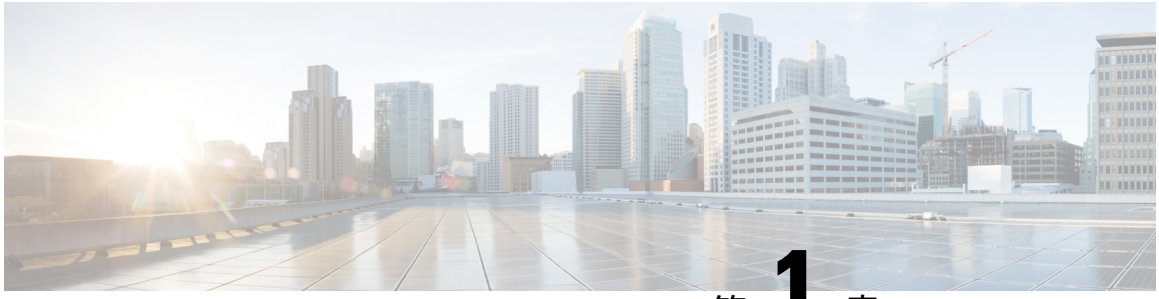
# Cisco Firepower バージョン 6.6 リリースノート

**初版**：2020 年 4 月 6 日

**最終更新**：2023 年 6 月 23 日


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

# 目 次



第 1 章

# ようこそ

このドキュメントには、Cisco Firepower Threat Defense、Firepower Management Center のバージョン 6.6 Firepower Device Manager、および Cisco Firepower 従来型デバイス（NGIPSv、ASA with FirePOWER Services）のリリース情報が含まれています。

FDM との Cisco Defense Orchestrator（CDO）については、「Cisco Defense Orchestrator の新機能」も参照してください。



## リリース日

シスコは、更新版ビルドを適宜リリースしています。ほとんどの場合、各プラットフォームの最新のビルド番号のみが、シスコ サポートおよびダウンロード サイト で入手可能です。最新のビルドを使用することを強くお勧めします。以前のビルドをダウンロードした場合は使用しないでください。詳細については、新しいビルドで解決されたバグ （96 ページ）を参照してください。

**表 *1*：バージョン *6.6* のリリース日**

| バージョン | ビルド | 日付 | プラットフォーム |
|---|---|---|---|
| 6.6.7.1 | 54 | 2023 年 1 月 26 日 | すべて |
| 6.6.7 | 223 | 2022 年 7 月 14 日 | すべて |
| 6.6.5.2 | 14 | 2022 年 3 月 24 日 | すべて |

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

# 推奨リリース

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

また、新機能ガイドにも推奨リリースを示します。

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

### 古いアプライアンスの推奨リリース

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

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

# シスコとのデータの共有

次の機能はシスコとデータを共有します。

### Cisco Success Network

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

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

### Cisco Support Diagnostics

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

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

### Web 分析

Web分析は、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提供します。

デフォルトで登録されていますが、初期設定の完了後にいつでも登録を変更できます。広告ブロッカーは Web 分析をブロックできるため、登録したままにする場合は、Cisco アプライアンスのホスト名/IP アドレスの広告ブロックを無効にしてください。

# 支援が必要な場合

### オンラインリソース

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

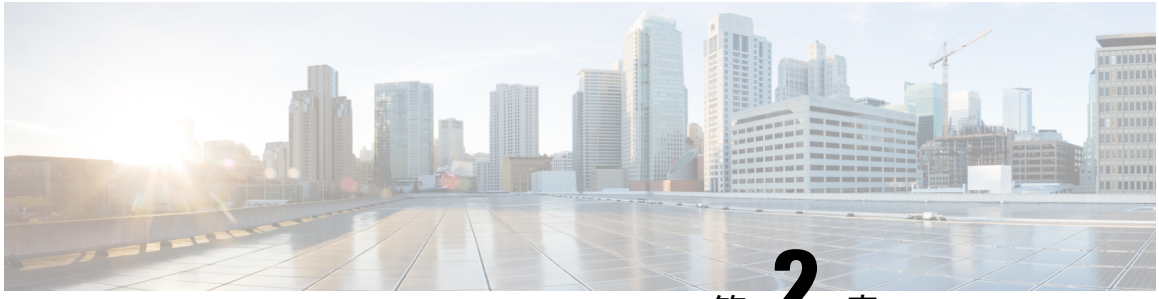
- マニュアル：http://www.cisco.com/jp/go/threatdefense-66-docs
- シスコ サポートおよびダウンロード サイト：https://www.cisco.com/c/en/us/support/index.html
- シスコ バグ検索ツール：https://tools.cisco.com/bugsearch/
- シスコ通知サービス：https://www.cisco.com/cisco/support/notifications.html

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

### シスコへのお問い合わせ

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

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



第 2 章

# システム要件

このドキュメントでは、バージョン 6.6 のシステム要件を記載します。



## FMC プラットフォーム

FMC 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します。FMC とのデバイスの互換性については、「デバイス管理 （9 ページ）」を参照してください。一般的な互換性情報については、Cisco Secure Firewall Management Center 互換性ガイド を参照してください。

### FMC ハードウェア

バージョン 6.6 は次の FMC ハードウェアをサポートします。

- FMC 1600、2600、4600
- FMC 1000、2500、4500
- FMC 2000、4000

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

### FMCv

バージョン 6.6 はパブリッククラウドに加えて、プライベートクラウドやオンプレミスクラウドでの FMCv 導入をサポートします。

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

表 *2:* バージョン *6.6 FMCv* プラットフォーム

| プラットフォーム | 管理対象デバイス | | ハイ アベイラビリティ |
|---|---|---|---|
| | 2、10、25 | 300 | |
| **パブリック クラウド** | | | |
| Amazon Web Services（AWS） | 対応 | — | — |
| Microsoft Azure | 対応 | — | — |
| **オンプレミス/プライベートクラウド** | | | |
| カーネルベース仮想マシン（KVM） | 対応 | — | — |
| VMware vSphere/VMware ESXi 6.0、6.5、または 6.7 | 対応 | 対応 | — |

### クラウド提供型の管理センター

Cisco クラウド提供型 Firewall Management Center は、複数のシスコ セキュリティ ソリューションの管理を統合する Cisco Defense Orchestrator（CDO）プラットフォームを通して提供されます。クラウド提供型 Firewall Management Center にはバージョンがないため、機能の更新はシスコが行います。

顧客展開型の管理センターは、仮想プラットフォームの場合でも、オンプレミス FMC と呼ばれることが多いことに注意してください。

（注） クラウド提供型の Management Center では、バージョン 6.6 デバイスを管理できません。

# デバイスプラットフォーム

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。デバイスの管理方法については、「デバイス管理 （9 ページ）」を参照してください。一般的な互換性情報については、Cisco Secure Firewall Threat Defense 互換性ガイド または Cisco Firepower Classic Device 互換性ガイド を参照してください。

### FTD ハードウェア

バージョン 6.6 FTD のハードウェアは、多様なスループット、拡張性、およびフォームファクタに対応します。

表 *3* : バージョン *6.6 FTD* ハードウェア

| プラットフォーム | FMC 互換 | | FDM 互換 | | 注記 |
|---|---|---|---|---|---|
| | お客様が導入 | クラウド提供型 | FDM のみ | FDM + CDO | |
| Firepower1010、1120、1140、1150 | 対応 | — | 対応 | 対応 | — |
| Firepower 2110、2120、2130、2140 | 対応 | — | 対応 | 対応 | — |
| Firepower 4110、4120、4140、4150<br>Firepower 4112、4115、4125、4145<br>Firepower 9300：SM-24、SM-36、SM-44 モジュール<br>Firepower 9300：SM-40、SM-48、SM-56 モジュール | 対応 | — | 対応 | 対応 | FXOS 2.8.1.15 以降のビルドが必要です。<br>最新のファームウェアを推奨します。Cisco Firepower 4100/9300 FXOS ファームウェアアップグレードガイドを参照してください。 |
| ASA 5508-X、5516-X<br>ASA 5525-X、5545-X、5555-X | 対応 | — | 対応 | 対応 | ASA 5508-Xおよび5516-Xデバイスには、ROMMON の更新が必要な場合があります。Cisco Secure Firewall ASA および Secure Firewall Threat Defense 再イメージ化ガイドを参照してください。 |
| ISA 3000 | 対応 | — | 対応 | 対応 | ROMMON の更新が必要な場合があります。Cisco Secure Firewall ASA および Secure Firewall Threat Defense 再イメージ化ガイドを参照してください。 |

### FTDv

バージョン 6.6 は、以下の FTDv 導入をサポートしています。サポートされているインスタンス、スループット、およびその他のホスティング要件の詳細については、『Cisco Secure Firewall Threat Defense Virtual Getting Started Guide.』を参照してください。

表 *4 :* バージョン *6.6 FTDv* プラットフォーム

| デバイスのプラットフォーム | FMC 互換 | | FDM 互換 | |
|---|---|---|---|---|
| | お客様が導入 | クラウド提供型 | FDM のみ | FDM + CDO |
| **パブリック クラウド** | | | | |
| Amazon Web Services（AWS） | 対応 | — | 対応 | 対応 |
| Microsoft Azure | 対応 | — | 対応 | 対応 |
| **オンプレミス/プライベートクラウド** | | | | |
| カーネルベース仮想マシン（KVM） | 対応 | — | 対応 | 対応 |
| VMware vSphere/VMware ESXi 6.0、6.5、または 6.7 | 対応 | — | 対応 | 対応 |

### Firepower Classic：ASA FirePOWER、NGIPSv

Firepower Classic デバイスでは、次のプラットフォームで NGIPS ソフトウェアが実行されます。

- ASA デバイスでは、NGIPS ソフトウェアを個別のアプリケーション（ASA FirePOWER モジュール）として実行できます。ASA ファイアウォールポリシーが適用された後に、トラフィックがモジュールに送信されます。 ASA と ASA FirePOWER のバージョン間には広い互換性がありますが、アップグレードすることで、新機能と解決された問題を活用できます。
- NGIPSv は、仮想環境でソフトウェアを実行します。

表 *5 :* バージョン *6.6 NGIPS* プラットフォーム

| デバイスのプラットフォーム | FMC の互換性 | ASDM の互換性 | 注記 |
|---|---|---|---|
| ASA 5508-X、5516-X | 対応 | ASDM 7.14(1) が必要です。 | ASA 9.5(2) ～ 9.16(x) が必要です。<br>ROMMON の更新が必要な場合があります。Cisco Secure Firewall ASA および Secure Firewall Threat Defense 再イメージ化ガイドを参照してください。 |
| ASA 5525-X、5545-X、5555-X | 対応 | ASDM 7.14(1) が必要です。 | ASA 9.5(2) ～ 9.14(x) が必要です。 |
| ISA 3000 | 対応 | ASDM 7.14(1) が必要です。 | ASA 9.5(2) ～ 9.16(x) が必要です。<br>ROMMON の更新が必要な場合があります。Cisco Secure Firewall ASA および Secure Firewall Threat Defense 再イメージ化ガイドを参照してください。 |
| NGIPSv | 対応 | — | VMware vSphere/VMware ESXi 6.0、6.5、または 6.7 が必要です。<br>サポート対象のインスタンスやスループットをはじめとしたホスティング要件については、 Cisco Firepower NGIPSv Quick Start Guide for VMware を参照してください。 |

# デバイス管理

デバイスモデルとバージョンに応じて、次のデバイス管理方法をサポートしています。

### FMC

すべてのデバイスは、FMC によるリモート管理に対応しています。FMC では管理対象デバイスと同じまたはそれ以降のバージョンを実行する必要があります。これは、以下を意味します。

- より新しい FMC でより古いデバイスを管理できます。通常は、メジャーバージョンをいくつか遡ることができます。ただし、導入環境全体を常に更新することをお勧めします。多くの場合、新機能の使用や問題解決の適用には、FMC とその管理対象デバイスの両方で最新リリースが必要になります。

- FMC よりも新しいバージョンのデバイスをアップグレードすることはできません。メンテナンス（3 桁）リリースの場合でも、最初に FMC をアップグレードする必要があります。

ほとんどの場合、旧バージョンのデバイスは FMC のメジャーバージョンまたはメンテナンスバージョンに直接アップグレードできます。ただし、対象バージョンがデバイスでサポートされていても、直接アップグレードできない旧バージョンのデバイスを管理している場合があります。リリース固有の要件については、を参照してください。アップグレードする最小バージョン （46 ページ）。

表 *6 : FMC* : デバイスの互換性

| FMC バージョン | 管理可能な最も古いデバイスバージョン |
|---|---|
| 7.3 | 6.7 |
| 7.2 | 6.6 |
| 7.1 | 6.5 |
| 7.0 | 6.4 |
| 6.7 | 6.3 |
| 6.6 | 6.2.3 |
| 6.5 | 6.2.3 |
| 6.4 | 6.1 |
| 6.3 | 6.1 |
| 6.2.3 | 6.1 |
| 6.2.2 | 6.1 |
| 6.2.1 | 6.1 |
| 6.2 | 6.1 |
| 6.1 | 5.4.0.2/5.4.1.1 |
| 6.0.1 | 5.4.0.2/5.4.1.1 |
| 6.0 | 5.4.0.2/5.4.1.1 |

| FMC バージョン | 管理可能な最も古いデバイスバージョン |
|---|---|
| 5.4.1 | 5.4.1（ASA-5506-X シリーズ、ASA5508-X、および ASA5516-X の ASA FirePOWER）。<br>5.3.1（ASA5512-X、ASA5515-X、ASA5525-X、ASA5545-X、ASA5555-X、および ASA-5585-X シリーズの ASA FirePOWER）。<br>5.3.0（Firepower 7000/8000 シリーズおよびレガシーデバイス）。 |

### FDM

FDM を使用すると、単一の FTD デバイスをローカルに管理できます。

必要に応じて、FMC の代替策として、Cisco Defense Orchestrator（CDO）を追加し、複数の FTD デバイスをリモートで管理します。一部の構成では引き続き FDM が必要ですが、CDO を使用することで、展開したすべての FTD を通して一貫したセキュリティポリシーを確立して維持できます。

### ASDM

ASDM を使用して、ASA デバイス上の個別のアプリケーションである単一の ASA FirePOWER モジュールをローカルで管理できます。ASA ファイアウォールポリシーが適用された後に、トラフィックがモジュールに送信されます。新しいバージョンの ASDM では、新しいバージョンの ASA FirePOWER モジュールを管理できます。

# ブラウザ要件

### ブラウザ

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

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

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

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

### ブラウザの設定と拡張

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

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

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

### 画面解像度

| インターフェイス | 最小解像度 |
|---|---|
| FMC | 1280 X 720 |
| FDM | 1024 X 768 |
| ASA FirePOWER module を管理している ASDM | 1024 X 768 |
| Firepower 4100/9300 用 Firepower Chassis Manager | 1024 X 768 |

### セキュア通信

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

自己署名証明書の置き換えを開始する手順は、次のとおりです。

- FMC：**[システム（System）]**>**[設定（Configuration）]**を選択し、[HTTPS証明書（HTTPS Certificates）] をクリックします。
- FDM：[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サーバー（Management Web Server）] タブをクリックします。

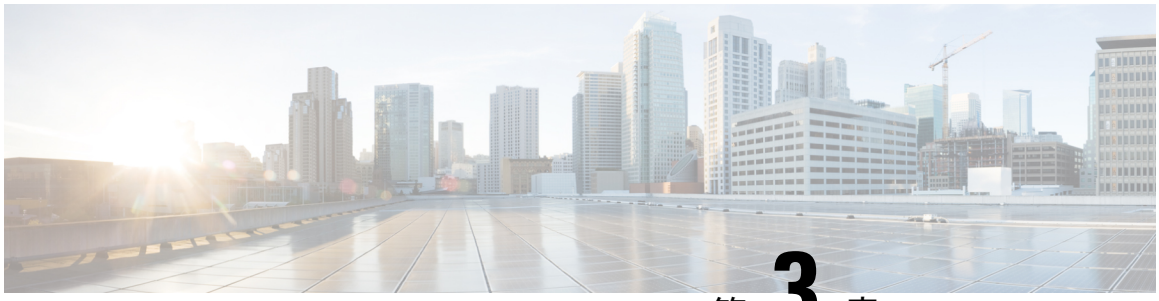
詳しい手順については、オンラインヘルプまたはご使用の製品のコンフィギュレーション ガイドを参照してください。

（注） 自己署名証明書を置き換えない場合は、次の手順を実行します。

- Google Chrome は、画像、CSS、JavaScript などの静的コンテンツをキャッシュしません。これにより、特に低帯域幅環境では、ページの読み込み時間が長くなります。
- Mozilla Firefox は、ブラウザの更新時に自己署名証明書を信頼しなくなる場合があります。この場合は Firefox を更新できますが、一部の設定が失われることに注意してください。Mozilla の Firefox 更新サポートページを参照してください 。

### 監視対象ネットワークからの参照

多くのブラウザでは、デフォルトで Transport Layer Security（TLS）v1.3 が使用されています。暗号化されたトラフィックを処理するために SSL ポリシーを使用していて、モニター対象ネットワーク内のユーザーが TLS v1.3 を有効にしてブラウザを使用している場合、TLS v1.3 をサポートする Web サイトのロードに失敗することがあります。詳細については、『Failures loading websites using TLS 1.3 with SSL inspection enabled』というタイトルのソフトウェアアドバイザリを参照してください。



第 3 章

# 特長と機能

このドキュメントでは、バージョン6.6の新機能と廃止された機能について説明します。また、アップグレードによる影響についても言及します。 Cisco Defense Orchestrator（CDO）の導入については、Cisco Defense Orchestrator の新機能 を参照してください。

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



# FMC バージョン 6.6 の新機能

新しい FMC で古いデバイスを管理できますが、常に環境全体を更新することを推奨します。新しいトラフィック処理機能では、通常は FMC とデバイスの両方で最新のリリースが必要です。 デバイスが明らかに関与していない機能（Web インターフェイスの外観の変更、クラウド統合）では、FMC の最新バージョンのみを必須条件としているにもかかわらず、それが保証されない場合があります。このドキュメントでは、バージョンの要件が標準で想定される条件から逸脱している場合は明示しています。

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

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

## 新機能

表 *7: FMC* バージョン *6.6.3* の新機能

| 新機能 | 説明 |
|---|---|
| アップグレードがスケジュールされたタスクを延期する。 | **アップグレードの影響。**<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 6.6.3 以降を実行している Firepower アプライアンスでサポートされています。バージョン 6.4.0.10 以降のパッチからアップグレードする場合を除き、バージョン 6.6.3 へのアップグレードはサポートされません。 |

| 新機能 | 説明 |
| --- | --- |
| アプライアンス設定のリソース使用率の正常性モジュール。 | **バージョン 6.7.0 のアップグレードの影響。**<br>バージョン 6.6.3 では、デバイスのメモリ管理が改善され、新しい正常性モジュールであるアプライアンス設定のリソース使用率が導入されています。<br>モジュールは、展開された設定のサイズに基づき、デバイスのメモリが不足するリスクがある場合にアラートを出します。アラートには、設定に必要なメモリ量と、使用可能なメモリ量を超過した量が示されます。アラートが出た場合は、設定を再評価してください。ほとんどの場合、アクセス制御ルールまたは侵入ポリシーの数または複雑さを軽減できます。詳細については、コンフィギュレーション ガイドの「アクセス制御のベストプラクティス」を参照してください。<br>アップグレードプロセスにより、すべての正常性ポリシーにこのモジュールが自動的に追加され、有効になります。アップグレード後、正常性ポリシーを管理対象デバイスに適用して、モニタリングを開始します。<br>（注） このモジュールには、FMC と管理対象デバイスの両方に、バージョン 6.6.3 以降の 6.6.x リリース、 またはバージョン 7.0 以降が必要です。<br>バージョン 6.7 では、このモジュールのサポートが部分的および一時的に廃止されています。詳細については、バージョン 6.7 リリースノートを参照してください。バージョン 7.0 ではフルサポートが提供され、モジュールの名前が構成メモリ割り当てに変更されています。 |

表 *8 : FMC* バージョン *6.6.0* の新機能

| 新機能 | 説明 |
| --- | --- |
| **プラットフォーム** | |
| Firepower 4112 上の FTD。 | Firepower 4112 が導入されました。このプラットフォームでは、ASA 論理デバイスを展開することもできます。FXOS 2.8.1 が必要です。 |

| 新機能 | 説明 |
|---|---|
| AWS の展開用の大型のインスタンス。 | **アップグレードの影響。**<br>FTDv for AWS により、次の大型のインスタンスのサポートが追加されています。<br>• C5.xlarge<br>• C 5.2 xlarge<br>• C5.4xlarge<br>FMCv for AWS により、次の大型のインスタンスのサポートが追加されています。<br>• C3.4xlarge<br>• C4.4xlarge<br>• C5.4xlarge<br>AWS インスタンスタイプの既存の FMCv はすべて廃止になりました（c3.xlarge、c3.2xlarge、c4.xlarge、c4.2xlarge）。アップグレードする前に、サイズを変更する必要があります。詳細については、FMCv には 28 GB の RAM が必要 （52 ページ） を参照してください。 |
| クラウドベースの FTDv 展開の自動スケール。 | AWS 自動スケール/Azure 自動スケールのサポートが導入されました。<br>クラウドベースの展開におけるサーバーレス インフラストラクチャでは、キャパシティのニーズに基づいて、自動スケールグループ内の FTDv インスタンスの数が自動的に調整されます。これには、管理側の FMC との自動登録/登録解除が含まれています。<br>サポートされているプラットフォーム：FTDv for AWS、FTDv for Azure |
| **Firepower Threat Defense**：**デバイス管理** | |
| DHCP を使用した初期管理インターフェイスの IP アドレスの取得。 | Firepower 1000/2000 シリーズと ASA-5500-X シリーズのデバイスの場合、管理インターフェイスはデフォルトで DHCP から IP アドレスを取得するようになりました。この変更により、既存のネットワーク上に新しいデバイスを簡単に展開できるようになりました。<br>この機能は、論理デバイスを展開するときに IP アドレスを設定する Firepower 4100/9300 シャーシではサポートされていません。また、FTDv や ISA 3000 でもサポートされていません。これらについては、引き続きデフォルトで 192.168.45.45 になります。<br>サポートされているプラットフォーム：Firepower 1000/2000 シリーズ、ASA-5500-X シリーズ |

| 新機能 | 説明 |
|---|---|
| CLI での MTU 値の設定。 | FTD CLI を使用して、FTD デバイスインターフェイスの MTU（最大伝送単位）値を設定できるようになりました。デフォルト値は 1500 バイトです。MTU の最大値は次のとおりです。<br>• 管理インターフェイス：1500 バイト<br>• イベントインターフェイス：9000 バイト<br>新しい FTD CLI コマンド： **configure network mtu**<br>変更された FTD CLI コマンド：**mtu-event-channel** キーワードと **mtu-management-channel** キーワードが **configure network management-interface** コマンドに追加されました。<br>サポートされるプラットフォーム：FTD |
| 内部 Web サーバーからの Threat Defense アップグレードパッケージの取得。 | FTD デバイスは、FMC からではなく、独自の内部 Web サーバーからアップグレードパッケージを取得できるようになりました。これは、FMC とそのデバイスの間の帯域幅が制限されている場合に特に役立ちます。また、FMC 上の領域も節約できます。<br>（注） この機能は、バージョン 6.6.0+ を実行している FTD デバイスでのみサポートされています。バージョン 6.6.0 へのアップグレードではサポートされておらず、FMC または従来のデバイスでもサポートされていません。<br>新規/変更されたページ：[システム（System）] > [更新（Updates）] > [更新のアップロード（Upload Update）] ボタン > [ソフトウェア更新ソースの指定（Specify Software Update Source）] オプション<br>サポートされるプラットフォーム：FTD |
| 接続ベースのトラブルシューティングの機能拡張。 | FTD CLI 接続ベースのトラブルシューティングに次の機能拡張が加えられました（デバッギング）。<br>• **debug packet-module trace**：モジュールレベルのパケットトレースを有効にするために追加されました。<br>• **debug packet-condition**：進行中の接続のトラブルシューティングをサポートするように変更されました。<br>サポートされるプラットフォーム：FTD |
| **Firepower Threat Defense**：クラスタリング | |

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

| 新機能 | 説明 |
|---|---|
| 仮想ルータと VRF-Lite。 | 複数の仮想ルータを作成して、インターフェイスグループの個別のルーティングテーブルを管理できるようになりました。各仮想ルータには独自のルーティングテーブルがあるため、デバイスを流れるトラフィックを明確に分離できます。<br><br>仮想ルータは、Virtual Routing and Forwarding の「Light」バージョンである VRF-Lite を実装しますが、この VRF-Lite は Multiprotocol Extensions for BGP（MBGP）をサポートしていません。<br><br>作成できる仮想ルータの最大数は 5 ~ 100 の範囲で、デバイスのモデルによって異なります。完全なリストについては、『Firepower Management Center Configuration Guide』の「Virtual Routing for Firepower Threat Defense」の章を参照してください。<br><br>新規/変更されたページ：[デバイス（Devices）] > [デバイス管理（Device Management）] > [デバイスの編集（edit device）] > [ルーティング（Routing）] タブ<br><br>新しい FTD CLI コマンド：**show vrf**。<br><br>変更された FTD CLI コマンド：［**vrf** *name* \| **all**］キーワードセットを CLI コマンド **clear ospf**、**clear route**、**ping**、**show asp table routing**、**show bgp**、**show ipv6 route**、**show ospf**、**show route**、**show snort counters** に追加し、必要に応じて出力が仮想ルータ情報を表示するように変更しました。<br><br>サポートされるプラットフォーム：FTD（Firepower 1010 および ISA 3000 を除く） |
| **Firepower Threat Defense**：**VPN** | |
| リモートアクセス VPN 内の DTLS 1.2。 | Datagram Transport Layer Security（DTLS） 1.2 を使用して、RA VPN 接続を暗号化できるようになりました。<br><br>FTD プラットフォーム設定を使用して、FTD デバイスが RA VPN サーバーとして動作するときに使用する最小 TLS プロトコルバージョンを指定します。また、DTLS 1.2 を指定する場合は、最小 TLS バージョンとして TLS 1.2 を選択する必要もあります。<br><br>Cisco AnyConnect セキュア モビリティ クライアント バージョン 4.7 以降が必要です。<br><br>新規/変更されたページ：[デバイス（Devices）] > [プラットフォーム設定（Platform Settings）] > [Threat Defense ポリシーの追加/編集（Add/Edit Threat Defense Policy）] > [SSL] > [DTLS バージョン（DTLS Version）] オプション<br><br>サポートされるプラットフォーム：FTD（ASA 5508-X および ASA 5516-X を除く） |

| 新機能 | 説明 |
| --- | --- |
| 複数のピアに対するサイト間 VPN IKEv2 のサポート。 | IKEv1 と IKEv2 のポイントツーポイント エクストラネットおよびハブアンドスポークトポロジのために、サイト間VPN接続にバックアップピアを追加できるようになりました。これまで設定できたのは、IKEv1 ポイントツーポイント トポロジのバックアップピアのみでした。<br><br>新規/変更されたページ：[デバイス（Devices）] > [VPN] > [サイト間（Site To Site）] > [ポイントツーポイントまたはハブアンドスポーク FTD VPN トポロジの追加または編集（Add or Edit a Point to Point or Hub and Spoke FTD VPN Topology）] > [エンドポイントの追加（Add Endpoint）] > [IP アドレス（IP Address）] フィールドで、カンマ区切りのバックアップピアがサポートされるようになりました。<br><br>サポートされるプラットフォーム：FTD |
| **セキュリティ ポリシー** | |
| セキュリティポリシーの使いやすさの向上。 | バージョン 6.6.0 を使用すると、アクセス制御ルールとプレフィルタルールが簡単に使用できるようになります。次の作業に進んでください。<br><br>• 1 回の操作（状態、アクション、ロギング、侵入ポリシーなど）で、複数のアクセス制御ルールの特定の属性を編集します。<br><br>アクセス コントロール ポリシー エディタで、関連するルールを選択し、右クリックして [編集（Edit）] を選択します。<br><br>• 複数のパラメータによってアクセス制御ルールを検索します。<br><br>アクセス コントロール ポリシー エディタで、[ルールの検索（Search Rules）] テキストボックスをクリックしてオプションを表示します。<br><br>• アクセス制御ルールまたはプレフィルタルール内のオブジェクトの詳細と使用状況を表示します。<br><br>アクセス コントロール ポリシー エディタまたはプレフィルタ ポリシー エディタで、ルールを右クリックし、[オブジェクトの詳細（Object Details）] を選択します。<br><br>サポートされるプラットフォーム：FMC |

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

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

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

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

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

| 新機能 | 説明 |
|---|---|
| 追加の FTD プラットフォームでの Cisco Support Diagnostics。 | **アップグレードの影響。**<br>Cisco Support Diagnostics は、すべての FMC および FTD デバイスで完全にサポートされるようになりました。以前は、サポートは FMC、FTD 搭載 Firepower 4100/9300、および Azure 向け FTDv に限定されていました。詳細については、「シスコとのデータの共有 （3 ページ）」を参照してください。<br>サポートされるプラットフォーム：FMC、FTD |
| **ユーザビリティ** | |
| ライトテーマ。 | FMC はデフォルトでバージョン 6.5.0 のベータ機能として導入されたライトテーマに設定されます。バージョン 6.6.0 にアップグレードすると、ライトテーマに自動的に切り替わります。これは、ユーザー設定で従来のテーマに戻すことができます。<br>すべてに返信することはできませんが、ライトテーマについてのフィードバックを歓迎します。[ユーザー設定（User Preferences）] ページのフィードバックリンクを使用するか、fmc-light-theme-feedback@cisco.com からフィードバックをお送りください。<br>サポート対象プラットフォーム：FMC |
| アップグレードの残り時間の表示。 | FMC のメッセージセンターに、アップグレードが完了するまでのおおよその残り時間が表示されるようになりました。これには、リブート時間は含まれません。<br>新規/変更されたページ：メッセージセンター<br>サポート対象プラットフォーム：FMC |
| **セキュリティと強化** | |
| デフォルトの HTTPS サーバー証明書の更新期限は 800 日。 | **アップグレードの影響。**<br>現在のデフォルトの HTTPS サーバー証明書がすでに 800 日である場合を除き、バージョン 6.6.0 にアップグレードすることで証明書が更新され、有効期限がアップグレード日から 800 日後になりました。今後の更新はすべて、有効期間が 800 日になります。<br>古い証明書は、生成日に応じて期限切れになるように設定されていました。<br>サポート対象プラットフォーム：FMC |
| **Firepower Management Center REST API** | |

| 新機能 | 説明 |
| --- | --- |
| 新しい REST API 機能。 | バージョン 6.6.0 の機能をサポートするための次の REST API サービスが追加されました。<br>• bgp、bgpgeneralsettings、ospfinterface、ospfv2routes、ospfv3interfaces、ospfv3routes、virtualrouters、routemaps、ipv4prefixlists、ipv6prefixlists、aspathlists、communitylists、extendedcommunitylists、standardaccesslists、standardcommunitylists、policylists：ルーティング<br>• virtualrouters、virtualipv4staticroutes、virtualipv6staticroutes、virtualstaticroutes：仮想ルーティング<br>• timeranges、globaltimezones、timezoneobjects：時間ベースのルール<br>• commands：REST API から CLI コマンドの限定的なセットを実行<br>• pendingchanges：保留中の改善点を展開<br>古い機能をサポートするために、次の REST API サービスが追加されました。<br>• intrusionrules、intrusionpolicies：侵入ポリシー<br>サポート対象プラットフォーム：FMC |
| 拡張アクセスリストの REST API サービス名の変更。 | **アップグレードの影響。**<br>FMC REST API の extendedaccesslist（単数形）サービスは、extendedaccesslist**s**（複数形）になりました。クライアントを更新していることを確認します。古いサービス名を使用すると失敗し、無効な URL エラーが返されます。<br>要求タイプ：GET<br>特定の ID に関連付けられている拡張アクセスリストを取得するための URL：<br>• 旧：/api/fmc_config/v1/domain/{domainUUID}/object/extendedaccesslist/{objectId}<br>• 新：/api/fmc_config/v1/domain/{domainUUID}/object/extendedaccesslist**s**/{objectId}<br>すべての拡張アクセスリストを取得するための URL：<br>• 旧：/api/fmc_config/v1/domain/{domainUUID}/object/extendedaccesslist<br>• 新：/api/fmc_config/v1/domain/{domainUUID}/object/extendedaccesslist**s**<br>サポート対象プラットフォーム: FMC |

## 廃止された機能

表 *9* : バージョン *6.6.1* で廃止された機能

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

表 *10* : バージョン *6.6.0* で廃止された機能

| 廃止された機能 | 説明 |
|---|---|
| 廃止：クラウドベースの FMCv 展開でのメモリ不足のインスタンス。 | パフォーマンス上の理由から、次の FMCv インスタンスはサポートされなくなりました。<br>• AWS での c3.xlarge<br>• AWS での c3.2xlarge<br>• AWS での c4.xlarge<br>• AWS での c4.2xlarge<br>• Azure での Standard_D3_v2<br>AWS インスタンスタイプの既存の FMCv はすべて廃止になりました（c3.xlarge、c3.2xlarge、c4.xlarge、c4.2xlarge）。アップグレードする前に、サイズを変更する必要があります。詳細については、FMCv には 28 GB の RAM が必要 （52 ページ） を参照してください。<br>さらに、バージョン 6.6 リリースの時点で、クラウドベースの FMCv の展開におけるメモリ不足のインスタンスタイプが完全に廃止されました。以前の Firepower バージョンであっても、これらを使用して新しい FMCv インスタンスを作成することはできません。既存のインスタンスは引き続き実行できます。 |

