互換性

一般的な互換性情報については、次を参照してください。

- Cisco Firepower Compatibility Guide：バンドルされている OS やその他のコンポーネントのバージョンやビルドを含む、サポート対象のすべてのバージョンの詳細な互換性情報、および廃止されたプラットフォームの販売終了やサポート終了の通知へのリンク。
- Cisco NGFW 製品ラインのソフトウェアリリースおよび持続性に関する速報：管理プラットフォームやオペレーティングシステムなど、シスコ□次世代ファイアウォール製品ラインに関するサポートタイムライン。

本バージョンの互換性情報については、次を参照してください。

Firepower Management Center

Firepower Management Center は、一元化されたファイアウォール管理コンソールを提供するフォールトトレラントな専用ネットワーク アプライアンスです。Firepower Management Center Virtual は、仮想環境に完全なファイアウォール管理機能を提供します。

Firepower Management Center

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

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

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

Firepower Management Center Virtual

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

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

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

- Firepower Management Center Virtualカーネルベース仮想マシン（KVM）用
- Firepower Management Center VirtualVMware vSphere および VMware ESXi 6.0、6.5、6.7 用

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

Firepower デバイス

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

（注） これらのリリースノートには、本リリースでサポートされているデバイスが掲載されています。古いデバイスが EOL に達していて、アップグレードできなくなった場合でも、数バージョンの範囲内であれば、より新しい FMC を使用してそのデバイスを管理できます。同様に、より新しいバージョンの ASDM では、より古いバージョンの ASA FirePOWER モジュールを管理できます。下位互換性を含む、サポート対象の管理方法については、「マネージャとデバイスの互換性 （5 ページ）」を参照してください。

表 *1 : バージョン 6.6.0/6.6.x の Firepower Threat Defense*

FTD プラットフォーム	OS/ハイパーバイザ	詳細情報
Firepower 1010、1120、1140、1150 Firepower 2110、2120、2130、2140	—	—

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

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

表 *2 :* バージョン *6.6.0/6.6.x* の *NGIPS/ASA FirePOWER*

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

マネージャとデバイスの互換性

Firepower Management Center

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

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

表 *3 : FMC*とデバイス間の互換性

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

Firepower Device ManagerおよびCisco Defense Orchestrator

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

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

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

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

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

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

表 *4 : FTD* との *FDM* および *CDO* の互換性

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

Adaptive Security Device Manager

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

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

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

表 *5 : ASDM* と *ASA FirePOWER* の互換性

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

ASA FirePOWER のバージョン	最小 ASDM バージョン
6.2.3	7.9.2

Web ブラウザの互換性

ブラウザ

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

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

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

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

ブラウザの設定と拡張

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

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

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

一部のブラウザ拡張機能では、PKI オブジェクトの証明書やキーなどのフィールドに値を保存できないことに注意してください。これらの拡張機能には Grammarly や Whatfix Editor などがありますが、それに限りません。この問題は、これらの拡張機能によってフィールドに文字

（HTML など） が挿入され、システムが無効と見なすために発生します。シスコの製品にログインしている間は、これらの拡張機能を無効にすることをお勧めします。

セキュア通信

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

自己署名証明書の置き換えを開始する手順は、次のとおりです。

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

詳しい手順については、オンラインヘルプまたはご使用の製品の構成ガイドを参照してください。

（注） 自己署名証明書を置き換えない場合は、次の手順を実行します。

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

監視対象ネットワークからの参照

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

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

画面解像度の要件

表 *6 :* 画面解像度の要件

インターフェイス	解決策
Firepower Management Center	1280 X 720
Firepower Device Manager	1024 X 768
ASA FirePOWER moduleを管理している ASDM	1024 X 768
Firepower 4100/9300 用 Firepower Chassis Manager	1024 X 768