システム要件

このドキュメントでは、バージョン 7.2 のシステム要件を記載します。

- Threat Defense プラットフォーム （1 ページ）
- Management Center プラットフォーム （3 ページ）
- Management Center （5 ページ）
- ブラウザ要件 （6 ページ）

Threat Defense プラットフォーム

このドキュメントでは、バージョン 7.2 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 を参照してください。

デバイスの管理方式

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。

- Secure Firewall Management Center：複数のデバイスをリモートで管理します。

  management center は、顧客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実装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management centerは、管理対象デバイスと同じまたは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では、バージョンの概念はなく、機能の更新が処理されます。

- Secure Firewall Device Manager：単一の Threat Defense デバイスをローカルで管理します。

  必要に応じて、management center の代替策として、Cisco Defense Orchestrator（CDO）を追加し、複数の Threat Defense 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 Device Manager が必要ですが、CDO を使用することで、展開したすべての Threat Defense 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。

Threat Defense ハードウェア

Threat Defense 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 :* バージョン *7.2 Threat Defense* ハードウェア

プラットフォーム（Platform）	Management Center 互換		Device Manager 互換		注記
	お客様が導入	クラウド提供型	Device Manager のみ	Device Manager + CDO	
Firepower 1010、1120、1140、1150	対応	対応	対応	対応	—
Firepower 2110、2120、2130、2140	対応	対応	対応	対応	—
Secure Firewall 3110、3120、3130、3140	対応	対応	対応	対応	—
Firepower 4110、4120、4140、4150 Firepower 4112、4115、4125、4145	対応	対応	対応	対応	FXOS 2.12.0.31 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	対応	対応	対応	対応	FXOS 2.12.0.31 以降のビルドが必要です。
ISA 3000	対応	対応	対応	対応	最新の ROMMON イメージが必要です。 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。

Threat Defense Virtual

仮想版 Threat Defense 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 :* バージョン *7.2 Threat Defense Virtual* 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	Management Center 互換		Device Manager 互換	
	お客様が導入	クラウド提供型	Device Manager のみ	CDO および Device Manager
Alibaba	対応	対応	—	—
Amazon Web Services（AWS）	対応	対応	対応	対応
Microsoft Azure	対応	対応	対応	対応
Google Cloud Platform（GCP）	対応	対応	対応	対応
Oracle Cloud Infrastrucure（OCI）	対応	対応	—	—

表 *3 :* バージョン *7.2 Threat Defense Virtual* 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	Management Center 互換		Device Manager 互換	
	お客様が導入	クラウド提供型	Device Manager のみ	CDO および Device Manager
Cisco Hyperflex	対応	対応	対応	対応
カーネルベース仮想マシン（KVM）	対応	対応	対応	対応
Nutanix エンタープライズクラウド	対応	対応	対応	対応
OpenStack	対応	対応	—	—
VMware vSphere/VMware ESXi 6.5、6.7、または 7.0	対応	対応	対応	対応

Management Center プラットフォーム

このセクションでは、バージョン 7.2 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 management center 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、『Management Center （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。

Management Center ハードウェア

バージョン 7.2 は次の management center ハードウェアをサポートします。

- FMC 1600
- FMC 2600
- FMC 4600

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）。

Management Center Virtual

バージョン 7.2 は、次の Management Center Virtual プラットフォームをサポートしています。

Management Center Virtual 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。さらに、FMCv2 は高可用性をサポートしていません。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 *4 :* バージョン *7.2 Management Center Virtual* 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（Platform）	FMCv2、10、25	FMCv300	ハイ アベイラビリティ
Alibaba	対応	—	—
Amazon Web Services（AWS）	対応	対応	対応
Google Cloud Platform（GCP）	対応	—	—
Microsoft Azure	対応	—	—
Oracle Cloud Infrastrucure（OCI）	対応	対応	対応

表 *5 :* バージョン *7.2 Management Center Virtual* 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（Platform）	FMCv2、10、25	FMCv300	ハイ アベイラビリティ
Cisco HyperFlex	対応	—	—
カーネルベース仮想マシン（KVM）	対応	—	—
Nutanix エンタープライズクラウド	対応	—	—

プラットフォーム（Platform）	FMCv2、10、25	FMCv300	ハイ アベイラビリティ
OpenStack	対応	—	—
VMware vSphere/VMware ESXi 6.5、6.7、または 7.0	対応	対応	対応

Management Center

すべての デバイスは、management center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 Management Center

お客様が導入したハードウェアまたは仮想management centerは、管理対象デバイスと同じまたは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 management center 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、management center 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。
- management center 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 management center をアップグレードする必要があります。

表 *6 : Management Center*とデバイス間の互換性

Management Center 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

Management Center バージョン	管理可能な最も古いデバイスバージョン
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。更新について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 以降のお客様導入の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
Management Center	1280 X 720
Device Manager	1024 X 768
Firepower 4100/9300 用 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。

- Management Center：**[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。

- Device Manager ：[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。

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。