Cisco Secure Firewall Management Center 互換性ガイド

最終更新：2025 年 4 月 8 日

Cisco 互換性ガイド

（注） すべてのソフトウェアバージョン、特にパッチがすべてのプラットフォームに適用されるわけではありません。バージョンがサポートされているか確認するには、そのバージョンのアップグレードまたはインストールパッケージが シスコ サポートおよびダウンロード サイト に掲載されているか確認するのが簡単な方法です。サイトにアップグレードまたはインストールパッケージが「見つからない」場合、そのバージョンはサポートされていません。リリースノートとサポート終了の通知 （21 ページ）を確認することもできます。バージョンが見つからないのは変だと思う場合は、Cisco TAC にお問い合わせください。

表 *1*：関連リソース

説明	リソース
持続性に関する速報には、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が記載されています。	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
互換性ガイドには、バンドルコンポーネントや統合製品など、サポートされているハードウェアモデルとソフトウェアバージョンに関する詳細な互換性情報が記載されています。	
リリースノートには、アップグレードの警告や動作の変更など、リリース固有の情報が記載されています。 リリースノートには、アップグレードおよびインストール手順へのクイックリンクも含まれています。	Cisco Firepower リリースノート
新機能ガイドには、リリースごとの新機能および廃止された機能が記載されています。	Cisco Secure Firewall Management Center の新機能（リリース別）

説明	リソース
ドキュメントロードマップには、現在使用可能なドキュメントおよび従来のドキュメントへのリンクがあります。 探している内容が上記にない場合は、ロードマップを試してください。	Cisco Secure Firewall Threat Defense ドキュメントにアクセス

推奨リリース：バージョン 7.4.2

新しい機能と解決済みの問題を利用するには、対象となるすべてのアプライアンスを最新パッチを含む推奨リリース以上にアップグレードすることをお勧めします。シスコサポートおよびダウンロード サイトでは、推奨リリースに金色の星が付いています。バージョン 7.2.6 以降または 7.4.1 以降では、新しい推奨リリースが使用可能になると Management Center から通知され、製品のアップグレードページに推奨リリースが表示されます。

古いアプライアンスの推奨リリース

アプライアンスが古すぎて推奨リリースを実行できず、ハードウェアを今すぐ更新しない場合は、メジャーバージョンを選択してから可能な限りパッチを適用します。一部のメジャーバージョンは長期または超長期に指定されているため、いずれかを検討してください。これらの用語の説明については、「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」を参照してください。

ハードウェアの更新に関心がある場合は、シスコの担当者またはパートナー担当者にお問い合わせください。

Management Center ハードウェア

バージョン 7.0 以降の FMCv は FXOS オペレーティングシステムを使用します。FMCv ソフトウェアをアップグレードすると、FXOS が自動的にアップグレードされます。バンドルされている FXOS バージョンについては、「バンドルされたコンポーネント （13 ページ）」を参照してください。

表 2 : *Management Center* ハードウェアの互換性

Management Center	Cisco Secure Firewall Management Center	Firepower Management Center				Defense Center
	1700 2700 4700	1600 2600 4600	1000 2500 4500	2000 4000	750 1500 3500	500 1000 3000
7.6	YES	YES	—	—	—	—
7.4	YES	YES	—	—	—	—

Management Center	Cisco Secure Firewall Management Center	Firepower Management Center				Defense Center
	1700 2700 4700	1600 2600 4600	1000 2500 4500	2000 4000	750 1500 3500	500 1000 3000
7.3	—	**YES**	—	—	—	—
7.2	—	**YES**	—	—	—	—
7.1	—	**YES**	—	—	—	—
7.0	—	**YES**	**YES**	—	—	—
6.7	—	**YES**	**YES**	—	—	—
6.6	—	**YES**	**YES**	**YES**	—	—
6.5	—	**YES**	**YES**	**YES**	—	—
6.4	—	**YES**	**YES**	**YES**	**YES**	—
6.3	—	**YES**	**YES**	**YES**	**YES**	—
6.2.3	—	—	**YES**	**YES**	**YES**	—
6.2.2	—	—	**YES**	**YES**	**YES**	—
6.2.1	—	—	**YES**	**YES**	**YES**	—
6.2.0	—	—	**YES**	**YES**	**YES**	—
6.1	—	—	—	**YES**	**YES**	—
6.0.1	—	—	—	**YES**	**YES**	—
6.0.0	—	—	—	**YES**	**YES**	—
5.4 *	—	—	—	**YES**	**YES**	**YES**

* 5.4.x デバイスを管理するには 5.4.1.x の Defense Center を使用します。

FMC ハードウェアの BIOS およびファームウェア

FMC ハードウェアの BIOS および RAID コントローラファームウェアのアップデートを提供します。FMC が要件を満たしていない場合は、適切なホットフィックスを適用してください。使いの FMC モデルとバージョンがリストになく、更新が必要だと思われる場合は、Cisco TAC までお問い合わせください。

