ファイアウォール サービスの概要

Firewall ポリシー フォルダ（デバイス ビューまたはポリシー ビュー）には、ファイアウォールに関連するポリシーが含まれています。これらのポリシーは、Adaptive Security Appliance（ASA; 適応型セキュリティ アプライアンス）、PIX ファイアウォール（PIX）、Catalyst Firewall Services Module（FWSM; ファイアウォール サービス モジュール）、および Cisco IOS ソフトウェアを実行しているセキュリティ ルータに展開できます。これらのポリシーを使用すると、デバイスを介したネットワーク アクセスを制御できます。

この章は次のトピックで構成されています。

ファイアウォール サービスの概要

Firewall ポリシーフォルダ（デバイスビューまたはポリシービュー）には、ファイアウォールに関連するポリシーが含まれています。これらのポリシーは、適応型セキュリティアプライアンス（ASA）、PIX ファイアウォール（PIX）、Catalyst Firewall Services Module（FWSM）に展開できます。

（注）　バージョン 4.21 以降、Cisco Security Manager は、すべてのアグリゲーション サービス ルータ、統合サービスルータ、組み込み型サービスルータ、および Cisco IOS ソフトウェアで動作するすべてのデバイスについて、バグ修正または拡張機能のサポートを含むサポート全体を終了します。

これらのポリシーは、デバイスへのアクセス（つまり、デバイスの設定を変更したり **show** コマンドを使用したりするためにデバイスにログインすること）ではなく、デバイスを介したアクセスの制御に焦点を置いたものです。次に、使用可能なファイアウォール ポリシーについて概説し、詳細な情報を示す項へのポインタを示します。

- AAA ルール：AAA ファイアウォールまたは認証プロキシのルールです。これにより、ユーザが（ユーザ名とパスワードを使用した）認証および認可（任意）を受けて初めて、デバイスを介したネットワーク接続がユーザに許可されるように設定できます。また、ア

ファイアウォール サービスの概要

カウンティング、セキュリティ、またはリソース割り当て情報を作成することもできます。詳細については、AAA ルールについてを参照してください。

- アクセス規則：従来的なインターフェイスベースの拡張アクセス コントロール規則です。パケットは、送信元アドレス、宛先アドレス、送信元インターフェイス、およびサービスに基づいて許可または拒否されます。これらのルールは、in 方向と out 方向のどちらにも適用できます。詳細については、アクセス ルールについてを参照してください。
- インスペクション ルール：従来的な Context-Based Access Control（CBAC; コンテキストベース アクセス コントロール）であり、アプリケーション レイヤ プロトコル セッション情報に基づいて不正な TCP/UDP パケットをフィルタで除外し、選択したサービスの戻りトラフィックをイネーブルにします。詳細については、インスペクション ルールについてを参照してください。
- Web フィルタ ルール：要求された URL に基づいて Web トラフィックをフィルタリングするタイプのインスペクション ルールです。これにより、望ましくない Web サイトへの接続を阻止できます。詳細については、Web フィルタ ルールについてを参照してください。
- ゾーンベースのファイアウォール ルール：インターフェイスではなくゾーンに基づいてルールを設定する場合、これらのルールで、IOS デバイス上のアクセス ルール、インスペクション ルール、および Web フィルタ ルールを置き換えます。ゾーンとは、同じセキュリティ ロールを実行する定義済みのインターフェイス グループのことです（Inside や Outside など）。ゾーン ルールを使用すると、他のタイプのルールを使用するよりもコンパクトなデバイス設定を作成できます。詳細については、ゾーンベースのファイアウォール ルールについてを参照してください。
- ボットネット トラフィック フィルタ ルール：これらのルールを使用すると、既知の不正なアドレスに送信されたボットネット トラフィックを見つけることができます。ボットネットは、無警戒なコンピュータ上に悪意のあるソフトウェアをインストールし、これらのコンピュータをプロキシとして使用して悪意のあるアクションを実行します。詳細については、ファイアウォールの Botnet Traffic Filter ルールの管理を参照してください。
- トランスペアレント ルール：トランスペアレント インターフェイスまたはブリッジド インターフェイス上の非 IP のレイヤ 2 トラフィックに適用される Ethertype アクセス コントロール ルールです。詳細については、トランスペアレント ファイアウォール ルールの設定を参照してください。

ほとんどのファイアウォール ルール ポリシーは、ルール テーブル内で設定します。これらのテーブルを使用すると、ほとんどのセルのインライン編集、セクションを使用したルール編成、およびルールの順序変更を行うことができます。共有ルール ポリシーを作成すると、多数のデバイス（異なるオペレーティング システムを実行しているデバイスを含む）にそれを適用できます。Security Manager により適切なデバイス コマンドが自動的に作成されて、個々のデバイスの特性に基づいてポリシーが設定され、デバイスに適用されない設定はフィルタで除外されます。ルール テーブルの使用方法の詳細については、ルール テーブルの管理 （9 ページ）を参照してください。

また、ほとんどのファイアウォール ルール ポリシーで使用される強力な機能に、継承という考え方があります。共有ポリシーを作成するとき、デバイスにポリシーを割り当てるのではな

く、デバイスにポリシーを継承させるという選択もできます。このため、一方で一連の共有ルールをすべてのデバイスに適用し、他方で固有のルールを該当のデバイスだけに適用することができます。継承の詳細については、次の項を参照してください。

- ルールの継承について
- 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

ここでは、ファイアウォール サービス ポリシーの概要について説明します。

- ファイアウォール ルールの処理順序について （3 ページ）
- NAT がファイアウォール ルールに与える影響について （4 ページ）
- Security Manager によって保持される ACL 名 （5 ページ）

ファイアウォール ルールの処理順序について

ファイアウォール ルール ポリシーを設定する際は、ルールが処理される論理順序を覚えておく必要があります。たとえば、あるアクセス ルールで特定タイプのすべてのトラフィックをドロップする場合は、そのタイプのトラフィックに適用されるルールを他のファイアウォール ポリシー内に作成しても意味がありません。そのようなルールがトリガーされることはないためです。逆に、特定タイプのインスペクションまたは Web フィルタリングをトラフィックに適用する場合は、そのトラフィックがデバイスに入ることを、このアクセス ルールが最初に許可するように設定する必要があります。

ファイアウォール ルールの一般的な論理処理順序は、次のとおりです。

- AAA ルール：（認可の有無に関係なく）認証が必要な場合、ユーザはテストに合格する必要があります。合格しない場合、トラフィックはドロップされます。
- アクセスルール（イン方向）：トラフィックがアクセスルールを通過する必要があります。AAA ルールを使用する場合、ユーザーのセッションに対してユーザー単位の一時的なアクセスルールを設定できます。これらのユーザ単位のルールは、Security Manager ではなく AAA サーバで設定します。

  ASA 8.3 以降のデバイスでは、グローバル アクセス ルールはインターフェイス固有のアクセス ルールのあとに処理されます。詳細については、グローバル アクセス ルールについてを参照してください。
- 検査ルール（イン方向）、Web フィルタルール（イン方向）、ボットネットルール、サービスポリシールール（IPS、QoS、接続）：これらのすべてがトラフィックに適用されます。方向を設定できないデバイスの場合は、すべてのルールが In 方向であると見なされます。
- ゾーンベースのファイアウォール ルール：IOS デバイスに対してゾーンベースのルールを設定した場合、これらのルールがインスペクション ルールと Web フィルタ ルールを置き換えます（ボットネット ルールは IOS デバイスに適用されません）。

- 次に、ルーティングプロトコルがトラフィックに適用されます。トラフィックをルーティングできない場合、そのトラフィックはドロップされます（ルーティングポリシーは、各種デバイス タイプ用の Platform フォルダの中にあり、ファイアウォール ポリシーとは見なされません）。
- ScanSafe Web セキュリティポリシー、検査ルール（アウト方向）、Web フィルタルール（アウト方向）：IOS デバイスに限り、アウト方向で作成した ScanSafe ポリシー、検査ルールまたは Web フィルタルールが適用されるようになりました。
- アクセス規則（Out 方向）：最後に、トラフィックは Out 方向のアクセス規則を通過する必要があります。

トランスペアレント ルールはこの概要には該当しません。トランスペアレント ルールは非 IP のレイヤ2トラフィックだけに適用されるため、あるトランスペアレントルールがパケットに適用されると、その他のファイアウォールルールは適用されません。また逆に、他のルールが適用されると、そのトランスペアレント ルールは適用されません。

関連項目

- AAA ルールについて
- アクセス ルールについて
- インスペクション ルールについて
- Web フィルタ ルールについて
- ゾーンベースのファイアウォール ルールについて
- ファイアウォールの Botnet Traffic Filter ルールの管理
- トランスペアレント ファイアウォール ルールの設定

NAT がファイアウォール ルールに与える影響について

ファイアウォール規則をサポートしているデバイスでは、ネットワークアドレス変換（NAT）を設定することもできます。NAT は、パケット内の実際のアドレスを、宛先ネットワーク上のマップされているルーティング可能なアドレスと置き換えます。

NAT をインターフェイスで実行するように設定した場合、そのインターフェイスで同様に設定されているファイアウォール ルールで、元の（NAT 実行前の）アドレスではなく、変換されたアドレスに基づいてトラフィックが評価される必要があります（ASA 8.3+ デバイスの場合を除く）。

ASA ソフトウェアリリース 8.3 以降を実行しているデバイスでは、トラフィックを評価する際に、元の（実際の）IP アドレスが使用されます（IPSec VPN トラフィックポリシーの場合を除く）。このため、ファイアウォール ルール、ACL ポリシー オブジェクト、または IOS、QoS、および接続ルール プラットフォーム サービス ポリシーを設定する場合は、必ず元のアドレスを使用してください。

NAT の詳細については、次の項を参照してください。

- ASA、PIX、FWSM デバイス：ネットワーク アドレス変換について
- IOS デバイス：Cisco IOS ルータにおける NAT ポリシー

Security Manager によって保持される ACL 名

Security Manager は、ユーザー定義のアクセス制御リスト（ACL）名を、デバイスで設定されているとおりに保持しようとします。次の場合、Security Manager は、デバイスで設定されている ACL 名を保持できます。

- ACL 名が Security Manager で指定されている場合。

アクセスルールポリシーの場合、**[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）]** で ACL 名を指定できます。特定の名前を単一のインターフェイスおよび方向に対して指定できますが、その名前は、同じ ACL を使用する他のすべてのインターフェイスおよび方向に使用されます。デバイスで他のポリシーに割り当てる ACL ポリシー オブジェクトと同じ名前を使用することはできません。また、IPv4 ACL と IPv6 ACL に同じ名前を使用することはできません。

（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。Security Manager 4.4 および ASA 9.0+ では、これらのポリシーとポリシーオブジェクトが結合または統合されました。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、AAA ルール、アクセスルール、およびインスペクションルールのポリシータイプの IPv4 および統合バージョンが提供されます。

- ポリシーで ACL ポリシー オブジェクトを使用する場合、そのポリシー オブジェクトの名前が ACL 名に使用されます。検出中に作成された ACL ポリシーでは、可能なかぎり、デバイスで定義されている ACL の名前が使用されます。動作は管理設定によって異なります。
  - **[ツール（Tools）] > [Security Manager管理（Security Manager Administration）] > [検出（Discovery）]** の順に選択して [ポリシーオブジェクトでデバイスのオーバーライドを許可（Allow Device Override for Policy Objects）] を選択すると、同じ名前で内容が異なるポリシーオブジェクトが Security Manager に存在していれば、その名前が再利用され、デバイスレベルのオーバーライドが作成されます。
  - そのオプションを選択しない場合は、同じ名前に番号を追加して（ACLobject_1 など）ポリシー オブジェクトが作成されます。これはデフォルトの動作です。
- **[ツール（Tools）] > [Security Manager管理（Security Manager Administration）] > [展開（Deployment）]** の順に選択して表示される [ファイアウォールアクセスリスト名（Firewall

Access List Names）] 設定で [既存の名前を再利用（Reuse Existing Names）] を選択した場合、ACL を生成するファイアウォールルールに対して、デバイスで定義されている名前が再利用されます。

- ACL が共有されない場合（Security Manager で ACL の内容を変更した場合も同じ）。
- ACL は共有されるが、その ACL を共有する各ポリシーが Security Manager で同様には定義されていない場合。ACL の内容を変更すると、1 つの ACL が名前を保持し、その他の ACL には生成された名前が割り当てられます。

（注） ASA デバイス、またはバージョン 6.3(x) を実行していない PIX デバイスでは、ACL 名が NAT ポリシー スタティック ルールで使用されていて、さらにオブジェクトグループを含んでいる場合、その ACL 名は Security Manager により再利用されません。ACL は、送信元として定義されているオブジェクトグループの内容とともに展開されます。これは、デバイスでは ACL 内のすべての ACE の送信元がすべて同じである必要があるためです。

ヒント

- ACL ポリシー オブジェクトの名前が、デバイスですでに定義されている ACL でも使用される名前と同じであり、既存の ACL が Security Manager でサポートされないコマンドに対応している場合は、展開エラーが発生し、別の名前を選択するよう要求されます。このエラーが発生した場合は、ポリシー オブジェクトの名前を変更します。
- IOS デバイスでは、<number>_<number> という名前の ACL は無効です。Security Manager により、展開前にサフィックスが取り除かれます。つまり、同じ番号のプレフィックスを使用して IOS デバイスを複数の ACL オブジェクトに割り当てることはできません。ただし、番号付きサフィックスを持つ名前の ACL は許可されます（ACLname_1 など）。
- 番号付き ACL では、IOS デバイスに対する適切な番号範囲を使用する必要があります。標準 ACL は、1 ～ 99 または 1300 ～ 1999 の範囲にする必要があります。拡張 ACL は、100 ～ 199 または 2000 ～ 2699 の範囲にする必要があります。
- IOS デバイスの ACL 名の開始文字をアンダースコア（_）にすることはできません。
- ユーザ定義の名前を保持しないポリシーには、SSL VPN ポリシー、トランスペアレント ファイアウォール ルール、および AAA ルール（IOS デバイスの場合）があります。

