Cisco Secure Firewall Threat Defense 互換性ガイド

最終更新：2024 年 8 月 21 日

Cisco Secure Firewall Threat Defense 互換性ガイド

このガイドでは、Cisco Secure Firewall Threat Defense のソフトウェアとハードウェアの互換性について説明します。関連する互換性ガイドについては、次の表を参照してください。

（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 （36 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。	Cisco Secure Firewall Management Center 互換性ガイド Cisco Firepower 4100/9300 FXOS の互換性
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 Secure Firewall Threat Defense リリースノート Cisco Firepower 4100/9300 FXOS リリースノート

説明	リソース
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） Cisco Secure Firewall デバイスマネージャの新機能（リリース別）
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 Cisco FXOS ドキュメント一覧

推奨リリース：バージョン 7.2.5.x

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。

Threat Defense Platform サマリー

以下の表に、Threat Defense でサポートされているデバイスとオンプレミス（お客様による導入）の管理方法を示します。

（注） クラウド管理型の展開では、クラウド提供型 Firewall Management Center は、バージョン 7.0.3 ～ 7.4.1（バージョン 7.1 を除く）を実行している Threat Defense デバイスを管理できます。デバイスマネージャに CDO 管理を追加するには、Threat Defense バージョン 6.4 以上を実行している必要があります。新しい管理センターでのクラウド管理や古いデバイスの管理など、デバイス管理の詳細については、Threat Defense 管理 （15 ページ）を参照してください。

Threat Defense のハードウェア

表 *2 : Cisco Secure Firewall Threat Defense* マネージャとバージョン別のハードウェア

デバイスのプラットフォーム	デバイスのバージョン：オンプレミス **Management Center** を使用	デバイスのバージョン：**Device Manager** を使用
Firepower 1010、1120、1140	6.4 以降	6.4 以降
Firepower 1010E	7.2.3 以降 7.3 ではサポートなし	7.2.3 以降 7.3 ではサポートなし
Firepower 1150	6.5 以降	6.5 以降
Firepower 2110、2120、2130、2140	6.2.1 以降	6.2.1 以降
Cisco Secure Firewall 3105	7.3.1 以降	7.3.1 以降
Secure Firewall 3110、3120、3130、3140	7.1+	7.1+
Firepower 4110、4120、4140	6.0.1 ～ 7.2	6.5 ～ 7.2
Firepower 4150	6.1 ～ 7.2	6.5 ～ 7.2
Firepower 4115、4125、4145	6.4 以降	6.5 以降
Firepower 4112	6.6 以降	6.6 以降
Cisco Secure Firewall 4215、4225、4245	7.4.0+	—
Firepower 9300：SM-24、SM-36、SM-44	6.0.1 ～ 7.2	6.5 ～ 7.2
Firepower 9300：SM-40、SM-48、SM-56	6.4 以降	6.5 以降
ISA 3000	6.2.3 以降	6.2.3 以降
ASA 5506-X、5506H-X、5506W-X	6.0.1 ～ 6.2.3	6.1 ～ 6.2.3
ASA 5508-X、5516-X	6.0.1 ～ 7.0	6.1 ～ 7.0
ASA 5512-X	6.0.1 ～ 6.2.3	6.1 ～ 6.2.3
ASA 5515-X	6.0.1 ～ 6.4	6.1 ～ 6.4
ASA 5525-X、5545-X、5555-X	6.0.1 ～ 6.6	6.1 ～ 6.6

Threat Defense Virtual

表 *3 : Threat Defense Virtual* マネージャとバージョン別

デバイスのプラットフォーム	デバイスのバージョン：オンプレミス **Management Center** を使用	デバイスのバージョン：**Device Manager** を使用
パブリック クラウド		
AWS	6.0.1 以降	6.6 以降
Azure	6.2 以降	6.5 以降
GCP	6.7 以降	7.2 以降
OCI	6.7 以降	—
オンプレミス/プライベートクラウド		
[HyperFlex]	7.0 以上	7.0 以上
KVM	6.1 以降	6.2.3 以降
Nutanix	7.0 以上	7.0 以上
OpenStack	7.0 以上	—
VMware 7.0	7.0 以上	7.0 以上
VMware 6.7	6.5 以降	6.5 以降
VMware 6.5	6.2.3 以降	6.2.3 以降
VMware 6.0	6.0 ～ 6.7	6.2.2 ～ 6.7
VMware 5.5	6.0.1 ～ 6.2.3	6.2.2 ～ 6.2.3
VMware 5.1	6.0.1 のみ	—

脅威防御ハードウェア

Firepower 1000/2100 シリーズ

Firepower 1000/2100 シリーズデバイスは、FXOS オペレーティングシステムを使用します。脅威防御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 （17 ページ）」を参照してください。これらのデバイスは、脅威防御の代わりに ASA も実行できます。『Cisco Secure Firewall ASA の互換性』を参照してください。

