ファイアウォール インスペクション ルールの管理

インスペクション ルールでは、デバイスに対するプロトコル インスペクションを設定します。インスペクションでは、アクセス ルールに一時的な穴を開けて、信頼ネットワーク内で開始された接続に対するリターン トラフィックを許可します。また、トラフィックが検査されるとき、デバイスでは、検査されるプロトコルに基づいて誤った形式のパケットを除外するための追加の制御も実装します。

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き PIX、FWSM、および IPS の機能をサポートしていますが、拡張機能はサポートしていません。

インスペクション ルールに対して生成されるデバイス コマンドは、デバイス タイプに応じて異なります。ASA、PIX 7.0+、および FWSM 3.x+ を実行しているデバイスでは、access-list、policy-map、class-map の各コマンドが使用されます。古い FWSM および PIX 6.3 デバイスでは、fixup コマンドが使用されます。IOS デバイスでは、ip-inspect コマンドが使用されます。

インスペクション ルールの使用方法については、次の項を参照してください。

- インスペクション ルールについて （1 ページ）
- インスペクション ルールの設定 （7 ページ）
- [Inspection Rules] ページ （10 ページ）
- インスペクションのプロトコルおよびマップの設定 （28 ページ）
- IOS デバイスのインスペクション ルールの設定 （152 ページ）

インスペクション ルールについて

インスペクション ルールでは、Context-Based Access Control（CBAC; コンテキストベース アクセス コントロール）インスペクション コマンドを設定します。CBAC では、デバイスを通過するトラフィックを検査して、TCP および UDP セッションの状態情報を検出および管理します。デバイスでは、この状態情報を使用して、許容できるセッションのリターン トラフィックおよび追加のデータ接続を許可するための一時的な穴を作成します。

CBAC では、ファイアウォール インターフェイスでアクセス リストに一時的な穴を作成します。これらの穴は、検査されるトラフィックがファイアウォールを通過して内部ネットワークから出るときに作成されます。リターン トラフィック（通常はブロックされます）と追加のデータ チャネルは、この穴からファイアウォールを通って内部ネットワークに入ることができます。トラフィックは、そのトラフィックがファイアウォールを通って出るときにインスペクションをトリガーした、元のトラフィックと同じセッションの一部となっている場合にだけ、ファイアウォールを通って戻ることができます。

インスペクション ルールは、アクセス ルールのあとに適用されるため、アクセス ルールで拒否したトラフィックは検査されません。トラフィックが検査されるようにするには、入力インターフェイスと出力インターフェイスの両方で、アクセス ルールによってトラフィックが許可される必要があります。アクセス ルールではレイヤ 3（ネットワーク、IP）または 4（トランスポート、TCP または UDP プロトコル）で接続を制御できますが、インスペクション ルールを使用すると、アプリケーション レイヤ プロトコル セッション情報を使用してトラフィックを制御できます。

すべてのプロトコルについて、プロトコルを検査するときに、デバイスによって次の機能が提供されます。

- トラフィックのリターン パスを自動的に開く（送信元アドレスと宛先アドレスを反転する）ため、リターン トラフィックを許可するアクセス ルールを作成する必要がない。各接続はセッションと見なされ、デバイスはセッション状態情報を保持し、有効なセッションのリターン トラフィックだけを許可します。TCP を使用するプロトコルには明示的なセッション情報が含まれますが、UDP アプリケーションでは、送信元および宛先アドレスと一連の UDP パケットの時間的な近さに基づき、デバイスがセッションと同等のものをモデル化します。

これらの一時的なアクセス リストは動的に作成され、セッションが終了するとき、削除されます。

- すべての TCP パケットのシーケンス番号を追跡し、想定範囲内にないシーケンス番号を持つパケットをドロップする。
- タイムアウトとしきい値を使用してセッション状態情報を管理することによって、完全には確立されていないセッションをいつドロップするかの判断に役立てる。セッションがドロップまたはリセットされると、デバイスは、セッションの送信元と宛先の両方に接続をリセットするよう通知して、リソースを解放し、Denial of Service（DoS; サービス拒絶）攻撃の可能性を低減します。

ここでは、インスペクションについて詳しく説明します。

- インスペクション ルールのインターフェイスの選択　（3 ページ）
- 検査するプロトコルの選択　（4 ページ）
- インスペクション ルールのアクセス ルール要件について　（5 ページ）
- IOS デバイスでの Denial of Service（DoS; サービス拒絶）攻撃を防ぐためのインスペクションの使用　（6 ページ）

• インスペクションのプロトコルおよびマップの設定 （28 ページ）
• インスペクション ルールの設定 （7 ページ）
• IOS デバイスのインスペクション ルールの設定 （152 ページ）

インスペクション ルールのインターフェイスの選択

内部ネットワークを保護するインスペクションをデバイスに設定します。TCP、UDP、またはその他の特定のプロトコルとともに使用します。トラフィックセッションがデバイスの特定の側から（通常は、保護されている内部ネットワークから）開始された場合にだけ、アプリケーションのトラフィックがデバイスを通過できるようにするには、これらのアプリケーションを検査します。

ヒント IOSデバイスでは、インスペクションを明示的に設定する必要があり、検査するトラフィックの方向を指定できます。ASA、PIX、および FWSM の各デバイスでは、方向を指定できず、インスペクションを設定する必要があるのはインスペクションのデフォルトを使用しない場合だけです。以降の説明では、方向に関する文は IOS デバイスにだけ適用されます。ASA、PIX、および FWSM では、単純に指定されたインターフェイスにインスペクションを設定します。

多くの場合、単一のインターフェイスで一方向にだけインスペクションを設定します。これにより、トラフィックは許容される（有効、既存）セッションに属する場合にだけ内部ネットワークに戻ることができます。これは、インターネット上で発生したトラフィックから内部ネットワークを保護するための一般的な設定です。

1 つ以上のインターフェイスで、双方向のインスペクションを設定することもできます。エクストラネット設定やイントラネット設定などを使用して、ファイアウォールの両側のネットワークを保護する必要がある場合、および DoS 攻撃から保護する場合に、双方向のインスペクションを設定します。たとえば、デバイスが 2 つのパートナー企業のネットワークの間にある場合は、特定のアプリケーションに対してトラフィックを一方向に制限し、他のアプリケーションに対してトラフィックを反対方向に制限することが必要となることがあります。DMZ ゾーン内の Web サーバを保護している場合は、HTTP トラフィックに詳細なインスペクションを設定して、望ましくない特性を持つ接続を識別し、リセットすることが必要となることがあります。

インターネットまたは別の制御対象外ネットワークに接続するネットワークのアウトバウンドインターフェイスにインスペクション ルールを設定する一方で、信頼ネットワーク内ではフィルタリングされない接続を許可することが必要となる場合があります。このため、デバイスでは、保護されていないことによって潜在的な危険性のあるネットワーク上を移動するセッションにだけ、インスペクションのリソースが使用されます。

関連項目

• 検査するプロトコルの選択 （4 ページ）

- インスペクション ルールのアクセス ルール要件について （5 ページ）
- IOS デバイスでの Denial of Service（DoS; サービス拒絶）攻撃を防ぐためのインスペクションの使用 （6 ページ）
- インスペクションのプロトコルおよびマップの設定 （28 ページ）
- インスペクション ルールの設定 （7 ページ）

検査するプロトコルの選択

TCP および UDP は汎用的に検査できます。これにより、これらのプロトコルを使用するすべてのアプリケーションがカバーされます。ただし、より特定的なプロトコルを検査することもできます。場合によっては、特定のプロトコルの検査によって、汎用的な TCP/UDP インスペクションよりも優れたサービスが提供されることがあります。TCP および UDP のインスペクションでは、アプリケーション固有のコマンドが認識されないため、あるアプリケーションのすべてのリターン パケットが許可されないことがあります。特に、リターン パケットのポート番号が前の既存パケットとは異なる場合は、その可能性が高くなります。

次に例を示します。

- 一部のプロトコルでは、詳細なインスペクションを設定できる。詳細なインスペクションでは、トラフィック ストリームに対して、より具体的なルールを設定できます。たとえば、要求および応答のコンテンツ タイプが一致しない HTTP 接続をドロップできます。詳細なインスペクションと設定オプションについては、インスペクションのプロトコルおよびマップの設定 （28 ページ）を参照してください。
- FTP など、リターン チャネルをネゴシエーションするプロトコルは、明示的に検査する必要がある。FTP トラフィックの単純な汎用 TCP インスペクションを使用する場合は、ネゴシエーションされたチャネルは開かれず、接続が失敗します。FTP を許可する場合は、FTP 用の明示的なインスペクション ルールを作成してください。

また、マルチメディア プロトコルもリターン チャネルをネゴシエーションするため、明示的に検査する必要があります。これらのプロトコルには、H.323、Real Time Streaming Protocol（RTSP; リアルタイム ストリーミング プロトコル）、およびその他のアプリケーション固有のプロトコルが含まれます。一部のアプリケーションでは汎用 TCP チャネルも使用するため、汎用 TCP インスペクションも設定する必要があります。汎用的な TCP インスペクション ルールは、テーブル内でより明示的なインスペクション ルールよりも下にある必要があります（つまり、TCP または UDP を指定するルールは、すべて、インスペクション ルール テーブルの最後にある必要があります）。

関連項目

- インスペクション ルールのインターフェイスの選択 （3 ページ）
- インスペクション ルールのアクセス ルール要件について （5 ページ）
- IOS デバイスでの Denial of Service（DoS; サービス拒絶）攻撃を防ぐためのインスペクションの使用 （6 ページ）

• インスペクション ルールの設定 （7 ページ）

インスペクション ルールのアクセス ルール要件について

アクセス ルールは、インスペクション ルールよりも前に適用されます。このため、検査するトラフィックがアクセス ルールで禁止されないようにする必要があります。次の注意事項に従ってください。

- 検査したトラフィックがファイアウォールを通過してネットワークから出ることを許可する。

検査されるトラフィックは、保護ネットワークから出るトラフィックを評価する、すべてのアクセス ルールで許可される必要があります。たとえば、Telnet が検査される場合、Telnet トラフィックは、ネットワークから出るトラフィックに適用されるすべてのアクセスルールで許可される必要があります。

- 検査されるリターン トラフィックがファイアウォールを通過してネットワークに入ることを拒否する。

アクセス リストに一時的な穴を作成する場合、アクセス リストでは、検査されるリターン トラフィックを拒否する必要があります。これは、インスペクション エンジンによって、このトラフィックのアクセス リストに一時的な穴が開けられるためです（通常、ネットワークに入るトラフィックはブロックされるようにします）。

- ネットワークでの必要性に応じて、検査できないトラフィック、または検査する必要のないトラフィックを許可または拒否する。

たとえば、ICMP トラフィックを検査しないで、一部の ICMP トラフィックを許可する場合は、両方向のトラフィックが許可されるようにアクセス ルールを設定します。少なくとも、（ping コマンドに対する）echo reply、（トレース ルートに対する）time-exceeded、（パス MTU ディスカバリに対する）packet-too-big、（トレース ルートに対する）traceroute、および（ホストが見つからないことを通知する）unreachable の ICMP メッセージ タイプを許可することを検討します。

- 保護ネットワーク上のアドレスと一致する送信元アドレスからのすべてのネットワーク トラフィックを拒否するアクセス ルール エントリを追加する。

この方法は、保護されていないネットワークからのトラフィックが、保護ネットワーク上のデバイスの識別情報を偽って使用することを防ぐため、アンチ スプーフィング保護と呼ばれます。

- 送信元アドレスが 255.255.255.255 のブロードキャスト メッセージを拒否するエントリを追加する。

このエントリは、ブロードキャスト攻撃を防ぐのに役立ちます。

関連項目

- アクセス ルールについて
- インスペクション ルールのインターフェイスの選択 （3 ページ）
- 検査するプロトコルの選択 （4 ページ）
- インスペクション ルールの設定 （7 ページ）

IOS デバイスでの Denial of Service（DoS; サービス拒絶）攻撃を防ぐためのインスペクションの使用

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き PIX、FWSM、および IPS の機能をサポートしていますが、拡張機能はサポートしていません。

アプリケーション層でパケットを検査すること、および TCP セッション情報と UDP セッション情報を保持することによって、デバイスは、SYN フラッディングなどの特定のタイプのネットワーク攻撃を検出および回避できます。SYN フラッド攻撃は、ネットワーク攻撃者がサーバに膨大な数の接続要求をフラッドし、接続を完了しないことによって発生します。これにより、ハーフオープン接続が大量に発生してサーバが処理しきれなくなり、有効な要求へのサービスが拒否されます。ネットワーク デバイスへのアクセスを拒否するネットワーク攻撃を、Denial-of-Service（DoS; サービス拒絶）攻撃と呼びます。

インスペクションは、他の方法で DoS 攻撃から保護するのに役立ちます。インスペクションは、TCP 接続のパケット シーケンス番号を参照し、それらが想定範囲内にあるかどうかを確認して、すべての疑わしいパケットをドロップします。また、ハーフオープン接続をドロップするインスペクション設定をすることもできます。このことを行うには、ファイアウォール処理とメモリ リソースの維持が必要です。これ以外に、インスペクションでは、新しい接続で頻繁に発生するエラーを検出してアラート メッセージを発行できます。

IOS デバイスでは、複数のインスペクション設定パラメータを設定して、SYN フラッディングとハーフオープン接続からの保護を微調整できます。**[ファイアウォール（Firewall）] > [設定（Settings）] > [検査（Inspection）]** ポリシーを設定します。各設定の詳細については、IOS デバイスのインスペクション ルールの設定 （152 ページ）を参照してください。

インスペクションは、フラグメント化された IP パケットに関連する特定の DoS 攻撃からも保護できます。ファイアウォールは攻撃者が特定のホストに実際に接続することを防ぎますが、攻撃者はそのホストによって提供されるサービスを中断させることがあります。このことは、多くの非初期 IP フラグメントを送信するか、または、フラグメント化されたパケットの最初のフラグメントをフィルタする ACL を持つルータを経由して、完全にフラグメント化されたパケットを送信することによって行われます。ターゲット ホストでは不完全なパケットを再構成しようとし、これにより、これらのフラグメントによって、ターゲット ホスト上のリソースが占有されます。フラグメント インスペクションを微調整するには、**フラグメント**プロトコル

のインスペクションルールを設定し、許可するフラグメントの最大数とタイムアウト値を設定します。

関連項目

- インスペクション ルールについて （1 ページ）
- 検査するプロトコルの選択 （4 ページ）
- インスペクションのプロトコルおよびマップの設定 （28 ページ）
- インスペクション ルールの設定 （7 ページ）

インスペクション ルールの設定

インスペクション ルール ポリシーは、インターフェイスを通じて検査されるトラフィックを識別します。インスペクションでは、許可されるセッションを追跡し、リターン トラフィックを許可するために、アクセス ルールに一時的な穴を開けます。

インスペクション ルールはアクセス ルールよりもあとに処理されるため、アクセス ルールでドロップされたトラフィックは検査されません。拒否ルールを使用して、特定のタイプのトラフィックを検査から選択的に除外することもできます。たとえば、他のすべての DNS トラフィックが検査されているときに、特定のクラスの DNS トラフィックが検査されないようにする検査拒否ルールを作成できます。基本的な手順は次のとおりです。

- 特定のプロトコルのデフォルトの検査ルールの前に、新しい拒否ルールを追加します。[トラフィックの照合基準（Match Traffic By）] オプションで、[送信元と宛先のアドレスおよびポート（Source and Destination Address and Port）] を選択します。次に、送信元と宛先のネットワーク IP アドレスを指定し、目的のサービスタイプ（DNS-TCP など）を選択して、特定のタイプのトラフィックを定義します。最後に、検査ルールウィザードの 3 番目の画面で、適切なプロトコル（DNS など）を選択します。
- 次に、デフォルトの検査ルールを編集します（表の新しい拒否ルールの下）。[トラフィックの照合基準（Match Traffic By）] オプションで [送信元と宛先のアドレスおよびポート（Source and Destination Address and Port）] を再度選択します。これが許可ルールであることを確認し、送信元アドレスと宛先アドレスとして all-addresses オプションを指定し、サービスタイプとして IP を入力します。3 番目の画面では、選択したプロトコルを保持します。必要に応じて、関連するマップを設定または削除します。

この手順とプロセスに関する詳細情報については、 [Inspection Rules] ページ （10 ページ）および Add Inspect/Application FW Rule ウィザードまたは Edit Inspect/Application FW Rule ウィザード （15 ページ）を参照してください。

インスペクションルールを作成するときに検討する必要のある事項の詳細については、次の各項を参照してください。

- インスペクション ルールについて （1 ページ）
- インスペクション ルールのインターフェイスの選択 （3 ページ）

- 検査するプロトコルの選択 （4 ページ）
- インスペクション ルールのアクセス ルール要件について （5 ページ）
- IOS デバイスでの Denial of Service（DoS; サービス拒絶）攻撃を防ぐためのインスペクションの使用 （6 ページ）
- インスペクションのプロトコルおよびマップの設定 （28 ページ）
- マップ オブジェクトについて

はじめる前に

あるインスペクション ルールの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インスペクション 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。

ステップ 1 次のいずれかを実行して、 [Inspection Rules] ページ （10 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）] > [インスペクション ルール（Inspection 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）] > [インスペクション ルール（Inspection 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 Inspect/Application FW Rule ウィザードまたは Edit Inspect/Application FW Rule ウィザード （15 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、ルールの編集を参照してください。

ステップ 3 ルールをデバイスのすべてのインターフェイスに適用するか、指定したインターフェイスにだけ適用するかを選択します。

インターフェイスを指定することを選択した場合は、インターフェイス名またはインターフェイス ロールを入力するか、[選択（Select）] をクリックしてリストから選択します。また、IOS デバイスの場合は、ルールを出力方向（インターフェイスから出るトラフィック）に適用するかどうかも選択できます。他のすべてのデバイス タイプには入力方向を使用します。

ステップ 4 トラフィックのマッチングに使用する基準を選択します。この基準により、このルールに基づいて検査される対象が決まります。

- [デフォルト プロトコル ポート（Default Protocol Ports）]：このオプションは、検査しているプロトコルでネットワークのデフォルト ポートが使用されている場合に選択します。

送信元アドレスまたは宛先アドレスに基づいてインスペクションを制約する場合は、[[送信元と宛先のIPアドレス間で検査を制限する（Limit inspection between source and destination IP addresses）] も選択します（ASA、PIX 7.x+、および FWSM 3.x+ デバイスでだけ使用できます）。[次へ（Next）] をクリックすると、送信元アドレスと宛先アドレスの入力を求められます。他の値を設定することだけが目的である場合は、送信元またはアドレスに [任意（any）] を指定できます。

- [カスタム宛先ポート（Custom Destination Ports）]：このオプションは、追加のデフォルト以外の TCP または UDP ポートを特定のプロトコルに関連付ける場合（たとえば、宛先ポート 8080 上の TCP トラフィックを HTTP トラフィックとして扱う場合）に選択します。[次へ（Next）] をクリックすると、ポートまたはポート範囲の入力を求められます。
- [宛先アドレスとポート（Destination Address and Port）]（IOS デバイスのみ）：このオプションは、トラフィックが特定の宛先に向かっている場合にだけ、デフォルト以外の追加の TCP または UDP ポートを特定のプロトコルに関連付ける場合（たとえば、トラフィックが 192.168.1.10 に向かっている場合にだけ、宛先ポート 8080 上のトラフィックを HTTP として扱う場合）に選択します。[次へ（Next）] をクリックすると、宛先アドレスとポート情報の入力を求められます。
- [送信元と宛先のアドレスおよびポート（Source and Destination Address and Port）]（PIX 7.x+、ASA、FWSM 3.x+）：このオプションは、IOS デバイスで [宛先アドレスとポート（Destination Address and Port）] を選択するのと同じ理由で選択しますが、トラフィックの送信元を識別する追加オプションがあります。[次へ（Next）] をクリックすると、送信元アドレス、宛先アドレス、およびサービスポート情報の入力を求められます。

（注） FWSM 2.x および PIX 6.3(x) の場合は、[Default Inspection Traffic] または [Custom Destination Ports] だけを選択できます。

ステップ 5 [次へ（Next）] をクリックします。[デフォルトプロトコルポート（Default Protocol Ports）] 以外のオプションを選択した場合は、上記で説明した必要なアドレッシングとポート情報を入力し、[次へ（Next）] をクリックします。[検査/アプリケーション FW ルールの追加または編集（Add or Edit Inspect/Application FW Rule）] ウィザード、ステップ 2 （18 ページ）を参照してください。

ステップ 6 [検査/アプリケーションFWルールの追加または編集（Add or Edit Inspect/Application FW Rule）] ウィザード、[検査対象プロトコル（Inspected Protocol）] ページ （22 ページ）で、検査するプロトコルをリストから選択します。ルールを割り当てているデバイスでそのプロトコルのインスペクションがサポートされていることが [Device Type] フィールドに示されていることを確認します（サポートされていないデバイス タイプにルールを割り当てた場合、ルールは無視されますが、検証の警告が生成されます）。

選択したプロトコルで追加設定が許可されている場合は、[設定（Configure）] ボタンがアクティブになります。このボタンをクリックして、オプションを選択します。詳細については、インスペクションのプロトコルおよびマップの設定 （28 ページ）を参照してください。

IOS デバイスのみ：

- トラフィックの一致基準として [カスタム宛先ポート（Custom Destination Ports）] または [宛先アドレスとポート（Destination Address and Port）] を選択した場合は、プロトコル名として [カスタムプロトコル（custom protocol）] を選択し、[設定（Configure）] をクリックして設定に名前を割り当てることができる。
- インスペクション設定ポリシーで設定された値を上書きする追加のアラート、監査、およびタイムアウトを設定できる。また、限られた数のプロトコルに対して、ルータによって設定されたトラフィッ

クを検査するかどうかも指定できます。インスペクション設定の詳細については、IOS デバイスのインスペクション ルールの設定 （152 ページ）を参照してください。

ステップ 7 [終了（Finish）] をクリックしてルールを保存します。

ステップ 8 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。

次のタスク

ASA 9.9.1 以降、Security Gateway 機能が有効になっているクラスタモードのデバイスでは、次の集中検査のリストが無効になっています。

- DCERPC
- NetBIOS
- PPTP
- RADIUS
- RSH
- SUNRPC
- TFTP
- XDMCP

プレビューの設定中に、サポートされていないデバイスに対して検査ルールが設定されている場合、検証エラーが表示されます。

（注） デバイスのロールバックがある場合、デフォルトの DNS ポリシーマップ設定がデバイスに自動的に追加されます。したがって、Cisco Security Manager がデバイスのロールバックを処理した後、デバイスが再検出されると、デフォルトの dns-policy-map 設定が Cisco Security Manager で検出されます。

[Inspection Rules] ページ

[Inspection Rules] ページを使用して、デバイス インターフェイスのインスペクション ルールを設定します。インスペクションでは、デバイスを通過するトラフィックを調べて、TCP および UDP セッションの状態情報を検出および管理します。デバイスでは、この状態情報を使用して、許容できるセッションのリターン トラフィックおよび追加のデータ接続を許可するための一時的な穴を作成します。

（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 インスペクション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」されています。つまり、IPv4 または IPv6 アドレス、あるいは両方のアドレスを合わせて使用できる一組のインスペクション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、IPv4 および統合バージョンのインスペクション ポリシー タイプが提供されています。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用意されています（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、インスペクション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 インスペクション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、割り当てた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、統合インスペクション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、割り当てた共有ポリシーの 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ません。

インスペクションルールは、アクセスルールのあとに処理されます。このため、アクセスルールで拒否されたトラフィックは検査されません。

インスペクション ルールを設定する前に、次の項を読んでください。

- インスペクション ルールについて （1 ページ）
- インスペクション ルールのインターフェイスの選択 （3 ページ）
- 検査するプロトコルの選択 （4 ページ）
- インスペクション ルールのアクセス ルール要件について （5 ページ）
- IOS デバイスでの Denial of Service（DoS; サービス拒絶）攻撃を防ぐためのインスペクションの使用 （6 ページ）
- インスペクション ルールの設定 （7 ページ）

ヒント ディセーブルなルールには、テーブルの行にハッシュ 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。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

[Inspection Rules] ページにアクセスするには、次のいずれかを実行します。

- （デバイスビュー）デバイスを選択してから、ポリシーセレクタで **[ファイアウォール（Firewall）] > [インスペクションルール（Inspection 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）] > [インスペクションルール（Inspection 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）] > [インスペクションルール（Inspection Rules）] を選択します。

関連項目

- 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

表 *1 : [Inspection Rules]* ページ

要素	説明
すべての行を展開する/すべての行を折りたたむ（Expand all rows/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） 各ボタンは、インスペクション 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。
競合インジケータアイコン（Conflict Indicator icons）	競合を識別し、競合の種類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、自動競合検出について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、検査する必要のあるトラフィックがルールによって識別されるかどうか。 • [Permit]：検査するトラフィックを特定します。緑色のチェックマークとして表示されます。 • [Deny]：トラフィックを検査から免除します。トラフィックが許可されるかブロックされるかは、アクセスルールによって決定されます。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のソース。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。
Traffic Match	ルールで使用される一致のタイプ。 • [default-inspection]：ルールにより、デフォルトポートに基づいてトラフィックが検査されます。 • [TCP、UDP/ポート番号（TCP,UDP/port number）]：ルールにより、カスタムポート番号に基づいてトラフィックが検査されます。 • [Service]：ルールでは、サービスの仕様またはサービス オブジェクトに基づいてトラフィックが検査されます。複数のエントリがある場合は、テーブルセル内に個別のサブフィールドとして表示されます。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。
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。[グローバル（Global）] は、ルールがすべてのインターフェイスに割り当てられていることを示します。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。複数のエントリがある場合は、テーブル セル内に個別のサブフィールドとして表示されます。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。
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。
Inspected Protocol	検査されるプロトコル。場合によってはプロトコルの設定の一部。このセルを右クリックし、[検査済みプロトコルの編集（Edit Inspected Protocol）] を選択してプロトコルを編集できます。詳細については、[検査/アプリケーションFWルールの追加または編集（Add or Edit Inspect/Application FW Rule）] ウィザード、[検査対象プロトコル（Inspected Protocol）] ページ （22 ページ）を参照してください。
時間範囲	ルールに割り当てられている時間範囲ポリシー オブジェクト。このオブジェクトでは、インスペクションが行われる時間枠を定義します。

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。
説明	ルールの説明（ある場合）。
最後のチケット（Last Ticket(s)）	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	
クエリ	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。
[Add Row] ボタン	Add Inspect/Application FW Rule ウィザードまたは Edit Inspect/Application FW Rule ウィザード （15 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。

Add Inspect/Application FW Rule ウィザードまたは Edit Inspect/Application FW Rule ウィザード

Add Inspect/Application FW Rule ウィザードまたは Edit Inspect/Application FW Rule ウィザードを使用して、インスペクション ルールを追加および編集します。ウィザードでは、このページの [トラフィック一致基準（Match Traffic By）] グループでの選択に基づいてインスペクション ルールを設定するプロセスの手順が示されます。

インスペクション ルールを設定する前に、次の項を読んでください。

- インスペクション ルールについて （1 ページ）
- インスペクション ルールのインターフェイスの選択 （3 ページ）
- 検査するプロトコルの選択 （4 ページ）
- インスペクション ルールのアクセス ルール要件について （5 ページ）
- IOS デバイスでの Denial of Service（DoS; サービス拒絶）攻撃を防ぐためのインスペクションの使用 （6 ページ）
- インスペクション ルールの設定 （7 ページ）

ナビゲーション パス

[Inspection Rules] ページ （10 ページ）から、[列の追加（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。

関連項目

- [検査/アプリケーション FW ルールの追加または編集（Add or Edit Inspect/Application FW Rule）] ウィザード、ステップ 2 （18 ページ）
- [検査/アプリケーションFWルールの追加または編集（Add or Edit Inspect/Application FW Rule）] ウィザード、[検査対象プロトコル（Inspected Protocol）] ページ （22 ページ）
- インターフェイス ロール オブジェクトについて
- ルールの編集

フィールド リファレンス

表 *2 : Add Inspect/Application FW Rule* ウィザードまたは *Edit Inspect/Application FW Rule* ウィザードの手順 *1*：トラフィック一致方式

要素	説明
ルールの有効化（Enable Rule）	ルールをイネーブルにするかどうか。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。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。
Apply the Rule to	ルールが適用されるインターフェイス。 • [All Interfaces]：ルールをすべてのインターフェイスに適用します。ルールは、ASA、PIX、およびFWSMデバイスでグローバルルールになります。IOSデバイスの場合は、各インターフェイスに対してルールが入力方向に設定されます。 • [Interface (PIX 7.x+, ASA, FWSM 3.x+, IOS)] - [Interfaces] フィールドで指定されたインターフェイスにだけルールを適用します。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するか、[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インターフェイスロールを選択するか、あるい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。 IOSデバイスの場合にのみ、このルールが適用されるトラフィックの方向（インターフェイスに入るトラフィック（[In]）またはインターフェイスから出るトラフィック（[Out]））を選択します。その他のデバイスの場合は、方向を [In] のままにします。
Match Traffic By 検査するトラフィックを識別する方法。デフォルトのプロトコルポート（単独）以外を選択した場合、[次へ（Next）] をクリックすると、他のポートまたはアドレス情報の入力を求められます。	

要素	説明
Default Protocol Ports Limit inspection between source and destination IP addresses（PIX 7.x+、ASA、FWSM 3.x+）	プロトコルに割り当てられているデフォルト ポートに基づいてトラフィックを検査します。次のページ（[検査/アプリケーションFWルールの追加または編集（Add or Edit Inspect/Application FW Rule）] ウィザード、[検査対象プロトコル（Inspected Protocol）] ページ （22 ページ））でプロトコルを選択します。 また、[送信元と宛先の IP アドレス間で検査を制限する（Limit inspection between source and destination IP addresses）] を選択して、指定した送信元と宛先間でのみ検査を実行するように設定できます。検査するトラフィックに制約を適用しないでプロトコルを検査する場合は、このオプションを選択しないでください。 このオプションも選択した場合、ウィザードの次のページの説明については、[検査/アプリケーション FW ルールの追加または編集（Add or Edit Inspect/Application FW Rule）] ウィザード、ステップ 2 （18 ページ）を参照してください。
Custom Destination Ports	指定したデフォルト以外の TCP または UDP 宛先ポートに基づいてトラフィックを検査します。このオプションは、追加の TCP または UDP トラフィックを特定のプロトコルに関連付ける場合（たとえば、宛先ポート 8080 上の TCP トラフィックを HTTP トラフィックとして扱う場合）に選択します。 ウィザードの次のページでプロトコルとポートを指定します。[検査/アプリケーション FW ルールの追加または編集（Add or Edit Inspect/Application FW Rule）] ウィザード、ステップ 2 （18 ページ）を参照してください。
宛先アドレスとポート（IOSデバイスのみ）（Destination Address and Port (IOS devices only)）	宛先 IP アドレスとポートに基づいて IOS デバイス上のトラフィックを検査します。このオプションは、トラフィックが特定の宛先に向かっている場合にだけ、デフォルト以外の追加の TCP または UDP ポートを特定のプロトコルに関連付ける場合（たとえば、トラフィックが 192.168.1.10 に向かっている場合にだけ、宛先ポート 8080 上のトラフィックを HTTP として扱う場合）に選択します。
Source and Destination Address and Port（PIX 7.x、ASA、FWSM 3.x）	送信元と宛先の IP アドレスとサービスに基づいて、PIX 7.x+、ASA、および FWSM 3.x+ デバイス上のトラフィックを検査します。このオプションは、IOS デバイスで [Destination Address and Port] を選択するのと同じ理由で選択しますが、トラフィックの送信元を識別する追加オプションがあります。 ウィザードの次のページで、アクション、送信元、宛先、およびサービスを指定します。[検査/アプリケーション FW ルールの追加または編集（Add or Edit Inspect/Application FW Rule）] ウィザード、ステップ 2 （18 ページ）を参照してください。

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。
説明	オプションで入力するルールの説明（最大 1024 文字）。

[検査/アプリケーション FW ルールの追加または編集（Add or Edit Inspect/Application FW Rule）] ウィザード、ステップ 2

[検査/アプリケーション FW ルール（Inspect/Application FW Rule）] ウィザードの 2 ページ目に表示されるオプションは、最初のページでの [トラフィック照合基準（Match Traffic By）] の選択によって異なります（Add Inspect/Application FW Rule ウィザードまたは Edit Inspect/Application FW Rule ウィザード （15 ページ）を参照）。表示されるオプションは、次のとおりです。

- 最初のページで [デフォルトプロトコルポート（Default Protocol Ports）] を選択し、[送信元と宛先の IP アドレス間で検査を制限する（Limit inspection between source and destination IP addresses）] を選択しない場合、2 ページ目は [検査/アプリケーションFWルールの追加または編集（Add or Edit Inspect/Application FW Rule）] ウィザード、[検査対象プロトコル（Inspected Protocol）] ページ （22 ページ）で説明されているオプションで構成されます。
- 最初のページで [デフォルトプロトコルポート（Default Protocol Ports）] を選択し、[送信元と宛先の IP アドレス間で検査を制限する（Limit inspection between source and destination IP addresses）] を選択する場合、このセクションにある 2 つ目の表で説明されているオプションで構成されます（3 ページ目は、[検査/アプリケーションFWルールの追加または編集（Add or Edit Inspect/Application FW Rule）] ウィザード、[検査対象プロトコル（Inspected Protocol）] ページ （22 ページ）で説明されているオプションで構成されます）。
- 最初のページで [カスタム宛先ポート（Custom Destination Ports）] を選択する場合、2 ページ目は、このセクションにある最初の表で説明されているオプションで構成されます（3 ページ目は、[検査/アプリケーションFWルールの追加または編集（Add or Edit Inspect/Application FW Rule）] ウィザード、[検査対象プロトコル（Inspected Protocol）] ページ （22 ページ）で説明されているオプションで構成されます）。
- 最初のページで [送信元と宛先のアドレスおよびポート（Source and Destination Address and Port）] を選択する場合、2 ページ目は、このセクションにある 2 つ目の表で説明されているオプションで構成されます（3 ページ目は、[検査/アプリケーションFWルールの追加または編集（Add or Edit Inspect/Application FW Rule）] ウィザード、[検査対象プロトコル（Inspected Protocol）] ページ （22 ページ）で説明されているオプションで構成されます）。

ナビゲーション パス

Add Inspect/Application FW Rule ウィザードまたは Edit Inspect/Application FW Rule ウィザード（15 ページ）から、[トラフィック照合基準（Match Traffic By）] オプションを選択し、[次へ（Next）] をクリックします。

関連項目

- インスペクション ルールについて （1 ページ）
- インスペクション ルールのインターフェイスの選択 （3 ページ）
- 検査するプロトコルの選択 （4 ページ）
- インスペクション ルールのアクセス ルール要件について （5 ページ）
- IOS デバイスでの Denial of Service（DoS; サービス拒絶）攻撃を防ぐためのインスペクションの使用 （6 ページ）
- インスペクション ルールの設定 （7 ページ）
- インターフェイス ロール オブジェクトについて
- ルールの編集

