ポリシー オブジェクトの管理

ポリシー オブジェクトを使用すると、要素の論理集合を定義できます。ポリシー オブジェクトは再利用可能な名前付きコンポーネントであり、他のオブジェクトやポリシーで使用できます。オブジェクトを使用すると、ポリシーを定義するたびにそのコンポーネントを定義する必要がなくなるため、ポリシーを定義するときに役立ちます。また、オブジェクトを使用すると、オブジェクトはオブジェクトまたはポリシーの内蔵コンポーネントになります。つまり、特定のオブジェクトの定義を変更すると、そのオブジェクトを参照しているすべてのオブジェクトおよびポリシーにこの変更が反映されます。

オブジェクトは個別に識別でき、また1箇所に集めて維持できるため、ネットワーク更新を簡単に行うことができます。たとえば、ネットワーク内のサーバを、MyServersという名前のネットワーク/ホスト オブジェクトとして識別し、これらのサーバで許可するプロトコルをサービス オブジェクトとして識別します。次に、サービス オブジェクトで定義されているサービスのトラフィックを、MyServersネットワーク/ホスト オブジェクトが送受信することを許可するアクセス ルールを作成します。これらのサーバで変更を行う場合は、ネットワーク/ホスト オブジェクトまたはサービス オブジェクトを更新して再展開するだけで済み、サーバを使用している各ルールを見つけて編集する必要がなくなります。

オブジェクトはグローバルに定義されます。つまり、オブジェクトの定義は、そのオブジェクトを参照しているすべてのオブジェクトおよびポリシーで同じになります。ただし、多くのオブジェクト タイプ（インターフェイス ロールなど）は、デバイス レベルで上書きできます。したがって、ほとんどのデバイスに対して有効なオブジェクトを作成してから、要件が若干異なる特定のデバイスの設定にあうようにオブジェクトをカスタマイズできます。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 （24 ページ）を参照してください。

この章は次のトピックで構成されています。

ポリシーのオブジェクトの選択

ドラッグアンドドロップを使用したポリシーの変更

既存のポリシーを変更する場合は、Policy Object Manager からポリシーの該当するフィールドにオブジェクトをドラッグアンドドロップすることで、ポリシー定義を簡単に更新できます。[Policy Object Manager] ウィンドウからオブジェクトの範囲を選択するには、範囲内の最初のオブジェクトを選択してから、Shift キーを押しながら範囲内の最後のオブジェクトを選択します。Ctrl キーを押しながらオブジェクトをクリックすると、複数のオブジェクトを選択できます。オブジェクトの範囲を選択してから、Ctrl キーを使用して選択範囲にオブジェクトを追加することもできます。複数のオブジェクトをドラッグするには、Ctrl キーを押しながらドラッグするか、マウスの右ボタンを使用してドラッグします。

オブジェクトセレクタを使用したポリシーの作成

ポリシーを作成するときに、多くの場合、ポリシー定義に含めるオブジェクトを 1 つ以上選択する必要があります。たとえば、ファイアウォール ポリシーでは、ネットワーク/ホスト オブジェクト、インターフェイス ロール オブジェクト、およびサービス オブジェクトが使用されます。

オブジェクトをポリシーに含めるには、オブジェクト名を手動で入力するか、[選択（Select）] ボタンをクリックしてオブジェクト セレクタ ダイアログボックスを表示します。オブジェクトセレクタは、設定しているポリシーに適用可能なオブジェクトだけを表示するように、事前にフィルタリングされている場合があります。たとえば、サブネットを必要とするポリシーを設定している場合、オブジェクト セレクタには、単一ホストを表すネットワーク/ホスト オブジェクトではなく、サブネットを表すネットワーク/ホスト オブジェクトだけが表示されます。オブジェクトセレクタにより、特定のポリシーに含めるオブジェクトを簡単に選択できます。

また、オブジェクトセレクタでは、そのタイプのオブジェクトをその場で作成および編集できます。これにより、定義中のポリシーを離れて Policy Object Manager を開かなくても、オブジェクトを簡単に操作できます。たとえば、ダイナミック NAT ルールの作成中に、必要な ACL オブジェクトが存在しないことがわかった場合、[Create] ボタンをクリックして、ACL オブジェクトを作成するためのダイアログボックスを開くことができます。オブジェクトの作成を終了すると、オブジェクト セレクタに戻ります。オブジェクト セレクタでは、新しいオブジェクトが選択され、ポリシーに含めることができるようになっています。既存のオブジェクトを変更してから使用する必要がある場合は、そのオブジェクトを選択し、[Edit] ボタンをク

リックして変更し、[OK] をクリックして変更を保存します。これにより、オブジェクト セレクタに戻ります。

セレクタからオブジェクト エディタを開いてオブジェクトを作成する場合、新しいオブジェクトは、セレクタが開かれた元のフィールドの要件に準拠している必要があります。たとえば、ホストを必要とするフィールドからセレクタを開き、そのフィールドのネットワーク/ホスト オブジェクトを作成する場合は、ネットワーク/ホスト オブジェクトをホストとして定義する必要があります。

オブジェクト セレクタには 2 つのタイプがあります。1 つのオブジェクトを選択する必要があるポリシー用の単純リスト セレクタと、特定のタイプの複数のオブジェクトを選択できるポリシー用のデュアル セレクタです。次の表に、これらのセレクタとその使用方法を示します。

表 *1:* オブジェクト セレクタ

要素	説明
タイプ	セレクタに表示するオブジェクトのタイプ（オプションがある場合）。次に例を示します。 • 一部のルールベースのポリシーで送信元および宛先を設定する場合、ネットワーク/ホスト オブジェクトまたはインターフェイス ロールを選択できます。 • 一部の ACL を設定する場合（Catalyst 6500/7600 デバイスで VLAN ACL を設定する場合など）、標準または拡張 ACL オブジェクトを選択できます。 **ヒント** 一部のポリシーでは、複数のオブジェクト タイプを選択した場合、フィールド内の別のタブに表示されます。
Available（オブジェクト タイプ）	設定しているポリシーまたはオブジェクトに関連するすべてのオブジェクトが表示されます。 インターフェイスを選択するときは、同じ名前のインターフェイスやインターフェイス ロールが存在する場合があることに注意してください。これらは名前の横に表示されるアイコンで区別できます。詳細については、ポリシー定義中のインターフェイスの指定 （100 ページ）を参照してください。 **ヒント** リスト ボックスを選択してオブジェクト名の入力を開始することによって、セレクタ内でオブジェクトを迅速に見つけることができます。
Selected（オブジェクト タイプ）	編集しているポリシーまたはオブジェクトに適用するために選択したオブジェクトが表示されます。
複数オブジェクト セレクタ ボタン	

要素	説明
[>>] ボタン [<<] ボタン	選択したオブジェクトが一方のリストから他方のリスト（示されている方向）に移動します。Ctrl を押しながらクリックすることで、複数のオブジェクトを選択できます。 ダブルクリックするか、選択して Enter を押すことによって、リスト間でオブジェクトを移動することもできます。
上下の矢印ボタン	オブジェクトタイプの数が制限される場合、順序が問題になります。セレクタに [上へ移動（Move Up）] および [下へ移動（Move Down）] ボタンがある場合は、オブジェクトを優先順に配置します。たとえば、AAA の方式リストを定義する場合、矢印を使用して、さまざまなタイプの AAA サーバ グループが使用される順序を決定します。
共通ボタン	
[Create] ボタン	このタイプのオブジェクトを作成するには、このボタンをクリックします。 **ヒント** ネットワーク/ホストオブジェクトやサービスオブジェクトなどでは、このボタンをクリックするとリストが表示され、そのリストからオブジェクトの特定のタイプを選択する必要があります。
[編集（Edit）] ボタン	選択したユーザ定義オブジェクトを編集するには、このボタンをクリックします。システム定義のオブジェクトを編集しようとした場合は、読み取り専用モードで開かれます。

関連項目

- ポリシー オブジェクトの上書きの許可 （25 ページ）
- セレクタ内の項目のフィルタリング

Policy Object Manager

Policy Object Manager は、次の目的に使用します。

- 使用可能なすべてのオブジェクトをオブジェクトタイプ別にグループ化して表示する。
- ポリシー オブジェクトを作成、コピー、編集、および削除します。
- オブジェクトを既存のポリシーにドラッグアンドドロップして、ポリシー定義を更新する。
- 使用状況レポートを生成します。このレポートでは、選択したオブジェクトが他の Security Manager オブジェクトおよびポリシーによってどのように使用されているかが示されます。

ナビゲーション パス

デバイスビューまたはポリシービューで、ツールバーの [Policy Object Manager] ボタンをクリックするか、[管理（Manage）] メニューから [ポリシーオブジェクト（Policy Objects）] を選択します（Policy Object Manager は、マップビューから開くことはできません）。

（注） Policy Object Manager を開くと、オブジェクトのドラッグアンドドロップを容易にするために、最初は現在のビューの下半分にペインとして表示されます。このペインのドッキングを解除して、Policy Object Manager を別のウィンドウにすることができます。ウィンドウを再度ドッキングすることもできます。詳細については、ポリシーオブジェクト マネージャー: ドッキング解除とドッキング （10 ページ）を参照してください。

関連項目

- ポリシー オブジェクトの作成 （13 ページ）
- ポリシーのオブジェクトの選択 （2 ページ）
- オブジェクト使用状況レポートの生成 （20 ページ）
- オブジェクト オーバーライドの管理 （23 ページ）
- テーブルのフィルタリング

フィールド リファレンス

表 *2 : [Policy Object Manager]* ウィンドウ

要素	説明
オブジェクトタイプセレクタまたはコンテンツテーブル （左側のペイン）	Security Manager で使用可能なオブジェクト タイプが一覧表示されます。オブジェクトタイプを選択すると、そのタイプの既存のすべてのオブジェクトが右側のペインの表に表示されます。 オブジェクトは、[お気に入り（Favorites）]、[最新オブジェクト（Recent Objects）]、および[すべてのオブジェクトタイプ（All Object Types）] の 3 つのフォルダに編成されます。フォルダ名の左側にある矢印をクリックして、そのフォルダを展開します。 お気に入りのオブジェクトタイプを指定できます。これらのオブジェクトタイプは別のリストに表示されるため、より簡単にアクセスできます。オブジェクトタイプをお気に入りリストに追加するには、オブジェクトを右クリックし、[お気に入りに追加（Add to Favorites）] を選択します。お気に入りリストからオブジェクトタイプを削除するには、オブジェクトを右クリックし、[お気に入りから削除（Remove from Favorites）] を選択します。 [最新オブジェクト（Recent Objects）] は、最近変更された 10 個のオブジェクトのリストです。最新オブジェクトをクリックすると、名前、タイプ、説明、最終更新日を含むオブジェクトの概要が表示されます。オブジェクトの [オブジェクトの表示（View Object）]、[オブジェクトの編集（Edit Object）]、および [使用状況の検索（ Find Usage）] ボタンにアクセスすることもできます。 [すべてのオブジェクトタイプ（All Object Types）] フォルダを展開すると、使用可能なすべてのタイプのオブジェクトが表示されます。

要素	説明
ポリシー オブジェクト テーブル（右側のペイン） 右側のペインのポリシー オブジェクト テーブルには、コンテンツ テーブルで選択されたタイプの既存のオブジェクトが表示されます。このテーブルを使用して、新しいオブジェクトを作成し、既存のオブジェクトを操作します。テーブルの下にあるボタンを使用するか、テーブル内を右クリックしてその他のコマンドを表示できます（Policy Object Manager のショートカットメニュー （11 ページ）を参照）。 アクセス コントロール リスト（ACL）オブジェクトを除き、オブジェクト タイプごとに 1 つのテーブルがあります。ACL の場合は、拡張 ACL、標準 ACL、Web ACL および統合 ACL を分けるタブがあります。該当するタブを選択して、目的のオブジェクト タイプを操作します。 テーブルのカラムは、選択するオブジェクトのタイプによって異なります。テーブルの見出しを右クリックし、[Show Columns] コマンドのカラムを選択または選択解除することによって、テーブルに表示されるカラムを変更できます。カラム見出しをクリックすることで、カラムのコンテンツによって情報をソートすることもできます。見出しをクリックして、アルファベット順のソートと逆アルファベット順のソートを切り替えます。 テーブルに表示される設定の詳細については、テーブルの下にある [Create] または [Edit] ボタンをクリックし、開かれるダイアログボックスで [Help] をクリックしてください。次のセクション「表のカラム」では、通常表示される列について説明します。	
表の上のボタン	
参照（Referenced）	オブジェクトの参照情報を表示するには、このオプションを選択します。選択すると、[参照（Referenced）]列がテーブルに追加され、オブジェクトがポリシーまたはポリシーオブジェクトによって使用されているかどうかに関する情報が表示されます。
Find Usage	使用状況の検索機能を使用して、選択したオブジェクトを使用しているポリシーまたはポリシーオブジェクト、およびオブジェクトのデバイスオーバーライドに関するレポートを表示します。詳細については、オブジェクト使用状況レポートの生成 （20 ページ）を参照してください。
View Object	テーブルで 1 つのオブジェクトが選択されている場合、このボタンをクリックすると、そのタイプのオブジェクトの [編集（Edit）] ダイアログボックスが読み取り専用モードで開き、その特定のオブジェクトの設定を表示できます。
エクスポート	エクスポート機能を使用して、選択したオブジェクトタイプのオブジェクトデータの CSV ファイルをダウンロードします。
印刷（Print）	印刷機能を使用して、選択したオブジェクトタイプのオブジェクトデータを印刷します。

要素	説明
Filter	行をフィルタリングして表示し、大きいテーブルで項目を見つけやすくします。詳細については、テーブルのフィルタリングを参照してください。
表のカラム	
*	ポリシーオブジェクトのステータスを示します。 • - ポリシーオブジェクトは編集がロックされています。ロックアイコンにカーソルを合わせると、オブジェクトをロックしているユーザとチケット/アクティビティが表示されます。 • - 現在のチケット/アクティビティでポリシーオブジェクトが変更されましたが、変更が送信されていません。 （注） ステータスアイコンにカーソルを合わせると、ポリシーオブジェクトを変更/ロックしたチケット/アクティビティの詳細を表示したり、そのチケット/アクティビティに移動したりできます。
アイコン（ラベルのないフィールド）	オブジェクトが表示される場所（ルール テーブル内など）では常に、ポリシー オブジェクト タイプに対して表示されるアイコンによって、そのタイプのオブジェクトが識別されます。アイコン内に鉛筆のイメージがある場合は、編集が可能です。
名前	ポリシー オブジェクトの名前。
Content	オブジェクト定義の概要。定義されているすべての設定が含まれていない場合があります。
許可（Permit）	ACL オブジェクトの場合、アクセス コントロール エントリ（ACE）によってトラフィックが許可されるときに、[Permit] カラムにチェックマークが表示されます。アクションが拒否の場合は、スラッシュの入った赤色の丸が表示されます。
カテゴリ	オブジェクトに割り当てられているカテゴリ オブジェクト（ある場合）。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。詳細については、カテゴリ オブジェクトの使用（18 ページ）を参照してください。

要素	説明
オーバーライド	ユーザがデバイス レベルでオブジェクトのプロパティを上書きできるかどうか。チェックマークは、オブジェクトを上書きできることを示します。すべてのオブジェクトタイプを上書きできるわけではありません。 オブジェクトがオーバーライドされている場合、[オーバーライド（Overrides）]列には、そのオブジェクトのオーバーライドの数が表示されます。数字をクリックすると、オーバーライドのリストが表示されます。 デバイスのオーバーライドの詳細については、オブジェクト オーバーライドの管理 （23 ページ）を参照してください。
参照（Referenced）	オブジェクトがポリシー定義で使用されているかどうか。使用状況の検索機能を使用して、選択したオブジェクトを使用しているポリシーまたはポリシーオブジェクト、およびオブジェクトのデバイス オーバーライドを見つけることができます（オブジェクト使用状況レポートの生成 （20 ページ）を参照）。 （注） 参照情報を表示するには、ポリシーオブジェクトテーブルの上にあるツールバーで [参照（Referenced）] オプションが選択されていることを確認します。 （注） [参照（Referenced）] 列では、すべてのアクティビティ/チケット全体にわたるコミットされたデータとコミットされていないデータの両方に基づいた使用状況がレポートされますが、[使用状況の検索（Find Usage）]機能では、コミットされたデータと現在のアクティビティ/チケットからのデータに基づいた使用状況のみがレポートされます。
説明	オブジェクトの説明。列が狭すぎて説明を表示できない場合は、アイコンをダブルクリックして説明を表示するか、アイコンの上にマウスを移動します。
[最後のチケット（Last Ticket(s)）]	チケットが有効になっている場合、オブジェクトの変更に最後に使用されたチケットのチケット ID が表示されます。をクリックできます。 チケットが有効になっている場合、オブジェクトへの最後の変更に関連付けられたチケットが表示されます。[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）。
最終更新日	オブジェクトが最後に変更された日時を示します。

要素	説明
テーブルの下のボタン	
	新しいオブジェクトを作成するには、[New Object] ボタンをクリックします。テーブルに項目を追加するすべてのボタンに、同じアイコンが使用されます。 **ヒント** ネットワーク/ホストオブジェクトやサービスオブジェクトなどでは、このボタンをクリックするとリストが表示され、そのリストからオブジェクトの特定のタイプを選択する必要があります。 このボタンをクリックすると、オブジェクトを作成するダイアログボックスが開きます。選択されたオブジェクトタイプについては、ダイアログボックス内の [Help] ボタンをクリックしてください。また、「ポリシー オブジェクトの作成 （13 ページ）」を参照してください。
	選択したオブジェクトを編集するには、[Edit Object] ボタンをクリックします。テーブル内のオブジェクトの編集には、同じアイコンが使用されます。 オブジェクトの編集に使用するダイアログボックスは、オブジェクトの作成に使用するダイアログボックスと同じです。システム定義のデフォルトオブジェクトを編集しようとすると、オブジェクトのコンテンツの表示だけが許可されます。設定については、ダイアログボックス内の [Help] ボタンをクリックしてください。詳細については、オブジェクトの編集 （17 ページ）を参照してください。
	選択したオブジェクトを削除するには、[Delete Object] ボタンをクリックします。ポリシーまたは別のポリシーオブジェクトで現在使用されていないユーザ定義のオブジェクトだけを削除できます。詳細については、オブジェクトの削除 （22 ページ）を参照してください。

ポリシーオブジェクト マネージャー: ドッキング解除とドッキング

Policy Object Manager を開くたびに、オブジェクトのドラッグアンドドロップを容易にするため、最初は現在のビューの下半分にペインとして表示されます。このペインのドッキングを解除して、Policy Object Manager を別のウィンドウにすることができます。ウィンドウを再度ドッキングすることもでき、ペインまたはウィンドウを閉じることも可能です。

- [Configuration Manager] ウィンドウの現在のビューから [Policy Object Manager] をドッキング解除するには、ペインのタイトルバーの右上隅にある [ウィンドウのドッキング解除（Undock Window）] ボタンをクリックします。

- フローティングウィンドウをもう一度 [Configuration Manager] ウィンドウのペインにするには、[Policy Object Manager] ウィンドウの右上隅にある [フレームのドッキング（Dock Frame）] ボタンをクリックします。
- ペインまたはフローティングウィンドウを閉じるには、右上隅にある [閉じる（Close）] ボタンをクリックします。

ナビゲーション パス

デバイスビューまたはポリシービューで、ツールバーの [Policy Object Manager] ボタンをクリックするか、[管理（Manage）] メニューから [ポリシーオブジェクト（Policy Objects）] を選択します（Policy Object Manager をマップビューから開くことはできません）。

Policy Object Manager のショートカットメニュー

Policy Object Manager （4 ページ）でポリシー オブジェクト テーブル内を右クリックすると、選択したオブジェクト タイプに対してさまざまな機能を実行するためのショートカット メニューが表示されます。

フィールド リファレンス

表 *3 : Policy Object Manager* のショートカットメニュー

メニュー コマンド	説明
New Object	新しいポリシーオブジェクトを作成するには、このコマンドを選択します。オブジェクトタイプ固有の情報については、開かれるダイアログボックス内の [Help] をクリックしてください。また、「ポリシー オブジェクトの作成 （13 ページ）」を参照してください。 **ヒント** ネットワーク/ホスト オブジェクトまたはサービス オブジェクトの場合、サブメニューからオブジェクト タイプを選択する必要もあります。
Edit Object	テーブルで選択したポリシーオブジェクトを編集するには、このコマンドを選択します。システム定義のデフォルト オブジェクトを選択すると、オブジェクト定義の参照専用の画面が表示されます。詳細については、オブジェクトの編集 （17 ページ）を参照してください。
Delete Object	テーブルで選択したポリシーオブジェクトを削除するには、このコマンドを選択します。ポリシーまたは別のポリシー オブジェクトで使用されていないユーザ定義のオブジェクトだけを削除できます。詳細については、オブジェクトの削除 （22 ページ）を参照してください。

メニュー コマンド	説明
デバイスのオーバーライドの有効化/無効化	Enable Device Overrides コマンドを選択して、オーバーライドが無効になっている 1 つ以上のデバイスでデバイスオーバーライドを有効にします。Disable Device Overrides コマンドを選択して、オーバーライドが有効になっている 1 つ以上のデバイスでデバイスオーバーライドを無効にします。
Edit Device Overrides	[Policy Object Overrides] ウィンドウ （28 ページ）を使用してこのオブジェクトのデバイスレベルのオーバーライドを変更するには、このコマンドを選択します。オーバーライドを作成、編集、および削除できます。詳細については、 オブジェクト オーバーライドの管理 （23 ページ）を参照してください。
Clone Object	ポリシーオブジェクトのコピーを作成するには、このコマンドを選択します。詳細については、 オブジェクトのクローニング（複製） （19 ページ）を参照してください。
Copy Object	選択した 1 つまたは複数のオブジェクトをシステムのクリップボードにコピーするには、このコマンドを選択します。 ヒント　**Ctrl+C** を使用してオブジェクトをコピーすることもできます。
Paste Object	このコマンドを選択して、システムクリップボードのオブジェクトを別のオブジェクトに貼り付けます。たとえば、ホストタイプのネットワーク/ホストオブジェクトを既存のグループタイプのネットワーク/ホストオブジェクトに追加できます。2 つのオブジェクトタイプに互換性がある必要があります。 ヒント　**Ctrl+V** を使用して、オブジェクトを貼り付けることもできます。
Find Usage	[オブジェクトの使用状況（Object Usage）] ダイアログボックスを使用して、選択したオブジェクトの使用状況レポートを生成するには、このコマンドを選択します。使用状況レポートには、オブジェクトが現在使用されている場所が示されます。詳細については、オブジェクト使用状況レポートの生成 （20 ページ）を参照してください。
View Object	オブジェクトの編集ダイアログボックスの読み取り専用バージョンを使用してオブジェクトの定義を表示するには、このコマンドを選択します。詳細については、 オブジェクトの詳細の表示 （19 ページ）を参照してください。

ポリシー オブジェクトの操作：基本手順

次の項では、ポリシーオブジェクトに対して実行できるアクションについて説明します。一部のタスクは、特定のタイプのオブジェクトに限定されます。たとえば、すべてのタイプのオブ

ジェクトを上書きできるわけではありません。定義済みオブジェクトは編集できません。また、すべてのオブジェクトをインポートまたはエクスポートできるわけではありません。

ここでは、次の内容について説明します。

ポリシー オブジェクトの作成

Security Manager には、ポリシーを定義するために使用できる、さまざまなタイプの定義済みポリシーオブジェクトがあります。また、必要に応じて独自のオブジェクトを作成できます。

次の 2 つの方法のいずれかでオブジェクトを作成できます。

- [Policy Object Manager] ウィンドウの使用。このオプションは、特定のポリシーを定義するとき以外に、1 つ以上のオブジェクトを定義する状況に最適です。 Policy Object Manager （4 ページ）を参照してください。
- オブジェクトセレクタの使用。オブジェクトを使用するポリシーを定義する際には、オブジェクトを作成および編集するためのボタンがオブジェクトセレクタに表示されるため、定義しているポリシーを離れる必要はありません。ポリシー作成中に、状況に適した特定のオブジェクトタイプが要求され、ポリシーに対して必要な設定をより意識するようになるため、多くの場合これが最適な方法です。ポリシーのオブジェクトの選択 （2 ページ）を参照してください。

ヒント 同じ定義の複数のオブジェクトを作成できるかどうかは、[Cisco Security Manager管理（Security Manager Administration）] ウィンドウ（**[ツール（Tools）] > [Cisco Security Manager管理（Security Manager Administration）]** を選択）の [ポリシーオブジェクト（Policy Objects）] ページの設定によって決まります。デフォルトでは、既存のオブジェクトの定義と同じ定義のオブジェクトを作成すると、Security Manager から警告が表示されますが、続行できます。詳細については、[Policy Objects] ページを参照してください。

関連項目

- ポリシー オブジェクトの管理 （1 ページ）
- ポリシー オブジェクトの操作：基本手順 （12 ページ）

ステップ 1 次のいずれかを実行します。

- **[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）]** を選択して、 Policy Object Manager （4 ページ）を開きます。作成するオブジェクトのタイプを目次から選択し、テーブル内を右クリックして、[新規オブジェクト（New Object）] を選択します。
- ルールの設定中に、ポリシーオブジェクトを許可または要求するフィールドの横にある [選択（Select）] を選択します。オブジェクトセレクタで、使用可能なオブジェクトリストの下にある [作成（Create）] ボタンをクリックします。

ヒント ネットワーク/ホスト オブジェクトやサービス オブジェクトなどでは、これらのボタンをクリックするとリストが表示され、そのリストからオブジェクトの特定のタイプを選択する必要があります。

選択したタイプのオブジェクトを追加するためのダイアログボックスが開きます。オブジェクトの個々のタイプの詳細については、次の項を参照してください。

- AAA サーバおよびサーバ グループ オブジェクトについて （37 ページ）
- アクセス コントロール リスト オブジェクトの作成 （70 ページ）
- [ASパスオブジェクトの追加（（Add AS Path Object））]/[ASパスオブジェクトの編集（Edit AS Path Object）] ダイアログボックス
- [ASA Group Policies] ダイアログボックス
- [BFDテンプレートの追加または編集（Add or Edit BFD Template）] ダイアログボックス
- カテゴリ オブジェクトの使用 （18 ページ）
- [コミュニティリストオブジェクトの追加または編集（Add or Edit Community List Object）] ダイアログボックス
- クレデンシャル ポリシー オブジェクトの設定
- [Add File Object]/[Edit File Object] ダイアログボックス
- FlexConfig ポリシーとポリシー オブジェクトについておよびFlexConfig ポリシー オブジェクトの作成
- アイデンティティ ユーザ グループ オブジェクトの作成
- [IKEv1 Proposal] ポリシー オブジェクトの設定
- [IKEv2 Proposal] ポリシー オブジェクトの設定
- インターフェイス ロール オブジェクトについて （95 ページ）
- IPSec IKEv1 または IKEv2 トランスフォーム セット ポリシー オブジェクトの設定

- [Add LDAP Attribute Map]/[Edit LDAP Attribute Map] ダイアログボックス （61 ページ）
- マップ オブジェクトについて （102 ページ）
- ネットワーク/ホストオブジェクトについて （105 ページ）
- [PKI Enrollment] ダイアログボックス
- [ポリシーリストオブジェクトの追加/編集（Add or Edit Policy List Object）] ダイアログボックス
- プールオブジェクトについて （121 ページ）
- [Add Port Forwarding List]/[Edit Port Forwarding List] ダイアログボックス
- ポート リスト オブジェクトの設定 （134 ページ）
- [プレフィックスリストオブジェクトの追加/編集（Add or Edit Prefix List Object）] ダイアログボックス
- リスク評価ポリシーオブジェクトの構成
- [ルートマップオブジェクトの追加または編集（Add or Edit Route Map Object）] ダイアログボックス
- セキュリティ グループ オブジェクトの作成
- Cisco Secure Desktop 設定オブジェクトの作成
- 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 （132 ページ）
- [Add Single Sign On Server]/[Edit Single Sign On Server] ダイアログボックス
- 接続を維持するためのサービス レベル契約（SLA）のモニタリング
- ASA デバイスおよび IOS デバイスの SSL VPN ブックマーク リストの設定
- SSL VPN カスタマイゼーション オブジェクトを使用した ASA ポータル表示の設定
- [Add SSL VPN Gateway]/[Edit SSL VPN Gateway] ダイアログボックス
- [Add Smart Tunnel Auto Signon List]/[Edit Smart Tunnel Auto Signon List] ダイアログボックス
- ASA デバイスの SSL VPN スマート トンネルの設定
- [Add Text Object]/[Edit Text Object] ダイアログボックス
- 時間範囲オブジェクトの設定 （93 ページ）
- トラフィック フロー オブジェクトの設定
- [Add User Group]/[Edit User Group] ダイアログボックス
- WINS/NetBIOS Name Service（NBNS）サーバの設定による SSL VPN でのファイル システム アクセスのイネーブル化

ステップ 2 オブジェクトの名前を入力し、任意でオブジェクトの説明を入力します。

オブジェクト名は、大文字と小文字が区別されず、128 文字に制限されています。オブジェクト名は、文字、数字、またはアンダースコアで始めることができます。オブジェクト名の残りの部分では、文字、数字、特殊文字、およびスペースを混在させることができます。

サポートされている特殊文字は次のとおりです。

- ハイフン（-）、
- 下線（_）、
- ピリオド（.）、および、
- プラス記号（+）。

バージョン 4.12 以降、Cisco Security Manager では、次の追加の特殊文字を使用できます。

- 感嘆符（!）、
- アットマーク（@）、
- ハッシュ記号（#）、
- パーセント記号（%）、
- アンパサンド記号（&）、および
- 括弧または丸括弧（）。

Cisco Security Manager は、次の文字をサポートしていません。

- キャレット文字（^）
- ドル文字（$）

一部のオブジェクトでは、オブジェクト名にコロン（:）を使用できますが、名前にコロンが含まれているオブジェクトは、IPS デバイスではサポートされていません。IPS デバイスを含む異なるデバイスタイプ間でオブジェクトを共有する場合は、オブジェクト名にコロン（:）を使用しないでください。

（注） 特定のオブジェクト タイプ（AAA サーバ グループ、ASA ユーザ グループ、マップ、ネットワーク/ホスト オブジェクト、サービス オブジェクト、トラフィック フローなど）には、異なる命名ガイドラインがあります。詳細については、各オブジェクト タイプの作成中にオンライン ヘルプを参照してください。

ステップ 3 オブジェクト タイプ固有の設定を行います。ダイアログボックスについては、オンライン ヘルプ ページを参照してください。

ステップ 4 （任意）[Category] の下で、[Objects] テーブルでこのオブジェクトを識別するために使用するカテゴリを選択します。カテゴリ オブジェクトの使用 （18 ページ）を参照。

ステップ 5 （任意）オブジェクトタイプにオプションがある場合は、[デバイスごとに値のオーバーライドを許可（Allow Value Override per Device）] を選択して、そのオブジェクトのプロパティを個々のデバイスで再定義できます。ポリシー オブジェクトの上書きの許可 （25 ページ）を参照してください。

ステップ 6 [OK] をクリックしてオブジェクトを保存します。

オブジェクトの編集

必要に応じて、ユーザ定義オブジェクトを編集できます。オブジェクトに対して行った変更は、そのオブジェクトを使用するすべてのポリシー（およびその他のオブジェクト）に反映されます。ただし、デバイスに対してオブジェクトのオーバーライドがすでに定義されている場合、編集はそれらのデバイスで使用されているオブジェクトに反映されません。

ヒント

- 定義済みオブジェクトは編集できませんが、コピーして新しいオブジェクトを作成できます。 オブジェクトのクローニング（複製） （19 ページ）を参照してください。
- [Edit] ダイアログボックスの一番上に、次の状況を示すメッセージが表示されます。
  - オブジェクトへの読み取り専用アクセスができます。これらのオブジェクトへの変更を保存できません。
  - ポリシーまたはデバイスのインポートで説明する手順を使用して、ポリシー オブジェクトがインポートされました。インポートされたオブジェクトを使用する共有ポリシーが異なるサーバで管理されている場合、そのオブジェクトは今後、再度インポートされる可能性があります。ポリシー オブジェクトに加えた変更は、ポリシー オブジェクトが再度インポートされた場合には削除されます。オブジェクトを編集する前に、ポリシー管理およびインポート用に組織で使用されているプロトコルを確実に理解してください。**[ツール（Tools）] > [Security Manager管理（Security Manager Administration）] > [ポリシー管理（Policy Management）]** ページのオプションを使用して、このメッセージを表示するかどうかを制御できます（[Policy Management] ページを参照）。
- このオブジェクトタイプを使用するポリシーまたはオブジェクトを定義するときに、オブジェクトを編集することもできます。詳細については、ポリシーのオブジェクトの選択（2 ページ）を参照してください。

はじめる前に

オブジェクトが使用されているかどうか、および変更の影響を受けるポリシー、オブジェクト、デバイスを判別します。このために使用状況レポートを生成できます。 オブジェクト使用状況レポートの生成 （20 ページ） を参照してください。

関連項目

- ポリシー オブジェクトの作成 （13 ページ）

ステップ 1 **[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）]** を選択して、 Policy Object Manager （4 ページ）を開きます。

ステップ 2 コンテンツ テーブルからオブジェクト タイプを選択します。

ステップ 3 編集するオブジェクトを右クリックし、[オブジェクトの編集（Edit Object）] を選択します。

ステップ 4 必要に応じて、そのオブジェクトタイプの [編集（Edit）] ダイアログボックスでフィールドを変更し、[OK] をクリックして変更を保存します。オブジェクト タイプ固有の情報については、[Help] ボタンをクリックしてください。

カテゴリ オブジェクトの使用

カテゴリは、オブジェクトに関する中間レベルの詳細を示します。カテゴリをオブジェクトに割り当てることによって、カテゴリの名前および色を確認して、ルールテーブル内のルールおよびオブジェクトを簡単に識別できます。ルールを作成するときに、ルールまたはオブジェクトにカテゴリを割り当てることができます。または、カテゴリ情報が含まれるようにルールまたはオブジェクトをあとで編集できます。カテゴリ割り当てに対してデバイス コンフィギュレーション コマンドは生成されません。

ポリシー オブジェクトにカテゴリを割り当てることの利点は、次のとおりです。

- 分類されたオブジェクトを使用してルールテーブルを表示すると、可視性が向上します。
- カテゴリに基づいてルールテーブル内でオブジェクトをフィルタリングでき、ルールを保守しやすくなります。

たとえば、ネットワーク/ホスト オブジェクトを作成し、管理のためにその使用を追跡する場合があります。このネットワーク/ホスト オブジェクトを定義するときに、カテゴリに関連付けます。アクセス ルール テーブルを表示すると、このネットワーク/ホスト オブジェクトを使用しているルールを簡単に識別できます。テーブルをフィルタリングして、カテゴリに関連付けられている項目だけを表示することもできます。

Security Manager には、定義済みのカテゴリのセットがあります。色は変更できませんが、名前および説明を変更できます。次の手順では、名前および説明を変更する方法について説明します。

ステップ 1 **[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）]** を選択して [Policy Object Manager] を開きます（Policy Object Manager （4 ページ）を参照）。

ステップ 2 オブジェクトタイプセレクタから [カテゴリ（Categories）] を選択します。

ステップ 3 [オブジェクトの編集（Edit Object）] をクリックして、[カテゴリエディタ（Category Editor）] ダイアログボックスを開きます。

ステップ 4 必要に応じて、定義済みのカテゴリ オブジェクトの名前および説明を変更します。

- [Label]：カテゴリに関連付けられている色。
- [Name]：カテゴリ名。名前は最大 128 文字で、特殊文字とスペースを使用できます。
- [Description]：オブジェクトに関する追加情報（最大 1024 文字）。

ステップ 5 [OK] をクリックして変更を保存します。

オブジェクトのクローニング（複製）

ポリシーオブジェクトを最初から作成する代わりに、既存のオブジェクトのクローン作成または複製ができます。新しいオブジェクトには、コピー元のオブジェクトの属性がすべて含まれます。必要に応じて、名前およびすべての属性を変更できます。

クローニングは、編集できない定義済みオブジェクトに基づいたオブジェクトの作成に役立ちます。

関連項目

- ポリシー オブジェクトの操作：基本手順 （12 ページ）

ステップ 1 **[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）]** を選択して、 Policy Object Manager （4 ページ）を開きます。