表 *4 : Firepower 1000/2100* シリーズとの互換性

Threat Defense	Firepower 1150	Firepower 1010E	Firepower 1010 Firepower 1120 Firepower 1140	Firepower 2110 Firepower 2120 Firepower 2130 Firepower 2140
7.4.1 ～ 7.4.x	**YES**	**YES**	**YES**	**YES**
7.4.0	—	—	—	—
7.3	**YES**	—	**YES**	**YES**
7.2	**YES**	**YES** 7.2.3 以降が必要	**YES**	**YES**
7.1	**YES**	—	**YES**	**YES**
7.0	**YES**	—	**YES**	**YES**
6.7	**YES**	—	**YES**	**YES**
6.6	**YES**	—	**YES**	**YES**
6.5	**YES**	—	**YES**	**YES**
6.4	—	—	**YES**	**YES**
6.3	—	—	—	**YES**
6.2.3	—	—	—	**YES**
6.2.2	—	—	—	**YES**
6.2.1	—	—	—	**YES**

Secure Firewall 3100/4200 シリーズ

Secure Firewall 3100/4200 シリーズ デバイスは、FXOS オペレーティングシステムを使用します。FXOS のアップグレード方法は、デバイスがアプリケーションモードかマルチインスタンスモードかによって異なります。これらのデバイスは、脅威防御の代わりに ASA も実行できます。『Cisco Secure Firewall ASA の互換性』を参照してください。

アプリケーションモードの Cisco Secure Firewall シリーズ 3100/4200

アプリケーションモードでは、Threat Defense 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 （17 ページ）」を参照してください。

表 *5 : Cisco Secure Firewall 3100/4200* シリーズのアプリケーションモードの互換性

脅威防御	**Cisco Secure Firewall 4215** **Cisco Secure Firewall 4225** **Cisco Secure Firewall 4245**	**Cisco Secure Firewall 3105**	**Secure Firewall 3110** **Secure Firewall 3120** **Secure Firewall 3130** **Secure Firewall 3140**
7.4.1 ～ 7.4.x	**YES**	**YES**	**YES**
7.4.0	**YES**	—	—
7.3	—	**YES**	**YES**
7.2	—	—	**YES**
7.1	—	—	**YES**

マルチインスタンスモードの Cisco Secure Firewall 3100 シリーズ

マルチインスタンスモードでは、シャーシ（FXOS およびファームウェア）と脅威防御を個別にアップグレードします。ただし、両方のコンポーネントが 1 つのパッケージに含まれています。シャーシのみのアップグレードまたは Threat Defense のみのアップグレードを実行できます。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 （17 ページ）」を参照してください。

新しいFXOS で古い脅威防御インスタンスを実行できますが、多くの場合、新機能と解決済みの問題への対応にはフルアップグレードが必要です。

表 *6 : Cisco Secure Firewall 3100* シリーズのマルチインスタンスモードの互換性

脅威防御	**Secure Firewall 3110** **Secure Firewall 3120** **Secure Firewall 3130** **Secure Firewall 3140**
7.4.1 ～ 7.4.x	**YES**

Firepower 4100/9300

Firepower 4100/9300 の場合、リストに**太字**で示すように、Threat Defense のメジャーバージョンに特別に認定され**推奨される**付随の FXOS バージョンがあります。これらの組み合わせの拡張テストを実施するため、これらの組み合わせは可能な限り使用してください。問題を解決するには、FXOS を最新のビルドにアップグレードする必要がある場合があります。判断のヒントについては、Cisco Firepower 4100/9300 FXOS リリースノートを参照してください。

これらのデバイスは、Threat Defense の代わりに ASA を実行することもできます。ASA 9.12+ および Threat Defense 6.4.0+ では、同じ Firepower 9300 シャーシ内の別のモジュールで ASA と Threat Defense の両方を実行できます。詳細については、「Cisco Firepower 4100/9300 FXOS の互換性」を参照してください。

表 *7 : Firepower 4100/9300 FXOS* との互換性

脅威防御	FXOS	Firepower 9300		Firepower 4100 シリーズ			
		SM-24 SM-36 SM-44	SM-40 SM-48 SM-56	4110 4120 4140	4150	4112	4115 4125 4145
7.4.1	**2.14.1.131 以降**	—	**YES**	—	—	**YES**	**YES**
7.4.0	—	—	—	—	—	—	—
7.3	**2.13.0.198+** 2.14.1.131 以降	—	**YES**	—	—	**YES**	**YES**
7.2	**2.12.0.31+** 2.13.0.198+ 2.14.1.131 以降	**YES** no 2.13+	**YES**	**YES** no 2.13+	**YES** no 2.13+	**YES**	**YES**
7.1	**2.11.1.154+** 2.12.0.31+ 2.13.0.198+ 2.14.1.131 以降	**YES** no 2.13+	**YES**	**YES** no 2.13+	**YES** no 2.13+	**YES**	**YES**
7.0	**2.10.1.159+** 2.11.1.154+ 2.12.0.31+ 2.13.0.198+ 2.14.1.131 以降	**YES** no 2.13+	**YES**	**YES** no 2.13+	**YES** no 2.13+	**YES**	**YES**
6.7	**2.9.1.131+** 2.10.1.159+ 2.11.1.154+ 2.12.0.31+ 2.13.0.198+ 2.14.1.131 以降	**YES** no 2.13+	**YES**	**YES** no 2.13+	**YES** no 2.13+	**YES**	**YES**

