ファイアウォール アクセス ルールの管理

アクセス ルールでは、トラフィックがインターフェイスを通過するために満たす必要のあるルールを定義します。着信トラフィックのルールを定義した場合、そのルールが他のどのポリシーよりも先にトラフィックに適用されます（ただし、一般的でない AAA ルールは例外です）。このため、アクセス ルールは防御の最前線となります。

デバイスの一部のタイプでは、IPv4 アクセス ルールに加えて IPv6 アクセス ルールを設定できます。サポートされているデバイスタイプについては、「Security Manager での IPv6 サポート」（8 ページ）を参照してください。

アクセス ルールの概要および使用方法については、次の項を参照してください。

アクセス ルールについて

アクセス ルール ポリシーでは、インターフェイスを通過するトラフィックを許可または拒否するルールを定義します。通常は、インターフェイスに入るトラフィックのアクセスルールを作成します。これは、特定タイプのパケットを拒否する場合、デバイスがパケットの処理に多くの時間を費やす前にパケットを拒否する方が有効なためです。

アクセス ルールは、デバイスに展開されると、インターフェイスに接続されているアクセス コントロール リスト（ACL）の 1 つ以上のエントリ（ACE）となります。通常、これらのアクセス ルールが、パケットに最初に適用されるセキュリティ ポリシーとなります。つまり、防御の最前線となります。アクセス ルールを使用して、サービス（プロトコルとポート番号）、

送信元アドレス、および宛先アドレスに基づいて、トラフィックを許可または拒否（ドロップ）することにより、望ましくないトラフィックをフィルタリングして除外します。インターフェイスに到着したパケットごとに、指定した基準に基づいてパケットを転送するかドロップするかが決定されます。Out 方向のアクセス ルールを定義した場合、パケットは、インターフェイスを出ていくときにも分析されます。

ヒント　ASA 8.3+ デバイスの場合は、グローバルなアクセス ルールを使用して、インターフェイス固有のアクセス ルールを増強できます。詳細については、グローバル アクセス ルールについて（3 ページ）を参照してください。

アクセスルールでトラフィックを許可しても、後続のポリシーによってそのトラフィックが最終的にドロップされることがあります。たとえば、インスペクションルール、Web フィルタルール、およびゾーンベースのファイアウォールルールは、パケットがインターフェイスのアクセスルールに合格したあとに適用されます。この場合、これらの後続のルールによって、さらに深いトラフィック分析に基づいてトラフィックがドロップされることがあります。たとえば、パケット ヘッダーが検査要件を満たしていない場合や、Web 要求の URL が望ましくない Web サイトに対応している場合などです。

このため、アクセス ルールを定義する際は、作成する他のタイプのファイアウォール ルールについて慎重に検討する必要があります。検査する必要があるトラフィックに対しては、アクセスルールで全面的な拒否ルールを作成しないでください。一方、特定のホストやネットワークを起点または宛先とするサービスをどのような場合にも許可しないことがわかっている場合は、アクセス ルールを使用してトラフィックを拒否してください。

アクセスルールの順序に留意してください。つまり、デバイスは、ルールに基づいてパケットを比較するとき、上から下に検索を行い、一致した最初のルールに対するポリシーを適用します。それ以降のルールは、（最初のルールより一致率が高くても）すべて無視されます。したがって、特定のルールが無視されないようにするには、そのルールを汎用性の高いルールよりも上に配置する必要があります。IPv4 ルールがまったく一致しないケースを特定する場合、および冗長なルールを特定する場合は、自動競合検出ツールやポリシークエリツールを使用すると便利です。詳細については、自動競合検出の使用　（37 ページ）およびポリシー クエリー レポートの生成を参照してください。

次の方法でも、アクセス ルールを評価できます。

- ルールを結合する：IPv4 ルールを評価するためのツールを使用し、各ルールを結合することによって、より少ない数のルールで同じ機能を実行できます。これにより、ルールのリストが縮小され、管理が簡単になります。詳細については、ルールの結合を参照してください。
- ヒット カウントを生成する：IPv4 および IPv6 ACL のデバイスで管理されるヒット カウント統計を表示するためのツールを使用できます。これにより、ルールでトラフィックが許可または拒否された頻度がわかります。詳細については、ヒットカウントの詳細の表示（48 ページ）を参照してください。
- CS-MARS により収集されたイベントを表示する：デバイスをモニタするように Cisco Security Monitoring, Analysis and Response System アプリケーションを設定した場合、およ

びsyslogメッセージを生成するようにルールを設定した場合は、このアプリケーションを使用して、IPv4ルールに関連するリアルタイムのイベントと過去のイベントを分析できます。詳細については、IPS シグニチャの CS-MARS イベントの表示を参照してください。

アクセス ルールの概念的な詳細については、次の項を参照してください。

- グローバル アクセス ルールについて （3 ページ）
- デバイス固有のアクセス ルールの動作について （5 ページ）
- アクセス ルールのアドレス要件およびルールの展開方法について （6 ページ）

関連項目

- アクセス ルールの設定 （8 ページ）
- アクセス ルールの有効期限の設定 （29 ページ）
- アクセス コントロール ポリシー設定の指定 （30 ページ）
- 検出中のオブジェクト グループの展開
- ルールのインポート （55 ページ）
- ルールの追加および削除
- ルールの編集
- ルールのイネーブル化とディセーブル化
- ルールの移動とルール順序の重要性

グローバル アクセス ルールについて

アクセルルール（ACL）は、どのトラフィックがデバイスを通過できるかを制御するものであり、従来からデバイス インターフェイスに適用されています。ただし、ソフトウェア リリース 8.3+ が動作している ASA デバイスを使用している場合は、IPv4 および IPv6 に対してグローバル アクセス ルールを作成することもできます。

グローバル アクセス ルールは、デバイス上のインターフェイスごとに、インターフェイスに入るトラフィックに対して処理される特殊な ACL として定義します。このため、ACL はデバイスで 1 回だけ設定されますが、In 方向に対して定義されたインターフェイス固有のセカンダリ ACL のように機能します（グローバル ルールは常に、Out 方向ではなく In 方向に適用されます）。

ASA 8.3+ デバイス上のインターフェイスにトラフィックが入ると、デバイスは、ACL を適用する際に、まずインターフェイス固有のアクセスルールをトラフィックに適用します。次に、グローバル ルールを適用します（全体的な処理については、ファイアウォール ルールの処理順序についてを参照してください）。

着信インターフェイスに関係なくデバイスに入ってくるすべてのトラフィックに適用するルールには、グローバル ルールを使用すると最適です。たとえば、常に拒否または常に許可する特定のホストまたはサブネットがあるとします。これらをグローバル ルールとして作成すると、デバイス上で1回だけ設定すれば、各インターフェイスに対して繰り返し設定する必要がありません（機能的には、[All-Interfaces] ロールに対してインターフェイス固有のルールを設定した場合と同じですが、[All-Interfaces] ルールはデバイス上で 1 回だけ設定するのではなく、各インターフェイスに対して繰り返して設定します）。

ヒント 複数のデバイスに対して同じグローバル ルール セットを設定する場合は、共有ポリシーを作成して、デバイスごとに IPv4 または IPv6 アクセス ルール ポリシー内に継承します。すべてのグローバル ルールを共有ポリシーの [Default] セクション内に配置する必要があります。いずれかのグローバル ルールを [Mandatory] セクションに配置した場合は、ローカルなインターフェイス固有のアクセス ルールが定義されているデバイス上でそのルールを継承できなくなります。共有ポリシーおよび継承ポリシーの詳細については、ローカルポリシーと共有ポリシーおよびルールの継承についてを参照してください。

Security Manager で ASA 8.3+ デバイスに対してアクセス ルールを設定する場合、インターフェイス固有のルールとグローバル ルールは同じポリシー内に設定されます。ただし、デバイスでは常にインターフェイス固有のルールが最初に処理されるため、Security Manager ではこれらの異なるタイプのルールを混在させることはできません。そのため、1 つのデバイス上でインターフェイス固有のルールとグローバルルールの両方を設定する場合は、次の点に注意してください。

- アクセス ルール ポリシー内では、常にグローバル ルールが最後に処理されます。インターフェイス固有のルールはいずれも、グローバル ルールよりも先に処理されます。
- 決められた順序に違反するようなルールの移動はできません。たとえば、インターフェイス固有のルールをグローバル ルールの下に移動したり、グローバル ルールをインターフェイス固有のルールの上に移動したりすることはできません。
- 決められた順序に違反する場所にルールを作成することはできません。たとえば、インターフェイス固有のルールを選択し、インターフェイス固有の別のルールをテーブル内でその次に配置した場合、グローバル ルールを作成することはできません。間違った種類のルールを作成しようとすると、ルールを保存するときに、Security Manager によって、ルールを最も近い有効な場所に作成できるかどうか尋ねられます。この提案を受け入れないと、ルールはテーブルに追加されません。提案された場所が不適切な場合は、ルールの作成後にいつでもルールを移動できます（ただし、ルールの順序に違反しない場合にかぎります）。
- 決められた順序に継承ポリシー内のルールが違反する場合、そのポリシーは継承できません。たとえば、デバイス ポリシー内にグローバル ルールを作成し、[Default] セクション内でインターフェイス固有のルールを含む共有ポリシーを継承しようとすると、Security Manager でそのポリシーが継承できなくなります。
- 共有ポリシーの割り当て後または継承後は、そのポリシーを使用するデバイス上のルール順序に違反するようなポリシーの編集はできません。

- グローバル ルールをサポートしていないデバイス上で、グローバル ルールを含むポリシーを割り当てまたは継承した場合、そのデバイスではすべてのグローバル ルールが無視され、設定はされません。たとえば、共有ポリシー内のグローバル ルールでホスト 10.100.10.10 からのすべてのトラフィックを許可し、そのポリシーを IOS デバイスに割り当てた場合、10.100.10.10 アクセスを許可するルールは IOS デバイス上では設定されません。そのホストからのトラフィックは、別のインターフェイス固有ポリシーか、またはデフォルトの deny all ポリシーによって処理されます。グローバル ルールをサポートしないデバイスには、グローバル ルールを含む共有ポリシーを割り当てないようにすることを推奨します。そうすれば、グローバル ルールで定義されているポリシーが、サポートされていないデバイスで設定されていると誤解することがありません。

また、特定のツールでグローバル ルールが処理される方法に関して、いくつかの変更点があります。

- Find/Replace：グローバル ルールは、Global というインターフェイス名を使用して検索できます。ただし、グローバル ルールとインターフェイス固有のルールを変換する方法はありません。グローバル ルールはグローバル インターフェイス名を使用して検索できますが、インターフェイス名を「Global」という名前で置換しようとすると、実際には Global という名前のポリシー オブジェクトを使用する、インターフェイス固有のアクセス ルールが作成されます。
- Rule Combiner：インターフェイス固有のルールとグローバル ルールが結合されることはありません。

関連項目

- グローバル アクセス ルールについて （3 ページ）
- デバイス固有のアクセス ルールの動作について （5 ページ）
- アクセス ルールのアドレス要件およびルールの展開方法について （6 ページ）
- アクセス ルールの設定 （8 ページ）
- ルールの移動とルール順序の重要性

デバイス固有のアクセス ルールの動作について

次に、アクセス ルール ポリシーを作成しない場合のデフォルトの動作をデバイス タイプに基づいて示し、アクセス ルールを作成したときに行われる処理を示します。

- IOS デバイス：インターフェイスを通過するすべてのトラフィックを許可します。

送信元 A から宛先 B へのトラフィックを許可しているものの、インスペクション ルール テーブルに TCP/UDP インスペクションを設定していないか、ルールに [established] 拡張オプションを設定していない場合、デバイスは A から B へのパケットをすべて許可します。ただし、B から A に戻るパケットについては、そのパケットを許可するためのアクセス ルールがないかぎり、パケットは許可されません。トラフィックのインスペクション ルール テーブルに TCP/UDP

インスペクションを設定した場合、BからAに戻るパケットはいずれも自動的にデバイスを通過するため、アクセス ルール内に B から A を許可するルールは必要ありません。

- ASA および PIX デバイス：高いセキュリティのインターフェイスから低いセキュリティのインターフェイスへのトラフィックを許可します。それ以外のトラフィックはすべて拒否されます。

アクセス ルールで単方向の TCP/UDP トラフィックが許可されている場合、アプライアンスによりリターン トラフィックが自動的に許可されます（リターン トラフィックのためのルールを設定する必要はありません）。ただし、ICMP トラフィックの場合は例外で、リターン ルールが必要となります（逆方向の送信元および宛先を許可します）。あるいは、ICMP のインスペクション ルールを作成する必要があります。

- FWSMデバイス：インターフェイスに入るすべてのトラフィックを拒否し、インターフェイスを出るすべてのトラフィックを許可します。

デバイスに入るすべてのトラフィックを許可するためのアクセスルールを設定する必要があります。

任意のタイプのデバイスに対してインターフェイスのルールを作成すると、デバイスによってポリシーの最後に暗黙的な [deny any] ルールが追加されます。このルールは、場所を忘れないように自分で追加することを推奨します。また、ルールを追加すると、ルールのヒットカウント情報を取得できます。詳細については、ヒットカウントの詳細の表示 （48 ページ）を参照してください。

ヒント アクセス ルール ポリシーを作成する場合、Security Manager サーバからデバイスへのアクセスを許可するルールを含める必要があります。そうしない場合、この製品を使用してデバイスを管理できなくなります。

関連項目

- アクセス ルールについて （1 ページ）
- アクセス ルールのアドレス要件およびルールの展開方法について （6 ページ）

アクセス ルールのアドレス要件およびルールの展開方法について

コマンドライン インターフェイス（CLI）でオペレーティング システム コマンドを使用してアクセス制御リストを作成する場合の複雑な点の1つは、送信元アドレスと宛先アドレスのIPアドレス形式がオペレーティングシステムで異なっていることです。

たとえば、Cisco IOS Software では、サブネット マスクではなくワイルドカード マスクを使用してアドレスを入力する必要があります。10.100.10.0/24 ネットワーク（サブネット マスク 255.255.255.0）のルールを作成するには、アドレスを 10.100.10.0 0.0.0.255 として入力する必要があります。ワイルドカードマスクとサブネットマスクでは、0 と 1 の意味が逆になります。

ただし、ASA、PIX、および FWSM ソフトウェアでは、サブネットマスクを使用するため、10.100.10.0 255.255.255.251 と入力します。

Security Manager では、アクセス ルールのアドレッシング要件が単純化されており、常にサブネット マスクを使用します。ワイルドカード マスクは入力できません。アクセス ルールをデバイスに展開すると、Security Manager によって、デバイスのオペレーティング システムが考慮され、必要に応じてサブネット マスクがワイルドカード マスクに自動変換されます。

このため、論理ポリシーに基づいて共有ルールを作成して、すべてのデバイスに適用することが可能になります。たとえば、すべてのデバイスで使用するアクセス ルール セットがある場合は、共有ポリシーを作成して、それをすべてのデバイスの継承ポリシーとして割り当てます。デバイスタイプごとに「適切な」構文を使用してルールを定義する必要はありません。他のポリシー タイプで使用する同じネットワーク/ホスト オブジェクトを使用して、対象のホストおよびネットワークを識別できます。

展開された設定内に生成される特定の CLI コマンドも、デバイス タイプに基づきます。IOS デバイスの場合、**ip access-list** コマンドを使用します。ASA、PIX、FWSM デバイスの場合、**access-list** または **ipv6 access-list** コマンドを使用し、**access-group** コマンドを使用してインターフェイスにバインドします。ASA、PIX、FWSM、および IOS 12.4(20)T 以降のデバイスでは、ネットワーク/ホストオブジェクトを使用してルールの送信元アドレスまたは宛先アドレスを識別する場合、それらのネットワーク/ホストオブジェクトに対してオブジェクトグループを作成するために、**object-group** コマンドを使用します。また、サービス オブジェクトに対してもオブジェクト グループが作成されます。

ヒント

- ネットワーク/ホスト オブジェクトを使用してルールの送信元アドレスや宛先アドレスを識別でき、またルールに対して展開の最適化を設定できるため、アクセス ルールと ACL の CLI 定義内の ACE が必ずしも 1 対 1 の関係になるとはかぎりません。
- ファイアウォール ルールから作成されるアクセス リストはすべて、（標準アクセス リストではなく）拡張アクセス リストです。[Access Control Settings] ページ （31 ページ）で ACL の名前を指定していない場合、Security Manager によってシステム生成名が ACL に適用されます。この名前は、名前が定義されているインターフェイスおよび方向に関連するすべてのルールが含まれる ACL に適用されます。
- オブジェクト グループの展開方法を制御する展開オプションがいくつかあります。この項では、デフォルトの動作について説明します。[Deployment] ページ（**[ツール（Tools）] > [Cisco Security Manager管理（Security Manager Administration）] > [展開（Deployment）]** を選択）で、ネットワーク/ホストオブジェクトからオブジェクトグループを作成するためのオプションの選択を解除できます。また、展開中にオブジェクト グループを最適化したり（ファイアウォール ルールの展開時のネットワーク オブジェクト グループの最適化 を参照）、複数のサービスまたは送信元アドレスや宛先アドレスを持つルールから新しいオブジェクト グループを作成したり、使用していないオブジェクト グループを削除したりできます。
- 展開オプションには、アクセス ルールから生成される ACL の名前および作成される ACL の数を制御する設定も含まれます。デフォルトでは、Security Manager により、インター

フェイスごとに一意の ACL が作成されます。このため、複数の重複する ACL が作成されることがあります。

[ファイアウォールルールに対するACL共有の有効化（Enable ACL Sharing for Firewall Rules）] を選択した場合、Cisco Security Manager は単一の ACL を作成して複数のインターフェイスに適用できるため、重複する不要な ACL は作成されません。ただし、ACL の共有が行われるのは、ACL 命名要件が保たれている間に実行できる場合にかぎります。

- インターフェイスおよび方向に対して ACL 名を指定した場合は、その名前が常に使用されます。このため、重複する ACL が作成されることがあります。詳細については、アクセス コントロール ポリシー設定の指定 （30 ページ）を参照してください。
- [ファイアウォールアクセルリスト名（Firewall Access-List Names）] プロパティの [既存の名前を再利用（Reuse Existing Names）] を選択すると、既存の名前は保存されます（アクセス制御設定ポリシーで名前をオーバーライドした場合を除く）。つまり、重複する ACL がデバイスにすでに存在する場合は、異なる名前で ACL が重複して作成されます。