ステップ 2 コンテンツ テーブルからオブジェクト タイプを選択します。

ステップ 3 複製するオブジェクトを右クリックし、[オブジェクトの複製（Clone Object）] を選択します。

そのオブジェクトタイプのダイアログボックスが表示されます。[名前（Name）]フィールドには、新しいオブジェクトのデフォルト名（Copy of コピー元オブジェクトの名前）が入ります。残りのフィールドには、コピー元オブジェクトと同じ値が入ります。

ステップ 4 必要に応じて、新しいオブジェクトの名前およびその設定を変更します。そのオブジェクト タイプ固有の情報については、[Help] ボタンをクリックしてください。

ステップ 5 [OK] をクリックして変更を保存します。

オブジェクトの詳細の表示

オブジェクトが別のアクティビティによってロックされている場合でも、オブジェクトのコンテンツを読み取り専用モードで表示できます。これは、[Policy Object Manager] ウィンドウでは定義を完全には表示できない複雑なオブジェクトの設定の詳細を完全に表示する必要がある場合、またはユーザ権限によってオブジェクト情報の表示だけが許可されている場合に役立ちます。

関連項目

- ポリシー オブジェクトの操作：基本手順 （12 ページ）

ステップ 1 [管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択して、 Policy Object Manager （4 ページ）を開きます。

ステップ 2 コンテンツ テーブルからオブジェクト タイプを選択します。

ステップ 3 オブジェクトを右クリックし、[オブジェクトの表示（View Object）] を選択します。

そのオブジェクトのダイアログボックスが読み取り専用モードで表示されます。

オブジェクト使用状況レポートの生成

ポリシーオブジェクトを変更する前に、そのオブジェクトが使用されているかどうかを判別する必要があります。これを行うには、[Policy Object Manager] ウィンドウの [参照（Referenced）] 列を表示します。ポリシーオブジェクトテーブルの上にある [参照（Referenced）] ボタンを選択して [参照（Referenced）] 列を有効にします。

参照されているオブジェクトについて、選択したオブジェクトが使用されているために、そのオブジェクトに対する変更の影響を受けるポリシー、オブジェクト、VPN、およびデバイスを示す使用状況レポートを生成できます。使用状況レポートには、現在のアクティビティで選択したオブジェクトへの参照、およびデータベースにコミットされたデータで見つかった参照が含まれています。

（注） [参照（Referenced）] 列では、すべてのアクティビティ/チケット全体にわたるコミットされたデータとコミットされていないデータの両方に基づいた使用状況がレポートされますが、[使用状況の検索（Find Usage）] 機能では、コミットされたデータと現在のアクティビティ/チケットからのデータに基づいた使用状況のみがレポートされます。

次の方式のいずれかを使用して、使用状況レポートを生成できます。

- Policy Object Manager：[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択して、Policy Object Manager （4 ページ）を開きます。オブジェクトのタイプを目次から選択し、オブジェクトを右クリックして、[使用状況の検索（Find Usage）] を選択します。
- ファイアウォール ルール ポリシー：ファイアウォール ルール テーブルでオブジェクトをクリックし、右クリックして、[使用状況の検索（Find Usage）] を選択します。

使用状況情報が [Object Usage] ダイアログボックスに表示されます。テーブルの上にある適切な使用状況タイプを選択して、選択したオブジェクトを使用するデバイス、ポリシー、VPN、またはその他のオブジェクトを表示します。

特定のポリシー：

次の表に、ダイアログボックスのフィールドを示します。

表 *4 : [Object Usage]* ダイアログボックス

要素	説明
名前 タイプ 説明	使用状況を検索しているオブジェクトに関する一般情報は、[オブジェクトの使用状況（Object Usage）] ダイアログボックスの上部に表示されます。
デバイス ポリシー オブジェクト VPN	表示する参照のタイプ。たとえば、[オブジェクト（Objects）] を選択すると、他のオブジェクトからのオブジェクトの参照だけを表示できます。
使用者	選択したオブジェクトを参照しているデバイス、ポリシー、VPN、またはオブジェクトの名前。
タイプ（Type）	選択したオブジェクトを参照している項目のタイプ。これは、デバイス、ポリシー、VPN、または別のオブジェクトです。
使用方法（Usage）	オブジェクトがどのように参照されているかが示されます。たとえば、選択したオブジェクトがデバイスによって参照されている場合、このカラムには、オブジェクトを参照しているのはデバイスに割り当てられたポリシーであることが示されます。
プロキシミティ（Proximity）	選択したオブジェクトとそれを使用している項目との関係が示されます。次に例を示します。 • 定義内にネットワーク/ホストオブジェクトが含まれているポリシーは、そのオブジェクトと直接的な関係を持ち、オブジェクトに含まれる他のネットワーク/ホストオブジェクトと間接的な関係を持ちます。 • このポリシーが割り当てられているデバイスは、ネットワーク/ホストオブジェクトを直接的に参照し、オブジェクトに含まれる他のネットワーク/ホストオブジェクトを間接的に参照します。

要素	説明
詳細パネル	特定のタイプの参照に関する追加の詳細情報が表示されます。 • [デバイス（Devices）]：サポートされているポリシータイプの場合、デバイス情報が [詳細（Details）] パネルに表示されます。 • [ポリシー（Policies）]：次のサポートされているポリシータイプの場合、オブジェクトを参照する実際のルールが [詳細（Details）] パネルに表示されます。 • AAA ルール • アクセル ルール • IPv6 アクセスルール • インスペクション ルール • 変換ルール • Web フィルタルール（PIX/FWSM/ASA） • ゾーンベースのファイアウォールルール [詳細（Details）] パネルから、ルールへの移動、ルールデータのエクスポート、またはルールデータの印刷を行うことができます。 • [オブジェクト（Objects）]：指定したオブジェクトを参照している他のオブジェクトの詳細情報が [詳細（Details）] パネルに表示されます。[オブジェクトの使用状況（Object Usage）] ダイアログボックスの [詳細（Details）] パネルから、詳細情報のエクスポート、情報の印刷、読み取り専用モードでのオブジェクトの表示、オブジェクトの編集、またはオブジェクトの使用状況の検索を行うことができます。

オブジェクトの削除

ユーザ定義のオブジェクトは、ポリシーまたは他のオブジェクトで使用されていない場合にだけ削除できます。定義済みのオブジェクトは削除できません。デバイスレベルのオーバーライドが定義されているオブジェクトを削除すると、オーバーライドもすべて削除されます。

ヒント　使用されていないオブジェクトをデータベースから削除できない場合があります。たとえば、オブジェクトを使用していたローカル ポリシーを、オブジェクトを使用しない共有ポリシーと置き換える場合などです。オブジェクトの削除が失敗する場合は、保留中の変更をすべて送信または廃棄してから（Workflow モードで、保留中のアクティビティをすべて送信または廃棄）、オブジェクトの削除を再試行します。または、データベース内の使用されていないオブジェクトはポリシーに影響しないため、そのままにしておくことができます。

はじめる前に

オブジェクトが現在使用されているかどうか、および削除の影響を受けるポリシー、オブジェクト、デバイスを判別します。オブジェクトを削除する前に、オブジェクトへの参照をすべて削除する必要があります。このために使用状況レポートを生成できます。オブジェクト使用状況レポートの生成　（20 ページ）を参照してください。

ステップ 1　**[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）]** を選択して、Policy Object Manager　（4 ページ）を開きます。

ステップ 2　コンテンツ テーブルからオブジェクト タイプを選択します。

ステップ 3　削除するオブジェクトを右クリックして [オブジェクトの削除（Delete Object）] を選択するか、オブジェクトを選択して [オブジェクトの削除（Delete Object）] ボタンをクリックします。削除の確認が求められます。

オブジェクト オーバーライドの管理

ポリシー オブジェクトを作成するときに、オブジェクトの上書きを許可できます。これにより、一般的なポリシーの作成を可能にする汎用オブジェクトを作成できるようになります。個々のデバイスで、ポリシー オブジェクト定義を上書きして、ポリシーがデバイスに適切に適用されるようにします。

Policy Object Manager　（4 ページ）から、上書き可能なポリシー オブジェクトを選択し、そのグローバル オブジェクトに対して定義するデバイス レベルのオーバーライド テーブルを生成できます。オブジェクトを右クリックし、[デバイスのオーバーライドの編集（Edit Device Overrides）] を選択してテーブルを生成します（[Policy Object Overrides] ウィンドウ　（28 ページ）を参照）。

デバイス レベルのオーバーライドは、次の 2 つの場所で作成できます。

- 選択したデバイスの [Device Properties] ウィンドウ。選択したデバイスだけのオーバーライドを作成および管理できます。詳細については、単一デバイスのオブジェクト オーバーライドの作成または編集　（26 ページ）を参照してください。

- [Policy Object Manager] ウィンドウ。複数のデバイスのオーバーライドを一度に作成および管理できます。詳細については、複数デバイスのオブジェクト オーバーライドの一括での作成または編集 （27 ページ）を参照してください。

ヒント　デバイス レベルでオブジェクト定義を上書きすると、あとからグローバル レベルでポリシー定義を変更しても、オブジェクトが上書きされたデバイスには影響しません。

次の項では、ポリシー オブジェクト オーバーライドについてより詳細に説明します。

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

多くのタイプのポリシーオブジェクトでは、特定のデバイスについてオブジェクトの上書きを許可できます。そのため、ほとんどのデバイスに定義を適用できるオブジェクトを作成し、若干異なる定義を必要とする少数のデバイスについてオブジェクトを変更することが可能です。または、上書きが必要なオブジェクトをすべてのデバイスに対して作成することもできます。これにより、すべてのデバイスに対してポリシーを1つ作成できます。オブジェクト オーバーライドでは、デバイス全体で使用する共有ポリシーの小さなセットを作成し、個々のデバイスに対して必要に応じてポリシーを変更することが可能です。

たとえば、社内のさまざまな部門へのICMPトラフィックを拒否する場合があります。それぞれの部門は、異なるネットワークに接続されています。これを実行するには、Departmental Networkという名前のネットワーク/ホスト オブジェクトを含むルールを使用して、アクセス ルール ファイアウォール ポリシーを定義します。このオブジェクトのデバイス オーバーライドを許可することによって、関連する各デバイスで、デバイスが接続されている実際のネットワークを指定するオーバーライドを作成できます。

デバイスレベルのオブジェクトオーバーライドは、VPNポリシーの定義にグローバルオブジェクトが含まれている場合に特に重要です。VPN ポリシーは VPN トポロジ内のすべてのデバイスに適用されます。たとえば、サイト間 VPN で PKI ポリシーを定義するときに、PKI 登録オブジェクトを選択します。VPNのハブでスポークとは異なるCAサーバが使用されている場合は、デバイスレベルのオーバーライドを使用して、ハブで使用されているCAサーバを指定する必要があります。PKI ポリシーは 1 つの PKI 登録オブジェクトを参照しますが、このオブジェクトによって表される実際のCAサーバは、定義するデバイスレベルのオーバーライドに基づいて、ハブごとに異なります。

オブジェクトがオーバーライド可能かどうかは、 Policy Object Manager （4 ページ）のオブジェクトテーブルの [オーバーライド（Overridable）] 列ですぐに確認できます。緑色のチェックマークは、オブジェクトに対してオーバーライドを作成できることを示します。カラムが存在することは、オブジェクト タイプでオーバーライドが許可されていることを示します。

関連項目

- ポリシー オブジェクトの上書きの許可 （25 ページ）
- 単一デバイスのオブジェクト オーバーライドの作成または編集 （26 ページ）
- 複数デバイスのオブジェクト オーバーライドの一括での作成または編集 （27 ページ）
- デバイス レベルのオブジェクト オーバーライドの削除 （29 ページ）

ポリシー オブジェクトの上書きの許可

オブジェクトのオーバーライドを作成するには、オブジェクトでオーバーライドが許可されている必要があります。すべてのオブジェクト タイプでオーバーライドが許可されているわけではありません。

オーバーライドを許可する場合、オブジェクトを定義するときに [デバイスごとに値のオーバーライドを許可（Allow Value Override per Device）] を選択し、オーバーライド許可としてオブジェクトを定義します。このオプションを選択したあと、オーバーライドを定義する前に、[OK] をクリックしてオブジェクトを保存する必要があります。オブジェクトの作成の詳細については、 ポリシー オブジェクトの作成 （13 ページ）を参照してください。

インベントリに追加するデバイスでポリシーを検出するときに、既存のオブジェクトに対してデバイス レベルのオーバーライドを作成するように Security Manager を設定することもできます。検出中に、検出されたポリシーに既存のオブジェクトが該当するが、完全には適合しないと Security Manager が判断した場合、オブジェクトは使用されますが、差異を表すためにデバイス レベルのオーバーライドが作成されます。たとえば、Security Manager で、ACL ポリシー オブジェクトと同じ名前の ACL を持つデバイスでポリシー検出を実行すると、検出されたポリシー オブジェクトの名前が再利用されますが、オブジェクトに対してデバイス レベルのオーバーライドが作成されます。検出中にデバイス レベルのオーバーライドを許可しない場合、名前に番号が付加されて新しいポリシー オブジェクトが作成されます。これがデフォルトです。

検出中にデバイスのオーバーライドを許可するように Security Manager を設定するには、[ツール（Tools）] > [Security Manager管理（Security Manager Administration）] > [検出（Discovery）] を選択し、[検出されたポリシーオブジェクトに対するデバイスのオーバーライドを許可（Allow Device Override for Discovered Policy Objects）] を選択します。

（注） 検出中に特定のポリシーオブジェクトがデバイス レベルのオーバーライドに再利用されるようにするには、ポリシー検出の前に、Policy Object Manager で、該当するポリシーオブジェクトに対して [デバイスごとに値のオーバーライドを許可（Allow Value Override per Device）] 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。

関連項目

- 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 （24 ページ）
- 単一デバイスのオブジェクト オーバーライドの作成または編集 （26 ページ）
- 複数デバイスのオブジェクト オーバーライドの一括での作成または編集 （27 ページ）
- デバイスレベルのオブジェクト オーバーライドの削除 （29 ページ）

単一デバイスのオブジェクト オーバーライドの作成または編集

[Device Properties] ウィンドウから、デバイスレベルのオブジェクト オーバーライドを作成または編集できます。

オーバーライドによって、選択したデバイスだけに影響するグローバル オブジェクトの定義が指定されます。たとえば、あるデバイスについて、他のデバイスとは異なる AAA サーバ グループを表すように、AAA サーバ グループ オブジェクトの定義を上書きできます。

関連項目

- ポリシー オブジェクトの上書きの許可 （25 ページ）
- 複数デバイスのオブジェクト オーバーライドの一括での作成または編集 （27 ページ）
- 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 （24 ページ）
- デバイスレベルのオブジェクト オーバーライドの削除 （29 ページ）

ステップ 1 （デバイスビュー）デバイスセレクタでデバイスを右クリックして、[デバイスのプロパティ（Device Properties）] を選択します。

ステップ 2 上書きするオブジェクトタイプを [ポリシーオブジェクトの上書き（Policy Object Overrides）] フォルダから選択します。

デバイス レベルで上書き可能な、選択したタイプのすべてのオブジェクトがテーブルに表示されます。オブジェクトにデバイスに対するオーバーライドがすでに定義されている場合、[値がオーバーライドされているか（Value Overridden?）] カラムにチェックマークが付けられます。

ステップ 3 オーバーライドを変更するオブジェクトを選択し、次のいずれかを実行します。

- [オーバーライドの作成（Create Override）] ボタンをクリックするか、右クリックして [オーバーライドの作成（Create Override）] を選択します。
- [オーバーライドの編集（Edit Override）] ボタンをクリックするか、右クリックして [オーバーライドの編集（Edit Override）] を選択します。

そのタイプのオブジェクトを定義するためのダイアログボックスが表示され、現在のプロパティ（グローバル プロパティまたはローカル オーバーライド）が示されます。

ステップ 4 オブジェクトの定義を変更し、[OK] をクリックして、デバイスレベルのオーバーライドを保存します。[Device Properties] ウィンドウで、[Value Overridden?] カラムに緑色のチェック マークが表示されます。

複数デバイスのオブジェクト オーバーライドの一括での作成または編集

[Policy Object Manager] ウィンドウから、デバイスレベルのオブジェクト オーバーライドを作成または編集できます。

この方式では、複数のデバイスに対してオブジェクト オーバーライドを同時に作成できます。同じ VPN トポロジに参加している複数のデバイスのオーバーライドを作成するときに特に役立ちます。たとえば、VPN のある部分に配置されたスポークが、VPN の別の部分に配置されたスポークとは異なる CA サーバを使用する場合、これらのデバイスのサーバを定義する PKI 登録オブジェクトを上書きできます。これは、デバイス ビューから各デバイスを個別に選択し、[Device Properties] ウィンドウでオーバーライドを定義するよりも便利な方式です。

関連項目

- 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 （24 ページ）
- ポリシー オブジェクトの上書きの許可 （25 ページ）
- 単一デバイスのオブジェクト オーバーライドの作成または編集 （26 ページ）
- デバイスレベルのオブジェクト オーバーライドの削除 （29 ページ）

ステップ 1 **[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）]** を選択して、 Policy Object Manager （4 ページ）を開きます。

ステップ 2 上書きするオブジェクト タイプをコンテンツ テーブルから選択し、上書きするオブジェクトを選択します。

ヒント すべてのオブジェクト タイプでオーバーライドが許可されているわけではなく、すべてのオブジェクトが上書き可能として定義されているわけではありません。[Overridable] カラムの緑色のチェックマークを確認してください。オブジェクト タイプでオーバーライドが許可されているが、このオブジェクトにチェックマークがない場合は、オブジェクトのオーバーライドを許可するようにオブジェクトを編集します（ポリシー オブジェクトの上書きの許可 （25 ページ）を参照）。

ステップ 3 チェックマークをダブルクリックするか、オブジェクトを右クリックして[デバイスオーバーライドの編集（Edit Device Overrides）] を選択し、 [Policy Object Overrides] ウィンドウ （28 ページ）を開きます。このウィンドウには、オブジェクトに対してオーバーライドが定義されている各デバイスを一覧表示するテーブルがあります。

ヒント オーバーライド可能なオブジェクトを編集し、[オーバーライド（Overrides）] フィールドの横の [編集（Edit）] をクリックすることもできます。

ステップ 4 次のいずれかを実行します。

- オーバーライドを追加するには、[オーバーライドの作成（Create Override）] ボタンをクリックし、オーバーライドを適用するデバイスを選択して、オーバーライドを定義します。

オーバーライドを作成および編集するためのダイアログボックスは、オブジェクトの作成に使用されるものと同じです。[Help] ボタンをクリックすると、オブジェクトのタイプに関する情報が表示されます。

作成したオーバーライドは、オブジェクトを使用するデバイス上のすべてのポリシーに適用されます。あるポリシーについてオブジェクトをオーバーライドし、別のポリシーについてはオーバーライドしない、という処理は不可能です。

- オーバーライドを編集するには、オーバーライドを選択し、[オーバーライドの編集（Edit Override）] ボタンをクリックします。

[Policy Object Overrides] ウィンドウ

[Policy Object Overrides] ウィンドウを使用して、選択したオブジェクトに対して定義されているすべてのデバイスレベルのオーバーライドのリストを表示します。テーブルに表示されるコンテンツはオブジェクトのタイプによって異なりますが、デバイス名、デバイスの説明、およびカテゴリは常に含まれます。オーバーライドなどのオブジェクトのコンテンツが表示される場合もあります。

- オーバーライドを追加するには、[オーバーライドの作成（Create Override）] ボタンをクリックします。[デバイスのオーバーライドの作成（Create Overrides for Device）] ウィンドウで、使用可能リストからデバイスを選択し、[>>] をクリックして選択済みリストに移動します。[OK] をクリックすると、オーバーライドを定義するためのダイアログボックスが表示されます。オーバーライドは新しく選択したすべてのデバイスに適用されます（グレーになっているデバイスのオーバーライドは変更されません）。

（注） 使用可能なデバイスのリストには、オブジェクトに対してオーバーライドがまだ定義されていないデバイスが表示されます。オーバーライドを持つデバイスは、選択済みのデバイスのリストにグレーで表示されます。

オーバーライドを作成および編集するためのダイアログボックスは、オブジェクトの作成に使用されるものと同じです。[Help] ボタンをクリックすると、オブジェクトのタイプに関する情報が表示されます。

作成したオーバーライドは、オブジェクトを使用するデバイス上のすべてのポリシーに適用されます。あるポリシーについてオブジェクトをオーバーライドし、別のポリシーについてはオーバーライドしない、という処理は不可能です。

- オーバーライドを編集するには、オーバーライドを選択し、[オーバーライドの編集（Edit Override）] ボタンをクリックします。
- オーバーライドを削除するには、オーバーライドを選択し、[オーバーライドの削除（Delete Override）] ボタンをクリックします。

オーバーライドの削除によって、オブジェクトの削除またはデバイス割り当てからのオブジェクトの削除は行われません。オーバーライドを削除すると、オブジェクトを使用するデバイスのポリシーでは、オブジェクトのグローバル定義の使用が開始されます。これにより、ポリシーの意味が変わります。

ヒント　選択したデバイスの [Device Properties] ウィンドウから、デバイスレベルのオーバーライドを作成および編集することもできます。[Device Properties] ウィンドウを使用すると、単一デバイスによって使用されているすべてのオブジェクトのオーバーライドの管理が簡単になります。詳細については、単一デバイスのオブジェクト オーバーライドの作成または編集　（26 ページ）を参照してください。

ナビゲーション パス

Policy Object Manager　（4 ページ） を開きます。上書き可能なオブジェクトタイプ（オブジェクトページに[オーバーライド（Overrides）]というカラムがある）を選択し、次のいずれかを実行します。

- [オーバーライド（Overrides）] カラムの緑色のチェックマークをダブルクリックします。
- オブジェクトを右クリックし、[デバイスのオーバーライドの編集（Edit Device Overrides）] を選択します。
- 上書き可能なオブジェクトを編集し、[オーバーライド（Overrides）] フィールドの横の [編集（Edit）] をクリックします。

関連項目

- 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　（24 ページ）
- ポリシー オブジェクトの上書きの許可　（25 ページ）
- 複数デバイスのオブジェクト オーバーライドの一括での作成または編集　（27 ページ）
- デバイスレベルのオブジェクト オーバーライドの削除　（29 ページ）
- テーブルのフィルタリング
- セレクタ内の項目のフィルタリング

デバイスレベルのオブジェクト オーバーライドの削除

デバイスレベルのオブジェクト オーバーライドを削除すると、オブジェクトのグローバル定義が、選択したデバイスに復元されます。オーバーライドは、[Device Properties] ウィンドウまたは [Policy Object Manager] ウィンドウから削除できます。

- デバイスビューからのオーバーライドの削除：デバイスを右クリックし、[デバイスプロパティ（Device Properties）] を選択し、[ポリシーオブジェクトオーバーライド（Policy

Object Overrides）] フォルダからオブジェクトタイプを選択します。削除するオーバーライドを選択し、[オーバーライドの削除（Delete Override）] をクリックします。

- Policy Object Manager からのオーバーライドの削除：コンテンツテーブルからオブジェクトタイプを選択し、オブジェクトを右クリックして [デバイスのオーバーライドの編集（Edit Device Overrides）] を選択します。削除するオーバーライドを選択し、[オーバーライドの削除（Delete Override）] をクリックします。

関連項目

- 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 （24 ページ）
- ポリシー オブジェクトの上書きの許可 （25 ページ）
- ポリシー オブジェクト オーバーライドのページ
- [Policy Object Overrides] ウィンドウ （28 ページ）

Cisco Security Manager のオーバーライド可能なオブジェクト

Security Manager では、次のオブジェクトをオーバーライドできます。

- **VPN オブジェクト**
  - AAA サーバーグループ
  - PKI 登録 （CA サーバー）
  - WINS Server List
  - SSL VPN カスタマイゼーション
  - SAML ID プロバイダー
  - Web ACL
  - Port Forwarding List
  - ブックマーク
  - スマートトンネルリスト
  - スマート トンネル ネットワーク リスト
  - スマートトンネル自動サインオンリスト
  - シングルサインオンサーバー
  - 参照 ID
- **ファイアウォールオブジェクト**
  - アイデンティティ ユーザー グループ
  - Networks/Hosts

- Port Lists
- セキュリティ グループ（Security Group）
- サービス
- アクセスコントロールリスト（拡張、標準、Web、統合）
- AS パス
- BFD テンプレート（BFD Template）
- コミュニティ リスト（Community List）
- 資格情報
- アイデンティティポリシー（IOS）
- アイデンティティ ユーザー グループ
- Interface Roles
- LDAP 属性マップ
- LDAP 属性マップ（IOS）
- ポリシー リスト
- プレフィックス リスト
- プレフィックスリスト IPV6
- Risk Rating
- ルート マップ
- セキュリティ グループ（Security Group）
- テキスト オブジェクト
- TLS プロキシ
- プールオブジェクト（DHCP V6、IPV4 プール、IPV6 プール、MAC アドレスプール、NET プール）
- マップ（AVP、正規表現グループ、正規表現、TCP マップ）
- クラスマップ：検査（AOL、DCE/RPC、DIAMETER、DNS、eDonkey、FastTrack、FTP、GunTella、H.323（ASA/PIX/FWSM）、H.323（IOS）、HTTP（ASA/PIX/FWSM）、HTTP（IOS）、ICQ、IM、IMAP、Kazaa2、MSN メッセンジャー、POP3、Scansafe、SIP（ASA/PIX/FWSM）、SIP（IOS）、SMTP、SUN RPC、Windows Messenger、Yahoo Messenger）
- クラスマップ：Web フィルタ（ローカル、N2H2、トレンド、Websense）
- パラメータマップ：検査（検査パラメータ、プロトコル情報パラメータ）

- パラメータマップ：Web フィルタ（Loal、N2H2、傾向、URL フィルタ、URLF Glob パラメータ、Websense）
- ポリシーマップ：検査（DCE/RPC、DIAMETER、DNS、ESMTP、FTP、GTP、H.323（ASA/PIX/FWSM）、H.323（IOS）、HTTP ASA7.1.x/PIX7.1.x/ FWSM3.x/IOS）、HTTP（ASA7.2 以降/PIX7.2 以降）、HTTP（ゾーンベースの IOS）、IM（ASA7.2 以降/PIX7.2 以降）、IM（IOS）、IM（ゾーンベースのIOS）、IMAP、IP オプション、IPSec パススルー、IPV6、LISP、M3UA、NetBIOS、P2P、POP3、Scansafe、Sctp、SIP（ASA/PIX/FWSM）、SIP（IOS）、Skinny、SMTP、SNMP、SUN RPC）
- ポリシーマップ：Web フィルタ（Web フィルタ）

ポリシー オブジェクトのインポートおよびエクスポート

Security Manager には Perl スクリプトが含まれており、このスクリプトを使用して、ネットワーク/ホスト オブジェクト、サービス オブジェクト、およびポート リスト ポリシー オブジェクトを別の Security Manager サーバにインポートできるように、エクスポートできます。この情報には、ポリシー オブジェクトのデバイス レベルのオーバーライドが含まれています。

（注） コマンドは、IPv4 アドレスのみを含むネットワーク/ホスト オブジェクトで機能します。コマンドを使用して、ネットワーク/ホスト IPv6 オブジェクトをインポートすることはできません。

インポート可能な CSV ファイルを手動で作成することもできます。たとえば、ネットワークへのエントリを拒否するネットワークまたはホストを識別する IP アドレスのリストを取得できます。Policy Object Manager でオブジェクトを手動で作成するよりも簡単な場合は、リストを 1 つ以上のネットワーク/ホスト オブジェクトとしてバルクロードする CSV ファイルを作成できます。

ヒント このコマンドを使用する以外に、他の機能を使用して、共有ポリシーに割り当てられたポリシー オブジェクトまたはローカル デバイス ポリシーで設定されたポリシー オブジェクトをエクスポートおよびインポートできます。詳細については、トピック Security Manager クライアントからのデバイス インベントリのエクスポート、共有ポリシーのエクスポート、およびポリシーまたはデバイスのインポートを参照してください。

Perl コマンドは $NMSROOT\bin（通常は C:\Program Files\CSCSpx\bin）にあります。コマンドの構文は次のとおりです。

perl [*path*]**PolicyObjectImportExport.pl -u** *username* **-p** *password* **-o {import | export}** [**-a** *activity*] **-t** *object_type* **-f** *filename* [**-c {true | false}**] [**-d {true | false}**] [**-e {true | false}**] [**-g {true | false}**] [**-h**]

構文

perl [*path*] **PolicyObjectImportExport.pl**	Perl スクリプト コマンド。システム パス変数内に PolicyObjectImportExport.pl ファイルへのパスが定義されていない場合は、そのパスを追加します。 ヒント　「perl」コマンドを含めるのを忘れた場合、システムは入力を受け入れますが、何も行われず、エラーに関するフィードバックも提供しません。Ctrl+Z を使用して、コマンドプロンプトに戻ります。
-u *username*	Security Manager のユーザ名。エクスポートされるデータは、このユーザに割り当てられた権限によって制限されます。ポリシー オブジェクトのインポートまたはエクスポートには、ユーザに Modify Objects 権限が必要であり、デバイス レベルのオーバーライドのインポートまたはエクスポートには、さらに Modify Devices 権限が必要です。 Workflow 以外のモードでオブジェクトをインポートする場合は、Submit および Approve 権限も必要です。
-p *password*	ユーザーのパスワード。
-o {import | export}	実行する操作のタイプ。ポリシー オブジェクトを既存のファイルからインポートするか、ポリシー オブジェクトを CSV ファイルにエクスポートするかです。コミットされたオブジェクトだけがエクスポートされます。
-a *activity*	（オプション）Workflow アクティビティの名前。名前を指定しない場合、新しいアクティビティは username_time という名前で作成されます。
-t *object_type*	オブジェクト タイプ。次のいずれかです。 • network：ネットワーク/ホスト オブジェクトの場合。 • service：サービス オブジェクトの場合。 • portlist：ポートリストオブジェクトの場合。
-f *filename*	CSV ファイルの名前。エクスポート時にファイルが存在する場合は、上書きされます。

-c {true | false}	（オプション）オブジェクトをインポートするときに、ポリシー オブジェクトの競合検出をイネーブルにするかどうか。 • false：既存のオブジェクトに同じコンテンツがある場合でも、オブジェクトはインポートされます。 • true：インポートされるオブジェクトと同じコンテンツが既存のオブジェクトにある場合、インポートされるオブジェクトはスキップされます。[Policy Objects] ページの [冗長オブジェクトが検出された場合（When Redundant Objects Detected）] オプションで、[適用（Enforce）] を選択する必要もあります。
-d {true | false}	（オプション）インポートまたはエクスポート操作中にデバイス レベルのポリシー オブジェクト オーバーライドを処理する方法。 • true：グローバルに定義されたすべてのオブジェクトおよびオブジェクトのデバイス レベルのすべてのオーバーライドを含めます。 • false：ポリシー オブジェクトのグローバル定義だけを含めます。デバイス レベルのポリシー オブジェクト オーバーライド情報は含めません。これがデフォルトです。
-e {true | false}	（オプション）サービス オブジェクトおよびサービス グループ オブジェクトのポートリスト オブジェクトを「フラット化」するかどうか。 • true：サービス オブジェクトおよびサービス グループ オブジェクトで見つかったポートリスト オブジェクトの名前は、リストの実際のポートに置き換えられます。つまり、2 つのオブジェクト（ポートリストとサービス、またはポートリストとサービス グループ）は、単一のサービスまたはサービス グループに「フラット化」されます。 ポートリスト オブジェクトは、Security Manager でポート定義のセットをグループ化するために使用され、サービスおよびサービス グループ オブジェクトを定義するときに使用されます。ただし、PRSM ではポートリスト オブジェクトはサポートされていません。 • false：サービス内のポートリスト オブジェクトおよびサービス グループ オブジェクトはフラット化されません。これがデフォルトです。

-g {true | false}	（オプション）CSV ファイルにオブジェクトタイプとオブジェクトグループタイプを含めるかどうか。 • true：ファイルの最後の列は[タイプ（Type）]で、「サービス」または「ネットワーク」を示します。 • false：[タイプ（Type）]列は含まれません。これがデフォルトです。
-h	（オプション）コマンドラインのヘルプを表示します。このオプションを指定すると、他のすべてのオプションは無視されます。

ポリシー オブジェクトのインポート

オブジェクトをインポートするときに、オブジェクトが別のオブジェクトを参照している場合は、そのオブジェクトが Security Manager ですでに定義されている必要があります。または、インポートする同じ CSV ファイル内で定義されている必要があります。そのオブジェクトが同じ CSV ファイル内にある場合は、それを参照するオブジェクトよりも前にある必要があります（Security Manager では、オブジェクトはエクスポート時に必要に応じて自動的にソートされます）。

インポートするポリシー オブジェクトと同じ名前のポリシー オブジェクトが Security Manager 内にすでに存在する場合、オブジェクトはスキップされてインポートされません。名前の競合は、別のユーザがオブジェクトを作成したが、まだ公開用にコミットしていない場合にも発生する可能性があります。そのため、競合しているオブジェクトを参照できない場合があります。Security Manager では、新しいオブジェクトだけが作成され、既存のオブジェクトは更新されません。-c オプションを使用して、既存のオブジェクトと同じコンテンツの新しいオブジェクトを作成できるかどうかを指定します。

コマンドを実行したときに、ファイル内にエラーがあると、影響を受けるオブジェクトだけがインポートされません。これらの問題は発生時にエラー メッセージによって示され、Security Manager ではファイル内のすべてのレコードの評価が続行されます。正しく定義されたすべてのポリシーオブジェクトはインポートされ、エラーがあるオブジェクトはスキップされます。インポートされなかったポリシー オブジェクトの合計数と名前が出力画面に表示されます。

インポート コマンドの完了後、追加のアクションは、使用している Workflow モードによって異なります。

- Workflow モード：同じユーザ名とパスワードを使用して Security Manager にログインし、インポート中に指定したアクティビティを送信する必要があります。変更を有効にするには、アクティビティが送信されて承認される必要があります。
- Workflow 以外のモード：インポートされたオブジェクトは自動的に送信されて承認されます。アクションは必要ありません。ただし、入力したユーザ名に Submit および Approve 権限がない場合はエラーが表示され、インポート操作は失敗します。

CSV ファイル形式

1 つのファイル内のすべてのオブジェクトは、同じポリシー オブジェクト タイプになります。ファイルは、標準的な Comma-Separated Values（CSV; カンマ区切り値）形式です。最初の行はカラムの見出しです。各行は、1 つのポリシー オブジェクトを表します。カラムは、左から右へという順で、次のとおりです。

- [名前（Name）]：（必須）オブジェクトの名前。
- [Node]：ポリシー オブジェクトのオーバーライドが定義されているデバイスの表示名。ポリシー オブジェクトがグローバル レベルで定義されている場合、このフィールドは空です。オブジェクトをインポートするときに、表示名が Security Manager インベントリにすでにあるデバイスと一致しない場合、オブジェクトはスキップされてインポートされません。
- [Description]：オブジェクトの説明（ある場合）。
- [Category]：オブジェクトのカテゴリ ID（ある場合）。カテゴリ ID は 10 ～ 19 です。
- [Allow Override]：オブジェクトが上書き可能かどうか。ポリシー オブジェクトがデバイス レベルで上書き可能な場合は True。上書き不可の場合は False（または空のフィールド）。
- [Group]：このポリシー オブジェクトによって参照される、同じタイプの他のポリシー オブジェクトの名前。複数のオブジェクトがある場合は、カンマで区切られます。たとえば、ネットワーク構築ブロック Net1 がネットワーク構築ブロック Net2 および Net3 を参照しています。Net1 の [グループ（Group）] フィールドの値は、「Net2,Net3」になります。
- [Data]：オブジェクトのコンテンツ。
- [Subtype]：ネットワーク/ホスト オブジェクトおよびサービス オブジェクトのオブジェクト サブタイプ（ある場合）。ネットワーク/ホストオブジェクトタイプおよびサービスオブジェクトタイプの説明については、ネットワーク/ホストオブジェクトについて （105 ページ）および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 （132 ページ）を参照してください。値は以下のとおりです。
  - ブランク（スペース）：オブジェクトはグループ オブジェクト（ネットワーク/ホストまたはサービス）です。
  - NH：（ネットワーク/ホストオブジェクトのみ）単一ホストのネットワーク/ホストオブジェクト。
  - NF：（ネットワーク/ホストオブジェクトのみ）単一の完全修飾ドメイン名（FQDN）ネットワーク/ホストオブジェクト。
  - NN：（ネットワーク/ホストオブジェクトのみ）単一のネットワークアドレスのネットワーク/ホストオブジェクト。
  - NR：（ネットワーク/ホストオブジェクトのみ）単一のアドレス範囲のネットワーク/ホストオブジェクト。
  - SO：（サービスオブジェクトのみ）単一サービスのサービスオブジェクト。