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

| 廃止された機能 | 説明 |
|---|---|
| 廃止：イベントビューアから接続イベントを削除する機能。 | バージョン 6.6 は、接続イベントとセキュリティ インテリジェンス イベントをイベントビューアから削除するためのサポートを終了しています。データベースを消去するには、**[システム（System）]**>**[ツール（Tools）]** > **[データの消去（Data purge）]** を選択します。<br>廃止されたオプション：<br>• **[分析（Analysis）]**>**[接続（Connections）]**>**[イベント（Events）]** > [削除（Delete）] と [すべて削除（Delete All）]<br>• **[分析（Analysis）]** > **[接続（Connections）]** > **[セキュリティ インテリジェンス イベント（Security Intelligence Events）]** > [削除（Delete）] と [すべて削除（Delete All）] |
| 廃止：地理位置情報の詳細。 | 2022 年 5 月、GeoDB が 2 つのパッケージに分割されました。IP アドレスを国/大陸にマッピングする国コードパッケージと、ルーティング可能な IP アドレスに関連付けられた追加のコンテキストデータを含む IP パッケージです。IP パッケージのコンテキストデータには、追加のロケーションの詳細に加えて、ISP、接続タイプ、プロキシタイプ、ドメイン名などの接続情報を含めることができます。<br>新しい国コードパッケージのファイル名は、古いオールインワンパッケージと同じ（Cisco_GEODB_Update-*date-build*）です。これにより、バージョン 7.1 以前を実行している環境では、引き続き GeoDB の更新プログラムを取得できます。GeoDB 更新プログラムを手動でダウンロードする場合（エアギャップ展開など）、IP パッケージではなく、必ず国コードパッケージを取得してください。<br>**重要** この分割による地理位置情報ルールやトラフィック処理への影響はありません。これらのルールは、国コードパッケージのデータのみに依存しています。ただし、オールインワンパッケージは原則的に国コードパッケージに置き換えられるため、コンテキストデータは更新されなくなり、陳腐化されます。最新のデータを取得するには、FMC をバージョン 7.2 以降にアップグレードするか再イメージ化して、GeoDB を更新します。 |

# FDM バージョン 6.6 の新機能

**表 *11 : FDM* バージョン *6.6* の新機能と廃止された機能**

| 機能 | 説明 |
|---|---|
| プラットフォーム機能 | |

| 機能 | 説明 |
| --- | --- |
| Amazon Web Services（AWS）クラウド用 FTDv における FDM のサポート。 | FDM を使用して AWS クラウド用 FTDv で Firepower Threat Defense を設定できます。 |
| Firepower 4112 用 FDM。 | Firepower 4112 用 Firepower Threat Defense が導入されました。<br>（注） FXOS 2.8.1 が必要です。 |
| VMware 向け FTDv の e1000 インターフェイス。 | **アップグレードされないようにします。**<br>バージョン 6.6 では、VMware 向け FTDv の e1000 インターフェイスのサポートを終了します。vmxnet3 または ixgbe インターフェイスに切り替えるまで、アップグレードすることはできません。または、新しいデバイスを展開できます。<br>詳細については、『Cisco Secure Firewall Threat Defense Virtual Getting Started Guide』を参照してください。 |
| **ファイアウォールと IPS の機能** | |
| デフォルトでは無効になっている、侵入ルールを有効にする機能。 | 各システム定義の侵入ポリシーには、デフォルトで無効になっているルールがいくつかあります。以前は、これらのルールのアクションをアラートまたはドロップに変更できませんでした。現在では、デフォルトで無効になっているルールのアクションを変更できるようになりました。<br>[侵入ポリシー（Intrusion Policy）] ページが変更され、デフォルトで無効になっているルールもすべて表示されるようになりました。また、これらのルールのアクションも編集できます。 |
| 侵入ポリシーの侵入検知システム（IDS）モード。 | 侵入検知システム（IDS）モードで動作するように侵入ポリシーを設定できるようになりました。IDS モードでは、アクティブな侵入ルールは、ルールアクションがドロップであってもアラートのみを発行します。したがって、侵入ポリシーをネットワーク内でアクティブな防御ポリシーにする前に、その侵入ポリシーの動作をモニタリングまたはテストできます。<br>FDM では、**[Policies]** > **[Intrusion]** ページの各侵入ポリシーに、検査モードの表示が追加されました。また [Edit] リンクが追加され、モードを変更できるようになりました。<br>Firepower Threat Defense API では、IntrusionPolicy リソースに inspectionMode 属性が追加されました。 |

| 機能 | 説明 |
| --- | --- |
| 脆弱性データベース（VDB）、地理位置情報データベース、および侵入ルールの更新パッケージを手動でアップロードするためのサポート。 | VDB、地理位置情報データベース、および侵入ルールの更アップデートパッケージを手動で取得し、FDM を使用してワークステーションから Firepower Threat Defense 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><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、**[デバイス（Device）]** > **[更新（Updates）]** ページが更新されました。 |
| Firepower Threat Defense 時間に基づいて制限されているアクセス制御ルールの API サポート。 | Firepower Threat Defense API を使用して、時間範囲オブジェクトを作成できます。このオブジェクトでは、1 回限りの時間範囲または繰り返しの時間範囲を指定します。オブジェクトはアクセス制御ルールに適用します。時間範囲を使用すると、特定の時間帯または一定期間にわたってトラフィックにアクセス制御ルールを適用して、ネットワークを柔軟に使用できます。FDM を使用して時間範囲を作成したり、適用したりはできません。また、アクセス制御ルールに時間範囲が適用されている場合、FDM は表示されません。<br><br>TimeRangeObject、Recurrence、TimeZoneObject、DayLightSavingDateRange、および DayLightSavingDayRecurrence リソースが Firepower Threat Defense API に追加されました。時間範囲をアクセス制御ルールに適用するために、timeRangeObjects 属性が accessrules リソースに追加されました。さらに、GlobalTimeZone および TimeZone リソースに変更が加えられました。 |

| 機能 | 説明 |
| --- | --- |
| アクセス コントロール ポリシーのオブジェクトグループ検索。 | 動作中、Firepower Threat Defense デバイスは、アクセスルールで使用されるネットワークオブジェクトの内容に基づいて、アクセス制御ルールを複数のアクセスコントロールリストのエントリに展開します。オブジェクトグループ検索を有効にすることで、アクセス制御ルールの検索に必要なメモリを抑えることができます。オブジェクトグループ検索を有効にした場合、システムによってネットワークオブジェクトは拡張されませんが、オブジェクトグループの定義に基づいて一致するアクセスルールが検索されます。オブジェクトグループ検索は、アクセスルールがどのように定義されているかや、FDM にどのように表示されるかには影響しません。アクセス制御ルールと接続を照合するときに、デバイスがアクセス制御ルールを解釈して処理する方法のみに影響します。オブジェクトグループ検索はデフォルトで無効になっています。<br><br>FDM では、FlexConfig を使用して **object-group-search access-control** コマンドを有効にする必要があります。 |
| **VPN 機能** | |
| サイト間 VPN のバックアップピア（Firepower Threat Defense API のみ）。 | Firepower Threat Defense API を使用して、サイト間 VPN 接続にバックアップピアを追加できます。たとえば、2 つの ISP がある場合は、最初の ISP への接続が使用できなくなった場合に、バックアップ ISP にフェールオーバーするように VPN 接続を設定できます。<br><br>バックアップピアのもう 1 つの主な用途は、プライマリハブやバックアップハブなど、トンネルのもう一方の端に 2 つの異なるデバイスがある場合です。通常、システムはプライマリハブへのトンネルを確立します。VPN 接続が失敗すると、システムはバックアップハブとの接続を自動的に再確立できます。<br><br>SToSConnectionProfile リソースで outsideInterface に対して複数のインターフェイスを指定できるように、Firepower Threat Defense API が更新されました。また、BackupPeer リソースと remoteBackupPeers 属性が SToSConnectionProfile リソースに追加されました。<br><br>FDM を使用してバックアップピアを設定したり、バックアップピアの存在を FDM に表示したりはできません。 |

| 機能 | 説明 |
| --- | --- |
| リモートアクセス VPN での Datagram Transport Layer Security（DTLS）1.2 のサポート。 | リモートアクセス VPN で DTLS 1.2 を使用できるようになりました。これは、Firepower Threat Defense API のみを使用して設定できます。FDM を使用して設定することはできません。ただし、DTLS 1.2 はデフォルトの SSL 暗号グループの一部になったため、グループポリシーの AnyConnect 属性で FDM を使用して DTLS の一般的な使用が可能になりました。DTLS 1.2 は、ASA 5508-X または 5516-X モデルではサポートされていないことに注意してください。<br><br>DTLSV1_2 を列挙値として受け入れるように sslcipher リソースの protocolVersion 属性が更新されました。 |
| 安全性の低い Diffie-hellman グループ、および暗号化アルゴリズムとハッシュアルゴリズムのサポートを廃止。 | 次の機能は廃止されており、将来のリリースでは削除されます。VPN で使用するために、IKE プロポーザルまたは IPSec ポリシーでこれらの機能を設定しないでください。これらの機能から移行し、実用可能になったらすぐにより強力なオプションを使用してください。<br><br>• Diffie-Hellman グループ：2、5、および 24。<br><br>• 強力な暗号化の輸出規制を満たすユーザー向けの暗号化アルゴリズム：DES、3DES、AES-GMAC、AES-GMAC-192、AES-GMAC-256。輸出規制を満たしていないユーザーの場合、DES は引き続きサポートされます（これが唯一のオプションです）。<br><br>• ハッシュアルゴリズム：MD5。 |
| **ルーティング機能** | |

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

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

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

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

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

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

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

# 侵入ルールとキーワード

アップグレードにより侵入ルールをインポートして自動的に有効化が可能です。

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

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

Snort のバージョンを確認するには、互換性ガイドの「バンドルされたコンポーネント」の項を参照するか、次のコマンドのいずれかを使用します。

- FMC：**[ヘルプ（Help）] > [概要（About）]**を選択します。

- FDM：**show summary** CLI コマンドを使用します。

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

# 廃止された FlexConfig コマンド

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

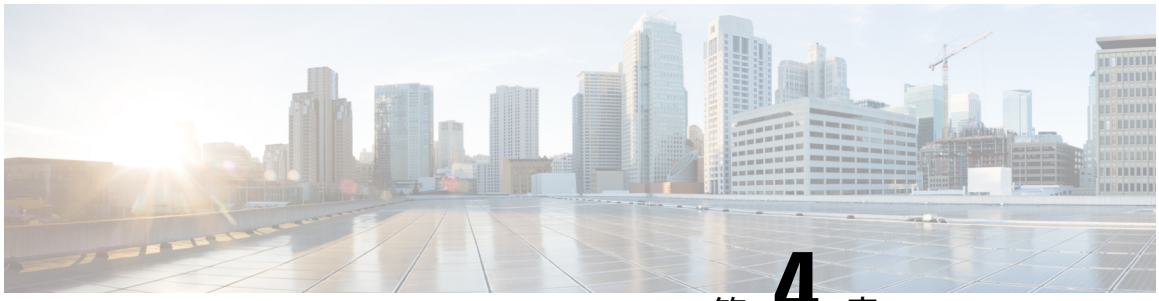
**注意** ほとんどの場合、既存のFlexConfig設定はアップグレード後も引き続き機能し、展開ができます。ただし、廃止されたコマンドを使用すると、展開の問題が発生する場合があります。

## FlexConfig について

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

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

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



第 4 章

# のアップグレードガイドライン

このドキュメントには、バージョン 6.6 の重要なリリース固有のアップグレードガイドラインが記載されています。



# アップグレードの計画

誤りを避けるには、注意深い計画と準備が役立ちます。この表はアップグレードの計画プロセスを要約したものです。詳細なチェックリストと手順については、該当するアップグレードガイドとコンフィギュレーション ガイド（http://www.cisco.com/jp/go/threatdefense-66-docs）を参照してください。

**表 *12*：アップグレードの計画フェーズ**

| 計画フェーズ | 次を含む |
|---|---|
| 計画と実現可能性 | 展開を評価します。<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 | 次を含む |
|---|---|
| バックアップ | ソフトウェアをバックアップします。<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 のファームウェア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>設定を展開します。<br>準備状況チェックを実行します。<br>ディスク容量を確認します。<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

## アップグレードする最小バージョン

次のように、メンテナンスリリースを含む バージョン 6.6 に直接アップグレードできます。

**表 *13 :* バージョン *6.6* にアップグレードするための最小バージョン**

| プラットフォーム | 最小バージョン |
|---|---|
| FMC | 6.2.3 |

| プラットフォーム | 最小バージョン |
|---|---|
| FTD | 6.2.3<br>Firepower 4100/9300 には FXOS 2.8.1.15 が必要です。ほとんどの場合、各メジャーバージョンで最新の FXOS ビルドを使用することを推奨します。判断のヒントについては、Cisco Firepower 4100/9300 FXOS Release Notes, 2.8(1) を参照してください。 |
| ASA with FirePOWER サービス | 6.2.3<br>モデルの ASA 要件については、デバイスプラットフォーム（6 ページ）を参照してください。ASA と ASA FirePOWER のバージョン間には広い互換性がありますが、アップグレードすることで、新機能と解決された問題を活用できます。判断のヒントについては、Cisco Secure Firewall ASA リリースノートを参照してください。 |
| NGIPSv | 6.2.3 |

### パッチを適用する最小バージョン

パッチは4桁目のみを変更します。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。

# バージョン 6.6 のアップグレードガイドライン

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

**表 *14 : FMC* を使用した *FTD* のアップグレードガイドラインバージョン *6.6***

| ✓ | 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 |
|---|---|---|---|---|
| | Cisco Secure Firewall Management Center の新機能（リリース別）：アップグレードに影響を与える新機能および廃止された機能が記載されています。現在のバージョンと対象バージョンの間にあるすべてのバージョンを確認してください。 | 任意（Any） | 任意（Any） | 任意（Any） |

| ✓ | 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 |
|---|---|---|---|---|
| | 未解決のバグおよび解決されたバグ（93 ページ）：アップグレードに影響を与えるバグが記載されています。現在のバージョンと対象バージョン間にあるすべてのバージョンのリリースノートを確認してください。 | 任意（Any） | 任意（Any） | 任意（Any） |
| | アップグレードする最小バージョン（46 ページ） | 任意（Any） | 任意（Any） | 任意（Any） |
| | FXOS のアップグレードガイドライン（67 ページ） | Firepower 4100/9300 | 任意（Any） | 任意（Any） |
| | アップグレード禁止：FMC バージョン 6.6.5 以降からバージョン 6.7.0（51 ページ） | FMC | 6.6.5 以降 6.6.x リリース | 6.7.0 のみ |
| | アップグレードの失敗：侵入イベントに関する電子メールアラート機能を搭載した FMC（52 ページ） | FMC | 6.2.3 ～ 6.7.0.x | 6.7.0<br>6.6.0、6.6.1、6.6.3<br>これらのリリースに対するすべてのパッチ |
| | FMCv には 28 GB の RAM が必要（52 ページ） | FMCv | 6.2.3 ～ 6.5.0.x | 6.6 以降 |
| | Firepower 1000 シリーズ デバイスではアップグレード後に電源の再投入が必要（54 ページ） | Firepower 1000 シリーズ | 6.4.0 | 6.5 以降 |
| | 新しい URL カテゴリとレピュテーション（54 ページ） | いずれか | 6.2.3 ～ 6.4.0.x | 6.5 以降 |
| | TLS 暗号化アクセラレーションの有効化/無効にすることは不可（63 ページ） | Firepower 2100 シリーズ<br>Firepower 4100/9300 | 6.2.3 ～ 6.3.0.x | 6.4 以降 |

| ✓ | ガイドライン | プラットフォーム | アップグレード元 | 直接アップグレード先 |
|---|---|---|---|---|
| | 名前が変更されたアップグレードとインストール パッケージ （63 ページ） | FMC<br>Firepower 7000/8000 シリーズ<br>NGIPSv | いずれか | 6.3+ |
| | FMC、NGIPSv で準備状況チェックに失敗する可能性 （64 ページ） | FMC<br>Firepower 7000/8000 シリーズ<br>NGIPSv | 6.1.0 ～ 6.1.0.6<br>6.2.0 ～ 6.2.0.6<br>6.2.1<br>6.2.2 ～ 6.2.2.4<br>6.2.3 ～ 6.2.3.4 | 6.3+ |
| | リモートアクセス VPN のデフォルト設定の変更によって VPN トラフィックがブロックされる可能性（65 ページ） | FTD | 6.2.0 ～ 6.2.3.x | 6.3+ |
| | セキュリティ インテリジェンスによって可能になるアプリケーションの識別 （65 ページ） | FMC の展開 | 6.1.0 ～ 6.2.3.x | 6.3+ |
| | アップグレード後に VDB を更新して CIP 検出を有効化 （66 ページ） | いずれか | 6.1.0 ～ 6.2.3.x | 6.3+ |
| | 無効な侵入変数セットによって展開に失敗する可能性 （66 ページ） | いずれか | 6.1.0 ～ 6.2.3.x | 6.3+ |

表 *15 : FDM* を使用した *FTD* のアップグレードガイドラインバージョン *6.6*

| ✓ | 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 |
|---|---|---|---|---|
| | Cisco Secure Firewall Device Manager の新機能（リリース別）：アップグレードに影響を与える新機能および廃止された機能が記載されています。現在のバージョンと対象バージョンの間にあるすべてのバージョンを確認してください。 | 任意（Any） | 任意（Any） | 任意（Any） |

| ✓ | 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 |
|---|---|---|---|---|
| | 未解決のバグおよび解決されたバグ （93 ページ）：アップグレードに影響を与えるバグが記載されています。現在のバージョンと対象バージョン間にあるすべてのバージョンのリリースノートを確認してください。 | 任意（Any） | 任意（Any） | 任意（Any） |
| | アップグレードする最小バージョン （46 ページ） | 任意（Any） | 任意（Any） | 任意（Any） |
| | FXOS のアップグレードガイドライン （67 ページ） | Firepower 4100/9300 | 任意（Any） | 任意（Any） |
| | FDM を使用したバージョン 6.6.0.1 FTD アップグレードによる HA の一時停止 （51 ページ） | 任意（Any） | 6.6.0 | 6.6.0.1 |
| | Firepower 1000 シリーズ デバイスではアップグレード後に電源の再投入が必要 （54 ページ） | Firepower 1000 シリーズ | 6.4.0 | 6.5 以降 |
| | FDM を使用した FTD のアップグレード時に削除される履歴データ （54 ページ） | いずれか | 6.2.3 ～ 6.4.0.x | 6.5 以降 |
| | 新しい URL カテゴリとレピュテーション （54 ページ） | いずれか | 6.2.3 ～ 6.4.0.x | 6.5 以降 |
| | TLS 暗号化アクセラレーションの有効化/無効にすることは不可（63 ページ） | Firepower 2100 シリーズ<br>Firepower 4100/9300 | 6.2.3 ～ 6.3.0.x | 6.4 以降 |
| | アップグレード後に VDB を更新して CIP 検出を有効化 （66 ページ） | いずれか | 6.1.0 ～ 6.2.3.x | 6.3+ |
| | 無効な侵入変数セットによって展開に失敗する可能性 （66 ページ） | いずれか | 6.1.0 ～ 6.2.3.x | 6.3+ |

# FDM を使用したバージョン 6.6.0.1 FTD アップグレードによる HA の一時停止

**展開**：FTD と FDM をハイアベイラビリティペアとして設定

**アップグレード元**：バージョン 6.6.0

**直接アップグレード先**：バージョン 6.6.0.1

**関連バグ**：CSCvv45500

ハイアベイラビリティ（HA）の FDM 管理 FTD デバイスをバージョン 6.6.0.1 にアップグレードすると、アップグレード後の再起動後にデバイスが一時停止モードになります。HA を手動で再開する必要があります。

FMC 展開は影響を受けません。

FDM 管理 FTD HA ペアをバージョン 6.6.0.1 にアップグレードするには、次の手順を実行します。

1. スタンバイデバイスをアップグレードします。
2. アップグレードが完了してデバイスがリブートしたら、手動で HA を再開します。FDM または CLI を使用できます。
   - FDM：**[Device]** > **[High Availability]**をクリックし、ギアメニュー（⚙）から [Resume HA] を選択します。
   - CLI： **configure high-availability resume**

   新しくアップグレードされたデバイスの HA ステータスは、スタンバイ装置として、装置がピアとネゴシエートした後に正常に戻ります。
3. 新しくアップグレードしたデバイスがアクティブピアになるように、アクティブピアとスタンバイピアを切り替えます（強制フェールオーバー）。
4. 新しいスタンバイピアに対してこの手順を繰り返します。

FDM でのハイアベイラビリティの設定と管理の詳細については、『『Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager』』を参照してください。

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

**展開**：FMC

**アップグレード元**：バージョン 6.6.5 以降のメンテナンスリリース

**直接アップグレード先**：バージョン 6.7.0 のみ

バージョン 6.6.5 以降の 6.6.x メンテナンスリリースからバージョン 6.7.0 にアップグレードすることはできません。これは、バージョン 6.6.5 のデータストアがバージョン 6.7.0 のデータス

トアよりも新しいためです。バージョン 6.6.5 以降を実行している場合は、バージョン 7.0.0 以降に直接アップグレードすることをお勧めします。

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

**展開**：Firepower Management Center

**アップグレード元**：バージョン 6.2.3 ～ 6.7.0.x

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

**関連するバグ**：CSCvw38870、CSCvx86231

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

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

侵入に関する電子メールアラートを完全に無効にするには、次の操作を行います。

1. Firepower Management Center で、**[Policies]** > **[Actions]** > **[Alerts]**を選択し、**[Intrusion Email]** をクリックします。
2. [State] を [off] に設定します。
3. [Rules] の横にある [Email Alerting per Rule Configuration] をクリックし、ルールの選択を解除します。

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

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

4. 設定を保存します。

# FMCv には 28 GB の RAM が必要

**展開**：FMCv

**アップグレード元**：バージョン 6.2.3 ～ 6.5

**直接アップグレード先**：バージョン 6.6 以降

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

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

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

次の表に、メモリが不足している展開のアップグレード前の要件を示します。

**表 *16*：バージョン *6.6* 以降 にアップグレードする場合の *FMCv* のメモリ要件**

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

| プラットフォーム | アップグレード前のアクション | 詳細 |
|---|---|---|
| Azure | インスタンスのサイズを変更します。<br>• Standard_D3_v2 から Standard_D4_v2 へ。 | Azure ポータルまたは PowerShell を使用します。サイズを変更する前にインスタンスを停止する必要はありませんが、停止すると追加のサイズが表示される場合があります。サイズ変更により、実行中の仮想マシンが再起動されます。<br>手順については、Windows VM のサイズ変更に関する Azure のマニュアルを参照してください。 |

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

**展開**：Firepower 1000 シリーズ デバイス

**アップグレード元**：バージョン 6.4.0.x

**直接アップグレード先**：バージョン 6.5.0+

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

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

# FDM を使用した FTD のアップグレード時に削除される履歴データ

**展開**：FTD（FDM を使用）

**アップグレード元**：バージョン 6.2.3 ～ 6.4.0.x

**直接アップグレード先**：バージョン 6.5.0 以降

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

# 新しい URL カテゴリとレピュテーション

**展開**：すべて

**アップグレード元**：バージョン 6.2.3 ～ 6.4.0.x

**直接アップグレード先**：バージョン 6.5.0+

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

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

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

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

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

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

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

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

表 *17:* アップグレード時の展開の変更

| 変更内容 | 詳細 |
|---|---|
| URLルールのカテゴリが変更されます。 | アップグレードにより、次のポリシーで、新しいカテゴリセットのほぼ同等のルールが使用されるように URL ルールが変更されます。<br>• アクセス コントロール<br>• SSL<br>• QoS（FMC のみ）<br>• 相関（FMC のみ）<br>これらの変更により、余分なルールや無効になったルールが生じ、パフォーマンスが低下する可能性があります。マージされたカテゴリが設定に含まれている場合、許可またはブロックされる URL が若干変更されることがあります。 |
| URL ルールのレピュテーションの名前が変更されます。 | アップグレードにより、新しいレピュテーション名を使用するように URL ルールが変更されます。<br>**1.** 信頼されていない（「高リスク」だった）<br>**2.** 疑わしい（「疑わしいサイト」だった）<br>**3.** ニュートラル（「セキュリティリスクのある無害なサイト」だった）<br>**4.** 好ましい（「無害なサイト」だった）<br>**5.** 信頼されている（「十分に既知」だった） |
| URLキャッシュをクリアします。 | アップグレードによって URL キャッシュがクリアされます。このキャッシュには、システムが以前にクラウドで検索した結果が含まれています。ローカル データ セットに含まれていない URL については、アクセス時間が一時的に少し長くなることがあります。 |
| 「レガシー」イベントにラベルを付けます。 | すでにログに記録されているイベントの場合、アップグレードにより、関連する URL のカテゴリおよびレピュテーション情報が「レガシー」としてラベル付けされます。これらのレガシー イベントは時間の経過とともにデータベースからエージ アウトします。 |

## URL カテゴリおよびレピュテーションのアップグレード前のアクション

アップグレードする前に、次のアクションを実行します。

表 *18* : アップグレード前のアクション

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

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

## URL カテゴリおよびレピュテーションのアップグレード後のアクション

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

**表 *19*：アップグレード後の操作**

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

| アクション | 詳細 |
|---|---|
| **マージされたカテゴリ**の結果として変更されたルールを評価します。 | 影響を受けたカテゴリのいずれかが含まれている各ルールに影響を受けたすべてのルールが含まれるようになります。元のカテゴリが異なるレピュテーションに関連付けられていた場合、新しいルールはさらに広い、より包含的なレピュテーションに関連付けられます。以前と同様にURLをフィルタリングするには、いくつかの設定を変更する必要があります。「マージされた URL カテゴリを持つルールのガイドライン（59 ページ）」を参照してください。<br><br>変更内容とプラットフォームがルールの警告を処理する方法に応じて、変更がマークされることがあります。たとえば、FMCは完全に冗長および完全にプリエンプション処理されたルールをマークしますが、部分的に重複したルールはマークしません。 |
| **分割されたカテゴリ**の結果として変更されたルールを評価します。 | アップグレードにより、URL ルール内の古い単一のカテゴリが新しいカテゴリすべてに置き換えられ、新しいカテゴリは古いカテゴリにマッピングされます。これによりURLのフィルタリング方法は変更されませんが、影響を受けるルールを変更して、新しい精度を活用することができます。<br><br>これらの変更はマークされません。 |
| **名前が変更された**カテゴリまたは**変更されていない**カテゴリを把握します。 | 特に対処の必要はありませんが、これらの変更に注意する必要があります。<br><br>これらの変更はマークされません。 |
| **未分類**および**レピュテーションのない**URLの処理方法を評価します。 | 未分類の URL とレピュテーションのない URL を使用できるようになりましたが、未分類の URL をレピュテーションでフィルタ処理することも、レピュテーションのない URL をフィルタ処理することもできません。<br><br>[未分類（Uncategorized）] カテゴリまたは [すべて（Any）] のレピュテーションでフィルタ処理されるルールが、期待どおりに動作することを確認してください。 |

## マージされた URL カテゴリを持つルールのガイドライン

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

表 *20 :* マージされた *URL* カテゴリを持つルールのガイドライン

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

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

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

**表 *21 :* マージされた *URL* カテゴリを持つルールの例**

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

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

# TLS 暗号化アクセラレーションの有効化/無効にすることは不可

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

**アップグレード元**：バージョン 6.1.0 ～ 6.3.x

**直接アップグレード先**：バージョン 6.4.0 以降

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

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

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

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

# 名前が変更されたアップグレードとインストール パッケージ

**展開**： FMC、7000/8000 シリーズ、NGIPSv

**アップグレード元**：バージョン 6.1.0 ～ 6.2.3.x

**直接アップグレード先**：バージョン 6.3 +

アップグレード、パッチ、ホットフィックス、およびインストールパッケージの命名スキーム（名前の最初の部分）は、当該プラットフォーム上で「Version 6.3.0」で始まるように変更されました。

（注） この変更により、古い物理アプライアンス（DC750、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。バージョン 5.x を現在実行していて、これらのアプライアンスのいずれかにバージョン 6.3.0 または 6.4.0 を新規インストールする必要がある場合は、シスコ サポートおよびダウンロード サイト からインストール 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。 これらのアプライアンスをバージョン 6.5+ に再イメージ化することはできません。

表 *22 :* 命名スキーム：アップグレード、パッチ、およびホットフィックス パッケージ

| プラットフォーム | 命名方式 |
|---|---|
| FMC | 新： Cisco_Firepower_Mgmt_Center<br>旧： Sourcefire_3D_Defense_Center_S3 |
| NGIPSv | 新： Cisco_Firepower_NGIPS_Virtual<br>旧： Sourcefire_3D_Device_VMware<br>旧： Sourcefire_3D_Device_Virtual64_VMware |

表 *23 :* 命名スキーム：インストール パッケージ

| プラットフォーム | 命名方式 |
|---|---|
| FMC （物理） | 新： Cisco_Firepower_Mgmt_Center<br>旧： Sourcefire_Defense_Center_M4<br>旧： Sourcefire_Defense_Center_S3 |
| FMCv: VMware | 新： Cisco_Firepower_Mgmt_Center_Virtual_VMware<br>旧： Cisco_Firepower_Management_Center_Virtual_VMware |
| FMCv: KVM | 新： Cisco_Firepower_Mgmt_Center_Virtual_KVM<br>旧： Cisco_Firepower_Management_Center_Virtual |
| Firepower 7000/8000 シリーズ | 新： Cisco_Firepower_NGIPS_Appliance<br>旧： Sourcefire_3D_Device_S3 |
| NGIPSv | 新： Cisco_Firepower_NGIPSv_VMware<br>旧： Cisco_Firepower_NGIPS_VMware |

# FMC、NGIPSv で準備状況チェックに失敗する可能性

**展開**：FMC、NGIPSv

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

**直接アップグレード先**：バージョン 6.3.0+

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

表 *24 :* バージョン *6.3.0* 以降用の準備状況チェックを備えたパッチ

| 準備完了チェックがサポートされない | 修正された最初のパッチ |
|---|---|
| 6.1.0 ～ 6.1.0.6 | 6.1.0.7 |
| 6.2.0 ～ 6.2.0.6 | 6.2.0.7 |
| 6.2.1 | なし。バージョン 6.2.3.5+ にアップグレードしてください。 |
| 6.2.2 ～ 6.2.2.4 | 6.2.2.5 |
| 6.2.3 ～ 6.2.3.4 | 6.2.3.5 |

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

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

**アップグレード元**：バージョン 6.2.x

**直接アップグレード先**：バージョン 6.3 +

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

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

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

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

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

# セキュリティインテリジェンスによって可能になるアプリケーションの識別

**展開**：Firepower Management Center

**アップグレード元**：バージョン 6.1 ～ 6.2.3.x

**直接アップグレード先**：バージョン 6.3 +

バージョン 6.3 では、セキュリティ インテリジェンスの設定によりアプリケーションの検出と識別が可能になります。現在の展開で検出を無効にした場合は、アップグレード プロセスによって再び検出が有効になる可能性があります。必要がない場合（たとえば、IPS のみの展開など）に検出を無効にするとパフォーマンスが向上する可能性があります。

検出を無効にするには、次の手順を実行する必要があります。

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

# アップグレード後に VDB を更新して CIP 検出を有効化

**展開**：すべて

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

**直接アップグレード先**：バージョン 6.3.0+

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

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

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

# 無効な侵入変数セットによって展開に失敗する可能性

**展開**：すべて

**アップグレード元**：バージョン 6.1 ～ 6.2.3.x

**直接アップグレード先**：バージョン 6.3.0+

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

| 有効 | 無効 |
|---|---|
| 含める：10.0.0.0/8<br>除外する：10.1.0.0/16 | 含める：10.1.0.0/16<br>除外する：172.16.0.0/12<br>除外する：10.0.0.0/8 |

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

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

# FXOS のアップグレードガイドライン

Firepower 4100/9300 の場合、FTD のメジャーアップグレードには FXOS のアップグレードも必要です。

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

また、最新のファームウェアを推奨します（『Cisco Firepower 4100/9300 FXOS ファームウェア アップグレード ガイド』を参照）。

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

### FTD をアップグレードするために必要な FXOS の最小バージョン

バージョン 6.6 を実行するために必要な FXOS の最小バージョンは、FXOS 2.8.1.15 です。

### FXOS をアップグレードするために必要な FXOS の最小バージョン

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

### FXOS アップグレードの所要時間

FXOS のアップグレードには最長 45 分かかることがあり、トラフィックフローやインスペクションに影響を与える場合があります。詳細については、FXOS のアップグレードでのトラフィックフローとインスペクション （71 ページ）を参照してください。

# 応答しないアップグレード

アップグレード中は、設定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、アップグレード中は手動で再起動またはシャットダウンしないでください。システムが使用できない状態になり、再イメージ化が必要になる場合があります。アップグレードに失敗する、アプライアンスが応答しないなど、アップグレードで問題が発生した場合には Cisco TAC にお問い合わせください。

# パッチをアンインストールする

FMC 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。以前のメジャーリリースまたはメンテナンスリリースに戻す必要がある場合は、イメージを再作成する必要があります。ガイドライン、制限、および手順については、 FMC アップグレードガイドの「Uninstall a Patch」またはこれらのリリースノートの「ASDM による ASA FirePOWER パッチのアンインストール （68 ページ）」を参照してください。

## ASDM による ASA FirePOWER パッチのアンインストール

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

ASA フェールオーバーペアおよびクラスタの場合、一度に 1 つのアプライアンスからアンインストールすることにより、中断を最小限に抑えます。次に移る前に、パッチが 1 つのユニットから完全にアンインストールされるまで待ちます。

表 *25 : ASA* フェールオーバーペア/クラスタ内の *ASA with FirePOWER Services* のアンインストール順序

| 設定 | アンインストール順序 |
|---|---|
| ASA FirePOWER が有効な ASA アクティブ/スタンバイ フェールオーバー ペア | 常にスタンバイからアンインストールします。<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 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。 |

⚠

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

### 始める前に

- ASA のフェールオーバーやクラスタの展開では、正しいデバイスからアンインストールしようとしていることを確認してください。
- 正常に展開され、通信が確立されていることを確認します。

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

アンインストールする前に展開すると、失敗する可能性が減少します。展開とその他の必須のタスクが完了していることを確認してください。アンインストールの開始時に実行中だったタスクは停止され、失敗したタスクとなって再開できなくなります。後で失敗ステータス メッセージを手動で削除できます。

