サービス ポリシーの設定

サービス ポリシーでは、一貫性と柔軟性を備えた方法で ASA 機能を設定できます。たとえば、サービス ポリシーを使用すると、すべての TCP アプリケーションに適用されるタイムアウト コンフィギュレーションではなく、特定の TCP アプリケーションに固有のタイムアウト コンフィギュレーションを作成できます。サービス ポリシーは、1 つのインターフェイスに適用されるか、またはグローバルに適用される複数のサービス ポリシー ルールで構成されます。

この章は、次の項で構成されています。

サービス ポリシーに関する情報

この項では、サービス ポリシーの機能について説明します。説明する項目は次のとおりです。

サポートされる機能

表 1-1 に、サービス ポリシー ルールでサポートされる機能を示します。

表 1-1　サービス ポリシー ルールの機能

機能	通過トラフィック用か	管理トラフィック用か	参照先
アプリケーション インスペクション（複数タイプ）	RADIUS アカウンティングを除く**すべて**	**RADIUS アカウンティング**のみ	• 第 9 章「アプリケーション レイヤ プロトコル インスペクションの準備」 • 第 10 章「基本インターネット プロトコルのインスペクションの設定」 • 第 11 章「音声とビデオのプロトコルのインスペクションの設定」 • 第 12 章「データベースとディレクトリのプロトコル インスペクションの設定」 • 第 13 章「管理アプリケーション プロトコルのインスペクションの設定」 • 第 24 章「Cisco クラウド Web セキュリティ用の ASA の設定」
ASA CSC	**Yes**	No	第 31 章「ASA CSC モジュールの設定」
ASA IPS	**Yes**	No	第 29 章「ASA IPS モジュールの設定」
ASA CX	**Yes**	No	第 30 章「ASA CX モジュールの設定」
NetFlow セキュア イベント ロギングのフィルタリング	**Yes**	**Yes**	一般的な操作のコンフィギュレーション ガイドの Chapter 41, “Configuring NetFlow Secure Event Logging (NSEL),”
QoS 入出力ポリシング	**Yes**	No	第 22 章「QoS の設定」
QoS 標準プライオリティ キュー	**Yes**	No	第 22 章「QoS の設定」
QoS トラフィック シェーピング、階層型プライオリティ キュー	**Yes**	**Yes**	第 22 章「QoS の設定」
TCP と UDP の接続制限値とタイムアウト、および TCP シーケンス番号のランダム化	**Yes**	**Yes**	第 21 章「接続の設定」
TCP の正規化	**Yes**	No	第 21 章「接続の設定」
TCP ステート バイパス	**Yes**	No	第 21 章「接続の設定」
アイデンティティ ファイアウォールのユーザ統計情報	**Yes**	**Yes**	コマンド リファレンスの **user-statistics** コマンドを参照してください。

機能の方向

アクションは、機能に応じて双方向または単方向にトラフィックに適用されます。双方向に適用される機能の場合、トラフィックが両方向のクラス マップと一致した場合に、ポリシー マップを適用するインターフェイスを出入りするすべてのトラフィックが影響を受けます。

（注）　グローバル ポリシーを使用する場合は、すべての機能が単方向です。単一インターフェイスに適用する場合に通常双方向の機能は、グローバルに適用される場合、各インターフェイスの入力にのみ適用されます。ポリシーはすべてのインターフェイスに適用されるため、ポリシーは両方向に適用され、この場合の双方向は冗長になります。

QoS プライオリティ キューなど単方向に適用される機能の場合は、ポリシー マップを適用するインターフェイスに出入りする（機能によって異なります）トラフィックだけが影響を受けます。各機能の方向については、表 1-2 を参照してください。

表 1-2　機能の方向

機能	単一インターフェイスでの方向	グローバルでの方向
アプリケーション インスペクション（複数タイプ）	双方向	入力
ASA CSC	双方向	入力
ASA CX	双方向	入力
ASA CX 認証プロキシ	入力	入力
ASA IPS	双方向	入力
NetFlow セキュア イベント ロギングのフィルタリング	該当なし	入力
QoS 入力ポリシング	入力	入力
QoS 出力ポリシング	出力	出力
QoS 標準プライオリティ キュー	出力	出力
QoS トラフィック シェーピング、階層型プライオリティ キュー	出力	出力
TCP と UDP の接続制限値とタイムアウト、および TCP シーケンス番号のランダム化	双方向	入力
TCP の正規化	双方向	入力
TCP ステート バイパス	双方向	入力
アイデンティティ ファイアウォールのユーザ統計情報	双方向	入力

サービス ポリシー内の機能照合

パケットが所定のインターフェイスのポリシー内のルールと照合される方法については、次の情報を参照してください。

1. パケットは、機能タイプごとにインターフェイスのルールの 1 つとだけ一致することができます。
2. パケットが 1 つの機能タイプのルールと一致する場合、ASA は、その機能タイプの後続のどのルールに対してもそのパケットを照合しません。
3. ただし、そのパケットが異なる機能タイプの後続のルールと一致する場合、ASA は後続ルールのアクションも適用します（サポートされている場合）。サポートされていない組み合わせの詳細については、「特定の機能アクションの非互換性」（P.1-5）を参照してください。

（注）　アプリケーション インスペクションには、複数のインスペクション タイプが含まれ、ほとんどのタイプは相互に排他的です。組み合わせ可能なインスペクションの場合、各インスペクションは個々の機能と見なされます。

たとえば、パケットが接続制限のルールと一致し、アプリケーション インスペクションのルールとも一致する場合は、両方のアクションが適用されます。

パケットが HTTP インスペクションのルールと一致するが、HTTP インスペクションを含む別のルールとも一致する場合、2 番目のルールのアクションは適用されません。

パケットが HTTP インスペクションのルールと一致するが、FTP インスペクションを含む別のルールとも一致する場合、2 番目のルールのアクションは HTTP および FTP インスペクション cannpt が組み合わされているため、適用されません。

パケットが HTTP インスペクションのルールと一致するが、IPv6 インスペクションを含む別のルールとも一致する場合、両方のアクションは IPv6 インスペクションが他のインスペクションのタイプと組み合わせることができるため、適用されません。

