Cisco Secure Firewall 移行ツールのスタートアップガイド

- Cisco Secure Firewall 移行ツールについて （1 ページ）
- Cisco Secure Firewall 移行ツールの最新情報 （4 ページ）
- Cisco Secure Firewall 移行ツールのライセンス （8 ページ）
- Cisco Secure Firewall 移行ツールのプラットフォーム要件 （8 ページ）
- Threat Defense デバイスの要件および前提条件 （9 ページ）
- 注意事項と制約事項 （9 ページ）
- 移行がサポートされるプラットフォーム （13 ページ）
- サポートされる移行先の管理センター （14 ページ）
- 移行でサポートされるソフトウェアのバージョン （16 ページ）

Cisco Secure Firewall 移行ツールについて

このガイドでは、Cisco Secure Firewall 移行ツールをダウンロードして移行を完了する方法について説明します。さらに、発生する可能性のある移行の問題を解決するのに役立つトラブルシューティングのヒントも提供します。

本書に記載されている移行手順の例（移行例： PAN から Threat Defense 2100）は、移行プロセスに関する理解を促進するのに役立ちます。

Cisco Secure Firewall 移行ツールは、サポートされている PAN 構成をサポートされている 脅威に対する防御 プラットフォームに変換します。Cisco Secure Firewall 移行ツールを使用すると、サポートされている PAN の機能とポリシーを自動的に 脅威に対する防御 に移行できます。サポートされていない機能はすべて、手動で移行する必要があります。

Cisco Secure Firewall 移行ツールは PAN の情報を収集して解析し、最終的に Secure Firewall Management Center にプッシュします。解析フェーズ中に、Cisco Secure Firewall 移行ツールは、以下を特定する**移行前レポート**を生成します。

- エラーのある PAN 構成の XML 行

- PAN には、Cisco Secure Firewall 移行ツールが認識できない PAN XML 行がリストされています。**移行前レポート**とコンソールログのエラーセクションの下には、XML 構成行が記載されています。これにより、移行がブロックされています

解析エラーがある場合は、問題を修正し、新しい構成を再アップロードし、接続先デバイスに接続し、インターフェイスを脅威に対する防御インターフェイスにマッピングし、アプリケーションをマッピングし、セキュリティゾーンをマッピングして、構成の確認と検証に進むことができます。その後、構成を接続先デバイスに移行できます。

コンソール

Cisco Secure Firewall 移行ツールを起動すると、コンソールが開きます。コンソールには、Cisco Secure Firewall 移行ツールの各ステップの進行状況に関する詳細情報が表示されます。コンソールの内容は、Cisco Secure Firewall 移行ツールのログファイルにも書き込まれます。

Cisco Secure Firewall 移行ツールが開いていて実行中の間は、コンソールを開いたままにする必要があります。

重要 Cisco Secure Firewall 移行ツールを終了するために Web インターフェイスが実行されているブラウザを閉じると、コンソールはバックグラウンドで実行され続けます。Cisco Secure Firewall 移行ツールを完全に終了するには、キーボードの Command キー + C を押してコンソールを終了します。

ログ

Cisco Secure Firewall 移行ツールは、各移行のログを作成します。ログには、移行の各ステップで発生した内容の詳細が含まれるため、移行が失敗した場合の原因の特定に役立ちます。

Cisco Secure Firewall 移行ツールのログファイルは、`<migration_tool_folder>\logs` にあります。

リソース

Cisco Secure Firewall 移行ツールは、**移行前レポート**、**移行後レポート**、 PAN 構成、およびログのコピーを `resources` フォルダに保存します。

`resources` フォルダは、`<migration_tool_folder>\resources` にあります。

未解析ファイル

未解析ファイルは、`<migration_tool_folder>\resources` にあります。

Cisco Secure Firewall 移行ツールでの検索

[最適化、確認および検証（Optimize, Review and Validate）] ページの項目など、Cisco Secure Firewall 移行ツールに表示されるテーブル内の項目を検索できます。

テーブルの任意の列または行の項目を検索するには、テーブルの上の **検索**（🔍） をクリックし、フィールドに検索語を入力します。Cisco Secure Firewall 移行ツールはテーブル行をフィルタ処理し、その検索語を含む行のみを表示します。

単一の列で項目を検索するには、列見出しにある [検索（Search）] フィールドに検索語を入力します。Cisco Secure Firewall 移行ツールはテーブル行をフィルタ処理し、検索語に一致する行のみを表示します。