ここでは、ACL 命名に関する追加情報を提供します。

- ACL 命名ルール （7 ページ）
- ユーザー定義の ACL ポリシーの名前付けの競合の解決 （9 ページ）
- ポリシー間での ACL 名前競合の解決 （9 ページ）

ACL 命名ルール

ACL の名前が Security Manager により生成される場合、その名前は、定義しているルールまたはプラットフォームのタイプと、それを固有にしている設定から導出されます。新しく作成された ACL には、次の表に示す命名ルールに基づいて名前が割り当てられます。

ヒント　展開中、既存の ACL を編集できない場合は、サフィックス *.n*（n は整数）が付加されることがあります。たとえば、acl_mdc_outside_10 という名前の ACL がすでにデバイスに存在している場合、この古い ACL を削除せずに新しい ACL を展開すると、acl_mdc_outside_10.1 という名前の新しい ACL が作成されます。

表 *1 : ACL* 命名ルール

ポリシー タイプ	命名ルール
アクセス ACL	• インバウンド：CSM_FW_ACL_InterfaceName • アウトバウンド：CSM_FW_ACL_OUT_InterfaceName
IPv6 アクセス ACL	• インバウンド：CSM_IPV6_FW_ACL_InterfaceName • アウトバウンド：CSM_IPV6_FW_ACL_OUT_InterfaceName （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。Security Manager 4.4 および ASA 9.0+ では、これらのポリシーとポリシーオブジェクトが結合または統合されました。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、AAA ルール、アクセスルール、およびインスペクションルールのポリシータイプの IPv4 および統合バージョンが提供されます。
インスペクション ルール	• ASA 7.0+/PIX 7.0+：CSM_CMAP_ACL_n（n は 1 から始まる整数）。 • IOS デバイスの場合、番号付き ACL。
NAT0 ACL	• インバウンド：CSM_nat0_InterfaceName_in • アウトバウンド：CSM_nat0_InterfaceName

ポリシー タイプ	命名ルール
NAT ACL	• インバウンド：CSM_nat_InterfaceName_poolID_in • アウトバウンド：CSM_nat_InterfaceName_poolID （注） PIX 6.3(x) デバイスの場合、ACL 名には、add _dns（dns）、_nrseq（norandomseq）、_emb##（初期接続制限）、_tcp##（tcp の最大接続制限）、および _udp##（udp の最大接続制限）が追加されます。
NAT ポリシー スタティック変換ルール ACL	• PIX 6.3(x) デバイス： • IP の場合：CSM_static_globalIP_LocalInterfaceName_globalInterfaceName • その他のプロトコルの場合：CSM_static_globalIP_LocalInterfaceName_globalInterfaceName_protocol _globalPort • 他の OS バージョンを実行しているデバイスの場合、localIP 文字列が追加されます。 • IP の場合：CSM_static_localIP_globalIP_LocalInterfaceName_globalInterfaceName • その他のプロトコルの場合：CSM_static_localIP_globalIP_LocalInterfaceName_globalInterfaceName_protocol _globalPort
AAA ACL	PIX/ASA/FWSM の場合：CSM_AAA_{AUTHO | ATHEN | ACCT}_InterfaceName _ServerGroupName IOS デバイスの認証プロキシ： • NAC を使用しないインターフェイス：CSM_AUTH-PROXY_InterfaceName_traffic type_ACL。ここで、InterfaceName はルールが適用されるインターフェイスです。traffic type は、HTTP、Telnet、または FTP です。 • 同じインターフェイス上の AuthProxy および NAC：CSM_ADMISSION_ID_ACL。ここで、ID は Security Manager 内の NAC が適用されるインターフェイス ロールの内部識別子です。
Web フィルタ ルール ACL	ASA 7.0+/PIX 7.0+：デバイスはフィルタ コマンドに一致します。 IOS デバイスの場合、番号付き ACL。

ユーザー定義の ACL ポリシーの名前付けの競合の解決

Cisco Security Manager は、「CSM_」で始まる ACL 名を生成します。デバイスで ACL を定義するときは、同じ命名パターンを使用しないでください。デバイスで「CSM_」プレフィックスを使用して ACL 名を宣言すると、Cisco Security Manager でのデバイス設定の検出中に、それらの ACL 名は Security Manager で生成された名前に置き換えられ、それぞれの設定のデルタが次の展開でデバイスに適用されます。

たとえば、Cisco Security Manager には、着信ファイアウォール インターフェイスの ACL 命名パターンとして CSM_FW_ACL_InterfaceName があります。デバイスの ACL 名の宣言に CSM パターン（CSM_xyz など）を使用すると、Security Manager はその名前を「CSM_FW_ACL_InterfaceName」に変更します。

（注） このルールはファイアウォール アクセス リストに対して有効であり、[ツール（Tools）] > [Security Managerの管理（Security Manager Administration）] > [展開（Deployment）] で [既存の名前を再利用する（Reuse existing names）] 設定が選択されている場合でも、デルタが生成されてデバイスに適用されます。

ポリシー間での ACL 名前競合の解決

ACL は共有されるが、その ACL を共有するポリシーが Security Manager で同様には定義されていない場合、1 つのポリシーが ACL の元の名前を使用し、その他のポリシーは Security Manager により生成された新しい名前を使用します。元の名前を使用するポリシーを決定する際の優先順位は、次のとおりです。

- アクセス リスト ACL
- AAA ACL
- スタティック ACL
- NAT0 ACL
- NAT ACL

たとえば、アクセス ACL と NAT0 ACL が同じ ACL を再利用しようとする場合は、アクセス ACL がデバイスで設定されている元の名前を使用し、NAT0 ACL は Security Manager によって名前変更されます。

ルール テーブルの管理

ここでは、多くのファイアウォール ルール、NAT、およびその他のポリシーに関連する、ルール テーブルの基本的な使用方法について説明します。

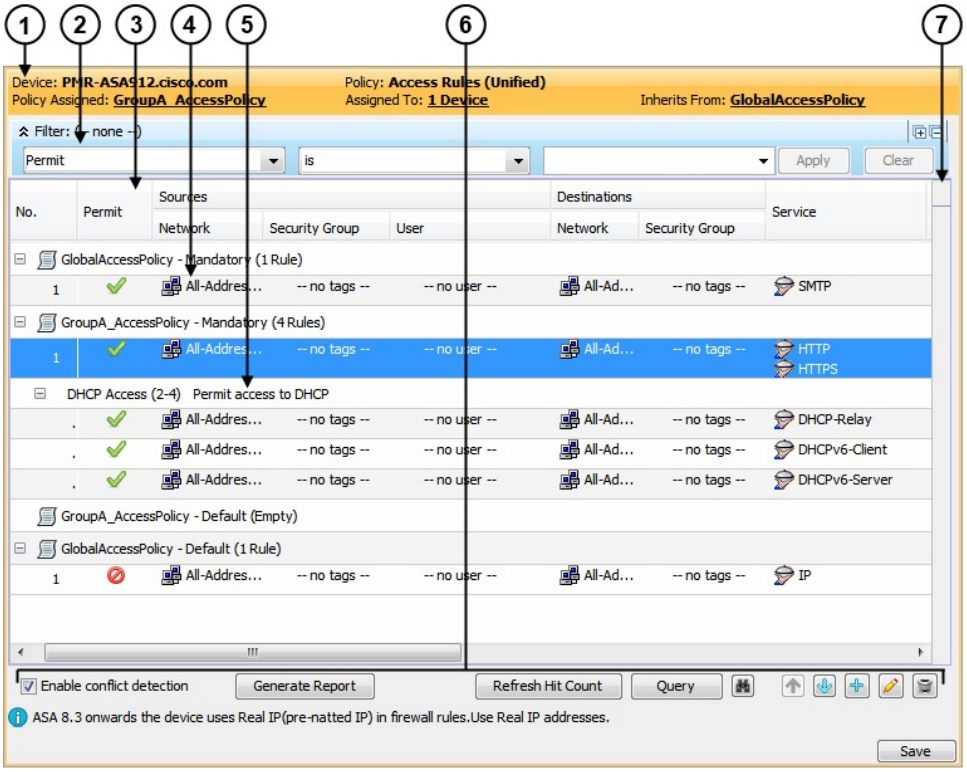
- ルール テーブルの使用 （10 ページ）
- ルールの追加および削除 （12 ページ）

ルール テーブルの使用

Security Manager のルール テーブルには、ポリシーを構成するルール セット（アクセス ルールなど）が表示されます。これらのタイプのテーブルは、特定のポリシー グループだけで使用されますが、多くのファイアウォール サービス ルール ポリシーで使用されます。ポリシー内のルールの順序が重要な場合は、ルール テーブルが使用されます。

下の図で、ルールテーブルに含まれる機能について説明します。

図 *1* : ルール テーブルの例



次に、ルール テーブルの機能について、番号付きのコールアウトで説明します。

- **デバイスおよびポリシーの識別バナー（1）**：このバナーに、ポリシーの共有および継承の情報が示され、いくつかのアクションを実行できることが示されます。詳細については、ポリシー バナーの使用を参照してください。
- **テーブルフィルタ（2）**：大きなテーブルの中でルールを簡単に見つけられるように、ルールをフィルタリングできます。詳細については、テーブルのフィルタリングを参照してください。
- **テーブルのカラム見出し（3）**：カラムごとのソート、カラムの移動、カラムの表示/非表示の切り替えを実行できます。詳細については、テーブル カラムおよびカラム見出しの機能を参照してください。
- **ルール、作業領域（4）**：テーブルの本文に、ポリシーに含まれているルールが表示されます。
- **ユーザー定義のセクション（5）**：便宜上、ルールをセクション単位にグループ化できます。詳細については、セクションを使用したルール テーブルの編成 （29 ページ）を参照してください。
- **テーブルボタン（6）**：次の操作を実行する場合は、テーブルの下にあるボタンを使用します。

- 自動競合検出を有効にします（アクセスルールのみ）。詳細については、自動競合検出の使用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、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。

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。

- テーブルに表示されるヒットカウント情報の更新。詳細については、ヒットカウントの詳細の表示および[Hit Count Selection Summary] ダイアログボックスを参照してください。
- ポリシークエリの実行。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 （39 ページ）を参照してください。
- ルール内の項目の検索と置換（双眼鏡アイコンが付いたボタン）：詳細については、ルール テーブルの項目の検索と置換 （23 ページ）を参照してください。
- ルールの移動と並べ替え（上矢印および下矢印）：詳細については、ルールの移動とルール順序の重要性 （27 ページ）を参照してください。
- テーブルにルールを追加（+アイコン）：詳細については、ルールの追加および削除 （12 ページ）を参照してください。
- 選択したルールの編集（鉛筆アイコン）：詳細については、 ルールの編集 （13 ページ）を参照してください。
- 選択したルールの削除（ゴミ箱アイコン）：詳細については、 ルールの追加および削除 （12 ページ）を参照してください。
- **競合ナビゲーションバー（7）**：競合ナビゲーションバーを使用して、ルールテーブル内の競合するルールに移動します。詳細については、自動競合検出の使用を参照してください。

ルールの追加および削除

ルール テーブルを使用するポリシーを操作するとき、ファイアウォール ルール ポリシーの多くと同様に、いくつかの方法を使用してポリシーにルールを追加できます。

- [行の追加（Add Row）] ボタン（+ アイコン）：テーブルの下の [行の追加（Add Row）] ボタンをクリックすることが、新しいルールを追加するための標準的な方法です。このボタンをクリックすると、そのポリシータイプに固有のルールを追加するためのダイアログボックスが開きます。行またはセクション見出しを選択すると、選択した行の後ろに新しいルールが追加されます。選択しない場合、新しいルールは適切なスコープ（通常はローカル スコープ）の末尾に追加されます。

- 行を右クリックして[行の追加（Add Row）]を選択：行を選択して[行の追加（Add Row）]ボタンをクリックするのと同じです。
- コピーアンドペースト：既存のルールと類似する新しいルールを作成するには、そのルールを選択し、右クリックして[コピー（Copy）]を選択します。次に、ルールを挿入する位置の前の行を選択し、右クリックして[貼り付け（Paste）]を選択します。これにより複製されたルールが作成されるので、それを選択して編集できます（ルールの編集　（13 ページ）を参照）。
- カットアンドペースト：カットアンドペーストはコピーアンドペーストと似ていますが、[カット（Cut）]コマンドを選択すると既存のルールは削除されます。カット アンド ペーストの代わりに、ルールを移動することを考慮してください（ルールの移動とルール順序の重要性　（27 ページ）を参照）。

ルールが不要になったときは、そのルールを選択して[行の削除（Delete Row）]ボタン（ゴミ箱アイコン）をクリックすると、そのルールを削除できます。

ヒント　ルールを削除する代わりに、まずルールをディセーブルにすることを考慮してください。ルールをディセーブルにすると、（設定を再展開したときに）そのルールはデバイスから削除されますが、Security Manager から削除されることはありません。あとで結局そのルールが必要であるとわかった場合は、ルールをイネーブルにして、設定を再展開するだけで済みます。ルールを削除した場合は、作成し直す必要があります（元に戻す機能はありません）。このため、ルールを削除するポリシーを進めるのは、ルールを一定時間ディセーブルにしてからにしてください。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　（28 ページ）を参照してください。