ヒント：ACL 共有を最大限に利用するには、[ファイアウォールアクセスリスト名（Firewall Access-List Names）] プロパティに [CS-Managerの生成名にリセット（Reset to CS-Manager Generated Names）] を選択し、[アクセスルールの展開の最適化対象（Optimize the Deployment of Access Rules For）] プロパティに [速度（Speed）] を選択する必要があります。アクセス制御設定ポリシー内に ACL 名は設定しないでください。

[ファイアウォールルールに対するACL共有の有効化（Enable ACL Sharing for Firewall Rules）] プロパティの詳細については、[Deployment] ページを参照してください。

- IPv4 および IPv6 ACL は同じ名前を持てません。

関連項目

- アクセス ルールについて （1 ページ）
- アクセス ルールの設定 （8 ページ）
- アクセス コントロール ポリシー設定の指定 （30 ページ）
- 検出中のオブジェクト グループの展開

アクセス ルールの設定

アクセス ルール ポリシーでは、トラフィックがインターフェイスを通過することを許可するためのルールを定義します。アクセス ルール ポリシーを設定しない場合、デバイス固有のアクセス ルールの動作について （5 ページ）に説明するように、デバイスの動作はデバイス タイプによって異なります。

（注） Security Manager 4.4 およびバージョン 9.0 以降の ASA のリリースより前は、IPv4 および IPv6 ファイアウォールルールとポリシーを設定するための個別のページ、ポリシー、およびポリシーオブジェクトが提供されていました。Cisco Security Manager 4.4 と ASA のバージョン 9.0 以降では、これらのポリシーとポリシーオブジェクトが「統合」されました。つまり、IPv4 または IPv6 アドレス、あるいは両方のアドレスを使用できる一組のアクセスルールになりました（詳細については、Cisco Security Manager 4.4 でのポリシーオブジェクトの変更を参照してください）。ただし、以前の ASA バージョンでは、IPv6 アクセスルールの別のページが引き続きデバイスビューで提供されますが、ポリシービューでは、IPv4 および統合バージョンのアクセスルールポリシータイプが提供されます。さらに、既存の IPv4 ポリシーの変換に使用できるユーティリティが提供されています（IPv4 ルールから統合ルールへの変換を参照）。次の説明は、特に明記されている場合を除き、アクセスルールテーブルのすべてのバージョンに適用されます。IPv4 アクセスルール共有ポリシーを 9.0 以降のデバイスに割り当てると、それらのポリシーの統合バージョンをそのデバイスに割り当てることはできなくなります。同様に、統合 アクセスルール共有ポリシーを 9.0 以降のデバイスに割り当てると、それらの共有ポリシーの IPv4 バージョンをそのデバイスに割り当てることはできなくなります。そのデバイスは、共有ポリシーの [割り当て（Assignments）] タブの使用可能なデバイスのリストには含まれなくなります。

アクセス ルールを設定する前に、これから設定する他のタイプのファイアウォール ルールについて検討してください。アクセスルールは、他のタイプのルール（AAA ルールを除く）よりも先に処理されます。検討する必要のある事項の詳細については、次の項を参照してください。

- アクセス ルールについて （1 ページ）
- グローバル アクセス ルールについて （3 ページ）
- アクセス ルールのアドレス要件およびルールの展開方法について （6 ページ）

はじめる前に

アクセス ルール セットをすべてのデバイスに適用するとします。このためには、共有ルールを作成して、そのルールを各デバイスのアクセスルールポリシーに継承します。詳細については、新しい共有ポリシーの作成およびルールの継承または継承の解除を参照してください。

関連項目

- セクションを使用したルール テーブルの編成
- デバイス間でのポリシーのコピー
- デバイス ビューまたは Site-to-Site VPN Manager における共有ポリシーの使用
- ネットワーク/ホストオブジェクトについて
- インターフェイス ロール オブジェクトについて
- サービスとサービス オブジェクトおよびポート リスト オブジェクトの理解と指定

ステップ 1 次のいずれかを実行して、[Access Rules] ページ （12 ページ）を開きます。

- （デバイスビュー）ポリシーセレクタから **[ファイアウォール（Firewall）]>[アクセスルール（Access Rules）]**（または **[ファイアウォール（Firewall）] > [設定（Settings）] > [IPv6アクセスルール（IPv6 Access Rules）]**）を選択します。
- （ポリシービュー）ポリシータイプセレクタから **[ファイアウォール（Firewall）] > [アクセスルール（Access Rules）]**（または **[ファイアウォール（Firewall）] > [設定（Settings）] > [IPv6アクセスルール（IPv6 Access Rules）]**）を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

ステップ 2 ルールを作成する行を選択して [行の追加（Add Row）] ボタンをクリックするか、または行を右クリックして [行の追加（Add Row）] を選択します。[Add Access Rule]/[Edit Access Rule] ダイアログボックス （18 ページ）が開きます。

ヒント 行を選択しなかった場合、新しいルールはローカル範囲の最後に追加されます。既存の行を選択して、行全体または特定のセルを編集することもできます。詳細については、ルールのイネーブル化とディセーブル化を参照してください。1 つのポリシー内にインターフェイス固有のルールとグローバル ルールを混在させた場合は、特殊なルールが適用されます。詳細については、グローバル アクセス ルールについて （3 ページ）を参照してください。

ステップ 3 ルールを設定します。次に、ルールの設定時に判断が必要となることが多い重要な点を示します。フィールドを設定する方法の詳細については、[Add Access Rule]/[Edit Access Rule] ダイアログボックス （18 ページ）を参照してください。

- 許可または拒否：ルールに一致したトラフィックを許可するか、またはドロップするか。
- 送信元アドレスおよび宛先アドレス：トラフィックを生成したアドレスまたはその宛先にかかわらず、ルールを適用する場合は、送信元または宛先に「All-Addresses」を使用します。ルールがホストまたはネットワークに固有の場合は、アドレスまたはネットワーク/ホストオブジェクトを入力します。受け入れられるアドレス形式の詳細については、ポリシー定義中の IP アドレスの指定を参照してください。
- 送信元および宛先のセキュリティグループ（ASA 9.0+ のみ）：送信元および宛先アドレスに加えて、トラフィックのフィルタリングに使用される TrustSec セキュリティグループを指定できます。セキュリティグループの詳細については、ポリシーでのセキュリティグループの選択、TrustSec ベースのファイアウォールルールの設定、およびセキュリティ グループ オブジェクトの作成を参照してください。
- 送信元ユーザー（ASA 8.4.2 以降のみ）：Active Directory（AD）ユーザー名（NetBIOS_DOMAIN\username 形式）、ユーザーグループ（NetBIOS_DOMAIN\\user_group）、または名前とグループを定義するアイデンティティ ユーザー グループ オブジェクトを指定して、トラフィックの送信元をさらに定義できます。ユーザ指定は送信元アドレスと結合され、送信元アドレス範囲の中で照合するユーザ アドレスを制限します。詳細については、アイデンティティ ベースのファイアウォール ルールの設定およびアイデンティティ ユーザ グループ オブジェクトの作成を参照してください。
- サービス：IP サービスを使用して、すべてのトラフィックに適用します（たとえば、特定の送信元からのすべてのトラフィックを拒否する場合）。または、対象となるより具体的なサービス（プロトコルとポートの組み合わせ）を選択します。

- インターフェイスまたはグローバル：ルールを設定するインターフェイスまたはインターフェイス ロールを選択するか、ASA 8.3+ デバイスでグローバル アクセス ルールを作成する場合は [Global] を選択します（グローバル アクセス ルールについて （3 ページ）を参照）。
- 詳細設定：[詳細設定（Advanced）] をクリックして、追加設定を行うための [詳細設定（Advanced）] ダイアログボックスを開きます。次のオプションを設定できます。詳細については、[Advanced]/[Edit Options] ダイアログボックス （23 ページ）を参照してください。
  - ロギング オプション。Security Manager または CS-MARS を使用してデバイスをモニタしている場合は、ロギングをイネーブルにする必要があります。
  - このルールを適用するトラフィックの方向（[in] または [out]）。デフォルトは [入力（in）] です。グローバルルールでは、この設定を変更できません。
  - ルールの時間範囲。これにより、特定の期間中（勤務時間中など）だけ有効になるルールを設定できます。詳細については、時間範囲オブジェクトの設定を参照してください。
  - フラグメンテーションを行い、確立されたアウトバウンド セッションのトラフィックのリターンを許可するための IOS デバイス オプション。
  - ルールの有効期限および通知の設定。詳細については、アクセス ルールの有効期限の設定 （29 ページ）を参照してください。

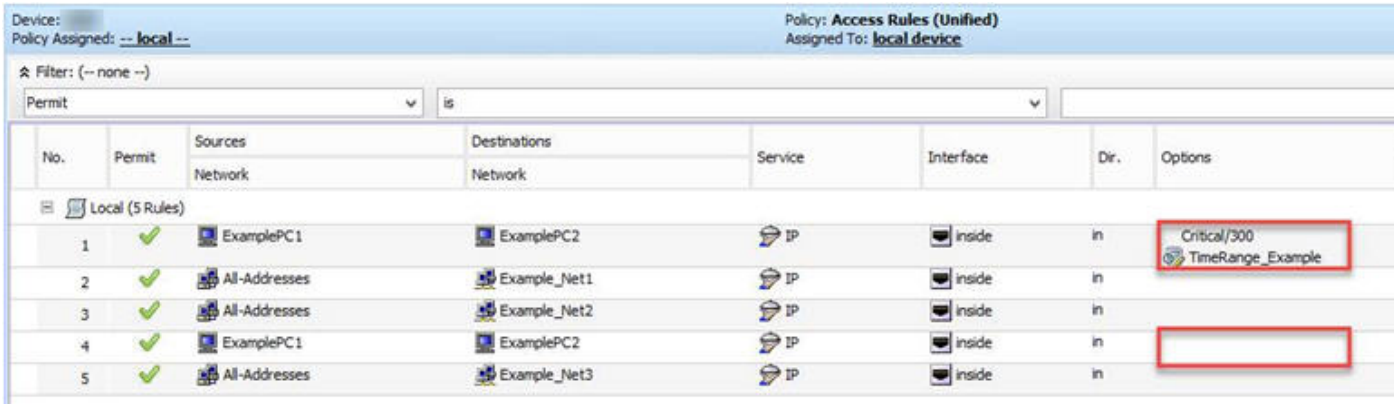
ステップ 4 ルールの定義が完了したら、[OK] をクリックします。

（注） 競合検出をイネーブルにして（競合検出の有効化 （43 ページ）を参照）、新しいルールが他のルールと競合または重複しているかどうかを確認できます。詳細については、自動競合検出の使用 （37 ページ）を参照してください。

ルールを追加または編集しているときに、時間範囲またはロギング値（[Advanced]/[Edit Options] ダイアログボックス （23 ページ）で定義）の違いを除いて、任意の 2 つのルールが同一になる場合があります（例：図 1 : 同一のルール （12 ページ）の 1 と 2）。

- Cisco Security Manager では、一番下にあるルールのみが展開されます（図 1 : 同一のルール （12 ページ）の 2）。
- 設定のプレビューでの設定変更の識別には、ルール（2）のみが使用されます。（設定のプレビューを参照）。
- ルール（2）がデバイスに展開されている場合、設定のプレビューでは変更が検出されません。

図 *1 :* 同一のルール



ステップ 5 Cisco Security Manager による最上位のルール（図 1 : 同一のルール （12 ページ）の 1）の展開を阻止している最下位のルール（例：図 1 : 同一のルール （12 ページ）の（2））を特定する必要がある場合は、次の手順を実行します。

a) デバイスで、競合検出の有効化 （43 ページ） 。

b) 見つかった競合について、レポートの作成（Generate Report） （43 ページ）。

c) レポートの[ルール番号（Rule No）] の 列で最下位のルール （2）を見つけ、競合するルール番号を特定し（ルール（1））、必要に応じてルール（1）を削除します。

ステップ 6 適切な行を選択しないでルールを追加した場合は、追加されたルールを選択し、上下の矢印ボタンを使用して適切な位置にルールを移動します。詳細については、ルールの移動とルール順序の重要性を参照してください。インターフェイス固有のルールとグローバル ルールを混在させた場合には、ルールの移動に関する特別な制約はありません（ グローバル アクセス ルールについて （3 ページ）を参照）。

ステップ 7 すでに多数のルールが存在している場合は、新しいルールを展開する前に、ルールを分析して結合することを検討します。競合検出ツールを使用して、ルールを分析できます（ 自動競合検出の使用 （37 ページ）を参照）。分析により冗長なルールが多数あることが示された場合は、ルールテーブル内の任意の場所を右クリックして [ルールの結合（Combine Rules）] を選択し、ルールを結合します。ルール結合ツールを起動する前に、Security Manager で結合についてすべてのルールを評価するか、選択したルールだけを評価するかを選択できます。詳細については、ルールの結合を参照してください。

[Access Rules] ページ

[アクセスルール（Access Rules）] ページを使用して、デバイスインターフェイスに対してアクセスコントロールルールを設定します。アクセス ルール ポリシーでは、インターフェイスを通過するトラフィックを許可または拒否するルールを定義します。通常は、インターフェイスに入るトラフィックのアクセスルールを作成します。これは、特定タイプのパケットを拒否する場合、デバイスがパケットの処理に多くの時間を費やす前にパケットを拒否する方が有効なためです。アクセス ルールは、他のタイプのファイアウォール ルールよりも先に処理されます。

（注） Cisco Security Manager 4.4 のリリースと ASA のバージョン 9.0 以降では、IPv4 および IPv6 アクセスルールを設定するための個別のポリシーとオブジェクトが「統合」されました。つまり、IPv4 または IPv6 アドレス、あるいは両方のアドレスをどちらも使用できる一組のアクセスルールになりました。（詳細については、Cisco Security Manager 4.4 でのポリシーオブジェクトの変更を参照してください。）ポリシービューでは、アクセスポリシータイプの IPv4 および統合バージョンが提供されます。さらに、既存の IPv4 ポリシーの変換に使用できるユーティリティが提供されています（IPv4 ルールから統合ルールへの変換を参照）。以下の説明は、特に明記されている場合を除き、アクセスルールテーブルのすべてのバージョンに適用されます。

アクセス ルールを設定する前に、次の項を参照してください。

- アクセス ルールについて （1 ページ）
- グローバル アクセス ルールについて （3 ページ）
- デバイス固有のアクセス ルールの動作について （5 ページ）
- アクセス ルールのアドレス要件およびルールの展開方法について （6 ページ）
- アクセス ルールの設定 （8 ページ）

ヒント 無効なルールはグレー表示されます。設定を展開すると、ディセーブルなルールはデバイスから削除されます。詳細については、ルールのイネーブル化とディセーブル化を参照してください。

ナビゲーション パス

[Access Rules] ページを開くには、次のいずれかを実行します。

- （デバイスビュー）デバイスを選択し、次にポリシーセレクタから **[ファイアウォール（Firewall）] > [アクセスルール（Access Rules）]**（または **[ファイアウォール（Firewall）] > [設定（Settings）] > [IPv6アクセスルール（IPv6 Access Rules）]**）を選択します。
- （ポリシービュー）ポリシータイプセレクタから **[ファイアウォール（Firewall）] > [アクセスルール（Access Rules）]**（または **[ファイアウォール（Firewall）] > [設定（Settings）] > [IPv6アクセスルール（IPv6 Access Rules）]**）を選択します。新しいポリシーを作成するか、または既存のポリシーを選択します。
- （マップビュー）デバイスを右クリックし、**[ファイアウォールポリシーの編集（Edit Firewall Policies）] > [アクセスルール（Access Rules）]**（または **[ファイアウォールポリシーの編集（Edit Firewall Policies）] > [IPv6アクセスルール（IPv6 Access Rules）]**）を選択します。

関連項目

- アクセス ルールの有効期限の設定 （29 ページ）
- アクセス コントロール ポリシー設定の指定 （30 ページ）
- ルールの追加および削除
- ルールの編集
- ルールのイネーブル化とディセーブル化
- ルールの移動とルール順序の重要性
- セクションを使用したルール テーブルの編成
- ルール テーブルの使用
- テーブルのフィルタリング

フィールド リファレンス

（注） 自動競合検出機能の一部として使用できるフィールドとユーザーインターフェイス要素の詳細については、 自動競合検出のユーザー インターフェイスについて （40 ページ）を参照してください。

表 1 : [Access Rules] ページ

要素	説明
[すべての行を展開する（Expand all rows）]/[すべての行を折りたたむ（Collapse all rows）]	ルールテーブルのすべてのセクションを展開または折りたたむには、これらのボタンを使用します。 （注） ボタンは、アクセスルールテーブルの上にある [フィルタ（Filter）] 領域の右上隅にあります。
[競合インジケータ（Conflict Indicator）] アイコン	競合を識別し、競合のタイプをすばやく視覚的に表現します。競合の種類や、この列から実行できるアクションなどの詳細については、自動競合検出のユーザーインターフェイスについて （40ページ）を参照してください。
番号	順序が付けられたルール番号。
許可（Permit）	設定された次の条件に基づいて、ルールがトラフィックを許可または拒否するかどうか。 • [Permit]：緑色のチェック マークとして表示されます。 • [Deny]：スラッシュの入った赤色の丸として表示されます。

要素	説明
ソース	このルールのトラフィック ソース。つまり、ネットワーク、セキュリティ グループ（ASA 9.0 以降のみ）、およびユーザーになります。複数のエントリは、テーブル セル内の個別の行に表示されます。
宛先	このルールの宛先。つまり、ネットワークおよびセキュリティ グループになります（ASA 9.0 以降のみ）。複数のエントリは、テーブル セル内の個別の行に表示されます。
サービス	ルールが適用されるトラフィックのプロトコルおよびポートを指定するサービスまたはサービス オブジェクト。複数のエントリは、テーブル セル内の個別の行に表示されます。サービスとサービス オブジェクトおよびポート リスト オブジェクトの理解と指定を参照してください。
ヒット カウント（Hit Count）	このルールが「ヒット」された回数。つまり、トラフィックを許可または拒否した回数です。実際には、ルールによって作成されたすべてのアクセス制御エントリ（ACE）のヒットカウントの合計となります。この情報は、展開されたポリシーをデバッグする際に役立ちます。 ヒット情報を更新するには、このページの下部にある [ヒットカウントの更新（Refresh Hit Count）] ボタンを使用します。 [Hit Count Selection Summary] ダイアログボックス （26 ページ）が開きます。 （注） 同じルール内または異なるルール内の重複した ACE のヒットカウントは、常に 0 に設定されます。 このセルを右クリックして [ヒットカウントの詳細を表示（Show Hit Count Details）] を選択すると、[Configuration Manager] ウィンドウの下部にある [ヒットカウントの詳細（Hit Count Details）] ペインを開くことができます。詳細については、 ヒットカウントの詳細の表示 （48 ページ）を参照してください。
前回のヒット時刻（Last Hit Time）	最新のヒットのタイムスタンプ。

