

# Cisco Secure Firewall 移行ツール互換性ガイド

初版：2020年10月29日

最終更新：2023年2月2日

## Cisco Secure Firewall 移行ツール互換性ガイド

このガイドには、オペレーティングシステムとホスティング環境の要件を含む、Cisco Secure Firewall ソフトウェアとハードウェアの互換性が記載されています。

### 移行がサポートされるプラットフォーム

Cisco Secure Firewall 移行ツールによる移行では、以下の ASA、ASA with FPS、FDM 管理対象デバイス、およびターゲット Threat Defense プラットフォームがサポートされています。

#### サポートされる送信元 ASA プラットフォーム

Cisco Secure Firewall 移行ツールを使用して、次のシングルコンテキスト/マルチコンテキスト ASA プラットフォームから構成を移行できます。



(注) Cisco Secure Firewall 移行ツールは、スタンドアロン ASA デバイスからスタンドアロン 脅威に対する防御 デバイスへの移行のみをサポートします。

- ASA 5510
- ASA 5520
- ASA 5540
- ASA 5550
- ASA 5580
- ASA 5506
- ASA 5506W-X
- ASA 5506H-X
- ASA 5508-X
- ASA 5512-X

- ASA 5515-X
- ASA 5516-X
- ASA 5525-X
- ASA 5545-X
- ASA 5555-X
- ASA 5585-X (ASA のみ。Cisco Secure Firewall 移行ツールは ASA FirePOWER module から構成を移行しません)
- Firepower 1000 シリーズ
- Firepower 2100 シリーズ
- Firewall 3100 シリーズ
- Firepower 4100 シリーズ
- Firepower 9300 シリーズ
  - SM-24
  - SM-36
  - SM-40
  - SM-44
  - SM-48
  - SM-56
- VMware ESXi、VMware vSphere Web クライアント、または vSphere スタンドアロンクライアントを使用して展開された VMware 上の ASA Virtual

#### ASA with FPS の移行でサポートされる送信元 ASA モデル

Cisco ASA FirePOWER モジュールは、次のデバイスに展開されます。



---

(注) Cisco Secure Firewall 移行ツールは、スタンドアロン ASA with FPS デバイスからスタンドアロン脅威に対する防御 デバイスへの移行のみをサポートします。

---

- ASA5506-X
- ASA5506H-X
- ASA5506W-X
- ASA5508-X
- ASA5512-X

- ASA5515-X
- ASA5516-X
- ASA5525-X
- ASA5545-X
- ASA5555-X
- ASA5585-X-SSP-10
- ASA5585-X-SSP-20
- ASA5585-X-SSP-40
- ASA5585-X-SSP-60

#### サポートされるソース **FDM** 管理対象デバイスプラットフォーム

Cisco Secure Firewall 移行ツールを使用して、次のシングルコンテキスト/マルチコンテキスト FDM 管理対象デバイスプラットフォームから構成を移行できます。

- Firepower 1000 シリーズ
- Firepower 2100 シリーズ
- Firewall 3100 シリーズ
- Firepower 4100 シリーズ
- Firepower 9300 シリーズ
- VMware、AWS、Azure、KVM 上の FDM Virtual

#### サポートされるターゲット **Threat Defense** プラットフォーム

Cisco Secure Firewall 移行ツールを使用して、次の脅威に対する防御 プラットフォームのスタンドアロンまたはコンテナインスタンスに送信元 ASA、ASA with FPS、Check Point、PAN、Fortinet 構成を移行できます。

- ASA 5506
- ASA 5506W-X
- ASA 5506H-X
- ASA 5508-X
- ASA 5512-X
- ASA 5515-X
- ASA 5516-X
- ASA 5525-X
- ASA 5545-X

- ASA 5555-X
- Firepower 1000 シリーズ
- Firepower 2100 シリーズ
- Firewall 3100 シリーズ
- Firepower 4100 シリーズ
- Firepower 9300 シリーズ (次を含む) :
  - SM-24
  - SM-36
  - SM-40
  - SM-44
  - SM-48
  - SM-56
- Threat Defense Virtual (VMware 上)。VMware ESXi、VMware vSphere Web クライアント、または vSphere スタンドアロンクライアントを使用して展開されていること

## 移行でサポートされるソフトウェアのバージョン

移行可能な ASA、ASA with FPS、Check Point、PAN、Fortinet、脅威に対する防御 のバージョンは次のとおりです。

### サポートされている ASA ファイアウォールのバージョン

Cisco Secure Firewall 移行ツールは、ASA ソフトウェアバージョン 8.4 以降を実行しているデバイスからの移行をサポートしています。

### サポートされている ASA with FPS ファイアウォールのバージョン

Cisco Secure Firewall 移行ツールは、ASA with FPS ソフトウェアバージョン 9.2.2 以降を実行しているデバイスからの移行をサポートしています。

詳細については、Cisco ASA 互換性ガイドの「[ASA FirePOWER Module Compatibility](#)」セクションを参照してください。

