CHAPTER 9

ポリシー要素の管理

ACS ネットワークにアクセスを試みるクライアントを認証および認可する処理は、ポリシーによって定義されます。ユーザ、ネットワーク デバイス、またはネットワーク デバイスに関連付けられているユーザがクライアントとなります。

ポリシーは、規則のセットです。規則にはポリシー要素が含まれています。ポリシー要素は、規則テーブルに編成された条件と結果のセットです。ポリシーの設計および ACS でのポリシーの実装方法の詳細については、第 3 章「ACS 5.x ポリシー モデル」を参照してください。

ポリシー規則を設定する前に、ポリシー要素を作成する必要があります。ポリシー要素は、ポリシーで使用される条件および結果です。作成したポリシー要素は、ポリシー規則で使用できます。サービス、ポリシー、およびポリシー規則の管理の詳細については、第 10 章「アクセス ポリシーの管理」を参照してください。

この章は、次の内容で構成されています。

（注） Cisco TrustSec ライセンスがインストールされている場合は、あとで TrustSec 認可ポリシーで使用できる、セキュリティ グループおよび Security Group Access Control Lists（SGACL; セキュリティ グループ アクセス コントロール リスト）も設定できます。TrustSec 用のセキュリティ グループの設定については、「セキュリティ グループの作成」（P.4-24）を参照してください。

ポリシー条件の管理

規則テーブルには、次の項目を条件として設定できます。

- 要求/プロトコル アトリビュート：これらのアトリビュートは、ACS によって、ユーザが発行した認証要求から取得されます。
- ID アトリビュート：これらのアトリビュートは、要求を実行するユーザの ID と関連しています。これらのアトリビュートは、内部 ID ストア内のユーザ定義、または外部リポジトリ（LDAP や AD など）に保存されているユーザ定義から取得できます。
- ID グループ：ACS では、すべてのタイプのユーザおよびホストに使用される単一の ID グループ階層が保持されます。内部ユーザまたはホストの各定義に、この階層内の単一の ID グループとの関連付けを含めることができます。

グループ マッピング ポリシーを使用して、ユーザおよびホストを ID グループにマッピングできます。グループ内のすべてのユーザに対する共通のポリシー条件を設定するために、ID グループを条件に含めることができます。ID グループの作成の詳細については、「ID アトリビュートの管理」（P.8-7）を参照してください。

- ネットワーク デバイス グループ（NDG）：要求を発行するデバイスが、1 つ以上、最大 12 のデバイス階層に含まれています。ポリシー条件には階層の要素を含めることができます。NDG の作成の詳細については、「ネットワーク デバイス グループ」（P.7-2）を参照してください。
- 日付と時刻の条件：複数の特定の曜日について特定の時間間隔を定義する、名前付き条件を作成できます。また、日付と時刻の条件に有効期限を関連付けることもできます。

  日付と時刻の条件に現在の日付および時刻を指定すると、実質的に、条件が満たされているかどうかを示す true または false が返されます。日付と時刻の条件には、次の 2 つのコンポーネントがあります。

  - 期間のイネーブル化：このオプションは、開始時刻、終了時刻、または両方を任意で指定して、条件をイネーブルにする期間を制限する場合に使用します。このコンポーネントを使用すると、期間が限定され、実質的に失効する規則を作成できます。

    この条件がイネーブルでない場合は、日付と時刻の条件のこのコンポーネントによって false が返されます。
  - 時間間隔：ACS Web インターフェイスには、曜日および各日の時間を示す、時間のグリッドが表示されます。グリッド内の各セルは、1 時間を表します。これらのセルを設定またはクリアできます。

    要求が処理される日付および時刻が、対応する時間間隔が設定された時間内に収まる場合は、日付と時刻の条件のこのコンポーネントによって true が返されます。

  要求が処理されるとき、日付と時刻の条件の両方のコンポーネントが考慮されます。日付と時刻の条件は、両方のコンポーネントによって true 値が返された場合にだけ評価されます。
- ネットワークの条件：ネットワークへのアクセスを制限するために、次のタイプのフィルタを作成できます。
  - 端末フィルタ：接続を開始および終了する端末を対象とします。端末は、要求から取得される IP アドレス、MAC アドレス、発信番号識別（CLI）、または Dialed Number Identification Service（DNIS; 着信番号識別サービス）の各フィールドによって識別されます。
  - ネットワーク デバイス フィルタ：要求を処理する AAA クライアントを対象とします。ネットワーク デバイスは、その IP アドレス、ネットワーク デバイス リポジトリで定義されているデバイス名、または NDG によって識別されます。
  - デバイス ポート フィルタ：ネットワーク デバイス定義は、端末が関連付けられているデバイス ポートによって補完される場合があります。

  各ネットワーク デバイス条件には、オブジェクトのリストを定義します。このリストは、あとでポリシー条件に含めることができ、これにより、要求で示される定義と照合される定義セットになります。

  条件で使用する演算子は、*match*（示されている値がネットワーク条件の少なくとも 1 つのエントリと一致する必要がある場合）、または *no matches*（フィルタに存在するオブジェクト セット内のいずれのエントリにも一致しない必要がある場合）のいずれかになります。

プロトコル アトリビュートおよび ID アトリビュートをカスタム条件または複合条件で定義して、これらのアトリビュートを条件に含めることができます。

複合条件は、ポリシー規則プロパティ ページで定義し、個別の名前付き条件としては定義しません。「複合条件の設定」（P.10-39）を参照してください。

カスタム条件および日付と時刻の条件は、セッション条件と呼ばれます。

ここでは、次の内容について説明します。

ポリシー規則で使用できる（ただし設定はできない）その他の条件については、第 3 章「ACS 5.x ポリシー モデル」を参照してください。

日付と時刻の条件の作成、複製、および編集

日付と時刻の条件を作成して、時間間隔および期間を指定します。たとえば、特定の休日期間におけるシフトを定義できます。ACS で日付と時刻の条件を含む規則が処理されるとき、日付と時刻の条件は、要求を処理している ACS インスタンスの日付と時刻の情報と比較されます。この条件に関連付けられているクライアントは、セッションの継続中はこの条件の対象となります。

ポリシー決定を行うとき、ACS サーバでの時刻が使用されます。したがって、ACS サーバが属しているタイムゾーンに対応して、日付と時刻の条件を設定したことを確認してください。ユーザが使用しているタイムゾーンが ACS サーバのタイムゾーンとは異なる場合があります。

セッション条件を複製して、既存のセッション条件と同じか、または類似する新しいセッション条件を作成できます。複製の完了後、（元のまたは複製された）各セッション条件に個別にアクセスして、編集または削除します。

日付と時刻の条件を作成、複製、または編集するには、次の手順を実行します。

ステップ 1　[Policy Elements] > [Session Conditions] > [Date and Time] を選択します。

[Date and Time Conditions] ページが表示されます。

ステップ 2　次のいずれかを実行します。

- [Create] をクリックします。
- 複製する条件の隣にあるチェックボックスをオンにし、[Duplicate] をクリックします。
- 変更する名前をクリックします。または、変更する条件の隣にあるチェックボックスをオンにして [Edit] をクリックします。

[Date and Time Properties] ページが表示されます。

ステップ 3　表 9-1 の説明に従って、必須フィールドに有効な設定データを入力します。

表 9-1　[Date and Time Properties] ページ

オプション	説明
General	
Name	時刻と日付の条件の名前を入力します。
Description	時刻と日付の条件の具体的な日付や時刻などの説明を入力します。
Duration	

表 9-1　[Date and Time Properties] ページ（続き）

オプション	説明
Start	次のオプションのいずれかをクリックします。 • Start Immediately：この条件に関連付けられている規則が有効であり、それらの規則が現在の日付から開始されることを指定します。 • Start On：関連するフィールドの隣にあるカレンダー アイコンをクリックして開始日を指定することで、条件がアクティブになる特定の開始日を選択します（開始日の始まりは 24 時間クロックでの時刻 00:00:00 として示されます）。 時刻は *hh*:*mm* 形式で指定できます。
End	次のオプションのいずれかをクリックします。 • No End Date：日付と時刻の条件に関連付けられている規則が、指定された開始日のあとは常にアクティブとなることを指定します。 • End By：関連するフィールドの隣にあるカレンダー アイコンをクリックして終了日を指定することで、日付と時刻の条件が非アクティブになる特定の終了日を選択します（終了日の終わりは 24 時間クロックでの時刻 23:59:59 として示されます）。 時刻は *hh*:*mm* 形式で指定できます。
Days and Time	
Days and Time section grid	日付と時刻グリッドのそれぞれの四角は、1 時間に相当します。四角いグリッドを選択して、対応する時間をアクティブにします。日付と時刻の条件に関連付けられている規則がその時間中は有効になります。 緑の（または色の濃い）四角いグリッドは、アクティブな時間を示します。 ACS サーバが属しているタイムゾーンに対応する日付と時刻の条件を設定していることを確認してください。ユーザが使用しているタイムゾーンが ACS サーバのタイムゾーンとは異なる場合があります。 たとえば、現在の時刻よりも 1 時間先であるものの、ACS サーバのタイムゾーンではすでに過去の時間となっている日付と時刻の条件を設定すると、エラー メッセージが表示される場合があります。
Select All	グリッド内のすべての四角をアクティブ状態に設定する場合にクリックします。日付と時刻の条件に関連付けられている規則が、常に有効になります。
Clear All	グリッド内のすべての四角を非アクティブ状態に設定する場合にクリックします。日付と時刻の条件に関連付けられている規則が、常に無効になります。
Undo All	日付と時刻のグループに対して選択した日付と時刻のアクティブ化および非アクティブ化に関する最新の変更内容を削除する場合にクリックします。