要素	説明
インターフェイス	ルールが割り当てられるインターフェイスまたはインターフェイス ロール。インターフェイス ロール オブジェクトは、各デバイスの設定が生成されるときに、実際のインターフェイス名で置き換えられます。複数のエントリは、テーブルセル内の個別の行に表示されます。インターフェイス ロール オブジェクトについてを参照してください。 ASA 8.3+ デバイスの場合、グローバルルールには **Global** という名前が付き、インターフェイスまたはインターフェイスロールの名前を使用するルールと区別するための特別なアイコンが示されます（アイコンの説明については、ポリシー定義中の IP アドレスの指定を参照してください）。
Dir.	このルールが適用されるトラフィックの方向。 • [In]：インターフェイスで受信するパケット。 • [Out]：インターフェイスから送信するパケット。
オプション	ルールに設定される追加のオプション。これには、ロギング、時間範囲、およびその他の IOS ルール オプションが含まれます。[Advanced]/[Edit Options] ダイアログボックス （23 ページ）を参照してください。
カテゴリ	ルールに割り当てられるカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。カテゴリ オブジェクトの使用を参照してください。
説明	ルールの説明（ある場合）。
期限日（Expiration Date）	ルールが期限切れになる日付。期限切れになったルールは、太字で[期限切れ（Expired）]と示されます。期限切れになったルールは自動的には削除されません。
最後のチケット	ルールの最終変更に関連付けられたチケットを表示します。[最後のチケット（Last Ticket(s)）] 列のチケット ID をクリックして、チケットの詳細を表示し、そのチケットに移動できます。外部チケット管理システムへのリンクが設定されている場合は、チケットの詳細からそのシステムに移動することもできます（[チケット管理（Ticket Management）] ページを参照）。
ルールテーブルの下のページ要素	

要素	説明
競合検出の有効化（Enable conflict detection） レポートの作成（Generate Report） （[IPv6アクセス制御（IPv6 Access Control）] ページにはどちらのオプションも表示されません）	自動競合検出を有効または無効にします。この機能はデフォルトで有効になっており、設定はユーザーごとに管理されます。1つのアクセスルールテーブルの競合検出を無効にすると、他のアクセスルールテーブルの機能も無効になります。 ルールテーブルの作成中または大規模な変更中は競合検出を無効にし、変更を検証する準備ができたら再度有効にすることができます。 自動競合検出の使用 （37 ページ）を参照してください。 （注） 自動競合検出機能の一部として使用できるフィールドとユーザーインターフェイス要素の詳細については、自動競合検出のユーザー インターフェイスについて（40 ページ）を参照してください。 競合検出が有効になっている場合は、[レポートの生成（Generate Report）] ボタンをクリックして、検出されたルールの競合に関する HTML レポートを作成できます。このレポートは印刷または別のアプリケーションにエクスポートすることができます。
ヒットカウントの更新（Refresh Hit Count） （[IPv6アクセス制御（IPv6 Access Control）] ページには表示されません）	テーブルに表示されるヒット情報を更新するには、このボタンをクリックします。 [Hit Count Selection Summary] ダイアログボックス（26 ページ）が開きます。
クエリ （[IPv6アクセス制御（IPv6 Access Control）] ページには表示されません）	ポリシークエリを実行するには、このボタンをクリックします。実行すると、ルールを評価して、効果のないルールを特定できます。 ポリシー クエリー レポートの生成を参照してください
[Find and Replace] ボタン（双眼鏡アイコン）	テーブル内のさまざまなタイプの項目を検索し、必要に応じてその項目を置換するには、このボタンをクリックします。 ルール テーブルの項目の検索と置換を参照してください。
[Up Row] ボタンと [Down Row] ボタン（矢印アイコン）	選択したルールを範囲内またはセクション内で上下に移動するには、これらのボタンをクリックします。詳細については、 ルールの移動とルール順序の重要性を参照してください。

要素	説明
[Add Row] ボタン	[Add Access Rule]/[Edit Access Rule] ダイアログボックス （18 ページ）を使用して選択したテーブルの行のあとにルールを追加するには、このボタンをクリックします。行を選択しなかった場合は、ローカル範囲の最後にルールが追加されます。ルールを追加する方法の詳細については、ルールの追加および削除を参照してください。
[Edit Row] ボタン	選択したルールを編集するには、このボタンをクリックします。個々のセルを編集することもできます。詳細については、ルールの編集を参照してください。
[Delete Row] ボタン	選択したルールを削除するには、このボタンをクリックします。

右クリックメニュー

右クリックメニューも使用できます。このメニューから、上記の機能の多くにアクセスできます。表示されるオプションは、右クリックした場所によって異なります。

- テーブル内のルールを右クリックすると、右クリックした特定のテーブルセルに関連した編集機能がオプションに含められる場合があります。たとえば、[ヒットカウント（Hit Count）]セルを右クリックすると、[ヒットカウントの詳細を表示（Show Hit Count Details）]コマンドが含まれます。詳細については、ルールの編集を参照してください。
- イベントビューアまたは CS MARS のいずれかで、ルールからそのルールに関連付けられたイベントに移動することもできます。詳細については、アクセスルールのイベントの表示およびIPS シグニチャの CS-MARS イベントの表示を参照してください。
- 右クリックメニューには、[ルールのインポート（Import Rules）] および [ルールの結合（Combine Rules）]オプションも含まれています。これらのオプションの詳細については、ルールのインポート （55 ページ）およびルールの結合を参照してください。

[Add Access Rule]/[Edit Access Rule] ダイアログボックス

security-device アクセスルールを追加または編集するには、[アクセスルールの追加（Add Access Rule）] および [アクセスルールの編集（Edit Access Rule）] ダイアログボックスを使用します。

（注） Security Manager 4.4 のリリースと ASA のバージョン 9.0 以降では、IPv4 および IPv6 アクセスルールを設定するための個別のページが統合されました。ただし、それ以前の ASA バージョンでは、IPv6 アクセスルールの個別のページが引き続き提供されます。以下の説明は、特に明記されている場合を除き、すべてのバージョンのページに適用されます。

アクセス ルールを設定する前に、次の項を参照してください。

- アクセス ルールについて （1 ページ）

- グローバル アクセス ルールについて （3 ページ）
- デバイス固有のアクセス ルールの動作について （5 ページ）
- アクセス ルールのアドレス要件およびルールの展開方法について （6 ページ）
- アクセス ルールの設定 （8 ページ）

ナビゲーション パス

[Access Rules] ページ （12 ページ）で、[行の追加（Add Row）] ボタンをクリックするか、行を選択して [行の編集（Edit Row）] ボタンをクリックします。

（注） Cisco Security Manager 4.13 より前は、[アクセスルールの追加（Add Access Rule）] ダイアログにデフォルト値が入力されていました。4.13 以降、ユーザーは csm.properties ファイルを更新することにより、デフォルト値の状況をカスタマイズできます。詳細については、[アクセス ルールの追加（Add Access Rule）] ダイアログでのデフォルトのカスタマイズ （64 ページ）を参照してください。

関連項目

- アクセス ルールの有効期限の設定 （29 ページ）
- ルールの編集
- ルールの追加および削除
- ルールのインポート （55 ページ）
- ネットワーク/ホストオブジェクトについて
- サービスとサービス オブジェクトおよびポート リスト オブジェクトの理解と指定

フィールド リファレンス

表 *2 : [Add Access Rule]/[Edit Access Rule]* ダイアログボックス

要素	説明
ルールの有効化（Enable Rule）	このチェックボックスをオンにするとルールがイネーブルになります。イネーブルにすると、デバイスに設定を展開したときにルールがアクティブになります。選択を解除すると、ルールはディセーブルになりますが、ルール定義は保持されます。ディセーブルなルールには、ルール テーブルにハッシュ マークが重なって表示されます。詳細については、ルールのイネーブル化とディセーブル化を参照してください。
操作	定義した条件に基づいて、ルールがトラフィックを許可または拒否するかどうか。

要素	説明
ソース	

要素	説明

	このルールのトラフィック ソースを提供します。ネットワーク、セキュリティ グループ、およびユーザーになります。次の 1 つ以上のタイプのソースに対して、値またはオブジェクト名を入力するか、オブジェクトを選択できます。
	• ネットワーク – さまざまなネットワーク、ホスト、およびインターフェイスの定義を、個別に、またはオブジェクトとして指定できます。インターフェイスオブジェクトをソースとして選択した場合、ダイアログボックスにタブが表示され、ホスト/ネットワークとインターフェイスが区別されます。
	
	「All-Address」オブジェクトは、ルールを特定のホスト、ネットワーク、またはインターフェイスに制限しません。これらのアドレスは、ホストまたはネットワーク、ネットワーク/ホスト オブジェクト、インターフェイス、またはインターフェイス ロールの IPv4 または IPv6 アドレスです。
	（注） 完全修飾ドメイン名（FQDN）は、FQDN ネットワーク/ホストオブジェクトまたは FQDN オブジェクトを含むグループオブジェクトを提供することによってのみ指定できます。FQDN を直接入力することはできません。
	これらの定義の詳細については、ネットワーク/ホストオブジェクトについて、ポリシー定義中の IP アドレスの指定およびインターフェイス ロール オブジェクトについてを参照してください。
	• セキュリティグループ（ASA 9.0 以降）– ルールについて、1 つ以上のソースセキュリティグループの名前またはタグ番号を入力するか選択します（存在する場合）。セキュリティグループの詳細については、ポリシーでのセキュリティグループの選択、TrustSec ベースのファイアウォールルールの設定、およびセキュリティ グループ オブジェクトの作成を参照してください。
	• ユーザー - ルールの Active Directory（AD）ユーザー名、ユーザーグループ、またはアイデンティティユーザーグループオブジェクト（使用する場合）。次のものを組み合わせて入力できます。
	  • 個別のユーザ名：NetBIOS_DOMAIN\username
	  • ユーザ グループ（\ を二重にします）：NetBIOS_DOMAIN\\user_group
	  • アイデンティティ ユーザ グループ オブジェクト名。
	
	詳細については、以下を参照してください。
	• ポリシーでのアイデンティティ ユーザの選択
	• アイデンティティ ベースのファイアウォール ルールの設定
	• アイデンティティ ユーザ グループ オブジェクトの作成

要素	説明
	（注） Enter more than one value in any of these fields by separating the items with commas.ロゴのソースイメージファイルに指定できるのは、GIF ファイル、JPG ファイル、または PNG ファイルです。ファイル名は最大 255 文字、サイズは最大 100 KB です。 各仕様を他の仕様と組み合わせて、トラフィックの一致をすべての定義を含むフローのみに制限します。たとえば、指定された送信元アドレス範囲内から発信された指定されたユーザトラフィックです。
宛先	このルールのトラフィックの宛先を指定します。ネットワークまたはセキュリティグループにすることができます。送信元と同様に、ネットワークおよびセキュリティグループ（ASA 9.0 以降）タイプの 1 つ以上の宛先について、値またはオブジェクト名を入力するかオブジェクトを選択できます。
サービス	動作対象のトラフィックタイプを定義するサービス。サービスオブジェクトおよびサービスタイプの任意の組み合わせ（通常はプロトコルとポートの組み合わせ）を入力するか選択できます。 項目をカンマで区切って複数の値を入力します。 サービスを指定する方法の詳細については、サービスとサービス オブジェクトおよびポート リスト オブジェクトの理解と指定を参照してください。
インターフェイス Global（ASA 8.3+）	インターフェイス固有のルールまたはグローバル ルールのいずれを作成するかを指定します。グローバル ルールは ASA 8.3+ のデバイスだけで使用でき、特別なルールに従って処理されます（詳細については、グローバル アクセス ルールについて （3 ページ）を参照してください）。 [インターフェイス（Interfaces）] を選択した場合は、ルールを割り当てるインターフェイスまたはインターフェイスロールの名前を入力します。あるいは、[選択（Select）] をクリックして、リストからインターフェイスまたはロールを選択します。インターフェイスをリストに表示するには、あらかじめ定義しておく必要があります。 ルーテッド モードのブリッジ グループでは、ブリッジ仮想インターフェイス（BVI）と各ブリッジ グループ メンバーのインターフェイスの両方にアクセス ルールを作成できます。 インターフェイス ロール オブジェクトは、各デバイスの設定が生成されるときに、実際のインターフェイス名で置き換えられます。インターフェイス ロール オブジェクトについてを参照してください。グローバルルールは、特定のインターフェイスに関連付けられていない特殊なグローバル ACL として作成されますが、インターフェイス固有のルールの後で、着信方向ですべてのインターフェイスに対して処理されます。
説明	オプションで入力するルールの説明（最大 1024 文字）。

要素	説明
カテゴリ	ルールに割り当てられるカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。カテゴリ オブジェクトの使用を参照してください。
[Advanced] ボタン	このボタンをクリックして、ルールのその他の設定（ロギング設定、トラフィック方向、時間範囲、およびルールの有効期限など）を行います。詳細については、「[Advanced]/[Edit Options] ダイアログボックス （23 ページ）」を参照してください。

[Advanced]/[Edit Options] ダイアログボックス

[詳細（Advanced）] ダイアログボックスを使用して、アクセスルールの追加の設定を行います。アクセスルールテーブルの3つの異なるセルに、方向、オプション、およびルールの有効期限の設定が表示されます。その後、該当するセルを右クリックして、設定を直接編集できます。

（注） Security Manager 4.4 のリリースと ASA のバージョン 9.0 以降では、IPv4 および IPv6 アクセスルールを設定するための個別のページが統合されました。ただし、それ以前の ASA バージョンでは、IPv6 アクセスルールの個別のページが引き続き提供されます。以下の説明は、特に明記されている場合を除き、すべてのバージョンのページに適用されます。

ナビゲーション パス

[詳細（Advanced）] ダイアログボックスにアクセスするには：

- [Add Access Rule]/[Edit Access Rule] ダイアログボックス （18 ページ）で [詳細（Advanced）] ボタンをクリックします。

[オプションの編集（Edit options）] ダイアログボックスのいずれかにアクセスするには：

- （[Access Rules] ページ （12 ページ）の）アクセスルールの [オプション（Options）] または [有効期限（Expiration Date）] セルを右クリックし、関連する [編集（Edit）] コマンドを選択します。ルールの方向を変更するには、[方向（Dir.）] を右クリックして、反対の方向（インまたはアウト）を選択します。

複数の行を選択すると、選択したすべてのルールのオプションが、変更によって置き換えられます。

関連項目

- アクセス ルールの設定 （8 ページ）
- ルールの編集
- アクセス ルールについて （1 ページ）

- ファイアウォール アクセス ルールの管理 （1 ページ）
- 時間範囲オブジェクトの設定

フィールド リファレンス

表 *3 : [Advanced]* ダイアログボックス

要素	説明
Enable Logging（PIX、ASA、FWSM）	PIX、ASA、および FWSM デバイスの場合、ルールエントリ（アクセス制御エントリ、または ACE とも呼ばれる）についての syslog メッセージを生成するかどうかを指定します。選択すると、次の追加オプションが有効になります。 • [Default Logging]：デフォルトのロギング動作を使用します。パケットが拒否されると、メッセージ 106023 が生成されます。パケットが許可された場合、syslog メッセージは生成されません。デフォルトのロギング間隔は 300 秒です。 • [Per ACE Logging]：このエントリに固有のロギングを設定します。ACE のログイベントに対して使用するロギングレベルを選択し、ロギング間隔（1 ～ 600 秒の範囲）を指定します。ACE に対して syslog メッセージ 106100 が生成されます。 使用可能なロギングレベル： • [Emergency]：（0）システムが不安定 • [Alert]：（1）即時処理が必要 • [Critical]：（2）クリティカル条件 • [Error]：（3）エラー条件 • [Warning]：（4）警告条件 • [Notification]：（5）正常ではあるが重大な条件 • [Informational]：（6）情報メッセージだけ • [Debugging]：（7）デバッグ メッセージ （注） [オプション（Options）] セルを右クリックし、[オプションの編集（Edit Options）] を選択すると、[Access Rules] ページ（12 ページ）のテーブルに含まれる既存ルールのファイアウォールおよび IOS ロギングオプションを変更できます。

要素	説明
Enable Logging（IOS） Log Input （IPv4 のみ。[IPv6 アクセス制御（IPv6 Access Control）] ページにはどちらのオプションも表示されません）	IOS デバイスのコンソールに送信されるエントリに一致したパケットに関するロギング情報メッセージを生成するかどうかを指定します。メッセージは IOS デバイスのコンソールに送信されます。 入力インターフェイスおよび送信元 MAC アドレスまたは仮想回線をロギング出力に含める場合は、[Log Input] を選択します。
トラフィックの方向	インターフェイス固有のアクセス ルールの場合、このルールが適用されるトラフィックの方向。 • [In]：インターフェイスで受信するパケット。 • [Out]：インターフェイスから送信するパケット。 （注） [方向（Dir.）] セルを右クリックして反対の方向を選択することで、[Access Rules] ページ （12 ページ）のテーブルに含まれる既存ルールの方向を変更できます。 グローバル ルールは常に In 方向で適用されるため、グローバル ルールの設定時にはこの設定を変更できません。
時間範囲	このルールが適用される時間を定義する時間範囲ポリシー オブジェクトの名前。時刻は、デバイスのシステム クロックに基づきます。この機能は、NTP を使用してシステム クロックを設定している場合に最適に機能します。 名前を入力するか、オブジェクトを選択します。必要なオブジェクトが表示されていない場合は、[Create] ボタンをクリックして作成します。 （注） 時間範囲は、FWSM 2.x デバイスまたは PIX 6.3 デバイスではサポートされていません。