フィールド リファレンス

次の表では、ウィザードの最初のページで [カスタム宛先ポート（Custom Destination Ports）] を選択した後に [検査/アプリケーション FW ルール（Inspect/Application FW Rule）] ウィザードの 2 ページ目に表示されるオプションについて説明します（ Add Inspect/Application FW Rule ウィザードまたは Edit Inspect/Application FW Rule ウィザード （15 ページ）を参照）。

表 *3 : [*検査/アプリケーション *FW* ルールの追加および編集（*Add or Edit Inspect/Application FW Rule*）*]* ウィザードのステップ *2* : *[*プロトコルおよびポート（*Protocol and Port*）*]* ページ

要素	説明
プロトコル	指定しているポートのプロトコル（TCP、UDP、または TCP/UDP）。 IOS デバイスに対して [Custom Destination Ports] を設定している場合は、TCP/UDP を選択する必要があります。

要素	説明
ポート	検査するトラフィックで使用されるポート。有効値の範囲は 1 ～ 65535 です。 • [Single]：ポート番号を 1 つだけ指定します。 • [Range]：10000-11000 など、ポートの範囲を指定します。 カスタム ポートを設定する場合、一部のプラットフォームまたは OS バージョンではポート範囲がサポートされないことに注意してください。すべての競合は、このルールを編集しているときではなく、ポリシーの検証中に識別されます。 **ヒント** 定義済みのポート マッピングと競合するポートまたはポート範囲を指定した場合は、デバイスでポートの再マッピングが許可されません。

次の表では、ウィザードの最初のページで [デフォルトプロトコルポート（Default Protocol Ports）] と [送信元と宛先の IP アドレス間で検査を制限する（Limit inspection between source and destination IP addresses）] を選択し、[送信元と宛先のアドレス（Source and Destination Address）] を選択した場合に、[検査/アプリケーション FW ルール（Inspect/Application FW Rule）] ウィザードの 2 ページ目に表示されるオプションについて説明します。ウィザードの最初のページについては、Add Inspect/Application FW Rule ウィザードまたは Edit Inspect/Application FW Rule ウィザード （15 ページ）で説明されています。

表 *4 : [検査/アプリケーション FW ルールの追加および編集（Add and Edit Inspect/Application FW Rule）] ウィザードのステップ 2 : [アクション、送信元、宛先、およびサービス（Action, Sources, Destinations, and Services）] ページ*

要素	説明
操作	設定された次の条件に基づいて、検査する必要のあるトラフィックを識別するかどうか。通常は、[許可（Permit）] ルールを作成します。 • [Permit]：検査するトラフィックを特定します。 • [Deny]：トラフィックを検査から免除します。トラフィックが許可されるかブロックされるかは、アクセス ルールによって決定されます。

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/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。 • 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）。 • 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。 （注） これらのフィールドのいずれかに、項目をカンマで区切って複数の値を入力します。 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ートラフィックです。
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。

要素	説明
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。
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、[選択（Select）] をクリックして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、[作成（Create）] ボタンをクリックして作成します。

[検査/アプリケーションFWルールの追加または編集（Add or Edit Inspect/Application FW Rule）] ウィザード、[検査対象プロトコル（Inspected Protocol）] ページ

[検査/アプリケーションFWルール（Inspect/Application FW Rule）] ウィザードの [検査対象プロトコル（Inspected Protocol）] ページを使用して、このインスペクションルールによって監視されるプロトコルを設定します。

このセクションのオプションは、ファイアウォール インスペクション ルールを追加または編集したとき、および [Inspection Rules] ページ （10 ページ）のテーブルにある既存のルールの [検査対象のプロトコル（Inspected Protocol）] セルを右クリックしたときに表示されます。

（注） バージョン 4.9 以降、Security Manager では、ソフトウェアバージョン 9.4.0 以降を実行している ASA クラスタデバイスの SIP プロトコルをサポートします。

ナビゲーション パス

次のいずれかを実行します。

- Add Inspect/Application FW Rule ウィザードまたは Edit Inspect/Application FW Rule ウィザード （15 ページ）から、このページに達するまで [次へ（Next）] をクリックする。
- [検査対象プロトコルの編集（Edit Inspected Protocols）] ダイアログボックスを開くには、インスペクションルールの [検査対象プロトコル（Inspected Protocol）] セルを右クリックし、[検査対象プロトコルの編集（Edit Inspected Protocol）] を選択する。複数の行を選択すると、選択したすべてのルールに定義されている検査対象プロトコルが、変更によって置き換えられます。

関連項目

- [検査/アプリケーション FW ルールの追加または編集（Add or Edit Inspect/Application FW Rule）] ウィザード、ステップ 2 （18 ページ）
- インスペクション ルールについて （1 ページ）
- インスペクション ルールのインターフェイスの選択 （3 ページ）
- 検査するプロトコルの選択 （4 ページ）
- インスペクション ルールのアクセス ルール要件について （5 ページ）
- IOS デバイスでの Denial of Service（DoS; サービス拒絶）攻撃を防ぐためのインスペクションの使用 （6 ページ）
- ルールの編集
- テーブルのフィルタリング
- インスペクション ルールの設定 （7 ページ）

フィールド リファレンス

表 *5 : [*検査対象プロトコル（*Inspected Protocol***）*]* のオプション**

要素	説明
Protocols table	検査できるプロトコルのリストが表示されます。ルールごとに 1 つのプロトコルを選択できます。リストには、プロトコルのインスペクションを許可するデバイスのオペレーティングシステムに関する情報が含まれています。インスペクション ルール ポリシーを適用するデバイスタイプでサポートされていないプロトコルは選択しないでください。 **ヒント** IOS デバイスでは、ウィザードの最初のページで一致タイプに [カスタム宛先ポート（Custom Destination Ports）] または [宛先アドレスとポート（Destination Address and Port）] を選択した場合に、[カスタム プロトコル（custom protocol）] を選択し、[設定（Configure）] をクリックしてプロトコルに名前を付けることができます。その他のデバイス タイプでは、前に指定したポートに関連付けるプロトコルを選択します。 [オプション（Options）] 列には、選択したプロトコルに対して設定されているオプションが表示されます（存在する場合）。 [グループ（Group）] 列には、一部のプロトコルの使用に関する追加情報が表示されます。

要素	説明
Selected Protocol [Configure] ボタン	選択したプロトコルが表示されます。プロトコルで追加の設定が許可されている場合は、[Configure] ボタンがアクティブになります。このボタンをクリックするとオプションが表示され、開かれるダイアログボックスで [Help] ボタンをクリックすると、オプションに関する情報が表示されます。設定が許可されるプロトコルの詳細については、インスペクションのプロトコルおよびマップの設定 （28 ページ）を参照してください。
Rule Settings (IOS)	ルールが Cisco IOS ソフトウェアを実行しているデバイスで使用されている場合は、そのルールの追加設定。[Use Default Inspection] 設定を選択した場合は、IOS のデフォルト、またはインスペクション設定ポリシーで定義されている設定（IOS デバイスのインスペクション ルールの設定 （152 ページ）を参照）が使用されます。これらは、イネーブルまたはディセーブルにできる設定です。 • [Alert]：ステートフル パケット インスペクションのアラート メッセージをコンソールで生成するかどうか。 • [Audit]：監査証跡メッセージを syslog サーバまたはルータに記録するかどうか。 • [Timeout]：アクティビティがない場合にセッションが管理される時間の長さ（秒単位）を設定するかどうか。[タイムアウトを指定（Specify Timeout）] を選択した場合は、5 ～ 43200 秒のタイムアウト値を入力します。 • [Inspect Router Generated Traffic]：デバイス自体によって生成されるトラフィックを検査するかどうか。このオプションは、限られた数のプロトコルに対して使用できます。

[Configure DNS] ダイアログボックス

[Configure DNS] ダイアログボックスを使用して、PIX 7.0+、ASA、FWSM、および IOS デバイスでの DNS インスペクションを設定します。

ナビゲーション パス

[検査/アプリケーションFWルールの追加または編集（Add or Edit Inspect/Application FW Rule）] ウィザード、[検査対象プロトコル（Inspected Protocol）] ページ （22 ページ）に移動し、プロトコルテーブルで [DNS] を選択して、[設定（Configure）] をクリックします。

フィールド リファレンス

表 6 : [Configure DNS] ダイアログボックス

要素	説明
Maximum DNS Packet Length	最大 DNS パケット長。値は 512 ～ 65535 です。

要素	説明
DNS Map	トラフィックの一致条件とアクション、プロトコル準拠ポリシー、およびフィルタ設定を定義するDNSポリシーマップ オブジェクト。オブジェクト名を入力するか、[選択（Select）]をクリックして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、[作成（Create）] ボタンをクリックして作成します。
動的フィルタスヌーピングの有効化（Enable Dynamic Filter Snooping）	DNS ルックアップ情報のデータベースを構築するために、セキュリティ アプライアンスに DNS パケットのスヌープを許可するかどうか。この情報は、DNS名とIPアドレスをマッチングするためにボットネット トラフィック フィルタリングで使用されます。 ボットネット トラフィック フィルタリング ルール ポリシーを設定する場合は、このオプションを選択します。それ以外の場合は、このオプションを選択しないでください。詳細については、[Botnet Traffic Filter Rules] ページを参照してください。

[Configure SMTP] ダイアログボックス

SMTP のダイアログボックスを使用して、Simple Mail Transfer Protocol（SMTP; シンプル メール転送プロトコル）インスペクションの設定を編集します。SMTP は、インターネット上でのサーバとクライアント間の電子メールの転送に使用されます。

SMTP インスペクションでは、不正なコマンドがあるパケットがすべてドロップされます。パケットの最大データ長を設定できます。0 ～ 4294967295 の範囲の長さを入力します。

ナビゲーション パス

[検査/アプリケーションFWルールの追加または編集（Add or Edit Inspect/Application FW Rule）] ウィザード、[検査対象プロトコル（Inspected Protocol）] ページ （22 ページ）に移動し、プロトコルテーブルで [SMTP] を選択して、[設定（Configure）] をクリックします。

[Configure ESMTP] ダイアログボックス

[Configure ESMTP] ダイアログボックスを使用して、Extended Simple Mail Transport Protocol（ESMTP; 拡張シンプル メール転送プロトコル）インスペクションの設定を編集します。プラットフォームに基づいて、次の設定を行うことができます。

- [IOS devices]：パケットの最大データ長を設定できます。0 ～ 4294967295 の範囲の長さを入力します。
- [ASA/PIX 7.x+ devices]：ESMTP ポリシー マップ オブジェクトを指定して、詳細インスペクション パラメータを定義できます。オブジェクトの名前を入力するか、[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。

ナビゲーション パス

[検査/アプリケーションFWルールの追加または編集（Add or Edit Inspect/Application FW Rule）] ウィザード、[検査対象プロトコル（Inspected Protocol）] ページ （22 ページ）に移動し、プロトコルテーブルで [ESMTP] を選択して、[設定（Configure）] をクリックします。

[Configure Fragments] ダイアログボックス

[Configure Fragments] ダイアログボックスを使用して、IOS デバイスのフラグメント インスペクションの設定を編集します。

ナビゲーション パス

[検査/アプリケーションFWルールの追加または編集（Add or Edit Inspect/Application FW Rule）] ウィザード、[検査対象プロトコル（Inspected Protocol）] ページ （22 ページ）に移動し、プロトコルテーブルで [フラグメント（fragment）] を選択して、[設定（Configure）] をクリックします。

フィールド リファレンス

表 *7 : [Configure Fragments]* ダイアログボックス

要素	説明
Maximum Fragments	Cisco IOS ソフトウェアによって状態情報（構造）が割り当てられる、アセンブルされていないパケットの最大数。アセンブルされていないパケットとは、セッションの初期パケットよりも前に、ルータ インターフェイスに到着したパケットのことです。値は 0 ～ 10000 の状態エントリです。デフォルトは 256 です。 （注） 状態構造にはメモリが割り当てられます。この値をより大きい数値に設定すると、メモリ リソースが枯渇することがあります。
[タイムアウト(秒)（Timeout (sec)）]	パケット状態構造がアクティブに保たれる秒数。タイムアウト値が経過すると、アセンブルされていないパケットがルータによってドロップされ、別のパケットで使用できるように構造が解放されます。値は 1 ～ 1000 です。デフォルトのタイムアウト値は 1 秒です。

[Configure IMAP]/[Configure POP3] ダイアログボックス

[Configure IMAP]/[Configure POP3] ダイアログボックスを使用して、IOS デバイスの Internet Message Access Protocol（IMAP）または Post Office Protocol 3（POP3）インスペクションの設定を編集します。

- IMAP は、共有できるメール サーバ上に保持される電子メールまたは掲示板メッセージにアクセスするためのメソッドです。クライアント電子メールプログラムが、リモート メッセージにローカルであるかのようにアクセスできます。

- メール サーバに格納されている電子メールを受信するには POP3 が使用されます。IMAP とは異なり、POP はリモート ホストだけからメールを取得します。

ナビゲーション パス

[検査/アプリケーションFWルールの追加または編集（Add or Edit Inspect/Application FW Rule）] ウィザード、[検査対象プロトコル（Inspected Protocol）] ページ （22 ページ）に移動し、[IMAP] または [POP3] を選択して、[設定（Configure）] をクリックします。

フィールド リファレンス

表 *8 : [Configure IMAP]/[Configure POP3]* ダイアログボックス

要素	説明
Reset Connection on Invalid IMAP/POP3 packet	無効なパケットが検出された場合に、クライアントとサーバ間の接続をリセットするか、またはドロップするか。クライアントは、サーバに再接続するために検証プロセスを繰り返す必要があります。
Enforce Secure Authentication	パスワードがクリアテキストで送信されないように、クライアントがサーバへのセキュア ログインを使用する必要があるかどうか。

[Configure RPC] ダイアログボックス

RPC のダイアログボックスを使用して、IOS デバイスの RPC インスペクションの設定を編集します。RPC インスペクションでは、指定した RPC プログラムを除くすべての RPC プログラムのトラフィックがブロックされます。複数の RPC プログラムを許可するには、許可するプログラム番号ごとにルールを作成します。

ナビゲーション パス

[検査/アプリケーションFWルールの追加または編集（Add or Edit Inspect/Application FW Rule）] ウィザード、[検査対象プロトコル（Inspected Protocol）] ページ （22 ページ）に移動し、プロトコルテーブルで [RPC] を選択して、[設定（Configure）] をクリックします。

フィールド リファレンス

表 *9 : [Configure RPC]* ダイアログボックス

要素	説明
プログラム番号	許可するプログラム番号。値は 1 ～ 4294967295 です。
待ち時間（Wait Time）	同じ送信元アドレスから同じ宛先アドレスおよびポートへの後続の接続を許可するために、ファイアウォールの穴を開けたまま維持する時間（分単位）。値は 0 ～ 35791 分です。デフォルトは 0 です。

[Custom Protocol] ダイアログボックス

[Custom Protocol] ダイアログボックスを使用して、[検査/アプリケーション FW ルールの追加または編集（Add or Edit Inspect/Application FW Rule）] ウィザード、ステップ 2 （18 ページ）で IOS デバイスに対して設定したプロトコルとポートの指定に名前を割り当てます。

ナビゲーション パス

[検査/アプリケーションFWルールの追加または編集（Add or Edit Inspect/Application FW Rule）] ウィザード、[検査対象プロトコル（Inspected Protocol）] ページ （22 ページ）に移動し、プロトコルテーブルでカスタムプロトコルを選択して、[設定（Configure）] をクリックします。

[Configure] ダイアログボックス

[Configure] ダイアログボックスを使用して、HTTP または IM インスペクションのポリシーマップオブジェクトを選択します。これらのタイプのインスペクションに使用されるマップは、デバイスで使用されているオペレーティング システム バージョンによって異なります。目的のバージョンを選択し、[選択（Select）] をクリックして、目的のポリシーマップオブジェクトを選択するか、新規に作成します。

ナビゲーション パス

[検査/アプリケーションFWルールの追加または編集（Add or Edit Inspect/Application FW Rule）] ウィザード、[検査対象プロトコル（Inspected Protocol）] ページ （22 ページ）に移動し、プロトコルテーブルで [HTTP] または [IM] を選択して、[設定（Configure）] をクリックします。

インスペクションのプロトコルおよびマップの設定

デバイスのインスペクションルールを設定する場合は、検査するプロトコルを選択します。これらのプロトコルの一部では、詳細インスペクション用の追加設定が可能です。詳細インスペクションでは、パケットがデバイスを通過するために満たす必要のある追加要件を指定できます。たとえば、要求および応答のコンテンツ タイプが一致しない HTTP 接続をドロップできます。（検査可能なプロトコルの完全なリストについては、[インスペクションルール（Inspection Rule）] ページで [行の追加（Add Row）] をクリックし、[次へ（Next）] をクリックしてプロトコルリストを表示します）。

設定できる内容は、プロトコルだけでなく、デバイスのオペレーティングシステムとバージョン番号によっても異なります。通常は、IOS デバイスに比べて ASA デバイスの方がインスペクションを細かく微調整できます（IOS デバイスを設定するとき、インスペクションをより詳細に制御するには、ゾーンベースのファイアウォールインスペクションの設定を検討します。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）。

一部の詳細インスペクション設定は、インスペクションルールで直接行います。ただし、一部のプロトコルでは、独立したポリシー オブジェクトとして作成するポリシー マップを含むようにインスペクションルールを設定できます（デフォルトのインスペクションオプション以外が必要な場合にのみ、ポリシーマップを設定する必要があります）。これらのマップは、ポリシーの設定時にポリシー オブジェクト セレクタ ダイアログボックスから設定するか、[Policy

Object Manager] ウィンドウ（**[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）]** を選択）で設定できます。

ポリシーマップを使用するプロトコルでは、ターゲットトラフィックの一致条件を定義する、目的のポリシー マップを選択できます。ASA、PIX、および FWSM の各デバイスでは、これらのポリシー マップは一致条件を定義するクラス マップを指す場合があります。これらのポリシーマップを Policy Object Manager で作成するには、**[マップ（Maps）] > [ポリシーマップ（Policy Maps）] > [検査（Inspect）]** フォルダの次のテーブルにリストされているマップの 1 つを選択し、記載されているリファレンスで詳細な使用方法情報を確認します。**[マップ（Maps）] > [クラスマップ（Class Maps）] > 検査（Inspect）]** フォルダにあるクラスマップの作成の詳細については、一致条件ダイアログボックスに関する参照情報と インスペクション ポリシーのクラス マップの設定 （34 ページ）を参照してください。

表 *10*：インスペクション ルールでの詳細インスペクションのプロトコルの設定

プロトコル	Device Types	ポリシーマップ	クラスマップ（ASA、PIX、FWSM のみ）	説明および一致基準の参照
DNS	ASA、PIX、FWSM、IOS	DNS	DNS	クラス マップおよびポリシー マップを使用して、広範な基準に基づいてトラフィックを検査します。これにより、DNS パケットの広範な制御が可能になります。また、インスペクション ルールで最大長を設定し、（ASA デバイスで）ボットネット ルールでの動的 DNS スヌーピングの使用をイネーブルにできます。次のトピックを参照してください。 • DNS マップの設定 （40 ページ） • DNS クラス マップおよび DNS ポリシー マップの [Add Match Condition and Action]/[Edit Match Condition and Action] ダイアログボックス （46 ページ） • [Configure DNS] ダイアログボックス （24 ページ）
FTP Strict	ASA、PIX、FWSM、IOS	FTP	FTP	ファイル名、タイプ、サーバ、ユーザ、または FTP コマンドに基づいてトラフィックを検査します。 FTP マップの設定 （54 ページ）および FTP クラス マップおよび FTP ポリシー マップの [Add Match Condition and Action]/[Edit Match Condition and Action] ダイアログボックス （56 ページ）を参照してください。

プロトコル	**Device Types**	ポリシーマップ	クラスマップ（**ASA、PIX、FWSM** のみ）	説明および一致基準の参照
GTP	ASA、PIX、FWSM、IOS	GTP	GTP	タイムアウト値、メッセージサイズ、トンネル数、およびセキュリティアプライアンスを通過するGTPバージョンに基づいてトラフィックを検査します。GTP マップの設定 （59 ページ）およびGTP ポリシー マップの [Add Match Condition and Action]/[Edit Match Condition and Action] ダイアログボックス （64 ページ）を参照してください。
H.323 H.225 H.323 RAS	ASA、PIX、FWSM	H.323（ASA、PIX、FWSM）	H.323（ASA、PIX、FWSM）	H.323 メッセージ タイプ、発信側、着信側などの広範な基準に基づいてトラフィックを検査します。H.323 マップの設定 （67 ページ）およびH.323 クラス マップおよび H.323 ポリシー マップの [Add Match Condition and Action]/[Edit Match Condition and Action] ダイアログボックス（72 ページ）を参照してください。
HTTP	ASA、PIX、FWSM、IOS	HTTP（ASA 7.1.x、PIX 7.1.x、FWSM 3.x、IOS） HTTP（ASA 7.2 以降、PIX 7.2 以降）	HTTP（ASA、PIX、FWSM）	ヘッダーや本文の内容、ポートの誤用、トラフィックにJavaアプレットが含まれているかどうかなど、広範な基準に基づいてトラフィックを検査します。使用されるマップは、オペレーティングシステムとバージョンによって異なります。 **ASA/PIX 7.2 以降**の場合は、ASA 7.2+ および PIX 7.2+ デバイスの HTTP マップの設定 （85 ページ）およびHTTP クラスマップおよびHTTP ポリシー マップ（ASA 7.2+/PIX 7.2+）の [Add Match Condition and Action]/[Edit Match Condition and Action] ダイアログボックス （87 ページ）を参照してください。 **ASA/PIX 7.1.x、FWSM 3.x 以降、および IOS** の場合は、ASA 7.1.x、PIX 7.1.x、FWSM 3.x、および IOS デバイスの HTTP マップの設定 （74 ページ）を参照してください。

プロトコル	**Device Types**	ポリシーマップ	クラスマップ（**ASA、PIX、FWSM** のみ）	説明および一致基準の参照
SIP	ASA、PIX、FWSM	SIP（ASA、PIX、FWSM）	SIP（ASA、PIX、FWSM）	広範な基準に基づいてトラフィックを検査します。SIP マップの設定 （112 ページ）および SIP クラス マップおよびポリシー マップの [Add Match Condition and Action]/[Edit Match Condition and Action] ダイアログボックス （114 ページ）を参照してください。
Skinny	ASA、PIX、FWSM、IOS	Skinny	（なし）	広範な基準に基づいてトラフィックを検査します。Skinny マップの設定 （118 ページ）および Skinny ポリシー マップの [Add Match Condition and Action]/[Edit Match Condition and Action] ダイアログボックス （121 ページ）を参照してください。
SMTP	ASA、PIX 7.x+、FWSM 3.x+、IOS	（なし）	（なし）	Simple Mail Transfer Protocol（SMTP; シンプルメール転送プロトコル）トラフィックを検査し、無効なコマンドを使用するパケットをすべてドロップします。パケットの最大データ長を設定できます。 [Configure SMTP] ダイアログボックス （25 ページ）を参照してください。
SNMP	ASA、PIX、FWSM 3.x+、IOS	SNMP	（なし）	SNMP バージョンに基づいて SNMP トラフィックを検査します。 SNMP マップの設定 （122 ページ）を参照してください。
NetBIOS	ASA、PIX 7.x+、FWSM	NetBIOS	（なし）	NetBIOS トラフィックを検査し、セキュリティアプライアンスの NAT 設定に従って NetBIOS Name Service（NBNS）パケット内の IP アドレスを変換します。プロトコルに違反するパケットをドロップできます。 NetBIOS マップの設定 （109 ページ）を参照してください。
IPSec Pass Through	ASA、PIX 7.x+	IPsec Pass Through	（なし）	IPSec トラフィックを検査し、ESP または AH トラフィックが許可されるかどうかを制御します。 IPsec パススルー マップの設定 （107 ページ）を参照してください。

プロトコル	**Device Types**	ポリシーマップ	クラスマップ（**ASA、PIX、FWSM** のみ）	説明および一致基準の参照
DCE/RPC	ASA 7.2+、PIX 7.2+、FWSM 3.2+	DCE/RPC	（なし）	タイムアウトとマッパーサービスの実行に基づいてトラフィックを検査します。DCE/RPC マップの設定 （36 ページ）を参照してください。
IP オプション	ASA 8.2(2)+	IP オプション	（なし）	IP ヘッダーの Options セクションに特定のオプションが設定されている IP パケットを許可します。ルーテッドモードでは、router-alert オプションを含むパケットが許可されます。それ以外の場合は、いずれかのオプションが設定されていると、パケットがドロップされます。IP オプションはほとんどの通信で必要ではありませんが、NOP（no operation）オプションがパディングに使用される場合があるため、このオプションを許可することが必要となることがあります。IP オプション マップの設定 （98 ページ）を参照してください。
IPv6	ASA 8.4(2)+	IPv6	（なし）	IPv6 パケット内の任意の場所で見つかった次のタイプの拡張ヘッダーに基づいて IPv6 トラフィックを検査します。ホップバイホップオプション、ルーティング（タイプ 0）、フラグメント、宛先オプション、認証、およびカプセル化セキュリティペイロード。IPv6 マップの設定 （102 ページ）および IPv6 ポリシーマップの [マッチ条件とアクションの追加または編集（Add/Edit Match Condition and Action] ダイアログボックス （104ページ）を参照してください。
ESMTP	ASA、PIX 7.x+、FWSM 3.x+、IOS	ESMTP	（なし）	ESMTP トラフィックを検査します。IOS では、最大データ長だけを設定できます。ASA、PIX、FWSM では、広範な基準に基づいてトラフィックを検査できます。 [Configure ESMTP] ダイアログボックス （25 ページ）を参照してください。
フラグメント	IOS	（なし）	（なし）	アセンブルされていないパケットフラグメントの最大許容数に基づいてトラフィックを検査します。 [Configure Fragments] ダイアログボックス （26 ページ）を参照してください。

プロトコル	**Device Types**	ポリシーマップ	クラスマップ（**ASA、PIX、FWSM** のみ）	説明および一致基準の参照
Internet Message Access Protocol（IMAP） Post Office Protocol 3（POP3）	IOS	（なし）	（なし）	無効なコマンドまたはクリアテキストログインに基づいてトラフィックを検査します。[Configure IMAP]/[Configure POP3] ダイアログボックス （26 ページ）を参照してください。
Sun Remote Procedure Call（RPC; リモートプロシージャ コール）	FWSM 2.x、IOS	（なし）	（なし）	RPC プロトコル番号に基づいてトラフィックを検査します。[Configure RPC] ダイアログボックス （27 ページ）を参照してください。
IM	ASA、PIX 7.x+、IOS	IM（ASA 7.2+、PIX 7.2+） IM（IOS）	IM（ASA、PIX のみ）	広範な基準に基づいてトラフィックを検査します。許可されるマップは、オペレーティングシステムのバージョンによって異なります。 **ASA、PIX** の場合は、ASA 7.2+、PIX 7.2+ デバイスの IM マップの設定 （92 ページ）および IM クラス マップおよび IM ポリシー マップ（ASA 7.2+/PIX 7.2+）の [Add Match Condition and Action]/[Edit Match Condition and Action] ダイアログボックス （94 ページ）を参照してください。 **IOS** の場合は、IOS デバイスの IM マップの設定 （96 ページ）を参照してください。
SCTP	ASA 9.5(2)+	SCTP	（なし）	ペイロード PID（PPID）に基づいてトラフィックを検査します。SCTP マップの設定 （123 ページ）および SCTP ポリシーマップの [一致条件とアクションの追加または編集（Add or Edit Match Condition and Action] ダイアログボックス （125 ページ）を参照してください。

プロトコル	Device Types	ポリシーマップ	クラスマップ（ASA、PIX、FWSM のみ）	説明および一致基準の参照
Diameter	ASA 9.5(2)+	Diameter	Diameter	アプリケーションID、コマンドコード、および AVP に基づいてトラフィックを検査します。Diameter マップの設定 （126 ページ）および Diameter クラスとポリシーマップの [一致条件（とアクション）の追加または編集（Add or Edit Match Condition (and Action)] ダイアログボックス （129 ページ）を参照してください。
LISP	ASA 9.5(2)+	LISP	なし（None）	エンドポイント識別子アクセスリストおよび検証キーで許可されたトラフィックを検査します。LISP マップの設定 （139 ページ）を参照してください
M3UA	ASA 9.6(2)+	M3UA	なし（None）	M3UA プロトコル準拠を満たさないパケットをドロップしてログに記録します。M3UA マップの設定 （141 ページ）を参照してください

関連項目

- 検査するプロトコルの選択 （4 ページ）
- インスペクション ルールについて （1 ページ）
- IOS デバイスでの Denial of Service（DoS; サービス拒絶）攻撃を防ぐためのインスペクションの使用 （6 ページ）
- インスペクション ルールの設定 （7 ページ）
- ポリシー オブジェクトの作成
- マップ オブジェクトについて
- 正規表現の追加/編集 （149 ページ）
- 正規表現グループの設定 （148 ページ）

インスペクション ポリシーのクラス マップの設定

[Add Class Map]/[Edit Class Map] ダイアログボックスを使用すると、同じタイプのポリシーマップで使用するクラスマップを定義できます。ダイアログボックスの名前は、作成するマップのタイプを示します。

クラス マップでは、アプリケーション固有の基準に基づいてトラフィックを定義します。次に、対応するポリシー マップ内のクラス マップを選択し、選択したトラフィックに適用するアクションを設定します。したがって、各クラスマップには、同じ方法（許可する、ドロップするなど）で処理するトラフィックを含める必要があります。

ASA/PIX 7.2 以降、または FWSM を実行しているデバイスのインスペクションルールを設定している場合は、DNS、FTP、H.323、HTTP、IM、SIP、および ScanSafe のトラフィックタイプのインスペクション用クラスマップを作成できます。

関連ポリシー マップにクラス基準を定義することもできます。ただし、クラス マップを作成すると、複数のポリシー マップでマップを再利用できます。

ここでは、使用可能な一致基準について説明します。

- DNS クラス マップおよび DNS ポリシー マップの [Add Match Condition and Action]/[Edit Match Condition and Action] ダイアログボックス （46 ページ）
- FTP クラス マップおよび FTP ポリシー マップの [Add Match Condition and Action]/[Edit Match Condition and Action] ダイアログボックス （56 ページ）
- H.323 クラス マップおよび H.323 ポリシー マップの [Add Match Condition and Action]/[Edit Match Condition and Action] ダイアログボックス （72 ページ）
- HTTP クラス マップおよび HTTP ポリシー マップ（ASA 7.2+/PIX 7.2+）の [Add Match Condition and Action]/[Edit Match Condition and Action] ダイアログボックス （87 ページ）
- IM クラス マップおよび IM ポリシー マップ（ASA 7.2+/PIX 7.2+）の [Add Match Condition and Action]/[Edit Match Condition and Action] ダイアログボックス （94 ページ）
- SIP クラス マップおよびポリシー マップの [Add Match Condition and Action]/[Edit Match Condition and Action] ダイアログボックス （114 ページ）
- Diameter クラスとポリシーマップの [一致条件（とアクション）の追加または編集（Add or Edit Match Condition (and Action)] ダイアログボックス （129 ページ）

ナビゲーション パス

[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択し、コンテンツテーブルの [マップ（Maps）] > [クラスマップ（Class Maps）] > [検査（Inspect）] フォルダで [DNS]、[FTP]、[H.323 (ASA/PIX/FWSM)]、[HTTP (ASA/PIX/FWSM)]、[IM]、[SIP (ASA/PIX/FWSM)]、または [Diameter] を選択します。作業領域内を右クリックしてから [新規オブジェクト(New Object] を選択するか、行を右クリックしてから [オブジェクトの編集（Edit Object）] を選択します。

関連項目

- マップ オブジェクトについて
- インスペクションのプロトコルおよびマップの設定 （28 ページ）
- インスペクション ルールについて （1 ページ）

フィールド リファレンス

表 *11* : インスペクション ルールの *[Add Class Maps]/[Edit Class Maps]* ダイアログボックス

要素	説明
名前	ポリシー オブジェクトの名前。最大 40 文字を使用できます。
説明	ポリシー オブジェクトの説明。最大 200 文字を使用できます。
[Match] テーブル 一致タイプ（Match Type）	[Match] テーブルには、クラスマップに含まれている基準が表示されます。各行には、各基準に一致する、または一致しないトラフィックを検査で検索するかどうか、および検査される基準と値が示されます。 • 基準を追加するには、[Add] ボタンをクリックし、[Match Criterion] ダイアログボックスに入力します。詳細については、上記で示している項を参照してください。 • 基準を編集するには、基準を選択し、[Edit] ボタンをクリックします。 • 基準を削除するには、基準を選択し、[Delete] ボタンをクリックします。
カテゴリ	オブジェクトに割り当てられたカテゴリ。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。
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、ポリシー オブジェクトの上書きの許可および個々のデバイスのポリシー オブジェクト オーバーライドについてを参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）] ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）] フィールドには、このオブジェクトに対するオーバーライドを持つデバイスの数が表示されます。

DCE/RPC マップの設定

[Add DCE/RPC Map]/[Edit DCE/RPC Map] ダイアログボックスを使用して、DCE/RPC インスペクションのマップを定義します。DCE/RPC インスペクション ポリシー マップを使用すると、DCE/RPC インスペクションに使用されるデフォルトの設定値を変更できます。

DCE/RPC は、Microsoft 分散クライアントおよびサーバ アプリケーションで広く使用されているプロトコルであり、ソフトウェア クライアントがサーバ上のプログラムをリモートで実行できるようにします。

このような処理では、一般的に、必要なサービスに動的に割り当てられるネットワーク情報を取得するために、エンドポイント マッパーと呼ばれるサーバのウェルノウン ポート番号をリスニングすることによって、クライアントがクエリーを実行します。次に、クライアントは、サービスを提供しているサーバーのインスタンスへのセカンダリ接続をセットアップします。セキュリティ アプライアンスは、適切なポート番号とネットワーク アドレスへのセカンダリ接続を許可し、必要に応じて NAT を適用します。

DCE/RPC インスペクション マップは、EPM とウェルノウン TCP ポート 135 上のクライアントとの間のネイティブ TCP 接続を検査します。クライアント用に EPM のマッピングとルックアップがサポートされています。クライアントとサーバーは、どのセキュリティ ゾーンにあってもかまいません。埋め込みサーバ IP アドレスとポート番号は、該当する EPM 応答メッセージから受信されます。クライアントは EPM によって返されたサーバ ポートに複数の接続を試行できるため、ユーザが設定可能なタイムアウトのあるピンホールを複数使用できます。

ナビゲーション パス

[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択し、オブジェクトタイプセレクタから [マップ（Maps）] > [ポリシーマップ（Policy Maps）] > [検査（Inspect）] > [DCE/RPC] を選択します。作業領域内を右クリックしてから [新規オブジェクト（New Object）] を選択するか、行を右クリックしてから [オブジェクトの編集（Edit Object）] を選択します。