**ステップ 2** ASA FirePOWER モジュールの Firepower CLI にアクセスします。`admin` として、または設定アクセス権を持つ別の Firepower CLI ユーザーとしてログインします。

モジュールの管理インターフェイスに SSH 接続するか（ホスト名または IP アドレス）、コンソールを使用できます。コンソールポートはデフォルトで ASA CLI に設定されており、Firepower CLI にアクセスするには `session sfr` コマンドを使用する必要があることにご注意ください。

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

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

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

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

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

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

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

**ステップ 6** ログアウトするまでアンインストールを監視します。

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

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

それ以外の場合は、コンソールか端末で進行状況を監視します。

**ステップ 7** アンインストールが成功したことを確認します。

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

**ステップ 8** 構成を再展開します。

### 次のタスク

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

# トラフィック フローとインスペクション

デバイスのアップグレード（ソフトウェアおよびオペレーティングシステム）により、トラフィックフローとインスペクションが影響を受けます。影響が最も少ない時間帯にメンテナンス期間をスケジュールします。

## FXOS のアップグレードでのトラフィックフローとインスペクション

FXOS をアップグレードするとシャーシが再起動します。ハイアベイラビリティやスケーラビリティ環境でも、各シャーシのFXOSを個別にアップグレードします。中断を最小限に抑えるには、1 つずつシャーシをアップグレードします。

**表 *26 :* トラフィックフローとインスペクション：*FXOS* のアップグレード**

| FTD の導入 | トラフィックの挙動 | メソッド |
|---|---|---|
| スタンドアロン | 廃棄 | — |
| 高可用性 | 影響なし。 | **ベストプラクティス**：スタンバイで FXOS を更新し、アクティブピアを切り替えて新しいスタンバイをアップグレードします。 |
| | 1 つのピアがオンラインになるまでドロップされる。 | スタンバイでアップグレードが終了する前に、アクティブ ピアで FXOS をアップグレードします。 |

| FTD の導入 | トラフィックの挙動 | メソッド |
|---|---|---|
| シャーシ間クラスタ | 影響なし。 | **ベストプラクティス**：少なくとも 1 つのモジュールを常にオンラインにするため、一度に 1 つのシャーシをアップグレードします。 |
| | 少なくとも 1 つのモジュールがオンラインになるまでドロップされる。 | ある時点ですべてのモジュールを停止するため、シャーシを同時にアップグレードします。 |
| シャーシ内クラスタ（FirePOWER 9300 のみ） | 検査なしで受け渡される。 | ハードウェアバイパス有効：[Bypass: Standby] または [Bypass-Force]。 |
| | 少なくとも 1 つのモジュールがオンラインになるまでドロップされる。 | ハードウェアバイパス無効：[Bypass: Disabled]。 |
| | 少なくとも 1 つのモジュールがオンラインになるまでドロップされる。 | ハードウェアバイパスモジュールなし。 |

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

### スタンドアロンデバイスでのソフトウェアのアップグレード

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

**表 *27:* トラフィックフローとインスペクション：スタンドアロンデバイスでのソフトウェアのアップグレード**

| インターフェイス コンフィギュレーション | トラフィックの挙動 |
|---|---|
| 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<br><br>ISA 3000 のブリッジ グループ インターフェイスの場合に限り、FlexConfig ポリシーを使用して、停電時のハードウェアバイパスを設定できます。これにより、ソフトウェアのアップグレード中にトラフィックのドロップが発生しますが、デバイスがアップグレード後の再起動中、インスペクションなしでトラフィックが通過します。 |

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

### 高可用性および拡張性に関するソフトウェアのアップグレード

高可用性デバイスやクラスタ化されたデバイスのアップグレード中に、トラフィックフローや検査が中断されることはありません。高可用性ペアの場合、スタンバイデバイスが最初にアップグレードされます。デバイスの役割が切り替わり、新しくスタンバイになったデバイスがアップグレードされます。

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

### ソフトウェアのアンインストール（パッチ）

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

### 設定変更の導入

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

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

**表 *28 :* トラフィックフローとインスペクション：設定変更の展開**

| インターフェイス コンフィギュレーション | | トラフィックの挙動 |
|---|---|---|
| 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、[フェールセーフ（Failsafe）] が有効または無効。 | 検査なしで受け渡される。<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フェールオープン：ダウン（Snort Fail Open: Down）]：無効 | 廃棄 |
| | インライン、[Snortフェールオープン：ダウン（Snort Fail Open: Down）]：有効 | 検査なしで受け渡される。 |
| | インラインセット、タップモード。 | パケットをただちに出力、コピーへのインスペクションなし。 |
| | パッシブ、ERSPAN パッシブ。 | 中断なし、インスペクションなし。 |

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

### ソフトウェアのアップグレード

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

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

### 設定変更の導入

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

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

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

### ソフトウェアのアップグレード

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

**表 *29 :*** トラフィックフローとインスペクション：***ASA FirePOWER*** のアップグレード

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

### ソフトウェアのアンインストール（パッチ）

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

### 設定変更の導入

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

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

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

### ソフトウェアのアップグレード

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

**表 *30 :* トラフィックフローとインスペクション：*NGIPSv* のアップグレード**

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

### ソフトウェアのアンインストール（パッチ）

パッチのアンインストール中のトラフィックフローと検査の中断は、アップグレードの場合と同じになります。

### 設定変更の導入

Snort プロセスを再開すると、一時的にトラフィックフローと検査が中断されます。インターフェイス設定により、中断中にインスペクションせずにトラフィックをドロップするか受け渡

すかが決定されます。Snort を再起動せずに展開すると、リソース要求時にいくつかのパケットが検査なしでドロップされることがあります。

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

**表 *31 :* トラフィックフローとインスペクション：設定変更の展開**

| インターフェイス コンフィギュレーション | トラフィックの挙動 |
|---|---|
| インライン、[フェールセーフ（Failsafe）] が有効または無効 | 検査なしで受け渡される。<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、FMC およびソフトウェアのアップグレードにかかる時間とディスク容量のテストに関するレポートを提供しています。

### 時間テスト

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

⚠

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

表 *32 :* 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 | デバイスアップグレードの時間は、FMC展開でのテストに基づいています。同様の条件の場合、リモートとローカルの管理対象デバイスのraw アップグレード時間は類似しています。 |
| バージョン | メジャーリリースおよびメンテナンスリリースでは、以前のすべての対象メジャーバージョンからのアップグレードをテストします。パッチについては、ベースバージョンからアップグレードをテストします。アップグレードでバージョンがスキップされると、通常、アップグレード時間は長くなります。 |
| モデル | ほとんどの場合、各シリーズの最もローエンドのモデルでテストし、場合によってはシリーズの複数のモデルでテストします。 |
| 仮想アプライアンス | メモリおよびリソースのデフォルト設定を使用してテストします。ただし、仮想展開でのアップグレード時間はハードウェアに大きく依存することに注意してください。 |
| 高可用性/拡張性 | 特に断りのない限り、スタンドアロンデバイスでテストします。<br>高可用性の構成またはクラスタ化された構成では、動作の継続性を保持するため、複数のデバイスは1つずつアップグレードされます。アップグレード中は、各デバイスはメンテナンスモードで動作します。そのため、デバイスペアまたはクラスタ全体のアップグレードには、スタンドアロンデバイスのアップグレードよりも長い時間がかかります。 |
| 設定 | シスコでは、構成およびトラフィック負荷が最小限のアプライアンスでテストを行います。<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（/Volume または /var 内）に必要な容量も報告します。FTD アップグレードパッケージ用の内部サーバーがある場合、または FDM を使用している場合は、それらの値を無視してください。

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

空きディスク容量が十分でない場合、アップグレードは失敗します。

**表 *33* : ディスク容量の確認**

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

# バージョン 6.6.7.1 の時間とディスク容量

**表 *34* : バージョン *6.6.7.1* の時間とディスク容量**

| プラットフォーム | ボリュームの容量 | 必要容量 | FMC の容量 | アップグレード時間 | リブート時間 |
|---|---|---|---|---|---|
| FMC | /var 内で 2.8 GB | / 内で 20 MB | — | 37 分 | 9 分 |
| FMCv：VMware | /var 内で 3.4 GB | / 内で 23 MB | — | 35 分 | 7 分 |
| Firepower 1000 シリーズ | — | /ngfw 内で 3.8 GB | 870 MB | 9 分 | 7 分 |
| Firepower 2100 シリーズ | — | /ngfw 内で 2.9 GB | 900 MB | 7 分 | 13 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 4100 シリーズ | — | /ngfw 内で 3.1 GB | 680 MB | 6 分 | 8 分 |
| Firepower 4100 シリーズコンテナインスタンス | — | /ngfw 内で 2.3 GB | 680 MB | 6 分 | 5 分 |
| Firepower 9300 | — | /ngfw 内で 3.2 GB | 680 MB | 5 分 | 10 分 |
| FTD を搭載した ASA 5500-X シリーズ | /home 内で 3.1 GB | /ngfw 内で 120 MB | 630 MB | 10 分 | 16 分 |
| FTDv：VMware | /home 内で 2.5 GB | /ngfw 内で 120 MB | 630 MB | 7 分 | 6 分 |
| ASA FirePOWER | /var 内で 2.9 GB | / 内で 21 MB | 430 MB | 22 分 | 6 分 |
| NGIPSv | /var 内で 940 MB | / 内で 19 MB | 290 MB | 6 分 | 6 分 |

# バージョン 6.6.7 の時間とディスク容量

**表 *35 :* バージョン *6.6.7* 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 | リブート時間 |
|---|---|---|---|---|---|
| FMC | /var 内で 17.0 GB | / 内で 23 MB | — | 49 分 | 14 分 |
| FMCv：VMware | /var 内で 20.1 GB | / 内で 29 MB | — | 48 分 | 7 分 |
| Firepower 1000 シリーズ | — | /ngfw 内で 10.4 GB | 1.0 GB | 19 分 | 18 分 |
| Firepower 2100 シリーズ | — | /ngfw 内で 10.3 GB | 1.0 GB | 17 分 | 15 分 |
| Firepower 4100 シリーズ | — | /ngfw 内で 10.1 GB | 970 MB | 10 分 | 11 分 |
| Firepower 4100 シリーズコンテナインスタンス | — | /ngfw 内で 10.4 GB | 970 MB | 10 分 | 8 分 |
| Firepower 9300 | — | /ngfw 内で 10.2 GB | 970 MB | 14 分 | 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 | リブート時間 |
|---|---|---|---|---|---|
| FTD を搭載した ASA 5500-X シリーズ | /home 内で 8.6 GB | /ngfw 内で 752 KB | 1.2 GB | 22 分 | 22 分 |
| FTDv：VMware | /home 内で 9.3 GB | /ngfw 内で 752 KB | 1.2 GB | 13 分 | 20 分 |
| ASA FirePOWER | /var 内で 12 GB | / 内で 26 MB | 1.3 GB | 73 分 | 16 分 |
| NGIPSv | /var 内で 7.4 GB | / 内で 21 MB | 870 MB | 12 分 | 7 分 |

# バージョン 6.6.5.2 の時間とディスク容量

表 *36 :* バージョン *6.6.5.2* の時間とディスク容量

| プラットフォーム | ボリュームの容量 | 必要容量 | FMC の容量 | アップグレード時間 | リブート時間 |
|---|---|---|---|---|---|
| FMC | /var 内で 2.8 GB | / 内で 20 MB | — | 39 分 | 8 分 |
| FMCv：VMware | /var 内で 3.4 GB | / 内で 23 MB | — | 26 分 | 8 分 |
| Firepower 1000 シリーズ | — | /ngfw 内で 3.0 GB | 630 MB | 8 分 | 12 分 |
| Firepower 2100 シリーズ | — | /ngfw 内で 2.9 GB | 660 MB | 7 分 | 12 分 |
| Firepower 9300 | — | /ngfw 内で 2.4 GB | 430 MB | 5 分 | 8 分 |
| Firepower 4100 シリーズ | — | /ngfw 内で 2.9 GB | 430 MB | 6 分 | 8 分 |
| Firepower 4100 シリーズコンテナインスタンス | — | /ngfw 内で 2.5 GB | 430 MB | 5 分 | 6 分 |
| FTD を搭載した ASA 5500-X シリーズ | /home 内で 2.2 GB | /ngfw 内で 120 MB | 380 MB | 10 分 | 15 分 |
| FTDv：VMware | /home 内で 1.8 GB | /ngfw 内で 120 MB | 380 MB | 5 分 | 6 分 |
| ASA FirePOWER | /var 内で 2.9 GB | / 内で 21 MB | 450 MB | 68 分 | 22 分 |
| NGIPSv | /var 内で 920 MB | / 内で 19 MB | 310 MB | 6 分 | 5 分 |

# バージョン 6.6.5.1 の時間とディスク容量

表 *37* : バージョン *6.6.5.1* の時間とディスク容量

| プラットフォーム | ボリュームの容量 | 必要容量 | FMC の容量 | アップグレード時間 | リブート時間 |
|---|---|---|---|---|---|
| FMC | /var 内で 2.2 GB | / 内で 20 MB | — | 34 分 | 8 分 |
| FMCv：VMware | /var 内で 2.2 GB | 23 MB | — | 28 分 | 6 分 |
| Firepower 1000 シリーズ | — | /ngfw 内で 1.5 GB | 340 MB | 8 分 | 12 分 |
| Firepower 2100 シリーズ | — | /ngfw 内で 1.4 GB | 370 MB | 6 分 | 11 分 |
| Firepower 9300 | — | /ngfw 内で 770 MB | 140 MB | 5 分 | 8 分 |
| Firepower 4100 シリーズ | — | /ngfw 内で 790 MB | 140 MB | 5 分 | 8 分 |
| Firepower 4100 シリーズコンテナインスタンス | — | /ngfw 内で 730 MB | 140 MB | 6 分 | 5 分 |
| FTD を搭載した ASA 5500-X シリーズ | /home 内で 590 MB | /ngfw 内で 120 MB | 85 MB | 9 分 | 9 分 |
| FTDv：VMware | /home 内で 590 MB | /ngfw 内で 120 MB | 85 MB | 6 分 | 5 分 |
| ASA FirePOWER | /var 内で 1.7 GB | / 内で 21 MB | 130 MB | 69 分 | 7 分 |
| NGIPSv | /var 内で 78 MB | / 内で 19 MB | 16 MB | 6 分 | 5 分 |

# バージョン 6.6.5 の時間とディスク容量

表 *38* : バージョン *6.6.5* の時間とディスク容量

| プラットフォーム | ボリュームの容量 | 必要容量 | FMC の容量 | アップグレード時間 | リブート時間 |
|---|---|---|---|---|---|
| FMC | /var 内で 16.5 GB | / 内で 23 MB | — | 55 分 | 14 分 |
| FMCv：VMware | /var 内で 21 GB | / 内で 29 MB | — | 51 分 | 9 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 1000 シリーズ | /ngfw/var 内で 9.7 GB | /ngfw 内で 400 MB | 1.1 GB | 20 分 | 16 分 |
| Firepower 2100 シリーズ | /ngfw/var 内で 10.2 GB | /ngfw 内で 450 MB | 1.1 GB | 17 分 | 15 分 |
| Firepower 9300 | 10.2 GB<br>/ngfw/var 内で 11 | /ngfw 内で MB | 1.1 GB | 12 分 | 10 分 |
| Firepower 4100 シリーズ | /ngfw/var 内で 10.1 MB | /ngfw 内で 10 MB | 1.1 GB | 10 分 | 11 分 |
| Firepower 4100 シリーズコンテナインスタンス | /ngfw/var 内で 10.7 GB | /ngfw 内で 11 MB | 1.1 GB | 12 分 | 7 分 |
| FTD を搭載した ASA 5500-X シリーズ | /ngfw/var 内で 8.6 GB | /ngfw 内で 756 KB | 1.3 GB | 22 分 | 30 分 |
| FTDv：VMware | /ngfw/var 内で 9.1 GB | /ngfw 内で 756 KB | 1.3 GB | 12 分 | 21 分 |
| ASA FirePOWER | /var 内で 12 GB | / 内で 26 MB | 1.4 GB | 65 分 | 25 分 |
| NGIPSv | 7.4 GB<br>/var 内で 21 | MB/内 | 910 MB | 12 分 | 21 分 |

# バージョン 6.6.4 の時間とディスク容量

**表 *39 :* バージョン *6.6.4* の時間とディスク容量**

| プラットフォーム | ボリュームの容量 | 必要容量 | FMC の容量 | アップグレード時間 | リブート時間 |
|---|---|---|---|---|---|
| FMC | /var 内で 15.1 GB | / 内で 23 MB | — | 60 分 | 28 分 |
| FMCv：VMware | /var 内で 23.7 GB | / 内で 29 MB | — | 43 分 | 8 分 |
| Firepower 1000 シリーズ | /ngfw/var 内で 9.7 GB | /ngfw 内で 400 MB | 1 GB | 21 分 | 16 分 |
| Firepower 2100 シリーズ | /ngfw/var 内で 10.1 GB | /ngfw 内で 450 MB | 1 GB | 21 分 | 13 分 |

| プラットフォーム | ボリュームの容量 | 必要容量 | FMC の容量 | アップグレード時間 | リブート時間 |
|---|---|---|---|---|---|
| Firepower 9300 | /ngfw/var 内で 10.1 GB | /ngfw 内で 11 MB | 970 MB | 14 分 | 10 分 |
| Firepower 4100 シリーズ | /ngfw/var 内で 8.9 GB | /ngfw 内で 11 MB | 970 MB | 11 分 | 9 分 |
| Firepower 4100 シリーズコンテナインスタンス | /ngfw/var 内で 10.9 GB | /ngfw 内で 10 MB | 970 MB | 10 分 | 7 分 |
| FTD を搭載した ASA 5500-X シリーズ | /ngfw/var 内で 8.5 GB | /ngfw 内で 756 KB | 1.2 GB | 20 分 | 19 分 |
| FTDv：VMware | /ngfw/var 内で 7.7 GB | /ngfw 内で 756 KB | 1.2 GB | 19 分 | 12 分 |
| ASA FirePOWER | /var 内で 11.4 GB | / 内で 26 MB | 1.3 GB | 59 分 | 16 分 |
| NGIPSv | /var 内で 7.4 GB | / 内で 21 MB | 870 MB | 13 分 | 8 分 |

# バージョン 6.6.3 の時間とディスク容量

**表 *40 :* バージョン *6.6.3* の時間とディスク容量**

| プラットフォーム | ボリュームの容量 | 必要容量 | FMC の容量 | アップグレード時間 | リブート時間 |
|---|---|---|---|---|---|
| FMC | /var 内で 15.1 GB | / 内で 23 MB | — | 60 分 | 28 分 |
| FMCv：VMware | /var 内で 23.7 GB | / 内で 29 MB | — | 43 分 | 8 分 |
| Firepower 1000 シリーズ | /ngfw/var 内で 9.7 GB | /ngfw 内で 400 MB | 1 GB | 21 分 | 16 分 |
| Firepower 2100 シリーズ | /ngfw/var 内で 10.1 GB | /ngfw 内で 450 MB | 1 GB | 21 分 | 13 分 |
| Firepower 4100 シリーズ | /ngfw/var 内で 8.9 GB | /ngfw 内で 11 MB | 970 MB | 11 分 | 9 分 |
| Firepower 4100 シリーズコンテナインスタンス | /ngfw/var 内で 10.9 GB | /ngfw 内で 10 MB | 970 MB | 10 分 | 7 分 |

| プラットフォーム | ボリュームの容量 | 必要容量 | FMC の容量 | アップグレード時間 | リブート時間 |
|---|---|---|---|---|---|
| Firepower 9300 | /ngfw/var 内で 10.1 GB | /ngfw 内で 11 MB | 970 MB | 14 分 | 10 分 |
| FTD を搭載した ASA 5500-X シリーズ | /ngfw/var 内で 8.5 GB | /ngfw 内で 756 KB | 1.2 GB | 20 分 | 19 分 |
| FTDv：VMware | /ngfw/var 内で 7.7 GB | /ngfw 内で 756 KB | 1.2 GB | 19 分 | 12 分 |
| ASA FirePOWER | /var 内で 11.4 GB | / 内で 26 MB | 1.3 GB | 59 分 | 16 分 |
| NGIPSv | /var 内で 7.4 GB | / 内で 21 MB | 870 MB | 13 分 | 8 分 |

# バージョン 6.6.1 の時間とディスク容量

表 *41 :* バージョン *6.6.1* の時間とディスク容量

| プラットフォーム | 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 | 18.6 GB | 23 MB | — | 54 分 | 14 分 |
| FMCv：VMware | 15.8 GB | 58 MB | — | 56 分 | 13 分 |
| Firepower 1000 シリーズ | 10.8 GB | 400 MB | 1.1 GB | 20 分 | 17 分 |
| Firepower 2100 シリーズ | 10.9 GB | 450 MB | 1.1 GB | 16 分 | 21 分 |
| Firepower 4100 シリーズ | 9.7 GB | 10 MB | 1 GB | 15 分 | 14 分 |
| Firepower 4100 シリーズコンテナインスタンス | 11.2 GB | 9 MB | 1 GB | 10 分 | 13 分 |
| Firepower 9300 | 9.8 GB | 11 MB | 1 GB | 15 分 | 15 分 |
| FTD を搭載した ASA 5500-X シリーズ | 9.3 GB | 1 MB | 1.2 GB | 21 分 | 24 分 |
| FTDv：VMware | 9.3 GB | 1 MB | 1.2 GB | 18 分 | 19 分 |

| プラットフォーム | ボリュームの容量 | 必要容量 | FMC の容量 | アップグレード時間 | リブート時間 |
|---|---|---|---|---|---|
| ASA FirePOWER | 12.3 GB | 26 MB | 1.4 GB | 72 分 | 23 分 |
| NGIPSv | 7.1 GB | 54 MB | 860 MB | 14 分 | 20 分 |

# バージョン 6.6.0.1 の時間とディスク容量

この表で、アップグレード時間には再起動が含まれます。

**表 *42 :* バージョン *6.6.0.1* の時間とディスク容量**

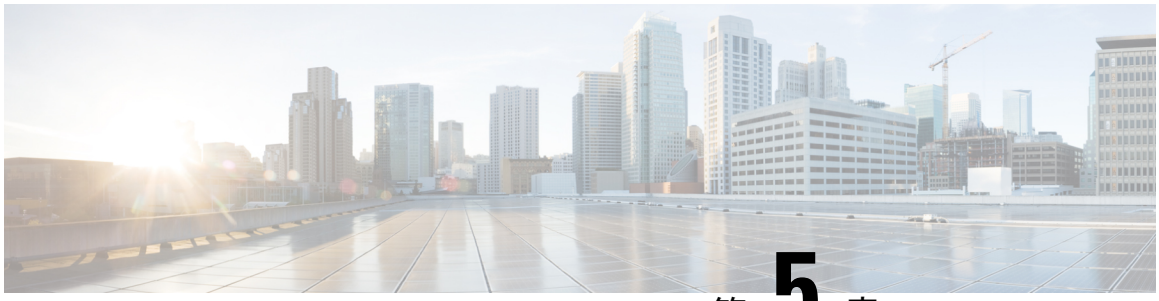
| プラットフォーム | ボリュームの容量 | 必要容量 | FMC の容量 | アップグレードおよび再起動時間 |
|---|---|---|---|---|
| FMC | 31 MB | 20 MB | — | 22 分 |
| FMCv：VMware | 1.1 GB | 23 MB | — | 17 分 |
| Firepower 1000 シリーズ | 450 MB | 450 MB | 240 MB | 21 分 |
| Firepower 2100 シリーズ | 260 MB | 260 MB | 270 MB | 17 分 |
| Firepower 4100 シリーズ | 470 MB | 470 MB | 46 MB | 11 分 |
| Firepower 9300 | 460 MB | 460 MB | 46 MB | 33 分 |
| FTD を搭載した ASA 5500-X シリーズ | 440 MB | 120 MB | 46 MB | 17 分 |
| FTD を使用した ISA 3000 | 440 MB | 120 MB | 46 MB | 21 分 |
| FTDv：VMware | 430 MB | 120 MB | 46 MB | 11 分 |
| ASA FirePOWER | 80 MB | 20 MB | 15 MB | 18 分 |
| NGIPSv | 64 MB | 28 MB | 15 MB | 9 分 |

# バージョン 6.6.0 の時間とディスク容量

（注） ASA 5545-X with FirePOWER Services では、デバイス上の SRU がバージョン 6.6.0 アップグレードパッケージ（2020-01-16-001-vrt）と同じか、またはそれよりも新しい場合は、想定よりもアップグレードに時間がかかる場合があります（1 時間以上）。これによる影響があるかどうかを判断するには、デバイス上の Firepower CLI にログインし、**show version** コマンドを使用して**ルールの更新バージョン**を表示します。

表 *43 :* バージョン *6.6.0* の時間とディスク容量

| プラットフォーム | ボリュームの容量 | 必要容量 | FMC の容量 | アップグレード時間 | リブート時間 |
|---|---|---|---|---|---|
| FMC | /var 内で 16.5 GB | 71 MB/内 | — | 46 分 | 15 分 |
| FMCv：VMware | /var 内で 16.7 GB | 57 MB/内 | — | 36 分 | 7 分 |
| Firepower 1000 シリーズ | /ngfw/var 内で 410 MB | /ngfw 内で 11.5 GB | 1.1 GB | 20 分 | 17 分 |
| Firepower 2100 シリーズ | /ngfw/var 内で 470 MB | /ngfw 内で 10.3 GB | 1 GB | 14 分 | 14 分 |
| Firepower 4100 シリーズ | /ngfw/var 内で 61 MB | /ngfw 内で 9.3 GB | 980 MB | 11 分 | 9 分 |
| Firepower 4100 シリーズコンテナインスタンス | /ngfw/var 内で 46 MB | /ngfw 内で 11.3 GB | 980 MB | 11 分 | 6 分 |
| Firepower 9300 | /ngfw/var 内で 64 MB | /ngfw 内で 8.7 GB | 980 MB | 15 分 | 12 分 |
| FTD を搭載した ASA 5500-X シリーズ | /ngfw/var 内で 8.7 GB | /ngfw 内で 70 KB | 1.2 GB | 23 分 | 26 分 |
| FTDv：VMware | /ngfw/var 内で 8.7 GB | /ngfw 内で 70 KB | 1.2 GB | 14 分 | 17 分 |
| ASA FirePOWER | /var 内で 11.4 GB | 63 MB/内 | 1.4 GB | 93 分 | 10 分 |
| NGIPSv | /var 内で 6.1 GB | 53 MB/内 | 860 MB | 10 分 | 5 分 |



第 5 章

# ソフトウェアのインストール

バージョン6.6にアップグレードできない場合、またはアップグレードしない場合は、メジャーリリースおよびメンテナンスリリースを新規インストールできます。これは再イメージ化とも呼ばれます。パッチ用のインストールパッケージは提供していません。特定のパッチを実行するには、適切なメジャーリリースまたはメンテナンスリリースをインストールしてからパッチを適用してください。



## 設置に関するガイドライン

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

### バックアップ

再イメージ化の前に、安全なリモートロケーションにバックアップし、正常に転送されたことを確認することを強く推奨します。再イメージ化によって、システムパスワードを含むほとんどの設定が工場出荷時の初期状態に戻ります。アプライアンスに残っているすべてのバックアップが削除されます。

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

### アプライアンス アクセス

アプライアンスに物理的にアクセスできない場合、現在のメジャーリリースまたはメンテナンスリリースへの再イメージ化によって管理ネットワークの設定を維持できます。これにより、再イメージ化した後、アプライアンスに接続して、初期設定を実行できます。ネットワーク設

定を削除する場合や以前のリリースに再イメージ化する場合は、アプライアンスに物理的にアクセスできる必要があります。Lights-Out 管理（LOM）を使用することはできません。

デバイスに関して、ユーザーの位置からのトラフィックがデバイスの管理インターフェイスにアクセスするためにデバイス自体を通過する必要がないことを確認してください。FMC の展開では、デバイスを経由せずにFMC管理インターフェイスにアクセスできる必要もあります。

### Smart Software Manager からのの登録解除

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

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

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

**表 *44 : CSSM* からの登録解除シナリオ（バックアップから復元しない）**

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

### FMC からのデバイスの削除

FMC の展開で再イメージ化されたアプライアンスを手動で設定する予定がある場合は、再イメージ化する前に、FMC からデバイスを削除します。バックアップからの復元を予定している場合は、これを行う必要はありません。

表 *45 : FMC* からデバイスを削除するシナリオ（バックアップから復元しない）

| シナリオ | アクション |
|---|---|
| FMC を再イメージ化します。 | 管理からデバイスを削除します。 |
| FTD を再イメージ化します。 | 管理から任意のデバイスを削除します。 |
| FTD を FMC から FDM へ切り替えます。 | 管理から任意のデバイスを削除します。 |

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

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

表 *46 :* 完全な再イメージ化のシナリオ

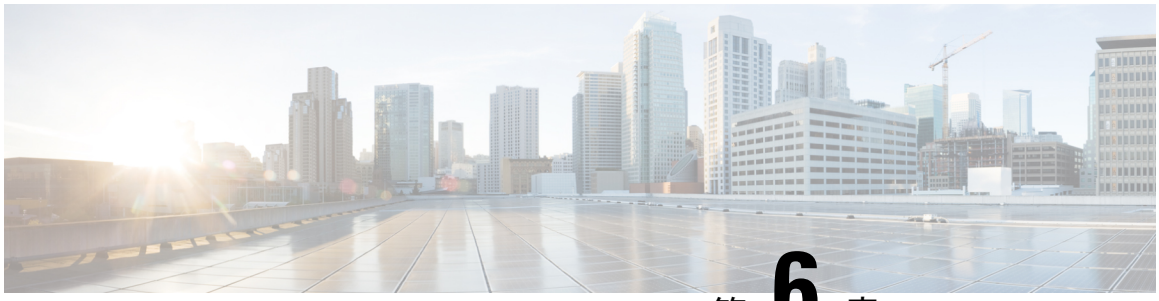
| モデル | 詳細 |
|---|---|
| Firepower 1000 シリーズ<br>Firepower 2100 シリーズ | **erase configuration** メソッドを使用してイメージを再作成すると、FXOS がソフトウェアとともにダウングレードされない場合があります。この場合、特にハイ アベイラビリティ展開では、障害が発生する可能性があります。これらのデバイスの完全な再イメージ化を実行することを推奨します。 |
| Firepower 4100/9300 | FTD を復元しても FXOS はダウングレードされません。<br>Firepower 4100/9300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

# 設置ガイド

表 *47 :* 設置ガイド

| プラットフォーム | ガイド |
|---|---|
| **FMC** | |

| プラットフォーム | ガイド |
|---|---|
| FMC 1600、2600、4600 | Cisco Firepower Management Center 1600, 2600, and 4600 Getting Started Guide |
| FMC 1000、2500、4500 | Cisco Firepower Management Center 1000, 2500, and 4500 Getting Started Guide |
| FMC 2000、4000 | Cisco Firepower Management Center 750, 1500, 2000, 3500 and 4000 Getting Started Guide |
| FMCv | Cisco Secure Firewall Management Center Virtual 入門ガイド |
| **FTD** | |
| Firepower 1000/2100 シリーズ | Cisco Secure Firewall ASA および Secure Firewall Threat Defense 再イメージ化ガイド<br>Firepower 1000/2100 および Secure Firewall 3100 と Firepower Threat Defense の Cisco FXOS トラブルシューティング ガイド |
| 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 Getting Started Guide<br>Cisco Firepower 9300 Getting Started Guide |
| ASA 5500-X シリーズ | Cisco Secure Firewall ASA および Secure Firewall Threat Defense 再イメージ化ガイド |
| ISA 3000 | Cisco Secure Firewall ASA および Secure Firewall Threat Defense 再イメージ化ガイド |
| FTDv | Cisco Secure Firewall Threat Defense Virtual Getting Started Guide |
| **ASA FirePOWER/NGIPSv** | |
| ASA FirePOWER | Cisco Secure Firewall ASA および Secure Firewall Threat Defense 再イメージ化ガイド<br>ASDM ブック 2：Cisco ASA シリーズ ファイアウォール ASDM コンフィギュレーション ガイド |
| NGIPSv | Cisco Firepower NGIPSv Quick Start Guide for VMware |



第 6 章

# 未解決のバグおよび解決されたバグ

このドキュメントには、バージョン 6.6 デバイスならびに Management Center の未解決のバグと解決済みのバグの一覧が記載されています。

**重要** バグリストは一度自動生成されると、その後は更新されない場合があります。更新された場合、「表の最終更新日」は、リストがその日付で完全に正確になったことを意味するのではありません。一部に変更が加えられただけです。バグがシステムでどのように分類または更新されたかとその時期によっては、リリースノートに記載されない場合があります。メンテナンスリリースまたはパッチの未解決のバグも記載していません。サポート契約がある場合は、Cisco バグ検索ツールを使用して最新のバグリストを取得できます。