ポート

Cisco Secure Firewall 移行ツールは、ポート 8321 ー 8331 およびポート 8888 の 12 ポートのうちいずれかのポートで実行されるテレメトリをサポートします。デフォルトでは、Cisco Secure Firewall 移行ツールはポート 8888 を使用します。ポートを変更するには、`app_config` ファイルのポート情報を更新します。更新後、ポートの変更を有効にするために、Cisco Secure Firewall 移行ツールを再起動します。`app_config` ファイルは、*<migration_tool_folder>*`\app_config.txt` にあります。

（注） テレメトリはこれらのポートでのみサポートされているため、ポート 8321 ～ 8331 およびポート 8888 を使用することを推奨します。Cisco Success Network を有効にすると、Cisco Secure Firewall 移行ツールに他のポートを使用できなくなります。

Cisco Success Network

Cisco Success Network はユーザ対応のクラウドサービスです。Cisco Success Network を有効にすると、Cisco Secure Firewall 移行ツールと Cisco Cloud 間にセキュアな接続が確立され、使用状況に関する情報と統計情報がストリーミングされます。テレメトリをストリーミングすることによって、Cisco Secure Firewall 移行ツールからの対象のデータを選択して、それを構造化形式でリモートの管理ステーションに送信するメカニズムが提供されるため、次のメリットが得られます。

- ネットワーク内の製品の有効性を向上させるために、利用可能な未使用の機能について通知します。
- 製品に利用可能な、追加のテクニカルサポートサービスとモニタリングについて通知します。
- シスコ製品の改善に役立ちます。

Cisco Secure Firewall 移行ツールはセキュアな接続を確立および維持し、Cisco Success Network に登録できるようにします。Cisco Success Network を無効にすることで、いつでもこの接続をオフにできます。これにより、デバイスが Cisco Success Network クラウドから接続解除されます。

Cisco Secure Firewall 移行ツールの最新情報

バージョン	サポートされる機能
5.0.1	このリリースには、次の新機能と機能拡張が含まれています。 • Cisco Secure Firewall 移行ツールは、Cisco Secure Firewall ASA から Threat Defense デバイスへの複数のトランスペアレント ファイアウォール モードのセキュリティコンテキストの移行をサポートするようになりました。Cisco Secure Firewall ASA デバイス内の 2 つ以上のトランスペアレント ファイアウォール モードのコンテキストをトランスペアレントモードのインスタンスにマージし、それらを移行できます。1 つ以上のコンテキストに VPN 設定がある場合の VPN 設定の ASA 展開では、VPN 設定をターゲットの Threat Defense に移行するコンテキストを 1 つ選択できます。選択しなかったコンテキストからは、VPN 設定以外のすべての設定が移行されます。 詳細については、「ASA セキュリティコンテキストの選択 」を参照してください。 • Cisco Secure Firewall 移行ツールを使用して、サイト間およびリモートアクセス VPN 設定を Fortinet および Palo Alto Networks ファイアウォールから Threat Defense に移行できるようになりました。**[機能の選択（Select Features）]** ペインから、移行する VPN 機能を選択します。Palo Alto Networks および Fortinet ファイアウォール移行ガイドの**「Cisco Secure Firewall 移行ツールの接続先パラメータの指定」**セクションを参照してください。 • Cisco Secure Firewall ASA デバイスから 1 つ以上のルーテッドまたはトランスペアレント ファイアウォール モードのセキュリティコンテキストを選択し、Cisco Secure Firewall 移行ツールを使用してシングルコンテキストまたはマルチコンテキストを移行できるようになりました。