関連項目

- マップ オブジェクトについて
- インスペクションのプロトコルおよびマップの設定 （28 ページ）

フィールド リファレンス

表 *12 : [Add DCE/RPC]/[Edit DCE/RPC]* ダイアログボックス

要素	説明
名前	ポリシー オブジェクトの名前。最大 40 文字を使用できます。
説明	ポリシー オブジェクトの説明。最大 200 文字を使用できます。
Pinhole Timeout	DCE/RPC ピンホールのタイムアウト。デフォルトは 2 分（00:02:00）です。有効な値は、00:00:01 ～ 1193:00:00 です。
Enforce Endpoint Mapper Service	バインディング時にエンドポイント マッパー サービスを実行するかどうか。このサービスを使用して、クライアントはエンドポイント マッパーと呼ばれるサーバに、必要なサービスについて動的に割り当てられたネットワーク情報をクエリーします。

要素	説明
Enable Endpoint Mapper Service Lookup Service Lookup Timeout	エンドポイントマッパーサービスの検索操作をイネーブルにするかどうか。このオプションを選択した場合は、検索操作のタイムアウトを入力できます。タイムアウトを指定しない場合は、ピンホールタイムアウトまたはデフォルトのピンホール タイムアウト値が使用されます。有効な値は、00:00:01 ～ 1193:00:00 です。
[Match Condition and Action] タブ [Match All] テーブルに、ポリシーマップに含まれている基準が表示されます。各行には、各基準に一致する、または一致しないトラフィックを検査で検索するかどうか、検査される基準と値、および条件を満たすトラフィックに対して実行されるアクションが示されます。 • 基準を追加するには、[Add] ボタンをクリックし、[Match Condition and Action] ダイアログボックスに入力します（DCE/RPC クラスとポリシーマップの [一致条件（とアクション）の追加（Add Match Condition (and Action)）]/[一致条件（とアクション）の編集（Edit Match Condition (and Action)）] ダイアログボックス （38 ページ）を参照）。 • 基準を編集するには、基準を選択し、[Edit] ボタンをクリックします。 • 基準を削除するには、基準を選択し、[Delete] ボタンをクリックします。	
カテゴリ	オブジェクトに割り当てられたカテゴリ。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。
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、ポリシーオブジェクトの上書きの許可および個々のデバイスのポリシーオブジェクト オーバーライドについてを参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）] ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）] フィールドには、このオブジェクトに対するオーバーライドを持つデバイスの数が表示されます。

DCE/RPC クラスとポリシーマップの [一致条件（とアクション）の追加（Add Match Condition (and Action)）]/[一致条件（とアクション）の編集（Edit Match Condition (and Action)）] ダイアログボックス

[DCE/RPC一致基準の追加（Add DCE/RPC Match Criterion）]/[DCE/RPC一致基準の編集（Edit DCE/RPC Match Criterion）] ダイアログボックス（DCE/RPC クラスマップの場合）または [一致条件とアクションの追加（Add Match Condition and Action）]/[一致条件とアクションの編集（Edit Match Condition and Action）] ダイアログボックス（DCE/RPC ポリシーマップの場合）を使用して、次の処理を行います。

- DCE/RPC クラスマップの一致基準と値を定義します。
- DCE/RPC ポリシーマップを作成するときに、DCE/RPC クラスマップを選択します。
- DCE/RPC ポリシーマップで一致基準、値、およびアクションを直接定義します。

このダイアログボックスのフィールドは、選択した基準、およびクラスマップとポリシーマップのどちらを作成しているかによって変わります。

ナビゲーション パス

DCE/RPC クラスマップを作成している場合は、[Policy Object Manager] で、DCE/RPC の [クラスマップの追加（Add Class Maps）]/[クラスマップの編集（Edit Class Maps）] ダイアログボックスのテーブル内を右クリックして [行の追加（Add Row）] を選択するか、行を右クリックして [行の編集（Edit Row）] を選択します。インスペクション ポリシーのクラス マップの設定（34 ページ）を参照してください。

DNS ポリシーマップを作成している場合は、[Policy Object Manager] で、[DNSマップの追加（Add DNS Map）]/[DNSマップの編集（Edit DNS Map）] ダイアログボックスの [一致条件とアクション（Match Condition and Action）] タブのテーブル内を右クリックして [行の追加（Add Row）] を選択するか、行を右クリックして [行の編集（Edit Row）] を選択します。DCE/RPC マップの設定 （36 ページ） を参照してください。

関連項目

- マップ オブジェクトについて
- インスペクションのプロトコルおよびマップの設定 （28 ページ）

フィールド リファレンス

表 *13 : DCE/RPC* クラスとポリシーマップの *[*一致条件とアクションの追加（*Add Match Condition and Action*）*]/[*一致条件とアクションの編集（*Edit Match Condition and Action*）*]* ダイアログボックス

要素	説明
一致タイプ（Match Type） クラス名 （ポリシー マップのみ）	既存の DCE/RPC クラスマップを使用するか、新規 DCE/RPC クラスマップを定義できます。 • [Use Specified Values]：このダイアログボックスでクラス マップを定義する場合。 • [クラスマップの値を使用（Use Values in Class Map）]：既存の DCE/RPC クラス マップ ポリシー オブジェクトを選択する場合。DNS クラスマップの名前を [クラス名（Class Name）] フィールドに入力します。[選択（Select）] をクリックしてリストからマップを選択するか、新しいクラスマップオブジェクトを作成します。

要素	説明
基準	照合するトラフィック基準を指定します。 • ms-rpc-epm：Microsoft RPC EPM メッセージを照合します。 • ms-rpc-isystemactivator：ISystemMapper メッセージを照合します。 • ms-rpc-oxidresolver：OxidResolver メッセージを照合します。
タイプ（Type）	基準に一致する、または一致しないトラフィックをマップに含めるかどうかを指定します。たとえば、文字列「example.com」で [一致しない（Doesn’t Match）] を選択した場合、「example.com」を含むトラフィックはすべてマップの対象外になります。 • [Matches]：基準に一致する。 • [一致しない（Doesn't Match）]：基準に一致しない。
操作 （ポリシー マップのみ）	定義された基準に一致するトラフィックに対してデバイスが適用するアクション。 • [リセット（Reset）]：パケットをドロップし、接続を閉じ、サーバーとクライアントの両方またはいずれかに TCP リセットを送信します。 • [ログ（Log）]：システムログメッセージを送信します。このオプションは単独で使用するか、または他のアクションのいずれかと一緒に使用できます。 • [リセットとログ（Reset and Log）]：リセットアクションとログアクションを実行します。

DNS マップの設定

[Add DNS Map]/[Edit DNS Map] ダイアログボックスを使用して、インスペクション用の DNS マップを定義します。DNS マップを使用すると、DNS アプリケーション インスペクションに使用するデフォルト設定値を変更できます。

DNS アプリケーション インスペクションは、DNS スプーフィングとキャッシュ ポイズニングを防ぐための DNS メッセージ制御をサポートしています。特定の DNS タイプを許可、ドロップ、または記録し、その他の DNS タイプをブロックするルールを設定できます。たとえば、サーバ間でのゾーン転送を制限できます。

公開サーバが特定の内部ゾーンだけをサポートしている場合に、DNS ヘッダーにある Recursion Desired フラグと Recursion Available フラグをマスクして、サーバを攻撃から守ることができます。また、DNS ランダム化をイネーブルにすると、ランダム化をサポートしていないサーバや強度の低い疑似乱数ジェネレータを使用するサーバのスプーフィングやキャッシュ侵害を回避

できます。クエリーできるドメイン名を制限することによって、パブリック サーバがより確実に保護されます。

不一致の DNS 応答を過度に多数受信した（このことはキャッシュ侵害攻撃を示している可能性があります）場合に、DNS 不一致のアラートを設定して通知できます。

ナビゲーション パス

[管理（Manage）]>[ポリシーオブジェクト（Policy Objects）] を選択し、オブジェクトタイプセレクタから **[マップ（Maps）]>[ポリシーマップ（Policy Maps）]>[検査（Inspect）]>[DNS]** を選択します。作業領域内を右クリックしてから [新規オブジェクト（New Object）] を選択するか、行を右クリックしてから [オブジェクトの編集（Edit Object）] を選択します。

関連項目

- マップ オブジェクトについて
- インスペクションのプロトコルおよびマップの設定 （28 ページ）
- インスペクション ポリシーのクラス マップの設定 （34 ページ）

フィールド リファレンス

表 *14 : [Add DNS Map]/[Edit DNS Map]* ダイアログボックス

要素	説明
名前	ポリシー オブジェクトの名前。最大 40 文字を使用できます。
説明	ポリシー オブジェクトの説明。最大 200 文字を使用できます。
[Protocol Conformance] タブ DNS セキュリティの設定とアクションを定義します。このタブのオプションの詳細については、 DNS マップの [Protocol Conformance] タブ （43 ページ）を参照してください。	
[Filtering] タブ DNS のフィルタリング設定を定義します。このタブのオプションの詳細については、 DNS マップの [Filtering] タブ （44 ページ）を参照してください。	

要素	説明
[Mismatch Rate] タブ [DNS IDの不一致レートが超過した場合にロギング（Log When DNS ID Mismatch Rate Exceeds）] オプションでは、DNS 識別子不一致が過度に発生した場合に、次の基準に基づいてレポートするかどうかを決定します。 • [Threshold]：システム メッセージ ログが送信される前に許容される不一致の最大発生数。値は 0 ～ 4294967295 です。 • [Time Interval]：モニタする期間（秒単位）。値は 1 ～ 31536000 です。	
[Cisco Umbrellaコネクタ（Cisco Umbrella Connector）] タブ DNS の DNS Umbrella コネクタ設定を定義します。このタブのオプションの詳細については、[DNS Umbrellaコネクタ（DNS Umbrella Connector）] タブ （45 ページ）を参照してください。	
[Match Condition and Action] タブ [Match All] テーブルに、ポリシー マップに含まれている基準が表示されます。各行には、各基準に一致する、または一致しないトラフィックを検査で検索するかどうか、検査される基準と値、および条件を満たすトラフィックに対して実行されるアクションが示されます。 • 基準を追加するには、[Add] ボタンをクリックし、[Match Condition and Action] ダイアログボックスに入力します（DNS クラス マップおよび DNS ポリシー マップの [Add Match Condition and Action]/[Edit Match Condition and Action] ダイアログボックス （46 ページ）を参照）。 • 基準を編集するには、基準を選択し、[Edit] ボタンをクリックします。 • 基準を削除するには、基準を選択し、[Delete] ボタンをクリックします。	
カテゴリ	オブジェクトに割り当てられたカテゴリ。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。

要素	説明
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、ポリシー オブジェクトの上書きの許可および個々のデバイスのポリシー オブジェクト オーバーライドについてを参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）] ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）] フィールドには、このオブジェクトに対するオーバーライドを持つデバイスの数が表示されます。

DNS マップの [Protocol Conformance] タブ

[Protocol Conformance] タブを使用して、DNS マップの DNS セキュリティ設定とアクションを定義します。

ナビゲーション パス

[Add DNS Map]/[Edit DNS Map] ダイアログボックスの [Protocol Conformance] タブをクリックします。 DNS マップの設定 （40 ページ） を参照してください。

関連項目

- マップ オブジェクトについて
- インスペクションのプロトコルおよびマップの設定 （28 ページ）

フィールド リファレンス

表 15 : DNS マップの [Protocol Conformance] タブ

要素	説明
Enable DNS Guard Function	DNS ヘッダーの識別子フィールドを使用して DNS クエリーおよび応答の不一致チェックを実行するかどうか。クエリーごとに 1 つの応答がセキュリティ アプライアンスを通過できます。
Generate Syslog for ID Mismatch	DNS 識別子の不一致が過度に発生した場合に syslog エントリを作成するかどうか。
Randomize the DNS Identifier for DNS Query	DNS クエリー メッセージの DNS 識別子をランダム化するかどうか。

要素	説明
Enable NAT Rewrite Function	DNS 応答の A レコードで IP アドレス変換をイネーブルにするかどうか。
Enable Protocol Enforcement	ドメイン名、ラベル長、圧縮、ループ ポインタのチェックなど、DNS メッセージ形式チェックをイネーブルにするかどうか。
Enable DNS on TCP	DNS over TCP トラフィックのインスペクションを有効にするかどうかを指定します。DNS/TCP ポート 53 トラフィックが、DNS インスペクションを適用するクラスの一部であることを確認します。インスペクションのデフォルト クラスには、TCP/53 が含まれています。
Require Authentication Between DNS Server (RFC2845) 操作	RFC 2845 の規定に従って、DNS サーバ間で認証を要求するかどうか。このオプションを選択した場合は、認証がない場合に実行するアクションを選択します。

DNS マップの [Filtering] タブ

[Filtering] タブを使用して、DNS マップの DNS フィルタリング設定とアクションを定義します。

ナビゲーション パス

[Add DNS Map]/[Edit DNS Map] ダイアログボックスの [Filtering] タブをクリックします。 DNS マップの設定 （40 ページ） を参照してください。

関連項目

- マップ オブジェクトについて
- インスペクションのプロトコルおよびマップの設定 （28 ページ）

フィールド リファレンス

表 16 : DNS マップの [Filtering] タブ

要素	説明
Drop Packets that Exceed Specified Length Maximum Packet Length	指定したバイト単位の最大長を超えたパケットをドロップするかどうか。これはグローバル設定です。
Drop Packets Sent to Server that Exceed Specified Maximum Length 最大長（Maximum Length）	指定したバイト単位の最大長を超えた、サーバに送信されたパケットをドロップするかどうか。

要素	説明
Drop Packets Sent to Server that Exceed Length Indicated by Resource Record	サーバに送信されたパケットのうち、リソース レコードで指定された長さを超えるものをドロップするかどうか。
Drop Packets Sent to Client that Exceed Specified Length 最大長（Maximum Length）	クライアントに送信されたパケットのうち、指定したバイト単位の最大長を超えたものをドロップするかどうか。
Drop Packets Sent to Client that Exceed Length Indicated by Resource Record	リソース レコードで指定された長さを超えた、クライアントに送信されたパケットをドロップするかどうか。

[DNS Umbrellaコネクタ（DNS Umbrella Connector）] タブ

[Umbrellaコネクタ（Umbrella Connector）] タブを使用して、DNS マップの DNS Umbrella コネクタ設定を定義します。Cisco Security Manager バージョン 4.18 以降、Umbrella グローバルポリシーは ASA 9.10.1 以降のデバイスでサポートされています。

ナビゲーション パス

[DNSマップの追加（Add DNS Map）]/[DNSマップの編集（Edit DNS Map）] ダイアログボックスの [Umbrellaコネクタ（Umbrella Connector）] タブをクリックします。 DNS マップの設定（40 ページ） を参照してください。

関連項目

- Umbrella グローバルポリシーの設定

フィールド リファレンス

表 17 : [DNS Umbrellaコネクタ（DNS Umbrella Connector）] タブ

要素	説明
Umbrellaポリシーの Umbrellaコネクタタグの有効化（Enable Umbrella Connector Tag for Umbrella Policy）	チェックボックスをオンにして、DNS ポリシーマップ Umbrella タグ名を入力します。tag 名には、最大 50 文字を指定できます。タグ名が 50 文字を超える場合、Cisco Security Manager からエラーメッセージがスローされます。 （注） Umbrella グローバルポリシーが設定されていない場合、Cisco Security Manager からアクティビティ検証エラーが表示されます。Umbrella グローバルポリシー設定の詳細については、Umbrella グローバルポリシーの設定を参照してください。

要素	説明
フェールオープンの有効化（Enable Fail-Open）	Umbrella DNS サーバーが使用できない場合に DNS 解決を動作させるには、このチェックボックスをオンにします。 フェールオープンが選択されていて、Cisco Umbrella DNS サーバーが使用できない場合、このポリシーマップで Umbrella 自体が無効になり、システム上に設定された他の DNS サーバー（存在する場合）に DNS 要求を移動できます。Umbrella DNS サーバーが再度使用可能になると、ポリシーマップはそれらの使用を再開します。このオプションを選択しない場合、アクセスできない Umbrella リゾルバに DNS 要求が移動し続けるため応答を得られません。
デバイスID	デバイス ID は、デバイスが Umbrellaサーバーに正常に登録された後に生成されます。ID は、Cisco Security Manager でデバイスを再検出した後にのみ、このフィールドに表示されます。 （注） デバイス ID に変更がある場合は常に、Cisco Security Manager でデバイスを再検出して、変更内容と同期させる必要があります。
DNSCryptの有効化（Enable DNScrypt）	Umbrella データパスで DNS 暗号化を有効にするには、このチェックボックスをオンにします。1 時間ごとに、秘密鍵がキーエクスチェンジスレッドと Umbrella リゾルバの間で交換されます。 [Umbrellaコネクタの有効化（Enable Umbrella Connector）] チェックボックスがオンになっていることを確認します。チェックボックスがオフの場合、設定の不一致に関するエラーメッセージが表示されます。 （注） Umbrella グローバルポリシーが設定されていない場合、Cisco Security Manager からアクティビティ検証エラーが表示されます。Umbrella グローバルポリシー設定の詳細については、Umbrella グローバルポリシーの設定を参照してください。

DNS クラス マップおよび DNS ポリシー マップの [Add Match Condition and Action]/[Edit Match Condition and Action] ダイアログボックス

[Add DNS Match Criterion]/[Edit DNS Match Criterion] ダイアログボックス（DNS クラス マップの場合）または [Add Match Condition and Action]/[Edit Match Condition and Action] ダイアログボックス（DNS ポリシー マップの場合）を使用して、次の処理を行います。

- DNS クラス マップの一致基準と値を定義する。
- DNS ポリシー マップの作成時に DNS クラス マップを選択する。
- DNS ポリシー マップに一致基準、値、およびアクションを直接定義する。

このダイアログボックスのフィールドは、選択した基準、およびクラスマップとポリシーマップのどちらを作成しているかによって変わります。

ナビゲーション パス

DNS クラスマップを作成している場合は、[Policy Object Manager] で、DNS の [クラスマップの追加（Add Class Maps）]/[クラスマップの編集（Edit Class Maps）] ダイアログボックスのテーブル内を右クリックして [行の追加（Add Row）] を選択するか、行を右クリックして [行の編集（Edit Row）] を選択します。 インスペクション ポリシーのクラス マップの設定 （34 ページ）を参照してください。

DNS ポリシーマップを作成している場合は、[Policy Object Manager] で、[DNSマップの追加（Add DNS Map）]/[DNSマップの編集（Edit DNS Map）] ダイアログボックスの [一致条件とアクション（Match Condition and Action）] タブのテーブル内を右クリックして [行の追加（Add Row）] を選択するか、行を右クリックして [行の編集（Edit Row）] を選択します。 DNS マップの設定 （40 ページ） を参照してください。

関連項目

- マップ オブジェクトについて
- インスペクションのプロトコルおよびマップの設定 （28 ページ）

フィールド リファレンス

表 *18 : DNS* クラス マップおよび *DNS* ポリシー マップの *[Add Match Condition and Action]/[Edit Match Condition and Action]* ダイアログボックス

要素	説明
一致タイプ（Match Type） クラス名 （ポリシー マップのみ）	既存の DNS クラス マップを使用するか、新規 DNS クラス マップを定義できます。 • [Use Specified Values]：このダイアログボックスでクラス マップを定義する場合。 • [Use Values in Class Map]：既存の DNS クラス マップ ポリシー オブジェクトを選択する場合。DNS クラスマップの名前を [クラス名（Class Name）] フィールドに入力します。[選択（Select）] をクリックしてリストからマップを選択するか、新しいクラスマップオブジェクトを作成します。

要素	説明
基準	照合するトラフィック基準を指定します。 • [DNS Class]：DNS クエリーまたはリソース レコードのクラスを照合します。 • [DNS Type]：DNS クエリーまたはリソース レコードのタイプを照合します。 • [Domain Name]：DNS クエリーまたはリソース レコードのドメイン名を照合します。 • [Header Flag]：ヘッダー内の DNS フラグを照合します。 • [Question]：DNS の質問を照合します。 • [Resource Record]：DNS リソース レコードを照合します。
タイプ（Type）	基準に一致する、または一致しないトラフィックをマップに含めるかどうかを指定します。たとえば、文字列「example.com」で [一致しない（Doesn’t Match）] を選択した場合、「example.com」を含むトラフィックはすべてマップの対象外になります。 • [Matches]：基準に一致する。 • [一致しない（Doesn't Match）]：基準に一致しない。
操作 （ポリシー マップのみ）	定義された基準に一致するトラフィックに対してデバイスが適用するアクション。
可変フィールド 次のフィールドは、[Criterion] フィールドでの選択内容によって変わります。このリストは、表示されると想定されるフィールドのスーパーセットです。	
値 （DNS クラス基準の場合）	検査する DNS クラス。 • [Internet]：インターネット DNS クラスと一致します。 • [DNS Class Field Value]：指定した数値と一致します。 • [DNS Class Field Range]：指定した数値範囲と一致します。

要素	説明
値 （DNS タイプ基準の場合）	検査する DNS タイプ。 • [DNS Type Field Name]：DNS タイプの名前と一致します。 • [A]：IPv4 アドレス。 • [AXFR]：完全（ゾーン）転送。 • [CNAME]：正規の名前。 • [IXFR]：増分（ゾーン）転送。 • [NS]：権限ネームサーバ。 • [SOA]：権限のゾーンの開始。 • [TSIG]：トランザクション シグニチャ。 • [DNS Type Field Value]：指定した数値と一致します。 • [DNS Type Field Range]：指定した数値範囲と一致します。
値 （ドメイン名基準の場合）	評価する正規表現。次のいずれかを選択できます。 • [Regular Expression]：パターン マッチングに使用する正規表現を定義する、正規表現オブジェクト。オブジェクトの名前を入力します。[選択（Select）] をクリックして既存のオブジェクトのリストからオブジェクトを選択するか、または新しい正規表現オブジェクトを作成できます。 • [Regular Expression Group]：パターン マッチングに使用する正規表現を定義する、正規表現グループ オブジェクト。オブジェクトの名前を入力します。[選択（Select）] をクリックして既存のオブジェクトのリストからオブジェクトを選択するか、または新しい正規表現グループオブジェクトを作成できます。

要素	説明
オプション 値 （ヘッダー フラグ基準の場合）	検査するヘッダー フラグ。[Options] フィールドを使用して、完全一致（等しい）または部分一致（含む）のどちらを適用するかを指定します。 • [Header Flag Name]：選択したヘッダー フラグ名と一致します。 • AA（権威のある回答） • QR（クエリー） • RA（再帰可能） • RD（再帰拒否） • TC（切り捨て）フラグ ビット • [Header Flag Value]：指定した 16 ビットの 16 進数値と一致します。
Resource Record	照合するセクションをリストします。 • [Additional]：DNS 追加リソース レコード。 • [Answer]：DNS 回答リソース レコード。 • [Authority]：DNS 権限リソース レコード。

ESMTP マップの設定

[Add ESMTP Map]/[Edit ESMTP Map] ダイアログボックスを使用して、ESMTP 検査マップの一致基準と値を定義します。ESMTP ポリシーマップを使用すると、ESMTP インスペクションに使用するデフォルト設定値を変更できます。

ESMTP インスペクションでは、スパム、フィッシング、不正形式メッセージ攻撃、バッファオーバーフロー/アンダーフロー攻撃などの攻撃を検出します。また、アプリケーションセキュリティとプロトコル準拠により、正常な ESMTP メッセージだけを通し、各種の攻撃の検出や送受信者およびメール中継のブロックも行います。

ナビゲーション パス

[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択し、オブジェクトタイプセレクタから **[マップ（Maps）] > [ポリシーマップ（Policy Maps）] > [検査（Inspect）] > [ESMTP]** を選択します。テーブル内を右クリックしてから [新規オブジェクト（New Object）] を選択するか、行を右クリックしてから [オブジェクトの編集（Edit Object）] を選択します。

関連項目

- マップ オブジェクトについて

- インスペクションのプロトコルおよびマップの設定 （28 ページ）

フィールド リファレンス

表 *19 : [Add ESMTP Map]/[Edit ESMTP Map]* ダイアログボックス

要素	説明
名前	ポリシー オブジェクトの名前。最大 40 文字を使用できます。
説明	ポリシー オブジェクトの説明。最大 200 文字を使用できます。
[パラメータ（Parameters）] タブ	
Mask Server Banner	クライアントがサーバ情報を検出することを防ぐためにサーバ バナーをマスクするかどうか。
Configure Mail Relay ドメイン名 操作	ESMTP インスペクションでメール中継を検出するかどうか。このオプションを選択する場合は、検査しているドメイン名を入力し、メール中継が検出された場合に実行するアクションを選択します。
Special Character（ASA7.2.3+/PIX7.2.3+） 操作	送信者または受信者の電子メール アドレス内の特殊文字を検出するかどうか。このオプションを選択した場合は、特殊文字が検出された場合に実行するアクションを選択します。
Allow TLS（ASA7.2.3+、8.0.3+/PIX7.2.3） Action Log	セキュリティ アプライアンスで TLS プロキシを許可するかどうか。このオプションを選択した場合は、[Action Log] も選択して、TLS の検出時にログ エントリを作成できます。
[Match Condition and Action] タブ [Match All] テーブルに、ポリシー マップに含まれている基準が表示されます。各行には、各基準に一致する、または一致しないトラフィックを検査で検索するかどうか、検査される基準と値、および条件を満たすトラフィックに対して実行されるアクションが示されます。 • 基準を追加するには、[Add] ボタンをクリックし、[Match Condition and Action] ダイアログボックスに入力します（ESMTP ポリシー マップの [Add Match Condition and Action]/[Edit Match Condition and Action] ダイアログボックス （52 ページ）を参照）。 • 基準を編集するには、基準を選択し、[Edit] ボタンをクリックします。 • 基準を削除するには、基準を選択し、[Delete] ボタンをクリックします。	

要素	説明
カテゴリ	オブジェクトに割り当てられたカテゴリ。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。
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、ポリシー オブジェクトの上書きの許可および個々のデバイスのポリシー オブジェクト オーバーライドについてを参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）]ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）] フィールドには、このオブジェクトに対するオーバーライドを持つデバイスの数が表示されます。

ESMTP ポリシー マップの [Add Match Condition and Action]/[Edit Match Condition and Action] ダイアログボックス

[Add Match Condition and Action]/[Edit Match Condition and Action] ダイアログボックスを使用して、ESMTP ポリシー マップの一致基準、値、およびアクションを定義します。

このダイアログボックスのフィールドは、選択した基準によって変わります。次の基準を使用できます。

- [Body Length]：メッセージ本文の長さと一致します。
- [Body Line Length]：メッセージ本文の行の長さと一致します。
- [Commands]：ESMTP コマンドと一致します。
- [Command Recipient Count]：受信者の電子メール アドレスの数と一致します。
- [Command Line Length]：コマンドラインの文字数と一致します。
- [EHLO Reply Parameters]：ESMTP EHLO 応答パラメータと一致します。
- [Header Length]：ヘッダーの文字数と一致します。
- [Header Line Length]：メッセージ ヘッダー内の行の文字数と一致します。
- [To Recipients Count]：ヘッダーの To フィールドの受信者数と一致します。
- [Invalid Recipients Count]：ヘッダー内の無効な受信者数と一致します。
- [MIME File Type]：MIME ファイル タイプと一致します。
- [MIME Filename Length]：ファイル名の文字数と一致します。
- [MIME Encoding]：MIME 符号化スキームと一致します。
- [Sender Address]：送信元のアドレスと一致します。

- [送信元アドレスの長さ（Sender Address Length）]：送信元のアドレスの文字数と一致します。

ナビゲーション パス

[Policy Object Manager] で、[ESMTPマップの追加（Add ESMTP Map）]/[ESMTPマップの編集（Edit ESMTP Map）] ダイアログボックスの [一致条件とアクション（Match Condition and Action）] タブのテーブル内を右クリックして [行の追加（Add Row）] を選択するか、行を右クリックして [行の編集（Edit Row）] を選択します。 ESMTP マップの設定 （50 ページ） を参照してください。

関連項目

- マップ オブジェクトについて
- インスペクションのプロトコルおよびマップの設定 （28 ページ）

フィールド リファレンス

表 20 : ESMTP ポリシー マップの [Add Match Condition and Action]/[Edit Match Condition and Action] ダイアログボックス

要素	説明
基準	照合する ESMTP トラフィック基準を指定します。基準については、上記で説明しています。
タイプ（Type）	基準に一致する、または一致しないトラフィックをマップに含めるかどうかを指定します。たとえば、文字列「example.com」で [一致しない（Doesn’t Match）] を選択した場合、「example.com」を含むトラフィックはすべてマップの対象外になります。 • [Matches]：基準に一致する。 • [一致しない（Doesn't Match）]：基準に一致しない。
操作	定義された基準に一致するトラフィックに対してデバイスが適用するアクション。
可変フィールド 次のフィールドは、[Criterion] フィールドでの選択内容によって変わります。このリストは、表示されると想定されるフィールドのスーパーセットです。	
最大長	評価されるフィールドの長さ（バイト単位）。この基準は、長さが指定した数値よりも大きい場合に一致し、フィールドが指定した数値よりも小さい場合は一致しません。 ダイアログボックスでは、[Body Length] および [Header Length] を除き、1 ～ 4294967295 を指定できる有効な長さ範囲を指定します。

要素	説明
コマンド	検査する ESMTP コマンド バーブ。
Greater Than Count	評価される項目の数。この基準は、カウントが指定した数値よりも大きい場合に一致し、カウントが指定した数値よりも小さい場合は一致しません。
パラメータ	検査する ESMTP EHLO 応答パラメータ。
値	評価する正規表現。次のいずれかを選択できます。 • [Regular Expression]：パターン マッチングに使用する正規表現を定義する、正規表現オブジェクト。オブジェクトの名前を入力します。[選択（Select）] をクリックして既存のオブジェクトのリストからオブジェクトを選択するか、または新しい正規表現オブジェクトを作成できます。 • [Regular Expression Group]：パターン マッチングに使用する正規表現を定義する、正規表現グループ オブジェクト。オブジェクトの名前を入力します。[選択（Select）] をクリックして既存のオブジェクトのリストからオブジェクトを選択するか、または新しい正規表現グループオブジェクトを作成できます。
MIME Encoding	検査する MIME 符号化スキーム。

FTP マップの設定

[Add FTP Map]/[Edit FTP Map] ダイアログボックスを使用して、FTP 検査マップの一致基準と値を定義します。FTP マップを使用して、FTP PUT などの特定の FTP プロトコル方式がセキュリティ アプライアンスを通過して FTP サーバに到達するのをブロックできます。

ナビゲーション パス

[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択し、オブジェクトタイプセレクタから **[マップ（Maps）] > [ポリシーマップ（Policy Maps）] > [検査（Inspect）] > [FTP]** を選択します。テーブル内を右クリックしてから [新規オブジェクト（New Object）] を選択するか、行を右クリックしてから [オブジェクトの編集（Edit Object）] を選択します。

関連項目

- マップ オブジェクトについて
- インスペクションのプロトコルおよびマップの設定 （28 ページ）
- インスペクション ポリシーのクラス マップの設定 （34 ページ）

フィールド リファレンス

表 21 : [Add FTP Map]/[Edit FTP Map] ダイアログボックス

要素	説明
名前	ポリシー オブジェクトの名前。最大 40 文字を使用できます。
説明	ポリシー オブジェクトの説明。最大 200 文字を使用できます。
[パラメータ（Parameters）] タブ	
Mask Greeting Banner from Server	FTP サーバのグリーティング バナーをマスクして、クライアントがサーバ情報を検出するのを防ぐかどうか。
Mask Reply to SYST Command	**syst** コマンドへの応答をマスクして、クライアントがサーバー情報を検出するのを防ぐかどうか。
[Match Condition and Action] タブ [Match All] テーブルに、ポリシー マップに含まれている基準が表示されます。各行には、各基準に一致する、または一致しないトラフィックを検査で検索するかどうか、検査される基準と値、および条件を満たすトラフィックに対して実行されるアクションが示されます。 • 基準を追加するには、[Add] ボタンをクリックし、[Match Condition and Action] ダイアログボックスに入力します（FTP クラス マップおよび FTP ポリシー マップの [Add Match Condition and Action]/[Edit Match Condition and Action] ダイアログボックス （56 ページ）を参照）。 • 基準を編集するには、基準を選択し、[Edit] ボタンをクリックします。 • 基準を削除するには、基準を選択し、[Delete] ボタンをクリックします。	
カテゴリ	オブジェクトに割り当てられたカテゴリ。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。
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、ポリシー オブジェクトの上書きの許可および個々のデバイスのポリシー オブジェクト オーバーライドについてを参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）]ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）] フィールドには、このオブジェクトに対するオーバーライドを持つデバイスの数が表示されます。

要素	説明
Validate For [Validate] ボタン	オブジェクトを検証するデバイス プラットフォーム。オブジェクトを使用するプラットフォームを選択し、[検証（Validate）] をクリックして、そのオブジェクトがポリシー展開を回避するように設定されているか判断します。

FTP クラス マップおよび FTP ポリシー マップの [Add Match Condition and Action]/[Edit Match Condition and Action] ダイアログボックス

[Add FTP Match Criterion]/[Edit FTP Match Criterion] ダイアログボックス（FTP クラス マップの場合）または [Add Match Condition and Action]/[Edit Match Condition and Action] ダイアログボックス（FTP ポリシー マップの場合）を使用して、次の処理を行います。

- FTP クラス マップの一致基準と値を定義する。
- FTP ポリシー マップの作成時に FTP クラス マップを選択する。
- FTP ポリシー マップに一致基準、値、およびアクションを直接定義する。

このダイアログボックスのフィールドは、選択した基準、およびクラスマップとポリシーマップのどちらを作成しているかによって変わります。

ナビゲーション パス

FTP クラスマップを作成している場合は、Policy Object Manager で、FTP の [クラスマップの追加（Add Class Maps）]/[クラスマップの編集（Edit Class Maps）] ダイアログボックスのテーブル内を右クリックして [行の追加（Add Row）] を選択するか、行を右クリックして [行の編集（Edit Row）] を選択します。インスペクション ポリシーのクラス マップの設定 （34 ページ）を参照してください。

FTP ポリシーマップを作成している場合は、Policy Object Manager で、[FTPマップの追加（Add FTP Map）]/[FTPマップの編集（Edit FTP Map）] ダイアログボックスの [一致条件とアクション（Match Condition and Action）] タブのテーブル内を右クリックして [行の追加（Add Row）] を選択するか、行を右クリックして [行の編集（Edit Row）] を選択します。FTP マップの設定（54 ページ） を参照してください。

関連項目

- マップ オブジェクトについて
- インスペクションのプロトコルおよびマップの設定 （28 ページ）

フィールド リファレンス

表 *22 : FTP* クラス マップおよび *FTP* ポリシー マップの *[Add Match Condition and Action]/[Edit Match Condition and Action]* ダイアログボックス