複数の機能アクションが適用される順序

サービス ポリシーの各種のアクションが実行される順序は、アクションがテーブルに表示される順序とは無関係です。

（注）　NetFlow セキュア イベント ロギングのフィルタリングとアイデンティティ ファイアウォールのユーザ統計情報は順番に依存しません。

アクションは次の順序で実行されます。

1. QoS 入力ポリシング
2. TCP の正規化、TCP と UDP の接続制限値とタイムアウト、TCP シーケンス番号のランダム化、および TCP ステート バイパス

（注）　ASA がプロキシ サービス（AAA や CSC など）を実行したり、TCP ペイロード（FTP インスペクション）を変更したりするときは、TCP ノーマライザはデュアル モードで動作します。その場合、サービスを変更するプロキシやペイロードの前後で適用されます。

3. ASA CSC
4. 他のインスペクションと組み合わせることができるアプリケーション インスペクション：
   a. IPv6
   b. IP オプション
   c. WAAS
5. 他のインスペクションと組み合わせることができないアプリケーション インスペクション：詳細については、「特定の機能アクションの非互換性」（P.1-5）を参照してください。
6. ASA IPS
7. ASA CX
8. QoS 出力ポリシング

9. QoS 標準プライオリティ キュー
10. QoS トラフィック シェーピング、階層型プライオリティ キュー

特定の機能アクションの非互換性

一部の機能は同じトラフィックに対して相互に互換性がありません。次のリストには、すべての非互換性が含まれていない場合があります。各機能の互換性については、機能に関する章または項を参照してください。

- QoS プライオリティ キューイングと QoS ポリシングは同じトラフィックの集合に対して設定できません。
- ほとんどのインスペクションは別のインスペクションと組み合わせられないため、同じトラフィックに複数のインスペクションを設定しても、ASA は 1 つのインスペクションだけを適用します。HTTP インスペクションはクラウド Web セキュリティ インスペクションと組み合わせることができます。他の例外は、「複数の機能アクションが適用される順序」（P.1-4）に記載されています。
- トラフィックを ASA CX および ASA IPS などの複数のモジュールに送信されるように設定できません。
- HTTP インスペクションは、ASA CX と互換性がありません。
- ASA CX はクラウド Web セキュリティと互換性がありません。

（注）　デフォルトのグローバル ポリシーで使用される Default Inspection Traffic トラフィック クラスは、すべてのインスペクションに対してデフォルトのポートを照合するための特別な CLI ショートカットです。ポリシー マップで使用すると、このクラス マップでは、トラフィックの宛先ポートに基づいて、各パケットに正しいインスペクションが適用されます。たとえば、宛先がポート 69 の UDP トラフィックが ASA に到達すると、ASA は TFTP インスペクションを適用し、宛先がポート 21 の TCP トラフィックが到着すると、ASA は FTP インスペクションを適用します。そのため、この場合に限って同じクラス マップに複数のインスペクションを設定できます。通常、ASA は、ポート番号を使用して適用するインスペクションを決定しないため、標準以外のポートなどにも柔軟にインスペクションを適用できます。

このトラフィック クラスには、クラウド Web セキュリティ インスペクション用のデフォルト ポートは含まれません（80 および 443）。

複数のサービス ポリシーの場合の機能照合

TCP および UDP トラフィック（およびステートフル ICMP インスペクションがイネーブルの場合は ICMP）の場合、サービス ポリシーはトラフィック フローに対して作用し、個々のパケットに限定されません。トラフィックが、1 つのインターフェイスのポリシーで定義されている機能に一致する既存の接続の一部である場合、そのトラフィック フローを別のインターフェイスのポリシーにある同じ機能と照合することはできません。最初のポリシーのみが使用されます。

たとえば、HTTP トラフィックが、HTTP トラフィックを検査する内部インターフェイスのポリシーと一致するときに、HTTP インスペクション用の外部インターフェイスに別のポリシーがある場合、そのトラフィックが外部インターフェイスの出力側でも検査されることはありません。同様に、その接続のリターン トラフィックが外部インターフェイスの入力ポリシーによって検査されたり、内部インターフェイスの出力ポリシーによって検査されたりすることもありません。

ステートフル ICMP インスペクションをイネーブルにしない場合の ICMP のように、フローとして扱われないトラフィックの場合は、リターン トラフィックを戻り側のインターフェイスの別のポリシー マップと照合できます。たとえば、内部および外部のインターフェイスで IPS を設定するとき、内部ポリシーでは仮想センサー 1 を使用するのに対して、外部ポリシーでは仮想センサー 2 を使用する場合、非ステートフル ping は仮想センサー 1 の発信側を照合するだけでなく、仮想センサー 2 の着信側も照合します。

サービス ポリシーのライセンス要件

モデル	ライセンス要件
すべてのモデル	基本ライセンス

ガイドラインと制限事項

この項では、この機能のガイドラインと制限事項について説明します。

コンテキスト モードのガイドライン

シングル コンテキスト モードとマルチ コンテキスト モードでサポートされています。

ファイアウォール モードのガイドライン

ルーテッド ファイアウォール モードとトランスペアレント ファイアウォール モードでサポートされています。

IPv6 のガイドライン

IPv6 は次の機能でサポートされています。

- DNS、FTP、HTTP、ICMP、ScanSafe、SIP、SMTP、IPsec-pass-thru、および IPv6 のアプリケーション インスペクション
- ASA IPS
- ASA CX
- NetFlow セキュア イベント ロギングのフィルタリング
- TCP と UDP の接続制限値とタイムアウト、および TCP シーケンス番号のランダム化
- TCP の正規化
- TCP ステート バイパス
- アイデンティティ ファイアウォールのユーザ統計情報

トラフィック クラスのガイドライン

すべてのタイプのトラフィック クラスの最大数は、シングル モードでは 255 個、マルチ モードではコンテキストごとに 255 個です。クラス マップには、次のタイプがあります。