表 *3: BIOS* およびファームウェアの最小要件

プラットフォーム	バージョン	ホットフィックス	BIOS	RAID コントローラのファームウェア	CIMC ファームウェア
FMC 1700、2700、4700	7.6 7.4	BIOS のアップデート ホットフィックス FC	C225M6.4.3.4b.0	52.26.0-5016	4.3(4.242038)
FMC 1600、2600、4600	7.6 7.4 7.3 7.2 7.1 7.0	BIOS のアップデート ホットフィックス FC	C220M5.4.3.2b.0	51.23.0-5009	4.3(2.240077)
	6.7 6.6 6.4	BIOS のアップデート ホットフィックス EN	C220M5.4.2.3b.0	51.10.0-3612	4.2(3b)
FMC 1000、2500、4500	7.0 6.7 6.6 6.4	BIOS のアップデート ホットフィックス EN	C220M5.4.2.3b.0	51.10.0-3612	4.2(3b)
	6.2.3	BIOS のアップデート ホットフィックス EL	C220M4.4.1.2c.0	24.12.1-0456	4.1(2g)
FMC 2000、4000	6.6 6.4 6.2.3	BIOS のアップデート ホットフィックス EI	C220M3.3.0.4e.0	23.33.1-0060	3.0(4s)
FMC 750、1500、3500	6.4 6.2.3	BIOS のアップデート ホットフィックス EI	C220M3.3.0.4e.0	23.33.1-0060	3.0(4s)

ホットフィックスは、BIOS および RAID コントローラファームウェアを更新する唯一の方法です。ソフトウェアをアップグレードしても、このタスクは実行されず、新しいバージョンに再イメージ化されません。FMC がすでに最新の状態である場合、ホットフィックスは効果がありません。

ヒント　これらのホットフィックスにより、CIMC ファームウェアも更新されます。解決された問題については、Cisco UCS ラックサーバソフトウェアのリリースノートを参照してください。一般に、CIMC の使用での設定の変更はサポートされていないことに注意してください。FMCただし、無効なCIMCユーザー名のロギングを有効にするには、最新のホットフィックスを適用してから、『Cisco UCS C-Series Servers Integrated Management Controller CLI Configuration Guide』バージョン 4.0 以降の「*Viewing Faults and Logs*」の章の手順に従ってください。

通常のアップグレードプロセスを使用して、ホットフィックスを適用します。シスコサポートおよびダウンロード サイト へのクイックリンクを含むホットフィックスのリリースノートについては、Cisco Secure Firewall Threat Defense/Firepower ホットフィックス リリース ノート を参照してください。

（注）　FMC Web インターフェイスは、現在のソフトウェアバージョンとは異なる（通常はそれ以降の）バージョンでこれらのホットフィックスを表示する場合があります。これは予想される動作であり、このホットフィックスは適用しても安全です。

BIOS およびファームウェアバージョンの確認

FMC での現在のバージョンを確認するには、Linux シェル/エキスパートモードで次のコマンドを実行します。

- BIOS: **sudo dmidecode -t bios -q**
- RAID コントローラファームウェア（FMC 4500）：**sudo MegaCLI -AdpAllInfo -aALL | grep "FW Package"**
- RAID コントローラファームウェア（他のすべてのモデル）：**sudo storcli /c0 show | grep "FW Package"**

FMCv

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。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。

バージョン 7.0 以降の FMCv は FXOS オペレーティングシステムを使用します。FMCv ソフトウェアをアップグレードすると、FXOS が自動的にアップグレードされます。バンドルされている FXOS バージョンについては、「バンドルされたコンポーネント （13 ページ）」を参照してください。

Management Center Virtual：パブリッククラウド

表 *4 : Management Center Virtual 300* の互換性：パブリッククラウド

Management Center 300	Amazon Web Services（AWS）	Microsoft Azure（Azure）	Oracle Cloud Infrastrucure（OCI）
7.6	**YES**	**YES**	**YES**
7.4	**YES**	**YES** 7.4.2 以降が必要	**YES**
7.3	**YES**	—	**YES**
7.2	**YES**	—	**YES**
7.1	**YES**	—	**YES**

表 *5 : Management Center Virtual 2、10、25* の互換性：パブリッククラウド

Management Center 2、10、25	Amazon Web Services（AWS）	Microsoft Azure（Azure）	Google Cloud Platform（GCP）	Oracle Cloud Infrastrucure（OCI）
7.6	**YES**	**YES**	**YES**	**YES**
7.4	**YES**	**YES**	**YES**	**YES**
7.3	**YES**	**YES**	**YES**	**YES**
7.2	**YES**	**YES**	**YES**	**YES**
7.1	**YES**	**YES**	**YES**	**YES**
7.0	**YES**	**YES**	**YES**	**YES**
6.7	**YES**	**YES**	**YES**	**YES**
6.6	**YES**	**YES**	—	—
6.5	**YES**	**YES**	—	—
6.4	**YES**	**YES**	—	—
6.3	**YES**	—	—	—
6.2.3	**YES**	—	—	—
6.2.2	**YES**	—	—	—
6.2.1	**YES**	—	—	—
6.2.0	**YES**	—	—	—