バージョン	サポートされる機能
5.0	• Cisco Secure Firewall 移行ツールは、Cisco Secure Firewall ASA から Threat Defense デバイスへの複数のセキュリティコンテキストの移行をサポートするようになりました。いずれかのコンテキストから設定を移行するか、すべてのルーテッド ファイアウォール モードのコンテキストから設定をマージして移行するかを選択できます。複数のトランスペアレント ファイアウォール モード コンテキストからの設定のマージのサポートは、まもなく利用可能になります。詳細については、「ASA プライマリ セキュリティ コンテキストの選択」を参照してください。 • 移行ツールは、仮想ルーティングおよび転送（VRF）機能を活用して、マルチコンテキストの ASA 環境で観察される分離されたトラフィックフローを複製します。これは、新たにマージされた設定の一部になります。移行ツールが検出したコンテキストの数は、新しい **[コンテキスト（Contexts）]** タイルで確認でき、解析後は **[解析の概要（Parsed Summary）]** ページの新しい **[VRF]** タイルで確認できます。また移行ツールは、**[セキュリティゾーンとインターフェイスグループへのインターフェイスのマッピング（Map Interfaces to Security Zones and Interface Groups）]** ページに、これらの VRF がマッピングされているインターフェイスを表示します。 • Cisco Secure Firewall 移行ツールの新しいデモモードを使用して移行ワークフロー全体を試し、実際の移行がどのようになるかを可視化できるようになりました。詳細については、「ファイアウォール移行ツールでのデモモードの使用」を参照してください。 • 新しい機能拡張とバグの修正により、Cisco Secure Firewall 移行ツールは、Palo Alto Networks ファイアウォールの Threat Defense への移行に関して、改善された迅速な移行エクスペリエンスをご提供します。
4.0.3	Cisco Secure Firewall 移行ツール 4.0.3 には、バグの修正と、次の新たな拡張機能が含まれています。 • 移行ツールで、PAN 設定を Threat Defense に移行するための強化された **[アプリケーションマッピング（Application Mapping）]** 画面が提供されるようになりました。詳細については、『移行ツールを使用した *Palo Alto Networks* ファイアウォールから *Cisco Secure Firewall Threat Defense* への移行』ガイドの「構成とアプリケーションのマッピング」を参照してください。

バージョン	サポートされる機能
4.0.2	Cisco Secure Firewall 移行ツール 4.0.2 には、次の新機能と拡張機能が含まれています。 • Secure Firewall 移行ツール は、ルールごとのアプリケーションによるアクセス制御リスト（ACL）の分割をサポートするようになりました。Palo Alto Networks ファイアウォール設定に、1 つのルールが複数のアプリケーションに設定されたACLが含まれている場合は、**ルールごとのアプリケーションによる ACL の分割**オプションを使用して、1 つのルールにつきアプリケーションが 1 つの複数のルールに分割できます。移行ツールは、1 つのアプリケーションに対して1つのルールが設定されるように新しいルールを作成します。これにより、設定の確認と検証がより明確になります。 • 移行ツールは、ダイナミック IP またはポートフォールバック アドレスの送信元ファイアウォールのNAT設定を検証し、フォールバックアドレスが宛先ゾーンアドレスと同じである場合にのみ設定を移行するようになりました。これは Cisco Secure Firewall Management Center が、ダイナミック IP またはポート フォールバック インターフェイスとして宛先アドレスしか持てないためです。 • 移行ツールに常時接続のテレメトリが追加されました。ただし、限定的なテレメトリデータまたは広範なテレメトリデータの送信を選択できるようになっています。限定的なテレメトリデータにデータポイントはほとんど含まれませんが、広範なテレメトリデータは、より詳細なテレメトリデータのリストを送信します。この設定は、**[設定（Settings）] > [テレメトリデータをシスコに送信しますか（Send Telemetry Data to Cisco?）]** から変更できます。.

バージョン	サポートされる機能
4.0.1	Cisco Secure Firewall 移行ツール 4.0.1 には、次の新機能と拡張機能が含まれています。 • Secure Firewall 移行ツールは、Management Center バージョン 7.1 以降に移行するときに、変換された宛先で完全修飾ドメイン名（FQDN）オブジェクトを使用するネットワークアドレス変換（NAT）ルールをサポートするようになりました。 **重要** 変換されたソースに FQDN オブジェクトまたは FQDN オブジェクトグループがある NAT ルール、元のソースと宛先の両方に FQDN オブジェクトと FQDN オブジェクトグループがある NAT ルール、および変換された宛先に FQDN オブジェクトグループがある NAT ルールはサポートされていません。 • ACL の最適化が強化され、最適化されたアプリケーションを一覧表示する新しい [アプリケーション（Application）] 列が移行後レポートに含まれるようになりました。
3.0.1	• ASA with FirePOWER Services、Check Point、Palo Alto Networks、および Fortinet の場合、Secure Firewall 3100 シリーズは宛先デバイスとしてのみサポートされます。
3.0	Cisco Secure Firewall 移行ツール 3.0 は、移行先の管理センターが 7.2 以降の場合、Palo Alto Networks からクラウド提供型 Firewall Management Center への移行をサポートするようになりました。

