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 （5 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 *1 :* 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 （5 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 *2* : 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 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	対応	—	対応	対応	FXOS 2.8.1.15 以降のビルドが必要です。 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 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 *3 :* 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 *4 :* 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。 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。 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。 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。

表 *5: 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）。 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）。 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。

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。