関連項目

- ルール テーブルの使用　（10 ページ）
- セクションを使用したルール テーブルの編成　（29 ページ）

ルールの編集

ルールテーブルを使用するルールポリシー内の既存のルールを編集するには、ルールを選択して[行の編集（Edit Row）]ボタンをクリックするか、右クリックして[行の編集（Edit Row）]を選択します。これにより、選択したルールのすべての側面を編集できます。

ヒント　ローカル デバイス ルール ポリシーからの継承ルールについては、いずれの側面も編集できません。継承ルールはポリシー ビューで編集します。

ほとんどのルール テーブルでは、ルール全部を編集せずに、右クリック メニューに表示されるコマンドを使用して特定の属性やテーブル セルを編集することもできます。

セルを編集できるかどうかは、その内容を編集することが適切かどうかによって制限されます。たとえば、インスペクション ルールには、ルールの設定に基づいて多くの制限があります。

- [All Interfaces] にルールを適用した場合、送信元アドレス、宛先アドレス、インターフェイス、またはルールの方向はいずれも編集できません。
- （送信元と宛先の間のインスペクションを制限するためのオプションを選択せずに）トラフィック一致基準に [Default Inspection Traffic] を選択した場合、または [Custom Destination Ports] を選択した場合、送信元アドレスや宛先アドレスは編集できません。
- [Destination Address and Port (IOS)] を選択した場合、送信元アドレスは編集できません。

次のセルレベル コマンドが使用可能ですが、ルール テーブルを使用するすべてのポリシーで、複数の行の編集機能がサポートされているわけではありません。

- [<属性タイプ>の追加（Add <Attribute Type>）]：複数の行を選択して、[送信元（Source）]、[ユーザー（User）]、[宛先（Destination）]、[サービス（Services）]、または [インターフェース（Interface）] セルを右クリックすると、[追加（Add）] コマンドを選択して、選択したセル内の既存のデータにエントリを追加できます。[追加（Add）] コマンドの完全な名前には、属性の名前が含まれます（[送信元の追加（Add Source）] など）。
- [<属性タイプ>の編集（Edit <Attribute Type>）]：ほとんどの属性で、内容を編集できます。編集すると、セルの内容が置き換わります。単一のセルを編集することも、複数の行を選択して、すべての行で同じタイプのセルの内容を一度に編集することもできます。[編集（Edit）] コマンドの完全な名前には、属性の名前が含まれます（[インターフェースの編集（Edit Interfaces）] など）。
- [<エントリ>の編集（Edit <Entry>）]：[送信元（Source）]、[ユーザー（User）]、[宛先（Destination）]、[サービス（Services）]、または [インターフェース（Interface）] を編集するときに、セル内のエントリを選択し、そのエントリだけを編集できる場合もあります。たとえば、[Sources] セルに 3 つのネットワーク/ホスト オブジェクトと 1 つの IP アドレスが含まれる場合、そのいずれかを選択してエントリを編集できます。[Edit] コマンドには、エントリの名前が含まれます（[Edit HostObject] など）。
- [<エントリ>の削除（Remove <Entry>）]：[送信元（Source）]、[ユーザー（User）]、[宛先（Destination）]、[サービス（Services）]、または [インターフェース（Interface）] を編集するときに、セル内のエントリを選択し、そのエントリを削除できる場合もあります。セル内の最後のエントリは削除できません。削除するとルールが無効になります。[Remove] コマンドには、エントリの名前が含まれます（[Remove IP] など）。
- [セルコンテンツからオブジェクトを作成（**Create <Object Type> Object from Cell Contents**）]：[送信元（Source）]、[ユーザー（User）]、[宛先（Destination）]、および [サービス（Services）] セルで、[作成（Create）] コマンドを選択して適切なタイプのポリシーオブジェクトを作成できます。また、セル内のエントリを選択して、選択した項目だけからポリシー オブジェクトを作成することもできます。[Create] コマンドには、作成できるポリシー オブジェクト タイプ、およびオブジェクトの送信元である項目の名前（セル内のすべての要素のセル コンテンツ、または選択したセルのエントリの名前）が含まれ

ます。ネットワーク/ホストオブジェクトを作成すると、必ずネットワーク/ホストグループ オブジェクトを作成することになります。

- [<属性タイプ>コンテンツの表示、<エントリ>コンテンツの表示（Show <Attribute Type> Contents; Show <Entry> Contents）]：[表示（Show）] コマンドを使用すると、セル内に定義されている実際のデータを参照できます。結果は、現在のビューによって異なります。
  - デバイスビュー、マップビュー、またはインポートルール：特定のデバイスに対してルールが適用される実際の IP アドレス、完全修飾ドメイン名（FQDN）、サービス、またはインターフェイスが表示されます。たとえば、ルールでネットワーク/ホストオブジェクトが使用されている場合は、それらのオブジェクトによって定義されている特定の IP アドレスまたは FQDN が表示されます。ルールでインターフェイス オブジェクトが使用されている場合は、オブジェクトによって識別される、デバイスに定義されている特定のインターフェイスが表示されます（ある場合）。

ネットワーク/ホスト オブジェクトの IP アドレスは、IP アドレスに基づいて昇順にソートされ、その後サブネット マスクに基づいて降順にソートされます。

サービス オブジェクトは、プロトコル、送信元ポート、および宛先ポートに基づいてソートされます。

インターフェイス オブジェクトは、アルファベット順に表示されます。インターフェイスがインターフェイス オブジェクト内のパターンと一致するために選択されている場合は、そのパターンが最初に表示され、そのあとに一致するインターフェイスがカッコで囲まれて表示されます。たとえば、「* (Ethernet1)」は、デバイス上の Ethernet1 インターフェイスが * パターンと一致（すべてのインターフェイスと一致）しているために選択されています。

- ポリシー ビュー：ポリシー オブジェクトに定義されているパターンとポリシーに定義されているエントリが表示されます。エントリはアルファベット順にソートされ、数字や特殊文字を先頭に含むエントリが先頭に表示されます。

関連項目

- ルール テーブルの使用　（10 ページ）
- ルールの追加および削除　（12 ページ）
- ルールの移動とルール順序の重要性　（27 ページ）
- ルールのイネーブル化とディセーブル化　（28 ページ）
- セクションを使用したルール テーブルの編成　（29 ページ）

ルール テーブルの [Address] セルの追加または編集

[Add Sources or Destinations]/[Edit Sources or Destinations] ダイアログボックス、または NAT テーブルの [Address] ダイアログボックスを使用して、送信元または宛先を含むルール テーブル内の送信元エントリまたは宛先エントリを編集します。ファイアウォール ルールのセルの編集に関する詳細については、ルールの編集　（13 ページ）を参照してください。

次のアドレス タイプを自由に組み合わせて入力し、トラフィックの送信元または宛先を定義できます。ポリシーのタイプによって、IPv4 または IPv6 のいずれのアドレスが必要であるかが決まります。アドレス タイプを混在させることはできません。項目をカンマで区切って複数の値を入力できます。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。

- ネットワーク/ホスト オブジェクト。オブジェクトの名前を入力するか、または [選択（Select）] をクリックしてリストから名前を選択します。選択リストから新しいオブジェクトを作成することもできます。

（注） Fully-Qualified Domain Name（FQDN; 完全修飾ドメイン名）を指定するには、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 オブジェクトを使用する必要があります。FQDN を直接入力することはできません。すべてのポリシー タイプで FQDN が許可されるわけではありません。ポリシーで許可されていない場合は、FQDN オブジェクトを含むオブジェクトを指定できません。

- ホスト IP アドレス（10.10.10.100（IPv4）または 2001:DB8::200C:417A（IPv6）など）。
- IPv4 ネットワーク アドレスとサブネット マスク。形式は 10.10.10.0/24 または 10.10.10.0/255.255.255.0。
- IPv6 ネットワーク アドレスとプレフィックス長。形式は、2001:DB8::/32。
- IP アドレスの範囲（10.10.10.100-10.10.10.200（IPv4）または 2001:DB8::1-2001:DB8::100（IPv6）など）。
- （IPv4 のみ）10.10.0.10/255.255.0.255 形式の IP アドレスのパターン。この場合のマスクは不連続なビット マスクです（連続および不連続ネットワーク マスク（IPv4 アドレスに対応）を参照）。
- インターフェイス ロール オブジェクト。オブジェクトの名前を入力するか、または [選択（Select）] をクリックしてリストから名前を選択します（オブジェクト タイプとして [インターフェイス ロール（Interface Role）] を選択する必要があります）。インターフェイス ロールを使用する場合は、選択したインターフェイスの IPv4 または IPv6 のアドレスを指定した場合と同様にルールが動作します。デバイスに割り当てられる IP アドレスを把握できないため、DHCP を経由してアドレスを取得するインターフェイスの場合に有効です。詳細については、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。

インターフェイス ロールを送信元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、ホストまたはネットワークとインターフェイス ロールが区別されます。

ナビゲーション パス

送信元、宛先、またはその他のアドレス セルを含むルール ポリシー内で、次のいずれかを実行します。

- ルールテーブル内のアドレスセルを右クリックし、[ソースの編集（Edit Sources）] または [宛先の編集（Edit Destinations）] あるいは類似のコマンドを選択します。選択したセルの内容が入力したデータに置き換えられます。
- アドレスセル内のエントリを選択し、[<エントリ>の編集（Edit <Entry>）] を選択します。選択したエントリが入力したデータに置き換えられます。
- 複数のルールを選択し、[送信元（Sources）] または [宛先（Destination）] セルを右クリックして [送信元の追加（Add Sources）] または [宛先の追加（Add Destinations）] を選択します。セルにすでに入力されているデータに、入力したデータが付加されます。

ルールテーブルの [ユーザー（User）] セルの追加または編集

ヒント ユーザーセルは、ASA 8.4(2 以降) にのみ適用されます。他のデバイスタイプまたは OS バージョンについては、セルでの設定内容はすべて無視されます。

[ユーザーの追加（Add Users）] または [ユーザーの編集（Edit Users）] ダイアログボックスを使用して、ユーザー アイデンティティ グループを含むルールテーブルのユーザーエントリを編集します。ファイアウォール ルールのセルの編集に関する詳細については、ルールの編集（13 ページ）を参照してください。

次の任意の組み合わせを入力して、Active Directory（AD）ユーザーまたはユーザーグループ名に基づいてトラフィックを識別できます。アイデンティティ ユーザー グループを設定する場合、それらは送信元トラフィックにのみ適用されます。ルールに一致するトラフィックの場合、送信元アドレスとアイデンティティ ユーザ グループの両方が一致する必要があります。つまり、ルールは、宛先に向けられた際に送信元フィールドに定義された特定のネットワークまたはホスト上のユーザから送信されたトラフィックに適用されます。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 ルールの設定を参照してください。

送信元アドレスに関係なくルールをユーザーに適用するには、送信元セルに「any」を指定します。

項目をカンマで区切って複数の値を入力できます。サポートされるフォーマットは次のとおりです。

- アイデンティティ ユーザー グループ オブジェクト
- 個別のユーザ：NETBIOS_DOMAIN\user
- ユーザ グループ（\ を二重にします）：NETBIOS_DOMAIN\\user_group

[選択（Select）] をクリックしてリストからオブジェクト、ユーザー、またはユーザーグループを選択するか、新しいオブジェクトを作成します。詳細については、ポリシーでのアイデンティティ ユーザの選択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。

ナビゲーション パス

[User] セルを含むルール ポリシー内で、次のいずれかを実行します。

- ルールテーブル内の [ユーザー（User）] セルを右クリックし、[ユーザーの編集（Edit Users）] を選択します。選択したセルの内容が入力したデータに置き換えられます。
- [ユーザー（User）] セル内のエントリを選択し、[<Entry> の編集（Edit <Entry>）] を選択します。選択したエントリが入力したデータに置き換えられます。
- 複数のルールを選択し、[ユーザー（User）] セルを右クリックして [ユーザーの追加（Add User）] を選択します。セルにすでに入力されているデータに、入力したデータが付加されます。

ルール テーブルの [Services] セルの追加または編集

[Edit Services] ダイアログボックスを使用して、対象となるトラフィックのタイプを定義するサービスを編集します。項目をカンマで区切って複数の値を入力できます。

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）を入力できます。サービスを入力する場合は、有効な値の入力を求められます。リストから値を選択して、Enter または Tab を押します。また、[選択（Select）] をクリックして、リストからサービスを選択するか、新しいサービスを作成することもできます。

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。

ファイアウォール ルールのセルの編集に関する詳細については、ルールの編集 （13 ページ）を参照してください。

ナビゲーション パス

サービスを含むルール ポリシー内で、次のいずれかを実行します。

- ルールテーブル内の [サービス（Services）] セルを右クリックし、[サービスの編集（Edit Services）] を選択します。選択したセルの内容が入力したデータに置き換えられます。
- [サービス（Services）] セル内のエントリを選択し、[<Entry> の編集（Edit <Entry>）] を選択します。選択したエントリが入力したデータに置き換えられます。
- 複数のルールを選択し、[サービス（Services）] セルを右クリックして [サービスの追加（Add Services）] を選択します。セルにすでに入力されているデータに、入力したデータが付加されます。

ヒント インスペクション ルールでは、[Traffic Match] カラムにサービスが表示されます。ただし、サービスが表示されるのは、トラフィックが送信元、宛先、およびポートと一致するルールの場合だけです。

ルール テーブルの [Interfaces] セルまたは [Zones] セルの追加または編集

[Add or Edit Interfaces] または [Add or Edit Zones] ダイアログボックスを使用して、ルールが定義されているインターフェイスまたはゾーンを編集します。ファイアウォールルールのセルの編集に関する詳細については、ルールの編集 （13 ページ）を参照してください。

