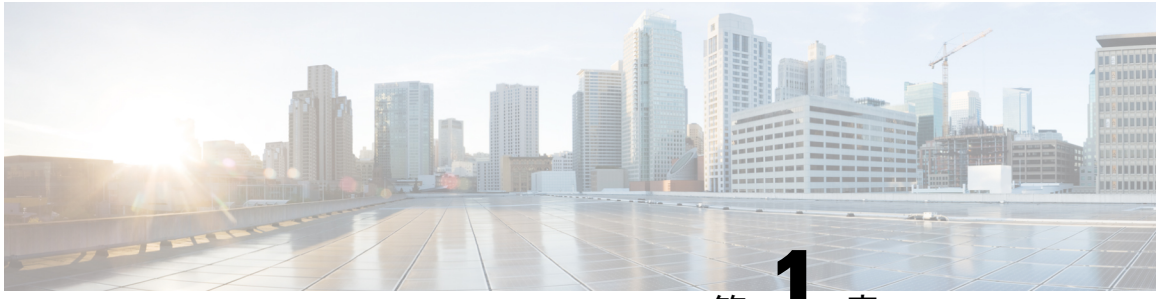
Cisco ASA から Firepower Threat Defense への移行ガイド、バージョン 6.2.1

最終更新：2026 年 4 月 8 日

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/

【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。

目 次



第 1 章

Cisco ASAから Firepower Threat Defense への移行の概要

このガイドでは、シスコの移行ツールを使用して、Cisco ASA から Firepower Threat Defense デバイスへファイアウォールポリシー設定を移行する方法について説明します。

Cisco ASA は、高度なステートフル ファイアウォールと VPN コンセントレータの機能を 1 つの装置に組み合わせたものです。これは、ファイアウォールの業界標準規格です。この製品の詳細については、「http://www.cisco.com/go/asa」を参照してください。

Firepower Threat Defense は、ファイアウォールの進化における次のステップです。これは、統合した NGFW と次世代 IPS 機能を提供します。Firepower ソフトウェアモデルで利用可能な IPS 機能に加え、ファイアウォールとプラットフォーム機能には、サイト間 VPN、堅牢なルーティング、NAT、クラスタリングおよび、アプリケーション可視化やアクセスコントロールにおける各種最適化が含まれます。Firepower Threat Defense は、Cisco Advanced Malware Protection（AMP）と URL フィルタリングもサポートします。この製品の詳細については、「http://www.cisco.com/go/ngfw」を参照してください。

シスコの移行ツールを使用すると、Cisco ASA 構成の特定の機能を Firepower Threat Defense 構成の同等の機能に変換できます。変換後、変換されたポリシーを調整し、追加の Firepower Threat Defense ポリシーを構成して移行を手動で構成することをシスコはお勧めします。

Cisco ASA 構成は、新しい Firepower Threat Defense デバイス、または、更新後、Firepower Threat Defense デバイスとして元の Cisco ASA デバイスに移行できます。

移行プロセスの概要については、https://www.youtube.com/watch?v=N06xXat59B0 のリンクにある動画をご視聴ください。

Firepower Management Center およびサポートされる移行ツール

次の表に、Firepower Management Center のさまざまなバージョンでサポートされている移行ツールを示します。

Firepower Management Center	Cisco ASA から Firepower Threat Defense への移行ツール	FirePOWER 移行ツール
バージョン 6.2、6.2.1、6.2.2	はい	いいえ

Firepower Management Center	Cisco ASA から Firepower Threat Defense への移行ツール	FirePOWER 移行ツール
バージョン 6.2.3 ～ 6.4	はい	はい
バージョン 6.5 以降	いいえ	はい

Cisco ASA から Firepower Threat Defense への移行ツール

Cisco ASA 構成を Firepower Threat Defense 構成 Firepower Management Center に移行するには、「専用の Firepower Management Center Virtual for VMware を準備するために Cisco ASA から Firepower Threat Defense 以降ツールイメージを使用する」を参照してください。この専用の FMC は、デバイスと通信しません。代わりに、移行ツールを使用して、.cfg または .txt 形式の Cisco ASA 構成ファイルを.sfo 形式の Firepower インポートファイルに変換できます。その後、本運用 FMC をインポートします。

移行ツールは、Cisco ASA 構成形式でデータのみを変換できます（つまり、適切な順番の Cisco ASA CLI コマンドのフラットファイル）。移行ツールを使用すると、システムがファイル形式を検証します。たとえば、ファイルには ASA version コマンドを含める必要があります。システムがファイルを検証できない場合、変換は失敗します。

Cisco ASA デバイスの要件

移行ツールは、次の Cisco ASA デバイスから構成データを移行できます。

表 *1* : バージョン *6.2.1* でサポートされているプラットフォームと環境

サポートされるプラットフォーム	対応環境
任意	ASA バージョン 9.8/ASDM バージョン 7.8 ASA バージョン 9.7/ASDM バージョン 7.7 ASA バージョン 9.6/ASDM バージョン 7.6 Cisco ASA バージョン 9.5/ASDMバージョン 7.5 ASA バージョン 9.4/ASDM バージョン 7.4 Cisco ASA バージョン 9.3/ASDMバージョン 7.3 ASA バージョン 9.2/ASDM バージョン 7.2 ASA バージョン 9.1/ASDM バージョン 7.1 Cisco ASA バージョン 9.0/ ASDMバージョン 7.0 ASA バージョン 8.4/ASDM バージョン 6.4

さらに、Cisco ASA デバイスは次の条件を満たしている必要があります。

- シングルコンテキストモードを実行する。
- フェイルオーバーペアの一部である場合のアクティブユニット。
- クラスターの一部である場合のマスターユニット。

Cisco ASA デバイスは、透過的なモードまたはルーテッドモードで実行できます。

Firepower デバイスの要件

このドキュメントで説明する移行プロセスでは、次の Firepower デバイスが必要です。

- 専用の Firepower Management Center Virtual for VMware で実行されている移行ツール。
- 本運用 Firepower Management Center。サポートされているプラットフォームでサポートされている環境を実行する必要があります。

サポートされている Firepower Management Center プラットフォーム	サポートされている Firepower Management Center 環境
Firepower Management Center：FS750、FS1000、FS1500、FS2000、FS2500、FS3500、FS4000、Virtual	移行ツールと同じバージョンである必要があります。

- 本運用 Firepower Threat Defense デバイス（Cisco ASA デバイスで再イメージ可能）。Firepower Threat Defense でサポートされているプラットフォームと環境の一覧については、「Cisco Firepower Compatibility Guide」を参照してください。

ライセンス要件

このドキュメントに記載されている移行された構成を使用するには、Base Firepower Threat Defense ライセンスが必要です。詳細については、「http://www.cisco.com/c/en/us/td/docs/security/firepower/roadmap/firepower-licenseroadmap.html」を参照してください。

Cisco ASA デバイスには、Firepower Threat Defense デバイスとは異なるライセンスが必要なため、移行ツールは、ライセンス情報を移行しません。Firepower Threat Defense デバイス向けに新しいライセンスを購入する必要があります。移行コンテキストのライセンス価格については、セールス担当者にお問い合わせください。

移行でサポートされる Cisco ASA 機能

移行ツールを使用すると、次の Cisco ASA 機能を移行できます。

- 拡張済みアクセスルール（インターフェイスへの割り当ておよびグローバルな割り当てが可能）
- Twice NAT およびネットワークオブジェクト NAT ルール
- ツールが変換する拡張済みアクセスルールと NAT ルールに関連付けられたネットワークオブジェクト/グループまたはサービスオブジェクト/グループ

このツールが Cisco ASA 構成を Firepower Threat Defense 構成に変換する方法の詳細については、「変換マッピングの概要 （19 ページ）」を参照してください。

移行制限

Cisco ASA に移行時は、次の制限に注意します。

Cisco ASA 構成のみ
移行ツールは、Cisco ASA 構成のみを変換します。既存の ASA FirePOWER 構成は変換されません。既存の ASA FirePOWER 構成を Firepower Threat Defense 構成に手動で変換する必要があります。

ACL と ACE の制限
移行ツールが変換できる Cisco ASA 構成ファイルのサイズには具体的な制限はありません。ただし、シスコでは、変換前に Cisco ASA 構成の複雑さとサイズを可能な限り軽減することを推奨しています。複雑なポリシーやルールは、重要なリソースを消費し、パフォーマンスに悪影響を与える可能性があります。Firepower で構成変更をデプロイする際、システムはすべてのルールをまとめて評価し、ターゲット デバイスでネットワーク トラフィックを評価するために使用する拡張基準セットを作成します。それらの基準がターゲットデバイスのリソース（物理メモリ、プロセッサなど）を上回っている場合、そのデバイスに構成をデプロイできません。

適用されるルールとオブジェクトのみ

移行ツールは、インターフェイスに適用される ACL のみを変換します。つまり、Cisco ASA 構成ファイルには、ペアになっている**access-list** および **access-group** コマンドが含まれます。

オブジェクトが、アクティブに適用される ACL または NAT ルールのいずれかに関連付けられている場合、移行ツールは、そのオブジェクトのみを変換します。つまり、Cisco ASA 構成ファイルには、適切に関連付けられている **object**、**access-list**、**access-group** および **nat** コマンドが含まれます。ネットワークオブジェクトとサービスオブジェクトのみを移行できません。

サポートされていない ACL および NAT 構成

移行ツールは、具体的な例外を除き、ほとんどの ACL および NAT 構成をサポートしています。サポートされていない ACL および NAT 構成は次のように処理されます。

[変換するが無効にする（Converts but Disables）] - 移行ツールは次を使用する ACE を完全に変換できません。

- 時間範囲オブジェクト
- 完全修飾ドメイン名（FQDN）
- ローカルユーザーとユーザーグループ
- セキュリティグループ（SGT）オブジェクト
- 送信元ポートと宛て先ポートの両方に対するネストされたサービスグループ

  サポート対象外の要素に対して Firepower の同等の機能がないため、これらのルールの特定の要素は変換できません。これらの場合、ツールは Firepower の同等のものがあるルール要素（ソースネットワークなど）を変換し、Firepower の同等のものがないルール要素（時間範囲など）を除外し、作成される新しいアクセス コントロール ポリシーまたはプレフィルタポリシーでルールを無効にします。

  Cisco ASA 構成から移行されるエグレス ACL ルールは、サポートされないルールです。これらは無効な状態で表示されます。

  無効化された各ルールの場合、システムはルール名に `(unsupported)` と追加し、移行中にルールが無効化された理由を示すコメントもルールに追加します。 で無効化されたルールをインポートしたら、Firepower Management CenterFirepower システムでデプロイメントを成功させるためにルールを手動で編集したり、置き換えたりできます。

[除外（Excludes）] - 移行ツールは、作成するポリシーから、EtherType ACL または WebType ACL、ホストアドレス名のエイリアスを使用する ACE（**name** コマンドで指定）、事前定義された（デフォルト）サービスオブジェクトを使用する ACE の構成を除外します。これらの除外された構成の詳細については、『*CLI* ブック *2*：*Cisco ASA* シリーズファイアウォール *CLI* 構成ガイド』または『*ASDM* ブック *2*：*Cisco ASA* シリーズファイアウォール *ASDM* 構成ガイド』を参照してください。

サポートされていないその他の Cisco ASA 構成

移行ツールは、このドキュメントで指定されていないCisco ASA機能の移行をサポートしていません。このツールは、Cisco ASA 構成ファイルを処理する際に、サポートされていない機能の構成データを無視します。

移行のチェックリスト

移行ツールを使用する前に、次を確認します。

- Cisco ASAデバイスが移行のすべての条件を満たしているかを確認するには、「Cisco ASA デバイスの要件 （2 ページ）」を参照してください。
- Cisco ASA 構成ファイルは、.cfg または .txt のいずれかの形式です。
- Cisco ASA 構成ファイルには、サポートされている構成のみが含まれます。移行に必要な制限を満たしていることを確認するには、「移行制限 （4 ページ）」を参照してください。
- Cisco ASA構成ファイルには、有効なCisco ASA CLI構成のみを含めます。続行する前に、誤ったコマンドまたは不完全なコマンドを修正します。ファイルに無効な構成が含まれている場合、移行は失敗します。
- 変換された Cisco ASA 構成ファイルをインポートするには、Firepower Management Center を構成を変換する移行ツールと同じバージョンで実行する必要があります。この制限は、メジャーリリースとマイナーリリースの両方で適用されます。たとえば、移行ツールがバージョン6.2.1を実行していて、ファイルをインポートするFirepower Management Centerがバージョン6.1.0.2を実行している場合、変換したCisco ASA構成ファイルをインポートする前に、Firepower Management Center 6.2.1 にアップグレードする必要があります。

