Cisco Secure Firewall Threat Defense バージョン 7.6.1 モデル移行ガイド

改訂：2025 年 10 月 22 日

Secure Firewall Threat Defense モデルの移行について

Secure Firewall Threat Defense のモデル移行ウィザードを使用すると、古い Firewall Threat Defense モデルから別のモデルに設定を移行できます。移行後、ソース Firewall Threat Defense デバイスからのすべてのルーティングおよびインターフェイス設定はターゲット Firewall Threat Defense で使用できます。

このウィザードは、ソースデバイスとターゲットデバイスとして複数のモデルをサポートしています。詳細については、移行でサポートされるデバイス （2 ページ）を参照してください。

Firepower 4100 および 9300 シリーズ デバイスをサポートされているモデルに移行すると、要件に応じてインターフェイス属性を設定できるようになりました。ソースデバイスインターフェイスをターゲットデバイスインターフェイスにマップできます。移行により、ソースデバイスとターゲットデバイスがロックされます。

移行でサポートされるデバイス

サポートされているソースデバイス

- Cisco Firepower 1120
- Cisco Firepower 1140
- Cisco Firepower 1150
- Cisco Firepower 2110
- Cisco Firepower 2120
- Cisco Firepower 2130
- Cisco Firepower 2140
- Cisco Firepower 4110
- Cisco Firepower 4120
- Cisco Firepower 4140
- Cisco Firepower 4150
- Cisco Firepower 9300 シリーズ SM-24
- Cisco Firepower 9300 シリーズ SM-36
- Cisco Firepower 9300 シリーズ SM-44

（注） ソースデバイスはバージョン 7.2.x 以降である必要があります。

サポートされるターゲットデバイス

- Cisco Secure Firewall 3105
- Cisco Secure Firewall 3110
- Cisco Secure Firewall 3120
- Cisco Secure Firewall 3130
- Cisco Secure Firewall 3140
- Cisco Firepower 4215
- Cisco Firepower 4225
- Cisco Firepower 4245

（注） ターゲットデバイスはバージョン 7.4.1 以降である必要があります。

サポートされている移行パス

次の表に、現在のソース Firewall Threat Defense モデルから移行できるサポート対象のターゲット Firewall Threat Defense モデルを示します。

移行元モデル	移行先モデル			
	Cisco Secure Firewall 3100 シリーズ	**Cisco Secure Firewall 4200 シリーズ**	**Cisco Secure Firewall 3100 シリーズのインスタンス**	**Cisco Secure Firewall 4200 シリーズのインスタンス**
Firepower 1100 シリーズ	対応	—	—	—
Firepower 2100 シリーズ	対応	—	—	—
Firepower 4100 シリーズ	対応	対応	—	—
Firepower 9300 シリーズ	対応	対応	—	—
Firepower 4100 シリーズのインスタンス	—	—	対応	対応
Firepower 9300 シリーズのインスタンス	—	—	対応	対応

移行用のライセンス

- スマート ライセンス アカウントには、ターゲットデバイスのソフトウェア利用資格が必要です。

- スマート ライセンス アカウントにデバイスを登録する必要があります。移行すると、ソースデバイスのライセンスがターゲットデバイスにコピーされます。

移行の前提条件

- **一般的なデバイスの前提条件**
  - ソースデバイスとターゲットデバイスを Firewall Management Center に登録する必要があります。
  - ターゲットデバイスが、何も設定されていない新しく登録されたデバイスであることを確認します。
  - ソースデバイスとターゲットデバイスは以下の状態とモードが同じである必要があります。
    - ドメイン
    - ファイアウォールモード：ルーテッドまたはトランスペアレント
    - コンプライアンスモード（CC または UCAPL）
    - 管理状態