# 未解決のバグ

## バージョン 6.6.0 で未解決のバグ

表の最終更新日：2022-11-02

**表 *48* : バージョン *6.6.0* で未解決のバグ**

| 不具合 ID | タイトル |
|---|---|
| CSCvr90564 | ユーザー VRF のエリア間 OSPF 設定を無効にすると、展開が失敗する |
| CSCvt14898 | RAVPN を使用したアップグレード後に展開に失敗する（no split-tunnel-network-list value RA-VPN-policy\|splitAcl） |
| CSCvt29546 | 同じボックスにバックアップを復元した後に、ライセンスの登録が解除される |

| 不具合 ID | タイトル |
|---|---|
| CSCvt37753 | MI クラスタでポリシーの展開が失敗する |
| CSCvt39442 | 管理者ユーザーが原因でダッシュボードウィジェットが表示されない |
| CSCvt43431 | CLI の管理インターフェイス設定の変更後、UI では CLI の変更が更新されていなかった。OOB の同期の問題 |
| CSCvt61370 | 通信のデッドロックが原因で、デバイスからのイベントが停止することがある |
| CSCvt66906 | セッションでアプリケーションが検出された場合でも、Appid はダイナミックキャッシュを検索する |
| CSCvt68316 | インポートの失敗後に展開が絶えず失敗し、変更を破棄できない |
| CSCvt68819 | アップグレード前に存在していたイベントをコピーすると、クリップボードへのコピーが失敗することがある |
| CSCvt69260 | 接続イベントに古いデバイス名が表示される |
| CSCvt70854 | 6.6.0-90： [Firepower 1010] メモリ不足のため、SRU の更新中に tomcat が再起動する |
| CSCvt77143 | Apache Commons FileUpload の HTTP リクエストヘッダーの値の処理の拒否 |
| CSCvt77210 | 1.2.2 よりも前の minimist では正しく追加または変更されているように見える場合がある |
| CSCvt78634 | アサーションドメイン ID を使用したポリシー展開時に FTD lina がトレースバックする |
| CSCvt79988 | FMC を 6.6 にアップグレードした後、SNMP 設定が原因でポリシー展開が失敗する |
| CSCvt86467 | c3p0 0.9.5.2 では、com/mcha の extractXmlConfigFromInputStream で XXE が許可される |
| CSCvt87117 | libexpat 不適切な解析によるサービス拒否の脆弱性 |
| CSCvt87123 | Expat libexpat XML パーサーに関するサービス拒否の脆弱性 |
| CSCvt89042 | dom4j XML インジェクションの脆弱性 |
| CSCvt89045 | Redis redis-cli バッファオーバーフローの脆弱性 |
| CSCvt89378 | ログイン時に「データベースに重大なエラーが発生しました。再起動する必要があります（The database has encountered a critical error, and needs to be restarted.）」という UI エラーが表示される |

| 不具合 ID | タイトル |
|---|---|
| CSCvt91258 | FDM：管理ゲートウェイとしてデータインターフェイスを使用して、どの NTP サーバーにも到達しない |
| CSCvt97205 | ASA 9.14.1 上で SNMPPOLL/SNMPTRAP からリモートエンド（サイト間 VPN）ASA インターフェイスが失敗する |
| CSCvt99082 | Rest API：拡張アクセスリストの URL が extendedaccesslist から extendedaccesslist に変更された |
| CSCvu06882 | KVM ASAv からの virtio インターフェイスのホットプラグ削除によりクラッシュが発生する |
| CSCvu12608 | ASA5506/5508/5516 デバイスが正しく起動しない/ブートループが発生する |
| CSCvu13287 | FDM のアップグレードが 800_post/100_ftd_onbox_data_import.sh で失敗する |
| CSCvu16826 | リリース6.6へのアップグレード後に snort ルールが破損しているため、FTD snort インスタンスがダウンする |
| CSCvu18510 | MonetDB のイベントデータベースのクラッシュにより、FMC 6.6.0 の接続イベントが失われる |
| CSCvu20690 | 2.1.3 より前の dom4j で、外部 DTD および外部エンティティがデフォルトで許可される |
| CSCvu29145 | Snort フロー IP プロファイリングでは、「system support flow-ip-profiling start」コマンドを使用して有効にできない |
| CSCvu30441 | FMC 6.6 REST API GUI では、新しいアクセスルールを PUT または POST しようとする際に応答がない |
| CSCvu30748 | PTHREAD-1859 でバージョン 9.14.1 にアップグレードした後の ASAv のトレースバックおよびリロード |
| CSCvu35426 | リーフドメインのスケジュール展開では、1 つのデバイスのみがポリシーを展開する |
| CSCvu35768 | FMC を 6409-59 から 6.6.0-90 にアップグレードした後、サブドメイン内の Radius 外部ユーザーを使用して UI をログに記録できない |
| CSCvu50400 | Firepower 6.2.3.x から 6.6.0 にアップグレードした後、ASDM を使用する ASA FirePOWER の CPU 使用率が高くなる |
| CSCvu65890 | サポートされていないにも関わらず、FMC が SNMP3 設定で MD5 および DES から切り替えることができない |
| CSCvu70622 | リロード後に CTS SGT 伝播が有効になる |

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

# 解決済みのバグ

## 新しいビルドで解決されたバグ

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

同じソフトウェアバージョンに対して、1つのビルドから別のビルドにアップグレードすることはできません。影響を受けるビルドをすでに実行している場合は、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判断します。それ以外の場合は、Cisco TAC にお問い合わせください。公的に利用可能なホットフィックスへのクイックリンクについては、Cisco Firepower ホットフィックス リリース ノート を参照してください。

表 *49* : バージョン *6.6* の新しいビルド

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

# バージョン 6.6.7.1 で解決済みのバグ

表の最終更新日：2023-01-24

表 *50* : バージョン *6.6.7.1* で解決済みのバグ

| 不具合 ID | タイトル |
|---|---|
| CSCvk00122 | FMC で定期的にスケジュールされたタスクが作成され、タスクが指定された時間に実行されない - [ツール（Tools）]>[スケジュール（Scheduling）] |
| CSCvq29993 | FPR2100 のみ：サイズが 9472 および 1550 のメモリブロックで永続的なブロックリークとブラックホールトラフィックが発生する |
| CSCvr33586 | FPR1010：しきい値を超えた場合の SSD の温度/警告を追加する |
| CSCvs95188 | 異なるインスタンス間で共有される FXOS FTD マルチインスタンス CPU コア |
| 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 |

| 不具合 ID | タイトル |
|---|---|
| CSCvt35774 | SNMP ログファイルのローテーションがないため、ディスク使用率が高くなる |
| CSCvt44295 | ポリシー展開中に生成される Snort コアである |
| 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 |
| CSCvt66186 | FP2100 上の ASA が ASA-4-199016（9.13.1、アプライアンスモード）を生成し続ける |
| CSCvt68055 | snmpd が FP21xx デバイスの FXOS で頻繁に再生成される |
| CSCvu65654 | RADIUS ユーザーが SSH セッションを確立すると、4100 プラットフォームで権限拒否エラーが発生する |
| CSCvu84127 | 明確な理由なしに Firepower がリブートすることがある |
| CSCvu97112 | SNMP ポーリングが HA のアクティブデバイスで動作を停止した |
| 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 |
| CSCvv36788 | MsgLayer[PID]：エラー：Msglyr::ZMQWrapper::registerSender()：ZeroMQ ソケットのバインドに失敗した |
| CSCvv52349 | 2100/1000 シリーズ Firepower デバイスに XFS 破損を処理するユーティリティがない |
| CSCvv54829 | FPR デバイスが 8GB を超える USB/ペンドライブを認識しない |
| CSCvv74658 | FTD/ASA は、ファイル名に「!」の文字を含むコアダンプファイルを作成する（CSCvv40406 の zmq 変更（fxos）） |
| CSCvw05392 | diagnostic-cli に常に表示されるメッセージ |
| CSCvw15359 | KP fxos snmp に、EPM インデックスの entPhysicalSerialNum,entPhysicalAssetID に初期化されていない文字列がある |
| CSCvw16165 | ポートチャネルのメンバーがダウンすると、Firepower 1010 シリーズがトラフィックの通過を停止する |
| CSCvw29647 | FTD：NAS-IP-Address:0.0.0.0 が Radius 要求パケットで aaa-server のネットワークインターフェイスとして定義されていない |
| 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 |
| CSCvw72260 | ASA のアップグレードが「CSP directory does not exist - STOP_FAILED Application_Not_Found」で失敗する |

| 不具合 ID | タイトル |
|---|---|
| CSCvw90634 | FP2100 ASA：9.15.1.1 へのアップグレード後にネットワークモジュールがダウン/ダウンの 1 Gbps SFP |
| 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 |
| CSCvw94160 | CIAM：OpenSSL CVE-2020-1971 |
| 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 |
| CSCvw98315 | FXOS は 6.7.0 への FTD アップグレード後に古い FTD バージョンを報告する |
| 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 |
| CSCvx16700 | 「MIO が強制時刻同期に応答しない（MIO DID NOT RESPOND TO FORCED TIME SYNC）」ために、ブレードの起動中に FXOS クロック同期の問題が発生する |
| CSCvx24207 | IPv4 および IPv6 アドレスのみを含む FQDN オブジェクトは IPv6 エントリのみをインストールする |
| CSCvx29429 | CSCvx07389 の修正にもかかわらず、FPR4100/FPR9300 で ma_ctx*.log が大きなディスク領域を消費する |
| 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 |
| 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 |
| CSCvx59252 | FXOS は管理インターフェイスのログファイルをローテーションしていない |
| CSCvx66329 | FTD ホットフィックス Cisco_FTD_SSP_FP2K_Hotfix_O のインストールがスクリプト 000_start/125_verify_bundle.sh で失敗する |
| 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 |
| CSCvx73164 | シスコ製品に影響を及ぼす Lasso SAML 実装の脆弱性：2021 年 6 月 |
| CSCvx89827 | FPR 2110 でバンコクタイムゾーンを設定できない |

| 不具合 ID | タイトル |
|---|---|
| CSCvx98807 | CCM レイヤ（スプリント 109、シーケンス 9）での WR6 および WR8 コミット ID の更新である |
| 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 |
| 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 |
| CSCvy08798 | CCM レイヤ（スプリント 110、シーケンス 10）での LTS18 コミット ID の更新である |
| CSCvy10789 | LDAP パスワードで FTD 2110 ASCII 文字を使用できない |
| CSCvy12991 | シャーシのローカル日付と時刻が、再起動後に 2015 年 1 月 1 日の午前 0 時に戻る場合がある |
| CSCvy26511 | ローエンドプラットフォームの管理対象外ディスクアラートのしきい値を調整 |
| CSCvy33879 | FTD：repair_users.pl が FTD のリブート失敗の原因となる rogue.firstboot ファイルを作成する |
| CSCvy34333 | ASA のアップグレードに失敗した場合、プラットフォームとアプリケーションの間でバージョンステータスの同期が解除される |
| 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 |
| CSCvy39791 | Lina のトレースバックとコアファイルサイズが 40G を超えており、圧縮に失敗する |
| CSCvy40482 | 9.14MR3：snmpwalk が [Errno 146] の接続拒否エラーで失敗した |
| CSCvy63463 | 特殊文字が原因でユーザーの削除でエラーが発生 |
| CSCvy64145 | CCM レイヤ（スプリント 113、シーケンス 12）での WR6、WR8 コミット ID の更新 |
| CSCvy65178 | Firepower プラットフォームのボックス BGP トラフィックに専用の Rx リングが必要である |
| CSCvy86817 | カスタム CCL IP サブネットが設定されている場合、Cruz ASIC CLU フィルタに誤った src/dst IP サブネットが存在する |
| CSCvy89648 | CSCvx29429 の回避策を適用した後、ma_ctx ファイルが拡張子「.backup」で表示される |

| 不具合 ID | タイトル |
|---|---|
| CSCvy89658 | CCM レイヤ（スプリント 114、シーケンス 13）での WR6、WR8 および LTS18 コミット ID の更新 |
| 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 |
| CSCvz05767 | FP-1010 HA リンクがダウンするか、新しいホストがデバイスに接続できない |
| CSCvz06652 | SNMP の有効期間設定で snmpd コアファイルが検出される |
| CSCvz07004 | SNORT2：SSL ルールに DND アクションがある場合でも、FTD はフルプロキシを実行している |
| CSCvz12494 | FPR2100 では、電源オフ/オン後、FXOS のバージョンが ASA のバージョンと一致しない |
| CSCvz15676 | Firepower 1010 デバイスで、ASA アプリをアップグレードした後、デバイスがフェールセーフモードになる |
| CSCvz15755 | FTD：アップグレード後にポートチャネルが起動せず、コアファイルが生成される場合がある |
| CSCvz22668 | VMS データベースの復元の失敗により、FMC バックアップの復元が失敗することがある |
| CSCvz34289 | 場合によっては、軽量プロキシへの移行が Do Not Decrypt フローで機能しない |
| CSCvz39455 | ASA：21xx でのソフトウェアアップグレード後に SNMPv3 ウォーク/ポーリングを実行できない |
| CSCvz41551 | FP2100：脅威検出統計を備えた ASA/FTD が、スレッド名「lina」でトレースバックおよびリロードすることがある |
| CSCvz53884 | SNMP OID HOST-RESOURCES-MIB（1.3.6.1.2.1.25）が FMC に存在しない |
| CSCvz55140 | CCM レイヤ（スプリント 117、シーケンス 17）での WR6、WR8 および LTS18 コミット ID の更新 |
| CSCvz61456 | 明確な理由がなく ASA アプリケーションのソフトウェアアップグレードが失敗することがある |
| CSCvz61689 | ソフトウェアのアップグレード後にポートチャネル メンバーインターフェイスが失われ、ダウン状態になる |

| 不具合 ID | タイトル |
|---|---|
| CSCvz66474 | snmpd コアファイルが FTD で生成される |
| CSCvz67386 | pmtool コマンドの代わりに Linux コマンドを使用して Snort のステータスとバージョンを取得する |
| CSCvz71596 | 「アクティブとスタンバイのインターフェイスの数が一致していません」という警告の syslog がトリガーされるはずである |
| CSCvz78816 | FO 後にアクティブ IP アドレスとスタンバイ MAC アドレスを使用した SSH セッションと HTTPS セッションが ASA で切断される |
| CSCvz83432 | CCM レイヤ（スプリント 121、シーケンス 18）での WR6、WR8 および LTS18 コミット ID の更新 |
| CSCvz84733 | inline-set を通過する LACP パケットが確認なくドロップされる |
| CSCvz85913 | ASN.1 文字列が、CISCO-SSL-1.0.2 の ASN1_STR として OpenSSL 内で内部的に表される |
| CSCwa00038 | /mnt/disk0 パーティションがいっぱいになってブレードが再起動されるとディスクが破損する |
| CSCwa04262 | Cisco ASA ソフトウェアの SSL VPN クライアント側リクエストの、「/」URI を介したスマグリングの脆弱性 |
| CSCwa05385 | CCM レイヤ（スプリント 124、シーケンス 19）での WR6、WR8 および LTS18 コミット ID の更新 |
| CSCwa20758 | CCM レイヤ（スプリント 124、シーケンス 20）での WR6、WR8 および LTS18 コミット ID の更新 |
| CSCwa32286 | CCM レイヤ（スプリント 125、シーケンス 21）での WR6、WR8 および LTS18 コミット ID の更新 |
| CSCwa36535 | 構成サイズが大きいため、スタンバイユニットがフェールオーバーの参加に失敗 |
| CSCwa42350 | 「利用可能なリソースがモジュールで更新されていません（Available resources not updated by module）」という内部エラーが原因で ASA のインストール/アップグレードが失敗する |
| CSCwa43311 | サイズが大きい（1G）ファイルをダウンロードすると、Snort がパケットをブロックしてドロップする |
| CSCwa43475 | netsnmp_subtree_split での ASA snmpd トレースバック |
| CSCwa46905 | WM 1010 の速度/デュプレックス設定が有効にならず、インターフェイスが不安定になる |

| 不具合 ID | タイトル |
|---|---|
| CSCwa47737 | ASA/FTD が、SNMP 設定の書き込みに関連するウォッチドッグ トレースバックにヒットする可能性がある |
| CSCwa48169 | netsnmp_handler_check_cache 関数での ASA/FTD のトレースバックとリロード |
| CSCwa51241 | スイッチで FPR1140 管理インターフェイスからの不明な MAC アドレスを検出 |
| CSCwa52342 | FTD 6.6.4 SSL ポリシーがダウンロード速度を低下させている |
| CSCwa55562 | 同じ送信元 IP に異なる CG-NAT ポートブロックが割り当てられたことが原因で、ホストごとの PAT ポートブロックが枯渇する |
| CSCwa59907 | LINA は、スレッド名「snmp_client_callback_thread」でトレースバックを観察した |
| CSCwa69009 | トラブルシューティングで、FTD マルチインスタンス Ha ペアのアップグレード中に大量のログが生成される |
| CSCwa72929 | プライバシーアルゴリズムの AES192 または AES256 を使用した場合、SNMPv3 ポーリングが失敗することがある |
| CSCwa76822 | syslog-ng 宛先のスロットリングフロー制御が調整される |
| CSCwa79676 | HA 印刷の FPR1010 で複数のインターフェイスのブロードキャスト ストーム アラートが発生する |
| CSCwb01633 | モジュールの show-tech ファイル生成エラーの根本原因を診断するためのログが FXOS にない |
| CSCwb01983 | Cisco Firepower Management Center のクロスサイト スクリプティングの脆弱性 |
| CSCwb01990 | Cisco Firepower Management Center のクロスサイト スクリプティングの脆弱性 |
| CSCwb01995 | Cisco Firepower Management Center のクロスサイト スクリプティングの脆弱性 |
| CSCwb02018 | Cisco Firepower Management Center のクロスサイト スクリプティングの脆弱性 |
| CSCwb02026 | Cisco Firepower Management Center のクロスサイト スクリプティングの脆弱性 |
| CSCwb05291 | Cisco ASDM および ASA ソフトウェアのクライアント側で任意のコードが実行される脆弱性 |

| 不具合 ID | タイトル |
|---|---|
| CSCwb13294 | CCM レイヤ（シーケンス 25）での WR8、LTS18、および LTS21 コミット ID の更新 |
| CSCwb17206 | FTD マルチインスタンス クラスタリング：RPC_SYSTEMERROR メッセージが表示され、データ ノードが参加できない |
| CSCwb33184 | MessageService のメモリリークが原因で UI が遅くなる |
| CSCwb37737 | FTD Syncd.pl メモリリークにより OOM イベントが発生し、FMC 登録が失敗する |
| CSCwb41854 | Cisco FXOS ソフトウェアおよび Cisco FXOS ソフトウェアのコマンドインジェクションの脆弱性 |
| CSCwb46949 | CCM レイヤ（シーケンス 27）での LTS18 コミット ID の更新 |
| CSCwb61901 | Cisco Firepower Management Center のクロスサイト スクリプティングの脆弱性 |
| CSCwb61908 | Cisco Firepower Management Center のクロスサイト スクリプティングの脆弱性 |
| CSCwb74357 | FXOS はパーティション opt_cisco_platform_logs のログファイルをローテーションしていない |
| CSCwb78971 | 致命的なエラー：アップグレードに失敗した：無効なパスワード：空白またはマスクされたパスワードは使用できない |
| CSCwb80192 | CCM レイヤ（シーケンス 30）での WR6、WR8 コミット ID の更新 |
| CSCwb88587 | Cisco Firepower Management Center のクロスサイト スクリプティングの脆弱性 |
| CSCwb89963 | スレッド名：「Datapath」 での ASA トレースバックとリロード |
| CSCwb92937 | エラー 403：ビューグループオブジェクトでの展開時は禁止されている |
| CSCwb93914 | Cisco ASA ソフトウェアと FTD ソフトウェアの Web サービスインターフェイス拒否攻撃に対する脆弱性である |
| CSCwc01225 | APP SYNC のタイムアウトが原因で状態の進行に失敗したことにより、FTD が HA に参加できない |
| CSCwc02133 | Cisco FXOS ソフトウェアおよび Cisco FXOS ソフトウェアのコマンドインジェクションの脆弱性 |
| CSCwc03507 | CPU ホグの証拠がほとんどないにもかかわらず、内部データインターフェイスでの継続的なバッファなしドロップが発生する |

| 不具合 ID | タイトル |
|---|---|
| CSCwc08676 | CCM レイヤ（シーケンス 32）での WR6、WR8、LTS18、および LTS21 コミット ID の更新 |
| CSCwc09065 | ConcurrentModificationException による APP SYNC タイムアウトが原因で FTD 6.6 HA が失敗した |
| CSCwc10037 | Cisco Firepower Management Center のクロスサイト スクリプティングの脆弱性 |
| CSCwc10792 | ASA/FTD IPSEC のデバッグで、ピアアドレスの変更とタイマー削除の理由が見つからない |
| CSCwc13017 | ../inspect/proxy.h:439 で FTD/ASA のトレースバックとリロードが発生する |
| CSCwc25207 | CCM レイヤ（シーケンス 33）での WR6、WR8、LTS18、および LTS21 コミット ID の更新 |
| CSCwc26648 | ASA/FTD がスレッド名 Lina または Datatath でトレースバックおよびリロードする |
| CSCwc28532 | インラインセットインターフェイスの内部フロー処理によってフラグメント化された GRE トラフィックが原因で、9344 ブロックでリークが発生する |
| CSCwc28806 | プロセス名 Lina で ASA がトレースバックし、リロードする |
| CSCwc28854 | 複数のコンテキストでフェールオーバーが設定されている場合の不適切な IF-MIB 応答である |
| CSCwc32246 | オブジェクトサブネット 0.0.0.0 0.0.0.0 が使用されている場合、NAT64 はすべての IPv6 アドレスを 0.0.0.0/0 に変換する |
| CSCwc35969 | 同様の IP がすでにリストにある場合、イベントから IP をグローバルリスト（ブロックするまたはブロックしない）に追加できない |
| CSCwc36905 | 「slib_malloc.c でヒープ メモリが破損」した結果、ASA がトレースバックしリロードする |
| CSCwc36950 | PM から CriticalStatus を取得する際の操作タイムアウトによる ASA/SFR サービスカードの障害である |
| CSCwc38567 | SCH コードの実行中に ASA/FTD がトレースバックおよびリロードする場合がある |
| CSCwc41661 | ログローテーションの問題が原因で、FTD でサイズが 0 バイトの複数のログファイルがある |
| CSCwc44289 | FTD：IPv4 <> IPv6 NAT 変換を実行するときのトレースバックとリロード |

| 不具合 ID | タイトル |
|---|---|
| CSCwc45108 | ASA/FTD：9344 サイズのブロックリークを引き起こす GTP インスペクション |
| CSCwc45397 | ASA HA：プライマリの復元で、バックアップ後に行われた新しいインターフェイス設定が削除されない |
| CSCwc46569 | CCM レイヤ（シーケンス 34）での WR8、LTS18、および LTS21 コミット ID の更新 |
| CSCwc48375 | インバウンド IPSEC SA が非アクティブのままスタックする：「show crypto ipsec sa」の 1 つのアウトバウンド SPI に対して多数のインバウンド SPI がある |
| CSCwc49095 | フラグメントが結合されて PDTS に送信される場合、ASA/FTD 2100 プラットフォームがトレースバックおよびリロードする |
| CSCwc50887 | FTD：CCL リンク経由でリダイレクトされる UDP フローの NAT IPv4 <> IPv6 でのトレースバックとリロード |
| CSCwc51326 | FXOS ベースの Firepower プラットフォームで、RX リングウォーターマークの値が高いにもかかわらず、「バッファなし」ドロップを示す |
| CSCwc52351 | 「any」およびグローバル IP/範囲がブロードキャスト IP に一致する NAT が原因で起こる ASA/FTD クラスタスプリットブレイン |
| CSCwc53280 | ASA パーサーが OSPF プロセスの下で不完全なネットワークステートメントを受け取り、show run に表示される |
| CSCwc54984 | IKEv2キー の再生成：Create_Child_SA 応答の直後に受信した新しい SPI に対して無効な SPI を応答する |
| CSCwc60037 | ASA が IPSEC エラーでキーの再生成に失敗する: アウトバウンド ハードウェア コンテキストの割り当てに失敗する |
| CSCwc60907 | CCM レイヤ（シーケンス 35）での WR6、WR8、LTS18、および LTS21 コミット ID の更新 |
| CSCwc61912 | ASA/FTD OSPFv3 が IPv6 のメッセージタイプ 8 LSA を生成しない |
| CSCwc62384 | TCP ポート 885 の Cisco FTD キャプティブポータルの脆弱性である |
| CSCwc66757 | ASA/FTD がスレッド名「lina」でトレースバックし、リロードすることがある |
| CSCwc67886 | ASA/FTD がスレッド名「lina_inotify_file_monitor_thread」でトレースバックおよびリロードすることがある |

| 不具合 ID | タイトル |
|---|---|
| CSCwc68969 | SSL ポリシーは、SFR モジュールを使用して特定の Web サイトをブロックしている |
| CSCwc72155 | ASA/FTD が関数「snp_cluster_trans_allocb」でトレースバックおよびリロードする |
| CSCwc72284 | TACACS アカウンティングに、クライアントの誤った IPv6 アドレスが含まれる |
| CSCwc73224 | スタンバイデバイスの Call Home 設定がリロード後に失われる |
| CSCwc74103 | ASA/FTD がスレッド名「DATAPATH-11-32591」でトレースバックおよびリロードすることがある |
| CSCwc79366 | 展開中に、デバイスが構成要求の処理中にスタックする |
| CSCwc79520 | Snort プロセスは ssl_debug_log_config でトレースバックし、コアファイルを生成する可能性がある |
| CSCwc81184 | ASA/FTD が SNMP プロセス障害によりトレースバックおよびリロードする |
| CSCwc81960 | アクセスリストでオブジェクトグループを使用すると、ルート マップで「match ip address」を設定できない |
| CSCwc88897 | DNS インスペクションポリシー変更後の Cisco Umbrella のヌルポインタが原因で ASA がトレースバックおよびリロードする |
| CSCwc90091 | ユーザー統計がある ASA 9.12(4)47 が、「policy-server xxxx global」の可視性に影響する |
| CSCwc93166 | ユーザーコンテキストで write standby を使用すると、セカンダリファイアウォールのライセンスステータスが無効な状態のままになる |
| CSCwc94501 | ASA/FTD が ctm_n5 リセットによりトレースバックする |
| CSCwc96805 | スレッド unicorn の tcp インターセプト統計によりトレースバックおよびリロードする |
| CSCwd00386 | 「snp_clear_acl_log_flow_all」が原因で設定をクリアすると、ASA/FTD がトレースバックおよびリロードすることがある |
| CSCwd00778 | SNMP ポーリングによる ifAdminStatus の出力が異常 |
| CSCwd03731 | 6.4.0.4 から 7.0.x への FPR4110 FTD アップグレードが 901_reapply_sensor_policy.pl で失敗する |

| 不具合 ID | タイトル |
|---|---|
| CSCwd07558 | ASDM によって管理される SFR で 7.0.4 にアップグレードした後、アクセス コントロール ポリシーの展開が失敗する |
| CSCwd11303 | ikev2 プロセスで ASA がトレースバックを生成し、リロードすることがある |
| CSCwd11855 | ASA/FTD がスレッド名「ikev2_fo_event」でトレースバックおよびリロードすることがある |
| CSCwd11963 | ログに表示されるエラーメッセージ「PM からの CriticalStatus の取得でエラー操作がタイムアウトしました（Error operation timed out getting CriticalStatus from PM）」 |
| CSCwd26867 | リブートがトリガーされたら、デバイスがアクティブ状態に移行しない必要がある |
| CSCwd30977 | ポリシーの展開中に生成された誤ったデルタが原因で、FMC はいくつかのアクセスルールを削除した |

# バージョン 6.6.7 で解決済みのバグ

表の最終更新日：2022-07-11

**表 *51* : バージョン *6.6.7* で解決済みのバグ**

| 不具合 ID | タイトル |
|---|---|
| CSCum03297 | 「show processes cpu-hog」出力に MAXHOG タイムスタンプが表示されない |
| CSCvc57575 | ISIS：コンテキストの削除中に無効な ISIS デバッグが表示される |
| CSCvf89237 | CVE-2017-9233 についてのユニコーン企業の評価 |
| 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 |
| CSCvk40714 | リモートストレージの SSH オプションを設定できない |
| CSCvk62945 | ASA：ルートの追加/削除に関する Syslog |
| CSCvo77184 | VMware ASAv は、e1000 ではなく vmxnet3 にデフォルト設定する必要がある |
| CSCvq29993 | FPR2100 のみ：サイズが 80、256、1550 のメモリブロックで永続的なブロックリークとブラックホールトラフィックが発生 |

| 不具合 ID | タイトル |
|---|---|
| CSCvr33586 | FPR1010：しきい値を超えた場合の SSD の温度/警告を追加する |
| CSCvs33392 | サーバーがサポートされていない TLS オプションを使用している場合、既知のキー SSL 復号および接続が失敗することがある |
| CSCvs42388 | 文字列の Gratuitous ロギング：「プリプロセッサのメモリ統計情報が Null」と表示される |
| CSCvv63863 | Firepower 2100：メモリトラッキングに空のコールスタックが表示される |
| 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 |
| CSCvt67167 | スレッド名「logger」で、データユニットがトラフィックなしでトレースバックおよりリロードする |
| CSCvu14647 | FMC HA 同期中にコンフィギュレーション データベース エラーを停止できない |
| CSCvu18510 | MonetDB のイベントデータベースのクラッシュにより、FMC の接続イベントが失われる |
| CSCvu23149 | データベーステーブル rule_opts の SID_GID_ORD インデックスの破損が原因で、FMC でバックアップの生成に失敗する |
| CSCvu91292 | nmap を使用して新しいカスタムアプリケーションが識別されると、Snort が繰り返し再起動する |
| CSCvv17599 | cpe:2.3:o:linux:linux_kernel:4.14.187 の複数の脆弱性 |
| CSCvv27113 | 侵入イベントの ProcessMetadata が間違った local_sid 制約を使用してエントリをルックアップする |
| CSCvv54829 | FPR デバイスが 8GB を超える USB/ペンドライブを認識しない |
| 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 |
| CSCvv83841 | アップグレード：600_schema/100_update_database.sh に十分なルートディスク容量がない |
| CSCvv84172 | 登録失敗時のクラスタ化されたテーブルと EO のダングリング参照 |
| CSCvv91622 | ブロックが設定されている AC ルールを使用すると、「show access list」に時間範囲が表示されない |
| CSCvw01547 | FMC を 6.7.0 から 6.8.0 にアップグレードすると、MI FTD HA で展開が失敗する |

| 不具合 ID | タイトル |
|---|---|
| CSCvw37408 | Perl の 1.643 より前の DBI モジュールで問題が発見された。問題 |
| CSCvw43610 | 9d より前の IJG JPEG（別名 libjpeg）、jmemnob の jpeg_mem_available() |
| CSCvw56551 | インターフェイス設定を変更すると、ASA で NAT の表面的な警告メッセージが表示される |
| CSCvw62288 | ASA：syslog レートが高い場合に 256 バイトのブロックが枯渇する |
| CSCvw82067 | 大量のフラグメント化されたトラフィックにより ASA/FTD 9344 ブロックが枯渇する |
| CSCvw94160 | CIAM：OpenSSL CVE-2020-1971 |
| CSCvx37672 | AC ポリシーに 10,000 を超えるルールがある場合、PDF の生成に失敗して PDF が破損する |
| CSCvx41045 | FMC の sfmbservice で CPU 使用率が高い |
| 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 |
| CSCvx47636 | OpenLDAP 2.4.57 より前の ldap_X509dn2bv で欠陥を発見 |
| CSCvx47643 | 2.4.57 より前の OpenLDAP で slapd クラッシュにつながる欠陥を発見 |
| CSCvx47644 | 2.4.57 より前の OpenLDAP でアサーションにつながる欠陥を発見 |
| CSCvx49600 | 6.6.3-59：FXOS を 2.10.1.106 にアップグレード後、FDM UI にイベントが表示されない |
| CSCvx49717 | 2.66.6 および 2.67.x より前の GNOME GLib で問題を発見 |
| CSCvx51123 | FMC UI エラー：ドメインの保存中にエラーが発生 |
| CSCvx70480 | ポリシーにアクセスすると 403 エラーが発生 -> FMC（4600）から FMCv にユーザーロールをエクスポートした後のアクセス制御 |
| CSCvx78395 | /boot の高いディスク使用率のアラート |
| CSCvx89451 | ISA3000：shutdown コマンドがシステムをシャットダウンする代わりに再起動する |
| CSCvx91317 | MariaDB 10.2 でバージョン 10 より前のリモートコード実行の問題を発見 |
| CSCvx93254 | DHCP リレーサーバーで「無効なヘルパーアドレス」のエラーが発生 |
| CSCvx96024 | ポリシーの展開がタイムアウトで時々失敗する（その後、すべての展開が失敗する) |

| 不具合 ID | タイトル |
|---|---|
| CSCvx97053 | 異なるコンテキストで同じインターフェイスとネットワークにipv6アドレス/プレフィックスを設定できない |
| CSCvy02240 | Cisco Firepower Threat Defense イーサネット産業用プロトコルのポリシーバイパスの脆弱性 |
| CSCvy02247 | Cisco Firepower システム ソフトウェア ルール エディタの影響のないバッファオーバーフローの脆弱性 |
| CSCvy04430 | 管理セッションが数週間後に接続に失敗 |
| CSCvy08351 | 侵入および相関の電子メールアラートがメールサーバーに送信されなくなる |
| CSCvy12991 | シャーシのローカル日付と時刻が、再起動後に 2015 年 1 月 1 日の午前 0 時に戻る場合がある |
| 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 |
| CSCvy16004 | 差分計算の遅延により、展開で問題が発生し、FTD で HA アプリの同期タイムアウト発生の可能性がある |
| CSCvy18138 | 登録フラグ付きのカプセル化されたパケットが RP に送信されたときに、PIM Register Sent カウンタが増加しない |
| CSCvy18166 | 大量のトラフィック ログによる AAB Snort コア |
| CSCvy19170 | SAML：AnyConnect IKEv2 でメモリリークを検出 |
| CSCvy24921 | SNMPv3：構成が変更されるたびに SNMP EngineID が変更される |
| CSCvy30101 | SSL 復号を使用すると、Snort2 のメモリ使用量が予想される制限を超えて増加する可能性がある |
| CSCvy30392 | テーブル ids_event_msg_map の破損した int_id インデックスが原因で、FMC でのバックアップ生成に失敗する |
| 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 |
| CSCvy31521 | syslog-ng モニターを FMC と NGIPS に追加する |
| CSCvy32154 | ポリシーマップでオフロードCLIを無効にした後、フローがオフロードされる |
| CSCvy37484 | device_policy_ref のエントリが大きいため、デバイス管理ページを開くときにパフォーマンスが低下する |