脅威防御	FXOS	Firepower 9300		Firepower 4100 シリーズ			
		SM-24 SM-36 SM-44	SM-40 SM-48 SM-56	4110 4120 4140	4150	4112	4115 4125 4145
6.6	**2.8.1.105+** 2.9.1.131+ 2.10.1.159+ 2.11.1.154+ 2.12.0.31+ 2.13.0.198+ 2.14.1.131 以降	**YES** no 2.13+	**YES**	**YES** no 2.13+	**YES** no 2.13+	**YES**	**YES**
6.5	**2.7.1.92 +** 2.8.1.105+ 2.9.1.131+ 2.10.1.159+ 2.11.1.154+ 2.12.0.31+	**YES**	**YES**	**YES**	**YES**	—	**YES**
6.4	**2.6.1.157+** 2.7.1.92+ 2.8.1.105+ 2.9.1.131+ 2.10.1.159+ 2.11.1.154+ 2.12.0.31+	**YES**	**YES**	**YES**	**YES**	—	**YES**
6.3	**2.4.1.214+** 2.6.1.157+ 2.7.1.92+ 2.8.1.105+ 2.9.1.131+ 2.10.1.159+ 2.11.1.154+ 2.12.0.31+	**YES**	—	**YES**	**YES**	—	—

脅威防御	FXOS	Firepower 9300		Firepower 4100 シリーズ			
		SM-24 SM-36 SM-44	SM-40 SM-48 SM-56	4110 4120 4140	4150	4112	4115 4125 4145
6.2.3	**2.3.1.73+** 2.4.1.214+ 2.6.1.157+ 2.7.1.92+ 2.8.1.105+ （注） Firepower 6.2.3.16+ には FXOS 2.3.1.157+ が必要です。	**YES**	—	**YES**	**YES**	—	—
6.2.2	**2.2.2.x** 2.3.1.73+ 2.4.1.214+ 2.6.1.157+ 2.7.1.92+	**YES**	—	**YES**	**YES**	—	—
6.2.1	—	—	—	—	—	—	—
6.2.0	**2.1.1.x**、**2.2.1.x**、**2.2.2.x** 2.3.1.73+ 2.4.1.214+ 2.6.1.157+	**YES**	—	**YES**	**YES**	—	—
6.1	**2.0.1.x** 2.1.1.x 2.3.1.73+	**YES**	—	**YES**	**YES**	—	—
6.0.1	**1.1.4.x** 2.0.1.x	**YES**	—	**YES**	—	—	—

ASA 5500-X シリーズおよび ISA 3000

ASA 5500-X シリーズおよび ISA 3000 デバイスは、ASA オペレーティングシステムを使用します。Threat Defense をアップグレードすると、ASA 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 ASA バージョンについては、「バンドルされたコンポーネント（17ページ）」[英語] を参照してください。

バージョン 7.0 は、ASA 5500-X シリーズデバイスをサポートする最後のメジャー Threat Defense リリースです。

表 *8 : ASA 5500-X* シリーズおよび *ISA 3000* との互換性

脅威防御	ISA 3000	ASA 5508-X ASA 5516-X	ASA 5525-X ASA 5545-X ASA 5555-X	ASA 5515-X	ASA 5506-X ASA 5506H-X ASA 5506W-X ASA 5512-X
7.4.1 ～ 7.4.x	**YES**	—	—	—	—
7.4.0	—	—	—	—	—
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**	**YES**	**YES**
6.2.2	—	**YES**	**YES**	**YES**	**YES**
6.2.1	—	—	—	—	—
6.2.0	—	**YES**	**YES**	**YES**	**YES**
6.1	—	**YES**	**YES**	**YES**	**YES**
6.0.1	—	**YES**	**YES**	**YES**	**YES**

Threat Defense Virtual

バージョン 7.0 以降では、Threat Defense Virtual は、スループット要件とリモートアクセス VPN セッション制限に基づいて、パフォーマンス階層 スマート ソフトウェア ライセンシング をサポートします。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、展開の詳細については、使用しているバージョンの『*Cisco Secure Firewall Threat Defense Virtual Getting Started Guide*』 [英語] を参照してください。

表 *9 : Threat Defense Virtual* の互換性：パブリッククラウド

Threat Defense Virtual	Amazon Web Services（AWS）	Microsoft Azure（Azure）	Google Cloud Platform（GCP）	Oracle Cloud Infrastrucure（OCI）
7.4.1 ～ 7.4.x	**YES**	**YES**	**YES**	**YES**
7.4.0	—	—	—	—
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**	—	—
6.6	**YES**	**YES**	—	—
6.4	**YES**	**YES**	—	—
6.3	**YES**	**YES**	—	—
6.2.3	**YES**	**YES**	—	—
6.2.2	**YES**	**YES**	—	—
6.2.1	—	—	—	—
6.2	**YES**	**YES**	—	—
6.1	**YES**	—	—	—
6.0.1	**YES**	—	—	—