      デバイスには、同じタイプのマネージャ アクセス インターフェイス（管理インターフェイスまたはデータインターフェイス）が必要です。
    - マルチインスタンスモードまたはアプライアンスモード
  - デバイスに対する変更権限を持っていることを確認します。
  - ソースデバイスの設定は有効で、エラーがない必要があります。
  - 移行中は、いずれのデバイスでも展開、インポート、またはエクスポートタスクを実行しないでください。ソースデバイスには、保留中の展開を設定できます。
- **変更管理の前提条件**
  - ソースデバイスとターゲットデバイスが変更管理チケットによってロックされていないことを確認します。
  - ソースデバイスに割り当てられた共有ポリシーが変更管理チケットによってロックされていないことを確認します。
- **HA デバイスの前提条件**
  - アクティブな Firewall Management Center からのみデバイスを移行します。
- **マルチインスタンスモードのデバイスの前提条件**
  - ソースデバイスとターゲットデバイスがマルチインスタンスモードであることを確認します。
  - シャーシの構成は手動で移行してください。インスタンス設定をターゲットインスタンスに移行する前に、インスタンスを作成します。ターゲットデバイスには互換性のあるインターフェイスが必要です。たとえば、ターゲットデバイスで EtherChannel インターフェイスを作成し、それらのインターフェイスに対してタグ付き、タグなし、専用、または共有のインターフェイスをターゲットデバイスで作成する必要があります。

- **アウトオブバンド構成を持つデバイスの前提条件**
  - アウトオブバンドの変更を確認し、Firewall Management Center内の設定と一致していることを確認します。これらの構成のデバイスは移行できません。アウトオブバンド設定を表示するには：
    1. [デバイス（Devices）] > [デバイス管理（Device Management）] を選択します。
    2. デバイスの横にある編集アイコンをクリックし、[インターフェイス（Interfaces）] タブをクリックします。

- **マネージャ アクセス インターフェイスを持つデバイスの前提条件**

  デバイスがデータ転送状態または管理転送状態になっていないことを確認します。デバイスがこれらの状態にある場合は移行できません。
  - データ転送状態：デバイス上の変更を展開することなく、マネージャ アクセス インターフェイスがデータインターフェイスから管理インターフェイスに変更された場合のデバイス状態。
  - 管理転送状態：デバイス上の変更を展開することなく、マネージャアクセスインターフェイスが管理インターフェイスからデータインターフェイスに変更されたときのデバイス状態。

- **マージされた管理インターフェイスと診断インターフェイスを持つデバイスの前提条件**

  ターゲットデバイスが常にマージモードになっていることを確認します。

ウィザードで移行される設定

移行ウィザードにより、次の設定がソースデバイスからターゲットデバイスにコピーされます。

- ライセンス
- インターフェイス設定
- インラインセット設定
- ルーティング設定
- DHCP および DDNS 構成
- 仮想ルータ設定
- ポリシー
- 関連するオブジェクトとオブジェクトのオーバーライド
- プラットフォーム設定
- リモートブランチ展開の構成

移行ウィザードにより、次のポリシー設定がソースデバイスからターゲットデバイスにコピーされます。

- 正常性ポリシー

- NAT ポリシー
- QoS ポリシー
- リモートアクセス VPN ポリシー
- FlexConfig ポリシー
- アクセス コントロール ポリシー
- プレフィルタ ポリシー
- IPS ポリシー
- DNS ポリシー
- SSL ポリシー
- マルウェアおよびファイルポリシー
- ID ポリシー
- 共有ポリシー

移行ウィザードにより、次のルーティング設定がソースデバイスからターゲットデバイスにコピーされます。

- ECMP
- BFD
- OSPFv2/v3
- EIGRP
- RIP
- BGP
- ポリシーベースルーティング
- スタティックルート
- マルチキャストルーティング
- 仮想ルータ

移行ウィザードにより、次のインターフェイスがソースデバイスからターゲットデバイスにコピーされます。

- 物理インターフェイス
- サブインターフェイス
- EtherChannel インターフェイス
  - スタンドアロンデバイスでは、ウィザードは EtherChannel をソースデバイスからターゲットデバイスにコピーします。

- マルチインスタンスモードのデバイスの場合は、シャーシでEtherChannelを作成してインスタンスに割り当てる必要があります。

- □ブリッジ グループ インターフェイス
- VTI インターフェイス
- VNI インターフェイス
- ループバック インターフェイス
- インラインインターフェイス
- VXLAN トンネルエンドポイント（VTEP）インターフェイス