日付と時刻の条件をポリシーに追加するには、最初に規則テーブルをカスタマイズする必要があります。「ポリシーのカスタマイズ」（P.10-4）を参照してください。

ステップ 4　[Submit] をクリックします。

日付と時刻の条件が保存されます。[Date and Time Conditions] ページが表示され、作成または複製した新しい日付と時刻の条件が示されます。

関連トピック

- 「カスタム セッション条件の作成、複製、および編集」（P.9-5）
- 「セッション条件の削除」（P.9-6）
- 「アクセス サービス ポリシーの設定」（P.10-21）

カスタム セッション条件の作成、複製、および編集

プロトコルおよび ID ディクショナリには、多数のアトリビュートが含まれています。これらのアトリビュートのいずれかをポリシー規則の条件として使用するには、そのアトリビュートのカスタム条件を最初に作成する必要があります。カスタム条件により、ポリシー条件で使用する小さなアトリビュート サブセットを定義し、規則テーブル用の条件タイプの選択時に使用する焦点を絞った小さなリストを指定します。

複合条件にプロトコル アトリビュートおよび ID アトリビュートを含めることもできます。複合条件の詳細については、「複合条件の設定」（P.10-39）を参照してください。

カスタム条件を作成するには、いずれかのディクショナリから特定のプロトコル（RADIUS や TACACS+）または ID アトリビュートを選択し、カスタム条件に名前を付ける必要があります。プロトコルおよび ID ディクショナリの詳細については、「グローバル システム オプションの設定」（P.18-1）を参照してください。

ID アトリビュートまたは RADIUS アトリビュートを含むカスタム条件を作成する場合は、これらのアトリビュートの定義を含めることもできます。これにより、特定のアトリビュートに関連付けられている既存のカスタム条件を簡単に表示できます。

カスタム セッション条件を作成、複製、または編集するには、次の手順を実行します。

ステップ 1　[Policy Elements] > [Session Conditions] > [Custom] を選択します。

[Custom Conditions] ページが表示されます。

ステップ 2　次のいずれかを実行します。

- [Create] をクリックします。
- 複製する条件の隣にあるチェックボックスをオンにし、[Duplicate] をクリックします。
- 変更する名前をクリックします。または、変更する条件の隣にあるチェックボックスをオンにして [Edit] をクリックします。

[Custom Condition Properties] ページが表示されます。

ステップ 3　表 9-2 に従い、必須フィールドに有効な設定データを入力します。

表 9-2　[Policy Custom Condition Properties] ページ

オプション	説明
General	
Name	カスタム条件の名前。
Description	カスタム条件の説明。
Condition	
Dictionary	ドロップダウン リスト ボックスから、特定のプロトコルまたは ID ディクショナリを選択します。
Attribute	[Dictionary] フィールドでの選択に基づいて外部 ID ストア ディクショナリのリストを表示するには、[Select] をクリックします。カスタム条件に関連付けるアトリビュートを選択し、[OK] をクリックします。ポリシーで使用されているカスタム条件を編集している場合は、そのカスタム条件によって参照されるアトリビュートは編集できません。

カスタム条件をポリシーに追加するには、最初に規則テーブルをカスタマイズする必要があります。「ポリシーのカスタマイズ」（P.10-4）を参照してください。

ステップ 4　[Submit] をクリックします。

新しいカスタム セッション条件が保存されます。[Custom Condition] ページが表示され、新しいカスタム セッション条件が示されます。この条件に関連付けられているクライアントは、セッションの継続中はこの条件の対象となります。

関連トピック

- 「日付と時刻の条件の作成、複製、および編集」（P.9-3）
- 「セッション条件の削除」（P.9-6）
- 「アクセス サービス ポリシーの設定」（P.10-21）

セッション条件の削除

セッション条件を削除するには、次の手順を実行します。

ステップ 1　[Policy Elements] > [Session Conditions] > *session condition* を選択します。ここで、*session condition* は、[Date and Time] または [Custom] です。

[Session Condition] ページが表示されます。

ステップ 2　削除するセッション条件の隣にあるチェックボックスを 1 つ以上オンにして、[Delete] をクリックします。

次のメッセージが表示されます。

```
Are you sure you want to delete the selected item/items?
```

ステップ 3　[OK] をクリックします。

[Session Condition] ページが表示されます。このとき、削除したカスタム セッション条件は表示されません。

関連トピック

- 「日付と時刻の条件の作成、複製、および編集」（P.9-3）
- 「カスタム セッション条件の作成、複製、および編集」（P.9-5）

ネットワーク条件の管理

フィルタは、端末、ネットワーク デバイス、およびネットワーク デバイス ポート用に作成した再利用可能なネットワーク条件です。フィルタを使用すると、ACS 5.2 では次のことを実行できます。

- ユーザおよびデイバスにネットワーク アクセスを許可するか許可しないかを決定する。
- ポリシーで使用する ID ストア、サービスなどに関する決定を行う。

名前の付いたフィルタを作成すると、その名前を参照して、さまざまな規則およびポリシーでそのフィルタを何度でも再利用できます。

（注）　ACS 5.2 でのフィルタは、ACS 4.x での NAR に似ています。ACS 4.x では、NAR はユーザまたはユーザ グループに基づいていました。5.2 でのフィルタは、さまざまな規則およびポリシーで再利用できる独立した条件です。

ACS では、次の 3 つのタイプのフィルタが用意されています。

- 端末フィルタ：端末（端末の IP アドレス、MAC アドレス、CLID 番号、または DNIS 番号に基づいて接続を開始するラップトップやプリンタなど）をフィルタリングします。

  端末の ID は、端末を一意に識別する IP アドレス、MAC アドレス、またはその他の任意の文字列になります。これは、プロトコル認識アトリビュート タイプの文字列であり、端末 ID のコピーが含まれています。

  - RADIUS 要求では、この ID はアトリビュート 31（Calling-Station-Id）で使用できます。
  - TACACS 要求では、ACS によって、（すべてのフェーズの）開始要求のリモート アドレス フィールドからこの ID が取得されます。ACS では、スラッシュ（/）区切り文字が存在する場合は、その前のリモート アドレス値が取得され、それ以外の場合はリモート アドレス値全体が取得されます。

  端末 IPv4 は、IPv4 バージョンの端末 ID です。端末 MAC は、端末 ID の標準化された MAC アドレスです。

- デバイス フィルタ：端末の Policy Enforcement Point（PEP）として機能するネットワーク デバイス（AAA クライアント）を、ネットワーク デバイスの IP アドレスや名前、または端末が属するネットワーク デバイス グループに基づいてフィルタリングします。

  デバイス ID は、デバイスの IP アドレスや名前である場合、またはデバイスが属するネットワーク デバイス グループに基づく場合があります。

  この IP アドレスは、IPv4 タイプのプロトコル認識アトリビュートであり、要求から取得したデバイス IP アドレスのコピーが含まれています。

  - RADIUS 要求では、アトリビュート 4（NAS-IP-Address）が存在すると、ACS によってアトリビュート 4 から IP アドレスが取得されます。それ以外の場合は、アトリビュート 32（NAS-Identifier）が存在すると、ACS によってアトリビュート 32 から IP アドレスが取得されるか、または受信したパケットから IP アドレスが取得されます。
  - TACACS 要求では、IP アドレスは ACS が受信したパケットから取得されます。

  デバイス名は、ACS リポジトリから取得されるデバイス名のコピーを含む文字列タイプのアトリビュートです。

  デバイス ディクショナリ（NDG ディクショナリ）には、Location、Device Type、NDG を表すその他の動的に作成されたアトリビュートなどのネットワーク デバイス グループ アトリビュートが含まれています。これらのアトリビュートには、現在のデバイスが関連付けられているグループが含まれています。

- デバイス ポート フィルタ：端末が接続しているデバイスの物理ポートをフィルタリングします。フィルタリングはデバイスの IP アドレス、名前、デバイスが属している NDG、およびポートに基づいて行われます。

  デバイス ポート ID は、次のような文字列タイプのアトリビュートです。

  - RADIUS 要求では、アトリビュート 5（NAS-Port）が要求に含まれていると、ACS によってアトリビュート 5 から値が取得され、アトリビュート 87（NAS-Port-Id）が要求に含まれていると、ACS によってアトリビュート 87 から要求が取得されます。
  - TACACS 要求では、ACS によって、（すべてのフェーズの）開始要求のポート フィールドからこの ID が取得されます。

  デバイス名は、ACS リポジトリから取得されるデバイス名のコピーを含む文字列タイプのアトリビュートです。

  デバイス ディクショナリ（NDG ディクショナリ）には、Location、Device Type、NDG を表すその他の動的に作成されたアトリビュートなどのネットワーク デバイス グループ アトリビュートが含まれています。これらのアトリビュートには、現在のデバイスが関連付けられているグループが含まれています。

これらのフィルタを作成、複製、および編集できます。フィルタの内容を .csv ファイルから一括インポートしたり、ACS のフィルタを .csv ファイルにエクスポートしたりできます。ネットワーク条件の一括インポート方法の詳細については、「ネットワーク条件のインポート」（P.9-8）を参照してください。

ここでは、次の内容について説明します。

ネットワーク条件のインポート

一括インポート機能を使用して、次のネットワーク条件の内容をインポートできます。

- 端末フィルタ
- デバイス フィルタ
- デバイス ポート フィルタ

一括インポートの場合は、ACS から .csv ファイル テンプレートをダウンロードし、.csv ファイルにインポートするレコードを追加し、そのファイルをハード ドライブに保存する必要があります。Download Template 機能を使用して、.csv ファイルが要件に準拠するようにします。

端末フィルタ、デバイス フィルタ、およびデバイス ポート フィルタの .csv テンプレートは、それぞれのタイプに固有のテンプレートです。たとえば、[End Station Filters] ページからアクセスしてダウンロードしたテンプレートは、デバイス フィルタまたはデバイス ポート フィルタのインポートには使用できません。.csv ファイルは次の要件に準拠している必要があります。