- レイヤ 3/4 クラスマップ（通過トラフィックと管理トラフィック向け）
- インスペクション クラス マップ
- 正規表現クラス マップ

- インスペクション ポリシー マップ下で直接使用される **match** コマンド

この制限にはすべてのタイプのデフォルト トラフィック クラスも含まれ、ユーザ設定のトラフィック クラスを約 235 に制限します。「デフォルトのトラフィック クラス」（P.1-8）を参照してください。

サービス ポリシーのガイドライン

- インターフェイス サービス ポリシーは、特定の機能に対するグローバル サービス ポリシーより優先されます。たとえば、FTP インスペクションのグローバル ポリシーと、TCP 正規化のインターフェイス ポリシーがある場合、FTP インスペクションと TCP 正規化の両方がインターフェイスに適用されます。これに対し、FTP インスペクションのグローバル ポリシーと、FTP インスペクションのインターフェイス ポリシーがある場合は、インターフェイス ポリシーの FTP インスペクションだけがインターフェイスに適用されます。
- 適用できるグローバル ポリシーは 1 つだけです。たとえば、機能セット 1 が含まれたグローバル ポリシーと、機能セット 2 が含まれた別のグローバル ポリシーを作成できません。すべての機能は 1 つのポリシーに含める必要があります。
- コンフィギュレーションに対してサービス ポリシーの変更を加えた場合は、すべての*新しい*接続で新しいサービス ポリシーが使用されます。既存の接続では、その接続が確立された時点で設定されていたポリシーの使用が続行されます。**show** コマンドの出力には、古い接続に関するデータが含まれていません。

  たとえばインターフェイスから QoS サービス ポリシーを削除し、変更したバージョンを再度追加した場合、**show service-policy** コマンドには、新しいサービス ポリシーに一致する新しい接続に関連付けられた QoS カウンタだけが表示されます。古いポリシーの既存の接続はコマンド出力には表示されなくなります。

  すべての接続が新しいポリシーを確実に使用するように、現在の接続を解除し、新しいポリシーを使用して再度接続できるようにします。**clear conn** または **clear local-host** コマンドを参照してください。

デフォルト設定

モジュラ ポリシー フレームワークのデフォルト設定については、次の項目で説明します。

- 「デフォルト コンフィギュレーション」（P.1-7）
- 「デフォルトのトラフィック クラス」（P.1-8）

デフォルト コンフィギュレーション

デフォルトでは、すべてのデフォルト アプリケーション インスペクション トラフィックに一致するポリシーがコンフィギュレーションに含まれ、特定のインスペクションがすべてのインターフェイスのトラフィックに適用されます（グローバル ポリシー）。すべてのインスペクションがデフォルトでイネーブルになっているわけではありません。適用できるグローバル ポリシーは 1 つだけなので、グローバル ポリシーを変更する場合は、デフォルトのポリシーを編集するか、デフォルトのポリシーをディセーブルにして新しいポリシーを適用します。（特定の機能では、グローバル ポリシーはインターフェイス ポリシーより優先されます）。

デフォルト ポリシーには、次のアプリケーション インスペクションが含まれます。

- メッセージの最大長 512 バイトに対する DNS インスペクション
- FTP
- H323（H225）

- H323（RAS）
- RSH
- RTSP
- ESMTP
- SQLnet
- Skinny（SCCP）
- SunRPC
- XDMCP
- SIP
- NetBios
- TFTP
- IP オプション

デフォルトのトラフィック クラス

コンフィギュレーションには、デフォルト グローバル ポリシーで ASA が使用するデフォルトのトラフィック クラスが含まれます。これは Default Inspection Traffic と呼ばれ、デフォルト インスペクション トラフィックと一致します。デフォルト グローバル ポリシーで使用されるこのクラスは、デフォルト ポートをすべてのインスペクションと照合する特別なショートカットです。ポリシーで使用すると、このクラスでは、トラフィックの宛先ポートに基づいて、各パケットに正しいインスペクションが適用されます。たとえば、宛先がポート 69 の UDP トラフィックが ASA に到達すると、ASA は TFTP インスペクションを適用し、宛先がポート 21 の TCP トラフィックが到着すると、ASA は FTP インスペクションを適用します。そのため、この場合に限って同じクラス マップに複数のインスペクションを設定できます。通常、ASA は、ポート番号を使用して適用するインスペクションを決定しないため、標準以外のポートなどにも柔軟にインスペクションを適用できます。

デフォルト コンフィギュレーションにある別のクラス マップは、class-default と呼ばれ、すべてのトラフィックと一致します。任意のトラフィック クラスを使用する代わりに、必要に応じて class-default クラスを使用できます。実際のところ、class-default で使用可能な機能は、QoS トラフィック シェーピングなどの一部の機能だけです。

サービス ポリシーを設定するためのタスク フロー

この項は、次の内容で構成されています。

- 「サービス ポリシー ルールの設定のタスク フロー」（P.1-8）

サービス ポリシー ルールの設定のタスク フロー

サービス ポリシーの設定では、インターフェイスあたりのサービス ポリシー ルール、またはグローバル ポリシーのサービス ポリシー ルールを 1 つ以上追加します。それぞれのルールごとに、次の要素を指定します。