移行ウィザードは、ターゲットデバイスのデバイスグループを保持します。

移行に関するガイドラインと制限事項

ガイドライン

- **マルチインスタンスモードのデバイスの場合**：

  移行中に、次の表に従ってインターフェイスをマッピングしていることを確認します。

ソースデバイス	ターゲットデバイス
物理インターフェイス	物理インターフェイス
EtherChannel インターフェイス	EtherChannel インターフェイス
スーパーバイザがプロビジョニングしたサブインターフェイス	スーパーバイザがプロビジョニングしたサブインターフェイス
タグ付けされたインターフェイス	タグ付けされたインターフェイス
タグなしインターフェイス	タグなしインターフェイス
共有インターフェイス	共有および専用インターフェイス
専用インターフェイス	専用インターフェイス

  スーパーバイザがプロビジョニングしたサブインターフェイスを、インスタンスが作成したサブインターフェイスにマッピングすることはできません。

- **HA デバイスの場合**、次のものを移行できます。
  - 送信元 HA デバイスからターゲット HA デバイスへ。
  - 送信元 HA デバイスからターゲット スタンドアロン デバイスへ。

- **リモートブランチ展開のデバイスの場合**：
  - ソース マネージャ アクセス インターフェイスからターゲット マネージャ アクセス インターフェイスにマッピングします。
  - ソースおよびターゲット Firewall Management Center のマネージャ アクセス インターフェイスが同じ IP アドレスタイプ（静的または DHCP）であることを確認します。
  - 両方のマネージャ アクセス インターフェイスに IPv4 または IPv6 アドレスが必要です。
  - マネージャ アクセス インターフェイスに静的 IP アドレスがある場合は、それらが同じサブネット内にあることを確認します。
- **Snort の場合**：
  - ターゲットデバイスが Snort 3 の場合、移行後は Snort 3 になります。
  - ソースデバイスとターゲットデバイスに Snort 2 がある場合、移行後はターゲットデバイスに Snort 2 が設定されます。
- **診断インターフェイスを使用するデバイスの場合**：

  移行後、ターゲットデバイスではマージされた管理インターフェイスのみを使用できます。

制限事項

- 移行ウィザードは以下のものを移行しません。
  - サイト間 VPN ポリシー
  - Firepower 2100 シリーズの SNMP デバイス設定

    移行後、デバイスのプラットフォーム設定を使用して SNMP を設定できます。
- 一度に実行できる移行は 1 つだけです。
- リモートアクセス VPN トラストポイント証明書は移行後、登録されません。
- HA デバイスの場合：
  - ターゲットデバイス：スタンドアロンデバイスを HA デバイスに移行することはできません。
- クラスタリングはサポートされません。
- リモートブランチ展開のデバイスの場合：
  - ウィザードは、単一の WAN マネージャ アクセス データ インターフェイスをデュアル WAN マネージャ アクセス データ インターフェイスに移行しません。

Secure Firewall Threat Defense の移行

始める前に

必ず移行の前提条件 （4 ページ）および移行に関するガイドラインと制限事項 （7 ページ）を確認してください。

手順

ステップ 1 [ファイアウォールデバイス（Firewall Devices）]>[デバイス管理（Device Management）] を選択します。

ステップ 2 ページの右上隅にある [移行（Migrate）] をクリックします。

ステップ 3 [ソースデバイスとターゲットデバイスの選択（Select source and target devices）] :

a) [ソースデバイス（Source Device）] ドロップダウンリストからデバイスを選択します。

b) [ターゲットデバイス（Target Device）] ドロップダウンリストからデバイスを選択します。

ソースデバイスとターゲットデバイスは、次のタグを持つことができます。

- [ルーテッド（Routed）] : ルーテッド ファイアウォール モードのデバイス。
- [透過型（Transparent）] : 透過型ファイアウォールモードのデバイス。
- [コンテナ（Container）] : マルチインスタンスモードのデバイス。
- [高可用性（High Availability）] : 高可用性モードのデバイス。
- [分析のみ（Analytics Only）] : Security Cloud Control と Firewall Management Center によって管理されるデバイスは、イベントの受信と表示のみを行います（分析専用 Firewall Management Center）。