表 *10 : Threat Defense Virtual* の互換性：オンプレミス/プライベートクラウド

Threat Defense Virtual	VMware vSphere/VMware ESXi	Cisco HyperFlex（HyperFlex）	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
7.4.1 ～ 7.4.x	**YES** VMware 6.5、6.7、7.0	**YES**	**YES**	**YES**	**YES**
7.4.0	—	—	—	—	—
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**	—	—
6.5	**YES** VMware 6.0、6.5、6.7	—	**YES**	—	—
6.4	**YES** VMware 6.0、6.5	—	**YES**	—	—

Threat Defense Virtual	VMware vSphere/VMware ESXi	Cisco HyperFlex（HyperFlex）	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
6.3	**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	—	—	—	—	—
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	—	—	—	—

Threat Defense 高可用性とクラスタリング

これらの表は、高可用性とクラスタリングに対する脅威防御のサポートを示しています。脅威防御ハードウェアの場合、スタンドアロンデバイス（ネイティブインスタンスまたはアプリケーションモードとも呼ばれます）、またはコンテナインスタンス（マルチインスタンスモードとも呼ばれます）を使用しているかどうかによって、サポートが異なります。Threat Defense Virtual はコンテナインスタンスをサポートしていません。

スタンドアロン デバイス

この表は、スタンドアロンデバイスによる高可用性とクラスタリングのための脅威防御ハードウェアサポートを示しています。管理センターの展開では、すべての脅威防御ハードウェアが高可用性をサポートしています。デバイスマネージャの場合、高可用性はバージョン 6.3 からサポートされていますが、クラスタリングはサポートされていません。

表 *11*：ハードウェア スタンドアロン デバイス：高可用性とクラスタリングのサポート

プラットフォーム	ハイ アベイラビリティ	クラスタリング
Firepower 1000 シリーズ	**YES**	—
Firepower 2100 シリーズ	**YES**	—
Secure Firewall 3100 シリーズ	**YES**	7.1 以降（8 ノード）
Cisco Secure Firewall 4200 シリーズ	**YES**	7.4 以降（8 ノード）
Firepower 4100 シリーズ	**YES**	7.2 以降（16 ノード） 6.2 ～ 7.1（6 ノード）
Firepower 9300	**YES**	7.2 以降（16 ノード） 6.2 ～ 7.1（6 ノード） シャーシ内クラスタリング（3 ノード）もすべてのバージョンでサポートされています。
ASA 5500-X シリーズ	**YES**	—
ISA 3000	**YES**	—

この表は、高可用性（管理センターまたはデバイスマネージャを使用）およびクラスタリング（管理センターのみ）に対する脅威防御の仮想サポートを示しています。

表 *12*：仮想スタンドアロンデバイス：高可用性とクラスタリングのサポート

プラットフォーム	高可用性	クラスタリング
パブリック クラウド		
AWS	—	7.2 以降（16 ノード）
Azure	—	7.3 以降（16 ノード）
GCP	—	7.3 以降（16 ノード）
オンプレミス/プライベートクラウド		
KVM	7.3	7.4.1 以降（16 ノード） 7.2 以降（4 ノード）
VMware	6.7	7.4.1 以降（16 ノード） 7.2 以降（4 ノード）

コンテナインスタンス

この表は、コンテナインスタンスを使用した高可用性とクラスタリングのサポートを示しています。管理センター展開の一部の脅威防御ハードウェアでのみ利用できます。

表 *13*：コンテナインスタンス：高可用性およびクラスタリングのサポート

プラットフォーム	ハイ アベイラビリティ	クラスタリング
Secure Firewall 3100 シリーズ	7.4.1 以降	—
Firepower 4100 シリーズ	6.3+	7.2 以降（16 ノード） 6.6 ～ 7.1（6 ノード）
Firepower 9300	6.3+	7.2 以降（16 ノード） 6.6 ～ 7.1（6 ノード） シャーシ内クラスタリング（3 ノード）もバージョン 6.6 以降でサポートされています。

Threat Defense 管理

デバイスモデルとバージョンに応じて、いくつか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。また、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。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 *14 :* 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
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、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

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

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。

バンドルされたコンポーネント

これらの表は、Threat Defense にバンドルされているさまざまなコンポーネントのバージョンを示しています。この情報を使用して、バンドルされたコンポーネントにおける未解決または解決済みのバグのうち、展開に影響を及ぼす可能性があるものを特定してください。

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。

オペレーティング システム

ASA 5500-X シリーズおよび ISA 3000 デバイスは、ASA オペレーティングシステムを使用します。Firepower 1000/2100 および Secure Firewall 3100/4200 シリーズデバイスは、FXOS オペレーティングシステムを使用します。Firepower 4100/9300 については、Firepower 4100/9300 （6 ページ）を参照してください。

表 *15*：

脅威防御	ASA	FXOS
7.4.1.1	9.20(2.201)	2.14.1.131
7.4.1	9.20(2.2)	2.14.1.131
7.4.0	9.20(1.84)	2.14.0.475

