** > **[Monitoring]** > **[Statistics]**を選択し、FMC を選択します。[Disk Usage] で、[By Partition] の詳細を展開します。 |
| FMC を使用した FTD | **[System]** > **[Monitoring]** > **[Statistics]**を選択し、確認するデバイスを選択します。[Disk Usage] で、[By Partition] の詳細を展開します。 |
| FDM を使用した FTD | **show disk** CLI コマンドを使用します。 |

# バージョン 6.4.0.14 の時間とディスク容量

**表 *28* : バージョン *6.4.0.14* の時間とディスク容量**

| プラットフォーム | ボリュームの容量 | 必要容量 | FMC の容量 | アップグレード時間 | リブート時間 |
|---|---|---|---|---|---|
| FMC | /var 内 4.5 GB | / 内 170 MB | — | 42 分 | 18 分 |
| FMCv：VMware | /var 内 5.2 GB | / 内 170 MB | — | 25 分 | 2 分 |
| Firepower 1000 シリーズ | — | /ngfw 内 2.4 GB | | 11 分 | 11 分 |
| Firepower 2100 シリーズ | — | /ngfw 内 1.9 GB | | 8 分 | 10 分 |
| Firepower 4100 シリーズ | — | /ngfw 内 2.5 GB | | 4 分 | 9 分 |
| Firepower 9300 | — | /ngfw 内 2.5 GB | | 4 分 | 8 分 |
| FTD を搭載した ASA 5500-X シリーズ | /home 内 2.0 GB | /ngfw 内 110 MB | | 12 分 | 42 分 |
| FTDv：VMware | /home 内 1.9 GB | /ngfw 内 110 MB | | 6 分 | 2 分 |
| Firepower 7000/8000 シリーズ | 3.7 GB | / 内 170 MB | | 10 分 | 2 分 |
| ASA FirePOWER | /var 内 4.2 GB | / 内 38 MB | | 43 分 | 51 分 |
| NGIPSv | /var 内 2.2 GB | / 内 170 MB | | 6 分 | 4 分 |

# バージョン 6.4.0.13 の時間とディスク容量

表 *29 :* バージョン *6.4.0.13* の時間とディスク容量

| プラットフォーム | ボリュームの容量 | 必要容量 | FMC の容量 | アップグレード時間 | リブート時間 |
|---|---|---|---|---|---|
| FMC | /var 内 3.8 GB | / 内 170 MB | — | 34 分 | 8 分 |
| FMCv：VMware | /var 内 3.9 GB | / 内 170 MB | — | 21 分 | 4 分 |
| Firepower 1000 シリーズ | — | /ngfw 内 3.0 GB | 540 MB | 11 分 | 13 分 |
| Firepower 2100 シリーズ | — | /ngfw 内 2.6 GB | 510 MB | 8 分 | 12 分 |
| Firepower 4100 シリーズ | — | /ngfw 内 2.5 GB | 450 MB | 4 分 | 9 分 |
| Firepower 9300 | — | /ngfw 内 2.5 GB | 450 MB | 4 分 | 9 分 |
| FTD を搭載した ASA 5500-X シリーズ | /home 内 2.0 GB | /ngfw 内 110 MB | 295 MB | 12 分 | 9 分 |
| FTDv：VMware | /home 内 1.9 GB | /ngfw 内 110 MB | 295 MB | 7 分 | 5 分 |
| Firepower 7000/8000 シリーズ | /var 内 3.7 GB | / 内 170 MB | 670 MB | 11 分 | 14 分 |
| ASA FirePOWER | /var 内 4.2 GB | / 内 38 MB | 660 MB | 43 分 | 8 分 |
| NGIPSv | /var 内 2.2 GB | / 内 170 MB | 460 MB | 6 分 | 4 分 |

# バージョン 6.4.0.12 の時間とディスク容量

表 *30 :* バージョン *6.4.0.12* の時間とディスク容量

| プラットフォーム | ボリュームの容量 | 必要容量 | FMC の容量 | アップグレード時間 | リブート時間 |
|---|---|---|---|---|---|
| FMC | /var 内 3.8 GB | / 内 170 MB | — | 25 分 | 8 分 |
| FMCv：VMware | /var 内 3.8 GB | / 内 170 MB | — | 27 分 | 4 分 |
| Firepower 1000 シリーズ | | /ngfw 内 2.9 GB | 530 MB | 10 分 | 13 分 |
| Firepower 2100 シリーズ | | /ngfw 内 2.5 GB | 510 MB | 8 分 | 32 分 |
| Firepower 4100 シリーズ | | /ngfw 内 2.5 GB | 440 MB | 4 分 | 9 分 |
| Firepower 9300 | | /ngfw 内 2.5 GB | 440 MB | 4 分 | 8 分 |

| プラットフォーム | ボリュームの容量 | 必要容量 | FMC の容量 | アップグレード時間 | リブート時間 |
|---|---|---|---|---|---|
| FTD を搭載した ASA 5500-X シリーズ | /home 内 1.9 GB | /ngfw 内 110 MB | 290 MB | 12 分 | 40 分 |
| FTDv：VMware | /home 内 1.9 GB | /ngfw 内 110 MB | 290 MB | 7 分 | 5 分 |
| Firepower 7000/8000 シリーズ | /var 内 3.7 GB | / 内 170 MB | 660 MB | 10 分 | 15 分 |
| ASA FirePOWER | /var 内 4.2 GB | / 内 37 MB | 600 MB | 47 分 | 51 分 |
| NGIPSv | /var 内 2.2 GB | / 内 150 MB | 460 MB | 7 分 | 5 分 |

# バージョン 6.4.0.11 の時間とディスク容量

**表 *31 :* バージョン *6.4.0.11* の時間とディスク容量**

| プラットフォーム | ボリュームの容量 | 必要容量 | FMC の容量 | アップグレード時間 | リブート時間 |
|---|---|---|---|---|---|
| FMC | 3.8 GB | 170 MB | — | 30 分 | 8 分 |
| FMCv：VMware | 4.1 GB | 170 MB | — | 27 分 | 7 分 |
| Firepower 1000 シリーズ | 3.0 GB | 3.0 GB | 530 MB | 14 分 | 9 分 |
| Firepower 2100 シリーズ | 2.5 GB | 2.5 GB | 510 MB | 9 分 | 6 分 |
| Firepower 4100 シリーズ | 1.8 GB | 1.8 GB | 310 MB | 8 分 | 7 分 |
| Firepower 9300 | 1.8 GB | 1.8 GB | 310 MB | 9 分 | 9 分 |
| FTD を搭載した ASA 5500-X シリーズ | 1.6 GB | 110 MB | 290 MB | 12 分 | 12 分 |
| FTDv：VMware | 4.4 GB | 170 MB | 290 MB | 28 分 | 4 分 |
| Firepower 7000/8000 シリーズ | 3.6 GB | 170 MB | 680 MB | 11 分 | 97 分 |
| ASA FirePOWER | 4.2 GB | 36 MB | 630 MB | 54 分 | 51 分 |
| NGIPSv | 2.4 GB | 150 MB | 470 MB | 11 分 | 15 分 |

# バージョン 6.4.0.10 の時間とディスク容量

表 *32 :* バージョン *6.4.0.10* の時間とディスク容量

| プラットフォーム | ボリュームの容量 | 必要容量 | FMC の容量 | アップグレード時間 | リブート時間 |
|---|---|---|---|---|---|
| FMC | 3.8 GB | 170 MB | — | 30 分 | 8 分 |
| FMCv：VMware | 4.1 GB | 170 MB | — | 27 分 | 7 分 |
| Firepower 1000 シリーズ | 2.9 GB | 2.9 GB | 560 MB | 11 分 | 14 分 |
| Firepower 2100 シリーズ | 2.5 GB | 2.5 GB | 530 MB | 8 分 | 13 分 |
| Firepower 4100 シリーズ | 1.8 GB | 1.8 GB | 330 MB | 5 分 | 11 分 |
| Firepower 9300 | 1.8 GB | 1.8 GB | 330 MB | 5 分 | 17 分 |
| FTD を搭載した ASA 5500-X シリーズ | 1.9 GB | 110 MB | 310 MB | 12 分 | 31 分 |
| FTDv：VMware | 2.0 GB | 110 MB | 310 MB | 8 分 | 8 分 |
| Firepower 7000/8000 シリーズ | 3.6 GB | 170 MB | 680 MB | 11 分 | 97 分 |
| ASA FirePOWER | 4.2 GB | 36 MB | 630 MB | 54 分 | 51 分 |
| NGIPSv | 2.4 GB | 150 MB | 470 MB | 11 分 | 15 分 |

# バージョン 6.4.0.9 の時間とディスク容量

表 *33 :* バージョン *6.4.0.9* の時間とディスク容量

| プラットフォーム | ボリュームの容量 | 必要容量 | FMC の容量 | アップグレード時間 | リブート時間 |
|---|---|---|---|---|---|
| FMC | 3.7 GB | 170 MB | — | 41 分 | 10 分 |
| FMCv：VMware | 3.7 GB | 170 MB | — | 28 分 | 6 分 |
| Firepower 1000 シリーズ | 2.9 GB | 2.9 GB | 530 MB | 11 分 | 14 分 |

| プラットフォーム | ボリュームの容量 | 必要容量 | FMC の容量 | アップグレード時間 | リブート時間 |
|---|---|---|---|---|---|
| Firepower 2100 シリーズ | 2.6 GB | 2.6 GB | 510 MB | 10 分 | 13 分 |
| Firepower 4100 シリーズ | 1.8 GB | 1.8 GB | 310 MB | 4 分 | 10 分 |
| Firepower 9300 | 1.8 GB | 1.8 GB | 310 MB | 4 分 | 10 分 |
| FTD を搭載した ASA 5500-X シリーズ | 1.9 GB | 290 MB | 290 MB | 12 分 | 42 分 |
| FTDv：VMware | 1.9 GB | 290 MB | 290 MB | 7 分 | 9 分 |
| Firepower 7000/8000 シリーズ | 3.7 GB | 170 MB | 650 MB | 20 分 | 6 分 |
| ASA FirePOWER | 4.2 GB | 36 MB | 600 MB | 48 分 | 48 分 |
| NGIPSv | 2.1 GB | 150 MB | 450 MB | 6 分 | 4 分 |

# バージョン 6.4.0.8 の時間とディスク容量

**表 *34 :* バージョン *6.4.0.8* の時間とディスク容量**

| プラットフォーム | ボリュームの容量 | 必要容量 | FMC の容量 | アップグレード時間 |
|---|---|---|---|---|
| FMC | 5.0 GB | 170 MB | — | 44 分 |
| FMCv：VMware | 5.1 GB | 170 MB | — | 32 分 |
| Firepower 1000 シリーズ | 3.0 GB | 3.0 GB | 530 MB | 18 分 |
| Firepower 2100 シリーズ | 2.5 GB | 2.5 GB | 510 MB | 18 分 |
| Firepower 4100 シリーズ | 1.8 GB | 1.8 GB | 310 MB | 14 分 |
| Firepower 9300 | 2.0 GB | 2.0 GB | 310 MB | 11 分 |
| FTD を搭載した ASA 5500-X シリーズ | 1.8 GB | 110 MB | 290 MB | 17 分 |
| FTDv：VMware | 1.9 GB | 110 MB | 290 MB | 12 分 |
| Firepower 7000/8000 シリーズ | 3.7 GB | 190 MB | 650 MB | 25 分 |

| プラットフォーム | ボリュームの容量 | 必要容量 | FMC の容量 | アップグレード時間 |
|---|---|---|---|---|
| ASA FirePOWER | 2.2 GB | 110 MB | 590 MB | 16 分 |
| NGIPSv | 2.1 GB | 150 MB | 450 MB | 9 分 |

# バージョン 6.4.0.7 の時間とディスク容量

表 *35 :* バージョン *6.4.0.7* の時間とディスク容量

| プラットフォーム | ボリュームの容量 | 必要容量 | FMC の容量 | アップグレード時間 |
|---|---|---|---|---|
| FMC | 4.9 GB | 170 MB | — | 41 分 |
| FMCv：VMware | 5.1 GB | 170 MB | — | 32 分 |
| Firepower 1000 シリーズ | 2.9 GB | 2.9 GB | 530 MB | 17 分 |
| Firepower 2100 シリーズ | 2.4 GB | 2.4 GB | 500 MB | 17 分 |
| Firepower 4100 シリーズ | 1.7 GB | 1.7 GB | 310 MB | 15 分 |
| Firepower 9300 | 2.4 GB | 2.4 GB | 310 MB | 12 分 |
| FTD を搭載した ASA 5500-X シリーズ | 1.9 GB | 110 MB | 290 MB | 18 分 |
| FTDv：VMware | 1.8 GB | 110 MB | 290 MB | 9 分 |
| Firepower 7000/8000 シリーズ | 3.7 GB | 190 MB | 650 MB | 28 分 |
| ASA FirePOWER | 4.2 GB | 36 MB | 590 MB | 54 分 |
| NGIPSv | 2.3 GB | 150 MB | 450 MB | 9 分 |

# バージョン 6.4.0.6 の時間とディスク容量

バージョン 6.4.0.6 は 2019 年 12 月 19 日に シスコ サポートおよびダウンロード サイト から削除されました。このバージョンを実行している場合は、アップグレードすることをお勧めします。

# バージョン 6.4.0.5 の時間とディスク容量

表 *36 :* バージョン *6.4.0.5* の時間とディスク容量

| プラットフォーム | ボリュームの容量 | 必要容量 | FMC の容量 | アップグレード時間 |
|---|---|---|---|---|
| FMC | 5.0 GB | 170 MB | — | 39 分 |
| FMCv：VMware | 3.7 GB | 170 MB | — | 27 分 |
| Firepower 1000 シリーズ | 2.9 GB | 2.9 GB | 530 MB | 26 分 |
| Firepower 2100 シリーズ | 2.5 GB | 2.5 GB | 500 MB | 16 分 |
| Firepower 4100 シリーズ | 1.8 GB | 1.8 GB | 310 MB | 12 分 |
| Firepower 9300 | 1.8 GB | 1.8 GB | 310 MB | 11 分 |
| FTD を搭載した ASA 5500-X シリーズ | 1.8 GB | 110 MB | 290 MB | 20 分 |
| FTDv：VMware | 1.8 GB | 110 MB | 290 MB | 10 分 |
| Firepower 7000/8000 シリーズ | 3.6 GB | 170 MB | 650 MB | 26 分 |
| ASA FirePOWER | 4.1 GB | 36 MB | 590 MB | 45 分 |
| NGIPSv | 2.1 GB | 150 MB | 450 MB | 10 分 |

# バージョン 6.4.0.4 の時間とディスク容量

表 *37 :* バージョン *6.4.0.4* の時間とディスク容量

| プラットフォーム | ボリュームの容量 | 必要容量 | FMC の容量 | アップグレード時間 |
|---|---|---|---|---|
| FMC | 4.4 GB | 170 MB | — | 35 分 |
| FMCv：VMware | 4.8 GB | 170 MB | — | 31 分 |
| Firepower 1000 シリーズ | 2.9 GB | 2.9 GB | 520 MB | 28 分 |
| Firepower 2100 シリーズ | 2.4 GB | 2.4 GB | 500 MB | 10 分 |
| Firepower 4100 シリーズ | 2.0 GB | 2.0 GB | 310 MB | 12 分 |
| Firepower 9300 | 1.7 GB | 1.7 GB | 310 MB | 10 分 |

| プラットフォーム | ボリュームの容量 | 必要容量 | FMC の容量 | アップグレード時間 |
|---|---|---|---|---|
| FTD を搭載した ASA 5500-X シリーズ | 1.8 GB | 110 MB | 290 MB | 29 分 |
| FTDv：VMware | 1.8 GB | 110 MB | 290 MB | 8 分 |
| Firepower 7000/8000 シリーズ | 3.6 GB | 170 MB | 650 MB | 24 分 |
| ASA FirePOWER | 4.2 GB | 36 MB | 600 MB | 55 分 |
| NGIPSv | 2.1 GB | 150 MB | 550 MB | 10 分 |

# バージョン 6.4.0.3 の時間とディスク容量

**表 *38 :* バージョン *6.4.0.3* の時間とディスク容量**

| プラットフォーム | ボリュームの容量 | 必要容量 | FMC の容量 | アップグレード時間 |
|---|---|---|---|---|
| FMC | 3.2 GB | 24 MB | — | 34 分 |
| FMCv：VMware | 2.5 GB | 23 MB | — | 25 分 |
| Firepower 1000 シリーズ | 2.9 GB | 2.9 GB | 520 MB | 22 分 |
| Firepower 2100 シリーズ | 2.4 GB | 2.4 GB | 500 MB | 19 分 |
| Firepower 4100 シリーズ | 1.7 GB | 1.7 GB | 310 MB | 12 分 |
| Firepower 9300 | 1.7 GB | 1.7 GB | 310 MB | 14 分 |
| FTD を搭載した ASA 5500-X シリーズ | 1.8 GB | 110 MB | 290 MB | 18 分 |
| FTDv：VMware | 1.8 GB | 110 MB | 290 MB | 12 分 |
| Firepower 7000/8000 シリーズ | 1.9 GB | 21 MB | 370 MB | 20 分 |
| ASA FirePOWER | 2.5 GB | 2.5 GB | 320 MB | 28 分 |
| NGIPSv | 690 MB | 21 MB | 210 MB | 8 分 |

# バージョン 6.4.0.2 の時間とディスク容量

表 *39 :* バージョン *6.4.0.2* の時間とディスク容量

| プラットフォーム | ボリュームの容量 | 必要容量 | FMC の容量 | アップグレード時間 |
|---|---|---|---|---|
| FMC | 3.1 GB | 24 MB | — | 39 分 |
| FMCv：VMware | 2.5 GB | 23 MB | — | 24 分 |
| Firepower 2100 シリーズ | 1.9 GB | 1.9 GB | 480 MB | 19 分 |
| Firepower 4100 シリーズ | 2.3 GB | 2.3 GB | 290 MB | 11 分 |
| Firepower 9300 | 1.7 GB | 1.7 GB | 290 MB | 11 分 |
| FTD を搭載した ASA 5500-X シリーズ | 1.8 GB | 110 MB | 270 MB | 21 分 |
| FTDv：VMware | 1.2 GB | 110 MB | 270 MB | 10 分 |
| Firepower 7000/8000 シリーズ | 1.9 GB | 36 MB | 350 MB | 20 分 |
| ASA FirePOWER | 2.0 GB | 21 MB | 300 MB | 34 分 |
| NGIPSv | 630 MB | 21 MB | 190 MB | 10 分 |

# バージョン 6.4.0.1 の時間とディスク容量

表 *40 :* バージョン *6.4.0.1* の時間とディスク容量

| プラットフォーム | ボリュームの容量 | 必要容量 | FMC の容量 | アップグレード時間 |
|---|---|---|---|---|
| FMC | 1.8 GB | 24 MB | — | 50 分 |
| FMCv：VMware | 1.8 GB | 23 MB | — | 20 分 |
| Firepower 2100 シリーズ | 1.4 GB | 1.4 GB | 300 MB | 17 分 |
| Firepower 4100 シリーズ | 1.1 GB | 1.1 GB | 95 MB | 9 分 |
| Firepower 9300 | 1.1 GB | 1.1 GB | 95 MB | 10 分 |
| FTD を搭載した ASA 5500-X シリーズ | 550 MB | 110 MB | 76 MB | 16 分 |
| FTDv：VMware | 550 MB | 110 MB | 76 MB | 15 分 |

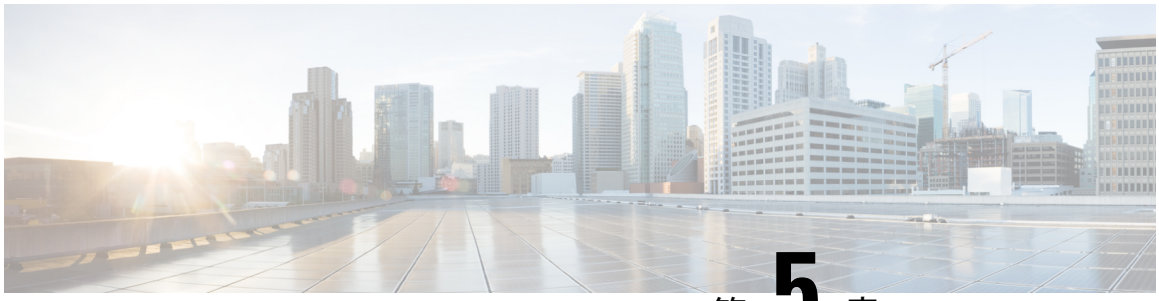
| プラットフォーム | ボリュームの容量 | 必要容量 | FMC の容量 | アップグレード時間 |
|---|---|---|---|---|
| Firepower 7000/8000 シリーズ | 59 MB | 21 MB | 2 MB | 14 分 |
| ASA FirePOWER | 85 MB | 20 MB | 2 MB | 30 分 |
| NGIPSv | 45 MB | 21 MB | 2 MB | 10 分 |

# アップグレード手順

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

**表 *41 : Firepower* アップグレード手順**

| タスク | ガイド |
|---|---|
| Firepower Management Center の展開でアップグレードします。 | Cisco Firepower Management Center Upgrade Guide, Version 6.0–7.0 |
| Firepower Device Manager を搭載した Firepower Threat Defense をアップグレードします。 | Firepower Device Manager 用 Cisco Firepower Threat Defense 構成ガイド<br>アップグレード先のバージョンではなく、現在実行している Firepower Threat Defense バージョンのガイドの「*System Management*」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, Firepower 6.0.1–7.0.x or ASA 9.4(1)–9.16(x) with FXOS 1.1.1–2.10.1 |
| 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 5508-X、ASA 5516-X で ROMMON イメージをアップグレードします。 | Cisco ASA and Firepower Threat Defense Reimage Guide<br>「*Upgrade the ROMMON Image*」のセクションを参照してください。常に最新のイメージがあることを確認してください。 |



第 5 章

# パッチのアンインストール

Firepower Management Center および ASDM の展開では、ほとんどのパッチをアンインストールすることができます。アンインストールすると、アップグレード前のバージョンに戻り、設定は変更されません。

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



## アンインストールに対応するパッチ

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

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

⚠

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

### アンインストールに対応したバージョン 6.4.0 のパッチ

この表は、バージョン 6.4.0 のパッチでサポートされているアンインストールのシナリオを示しています。アンインストールすると、アップグレード前のパッチレベルに戻ることに注意してください。アンインストールによってサポートされているよりも前に戻る場合は、イメージを再作成してから、目的のパッチレベルにアップグレードすることをお勧めします。

**表 *42 :* アンインストールに対応したバージョン *6.4.0* のパッチ**

| 現在のバージョン | アンインストールすべき最も古いバージョン | | |
|---|---|---|---|
| | **FTD/FTDv** | **Firepower 7000/8000<br>ASA FirePOWER<br>NGIPSv** | **FMC/FMCv** |
| 6.4.0.5 以降 | 6.4.0.4 | 6.4.0.4 | 6.4.0.4 |
| 6.4.0.4 | — | — | — |
| 6.4.0.3 | 6.4.0 | — | — |
| 6.4.0.2 | 6.4.0 | — | — |
| 6.4.0.1 | 6.4.0 | 6.4.0 | 6.4.0 |

# アンインストールパッチのガイドライン

### シェルを使用して先にデバイスからアンインストールする

Firepower Management Center では、その管理対象デバイスと同じまたはより新しいバージョンを実行する必要があります。これは FMC 展開で、最初に管理対象デバイスからパッチをアンインストールすることを意味します。

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

- 高可用性および拡張性展開のデバイスからパッチを一括でアンインストールすることはできません。中断を最小限に抑えるアンインストール順序を計画するには、「HA/スケーラビリティ環境でのアンインストール順序 （55 ページ）」を参照してください。
- FMC または ASDM を使用してデバイスからパッチをアンインストールすることも、7000/8000 シリーズデバイスのローカル Web インターフェイスを使用することもできません。
- FMC のユーザーアカウントを使用して、いずれかの管理対象デバイスにログインしてデバイスからパッチをアンインストールすることはできません。デバイスでは、独自のユーザーアカウントが維持されます。

- デバイスの admin ユーザーとして、または CLI 設定アクセス権を持つ別のローカル ユーザーとして、デバイス シェルにアクセスできる必要があります。シェル アクセスを無効にした場合、デバイスパッチをアンインストールすることはできません。デバイスのロックダウンを元に戻すには、Cisco TAC にご連絡ください。

### デバイスの後に FMC からアンインストールする

管理対象デバイスからアンインストールした後に、FMC からパッチをアンインストールします。アップグレードと同様に、高可用性 FMC から一度に 1 つずつアンインストールする必要があります。詳しくは、「HA/スケーラビリティ環境でのアンインストール順序 （55 ページ）」を参照してください。

