システム要件

このドキュメントでは、Version7.0 のシステム要件を記載します。

デバイスプラットフォーム

このドキュメントでは、Version7.0 でサポートされているデバイスと管理方法を記載します。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。

デバイスの管理方式

次のデバイス管理方法をサポートしています。

- Firepower Management Center：複数のデバイスをリモートで管理します。FMC は、お客様が導入したハードウェアまたは仮想プラットフォームとして、または Cisco Defense Orchestrator（CDO）プラットフォームを使用するシスコが管理するクラウド導入として利用できます。お客様が導入したハードウェアまたは仮想 FMC では、その管理対象デバイスと同じかより新しいバージョンを実行する必要があります。クラウド提供型の管理センターにはバージョンの概念がなく、シスコが機能を更新します。
- Firepower Device Manager：単一の FTD デバイスをローカルで管理します。
- FDM 搭載 Cisco Defense Orchestrator（CDO）：FMC の代わりに、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：単一の ASAFirePOWER モジュールをローカルで管理します。ASA FirePOWER は、ASA デバイスに個別にインストールされるモジュールです。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。

FTD ハードウェア

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 *1 : Version7.0 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	
Firepower 1010、1120、1140、1150	**YES**	**YES** 7.0.3 以降のバージョンが必要です。	**YES**	**YES**	—
Firepower 2110、2120、2130、2140	**YES**	**YES** 7.0.3 以降のバージョンが必要です。	**YES**	**YES**	—
Firepower 4110、4120、4140、4150 Firepower 4112、4115、4125、4145	**YES**	**YES** 7.0.3 以降のバージョンが必要です。	**YES**	**YES**	FXOS 2.10.1.159 以降のビルドが必要です。
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	**YES**	**YES** 7.0.3 以降のバージョンが必要です。	**YES**	**YES**	FXOS 2.10.1.159 以降のビルドが必要です。

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	
ASA 5508-X、5516-X	**YES**	**YES** 7.0.3 以降のバージョンが必要です。	**YES**	**YES**	最新の ROMMON イメージが必要です。Cisco Secure Firewall ASA および Cisco Secure Firewall Threat Defense 再イメージ化ガイドを参照してください。
ISA 3000	**YES**	**YES** 7.0.3 以降のバージョンが必要です。	**YES**	**YES**	最新の ROMMON イメージが必要です。Cisco Secure Firewall ASA および Cisco Secure Firewall Threat Defense 再イメージ化ガイドを参照してください。

FTDv

仮想版 FTD の導入により、スループット要件とリモートアクセス VPN セッションの制限に基づいて、パフォーマンス階層型のスマート ソフトウェア ライセンスがサポートされます。オプションは、FTDv5（100 Mbps/50 セッション）から FTDv100（16 Gbps/10,000 セッション）までです。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、該当するスタートアップガイドを参照してください。

表 *2 : Version7.0 FTDv* パブリック クラウド 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	CDO および FDM
Amazon Web Services（AWS）	**YES**	**YES** 7.0.3 以降 のバージョンが必要です。	**YES**	**YES**
Microsoft Azure	**YES**	**YES** 7.0.3 以降 のバージョンが必要です。	**YES**	**YES**

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	CDO および FDM
Google Cloud Platform（GCP）	**YES**	**YES** 7.0.3 以降のバージョンが必要です。	—	—
Oracle Cloud Infrastrucure（OCI）	**YES**	**YES** 7.0.3 以降のバージョンが必要です。	—	—

表 *3 : Version7.0 FTDv* オンプレミス/プライベート クラウド 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	CDO および FDM
Cisco Hyperflex	**YES**	**YES** 7.0.3 以降のバージョンが必要です。	**YES**	**YES**
カーネルベース仮想マシン（KVM）	**YES**	**YES** 7.0.3 以降のバージョンが必要です。	**YES**	**YES**
Nutanix エンタープライズクラウド	**YES**	**YES** 7.0.3 以降のバージョンが必要です。	**YES**	**YES**
OpenStack	**YES**	**YES** 7.0.3 以降のバージョンが必要です。	—	—
VMware vSphere/VMware ESXi 6.5、6.7、または 7.0	**YES**	**YES** 7.0.3 以降のバージョンが必要です。	**YES**	**YES**