- インターフェイスを編集する際は、特定のインターフェイス名またはインターフェイス ロールを自由に組み合わせて入力できます。項目をカンマで区切って複数の値を入力できます。名前を入力します。または、[選択（Select）] をクリックしてリストからインターフェイスおよびロールを選択するか、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。

ポリシーをデバイスに展開すると、インターフェイス ロールが実際のインターフェイス名で置き換えられます。これは、そのデバイスで実際に設定されているインターフェイスだけです。ルールによって実際に選択されるインターフェイスを表示するには、[インターフェイス（Interfaces）] セルを右クリックして [インターフェイスの表示（Show Interfaces）] を選択します。

- ゾーンの編集時には、インターフェイス ロールを 1 つだけ選択できます。個々のインターフェイスは選択できません。ゾーン ベースのファイアウォール ルールにゾーンを作成するには、インターフェイス ロールを使用します。ゾーンに属するインターフェイスを表示するには、[ゾーン（Zones）] セルを右クリックして [ゾーンコンテンツの表示（Show Zone Contents）] を選択します。

インターフェイス ロールおよびインターフェイスの選択に関する詳細については、次の項を参照してください。

- インターフェイス ロール 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

ナビゲーション パス

インターフェイスまたはゾーンを含むルール ポリシー内で、次のいずれかを実行します。

- ルールテーブル内の [インターフェイス（Interfaces）] または [ゾーン（Zones）] セルを右クリックし、[インターフェイスの編集（Edit Interfaces）]、[ゾーンの編集（Edit Zones）]、または類似のコマンドを選択します。選択したセルの内容が入力したデータに置き換えられます。
- [インターフェイス（Interfaces）] セル内のエントリを選択し、[<エントリ>の編集（Edit <Entry>）] を選択します。選択したエントリが入力したデータに置き換えられます。ゾーン内のエントリを編集することはできません。
- 複数のルールを選択し、[インターフェイス（Interfaces）] セルを右クリックして [インターフェイスの追加（Add Interfaces）] を選択します。セルにすでに入力されているデータに、入力したデータが付加されます。エントリをゾーンに追加することはできません。

ルール テーブルの [Category] セルの編集

[Edit Category] ダイアログボックスを使用して、ルールに割り当てられているカテゴリを変更します。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。ファイアウォール ルールのセルの編集に関する詳細については、ルールの編集 （13 ページ）を参照してください。

ナビゲーション パス

カテゴリを含むルールポリシー内の [カテゴリ（Category）] セルを右クリックし、[カテゴリの編集（Edit Category）] を選択します。

ルール テーブルの [Description] セルの編集

[Edit Description] ダイアログボックスを使用して、ルールの説明を編集します。説明を使用すると、ルールの目的を明確にできます。最大 1024 文字です。ルールのセルの編集に関する詳細については、ルールの編集 （13 ページ）を参照してください。

ナビゲーション パス

説明を含むルールポリシー内の [説明（Description）] セルを右クリックし、[説明の編集（Edit Description）] を選択します。

ルール テーブルのセルの内容の表示

[Show Contents] ダイアログボックスを使用して、送信元、ユーザ、宛先、サービス、インターフェイス、またはゾーンのセルや、それらの要素を定義するアドレス、アイデンティティ ユーザ グループ、インターフェイス、サービス、またはポリシー オブジェクトを含むルール テーブル内のその他のセルで定義されている実際の変換済みデータを表示します。ダイアログボックスのタイトルは、調べるセルまたはエントリを示しています。この情報を使用して、デバイスに展開されたルールが実際に適用されるアドレス、サービス、またはインターフェイスを判別します。セルの内容の編集または表示に関する詳細については、ルールの編集 （13 ページ）を参照してください。

ダイアログボックスに表示される内容は、現在のビューによって異なります。

- デバイス ビュー、マップ ビュー：特定のデバイスに対してルールが適用される実際の IP アドレス、ユーザ、サービス、またはインターフェイスが表示されます。たとえば、ルールでネットワーク/ホスト オブジェクトが使用されている場合は、それらのオブジェクトによって定義されている特定の IP アドレスまたは Fully-Qualified Domain Name（FQDN; 完全修飾ドメイン名）が表示されます。ルールでインターフェイス オブジェクトが使用されている場合は、オブジェクトによって識別される、デバイスに定義されている特定のインターフェイスが表示されます（ある場合）。
  - ネットワーク/ホスト オブジェクトの IP アドレスは、IP アドレスに基づいて昇順にソートされ、その後サブネット マスクに基づいて降順にソートされます。
  - サービス オブジェクトは、プロトコル、送信元ポート、および宛先ポートに基づいてソートされます。

- インターフェイス オブジェクトは、アルファベット順に表示されます。インターフェイスがインターフェイス オブジェクト内のパターンと一致するために選択されている場合は、そのパターンが最初に表示され、そのあとに一致するインターフェイスがカッコで囲まれて表示されます。たとえば、「*(Ethernet1)」は、デバイス上のEthernet1インターフェイスが*パターンと一致（すべてのインターフェイスと一致）しているために選択されています。

- ポリシー ビュー：ポリシー オブジェクトに定義されているパターンとポリシーに定義されているエントリが表示されます。エントリはアルファベット順にソートされ、数字や特殊文字を先頭に含むエントリが先頭に表示されます。

コンテンツのフィルタリング

[コンテンツの表示（Show Contents）]ダイアログボックスの結果の上にリストフィルタフィールドが表示されます。リストフィルタフィールドを使用すると、指定したテキスト文字列を含むエントリをすばやく見つけることができます。

図 *2:* リストフィルタフィールド

1	フィルタパラメータボタン	2	クリアボタン

[コンテンツの表示（Show Contents）]リストで特定のテキスト文字列を検索するには、次のように操作します。

- リストフィルタフィールドをクリックしてテキストカーソルを置き、入力を開始します。

これらは「ライブフィルタ」フィールドです。つまり、各文字を入力すると、現在のテキスト文字列を含まないエントリがリストまたはテーブルから除外されます。

リストフィルタフィールドをクリアするには、次のように操作します。

- フィールドの右側にあるクリアボタンをクリックします。

このボタンは、フィールドへの入力を開始すると表示されます(文字を強調表示して、キーボードの Delete キーまたは Backspace キーを押すこともできます)。

リストフィルタフィールドをクリアすると、リスト内のすべてのエントリが再び表示されます。

大文字と小文字を区別するか区別しないかを選択し、ワイルドカードまたは正規表現を許可し、返される文字列のどこに文字が配置されている必要があるかを指定することにより、フィルタ結果を調整できます。

リストフィルタ条件を変更するには、次のように操作します。

1. リストフィルタフィールドの左側にあるフィルタ パラメーターボタン（虫眼鏡）をクリックして、パラメーターメニューを開きます。
2. オプションを選択します。

メニューは 3 つのセクションで構成されています。

- [大文字と小文字を区別する（Case sensitive）]および[大文字と小文字を区別しない（Case insensitive）]：いずれかを選択します。[大文字と小文字を区別する（Case sensitive）]を選択した場合、見つかったテキストは、入力した文字だけでなく、大文字と小文字も入力されたものと一致する必要があります。
- [ワイルドカードを使用する（Use wildcards）] および [正規表現を使用する（Use regular expression）]：いずれかを選択します。次のワイルドカードが認識されます。
- *****（アスタリスク）：文字列内のその位置にある 0 個以上の文字に一致します。
- **+**（プラス記号）：文字列内のその位置にある 1 個以上の文字に一致します。
- **?**（疑問符）：文字列内のその位置にある 1 文字に一致します。
- [最初から一致（Match from start）]、[完全一致（Match exactly）]、および [一部が一致（Match anywhere）]：1 つを選択します。[最初から一致（Match from start）]とは、入力した文字列がエントリの先頭で見つかる必要があることを意味します。ただし、より大きな文字セットの一部でも可能です。[完全一致（Match exactly）] では、入力した文字列がカラムエントリ全体と完全に一致する必要があります。 [一部が一致（Match anywhere）] とは、文字列がエントリ内のどこかで見つかることを意味し、より大きな文字セットの一部でも可能です。
- 別のパラメータを変更するには、手順 1 と 2 を繰り返します。

ナビゲーション パス

送信元、ユーザ、宛先、サービス、インターフェイス、またはゾーンや、ネットワーク、アイデンティティユーザグループ、インターフェイス、またはサービスを指定するその他のフィールドを含むルールポリシー内で、次のいずれかを実行します。また、ルールを操作する（ルールのインポートなど）ツールを使用する際にも、内容を表示できます。

- これらのセルの 1 つを右クリックし、[<Attribute Type>のコンテンツを表示（Show <Attribute Type> Contents）]（attribute type はセル名）を選択します。データには、セル内に定義されているすべてのエントリが含まれます。
- これらのセルの 1 つのエントリを右クリックし、[<Entry>のコンテンツを表示（Show <Entry> Contents）] を選択します。コマンド名には、選択したエントリの名前が含まれます。表示されるデータは、選択したエントリだけに対応するデータです。

ヒント　インスペクション ルールでは、[Traffic Match] カラムにサービスが表示されます。ただし、サービスが表示されるのは、トラフィックが送信元、宛先、およびポートと一致するルールの場合だけです。

ルール テーブルの項目の検索と置換

ルールテーブルを使用するポリシー内で、いくつかのセルの項目を検索し、選択的に置換できます。検索できるセルは、ポリシーによって異なります。パターンマッチングに基づいて項目を検索する場合、ワイルドカード文字を使用できます。たとえば、関連するいくつかのネットワークを、それらに定義されている新しいネットワーク/ホスト ポリシー オブジェクトで置き換えることができます。

検索と置換を使用するには、ルールテーブルを使用するポリシーの一番下にある [検索と置換（Find and Replace）]（双眼鏡アイコン）ボタンをクリックして、[Find and Replace] ダイアログボックス （24 ページ）を開きます。Firewall フォルダでは、これに AAA 規則、アクセス規則、IPv6 アクセス規則、インスペクション規則、ゾーン ベースのファイアウォール規則、および Web フィルタ規則（ASA/PIX/FWSM デバイスのみ）が含まれます。ASA/PIX/FWSM デバイスでは、NAT 変換ルール ポリシー（ただし、コンテキストと動作モードのすべての組み合わせに当てはまるとはかぎりません）と IOS、QoS、および接続ルールのプラットフォーム サービス ポリシーも含まれます。

項目を検索するときは、項目のタイプおよび検索するカラムを選択し、検索する文字列を入力します。また任意で、置換に使用する文字列を入力します。次の項目タイプを検索および置換できます。

- [ネットワーク（Network）]：ネットワーク/ホストオブジェクト名またはホストやネットワークの IP アドレス。
- [User]：Active Directory（AD）ユーザ名（NetBIOS_DOMAIN\user）、ユーザ グループ名（NetBIOS_DOMAIN\\user_group）、またはアイデンティティ ユーザ グループ オブジェクト名。
- [Service]：サービス オブジェクト名またはプロトコルとポート。たとえば、TCP/80。検索は意味ではなく構文によるものです。つまり、TCP/80 を検索し、ルールで HTTP が使用されている場合、検索結果には TCP/80 は含まれません。
- [Interface Role]：インターフェイス名またはインターフェイス ロール オブジェクト名。

（注） アクセス ルールでは、グローバル インターフェイス名を使用してグローバル ルールを検索できます。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。

- [Text]：[Description] フィールドのテキスト文字列。

次に、検索と置換に関連する操作の例をいくつか示します。

- 10.100.0.0/16 の範囲内のすべてのネットワークに対して network10.100 という名前の新しいネットワーク/ホスト オブジェクトを作成すると、すべての従属ネットワーク指定を検索および置換できます。たとえば、^10.100* を検索すると、10.100.10.0/24 のようなアドレスすべてを検索できます。[全単語のみ検索（Find Whole Words Only）] および [ワイルドカードを許可（Allow Wildcard）] オプションを選択して、置換文字列として「network10.100」と入力します。[Find Whole Words Only] を選択したため、置換される文字列は、10.100 の部分だけでなく 10.100.10.0/24 文字列全体です。
- （ネットワーク/ホスト オブジェクトの代わりに）IP アドレスを使用するすべてのルールを検索する場合は、*.*.*.* を検索すると、すべてのホストまたはネットワーク IP アドレスが検索されます。次に、[Find and Replace] ダイアログボックスが開いている間に、選択的にセルを編集できます。
- 名前に「side」が含まれるすべてのインターフェイス ロール オブジェクト（inside や outside など）を、External という名前のインターフェイス ロール オブジェクトで置換する場合は、[全単語のみ検索（Find Whole Words Only）] オプションと [ワイルドカードを許可（Allow Wildcard）] オプションを選択して *side を検索し、[置換（Replace）] フィールドに External を入力します。

関連項目

- ルールの編集 （13 ページ）

[Find and Replace] ダイアログボックス

[Find and Replace] ダイアログボックスを使用して、ルール テーブルのセル内の項目を検索し、任意で置換します。検索できる項目のタイプは、表示されているポリシーによって異なります。

ナビゲーション パス

ルールテーブルを使用するポリシーの一番下にある [検索と置換（Find and Replace）]（双眼鏡アイコン）ボタンをクリックします。Firewall フォルダでは、これに AAA 規則、アクセス規則、IPv6 アクセス規則、インスペクション規則、ゾーン ベースのファイアウォール規則、お

よびWebフィルタ規則（ASA/PIX/FWSMデバイスのみ）が含まれます。ASA/PIX/FWSMデバイスでは、NAT変換ルール ポリシー（ただし、コンテキストと動作モードのすべての組み合わせに当てはまるとはかぎりません）とIOS、QoS、および接続ルールのプラットフォーム サービス ポリシーも含まれます。