要素	説明
Options（IOS） （IPv4 のみ。[IPv6 アクセス制御（IPv6 Access Control）] ページには表示されません）	IOS デバイス用の追加オプション： • [なし（none）]：適用されません。 • [Fragment]：フラグメンテーションを有効にします。これにより、パケット フラグメンテーションの追加管理が行われ、NFS との互換性が向上します。 デフォルトで、完全な IP パケットを再構築するために最大で 24 のフラグメントを受け入れます。ただし、ネットワークセキュリティポリシーによっては、フラグメント化されたパケットがファイアウォールを通過しないようにデバイスを設定することが必要な場合もあります。 • [確立済み（Established）]：デバイスを介したアウトバウンド TCP 接続のリターンアクセスを有効にします。このオプションは、デバイスにより保護されたネットワークからのアウトバウンドの元の接続と、外部ホスト上の同じ 2 つのデバイス間のインバウンドのリターン接続という、2 つの接続に対して機能します。
Rule Expiration	ルールに有効期限を設定できます。カレンダー アイコンをクリックして、日付を選択します。詳細については、アクセス ルールの有効期限の設定 （29 ページ）を参照してください。 また、有効期限を設定している場合は、有効期限が近いことを示す通知を、ルールが失効する何日前に送信するか、およびその送信先となる電子メールアドレスを設定することもできます。最初、これらのフィールドには、[ルール有効期限の管理設定（Rule Expiration administrative settings）] ページ（[ツール（Tools）] > [Security Manager管理（Security Manager Administration）] > [ルールの有効期限（Rule Expiration）] を選択）で設定した情報が設定されています。 [有効期限（Expiration Date）] セルを右クリックし、[ルールの有効期限の編集（Edit Rule Expiration）] を選択することにより、[Access Rules] ページ （12 ページ）のテーブルに含まれる既存ルールの該当するオプションを変更できます。 （注） 期限切れになったルールは自動的には削除されません。これらの情報を手動で削除し、デバイスに設定を再配布する必要があります。

[Hit Count Selection Summary] ダイアログボックス

[ヒットカウント選択サマリー（Hit Count Selection Summary）] ダイアログボックスを使用して、ヒットカウント情報を更新するルールを選択します。選択できるオプションは、[ヒットカウントの更新（Refresh Hit Count button）] ボタンをクリックする前に選択したルールによって制限されます。このダイアログボックスで [OK] をクリックすると、デバイスから更新され

たヒットカウント情報が取得されます。これには時間がかかることがあるため、途中で操作を中断できます。

（注） 同じルール内または異なるルール内の重複した ACE のヒットカウントは、常に 0 に設定されます。

ヒント [Access Rules] ページ （12 ページ）でそのルールの [ヒットカウント（Hit Count）] セルを右クリックすると、ルールの詳細なヒットカウント情報を表示できます。ヒットカウントの詳細の表示 （48 ページ）で説明されているように、詳細なヒットカウント情報が [ヒットカウントの詳細（Hit Count Details）] ウィンドウに表示されます。

ナビゲーション パス

（デバイスビューのみ） [Access Rules] ページ （12 ページ）テーブルで、詳細なヒットカウント情報が必要なアクセスルールを 1 つ選択し、[ヒットカウント（Hit Count）] カラムを右クリックして、[ヒットカウント詳細の表示（Show Hit Count Details）] を選択します。

関連項目

- ヒットカウントの詳細の表示 （48 ページ）
- アクセス ルールについて （1 ページ）

フィールド リファレンス

表 4 : [Hit Count Selection Summary] ダイアログボックス

要素	説明
Policy Selected	選択されているポリシーを識別します。ポリシーを選択しなかった場合、これは通常、デバイスに特定のルールが定義されていることを示す [ローカル（Local）] です。ポリシーが、共有ポリシーまたは継承ポリシー内の範囲となることもあります。 このフィールドの表示内容によって、ヒットカウントレポートの範囲が実際に制限されることはありません。

要素	説明
Rules Selected	ヒットカウント詳細を取得するルール。以下を選択します。 • 選択したルールのみの情報を取得する場合は、[ルール（rules）] オプションを選択します。範囲の名前、セクション名、または複数の個別のルールに関連する行を選択したり、フィルタを作成してフィルタリングされたすべてのルールを選択したりできます。ヒットカウントレポートの開始時にいずれかの行が選択されていた場合は、これがデフォルトとなります。 • すべての継承ルール、共有ルール、およびローカルルールに対するヒットカウントを取得する場合は、[すべてのルール（All Rules）] を選択します。オプションは、[Policy Selected] フィールドで指定されている範囲に限定されません。 ヒットカウントレポートの開始前にルールを選択しなかった場合、このオプションだけが選択可能になります。
Fetch Data From	次のいずれかのオプションを選択し、[ヒットカウントの更新（Refresh Hit Count）] をクリックします。 • [デバイス（Device）]：Security Manager はデバイスからヒットカウント情報をフェッチし、[アクセスルールポリシー（Access Rules policy）] ページに同じ情報を表示します。バージョン 4.9 以降、Security Manager は ASA および ASASM デバイスのデータベースにヒットカウント情報を保存します。 • [履歴（History）]： Security Manager は、特定の ACE の最新のヒットカウント情報をデータベース（ヒットカウントの履歴）からフェッチし、[アクセスルールポリシー（Access Rules policy）] ページに同じ情報を表示します。 **注**： オープンなアクティビティがある場合、ヒットカウントデータは Security Manager データベースに保持されません。この機能は、ASASM/ASA バージョン 8.3 以降の IPv4 アクセスルールおよび ASASM/ASA バージョン 9.0 以降のユニファイドアクセスルールでサポートされています。 [デバイスからデータをフェッチ（Fetch Data From Device）] が [選択したルール（Rules Selected）] オプションに基づいている場合、ヒットカウント保持サポートは有効になりません。ヒットカウント保持サポートは、[デバイスからデータをフェッチ（Fetch Data From Device）] で [すべてのルール（All Rules）] オプションを選択した場合にのみ有効になります。 履歴からデータをフェッチした場合に、[ヒットカウント（Hit Count）] の値がゼロの場合、Security Manager は、ルールの [ヒットカウント履歴（Hit Count History）] に基づいてルールが以前にヒットしたかどうかを確認し、対応する値を表示します。Security Manager が履歴から以前のヒットの値を見つけられない場合、[ヒットカウント（Hit Count）] の値はゼロとして表示されます。

アクセス ルールの有効期限の設定

アクセスルールを頻繁に使用することは、ネットワークへの一時的なアクセスを提供することです。たとえば、特定のプロジェクトの期間中にパートナーアクセスを許可するようなアクセス ルールを設定するとします。この場合、プロジェクトの完了時にはアクセス ルールを削除することが理想的です。しかし、アクセス ルール リストが大きくなるにつれて、リストの管理が困難になり、どのルールを一時的なものとして設定したか覚えていられなくなります。

この問題に対処するために、アクセス規則に有効期限を設定できます。有効期限を設定することにより、ルールが必要でなくなる日時を計画できます。

有効期限は変更可能な日付で、期限切れになったルールが Security Manager によって削除されることはありません。代わりに、期限切れになった場合、Security Manager では、期限切れになったルールの [期限日（Expiration Date）] カラムに「Expired」という太字が表示されます。[期限日（expiration date）] フィールドに基づいて、[アクセスルール（access rules）] ページをフィルタリングできます。たとえば、「expiration date has passed」でフィルタリングすると、期限切れになったすべてのルールが表示されます。

ルールが必要でなくなった場合は、そのルールを削除する（右クリックして [行の削除（Delete Row）] を選択）か、またはディセーブルにし（右クリックして [無効化（Disable）] を選択）、そのあとで設定をデバイスに再展開できます。最初はルールをディセーブルにしておいて、そのルールがあとで必要だとわかったときのために、そのルールを（ハッシュ マークが重なって表示された）テーブルに残しておけば、ルールを再作成する時間を節約できます。この場合は、ルールをイネーブルにし（右クリックして [有効化（Enable）] を選択）、設定を再展開するだけです。

有効期限を設定するときに、通知設定も行うことができます。有効期限が近づいたときに通知を受ける電子メールアドレスを指定します。ルールを評価する時間を与えるために、電子メールの通知メッセージの送信日から有効期限までの日数を指定できます。通知設定には、最初は管理設定で（[ツール（Tools）] > [Security Manager管理（Security Manager Administration）] > [ルールの有効期限（Rule Expiration）] を選択して）設定された値が入力されています。特定のルールに対して別の設定を入力できます。

ルールの有効期限を設定するには、次の手順を実行します。

- 新しいルールを作成する場合、またはルール全部を編集する場合は、[Add Access Rule]/[Edit Access Rule] ダイアログボックス （18 ページ）の [詳細設定（Advanced）] ボタンをクリックして、ルールの有効期限の設定を表示します。
- 既存のルールの場合は、ルール全部を編集せずに、有効期限の設定を追加または編集できます。ルールの [期限日（Expiration Date）] セルを右クリックし、[ルールの期限日の編集（Edit Rule Expiration）] を選択します。複数の行を選択して、同じルール有効期限を設定できます。詳細については、[Advanced]/[Edit Options] ダイアログボックス （23 ページ）を参照してください。

関連項目

- [Rule Expiration] ページ
- アクセス ルールの設定　（8 ページ）

アクセス コントロール ポリシー設定の指定

セキュリティデバイスアクセス制御リストに適用されるさまざまな設定を指定できます。これらの設定は、アクセスルールポリシーとともに機能します。インターフェイスとトラフィック方向の各組み合わせに対して、またはASA 8.3+デバイスではグローバルACLに対して、独自のACL名を設定できる点が重要です。PIX、ASA、およびFWSMデバイスの場合は、同時フローの最大数および関連するSyslog間隔も制御できます。

また、PIX、ASA、およびFWSMデバイスの場合は、ユーザ単位のダウンロード可能ACLが許可されるようにインターフェイスを設定することもできます。これにより、AAAサーバでユーザベースのACLを設定して、デバイスで定義されているACLを上書きできます。

（注）　Security Manager 4.4 のリリースと ASA のバージョン 9.0 以降で、IPv4 アクセス制御と IPv6 アクセス制御を設定するための別個のページが統合されましたただし、それ以前のバージョンの ASA では、IPv6 設定用の個別のページが引き続き提供されます。以下の説明は、特に明記されている場合を除き、すべてのバージョンのページに適用されます。

関連項目

- アクセス ルールの設定　（8 ページ）

ステップ 1　次のいずれかを実行して、 [Access Control Settings] ページ　（31 ページ）を開きます。

- （デバイスビュー）ポリシーセレクタから [ファイアウォール（Firewall）] > [設定（Settings）] > [アクセス制御（Access Control）]（または [ファイアウォール（Firewall）] > [設定（Settings）] > [IPv6 アクセス制御（IPv6 Access Control）]）を選択します。
- （ポリシービュー）ポリシータイプセレクタから [ファイアウォール（Firewall）] > [設定（Settings）] > [アクセス制御（Access Control）]（または [ファイアウォール（Firewall）] > [設定（Settings）] > [IPv6 アクセス制御（IPv6 Access Control）]）を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

ステップ 2　ページの上部でグローバル設定を指定します。PIX、ASA、およびFWSMデバイスの場合は、現在の拒否フローの最大数および関連するsyslog間隔を定義できます。ASA 8.3 以降デバイスの場合、オブジェクトグループ検索をイネーブルにして、Checkpointから変換する際のACLパフォーマンスを最適化できます。ただし、この設定が推奨されるのは、デバイスにメモリの制約がある場合だけです（[IPv6 アクセス制御（IPv6 Access Control）] ページでは使用できません）。

これらの設定の具体的な情報、および ACL コンパイルをサポートするプラットフォームについては、[Access Control Settings] ページ （31 ページ）を参照してください。

ステップ 3 ACL 名を設定するインターフェイスごと、またはユーザー単位の ACL をイネーブルにするインターフェイスごとに、テーブルの下の [行の追加（Add Row）] ボタンをクリックし、[Firewall ACL Setting] ダイアログボックス （34 ページ）に値を入力して、インターフェイスをインターフェイステーブルに追加します。次の点を考慮してください。

- ACL 名を設定すると、その名前が特定のインターフェイスおよび方向に適用されます。名前を指定していないインターフェイスと方向の組み合わせに対しては、Security Manager によってシステム生成名が作成されます。
- また、ASA 8.3+ デバイスでは、グローバル ACL の名前も指定できます。

リスト内の既存のエントリを編集するには、そのエントリを選択して [行の編集（Edit Row）] をクリックします。また、リスト内のエントリを削除するには、[行の削除（Delete Row）] をクリックします。

[Access Control Settings] ページ

[Access Control Settings] ページを使用して、アクセス ルール ポリシーとともに使用する値を設定します。パフォーマンスおよびロギングの機能を制御し、各インターフェイスに対して ACL 名を設定できます。

（注） Cisco Security Manager 4.4 のリリースと ASA のバージョン 9.0 以降では、IPv4 および IPv6 アクセス制御を設定するための個別のポリシーとオブジェクトが「統合」されました。つまり、IPv4 または IPv6 アドレス、あるいは両方のアドレスをどちらも使用できる一組のルールになりましたただし、それ以前のバージョンの ASA では、IPv6 設定用の個別のページが引き続き提供されます。（詳細については、Cisco Security Manager 4.4 でのポリシーオブジェクトの変更を参照してください）。以下の説明は、特に明記されている場合を除き、すべてのバージョンのページに適用されます。

従って、これらの設定の多くは、特定のデバイスタイプまたはソフトウェアバージョンにだけ適用されます。オプションを設定し、サポートされていないデバイスタイプにポリシーを適用した場合、それらのサポートされていないデバイスではそのオプションが無視されます。

ナビゲーション パス

アクセス制御ページを開くには、次のいずれかを実行します。

- （デバイスビュー）デバイスを選択し、次にポリシーセレクタから **[ファイアウォール（Firewall）] > [設定（Settings）] > [アクセス制御（Access Control）]**（または **[ファイアウォール（Firewall）] > [設定（Settings）] > [IPv6アクセス制御（IPv6 Access Control）]**）を選択します。

- （ポリシービュー）ポリシータイプセレクタから **[ファイアウォール（Firewall）] > [設定（Settings）] > [アクセス制御（Access Control）]**（または **[ファイアウォール（Firewall）] > [設定（Settings）] > [IPv6アクセス制御（IPv6 Access Control）]**）を選択します。新しいポリシーを作成するか、または既存のポリシーを選択します。
- （マップビュー）デバイスを右クリックし、**[ファイアウォールポリシーの編集（Edit Firewall Policies）] > [アクセス制御（Access Control）]**（または **[ファイアウォール設定の編集（Edit Firewall Settings）] > [IPv6アクセス制御（IPv6 Access Control）]**）を選択します。

関連項目

- アクセス コントロール ポリシー設定の指定 （30 ページ）
- アクセス ルールについて （1 ページ）
- デバイス固有のアクセス ルールの動作について （5 ページ）
- アクセス ルールのアドレス要件およびルールの展開方法について （6 ページ）
- インターフェイス ロール オブジェクトについて

フィールド リファレンス

表 5 : [Access Control Settings] ページ

要素	説明
同時フローの最大数（Maximum number of concurrent flows）（PIX、ASA、FWSM） （[IPv6アクセス制御（IPv6 Access Control）] ページには表示されません）	デバイスが作成できる並行拒否フローの最大数。デバイスがこの数に達すると、syslog メッセージ 106101 が生成されます。使用する必要のある範囲は、デバイスで使用可能なフラッシュ メモリの大きさによって異なります。 • 64 MB より大きい：値は 1 ～ 4096 です。デフォルトは 4096 です。 • 16 MB より大きい：値は 1 ～ 1024 です。デフォルトは 1024 です。 • 16 MB 以下：値は 1 ～ 256 です。デフォルトは 256 です。
Syslog 間隔（Syslog interval）（PIX、ASA、FWSM） （[IPv6アクセス制御（IPv6 Access Control）] ページには表示されません）	セキュリティ アプライアンスが拒否フローの最大値に達したことを警告する syslog メッセージ 106101 を生成するための時間間隔。拒否フローの最大値に達した場合、最後の 106101 メッセージから指定の秒数が経過すると、新たに 106101 メッセージが生成されます。値は 1 ～ 3600 ミリ秒です。デフォルトは 300 です。

要素	説明
Enable Access List Compilation（グローバル） （IPv4 のみ。[IPv6アクセス制御（IPv6 Access Control）] ページにも表示されません）	アクセス リストをコンパイルするかどうか。コンパイルすると、サイズの大きなルールテーブルの処理が高速になります。コンパイルにより、すべての ACL に対するポリシー ルールおよびパフォーマンスが最適化されます。ただし、コンパイルがサポートされる旧式のプラットフォームの数は次のように限られています。 • ルータ（グローバル設定のみ）：7120、7140、7200、7304、および 7500 • PIX 6.3 ファイアウォール（グローバル モードまたはインターフェイス単位） ACL は、アクセス リスト要素の数が 19 以上である場合にだけコンパイルされます。推奨されるエントリの最大数は 16,000 です。 アクセスリストをコンパイルするには、デバイスに少なくとも 2.1 MB のメモリが必要となります。アクセス リストのコンパイルは、Turbo ACL とも呼ばれます。
Enable Object Group Search（ASA 8.3+） （[IPv6アクセス制御（IPv6 Access Control）] ページには表示されません）	ASA 8.3+ デバイスでオブジェクト グループ検索をイネーブルにするかどうか。これにより、オブジェクト グループを展開せずに ACL パフォーマンスを最適化できます。オブジェクト グループ検索は主に、Checkpoint から ASA への移行時に使用されます。デバイスにメモリ制約がある場合（つまり、操作中にメモリが不足しているとわかった場合）は、これによってアクセス ルールの数が大幅に増加することがあります。 ASA 9.18 以降のデバイスでは、[オブジェクトグループ検索の有効化（Enable Object Group Search）] オプションがデフォルトで有効になっています。
オブジェクトグループ検索のしきい値の有効化（Enable Threshold Object Group Search） （IPv4 のみ。[IPv6アクセス制御（IPv6 Access Control）] ページにも表示されません）	オブジェクトグループ検索のしきい値制限を有効にするには、このボックスをオンにします。デフォルトでは、しきい値は有効になっていません。

