



最適なアプリケーションとマネージャを見つける方法

ハードウェアプラットフォームは、2つのアプリケーションのいずれかを実行できます。アプリケーションごとに、マネージャを選択できます。この章では、アプリケーションとマネージャの選択肢について説明します。

- [アプリケーション \(1 ページ\)](#)
- [マネージャ \(1 ページ\)](#)

アプリケーション

ハードウェアプラットフォームでは、Cisco Secure Firewall ASA または Secure Firewall Threat Defense (旧 Firepower Threat Defense) のいずれかのアプリケーションを使用できます。

- ASA : ASA は、従来の高度なステートフルファイアウォールおよびVPN コンセントレータです。
- Threat Defense —脅威防御は、高度なステートフルファイアウォール、VPN コンセントレータ、および次世代IPSを組み合わせた次世代ファイアウォールです。

シスコでは、ASA から Threat Defense への移行ツールを提供しています。このツールは、ASA の使用を開始し、後に Threat Defense に再イメージ化する場合に、ASA を Threat Defense に変換するのに役立ちます。

ASA と Threat Defense 間での再イメージ化の方法については、『[Cisco Secure Firewall ASA and Secure Firewall Threat Defense Reimage Guide](#)』を参照してください。

マネージャ

Threat Defense と ASA は複数のマネージャをサポートします。

Threat Defense マネージャ



(注) Secure Firewall Device Manager (旧 Firepower Device Manager) は、Cisco Secure Firewall 4200 ではサポートされていません。

表 1: Threat Defense マネージャ

マネージャ	説明
Secure Firewall Management Center (旧 Firepower Management Center)	<p>Management Center はマルチデバイスマネージャで、独自のサーバーハードウェア上で、またはハイパーバイザ上の仮想デバイスとして稼働します。</p> <p>管理ネットワークで Management Center を開始するには、「Management Center での Threat Defense の展開」を参照してください。</p> <p>リモートネットワークで Management Center を開始するには、「リモート Threat Defense による Management Center の展開」を参照してください。</p>
Cisco Defense Orchestrator (CDO) クラウド提供型 Firewall Management Center	<p>CDO のクラウド提供型 Firewall Management Center には、オンプレミス管理センターのすべての設定機能があります。分析機能については、クラウドソリューションまたはオンプレミスの管理センターを使用できます。CDO は、ASA などの他のセキュリティデバイスも管理します。</p> <p>CDO プロビジョニングを開始するには、CDO での Threat Defense の展開 を参照してください。</p>
Cisco Secure Firewall Threat Defense REST API	<p>Threat Defense REST API を使用すると、Threat Defense の直接設定を自動化できます。Management Center を使用して Threat Defense を管理している場合は、この API を使用できません。</p> <p>このガイドでは、Threat Defense REST API について説明しません。詳細については、Cisco Secure Firewall Threat Defense REST API ガイドを参照してください。</p>
Secure Firewall Management Center REST API	<p>Management Center REST API を使用すると、管理対象の Threat Defense に適用可能な Management Center ポリシーの設定を自動化できます。この API は、Threat Defense を直接管理しません。</p> <p>このガイドでは、Management Center REST API について説明しません。詳細については、Cisco Secure Firewall Management Center REST API クイックスタートガイドを参照してください。</p>

ASA マネージャ

表 2: ASA マネージャ

マネージャ	説明
Adaptive Security Device Manager (ASDM)	<p>ASDM は Java ベースのオンデバイスマネージャであり、ASA のすべての機能を提供します。</p> <p>ASDM を使用する前に ASDM を使用した ASA の展開 を参照してください。</p>
CLI	<p>CLI を使用して、すべての ASA 機能を設定できます。</p> <p>CLI については、このガイドでは取り上げていません。詳細については、『ASA 構成ガイド』を参照してください。</p>
CDO	<p>CDO はクラウドベースのマルチデバイスマネージャです。CDO は Threat Defense などの他のセキュリティデバイスも管理します。</p> <p>ASA の CDO については、このガイドでは取り上げていません。CDO を使用する前に、CDO のホームページ を参照してください。</p>
Cisco Security Manager (CSM)	<p>CSM は、独自のサーバーハードウェア上で動作するマルチデバイスマネージャです。CSM は Threat Defense の管理をサポートしていません。</p> <p>CSM については、このガイドでは取り上げていません。詳細については、『CSM ユーザーガイド』を参照してください。</p>
ASA HTTP インターフェイス	<p>HTTP を使用すると、自動化ツールは特定形式の URL にアクセスすることで、ASA でコマンドを実行できます。</p> <p>ASA HTTP インターフェイスについては、このガイドでは取り上げていません。詳細については、「自動化向けの Cisco Secure Firewall ASA HTTP インターフェイス」を参照してください。</p>

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。