ステップ 1　ルールを適用するインターフェイスを指定するか、またはグローバル ポリシーを指定します。

ステップ 2　アクションを適用するトラフィックを指定します。レイヤ 3 および 4 の通過トラフィックを指定できます。

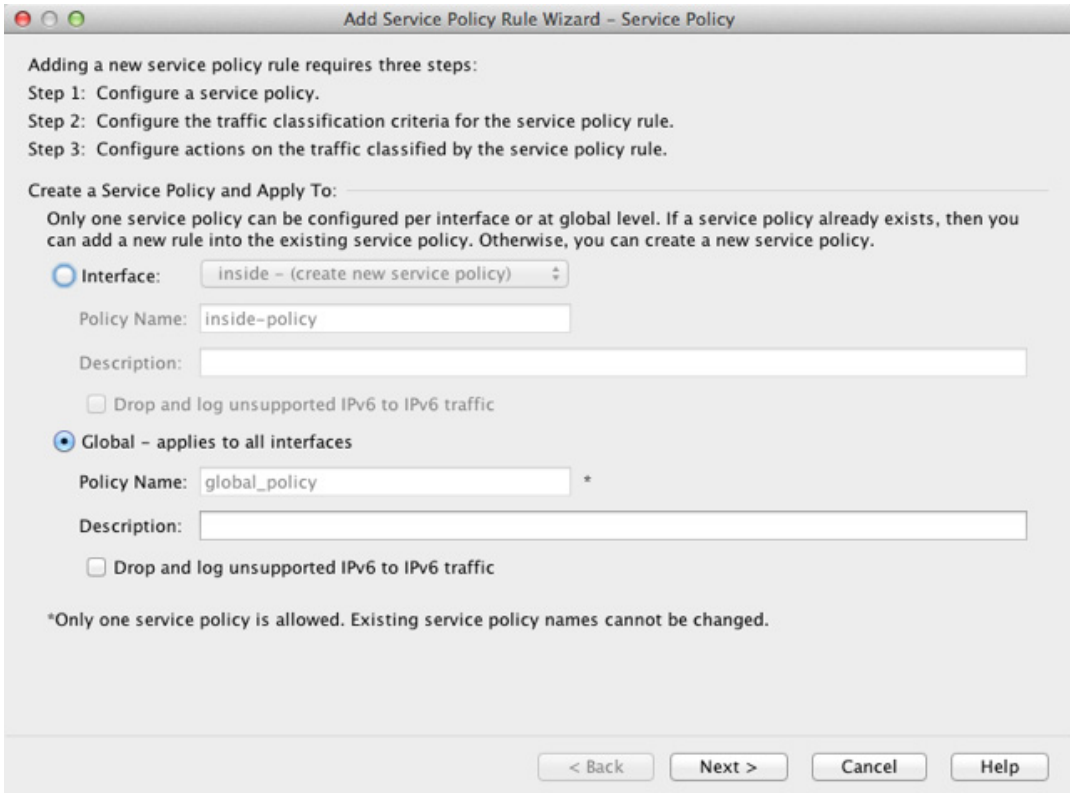
ステップ 3　トラフィック クラスにアクションを適用します。トラフィック クラスごとに複数のアクションを適用できます。

通過トラフィックのサービス ポリシー ルールの追加

詳細については、「サポートされる機能」（P.1-1）を参照してください。通過トラフィックのサービス ポリシー ルールを追加するには、次の手順を実行します。

ステップ 1　[Configuration] > [Firewall] > [Service Policy Rules] ペインを選択して、[Add] をクリックします。

[Add Service Policy Rule Wizard - Service Policy] ダイアログボックスが表示されます。



（注）　[Add] ボタンの右側にある小さな矢印ではなく [Add] ボタンをクリックすると、通過トラフィック ルールがデフォルトで追加されます。[Add] ボタン上の矢印をクリックすると、通過トラフィック ルールと管理トラフィック ルールのいずれかを選択できます。

ステップ 2　[Create a Service Policy and Apply To] 領域で、次のオプションの 1 つをクリックします。

- [Interface]。このオプションでは、サービス ポリシーが 1 つのインターフェイスに適用されます。インターフェイス サービス ポリシーは、特定の機能に対するグローバル サービス ポリシーより優先されます。たとえば、FTP インスペクションを行うグローバル ポリシーと、TCP 接続制限を行うインターフェイス ポリシーが設定されている場合、インターフェイスには FTP インスペクションおよび TCP 接続制限がどちらも適用されます。これに対し、FTP インスペクションのグローバル ポリシーと、FTP インスペクションのインターフェイス ポリシーがある場合は、インターフェイス ポリシーの FTP インスペクションだけがインターフェイスに適用されます。

  a. ドロップダウン リストからインターフェイスを選択します。

  すでにポリシーが適用されているインターフェイスを選択する場合は、ウィザードの指示に従って、新しいサービス ポリシー ルールをそのインターフェイスに追加できます。

  b. 新しいサービス ポリシーの場合は、[Policy Name] フィールドに名前を入力します。

  c. （任意）[Description] フィールドに説明を入力します。

  d. （任意）[Drop and log unsupported IPv6 to IPv6 traffic] チェックボックスをオンにして、IPv6 トラフィックをサポートしないアプリケーション インスペクションによってドロップされる IPv6 トラフィックの syslog（767001）を生成します。デフォルトでは、syslog が生成されません。IPv6 をサポートするインスペクションのリストについては、「IPv6 のガイドライン」（P.1-6）を参照してください。

- [Global - applies to all interfaces]。このオプションでは、サービス ポリシーがすべてのインターフェイスにグローバルに適用されます。デフォルト アプリケーション インスペクションのサービス ポリシー ルールを含むグローバル ポリシーは、デフォルトで存在します。詳細については、「デフォルト設定」（P.1-7）を参照してください。ウィザードを使用してルールをグローバル ポリシーに追加できます。

  a. 新しいサービス ポリシーの場合は、[Policy Name] フィールドに名前を入力します。

  b. （任意）[Description] フィールドに説明を入力します。

  c. （任意）[Drop and log unsupported IPv6 to IPv6 traffic] チェックボックスをオンにして、IPv6 トラフィックをサポートしないアプリケーション インスペクションによってドロップされる IPv6 トラフィックの syslog（767001）を生成します。デフォルトでは、syslog が生成されません。IPv6 をサポートするインスペクションのリストについては、「IPv6 のガイドライン」（P.1-6）を参照してください。

ステップ 3　[Next] をクリックします。

[Add Service Policy Rule Wizard - Traffic Classification Criteria] ダイアログボックスが表示されます。

ステップ 4　次のオプションのいずれかをクリックして、ポリシーのアクションを適用するトラフィックを指定します。

- [Create a new traffic class]。[Create a new traffic class] フィールドにトラフィック クラス名を入力し、説明（任意）を入力します。

  基準のいずれかを使用してトラフィックを特定します。

  - [Default Inspection Traffic]：このクラスは、ASA が検査可能なすべてのアプリケーションによって使用される、デフォルトの TCP および UDP ポートを照合します。