要素	説明
[アクセス制御の設定（Access Control settings）] テーブル	このテーブルには、特別な処理を設定するインターフェイスが示されます。[インターフェイス名（Interface Name）] は、特定のインターフェイスまたはインターフェイスロールを指します。また、ASA 8.3+ デバイスでのグローバル ACL 設定の場合は、[グローバル（Global）] です。 このテーブルを使用すると、Security Manager によるシステム生成名の自動設定を行わない場合に、ACL に名前を設定できます。この名前は、インターフェイスに対して生成された特定方向の ACL に適用されます。 ユーザー単位のダウンロード可能 ACL、オブジェクトグループ検索および ACL コンパイルに対して、インターフェイスレベルの設定を行うこともできます。 • アクセス制御のインターフェイス設定を追加するには、[行の追加（Add Row）] ボタンをクリックし、 [Firewall ACL Setting] ダイアログボックス （34 ページ）に入力します。 • アクセス制御のインターフェイス設定を編集するには、インターフェイス設定を選択し、[行の編集（Edit Row）] ボタンをクリックします。 • アクセス制御のインターフェイス設定を削除するには、インターフェイス設定を選択し、[行の削除（Delete Row）] ボタンをクリックします。

（注） CSM は、ASA デバイスの前方参照オプションをサポートしていません。CSM は、参照リンクが正しく確立されていないデバイスで設定されている CLI を検出しません。これらの CLI はサポート対象外として分類され、CSM 経由で管理されません。

[Firewall ACL Setting] ダイアログボックス

[ファイアウォールACL設定（Firewall ACL Setting）] ダイアログボックスを使用して、セキュリティデバイス アクセス ルール ポリシーとともに使用する、特定のインターフェイス、インターフェイスロール、またはグローバルルールの設定を行います。

ナビゲーション パス

[Access Control Settings] ページ （31 ページ）に移動し、インターフェイステーブルの下の [行の追加（Add Row）] ボタンをクリックするか、またはテーブル内の行を選択して [行の編集（Edit Row）] ボタンをクリックします。

関連項目

- アクセス コントロール ポリシー設定の指定 （30 ページ）
- アクセス ルールについて （1 ページ）
- グローバル アクセス ルールについて （3 ページ）
- デバイス固有のアクセス ルールの動作について （5 ページ）
- アクセス ルールのアドレス要件およびルールの展開方法について （6 ページ）
- インターフェイス ロール オブジェクトについて

フィールド リファレンス

表 *6 : [Firewall ACL Setting]* ダイアログボックス

要素	説明
インターフェイス（Interface） Global（ASA 8.3+）	設定の対象が特定のインターフェイス（またはインターフェイス ロール）か、あるいは ASA 8.3+ デバイスのグローバルルールかを指定します。 [インターフェイス（Interface）] を選択した場合は、設定するインターフェイスまたはインターフェイスロールの名前を指定します。名前を入力するか、[選択（Select）] をクリックしてリストから選択するか、または新しいオブジェクトを作成します。 [Global] を選択した場合は、グローバル ACL の名前を指定するオプションしかありません。
トラフィックの方向	インターフェイスを通過するトラフィックの方向（[イン（in）] または [アウト（out）]）。方向が関係する場合、設定した値はこの方向にだけ適用されます。 ASA 8.3+ デバイスでは、グローバル ACL の方向は常に [in] です。

要素	説明
ユーザー定義の ACL 名（[IPv6アクセス制御（IPv6 Access Control）] ページにチェックボックスは表示されない） ACL Name	ACL に名前を指定するかどうか。このオプションを選択した場合、使用する名前を入力します。これは、インターフェイスと方向の組み合わせに対して生成された ACL に適用されます。名前は、デバイス上で一意である必要があります。 ASA 8.3+ デバイスでグローバル ACL に名前を設定する場合、オプションは自動的に選択されるため、目的の名前を入力するだけです。 （注） ファイアウォールルールの ACL 名が一意であり、Policy Object Manager で定義された ACL オブジェクトと同じ名前でないことを確認してください。詳細については、アクセスコントロールリストオブジェクトの作成を参照してください。 名前を設定しなかった場合は、Security Manager により自動的に名前が生成されます。
Enable Per User Downloadable ACLs（PIX、ASA、FWSM） （[IPv6アクセス制御（IPv6 Access Control）] ページには表示されません）	ユーザ単位の ACL のダウンロードをイネーブルにしてインターフェイス上の ACL を上書きするかどうか。ユーザ ACL は、Security Manager で設定されるのではなく、AAA サーバで設定されます。ユーザ単位の ACL がない場合は、インターフェイスに設定されているアクセスルールがトラフィックに適用されます。 このオプションは、トラフィックの方向が [イン（in）] の場合にのみ、指定されたインターフェイスのデバイスで設定されます。
Enable Object Group Search（PIX 6.x） （[IPv6アクセス制御（IPv6 Access Control）] ページには表示されません）	PIX 6.x インターフェイスでオブジェクトグループ検索をイネーブルにするかどうか。イネーブルにすると、サイズの大きい ACL を保持するためのデバイスのメモリ要件が少なくなります。ただし、オブジェクト グループ検索によって、各パケットでの ACL 処理が低速になるため、パフォーマンスに影響します。 非常に大きなオブジェクトグループが存在する場合は、オブジェクトグループ検索を推奨します。 ヒント ASA 8.3+ デバイスでは、オブジェクト グループ検索の設定は、[Access Control Settings] ページ （31 ページ）で行います。

要素	説明
Enable Access List Compilation（PIX 6.x） （[IPv6アクセス制御（IPv6 Access Control）] ページには表示されません）	PIX 6.x デバイスで、このインターフェイス上のアクセス リストをコンパイルするかどうか。この設定は、[Access Control Settings] ページで設定した同等のグローバル設定を上書きします。 ACL をコンパイルすると、サイズの大きいルールテーブルの処理が高速になり、インターフェイスのポリシールールおよびパフォーマンスが最適化されます。ACL は、アクセス リスト要素の数が 19 以上である場合にだけコンパイルされます。推奨されるエントリの最大数は 16,000 です。 アクセス リストをコンパイルするには、デバイスに少なくとも 2.1 MB のメモリが必要となります。

自動競合検出の使用

Security Manager は、アクセスルール向けの自動競合検出機能を提供します。自動競合検出を使用すると、アクセスルールのロジックを評価できます。自動競合検出が有効になると、アクセスルールポリシー内の他のルールと重複または競合するルールが識別されます。この情報を使用して、削除、移動、または編集が必要なルールを特定します。

ここでは、次の内容について説明します。

- 自動競合検出について （37 ページ）
- 自動競合検出のユーザー インターフェイスについて （40 ページ）
- 競合の解決 （45 ページ）

自動競合検出について

Security Manager には、不要な冗長または重複したルールを特定するのに役立つ自動競合検出機能が用意されています。競合していても、導入後にデバイスに影響しないルールもありますが、ルールテーブルに不要なクラスタが作成されます。そのようなルールを検出することにより、ルールセットをクリーンアップして、より使いやすく、効率的なアクセスルールポリシーを作成することができます。

競合するルールによっては、ネットワークに望ましくない結果が生じる可能性があります。それらの競合するルールを検出することにより、セキュリティ面のニーズを意図したとおり満たすために削除、移動、または編集する必要のあるルールを特定できます。

（注） 競合検出機能は、2 つのルール間での最初の競合を報告します。特定のルールと競合する付加的な複数のルールがテーブルにある場合、最初の競合が解決されるまで、それらのルールについては報告されません。

Security Manager によって検出された競合は、次のように分類されます。

- 冗長オブジェクト：ルールのフィールドに含まれる 1 つの要素が、ルールの同じフィールドに含まれる 1 つ以上の要素のサブセットになっています。次の例では、ソースセルに *net-group2* と *net-group1* の 2 つのネットワークオブジェクトがあります。*net-group2* は *net-group1* のサブセットなので、冗長なオブジェクトであり、安全に削除できます。

```
object-group network net-group1
network-object 10.2.0.0 255.255.0.0
object-group network net-group2
network-object 10.2.1.1 255.255.255.255
```

- 冗長なルール：基本ルールでも 2 つのルールによって同じタイプのトラフィックに同じ処理が適用される場合、基本ルールを削除しても最終的な結果は変わりません。たとえば、特定のネットワークの FTP トラフィックを許可するルールに、同じネットワークの IP トラフィックを許可するルールが続き、その間にアクセスを拒否するルールがない場合、最初のルールは冗長であり、削除できます。

次に、冗長なルールの単純な例を示します。

```
access-list acl permit ip 2.1.1.1 255.255.255.255 any
access-list acl permit ip 2.1.1.0 255.255.255.0 any
```

- 部分的に冗長なルール：複合ルールの一部が、1 つのルールまたはそれに続く複合ルールの一部に対して冗長になっています。

- シャドウイング状態のルール：これは、冗長なルールの逆です。この場合は、あるルールが別のルールと同じトラフィックに一致し、2 番目のルールはアクセス リスト内であとに配置されているためにいずれのトラフィックにも適用されません。両方のルールのアクションが同じ場合は、シャドウイング状態のルールを削除できます。2 つのルールがトラフィックに対して異なるアクションを指定している場合、必要なポリシーを導入するには、シャドウイング状態のルールを移動するか、いずれかのルールの編集が必要になる場合があります。たとえば、1 つの送信元または宛先に対して、基本ルールで IP トラフィックを拒否し、シャドウイング状態のルールで FTP トラフィックを許可する場合などです。

次に、シャドウイング状態のルールの単純な例を示します。

```
access-list acl permit ip 1.0.0.0 255.0.0.0 any
access-list acl permit ip 1.1.0.0 255.255.0.0 any
```

（注） 重複するルールは、自動競合検出機能によって、シャドウイング状態のルールとして報告されます。

- 部分的にシャドウイング状態のルール：複合ルールの一部が、その前のルールによってシャドウイングされます。両方のルールのアクションが同じ場合は、ルールのシャドウイングされている部分を削除できます。2つのルールがトラフィックに対して異なるアクションを指定している場合、必要なポリシーを導入するには、シャドウイング状態のルールを移動するか、いずれかのルールの編集が必要になる場合があります。

自動競合検出の範囲

競合を検出する際、Security Manager は、アクセスルールに含まれる次の情報を評価します。

- source
- destination
- サービス
- ユーザ
- interfaces

（注） バージョン 4.23 以降、Cisco Security Manager では、競合検出機能に次の新しい拡張機能が導入されています。

- 競合検出は、特定のフィールドが更新された場合にのみトリガーされます。たとえば、ルールポリシーの送信元、宛先、セキュリティグループタグ、ユーザーインターフェイス、およびトラフィック検出などのフィールドです。
- ACL の変更の場合、競合検出は検出時にバックグラウンドでトリガーされます。ユーザーインターフェイスには影響しません。
- ACL ポリシーに対して最大 5 つの変更を同時に実行するとともに、その進行状況を確認できるようになりました。別の変更を実行しようとすると、続行する前に先行の変更が検証されるまで待つ必要があることを示すポップアップメッセージが表示されます。
- 競合検出オプションを無効にすると、Security Manager は消費されていたメモリ領域を即座に解放します。これにより、メモリ使用量が最適化され、過負荷の可能性が減少します。これを実行するため、クライアント LAX ファイルのパラメータを変更して、Security Manager がより多くの領域をクリアできるようにします。
- 競合検出を無効にしたときに Security Manager が空き領域を増やすことを可能にするには、クライアント LAX ファイルに次の変更を加えます。

```
# LAX.NL.JAVA.OPTION.ADDITIONAL
 # required for optimized garbage collection
 lax.nl.java.option.additional=-client -Djdk.tls.client.protocols="TLSv1.2"
-XX:+UseG1GC
 -XX:NewRatio=3 -XX:PermSize=64m -XX:MaxPermSize=128m -XX:+HeapDumpOnOutOfMemoryError

 -XX:HeapDumpPath=./logs -XX:+UseCompressedOops -Xdebug
 -Xrunjdwp:transport=dt_socket,address=5005,server=y,suspend=n
```

- 競合検出のディープスキャンでは、Cisco Security Manager 4.16 と比較して、より多くの時間とメモリ使用量が必要です。そのため、必要に応じて Cisco Security Manager のプロパティで `fwsvc.Legacy_4_16_RuleAnalysis` を true に設定し、この機能を無効にすることができます。

（注） 競合検出には、次の注意事項が適用されます。

- 競合検出は、デバイスまたは共有ポリシーのアクセスルールポリシーに含まれるアクセスルールに対してのみ使用できます。競合検出は、AAA ルールや検査ルールなど、他のポリシーの一部であるアクセスルールに対しては使用できません。
- ルールに FQDN ネットワーク/ホストオブジェクトが含まれている場合、FQDN オブジェクトは無視されますが、そうではない場合は FQDN オブジェクトが分析に含まれます。
- 無効化されたルールは、競合検出時に評価されません。
- 競合検出では、アクセスルールの評価の際、時間範囲は考慮されません。競合検出時にフラグが立てられたルールを削除する前に、該当するルールが本当に競合していることを確認してください。

関連項目

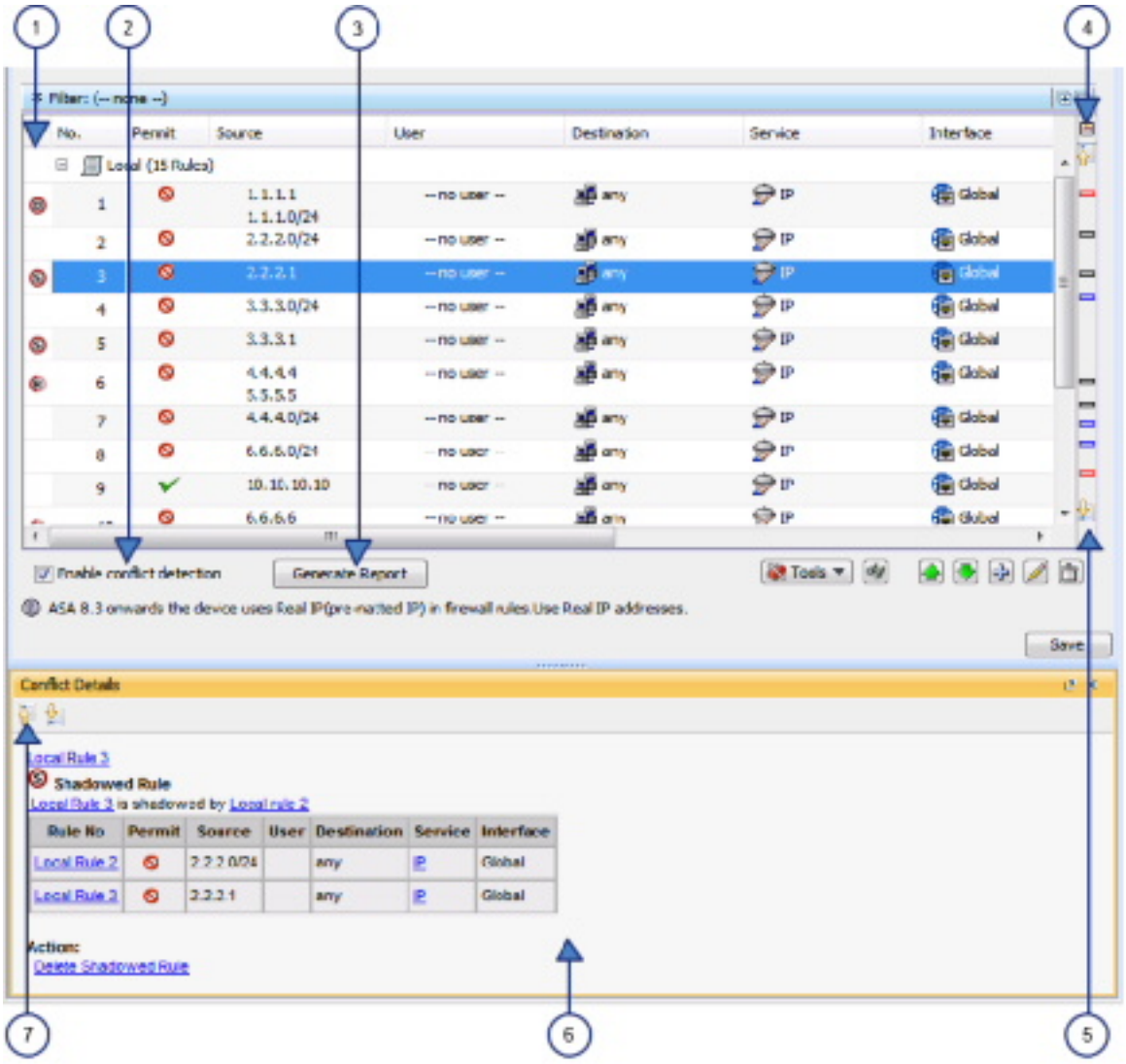
- 自動競合検出のユーザー インターフェイスについて （40 ページ）
- 競合の解決 （45 ページ）
- アクセス ルールについて （1 ページ）
- デバイス固有のアクセス ルールの動作について （5 ページ）
- アクセス ルールのアドレス要件およびルールの展開方法について （6 ページ）
- アクセス ルールの設定 （8 ページ）

自動競合検出のユーザー インターフェイスについて

自動競合検出機能は、競合を識別し、それらの競合をより迅速かつ簡単に解決するために、アクセスルールテーブルと緊密に結合されています。競合検出が有効になっている場合、競合間を移動したり、競合を解決したりするために、追加のユーザーインターフェイス要素を使用できます。

（注） アクセスルール ページの標準的な要素については、[Access Rules] ページ （12 ページ）を参照してください。

図 *2 :* 自動競合検出



1	競合インジケータアイコン	2	競合検出の有効化
3	[Generate Report] ボタン	4	注釈表示オプション
5	競合ナビゲーションバー	6	競合の詳細領域
7	競合ナビゲーションボタン		

競合インジケータアイコン

競合インジケータアイコンは、競合を識別し、競合の種類をすばやく視覚的に表現するために使用されます。次の表に、使用可能なアイコンの詳細を示します。

（注） 競合の種類の説明については、自動競合検出について （37 ページ）を参照してください。

	冗長オブジェクト
	冗長ルール
	部分的な冗長ルール
	シャドウルール
	部分的なシャドウルール
（注） アクセスルールに複数の競合がある場合、またはユーザーメモが添付されている場合、そのルールの競合インジケータアイコンに小さなプラス記号（+）が表示されます。	