デバイスが HA ペアの一部である場合、HA ペア名のみが表示されます。

ステップ 4 [次へ（Next）] をクリックします。

ステップ 5 （アプライアンスモードの Firepower 4100 および 9300 シリーズ デバイスのみ）[シャーシマネージャの詳細（Chassis manager details）] で次の手順を実行します。

a) 必要に応じて、[シャーシマネージャのスキップ（Skip chassis manager）] チェックボックスをオンにします。

b) [シャーシのホスト名またはIPアドレス（Chassis hostname or IP address）] フィールドに、値を入力します。

（注）
- Firewall Management Center から Cisco Secure Firewall Chassis Manager に到達できることを確認します。
- Firewall Management Center では選択が検証されないため、ソースデバイスに対して正しいシャーシマネージャを選択してください。

c) [証明書の確認（Verify certificate）] をクリックして、シャーシマネージャの証明書を確認します。

d) [ユーザー名（Username）] および [パスワード（Password）] フィールドに、シャーシマネージャのログイン情報を入力します。

ステップ 6 [次へ（Next）] をクリックします。

ステップ 7 [インターフェイスの設定（Configure interfaces）] で、次の操作を行います。

デフォルトでは、送信元インターフェイスとターゲットインターフェイスは、インターフェイスのハードウェア名を使用してマッピングされます。名前付きインターフェイス、論理インターフェイス、および他のインターフェイスの一部であるインターフェイスをマッピングする必要があります。他のすべてのインターフェイスのマッピングは、必須ではありません。ウィザードでは、ユーザーが提供するインターフェイスマッピングに従って、論理インターフェイスが作成されます。

HA フェールオーバー構成の一部であるインターフェイスはマッピングできません。それらのインターフェイスは、ウィザードで無効化されています。

アプライアンスモードの Firepower 4100 および 9300 シリーズ デバイス：

これらのデバイスの場合、Firewall Management Center はシャーシマネージャから速度、デュプレックス、自動ネゴシエーションなどのインターフェイス属性を取得します。

a) 次のいずれかのオプションをクリックして、ターゲットデバイスでこれらのインターフェイス属性を設定します。

- [ターゲットデバイスの値の保持（Retain target device values）]：（デフォルト）ターゲットデバイスで設定されているインターフェイス属性を保持します。
- [ソースデバイスからコピー（Copy from source device）]：ソースデバイスからインターフェイス属性をコピーします。

  このオプションは、Firewall Management Center がシャーシマネージャに正常に接続した場合にのみ有効になります。このオプションを使用することをお勧めします。物理インターフェイスの速度、デュプレックス、および自動ネゴシエーションの値は、ターゲットデバイスと互換性がない場合はデフォルト値に設定されます。

- [デバイス値のカスタマイズ（Customize device values）]：ターゲットデバイスで必要なインターフェイス属性の値を設定できます。

b) インターフェイスマッピングをデフォルトのマッピングから変更するには、[マップ済みのインターフェイス（Mapped interface）] ドロップダウンリストからインターフェイスを選択します。

c) EtherChannel の場合は、インターフェイス属性を設定してから [メンバーインターフェイスの追加（Add member interface）] をクリックして、メンバーインターフェイスを追加できます。

EtherChannel のインターフェイス属性は、最初のメンバーインターフェイスのインターフェイス属性に基づいて設定されます。最大 16 個のメンバーインターフェイスを追加できます。

マルチインスタンスモードの Firepower 1100 および 2100 シリーズ デバイス、および Firepower 4100 および 9300 シリーズ デバイス：

これらのデバイスでは、ソースデバイスのインターフェイスをターゲットデバイスのインターフェイスにマッピングする必要があります。

マルチインスタンスモードの Firepower 4100 および 9300 シリーズ デバイスでは、インターフェイスマッピングのみを実行できます。速度、デュプレックス、自動ネゴシエーション、FEC モードなどのインターフェイス属性を設定することはできません。