Management Center 2、10、25	Amazon Web Services（AWS）	Microsoft Azure（Azure）	Google Cloud Platform（GCP）	Oracle Cloud Infrastrucure（OCI）
6.1	**YES**	—	—	—
6.0.1	**YES**	—	—	—

Management Center Virtual：オンプレミス/プライベートクラウド

表 *6 : Management Center Virtual 300* の互換性：オンプレミス/プライベートクラウド

Management Center 300	VMware vSphere/VMware ESXi	カーネルベース仮想マシン（KVM）
7.6	**YES** VMware 6.5、6.7、7.0、8.0	**YES**
7.4	**YES** VMware 6.5、6.7、7.0	**YES**
7.3	**YES** VMware 6.5、6.7、7.0	**YES**
7.2	**YES** VMware 6.5、6.7、7.0	—
7.1	**YES** VMware 6.5、6.7、7.0	—
7.0	**YES** VMware 6.5、6.7、7.0	—
6.7	**YES** VMware 6.0、6.5、6.7	—
6.6	**YES** VMware 6.0、6.5、6.7	—
6.5	**YES** VMware 6.0、6.5、6.7	—

表 *7 : Management Center Virtual 2*、*10*、*25* の互換性：オンプレミス/プライベートクラウド

Management Center 2、10、25	VMware vSphere/VMware ESXi	Cisco HyperFlex（HyperFlex）	Microsoft Hyper-V（Hyper-V）	カーネルベース仮想マシン（KVM）	Nutanix エンタープライズクラウド（Nutanix）	Openstack
7.6	**YES** VMware 6.5、6.7、7.0、8.0	**YES**	**YES**	**YES**	**YES**	**YES**
7.4	**YES** VMware 6.5、6.7、7.0	**YES**	**YES**	**YES**	**YES**	**YES**
7.3	**YES** VMware 6.5、6.7、7.0	**YES**	—	**YES**	**YES**	**YES**
7.2	**YES** VMware 6.5、6.7、7.0	**YES**	—	**YES**	**YES**	**YES**
7.1	**YES** VMware 6.5、6.7、7.0	**YES**	—	**YES**	**YES**	**YES**
7.0	**YES** VMware 6.5、6.7、7.0	**YES**	—	**YES**	**YES**	**YES**
6.7	**YES** VMware 6.0、6.5、6.7	—	—	**YES**	—	—
6.6	**YES** VMware 6.0、6.5、6.7	—	—	**YES**	—	—

Management Center 2、10、25	VMware vSphere/VMware ESXi	Cisco HyperFlex（HyperFlex）	Microsoft Hyper-V（Hyper-V）	カーネルベース仮想マシン（KVM）	Nutanix エンタープライズクラウド（Nutanix）	Openstack
6.5	**YES** VMware 6.0、6.5、6.7	—	—	**YES**	—	—
6.4	**YES** VMware 6.0、6.5	—	—	**YES**	—	—
6.3	**YES** VMware 6.0、6.5	—	—	**YES**	—	—
6.2.3	**YES** VMware 5.5、6.0、6.5	—	—	**YES**	—	—
6.2.2	**YES** VMware 5.5、6.0	—	—	**YES**	—	—
6.2.1	**YES** VMware 5.5、6.0	—	—	**YES**	—	—
6.2.0	**YES** VMware 5.5、6.0	—	—	**YES**	—	—
6.1	**YES** VMware 5.5、6.0	—	—	**YES**	—	—
6.0.1	**YES** VMware 5.1、5.5	—	—	—	—	—
6.0.0	**YES** VMware 5.1、5.5	—	—	—	—	—

Management Center 2、10、25	VMware vSphere/VMware ESXi	Cisco HyperFlex（HyperFlex）	Microsoft Hyper-V（Hyper-V）	カーネルベース仮想マシン（KVM）	Nutanix エンタープライズクラウド（Nutanix）	Openstack
5.4 *	**YES** VMware 5.0、5.1、5.5	—	—	—	—	—

* 5.4.x デバイスを管理するには 5.4.1.x の Defense Center を使用します。

Management Center の高可用性

クラウド提供型 Firewall Management Center

クラウド提供型 Firewall Management Center は、高可用性をサポートしていません。

Management Center ハードウェア

現在サポートされているすべてのハードウェア管理センターは、高可用性をサポートしています。

仮想 Management Center

表 *8 : Management Center Virtual*：高可用性サポート

プラットフォーム	ハイ アベイラビリティ
パブリック クラウド	
Amazon Web Services（AWS）	7.1+
Google Cloud Platform（GCP）	—
Microsoft Azure	7.4.2+
Oracle Cloud Infrastrucure（OCI）	7.1+
オンプレミス/プライベートクラウド	
Cisco HyperFlex	7.0+
カーネルベース仮想マシン（KVM）	7.3+
Microsoft Hyper-V	7.4+
Nutanix エンタープライズクラウド	—
OpenStack	—

プラットフォーム	ハイ アベイラビリティ
VMware vSphere/VMware ESXi	6.7+

デバイス管理

オンプレミス Management Center

すべてのデバイスは、お客様が導入した（オンプレミス）FMC によるリモート管理に対応していますが、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。また、特定の FMC 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。リリース固有の要件については、リリースノートを参照してください。