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

# HA/スケーラビリティ環境でのアンインストール順序

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

通常は次のことに注意してください。

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

表 *43 : HA* 内の *FMC* の場合におけるアンインストール順序

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

表 *44 : HA* またはクラスタ内の *FTD* デバイスの場合におけるアンインストール順序

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

表 *45 : HA* またはスタック内の *7000/8000* シリーズ デバイスの場合におけるアンインストール順序

| 7000/8000 シリーズの環境 | アンインストール順序 |
|---|---|
| 7000/8000 シリーズ ハイ アベイラビリティ | 常にスタンバイからアンインストールします。HA ペア内の 7000/8000 シリーズ デバイスは、パッチのアンインストール中はメンテナンス モードで動作します。<br>**1.** スタンバイからアンインストールします。<br>**2.** ロールを切り替えます。<br>**3.** 新しいスタンバイからアンインストールします。 |
| 8000 シリーズ スタック | スタック内のすべてのデバイスから同時にアンインストールします。すべてのデバイスからパッチをアンインストールするまで、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。 |

表 *46 : ASA* フェール オーバーペア/クラスタ内の *ASA with FirePOWER Services* デバイスの場合におけるアンインストール順序

| ASA 展開 | アンインストール順序 |
|---|---|
| ASA FirePOWER が有効な ASA アクティブ/スタンバイ フェールオーバー ペア | 常にスタンバイからアンインストールします。<br>**1.** スタンバイ ASA デバイスの ASA FirePOWER モジュールからアンインストールします。<br>**2.** フェールオーバーします。<br>**3.** 新しいスタンバイ ASA デバイスの ASA FirePOWER モジュールからアンインストールします。 |
| ASA FirePOWER が有効な ASA アクティブ/アクティブ フェールオーバー ペア | アンインストールしないユニットの両方のフェールオーバー グループをアクティブにします。<br>**1.** プライマリ ASA デバイスの両方のフェールオーバー グループをアクティブにします。<br>**2.** セカンダリ ASA デバイスの ASA FirePOWER モジュールからアンインストールします。<br>**3.** セカンダリ ASA デバイスの両方のフェールオーバー グループをアクティブにします。<br>**4.** プライマリ ASA デバイスの ASA FirePOWER モジュールからアンインストールします。 |

| ASA 展開 | アンインストール順序 |
|---|---|
| ASA FirePOWER が有効な ASA クラスタ | アンインストールの前に、各ユニットでクラスタリングを無効にします。一度に1つのユニットからアンインストールし、制御ユニットを最後に残します。<br>**1.** データユニットでクラスタリングを無効にします。<br>**2.** そのユニットの ASA FirePOWER モジュールからアンインストールします。<br>**3.** クラスタリングを再び有効にします。ユニットが再びクラスタに参加するのを待ちます。<br>**4.** 各データユニットに対して手順を繰り返します。<br>**5.** 制御ユニットでクラスタリングを無効にします。新しい制御ユニットが引き継ぐまで待ちます。<br>**6.** 以前の制御ユニットの ASA FirePOWER モジュールからアンインストールします。<br>**7.** クラスタリングを再び有効にします。 |

# アンインストールの手順

## スタンドアロン FMC からのアンインストール

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

### 始める前に

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

**ステップ 1** 構成が古い管理対象デバイスに展開します。

アンインストールする前に展開すると、失敗する可能性が減少します。

**ステップ 2** 事前チェックを実行します。

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

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

**ステップ 3** **[システム（System）] > [更新（Updates）]** を選択します。

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

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

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

アンインストールすることを確認し、FMC を再起動します。

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

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

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

**ステップ 8** 成功したことを確認します。

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

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

**ステップ 10** 構成を再展開します。

# ハイ アベイラビリティ FMC からのアンインストール

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

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

### 始める前に

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

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

アンインストールする前に展開すると、失敗する可能性が減少します。

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

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

**ステップ 3** 同期を一時停止します。

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

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

「スタンドアロン FMC からのアンインストール （58 ページ）」の手順に従います。ただし、初期の展開は省略し、各 FMC で更新が成功したことを確認したら停止します。要約すると、それぞれの FMC で以下の手順を実行します。

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

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

**ステップ 5** アクティブ ピアにする FMC で、同期を再開します。

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

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

**ステップ 7** 構成を再展開します。

# 任意のデバイスからのアンインストール（FMC マネージド）

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

### 始める前に

特にHA/スケーラビリティの環境において、正しいデバイスからアンインストールしようとしていることを確認してください。「HA/スケーラビリティ環境でのアンインストール順序（55 ページ）」を参照してください。

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

アンインストールする前に展開すると、失敗する可能性が減少します。

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

**ステップ 2** 事前チェックを実行します。

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

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

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

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

| | |
|---|---|
| Firepower 1000 シリーズ | `connect ftd` |
| Firepower 2100 シリーズ | `connect ftd` |
| Firepower 4100/9300 | `connect module` *slot_number* `console`、次に `connect ftd`（最初のログインのみ） |
| ASA FirePOWER（ASA 5585-X シリーズを除く） | `session sfr` |

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

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

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

Firepowerアプライアンスにパッチを適用すると、そのパッチを簡単に識別できるアンインストーラーが、アップグレードディレクトリに自動的に作成されます。「パッケージのアンインストール（64ページ）」を参照してください。

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

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

**ステップ 6** アンインストールをモニターします。

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

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

**ステップ 7** 成功したことを確認します。

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

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

**ステップ 9** 構成を再展開します。

**例外**：HA または 拡張性の展開では、混合したバージョンのクラスタ、スタック、または HA ペアには展開しないでください。展開は、すべてのメンバーについてこの手順を繰り返した後にのみ行います。

### 次のタスク

HA/スケーラビリティ環境の場合は、各デバイスについて計画した順序でこの手順を繰り返します。その後、最終的な調整を行います。たとえば、FTD HA 環境では、両方のピアからアンインストールした後に HA を再確立します。

# ASA FirePOWER からのアンインストール（ASDM マネージド）

次の手順を実行して、ローカル管理されている ASA FirePOWER モジュールからパッチをアンインストールします。FMC を使用して ASA FirePOWER を管理している場合は、「任意のデバイスからのアンインストール（FMC マネージド）（60 ページ）」を参照してください。

### 始める前に

特に ASA のフェールオーバー/クラスタ環境において、正しいデバイスからアンインストールしようとしていることを確認してください。「HA/スケーラビリティ環境でのアンインストール順序 （55 ページ）」を参照してください。

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

アンインストールする前に展開すると、失敗する可能性が減少します。

**ステップ 2** 事前チェックを実行します。

- システム ステータス：**[モニターリング（Monitoring）] > [ASA FirePOWER のモニターリング（ASA FirePOWER Monitoring）] > [統計情報（Statistics）]** を選択し、すべてが想定どおりであることを確認します。
- 実行中のタスク：**[モニターリング（Monitoring）] > [ASA FirePOWER のモニターリング（ASA FirePOWER Monitoring）] > [タスク（Task）]** を選択し、必須タスクが完了していることを確認します。アンインストールの開始時に実行中だったタスクは停止され、失敗したタスクとなって再開できなくなります。後で失敗ステータス メッセージを手動で削除できます。

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

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

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

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

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

署名付きの（.tar）パッケージは解凍しないでください。

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

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

**ステップ 6** アンインストールをモニターします。

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

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

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

**ステップ 7** 成功したことを確認します。

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

**ステップ 8** 構成を再展開します。

### 次のタスク

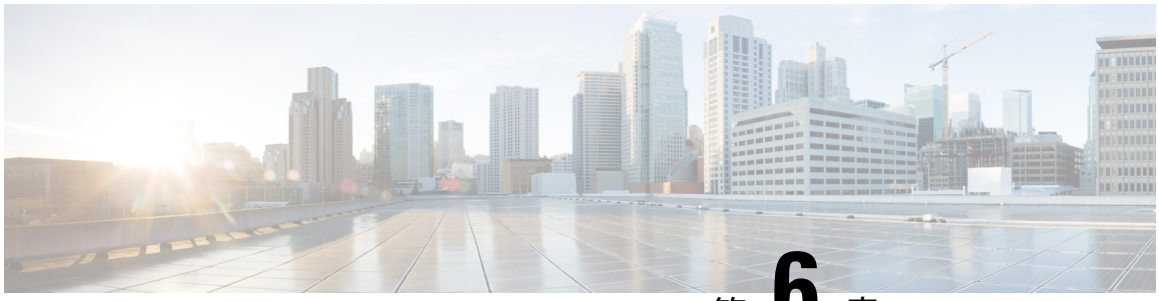
ASA フェールオーバー/クラスタ環境の場合は、各デバイスについて計画した順序でこの手順を繰り返します。

# パッケージのアンインストール

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

- `/ngfw/var/sf/updates`（Firepower Threat Defense デバイスの場合）
- `/var/sf/updates`（Firepower Management Center および NGIPS デバイス（7000/8000 シリーズ、ASA FirePOWER、NGIPSv）の場合）

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



第 6 章

# ソフトウェアのインストール

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

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



## インストールにおけるチェックリストおよびガイドライン

再イメージ化によって、システムパスワードを含むほとんどの設定が工場出荷時の初期状態に戻ります。このチェックリストは、一般的な再イメージ化の問題を回避できるアクションを示しています。ただし、このチェックリストは包括的なものではありません。詳細な手順については、該当する設置ガイド『取り付け手順 （69 ページ）』を参照してください。

表 *47:*

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

| ✓ | アクション/チェック |
|---|---|
| | **FMC 管理からデバイスを削除する必要があるか判断します。**<br>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。<br>• 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。<br>• 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。<br>再イメージ化後にバックアップから復元する場合は、デバイスをリモート管理から削除する必要はありません。 |
| | **ライセンスの問題に対処します。**<br>アプライアンスを再イメージ化する前に、ライセンスの問題に対処してください。孤立した権限付与の発生を防ぐために、Cisco Smart Software Manager（CSSM）から登録解除することが必要になる場合があります。これで、再登録を防ぐことができます。または、新しいライセンスについてセールス部門に連絡する必要がある場合があります。<br>詳細については、以下を参照してください。<br>• ご使用の製品の設定ガイド。<br>• スマート ライセンスの登録解除 （68 ページ）<br>• Cisco Firepower System Feature Licenses Guide<br>• Frequently Asked Questions (FAQ) about Firepower Licensing |

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

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

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

### バージョン 6.3.0 以降へのバージョン 5.x ハードウェアの再イメージ化

バージョン 6.3+ のインストールパッケージの名前が変更されていると、古い物理アプライアンス（FMC 750、1500、2000、3500、4000 のほか、7000/8000 シリーズ デバイスと AMP モデル）の再イメージ化に関する問題が発生します。現在バージョン 5.x を実行していて、バージョン 6.4.0 を新規にインストールする必要がある場合は、インストールパッケージをダウンロードした後、その名前を「古い」名前に変更します。『Cisco Firepower Release Notes, Version 6.3.0』の「Renamed Upgrade and Installation Packages」の情報を参照してください。

FMC（Defense Center）をバージョン5.xからより新しいバージョンに再イメージ化した後、古いデバイスを管理することはできません。また、これらのデバイスを再イメージ化してから、FMC に再度追加する必要があります。シリーズ 2 デバイスは EOL であり、Firepower ソフトウェアの過去バージョン5.4.0.xを実行できないことに注意してください。それらのデバイスを置き換える必要があります。

# スマート ライセンスの登録解除

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

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

登録を解除すると、仮想アカウントからアプライアンスが削除され、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。

# 取り付け手順

表 *48 : Firepower Management Center* 取り付け手順

| FMC | ガイド |
|---|---|
| FMC 1600、2600、4600 | Cisco Firepower Management Center 1600, 2600, and 4600 Getting Started Guide |
| FMC 1000、2500、4500 | Cisco Firepower Management Center 1000, 2500, and 4500 Getting Started Guide |
| FMC 750、1500、3500<br>FMC 2000、4000 | Cisco Firepower Management Center 750, 1500, 2000, 3500 and 4000 Getting Started Guide |
| FMCv | Cisco Firepower Management Center Virtual Getting Started Guide |

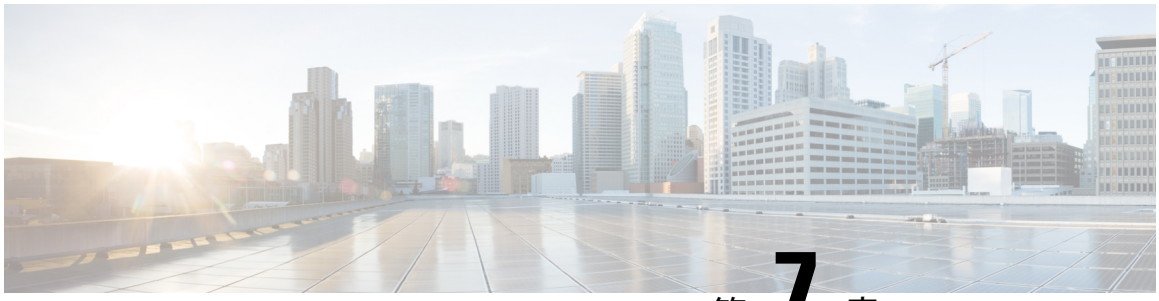
表 *49 : Firepower Threat Defense* 取り付け手順

| FTD プラットフォーム | ガイド |
|---|---|
| Firepower 1000/2100 シリーズ | Cisco ASA and Firepower Threat Defense Reimage Guide<br>Cisco FXOS Troubleshooting Guide for the Firepower 1000/2100 Series Running Firepower Threat Defense |
| Firepower 4100/9300 | Cisco Firepower 4100/9300 FXOS Configuration Guides：イメージ管理に関する章<br>Cisco Firepower 4100 スタートアップガイド<br>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：AWS | Cisco Firepower Threat Defense Virtual for the AWS Cloud Getting Started Guide |
| FTDv：Azure | Cisco Firepower Threat Defense Virtual for the Microsoft Azure Cloud Quick Start Guide |

| FTDプラットフォーム | ガイド |
|---|---|
| FTDv：KVM | Cisco Firepower Threat Defense Virtual for KVM Getting Started Guide |
| FTDv：VMware | Cisco Firepower Threat Defense Virtual for VMware Getting Started Guide |

表 *50 : 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<br>ASDM Book 2: Cisco ASA Series Firewall ASDM Configuration Guide：Managing the ASA FirePOWER Module |



第 7 章

# 資料

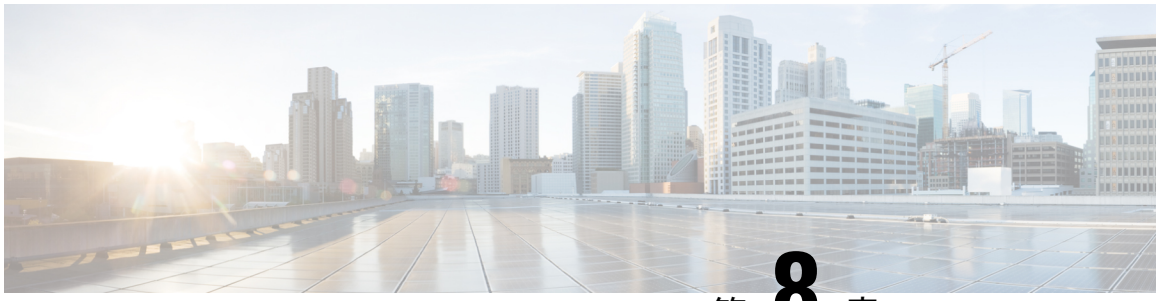
パッチで必要な場合は、Firepower のマニュアルを更新します。


- ドキュメント ロードマップ （71 ページ）


# ドキュメント ロードマップ

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

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



第 8 章

# 解決済みの問題

便宜上、リリースノートには、各パッチの解決済みの問題が記載されています。

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

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

# 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 *51* : 新しいビルドを使用したバージョン *6.4.0.x* パッチ**

| バージョン | 新しいビルド | リリース日 | プラットフォーム | 解決済み |
|---|---|---|---|---|
| 6.4.0.2 | 35 | 2019 年 7 月 3 日 | FMC/FMCv<br>FTD/FTDv（FirePOWER 1000 シリーズ以外） | CSCvq34224：マネージャをアップグレードすると、Firepower プライマリ検出エンジン プロセスが終了する。<br>すでにバージョン 6.4.0.2-34 にアップグレードしていて、ハイアベイラビリティ用に FTD デバイスが設定されている場合は、ホットフィックス F を適用します。FMC 展開では、FMC にホットフィックスを適用します。FDM 展開では、両方のデバイスにホットフィックスを適用します。 |

# バージョン 6.4.0.14 で解決済みの問題

**表 *52* : バージョン *6.4.0.14* で解決済みの問題**

| 不具合 ID | タイトル |
|---|---|
| CSCwa46963 | セキュリティ：CVE-2021-44228 -> Log4j 2 の脆弱性 |
| CSCwa70008 | 期限切れの証明書がセキュリティ Intel を引き起こし、マルウェアファイルの事前分類署名の更新が失敗する |
| CSCwa88571 | スマートポータルを使用して FMC を登録できない |

# バージョン 6.4.0.13 で解決済みの問題

表 *53* : バージョン *6.4.0.13* で解決済みの問題

| 不具合 ID | タイトル |
|---|---|
| CSCum03297 | ENH：ASA は MAXHOG のタイムスタンプを「show proc cpu-hog」に保存する必要がある |
| CSCvg66052 | Firepower アプライアンスで 2 つの CPU コアが継続的にスパイクする |
| CSCvi58484 | クラスタ：別のクラスタユニットに応答が着信する場合は、外部 IP への FTD/ASA を送信元とする ping が失敗することがある |
| CSCvm76755 | DP-CP arp-in キューと adj-absent キューを分離する必要があります |
| CSCvp16933 | Cisco Firepower Threat Defense ソフトウェアのシェルアクセスの脆弱性 |
| CSCvp69936 | ASA：tcp_intercept スレッド名 thread detection でのトレースバック |
| CSCvq39187 | KP：ホストへの SSH 中にホストキーの検証が失敗する |
| CSCvq43454 | ENH：SAML 認証を使用しているときに、「NotValidBefore」タイムスタンプの許容時間をサポートする |
| CSCvq54299 | 両方の A/S ユニットの再起動後、2100 で SL を使用すると、一部のコンテキスト設定がロードされない場合がある |
| CSCvr11958 | AWS FTD：「ERROR: failed to set interface to promiscuous mode」により展開が失敗する |
| CSCvr33586 | FPR1010：しきい値を超えた場合の SSD の温度/警告を追加する |
| CSCvr38379 | FPR2100 の「自動インストール」機能を使用すると、アップグレードした FTD がベース FTD バージョンに再イメージ化されない |
| CSCvr39217 | リブート後、FXOS SNMP ユーザーが永続されない |
| CSCvs27336 | Smart Call Home プロセスにより ASA がトレースバックする |
| CSCvs47365 | FXOS 2.9.1 アップデートを使用すると、FMC で発生するイベントレートが低下するか、デバイスからイベントレートが来なくなる |
| CSCvt10944 | VTI トンネル経由で EMIX トラフィックを送信しているときに CTM がクラッシュした |
| CSCvt15348 | マルチコアプラットフォームで ASA show processes cpu-usage output が誤解を招く |

| 不具合 ID | タイトル |
|---|---|
| CSCvt25917 | FTD CLI：無効になっているローカルユーザーの表示に失敗し、元に戻すことができない |
| CSCvt31292 | FTD デバイスが SSE にイベントを送信しない場合がある |
| CSCvt64238 | FXOS pktmgr Rx Drops カウンタが LACP ポートチャネルで増加し続ける |
| CSCvt85766 | FPR2k：アップグレード後に FCM Syslog の [Remote Destinations] タブが表示されなくなる |
| CSCvu36302 | vpn-addr-assign local reuse-delay が設定されている場合、%ASA-3-737403 が誤って使用される |
| CSCvu97242 | FTD 2100：クラッシュ時に Corefile と crashinfo の両方が切り捨てられ、不完全になることがある |
| CSCvv07917 | ASA が新しいルートを学習すると、フローティングスタティックによって作成された ASP ルートテーブルが削除される |
| CSCvv20780 | ポリシーの展開が「展開トランザクションを保持できませんでした」エラーで失敗する |
| CSCvv24647 | FTD 2100 - SNMP：不正な値がイーサネット統計ポーリングに返される |
| CSCvv43190 | GRE ヘッダープロトコルフィールドが内部 IP ヘッダーのプロトコルフィールドと一致しない場合の暗号エンジンエラー |
| CSCvv48594 | メモリリーク：脅威の検出での snp_tcp_intercept_stat_top_n_integrate() による |
| CSCvv48942 | Snmpwalk がフェールオーバーインターフェイスのトラフィックカウンターを 0 として表示する |
| CSCvv55248 | ACL トランザクションコミット用に生成された Syslog が一貫した形式でなく、利用できない場合がある |
| CSCvv62499 | FMC：FTD がクラスタのメンバーである場合、Remove_peers.pl スクリプトが機能する必要がある |
| CSCvv71097 | トレースバック：ASA が snp_fdb_destroy_fh_callback + 104 をリロードする |
| CSCvv79459 | CCM レイヤ（スプリント 94、シーケンス 1）における WR6、WR8 および LTS18 コミット ID の更新 |
| CSCvv84172 | 登録失敗時のクラスタ化されたテーブルと EO のダングリング参照 |
| CSCvv85029 | スレッド名 ace_work で ASA5555 がトレースバックし、リロードする |

| 不具合 ID | タイトル |
|---|---|
| CSCvv89715 | Firepower 8000 シリーズスタックの Fastpath ルールが FMC からランダムに消える |
| CSCvw03628 | RFC822Name が空に設定された名前制約により、ASA が CA 証明書をインポートしない |
| CSCvw06298 | 異なるコンテキストの共有インターフェイスで ASA が MAC アドレスを複製して、トラフィックに影響を与える |
| CSCvw13348 | CCM レイヤ（スプリント 98、seq 2）における WR6、WR8 および LTS18 コミット ID の更新 |
| CSCvw16165 | ポートチャネルのメンバーがダウンすると、Firepower 1010 シリーズがトラフィックの通過を停止する |
| CSCvw18614 | LINA プロセスでの ASA および FTD のトレースバック |
| CSCvw48829 | 「show clock」のタイムゾーンが「show run clock」のタイムゾーンと異なる |
| CSCvw62526 | エンジニアリング ASA Build での ASAトレースバックとリロード：9.12.3.237 |
| CSCvw68593 | Linux カーネル f の応答 ICMP パケットが制限される方法に欠陥がある |
| CSCvw71405 | 暗号化プロセスで FPR1120 が ASA トレースバックとリロードを実行している |
| CSCvw90923 | CCM レイヤ（スプリント 101、シーケンス 4）における WR6、WR8 および LTS18 コミット ID の更新 |
| CSCvw93159 | Firepower 2100：ASA および FTD が「Local disk 2 missing on server 1/1」というメッセージを生成する |
| CSCvw93276 | Cisco Firepower Management Center ソフトウェアのクロスサイト スクリプティングに対する脆弱性 |
| CSCvw97256 | リンク状態APIの読み取りが失敗した場合にリンク状態の更新を無視するには、rmu 読み取りエラーの処理が必要 |
| CSCvx04003 | CP への ARP スロットリング欠如のミス表示により、オーバーサブスクリプションになる |
| CSCvx06920 | CCM レイヤ（スプリント 103、シーケンス 5）における WR6、WR8 および LTS18 コミット ID の更新 |
| CSCvx14031 | IKEv2 セッションの CoA の後に DACL が削除されると、IPv4 DACL がアクティブデバイスでスタックする（トラフィックは影響を受けない） |

| 不具合 ID | タイトル |
|---|---|
| CSCvx16134 | マルチコアを使用しているにもかかわらず、「show processes cpu-usage」で見られる一部のプロセスで CPU の使用率が 100% になる |
| CSCvx23833 | IKEv2キー の再生成：Create_Child_SA 応答の直後に受信した新しい SPI を使用した ESP パケットの SPI が無効になる |
| CSCvx24537 | SAML：同じサブジェクト名を持つ 2 つ以上の IDP 証明書がある場合、SAML 認証が失敗する可能性がある |
| CSCvx25719 | X-Frame-Options ヘッダーが webvpn 応答ページで設定されていない |
| CSCvx29814 | DHCP GIADDR フィールドの IP アドレスが DHCP DECLINE を DHCP サーバに送信した後に反転する |
| CSCvx33904 | 1.9.5p2 より前の sudo には、ヒープベースのバッファオーバーフローがあり、特権昇格を使用できる |
| CSCvx34237 | FIPS 障害による ASA のリロード |
| CSCvx42081 | FPR4150 ASA Standby Ready ユニットのループが失敗し、設定を削除してインストールし直す必要がある |
| CSCvx43150 | FMC で、RMA 後のメンバーデバイスの登録プロセスが失敗する |
| CSCvx45976 | スレッド名：vnet-proxy（rip：socks_proxy_datarelay）で ASA および FTD のウォッチドッグが強制的にトレースバックとリロードを実行する |
| CSCvx47230 | IE および Windows プラットフォームの古いバージョンの X-Frame-Options ヘッダーのサポート |
| CSCvx47550 | CCM レイヤ（スプリント 105、シーケンス 6）での WR6、WR8 および LTS18 コミット ID の更新 |
| CSCvx49715 | EVP_CipherUpdate、EVP_EncryptUpdate、EVP_DecryptUpdate への呼び出しは、 |
| CSCvx50980 | ASA CP の誤った計算により、パーセンテージが高くなる（CP CPU 100%） |
| CSCvx54235 | ASP キャプチャの dispatch-queue-limit にパケットがないと表示される |
| CSCvx57417 | スマートトンネルコード署名証明書の更新 |
| CSCvx64478 | SAML トランザクション中に不要なコンソールが出力される |
| CSCvx65745 | FPR2100：UE イベントがクラッシュをトリガーするために、octeon でカーネルパニックを有効にします。 |
| CSCvx66329 | FTD ホットフィックス Cisco_FTD_SSP_FP2K_Hotfix_O のインストールがスクリプト 000_start/125_verify_bundle.sh で失敗する |