- 最初のレコード（.csv ファイルの最初の行）の内容は変更しないでください。
- 各レコードに対して使用するのは 1 行だけです。
- フィールドに改行文字を埋め込まないでください。
- 英語以外の言語では、.csv ファイルを utf-8 符号化で符号化するか、Unicode をサポートするフォントを使用して保存します。

インポート プロセスでは、ACS の既存のフィルタ リストにフィルタが追加されるのではなく、既存のリストが置き換えられます。.csv ファイルからレコードをインポートすると、ACS の既存のフィルタ設定が、.csv ファイルのフィルタ設定に置き換えられます。

ステップ 1　Web インターフェイスの [End Station Filter]、[Device Filter]、または [Device Port Filter] ページ上の [Replace from File] ボタンをクリックします。

[Replace from File] ダイアログボックスが表示されます。

ステップ 2　.csv ファイル テンプレートがない場合は、[Download Template] をクリックして、.csv ファイル テンプレートをダウンロードします。

ステップ 3　[Browse] をクリックして、.csv ファイルに移動します。

ステップ 4　[Start Replace] をクリックして、一括インポート プロセスを開始します。

インポートの進行状況が同じページに表示されます。一括インポートの進行状況を監視できます。.csv ファイルのレコードのデータ転送失敗が表示されます。

ステップ 5　[Import Progress] ウィンドウを閉じるには、[Close] をクリックします。

システムに一度に送信できる .csv ファイルは 1 つだけです。インポートが進行中である場合、追加のインポートは、最初のインポートが完了するまで成功しません。

ワンポイントアドバイス

テンプレートをダウンロードしてインポート ファイルを作成する代わりに、特定のフィルタのエクスポート ファイルを使用して、そのファイル内の情報を更新し、保存し、それをインポート ファイルとして再利用できます。

ネットワーク条件のエクスポート

ACS 5.2 では、.csv ファイル形式でフィルタ設定データをエクスポートするための一括エクスポート機能を提供しています。次のフィルタ設定をエクスポートできます。

- 端末フィルタ
- デバイス フィルタ
- デバイス ポート フィルタ

これらいずれかのフィルタの作成、編集、または複製のページで、[Export to File] をクリックして、フィルタ設定を .csv ファイルとしてローカル ハード ドライブに保存します。

端末フィルタの作成、複製、および編集

[End Station Filters] ページを使用して、端末フィルタを作成、複製、および編集します。次の内容を実行します。

ステップ 1　[Policy Elements] > [Session Conditions] > [Network Conditions] > [End Station Filters] を選択します。

[End Station Filters] ページが表示され、設定した端末フィルタのリストが示されます。

ステップ 2　[Create] をクリックします。次のことも実行できます。

- 複製する端末フィルタの隣にあるチェックボックスをオンにし、[Duplicate] をクリックします。
- 編集する端末フィルタの隣にあるチェックボックスをオンにし、[Edit] をクリックします。
- [Export] をクリックして、端末フィルタのリストを .csv ファイルに保存します。詳細については、「ネットワーク条件のエクスポート」（P.9-9）を参照してください。
- [Replace from File] をクリックして、.csv インポート ファイルから端末フィルタの一括インポートを実行します。詳細については、「ネットワーク条件のインポート」（P.9-8）を参照してください。

ステップ 3　次のフィールドに値を入力します。

- Name：端末フィルタの名前。
- Description：端末フィルタの説明。

ステップ 4　次の 1 つ以上のタブのフィールドを編集します。

- IP Address：このタブのフィールドについては、「IP アドレスベースの端末フィルタの定義」（P.9-10）を参照してください。
- MAC Address：このタブのフィールドについては、「MAC アドレスベースの端末フィルタの定義」（P.9-10）を参照してください。
- CLI/DNIS：このタブのフィールドについては、「CLI または DNIS ベースの端末フィルタの定義」（P.9-11）を参照してください。

（注）　フィルタを設定するには、最低限、3 つのタブの少なくとも 1 つにフィルタ基準を入力する必要があります。

ステップ 5　[Submit] をクリックして変更を保存します。

関連トピック

- 「ネットワーク条件の管理」（P.9-6）
- 「ネットワーク条件のインポート」（P.9-8）
- 「デバイス フィルタの作成、複製、および編集」（P.9-12）
- 「デバイス ポート フィルタの作成、複製、および編集」（P.9-14）

IP アドレスベースの端末フィルタの定義

端末へのアクセスを許可または拒否する場合、その端末の IP アドレスを作成、複製、および編集できます。次の内容を実行します。

ステップ 1　[IP Address] タブから、次のいずれかを実行します。

- [Create] をクリックします。
- 複製する IP ベースの端末フィルタの隣にあるチェックボックスをオンにし、[Duplicate] をクリックします。
- 編集する IP ベースの端末フィルタの隣にあるチェックボックスをオンにし、[Edit] をクリックします。

  ダイアログボックスが表示されます。

ステップ 2　次のいずれかを選択します。

- Single IP Address：このオプションを選択した場合、有効な IPv4 アドレスを *x.x.x.x* 形式で入力する必要があります。*x* は 0 ～ 255 の任意の数字です。
- IP Range(s)：このオプションを選択した場合、有効な IPv4 アドレスおよびサブネット マスクを入力して、IP アドレスの範囲をフィルタリングする必要があります。デフォルトでは、サブネット マスクの値は 32 です。

ステップ 3　[OK] をクリックします。

関連トピック

- 「ネットワーク条件の管理」（P.9-6）
- 「端末フィルタの作成、複製、および編集」（P.9-9）
- 「MAC アドレスベースの端末フィルタの定義」（P.9-10）
- 「CLI または DNIS ベースの端末フィルタの定義」（P.9-11）

MAC アドレスベースの端末フィルタの定義

端末または宛先へのアクセスを許可または拒否する場合、その端末または宛先の MAC アドレスを作成、複製、および編集できます。次の内容を実行します。

ステップ 1　[MAC Address] タブから、次のいずれかを実行します。

- [Create] をクリックします。
- 複製する MAC アドレスベースの端末フィルタの隣にあるチェックボックスをオンにし、[Duplicate] をクリックします。
- 編集する MAC アドレスベースの端末フィルタの隣にあるチェックボックスをオンにし、[Edit] をクリックします。

ダイアログボックスが表示されます。

ステップ 2　[End Station MAC] チェックボックスをオンにして、端末の MAC アドレスを入力します。

任意で、このフィールドを ANY に設定して任意の MAC アドレスを参照できます。

ステップ 3　[Destination MAC] チェックボックスをオンにして、宛先マシンの MAC アドレスを入力します。

任意で、このフィールドを ANY に設定して任意の MAC アドレスを参照できます。

（注）　MAC アドレスを *xxxxxxxxxxxx*、*xx-xx-xx-xx-xx-xx*、*xx*:*xx*:*xx*:*xx*:*xx*:*xx*、または *xxxx*.*xxxx*.*xxxx* のいずれかの形式で入力する必要があります。x は、0 ～ 9 または A ～ F の任意の数字です。MAC アドレスにワイルドカード文字は使用できません。

ステップ 4　[OK] をクリックします。

関連トピック

- 「ネットワーク条件の管理」（P.9-6）
- 「端末フィルタの作成、複製、および編集」（P.9-9）
- 「IP アドレスベースの端末フィルタの定義」（P.9-10）
- 「CLI または DNIS ベースの端末フィルタの定義」（P.9-11）

CLI または DNIS ベースの端末フィルタの定義

端末や宛先へのアクセスを許可または拒否する場合、その端末や宛先の CLI および DNIS 番号を作成、複製、および編集できます。次の内容を実行します。

ステップ 1　[CLI/DNIS] タブから、次のいずれかを実行します。

- [Create] をクリックします。
- 複製する CLI または DNIS ベースの端末フィルタの隣にあるチェックボックスをオンにし、[Duplicate] をクリックします。
- 編集する CLI または DNIS ベースの端末フィルタの隣にあるチェックボックスをオンにし、[Edit] をクリックします。

ダイアログボックスが表示されます。

ステップ 2　[CLI] チェックボックスをオンにして、端末の CLI 番号を入力します。

任意で、このフィールドを ANY に設定して任意の CLI アドレスを参照できます。

ステップ 3　[DNIS] チェックボックスをオンにして、宛先マシンの DNIS 番号を入力します。

任意で、このフィールドを ANY に設定して任意の DNIS 番号を参照できます。

（注）　? 文字 およびワイルドカード文字（*）を使用して、任意の単一文字または 1 つ以上の連続する文字をそれぞれ参照できます。

ステップ 4　[OK] をクリックします。

関連トピック

- 「ネットワーク条件の管理」（P.9-6）
- 「端末フィルタの作成、複製、および編集」（P.9-9）
- 「IP アドレスベースの端末フィルタの定義」（P.9-10）
- 「MAC アドレスベースの端末フィルタの定義」（P.9-10）

デバイス フィルタの作成、複製、および編集

[Device Filters] ページを使用して、デバイス フィルタを作成、複製、および編集できます。次の内容を実行します。

ステップ 1　[Policy Elements] > [Session Conditions] > [Network Conditions] > [Device Filters] を選択します。

[Device Filters] ページが表示され、設定したデバイス フィルタのリストが示されます。

ステップ 2　[Create] をクリックします。次のことも実行できます。

- 複製するデバイス フィルタの隣にあるチェックボックスをオンにし、[Duplicate] をクリックします。
- 編集するデバイス フィルタの隣にあるチェックボックスをオンにし、[Edit] をクリックします。
- [Export] をクリックして、デバイス フィルタのリストを .csv ファイルに保存します。詳細については、「ネットワーク条件のエクスポート」（P.9-9）を参照してください。
- [Replace from File] をクリックして、.csv インポート ファイルからデバイス フィルタの一括インポートを実行します。詳細については、「ネットワーク条件のインポート」（P.9-8）を参照してください。