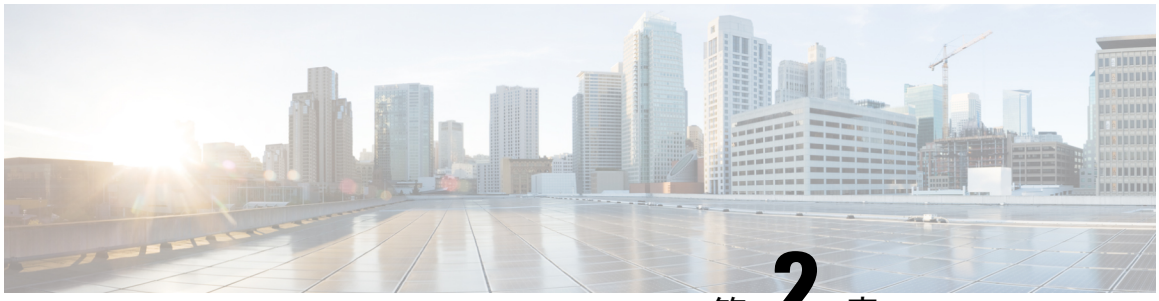
表記法

このドキュメントでは、Firepower Threat Defense 構成に変換された Cisco ASA 構成の例を示します。これらの例のほとんどの列は、関連するルールエディタまたは Firepower Management Centerのオブジェクトマネージャのコンポーネントに直接マップします。次の表に、Firepower UI コンポーネントに直接マッピングされない列を示します。

表 *2:* 間接値を使用する列

列	値	説明
有効化	True/False	アクセスコントロールまたはプレフィルタルールで、**[有効化（Enabled）]** チェックボックスをオンにするかオフにするかを指定します。

列	値	説明
アクション	同等に許可	次のように、変換時に選択した選択肢に応じて、決定される値を指定します。 • アクセスルールをアクセスコントロールルールに変換する場合は、この値を **[許可（Allow）]** または **[True]** のどちらにするかも選択します。 • アクセスルールをプレフィルタルールに変換する場合は、この値を **[許可Fastpath]** または **[分析（Analyze）]** のどちらにするかも選択します。
ドメイン	なし	変換時点では、このフィールドは空欄です。これは、システムが、本運用 Firepower Management Center にインポートするまで、システムがドメインを割り当てないためです。インポート時に、システムは、変換された構成をインポートするドメインに基づいてドメインを割り当てます。
オーバーライド	True/False	オブジェクトで **[オーバーライドを許可（Allow Overrides）]** チェックボックスをオンにするかオフにするかを指定します。



第 2 章

Firepower Threat Defense 構成に Cisco ASA 構成を移行する

移行に向けて Cisco ASA を準備する

手順

ステップ 1 Cisco ASA デバイスが構成の移行要件を満たしているかどうかを確認するには、「Cisco ASA デバイスの要件 （2 ページ）」を参照してください。

ステップ 2 エクスポートするアクセス制御リスト（ACL）と NAT ポリシーを特定します。

ステップ 3 できるだけ多くの重要でないルールを構成からプルーニングします。シスコでは、変換前に Cisco ASA 構成の複雑さとサイズを可能な限り軽減することを推奨しています。ACL に含まれているエントリの数を確認するには：

```
show access-list acl_name | i elements
```

移行ツールのインストール

⚠

注意 本運用 Firepower Management Center に移行ツールをインストール**しないでください**。このツールの使用は、本運用デバイスではサポートされていません。移行ツールをインストールしたら、指名された Firepower Management Center を再イメージすることによってのみツールをアンインストールできます。

手順

ステップ 1 サポートから次のいずれかのイメージをダウンロードします。

- Firepower Management Center Virtual for VMware
- Firepower Management Center Virtual for KVM

ステップ 2 該当するガイドの説明に従って、イメージファイルを使用して指名された Firepower Management Center Virtual をインストールします。

- 『*VMware* 導入向け *Cisco Firepower Management Center Virtual* クイックスタートガイド』
- *Cisco Firepower Management Center Virtual for KVM Deployment* クイックスタートガイド

ステップ 3 `admin` ユーザー名を使用して`ssh` 経由で Firepower Management Center に接続します。

ステップ 4 Root Shell にログインします。

```
sudo su -
```

ステップ 5 次のコマンドを実行します。

```
enableMigrationTool.pl
```

（注）
プロセスが完了したら、Firepower Management Center で実行中の Web インターフェイスセッションを更新して、移行ツールを使用します。

Cisco ASA 構成ファイルを保存する

移行ツールは、Cisco ASA 構成ファイルを .cfg または .txt 形式に変換できます。

手順

ステップ 1 設定を保存します。

この構成を保存するために使用するコマンドは、Cisco ASA デバイスのバージョンによって異なる場合があります。詳細については、http://www.cisco.com/c/en/us/td/docs/security/asa/roadmap/asaroadmap.html#pgfId-126642 の Cisco ASA のドキュメントロードマップに一覧されている該当するバージョンの『Cisco ASA 構成ガイド』を参照してください。

ステップ 2 保存した構成ファイルを、移行ツールからアクセス可能な場所（たとえば、ローカルコンピュータまたはネットワーク上の共有ドライブ）に転送します。

Cisco ASA 構成ファイルを変換する

次の手順を実行して、Cisco ASA 構成ファイル（.cfg または .txt）を Firepower 構成ファイル（.sfo）に変換します。

注意 移行ツールの UI は、Firepower Management Center UI の拡張機能です。ただし、この手順で説明されている機能のみを実行できます。

手順

ステップ 1 ブラウザで `https://hostname/` にアクセスします。*hostname* 要素は、移行ツールがインストールされている専用の Firepower Management Center Virtual のホスト名に対応しています。

ステップ 2 `admin` ユーザーとしてログインします。

ステップ 3 **[System]** > **[Tools]** > **[Import/Export]** を選択します。

ステップ 4 [パッケージのアップロード（Upload Package）] をクリックします。

ステップ 5 **[参照（Browse）]** をクリックし、Cisco ASA からエクスポートした構成ファイルを選択します。

ステップ 6 **[次へ（Next）]** をクリックします。

ステップ 7 アクセスルールの変換時にシステムが使用するポリシーを選択します。

- **プレフィルタポリシー** - アクセスルールをプレフィルタルールに変換します。
- **アクセス コントロール ポリシー** - アクセスルールをアクセスコントロールルールに変換します。

ステップ 8 **プレフィルタポリシー**を選択した場合、Permit アクションを持つアクセスルールに対して、システムに割り当てるアクションを選択します。

- **Fastpath**—アクセスコントロール、ID 要件、レート制限を含む、すべての詳細な検査および制御から一致するトラフィックを免除します。トンネルを高速パス化すると、すべてのカプセル化された接続が高速パス化されます。
- **分析** - トラフィックが残りのアクセスコントロールによって引き続き分析されることを許可します。アクセス制御および関連するディープインスペクションによって渡された場合、このトラフィックはレート制限も行われる場合があります。

ステップ 9 **アクセス コントロール ポリシー**を選択した場合、Permit アクションを持つルールに対して、システムに割り当てるアクションを選択します。

- **信頼** - ディープインスペクションやネットワーク検出をせずにトラフィックを通過させます。信頼されたトラフィックは、アイデンティティポリシーによって強制される認証要件、およびレート制限が適用され続けます。
- **許可** - 一致するトラフィックの通過を許可します。許可されるトラフィックには、アイデンティティ ポリシーによって強制される認証要件が適用され続けます。レート制限、および詳細検査（設定されている場合）も適用され続けます。

ステップ 10 **[次へ（Next）]** を選択します。

システムは、移行をタスクとしてキューします。タスクの状態は、メッセージセンタ - で表示できます。

ステップ 11 [システム ステータス（System Status）] アイコンをクリックして、メッセージ センターを表示します。

ステップ 12 **[タスク（Tasks）]** タブをクリックします。

移行タスクは最上位のメッセージとして表示されます。これは、中間 Firepower Management Center で実行できるタスクが移行ツールのタスクに限られているためです。

ステップ 13 移行が失敗した場合は、該当するログでエラーメッセージを確認します。詳細については、「変換エラーをトラブルシューティングする （13 ページ）」を参照してください。

ステップ 14 移行が成功した場合：

- **[.sfo をダウンロード（Download .sfo）]** をクリックして、ローカルコンピュータに変換したファイルをコピーします。
- **[移行レポート（Migration Report）]** をクリックすると、移行レポートを表示できます。

ステップ 15 移行レポートを確認します。

移行レポートには、Firepower Threat Defense 構成に変換できた Cisco ASA 構成および正常に変換できなかった Cisco ASA 構成が要約されています。正常に変換できなかった構成として、次が挙げられます。

- Firepower システムでサポートされていない Cisco ASA 構成
- Firepower システム（Firepower に相当する機能がある）でサポートされているが、移行ツールが変換しない Cisco ASA 構成

Firepower に相当する機能があるにもかかわらず変換に失敗した構成については、変換済みポリシーを本運用Firepower Management Center にインポートした後で手動で追加します。

変換エラーをトラブルシューティングする

専用 Firepower Management Center で変換が失敗した場合、移行ツールは、ローカルコンピュータにダウンロードできるトラブルシューティング ファイルにエラーデータを記録します。

手順

ステップ 1 **[System]** > **[Health]** > **[Monitor]**を選択します。

ステップ 2 アプライアンスリストの **[アプライアンス（Appliance）]** 列で、専用の Firepower Management Center の名前をクリックします。

ステップ 3 [トラブルシューティング ファイルの生成（Generate Troubleshooting Files）] をクリックします。

ステップ 4 **[すべてのデータ（All Data）]** チェックボックスをオンにします。

ステップ 5 [生成（Generate）] をクリックします。
システムはトラブルシューティング ファイルの生成をタスクとしてキューします。

ステップ 6 メッセージセンターを表示するとタスクの進捗状況を追跡できます。

ステップ 7 システムがトラブルシューティング ファイルを生成し、タスク状態が [完了（Completed）] に変ったら、**[クリックして生成されたファイルを取得（Click to retrieve generated files）]** をクリックします。

ステップ 8 圧縮ファイルをローカルコンピューターに保存して、ファイルを解凍します。

ステップ 9 次のファイルでエラーメッセージを確認します。

- `dir-archives/var-log/action_queue.log.#.gz`
- `dir-archives/var-log/mojo/mojo.log.#`
- `dir-archives/var-opt-CSCOpx-MDC-log-operation/usmsharedsvcs.log`
- `dir-archives/var-opt-CSCOpx-MDC-log-operation/vmsbesvcs.log`
- `dir-archives/var-opt-CSCOpx-MDC-log-operation/vmssharedsvcs.log`

変換した Cisco ASA 構成をインポートする

Firepower Management Center のマルチドメインデプロイメントで、システムは、変換した Cisco ASA 構成をそれをインポートするドメインに変換します。インポート時に、システムは、変換したオブジェクトの **[ドメイン（Domain）]** フィールドに値を入力します。

手順

ステップ 1 本運用 Firepower Management Center で、**[[System]** > **[Tools]** > **[Import/Export]]** を選択します。

ステップ 2 [パッケージのアップロード（Upload Package）] をクリックします。

ステップ 3 **[ファイルを選択（Choose File）]** をクリックし、[参照（browse）] を使用して、ローカルコンピュータ上の適切な .sfo ファイルを選択します。

ステップ 4 **[アップロード（Upload）]**をクリックします。

ステップ 5 インポートするポリシーを選択します。ポリシーには、以前の移行で選択した選択肢に応じて、アクセス コントロール ポリシー、プレフィルタポリシー、または NAT ポリシーが含まれる場合があります。

ステップ 6 **[インポート（Import）]** をクリックします。
システムはファイルを分析し、[競合をインポート（Import Conflict）] ページを表示します。

ステップ 7 [競合をインポート（Import Conflict）] ページで、次の手順を実行します。

- 構成の競合を解決します。Firepower Management Center Configuration Guide の「競合解決をインポート」を参照してください。
- 元の Cisco ASA 構成でインターフェイスごとにルールがグループ化されていた方法を複製するか、そのグループの関連付けを新しいものに置き換えます。これを行うには、次のように、アクセスコントロールルールをセキュリティゾーンに割り当て、プレフィルタルールまたは NAT ルールをインターフェイスグループに割り当てる必要があります。

タイプ	ソース	次の場合、このゾーンまたはグループを選択します。
システム生成のセキュリティゾーン/インターフェイスグループ	移行ツールは、変換中にこのセキュリティゾーン/インターフェイスグループを自動作成します。	元の Cisco ASA 構成のインターフェイスごとにルールがグループ化された方法を複製します。
変換された Cisco ASA 構成をインポートする前に作成されたセキュリティゾーン/インターフェイスグループ	変換された Cisco ASA 構成をインポートする前にこのセキュリティゾーン/インターフェイスグループを作成します。	ルールを、Firepower Management Center ですでに既存するセキュリティゾーン/インターフェイスグループに関連付けます。
インポートプロセス中にその場で作成されたセキュリティゾーン/インターフェイスグループ	ルール一式の横にあるドロップダウンリストで、[新規...（New...）] を選択して、このセキュリティゾーン/インターフェイスグループを作成します。	ルールを、Firepower Management Center の新しいセキュリティゾーン/インターフェイスグループに関連付けます。