脅威防御	ASA	FXOS
7.3.1.1	9.19(1.202)	2.13.0.1022
7.3.1	9.19(1.200)	2.13.0.1022
7.3.0	9.19(1)	2.13.0.198
7.2.7	9.18(4.201)	2.12.1.73
7.2.6	9.18(4.22)	2.12.1.73
7.2.5.2	9.18(3.61)	2.12.0.530
7.2.5.1	9.18(3.60)	2.12.0.530
7.2.5	9.18(3.53)	2.12.0.519
7.2.4.1	9.18(3.53)	2.12.0.519
7.2.4	9.18(3.39)	2.12.0.499
7.2.3.1	—	—
7.2.3	9.18(2.219)	2.12.0.1030
7.2.2	9.18(2.200)	2.12.0.1104
7.2.1	9.18(2.4)	2.12.0.442
7.2.0.1	9.18(1.200)	2.12.0.31
7.2.0	9.18(1)	2.12.0.31
7.1.0.3	9.17(1.24)	2.11.1.191
7.1.0.2	9.17(1.201)	2.11.1.1300
7.1.0.1	9.17（1.150）	2.11.1.154
7.1.0	9.17（1.0）	2.11.1.154
7.0.6.2	9.16(4.57)	2.10.1.1625
7.0.6.1	9.16(4.45)	2.10.1.1614
7.0.6	9.16(4.35)	2.10.1.1603
7.0.5.1	—	—
7.0.5	9.16(4.200)	2.10.1.1400
7.0.4	9.16(3.18)	2.10.1.208
7.0.3	9.16(3.201)	2.10.1.1200

脅威防御	ASA	FXOS
7.0.2.1	9.16(3.200)	2.10.1.192
7.0.2	9.16(3.11)	2.10.1.192
7.0.1.1	9.16（2.5）	2.10.1.175
7.0.1	9.16（2.5）	2.10.1.175
7.0.0.1	9.16（1.25）	2.10.1.159
7.0.0	9.16(1)	2.10.1.159
6.7.0.3	9.15（1.19）	2.9.1.138
6.7.0.2	9.15(1.15)	2.9.1.138
6.7.0.1	9.15(1.8)	2.9.1.135
6.7.0	9.15(1)	2.9.1.131
6.6.7.2	9.14(4.201)	2.8.1.192
6.6.7.1	9.14(4.21)	2.8.1.192
6.6.7	9.14(4.13)	2.8.1.186
6.6.5.2	9.14(3.22)	2.8.1.172
6.6.5.1	9.14（3.15）	2.8.1.172
6.6.5	9.14（3.6）	2.8.1.165
6.6.4	9.14(2.155)	2.8.1.1148
6.6.3	9.14(2.151)	2.8.1.1146
6.6.1	9.14(1.150)	2.8.1.129
6.6.0.1	9.14(1.216)	2.8.1.105
6.6.0	9.14(1.1)	2.8.1.105
6.5.0.5	9.13(1.18)	2.7.1.129
6.5.0.4	9.13(1.5)	2.7.1.117
6.5.0.3	9.13(1.4)	2.7.1.117
6.5.0.2	9.13(1.151)	2.7.1.115
6.5.0.1	9.13(1.2)	2.7.1.115
6.5.0	9.13(1)	2.7.1.107

脅威防御	ASA	FXOS
6.4.0.18	9.12(4.68)	2.6.1.272
6.4.0.17	9.12(4.62)	2.6.1.265
6.4.0.16	9.12(4.54)	2.6.1.260
6.4.0.15	9.12(4.41)	2.6.1.254
6.4.0.14	9.12（4.37）	2.6.1.239
6.4.0.13	9.12（4.37）	2.6.1.239
6.4.0.12	9.12(4.152)	2.6.1.230
6.4.0.11	9.12(2.40)	2.6.1.214
6.4.0.10	9.12(2.38)	2.6.1.214
6.4.0.9	9.12(2.33)	2.6.1.201
6.4.0.8	9.12(2.18)	2.6.1.166
6.4.0.7	9.12(2.151)	2.6.1.156
6.4.0.6	9.12(2.12)	2.6.1.156
6.4.0.5	9.12(2.4)	2.6.1.144
6.4.0.4	9.12(2.4)	2.6.1.144
6.4.0.3	9.12(1.12)	2.6.1.133
6.4.0.2	9.12(1.10)	2.6.1.133
6.4.0.1	9.12(1.7)	2.6.1.133
6.4.0	9.12(1.6)	2.6.1.133
6.3.0.5	9.10(1.31)	2.4.1.255
6.3.0.4	9.10(1.28)	2.4.1.248
6.3.0.3	9.10(1.18)	2.4.1.237
6.3.0.2	9.10(1.12)	2.4.1.237
6.3.0.1	9.10(1.8)	2.4.1.222
6.3.0	9.10(1.3)	2.4.1.216
6.2.3.18	9.9（2.91）	2.3.1.219
6.2.3.17	9.9（2.88）	2.3.1.217