ASA FirePOWER および NGIPSv

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（*ASA FirePOWER* モジュール）です。NGIPSv は、仮想環境でソフトウェアを実行します。これらのデバイスは、クラウド提供型の FMC では管理できません。

表 *4 : Version7.0ASA FirePOWER* および *NGIPSv* プラットフォーム

デバイスのプラットフォーム	FMC 互換	ASDM の互換性	注記
ASA 5508-X with FirePOWER Services ASA 5516-X with FirePOWER Services ISA 3000 with FirePOWER Services	**YES**	ASDM 7.16(1) が必要です。	ASA 9.5(2) ～ 9.16(x) が必要です。 最新の ROMMON イメージが必要です。Cisco Secure Firewall ASA および Cisco Secure Firewall Threat Defense 再イメージ化ガイドを参照してください。
NGIPSv	**YES**	—	VMware 6.5、6.7、または 7.0 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。

FMC プラットフォーム

このセクションでは、Version7.0 でサポートされている、お客様が導入したハードウェアと仮想 FMC を示します。クラウド提供型の管理センターの互換性情報については、『FMC でのデバイス管理 （6 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

Version7.0 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

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 Firepower ホットフィックス リリース ノート を参照）。

FMCv

Version7.0 は、次の FMCv プラットフォームをサポートしています。

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。一部のプラットフォームのみが FMCv300 をサポートすることに注意してください。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 スタートアップガイド を参照してください。

表 *5 : Version7.0 FMCv* パブリック クラウド プラットフォーム

プラットフォーム	FMCv2、10、25	FMCv300
Amazon Web Services（AWS）	**YES**	—
Google Cloud Platform（GCP）	**YES**	—
Microsoft Azure	**YES**	—
Oracle Cloud Infrastrucure（OCI）	**YES**	—

表 *6 : Version7.0 FMCv* オンプレミス/プライベート クラウド プラットフォーム

プラットフォーム	FMCv2、10、25	FMCv300
Cisco HyperFlex	**YES**	—
カーネルベース仮想マシン（KVM）	**YES**	—
Nutanix エンタープライズクラウド	**YES**	—
OpenStack	**YES**	—
VMware vSphere/VMware ESXi 6.5、6.7、または 7.0	**YES**	**YES**

FMC でのデバイス管理

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。

お客様が導入した FMC

お客様が導入したハードウェアまたは仮想 FMC では、その管理対象デバイスと同じかより新しいバージョンを実行する必要があります。これは、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。

表 *7: 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
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
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）。

クラウド提供型の管理センター

クラウド提供型の管理センターは、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。機能の更新

はシスコが行います。クラウド提供型の管理センターは、以下を実行する Threat Defense デバイスを管理できます。

- 7.0.3 以降のメンテナンスリリース
- バージョン 7.2.0 以降

クラウド提供型の管理センターは、バージョン 7.1 を実行している脅威防御デバイス、または任意のバージョンを実行している従来のデバイスを管理できません。クラウド管理を登録解除して無効にしない限り、クラウド提供型の管理センターに登録されている脅威防御デバイスをバージョン 7.0.x からバージョン 7.1 にアップグレードすることはできません。バージョン 7.2 以降に直接アップグレードすることをお勧めします。

クラウド管理型のデバイスは、イベントのログ記録と分析の目的でのみ、バージョン 7.2 以降のお客様が導入した管理センターに追加できます。あるいは、シスコのセキュリティ分析とロギング（SaaS）シスコのセキュリティ分析とロギング（SaaS） を使用して、Cisco Cloud にセキュリティイベントを送信できます。

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 Edge（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 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 Edge 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 Edge を使用している場合は、IE モードを有効にしないでください。

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：[Device] をクリックしてから **[System Settings]** > **[Management Access]** リンクをクリックし、次に [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。