要素	説明
一致タイプ（Match Type） クラス名 （ポリシー マップのみ）	既存の FTP クラス マップを使用するか、新規 FTP クラス マップを定義できます。 • [Use Specified Values]：このダイアログボックスでクラス マップを定義する場合。 • [Use Values in Class Map]：既存の FTP クラス マップ ポリシー オブジェクトを選択する場合。FTP クラスマップの名前を [クラス名（Class Name）] フィールドに入力します。[選択（Select）] をクリックしてリストからマップを選択するか、新しいクラスマップオブジェクトを作成します。
基準	照合する FTP トラフィック基準を指定します。 • [Request Command]：FTP 要求コマンドを照合します。 • [Filename]：FTP 転送のファイル名を照合します。 • [File Type]：FTP 転送のファイル タイプを照合します。 • [Server]：FTP サーバ名を照合します。 • [Username]：FTP ユーザ名を照合します。
タイプ（Type）	基準に一致する、または一致しないトラフィックをマップに含めるかどうかを指定します。たとえば、文字列「example.com」で [一致しない（Doesn’t Match）] を選択した場合、「example.com」を含むトラフィックはすべてマップの対象外になります。 • [Matches]：基準に一致する。 • [一致しない（Doesn't Match）]：基準に一致しない。
操作 （ポリシー マップのみ）	定義された基準に一致するトラフィックに対してデバイスが適用するアクション。
可変フィールド 次のフィールドは、[Criterion] フィールドでの選択内容によって変わります。このリストは、表示されると想定されるフィールドのスーパーセットです。	

要素	説明
Request Commands	検査する FTP コマンド。 • [Append (APPE)]：ファイルに追加します。 • [Delete (DELE)]：サーバ サイトでファイルを削除します。 • [Help (HELP)]：サーバからヘルプ情報を提供します。 • [Put (PUT)]：stor（ファイルの保存）コマンドの FTP クライアント コマンド。 • [Rename From (RNFR)]：名前変更する元のファイル名を指定します。 • [Server Specific Command (SITE)]：サーバに固有のコマンドを指定します。通常、リモート管理に使用します。 • [Change to Parent (CDUP)]：現在の作業ディレクトリの親ディレクトリに変更します。 • [Get (GET)]：retr（ファイルの取得）コマンドの FTP クライアント コマンド。 • [Create Directory (MKD)]：ディレクトリを作成します。 • [Remove Directory (RMD)]：ディレクトリを削除します。 • [Rename To (RNTO)]：名前変更する先の名前を指定します。 • [Store File with Unique Name (STOU)]：ファイルを一意のファイル名で保存します。
値	評価する正規表現。次のいずれかを選択できます。 • [Regular Expression]：パターン マッチングに使用する正規表現を定義する、正規表現オブジェクト。オブジェクトの名前を入力します。[選択（Select）] をクリックして既存のオブジェクトのリストからオブジェクトを選択するか、または新しい正規表現オブジェクトを作成できます。 • [Regular Expression Group]：パターン マッチングに使用する正規表現を定義する、正規表現グループ オブジェクト。オブジェクトの名前を入力します。[選択（Select）] をクリックして既存のオブジェクトのリストからオブジェクトを選択するか、または新しい正規表現グループオブジェクトを作成できます。

GTP マップの設定

[Add GTP Map]/[Edit GTP Map] ダイアログボックスを使用して、GTP 検査マップの一致基準と値を定義します。

GPRS Tunnel Protocol（GTP; GPRS トンネル プロトコル）は、モバイル サブスクライバに対して、GSM ネットワークと企業ネットワークまたはインターネットの間の中断のない接続を提供します。GTP は、トンネリング メカニズムを使用して、ユーザー データ パケットを伝送するためのサービスを提供します。

GTP マップ オブジェクトを使用すると、GTP アプリケーション インスペクションに使用するデフォルト設定値を変更できます。GTP プロトコルは、インターネットなどの TCP/IP ネットワークへのワイヤレス接続にセキュリティを提供する設計になっています。GTP マップを使用して、タイムアウト値、メッセージ サイズ、トンネル数、およびセキュリティ アプライアンスを通過する GTP バージョンを制御できます。

バージョン 4.18 以降、Cisco Security Manager は ASA 9.10.1 のアンチリプレイ機能をサポートします。データパケットのリプレイを有効にすることで、ネットワークはリプレイアタックから保護されます。

ヒント　GTP インスペクションには、特別なライセンスが必要です。必要なライセンスがない場合は、GTP マップを展開しようとした場合にデバイス エラーが発生します。

ナビゲーション パス

[管理（Manage）]>[ポリシーオブジェクト（Policy Objects）] を選択し、オブジェクトタイプセレクタから **[マップ（Maps）]>[ポリシーマップ（Policy Maps）]>[検査（Inspect）]>[GTP]** を選択します。作業領域内を右クリックしてから [新規オブジェクト(New Object] を選択するか、行を右クリックしてから [オブジェクトの編集（Edit Object）] を選択します。

関連項目

- マップ オブジェクトについて
- インスペクションのプロトコルおよびマップの設定　（28 ページ）

フィールド リファレンス

表 23 : [Add GTP Map]/[Edit GTP Map] ダイアログボックス

要素	説明
名前	ポリシー オブジェクトの名前。最大40 文字を使用できます。
説明	ポリシー オブジェクトの説明。最大 200 文字を使用できます。

要素	説明
[パラメータ（Parameters）] タブ	
Country and Network Codes Table	マップに含める 3 桁の Mobile Country Code（mcc; モバイル国コード）および Mobile Network Code（mnc; モバイル ネットワーク コード）。コードは 000 ～ 999 です。 • コードを追加するには、[Add] ボタンをクリックし、ダイアログボックスに入力します。 • 行を編集するには、行を選択し、[Edit] ボタンをクリックします。 • 行を削除するには、行を選択し、[Delete] ボタンをクリックします。
Permit Response Table	応答の送信先とは異なる GSN からの GTP 応答を許可するネットワーク/ホスト ポリシー オブジェクト。 • オブジェクトを追加するには、[Add] ボタンをクリックし、ダイアログボックスに入力します。詳細については、[Add Permit Response]/[Edit Permit Response] ダイアログボックス （63 ページ）を参照してください。 • 行を編集するには、行を選択し、[Edit] ボタンをクリックします。 • 行を削除するには、行を選択し、[Delete] ボタンをクリックします。
Request Queue	キュー内で許可される最大要求数。この上限に達した後に新しい要求が到着すると、最も長い時間キューに入っていた要求が削除されます。値は 1 ～ 9999999 です。デフォルトは 200 です。
Tunnel Limit	許可されるトンネルの最大数。
Permit Errors	エラーがあるか GTP バージョンが異なるパケットを許可するかどうか。デフォルトでは、解析時に失敗したすべての無効パケットがドロップされます。

要素	説明
データパケットリプレイウィンドウの有効化（Enable Data Packet Replay Window）	チェックボックスをオンにしてアンチリプレイを設定し、4 つのウィンドウサイズ（128、256、512、または 1024）からいずれかを選択します。ウィンドウサイズ外のメッセージはドロップされます。 GTP マップポリシーの設定については、[検査/アプリケーションFWルールの追加または編集（Add or Edit Inspect/Application FW Rule）] ウィザード、[検査対象プロトコル（Inspected Protocol）] ページ （22 ページ）を参照してください。
ヘッダーチェックの有効化（Enable Header Check）	データパケットのヘッダーチェックを有効にするには、このチェックボックスをオンにします。
アンチユーザースプーフィング（Anti-User Spoofing）	このフィールドは、[ヘッダーチェックの有効化（Enable Header Check）] チェックボックスをオンにした場合にのみ有効になります。関連するオプションを選択します。 • [バイパス（Bypass）]：ヘッダーチェックに合格したパケットを転送します。 • [ドロップ（Drop）]：ヘッダーチェックに合格したパケットをドロップします。
[Edit Timeouts] ボタン	このボタンをクリックして、さまざまな操作のタイムアウト値を設定します。これらのオプションの詳細については、[GTP Map Timeouts] ダイアログボックス （63 ページ）を参照してください。
ロケーションロギングの有効化（Enable Location Logging）	このチェックボックスをオンにすると、モバイル国コードとモバイルネットワークコードを含む syslog メッセージを介して位置情報が取得されます。この syslog メッセージは、GTPv0/v1 の Gn/Gp または GTPv2 の S5/S8 で PDP コンテキストをアクティブ化または更新するときに表示されます。

要素	説明
セルIDの有効化（Enable Cell ID）	（任意）このチェックボックスをオンにして、セル ID を syslog メッセージに追加します。 （注） このオプションは、[ロケーションロギングの有効化（Enable Location Logging）] チェックボックスをオンにした場合にのみ有効になります。
[Match Condition and Action] タブ [Match All] テーブルに、ポリシー マップに含まれている基準が表示されます。各行には、各基準に一致する、または一致しないトラフィックを検査で検索するかどうか、検査される基準と値、および条件を満たすトラフィックに対して実行されるアクションが示されます。 • 基準を追加するには、[追加（Add）]ボタンをクリックし、[一致条件とアクション（Match Condition and Action）] ダイアログボックスに入力します（GTP ポリシー マップの [Add Match Condition and Action]/[Edit Match Condition and Action] ダイアログボックス （64 ページ）を参照）。 • 基準を編集するには、基準を選択し、[Edit] ボタンをクリックします。 • 基準を削除するには、基準を選択し、[Delete] ボタンをクリックします。	
カテゴリ	オブジェクトに割り当てられたカテゴリ。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。
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、ポリシー オブジェクトの上書きの許可および個々のデバイスのポリシー オブジェクト オーバーライドについてを参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）] ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）] フィールドには、このオブジェクトに対するオーバーライドを持つデバイスの数が表示されます。
Validate For [Validate] ボタン	オブジェクトを検証するデバイス プラットフォーム。オブジェクトを使用するプラットフォームを選択し、[検証（Validate）] をクリックして、そのオブジェクトがポリシー展開を回避するように設定されているか判断します。

[Add Country Network Codes]/[Edit Country Network Codes] ダイアログボックス

[Add Country Network Codes]/[Edit Country Network Codes] ダイアログボックスを使用して、Mobile Country Code（mcc; モバイル国コード）および Mobile Network Code（mnc; モバイル ネットワーク コード）値を GTP ポリシー マップに追加します。コードは 000 ～ 999 です。

ナビゲーション パス

[GTPマップの追加（Add GTP Map）]/[GTPマップの編集（Edit GTP Map）] ダイアログボックスで、[国コードとネットワークコード（Country and Network codes）] テーブルの [追加（Add）] ボタンをクリックするか、行を選択して [編集（Edit）] ボタンをクリックします。GTP マップの設定 （59 ページ） を参照してください。

[Add Permit Response]/[Edit Permit Response] ダイアログボックス

[Add Permit Response]/[Edit Permit Response] ダイアログボックスを使用して、応答の送信先とは異なる GSN からの GTP 応答を許可します。

トラフィックの宛先（[宛先オブジェクトグループ（To Object Group）]）および送信元（[送信元オブジェクトグループ（From Object Group）]）を定義するネットワーク/ホストポリシーオブジェクトの名前を入力します。[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。[オブジェクトセレクタ（Object Selector）] ダイアログボックスの [作成（Create）] ボタンをクリックして、新しいオブジェクトを作成することもできます。

「any」という名前のネットワーク/ホストオブジェクトは使用できません。

ナビゲーション パス

[GTPマップの追加（Add GTP Map）]/[GTPマップの編集（Edit GTP Map）] ダイアログボックスで、[応答の許可（Permit Response）] テーブルの [追加（Add）] ボタンをクリックするか、行を選択して [編集（Edit）] ボタンをクリックします。GTP マップの設定 （59 ページ） を参照してください。

[GTP Map Timeouts] ダイアログボックス

[GTP Map Timeouts] ダイアログボックスを使用して、GTP マップのタイムアウト値を設定します。

ナビゲーション パス

[GTPマップの追加（Add GTP Map）]/[GTPマップの編集（Edit GTP Map）] ダイアログボックスで、[パラメータ（Parameters）] タブの [タイムアウトの編集（Edit Timeouts）] ボタンをクリックします。GTP マップの設定 （59 ページ）を参照してください。

フィールド リファレンス

表 24 : [GTP Map Timeouts] ダイアログボックス

要素	説明
GSN タイムアウト（GSN Timeout）（ASA 9.5(1) より前） エンドポイントタイムアウト（Endpoint Timeout）（ASA 9.5(1) 以降）	非活動状態のままこの時間（hh:mm:ss）が経過すると GSN が削除されます。デフォルトは 30 分です。すぐにティアダウンしない場合は、0 を入力します。
PDP Context Timeout	PDP コンテキストの受信を開始する前に許容される最大期間（hh:mm:ss）。デフォルトは 30 分です。制限なしを指定する場合は、0 を入力します。
Request Queue Timeout	GTP メッセージの受信を開始する前に許容される最大期間（hh:mm:ss）。デフォルトは 60 秒です。制限なしを指定する場合は、0 を入力します。
Signaling Connections Timeout	非活動状態のままこの時間（hh:mm:ss）が経過すると GTP シグナリングが削除されます。デフォルトは 30 分です。シグナルを削除しない場合は、0 を入力します。
Tunnel Timeout	非活動状態のままこの時間（hh:mm:ss）が経過すると GTP トンネルがティアダウンされます。デフォルトは 60 秒です（PDP コンテキストの削除要求を受信していない場合）。すぐにティアダウンしない場合は、0 を入力します。
T3 Response Timeout	接続を除去する前に応答を待機する最大時間。

GTP ポリシー マップの [Add Match Condition and Action]/[Edit Match Condition and Action] ダイアログボックス

[Add Match Condition and Action]/[Edit Match Condition and Action] ダイアログボックスを使用して、GTP ポリシー マップの一致基準、値、およびアクションを定義します。

このダイアログボックスのフィールドは、選択した基準によって変わります。

ナビゲーション パス

[Policy Object Manager] で、[GTPマップの追加（Add GTP Map）]/[GTPマップの編集（Edit GTP Map）] ダイアログボックスの [一致条件とアクション（Match Condition and Action）] タブのテーブル内を右クリックして [行の追加（Add Row）] を選択するか、行を右クリックして [行の編集（Edit Row）] を選択します。 GTP マップの設定 （59 ページ） を参照してください。

関連項目

- マップ オブジェクトについて
- インスペクションのプロトコルおよびマップの設定 （28 ページ）

フィールド リファレンス

表 *25 : GTP* ポリシー マップの *[Add Match Condition and Action]/[Edit Match Condition and Action]* ダイアログボックス

要素	説明
基準	照合する GTP トラフィック基準を指定します。 • [Access Point Name]：アクセス ポイント名を照合します。このため、GTP アプリケーションのインスペクションがイネーブルになっている場合にドロップするアクセス ポイントを定義できます。 • [Message ID]：ドロップするメッセージの数値 ID を照合します。デフォルトでは、すべての有効なメッセージ ID が許可されます。 • [Message Length]：UDP パケットの長さを照合します。この基準を使用して、UDP ペイロードに対して許可されるメッセージの最大長のデフォルトを変更します。 • [Version]：GTP バージョンを照合します。 • [MSISDN]：MSISDN を正規表現またはクラスと照合し、一致する MSISDN を持つすべての GTP パケットをドロップします。 • [選択モード（Selection Mode）]：0 ～ 3 の範囲。
タイプ（Type）	基準に一致する、または一致しないトラフィックをマップに含めるかどうかを指定します。たとえば、文字列「example.com」で [一致しない（Doesn’t Match）] を選択した場合、「example.com」を含むトラフィックはすべてマップの対象外になります。 • [Matches]：基準に一致する。 • [一致しない（Doesn't Match）]：基準に一致しない。
操作	定義された基準に一致するトラフィックに対してデバイスが適用するアクション。 • [Drop Packet]：デフォルトでは、解析時に失敗したすべての無効パケットがドロップされます。 • Drop Packet and Log • レート制限

要素	説明
可変フィールド 次のフィールドは、[Criterion] フィールドでの選択内容によって変わります。このリストは、表示されると想定されるフィールドのスーパーセットです。	
アクセス ポイント名（Access Point Name）	GTP アプリケーションのインスペクションがイネーブルになっている場合に作用するアクセス ポイント。 • [Specified By]：ドロップするアクセス ポイント名。デフォルトでは、有効な APN を持つすべてのメッセージが検査され、すべての APN が許可されます。 • [Regular Expression]：パターン マッチングに使用する正規表現を定義する、正規表現オブジェクト。オブジェクトの名前を入力します。[選択（Select）] をクリックして既存のオブジェクトのリストからオブジェクトを選択するか、または新しい正規表現オブジェクトを作成できます。 • [Regular Expression Group]：パターン マッチングに使用する正規表現を定義する、正規表現グループ オブジェクト。オブジェクトの名前を入力します。[選択（Select）] をクリックして既存のオブジェクトのリストからオブジェクトを選択するか、または新しい正規表現グループオブジェクトを作成できます。
ID タイプ	操作対象のメッセージの数値 ID。 • [Value]：単一のメッセージ ID。値は、1 ～ 255 です。 • [Range]：メッセージ ID の範囲。範囲は 1 ～ 255 です。
最小長（Minimum Length）	UDP ペイロード内の最小バイト数。
最大長（Maximum Length）	UDP ペイロード内の最大バイト数。
バージョン	バージョン 4.9 以降、Security Manager は、ASA デバイス 9.5(1) 以降の GTP マップ オブジェクトで GPRS トンネル プロトコル（GTP）v2 および拡張 v1 のサポートを提供します。GTPv1 と GTPv2 に個別のメッセージ ID 照合を設定できるようになりました。 ASA デバイス 9.5(1) 以降の場合、条件としてメッセージ ID を選択すると、v1 と v2 の 2 つのバージョンのオプションが表示されます。v1 または v2 を選択し、1 から 255 までの単一の値、または 1 から 255 までの値の範囲を入力します。

要素	説明
Version Type	ASA バージョン 9.5(1) より前のバージョン：バージョン 0 を指定するには 0 を使用し、バージョン 1 を指定するには 1 を使用します。バージョン 0 の GTP ではポート 2123 を使用し、バージョン 1 ではポート 3386 を使用します。デフォルトでは、すべての GTP バージョンが許可されます。
正規表現	バージョン 4.18 以降、Cisco Security Manager では、正規表現を使用して MSISDN を設定し、一致する MSISDN を持つすべての GTP パケットをドロップできます。このフィールドは、[条件（Criterion）] ドロップダウンで MSISDN を選択すると表示されます。
正規表現グループ（Regular Expression Group）	バージョン 4.18 以降、Cisco Security Manager では、正規表現クラスを使用して MSISDN を設定し、一致する MSISDN を持つすべての GTP パケットをドロップできます。このフィールドは、[条件（Criterion）] ドロップダウンで MSISDN を選択すると表示されます。
モード値（Mode Value）	[条件（Criterion）] ドロップダウンで [選択項目（Selection）] が選択されている場合、このフィールドが表示されます。モード値を 0 ～ 3 の範囲で入力します。これは必須フィールドです。

H.323 マップの設定

[Add H.323 Map]/[Edit H.323 Map] ダイアログボックスを使用して、H.323 検査マップの一致基準と値を定義します。H.323 ポリシー マップを使用すると、H.323 インスペクションに使用するデフォルト設定値を変更できます。

H.323 インスペクションでは、Cisco CallManager や VocalTec Gatekeeper などの H.323 準拠アプリケーションがサポートされます。H.323 は、国際電気通信連合によって定義されている、LAN を介したマルチメディア会議用のプロトコル群です。セキュリティ アプライアンスでは、バージョン 4 までの H.323 がサポートされます。これには、H.323 v3 機能である Multiple Calls on One Call Signaling Channel（1 つのコール シグナリング チャネルでの複数コール）が含まれます。

H.323 インスペクションがイネーブルになっている場合、セキュリティ アプライアンスでは、H.323 バージョン 3 で導入された機能である同じコール シグナリング チャネルでの複数コールがサポートされます。この機能により、コール セットアップ時間が短縮され、セキュリティ アプライアンス上で使用されるポート数が削減されます。H.323 インスペクションの 2 つの主要機能は次のとおりです。

- H.225 と H.245 の両メッセージ内に埋め込まれている必要な IPv4 アドレスを NAT 処理します。H.323 メッセージは PER 符号化フォーマットで符号化されているため、セキュリティ アプライアンスでは、ASN.1 デコーダを使用して H.323 メッセージをデコードします。
- ネゴシエートされた H.245 と RTP/RTCP 接続をダイナミックに割り当てます。

ナビゲーション パス

[管理（Manage）]>[ポリシーオブジェクト（Policy Objects）]を選択し、オブジェクトタイプセレクタから**[マップ（Maps）]>[ポリシーマップ（Policy Maps）]>[検査（Inspect）]>[H.323 (ASA/PIX/FWSM)]**を選択します。作業領域内を右クリックしてから [新規オブジェクト（New Object）] を選択するか、行を右クリックしてから [オブジェクトの編集（Edit Object）] を選択します。

関連項目

- マップ オブジェクトについて
- インスペクションのプロトコルおよびマップの設定 （28 ページ）
- インスペクション ポリシーのクラス マップの設定 （34 ページ）

フィールド リファレンス

表 26 : [Add H.323 Map]/[Edit H.323 Map] ダイアログボックス

要素	説明
名前	ポリシー オブジェクトの名前。最大 40 文字を使用できます。
説明	ポリシー オブジェクトの説明。最大 200 文字を使用できます。
[パラメータ（Parameters）] タブ	
HSI Group table	マップに含める HSI グループ。グループ番号、HSI ホストの IP アドレス、およびセキュリティ アプライアンスに接続しているクライアントの IP アドレスとインターフェイス名がテーブルに表示されます。グループあたり最大 5 つの HSI ホスト、HSI グループあたり最大 10 個のエンド ポイントが許可されます。 • グループを追加するには、[Add] ボタンをクリックし、ダイアログボックスに入力します（[Add HSI Group]/[Edit HSI Group] ダイアログボックス （70 ページ）を参照）。 • グループを編集するには、グループを選択し、[Edit] ボタンをクリックします。 • グループを削除するには、グループを選択し、[Delete] ボタンをクリックします。
Call Duration Limit	秒単位でのコール期間制限。範囲は 0:0:0 ～ 1163:0:0 です。値 0 は、タイムアウトしないことを示します。

要素	説明
Enforce Presence of Calling and Called Party Numbers	コールの確立で使用されるコールと着番号を強制するかどうか。
H.460.18 の SETUP の前に FACILITY メッセージを許可する（Allow the facility message before SETUP for H.460.18）	着信メッセージ手順の一部として、SETUP メッセージの前に FACILITY メッセージを送信できるようにするかどうか。 （注） H.460.18 では、ネットワーク アドレス変換機能とファイアウォールを越えて H.323 シグナリングを伝送するための方法が定義されています。
Check State Transition on H.225 Messages	H.225 メッセージで状態チェック検証をイネーブルにするかどうか。
Check State Transition on RAS Messages	RAS メッセージで状態チェック検証をイネーブルにするかどうか。
Create Pinholes on Seeing RCF Packets	ネットワークの内部にゲートキーパーがある場合に、H.323 エンドポイント間でコールの確立をイネーブルにするかどうか。デバイスは、Registration Request/Registration Confirm（RRQ/RCF）メッセージに基づいてコールのピンホールを開けます。これらの RRQ/RCF メッセージは Gatekeeper との間で送受信されるので、発信側エンドポイントの IP アドレスは不明で、デバイスは発信元 IP アドレス/ポート 0/0 を通じてピンホールを開きます。 このオプションは、ASA 8.0(5)+ デバイスで使用可能です。
Check for H.245 Tunneling 操作	H.245 トンネル ブロッキングを実施し、[Action] リストボックスで選択したアクションを実行するかどうか。
Check RTP Packets for Protocol Conformance	プロトコル準拠のために、RTP パケットのフローがピンホールを経由することを調べるかどうか。
Payload Type must be Audio or Video based on Signaling Exchange	シグナリング交換に基づいてペイロード タイプをオーディオまたはビデオに強制するかどうか。

要素	説明
[Match Condition and Action] タブ [Match All] テーブルに、ポリシー マップに含まれている基準が表示されます。各行には、各基準に一致する、または一致しないトラフィックを検査で検索するかどうか、検査される基準と値、および条件を満たすトラフィックに対して実行されるアクションが示されます。 • 基準を追加するには、[Add] ボタンをクリックし、[Match Condition and Action] ダイアログボックスに入力します（H.323 クラス マップおよび H.323 ポリシー マップの [Add Match Condition and Action]/[Edit Match Condition and Action] ダイアログボックス （72 ページ）を参照）。 • 基準を編集するには、基準を選択し、[Edit] ボタンをクリックします。 • 基準を削除するには、基準を選択し、[Delete] ボタンをクリックします。	
カテゴリ	オブジェクトに割り当てられたカテゴリ。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。
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、ポリシー オブジェクトの上書きの許可および個々のデバイスのポリシー オブジェクト オーバーライドについてを参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）] ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）] フィールドには、このオブジェクトに対するオーバーライドを持つデバイスの数が表示されます。

[Add HSI Group]/[Edit HSI Group] ダイアログボックス

[Add HSI Group]/[Edit HSI Group] ダイアログボックスを使用して、H.323 ポリシー インスペクション マップに HSI グループを追加します。

ナビゲーション パス

[H.323マップの追加（Add H.323 Map）]/[H.323マップの編集（Edit H.323 Map）] ダイアログボックスの [パラメータ（Parameters）] タブで、[HSIグループ（HSI group）] テーブルの [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。 H.323 マップの設定 （67 ページ）を参照してください。

フィールド リファレンス

表 27 : [Add HSI Group]/[Edit HSI Group] ダイアログボックス

要素	説明
グループ ID（Group ID）	HSI グループの ID 番号（0 ～ 2147483647）。
IPアドレス	HSI ホストの IP アドレス。
Endpoint table	HSI グループに関連付けられているエンドポイント。グループあたり最大 10 個のエンド ポイントを追加できます。エンド ポイントごとに、IP アドレスとインターフェイス ポリシー グループを指定します。 • エンド ポイントを追加するには、[Add] ボタンをクリックし、ダイアログボックスに入力します（ [Add HSI Endpoint IP Address]/[Edit HSI Endpoint IP Address] ダイアログボックス （71 ページ）を参照）。 • エンド ポイントを編集するには、エンド ポイントを選択し、[Edit] ボタンをクリックします。 • エンドポイントを削除するには、エンドポイントを選択し、[Delete] ボタンをクリックします。

[Add HSI Endpoint IP Address]/[Edit HSI Endpoint IP Address] ダイアログボックス

[Add HSI Endpoint IP Address]/[Edit HSI Endpoint IP Address] ダイアログボックスを使用して、HSI グループにエンド ポイントを追加します。

ナビゲーション パス

[HSI グループの追加（Add HSI Group）]/[HSI グループの編集（Edit HSI Group）] ダイアログボックスで、エンドポイントテーブルの [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。 H.323 マップの設定 （67 ページ）を参照してください。

フィールド リファレンス

表 28 : [Add HSI Endpoint IP Address]/[Edit HSI Endpoint IP Address] ダイアログボックス

要素	説明
Network/Host	エンド ポイント ホストまたはネットワークの IP アドレス。

要素	説明
インターフェイス	セキュリティ アプライアンスに接続されているインターフェイスを識別するインターフェイス ポリシー グループ。ポリシーグループの名前を入力するか、[選択（Select）] をクリックしてリストから選択します。ここで新しいポリシーグループを作成することもできます。

H.323 クラス マップおよび H.323 ポリシー マップの [Add Match Condition and Action]/[Edit Match Condition and Action] ダイアログボックス

[Add H.323 Match Criterion]/[Edit H.323 Match Criterion] ダイアログボックス（H.323 クラス マップの場合）または [Add Match Condition and Action]/[Edit Match Condition and Action] ダイアログボックス（H.323 ポリシー マップの場合）を使用して、次の処理を行います。

- H.323 クラス マップの一致基準と値を定義する。
- H.323 ポリシー マップの作成時に H.323 クラス マップを選択する。
- H.323 ポリシー マップに一致基準、値、およびアクションを直接定義する。

このダイアログボックスのフィールドは、選択した基準、およびクラスマップとポリシーマップのどちらを作成しているかによって変わります。

ナビゲーション パス

H.323 クラスマップを作成している場合は、Policy Object Manager で、H.323 の [クラスマップの追加（Add Class Maps）]/[クラスマップの編集（Edit Class Maps）] ダイアログボックスのテーブル内を右クリックして [行の追加（Add Row）] を選択するか、行を右クリックして [行の編集（Edit Row）] を選択します。インスペクション ポリシーのクラス マップの設定 （34 ページ）を参照してください。

H.323 ポリシーマップを作成している場合は、Policy Object Manager で、[H.323マップの追加（Add H.323 Map）]/[H.323マップの編集（Edit H.323 Map）] ダイアログボックスの [一致条件とアクション（Match Condition and Action）] タブのテーブル内を右クリックして [行の追加（Add Row）] を選択するか、行を右クリックして [行の編集（Edit Row）] を選択します。H.323 マップの設定 （67 ページ） を参照してください。

関連項目

- マップ オブジェクトについて
- インスペクションのプロトコルおよびマップの設定 （28 ページ）

フィールド リファレンス

表 *29 : H.323* クラス マップおよび *H.323* ポリシー マップの *[Add Match Condition and Action]/[Edit Match Condition and Action]* ダイアログボックス

要素	説明
一致タイプ（Match Type） クラス名 （ポリシー マップのみ）	既存の H.323 クラス マップを使用するか、新規 H.323 クラス マップを定義できます。 • [Use Specified Values]：このダイアログボックスでクラス マップを定義する場合。 • [Use Values in Class Map]：既存の H.323 クラス マップ ポリシー オブジェクトを選択する場合。H.323 クラスマップの名前を [クラス名（Class Name）] フィールドに入力します。[選択（Select）] をクリックしてリストからマップを選択するか、新しいクラス マップオブジェクトを作成します。
基準	照合する H.323 トラフィック基準を指定します。 • [Called Party]：着信ユーザ アドレスを照合します。 • [Calling Party]：発信側アドレスを照合します。 • [Media Type]：メディア タイプを照合します。
タイプ（Type）	基準に一致する、または一致しないトラフィックをマップに含めるかどうかを指定します。たとえば、文字列「example.com」で [一致しない（Doesn’t Match）] を選択した場合、「example.com」を含むトラフィックはすべてマップの対象外になります。 • [Matches]：基準に一致する。 • [一致しない（Doesn't Match）]：基準に一致しない。
操作 （ポリシー マップのみ）	定義された基準に一致するトラフィックに対してデバイスが適用するアクション。
可変フィールド 次のフィールドは、[Criterion] フィールドでの選択内容によって変わります。このリストは、表示されると想定されるフィールドのスーパーセットです。	

要素	説明
値	評価する正規表現。次のいずれかを選択できます。 • [Regular Expression]：パターン マッチングに使用する正規表現を定義する、正規表現オブジェクト。オブジェクトの名前を入力します。[選択（Select）]をクリックして既存のオブジェクトのリストからオブジェクトを選択するか、または新しい正規表現オブジェクトを作成できます。 • [Regular Expression Group]：パターン マッチングに使用する正規表現を定義する、正規表現グループ オブジェクト。オブジェクトの名前を入力します。[選択（Select）]をクリックして既存のオブジェクトのリストからオブジェクトを選択するか、または新しい正規表現グループオブジェクトを作成できます。
メディア タイプ（Media Type）	検査するメディアのタイプ（オーディオ、ビデオ、またはデータ）。

ASA 7.1.x、PIX 7.1.x、FWSM 3.x、および IOS デバイスの HTTP マップの設定

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き PIX、FWSM、および IPS の機能をサポートしていますが、拡張機能はサポートしていません。

[Add HTTP Map]/[Edit HTTP Map] ダイアログボックスを使用して、ASA 7.1.x、PIX 7.1.x、FWSM 3.x、および IOS デバイスの HTTP マップを定義します。

アプリケーションファイアウォールとも呼ばれる拡張HTTPインスペクション機能では、HTTP メッセージが RFC 2616 に準拠していること、RFC で規定された方式を使用していること、およびその他のさまざまな基準に準拠していることを確認します。このことは、HTTP メッセージを使用してネットワーク セキュリティ ポリシーを回避することによる攻撃を防止するのに役立ちます。

HTTP マップで HTTP インスペクションをイネーブルにした場合は、リセットおよびログ アクションを伴う厳格な HTTP インスペクションがデフォルトでイネーブルになります。インスペクションの失敗に対して実行するアクションは変更できますが、HTTP マップがイネーブルになっているかぎり、厳格なインスペクションはディセーブルにできません。Cisco Security Manager では、**http-map** コマンドを使用してデバイスにマップを設定します。

ナビゲーション パス

[管理（Manage）]>[ポリシーオブジェクト（Policy Objects）] を選択し、オブジェクトタイプ セレクタから **[マップ（Maps）]>[ポリシーマップ（Policy Maps）]>[検査（Inspect）]>[HTTP**

（**ASA 7.1.x/PIX 7.1.x/FWSM3.x/IOS**）] を選択します。作業領域内を右クリックしてから [新規オブジェクト(New Object] を選択するか、行を右クリックしてから [オブジェクトの編集（Edit Object）] を選択します。

関連項目

- マップ オブジェクトについて
- インスペクションのプロトコルおよびマップの設定 （28 ページ）

フィールド リファレンス

表 30 : ASA 7.1.x/PIX 7.1.x/FWSM 3.x/IOS デバイスの [Add HTTP Map]/[Edit HTTP Map] ダイアログボックス

要素	説明
名前	ポリシー オブジェクトの名前。最大 40 文字を使用できます。
説明	ポリシー オブジェクトの説明。最大 200 文字を使用できます。
[一般（General）] タブ	準拠していない HTTP 要求が受信された場合に実行するアクションを定義し、コンテンツ タイプの検証をイネーブルにします。オプションの詳細については、 HTTP マップの [General] タブ （76 ページ）を参照してください。
[Entity Length] タブ	HTTP コンテンツの長さが設定したターゲットの範囲外の場合に実行するアクションを定義します。オプションの詳細については、HTTP マップの [Entity Length] タブ （78 ページ）を参照してください。
[RFC Request Method] タブ	HTTP 要求で特定の RFC 要求メソッドが使用されている場合にセキュリティ アプライアンスが実行する必要のあるアクションを定義します。オプションの詳細については、 HTTP マップの [RFC Request Method] タブ （79 ページ）を参照してください。
[Extension Request Method] タブ	HTTP 要求で特定の拡張要求メソッドが使用されている場合に実行されるアクションを定義します。オプションの詳細については、HTTP マップの [Extension Request Method] タブ （81 ページ）を参照してください。
[Port Misuse] タブ	特定の望ましくないアプリケーションが検出された場合に実行するアクションを定義します。オプションの詳細については、HTTP マップの [Port Misuse] タブ （82 ページ）を参照してください。
[Transfer Encoding] タブ	HTTP 要求で特定の転送符号化タイプが使用されている場合に実行されるアクションを定義します。オプションの詳細については、HTTP マップの [Transfer Encoding] タブ （83 ページ）を参照してください。