ヒント
ルール一致機の横にある矢印を使用して、セットに関する追加情報を展開します。

（注）
移行ツールはインターフェイス構成を変換しません。デバイスを手動で追加し、変換された Cisco ASA 構成をインポートした後、それらのデバイスのインターフェイスを構成する必要があります。ただし、このインポート手順により、ACL または NAT ポリシーと単一のエンティティ（セキュリティゾーンまたはインターフェイスグループ）との関連付けを保持し、新しい Firepower Threat Defense デバイスのインターフェイスとすぐに関連付けることができます。セキュリティゾーン/インターフェイスグループとインターネットへの関連付けの詳細については、「移行したポリシーを構成する （16 ページ）」を参照してください。

ステップ 8 **[インポート（Import）]** をクリックします。
インポートが完了すると、システムにメッセージセンターに誘導するメッセージが表示されます。

ステップ 9 [システム状態（System Status）] アイコンをクリックして、メッセージセンターを表示します。

ステップ 10 [タスク（Tasks）] タブをクリックします。

ステップ 11 インポートレポートをダウンロードするには、インポートタスク内のリンクをクリックします。

Firepower Threat Defense をインストールする

手順

次の表に記載されている適切なクイックスタートガイドを使用して Firepower Threat Defense をインストールします。

（注）
クイックスタートガイドの手順には、デバイスへの新しいイメージのインストールが記載されているため、同じ手順を使用して、新しいデバイスに Firepower Threat Defense をインストールしたり、Firepower Threat Defense に元の Cisco ASA を再イメージすることもできます。

プラットフォーム	クイック スタート ガイド
Firepower Threat Defense：Cisco ASA 5506-X、Cisco ASA 5506H-X、Cisco ASA 5506W-X、Cisco ASA 5508-X、Cisco ASA 5512-X、Cisco ASA 5515-X、Cisco ASA 5516-X、Cisco ASA 5525-X、Cisco ASA 5545-X、Cisco ASA 5555-X	http://www.cisco.com/c/en/us/td/docs/security/firepower/quick_start/5500X/ftd-55xx-X-qsg.html
Threat Defense を搭載した Firepower 4100 シリーズ：4110、4120、および 4140	http://www.cisco.com/c/en/us/td/docs/security/firepower/quick_start/fp4100/ftd-4100-qsg.html
Threat Defense を搭載した Firepower 9300	http://www.cisco.com/c/en/us/td/docs/security/firepower/quick_start/fp9300/ftd-9300-qsg.html
Firepower Threat Defense Virtual：VMware	http://www.cisco.com/c/en/us/td/docs/security/firepower/quick_start/vmware/ftdv/ftdv-vmware-qsg.html
Firepower Threat Defense Virtual：AWS Cloud	http://www.cisco.com/c/en/us/td/docs/security/firepower/quick_start/aws/ftdv-aws-qsg.html

移行したポリシーを構成する

この手順では、Firepower Management Center に移行したポリシーを構成するための大まかな手順を説明します。各手順の詳細については、Firepower Management Center Configuration Guide に記載されている関連手順を参照してください。

手順

ステップ 1 Firepower Threat Defense デバイスのインターフェイスを変換プロセス中に作成されたインターフェイスグループのセキュリティゾーンに割り当てます。

ステップ 2 Cisco ASA アクセスルールをアクセス コントロール ポリシーに移行する場合：

- 必要に応じて、無効なルールを有効または無効にし、ポリシーのルールを調整、追加、削除できます。またルールの順番を変更できます。たとえば、別の送信元プロトコルおよび接続先プロトコルまたは複数のプロトコルを指定するルールを変更する場合は、「複数のプロトコルを指定するアクセスルール （30 ページ）」を参照してください。
- 必要に応じて、ツールが変換しない Cisco ASA パラメータに Firepower と同等の機能を構成します。

Access Rule パラメータ	Access Control Rule パラメータ
ユーザー	選択されたユーザー条件
セキュリティグループ（送信元）	カスタム SGT 条件

- アクセス コントロール ポリシーを Firepower Threat Defense デバイスに割り当てます。

ステップ 3 Cisco ASA アクセスルールをプレフィルタポリシーに移行する場合：

- 必要に応じて、無効なルールを有効または無効にし、ポリシーのルールを調整、追加、削除できます。またルールの順番を変更できます。たとえば、別の送信元プロトコルおよび接続先プロトコルまたは複数のプロトコルを指定するルールを変更する場合は、「複数のプロトコルを指定するアクセスルール （30 ページ）」を参照してください。
- 必要に応じて、ツールが変換しない Cisco ASA パラメータに Firepower と同等の機能を構成します。

Access Rule パラメータ	Prefilter Rule パラメータ
ユーザー	選択されたユーザー条件
セキュリティグループ（送信元）	カスタム SGT 条件

- 変換中にシステムが作成するアクセス コントロール ポリシーを構成するか、プレフィルタポリシーを別のアクセス コントロール ポリシーに関連付けます。

警告
移行ツールは、移行済みアクセス コントロール ポリシーのデフォルトアクションを **[すべてのトラフィックをブロック（Block All Traffic）]** に設定します。これは、ACL における暗黙の拒否と同等の

設定です。移行したプレフィルタポリシーがある別のアクセスコントロールポリシーを使用する場合は、デフォルトの **[すべてのトラフィックをブロック（Block All Traffic）]** に設定することを検討します。そうしないと、セキュリティホールが生じる場合があります。

- 関連するアクセス コントロール ポリシーを Firepower Threat Defense デバイスに割り当てます。

ステップ 4 NAT ポリシーを移行した場合：

- 必要に応じて、無効なルールを有効または無効にし、ポリシーのルールを調整、追加、削除できます。またルールの順番を変更できます。
- NAT ポリシーを Firepower Threat Defense デバイスに割り当てます。

ステップ 5 必要に応じて、アプリケーションの可視性と制御、侵入保護、URL フィルタ処理、Cisco Advanced Malware Protection（AMP）を含む NGFW 機能を構成します。

ステップ 6 設定変更を展開します。設定変更をデプロイする （17 ページ）を参照してください。

設定変更をデプロイする

移行した構成をデプロイするには、次の手順を実行します。詳細については、『*Firepower Management Center* 構成ガイド』の「構成変更をデプロイする」を参照してください。

手順

ステップ 1 FMC メニュー バーで、[展開（Deploy）] をクリックします。

[ポリシーの展開（Deploy Policies）] ダイアログに、設定の期限が切れているデバイスがリストされます。ダイアログの上部の [バージョン（Version）] は、最後に設定変更を行った時期を示します。デバイステーブルの [現在のバージョン（Current Version）] 列は、変更を各デバイスに最後に展開した時期を示します。

ステップ 2 設定変更を展開するデバイスを特定して選択します。

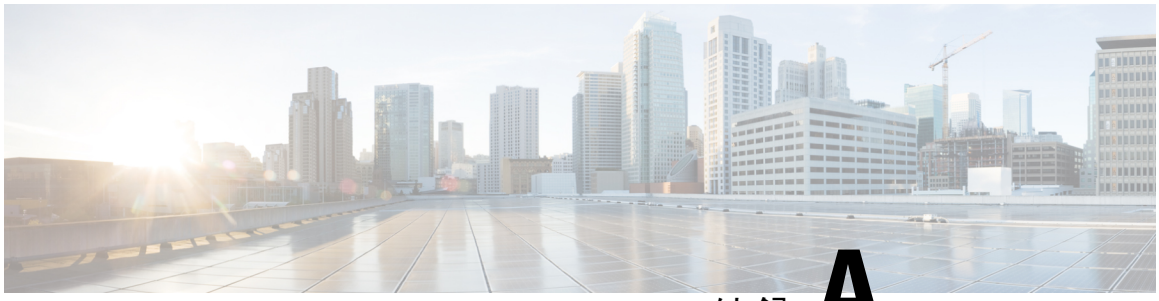
- [ソート（Sort）]：列ヘッダーをクリックすることで、デバイスリストをソートします。
- [展開（Expand）]：デバイスリストを展開して、展開される設定変更を表示するには、**プラス記号**をクリックします。システムは、期限切れのポリシーを**インデックス**でマーキングします。
- [フィルタ（Filter）]：デバイスリストをフィルタリングします。ディスプレイの列ヘッダーの右上隅にある矢印をクリックし、[フィルタ（Filters）] テキストボックスにテキストを入力し、Enter を押します。チェックボックスをオンまたはオフにして、フィルタをアクティブまたは非アクティブにします。
- 調整：マウスカーソルを列ヘッダーの上に移動し、列をドラッグアンドドロップして希望の順序にします。

ステップ 3 [Deploy] をクリックします。

ステップ 4 展開する変更に関するエラーや警告がシステムによって識別された場合は、[要求された展開のエラーと警告（Errors and Warnings for Requested Deployment）] ウィンドウにその内容が表示されます。

次の選択肢があります。

- [続行（Proceed）]：警告状態を解決せずに展開を続行します。システムがエラーを確認した場合は続行できません。
- [キャンセル（Cancel）]：展開せずに終了します。エラーおよび警告状態を解決し、設定の再展開を試行します。



付録 A

変換マッピング

次のトピックでは、移行ツールが Cisco ASA 構成を Firepower Threat Defense 構成に変換する方法について説明します。

変換マッピングの概要

以降ツールは、次のように Cisco ASA 構成を Firepower Threat Defense 構成に変換します。

表 *3*: 変換マッピングの概要

エンティティ	ASA の設定	Firepower Threat Defense の設定
ネットワーク オブジェクト	ネットワーク オブジェクト ネットワーク オブジェクト グループ ネストされたネットワーク オブジェクト グループ	ネットワーク オブジェクト ネットワーク オブジェクト グループ ネストされたネットワーク オブジェクト グループ

エンティティ	ASA の設定	Firepower Threat Defense の設定
サービス オブジェクト	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	複数ポートオブジェクト 複数ポートオブジェクトグループ 複数またはフラット化されたポートオブジェクトグループ 詳細については、「サービスオブジェクトとサービスグループの変換（36ページ）」を参照してください。
アクセスルール	アクセスルール	アクセス コントロール ポリシーまたはプレフィルタポリシー（選択されたもの）
NAT ルール	Twice NAT ルール ネットワークオブジェクト NAT ルール	手動 NAT ルール 自動 NAT ルール

変換した構成の命名規則

移行ツールは、Cisco ASA アクセスルール、NAT ルールおよび、関連オブジェクトを Firepower Threat Defense と同等のものに変換する際に後述されている命名規則を使用します。

オブジェクトとオブジェクトグループ名

オブジェクトとオブジェクトグループを変換する場合、移行ツールは Cisco ASA 構成ファイルからのオブジェクトとグループ名を保持します。

次に例を示します。

```
object network obj1
 host 1.2.3.4
object network obj2
 range 1.2.3.7 1.2.3.10
 subnet 10.83.0.0 255.255.0.0
object-group network obj_group1
 network-object object obj1
 network-object object obj2
```

このツールは、この構成を `obj1` および `obj2` という名前のネットワークオブジェクトに、`obj_group1` という名前のネットワーク オブジェクト グループに変換します。

サービスオブジェクトおよびサービスグループをポートオブジェクトおよびポートオブジェクトグループに変換する際、ツールは、特定の場合に、次の拡張子を元のオブジェクトまたはグループ名に付加する場合があります。

表 *4*: 変換されるサービスオブジェクトとグループの拡張子

内線	不可する理由
`_dst`	接続元ポートと宛て先ポートがあるサービスオブジェクトを2つのポートオブジェクトに分割します。システムは、この拡張子を使用するサービスオブジェクトに付加して、変換された宛て先ポートデータを保存します。詳細については、「送信元ポートと宛て先ポートを含むサービスオブジェクト （39 ページ）」を参照してください。
`_src`	接続元ポートと宛て先ポートがあるサービスオブジェクトを2つのポートオブジェクトに分割します。システムは、この拡張子を使用するサービスオブジェクトに付加して、変換された送信元ポートデータを保存します。詳細については、を参照してください。
`_#`	ネストされたサービスグループを変換します。「ネストされたサービスグループの変換 （41 ページ）」を参照してください。

ポリシー名

Cisco ASA 構成ファイルには、Cisco ASA に対してホスト名を指定する `hostname` パラメータが含まれます。移行ツールは、この値を使用して、ファイル変換時に作成するポリシーに名前を付けます。

- アクセス コントロール ポリシー — *hostname*-AccessPolicy-*conversion_date*
- プレフィルタポリシー — *hostname*-PrefilterPolicy-*conversion_date*
- NAT ポリシー — *hostname*-NATPolicy-*conversion_date*