| 不具合 ID | タイトル |
|---|---|
| CSCvx67468 | CCM レイヤ（スプリント 107、シーケンス 6）での WR6、WR8 および LTS18 コミット ID の更新 |
| CSCvx68355 | ASA：countryName が UTF8 としてエンコードされている場合、CA 証明書をインポートできない |
| CSCvx71571 | ASA：CSM で「エラー：ハッシュテーブルからエントリを削除できません」 |
| CSCvx75963 | キャプチャ取得中に ASA がトレースバックする |
| CSCvx77768 | Umbrella によるトレースバックとリロード |
| CSCvx80830 | Radius サーバーが dACL を送信し、vpn-simultaneous-logins が 1 に設定されていると、同じユーザーからの VPN 接続が失敗する |
| CSCvx86621 | ASA（lina）クロック（2010 年 1 月を常に表示）が fxos と正しく同期しない |
| CSCvx87709 | HAで FPR 2100 が ASA を実行するフェールオーバー中のウォッチドッグでのトレースバックとリロード |
| CSCvx95255 | 既存の ASDM コンテキストスイッチから新しい ASDM 接続を区別するための ASA のサポート変更 |
| CSCvx95884 | HA バルク同期中および通常の conn 同期中に CPU 使用率が高くなり、大量の「バッファなし」がドロップする |
| CSCvx97632 | クラスタコマンドを使用して長い宛先ファイル名を持つファイルをコピーする場合にASA がトレースバックおよびリロードする |
| CSCvx98807 | CCM レイヤ（スプリント 109、シーケンス 9）での WR6、WR8 および LTS18 コミット ID の更新 |
| CSCvy01752 | スレッド Lic HA クラスタでのトレースバック |
| CSCvy02448 | FPFPR2100 シリーズ プラットフォームの ASA で時刻同期が正しく機能しない |
| CSCvy02703 | CTM Message Handler による ASA および FTD のトレースバック |
| CSCvy03006 | uauth のデバッグ機能の改善 |
| CSCvy03045 | 管理のコンテキストが変更されると、マルチコンテキスト ASA から connect fxos admin で FXOS にアクセスできない |
| CSCvy03907 | アクセス コントロール ポリシーの作成および編集が「ルール名は既に存在します」というエラーで失敗する |

| 不具合 ID | タイトル |
|---|---|
| CSCvy04869 | ユーザー証明書のキーサイズが 8192 ビットの場合、AnyConnect 証明書認証が失敗する |
| CSCvy07491 | access-list の再設定時の ASA トレースバック |
| CSCvy08798 | CCM レイヤ（スプリント 110、シーケンス 10）での WR6、WR8 および LTS18 コミット ID の更新 |
| CSCvy08908 | Java によってポート転送アプリケーションがブロックされる |
| CSCvy10583 | スレッド名 DATAPATH での ASA トレースバックおよびリロード |
| CSCvy10789 | LDAP パスワードで FTD 2110 ASCII 文字を使用できない |
| CSCvy12782 | FTD/ASA：HA の ixgbe-vf SRIOV インターフェイスで設定すると、PAT されたトラフィックが影響を受ける |
| CSCvy14721 | CH パケットの宛先ポートが送信元ポート以下であるときに FTD によって SSL トラフィックがドロップされる |
| CSCvy16179 | CSCuz67596 の修正を実行中でも、スレッド名 Unicorn Admin Handler で ASA クラスタがトレースバックする |
| CSCvy17078 | トレースバック：LINA プロセスで FPR 2110 の ASA がトレースバックおよびリロードする |
| CSCvy17365 | REST API ログインページの問題 |
| CSCvy17470 | IKEv2 の A/S フェールオーバーペアで ASA トレースバックとリロードが発生する |
| CSCvy18366 | FPR1k および ISA3k で pdts_pd_segment.c:1941 からの LINA クラッシュ |
| CSCvy21334 | 「スイッチオーバーなし」の場合、アクティブは CoA アップデートをスタンバイに送信しようとする |
| CSCvy23349 | FTD がインラインペア展開で TCP フローを不必要に ACK する |
| CSCvy25849 | HTTP 応答に文字列「OK」が含まれていない場合、ASA が OCSP 応答の処理に失敗する |
| CSCvy31424 | QP FTD アプリケーションが、FXOS/FTD アップグレード後に古い affinity.conf が原因で起動に失敗する |
| CSCvy33105 | DNS ルックアップが有効な場合、「show route bgp」または「show route isis」であいまいなコマンドエラーが表示される |
| CSCvy33676 | 以前の動的 xlate が作成されると、FTD で UN-NAT が作成される |

| 不具合 ID | タイトル |
|---|---|
| CSCvy35737 | Anyconnect パッケージの検証中に FTD のトレースバックとリロードが発生する |
| CSCvy35948 | CCM レイヤ（スプリント 111、シーケンス 11）での WR6、WR8 および LTS18 コミット ID の更新 |
| CSCvy39621 | ASA/FTDは、最大再試行回数に達した後も連続的な RADIUS アクセス要求を送信する |
| CSCvy39659 | ASA/FTD がスレッド名「DATAPATH-15-14815」でトレースバックし、リロードすることがある |
| CSCvy43447 | マルチインスタンス FTD の Lic TMR スレッドでの FTDトレースバックとリロード |
| CSCvy46026 | [Device] > [Device management] でデバイスを開こうとすると、「Unable to load container (UUID)」と表示される |
| CSCvy47108 | UAuth エントリがスタックしているため、リモートアクセス IKEv2 VPN セッションを確立できない |
| CSCvy48159 | メモリヘッダー検証によるプロセス名 lina での ASA トレースバックとリロード |
| CSCvy49732 | ASA/FTD がスレッド名「ssh」でトレースバックし、リロードすることがある |
| CSCvy50011 | IKE デーモンプロセスでの ASA トレースバックおよびリロード |
| CSCvy51814 | Firepower フローオフロードが、すべての既存および新しいフローのオフロードを停止させる |
| CSCvy52074 | ASA/FTD がスレッド名「webvpn_task」でトレースバックおよびリロードすることがある |
| CSCvy53461 | RSA キーと証明書が ASA コード 9.12.x を使用した WS-SVC-ASA-SM1-K7 でリロード後に削除される |
| CSCvy55356 | ドキュメントに反して、10 ミリ秒未満の CPU 占有が発生する |
| CSCvy57905 | VTI トンネルインターフェイスが、HA の KP および WM プラットフォームでリロード後もダウンしたままになる |
| CSCvy60574 | ポート dcosAG リークの修正を CSCvx14602 から KP/WM へ |
| CSCvy61008 | Lina と FXOS 間の同期外れの時間 |

| 不具合 ID | タイトル |
|---|---|
| CSCvy64145 | CCM レイヤ（スプリント 113、シーケンス 12）での WR6、WR8 および LTS18 コミット ID の更新 |
| CSCvy64492 | ASAv が MAC テーブルの自身のアドレスに非アイデンティティ L2 エントリを追加し、HA hello をドロップする |
| CSCvy64911 | デバッグ：crasLocalAddress の SNMP MIB 値に IP アドレスが表示されない |
| CSCvy67756 | Firepower サービスの HTTPS トラフィックは、SSL ポリシーでルールを復号化しない（Do not decript）ルールと一致すると動作を停止する |
| CSCvy69189 | vpnfol_sync/Bulk-sync keytab がスタックしているため、FTD HA がバルク状態のままになる |
| CSCvy72846 | ASA アカウンティングが誤った Acct-Session-Time を報告する |
| CSCvy74781 | スタンバイデバイスが、フェールオーバー後に SSL トラフィックのキープアライブメッセージを送信する |
| CSCvy80202 | CSCvm48451 が修正されているにもかかわらず、4100 で侵入イベントパフォーマンスのグラフが空白になる |
| CSCvy89658 | CCM レイヤ（スプリント 114、シーケンス 13）での WR6、WR8 および LTS18 コミット ID の更新 |
| CSCvy91668 | スティッキネストラフィックによる PAT プールの枯渇は、新しい接続のドロップにつながる可能性があります。 |
| CSCvy92990 | 7.0 へのアップグレード後の SSL に関連する FTD トレースバックとリロード |
| CSCvy96625 | CSCvr33428 および CSCvy39659 で導入された「修正」を元に戻す |
| CSCvy96698 | FXOS portmgr で速度値を 2 回チェックするスプリアス ステータス アクションを解決する |
| CSCvy98027 | FXOS で物理インターフェイスが動作しているのにアプリケーションインターフェイスがダウンする |
| CSCvy98458 | FP21xx のトレースバック「Panic:DATAPATH-10-xxxx -remove_mem_from_head: Error - found a bad header」 |
| CSCvz00383 | スレッド名 Checkheaps で FTD lina トレースバックとリロードが発生する |
| CSCvz00699 | ASA のアップグレード後、webvpn でトレースバックとリロードが定期的に発生する |

| 不具合 ID | タイトル |
|---|---|
| CSCvz05189 | クラスタでの xlate の複製中に Lina トレースバックによる FTD のリロードが発生する |
| CSCvz07614 | ASA：孤立した SSH セッションでは、CLI からポリシーマップを削除できない |
| CSCvz15529 | スレッド名 Datapath での ASA のトレースバックおよびリロード |
| CSCvz20544 | Anyconnect プロファイルのループ処理で、ASA および FTD がトレースバックおよびリロードする場合がある |
| CSCvz20679 | FTDv - Lina のトレースバックおよびリロード |
| CSCvz21886 | nat が IP ではなくポート番号に一致する pbr ACL に一致した場合、nat の un-nat が 2 回発生しない |
| CSCvz25434 | BVI が DHCP クライアントとして設定されている場合、1550 ブロックの枯渇が原因で ASA および FTD がトラフィックをブラックホールする |
| CSCvz27714 | ポリシー展開中の 8350 センサーでのインターフェイスのフラッピング |
| CSCvz29233 | ASA：システムコンテキストでインターフェイスのフラップが発生したときに、カスタムコンテキストからの ARP エントリが削除されない |
| CSCvz34831 | ASA が DACL のダウンロードに失敗した場合、試行を停止しない |
| CSCvz37306 | 既存のユーザーで複数のコンテキストスイッチを実行した後、ASDM セッションが新しいユーザーに提供されない |
| CSCvz38361 | 直接接続されていないネイバーのために BGP パケットがドロップされる |
| CSCvz39565 | バルク VPN セッション接続中に ASA または FTD がトレースバックおよびリロードする |
| CSCvz39646 | ASA または AnyConnect - 古い RADIUS セッション |
| CSCvz40352 | アクセスリストに明確なルールが存在するにもかかわらず、暗黙の ACL によって ASA トラフィックがドロップする |
| CSCvz43414 | HA のフェイルオーバー後に内部 LDAP 属性マッピングが失敗する |
| CSCvz43455 | hostscan のアップグレード中に ASAv がトレースバックを確認する |
| CSCvz48407 | スレッド名 DATAPATH-15-18621 でのトレースバックおよびリロード |
| CSCvz53142 | ASA が、name-server コマンドで指定されたインターフェイスを使用して IPv6 DNS サーバーに到達しない |
| CSCvz57710 | conf t が、context-config モードで disk0:/t に変換される |

| 不具合 ID | タイトル |
|---|---|
| CSCvz58710 | SCTP トラフィックにより ASA がトレースバックする |
| CSCvz60901 | ASA：IPv6 ネイバーの到達可能性に関する問題 |
| CSCvz60970 | LU を スターリンクに送信する際、enic_put / FREEB 内のスレッド名 DATAPATH-4-23199 で ASA がトレースバックする |
| CSCvz64470 | ICMP 到達不能メッセージ生成時のメモリ破損による ASA および FTD のトレースバックとリロード |
| CSCvz66795 | コマンド「show access-list」実行時の SSH プロセスでの ASA のトレースバックとリロード |
| CSCvz69571 | anyconnect セッションが終了した後、ASA ログに転送されたデータの間違った値が表示される |
| CSCvz73709 | ASA および FTD のスタンバイユニットが HA に参加できない |
| CSCvz77744 | OSPFv3：FTD の間違った「転送アドレス」が ospfv3 データベースに追加される |
| CSCvz81934 | CSCvx95884 によって導入された「修正」を元に戻す |
| CSCvz84850 | 「タイマーサービス」機能により、ASA および FTD のトレースバックとリロードが発生する |
| CSCvz87824 | 「snp_svcmod_heart_beat_timeout_cb」機能での ASASM のトレースバックとリロード |

# バージョン 6.4.0.12 で解決済みの問題

**表 *54* : バージョン *6.4.0.12* で解決済みの問題**

| 不具合 ID | タイトル |
|---|---|
| CSCtx83747 | Syslog 718055 に、間違った形式の MAC アドレスが含まれている |
| CSCui74211 | 期限切れの DHCP クライアントのリースが ASA スタンバイユニットで消去されない |
| CSCuj60109 | ENH：ASA-IC-6GE-SFP-A に接続された SFP トランシーバが CLI に表示されない |
| CSCuj99176 | ASA-SSM cplane キープアライブの通信遅延対する許容度を上げる |

| 不具合 ID | タイトル |
|---|---|
| CSCun74870 | ASA IKEv2：TS_UNSUPPORTED の代わりに NO-PROPOSAL-CHOSEN が送信される |
| CSCuq47482 | ENH：ASA の show tech に「show module x detail」を含める必要がある |
| CSCut44164 | ASA：「show tech」に暗号統計を追加する |
| CSCuu60064 | ENH：ASAv show tech に「show vm」を含める必要がある |
| CSCuu84198 | DHCPRelay デバッグは、DHCP サーバーからの無効なパラメータを強調表示する必要がある |
| CSCuw51499 | ACE の追加/削除、ACL オブジェクト/オブジェクトグループの編集で TCM が機能しない |
| CSCuy53106 | ASA OS で Syslog 717054 の証明書の有効期限が誤って計算される |
| CSCvb92169 | ASA が、より適切なフラグメント関連のログと ASP ドロップの理由を提供する必要がある |
| CSCvc40724 | 無効なグループ URL により、不適切な形式のメッセージが AnyConnect に返される |
| CSCvf88062 | CTM：Nitrox S/G の長さを検証する必要がある |
| CSCvg59385 | ASA ScanSafe コネクタのセカンダリ CWS タワーへのフェールオーバーに時間がかかりすぎる |
| CSCvg69380 | ASA：まれに発生した CP 処理での破損によってコンソールロックが発生する |
| CSCvg73237 | ENH：VPN の総容量の単なる割合ではなく、絶対値として CAC が設定される |
| CSCvh30209 | マルチキャストのオン/オフを繰り返し切り替える際に mfib_idb_get でトレースバックが発生する |
| CSCvh85504 | 「バックログステータス」正常性モジュールの偽陰性アラート |
| CSCvi07901 | IKEv2 AnyConnect 用の ASA で CISCO-REMOTE-ACCESS-MONITOR-MIB crasIPSecNumSessions がゼロになる |
| CSCvi85020 | SSH 設定の順序により、起動時のエラーメッセージ「SSH バージョン 1 はセキュアではありません（SSH version 1 is not secure）」が生成される |
| CSCvk51778 | ASA 5515/5525/5545/5555 での「show inventory」（または）「show environment」でドライバ/ioctl エラーログが表示される |
| CSCvm15088 | ENH：ASA5525 の「show environment」に PSU の詳細を追加 |

| 不具合 ID | タイトル |
|---|---|
| CSCvm78605 | ASA フェールオーバー：「show interface tunnel」が、トンネルソースをスタンバイ IP アドレスとして表示する |
| CSCvm82290 | IRB/TFW 設定でホストが到達不能な場合に ASA コアブロックが枯渇する |
| CSCvm98585 | 5525 FTD で観察される idfw モジュールからの CPU ホグ |
| CSCvn12453 | フローがハッシュされる RX リング番号を表示する debug menu コマンドが実装される |
| CSCvn16864 | ENH：ASA HTTP WebVPN ポータルに Content-Security-Policy ヘッダーがない |
| CSCvn16877 | ENH：ASA HTTP WebVPN ポータルに X-Content-Type-Options ヘッダーがない |
| CSCvn16887 | ENH：ASA HTTP WebVPN ポータルに X-XSS-Protection ヘッダーがない |
| CSCvn64647 | tcp_retrans_timeout 内部スレッド処理による ASA トレースバックおよびリロード |
| CSCvn82441 | [SXP] FPR-2110 の ASA とスイッチ間での SXP 接続の確立に関する問題 |
| CSCvn93683 | ASA：cluster exec show コマンドですべての出力が表示されない |
| CSCvn95731 | スレッド名 SSH での ASA トレースバックおよびリロード |
| CSCvo11623 | ASAv および Azure：登録時、スマートライセンスがカスタムテンプレートのホスト名を使用しない |
| CSCvo12504 | ASA：モジュールの差異が発生した場合、フェールオーバー FSM はマルチコンテキストでスタックする |
| CSCvo33227 | BusyBox udhcp コンポーネントにおける境界外読み取り情報開示の脆弱性 |
| CSCvo33896 | snmpd()：クエリを処理するためのメモリが不足している |
| CSCvo34210 | スレッド名 Unicorn Proxy Thread で ASA が 9.6.4.20 トレースバックを実行する |
| CSCvo58030 | インターフェイスに設定されているフェールオーバー MAC アドレスでのサブインターフェイスの削除が許可されていない |
| CSCvo64516 | TCP の syslog がダウンしている場合に ASA がコマンド認可に失敗する |
| CSCvo68887 | クラッシュファイル名のタイムスタンプはUTCだが、ローカルタイムゾーンになる |

| 不具合 ID | タイトル |
|---|---|
| CSCvo78772 | ENH：ASA WebVPN は「Cache-Control: no-cache」の代わりに「Cache-Control: no-store」を送信する必要がある |
| CSCvo81249 | ASA は、ASA（DNS クライアントとして機能する）とサーバ間で高レートの DNS クエリを引き起こす可能性がある |
| CSCvo86485 | 不正な HTML <base> 文法ベースのパーサーによるタグ処理 |
| CSCvo87430 | FTD：疑問符を含む ISAKMP VPN を展開できない |
| CSCvo99076 | ENH：AAA によってクライアントに割り当てられた静的 IP に対する IKEv2 クイック接続プリエンプト |
| CSCvp09083 | DHCP サーバーとして動作する ASA が、DHCP クライアントから送信された DHCP 更新要求パケットをドロップする |
| CSCvp10079 | FMC HA スイッチで DB スイッチロールが失敗する |
| CSCvp13352 | VPN セッションがタイムアウトした後でも、ASA はクライアント側接続に対する TCP キープアライブを実行し続ける |
| CSCvp16618 | HTML ベースタグ内の URL が、GBP で処理された後も書き換えられなない |
| CSCvp23530 | write standby または reload 後に、OSPF neighbor コマンドがスタンバイに複製されない |
| CSCvp29554 | ファイルシステムにアクセスする際のウォッチドッグタイムアウトによるトレースバックとリロード（webvpn 関連） |
| CSCvp29803 | Apache HTTP サーバーモジュールでスクリプトが任意のコードを実行する脆弱性 |
| CSCvp31311 | 特定のプラットフォームにおける最大セッション数に対して十分な PKI ハンドルが必要である |
| CSCvp38774 | WebVPN リライタが Web サイトを正しくロードしない |
| CSCvp42484 | MTU が変更されたときに IS-IS hello パケット長が正しい MTU に更新されない |
| CSCvp42722 | ASA が、syslog の接続先（バッファ、トラップなど）に対してロギングメッセージ 611103 を生成しない |
| CSCvp52437 | ASA：設定を保存すると、「プラットフォームがアプライアンスモード設定をサポートしていません（Platform does not support appliance mode configuration.）」というメッセージが表示される |

| 不具合 ID | タイトル |
|---|---|
| CSCvp56719 | Cisco FMC および FTD ソフトウェアの sftunnel で確認された「Pass the Hash」攻撃に対する脆弱性 |
| CSCvp57417 | ASAv のダウングレード時に、ファイアウォールがトレースバックしてリロードすることがある |
| CSCvp67033 | ASA：IPv6 の名前エイリアスを識別できず、「incomplete command」エラーメッセージが表示される |
| CSCvp69229 | OpenSSL 0 バイトレコードパディング Oracle の情報漏えいの脆弱性 |
| CSCvp71766 | VPN トンネルを介して BVI からソースを取得すると、RADIUS 認証に失敗する |
| CSCvp71879 | quota-CLI が設定されていない場合、ssh/telnet に対する limit-resource CLI は効果を持たない |
| CSCvp72624 | OID 1.3.6.1.2.1.4.35（ipNetToPhysicalTable）における SNMP 制限 |
| CSCvp73394 | フェールオーバー ASA IKEv2 VTI：セカンダリ ASA がスタンバイ IP をトラフィックセレクタとして送信する |
| CSCvp75965 | お客様が FMC で Syslog 設定を指定した後にプライマリ FPR2110 がクラッシュする |
| CSCvp76904 | dhcp-network-scope が正しく設定されていない場合、ASA の DHCP デバッグで間違ったゲートウェイとネットマスクが表示される |
| CSCvp77226 | マルチコンテキストモードで詳細化された sysopt トラフィックでの ASA のトレースバックとリロード |
| CSCvp78171 | クラスタ内の ASA がピアユニットとの IPv6 ND テーブルの同期に失敗する |
| CSCvp91905 | ASA が、新しく設定された IPv6 アドレスを現在のリンクローカルアドレスに追加する |
| CSCvp94478 | ASA scp がかなり遅い |
| CSCvp96658 | 新しいバージョンでの show loggingにおけるタイムゾーンの不一致 |
| CSCvq00560 | ASA が、ESP 認証データフィールドサイズ（ICV）に違反するパケットをサイレントドロップする |
| CSCvq15976 | ASA メモリリーク：snp_svc_insert_dtls_session |
| CSCvq17551 | Syslog 711004 のイベントマネージャイベントのトリガーに一貫性がない |

| 不具合 ID | タイトル |
|---|---|
| CSCvq22358 | あるコンテキストのアンチリプレイを無効にすると、他のコンテキストのアンチリプレイも無効になる |
| CSCvq27016 | FMC が FTD HA に対して「フェールオーバー履歴を取得できません..（Unable to fetch failover history..）」と表示する |
| CSCvq37913 | vpn-sessiondb がスタンバイ ASA に複製されない |
| CSCvq47743 | AnyConnect と管理セッションが数週間後に接続に失敗する |
| CSCvq49124 | http_exec_cli スレッドで FP1010 の ASA がトレースバックする |
| CSCvq49718 | FQDN エントリの解決中に DNS デバッグが有効になっている ASA でトレースバックが観察される |
| CSCvq50944 | OSPFv3 ネイバーシップが約 30 分ごとにフラッピングしている |
| CSCvq54620 | 「vpn-sessions logoff all」を使用した後に FPR4110 がクラッシュする |
| CSCvq54624 | キャッシュミスが原因で DTLS AnyConnect トンネルが再開しない |
| CSCvq55426 | IPv6 デフォルトルートを追加すると CLI が 50 秒間ハングする |
| CSCvq58729 | 2140：暗号化アクセラレータのステータスが、デフォルトでソフトウェアモードを表示する |
| CSCvq65864 | rest-api agent を有効にすると HTTP CLI Exec でトレースバックする |
| CSCvq70536 | FTD：HA を中断し、グレースフルリスタートが設定にある場合に展開が失敗する |
| CSCvq73595 | ユーザー名が 32 文字より長い場合に ASA WebVPN が証明書 UPN からユーザー名を抽出できない |
| CSCvq76706 | 「show logging」の出力でメッセージログ統計をクリアする機能 |
| CSCvq78126 | HA-IKEv2 のクリプトマップ設定で逆ルートを設定した後でも V ルートが見つからない |
| CSCvq79042 | サーバーからの 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 |
| CSCvq81410 | ASA：Safari ブラウザを使用して HTTP 経由で ASA コマンドを実行できない |
| CSCvq81692 | ASA：admin-context を変更した後、call-home が新しい admin コンテキストの設定を使用しない |