- [タイプ（Type）]：このエントリによって表されるオブジェクトのタイプ（「ネットワーク」または「サービス」）。

特定のフィールドに値がない場合、そのフィールドは出力でブランクになります。フィールドに複数の値がある場合、フィールドは二重引用符で囲まれます。

AAAサーバおよびサーバグループオブジェクトについて

AAA サーバ オブジェクトを使用して、ネットワーク内で使用される AAA サーバを識別します。AAA によって、デバイスでは次に示すように、ユーザがだれか（認証）、ユーザが何を許可されているか（認可）、ユーザが実際に何をしたか（アカウンティング）を判別できます。

- 認証：認証とは、ネットワークおよびネットワーク サービスへのアクセスを許可される前に、ユーザが認証される方法です。有効なユーザー クレデンシャル（通常は、ユーザー名とパスワード）を要求することで、アクセスが制御されます。すべての認証方式（ローカル認証、回線パスワード認証、およびイネーブル認証を除く）は、AAA を使用して定義する必要があります。認証だけで使用することも、認可およびアカウンティングとともに使用することもできます。
- 認可：認証の完了後、認可によって、認証済みの各ユーザが使用できるサービスおよびコマンドが制御されます。認可は、ユーザが実行を認可されていることを示す属性のセットをアセンブルすることによって機能します。これらの属性は、データベースに含まれている特定のユーザの情報と比較され、結果は、ユーザの実際の機能と制約を決定するために AAA に返されます。データベースは、アクセス サーバまたはルータにローカルに配置するか、RADIUS または TACACS+ セキュリティ サーバでリモートでホスティングできます。認可を使用しない場合は、認証が単独で、認証済みのすべてのユーザに対してサービスへの同じアクセスを提供します。認可は認証とともに使用する必要があります。
- アカウンティング：アカウンティングは、ユーザがアクセスしているサービス、およびユーザが消費しているネットワーク リソース量を追跡するために使用されます。AAA アカウンティングをアクティブにすると、ネットワーク アクセス サーバによって、ユーザ アクティビティがアカウンティング レコードの形式で RADIUS または TACACS+ セキュリティ サーバ（実装したセキュリティ方式によって異なる）にレポートされます。アカウンティング情報には、セッションの開始時刻と停止時刻、ユーザー名、セッションごとのデバイスを通過したバイト数、使用されたサービス、および各セッションの時間が含まれています。このデータを、ネットワーク管理、クライアント請求、または監査のために分析できます。アカウンティングは、単独で使用するか、認証および認可とともに使用することができます。

AAA によって、アクセル ルール（ACL）だけを使用するよりも、ユーザ アクセスについて高いレベルの保護と制御が提供されます。たとえば、すべての外部ユーザが DMZ ネットワーク上のサーバで Telnet の使用を試行できるアクセス ルールを作成できます。一部のユーザだけが実際にサーバに到達できるようにする場合（さらに、それらのユーザの IP アドレスが常にわかるわけではないため、単純なアクセス ルールを設定できない場合）、認証済みまたは認可済みのユーザだけがネットワーク デバイス（ASA やルータなど）を通過することを AAA が許

可できるようにすることができます。そのため、ユーザはTelnetサーバに到達する前に認証する必要があり、サーバでは Telnet が別のログインを要求することもできます。

AAA サーバ オブジェクトを AAA サーバ グループ オブジェクトにまとめることができます。通常、AAA を必要とするポリシー（Easy VPN、リモート アクセス VPN、Secured Device Provisioning や 802.1x などのルータ プラットフォーム ポリシーなど）は、AAA サーバ グループ オブジェクトを参照します。これらのオブジェクトには、同じプロトコル（RADIUS や TACACS+ など）を使用する複数の AAA サーバが含まれています。AAA サーバ グループとは、ネットワーク セキュリティ ポリシー全体の特定の側面を実施することに焦点を当てた認証サーバの集合のことです。たとえば、内部トラフィック、外部トラフィック、またはリモート ダイヤルイン ユーザの認証専用のサーバや、ファイアウォール デバイスの管理を認可するサーバをグループ化できます。

次の項では、AAA サーバ オブジェクトを操作する方法について説明します。

サポートされる AAA サーバ タイプ

すべてのデバイスに RADIUS プロトコルを使用し、IPS 以外のすべてのデバイスに TACACS+ プロトコルと LDAP プロトコルを使用する AAA サーバを使用できます。ASA、PIX、および FWSM デバイスの場合は、 ASA、PIX、および FWSM デバイスでのその他の AAA サポート （39 ページ）で説明されているプロトコルを使用することもできます。

- RADIUS：Remote Authentication Dial-In User Service（RADIUS）は、無許可のアクセスに対してネットワークを保護する分散クライアント/サーバーシステムです。シスコの実装では、RADIUS クライアントはシスコ デバイス上で実行され、すべてのユーザ認証およびネットワーク サービス アクセス情報を持つ中央の RADIUS サーバに認証要求を送信します。

RADIUS は、固有のデバイス タイプでサポートされているプロトコルに応じて、他の AAA セキュリティ プロトコル（TACACS+、Kerberos、ローカル ユーザ名検索など）とともに使用できます。RADIUS はすべての Cisco プラットフォームでサポートされますが、RADIUS でサポートされる一部の機能は、指定されたプラットフォームだけで実行されます。

Cisco Security Manager 4.17 以降、IPv6 は RADIUS プロトコルで有効になっています。このサポートは、ASA 9.9.2 以上のデバイスにのみ適用されます。ユーザーは、[AAAサーバーを追加（Add AAA Server）] ダイアログボックスで Radius 認証の IPv6 ホストアドレスを設定できるようになりました（[Add AAA Server]/[Edit AAA Server] ダイアログボックス （45 ページ）を参照）。サポートされていないデバイスバージョンに対しても、アクティビティの検証が導入されています。

- TACACS+：Terminal Access Controller Access Control System（TACACS+）は、ユーザーによるルータまたはネットワーク アクセス サーバーへのアクセス試行の集中的な確認を可能にするセキュリティアプリケーションです。TACACS+ の目的は、単一の管理サービスから複数のネットワーク アクセス ポイントを管理する方法を提供することです。

TACACS+ では、独立したモジュラ型の認証、許可、アカウンティング機能が提供されます。TACACS+ では、単一のアクセス コントロール サーバ（TACACS+ デーモン）で各サービスを独立して提供することが可能です。

- LDAP：Lightweight Directory Access Protocol（LDAP）。LDAP サーバの使用法は、ポリシーごとに固有です。たとえば、ASA でのアイデンティティ ファイアウォール設定、ASA での VPN 設定、IOS デバイスでの ScanSage 設定などです。ASA での LDAP サーバの使用の詳細については、 ASA、PIX、および FWSM デバイスでのその他の AAA サポート （39 ページ）を参照してください。

関連項目

- ASA、PIX、および FWSM デバイスでのその他の AAA サポート （39 ページ）
- AAA サーバ オブジェクトの作成 （44 ページ）
- AAA サーバおよびサーバ グループ オブジェクトについて （37 ページ）

ASA、PIX、および FWSM デバイスでのその他の AAA サポート

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き PIX および FWSM 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。

RADIUS および TACACS+ をサポートする以外に、ASA、PIX 7.0+、および FWSM 3.1+ デバイスでは、次のプロトコルを実行する AAA サーバをサポートできます。詳細については、該当するデバイス タイプおよびオペレーティング システム バージョンの設定ガイドで AAA の使用方法の説明を参照してください。

- **Kerberos**：これらのデバイスでは、認証に Kerberos サーバーを使用できます。3DES、DES、および RC4 暗号化タイプがサポートされています。
- **NT**：これらのデバイスでは、NTLMv1 認証に Windows ドメインサーバーを使用できます。

- **SDI サーバー**：RSA Security, Inc. の SecurID サーバーは SDI サーバーと呼ばれます。ユーザが VPN アクセスを確立しようとし、該当するトンネル グループ ポリシーが SDI 認証サーバ グループを指定している場合、ASA デバイスはユーザ名およびワンタイム パスワードを SDI サーバに送信します。デバイスは、サーバからの応答に基づいてユーザ アクセスを付与するか拒否します。SDI のバージョン 5.0 では、単一ノード シークレット ファイル（SECURID）を共有する SDI プライマリ サーバーおよびセカンダリ サーバーの概念が導入されました。その結果、SDI サーバを AAA サーバ オブジェクトとして設定する場合、サーバがバージョン 5.0 かそれよりも前のバージョンかを指定する必要があります。
- **LDAP**：これらのデバイスでは、VPN 認可に Lightweight Directory Access Protocol（LDAP）サーバーを、アイデンティティ対応ファイアウォール ポリシーにユーザ グループ ID を使用できます。これらのデバイスでは LDAP バージョン 3 がサポートされ、任意の v3 または v2 ディレクトリ サーバと互換性があります。ただし、パスワード管理は、Sun Microsystems JAVA System Directory Server および Microsoft Active Directory だけでサポートされています。

その他のタイプの LDAP サーバ（Novell や OpenLDAP など）では、パスワード管理以外のすべての LDAP 機能がサポートされています。したがって、これらのサーバのいずれかを認証用に使用してこれらのデバイスのいずれかにログインしようとし、パスワードが期限切れになっている場合、デバイスでは接続はドロップされ、手動でのパスワードのリセットが必要になります。

LDAP サーバに対して LDAP クライアント（この場合は、ASA、PIX、または FWSM デバイス）を認証するように Simple Authentication and Security Layer（SASL）メカニズムを設定できます。これらのデバイスおよび LDAP サーバでは、複数のメカニズムをサポートできます。両方のメカニズム（MD5 および Kerberos）が使用可能な場合、ASA、PIX、または FWSM デバイスは、より強力なメカニズム（Kerberos）を認証に使用します。

VPN アクセスのユーザ認証が成功し、該当するトンネル グループ ポリシーが LDAP 認証サーバ グループを指定している場合、ASA、PIX、または FWSM デバイスは LDAP サーバを照会し、受け取った認可を VPN セッションに適用します。

- **HTTP-Form**：これらのデバイスでは、WebVPN ユーザだけの Single Sign-On（SSO; シングルサインオン）認証に HTTP Form プロトコルを使用できます。シングル サインオンのサポートによって、WebVPN ユーザはユーザ名とパスワードを 1 回だけ入力して、複数の保護されているサービスおよび Web サーバにアクセスできます。セキュリティ アプライアンスで実行されている WebVPN サーバは、認証サーバに対して、ユーザのプロキシとして機能します。ユーザがログインすると、SSO 認証要求（ユーザ名とパスワードを含む）が WebVPN サーバから認証サーバに HTTPS を使用して送信されます。サーバによって認証要求が承認されると、SSO 認証クッキーが WebVPN サーバに返されます。セキュリティ アプライアンスでは、ユーザに代わってこのクッキーが保持され、SSO サーバによって保護されているドメイン内のセキュア Web サイトに対してユーザを認証するために使用されます。

次の表に、各プロトコルでサポートされている AAA サービスを示します。

表 *5 : ASA*、*PIX*、および *FWSM* デバイスでサポートされている *AAA* サービス

AAA サービス	データベース タイプ							
	Local	RADIUS	TACACS+	SDI	NT	Kerberos	LDAP	HTTP Form
認証								
VPN ユーザ	対応	対応	対応	対応	対応	対応	対応	○ 1
ファイアウォール セッション	対応	対応	対応	対応	対応	対応	対応	×
管理者	対応	対応	対応	対応 2	対応	対応	対応	×
許可								
VPN ユーザ	対応	対応	×	×	×	×	対応	×
ファイアウォール セッション	なし	対応 3	対応	×	×	×	×	×
管理者	対応 4	×	対応	×	×	×	×	×
アカウンティング								
VPN 接続	×	対応	対応	×	×	×	×	×
ファイアウォール セッション	×	対応	対応	×	×	×	×	×
管理者	非対応	対応 5	対応	×	×	×	×	×

1. HTTP-Form プロトコルでは、WebVPN ユーザだけの Single Sign-On（SSO; シングル サインオン）認証がサポートされます。2. SDI は、HTTP 管理アクセスについてはサポートされません。3. ファイアウォール セッションの場合、RADIUS 許可はユーザ固有の ACL だけでサポートされます。ユーザ固有の ACL は、RADIUS 認証応答で受信または指定されます。4. ローカル コマンド許可は、特権レベルに限りサポートされます。5. コマンド アカウンティングは、TACACS+ でのみ使用できます。

関連項目

- サポートされる AAA サーバ タイプ （38 ページ）
- AAA サーバ オブジェクトの作成 （44 ページ）
- AAA サーバおよびサーバ グループ オブジェクトについて （37 ページ）

定義済みの AAA 認証サーバ グループ

特定の AAA サーバを指定しないで認証方式を定義するいくつかの定義済みの AAA サーバ グループがあります。IPSec プロポーザルなどのポリシーでは、これらの定義済みのサーバ グループを使用して、実行する AAA 認証のタイプとそれらの実行順序を定義できます。

以下の表に、定義済みの AAA 認証サーバーグループを示します。

表 *6*: 定義済みの *AAA* 認証サーバ グループ

名前	説明
有効化（Enable）	デバイス上で定義されたイネーブル パスワードを認証に使用します。
KRB5 KRB5-Telnet	Kerberos 5 を認証に使用します。Telnet を使用して接続する場合は、KRB5-Telnet を使用します。 Cisco IOS ルータの場合、Kerberos 5 クライアント設定は、このプロトコルをサポートする IOS ソフトウェア バージョンを実行している選択済みプラットフォームだけで使用できます。サーバ設定はサポートされていません。デバイスに Advanced シリーズ フィーチャ セット（k9 暗号イメージ）が含まれている必要があります。
if-authenticated	if-authenticated 方式を使用します。この方式では、認証済みの場合に、ユーザは要求した機能にアクセスできます。
回線（Line）	デバイス上で定義された回線パスワードを認証に使用します。
ローカル（Local） local-case	（デバイス上で定義された）ローカル ユーザ名データベースを認証に使用します。ログインで大文字と小文字を区別する場合に、local-case を使用します。
なし（None）	認証を使用しません。
RADIUS TACACS+	RADIUS または TACACS+ 認証を使用します（Cisco IOS ルータには適用されません）。 これらの AAA サーバ グループには AAA サーバは含まれていません。ポリシーを定義するときにこれらのいずれかを使用するには、デバイスレベルのオーバーライドを作成し、グループに関連付ける AAA サーバを定義する必要があります。詳細については、単一デバイスのオブジェクト オーバーライドの作成または編集 （26 ページ）を参照してください。

関連項目

- AAA サーバ グループ オブジェクトの作成 （63 ページ）
- デフォルトの AAA サーバ グループおよび IOS デバイス （43 ページ）
- AAA サーバおよびサーバ グループ オブジェクトについて （37 ページ）

デフォルトの AAA サーバ グループおよび IOS デバイス

IOS ソフトウェアを使用すると、AAA サーバ グループのメンバーとして、または個別のサーバとして、AAA サーバを定義できます。ただし、Security Manager では、すべての AAA サーバは AAA サーバ グループに属している必要があります。

したがって、AAA サーバ グループに属していない個別の AAA サーバがデバイス設定に含まれている IOS デバイスを検出した場合、それらのサーバを含めるために次のサーバ グループが Security Manager によって作成されます。

- RADIUS の場合：CSM-rad-grp
- TACACS+ の場合：CSM-tac-grp

これらの特別な AAA サーバ グループは、どちらも、Policy Object Manager で、これらのプロトコルのデフォルト グループとしてマークされます。これは、[このグループをデフォルトAAA サーバーグループとする（Make this Group the Default AAA Server Group）] チェックボックスで指定されます。

これらのグループは、Security Manager による管理のためだけに作成されます。展開中に、これらの特別なグループ内の AAA サーバは、グループの一部としてではなく、個別のサーバーとして IOS デバイスに展開されます。

独自のデフォルト グループを作成することもできます。デフォルト グループはほとんどの場合に使用できますが、同じプロトコルを使用する複数の AAA サーバ グループを設定する必要がある場合を除きます。たとえば、1 つのグループを認証用に使用し、もう 1 つのグループを認可用に使用できるように、複数の RADIUS グループを定義する場合があります。サービス プロバイダーは、VRF を使用するときに、カスタマーを分離するために同じプロトコルで複数のグループを定義する場合があります。

（注） PIX/ASA/FWSM デバイスに対して定義されるポリシーでこれらのデフォルト AAA サーバ グループのいずれかを使用する場合、AAA サーバは、個別のサーバとしてではなく、グループとしてそのデバイスに展開されます。これは、PIX/ASA/FWSM デバイス上のすべての AAA サーバは、AAA サーバ グループに属している必要があるためです。

注意 これらのデフォルトAAAサーバ グループをポリシー定義で使用する場合は注意してください。各 AAA サーバーグループに対して一度、すべての個別の AAA サーバーに対して一度定義できる特定のコマンドがあります（たとえば、**ip radius** および **ip tacacs**。これらは、[AAAサーバー（AAA Server）] ダイアログボックスの [インターフェイス（Interface）] フィールドを使用して定義されます）。デフォルトグループ内の AAA サーバーは IOS デバイスに個別のサーバーとして展開されるため、Security Manager によって管理されていないサーバを含む、デバイス上で設定されたすべての個別の AAA サーバーの **ip radius** または **ip tacacs** 設定を間違って変更する可能性があります。（その場合の設定は変更されないままとなります）

関連項目

- 定義済みの AAA 認証サーバ グループ （42 ページ）
- AAA サーバ グループ オブジェクトの作成 （63 ページ）
- AAA サーバおよびサーバ グループ オブジェクトについて （37 ページ）

AAA サーバ オブジェクトの作成

AAA サーバ オブジェクトを作成し、AAA ルール、Easy VPN、802.1x などのポリシーによって参照される AAA サーバ グループ オブジェクトに読み込むことができます。IPS デバイス上の AAA ポリシーなどでは、AAA サーバ オブジェクトがポリシーによって直接使用される場合があります。

AAA サーバーオブジェクトを作成する場合、外部 AAA サーバの IP アドレスまたは DNS 名、およびサーバーによって使用されるプロトコルを指定する必要があります。必要な他の設定はプロトコルによって異なります。

（注） PIX/ASA/FWSM デバイスでは、ポリシーによって参照されていないデバイス設定内の AAA オブジェクトは、次の展開中にデバイスから削除されます。ただし、RADIUS および TACACS+ という名前の定義済みの AAA オブジェクトは、ポリシーによって参照されていない場合でも、PIX 6.3 デバイスから削除されません。

関連項目

- ポリシー オブジェクトの作成 （13 ページ）
- サポートされる AAA サーバ タイプ （38 ページ）
- ASA、PIX、および FWSM デバイスでのその他の AAA サポート （39 ページ）
- AAA サーバおよびサーバ グループ オブジェクトについて （37 ページ）

ステップ 1 [管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択して [Policy Object Manager] を開きます（ Policy Object Manager （4 ページ）を参照）。

ステップ 2 オブジェクトタイプセレクタから [AAAサーバー（AAA Servers）] を選択します。

ステップ 3 作業領域を右クリックし、[新規オブジェクト（New Object）] を選択して [Add AAA Server]/[Edit AAA Server] ダイアログボックス （45 ページ）を開きます。

ステップ 4 オブジェクトの名前を入力し、任意でオブジェクトの説明を入力します。

ステップ 5 AAA サーバを識別します。

- [Host] フィールドに、AAA サーバの IP アドレスか、ASA または PIX 7.2 以降のデバイスの場合は、AAA サーバのホスト名を入力します。ホスト IP アドレスを含むネットワーク/ホストオブジェクトの名前を入力するか、または [選択（Select）] をクリックしてオブジェクトを選択することもできます。

- 任意で、[Interfaces] フィールドに、すべての発信 RADIUS または TACACS+ パケットに対して、その IP アドレスが使用されるインターフェイスまたはインターフェイス ロール（デバイスで単一のインターフェイス名に解決される必要があります）の名前を入力します。IPS デバイス上で使用されているオブジェクトのインターフェイスを指定しないでください。
- 任意で、AAA サーバを応答なしと見なすまでの待機時間を入力します。

ステップ 6 AAAサーバによって使用されるプロトコルを選択し、プロトコル固有のプロパティを設定します。RADIUS はすべてのデバイス タイプで使用でき、TACACS+ は IPS デバイス以外のすべてのデバイス タイプで使用できます。Kerberos、LDAP、NT、SDI、およびHTTP-FORMプロトコルは、ASA、PIX 7.x+、およびFWSM 3.1+ デバイスだけで使用できます。

プロパティの詳細については、次の項を参照してください。

- RADIUS： [AAA Server] ダイアログボックス - RADIUS 設定 （48 ページ）を参照してください。
- TACACS+： [AAA Server] ダイアログボックス - TACACS+ 設定 （51 ページ）を参照してください。
- Kerberos： [AAA Server] ダイアログボックス - Kerberos 設定 （52 ページ）を参照してください。
- LDAP： [AAA Server] ダイアログボックス - LDAP 設定 （53 ページ）を参照してください。
- NT： [AAA Server] ダイアログボックス - NT 設定 （57 ページ）を参照してください。
- SDI： [AAA Server] ダイアログボックス - SDI 設定 （58 ページ）を参照してください。
- HTTP-FORM： [AAA Server] ダイアログボックス - HTTP-FORM 設定 （59 ページ）を参照してください。

ステップ 7 （任意）[Category] の下で、[Objects] テーブルでこのオブジェクトを識別するために使用するカテゴリを選択します。 カテゴリ オブジェクトの使用 （18 ページ）を参照してください。

ステップ 8 [OK] をクリックしてオブジェクトを保存します。

[Add AAA Server]/[Edit AAA Server] ダイアログボックス

[Add AAA Server]/[Edit AAA Server] ダイアログボックスを使用して、AAA サーバ オブジェクトを作成、コピー、および編集します。これらのオブジェクトは AAA サーバ グループ オブジェクトにまとめられ、さまざまな AAA ポリシーを定義するときに、これらのオブジェクトによって使用する AAA サーバが識別されます。これらのオブジェクトは、AAA ポリシーで直接使用される場合があります。

使用できるプロトコルの説明については、 サポートされる AAA サーバ タイプ （38 ページ）および ASA、PIX、および FWSM デバイスでのその他の AAA サポート （39 ページ）を参照してください。

（注） オブジェクトがすでにAAAサーバグループに含まれている場合、プロトコルは編集できません。

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[AAAサーバー（AAA Servers）]を選択します。作業領域内を右クリックして[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[オブジェクトの編集（Edit Object）]を選択します。

関連項目

- AAA サーバおよびサーバ グループ オブジェクトについて （37 ページ）
- AAA サーバ オブジェクトの作成 （44 ページ）
- Policy Object Manager （4 ページ）

フィールド リファレンス

表 *7: [AAA Server]* ダイアログボックス - 一般設定

要素	説明
名前	最大 128 文字のオブジェクト名。オブジェクト名では、大文字と小文字が区別されません。詳細については、 ポリシー オブジェクトの作成 （13 ページ）を参照してください。
説明	（任意）オブジェクトの説明。
ホスト（Host）	認証要求の送信先の AAA サーバのアドレス。次のいずれかを指定します。 • IP アドレス：AAA サーバーの IPv4 または IPv6 アドレス。ホスト IP アドレスを含むネットワーク/ホストオブジェクトの名前を入力するか、または[選択（Select）]をクリックしてオブジェクトを選択することもできます。 （注） AAA：IPV6 ホストは、LDAP および TACACS+ プロトコルでのみサポートされます。Cisco Security Manager 4.17 以降、Radius プロトコルの IPv6 ホストは ASA 9.9(2) デバイス以降でサポートされます。 • [DNS Name]（PIX/ASA 7.2 以降のデバイスの場合だけ）：AAA サーバの DNS ホスト名。最大 128 文字。ホスト名は英数字およびハイフンですが、ホスト名の各要素は英数字で始まり、英数字で終わる必要があります。

要素	説明
インターフェイス	すべての発信 RADIUS または TACACS パケットに対して、その IP アドレスが使用されるインターフェイス（送信元インターフェイスと呼ばれます）。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、あるいは[選択（Select）] をクリックして、リストから名前を選択するか、新しいインターフェイスロールを作成します。 **ヒント** • インターフェイスの名前を入力する場合、この AAA オブジェクトを使用するポリシーが、この名前のインターフェイスを含むデバイスに割り当てられるようにします。 • インターフェイス ロールの名前を入力する場合、ロールが複数のインターフェイスではなく、1 つのインターフェイスを表すようにします。 • AAA サーバ グループ内の AAA サーバに対して定義できる送信元インターフェイスは 1 つだけです。グループ内の別の AAA サーバで異なる送信元インターフェイスが使用されている場合、変更を送信するとエラーが表示されます。 AAA サーバ グループ オブジェクトの作成 （63 ページ）を参照してください。 • IPS デバイス上で使用されている AAA サーバのインターフェイス名を指定しないでください。
タイムアウト（Timeout）	AAA サーバを応答なしと見なすまでの要求に対する待機時間。グループに他のサーバがなければ、次のサーバが試行されます。 • Cisco IOS ルータ：範囲は 1 ～ 1000 秒です。デフォルトは 5 秒です。 • ASA/PIX 7.x 以降、FWSM 3.1 以降のデバイス：範囲は 1 ～ 300 秒です。デフォルトは 10 秒です。 • PIX 6.3 ファイアウォール：範囲は 1 ～ 512 秒です。デフォルトは 5 秒です。 • IPS デバイス：範囲は 1 ～ 512 秒です。デフォルトは 3 秒です。

要素	説明
プロトコル	AAA サーバによって使用されるプロトコル。プロトコルリストの下側のフィールドは、選択によって変わります。 フィールドの詳細については、示されている項を参照してください。 • 次に、最も一般的なプロトコルを示します。 • RADIUS：すべてのデバイス タイプ。[AAA Server] ダイアログボックス - RADIUS 設定 （48 ページ）を参照してください。 • TACACS+：IPS 以外のすべてのデバイス タイプ。[AAA Server] ダイアログボックス - TACACS+ 設定 （51 ページ）を参照してください。 • 次のプロトコルは、ASA/PIX 7.x+ および FWSM 3.1+ デバイスについてサポートされます。LDAP は ScanSafe ポリシーをサポートする IOS デバイスでサポートされます。 • Kerberos：[AAA Server] ダイアログボックス - Kerberos 設定 （52 ページ）を参照してください。 • LDAP：[AAA Server] ダイアログボックス - LDAP 設定 （53 ページ）を参照してください。 • NT：[AAA Server] ダイアログボックス - NT 設定 （57 ページ）を参照してください。 • SDI：[AAA Server] ダイアログボックス - SDI 設定 （58 ページ）を参照してください。 • HTTP-FORM：[AAA Server] ダイアログボックス - HTTP-FORM 設定 （59 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 （18 ページ） を参照してください。

[AAA Server] ダイアログボックス - RADIUS 設定

[AAA Server] ダイアログボックスの RADIUS 設定を使用して、RADIUS AAA サーバ オブジェクトを設定します。

ナビゲーション パス

[Add AAA Server]/[Edit AAA Server] ダイアログボックス （45 ページ）に移動して、[プロトコル（Protocol）] フィールドで [RADIUS] を選択します。

関連項目

- AAA サーバ オブジェクトの作成 （44 ページ）
- AAA サーバおよびサーバ グループ オブジェクトについて （37 ページ）
- [AAA Server Group] ダイアログボックス （65 ページ）

フィールド リファレンス

表 *8 : [AAA Server]* ダイアログボックス - *RADIUS* 設定

要素	説明
キー（Key） 確認（Confirm）	ネットワーク デバイス（クライアント）と AAA サーバ間でデータを暗号化するために使用される共有秘密キー。キーでは、127 文字以下の英数字で、大文字と小文字を区別します。特殊文字も使用可能です。 このフィールドで定義したキーは、RADIUS サーバのキーと一致している必要があります。確認フィールドでもう一度キーを入力します。 次の点に注意してください。 • キーは、IPS AAA ポリシーで使用される AAA サーバ オブジェクトに必須です。それ以外の場合、キーはオプションです。 • PIX、ASA、または FWSM デバイスではスペースを使用できません。これ以外のデバイスでは、スペースは使用できません。 • キーを定義しない場合、AAA サーバとその AAA クライアント間のすべてのトラフィックは暗号化されずに送信されます。
Authentication/Authorization Port	AAA 認証および認可が実行されるポート。デフォルトは 1645 です。 **ヒント** IPS デバイスのデフォルト ポートは 1812 です。このため、IPS 用のオブジェクトの設定時にデフォルト ポートを使用する場合は、この値を変更する必要があります。
Accounting Port	AAA アカウンティングが実行されるポート。デフォルトは 1646 です。

要素	説明
RADIUS Password 確認（Confirm） （ASA、PIX 7.x 以上、および FWSM 3.x 以上のデバイスだけ）	このデバイスを介して RADIUS 認可サーバにアクセスするユーザに共通のキーワード（最大 127 文字で大文字と小文字を区別する英数字）です。[Confirm] フィールドにパスワードを再入力します。 RADIUS 認可サーバーでは、各接続ユーザーに対してパスワードおよびユーザー名が必要です。RADIUS サーバ管理者は、このデバイス経由で RADIUS サーバに対して認可を行う各ユーザにこのパスワードが関連付けられるように RADIUS サーバを設定する必要があります。この情報は、RADIUS サーバー管理者に伝えてください。 共通のユーザー パスワードを指定しなかった場合、各ユーザーのパスワードはユーザー名になります。 RADIUS 認可サーバーを認証に使用することは避けてください。共通パスワードやユーザー名を転用したパスワードは、ユーザーごとに一意のパスワードに比べ、安全性が低くなります。 **ヒント** • パスワードは認可サーバーにのみ適用され、認証サーバーには適用されません。RADIUS 認証サーバーに対しては、共通のパスワードは設定しないでください。 • このパスワードは、認可のため RADIUS プロトコルや RADIUS サーバによって要求されますが、ユーザが知っている必要はありません。デバイスはパスワードを自動的に提供します。
再試行間隔（Retry Interval） （ASA、PIX 7.x 以上、および FWSM 3.x 以上のデバイスだけ）	AAA サーバへのアクセス試行の間隔。値は次のとおりです。 • ASA/FWSM デバイス：1 ～ 10 秒。 • PIX デバイス：1 ～ 5 秒。

要素	説明
ACL Netmask Convert （ASA、PIX 7.x 以上、および FWSM 3.x 以上のデバイスだけ）	RADIUS サーバから受信したダウンロード可能 ACL に含まれているネットマスク表現を処理する方式。ASA/PIX/FWSM は、ダウンロード可能な ACL に標準ネットマスク表現が含まれていると想定します。一方、Cisco IOS ソフトウェアを使用するデバイスは、ダウンロード可能な ACL に、標準ネットマスク表現とは逆のワイルドカードネットマスク表現が含まれていると想定します。ワイルドカード マスクには、無視するビット位置に 1 が、一致するビット位置に 0 が入っています。ワイルドカード ネットマスク表現の変換は、RADIUS サーバ上で ACL の設定を変更しなくても、Cisco IOS ルータ用に作成されたダウンロード可能 ACL が ASA/PIX/FWSM デバイスによって使用可能であることを意味します。 次のオプションのいずれかを選択します。 • [Standard]：セキュリティ アプライアンスでは、RADIUS サーバから受信したすべてのダウンロード可能 ACL に標準ネットマスク表現だけが含まれていると想定します。ワイルドカード ネットマスク表現からの変換は実行されません。これがデフォルトです。 • [Auto-Detect]：セキュリティ アプライアンスでは、ダウンロード可能 ACL で使用されているネットマスク表現のタイプを判別しようとします。ワイルドカード ネットマスク表現を検出した場合は、標準ネットマスク表現に変換します。 RADIUS サーバーの設定方法が不明な場合は、このオプションが役立ちます。ただし、「穴」があるワイルドカードネットマスク表現は、正しく検出および変換できません。たとえば、ワイルドカードネットマスク 0.0.255.0 は、第 3 オクテットに任意の値を許可します。ただし、デバイスでは、この表現をワイルドカードネットマスクとして検出できません。 • [Wildcard]：セキュリティ アプライアンスでは、RADIUS サーバから受信したすべてのダウンロード可能 ACL にワイルドカード ネットマスク表現だけが含まれていると想定します。ワイルドカード ネットマスク表現は、標準ネットマスク表現に変換されます。

[AAA Server] ダイアログボックス - TACACS+ 設定

[AAA Server] ダイアログボックスの TACACS+ 設定を使用して、TACACS+ AAA サーバ オブジェクトを設定します。

ナビゲーション パス

[Add AAA Server]/[Edit AAA Server] ダイアログボックス （45 ページ）に移動して、[プロトコル（Protocol）] フィールドで [TACACS+] を選択します。

関連項目

- AAA サーバ オブジェクトの作成 （44 ページ）
- AAA サーバおよびサーバ グループ オブジェクトについて （37 ページ）
- [AAA Server Group] ダイアログボックス （65 ページ）

フィールド リファレンス

表 *9 : [AAA Server]* ダイアログボックス - *TACACS+* 設定

要素	説明
キー（Key） 確認（Confirm）	クライアントと AAA サーバ間でデータを暗号化するために使用される共有秘密キー。キーは、大文字と小文字が区別される最大 127 文字の英数字文字列（米国英語）です。スペースと特殊文字を使用できます。 このフィールドで定義するキーは、TACACS+ サーバ上のキーと一致する必要があります。確認フィールドでもう一度キーを入力します。 次の点に注意してください。 • PIX、ASA、または FWSM デバイス上でスペースを含むキーを定義しようとすると、アクティビティ検証が失敗します。 • キーを定義しない場合、AAA サーバとその AAA クライアント間のすべてのトラフィックは暗号化されずに送信されます。
サーバポート（Server Port）	AAA サーバとの通信に使用するポート。デフォルトは 49 です。

[AAA Server] ダイアログボックス - Kerberos 設定

[AAA Server] ダイアログボックスの Kerberos 設定を使用して、Kerberos AAA サーバ オブジェクトを設定します。

（注） このタイプの AAA サーバは、ASA、PIX 7.x 以上、および FWSM 3.1 以上のデバイスだけで設定できます。

ナビゲーション パス

[Add AAA Server]/[Edit AAA Server] ダイアログボックス （45 ページ）に移動して、[プロトコル（Protocol）] フィールドで [Kerberos] を選択します。

関連項目

- AAA サーバ オブジェクトの作成 （44 ページ）
- AAA サーバおよびサーバ グループ オブジェクトについて （37 ページ）
- [AAA Server Group] ダイアログボックス （65 ページ）

フィールド リファレンス

表 *10 : [AAA Server]* ダイアログボックス - *Kerberos* 設定

要素	説明
サーバポート（Server Port）	AAA サーバとの通信に使用するポート。デフォルトは 88 です。
Kerberos レルム名	Kerberos 認証サーバーおよびチケット保証サーバーを含むレルムの名前（最大 64 文字、通常はすべて大文字）。たとえば、EXAMPLE.COM となります。
再試行間隔（Retry Interval）	AAA サーバへのアクセス試行の間隔。間隔の範囲は、1 ～ 10 秒です。

[AAA Server] ダイアログボックス - LDAP 設定

[AAA Server] ダイアログボックスの LDAP 設定を使用して、LDAP AAA サーバ オブジェクトを設定します。

（注） このタイプの AAA サーバーは、ASA、PIX 7.x 以上、FWSM 3.1 以上、および IOS のデバイスだけで設定できます。

ナビゲーション パス

[Add AAA Server]/[Edit AAA Server] ダイアログボックス （45 ページ）に移動して、[プロトコル（Protocol）] フィールドで [LDAP] を選択します。

関連項目

- AAA サーバ オブジェクトの作成 （44 ページ）
- AAA サーバおよびサーバ グループ オブジェクトについて （37 ページ）
- [AAA Server Group] ダイアログボックス （65 ページ）