ルール名

変換されたアクセスコントロール、プレフィルタ、および NAT ルールの場合、システムは次の形式を使用して新しい各ルールに名前を付けます。

ACL_name-#rule_index

値は次のとおりです。

- *ACL_name* —ルールが属していた ACL の名前。
- *rule_index* — ACL 内の他のルールに対して、このルールがどの順序で変換されたかを示すシステム生成の整数。

次に例を示します。

```
acl1#1
```

システムが、サービスオブジェクト変換中に単一アクセスルールを複数ルールに拡張する必要がある場合は、システムは拡張子を付加します。

ACL_name#rule_index_sub_index

ここで、付加された # は、展開されたシーケンス内の新しいルールの位置を表します。

次に例を示します。

```
acl1#1_1

acl1#1_2
```

ルール名が 30 文字を超えているとシステムが判断した場合、システムはACL 名を短縮し、圧縮された名前をチルダ（~）で終了します。

```
ACL Name~#rule index
```

たとえば、元の ACL 名が `accesslist_for_outbound_traffic` の場合、システムは ACL 名を次のように切り捨てます。

```
accesslist_for_outbound_tr~#1
```

セキュリティゾーンとインターフェイスグループ名

移行ツールが、Cisco ASA 構成ファイルで `access-group` コマンドを変換する際、ツールは、（変換中の選択肢に応じて）セキュリティゾーンまたはインターフェイスグループのいずれかを作成してコマンドのイグレスおよびエングレス情報をキャプチャします。次の形式を使用して、これらの新しいセキュリティゾーンまたはインターフェイスグループに名前を付けます。

*ACL_name_interface_name_direction_keyword*_zone

値は次のとおりです。

- *ACL_name* — `access-group` コマンドの ACL の名前。
- *interface_name* — `access-group` コマンドのインターフェイスの名前。
- *direction_keyword* — `access-group` コマンドの direction キーワード（`in` または `out`）。

次に例を示します。

```
access-list acp1 permit tcp any host 209.165.201.3 eq 80
access-group acp1 in interface outside
```

ツールは、この構成を `acp1_outside_in_zone` という名前のセキュリティゾーンまたはインターフェイスグループに変換します。

Firepowerオブジェクトおよびオブジェクトグループの固有フィールド

Firepower ネットワークおよびポートオブジェクト/グループには、Cisco ASA オブジェクトとグループに存在しないフィールドがいくつかあります。移行ツールは、変換されたネットワークおよびポートのオブジェクト/グループのこれらの Firepower 固有フィールドに、次のデフォルト値を入力します。

表 *5 : Firepower* オブジェクト/グループの固有フィールドのデフォルト値

Firepowerオブジェクト/グループのフィールド	変換された Cisco ASA オブジェクト/グループのデフォルト値
ドメイン	なし
オーバーライド	False

これらのデフォルト値の詳細については、「表記法 （6 ページ）」を参照してください。

アクセスルールの変換

移行ツールは、移行中の選択肢に応じて、Cisco ASA アクセスルールを、アクセスコントロールルールまたはプレフィルタルールのいずれかに変換できます。

アクセスルールをアクセスコントロールルールに変換する

Cisco ASA アクセスルールを Firepower Threat Defense アクセスコントロールルールに変換する場合：

- システムは、変換されたルールを、アクセス コントロール ポリシーの**デフォルト**ルールセクションに追加します。
- システムでは、[説明（Description）] フィールドの内容は、ルールの **[コメント履歴（Comments History）]** のエントリとして保持されます。
- システムは、ルールが変換されたことを示すエントリを、**[コメント履歴（Comments History）]** に追加します。
- システムはアクセスコントロールルールの**アクション**を次のように設定します。

アクセスルールのアクション	アクセスコントロールルールのアクション
許可	移行中に選択した選択肢に応じて、**[許可（Allow）]**または **[信頼する（Trust）]**
拒否	ブロック

- システムは、アクセスコントロールルールの**送信元ゾーン**および**接続先ゾーン**を次のように設定します。

ACL タイプ	送信元ゾーン	宛先ゾーン
グローバル（すべてのインターフェイスに適用）	任意	任意

ACL タイプ	送信元ゾーン	宛先ゾーン
特定のインターフェイスに適用れる	インポート時に選択するセキュリティゾーン	任意

- アクセスルールが非アクティブの場合、ツールは、そのルールを無効なアクセスコントロールルールに変換します。

移行ツールは、次のデフォルトパラメータを使用して変換したルールをアクセス コントロール ポリシーに変換します。

- システムは、新しいアクセス コントロール ポリシーのデフォルトアクションを**[すべてのトラフィックをブロック（Block All Traffic）]** に設定します。
- システムは、アクセス コントロール ポリシーをデフォルトのプレフィルタポリシーに関連付けます。

アクセス コントロール ルール フィールドにマッピングされたアクセスルールフィールド

移行ツールは、次の表に示すように、Cisco ASA アクセスルールのフィールドを Firepower Threat Defense アクセスコントロールルールのフィールドに変換します。

（注）

- 列 1 のフィールド名（Cisco ASA アクセスルールフィールド）は、ASDM インターフェイスのフィールドラベルに対応しています。
- 列 2 のフィールド名（Firepower アクセス コントロール ルール フィールド）は、Firepower Management Center インターフェイスのフィールドラベルに対応しています。

表 *6 : Firepower* アクセス コントロール ルール フィールドにマッピングされた *Cisco ASA* アクセスルールフィールド

Cisco ASA アクセスルールフィールド	Firepower アクセス コントロール ルール フィールド
インターフェイス	同等のフィールドなし
アクション	アクション
ソース	送信元ネットワーク
ユーザー	変換しない、選択されたユーザー条件と同等
セキュリティグループ（送信元）	変換なし、カスタム SGT 条件と同等
接続先	接続先ネットワーク
セキュリティグループ（宛て先）	同等のフィールドなし

Cisco ASA アクセスルールフィールド	Firepower アクセス コントロール ルール フィールド
サービス	選択した宛て先ポート、事前定義サービスが指定されている場合、変換しない
説明	備考
ロギング/ロギングレベルを有効にする	接続の開始時および接続の終了時にログに記録します。ACE のロギングが、デフォルト以外のロギングレベルで有効な場合、ツールは、接続の開始および切断時の両方で変換されたルールの接続ロギングを有効にします。ACE のロギングが、デフォルトレベルで有効な場合、釣るは、変換されたルールの接続路銀府を無効にします。
ロギング間隔	同等のフィールドなし
ルールの有効化	有効
トラフィックの方向	同等のフィールドなし
送信元サービス	選択した接続元ポート、事前定義サービスが指定されている場合、変換しない
時間範囲	同等のフィールドなし

（注） ACE にログレベルが割り当てられたログオプションがある場合、ACE は有効になります。ログレベルの内 ACE は、無効とみなされます。ACE が、デフォルトのログレベルに関連付けられている場合、ACE ログレベルは無効になります。

アクセスコントロールルール固有のフィールド

Firepower Threat Defense アクセス コントロール ルールには、Cisco ASA アクセスルールに存在しないフィールドがいくつか含まれます。移行ツールは、変換されたアクセスコントロールルールのこれらの Firepower 固有フィールドに、次のデフォルト値を入力します。

表 7: アクセスコントロールルールの固有フィールドのデフォルト値

アクセス コントロール ルール フィールド	変換されたアクセスルールのデフォルト値
名前	システム生成（変換した構成の命名規則 （20 ページ） を参照）

アクセス コントロール ルール フィールド	変換されたアクセスルールのデフォルト値
送信元ゾーン	• ACLがグローバルに適用される場合、[任意（Any）] • ACL が特定のインターフェイスに適用される場合、変換中にツールが作成するセキュリティゾーン
宛先ゾーン	任意（すべてのアクセスコントロールルールのデフォルト値）
選択された VLAN タグ	デフォルト（インポート後に条件を手動で追加できます）
選択したアプリケーションとフィルタ	デフォルト（インポート後に条件を手動で追加できます）
選択された URL	デフォルト（インポート後に条件を手動で追加できます）

アクセスルールをプレフィルタルールに変換する

Cisco ASA アクセスルールを Firepower Threat Defense プレフィルタルールに変換する場合：

- システムでは、[説明（Description）] フィールドの内容は、ルールの **[コメント履歴（Comments History）]** のエントリとして保持されます。
- ルールが変換されたことを示すエントリを、**[コメント履歴（Comments History）]** に追加します。
- システムは、プレフィルタルールの **[アクション（Action）]** を次のように設定します。

アクセスルールのアクション	プレフィルタルールのアクション
許可	移行中に選択した選択肢に応じて、**[fastpath]** または **[分析（Analyze）]**
拒否	ブロック

- システムは、プレフィルタルールの **[送信元インターフェイスオブジェクト（Source Interface Objects）]** と **[接続先インターフェイスオブジェクト（Destination Interface Objects）]** を次のように設定します。

ACL タイプ	送信元インターフェイス オブジェクト	接続先インターフェイス オブジェクト
グローバル（すべてのインターフェイスに適用）	任意	任意

ACL タイプ	送信元インターフェイス オブジェクト	接続先インターフェイス オブジェクト
特定のインターフェイスに適用れる	インポート時に選択するインターフェイスグループ	任意

- アクセスルールが非アクティブの場合、ツールは、そのルールを無効なプレフィルタルールに変換します。

移行ツールは、次のデフォルトパラメータを使用して変換したルールをプレフィルタポリシーに変換します。

- システムは、新しいプレフィルタポリシーのデフォルトアクションを **[すべてのトンネルトラフィックを分析（Analyze All Tunnel Traffic）]** に設定します。
- システムでは、プレフィルタポリシーと同じ名前のアクセス コントロール ポリシーが作成され、プレフィルタポリシーがそのアクセス コントロール ポリシーに関連付けられます。システムは、新しいアクセス コントロール ポリシーのデフォルトアクションを **[すべてのトラフィックをブロック（Block All Traffic）]** に設定します。

プレフィルタ ルール フィールドにマッピングされたアクセスルールフィールド

移行ツールは、次の表に示すように、Cisco ASA アクセスルールのフィールドを Firepower Threat Defense プレフィルタルールのフィールドに変換します。

（注）

- 列 1 のフィールド名（Cisco ASA アクセスルールフィールド）は、ASDM インターフェイスのフィールドラベルに対応しています。
- 列 2 のフィールド名（Firepower プレフィルタ ルール フィールド）は、Firepower Management Center インターフェイスのフィールドラベルに対応しています。

表 *8 : Firepower* プレフィルタ ルール フィールドにマッピングされた *Cisco ASA* アクセスルールフィールド

Cisco ASA アクセスルールフィールド	Firepower プレフィルタ ルール フィールド
インターフェイス	同等のフィールドなし
ルールの有効化	有効
アクション	アクション
ソース	送信元ネットワーク
ユーザー	同等のフィールドなし
セキュリティグループ（送信元）	同等のフィールドなし
接続先	接続先ネットワーク

Cisco ASA アクセスルールフィールド	Firepower プレフィルタ ルール フィールド
セキュリティグループ（宛て先）	同等のフィールドなし
サービス	選択された送信元ポート 選択された宛て先ポート
説明	備考
ロギング/ロギングレベルを有効にする	接続の開始時および接続の終了時にログに記録します。ACE のロギングが、デフォルト以外のロギングレベルで有効な場合、ツールは、接続の開始および切断時の両方で変換されたルールの接続ロギングを有効にします。ACE のロギングが、デフォルトレベルで有効な場合、釣るは、変換されたルールの接続路銀府を無効にします。
ロギング間隔	同等のフィールドなし
トラフィックの方向	同等のフィールドなし
送信元サービス	選択した接続元ポート、事前定義サービスが指定されている場合、変換しない
時間範囲	同等のフィールドなし

Firepower プレフィルタルール固有のフィールド

Firepower Threat Defense プレフィルタルールには、Cisco ASA アクセスルールに存在しないフィールドがいくつか含まれます。移行ツールは、変換されたプレフィルタルールのこれらの Firepower 固有フィールドに、次のデフォルト値を入力します。

表 *9 : Firepower* プレフィルタルール固有フィールドのデフォルト値

プレフィルタ ルール フィールド	変換されたアクセスルールのデフォルト値
名前	システム生成（変換した構成の命名規則 （20 ページ） を参照）
送信元インターフェイス オブジェクト	• ACL がグローバルに適用される場合、[任意（Any）] • ACL が特定のインターフェイスに適用される場合、変換中にツールが作成するインターフェイスグループ

プレフィルタ ルール フィールド	変換されたアクセスルールのデフォルト値
接続先インターフェイス オブジェクト	任意（すべてのプレフィルタルールのデフォルト値）
選択された VLAN タグ	デフォルト（インポート後に条件を手動で追加できます）