関連項目

- ルール テーブルの項目の検索と置換 （23 ページ）
- ルールの編集 （13 ページ）

フィールド リファレンス

表 2 : [Find and Replace] ページ

要素	説明
タイプ	検索する項目のタイプ。タイプを選択し、検索するカラムを選択します。[All Columns] を選択すると、検索されたカラムは、[All Columns] 項目とともに一覧表示されます（検索では、テーブル内のすべてのカラムが考慮されるわけではありません）。 • [ネットワーク（Network）]：ネットワーク/ホストオブジェクト名またはホストやネットワークのIPアドレス。 • [User]：Active Directory（AD）ユーザ名（NetBIOS_DOMAIN\user）、ユーザ グループ名（NetBIOS_DOMAIN\\user_group）、またはアイデンティティ ユーザ グループ オブジェクト名。 • [Service]：サービス オブジェクト名またはプロトコルとポート。たとえば、TCP/80。検索は意味ではなく構文によるものです。つまり、TCP/80を検索し、ルールでHTTPが使用されている場合、検索結果にはTCP/80は含まれません。 • [Interface Role]：インターフェイス名またはインターフェイス ロール オブジェクト名。 （注） アクセス ルールでは、グローバル インターフェイス名を使用してグローバル ルールを検索できます。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。 • [Text]：[Description] フィールドのテキスト文字列。

要素	説明
検索（Find）	検索文字列。ポリシーオブジェクトを検索する場合は、[選択（Select）] をクリックして、リストからオブジェクトを選択します。
置換（Replace）	（任意）検索文字列を置換するために使用する文字列。置換される文字列は、検索オプションで制御します。検索文字列をポリシーオブジェクト名で置換する場合は、[選択（Select）] をクリックして、リストからオブジェクトを選択します。 検索文字列を複数の項目で置換できます。複数の項目はカンマで区切ります。たとえば、TCP サービスを検索し、それを TCP, UDP で置き換えます。 [置換（Replace）] フィールドに何も入力せずに [置換（Replace）] ボタンをクリックすると、項目を削除できます。 テーブルで編集が許可されていない場合は、このフィールドがグレー表示されます。
方向	現在選択されている行またはセルを基準にした検索の方向（[up] または [down]）。テーブルの終わりに達すると、引き続きテーブルの一番上から検索されます。
Match Case	テキスト検索の場合、[Find] フィールドで使用した大文字と小文字の違いを一致させるかどうか。
Find Whole Words Only	検索で単語全体（スペースまたは句読点で区切られた文字列）だけを検索して選択するかどうか。たとえば、SanJose を単語全体で検索すると、SanJose は検出されますが、SanJose1 は検出されません。 このオプションを [Allow Wildcard] オプションとともに使用すると、部分文字列を検索できます。ただし、検出された文字列を置換すると、部分文字列ではなく単語全体が置換されます。たとえば、^10.100* を検索すると、10.100.10.0/24 のようなすべてのアドレスが検出され、それらが network10.100 ポリシー オブジェクトで置換されます。[Whole Words] を選択することにより、検索対象の部分だけでなくアドレス全体がネットワーク/ホストオブジェクトで置換されます。 テキスト検索の場合、このオプションと [Allow Wildcards] オプションは相互に排他的です。

要素	説明
Allow Wildcards	検索文字列または置換文字列でワイルドカード文字を使用するかどうか。このオプションを選択しない場合、すべての文字が文字どおりに処理されます。 Java 正規表現を使用して、次の例外を含む表現を作成できます。 • ピリオド（.）：ピリオドはリテラル ピリオドであり、暗黙的にエスケープされます。 • 疑問符（?）：疑問符は単一文字を表します。 • アスタリスク（*）：アスタリスクは、1 つ以上の文字と一致します。0 文字とは一致しません。 • プラス記号（+）：プラス記号はアスタリスクと同じ意味で、1 つ以上の文字と一致します。
[Find Next] ボタン	検索文字列の次のオカレンスを検索する場合は、このボタンをクリックします。
[Replace] ボタン	見つかった文字列を置換文字列で置換する場合、このボタンをクリックします。
[Replace All] ボタン	検索文字列を自動的に検索し、テーブル全体にわたってそれを置換する場合は、このボタンをクリックします。

ルールの移動とルール順序の重要性

ルール テーブルを使用するルール ポリシーは、順序付けられたリストです。つまり、ルールの上から下への順序が重要であり、ポリシーに影響を与えます。

デバイスは、ルール ポリシーに照らしてパケットを分析するとき、上から下に順にルールを検索します。パケットに一致した最初のルールが、そのパケットに適用されるルールです。それ以降のルールはすべて無視されます。このため、特定の送信元または宛先の HTML トラフィックに関連する具体的なルールの前に、IP トラフィックに関連する一般的なルールを配置すると、具体的なルールの方が適用されないことがあります。

アクセス制御ルールの場合は、自動競合検出ツールを使用して、どのような場合に、ルール順序によってルールがトラフィックに適用されなくなるかを特定できます（詳細については、自動競合検出の使用を参照してください）。その他のルール ポリシーの場合は、テーブルをよく調べて、ルール順序に関連する問題を特定してください。

ルールの順序を並べ替える必要があると判断した場合は、移動する必要のあるルールを選択し、適宜、[上の行へ（Up Row）]（上矢印）または [下の行へ（Down Row）]（下矢印）ボタンをクリックします。これらのボタンがルール テーブルの下に表示されない場合、ルール順序は問題ではないため、その順序を並べ替えることはできません。

セクションを使用してルールを編成した場合は、セクション内でだけルールを移動できます。セクション外部のルールを移動する場合、そのセクションの上または下に移動できます。セクションでの作業の詳細については、セクションを使用したルール テーブルの編成 （29 ページ）を参照してください。

ヒント　ポリシー内でインターフェイスに固有のルールとグローバル ルールを組み合わせる場合は、移動するアクセス ルールに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 ルールについてを参照してください。

関連項目

- ルール テーブルの使用 （10 ページ）
- ルールの追加および削除 （12 ページ）
- ルールの編集 （13 ページ）
- ルールのイネーブル化とディセーブル化 （28 ページ）
- セクションを使用したルール テーブルの編成 （29 ページ）

ルールのイネーブル化とディセーブル化

ルール テーブルを使用するポリシー（ほとんどのファイアウォール サービス ルール ポリシーなど）内で、個々のルールをイネーブル化およびディセーブル化できます。変更は、設定をデバイスに再展開すると有効になります。

ルールがディセーブルになっている場合、テーブルでそのルールにハッシュ マークが重なって表示されます。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。

ディセーブルなルールは便宜的に Security Manager のルール ポリシー内に保持されます。ルールが必要になった場合は、ルールを再作成しなくとも簡単にイネーブルにできます。このため、不要になったと思われるルールは、すぐに削除してしまわずに、ディセーブルにすることを推奨します。

ルールがイネーブルかディセーブルかを変更するには、ルールを選択して右クリックし、[有効化（Enable）] または [無効化（Disable）] を必要に応じて選択します。

関連項目

- ルール テーブルの使用 （10 ページ）
- ルールの追加および削除 （12 ページ）
- ルールの編集 （13 ページ）
- ルールの移動とルール順序の重要性 （27 ページ）
- セクションを使用したルール テーブルの編成 （29 ページ）

セクションを使用したルール テーブルの編成

ルールテーブルを使用するポリシーは、セクション単位に編成できます。次の2つのタイプのセクションがあります。

- スコープ：ポリシーと継承ポリシーの継承関係を定義します。このセクションは、ポリシーを継承すると自動的に作成されます。詳細については、ルールの継承についてを参照してください。
- ユーザ定義セクション：ポリシーの評価および編集が簡単になるようにルールを編成する際に役立つ便利なグループです。このタイプのセクションは、多数のルールが含まれるポリシーに対して最も効果を発揮します。

セクション内のすべてのルールは順序付けられている必要があります。ルールをランダムにグループ化することはできません。連続しないルールどうしを関連付けて指定するには、それらのルールに同じカテゴリを割り当てることができます。

ユーザ定義セクションは、インデントされたセクション見出しによって、テーブル内の他のルールから目立つように表示されます。見出しには、左から順に、セクションを開いたり閉じたりするための +/- アイコン、セクションに割り当てたカテゴリ（ある場合）を識別する色の帯、セクション名、セクションに含まれる最初と最後のルール番号（4-8 など）、および入力したセクションの説明（ある場合）が表示されます。

（注） セクション内のルールの番号付けを表示するには、ルール番号の列のサイズを変更する必要がある可能性があります。

ユーザ定義セクションを作成するかどうかは、ユーザの自由です。これらのタイプのセクションを作成することが有益だと判断した場合は、次の情報に示すセクションの作成方法と使用方法を参照してください。

- 新しいセクションを作成するには、セクションを挿入する行を右クリックし、[新しいセクションに含める（Include in New Section）] を選択します（Shift を押しながらクリックして、ルールのブロックを選択することもできます）。セクションの名前、説明、およびカテゴリを入力するように要求されます（必須の要素は名前だけです）。
- 既存のルールをセクションに移動するには、1つ以上の連続するルールを選択し、右クリックして [<セクション名> セクションに含める（Include in Section <name of section>）] を選択します。このコマンドは、選択した行が既存のセクションの隣にある場合にだけ表示されます。セクションに追加する行が現在そのセクションの隣にない場合は、セクションの隣に来るまでルールを移動するか、ルールをカットしてセクションにペーストします。
- セクションの移動はできません。このため、セクションの外側のルールをセクション周りに移動する必要があります。セクション内にはないが、セクションの隣にあるルールを移動すると、ルールはそのセクションを飛び越えます。
- ルールをセクションの外部に移動したり、セクションを通過して移動したりすることはできません。セクションとは、ルールを移動できる範囲の境界を定義するものです。ルール

をセクションの外側に移動して Local スコープセクションに戻すには、1 つ以上の連続するルールを選択し、右クリックして [<name of section> セクションから削除する（Remove from Section <name of section>）] を選択します。このコマンドを使用するには、ルールがセクションの開始位置または終了位置にある必要があります。そうでない場合、ルールが開始位置または終了位置に来るまでルールを移動するか、ルールをカット アンド ペーストしてセクションの外側に移動できます。

- 新しいルールをセクションに追加するには、目的の位置のすぐ前にあるルールを選択し、[Add Row] ボタンをクリックします。ルールをセクションの開始位置に挿入するには、セクション見出しを選択します。

ルールを（セクションの外部だが）セクションの後ろに作成するには、ルールをセクション内の最後のルールとして作成してから、セクションから削除します。または、ルールをセクションのすぐ上に作成し、下矢印ボタンをクリックします。

- セクション見出しを右クリックして [セクションの編集（Edit Section）] を選択することにより、セクションの名前、説明、またはカテゴリを変更できます。
- セクションを削除すると、セクションに含まれているすべてのルールは保持されて、Local スコープ セクションに再び移されます。削除されるルールはありません。セクションを削除するには、セクション見出しを右クリックし、[セクションの削除（Delete Section）] を選択します。
- Combine Rules ツールを使用する場合、結果として結合されたルールではセクションが考慮されます。セクション内にあるルールは、そのセクション内の他のルールとだけ結合できます。

関連項目

- ルール テーブルの使用 （10 ページ）
- ルールの追加および削除 （12 ページ）
- ルールの編集 （13 ページ）
- ルールの移動とルール順序の重要性 （27 ページ）
- ルールのイネーブル化とディセーブル化 （28 ページ）

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

[Add and Edit Rule Section] ダイアログボックスを使用して、ルール テーブルでユーザ定義セクション見出しを追加または編集します。セクションを使用してルール テーブルを編成する方法の詳細については、セクションを使用したルール テーブルの編成 （29 ページ）を参照してください。

ナビゲーション パス

次のいずれかを実行します。

- ルールテーブル内の 1 つ以上のルールを選択し、右クリックして [新しいセクションに含める（Include in New Section）] を選択します。
- セクション見出しを右クリックし、[セクションの編集（Edit Section）] を選択します。

フィールド リファレンス

表 *3 : [Add Rule Section]/[Edit Rule Section]* ダイアログボックス

要素	説明
名前	セクションの名前。
説明	セクションの説明。最大 1024 文字です。
カテゴリ	セクション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。

ルールの結合

アクセス ルール ポリシーおよび AAA ルール ポリシーは時間とともに拡大し、多数のルールを含むことがあります。これらのポリシーの大きさによっては、ポリシーの管理が困難になることがあります。この問題を軽減するために、ルール結合ツールを使用できます。これにより、ポリシーがトラフィックを処理する方法を変更することなく、ポリシー内のルールの数を減らすことができます。

ヒント ルールを結合すると、特定のセキュリティ ポリシーを実装するために必要なアクセス ルールの数を大幅に圧縮できます。たとえば、あるポリシーでアクセス ルールが 3,300 個必要な場合、ホストとサービスを効率的にグループ化すると、必要なルールを 40 個に減らすことができます。ただし、Rule Combiner は IPv6 アクセス ルールで使用できません。また、ユーザまたはユーザ グループを指定するルールでも、直接とアイデンティティ ユーザ グループ オブジェクトのどちらでも使用できません。FQDN ネットワーク/ホスト オブジェクトを使用するルールで、このツールを使用できます。

（送信元としての）信頼できる各種ホストに対する特定範囲のサービスを（宛先としての）各種パブリック サーバに対して許可するような、複数のルールが存在するとします。この状況で 10 個のルールを適用する場合は、その 10 個のルールを 1 つのルールに結合できます。これにより、サービスの集まり（AllowedServices など）、ホスト（TrustedHosts など）、およびサーバ（PublicServers など）に対して新しいポリシー オブジェクトを作成できます。ルール結合中に新しいオブジェクトを作成するには、新しく結合したセルを右クリックし、[ネットワーク（またはサービス）オブジェクトをセルコンテンツから作成する（Create Network (or Service) Object from Cell Contents）] を選択します。