脅威防御	ASA	FXOS
6.2.3.16	9.9(2.74)	2.3.1.180
6.2.3.15	9.9(2.60)	2.3.1.167
6.2.3.14	9.9(2.55)	2.3.1.151
6.2.3.13	9.9(2.51)	2.3.1.144
6.2.3.12	9.9(2.48)	2.3.1.144
6.2.3.11	9.9(2.43)	2.3.1.132
6.2.3.10	9.9(2.41)	2.3.1.131
6.2.3.9	9.9(2.37)	2.3.1.122
6.2.3.8	9.9(2.37)	2.3.1.122
6.2.3.7	9.9(2.32)	2.3.1.118
6.2.3.6	9.9(2.26)	2.3.1.115
6.2.3.5	9.9(2.245)	2.3.1.108
6.2.3.4	9.9(2.15)	2.3.1.108
6.2.3.3	9.9(2.13)	2.3.1.104
6.2.3.2	9.9(2.8)	2.3.1.85
6.2.3.1	9.9(2.4)	2.3.1.84
6.2.3	9.9(2)	2.3.1.84
6.2.2.5	9.8(2.44)	2.2.2.107
6.2.2.4	9.8(2.36)	2.2.2.86
6.2.2.3	9.8(2.30)	2.2.2.79
6.2.2.2	9.8(2.22)	2.2.2.75
6.2.2.1	9.8(2.10)	2.2.2.63
6.2.2	9.8(2.3)	2.2.2.52
6.2.1	9.8(1)	2.2.1.49
6.2.0.6	9.7(1.25)	—
6.2.0.5	9.7(1.23)	—
6.2.0.4	9.7(1.19)	—
6.2.0.3	9.7(1.15)	—

脅威防御	ASA	FXOS
6.2.0.2	9.7(1.10)	—
6.2.0.1	9.7(1.7)	—
6.2.0	9.7(1.4)	—
6.1.0.7	9.6(4.12)	—
6.1.0.6	9.6(3.23)	—
6.1.0.5	9.6(2.21)	—
6.1.0.4	9.6(2.16)	—
6.1.0.3	9.6(2.16)	—
6.1.0.2	9.6(2.4)	—
6.1.0.1	9.6(2.4)	—
6.1.0	9.6(2)	—
6.0.1.4	9.6(1.19)	—
6.0.1.3	9.6(1.12)	—
6.0.1.2	9.6(1.11)	—
6.0.1.1	9.6(1)	—
6.0.1	9.6(1)	—
6.0.0.1	9.6(1)	—
6.0.0	9.6(1)	—

Snort

Snort は主要検査エンジンです。Snort 3 は、Device Manager とバージョン 6.7 以降、Management Center とバージョン 7.0 以降で使用できます。

表 *16 :*

脅威防御	Snort 2	Snort 3
7.4.1.1	2.9.22-1103	3.1.53.100-56
7.4.1	2.9.22-1009	3.1.53.100-56
7.4.0	2.9.22-181	3.1.53.1-40
7.3.1.1	2.9.21-1109	3.1.36.101-2

脅威防御	Snort 2	Snort 3
7.3.1	2.9.21-1000	3.1.36.100-2
7.3.0	2.9.21-105	3.1.36.1-101
7.2.7	2.9.20-6102	3.1.21.600-26
7.2.6	2.9.20-6102	3.1.21.600-26
7.2.5.2	2.9.20-5201	3.1.21.501-27
7.2.5.1	2.9.20-5100	3.1.21.501-26
7.2.5	2.9.20-5002	3.1.21.500-21
7.2.4.1	2.9.20-4103	3.1.21.401-6
7.2.4	2.9.20-4004	3.1.21.400-24
7.2.3.1	2.9.20-3100	3.1.21.100-7
7.2.3	2.9.20-3010	3.1.21.100-7
7.2.2	2.9.20-2001	3.1.21.100-7
7.2.1	2.9.20-1000	3.1.21.100-7
7.2.0.1	2.9.20-108	3.1.21.1-126
7.2.0	2.9.20-107	3.1.21.1-126
7.1.0.3	2.9.19-3000	3.1.7.3-210
7.1.0.2	2.9.19-2000	3.1.7.2-200
7.1.0.1	2.9.19-1013	3.1.7.2-200
7.1.0	2.9.19-92	3.1.7.1-108
7.0.6.2	2.9.18-6201	3.1.0.602-26
7.0.6.1	2.9.18-6008	3.1.0.600-20
7.0.6	2.9.18-6008	3.1.0.600-20
7.0.5.1	2.9.18-5100	—
7.0.5	2.9.18-5002	3.1.0.500-7
7.0.4	2.9.18-4002	3.1.0.400-12
7.0.3	2.9.18-3005	3.1.0.300-3
7.0.2.1	2.9.18-2101	3.1.0.200-16
7.0.2	2.9.18-2022	3.1.0.200-16