アクセスルールのポート引数演算子

拡張済みアクセスルールには、サービスオブジェクトで使用されるものと同じ演算子を使用する `port_argument` 要素を含めることができます。移行ツールは、アクセスルール内のこれらの演算子をサービスオブジェクトを変換する際に、アクセスルールに、単一のポート引数演算子または複数のポート引数演算子が含まれているかどうかに応じて、同じ演算子に使用する方法とは少しだけ異なる方法で変換します。

次の表に、使用できる演算子および単一演算子の使用例を示します。

表 *10*：アクセスルールのポート引数演算子

演算子	説明	例
`lt`	より小さい。	`access-list acp1 extended permit tcp any lt 300`
`gt`	より大きい。	`access-list acp2 extended permit tcp any gt 300`
`eq`	次の値と等しい。	`access-list acp3 extended permit tcp any eq 300`
`neq`	等しくない。	`access-list acp4 extended permit tcp any neq 300`
`range`	値の包括範囲。この演算子を使用する場合は、2つのポート番号を指定します（例：range 100 200）。	`access-list acp5 extended permit tcp any range 9000 12000`

アクセスルールに、単一のポート引数演算子が含まれている場合、移行ツールはアクセスルールを単一アクセスコントロールまたはプレフィルタ規則に次のように変換します。

表 *11*：アクセスコントロールまたはプレフィルタルールに変換された単一ポート引数演算子を使用するアクセスルール

Op	名前	送信元ゾーン	宛先ゾーン	送信元ネットワーク	宛先ネットワーク	送信元ポート	宛先ポート	アクション	有効
`lt`	acp1#1	任意	任意	任意	任意	1-299	任意	同等に許可	はい（True）
`gt`	acp2#1	任意	任意	任意	任意	301-65535	任意	同等に許可	はい（True）

Op	名前	送信元ゾーン	宛先ゾーン	送信元ネットワーク	宛先ネットワーク	送信元ポート	宛先ポート	アクション	有効
eq	acp3#1	任意	任意	任意	任意	300	任意	同等に許可	はい（True）
neq	acp4#1	任意	任意	任意	任意	1-299、301-65535	任意	同等に許可	はい（True）
range	acp5#1	任意	任意	任意	任意	9000-2000	任意	同等に許可	はい（True）

わかりやすくするために、この表の [元の演算子（**Op**）] 列を表示しています。これは、アクセスコントロールルールのフィールドには表示されません。

アクセスルールに、複数のポート演算子（例：`access-list acp6 extended permit tcp any neq 300 any neq 400`）が含まれている場合、移行ツールは、単一のアクセスルールを複数のアクセスコントロールまたはプレフィルタルールに次のように変換します。

表 *12*：アクセスコントロールに変換された複数ポート引数演算子を使用するアクセスルール

Op	名前	送信元ゾーン	宛先ゾーン	送信元ネットワーク	宛先ネットワーク	送信元ポート	宛先ポート	アクション	有効
neq	acp6#1_1	任意	任意	任意	任意	1-299	1-399	同等に許可	はい（True）
neq	acp6#1_2	任意	任意	任意	任意	301-65535	1-399	同等に許可	はい（True）
neq	acp6#1_3	任意	任意	任意	任意	1-299	401-65535	同等に許可	はい（True）
neq	acp6#1_4	任意	任意	任意	任意	301-65535	401-65535	同等に許可	はい（True）

わかりやすくするために、この表の [元の演算子（**Op**）] 列を表示しています。これは、アクセスコントロールルールのフィールドには表示されません。

複数のプロトコルを指定するアクセスルール

Cisco ASA では、アクセスルールで送信元と宛て先ポートを構成し、複数プロトコル（例：TCP と UDP）を指定するプロトコルサービスオブジェクトを使用できます。次に例を示します。

```
object-group protocol TCPUDP
 protocol-object udp
 protocol-object tcp
access-list acp1 extended permit object-group TCPUDP any any
```

ただし、Firepower システムでは、アクセスコントロールルールとプレフィルタルールのみを次のように構成できます。

- 送信元ポートと宛て先ポートの両方で、同じプロトコルを指定する必要があります。
- 宛て先ポートでは複数のプロトコルを指定できますが、送信元ポートでは何も指定する必要はありません。

プロトコル オブジェクト グループ tcp および udp を含むアクセスルールは、サポートされていないルールとして移行されます。そのため、ルールは、**「tcp と udp の両方が含まれるオブジェクト グループ プロトコルはサポートされていません」**のコメントで無効になります。

NAT ルールの変換

次の表に要約されているように、Cisco ASA 向け NAT と Firepower Threat Defense 向け NAT は、同等機能をサポートします。

表 *13 : Firepower Threat Defense NAT* ポリシーにマッピングされている *Cisco ASA NAT* ポリシー

Cisco ASA NAT ポリシー	Firepower Threat Defense NAT ポリシー	特性を定義する
Twice NAT	手動 NAT	• 1 つのルール内で送信元と宛先アドレスの両方を指定します。 • 直接構成します。 • ネットワーク オブジェクト グループを使用できます。 • NAT テーブル内で、手動で順序付けが行われます（自動 NAT ルールの前または後）。
ネットワークオブジェクト NAT	自動NAT	• 送信元または宛先アドレスのいずれかを指定します。 • ネットワーク オブジェクトのパラメータとして構成されます。 • ネットワーク オブジェクト グループを使用できません。 • NAT テーブルで自動で順序付けされます。

移行ツールは、Cisco ASA NAT 構成を Firepower Threat Defense NAT 構成に変換します。ただし、このツールは、サポートされていないネットワークオブジェクトを使用する Cisco ASA NAT 構成を変換することはできません。その場合、変換は失敗します。

Firepower Threat Defense ルールフィールドにマッピングされた Cisco ASA NAT ルールフィールド

移行ツールは、次の表に示すように、Cisco ASA NAT ルールのフィールドを Firepower Threat Defense NAT ルールのフィールドに変換します。

（注）

- 列 1 のフィールド名（Cisco ASA NAT ルールフィールド）は、ASDM インターフェイスのフィールドラベルに対応しています。
- 列 2 のフィールド名（Firepower Threat Defense ルールフィールド）は、Firepower Management Center インターフェイスのフィールドラベルに対応しています。

表 *14 : Firepower Threat Defense NAT* ルールフィールドにマッピングされた *Cisco ASA NAT* ルールフィールド

Cisco ASA NAT ルールフィールド	Firepower Threat Defense ルールフィールド
元のパケット - 送信元インターフェイス	インターフェイス オブジェクト - 送信元インターフェイス オブジェクト
元のパケット - 送信元アドレス	元のパケット - 元の送信元
元のパケット - 接続先インターフェイス	インターフェイス オブジェクト - 接続先インターフェイス オブジェクト
元のパケット - 宛先アドレス	元のパケット - 元の接続先 - アドレスタイプ 元のパケット - 元の接続先 - ネットワーク
元のパケット - サービス	元のパケット - 元の送信元ポート 元のパケット - 元の宛て先ポート
変換済みパケット - 送信元 NAT タイプ	タイプ
変換済みパケット - 送信元アドレス	変換済みパケット - 変換済み送信元 - アドレスタイプ 変換済みパケット - 変換済み送信元 - ネットワーク
変換済みパケット - 宛先アドレス	変換済みパケット - 変換済み接続先

Cisco ASA NAT ルールフィールド	Firepower Threat Defense ルールフィールド
変換済みパケット - サービス	変換済みパケット - 変換済み送信元ポート 変換済みパケット - 変換済み宛て先ポート
1 対 1 のアドレス変換を使用する	高度 - ネット間マッピング
PAT プール変換済みアドレス	PAT プール - PAT - アドレスタイプ PAT プール - PAT - ネットワーク
ラウンドロビン	PAT プール - ラウンドロビン割り当てを使用する
PAT の一意性をインターフェイスごとではなく、接続先ごとに拡張する	PAT プール - 拡張済み PAT テーブル
TCP ポートと UDP ポートをフラットな範囲 1024 ～ 65535 に変換する	PAT プール - フラットなポート範囲
1 ～ 1023 の範囲を含める	PAT プール - 予約ポートを含める
ブロック割り当てを有効にする	同等のものはなし
送信元インターフェイス PAT に対して IPv6 を使用する	同等のものはなし
接続先インターフェイス PAT に対して IPv6 を使用する	高度 - IPv6
ルールを有効化する	有効
このルールに一致する DNS 回答の変換	高度 - このルールに一致する DNS 返信を変換する
出力インターフェイスでプロキシ ARP を無効にする	高度 - 接続先インターフェイスで ARP をプロキシしない
出力インターフェイスを特定するためにルートテーブルをルックアップする	同等のものはなし
方向	高度 - 単一方向
説明	説明

ネットワークオブジェクトおよびネットワークオブジェクト グループ変換

ネットワークオブジェクトおよびネットワーク オブジェクト グループは、IP アドレスまたはホスト名を特定します。Cisco ASA と Firepower Threat Defense の両方では、これらのオブジェクトとグループをアクセスルールと NAT ルールで使用できます。

Cisco ASA では、1 つのネットワーク オブジェクトには、1 つのホスト、ネットワーク IP アドレス、IP アドレスの範囲、または完全修飾ドメイン名（FQDN）を入れることができます。Firepower システムでは、ネットワークオブジェクトは、FQDNを除き、これらと同じ値をサポートします。

移行ツールは、複数のアクセスルールまたは NAT ルールでオブジェクトが使用されているかどうかにかかわらず、Cisco ASA ネットワークオブジェクトまたはグループを 1 度変換します。

ネットワークオブジェクト変換

変換する各 Cisco ASA ネットワークオブジェクトの場合、移行ツールは、Firepower ネットワークオブジェクトを作成します。

移行ツールは、次のように Cisco ASA ネットワークオブジェクトのフィールドをFirepower ネットワークオブジェクトに変換します。

表 *15 : Firepower* ネットワーク オブジェクト フィールドにマッピングされた *Cisco ASA* ネットワーク オブジェクト フィールド

Cisco ASA ネットワーク オブジェクト フィールド	**Firepower** ネットワーク オブジェクト フィールド
名前	システム生成。「変換した構成の命名規則（20 ページ）」を参照
タイプ	タイプ
IP バージョン	同等のフィールドなし
IP アドレス（IP Address）	値
ネットマスク	値（CIDR 表記に含まれる）
説明	説明
オブジェクト NAT アドレス	同等のフィールドなし

例：アクセス制御リストのネットワークオブジェクト

Cisco ASA 構成がいるに次のコマンドが存在する場合：

```
object network obj1
 host 1.2.3.4
object network obj2
 range 1.2.3.7 1.2.3.10
object network obj3
 subnet 10.83.0.0 255.255.0.0
access-list sample_acl extended permit ip object obj1 object obj2
access-list sample_acl extended permit ip object obj3 object obj1
access-group gigabitethernet_access_in in interface gigabitethernet1/1
```

システムはこれらのオブジェクトを次のように変換します。

名前	ドメイン	値（ネットワーク）	タイプ	オーバーライド
obj1	なし	1.2.3.4	ホスト	False
obj2	なし	1.2.3.7-1.2.3.10	アドレス範囲	False
obj3	なし	10.83.0.0/16	ネットワーク	False

例：NAT ルールのネットワークオブジェクト

Cisco ASA 構成ファイルに次のコマンドが存在する場合：

```
nat (gigabitethernet1/1,gigabitethernet1/2) source static obj1 obj1
```

システムは、このルールのオブジェクト `obj1` を、上記のアクセスルール例のオブジェクト `obj1` を変換するのと同じ方法で変換します。

ネットワーク オブジェクト グループ変換

変換する各 Cisco ASA ネットワーク オブジェクト グループの場合、移行ツールは、Firepower ネットワーク オブジェクト グループを作成します。また、グループに含まれるオブジェクトがまだ変換されていない場合は、それらのオブジェクトも変換されます。

移行ツールは、次のように Cisco ASA ネットワークのフィールドをFirepower ネットワーク オブジェクト グループに変換します。

表 *16 : Firepower* ネットワーク オブジェクト グループ フィールドにマッピングされた *Cisco ASA* ネットワーク オブジェクト グループ フィールド

Cisco ASA ネットワーク オブジェクト グループ フィールド	**Firepower** ネットワーク オブジェクト グループ フィールド
グループ名	名前
説明	説明

Cisco ASA ネットワーク オブジェクト グループ フィールド	Firepower ネットワーク オブジェクト グループ フィールド
グループ内のメンバー	値（選択したネットワーク）

例：アクセス制御リストのネットワーク オブジェクト グループ

Cisco ASA 構成がいるに次のコマンドが存在する場合：

```
object network obj1
 host 1.2.3.4
object network obj2
 range 1.2.3.7 1.2.3.10
object network obj3
 subnet 10.83.0.0 255.255.0.0
object-group network obj_group1
 network-object object obj1
 network-object object obj2
 network-object object obj3
access-list sample_acl extended permit ip object-group obj_group1 any
access-group gigabitethernet_access_in in interface gigabitethernet1/1
```