ステップ 3　次のフィールドに値を入力します。

- Name：デバイス フィルタの名前。
- Description：デバイス フィルタの説明。

ステップ 4　次のいずれかのタブまたはすべてのタブのフィールドを編集します。

- IP Address：このタブのフィールドについては、「IP アドレスベースのデバイス フィルタの定義」（P.9-13）を参照してください。
- Device Name：このタブのフィールドについては、「名前ベースのデバイス フィルタの定義」（P.9-13）を参照してください。
- Network Device Group：このタブのフィールドについては、「NDG ベースのデバイス フィルタの定義」（P.9-14）を参照してください。

（注）　フィルタを設定するには、最低限、3 つのタブの少なくとも 1 つにフィルタ基準を入力する必要があります。

ステップ 5　[Submit] をクリックして変更を保存します。

関連トピック

- 「ネットワーク条件の管理」（P.9-6）
- 「ネットワーク条件のインポート」（P.9-8）
- 「端末フィルタの作成、複製、および編集」（P.9-9）
- 「デバイス ポート フィルタの作成、複製、および編集」（P.9-14）

IP アドレスベースのデバイス フィルタの定義

ネットワーク デバイスへのアクセスを許可または拒否する場合、そのネットワーク デバイスの IP アドレスを作成、複製、および編集できます。次の内容を実行します。

ステップ 1　[IP Address] タブから、次のいずれかを実行します。

- [Create] をクリックします。
- 複製する IP ベースのデバイス フィルタの隣にあるチェックボックスをオンにし、[Duplicate] をクリックします。
- 編集する IP ベースのデバイス フィルタの隣にあるチェックボックスをオンにし、[Edit] をクリックします。

ダイアログボックスが表示されます。

ステップ 2　次のいずれかを選択します。

- Single IP Address：このオプションを選択した場合、有効な IPv4 アドレスを *x.x.x.x* 形式で入力する必要があります。*x* は 0 ～ 255 の任意の数字です。
- IP Range(s)：このオプションを選択した場合、有効な IPv4 アドレスおよびサブネット マスクを入力して、IP アドレスの範囲をフィルタリングする必要があります。デフォルトでは、サブネット マスクの値は 32 です。

ステップ 3　[OK] をクリックします。

関連トピック

- 「ネットワーク条件の管理」（P.9-6）
- 「デバイス フィルタの作成、複製、および編集」（P.9-12）
- 「名前ベースのデバイス フィルタの定義」（P.9-13）
- 「NDG ベースのデバイス フィルタの定義」（P.9-14）

名前ベースのデバイス フィルタの定義

ネットワーク デバイスへのアクセスを許可または拒否する場合、そのネットワーク デバイスの名前を作成、複製、および編集できます。次の内容を実行します。

ステップ 1　[Device Name] タブから、次のいずれかを実行します。

- [Create] をクリックします。
- 複製する名前ベースのデバイス フィルタの隣にあるチェックボックスをオンにし、[Duplicate] をクリックします。

- 編集する名前ベースのデバイス フィルタの隣にあるチェックボックスをオンにし、[Edit] をクリックします。

  ダイアログボックスが表示されます。

ステップ 2　[Select] をクリックして、フィルタリングするネットワーク デバイスを選択します。

ステップ 3　[OK] をクリックします。

関連トピック

- 「ネットワーク条件の管理」（P.9-6）
- 「デバイス フィルタの作成、複製、および編集」（P.9-12）
- 「IP アドレスベースのデバイス フィルタの定義」（P.9-13）
- 「NDG ベースのデバイス フィルタの定義」（P.9-14）

NDG ベースのデバイス フィルタの定義

ネットワーク デバイス グループ タイプへのアクセスを許可または拒否する場合、そのネットワーク デバイス グループ タイプを作成、複製、および編集できます。次の内容を実行します。

ステップ 1　[Network Device Group] タブから、次のいずれかを実行します。

a.　[Create] をクリックします。

b.　複製する NDG ベースのデバイス フィルタの隣にあるチェックボックスをオンにし、[Duplicate] をクリックします。

c.　編集する NDG ベースのデバイス フィルタの隣にあるチェックボックスをオンにし、[Edit] をクリックします。

ダイアログボックスが表示されます。

ステップ 2　[Select] をクリックして、フィルタリングするネットワーク デバイス グループ タイプを選択します。

ステップ 3　[Select] をクリックして、フィルタリングするネットワーク デバイス グループ値を選択します。

ステップ 4　[OK] をクリックします。

関連トピック

- 「ネットワーク条件の管理」（P.9-6）
- 「デバイス フィルタの作成、複製、および編集」（P.9-12）
- 「IP アドレスベースのデバイス フィルタの定義」（P.9-13）
- 「名前ベースのデバイス フィルタの定義」（P.9-13）

デバイス ポート フィルタの作成、複製、および編集

[Device Port Filters] ページを使用して、デバイス ポート フィルタを作成、複製、および編集できます。次の内容を実行します。

ステップ 1　[Policy Elements] > [Session Conditions] > [Network Conditions] > [Device Port Filters] を選択します。

[Device Port Filters] ページが表示され、設定したデバイス ポート フィルタのリストが示されます。

ステップ 2　[Create] をクリックします。次のことも実行できます。

- 複製するデバイス ポート フィルタの隣にあるチェックボックスをオンにし、[Duplicate] をクリックします。
- 編集するデバイス ポート フィルタの隣にあるチェックボックスをオンにし、[Edit] をクリックします。
- [Export] をクリックして、デバイス ポート フィルタのリストを .csv ファイルに保存します。詳細については、「ネットワーク条件のエクスポート」（P.9-9）を参照してください。
- [Replace from File] をクリックして、.csv インポート ファイルからデバイス ポート フィルタの一括インポートを実行します。詳細については、「ネットワーク条件のインポート」（P.9-8）を参照してください。

ステップ 3　次のフィールドに値を入力します。

- Name：デバイス ポート フィルタの名前。
- Description：デバイス ポート フィルタの説明。

ステップ 4　次のいずれかのタブまたはすべてのタブのフィールドを編集します。

- IP Address：このタブのフィールドについては、「IP アドレスベースのデバイス ポート フィルタの定義」（P.9-15）を参照してください。
- Device Name：このタブのフィールドについては、「NDG ベースのデバイス ポート フィルタの定義」（P.9-17）を参照してください。
- Network Device Group：このタブのフィールドについては、「NDG ベースのデバイス ポート フィルタの定義」（P.9-17）を参照してください。

（注）　フィルタを設定するには、最低限、3 つのタブの少なくとも 1 つにフィルタ基準を入力する必要があります。

ステップ 5　[Submit] をクリックして変更を保存します。

関連トピック

- 「ネットワーク条件の管理」（P.9-6）
- 「ネットワーク条件のインポート」（P.9-8）
- 「端末フィルタの作成、複製、および編集」（P.9-9）
- 「デバイス フィルタの作成、複製、および編集」（P.9-12）

IP アドレスベースのデバイス ポート フィルタの定義

ネットワーク デバイス ポートへのアクセスを許可または拒否する場合、そのネットワーク デバイス ポートの IP アドレスを作成、複製、および編集できます。次の内容を実行します。

ステップ 1　[IP Address] タブから、次のいずれかを実行します。

- [Create] をクリックします。
- 複製する IP ベースのデバイス ポート フィルタの隣にあるチェックボックスをオンにし、[Duplicate] をクリックします。
- 編集する IP ベースのデバイス ポート フィルタの隣にあるチェックボックスをオンにし、[Edit] をクリックします。

ダイアログボックスが表示されます。

ステップ 2　次のいずれかを選択します。

- Single IP Address：このオプションを選択した場合、有効な IPv4 アドレスを *x.x.x.x* 形式で入力する必要があります。*x* は 0 ～ 255 の任意の数字です。
- IP Range(s)：このオプションを選択した場合、有効な IPv4 アドレスおよびサブネット マスクを入力して、IP アドレスの範囲をフィルタリングする必要があります。デフォルトでは、サブネット マスクの値は 32 です。

ステップ 3　[Port] チェックボックスをオンにして、ポート番号を入力します。このフィールドは文字列タイプであり、数字または文字を含めることができます。次のワイルドカード文字を使用できます。

- ?：単一文字の一致
- *：一連の文字の一致

たとえば、文字列「p*1*」は、「p」の文字で始まり、数字の 1 を含むすべての単語と一致します（port1、port15 など）。

ステップ 4　[OK] をクリックします。

関連トピック

- 「ネットワーク条件の管理」（P.9-6）
- 「デバイス ポート フィルタの作成、複製、および編集」（P.9-14）
- 「名前ベースのデバイス ポート フィルタの定義」（P.9-16）
- 「NDG ベースのデバイス ポート フィルタの定義」（P.9-17）

名前ベースのデバイス ポート フィルタの定義

ネットワーク デバイスおよびポートへのアクセスを許可または拒否する場合、そのネットワーク デバイスおよびポートの名前を作成、複製、および編集できます。次の内容を実行します。

ステップ 1　[Device Name] タブから、次のいずれかを実行します。

- [Create] をクリックします。
- 複製する名前ベースのデバイス ポート フィルタの隣にあるチェックボックスをオンにし、[Duplicate] をクリックします。
- 編集する名前ベースのデバイス ポート フィルタの隣にあるチェックボックスをオンにし、[Edit] をクリックします。

ダイアログボックスが表示されます。

ステップ 2　[Select] をクリックして、フィルタリングするネットワーク デバイスを選択します。

ステップ 3　[Port] チェックボックスをオンにして、ポート番号を入力します。

ステップ 4　[OK] をクリックします。

関連トピック

- 「ネットワーク条件の管理」（P.9-6）
- 「デバイス ポート フィルタの作成、複製、および編集」（P.9-14）

- 「IP アドレスベースのデバイス ポート フィルタの定義」（P.9-15）
- 「NDG ベースのデバイス ポート フィルタの定義」（P.9-17）

NDG ベースのデバイス ポート フィルタの定義

ネットワーク デバイス グループ タイプおよびポートへのアクセスを許可または拒否する場合、そのネットワーク デバイス グループ タイプおよびポートの名前を作成、複製、および編集できます。次の内容を実行します。