| 不具合 ID | タイトル |
|---|---|
| CSCvq83060 | SNMP：フェールオーバーリンクの情報をマルチモードの OID から取得できない |
| CSCvq84444 | 静的ルートを設定すると、スタンバイルート ASA で「ルートセッション」の rerr カウンタが増加する |
| CSCvq87625 | ENH：「show tech」出力への「show run all sysopt」の追加 |
| CSCvq92240 | AnyConnect ssl vpn テストの実行中にメモリリークが発生する |
| CSCvq93640 | CCM レイヤで WRL6 と WRL8 のコミット ID が更新される（Sprint 67） |
| CSCvq93836 | ENH：「show tech」出力への「show logging setting」の追加 |
| CSCvq98396 | ASA：暗号化セッションがスタンバイユニットでリークを処理する |
| CSCvq99107 | ASA で SFP のホットスワップが有効になっていない |
| CSCvr03705 | 次のハブが同じである場合に AD を持つと同時にトンネリングされたデフォルトルートが必要になる |
| CSCvr04203 | AnyConnect ssl vpn テストの実行中にメモリリークが発生する |
| CSCvr09399 | 動的フローオフロードを無効にできない |
| CSCvr12018 | ASA：デフォルトルートが BGP を介して学習されている場合は、VPN トラフィックがトンネルルートを取得できない |
| CSCvr15503 | ASA：SSH と ASDM セッションが CLOSE_WAIT でスタックし、ASA の MGMT が不足する |
| CSCvr20486 | FTD 1010 パッシブインターフェイスがユニキャストパケットを受信しない |
| CSCvr20757 | Cisco Umbrella DNS インスペクションの実行中に ASA でブロックリークが発生する |
| CSCvr20876 | メモリが少ないとカーネルが起動し（OOM）、デバイスがリロードされ、KP の rlimit が変更される |
| CSCvr23580 | 2 つ以上の IP アドレスプールを削除できない |
| 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 |
| CSCvr33428 | FMC が SYN フラッド攻撃から接続イベントを生成する |
| CSCvr35872 | スレッド名 DATAPATH での PBR が設定された ASA トレースバック |

| 不具合 ID | タイトル |
|---|---|
| CSCvr37486 | ASP テーブルで確立されているルールが、設定の削除時にアンインストールされない |
| CSCvr37502 | libexpat 不適切な解析によるサービス拒否の脆弱性 |
| CSCvr39516 | modexp-octeon での malloc 障害によって lina のセグメンテーション違反またはリロードが発生する |
| CSCvr50509 | 一部の 3DES 関連の設定がブート後に失われる |
| CSCvr50630 | ASA トレースバック：SCTP バルク同期と HA 同期 |
| CSCvr50718 | ASA：ICMP6 ルールの ICMP-TYPE オブジェクトの不適切な処理 |
| CSCvr51426 | ASA はアカウンティングパケットでマスクを送信していない |
| CSCvr55518 | ルールの作成に失敗したときにクリーンアップが行われない |
| CSCvr57605 | リロード後の ASA のライセンスコンテキスト数がプラットフォームの制限を超える |
| CSCvr58411 | 新しいスタティックスポークを追加または変更した場合、新しいスタティックハブ/スポーク設定の RRI がハブで動作しない |
| CSCvr60195 | マルチキャストコマンドを繰り返し追加および削除すると、ASA および FTD がトレースバックとリロードを行うことがある |
| CSCvr68146 | FTD クラスタを自動で再参加させることができない |
| CSCvr68872 | セカンダリユニットが、フェールオーバー リンク ダウン時のスプリットブレイン シナリオでプラットフォーム コンテキスト カウント制限を超過する |
| CSCvr72648 | ec_bits() での BIGNUM リーク |
| CSCvr80164 | CCM レイヤで WR6 と WR8 のコミット ID が更新される（スプリント 72） |
| CSCvr83372 | 書き込み中に I / O エラーが発生する（fd='28', error='Resource temporarily unavailable (11)'） |
| CSCvr86077 | re_multi_match_ascii によるデータパスでの ASA のトレースバック/ページフォルト |
| CSCvr90079 | show run all で HSTS 設定オプションが更新されない |
| CSCvr90462 | 一時的なアクティブ/アクティブの場合に ipv6 が無効にならないように、ipv6 重複アドレス検出を改善する |

| 不具合 ID | タイトル |
|---|---|
| CSCvr92311 | スタンバイ ASA ロギング %ASA-4-720022: (VPN-Secondary) Cannot find trust point __tmpCiscoM1Root__ |
| CSCvr98924 | ルーティングサブシステムによって引き起こされる ASA のトレースバックとリロード |
| CSCvr99642 | トレース「webvpn_periodic_signal」を使用した複数回の ASA トレースバックおよびリロード |
| CSCvs02954 | ASA OSPF：トポロジが変更されると RIB からプレフィックスが削除され、別の SPF が実行されると再び追加される |
| CSCvs04179 | ASA：ssh または fover_rx スレッドで 9.8.4.12 がトレースバックし、リロードする |
| CSCvs05262 | デクリメント TTL で間違った結果が表示される |
| CSCvs13204 | SR-IOV インターフェイス上の ASAv フェールオーバー トラフィックが、インターフェイスのダウンによりドロップされることがある |
| CSCvs16073 | ホストとホストグループが設定された SNMP ポーリングが失敗する |
| CSCvs27264 | ASA の mroute エントリが更新されない |
| CSCvs28213 | アサーション slib_malloc.c を使用したスレッド名 SSH での ASA トレースバック |
| CSCvs29779 | 「DATAPATH-12-1899」プロセスの完了を待っているときに ASA がトレースバックし、リロードすることがある |
| CSCvs31159 | CSCOGet_location ラッパー内の空のロケーション処理が正しくない |
| CSCvs31443 | ASA が「%ASA-5-321001: Resource 'memory' limit'」メッセージで負のメモリ値を報告する |
| CSCvs31470 | OSPF Hello により 9K ブロックが枯渇し、制御ポイントの CPU が 100% になり、クラスタが不安定になる |
| CSCvs32907 | STRAP 実装のデバッグカウンタが追加されました。 |
| CSCvs33102 | ASA/FTD がスレッド名「EIGRP-IPv4」でトレースバックし、リロードすることがある |
| CSCvs33852 | バージョン 9.6.4.34 へのアップグレード後、アクセスグループを追加できない |
| CSCvs38785 | syslog のタイムスタンプ形式が一貫していない |

| 不具合 ID | タイトル |
|---|---|
| CSCvs39589 | データチャネルがネゴシエートされていない場合は ASA が SSH タイムアウトを実行しない |
| CSCvs40230 | ICMP が機能せず、「inspect-icmp-seq-num-not-matched」によって失敗する |
| CSCvs43154 | アグレッシブ警告メッセージのためにセカンダリ ASA がフェールオーバーに参加できない |
| CSCvs45111 | CCM レイヤ（スプリント 75）での WR6 および WR8 コミット ID の更新 |
| CSCvs45548 | 再アクティブ化モードが時間切れになることで、障害が発生したサーバーが不適切なタイミングで再アクティブ化される |
| CSCvs47283 | object-group-search が有効になっていると、トラフィックがアクセスリストと誤って一致することがある |
| CSCvs48437 | ASA が同時に 2 つの UDP ポートに syslog を送信できない |
| CSCvs52108 | Umbrella インスペクションによる ASA トレースバック |
| CSCvs52169 | AnyConnect からのデバイス ID が長すぎると、ASA が不正な形式の RADIUS メッセージを送信する |
| CSCvs55603 | ACL で一致した場合に ICMP 応答がドロップされた |
| CSCvs56802 | Cisco Firepower 2100 シリーズの SSL/TLS 検証におけるサービス拒否攻撃に対する脆弱性 |
| CSCvs59487 | 99.14.1.64 イメージへのアップグレード中に KP デバイスでクラッシュが確認された |
| CSCvs59558 | プライマリのアクティブユニットのリロード時にフェールオーバー MAC アドレスが削除される |
| CSCvs59966 | OID「cipSecGlobalActiveTunnels」について間違った値がレポートされる（ASDM と同様） |
| CSCvs60254 | libxml2 xmlParseBalancedChunkMemoryRecover メモリリークの脆弱性 |
| CSCvs63484 | SAML トークンがハッシュテーブルから削除されない |
| CSCvs70260 | IKEv2 vpn-filter がボリュームベースのキー再生成コリジョン後に暗黙的な拒否によりトラフィックをドロップする |
| CSCvs71698 | 管理デフォルトルートがデフォルト データ ルーティングと競合する |
| CSCvs71969 | 複数のシスコ製品での Snort HTTP 検出エンジンのファイルポリシーバイパスの脆弱性 |

| 不具合 ID | タイトル |
|---|---|
| CSCvs72378 | 異なるコンテキスト間で切り替えると、ASDM セッションが突然終了する |
| CSCvs72450 | FXOS：サービスモジュールの hwclock を同時書き込みコリジョンによる破損から修復 |
| CSCvs73663 | IPsec message handler スレッドでの ASA のトレースバック |
| CSCvs73754 | ASA/FTD：BVI の ARP が物理インターフェイスに割り当てられていないために発生するブロック 256 サイズの枯渇 |
| CSCvs76605 | FXOS 2.6(1.174) にリストされているモジュールのバージョンが間違っている |
| CSCvs77818 | トレースバック：spin_lock_fair_mode_enqueue：ロック（np_conn_shrlock_t）が長期間にわたって保持されている |
| CSCvs82726 | マルチコンテキストモードで CSCvs31470 に対処するためのプレースホルダ |
| CSCvs84542 | スレッド idfw_proc での ASA のトレースバック |
| CSCvs85196 | ASA SIP 接続が連続した複数回のフェールオーバー後にドロップする：ピンホールタイムアウト/インスペクションによるクローズ |
| CSCvs87795 | ASA：バックアップコンテキストが失敗し「ERROR: No such file or directory」と表示される |
| CSCvs88413 | バージョン 9.8 へのアップグレードにポートチャネルのバンドルに失敗する |
| CSCvs90100 | ASA/FTD がスレッド名「License Thread」でトレースバックおよびリロードすることがある |
| CSCvs94486 | CSCvs59487 を解決するには追加の修正が必要 |
| CSCvs97863 | フラッシュファイルシステムでのクローズ時の fsync コールの数を減らす |
| CSCvs97908 | 無効な scp セッションが他のアクティブな http と scp のセッションを終了させる |
| CSCvt00255 | カーネルを cpe:2.3:o:linux:linux_kernel:4.14.187: にアップグレード |
| CSCvt01282 | CCM レイヤ（スプリント 79）での WR6 および WR8 コミット ID の更新 |
| CSCvt05862 | サーバーが管理インターフェイスを介して到達可能な場合、IPv6 DNS サーバーの解決が失敗する |
| CSCvt06606 | フローオフロードが FTD 6.2(3.10) と FXOS 2.6(1.169) の組み合わせで機能しない |

| 不具合 ID | タイトル |
|---|---|
| CSCvt06841 | ASA でのキャプチャを使用して設定すると、誤ったアクセスリストのヒットカウントが表示される |
| CSCvt08492 | FXOS のアップグレード後に FDM でイベントが生成されない |
| CSCvt11302 | FIPS デバイスで FIPS が有効になっている場合、Webtype ACL を作成できない |
| CSCvt11547 | Cisco Firepower Device Manager ソフトウェアにおけるファイルシステム容量の枯渇によるサービス拒否の脆弱性 |
| CSCvt11661 | DOC：show asp dropでの mp-svc-flow-control の意味を明確にする |
| CSCvt11742 | ASA/FTD がスレッド名「ssh」でトレースバックし、リロードすることがある |
| CSCvt12463 | ASA：Unicorn Admin Handler スレッドでのトレースバック |
| CSCvt13301 | 非標準ポートを使用したデフォルトの Syslog が侵入イベントに対して機能しない |
| CSCvt13822 | ASA：一致する暗号マップエントリがないため、VTI が IPSec トンネルを拒否する |
| CSCvt15056 | ASDM によって管理される SFR：システムポリシーが適用されない |
| CSCvt17912 | lina_free_exec_st で segfault/reload を引き起こすプラットフォームの制限をプッシュするストレス |
| CSCvt18199 | スタンドアロン ASA の「overlaps with inside standby interface address」エラーで IPv6 NAT が拒否される |
| CSCvt22356 | ASA のリブート後、ASA クラスタの Health-check monitor-interface debounce-time が 9000ms にリセットされる |
| CSCvt23643 | データを復旧するための、VPN フェールオーバーリカバリに約 30 秒かかる |
| CSCvt25225 | ASA：OSPF 同期中の設定同期状態時のアクティブユニットの HA トレースバックとリロード |
| CSCvt26031 | ASAv が IPv6 を使用してスマートライセンスを登録できない |
| CSCvt26530 | 「Snort の障害により他のユニットのインスペクションエンジンに障害が発生しました（Inspection engine in other unit has failed due to snort failure）」が原因で FTD がフェールオーバーした |

| 不具合 ID | タイトル |
|---|---|
| CSCvt27585 | スタンバイからのフェールオーバー切り替え実行中に 2100 でのトレースバックが発生する。 |
| CSCvt30731 | CCM レイヤ（スプリント 80）での WR6、WR8 および LTS18 コミット ID の更新 |
| CSCvt35945 | 9.8 トレインで SSH バージョン2を有効にする場合に Encryption-3DES-AES が必要であってはならない |
| CSCvt36542 | FPR 上のマルチコンテキスト ASA/LINA が DHCP リリースメッセージを送信しない |
| CSCvt38279 | ISA3000 で disk0 を消去すると、ファイルシステムがサポートされなくなる |
| CSCvt39977 | PSNG_TCP_PORTSCAN [122:1:1] ルールアラートの場合の無効なパケットデータ |
| CSCvt41357 | syslog ホストにアクセスできない場合、「no logging permit-hostdown」コマンドで接続がブロックされない |
| CSCvt43136 | 複数のシスコ製品 Snort TCP 高速オープン ファイル ポリシー バイパスの脆弱性 |
| CSCvt43967 | ゼロを含む長さが 46 バイト以下のパディングパケットを RA トンネルから受信した |
| CSCvt46289 | Firepower 1000 シリーズで ASA LDAPS 接続が失敗する |
| CSCvt48601 | Cisco Firepower Management Center ソフトウェアに蓄積されたクロスサイトスクリプティングの脆弱性 |
| CSCvt50528 | ASA/FTD - CLI での証明書のインストールに関するデフォルト設定の警告メッセージ |
| CSCvt51349 | フラグメント所有者に転送されたフラグメント化されたパケットが、データ インターフェイス キャプチャで表示されない |
| CSCvt51987 | ASA FPR9300 SM56 での 80 サイズのブロックの枯渇によりトラフィックが停止する |
| CSCvt53640 | SFR を 6.4.0 から 6.4.0.x にアップグレードした後に ASA5585 がトレースバックおよびリロードする場合がある |
| CSCvt54182 | FTD が SSL 複合を実行するように設定されている場合に LINA コアが生成される |

| 不具合 ID | タイトル |
|---|---|
| CSCvt63027 | Cisco Firepower Management Center における XML エンティティ拡張の脆弱性 |
| CSCvt63484 | igb_saleen_io_sfp_mod_poll_thre プロセスにより ASA の CPU 使用率が高くなる |
| CSCvt64035 | remote acess mib：ラップアラウンド前に SNMP 64ビットのみが 4Gb を報告する |
| CSCvt64952 | 「Show crypto accelerator load-balance detail」が欠落しており、出力が未定義 |
| CSCvt65982 | RRI ルートの削除時にスレーブユニットでルートフォールバックが発生しない |
| CSCvt68294 | Firepower 4120 の最大 VPN セッション制限を 20,000 に調整する |
| CSCvt70664 | ASA：AnyConnect の Radius Acct-Requests に acct-session-time アカウンティング属性がない |
| CSCvt71529 | SSL ハンドシェイク中の ASA のトレースバックとリロード |
| CSCvt72683 | FP 8130 での NAT ポリシーの展開後の NAT ポリシーの設定が表示されない |
| CSCvt73407 | ASA デバイスの ユーザー名 enable_15 に対する TACACS フォールバック認証が失敗する |
| CSCvt75760 | HTTP クリーンアップによるクライアントレス WebVPN のトレースバックまたはページ障害 |
| CSCvt80126 | CLI の「show asp table socket 18421590 det」で ASA がトレースバックし、リロードする |
| CSCvt80134 | WebVPN リライタが SAP Netweaver からのデータを解析できない。 |
| CSCvt80172 | CVE-2017-11610 に対処するには、スーパーバイザソフトウェアをアップグレードする必要がある |
| CSCvt83133 | group-url を使用して Google Chrome から anyconnect webvpn ポータルにアクセスできない |
| CSCvt90330 | スレッド名 coa_task での ASA トレースバックおよびリロード |
| CSCvt91521 | 暗号化アクセラレータバイアス設定を show tech に含める必要がある |
| CSCvt92647 | ASA のアップグレード後に、IPv6 アドレスで設定されたステートリンクを介した接続が失われる |

| 不具合 ID | タイトル |
|---|---|
| CSCvt98599 | IKEv2 コールアドミッション統計情報の「Active SAs」カウンタが実際のセッション数と同期していない |
| CSCvt99020 | Cisco Firepower Management Center ソフトウェアに蓄積されたクロスサイトスクリプティングの脆弱性 |
| CSCvt99137 | クラスタに大量の FTP トラフィックがあると、SEC_FLOW メッセージが再送信ループ状態になる |
| CSCvu00112 | ssh クォータ制限が ci_cons_shell でヒットしたときに tsd0 がリセットされない |
| CSCvu03107 | AnyConnect 統計情報が %ASA-4-113019 と RADIUS アカウンティングの両方で二重になる |
| CSCvu03562 | ユーザー名とパスワードを入力すると、デバイスの SSH 接続が失われる |
| CSCvu03675 | FPR2100：メモリ不足の状態で ASA コンソールがハングして応答しなくなることがある |
| CSCvu05180 | リモートアクセス VPN ポリシーの展開後、FTD で AAA サーバー設定が欠落している |
| CSCvu06767 | マルチインスタンス上の Lina コアにより両方の論理デバイスでブートループが発生する |
| CSCvu07602 | FPR-41x5：「clear crypto accelerator load-balance」によりトレースバックおよびリロードが発生する |
| CSCvu07880 | QP プラットフォーム上の ASA で誤ったコアダンプファイルシステム領域（50 GB）が表示される |
| CSCvu12039 | 起動後にクラスタデータユニットが制御ユニットからの SCTP 設定の同期に失敗することがある |
| CSCvu12045 | 「System (/etc/rc.d/init.d/netif-speed eth0) Failed」というエラーで NGIPS の展開が失敗する |
| CSCvu12248 | ユーザーが AnyConnect VPN を使用して接続する場合の ASA-FPWR 1010 トレースバックおよびリロード |
| CSCvu16423 | ASA 9.12(2)：ユニコーンプロキシスレッドによる複数のトレースバック |
| CSCvu17924 | DATAPATH での FTD フェールオーバーユニットのトレースバックおよびリロード |
| CSCvu17965 | 手動 NAT ルールのポート値を変更すると、ASA でトレースバックが生成され、リロードされる |

| 不具合 ID | タイトル |
|---|---|
| CSCvu20007 | LINA からの Config_XML_Response の形式が正しくない。Lina が使用可能なメモリがないと報告している。 |
| CSCvu20666 | 一部の FPR 2100 シリーズの外部認証 RADIUS が設定を行わない |
| CSCvu26296 | ASA インターフェイス ACL が ASA からの snmp コントロールプレーン トラフィックをドロップしている |
| CSCvu26561 | Kerberos と統合すると、WebVPN SSO が予期しない結果になる |
| CSCvu29184 | Cisco Firepower Threat Defense ソフトウェアにおけるコマンドファイルの上書きの脆弱性 |
| CSCvu29395 | アクティブな IGMP join でマスターロールの変更を実行中にトレースバックが発生した |
| CSCvu29660 | 使用可能なブロックがゼロになっても、ブロック枯渇スナップショットが作成されない |
| CSCvu32698 | 「key config-key password-encryption」が存在する場合、クラスタに参加する際に ASA が SNMP でクラッシュする |
| CSCvu33992 | トレースバック：ASA が lina_sigcrash+1394 をリロードした |
| CSCvu34413 | リロード後に ASA で SSH キーが失われる |
| CSCvu40213 | スレッド名 kerberos_recv での ASA トレースバック |
| CSCvu40324 | フロールックアップ呼び出しトレースバックによる ASA トレースバックおよびリロード |
| CSCvu40398 | FIPS を有効にした後の FIPS SELF-TEST FAILURE による ASAv のリロード |
| CSCvu43924 | DHCP 検出パケットの GIADDR が dhcp-network-scope の IP アドレスに変更される |
| CSCvu45748 | スレッド名「ppp_timer_thread」での ASA トレースバック |
| CSCvu45822 | ASA でトレースバックが発生し、リロードされた |
| CSCvu48886 | デフォルト以外の「crypto ikev2 limit max-in-negotiation-sa」を削除すると FTD の展開が失敗する |
| CSCvu49625 | [PKI] 標準ベースの IKEv2 証明書認証セッションが 2 番目の userfromcert ルックアップを不必要に実行する |
| CSCvu55469 | FTD：接続アイドルタイムアウトがリセットされない |

| 不具合 ID | タイトル |
|---|---|
| CSCvu55843 | TACACS 承認ユーザーによる設定変更後の ASA トレースバック |
| CSCvu61704 | ASA の intel_82576_check_link_thread を使用した高い CPU 使用率がユニット全体のパフォーマンスに影響する |
| CSCvu65688 | CSCvt98599 にもかかわらず、IKEv2 CAC の「Active SAs」カウンタが実際のセッション数と同期していない |
| CSCvu68529 | Embryonic 接続制限が一貫して機能しない |
| CSCvu70931 | 「no key config-key」を入力した後でクラスタ/AAA サーバーキーが欠如する |
| CSCvu72094 | スレッド名 DATAPATH での ASA トレースバックおよびリロード |
| CSCvu73207 | AnyConnect ユーザーへの DTLS パケットで保持されない DSCP 値 |
| CSCvu77095 | ASA がリマーク付きの ACE を削除できず、「指定されたリマークが存在しません」というエラーが表示される |
| CSCvu78721 | アップグレード後にインターフェイス速度を変更（修正）できない |
| CSCvu89110 | ASA：「logging permit-hostdown」が設定され、TCP syslog がダウンしている場合も新しい接続をブロックする |
| CSCvu90727 | EAP-TLS 認証を使用するネイティブ VPN クライアントが ASA に接続できない |
| CSCvu91097 | Cisco Firepower Management Center ソフトウェアにおけるポリシーの脆弱性 |
| CSCvu91792 | Internal-Data 0/0 および 0/1 の SNMP IfInDiscards OID が間違った値を返す |
| CSCvu98222 | SSL 復号ポリシーを有効にした後、FTD Lina エンジンがデータパスでトレースバックすることがある |
| CSCvv04584 | resson no-mcast-intrf でマルチキャストトラフィックがドロップされている |
| CSCvv07721 | FirePOWER：Firepower 7000 および Firepower 8000 シリーズで [System] > [User] > [User Roles] のページが空白になる |
| CSCvv07864 | マルチキャスト EIGRP トラフィックが内部 FTD インターフェイスで表示されない |
| CSCvv08244 | Firepower モジュールによって「復号しない」SSL 復号ルールに一致する信頼できる HTTPS 接続がブロックされることがある |
| CSCvv08684 | クラスタサイト固有の MAC アドレスが、フローオフロードによって書き換えられない |

| 不具合 ID | タイトル |
|---|---|
| CSCvv09396 | セッション終了後に、L2TP の VPN ルートが陳腐化する |
| CSCvv10778 | 9.12.4 へのアップグレード後のスレッド名 DATAPATH（5585）または Lina（2100）のトレースバック |
| CSCvv12127 | 多数の IPV4 ソースおよび接続先 AC ルールを追加すると、シリーズ 3 でのポリシーの展開が失敗する場合がある。 |
| CSCvv12857 | 暗号化エンジンの障害後に ASA がフリーズする |
| CSCvv15572 | 新しいコンテキストの作成中に「config-url」を入力すると、ASA のトレースバックが発生する |
| CSCvv16082 | stress/low memory: assert: mh->mh_mem_pool > MEMPOOL_UNDEFINED && mh->mh_mem_pool < MEMPOOL_MAX_TYPE |
| CSCvv19230 | ASAv AnyConnect ユーザがアイドルタイムアウトで予期せず切断される |
| CSCvv20450 | FMC 6.4 から 6.7 へのアップグレードが失敗する「Error running script 500_rpms/110_generate_dbaccess.sh」 |
| CSCvv23370 | webVPN、SNMP 関連トラフィックの実行中に FPR2130 でトレースバックが発生した。 |
| CSCvv25394 | アップグレード後、ASA がディスクの名前を交換して disk0 が disk1になり、disk1 が disk0 になった |
| CSCvv25839 | SSl 復号が有効な場合、reCAPTCHA が機能しない |
| CSCvv28997 | スレッド名 Crypto CA での ASA トレースバックおよびリロード |
| CSCvv29687 | ASA でのデフォルトの syslog 780001/780002 のレート制限 |
| CSCvv30172 | リブート後に ADI が断続的に KCD に参加できなくなる |
| CSCvv31334 | 6.6.1 ー 63 の KP HA でピアを切り替えようとすると、Lina のトレースバックとリロードが発生する |
| CSCvv31629 | トラフィックが非対称的に通過すると、断続的に埋め込まれた GRE 経由の ping 応答が FTD クラスタでドロップする。 |
| CSCvv32333 | ASA は現在もマルチモードでの SNMP を介した internal-data0/0 カウンタのポーリングを許可しない |
| CSCvv32425 | show asp table classify domain permit を実行した場合の ASA トレースバック |
| CSCvv34003 | ISA 3000 で OID 1.3.6.1.2.1.47.1.1.1.1.5 の snmpwalk が、.16 および .17 に対して値 0 を返す |