システムは、次のネットワークグループを作成します。

名前	ドメイン	値（ネットワーク）	タイプ	オーバーライド
obj_group1	なし	obj1 obj2 obj3	グループ	False

関連付けられたオブジェクトがまだ変換されていない場合、システムはネットワークオブジェクト変換 （34 ページ）の説明に従ってそれらのオブジェクトを変換します。

例：NAT ルールのネットワーク オブジェクト グループ

Cisco ASA 構成ファイルに次のコマンドが存在する場合：

```
nat (interface1,interface2) source static obj_group1 obj_group1
```

システムは、このルールの `obj_group1` を 、上記のアクセスルール例で `obj_group1` を変換するのと同じ方法で変換します。

サービスオブジェクトとサービスグループの変換

Cisco ASA では、サービスオブジェクトとサービスグループは、プロトコルとポートを指定し、これらのポートを送信元ポートまたは宛て先ポートとして指名します。サービスオブジェクトとグループは、アクセスルールと NAT ルールの両方で使用できます。

Firepower システムでは、ポートオブジェクトとポートオブジェクトグループがプロトコルとポートを指定しますが、オブジェクトをアクセスコントロール、プレフィルタ、または NAT

ルールに追加した場合、システムは、これらのポートを接続元ポートまたは宛て先ポートとして指名します。サービスオブジェクトを Firepower システムの同等の機能に変換する場合は、移行ツールを使用して、サービスオブジェクトをポートオブジェクトまたはグループに変換し、関連するアクセスコントロール、プレフィルタ、または NAT ルールに具体的な変更を加えます。結果として、移行ツールは、変換中に単一サービスオブジェクト/サービスグループおよび関連するアクセスルールまたは NAT ルールを複数のポートオブジェクト/グループおよび関連するアクセスコントロール、プレフィルタ、NAT ルールに展開する場合があります。

サービスオブジェクトの変換

移行ツールを使用して、1 つ以上のポートオブジェクトとこれらのポートオブジェクトを参照する 1 つ以上のアクセスコントロールまたはプレフィルタルールを作成して Cisco Cisco ASA サービスオブジェクトを変換します。

移行ツールは、次のサービスオブジェクトタイプを変換できます。

- プロトコル
- TCP および UDP
- ICMP/ICMPv6

移行ツールは、Cisco ASA サービスオブジェクトのフィールドを次のように Firepower ポートオブジェクトのフィールドに変換します。

表 *17 : Firepower* ポートオブジェクトフィールドにマッピングされた *Cisco ASA* サービスオブジェクトフィールド

Cisco ASA サービス オブジェクト フィールド	**Cisco ASA サービスオブジェクトタイプ**	**Firepower ポート オブジェクト フィールド**
名前	任意	システム生成（変換した構成の命名規則 （20 ページ） を参照）
サービス タイプ	TCP/UDP、ICMP/ICMPv6	プロトコル
プロトコル	プロトコルのみ	プロトコル
説明	任意	同等なし、コンテンツは無視される
宛先ポート/範囲	TCP/UDP のみ	ポート
送信元ポート/範囲	TCP/UDP のみ	ポート
ICMP タイプ	ICMP/ICMPv6 のみ	タイプ
ICMP コード	ICMP/ICMPv6 のみ	コード

サービスオブジェクトのポートリテラル値

Cisco ASA サービスオブジェクトでは、ポート番号ではなくポートリテラル値を指定できます。次に例を示します。

```
object service http
 service tcp destination eq www
```

Firepower システムはこれらのポートのリテラル値をサポートしていないため、移行ツールはそれらのポートのリテラル値を、対応するポート番号に変換します。このツールは、上記の例を次のポートオブジェクトに変換します。

名前	タイプ	ドメイン	値（プロトコル/ポート）	オーバーライド
http	オブジェクト	なし	TCP(6)/80	False

ポートリテラル値と関連するポート番号の完全な一覧については、『*CLI* ブック *1*：*Cisco ASA* シリーズ汎用操作 *CLI* 構成ガイド』の「TCP および UDP ポート」を参照してください。

サービスオブジェクトのポート引数演算子

Cisco ASA サービスオブジェクトでは、ポート引数で次の演算子を使用できます。

表 *18*：サービスオブジェクトのポート引数演算子

演算子	説明	例
`lt`	より小さい。	`object service testOperator` ` service tcp source lt 100`
`gt`	より大きい。	`object service testOperator` ` service tcp source gt 100`
`eq`	次の値と等しい。	`object service http-proxy` ` service tcp source eq 8080`
`neq`	等しくない。	`object service testOperator` ` service tcp source neq 200`
`range`	値の包括範囲。	`object service http-proxy` ` service tcp source range 9000 12000`

移行ツールは、これらの演算子を次のように変換します。

表 *19*：ポートオブジェクト/グループに変換されるポート引数演算子を持つサービスオブジェクト

オペレータ	変換先	ポートオブジェクト値の例（プロトコル/ポート）
`lt`	指定数より小さいポート番号の範囲を指定する単一のポートオブジェクト。	`TCP(6)/1-99`

オペレータ	変換先	ポートオブジェクト値の例（プロトコル/ポート）
gt	指定数より大きいポート番号の範囲を指定する単一のポートオブジェクト。	TCP(6)/101-65535
eq	単一のポート番号を指定する単一のポートオブジェクト。	TCP(6)/8080
neq	2 つのポートオブジェクトと 1 つのポートオブジェクトグループ。最初のポートオブジェクトは、指定されたポートよりも低い範囲を指定しています。2 番目のポートオブジェクトは、指定されたポートよりも大きい範囲を指定しています。ポートオブジェクトグループには両方のポートオブジェクトが含まれます。	最初のオブジェクト（testOperator_src_1）： TCP(6)/1-199 2 番目のオブジェクト（testOperator_src_2）： TCP(6)/201-65535 オブジェクトグループ（testOperator_src）： testOperator_src_1 testOperator_src_2
range	包括的な値の範囲を指定する単一のポートオブジェクト。	TCP(6)/9000-12000

送信元ポートと宛て先ポートを含むサービスオブジェクト

Cisco ASA では、1 つのサービスオブジェクトで送信元ポートと接続先ポートの両方のポートを指定できます。Firepower システムでは、ポートオブジェクトはポート値のみを指定します。アクセスコントロールルールまたはプレフィルタルールでポートオブジェクトを使用するまで、システムはポートを送信元または接続先として指定しません。

この違いに対応するために、移行ツールは、送信元 と接続先 の両方を指定する Cisco ASA サービスオブジェクトを変換するときに、単一のオブジェクトを 2 つのポートオブジェクトに展開します。オブジェクト名に拡張子を追加して宛て先ポートの下の接続先 *_src* for source ports and *_dst* を示します。

例

```
object service http-proxy
 service tcp source range 9000 12000 destination eq 8080
```

ツールは、このサービスオブジェクトを次のポートオブジェクトに変換します。

名前	タイプ	ドメイン	値（プロトコル/ポート）	オーバーライド
http-proxy_src	オブジェクト	なし	TCP(6)/9000-12000	False
http-proxy_dst	オブジェクト	なし	TCP(6)/8080	False

例：プロトコル サービス オブジェクトの変換

Cisco ASA 構成：

```
object service protocolObj1
 service snp
 description simple routing
```

変換先：

表 *20 :* ポートオブジェクト

名前	タイプ	ドメイン	値（プロトコル）	オーバーライド
protocolObj1	オブジェクト	なし	SNP (109)	False

例：TCP/UDP サービスオブジェクトの変換

Cisco ASA の構成：

```
object service servObj1
 service tcp destination eq ssh
```

変換先：

表 *21 :* ポートオブジェクト

名前	タイプ	ドメイン	値（プロトコル/ポート）	オーバーライド
servObj1	オブジェクト	なし	TCP(6)/22	False

例：ICMP/ICMPv6 サービス オブジェクトの変換

ICMP

Cisco ASA の構成：

```
object service servObj1
 service icmp alternate-address 0
```

変換先：

表 *22 :* ポートオブジェクト

名前	タイプ	ドメイン	値（プロトコル/Type:Code）	オーバーライド
servObj1	オブジェクト	なし	ICMP(1)/代替ホストアドレス：ホストの代替アドレス	False

ICMPv6

Cisco ASA の構成：

```
object service servObj1
 service icmp6 unreachable 0
```

変換先：

表 *23 :* ポートオブジェクト

名前	タイプ	ドメイン	値（プロトコル/Type:Code）	オーバーライド
servObj1	オブジェクト	なし	IPV6-ICMP (58)/接続先到達不能：接続先へのルートなし	False

サービスグループの変換

移行ツールは、ポートオブジェクトグループを作成し、それらのポートオブジェクトグループを関連するアクセスコントロールルールまたはプレフィルタルールに関連付けることにより、Cisco ASA サービスグループを変換します。

移行ツールは、次のサービスグループタイプを変換できます。

- プロトコル
- TCP および UDP
- ICMP/ICMPv6

移行ツールは、Cisco ASA サービスオブジェクトのフィールドを次のように Firepower ポートオブジェクトのフィールドに変換します。

表 *24 : Firepower* ポートオブジェクトフィールドにマッピングされた *Cisco ASA* サービスグループフィールド

Cisco ASA サービスグループフィールド	ポート グループ オブジェクト フィールド
名前	システム生成（変換した構成の命名規則 （20 ページ） を参照）
説明	説明
グループ内のメンバー	選択したポート

ネストされたサービスグループの変換

Cisco ASA は、ネストされたサービスグループ（つまりその他のサービスグループを含むサービスグループ）をサポートします。Firepower システムは、ネストされたポートグループをサ

ポートしませんが、複数のグループを単一のアクセスコントロールルールまたはプレフィルタ規則に関連付けることで、同様の機能を実現できます。ネストされたサービスグループを変換する場合、移行ツールはグループ構造を「フラット化」し、最も内側のサービスオブジェクトおよびグループをポートオブジェクトおよびポートオブジェクトグループに変換し、それらの変換されたグループをアクセスコントロールルールまたはプレフィルタルールに関連付けます。

1つのアクセスコントロールルールまたはプレフィルタルールに最大50のポートオブジェクトを関連付けることができます。新しいポートオブジェクト数が50を超えると、このツールは、すべての新しいポートオブジェクトをルールに関連付けるまで、重複アクセスコントロールルールまたはプレフィルタルールを作成します。

送信元サービスと接続先サービスの両方として使用される、ネストされたサービスオブジェクトを含むFirepowerシステムルールはサポートされません。

例

```
object-group service http-8081 tcp
 port-object eq 80
 port-object eq 81

object-group service http-proxy tcp
 port-object eq 8080

object-group service all-http tcp
 group-object http-8081
 group-object http-proxy

access-list FMC_inside extended permit tcp host 33.33.33.33 object-group all-http host
33.33.33.33 object-group all-http
```

上記の例では、サービスオブジェクト *http-8081* および *http-proxy* が *all-http* サービスグループ内にネストされています。

このようなシナリオでは、ポートオブジェクトに関連するルールは無視されます。システムは、オブジェクトをインポートしますが、関連するアクセスコントロールまたはプレフィルタルールを無効にし、**「送信元と接続先の両方でネストされたサービスグループはサポートされていません」**のコメントをルールに追加します。

変換中にシステムが作成する場合がある変換されたサービスオブジェクト、サービスグループおよび任意の重複ルールにツールが使用する命名規則の詳細については、「変換した構成の命名規則 （20 ページ）」を参照してください。

例

Cisco ASA の構成：

```
object-group service legServGroup1 tcp
 port-object eq 78
 port-object eq 79
object-group service legServGroup2 tcp
 port-object eq 80
 port-object eq 81
object-group service legacyServiceNestedGrp tcp
 group-object legServGroup1
```

```
 group-object legServGroup2
access-list  acp1 extended permit tcp  3.4.5.0  255.255.255.0  5.6.7.0 255.255.255.0
object-group legacyServiceNestedGrp
access-group acp1 global
```

変換先：

表 *25*：ポートオブジェクトグループ

名前	タイプ	ドメイン	値（プロトコル/ポート）	オーバーライド
legServGroup1_1	オブジェクト	なし	TCP(6)/78	False
legServGroup1_2	オブジェクト	なし	TCP(6)/79	False
legServGroup2_1	オブジェクト	なし	TCP(6)/80	False
legServGroup2_2	オブジェクト	なし	TCP(6)/81	False
legServGroup1	グループ	なし	legServGroup1_1 legServGroup1_2	False
legServGroup2	グループ	なし	legServGroup2_1 legServGroup2_2	False

表 *26*：アクセスコントロールルールまたはプレフィルタルール

名前	送信元ゾーン	宛先ゾーン	送信元ネットワーク	宛先ネットワーク	送信元ポート	宛先ポート	アクション	有効
acp1#1	任意	任意	3.4.5.0/24	5.6.7.0/24	TCP(6)	legServGroup1 legServGroup2	同等に許可	True