たとえば、インターフェイス FastEthernet0 に次の 2 つのルールがあるとします。

- Permit TCP for source 10.100.10.1 to destination 10.100.12.1
- Permit TCP for source 10.100.10.1 to destination 10.100.13.1

この 2 つを結合して、permit TCP for source 10.100.10.1 to destination 10.100.12.1, 10.100.13.1 という 1 つのルールにできます。

ルールを結合するには、多次元のソートが使用されます。たとえば、アクセス ルールの場合、次のようになります。

1. ルールは送信元によってソートされるため、送信元が同じルールはまとめて配置されます。
2. 送信元が同じルールは宛先によってソートされるため、送信元も宛先も同じルールはまとめて配置されます。
3. 送信元も宛先も同じルールは 1 つのルールに結合され、サービスが連結されます。
4. 隣接するルールは、送信元およびサービスが同じかどうかチェックされます。同じであった場合、1 つのルールに結合され、宛先が連結されます。
5. 隣接するルールは、宛先およびサービスが同じかどうかチェックされます。同じであった場合、1 つのルールに結合され、送信元が連結されます。

今度は、宛先と（送信元の代わりに）サービスに基づいてソートが繰り返されます。

ヒント セクションの異なるルールが結合されることはありません。ルールを整理するために作成したセクションによって、可能な結合の範囲が制限されます。また、インターフェイス固有のアクセス ルールとグローバル アクセス ルールが結合されることはありません。グローバル ルールの詳細については、グローバル アクセス ルールについてを参照してください。

関連項目

- ファイアウォール AAA ルールの管理
- ファイアウォール アクセス ルールの管理

ステップ 1 **Firewall** フォルダから、結合するルールのポリシーを選択します。次のタイプのポリシーに対してルールを結合できます。

- AAA ルール
- アクセス ルール

ステップ 2 ツールで可能な結合が特定のルール グループに制限されるようにする場合は、それらのルールを選択します。Shift および Ctrl を押しながらクリックすると、複数のルールを選択できます。セクション見出しを選択すると、セクション内のすべてのルールを選択できます。スコープ見出し（[Local] など）を選択する

と、スコープ内のすべてのルールを選択できます。ツールを制限しない場合は、テーブルから何も選択しないでください。次の点を考慮してください。

- デバイス ビューでは、ローカル ルールに対する結合だけを保存できます。ツールは共有ルールおよび継承ルールに対して実行できますが、結果を保存することはできません。ルールを選択しない場合、デフォルトですべてのローカル スコープ ルールが考慮されます。
- 共有ポリシー内のルールを結合するには、ポリシー ビューでツールを実行する必要があります。ルールを選択しない場合、デフォルトですべての必須ルールが考慮されます。

結果を保存できない場合にツールを実行しようとすると、警告されます。

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、[ルールの結合（Combine Rules）] を選択して [Combine Rules Selection Summary] ダイアログボックス （33 ページ）を開きます。組み合わせを制限する特定のルールを選択した場合は、選択したルールの 1 つで右クリックしてください。そうしないと、ルールの選択が解除されます。

ステップ 4 ルールで結合を考慮するカラムを選択します。カラムを選択しない場合、結合されたルールの設定が、結合対象のカラム内の設定と同じである必要があります。

また、選択したルールの結合を考慮するように選択したり、ポリシー内のすべてのルールの結合を考慮するように選択することもできます。

ヒント カラム タイプが表示されていない場合、結合されたルールの内容が、[Description] セルを除くセルの内容と同じである必要があります。セルの内容が異なるルールどうしは結合されません。

ステップ 5 [OK] をクリックすると、結合が生成され、[ルールの結合結果（Rule Combiner Results）] ダイアログボックスに結果が表示されます。

結果を分析し、結合を保存するかどうかを評価します。全部を保存するか、何も保存しないかのどちらかです。保存する結合を選択することはできません。

結果の評価の詳細については、 Rule Combiner 結果の解釈 （35 ページ）を参照してください。例については、 Rule Combiner 結果の例 （37 ページ）を参照してください。

ステップ 6 [OK] をクリックすると、ルールテーブル内の元のルールが、結合されたルールに置き換わります。

[Combine Rules Selection Summary] ダイアログボックス

[Combine Rules Selection Summary] ダイアログボックスを使用して、ファイアウォール ルール ポリシー内のルールを結合するために使用するパラメータを定義します。[OK] をクリックすると、結合の結果が [Rule Combiner結果（Rule Combiner Results）] ダイアログボックスに表示されます。このダイアログボックスで、 Rule Combiner 結果の解釈 （35 ページ）の説明に従い、結果の保存または破棄を選択できます。

ナビゲーション パス

[AAA Rules] ページと [Access Rules] ページからルールを結合できます。テーブルの一番下にある [ツール（Tools）] をクリックし、[ルールの結合（Combine Rules）] を選択します。

フィールド リファレンス

表 *4 : [Combine Rules Selection Summary]* ダイアログボックス

要素	説明
Policy Selected	選択したポリシーおよびスコープが表示されます。[Local] は、ローカル デバイス ルールを表します。それ以外の場合、フィールドには共有ポリシーの名前と、そのポリシー内で選択されているスコープ（ある場合）が示されます。
Rules to be combined	ツールで結合を考慮するルール： • [All Rules]：選択したポリシー内のすべてのルールの結合が考慮されます。 • [Selected Rules]：ツールの起動前にポリシー内で選択したルールだけの結合が考慮されます。 ツールの実行前のルールの選択に関する詳細については、ルールの結合（31 ページ）を参照してください。

Choose which columns to combine	ルールテーブル内の結合可能なカラム。2つのルールを結合するには、選択していないカラムの内容がいずれも同一である必要があります（結合可能カラムとして一覧表示されていないカラムも含む。ただし、[Description] カラムを除く）。結合できるカラムは、次のとおりです。
	• ソース
	• ユーザー（User）
	• [接続先（Destination）]
	• サービス
	• インターフェイス
	• [セキュリティ送信先（Security Sources）]
	• [セキュリティ宛先（Security Destinations）]
	• AAA ルールの場合、他に次のカラムも結合できます。
	  • 操作
	  • Auth Proxy

Rule Combiner 結果の解釈

[Rule Combiner Results] ダイアログボックスを使用して、ルール結合の結果を評価できます（ルールの結合 （31 ページ）を参照）。このダイアログボックスには結果が要約され、[OK] をクリックすると作成される新しいルールが表示されます。

変更されるルールのセルの枠は赤色になります。上半分のテーブルで結合済みのルールを選択すると、そのルールを作成するために結合されたルールが下半分のテーブルに表示されます。

このウィンドウで、結果の要素を改良できます。

- 複数の要素を持つ [送信元（Source）]、[宛先（Destination）]、[サービス（Service）] セルを右クリックし、[ネットワーク（またはサービス）オブジェクトをセルコンテンツから作成する（Create Network (or Service) Object from Cell Contents）] を選択すると、結合されたセルの内容を含む新しいポリシーオブジェクトを作成できます。セルの内容が新しいオブジェクトに置き換わります。

また、展開された設定内にネットワーク オブジェクト グループを自動的に作成して、ルール テーブル セル内のカンマ区切りの値を置き換えることもできます。ネットワーク オブジェクトは展開中に作成されます。これがルール ポリシーの内容に影響することはありません。このオプションをイネーブルにするには、[ツール（Tools）] > [Security Manager の管理（Security Manager Administration）] > [展開（Deployment）] を選択して[Deployment] ページを開き、[ルール内の複数の送信元、宛先、またはサービスのオブジェクトグループを作成（Create Object Groups for Multiple Sources, Destinations, or Services in a Rule）] を選択します。

- [説明（Description）] を右クリックし、[説明の編集（Edit Description）] を選択して説明を変更します。結合済みのルールの説明は、改行で区切られた古いルールの各説明を連結したものです。

例については、Rule Combiner 結果の例 （37 ページ）を参照してください。

ヒント

- 結合された結果は、[OK] をクリックするまでポリシーに適用されません。結合の結果に満足しない場合は、[キャンセル（Cancel）] をクリックして、より小さなルールグループを選択して Combine Rules ツールのスコープを制限することを考慮します。

[OK] をクリックしたあとで、その変更の受け入れを取り消すには、次の 2 つのオプションがあります。1 つめは、ポリシーページで [保存（Save）] をクリックしないようにし、別のポリシーを選択して、ポリシーの変更を保存するように要求されたら [いいえ（No）] をクリックします。すでに [保存（Save）] をクリックした場合でも、（たとえば、[ファイル（File）] > [廃棄（Discard）] を選択して）アクティビティまたは設定セッションを廃棄することにより、変更を元に戻すことができます。ただし、これを行うと、他のポリシーに対して行った他の変更内容もすべて廃棄されます。変更を送信したあと、またはアクティビティが承認されたあとは、変更を元に戻すことはできません。

- 保存が許可されていないポリシーに対してルールを結合する場合でも、Combine Rules ツールは実行できます。たとえば、デバイス ビューでは共有ポリシーまたは継承ポリシーの結

合済みルールを保存できません。結果を保存できない場合は、ツールの実行前に警告が表示されます。

- セクションの異なるルールが結合されることはありません。ルールを整理するために作成したセクションによって、可能な結合の範囲が制限されます。また、インターフェイス固有のアクセス ルールとグローバル アクセス ルールが結合されることはありません。グローバル ルールの詳細については、グローバル アクセス ルールについてを参照してください。

ナビゲーション パス

[AAA Rules] ページと[Access Rules] ページからルールを結合できます。テーブルの一番下にある [ツール（Tools）] をクリックして [ルールの結合（Combine Rules）] を選択し、 [Combine Rules Selection Summary] ダイアログボックス （33 ページ）を入力して [OK] をクリックします。

フィールド リファレンス

表 *5:* 結合されたルールの結果の要約

要素	説明
Result Summary	何らかの結合を行うことができる場合、結合の結果の要約が示され、元のルールの数、結合後に残るルールの数、変更されるルールの数、および変更されないルールの数が示されます。
[Resulting Rules] テーブル	ポリシー内に現存するルールを置換するルール。[OK] をクリックした場合、これらのルールがポリシーの一部となります。カラムは、関連付けられたポリシー内のカラム（[AAA Rules] ページまたは[Access Rules] ページを参照）に、[Rule State] カラムが追加されたものです。 [Rule State] カラムには、ルールのステータスが示されます。 • [Modified]、[Combined]：新しいルールは、1 つ以上のルールを結合した結果、または既存のルールを変更した結果として生成されたものです。セルの枠が赤い場合、内容が結合されたセルであることを示します。 • [Unchanged]：ルールは他のルールと結合できなかったため、変更されていません。 • [Not Selected]：可能な結合に対してルールを選択していません。 ルールが多数存在する場合、テーブルの下のボタンを使用して、変更のあるルール全部をスクロールできます。変更されていないルールおよび選択されていないルールはスキップされます。
[Original rules] テーブル（下半分のテーブル）	ダイアログボックスの下半分のテーブルに、上半分のテーブルで選択したルールを作成するために結合された元のルールが表示されます。

要素	説明
[Detail Report] ボタン	このボタンをクリックすると、結果の HTML レポートが作成されます。レポートには結果が要約され、結果のルールの詳細と、新しいルールを作成するために結合されたルールも表示されます。 結合されたルールのセル内に多数のエントリがある場合、このレポートを使用すると、結果を簡単に解釈できます。あとで使用できるようにレポートを印刷または保存することもできます。

Rule Combiner 結果の例

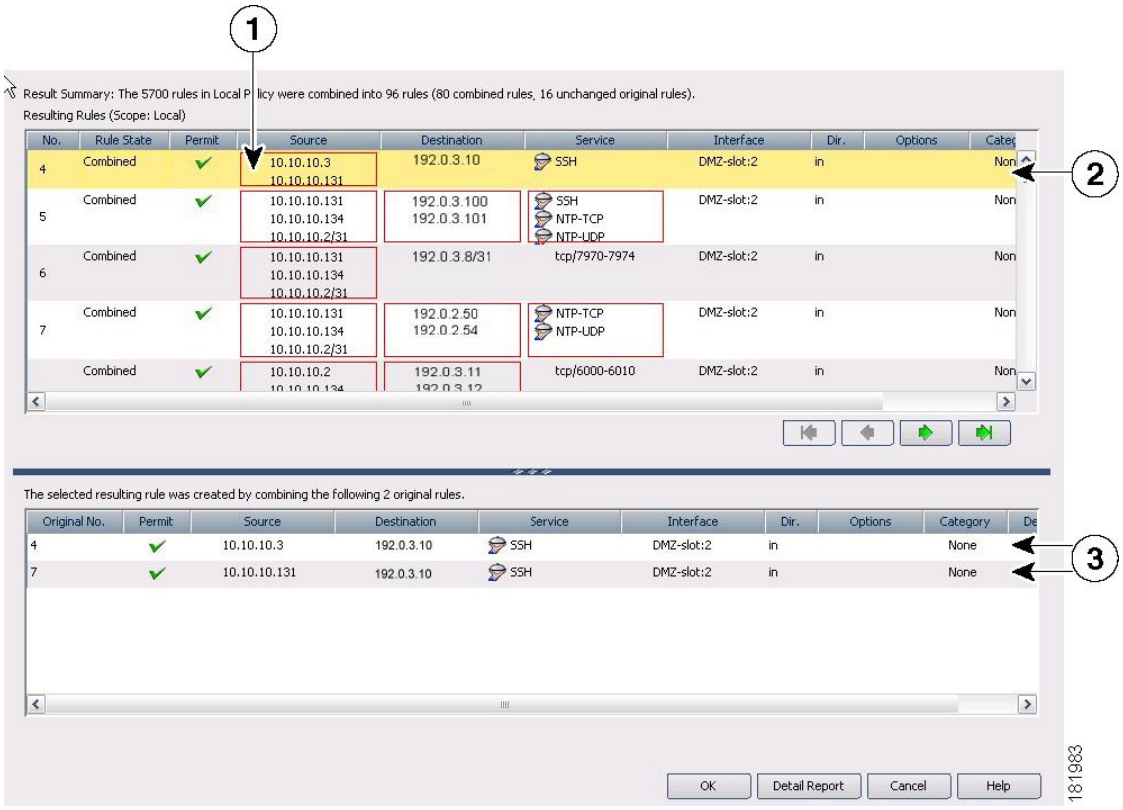
ルールの結合 （31 ページ）で説明されているように Combine Rules ツールを実行すると、結合の結果が [Rule Combiner Results] ダイアログボックスに表示されます（Rule Combiner 結果の解釈 （35 ページ）を参照）。