| 不具合 ID | タイトル |
|---|---|
| CSCvv34140 | ASA IKEv2 VTI：レスポンダとして CTM から SPI を要求できない |
| CSCvv36518 | ASA：CSCuw51499 修正後のリロード後のダウンタイムが延長される |
| CSCvv36725 | ASA logging rate-limit 1 5 message ... 5 秒ではなく 10 秒内に 1 メッセージに制限 |
| CSCvv37629 | 不正な SIP パケットにより SIP 接続タイムアウトまで 4k ブロックのホールドアップが発生し、トラフィックの問題を引き起こす可能性がある |
| CSCvv40223 | user-db を変更または読み取る際、flash:/LOCAL-CA-SERVER/LOCAL-CA-SERVER.cdb の解析中にエラーが発生する |
| CSCvv41453 | 管理専用ルートテーブルからスタティック IPv6 ルートを削除すると、データトラフィックに影響する |
| CSCvv43484 | システムアップグレード後に ASA が RIP パケットの処理を停止する |
| CSCvv44270 | ASAv5 がトレースバックなしでリロードする。 |
| CSCvv48942 | Snmpwalk がフェールオーバーインターフェイスのトラフィックカウンターを 0 として表示する |
| CSCvv49698 | ASA Anyconnect url-redirect が IPv6 で機能しない |
| CSCvv49800 | ASA/FTD：HA スイッチオーバーが Firepower シャーシのグレースフル再起動で発生しない |
| CSCvv50338 | snpi_nat_xlate_destroy+2508 でのトレースバック クラスタ ユニット |
| CSCvv53696 | Anyconnect ユーザーの AAA または CoA タスク中の ASA/FTD トレースバックおよびリロード |
| CSCvv56644 | Cisco 適応型セキュリティアプライアンスと Firepower Threat Defense ソフトウェアの Web DoS の脆弱性 |
| CSCvv57590 | ASA：スタンバイでの ACL のコンパイルに時間がかかる |
| CSCvv57842 | WebSSL クライアントレス ユーザー アカウントが最初の不正なパスワードでロックアウトされている |
| CSCvv58332 | ASA/FTD が BGP MP_REACH_NLRI 属性のネクストホップバイトを逆順で読み取る |
| CSCvv58605 | スレッドでの ASA トレースバックおよびリロード：暗号化 CA、MTX 内の非仮想化 pki グローバルテーブルによるメモリ破損 |
| CSCvv59036 | ユーザーが削除していないのに、FMC から静的ルートが削除される。 |

| 不具合 ID | タイトル |
|---|---|
| CSCvv59676 | Snort2：TLS の証明書キャッシュのアグレッシブプルーニングを実装してメモリを解放する |
| CSCvv62305 | フェールオーバーペアに参加しようとした場合の fover_parse での ASA トレースバックとリロード |
| CSCvv63412 | tmatch のコンパイルが進行中のとき、ASA がすべてのトラフィックを理由「No route to host」でドロップする |
| CSCvv65184 | Cisco 適応型セキュリティアプライアンスと Firepower Threat Defense ソフトウェアの Web DoS の脆弱性 |
| CSCvv66005 | inspect esmtp での ASA のトレースバックとリロード |
| CSCvv66920 | 内部フロー：U ターン GRE フローが不正な接続フローの作成をトリガーする |
| CSCvw41728 | DATAPATH での ASA 9.12 のランダムトレースバックおよびリロード |
| CSCvv70984 | ブックマーク SSL 暗号設定の変更中の ASA トレースバック |
| CSCvv72466 | ASA のアップグレード後、startup-config で OSPF ネットワークコマンドが欠落する |
| CSCvv73017 | fover および SSH スレッドによるトレースバック |
| CSCvv79897 | Lina のクラッシュとシステムの再起動イベントの発生を防ぐために、FTD ユニットの「sensor restart」コマンドをブロックする |
| CSCvv86926 | コアファイルを作成する FTD での予期しないトレースバックとリロード |
| CSCvv87232 | ASA：igb_saleen_io_sfp_mod_poll_thread プロセスで CPU 専有の値が高くなる |
| CSCvv87496 | 「VPN packet redirect on peer」による ASA クラスタメンバー 2048 ブロックの枯渇 |
| CSCvv88017 | ASA：EasyVPN HW クライアントが重複したフェーズ 2 のキー再生成をトリガーし、トンネル経由で切断される |
| CSCvv90181 | 展開中に「show running-config」が実行されている場合、トランスクリプトに展開失敗の理由が表示されない |
| CSCvv90720 | ASA/FTD：HA スイッチオーバー後に接続されたスイッチで MAC アドレステーブルのフラッピングが表示される |
| CSCvv94701 | ASA が「octnic_hm_thread」でリロードし続け、リロード後は回復するまでに非常に長い時間がかかる |

| 不具合 ID | タイトル |
|---|---|
| CSCvv97877 | セカンダリユニットがクラスタに参加できない |
| CSCvw01028 | 6.4.0 より前のリリースから 6.4.0. [9、10、11] にアップグレードすると、7K および 8K デバイスが応答しなくなる |
| CSCvw05393 | OCSP 失効チェックで証明書の検証の syslog が生成されない |
| CSCvw06195 | ASA トレースバック cp_midpath_process_thread |
| CSCvw07000 | PDTS Tx キューがスタックしたまま Snort がビジー状態でドロップする |
| CSCvw12008 | 「show tech-support」コマンドの実行中の ASA トレースバックとリロード |
| CSCvw12100 | サイト間セッションおよび AnyConnect セッションで ASA の古い VPN コンテキストが表示される |
| CSCvw19272 | 複数のシスコ製品での Snort HTTP 検出エンジンのファイルポリシーバイパスの脆弱性 |
| CSCvw21844 | カプセル化されたフローを処理する際の DATAPATH スレッドでの FTD トレースバックとリロード |
| CSCvw22881 | radius_rcv_auth により、コントロールプレーンの CPU 使用率が 100% になることがある |
| CSCvw22986 | プライマリユニットのインターフェイスが init 状態のままであるため、セカンダリユニットがバルク同期状態で無限にスタックする |
| CSCvw23199 | スレッド名 Logger での ASA/FTD のトレースバックとリロード |
| CSCvw24164 | ハートビートの誤検知 |
| CSCvw24556 | フローオフロードが有効になっている場合、TCP ファイル転送（ビッグファイル）が正しく閉じない |
| CSCvw24700 | 9.12.4.7 を実行している FPR2100 ASA がエラー（FIPS Self-Test failure, fipsPostGFSboxKat）で起動に失敗する |
| CSCvw26171 | strncpy NULL 文字列が SSL ライブラリから渡されている間の ASA syslog トレースバック |
| CSCvw26331 | スレッド名 ci/console での ASA のトレースバックとリロード |
| CSCvw26544 | Cisco ASA および FTD ソフトウェアの SIP で確認されたサービス拒否攻撃に対する脆弱性 |
| CSCvw27301 | EAP を使用した IKEv2 で、MOBIKE ステータスが処理されない |

| 不具合 ID | タイトル |
|---|---|
| CSCvw28894 | vuln テーブルのエントリが重複しているため、SFDataCorrerator の起動が遅くなり、vuln の再マッピングが発生する |
| CSCvw31254 | 8350 センサーでシェルが /bin/false に設定されているユーザーが原因で展開が失敗する |
| CSCvw31569 | ディレクタ/バックアップフローは残され、このフローに関連するトラフィックがブラックホール化される |
| CSCvw32518 | 9.12(4)4 以降にアップグレード後の ASASM トレースバックおよびリロード |
| CSCvw33987 | アップグレード後の ASAv/2100 におけるスマートライセンス障害 |
| CSCvw36662 | TACACS+ ASCII パスワード変更要求が正しく処理されない |
| CSCvw37259 | デバイスがハング状態になるまで 600/秒のレートで VPN syslog が生成される |
| CSCvw41728 | FTD で CLI を使用して syslog を設定できない |
| CSCvw42999 | FPR2110 上の 9.10.1.11 ASA がランダムにトレースバックおよびリロードする |
| CSCvw43486 | PBR 設定変更時の ASA/FTD トレースバックとリロード |
| CSCvw43534 | Mozilla Network S に Null ポインタの逆参照の脆弱性が存在する... |
| CSCvw43543 | zlib 1.2.8 の inflate.c の inflateMark 関数は、継続を許可する場合がある... |
| CSCvw43586 | 3.5.8 から 3.6.7 のバージョンの gnutls に脆弱性が見つかった... |
| CSCvw43615 | 3.6.15 以前の GnuTLS で問題が発見された。サーバーはトリガーできる... |
| CSCvw44122 | ASA：非 DNS トラフィックを DNS 検査エンジンにリダイレクトする「class-default」クラスマップ |
| CSCvw46702 | アプリケーション設定の同期のタイムアウトが原因で FTD クラスタのセカンダリユニットがクラスタに参加できない |
| CSCvw47321 | 一部の FPR プラットフォームのインバウンドトラフィックの IPSec トランスポート モード トラフィックの破損 |
| CSCvw48517 | ASA を 9.13(1)13 にアップグレードすると、DAP が動作しなくなる |
| CSCvw49531 | VDB のアップグレード後にアプリケーションが誤って分類される |
| CSCvw51462 | IPv4 デフォルトトンネルルートが拒否される |

| 不具合 ID | タイトル |
|---|---|
| CSCvw51950 | FPR 4K：手動フェールオーバー後に新しいアクティブ ASA から SSL トラストポイントが削除される |
| CSCvw51985 | ASA：IPv6 DACL 障害により、AnyConnect セッションを再開できない |
| CSCvw52098 | 6.4.0.11 へのアップグレードが、スタンバイ 2120 の 800_post/901_reapply_sensor_policy.pl で失敗する |
| CSCvw52609 | Cisco ASA と FTD ソフトウェアの Web サービスバッファオーバーフローによるサービス拒否の脆弱性 |
| CSCvw53255 | FTD/ASA HA：トレースバックによるフェールオーバー後でも、スタンバイユニット FXOS がトラフィックを転送できる |
| CSCvw53427 | ASA が複数のクエリパラメータを含む SAML アサーションで HTTP POST を処理できない |
| CSCvw53796 | Cisco ASA および FTD Web サービスインターフェイスで確認されたクロスサイト スクリプティングの脆弱性 |
| CSCvw53884 | ASA5506 上の M500IT モデルのソリッドステートドライブが 3 年 2 ヵ月のサービス期間後に応答しなくなることがある |
| CSCvw54640 | FPR-4150：スレッド名 DATAPATH での ASA トレースバックおよびリロード |
| CSCvw54802 | サーバーが利用できないために ocsp チェックが失敗した後、失効チェックが none に移動しない |
| CSCvw58414 | タイプ dynamic-split-exclude-domains の AnyConnect カスタム属性の名前がリロード後に変更される |
| CSCvw58865 | sftunnel TLS ハンドシェイクに NewSessionTicket が含まれてしまう |
| CSCvw59035 | FTD BVI アドレスから直接接続された IP への接続の問題 |
| CSCvw60177 | スタンバイまたはセカンダリのクラスタユニットがスレッド名 fover_parse および「cluster config sync」でクラッシュすることがある |
| CSCvw62526 | エンジニアリング ASA Build での ASAトレースバックとリロード：9.12.3.237 |
| CSCvw62820 | Memcached 1.5.6 以降の更新 |
| CSCvw63862 | ASA：ランダムな L2TP ユーザが古い ACL フィルタエントリが原因でリソースにアクセスできない |
| CSCvw71766 | IKev 2 Daemon スレッドでの ASA トレースバックおよびリロード |

| 不具合 ID | タイトル |
|---|---|
| CSCvw74495 | ログインに失敗すると、FTP サービスのアプリケーション検出が失敗する。 |
| CSCvw74940 | IKE デーモンでの ASA トレースバックおよびリロード |
| CSCvw79208 | 入力文字列の後半に「http://」サブストリングがある場合、URL の正規化が正しく行われない |
| CSCvw79294 | sftunnel が大量のログをメッセージファイルに記録する |
| CSCvw81322 | マルチインスタンスモードを実行している FTD が、SRU のインストールと展開後に snort GID 3 ルールを無効にする |
| CSCvw81897 | ASA：OpenSSL の脆弱性 CVE-2020-1971 |
| CSCvw82629 | ACL に関する「設定セッション」の変更時に ASA トレースバックが発生する。 |
| CSCvw83572 | バージョン 9.14.1.30 以降で BVI HTTP/SSH アクセスが機能しない |
| CSCvw84339 | ホスト名が 30 文字を超えると、FTD の管理対象デバイスのバックアップが失敗する |
| CSCvw85377 | アクセスポリシーの URL フィルタリングルールで URL が更新されていない |
| CSCvw87788 | ASA トレースバックとリロードの WebVPN スレッド |
| CSCvw89365 | 証明書の変更中に ASA/FTD がトレースバックおよびリロードすることがある。 |
| CSCvw93272 | Cisco Firepower Management Center ソフトウェアのクロスサイト スクリプティングに対する脆弱性 |
| CSCvw93282 | Cisco Firepower Management Center ソフトウェアのクロスサイト スクリプティングに対する脆弱性 |
| CSCvw93513 | Cisco Firepower Management Center ソフトウェアのクロスサイト スクリプティングに対する脆弱性 |
| CSCvw95301 | キャプチャが削除されたときに ASA がトレースバックを実行し、スレッド名：ssh でリロードされる |
| CSCvw96295 | FMC 6.4.0.10 の静的ルートにルートトラッキングを追加できない |
| CSCvw96488 | inspect_h323_ras+1810 のトレースバック |
| CSCvw97821 | ASA：CoA で dACL が提供されない場合、VPN トラフィックが渡されない |

| 不具合 ID | タイトル |
|---|---|
| CSCvw98840 | ASA：CoA 後の v6 トラフィックに IPv6 エントリのない dACL が適用されない |
| CSCvx01381 | 手動時刻設定用の FMC GUI の [Year] ドロップダウンリストに 2020年 までしか表示されない |
| CSCvx02869 | スレッド名のトレースバック：Lic TMR |
| CSCvx03764 | アイデンティティ NAT トラフィックおよびクラスタリング環境では、オフロード書き換えデータを修正する必要がある |
| CSCvx04057 | SGT 名が未解決のまま ACE で使用されている場合、回線が無視または非アクティブ状態にならない |
| CSCvx04643 | ASA のリロードで「content-security-policy」設定が削除される |
| CSCvx05381 | Cisco ASA および FTD ソフトウェアのコマンドインジェクションの脆弱性 |
| CSCvx05956 | navl 属性のコピー中に snort CPU 使用率が高くなる |
| CSCvx08734 | ASA：デフォルトの IPv6/IPv4 ルートトンネリングが機能しない |
| CSCvx11295 | スレッド Crypto CA で ASA がトレースバックおよびリロードする |
| CSCvx11460 | リモートエンドで TFC が有効になっている状態で Firepower 2110 がトラフィックをサイレントにドロップする |
| CSCvx13694 | スレッド名 PTHREAD-4432 で ASA/FTD トレースバックする |
| CSCvx15040 | ASA/FTD で DHCP プロキシオファーがドロップされる |
| CSCvx16202 | FMC からプッシュされた自己参照オブジェクトにより、エラーで lina がクラッシュする（GRP 階層でループする） |
| CSCvx17664 | ASA がスレッド名「webvpn_task」でトレースバックおよびリロードすることがある |
| CSCvx17785 | ACL を追加または削除し、route-map コマンドに入力すると、クラッシュが絶えず発生する |
| CSCvx20352 | アップグレード中または大量のトラフィックの負荷が発生すると、Snort PDTS バッファが破損する |
| CSCvx26286 | IPV6 アドレスが両方のユニットで重複としてマークされ、フェールオーバー後に ipv6 トラフィックが停止した。 |
| CSCvx26808 | FPR2100 シリーズのプロセス lina での FTD のトレースバックおよびリロード |

| 不具合 ID | タイトル |
|---|---|
| CSCvx27430 | ASA：FIPS が有効な場合、PAC ファイルをインポートできない。 |
| CSCvx29771 | フローオフロードによる一括ルーティング更新後にファイアウォールCPUが増加することがある |
| CSCvx30314 | SSL midpath での ASA 9.15.1.7 トレースバックおよびリロード |
| CSCvx41171 | ACL 設定を同時に変更すると、「show running-config」の出力が完全に中断される |
| CSCvx42197 | ASA EIGRP ルートがネイバーの切断後にスタックする |
| CSCvx44401 | スレッド名 Unicorn Proxy Thread で FTD/ASA がトレースバックする |
| CSCvx48490 | 「Initiator/Responder」パケットを 0 として示す SSL 復号化された https フローの EOF イベント |
| CSCvx50366 | スレッド名 fover_health_monitoring_thread でのトレースバック |
| CSCvx51860 | 6.4.0.x でセンサーの URL ルックアップが有効になっている場合、ライセンスチェックが原因でルックアップが失敗する |
| CSCvx52122 | トランスペアレントコンテキストの削除中の SNMP 通知スレッドでの ASA トレースバックとリロード |
| CSCvx59120 | データトンネルが起動する前に COA を受信すると、親セッションが切断される |
| CSCvx71434 | asa_run_ttyS0 スクリプトによるスレッド名 pix_startup_thread での ASA/FTD トレースバックおよびリロード |
| CSCvx74035 | 複数の ACL とオブジェクトが設定された状態で「clear configure all」を実行すると、ASA がトレースバックおよびリロードする |
| CSCvy09252 | Syncd が 6.4.0.12 ～ 97 の FMC-HA ペアのセカンダリ FMC で繰り返し終了する |

# バージョン 6.4.0.11 で解決済みの問題

表 *55* : バージョン *6.4.0.11* で解決済みの問題

| 不具合 ID | タイトル |
|---|---|
| CSCvv59788 | 6.4.0.8 から 6.4.0.9 へのアップグレード後の 21xx での Lina トレースバック |
| CSCvw42241 | FP1k に CRL コマンドがない |

# バージョン 6.4.0.10 で解決済みの問題

表 *56* : バージョン *6.4.0.10* で解決済みの問題

| 不具合 ID | タイトル |
|---|---|
| CSCuw95798 | Cisco Firepower Management Center ソフトウェアのクロスサイト スクリプティングに対する脆弱性 |
| CSCuz24872 | インライン正規化が有効になっている場合、ドロップされたイベントに対して元のクライアント IP が入力されない |
| CSCvh19161 | スレッド名：SXP CORE での ASA/FTD トレースバックおよびリロード |
| CSCvi46896 | ダウンロードが完了した後に、FeedDownloader がステータスをダウンロード中に更新するべきではない |
| CSCvj93609 | spin_lock_release_actual での ASA トレースバック |
| CSCvm69545 | 複数のシスコ製品で確認された Snort HTTP 検出エンジンのファイルポリシーバイパスの脆弱性 |
| CSCvn27043 | Hostscan：LastSuccessfulInstallParams を Hostscan で検出できない |
| CSCvn78076 | Firepower：[システム（System）] > [モニターリング（Monitoring）] > [統計情報（Statistics）] で、[メモリ使用量（Memory Usage）] に関連して誤解を招く統計情報が表示される |
| CSCvo26597 | CLI バナーが FTD に表示されない |
| CSCvo59683 | EOAttributes テーブル内の古いオブジェクトの数が多いと、高 CPU 使用率/バックアップ障害が発生する |
| CSCvp45786 | Threat Intelligence Director で STIX またはフラットファイルを手動でアップロードできない |
| CSCvp56719 | Cisco FMC および FTD ソフトウェアの sftunnel で確認された「Pass the Hash」攻撃に対する脆弱性 |
| CSCvp56744 | Cisco FMC および FTD ソフトウェアで確認されたディレクトリトラバーサルの脆弱性 |
| CSCvp76950 | thread_logger の Lina スレッドでの FTD のトレースバックおよびリロード |
| CSCvp99327 | スマートサテライトにスマートライセンスを登録しようとした後に FMC UI が応答しなくなる |
| CSCvq04619 | 6.4.0 からのアップグレード後に FTD ftd_sftunnel コアが生成される |

| 不具合 ID | タイトル |
|---|---|
| CSCvq11282 | Cisco Firepower Management Center ソフトウェアのサービス拒否攻撃（DoS）に対する脆弱性 |
| CSCvq20707 | アラートのアクションを持つルールの Snort レンダリングブロックの判定 |
| CSCvq43920 | Cisco Firepower Threat Defense ソフトウェアで確認された隠しコマンドの脆弱性 |
| CSCvq46587 | フェールオーバー後、アクティブユニットの TCP セッションがタイムアウトに達したときに削除されない |
| CSCvq53902 | Cisco Firepower Management Center のクロスサイト スクリプティングの複数の脆弱性 |
| CSCvq63653 | フラグメント化されたパケットの処理時に FTD がクラッシュすることがある |
| CSCvq95694 | メモリリーク SSL_ALLOC [ERROR] ssl_alloc.c:113:ssl_alloc_destroy() |
| CSCvr27584 | estreamer プロセスが rna_policy_rules テーブル用に誤ったデータベースをクエリし、過剰なロギングが発生する |
| CSCvr46901 | 分析接続イベントで、UI にすべてのイベントは表示および報告されない |
| CSCvr49229 | sfmbservice で FMC CPU 使用率が高い |
| CSCvr51955 | Estreamer は、長時間ぶわたって ACK を受信しない場合に接続を終了する必要がある |
| CSCvr53058 | Cisco Firepower Threat Defense ソフトウェアの TCP インターセプトバイパスの脆弱性 |
| CSCvr55741 | 展開に成功した後、FMC に旧ポリシーが表示される |
| CSCvr57051 | ポリシーの展開にエラー「HASH 参照としての未定義の値を使用できません（Can't use an undefined value as a HASH reference）」で失敗しました。 |
| CSCvr63851 | 外部認証経由で NGIPS への SSH 接続が成功しても、すぐに終了する |
| CSCvr66798 | DNS アプリケーションディテクタが DNS トラフィックを検出できないことがある |
| CSCvr76029 | FTD-HA：FTD-HA バックアップファイルを復元した後に、snort プロセスがダウンする |
| CSCvr76044 | FTD Snort ルールプロファイリングが一貫して機能しない：ログフォルダがない |

| 不具合 ID | タイトル |
|---|---|
| CSCvr79974 | フェールオーバーリンクでのパケット損失時に設定が複製されないことがある |
| CSCvr86016 | v3.sds.cisco.com への FMC 接続がプロキシをバイパスしている |
| CSCvr94406 | HTTP でも、HTTPS でもインテリジェンスソース v6.2.3 ～ v6.4.0.4 で TAXII フィードをダウンロードできない |
| CSCvr99222 | NTP 設定がマルチインスタンスの LINA と同期されていない |
| 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 |
| CSCvs05066 | Snort ファイルのメモリプールの破損によりパフォーマンスが低下し、プロセスが失敗する |
| CSCvs09533 | FP2100：3 つ以上のインラインセットを介したトラフィックの処理時のトレースバックおよびリロード |
| CSCvs10748 | Cisco ASA ソフトウェアと FTD ソフトウェアの Web サービス拒否攻撃に対する脆弱性 |
| CSCvs21705 | admin ユーザーは、ドメイン内のデバイスルーティング設定にアクセスする権限がない |
| CSCvs24215 | SSL キー再生成を無効にする Firepower Device Manager（FDM）オプションが設定に反映されない |
| CSCvs28290 | Cisco Firepower Threat Defense ソフトウェアの SSL 入力検証で確認されたサービス拒否攻撃に対する脆弱性 |
| CSCvs39253 | バージョン 6.4 で Firepower 7000 および 8000 が電子メールを送信できない |
| CSCvs41883 | ND ポリシー参照が見つからない場合、6.4.0.x へのアップグレード後に展開が失敗する |
| CSCvs49104 | ネットワークグループを使用する場合、ネットワーク検出ポリシールールは無視される |
| CSCvs50137 | ACP ルールで使用されているのと同じセキュリティゾーンが NGFW ルールにプッシュされない |
| CSCvs50931 | SRU の後でポリシーの展開が失敗する |
| CSCvs56802 | Cisco Firepower 2100 シリーズの SSL/TLS 検証におけるサービス拒否攻撃に対する脆弱性 |
| CSCvs56888 | Cisco Firepower Threat Defense ソフトウェアの TCP フラッド DoS 攻撃に対する脆弱性 |