要素	説明
カテゴリ	オブジェクトに割り当てられたカテゴリ。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。
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、ポリシー オブジェクトの上書きの許可および個々のデバイスのポリシー オブジェクト オーバーライドについてを参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）]ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）]フィールドには、このオブジェクトに対するオーバーライドを持つデバイスの数が表示されます。

HTTP マップの [General] タブ

[General] タブを使用して、準拠していない HTTP 要求が受信された場合に実行するアクションを定義し、コンテンツ タイプの検証をイネーブルにします。

ナビゲーション パス

ASA 7.1.x/PIX 7.1.x/FWSM 3.x/IOS デバイスの [Add HTTP Map]/[Edit HTTP Map] ダイアログボックスの [General] タブをクリックします。 ASA 7.1.x、PIX 7.1.x、FWSM 3.x、および IOS デバイスの HTTP マップの設定 （74 ページ） を参照してください。

関連項目

- 詳細については、ポリシー オブジェクトの上書きの許可および個々のデバイスのポリシー オブジェクト オーバーライドについてを参照してください。
- インスペクションのプロトコルおよびマップの設定 （28 ページ）

フィールド リファレンス

表 *31 : HTTP* マップの *[General]* タブ

要素	説明
Take action for non-RFC 2616 compliant traffic	RFC 2616 に準拠しないトラフィックに対して実行するアクションを設定するかどうか。指定できるアクションは、次のとおりです。 • [Allow Packet]：メッセージを許可します。 • [Drop Packet]：接続を閉じます。 • [Reset Connection]（デフォルト）：TCP リセット メッセージをクライアントとサーバに送信します。 [Syslogの生成（Generate Syslog）] を選択して、非準拠トラフィックが検出された場合にメッセージを syslog に書き込むこともできます。
Verify Content-type field belongs to the supported internal content-type list.	サポートされる内部コンテンツ タイプ リストにコンテンツ タイプがないトラフィックに対して実行するアクションを設定するかどうか。指定できるアクションは、次のとおりです。 • [Allow Packet]：メッセージを許可します。 • [Drop Packet]：接続を閉じます。 • [Reset Connection]（デフォルト）：TCP リセット メッセージをクライアントとサーバに送信します。 次のオプションも選択できます。 • [要求のACCEPTフィールドと応答のContent-typeフィールドの一致を検証する（Verify Content-type field for response matches the ACCEPT field of request）]：応答のコンテンツタイプが要求と一致することも確認します。 • [Syslogの生成（Generate Syslog）]：非準拠トラフィックが検出された場合にメッセージを syslog に書き込みます。
Override Global TCP Idle Timeout (IOS only)	TCP アイドル タイムアウトのデフォルト設定を変更するかどうか。この時間の経過後に通信アクティビティがない場合、IOS デバイスは接続を終了します。このオプションを選択した場合は、目的のタイムアウト値を秒単位で指定します。
Override Global Audit Trail Setting (IOS only) Enable Audit Trail	IOS デバイスの監査証跡設定を変更するかどうか。このオプションを選択した場合は、[監査証跡の有効化（Enable Audit Trail）] を選択して監査証跡メッセージを生成できます。

HTTP マップの [Entity Length] タブ

[Entity Length] タブを使用して、HTTP コンテンツの長さに基づくインスペクションをイネーブルにします。

ナビゲーション パス

ASA 7.1.x/PIX 7.1.x/FWSM 3.x/IOS デバイスの [Add HTTP Map]/[Edit HTTP Map] ダイアログボックスの [Entity Length] タブをクリックします。 ASA 7.1.x、PIX 7.1.x、FWSM 3.x、および IOS デバイスの HTTP マップの設定 （74 ページ） を参照してください。

関連項目

- マップ オブジェクトについて
- インスペクションのプロトコルおよびマップの設定 （28 ページ）

フィールド リファレンス

表 32 : HTTP マップの [Entity Length] タブ

要素	説明

Inspect URI Length	URI の長さに基づくインスペクションをイネーブルにするかどうか。このオプションを選択した場合は、次の項目を設定します。
	• [Maximum]：バイト単位での URI の最大長（1 ～ 65535）。
	• [Excessive URI Length Action]：長さを超過した場合に実行するアクション。
	  • [Allow Packet]：メッセージを許可します。
	  • [Drop Packet]：接続を閉じます。
	  • [Reset Connection]：TCP リセット メッセージをクライアントとサーバに送信します。
	• [Generate Syslog]：違反が発生した場合に syslog メッセージを生成するかどうか。

要素	説明

Inspect Maximum Header Length	HTTP ヘッダーの長さに基づくインスペクションをイネーブルにするかどうか。このオプションを選択した場合は、次の項目を設定します。
	• [Request]：バイト単位での要求ヘッダーの最大長（1 ～ 65535）。
	• [Response]：バイト単位での応答ヘッダーの最大長（1 ～ 65535）。
	• [Excessive Header Length Action]：長さを超過した場合に実行するアクション。
	  • [Allow Packet]：メッセージを許可します。
	  • [Drop Packet]：接続を閉じます。
	  • [Reset Connection]：TCP リセット メッセージをクライアントとサーバに送信します。
	• [Generate Syslog]：違反が発生した場合に syslog メッセージを生成するかどうか。

Inspect Body Length	メッセージ本文の長さに基づくインスペクションをイネーブルにするかどうか。このオプションを選択した場合は、次の項目を設定します。
	• [Minimum Threshold]：バイト単位でのメッセージ本文の最小長（1 ～ 65535）。
	• [Maximum Threshold]：バイト単位でのメッセージ本文の最大長（1 ～ 65535）。
	• [Body Length Threshold Action]：メッセージ本文が設定した境界の範囲外の場合に実行するアクション。
	  • [Allow Packet]：メッセージを許可します。
	  • [Drop Packet]：接続を閉じます。
	  • [Reset Connection]：TCP リセット メッセージをクライアントとサーバに送信します。
	• [Generate Syslog]：違反が発生した場合に syslog メッセージを生成するかどうか。

HTTP マップの [RFC Request Method] タブ

[RFC Request Method] タブを使用して、HTTP 要求で特定の要求メソッドが使用されている場合に実行するアクションを定義します。

ナビゲーション パス

ASA 7.1.x/PIX 7.1.x/FWSM 3.x/IOS デバイスの [Add HTTP Map]/[Edit HTTP Map] ダイアログボックスの [RFC Request Method] タブをクリックします。 ASA 7.1.x、PIX 7.1.x、FWSM 3.x、および IOS デバイスの HTTP マップの設定 （74 ページ） を参照してください。

関連項目

- マップ オブジェクトについて
- インスペクションのプロトコルおよびマップの設定 （28 ページ）

フィールド リファレンス

表 33 : HTTP マップの [RFC Request Method]

要素	説明
Available and Selected Methods 操作 Syslog を生成する	[Available Methods] リストには、RFC 2616 で規定されている要求メソッドが表示されます。 メソッドのアクションを設定するには、メソッドを選択してから、アクションを選択します。選択したメソッドが含まれた HTTP 要求が発生したときに syslog にメッセージが追加されるようにする場合は、任意で [Syslogの生成（Generate Syslog）] を選択します。[>>] ボタンをクリックして、メソッドを [選択済みのメソッド（Selected Methods）] リストに追加します（メソッドを選択済みリストから削除するには、メソッドを選択し、[<<] ボタンをクリックします）。 **ヒント** アクションと syslog 要求がそれぞれ同じである場合は、Ctrl を押しながらクリックすることで、一度に複数のメソッドを選択できます。 指定できるアクションは次のとおりです。 • [Allow Packet]：メッセージを許可します。 • [Drop Packet]：接続を閉じます。 • [Reset Connection]（デフォルト）：TCP リセット メッセージをクライアントとサーバに送信します。
Specify the action to be applied for the remaining available methods above.	上記で特定のアクションを指定していないメソッドのデフォルトアクションを定義するかどうか。このオプションを選択した場合は、アクション、およびデフォルトアクションに使用する syslog 設定を選択します。

HTTP マップの [Extension Request Method] タブ

[Extension Request Method] タブを使用して、HTTP 要求で特定の拡張要求メソッドが使用されている場合に実行するアクションを定義します。

ナビゲーション パス

ASA 7.1.x/PIX 7.1.x/FWSM 3.x/IOS デバイスの [Add HTTP Map]/[Edit HTTP Map] ダイアログボックスの [Extension Request Method] タブをクリックします。 ASA 7.1.x、PIX 7.1.x、FWSM 3.x、および IOS デバイスの HTTP マップの設定 （74 ページ） を参照してください。

関連項目

- マップ オブジェクトについて
- インスペクションのプロトコルおよびマップの設定 （28 ページ）

フィールド リファレンス

表 *34 : HTTP* マップの *[Extension Request Method]* タブ

要素	説明
Available and Selected Methods 操作 Syslog を生成する	[Available Methods] リストには、RFC 2616 で規定されている拡張要求メソッドが表示されます。 メソッドのアクションを設定するには、メソッドを選択してから、アクションを選択します。選択したメソッドが含まれた HTTP 要求が発生したときに syslog にメッセージが追加されるようにする場合は、任意で [Syslogの生成（Generate Syslog）] を選択します。[>>] ボタンをクリックして、メソッドを [選択済みのメソッド（Selected Methods）] リストに追加します（メソッドを選択済みリストから削除するには、メソッドを選択し、[<<] ボタンをクリックします）。 **ヒント** アクションと syslog 要求がそれぞれ同じである場合は、Ctrl を押しながらクリックすることで、一度に複数のメソッドを選択できます。 指定できるアクションは次のとおりです。 • [Allow Packet]：メッセージを許可します。 • [Drop Packet]：接続を閉じます。 • [Reset Connection]（デフォルト）：TCP リセット メッセージをクライアントとサーバに送信します。

要素	説明
Specify the action to be applied for the remaining available methods above.	上記で特定のアクションを指定していないメソッドのデフォルト アクションを定義するかどうか。このオプションを選択した場合は、アクション、およびデフォルト アクションに使用する syslog 設定を選択します。

HTTP マップの [Port Misuse] タブ

[Port Misuse] タブを使用して、ポートの誤用アプリケーション ファイアウォール インスペクションをイネーブルにします。設定できるアプリケーション カテゴリは次のとおりです。

- [IM]：インスタント メッセージング。チェックされるアプリケーションは、Yahoo! Messenger、AIM、および MSN IM です。
- [P2P]：ピアツーピア アプリケーション。Kazaa アプリケーションがチェックされます。
- [Tunneling]：トンネリング アプリケーション。チェックされるアプリケーションは、HTTPort/HTTHost、GNU Httptunnel、GotoMyPC、Firethru、および Http-tunnel.com Client です。

ナビゲーション パス

ASA 7.1.x/PIX 7.1.x/FWSM 3.x/IOS デバイスの [Add HTTP Map]/[Edit HTTP Map] ダイアログボックスの [Port Misuse] タブをクリックします。 ASA 7.1.x、PIX 7.1.x、FWSM 3.x、および IOS デバイスの HTTP マップの設定 （74 ページ） を参照してください。

関連項目

- マップ オブジェクトについて
- インスペクションのプロトコルおよびマップの設定 （28 ページ）

フィールド リファレンス

表 *35 : HTTP* マップの *[Port Misuse]* タブ

要素	説明
Available and Selected Application Categories 操作 Syslog を生成する	[Available Application Categories] リストには、ファイアウォール インスペクション設定を定義できるカテゴリが表示されます。 カテゴリのアクションを設定するには、カテゴリを選択し、次にアクションを選択します。選択したアプリケーションが含まれるHTTP要求が発生したときにsyslogにメッセージが追加されるようにする場合は、任意で [Syslogの生成（Generate Syslog）] を選択します。[>>] ボタンをクリックして、カテゴリを [選択されたカテゴリ（Selected Categories）] リストに追加します（カテゴリを選択済みリストから削除するには、カテゴリを選択し、[<<] ボタンをクリックします）。 ヒント　アクションとsyslog要求がそれぞれ同じである場合は、Ctrlを押しながらクリックすることで、一度に複数のカテゴリを選択できます。 指定できるアクションは次のとおりです。 • [Allow Packet]：メッセージを許可します。 • [Drop Packet]：接続を閉じます。 • [Reset Connection]（デフォルト）：TCP リセット メッセージをクライアントとサーバに送信します。
Specify the action to be applied for the remaining available categories above.	上記で特定のアクションを指定していないカテゴリのデフォルト アクションを定義するかどうか。このオプションを選択した場合は、アクション、およびデフォルト アクションに使用する syslog 設定を選択します。

HTTP マップの [Transfer Encoding] タブ

[Transfer Encoding] タブを使用して、転送符号化タイプに基づくインスペクションをイネーブルにします。設定できる符号化タイプは次のとおりです。

- [Chunked]：メッセージ本文が一連のチャンクとして転送される転送符号化タイプを識別します。
- [Compressed]：メッセージ本文が UNIX ファイル圧縮を使用して転送される転送符号化タイプを識別します。
- [Deflate]：メッセージ本文が zlib 形式（RFC 1950）および deflate 圧縮（RFC 1951）を使用して転送される転送符号化タイプを識別します。
- [GZIP]：メッセージ本文が GNU zip（RFC 1952）を使用して転送される転送符号化タイプを識別します。

- [Identity]：メッセージ本文で転送符号化が実行されない接続を識別します。

ナビゲーション パス

ASA 7.1.x/PIX 7.1.x/FWSM 3.x/IOS デバイスの [Add HTTP Map]/[Edit HTTP Map] ダイアログボックスの [Transfer Encoding] タブをクリックします。 ASA 7.1.x、PIX 7.1.x、FWSM 3.x、および IOS デバイスの HTTP マップの設定 （74 ページ） を参照してください。

関連項目

- マップ オブジェクトについて
- インスペクションのプロトコルおよびマップの設定 （28 ページ）

フィールド リファレンス

表 36 : HTTP マップの [Transfer Encoding] タブ

要素	説明
Available and Selected Encoding Types 操作 Syslog を生成する	[Available Encoding Types] リストには、ファイアウォール インスペクション設定を定義できる転送符号化のタイプが表示されます。 あるタイプのアクションを設定するには、タイプを選択し、アクションを選択します。選択したタイプを含むHTTPリクエストが発生したときにsyslogにメッセージが追加されるようにする場合は、必要に応じて [Syslogの生成（Generate Syslog）] を選択します。[>>] ボタンをクリックして、タイプを [選択済みのエンコードのタイプ（Selected Encoding Types）] リストに追加します（あるタイプを選択済みリストから削除するには、タイプを選択し、[<<]ボタンをクリックします）。 **ヒント** アクションとsyslog要求がそれぞれ同じである場合は、Ctrlを押しながらクリックすることで、一度に複数のタイプを選択できます。 指定できるアクションは次のとおりです。 • [Allow Packet]：メッセージを許可します。 • [Drop Packet]：接続を閉じます。 • [Reset Connection]（デフォルト）：TCPリセットメッセージをクライアントとサーバに送信します。
Specify the action to be applied for the remaining available encoding types above.	上記で特定のアクションを指定していないタイプのデフォルト アクションを定義するかどうか。このオプションを選択した場合は、アクション、およびデフォルト アクションに使用する syslog 設定を選択します。

ASA 7.2+ および PIX 7.2+ デバイスの HTTP マップの設定

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き PIX の機能をサポートしていますが、拡張機能はサポートしていません。

[HTTPマップの追加（Add HTTP Map）]/[HTTPマップの編集（Edit HTTP Map）] ダイアログボックスを使用して、ASA および PIX ソフトウェアリリース 7.2 以降の HTTP 検査マップの一致基準と値を定義します。

ナビゲーション パス

[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択し、次にオブジェクトタイプセレクタから [マップ（Maps）] > [ポリシーマップ（Policy Maps）] > [検査（Inspect）] > [HTTP (ASA 7.2+/PIX 7.2+)] を選択します。作業領域内を右クリックしてから [新規オブジェクト(New Object] を選択するか、行を右クリックしてから [オブジェクトの編集（Edit Object）] を選択します。

関連項目

- マップ オブジェクトについて
- インスペクションのプロトコルおよびマップの設定 （28 ページ）
- インスペクション ポリシーのクラス マップの設定 （34 ページ）

フィールド リファレンス

表 37 : [Add HTTP Map]/[Edit HTTP Map] ダイアログボックス（ASA 7.2+/PIX 7.2+）

要素	説明
名前	ポリシー オブジェクトの名前。最大 40 文字を使用できます。
説明	ポリシー オブジェクトの説明。最大 200 文字を使用できます。
[パラメータ（Parameters）] タブ	
Body Match Maximum	本文一致で検索する必要のある HTTP メッセージの本文の最大文字数。 **ヒント** 値が大きいと、パフォーマンスに多大な影響を与えることがあります。
Check for protocol violations	プロトコル違反をチェックするかどうか。

要素	説明
操作	定義した設定に基づいて実行するアクション。接続をドロップ、リセット、または記録できます。
Spoof Server	サーバHTTPヘッダー値を指定した文字列で置換できます。
[Match Condition and Action] タブ [Match All] テーブルに、ポリシー マップに含まれている基準が表示されます。各行には、各基準に一致する、または一致しないトラフィックを検査で検索するかどうか、検査される基準と値、および条件を満たすトラフィックに対して実行されるアクションが示されます。 • 基準を追加するには、[Add] ボタンをクリックし、[Match Condition and Action] ダイアログボックスに入力します（HTTP クラス マップおよび HTTP ポリシー マップ（ASA 7.2+/PIX 7.2+）の [Add Match Condition and Action]/[Edit Match Condition and Action] ダイアログボックス （87 ページ）を参照）。 • 基準を編集するには、基準を選択し、[Edit] ボタンをクリックします。 • 基準を削除するには、基準を選択し、[Delete] ボタンをクリックします。	
カテゴリ	オブジェクトに割り当てられたカテゴリ。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。
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、ポリシー オブジェクトの上書きの許可および個々のデバイスのポリシー オブジェクト オーバーライドについてを参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）] ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）] フィールドには、このオブジェクトをオーバーライドするデバイスの数が表示されます。
Overrides: None	デバイスにオーバーライドが存在しないことを示します。表示を変更するには、オーバーライドを手動で設定する必要があります。詳細については、個々のデバイスのポリシー オブジェクト オーバーライドについてを参照してください。 （注） [Allow Value Override per Device] を選択してもオーバーライドは自動的には設定されません。

HTTPクラスマップおよびHTTPポリシーマップ（ASA7.2+/PIX7.2+）の[Add Match Condition and Action]/[Edit Match Condition and Action] ダイアログボックス

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き PIX の機能をサポートしますが、拡張機能はサポートしていません。

[Add HTTP Match Criterion]/[Edit HTTP Match Criterion] ダイアログボックス（HTTP クラス マップの場合）または [Add Match Condition and Action]/[Edit Match Condition and Action] ダイアログボックス（HTTP ポリシー マップの場合）を使用して、次の処理を行います。

- HTTP クラス マップの一致基準と値を定義する。
- HTTP ポリシー マップの作成時に HTTP クラス マップを選択する。
- HTTP ポリシー マップに一致基準、値、およびアクションを直接定義する。

これらのタイプのマップは、ASA 7.2 以降または PIX 7.2 以降のオペレーティングシステムを実行しているデバイスにのみ使用されます。

このダイアログボックスのフィールドは、選択した基準、およびクラスマップとポリシーマップのどちらを作成しているかによって変わります。次の基準を使用できます。

- [Request/Response Content Type Mismatch]：応答のコンテンツ タイプが要求の accept フィールドの MIME タイプの 1 つと一致する必要があることを指定します。
- [Request Arguments]：要求の引数に正規表現照合を適用します。
- [Request Body]：要求の本文に正規表現照合を適用します。
- [Request Body Length]：要求の本文の長さが指定したバイト数よりも大きいまたは小さいものが一致することを指定します。
- [Request Header Count]：要求のヘッダー数が指定した数よりも大きいまたは小さいものが一致することを指定します。
- [Request Header Length]：要求のヘッダーの長さが指定したバイト数よりも大きいまたは小さいものが一致することを指定します。
- [Request Header Field]：要求のヘッダーに正規表現照合を適用します。
- [Request Header Field Count]：指定したヘッダー フィールド数に基づいて、要求のヘッダーに正規表現照合を適用します。
- [Request Header Field Length]：指定したフィールド長に基づいて、要求のヘッダーに正規表現照合を適用します。
- [Request Header Content Type]：要求の content-type ヘッダー フィールドで評価するコンテンツ タイプを指定します。

- [Request Header Transfer Encoding]：要求の transfer-encoding ヘッダー フィールドで評価する転送符号化を指定します。
- [Request Header Non-ASCII]：要求のヘッダーに非 ASCII 文字があるかどうかを指定します。
- [Request Method]：照合する要求メソッドを指定します。
- [Request URI]：要求の URI に正規表現照合を適用します。
- [Request URI Length]：要求の URI の長さが指定したバイト数よりも大きいまたは小さいものが一致することを指定します。
- [Response Body ActiveX]：要求の本文に ActiveX コンテンツがあるかどうかを指定します。
- [Response Body Java Applet]：要求の本文に Java アプレットがあるかどうかを指定します。
- [Response Body]：応答の本文に正規表現照合を適用します。
- [Response Body Length]：応答の本文の長さが指定したバイト数よりも大きいまたは小さいものが一致することを指定します。
- [Response Header Count]：応答のヘッダー数が指定した数よりも大きいまたは小さいものが一致することを指定します。
- [Response Header Length]：応答のヘッダーの長さが指定したバイト数よりも大きいまたは小さいものが一致することを指定します。
- [Response Header Field]：応答のヘッダーに正規表現照合を適用します。
- [Response Header Field Count]：指定したヘッダー フィールド数に基づいて、応答のヘッダーに正規表現照合を適用します。
- [Response Header Field Length]：指定したフィールド長に基づいて、応答のヘッダーに正規表現照合を適用します。
- [Response Header Content Type]：応答の content-type ヘッダー フィールドで評価するコンテンツ タイプを指定します。
- [Response Header Transfer Encoding]：応答の transfer-encoding ヘッダー フィールドで評価する転送符号化を指定します。
- [Response Header Non-ASCII]：応答のヘッダーに非 ASCII 文字があるかどうかを指定します。
- [Response Status Line]：応答の状況表示行に正規表現照合を適用します。

ナビゲーション パス

HTTP クラスマップを作成している場合は、Policy Object Manager で、HTTP の [クラスマップの追加（Add Class Maps）]/[クラスマップの編集（Edit Class Maps）] ダイアログボックスのテーブル内を右クリックして [行の追加（Add Row）] を選択するか、行を右クリックして [行の編

集（Edit Row）] を選択します。 インスペクション ポリシーのクラス マップの設定 （34 ページ）を参照してください。

HTTP ポリシーマップを作成している場合は、Policy Object Manager で、ASA/PIX 7.2+ のデバイスの [HTTPマップの追加（Add HTTP Map）]/[HTTPマップの編集（Edit HTTP Map）] ダイアログボックスの [一致条件とアクション（Match Condition and Action）] タブのテーブル内を右クリックして [行の追加（Add Row）] を選択するか、行を右クリックして [行の編集（Edit Row）] を選択します。 ASA 7.2+ および PIX 7.2+ デバイスの HTTP マップの設定 （85 ページ） を参照してください。

関連項目

- マップ オブジェクトについて
- インスペクションのプロトコルおよびマップの設定 （28 ページ）

フィールド リファレンス

表 38 : HTTP クラス マップおよび HTTP ポリシー マップ（ASA 7.2+/PIX 7.2+）の [Add Match Condition and Action]/[Edit Match Condition and Action] ダイアログボックス

要素	説明
一致タイプ（Match Type） クラス名 （ポリシー マップのみ）	既存の HTTP クラス マップを使用するか、新規 HTTP クラス マップを定義できます。 • [Use Specified Values]：このダイアログボックスでクラス マップを定義する場合。 • [Use Values in Class Map]：既存の HTTP クラス マップ ポリシー オブジェクトを選択する場合。HTTP クラスマップの名前を [クラス名（Class Name）] フィールドに入力します。[選択（Select）] をクリックしてリストからマップを選択するか、新しいクラスマップオブジェクトを作成します。
基準	照合する HTTP トラフィック基準を指定します。基準については、上記で説明しています。
タイプ（Type）	基準に一致する、または一致しないトラフィックをマップに含めるかどうかを指定します。たとえば、文字列「example.com」で [一致しない（Doesn’t Match）] を選択した場合、「example.com」を含むトラフィックはすべてマップの対象外になります。 • [Matches]：基準に一致する。一部の基準では、これは使用可能な唯一のオプションです。 • [一致しない（Doesn't Match）]：基準に一致しない。

要素	説明
操作 （ポリシー マップのみ）	定義された基準に一致するトラフィックに対してデバイスが適用するアクション。アクションのタイプは選択した基準によって決まります。
可変フィールド 次のフィールドは、[Criterion] フィールドでの選択内容によって変わります。このリストは、表示されると想定されるフィールドのスーパーセットです。	
フィールド名	評価するヘッダー フィールドの名前。次のいずれかを選択できます。 • [Predefined]：定義済みの HTTP ヘッダー フィールド。 • [Regular Expression]：パターン マッチングに使用する正規表現を定義する、正規表現オブジェクト。オブジェクトの名前を入力します。[選択（Select）] をクリックして既存のオブジェクトのリストからオブジェクトを選択するか、または新しい正規表現オブジェクトを作成できます。

要素	説明
値	評価する正規表現。次のいずれかを選択できます。 • [Regular Expression]：パターン マッチングに使用する正規表現を定義する、正規表現オブジェクト。オブジェクトの名前を入力します。[選択（Select）]をクリックして既存のオブジェクトのリストからオブジェクトを選択するか、または新しい正規表現オブジェクトを作成できます。 • [Regular Expression Group]：パターン マッチングに使用する正規表現を定義する、正規表現グループ オブジェクト。オブジェクトの名前を入力します。[選択（Select）]をクリックして既存のオブジェクトのリストからオブジェクトを選択するか、または新しい正規表現グループオブジェクトを作成できます。 [Request Header Transfer Encoding] または [Response Header Transfer Encoding] 基準を評価する場合は、次のオプションも指定できます。 • [Specified By]：転送符号化の次の定義済みタイプの 1 つ。 • [Chunked]：メッセージ本文は、一連のチャンクとして転送されます。 • [Compressed]：メッセージ本文は、UNIX ファイル圧縮を使用して転送されます。 • [Deflate]：メッセージ本文は、zlib 形式（RFC 1950）および deflate 圧縮（RFC 1951）を使用して転送されます。 • [GZIP]：メッセージ本文は、GNU zip（RFC 1952）を使用して転送されます。 • [Identity]：転送の符号化は実行されません。 • [Empty]：要求ヘッダーの transfer-encoding フィールドは空です。
最大長	評価されるフィールドの長さ（バイト単位）。この基準は、長さが指定した数値よりも大きい場合に一致し、フィールドが指定した数値よりも小さい場合は一致しません。
Greater Than Count	評価される項目の数。この基準は、カウントが指定した数値よりも大きい場合に一致し、カウントが指定した数値よりも小さい場合は一致しません。

要素	説明
コンテンツ タイプ（Content Type）	コンテンツ タイプ ヘッダー フィールドで指定した、評価するコンテンツ タイプ。次のいずれかを選択できます。 • [Specified By]：定義済み MIME タイプ。 • [Unknown]：MIME タイプは不明です。既知のすべての MIME タイプに照らして項目を評価する場合は、[Unknown] を選択します。 • [Violation]：本文のマジック番号は、コンテンツ タイプ ヘッダー フィールドの MIME タイプに対応している必要があります。 • [Regular Expression]、[Regular Expression Group]：評価する正規表現または正規表現グループ。これらのオプションの詳細については、[Value] フィールドの説明を参照してください。
要求メソッド	照合する指定済み要求メソッド。次のいずれかを選択できます。 • [Specified By]：定義済みの要求メソッド。 • [Regular Expression]、[Regular Expression Group]：評価する正規表現または正規表現グループ。これらのオプションの詳細については、[Value] フィールドの説明を参照してください。

ASA 7.2+、PIX 7.2+ デバイスの IM マップの設定

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き PIX の機能をサポートしますが、拡張機能はサポートしていません。

[IM Mapの追加（Add IM Map）]/[IM Mapの編集（Edit IM Map）] ダイアログボックスを使用して、ASA/PIX 7.2 以降を実行しているデバイスの Instant Messenger（IM）検査マップを定義するための設定を行います。IMマップを使用すると、IMアプリケーションインスペクションに使用するデフォルト設定値を変更できます。

インスタント メッセージングでは、業務の実行時にクリア テキストが使用されることから、潜在的なネットワーク攻撃やウイルスの拡散が懸念されます。このため、特定のタイプのインスタントメッセージの発生はブロックする一方で、他のタイプは許可することが必要となる場合があります。

ASA および PIX デバイスでは、IM アプリケーション インスペクションにより、ネットワークの使用を制御するための詳細なアクセス コントロールが提供されます。正規表現を使用して、機密データの漏れとネットワークの脅威の伝播を阻止できます。Yahoo! Messenger または MSN Messenger トラフィックを検査できます。

ナビゲーション パス

[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択し、次にオブジェクトタイプセレクタから[マップ（Maps）] > [ポリシーマップ（Policy Maps）] > [検査（Inspect）] > [IM (ASA 7.2+/PIX 7.2+)] を選択します。作業領域内を右クリックしてから [新規オブジェクト（New Object）] を選択するか、行を右クリックしてから [オブジェクトの編集（Edit Object）] を選択します。

関連項目

- マップ オブジェクトについて
- インスペクションのプロトコルおよびマップの設定 （28 ページ）

フィールド リファレンス

表 *39 : [Add IM Map]/[Edit IM Map]* ダイアログボックス

要素	説明
名前	ポリシー オブジェクトの名前。最大 40 文字を使用できます。
説明	ポリシー オブジェクトの説明。最大200 文字を使用できます。
[Match Condition and Action] タブ [Match All] テーブルに、ポリシー マップに含まれている基準が表示されます。各行には、各基準に一致する、または一致しないトラフィックを検査で検索するかどうか、検査される基準と値、および条件を満たすトラフィックに対して実行されるアクションが示されます。 • 基準を追加するには、[Add] ボタンをクリックし、[Match Condition and Action] ダイアログボックスに入力します（IM クラス マップおよび IM ポリシー マップ（ASA 7.2+/PIX 7.2+）の [Add Match Condition and Action]/[Edit Match Condition and Action] ダイアログボックス （94 ページ）を参照）。 • 基準を編集するには、基準を選択し、[Edit] ボタンをクリックします。 • 基準を削除するには、基準を選択し、[Delete] ボタンをクリックします。	
カテゴリ	オブジェクトに割り当てられたカテゴリ。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。

要素	説明
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、ポリシー オブジェクトの上書きの許可および個々のデバイスのポリシー オブジェクト オーバーライドについてを参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）] ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）] フィールドには、このオブジェクトに対するオーバーライドを持つデバイスの数が表示されます。

IM クラス マップおよび IM ポリシー マップ（ASA 7.2+/PIX 7.2+）の [Add Match Condition and Action]/[Edit Match Condition and Action] ダイアログボックス

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き PIX の機能をサポートしていますが、拡張機能はサポートしていません。

[Add IM Match Criterion]/[Edit IM Match Criterion] ダイアログボックス（IM クラス マップの場合）または [Add Match Condition and Action]/[Edit Match Condition and Action] ダイアログボックス（IM ポリシー マップの場合）を使用して、次の処理を行います。

- IM クラス マップの一致基準と値を定義する。
- IM ポリシー マップの作成時に IM クラス マップを選択する。
- IM ポリシー マップに一致基準、値、およびアクションを直接定義する。

これらのタイプのマップは、ASA 7.2 以降または PIX 7.2 以降のオペレーティングシステムを実行しているデバイスにのみ使用されます。

このダイアログボックスのフィールドは、選択した基準、およびクラスマップとポリシーマップのどちらを作成しているかによって変わります。

ナビゲーション パス

IM クラスマップを作成している場合は、Policy Object Manager で、IM の [クラスマップの追加（Add Class Maps）]/[クラスマップの編集（Edit Class Maps）] ダイアログボックスのテーブル内を右クリックして [行の追加（Add Row）] を選択するか、行を右クリックして [行の編集（Edit Row）] を選択します。 インスペクション ポリシーのクラス マップの設定 （34 ページ）を参照してください。

IM ポリシーマップを作成している場合は、Policy Object Manager で、ASA 7.2/PIX 7.2 の [IM マップの追加（Add IM Map）]/[IMマップの編集（Edit IM Map）] ダイアログボックスの [一致

条件とアクション（Match Condition and Action）] タブのテーブル内を右クリックして [行の追加（Add Row）] を選択するか、行を右クリックして [行の編集（Edit Row）] を選択します。ASA 7.2+、PIX 7.2+ デバイスの IM マップの設定 （92 ページ） を参照してください。

関連項目

- マップ オブジェクトについて
- インスペクションのプロトコルおよびマップの設定 （28 ページ）

フィールド リファレンス

表 *40 : IM* クラス マップおよび *IM* ポリシー マップ（*ASA 7.2+/PIX 7.2+*）の *[Add Match Condition and Action]/[Edit Match Condition and Action]* ダイアログボックス

要素	説明
一致タイプ（Match Type） クラス名 （ポリシー マップのみ）	既存の IM クラス マップを使用するか、新規 IM クラス マップを定義できます。 • [Use Specified Values]：このダイアログボックスでクラス マップを定義する場合。 • [Use Values in Class Map]：既存の IM クラス マップ ポリシー オブジェクトを選択する場合。IM クラスマップの名前を [クラス名（Class Name）] フィールドに入力します。[選択（Select）] をクリックしてリストからマップを選択するか、または新しいクラス マップオブジェクトを作成します。
基準	照合する IM トラフィック基準を指定します。基準は次のとおりです。 • [Filename]：IM ファイル転送サービスのファイル名を照合します。 • [Client IP Address]：送信元クライアント IP アドレスを照合します。 • [Client Login Name]：IM サービスのクライアント ログイン名を照合します。 • [Peer IP Address]：ピアまたは宛先の IP アドレスを照合します。 • [Peer Login Name]：IM サービスのピアまたは宛先のログイン名を照合します。 • [Protocol]：IM プロトコルを照合します。 • [Service]：IM サービスを照合します。 • [File Transfer Service Version]：IM ファイル転送サービス バージョンを照合します。