フィールド リファレンス

表 *11 : [AAA Server]* ダイアログボックス - *LDAP* 設定

要素	説明
[LDAP over SSL/セキュア通信を有効にする（Enable LDAP over SSL/Secure Communication）]	デバイスと LDAP サーバ間にセキュアな SSL 接続を確立するかどうか。 **ヒント** パスワード管理をイネーブルにするために Microsoft Active Directory LDAP サーバを使用する場合は、このオプションを選択する必要があります。
[非ネゴシエーション（No Negotiation）] （IOS のみ）	このチェックボックスをオンにすると、以降はネゴシエーションが行われなくなり、以前に確立され、受け入れられたチャネルを受け入れるようになります。
サーバポート（Server Port）	AAA サーバとの通信に使用するポート。デフォルトは 389 です。
[ログインディレクトリ（Login Directory）]	認証済みバインディングに使用される LDAP 階層内のユーザー名またはディレクトリオブジェクトの名前（最大 128 文字）。認証済みバインディングは、一部の LDAP サーバ（Microsoft Active Directory サーバなど）によって、他の LDAP 操作の実行前に要求されます。このフィールドには、デバイスの認証特性が記述されます。これらの特性は、管理者特権を持つユーザーの特性に対応している必要があります。 この文字列では、大文字と小文字が区別されます。文字列でスペースは使用できませんが、他の特殊文字は使用できます。 通常は、DOMAIN\Administrator などのユーザ名です。従来型のフォーマット（cn=Administrator、OU=Employees、DN=example、DN=com など）を使用してもかまいません。
ログイン パスワード	LDAP サーバにアクセスするための、大文字と小文字が区別される英数字のパスワード（最大 64 文字）。スペースは使用できません。
[暗号化（IOS）（Encrypted (IOS)）]	ログイン パスワードを暗号化するかどうか。
LDAP Hierarchy Location	ベース Distinguished Name（DN; 識別名）。これは、認証サーバが認可要求を受け取ったときに検索する LDAP 階層内の場所です。たとえば、OU=Cisco のように指定します。最大長は 128 文字です。 文字列では、大文字と小文字が区別されます。スペースは使用できませんが、他の特殊文字は使用できます。
[PIX/ASA/FWSM] タブ	

要素	説明
LDAP Scope	認可要求を受け取ったサーバで行われる検索の範囲を指定します。次のオプションを使用できます。 • [onelevel]：ベース DN の 1 レベル下だけを検索します。このタイプの検索スコープは、範囲が狭いためサブツリー検索よりも高速です。これがデフォルトです。 • [サブツリー（subtree）]：ベース DN の下にあるすべてのレベル（つまりサブツリー階層全体）が検索対象となります。このオプションを選択すると、検索の実行に時間がかかります。
LDAP Distinguished Name	LDAP サーバのエントリを一意に識別する Relative Distinguished Name 属性を指定します（複数可）。共通の名前付き属性は、Common Name（CN）、sAMAccountName、userPrincipalName、および User ID（uid）です。この英数字の文字列は、最大 128 文字で、大文字と小文字が区別されます。文字列でスペースは使用できませんが、他の特殊文字は使用できます。
SASL MD5 Authentication SASL Kerberos Authentication Kerberos Server Group	これらのオプションによって、LDAP クライアント（ASA/PIX/FWSM デバイス）を LDAP サーバに認証するために、Simple Authentication and Security Layer（SASL）メカニズムが確立されます。これらのオプションのいずれかを選択しない場合は、シンプルなメカニズムが使用され、ユーザー名とパスワードがクリアテキストで送信されます。 1 つまたは両方の SASL 認証メカニズムを定義できます。SASL 認証のネゴシエーション時に、ASA/PIX/FWSM デバイスは、LDAP サーバで設定されている SASL メカニズムのリストを取得し、両方のデバイスで設定されている最も強力なメカニズムを選択します。 • [SASL MD5 Authentication]：デバイスから LDAP サーバに、ユーザ名とパスワードから計算された MD5 値を送信するかどうか。ユーザーパスワードを元に戻せる方法で保存するように LDAP サーバーを設定する必要があります。そうしないと LDAP サーバーがパスワードを検証できません。 • [SASL Kerberos Authentication]：デバイスから LDAP サーバに、Generic Security Services Application Programming Interface（GSSAPI）Kerberos メカニズムを使用してユーザ名とレルムを送信するかどうか。このメカニズムの方が MD5 メカニズムよりも強力です。 Kerberos を選択する場合、SASL 認証に使用される Kerberos AAA サーバ グループの名前も入力する必要があります。最大長は 16 文字です。

要素	説明
[LDAPサーバータイプ（LDAP Server Type）]	AAA に使用される LDAP サーバのタイプ。 • [Auto-Detect]：ASA/PIX/FWSM デバイスがサーバ タイプを自動的に判別しようとします。これがデフォルトです。 • [Microsoft]：LDAP サーバは Microsoft Active Directory サーバです。 （注） Microsoft Active Directory によるパスワード管理をイネーブルにするように LDAP over SSL を設定する必要があります。 • [Sun]：LDAP サーバは Sun Microsystems JAVA System Directory Server です。 • [OpenLDAP]：サーバは OpenLDAP サーバです。これは、ASA/PIX 8.0 以上のデバイスだけで使用できます。 • [Novell]：サーバは Novell LDAP サーバです。これは、ASA/PIX 8.0 以上のデバイスだけで使用できます。
LDAP Attribute Map	LDAP サーバにバインドするための LDAP 属性設定。LDAP 属性マップポリシーオブジェクトの名前を入力するか、または [選択（Select）] をクリックして、リストから名前を選択するか新しいオブジェクトを作成します。 LDAP 属性マップは、ユーザが定義した属性名をシスコ定義の属性にマッピングします。詳細については、[Add LDAP Attribute Map]/[Edit LDAP Attribute Map] ダイアログボックス （61 ページ）を参照してください。
Group Base DN	（Microsoft LDAP AD サーバーのみ）すべてのユーザーグループが定義されるベース指定名（DN）。ASA がユーザ グループ メンバーシップについて AD サーバにアクセスすると、検索はこの DN で開始されます。すべてのグループは、LDAP ディレクトリ階層内のこの DN の下に存在する必要があります。このパスの外側にはグループを配置できません。グループを配置した場合には、グループは見つけられません。この場所を指定すると、ユーザ グループ検索の実行にかかる時間が短縮されます。 英数字文字列は大文字と小文字が区別され、最大 128 文字まで指定できます。文字列でスペースは使用できませんが、他の特殊文字は使用できます。 次に例を示します。 DN=cisco,DN=com ヒント グループベース DN を指定しない場合、LDAP 識別名の設定がグループ検索の開始点として使用されます。

要素	説明
Group Search Timeout	（Microsoft LDAP AD サーバーのみ）ユーザーグループ情報のクエリーに対する Active Directory サーバーからの応答を待機する最長時間（秒単位）。デフォルトは 10 秒で、範囲は 1 ～ 300 秒です。
[IOS] タブ	
[セキュアな暗号（Secure Cipher）]	使用される暗号化方式。
Attribute Map (IOS)	サーバーが使用する IOS 属性マップの名前。
[セキュアなトラストポイント（Secure Trust Point）]	証明書のトラストポイントの名前。
[認証でバインドが先（Authentication bind-first）]	このオプションにより、認証要求の検索とバインドの順序を設定できます。デフォルトでは、検索の後にバインドが実行されます。
[承認は不要（No Authorization Required）]	認証要求に承認は不要です。
Authentication Compare	このチェックボックスを選択すると、バインド要求を認証の比較要求に置き換えることができます。デフォルトでは、認証要求はバインド要求で実行されます。
User Object Filter	検索要求で使用される検索フィルタのユーザー属性タイプを指定します。これは、検索要求されたユーザーをフィルタ処理するために役立ちます。

[AAA Server] ダイアログボックス - NT 設定

[AAA Server] ダイアログボックスの NT 設定を使用して、NT AAA サーバ オブジェクトを設定します。

（注） このタイプの AAA サーバは、ASA、PIX 7.x 以上、および FWSM 3.1 以上のデバイスだけで設定できます。

ナビゲーション パス

[Add AAA Server]/[Edit AAA Server] ダイアログボックス （45 ページ）に移動して、[プロトコル（Protocol）] フィールドで [NT] を選択します。

関連項目

- AAA サーバ オブジェクトの作成　（44 ページ）
- AAA サーバおよびサーバ グループ オブジェクトについて　（37 ページ）
- [AAA Server Group] ダイアログボックス　（65 ページ）

フィールド リファレンス

表 *12 : [AAA Server]* ダイアログボックス - *NT* 設定

要素	説明
サーバポート（Server Port）	AAA サーバとの通信に使用するポート。デフォルトは 139 です。
NT Authentication Host	認証ドメイン コントローラ ホスト名の名前（最大 16 文字）。

[AAA Server] ダイアログボックス - SDI 設定

[AAA Server] ダイアログボックスの SDI 設定を使用して、SDI AAA サーバ オブジェクトを設定します。

（注）　このタイプの AAA サーバは、ASA、PIX 7.x 以上、および FWSM 3.1 以上のデバイスだけで設定できます。

ナビゲーション パス

[Add AAA Server]/[Edit AAA Server] ダイアログボックス　（45 ページ）に移動して、[プロトコル（Protocol）] フィールドで [SDI] を選択します。

関連項目

- AAA サーバ オブジェクトの作成　（44 ページ）
- AAA サーバおよびサーバ グループ オブジェクトについて　（37 ページ）
- [AAA Server Group] ダイアログボックス　（65 ページ）

フィールド リファレンス

表 *13 : [AAA Server]* ダイアログボックス - *SDI* 設定

要素	説明
サーバポート（Server Port）	AAA サーバとの通信に使用するポート。デフォルトは 5500 です。
再試行間隔（Retry Interval）	AAA サーバへのアクセス試行の間隔。間隔の範囲は、1 ～ 10 秒です。デフォルトは 10 秒です。
SDI Server Version	SDI サーバのバージョン。 • [SDI-pre-5]：バージョン 5.0 よりも前のすべての SDI バージョン。 • [SDI-5]：SDI バージョン 5.0 以降。
SDIバージョン5より前のセカンダリサーバー（SDI pre-5 Secondary Server）	（任意）5.0 よりも前の SDI バージョンを使用している場合に、プライマリ サーバに障害が発生したときに認証に使用されるセカンダリ サーバ。ネットワーク/ホストオブジェクトの IP アドレスまたは名前を入力するか [選択（Select）] をクリックしてオブジェクトを選択します。または、新しいオブジェクトを作成します。

[AAA Server] ダイアログボックス - HTTP-FORM 設定

[AAA Server] ダイアログボックスの HTTP-FORM 設定を使用して、Single Sign-On 認証（SSO; シングル サインオン）用の HTTP-Form AAA サーバ オブジェクトを設定します。

（注） このタイプの AAA サーバは、ASA、PIX 7.x 以上、および FWSM 3.1 以上のデバイスだけで設定できます。

ナビゲーション パス

[Add AAA Server]/[Edit AAA Server] ダイアログボックス （45 ページ）に移動して、[プロトコル（Protocol）] フィールドで [HTTP-FORM] を選択します。

関連項目

- AAA サーバ オブジェクトの作成 （44 ページ）
- AAA サーバおよびサーバ グループ オブジェクトについて （37 ページ）
- [AAA Server Group] ダイアログボックス （65 ページ）

フィールド リファレンス

表 *14 : [AAA Server]* ダイアログボックス - *HTTP-Form* 設定

要素	説明
Start URL	セキュリティ アプライアンスの WebVPN サーバがオプションのプリログイン クッキーを取得する URL。URL の最大長は 1024 文字です。 認証 Web サーバは、ログイン ページのコンテンツとともに Set-Cookie ヘッダーを送信することによって、プリログイン シーケンスを実行する場合があります。このフィールドの URL によって、クッキーを取得する場所が定義されます。 （注） 実際のログインシーケンスは、プリログインクッキーシーケンスのあとに開始されます。
Action URI	セキュリティアプライアンスが Single Sign-On（SSO; シングル サインオン）認証の HTTP POST 要求を送信する Web サーバ上の認証プログラムの場所と名前を定義する Uniform Resource Identifier（URI）。 アクション URI の最大長は 2048 文字です。 ヒント 認証 Web サーバー上のアクション URI を見つけるには、ブラウザで直接 Web サーバーのログインページに接続します。ブラウザに表示されるログイン Web ページの URL が、認証 Web サーバーのアクション URI です。
Username Parameter	SSO 認証の HTTP POST 要求に含まれているユーザ名パラメータの名前。最大長は 128 文字です。 ログイン時に、ユーザは実際の名前の値を入力します。それが HTTP POST 要求に入力され、認証 Web サーバに渡されます。
Password Parameter	SSO 認証の HTTP POST 要求に含まれているパスワードパラメータの名前。最大長は 128 文字です。 ログイン時に、ユーザは実際のパスワードの値を入力します。それが HTTP POST 要求に入力され、認証 Web サーバに渡されます。
Hidden Values	SSO 認証の HTTP POST 要求に含まれている非表示パラメータ。ユーザ名やパスワードと異なりユーザには表示されないため、非表示パラメータと呼ばれます。 非表示パラメータの最大長は 2048 文字です。 ヒント 認証 Web サーバから受け取るフォームで HTTP ヘッダー アナライザを使用することによって、Web サーバが POST 要求で想定している非表示パラメータを検出できます。

要素	説明
Authentication Cookie Name	セキュリティ アプライアンスによって SSO に使用される認証クッキーの名前。最大長は 128 文字です。 SSO 認証が成功すると、認証 Web サーバはこの認証クッキーをクライアント ブラウザに渡します。クライアント ブラウザは、このクッキーを提示して、SSO ドメイン内の他の Web サーバに対して認証します。

[Add LDAP Attribute Map]/[Edit LDAP Attribute Map] ダイアログボックス

[Add LDAP Attribute Map]/[Edit LDAP Attribute Map] ダイアログボックスを使用して、Cisco Lightweight Directory Access Protocol（LDAP）属性名をカスタムのユーザ定義属性名に解釈する名前マッピングを使用する属性マップを読み込みます。

既存の LDAP ディレクトリにセキュリティ アプライアンスを導入している場合、既存のカスタム LDAP 属性の名前と値は、Cisco 属性の名前と値とは異なる場合があります。既存の属性の名前を変更するのではなく、カスタムの属性名と値を Cisco の属性名と値にマッピングする、LDAP 属性マップを作成できます。セキュリティ アプライアンスは、単純な文字列置換を使用して、ユーザ独自のカスタム名と値だけを提供します。次に、ユーザは、必要に応じてこれらの属性マップを LDAP サーバにバインドしたり、削除したりできます。属性マップ全体を削除したり、名前および値の個々のエントリを削除したりできます。

ASA、PIX、および FWSM デバイスでの LDAP のサポートの詳細については、ASA、PIX、および FWSM デバイスでのその他の AAA サポート （39 ページ）を参照してください。

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 [LDAP属性マップ（LDAP Attribute Map）] 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

- AAA サーバ オブジェクトの作成 （44 ページ）
- [AAA Server] ダイアログボックス - LDAP 設定 （53 ページ）

フィールド リファレンス

表 15 : [Add LDAP Attribute Map]/[Edit LDAP Attribute Map] ダイアログボックス

要素	説明
名前	最大 128 文字のオブジェクト名。オブジェクト名では、大文字と小文字が区別されません。詳細については、ポリシー オブジェクトの作成 （13 ページ）を参照してください。

要素	説明
説明	（任意）オブジェクトの説明。
[Attribute Map] テーブル	このテーブルには、マッピングされた値が表示されます。各エントリは、カスタマー マップ名、Cisco マップ名、およびカスタマー名から Cisco 名への属性マッピングを示します。 • マッピングを追加するには、[行の追加（Add Row）] ボタンをクリックして、 [Add LDAP Attribute Map Value]/[Edit LDAP Attribute Map Value] ダイアログボックス （62 ページ）を開きます。 • マッピングを編集するには、マッピングを選択し、[行の編集（Edit Row）] ボタンをクリックします。 • マッピングを削除するには、マッピングを選択し、[行の削除（Delete Row）] 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 （18 ページ）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 （25 ページ）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 （24 ページ）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。

[Add LDAP Attribute Map Value]/[Edit LDAP Attribute Map Value] ダイアログボックス

[Add LDAP Attribute Map Value]/[Edit LDAP Attribute Map Value] ダイアログボックスを使用して、カスタムの属性名および一致した Cisco 属性名と値に対してユーザ定義の属性値を適用する値マッピングを使用する属性マップを読み込みます。

ナビゲーション パス

[Add LDAP Attribute Map]/[Edit LDAP Attribute Map] ダイアログボックス （61 ページ）で、[行の追加（Add Row）] ボタンをクリックして新しいマッピングを追加するか、または行を選択して [行の編集（Edit Row）] ボタンをクリックします。

フィールド リファレンス

表 16 : [Add LDAP Attribute Map Value]/[Edit LDAP Attribute Map Value] ダイアログボックス

要素	説明
Customer Map Name	Cisco マップに関連する属性マップの名前。
Cisco Map Name	カスタマー マップ名にマッピングする Cisco 属性マップ名。
[Customer to Cisco Map Value] テーブル	カスタマー名から Cisco 名へのマッピング。 • マッピングを追加するには、[行の追加（Add Row）] ボタンをクリックして、[Add Map Value]/[Edit Map Value] ダイアログボックス （63 ページ）を開きます。 • マッピングを編集するには、マッピングを選択し、[行の編集（Edit Row）] ボタンをクリックします。 • マッピングを削除するには、マッピングを選択し、[行の削除（Delete Row）] ボタンをクリックします。

[Add Map Value]/[Edit Map Value] ダイアログボックス

[Add Map Value]/[Edit Map Value] ダイアログボックスを使用して、カスタマー LDAP 属性値を Cisco マップ値にマッピングします。Cisco 値と一致させる、LDAP マップの値を入力します。

ナビゲーション パス

[Add LDAP Attribute Map Value]/[Edit LDAP Attribute Map Value] ダイアログボックス （62 ページ）で、[行の追加（Add Row）] ボタンをクリックして新しいマッピングを追加するか、または行を選択して [行の編集（Edit Row）] ボタンをクリックします。

AAA サーバ グループ オブジェクトの作成

認証や認可などの AAA サービスを必要とする Security Manager ポリシー用に、AAA サーバ グループ オブジェクトを作成できます。各 AAA サーバ グループ オブジェクトには複数の AAA サーバを含めることができ、それらはすべて同じプロトコル（RADIUS や TACACS+ など）を使用します。たとえば、RADIUS を使用してネットワーク アクセスを認証し、TACACS+ を使用して CLI アクセスを認証する場合、少なくとも 2 つの AAA サーバ グループ オブジェクトを作成する必要があります。1 つは RADIUS サーバ用、1 つは TACACS+ サーバ用です。

また、グループ内の AAA サーバに対して定義できる送信元インターフェイスは 1 つだけです。グループ内の別の AAA サーバで異なる送信元インターフェイスが使用されている場合、変更を送信するとエラーが表示されます。

（注） エラーは、送信元として定義されている実際のインターフェイスによってトリガーされます。インターフェイスを表すインターフェイス ロールの名前ではありません。つまり、2 つの AAA サーバは、どちらも同じデバイス インターフェイスに解決されるかぎり、送信元インターフェイスとして定義された異なるインターフェイス ロールを持つことができます。送信元インターフェイスに対して定義されたインターフェイス ロールが、デバイス上の複数の実際のインターフェイスと一致した場合にも、エラーが表示されます。

作成できる AAA サーバ グループ オブジェクトの数および各グループ オブジェクトに含めることができる AAA サーバ オブジェクトの数は、選択されているプラットフォームによって異なります。たとえば、ASA デバイスでは、最大 18 個のシングルモード サーバ グループ（それぞれ最大 16 個のサーバ）と、7 個のマルチモード サーバ グループ（それぞれ最大 4 個のサーバ）がサポートされます。PIX ファイアウォールでは、最大 14 個のサーバ グループ（それぞれ最大 14 個のサーバ）がサポートされます。

（注） Security Manager には、認証を Cisco IOS ルータ内でローカルに実行するときに使用できる定義済みの AAA サーバ グループ オブジェクトが含まれています。

ヒント このオブジェクト タイプを使用するポリシーまたはオブジェクトを定義するときに、AAA サーバ グループ オブジェクトを作成することもできます。詳細については、ポリシーのオブジェクトの選択 （2 ページ）を参照してください。

関連項目

- ポリシー オブジェクトの作成 （13 ページ）
- 定義済みの AAA 認証サーバ グループ （42 ページ）
- デフォルトの AAA サーバ グループおよび IOS デバイス （43 ページ）
- AAA サーバおよびサーバ グループ オブジェクトについて （37 ページ）

ステップ 1 [管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択して [Policy Object Manager] を開きます（Policy Object Manager （4 ページ）を参照）。

ステップ 2 オブジェクトタイプセレクタから [AAAサーバーグループ（AAA Server Groups）] を選択します。

ステップ 3 作業領域を右クリックし、[新規オブジェクト（New Object）] を選択して [AAA Server Group] ダイアログボックス （65 ページ）を開きます。

ステップ 4 オブジェクトの名前を入力します。名前の最大長は、このオブジェクトを ASA、PIX、または FWSM デバイスで使用する場合は 16 文字、Cisco IOS ルータの場合は 128 文字です。スペースはサポートされていません。

（注） Cisco IOS ルータでは、AAA サーバ グループ名として RADIUS、TACACS、TACACS+ はサポートされていません。また、これらの名前の短縮形（rad や tac など）を使用することは推奨しません。

ステップ 5 グループ内のサーバによって使用されるプロトコルを選択します。

ステップ 6 グループに含める AAA サーバを定義する AAA サーバ ポリシー オブジェクトの名前を入力します。[選択（Select）] を選択して、選択したプロトコルによってフィルタリングされたリストからオブジェクトを選択します。選択リストから、新しい AAA サーバ オブジェクトを作成することもできます。複数のオブジェクトを指定する場合は、カンマで区切ります。

ステップ 7 必要な追加オプションを設定します。

- [Make this Group the Default AAA Server Group]：IOS デバイスの場合だけ、このグループをデフォルト グループとして使用するかどうか。AAA を必要とするすべてのポリシーに対して、このプロトコルの単一のグローバル サーバ グループを持つ場合、このオプションを使用します。詳細については、デフォルトの AAA サーバ グループおよび IOS デバイス （43 ページ）を参照してください。
- ASA 8.4(2) 以降のデバイス：Active Directory エージェントサーバーを含む RADIUS グループを作成している場合は、[AD エージェントモード（AD Agent Mode）] を選択します。このオプションは、グループ内のサーバーがフル機能の RADIUS サーバーではなく、アイデンティティ認識型ファイアウォールに AD エージェント機能を提供することを示します。このグループは、アイデンティティ オプションのポリシーで使用してください。
- ASA、PIX、FWSM デバイス：応答を停止した AAA サーバの処理方法について、およびアカウンティング メッセージの送信方法について、オプションを選択します。詳細については、[AAA Server Group] ダイアログボックス （65 ページ）を参照してください。

ステップ 8 （任意）[Category] の下で、[Objects] テーブルでこのオブジェクトを識別するために使用するカテゴリを選択します。カテゴリ オブジェクトの使用 （18 ページ）を参照してください。

ステップ 9 （任意）[デバイスごとに値のオーバーライドを許可（Allow Value Override per Device）] を選択して、このオブジェクトのプロパティを個々のデバイスで再定義できるようにします。ポリシー オブジェクトの上書きの許可 （25 ページ）を参照してください。

ステップ 10 [OK] をクリックしてオブジェクトを保存します。

[AAA Server Group] ダイアログボックス

[AAA Server Group] ダイアログボックスを使用して、AAA サーバ グループを作成、コピー、および編集します。認証、許可、またはアカウンティングに AAA サーバを使用するポリシーを定義するときは、サーバが属しているサーバ グループを選択することによって、サーバを選択します。

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 [AAAサーバーグループ（AAA Server Groups）] を選択します。作業領域内を右

クリックして [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 [オブジェクトの編集（Edit Object）] を選択します。

関連項目

- AAA サーバ グループ オブジェクトの作成 （63 ページ）
- AAA サーバおよびサーバ グループ オブジェクトについて （37 ページ）
- ポリシー オブジェクトの作成 （13 ページ）
- [Add AAA Server]/[Edit AAA Server] ダイアログボックス （45 ページ）
- Policy Object Manager （4 ページ）

フィールド リファレンス

表 17 : [AAA Server Group] ダイアログボックス

要素	説明
名前	オブジェクト名（このオブジェクトをファイアウォール デバイスで使用する場合は最大 16 文字。Cisco IOS ルータの場合は最大 128 文字）。オブジェクト名では、大文字と小文字が区別されません。スペースはサポートされていません。 次の重要事項を考慮してください。 • Cisco IOS ルータでは、RADIUS、TACACS、または TACACS+ という名前の AAA サーバ グループはサポートされていません。また、これらの名前の短縮形（rad や tac など）を使用することは推奨しません。 • この AAA サーバ グループを RADIUS または TACACS+ のデフォルト グループとして定義する場合、ここで定義する名前は、展開時にデバイス設定でデフォルト名（RADIUS または TACACS+）によって自動的に置き換えられます。
説明	（任意）オブジェクトの説明。
プロトコル	グループ内の AAA サーバによって使用されるプロトコル。これらのオプションの詳細については、サポートされる AAA サーバ タイプ （38 ページ）および ASA、PIX、および FWSM デバイスでのその他の AAA サポート （39 ページ）を参照してください。

要素	説明
AAAサーバ	サーバ グループを構成する AAA サーバ ポリシー オブジェクト。オブジェクトの名前を入力するか、または [選択（Select）] をクリックして、選択したプロトコルを使用する AAA サーバーオブジェクトだけを表示するようにフィルタ処理されたリストから選択します。複数のオブジェクトを指定する場合は、カンマで区切ります。選択リストから新しいオブジェクトを作成することもできます。
Make this Group the Default AAA Server Group (IOS) （IOS デバイスのみ）	この AAA サーバ グループを RADIUS または TACACS+ プロトコルのデフォルト グループとして指定するかどうか。AAA を必要とする特定のデバイスのすべてのポリシーに対して、選択したプロトコルで 1 つのグローバル グループを使用する場合、このオプションを選択します。 複数の RADIUS または TACACS+ AAA サーバ グループを作成する場合は、このオプションを選択しないでください。異なる AAA 機能を分離するため（たとえば、認証用に 1 つのグループを使用し、認可用に別のグループを使用）、または VRF 環境で異なるカスタマーを分離するために、複数のグループを使用できます。 （注） IOS ルータを検出するときに、AAA サーバ グループのメンバーではないデバイス設定内の AAA サーバは、CSM-rad-grp（RADIUS の場合）および CSM-tac-grp（TACACS+ の場合）という特別なグループに配置されます。これらはどちらもデフォルト グループとしてマークされています。これら 2 つのグループは、Security Manager でこれらのサーバを管理できるようにするためだけに作成されています。展開中に、これらの特別なグループ内の AAA サーバは、個別のサーバとしてデバイスに展開されます。詳細については、デフォルトの AAA サーバ グループおよび IOS デバイス （43 ページ）を参照してください。
ADエージェントモード（AD Agent Mode） （ASA 8.4(2) 以降のデバイスのみ）。	グループ内のサーバーが、ID 認証ファイアウォール構成で使用される Active Directory エージェントであるかどうかを指定します。AD エージェントグループがフル機能の RADIUS サーバーグループではないことを示すには、このオプションを選択する必要があります。 AD エージェントグループは、アイデンティティオプションのポリシーで使用します。詳細については、Active Directory サーバおよびエージェントの識別を参照してください。

要素	説明
動的認可（Dynamic Authorization） （ASA 9.2(1) 以降のデバイスのみ）。	RADIUS プロトコルを使用している場合は、[動的認可（Dynamic Authorization）]チェックボックスをオンにして、AAA サーバーグループに対して RADIUS 動的認可の認可変更（CoA）サービスを有効にします。 [ポート（Port）] フィールドで、RADIUS CoA 要求のリスニング ポートを指定します。有効数は 1024 ～ 65535 であり、デフォルト値は 1700 です。 一旦定義されると、対応する RADIUS サーバーグループが CoA 通知用に登録され、AAA は Cisco Identity Services Engine（ISE）から CoA ポリシーの更新を行うポートをリッスンします。
中間アカウントの更新（Interim Account Update） （ASA 9.2(1) 以降のデバイスのみ）。	RADIUS プロトコルを使用している場合は、[中間アカウントの更新（Interim Account Update）] チェックボックスをオンにして、RADIUS 中間アカウンティング更新メッセージの生成を有効にします。現在、これらのメッセージは、VPN トンネル接続がクライアントレス VPN セッションに追加された場合にだけ生成されます。これが発生した場合、新たに割り当てられた IP アドレスを RADIUS に通知するためのアカウンティング アップデートが生成されます。 [間隔（Interval）] フィールドの定期アカウンティング更新の間隔（時間単位）を指定します。有効数は 1 ～ 120 であり、デフォルト値は 24 です。
認可のみ（Authorize only） （ASA 9.2(1) 以降のデバイスのみ）。	RADIUS プロトコルを使用している場合は、[認可のみ（Authorize only）] チェックボックスをオンにして、RADIUS サーバーグループの認可専用モードを有効にします。このチェックボックスを選択する場合、個別の AAA サーバに対して設定する共通パスワードは不要なため、設定する必要はありません。
Max Failed Attempts （PIX、ASA、FWSM デバイスだけ）	サーバーグループ内の所定のサーバーが非アクティブ化されるまでに、そのサーバーで許容される接続試行の失敗回数。デフォルトは 3、指定できる範囲は 1 ～ 5 です。
内部レルムID（Internal Realm ID） （ASA 9.8(1) 以降のデバイスのみ）	AAA サーバー グループ ポリシー オブジェクトの RADIUS または LDAP プロトコルに対応するレルム ID を入力します。 （注） レルム ID は、1 から 65535 の一意の値であり、RADIUS および LDAP プロトコルにのみ適用されます。

要素	説明
Reactivation Mode （PIX、ASA、FWSM デバイスだけ）	グループ内の障害が発生したサーバーを再アクティブ化するときに使用する方式。 • [枯渇（Depletion）]：グループ内のすべてのサーバーが非アクティブになった後に、障害の発生したサーバーのみ再度アクティブ化します。これがデフォルトです。 非アクティブになったサーバーは、グループにある他のすべてのサーバーが非アクティブになるまで非アクティブのままです。すべてのサーバーが非アクティブになると、グループ内のすべてのサーバーが再アクティブ化されます。このアプローチでは、障害が発生したサーバーに起因する接続遅延の発生を最小限に抑えられます。 ローカルデータベースを使用してフォールバック方式（管理アクセス専用）を設定していて、グループ内のすべてのサーバーが応答しない場合、そのグループは応答なしと見なされ、フォールバック方式が試行されます。グループの最後のサーバーが無効になってから、すべてのサーバーを再度有効にするまでの経過時間（分単位）を決定する [再アクティブ化のデッドタイム（Reactivation Deadtime）] 値を設定できます。 フォールバック方式として設定されていない場合、デバイスは引き続きグループ内のサーバーにアクセスしようとします。 • [Timed]：ダウンタイムの 30 秒後に、障害が発生したサーバを再アクティブ化します。このオプションは、グループの最初のサーバーがプライマリサーバーであり、可能な限りバックアップサーバーではなくプライマリサーバーを使用する場合に役立ちます。このポリシーは、UDP サーバーの場合は機能しません。サーバーが存在しない場合でも UDP サーバーへの接続は失敗しないため、UDP サーバーはすぐに再度オンラインになります。サーバーグループに到達不能な複数のサーバーが含まれている場合、接続時間が遅くなったり、接続に失敗したりする場合があります。
Reactivation Deadtime （PIX、ASA、FWSM デバイスだけ）	再アクティブ化モードとして [枯渇（Depletion）] を選択した場合、グループ内にある最後のサーバーの非アクティブ化とグループ内の全サーバーの再アクティブ化の間に必要な時間（分）。デフォルトは 10 で、範囲は 0 ～ 1440（24 時間）です。

要素	説明
Group Accounting Mode （PIX、ASA、FWSM デバイスだけ）	RADIUS または TACACS+ プロトコルを使用する場合、アカウンティング メッセージをグループ内の AAA サーバに送信する方式。 アカウンティングにサーバーグループを使用する場合（プロトコルは RADIUS または TACACS+）、アカウンティングメッセージをグループ内の AAA サーバーに送信する方式。 • [Single]：アカウンティング メッセージは、グループ内の 1 つのサーバに送信されます。これがデフォルトです。 • [Simultaneous]：アカウンティング メッセージは、グループ内のすべてのサーバに同時に送信されます。このオプションを選択する場合、再アクティブ化モードとして [指定時刻（Timed）] を使用することが ASA により強制されます。
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 （18 ページ）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 （25 ページ）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 （24 ページ）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。

アクセス コントロール リスト オブジェクトの作成

アクセス コントロール リスト（ACL）オブジェクトは、1 つ以上のアクセス コントロール エントリ（ACE）、1 つ以上の ACL オブジェクト、または両方の組み合わせで構成されます。各 ACE は、ACL 内の個々の許可または拒否ステートメントです。ACL ポリシー オブジェクトを、複数のその他のポリシーおよびポリシー オブジェクト内で使用できます。

Cisco Security Manager バージョン 4.13 以降、オブジェクトグループに VM 属性が含まれていて、それが他のポリシー （アクセス ルールを除く）に適用されている場合、展開は失敗します。VM 属性オブジェクトは、object-group-search access-control がイネーブルになっている場合に、ASA 9.7.1 以降のデバイスに適用されます。

次のタイプの ACL オブジェクトを作成できます。

- 拡張：拡張 ACL では、送信元および宛先アドレスとサービス（またはトラフィックプロトコル）を指定できます。さらに、プロトコルタイプに基づいて、ポート（TCP または UDP の場合）または ICMP タイプ（ICMP の場合）を指定できます。拡張 ACL オブジェ

クトの詳細については、 拡張アクセス コントロール リスト オブジェクトの作成 （71 ページ）を参照してください。

- 標準：標準 ACL は、トラフィックの照合に送信元アドレスを使用します。標準 ACL オブジェクトの詳細については、標準アクセス コントロール リスト オブジェクトの作成 （74 ページ）を参照してください。
- Web：Web ACL では、宛先アドレスおよびポート、または URL フィルタが使用されます。Web タイプ ACL オブジェクトの詳細については、 Web アクセス コントロール リスト オブジェクトの作成 （75 ページ）を参照してください。
- 統合：統合 ACL オブジェクトを使用すると、送信元ネットワーク/ホスト、送信元セキュリティグループ、ユーザ、宛先ネットワーク/ホスト、宛先セキュリティグループ、およびサービスを使用してトラフィックを照合できます。さらに、ネットワーク/ホストの指定には、IPv4 アドレス、IPv6 アドレス、またはその両方の組み合わせを含めることができます（Security Manager 4.4 および ASA 9.0 以降のリリースでは、個別の IPv4 および IPv6 アドレス指定/オブジェクトが「統合」されました）。これらの ACL の詳細については、統合アクセス制御リストオブジェクトの作成 （77 ページ）を参照してください。
- Ethertype：EtherType ACL は、ルーテッドモードおよびトランスペアレントモードのブリッジ グループ メンバーのインターフェイスの非 IP レイヤ 2 トラフィックにのみ適用されます。これらのルールを使用して、レイヤ 2 パケットの EtherType 値に基づいてトラフィックを許可またはドロップできます。EtherType ACL を使用すると、デバイス全体の非 IP トラフィックのフローを制御できます。トランスペアレント ファイアウォール ルールの設定を参照してください。

これらのオブジェクトで使用されるダイアログボックスの参照情報については、 [Add Access List]/[Edit Access List] ダイアログボックス （79 ページ）を参照してください。

（注） CSM には、参照位置の ACL オブジェクトに対する設計レベルの制約があります。したがって、[Policy Object Manager] テーブルの [参照（Referenced）] ボタンは無効になります。

拡張アクセス コントロール リスト オブジェクトの作成

拡張アクセス コントロール リストを使用すると、特定の IP アドレスから特定の宛先 IP アドレスおよびポートへのトラフィックを許可または拒否でき、トラフィックのプロトコル（ICMP、TCP、UDP など）を指定できます。拡張 ACL の範囲は 100 ～ 199 であり、Cisco IOS ソフトウェアリリース 12.0.1 以降を実行しているデバイスの場合は 2000 ～ 2699 です。

拡張 ACL の例：

```
access-list 110 - Applied to traffic leaving the office (outgoing)
access-list 110 permit tcp 10.128.2.0 0.0.0.255 any eq 80
```

ACL 110 は、10.128.2.0 ネットワーク上の任意のアドレスから送信されたトラフィックを許可します。「All-IPv4-Addresses」ステートメントは、ポート 80 へという制限付きで、トラフィックが任意の宛先アドレスを持つことが許可されることを意味します。0.0.0.0/255.255.255.255 という値を「All-IPv4-Addresses」として指定できます。