| 不具合 ID | タイトル |
|---|---|
| CSCvs64510 | メッセージ（「Can't call method "binip" on unblessed reference」）が表示されて展開が失敗する |
| CSCvs71766 | Cisco Firepower Management Center ソフトウェアのオープンリダイレクトの脆弱性 |
| CSCvs74452 | マルウェアシードファイルのロード中に SFDatacorrelator と Snort がコアを繰り返し生成する |
| CSCvs74586 | Firepower FTD トランスペアレントが非 IP パケットを復号化しない |
| CSCvs77334 | 「別のユニットのインスペクションエンジンが Snort とディスクの障害により失敗しました（Inspection engine in other unit has failed due to snort and disk failure）」というエラーにより FTD がフェールオーバーする |
| CSCvs82829 | Anyconnect 設定がサイト間 VPN トンネルに追加されるとコールが失敗する |
| CSCvs87168 | 範囲外のインターフェイス ID による Snort の致命的なエラー |
| CSCvs91270 | インスペクションの中断：展開ページでエラーが発生 |
| CSCvt00113 | SNMP コミュニティストリングのメモリリークによる ASA/FTD トレースバックおよびリロード |
| CSCvt01763 | フローがブルートフォース失敗としてマークされている場合、アプリケーション分類が再試行されない |
| CSCvt02409 | Cisco Firepower Threat Defense ソフトウェアのインラインペア/パッシブモード DoS の脆弱性 |
| CSCvt03598 | Cisco ASA ソフトウェアおよび FTD ソフトウェア Web サービスの読み取り専用パストラバーサルの脆弱性 |
| CSCvt03794 | パッシブゾーンを使用した FTD での SRU 更新後のポリシー展開の失敗 |
| CSCvt04377 | VLAN カプセル化が超過すると、デコードエラーによりディスク領域が枯渇する |
| CSCvt04535 | エラー回復を実行する前、30 秒間 NFE マイクロエンジンがハートビート障害を検出しない |
| CSCvt04560 | クラスタ展開でのファイアウォールで SCTP ハートビートが失敗する |
| CSCvt09940 | Cisco Firepower 4110 の ICMP ソフトウェアの TCP フラッド DoS 攻撃に対する脆弱性 |

| 不具合 ID | タイトル |
|---|---|
| CSCvt13445 | Cisco ASA および FTD ソフトウェアの FTP インスペクションバイパスの脆弱性 |
| CSCvt16642 | FMC がリモートの syslog サーバーに対して一部の監査メッセージを送信していない |
| CSCvt18028 | Cisco ASA および FTD WebVPN の CRLF インジェクションの脆弱性 |
| CSCvt20709 | SSL を挿入した RESET での方向が誤っていたため、誤ったインターフェイスから出力され、MAC フラップが発生する |
| CSCvt24328 | FTD：lina_host_file_open_raw 関数に関連するトレースバックとリロード |
| CSCvt26067 | セカンダリインターフェイスが FTD で使用されている場合、アクティブ FTP が失敗する |
| CSCvt28182 | sctp-state-bypass がインライン FTD に対して呼び出されない |
| CSCvt35053 | Cisco Firepower Management Center ソフトウェアのクロスサイト スクリプティングに対する脆弱性 |
| CSCvt35233 | DAQ モジュール process_snort_verdict 判定ブラックリストからの過剰なロギング |
| CSCvt35897 | Cisco 適応型セキュリティ アプライアンス ソフトウェアと Firepower Threat Defense ソフトウェアの DoS 攻撃に対する脆弱性 |
| CSCvt39135 | SSL ポリシーが適用された状態で、SSL 以外のトラフィックが少ないときに Snort インスタンスにより CPU が 90% を超えてスパイクする |
| CSCvt39349 | 展開ステータスが [展開済み（DEPLOYED）] または [失敗（FAILED）] である限り、デバイスの登録を許可する必要がある |
| CSCvt41333 | IKEv2 トンネルのダウン時にダイナミック RRI ルートが破棄されない |
| CSCvt45863 | IP ヘッダーの長さがパケット長と一致しない場合に暗号リングが停止する |
| CSCvt48941 | 「APP SYNC のタイムアウトにより HA の状態の進行に失敗しました（HA state progression failed due to APP SYNC timeout）」により、FTD スタンバイユニットが HA スイッチオーバー に参加しない |
| CSCvt50263 | FMC が WM モデルデバイスから VPN トラブルシューティングのログを取得できない |
| CSCvt50946 | CSCvi42008 の修正にもかかわらず stuck uauth エントリが AnyConnect ユーザー接続を拒否する |
| CSCvt52782 | ASA トレースバックスレッド名：webvpn_task |

| 不具合 ID | タイトル |
|---|---|
| CSCvt54267 | Cisco Firepower Management Center ソフトウェアのサービス拒否攻撃（DoS）に対する脆弱性 |
| CSCvt59015 | KP IOQ ドライバ。防御パラメータと状態チェックを追加する。 |
| CSCvt59253 | Hostscan データ処理中の ASA 9.13.1.7 のトレースバックとリロード（プロセス名 LINA） |
| CSCvt60190 | Cisco ASA および FTD の Web サービスで確認されたファイルアップロードのサービス拒否攻撃に対する脆弱性 |
| CSCvt61370 | 通信のデッドロックが原因で、デバイスからのイベントが停止することがある |
| CSCvt63556 | 6.4.0.9 でローカルユーザーパスワードが更新されない |
| CSCvt64270 | ASA が、誤った宛先 MAC アドレスを持つフェールオーバーインターフェイス チェック制御パケットを送信している |
| CSCvt64642 | FMC：証明書を照合するために Anyconnect の「証明書マップ」が「DC（ドメインコンポーネント）」を使用中、展開エラーが発生 |
| CSCvt66136 | CC モードを使用した 6.4.0 から 6.4.0.9 へのアップロードにより httpsd.conf に誤った設定が発生する |
| CSCvt66351 | NetFlow のレポートのフローのバイト数が非常に大きい |
| CSCvt66875 | AppId は UltraSurf にトンネリングされた IP ではなく、プロキシ IP をキャッシュする |
| CSCvt68131 | スレッド「IKEv2 Mgd Timer Thread」で FTD がトレースバックし、リロードする |
| CSCvt70322 | Cisco ASA ソフトウェアと FTD ソフトウェアの Web サービス拒否攻撃に対する脆弱性 |
| CSCvt73806 | FP2120 LINA アクティブボックスでの FTD のトレースバックとリロード。[VPN] |
| CSCvt73808 | DAQ から Oct ドライバに送られるヘッダーが長いメッセージの対処 |
| CSCvt75241 | FPR2100 で FTD をリロードした後、VPN でアドバタイズされたスタティックルートの再配布が失敗する |
| CSCvt78068 | FP1000/1100 シリーズプラットフォームの FTD で時刻同期が正しく機能しない |
| CSCvt79777 | sfipproxy.conf で IP アドレスが重複している |

| 不具合 ID | タイトル |
|---|---|
| CSCvt81628 | Ultrasurf の誤検出 |
| CSCvt83121 | Cisco ASA および FTD ソフトウェアの OSPFv2 リンクローカルシグナリングで確認されたサービス拒否攻撃に対する脆弱性 |
| CSCvt86188 | 診断インターフェイスを介して SNMP トラップを生成できない |
| CSCvt93142 | ASA は、クライアント認証の証明書にヌルシーケンスのエンコーディングを許可する必要がある |
| CSCvt95517 | FTD 上の AnyConnect の証明書マッピングが機能しない |
| CSCvu01039 | トレースバック：アクティブなトラフィックでの FTD インラインセットタップモード設定の変更 |
| CSCvu08013 | DTLS v1.2 および AES-GCM 暗号を使用すると、特定のサイズのパケットが頻繁にドロップされる |
| CSCvu08422 | Cisco Firepower Threat Defense ソフトウェアのマルチインスタンスコンテナのエスケープにおける脆弱性 |
| CSCvu12684 | HKT：9.8.4.15 へのアップグレードでフェールオーバー時間が増加する |
| CSCvu15801 | Cisco ASA および FTD ソフトウェアの SIP で確認されたサービス拒否攻撃に対する脆弱性 |
| CSCvu25030 | スレッド名：CP processing での FTD 6.4.0.8 トレースバックおよびリロード |
| CSCvu30134 | logrotate と /var/spool/cron/root ディレクトリがないため、/ngfw で管理されていないディスクの使用率が高い |
| CSCvu38795 | 無効なインターフェイスの GOID エントリが原因で、トレースバック後に FTD ファイアウォールユニットがクラスタに参加できない |
| CSCvu42434 | ASA：実行中の SSH セッションがスタックしているため CPU 使用率が高い/ASA に SSH できない |
| CSCvu43355 | 二重解放によるデータパスでの FTD Lina トレースバック |
| CSCvu44910 | Cisco ASA ソフトウェアと FTD ソフトウェアの Web サービスで確認されたクロスサイト スクリプティングの脆弱性 |
| CSCvu46685 | Cisco ASA および FTD ソフトウェアの SSL/TLS セッションで確認されたサービス拒否攻撃に対する脆弱性 |
| CSCvu47925 | Cisco ASA および FTD IP フラグメントで確認されたメモリリークの脆弱性 |

| 不具合 ID | タイトル |
|---|---|
| CSCvu48285 | TACACS REST API：/cli api を使用して設定された ASA が「Command authorization failed」メッセージで失敗する |
| CSCvu53258 | FMC が証明書マップを誤って lina にプッシュする |
| CSCvu57834 | 100% CPU を使用する syslog-ng プロセス |
| CSCvu59817 | Cisco ASA および FTD ソフトウェアの SSL VPN ダイレクトメモリアクセスで確認されたサービス拒否攻撃に対する脆弱性 |
| CSCvu60923 | Radius サーバーグループオブジェクトの IP を編集すると、IP アドレスの値が意図しないものになる |
| CSCvu63458 | FPR2100：show tech でクラッシュ出力を表示すると、最新のトレースバックからの出力が表示されない |
| CSCvu66119 | シリーズ 3 で URL ルールが誤って昇格されると、トラフィックが誤ったルールに一致する |
| CSCvu70529 | snort のリロード時にバイナリルール（SO ルール）がロードされない |
| CSCvu72658 | AnyConnect 接続クライアント IP が断続的に OSPF にアドバタイズされない |
| CSCvu75581 | Cisco ASA および FTD Web サービスインターフェイスで確認されたクロスサイト スクリプティングの脆弱性 |
| CSCvu75594 | FTD：すでに適用されているキャプチャでキャプチャ バッファ オプションを変更する場合のトレースバックとリロード |
| CSCvu75615 | Cisco ASA ソフトウェアおよび FTD ソフトウェアの WebVPN ポータル アクセス ルール バイパスの脆弱性 |
| CSCvu80370 | Cisco Firepower Threat Defense ソフトウェアの SNMP で確認されたサービス拒否攻撃に対する脆弱性 |
| CSCvu82743 | エンコードされたルールプラグイン SID 値、GID 3 が正しく登録されいない。このルールを無効にする |
| CSCvu83178 | ダイナミック ルーティング プロトコルのサマリールートがスタンバイに複製されない |
| CSCvu83309 | Cisco ASA および FTD Web サービスインターフェイスで確認されたクロスサイト スクリプティングの脆弱性 |
| CSCvu91105 | process_stdout.log ファイルが大きいため、/ngfw で管理対象外ディスクの使用率が高くなる |

| 不具合 ID | タイトル |
|---|---|
| CSCvu98197 | 「復号しない」SSL 復号ルールに一致する HTTPS 接続がブロックされることがある |
| CSCvv09944 | WCCP 設定がプッシュされているときに FTD 展開時に LINA がトレースバックする |
| CSCvv13835 | Cisco ASA および FTD Web サービスインターフェイスで確認されたクロスサイト スクリプティングの脆弱性 |
| CSCvv13993 | Cisco Firepower 1000 シリーズの Bleichenbacher 攻撃に対する脆弱性 |
| CSCvv16245 | Cisco Firepower Management Center ソフトウェアの共通アクセスカード認証バイパスの脆弱性 |
| CSCvv33712 | Cisco ASA ソフトウェアの Web ベース管理インターフェイスに影響するクロスサイト スクリプティングの脆弱性 |
| CSCvv40916 | 展開中に、AbstractBaseDeploymentValidationHandler.validatePreApply に 3 分の遅延が発生する |
| CSCvv44051 | GRE/IPiniP パッセンジャフローによる snp_cluster_forward_and_free_packet でのクラスタ ユニット トレースバック |
| CSCvv50107 | HA でピアを切り替えようとすると FTD がトレースバックとリロードを実行する |
| CSCvv52591 | ctm_hw_malloc_from_pool で DMA メモリリークが発生し、管理接続と VPN 接続が失敗する |
| CSCvv58604 | トラフィックが、ブロック/リセットおよび SSL インスペクションで設定された AC ポリシーと一致する場合、リセットが送信されない |
| CSCvv70096 | Snort 2：SSL 復号化および再署名プロセスでのメモリリーク |
| CSCvv77910 | FQDN ルールが 1K プラットフォームで機能しない |
| CSCvv98534 | アップグレードに失敗しても、syslog に監査メッセージが作成されない |
| CSCvw48033 | SNMP アラートの SNMPv3 認証およびプライバシーパスワードの変更がすぐに反映されない |

# バージョン 6.4.0.9 で解決済みの問題

表 *57* : バージョン *6.4.0.9* で解決済みの問題

| 不具合 ID | タイトル |
|---|---|
| CSCvi34123 | 拡張機能：リストの先頭に _ が含まれている DNS リストを追加できない |
| CSCvj00997 | 「show open-network-ports」で FP4100 シリーズの適切な情報が表示されない |
| CSCvm77115 | 無効な TSC 値による Lina のトレースバック |
| CSCvo31790 | Cisco Firepower Threat Defense ソフトウェア管理インターフェイス DoS 脆弱性 |
| CSCvo76866 | 2100 でのトレースバック：ウォッチドッグ |
| CSCvo80853 | Cisco Firepower Threat Defense ソフトウェアのパケットにおけるサービス拒否攻撃に対する脆弱性 |
| CSCvp57643 | FTD/ASA：クラスタ/HA ： マスター/アクティブ ユニットではすべてのルート変更がスレーブ/スタンバイに更新されない |
| CSCvp63814 | FTD - 内部フロー：キャリア ID フロールックアップの強化 |
| CSCvp90847 | FTD/FMC での再署名に SSL が使用するルート CA の更新 |
| CSCvp93468 | Cisco ASA ソフトウェアと Cisco FTD ソフトウェアの SSL VPN におけるサービス拒否攻撃に対する脆弱性 |
| CSCvp99930 | プライマリがアクティブの間に sftunnel の例外で展開が失敗する |
| CSCvq09357 | FMC での無制限のファイルのアップロード：バックアップの管理：バックアップのアップロード |
| CSCvq10500 | CLISH と LINA の両方のキャプチャが IPv6 アドレスで機能しない |
| CSCvq24258 | 大規模なアプライアンスで Mojo サーバーのワーカー数が増加する |
| CSCvq35440 | Anyconnect のストラップ検証へのアップグレードの機能拡張：Cisco VPN セッションリプレイの脆弱性 |
| CSCvq38889 | slib memory manager： mempool mutex vs spinlock selection |
| CSCvq39344 | Firepower の管理対象デバイスが SNMPv3 GET/WALK 要求への応答を停止することがある |
| CSCvq61601 | FTD での OpenSSL の脆弱性 CVE-2019-1559 |

| 不具合 ID | タイトル |
|---|---|
| CSCvq71351 | FMC：インラインセットの編集時にページがスタックする |
| CSCvq79913 | Null pdts_info の ICMP エラーパケットがドロップされる |
| CSCvq89361 | Cisco Firepower 1000 シリーズの SSL/TLS におけるサービス拒否攻撃に対する脆弱性 |
| CSCvq89794 | FDM：ユーザーダウンロードが LDAPS で機能しない |
| CSCvq93572 | 外部認証を使用して FTD にユーザーを追加することができません。 |
| CSCvq93669 | Cisco Firepower Threat Defense ソフトウェアの SSL/TLS URL カテゴリバイパスの脆弱性 |
| CSCvq96495 | FPR2100 のコンソール接続が約 20 分間ランダムに切断される |
| CSCvr07460 | 暗号 PKI の動作に関連して ASA がトレースバックおよびリロードする |
| CSCvr09468 | CLI 「Show nat pool」の ASA トレースバックとリロード |
| CSCvr13278 | リロード後に PPPoE セッションが起動しない。 |
| CSCvr17735 | SI 更新時の SFDataCorrelator で CPU の使用率が高くなる |
| CSCvr19922 | クラスタ：特定の状況下で BGP ルートが同期しなくなる場合がある |
| CSCvr20449 | 実際には失敗しているポリシー展開が FMC で成功したとレポートされる |
| CSCvr20893 | ポリシーの展開後に ids_event_proce プロセスで HA ペアの FTD がクラッシュする |
| 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 |
| CSCvr30694 | FMC：FMC が HA 同期の失敗を検出する |
| CSCvr33586 | FPR1010：しきい値を超えた場合の SSD の温度/警告を追加する |
| CSCvr35125 | フェールオーバーリンクを介したパケット損失が Split-Brain をトリガーする |
| CSCvr39556 | libclamav.so のセグメンテーション違反（SFDataCorrelator のコンテキスト内） |
| CSCvr42344 | PBR に設定されたアクセスリストからのルールの削除時の snp_policy_based_route_lookup でのトレースバック |
| CSCvr49833 | Cisco Firepower 2100 シリーズのセキュリティアプライアンスの ARP におけるサービス拒否攻撃に対する脆弱性 |

| 不具合 ID | タイトル |
|---|---|
| CSCvr51998 | BGP 経由でデフォルトルートを学習後、ASA スタティックルートが ASP テーブルから消える |
| CSCvr54250 | レルムが設定されていない場合でも user_ip_map ファイルの数が多い |
| CSCvr54980 | FPR2100：シャーシの背面にある電源ボタンをオフにしても、電源がオフにならない |
| CSCvr56031 | スレッド名「cli_xml_server」でFTD/LINAがトレースバックし、リロードされる |
| CSCvr72665 | FMC の 6.3/6.4 へのアップグレードで、既存の廃止済み flexconfig を削除しないようにする必要がある |
| CSCvr73115 | ポリシーインポート後の初期 FTD の展開によって未使用オブジェクトが発生し、ポリシーサイズが膨張する |
| CSCvr78166 | 「実行コンフィギュレーションの取得に失敗しました（failed to retrieve running configuration）」という理由で、展開が FTD 上で失敗した |
| CSCvr79008 | 不正なユーザー名の正規化を実行しているすべてのディレクトリサーバーを FMC が非効率的に照会するため、セッション処理が遅延する |
| CSCvr86213 | CD は、クラスタノードリリースの Lina の状態の Cluster-Msg-Delivery-Confirmation を無視する必要がある |
| CSCvr90768 | FTD：低速リンクを通じた展開は失敗する場合がある |
| CSCvr90965 | Azure で FTDv 展開を行うと、「no dns domain-lookup any」により回復不能なトレース状態が発生する。 |
| CSCvr92168 | Cisco ASA および Cisco FTD ソフトウェアの OSPF パケット処理によるメモリリークの脆弱性 |
| CSCvr92327 | ASA/FTDがスレッド名「PTHREAD-1533」でトレースバックおよびリロードすることがある |
| CSCvr92617 | SecurityIntelligenceEoConvertor の NPE によって、Lucene のインデックスの作成が失敗する |
| CSCvr93978 | スレッド DATAPATH-0-2064 で ASA がトレースバックし、リロードする |
| CSCvr96527 | 新しいルールの追加中に FMC の既存ルールがエラーになる |
| CSCvs00023 | CLISH CLI からの「shutdown」コマンドでポートマネージャがクラッシュする |
| 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 |

| 不具合 ID | タイトル |
|---|---|
| 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 |
| CSCvs04067 | Catalina へのアップグレード後、Mac 上の Chrome では FMC デバイスにアクセスできない |
| CSCvs06043 | ngfwManager の CSM_CCMservice 用の TunnelClient が FMC の CSM_CCM サービスから送信された ACK を読み取らない |
| CSCvs07668 | SIP インスペクションが有効になっていると、スレッド DATAPATH-1-15076 で FTD がトレースバックし、リロードする。 |
| CSCvs07982 | ASA トレースバック：sctpProcessNextSegment - SCTP_INIIT_CHUNK |
| CSCvs10443 | 6.5 CloudEvent コードが、6.4 コードが理解しない方法で config ファイルを書き込む |
| CSCvs10526 | FTD での SSE 試行のスロットル |
| CSCvs12288 | SSL ポリシーが有効になっている状態で debug_policy_all が設定されていると Snort が予期せず終了する |
| CSCvs15276 | エラー：IPv6 ICMP の設定時に ::/0 のエントリが存在する |
| CSCvs15972 | SSL ポリシーが有効な場合にネットワークパフォーマンスが低下する |
| CSCvs19968 | スタックし、HA FTD ポリシー展開エラーが発生しないようにコンソールを修正する |
| CSCvs22503 | 「ポリシーイベントの逆シリアル化に失敗しました（Failed to deserialize policy event）」の後に eStreamer が繰り返し終了する |
| CSCvs23750 | 6.4.0.4 FMC WebUI でシリーズ 3 スタックを作成できない（プライマリデバイスを選択できない） |
| CSCvs25607 | 制約事項に netmap_num を追加するとパフォーマンスが低下する |
| CSCvs28094 | FP8000 センサーのユーザー設定を編集するとエラー 403 が表示される |
| CSCvs28580 | 高負荷状態で SSL トラフィックを処理するときのトレースバック |
| CSCvs29405 | CMD フィールドがフレーム内に存在しない場合、Snort がトラフィックをタグ付きとして処理する |
| CSCvs32303 | snmpd プロセスが待機状態であるため、スタンバイ FMC で SNMP ポーリングが失敗する |
| CSCvs33416 | カーネルを cpe:2.3:o:linux:linux_kernel:4.14.158: にアップグレード |

| 不具合 ID | タイトル |
|---|---|
| CSCvs34844 | ハードウェアと通信すると、pm プロセスがランダムにデッドロック状態になる |
| CSCvs34854 | FMC がアクセスリスト CLI の差分の後ろに参照インターフェイス CLI の差分を生成する |
| CSCvs37013 | octeon_init がスタックし、HA FTD ポリシー展開エラーを発生させないようにする |
| CSCvs39388 | FTD が CC モードでシステム syslog メッセージを送信しない |
| CSCvs40531 | AnyConnect 4.8 が FPR1000 シリーズで動作していない |
| CSCvs45111 | CCM レイヤ（スプリント 75）での WR6 および WR8 コミット ID の更新 |
| CSCvs47201 | デバイスレコードに対して GET ALL を実行すると、「isPartOfContainer」が返される。HA とクラスタの一部であるデバイスでは偽 |
| CSCvs47252 | コマンド「clear capture/」を実行している場合の ASA トレースバックとリロード |
| CSCvs50459 | Cisco ASA および Cisco FTD の不正な OSPF パケット処理によるサービス拒否攻撃に対する脆弱性 |
| CSCvs50952 | 6.4.0.4-34 を 6.4.0.6 にアップグレードすると、静的ルートが削除される |
| 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 |
| CSCvs61392 | Firepowerデバイスで、ポリシーが正常に展開された後、ハードウェアルールが更新されない |
| CSCvs79023 | スレッド名での ASA/FTD のトレースバック：DNS インスペクションによる DATAPATH |
| CSCvs80157 | スレッド名 IKE Daemon での ASA のトレースバック |
| 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 |
| CSCvs91389 | FTD トレースバック Lina プロセス |
| CSCvs91869 | FPR-1000 シリーズのランダム番号生成エラー |
| CSCvs98634 | catalina.<date>.log のファイルは、パーティション内のすべてのディスク容量を消費する可能性がある |
| CSCvt01397 | LINA 設定がプッシュされなかったにもかかわらず、展開は正常としてマークされる |

| 不具合 ID | タイトル |
|---|---|
| CSCvt10097 | セキュリティゾーンにインターフェイスがある場合でも、SF_Egress_Zone/SF_Ingress_Zone に関するログが空になる |
| CSCvt15163 | Cisco ASA および FTD ソフトウェアの Web サービスに関する情報漏洩の脆弱性 |
| CSCvt21041 | スレッド「ctm_ipsec_display_msg」での FTD のトレースバック |
| CSCvt33785 | ランダム VPN ピアの IPSec SA が作成されない |
| CSCvt46830 | FPR2100 「show crypto accelerator statistics」 カウンタは対称暗号を追跡しない |
| CSCvt79988 | FMC を 6.6 にアップグレードした後、SNMP 設定が原因でポリシー展開が失敗する |
| CSCvt93177 | デフォルトでフルプロキシを無効化してライトウェイトプロキシにする。（FP2LWP）FTD デバイス |