表 *9*: オンプレミス *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
7.6	7.1
7.4 NGIPS デバイス管理の最後のサポート。	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

FMC バージョン	管理可能な最も古いデバイスバージョン
6.4	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 Firewall Management Center

クラウド提供型 Firewall Management Center は、**バージョン7.0.3 ～ 7.6.0（バージョン 7.1 を除く）**を実行している FTD デバイスを管理できます。

クラウド管理型デバイスは、イベントのロギングと分析の目的でのみバージョン 7.2 以降のオンプレミスFMCと共同管理できます。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。

Analytics Management Center によるデバイスの共同管理

クラウド提供型 Firewall Management Center はオンプレミス Management Center よりも広範な管理対象デバイスのバージョンをサポートしているため、分析にオンプレミス Management Center を使用する場合に問題が発生することがあります。これは、共同管理するにはデバイスが「古すぎたり」、「新しすぎたり」する可能性があるためです。

次の処理が妨げられる可能性があります。

- Management Center のアップグレードが古いデバイスによってブロックされているため、新しいデバイスが Analytics Management Center に登録される。
- Analytics Management Center が古いリリースで「スタック」しているため、共同管理デバイスを最新リリースにアップグレードされる。

- デバイスのアップグレードを元に戻した場合に、デバイスの Analytics Management Center との互換性が失われる。

例として、現在共同管理バージョン7.0.xのデバイスが含まれている展開に、共同管理バージョン7.6.0のデバイスを追加するシナリオについて考えます。クラウド提供型Firewall Management Center は該当範囲のデバイスをすべて管理できますが、オンプレミス Analytics Management Center は管理できません。

優先順位に従って、次のことができます。

- バージョン 7.0.x のデバイスをバージョン 7.2.0 以降にアップグレードし、Analytics Management Center をバージョン 7.6.0 にアップグレードしてから、バージョン 7.6.0 のデバイスを両方の Management Center に追加します。
- Analytics Management Center からバージョン 7.0.x のデバイスを削除し、Analytics Management Center をバージョン 7.6.0 にアップグレードしてから、バージョン 7.6.0 のデバイスを両方の Management Center に追加します。
- Analytics Management Center はそのままにして、バージョン 7.6.0 のデバイスは追加しないでください。

次の選択肢があります。

- すべてのデバイスからイベントを取得するには、Analytics Management Center と古いデバイスをアップグレード（または交換）します。
- 古いデバイスからのイベントを除外するには、Analytics Management Center のみをアップグレード（または交換）します。
- 新しいデバイスからのイベントを除外するには、Analytics Management Center を古いリリースのままにします。

バンドルされたコンポーネント

一部のリリースの更新されたビルドをリリースする場合があることに注意してください。バンドルされたコンポーネントがビルドごとに変わる場合は、最新のビルドのコンポーネントを一覧表示します。（ほとんどの場合、最新のビルドのみをダウンロードできます。）新しいビルドとそれらが解決する問題の詳細については、ご使用のバージョンのリリースノートを参照してください。

システムデータベース

の脆弱性データベース（VDB）は、ホストが影響を受ける可能性がある既知の脆弱性、およびオペレーティングシステム、クライアント、アプリケーションのフィンガープリントを格納するデータベースです。システムでは、VDB を使用して、特定のホストで感染のリスクが高まるかどうかを判断します。

地理位置情報データベース（GeoDB）は、地理的な位置に基づいてトラフィックを表示およびフィルタリングするために利用できるデータベースです。

表 *10*：

	VDB	GeoDB
7.4.1 ～ 7.4.x	4.5.0-376	2022-07-04-101
7.4.0	4.5.0-365	2022-07-04-101
7.3.0 ～ 7.3.x	4.5.0-358	2022-07-04-101
7.2.0 ～ 7.2.x	4.5.0-353	2022-05-11-103
7.1.0	4.5.0-346	2020-04-28-002
6.7.0 ～ 7.0.x	4.5.0-338	2020-04-28-002
6.6.1 ～ 6.6.x	4.5.0-336	2019-06-03-002
6.6.0	4.5.0-328	2019-06-03-002
6.5.0	4.5.0-309	2019-06-03-002
6.4.0	4.5.0-309	2018-07-09-002
6.3.0	4.5.0-299	2018-07-09-002
6.2.3	4.5.0-290	2017-12-12-002
～ 6.2.2	4.5.0-271	2015-10-12-001

統合された製品

以下にリストされているシスコ製品には、他の互換性要件がある場合があります。たとえば、特定のハードウェアまたは特定のオペレーティングシステムで実行する必要がある場合があります。詳細については、該当する製品マニュアルを参照してください。

（注） 可能な限り、各統合製品の最新（最新）の互換性のあるバージョンを使用することをお勧めします。そうすることで、最新の機能、バグ修正、およびセキュリティパッチを確実に入手できます。

Identity Services およびユーザー制御

次の点に注意してください。

- Cisco ISE および ISE-PIC：他の組み合わせでも機能する可能性がありますが、拡張互換性テストを提供する ISE および ISE-PIC のバージョンをリストします。