脅威防御	Snort 2	Snort 3
7.0.1.1	2.9.18-1026	3.1.0.100-11
7.0.1	2.9.18-1026	3.1.0.100-11
7.0.0.1	2.9.18-1001	3.1.0.1-174
7.0.0	2.9.18-174	3.1.0.1-174
6.7.0.3	2.9.17-3014	3.0.1.4-129
6.7.0.2	2.9.17-2003	3.0.1.4-129
6.7.0.1	2.9.17-1006	3.0.1.4-129
6.7.0	2.9.17-200	3.0.1.4-129
6.6.7.2	2.9.16-7101	—
6.6.7.1	2.9.16-7100	—
6.6.7	2.9.16-7017	—
6.6.5.2	2.9.16-5204	—
6.6.5.1	2.9.16-5107	—
6.6.5	2.9.16-5034	—
6.6.4	2.9.16-4022	—
6.6.3	2.9.16-3033	—
6.6.1	2.9.16-1025	—
6.6.0.1	2.9.16-140	—
6.6.0	2.9.16-140	—
6.5.0.5	2.9.15-15510	—
6.5.0.4	2.9.15-15201	—
6.5.0.3	2.9.15-15201	—
6.5.0.2	2.9.15-15101	—
6.5.0.1	2.9.15-15101	—
6.5.0	2.9.15-7	—
6.4.0.18	2.9.14-28000	—
6.4.0.17	2.9.14-27005	—
6.4.0.16	2.9.14-26002	—

脅威防御	Snort 2	Snort 3
6.4.0.15	2.9.14-25006	—
6.4.0.14	2.9.14-24000	—
6.4.0.13	2.9.14-19008	—
6.4.0.12	2.9.14-18011	—
6.4.0.11	2.9.14-17005	—
6.4.0.10	2.9.14-16023	—
6.4.0.9	2.9.14-15906	—
6.4.0.8	2.9.14-15707	—
6.4.0.7	2.9.14-15605	—
6.4.0.6	2.9.14-15605	—
6.4.0.5	2.9.14-15507	—
6.4.0.4	2.9.12-15301	—
6.4.0.3	2.9.14-15301	—
6.4.0.2	2.9.14-15209	—
6.4.0.1	2.9.14-15100	—
6.4.0	2.9.14-15003	—
6.3.0.5	2.9.13-15503	—
6.3.0.4	2.9.13-15409	—
6.3.0.3	2.9.13-15307	—
6.3.0.2	2.9.13-15211	—
6.3.0.1	2.9.13-15101	—
6.3.0	2.9.13-15013	—
6.2.3.18	2.9.12-1813	—
6.2.3.17	2.9.12-1605	—
6.2.3.16	2.9.12-1605	—
6.2.3.15	2.9.12-1513	—
6.2.3.14	2.9.12-1401	—
6.2.3.13	2.9.12-1306	—

脅威防御	Snort 2	Snort 3
6.2.3.12	2.9.12-1207	—
6.2.3.11	2.9.12-1102	—
6.2.3.10	2.9.12-902	—
6.2.3.9	2.9.12-806	—
6.2.3.8	2.9.12-804	—
6.2.3.7	2.9.12-704	—
6.2.3.6	2.9.12-607	—
6.2.3.5	2.9.12-506	—
6.2.3.4	2.9.12-383	—
6.2.3.3	2.9.12-325	—
6.2.3.2	2.9.12-270	—
6.2.3.1	2.9.12-204	—
6.2.3	2.9.12-136	—
6.2.2.5	2.9.11-430	—
6.2.2.4	2.9.11-371	—
6.2.2.3	2.9.11-303	—
6.2.2.2	2.9.11-273	—
6.2.2.1	2.9.11-207	—
6.2.2	2.9.11-125	—
6.2.1	2.9.11-101	—
6.2.0.6	2.9.10-301	—
6.2.0.5	2.9.10-255	—
6.2.0.4	2.9.10-205	—
6.2.0.3	2.9.10-160	—
6.2.0.2	2.9.10-126	—
6.2.0.1	2.9.10-98	—
6.2.0	2.9.10-42	—
6.1.0.7	2.9.9-312	—

脅威防御	Snort 2	Snort 3
6.1.0.6	2.9.9-258	—
6.1.0.5	2.9.9-225	—
6.1.0.4	2.9.9-191	—
6.1.0.3	2.9.9-159	—
6.1.0.2	2.9.9-125	—
6.1.0.1	2.9.9-92	—
6.1.0	2.9.9-330	—
6.0.1.4	2.9.8-490	—
6.0.1.3	2.9.8-461	—
6.0.1.2	2.9.8-426	—
6.0.1.1	2.9.8-383	—
6.0.1	2.9.8-224	—

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 *17*:

脅威防御	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

脅威防御	VDB	GeoDB
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
6.0.1 ～ 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 Management Center 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。
- 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 *18 :* 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

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		
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
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

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		
7.0	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
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

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		
6.2.2	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	—

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 Management Center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
- Secure Firewall Management Center にバンドルされています：Cisco Secure Firewall Management Center デバイス構成ガイド

表 *19 :* 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	クラウド提供型（CDO を使用）
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、Secure Firewall 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 *20 : 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	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	×	×	対応	対応	×	×	×	×	対応	対応	×	×
バージョン 2.0（オンプレミス）	対応	×	×	対応	対応	×	×	×	対応	対応	対応	×	×
Secure Firewall Management Center 7.4.1	対応	×	×	対応	対応	×	対応	対応	対応	対応	対応	対応	対応