    デフォルト グローバル ポリシーで使用されるこのオプションは、ルール内で使用されると、トラフィックの宛先ポートに基づいて、パケットごとに正しい検査が適用されるようにします。たとえば、宛先がポート 69 の UDP トラフィックが ASA に到達すると、ASA は TFTP インスペクションを適用し、宛先がポート 21 の TCP トラフィックが到着すると、ASA は FTP インスペクションを適用します。つまり、この場合に限り、同じルールに対して複数の検査を設定できます（アクションの組み合わせの詳細については、「特定の機能アクションの非互換性」（P.1-5）を参照してください）。通常、ASA は、ポート番号を使用して適用するインスペクションを決定しないため、標準以外のポートなどにも柔軟にインスペクションを適用できます。

デフォルト ポートのリストについては、「デフォルト設定」（P.9-4）を参照してください。ASA には、デフォルトのインスペクション トラフィックに一致して、すべてのインターフェイス上のトラフィックに共通検査を適用するデフォルト グローバル ポリシーが含まれます。Default Inspection Traffic クラスにポートが含まれているすべてのアプリケーションが、ポリシー マップにおいてデフォルトでイネーブルになっているわけではありません。

Source and Destination IP Address (uses ACL) クラスを Default Inspection Traffic クラスと一緒に指定して、照合されるトラフィックを絞り込むことができます。Default Inspection Traffic クラスは一致するポートとプロトコルを指定するので、アクセス リストのポートとプロトコルはすべて無視されます。

- [Source and Destination IP Address (uses ACL)]：このクラスは拡張アクセス リストで指定されているトラフィックを照合します。ASA がトランスペアレント ファイアウォール モードで動作している場合は、EtherType ACL を使用できます。

（注）　このタイプの新しいトラフィック クラスを作成する場合は、最初にアクセス コントロール エントリ（ACE）を 1 つだけ指定できます。ルールを追加した後は、同じインターフェイスまたはグローバル ポリシーに新しいルールを追加し、それから [Traffic Classification] ダイアログボックス（以下を参照）で [Add rule to existing traffic class] を指定することによって、ACE を追加できます。

- [Tunnel Group]：このクラスは、QoS を適用するトンネル グループのトラフィックを照合します。その他にもう 1 つのトラフィック照合オプションを指定してトラフィック照合対象をさらに絞込み、[Any Traffic]、[Source and Destination IP Address (uses ACL)]、または [Default Inspection Traffic] を排除できます。
- [TCP or UDP Destination Port]：1 つのポートまたは連続する一定範囲のポートを照合します。

ヒント　複数の非連続ポートを使用するアプリケーションの場合は、[Source and Destination IP Address (uses ACL)] を使用して各ポートを照合します。

- [RTP Range]：クラス マップは、RTP トラフィックを照合します。
- [IP DiffServ CodePoints (DSCP)]：このクラスは、IP ヘッダーの最大 8 つの DSCP 値を照合します。
- [IP Precedence]：このクラス マップは、IP ヘッダーの TOS バイトによって表される、最大 4 つの Precedence 値を照合します。
- [Any Traffic]：すべてのトラフィックを照合します。

- [Add rule to existing traffic class]。すでに同じインターフェイスにサービス ポリシー ルールを指定している場合、またはグローバル サービス ポリシーを追加する場合は、このオプションによって既存のアクセス リストに ACE を追加できます。このインターフェイスのサービス ポリシー ルールで [Source and Destination IP Address (uses ACL)] オプションを選択した場合は、事前に作成したすべてのアクセス リストに ACE を追加できます。このトラフィック クラスでは、複数の ACE を追加する場合であっても、1 セットのルール アクションしか指定できません。この手順全体を繰り返すことによって、複数の ACE を同じトラフィック クラスに追加できます。ACE の順序の変更方法については、「サービス ポリシー ルールの順序の管理」（P.1-17）を参照してください。
- [Use an existing traffic class]。別のインターフェイスのルールで使用されるトラフィック クラスを作成した場合は、そのトラフィック クラス定義をこのルールで再使用できます。1 つのルールのトラフィック クラスを変更すると、その変更は同じトラフィック クラスを使用するすべてのルール

に継承されます。コンフィギュレーションに CLI で入力した **class-map** コマンドが含まれている場合は、それらのトラフィック クラス名も使用できます（ただし、そのトラフィック クラスの定義を表示するには、そのルールを作成する必要があります）。

- [Use class default as the traffic class]。このオプションでは、すべてのトラフィックを照合する class-default クラスを使用します。class-default クラスは、ASA によって自動的に作成され、ポリシーの最後に配置されます。このクラスは、アクションを何も適用しない場合でも ASA によって作成されますが、内部での使用に限られます。必要に応じて、このクラスにアクションを適用できます。これは、すべてのトラフィックを照合する新しいトラフィック クラスを作成するよりも便利な場合があります。class-default クラスを使用して、このサービス ポリシーにルールを 1 つだけ作成できます。これは、各トラフィック クラスを関連付けることができるのは、サービス ポリシーごとに 1 つのルールだけであるためです。

ステップ 5　[Next] をクリックします。

ステップ 6　次に表示されるダイアログボックスは、選択したトラフィック照合基準に応じて異なります。

（注）　[Any Traffic] オプションの場合には、追加設定を行うための特別なダイアログボックスはありません。

- [Default Inspections]：このダイアログボックスは情報提供の目的でだけ表示され、トラフィック クラスに含まれるアプリケーションとポートが示されます。
- [Source and Destination Address]：このダイアログボックスでは、送信元アドレスと宛先アドレスを設定できます。

  a. [Match] または [Do Not Match] をクリックします。

  [Match] オプションでは、アドレスが一致するトラフィックにアクションを適用する場合のルールを作成します。[Do Not Match] オプションでは、トラフィックを指定したアクションの適用から免除します。たとえば、10.1.1.25 を除いて、10.1.1.0/24 のトラフィックすべてを照合し、そのトラフィックに接続制限を適用するとします。この場合は、2 つのルール（[Match] オプションを使用した 10.1.1.0/24 に対するルールおよび [Do Not Match] オプションを使用した 10.1.1.25 に対するルール）を作成します。必ず、Do Not Match ルールが Match ルールの上になるように配置してください。順序を逆にすると、10.1.1.25 が最初に Match ルールを照合することになります。

  b. [Source] フィールドで、送信元 IP アドレスを入力するか、[...] ボタンをクリックして ASDM にすでに定義されている IP アドレスを選択します。