- Cisco Firepower User Agent バージョン 6.6 は、ユーザー エージェント ソフトウェアをアイデンティティソースとしてサポートする最後の FMC リリースであり、バージョン 6.7 以降へのアップグレードはブロックされます。

  代わりに、 Microsoft Active Directory で パッシブ ID エージェント を使用できます。詳細については、「User Control With the パッシブ ID エージェント」[英語] を参照してください。

- Cisco TS エージェントのバージョン 1.0 および 1.1 は使用できなくなりました。

表 *11* : 統合型製品 : *Identity Services*/ユーザー制御

Management Center/Threat Defense	Cisco Identity Services Engine（ISE）		Cisco Firepower User Agent	シスコターミナルサービス（TS）エージェント
	ISE	ISE-PIC		
次でサポートされています...	Management center デバイス マネージャ	Management center デバイス マネージャ	Management center のみ	Management center のみ
クラウド提供型の管理センター（バージョンなし）	3.3 3.2 3.1 パッチ 2 以降 3.0 + パッチ 6 以降 2.7 パッチ 2 以降	3.2 3.1 2.7 パッチ 2 以降	—	1.4
7.4	3.3 3.2 3.1 パッチ 2 以降 3.0 + パッチ 6 以降	3.2 3.1	—	1.4
7.3	3.2 3.1 3.0 2.7 パッチ 2 以降	3.2 3.1 2.7 パッチ 2 以降	—	1.4 1.3
7.2.4 ～ 7.2.x	3.3 3.2 3.1 3.0 2.7 パッチ 2 以降	3.2 3.1 2.7 パッチ 2 以降	—	1.4 1.3

Management Center/Threat Defense	Cisco Identity Services Engine（ISE）		Cisco Firepower User Agent	シスコターミナルサービス（TS）エージェント
	ISE	ISE-PIC		
7.2.0 ～ 7.2.3	3.2 3.1 3.0 2.7 パッチ 2 以降	3.2 3.1 2.7 パッチ 2 以降	—	1.4 1.3
7.1	3.2 3.1 3.0 2.7 パッチ 2 以降	3.2 3.1 2.7 パッチ 2 以降	—	1.4 1.3
7.0	3.2 3.1 3.0 2.7 パッチ 2 以降 2.6 パッチ 6 以降	3.2 3.1 2.7 パッチ 2 以降 2.6 パッチ 6 以降	—	1.4 1.3
6.7	3.0 2.7 パッチ 2 以降 2.6 パッチ 6 以降	2.7 パッチ 2 以降 2.6 パッチ 6 以降	—	1.4 1.3
6.6	3.0 2.7、任意のパッチ 2.6、任意のパッチ 2.4	2.7、任意のパッチ 2.6、任意のパッチ 2.4	2.5 2.4	1.4 1.3 1.2
6.5	2.6 2.4	2.6 2.4	2.5 2.4	1.4 1.3 1.2 1.1
6.4	2.4 2.3 パッチ 2 2.3	2.4 2.2 パッチ 1	2.5 2.4 2.3。ASA FirePOWER 以外	1.4 1.3 1.2 1.1

Management Center/Threat Defense	Cisco Identity Services Engine（ISE）		Cisco Firepower User Agent	シスコターミナルサービス（TS）エージェント
	ISE	ISE-PIC		
6.3	2.4 2.3 パッチ 2 2.3	2.4 2.2 パッチ 1 2.4	2.4 2.3。ASA FirePOWER 以外	1.2 1.1
6.2.3	2.3 パッチ 2 2.3 2.2 パッチ 5 2.2 パッチ 1 2.2	2.2 パッチ 1	2.4 2.3	1.2 1.1
6.2.2	2.3 2.2 パッチ 1 2.2 2.1	2.2 パッチ 1	2.3	1.2 1.1 1.0
6.2.1	2.1 2.0.1 2.0	2.2 パッチ 1	2.3	1.1 1.0
6.2.0	2.1 2.0.1 2.0 1.3	—	2.3	—
6.1	2.1 2.0.1 2.0 1.3	—	2.3	—
6.0.1	1.3	—	2.3	—
5.x	—	—	2.2	—

Cisco Secure 動的属性コネクタ

Cisco Secure 動的属性コネクタ は、クラウドまたは仮想ワークロードの変更に基づいてFMCのファイアウォールポリシーを迅速かつシームレスに更新する軽量アプリケーションです。詳細については、次のいずれかを参照してください。

- オンプレミスコネクタ：Cisco Secure 動的属性コネクタ コンフィギュレーション ガイド [英語]
- クラウド提供型コネクタ：*Managing the Cisco Secure Dynamic Attributes Connector with Cisco Defense Orchestrator*」の章

表 *12*：統合型製品：*Cisco Secure* 動的属性コネクタ

Management Center	Cisco Secure 動的属性コネクタ	
	オンプレミス	Cloud-delivered (with CDO)
クラウド提供型の管理センター（バージョンなし）	3.0 2.2 2.0	**YES**
7.1+	3.0 2.2 2.0 1.1	**YES**
7.0	3.0 2.2 2.0 1.1	—