用途：

- NAT（ポリシー NAT および NAT 免除）のアドレスの識別：ポリシー NAT では、拡張アクセス リストで送信元および宛先アドレスとポートを指定することによって、アドレス変換のローカル トラフィックを識別できます。通常の NAT では、ローカル アドレスだけを考慮できます。ポリシー NAT とともに使用されるアクセス リストは、アクセス コントロール エントリ（ACE）を拒否するように設定することはできません。
- IOS ダイナミック NAT のアドレスの識別：ユーザ定義の ACL の場合、VPN トラフィックから NAT トラフィックを推定するときに、NAT プラグインによって独自の ACL CLI が生成されます。
- Network Admission Control（NAC; ネットワーク アドミッション コントロール）によって代行受信されるトラフィックのフィルタリング。
- モジュラ ポリシーのトラフィック クラス マップ内のトラフィックの識別：アクセス リストを使用して、クラス マップ内のトラフィックを識別できます。クラス マップは、TCP および一般接続設定、検査、IPS、QoS など、Modular Policy Framework をサポートする機能のために使用されます。1 つ以上のアクセス リストを使用して、特定のタイプのトラフィックを識別できます。
- トランスペアレント モードの場合、ルーテッド モードのセキュリティ アプライアンスによってブロックされるプロトコル（BGP、DHCP、マルチキャスト ストリームなど）のイネーブル化。これらのプロトコルには、リターン トラフィックを許可するセキュリティ アプライアンス上のセッションがないため、両方のインターフェイス上にアクセス リストも必要です。
- VPN アクセスの確立：VPN コマンドで拡張アクセス リストを使用して、IPsec サイト間トンネルについてデバイスでトンネリングする必要があるトラフィックを識別できます。または、VPN クライアントについてデバイスでトンネリングする必要があるトラフィックを識別できます。次の表に示すポリシーオブジェクトおよび設定とともに使用します。

表 *18 :* ポリシー オブジェクトおよび設定

ポリシーオブジェクト	Device	目的
VPN トポロジ	任意（Any）	保護ネットワークの選択。
ASA ユーザ グループ	ASA	インバウンド ファイアウォール ポリシー、アウトバウンド ファイアウォール ポリシー、フィルタ ACL。

ポリシーオブジェクト	Device	目的
トラフィック フロー	ASA、PIX 7+	サービス ポリシールール（MPC）。トラフィック フローBB（クラスマップ）は、トラフィック一致タイプの 1 つとして拡張 ACL を使用します。
ユーザー グループ	• IOS • Catalyst 6500/7600 • PIX 6.3	Easy VPN、スプリット トンネル ACL、およびファイアウォール ACL（IOS デバイスだけ）用。

関連項目

- アクセス コントロール リスト オブジェクトの作成 （70 ページ）
- アクセス ルールのアドレス要件およびルールの展開方法について
- ポリシー オブジェクトの作成 （13 ページ）
- ネットワーク/ホストオブジェクトについて （105 ページ）
- 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 （132 ページ）

ステップ 1 **[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）]** を選択して [Policy Object Manager] を開きます（ Policy Object Manager （4 ページ）を参照）。

ステップ 2 オブジェクトタイプセレクタから [アクセスコントロールリスト（Access Control Lists）] を選択します。

[Access Control List] ページが表示されます。デフォルトで [拡張（Extended）] タブが表示されます。

ステップ 3 作業領域内で右クリックし、[新規オブジェクト（New Object）] を選択します。

[Add Extended Access List] ダイアログボックスが表示されます（ [Add Access List]/[Edit Access List] ダイアログボックス （79 ページ）を参照）。

ステップ 4 オブジェクトの名前を入力し、任意でオブジェクトの説明を入力します。

（注） ACL オブジェクトの名前が一意であり、ファイアウォール ACL 設定で定義されたファイアウォール ルール ACL と同じ名前でないことを確認してください。詳細については、[Firewall ACL Setting] ダイアログボックスを参照してください。

ステップ 5 ダイアログボックスのテーブル内で右クリックし、[追加（Add）] を選択します。

[Add Extended Access Control Entry] ダイアログボックスが表示されます。

ステップ 6 アクセス コントロール エントリを作成します。

- [タイプ（Type）] で [アクセスコントロールエントリ（Access Control Entry）] を選択した場合は、照合するトラフィックの特性とトラフィックを許可または拒否するかを指定します。トラフィックが発生する送信元アドレス、トラフィックが到達する宛先アドレス、およびトラフィックの特性を定義す

るサービスを入力します。[詳細設定（Advanced）] をクリックして、ロギングオプションを定義します。ダイアログボックスのフィールドの詳細については、[Add Extended Access Control Entry]/[Edit Extended Access Control Entry] ダイアログボックス （81 ページ）を参照してください。

- [ACLオブジェクト（ACL Object）] を選択した場合は、使用可能なオブジェクトのリストでオブジェクトを選択し、[>>] をクリックしてそのオブジェクトを選択されたオブジェクトのリストに追加します。

ステップ 7 [OK] をクリックして変更を保存します。

ダイアログボックスが閉じ、[Add Extended Access List] ページに戻ります。新しいエントリがテーブルに表示されます。必要に応じて、そのエントリを選択し、上下ボタンをクリックして目的の位置に移動します。

ステップ 8 （任意）[Category] の下で、[Objects] テーブルでこのオブジェクトを識別するために使用するカテゴリを選択します。カテゴリ オブジェクトの使用 （18 ページ）を参照してください。

ステップ 9 [OK] をクリックしてオブジェクトを保存します。

標準アクセス コントロール リスト オブジェクトの作成

標準アクセス コントロール リストを使用すると、特定の IP アドレスからのトラフィックを許可または拒否できます。パケットの宛先と関連するポートは任意です。標準 IP ACL の範囲は 1 ～ 99 です。

標準 ACL の例：

```
access-list 10 permit 192.168.2.0 0.0.0.255
```

用途：

- OSPF ルート再配布の識別。
- SNMP を使用するコミュニティ ストリングのユーザのフィルタリング。
- Catalyst 6500/7600 デバイスの VLAN ACL の設定。

関連項目

- アクセス コントロール リスト オブジェクトの作成 （70 ページ）
- アクセス ルールのアドレス要件およびルールの展開方法について
- ポリシー オブジェクトの作成 （13 ページ）
- ネットワーク/ホストオブジェクトについて （105 ページ）

ステップ 1 **[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）]** を選択して [Policy Object Manager] を開きます（Policy Object Manager （4 ページ）を参照）。

ステップ 2 オブジェクトタイプセレクタから [アクセスコントロールリスト（Access Control Lists）] を選択します。

[Access Control List] ページが表示されます。

ステップ 3 [標準（Standard）] タブをクリックします。

ステップ 4 作業領域内で右クリックし、[新規オブジェクト（New Object）] を選択します。

[Add Standard Access List] ダイアログボックスが表示されます（[Add Access List]/[Edit Access List] ダイアログボックス （79 ページ）を参照）。

ステップ 5 オブジェクトの名前を入力し、任意でオブジェクトの説明を入力します。

（注） ACL オブジェクトの名前が一意であり、ファイアウォール ACL 設定で定義されたファイアウォール ルール ACL と同じ名前でないことを確認してください。詳細については、[Firewall ACL Setting] ダイアログボックスを参照してください。

ステップ 6 テーブル内で右クリックし、[追加（Add）] を選択します。

[Add Standard Access Control Entry] ダイアログボックスが表示されます。

ステップ 7 アクセス コントロール エントリを作成します。

- [タイプ（Type）] で [アクセスコントロールエントリ（Access Control Entry）] を選択した場合は、照合するトラフィックの特性とトラフィックを許可または拒否するかを指定します。トラフィックが発生する送信元アドレスを入力し、ロギング オプションを選択します。ダイアログボックスのフィールドの詳細については、[Add Standard Access Control Entry]/[Edit Standard Access Control Entry] ダイアログボックス （84 ページ）を参照してください。
- [ACL オブジェクト（ACL Object）] を選択した場合は、使用可能なオブジェクトのリストでオブジェクトを選択し、[>>] をクリックしてそのオブジェクトを選択されたオブジェクトのリストに追加します。

ステップ 8 [OK] をクリックして変更を保存します。

ダイアログボックスが閉じ、[Add Standard Access List] ダイアログボックスに戻ります。新しいエントリがテーブルに表示されます。必要に応じて、そのエントリを選択し、上下ボタンをクリックして目的の位置に移動します。

ステップ 9 （任意）[Category] の下で、[Objects] テーブルでこのオブジェクトを識別するために使用するカテゴリを選択します。カテゴリ オブジェクトの使用 （18 ページ）を参照してください。

ステップ 10 [OK] をクリックしてオブジェクトを保存します。

Web アクセス コントロール リスト オブジェクトの作成

Web ACL（WebVPN とも呼ばれる）を使用すると、Web ブラウザを使用して、セキュリティ アプライアンスへのセキュアなリモート アクセス VPN トンネルを確立できます。ソフトウェアまたはハードウェア クライアントは必要ありません。WebVPN によって、幅広い Web リソースや、Web 対応アプリケーションとレガシー アプリケーションの両方に、HTTPS インターネット サイトに到達できるほとんどのコンピュータから簡単にアクセスできます。WebVPN では、Secure Socket Layer プロトコルとその後継である Transport Layer Security（SSL/TLS1）を

使用して、リモートユーザーと、セントラルサイトで設定した特定のサポート対象内部リソース間のセキュアな接続が提供されます。

次の表に、Web VPN ACL の例を示します。

表 *19 : Web VPN ACL* の例

Action	フィルタ	影響
拒否	url http://*.yahoo.com/	Yahoo! すべてへのアクセスを拒否します。
拒否	url cifs://fileserver/share/directory	指定された場所にあるすべてのファイルへのアクセスを拒否します。
拒否	url https://www.company.com/directory/file.html	指定されたファイルへのアクセスを拒否します。
許可	url https://www.company.com/directory	指定された場所へのアクセスを許可します。
拒否	url http://*:8080/	ポート 8080 を介した任意の場所への HTTPS アクセスを拒否します。
拒否	url http://10.10.10.10	10.10.10.10 への HTTP アクセスを拒否します。
許可	url any	任意の URL へのアクセスを許可します。通常は、url アクセスを拒否する ACL のあとに使用されます。

用途：

- ASA ユーザ グループ ポリシー オブジェクトのフィルタ ACL として（[SSL VPN] > [Clientless]）。

関連項目

- アクセス コントロール リスト オブジェクトの作成 （70 ページ）
- アクセス ルールのアドレス要件およびルールの展開方法について
- ポリシー オブジェクトの作成 （13 ページ）

ステップ 1 **[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）]** を選択して [Policy Object Manager] を開きます（ Policy Object Manager （4 ページ）を参照）。

ステップ 2 オブジェクトタイプセレクタから [アクセスコントロールリスト（Access Control Lists）] を選択します。

[Access Control List] ページが表示されます。

ステップ 3 [Web] タブをクリックします。

ステップ 4 作業領域内で右クリックし、[新規オブジェクト（New Object）] を選択します。

[Add WebType Access List] ダイアログボックスが表示されます（ [Add Access List]/[Edit Access List] ダイアログボックス （79 ページ）を参照）。

ステップ 5 オブジェクトの名前を入力し、任意でオブジェクトの説明を入力します。

（注） ACL オブジェクトの名前が一意であり、ファイアウォール ACL 設定で定義されたファイアウォール ルール ACL と同じ名前でないことを確認してください。詳細については、[Firewall ACL Setting] ダイアログボックスを参照してください。

ステップ 6 アクセス コントロール エントリ テーブル内で右クリックし、[追加（Add）] を選択します。

[Add Web Access Control Entry] ダイアログボックスが表示されます。

ステップ 7 アクセス コントロール エントリを作成します。

- [タイプ（Type）] で [アクセスコントロールエントリ（Access Control Entry）] を選択した場合は、照合するトラフィックの特性とトラフィックを許可または拒否するかを指定します。トラフィックのネットワーク宛先（ネットワーク フィルタ）または Web アドレス（URL フィルタ）に基づいてフィルタリングできます。ダイアログボックスのフィールドの詳細については、[Add Web Access Control Entry]/[Edit Web Access Control Entry] ダイアログボックス （86 ページ）を参照してください。
- [ACL オブジェクト（ACL Object）] を選択した場合は、使用可能なオブジェクトのリストでオブジェクトを選択し、[>>] をクリックしてそのオブジェクトを選択されたオブジェクトのリストに追加します。

ステップ 8 [OK] をクリックして変更を保存します。

ダイアログボックスが閉じ、[Add WebType Access List] ページに戻ります。新しいエントリがテーブルに表示されます。必要に応じて、そのエントリを選択し、上下ボタンをクリックして目的の位置に移動します。

ステップ 9 （任意）[Category] の下で、[Objects] テーブルでこのオブジェクトを識別するために使用するカテゴリを選択します。 カテゴリ オブジェクトの使用 （18 ページ）を参照してください。

ステップ 10 [OK] をクリックしてオブジェクトを保存します。

統合アクセス制御リストオブジェクトの作成

統合アクセス制御リストを使用すると、特定のネットワーク、ホスト、セキュリティグループ、およびユーザーからの、特定のネットワーク、ホスト、およびセキュリティグループ宛てのトラフィックを許可または拒否できます。関連するサービスも指定します。

関連項目

- アクセス コントロール リスト オブジェクトの作成 （70 ページ）
- アクセス ルールのアドレス要件およびルールの展開方法について
- ポリシー オブジェクトの作成 （13 ページ）
- ネットワーク/ホストオブジェクトについて （105 ページ）

ステップ 1 [管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択して [Policy Object Manager] を開きます（Policy Object Manager （4 ページ）を参照）。

ステップ 2 オブジェクトタイプセレクタから [アクセス制御リスト（Access Control Lists）] を選択します。

[Access Control List] ページが表示されます。

ステップ 3 [統合（Unified）] タブをクリックします。

ステップ 4 作業領域内で右クリックし、[新規オブジェクト（New Object）] を選択します。

[拡張アクセスリストの追加（Add Extended Access List）] ダイアログボックスが表示されます（[Add Access List]/[Edit Access List] ダイアログボックス （79 ページ）を参照）。

ステップ 5 オブジェクトの名前を入力し、任意でオブジェクトの説明を入力します。

（注） ACL オブジェクトの名前が一意であり、ファイアウォール ACL 設定で定義されたファイアウォール ルール ACL と同じ名前でないことを確認してください。詳細については、[Firewall ACL Setting] ダイアログボックスを参照してください。

ステップ 6 ダイアログボックスのテーブル内で右クリックし、[追加（Add）] を選択します。

[統合アクセス制御エントリの追加（Add Unified Access Control Entry）] ダイアログボックスが表示されます。

ステップ 7 アクセス コントロール エントリを作成します。

- [タイプ（Type）] で [アクセス制御エントリ（Access Control Entry）] を選択した場合は、照合するトラフィックの特性とトラフィックを許可または拒否するかを指定します。トラフィックが発生する送信元アドレスを入力し、ロギング オプションを選択します。ダイアログボックスのフィールドの詳細については、[Webアクセスコントロールエントリの追加（Add Web Access Control Entry）]/[Webアクセスコントロールエントリの編集（Edit Web Access Control Entry）] ダイアログボックス （89 ページ）を参照してください。
- [ACL オブジェクト（ACL Object）] を選択した場合は、使用可能なオブジェクトのリストでオブジェクトを選択し、[>>] をクリックしてそのオブジェクトを選択されたオブジェクトのリストに追加します。

ステップ 8 [OK] をクリックして変更を保存します。

ダイアログボックスが閉じ、[標準アクセスリストの追加（Add Standard Access List）] ダイアログボックスに戻ります。新しいエントリがテーブルに表示されます。必要に応じて、そのエントリを選択し、上下ボタンをクリックして目的の位置に移動します。

ステップ 9 （任意）[Category] の下で、[Objects] テーブルでこのオブジェクトを識別するために使用するカテゴリを選択します。カテゴリ オブジェクトの使用 （18 ページ）を参照してください。

ステップ 10 [OK] をクリックしてオブジェクトを保存します。

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

[Add Access List]/[Edit Access List] ダイアログボックスを使用して、ACL オブジェクトのアクセス コントロール エントリ（ACE）を定義します。このページから、テーブル内の ACE と ACL オブジェクトの順序の変更、ACE と ACL オブジェクトの追加、編集、削除を行うことができます。

ダイアログボックスのタイトルは、作成する ACL のタイプ（拡張、標準、または Web タイプ）を示します。ダイアログボックスは基本的には同じであり、ACEテーブルに表示されるカラムだけが異なります。

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、次にオブジェクトタイプセレクタから [アクセス制御リスト（Access Control Lists）] を選択します。作成する ACL オブジェクトのタイプのタブを選択し、作業領域内で右クリックして [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 [オブジェクトの編集（Edit Object）] を選択します。

関連項目

- アクセス コントロール リスト オブジェクトの作成 （70 ページ）
- 拡張アクセス コントロール リスト オブジェクトの作成 （71 ページ）
- 標準アクセス コントロール リスト オブジェクトの作成 （74 ページ）
- Web アクセス コントロール リスト オブジェクトの作成 （75 ページ）
- ネットワーク/ホストオブジェクトについて （105 ページ）
- 連続および不連続ネットワーク マスク（IPv4 アドレスに対応） （107 ページ）
- 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 （132 ページ）

フィールド リファレンス

表 20 : [Add Access List]/[Edit Access List] ダイアログボックス

要素	説明
名前	最大 128 文字のオブジェクト名。オブジェクト名では、大文字と小文字が区別されません。詳細については、 ポリシー オブジェクトの作成 （13 ページ）を参照してください。
説明	（任意）オブジェクトの説明。

要素	説明

Access Control Entry table	ACL の一部であるアクセス コントロール エントリ（ACE）および ACL オブジェクト。テーブルには、エントリまたはオブジェクトの名前、説明、オプション、サービス、およびエントリのその他の属性が表示されます。
	
	[Permit] カラムで、緑色のチェックマークはエントリがトラフィックを許可することを示し（通常、トラフィックは定義しているサービスについて一致と見なされます）、スラッシュの入った赤色の丸はトラフィックが拒否されることを示します（通常、トラフィックは不一致と見なされ、定義しているサービスは拒否されたトラフィックには適用されません）。
	
	送信元アドレスおよび（該当する場合）宛先アドレスは、ホスト IP アドレス、ネットワーク アドレス、またはネットワーク/ホスト ポリシー オブジェクトです。
	
	• ACE を追加するには、[Add] ボタンをクリックし、作成するタイプの ACL のダイアログボックスに入力を行います。
	  • [Add Extended Access Control Entry]/[Edit Extended Access Control Entry] ダイアログボックス （81 ページ）
	  • [Add Standard Access Control Entry]/[Edit Standard Access Control Entry] ダイアログボックス （84 ページ）
	  • [Add Web Access Control Entry]/[Edit Web Access Control Entry] ダイアログボックス （86 ページ）
	
	• ACE を編集するには、ACE を選択し、[Edit] ボタンをクリックします。
	
	• ACE を削除するには、ACE を選択し、[Delete] ボタンをクリックします。
	
	• エントリの位置を変更するには、エントリを選択し、必要に応じて上下の矢印ボタンをクリックします。エントリは上から下へ評価されるため、正しく位置付けることが意図した結果を得るために重要です。

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（18 ページ）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 （25 ページ）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 （24 ページ）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。

[Add Extended Access Control Entry]/[Edit Extended Access Control Entry] ダイアログボックス

[Add Extended Access Control Entry]/[Edit Extended Access Control Entry] ダイアログボックスを使用して、アクセス コントロール エントリ（ACE）または ACL オブジェクトを拡張 ACL オブジェクトに追加します。

ナビゲーション パス

拡張 ACL オブジェクトの [Add Access List]/[Edit Access List] ダイアログボックス （79 ページ）から、ACE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。

関連項目

- 拡張アクセス コントロール リスト オブジェクトの作成 （71 ページ）
- アクセス ルールのアドレス要件およびルールの展開方法について
- ネットワーク/ホストオブジェクトについて （105 ページ）
- 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 （132 ページ）
- セレクタ内の項目のフィルタリング

フィールド リファレンス

表 21 : [Add Extended Access Control Entry]/[Edit Extended Access Control Entry] ダイアログボックス

要素	説明
タイプ	追加するエントリのタイプ。ダイアログボックスのフィールドは、選択に応じて変わります。 • [Access Control Entry]：ACE を定義します。 • [ACL Objects]：既存の ACL オブジェクトを追加します。使用可能な ACL オブジェクトのリストが表示されます。追加するオブジェクトを選択し、[>>]ボタンをクリックして選択されたオブジェクトリストに移動します。オブジェクトを削除するには、オブジェクトを選択して[<<]をクリックします。選択されたオブジェクト リスト内のオブジェクトを編集することもできます。

要素	説明
操作	エントリで定義されトラフィックに対するアクション： • [Permit]：この ACL に関連付けられているサービスはこのトラフィックに適用されます。つまり、トラフィックはサービスの使用が許可されます。 • [Deny]：この ACL に関連付けられているサービスはこのトラフィックに適用されません。サービスに複数の ACL が設定されている場合、拒否されたトラフィックは、通常はリスト内の次の ACL と比較されます。そのトラフィックが ACL 内の permit エントリと一致しない場合、サービスはトラフィックに適用されません。トラフィックがネットワークからドロップされるかどうかは、サービスによって決まります。
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 （18 ページ）を参照してください。
送信元 接続先	トラフィックの送信元または宛先。項目をカンマで区切って複数の値を入力できます。 次のアドレス タイプを組み合わせて入力できます。詳細については、ポリシー定義中の IP アドレスの指定 （115 ページ）を参照してください。 • ネットワーク/ホスト オブジェクト。オブジェクトの名前を入力するか、または [選択（Select）] をクリックしてリストから名前を選択します。選択リストから、新しいネットワーク/ホスト オブジェクトを作成することもできます。 （ASA 8.4(2) 以降のみ）FQDN ネットワーク/ホストオブジェクトを選択して、完全修飾ホスト名に基づいてトラフィックを選択できます。 • ホスト IP アドレス（10.10.10.100 など）。 • ネットワーク アドレスとサブネット マスク。形式は 10.10.10.0/24 または 10.10.10.0/255.255.255.0。 • IP アドレスの範囲（10.10.10.100-10.10.10.200 など）。 • 10.10.0.10/255.255.0.255 形式の IP アドレスのパターン。この場合のマスクは不連続なビット マスクです（連続および不連続ネットワーク マスク（IPv4 アドレスに対応） （107 ページ）を参照）。

要素	説明
Users	（ASA 8.4(2) 以降のみ）ルールの Active Directory（AD）ユーザー名、ユーザー グループ、またはアイデンティティ ユーザー グループ オブジェクト（使用する場合）。ユーザ指定は送信元アドレスと結合され、送信元アドレス範囲の中で照合するユーザ アドレスを制限します。項目をカンマで区切って複数の値を入力できます。 次の値を組み合わせて入力できます。 • 個別のユーザ名：NetBIOS_DOMAIN\username • ユーザ グループ（\ を二重にします）：NetBIOS_DOMAIN\\user_group • アイデンティティ ユーザ グループ オブジェクト名。 [選択（Select）] をクリックしてリストからオブジェクト、ユーザー、またはユーザーグループを選択するか、新しいオブジェクトを作成します。 詳細については、以下を参照してください。 • ポリシーでのアイデンティティ ユーザの選択 • アイデンティティ ベースのファイアウォール ルールの設定 • アイデンティティ ユーザ グループ オブジェクトの作成
サービス	動作対象のトラフィック タイプを定義するサービス。項目をカンマで区切って複数の値を入力できます。 サービス オブジェクトおよびサービス タイプの任意の組み合わせ（通常はプロトコルとポートの組み合わせ）を入力できます。サービスを入力する場合は、有効な値の入力を求められます。リストから値を選択して、Enter または Tab を押します。 サービスを指定する方法の詳細については、サービスとサービス オブジェクトおよびポート リスト オブジェクトの理解と指定 （132 ページ）を参照してください。
説明	（任意）オブジェクトの説明。

要素	説明
[Advanced] ボタン	このボタンをクリックして、エントリのロギング オプションを定義します。 • PIX、ASA、および FWSM デバイスの場合、次の項目をイネーブルにすることができます。 • [Default logging]：パケットが拒否されると、メッセージ 106023 が生成されます。パケットが許可された場合、メッセージは生成されません。 • [Per ACE logging]：パケットが拒否されると、メッセージ 106100 が生成されます。メッセージのロギング重大度レベルおよびメッセージを生成する間隔（1 ～ 600 秒）を選択できます。 • IOS デバイスの場合、ロギングをイネーブルにすると、エントリと一致したパケットに関する情報メッセージがコンソールに送信されます。入力インターフェイスおよび送信元 MAC アドレスまたは VC をロギング出力に含めるように選択することもできます。

[Add Standard Access Control Entry]/[Edit Standard Access Control Entry] ダイアログボックス

[Add Standard Access Control Entry]/[Edit Standard Access Control Entry] ダイアログボックスを使用して、アクセス コントロール エントリ（ACE）または ACL オブジェクトを標準 ACL オブジェクトに追加します。

ナビゲーション パス

標準 ACL オブジェクトの [Add Access List]/[Edit Access List] ダイアログボックス （79 ページ）から、ACE 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。

関連項目

- 標準アクセス コントロール リスト オブジェクトの作成 （74 ページ）
- アクセス ルールのアドレス要件およびルールの展開方法について
- ネットワーク/ホストオブジェクトについて （105 ページ）
- 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 （132 ページ）
- セレクタ内の項目のフィルタリング

フィールド リファレンス

表 *22 : [Add Standard Access Control Entry]/[Edit Standard Access Control Entry]* ダイアログボックス

要素	説明
タイプ	追加するエントリのタイプ。ダイアログボックスのフィールドは、選択に応じて変わります。 • [Access Control Entry]：ACE を定義します。 • [ACL Objects]：既存の ACL オブジェクトを追加します。使用可能な ACL オブジェクトのリストが表示されます。追加するオブジェクトを選択し、[>>] ボタンをクリックして選択されたオブジェクトリストに移動します。オブジェクトを削除するには、オブジェクトを選択して [<<] をクリックします。選択されたオブジェクト リスト内のオブジェクトを編集することもできます。
操作	エントリで定義されトラフィックに対するアクション： • [Permit]：この ACL に関連付けられているサービスはこのトラフィックに適用されます。つまり、トラフィックはサービスの使用が許可されます。 • [Deny]：この ACL に関連付けられているサービスはこのトラフィックに適用されません。サービスに複数の ACL が設定されている場合、拒否されたトラフィックは、通常はリスト内の次の ACL と比較されます。そのトラフィックが ACL 内の permit エントリと一致しない場合、サービスはトラフィックに適用されません。トラフィックがネットワークからドロップされるかどうかは、サービスによって決まります。
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 （18 ページ）を参照してください。

要素	説明
ソース（Source）	トラフィックの送信元。項目をカンマで区切って複数の値を入力できます。 次のアドレス タイプを組み合わせて入力できます。詳細については、ポリシー定義中の IP アドレスの指定 （115 ページ）を参照してください。 • ネットワーク/ホスト オブジェクト。オブジェクトの名前を入力するか、または [選択（Select）] をクリックしてリストから名前を選択します。選択リストから、新しいネットワーク/ホスト オブジェクトを作成することもできます。 • ホスト IP アドレス（10.10.10.100 など）。 • ネットワーク アドレスとサブネット マスク。形式は 10.10.10.0/24 または 10.10.10.0/255.255.255.0。 • IP アドレスの範囲（10.10.10.100-10.10.10.200 など）。 • 10.10.0.10/255.255.0.255 形式の IP アドレスのパターン。この場合のマスクは不連続なビットマスクです（連続および不連続ネットワーク マスク（IPv4 アドレスに対応） （107 ページ）を参照）。
説明	（任意）オブジェクトの説明。
Log Option	トラフィックがエントリ基準を満たしたときにログ エントリを作成するかどうか。ACL ロギングによって、拒否されたパケットに対して syslog メッセージ 106023 が生成されます。拒否されたパケットをログに記録するには、拒否パケットが存在している必要があります。

[Add Web Access Control Entry]/[Edit Web Access Control Entry] ダイアログボックス

[Add Web Access Control Entry]/[Edit Web Access Control Entry] ダイアログボックスを使用して、アクセス コントロール エントリ（ACE）または ACL オブジェクトを Web タイプ ACL オブジェクトに追加します。

ナビゲーション パス

Web タイプ ACL オブジェクトの [Add Access List]/[Edit Access List] ダイアログボックス （79 ページ）から、ACE 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。

関連項目

- Web アクセス コントロール リスト オブジェクトの作成 （75 ページ）
- アクセス ルールのアドレス要件およびルールの展開方法について
- ネットワーク/ホストオブジェクトについて （105 ページ）

- 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 （132 ページ）
- セレクタ内の項目のフィルタリング

フィールド リファレンス

表 23 : [Add Web Access Control Entry]/[Edit Web Access Control Entry] ダイアログボックス

要素	説明
タイプ	追加するエントリのタイプ。ダイアログボックスのフィールドは、選択に応じて変わります。 • [Access Control Entry]：ACE を定義します。 • [ACL Objects]：既存の ACL オブジェクトを追加します。使用可能な ACL オブジェクトのリストが表示されます。追加するオブジェクトを選択し、[>>] ボタンをクリックして選択されたオブジェクトリストに移動します。オブジェクトを削除するには、オブジェクトを選択して [<<] をクリックします。選択されたオブジェクト リスト内のオブジェクトを編集することもできます。
操作	エントリで定義されトラフィックに対するアクション： • [Permit]：この ACL に関連付けられているサービスはこのトラフィックに適用されます。つまり、トラフィックはサービスの使用が許可されます。 • [Deny]：この ACL に関連付けられているサービスはこのトラフィックに適用されません。サービスに複数の ACL が設定されている場合、拒否されたトラフィックは、通常はリスト内の次の ACL と比較されます。そのトラフィックが ACL 内の permit エントリと一致しない場合、サービスはトラフィックに適用されません。トラフィックがネットワークからドロップされるかどうかは、サービスによって決まります。
Filter Destination	エントリがネットワーク フィルタ（ホストまたはネットワーク アドレス）を指定するか、URL フィルタ（Web サイト アドレス）を指定するか。ダイアログボックスのフィールドは、選択に応じて変わります。そのフィールドについては次で説明します。

要素	説明
[接続先（Destination）] （ネットワーク フィルタだけ）	トラフィックの宛先。項目をカンマで区切って複数の値を入力できます。 次のアドレス タイプを組み合わせて入力できます。詳細については、ポリシー定義中の IP アドレスの指定 （115 ページ）を参照してください。 • ネットワーク/ホスト オブジェクト。オブジェクトの名前を入力するか、または [選択（Select）] をクリックしてリストから名前を選択します。選択リストから、新しいネットワーク/ホスト オブジェクトを作成することもできます。 • ホスト IP アドレス（10.10.10.100 など）。 • ネットワーク アドレスとサブネット マスク。形式は 10.10.10.0/24 または 10.10.10.0/255.255.255.0。 • IP アドレスの範囲（10.10.10.100-10.10.10.200 など）。 • 10.10.0.10/255.255.0.255 形式の IP アドレスのパターン。この場合のマスクは不連続なビット マスクです（連続および不連続ネットワーク マスク（IPv4 アドレスに対応） （107 ページ）を参照）。
ポート （ネットワーク フィルタだけ）	トラフィックが使用するポートを定義するポート番号またはポート リスト ポリシー オブジェクト（ポート ID を使用する場合）。項目をカンマで区切って複数の値を入力できます。 次のタイプを組み合わせて入力できます。 • ポート リスト オブジェクト。オブジェクトの名前を入力するか、または [選択（Select）] をクリックしてリストから名前を選択します。選択リストから、新しいポート リスト オブジェクトを作成することもできます。 • ポート番号。80 など。 • ポート範囲。80 ～ 90 など。
URL Filter （URL フィルタだけ）	トラフィックの Universal Resource Locator（URL）つまり Web アドレス。すべての値と一致するワイルドカードとして、アスタリスクを使用できます。たとえば、http://*.cisco.com は、cisco.com ネットワーク上のすべてのサーバと一致します。任意の有効な URL を指定できます。
ログ	このエントリに対して使用するロギングのタイプ。 • ログ エントリを作成しない場合は、[Log Disabled] を選択します。 • デバイスのデフォルト設定を使用する場合は、[Default] を選択します。 • 使用可能なその他のすべてのオプションでは、ロギングがイネーブルになり、使用されるログ レベルが指定されます。

要素	説明
ロギング間隔（Logging Interval）	ロギング メッセージの生成に使用される間隔（秒単位）。1～600。デフォルトは 300 です。このフィールドは、[Logging] フィールドでロギング レベルを選択した場合にだけ変更できます。
時間範囲	エントリに関連付けられる時間範囲を定義する時間範囲ポリシー オブジェクト。時間範囲によってデバイスへのアクセスが定義されます。時間範囲は、デバイスのシステムクロックによって異なります。詳細については、時間範囲オブジェクトの設定 （93 ページ）を参照してください。 オブジェクトの名前を入力するか、または [選択（Select）] をクリックしてリストから名前を選択します。選択リストから、新しい時間範囲オブジェクトを作成することもできます。 （注） 時間範囲は、FWSM 2.x デバイスまたは PIX 6.3 デバイスではサポートされていません。
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（18 ページ）を参照してください。
説明	（任意）オブジェクトの説明。

[Webアクセスコントロールエントリの追加（Add Web Access Control Entry）]/[Webアクセスコントロールエントリの編集（Edit Web Access Control Entry）] ダイアログボックス

[ユニファイドアクセスコントロールエントリの追加（Add Unified Access Control Entry）]/[ユニファイドアクセスコントロールエントリの編集（Edit Unified Access Control Entry）] ダイアログボックスを使用して、アクセス コントロール エントリ（ACE）または ACL オブジェクトをユニファイド ACL オブジェクトに追加します。

ナビゲーション パス

拡張 ACL オブジェクトの [Add Access List]/[Edit Access List] ダイアログボックス （79 ページ）から、ACE 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。

関連項目

- 統合アクセス制御リストオブジェクトの作成 （77 ページ）
- アクセス ルールのアドレス要件およびルールの展開方法について
- ネットワーク/ホストオブジェクトについて （105 ページ）
- 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 （132 ページ）

- セレクタ内の項目のフィルタリング

フィールド リファレンス

表 *24 : [Webアクセスコントロールエントリの追加（Add Web Access Control Entry）]/[Webアクセスコントロールエントリの編集（Edit Web Access Control Entry）] ダイアログボックス*

要素	説明
タイプ	エントリのタイプ。ダイアログボックスのフィールドは、選択した項目に応じて変化します。 • [Access Control Entry]：ACE を定義します。 • [ACLオブジェクト（ACL Objects）]：1 つ以上の既存の ACL オブジェクトを追加します。使用可能な ACL オブジェクトのリストが表示されます。追加するオブジェクトを選択し、[>>] ボタンをクリックして選択されたオブジェクトリストに移動します。オブジェクトを削除するには、オブジェクトを選択して [<<] をクリックします。選択されたオブジェクトリスト内のオブジェクトを編集することもできます。
操作	エントリで定義されトラフィックに対するアクション： • [許可（Permit）]：ACEに関連付けられているサービスはこのトラフィックに適用されます。つまり、このエントリで定義されたトラフィックはサービスの使用が許可されます。 • [拒否（Deny）]：ACE に関連付けられているサービスはこのトラフィックに適用されません。サービスに複数のACLが設定されている場合、拒否されたトラフィックは、通常はリスト内の次のACEと比較されます。そのトラフィックがACL内の許可エントリと一致しない場合、サービスはトラフィックに適用されません。トラフィックがネットワークからドロップされるかどうかは、サービスによって決まります。

要素	説明
ソース	このルールのトラフィックソースを指定します。ネットワークとホストを指定できます。次の1つ以上に対して、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/ホスト（Networks/Hosts）]：さまざまなネットワーク、ホスト、およびインターフェイスの定義を、個別に、またはオブジェクトとして指定できます。インターフェイスオブジェクトをソースとして選択した場合、ダイアログボックスにタブが表示され、ホスト/ネットワークとインターフェイスが区別されます。これらのフィールドのいずれかに、項目をカンマで区切るか範囲を指定して、複数の値を入力します。 「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） （ASA 8.4.2 以降のみ）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入力することによってのみ指定できます。FQDN を直接入力することはできません。 これらの定義の詳細については、 ネットワーク/ホストオブジェクトについて （105 ページ）、ポリシー定義中の IP アドレスの指定 （115 ページ）およびインターフェイス ロール オブジェクトについて （95 ページ）を参照してください。 （注） IPv6アドレスは、コンマ区切りの値のみで入力してください。IPv6アドレスが範囲として指定されている場合、設定のプレビューでエラーが表示されます。 すべての送信元、送信元SG、およびユーザの指定領域を組み合わせて、トラフィックの一致をすべてのソース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。
送信元SG（Source SG）	（ASA 9.0 以降のみ）ACE の 1 つ以上の送信元セキュリティグループの名前またはタグ番号を入力または選択します（存在する場合）。セキュリティグループの詳細については、次を参照してください。 • ポリシーでのセキュリティグループの選択 • TrustSec ベースのファイアウォールルールの設定 • セキュリティ グループ オブジェクトの作成