要素	説明
タイプ（Type）	基準に一致する、または一致しないトラフィックをマップに含めるかどうかを指定します。たとえば、文字列「example.com」で [一致しない（Doesn't Match）] を選択した場合、「example.com」を含むトラフィックはすべてマップの対象外になります。 • [一致（Matches）]：基準に一致する。 • [一致しない（Doesn't Match）]：基準に一致しない。
操作 （ポリシー マップのみ）	定義された基準に一致するトラフィックに対してデバイスが適用するアクション。
可変フィールド 次のフィールドは、[Criterion] フィールドでの選択内容によって変わります。このリストは、表示されると想定されるフィールドのスーパーセットです。	
値	評価する正規表現。次のいずれかを選択できます。 • [Regular Expression]：パターン マッチングに使用する正規表現を定義する、正規表現オブジェクト。オブジェクトの名前を入力します。[選択（Select）] をクリックして既存のオブジェクトのリストからオブジェクトを選択するか、または新しい正規表現オブジェクトを作成できます。 • [Regular Expression Group]：パターン マッチングに使用する正規表現を定義する、正規表現グループ オブジェクト。オブジェクトの名前を入力します。[選択（Select）] をクリックして既存のオブジェクトのリストからオブジェクトを選択するか、または新しい正規表現グループオブジェクトを作成できます。
IPアドレス	照合する IP アドレス。
プロトコル	IM プロトコル（MSN Messenger または Yahoo! Messenger）。
サービス	検査する IM サービス。表示されているサービスの 1 つ以上を選択します。

IOS デバイスの IM マップの設定

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き PIX、FWSM、および IPS の機能をサポートしていますが、拡張機能はサポートしていません。

[Add IM Map (IOS)]/[Edit IM Map (IOS)] ダイアログボックスを使用して、IOS デバイスの Instant Messaging（IM; インスタント メッセージング）インスペクション ポリシー マップ オブジェクトを設定します。IM マップを使用すると、IM アプリケーション インスペクションに使用するデフォルト設定値を変更できます。

インスタント メッセージングでは、業務の実行時にクリア テキストが使用されることから、潜在的なネットワーク攻撃やウイルスの拡散が懸念されます。このため、特定のタイプのインスタント メッセージの発生はブロックする一方で、他のタイプは許可することが必要となる場合があります。

IM アプリケーション インスペクションにより、ネットワークの使用を制御するための詳細なアクセス コントロールが提供されます。機密データの漏れおよびネットワークの脅威の伝播を阻止するのにも役立ちます。許可または拒否されるサーバを指定することで、スコープを限定できます。Yahoo! Messenger、MSN Messenger、および AOL インスタント メッセージのインスペクションがサポートされます。

ナビゲーション パス

[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択し、次にオブジェクト タイプセレクタから **[マップ（Maps）] > [ポリシーマップ（Policy Maps）] > [検査（Inspect）] > [IM (IOS)]** を選択します。作業領域内を右クリックしてから [新規オブジェクト(New Object] を選択するか、行を右クリックしてから [オブジェクトの編集（Edit Object）] を選択します。

関連項目

- マップ オブジェクトについて
- インスペクションのプロトコルおよびマップの設定 （28 ページ）

フィールド リファレンス

表 41 : [Add IM Map (IOS)]/[Edit IM Map (IOS)] ダイアログボックス

要素	説明
名前	ポリシー オブジェクトの名前。最大 40 文字を使用できます。
説明	ポリシー オブジェクトの説明。最大 200 文字を使用できます。
サービス タブ さまざまな IM サービス プロバイダーを表すタブ。各タブで使用できる設定は同じです。サービス プロバイダーごとに個別に設定する必要があります。次のフィールドの説明は、Yahoo!、MSN、および AOL の各サービスに適用されます。	
Text Chat	許可、拒否、記録、またはそのいくつかの組み合わせなど、テキスト チャット サービスの処理方法。

要素	説明
その他のサービス	許可、拒否、記録、またはそのいくつかの組み合わせなど、テキスト チャット以外のサービスの処理方法。IOS ソフトウェアは、音声チャット、ビデオチャット、ファイルの共有と転送、ゲームなど、テキスト チャット以外のすべてのサービスを 1 つのグループとして認識します。
Permit Servers	ここで指定したサーバからのトラフィックを許可します。使用できる形式は、カンマで区切られた IP アドレス、IP 範囲、およびホスト名です。
Deny Servers	ここで指定したサーバからのトラフィックを拒否します。使用できる形式は、カンマで区切られた IP アドレス、IP 範囲、およびホスト名です。
アラート（Alert）	アラートをイネーブルにするかディセーブルにするか。デフォルトは、デフォルトのインスペクション設定の使用です。
Audit	監査証跡をイネーブルにするかディセーブルにするか。デフォルトは、デフォルトのインスペクション設定の使用です。
タイムアウト（Timeout）	サービスのタイムアウト。デフォルトのインスペクション設定を使用するか、タイムアウトを指定することを選択できます。[Specify Timeout] を選択した場合は、タイムアウト値を秒単位で入力します。
カテゴリ	オブジェクトに割り当てられたカテゴリ。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。
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、ポリシー オブジェクトの上書きの許可および個々のデバイスのポリシー オブジェクト オーバーライドについてを参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）] ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）] フィールドには、このオブジェクトに対するオーバーライドを持つデバイスの数が表示されます。

IP オプション マップの設定

[Add IP Options Map]/[Edit IP Options Map] ダイアログボックスを使用して、ASA 8.2(2)+ デバイスの IP パケット ヘッダー内のオプションのインスペクション用マップを定義します。options

フィールドで提供される制御機能は、一部の状況では必須ですが、ほとんどの一般的な状況では不要です。

IP オプション インスペクションを設定しない場合、ASA デバイスは、オプションが設定されているすべてのパケットをドロップしますが、例外が 1 つあります。ルーテッドモードでは、ルータ アラート オプションを含むパケットが許可されます（ルータ アラート パケットを禁止するには、ルータ アラートを選択解除した IP オプション マップを作成し、ポリシー マップを使用して IP オプションを検査するようにインスペクション ルールを設定します）。

ヒント パケット ヘッダー サイズと位置合わせを適切に保つために No Operation（NOP）オプションがパディングとして使用される場合があるため、NOP を許可することが必要な場合があります。

各オプションについて、次の動作を選択できます。

- [許可（Allow）]：パケットを許可し、IP ヘッダーの options フィールドを変更しません。
- [クリア（Clear）]：パケットを許可し、IP ヘッダーの options フィールドのオプションをクリアします。

オプションを選択しない場合は、オプションが禁止され、オプションを含むパケットがドロップされます。ここにリストされていないオプションを選択しても、パケットがドロップされます。この動作は変更できません。

ナビゲーション パス

[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択し、オブジェクトタイプ セレクタから [マップ（Maps）] > [ポリシーマップ（Policy Maps）] > [検査（Inspect）] > [IPオプション（IP Options）] を選択します。作業領域内を右クリックしてから [新規オブジェクト（New Object）] を選択するか、行を右クリックしてから [オブジェクトの編集（Edit Object）] を選択します。

関連項目

- マップ オブジェクトについて
- インスペクションのプロトコルおよびマップの設定　（28 ページ）

フィールド リファレンス

表 *42 : [Add IP Options Map]/[Edit IP Options Map]* ダイアログボックス

要素	説明
名前	ポリシー オブジェクトの名前。最大 128 文字を使用できます。
説明	ポリシー オブジェクトの説明。

要素	説明
End of Options List	End of Options List（EOOL）、または IP オプション 0 は、単一の 0 バイトだけを含み、オプションのリストの終わりを示すためにすべてのオプションの最後に置かれます。これは、ヘッダー長に基づくヘッダーの末尾とは一致しない場合があります。
No operation	No Operation（NOP）、または IP オプション 1 はパディングに使用されます。IP ヘッダーの Options フィールドには、オプションを 0 個、1 個、またはそれ以上含めることができ、これがフィールド変数全体の長さになります。ただし、IP ヘッダーは 32 ビットの倍数である必要があります。すべてのオプションのビット数が 32 ビットの倍数でない場合は、NOP オプションを使用してオプションが 32 ビット境界に合わせられます。
Router alert	Router Alert（RTRALT）、または IP オプション 20 は、パケットがそのルータ宛ではない場合でも、パケットの内容を検査するように通過ルータに通知します。この検査は、RSVP を導入している場合に役に立ちます。同様のプロトコルは、パケットの配信パス上にあるルータでの比較的複雑な処理を必要とします。
[基本セキュリティ（Basic Security）]（*ASA* デバイス *9.5(1)* 以降）	RFC 1108 の IP オプション基本セキュリティ（番号 130）。デフォルトはドロップです。
[商用セキュリティ（Commercial Security）]（*ASA* デバイス *9.5(1)* 以降）	IP オプション商用セキュリティ（番号 134）。デフォルトはドロップです。
[デフォルト（Default）]（*ASA* デバイス *9.5(1)* 以降）	IP オプションデフォルト設定。デフォルトはドロップです。
[実験的フロー制御（Experimental Flow Control）]（*ASA* デバイス *9.5(1)* 以降）	IP オプション実験的フロー制御（番号 205）。デフォルトはドロップです。
[実験的測定（Experimental Measurement）]（*ASA* デバイス *9.5(1)* 以降）	IP オプション実験的測定（番号 10）。デフォルトはドロップです。
[拡張セキュリティ（Extended-Security）]（*ASA* デバイス *9.5(1)* 以降）	RFC 1108 の IP オプション拡張セキュリティ（番号 133）。デフォルトはドロップです。

要素	説明
[IMI トラフィック記述子（IMI Traffic Descriptor）]（*ASA* デバイス *9.5(1)* 以降）	IP オプション IMI トラフィック記述子（番号 144）。デフォルトはドロップです。
[クイックスタート（Quick Start）]（*ASA* デバイス *9.5(1)* 以降）	RFC 4782 の IP オプションルータアラート（番号 25）。デフォルトはドロップです。
[レコードルート（Record Route）]（*ASA* デバイス *9.5(1)* 以降）	RFC 791 の IP オプションレコードルート（番号 7）。デフォルトはドロップです。
[タイムスタンプ（Time Stamp）]（*ASA* デバイス *9.5(1)* 以降）	RFC 791 の IP オプションルータアラート（番号 68）。デフォルトはドロップです。
（注） バージョン 4.9 以降、Security Manager は、ソフトウェアバージョン 9.5(1) 以降を実行している ASA デバイスに対して 10 の新しい IP オプションをサポートします。標準的または試行的なオプションを許可、クリア、またはドロップするように検査を調整できます。定義されているものとは別に、特定の IP オプションを設定することもできます。たとえば、0 ～ 255 の範囲の値を使用して、IP オプションを直接設定できます。Security Manager は CLI「[no] 0-255 allow | clear」をサポートします。また、IP オプションインスペクションマップで明示的に定義されていないオプションのデフォルトの動作を設定できます。許可およびオプションでクリアするオプションを選択するようになりました。IP オプションおよび関連する RFC の参照のリストについては、IANA のページ（http://www.iana.org/assignments/ip-parameters/ip-parameters.xhtml [英語]）を参照してください。	
カテゴリ	オブジェクトに割り当てられたカテゴリ。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。
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、ポリシー オブジェクトの上書きの許可および個々のデバイスのポリシー オブジェクト オーバーライドについてを参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）] ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）] フィールドには、このオブジェクトをオーバーライドするデバイスの数が表示されます。

IPv6 マップの設定

[IPv6マップの追加（Add IPv6 Map）]/[IPv6マップの編集（Edit IPv6 Map）] ダイアログボックスを使用して、IPv6 インスペクションマップの一致基準と値を定義します。IPv6 マップを使用して、IPv6 パケットにある拡張ヘッダーの次に示すタイプに基づいて、選択的に IPv6 パケットをドロップすることができます。

- ホップバイホップ オプション
- ルーティング（タイプ 0）
- フラグメント
- 宛先オプション
- 認証
- カプセル化セキュリティ ペイロード

これらのプロトコルに対応するサービスオブジェクトは、Policy Object Manager のサービステーブルで利用できます。

（注） Security Manager 4.4 のリリースと ASA のバージョン 9.0 以降で、IPv4 インスペクションルールと IPv6 インスペクションルールを設定するための別個のポリシーが統合されました。ただし、IPv6 マップは、以前のバージョンをサポートするために引き続き提供されます。

ナビゲーション パス

[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択し、次にオブジェクトタイプセレクタから [マップ（Maps）] > [ポリシーマップ（Policy Maps）] > [検査（Inspect）] > [FTP] を選択します。テーブル内を右クリックしてから [新規オブジェクト（New Object）] を選択するか、行を右クリックしてから [オブジェクトの編集（Edit Object）] を選択します。

関連項目

- マップ オブジェクトについて
- インスペクションのプロトコルおよびマップの設定 （28 ページ）

フィールド リファレンス

表 *43 : [IPv6マップの追加（Add IPv6 Map）]/[IPv6マップの編集（Edit IPv6 Map）] ダイアログボックス*

要素	説明
名前	ポリシー オブジェクトの名前。最大 40 文字を使用できます。

要素	説明
説明	ポリシー オブジェクトの説明。最大 200 文字を使用できます。
[パラメータ（Parameters）] タブ	
[既存の拡張ヘッダーのみを許可（Permit only known Extension Headers）]	ASA が IPv6 拡張ヘッダーを検証するかどうかを指定します。これが選択された場合、不明な IPv6 拡張ヘッダーが検出されると、ASA はパケットをドロップし、アクションをログに記録します。 このオプションは、デフォルトで選択されます。
[拡張ヘッダーの順序を適用（Enforce Extension Header Order）]	RFC 2460 仕様で定義されている IPv6 拡張ヘッダーの順序を適用するかどうかを指定します。これが選択された場合、エラーが検出されると、ASA はパケットをドロップし、アクションをログに記録します。 このオプションは、デフォルトで選択されます。
[Match Condition and Action] タブ [Match All] テーブルに、ポリシー マップに含まれている基準が表示されます。各行には、各基準に一致する、または一致しないトラフィックを検査で検索するかどうか、検査される基準と値、および条件を満たすトラフィックに対して実行されるアクションが示されます。 これらの基準エントリは、IPv6 ポリシーマップの [マッチ条件とアクションの追加または編集（Add/Edit Match Condition and Action] ダイアログボックス （104 ページ）で作成および編集されます。	
カテゴリ	オブジェクトに割り当てられたカテゴリ。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。
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、ポリシー オブジェクトの上書きの許可および個々のデバイスのポリシー オブジェクト オーバーライドについてを参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）] ボタンをクリックして、[Policy Object Overrides] ウィンドウでオーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）] フィールドには、このオブジェクトをオーバーライドするデバイスの数が表示されます。

IPv6ポリシーマップの[マッチ条件とアクションの追加または編集（Add/EditMatchCondition and Action] ダイアログボックス

[一致条件とアクションの追加（Add Match Condition and Action）]/[一致条件とアクションの編集（Edit Match Condition and Action）] ダイアログボックスを使用して、IPv6 ポリシーマップの拡張ヘッダー一致基準およびアクションを定義します。拡張ヘッダーの内容は処理されません。アクションは、指定された EH タイプの存在のみに基づいて適用されます。

これらのダイアログボックスのフィールドは、選択した基準によって変わります。

（注） 複数の一致定義を 1 つの IPv6 ポリシーマップに適用できます。

ナビゲーション パス

[Policy Object Manager] で、[IPv6 マップの追加（Add IPv6 Map）]/[IPv6 マップの編集（Edit IPv6 Map）] ダイアログボックスの [一致条件とアクション（Match Condition and Action）] タブのテーブル内を右クリックして [行の追加（Add Row）] を選択するか、行を右クリックして [行の編集（Edit Row）] を選択します。IPv6 マップの設定 （102 ページ） を参照してください。

関連項目

- マップ オブジェクトについて
- インスペクションのプロトコルおよびマップの設定 （28 ページ）

フィールド リファレンス

表 *44 : IPv6* ポリシーマップの *[*マッチ条件とアクションの追加または編集（*Add/Edit Match Condition and Action]* ダイアログボックス

要素	説明
基準	

要素	説明
	一致させる IPv6 拡張ヘッダーのタイプを選択します。 • [認証ヘッダー（AH）（Authentication Header (AH)）]：IP パケットの整合性とデータ発信元の認証を提供します。 • [宛先オプションヘッダー（Destination Options Header）]：IPv6 モビリティに使用され、特定のアプリケーションのサポートにも使用されます。 • [カプセル化セキュリティペイロード（ESP）ヘッダー（Encapsulating Security Payload (ESP) Header）]：ESP ヘッダーに続くすべての情報は暗号化され、中間ネットワーク デバイスからアクセスできません。 • [フラグメントヘッダー（Fragment Header）]：トラフィック送信元のフラグメント化パケット通信をサポートします。 • [ホップバイホップオプションヘッダー（Hop-by-Hop Options Header）]：パケットの配信パス内のすべてのノードによって検査される必要があるオプションの情報。 • [ヘッダー数（Header Count）]：パケット内のヘッダーの数。このオプションを選択すると、次のフィールドが表示されます。ここで、ヘッダー数の上限を指定します。 • [次より多い数（Greater Than Count）]：0 ～ 255 の値を入力します。 ヘッダー数が指定した数値よりも大きい場合に、パケットは一致とみなされます。ヘッダー数が指定した数値以下の場合は一致しません。 • [ルーティングヘッダータイプ（Routing Header Type）]：このオプションを使用して、ヘッダーコードに基づいて 1 つのヘッダータイプ、または複数の EH タイプを一致させます。このタイプを選択すると次の値オプションが表示されます。いずれかの値を指定します。 • [ルーティングタイプ（Routing Type）]：1 つの拡張ヘッダーコードを入力します（例：認証ヘッダーの場合は 51）。 • [ルーティングタイプフィールド範囲（Routing Type Field Range）]：開始値と終了値を入力して、EH コードの範囲を定義します。 • [ルーティングヘッダーアドレスカウント（Routing Header Address Count）]：パケットに埋め込まれている IP アドレスの数。このオプションを選択すると、次のフィールドが表示されます。アドレス数の上限を指定します。 • [次より多い数（Greater Than Count）]：0 ～ 255 の値を入力します。 アドレス数が指定した数値よりも大きい場合に、パケットは一致とみなされます。アドレス数が指定した数値以下の場合は一致しません。

要素	説明
タイプ（Type）	定義された基準に一致するトラフィックにのみマップが適用されることを指定します。
操作	定義された基準に一致するトラフィックに対してデバイスが適用するアクションを選択します。 • [パケットをドロップ（Drop Packet）]：一致するパケットは通知なしでドロップされます。 • [パケットをドロップしてログに記録（Drop Packet and Log）]：一致するパケットはログに記録されてからドロップされます。 • [ログに記録（Log）]-一致するパケットがログに記録され、処理が続行されます。

IPsec パススルー マップの設定

[Add IPsec Pass Through Map]/[Edit IPsec Pass Through Map] ダイアログボックスを使用して、IPsec パススルー マップ ポリシー オブジェクトを設定します。IPsec パススルー マップ ポリシー マップを使用すると、IPsec パススルー インスペクションに使用するデフォルトの設定値を変更できます。

IPSecパススルーインスペクションエンジンを使用すると、セキュリティアプライアンスで、特定の ESP または AH アクセス リストを必要とすることなく、IKE（UDP ポート 500）ネゴシエーションが正常に行われたことによって 2 つのホスト間に生成される、ESP（IP プロトコル 50）および AH（IP プロトコル 51）トラフィックを渡すことができます。

ESP または AH トラフィックは、既存の制御フローが MPF フレームワークで定義された接続制限内である場合に、インスペクションエンジンによって許可されます。このとき、設定されたアイドル タイムアウトが適用されます。制御フローがない場合は、UDP アイドル タイムアウトが設定された IKE UDP ポート 500 トラフィックに対して新しい制御フローが作成されます。または、既存のフローが使用されます。

インスペクションエンジンにパケットが確実に到着するように、このようなすべてのトラフィック（ESP および AH）のために穴を開けます。この検査は制御フローに付加されます。制御フローは、少なくとも 1 つのデータ フロー（ESP または AH）が確立されているかぎり存在しますが、トラフィックのフローは常に同じ接続を経由します。この IKE 接続は、データ フローがあるかぎり開いた状態で保たれるため、キーの再生成は常に成功します。フローは、NAT が使用されているかどうかに関係なく作成されます。ただし、PAT はサポートされません。

ナビゲーション パス

[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択し、次にオブジェクトタイプセレクタから [マップ（Maps）] > [ポリシーマップ（Policy Maps）] > [検査（Inspect）] > [IPSecパススルー（IPsec Pass Through）] を選択します。作業領域内を右クリックしてから [新

規オブジェクト（New Object）] を選択するか、行を右クリックしてから [オブジェクトの編集（Edit Object）] を選択します。

関連項目

- マップ オブジェクトについて
- インスペクションのプロトコルおよびマップの設定 （28 ページ）

フィールド リファレンス

表 *45 : [Add IPsec Pass Through Map]/[Edit IPsec Pass Through Map]* ダイアログボックス

要素	説明
名前	ポリシー オブジェクトの名前。最大 40 文字を使用できます。
説明	ポリシー オブジェクトの説明。最大 200 文字を使用できます。
Allow ESP Maximum ESP Tunnels per Client ESP Idle Timeout	ESP トラフィックを許可するかどうか。このオプションを選択した場合は、各クライアントで使用できるESPトンネルの最大数と、ESP トンネルが閉じられる前にアイドル状態のままでいられる時間（時間:分:秒の形式）を設定できます。デフォルトのタイムアウトは 10 分（00:10:00）です。
Allow AH Maximum AH Tunnels per Client AH Idle Timeout	AH トラフィックを許可するかどうか。このオプションを選択した場合は、各クライアントで使用できる AH トンネルの最大数と、AH トンネルが閉じられる前にアイドル状態のままでいられる時間（時間:分:秒の形式）を設定できます。デフォルトのタイムアウトは 10 分（00:10:00）です。
カテゴリ	オブジェクトに割り当てられたカテゴリ。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。
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、ポリシー オブジェクトの上書きの許可および個々のデバイスのポリシー オブジェクト オーバーライドについてを参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）] ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）] フィールドには、このオブジェクトに対するオーバーライドを持つデバイスの数が表示されます。

NetBIOS マップの設定

[Add NetBIOS Map]/[Edit NetBIOS Map] ダイアログボックスを使用して、NetBIOS インスペクションのマップを定義します。NetBIOS ポリシー マップを使用すると、NetBIOS インスペクションに使用するデフォルト設定値を変更できます。

NetBIOS インスペクション エンジンは、セキュリティ アプライアンスの NAT 設定に従って NetBIOS Name Service（NBNS）パケット内の IP アドレスを変換します。

ナビゲーション パス

[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択し、オブジェクトタイプセレクタから **[マップ（Maps）] > [ポリシーマップ（Policy Maps）] > [検査（Inspect）] > [NetBIOS]** を選択します。作業領域内を右クリックしてから [新規オブジェクト(New Object] を選択するか、行を右クリックしてから [オブジェクトの編集（Edit Object）] を選択します。

関連項目

- マップ オブジェクトについて
- インスペクションのプロトコルおよびマップの設定 （28 ページ）

フィールド リファレンス

表 46 : [Add NetBIOS Map]/[Edit NetBIOS Map] ダイアログボックス

要素	説明
名前	ポリシー オブジェクトの名前。最大 40 文字を使用できます。
説明	ポリシー オブジェクトの説明。最大 200 文字を使用できます。
Check for Protocol Violation 操作	NetBIOS プロトコル違反をチェックするかどうか。このオプションを選択した場合は、違反の発生時に実行するアクションを選択します。
カテゴリ	オブジェクトに割り当てられたカテゴリ。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。

要素	説明
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、ポリシー オブジェクトの上書きの許可および個々のデバイスのポリシー オブジェクト オーバーライドについてを参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）]ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）] フィールドには、このオブジェクトに対するオーバーライドを持つデバイスの数が表示されます。

ScanSafe マップの設定

[NetBIOSマップの追加（Add NetBIOS Map）]/[NetBIOSマップの編集（Edit NetBIOS Map）] ダイアログボックスを使用して、NetBIOS インスペクションのマップを定義します。ScanSafe ポリシーマップを使用すると、ScanSafe インスペクションに使用するデフォルト設定値を変更できます。

このダイアログボックスのフィールドは、クラスマップとポリシーマップのどちらを作成しているかによって変わります。

ナビゲーション パス

[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択し、オブジェクトタイプセレクタから **[マップ（Maps）] > [ポリシーマップ（Policy Maps）] > [検査（Inspect）] > [ScanSafe]** を選択します。作業領域内を右クリックしてから [新規オブジェクト（New Object）] を選択するか、行を右クリックしてから [オブジェクトの編集（Edit Object）] を選択します。

関連項目

- マップ オブジェクトについて
- インスペクションのプロトコルおよびマップの設定 （28 ページ）

フィールド リファレンス

表 47 : ScanSafe の [一致条件およびアクションの追加（Add Match Condition and Action）] ダイアログボックス

要素	説明
パラメータ	

要素	説明
トランスポート プロトコル（Transport Protocol）	HTTPS または HTTP のいずれかを選択できます。 HTTPS の場合、許容される値の範囲は 1 ～ 65535 です。 HTTP の場合、許容される値の範囲は 1 ～ 65535 です。デフォルト値は 8080 です。
デフォルトのユーザー名（Default User Name）	ScanSafe サーバーのデフォルトのユーザー名
デフォルトのグループ名（Default Group Name）	ScanSafe サーバーのデフォルトのグループ名
カテゴリ	Cat-A ～ Cat-G を選択できます。 これは、オブジェクトに割り当てられたカテゴリです。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。
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、ポリシー オブジェクトの上書きの許可および個々のデバイスのポリシー オブジェクト オーバーライドについてを参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）] ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）] フィールドには、このオブジェクトに対するオーバーライドを持つデバイスの数が表示されます。
[一致条件とアクション（Match Condition and Action）] タブのみ	
クラス	クラスマップの名前
操作	ポリシー違反が発生したときに実行するアクションを選択できます
+（「追加」ボタン）	[一致条件およびアクションの追加（Add Match Condition and Action）] ダイアログボックスを開きます。このダイアログボックスには、次のフィールドがあります。 • 一致タイプ（Match Type） • クラスマップ • 操作

SIP マップの設定

[Add SIP Map]/[Edit SIP Map] ダイアログボックスを使用して、SIP アプリケーション インスペクションに使用する値を設定します。SIP インスペクション マップを使用すると、SIP アプリケーション インスペクションに使用するデフォルト設定値を変更できます。

SIP は、インターネット会議、テレフォニー、プレゼンス、イベント通知、およびインスタントメッセージングに広く使用されているプロトコルです。テキストベースの性質とその柔軟性により、SIP ネットワークは数多くのセキュリティ脅威にさらされます。

SIP アプリケーション インスペクションでは、メッセージ ヘッダーおよび本文のアドレス変換、ポートの動的なオープン、および基本的な健全性チェックが行われます。SIP メッセージの健全性を実現するアプリケーション セキュリティおよびプロトコルへの準拠と、SIP ベースの攻撃の検出もサポートされます。

ナビゲーション パス

[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択し、オブジェクトタイプセレクタから [マップ（Maps）] > [ポリシーマップ（Policy Maps）] > [検査（Inspect）] > [SIP (ASA/PIX/FWSM)] を選択します。作業領域内を右クリックしてから [新規オブジェクト（New Object）] を選択するか、行を右クリックしてから [オブジェクトの編集（Edit Object）] を選択します。

関連項目

- マップ オブジェクトについて
- インスペクションのプロトコルおよびマップの設定 （28 ページ）
- インスペクション ポリシーのクラス マップの設定 （34 ページ）

フィールド リファレンス

表 48 : [Add SIP Map]/[Edit SIP Map] ダイアログボックス

要素	説明
名前	ポリシー オブジェクトの名前。最大 40 文字を使用できます。
説明	ポリシー オブジェクトの説明。最大 200 文字を使用できます。
[パラメータ（Parameters）] タブ	
Enable SIP Instant Messaging Extensions	インスタントメッセージング拡張をイネーブルにするかどうか。

要素	説明
Permit Non-SIP Traffic on SIP Port	SIP ポートで SIP 以外のトラフィックを許可するかどうか。
[サーバーとエンドポイントのIPアドレスの非表示（Hide Server's and Endpoint's IP Address）]	IPアドレスを非表示にして、IPアドレスのプライバシーをイネーブルにするかどうか。
Check RTP Packets for Protocol Conformance Limit Payload to Audio or Video based on the Signaling Exchange	プロトコル準拠のために、RTP/RTCP パケットのフローがピンホールを経由することを調べるかどうか。このオプションを選択した場合は、シグナリング交換に基づいてペイロード タイプをオーディオ/ビデオに強制することも選択できます。
If Number of Hops to Destination is Greater Than 0	Max-Forwards ヘッダーの値が 0 かどうかをチェックするかどうか。0 よりも大きい場合は、[Action] フィールドで選択するアクションが実装されます。デフォルトは、パケットのドロップです。
If State Transition is Detected	SIP 状態遷移をチェックするかどうか。遷移が検出された場合は、[Action] フィールドで選択するアクションが実装されます。デフォルトは、パケットのドロップです。
If Header Fields Fail Strict Validation	SIP ヘッダー フィールドが無効な場合に [Action] フィールドで指定したアクションを実行するかどうか。デフォルトは、パケットのドロップです。
[サーバーおよびエンドポイントのソフトウェアバージョンの検査（Inspect Server's and Endpoint's Software Version）]	User-Agent および Server ヘッダーで SIP エンドポイント ソフトウェア バージョンを検査するかどうか。デフォルトは、情報のマスクです。
If Non-SIP URI is Detected	SIP 以外の URI が Alert-Info および Call-Info ヘッダーに検出された場合に、[Action] フィールドで指定したアクションを実行するかどうか。デフォルトは、情報のマスクです。

要素	説明
[Match Condition and Action] タブ [Match All] テーブルに、ポリシー マップに含まれている基準が表示されます。各行には、各基準に一致する、または一致しないトラフィックを検査で検索するかどうか、検査される基準と値、および条件を満たすトラフィックに対して実行されるアクションが示されます。 • 基準を追加するには、[Add] ボタンをクリックし、[Match Condition and Action] ダイアログボックスに入力します（SIP クラス マップおよびポリシー マップの [Add Match Condition and Action]/[Edit Match Condition and Action] ダイアログボックス （114 ページ）を参照）。 • 基準を編集するには、基準を選択し、[Edit] ボタンをクリックします。 • 基準を削除するには、基準を選択し、[Delete] ボタンをクリックします。	
カテゴリ	オブジェクトに割り当てられたカテゴリ。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
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、ポリシー オブジェクトの上書きの許可および個々のデバイスのポリシー オブジェクト オーバーライドについてを参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）] ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）] フィールドには、このオブジェクトをオーバーライドするデバイスの数が表示されます。

SIP クラス マップおよびポリシー マップの [Add Match Condition and Action]/[Edit Match Condition and Action] ダイアログボックス

[Add SIP Match Criterion]/[Edit SIP Match Criterion] ダイアログボックス（SIP クラス マップの場合）または [Add Match Condition and Action]/[Edit Match Condition and Action] ダイアログボックス（SIP ポリシー マップの場合）を使用して、次の処理を行います。

- SIP クラス マップの一致基準と値を定義する。
- SIP ポリシー マップの作成時に SIP クラス マップを選択する。
- SIP ポリシー マップに一致基準、値、およびアクションを直接定義する。

このダイアログボックスのフィールドは、選択した基準、およびクラスマップとポリシーマップのどちらを作成しているかによって変わります。

ナビゲーション パス

SIP クラスマップを作成している場合は、Policy Object Manager で、SIP の [クラスマップの追加（Add Class Maps）]/[クラスマップの編集（Edit Class Maps）] ダイアログボックスのテーブル内を右クリックして [行の追加（Add Row）] を選択するか、行を右クリックして [行の編集（Edit Row）] を選択します。 インスペクション ポリシーのクラス マップの設定 （34 ページ）を参照してください。

DNS ポリシーマップを作成している場合は、Policy Object Manager で、[SIPマップの追加（Add SIP Map）]/[SIPマップの編集（Edit SIP Map）] ダイアログボックスの [一致条件とアクション（Match Condition and Action）] タブのテーブル内を右クリックして [行の追加（Add Row）] を選択するか、行を右クリックして [行の編集（Edit Row）] を選択します。 SIP マップの設定（112 ページ） を参照してください。

関連項目

- マップ オブジェクトについて
- インスペクションのプロトコルおよびマップの設定 （28 ページ）

フィールド リファレンス

表 *49 : SIP* クラス マップおよび *SIP* ポリシー マップの *[Add Match Condition and Action]/[Edit Match Condition and Action]* ダイアログボックス

要素	説明
一致タイプ（Match Type） クラス名 （ポリシーマップのみ）	既存の SIP クラス マップを使用するか、新規 SIP クラス マップを定義できます。 • [Use Specified Values]：このダイアログボックスでクラス マップを定義する場合。 • [Use Values in Class Map]：既存の SIP クラス マップ ポリシー オブジェクトを選択する場合。IM クラスマップの名前を [クラス名（Class Name）] フィールドに入力します。[選択（Select）] をクリックしてリストからマップを選択するか、新しいクラスマップオブジェクトを作成します。

要素	説明
基準	照合する SIP トラフィック基準を指定します。 • [Called Party]：To ヘッダーで指定された着信側を照合します。 • [Calling Party]：From ヘッダーで指定された発信側を照合します。 • [Content Length]：Content Length ヘッダーを照合します。 • [Content Type]：Content Type ヘッダーを照合します。 • [IM Subscriber]：SIP インスタント メッセンジャの加入者を照合します。 • [Message Path]：SIP Via ヘッダーを照合します。 • [Third Party Registration]：サードパーティ登録の要求者を照合します。 • [URI Length]：SIP ヘッダーの URI を照合します。 • [Request Method]：SIP 要求メソッドを照合します。
タイプ（Type）	基準に一致する、または一致しないトラフィックをマップに含めるかどうかを指定します。たとえば、文字列「example.com」で [一致しない（Doesn’t Match）] を選択した場合、「example.com」を含むトラフィックはすべてマップの対象外になります。 • [Matches]：基準に一致する。 • [一致しない（Doesn't Match）]：基準に一致しない。
操作 （ポリシーマップのみ）	定義された基準に一致するトラフィックに対してデバイスが適用するアクション。
可変フィールド 次のフィールドは、[Criterion] フィールドでの選択内容によって変わります。このリストは、表示されると想定されるフィールドのスーパーセットです。	

要素	説明
値	評価する正規表現。次のいずれかを選択できます。 • [Regular Expression]：パターン マッチングに使用する正規表現を定義する、正規表現オブジェクト。オブジェクトの名前を入力します。[選択（Select）] をクリックして既存のオブジェクトのリストからオブジェクトを選択するか、または新しい正規表現オブジェクトを作成できます。 • [Regular Expression Group]：パターン マッチングに使用する正規表現を定義する、正規表現グループ オブジェクト。オブジェクトの名前を入力します。[選択（Select）] をクリックして既存のオブジェクトのリストからオブジェクトを選択するか、または新しい正規表現グループオブジェクトを作成できます。
URI Type	照合する URI のタイプ（SIP または TEL）。
最大長	評価されるフィールドの長さ（バイト単位）。この基準は、長さが指定した数値よりも大きい場合に一致し、フィールドが指定した数値よりも小さい場合は一致しません。
コンテンツ タイプ（Content Type）	コンテンツ タイプ ヘッダー フィールドで指定した、評価するコンテンツ タイプ。次のいずれかを選択できます。 • [SDP]：SDP SIP コンテンツ ヘッダー タイプを照合します。 • [Regular Expression]、[Regular Expression Group]：評価する正規表現または正規表現グループ。これらのオプションの詳細については、[Value] フィールドの説明を参照してください。