[競合インジケータ（Conflict Indicator）] アイコンを使用すると、次のアクションを実行できます。

- [競合インジケータ（Conflict Indicator）] アイコンにマウスポインタを合わせると、競合に添付されたユーザーメモを含め、競合の説明が表示されます。
- [競合インジケータ（Conflict Indicator）] アイコンをクリックするか、アイコンを右クリックして [競合の詳細を表示（Show Conflict Detail）] を選択して、選択した競合の [競合の詳細（Conflict Details）] ペインを開きます。
- 冗長オブジェクトの [競合インジケータ（Conflict Indicator）] アイコンを右クリックし、[冗長オブジェクトの削除（Remove Redundant Object）] を選択して、ルールから冗長オブジェクトを削除します。
- [競合インジケータ（Conflict Indicator）] アイコンを右クリックし、[ユーザーメモの追加（Add User Note）] を選択して、選択した競合の [ユーザーメモの追加（Add User Note）] ダイアログボックスを開きます。[ユーザーメモの追加（Add User Note）] ダイアログボックスを使用して、競合に関するメモを入力できます。このメモは、後でルール分析詳細レポートに含めることができます。

（注） アクセスルールページを終了するとき、またはユーザーメモが入力されたルールを編集した後は、ユーザーメモは保存されません。

競合検出の有効化

[競合検出の有効化（Enable Conflict Detection）] オプションは、自動競合検出を有効にするかどうかを制御します。競合検出はデフォルトで有効になっていますが、このオプションの選択を解除すると無効にできます。この設定はユーザーごとに管理され、1つのアクセスルールテーブルの競合検出を有効または無効にすると、他のアクセスルールテーブルの機能も有効または無効になります。

レポートの作成（Generate Report）

競合検出が有効になっている場合は、[レポートの生成（Generate Report）] ボタンをクリックして、競合の HTML レポートを作成し、出力したり、別のツールにエクスポートしたりできます。ルール分析の詳細レポートには、ルールテーブル内のすべての競合の詳細が表示され、競合について入力されたユーザーのメモが含まれています。[注釈表示オプション（Annotation Display Options）] ダイアログボックスで選択した設定は使用されず、テーブルに定義されているフィルタ設定は考慮されません。

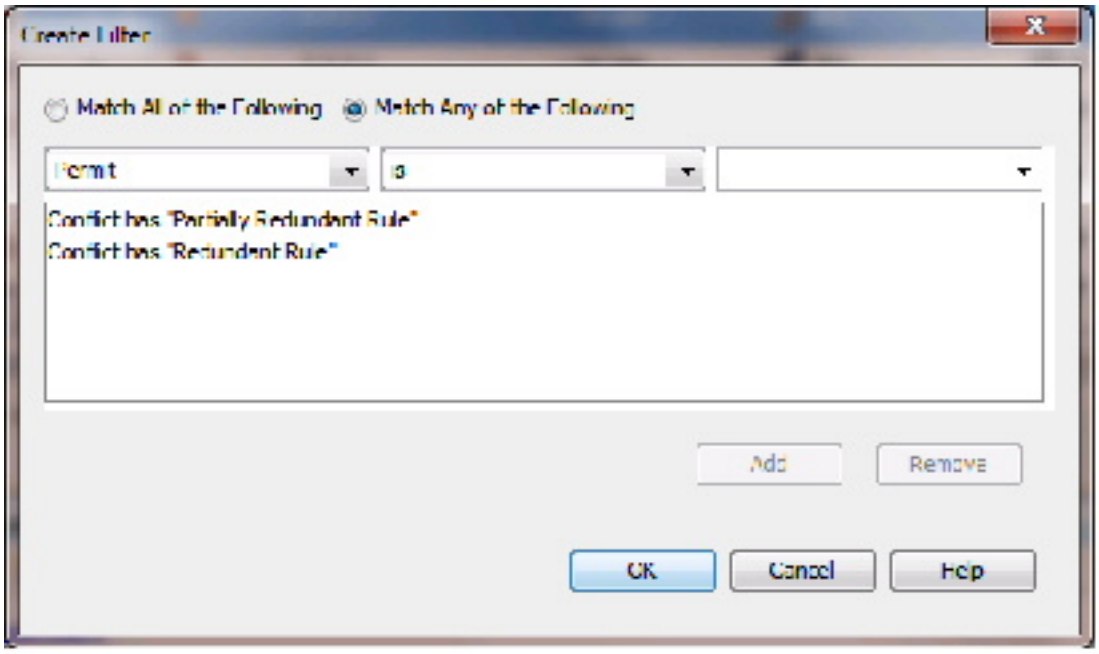
（注） アクセスルールページを終了するとき、またはユーザーメモが入力されたルールを編集した後は、ユーザーメモは保存されません。

最初に [アクセスルール（Access Rules）] ページを開くと、[レポートの生成（Generate Report）] ボタンが進行状況バーに置き換えられます。競合分析が完了すると、他の競合検出機能とともに [レポートの生成（Generate Report）] ボタンが使用できるようになります。

[注釈表示オプション（Annotation Display Options）] ボタン

[注釈表示オプション（Annotation Display Options）] ボタンをクリックすると、[注釈表示オプション（Annotation Display Options）] ダイアログボックスが開きます。このダイアログボックスは、報告する必要のある競合のタイプを選択するために使用します。競合の種類の説明については、自動競合検出について （37 ページ）を参照してください。

特定のタイプの競合を無効にしても、それらのルールはアクセスルールテーブルから削除されません。これらのタイプの競合に対する、ルールの競合通知がオフになるだけです。特定のタイプの競合ルールのみを非表示または表示するには、テーブルフィルタ機能を使用できます。たとえば、冗長および部分的に冗長なルールの競合のみを確認したい場合は、次の高度なフィルタを設定できます。



マウスポインタを [注釈表示オプション（Annotation Display Options）] ボタンの上に置くと、各タイプの競合の概要を表示でき、無効になっている競合タイプの確認もできます。

（注） 選択した [注釈表示オプション（Annotation Display Options）] は、オプションが変更されるまで有効です。競合の解決に取り組んでいるときは常に、これらの設定を確認してください。

競合ナビゲーションバー

競合ナビゲーションバーを使用して、競合に移動します。競合ナビゲーションバーの [前の競合（Previous Conflict）] ボタンと [次の競合（Next Conflict）] ボタンを使用して、競合間を移動できます。競合ナビゲーションバーの競合ロケータの 1 つをクリックして、特定の競合に直接移動することもできます。これは、大きなルールテーブルを操作する場合に特に役立ちます。

ヒント 競合ロケーターにカーソルを合わせると、競合の簡単な概要が表示されます。

競合ロケータは、次のように色分けされています。

- **赤色のロケータ**：冗長オブジェクト
- **青色のロケータ**：冗長ルールおよび部分的に冗長なルール
- 黒のロケーター：シャドウルールおよび部分的なシャドウルール

競合の詳細領域

[競合の詳細（Conflict Details）] ペインには、選択した競合の詳細が表示されます。必要に応じてペインをドッキングしたり、ドッキングを解除したりできます。[競合の詳細（Conflict Details）] ペインがドッキングされているときに [Policy Object Manager] ペインもドッキングされている場合、ウィンドウの下部にあるタブを使用して 2 つの機能間を移動できます。

直接比較しやすいように、競合するルールがテーブルにまとめて表示されます。競合のタイプはテーブルの上に表示されます。手動で解決する必要がある、部分的に冗長なルールと部分的にシャドウされたルールを除くすべての競合について、テーブルの下に推奨のアクションが表示されます。関連するルールへの直接移動するためのリンクがあります。競合するルールの一部であるポリシーオブジェクトをクリックして展開すると、オブジェクトの内容が表示されます。もう一度クリックすると、ポリシーオブジェクトが折りたたまれます。

提供されているリンクを使用して、競合するルールに移動できます。[アクション（Action）] の下のリンクをクリックして、Security Manager に提案されたアクションを自動的に実行させることもできます。

競合ナビゲーションボタン

[競合の詳細（Conflict Details）] ペインの上部にある [前の競合（Previous Conflict）] ボタンと [次の競合（Next Conflict）] ボタンを使用すると、[競合の詳細（Conflict Details）] ペインを離れることなく、解決する必要がある競合間を移動できます。

関連項目

- 自動競合検出について （37 ページ）
- 競合の解決 （45 ページ）
- アクセス ルールについて （1 ページ）
- デバイス固有のアクセス ルールの動作について （5 ページ）
- アクセス ルールのアドレス要件およびルールの展開方法について （6 ページ）
- アクセス ルールの設定 （8 ページ）

競合の解決

次の手順では、自動競合検出機能を使用してアクセスルールの競合を解決する方法について説明します。

ヒント Combine Rules ツールを使用して、ルールを評価するように Cisco Security Manager を設定し、より効率のよいルールに結合する方法を理解できます。詳細については、ルールの結合を参照してください。

関連項目

- 自動競合検出について （37 ページ）
- 自動競合検出のユーザー インターフェイスについて （40 ページ）
- アクセス ルールについて （1 ページ）
- デバイス固有のアクセス ルールの動作について （5 ページ）
- アクセス ルールのアドレス要件およびルールの展開方法について （6 ページ）
- アクセス ルールの設定 （8 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ポリシーセレクタから **[ファイアウォール（Firewall）]>[アクセスルール（Access Rules）]** の順に選択します。
- （ポリシービュー）ポリシータイプセレクタから **[ファイアウォール（Firewall）] > [アクセスルール（Access Rules]** を選択し、既存のポリシーを選択します。

[Access Rules] ページ （12 ページ）が開きます。競合検出が有効になっている場合、テーブルのロード後にアクセスルールの競合が分析されます。競合検出が無効になっている場合、[競合検出の有効化（Enable Conflict Detection）] を選択して競合分析を開始します。

分析の進行状況は、ルールテーブルの下に表示されます。競合検出機能以外の機能は、ルールの分析中にルールテーブルに対して実行できます。分析が完了すると、競合検出機能が有効になります。

ステップ 2 分析対象のルールがルールテーブルに表示されていることを確認してください。確認には、セクションの展開、およびフィルタを使用している場合は各フィルタが正しく設定されていることの確認が含まれます。フィルタ処理されているルール、または折りたたまれているセクションにあるルールは、競合検出分析に含まれません。

ヒント アクセスルールテーブルの上にある [フィルタ（Filter）] 領域の右上隅にある [すべての行を展開（Expand all rows）] または [すべての行を折りたたむ（Collapse all rows）] ボタンを使用して、ルールテーブルのすべてのセクションをすばやく展開または折りたたむことができます。

ステップ 3 垂直スクロールバーの右側にある競合ナビゲーションバーの上にある [注釈表示オプション（Annotation Display Options）] ボタンをクリックして、[注釈表示オプション（Annotation Display Options）] ダイアログボックスを開きます。検出する競合のタイプがすべて有効になっていることを確認し、[OK] をクリックします。

ヒント マウスポインタを [注釈表示オプション（Annotation Display Options）] ボタンの上に置くと、各タイプの競合の概要を表示でき、無効になっている競合タイプの確認もできます。

（注） 選択した [注釈表示オプション（Annotation Display Options）] は、オプションが変更されるまで有効です。競合の解決に取り組んでいるときは常に、これらの設定を確認してください。

ステップ 4 ルールテーブルで見つかった競合のコピーを印刷または保存する場合は、[レポートの生成（Generate Report）] をクリックします。

ブラウザでルール分析詳細レポートが開きます。ルール分析詳細レポートには、ルールテーブル内のすべての競合の詳細が表示されます。[注釈表示オプション（Annotation Display Options）] ダイアログボックスで選択した設定は使用されず、テーブルに定義されているフィルタ設定は考慮されません。レポートは、保存したり、必要に応じて印刷したりできます。

ステップ 5 競合ナビゲーションバーを使用して、競合に移動します。競合ナビゲーションバーの [前の競合（Previous Conflict）] ボタンと [次の競合（Next Conflict）] ボタンを使用して、競合間を移動できます。競合ナビゲーションバーの競合ロケータの 1 つをクリックして、特定の競合に直接移動することもできます。これは、大きなルールテーブルを操作する場合に特に役立ちます。

ヒント 競合ロケーターにカーソルを合わせると、競合の簡単な概要が表示されます。

競合ロケータは、次のように色分けされています。

- **赤色のロケータ**：冗長オブジェクト
- **青色のロケータ**：冗長ルールおよび部分的に冗長なルール
- **灰色のロケータ**：シャドウルールおよび部分的にシャドウされたルール

ステップ 6 選択した競合の [競合インジケータ（Conflict Indicator）] アイコンをクリックして、[競合の詳細（Conflict Details）] ペインを開きます。[競合インジケータ（Conflict Indicator）] アイコンの詳細については、自動競合検出のユーザー インターフェイスについて （40 ページ）を参照してください。

[競合の詳細（Conflict Details）] ペインには、選択した競合の詳細が表示されます。直接比較しやすいように、競合するルールがテーブルにまとめて表示されます。競合のタイプはテーブルの上に表示されます。手動で解決する必要がある、部分的に冗長なルールと部分的にシャドウされたルールを除くすべての競合について、テーブルの下に推奨のアクションが表示されます。関連するルールへの直接移動するためのリンクがあります。競合するルールの一部であるポリシーオブジェクトをクリックして展開すると、オブジェクトの内容が表示されます。もう一度クリックすると、ポリシーオブジェクトが折りたたまれます。

ステップ 7 提供されているリンクを使用してルールに移動し、必要に応じて競合を解決するか、[アクション（Action）] の下にあるリンクをクリックして、提案されたアクションを Cisco Security Manager に自動的に実行させます。

（注） この時点で競合を解決しない場合は、アクセスルールテーブルの競合の左側にある [競合インジケータ（Conflict Indicator）] アイコンを右クリックし、[ユーザー ノートの追加（Add User Note）] を選択して、競合に関するメモを入力できます。ユーザーメモはルール分析詳細レポートに含まれますが、[アクセスルール（Access Rules）] ページを終了するとき、またはユーザーメモを含むルールを編集した後は保存されません。

ステップ 8 競合ナビゲーションバー、または [競合の詳細（Conflict Details）] ペインの上部にある [前の競合（Previous Conflict）] ボタンと [次の競合（Next Conflict）] ボタンを使用して、解決する必要があるその他の競合にアクセスします。

ステップ 9 この時点で解決しない競合が残っている場合は、必要に応じて、[レポートの生成（Generate Report）] をクリックして、残りの競合のコピーを印刷または保存できます。

ヒットカウントの詳細の表示

[ヒットカウントの詳細（Hit Count Details）] ウィンドウを使用して、アクセスルールがトラフィックに適用された回数に関する情報を表示します。これらのルールは、デバイス上でインターフェイス ACL となるルールです。このヒット カウント結果には、他のタイプの ACL（クラス マップまたは AAA ルールで使用される ACL など）のカウントは示されません。

ASA 8.3(1) 以降のデバイスに関するアクセスルールの場合、詳細なヒットカウントレポートには、アクセスルールポリシーがトラフィックに最後に適用された時刻も表示されます。この情報は、他のポリシーの変更によって置き換えられた可能性のあるルールを判断するのに役立ちます。

ヒット カウント情報を使用すると、アクセス ルールのデバッグに役立ちます。この情報は、ヒットしたことがない（つまり、不要であるか、または ACL における優先度の高いルールと重複している可能性がある）ルールや、頻繁にヒットする（つまり、改良が必要な）ルールを識別するのに役立ちます。

ヒント ルールの詳細を表示する前に、ページの下部にある [ヒットカウントの更新（Refresh Hit Count）] ボタンをクリックして、ヒットカウント情報を更新できます。詳細については、[Hit Count Selection Summary] ダイアログボックス （26 ページ）を参照してください。

ヒットカウントの詳細を分析する際には、次の点を考慮してください。

- ヒット カウントの表示前に、デバイスにポリシーを展開すると、最善の結果が得られます。デバイスを検出し、ヒット カウント レポートを生成したあとで展開した場合、結果が不完全になったり、解釈が困難になることがあります。たとえば、アクセス ルールにヒット カウント情報が含まれないことがあります。
- ヒット カウント統計は、インターフェイスではなく ACL に基づきます。[Cisco Security Manager管理の展開（Security Manager Administration Deployment）] ページ（[Deployment] ページを参照）で [ファイアウォールルールに対するACL共有の有効化（Enable ACL Sharing for Firewall Rules）] を選択した場合、共有 ACL により、その ACL を共有するすべてのインターフェイスの情報を統合した統計情報が提供されます。
- ファイアウォール ルールの展開時のネットワーク オブジェクト グループの最適化の説明に従ってネットワーク オブジェクト グループ最適化をイネーブルにした場合、正確なヒット カウント情報が得られない可能性があります。
- 展開中のアクセス ルールの自動最適化 （62 ページ）の説明に従って ACL 最適化をイネーブルにした場合、ヒット カウント結果でのデバイスからアクセス ルールへの ACE のマッチングに問題がある可能性があります。このため、アクセス ルールを選択したときに、そのルールに対するカウント結果が得られないことがあります。
- FQDN ネットワーク/ホストオブジェクトは無視されます。これらのオブジェクトのヒットカウント情報は取得できません。

- ヒットカウントと最終ヒット時間の情報は、デバイスの再起動時にクリアされます。
- 同じルール内または異なるルール内の複製された ACE のヒットカウントは、常に 0 に設定されます。

はじめる前に

ヒット カウント レポートには次の制限事項があります。

- ヒット カウント レポートは、デバイスに固有です。このレポートは、デバイスビューからのみ、一度に 1 つのデバイスに対して生成できます。レポートを生成する前に、デバイスにポリシーを展開する必要があります。
- ASA 8.3+ デバイスでオブジェクト グループ検索をイネーブルにした場合は、Hit Count ツールを使用できません。オブジェクト グループ検索は、[Access Control Settings] ページ（31 ページ）で設定します。
- FQDN ネットワーク/ホストオブジェクトを含むルールを選択できますが、それらのオブジェクトはヒットカウントの結果では無視されます。

ナビゲーション パス

（デバイスビューのみ）[Access Rules] ページ （12 ページ）で、テーブル内のルールの [ヒットカウント（Hit Count）] セルを右クリックし、[ヒットカウントの詳細を表示（Show Hit Count Details）] を選択します。

[ヒットカウントの詳細（Hit Count Details）] ウィンドウが、アクセスルールテーブルの下部にペインとして開きます。タイトルバーの右側にある [展開（expand）] ボタンをクリックして、ヒットカウントの詳細を別のウィンドウに表示します。