次の図に、ルールの結合の例を示します。

新しいルールが上半分のテーブルに表示されます。新しいルールが変更済みルールまたは結合済みルールとして示され、変更されたセルの枠は赤色になります。上半分のテーブルで新しいルールを選択すると、下半分のテーブルに、新しいルールを作成するために結合された古いルールが表示されます。この例では、2 つの古いルールは、宛先、サービス、およびインターフェイスが同じです。また、2 つの異なる送信元が連結されて、新しいルールを構成しています。

レポートの一番上に、結果が要約されます。この例では、5700 個のルールが 96 個に縮小されました。

図 *3 : Rule Combiner* の結果例



1	結合されたセル	3	元のルール
2	新しく結合されたルール		

関連項目

- ファイアウォール AAA ルールの管理
- ファイアウォール アクセス ルールの管理

IPv4 ルールから統合ルールへの変換

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。Security Manager 4.4 および ASA 9.0+ では、これらのポリシーとポリシーオブジェクトが結合または統合されました。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、AAA、アクセス、および検査ルールのポリシー タイプの IPv4 および統合バージョンが提供されます。

個別の IPv4 および IPv6 ファイアウォールルールを「統合」ルールに変換するユーティリティが Security Manager 4.4 で提供され、ASA を以前のバージョンから 9.0 以降にアップグレードするときに使用できます。

ナビゲーション パス

ファイアウォールルール統合ユーティリティにアクセスするには、次の手順を実行します。

- （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 IPv4 ルールタイプを選択し、[ポリシー（Policies）] ペインで目的のポリシーを右クリックします。 [< ルールタイプ >ルール（統合）に変換（Convert to <rule-type > Rules (Unified)）] を選択します。

関連項目

- [AAA Rules] ページ
- [Access Rules] ページ
- [Inspection Rules] ページ

上記のようにユーティリティを開きます。 [ポリシーの変換（Convert Policy）] ダイアログボックスで新しい統合ポリシーの名前を指定して、[OK] をクリックします。

処理後、新しい統合ルールポリシーが表示されます。このポリシーを ASA 9.0 以降のデバイスに割り当てることができるようになりました。

ポリシー クエリー レポートの生成

ほとんどのファイアウォール ルール ポリシーでは、ルールの評価に役立つポリシー クエリー レポートを生成できます。ポリシー クエリー レポートを使用すると、新しいルールを作成して特定の送信元、ユーザ、宛先、インターフェイス、サービス、またはゾーンに適用する前に、これらの項目に対してすでに存在しているルールを判別できます。

また、ルールの使用を禁止しているブロッキングルールや、削除できる冗長なルールがあるかどうかも、ある程度は判別できます。ただし、アクセスルールを評価する場合は、これらの問題を判別するためのより強力なルール分析ツールを使用する方が得策です。

ポリシークエリーを作成する場合は、ルールの作成時にトラフィックを説明するのと同様の方法で、関連するトラフィックを説明します。クエリーの作成方法は基本的に、ルールの作成方法と同じです。しかし、ルールの説明をより広範にして、取得するトラフィック セットの幅を広げた方が、単一のルールまたはかぎられた数のルールではなく、関連するルールのセットを確認できます。作成するクエリーは、検出する目的の情報によって決まります。

クエリーの可能なレベルは、現在のビューによって異なります。

- デバイス ビューまたはマップ ビュー：クエリーは、選択したデバイスに制限されます。ただし、サポートされているすべてのルールタイプにわたってクエリーを実行できます。これにより、同じトラフィックに適用されるさまざまなタイプのルールを比較できます。

- ポリシー ビュー：クエリーは、選択したポリシーに制限されます。そのポリシー内で定義されているルールだけが表示されます。他のポリシー タイプを照会することはできません。他のポリシーを調べている間に共有ポリシーを照会する場合は、共有ポリシーに割り当てられているデバイスを選択し、デバイス ビューでデバイスからポリシーを照会します。

関連項目

- [AAA Rules] ページ
- [Access Rules] ページ
- [Inspection Rules] ページ
- [Inspection Rules] ページ
- [Zone-based Firewall Rules] ページ

ステップ 1 [ファイアウォール（Firewall）] フォルダから、照会するポリシーを選択します。次のいずれかのタイプのポリシーを照会できます。

- AAA ルール
- アクセル ルール
- インスペクション ルール
- Web フィルタ ルール（PIX/ASA/FWSM）
- ゾーン ベースのルール

ステップ 2 テーブルの下の [クエリ（Query）] ボタンをクリックし、[デバイスまたはポリシーのクエリ（Querying Device or Policy）] ダイアログボックスを開きます。

ステップ 3 照会するルールを定義するパラメータを入力します。クエリーを設定するときに、少なくとも 1 つのルール タイプ（イネーブル、ディセーブル、または両方、許可、拒否、または両方、および必須、デフォルト、または両方）を選択する必要があります。クエリー パラメータの詳細については、[Querying Device or Policy] ダイアログボックス （41 ページ）を参照してください。

ポリシー ビューで、照会するルールのタイプを変更することはできません。デバイス ビューで、ルール タイプの結合を照会することはできません。

ステップ 4 [OK] をクリックすると、基準と一致したルールが [ポリシークエリ結果（Policy Query Results）] ダイアログボックスに表示されます。このレポートの解釈については、ポリシー クエリー結果の解釈 （45 ページ）を参照してください。

ポリシー クエリー レポートの例については、[Policy Query Result] の例 （47 ページ）を参照してください。

[Querying Device or Policy] ダイアログボックス

[Querying Device] または [Querying Policy] ダイアログボックスを使用して、クエリーのパラメータを設定します。クエリー結果に、パラメータと一致したルールが表示されます。ダイアログボックスのタイトルは、照会する内容を示しています。

- デバイス ビューまたはマップ ビューでは、選択したデバイスに対して定義されているルールを照会します。
- ポリシー ビューでは、選択したポリシーの中だけのルールを照会します。

これらのポリシー タイプから、AAA ルール、アクセル ルール、インスペクション ルール、Web フィルタ ルール（ASA/PIX/FWSM の場合）、およびゾーン ベースのファイアウォール ルールを照会できます。

クエリーを設定するときに、少なくとも 1 つのルール タイプ（イネーブル、ディセーブル、または両方、許可、拒否、または両方、および必須、デフォルト、または両方）を選択する必要があります。

（注） インスペクション ルールでは、インターフェイス値として Global を入力した場合、一致が完了しても、一致ステータス結果は部分一致として表示されます。

結果は、[Policy Query Results] ダイアログボックス（ポリシー クエリー結果の解釈 （45 ページ）を参照）に表示されます。

ナビゲーション パス

ポリシー クエリー レポートを生成するには、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、Firewall フォルダから、サポートされているファイアウォール ルール ポリシーのいずれかを選択して、テーブルの下にある [クエリ（Query）] ボタンをクリックします。
- （ポリシービュー）Firewall フォルダから、サポートされているファイアウォール ルール ポリシーのいずれかを選択し、共有ポリシーセレクタから特定のポリシーを選択して、テーブルの下にある [クエリ（Query）] をクリックします。
- （マップ ビュー）デバイスを右クリックし、[Edit Firewall Policies] メニューから、サポートされているファイアウォール ルール ポリシーを選択します。[クエリ（Query）] ボタンをクリックします。

関連項目

- ポリシー クエリー レポートの生成 （39 ページ）
- [Policy Query Result] の例 （47 ページ）

フィールド リファレンス

表 *6 : [Querying Device or Policy]* ダイアログボックス

要素	説明
Rule Types	照会するルールのタイプ。ポリシー ビューで照会する場合は、選択内容を変更できません。デバイス ビューで照会する場合は、次のいずれかのタイプのルールを選択できます。クエリーのスコープは、選択したデバイスに制限されます。 • AAA ルール • アクセル ルール • インスペクション ルール • Web フィルタ ルール • ゾーン ベースのルール
Enabled and/or Disabled Rules	イネーブルなルール、ディセーブルなルール、またはその両方を照会するか。
Mandatory and/or Default Rules	必須セクション内のルール、デフォルト セクション内のルール、または両方のセクション内のルールを照会するか。
一致（Match）	トラフィックを許可するルール、否定するルール、またはその両方を照会するか。

要素	説明
ソース 宛先	トラフィックの送信元または宛先。項目をカンマで区切って複数の値を入力できます。 （注） フィールドをブランクのままにした場合、クエリーはそのフィールドに対する任意のアドレスと一致します。 次のアドレス タイプを自由に組み合わせて入力し、トラフィックの送信元または宛先を定義できます。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。 • ネットワーク/ホスト オブジェクト。オブジェクトの名前を入力するか、または [選択（Select）] をクリックしてリストから名前を選択します。選択リストから、新しいネットワーク/ホスト オブジェクトを作成することもできます。 • ホスト IP アドレス（10.10.10.100 など）。 • ネットワーク アドレスとサブネット マスク。形式は 10.10.10.0/24 または 10.10.10.0/255.255.255.0。 • IP アドレスの範囲（10.10.10.100-10.10.10.200 など）。 • 10.10.0.10/255.255.0.255 形式の IP アドレスのパターン。この場合のマスクは不連続なビット マスクです（連続および不連続ネットワーク マスク（IPv4 アドレスに対応）を参照）。 ヒント 将来のポリシー クエリー要求を容易にするために、IP アドレスのリストとともにオブジェクトを作成できます。

要素	説明
ユーザー（User）	（ASA 8.4(2) 以降のみ）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）。項目をカンマで区切って複数の値を入力できます。 （注） フィールドをブランクのままにした場合、クエリーは[User]フィールドに何も入っていないルールにのみ一致します。 次の値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。 [選択（Select）]をクリックしてリストからオブジェクト、ユーザー、またはユーザーグループを選択するか、新しいオブジェクトを作成します。 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
サービス	対象となるトラフィックのタイプを定義するサービス。項目をカンマで区切って複数の値を入力できます。 （注） フィールドをブランクのままにした場合、クエリーは任意のサービスと一致します。 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）を入力できます。サービスを入力する場合は、有効な値の入力を求められます。リストから値を選択して、Enter または Tab を押します。 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。 ヒント 将来のポリシー クエリー要求を容易にするために、サービスのリストとともにオブジェクトを作成できます。
インターフェイス	ルールが定義されているインターフェイス。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。名前を入力するか、[選択（Select）]をクリックして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します。 （注） フィールドをブランクのままにした場合、クエリーは任意のインターフェイスまたはインターフェイス ロールと一致します。

要素	説明
Query for Global Rules	アクセス ルールまたはインスペクション ルールを照会するとき、クエリーでグローバル ルールも考慮する必要があるかどうか。
From Zone To Zone	ゾーン ベースのファイアウォール ルールの場合、ルールに定義されているゾーン。ゾーン名（インターフェイスロール）を入力するか、[選択（Select）] をクリックしてリストからゾーンを選択します。
アクション（Actions）	ゾーン ベースのファイアウォール ルールの場合、ルールに定義されているアクション。
Check if Matching Rules Are Shadowed by Rules Above	ポリシー クエリー結果に競合検出情報を含めるかどうか。このオプションを選択すると、パフォーマンスおよびコストの結果に影響を及ぼす可能性があります。

ポリシー クエリー結果の解釈

[Policy Query Results] ダイアログボックスを使用して、[Query Device or Policy] ダイアログボックスで定義したポリシー クエリーの結果を参照します。結果レポートは、[Querying Device or Policy] ダイアログボックス （41 ページ）でクエリパラメータを定義して [OK] をクリックすると開きます。手順については、ポリシー クエリー レポートの生成 （39 ページ）を参照してください。レポート例については、[Policy Query Result] の例 （47 ページ）を参照してください。

ヒント　クエリ結果テーブルで、行をダブルクリックするか、右クリックして[ルールに移動（Go to Rule）] を選択して、ルールを編集できる [ルールポリシー（rules policy）] ページでルールを選択します。ポリシー セレクタで適切なルール ポリシーがまだ選択されていない場合は、これを 2 回行って、実際にルールを選択する必要があることがあります。

レポートを解釈するには、次のレポート セクションを考慮してください。

- [クエリパラメータ（Query Parameters）]：レポートの最上部分で、クエリに対して入力したパラメータを指定します。パラメータを変更する場合は、[クエリの編集（Edit Query）] をクリックして[Querying Device or Policy] ダイアログボックス （41 ページ）を開きます。ここで、変更を行い、レポートを再生成できます。
- [結果（Results）]テーブル：このテーブルには、クエリと一致するすべてのルールが一覧表示されます。複数タイプのルールをクエリした場合、[表示（Display）]フィールドで、調査するルールタイプを選択します。このテーブル内のカラムは、そのタイプのルールのカラムに、次のカラムが追加されたものです。
  - [Match Status]：ルールをクエリーと一致させる方法を示します。