ステップ 1　[Network Device Group] タブから、次のいずれかを実行します。

- [Create] をクリックします。
- 複製する NDG ベースのデバイス ポート フィルタの隣にあるチェックボックスをオンにし、[Duplicate] をクリックします。
- 編集する NDG ベースのデバイス ポート フィルタの隣にあるチェックボックスをオンにし、[Edit] をクリックします。

ダイアログボックスが表示されます。

ステップ 2　[Select] をクリックして、フィルタリングするネットワーク デバイス グループ タイプを選択します。

ステップ 3　[Select] をクリックして、フィルタリングするネットワーク デバイス グループ値を選択します。

ステップ 4　[Port] チェックボックスをオンにして、ポート番号を入力します。

ステップ 5　[OK] をクリックします。

関連トピック

- 「ネットワーク条件の管理」（P.9-6）
- 「デバイス フィルタの作成、複製、および編集」（P.9-12）
- 「IP アドレスベースのデバイス フィルタの定義」（P.9-13）
- 「名前ベースのデバイス フィルタの定義」（P.9-13）

認可および権限の管理

認可および権限を定義して、特定のポリシー規則に関連付けられている結果を決定できます。

次のことを定義できます。

- ネットワーク アクセス認可用の認可プロファイル（RADIUS 用）。
- TACACS+ シェル セッション用のシェル プロファイル、およびデバイス管理用のコマンド セット。
- ダウンロード可能 ACL。
- Cisco TrustSec のセキュリティ グループおよびセキュリティ グループ ACL。これらのポリシー要素の設定については、「ACS および Cisco TrustSec」（P.4-23）を参照してください。

次の項で、認可および権限を管理する方法について説明します。

- 「ネットワーク アクセス用の認可プロファイルの作成、複製、および編集」（P.9-18）
- 「セキュリティ グループの作成および編集」（P.9-23）
- 「デバイス管理用のシェル プロファイルの作成、複製、および編集」（P.9-23）

- 「管理デバイス用のコマンド セットの作成、複製、および編集」（P.9-28）
- 「ダウンロード可能 ACL の作成、複製、および編集」（P.9-30）
- 「認可および権限のポリシー要素の削除」（P.9-32）
- 「セキュリティ グループ アクセス コントロール リストの設定」（P.9-32）

ネットワーク アクセス用の認可プロファイルの作成、複製、および編集

認可プロファイルを作成して、さまざまなタイプのユーザにネットワークへのアクセスを認可する方法を定義します。たとえば、VPN 接続を介してネットワークへのアクセスを試みるユーザには、有線接続を介してネットワークへのアクセスを試みるユーザよりも厳しく取り扱うことを定義できます。

認可プロファイルでは、Access-Accept 応答が返すアトリビュートと値のセットが定義されます。次を指定することができます。

- VLAN 情報、リダイレクト用の URL などの共通データ。この情報は、未加工の RADIUS パラメータ情報に自動的に変換されます。
- RADIUS 認可パラメータ：任意の RADIUS アトリビュートを選択し、返す対応値を指定できます。

認可プロファイルを複製して、既存の認可プロファイルと同じか、または類似する新しい認可プロファイルを作成できます。複製の完了後、（元のまたは複製された）各認可プロファイルに個別にアクセスして、編集または削除します。

作成した認可プロファイルは、ネットワーク アクセス セッションの認可ポリシーの結果として使用できます。

認可プロファイルを作成、複製、または編集するには、次の手順を実行します。

ステップ 1　[Policy Elements] > [Authorization and Permissions] > [Network Access] > [Authorization Profile] を選択します。

[Authorization Profiles] ページが表示され、表 9-3 で説明されているフィールドが示されます。

表 9-3　[Authorization Profiles] ページ

オプション	説明
Name	既存のネットワーク アクセス認可定義のリスト。
Description	*表示のみ。*ネットワーク アクセス認可定義の説明。

ステップ 2　次のいずれかを実行します。

- [Create] をクリックします。
- 複製する認可プロファイルの隣にあるチェックボックスをオンにし、[Duplicate] をクリックします。
- 変更する名前をクリックします。または、変更する名前の隣にあるチェックボックスをオンにして [Edit] をクリックします。

[Authorization Profile Properties] ページが表示されます。

ステップ 3　各タブの必須フィールドに有効な設定データを入力します。次の章を参照してください。

- 「認可プロファイルの指定」（P.9-19）
- 「認可プロファイルでの共通アトリビュートの指定」（P.9-19）

- 「認可プロファイルでの RADIUS アトリビュートの指定」（P.9-21）

ステップ 4　[Submit] をクリックします。

認可プロファイルが保存されます。[Authorization Profiles] ページが表示され、作成または複製した認可プロファイルが示されます。

認可プロファイルの指定

認可プロファイルのタブを使用して、ネットワーク アクセス認可プロファイルの名前および説明を設定します。

ステップ 1　[Policy Elements] > [Authorization and Permissions] > [Network Access] > [Authorization Profiles] を選択し、次の項目をクリックします。

- 新しいネットワーク アクセス認可定義を作成するには、[Create]。
- ネットワーク アクセス認可定義を複製するには、[Duplicate]。
- ネットワーク アクセス認可定義を編集するには、[Edit]。

ステップ 2　表 9-4 に従い、[Authorization Profile: General] ページの必須フィールドに入力します。

表 9-4　[Authorization Profile: General] ページ

オプション	説明
Name	ネットワーク アクセス認可定義の名前。
Description	ネットワーク アクセス認可定義の説明。

ステップ 3　次のいずれかをクリックします。

- 変更を保存して [Authorization Profiles] ページに戻るには、[Submit]。
- 認可プロファイルの共通タスクを設定するには、[Common Tasks] タブ。「認可プロファイルでの共通アトリビュートの指定」（P.9-19）を参照してください。
- 認可プロファイルの RADIUS アトリビュートを設定するには、[RADIUS Attributes] タブ。「認可プロファイルでの RADIUS アトリビュートの指定」（P.9-21）を参照してください。

認可プロファイルでの共通アトリビュートの指定

認可プロファイルのタブを使用して、ネットワーク アクセス認可プロファイルに含める共通 RADIUS アトリビュートを指定します。ACS では、指定した値が必須の RADIUS アトリビュートと値のペアに変換され、[RADIUS Attributes] タブに表示されます。

ステップ 1　[Policy Elements] > [Authorization and Permissions] > [Network Access] > [Authorization Profiles] を選択し、次の項目をクリックします。

- [Create] をクリックして新しいネットワーク アクセス認可定義を作成してから、[Common Tasks] タブをクリックします。
- [Duplicate] をクリックしてネットワーク アクセス認可定義を複製してから、[Common Tasks] タブをクリックします。

- [Edit] をクリックしてネットワーク アクセス認可定義を編集してから、[Common Tasks] タブをクリックします。

ステップ 2　表 9-5 に従い、[Authorization Profile: Common Tasks] ページの必須フィールドに入力します。

表 9-5　[Authorization Profile: Common Tasks] ページ

オプション	説明
ACL	
Downloadable ACL Name	定義済みのダウンロード可能 ACL が含まれます。ダウンロード可能 ACL の定義については、「ダウンロード可能 ACL の作成、複製、および編集」（P.9-30）を参照してください。
Filter-ID ACL	ACL フィルタ ID が含まれます。
Proxy ACL	プロキシ ACL が含まれます。
Voice VLAN	
Permission to Join	[Static] を選択します。このパラメータの値が表示されます。
VLAN	
VLAN ID/Name	VLAN 割り当てが含まれます。
Reauthentication	
Reauthentication Timer	セッション タイムアウト値を使用するかどうかを選択します。 • [Static] を選択した場合は、[Seconds] フィールドに値を入力する必要があります。 • [Dynamic] を選択した場合は、ダイナミック パラメータを選択する必要があります。
Maintain Connectivity during Reauthentication	再認証の実行時に接続が確実に保持されるようにするには、[Yes] をクリックします。デフォルトでは、[Yes] が選択されています。このフィールドは、再認証タイマーを定義した場合にだけイネーブルになります。
QoS	
Input Policy Map	QoS 入力ポリシー マップが含まれます。
Output Policy Map	QoS 出力ポリシー マップが含まれます。
802.1X-REV	
LinkSec Security Policy	[Static] を選択した場合は、802.1X-REV LinkSec セキュリティ ポリシーの値を選択する必要があります。有効なオプションは次のとおりです。 • must-not-secure • should-secure • must-secure
URL Redirect	
URL がリダイレクト用に定義されている場合は、ACL も定義する必要があります。	
URL for Redirect	URL リダイレクトが含まれます。
URL Redirect ACL	URL リダイレクト用のアクセス コントロール リスト（ACL）の名前が含まれます。 URL リダイレクトを定義した場合は、その URL リダイレクション用の ACL も定義する必要があります。

認可プロファイルでの RADIUS アトリビュートの指定

認可プロファイルのタブを使用して、認可プロファイルの Access-Accept パケットに含める RADIUS アトリビュートを設定します。タブには、[Common Tasks] タブで選択した RADIUS アトリビュート パラメータも表示されます。

ステップ 1　[Policy Elements] > [Authorization and Permissions] > [Network Access] > [Authorization Profiles] を選択し、次の項目をクリックします。

- [Create] をクリックして新しいネットワーク アクセス認可定義を作成してから、[RADIUS Attributes] タブをクリックします。
- 複製する認可プロファイルの隣にあるチェックボックスをオンにして、[Duplicate] をクリックし、次に、[RADIUS Attributes] タブをクリックします。
- 編集する認可プロファイルの隣にあるチェックボックスをオンにして、[Edit] をクリックし、次に、[RADIUS Attributes] タブをクリックします。