要素	説明
Users	（ASA 8.4.2 以降のみ）ACE の Active Directory（AD）ユーザ名、ユーザグループ、またはアイデンティティ ユーザ グループ オブジェクトを入力するか選択します（存在する場合）。ユーザ指定は送信元アドレスと結合され、送信元アドレス範囲の中で照合するユーザ アドレスを制限します。項目をカンマで区切って複数の値を入力できます。 次の値の任意の組み合わせを入力できます。 • 個別のユーザ名：NetBIOS_DOMAIN\username • ユーザ グループ（\ を二重にします）：NetBIOS_DOMAIN\\user_group • アイデンティティ ユーザ グループ オブジェクト名。 詳細については、以下を参照してください。 • ポリシーでのアイデンティティ ユーザの選択 • アイデンティティ ベースのファイアウォール ルールの設定 • アイデンティティ ユーザ グループ オブジェクトの作成
[接続先（Destination）]	トラフィックの送信元または宛先。項目をカンマで区切って複数の値を入力できます。 （注） IPv6アドレスは、コンマ区切りの値のみで入力してください。IPv6アドレスが範囲として指定されている場合、設定のプレビューでエラーが表示されます。 この ACE のトラフィックの宛先、およびオプションで宛先セキュリティ グループ（ASA 9.0 以降のみ）を提供します。送信元エントリと同様に、次の 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。
宛先SG（Destination SG）	（ASA 9.0 以降のみ）ACE の 1 つ以上の送信元セキュリティグループの名前またはタグ番号を入力または選択します（存在する場合）。セキュリティグループの詳細については、次を参照してください。 • ポリシーでのセキュリティグループの選択 • TrustSec ベースのファイアウォールルールの設定 • セキュリティ グループ オブジェクトの作成

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。項目をカンマで区切って複数の値を入力できます。 サービスオブジェクトおよびサービスタイプの任意の組み合わせ（通常はプロトコルとポートの組み合わせ）を入力するか選択できます。サービスを入力する場合は、有効な値の入力を求められます。 サービスを指定する方法の詳細については、サービスとサービス オブジェクトおよびポート リスト オブジェクトの理解と指定 （132 ページ）を参照してください。
[Advanced] ボタン	このボタンをクリックして [詳細設定（Advanced）] ダイアログボックスを開き、ACE のログオプションを定義します。PIX、ASA、および FWSM デバイスの場合、次の項目をイネーブルにすることができます。 • [Default logging]：パケットが拒否されると、メッセージ 106023 が生成されます。パケットが許可された場合、メッセージは生成されません。 • [Per ACE logging]：パケットが拒否されると、メッセージ 106100 が生成されます。メッセージのロギング重大度レベルおよびメッセージを生成する間隔（1 ～ 600 秒）を選択できます。
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 （18 ページ）を参照してください。
説明	（任意）オブジェクトの説明。

時間範囲オブジェクトの設定

[Add Time Range]/[Edit Time Range] ダイアログボックスを使用して、時間範囲オブジェクトを作成、編集、またはコピーします。

時間ベースの ACL および一部のファイアウォール ルールを作成するときに使用する時間範囲オブジェクトを作成できます。機能は拡張 ACL と同様ですが、時間ベースの ACL では時間を考慮したアクセス コントロールが可能です。時間範囲が特定のルールに適用され、それらのルールは範囲で定義された特定の時間アクティブになります。たとえば、特定のタイプのアクセスを許可または阻止する通常の勤務時間のルールを実装できます。

また、VPN アクセスを週のうちの特定の時間に制限するように ASA ユーザ グループを定義する場合に、時間範囲オブジェクトを使用できます。詳細については、ASA グループ ポリシーの SSL VPN 設定を参照してください。

時間範囲オブジェクトは、デバイスのシステムクロックに依存させることができますが、ネットワーク タイム プロトコル（NTP）同期を使用すると最適に動作します。

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 [時間範囲（Time Ranges）] を選択します。作業領域内を右クリックして [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 [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 25 : [Time Range] ダイアログボックス

要素	説明
名前	最大 128 文字のオブジェクト名。オブジェクト名では、大文字と小文字が区別されません。詳細については、ポリシー オブジェクトの作成 （13 ページ）を参照してください。
説明	（任意）最大 1024 文字のオブジェクトの説明。
開始時刻（Start Time） 終了時間（End Time）	時間範囲オブジェクトの全体的な開始時刻および終了時刻。 • [Start Now]：展開の時刻を開始時刻として定義します。 • [Never End]：範囲の終了時刻を定義しません。 • [Start At]、[End At]：特定の開始日と開始時刻または終了日と終了時刻を定義します。カレンダー アイコンをクリックして、日付選択用のツールを表示します。24 時間形式（HH:MM）を使用して [Time] フィールドに時刻を入力します。
Recurring Ranges	全体的な開始時刻および終了時刻内で発生する繰り返し期間（ある場合）。たとえば、勤務時間を定義する時間範囲オブジェクトを作成する場合、全体的な範囲については [Start Now] および [Never End] を選択し、平日の 08:00 ～ 18:00 という繰り返し範囲を入力できます。 • 範囲を追加するには、[新しい繰り返し範囲（New Recurring Range）] ボタンをクリックし、[Recurring Ranges] ダイアログボックス （95 ページ）に入力します。 • 範囲を編集するには、その範囲を選択して [繰り返し範囲の編集（Edit Recurring Range）] ボタンをクリックします。 • 範囲を削除するには、その範囲を選択して [繰返し範囲の削除（Delete Recurring Range）] 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 （18 ページ） を参照してください。

[Recurring Ranges] ダイアログボックス

[Recurring Ranges] ダイアログボックスを使用して、時間範囲オブジェクトの一部として定義される繰り返し時間間隔を追加または編集します。必要な数の繰り返し範囲を定義できます。

ナビゲーション パス

[時間範囲の追加（Add Time Range）]/[時間範囲の編集（Edit Time Range）] ダイアログボックスに移動し、[繰り返し範囲（Recurring Ranges）] の下の [新しい繰り返し範囲（New Recurring Range）] ボタンをクリックするか、範囲を選択して [繰り返し範囲の編集（Edit Recurring Range）] をクリックします。時間範囲オブジェクトの設定 （93 ページ）を参照してください。

フィールド リファレンス

表 *26 : [Recurring Ranges]* ダイアログボックス

要素	説明
Specify days of the week and times during which this recurring range will be active	特定の曜日と時間に基づく繰り返し範囲を定義します。次の中から選択できます。 • 毎日 • 平日（Weekdays） • Weekends • [On these days of the week]：範囲に含める特定の日を選択します。 1 日のうちの開始時刻と終了時刻も選択します。デフォルトはすべての日です。
Specify a weekly interval during which this recurring range will be active	毎週の繰り返し範囲を定義します。開始日と開始時刻および終了日と終了時刻を選択します。たとえば、週の期間を日曜日に開始し、木曜日に終了できます。

インターフェイス ロール オブジェクトについて

インターフェイス ロール オブジェクトには次の用途があります。

- 複数のインターフェイスの指定：インターフェイス ロール オブジェクトを使用すると、各インターフェイスの名前を手動で定義することなく、複数のデバイス上の特定のインターフェイスにポリシーを適用できます。ほとんどのデバイスはインターフェイスについて標準的な命名ルールに従っているため、特定のインターフェイス タイプを示す命名パターンを定義し、そのパターンと一致するすべてのインターフェイスにポリシーを適用できます。

- ゾーン：インターフェイス ロール オブジェクトを使用して、ゾーンベースのファイアウォール ルール ポリシーでゾーンを定義できます。

たとえば、DMZ* という命名パターンでインターフェイス ロールを定義します。このインターフェイスロールをポリシーに含めると、そのポリシーは、選択したデバイス上の名前が「DMZ」で始まるすべてのインターフェイスに適用されます。結果として、たとえばすべての DMZ インターフェイスでアンチ スプーフィング チェックを有効にするポリシーを、該当するすべてのデバイス インターフェイスに 1 回のアクションで適用できます。インターフェイス ロールは、デバイス上の実際のインターフェイスのいずれかを参照できます。インターフェイスには、物理インターフェイス、サブインターフェイス、仮想インターフェイス（ループバック インターフェイスなど）があります。

インターフェイス ロールは、一方のインターフェイスと他方のポリシー間の間接エンティティとして機能します。このことにより、割り当てられたロールに基づいて、特定のデバイス インターフェイスにポリシーを適用できます。また、特定のインターフェイス タイプに対して使用されている命名ルールを変更する場合に、どのポリシーが変更を影響を受けるかを判別する必要がありません。インターフェイス ロールを編集するだけで済みます。

インターフェイス ロールは、新しいデバイスにポリシーを適用するときに特に役立ちます。追加するデバイスが既存のデバイスと同じインターフェイス命名方式を共有しているかぎり、追加割り当てを行わなくても、該当するポリシーをそれらに拡張できます。

Security Manager には、次の定義済みのインターフェイス ロールがあります。

- All-Interfaces：特定のデバイスで定義されているすべてのインターフェイスが含まれます。
- Internal：ネットワークの内側にある、特定のインターフェイスだけが含まれます。リストについてはオブジェクト定義を参照してください。
- External：ネットワークの外側にある、特定のインターフェイスだけが含まれます。リストについてはオブジェクト定義を参照してください。
- Self：いずれのインターフェイスも含まれません。Self インターフェイス ロールは、ゾーンベースのファイアウォール ルール ポリシーに固有です。Self ゾーンはルータ自体です。これを使用して、ルータから送信されたトラフィックまたはルータに送信されるトラフィックを識別できます。ルータを通過するトラフィックは含まれません。

次の項では、インターフェイス ロール オブジェクトを操作する方法について説明します。

- インターフェイス ロール オブジェクトの作成 （97 ページ）
- ポリシー定義中のインターフェイスの指定 （100 ページ）
- 単一のインターフェイス指定が許可されている場合のインターフェイス ロールの使用 （101 ページ）
- インターフェイスとインターフェイス ロール間の名前の競合の処理 （102 ページ）
- トラフィック ゾーンの管理

インターフェイス ロール オブジェクトの作成

デバイス上の 1 つ以上のインターフェイスを表すインターフェイス ロール オブジェクトを作成できます。これらのロールは、インターフェイスまたはゾーンを必要とするポリシーを定義するときに使用できます。インターフェイス ロール オブジェクトを作成する場合、オブジェクトに含めるデバイスインターフェイスの命名パターンを定義する必要があります。インターフェイス ロールは、デバイス上の実際のインターフェイスのいずれかを参照できます。インターフェイスには、物理インターフェイス、サブインターフェイス、仮想インターフェイスがあります。

ヒント このオブジェクト タイプを使用するポリシーまたはオブジェクトを定義するときに、インターフェイス ロール オブジェクトを作成することもできます。詳細については、ポリシーのオブジェクトの選択 （2 ページ）を参照してください。

関連項目

- ポリシー オブジェクトの作成 （13 ページ）
- ポリシー定義中のインターフェイスの指定 （100 ページ）
- インターフェイス ロール オブジェクトについて （95 ページ）
- 単一のインターフェイス指定が許可されている場合のインターフェイス ロールの使用 （101 ページ）
- オブジェクト オーバーライドの管理 （23 ページ）
- トラフィック ゾーンの管理

ステップ 1 [管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択して [Policy Object Manager] を開きます（Policy Object Manager （4 ページ）を参照）。

ステップ 2 オブジェクトタイプセレクタから [インターフェイスロール（Interface Roles）] を選択します。

ステップ 3 作業領域内で右クリックし、[新規オブジェクト（New Object）] を選択します。

[Interface Role] ダイアログボックスが表示されます。

ステップ 4 オブジェクトの名前を入力し、任意でオブジェクトの説明を入力します。名前は最大 128 文字、説明は最大 1024 文字です。

ステップ 5 インターフェイス ロール オブジェクトの命名パターンを 1 つ以上入力します。名前は、インターフェイス、サブインターフェイス、およびその他の仮想インターフェイスの完全な名前または名前の一部です。複数の名前パターンを指定する場合は、カンマで区切ります。

次のワイルドカードを使用して、複数のインターフェイスに適用する名前パターンを作成できます。

- ピリオド（.）は、1 文字を表すワイルドカードとして使用します。ピリオドをパターン自体の一部として使用するには、ピリオドの前にバックスラッシュ（\）を入力します。

- アスタリスク（*）は、インターフェイス パターンの末尾にある 1 つ以上の文字を表すワイルドカードとして使用します。

たとえば、**DMZ*** には名前が「DMZ」で始まるすべてのインターフェイスが含まれ、**DMZ.** は DMZ1 や DMZ2 などのインターフェイスには一致しますが、DMZ10 には一致しません。

パターンにワイルドカードが含まれていない場合は、インターフェイスの名前と正確に一致する必要があります。たとえば、パターン**FastEthernet** は、パターンの最後にアスタリスクを含めない限り、FastEthernet0/1 とは一致しません。

ステップ 6 （任意）[Category] の下で、[Objects] テーブルでこのオブジェクトを識別するために使用するカテゴリを選択します。カテゴリ オブジェクトの使用 （18 ページ）を参照してください。

ステップ 7 （任意）[デバイスごとに値のオーバーライドを許可（Allow Value Override per Device）] を選択して、このオブジェクトのプロパティを個々のデバイスで再定義できるようにします。ポリシー オブジェクトの上書きの許可 （25 ページ）を参照してください。

ステップ 8 [OK] をクリックしてオブジェクトを保存します。

[Interface Role] ダイアログボックス

[Interface Role] ダイアログボックスを使用して、インターフェイス ロール オブジェクトを作成、コピー、または編集します。インターフェイス ロール オブジェクトには次の用途があります。

- 複数のインターフェイスの指定：インターフェイス ロール オブジェクトを使用すると、各インターフェイスの名前を手動で定義することなく、複数のデバイス上の特定のインターフェイスにポリシーを適用できます。
- ゾーン：インターフェイス ロール オブジェクトを使用して、ゾーンベースのファイアウォール ルール ポリシーでゾーンを定義できます。

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 [インターフェイスロール（Interface Roles）] を選択します。作業領域内を右クリックして [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 [オブジェクトの編集（Edit Object）] を選択します。

関連項目

- ポリシー オブジェクトの作成 （13 ページ）
- インターフェイス ロール オブジェクトの作成 （97 ページ）
- 単一のインターフェイス指定が許可されている場合のインターフェイス ロールの使用 （101 ページ）
- ポリシー定義中のインターフェイスの指定 （100 ページ）

- インターフェイス ロール オブジェクトについて （95 ページ）
- Policy Object Manager （4 ページ）

フィールド リファレンス

表 *27 : [Interface Role]* 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 1024 文字を使用できます。
Interface Name Patterns	このインターフェイス ロールに含める名前。名前は、インターフェイス、サブインターフェイス、およびその他の仮想インターフェイスの完全な名前または名前の一部です。複数の名前パターンを指定する場合は、カンマで区切ります。 （注） ファイアウォールデバイスの場合は、ハードウェアポート識別子（Ethernet0 など）ではなく、インターフェイスに割り当てられた名前（内部、外部、または DMZ など）を使用します。 次のワイルドカードを使用して、複数のインターフェイスに適用する名前パターンを作成できます。 • ピリオド（.）は、1 文字を表すワイルドカードとして使用します。ピリオドをパターン自体の一部として使用するには、ピリオドの前にバックスラッシュ（\）を入力します。 • アスタリスク（*）は、インターフェイス パターンの末尾にある 1 つ以上の文字を表すワイルドカードとして使用します。 たとえば、DMZ* には、名前が「DMZ」で始まるすべてのインターフェイスが含まれ、DMZ. は DMZ1 や DMZ2 などのインターフェイスには一致しますが、DMZ10 には一致しません。 パターンにワイルドカードが含まれていない場合は、インターフェイスの名前と正確に一致する必要があります。たとえば、パターン「FastEthernet」は、パターンの最後にアスタリスクを含めない限り、FastEthernet0/1 とは一致しません。
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 （18 ページ）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 （25 ページ）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 （24 ページ）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。

ポリシー定義中のインターフェイスの指定

インターフェイスの識別を必要とするポリシーを設定する場合、次に示すように、インターフェイスを指定するための複数のオプションがあります。

- インターフェイスの名前（Ethernet0 など）を手動で入力します。

ポリシー定義の一部としてサブインターフェイスを手動で指定するには、ピリオドの前にバックスラッシュ（\）を入力する必要があります。Ethernet0\.1 などのように入力します。

バックスラッシュなしでピリオドを入力すると、ピリオドは Security Manager によって 1 文字のワイルドカードとして処理されます。たとえば、Ethernet1/1.0 をアクセスルールの一部として定義する場合は、**Ethernet1/1\.0** と入力する必要があります。代わりに **Ethernet1/1.0** と入力すると、単独のピリオドはワイルドカードとして処理されるため、名前は Ethernet1/1.0 や Ethernet1/1/0 というインターフェイスと一致します。

- インターフェイス ロールの名前を手動で入力します。インターフェイス ロールの詳細については、 インターフェイス ロール オブジェクトについて （95 ページ）を参照してください。
- インターフェイスまたはインターフェイス ロールをリストから選択します。[インターフェイス（Interfaces）] フィールドの横の [選択（Select）] をクリックすることにより、有効なインターフェイス名およびインターフェイスロールのリストが表示されます。サブインターフェイスは、名前の中のピリオドの前にバックスラッシュが付いて表示されます。

リストから選択することによって、エントリが有効であることを保証できます。詳細については、ポリシーのオブジェクトの選択 （2 ページ）を参照してください。

ポリシーで複数のインターフェイスが許可されている場合、エントリをカンマで区切ります。

ポリシーおよびオブジェクト セレクタでは、インターフェイスとインターフェイス ロールはアイコンによって区別されます。インターフェイスと同じ名前のインターフェイス ロールを作成する場合は、必要なものを正確に選択するように注意してください。次の表でアイコンについて説明します。

表 *28*：インターフェイスおよびインターフェイス ロールのアイコン

タイプ（Type）	アイコン
インターフェイス	
インターフェイス ロール ロールを編集できる場合は、鉛筆のイメージがアイコンに重なっています。	
ASA 8.3+デバイス上のグローバル「インターフェイス」。インターフェイス固有ではなくグローバルとして作成されたルールに対して使用されます。	

関連項目

- Cisco IOS ルータでの基本的なインターフェイス設定
- ファイアウォール デバイスのインターフェイスの設定
- インターフェイス ロール オブジェクトについて （95 ページ）
- インターフェイス ロール オブジェクトの作成 （97 ページ）
- 単一のインターフェイス指定が許可されている場合のインターフェイス ロールの使用（101 ページ）

単一のインターフェイス指定が許可されている場合のインターフェイス ロールの使用

インターフェイス ロール オブジェクトは、ロールの定義方法に応じて、デバイス上で定義されている実際のインターフェイスと一致する数が変化します。つまり、特定のデバイスについて、インターフェイスロールが 0 個、1 個、または複数個のインターフェイスと一致する場合があります。インターフェイス ロールをポリシーで使用すると、Security Manager によってロールはコマンドに変換されます。これらのコマンドによって、デバイス上で定義されている、ロールと一致するすべてのインターフェイスが設定されます。

ただし、多くのポリシーでは、単一のインターフェイス名を指定する必要があります。ポリシーによって単一のインターフェイス名が許可されている状況でインターフェイス ロールを使用する場合は、単一のインターフェイスと一致するようにインターフェイス ロールを定義する必要があります。デバイス上の複数のインターフェイスと一致するインターフェイス ロールを使用すると、Security Manager によってロールと一致するデバイス上の最初のインターフェイスが選択されますが、それが該当するインターフェイスではない場合があります（該当するインターフェイスの場合は適切に機能します）。

関連項目

- ポリシー定義中のインターフェイスの指定 （100 ページ）

- インターフェイス ロール オブジェクトについて （95 ページ）
- インターフェイス ロール オブジェクトの作成 （97 ページ）

インターフェイスとインターフェイス ロール間の名前の競合の処理

通常の状況では、デバイス上の実際のインターフェイスと同じ名前のインターフェイス ロールを設定できます。ポリシーを定義するときにオブジェクトセレクタを使用する場合（ポリシーのオブジェクトの選択 （2 ページ）を参照）、使用可能な選択肢としてインターフェイスとインターフェイス ロールの両方が表示され、いずれかを選択できます。ポリシーを定義するときにこの共通の名前を入力すると、Security Manager によって、インターフェイスではなくインターフェイス ロールがポリシーに自動的に関連付けられます。

ただし、次の状況では名前の競合が発生する可能性があります。

1. ポリシーを定義するときにインターフェイスの名前を入力します。
2. その後、同じ名前のインターフェイス ロールを作成します。
3. ポリシーを定義するときにこの名前を再度入力します。
4. [選択（Select）] をクリックしてオブジェクトセレクタを表示するか、[保存（Save）] をクリックしてポリシーを保存するか、一部の場合には、[OK] をクリックしてポリシーを更新します。

この一連のイベントが発生すると、インターフェイスを指定するかインターフェイス ロールを指定するかを選択できるように、[Interface Name Conflict] ダイアログボックスが自動的に開きます。ダイアログボックスには、競合が発生している名前だけが表示されます。

関連項目

- ポリシー定義中のインターフェイスの指定 （100 ページ）
- インターフェイス ロール オブジェクトについて （95 ページ）

マップ オブジェクトについて

Policy Object Manager の Maps フォルダ内のオブジェクトを使用すると、インスペクション ルール、ゾーンベースのファイアウォール ルール、IPS、QoS、接続ルールの各ポリシーのクラス マップ、パラメータ マップ、およびポリシー マップを設定できます。これらのポリシーで使用できるマップのタイプは、デバイスで実行されているオペレーティング システムおよび特定のバージョン番号によって異なるため、通常は、ポリシーを設定するときにマップを設定するのが最適です。

ヒント　デバイスでは、設定するすべてのマップに一意の名前が必要です。たとえば、同じデバイス上の FTP と DNS クラス マップに対して同じ名前は使用できません。デバイスに対して同じ名前のマップを選択すると、Security Manager によって、重複する名前に数値のサフィックスが自動的に付加されます。dnsmap_1 などです。

Maps フォルダには、次のフォルダが含まれています。サブフォルダによって、マップはインスペクションに使用されるか Web コンテンツ フィルタリングに使用されるかに基づいて整理されます。

- Class Maps：動作対象のトラフィックを識別するために使用されるレイヤ 7 クラス マップ。
- Parameter Maps：ゾーンベースのファイアウォール ルール ポリシーで使用される設定を設定するパラメータ マップ、またはその他のマップ。
- Policy Maps：選択されたトラフィックに対して実行するアクションを識別するために使用されるレイヤ 7 ポリシー マップ。

Maps フォルダには、TCP マップ オブジェクト（レイヤ 4 オブジェクト）、正規表現オブジェクト、および正規表現グループ オブジェクトのエントリも含まれています。

次の項では、さまざまなタイプのマップについて詳細に説明します。

クラス マップ

クラス マップは、ポリシー マップの下位にあります。クラス マップをデバイス ポリシーで直接指定することはできません。代わりに、ポリシー マップを作成してクラス マップを組み込みます。クラス マップ自体では、インスペクション ルールまたはゾーンベースのファイアウォール ルールで対象とするトラフィックの一致条件が定義されます。

- ASA/PIX 7.2 以降、および FWSM デバイス：DNS、FTP、HTTP、IM、および SIP トラフィックのインスペクション用のクラスマップを作成できます。トラフィック一致をポリシー マップ オブジェクト内で直接定義するオプションもありますが、別々のクラス マップを作成すると、複数のポリシー マップで再利用できます。
- IOS 12.4(6)T 以降のデバイス：IM アプリケーション（AOL、ICQ、MSN Messenger、Windows Messenger、および Yahoo Messenger）、P2P アプリケーション（eDonkey、FastTrack、Gnutella、Kazaa2）、H.323、HTTP、IMAP、POP3、SIP、SMTP、Sun RPC のインスペクション用のクラスマップを作成できます。ローカル、N2H2、Trend、および Websense オブジェクトを使用して、Web コンテンツのフィルタリング用のクラス マップを作成することもできます。

ASA/PIX/FWSM に使用されるクラス マップとは異なり、別々のクラス マップを作成し、関連するポリシー マップから参照する必要があります。これらのポリシー マップは、ゾーンベースのファイアウォール インスペクション ルールまたはコンテンツ フィルタリング ルールで使用できます。詳細については、次の項を参照してください。

- ゾーンベースのファイアウォール ポリシーのインスペクション マップの設定

- ゾーンベースのファイアウォール ポリシーのコンテンツ フィルタリング マップの設定

クラス マップを作成するには、次の項を参照してください。

- インスペクション ポリシーのクラス マップの設定
- ゾーンベースのファイアウォール ポリシーのクラス マップの設定

クラス マップ、パラメータ マップ、およびポリシー マップで使用できる正規表現および正規表現グループを作成するには、次の項を参照してください。

- 正規表現の追加/編集
- 正規表現グループの設定

パラメータ マップ

パラメータ マップによって、ゾーンベースのファイアウォール インスペクション ルールまたはコンテンツ フィルタリング ルール、あるいは他のポリシー マップ オブジェクトで使用できる設定が定義されます。

- インスペクション：一般的なゾーンベースのファイアウォール ルール パラメータ用のインスペクション パラメータ マップ、または IM アプリケーション インスペクションで使用するプロトコル情報パラメータ マップを作成できます。
- コンテンツ フィルタリング：ローカル、N2H2、Trend、URL フィルタ、URLF Glob、Websense パラメータ マップを作成して、Web コンテンツ フィルタリングを定義できます。

ポリシー マップ

ポリシー マップを設定して、インスペクションのデフォルト アクションを変更したり、ゾーンベースのファイアウォール設定ポリシーで Web コンテンツ フィルタリングを設定したりすることができます。ポリシーマップは、通常、特別な処理を必要とするアプリケーションに適用されます。特別な処理は、埋め込み IP アドレス情報が存在したり、動的に割り当てられたポート上でトラフィックがセカンダリ チャネルを開く場合などに必要となります。

ポリシーマップによって、マップ内で指定された条件と一致するトラフィックに対して実行するアクションが識別されます。ほとんどのポリシー マップでは、クラス マップを参照することによってトラフィック一致条件を指定できます。ただし、一部のポリシーマップでは、ポリシー マップ内で一致基準を指定する必要があります。

次のタイプのポリシー マップを設定できます。

- インスペクションルール：インスペクションルールを設定する場合、Security Manager を使用して、次のアプリケーションのポリシーマップオブジェクトを作成できます。DCE/RPC、DNS、ESMTP、FTP、GTP、H.323、HTTP、IM、IP options、IPsec、NetBIOS、SIP、Skinny、および SNMP。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を参照してください。

- ゾーンベースのファイアウォール インスペクション ルール：ゾーンベースのファイアウォール インスペクション ルールを設定する場合、Security Manager を使用して、次のアプリケーションのポリシーマップオブジェクトを作成できます。H.323、HTTP、IM（AOL、ICQ、MSN Messenger、Windows Messenger、Yahoo Messenger を含む）、IMAP、P2P（eDonkey、FastTrack、Gnutella、Kazaa2 を含む）、POP3、SIP、SMTP、Sun RPC。詳細については、ゾーンベースのファイアウォール ポリシーのインスペクション マップの設定を参照してください。
- ゾーンベースのファイアウォール コンテンツ フィルタリング ルール：ゾーンベースのファイアウォール コンテンツ フィルタリング ルールを設定する場合、Security Manager を使用して Web フィルタ ポリシー マップを作成できます。HTTP トラフィックを検査するように HTTP ポリシー マップを設定することもできます。詳細については、ゾーンベースのファイアウォール ポリシーのコンテンツ フィルタリング マップの設定を参照してください。
- IPS、QoS、および接続ルール：PIX 7.x+ および ASA デバイスに固有のこのサービス ポリシーを設定する場合、TCP マップを使用して TCP インスペクションをカスタマイズできます。詳細については、「TCP マップの設定」および「ファイアウォール デバイスでのサービス ポリシールールの設定」を参照してください。

ネットワーク/ホストオブジェクトについて

ネットワーク/ホストオブジェクトは、ネットワーク、ホスト、またはこれらの両方を表す IP アドレスの論理集合です。

（注） Security Manager 4.4 では、IPv4 と IPv6 で別々のネットワーク/ホストオブジェクトが使用されなくなりました。単一の統合されたネットワーク/ホストオブジェクトがあり、IPv4 アドレス、IPv6 アドレス、またはその両方（グループオブジェクトの場合）を受け入れることができます。ただし、IPv4 アドレスと IPv6 アドレスが混在するグループオブジェクトは、ASA 9.0.1 以降のデバイスのポリシーにのみ割り当てることができます。詳細については、Cisco Security Manager 4.4 でのポリシーオブジェクトの変更を参照してください。

ネットワーク/ホストオブジェクトを作成するときに、オブジェクトのタイプを選択する必要があります。これにより、オブジェクトに含めることができるアドレスのタイプが定義および制限されます。

- グループ：次のタイプのアドレスの組み合わせを含めることができます。
  - ネットワークまたはサブネット。IPv4 アドレスとサブネットマスク、または IPv6 プレフィックスとプレフィックス長で指定されます。
  - IPv4 または IPv6 ネットワーク アドレスの範囲。
  - 個別のホスト。IPv4 または IPv6 アドレス（ドメイン名ではなく）で指定されます。

- その他のネットワーク/ホストオブジェクト。完全修飾ドメイン名（FQDN）オブジェクトを含む、既存のネットワーク/ホストオブジェクトのリストから選択されます。

- FQDN：（ASA 8.4(2) 以降のみ）このオブジェクトには、www.cisco.com などの単一ホストの完全修飾ドメイン名を含めることができます。デバイスは DNS を使用して FQDN をその IP アドレスに定期的に解決します。
- ホスト：このオブジェクトには、単一のホストの IPv4 または IPv6 アドレスを含めることができます（10.100.10.10、2001:DB8::0DB8:800:200C:417A など）。
- 属性：このオブジェクトには、1 つ以上のポリシーベースの VM 属性エージェントを含めることができます。これにより、ユーザはネットワークオブジェクトを定義することにより、VMware vCenter で管理している VMware ESXi 環境の 1 つ以上の仮想マシン（VM）に関連付けられている属性に従ってトラフィックをフィルタリングできます。各 VM 属性エージェントは、単一の vCenter サーバーと通信します。
- アドレス範囲：このオブジェクトには、IPv4 または IPv6 アドレスの範囲を 1 つ含めることができます。開始アドレスと終了アドレスは異ななる必要があり、開始アドレスが終了アドレスよりも小さい必要があります。
- ネットワーク：このオブジェクトには、単一の IPv4 ネットワークアドレスおよびサブネットマスク（10.100.10.0/24 など）、または単一の IPv6 プレフィックスおよびプレフィックス長（2001:DB8::/32 など）を含めることができます。

ネットワーク/ホストグループオブジェクトによって、スケーラブルなポリシーの管理が簡単になります。ネットワーク/ホストオブジェクトの連携機能を使用することで、ネットワークとともにポリシーを拡張できます。たとえば、ネットワーク/ホストオブジェクトに含まれているアドレスのリストを変更すると、変更は、その他のすべてのネットワーク/ホストオブジェクトおよびそのネットワーク/ホストオブジェクトを参照するポリシーに伝播します。

ホスト、ネットワーク、アドレス範囲オブジェクトには、ASA 8.3 以降のデバイスのポリシーで使用される際の特別な用途があります。これらのデバイスでは、ポリシー オブジェクト自体にオブジェクト NAT ルールを設定できます。その他のタイプのデバイスでオブジェクトを使用した場合、この NAT 設定は無視されます。

次の項では、ネットワーク/ホストオブジェクトを操作する方法について説明します。

- 連続および不連続ネットワーク マスク（IPv4 アドレスに対応） （107 ページ）
- ネットワーク/ホストオブジェクトの作成 （108 ページ）
- 未指定ネットワーク/ホストオブジェクトの使用 （114 ページ）
- ポリシー定義中の IP アドレスの指定 （115 ページ）
- VM 属性ポリシー （117 ページ）

連続および不連続ネットワーク マスク（IPv4 アドレスに対応）

ネットワーク マスクによって、IPv4 アドレスのどの部分でネットワークを識別し、どの部分でホストを識別するかが決定されます。IP アドレスと同様に、マスクは 4 つのオクテットで表されます（オクテットは、0 ～ 255 の範囲の 10 進数に相当する 8 ビットの 2 進数です。）マスクの特定のビットが 1 の場合、IP アドレスの対応するビットはアドレスのネットワーク部分にあり、マスクの特定のビットが 0 の場合、IP アドレスの対応するビットはホスト部分にあります。

標準の（つまり、連続した）ネットワーク マスクは、0 個以上の 1 で始まり、そのあとに 0 個以上の 0 が続きます。このようなネットワーク マスクは、連続した IP アドレス範囲で構成されるネットワークを表すため、連続と見なされます。たとえば、ネットワーク 192.168.1.0/255.255.255.0 には、192.168.1.0 ～ 192.168.1.255 の範囲のすべての IP アドレスが含まれます。

次の表に、一般的に使用される標準のネットワーク マスクを表すさまざまな方式を示します。

表 *29 :* 標準のネットワーク マスク

ドット付き 10 進表記	Classless Inter-Domain Routing（CIDR）表記
255.0.0.0	/8
255.255.0.0	/16
255.255.255.0	/24
255.255.255.255	/32

たとえば、255.255.255.0 は、IP アドレスの最初の 3 つのオクテット（24 ビット、または CIDR 表記で /24）が 1 で構成され、ネットワークを示します。最後のオクテットは 0 で構成され、ホストを示します。

不連続ネットワーク マスク

非標準の（つまり、不連続の）ネットワーク マスクは、連続フォーマットに準拠しないマスクです。たとえば、10.0.1.1/255.0.255.255 は、オクテット 1、3、および 4 と正確に一致するアドレスを照合するが、オクテット 2 については任意の値が受け入れられることを示します。

不連続ネットワーク マスクは通常はネットワーク設定で使用しませんが、特定のコマンド用に使用する場合があります。アクセス コントロール リスト（ACL）を定義するときのフィルタリング コマンドなどです。Security Manager では、非標準のネットワーク マスクは、非標準のネットワーク マスクの使用が CLI コマンドによってサポートされているポリシーで使用できます。不連続ネットワーク マスクがサポートされていないポリシーで不連続ネットワーク マスクを定義しようとすると、エラーが表示されます。

ネットワーク マスクと検出

検出中に、Security Manager は、ネットワーク/ホスト オブジェクトを Policy Object Manager に定義されている既存の同等のオブジェクトと照合しようとします。

- 連続ネットワーク マスクの場合：標準のネットワークだけを含む 2 つのネットワーク/ホスト オブジェクトが同じ IP アドレスのセットで構成されている場合、同等と見なされます。
- 不連続ネットワーク マスクの場合：標準のネットワークが同じ IP アドレスのセットで構成され、非標準のネットワークが構文的に同等の場合にだけ、2 つのネットワーク/ホスト オブジェクトは同等と見なされます。

ネットワーク マスクの表示方法

ドット付き 10 進表記を使用して連続ネットワーク マスクと不連続ネットワーク マスクの両方を入力できますが、すべての連続ネットワーク マスクは CIDR 表記に変換されます。このことにより、ドット付き 10 進表記だけで表示される不連続ネットワーク マスクと区別しやすくなります。

関連項目

- ネットワーク/ホストオブジェクトの作成 （108 ページ）
- ポリシー定義中の IP アドレスの指定 （115 ページ）
- 未指定ネットワーク/ホストオブジェクトの使用 （114 ページ）
- ネットワーク/ホストオブジェクトについて （105 ページ）

ネットワーク/ホストオブジェクトの作成

ネットワーク、個別のホスト、または両方のグループを表すネットワーク/ホストオブジェクトを作成できます。ネットワーク/ホストオブジェクトを作成するときは、オブジェクトのタイプ（グループ、ホスト、FQDN、ネットワーク、属性、アドレス範囲）を選択する必要があります。作成後は、オブジェクト タイプを変更できません。