Cisco Secure 動的属性コネクタ では、さまざまなクラウドサービスプラットフォームのサービスタグとカテゴリをセキュリティルールで使用できます。

次の表に、Firepower Management Center で提供される Cisco Secure 動的属性コネクタ（CSDAC）でサポートされるコネクタを示します。オンプレミス CSDAC でサポートされるコネクタのリストについては、Cisco Secure 動的属性コネクタ コンフィギュレーション ガイドを参照してください。

表 *13*：*Cisco Secure* 動的属性コネクタ バージョンおよびプラットフォーム でサポートされているコネクタのリスト

CSDAC バージョン/プラットフォーム	AWS	AWS セキュリティグループ	AWS サービスタグ	Azure	Azure サービスタグ	Cisco Cyber Vision	Cisco Multicloud Defense	汎用テキスト	GitHub	Google クラウド	Microsoft Office 365	vCenter	Webex	Zoom
バージョン1.1（オンプレミス）	対応	非対応	非対応	対応	対応	非対応	非対応	非対応	非対応	非対応	対応	対応	非対応	非対応
バージョン2.0（オンプレミス）	対応	非対応	非対応	対応	対応	非対応	非対応	非対応	非対応	対応	対応	対応	非対応	非対応

CSDAC バージョン/プラットフォーム	AWS	AWS セキュリティグループ	AWS サービスタグ	Azure	Azure サービスタグ	Cisco Cyber Vision	Cisco Multicloud Defense	汎用テキスト	GitHub	Google クラウド	Microsoft Office 365	vCenter	Webex	Zoom
バージョン 2.2（オンプレミス）	対応	非対応	非対応	対応	対応	非対応	非対応	非対応	対応	対応	対応	対応	非対応	非対応
バージョン 2.3（オンプレミス）	対応	非対応	非対応	対応	対応	非対応	非対応	非対応	対応	対応	対応	対応	対応	対応
バージョン 3.0（オンプレミス）	対応	対応	対応	対応	対応	対応	非対応	対応	対応	対応	対応	対応	対応	対応

脅威の検出

次の点に注意してください。

- シスコのセキュリティ分析とロギング（オンプレミス）には、Stealthwatch 管理コンソール（SMC）用のセキュリティ分析とロギングオンプレミスアプリが必要です。SMC の Stealthwatch Enterprise（SWE）要件については、オンプレミスにおけるシスコのセキュリティ分析とロギング：Firepower Event Integration Guide [英語] を参照してください。
- バージョン 6.4 ～ 7.4 で使用可能だったCisco SecureX 統合のサポートが終了しました。代替テクノロジーについては、シスコの担当者またはパートナーにお問い合わせください。

表 *14*：統合製品：脅威の検出

Management Center/Threat Defense	Cisco Security Analytics and Logging (SaaS)	シスコのセキュリティ分析とロギング（オンプレミス）	Cisco Secure Malware Analytics	Cisco Security Packet Analyzer
次でサポートされています...	Management center デバイス マネージャ	Management center のみ	Management center のみ	Management center のみ
6.5 以降	**YES**	**YES**	**YES**	—
6.4	**YES**	**YES**	**YES**	**YES**
6.3	—	—	**YES**	**YES**
6.1 ～ 6.2.3	—	—	**YES**	—

FTD リモート アクセス VPN

リモートアクセス仮想プライベートネットワーク（RA VPN）を使用すると、個々のユーザーは、コンピュータまたはサポートされているモバイルデバイスを使用して、リモートの場所か

らネットワークに接続できます。新しい Threat Defense 機能では、新しいバージョンのクライアントが必要になる場合があることに注意してください。

詳細については、Cisco Secure クライアント/AnyConnect セキュア モビリティ クライアント コンフィギュレーション ガイドを参照してください。

表 *15*：統合型製品：*FTD RA VPN*

FTD	Cisco Secure クライアント/Cisco AnyConnect セキュア モビリティ クライアント
6.2.2 以降	4.0 以降

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。

表 *16*：ブラウザ

ブラウザ	
Google Chrome	任意（Any）
Mozilla Firefox	任意（Any）
Microsoft Edge（Windows のみ）	バージョン 6.7 以降
Apple Safari	広範囲にわたるテストは行われていません。フィードバックをお待ちしています。

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、またはフィードバックがある場合は、Cisco TAC にご連絡ください。

ブラウザの設定と拡張

ブラウザに関係なく、javascript と cookie を有効にします。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

表 *17*：画面解像度

インターフェイス	最小解像度
Firepower 4100/9300 のシャーシマネージャ	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。

（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。

（注） バージョン 6.2.3 以前の場合、TLS v1.3 をサポートする Web サイトでは常にロードが失敗します。回避策として、ClientHello ネゴシエーションから拡張 43（TLS 1.3）を削除するように管理対象 デバイスを設定できます。「*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。バージョン 6.2.3.7 以降では、ダウングレードするタイミングを指定できます。Cisco TAC にご相談のうえ、Cisco Secure Firewall Threat Defense コマンドリファレンス の **system support** コマンドを参照してください。