  プレフィックス / 長さ表記（10.1.1.0/24 など）を使用してアドレスとサブネット マスクを指定します。マスクを使用せずに IP アドレスを入力すると、そのアドレスは最後が 0 であってもホスト アドレスと見なされます。

  任意の送信元アドレスを指定するには、**any** を入力します。

  アドレスが複数ある場合はカンマで区切ります。

  c. [Destination] フィールドで、宛先 IP アドレスを入力するか、[...] ボタンをクリックして ASDM にすでに定義されている IP アドレスを選択します。

  プレフィックス / 長さ表記（10.1.1.0/24 など）を使用してアドレスとサブネット マスクを指定します。マスクを使用せずに IP アドレスを入力すると、そのアドレスは最後が 0 であってもホスト アドレスと見なされます。

  任意の宛先アドレスを指定するには、**any** を入力します。

  アドレスが複数ある場合はカンマで区切ります。

  d. [Service] フィールドで、宛先サービスの IP サービス名または番号を入力するか、[...] ボタンをクリックしてサービスを選択します。

TCP または UDP のポート番号、あるいは ICMP サービス番号を指定する場合は、*プロトコル / ポート*を入力します。たとえば、TCP/8080 と入力します。

デフォルトでは、サービスは IP です。

サービスが複数ある場合はカンマで区切ります。

e. （任意）[Description] フィールドに説明を入力します。

f. （任意）TCP または UDP の送信元サービスを指定するには、[More Options] 領域をクリックして開き、[Source Service] フィールドに TCP サービスまたは UDP サービスを入力します。

宛先サービスと送信元サービスは同じである必要があります。[Destination Service] フィールドをコピーし、[Source Service] フィールドに貼り付けます。

g. （任意）ルールを非アクティブにするには、[More Options] 領域をクリックして開き、[Enable Rule] をオフにします。

この設定は、ルールを削除せずに無効にしたい場合に便利です。

h. （任意）ルールの時間範囲を指定するには、[More Options] 領域をクリックして開き、[Time Range] ドロップダウン リストから時間範囲を選択します。

新しい時間範囲を追加するには、[...] ボタンをクリックします。詳細については、一般的な操作のコンフィギュレーション ガイドの “Configuring Time Ranges” section on page 15-26 を参照してください。

この設定は、事前に設定した時間にだけルールをアクティブにする場合に便利です。

- [Tunnel Group] : [Tunnel Group] ドロップダウン リストからトンネル グループを選択するか、または [New] をクリックして新しいトンネル グループを追加します。詳細については、VPN コンフィギュレーション ガイドの “Add or Edit an IPsec Remote Access Connection Profile” section on page 74-78 を参照してください。

  各フローをポリシングするには、[Match flow destination IP address] をオンにします。固有の IP 宛先アドレスに向かうトラフィックは、すべてフローと見なされます。

- [Destination Port] : [TCP] または [UDP] をクリックします。

  [Service] フィールドに、ポート番号または名前を入力するか、または [...] をクリックして ASDM で定義済みのサービスを選択します。

- [RTP Range] : RTP ポート範囲を 2000 ～ 65534 の間で入力します。範囲内の最大ポート数は、16383 です。

- [IP DiffServ CodePoints (DSCP)] : [DSCP Value to Add] 領域で、[Select Named DSCP Values] から値を選択するか、または [Enter DSCP Value (0-63)] フィールドに値を入力し、[Add] をクリックします。

  必要に応じて値を追加するか、または [Remove] ボタンを使用して値を削除します。

- [IP Precedence] : [Available IP Precedence] 領域で値を選択し、[Add] をクリックします。

  必要に応じて値を追加するか、または [Remove] ボタンを使用して値を削除します。

ステップ 7　[Next] をクリックします。

[Add Service Policy Rule - Rule Actions] ダイアログボックスが表示されます。

ステップ 8　1 つ以上のルール アクションを設定します。機能のリストについては、「サポートされる機能」（P.1-1）を参照してください。

ステップ 9　[Finish] をクリックします。

管理トラフィックのサービス ポリシー ルールの追加

管理目的でASAに転送されるトラフィックのサービス ポリシーを作成できます。詳細については、「サポートされる機能」（P.1-1）を参照してください。この項では、次のトピックについて取り上げます。

管理トラフィックのサービス ポリシー ルールの設定

管理トラフィックのサービス ポリシーを追加するには、次の手順を実行します。

ステップ 1　[Configuration] > [Firewall] > [Service Policy Rules] ペインで、[Add] の横の下矢印をクリックします。

ステップ 2　[Add Management Service Policy Rule] を選択します。

[Add Management Service Policy Rule Wizard - Service Policy] ダイアログボックスが表示されます。

ステップ 3　[Create a Service Policy and Apply To] 領域で、次のオプションの 1 つをクリックします。

- [Interface]。このオプションでは、サービス ポリシーが 1 つのインターフェイスに適用されます。インターフェイス サービス ポリシーは、特定の機能に対するグローバル サービス ポリシーより優先されます。たとえば、RADIUS アカウンティング インスペクションを使用するグローバル ポリシーと接続制限を使用するインターフェイス ポリシーがある場合、RADIUS アカウンティングと接続制限の両方がそのインターフェイスに適用されます。ただし、RADIUS アカウンティングを使用するグローバル ポリシーと RADIUS アカウンティングを使用するインターフェイス ポリシーがある場合、インターフェイス ポリシー RADIUS アカウンティングだけがそのインターフェイスに適用されます。
  a. ドロップダウン リストからインターフェイスを選択します。