ヒント このオブジェクトタイプを使用するポリシーまたはオブジェクトを定義するときに、ネットワーク/ホストオブジェクトを作成できます。詳細については、ポリシーのオブジェクトの選択 （2 ページ）を参照してください。

ロールにマップされた変更権限を持っている場合にのみ、NAT オブジェクトを指定できます。

関連項目

- ネットワーク/ホストオブジェクトについて （105 ページ）
- ポリシー オブジェクトの作成 （13 ページ）
- 連続および不連続ネットワーク マスク（IPv4 アドレスに対応） （107 ページ）
- ポリシー定義中の IP アドレスの指定 （115 ページ）
- VM 属性ポリシー （117 ページ）

- 未指定ネットワーク/ホストオブジェクトの使用 （114 ページ）
- ネットワーク/ホスト オブジェクト、ポート リスト オブジェクト、およびサービス オブジェクトがオブジェクト グループとしてプロビジョニングされるときの命名方法 （141 ページ）

ステップ 1 [管理（Manage）] メニューから [ポリシーオブジェクト（Policy Objects）] を選択するか、ボタンバーの [Policy Object Manager] ボタンをクリックして、[Configuration Manager] ウィンドウの下部にある [Policy Object Manager] ペインを開きます。詳細については、 Policy Object Manager （4 ページ）を参照してください。

ステップ 2 オブジェクトタイプセレクタから [ネットワーク/ホスト（Networks/Hosts）] を選択します。

ステップ 3 ウィンドウの下部にある [新規オブジェクト（New Object）] ボタンをクリックし、次のタイプのネットワーク/ホスト オブジェクトのいずれかを選択して [Add Network/Host]/[Edit Network/Host] ダイアログボックス（109 ページ）を開きます。作業領域で右クリックして [新規オブジェクト（New Object）] を選択し、次のオプションのいずれかを選択してダイアログボックスを開くこともできます。

- [グループ（Group）] : 1 つ以上のエントリを持つオブジェクトを作成します。ネットワーク、ホスト、アドレス範囲、または他のネットワーク/ホストオブジェクト（FQDN オブジェクトを含む）の組み合わせを含めることができます。
- [FQDN] : （ASA 8.4(2) 以降のみ）www.cisco.com などの単一ホストの完全修飾ドメイン名を持つオブジェクトを作成します。
- [ホスト（Host）] : 単一のホストアドレス（10.100.10.10（IPv4）、2001:DB8::12ab:5689（IPv6）など）を持つオブジェクトを作成します。
- [属性（Attribute）] : （ASA 9.7.1以降のみ）ネットワークオブジェクトを定義して、VMware vCenter で管理している VMware ESXi 環境の 1 つ以上の仮想マシン（VM）に関連付けられている属性に従ってトラフィックをフィルタリングします。
- [アドレス範囲（Address Range）] : 単一のアドレス範囲（10.100.10.1-10.100.10.255 など）を持つオブジェクトを作成します。
- [ネットワーク（Network）] : 単一のネットワークアドレス（10.100.10.0/24、2001:DB8::/32 など）を持つオブジェクトを作成します。

ヒント ホスト、ネットワーク、およびアドレス範囲オブジェクトについては、ASA 8.3 以降のデバイスのオブジェクト NAT 規則を設定することもできます。その他のデバイスでは NAT 設定は無視されます。

ステップ 4 [Add Network/Host]/[Edit Network/Host] ダイアログボックス （109 ページ）に、適切な情報を入力します。

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

[Add Network/Host]/[Edit Network/Host] ダイアログボックスを使用して、ネットワーク/ホストオブジェクトを表示、作成、または編集します。ダイアログボックスのタイトル、コンテンツ

および外観は、作成するネットワーク/ホストオブジェクトのタイプ（グループ、FQDN、ホスト、属性、アドレス範囲、またはネットワーク）によってもいくらか異なります。FQDN オブジェクトには、ASA 8.4.2 以降のデバイスが必要です。属性オブジェクトには、ASA 9.7.1 以降のデバイスが必要です。グループタイプでは、複数の定義を入力できるため、ネットワーク、ホスト、および他のネットワーク/ホストオブジェクトの集合にすることができますが、他のタイプでは単一の定義のみを入力できます。

[ホスト（Host）]、[ネットワーク（Network）]、および[アドレス範囲（Address Range）]バージョンのダイアログボックスには、[全般（General）] と [NAT] の 2 つのタブ付きパネルオプションがあります。次の表で、[全般（General）]パネルのオプションと、タブのないバージョンのダイアログボックスについて説明します。 NAT オプションについては[Add Network/Host]/[Edit Network/Host] ダイアログボックス - [NAT] タブで説明されています。

（注） Security Manager 4.4 では、IPv4 と IPv6 で別々のネットワーク/ホストオブジェクトが使用されなくなりました。単一の統合されたネットワーク/ホストオブジェクトがあり、IPv4 アドレス、IPv6 アドレス、またはその両方（グループオブジェクトのみの場合）を受け入れることができます。ただし、IPv4 アドレスと IPv6 アドレスが混在するグループオブジェクトは、ASA 9.0.1 以降のデバイスのポリシーにのみ割り当てることができます。

ASA 8.3 以降のデバイスで使用する IPv4 ベースのホスト、ネットワーク、またはアドレス範囲オブジェクトを作成する場合や、ASA 9.0.1 以降のデバイスで使用する統合されていないホスト、ネットワーク、またはアドレス範囲オブジェクトを作成する場合は、ダイアログボックスの [NAT] タブでオブジェクト NAT ルールを設定することもできます。どちらの場合も、オブジェクト NAT を許可するには、[デバイスごとに値のオーバーライドを許可（Allow Value Override per Device）] を選択する必要があります。[NAT] タブの参照情報については、[Add Network/Host]/[Edit Network/Host] ダイアログボックス - [NAT] タブを参照してください。

加えて、アドレスを持たないオブジェクトを作成できます。このようなオブジェクトの場合、[デバイスごとに値のオーバーライドを許可（Allow Value Override per Device）] を選択し、そのオブジェクトを使用するすべてのデバイスに対してオーバーライドを作成する必要もあります。未指定アドレスの使用の詳細については、未指定ネットワーク/ホストオブジェクトの使用 （114 ページ）を参照してください。

ナビゲーション パス

[管理（Manage）] メニューから [ポリシーオブジェクト（Policy Objects）] を選択するか、ボタンバーの [Policy Object Manager] ボタンをクリックして、[Configuration Manager] ウィンドウの下部にある [Policy Object Manager] ペインを開きます。オブジェクトタイプセレクタから [ネットワーク/ホスト（Networks/Hosts）] を選択します。作業領域内で右クリックして [新規オブジェクト（New Object）] を選択し、オブジェクトタイプを選択するか、または行を右クリックして [オブジェクトの編集（Edit Object）] を選択します。ペインの下部にある関連ボタンを使用して、いずれかのダイアログボックスを開くこともできます。

関連項目

- ネットワーク/ホストオブジェクトの作成 （108 ページ）

- ネットワーク/ホストオブジェクトについて （105 ページ）
- Policy Object Manager （4 ページ）
- ネットワーク/ホスト オブジェクト、ポート リスト オブジェクト、およびサービス オブジェクトがオブジェクト グループとしてプロビジョニングされるときの命名方法 （141 ページ）
- セレクタ内の項目のフィルタリング

フィールド リファレンス

表 *30 : [*ネットワーク/ホスト（*Networks/Hosts***）*]* ダイアログボックス（*[*全般（***General***）*]* タブ）**

要素	説明
名前	オブジェクト名（最大 64 文字）。オブジェクト名では、大文字と小文字が区別されません。詳細については、 ポリシー オブジェクトの作成 （13 ページ）を参照してください。
説明	（任意）オブジェクトの説明。
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 （18 ページ）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 （25 ページ）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 （24 ページ）を参照してください。 **ヒント** ホスト、アドレス範囲、またはネットワーク オブジェクトの NAT を設定する場合は、このオプションを選択する必要があります。NAT 設定はデバイスのオーバーライドとして作成され、オブジェクト内には保持されません。 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。
グループオブジェクトのオプション	

要素	説明
[使用可能なネットワーク/ホスト（Available Networks/Hosts）] [グループ内のメンバー（Members In Group）] [IPアドレスをカンマで区切って入力（Type in comma separated IP addresses）]	[グループ内のメンバー（Members In Group）] リストには、オブジェクトに含まれるネットワーク、ホスト、および他のネットワーク/ホストオブジェクトが表示されます。リストに入力するには、次のいずれかの組み合わせを実行します。 • [既存のネットワーク/ホスト（Existing Networks/Hosts）] リストで1つ以上のアドレス、属性、FQDN、グループ、ホスト、ネットワークの各オブジェクトを選択し、リスト間の [>>] ボタンをクリックします。 • [IPアドレスをカンマで区切って入力（Type in comma separated IP addresses）] フィールドに 1 つ以上の IP アドレスを入力し、リスト間の [>>] ボタンをクリックします。複数のアドレスをカンマで区切ります。これらは [メンバー（Members）] リストに別々の行として追加されます。 IPv4 アドレスの場合、ホストアドレス、ネットワークアドレス（/ 文字のあとにサブネットマスクを入力。10.100.10.0/24 など）、またはアドレスの範囲（開始アドレスと終了アドレスをハイフンで区切り、オプションでサブネットマスクを指定）を含めることができます。 IPv6 アドレスの場合、ホストアドレス、ネットワークアドレス（/ 文字のあとにプレフィックスを入力。2001:DB8::/32 など）、またはアドレスの範囲（2001:DB8::1-2001:DB8::100 など）を含めることができます。 詳細については、ポリシー定義中の IP アドレスの指定 （115 ページ）を参照してください。 • [グループ内のメンバー（Members In Group）] リストから項目を削除するには、項目を選択し、該当する [<<] ボタンをクリックして、項目を元の場所に戻します。一度に複数の項目を選択して削除できます。 （注） IPv4アドレスとIPv6アドレスが混在するグループオブジェクトは、ASA 9.0.1 以降のデバイスのポリシーにのみ割り当てることができます。
FQDN オブジェクトのオプション	

要素	説明
[FQDN] [FQDNタイプ（FQDN Type）]	単一のホストの完全修飾ドメイン名（たとえば somehost.cisco.com など）。 FQDN タイプは、指定されたドメインにマッピングされる IP アドレスのタイプを指定します（[IPv4のみ（IPv4 Only）]、[IPv6のみ（IPv6 Only）]、またはデバイス固有のデフォルトが適用される [デフォルト（Default）]）。すべての非 ASA デバイスおよび 9.0.1 より前の ASA デバイスの場合、デフォルトは IPv4 です。
ホストオブジェクトのオプション	
IPアドレス	オブジェクトに含める単一ホストの IPv4 または IPv6 アドレス。
属性オブジェクトのオプション	
エージェント名（Agent Name） タイプ（Type） 値	VM 属性エージェント名。VM 属性エージェントのリストから選択するか、新しい VM 属性エージェントを追加します。 [VM属性エージェントタイプ（VM Attribute Agent Type）] は 128 文字以下にする必要があります。 [VM属性エージェント値（VM Attribute Agent Value）] は 128 文字以下にする必要があります。 （注） ユーザーは、一連の VM にカスタム属性のタイプと値を割り当てて、共通のユーザー定義の特性を持つ一連の VM に共通のポリシーセットを適用できます。
アドレス範囲オブジェクトのオプション	
開始 IP アドレス 終了 IP アドレス	アドレスの範囲を定義する最初と最後の IP アドレス。開始アドレスと終了アドレスは異なっており、開始の方が終了よりも小さいアドレスである必要があります。
ネットワークオブジェクトのオプション	
IPアドレス [ネットマスク/プレフィックス（Net Mask/Prefix）]	ネットワークを表す IPv4 または IPv6 アドレス（たとえば 10.100.10.0 または 2001:DB8::/32 など）。 IPv4 アドレスを入力した場合は、そのサブネットマスクを [ネットマスク/プレフィックス（Net Mask/Prefix）] フィールドに入力します。マスクは、24（スラッシュなし）などの CIDR 形式、または 255.255.255.0 などのドット付き 10 進法形式のいずれかで入力できます。 IPv6 アドレスを入力した場合は、そのプレフィックス長を [ネットマスク/プレフィックス（Net Mask/Prefix）] フィールドに入力します。

未指定ネットワーク/ホストオブジェクトの使用

ネットワーク/ホストオブジェクトを定義するときに、[アドレス（address）]フィールドをブランクのままにして、値が未指定のネットワーク/ホストオブジェクトを作成できます。値が未指定のネットワーク/ホストオブジェクトでは、それらを使用するすべてのデバイスでオーバーライドを作成する必要があります。

値が指定されていないネットワーク/ホストオブジェクトを使用する利点は、そのオブジェクトを使用するすべてのデバイスで、デバイスレベルのオーバーライドを作成せずに変更を送信すると、Security Manager がエラーを表示することです。対照的に、プレースホルダ値（10.10.10.10 など）でグローバルオブジェクトを定義する場合、オーバーライドの定義に失敗すると、そのグローバル値が誤って展開される可能性があります。

次の手順では、値が未指定のネットワーク/ホストオブジェクトを作成および導入する方法について説明します。

関連項目

- 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 （24 ページ）
- ネットワーク/ホストオブジェクトの作成 （108 ページ）
- 連続および不連続ネットワーク マスク（IPv4 アドレスに対応） （107 ページ）
- ポリシー定義中の IP アドレスの指定 （115 ページ）
- ネットワーク/ホストオブジェクトについて （105 ページ）

ステップ 1 ネットワーク/ホストオブジェクトを作成します。次の点に注意します。

- [アドレス（address）] フィールドをブランクのままにします（Members In Group、IP Address、Net Mask/Prefix、FQDN、または Start IP Address、End IP Address など）。
- [デバイスごとの値のオーバーライドを許可（Allow Value Override per Device）] チェックボックスをオンにします。

詳細については、 ネットワーク/ホストオブジェクトの作成 （108 ページ）を参照してください。

ステップ 2 オブジェクトを使用する各デバイスのオーバーライドを作成します。

a) [ネットワーク/ホスト（Networks/Hosts）] テーブルのオブジェクトの [オーバーライド（Overridable）] カラムで、緑色のチェックマークをクリックして、 [Policy Object Overrides] ウィンドウ （28 ページ）を開きます。

b) [オーバーライドの作成（Create Override）] ボタンをクリックし、オーバーライドを作成するデバイスを選択して、[アドレス（address）] フィールドの値を定義します。この時点で、このオーバーライド値は選択したすべてのデバイスに適用されます。詳細については、 複数デバイスのオブジェクト オーバーライドの一括での作成または編集 （27 ページ）を参照してください。

c) [Policy Object Overrides] ダイアログボックスで各デバイスをダブルクリックし、そのデバイスが必要とする値のアドレス フィールドを変更します。

ステップ 3 このオブジェクトを必要とするポリシーを定義します。次の 2 つの方式のいずれかを使用できます。

- デバイス ビューで、1 つのデバイス上でポリシーを定義し、ポリシーを共有し、ポリシーを他のデバイスに割り当てます。ローカル ポリシーの共有およびデバイス ビューまたは Site-to-Site VPN Manager における共有ポリシー割り当ての変更を参照してください。
- ポリシー ビューで、共有ポリシーを作成し、[Assignments] タブを使用してポリシーを他のデバイスに割り当てます。ポリシー ビューにおけるポリシー割り当ての変更を参照してください。

（注） 値が未指定のネットワーク/ホストオブジェクトを参照するネットワーク/ホストグループオブジェクトを作成できます。オブジェクトを含むポリシーをデバイスに割り当てる前に、デバイスレベルのオーバーライドを作成する必要はありません。

ポリシー定義中の IP アドレスの指定

多くのポリシーおよびポリシー オブジェクトでは、ホストまたはネットワークの IP アドレスを入力する必要があります。一部のポリシーまたはオブジェクトについては、1 つのホストだけ、または1つのネットワークだけを入力する必要があります。その他のポリシーまたはオブジェクトについては、ホストとネットワークの組み合わせを入力できます。状況に合わないアドレスを入力または選択することはできません。

次に、IPv4およびIPv6アドレスの両方に使用できるすべての形式の説明を示します。ただし、特定のポリシーやオブジェクトでは使用できない形式もあります（たとえば、インターフェイスロールは、非常に限定された数のポリシーでのみアドレス指定として使用できます）。ポリシーまたはオブジェクトで許可されている場合、複数のアドレスをカンマで区切って入力できます。

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

（注） 完全修飾ドメイン名（FQDN）を指定するには、FQDNネットワーク/ホストオブジェクトまたは FQDN オブジェクトを含むグループオブジェクトを使用する必要があります。FQDN を直接入力することはできません。

- v4 または v6 形式のホスト IP アドレス。
  - 完全な IPv4 アドレス（10.10.10.100 など）
  - 8 つのコンポーネントすべてを示す完全な IPv6 アドレス。たとえば、2001:DB8:0:0:0DB8:800:200C:417A のように使用します。個々のフィールドに先行ゼロを含める必要はありません。Security Manager では、アドレスを可能な限り圧縮形式に変換します。

- 圧縮 IPv6 アドレス。フィールドのグループは 2 つのコロン（::）で置き換えられます。IPv6 アドレスには、通常、連続するゼロの 16 進フィールドが含まれます。IPv6 アドレスの先頭、中間、または末尾にある連続した 0 の 16 進フィールドを 2 つのコロン（::）を使用して圧縮すると、IPv6 アドレスが扱いやすくなります（2 つのコロンは連続した 0 の 16 進フィールドを表します）。IPv6 アドレスで :: は最大 1 回しか使えません。たとえば、2001:DB8::0DB8:800:200C:417A のように使用します。未指定のアドレス 0:0:0:0:0:0:0:0 は :: として表すことができます。ループバック アドレスは ::1 です。
- IPv4 アドレスの IPv6 表現。IPv4/IPv6 混合環境では、IPv4 アドレスを別の IPv6 形式（x:x:x:x:x:x:d.d.d.d）で表現できます（x は最初の 6 つのフィールドの 16 進値を示し、d はピリオドで区切られたオクテットで表した IPv4 アドレスを示します）。最初の 6 つのフィールドはすべて 0、::FFFF、または 2001:DB8:: のいずれかです。たとえば、0:0:0:0:0:0:10.1.68.3 は圧縮形式では ::10.1.68.3、0:0:0:0:0:FFFF:10.1.68.3、または 2001:DB8::10.1.68.3 になります。

- IPv4 または IPv6 形式のネットワークアドレス：
  - IPv4 アドレス（サブネットマスクを含む）。CIDR 形式（10.10.10.0/24）またはドット付き 10 進法形式（10.10.10.0/255.255.255.0）で指定。
  - IPv6 アドレス。IPv4 の CIDR 表記と同様の方法で指定する 10 進形式のプレフィックス長を含む（/64 など）。数字は、プレフィックスを構成する左端の連続したアドレス ビットの数を指定します。たとえば、2001:DB8:0:CD30::/60 のように使用します。

（注） 2001:DB8:0:CD30::/60 を 2001::CD30:0:0:0:0/60 のように入力することもできます。ただし、末尾の 0 を圧縮する方法を推奨します。Security Manager では、アドレスを 2001:DB8:0:CD30::/60 に変換します。

IPv6 アドレッシングの詳細については、IETF RFC 4291、IP Version 6 Addressing Architecture [英語]（http://www.ietf.org/rfc/rfc4291.txt）を参照してください。

- IP アドレスの範囲。最初のアドレスと最後のアドレスはハイフンで区切ります。この範囲は、ポリシーで要求されていないかぎり、1 つのサブネット内である必要はありません。

CIDR 形式のプレフィックスやサブネットマスクを含めることもできます。例：2001:db8::1 ～ 2001:db8::2/64 または 10.10.10.100 ～ 10.10.10.200/24。

- 10.10.0.10/255.255.0.255 形式の IPv6 アドレスのパターン。この場合のマスクは不連続なビットマスクです（連続および不連続ネットワーク マスク（IPv4 アドレスに対応）（107 ページ）を参照）。
- インターフェイス ロール オブジェクト（まれな場合）。オブジェクトの名前を入力するか、または [選択（Select）] をクリックしてリストから名前を選択します（オブジェクト タイプとして [インターフェイスロール（Interface Role）] を選択する必要があります）。インターフェイス ロールを使用する場合は、選択したインターフェイスの IP アドレスを

指定した場合と同様にルールが動作します。デバイスに割り当てられる IP アドレスを把握できないため、DHCP を経由してアドレスを取得するインターフェイスの場合に有効です。詳細については、インターフェイス ロール オブジェクトについて （95 ページ）を参照してください。

ネットワーク/ホストオブジェクトを作成するか、ポリシーの一部として IP アドレスを定義すると、Cisco Security Manager によって、アドレスの構文が正しいこと、および必要に応じてマスクやプレフィックスが入力されていることが検証されます。たとえば、ホストを必要とするポリシーを定義する場合、マスクやプレフィックスを入力する必要はありません。ただし、サブネットを必要とするポリシーを定義する場合、マスクやプレフィックスとともにアドレスを入力するか、マスクやプレフィックスが定義されたネットワーク/ホストオブジェクトを選択する必要があります。

関連項目

- ネットワーク/ホストオブジェクトの作成 （108 ページ）
- 連続および不連続ネットワーク マスク（IPv4 アドレスに対応） （107 ページ）
- 未指定ネットワーク/ホストオブジェクトの使用 （114 ページ）
- Policy Object Manager （4 ページ）
- ネットワーク/ホストオブジェクトについて （105 ページ）

VM 属性ポリシー

VMware ESXi 環境の 1 つ以上の仮想マシン（VM）に関連付けられている属性に基づき、ネットワークオブジェクトを定義し、トラフィックをフィルタリングできます。この環境は、VMware vCenter によって管理されます。ユーザは、ESXi 環境内の VM に属性を割り当て、属性エージェントを設定できます。属性エージェントは、HTTPS および要求を使用して vCenter または単一の ESXi ホストに接続し、特定の属性を ESXi VM のプライマリ IP アドレスに関連付ける 1 つ以上のバインディングを取得します。

1 つの ASA では複数の属性エージェントを定義でき、それぞれを異なる vCenter と通信させるか、または 複数の属性エージェントを同じ vCenter と通信させることができます。

これにより、ユーザはアクセス制御リスト（ACL）を定義して、1 つ以上の属性を共有する VM のグループからのトラフィックにポリシーを割り当てることができます。この機能は、VM 属性に基づくポリシーと呼ばれます。

VM 属性機能は、すべてのハードウェア プラットフォームと、ESXi、KVM または HyperV ハイパーバイザで動作するすべての ASAv プラットフォームでサポートされます。VM 属性は、ESXi ハイパーバイザ上で動作する VM からのみ取得できます。

（注） ASA では、属性または属性タイプという用語を使用して、監視対象の特性を表します。VMWare では、同じ特性に対してプロパティという用語を使用します。これらの用語は同義で使用される場合があります。

VM 属性エージェントと vCenter 間の通信

VM 属性エージェントと vCenter の間で交換されるメッセージには、プロパティリクエストとバインド更新の 2 種類があります。

- プロパティリクエスト：これは、ASA から vCenter Server の IP アドレスに送信される HTTPS メッセージであり、設定されている属性エージェントの属性に関連付けられたネットワークオブジェクトに現在設定されている属性タイプの完全なリストを示します。このメッセージには、vCenter への接続を認証するために必要な SSL ログイン情報が含まれています。vCenter は、対応する HTTPS 応答で応答します。
- バインド更新：これは、1 つ以上の VM の属性が変更されるたびに、vCenter から ASA に送信される非同期 HTTPS メッセージです。各バインド更新は、属性の変更を報告する VM の IP アドレスによって識別されます。複数の属性が 1 つのエージェントによってモニターされている場合、1 件のバインド更新に各 VM のすべてのモニター対象属性の現在の値が含まれます。エージェントによってモニターされている特定の属性が、ある VM には設定されていない場合、その VM のバインドには空の属性値が含まれます。ある VM にモニター対象の属性が設定されていない場合、vCenter はバインド更新を ASA に送信しません。

属性エージェントが新しい属性タイプを含むプロパティリクエストを発行すると、vCenter は、その属性タイプが設定されている各 VM に関するバインド更新で応答します。これ以降、VM で属性値が追加または変更されると、vCenter だけが新しいバインドを発行します。

属性エージェントの状態

属性エージェントの状態には、接続状態とエージェント状態の 2 種類があります。

- 接続状態：これは、属性エージェントが現在 vCenter と接続しているかどうかを示します。

接続状態（Connection State）	説明
ホストクレデンシャルなし（No Host Credentials）	ユーザは host サブコマンドを使用して vCenter ホストのクレデンシャルを入力していません。または、エージェントを引き続き使用しているネットワークオブジェクトが存在しているときに、エージェントが no attribute source-group コマンドを使用して削除されています。

接続状態（Connection State）	説明
切断（Disconnected）	エージェントにはホストクレデンシャルが定義されていますが、現在 vCenter と接続していません。ASA がキープアライブパケットに対する HTTP 200 応答を受信すると、接続が確立されます。
コネクテッド	エージェントは、vCenter から最新のキープアライブ パケットに対する応答を受け取りました。
無効なホストクレデンシャル（Invalid Host Credentials）	エージェントは、vCenter に接続してプロパティリクエストを発行しようとしましたが、ユーザ名またはパスワード（またはその両方）が正しくなかったため、リクエストは拒否されました。エージェントは、新しいクレデンシャルが入力されるまでこの状態を維持します。入力された時点で、vCenter からキープアライブ応答を受信するまで、切断状態に移行します。

- [エージェントの状態（Agent State）]：このエージェントを介して属性タイプをモニターするようにネットワークオブジェクトが構成されているかどうかを示します。

表 *31* : エージェント状態の表

エージェント状態（Agent State）	説明
非アクティブ	現在、エージェントには属性が設定されていません。
Active	エージェントには、1 つ以上の属性が設定されています。 vCenter への接続がない場合でも、エージェントをアクティブにすることができます。

vCenter 仮想マシンの設定に関するガイドライン

VM 属性機能を利用するには、管理対象の仮想マシンがそれらの属性を vCenter サーバーで使用できるようにする必要があります。例として、いくつかの属性について説明します。

- summary.config.name：仮想マシンに関連付けられたユーザー定義の名前（例：VM-build-machine-1）
- summary.config.guestFullName：仮想マシンで実行されているゲスト OS の完全な名前（例：Red Hat Enterprise Linux 7（64 ビット））
- summary.config.annotation：仮想マシンのテキスト説明フィールド。

文字列の属性値（summary.config.annotation など）の場合、ネットワークオブジェクト属性の定義に含まれる値は、VM から vCenter に報告される値と完全に一致している必要があります。たとえば、ネットワークオブジェクトの属性値「This is a Build Machine」は、VM の

summary.config.annotation 値「this is a build machine」と一致しません。後者の文字列を含むバインド更新は、前者のホストマップに追加されません。

VM 属性機能によってモニタリングされている VM には、VMware ツールがインストールされている必要があります。VMware ツールは、VM の IPv4 アドレスまたは IPv6 アドレスを vCenter サーバーに報告するソフトウェアコンポーネントです。VM 属性の機能は、IP アドレスを属性タイプ/値のペアにバインドすることであるため、vCenter は、VMware ツールを実行していない VM のバインド情報を報告しません。

ESXi 環境内では、VM はプライマリ IP アドレスによって定義されます。これは ASA の管理 IP アドレスにほぼ対応します。VM ごとに設定可能なプライマリアドレスは 1 つのみです。IPv4 アドレスと IPv6 アドレスのいずれかを使用できます。バインドは、常にプライマリ IP アドレスと属性のタイプ/値のペアの間で設定されます。VM に複数の IP アドレス（IPv6 リンクローカルアドレスなど）が設定されている場合、vCenter は、プライマリアドレス（通常は最初に設定されたアドレス）のバインド更新のみを送信します。

（注） ユーザーは、一連の VM にカスタム属性のタイプと値を割り当てて、共通のユーザー定義の特性を持つ一連の VM に共通のポリシーセットを適用できます。

属性の包括的なリストと関連するガイドラインについては、VMware vCenter 5.5/6.0 のドキュメントを参照してください。

VM 属性ポリシーの設定

VM 属性に基づいてポリシーを設定するには、次の 3 つの手順があります。

ステップ 1 ネットワークオブジェクト属性を設定します。

a) [管理（Manage）] メニューから [ポリシーオブジェクト（Policy Objects）] を選択するか、ボタンバーの [Policy Object Manager] ボタンをクリックして、[Configuration Manager] ウィンドウの下部にある [Policy Object Manager] ペインを開きます。オブジェクトタイプセレクタから [ネットワーク/ホスト（Networks/Hosts）] を選択します。作業領域内を右クリックし、[新規オブジェクト（New Object）] > [属性（Attribute）] を選択します。ペインの下部にある [+] ボタンを使用して新しいネットワークオブジェクト属性を追加することもできます。

（注） ネットワーク属性オブジェクトは、object-group-search が有効になっている場合にのみ使用できます。

b) VM 属性エージェントを選択し、VM 属性タイプを指定して、VM 属性値の値を追加します。

ステップ 2 VM 属性エージェントを追加します。

a) VM 属性エージェントの名前を指定し、VM 属性エージェントの説明を追加します。
b) デフォルトでは、エージェントタイプは esxi です。
c) [DNS のホスト名/IP アドレス（DNS Host Name/IP Address）] フィールドに vCenter サーバーのプライマリ IP アドレスを入力します。
d) vCenter サーバーへの認証を受けるユーザー名とパスワードを指定します。

e) エージェントが vCenter サーバーに接続しているときに接続がアクティブな状態を維持する時間を指定します。再試行間隔のデフォルト値は 30 秒です。

f) [再試行回数（Retry Count）] フィールドで、エージェントが vCenter サーバーを非アクティブと宣言する前にサーバーへの接続を試行する回数を指定します。デフォルト値は 3 です。

g) OK をクリックします。

ステップ 3 VM 属性を使用してアクセスリストを設定します。詳細については、アクセス コントロール リスト オブジェクトの作成 （70 ページ）を参照してください。

（注） VM 属性は、アクセスリストオブジェクトのみをサポートします。

プールオブジェクトについて

プールオブジェクトには次の用途があります。

- ASA クラスタのレイヤ 3 ロードバランシングで使用するプールの指定
- ASA クラスタのレイヤ 3 EIGRP および OSPFv3 で使用するプールの指定

次の項では、プールオブジェクトを操作する方法について説明します。

- [IPv4プールの追加または編集（Add or Edit IPv4 Pool）] ダイアログボックス （121 ページ）
- [IPv6プールの追加または編集（Add or Edit IPv6 Pool）] ダイアログボックス （123 ページ）
- [MACアドレスプールの追加または編集（Add or Edit MAC Address Pool）] ダイアログボックス （124 ページ）
- [NETプールオブジェクトの追加/編集（Add or Edit NET Pool Object）] ダイアログボックス（125 ページ）
- [DHCPv6プールの追加または編集（Add or Edit DHCPv6 Pool）] ダイアログボックス （127 ページ）

[IPv4プールの追加または編集（Add or Edit IPv4 Pool）] ダイアログボックス

[IPv4プールの追加または編集（Add or Edit IPv4 Pool）] ダイアログボックスを使用して、IPv4 プールオブジェクトを表示、作成、または編集します。

ナビゲーション パス

[管理（Manage）] メニューから [ポリシーオブジェクト（Policy Objects）] を選択するか、ボタンバーの [Policy Object Manager] ボタンをクリックして、[Configuration Manager] ウィンドウの下部にある [Policy Object Manager] ペインを開きます。オブジェクトタイプセレクタから **[プールオブジェクト（Pool Objects ）] > [IPv4プールオブジェクト（IPv4 Pool Object）]** を選択し

ます。作業領域内で右クリックして [新規オブジェクト（New Object）] を選択し、オブジェクトタイプを選択するか、または行を右クリックして [オブジェクトの編集（Edit Object）] を選択します。ペインの下部にある関連するボタンを使用して、いずれかのダイアログボックスを開くこともできます。

関連項目

- Policy Object Manager （4 ページ）
- ポリシーのオブジェクトの選択 （2 ページ）

フィールド リファレンス

表 *32 : [IPv4プールオブジェクトの追加（Add IPv4 Pool Object）] ダイアログボックス*

要素	説明
名前	オブジェクト名（最大 64 文字）。オブジェクト名では、大文字と小文字が区別されません。詳細については、 ポリシー オブジェクトの作成 （13 ページ）を参照してください。
説明	（任意）オブジェクトの説明。
タイプ（Type）	プールオブジェクトが単一の IP アドレスであるか、IP アドレスの範囲であるかを選択します。
アドレス（Address）	オブジェクトに含める単一ホストの IPv4 アドレス。
開始アドレス（Start Address） 終了アドレス（End Address）	アドレスの範囲を定義する最初と最後の IP アドレス。開始アドレスと終了アドレスは異なっており、開始の方が終了よりも小さいアドレスである必要があります。
Mask	IP アドレスまたはアドレスの範囲のサブネットマスク。
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 （18 ページ）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 （25 ページ）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 （24 ページ）を参照してください。 （注） IPv4 プールオブジェクトは常にオーバーライド可能です。このオプションをクリアすると、エラーが発生します。 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。

[IPv6プールの追加または編集（Add or Edit IPv6 Pool）] ダイアログボックス

[IPv6プールの追加または編集（Add or Edit IPv6 Pool）] ダイアログボックスを使用して、IPv6 プールオブジェクトを表示、作成、または編集します。

ナビゲーション パス

[管理（Manage）] メニューから [ポリシーオブジェクト（Policy Objects）] を選択するか、ボタンバーの [Policy Object Manager] ボタンをクリックして、[Configuration Manager] ウィンドウの下部にある [Policy Object Manager] ペインを開きます。オブジェクトタイプセレクタから [プールオブジェクト（Pool Objects ）] > [IPv6プールオブジェクト（IPv6 Pool Object）] を選択します。作業領域内で右クリックして [新規オブジェクト（New Object）] を選択し、オブジェクトタイプを選択するか、または行を右クリックして [オブジェクトの編集（Edit Object）] を選択します。ペインの下部にある関連ボタンを使用して、いずれかのダイアログボックスを開くこともできます。

関連項目

- Policy Object Manager （4 ページ）
- ポリシーのオブジェクトの選択 （2 ページ）

フィールド リファレンス

表 *33 : [IPv6*プールオブジェクトの追加（*Add IPv6 Pool Object*）*]* ダイアログボックス

要素	説明
名前	オブジェクト名（最大 64 文字）。オブジェクト名では、大文字と小文字が区別されません。詳細については、ポリシー オブジェクトの作成 （13 ページ）を参照してください。
説明	（任意）オブジェクトの説明。
アドレス（Address）	オブジェクトに含めるアドレス/プレフィックス長形式の IPv6 アドレス。
メンバー数（Count）	プールに含めるアドレスの数。1 から 16384 の間である必要があります。
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 （18 ページ）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 （25 ページ）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 （24 ページ）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。

[MACアドレスプールの追加または編集（AddorEditMACAddressPool）] ダイアログボックス

[MACアドレスプールの追加または編集（Add or Edit MAC Address Pool）] ダイアログボックスを使用して、MAC アドレスプールオブジェクトを表示、作成、または編集します。

ナビゲーション パス

[管理（Manage）] メニューから [ポリシーオブジェクト（Policy Objects）] を選択するか、ボタンバーの [Policy Object Manager] ボタンをクリックして、[Configuration Manager] ウィンドウの下部にある [Policy Object Manager] ペインを開きます。オブジェクトタイプセレクタから **[プールオブジェクト（Pool Objects ）] > [MACアドレスプールオブジェクト（MAC Address Pool Object）]** を選択します。作業領域内で右クリックして [新規オブジェクト（New Object）] を選択し、オブジェクトタイプを選択するか、または行を右クリックして [オブジェクトの編集

（Edit Object）] を選択します。ペインの下部にある関連するボタンを使用して、いずれかのダイアログボックスを開くこともできます。

関連項目

- Policy Object Manager （4 ページ）
- ポリシーのオブジェクトの選択 （2 ページ）

フィールド リファレンス

表 *34 : [MAC*アドレスプールの追加（*Add MAC Address Pool*）*]*ダイアログボックス

要素	説明
名前	オブジェクト名（最大 64 文字）。オブジェクト名では、大文字と小文字が区別されません。詳細については、ポリシー オブジェクトの作成 （13 ページ）を参照してください。
説明	（任意）オブジェクトの説明。
開始MACアドレス（Start MAC Address） 終了MACアドレス（End MAC Address）	アドレスの範囲を定義する最初と最後の MAC アドレス。開始アドレスと終了アドレスは異なっており、開始の方が終了よりも小さいアドレスである必要があります。
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 （18 ページ）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 （25 ページ）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 （24 ページ）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。