# バージョン 6.4.0.8 で解決済みの問題

**表 *58* : バージョン *6.4.0.8* で解決済みの問題**

| 不具合 ID | タイトル |
|---|---|
| CSCul34972 | FO ユニットが反転した後、DHCP クライアントプロキシが無効にならない |
| 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 |
| CSCvd33448 | バックアップ復元後、fireamp.pl が CPU を 100% 使用する |
| CSCvh75756 | 重複するプリプロセッサキーワード：ssl（Duplicate preprocessor keyword: ssl） |
| CSCvk55766 | デバイスをプラットフォーム設定ポリシーに割り当てようとすると、一連のデバイスがランダムにポリシーから消える |
| CSCvm85823 | SSH、ssh_exec を実行できない：コンソールでの open(pager) エラー |
| CSCvo74833 | 追跡されていないファイルが原因で、Firepowerデバイスの管理対象外ディスク容量が大きくなる |
| CSCvp04134 | 9.12.1 へのアップグレード時に HTTP CLI Exec でトレースバックする |

| 不具合 ID | タイトル |
|---|---|
| CSCvp06526 | 短い CPU アフィニティに一致するように sfhassd スレッド CPU アフィニティを管理する |
| CSCvp39970 | /var/opt/CSCOpx/MDC/tomcat/log/stdout.logs によってログメッセージが過剰に書き込まれ、ディスクがいっぱいになる場合がある |
| CSCvp70833 | ASA/FTD：同じサービスの NAT ルールがエラー「エラー：NAT がポートを予約できません（ERROR: NAT unable to reserve ports）」を 2 回表示する |
| CSCvp81083 | TLS/VPN に関連する ASA/Lina のトレースバック |
| CSCvq10239 | SSL HW アクセラレーションを有効にすると、FTD TCP プロキシが 3 回の再送信後に接続を切断する |
| CSCvq14954 | 管理専用のスレーブユニットがクラスタに参加できない |
| CSCvq29969 | 再生成されていない場合でも、Firepower 推奨ルール数が変更される |
| CSCvq34160 | fp1000 シリーズプラットフォームへの ASDM 接続の確立時のトレースバックとリロード |
| CSCvq43453 | サブドメインの変数セットで使用されている場合、ポートオブジェクトにオーバーライドを追加できない |
| CSCvq45105 | ENH：SSE/CDO を介して FDM flex-config CLI および CLI-console API の問題に「管理アクセス」を追加する |
| CSCvq46587 | フェールオーバー後、アクティブユニットの TCP セッションがタイムアウトに達したときに削除されない |
| CSCvq50587 | ASA/FTD がスレッド名「BGP Router」でトレースバックし、リロードすることがある |
| CSCvq51284 | FPR 2100、low block 9472 がデバイスを介してパケット損失を発生させる |
| CSCvq56257 | キャッシュされたマルウェアの処置が想定どおりに期限切れにならないことがある |
| CSCvq67271 | 子アクセスポリシーの ID によって特定ルールを取得すると、「404：見つかりませんでした（404: Not Found）」ステータスが返される |
| CSCvq73534 | Cisco ASA ソフトウェアのケルベロス認証バイパスの脆弱性 |
| CSCvq73599 | Cisco VPN セッションリプレイの脆弱性：ASA for SSL（OpenSSL 1.0.2）および SCEP プロキシのストラップ修正 |
| 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 |

| 不具合 ID | タイトル |
|---|---|
| CSCvq76198 | FreeBSD システムのトラフィックの中断 |
| CSCvq83019 | ACPolicy に多数のアプリケーション フィルタ オブジェクトが使用されている場合に、ポリシー展開タスクの挿入の処理に長時間かかる |
| CSCvq87797 | マルチコンテキスト 5585 ASA、透過的コンテキストで管理インターフェイス設定が失われる |
| CSCvq88644 | tcp-proxy でのトレースバック |
| CSCvq95058 | IPSEC SA が、リンクダウンによって発生したフェールオーバーにより削除される |
| CSCvq95826 | DCD が原因でスタンバイがプローブを送信する |
| CSCvq97346 | UI で NAT ルールを移動し、展開すると、FDM バックエンドから NAT ルールが削除される |
| CSCvr04954 | スタックユニット：NDPolicy obj err をロードできない別のドメインでのアップグレード後に展開が失敗する |
| CSCvr10777 | Ikev2 デーモンでの ASA トレースバック |
| CSCvr11395 | スケジュール済みの展開時にデバイスグループから展開された一部のデバイスのみ |
| CSCvr13823 | Cisco Firepower Threat Defense ソフトウェア管理アクセスリストバイパスの脆弱性 |
| CSCvr25768 | ASA が display_hole_og でトレースバックすることがある |
| 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 |
| CSCvr29638 | FMC から ACP を展開した後、FPR2110 で HA FTD がトレースバックする |
| CSCvr29978 | ルールを変更してすぐに保存すると、設定が削除されることがある |
| CSCvr36687 | サブドメインの変数セットで使用されている場合、ネットワークオブジェクトにオーバーライドを追加できない |
| CSCvr50266 | リロードの問題によってデュアルスタック ASAv フェールオーバーがトリガーされる |
| CSCvr53058 | tcp-intercept と AC ポリシーのモニターを設定すると、AC ポリシーのルックアップが SYN+ACK パケットに対して実行される |

| 不具合 ID | タイトル |
|---|---|
| CSCvr54054 | アイデンティティ NAT トラフィックに対して MAC の書き換えが実行される |
| CSCvr55400 | スレッド名「cli_xml_server」で FTD/LINA がトレースバックし、リロードされる |
| CSCvr55825 | Cisco ASA および FTD ソフトウェアのパストラバーサルの脆弱性 |
| CSCvr59927 | SRU インストールが進行中の場合、展開が失敗する |
| CSCvr60111 | 設定がスタンバイから削除され、アクティブ時に展開が失敗する |
| CSCvr61239 | 情報システムは、送信時に TLS を介して POST メソッドを使用する必要がある |
| CSCvr61241 | ファイルアップロード機能を実装する情報システムでは、ファイルサイズを検証する必要がある |
| CSCvr61252 | システムは、機密情報が cookie 内に格納されるのを防ぐ制御を実施する必要がある |
| CSCvr61492 | REST API コールに関連し、デバイスのロードが低速になる |
| CSCvr66768 | PBR 設定がプッシュされているときに FTD 展開時に LINA がトレースバックする |
| CSCvr81457 | TLS トラッカー（tls_trk_sniff_for_tls）がブロックを解放しようとすると、FTD がトレースバックする |
| CSCvr85295 | Cisco Adaptive Security Appliance と Firepower Threat Defense ソフトウェア リモート |
| CSCvs10114 | ネストされたネットワーク オブジェクト グループが NAP ルールに対して展開されていないため、導入が失敗する |
| CSCvs32023 | 出力最適化処理をオフにする |
| CSCvs53705 | AnyConnect セッションが誤って制限されている |

# バージョン 6.4.0.7 で解決済みの問題

表 *59* : バージョン *6.4.0.7* で解決済みの問題

| 不具合 ID | タイトル |
|---|---|
| CSCvh75756 | 重複するプリプロセッサキーワード：ssl（Duplicate preprocessor keyword: ssl） |
| CSCvr52109 | 複数のデバイスへの展開後、FTD が正しいアクセスコントロールルールに一致しないことがある |
| CSCvr88123 | マルチ展開により、侵入イベントが突然ドロップする |
| CSCvr95287 | Cisco Firepower Management Center LDAP 認証バイパスの脆弱性 |
| CSCvs32023 | 出力最適化処理をオフにする |

# バージョン 6.4.0.6 で解決済みの問題

（注） バージョン 6.4.0.6 は 2019 年 12 月 19 日に シスコ サポートおよびダウンロード サイト から削除されました。このバージョンを実行している場合は、アップグレードすることをお勧めします。ここに記載されているバグは、バージョン 6.4.0.7 でも修正されています。

表 *60* : バージョン *6.4.0.6* で解決済みの問題

| 不具合 ID | タイトル |
|---|---|
| CSCvm48451 | 4100 および 9300 で侵入イベントパフォーマンスのグラフが空白になる |
| CSCvn24920 | スタンバイデバイスが 9.12 イメージにアップグレードされている場合に、VPN セッションがスタンバイユニットに複製されない |
| CSCvn77388 | SDI - 一時停止されたサーバーにより、正常なサーバーでの認証の完了に 15 秒の遅延が発生する |
| CSCvo11280 | ASA 機能拡張：SDI クラスタのメンバーで状態が変更されたら、syslog メッセージを生成する |
| CSCvo28118 | メンバーがクラスタに参加しようとすると VPN クラスタリング HA のタイマースレッドでトレースバックが発生する |
| CSCvo43795 | OSPF プロセス のクリア後でも OSPF プロセス ID が変更されない |

| 不具合 ID | タイトル |
|---|---|
| CSCvo73250 | ENH：警告「重複する要素が見つかりました（found duplicate element）」の ACE の詳細 |
| CSCvo74397 | ENH：「コマンドは無視されました。設定中です...（Command Ignored, configuration in progress...）」にプロセス情報を追加 |
| 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 |
| CSCvp04186 | cts import-pac tftp：構文が機能しない |
| CSCvp12582 | ASA のウェルノウンポート名ではなくポート番号をアクセスリストで表示するオプション |
| CSCvp23109 | ASA HA IKEv2 汎用 RA -「AnyConnect Premium All In Use」がスタンバイ状態で正しく表示されない |
| CSCvp33341 | Cisco ASA および Firepower Threat Defense ソフトウェア WebVPN クロスサイト スクリプティングの脆弱性 |
| 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 |
| CSCvp55941 | ファイル復帰ブロックがランダムにスローされて、SMB 共有からのファイルへのアクセスに関する問題が発生する |
| CSCvp56805 | 「書き込み時のデータが多すぎます（Too much data during a write）」というメッセージが通信チャネルにフラッディングする |
| CSCvp76944 | Cisco ASA および FTD ソフトウェア WebVPN CPU のサービス妨害（DoS）脆弱性 |
| CSCvp85736 | クラスタマスターのリロードによって管理仮想 IP への ping が失敗する |
| CSCvp87623 | CAC（HTTPS クライアント証明書）の使用時に更新をアップロードすると「更新要求エンティティが大きすぎます（update request entity too large）」というエラーが発生する |
| CSCvq05113 | 設定の最初の 10 個のインターフェイスで ASA フェールオーバー LANTEST メッセージが送信される |
| CSCvq09093 | VPN 事前展開の検証がデバイスごとに約 20 秒かかる |
| CSCvq17263 | DATAPATH-8-15821 での FTD LINA のトレースバック |
| CSCvq24494 | FP2100 - FP2100 プラットフォームでリング/CPU コアをオーバーサブスクライブするフローによって動作中フローの中断が発生する |
| CSCvq28250 | ENH：syn cookie の問題に関する ASA クラスタのデバッグ |

| 不具合 ID | タイトル |
|---|---|
| CSCvq36042 | ハートビートが失われてリロードが発生する |
| CSCvq39317 | ASA がファイルの整合性を確認できない |
| CSCvq40943 | 6K スポークでの FTD 4150 VPN s2s 展開の失敗 |
| 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 |
| CSCvq45000 | NAT が設定されている場合に FP 8000 センサーへのポリシーの展開が失敗する |
| CSCvq46443 | Cisco Firepower Management Center に蓄積されたクロスサイトクリプティングの脆弱性 |
| CSCvq53915 | Cisco Firepower Management Center のクロスサイト スクリプティングの複数の脆弱性 |
| CSCvq54667 | SSL ネゴシエーションの問題により、SSL VPN が確立できない場合がある |
| CSCvq57591 | フェールオーバーリンクで IP 通信のみが中断される場合にデータインターフェイスで LANTEST メッセージが送信されない |
| CSCvq59702 | ハンドシェイクメッセージの喪失後にデバイスからの接続イベントが停止する |
| CSCvq60131 | デバイスへの EZVPN スポークの移動時に ASA のトレースバックが発生する |
| CSCvq63024 | デュアルスタック ASAv の手動フェールオーバーの問題 |
| CSCvq64742 | スレッド名 ssh での ASA5515-K9 スタンバイトレースバック |
| CSCvq65241 | スレッド名での Saleen の ASA トレースバック：IPv6 IDB |
| CSCvq65542 | すべてのバグが修正されるまで、fp2100 から asp load-balance per-packet 機能を無効にする |
| CSCvq69111 | トレースバック：スレッド名でのクラスタユニット lina のアサーション：クラスタコントローラ |
| CSCvq70468 | ASA クラスタが OSPF ルートをフラッシュしない |
| CSCvq70485 | 「securityzones」REST API が低速になる |
| CSCvq70775 | FPR2100 FTD スタンバイユニットで 9K ブロックがリークする |
| CSCvq71217 | CSCvn30118 の後、mysql-server.err によりローテーションが失敗して、ディスク使用率が高くなる |

| 不具合 ID | タイトル |
|---|---|
| CSCvq75743 | ASA：3 ホップ離れた宛先に対する BGP の再帰ルートルックアップが失敗する |
| CSCvq76533 | MC4000 の F_RNA_EVENT_LIMIT は 2000 万である必要がある |
| CSCvq77547 | ポートチャネルでのフェールオーバー記述子の不一致により、フェールオーバーで接続の複製が失敗する |
| CSCvq80318 | Internal-Data0/1 の列挙時に ASA が PCI cfg 領域に関する誤ったエラーメッセージを生成する |
| CSCvq81516 | FMC で 12 時～午後 1 時（UTC）の間の VPN イベントが表示されない |
| CSCvq83168 | FMC ではサーバーアドレスの後にインターフェイスを使用できないため、管理 VRF を使用した DNS ルックアップを実行できない |
| CSCvq87703 | アクティブデバイスが正しいピア状態を報告しない |
| CSCvq91645 | フローオフロードハッシュの動作変更 |
| CSCvq92126 | スレッド IPsec Message Handler での ASA のトレースバック |
| CSCvq94729 | デルタ CLI の LINA ONLY セクションでのエラー時に展開のロールバックによってトラフィックの瞬間的なドロップが発生する |
| CSCvr00892 | 外部データベースアクセスで where 句が機能しない |
| CSCvr07421 | セキュリティゾーン内にインターフェイスが 400 以上あると、deployDB の不適切な形成により、ポリシーの展開が失敗する |

# バージョン 6.4.0.5 で解決済みの問題

**表 *61* : バージョン *6.4.0.5* で解決済みの問題**

| 不具合 ID | タイトル |
|---|---|
| CSCvh73096 | 使用可能な場合に ISE から sAMAccountUserName を読み取る |
| CSCvo66546 | SFDataCorrelator プロセスで Firepower が頻繁にトレースバックおよび再起動する |
| CSCvp95663 | IPS イベント（「ブロックした場合（Would have blocked）」）の InlineResult でメタデータが欠落する |
| CSCvp97061 | URL フィルタリングですべての URL が未分類として表示される |

| 不具合 ID | タイトル |
|---|---|
| CSCvq32678 | アップグレードの異常によりポリシーの展開が失敗する：NGFW_UPGRADE がマップファイルで見つかりません（NGFW_UPGRADE is missing in map file） |
| CSCvq32681 | FTD のアップグレード時に複数のインターフェイスペアのインラインセットに対して Fail to Wire 設定が無効になる |
| CSCvq39083 | SSL ポリシーが有効になっている場合にブラックリストに登録された URL への HTTPS 接続がセキュリティ インテリジェンスでドロップされない |
| CSCvq41936 | 新しいユーザーを追加した後に FMC UI で SNMP を無効にしてから再度有効にする必要がある |
| CSCvq44594 | 「不明な HPQ ルールキー（Unknown HPQ rule key）」というメッセージがログに大量に出力される |
| CSCvq46804 | 大文字の RADIUS を含む AD ユーザー名でログインできない |
| CSCvq46918 | アップグレード後に SNMPv3 ユーザーが削除される |
| CSCvq54242 | SSL ポリシーでの警告「送信元ネットワークで、空のグループがあります（There is an empty group in the source networks）」 |
| CSCvq56138 | パスワードの文字列にスペースが含まれている場合に LDAP ユーザーの FMC GUI へのユーザーログインが失敗する |
| CSCvq56462 | ファイルポリシーが一部のマルウェアドキュメント（.doc）および Adobe Flash（.swf）ファイルを検査しない |
| CSCvq65092 | デバイス関連の REST API コールが低速になる |
| CSCvq66217 | FMT \| MTU 値が許容範囲内にない |
| CSCvr23858 | domain_snapshot_timeout（20m）により、FMC から FTD へのポリシーの展開が失敗する（または時間がかかる） |

# バージョン 6.4.0.4 で解決済みの問題

**表 *62 : バージョン 6.4.0.4* で解決済みの問題**

| 不具合 ID | タイトル |
|---|---|
| CSCvf83160 | スレッド名 DATAPATH-2-1785 でのトレースバック |
| CSCvg29468 | 一般的なマイクロエンジン障害が誤検出される可能性の減少 |

| 不具合 ID | タイトル |
|---|---|
| CSCvh13869 | ASA IKEv2 が aaa セッションを開けない：「セッション数の上限 [2048] に達しました（session limit [2048] reached）」 |
| CSCvj61580 | スレッドでの ASA トレースバック：DATAPATH-8-2035 |
| CSCvk22322 | アクティブユニット（cachefs_umount を含む）から設定を同期する際の ASA トレースバック（ウォッチドッグタイムアウト） |
| CSCvk26612 | 「デフォルトのキーリング証明書が無効です。理由：期限切れ（default Keyring's certificate is invalid, reason: expired）」 ヘルスアラート |
| CSCvk29685 | ASA の DATAPATH でのトレースバック |
| CSCvm36362 | ルート トラッキング エラー |
| CSCvm39901 | ENH：ASA - マルチモードでの 4 台を超えるサーバーのサポート |
| CSCvm40288 | HA リンクでのポートチャネルの問題 |
| CSCvm64400 | IKEv2：IKEv2-PROTO-2：「プラットフォームからの PSH の割り当てに失敗しました（IKEv2-PROTO-2: Failed to allocate PSH from platform）」 |
| CSCvm68648 | Firepower ソフトウェアの CVE-2016-8858（OpenSSH）に必要な更新 |
| CSCvm82966 | Linux カーネル 4.14 の脆弱性 |
| CSCvn76875 | BGP のグレースフルリスタートが断続的に動作しなくなる |
| CSCvn78593 | FTD でコントロールプレーン ACL が正しく機能しない |
| CSCvn78870 | 範囲外の allocate-interface コマンドによる ASA マルチコンテキストのトレースバックとリロード |
| CSCvo03700 | クラスタがスレーブユニットで有効になっている場合にスレッドロガーで ASA がトレースバックすることがある |
| CSCvo14961 | 「dns_cache_timer」プロセスの終了を待機している間に ASA がトレースバックし、リロードすることがある。 |
| CSCvo29989 | Cisco FirePower Threat Defense に関する情報漏えいの脆弱性 |
| CSCvo31695 | メモリブロックの解放時におけるスレッド名 DATAPATH-0-1668 でのトレースバック |
| CSCvo45755 | box stall mid-transfer への ASA SCP 転送 |
| CSCvo47390 | スレッド SSH での ASA トレースバック |
| CSCvo48838 | 長すぎる設定行のエラーを Lina が適切に報告しない |

| 不具合 ID | タイトル |
|---|---|
| CSCvo51265 | Cisco 適応型セキュリティ アプライアンス ソフトウェアのセキュアコピーのサービス拒否（DoS）攻撃に対する脆弱性 |
| CSCvo55809 | 一部のイメージにおいてインストール状態で ASA アプリケーションがスタックする |
| CSCvo65741 | ASA：フェールオーバーが発生して BGP ルートが変更されると、ルーティングテーブルで BGP ルートがクリアされる |
| CSCvo66534 | 影響を受けるスレッドとしてデータパスを示すトレースバックとリロード |
| CSCvo67421 | ASA：EzVPN クライアントが特定のリリースへのソフトウェアアップグレード後に機能しない |
| CSCvo68184 | セカンダリ FTD の診断 I/F の管理専用が表示されなくなる |
| CSCvo74350 | ASA がトレースバックしリロードすることがある。WebVPN トラフィックに関連する可能性がある |
| CSCvo74625 | 管理ゲートウェイがデータインターフェイスとして設定されている場合、6.4.0 - IPv6 ルーティングが WM および KP で機能しません |
| CSCvo77796 | グローバルなスナップショットの作成における IntrusionPolicy の手順が遅いために、導入が遅くなる |
| CSCvo78789 | Cisco 適応型セキュリティアプライアンスのスマートトンネルに関する脆弱性 |
| CSCvo80501 | 手動フェールオーバーの実行時にスタンバイファイアウォールがトレースバックしてリロードする |
| CSCvo83169 | Cisco ASA ソフトウェアと FTD ソフトウェアの FTP のインスペクションサービス拒否攻撃に対する脆弱性 |
| CSCvo87930 | w3m を使用した ipv6 の HTTP が失敗する |
| CSCvo87985 | ASA が「copy」コマンドのパスワードをプレーンテキストで送信する |
| CSCvo90153 | ASA が特殊文字を含むユーザーを https 経由で認証できない |
| 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 |
| CSCvo97979 | インターフェイス設定の delay コマンドが再起動後に変更される |
| CSCvp12052 | ASA がトレースバックおよびリロードすることがある。webvpn に関連する可能性がある |

| 不具合 ID | タイトル |
|---|---|
| CSCvp14674 | ASAv Azure：ASAv のフェールオーバー時にルートテーブルの BGP 伝達設定がリセットされる |
| CSCvp19910 | ヘッダー TEID : 0 の gtpv1 identification req メッセージを処理できない |
| CSCvp19998 | ASA がヘッダー TEID:0 の GTPV1 SGSN Context Req メッセージをドロップする |
| CSCvp23137 | SSD 2 が見つからない場合に ASA/FTD が syslog を生成する：/dev/sdb が存在する。ステータス：操作不能（/dev/sdb is present. Status: Inoperable） |
| CSCvp30447 | 侵入ポリシーでグローバルルールしきい値が無効になっている場合に syslog アラートがサーバーに送信されない |
| CSCvp32617 | 9.6.2 以降で「確立済み TCP」が機能しない |
| CSCvp35141 | ASA が POST 要求に対して無効なリダイレクト応答を送信する |
| CSCvp35384 | IKEv2 RA 汎用クライアント - asp テーブルエントリの発信時にスタックする - 古い SPI で暗号化されたトラフィック |
| CSCvp38530 | 100 を超える AAA サーバーグループの上限到達を設定できない |
| CSCvp42275 | WR8 の CCM インフラストラクチャの更新 |
| CSCvp45882 | Cisco ASA ソフトウェアと FTD ソフトウェアの SIP のインスペクションサービス拒否攻撃に対する脆弱性 |
| CSCvp46341 | 2100 Firepower プラットフォームで Fail-to-Wire（FTW）ポートが回復に失敗する |
| CSCvp49576 | xlate_detach のウォッチドッグによる FTD のトレースバック |
| CSCvp49790 | Cisco ASA ソフトウェアと FTD ソフトウェアの OSPF LSA 処理のサービス拒否攻撃に対する脆弱性 |
| CSCvp54261 | SFR モジュール/7000/8000 デバイスの監査 syslog で UDP ではなく TCP が syslog 通信に使用される |
| CSCvp55880 | Snort プロセスのダウン時にフェールクローズされた FTD でパケットがパススルーされる |
| CSCvp59864 | IP アドレスがローカルプールでスタックし、AnyConnect クライアントが切断されていても「使用中」と表示される |
| CSCvp63068 | スレッド名：CP DP SFR イベント処理のトレースバック |
| CSCvp65134 | ASA が BVI インターフェイス上の DHCP 要求パケットに応答しない |

| 不具合 ID | タイトル |
|---|---|
| CSCvp67257 | カーネルアップグレード（3.10 ～ 4.14）による USGv6 障害 |
| CSCvp70020 | 再起動後、「ssh version 1 2」が running-config に追加される |
| 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） |
| CSCvp71180 | RADIUS チャレンジを使用した MCA+AAA+OTP がチャレンジでの aggauth ハンドルの送信に失敗する |
| CSCvp72244 | CVE-2019-11815 の Cisco 8000 シリーズの評価 |
| CSCvp72412 | タイムゾーンが SYSLOG メッセージには表示されるが、ロギングバッファには表示されない |
| CSCvp73555 | ネットワーク検出の展開後に rna_networks が空になる |
| CSCvp79157 | 多数のデバイスへの同時展開の実行時に FTD/Firepower ポリシーの展開が失敗する |
| CSCvp80775 | クライアント側 WebVPN リライタでのサポートされていないランタイム JavaScript の例外処理 |
| CSCvp83687 | Firepower：ネットワークファイルのトラジェクトリグラフがロードされない |
| CSCvp84546 | ASA 9.9.2 クライアントレス WebVPN - HTML の処理時に HTML エンティティが誤って復号化される |
| CSCvq00005 | SSL 復号化 DND の保持による LINA での FTD のトレースバックとリロード |
| CSCvq00675 | Linux カーネル sas_expander.c が競合状態で任意のコードを実行... |
| CSCvq06790 | シリーズ 3 デバイスで Snort プロセスがメモリ破損でコアをダンプする |
| CSCvq08684 | 特殊文字および符号化によるポリシー展開の失敗 |
| CSCvq08767 | snort 検証での展開の失敗 - 「SMTP：SMTP mime mempool を割り当てることができませんでした（SMTP: Could not allocate SMTP mime mempool）」 |
| CSCvq11513 | トレースバック：「saml identity-provider」コマンドでマルチコンテキスト ASA がクラッシュする |
| CSCvq12411 | CSCvj98964 の修正があるにも関わらず、SCTP トラフィックにより ASA がトレースバックすることがある |
| CSCvq13442 | コンテキストを削除すると、ssh key-exchange がグローバルにデフォルトになる |

| 不具合 ID | タイトル |
|---|---|
| CSCvq16123 | Firepower ダイナミック Snort ルールが、Snort のリロードが関係する展開後に無効になる |
| CSCvq19525 | TCP_SACK の sfims の評価 |
| CSCvq21607 | CLI を使用してバックアップを復元すると、「ssl trust-point」コマンドが削除される |
| CSCvq24134 | ASA IKEv2 - フェーズ 2 のキー再生成の開始後に ASA が追加の削除メッセージを送信する |
| CSCvq25626 | バッファへのロギング時の ASAv のウォッチドッグ |
| CSCvq25912 | 6.4.0 では相関ルールアラートが動作しない |
| CSCvq26794 | 存在しない原因を含む GTP 応答メッセージがドロップされて、TID が 0 のエラーメッセージが発行される |
| 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 |
| CSCvq37902 | TID が URL としてのソースの追加に失敗する - フラットファイル |
| CSCvq39828 | 6.4.0 へのアップグレード後、packet_log テーブルへの挿入時に SFDC がクラッシュする |
| CSCvq50314 | 失敗した SSH ログイン試行が syslog 経由でエクスポートされない |
| CSCvq57710 | マネージャをアップグレードすると、Firepower プライマリ検出エンジンプロセスが終了することがある |
| CSCvq61651 | FMC での URL DB ダウンロード失敗アラート：FMC/FDM で新しい URL DB の更新が有効にならない |
| CSCvq86553 | 6.4.0 への更新後、トラフィックが期待される ACP ルールと一致しない |
| CSCvq97301 | 5525 を 6.4.0-102 から 6.4.0.4-31 にアップグレードする際に FMC GUI で致命的なエラーメッセージが表示されるが、アップグレードは完了する |

