システム要件

このドキュメントでは、バージョン 7.4 のシステム要件を記載します。

Management Center プラットフォーム

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します。Management Center とのデバイスの互換性については、「Threat Defense 管理 （4 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 Compatibility Guide を参照してください。

Management Center ハードウェア

バージョン 7.4 は次の Management Center ハードウェアをサポートします。

- Cisco Secure Firewall Management Center 1700、2700、4700
- Firepower Management Center 1600、2600、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 Secure Firewall Threat Defense/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 7.4 はパブリッククラウドとプライベートクラウドでの Management Center Virtual 導入をサポートします。

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。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。また、2 デバイスの仮想 Management Center 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 *1 :* バージョン *7.4 Management Center Virtual* プラットフォーム

プラットフォーム（Platform）	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	対応	対応
Google Cloud Platform（GCP）	対応	—	—
Microsoft Azure	対応	—	対応
Oracle Cloud Infrastrucure（OCI）	対応	対応	対応
プライベート クラウド			
Cisco HyperFlex	対応	—	対応
カーネルベース仮想マシン（KVM）	対応	対応	対応
Microsoft Hyper-V	対応 25 台のデバイスのみ。	—	対応
Nutanix エンタープライズクラウド	対応	—	—
OpenStack	対応	—	—
VMware vSphere/VMware ESXi 6.5、6.7、または 7.0	対応	対応	対応

クラウド提供型 Firewall Management Center

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。更新についてはシスコが行います。お客様が導入した Management Center は、仮想プラットフォームの場合でも、オンプレミスと呼ばれることが多いことに注意してください。

Threat Defense プラットフォーム

Threat Defense 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、「Threat Defense 管理 （4 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 Compatibility Guide を参照してください。

Threat Defense ハードウェア

バージョン 7.4 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 *2 :* バージョン *7.4 Threat Defense* ハードウェア

プラットフォーム	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 1010E、1010、1120、1140、1150	対応	対応	対応	対応	バージョン 7.4.1 以降が必要です。
Firepower 2110、2120、2130、2140	対応	対応	対応	対応	バージョン 7.4.1 以降が必要です。
Cisco Secure Firewall 3105、3110、3120、3130、3140	対応	対応	対応	対応	バージョン 7.4.1 以降が必要です。
Firepower 4112、4115、4125、4145 Firepower 9300 : SM-40、SM-48、SM-56 モジュール	対応	対応	対応	対応	バージョン 7.4.1 以降が必要です。 FXOS 2.14.1.131 以降のビルドが必要です。
Cisco Secure Firewall 4215、4225、4245	対応	対応	—	—	—
ISA 3000	対応	対応	対応	対応	バージョン 7.4.1 以降が必要です。 ROMMON の更新が必要な場合があります。Cisco Secure Firewall ASA and Secure Firewall Threat Defense Reimage Guideを参照してください。

Threat Defense Virtual

バージョン 7.4 Threat Defense Virtual 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 *3 :* バージョン *7.4 Threat Defense Virtual* 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	Device Manager + CDO
パブリック クラウド				
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	—	—
プライベート クラウド				
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

Threat Defense 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。

お客様が導入したManagement Center

すべてのデバイスは、お客様が導入した Management Center 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。

ほとんどの場合、旧バージョンのデバイスは Management Center 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。Threat Defense プラットフォーム （2 ページ） に記載されている特定の Management Center デバイスの組み合わせで、まれに問題が発生することがあります。

表 *4 :* お客様が導入した *Management Center* : デバイスの互換性

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
7.4	7.0
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

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
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 Firewall Management Center

クラウド提供型 Firewall Management Center は、次を実行している Threat Defense デバイスを管理できます。

- バージョン 7.2 以降
- 7.0.3 以降のメンテナンスリリース

クラウド提供型 Firewall Management Center は、バージョン 7.1 を実行している Threat Defense デバイス、または任意のバージョンを実行しているクラシックデバイスを管理できません。クラウド管理の登録を解除するか、または無効にしない限り、クラウド管理対象デバイスはバージョン 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 Management Center 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） 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。

Device Manager

Device Manager を使用すると、単一の Threat Defense デバイスをローカルに管理できます。

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。

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は実施していません。また、Management Center How-Tos 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**（⚙）> **[構成（Configuration）]** > **[HTTPS証明書（HTTPS Certificate）]** を選択します。

- 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。