| 不具合 ID | タイトル |
|---|---|
| CSCvy40401 | IPsec の設定で NULL 暗号化を使用すると、L2L VPN セッションの起動が失敗する |
| CSCvy41157 | 復元後に HA 構成に失敗する |
| CSCvy41763 | Cisco Firepower Threat Defense ソフトウェアの XML インジェクションの脆弱性 |
| CSCvy43002 | SNMPWalk + S2S-IKEv2 および AnyConnect TVM プロファイルの実行中にクラッシュを検出 |
| CSCvy60284 | 2.4.56 より前のバージョンの OpenLDAP で欠陥を発見。この欠陥は |
| CSCvy60285 | 2.33 までの GNU C ライブラリ（別名 glibc）の mq_notify 関数にメモリ解放後使用（use-after-free）がある |
| CSCvy60292 | libxml2 の xml エンティティ エンコーディング関数に欠陥がある |
| CSCvy60294 | 2.9.11 より前のバージョンの libxml2 に欠陥がある攻撃者 |
| CSCvy60295 | OpenLDAP で欠陥を発見。openLDAPâETMs slapd サーバーがアサーションエラーをトリガーする。 |
| CSCvy60299 | 5.2 より前の Linux カーネルのブロックサブシステムに、メモリ解放後使用（use-after-free）がある |
| CSCvy60305 | 7.0.11 より前のバージョンの ImageMagick で欠陥を発見。潜在的な暗号リークがある |
| CSCvy60320 | Linux カーネル SCTP ソケット （net/sctp/socket.c）の競合状態 |
| CSCvy60322 | バインド 9.0.0 -> 9.11.29、9.12.0 -> 9.16.13、およびバージョンバインド 9.9.3-S |
| CSCvy60326 | htmldoc 1.9.11 以前の整数オーバーフローにより、攻撃対象になる可能性がある |
| CSCvy60333 | 7.0.8-50 より前の ImageMagick に「初期化されていない値の使用」の脆弱性がある |
| CSCvy63464 | FTD 1100/2100 シリーズがクロックを 2033 に設定してリブートする |
| CSCvy66530 | バージョン 0.12.21~rc より前の lrzsz は、受信側で情報漏洩が発生する可能性がある |
| CSCvy66531 | 2.9.11 より前のバージョンの libxml2 の xmllint に欠陥があるAn atta |
| 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 |

| 不具合 ID | タイトル |
|---|---|
| CSCvy69453 | WM スタンバイデバイスは、再起動後にコールドスタートトラップを送信しない |
| CSCvy69730 | Cisco FMC ソフトウェア設定情報開示の脆弱性 |
| CSCvy72194 | Cisco FMC ソフトウェアにおける設定情報開示の脆弱性 |
| CSCvy73130 | FP4100 プラットフォーム：「show conn」コマンドを実行後、アクティブ/スタンバイがデュアルアクティブに変更される |
| CSCvy73554 | ASA：暗号 ACL の「deny ip any any」エントリにより、IKEv2 リモート AnyConnect アクセス接続が阻止される |
| CSCvy73585 | FMC は、FPR1010 で 8 を超えるポートチャネル ID の設定を許可できない |
| CSCvy75724 | ローエンドプラットフォームでの Msglyr プールメモリの減少による ZMQ OOM |
| CSCvy78209 | Snort が高 CPU 使用率アラートを示すが、top.log には高 CPU 使用率が示されない |
| CSCvy78525 | TCP ping の VRF ルートルックアップがない |
| CSCvy79952 | ダウングレード後の ASA/FTD トレースバックとリロード |
| CSCvy82668 | SSH セッションが解放されない |
| CSCvy89440 | s2sCryptoMap 設定の損失 |
| CSCvy90162 | スケーリングされた AC-SSL-SAML 認証 TVM プロファイルの Unicorn Proxy Thread でのウォッチドッグバーキングのトレースバック |
| CSCvy90821 | 「debug snmp ?」のオートコンプリートが ASA で動作していない |
| CSCvy95329 | AC ルールエントリが見つからないため、アクセスルールが正しく一致しない |
| CSCvy95430 | SNMP MA デバッグトークンの最初の 3 文字が欠落している。 |
| CSCvy95520 | SSH DOS 攻撃を防ぐために、IMS に fail2ban を組み込む |
| CSCvy96895 | フェールオーバー後、ASA がアクティブ IP アドレスとスタンバイ MAC アドレスを使用して VTY セッションを切断する |
| CSCvy99373 | AD で adSamAccountName を解決するときにADI セッション処理が遅延する |
| CSCvz00961 | ASA 設定の切り捨て/破損に関連した AnyConnect 接続障害が発生する |

| 不具合 ID | タイトル |
|---|---|
| CSCvz02076 | Snort のリロードがタイムアウトして再起動する |
| CSCvz05541 | ASA55XX：ソフトウェアアップグレード後に拡張モジュールインターフェイスが起動しない |
| CSCvz05687 | DND フローのフラグメント化された証明書の要求に失敗 |
| CSCvz08387 | ASP ドロップキャプチャ出力に誤ったドロップ理由が表示される場合がある |
| CSCvz09106 | Cisco ASA ソフトウェアと Cisco FTD ソフトウェアの SSL VPN におけるサービス拒否攻撃に対する脆弱性 |
| CSCvz09109 | ヘッダーのみが設定されているにもかかわらず、クラスタ CCL インターフェイスのキャプチャでフルパケットが表示される |
| CSCvz10165 | 6.6.5 リリースのアップグレードシナリオで、FTD デバイスで upgrade_resume.sh CLI を検出できない |
| CSCvz14305 | IKEv2RA サードパーティのデュアルスタック IPv4 および IPv6 が要求されました。ASA は IKEAuth に応答しません |
| CSCvz14377 | MySQL DB と EO から管理者とその他のユーザーが失われる |
| CSCvz15755 | FTD：アップグレード後にポートチャネルが起動せず、コアファイルが生成される場合がある |
| CSCvz19634 | FTD ソフトウェアのアップグレードが 200_pre/505_revert_prep.sh で失敗することがある |
| CSCvz24238 | Cisco Firepower Management Center のクロスサイト スクリプティングの脆弱性 |
| CSCvz24765 | snmpd コアでデバイスが再起動 |
| CSCvz25064 | 2.33 までの GNU C ライブラリ（別名 glibc）の wordexp 関数 |
| CSCvz25066 | 5.13.4 より前の Linux カーネル 3.16 から 5.13.x の fs/seq_file.c |
| CSCvz25454 | ASA：129 行の asp-drop キャプチャにドロップ理由がない |
| CSCvz30558 | Cisco Firepower Management Center のクロスサイト スクリプティングの脆弱性 |
| CSCvz30582 | Cisco Firepower Management Center のクロスサイト スクリプティングの脆弱性 |
| CSCvz31880 | スケーリングストレステストを停止した後、「ユニコーンプロキシスレッド CPU：9 watchdog_cycles」で ASA がクラッシュする。 |

| 不具合 ID | タイトル |
|---|---|
| CSCvz32386 | FMC が同じ暗号マップのエントリに PFS21 および IKEv1 設定をプッシュするときの FTD 展開エラー |
| CSCvz32593 | 無効な状態の QP4110 と QW4115 で CD App Sync エラーが発生し、アクティブなデバイスで Rsync が有効になっていない |
| CSCvz32623 | 2.37.1 までの util-linux の整数オーバーフローが不具合の潜在的な原因となる可能性がある |
| CSCvz35669 | KP-2110 スタンバイで 6.6.4-64 から 7.0.1-30 へのアップグレードが無効になっている「CD アプリ同期エラーはアプリ構成の適用に失敗しました」 |
| CSCvz35787 | 中間フローについて、FTD で誤解を招く OVER_SUBSCRIBED フローフラグが付けられる |
| CSCvz36862 | FMC ポリシーの展開で、フェーズ 3 にかかる時間が 15 分を超える |
| CSCvz36905 | V ルートと同じ v6 ルートを追加すると、重複したエントリが作成される |
| CSCvz36933 | ポリシーの展開時にセンサーの SNMP プロセスが再起動することがある |
| CSCvz38811 | 削除されたファイルが Java プロセスでディスク容量を保持している |
| CSCvz41761 | FMC では、$ 文字を使用した EIGRP 認証秘密鍵の作成は許可されない |
| CSCvz44339 | FTD：NGFW インターフェイスとホストグループが設定された SNMP ホストを削除しようとすると、展開が失敗する |
| CSCvz44645 | FTD がスレッド名「lina」でトレースバックおよびリロードする場合がある |
| CSCvz46333 | 内部ソケット接続の損失による FTD ポリシー展開の失敗 |
| CSCvz46879 | Sourcefire モジュールの mojo_server 設定の微調整 |
| CSCvz47709 | [IMS_7_1_0] アップグレード FMC 7.1.0 での DeployACPolicyPostUpgrade（2022） |
| CSCvz51157 | 2.34 までの GNU C ライブラリ（別名 glibc）の librt、sysdeps/unix/s |
| CSCvz51258 | show tech-support の出力は、crashinfo がある場合に混乱を招く可能性があり、クリーンアップするまたは直感的にする必要がある |
| CSCvz53884 | SNMP OID HOST-RESOURCES-MIB（1.3.6.1.2.1.25）が FMC に存在しない |
| CSCvz53993 | SSL フローでの Snort によるランダムなパケットのブロック |
| CSCvz57917 | /ngfw のアンマネージドディスクの使用率が高くなり、パッケージ フォルダ内が module-xxxx-x86_64.tgz ファイルで一杯になる |

| 不具合 ID | タイトル |
|---|---|
| CSCvz59950 | KP-FPR2130 のスケーリングの長時間テストで IKEv2 がクラッシュする |
| CSCvz60142 | ASA/FTD が SSL 接続の提供を停止する |
| CSCvz61431 | クラスタ構成の同期中に「Netsnmp_update_ma_config: ERROR Failed to build req」メッセージが表示される |
| CSCvz61456 | 明確な理由がなく ASA アプリケーションのソフトウェアアップグレードが失敗することがある |
| CSCvz61658 | update_mem_reference の CPU ホグ |
| CSCvz61689 | ソフトウェアのアップグレード後にポートチャネルメンバーインターフェイスが失われ、ダウン状態になる |
| CSCvz61767 | SNMPv2 または SNMPv1 が設定されたポリシーが展開されない |
| CSCvz62517 | SRU のインストールでは完了時にファイルを検証する必要がある |
| CSCvz63444 | FMC カスタムウィジェットがポーリングし続けてデータを返さない |
| CSCvz64548 | デバイス上の SFTunnel がイベントメッセージを処理しない |
| CSCvz65181 | Cisco Firepower Threat Defense ソフトウェアの セキュリティインテリジェンスにおける DNS フィードバイパスの脆弱性 |
| CSCvz66474 | snmpd コアファイルが FTD で生成される |
| CSCvz67001 | リモート SSH ストレージターゲットへの FMC イベントバックアップが失敗する |
| CSCvz67816 | FTD で変更される IPV6 DNS PTR クエリ |
| CSCvz68336 | 複数のインラインペアでの単一接続が原因で SSL 復号化が機能しない |
| CSCvz69729 | 不安定なクライアントプロセスは、FTD で LINA zmqio トレースバックを引き起こす可能性がある |
| CSCvz69834 | SSL インスペクションで Snort2 を有効にすると、メモリが予想外に増える可能性がある |
| CSCvz70958 | dhcpp_add_ipl_stby が原因でスタンバイのコントロールプレーンの CPU 使用率が高くなる |
| CSCvz71064 | ikev2 トンネルで約 2 分かかる ASA からのコンテキストを削除する |
| CSCvz71569 | プロセス ZeroMQ のメモリ不足状態が原因で FTD のトレースバックとリロードが発生 |

| 不具合 ID | タイトル |
|---|---|
| CSCvz81342 | Diskmanager が AMP ファイルのキャプチャファイルをプルーニングしない |
| CSCvz82562 | ASA/FTD：サイト間 VPN でトラフィックが正しくフラグメント化されていない |
| CSCvz83432 | CCM レイヤ（スプリント 121、シーケンス 18）での WR6、WR8 および LTS18 コミット ID の更新 |
| CSCvz84733 | inline-set を通過する LACP パケットが確認なくドロップされる |
| CSCvz85683 | 414004 に関する間違った syslog メッセージ形式 |
| CSCvz85913 | ASN.1 文字列が、CISCO-SSL-1.0.2 の ASN1_STR として OpenSSL 内で内部的に表される |
| CSCvz86256 | プライマリ ASA は、スプリットブレインが検出され、ピアがコールドスタンバイになるとすぐに GARP を送信する必要がある |
| CSCvz89126 | マルチ コンテキスト スイッチオーバーが ASDM から実行される場合、ASA で ASDM セッション/クォータカウントの不一致が発生する |
| CSCvz90375 | 起動時の ASA 9.14 の使用可能な DMA メモリが不足し、サポートされる AnyConnect セッションが減少する |
| CSCvz90722 | 暗号 ACL のオブジェクトグループでは、ヒットカウントの合計が個々の要素と一致しない |
| CSCvz91218 | 高速トラフィックでのインターフェイスリングのドロップにより、スタンバイユニットで Statelink hello メッセージがドロップした |
| CSCvz91618 | KP：SNMP ホストグループの追加および削除時のトレースバックを検出 |
| CSCvz95949 | FP1120 9.14.3：アクティブなデバイスの再起動後に一時的なスプリットブレインが発生 |
| CSCvz96462 | VPN セッションはないが、IP アドレスが「使用中」になる |
| CSCwa00038 | /mnt/disk0 パーティションがいっぱいになってブレードが再起動されるとディスクが破損する |
| CSCwa04134 | 5.9.4 より前の strongSwan のインメモリ証明書キャッシュに remot がある |
| CSCwa04395 | ユーザー エージェント セッションの処理により、6.6.5 スタンドアロンセンサーで SFDataCorrelator がクラッシュする |
| CSCwa05385 | CCM レイヤ（スプリント 124、シーケンス 19）での WR6、WR8 および LTS18 コミット ID の更新 |

| 不具合 ID | タイトル |
|---|---|
| CSCwa06960 | 内部ヘルステスト中にCTMデーモンが原因でASAのトレースバックとリロードが発生 |
| CSCwa11079 | DRBG ヘルス テスト用のサブコンテキストの事前割り当て |
| CSCwa11088 | ページの更新/読み込み前に編集しようとすると、制御ルールの順序が自動的に変更される |
| CSCwa11186 | AAA LDAP デバッグで機密情報がマスクされる |
| CSCwa13873 | 「failover active」コマンドの実行後に、状態遷移における遅延が原因でASA フェールオーバー スプリット ブレインが発生 |
| CSCwa15291 | 偽造されたリクエスト uri-path により mod_proxy がそのリクエストを送信元サーバーに転送する可能性がある |
| CSCwa18858 | ASA が、「ラベル長 164 バイトがプロトコルの制限である 63 バイトを超えている」という理由で非 DNS トラフィックをドロップする |
| CSCwa19713 | asp ドロップタイプ「no-adjacency」が原因でBVIインターフェイスで設定された ASA によってトラフィックがドロップした |
| CSCwa20516 | FMC ポリシーの展開に 14 分以上かかる |
| CSCwa20758 | CCM レイヤ（スプリント 124、シーケンス 20）での WR6、WR8 および LTS18 コミット ID の更新 |
| CSCwa26038 | ICMPインスペクションにより、適切にログに記録されないパケットドロップが発生する |
| CSCwa27822 | 6.7 または 7.0 への FTD のメジャーアップグレード後、Lina プロセスが開始状態のままになる |
| CSCwa28822 | FTD が UI 管理を FDM から FMC に移すと、トラフィックエラーが発生する |
| CSCwa30114 | オブジェクトサービスでポートの範囲を使用すると、「NATがポートを予約できません」というエラーが発生 |
| CSCwa31373 | ルールをコピーすると、FMC 6.6.5 で重複する ACP ルールが生成される |
| CSCwa32286 | CCM レイヤ（スプリント 125、シーケンス 21）での WR6、WR8 および LTS18 コミット ID の更新 |
| CSCwa32527 | ngfw-management インターフェイスで SNMP が設定されている場合、7.1 から 7.2 へのアップグレードがクラッシュする |

| 不具合 ID | タイトル |
|---|---|
| CSCwa33364 | MR ブランチで見られる中間フローの問題について、FTD で誤解を招く OVER_SUBSCRIBED フローフラグが付けられる |
| CSCwa35200 | AnyConnect SSL の一部の syslog が、ユーザーコンテキストではなく管理コンテキストで生成される |
| CSCwa36661 | ASP テーブル内にルートがないため、トラフィックがユーザー VRF の一部の出力インターフェイスにヒットしない |
| CSCwa36672 | ASDM を使用してキャプチャを実行するとき、FPR4100 の ASA でトレースバックとリロードが発生する |
| CSCwa36678 | FMC からの展開中にトレースバックを使用してランダム FTD がリロードされる |
| CSCwa40223 | Cisco Firepower Management Center ソフトウェアのクロスサイト スクリプティングに対する脆弱性 |
| CSCwa40237 | Cisco Firepower Management Center で確認されたファイル アップロード セキュリティがバイパスされる脆弱性 |
| CSCwa40719 | トレースバック：セカンダリファイアウォールがスレッド名「fover_parse」でリロード |
| CSCwa42350 | 「利用可能なリソースがモジュールで更新されていません（Available resources not updated by module）」という内部エラーが原因で ASA のインストール/アップグレードが失敗する |
| CSCwa43475 | netsnmp_subtree_split での ASA snmpd トレースバック |
| CSCwa43497 | AnyConnect-SSL の ICMP PMTU を送信するときにデータパスのデッドロックが発生する |
| CSCwa46963 | セキュリティ：CVE-2021-44228 → Log4j 2 における脆弱性 |
| CSCwa50145 | FPR8000 センサーの UI ログインにより、基本的な権限を持つシェルユーザーが作成される |
| CSCwa51241 | スイッチで FPR1140 管理インターフェイスからの不明な MAC アドレスを検出 |
| CSCwa53489 | ハッシュテーブルへのアクセス中に無効なメモリアクセスが原因で Lina のトレースバックとリロードが発生する |
| CSCwa55418 | アップグレード前に AnyConnect パッケージを使用して展開すると、複数の DB フォルダ current-policy-bundle が生成される |
| CSCwa56449 | HTTP cli EXEC コードで ASA のトレースバックが発生する |

| 不具合 ID | タイトル |
|---|---|
| CSCwa56975 | コントロールプレーンで DHCP オファーが表示されない |
| CSCwa57115 | オブジェクトで存在しない ACL を削除した後、新しいアクセスリストが有効にならない |
| CSCwa60574 | snp_ha_trans_alloc_msg_muxbuf_space 関数で ASA のトレースバックとリロードが発生する |
| CSCwa61218 | OID「1.3.6.1.4.1.9.9.171.1.3.2.1.2」をポーリングすると、関連するトンネルの負のインデックス値が得られる |
| CSCwa61361 | PBR で SD_WAN ACL を有効にしてから無効にした場合（またはその逆）に ASAv のトレースバックが発生する |
| CSCwa62025 | IPv6：グローバルおよびユーザー VRF ルートの出力インターフェースの一部が ASP テーブルに存在しない |
| CSCwa65389 | ASDM を介してインターフェイス設定を変更すると、Unicorn Admin Handler で ASA のトレースバックとリロードが発生する |
| CSCwa67884 | 条件付きフローオフロードのデバッグで出力が生成されない |
| CSCwa68660 | ASA を 9.12.4.x にアップグレードした後、FTP インスペクションが正しく機能しなくなる |
| CSCwa70029 | ソフトウェアアップグレード後の静的ルートに対する FDM UI と CLI の不一致 |
| CSCwa72530 | FTD：新しいノードがクラスタ制御ノードに参加するときに、履歴に表示される時間のギャップ/不一致 |
| CSCwa73172 | スレッド名「PIX Garbage Collector」で ASA のリロードとトレースバックが発生する |
| CSCwa74900 | debug webvpn cifs 255 を有効にすると、トレースバックとリロードが発生する |
| CSCwa75077 | プレフィルタルールに時間範囲オブジェクトが誤って入力される |
| CSCwa75966 | ASA：ページ違反のあるスレッド名 Unicorn Proxy Thread でのリロードとトレースバック：アドレスがマッピングされていない |
| CSCwa76564 | フェールオーバーの前後にマルチコンテキストが切り替わるとき、ASA で ASDM セッション/クォータ件数の不一致が発生する |
| CSCwa76822 | syslog-ng 宛先のスロットリングフロー制御が調整される |
| CSCwa77073 | SNMP が予期しない結果の順序で snmpgetbulk に応答している |

| 不具合 ID | タイトル |
|---|---|
| CSCwa77083 | ネットワーク検出ルールでセキュリティゾーンが設定されている場合、ホスト情報が欠落する |
| CSCwa78082 | FMC 侵入イベント検索の結果が一貫していない |
| CSCwa79494 | スポークからの IPSec トンネルがフラッピングすると、ハブでトラフィックエラーが継続的に発生する |
| CSCwa79676 | HA 印刷の FPR1010 で複数のインターフェイスのブロードキャスト ストーム アラートが発生する |
| CSCwa79980 | FPR の SNMP get コマンドがインターフェイスインデックスを表示しない |
| CSCwa85043 | トレースバック：ASA/FTD がスレッド名「Logger」でトレースバックおよびリロードする場合がある |
| CSCwa85138 | トランザクションコミット診断に関する複数の問題が発生する |
| CSCwa85340 | ネストされた大きいオブジェクトを含むアクセスポリシーで PDF を生成できない |
| CSCwa86210 | PM が mysqld を無効にすると、完全にシャットダウンするまでに予想以上に時間がかかることがある |
| CSCwa87315 | ASA/FTD が、スレッド名「IP Address Assign」でトレースバックおよびリロードする場合がある |
| CSCwa87597 | ASA/FTD フェールオーバー：アクティブユニットから設定の複製を受信すると、スタンバイユニットがリブートする |
| CSCwa88571 | スマートポータルを使用して FMC を登録できない |
| CSCwa91070 | バックアッププロセスの oom-k をトリガーする Cgroup |
| CSCwa94894 | ASA/FTD は、スレッド名「DATAPATH-4-9608」でトレースバックおよびリロードする場合がある |
| CSCwa95079 | NAT 設定に起因する ASA/FTD トレースバックとリロード |
| CSCwa96759 | Lina が tcpmod_proxy_handle_mixed_mode でトレースバックおよびリロードする場合がある |
| CSCwa97784 | ASA：ジャンボサイズのパケットが L2TP トンネル上でフラグメント化されない |
| CSCwa98684 | ポリシーの展開中にコンソールに過度の警告が発生する |
| CSCwa98853 | エラー F0854：FDM Keyring の RSA 係数が無効です（FDM Keyring's RSA modulus is invalid） |

| 不具合 ID | タイトル |
|---|---|
| CSCwa98983 | FPR2100-HA でのアップグレードが 800_post/901_reapply_sensor_policy.pl で失敗した |
| CSCwa99931 | 「update_mem_reference」プロセスで、HA ペアの CPU 使用率が高くなる |
| CSCwb01700 | ASA：SSH と ASDM セッションが CLOSE_WAIT でスタックし、ASA の MGMT が不足する |
| CSCwb01919 | FP2140 ASA 9.16.2 HA ユニットが lua_getinfo（getfuncname）でトレースバックおよびリロードする |
| CSCwb02316 | MAC アドレス設定中のエラー「「1」ではノンストップフォワーディングはサポートされません（Non stop forwarding not supported on '1'）」 |
| CSCwb06847 | ASA/FTD がスレッド名「DATAPATH-9-11543」でトレースバックおよびリロードする場合がある |
| CSCwb07908 | スタンバイ FTD/ASA が 0.0.0.0 の送信元 IP で DNS クエリを送信する |
| CSCwb07981 | トレースバック：スタンバイ FTD が再起動し、スレッド名 cli_xml_server でクラッシュ情報と lina コアを生成する |
| CSCwb08644 | Scaled S2S+AC-DTLS+SNMP の長時間テストからの IKEv2 における ASA/FTD のトレースバックとリロード |
| CSCwb11939 | ASA/FTD MAC の変更が、INSPECT がオンになっているフラグメント化されたパケットの処理で見られる |
| CSCwb12730 | FMC でのポリシー展開に失敗したが、FTD 展開ステータスは「INPROGRESS」を示している |
| CSCwb17206 | FTD マルチインスタンスクラスタリング：RPC_SYSTEMERROR メッセージが表示され、データノードが参加できない |
| CSCwb18252 | FTD/ASA：BFD 機能のトレースバックにより予期しないリブートを引き起こす |
| CSCwb19648 | crasLocalAddress の SNMP クエリで SSL/DTLS トンネルに割り当てられた IP が返されない |
| CSCwb24039 | ルーティングでの ASA のトレースバックとリロード |
| CSCwb25809 | シングルパス：古い ifc が原因でトレースバック |
| CSCwb28849 | ASA/FTD：OpenSSL の脆弱性 CVE-2022-0778 の緩和 |
| CSCwb32068 | Firepower Management Center での自動ダウンロード VDB の失敗 |

| 不具合 ID | タイトル |
|---|---|
| CSCwb32418 | Cisco FirePOWER Software for ASA FirePOWER モジュールのコマンドインジェクションの脆弱性 |
| CSCwb33334 | ASA：RAVPN トンネル経由で一部のトラフィックを送信した後にクラッシュする |
| CSCwb39431 | RFC5424 標準に従って FTD 統合ログのログが出力されない |
| CSCwb51707 | プロセス名 lina で ASA がトレースバックおよびリロードする |
| CSCwb53172 | FTD：IKEv2 トンネルが 24 時間ごとにフラップし、暗号アーカイブが生成される |
| CSCwb54791 | ASA DHCP サーバーが予約済みアドレスを Linux デバイスにバインドできない |
| CSCwb57615 | 行番号を使用した pbr アクセスリストの設定に失敗した。 |
| CSCwb59465 | VPN フェールオーバー サブシステムから syslog を生成するときに、ASA/FTD がトレースバック（ウォッチドッグ）してリロードする場合がある |
| CSCwb59488 | メモリ割り当てでの ASA/FTD のトレースバックが失敗した |
| CSCwb65447 | FTD：AAB コアが不完全で、復号されていない |
| CSCwb65718 | [SIオブジェクト（SI objects）] ページのロード時に FMC がスタックする |
| CSCwb67040 | FP4112\|4115：スレッド名 netfs_thread_init でのトレースバックとリロード |
| CSCwb68642 | スレッド名 SXP CORE での ASA のトレースバック |
| CSCwb71460 | スレッド名 fover_parse での ASA トレースバックが SNMP 関連機能によってトリガーされる |
| CSCwb74938 | ASA のトレースバックとリロードでエラー「"assertion "0" failed: file "timer_services.c", line 165」が表示される |
| CSCwb80559 | オフロードすべきでない SGT タグ付きパケットが FTD でオフロードされる |
| CSCwb82796 | IKE トンネルを切断すると、ASA/FTD ファイアウォールがトレースバックおよびリロードすることがある |
| CSCwb83388 | ASA HA アクティブ/スタンバイトレースバックが、約 2 ヵ月ごとに確認される。 |
| CSCwb85633 | メモリの snmpwalk 出力が show memory/show memory details と一致しない |

| 不具合 ID | タイトル |
|---|---|
| CSCwb86118 | TPK ASA：ディスクへの ftp コピー時にデバイスがスタックすることがある |
| CSCwb87498 | EIGRP ルート更新処理中の Lina のトレースバックとリロード。 |
| CSCwb89187 | Flex Config 許可：「timeout icmp-error hh:mm:ss」 |
| CSCwb90074 | ASA：マルチコンテキスト混合モード SFR リダイレクションの検証 |
| CSCwb93932 | タイマー サービス アサーションによる ASA/FTD のトレースバックとリロード |

# バージョン 6.6.5.2 で解決済みのバグ

表の最終更新日：2022-03-17

**表 *52 :* バージョン *6.6.5.2* で解決済みのバグ**

| 不具合 ID | タイトル |
|---|---|
| CSCvs42388 | 文字列の Gratuitous ロギング：「プリプロセッサのメモリ統計情報が Null」と表示される |
| CSCvx76665 | 2100 および 1010 で表示される「インターフェイスのアップデートに失敗しました」というエラーメッセージ |
| CSCvx78968 | スレッド名での ASA および FTD のトレースバックとリロード：VTI が設定された IKEv2 デーモン |
| CSCvy60831 | ASA および FTD メモリブロックの位置がデータパスでの断片化されたパケットに対して更新されない |
| CSCvy89440 | s2sCryptoMap 設定の損失 |
| CSCvz02076 | Snort のリロードがタイムアウトして再起動する |
| CSCvz02398 | 7.0 での SE リングタイムアウトで生成された暗号アーカイブ |
| CSCvz03524 | sha1 ではなく sha256 リクエストが原因で PKI の「OCSP 失効チェック」が失敗する |
| CSCvz32386 | FMC が同じ暗号マップのエントリに PFS21 および IKEv1 設定をプッシュするときの FTD 展開エラー |
| CSCvz33468 | FQDN_NAT で object-group/ nat のヒットカウントの変更が更新されないと、NAT が動作しなくなる |

| 不具合 ID | タイトル |
|---|---|
| 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 |
| CSCvz53993 | SSL フローでの Snort によるランダムなパケットのブロック |
| CSCvz55849 | LINA プロセスでの 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 |
| CSCvz76746 | 管理トンネルを実装している間、ユーザーはオープン接続を使用して AnyConnect をバイパスできる |
| CSCvz85437 | FXOS および FTD を 2.10.1.159 および 6.6.4 にアップグレードした後に FTD 100G のインターフェイスがダウンする |
| CSCvz89327 | OSPFv2 フローにクラスター集中型「c」フラグがない |
| CSCvz89545 | アップグレード後の SSL VPN のパフォーマンスの低下と重大な安定性に関する問題 |
| CSCvz92932 | ASA show tech の実行により、CPU でスパイクが発生し、IKEv2 セッションに影響を与える |
| CSCvz94153 | IPV4 アドレスが設定されていない場合、IPV6 での NTP 同期が失敗する |
| CSCvz95108 | デバイスでのメジャーバージョンの変更によるアップグレード後の FTD 展開の失敗 |
| CSCwa02929 | FTD が SSL フローエラーの CORRUPT_MESSAGE でトラフィックをブロックする |
| CSCwa03275 | BGP ルートが未解決と表示され、「ホストへのルートがありません」という ASP のドロップが原因となりパケットをドロップする |
| CSCwa03347 | IPv6 PIM パケットが、無効な IP の長さによるドロップが原因となり ASP でドロップする |
| CSCwa08262 | マッピングされたグループポリシーを持つ AnyConnect ユーザーは、トンネルグループの下にあるデフォルト GP から属性を取得する |
| CSCwa11052 | バージョン 9.14(2)15 へのアップグレード後に SNMP が応答しなくなる |
| CSCwa14725 | IKE デーモンスレッドでの ASA および FTD のトレースバックとリロード |
| CSCwa19443 | フローオフロード - 比較状態の値が長期間エラー状態のままになる |
| CSCwa20516 | FMC ポリシーの展開に 14 分以上かかる |

| 不具合 ID | タイトル |
|---|---|
| CSCwa28895 | FTD SSL プロキシは、設定可能または動的な最大 TCP ウィンドウサイズを許可する必要がある |
| CSCwa46963 | セキュリティ：CVE-2021-44228 → Log4j 2 における脆弱性 |
| CSCwa55878 | FTD サービスモジュールの障害：「ND がダウンした可能性があります」という誤ったアラーム |
| CSCwa58686 | OGS コンパイル動作における ASA および FTD の変更によりブートループが発生する |
| CSCwa67882 | オフロードされた GRE トンネルは、サイレントにオフロードを解除し、CPU にパントされる場合がある |
| CSCwa70008 | 期限切れの証明書により、セキュリティインテリジェンスの更新が失敗する |
| 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 6.6.5.1 で解決済みのバグ

表の最終更新日：2021-12-06

**表 *53* : バージョン *6.6.5.1* で解決済みのバグ**

| 不具合 ID | タイトル |
|---|---|
| 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 |
| 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 |
| CSCvs27336 | Smart Call Home プロセスにより ASA がトレースバックする |
| CSCvs61701 | Firepower 2100 のメモリリークが原因で DME のプロセスがクラッシュする |
| CSCvv43190 | GRE ヘッダープロトコルフィールドが内部 IP ヘッダーのプロトコルフィールドと一致しない場合の暗号エンジンエラー |
| CSCvv48942 | Snmpwalk がフェールオーバーインターフェイスのトラフィックカウンターを 0 として表示する |
| 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 |

| 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 |
| 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%） |
| CSCvx65178 | ファイアウォール MIB 内の特定の OID に対して SNMP 一括取得が機能せず、デバイスのパフォーマンスが低下する |
| 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 |
| CSCvx90486 | ifXTable の snmpwalk がデータインターフェイスを返さないことがある |
| 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 |
| CSCvy02247 | Cisco Firepower システム ソフトウェア ルール エディタの影響のないバッファオーバーフローの脆弱性 |
| CSCvy04343 | PLR モードの ASA で「ライセンスのスマート予約」が失敗する。 |
| CSCvy09436 | DHCP 予約で一部のデバイスに予約済みアドレスを適用できない |
| CSCvy10583 | スレッド名 DATAPATH での ASA トレースバックおよびリロード |
| 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 |
| 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 |
| 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 |
| CSCvy27283 | プライバシーアルゴリズムの AES192 または AES256 を使用した場合、ASA または FTD の SNMPv3 ポーリングが失敗することがある |
| CSCvy31229 | /ngfwに空き領域がない |
| CSCvy33105 | DNS ルックアップが有効な場合、「show route bgp」または「show route isis」であいまいなコマンドエラーが表示される |
| CSCvy33676 | 以前の動的 xlate が作成されると、FTD で UN-NAT が作成される |
| 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 |

| 不具合 ID | タイトル |
|---|---|
| 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 |
| CSCvy43447 | マルチインスタンス FTD の Lic TMR スレッドでの FTDトレースバックとリロード |
| CSCvy47108 | UAuth エントリがスタックしているため、リモートアクセス IKEv2 VPN セッションを確立できない |
| CSCvy48159 | メモリヘッダー検証によるプロセス名 lina での ASA トレースバックとリロード |
| CSCvy49732 | ASA/FTD がスレッド名「ssh」でトレースバックし、リロードすることがある |
| CSCvy50011 | IKE デーモンプロセスでの ASA トレースバックおよびリロード |
| CSCvy51659 | OCSP タイムアウトが長い場合、AnyConnect 認証が失敗することがある |
| CSCvy51814 | Firepower フローオフロードが、すべての既存およびおよび新しいフローのオフロードを停止させる |
| CSCvy52074 | ASA/FTD がスレッド名「webvpn_task」でトレースバックおよびリロードすることがある |
| CSCvy52924 | FTD がリブート時にすべての VRF インスタンスの OSPF ネットワークステートメント設定を失う |
| 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 |
| CSCvy56395 | キー設定が存在する場合の SNMP 暗号化コミュニティストリングによる ASA トレースバックとリロード |
| 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 |
| CSCvy58268 | ブロック 80 および 256 の枯渇スナップショットが作成されない |
| CSCvy60100 | HA の再起動後に SNMP v3 設定が失われる |
| 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 |

| 不具合 ID | タイトル |
|---|---|
| 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 |
| CSCvy72194 | Cisco FMC ソフトウェアにおける設定情報開示の脆弱性 |
| 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 |
| CSCvy74984 | デフォルトの外部ルートが使用されると、Azure 上の ASAv がメタデータサーバーへの接続を失う |
| CSCvy82794 | snmp コマンドを無効にする場合の ASA/FTD トレースバックとリロード |
| CSCvy90836 | スレッド名 SNMP ContextThread での ASA トレースバックおよびリロード |
| 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る。 |
| 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」を復元する |
| CSCvy96803 | SNMP 機能に関連するプロセス名 lina の FTD トレースバックとリロード |
| 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 |
| 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 |

| 不具合 ID | タイトル |
|---|---|
| CSCvz21886 | nat が IP ではなくポート番号に一致する pbr ACL に一致した場合、nat の un-nat が 2 回発生しない |
| CSCvz23157 | show コマンドが発行されると SNMP エージェントが再起動する |
| CSCvz25434 | BVI が DHCP クライアントとして設定されている場合、1550 ブロックの枯渇が原因で ASA および FTD がトラフィックをブラックホールする |
| CSCvz27235 | 複数のシスコ製品の Snort Modbus におけるサービス妨害の脆弱性 |
| CSCvz29233 | ASA：システムコンテキストでインターフェイスのフラップが発生したときに、カスタムコンテキストからの ARP エントリが削除されない |
| CSCvz30333 | 「show capture」コマンドが実行されると、FTD または Lina がトレースバックすることがある |
| CSCvz30933 | clear configure snmp-server コマンドが発行されると ASA のトレースバックとリロードが発生する |
| 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 |
| CSCvz38332 | FTD または ASA - 9.14.2.15 から 9.14.3 へのアップグレード後にブートループでスタックする |
| 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 |
| CSCvz38692 | snmp_master_callback_thread での ASAv のトレースバックとリロード |
| 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 |
| CSCvz43414 | HA のフェー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 |
| CSCvz58710 | SCTP トラフィックにより ASA がトレースバックする。 |

| 不具合 ID | タイトル |
|---|---|
| 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 |
| CSCvz61160 | ICMP エラーメッセージを処理する際、DATAPATH で ASA がトレースバックする |
| 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 |
| 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 |
| CSCvz73146 | FTD：スレッド名 DATAPATH でのトレースバック |
| 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 |
| CSCvz75988 | RFC5424 が有効な場合、一貫性のないロギングタイムスタンプが起こる |
| 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 |
| 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 |