バージョン	サポートされる機能
2.1	• PAN OS バージョン 6.1.x 以降をサポートします。 • Cisco Secure Firewall 移行ツールを使用すると、次の PAN の構成要素を 脅威に対する防御 に移行できます。 • インターフェイス • スタティック ルート • ネットワークオブジェクトおよびグループ • ポートオブジェクトおよびポートグループ • アクセスコントロールリスト（ポリシー） • ゾーン • アプリケーション • NAT ルール • [確認と検証（Review and Validate）] ページで使用可能なコンテンツベースの検索機能。 • UI の機能が強化され、進行状況バーが表示されるようになりました。

Cisco Secure Firewall 移行ツールのライセンス

Cisco Secure Firewall 移行ツールアプリケーションは無料であり、ライセンスは必要ありません。ただし、脅威に対する防御 デバイスの正常な登録とポリシーの展開のため、Management Center には関連する 脅威に対する防御 機能に必要なライセンスが必要です。

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

Threat Defense デバイスの要件および前提条件

管理センターに移行する場合、ターゲット Threat Defense デバイスが追加される場合とされない場合があります。Threat Defense デバイスへの今後の展開のために、共有ポリシーを管理センターに移行できます。デバイス固有のポリシーを Threat Defense に移行するには、管理センターに追加する必要があります。PANの設定の Threat Defense への移行を計画する場合は、次の要件と前提条件を考慮してください。

- ターゲット Threat Defense デバイスは、管理センターに登録されている必要があります。
- Threat Defense デバイスは、スタンドアロンデバイスまたはコンテナインスタンスにすることができます。クラスタまたは高可用性設定の一部であっては**なりません**。
  - ターゲット Threat Defense デバイスがコンテナインスタンスである場合、使用する物理インターフェイス、物理サブインターフェイス、ポート チャネル インターフェイス、およびポート チャネル サブインターフェイス（「管理専用」を除く）が、PAN の使用しているものと同数以上必要です。そうでない場合は、ターゲット Threat Defense デバイスに必要なタイプのインターフェイスを追加する必要があります。

（注）

- サブインターフェイスは、Cisco Secure Firewall 移行ツールでは作成されません。インターフェイスマッピングのみが許可されます。
- 異なるインターフェイスタイプ間のマッピングは許可されます。たとえば、物理インターフェイスをポート チャネル インターフェイスにマップできます。

注意事項と制約事項

Cisco Secure Firewall 移行ツールは、変換中にルールまたはポリシーで使用されるかどうかにかかわらず、サポートされているすべてのオブジェクトおよびルールに対して 1 対 1 のマッピングを作成します。Cisco Secure Firewall 移行ツールには、未使用のオブジェクト（ACL および NAT で参照されていないオブジェクト）の移行を除外できる最適化機能があります。

Cisco Secure Firewall 移行ツールは、サポートされていないオブジェクト、NAT ルール、およびルートを移行しません。

PAN 構成の制約事項

送信元 PAN 構成の移行には、次の制限があります。

- Cisco Secure Firewall 移行ツールを使用すると、マルチ VSYS を移行できます。
- システム構成は移行されません。
- Management Center では、ネストされたサービス オブジェクト グループまたはポートグループはサポートされていません。変換の一環として、Cisco Secure Firewall 移行ツールは、参照されているネストされたオブジェクトグループまたはポートグループの内容を展開します。
- Cisco Secure Firewall 移行ツールは、1 つの回線にある送信元ポートと宛先ポートを持つ拡張サービスのオブジェクトまたはグループを、複数の回線にまたがる異なるオブジェクトに分割します。このようなアクセスコントロールルールの参照は、同じ意味の Management Center ルールに変換されます。

PAN 移行の注意事項

Cisco Secure Firewall 移行ツールは、次のような 脅威に対する防御 構成のベストプラクティスを使用します。

- ACL ログオプションの移行は、脅威に対する防御 のベストプラクティスに従います。ルールのログオプションは、送信元 PAN 構成に基づいて有効または無効になります。アクションが **deny** のルールの場合、Cisco Secure Firewall 移行ツールは接続の開始時にロギングを構成します。アクションが **permit** の場合、Cisco Secure Firewall 移行ツールは接続の終了時にロギングを構成します。

サポートされる PAN 構成

Cisco Secure Firewall 移行ツールは、次の PAN 構成を完全に移行できます。

- ネットワークオブジェクトおよびグループ
- ゾーン（レイヤ 2、レイヤ 3、仮想ワイヤ）
- サービス オブジェクト
- サービス オブジェクト グループ（ネストされたサービス オブジェクト グループを除く）

（注） Management Center ではネストはサポートされていないため、Cisco Secure Firewall 移行ツールは参照されるルールの内容を拡張します。ただし、ルールは完全な機能で移行されます。