### サポートされているデバイスマネージャのバージョン

Cisco Secure Firewall 移行ツールは、バージョン 7.2 以降を実行しているデバイスマネージャからの移行をサポートしています。

### サポートされている Check Point ファイアウォールのバージョン

Cisco Secure Firewall 移行ツールは、Check Point OS バージョン r75 ~ r77.30 および r80 ~ r80.40 を実行している 脅威に対する防御 への移行をサポートしています。[送信元の選択 (Select Source)] ページで適切な Check Point バージョンを選択します。



(注) VSX はサポートされていません。

Cisco Secure Firewall 移行ツールは、現在、Check Point Platform Gaia からの移行をサポートしています。

### サポートされている Palo Alto Networks のファイアウォールのバージョン

Cisco Secure Firewall 移行ツールは、PAN ファイアウォール OS バージョン 6.1.x 以降を実行している 脅威に対する防御 への移行をサポートしています。

### サポートされている Fortinet Networks ファイアウォールのバージョン

Cisco Secure Firewall 移行ツールは、FortiNet ファイアウォール OS バージョン 5.0 以降を実行している 脅威に対する防御 への移行をサポートしています。

### ソース ASA 設定でサポートされている Secure Firewall Management Center のバージョン

ASA の場合、Cisco Secure Firewall 移行ツールは、バージョン 6.2.3 または 6.2.3+ を実行している Management Center によって管理される 脅威に対する防御 デバイスへの移行をサポートしています。



(注) 一部の機能は、以降のバージョンの Management Center および 脅威に対する防御 でのみサポートされています。



(注) 最適な移行時間を実現するには、Management Center を、[software.cisco.com/downloads](https://software.cisco.com/downloads) からダウンロードできる推奨リリースバージョンにアップグレードすることをお勧めします。

### 送信元 ASA with FPS 構成でサポートされている Management Center のバージョン

ASA with FPS の場合、Cisco Secure Firewall 移行ツールは、バージョン 6.5 以降を実行している Management Center によって管理される 脅威に対する防御 デバイスへの移行をサポートしています。

### ソース FDM 管理対象デバイス構成でサポートされる Management Center のバージョン

FDM 管理対象デバイスの場合、Cisco Secure Firewall 移行ツールは、バージョン 7.3 以降を実行している Management Center への移行をサポートしています。

### 送信元 Check Point、PAN、および Fortinet ファイアウォール構成でサポートされている Management Center のバージョン

Check Point、PAN、Fortinet ファイアウォールの場合、Cisco Secure Firewall 移行ツールは、バージョン 6.2.3.3 以降を実行している Management Center によって管理される 脅威に対する防御 デバイスへの移行をサポートしています。



(注) 一部の機能は、以降のバージョンの Management Center および 脅威に対する防御 でのみサポートされています。たとえば、Fortinet の時間ベース ACL は、Management Center 6.6 以降でサポートされています。



(注) 6.7 脅威に対する防御 デバイスへの移行は現在サポートされていません。そのため、デバイスに Management Center アクセス用のデータインターフェイスで設定されている場合、移行が失敗する可能性があります。

### サポートされる Threat Defense のバージョン

Cisco Secure Firewall 移行ツールでは、脅威に対する防御 のバージョン 6.2.3 以降を実行しているデバイスへの移行が推奨されます。

脅威に対する防御 のオペレーティングシステムとホスティング環境の要件を含めた Cisco Secure Firewall のソフトウェアとハードウェアの互換性の詳細については、『[Cisco Secure Firewall Compatibility Guide](#)』 [英語] を参照してください。

## Cisco Secure Firewall 移行ツールのプラットフォーム要件

Cisco Secure Firewall 移行ツールには、次のインフラストラクチャとプラットフォームの要件があります。

- Microsoft Windows 10 64 ビット オペレーティング システムまたは macOS バージョン 10.13 以降で実行している
- Google Chrome がシステムのデフォルトブラウザである
- (Windows) [Power & Sleep] で [Sleep] 設定が [Never put the PC to Sleep] に設定されているため、大規模な移行プッシュ中にシステムがスリープ状態にならない
- (macOS) 大規模な移行プッシュ中にコンピュータとハードディスクがスリープ状態にならないように [Energy Saver] 設定が構成されている

## 関連資料

このセクションでは、Cisco Secure Firewall 移行ツールに関連するドキュメントの概要を示します。

- 『[Cisco Secure Firewall Threat Defense Compatibility Guide](#)』 [英語] : オペレーティングシステムとホスティング環境の要件を含む、Cisco Firewall 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。
- 『[Cisco ASA Compatibility](#)』 : Cisco ASA ソフトウェアおよびハードウェアの互換性と要件を示します。
- 『[Cisco Firepower 4100/9300 FXOS Compatibility](#)』 [英語] : FXOS、Cisco Firepower 9300 および Cisco Firepower 4100 シリーズ セキュリティ アプライアンス、サポートされる論理デバイスのソフトウェアとハードウェアの互換性情報を示します。



## 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。