     すでにポリシーが適用されているインターフェイスを選択する場合は、ウィザードの指示に従って、新しいサービス ポリシー ルールをそのインターフェイスに追加できます。
  b. 新しいサービス ポリシーの場合は、[Policy Name] フィールドに名前を入力します。
  c. （任意）[Description] フィールドに説明を入力します。
- [Global - applies to all interfaces]。このオプションでは、サービス ポリシーがすべてのインターフェイスにグローバルに適用されます。デフォルト アプリケーション インスペクションのサービス ポリシー ルールを含むグローバル ポリシーは、デフォルトで存在します。詳細については、「デフォルト設定」（P.1-7）を参照してください。ウィザードを使用してルールをグローバル ポリシーに追加できます。

ステップ 4　[Next] をクリックします。

[Add Management Service Policy Rule Wizard - Traffic Classification Criteria] ダイアログボックスが表示されます。

ステップ 5　次のオプションのいずれかをクリックして、ポリシーのアクションを適用するトラフィックを指定します。

- [Create a new traffic class]。[Create a new traffic class] フィールドにトラフィック クラス名を入力し、説明（任意）を入力します。

  基準のいずれかを使用してトラフィックを特定します。
  - [Source and Destination IP Address (uses ACL)]：このクラスは拡張アクセス リストで指定されているトラフィックを照合します。ASA がトランスペアレント ファイアウォール モードで動作している場合は、EtherType ACL を使用できます。

（注） このタイプの新しいトラフィック クラスを作成する場合は、最初にアクセス コントロール エントリ（ACE）を 1 つだけ指定できます。ルールを追加した後は、同じインターフェイスまたはグローバル ポリシーに新しいルールを追加し、それから [Traffic Classification] ダイアログボックス（以下を参照）で [Add rule to existing traffic class] を指定することによって、ACE を追加できます。

– [TCP or UDP Destination Port] : 1 つのポートまたは連続する一定範囲のポートを照合します。

ヒント 複数の非連続ポートを使用するアプリケーションの場合は、[Source and Destination IP Address (uses ACL)] を使用して各ポートを照合します。

- [Add rule to existing traffic class]。すでに同じインターフェイスにサービス ポリシー ルールを指定している場合、またはグローバル サービス ポリシーを追加する場合は、このオプションによって既存のアクセス リストに ACE を追加できます。このインターフェイスのサービス ポリシー ルールで [Source and Destination IP Address (uses ACL)] オプションを選択した場合は、事前に作成したすべてのアクセス リストに ACE を追加できます。このトラフィック クラスでは、複数の ACE を追加する場合であっても、1 セットのルール アクションしか指定できません。この手順全体を繰り返すことによって、複数の ACE を同じトラフィック クラスに追加できます。ACE の順序の変更方法については、「サービス ポリシー ルールの順序の管理」（P.1-17）を参照してください。
- [Use an existing traffic class]。別のインターフェイスのルールで使用されるトラフィック クラスを作成した場合は、そのトラフィック クラス定義をこのルールで再使用できます。1 つのルールのトラフィック クラスを変更すると、その変更は同じトラフィック クラスを使用するすべてのルールに継承されます。コンフィギュレーションに CLI で入力した **class-map** コマンドが含まれている場合は、それらのトラフィック クラス名も使用できます（ただし、そのトラフィック クラスの定義を表示するには、そのルールを作成する必要があります）。

ステップ 6　[Next] をクリックします。

ステップ 7　次に表示されるダイアログボックスは、選択したトラフィック照合基準に応じて異なります。

- [Source and Destination Address] : このダイアログボックスでは、送信元アドレスと宛先アドレスを設定できます。

  a. [Match] または [Do Not Match] をクリックします。

  [Match] オプションでは、アドレスが一致するトラフィックにアクションを適用する場合のルールを作成します。[Do Not Match] オプションでは、トラフィックを指定したアクションの適用から免除します。たとえば、10.1.1.25 を除いて、10.1.1.0/24 のトラフィックすべてを照合し、そのトラフィックに接続制限を適用するとします。この場合は、2 つのルール（[Match] オプションを使用した 10.1.1.0/24 に対するルールおよび [Do Not Match] オプションを使用した 10.1.1.25 に対するルール）を作成します。必ず、Do Not Match ルールが Match ルールの上になるように配置してください。順序を逆にすると、10.1.1.25 が最初に Match ルールを照合することになります。

  b. [Source] フィールドで、送信元 IP アドレスを入力するか、[...] ボタンをクリックして ASDM にすでに定義されている IP アドレスを選択します。

  プレフィックス / 長さ表記（10.1.1.0/24 など）を使用してアドレスとサブネット マスクを指定します。マスクを使用せずに IP アドレスを入力すると、そのアドレスは最後が 0 であってもホスト アドレスと見なされます。

  任意の送信元アドレスを指定するには、**any** を入力します。

  アドレスが複数ある場合はカンマで区切ります。

c. [Destination] フィールドで、宛先 IP アドレスを入力するか、[...] ボタンをクリックして ASDM にすでに定義されている IP アドレスを選択します。

プレフィックス / 長さ表記（10.1.1.0/24 など）を使用してアドレスとサブネット マスクを指定します。マスクを使用せずに IP アドレスを入力すると、そのアドレスは最後が 0 であってもホスト アドレスと見なされます。

任意の宛先アドレスを指定するには、**any** を入力します。

アドレスが複数ある場合はカンマで区切ります。

d. [Service] フィールドで、宛先サービスの IP サービス名または番号を入力するか、[...] ボタンをクリックしてサービスを選択します。

TCP または UDP のポート番号、あるいは ICMP サービス番号を指定する場合は、*プロトコル / ポート*を入力します。たとえば、TCP/8080 と入力します。

デフォルトでは、サービスは IP です。

サービスが複数ある場合はカンマで区切ります。

e. （任意）[Description] フィールドに説明を入力します。

f. （任意）TCP または UDP の送信元サービスを指定するには、[More Options] 領域をクリックして開き、[Source Service] フィールドに TCP サービスまたは UDP サービスを入力します。

宛先サービスと送信元サービスは同じである必要があります。[Destination Service] フィールドをコピーし、[Source Service] フィールドに貼り付けます。

g. （任意）ルールを非アクティブにするには、[More Options] 領域をクリックして開き、[Enable Rule] をオフにします。

この設定は、ルールを削除せずに無効にしたい場合に便利です。

h. （任意）ルールの時間範囲を指定するには、[More Options] 領域をクリックして開き、[Time Range] ドロップダウン リストから時間範囲を選択します。