ステップ 2　表 9-6 に従い、[Authorization Profile: RADIUS Attributes] ページの必須フィールドに入力します。

表 9-6　[Authorization Profile: RADIUS Attributes] ページ

オプション	説明
Common Tasks Attributes	[Common Tasks] タブで定義したアトリビュートの名前、値、およびタイプが表示されます。
Manually Entered	このセクションを使用して、認可プロファイルに含める RADIUS アトリビュートを定義します。各アトリビュートを定義しているとき、その名前、値、およびタイプがテーブルに表示されます。次の内容を実行します。 • RADIUS アトリビュートを追加するには、テーブルの下のフィールドに入力し、[Add] をクリックします。 • RADIUS アトリビュートを編集するには、テーブルの該当する行を選択し、[Edit] をクリックします。RADIUS パラメータがテーブルの下のフィールドに表示されます。必要に応じて編集し、[Replace] をクリックします。
Dictionary Type	使用する RADIUS アトリビュートが含まれているディクショナリを選択します。

表 9-6　[Authorization Profile: RADIUS Attributes] ページ（続き）

オプション	説明
RADIUS Attribute	RADIUS アトリビュートの名前。[Select] をクリックして、指定したディクショナリから RADIUS アトリビュートを選択します。 ネットワーク内の VPN デバイスを認証するには、VPN アトリビュートを認可プロファイルに手動で追加する必要があります。ACS は、次に示すようにレイヤ 2 およびレイヤ 3 のさまざまなプロトコルで動作できます。 • IPSec：レイヤ 3 で動作します。必須アトリビュートを ACS 認可プロファイルで設定する必要はありませんが、任意のアトリビュートを設定できます。 • L2TP：L2TP トンネリング用です。次のアトリビュートを使用して ACS を設定する必要があります。 – CVPN3000/ASA/PIX7.x-Tunneling Protocols：このアトリビュートは、使用されるトンネリングのタイプを指定します。 – CVPN3000/ASA/PIX7.x-L2TP-Encryption：このアトリビュートが設定されている場合、VPN3000 は、MSCHAPv1 または MSCHAPv2 認証方式のいずれかで使用する必要がある Microsoft Point-to-Point Encryption（MPPE）キーをクライアントに伝えることができます。 • PPTP：トンネリング用です。次のアトリビュートを使用して ACS を設定する必要があります。 – CVPN3000/ASA/PIX7.x-Tunneling Protocols：このアトリビュートは、使用されるトンネリングのタイプを指定します。 – CVPN3000/ASA/PIX7.x-PPTP-Encryption：このアトリビュートが設定されていると、VPN3000 は、MSCHAPv1 または MSCHAPv2 認証方式のいずれかで使用する必要がある Microsoft Point-to-Point Encryption（MPPE）キーをクライアントに伝えることができます。
Attribute Type	ACS がアクセス要求を許可する対象となる、アトリビュートのクライアント ベンダー タイプ。これらのアトリビュート タイプについては、使用する AAA クライアントで稼動している Cisco IOS ソフトウェア リリースの Cisco IOS マニュアルを参照してください。
Attribute Value	アトリビュートの値。[Select] をクリックして、アトリビュート値のリストを表示します。これらのアトリビュート値については、使用する AAA クライアントで稼動している Cisco IOS ソフトウェア リリースの Cisco IOS マニュアルを参照してください。 トンネル プロトコルの場合、RFC 2868 に従って、特定のタグが付いたアトリビュート値が ACS によってアクセス応答内のデバイスに提供されます。 RADIUS アトリビュート タイプとして [Tagged Enum] または [Tagged String] を選択した場合は、[Tag] フィールドが表示されます。タグ値については、同じトンネルに属すアトリビュートをグループ化するために ACS で使用する数字を入力します。 Tagged Enum アトリビュート タイプの場合： • 適切なアトリビュート値を選択します。 • 適切なタグ値（0 ～ 31）を入力します。 Tagged String アトリビュート タイプの場合： • 適切な文字列アトリビュート値（最大 256 文字）を入力します。 • 適切なタグ値（0 ～ 31）を入力します。

ステップ 3　次の設定を行います。

- 認可プロファイルの基本情報。「認可プロファイルの指定」（P.9-19）を参照してください。

- 認可プロファイルの共通タスク。「認可プロファイルでの共通アトリビュートの指定」（P.9-19）を参照してください。

セキュリティ グループの作成および編集

セキュリティ グループのページを使用して、セキュリティ グループおよび Security Group Tag（SGT; セキュリティ グループ タグ）の名前および詳細を表示し、セキュリティ グループを作成、複製、および編集するためのページを開きます。

セキュリティ グループを作成すると、ACS によって固有の SGT が生成されます。ネットワーク デバイスは、ACS に SGT 情報を問い合せることができます。ネットワーク デバイスでは、この SGT 情報を使用して、入力時にパケットにタグ付けまたはペイントを行い、それらのパケットが出力時に出力ポリシーに従ってフィルタリングできるようにします。出力ポリシーの設定については、「[Egress Policy Matrix] ページ」（P.10-44）を参照してください。

ステップ 1　[Policy Elements] > [Authorizations and Permissions] > [Network Access] > [Security Groups] を選択します。

表 9-7 で説明されている [Security Groups] ページが表示されます。

表 9-7　[Security Groups] ページ

オプション	説明
Name	セキュリティ グループの名前。
SGT (Dec / Hex)	10 進数形式または 16 進数形式でのセキュリティ グループ タグの表現。
Description	セキュリティ グループの説明。

ステップ 2　次の項目をクリックします。

- 新しいセキュリティ グループを作成するには、[Create]。
- セキュリティ グループを複製するには、[Duplicate]。
- セキュリティ グループを編集するには、[Edit]。

ステップ 3　[Name] フィールドおよび [Description] フィールドに必須情報を入力し、[Submit] をクリックします。

関連トピック

- 「セキュリティ グループの作成」（P.4-24）

デバイス管理用のシェル プロファイルの作成、複製、および編集

Cisco IOS シェル プロファイルおよびコマンド セットの認可を設定できます。シェル プロファイルとコマンド セットは、認可のために結合されています。シェル プロファイル認可によって、認可を要求しているユーザに次の機能を許可するかどうかが決定され、この決定は、そのユーザのセッションの間適用されます。

- 特権レベル。
- デバイス管理やネットワーク アクセスなどの一般的な機能。

シェル プロファイル定義は、次の 2 つのコンポーネントに分けられています。

- 共通タスク
- カスタム アトリビュート

[Common Tasks] タブを使用すると、頻繁に使用されるプロファイル アトリビュートを選択および設定できます。このタブに含まれているアトリビュートは、TACACS プロトコルのドラフト規格で定義されているアトリビュートです。これらのアトリビュートは、特に、シェル サービスに関連しています。ただし、これらの値は、他のサービスからの要求の認可に使用される場合があります。

[Custom Attributes] タブを使用すると、追加のアトリビュートを設定できます。各定義は、アトリビュート名、アトリビュートが必須であるか任意であるかの指定、およびアトリビュートの値で構成されています。カスタム アトリビュートは、非シェル サービスに対して定義できます。

シェル プロファイルで指定するアトリビュートについては、使用する AAA クライアントで稼動している Cisco IOS ソフトウェア リリースの Cisco IOS マニュアルを参照してください。

作成したシェル プロファイルおよびコマンド セットは、規則テーブル内の認可および権限で使用できます。

既存のシェル プロファイルと同じか、または類似する新しいシェル プロファイルを作成する場合は、シェル プロファイルを複製できます。

複製の完了後、（元のまたは複製された）各シェル プロファイルに個別にアクセスして、編集または削除します。

シェル プロファイルを作成、複製、または編集するには、次の手順を実行します。

ステップ 1　[Policy Elements] > [Authorization and Permissions] > [Device Administration] > [Shell Profiles] を選択します。

[Shell Profiles] ページが表示されます。

ステップ 2　次のいずれかを実行します。

- [Create] をクリックします。
- 複製するシェル プロファイルの隣にあるチェックボックスをオンにし、[Duplicate] をクリックします。
- 変更する名前をクリックします。または、変更する名前の隣にあるチェックボックスをオンにして [Edit] をクリックします。

[Shell Profile Properties] ページの [General] タブが表示されます。

ステップ 3　各タブの必須フィールドに有効な設定データを入力します。最小設定としてシェル プロファイルの固有の名前を入力する必要があります。その他のフィールドはすべて任意です。次の章を参照してください。

- 「シェル プロファイルの一般プロパティの定義」（P.9-25）
- 「共通タスクの定義」（P.9-25）
- 「カスタム アトリビュートの定義」（P.9-27）

ステップ 4　[Submit] をクリックします。

シェル プロファイルが保存されます。[Shell Profiles] ページが表示され、作成または複製したシェル プロファイルが示されます。

関連トピック

- 「ネットワーク アクセス用の認可プロファイルの作成、複製、および編集」（P.9-18）
- 「管理デバイス用のコマンド セットの作成、複製、および編集」（P.9-28）
- 「認可および権限のポリシー要素の削除」（P.9-32）
- 「デバイス管理のシェル/コマンド認可ポリシーの設定」（P.10-35）

シェル プロファイルの一般プロパティの定義

シェル プロファイルのページを使用して、シェル プロファイルの一般プロパティを定義します。

ステップ 1　[Policy Elements] > [Authorization and Permissions] > [Device Administration] > [Shell Profiles] を選択してから、次のいずれかを実行します。

- [Create] をクリックします。
- 複製するシェル プロファイルの隣にあるチェックボックスをオンにし、[Duplicate] をクリックします。
- 変更する名前をクリックします。または、変更する名前の隣にあるチェックボックスをオンにして [Edit] をクリックします。