要素	説明
Resource Method	検査する要求メソッドを次に示します。 • [ack]：クライアントがINVITE要求に対する最終的な応答を受信したことを確認します。 • [bye]：コールを終了し、発信側または着信側から送信できます。 • [cancel]：保留中のすべての検索を取り消しますが、すでに受け入れられているコールは終了しません。 • [info]：コールのシグナリング パスを経由する中間セッション シグナリング情報を伝えます。 • [invite]：ユーザまたはサービスがコール セッションへの参加を招待されることを示します。 • [message]：各メッセージが他のメッセージに依存しないインスタント メッセージを送信します。 • [notify]：以前の SUBSCRIBE メソッドによって要求されたイベントが発生したことを SIP ノードに通知します。 • [options]：サーバの機能をクエリーします。 • [prack]：暫定応答確認。 • [refer]：受信者が要求で提供されているリソースを参照することを要求します。 • [register]：Toヘッダー フィールドにリストされているアドレスを SIP サーバに登録します。 • [subscribe]：1 つのイベントまたは一連のイベントに関する通知をあとで受け取ることを要求します。 • [unknown]：ネットワークのセキュリティに未知の影響を与える可能性がある非標準拡張を使用します。 • [update]：セッションのパラメータを更新することをクライアントに許可しますが、ダイアログの状態に影響はありません。

Skinny マップの設定

[Add Skinny Map]/[Edit Skinny Map] ダイアログボックスを使用して、Skinny インスペクションの Skinny マップを定義します。Skinny ポリシー マップを使用すると、Skinny インスペクションに使用するデフォルト設定値を変更できます。

Skinny（SCCP）は、VoIP ネットワークで使用される簡易プロトコルです。SCCP を使用する Cisco IP Phone は、H.323 環境でも使用できます。Cisco CallManager とともに使用する場合、

SCCP クライアントは H.323 準拠端末と相互運用できます。セキュリティ アプライアンスのアプリケーション層機能は、SCCP バージョン 3.3 を認識します。SCCP プロトコルには、2.4、3.0.4、3.1.1、3.2、3.3.2 の 5 つのバージョンがあります。

セキュリティ アプライアンスでは、3.3.2 までのすべてのバージョンがサポートされます。セキュリティ アプライアンスでは、SCCP に対して PAT と NAT がサポートされます。IP 電話で使用できるグローバル IP アドレスよりも IP 電話が多い場合は、PAT が必要です。SCCP シグナリング パケットの NAT および PAT をサポートすることで、Skinny アプリケーションは、すべての SCCP シグナリングおよびメディア パケットがセキュリティ アプライアンスを通過できることを保証します。

Cisco CallManager と Cisco IP Phones 間の通常のトラフィックは SCCP を使用しており、特別な設定をしなくても SCCP インスペクションによって処理されます。セキュリティアプライアンスでは、DHCP オプション 150 および 66 もサポートされます。これは、TFTP サーバの場所を Cisco IP Phone およびその他の DHCP クライアントに送信することで実現されます。Cisco IP Phone では、デフォルト ルートを設定する DHCP オプション 3 を要求に含めることもできます。

ナビゲーション パス

[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択し、次にオブジェクトタイプセレクタから [マップ（Maps）] > [ポリシーマップ（Policy Maps）] > [検査（Inspect）] > [Skinny] を選択します。作業領域内を右クリックしてから [新規オブジェクト(New Object] を選択するか、行を右クリックしてから [オブジェクトの編集（Edit Object）] を選択します。

関連項目

- マップ オブジェクトについて
- インスペクションのプロトコルおよびマップの設定 （28 ページ）

フィールド リファレンス

表 *50 : [Add Skinny Map]/[Edit Skinny Map]* ダイアログボックス

要素	説明
名前	Skinny マップの名前。最大 40 文字を使用できます。
説明	最大 200 文字の Skinny マップの説明。
[パラメータ（Parameters）] タブ	
Enforce Endpoint Registration	コールを行う前に登録を強制するかどうか。
Maximum SCCP Station Message ID 0x	許可される SCCP スタティック メッセージ ID の最大数（16 進数）。

要素	説明
Check RTP Packets for Protocol Conformance Enforce Payload Type to be Audio or Video based on Signaling Exchange	プロトコル準拠のために、RTP パケットのフローがピンホールを経由することを調べるかどうか。このオプションを選択した場合は、ペイロード タイプを強制するかどうかも選択できます。
Minimum SCCP Prefix Length	許可される最小の SCCP 長。
Maximum SCCP Prefix Length	許可される最大の SCCP 長。
Media Timeout	メディア接続のタイムアウト値。
Signaling Timeout	シグナリング接続のタイムアウト値。
[Match Condition and Action] タブ [Match All] テーブルに、ポリシー マップに含まれている基準が表示されます。各行には、各基準に一致する、または一致しないトラフィックを検査で検索するかどうか、検査される基準と値、および条件を満たすトラフィックに対して実行されるアクションが示されます。 • 基準を追加するには、[Add] ボタンをクリックし、[Match Condition and Action] ダイアログボックスに入力します（Skinny ポリシー マップの [Add Match Condition and Action]/[Edit Match Condition and Action] ダイアログボックス （121 ページ）を参照）。 • 基準を編集するには、基準を選択し、[Edit] ボタンをクリックします。 • 基準を削除するには、基準を選択し、[Delete] ボタンをクリックします。	
カテゴリ	オブジェクトに割り当てられたカテゴリ。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。
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、ポリシー オブジェクトの上書きの許可および個々のデバイスのポリシー オブジェクト オーバーライドについてを参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）] ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）] フィールドには、このオブジェクトをオーバーライドするデバイスの数が表示されます。

Skinny ポリシー マップの [Add Match Condition and Action]/[Edit Match Condition and Action] ダイアログボックス

[Add Match Condition and Action]/[Edit Match Condition and Action] ダイアログボックスを使用して、Skinny ポリシー マップの一致基準、値、およびアクションを定義します。

ナビゲーション パス

[Policy Object Manager] で、[スキニーマップの追加（Add Skinny Map）]/[スキニーマップの編集（Edit Skinny Map）] ダイアログボックスの [一致条件とアクション（Match Condition and Action）] タブのテーブル内を右クリックして [行の追加（Add Row）] を選択するか、行を右クリックして [行の編集（Edit Row）] を選択します。 Skinny マップの設定 （118 ページ） を参照してください。

関連項目

- マップ オブジェクトについて
- インスペクションのプロトコルおよびマップの設定 （28 ページ）

フィールド リファレンス

表 *51 : Skinny* ポリシー マップの *[Add Match Condition and Action]/[Edit Match Condition and Action]* ダイアログボックス

要素	説明
基準	照合する Skinny トラフィック基準を指定します。
タイプ（Type）	基準に一致する、または一致しないトラフィックをマップに含めるかどうかを指定します。たとえば、0xFFFF で [一致しない（Doesn't Match）] が選択されている場合は、メッセージ ID が 0xFFFF であるすべてのトラフィックがマップから除外されます。 • [Matches]：基準に一致する。 • [一致しない（Doesn't Match）]：基準に一致しない。
ID Type	検査するメッセージ ID の 16 進値。 • [Value]：単一の 16 進数値を照合します。 • [Range]：値の範囲を照合します。
操作	定義された基準に一致するトラフィックに対してデバイスが適用するアクション。

SNMP マップの設定

[Add SNMP Map]/[Edit SNMP Map] ダイアログボックスを使用して、SNMP インスペクションのマップを定義します。SNMP ポリシー マップを使用すると、SNMP アプリケーション インスペクションに使用するデフォルト設定値を変更できます。

SNMP アプリケーション インスペクションでは、SNMP トラフィックを特定のバージョンの SNMP に制限できます。以前のバージョンの SNMP は安全性が低いため、セキュリティ ポリシーを使用して特定の SNMP バージョンを拒否する必要が生じる場合もあります。セキュリティ アプライアンスでは、SNMP バージョン 1、2、2c、または 3 を拒否できます。許可するバージョンは、SNMP マップを作成して制御します。さらに、SNMP インスペクションをイネーブルにする場合に SNMP マップを適用します。

ナビゲーション パス

[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択し、オブジェクトタイプセレクタから [マップ（Maps）] > [ポリシーマップ（Policy Maps）] > [検査（Inspect）] > [SNMP] を選択します。作業領域内を右クリックしてから [新規オブジェクト（New Object）] を選択するか、行を右クリックしてから [オブジェクトの編集（Edit Object）] を選択します。

関連項目

- マップ オブジェクトについて
- インスペクションのプロトコルおよびマップの設定 （28 ページ）

フィールド リファレンス

表 *52 : [SNMP*マップの追加（*Add SNMP Map*）*]/[SNMP*マップの編集（*Edit SNMP Map*）*]* ダイアログボックス

要素	説明
名前	ポリシー オブジェクトの名前。最大 40 文字を使用できます。
説明	ポリシー オブジェクトの説明。最大 200 文字を使用できます。
Disallowed SNMP Versions	禁止する SNMP のバージョン。 • SNMP Version 1 • SNMP Version 2c（コミュニティ ベース） • SNMP Version 2（パーティ ベース） • SNMP バージョン 3
カテゴリ	オブジェクトに割り当てられたカテゴリ。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。

要素	説明
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、ポリシー オブジェクトの上書きの許可および個々のデバイスのポリシー オブジェクト オーバーライドについてを参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）] ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）] フィールドには、このオブジェクトをオーバーライドするデバイスの数が表示されます。

SCTP マップの設定

SCTP は、TCP や UDP と同様、プロトコル スタックの IP の最上部で動作するトランスポート層プロトコルです。SCTP は、複数の送信元 IP アドレスまたは宛先 IP アドレス上の 2 つのエンドノード間でアソシエーションと呼ばれる論理的な通信チャネルを作成します。アソシエーションでは、各ノード（送信元と宛先）での IP アドレスのセットと、各ノードでのポートが定義されます。任意の IP アドレスを、アソシエーションのデータパケットの送信元または宛先 IP アドレスとして使用できます。メッセージは、ストリームとして定義された IP アドレスのペア間で送信できます。

ASA を通過する SCTP トラフィックがある場合、SCTP ポートに基づいてアクセスを制御するために Cisco Security Manager を設定し、アプリケーション層のインスペクションを導入して、接続を有効にし、必要に応じてペイロードプロトコル ID でフィルタ処理を実行し、アプリケーションを選択的にドロップ、ログに記録、またはレート制限できます。

SCTP 検査マップを追加し、SCTP アプリケーションでフィルタリングすることにより、アクセスルールを改善できます。ペイロードプロトコル識別子（PPID）に基づいて、SCTP トラフィッククラスを選択的にドロップ、ログに記録、またはレート制限できます。

PPID でフィルタ処理する場合は、次の点に注意してください。

- PPID はデータ チャンクに含まれており、1 つのパケットが複数のデータ チャンクを持つ場合があります。パケットに異なる PPID を持つデータ チャンクが含まれている場合、パケットはフィルタ処理されず、割り当てられたアクションがパケットに適用されません。
- PPID フィルタリングを使用してパケットをドロップまたはレート制限する場合は、トランスミッタによりドロップされたパケットが再送されることに注意してください。レート制限が適用された PPID のパケットは再試行で通過する可能性がありますが、ドロップされた PPID のパケットは再びドロップされます。ネットワーク上のこのような反復的ドロップの最終成果を評価することができます。

[SCTPマップの追加（Add SCTP Map）]/[SCTPマップの編集（Edit SCTP Map）] ダイアログボックスを使用して、SCTP 検査マップの一致基準と値を定義します。SCTP マップを使用して、ペイロード PID 基準に基づいてパケットを検査できます。PPID 一致基準に基づいて、パケットに対して次のアクションを実行できます。

- アクションなし
- パケットのドロップ
- パケットのログ記録
- レート制限

SCTPプロトコルに対応するサービスオブジェクトは、マップオブジェクトについてのサービステーブルで利用できます。

（注） SCTP 検査マップは、Cisco Security Manager 4.10 および ASA バージョン 9.5.2 以降でサポートされています。

ナビゲーション パス

[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択し、オブジェクトタイプセレクタから **[マップ（Maps）] > [ポリシーマップ（Policy Maps）] > [検査（Inspect）] > [SCTP]** を選択します。テーブル内を右クリックしてから [新規オブジェクト（New Object）] を選択するか、行を右クリックしてから [オブジェクトの編集（Edit Object）] を選択します。

関連項目

- Policy Object Manager
- インスペクションのプロトコルおよびマップの設定 （28 ページ）

フィールド リファレンス

表 *53 : [SCTP*マップの追加（*Add SCTP Map*）*]/[SCTP*マップの編集（*Edit SCTP Map*）*]* ダイアログボックス

要素	説明
名前	ポリシー オブジェクトの名前。最大 40 文字を使用できます。
説明	ポリシー オブジェクトの説明。最大200 文字を使用できます。
[Match Condition and Action] タブ [Match All] テーブルに、ポリシー マップに含まれている基準が表示されます。各行には、各基準に一致する、または一致しないトラフィックを検査で検索するかどうか、検査される基準と値、および条件を満たすトラフィックに対して実行されるアクションが示されます。 これらの基準エントリは、SCTP ポリシーマップの [一致条件とアクションの追加または編集（Add or Edit Match Condition and Action] ダイアログボックス （125 ページ）で作成および編集されます。	

要素	説明
カテゴリ	オブジェクトに割り当てられたカテゴリ。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。
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、ポリシー オブジェクトの上書きの許可および個々のデバイスのポリシー オブジェクト オーバーライドについてを参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）] ボタンをクリックして、[Policy Object Overrides] ウィンドウでオーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）] フィールドには、このオブジェクトに対するオーバーライドを持つデバイスの数が表示されます。

SCTP ポリシーマップの [一致条件とアクションの追加または編集（Add or Edit Match Condition and Action] ダイアログボックス

[一致条件とアクションの追加（Add Match Condition and Action）]/[一致条件とアクションの編集（Edit Match Condition and Action）] ダイアログボックスを使用して、SCTP ポリシーマップのペイロードPIDの一致基準およびアクションを定義します。選択的に処理するすべてのPPIDを識別するまで、プロセスを繰り返します。

ナビゲーション パス

[Policy Object Manager] で、[IPv6マップの追加または編集（Add or Edit IPv6 Map）] ダイアログボックスの [一致条件とアクション（Match Condition and Action）] タブのテーブル内を右クリックして [行を追加（Add Row）] を選択するか、行を右クリックして [行の編集（Edit Row）] を選択します。 IPv6 マップの設定 （102 ページ） を参照してください。

関連項目

- マップ オブジェクトについて
- インスペクションのプロトコルおよびマップの設定 （28 ページ）

フィールド リファレンス

表 *54 : IPv6* ポリシーマップの *[*一致条件とアクションの追加または編集（*Add or Edit Match Condition and Action]* ダイアログボックス

要素	説明
基準	ペイロード PID（PPID）基準を選択します。

要素	説明
タイプ（Type）	定義された基準に一致するトラフィック、または一致しないトラフィックにのみマップが適用されることを指定します。
SCTP PPID の現在のリストは http://www.iana.org/assignments/sctp-parameters/sctp-parameters.xhtml#sctp-parameters-25 で確認できます。	
最小ペイロード PID	PPID 番号を入力します。Cisco Security Manager が受け入れ、内部で処理される、名前に関連付けられた特定の PPID があります。テキストボックスに PPID 番号を入力し、[OK] をクリックします。デフォルト名と一致する場合、対応する名前が一致アクションテーブルに表示されます。
最大ペイロード PID	（オプション）2番目に高いPPIDを入力して、PPIDの範囲を指定します。
操作	SCTP データチャンクの PPID に基づいてアクションを選択します。 • [パケットをドロップ（Drop Packet）]：一致するすべてのパケットをドロップし、ログに記録します。 • [ログ（Log）]：システムログメッセージを送信します。 • [レート制限（Rate Limit）]：メッセージのレートを制限します。1秒間のパケット数で表したレートです。

Diameter マップの設定

Diameter は、LTE（Long Term Evolution）および IMS（IP Multimedia Subsystem）用の EPS（Evolved Packet System）などの次世代モバイルと固定電気通信ネットワークで使用される認証、認可、およびアカウンティング（AAA）プロトコルです。RADIUS や TACACS がこれらのネットワークで Diameter に置き換えられます。

Diameter はトランスポート層として TCP および SCTP を使用し、TCP/TLS および SCTP/DTLS によって通信を保護します。また、オプションで、データ オブジェクトの暗号化も提供できます。Diameter の詳細については、RFC 6733 を参照してください。

Diameterアプリケーションは、課金のユーザー アクセス、サービス認証、QoS、およびレートの決定といったサービス管理タスクを実行します。Diameter アプリケーションは LTE アーキテクチャのさまざまなコントロール プレーン インターフェイスで使用されますが、ASA は、

次のインターフェイスについてのみ、Diameter コマンド コードおよび属性値ペア（AVP）を検査します。

- S6a：モビリティ マネージメント エンティティ（MME）- ホーム サブスクリプション サービス（HSS）
- S9：PDN ゲートウェイ（PDG）- 3GPP AAA プロキシ/サーバー
- Rx：ポリシー/課金ルール機能（PCRF） - コール セッション制御機能（CSCF）

Diameter インスペクションでは、Diameter エンドポイント用にピンホールを開いて通信を可能にします。このインスペクションは、3GPP バージョン 12 をサポートし、RFC 6733 に準拠しています。

パケットや接続のドロップまたはロギングなどの特別なアクションを適用するために、[Diameter マップの追加（Add Diameter Map）] および [Diameterマップの編集（Edit Diameter Map）] ダイアログボックスを使用し、アプリケーション ID、コマンドコード、および AVP に基づいてトラフィックをフィルタリングできます。新規に登録された Diameter アプリケーション用のカスタム AVP を作成できます。フィルタリングにより、ネットワークで許可するトラフィックを微調整できます。詳細については、カスタム AVP の作成と追加 （132 ページ）を参照してください。

（注） 他のインターフェイス上で動作するアプリケーションに対する Diameter メッセージはデフォルトで許可され、渡されます。ただし、アプリケーション ID によって該当するアプリケーションを破棄するための Diameter インスペクション ポリシー マップを設定できます。これらのサポートされていないアプリケーションに対してコマンドコードまたは AVP に基づいてアクションを指定することもできます。

ナビゲーション パス

[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択し、次にオブジェクト タイプセレクタから [マップ（Maps）] > [ポリシーマップ（Policy Maps）] > [調査（Inspect）] > [Diameter] を選択します。作業領域内を右クリックしてから [新規オブジェクト（New Object）] を選択するか、行を右クリックしてから [オブジェクトの編集（Edit Object）] を選択します。

関連項目

- マップ オブジェクトについて
- インスペクションのプロトコルおよびマップの設定 （28 ページ）
- インスペクション ポリシーのクラス マップの設定 （34 ページ）
- カスタム AVP の作成と追加 （132 ページ）

フィールド リファレンス

表 *55 : [Diameter*マップの追加および編集（*Add and Edit Diameter Map*）*]* ダイアログボックス

要素	説明
名前	ポリシー オブジェクトの名前。最大 128 文字を使用できます。
説明	ポリシー オブジェクトの説明。最大 200 文字を使用できます。
[パラメータ（Parameters）] タブ	
[サポートされていないアプリケーションIDアクションログ（Unsupported application-id action log）]	マップ内のサポートされていない Diameter アプリケーション識別子（Diameter アプリケーション名）を記録します。 アプリケーション ID は、マップ内の 0 ～ 4294967295 の番号です。これらのアプリケーションは IANA に登録されます。次のコア アプリケーションがサポートされますが、他のアプリケーションもフィルタ処理できます。 3gpp-rx-ts29214（16777236） 3gpp-s6a（16777251） 3gpp-s9（16777267） common-message（0）：これは基本 Diameter プロトコルです。
[サポートされていないコマンドコードアクションログ（Unsupported command code action log）]	サポートされていない Diameter コマンドコードを記録します。コードは Diameter コマンドコードの名前または番号（0 ～ 4294967295）です。
[サポートされていないAVPアクションログ（Unsupported avp action log）]	サポートされていない属性と値のペアのパラメータをログに記録します。
[厳格なパラメータ（Strict Parameters）]	
[セッション検証の有効化（Enable Session Validation）]	セッション ID AVP 関連メッセージを検証します。
[ステート検証の有効化（Enable State Validation）]	ステートマシンの検証を有効にします。

要素	説明
[Match Condition and Action] タブ [Match All] テーブルに、ポリシー マップに含まれている基準が表示されます。各行には、各基準に一致する、または一致しないトラフィックを検査で検索するかどうか、検査される基準と値、および条件を満たすトラフィックに対して実行されるアクションが示されます。 • 基準を追加するには、[Add] ボタンをクリックし、[Match Condition and Action] ダイアログボックスに入力します（Diameter クラスとポリシーマップの [一致条件（とアクション）の追加または編集（Add or Edit Match Condition (and Action)] ダイアログボックス（129 ページ）を参照）。 • 基準を編集するには、基準を選択し、[Edit] ボタンをクリックします。 • 基準を削除するには、基準を選択し、[Delete] ボタンをクリックします。	
カテゴリ	オブジェクトに割り当てられたカテゴリ。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。
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、ポリシー オブジェクトの上書きの許可および個々のデバイスのポリシー オブジェクト オーバーライドについてを参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）] ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）] フィールドには、このオブジェクトをオーバーライドするデバイスの数が表示されます。

Diameter クラスとポリシーマップの [一致条件（とアクション）の追加または編集（Add or Edit Match Condition (and Action)] ダイアログボックス

[Diameter一致基準の追加（Add Diameter Match Criterion）]/[Diameter一致基準の編集（Edit Diameter Match Criterion）] ダイアログボックス（Diameter クラスマップの場合）または [一致条件とアクション（Match Condition and Action）] ダイアログボックス（Diameter ポリシーマップの場合）を使用して、次の処理を行います。

- Diameter クラスマップの一致基準と値を定義する。
- Diameter ポリシーマップを作成するときに、Diameter クラスマップを選択する。
- Diameter ポリシーマップに直接、一致基準、値、およびアクションを定義する。

このダイアログボックスのフィールドは、選択した基準、およびクラスマップとポリシーマップのどちらを作成しているかによって変わります。

ナビゲーション パス

Diameter クラスマップを作成している場合は、Policy Object Manager で、Diameter の [クラスマップの追加（Add Class Maps）]/[クラスマップの編集（Edit Class Maps）] ダイアログボックスのテーブル内を右クリックして [行の追加（Add Row）] を選択するか、行を右クリックして [行の編集（Edit Row）] を選択します。インスペクション ポリシーのクラス マップの設定（34 ページ）を参照してください。

Diameter ポリシーマップを作成している場合は、[Policy Object Manager] で、Diameterマップの追加（Add Diameter Map）]/[Diameterマップの編集（Edit Diameter Map）] ダイアログボックスの [一致条件とアクション（Match Condition and Action）] タブのテーブル内を右クリックして [行の追加（Add Row）] を選択するか、行を右クリックして [行の編集（Edit Row）] を選択します。Diameter マップの設定 （126 ページ） を参照してください。

関連項目

- マップ オブジェクトについて
- インスペクションのプロトコルおよびマップの設定 （28 ページ）

フィールド リファレンス

表 56 : Diameter クラスとポリシーマップの [一致条件とアクションの追加および編集（Add and Edit Match Condition and Action）] ダイアログボックス

要素	説明
一致タイプ（Match Type） （ポリシーマップのみ）	既存の Diameter クラスマップを使用するか、新しい Diameter クラスマップを定義できます。 • [Use Specified Values]：このダイアログボックスでクラス マップを定義する場合。 • [Use Values in Class Map]：既存の Diameter クラス マップ ポリシー オブジェクトを選択する場合。Diameter クラスマップの名前を [クラス名（Class Name）] フィールドに入力します。[選択（Select）] をクリックしてリストからマップを選択するか、新しいクラスマップオブジェクトを作成します。

要素	説明
基準	照合する Diameter トラフィックの基準を指定します。 • [Application ID]：アプリケーション ID を照合します。アプリケーション ID は、[開始値（Begin Value）] フィールドの Diameter アプリケーションの名前または番号（0 ～ 4294967295）です。照合したい連続する番号が付いたアプリケーションの範囲がある場合は、[開始値（Begin Value）] フィールドの 2 番目の ID を含めることができます。アプリケーションの名前または番号別に範囲を定義でき、開始値と終了値間のすべての番号に適用されます。 • [Command Code]：コマンドコードを照合します。コードは、[開始値（Begin Value）] フィールドの Diameter コマンドコードの名前または番号（0 ～ 4294967295）です。照合したい連続する番号が付されたコマンドコードの範囲がある場合は、[開始値（Begin Value）] フィールドの 2 番目のコードを含めることができます。コマンド コードの名前または番号別に範囲を定義でき、開始値と終了値間のすべての番号に適用されます。 • [AVP]：属性値ペアを照合します。 • AVB ベースの属性値のみ照合するには、属性値ペアの名前または番号（1 ～ 4294967295）を指定します。最初のコードについては、カスタム AVP、RFC または 3GPP 技術仕様に登録されている AVP、およびソフトウェアで直接サポートされている AVP の名前を [開始値（Begin Value）] フィールドで指定できます。AVP の範囲を照合する場合は、[開始値（Begin Value）] フィールドの 2 番目のコードを番号で指定します。値によって AVP を照合する場合は、2 番目のコードを指定できません。[ベンダーID（Vendor ID）] フィールドに、一致するベンダーの ID 番号（0 ～ 4294967295）を指定します。たとえば、3GPP ベンダー ID は 10415、IETF は 0。 • 属性の値に基づいて AVP を照合するには、[AVPデータタイプ（AVP Data Type）] フィールドで追加の属性値を指定します。 （注） カスタム AVP を作成して、新規 Diameter アプリケーションに追加できます。詳細については、以下を参照してください。 カスタム AVP の作成と追加 （132 ページ）
タイプ（Type）	基準に一致する、または一致しないトラフィックをマップに含めるかどうかを指定します。たとえば、文字列「example.com」で[一致しない（Doesn't Match）] を選択した場合、「example.com」を含むトラフィックはすべてマップの対象外になります。 • [Matches]：基準に一致する。 • [一致しない（Doesn't Match）]：基準に一致しない。

要素	説明
可変フィールド 次のフィールドは、[Criterion] フィールドでの選択内容によって変わります。このリストは、表示されると想定されるフィールドのスーパーセットです。	
AVP データタイプ（AVP DataType）	これは、AVP の データ タイプがサポートされている場合にのみ設定できます。たとえば、アドレス データ タイプがある AVP の IP アドレスを指定できます。次に、サポートされているデータタイプの値オプションの特定の構文を示します。 • [Address]：照合する IPv4 または IPv6 アドレスを指定します。例：10.100.10.10 または 2001:DB8::0DB8:800:200C:417A。 • [Diameter Identity]、[Diameter URI]、[Octet String]、[UTF8tString]：これらのデータタイプの照合には正規表現または正規表現クラスオブジェクトを使用します。 • [Enumerated]：[開始範囲（Begin Range）] および [終了範囲]（End Range）] フィールドで数値の範囲を指定します。範囲は 0 ～ 4294967295 です。 • Float32：8 桁の小数点表現 • Float64：16 桁精度の小数点表記 • Integer32：-2147483647 ～ 2147483647 • Integer64：-9223372036854775807 ～ 9223372036854775807 • Unsigned32：0 ～ 4294967295 • Unsigned64：0 ～ 18446744073709551615 • [Time]：開始日時と終了日時を指定します。両方を指定する必要があります。時間は 24 時間形式で指定します。 （注） カスタム AVP を作成して、新規 Diameter アプリケーションに追加できます。
操作 （ポリシー マップのみ）	定義された基準に一致するトラフィックに対してデバイスが適用するアクション。

カスタム AVP の作成と追加

[AVPの追加（Add AVP）] ダイアログボックスを使用して、カスタム AVP を作成および追加します。カスタム AVP は IETF に登録して、新しい Diameter アプリケーションに追加できます。

（注） Cisco Security Manager では、一度作成したカスタム AVP オブジェクトは編集できません。ただし、[デバイスオーバーライド（Device Override）] オプションを使用すると、特定のデバイスのカスタム AVP を編集できます。カスタム AVP オブジェクトのパラメータを変更する場合は、Diameter 構成要素からカスタム AVP 参照を削除し（参照されている場合）、デバイスに展開します（デバイスに存在する場合）。次に、必要な値を設定してオブジェクトを再作成し、Diameter 構成要素で参照し直して、再度展開します。

ナビゲーション パス

Policy Object Manager でカスタム AVP を作成する場合、Diameter の [一致基準の追加（Add Match Criterion）] ダイアログボックスから [基準のAVP（AVP in the Criterion）] を選択し、[開始値（Begin Value）] を選択して、[AVPマップセレクタ（AVP Maps Selector）] ダイアログボックスで右クリックして AVP を追加します。

フィールド リファレンス

表 *57 : [AVP*の追加（*Add AVP***）*]* ダイアログボックス**

要素	説明
名前	カスタム AVP の名前。最大 32 文字で指定できます。 （注） 名前の少なくとも 1 文字はアルファベットにする必要があります。
説明	AVP の説明。最大 80 文字で指定できます。
AVP コード	特定のベンダーコードアドレス空間に属する AVP コード（256 ～ 4294967295）の値を設定します。

要素	説明
データタイプ（DataType）	これは、AVP の データ タイプがサポートされている場合にのみ設定できます。たとえば、アドレス データ タイプがある AVP の IP アドレスを指定できます。次に、サポートされているデータタイプの値オプションに固有の構文を示します。 • [Address]：照合する IPv4 または IPv6 アドレスを指定します。例：10.100.10.10 または 2001:DB8::0DB8:800:200C:417A。 • [Diameter Identity]、[Diameter URI]、[Octet String]、[UTF8tString]：これらのデータタイプの照合には正規表現または正規表現クラスオブジェクトを使用します。 • [Enumerated）]：[開始範囲（Begin Range）] および [終了範囲（End Range）] フィールドで数値の範囲を指定します。範囲は 0 ～ 4294967295 です。 • Float32：8 桁の小数点表現 • Float64：16 桁精度の小数点表記 • Integer32：-2147483647 ～ 2147483647 • Integer64：-9223372036854775807 ～ 9223372036854775807 • Unsigned32：0 ～ 4294967295 • Unsigned64：0 ～ 18446744073709551615 • [Time]：開始日時と終了日時を指定します。両方を指定する必要があります。時間は 24 時間形式で指定します。
ベンダー ID	[ベンダーID（Vendor ID）] フィールドに、ベンダーの ID 番号（0 ～ 4294967295）を指定します。たとえば、3GPP ベンダー ID は 10415、IETF は 0。
カテゴリ	オブジェクトに割り当てられたカテゴリ。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。
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、ポリシー オブジェクトの上書きの許可および個々のデバイスのポリシー オブジェクト オーバーライドについてを参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）] ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）] フィールドには、このオブジェクトに対するオーバーライドを持つデバイスの数が表示されます。

TLS プロキシオブジェクトの作成と追加

Diameter アプリケーションが TCP 上で暗号化されたデータを使用する場合、インスペクションはメッセージのフィルタリング ルールを実装するためにパケット内を確認することはできません。したがって、フィルタリング ルールを作成し、それらを暗号化された TCP トラフィックにも適用する場合は、TLS プロキシを設定する必要があります。暗号化されたトラフィックで厳密なプロトコルを適用するには、プロキシも必要です。この設定は SCTP/DTLS トラフィックには適用されません。

TLS プロキシは中間者として機能します。このプロキシは、トラフィックを復号化し、検査してから再度暗号化し、目的の宛先に送信します。したがって、接続の両側（Diameter サーバーと Diameter クライアント）は ASA を信頼する必要があり、すべての当事者が必要な証明書を保有している必要があります。TLS プロキシを実装するには、デジタル証明書を十分に理解しておく必要があります。

（注） TLS プロキシ機能は、バージョン ASA 9.7.1 以降のマルチコンテキストデバイスでサポートされています。

Diameter インスペクション用の TLS プロキシを設定するには、次のオプションがあります。

- フル TLS プロキシ：ASA および Diameter クライアントと ASA および Diameter サーバー間のトラフィックを暗号化します。サーバーとの信頼関係を確立するには、次のオプションがあります。
  - スタティック プロキシ クライアント トラストポイントを使用します。ASA は、Diameter サーバーとの通信時に、すべての Diameter クライアントに同じ証明書を示します。Diameter サーバーにとって全クライアントが同じように見えるので、クライアントごとに差別化サービスを提供することはできません。一方、このオプションは LDC 方式よりも高速です。
  - ローカルダイナミック証明書（LDC）を使用します。このオプションを使用すると、ASA は Diameter サーバーとの通信時に、Diameter クライアントごとに一意の証明書を示します。この方法では、Diameter サーバーでクライアントトラフィックの可視性が向上し、クライアントの特性に基づいて差別化サービスを提供できるようになります。
- TLS オフロード：ASA と Diameter クライアント間のトラフィックを暗号化しますが、ASA と Diameter サーバー間でクリアテキスト接続を使用します。このオプションは、デバイス間のトラフィックが保護された場所から離れることがないと確信している場合に、Diameter サーバーが ASA と同じデータセンターにあれば実行可能です。TLS オフロードを使用すると、必要な暗号化処理量が減るので、パフォーマンスを向上させることができます。これは、オプションの中で最速です。Diameter サーバーは、クライアントの IP アドレスのみに基づいて差別化サービスを適用できます。

ナビゲーション パス

[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択し、オブジェクトタイプセレクタから [TLS プロキシ（TLS Proxy）] を選択します。作業領域内を右クリックしてから [新規オブジェクト（New Object）] を選択するか、行を右クリックしてから [オブジェクトの編集（Edit Object）] を選択します。

フィールド リファレンス

表 *58 : [TLS* プロキシの追加（*Add TLS Proxy***）*]* ダイアログボックス**

要素	説明
名前	TLS プロキシオブジェクトの名前。最大 63 文字で指定できます。 （注） 名前の少なくとも 1 文字はアルファベットにする必要があります。
説明	TLS プロキシオブジェクトの説明。
サーバーの設定	
[サーバープロキシ証明書（Server Proxy Certificate）]	[選択（Select）] をクリックして、Diameter クライアントの証明書への署名に使用されている CA 証明書を ASA トラストポイントにインポートします。この手順では、TLS ハンドシェイク中に提示するプロキシトラストポイント証明書を指定します。トラストポイントは、自己署名の場合またはサードパーティによって発行される場合があります。 これにより、ASA が Diameter クライアントを信頼できます。
[TLS プロキシハンドシェイク時のクライアント認証を有効化（Enable client authentication during TLS proxy handshake）]	TLS ハンドシェイク時に、ASA に証明書の提示と TLS クライアントの認証を要求する場合にオンにします。