- IPv4 および IPv6 FQDN オブジェクトとグループ
- IPv6 変換のサポート（インターフェイス、スタティックルート、オブジェクト、ACL）

- アクセス ルール
- NAT ルール

（注） サービスに「application-default」が設定されているすべてのポリシーは、「any」として移行されます。脅威に対する防御 には同等の機能がないためです。

変換済み送信元と元の宛先には、「any」オブジェクトが Management Center で事前定義されていません。したがって、0.0.0.0/0 を持つ Obj_0.0.0.0 という名前のオブジェクトが作成され、プッシュされます。

- 変換された宛先に FQDN オブジェクトがある NAT ルール（バージョン 7.1 以降を実行している Secure Firewall Threat Defense に移行する場合）
- 物理インターフェイス
- サブインターフェイス（サブインターフェイス ID は、移行時に常に VLAN ID と同じ番号に設定されます）
- 集約インターフェイス（ポートチャネル）
- 静的ルート（移行されない Next VR および ECMP のルートとしてネクストホップが設定されているルートを除く）

（注） 送信元ファイアウォール（PAN）に静的ルートとして設定されたルートが接続されている場合、プッシュの失敗が発生します。Management Center では、接続済みルートの静的ルートを作成できません。そのようなルートを削除し、移行を続行します。

（注） 仮想ワイヤインターフェイスは移行されませんが、仮想ワイヤゾーンは移行されます。移行後、脅威に対する防御 で BVI インターフェイスを手動で作成する必要があります。

部分的にサポートされる PAN 構成

Cisco Secure Firewall 移行ツールは、次の PAN 構成の移行を部分的にサポートしています。これらの構成の一部には、詳細オプションを使用するルールが含まれ、それらのオプションなしで移行されます。Management Center がこれらの詳細オプションをサポートしている場合は、移行の完了後に手動で構成できます。

- プロファイルを使用したアクセス コントロール ポリシー ルール

- TCP、UDP、SCTP を含むプロトコルを使用するサービスオブジェクトを含むサービスグループ。

（注） SCTP タイプが削除され、サービスグループが部分的に移行されます。

- サポートされているオブジェクトとサポートされていないオブジェクトを含むオブジェクトグループは、サポートされていないオブジェクトを削除することによって移行されます。

サポートされない PAN 構成

Cisco Secure Firewall 移行ツールは、次の PAN 構成の移行をサポートしていません。これらの構成が Management Center でサポートされている場合、移行の完了後に手動で構成できます。

- 時間ベースのアクセス コントロール ポリシー ルール
- ユーザーベースのアクセス コントロール ポリシー ルール
- プロトコル SCTP を使用するサービスオブジェクト
- 特殊文字で始まる、または特殊文字を含む FQDN オブジェクト
- ワイルドカード FQDN
- SCTP で構成された NAT ルール
- 変換済み送信元に FQDN オブジェクトと FQDN オブジェクトグループを含む NAT ルール
- 元の送信元と宛先の両方に FQDN オブジェクトと FQDN オブジェクトグループを含む NAT ルール
- 変換済み接続先に FQDN オブジェクトグループを含む NAT ルール
- IPv6 NAT
- URL フィルタリングを使用するポリシー

脅威に対する防御 でサポートされていない機能を構成するには、『Threat Defense Configuration Guide』を参照してください。

（注） サポートされているポリシーもサポートされていないポリシーもすべて Management Center に移行されます。サポートされていないポリシーは、無効として移行されます。これらのポリシーは、回避策の後、または Management Center に従って構成した後に、有効にすることができます。

プロファイル URL フィルタリング、ユーザー ID、送信元、または宛先ネゲートを含むポリシーは**サポートされていません**。

Threat Defense デバイスに関する注意事項と制約事項

PAN 構成を 脅威に対する防御 に移行する予定で、ルート、インターフェイスなど、脅威に対する防御 に既存のデバイス固有の構成がある場合、プッシュ移行中に Cisco Secure Firewall 移行ツールは自動的にデバイスを消去し、PAN 構成から上書きします。

（注） デバイス（ターゲット 脅威に対する防御）構成データの望ましくない損失を防ぐために、移行前にデバイスを手動で消去することを推奨します。

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 PAN 、および 脅威に対する防御 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 脅威に対する防御 プラットフォームの詳細については、『Cisco Secure Firewall Compatibility Guide』[英語] を参照してください。

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、脅威に対する防御 プラットフォームの次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 構成を移行できます。