# バージョン 6.6.5 で解決済みのバグ

表の最終更新日：2021-08-03

**表 *54* : バージョン *6.6.5* で解決済みのバグ**

| 不具合 ID | タイトル |
|---|---|
| CSCvf88062 | CTM：Nitrox S/G の長さを検証する必要がある |
| CSCvg69380 | ASA：まれに発生した CP 処理での破損によってコンソールロックが発生する |
| CSCvh19737 | FTD データインターフェイス（オフボックス管理）での HTTPS アクセスが失敗する |
| CSCvi96835 | ルーティングポリシーで使用されるグループオブジェクトの一部であるホストを範囲に変更しても検証エラーが発生しない |
| CSCvj08826 | FMC ibdata1 ファイルのサイズが大きくなることがある |
| CSCvm82290 | IRB/TFW 設定でホストが到達不能な場合に ASA コアブロックが枯渇する |

| 不具合 ID | タイトル |
|---|---|
| CSCvo34210 | スレッド名 Unicorn Proxy Thread で ASA が 9.6.4.20 トレースバックを実行する |
| CSCvp13352 | VPN セッションがタイムアウトした後でも、ASA はクライアント側接続に対する TCP キープアライブを実行し続ける |
| CSCvp15559 | 設定同期中にセカンダリ ASA でトレースバックが発生する |
| CSCvp28713 | パケットトレーサーの RESULT の入出力インターフェイスが「UNKNOWN」と表示される |
| CSCvp69936 | ASA：tcp_intercept スレッド名 thread detection でのトレースバック |
| CSCvq98396 | ASA：暗号化セッションがスタンバイユニットでリークを処理する |
| CSCvr11958 | AWS FTD：「ERROR: failed to set interface to promiscuous mode」により展開が失敗する |
| CSCvr33428 | FMC が SYN フラッド攻撃から接続イベントを生成する |
| CSCvr77005 | インターフェイスが使用可能になると、トラフィックが暗号マップからプライマリインターフェイスにフォールバックしない |
| CSCvr85295 | Cisco Adaptive Security Appliance と Firepower Threat Defense ソフトウェア リモート |
| CSCvs13204 | SR-IOV インターフェイス上の ASAv フェールオーバー トラフィックが、インターフェイスのダウンによりドロップされることがある |
| CSCvs50538 | SSL エンジンが判定を返さない場合、ファイアウォールエンジンは SSL ハンドシェイクからの情報にフォールバックする必要がある |
| CSCvs72390 | Cisco Firepower Management Center のクロスサイト スクリプティングの脆弱性 |
| CSCvs72450 | FXOS：サービスモジュールの hwclock を同時書き込みコリジョンによる破損から修復 |
| CSCvs74802 | AnyConnect または S2S IKEv2 暗号化ポリシーがデバイスに展開されないことがある |
| CSCvs82926 | ASA「Chassis 0 Cooling Fan OK」SCH メッセージを使用した FRP 1000 および FPR2100 シリーズの重大な RPMアラート |
| CSCvs84542 | スレッド idfw_proc での ASA のトレースバック |
| CSCvs95188 | 異なるインスタンス間で共有される FXOS FTD マルチインスタンス CPU コア |

| 不具合 ID | タイトル |
|---|---|
| CSCvt10944 | VTI トンネル経由で EMIX トラフィックを送信しているときに CTM がクラッシュした |
| CSCvt11885 | 移行スクリプトの実行がメモリ不足エラーで終了する |
| CSCvt37303 | プレフィルタールールゾーンの検証（アクティビティの検証）が、UI の HW レイヤーでバイパスされる |
| CSCvt39977 | PSNG_TCP_PORTSCAN [122:1:1] ルールアラートの場合の無効なパケットデータ |
| CSCvt48260 | スタンバイユニットがアクティブユニットを検出すると、fover_parse でトレースバックしてブートループする |
| CSCvt52604 | FMC の [オブジェクト（Objects）] セクションから [インターフェイス（Interfaces）] ページがロードされない（ドメインページも影響を受けることがある） |
| CSCvt55927 | 6.4.0.9-34 FDM で HA を解除できない |
| CSCvt71529 | SSL ハンドシェイク中の ASA のトレースバックとリロード |
| CSCvt74194 | unified2 レコード取得中のエラー：ファイルの破損 |
| CSCvt75760 | HTTP クリーンアップによるクライアントレス WebVPN のトレースバックまたはページ障害 |
| CSCvt92077 | ASAv での ping の失敗：9.13（CAT9k の再起動後） |
| CSCvt97205 | ASA 9.14.1 上で SNMPPOLL/SNMPTRAP からリモートエンド（サイト間 VPN）ASA インターフェイスが失敗する |
| CSCvu02594 | 非同期セッションが多すぎるため、Snort の終了に時間がかかる |
| CSCvu09496 | 多くの ACP で同じ DNS ポリシーが参照されると、DNS データが繰り返し収集されエクスポートされる |
| CSCvu18510 | MonetDB のイベントデータベースのクラッシュにより、FMC 6.6.0 および 6.6.1 の接続イベントが失われる |
| CSCvu30704 | サイズ「0」のクラッシュ情報により ASA がトレースバックする |
| CSCvu33992 | トレースバック：ASA が lina_sigcrash+1394 をリロードした |
| CSCvu44472 | FMC システムプロセスが起動する |
| CSCvu75855 | 有効になるべきではないときに、管理対象デバイスで stunnel プロセスが有効になる |

| 不具合 ID | タイトル |
|---|---|
| CSCvu77689 | FileZilla への FTP が SMTP に誤って分類される |
| CSCvu82680 | パフォーマンスファイルの一部が、本来は含まれないはずの FTD バックアップの一部として含まれている |
| CSCvu84127 | 明確な理由なしに Firepower がリブートすることがある |
| CSCvu87906 | バックアップファイルが 6.6.0 ～ 90 で増大し続ける（統合イベントファイルが誤ってバックアップに含まれる） |
| CSCvu89110 | ASA：「logging permit-hostdown」が設定され、TCP syslog がダウンしている場合も新しい接続をブロックする |
| CSCvu94878 | OpenSSH 5.7 ～ 8.3 のクライアント側に、Observable Discrepan がある |
| CSCvu97112 | SNMP ポーリングが HA のアクティブデバイスで動作を停止した |
| CSCvu97242 | 2100：クラッシュが発生すると、コアファイルとクラッシュ情報の両方が切り捨てられ、不完全になる可能性がある |
| CSCvu98222 | SSL 復号ポリシーを有効にした後、FTD Lina エンジンがデータパスでトレースバックすることがある |
| CSCvv00719 | 時間範囲オブジェクトを含むアクセス コントロール ポリシーがヒットしない |
| CSCvv02925 | OSPF ネイバーシップが確立されていない |
| CSCvv07917 | ASA が新しいルートを学習すると、フローティングスタティックによって作成された ASP ルートテーブルが削除される |
| CSCvv10778 | 9.12.4 へのアップグレード後のスレッド名 DATAPATH（5585）または Lina（2100）のトレースバック |
| CSCvv15572 | 新しいコンテキストの作成中に「config-url」を入力すると、ASA のトレースバックが発生する |
| CSCvv17585 | 特定の状況下で Netflow テンプレートが送信されない |
| CSCvv19230 | ASAv AnyConnect ユーザーがアイドルタイムアウトで予期せず切断される |
| CSCvv20780 | ポリシーの展開が「展開トランザクションを保持できませんでした」エラーで失敗する |
| CSCvv24647 | FP2100-SNMP：不正な値がイーサネット統計ポーリングに返される |
| CSCvv24976 | RRI ルートインターフェイスをシャットダウンした後、静的デフォルトルートがリブにインストールされない |

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

| 不具合 ID | タイトル |
|---|---|
| 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 |
| CSCvv58332 | ASA/FTD が BGP MP_REACH_NLRI 属性のネクストホップバイトを逆順で読み取る |
| CSCvv62305 | フェールオーバーペアに参加しようとした場合の fover_parse での ASA トレースバックとリロード |
| CSCvv63412 | tmatch のコンパイルが進行中のとき、ASA がすべてのトラフィックを理由「No route to host」でドロップする |
| CSCvv64068 | ネットワーク/サービスオブジェクト名の変更後、syslog の ACL のハッシュ値で不一致が発生する |
| CSCvv65184 | Cisco 適応型セキュリティアプライアンスと Firepower Threat Defense ソフトウェアの Web DoS の脆弱性 |
| CSCvv66005 | inspect esmtp での ASA のトレースバックとリロード |
| CSCvv66561 | ssh pubkey-chain サーバーでのキー文字列のサポートが意図したとおりに機能しない。 |
| CSCvv66920 | 内部フロー：U ターン GRE フローが不正な接続フローの作成をトリガーする |
| CSCvv67196 | FTD が crl ファイルを取得するためにすべての crl URL を試行しない |
| CSCvv67398 | SNMP が無効な場合、Inspect-snmp で thru-the-box snmp paks がドロップされる |
| 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 |
| CSCvv68669 | 分類の失敗により、マスター ASA のシステムコンテキストで仮想 IP アドレスへのトラフィックがドロップされる |
| CSCvv69991 | FTD が 6.6.1 へのアップグレード後にメンテナンスモードでスタックする |
| CSCvv70984 | ブックマーク SSL 暗号設定の変更中の ASA トレースバック |
| CSCvv71097 | トレースバック：ASA が snp_fdb_destroy_fh_callback + 104 をリロードする |
| CSCvv72466 | ASA のアップグレード後、startup-config で OSPF ネットワークコマンドが欠落する |
| CSCvv73017 | fover および SSH スレッドによるトレースバック |
| CSCvv74658 | FTD/ASA は、ファイル名に「!」の文字を含むコアダンプファイルを作成する（CSCvv40406 の zmq 変更（fxos）） |

| 不具合 ID | タイトル |
|---|---|
| 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 |
| CSCvv80782 | トレースバックにより purg_process となる |
| CSCvv85029 | スレッド名 ace_work で ASA5555 がトレースバックし、リロードする |
| CSCvv86861 | SNMP トラフィックのテスト中にトレースバックする |
| CSCvv86926 | コアファイルを作成する FTD での予期しないトレースバックとリロード |
| CSCvv87232 | ASA：igb_saleen_io_sfp_mod_poll_thread プロセスで CPU 専有の値が高くなる |
| CSCvv87496 | 「VPN packet redirect on peer」による ASA クラスタメンバー 2048 ブロックの枯渇 |
| CSCvv88017 | ASA：EasyVPN HW クライアントが重複したフェーズ 2 のキー再生成をトリガーし、トンネル経由で切断される |
| CSCvv89355 | フェールオーバー後に DHCP プロキシ更新タイマーが起動しない |
| CSCvv89400 | AES 256 を使用すると ASA SNMPv3 ポーリングが失敗する |
| CSCvv89708 | ASA/FTD がスレッド名 fover_FSM_thread でトレースバックし、リロードすることがある |
| CSCvv89715 | 8000 シリーズのスタックの Fastpath ルールが FMC からランダムに消える |
| CSCvv90079 | 9300 シャーシ内クラスタで変更を行った後、ルータ BGP がプッシュされない |
| CSCvv90181 | 展開中に「show running-config」が実行されている場合、トランスクリプトに展開失敗の理由が表示されない |
| CSCvv90720 | ASA/FTD：HA スイッチオーバー後に接続されたスイッチで MAC アドレステーブルのフラッピングが表示される |
| CSCvv90753 | SLA が原因で同期プロセスがハングする |
| CSCvv94165 | FTD 6.6：snmpd プロセスの CPU がスパイクする |
| CSCvv94701 | ASA が「octnic_hm_thread」でリロードし続け、リロード後は回復するまでに非常に長い時間がかかる |
| CSCvv96193 | プロポーザルが選択されていない場合、ASA または FTD のデバッグで明確な失敗理由が出力されない |
| CSCvv97527 | asa config timeout コマンドが snort の DAQ 設定を壊す |

| 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 |
| CSCvw00161 | Firepower 2140 での VPNス レッドによる ASA のトレースバックとリロード |
| CSCvw01767 | 階層によっては、CRL フェールオープンオプションが機能しない場合がある |
| CSCvw03628 | RFC822Name が空に設定された名前制約により、ASA が CA 証明書をインポートしない |
| CSCvw05392 | diagnostic-cli に常に表示されるメッセージ |
| CSCvw06195 | ASA のトレースバック cp_midpath_process_thread |
| CSCvw06298 | 異なるコンテキストの共有インターフェイスで ASA が MAC アドレスを複製して、トラフィックに影響を与える |
| CSCvw07000 | PDTS Tx キューがスタックしたまま Snort がビジー状態でドロップする |
| CSCvw12008 | 「show tech-support」コマンドの実行中の ASA トレースバックとリロード |
| CSCvw12040 | 証明書チェーンの検証に失敗したため、ヒープキャッシュメモリが急激に枯渇している |
| CSCvw12100 | サイト間セッションおよび AnyConnect セッションで ASA の古い VPN コンテキストが表示される |
| CSCvw13348 | CCM レイヤ（スプリント 98、seq 2）における WR6、WR8 および LTS18 コミット ID の更新 |
| CSCvw15359 | KP fxos snmp に、EPM インデックスの entPhysicalSerialNum,entPhysicalAssetID に初期化されていない文字列がある |
| CSCvw16165 | ポートチャネルのメンバーがダウンすると、Firepower 1010 シリーズがトラフィックの通過を停止する |
| CSCvw16619 | オフロードされたトラフィックが ECMP セットアップでセカンダリルートにフェールオーバーされない |
| CSCvw18614 | LINA プロセスでの ASA トレースバック |
| CSCvw19227 | 使用されていないプレフィックスリストのオブジェクトを削除できない |
| CSCvw19907 | agx 通信の snmpd の再起動が snmp-sa に対して失敗する |
| CSCvw21145 | ポリシーを保存する際に起こる重複 NAT ルールエラー（重複する自動 NAT ルールが原因） |

| 不具合 ID | タイトル |
|---|---|
| CSCvw21161 | ポリシー保存時に起こる重複 NAT ルールエラー（異なるルールが重複として検出される） |
| CSCvw21844 | カプセル化されたフローを処理する際の DATAPATH スレッドでの FTD トレースバックとリロード |
| CSCvw22576 | スタンバイ時のみ state fover インターフェースで「no mfib forwarding」コマンドが実行される |
| CSCvw22881 | radius_rcv_auth により、コントロールプレーンの CPU 使用率が 100% になることがある |
| CSCvw22986 | プライマリユニットのインターフェイスが init 状態のままであるため、セカンダリユニットがバルク同期状態で無限にスタックする |
| CSCvw23199 | スレッド名 Logger での ASA/FTD のトレースバックとリロード |
| CSCvw24556 | フローオフロードが有効になっている場合、TCP ファイル転送（ビッグファイル）が正しく閉じない |
| CSCvw26171 | strncpy NULL 文字列が SSL ライブラリから渡されている間の ASA syslog トレースバック |
| CSCvw26331 | スレッド名 ci/console での ASA のトレースバックとリロード |
| CSCvw26544 | Cisco ASA および FTD ソフトウェアの SIP で確認されたサービス拒否攻撃に対する脆弱性 |
| CSCvw27301 | EAP を使用した IKEv2 で、MOBIKE ステータスが処理されない |
| CSCvw28814 | SNMP プロセスがクラッシュし、Lina のトレースバックが発生した |
| CSCvw30252 | ASA/FTD が SNMP のメモリ破損によりトレースバックおよびリロードすることがある |
| CSCvw31569 | ディレクタ/バックアップフローは残され、このフローに関連するトラフィックがブラックホール化される |
| CSCvw32518 | 9.12(4)4 以降にアップグレード後の ASASM トレースバックおよびリロード |
| CSCvw36662 | TACACS+ ASCII パスワード変更要求が正しく処理されない |
| CSCvw37259 | デバイスがハング状態になるまで 600/秒のレートで VPN syslog が生成される |
| CSCvw37340 | Oracle MySQL の MySQL サーバー製品の脆弱性（コンポーネント： |
| CSCvw37807 | NTP 認証が有効な場合に IPsec 送信エラーが増加する |

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

| 不具合 ID | タイトル |
|---|---|
| CSCvw46630 | FTD：NLP パスでリターン ICMP 接続先到達不能メッセージがドロップされている |
| CSCvw46702 | アプリケーション設定の同期のタイムアウトが原因で FTD クラスタのセカンダリユニットがクラスタに参加できない |
| CSCvw47321 | 一部の FPR プラットフォームのインバウンドトラフィックの IPSec トランスポート モード トラフィックの破損 |
| CSCvw48517 | ASA を 9.13(1)13 にアップグレードすると、DAP が動作しなくなる |
| CSCvw48829 | 「show clock」のタイムゾーンが「show run clock」のタイムゾーンと異なる |
| CSCvw50679 | アップグレード中に ASA/FTD がトレースバックおよびリロードすることがある |
| CSCvw51307 | プロセス名「Lina」で ASA/FTD がトレースバックおよびリロードする |
| CSCvw51462 | IPv4 デフォルトトンネルルートが拒否される |
| CSCvw51745 | ルーティングテーブルに再追加された SLA 監視対象の静的ルートが RIP データベースに入力されていない。 |
| CSCvw51950 | 手動フェールオーバー後に新しいアクティブの ASA から FPR SSL トラストポイントが削除される |
| CSCvw51985 | ASA：IPv6 DACL 障害により、AnyConnect セッションを再開できない |
| CSCvw52083 | FXOS logrotate がすべてのログファイルを正しくローテーションしない |
| CSCvw52609 | Cisco ASA と FTD ソフトウェアの Web サービスバッファオーバーフローによるサービス拒否の脆弱性 |
| CSCvw53255 | FTD/ASA HA：トレースバックによるフェールオーバー後でも、スタンバイユニット FXOS がトラフィックを転送できる |
| CSCvw53427 | ASA が複数のクエリパラメータを含む SAML アサーションで HTTP POST を処理できない |
| CSCvw53796 | Cisco ASA および FTD Web サービスインターフェイスで確認されたクロスサイト スクリプティングの脆弱性 |
| CSCvw54640 | FPR-4150：スレッド名 DATAPATH での ASA トレースバックおよびリロード |
| CSCvw56703 | ifc タイプの管理のみを変更すると、IPv6 静的ルートがインストールされない |

| 不具合 ID | タイトル |
|---|---|
| CSCvw58414 | タイプ dynamic-split-exclude-domains の AnyConnect カスタム属性の名前がリロード後に変更される |
| CSCvw59035 | FTD BVI アドレスから直接接続された IP への接続の問題 |
| CSCvw60177 | スタンバイまたはセカンダリのクラスタユニットがスレッド名 fover_parse および「cluster config sync」でクラッシュすることがある |
| CSCvw62526 | エンジニアリング ASA Build での ASAトレースバックとリロード：9.12.3.237 |
| CSCvw62528 | ASA が IPv6 NTP サーバーとの同期に失敗する |
| CSCvw63862 | ASA：ランダムなL2TPユーザーが古いACLフィルタエントリが原因でリソースにアクセスできない |
| CSCvw64623 | アクティブ IP アドレスを持つスタンバイインターフェイスから送信されたスタンバイ ASA リンクダウン SNMPTRAP |
| CSCvw68593 | Linux カーネル f の応答 ICMP パケットが制限される方法に欠陥がある |
| CSCvw71766 | IKev 2 Daemon スレッドでの ASA トレースバックおよびリロード |
| CSCvw72260 | ASA のアップグレードが「CSP directory does not exist - STOP_FAILED Application_Not_Found」で失敗する |
| CSCvw72608 | アクティブで受信したスタンバイの失敗イベントにより、スタンバイでの将来の展開がスキップされる |
| CSCvw73402 | リモートFTPへのクラスタコピーのキャプチャの失敗により、FTDのLINA CLI が応答しなくなる |
| CSCvw74940 | IKE デーモンでの ASA トレースバックおよびリロード |
| CSCvw75104 | ポートチャネルメンバーのインターフェイスの変更に対する FDM-HA での展開の失敗 |
| CSCvw75605 | ドメイン、カウント、およびその他のフィールドが選択されていると、接続イベントの表に関する表示レポートが失敗する。 |
| CSCvw77930 | トンネルグループ名に「.」が含まれている場合、ASAがSAMLアサーションの処理に失敗する |
| CSCvw79208 | 入力文字列の後半に「http://」サブストリングがある場合、URL の正規化が正しく行われない |
| CSCvw79294 | sftunnel が大量のログをメッセージファイルに記録する |

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

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

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

| 不具合 ID | タイトル |
|---|---|
| CSCvx16317 | 管理のコンテキストが変更されると、マルチコンテキスト ASA から connect fxos admin で FXOS にアクセスできない |
| CSCvx16592 | VRF が設定されている場合、FTD はパケットを WCCP Web キャッシュエンジンにリダイレクトしない |
| CSCvx16700 | 「MIO が強制時刻同期に応答しない（MIO DID NOT RESPOND TO FORCED TIME SYNC）」ために、ブレードの起動中に FXOS クロック同期の問題が発生する |
| CSCvx17664 | ASA がスレッド名「webvpn_task」でトレースバックおよびリロードすることがある |
| CSCvx17780 | FPR-2100-ASA：最新バージョンの ASA インターフェイスで ifType の SNMP ウォークに「other」が表示される |
| CSCvx17785 | ACL を追加または削除し、ルートマップコマンド（pbr_route_map_update）に入力すると、トレースバックが発生する |
| CSCvx17842 | FMC から送信されたオブジェクトループによる lina のトレースバックを防ぎます。代わりに展開を失敗させます。 |
| CSCvx19934 | 6.6.3 で snmpv1 を削除し、snmpv3 を一度に追加すると、snmp 設定の展開が失敗する |
| CSCvx20303 | ASA/FTD が SNMP ホストグループオブジェクトの変更後にトレースバックすることがある |
| CSCvx20692 | すべてのオブジェクトのタイプが同じ場合、Smart CLI で 10 個のオブジェクトのみが表示される |
| CSCvx20872 | netflow リフレッシュタイマーによる ASA/FTD トレースバックとリロード |
| CSCvx21782 | lina モニタが原因で Firepower プラットフォームが破損したコアダンプを生成する |
| CSCvx22695 | OCSP 応答データのクリーンアップ中に ASA がトレースバックおよびリロードする |
| CSCvx23833 | IKEv2キー の再生成：Create_Child_SA 応答の直後に受信した新しい SPI を使用した ESP パケットの SPI が無効になる |
| CSCvx23907 | CVE-2021-1405 に対する NGFW の影響を評価する |
| CSCvx24537 | SAML：同じサブジェクト名を持つ 2 つ以上の IDP 証明書がある場合、SAML 認証が失敗する可能性がある |

| 不具合 ID | タイトル |
|---|---|
| CSCvx25406 | パケットの MTU のサイズが出力インターフェイスの MTU のサイズより大きい場合、LINA はパケットを何の警告を出すことなくドロップする |
| CSCvx25719 | X-Frame-Options ヘッダーが webvpn 応答ページで設定されていない |
| CSCvx25836 | 「show crashinfo」による新しい出力ログの追加で ASA がトレースバックおよびリロードする |
| CSCvx26221 | handle_agentx_packet / snmp で SNMP にトレースバックすると、FP1k および 5508 での起動に時間がかかる |
| CSCvx26308 | chastrcpy_s: source の文字列が着信側に対して長すぎるため ASA がトレースバックおよびリロードする |
| CSCvx26525 | FMC が 6.6.1 にアップグレードされた後、FTD デバイスで SNMP の設定が無くなっていることが判明した |
| CSCvx26808 | FPR2100 シリーズのプロセス lina での FTD のトレースバックおよびリロード |
| CSCvx26927 | CH をセグメント化して再送信した際に TLS サイトがロードされない |
| CSCvx27077 | SAML：トンネルグループで参照されているときに、webvpn saml IDP 設定が削除されないようにする |
| CSCvx27430 | ASA：FIPS が有効な場合、PAC ファイルをインポートできない |
| CSCvx27914 | 地理位置情報ウィジェット FMC でイベントを表示できない |
| CSCvx28520 | DKK の顧客 SSL ルールを使用した SSL の復号化が失敗する |
| CSCvx29429 | CSCvx07389 の修正にもかかわらず、FPR4100/FPR9300 で ma_ctx*.log が大きなディスク領域を消費する |
| CSCvx29448 | FTD：管理 int をポーリングできる診断 int で SNMP ホストが設定される |
| CSCvx29771 | フローオフロードによる一括ルーティング更新後にファイアウォール CPU が増加することがある |
| CSCvx29814 | DHCP GIADDR フィールドの IP アドレスが DHCP DECLINE を DHCP サーバに送信した後に反転する |
| CSCvx29832 | フローオフロードを有効にした状態で大量のルートを更新すると、CPU のパフォーマンスが低下する |
| CSCvx30314 | SSL 中間パスで ASA がトレースバックおよびリロードする |
| CSCvx33822 | 4GB RAM と 2 つの CPU を搭載した ASAv を展開するオプションがない |

| 不具合 ID | タイトル |
|---|---|
| CSCvx33904 | 1.9.5p2 より前の sudo には、ヒープベースのバッファオーバーフローがあり、権限を使用できる |
| CSCvx34237 | FIPS 障害による ASA のリロード |
| CSCvx34335 | AAA LDAP サーバー：平均ラウンドトリップ時間が常に 0 ミリ秒になる |
| CSCvx37737 | HA 中断および 6.6.0 または 6.6.1 へのアップグレード後に OSPF NSF による HA の障害が発生する |
| CSCvx38124 | CP がピン接続されているコアでのコアローカルブロック割り当ての失敗によりドロップが発生する |
| CSCvx41171 | ACL 設定を同時に変更すると、「show running-config」の出力が完全に中断される |
| CSCvx41440 | Talos クラウドとローカル DB 間で URL レピュテーションの不一致が発生する。 |
| CSCvx42081 | FPR4150 ASA Standby Ready ユニットのループが失敗し、設定を削除してインストールし直す必要がある |
| CSCvx42197 | ASA EIGRP ルートがネイバーの切断後にスタックする |
| CSCvx44117 | 新しい net-snmp パッチの追加と未使用の net-snmp レシピのクリーンアップ |
| CSCvx44401 | スレッド名 Unicorn Proxy Thread で FTD/ASA がトレースバックする |
| CSCvx45976 | スレッド名：vnet-proxy（rip：socks_proxy_datarelay）で ASA および FTD のウォッチドッグが強制的にトレースバックとリロードを実行する |
| CSCvx47230 | IE および Windows プラットフォームの古いバージョンの X-Frame-Options ヘッダーのサポート |
| CSCvx47628 | 2.4.57 および 2.5.x ～ 2.5.1 alpha の OpenLDAP では、アサーション |
| CSCvx47634 | GNU C ライブラリ（別名 glibc または libc6）2.32 の iconv 関数 |
| CSCvx47642 | 2.4.57 より前の OpenLDAP で整数アンダーフローが発見された |
| CSCvx48490 | 「Initiator/Responder」パケットを 0 として示す SSL 復号化された https フローの EOF イベント |
| CSCvx49715 | EVP_CipherUpdate、EVP_EncryptUpdate、EVP_DecryptUpdate への呼び出しは、 |
| CSCvx49716 | 2.66.7 および 2.67.x より前の GNOME GLib で問題が発見された |

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

| 不具合 ID | タイトル |
|---|---|
| CSCvx68355 | ASA：countryName が UTF8 としてエンコードされている場合、CA 証明書をインポートできない |
| CSCvx68490 | SSL URL カテゴリが削除されたため、100_ftd_onbox_data_import.sh で FDM のアップグレードが失敗する |
| CSCvx68951 | SNMP を使用してインターフェイスの物理アドレスをポーリングすると、ASA が「00 00 00 00 00 00」で応答する |
| CSCvx69405 | スレッド名 SNMP ContextThread での ASA トレースバックおよびリロード |
| CSCvx71434 | asa_run_ttyS0 スクリプトによるスレッド名 pix_startup_thread での ASA/FTD トレースバックおよびリロード |
| CSCvx71571 | ASA：CSM で「エラー：ハッシュテーブルからエントリを削除できません」 |
| CSCvx72904 | ifmibポーリングの最適化 |
| CSCvx73164 | シスコ製品に影響を及ぼす Lasso SAML 実装の脆弱性：2021 年 6 月 |
| CSCvx74035 | 複数の ACL とオブジェクトが設定された状態で「clear configure all」を実行すると、ASA がトレースバックおよびリロードする |
| CSCvx75503 | 再送信された SYN が検査エンジンで検査されない |
| CSCvx75963 | キャプチャ取得中に ASA がトレースバックする |
| CSCvx76703 | ルールがインターフェイスグループによるトラフィックに一致している場合、FMC がプレフィルタのポリシー変更を保存しない |
| CSCvx77768 | Umbrella によるトレースバックとリロード |
| CSCvx78238 | ASA のトラフィックでのマルチコンテキストの Firepower サービスが不適切なインターフェイスに移動する |
| CSCvx79793 | SSL ポリシーを使用したファイル転送またはファイルアップロードが低速で、復号化の再署名アクションが適用される |
| CSCvx80835 | 手動登録が、証明書をインポートした後、LINA でスタック保留中のトラストポイントのエントリを作成する |
| CSCvx81405 | 既知のキールールに一致すると予想される接続が復号化されない場合がある |
| CSCvx85534 | データインターフェイスからの予期しない IP を持つ SNMP トラップが送信される |

| 不具合 ID | タイトル |
|---|---|
| CSCvx85922 | ASA/FTDは、設定をメモリに保存/書き込みするときにトレースバックおよびリロードすることがある |
| CSCvx86177 | FMC データベースを外部からポーリングするために使用される inet6_ntoa と unix_timestamp 関数がエラーを返す |
| CSCvx87679 | フェールオーバーライセンスの数がスタンバイのファイアウォールに同期されない。 |
| CSCvx87709 | HAで FPR 2100 が ASA を実行するフェールオーバー中のウォッチドッグでのトレースバックとリロード |
| CSCvx87790 | HAで FPR 2100 が ASA を実行するフェールオーバー中のウォッチドッグでのトレースバックとリロード |
| CSCvx88683 | ASA が BGP パスワードをスタンバイユニットに正しく複製しない |
| CSCvx89827 | FPR 2110 でバンコクタイムゾーンを設定できない |
| CSCvx91341 | 2.66.8 より前の GNOME GLib で問題が発見された。g_file_repla の場合 |
| CSCvx94326 | VPN ロードバランシングがスタックし、グループから切断されることがある |
| CSCvx94398 | セカンダリ ASA がスタートアップ コンフィギュレーションを取得できない |
| CSCvx95255 | 既存の ASDM コンテキストスイッチから新しい ASDM 接続を区別するための ASA のサポート変更 |
| CSCvx97632 | クラスタコマンドを使用して長い宛先ファイル名を持つファイルをコピーする場合にASA がトレースバックおよびリロードする |
| CSCvx98041 | FTD-API：ruleId の重複するシーケンス番号により、無効な snort ngfw.rules が展開される |
| CSCvx99373 | FMC：「beakerd」プロセスのコアファイルがデバッグシンボルをアーカイブしていないため、使用できない |
| CSCvy01752 | スレッド Lic HA クラスタでのトレースバック |
| CSCvy02448 | FPFPR2100 シリーズ プラットフォームの ASA で時刻同期が正しく機能しない |
| CSCvy02703 | CTM Message Handler による ASA および FTD のトレースバック |
| CSCvy03006 | uauth のデバッグ機能の改善 |

| 不具合 ID | タイトル |
|---|---|
| CSCvy03045 | 管理のコンテキストが変更されると、マルチコンテキスト ASA から connect fxos admin で FXOS にアクセスできない |
| CSCvy03907 | アクセス コントロール ポリシーの作成および編集が「ルール名は既に存在します」というエラーで失敗する |
| CSCvy04869 | ユーザー証明書のキーサイズが 8192 ビットの場合、AnyConnect 証明書認証が失敗する |
| CSCvy04965 | WM スタンバイが HA への再参加に失敗し、「CD App Sync エラーがスタンバイで SSP 設定を適用できませんでした」というメッセージが表示される |
| CSCvy05807 | FO 同期の操作後に SNMPWalk 失敗が確認された。 |
| CSCvy05966 | Snort 2.9.16.3-3033 トレースバック（FTD 6.6.3） |
| CSCvy07491 | access-list の再設定時の ASA トレースバック |
| CSCvy07654 | FTD：ndclientd の後にハートビートが見つからないため、TS ファイルを生成する際にフェールオーバーロールの変更が発生する |
| CSCvy08908 | Java によってポート転送アプリケーションがブロックされる |
| CSCvy09217 | 暗号の不一致が原因で HA がアクティブ/アクティブ状態になる |
| CSCvy09252 | Syncd が FMC HA のセカンダリの FMC 部分で繰り返し終了する |
| CSCvy10665 | Firepower 9000 シリーズ SM-56 で、ディスクマネージャの YYYY-MM-DD ファイルの filespec エントリがない |
| CSCvy13229 | FDM - GUI にアクセスできない（tomcat が開いているファイル記述子が多すぎる） |
| CSCvy17365 | REST API ログインページの問題 |
| CSCvy17470 | IKEv2 の A/S フェールオーバーペアでの ASA トレースバックとリロード。 |
| CSCvy19453 | MAC アドレスのみを持つ冗長な新しいホストイベントを含む SFDataCorrelator のパフォーマンスの問題 |
| CSCvy30016 | 「最大証明書キャッシュエントリ」プルーニングでは、SSL キャッシュをロックする必要がある |
| CSCvy34333 | ASA のアップグレードに失敗した場合、プラットフォームとアプリケーションの間でバージョンステータスの同期が解除される |
| CSCvy37835 | ssl 置換キーのみのアクションにより、検出エンジンのメモリ使用量が無制限になる場合がある |

| 不具合 ID | タイトル |
|---|---|
| CSCvy39191 | FMC への API 呼び出しを実行すると、T-ufin で内部サーバーエラー 500 が発生する |
| CSCvy39659 | ASA/FTD がスレッド名「DATAPATH-15-14815」でトレースバックし、リロードすることがある |
| CSCvy40482 | 9.14MR3：snmpwalk が [Errno 146] の接続拒否エラーで失敗した |
| CSCvy61008 | Lina と FXOS 間の同期外れの時間 |
| CSCvy83116 | WM スタンバイが HA への再参加に失敗し、「CD アプリの同期エラーは、SSP 設定の生成における失敗です（CD App Sync error is SSP Config Generation Failure）」というメッセージが表示される |