サポート終了の通知

次の表に、サポート終了の詳細を示します。過去の日付は太字で示されています。

Snort

Threat Defense でまだ Snort 2 検査エンジンを使用している場合は、検出とパフォーマンスを向上させるために、今すぐ Snort 3 に切り替えてください。Threat Defense バージョン 6.7 以降（デバイスマネージャを使用）およびバージョン 7.0 以降（Management Center を使用）で使用できます。Snort 2 は、今後のリリースで廃止されます。最終的には、Snort 2 デバイスはアップグレードできなくなります。

Management Center の展開では、Threat Defense バージョン 7.2 以降にアップグレードすると、対象の Snort 2 デバイスも Snort 3 にアップグレードされます。カスタム侵入またはネットワーク分析ポリシーを使用しているために不適格なデバイスの場合、手動で Snort をアップグレードします。Firepower Management Center Snort 3 Configuration Guideで、「*Migrate from Snort 2 to Snort 3*」を参照してください。

デバイスマネージャの展開では、Snort を手動でアップグレードします。Cisco Firepower Threat Defense Configuration Guide for Firepower Device Managerの「*Intrusion Policies*」を参照してください。

ソフトウェア

これらの主要なソフトウェアバージョンは、販売終了またはサポート終了になりました。サポートが終了したバージョンは、シスコ サポートおよびダウンロード サイトから削除されます。

表 *18*：ソフトウェアサポート終了の通知

バージョン	販売終了	更新終了	サポート終了	通知
7.1	**2023 年 12 月 22 日**	2024 年 12 月 21 日	2025 年 12 月 31 日	Cisco Firepower Threat Defense（FTD）7.1.(x)、Firepower Management Center（FMC）7.1.(x)、Adaptive Security Appliance（ASA）9.17.(x)、および Firepower eXtensible Operating System（FXOS）2.11.(x) の販売終了およびサポート終了の通知
6.7	**2021 年 7 月 9 日**	**2022 年 7 月 9 日**	**2024 年 7 月 31 日**	Cisco Firepower Threat Defense（FTD）6.7、Firepower Management Center（FMC）6.7、および Firepower eXtensible Operating System（FXOS）2.9(x) の販売終了およびサポート終了の通知
6.6	**2022 年 3 月 2 日**	**2023 年 3 月 2 日**	2025 年 3 月 31 日	Cisco Firepower Threat Defense（FTD/FTDv）6.6(x)、Firepower Management Center（FMC/FTDv）6.6(x)、および Firepower eXtensible Operating System（FXOS）2.8(x) の販売終了およびサポート終了の通知

バージョン	販売終了	更新終了	サポート終了	通知
6.5	**2020 年 6 月 22 日**	**2021 年 6 月 22 日**	**2023 年 6 月 30 日**	Cisco Firepower Threat Defense（FTD）6.5(x)、Firepower Management Center（FMC）6.5(x)、および Firepower eXtensible Operating System（FXOS）2.7(x) の販売終了およびサポート終了の通知
6.4	**2023 年 2 月 27 日**	**2024 年 2 月 27 日**	2026 年 2 月 28 日	Cisco Firepower Threat Defense（FTD）6.4(X)、Firepower Management Center（FMC）6.4(X)、および Firepower eXtensible Operating System（FXOS）2.6(x) の販売終了およびサポート終了の通知
6.3	**2020 年 4 月 30 日**	**2021 年 4 月 30 日**	**2023 年 4 月 30 日**	Cisco Firepower Threat Defense（FTD）6.2.2、6.3(x)、Firepower eXtensible Operating System（FXOS）2.4.1、および Firepower Management Center（FMC）6.2.2 と 6.3(x) の販売終了およびサポート終了の通知
6.2.3	**2022 年 2 月 4 日**	**2023 年 2 月 4 日**	2025 年 2 月 28 日	Cisco Firepower Threat Defense（FTD）6.2.3、Firepower Management Center（FMC）6.2.3、および Firepower eXtensible Operating System（FXOS）2.2(x) の販売終了およびサポート終了の通知
6.2.2	**2020 年 4 月 30 日**	**2021 年 4 月 30 日**	**2023 年 4 月 30 日**	Cisco Firepower Threat Defense（FTD）6.2.2、6.3(x)、Firepower eXtensible Operating System（FXOS）2.4.1、および Firepower Management Center（FMC）6.2.2 と 6.3(x) の販売終了およびサポート終了の通知
6.2.1	**2019 年 3 月 5 日**	**2020 年 3 月 4 日**	**2022 年 3 月 31 日**	Cisco Firepower Threat Defense バージョン 6.2.0 および6.2.1 の販売終了およびサポート終了の通知
6.2	**2019 年 3 月 5 日**	**2020 年 3 月 4 日**	**2022 年 3 月 31 日**	Cisco Firepower Threat Defense バージョン 6.2.0 および6.2.1 の販売終了およびサポート終了の通知
6.1	**2019 年 11 月 22 日**	**2021 年 5 月 22 日**	**2023 年 5 月 31 日**	Cisco Firepower Threat Defense バージョン 6.1、NGIPSv および NGFWv バージョン 6.1、Firepower Management Center 6.1、および Firepower eXtensible Operating System（FXOS）2.0(x) の販売終了およびサポート終了の通知

