



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 \(2 ページ\)](#)

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) 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 の高度な機能が必要ない場合、または Threat Defense ではまだ使用できない ASA 専用の機能が必要な場合は、ASA の使用が適しています。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。

- **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。つまり、Threat Defense は ASA の機能を最大限に活用し、最適な次世代ファイアウォールと IPS 機能を融合させます。

Threat Defense には ASA の主要な機能の大部分に加えて、次世代ファイアウォールと IPS 機能が追加されているため、ASA よりも FTD を使用することをお勧めします。

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

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 は強力な Web ベースのマルチデバイスマネージャです。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。マルチデバイスマネージャを必要とし、Threat Defense のすべての機能が必要な場合は、Management Center を使用する必要があります。Management Center は、トラフィックとイベントの強力な分析とモニタリングも提供します。</p> <p>(注) Management Center は Threat Defense 設定を持ち、Management Center をバイパスして Threat Defense を直接設定することはできないため、Management Center は他のマネージャとの互換性がありません。</p> <p>Management Center を開始する前に、「Firepower 9300 シャーシの初期設定」に従ってシャーシをセットアップします。また、「Management Center での Threat Defense の展開」を参照してください。</p>
Secure Firewall Device Manager (旧 Firepower Device Manager)	<p>Device Manager は、Web ベースのシンプルなオンデバイスマネージャです。簡素化されているため、一部の Threat Defense 機能は Device Manager では使用できません。少数のデバイスのみを管理し、マルチデバイスマネージャを必要としない場合は、Device Manager を使用するのに適しています。</p> <p>(注) FDM モードの Device Manager と CDO の両方でファイアウォールの設定を検出できるため、Device Manager と CDO を使用して同じファイアウォールを管理することが可能です。Management Center は他のマネージャと互換性がありません。</p> <p>Device Manager を開始する前に、「Firepower 9300 シャーシの初期設定」に従ってシャーシをセットアップします。また、「Device Manager での Threat Defense の展開」を参照してください。</p>

マネージャ	説明
Cisco Defense Orchestrator (CDO)	<p>CDO には 2 つの管理モードがあります。</p> <ul style="list-style-type: none"> • (7.2 以降) オンプレミスの管理センターのすべての設定機能を備えたクラウド提供型の管理センターモード。分析機能については、クラウド内の Secure Cloud Analytics またはオンプレミスの管理センターのいずれかを使用できます。 • (既存の CDO ユーザーのみ) ユーザーエクスペリエンスが簡素化されたデバイスマネージャモード。このモードは、すでに CDO を使用してデバイスマネージャモードで Threat Defense を管理しているユーザーのみが使用できます。このモードについては、このガイドでは説明していません。 <p>CDO はクラウドベースであるため、独自のサーバーで CDO を実行する必要はありません。CDO は ASA などの他のセキュリティデバイスも管理するため、すべてのセキュリティデバイスに単一のマネージャを使用できます。</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。Device Manager と CDO はどちらもファイアウォールで設定を検出できるため、この API はそれらの両方と互換性があります。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。CLI よりも GUI を使用することを好み、管理が必要な ASA が少数の場合は、ASDM の使用が適しています。ASDM はファイアウォールの設定を検出できるため、ASDM で CLI、CDO、または CSM を使用することも可能です。</p> <p>ASDM を開始する前に、Firepower 9300 シャーシの初期設定に従ってシャーシをセットアップします。また、ASDM を使用した ASA の展開を参照してください。</p>
CLI	<p>GUI よりも CLI を使用することを好む場合は、ASA CLI を使用してください。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、シンプルなクラウドベースのマルチデバイスマネージャです。シンプル化されているため、一部の ASA 機能は CDO では使用できません。シンプルな管理エクスペリエンスを提供するマルチデバイスマネージャが必要な場合、CDO を使用するのに適しています。また、CDO はクラウドベースであるため、独自のサーバーで CDO を実行する必要はありません。CDO は Threat Defense などの他のセキュリティデバイスも管理するため、すべてのセキュリティデバイスに単一のマネージャを使用できます。CDO はファイアウォールの設定を検出できるため、CLI や ASDM を使用することも可能です。</p> <p>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強力なマルチデバイスマネージャです。多数の ASA を管理する必要がある場合、CSM を使用するのに適しています。CSM はファイアウォールの設定を検出できるため、CLI や ASDM を使用することも可能です。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 REST API	<p>ASA REST API を使用すると、ASA の設定を自動化できます。ただし、API にはすべての ASA 機能が搭載されておらず、拡張されることもありません。</p> <p>ASA REST API 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、Cisco ASA REST API クイック スタートガイド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。