# バージョン 6.6.4 で解決済みのバグ

表の最終更新日：2023-01-18

**表 *55*：バージョン *6.6.4* で解決済みのバグ**

| 不具合 ID | タイトル |
|---|---|
| CSCvu84127 | 明確な理由なしに Firepower がリブートすることがある |
| CSCvy15046 | 6.6.3.81 から 6.6.4.59 へのアップグレードが 000_start/125_verify_bundle.sh で失敗した - 解凍の失敗である |
| CSCvx86231 | 999_finish/935_change_reconciliation_baseline.pl での 6.6.3 への FMC アップグレードの失敗 |

# バージョン 6.6.3 で解決済みのバグ

表の最終更新日：2021-03-15

**表 *56*：バージョン *6.6.3* で解決済みのバグ**

| 不具合 ID | タイトル |
|---|---|
| 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 |
| CSCvf88062 | CTM：Nitrox S/G の長さを検証する必要がある |
| CSCvg69380 | ASA：まれに発生した CP 処理での破損によってコンソールロックが発生する |

| 不具合 ID | タイトル |
|---|---|
| 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 |
| CSCvh75756 | 重複するプリプロセッサキーワード：ssl（Duplicate preprocessor keyword: ssl） |
| 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 |
| 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 |
| CSCvo11165 | WebVPN の言語変換表を更新する必要がある |
| 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 |
| CSCvo57004 | [ヒットカウントの分析（Analyze Hit Counts）] で、設定されたユーザータイムゾーンではなく UTC でタイムスタンプが表示される |
| CSCvp10079 | FMC HA スイッチで DB スイッチロールが失敗する |
| CSCvp47536 | FTD での AAA 要求が RRI から学習した V ルートをたどらない |
| CSCvq47743 | AnyConnect と管理セッションが数週間後に接続に失敗する |
| 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 |
| CSCvr02310 | TLS1.3 が DND ルールで唯一許可されている TLS バージョンである場合、Server Hello がドロップされる |
| CSCvr33428 | FMC が SYN フラッド攻撃から接続イベントを生成する |
| CSCvr35872 | ASA トレースバックスレッド名：DATAPATH-0-1388 PBR 9.10(1)22 |
| CSCvr55741 | 展開に成功した後、FMC に旧ポリシーが表示される |
| CSCvr85295 | Cisco Adaptive Security Appliance と Firepower Threat Defense ソフトウェアリモート |
| CSCvs07922 | アクティブ ASA で、IPv6 を使用した WebVPN に対して不正な IP を含むロギングメッセージが生成される |
| 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 |
| 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 |

| 不具合 ID | タイトル |
|---|---|
| CSCvs50274 | ASA5506 からボックスへ icmp 要求パケットが断続的にドロップされる |
| CSCvs68576 | 二重否定が原因で、自動 NAT ルールの削除時に展開に失敗する |
| 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 |
| 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 |
| CSCvs79606 | 「dns server-group DefaultDNS」CLI が無効にならない |
| CSCvs81763 | vFTD が VLAN タグ付きトラフィックを渡すことができない（トランクモード） |
| 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 |
| CSCvs85595 | ユニットの同期中に awk:fatal メッセージが表示される |
| CSCvs91270 | 検査の中断：展開ページでエラーが発生 |
| CSCvs91389 | FTD トレースバック Lina プロセス |
| CSCvs99356 | Snort2：SSP プラットフォームで SSL ポリシーが設定されていると、大きなファイルのダウンロードに時間がかかる |
| CSCvt00255 | カーネルを cpe:2.3:o:linux:linux_kernel:4.14.187: にアップグレード |
| CSCvt01938 | show ntp を実行すると、出力を得るためのパスワードを求められる |
| 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 |
| 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 |
| 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 |

| 不具合 ID | タイトル |
|---|---|
| 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 |
| 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 |
| 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 |
| 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。 |
| CSCvt29771 | [オブジェクト管理（Object Management）]ページからセキュリティゾーンを変更した場合の無効な応答メッセージ |
| CSCvt31292 | FTD デバイスが SSE にイベントを送信しない場合がある |
| CSCvt33785 | ランダム VPN ピアの IPSec SA が作成されない |
| CSCvt34973 | SFNotificationd によって「メッセージ」ファイルに過剰なロギングが発生することがある |
| CSCvt39292 | LDAPS 外部ユーザーが Firepower 4110 で「sudo su」を実行できない |
| CSCvt40306 | ASA：リロード後にスタンバイユニットの BVI インターフェイスが応答を停止する |
| CSCvt41357 | syslog ホストにアクセスできない場合、「no logging permit-hostdown」コマンドで接続がブロックされない |
| CSCvt42610 | SNMP ポーリング中に確認されたメモリリーク |
| 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 |
| CSCvt48260 | スタンバイユニットがアクティブユニットを検出すると、fover_parse でトレースバックしてブートループする |
| 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 |

| 不具合 ID | タイトル |
|---|---|
| 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 |
| CSCvt61196 | マルチコンテキストモードの ASA で、コンテキストを削除しても SSH キーが削除されない。 |
| 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 |
| CSCvt64952 | 「Show crypto accelerator load-balance detail」が欠落しており、出力が未定義 |
| 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 |
| CSCvt69260 | 接続イベントに古いデバイス名が表示される |
| CSCvt70664 | ASA：AnyConnect の Radius Acct-Requests に acct-session-time アカウンティング属性がない |
| 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 |
| CSCvt70879 | vpn-filter に使用される ACL での「clear configure access-list」がリソースにアクセスできない |
| 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 |
| CSCvt76688 | syslog メッセージ 201008 に、TCP サーバーがダウンした場合のドロップの理由が含まれている必要がある |
| 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 |
| CSCvt86467 | c3p0 0.9.5.2 では、com/mcha の extractXmlConfigFromInputStream で XXE が許可される |

| 不具合 ID | タイトル |
|---|---|
| CSCvt87074 | libxslt 1 の前に xsltNumberFormatGetMultipleLevel で Type Confusion が生じる |
| CSCvt88454 | クライアントレスポータルを使用すると、設定された言語と一致しない文字列がある |
| CSCvt89183 | FDM が管理 Web サーバー経由で CA 署名付き証明書をロードできない |
| CSCvt89790 | 「snmp-server location」を設定すると、ASA 9.14.1 の「snmp-server contact」にも同じ値が設定される |
| CSCvt92077 | ASAv での ping の失敗：9.13（CAT9k の再起動後） |
| CSCvt95176 | 2.1.0 より前の expat の readfilemap.c で、コンテキスト依存の攻撃者が許可される |
| CSCvt97205 | ASA 9.14.1 上で SNMPPOLL/SNMPTRAP からリモートエンド（サイト間 VPN）ASA インターフェイスが失敗する |
| 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 |
| 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 |
| CSCvu08339 | タップモードがオフで FTD インラインセット ブリッジ グループ ID が 0 に設定される |
| 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 |
| CSCvu17819 | vFTD での SSH RBAC の 6.7.0 へのアップグレードが失敗する |
| CSCvu17852 | MPF で接続制限が設定されている場合、「show service policy」で現在の接続数が負になる |
| CSCvu23539 | 内部フロー：LU flag3 オーバーラップ |
| CSCvu27287 | スケジュールバックアップが EEM を介した SCP で失敗する |
| CSCvu27868 | ASA：ASA のアップグレード後、外部 IPv6 ロギングサーバーへの特定の syslog メッセージの欠如 |
| 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 |

| 不具合 ID | タイトル |
|---|---|
| CSCvu30756 | ユーザー ID が、異なるネットマップの同一セッションを正しく処理しない |
| 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:）」 |
| CSCvu33591 | FPWR 4100 ：/var/sf/fwcfg/ にある破損ファイルが原因で Snort がダウンする |
| CSCvu33992 | トレースバック：ASA が lina_sigcrash+1394 をリロードした |
| CSCvu35768 | FMC を 6409-59 から 6.6.0-90 にアップグレードした後、サブドメイン内の Radius 外部ユーザーを使用して UI をログに記録できない |
| 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 |
| CSCvu40834 | ネイティブ SSP プラットフォームでのカレンダー更新のマージの損傷を修正 |
| CSCvu43355 | 二重解放によるデータパスでの FTD Lina トレースバック |
| CSCvu43827 | スレッド名「cluster config sync」または「fover_FSM_thread」での ASA および FTD クラスタ ユニット トレースバック |
| CSCvu44135 | SSH 管理接続制限を超えた場合に syslog 710004 が生成されない |
| CSCvu45822 | ASA でトレースバックが発生し、リロードされた |
| 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 |
| 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 |
| CSCvu55469 | FTD：接続アイドルタイムアウトがリセットされない |
| CSCvu58153 | RADIUS ポートの表現がビッグエンディアンではなくリトルエンディアンとして表示される |
| CSCvu59573 | 「admin」で始まるグループ URL が正しく機能しない |
| CSCvu63397 | 整数オーバーフロー（FileExtract 正常性アラート内）により、ログスパム「file capture perf stats」が発生する |
| 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 |

| 不具合 ID | タイトル |
|---|---|
| CSCvu71324 | ASA：dhcp-network-scope の使用により、自動 DENY ルールが複数のコンテキストに適用される |
| CSCvu75315 | 6.6.0 へのアップグレード後、レポートに棒グラフと円グラフで侵入イベントが表示されない |
| CSCvu79102 | FTD-API/FDM：HA 同期ステータスがスタンバイで失敗する |
| CSCvu82272 | 管理対象デバイスの非アクティブな古いエントリが原因で、Firepower Management Center でのアップグレードが失敗することがある |
| CSCvu82738 | インラインセットの show interface のドロップレートが正しくない |
| CSCvu83389 | ASA がヌル TEID の GTPV1 転送再配置要求メッセージをドロップする |
| CSCvu84066 | /32 マスクの BFD マップ送信元アドレスが機能しない |
| CSCvu85381 | スタンバイでのポリシー展開の失敗に続いて HA の再構成が失敗する |
| CSCvu85421 | 次のメッセージで展開が失敗する：「クリプトマップ s2sCryptoMap がインターフェイス内にありません（no crypto map s2sCryptoMap interface inside）」 |
| 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 |
| CSCvu93278 | AnyConnect-IKEv2 スケーリング接続で作業中に KP でクラッシュが確認される |
| CSCvu93834 | FDM/FTD-API：スタンバイ状態で管理ユーザーのパスワードを変更できない |
| CSCvu95109 | 6.6 から 6.7.0 への KVM/KP FDM のアップグレードがディスク容量が原因で失敗する/ngfw/var/cisco/deploy/fdm |
| CSCvu97764 | TAP モードの FTD が出力インターフェイスでキャプチャされない |
| CSCvu98222 | SSL 復号ポリシーを有効にした後、FTD Lina エンジンがデータパスでトレースバックすることがある |
| CSCvu98468 | SDI：新しいデバイスがフェールオーバーに参加すると、SDI ファイルがスタンバイに同期されない |
| CSCvu98505 | PLR 経由でライセンスされた ASA に「export-controlled functionality enabled」フラグが正しく設定されていない |
| CSCvu98780 | FTD-API：CDO テンプレートの適用によってルール削除のバグがトリガーされる |

| 不具合 ID | タイトル |
|---|---|
| CSCvv02245 | ASA「session sfr」コマンドが初期設定のために FirePOWER モジュールから切断する |
| CSCvv02925 | OSPF ネイバーシップが確立されていない |
| CSCvv04023 | FDM（オンボックスマネージャ）：インターフェイスが zones.conf から削除されたため、トラフィックが適切なルールでヒットしない |
| CSCvv04441 | アップグレード前に RA-VPN が設定されている場合、ngfw.rules がプライマリ FTD HA とセカンダリ FTD HA の間で一致しない |
| 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 |
| 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 |
| CSCvv09396 | セッション終了後に、L2TP の VPN ルートが陳腐化する |
| CSCvv09477 | Oracle MySQL の MySQL サーバー製品の脆弱性（コンポーネント： |
| 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 |
| CSCvv12857 | 暗号化エンジンの障害後に ASA がフリーズする |
| CSCvv14621 | クラスタでコマンド レプリケーション タイムアウトが発生した場合に表示されるエラーメッセージの修正 |
| 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 |
| CSCvv17585 | 特定の状況下で Netflow テンプレートが送信されない |
| CSCvv19230 | ASAv AnyConnect ユーザーがアイドルタイムアウトで予期せず切断される |
| CSCvv19573 | インターフェイスが管理専用のスタティックルートの更新に関連付けられている場合、展開が失敗する |
| CSCvv20405 | WEBVPN：ERROR：マルチコンテキスト ASA の無効なトンネルグループ名 |

| 不具合 ID | タイトル |
|---|---|
| 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」 |
| CSCvv21045 | データベースが新しい接続の受け入れを停止することがあり、イベント処理が停止する |
| CSCvv22208 | onbox モードで、展開が失敗したときに、zones.confがロールバックしない |
| 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 |
| CSCvv26683 | CLI から「configure high-availability disable」コマンドを実行すると、次の HAJoin で例外が発生する |
| 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 |
| 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。 |
| 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 |
| 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 |
| CSCvv36915 | 「Show NTP」コマンドがマルチインスタンス FTD で機能しない |
| CSCvv37108 | ネイバーからの OSPF LS アップデートメッセージを ASA がサイレントにドロップする |
| 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 |
| CSCvv40195 | Syslog トラップにログ内容が含まれていない |

| 不具合 ID | タイトル |
|---|---|
| CSCvv40316 | FDM：スマート CLI ルーティングオブジェクトを使用して BGP の 11 番目のネイバーを追加できない |
| CSCvv40916 | 展開中に、AbstractBaseDeploymentValidationHandler.validatePreApply に 3 分の遅延が発生する。 |
| CSCvv40961 | http-proxy 設定が原因でアップグレードが失敗する |
| 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 |
| CSCvv43771 | スケジュールされたバックアップに対して複数のデバイスを選択できない |
| CSCvv43864 | ポリシーを変更すると、変更ログのプレビューが空白になる |
| CSCvv43885 | キャリアライセンスが準拠していない場合、「show sctp」コマンドは使用できない |
| CSCvv44051 | GRE/IPiniP パッセンジャフローによる snp_cluster_forward_and_free_packet でのクラスタ ユニット トレースバック |
| CSCvv44270 | ASAv5 がトレースバックなしでリロードする。 |
| CSCvv45106 | csd-service.json ファイルが見つからないため、2100 で CSD が起動しない |
| CSCvv46490 | SnortAttribConfig のエラーにより FMC でポリシーの展開が失敗する |
| CSCvv48594 | メモリリーク：脅威の検出での snp_tcp_intercept_stat_top_n_integrate() による |
| 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 |
| CSCvv51623 | Manual-NAT-rule が、展開後、Lina の実行コンフィギュレーションの before-auto-nat-section に移動される |
| CSCvv52591 | ctm_hw_malloc_from_pool で DMA メモリリークが発生し、管理接続と VPN 接続が失敗する |
| CSCvv53696 | Anyconnect ユーザーの AAA または CoA タスク中の ASA/FTD トレースバックおよびリロード |

| 不具合 ID | タイトル |
|---|---|
| CSCvv54831 | パケットトレーサコマンドの実行時の ASA トレースバックおよびリロード |
| CSCvv55066 | FPR1010：SMB ファイル転送中に Internal-Data0/0 およびデータインターフェイスがフラッピングする |
| CSCvv55271 | FMC から監査ログを取得する REST API で、startIndex の有無にかかわらず最初の 25 エントリのみ返される |
| CSCvv57476 | Chrome 85、IE、および Edge ブラウザで CSS スタイルをロードすると問題が発生する |
| 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 |
| 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 |
| 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 |
| 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 |
| CSCvv60849 | Snort D-stateを回避するために、メモリ cgroup の制限を調整する必要がある |
| 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 |
| CSCvv62931 | src.port=dst.port の場合、FTD が Server Hello およびサーバー証明書をクライアントに送信しない |
| CSCvv63208 | ASA 5506/5508：再起動後に SNMP ポーリングが失敗するが、しばらくすると復元される |
| CSCvv63227 | アップグレードされたセットアップで SLA が動作を停止する |
| 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 |
| CSCvv66005 | inspect esmtp での ASA のトレースバックとリロード |

| 不具合 ID | タイトル |
|---|---|
| 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 |
| CSCvv67398 | SNMP が無効な場合、Inspect-snmp で thru-the-box snmp paks がドロップされる |
| 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 |
| CSCvv67754 | メモリの計算結果が正しくないため、Snort のメモリ使用率が高くなる |
| CSCvv69015 | 6.6.X のトラブルシューティング要求に CSD が応答しない |
| CSCvv69991 | FTD が 6.6.1 へのアップグレード後にメンテナンスモードでスタックする |
| 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 |
| 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 |
| CSCvv73540 | 特定の制限を超えるとファイルキャッシュをドロップするモニターを作成 |
| CSCvv74951 | システムのアップグレードスクリプトの実行中、メモリの cgroup を無効化 |
| CSCvv79705 | POE の NPE が原因で 800_post/100_ftd_onbox_data_import.sh で 6.6.0 または 6.6.1 へのアップグレードが失敗する |
| CSCvv80782 | トレースバックにより purg_process となる |
| CSCvv86861 | 夜間に VPN、EMIX、および SNMP トラフィックを実行中に、タイマーで KP のクラッシュが確認される |
| 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 |
| CSCvv87495 | FMC がランダムに応答しなくなる（SSH または GUI なし）：エラー 500 |
| 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 |
| CSCvv89400 | AES 256 を使用すると ASA SNMPv3 ポーリングが失敗する |

| 不具合 ID | タイトル |
|---|---|
| CSCvv89708 | ASA/FTD がスレッド名 fover_FSM_thread でトレースバックし、リロードすることがある |
| 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 |
| CSCvv91486 | リロード中のストリームでメモリリークが発生する |
| CSCvv92897 | バージョン 6.6.0 にアップグレードすると、システムが以前欠落していた memcap 制限に達することがある |
| CSCvv94165 | FTD 6.6：snmpd プロセスの CPU がスパイクする |
| 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 |
| 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 |
| CSCvw00161 | Firepower 2140 での VPNス レッドによる ASA のトレースバックとリロード |
| CSCvw03229 | 6.4 から 6.6.1 にアップグレードすると、デバイスがマルウェアおよび接続イベントを送信しなくなる |
| CSCvw03256 | [メッセージ（Message）]フィールドが選択されている場合、FMC ダッシュボードに侵入テーブルの「データなし」と表示される |
| CSCvw05415 | FDM：オブジェクトの S2S VPN 一致基準バージョンでオブジェクトグループの編集が更新されない |
| 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 |
| CSCvw07352 | Sybase 接続ステータスが 0 になると、SFDataCorrerator のログスパム、メタデータで障害が発生する |
| 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 |
| CSCvw16619 | オフロードされたトラフィックが ECMP セットアップでセカンダリルートにフェールオーバーされない |
| CSCvw19907 | agx 通信の snmpd の再起動が snmp-sa に対して失敗する |

| 不具合 ID | タイトル |
|---|---|
| CSCvw21628 | 6.6.x より前から 6.6.x 以降にアップグレードすると、侵入イベントのパケットドリルダウンが機能しなくなる |
| 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 |
| CSCvw22546 | ローカル管理 FTD で API を使用して DH グループを変更できない |
| 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 |
| CSCvw23286 | データベースオプティマイザが途中で終了するため、FMC で MySQL の CPU 使用率が高くなる |
| CSCvw24556 | フローオフロードが有効になっている場合、TCP ファイル転送（ビッグファイル）が正しく閉じない |
| CSCvw26171 | strncpy NULL 文字列が SSL ライブラリから渡されている間の ASA syslog トレースバック |
| CSCvw26331 | スレッド名 ci/console での ASA のトレースバックとリロード |
| CSCvw27301 | EAP を使用した IKEv2 で、MOBIKE ステータスが処理されない |
| CSCvw28814 | QP を v9.14.1.109 にアップグレード中に SNMP プロセスがクラッシュした |
| 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 |
| CSCvw30252 | ASA/FTD が SNMP のメモリ破損によりトレースバックおよびリロードすることがある |
| CSCvw31569 | ディレクタ/バックアップフローは残され、このフローに関連するトラフィックがブラックホール化される |
| CSCvw32518 | 9.12(4)4 以降にアップグレード後の ASASM トレースバックおよびリロード |
| CSCvw36662 | TACACS+ ASCII パスワード変更要求が正しく処理されない |
| CSCvw37259 | デバイスがハング状態になるまで 600/秒のレートで VPN syslog が生成される |
| CSCvw37369 | Python 3 ～ 3.9.0 の Lib/test/multibytecodec_support.py CJK |

| 不具合 ID | タイトル |
|---|---|
| CSCvw38810 | AWS の FTD：6.6.1 へのアップグレード後にディスクマネージャプロセスが開始されない |
| CSCvw38870 | 800_post/1027_ldap_external_auth_fix.pl で、6.7.0 への FMC のアップグレードが失敗する |
| 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 |
| CSCvw44122 | ASA：非 DNS トラフィックを DNS 検査エンジンにリダイレクトする「class-default」クラスマップ |
| CSCvw45863 | リロード時の ASAv SNMP トレースバック |
| 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 |
| CSCvw50679 | アップグレード中に ASA/FTD がトレースバックおよびリロードすることがある |
| CSCvw51307 | プロセス名「Lina」で ASA/FTD がトレースバックおよびリロードする |
| CSCvw51462 | IPv4 デフォルトトンネルルートが拒否される |
| CSCvw51985 | ASA：IPv6 DACL 障害により、AnyConnect セッションを再開できない |
| CSCvw53255 | FTD/ASA HA：トレースバックによるフェールオーバー後でも、スタンバイユニット FXOS がトラフィックを転送できる |
| 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 |
| 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 |
| 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 |

| 不具合 ID | タイトル |
|---|---|
| CSCvw59035 | FTD BVI アドレスから直接接続された IP への接続の問題 |
| CSCvw60741 | 6.6.1 へのアップグレード後に「show version」で出力が表示されない |
| CSCvw62820 | Memcached 1.5.6 以降の更新 |
| CSCvw63862 | ASA：ランダムな L2TP ユーザーが古い ACL フィルタエントリが原因でリソースにアクセスできない |
| CSCvw64623 | アクティブ IP アドレスを持つスタンバイインターフェイスから送信されたスタンバイ ASA リンクダウン SNMPTRAP |
| CSCvw66953 | URL カテゴリを Beaker に変換するときにアップグレードが失敗する |
| CSCvw74940 | IKE デーモンでの ASA トレースバックおよびリロード |
| CSCvw83498 | FTD-API：LDAP 属性マップで、ldapValue（スペースを含む）が処理されない |
| CSCvw83572 | バージョン 9.14.1.30 以降で BVI HTTP/SSH アクセスが機能しない |
| CSCvw83780 | プロセス名：lina におけるスタンバイ FTD 6.6.1 コア |
| CSCvw84786 | スレッド名 snmp_alarm_thread での ASA トレースバックおよびリロード |
| 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 |
| CSCvw88467 | eStreamer が Sybase の代わりに MySQL から ids_event_msg_map をクエリする |
| CSCvw97821 | ASA：CoA で dACL が提供されない場合、VPN トラフィックが渡されない |
| 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 [年（Year）] ドロップダウンリストに 2020 年 までしか表示されない |
| CSCvx09123 | ISA3000 上の M500IT モデルのソリッドステートドライブが 3 年 2 ヵ月のサービス期間後に応答しなくなることがある |
| CSCvx09248 | v2 および v3 の SNMP ウォークが失敗し、この OID でこのエージェントで使用可能なオブジェクトがありませんと表示される |

| 不具合 ID | タイトル |
|---|---|
| CSCvx09324 | 名前のない EtherChannel インターフェイス内の名前付き/名前のないサブインターフェイスの場合、設定のインポートが失敗する |
| CSCvx09535 | ASA トレースバック：失効した証明書でリロードがトリガーされる AnyConnect クライアントの CRL チェック |
| 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 |
| CSCvx26221 | handle_agentx_packet / snmp で SNMP にトレースバックすると、FP1k および 5508 での起動に時間がかかる |

# バージョン 6.6.1 で解決済みのバグ

表の最終更新日：2020-09-17

**表 *57* : バージョン *6.6.1* で解決済みのバグ**

| 不具合 ID | タイトル |
|---|---|
| CSCtb41710 | CDP が使用できない場合にのみ none にフォールバックする ASA 失効チェック |
| CSCvb92169 | ASA が、より適切なフラグメント関連のログと ASP ドロップの理由を提供する必要がある |
| CSCvh19161 | スレッド名：SXP CORE での ASA/FTD トレースバックおよびリロード |
| CSCvk51778 | ASA 5515/5525/5545/5555 での「show inventory」（または）「show environment」でドライバ/ioctl エラーログが表示される |
| CSCvn64647 | tcp_retrans_timeout 内部スレッド処理による ASA トレースバックおよびリロード |
| CSCvn82441 | [SXP] FPR-2110 の ASA とスイッチ間での SXP 接続の確立に関する問題 |
| CSCvn93683 | ASA：cluster exec show コマンドですべての出力が表示されない |
| CSCvn95731 | スレッド名 SSH での ASA トレースバックおよびリロード |
| CSCvq87625 | ENH：「show tech」出力への「show run all sysopt」の追加 |
| CSCvq93836 | ENH：「show tech」出力への「show logging setting」の追加 |
| CSCvr02080 | 多数のエントリを含む CRL のデコード中に、CERT API プロセスで CPU 占有が観察される |

| 不具合 ID | タイトル |
|---|---|
| CSCvr15503 | ASA：SSH と ASDM セッションが CLOSE_WAIT でスタックし、ASA の MGMT が不足する |
| CSCvr57051 | ポリシーの展開にエラー「Can't use an undefined value as a HASH reference」で失敗した |
| CSCvr58411 | 新しいスタティックスポークを追加または変更した場合、新しいスタティックハブ/スポーク設定の RRI がハブで動作しない |
| CSCvr60195 | ASA/FTD がスレッド名「HTTP Cli Exec」でトレースバックおよびリロードすることがある |
| CSCvr98881 | トレースバック：FTD ZeroMQ メモリアサーション |
| CSCvr99642 | トレース「webvpn_periodic_signal」を使用した複数回の ASA トレースバックおよびリロード |
| CSCvs09533 | FP2100：3 つ以上のインラインセットを介したトラフィックの処理時のトレースバックおよびリロード |
| CSCvs21705 | admin ユーザーは、ドメイン内のデバイスルーティング設定にアクセスする権限がない |
| CSCvs33852 | バージョン 9.6.4.34 へのアップグレード後、アクセスグループを追加できない |
| CSCvs38785 | syslog のタイムスタンプ形式が一貫していない |
| CSCvs39253 | バージョン 6.4 で Firepower 7000 および 8000 が電子メールを送信できない |
| CSCvs41883 | ND ポリシー参照が見つからない場合、6.4.0.x へのアップグレード後に展開が失敗する |
| CSCvs45111 | CCM レイヤ（スプリント 75）での WR6 および WR8 コミット ID の更新 |
| CSCvs52108 | Umbrella インスペクションによる ASA トレースバック |
| CSCvs55603 | ACL で一致した場合に ICMP 応答がドロップされた |
| CSCvs59056 | Float-Conn が有効になっている場合、ASA/FTD トンネルスタティックルートが準最適なルックアップによって無視される |
| CSCvs64510 | メッセージ（「Can't call method "binip" on unblessed reference」）が表示されて展開が失敗する |
| CSCvs72393 | FPR1010 温度しきい値を変更する必要がある |
| CSCvs73754 | ASA/FTD：BVI の ARP が物理インターフェイスに割り当てられていないために発生するブロック 256 サイズの枯渇 |

| 不具合 ID | タイトル |
|---|---|
| CSCvs79023 | スレッド名での ASA/FTD のトレースバック：DNS インスペクションによる DATAPATH |
| CSCvs82829 | Anyconnect 設定がサイト間 VPN トンネルに追加されるとコールが失敗する |
| CSCvs88413 | バージョン 9.8 へのアップグレードにポートチャネルのバンドルに失敗する |
| CSCvs90100 | ASA/FTD がスレッド名「License Thread」でトレースバックおよびリロードすることがある |
| CSCvs94061 | クロックのずれとトラフィックの中断を引き起こすNTP スクリプトエラー |
| CSCvs97863 | フラッシュファイルシステムでのクローズ時の fsync コールの数を減らす |
| CSCvt00113 | SNMP コミュニティストリングのメモリリークによる ASA/FTD トレースバックおよびリロード |
| CSCvt01282 | CCM レイヤ（スプリント 79）での WR6 および WR8 コミット ID の更新 |
| CSCvt01397 | LINA 設定がプッシュされなかったにもかかわらず、展開は正常としてマークされる |
| CSCvt02409 | FPR9300 3 ノードクラスタのネストされた VLAN トラフィックで 9.12.2.151 snp_cluster_ingress がトレースバックする |
| CSCvt03598 | Cisco ASA ソフトウェアおよび FTD ソフトウェア Web サービスの読み取り専用パストラバーサルの脆弱性 |
| CSCvt05862 | サーバーが管理インターフェイスを介して到達可能な場合、IPv6 DNS サーバーの解決が失敗する |
| CSCvt06606 | フローオフロードが FTD 6.2(3.10) と FXOS 2.6(1.169) の組み合わせで機能しない |
| CSCvt06841 | ASA でのキャプチャを使用して設定すると、誤ったアクセスリストのヒットカウントが表示される |
| CSCvt11742 | ASA/FTD がスレッド名「ssh」でトレースバックし、リロードすることがある |
| CSCvt12463 | ASA：Unicorn Admin Handler スレッドでのトレースバック |
| CSCvt13730 | FP1010/2100 - FTD：リリース 6.6.0 への FTD アップグレード後の管理ポートのダウン/ダウン |

| 不具合 ID | タイトル |
|---|---|
| CSCvt15062 | FTD 2100：デバイスのリブート時に BYPASS から NON-BYPASS への移行中にパケットがドロップする |
| CSCvt16642 | FMC がリモートの syslog サーバーに対して一部の監査メッセージを送信していない |
| CSCvt18337 | アップグレード後に HA ノードでフェールオーバーが無効になった |
| CSCvt20709 | SSL を挿入した RESET での方向が誤っていたため、誤ったインターフェイスから出力され、MAC フラップが発生する |
| CSCvt21041 | スレッド「ctm_ipsec_display_msg」での FTD のトレースバック |
| CSCvt23643 | データを復旧するための、VPN フェールオーバーリカバリに約 30 秒かかる |
| CSCvt24328 | FTD：lina_host_file_open_raw 関数に関連するトレースバックとリロード |
| CSCvt26031 | ASAv が IPv6 を使用してスマートライセンスを登録できない |
| CSCvt26067 | セカンダリインターフェイスが FTD で使用されている場合、アクティブ FTP が失敗する |
| CSCvt28182 | sctp-state-bypass がインライン FTD に対して呼び出されない |
| CSCvt29049 | FPR2100：アプライアンスモードでの ASA の SNMP 遅延 |
| CSCvt30731 | CCM レイヤ（スプリント 80）での WR6、WR8 および LTS18 コミット ID の更新 |
| CSCvt34894 | Snort が過剰なメモリを消費し、パフォーマンスの問題を引き起こす。 |
| CSCvt35233 | DAQ モジュール process_snort_verdict 判定ブラックリストからの過剰なロギング |
| CSCvt35945 | 9.8 トレインで SSH バージョン2を有効にする場合に Encryption-3DES-AES が必要であってはならない |
| CSCvt36542 | FPR 上のマルチコンテキスト ASA/LINA が DHCP リリースメッセージを送信しない |
| CSCvt37881 | https のブロックページが機能しない |
| CSCvt38279 | ISA3000 で disk0 を消去すると、ファイルシステムがサポートされなくなる |
| CSCvt39135 | SSL ポリシーが適用された状態で、SSL 以外のトラフィックが少ないときに Snort インスタンスにより CPU が 90% を超えてスパイクする |