[NETプールオブジェクトの追加/編集（Add or Edit NET Pool Object）] ダイアログボックス

[NETプールオブジェクトの追加または編集（Add or Edit NET Pool Object）] ダイアログボックスを使用して、Network Entity Title プールオブジェクトを表示、作成、または編集します。

ナビゲーション パス

[管理（Manage）] メニューから [ポリシーオブジェクト（Policy Objects）] を選択するか、ボタンバーの [Policy Object Manager] ボタンをクリックして、[Configuration Manager] ウィンドウの下部にある [Policy Object Manager] ペインを開きます。オブジェクトタイプセレクタから **[プールオブジェクト（Pool Objects）] > [NETプールオブジェクト（NET Pool Object）]** を選択します。作業領域内で右クリックして [新規オブジェクト（New Object）] を選択し、オブジェクトタイプを選択するか、または行を右クリックして [オブジェクトの編集（Edit Object）] を選択します。ペインの下部にある関連ボタンを使用して、いずれかのダイアログボックスを開くこともできます。

関連項目

- Policy Object Manager （4 ページ）
- ポリシーのオブジェクトの選択 （2 ページ）

フィールド リファレンス

表 *35 : [NETプールオブジェクトの追加（Add NET Pool Object）] ダイアログボックス*

要素	説明
名前	オブジェクト名（最大 64 文字）。オブジェクト名では、大文字と小文字が区別されません。詳細については、ポリシー オブジェクトの作成 （13 ページ）を参照してください。
説明	（任意）オブジェクトの説明。
開始NETアドレス（Start NET Address） 終了 NET アドレス（End NET Address）	アドレスの範囲を定義する最初と最後の NET アドレス。開始アドレスと終了アドレスは異なっており、開始の方が終了よりも小さいアドレスである必要があります。
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 （18 ページ）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 （25 ページ）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 （24 ページ）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。

[DHCPv6プールの追加または編集（Add or Edit DHCPv6 Pool）] ダイアログボックス

このダイアログボックスを使用して、DHCPv6 サーバープールを追加または編集します。ステートレスアドレス自動設定（SLAAC）をプレフィックス委任機能と併用するクライアントについては、クライアントが情報要求（IR）パケットを ASA に送信する際に情報（DNS サーバー、ドメイン名など）を提供するように ASA を設定できます。ASA は、IR パケットを受け取るだけで、クライアントにアドレスを割り当てません。

ナビゲーション パス

- [管理（Manage）] メニューから [ポリシーオブジェクト（Policy Objects）] を選択するか、ボタンバーの [Policy Object Manager] ボタンをクリックして、[Configuration Manager] ウィンドウの下部にある [Policy Object Manager] ペインを開きます。オブジェクトタイプセレクタから **[プールオブジェクト（Pool Objects）] > [DHCPv6プールオブジェクト（DHCPv6 Pool Object）]** を選択します。作業領域内で右クリックして [新規オブジェクト（New Object）] を選択し、オブジェクトタイプを選択するか、または行を右クリックして [オブジェクトの編集（Edit Object）] を選択します。ペインの下部にある関連するボタンを使用して、いずれかのダイアログボックスを開くこともできます。

または

- [DHCPv6プールの追加（Add DHCPv6 Pool）] ダイアログボックスには、[DHCPv6プールセレクタ（DHCPv6 Pool Selector）] ダイアログボックスからアクセスできます。[使用可能なDHCPv6プール（Available DHCPv6 Pool）] テーブルの下にある [行の追加（Add Row）] または[行の編集（Edit Row）]ボタンをクリックします。[DHCPv6プールセレクタ（DHCPv6 Pool Selector）] ダイアログボックスには、[インターフェイスの追加（Add Interface）] および [インターフェイスの編集（Edit Interface）] ダイアログボックスの [IPv6] パネルの [インターフェイスIPv6 DHCP（Interface IPv6 DHCP）] セクションにある [サーバープール（Server Pool）] オプションボタンからアクセスできます。

関連項目

- [IPv6 Address for Interface] ダイアログボックス
- [インターフェイスの追加/編集（Add/Edit Interface）] ダイアログボックス（PIX 7.0 以降/ASA/FPR/FWSM）
- デバイス インターフェイス、ハードウェア ポート、ブリッジ グループの管理
- Policy Object Manager （4 ページ）
- ポリシーのオブジェクトの選択 （2 ページ）

フィールド リファレンス

表 *36 : [DHCPv6プールの追加（Add DHCPv6 Pool）] ダイアログボックス*

要素	説明
名前	DHCPv6 プール名は 200 文字までです。オブジェクト名では、大文字と小文字が区別されません。 詳細については、ポリシー オブジェクトの作成 （13 ページ）を参照してください。
• 1 つ以上のタブでパラメータを設定し、IR メッセージに対する応答をクライアントに提供します。 • タブごとに、必要に応じて次の内容を指定します。 • DNS/SIP/NIS/NISP/SNTP サーバー：サーバー名を入力します。IPv6 アドレスが正しい形式であることを確認してください。IPv6 アドレス形式の詳細については、http://www.ietf.org/rfc/rfc2373.txt を参照してください。 • DNS/SIP/NIS/NISP ドメイン名：ドメイン名を入力します。ドメイン名の先頭と末尾は数字または文字にする必要があります。内部文字として使用できるのは文字、数字、ハイフンのみです。ラベルはドットで区切ります。各ラベルは最大 63 文字で、ホスト名全体は最大 255 文字です。ドメイン名形式の詳細については、http://www.ietf.org/rfc/rfc1123.txt を参照してください。 （注） import コマンドは、プレフィックス委任クライアント インターフェイスで ASA が DHCPv6 サーバから取得した 1 つ以上のパラメータを使用します。手動で設定されたパラメータとインポートされたパラメータを組み合わせて使用できますが、同じコマンドを手動と import コマンドで設定することはできません。	
[サーバ（Server）] タブ	（任意）DNS サーバー名とドメイン名を指定します。
[SIP] タブ	（任意）SIP サーバー名と SIP ドメイン名を指定します。
[NIS] タブ	（任意）NIS サーバー名と NIS ドメイン名を指定します。
[NISP] タブ	（任意）NISP サーバー名と NISP ドメイン名を指定します。
[SNTP] タブ	（任意）SNTP サーバー名を指定します。
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 （18 ページ）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 （25 ページ）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 （24 ページ）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。

SAML ID プロバイダの構成

バージョン 4.10 以降、Security Manager では、ASA VPN の Security Assertion Markup Language（SAML）2.0 ベースのシングルサインオンおよびシングルログアウトを設定できます。シングルサインオンサーバーの設定は、ASA バージョン 9.5(2) からサポートされなくなりました。これは SAML ID プロバイダーに置き換えられました。

セキュリティ アサーション マークアップ言語（SAML）は、当事者間、特に ID プロバイダーとサービスプロバイダーの間で認証および許可データを交換するための XML ベースのオープン標準のデータ形式です。アイデンティティプロバイダーは、ユーザーのアイデンティティを別のリソースにアサートできるサービスです。アイデンティティ プロバイダーは、アイデンティティ管理システムでユーザーを認証する責任があります。サービスプロバイダーは、ユーザーがアクセスするサービスです（パブリックまたはプライベート Web アプリケーションなど）。

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 [SAML IDプロバイダー（SAML Identity Provider）] を選択します。

SAML アイデンティティ プロバイダーの追加または編集

[SAMLアイデンティティプロバイダーの追加または編集（Add or Edit SAML Identity Provider）] ダイアログボックスを使用して、新しい SAML アイデンティティプロバイダーを追加するか、既存の行を編集します。

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 [SAMLアイデンティティプロバイダー（SAML Identity Provider）] を選択し

ます。作業領域内を右クリックして [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 [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 *37 : [SAML*アイデンティティプロバイダーの追加または編集（*Add or Edit SAML Identity Provider*）*]*

要素	説明
名前	SAML アイデンティティ プロバイダーの名前を 4 ～ 256 文字で入力します。
説明	（任意）SAML アイデンティティ プロバイダーの説明を入力します。
[サインインURL（Sign In URL）]	このURLは、アイデンティティプロバイダーへのサインインに使用されます。http:// またはhttps:// を先頭に付けます（大文字と小文字は区別されません）。サインイン URL の長さは 500 文字以下にする必要があります。[サインインURL（Sign In URL）] フィールドでは、次の特殊文字のみを使用できます。 :、/、*、[、]、.
[サインアウトURL（Sign Out URL）]	（任意）このURLは、アイデンティティプロバイダーからサインアウトする際のリダイレクトに使用されます。http:// またはhttps:// を先頭に付けます（大文字と小文字は区別されません）。サインアウト URL の長さは 500 文字以下にする必要があります。[サインアウトURL（Sign Out URL）] フィールドでは、次の特殊文字のみを使用できます。 :、/、*、[、]、.
[ベースURL（Base URL）]	（任意）クライアントレスVPNのベースURLです。このURLは、サードパーティ製アイデンティティ プロバイダーに提供される SAML メタデータで使用されます。そうすることで、アイデンティティ プロバイダーはエンドユーザーを ASA にリダイレクトできます。ベース URL が設定されていない場合は、ASA デバイスのホスト名とドメイン名から取得されます。たとえば、ホスト名が ssl-vpn でドメイン名が xyz の場合、使用されるベース URL は https://ssl-vpn.xyz.com になります。http:// または https:// をベース URL の先頭に付けます（大文字と小文字は区別されません）。ベース URL の長さは 500 文字以下にする必要があります。[ベースURL（Base URL）] フィールドでは、次の特殊文字のみを使用できます。 :、/、*、[、]、. （注） SAMLを設定するには、ベースURLまたはドメイン名のいずれかを ASA デバイスで設定する必要があります。

要素	説明
アイデンティティ プロバイダー	[CAサーバーセレクタ（CA Servers Selector）] ダイアログボックスから [アイデンティティプロバイダー（Identity Provider）] を選択します。アイデンティティ プロバイダーは、ユーザーのアイデンティティを別のリソースにアサートできるサービスです。アイデンティティ プロバイダーは、アイデンティティ管理システムでユーザーを認証する責任があります。
サービス プロバイダー	（任意）[CAサーバーセレクタ（CA Servers Selector）] ダイアログボックスから [サービスプロバイダー（Service Provider）] を選択します。サービスプロバイダーは、ユーザーがアクセスするサービスです（パブリックまたはプライベート Web アプリケーションなど）。
要求のタイムアウト（Request Timeout）	（任意）1 ～ 7200 の値を入力します。デフォルトでは、SAML タイムアウトは設定されていません。
Enable Signature	（任意）SAML 要求内の署名を有効または無効にします。これが有効になっている場合は、サービスプロバイダーを設定する必要があります。 [認証要求（Authentication Request）] ドロップダウンで署名用の暗号スイートを選択します。署名を有効にすると、SHA-256 暗号スイートがデフォルトで選択されます。暗号スイートは、[認証要求（Authentication Request）] ドロップダウンで変更できます。デフォルトでは、署名は無効になっており、[認証要求（Authentication Request）] ドロップダウンは非表示になっています。 （注） SAML署名の認証要求を指定できるのは、ASA 9.8.1 以降のみです。
[内部の有効化（Enable Internal）]	（任意）SAML アイデンティティ プロバイダーの内部フラグを有効または無効にします。有効にすると、内部フラグはプライベートネットワーク内のアイデンティティ プロバイダーを識別するようになり、SAML アイデンティティ プロバイダーには WebVPN 接続を介してのみアクセスできます。これは、ASA がゲートウェイとして機能することも意味します。 デフォルトでは、内部フラグは無効になっており、アイデンティティ プロバイダーに直接アクセスできます。
[再認証の強制の有効化（Enable Force Re-Authentication）]	（任意）SAML アイデンティティ プロバイダーの再認証の強制を有効または無効にします。有効にすると、アイデンティティ プロバイダーは、以前のセキュリティコンテキストに依存するのではなく、プレゼンタを直接認証する必要があります。 デフォルトでは、[再認証の強制（Force Re-Authentication）] フラグが有効になっています。

要素	説明
カテゴリ	（任意）CAT-A ～ CAT-J の間でカテゴリを選択します。
デバイスごとに値のオーバーライドを許可	（任意）[デバイスごとに値のオーバーライドを許可（Allow Value Override per Device）] が選択されている場合は、[オーバーライド（Overrides）] を編集します。

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

Security Manager の多くのポリシーでは、ポリシーが適用されるサービスを識別する必要があります。サービスは、プロトコルと、特定のタイプのトラフィックを識別するポート定義です。多くの場合、サービスはポリシー内に直接指定できます。必要なサービスを定義するサービス ポリシー オブジェクトを選択するか、サービス オブジェクトとポリシー固有のサービス指定の組み合わせを使用することもできます。

サービス オブジェクトを使用すると、特定のアプリケーションの構成を表すオブジェクトを作成したり、ネットワーク上に存在する論理組織（開発チームや企業部門など）を基にしてオブジェクトをモデル化したりできるため、サービス オブジェクトは有用です。次の 2 つのタイプのサービス ポリシー オブジェクトがあります。

- サービス グループ：1 つ以上のサービス（他のサービス オブジェクトを含む）を含めることができます。これは、すべての Security Manager 3.x リリースで使用可能だったサービス オブジェクトのタイプです。
- サービス オブジェクト：1 つのサービスを含めることができます。

サービスを識別する必要があるポリシーを設定するときに、[サービス（Services）] フィールドの横の [選択（Select）] ボタンをクリックして、サービスオブジェクトを選択または作成できます。選択ダイアログボックスから新しいサービスを作成するには、サービスリストの下の [追加（Add）] ボタンをクリックし、タイプ（グループまたはオブジェクト）を選択します。コンテンツテーブルから **[サービス（Services）]>[サービス（Services）]** を選択し、[オブジェクトの追加（Add Object）] ボタンをクリックし、グループまたはオブジェクトを選択することによって、[Policy Object Manager] からサービスを作成することもできます。サービス オブジェクトを作成するときに使用できる特定のフィールドについては、サービス オブジェクトの設定 （136 ページ）を参照してください。

Security Manager には、定義済みのサービス グループ オブジェクトの包括的なコレクションがあります。HTTP、Syslog、POP3、Telnet、SNMP など、一般的に使用されるサービス用の ICMP メッセージおよびオブジェクトが含まれています。定義済みのサービス グループ オブジェクトを使用する前に、オブジェクト定義を確認して、使用しているネットワーク実装に準拠していることを確認する必要があります。定義済みのオブジェクトがニーズに合わない場合（別の宛先ポートが必要な場合など）、新しいサービス オブジェクトを最初から作成するか、既存の

オブジェクトのコピーを基に作成できます。詳細については、オブジェクトのクローニング（複製） （19 ページ）を参照してください。

サービス オブジェクトを作成する場合もポリシー内にサービスを直接指定する場合も、次の形式を使用してサービスを指定できます。入力に応じて、Security Manager によってエントリに関連するテキストコンプリート オプションが示される場合があります。リストから値を選択して、Enter または Tab を押します。複数のサービスをカンマで区切って入力できます。

- *protocol*：プロトコルは、1 ～ 255 または tcp、udp、gre、icmp などの広く知られているプロトコル名です。数字を入力すると、その数字は関連付けられている名前に変換されます。
- **icmp**/*message_type* /*message_code* ：メッセージタイプは 1 ～ 255 またはエコーなどの既知の ICMP メッセージタイプ名であり、メッセージコードは 0 ～ 255 です（たとえば、**icmp/unreachable/1** または **icmp/echo-reply**）。
- **icmp6**/*message_type* /*message_code* ：メッセージタイプは 1 ～ 255 またはエコーなどの既知の ICMP メッセージタイプ名であり、メッセージコードは 0 ～ 255 です（たとえば、**icmp6/unreachable/1** または **icmp6/echo-reply**）。
- **{tcp | udp | tcp&udp}/**{*destination_port_number* | *port_list_object* }：宛先ポート番号は、1 ～ 65535 またはポートリストオブジェクトの名前です。ハイフンを使用してポート範囲を入力できます（たとえば、10-20）。送信元ポート番号は、Default Range ポート リスト オブジェクトです。Default Range オブジェクトには、[Policy Objects] ページ（[ツール（Tools）] > [Security Manager管理（Security Manager Administration）] > [ポリシーオブジェクト（Policy Objects）] を選択）で選択した設定に応じて、すべてのポート（1 ～ 65535）またはすべてのセキュアポート（1024 ～ 65535）が含まれています。

たとえば、サービスを tcp/10 として定義すると、10 が宛先ポートであり、送信元ポートは定義されないことを意味します。

ポートを指定するときに、番号の前に特別なキーワード **lt**（より小さい）、**gt**（より大きい）、**eq**（等しい）、および **neq**（等しくない）を使用することもできます。たとえば、**lt 440** と入力すると、440 未満のすべてのポートが指定されます。

ヒント　ポートリストオブジェクトを作成するには、[Policy Object Manager] で **[サービス（Services）] > [ポートリスト（Port Lists）]** を選択し、[オブジェクトの追加（Add Object）] ボタンをクリックします。詳細については、ポート リスト オブジェクトの設定 （134 ページ）を参照してください。

- **{tcp | udp | tcp&udp}/**{*source_port_number* | *port_list_object* }/ {*destination_port_number* | *port_list_object* }：送信元ポート番号および宛先ポート番号は、1 ～ 65535 またはポートリストオブジェクトの名前です。ハイフンを使用してポート範囲を入力できます（たとえば、10-20）。

たとえば、サービスを tcp/10/20 として定義すると、10 が送信元ポート、20 が宛先ポートであることを意味します。宛先ポートを指定しない場合は、Default Range ポート リスト オブジェクトを使用します。tcp/10/Default Range などです。

- （サービスグループのみ）*service_object_name*：別の既存のサービスオブジェクトの名前。他のオブジェクトを指定する場合、オブジェクト定義を入れ子にすることができます。[選択（Select）]をクリックしてサービス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。

IOS デバイスにのみ適用される次の ICMP メッセージタイプは、ASA/PIX/FWSM デバイスでサポートされる ICMP メッセージタイプに自動的に置き換えられます。

- ICMP-Mobile-Redirect
- ICMP-Host-Unreachable
- ICMP-Network-Redirect
- ICMP-Port-Unreachable
- ICMP-Protocol-Unreachable
- ICMP-Reassembly-Timeout
- ICMP-Redirect
- ICMP-protocol-redirect

関連項目

- ポリシーのオブジェクトの選択　（2 ページ）
- ポリシー オブジェクトの作成　（13 ページ）
- オブジェクトの編集　（17 ページ）
- カテゴリ オブジェクトの使用　（18 ページ）
- サービス オブジェクトがオブジェクト グループとしてプロビジョニングされる方法　（143 ページ）
- オブジェクト オーバーライドの管理　（23 ページ）
- ポリシー オブジェクトの上書きの許可　（25 ページ）

ポート リスト オブジェクトの設定

[Port List] ダイアログボックスを使用して、ポート リスト オブジェクトを作成、編集、またはコピーします。各ポート リスト オブジェクトには、1 つ以上のポートまたはポート範囲（1-1000 や 2000-2500 など）を含めることができます。また、ポート リスト オブジェクトに他のポート リスト オブジェクトを含めることもできます。

通常はサービスを定義するときにポート リスト オブジェクトを使用しますが、ポート番号を入力しないで、ポートを識別するためにさまざまなポリシーで使用することもできます。サービス定義でのポート リストの使用の詳細については、サービスとサービス オブジェクトおよびポート リスト オブジェクトの理解と指定 （132 ページ）を参照してください。

ヒント 定義済みの Default Range ポートリストオブジェクトには、[Security Manager管理（Security Manager Administration）] ウィンドウ（[ツール（Tools）] > [Security Manager管理（Security Manager Administration）] > [ポリシーオブジェクト（Policy Objects）] を選択。[Policy Objects] ページを参照）で選択した設定に応じて、すべてのポート（1 ～ 65535）またはすべてのセキュアポート（1024 ～ 65535）が含まれます。

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 [サービス（Services）] > [ポートリスト（Port Lists）] を選択します。作業領域内を右クリックして [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 [オブジェクトの編集（Edit Object）] を選択します。

関連項目

- 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 （132 ページ）
- サービス オブジェクトの設定 （136 ページ）

フィールド リファレンス

表 *38 : [Port List]* ダイアログボックス

要素	説明
名前	最大 128 文字のオブジェクト名。オブジェクト名では、大文字と小文字が区別されません。詳細については、ポリシー オブジェクトの作成 （13 ページ）を参照してください。
説明	（任意）オブジェクトの説明。

要素	説明
ポート	ポート リスト オブジェクトに含まれるポートまたは範囲。443 や 1-1000 など。単一ポート、ポートの範囲、複数のポート範囲、または単一ポートと範囲の組み合わせを定義できます。複数のエントリを指定する場合は、カンマで区切ります。ポート値の範囲は 1 ～ 65535 です。 次の演算子を使用して範囲を指定できます。 • **gt**：より大きい。gt 1000 など。 • **lt**：より小さい。lt 1000 など。 • **eq**：等しい。eq 1000 など。ただし、**eq 1000** は単純に **1000** と入力するのと同じ意味です。 • **neq**：等しくない。neq 1000 など。 この演算子を使用する場合、[Ports] フィールドでは neq 値だけを使用できます。ただし、オブジェクトにポート範囲を含めることができます。したがって、1150 を除く 1000 ～ 1200 のすべてのポートを指定するオブジェクトを作成する場合は、1000 ～ 1200 の範囲のポート リスト オブジェクトと、neq 1150 を指定し、さらにそのポート リスト オブジェクトを含む別のオブジェクトを作成します。
Port Lists	オブジェクトに含める他のポートリストオブジェクト（ある場合）。ポートリス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。複数のエントリを指定する場合は、カンマで区切ります。
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 （18 ページ）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 （25 ページ）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 （24 ページ）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。

サービス オブジェクトの設定

[Add Service]/[Edit Service] ダイアログボックスを使用して、サービス オブジェクトを作成または編集します。サービス オブジェクトを作成して、ネットワーク内のデバイスによって伝送さ

れるトラフィックのタイプを記述できます。サービス オブジェクトを作成するときは、サービスによって使用されるプロトコルを指定する必要があります。

サービス オブジェクトを作成するときは、オブジェクト タイプを選択する必要があります。

- サービス グループ：1 つ以上のサービス（他のサービス オブジェクトを含む）を含めることができます。これは、すべての Security Manager 3.x リリースで使用可能なサービス オブジェクトのタイプです。
- サービス オブジェクト：1 つのサービスを含めることができます。

Security Manager には、定義済みのサービス グループ オブジェクトが数多く用意されています。オブジェクトを作成する前に、Policy Object Manager でリストを参照し、既存のオブジェクトがニーズに合うかどうかを確認します。定義済みのオブジェクトは複製できますが、編集することはできません。

Cisco Security Manager は、show running configuration で使用可能な定義を持つサービスオブジェクトをサポートします。定義済みオブジェクトの場合、定義を show running configuration で使用することはできません。そのため、ASA デバイスの定義済みオブジェクトを使用して設定されたポリシーは、Cisco Security Manager では検出されません。

デバイスの動作に合わせるために、Cisco Security Manager バージョン 4.17 で、定義済みオブジェクトのサポートが導入されました。新しい定義済みサービスオブジェクトが ASA に追加されるたびにデバイスがそのオブジェクトを使用して更新される場合、ASA 定義済みオブジェクトが検出されます。この機能は、イメージをサポートするすべてのバージョンの ASA でサポートされています。

（注） PPTP の定義済みオブジェクトはサポートされていません。

ただし、Cisco Security Manager は、ASA バージョンに関するアクティビティの検証をサポートしていません。また、Cisco Security Manager の ICMP および ICMPv6 の定義済みオブジェクトは、デバイスの定義済みオブジェクトに変換されます。したがって、Cisco Security Manager の定義済みオブジェクトを使用すると、そのポリシーが無効になり再作成されます。

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 [サービス（Services）] > [サービス（Services）] を選択します。作業領域内を右クリックして [新規オブジェクト（New Object）] を選択するか（その後オブジェクトタイプを選択）、行を右クリックして [オブジェクトの編集（Edit Object）] を選択します。

関連項目

- 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 （132 ページ）
- Policy Object Manager （4 ページ）

フィールド リファレンス

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

要素	説明
名前	オブジェクト名。ソフトウェア バージョン 8.x を実行する ASA または PIX デバイス用のオブジェクトを使用する場合は、名前の長さを 64 文字に制限します。その他のデバイスの場合、名前は最大 128 文字です。 オブジェクト名では、大文字と小文字が区別されません。詳細については、ポリシー オブジェクトの作成 （13 ページ）を参照してください。
説明	（任意）オブジェクトの説明。
Services（グループの場合） Service（オブジェクトの場合）	このポリシー オブジェクトに含めるサービス。サービス グループを作成する場合、複数のサービスをカンマで区切って入力できます。サービス オブジェクトを作成する場合、1 つのサービスだけを入力できます。 次の形式を使用して、サービスを指定できます。入力に応じて、Security Managerによってエントリに関連するテキストコンプリート オプションが示される場合があります。定義済みのサービス オブジェクトに直接変換されるサービスを入力した場合、エントリは定義済みのオブジェクト名に変換されます。たとえば、TCP/80 は HTTP に変換されます。 • *protocol*：プロトコルは、1 ～ 255 または tcp、udp、gre、icmp などの広く知られているプロトコル名です。数字を入力すると、その数字は関連付けられている名前に変換されます。 • **icmp/***message_type* /*message_code* ：メッセージタイプは 1 ～ 255 またはエコーなどの既知のICMPメッセージタイプ名であり、メッセージコードは 0 ～ 255 です（たとえば、**icmp/unreachable/1** または **icmp/echo-reply**）。 • **icmp6/***message_type* /*message_code* ：メッセージタイプは 1 ～ 255 またはエコーなどの既知のICMPメッセージタイプ名であり、メッセージコードは 0 ～ 255 です（たとえば、**icmp6/unreachable/1** または **icmp6/echo-reply**）。

要素	説明
	• **{tcp | udp | tcp&udp}/**{*destination_port_number* | *port_list_object*}：宛先ポート番号には、1 ～ 65535 またはポートリストオブジェクトの名前を指定できます。ハイフンを使用してポート範囲を入力できます（たとえば、10-20）。この場合には、送信元ポート番号は、Default Range ポート リスト オブジェクト（1 ～ 65535 の範囲を指定）です（ポート リスト オブジェクトの作成および編集については、ポート リスト オブジェクトの設定 （134 ページ）を参照してください）。 ポートを指定するときにはいつでも、番号の前に特別なキーワード**lt**（より小さい）、**gt**（より大きい）、**eq**（等しい）、および **neq**（等しくない）を使用することもできます。たとえば、**lt 440** と入力すると、440 未満のすべてのポートが指定されます。 • **{tcp | udp | tcp&udp}/**{*source_port_number* | *port_list_object* }/{*destination_port_number* | *port_list_object*}：送信元ポート番号および宛先ポート番号には、1 ～ 65535 またはポートリストオブジェクトの名前を指定できます。ハイフンを使用してポート範囲を入力できます（たとえば、10-20）。 • （サービスグループのみ）*service_object_name* ：別の既存のサービスオブジェクトの名前。他のオブジェクトを指定する場合、オブジェクト定義を入れ子にすることができます。[選択（Select）]をクリックしてサービス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（18 ページ）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 （25 ページ）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 （24 ページ）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。

IOS デバイスにのみ適用される次の ICMP メッセージタイプは、ASA/PIX/FWSM デバイスでサポートされる ICMP メッセージタイプに自動的に置き換えられます。

- ICMP-Mobile-Redirect
- ICMP-Host-Unreachable
- ICMP-Network-Redirect
- ICMP-Port-Unreachable

- ICMP-Protocol-Unreachable
- ICMP-Reassembly-Timeout
- ICMP-Redirect
- ICMP-protocol-redirect

ポリシーオブジェクトがオブジェクトグループとしてプロビジョニングされる方法

オブジェクト グループは、ASA、PIX、FWSM、および IOS 12.4(20)T 以降のデバイスの機能であり、IP ホスト、ネットワーク、プロトコル、ポート、ICMP メッセージ タイプなどのオブジェクトをグループ化することによって、アクセス ルールのサイズを減らすことができます。オブジェクト グループの機能は Security Manager のポリシー オブジェクトの機能と似ていますが、実装において重要な違いがいくつかあります。

このため、ポリシーをデバイスに展開するときに、Security Manager で設定したポリシー オブジェクトの正確なコピーであるオブジェクト グループを作成できるとはかぎりません。たとえば、ポリシー オブジェクト名は Security Manager ではオブジェクト タイプごとに一意ですが（つまり、ネットワーク/ホスト オブジェクトとサービス オブジェクトを同じ名前で定義できます）、デバイス上で定義されるすべてのタイプのオブジェクト グループは、1 つの命名方式を共有します。したがって、デバイス上の既存のサービス オブジェクト グループと名前が一致するネットワーク/ホスト オブジェクトを展開する場合、サービス オブジェクト グループと区別するために、ネットワーク/ホスト オブジェクトの名前にサフィックスが付加されます。

（注） オブジェクト グループを展開するときに使用できるオプションについては、[Deployment] ページを参照してください。

同様に、デバイス上のポリシーを検出するときに、デバイス上で設定されたオブジェクト グループの正確なコピーであるポリシー オブジェクトを作成できるとはかぎりません。ただし、元の設定は Security Manager によって可能なかぎり保持されます。

（注） IOS デバイスの場合、アクセス コントロール リスト オブジェクトによって使用されるポリシー オブジェクトは、あとで展開中にオブジェクトのコンテンツによって置き換えられます。ACL オブジェクトで使用されるオブジェクト グループは保持されませんが、Security Manager ポリシー オブジェクトとして検出されます。

次の項では、ポリシー オブジェクトをデバイス上のオブジェクト グループにプロビジョニングするとき、またはこれらのデバイス上のポリシーの検出時にポリシー オブジェクトを作成するときに行われる変更について説明します。

ネットワーク/ホスト オブジェクト、ポート リスト オブジェクト、およびサービスオブジェクトがオブジェクトグループとしてプロビジョニングされるときの命名方法

ほとんどの場合、ネットワーク/ホスト オブジェクト、ポート リスト オブジェクト、およびサービス オブジェクトは、オブジェクト名が変更されることなく、オブジェクト グループとしてプロビジョニングされます。次のテーブルに、サポート対象デバイス上のオブジェクトグループにオブジェクト名を直接変換できない場合に、名前が変更される方法を示します。

（注） 定義済みのネットワーク/ホストオブジェクト **any** は、オブジェクトグループとしてプロビジョニングされません。

表 *40*：ネットワーク/ホスト オブジェクト、ポート リスト オブジェクト、およびサービス オブジェクトのオブジェクト グループとしての命名方法

条件	新しい名前（New Name）	例
オブジェクト名にスペースが含まれている。	スペースはアンダースコアに置き換えられます。	**my object** という名前のオブジェクトは、**my_object** という名前のオブジェクトグループとしてプロビジョニングされます。
オブジェクト名の長さが 64 文字（オブジェクト グループでサポートされる最大）を超えている。	64 文字の制限内に収めながらオブジェクト グループで必要とされるサフィックス（_TCP や _UDP など、または _1 などの一意の番号）を付加できるように、名前は切り捨てられます。	

条件	新しい名前（New Name）	例
デバイスにすでに同じ名前のオブジェクト グループ（プロトコル/ICMP/サービス）がある。	数値のサフィックスが1から順に名前に付加されます。	**West** という名前のネットワーク/ホストオブジェクトがあり、デバイスに **West** という名前の TCP サービス オブジェクト グループがすでにある場合、展開時にオブジェクトグループの名前は **West_1** に変更されます。
同じ名前のネットワーク/ホスト オブジェクト グループがすでに作成されている。	数値のサフィックスが1から順に名前に付加されます。	どちらも **West** という名前のネットワーク/ホストオブジェクトとポートリストまたはサービスオブジェクトがある場合、ネットワーク/ホストオブジェクトは **West** として展開され、ポートリストは **West_1** として展開されます。

（注） ASA ソフトウェアバージョン 8.2 以前の場合、Security Manager でネットワーク オブジェクト タイプのオブジェクトを作成する場合、オブジェクト名は同じでネットワーク オブジェクト グループ タイプのオブジェクトを持つ ASA デバイスを検出すると、Security Manager は新しいオブジェクトを作成しません。代わりに、既存のオブジェクトを再利用します。ただし、ASA ソフトウェアバージョン 8.3 以降では、Security Manager でネットワーク オブジェクト タイプのオブジェクトを作成する場合、オブジェクト名は同じでネットワーク オブジェクト グループ タイプのオブジェクトを持つ ASA デバイスを検出すると、Security Manager は、name_1、name_2 などのような新しいオブジェクトを作成します。これは、ソフトウェアバージョン 8.2 以前を実行している ASA デバイスを管理する Security Manager の場合、ASA をバージョン 8.3 以降にアップグレードすると、新しいオブジェクトが作成されることを意味します。

関連項目

- ネットワーク/ホストオブジェクトについて （105 ページ）
- 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 （132 ページ）
- サービス オブジェクトがオブジェクト グループとしてプロビジョニングされる方法 （143 ページ）
- ポリシー オブジェクトがオブジェクト グループとしてプロビジョニングされる方法 （140 ページ）

サービス オブジェクトがオブジェクト グループとしてプロビジョニングされる方法

次の表に、サービス オブジェクトをサポート対象デバイスに展開するときに、Security Manager によってオブジェクト グループが作成される方法を示します。

ヒント ASA 8.3 以降のデバイスの場合、サービスオブジェクトは **object-group** コマンドではなく **object service** コマンドを使用してプロビジョニングされます。

表 *41* : サービス オブジェクトがオブジェクト グループとしてプロビジョニングされる方法

条件	生成されるオブジェクト グループ	例

サービス オブジェクトに ICMP プロトコルおよび ICMP メッセージ タイプが含まれている。	ICMP タイプのオブジェクト グループがサービス オブジェクトと同じ名前で生成されます。	サービスオブジェクト service1：**icmp/icmp-echo, 23**
		オブジェクト グループ：
		`object-group icmp-type service1`
		`  icmp-object icmp-echo`
		`  icmp-object 23`

サービス オブジェクトにプロトコルだけが含まれている。	プロトコル オブジェクト グループがサービス オブジェクトと同じ名前で生成されます。	サービスオブジェクト service1：**tcp, gre, 34**
		オブジェクト グループ：
		`object-group protocol service1`
		`  protocol-object tcp`
		`  protocol-object gre`
		`  protocol-object 34`

サービス オブジェクトにより、送信元ポートと宛先ポート両方のポート リスト オブジェクトが使用されている。	ポート リスト オブジェクトと一致するサービス オブジェクト グループが生成されます。	

サービス オブジェクトに複数のポートまたはポート範囲が含まれているが、送信元ポートのポート リスト オブジェクトは使用されていない。	送信元ポートの <ObjectName>.src という名前のサービス オブジェクト グループが生成されます。	サービスオブジェクト serv1：**tcp/400,600/23-80**
		オブジェクト グループ：
		`object-group service serv1.src tcp`
		`  port-object eq 400`
		`  port-object eq 600`

条件	生成されるオブジェクト グループ	例

サービス オブジェクトに複数のポートまたはポート範囲が含まれているが、宛先ポートのポート リスト オブジェクトは使用されていない。	宛先ポートのサービス オブジェクト グループがサービス オブジェクトと同じ名前で生成されます。	サービスオブジェクト serv1：
		tcp/400,600/23-80, 566
		オブジェクト グループ：
		`object-group service serv1 tcp`
		`  port-object range 23 80`
		`  port-object eq 566`
		`object-group service serv1.src tcp`
		`  port-object eq 400`
		`  port-object eq 600`

サービス オブジェクトに TCP&UDP プロトコルが含まれており、定義済みのポートが含まれている。		サービスオブジェクト serv1：
		tcp&udp/400,600/23-80, 566
		オブジェクト グループ：
		`object-group service serv1 tcp`
		`  port-object range 23 80`
		`  port-object eq 566`
		`object-group service serv1.src tcp`
		`  port-object eq 400`
		`  port-object eq 600`
		`object-group protocol tcp-udp`
		`  protocol-object tcp`
		`  protocol-object udp`

関連項目

- 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 （132 ページ）
- ネットワーク/ホスト オブジェクト、ポート リスト オブジェクト、およびサービス オブジェクトがオブジェクト グループとしてプロビジョニングされるときの命名方法 （141 ページ）
- ポリシー オブジェクトがオブジェクト グループとしてプロビジョニングされる方法 （140 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。