# バージョン 6.4.0.3 で解決済みの問題

表 *63* : バージョン *6.4.0.3* で解決済みの問題

| 不具合 ID | タイトル |
|---|---|
| CSCve24102 | GUI で、DHCP プールごとに最大 256 個のアドレスを設定できる必要がある |
| CSCvo68448 | 5585 プラットフォームで ASA モジュールをリロードした後、ASA が SFR モジュールを「応答なし」として報告する |
| CSCvp01542 | 証明書の場所が原因で、FMC 6.3 マルチテナンシー/ドメイン LDAPS ユーザー/グループのダウンロードに失敗する |
| CSCvp10132 | AnyConnect 接続が TCP 接続制限の超過エラーで失敗する |
| CSCvp23579 | [ネットワークファイルトラジェクトリ（Network File Trajectory）] ページのロードに毎回 90 秒かかる |
| CSCvp25570 | グループポリシー属性と FQDN が同じウィザード フローで編集されている場合、RAVPN 接続プロファイルを作成できない |
| CSCvp32659 | 6.3.0.3-69 へのアップグレード後に FDM-HA の形成に失敗する |
| CSCvp33052 | 処理されていないリソースが一時的に使用できないという問題により Firepower 8000 インターフェイスがフラップする場合がある |
| CSCvp37779 | FTD のトラブルシューティング ファイルからの show tech が不完全である |
| CSCvp46173 | サブドメイン内のインターフェイスグループまたはインターフェイスゾーンの変更によってグローバルドメインが上書きされる |
| CSCvp56910 | ヘルプページが常に英語で表示される |
| CSCvp58028 | nfm_exceptiond の natd スレッドで約 90 ～ 100% の CPU 時間が使用される |
| CSCvp66559 | 大規模な XML 応答の解析時に例外により FTD HA で展開が失敗する |
| CSCvp72601 | FMC UI：VPN ハブアンドスポークトポロジのロードに時間がかかる |
| CSCvp72770 | vFTD が Azure プラットフォームで実行されている場合に、FMC から vFTD にコピーされた BCDB ファイルが切り捨てられる |
| CSCvp75594 | FTD を実行している ASA5500-X で 6.4 にアップグレードした後に展開に失敗する |
| CSCvp94588 | HTTP ブラックリスト - ブラックリストルールが FMC から割り当て解除されて展開された場合に、センサーから削除されない |

| 不具合 ID | タイトル |
|---|---|
| CSCvp97799 | SSL ポリシーのエクスポート時に openSSL コールで CC モードにして 6.5.0-1148 にアップグレードした後、ポリシーの展開に失敗する |
| CSCvp97916 | アクティブユニットで「フェールオーバー」を 2 回実行すると、スタンバイユニットのインターフェイス設定がクリアされる |
| CSCvp98066 | CD のリセット時にフラグ [parseFailoverReqIssued] をクリアしないと、ノードを結合できない |
| CSCvq07914 | FMC 6.4.0 - ポリシー展開の失敗 - domains.conf のドメインエントリが重複している |
| CSCvq14586 | データベースの更新が失敗した場合に 600_schema/100_update_database.sh はエラーを返す必要がある |

# バージョン 6.4.0.2 で解決済みの問題

**表 *64* : バージョン *6.4.0.2* で解決済みの問題**

| 不具合 ID | タイトル |
|---|---|
| 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 |
| CSCvi63474 | 6.2.2 へのアップグレード後に ASDM を介した SFR モジュールのシステムポリシーの編集ができない |
| CSCvk06386 | ファイル ポリシー判定にかかわらず、FTD ファイルが複数の既存の接続を介して許可される |
| CSCvk14242 | FTD の sfstunnel プロセスにすでに削除されている大規模なクラウド db ファイルが保持されている |
| CSCvm70274 | tcp プロキシ：データパスでの ASA のトレースバック |
| CSCvn07452 | インライン セットをタップからインラインに切り替えると 712x デバイスが不安定になる |
| CSCvn12381 | 4140 マルチインスタンスが 4 つのインスタンスで正しくロードバランシングされない |
| CSCvn34246 | AC ポリシー エディタのロードに時間がかかりすぎるためロード インジケータが必要になる |
| CSCvn45750 | 3D デバイスへの展開時に FMC 監査ログに管理者とシステムのみがオーナーとして表示される（GUI/SYSLOG） |

| 不具合 ID | タイトル |
|---|---|
| CSCvn46390 | Lina msglayer パフォーマンスの改善：ポートホットフィックス BO |
| CSCvn57284 | FTD でサポートされていない EC カーブ x25519 |
| CSCvn74112 | FTDv には vmxnet3 と ixgbevf インターフェイスが混在した初期起動の設定がない |
| CSCvn75368 | キー再生成中に IPsec VPN が断続的にダウンする |
| 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 |
| CSCvo02097 | ASA クラスタを 9.10.1.7 にアップグレードするとトレースバックが発生する |
| CSCvo17775 | 新しいサブインターフェイスが追加され、「ac-address auto」が有効になると EIGRP が中断する |
| CSCvo23366 | 適応型プロファイリングの設定ファイルが破損しているため展開に失敗した |
| CSCvo24145 | 大きな firewall_rule_cache テーブルによる ids_event_alerter の高メモリ使用率 |
| CSCvo33348 | 非標準ポートの Mysql トラフィックが正しく分類されない |
| CSCvo33851 | ngfw.properties が空の場合に ngfwManager が開始されない |
| 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 |
| CSCvo45209 | FTD - クラスタ：クラスタに新しいユニットを追加するとトラフィックのドロップが発生する場合がある |
| CSCvo45799 | Cisco Firepower Threat Defense ソフトウェアのコマンドインジェクションの脆弱性 |
| 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 |
| CSCvo50168 | 監査ログの設定の失敗によりシステム設定が編集できなくなる |
| CSCvo56836 | スケール：500 以上のデバイスを使用すると UMS によって UI がハングする（特に展開時） |
| CSCvo58847 | トンネル置き換えシナリオが原因で発生した高 IKE CPU に対処するための機能強化 |
| CSCvo60580 | 「show inventory」コマンド発行時の ASA のトレースバックとリロード |

| 不具合 ID | タイトル |
|---|---|
| CSCvo60862 | アクセス コントロール ポリシー編集時の内部エラー |
| CSCvo62031 | IKE デバッグ実行中の ASA のトレースバックとリロード |
| CSCvo62060 | FMC が大量のデバイスを管理しているときにテレメトリが送信されない |
| CSCvo66920 | 機能強化：重複するリモート プロキシのカウンタを追加 |
| CSCvo70545 | Cisco Firepower Detection Engine の RTF/RAR マルウェアおよびファイルポリシーバイパスの脆弱性 |
| CSCvo72179 | SMB ではリモート ストレージ設定でドット（.）を使ったバージョン文字列の設定を許可する必要がある |
| CSCvo72462 | ルールを復号しないとトラフィックが中断する |
| CSCvo74745 | 多数の連続 URL ルックアップ（30M 超）生成後のクラウド エージェントのコア化 |
| CSCvo83194 | Cisco Firepower Threat Defense ソフトウェアのマルチインスタンスコンテナのエスケープにおける脆弱性 |
| CSCvo86038 | flow-offloaded フローでの同時 FIN が接続の失効につながる |
| CSCvo88188 | App-ID 条件を持つ SSL ルールが復号機能を制限する可能性がある |
| CSCvo88306 | 重複するルールがあると NAT ルールが誤った順序で適用される可能性がある |
| CSCvo89224 | 展開用のデバイス リストの取得で 10 分後に FMC がタイムアウトになる |
| CSCvo90550 | Firepower の推奨事項では GID 3 の IPS ルールが有効にならない |
| CSCvo90805 | Cisco Firepower Management Center RSS のクロスサイト スクリプティングの脆弱性 |
| CSCvp03498 | FMC での ISE 接続のヘルスモニターリングのオプション。 |
| CSCvp07143 | DTLS 1.2 および AnyConnect oMTU |
| CSCvp14576 | ENH：FTD でのポート ブロック割り当てを設定するオプション |
| 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 |

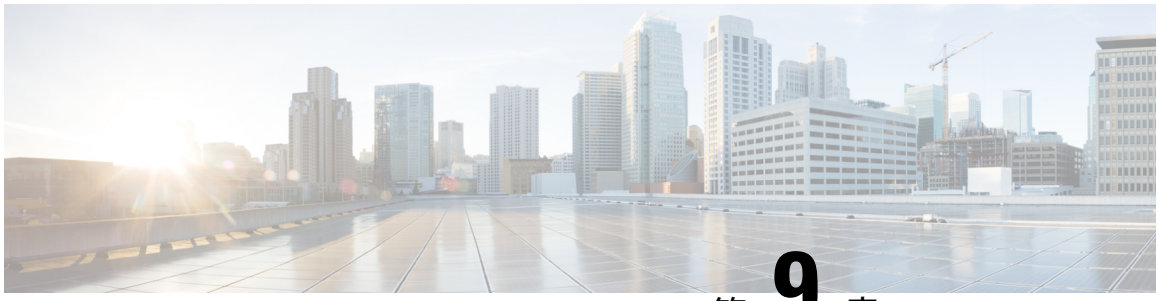
| 不具合 ID | タイトル |
|---|---|
| CSCvp21837 | FMC（6.5.0 より前）を経由することなく、FTD が URL ルックアップを直接実行できるようにする |
| CSCvp24728 | FTD によってランダムな SGT タグが追加される |
| CSCvp24787 | （snort）HTTPS 経由時にファイルが検出されなくなる（SSL 再署名） |
| CSCvp25583 | FMC GUI を介して BGP に OSPF を再配布すると FTD によって自動的にメトリックが 0 に設定される |
| CSCvp27263 | 6.5.0 より以前の Cisco Firepower Management Center における ClamAV の複数の脆弱性 |
| CSCvp29692 | ポリシー展開失敗後からのロールバック後に FIPS モードが無効になる |
| CSCvp35359 | 明示的な UPN と暗黙的な UPN が一致しないと FMC-ISE 統合が機能しない |
| 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 |
| CSCvp43474 | REST API クエリ /api/fmc_config/v1/domain/UUID/devices/devicerecords が失敗する |
| CSCvp43536 | アップグレードした FMC デバイスで、正常に展開された後も FXOS デバイスがダーティとして表示される |
| CSCvp54634 | 不明瞭な DND を使用しているときに正しくないルールが一致する |
| CSCvp58310 | pxgrid 機能の統合、接続のハング、curl のハングの問題 |
| CSCvp66222 | Cisco Firepower Detection Engine の RTF/RAR マルウェアおよびファイルポリシーバイパスの脆弱性 |
| 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 |
| CSCvp75098 | Flex Config ポリシーの展開中における展開警告メッセージの誤認 |
| CSCvp78197 | ポリシーの展開による ospf ネイバーの削除および追加 |
| CSCvp81967 | 管理対象デバイスが 500 以上ある場合に FMC のデバイス管理ページのロードが遅くなる |
| CSCvp82945 | NAT ポリシーの適用がエラーの重複で失敗する |
| CSCvp96934 | 重複する NAT を含むエラー メッセージがクリアされ実行可能であることを確認する |

| 不具合 ID | タイトル |
|---|---|
| CSCvq07573 | 6.4 へのアップグレード後、FMC のグローバルな事前展開フェーズに時間がかかる |
| CSCvq09209 | ポリシーの展開が snort 検証失敗のエラーで失敗した（memcap に指定された値が正しくない） |
| CSCvq34224 | マネージャをアップグレードすると、Firepower プライマリ検出エンジンプロセスが終了する |

# バージョン 6.4.0.1 で解決済みの問題

**表 *65 :* バージョン *6.4.0.1* で解決済みの問題**

| 不具合 ID | タイトル |
|---|---|
| CSCvh51853 | セッション プリプロセッサによるランダムなパケット ドロップ |
| CSCvp59960 | リテラル（ユーザーまたはシスコが作成したもの）を含むネットワーク グループでネットワーク検出が機能しない |



第 9 章

# 既知の問題

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

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

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

• バージョン 6.4.0 の既知の問題 （145 ページ）

# バージョン 6.4.0 の既知の問題

**表 *66* : バージョン *6.4.0* の既知の問題**

| 不具合 ID | タイトル |
|---|---|
| CSCvo00852 | FTDv ESXi 12 コアおよび FTDv KVM 12 コア プラットフォームで Lina CPU が低くトラフィックが失われる |
| CSCvo03589 | アプリケーション エージェントのハート ビートが、MI のシナリオで失われる可能性があります |
| CSCvo40478 | FMC ダッシュボードに FMC の最新の製品更新として誤った値が表示される |
| CSCvo80725 | 「エラー：ip_multicast_ctl によるチャネルの取得に失敗（ERROR: ip_multicast_ctl failed to get channel）」により vFTD 6.4 が OSPF 隣接関係を確立できない |

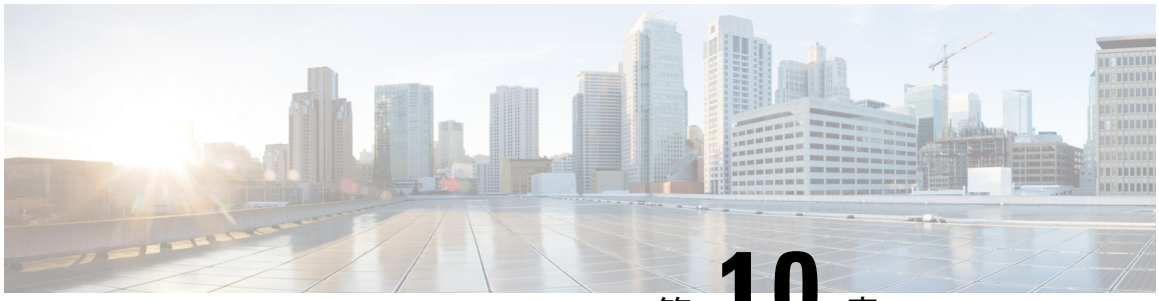
| 不具合 ID | タイトル |
|---|---|
| CSCvp06568 | 6.4 FMC によって管理されている 6.3 FTD の syslog で NAP ポリシー/SSL ポリシー名が不明 |
| CSCvp19669 | FDM イベントにユーザーが正しく表示されない |
| CSCvp21403 | 検証：データ プレーン：管理アクセスが RA-VPN ポート コリジョンを処理しない |
| CSCvp23703 | FTD で最初のブート スクリプト S97compress-client-resources が無応答で失敗した |
| CSCvp25570 | グループポリシー属性と FQDN が同じウィザード フローで編集されている場合、RAVPN 接続プロファイルを作成できない |
| CSCvp29817 | TempID を RealID に変換するときにログイン履歴の更新に失敗する（ID ごとに 1 個のログ、履歴が失われる） |
| CSCvp30194 | ASA SFR：IPS を使用して ACP をインポートしようとすると「SFO インポート中のエラー：コンテナをロードできません（Error importing SFO: Unable to load container）」が表示される |
| CSCvp33797 | FMC 上でセッションのあるユーザーが、ユーザー情報を AD からダウンロードした後に正常に更新されない |
| CSCvp37229 | ポリシー レイヤの「マイ チェンジ（My Changes）」レイヤから有効にした場合、一部のプロセッサが有効にならない |
| CSCvp45752 | カスタムアプリケーションをサブドメインに追加した場合、古いバージョンの登録済みデバイスで snort が再起動しない |
| CSCvp47260 | 日本語版でトラブルシューティング ファイルの生成が停止する |
| CSCvp47535 | 新しく追加したアプリケーション プロトコルを [ホスト（Hosts）] に表示できない |
| CSCvp48523 | 変更されたユーザーがアクセス ポリシーに正しく反映されない |
| CSCvp48525 | [タスクの詳細（Task details）] でスケジュールしたタスクを編集できない |
| CSCvp48534 | 侵入ルールにカテゴリを追加できない |
| CSCvp48545 | 日本語名のアラートを作成できない |
| CSCvp48565 | VPN トラブルシューティング ログのセットアップに異常に長い時間がかかる |
| CSCvp48583 | [IPv6 DAD] チェックボックスがデフォルトでオンになっている |

| 不具合 ID | タイトル |
|---|---|
| CSCvp56916 | S2S VPN ウィザードに、事前設定された使用可能な証明書がないことが示される |
| CSCvp56951 | FDM/FTDvirtual が「ignore-ipsec-keyusage」 flexconfig オブジェクトをサポート/展開できない |
| CSCvp57096 | メッセージ フィールドに NULL エントリがある ids_event_msg_map テーブルが原因で 6.4.0 へのアップグレードが失敗する場合がある |
| CSCvp59960 | リテラル（ユーザーまたはシスコが作成したもの）を含むネットワーク グループでネットワーク検出が機能しない |
| CSCvq29993 | SSL ポリシーにより 6.4.0-102 2140 で 1550 ブロックと 9472 ブロックが枯渇し、回復しない |
| CSCvq33956 | 展開プロセス（AQS サブグループ）のメモリ割り当てを最適化して大規模なポリシー展開を可能にする |
| CSCvq36298 | アップグレード後に ASAv/FTDv の MTU サイズを変更できない |
| CSCvq78471 | BVI とその DHCP プールを同時に削除するとポリシーの展開が失敗する |
| CSCvr01675 | 複数のシスコ製品での Snort HTTP 検出エンジンのファイルポリシーバイパスの脆弱性 |
| CSCvr35854 | Apache HTTP サーバーの URL 正規化のサービス拒否攻撃に対する脆弱性 |
| CSCvr35855 | Apache HTTP サーバーの mod_http2 Use-After-Free のサービス拒否攻撃に対する脆弱性 |
| CSCvr35856 | Apache HTTP サーバーの mod_auth_digest 競合状態のアクセス制御バイパス |
| CSCvr57468 | RunQuery は Java 開発キット 13 との互換性がない |
| CSCvs05066 | Snort ファイルのメモリプールの破損によりパフォーマンスが低下し、プロセスが失敗する |
| CSCvs24215 | SSL キー再生成を無効にする Firepower Device Manager（FDM）オプションが設定に反映されない |
| CSCvs37065 | /ngfw/var/sf/fwcfg/interface_info.conf ファイルにデータがないため、Snort がクラッシュする |
| CSCvs50931 | SRU の後でポリシーの展開が失敗する |
| CSCvs56923 | SQL クライアントが外部データベースアクセスを使用して FMC にクエリを実行できない |

| 不具合 ID | タイトル |
|---|---|
| CSCvs61881 | FTD 上の AnyConnect の証明書マッピングが機能しなくなった |
| CSCvs74586 | Firepower FTD トランスペアレントが非 IP パケットを復号化しない |
| CSCvs82829 | Anyconnect 設定がサイト間 VPN トンネルに追加されるとコールが失敗する |
| CSCvs88186 | SID で byte_extract と byte_math で同じ変数名を使用すると、snort 検証が中断される |
| CSCvt01763 | フローがブルートフォース失敗としてマークされている場合、アプリケーション分類が再試行されない |
| CSCvt03557 | GUI 上に設定された時間/タイムゾーンが仮想 Firepower Management Center 上で矛盾している |
| CSCvt06666 | 6.3.0.4 から 6.4 へのアップグレードが失敗した後で SFR httpsd プロセスがダウンする |
| CSCvt16642 | FMC がリモートの syslog サーバーに対して一部の監査メッセージを送信していない |
| CSCvt16723 | ngfw-onbox ログのログローテーションが想定しているログサイズで実行されていない |
| CSCvt18051 | dets ファイルが破損している場合、RabbitMQ がクラッシュし続ける |
| CSCvt20235 | Firepower 4100 シリーズのすべての FTW インターフェイスが同時にリンクフラップするが、まれにしか発生しない |
| CSCvt21986 | インスタンス間での Snort と Lina のコアの割り当てに一貫性がない |
| CSCvt34894 | Snort がメモリを消費し、ブロックが枯渇する |
| CSCvt35233 | DAQ モジュール process_snort_verdict 判定ブラックリストからの過剰なロギング |
| CSCvt35730 | 2 番目のトンネルに重複する暗号 ACL がある場合の FDM 展開エラー |
| CSCvt37745 | アクティブからスタンバイへセカンダリが復帰する間にトレースバックする |
| CSCvt42955 | SID 26932 誤検出 が NTP ではなく QUIC でトリガーされる |
| CSCvt52607 | SSL HW モードのフローテーブルメモリの使用率を引き下げて Snort が D 状態になる確率を低減する |
| CSCvt56923 | FTD の手動による証明書の登録が、組織の件名フィールドの "&"（アンパサンド）が原因で失敗する |

| 不具合 ID | タイトル |
|---|---|
| CSCvt62147 | プロセス名 LINA で ASA がトレースバックし、リロードする |
| CSCvt63407 | FTD 6.4.0.7 を実行している FP 2000 がプロセス名 LINA でトレースバックし、リロードする |
| CSCvt64696 | AAA RADIUS サーバーの接続障害 |
| CSCvt66136 | CC モードを使用した 6.4.0 から 6.4.0.9 へのアップロードにより httpsd.conf に誤った設定が発生する |
| CSCvt66875 | AppId は UltraSurf にトンネリングされた IP ではなく、プロキシ IP をキャッシュする |
| CSCvt67832 | ロックの競合が原因で、Lina スレッドで FTD がトレースバックし、リロードする |
| CSCvt68131 | スレッド「IKEv2 Mgd Timer Thread」で FTD がトレースバックし、リロードする |
| CSCvt70854 | 6.6.0-90： [Firepower 1010] メモリ不足のため、SRU の更新中に tomcat が再起動する |
| CSCvt70866 | sfipproxy がセカンダリ FMC のリスナーのバインドに失敗することがある |
| CSCvt72683 | FP 8130 での NAT ポリシーの展開後の NAT ポリシーの設定が表示されない |
| CSCvt80126 | CLI の「show asp table socket 18421590 det」で ASA がトレースバックし、リロードする |
| CSCvt80172 | CVE-2017-11610 に対処するには、スーパーバイザソフトウェアをアップグレードする必要がある |
| CSCvt86599 | Orac のレプリケーションコードにおける複数の SQL インジェクションの脆弱性 |
| CSCvt86906 | リダイレクトオプションを使用すると、Stunnel 5.00 ～ 5.13 が |
| CSCvt87064 | li の WebCore/platform/network/soup/SocketStreamHandleImplSoup.cpp |
| CSCvu32449 | FDM：AnyConnect「名前が重複しているため、検証に失敗しました：（Validation failed due to duplicate name:）」 |
| CSCvu43355 | QOS 機能での FTD Lina のトレースバックとリロード |
| CSCvu44697 | Firepower 4100/9300：show tech の収集中に Fail-to-wire（FTW）EPM ポートがリンクフラップする |
| CSCvu46584 | 2.64.2 までの GNOME glib-networking で、GTlsCli の導入 |

| 不具合 ID | タイトル |
|---|---|
| CSCvu53481 | HA 設定の同期にかかる時間が 1 時間を超えるため、FTD のアップグレードが失敗する |
| CSCvu56286 | FDM：進行中のトラフィックに対して HA フェールオーバーを実行した後に新しいファイアウォールセッションが作成される |
| CSCvu61711 | 「内部エラーが発生しました。（An internal error occurred.）」により、FMC が地理位置情報を含む ACL ルールを追加できない |
| CSCvu70529 | snort のリロード時にバイナリルール（SO ルール）がロードされない |
| CSCvu85127 | 同じ UUID のデバイスが接続しようとしている場合、展開できない |
| CSCvv00254 | ドロップ予定だったイベントが生成されると、一部のイベントデータが無効になる |



第 10 章

# サポートが必要な場合



## オンラインリソース

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

- マニュアル http://www.cisco.com/go/threatdefense-64-docs
- シスコ サポートおよびダウンロード サイト：https://www.cisco.com/c/en/us/support/index.html
- Cisco Bug Search Tool：https://tools.cisco.com/bugsearch/
- シスコ通知サービス：https://www.cisco.com/cisco/support/notifications.html

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

## シスコへのお問い合わせ

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

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