| 不具合 ID | タイトル |
|---|---|
| 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 |
| CSCvt43967 | ゼロを含む長さが 46 バイト以下のパディングパケットを RA トンネルから受信した |
| CSCvt45206 | アップグレード前に存在していたイベントを検索すると、イベント検索が失敗することがある |
| CSCvt45863 | IP ヘッダーの長さがパケット長と一致しない場合に暗号リングが停止する |
| CSCvt46289 | Firepower 1000 シリーズで ASA LDAPS 接続が失敗する |
| CSCvt46830 | FPR2100 「show crypto accelerator statistics」 カウンタは対称暗号を追跡しない |
| CSCvt50528 | ASA/FTD - CLI での証明書のインストールに関するデフォルト設定の警告メッセージ |
| CSCvt50946 | CSCvi42008 の修正にもかかわらず stuck uauth エントリが AnyConnect ユーザー接続を拒否する |
| CSCvt51346 | PKI-CRL：ダウンロード時のメモリリークおよび大きな CRL のクリア |
| CSCvt51348 | PKI-CRL：ループ内の大きな CRL をクリアせずにダウンロードした時のメモリリーク |
| CSCvt51349 | フラグメント所有者に転送されたフラグメント化されたパケットが、データ インターフェイス キャプチャで表示されない |
| CSCvt51987 | ASA FPR9300 SM56 での 80 サイズのブロックの枯渇によりトラフィックが停止する |
| CSCvt52607 | SSL HW モードのフローテーブルメモリの使用率を引き下げて Snort が D 状態になる確率を低減する |
| CSCvt52782 | ASA トレースバックスレッド名：webvpn_task |
| CSCvt53640 | SFR を 6.4.0 から 6.4.0.9-34 にアップグレードした後の ASA5585 トレースバックおよびリロード |
| CSCvt54182 | FTD が SSL 複合を実行するように設定されている場合に LINA コアが生成される |
| CSCvt59015 | KP IOQ ドライバ。防御パラメータと状態チェックを追加する。 |
| CSCvt59770 | FTD：SCEP を介した証明書の取得の失敗により停止する |

| 不具合 ID | タイトル |
|---|---|
| CSCvt61370 | 通信のデッドロックが原因で、デバイスからのイベントが停止することがある |
| CSCvt63484 | igb_saleen_io_sfp_mod_poll_thre プロセスにより ASA の CPU 使用率が高くなる |
| CSCvt64035 | remote acess mib：ラップアラウンド前に SNMP 64ビットのみが 4Gb を報告する |
| CSCvt64270 | ASA が、誤った宛先 MAC アドレスを持つフェールオーバーインターフェイス チェック制御パケットを送信している |
| CSCvt64822 | ASA が SSL ハンドシェイク後にトレースバックし予期せずリロードすることがある |
| CSCvt65982 | RRI ルートの削除時にスレーブユニットでルートフォールバックが発生しない |
| CSCvt66351 | NetFlow のレポートのフローのバイト数が非常に大きい |
| CSCvt68131 | スレッド「IKEv2 Mgd Timer Thread」で FTD がトレースバックし、リロードする |
| CSCvt68294 | Firepower 4120 の最大 VPN セッション制限を 20,000 に調整する |
| CSCvt68819 | アップグレード前に存在していたイベントをコピーすると、クリップボードへのコピーが失敗することがある |
| CSCvt73806 | FP2120 LINA アクティブボックスでの FTD のトレースバックとリロード。[VPN] |
| CSCvt75241 | FPR2100 で FTD をリロードした後、VPN でアドバタイズされたスタティックルートの再配布が失敗する |
| CSCvt75741 | netsnmp-5.8 を AES 192/256 サポートでコンパイルする |
| CSCvt79777 | sfipproxy.conf で IP アドレスが重複している |
| CSCvt79988 | FMC を 6.6 にアップグレードした後、SNMP 設定が原因でポリシー展開が失敗する |
| CSCvt80126 | CLI の「show asp table socket 18421590 det」で ASA がトレースバックし、リロードする |
| CSCvt83133 | group-url を使用して Google Chrome から anyconnect webvpn ポータルにアクセスできない |
| CSCvt85815 | 「機密データの検出」を有効にすると、ポリシーの展開が失敗する |

| 不具合 ID | タイトル |
|---|---|
| CSCvt86188 | 診断インターフェイスを介して SNMP トラップを生成できない |
| CSCvt90330 | スレッド名 coa_task での ASA トレースバックおよびリロード |
| CSCvt91258 | FDM：管理ゲートウェイとしてデータインターフェイスを使用して、どの NTP サーバーにも到達しない |
| CSCvt91521 | 暗号化アクセラレータバイアス設定を show tech に含める必要がある |
| CSCvt92647 | ASA のアップグレード後に、IPv6 アドレスで設定されたステートリンクを介した接続が失われる |
| CSCvt93142 | ASA は、クライアント認証の証明書にヌルシーケンスのエンコーディングを許可する必要がある。 |
| CSCvt93177 | デフォルトでフルプロキシを無効化してライトウェイトプロキシにする。（FP2LWP）FTD デバイス |
| CSCvt95517 | FTD 上の AnyConnect の証明書マッピングが機能しない。 |
| CSCvt97917 | AWS 9.13.1.7 BYOL イメージ上の ASAv を PLR に対して有効にできない |
| CSCvt98599 | IKEv2 コールアドミッション統計情報の「Active SAs」カウンタが実際のセッション数と同期していない |
| CSCvu00112 | ssh クォータ制限が ci_cons_shell でヒットしたときに tsd0 がリセットされない |
| CSCvu01039 | トレースバック：アクティブなトラフィックでの FTD インラインセットタップモード設定の変更 |
| CSCvu03107 | AnyConnect 統計情報が %ASA-4-113019 と RADIUS アカウンティングの両方で二重になる |
| CSCvu03562 | ユーザー名とパスワードを入力すると、デバイスの SSH 接続が失われる |
| CSCvu03675 | FPR2100：メモリ不足の状態で ASA コンソールがハングして応答しなくなることがある |
| CSCvu04279 | ASAv/AWS：AWS で C5 ASAv コードをアップグレードまたはダウングレードできない |
| CSCvu05180 | リモートアクセス VPN ポリシーの展開後、FTD で AAA サーバー設定が欠落している |
| CSCvu05216 | CRL CDP オーバーライドを指定する証明書マップでバックアップエントリが許可されない |
| CSCvu05336 | ASAv：SNMP プロセスでのトレースバックおよびリロード |

| 不具合 ID | タイトル |
|---|---|
| CSCvu05821 | タイムスタンプ形式が常に UTC で表示される |
| CSCvu07602 | FPR-41x5：「clear crypto accelerator load-balance」によりトレースバックおよびリロードが発生する |
| CSCvu07880 | QP プラットフォーム上の ASA で誤ったコアダンプファイルシステム領域（50 GB）が表示される |
| CSCvu08013 | DTLS v1.2 および AES-GCM 暗号を使用すると、特定のサイズのパケットが頻繁にドロップされる。 |
| CSCvu09199 | 6.7.0 FMC で 6.6.0 ftd イメージのプッシュ アップグレード イメージに 30 分かかる |
| CSCvu10053 | ASA トレースバックおよび関数 snmp_master_callback_thread のリロード |
| CSCvu10900 | 大量の ssl-certs-unified.log ファイルが、トラブルシューティングで 9GB に寄与 |
| CSCvu12039 | 起動後にスレーブユニットがクラスタマスターからの SCTP 設定の同期に失敗することがある |
| CSCvu12248 | ユーザーが AnyConnect VPN を使用して接続する場合の ASA-FPWR 1010 トレースバックおよびリロード |
| CSCvu12307 | FTD-HA：「ERROR：指定された AnyConnect クライアントイメージは存在しません。」 |
| CSCvu12684 | HKT：9.8.4.15 へのアップグレードでフェールオーバー時間が増加する |
| CSCvu13287 | FDM がサブジェクトまたは発行元のない証明書をインポートできず、アップグレードも失敗する |
| CSCvu15611 | FTD-HA：スタンバイが HA に参加できない「CD アプリ同期エラーはアプリ構成の適用に失敗しました」 |
| CSCvu17924 | DATAPATH での FTD フェールオーバーユニットのトレースバックおよびリロード |
| CSCvu17965 | 手動 NAT ルールのポート値を変更すると、ASA でトレースバックが生成され、リロードされる |
| CSCvu18510 | MonetDB のイベントデータベースのクラッシュにより、FMC 6.6.0 の接続イベントが失われる |
| CSCvu20007 | LINA からの Config_XML_Response の形式が正しくない。Lina が使用可能なメモリがないと報告している。 |

| 不具合 ID | タイトル |
|---|---|
| CSCvu20257 | CCM レイヤ（スプリント 85）での WR6、WR8 および LTS18 コミット ID の更新 |
| CSCvu23289 | 多数の neostore.transaction.db.* ファイルによってディスクがいっぱいになり、neo4j の問題が発生する |
| CSCvu25030 | スレッド名：CP processing での FTD 6.4.0.8 トレースバックおよびリロード |
| CSCvu26296 | ASA インターフェイス ACL が ASA からの snmp コントロールプレーン トラフィックをドロップしている |
| CSCvu26561 | Kerberos と統合すると、WebVPN SSO が予期しない結果になる |
| CSCvu26658 | SFDataCorrelator がバックアップ操作中にイベントをドロップすることがある |
| CSCvu29145 | Snort フロー IP プロファイリングでは、「system support flow-ip-profiling start」コマンドを使用して有効にできない |
| CSCvu29395 | アクティブな IGMP join でマスターロールの変更を実行中にトレースバックが発生した |
| CSCvu30512 | PKI-CRL：メモリトラッキングが有効になっている CRL のクリア中にトレースバックが発生した |
| CSCvu32698 | 「key config-key password-encryption」が存在する場合、クラスタに参加する際に ASA が SNMP でクラッシュする |
| CSCvu34413 | リロード後に ASA で SSH キーが失われる |
| CSCvu36539 | スマートライセンスデバイスが 6.2.2 -> 6.4.0 -> 6.6.0 にアップグレードされた場合、アップグレードが失敗する。 |
| CSCvu37547 | メモリリーク：リソース制限 MIB ハンドラが原因で、最終的にリロードが発生する |
| CSCvu38795 | 無効なインターフェイスの GOID エントリが原因で、トレースバック後に FTD ファイアウォールユニットがクラスタに参加できない |
| CSCvu40213 | スレッド名 kerberos_recv での ASA トレースバック |
| CSCvu40324 | フロールックアップ呼び出しトレースバックによる ASA トレースバックおよびリロード |
| CSCvu40398 | FIPS を有効にした後の FIPS SELF-TEST FAILURE による ASAv のリロード |

| 不具合 ID | タイトル |
|---|---|
| CSCvu40531 | pktmgr.out および lacp.out への FXOS LACP パケットロギングにより /opt/cisco/platform/logs が 100% になる |
| CSCvu42434 | ASA：実行中の SSH セッションがスタックしているため CPU 使用率が高い/ASA に SSH できない |
| CSCvu43924 | DHCP 検出パケットの GIADDR が dhcp-network-scope の IP アドレスに変更される |
| CSCvu45748 | スレッド名「ppp_timer_thread」での ASA トレースバック |
| CSCvu49625 | [PKI] 標準ベースの IKEv2 証明書認証セッションが 2 番目の userfromcert ルックアップを不必要に実行する |
| CSCvu53258 | FMC が証明書マップを誤って lina にプッシュする |
| CSCvu53585 | 6.6.0 へのアップグレード後に Elektra onbox ポリシーの展開が失敗する |
| CSCvu55843 | TACACS 承認ユーザーによる設定変更後の ASA トレースバック |
| CSCvu57834 | 100% CPU を使用する syslog-ng プロセス |
| CSCvu60011 | FTD：障害状態の HA に展開された Snort ポリシーの変更が完全に同期されない |
| CSCvu61704 | ASA の intel_82576_check_link_thread を使用した高い CPU 使用率がユニット全体のパフォーマンスに影響する |
| CSCvu63458 | FPR2100：show tech でクラッシュ出力を表示すると、最新のトレースバックからの出力が表示されない |
| CSCvu65070 | Lina 9.14：デバッグ snmp フレームワークを改善して agentx を使用し SIGHUP を回避する |
| CSCvu65688 | CSCvt98599 にもかかわらず、IKEv2 CAC の「Active SAs」カウンタが実際のセッション数と同期していない |
| CSCvu65843 | FP2100：6.6.0 での自動ネゴシエーションの変更によるファイバ SFP インターフェイスのダウン |
| CSCvu65936 | FDM 6.6.0 のアップグレード（または）configImport が EtherChannelInterface でフェールオーバーリンク検証の失敗として失敗する |
| CSCvu66119 | シリーズ 3 で URL ルールが誤って昇格されると、トラフィックが誤ったルールに一致する。 |
| CSCvu70529 | snort のリロード時にバイナリルール（SO ルール）がロードされない |
| CSCvu72094 | スレッド名 DATAPATH での ASA トレースバックおよびリロード |

| 不具合 ID | タイトル |
|---|---|
| CSCvu72278 | バージョン 1.41.0 より前の nghttp2 で、非常に大きな HTTP/2 SETTINGS fra |
| CSCvu72280 | PCR の pcre_jit_compile.c の compile_bracket_matchingpath 関数 |
| CSCvu72658 | AnyConnect 接続クライアント IP が断続的に OSPF にアドバタイズされない |
| CSCvu73207 | AnyConnect ユーザーへの DTLS パケットで保持されない DSCP 値 |
| CSCvu75594 | FTD：すでに適用されているキャプチャでキャプチャ バッファ オプションを変更する場合のトレースバックとリロード |
| CSCvu75930 | SMA リソースが枯渇すると、サービスモジュールがスーパーバイザにエラーを返さない |
| CSCvu75993 | トランスペアレント トラフィックが KVM で展開された FTDv を通過しない（ルーテッドモード） |
| CSCvu77095 | ASA がリマーク付きの ACE を削除できず、「指定されたリマークが存在しません」というエラーが表示される |
| CSCvu78721 | アップグレード後にインターフェイス速度を変更（修正）できない |
| CSCvu79125 | 高度なマルウェアリスクレポートの生成に失敗する |
| CSCvu80143 | 9.14.1.12 でトレースバック後に snmpd が戻らない |
| CSCvu82918 | HA 同期がスタンバイで予期しないエラーで失敗する |
| CSCvu83178 | EIGRP サマリールートがスタンバイに複製されず、スイッチオーバー後に停止する |
| CSCvu83599 | ASA がスレッド snmp_alarm_thread でトレースバックし、予期せずリロードすることがある |
| CSCvu90727 | EAP-TLS 認証を使用するネイティブ VPN クライアントが ASA に接続できない |
| CSCvu91105 | process_stdout.log ファイルが大きいため、/ngfw で管理対象外ディスクの使用率が高くなる |
| CSCvu98197 | 「復号しない」SSL 復号ルールに一致する HTTPS 接続がブロックされることがある |
| CSCvu98708 | ASA：HA：IPv6 インターフェイスのスタンバイで SNMP ポーリングが失敗する |
| CSCvv03130 | FTD clish で「show banner」コマンドを実行しても出力が返されない |

| 不具合 ID | タイトル |
|---|---|
| CSCvv04092 | イベントを表示しようとすると、誤った sql が生成される |
| CSCvv09944 | WCCP 設定がプッシュされているときに FTD 展開時に LINA がトレースバックする |
| CSCvv10948 | FDM アップグレード：UI で保留中の変更が表示されない（ただし、アップグレードは開始されていない） |
| CSCvv12273 | hardwareStatus MIB で複数の OID を持つ snmpget を使用した SNMP get-response が noSuchObject を返す |
| CSCvv12943 | 脅威データに FDM 6.5 以上のバージョンで、6.4 には存在していた GID：SID フィールドがない（CDO に影響） |
| CSCvv12988 | バックアップ中に tomcat が強制終了された後、正常に回復しない |
| CSCvv14442 | 将来のタイムスタンプを持つファイル/ディレクトリが含まれている場合、FMC バックアップの復元が失敗する |
| CSCvv17434 | Kenton5508 の 6.2.3 -> 6.6.1-50 アップグレードが失敗した |
| CSCvv21782 | 6.6.1：ASA SFR プラットフォームのすべてのトラフィックに対して無効な ID として表示されるプレフィルタポリシー値 |
| CSCvv26786 | 「プロセス名：lina」で ASA がトレースバックし、予期せずリロードする |
| CSCvv26845 | ASA：SNMP 機能でウォッチドッグのトレースバックとリロード |
| CSCvv27750 | ログがローテーションしないため、/ngfw で管理対象外ディスクの使用率が高くなる |
| CSCvv29275 | FMC OSPF エリアが 49 エントリまで制限される。50 番目のエントリを追加すると、プロセスは自動的に無効になる |
| CSCvv30371 | SNMP：VPN ポーリングのメモリリーク |
| CSCvv31334 | 6.6.1 ー 63 の KP HA でピアを切り替えようとすると、Lina のトレースバックとリロードが発生する（ネストされたクラッシュがロックされる） |
| CSCvv33013 | FDM：文字 ^ @ _ で秘密鍵を追加できない |
| CSCvv33621 | vftd：diskmanager のモニタリングがアップグレード時に正しく機能しない |
| CSCvv69991 | FTD が 6.6.1 へのアップグレード後にメンテナンスモードでスタックする |

# バージョン 6.6.0.1 で解決済みのバグ

表の最終更新日：2020-07-22

**表 *58* : バージョン *6.6.0.1* で解決済みのバグ**

| 不具合 ID | タイトル |
|---|---|
| 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 |
| CSCvu65843 | FP2100：6.6.0 での自動ネゴシエーションの変更によるファイバ SFP インターフェイスのダウン |

# バージョン 6.6.0 で解決済みのバグ

表の最終更新日：2020-05-28

**表 *59* : バージョン *6.6.0* で解決済みのバグ**

| 不具合 ID | タイトル |
|---|---|
| CSCvr25152 | 既存の外部認証オブジェクトを編集するときに（新しいユーザーの追加）、「名前が無効です（Name is invalid）」と表示される |
| CSCvr72708 | 6.6 接続イベントで 6.2.3/6.3.0/6.4.0/6.5.0 FTD の送信元 sgt が表示されない |
| 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 |
| CSCvq53002 | データの消去後、mysql のユーザーが削除済みとしてマークされていても引き続きユーザー制限にカウントされる |
| CSCvr51958 | ライト UI テーマのアラート通知がいつまでも回転し続ける |
| CSCvs70864 | 分析/ホスト/ネットワークマップ/アプリケーションプロトコルがいつまでもロード中になる |
| CSCvs40531 | AnyConnect 4.8 が FPR1000 シリーズで動作していない |
| 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。 |
| 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 |
| CSCvs78252 | TCP シーケンス番号ランダマイザが有効で SACK が使用されている場合、ASA/Lina のオフロード TCP フローが中断される |

| 不具合 ID | タイトル |
|---|---|
| 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 |
| 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 |
| CSCvq80147 | ASA SFR:：変数セットでネットワーク オブジェクト グループを使用するとすぐに展開が失敗する |
| CSCvr09468 | CLI 「Show nat pool」の ASA トレースバックとリロード |
| 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 |
| CSCvj65880 | ユーザーにルールインポートログを表示するための十分な権限がない場合の空白ページ |
| CSCvp95702 | CAC ログインボタンが新しい FMC GUI に表示されない |
| 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 |
| CSCvs24295 | 特定の証明書形式が原因で、ISE FMC サーバー証明書のドロップダウンが破損する |
| 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 |
| CSCvr94368 | 470_revert_prep.sh で mysql のマウント解除時に返送ステータスを確認する |
| CSCvs50459 | Cisco ASA および Cisco FTD の不正な OSPF パケット処理によるサービス拒否攻撃に対する脆弱性 |
| 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 |
| CSCvq55915 | 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 |
| CSCvq55929 | 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 |
| CSCvh20050 | Cisco Firepower システムソフトウェアの静的クレデンシャルの脆弱性：攻撃元区分がない |
| CSCvq07297 | Cisco Firepower Threat Defense ソフトウェアの HTTP フィルタリングバイパスの脆弱性 |

| 不具合 ID | タイトル |
|---|---|
| CSCvp72518 | .py ファイルが開始されないことを避けるためにブート/TID のスタートアップ中に毎回 .pyc ファイルがクリーンアップされることが、問題を引き起こす |
| CSCvo26597 | CLI バナーが FTD に表示されない |
| CSCvn28160 | LOM が更新されていない場合でも、LOM を使用したユーザーの設定が誤って成功する |
| CSCvq52582 | DCE/RPC NAP ポリシーが Vista 以降更新されていなかった |
| CSCvq72063 | FTD を削除すると、スマートライセンスが使用中のままになることがある |
| CSCvs61549 | 「snort 検証に失敗しました：不明なエラー（snort validation failed: Unknown error）」というメッセージで展開が失敗する、snort コア |
| CSCvr57984 | 名前のない FTD HA インターフェイスでの MAC アドレスの使用による展開の失敗 |
| CSCvs39202 | OSPF 認証設定がプッシュされた場合の展開の失敗 |
| CSCvi72863 | アクセス コントロール ポリシーで検査される管理トラフィックによる展開の不安定性 |
| CSCvr82965 | FCM から設定されていない場合、DNS エントリが /etc/resolv.conf および "show-network" に表示されない |
| CSCvq07838 | ドキュメント：FMC ガイドの API 例で、"DeploymentRequest" の "forceDeploy" 設定が true に設定されている |
| CSCvq74877 | ドキュメント：FTP トラフィックの推奨事項として、アプリケーションベースのルールが言及される必要がある |
| CSCvu24784 | ドキュメント：Firepower の互換性ページに 4112 ハードウェアの互換性情報がない |
| CSCvq00138 | ドキュメントに、FMC の復元後に侵入ルール/SRU を更新する必要があると記載されている。 |
| CSCvp33033 | Elektra が ext3 または ext4 の代わりに ext2 を使用する |
| 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 |
| CSCvr61575 | グローバルドメインで RA VPN を開くと、「オブジェクトは現在のドメインに属していません（Object does not belong to current domain）」というエラーが返される |
| CSCvq28406 | 6.3.0 での証明書のインポートの失敗に関するエラーが表示されない |

| 不具合 ID | タイトル |
|---|---|
| CSCvr05934 | 展開中に失敗した変数セットの検証に関するエラーレポートが、ユーザーにとって十分ではない |
| 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 |
| 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 |
| CSCvt55460 | SNMP アラートによる EventHandler のメモリリーク |
| CSCvs88209 | FMC と ASA/LINA の間の拡張コミュニティストリングの不一致 |
| CSCvr69380 | LDAPS Over SSL の外部認証設定で証明書の保存に失敗する |
| CSCvr27850 | FTD での SSH アクセスで、LDAP および Radius を使用した外部認証が失敗する |
| CSCvs12946 | 顧客がパスワード制限を設定している場合、FMC での CLI からの外部認証が失敗する |
| CSCvq72292 | アグレッシブモードを使用して複数のサイト間を展開できない |
| CSCvt82003 | VPN トンネルステータスの誤検出アラート |
| CSCvq76964 | 異常なモジュール FlexFlash コントローラ 1 の古いファームウェアに関連する障害 |
| CSCvr43341 | FDM 6.5.0：トランクインターフェイスを使用してアップグレードした場合、FPR1000 GUI が応答しなくなる |
| CSCvs88151 | カスタムトークンによる FDM 認証の失敗 |
| CSCvt80401 | 高可用性同期の完了に失敗するため、セカンダリ HA FTD で FDM GUI を使用できない |
| CSCvs64470 | FDM のオンボックス展開がエラー java.lang.NullPointerException で失敗する |
| CSCvs26443 | FDM で OSPF のサブインターフェイスを設定する際にトップダウン方式のアプローチを許可するべきである |
| CSCvs17981 | オブジェクトが RA VPN で使用されている場合、FDM がネットワークオブジェクトのネットワークから範囲への変更を許可するべきではない |
| CSCvs70704 | 6.5 への FDM のアップグレードが 100_ftd_onbox_data_import.sh.log で失敗する（「syslog を有効にすることはできません...（You cannot enable syslog with event...）」） |

| 不具合 ID | タイトル |
|---|---|
| CSCvq89794 | FDM：ユーザーダウンロードが LDAPS で機能しない |
| CSCvs47880 | RA VPN の DNS IP を変更する Firepower Device Manager（FDM）オプションが設定に反映されない |
| 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 |
| CSCvq32660 | FlexConfig が特殊文字に正しいエンコーディングを使用する必要がある |
| CSCvr30694 | FMC：FMC が HA 同期の失敗を検出する |
| CSCvq51795 | sftunnel の問題が原因で自動登録が失敗した場合、FMC がデバイスの詳細をクリーンアップしなかった |
| CSCvq11960 | FMC で 1 つのプレフィックスリスト エントリ内に同じ IP アドレス値のエントリが許可されない |
| CSCvr80621 | SecurID RSA を使用した FMC 外部認証は、バナーが有効になっている場合に失敗する |
| CSCvi97028 | 到達不能な syslog サーバーを設定すると fmc GUI が低速になる |
| CSCvp98570 | FMC が AAB と snort preserve-connection 設定を FTD にプッシュしない |
| CSCvq12758 | FMC が、スマートライセンスの登録解除後に FTD に "strong-encryption-disable" コマンドを展開するべきではない |
| CSCvp10983 | FMC でアクセスポリシールールの作成/編集中に無効な IP/範囲の入力を許可するべきではない |
| CSCvs23591 | FMC で 2 つの同一の VPN トンネルの設定を許可するべきではない |
| CSCvr49229 | FMC が sfmbservice で高い Cpu を示す |
| CSCvr72372 | FMC SLR 登録、SSMS サテライトからの移行後にデバイスがライセンス解除される |
| 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 |
| CSCvq54176 | FTD：新しいカスタム IKE ポリシーが適用されない、またはデフォルトポリシーを上書きする |
| CSCvs05084 | プロキシが原因の FTD Cisco Cloud 設定の失敗 |
| 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 |

| 不具合 ID | タイトル |
|---|---|
| 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 |
| 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 |
| CSCvr97778 | FTD 登録証明書がスタンバイ FMC で取り消され、デバイスが登録保留中になる |
| CSCvr75274 | 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 |
| 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 |
| 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 |
| CSCvm86658 | snap_get_retaddr_mips の snap.h:285 での FTD トレースバックおよびリロード |
| CSCvs91389 | FTD トレースバック Lina プロセス |
| CSCvq34340 | 出力最適化機能による 9344 ブロックサイズの枯渇による FTD トラフィックの停止 |
| CSCvr63858 | FTD のアップグレードが 600_schema/099_pre_multischema.pl で失敗する |
| 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 |
| 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 |
| CSCvq52914 | 展開の失敗を引き起こす可能性がある非常に大きな NAT ルールのエラーチェックを実装する |
| CSCvi09009 | インポートの失敗：インポートパッケージの抽出中のメモリ不足 |
| CSCvr33239 | ダッシュボード [セキュリティインテリジェンス統計（Security Intelligence Statistics）] のデータが正しくない |
| 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 |
| CSCvr82716 | 復号不可サイトリストが不十分だと、証明書ピニングが原因でTLS接続が失敗する |
| CSCvu35427 | SFR モジュールインスペクションを使用した 5500-X プラットフォームでの断続的な遅延 |

| 不具合 ID | タイトル |
|---|---|
| CSCvp19068 | SMTP パケットの侵入イベントのパケット情報に不完全なフィールドが表示され、ダウンロードされた pcap は正しい |
| CSCvq97698 | jQuery Object.prototype プロパティインジェクションの脆弱性 |
| CSCvq35512 | LINA が "\" をそのまま、無効な UTF-8 エンコーディングに変換せずに、受け入れる必要がある |
| 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 |
| CSCvq42723 | 無効にした後でも、GUI でイベントビューアへのロギングが有効になる |
| CSCvp20745 | セカンダリ FMC の手動設定時刻が常に 2019 年 3 月 5 日 13:57 にリセットされる |
| 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 |
| CSCvq95694 | メモリリーク SSL_ALLOC [ERROR] ssl_alloc.c:113:ssl_alloc_destroy() |
| CSCvn81332 | 同じ netmap_num を持つ複数のドメイン |
| 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 |
| CSCvo66039 | クラスタインターフェイス（CCL）と同じ番号で始まる ID を持つポートチャネルを編集できない |
| CSCvr92617 | SecurityIntelligenceEoConvertor の NPE によって、Lucene のインデックスの作成が失敗する |
| CSCvt27585 | スタンバイからのフェールオーバー切り替え実行中に KP でのクラッシュが確認された |
| CSCvt11728 | FDM で、vdb が現在のバージョンに複数回更新される |
| 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 |
| CSCvr76487 | 存在しないイメージをレポートで使用すると、PDF レポートが明確なエラーなしで失敗する |
| CSCvr50621 | 標準アクセスリストオブジェクトに 128.0.0.0/1 が含まれていると、ポリシーの展開が失敗する |
| 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 |
| CSCvr25705 | ポリシー展開の失敗が、設定の取得に失敗したと誤って報告される |

| 不具合 ID | タイトル |
|---|---|
| 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 |
| 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 |
| CSCvr67375 | HA のプライマリ FMC 6.3.0.3 がヘルスアラートの受信を突然停止する |
| CSCvp20905 | [プロトコル（Protocols）] フィールドが、[ポリシー（Policies）] -> [DNS/QQ アプリケーションのアプリケーションディテクタ（Application Detectors for DNS/QQ Apps）] の下に誤って追加される |
| CSCvr97009 | URL カテゴリを使用する場合、QoS（レート制限）が適用されない |
| CSCvq43413 | URL リストを使用する QoS ルールが FTD センサーの qos.rules ファイルにプッシュされない |
| CSCvs44149 | 大規模なオブジェクトグループを追加すると、調整レポートにすべてのネットワークが表示されない |
| CSCvs61421 | ホストのタイムアウトが長いため、SFDataCorrelator の再設定に時間がかかりすぎる |
| CSCvs14931 | GET ftddevicehapairs 応答の REST API コールに正しくない FTD-HA ステータスが表示される |
| CSCvt08466 | インターフェイス範囲を使用する REST API ポストが、チェック検証なしで FMC に追加される |
| CSCvc05004 | エラー「Lights-Out 管理ユーザーをクリアできません（Unable to clear Lights-Out Managment Users）」が発生して復元に失敗する |
| CSCvr30869 | レトロスペクティブ相関マルウェアアラートが、不要なスペースでエンコードされた base64 で送信される |
| 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 |
| CSCvr39556 | libclamav.so のセグメンテーション違反（SFDataCorrelator のコンテキスト内） |
| 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 |
| 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 |
| CSCvr17735 | SI 更新時の SFDataCorrelator で CPU の使用率が高くなる |

| 不具合 ID | タイトル |
|---|---|
| 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 |
| CSCvq39344 | SNMPv3 GET/WALK が正常に応答しない |
| 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 |
| CSCvr41230 | SFR モジュールで設定されたアイドルタイムアウトよりも前に Snort セッションがタイムアウトする |
| 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 |
| CSCvr24059 | 送信元 SGT の相関が FMC および FTD 6.5 で機能しない |
| CSCvq46674 | SRU 更新によりプリプロセッサルールのアラートしきい値が削除される |
| CSCvs33297 | FDM によって管理される FTD で、SSL キー再生成間隔が「分」でラベル付けされるべきときに「秒」でラベル付けされる。 |
| CSCvt10875 | FTD HA 間の show running config sync が原因で、Syslog アラートに誤ったホスト名が表示される |
| CSCvr95581 | [システム（System）]->[更新（Updates）]ページにアクセスしようとすると、System 500 の内部エラーが発生する |
| CSCvs82369 | 脅威データの更新：Cisco Cloud 設定：失敗 |
| CSCvr89663 | トレースバック：スレッド名 pix_flash_config_thread で WM1010 がリブートループに陥る |
| CSCvn32473 | IPV6 アドレスがデバイスによって使用される場合の FMC と FTD の間のファイルパス競合のトラブルシューティング |
| CSCvq52770 | Web トラフィックをプロキシするアンチウイルスソフトウェアで TSAgent が正しく動作しない |
| CSCvs05932 | /128 または ::/0 FMC 6.3 を使用して ipv6 ホストオブジェクトを追加できない |
| CSCvr82372 | ライセンスエラーが原因で snmpv3 を有効にできない |
| CSCve93565 | FMC でサブジェクト代替名（SAN）を使用して証明書を生成できない |
| CSCvs96054 | 仮想 FMC からハードウェア 2600 への移行後に 25 台を超えるデバイスを登録できない |

| 不具合 ID | タイトル |
|---|---|
| CSCvr92596 | アップグレードスクリプト 470_revert_prep.sh が、grep コマンドが原因でパーティションが多すぎる場合にハングする |
| CSCvs58934 | パスワードを更新する際に「ライトアウト管理のユーザーがすでに存在します（User already exists for lights-out management）」というエラーが表示される |
| CSCvr41377 | グループ名が重複している場合、ユーザーのダウンロードが失敗する |
| CSCvr67542 | vFMC 6.6.0 でアップグレードに少なくとも 28 GB が必要となる |
| 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 |
| CSCvq52636 | ルートで複数のオブジェクトをより具体的にする必要がある場合の、ポリシー展開が失敗する可能性の警告 |
| CSCvr98194 | カラムを無効にするとイベントが集約される場合にユーザーに警告する |

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。