新しい時間範囲を追加するには、[...] ボタンをクリックします。詳細については、一般的な操作のコンフィギュレーション ガイドの “Configuring Time Ranges” section on page 15-26 を参照してください。

この設定は、事前に設定した時間にだけルールをアクティブにする場合に便利です。

- [Destination Port] : [TCP] または [UDP] をクリックします。

  [Service] フィールドに、ポート番号または名前を入力するか、または [...] をクリックして ASDM で定義済みのサービスを選択します。

ステップ 8　[Next] をクリックします。

「Add Management Service Policy Rule - Rule Actions」ダイアログボックスが表示されます。

ステップ 9　RADIUS アカウンティング インスペクションを設定するには、[RADIUS Accounting Map] ドロップダウン リストからインスペクション マップを選択するか、または [Configure] をクリックしてマップを追加します。

詳細については、「サポートされる機能」（P.1-1）を参照してください。

ステップ 10　接続を設定するには、「接続の設定」（P.21-8）を参照してください。

ステップ 11　[Finish] をクリックします。

サービス ポリシー ルールの順序の管理

インターフェイス上またはグローバル ポリシー内でのサービス ポリシー ルールの順序は、トラフィックへのアクションの適用方法に影響します。パケットがサービス ポリシーのルールを照合する方法については、次のガイドラインを参照してください。

- パケットは、機能タイプごとにサービス ポリシーのルールを 1 つだけ照合できます。
- パケットが、1 つの機能タイプのアクションを含むルールを照合する場合、ASA は、その機能タイプを含む、後続のどのルールに対してもそのパケットを照合しません。
- ただし、そのパケットが異なる機能タイプの後続のルールを照合する場合、ASA は後続ルールのアクションも適用します。

たとえば、パケットが接続制限のルールを照合し、アプリケーション インスペクションのルールも照合する場合は、両方のアクションが適用されます。

パケットがアプリケーション インスペクションのルールを照合し、アプリケーション インスペクションを含む別のルールを照合する場合、2 番目のルール アクションは適用されません。

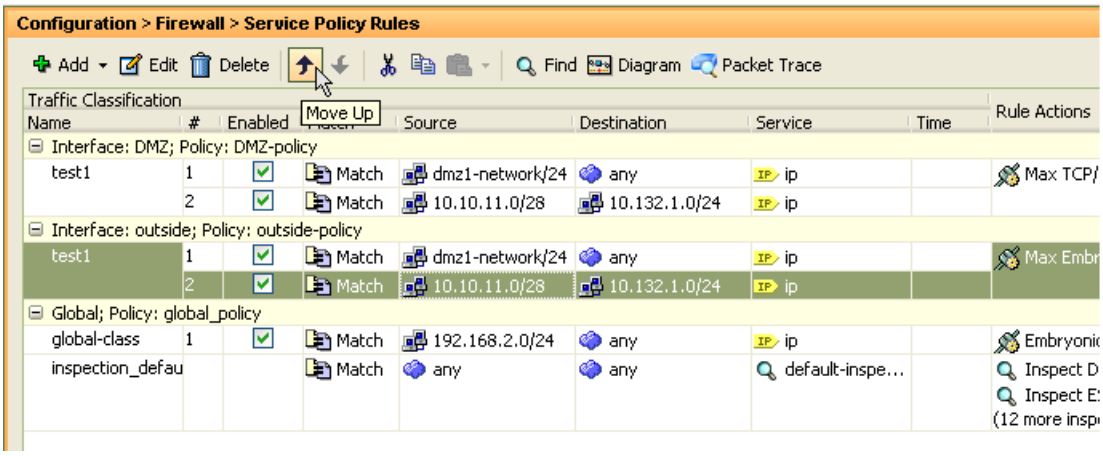
ルールに複数の ACE が組み込まれたアクセス リストが含まれる場合は、ACE の順序もパケット フローに影響します。ASA は、リストのエントリの順序に従って、各 ACE に対してパケットをテストします。一致が見つかると、ACE はそれ以上チェックされません。たとえば、すべてのトラフィックを明示的に許可する ACE を ACL の先頭に作成した場合は、残りのステートメントはチェックされません。

ルールまたはルール内での ACE の順序を変更するには、次の手順を実行します。

ステップ 1　[Configuration] > [Firewall] > [Service Policy Rules] ペインで、上または下に動かすルールまたは ACE を選択します。

ステップ 2　[Move Up] または [Move Down] カーソルをクリックします（図 1-1 を参照してください）。

図 1-1　ACE の移動



（注）　複数のサービス ポリシーで使用されるアクセス リストで ACE を並べ替えると、その変更はすべてのサービス ポリシーで継承されます。

ステップ 3　ルールまたは ACE を並べ替えたら、[Apply] をクリックします。

サービス ポリシーの機能履歴

表 1-3 に、この機能のリリース履歴の一覧を示します。

表 1-3　サービス ポリシーの機能履歴

機能名	リリース	機能情報
モジュラ ポリシー フレームワーク	7.0(1)	モジュラ ポリシー フレームワークが導入されました。
RADIUS アカウンティング トラフィックで使用する管理クラス マップ	7.2(1)	RADIUS アカウンティング トラフィックで使用する管理クラス マップが導入されました。**class-map type management** コマンドおよび **inspect radius-accounting** コマンドが導入されました。
インスペクション ポリシー マップ	7.2(1)	インスペクション ポリシー マップが導入されました。**class-map type inspect** コマンドが導入されました。
正規表現およびポリシー マップ	7.2(1)	インスペクション ポリシー マップで使用される正規表現およびポリシー マップが導入されました。**class-map type regex** コマンド、**regex** コマンド、および **match regex** コマンドが導入されました。
インスペクション ポリシー マップの match any	8.0(2)	インスペクション ポリシー マップで使用される **match any** キーワードが導入されました。トラフィックを 1 つ以上の基準に照合してクラス マップに一致させることができます。以前は、**match all** だけが使用可能でした。