関連項目

- アクセス ルールについて （1 ページ）
- テーブル カラムおよびカラム見出しの機能
- カテゴリ オブジェクトの使用

フィールド リファレンス

表 *7 : [ACE*ヒットカウントの詳細（*ACE Hit Count Details***）*]*ウィンドウ**

要素	説明
移行方法	ヒットカウント情報の表示方法として、[展開されたテーブル（Expanded Table）] または [未展開のACE（Raw ACE）] を選択できます（それぞれの説明を参照）。

要素	説明
展開されたテーブル	このビューには、このウィンドウを開いたときに [アクセスルール（Access Rules）] テーブル（ [Access Rules] ページ （12 ページ）） で選択したルールのアクセス制御リストエントリ（ACE）のヒットカウント情報が表示されます。ポリシーをデバイスに展開したときにアクセス ルールによって複数の ACE が生成された場合、このリストには複数の ACE が含まれます。 このテーブルの列は、[アクセスルール（Access Rules）] テーブルの列と対応していますが、ルールに含まれているネットワーク/ホスト、サービス、またはインターフェイス ロール オブジェクトの代わりに、ACE で設定されている特定のデータが含まれている場合があります。ただし、IOS 12.4(20)T 以降のデバイスは例外で、オブジェクトレベルのデータだけが表示されます。また、ACE を含む ACL の名前も表示されます。 [差分（Delta）] 列に、最後の更新以降の ACE に関するヒットカウントの差分が表示されます。[Hit Count] カラムには、ルール全体ではなく特定の ACE に対するヒット数が表示されます。 このテーブルの例については、 [サンプルヒットカウントの詳細（Sample Hit Count Details）] ウィンドウ （51 ページ） を参照してください。 **ヒント** 複数の列を同時にソートするには、Ctrl キーを押しながら列見出しをクリックします。ソートできるカラムは、[Interface]、[Direction]、および [ACL Name] 以外のカラムです。
未展開のACE（Raw ACE）	このビューには、[ヒットカウント（Hit Count）] と [最後のヒット時刻（Last Hit Time）] とともに、アクセス制御エントリに対する実際の CLI が表示されます。デバイス コマンドを評価する方が慣れている場合は、この情報を使用してください。 このテーブルの例については、 [サンプルヒットカウントの詳細（Sample Hit Count Details）] ウィンドウ （51 ページ） を参照してください。

要素	説明
（注）	• バージョン 4.9 以降、Cisco Security Manager では、[展開されたテーブル（Expanded Table）] と [未展開のACE（Raw ACE）] オプションでヒットカウントの履歴を表示できます。[履歴を表示（Show History）] リンクをクリックして、新しいウィンドウにヒットカウントの履歴を表示します。この新しい [ヒットカウント履歴の詳細（Hit Count History Details）] ウィンドウには、[ヒットカウント（Hit Count）] と [最後のヒット時刻（Last Hit Time）] の情報が表示されます。 • デバイスでオブジェクトグループ検索を有効にすると、[展開されたテーブル（Expanded Table）] オプションと [未展開のACE（Raw ACE）] オプションでヒットカウント履歴を表示できません。

[サンプルヒットカウントの詳細（Sample Hit Count Details）] ウィンドウ

ヒットカウントレポートを生成して、アクセスルールポリシー内の各ルールがトラフィックに一致する頻度を判断できます。たとえば、インターフェイス ロールを使用してルールを定義し、ロールが複数のインターフェイスに適用された場合、アクセス ルールが複数の Access Control Entries（ACE; アクセス コントロール エントリ）として展開されると、展開された ACE ごとに個別のヒット カウント情報が表示されます。このヒット カウント結果には、他のタイプの ACL（クラス マップまたは AAA ルールで使用される ACL など）のカウントは示されません。

ASA 8.3(1) 以降のデバイスに関するアクセスルールの場合、ヒットカウントレポートには、アクセスルールポリシーがトラフィックに最後に適用された時刻も表示されます。この情報は、他のポリシーの変更によって置き換えられた可能性のあるルールを判断するのに役立ちます。

ヒット カウント情報を使用すると、アクセス ルールのデバッグに役立ちます。この情報は、ヒットしたことがない（つまり、不要であるか、または ACL における優先度の高いルールと重複している可能性がある）ルールや、頻繁にヒットする（つまり、改良が必要な）ルールを識別するのに役立ちます。

次の各図に、ヒット カウント レポートの例と情報の使用方法を示します。

- 図 3 : 展開されたテーブル （53 ページ）は、デフォルトのビューを示しています。上半分のテーブルには、アクセス ルール ポリシー内に存在するルールが一覧表示されます。すべてのルールが表示されるか、またはレポートの生成前に選択したルールだけが表示されます。ルールを選択すると、そのルールに対してデバイス上で作成された ACE が、ウィンドウの下半分の展開されたテーブル内に一覧表示されます。最初にレポートを開くと、展開されたテーブルに、上半分のテーブル内に一覧表示されているすべてのポリシーに対する ACE が表示されます。

展開されたテーブル内のヒット カウントは、各 ACE に対応しています。一方、ルール テーブル内のカウントは、ルールにより作成されたすべての ACE に対するヒット カウントの合計で

す。ASA/PIX/FWSM デバイスおよび 12.4(20)T よりも前の IOS デバイスでは、展開されたテーブルに、ルールで使用されているポリシー オブジェクト内の各要素に対するヒット カウントが表示されます。一方、IOS 12.4(20)T+デバイスでは、オブジェクト グループ レベルの情報だけが提供されます。

- 図 4 : 未展開の ACE テーブル （54 ページ）は同じ ACE を CLI 形式で示しています。これらは、デバイス設定に存在する ACE です。

  ヒット カウント レポートの判読および解釈方法の詳細については、 ヒットカウントの詳細の表示 （48 ページ）を参照してください。

図 *3 :* 展開されたテーブル

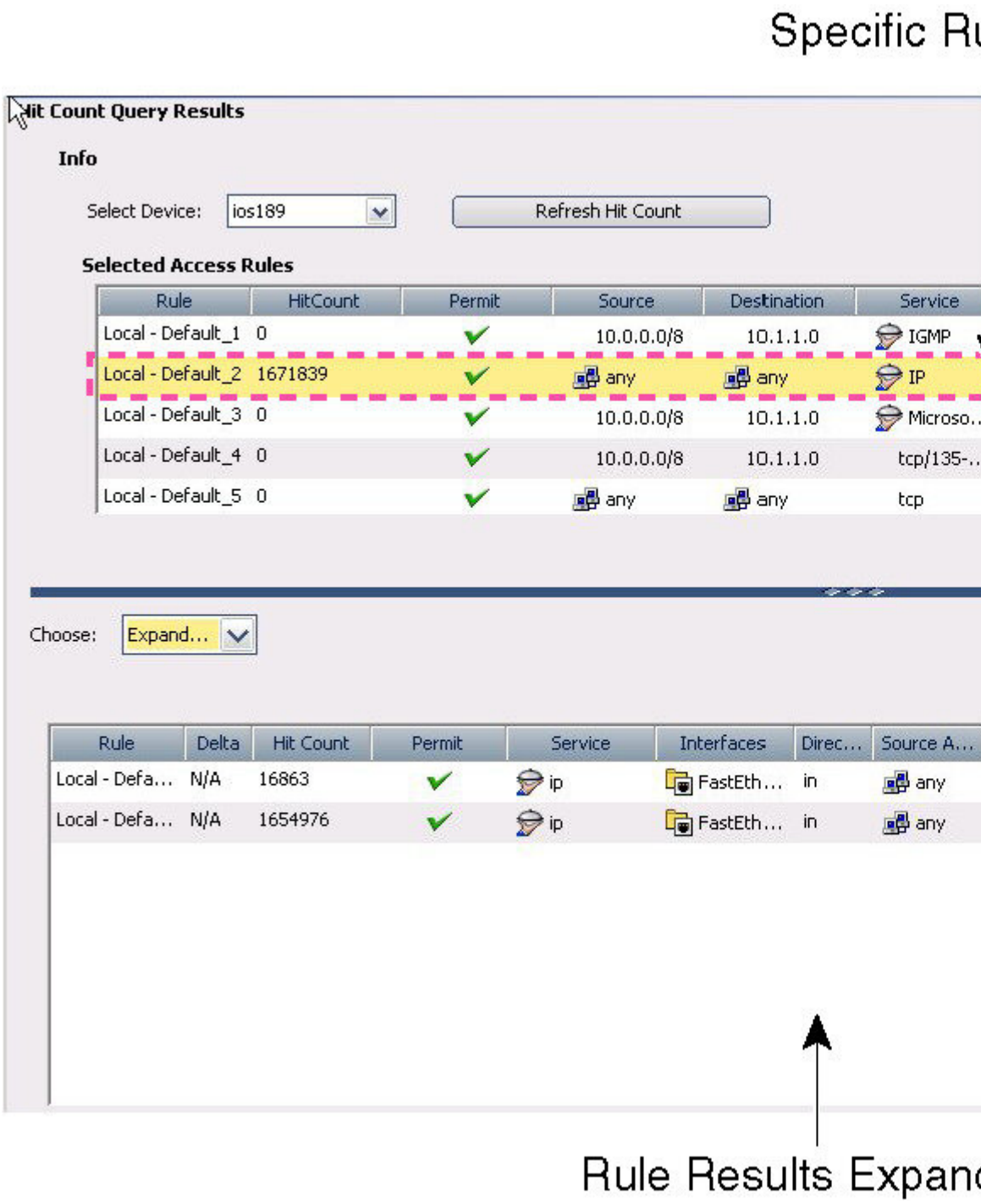
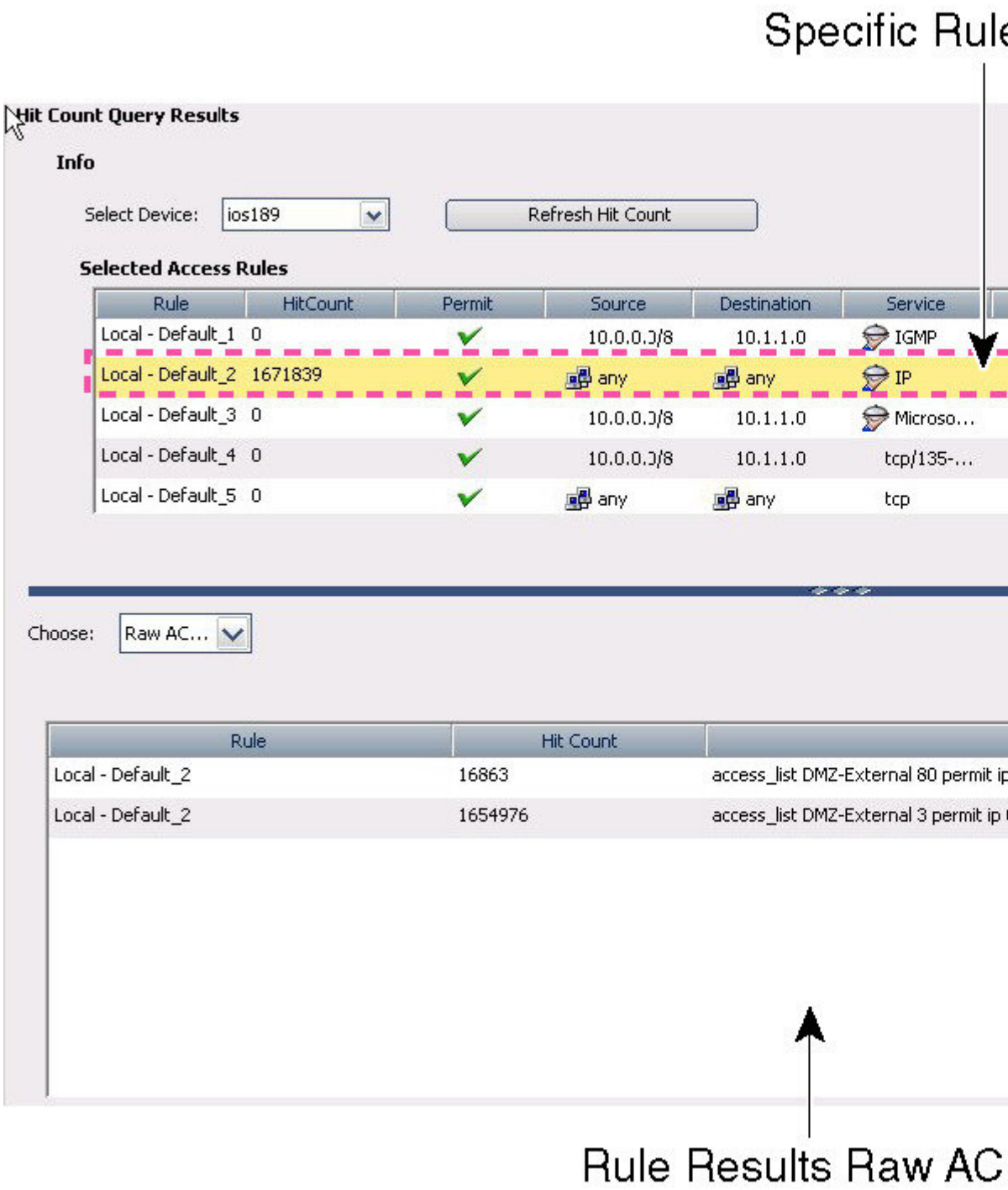


図 *4* : 未展開の *ACE* テーブル



関連項目

- アクセス ルールについて （1 ページ）

• アクセス ルールの設定 （8 ページ）

ルールのインポート

通常、デバイスを Security Manager に追加するときは、デバイスからポリシーを検出します。この処理により、デバイス上のすべてのアクティブなACLからのアクセス制御エントリ（ACE）が、アクセスルールポリシーに移入されます。

ポリシーに使用する ACE が含まれる ACL が他に存在している場合は、Security Manager で ACE を直接定義できます。

別の方法として、デバイス実行コンフィギュレーションからCLIエントリをコピーアンドペーストするか、目的のコマンドを入力することにより、ACEをインポートすることもできます。Import Rules ウィザードを使用すると、ACE および関連付けられたポリシーオブジェクトを、すでに機能している ACL からすばやく作成できます。また、ルールを定義するのに CLI コマンドを使用する方が慣れている場合は、この方法を使用すると便利です。

次の手順では、Import Rules ウィザードを使用して CLI ベースのルールを追加し、結果をプレビューする方法について説明します。

ステップ 1 （デバイスビューのみ）[ファイアウォール（Firewall）] > [アクセスルール（Access Rules）] を選択して、[Access Rules] ページ （12 ページ）を開きます。

ステップ 2 ルールの追加位置のすぐ上の行を選択します。ローカル範囲内の行を選択してください。行を選択しなかった場合は、ローカル範囲の最後にルールが追加されます。

ステップ 3 ルールテーブル内の任意の場所を右クリックし、[ルールのインポート（Import Rules）] を選択してウィザードを開始します。

3 ページのウィザードの最初のページ（[パラメータの入力（Enter Parameters）]）が表示されます。

ステップ 4 Import Rules ウィザード - [Enter Parameters] ページ （56 ページ） で、次の手順を実行します。

- 選択したデバイスに適した実行コンフィギュレーション形式で、目的の CLI 情報を入力します。インポート可能な CLI ベースのルールの例については、 インポートされたルールの例 （60 ページ）を参照してください。
- インターフェイス固有のルールの作成（その後にルールを適用するインターフェイスまたはインターフェイスロールを入力します）と、グローバルルールの作成（ASA 8.3+ デバイスの場合）のいずれかを選択します（ グローバル アクセス ルールについて （3 ページ）を参照）。
- インターフェイスに対するトラフィック方向を指定します（グローバルルールの場合、方向は常に [イン（In）] です）。

アクセス制御ルール以外に、次の項目がアクセス制御ルールによって参照される場合は、それらの項目も CLI 情報に含める必要があります。これらの項目を含めない場合、インポートを成功させるには、名前付きオブジェクトが Security Manager ですでに定義されている必要があります。

- 時間範囲オブジェクト（**time-range** コマンドとそのサブコマンド）。これにより、時間範囲ポリシー オブジェクトを作成できます。
- PIX、ASA、FWSM、および IOS 12.4(20)T+ デバイスの場合、オブジェクトグループ（**object-group** コマンドとそのサブコマンド）。これにより、ネットワーク/ホスト ポリシー オブジェクトを作成できます。

また、ASA 8.3 以降のデバイスの場合は、**object network** コマンドおよび **object service** コマンドを含めることができます。ただし、オブジェクト NAT 設定はインポートされません。

ステップ 5 [次へ（Next）] をクリックすると、ルールが処理され、Import Rules ウィザード - [Status] ページ （58 ページ）が開きます。

CLI の入力内容にエラーがある場合、[次へ（Next）] ボタンをクリックすると、プロンプトが表示されます。入力可能なコマンドに関するヒントについては、Import Rules ウィザード - [Enter Parameters] ページ（56 ページ）を参照してください。

CLI が評価され、インポート可能な場合は、CLI から作成されたオブジェクトのタイプが通知されます。

ステップ 6 [次へ（Next）] をクリックしてImport Rules ウィザード - [Preview] ページ （59 ページ）でルールおよびオブジェクトを確認するか、[完了（Finish）] をクリックしてルールをプレビューなしでインポートします。

[Preview] ページの情報は読み取り専用です。ルールに問題がなければ、[完了（Finish）] をクリックします。

変更する場合は、[戻る（Back）] ボタンをクリックしてウィザードの [パラメータの入力（Enter Parameters）] ページに戻るか、[完了（Finish）] をクリックして [アクセスルール（Access Rules）] ページでルールを編集します。

Import Rules ウィザード - [Enter Parameters] ページ

Import Rules ウィザードを使用して、ACL からデバイス実行コンフィギュレーション形式の一連のアクセス コントロール エントリをアクセス ルール ポリシーにインポートします。入力可能なコマンド構文は、ルールのインポート先のデバイスのタイプによって決まります。

アクセス制御ルール以外のルールによって参照される場合は、次の項目も CLI に含める必要があります。これらの項目を含めない場合、インポートを成功させるには、名前付きオブジェクトが Cisco Security Manager ですでに定義されている必要があります。

- 時間範囲オブジェクト（**time-range** コマンドとそのサブコマンド）。
- PIX、ASA、FWSM、および IOS 12.4(20)T デバイスの場合、オブジェクトグループ（**object-group** コマンドとそのサブコマンド）。