- Firepower 1000 シリーズ
- Firepower 2100 シリーズ
- Secure 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
- 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 Threat Defense（VMware 上）
- Microsoft Azure クラウドまたは AWS クラウド上の Threat Defense Virtual

（注）

- Azure における Threat Defense Virtual の前提条件と事前設定については、『Getting Started with Secure Firewall Threat Defense Virtual』[英語] を参照してください。
- AWS クラウドにおける Threat Defense Virtual の前提条件と事前設定については、「Threat Defense Virtual の前提条件」を参照してください。

これらの環境ごとに要件に従って事前設定された Cisco Secure Firewall 移行ツールには、Microsoft Azure または AWS クラウド内の Management Center に接続し、構成をそのクラウド内の Management Center に移行させるためのネットワーク接続が必要です。

（注） 移行を成功させるには、Cisco Secure Firewall 移行ツールを使用する前に、Management Center または Threat Defense Virtual を事前設定するための前提条件が満たされている必要があります。

サポートされる移行先の管理センター

Cisco Secure Firewall 移行ツールは、管理センターおよびクラウド提供型 Firewall Management Center によって管理される Threat Defense デバイスへの移行をサポートします。

Management Center

管理センターは強力な 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。移行のためのターゲット管理センターとして、オンプレミス管理センターと仮想管理センターの両方を使用できます。

管理センターは、移行に関する次のガイドラインを満たす必要があります。

- 移行でサポートされる Mangement Center ソフトウェアバージョン（移行でサポートされるソフトウェアのバージョン （16 ページ）を参照）。
- PAN の移行でサポートされる Management Center ソフトウェアバージョンは 6.1.x 以降です。
- PAN インターフェイスから移行する予定のすべての機能を含む 脅威に対する防御 用のスマートライセンスを取得済みおよびインストール済みであること。次を参照してください。
  - Cisco.com の「Cisco Smart Accounts」の「Getting Started」セクション。
  - Register the Firepower Management Center with the Cisco Smart Software Manager [英語]

- Licensing the Firewall System [英語]
- REST API の Management Center が有効になっています。

  Management Center Web インターフェイスで、**[システム（System）] > [設定（Configuration）] > [Rest API設定（Rest API Preferences）] > [Rest APIを有効にする（Enable Rest API）]**に移動し、**[Rest APIを有効にする（Enable Rest API）]**チェックボックスをオンにします。

重要 REST API を有効にするには、 Management Center の管理者ユーザーロールが必要です。管理センターのユーザーロールの詳細については、「ユーザーロール」を参照してください。

クラウド提供型 Firewall Management Center

クラウド提供型 Firewall Management Center は、Threat Defense デバイスの管理プラットフォームであり、Cisco Defense Orchestrator を介して提供されます。クラウド提供型 Firewall Management Center は、管理センターと同じ機能を多数提供します。

CDO からクラウド提供型 Firewall Management Center にアクセスできます。CDO は、Secure Device Connector（SDC）を介してクラウド提供型 Firewall Management Center に接続します。クラウド提供型 Firewall Management Center の詳細については、「クラウド提供型 Firewall Management Center による Cisco Secure Firewall Threat Defense デバイスの管理」を参照してください。

Cisco Secure Firewall 移行ツールは、移行先の管理センターとしてクラウド提供型 Firewall Management Center をサポートしています。クラウド提供型 Firewall Management Center を移行先の管理センターとして選択するには、CDO リージョンを追加し、CDO ポータルから API トークンを生成する必要があります。

CDO リージョン

CDO は 3 つの異なる地域で利用でき、地域は URL 拡張子で識別できます。

表 *1 : CDO* の地域と *URL*

地域	CDO URL
ヨーロッパ地域	https://defenseorchestrator.eu/
US リージョン	https://defenseorchestrator.com/
APJC リージョン	https://www.apj.cdo.cisco.com/

移行でサポートされるソフトウェアのバージョン

移行のためにサポートされている Cisco Secure Firewall 移行ツール、 PAN 、および 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 Cisco Secure Firewall 移行ツールのバージョン

software.cisco.com に掲載されているバージョンは、当社のエンジニアリングおよびサポート組織によって正式にサポートされているバージョンです。software.cisco.com から最新バージョンの Cisco Secure Firewall 移行ツールをダウンロードすることを強くお勧めします。

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。

送信元 PAN 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

PAN 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 Management Center デバイスへの移行をサポートしています。

（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 6.5 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 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 Firepower Compatibility Guide』[英語] を参照してください。

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。