ステップ 2　表 9-8 で説明されている [Shell Profile: General] フィールドに入力します。

表 9-8　[Shell Profile: General] ページ

オプション	説明
Name	シェル プロファイルの名前。
Description	（任意）シェル プロファイルの説明。

ステップ 3　次の項目をクリックします。

- 変更を保存して [Shell Profiles] ページに戻るには、[Submit]。
- 認可プロファイルの特権レベルを設定するには、[Common Tasks] タブ。「共通タスクの定義」（P.9-25）を参照してください。
- 認可プロファイルの RADIUS アトリビュートを設定するには、[Custom Attributes] タブ。「カスタム アトリビュートの定義」（P.9-27）を参照してください。

関連トピック

- 「共通タスクの定義」（P.9-25）
- 「カスタム アトリビュートの定義」（P.9-27）

共通タスクの定義

共通タスクのページを使用して、シェル プロファイルの特権レベルおよびアトリビュートを定義します。これらのアトリビュートは、TACACS+ プロトコルによって定義されます。

これらのアトリビュートについては、使用する AAA クライアントで稼動している Cisco IOS ソフトウェア リリースの Cisco IOS マニュアルを参照してください。

ステップ 1　[Policy Elements] > [Authorization and Permissions] > [Device Administration] > [Shell Profiles] を選択してから、次の項目をクリックします。

- [Create] をクリックして新しいシェル プロファイルを作成してから、[Common Tasks] をクリックします。
- [Duplicate] をクリックしてシェル プロファイルを複製してから、[Common Tasks] をクリックします。
- [Edit] をクリックしてシェル プロファイルを編集してから、[Common Tasks] をクリックします。

ステップ 2　表 9-9 の説明に従って、[Shell Profile: Common Tasks] ページに入力します。

表 9-9　Shell Profile: Common Tasks

オプション	説明
Privilege Level	
Default Privilege	（任意）シェル認可を介してクライアントに許可する最初の特権レベル割り当てをイネーブルにします。ディセーブルの場合、この設定は認可および権限で解釈されません。
	[Default Privilege Level] では、シェル プロファイルのデフォルトの（最初の）特権レベルを指定します。[Enable Default Privilege] オプションを選択すると、デフォルトの特権レベルを選択できます。有効なオプションは 0 ～ 15 です。
Maximum Privilege	（任意）最初のシェル認可のあと、クライアントに許可する最大特権レベル割り当てをイネーブルにします。
	[Maximum Privilege Level] では、シェル プロファイルの最大特権レベルを指定します。[Enable Change of Privilege Level] オプションを選択すると、最大特権レベルを選択できます。有効なオプションは 0 ～ 15 です。 デフォルトの特権レベルの割り当てと最大特権レベルの割り当てを両方選択する場合は、デフォルトの特権レベルの割り当てが最大特権レベルの割り当て以下である必要があります。
Shell Attributes	
（注）　次のオプションをイネーブルにしない場合は、それらのオプションに対して [Not in Use] を選択します。	
Access Control List	（任意）[Static] を選択し、イネーブルにするアクセス コントロール リストの名前を指定します。アクセス コントロール リストの名前には、最大で 27 文字を使用できます。名前には、ハイフン（-）、左角カッコ（[）、右角カッコ（]）、スラッシュ（/）、バックスラッシュ（\）、アポストロフィ（'）、左山カッコ（<）、および右山カッコ（>）は使用できません。
Auto Command	（任意）[Static] を選択し、イネーブルにするコマンドを指定します。
No Callback Verify	（任意）[Static] を選択し、コールバック検証が必要であるかどうかを指定します。有効なオプションは次のとおりです。 • [True]：コールバック検証が不要であることを指定します。 • [False]：コールバック検証が必要であることを指定します。
No Escape	（任意）[Static] を選択し、エスケープ防止が必要であるかどうかを指定します。有効なオプションは次のとおりです。 • [True]：エスケープ防止をイネーブルにすることを指定します。 • [False]：エスケープ防止をイネーブルにしないことを指定します。
No Hang Up	（任意）[Static] を選択し、切断なしが必要であるかどうかを指定します。有効なオプションは次のとおりです。 • [True]：切断なしを許可することを指定します。 • [False]：切断を許可することを指定します。

表 9-9　Shell Profile: Common Tasks（続き）

オプション	説明
Timeout	（任意）[Static] を選択して、許可されたタイムアウト期間を値フィールドでイネーブルにし、分単位で指定します。有効な範囲は 0 ～ 999 です。
Idle Time	（任意）[Static] を選択して、許可されたアイドル時間の期間を値フィールドでイネーブルにし、分単位で指定します。有効な範囲は 0 ～ 999 です。
Callback Line	（任意）[Static] を選択して、コールバック電話回線を値フィールドでイネーブルにし、指定します。
Callback Rotary	（任意）[Static] を選択して、コールバック ロータリー電話回線を値フィールドでイネーブルにし、指定します。

ステップ 3　次の項目をクリックします。

- 変更を保存して [Shell Profiles] ページに戻るには、[Submit]。
- 認可プロファイルの名前および説明を設定するには、[General] タブ。「シェル プロファイルの一般プロパティの定義」（P.9-25）を参照してください。
- 認可プロファイルのカスタム アトリビュートを設定するには、[Custom Attributes] タブ。「カスタム アトリビュートの定義」（P.9-27）を参照してください。

関連トピック

- 「カスタム アトリビュートの定義」（P.9-27）
- 「デバイス管理のシェル / コマンド認可ポリシーの設定」（P.10-35）

カスタム アトリビュートの定義

カスタム アトリビュートのタブを使用して、シェル プロファイルのカスタム アトリビュートを定義します。このタブには、[Common Tasks] タブで選択した共通タスク アトリビュートも表示されます。

ステップ 1　表 9-10 の説明に従って、[Custom Attributes] タブのフィールドを編集します。

表 9-10　[Shell Profile: Custom Attributes] ページ

オプション	説明
Common Tasks Attributes	[Common Tasks] タブで定義した共通タスク アトリビュートの名前、要件、および値が表示されます。
Manually Entered	このセクションを使用して、認可プロファイルに含めるカスタム アトリビュートを定義します。各アトリビュートを定義しているとき、その名前、要件、および値がテーブルに表示されます。次の内容を実行します。 • カスタム アトリビュートを追加するには、テーブルの下のフィールドに入力し、[Add] をクリックします。 • カスタム アトリビュートを編集するには、テーブルの該当する行を選択し、[Edit] をクリックします。 カスタム アトリビュート パラメータがテーブルの下のフィールドに表示されます。必要に応じて編集し、[Replace] をクリックします。
Attribute	カスタム アトリビュートの名前。

表 9-10　[Shell Profile: Custom Attributes] ページ（続き）

オプション	説明
Requirement	カスタム アトリビュートが必須であるか任意であるかを選択します。
Value	カスタム アトリビュートの値。

ステップ 2　次の項目をクリックします。

- 変更を保存して [Shell Profiles] ページに戻るには、[Submit]。
- 認可プロファイルの名前および説明を設定するには、[General] タブ。「シェル プロファイルの一般プロパティの定義」（P.9-25）を参照してください。
- シェル プロファイルの特権レベルおよびアトリビュートを認可プロファイルに設定するには、[Common Tasks] タブ。「共通タスクの定義」（P.9-25）を参照してください。

関連トピック

- 「シェル プロファイルの一般プロパティの定義」（P.9-25）
- 「共通タスクの定義」（P.9-25）

管理デバイス用のコマンド セットの作成、複製、および編集

コマンド セットによって、デバイス管理用に許可されたコマンドおよび引数が決まります。デバイス設定認可ポリシーの結果としてコマンド セットを指定できます。シェル プロファイルとコマンド セットは、認可のために統合されており、ユーザ セッションの間適用されます。

既存のコマンド セットと同じか、または類似する新しいコマンド セットを作成する場合は、コマンド セットを複製できます。複製の完了後、（元のまたは複製された）各コマンド セットに個別にアクセスして、編集または削除します。

作成したコマンド セットは、規則テーブル内の認可および権限で使用できます。規則に複数のコマンド セットが含まれている場合があります。*「デバイス管理用のシェル プロファイルの作成、複製、および編集」（P.9-23）*を参照してください。

（注）　コマンド セットでは、TACACS+ プロトコル アトリビュートだけがサポートされています。

新しいコマンド セットを作成、複製、または編集するには、次の手順を実行します。

ステップ 1　[Policy Elements] > [Authorization and Permissions] > [Device Administration] > [Command Sets] を選択します。

[Command Sets] ページが表示されます。

ステップ 2　次のいずれかを実行します。

- [Create] をクリックします。

  [Command Set Properties] ページが表示されます。
- 複製するコマンド セットの隣にあるチェックボックスをオンにし、[Duplicate] をクリックします。

  [Command Set Properties] ページが表示されます。

- 変更する名前をクリックします。または、変更する名前の隣にあるチェックボックスをオンにして [Edit] をクリックします。

  [Command Set Properties] ページが表示されます。
- [File Operations] をクリックして、次のいずれかの機能を実行します。
  - Add：コマンド セットをインポート ファイルから ACS に追加するには、このオプションを選択します。
  - Update：ACS でのコマンド セットのリストをインポート ファイル内のコマンド セットのリストに置き換えるには、このオプションを選択します。
  - Delete：インポート ファイルでリストされているコマンド セットを ACS から削除するには、このオプションを選択します。

  一括操作の詳細については、「ネットワーク リソースおよびユーザに関する一括操作の実行」（P.7-8）を参照してください。
- ACS からコマンド セットをローカル ハードディスクにエクスポートするには、[Export] をクリックします。