また、ASA 8.3 以降のデバイスの場合は、**object network** コマンドおよび **object service** コマンドを含めることができます。ただし、オブジェクト NAT 設定はインポートされません。

ナビゲーション パス

（デバイスビューのみ） [Access Rules] ページ （12 ページ）のルールテーブル内の任意の場所を右クリックし、[ルールのインポート（Import Rules）] を選択します。

関連項目

- ルールのインポート （55 ページ）
- インターフェイス ロール オブジェクトについて

フィールド リファレンス

表 *8 : Import Rules - [Enter Parameters]* ダイアログボックス

要素	説明
CLI	インポートするルールおよび関連オブジェクトを定義する OS コマンド。これらのルールは実行コンフィギュレーション形式にする必要があるため、設定からコピーして貼り付ける（Ctrl+V を使用してフィールドに貼り付ける）方法が最適です。また、コマンドを手動で入力することもできます。コマンドを解釈できない場合は、プロンプトが表示されます。 一度にインポートできる ACL は、1 つだけです。 インポートできる CLI の例については、 インポートされたルールの例 （60 ページ）を参照してください。 **ヒント** • オブジェクトを参照するが CLI を含めない場合、ルールは作成可能ですが、そのオブジェクトは使用されません。 • PIX、FWSM、ASA、および IOS 12.4(20)T+ の場合、オブジェクト グループおよび名前のコマンドを含めることができます。 • 非アクティブな ACL をインポートすると、その ACL は Security Manager に無効な状態で表示されます。設定を展開すると、その ACL はデバイスから削除されます。 • 拡張 ACL は、すべてのデバイス タイプに対してインポートできます。IOS デバイスに対しては標準 ACL をインポートできます。ただし、標準 ACL は拡張 ACL に変換されます。

要素	説明
インターフェイス（Interface） Global（ASA 8.3+）	インターフェイス固有のルールまたはグローバル ルールのいずれをインポートするかを選択します。グローバル ルールは ASA 8.3+ のデバイスだけで使用でき、特別なルールに従って処理されます（詳細については、グローバル アクセス ルールについて （3 ページ）を参照してください）。 [インターフェイス（Interfaces）] を選択した場合は、このルールを定義するインターフェイスまたはインターフェイスロールの名前を入力します。あるいは、[選択（Select）] をクリックして、リストからインターフェイスまたはロールを選択するか、または新しいロールを作成します。インターフェイスをリストに表示するには、あらかじめ定義しておく必要があります。インターフェイスまたはインターフェイス ロール名の任意の組み合わせを、カンマで区切って入力できます。
トラフィックの方向	インターフェイスに対するトラフィックの方向（[in] または [out]）。
カテゴリ	ルールに割り当てられるカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。カテゴリ オブジェクトの使用 を参照してください。

Import Rules ウィザード - [Status] ページ

Import Rules ウィザードの [Status] ページを使用して、インポート プロセスの結果に関する情報を参照します。

ナビゲーション パス

Import Rules ウィザードの開始方法の詳細については、Import Rules ウィザード - [Enter Parameters] ページ （56 ページ）を参照してください。

関連項目

- ルールのインポート （55 ページ）

フィールド リファレンス

表 9 : Import Rules ウィザード - [Status] ページ

要素	説明
進行状況バー	インポート プロセスのステータスが表示されます。
ステータス	インポートされた設定のステータス。
Rules Imported	インポートされるルールの数。

要素	説明
Policy Objects Created	作成されるポリシー オブジェクトの数。
メッセージ	重大度アイコンで示された、警告、エラー、および情報のメッセージ。通常の情報メッセージには、操作中に作成されたポリシー オブジェクトや、再利用された既存のポリシー オブジェクトの説明が表示されます。 項目を選択すると、右側の [Description] ボックスに詳細なメッセージが表示されます。右側の [Action] ボックスには、問題の修正方法が表示されます。
[Abort] ボタン	インポート操作を停止するには、このボタンをクリックします。

Import Rules ウィザード - [Preview] ページ

Import Rules ウィザードの [Preview] ページを使用して、[Finish] をクリックするとインポートされるルールおよびオブジェクトを確認します。

このプレビューは読み取り専用であるため、ルールまたはオブジェクトの編集はできません。ルールまたはオブジェクトの内容が希望どおりでない場合は、[Finish] をクリックしてルールおよびオブジェクトを追加し、アクセス ルール ページでそれを編集できます。たとえば、ルールの有効期限は Security Manager でだけ有効であるため、インポートできません。

このダイアログボックスのタブが表示されるのは、インポート対象のデータに、そのタブに表示される項目が含まれている場合だけです。

ヒント CLI が存在しないオブジェクト（時間範囲など）を参照している場合、そのオブジェクトはルールに含められません。前に戻ってそのオブジェクトの CLI を追加するか、または [Finish] をクリックし、手動でオブジェクトを作成して、ルールを編集することができます。

ナビゲーション パス

Import Rules ウィザードの開始方法の詳細については、Import Rules ウィザード - [Enter Parameters] ページ （56 ページ）を参照してください。

関連項目

- ルールのインポート （55 ページ）
- [Access Rules] ページ （12 ページ）
- ネットワーク/ホストオブジェクトについて
- インターフェイス ロール オブジェクトについて
- サービスとサービス オブジェクトおよびポート リスト オブジェクトの理解と指定

- テーブルのフィルタリング

フィールド リファレンス

表 *10 : Import Rules* ウィザード - *[Preview]* ページ

要素	説明
[Rules] タブ	アクセス ルール ポリシーにインポートされる、CLI から作成されたルール。CLI が標準 ACL に対応している場合でも、すべてのルールは拡張形式に変換されます。 アイコンにより、許可および拒否のステータスが示されます。 • [Permit]：緑色のチェック マークとして表示されます。 • [Deny]：スラッシュの入った赤色の丸として表示されます。 送信元、宛先、サービス、およびインターフェイスのセルを右クリックして [コンテンツの表示（Show Contents）] を選択すると、そのセル内に詳細情報が表示されます。 右クリックして [コピー（Copy）] を選択すると、ルールを HTML 形式でクリップボードにコピーできます。このデータをテキストエディタに貼り付けることもできます。
[Objects] タブ	CLI から作成されたポリシー オブジェクト（ある場合）。CLI に応じて、Security Manager により時間範囲、ネットワーク/ホスト オブジェクト、サービス オブジェクト、またはポート リスト オブジェクトが作成されることがあります。 オブジェクトを右クリックして [オブジェクトの表示（View Object）] を選択すると、オブジェクト定義が読み取り専用形式で表示されます。

インポートされたルールの例

次に、インポート可能な CLI と、その CLI から作成されたルールおよびポリシー オブジェクトの例をいくつか示します。ルールのインポート方法の詳細については、ルールのインポート（55 ページ）を参照してください。

例 1：ネットワークから FTP サーバへのアクセスを制限する（ASA デバイス）

次のアクセス リストでは、オブジェクト グループを使用して、10.200.10.0/24 ネットワークから一部の FTP サーバへのアクセスを制限しています。他のトラフィックはすべて許可されます。

```
object-group network ftp_servers
network-object host 172.16.56.195
network-object 192.168.1.0 255.255.255.224
access-list ACL_IN extended deny tcp 10.200.10.0 255.255.255.0 object-group ftp_servers
```

```
access-list ACL_IN extended permit ip any any
```

この例では、ftp_servers という名前の 1 つのネットワーク/ホスト オブジェクトと、2 つのアクセス ルールが作成されます。

No.	Permit	Source	Destination	Service	Interface	Dir.	Category
1	⊘	10.200.10.0/24	ftp_servers	TCP	Ethernet0	in	None
2	✓	any	any	IP	Ethernet0	in	None

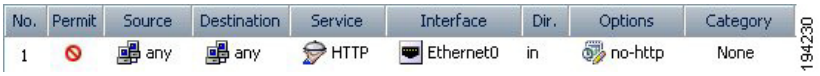
194227

例 2：勤務時間中の Web アクセスを制限する（ASA デバイス）

次の例では、午前 8 時～午後 6 時の間（通常の勤務時間）の HTTP 要求を拒否しています。

```
time-range no-http
 periodic weekdays 8:00 to 18:00
access-list 101 deny tcp any any eq www time-range no-http
```

この例では、no-http という名前の 1 つの時間範囲オブジェクトと、1 つのアクセス ルールが作成されます。



No.	Permit	Source	Destination	Service	Interface	Dir.	Options	Category
1	⊘	any	any	HTTP	Ethernet0	in	no-http	None

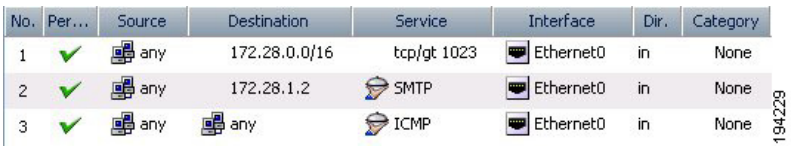
194230

例 3：ポート番号を使用して TCP および ICMP をフィルタリングする（IOS デバイス）

次の例では、goodports という名前の拡張アクセス リストの最初の行で、1023 よりも大きい宛先ポートを持つ着信 TCP 接続を許可しています。2 行目で、ホスト 172.28.1.2 の Simple Mail Transfer Protocol（SMTP）ポートへの着信 TCP 接続を許可しています。最後の行では、エラー フィードバックのための着信 ICMP メッセージを許可しています。

```
ip access-list extended goodports
 permit tcp any 172.28.0.0 0.0.255.255 gt 1023
 permit tcp any host 172.28.1.2 eq 25
 permit icmp any 172.28.0.0 255.255.255.255
```

この例では、3 つのアクセス ルールが作成されます。IOS ACL 構文で使用されているワイルドカード マスクは通常のサブネット マスクに変換されることに注意してください。Security Manager は、標準のネットワーク/ホスト サブネット マスク指定と、IOS ACL で必要なワイルドカード マスクの間で自動変換を行います。ASA/PIX/FWSM では、ACL コマンド内にサブネットマスクを使用する必要があるため、すべてのデバイスに適用可能なルールを作成することが可能になります。Security Manager によって、ルールが正しい構文に変換されます。



No.	Per...	Source	Destination	Service	Interface	Dir.	Category
1	✓	any	172.28.0.0/16	tcp/gt 1023	Ethernet0	in	None
2	✓	any	172.28.1.2	SMTP	Ethernet0	in	None
3	✓	any	any	ICMP	Ethernet0	in	None

194229

例 4：ホストを制限する標準 ACL（IOS デバイス）

次の例では、Jones に属するワークステーションがイーサネット インターフェイス 0 へのアクセスを許可され、Smith に属するワークステーションはアクセスを許可されていません。

```
ip access-list standard workstations
 remark Permit only Jones workstation through
 permit 172.16.2.88
 remark Do not allow Smith workstation through
 deny 172.16.3.13
```

この例では、（任意の宛先に対して）標準ルールを拡張ルールに変換する2つのルールが作成されます。備考は、[description] フィールドに保存されます。

No.	Permit	Source	Destination	Service	Interface	Dir.	Description
1	✓	172.16.2.88	any	IP	Ethernet0	in	Permit only Jo...
2	⊘	172.16.3.13	any	IP	Ethernet0	in	Do not allow S...

194228

コマンド言語形式での ACL のその他の例については、次の URL を参照してください。

- IOS デバイス：http://www.cisco.com/en/US/docs/ios/sec_data_plane/configuration/guide/sec_create_IP_apply.html#wp1027258
- ASA デバイス：http://www.cisco.com/en/US/docs/security/asa/asa82/configuration/guide/acl_extended.html

展開中のアクセス ルールの自動最適化

特定のデバイスまたはすべてのデバイスに展開するときに、アクセス ルール ポリシーから作成されたアクセス コントロール リスト（ACL）が最適化されるようにシステムを設定できます。この最適化の影響を受けるのは、展開されたポリシーだけであり、アクセス ルール ポリシーは変更されません。

最適化によって、冗長性と競合がなくなり、複数のエントリ（ACE）を単一エントリに結合できます。エントリの順序は変更されても、ポリシーの意味は保持されます。つまり、最適化された ACL は、最適化されていないフォームのときと同じパケット セットを受け入れるか、または拒否します。次に、変更が行われる基本的なケースを示します。

- 非効率的な ACE：あるエントリが別のエントリのサブセットになっているか、または別のエントリと同一である場合、非効率的な ACE が削除されます。次の例を考えてみます。

```
access-list acl_mdc_inside_access deny ip host 10.2.1.1 any
access-list acl_mdc_inside_access deny ip 10.2.1.0 255.255.255.0 any
```

最初の ACE は実際には 2 番めの ACE のサブセットです。ACL の最適化では、2 番めのエントリだけが展開されます。

- スーパーセット ACE：あるエントリが別のエントリのスーパーセットであり、ルールの順序が重要ではない場合、冗長なルールが削除されます。次の例を考えてみます。

```
access-list acl_mdc_inside_access permit tcp any any range 110 120
access-list acl_mdc_inside_access deny tcp any any range 115
```

2 番めの ACE がヒットすることはありません。ACL の最適化により 2 番めの ACE が削除され、最初の ACE だけが展開されます。

- 隣接する ACE：2 つのエントリがよく似ているため、1 つのエントリで同じジョブを実行できる場合。各ルールにヒットするパケットが変更されるような介入ルールは存在できません。次の例を考えてみます。

```
access-list myacl permit ip 1.1.1.0 255.255.255.128 any
access-list myacl permit ip 1.1.1.128 255.255.255.128 any
```

2 つの ACE がマージされて 1 つの ACE になります（access-list myacl permit ip 1.1.1.0 255.255.255.0 any）。

ACL の展開最適化を設定することにより、作成される ACL が小さくなり、効率も高くなります。これにより、拡張不可能な制約付きのメモリ（FWSM など）を搭載するデバイスでのパフォーマンスを改善し、これを複数の仮想コンテキスト間で共有できます。

ただし、ACL の展開最適化の設定にはデメリットもあります。

- 最適化を行うと、アクセス ルールに対して通常展開される内容が変更されるため、これらのルールを実際に展開されている ACE と相互に関連付けることが困難になります。この場合、ヒット カウント ツールの結果が使用できなくなることがあり、Cisco Security Monitoring, Analysis and Response System アプリケーションでイベントを相互に関連付けることが非常に困難になります。これらのツールを使用してアクセス ルールをモニタすることが必要な場合は、最適化をイネーブルにしないでください。詳細については、ヒットカウントの詳細の表示 （48 ページ）およびIPS シグニチャの CS-MARS イベントの表示を参照してください。
- 最適化を行っても、アクセス ルール ポリシー内の本質的な問題は解決されません。通常は、自動競合検出ツールを使用して冗長性と競合を事前に解決することを推奨します（自動競合検出の使用 （37 ページ）を参照）。また、展開の前に、ルール結合ツールを使用して、アクセス ルール ポリシー内のルールを最適化することもできます（ルールの結合を参照）。

ACL の展開最適化を設定することにした場合は、メモリ制約のあるデバイスに対してだけイネーブルにすることを検討してください。

ステップ 1 Security Manager サーバ上の Windows にログインします。

ステップ 2 NotePad などのテキストエディタを使用して、**C:\Program Files\CSCOpx\MDC\athena\config\csm.properties** ファイルを開きます。最適化のセクションを見つけて、指示を確認します。

- すべてのデバイスに対して完全な最適化を有効にするには、次のように入力します。

OPTIMIZE.*=full

- 特定のデバイスに対して完全な最適化を有効にするには、アスタリスクを、そのデバイスに対する Security Manager の表示名で置き換えます。たとえば、表示名が west_coast.cisco.com の場合は、次のように入力します。

OPTIMIZE.west_coast.cisco.com=full

- 最適化を有効にするが、ACE で使用されているオブジェクト グループを保持する場合は、キーワード全部を preserve_og で置き換えます。次に例を示します。

OPTIMIZE.west_coast.cisco.com=preserve_og

- 隣接するエントリをマージしない場合は、次のように入力します。

AclOptimization.doMerge=false

ステップ 3 ファイルを保存します。設定は即時に有効になり、後続のすべての展開ジョブに適用されます。

展開ジョブの最適化レポートを生成するには、**[ツール（Tools）] > [Cisco Security Manager管理（Security Manager Administration] > [デバッグオプション（Debug Options）]** から [検出/展開デバッグスナップショットのファイルへのキャプチャ（Capture Discovery/Deployment Debugging Snapshots to File）] を選択します。

展開結果には、情報メッセージとして要約された最適化結果が表示されます。これには、最適化前の最初の ACE の数と、最適化後の ACE の数が含まれます。結果は、サーバ上の C:\Program Files\CSCOpx\MDC\temp フォルダ内のファイルに保存されます。ファイル名の一部としてジョブ ID が使用されます。

[アクセスルールの追加（Add Access Rule）] ダイアログでのデフォルトのカスタマイズ

Cisco Security Manager 4.13 より前は、[アクセスルールの追加（Add Access Rule）] ダイアログにデフォルト値が入力されていました。4.13 以降、ユーザーは csm.properties ファイルを更新することにより、デフォルト値の状況をカスタマイズできます。

[アクセスルールの追加（Add Access Rule）] ダイアログでデフォルトをカスタマイズするには、次の手順を実行します。

ステップ 1 Cisco Security Manager インターフェイスを閉じて終了します。

ステップ 2 NotePad などのテキストエディタを使用して、**C:\Program Files\CSCOpx\MDC\athena\config\csm.properties** ファイルを開きます。

ステップ 3 csm.properties ファイルの下部にある CustDesk.Rule プロパティを見つけ、要件に基づいて値を true または false に設定します。

- CustDesk.Rule.Add.Op.Load.Intf.Default.Values：この値を true に設定すると、[アクセスルールの追加（Add Access Rule）] ダイアログでデフォルトのインターフェイス情報がロードされます。
- CustDesk.Rule.Add.Op.Load.Other.Default.Values：この値を true に設定すると、[アクセスルールの追加（Add Access Rule）] ダイアログで他のデフォルト値がロードされます。

ステップ 4 ファイルを保存します。

（注） この変更はすぐには有効になりません。カスタマイズしたデフォルト値を有効にするには、Cisco Security Manger サービスを再起動します。

ステップ 5 Cisco Security Manager インターフェイスを再度起動します。

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。