



ようこそ

このドキュメントでは、以下に示すバージョン 7.2 のリリース情報を記載しています。

- Cisco Secure Firewall Threat Defense
- Cisco Secure Firewall Management Center
- Cisco Secure Firewall Device Manager

このドキュメントでは、お客様が導入したハードウェアと仮想アプライアンスについて説明します。Cisco Defense Orchestrator (CDO)、またはクラウド提供型の管理センターで Secure Firewall Threat Defense を管理している場合は、「[Cisco Defense Orchestrator の新機能](#)」も参照してください。

- [リリースの主なポイント \(1 ページ\)](#)
- [リリース日 \(2 ページ\)](#)
- [推奨リリース \(2 ページ\)](#)
- [シスコとのデータの共有 \(3 ページ\)](#)
- [支援が必要な場合 \(3 ページ\)](#)

リリースの主なポイント

Cisco Secure Firewall へのブランド名の変更

以下の製品は、バージョン 7.2 でブランド名が変更されました。

表 1:バージョン 7.2でブランド名が変更された製品

旧製品名	変更後の製品名
Firepower Threat Defense (FTD)	Cisco Secure Firewall Threat Defense
Firepower Threat Defense Virtual (FTDv)	Cisco Secure Firewall Threat Defense Virtual
Firepower Device Manager (FDM)	Cisco Secure Firewall Device Manager

旧製品名	変更後の製品名
Firepower Management Center (FMC)	Cisco Secure Firewall Management Center
Firepower Management Center Virtual (FMCv)	Cisco Secure Firewall Management Center Virtual
Firepower Extensible Operating System (FXOS)	Cisco Secure Firewall Extensible Operating System (FXOS)
Firepower Chassis Manager	Cisco Secure Firewall Chassis Manager

リリース日

表 2:バージョン 7.2のリリース日

バージョン	ビルド	日付	プラットフォーム
7.2.0	82	2022-06-06	すべて

推奨リリース

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。

また、新機能ガイドにも推奨リリースを示します。

- [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 \(リリース別\)](#)

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。

シスコとのデータの共有

次の機能はシスコとデータを共有します。

Cisco Success Network

Cisco Success Network は、テクニカル サポートを提供するために不可欠な使用状況に関する情報と統計情報をシスコに送信します。

初期設定およびアップグレード中に、登録するか尋ねられます。登録はいつでも変更できます。

Cisco Support Diagnostics

Cisco Support Diagnostics（「シスコのプロアクティブサポート」とも呼ばれる）は、設定および運用上の健全性データをシスコに送信し、自動化された問題検出システムを通じてそのデータを処理して問題をプロアクティブに通知できるようにします。また、この機能により、Cisco TACTAC ケースの過程でデバイスから必要な情報を収集することもできます。

初期設定およびアップグレード中に、登録するか尋ねられます。登録はいつでも変更できます。この機能は Device Manager で現在サポートされていません。

Web 分析トラッキング

Web 分析のトラッキングは、これに限定されませんが、ページでの操作、ブラウザのバージョン、製品のバージョン、ユーザーの場所、management center の管理 IP アドレスまたはホスト名を含む、個人を特定できない使用状況データをシスコに送信します。

デフォルトで登録されていますが、初期設定の完了後にいつでも登録を変更できます。

支援が必要な場合

オンラインリソース

シスコは、ドキュメント、ソフトウェア、ツールのダウンロードのほか、バグを照会したり、サービスリクエストをオープンしたりするための次のオンラインリソースを提供しています。これらのリソースは、Cisco ソフトウェアをインストールして設定したり、技術的問題を解決したりするために使用してください。

- マニュアル : <http://www.cisco.com/go/threatdefense-72-docs>
- シスコサポートおよびダウンロードサイト : <https://www.cisco.com/c/en/us/support/index.html>
- Cisco Bug Search Tool : <https://tools.cisco.com/bugsearch/>
- シスコ通知サービス : <https://www.cisco.com/cisco/support/notifications.html>

シスコ サポートおよびダウンロードサイトの大部分のツールにアクセスする際は、Cisco.com のユーザー ID およびパスワードが必要です。

シスコへのお問い合わせ

上記のオンラインリソースを使用して問題を解決できない場合は、Cisco TAC にお問い合わせください。

- Cisco TAC の電子メール アドレス : tac@cisco.com
- Cisco TAC の電話番号（北米） : 1.408.526.7209 または 1.800.553.2447
- Cisco TAC の連絡先（世界全域） : [Cisco Worldwide Support の連絡先](#)

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。