脅威の検出

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。

表 21 : 統合製品：脅威の検出

Management Center/Threat Defense	Cisco SecureX	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 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**	**YES**	—
6.4	**YES**	**YES** FTD 6.4 の FMC が必要です。	**YES**	**YES**	**YES**
6.3	—	—	—	**YES**	**YES**
6.1 ～ 6.2.3	—	—	—	**YES**	—

Threat Defense 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 22 : 統合型製品：*Threat Defense RA VPN*

Threat Defense	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 *23 :* ブラウザ

ブラウザ	デバイスマネージャのバージョン
Google Chrome	任意（Any）
Mozilla Firefox	任意（Any）
Microsoft Edge（Windows のみ）	バージョン 6.7 以降
Microsoft Internet Explorer 11（Windows のみ）	バージョン 6.6 以前
Microsoft Internet Explorer 10（Windows のみ）	バージョン 6.2.3 以前
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、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。

Microsoft Internet Explorer 10 または 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。
- [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（Internet Explorer 11 のみ）。
- アプライアンスの IP アドレス/URL に対して [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

表 *24 :* 画面解像度

インターフェイス	最小解像度
デバイス マネージャ	1024 X 768
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。

デバイスマネージャで自己署名証明書の置き換えを開始するには、[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。 > 詳細な手順については、オンラインヘルプまたはCisco Secure Firewall Device Manager Configuration Guide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。

（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。Cisco Secure Firewall 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 Secure Firewall Device Manager Configuration Guide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 *25:* 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

バージョン	販売終了	更新終了	サポート終了	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
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

バージョン	販売終了	更新終了	サポート終了	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
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

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 *26 :* 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

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。

表 *27 : Threat Defense* ハードウェア *EOL* の通知

プラットフォーム	最後のデバイスバージョン	管理する最後の管理センター	販売終了	サポート終了	通知
Firepower 4110	7.2	TBD	2024 年 7 月 31 日	2027 年 1 月 31 日	Cisco Firepower 4110 シリーズ セキュリティ アプライアンスに関する 3 年間サブスクリプションの販売終了およびサポート終了の通知
			2022 年 1 月 31 日	2027 年 1 月 31 日	Cisco Firepower 4110 シリーズ セキュリティ アプライアンスに関する 5 年間サブスクリプションの販売終了およびサポート終了の通知
ASA 5508-X、5516-X	7.0	7.4	**2021 年 8 月 2 日**	2026 年 8 月 31 日	Cisco ASA5508 と ASA5516 シリーズセキュリティ アプライアンスおよび 5 年間サブスクリプションの販売終了およびサポート終了の通知
ASA 5525-X、5545-X、5555-X	6.6	7.2	**2020 年 9 月 4 日**	2025 年 9 月 30 日	Cisco ASA5525、ASA5545、ASA5555 シリーズ セキュリティ アプライアンスおよび 5 年間サブスクリプションの販売終了およびサポート終了の通知
Firepower 4120、4140、4150	7.2	TBD	**2020 年 8 月 31 日**	2025 年 8 月 31 日	Cisco Firepower 4120/40/50 および FPR 9300 SM24/36/44 シリーズ セキュリティ アプライアンスとモジュールおよび 5 年間サブスクリプションの販売終了およびサポート終了の通知
Firepower 9300 : SM-24、SM-36、SM-44 モジュール	7.2	TBD	**2020 年 8 月 31 日**	2025 年 8 月 31 日	Cisco Firepower 4120/40/50 および FPR 9300 SM24/36/44 シリーズ セキュリティ アプライアンスとモジュールおよび 5 年間サブスクリプションの販売終了およびサポート終了の通知

プラットフォーム	最後のデバイスバージョン	管理する最後の管理センター	販売終了	サポート終了	通知
ASA 5515-X	6.4	7.0	**2017 年 8 月 25 日**	**2022 年 8 月 31 日**	Cisco ASA 5512-X および ASA 5515-X の販売終了およびサポート終了の通知
ASA 5506-X、5506H-X、5506W-X	6.2.3	6.6	**2021 年 8 月 2 日**	2026 年 8 月 31 日	ASA ソフトウェアを搭載した Cisco ASA5506 シリーズ セキュリティ アプライアンスの販売終了およびサポート終了の通知
			2021 年 7 月 31 日	**2022 年 7 月 31 日**	Cisco ASA5506 シリーズ セキュリティ アプライアンスに関する 1 年間サブスクリプションの販売終了およびサポート終了の通知
			2020 年 5 月 5 日	**2022 年 7 月 31 日**	Cisco ASA5506 シリーズ セキュリティ アプライアンスに関する 3 年間サブスクリプションの販売終了およびサポート終了の通知
			2018 年 9 月 30 日	**2022 年 7 月 31 日**	Cisco ASA5506 シリーズ セキュリティ アプライアンスに関する 5 年間サブスクリプションの販売終了およびサポート終了の通知
ASA 5512-X	6.2.3	6.6	**2017 年 8 月 25 日**	**2022 年 8 月 31 日**	Cisco ASA 5512-X および ASA 5515-X の販売終了およびサポート終了の通知

用語とブランディング

表 ***28 :*** 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 *29* : 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 *30* : 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 *31* : 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。

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。