バージョン	販売終了	更新終了	サポート終了	通知
6.0.1	**2017 年 11 月 10 日**	**2018 年 11 月 10 日**	**2020 年 11 月 30 日**	Cisco Firepower ソフトウェアリリース 5.4、6.0、6.0.1 および Firepower Management Center ソフトウェアリリース 5.4、6.0、6.0.1 の販売終了およびサポート終了の通知
6.0.0	**2017 年 11 月 10 日**	**2018 年 11 月 10 日**	**2020 年 11 月 30 日**	Cisco Firepower ソフトウェアリリース 5.4、6.0、6.0.1 および Firepower Management Center ソフトウェアリリース 5.4、6.0、6.0.1 の販売終了およびサポート終了の通知
5.4	**2017 年 11 月 10 日**	**2018 年 11 月 10 日**	**2020 年 11 月 30 日**	Cisco Firepower ソフトウェアリリース 5.4、6.0、6.0.1 および Firepower Management Center ソフトウェアリリース 5.4、6.0、6.0.1 の販売終了およびサポート終了の通知
5.3	**2016 年 1 月 29 日**	**2016 年 7 月 30 日**	**2018 年 7 月 31 日**	Cisco FirePOWER ソフトウェア v5.3 と v5.3.1 および FireSIGHT Management Center ソフトウェア v5.3 と v5.3.1 の販売終了およびサポート終了の通知

まだサポートされているブランチのこれらのソフトウェアバージョンは シスコ サポートおよびダウンロード サイトから削除されました。

（注） バージョン 6.2.3 以降では、パッチ（4 桁番号のリリース）をアンインストールすると、アップグレード前のバージョンがアプライアンスで実行されます。つまり、単純に新しいパッチをアンインストールすると、廃止されたバージョンを実行することになります。特に明記されていない限り、廃止されたバージョンのままにしないでください。代わりに、アップグレードすることを推奨します。アップグレードできない場合は、廃止されたパッチをアンインストールします。

表 *19*：ソフトウェアで削除されたバージョン

バージョン	削除日	関連バグと追加情報
7.2.6	**2024-04-29**	CSCwi63113：リロード/アップグレード後に SNMP が有効になっている FTD ブートループ
6.4.0.6	**2019 年 12 月 19 日**	CSCvr52109：複数デバイスへの展開後、FTD が正しいアクセスコントロールルールに一致しないことがある
6.2.3.8	**2019 年 1 月 7 日**	CSCvn82378：FMC を 6.2.3.8 ～ 51 にアップグレードすると、ASA/FTD を経由するトラフィックの送受信が停止することがある

バージョン	削除日	関連バグと追加情報
5.4.0.1	**2015**	—
5.3.1.2	**2015**	—

ハードウェアおよび仮想プラットフォーム

これらのプラットフォームは、販売終了またはサポート終了になりました。

用語とブランディング

表 *20 :* 製品ライン

現在の名前	以前の名前
Cisco Secure Firewall Threat Defense	Firepower Firepower システム FireSIGHT システム Sourcefire 3D System

表 *21 :* デバイス

現在の名前		以前の名前
脅威防御	Cisco Secure Firewall Threat Defense	Firepower Threat Defense（FTD）
	Cisco Secure Firewall Threat Defense Virtual	Firepower Threat Defense Virtual（FTDv）
従来型 NGIPS	ASA FirePOWER ASA FirePOWER モジュール ASA with FirePOWER サービス	—
	7000/8000 シリーズ	シリーズ 3
	NGIPSv	仮想管理対象デバイス
レガシー（Legacy）	シリーズ 2	—
	Blue Coat X-Series 向け Cisco NGIPS	X シリーズの FireSIGHT ソフトウェア X シリーズの Sourcefire ソフトウェア

表 *22*：デバイス管理

現在の名前	以前の名前
Cisco Secure Firewall Management Center	Firepower Management Center（FMC） FireSight Management Center FireSIGHT Defense Center Defense Center
Cisco Secure Firewall Management Center Virtual	Firepower Management Center Virtual（FMCv） FireSIGHT Virtual Management Center FireSIGHT Virtual Defense Center 仮想防御センター
クラウド提供型 Firewall Management Center	—
Cisco Secure Firewall Device Manager	Firepower Device Manager（FDM）
Cisco Secure Firewall Adaptive Security Device Manager (ASDM)	Adaptive Security Device Manager（ASDM）
Cisco Secure Firewall Chassis Manager	Firepower Chassis Manager
Cisco Defense Orchestrator（CDO）	—

表 *23*：オペレーティング システム

現在の名前	以前の名前
Cisco Secure Firewall Extensible Operating System（FXOS）	Firepower Extensible Operating System（FXOS)
Cisco Secure Firewall Adaptive Security Appliance (ASA) Software	Adaptive Security Appliance (ASA) software

【注意】シスコ製品をご使用になる前に、安全上の注意（ **www.cisco.com/jp/go/safety_warning/** ）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2022–2024 Cisco Systems, Inc. All rights reserved.

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。