インターフェイスマッピングをデフォルトのマッピングから変更する場合は、[マップ済みのインターフェイス（Mapped interface）] ドロップダウンリストからインターフェイスを選択します。

[リセット（Reset）] をクリックして、デフォルトのインターフェイスマッピングを設定します。たとえば、ソースデバイスの Ethernet1/1 は、ターゲットデバイスの Ethernet1/1 にマッピングされます。

インターフェイスのタグの状態には次のものがあり得ます。

- [タグ付き（Tagged）]：シャーシ上の物理インターフェイス。
- [タグなし（Untagged）]：サブインターフェイスを持つ、シャーシ上の物理インターフェイス。
- [専用（Dedicated）]：特定のインスタンスに割り当てられ、複数のインスタンス間で共有されないインターフェイス。
- [共有（Shared）]：複数のインスタンスによって共有されるインターフェイス。
- [マネージャアクセス（Manager access）]：データインターフェイスはマネージャ アクセス インターフェイスです。

必要に応じて、[警告を無視（Ignore warning）] チェックボックスをオンにします。

ステップ 8 [次へ（Next）] をクリックします。

ステップ 9 [送信（Submit）] をクリックして移行を開始します。

ステップ 10 [通知（Notifications）] > [タスク（Tasks）] ページに移行ステータスが表示されます。

移行が完了すると、[デバイスモデルの移行（Device Model Migration）] レポートが生成されます。[通知（Notifications）] > [タスク（Tasks）] ページにこのレポートへのリンクが表示されます。

次のタスク

移行が成功したら、次のタスクを完了する必要があります。

- Threat Defense デバイス移行のベストプラクティス （11 ページ）の推奨事項を確認します。
- 設定を検証します。
- 設定をデバイスに展開します。

移行が失敗した場合、ターゲットデバイスは初期状態にロールバックされます。

Threat Defense デバイス移行のベストプラクティス

移行が成功したら、展開前に次のアクションを実行することをお勧めします。

- インターフェイスの IP アドレスがソースデバイスからターゲットデバイスにコピーされます。ソースデバイスが稼働中の場合は、ターゲット デバイス インターフェイスの IP アドレスを変更します
- 必ず、変更した IP アドレスで NAT ポリシーを更新してください。
- 移行後にインターフェイスの速度がデフォルト値に設定される場合は、それらの速度を設定します。
- ターゲットデバイスにデバイス証明書がある場合は、再登録します。
- （任意）リモートブランチ展開の設定を指定します。

  ソースデバイスまたはターゲットデバイスにデータインターフェイスを介したマネージャアクセス権があった場合、移行後にマネージャアクセス権が失われます。ターゲットデバイスのマネージャアクセス設定を更新します。詳細については、『Cisco Secure Firewall Management Center デバイス設定ガイド』またはオンラインヘルプの「管理アクセスインターフェイスの管理からデータへの変更」を参照してください。
- 必要に応じてサイト間 VPN を設定します。これらの設定は、ソースデバイスから移行されません。
- 展開前に展開プレビューを表示します。[展開（Deploy）] > [高度な展開（Advanced Deploy）] を選択し、デバイスの [プレビュー（Preview）] （  ） アイコンをクリックします。
- 正常性モニターでデバイスの正常性をモニターします（[トラブルシューティング（Troubleshooting）] > [正常性（Health）] > [モニター（Monitor）] を選択します）。移行後は、ソースデバイスの正常性ポリシーがターゲットデバイスの正常性ポリシーになります。デバイスに新しい正常性ポリシーを設定することもできます。

  移行後は、デバイスの UUID が移行前後で異なるため、デバイス モニタリング ダッシュボードに一時的に冗長な色付きの行が表示される場合があります。この冗長性は移行時にのみ表示されます。移行から 1 時間経つと、ダッシュボードでメトリックごとに 1 行で表示されるようになります。

【注意】シスコ製品をご使用になる前に、安全上の注意（**www.cisco.com/jp/go/safety_warning/**）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

この資料の記載内容は2008年10月現在のものです。
この資料に記載された仕様は予告なく変更する場合があります。

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255（フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

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。