  ダイアログボックスが表示され、コマンド セットをセキュアにエクスポートするための暗号化パスワードを入力するよう要求するプロンプトが表示されます。

a. [Password] チェックボックスをオンにして、エクスポート プロセスでファイルを暗号化するためのパスワードを入力し、[Start Export] をクリックします。

b. 暗号化を使用しない場合は、[Start Export] をクリックして、コマンド セットをエクスポートします。

ステップ 3　必須フィールドに有効な設定データを入力します。

最小設定としてコマンド セットの固有の名前を入力する必要があります。その他のフィールドはすべて任意です。コマンドおよび引数を定義できます。他のコマンド セットのコマンドと引数を追加することもできます。

[Command Set Properties] ページのフィールドについては、表 9-11 を参照してください。

表 9-11　[Command Set Properties] ページ

フィールド	説明
Name	コマンド セットの名前。
Description	（任意）コマンド セットの説明。
Permit any command that is not in the table below	Grant テーブルでコマンドが明示的に拒否されている場合を除き、要求されたすべてのコマンドを許可する場合にオンにします。Grant テーブルで明示的に許可されているコマンドだけを許可する場合はオフにします。
Command Set table	このセクションを使用して、認可プロファイルに含めるコマンドを定義します。各コマンドを定義しているとき、コマンドの詳細がテーブルに表示されます。次の内容を実行します。 • コマンドを追加するには、テーブルの下のフィールドに入力し、[Add] をクリックします。 • コマンドを編集するには、テーブルの該当する行を選択し、[Edit] をクリックします。コマンド ライン パラメータが、テーブルの下のフィールドに表示されます。必要に応じて編集し、[Replace] をクリックします。 Command Set テーブル内のコマンドの順序が重要となります。これは、最初に一致したコマンドおよび引数に応じてポリシー規則テーブルの処理が決まり、ポリシー結果の選択に関する決定が行われるためです。Command Set テーブルの右にあるコントロール ボタンを使用して、コマンドの順序を変更します。

表 9-11　[Command Set Properties] ページ（続き）

フィールド	説明
Grant	関連付けられたコマンドの権限レベルを選択します。次のオプションがあります。 • Permit：関連付けられたコマンドおよび引数は、自動的に許可されます。 • Deny：関連付けられたコマンドおよび引数は、自動的に拒否されます。 • Deny Always：関連付けられたコマンドおよび引数は、常に拒否されます。
Command	コマンド名を入力します。このフィールドは、大文字と小文字が区別されません。アスタリスク（*）を使用して、コマンド名のゼロ（0）以上の文字を表すことができます。疑問符（?）を使用して、コマンド名の単一文字を表すことができます。 有効なコマンド名のエントリ例： • SHOW • sH* • sho? • Sh*?
Arguments (field)	コマンド名に関連付けられている引数を入力します。このフィールドは、大文字と小文字が区別されません。 ACS 5.2 では、UNIX タイプの標準正規表現が使用されます。
Select Command/ Arguments from Command Set	別のコマンド セットからコマンドを追加するには、次の手順を実行します。 1. コマンド セットを選択します。 2. [Select] を選択して、使用可能なコマンドおよび引数がリストされているページを開きます。 3. コマンドを選択し、[OK] をクリックします。

ステップ 4　[Submit] をクリックします。

コマンド セットが保存されます。[Command Sets] ページが表示され、作成または複製したコマンド セットが示されます。

関連トピック

- 「ネットワーク アクセス用の認可プロファイルの作成、複製、および編集」（P.9-18）
- 「デバイス管理用のシェル プロファイルの作成、複製、および編集」（P.9-23）
- 「認可および権限のポリシー要素の削除」（P.9-32）
- 「デバイス管理用のシェル プロファイルの作成、複製、および編集」（P.9-23）

ダウンロード可能 ACL の作成、複製、および編集

ダウンロード可能 ACL を定義して、Access-Accept メッセージを返すことができます。ACL を使用して、ネットワークに不要なトラフィックが発生することを防止します。ACL では、RADIUS プロトコルを使用して、送信元 IP アドレスと宛先 IP アドレス、トランスポート プロトコルなどをフィルタリングできます。

名前付き権限オブジェクトとして作成したダウンロード可能 ACL は、認可プロファイルに追加できます。その後、これらの認可プロファイルを認可ポリシーの結果として指定できます。

既存のダウンロード可能 ACL と同じか、または類似する新しいダウンロード可能 ACL を作成する場合は、ダウンロード可能 ACL を複製できます。

複製の完了後、（元のまたは複製された）各ダウンロード可能 ACL に個別にアクセスして、編集または削除します。

ダウンロード可能 ACL を作成、複製、または編集するには、次の手順を実行します。

ステップ 1　[Policy Elements] > [Authorization and Permissions] > [Named Permission Objects] > [Downloadable ACLs] を選択します。

[Downloadable ACLs] ページが表示されます。

ステップ 2　次のいずれかを実行します。

- [Create] をクリックします。

  [Downloadable ACL Properties] ページが表示されます。
- 複製するダウンロード可能 ACL の隣にあるチェックボックスをオンにし、[Duplicate] をクリックします。

  [Downloadable ACL Properties] ページが表示されます。
- 変更する名前をクリックします。または、変更する名前の隣にあるチェックボックスをオンにして [Edit] をクリックします。

  [Downloadable ACL Properties] ページが表示されます。
- [File Operations] をクリックして、次のいずれかの機能を実行します。
  - Add : インポート ファイルから ACL を ACS に追加するには、このオプションを選択します。
  - Update : ACS での ACL のリストをインポート ファイル内の ACL のリストに置き換えるには、このオプションを選択します。
  - Delete : インポート ファイルでリストされている ACL を ACS から削除するには、このオプションを選択します。

  一括操作の詳細については、「ネットワーク リソースおよびユーザに関する一括操作の実行」（P.7-8）を参照してください。
- ACS から DACL をローカル ハードディスクにエクスポートするには、[Export] をクリックします。

  ダイアログボックスが表示され、DACL をセキュアにエクスポートするための暗号化パスワードを入力するよう要求するプロンプトが表示されます。
  - [Password] チェックボックスをオンにして、エクスポート プロセスでファイルを暗号化するためのパスワードを入力し、[Start Export] をクリックします。
  - 暗号化を使用しない場合は、[Start Export] をクリックして、DACL をエクスポートします。

ステップ 3　表 9-12 に従い、有効な設定データを必須フィールドに入力し、標準 ACL 構文を使用して 1 つ以上の ACL を定義します。

表 9-12　[Downloadable ACL Properties] ページ

オプション	説明
Name	DACL の名前。

表 9-12　[Downloadable ACL Properties] ページ（続き）

オプション	説明
Description	DACL の説明。
Downloadable ACL Content	ACL コンテンツを定義します。 標準 ACL コマンド構文と意味を使用します。ACL 定義は、1 つ以上の ACL コマンドで構成されています。各 ACL コマンドは、個別の行に挿入されています。 ACL 定義の詳細については、デバイス コンフィギュレーション ガイドのコマンド リファレンスを参照してください。

ステップ 4　[Submit] をクリックします。

ダウンロード可能 ACL が保存されます。[Downloadable ACLs] ページが表示され、作成または複製したダウンロード可能 ACL が示されます。

関連トピック

- 「ネットワーク アクセス用の認可プロファイルの作成、複製、および編集」（P.9-18）
- 「ネットワーク アクセスのセッション認可ポリシーの設定」（P.10-29）
- 「認可および権限のポリシー要素の削除」（P.9-32）

認可および権限のポリシー要素の削除

認可および権限のポリシー要素を削除するには、次の手順を実行します。

ステップ 1　[Policy Elements] > [Authorization and Permissions] を選択してから、必要なオプションに移動します。

対応するページが表示されます。

ステップ 2　削除する項目の隣にあるチェックボックスを 1 つ以上オンにして、[Delete] をクリックします。

次のメッセージが表示されます。

```
Are you sure you want to delete the selected item/items?
```

ステップ 3　[OK] をクリックします。

ページが表示されます。このとき、削除されたオブジェクトは表示されません。

セキュリティ グループ アクセス コントロール リストの設定

セキュリティ グループ アクセス コントロール リスト（SGACL）が、送信元 SGT および宛先 SGT に基づいて、入力時に適用されます。このページは、SGACL を表示、作成、複製、および編集する場合に使用します。SGACL の名前またはコンテンツを変更すると、ACS ではその生成 ID が更新されます。SGACL の生成 ID が変更されると、関連する TrustSec ネットワーク デバイスによって SGACL のコンテンツがリロードされます。

また、SGACL は、Role-Based ACL（RBACL; ロールベースの ACL）とも呼ばれます。

ステップ 1　[Policy Elements] > [Authorizations and Permissions] > [Named Permissions Objects] > [Security Group ACLs] を選択します。

[Security Group Access Control Lists] ページが表示され、表 9-13 で説明されているフィールドが示されます。

表 9-13　[Security Group Access Control Lists] ページ

オプション	説明
Name	SGACL の名前。
Description	SGACL の説明。

ステップ 2　次のオプションのいずれかをクリックします。

- 新しい SGACL を作成する場合は、[Create]。
- SGACL を複製する場合は、[Duplicate]。
- SGACL を編集する場合は、[Edit]。

ステップ 3　表 9-14 の説明に従って、[Security Group Access Control Lists Properties] ページのフィールドに入力します。

表 9-14　[Security Group Access Control List Properties] ページ

オプション	説明
General	
Name	SGACL の名前。名前にはスペース、ハイフン（-）、疑問符（?）、または感嘆符（!）を使用できません。SGACL を作成すると、その生成 ID が表示されます。
Generation ID	*表示のみ*。次の項目を変更すると、ACS では SGACL の生成 ID が更新されます。 • SGACL の名前。 • SGACL のコンテンツ（ACE）。 SGACL の説明を変更しても、生成 ID は更新されません。
Description	SGACL の説明。
Security Group ACL Content	ACL コンテンツを入力します。ACL 定義の構文および意味が有効であることを確認します。

ステップ 4　[Submit] をクリックします。