[完全一致（Complete Match）]：ルールはすべてのクエリパラメータと一致します。

[部分一致（Partial Match）]：すべての検索条件が重なるか、一致したルールのスーパーセットです。たとえば、送信元アドレス 10.100.20.0/24、宛先アドレス 10.200.100.0/24、および IP のサービスでルールが定義されている場合、クエリで送信元 10.100.20.0/24 を検索すると、クエリ結果はルールの定義の一部だけを表すため、一致ステータスは部分一致として表示されます。

[影響なし（No Effect）]：ルールが他の一致ルールによりブロックされているか、影響しない競合が存在しています。たとえば、A と B の 2 つの一致ルールがあるとします。ルール A の送信元アドレス、宛先アドレス、およびサービスがルールBのそれらと等しいか、それらを含む場合、ルールBはルールAによってブロックされます。したがって、ルールBはトラフィックには影響しません。

別の例として、グローバルな必須ルールによってサービスが許可されるが、デバイス（ローカル）レベルでのルールによってサービスが拒否されるとします。ルールは最初に一致したものから順に認識されるため、必須のグローバルスコープで一致が検出されると、それ以降は他のルールはチェックされません。ローカルルールは無効です。つまり、サービスは拒否されず、許可されます。適切な結果を得るためには、ポリシーを編集する必要があります。

- [Scope]：ルールが共有ルールかローカル ルールか、必須ルールかデフォルト ルールかを示します。

- [詳細（Details）] テーブル：[詳細（details）] テーブルには、[結果（results）] テーブルで選択されているルールの詳細なクエリ致情報が表示されます。左側のフォルダは、詳細情報を参照できる属性を表しています。詳細を表示するフォルダを選択します。

詳細には、定義したパラメータであるクエリー値と、パラメータと一致するルール内の項目が表示されます。一致の関係は次のいずれかです。

- [Identical]：パラメータは、ルール内の値と同じです。
- [Contains]：パラメータは、ルール内の値を含むスーパーセットです。たとえば、クエリーパラメータがネットワーク/ホスト オブジェクトであり、オブジェクト定義の一部である IP アドレスがルールで使用されている場合などです。
- [Is contained by]：パラメータは、ルールの値の中でネストされているサブセットです。
- [Overlaps]：クエリーパラメータでは、ルール内で使用されている複数のポリシーオブジェクトにまたがる結果が表示されます。たとえば、サービス クエリーパラメータが tcp/70-90 であり、tcp/80-100 として定義されているサービスが結果に表示される場合などです。

関連項目

- [AAA Rules] ページ
- [Access Rules] ページ
- [Inspection Rules] ページ
- [Webフィルタルール（Web Filter Rules）] ページ（ASA/PIX/FWSM）
- [Zone-based Firewall Rules] ページ

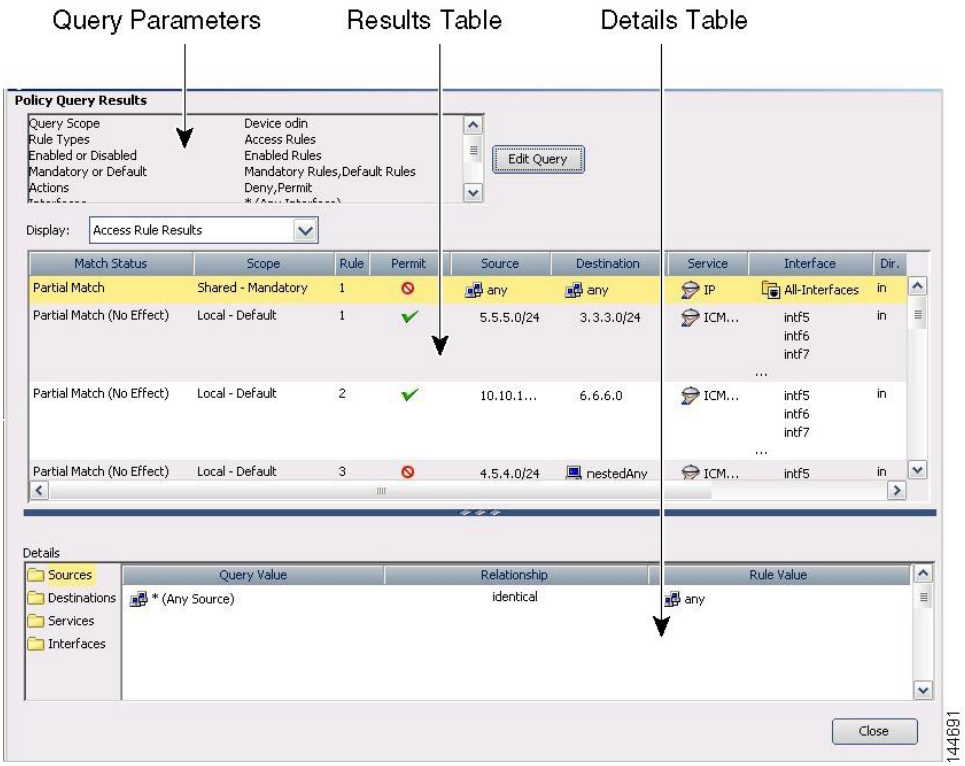
[Policy Query Result] の例

次に、アクセスルールに関するポリシークエリレポートの例を示します。基準によって送信先、宛先、サービス、およびインターフェイスのパラメータは制限されませんが、クエリーはイネーブルなルールに制限されます。共有ルールとローカル ルールの両方が含められます。

[Query Parameters] セクションに、レポートのクエリー基準が表示されます。この例では、結果テーブル内の最初の行が選択されています。また、ウィンドウの下半分の詳細テーブルに、そのルールの詳細情報が表示されています。この例では、詳細テーブルで送信元フォルダが選択されており、ルールの値 **any** が、クエリパラメータ ***** と完全に一致する（任意の送信元アドレスに相当する）ことが結果に示されています。

このレポートの解釈の詳細については、ポリシー クエリー結果の解釈 （45 ページ）を参照してください。

図 *4 : [Policy Query Results]*



関連項目

- ポリシー クエリー レポートの生成 （39 ページ）
- [AAA Rules] ページ
- [Access Rules] ページ
- [Inspection Rules] ページ

- [Webフィルタルール（Web Filter Rules）] ページ（ASA/PIX/FWSM）
- [Zone-based Firewall Rules] ページ

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

ファイアウォール ルール ポリシーを ASA、PIX、FWSM、または IOS 12.4(20)T 以降のデバイスに展開すると、関連付けられたネットワーク オブジェクト グループをデバイス上に作成するときに、ルールで使用するネットワーク/ホスト ポリシー オブジェクトを評価して最適化するように Security Manager を設定できます。最適化によって、隣接するネットワークがマージされ、冗長なネットワーク エントリが削除されます。これにより、実行時のアクセス リスト データ構造と設定のサイズが縮小されます。メモリ制約のある一部の FWSM および PIX デバイスでは、これによるメリットがあります。

たとえば、次のエントリを含みアクセスルール内で使用される **test** という名前のネットワーク/ホストオブジェクトについて考えてみます。

```
192.168.1.0/24
192.168.1.23
10.1.1.0
10.1.1.1
10.1.1.2/31
```

最適化をイネーブルにした場合、ポリシーを展開すると、結果のオブジェクト グループ設定が生成されます。説明に、グループが最適化されたことが示されることに注意してください。

```
object-group network test
 description (Optimized by CS-Manager)
 network-object 10.1.1.0 255.255.255.252
 network-object 192.168.1.0 255.255.255.0
```

最適化をイネーブルにしない場合、グループ設定は次のようになります。

```
object-group network test
 network-object 192.168.1.0 255.255.255.0
 network-object 192.168.1.23 255.255.255.255
 network-object 10.1.1.0 255.255.255.255
 network-object 10.1.1.1 255.255.255.255
 network-object 10.1.1.2 255.255.255.254
```

この最適化によってネットワーク/ホスト オブジェクトの定義が変更されることも、新しいネットワーク/ホスト ポリシー オブジェクトが作成されることもありません。デバイス上でポリシーを再検出すると、変更されていない既存のポリシー オブジェクトが使用されます。

（注） ネットワーク/ホスト オブジェクトに別のネットワーク/ホスト オブジェクトが含まれる場合、それらのオブジェクトは結合されません。それぞれのネットワーク/ホスト オブジェクトが個別に最適化されます。また、Security Manager は、連続しないサブネット マスクを使用するネットワーク/ホスト オブジェクト オブジェクトを最適化できません。

最適化を設定するには、[Deployment] ページで [展開中にネットワークオブジェクトグループを最適化する（Optimize Network Object-Groups During Deployment）] オプションを選択します（**[ツール（Tools）] > [Security Managerの管理（Security Manager Administration）]** を選択してコンテンツテーブルから [展開（Deployment）] を選択）。デフォルトでは、展開中にネットワーク オブジェクト グループは最適化されません。

（注）

CSM 4.17 SP1 および CSM 4.18 を設定せずに CSM 4.19 にアップグレードした場合、object-group service を含むファイアウォールの展開は、次のオブジェクトに対して失敗します。

- service-object gre
- service-object 41
- service-object ah

展開の失敗を回避するには、CSM サーバーの DB 側で次の SQL クエリを実行する必要があります。

```
$SIG{INT} = 'IGNORE';
use CRM;
use DBI;
use lib "$ENV{NMSROOT}/lib/perl/install";
use InstallUtility;
require "$ENV{NMSROOT}/cgi-bin/dbadmin/pdbadmin/dbAdminCommon.pl";
my $DROP_CONNECTION_FLAG = false;

checkDMisRunning();
&resolveGreSubTypeEntries();

sub checkDMisRunning
{
 my $d = '\\';
    my ($rc, $dmIsRunning, $line, @lines);
    $rc = open IN, "$ENV{NMSROOT}${d}bin${d}pdshow 2>&1 |";
    if (!$rc)
    {
        print "ERROR: *** Could not execute pdshow ***\n";
        print "ERROR: *** probable cause: daemon manger is corrupted ***";
        exit(-1);
    }

    @lines = <IN>;

    $dmIsRunning = 1;
    for $line (@lines)
    {

        if ($line =~ m/ERROR:\s+connect\s+to\s+dmgtd.*on\s+port\s+.+failed:/)
        {
   $dmIsRunning = 0;
            last;
        }
 }
    close IN;

    if ($dmIsRunning)
    {
        print "Daemon manager is  running ..\n";
     }
 else
 {
     print "Daemon manager is not running ..\n";
  print "Deamon manager should be running to execute this file\n";
  exit(-1);
  }
}
```

```
sub resolveGreSubTypeEntries
{

  $dsn="vms";
  $node_dbh = &dbinternal::connect("dsn=$dsn");

  if ($node_dbh)
  {
   print "\n*****************************************\n";
   print "\nScript Execution Starts \n" ;
   print "\n*****************************************\n";
   my $select_query = "select count(*) from BB_MAIN where OBJECTID =1106 and name='gre'
 and subtype!='SO'";
   my $select_query_prep = $node_dbh->prepare($select_query) || die "Error preparing
query" . $node_dbh->errstr;
   $select_query_prep->execute || die "Error executing query" . $select_query_prep->errstr;

   my @node_results;
      $impactedcount = 0;
   while (@node_results = $select_query_prep->fetchrow_array())
   {
         my $size = @node_results;
      for (my $j=0; $j < $size; $j++)
        {
     $impactedcount = $node_results[$j];
          }
      }
   if($impactedcount > 0){
       my $updateQuery = "update BB_MAIN set subtype='SO' where OBJECTID=1106";
       my $prep = $node_dbh->prepare($updateQuery) || die "Error preparing query" .
$node_dbh->errstr;
       $prep->execute || die "Error executing query" . $prep->errstr;
   }
   print "\n*****************************************\n";
   print "\nScript Execution Completed! \n" ;
   print "\n*****************************************\n";
     }

  return 0;

}
```

スクリプトを ~CSCOpx/bin ディレクトリにコピーし、次のコマンドを実行します。

```
C:\PROGRA~2\CSCOpx\bin\perl
C:\PROGRA~2\CSCOpx\bin\resolveDBEntriesCSCvj54910.pl#!/usr/bin/perl
```

検出中のオブジェクト グループの展開

オブジェクト グループを使用するデバイスからポリシーを検出するとき、グループからポリシー オブジェクトを作成するのではなく、それらのオブジェクト グループを構成する項目に展開するように設定できます。

たとえば、CSM_INLINE_55 という名前のオブジェクト グループにホスト 10.100.10.15、10.100.10.18、および10.100.10.25が含まれる場合、オブジェクトを展開することによりアクセス コントロール リストをインポートすると、CSM_INLINE_55 という名前のネットワーク/ホスト ポリシー オブジェクトではなく、3つすべてのアドレスが送信元セル（または該当する場合は宛先セル）に含まれるルールが作成されます。

展開を設定するには、展開するグループのプレフィックスを識別できるようなオブジェクト グループの命名方式が必要となります。デフォルトでは、プレフィックス CSM_INLINE で始まるすべてのオブジェクト グループが展開されます。[ツール（Tools）] > [Security Manager の管理（Security Manager Administration）] を選択し、目次で [検出（Discovery）] を選択することにより、[Discovery] ページの [これらのプレフィックスを持つオブジェクトグループを自動展開する（Auto-Expand Object Groups with These Prefixes）] フィールドでこれらのプレフィックスを設定します。

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。