要素	説明
暗号化（オプション）	4.14 以降、Cisco Security Manager では、TLS プロキシがサーバとして使用されている場合に暗号スイートを設定できます。 このフィールドでは、TLSハンドシェイク時に通知/照合される暗号スイートを定義します。 データの暗号化に必要なハッシュアルゴリズムを [使用可能なメンバー（Available Members）] リストから選択して [選択済みのメンバー（Selected Members）] リストに追加します。 （注） 4.19 以降、Cisco Security Manager では、ASA 9.12(1) デバイスの SSL 暗号において TLS プロキシを NULL SHA1 で設定すると、アクティビティ検証エラーメッセージが表示されます。
クライアント設定	
[リモート TCP サーバーとの通信にクリアテキスト使用するようにプロキシクライアントを設定（Configure the proxy client to use clear text to communicate with the remote TCP server）]	暗号化が必要ない場合は、クリアテキストを使用するプロキシクライアントを選択します。
[TLS クライアント用のプロキシ証明書を指定します。このクライアントプロキシ証明書は、自己署名の場合、CA に登録済みの場合、またはサードパーティによって発行される場合があります。（Specify the proxy certificate for the TLS client. The client proxy certificate could either be self-signed, enrolled with a CA or issued by a third party.）]	クライアントプロキシ証明書を指定する場合は、オンにします。 または、[選択（Select）] をクリックして TLS クライアント用の CA 証明書をインポートします。

要素	説明
[電話のローカルダイナミック証明書に署名する内部認証局を指定します。このローカル CA は、proxy-ldc-issuer が有効になっている自己署名証明書にするか、組み込みのローカルCA サーバーを使用して LDC を電話に発行することができます。（Specify the internal Certificate Authority to sign the local dynamic certificates for phones. This local CA can be self-signed certificate with proxy-ldc-issuer enabled or you may use embedded Local CA Server to issue LDC to phones.）]	ローカルダイナミック証明書の発行元を指定する場合は、オンにします。 または、[選択（Select）] をクリックして CA 証明書をインポートします。これは、ローカルダイナミック証明書（LDC）の発行者として機能します。
[ローカルダイナミック証明書のキーペア（Local Dynamic Certificate Key Pair）]	
[キーペア名（Key Pair Name）]	クライアントまたはサーバーのダイナミック証明書で使用する RSA キーペアを指定します。このキーペアは、「crypto key generate」コマンドで生成されている必要があります。 キーペアは、展開前にデバイスに存在している必要があります。
暗号化（オプション）	TLS ハンドシェイク時に通知/照合される暗号スイートを定義します。クライアントプロキシ（このプロキシはサーバーに対する TLS クライアントとして機能します）の場合、2 つの TLS レッグ間の非対称暗号化方式のために、ユーザー定義の暗号スイートで Hello メッセージの元の暗号スイートが置き換えられます。 データの暗号化に必要なハッシュアルゴリズムを [使用可能なメンバー（Available Members）] リストから選択して [選択済みのメンバー（Selected Members）] リストに追加します。 （注） ASA バージョン 9.7.1 以降、Cisco Security Manager は TLS1.2 の新しい暗号スイート（aes256-sha384 および aes128-sha256）をサポートしています。
カテゴリ	オブジェクトに割り当てられたカテゴリ。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。

要素	説明
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、ポリシー オブジェクトの上書きの許可および個々のデバイスのポリシー オブジェクト オーバーライドについてを参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）] ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）] フィールドには、このオブジェクトをオーバーライドするデバイスの数が表示されます。

TLS プロキシオブジェクトの編集

Cisco Security Manager では、一度作成された TLS プロキシオブジェクトを編集することはできません。ただし、[デバイスの上書き（Device Override）] オプションを使用すると、特定のデバイスの TLS プロキシオブジェクトを編集できます。

TLS プロキシオブジェクトのパラメータを変更する場合は、Diameter 構成要素（これを参照している場合）から TLS プロキシ参照を削除し、デバイスに展開します（デバイスに存在する場合）。次に、新しい名前と必要な値でオブジェクトを再作成し、それを Diameter 構成要素内で参照し直し、再度展開します。

クラスマップで TLS プロキシを編集するには、次の展開手順を実行します。

1. [プラットフォーム（Platform）] > [サービスポリシー（Service Policy] > [ルール（Rules）] に移動して、デバイスから既存の TLS プロキシサーバーを含む関連するクラスマップを削除します。
2. [プラットフォーム（Platform）]>[サービスポリシー（Service Policy）]>[ルール（Rules）] に移動して、新しい TLS プロキシサーバーを含む関連するクラスマップをデバイスに展開します。

LISP マップの設定

Locator/ID Separation Protocol（LISP）は、ネットワーク アーキテクチャ兼プロトコルです。LISP は、単一の IP アドレスを 2 つのナンバリング スペースで置き換えます。ナンバリング スペースの一方は、ネットワーク接続ポイントにトポロジ的に割り当てられ、そのネットワーク経由のパケットのルーティングおよび転送に使用されるルーティング ロケータ（RLOC）です。もう一方は、ネットワーク トポロジとは関係なく割り当てられ、ナンバリング デバイスに使用されて管理境界で集約されるエンドポイント ID です。

LISP が定義しているのは、これら 2 つのナンバリング スペースをマッピングし、ルーティング不可能な EID を使用してデバイスから発信されたトラフィックを、ルーティングと転送に RLOC を使用するネットワーク インフラストラクチャで転送できるようにカプセル化するための機能です。LISP では、デバイスがルーティング不可能な EID をルーティング可能な RLOC にマップする際に使用する情報を交換するための一連の機能を提供しています。

LISP での ACL の展開を検討する場合、次の側面が重要です。

- LISP カプセル化では、すべてのパケットの LISP ヘッダーの直前にある UDP ヘッダーを使用して、2つの異なるパケットグループを区別します。UDP宛先ポート（4342）を使用する LISP コントロール プレーン パケットと、UDP 宛先ポート（4341）を使用する LISP データプレーンパケットです。ACL では、これら2つのパケットグループ間の区別を考慮する必要がある場合があります。
- LISP はカプセル化プロトコルであり、ACL ではレイヤ 3 およびレイヤ 4 ヘッダー情報に基づいてのみフィルタ処理されるため、サイトのセキュリティポリシーを実装するためには、パケット転送および LISP カプセル化プロセス内の特定のポイントまたは複数の異なるポイントで ACL を適用する必要がある場合があります。ACL のアプリケーションポイントと方向によって、ACL 自体の中で EID 名前空間と RLOC 名前空間のどちらが使用されるかが決まります。パケットは、LISP カプセル化の直前または LISP カプセル化解除の直後に、EID名前空間を使用してフィルタ処理できます。パケットは、LISP カプセル化の直後または LISP カプセル化解除の直前に、RLOC 名前空間を使用してフィルタ処理できます。

[LISPマップの追加（Add LISP Map）] および [LISPマップの編集（Edit LISP Map）] ダイアログボックスを使用して、EIDアクセスリストと検証キーに基づいてトラフィックをフィルタ処理できます。フィルタリングにより、ネットワークで許可するトラフィックを微調整できます。

ナビゲーション パス

[管理（Manage）]>[ポリシーオブジェクト（Policy Objects）]を選択し、オブジェクトタイプセレクタから**[マップ（Maps）]>[ポリシーマップ（Policy Maps）]>[検査（Inspect）]>[LISP]**を選択します。作業領域内を右クリックしてから [新規オブジェクト（New Object）] を選択するか、行を右クリックしてから [オブジェクトの編集（Edit Object）] を選択します。

関連項目

- マップ オブジェクトについて
- インスペクションのプロトコルおよびマップの設定 （28 ページ）
- インスペクション ポリシーのクラス マップの設定 （34 ページ）

フィールド リファレンス

表 *59 : [LISP*マップの追加および編集（*Add and Edit LISP Map***）*]* ダイアログボックス**

要素	説明
名前	ポリシー オブジェクトの名前。最大 40 文字を使用できます。
説明	ポリシー オブジェクトの説明。最大200 文字を使用できます。
[パラメータ（Parameters）] タブ	

要素	説明
許可されたEIDアクセスリスト（Allowed Eid access-list）	統合アクセスリストの構成要素を選択できます。
検証キー（Validation key）	暗号化されていないクリアテキストパスワードを指定します。
カテゴリ	オブジェクトに割り当てられたカテゴリ。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。
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、ポリシー オブジェクトの上書きの許可および個々のデバイスのポリシー オブジェクト オーバーライドについてを参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）] ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）] フィールドには、このオブジェクトに対するオーバーライドを持つデバイスの数が表示されます。

M3UA マップの設定

MTP3 User Adaptation（M3UA）は、SS7 Message Transfer Part 3（MTP3）レイヤと連動する IP ベースアプリケーション用の SS7 ネットワークへのゲートウェイを提供するクライアント/サーバー プロトコルです。M3UA により、IP ネットワーク上で SS7 ユーザー パート（ISUP など）を実行することが可能になります。M3UA は RFC 4666 で定義されています。

M3UA は SCTP をトランスポート層として使用します。SCTP ポート 2905 が想定されるポートですが、異なるポートを使用するようにシグナリング ゲートウェイを設定することもできます。

MTP3 レイヤは、ルーティングおよびノードアドレッシングなどのネットワーク機能を提供しますが、ノードの識別にポイント コードを使用します。M3UA 層は、発信ポイント コード（OPC）および宛先ポイント コード（DPC）を交換します。これは、IP が IP アドレスを使用してノードを識別する仕組みと似ています。

M3UA インスペクションは、限定されたプロトコル準拠を提供します。オプションで、ポイント コードまたはサービス インジケータ（SI）に基づいてアクセス ポリシーを適用できます。また、メッセージのクラスおよびタイプに基づいてレート制限を適用できます。

M3UA プロトコル準拠

M3UA インスペクションでは、次の限定されたプロトコルを強制できます。インスペクションは、要件を満たさないパケットをドロップしてログに記録します。

- 共通のメッセージヘッダー。インスペクションでは、共通ヘッダー内のすべてのフィールドを確認します。
  - バージョン 1 のみ。
  - メッセージの長さが正しく設定されている必要があります。
  - 予約済みの値を使用したメッセージ タイプのクラスは許可されません。
  - メッセージ クラス内での無効なメッセージ ID は許可されません。
- ペイロード データ メッセージ。
  - 特定のタイプの 1 つのパラメータのみが許可されます。
  - SCTP ストリーム 0 でのデータ メッセージは許可されません。

M3UA インスペクションの制限事項

M3UA インスペクションには次の制限事項があります。

- NAT は、M3UA データに埋め込まれている IP アドレスではサポートされません。
- セグメント化された M3UA メッセージは検査されず、ドロップされる可能性が高いです。
- SCTP はマルチホーミングまたはマルチストリーミングをサポートしていません。マルチホームフローをサポートする必要がある場合は、それらを許可するアクセスリストを作成する必要があります。
- ステートフル フェールオーバーは、コールフローおよびメッセージではサポートされません。コールフロー中に障害が発生すると、パケットがドロップされ、コールが切断される可能性があります。

ナビゲーション パス

[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択し、オブジェクトタイプセレクタから [マップ（Maps）] > [ポリシーマップ（Policy Maps）] > [検査（Inspect）] > [M3UA] を選択します。作業領域内を右クリックしてから [新規オブジェクト（New Object）] を選択するか、行を右クリックしてから [オブジェクトの編集（Edit Object）] を選択します。

関連項目

- マップ オブジェクトについて
- インスペクションのプロトコルおよびマップの設定 （28 ページ）
- インスペクション ポリシーのクラス マップの設定 （34 ページ）

フィールド リファレンス

表 *60 : [M3UA* マップの追加および編集（*Add and Edit M3UA Map*）*]* ダイアログボックス

要素	説明
名前	ポリシー オブジェクトの名前。最大 40 文字を使用できます。
説明	ポリシーオブジェクトの説明。最大200文字を使用できます。
[パラメータ（Parameters）] タブ	
[SS7 バリアント（SS7 Variant）]	ネットワークで M3UA インスペクションに使用する SS7 バリアントを選択します。このオプションによって、ポイントコードの有効な形式が決定します。 オプションを設定して、M3UAポリシーを導入した後は、最初にポリシーを削除しないかぎり、ポリシーを変更することはできません。 デフォルトの SS7 バリアントは ITU です。
[M3UA アプリケーション サーバープロセス（ASP）状態検証を有効にする（Enable M3UA Application Server Process (ASP) State Validation）]	アプリケーション サーバー プロセス（ASP）状態検証を実行する場合はオンにします。システムはM3UAセッションの ASP の状態を維持し、検証結果に基づいて ASP メッセージをドロップします。 ASPの厳密な状態検証を無効にすると、すべてのASPメッセージが検査されずに転送されます。
[タイムアウトの適用（Enforce Timeout）]	
エンドポイント（Endpoint）	M3UAエンドポイントの統計情報を削除するアイドルタイムアウトを入力します（hh:mm:ss形式）。タイムアウトを付けない場合は、0を指定してください。デフォルトは30分（0:30:00）です。
セッション	ASPの厳密な状態検証を有効にしている場合にM3UAセッションを削除するためのアイドルタイムアウトを入力します（hh:mm:ss 形式）。 タイムアウトを付けない場合は、0 を指定してください。デフォルト値は 30 分（0:30:00）です。このタイムアウトが無効になっている場合、システムは古いセッションを削除できません。

要素	説明
[M3UA メッセージタグの検証（M3UA Message Tag Validation）] 指定したメッセージタイプの特定フィールドの内容を確認および検証するかどうかを指定します。検証で合格しなかったメッセージはドロップされます。検証はメッセージ タイプによって異なります。検証するメッセージを選択します。	
[利用できない宛先ユーザー部（DUPU）（Destination User Part Unavailable (DUPU)）]	ユーザー/理由フィールドが存在し、有効な理由およびユーザー コードのみが含まれている必要があります。
エラー（Error）	すべての必須フィールドが存在し、許可された値のみが含まれている必要があります。各エラー メッセージには、そのエラー コードの必須フィールドが含まれている必要があります。
通知	ステータス タイプおよびステータス情報フィールドには、許可された値のみが含まれている必要があります。
[一致条件およびアクション（Match Condition and Action）] タブ [Match All] テーブルに、ポリシー マップに含まれている基準が表示されます。各行には、各基準に一致する、または一致しないトラフィックを検査で検索するかどうか、検査される基準と値、および条件を満たすトラフィックに対して実行されるアクションが示されます。 • 基準を追加するには、[Add] ボタンをクリックし、[Match Condition and Action] ダイアログボックスに入力します（M3UA ポリシーマップの [一致条件とアクションの追加または編集（Add or Edit Match Condition and Action] ダイアログボックス （145 ページ）を参照）。 • 基準を編集するには、基準を選択し、[Edit] ボタンをクリックします。 • 基準を削除するには、基準を選択し、[Delete] ボタンをクリックします。	
カテゴリ	オブジェクトに割り当てられたカテゴリ。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
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、ポリシー オブジェクトの上書きの許可および個々のデバイスのポリシー オブジェクト オーバーライドについてを参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）]ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）] フィールドには、このオブジェクトに対するオーバーライドを持つデバイスの数が表示されます。

M3UA ポリシーマップの [一致条件とアクションの追加または編集（Add or Edit Match Condition and Action] ダイアログボックス

[一致条件とアクション（Match Condition and Action）] ダイアログボックスを使用して、M3UA ポリシーマップで一致基準、値、およびアクションを直接定義します。

このダイアログボックスのフィールドは、ポリシーマップの作成中に選択した基準によって変わります。

ナビゲーション パス

M3UA ポリシーマップを作成している場合は、[Policy Object Manager] で、[M3UAマップの追加（Add M3UA Map）]/[M3UAマップの編集（Edit M3UA Map）] ダイアログボックスの [一致条件とアクション（Match Condition and Action）] タブのテーブル内を右クリックして [行の追加（Add Row）] を選択するか、行を右クリックして [行の編集（Edit Row）] を選択します。M3UA マップの設定 （141 ページ） を参照してください。

関連項目

- マップ オブジェクトについて
- インスペクションのプロトコルおよびマップの設定 （28 ページ）

フィールド リファレンス

表 *61 : M3UA* ポリシーマップの *[*一致条件とアクションの追加および編集（*Add and Edit Match Condition and Action]* ダイアログボックス

要素	説明
基準	一致する SCTP トラフィックの基準（メッセージ、DPC、OPC、またはサービスインジケータ）を指定します。
メッセージ基準	M3UA メッセージのクラスとタイプを照合します。ここでは、メッセージクラス ID の可能な値とそれに対応するメッセージ ID について詳しく説明します。これらのメッセージの詳細については、M3UA の RFC およびドキュメンテーションを参照してください。 • クラス ID 0（管理メッセージ）：メッセージ ID 0-1 • クラス ID 1（メッセージの転送）：メッセージ ID 1 • クラス ID2（SS7 シグナリングネットワーク管理メッセージ）：メッセージ ID 1-6 • クラス ID 3（ASP 状態保守メッセージ）：メッセージ ID 1-6 • クラス ID 4（ASP トラフィック メンテナンス メッセージ）：メッセージ ID 1-4 • クラス ID 9（ルーティングキー管理メッセージ）：メッセージ ID 1-4

要素	説明
DPC 基準	データメッセージ内の宛先ポイントコードを照合します。ポイントコード は zone-region-sp 形式で、各要素に使用できる値は SS7 バリアントによって異なります。
OPC 基準	データメッセージ内の発信ポイントコード、つまりトラフィックの送信元を照合します。ポイント コードは zone-region-sp 形式で、各要素に使用可能な値は SS7 バリアントによって異なります。 • ITU：ポイント コードは 14 ビットで 3-8-3 形式です。値の範囲は、[0-7]-[0-255]-[0-7] です。 • ANSI：ポイント コードは 24 ビットで 8-8-8 形式です。値の範囲は、[0-255]-[0-255]-[0-255] です。 • Japan：ポイント コードは 16 ビットで 5-4-7 形式です。値の範囲は、[0-31]-[0-15]-[0-127] です。 • China：ポイント コードは 24 ビットで 8-8-8 形式です。値の範囲は、[0-255]-[0-255]-[0-255] です。

要素	説明
サービスインジケータ基準	サービスインジケータ番号を照合します（0 ～ 15）。使用可能なサービスインジケータは、変数セクションにリストされています。これらのサービスインジケータの詳細については、M3UA の RFC およびドキュメンテーションを参照してください。 • 0：シグナリング ネットワーク管理メッセージ • 1：シグナリング ネットワーク テストおよびメンテナンス メッセージ • 2：シグナリング ネットワーク テストおよびメンテナンス特別メッセージ • 3：SCCP • 4：電話ユーザー部 • 5：ISDN ユーザー部 • 6：データ ユーザー部（コールおよび回線関連のメッセージ） • 7：データ ユーザー部（設備の登録およびキャンセル メッセージ） • 8：MTP テスト ユーザー部に予約済み • 9：ブロードバンド ISDN ユーザー部 • 10：サテライト ISDN ユーザー部 • 11：予約済み • 12：AAL タイプ 2 シグナリング • 13：ベアラー非依存コール制御 • 14：ゲートウェイ制御プロトコル • 15：予約済み
タイプ（Type）	基準に一致する、または一致しないトラフィックをマップに含めるかどうかを指定します。たとえば、文字列「example.com」で[一致しない（Doesn’t Match）]を選択した場合、「example.com」を含むトラフィックはすべてマップの対象外になります。 • [Matches]：基準に一致する。 • [一致しない（Doesn't Match）]：基準に一致しない。

要素	説明
操作	定義された基準に一致するトラフィックに対してデバイスが適用するアクション。 • [Drop Packet]：デフォルトでは、解析時に失敗したすべての無効パケットがドロップされます。 • [ドロップパケットとログ（Drop Packet and Log）]：ドロップパケットと同じですが、加えてシステムログメッセージを送信します。 • [レート制限（Rate Limit）]：メッセージのレートを制限します。このオプションは、メッセージ基準が選択されている場合に使用できます。

正規表現グループの設定

[Add Regular Expression Groups]/[Edit Regular Expression Groups] ダイアログボックスを使用して、複数の正規表現を含む正規表現グループを定義します。グループにより、モジュール形式の正規表現を作成し、さまざまな用途のためにそれらの正規表現を複数の方法でグループ化できるようになります。オブジェクトは、一部のインスペクション クラス マップとインスペクション ポリシー マップで使用できます。

ナビゲーション パス

[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択し、次にオブジェクトタイプセレクタから **[マップ（Maps）] > [正規表現グループ（Regular Expressions Groups）]** を選択します。作業領域内を右クリックしてから [新規オブジェクト（New Object）] を選択するか、行を右クリックしてから [オブジェクトの編集（Edit Object）] を選択します。

関連項目

- マップ オブジェクトについて
- インスペクションのプロトコルおよびマップの設定 （28 ページ）
- ポリシー オブジェクトの作成

フィールド リファレンス

表 62 : [Add Regular Expression Class Map]/[Edit Regular Expression Class Map] ダイアログボックス

要素	説明
名前	ポリシー オブジェクトの名前。最大 40 文字を使用できます。
説明	ポリシー オブジェクトの説明。最大 200 文字を使用できます。

要素	説明
正規表現	グループに含める正規表現を含む正規表現ポリシー オブジェクト。オブジェクトの名前を入力します。または、[選択（Select）]をクリックしてリストからオブジェクトを選択するか新しいオブジェクトを作成します。
カテゴリ	オブジェクトに割り当てられたカテゴリ。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。
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、ポリシー オブジェクトの上書きの許可および個々のデバイスのポリシー オブジェクト オーバーライドについてを参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）]ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）]フィールドには、このオブジェクトに対するオーバーライドを持つデバイスの数が表示されます。

正規表現の追加/編集

[Add Regular Expression]/[Edit Regular Expression] ダイアログボックスを使用して、クラスおよびポリシー インスペクション マップ、または正規表現グループ ポリシー オブジェクトで使用する正規表現を定義します。正規表現は、リモートアクセス SSL VPN クライアントの設定でも使用されます。

正規表現は、厳密な文字列として、またはテキスト文字列の複数のバリアントと一致するようにメタ文字を使用して、テキスト文字列を照合します。正規表現をさまざまなタイプのクラスおよびポリシー インスペクション マップで使用して、さまざまなターゲット アイテムを照合できます。たとえば、HTTP パケット内の本文テキストなど、特定のアプリケーション トラフィックのコンテンツを照合できます。

ナビゲーション パス

- **[管理（Manage）]>[ポリシーオブジェクト（Policy Objects）]** を選択し、次にオブジェクトタイプセレクタから **[マップ（Maps）]>[正規表現（Regular Expressions）]** を選択します。作業領域内を右クリックしてから [新規オブジェクト（New Object）] を選択するか、行を右クリックしてから [オブジェクトの編集（Edit Object）] を選択します。
- ASA デバイスの [SSL VPNのその他の設定（SSL VPN Other Settings）] ポリシーの [クライアント設定（Client Settings）] タブから、[AnyConnectクライアントイメージ（AnyConnect Client Image）] テーブルの [行の追加（Add Row）] ボタンをクリックするか、イメージを選択して [行の編集（Edit Row）] ボタンをクリックします。タブを開く方法の詳細については、SSL VPN AnyConnect クライアント設定の定義（ASA）を参照してください。[AnyConnect クライアントイメージの追加（Add AnyConnect Client Image）] ダイアログボッ

クスで、[選択（Select）] をクリックして [正規表現セレクタ（Regular Expressions Selector）] ダイアログボックスを開きます。新しい正規表現を追加するには、[正規表現セレクタ（Regular Expressions Selector）] ダイアログボックスの [追加]（+）（Add (+)）] ボタンをクリックします。

関連項目

- マップ オブジェクトについて
- インスペクションのプロトコルおよびマップの設定 （28 ページ）
- ポリシー オブジェクトの作成

フィールド リファレンス

表 *63 : [Add Regular Expression]/[Edit Regular Expression]* ダイアログボックス

要素	説明
名前	ポリシー オブジェクトの名前。最大 40 文字を使用できます。
説明	ポリシー オブジェクトの説明。最大 200 文字を使用できます。
値	100 文字までの長さの正規表現。正規表現の作成に使用できるメタ文字の詳細については、 正規表現の作成に使用されるメタ文字 （150 ページ）を参照してください。
カテゴリ	オブジェクトに割り当てられたカテゴリ。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。
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、ポリシー オブジェクトの上書きの許可および個々のデバイスのポリシー オブジェクト オーバーライドについてを参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）] ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）] フィールドには、このオブジェクトに対するオーバーライドを持つデバイスの数が表示されます。

正規表現の作成に使用されるメタ文字

次の表で、[Add Regular Expression]/[Edit Regular Expression] ダイアログボックス（ 正規表現の追加/編集 （149 ページ）を参照）で正規表現の構築に使用できるメタ文字について説明します。

正規表現を作成するときは、次のことに注意してください。

- テキスト文字列に、文字どおりに使用するメタ文字を入力する場合は、それらの文字の前にバックスラッシュ（\）エスケープ文字を追加します。例：「example\.com」。
- 大文字、小文字ともに一致させる場合は、大文字と小文字の両方でテキストを入力します。たとえば、「cats」は「[cC][aA][tT][sS]」と入力します。

表 *64*：正規表現の作成に使用されるメタ文字

文字	説明	注記
.	ドット	任意の単一文字と一致します。たとえば、d.g は dog、dag、dtg、doggonnit など、これらの文字が含まれているすべての単語と一致します。
(exp)	サブ表現	サブ表現は、文字を周囲の文字から分離して、サブ表現に他のメタ文字を使用できるようにします。たとえば、d(o|a)g は dog および dag と一致しますが、do や ag とは一致しません。また、サブ表現を繰り返し限定作用素とともに使用して、繰り返す文字を区別できます。たとえば、ab(xy){3}z は、abxyxyxyz に一致します。
|	代替	このメタ文字によって区切られている複数の表現のいずれかと一致します。たとえば、dog|cat は dog または cat と一致します。
?	疑問符	直前の表現が 0 または 1 個存在することを示す修飾子。たとえば、lo?se は lse または lose と一致します。
*	アスタリスク	直前の表現が 0、1、または任意の個数存在することを示す修飾子。たとえば、lo*se は lse、lose、loose などと一致します。
+	プラス	直前の表現が少なくとも 1 個存在することを示す修飾子。たとえば、lo+se は lose および loose と一致しますが、lse とは一致しません。
{x}	繰り返し限定作用素	厳密に x 回繰り返します。たとえば、ab(xy){3}z は、abxyxyxyz に一致します。
	最小繰り返し限定作用素	少なくとも x 回繰り返します。たとえば、ab(xy){2,}z は abxyxyz、abxyxyxyz などと一致します。
[abc]	文字クラス	カッコ内の任意の文字と一致します。たとえば、[abc] は a、b、または c と一致します。
[^abc]	否定文字クラス	角カッコに含まれていない単一文字と一致します。たとえば、[^abc] は、a、b、c 以外の任意の文字に一致します。[^A-Z] は、大文字以外の任意の 1 文字に一致します。

文字	説明	注記
[a-c]	文字範囲クラス	範囲内の任意の文字と一致します。[a-z] は、任意の小文字と一致します。文字と範囲を混合できます。[abcq-z] は、a、b、c、q、r、s、t、u、v、w、x、y、z と一致し、[a-cq-z] も同じです。 ダッシュ（-）文字は、角カッコ内の最後または最初の文字である場合にだけリテラルになります（[abc-] または [-abc]）。
“”	引用符	文字列の末尾または先頭のスペースを保持します。たとえば、「test」 は、一致を検索する場合に先頭のスペースを保持します。
^	キャレット	行の先頭を指定します。
\	エスケープ文字	メタ文字とともに使用すると、リテラル文字と一致します。たとえば、\[は左の角カッコと一致します。
char	文字	文字がメタ文字でない場合は、リテラル文字と一致します。
\r	復帰	復帰 0x0d と一致します。
\n	改行	改行 0x0a と一致します。
\t	タブ	タブ 0x09 と一致します。
\f	改ページ	フォーム フィード 0x0c と一致します。
\xNN	エスケープされた 16 進数	16 進数（厳密に 2 桁）を使用した ASCII 文字と一致します。
\NNN	エスケープされた 8 進数	8 進数（厳密に 3 桁）としての ASCII 文字と一致します。たとえば、文字 040 はスペースを表します。

IOS デバイスのインスペクション ルールの設定

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き PIX、FWSM、および IPS の機能をサポートしていますが、拡張機能はサポートしていません。

インスペクション ルールを設定する場合は、インスペクション設定も設定して、IOS デバイスの一部のグローバル インスペクション パラメータのデフォルト設定を変更できます。ほとんどのインスペクション設定は、Denial of Service（DoS; サービス拒絶）攻撃の防止または軽減に関連します。これらのほとんどのオプションのデフォルト設定は、ほとんどのネットワークに適しているため、1 つ以上の設定を調整する必要がある場合にだけこのポリシーを設定しま

す。設定を変更しない場合は、デバイスに設定されません（デフォルトが設定されたままになります）。

[Inspection settings] 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）デバイスを選択してから、ポリシーセレクタで **[ファイアウォール（Firewall）] > [設定（Settings）] > [インスペクション（Inspection）]** 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）] > [インスペクション（Inspection）]** 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、**[ファイアウォール設定の編集（Edit Firewall Settings）] > [インスペクション（Inspection）]** を選択します。

次の表で、使用可能なインスペクション設定について説明します。

表 *65 : [Inspection]* ページ

要素	説明
Global Timeout Values	
TCP Establish Timeout (seconds)	セッションをドロップする前に、TCPセッションが設定された状態に到達するのを待機する時間の長さ。1 ～ 2147483 の秒単位です。デフォルトは 30 です。
FIN Wait Time (seconds)	ファイアウォールがFIN交換を検出したあと、TCPセッション状態情報を保持する時間の長さ。1 ～ 2147483 の秒単位です。TCP セッションを閉じる準備が整うと、FIN 交換が発生します。デフォルトは 5 です。
TCP Idle Time (seconds)	セッションでアクティビティがない間、TCPセッションを維持する時間の長さ。1 ～ 2147483 の秒単位です。デフォルトは 3600（1 時間）です。

要素	説明
UDP Idle Time (seconds)	セッションでアクティビティがない間、UDP セッションを維持する時間の長さ。1 ～ 2147483 の秒単位です。デフォルトは 30 です。 ソフトウェアは、有効な UDP パケットを検出すると、新しい UDP セッションの状態情報を確立します。UDP はコネクションレス型サービスであるため、実際のセッションは存在しません。したがって、ソフトウェアは、パケット内の情報を調べることでセッションを見積もり、そのパケットが他の UDP パケットと似ているかどうか（類似の送信元アドレスまたは宛先アドレスを持っているなど）、および別の類似 UDP パケットの直後にそのパケットが検出されたかどうかを判断します。 ソフトウェアが、UDP アイドル タイムアウトで定義されている期間中に UDP セッションの UDP パケットを検出しなかった場合、ソフトウェアは、そのセッションの状態情報の管理を継続しません。
DNS Timeout (seconds)	アクティビティがない間、DNS lookup セッションが管理される時間の長さ。1 ～ 2147483 の秒単位です。デフォルトは 5 です。
SYN Flooding DoS Attack Thresholds	
Maximum 1 Minute Connection Rate - low Maximum 1 Minute Connection Rate - high	新しい未確立セッションの数。これにより、システムは、ハーフオープン状態のセッションの削除を開始および停止します。[Low] フィールドには、[High] フィールドに入力した数値よりも小さい数値を必ず入力してください。使用できる値は 1 分あたり 1 ～ 2147483647 です。low のデフォルトは 400 で、high のデフォルトは 500 です。
Maximum Incomplete Sessions Stop Threshold Maximum Incomplete Sessions Start Threshold	既存のハーフオープン セッションの数。これにより、ソフトウェアは、ハーフオープン状態のセッションの削除を開始および停止します。[stop] フィールドには、[start] フィールドに入力した数値よりも小さい数値を必ず入力してください。使用できる値は 1 ～ 2147483647 です。low のデフォルトは 400 で、high のデフォルトは 500 です。
Thresholds per Host	
Max Sessions Per Host	ソフトウェアがホストへのハーフオープン セッションの削除を開始する前に同時に存在できる、同じホスト宛先アドレスを持つハーフオープン TCP セッションの数。使用できる値は 1 ～ 4294967295 です。デフォルトは 50 です。 ハーフオープン セッションの数が多い場合は、ホストに対する DoS 攻撃があることを示している可能性があります。

要素	説明
Max Sessions Blocking Interval (min)	ホストごとの最大セッション数のしきい値に達した場合に、TCP ホスト固有の Denial-of-Service（DoS; サービス拒絶）攻撃の可能性を軽減するために適用するブロック時間。使用できる値は 0 ～ 35791 分です。デフォルトは 0 です。 • ブロック時間値が 0 の場合、ソフトウェアは、最大セッション制限を超えるホストへの新規接続要求のたびに、ホストの最も古い既存のハーフオープン セッションを削除する。これにより、ホストに対するハーフオープン セッション数がしきい値を超えないことが保証されます。 • ブロック時間値が 0 よりも大きい場合、ソフトウェアはホストのすべての既存のハーフオープン セッションを削除し、ホストに対するすべての新規接続要求をブロックする。ソフトウェアは、ブロック時間が経過するまですべての新規接続要求のブロックを継続します。
その他	
Session Hash Table Size (buckets)	バケットの観点で見たハッシュ テーブルのサイズ。ハッシュ テーブルに使用できる値は、1024、2048、4096、および 8192 です。デフォルトは 1024 です。 デバイスを介して実行されているセッションの合計数が現在のハッシュ サイズのほぼ 2 倍の場合は、ハッシュ テーブル サイズを大きくする必要があります。セッションの合計数が現在のハッシュ サイズの約半分に減った場合は、ハッシュテーブルサイズを小さくします。基本的には、セッション数とハッシュ テーブルのサイズ間の比率を 1:1 に維持するようにしてください。
Enable Alert Messages	ステートフル パケット インスペクションのアラート メッセージをコンソールで生成するかどうか。
Enable Audit Trail Messages	監査証跡メッセージを syslog サーバまたはルータに記録するかどうか。
Permit DHCP Passthrough (Transparent Firewall)	DHCP パケットをブリッジ経由でインスペクションなしで転送することをトランスペアレント ファイアウォールに許可するかどうか。 DHCP パススルーを許可すると、DHCP パケットの ACL がオーバーライドされるため、ACL がすべての IP パケットを拒否するように設定されている場合でも、DHCP パケットが転送されます。このため、ブリッジの一方の側のクライアントは、ブリッジの反対側の DHCP サーバから IP アドレスを取得できます。

要素	説明
Block Non-SYN Packets	確立されたセッションに属さない TCP パケットをドロップするかどうか。これらは、セッションを開始しない TCP パケットです。つまり、これらのパケットでは SYN ビットが設定されていません。
Log Dropped Packets	ドロップしたパケットのログ メッセージを作成して、ドロップの理由を指定するかどうか。

関連項目

- インスペクション ルールについて （1 ページ）
- インスペクション ルールの設定 （7 ページ）
- IOS デバイスでの Denial of Service（DoS; サービス拒絶）攻撃を防ぐためのインスペクションの使用 （6 ページ）

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。