例：プロトコル サービス グループの変換

Cisco ASA の構成：

```
object-group protocol TCPUDP
 protocol-object udp
 protocol-object tcp
```

変換先：

表 *27:* ポート オブジェクトおよびグループ

名前	タイプ	ドメイン	値（プロトコル/ポート）	オーバーライド
TCPUDP_1	オブジェクト	なし	TCP(6)	False
TCPUDP_2	オブジェクト	なし	UDP(17)	False
TCPUDP	グループ	なし	TCPUDP_1 TCPUDP_2	False

例：TCP/UDP サービスグループの変換

グループ作成時に作成されるオブジェクト

Cisco ASA では、サービスグループの作成時にその場でオブジェクトを作成できます。これらのオブジェクトは、サービスオブジェクトとして分類されますが、Cisco ASA 構成ファイルのエントリは、`object service` ではなく、`port-object` を使用します。これらのオブジェクトは、個別に作成されたいため、移行ツールは、グループ作成とは別に作成されたオブジェクトの命名規則とは若干異なる命名規則が使用されます。

Cisco ASA の構成：

```
object-group service servGrp5 tcp-udp
 port-object eq 50
 port-object eq 55
```

変換先：

表 *28:* ポート オブジェクトおよびグループ

名前	タイプ	ドメイン	値（プロトコル/ポート）	オーバーライド
servGrp5_1	オブジェクト	なし	TCP(6)/50	False
servGrp5_2	オブジェクト	なし	TCP(6)/55	False
servGrp5	グループ	なし	servGrp5_1 servGrp5_2	False

グループから個別に作成されたオブジェクト

Cisco ASA の構成：

```
object service servObj1
 service tcp destination eq ssh
object service servObj2
 service udp destination eq 22
object service servObj3
 service tcp destination eq telnet
```

```
object-group service servGrp1
 service-object object servObj1
 service-object object servObj2
 service-object object servObj3
```

変換先：

表 *29 :* ポート オブジェクトおよびグループ

名前	タイプ	ドメイン	値（プロトコル/ポート）	オーバーライド
servObj1	オブジェクト	なし	TCP(6)/22	False
servObj2	オブジェクト	なし	UDP(17)/22	False
servObj3	オブジェクト	なし	TCP(6)/23	False
servGrp1	グループ	なし	servObj1 servObj2 servObj3	False

例：ICMP/ICMPv6 サービスグループの変換

ICMP

Cisco ASA の構成：

```
object-group icmp-type servGrp4
 icmp-object echo-reply
```

変換先：

表 *30 :* ポート オブジェクトおよびグループ

名前	タイプ	ドメイン	値（プロトコル/ポート）	オーバーライド
servGrp4_1	オブジェクト	なし	ICMP(1)/Echo Reply	False
servGrp4	グループ	なし	servGrp4_1	False

ICMPv6

Cisco ASA の構成：

```
object-group service servObjGrp3
 service-object icmp6 packet-too-big
 service-object icmp6 parameter-problem
```

変換先：

表 *31 :* ポート オブジェクトおよびグループ

名前	タイプ	ドメイン	値（プロトコル/ポート）	オーバーライド
servObjGrp3_1	オブジェクト	なし	IPV6-ICMP(58)/2	False
servObjGrp3_2	オブジェクト	なし	IPV6-ICMP(58)/4	False
servObjGrp3	グループ	なし	servObjGrp3_1 servObjGrp3_2	False

アクセスグループの変換

Cisco ASA で、ACL を適用するには、CLI で `access-group` コマンドを入力するか、ASDM アクセルルールエディタで、**[適用（Apply）]** を選択します。これらの操作を実行すると、Cisco ASA 構成ファイルで `access-group` エントリが生成されます（以下の例を参照）。

`access-group` コマンドは、システムが ACL を適用するインターフェイスと、システムがインターフェイスでインバウンド（イングレス）トラフィックまたはアウトバウンド（エグレス）トラフィックに ACL を適用するかどうかを指定します。

Firepower システムで同等の機能を構成するには、次の手順を実行します。

- セキュリティゾーンを作成し、セキュリティゾーンをインターフェイスに関連付け、そのセキュリティゾーンを送信元ゾーン条件（インバウンドトラフィックの場合）または宛先ゾーン条件（アウトバウンドトラフィックの場合）としてアクセスコントロールルールに追加します。
- インターフェイスグループを作成し、インターフェイスグループをインターフェイスに関連付け、インターフェイスグループを送信元インターフェイス グループ条件（インバウンドトラフィックの場合）または宛先インターフェイス グループ条件（アウトバウンドトラフィックの場合）としてプレフィルタルールに追加します。

`access-group` コマンドを変換する場合、移行ツールは、セキュリティゾーンまたはインターフェイスグループを作成し、関連するアクセスコントロールルールまたはプレフィルタルールの条件としてセキュリティゾーンとインターフェイスグループを追加することにより、入力情報と出力情報を取得します。ただし、移行ツールは、セキュリティゾーンまたはインターフェイスグループの名前のインターフェイス情報を保持しますが、関連するインターフェイスまたはデバイス構成は変換しません。これらの構成は、変換されたポリシーのインポート後に手動で追加する必要があります。変換されたポリシーをインポートした後、ポリシーをデバイスに、セキュリティゾーンまたはインターフェイス グループをインターフェイスに、手動で関連付ける必要があります。

ACLを変換する際、システムは、特定のインターフェースに適用されるルールの後に、グローバルに適用されるルールを配置します。

特別な事例

Cisco ASA 構成が単一 ACL をイングレスインターフェイスとエグレスインターフェイスの両方に適用する場合、ツールは、ACL を変換して、2 つのセットのアクセスコントロールルールとプレフィルタルールに変換します。

- 一連のイングレスルール（有効）
- 一連のエグレスルール（無効）

Cisco ASA 構成が単一 ACL をグローバルおよび特定のインターフェイスに適用する場合、ツールは、ACL を変換して、2 つのセットのアクセスコントロールルールとプレフィルタルールに変換します。

- 特定のインターフェイスに関連付けられた一連のルール（有効）
- 送信元ゾーンと宛先ゾーンが [任意（Any）] に設定された一連のルール（有効）

例：グローバルに適用された ACL

Cisco ASA の構成：

```
access-list global_access extended permit ip any any
access-group global_access global
```

移行ツールは、この構成を次に変換します。

表 *32:* アクセスコントロールルールまたはプレフィルタルール

名前	送信元ゾーン/インターフェイスグループ	宛先ゾーン/インターフェイスグループ	送信元ネットワーク	宛先ネットワーク	送信元ポート	宛先ポート	アクション	有効
global_access#1	任意	任意	任意	任意	任意	任意	同等に許可	はい（True）

例：特定のインターフェイスに適用された ACL

Cisco ASA の構成：

```
access-list acp1 permit tcp any host 209.165.201.3 eq 80
access-group acp1 in interface outside
```

次の例では、access-group コマンドによって、acp1 という ACL を outside というインターフェイス上のインバウンドトラフィックに適用します。

移行ツールは、この構成を次に変換します。

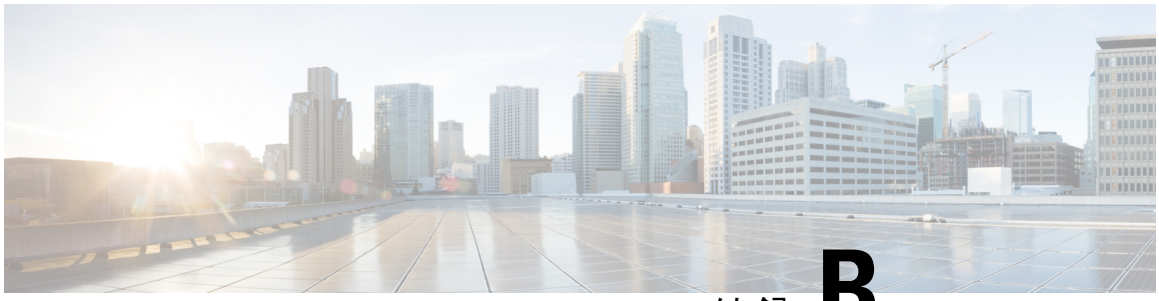
変換マッピング

表 *33*：セキュリティゾーン/インターフェイスグループ

名前	インターフェイスタイプ	ドメイン	選択したインターフェイス
acp1_outside_in_zone	• ルーテッド（Cisco ASA デバイスがルーテッドモードで実行されている場合） • スイッチ（Cisco ASA デバイスが透過モードで実行されている場合）	なし	任意

表 *34*：アクセスコントロールルールまたはプレフィルタルール

名前	送信元ゾーン/インターフェイスグループ	宛先ゾーン/インターフェイスグループ	送信元ネットワーク	宛先ネットワーク	送信元ポート	宛先ポート	アクション	有効
acp1#1	acp1_outside_in_zone	任意	任意	209.165.201.3	任意	TCP(6)/80	同等に許可	True



付録 B

変換の例

このセクションでは、Cisco ASA 構成と、移行ツールが変換する Firepower Threat Defense ルールとオブジェクトの例を示します。

例

個々のネットワークを指定するアクセスルール

Cisco ASA の構成：

```
access-list acp1 extended permit tcp 3.4.5.0 255.255.255.0 5.6.7.0 255.255.255.0
access-group acp1 global
```

変換先：

表 *35:* アクセスコントロールルールまたはプレフィルタルール

名前	送信元ゾーン	宛先ゾーン	送信元ネットワーク	宛先ネットワーク	送信元ポート	宛先ポート	アクション	有効
acp1#1	任意	任意	3.4.5.0/24	5.6.7.0/24	TCP(6)	任意	同等に許可	はい（True）

ネットワーク オブジェクト グループを使用するアクセスルール

Cisco ASA の構成：

```
access-list acp1 extended permit ip object-group host1 object-group host2
access-group acp1 global
```

変換先：

表 *36 :* ネットワーク オブジェクト グループ

名前	ドメイン	値（ネットワーク）	タイプ	オーバーライド
host1	なし	obj1 obj2	グループ	False
host2	なし	obj3 obj4	グループ	False

表 *37 :* ネットワーク オブジェクト グループを使用するアクセスルール

名前	送信元ゾーン	宛先ゾーン	送信元ネットワーク	宛先ネットワーク	送信元ポート	宛先ポート	アクション	有効
acp1#1	任意	任意	host1	host2	任意	任意	同等に許可	はい（True）

個々のネットワークとポートを指定するアクセスルール

Cisco ASA アクセスルール：

```
access-list acp1 extended permit tcp 3.4.5.0 255.255.255.0 eq 90 5.6.7.0 255.255.255.0
eq 80
access-group acp1 global
```

変換先：

表 *38 :* アクセスコントロールルールまたはプレフィルタルール

名前	送信元ゾーン	宛先ゾーン	送信元ネットワーク	宛先ネットワーク	送信元ポート	宛先ポート	アクション	有効
acp1#1	任意	任意	3.4.5.0/32	5.6.7.0/32	TCP(6)/90	TCP(6)/80	同等に許可	はい（True）

サービスオブジェクトを使用するアクセスルール

Cisco ASA の構成：

```
object service servObj1
 service tcp destination eq 78
access-list acp1 extended permit object servObj1 any any
access-group acp1 in interface outside
```

変換先：

表 *39 :* ポートオブジェクト

名前	タイプ	ドメイン	値（プロトコル/ポート）	オーバーライド
servObj1	オブジェクト	なし	TCP(6)/78	False

表 *40 :* アクセスコントロールルールまたはプレフィルタルール

名前	送信元ゾーン	宛先ゾーン	送信元ネットワーク	宛先ネットワーク	送信元ポート	宛先ポート	アクション	有効
acp1#1	任意	任意	任意	任意	任意	servObj1	同等に許可	はい（True）

サービス オブジェクト グループを使用するアクセスルール

Cisco ASA の構成：

```
object-group service legServGroup tcp
 port-object eq 78
access-list  acp1 extended permit tcp  3.4.5.0  255.255.255.0  5.6.7.0 255.255.255.0
object-group legServGroup
access-group acp1 global
```

変換先：

表 *41 :* ポートオブジェクト

名前	タイプ	ドメイン	値（プロトコル/ポート）	オーバーライド
legServGroup	オブジェクト	なし	TCP(6)/78	False

表 *42 :* アクセスコントロールルールまたはプレフィルタルール

名前	送信元ゾーン	宛先ゾーン	送信元ネットワーク	宛先ネットワーク	送信元ポート	宛先ポート	アクション	有効
acp1#1	任意	任意	3.4.5.0/24	5.6.7.0/24	TCP(6)	legServGroup	同等に許可	はい（True）

ネストされたサービス オブジェクト グループを使用するアクセスルール

Cisco ASA の構成：

```
object-group service legServGroup1 tcp
 port-object eq 78
 port-object eq 79
object-group service legServGroup2 tcp
 port-object eq 80
```

```
 port-object eq 81
object-group service legacyServiceNestedGrp tcp
 group-object legServGroup1
 group-object legServGroup2
access-list  acp1 extended permit tcp  3.4.5.0  255.255.255.0  5.6.7.0 255.255.255.0
object-group legacyServiceNestedGrp
access-group acp1 global
```

変換先：

表 *43*：ポート オブジェクトおよびグループ

名前	タイプ	ドメイン	値（プロトコル/ポート）	オーバーライド
legServGroup1_1	オブジェクト	なし	TCP(6)/78	False
legServGroup1_2	オブジェクト	なし	TCP(6)/79	False
legServGroup2_1	オブジェクト	なし	TCP(6)/80	False
legServGroup2_2	オブジェクト	なし	TCP(6)/81	False
legServGroup1	グループ	なし	legServGroup1_1 legServGroup1_2	False
legServGroup2	グループ	なし	legServGroup2_1 legServGroup2_2	False

ネストされたグループである LegacyServiceNestedGrp はフラット化されているため、変換された構成にはそのグループに相当するものが含まれないことに注意してください。

表 *44*：アクセスコントロールルールまたはプレフィルタルール

名前	送信元ゾーン	宛先ゾーン	送信元ネットワーク	宛先ネットワーク	送信元ポート	宛先ポート	アクション	有効
acp1#1	任意	任意	3.4.5.0/24	5.6.7.0/24	TCP(6)	legServGroup1 legServGroup2	同等に許可	はい（True）

ネストされた拡張サービス オブジェクト グループを使用するアクセスルール

Cisco ASA の構成：

```
object service http
 service tcp source range 9000 12000 destination eq www
object service http-proxy
 service tcp source range 9000 12000 destination eq 8080
object-group service all-http
 service-object object http
 service-object object http-proxy
object-group service all-httpz
 group-object all-http
 service-object tcp destination eq 443
```

変換の例

```
access-list acp1 extended permit object-group all-httpz any any
access-group acp1 in interface inside
```

変換先：

表 *45*：ポート オブジェクト

名前	タイプ	ドメイン	値（プロトコル/ポート）	オーバーライド
http_src	オブジェクト	なし	TCP(6)/9000-12000	False
http_dst	オブジェクト	なし	TCP(6)/80	False
http-proxy_src	オブジェクト	なし	TCP(6)/9000-12000	False
http-proxy_dst	オブジェクト	なし	TCP(6)/8080	False
all-httpz-dst	グループ	なし	TCP(6)/443	False

ネストされたグループである all-httpz はフラット化されているため、変換された構成にはそのグループに相当するものが含まれないことに注意してください。

表 *46*：アクセスコントロールとプレフィルタルール

名前	送信元ゾーン	宛先ゾーン	送信元ネットワーク	宛先ネットワーク	送信元ポート	宛先ポート	アクション	有効
acp1#1_1	任意	任意	任意	任意	http_src	http_dst	同等に許可	はい（True）
acp1#1_2	任意	任意	任意	任意	http-proxy_src	http-proxy_dst	同等に許可	はい（True）
acp1#1_3	任意	任意	任意	任意	任意	all-httpz-dst	同等に許可	はい（True）

「gt」および「neq」演算子を使用するサービスオブジェクトがあるアクセスルール

Cisco ASA の構成：

```
object service testOperator
 service tcp source gt 100 destination neq 200
access-list acp1 extended permit object testOperator any any
```

変換先：

表 *47 :* ポート オブジェクト

名前	タイプ	ドメイン	値（プロトコル/ポート）	オーバーライド
testOperator_src	オブジェクト	なし	TCP(6)/101-65535	False
testOperator_dst_1	オブジェクト	なし	TCP(6)/1-199	False
testOperator_dst_2	オブジェクト	なし	TCP(6)/201-65535	False
testOperator_dst	グループ	なし	testOperator_dst_1、testOperator_dst_2	False

表 *48 :* アクセスコントロールルールまたはプレフィルタルール

名前	送信元ゾーン	宛先ゾーン	送信元ネットワーク	宛先ネットワーク	送信元ポート	宛先ポート	アクション	有効
acp1#1	任意	任意	任意	任意	testOperator_src	testOperator_dst	同等に許可	はい（True）

「lt」および「neq」演算子を使用するセキュリティオブジェクトがあるアクセスルール

Cisco ASA の構成：

```
object service testOperator
 service tcp source gt 100 destination lt 200
access-list acp1 extended permit object testOperator any any
```

変換先：

表 *49 :* ポート オブジェクト

名前	タイプ	ドメイン	値（プロトコル/ポート）	オーバーライド
testOperator_src	オブジェクト	なし	TCP(6)/101-65535	False
testOperator_dst	オブジェクト	なし	TCP(6)/1-199	False

表 *50 :* アクセスコントロールルールまたはプレフィルタルール

名前	送信元ゾーン	宛先ゾーン	送信元ネットワーク	宛先ネットワーク	送信元ポート	宛先ポート	アクション	有効
acp1#1	任意	任意	任意	任意	testOperator_src	testOperator_dst	同等に許可	はい（True）

「eq」演算子およびポートのリテラル値を使用したTCPサービスオブジェクトがあるアクセスルール

Cisco ASA の構成：

```
object service svcObj1
 service tcp source eq telnet destination eq ssh
access-list acp1 extended permit object testOperator any any
```

変換先：

表 *51 :* ポート オブジェクト

名前	タイプ	ドメイン	値（プロトコル/ポート）	オーバーライド
svcObj1_src	オブジェクト	なし	TCP(6)/21	False
svcObj1_dst	オブジェクト	なし	TCP(6)/22	False

表 *52 :* アクセスコントロールルールまたはプレフィルタルール

名前	送信元ゾーン	宛先ゾーン	送信元ネットワーク	宛先ネットワーク	送信元ポート	宛先ポート	アクション	有効
acp1#1	任意	任意	任意	任意	svcObj1_src	svcObj1_dst	同等に許可	はい（True）

Cisco ASA の構成：

```
object-group service icmpObj
 service-object icmp echo-reply 8
 access-list acp1 extended permit object icmpObj any any
```

変換先：

表 *53 :* ポートオブジェクト

名前	タイプ	ドメイン	値（プロトコル/ポート）	オーバーライド
icmpObj	オブジェクト	なし	ICMP(1)/Echo reply	False

変換の例

表 *54 :* アクセスコントロールルールまたはプレフィルタルール

名前	送信元ゾーン	宛先ゾーン	送信元ネットワーク	宛先ネットワーク	送信元ポート	宛先ポート	アクション	有効
acp1#1	任意	任意	任意	任意	任意	icmpObj	同等に許可	はい（True）

プロトコル サービス オブジェクトを使用するアクセスルール

Cisco ASA の構成：

```
object-group protocol testProtocol
 protocol-object tcp
access-list acp1 extended permit object testProtocol any any
```

変換先：

表 *55 :* ポートオブジェクト

名前	タイプ	ドメイン	値（プロトコル/ポート）	オーバーライド
testProtocol	オブジェクト	なし	TCP(6)	False

表 *56 :* アクセスコントロールルールまたはプレフィルタルール

名前	送信元ゾーン	宛先ゾーン	送信元ネットワーク	宛先ネットワーク	送信元ポート	宛先ポート	アクション	有効
acp1#1	任意	任意	任意	任意	任意	testProtocol	同等に許可	はい（True）

拡張済みサービスオブジェクトを使用するアクセスルール（送信元のみ）

Cisco ASA の構成：

```
object service serviceObj
 service tcp source eq 300
 service tcp source eq 800
access-list acp1 extended permit object serviceObj any any
```

変換先：

表 *57 :* ポート オブジェクト

名前	タイプ	ドメイン	値（プロトコル/ポート）	オーバーライド
serviceObj_src_1	オブジェクト	なし	TCP(6)/300	False
serviceObj_src_2	オブジェクト	なし	TCP(6)/800	False
serviceObj	グループ	なし	serviceObj_src_1 serviceObj_src_2	False

表 *58 :* アクセスコントロールルールまたはプレフィルタルール

名前	送信元ゾーン	宛先ゾーン	送信元ネットワーク	宛先ネットワーク	送信元ポート	宛先ポート	アクション	有効
acp1#1	任意	任意	任意	任意	任意	serviceObj	同等に許可	はい（True）

拡張済みサービスオブジェクトを使用するアクセスルール（送信元および接続先のみ）

Cisco ASA の構成：

```
object service serviceObj
 service tcp source eq 300 destination eq 400
access-list acp1 extended permit tcp object serviceObj any any
```

変換先：

表 *59 :* ポート オブジェクト

名前	タイプ	ドメイン	値（プロトコル/ポート）	オーバーライド
serviceObj_src	オブジェクト	なし	TCP(6)/300	False
serviceObj_dst	オブジェクト	なし	TCP(6)/400	False

表 *60 :* アクセスコントロールルールまたはプレフィルタルール

名前	送信元ゾーン	宛先ゾーン	送信元ネットワーク	宛先ネットワーク	送信元ポート	宛先ポート	アクション	有効
acp1#1	任意	任意	任意	任意	serviceObj_src	serviceObj_dst	同等に許可	はい（True）

送信元ポートのポート引数演算子「neq」を使用するアクセスルール

Cisco ASA の構成：

```
access-list acp1 extended permit tcp any neq 300
```

変換先：

表 *61 :* アクセスコントロールルールまたはプレフィルタルール

名前	送信元ゾーン	宛先ゾーン	送信元ネットワーク	宛先ネットワーク	送信元ポート	宛先ポート	アクション	有効
acp1#1	任意	任意	任意	任意	1-299、301-65535	任意	同等に許可	はい（True）

送信元ポートと宛て先ポートのポート引数演算子「neq」を使用するアクセスルール

Cisco ASA の構成：

```
access-list acp1 extended permit tcp any neq 300 any neq 400
```

変換先：

表 *62 :* アクセスコントロールとプレフィルタルール

名前	送信元ゾーン	宛先ゾーン	送信元ネットワーク	宛先ネットワーク	送信元ポート	宛先ポート	アクション	有効
acp1#1_1	任意	任意	任意	任意	1-299	1-399	同等に許可	はい（True）
acp1#1_2	任意	任意	任意	任意	301-65535	1-399	同等に許可	はい（True）
acp1#1_3	任意	任意	任意	任意	1-299	401-65535	同等に許可	はい（True）
acp1#1_4	任意	任意	任意	任意	301-65535	401-65535	同等に許可	はい（True）

非アクティブなアクセスルール

Cisco ASA の構成：

```
access-list acp1 extended permit tcp 3.4.5.0 255.255.255.0 5.6.7.0 255.255.255.0 inactive
access-group acp1 global
```

変換先：

表 *63 :* アクセスコントロールルールまたはプレフィルタルール

名前	送信元ゾーン	宛先ゾーン	送信元ネットワーク	宛先ネットワーク	送信元ポート	宛先ポート	アクション	有効
acp1#1	任意	任意	3.4.5.0/24	5.6.7.0/24	TCP(6)	任意	同等に許可	False

インバウンドトラフィックに適用されるアクセス制御リスト

Cisco ASA の構成：

```
access-list acp1 extended permit tcp 3.4.5.0 255.255.255.0 eq 90 any eq 80
access-group acp1 in inside
```

変換先：

表 *64 :* セキュリティゾーン/インターフェイスグループ

名前	インターフェイスタイプ	ドメイン	選択したインターフェイス
acp1_inside_in_zone	• ルーテッド（Cisco ASA デバイスがルーテッドモードで実行されている場合） • スイッチ（Cisco ASA デバイスが透過モードで実行されている場合）	なし	任意

表 *65 :* アクセスコントロールルールまたはプレフィルタルール

名前	送信元ゾーン	宛先ゾーン	送信元ネットワーク	宛先ネットワーク	送信元ポート	宛先ポート	アクション	有効
acp1#1	acp1_inside_in_zone	任意	3.4.5.0/24	任意	TCP(6)/90	TCP(6)/80	同等に許可	はい（True）

アウトバウンドトラフィックに適用されるアクセス制御リスト

Cisco ASA の構成：

```
access-list acp1 extended permit tcp 3.4.5.0 255.255.255.0 eq 90 any eq 80
access-group acp1 out outside
```

変換先：

表 *66 :* セキュリティゾーン/インターフェイスグループ

名前	インターフェイスタイプ	ドメイン	選択したインターフェイス
acp1_outside_out_zone	• ルーテッド（Cisco ASA デバイスがルーテッドモードで実行されている場合） • スイッチ（Cisco ASA デバイスが透過モードで実行されている場合）	なし	任意

表 *67 :* アクセスコントロールルールまたはプレフィルタルール

名前	送信元ゾーン	宛先ゾーン	送信元ネットワーク	宛先ネットワーク	送信元ポート	宛先ポート	アクション	有効
acp1#1	acp1_outside_out_zone	任意	3.4.5.0/24	任意	TCP(6)/90	TCP(6)/80	同等に許可	True

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。