許可ポリシーおよびプロファイルの管理

許可ポリシーは、Cisco Identity Services Engine（Cisco ISE）で許可プロファイルを作成する場合に使用されます。

許可ポリシーは許可ルールで構成されます。許可ルールには、名前、属性、および権限の 3 つの要素があります。許可プロファイルにマッピングする権限要素。

この章では、許可ポリシーについて説明し、次の許可ポリシー関連タスクの手順の例を示します。

Cisoc ISE の許可プロファイル

許可ポリシーは、Cisco ISE ネットワーク許可サービスのコンポーネントです。ネットワーク リソースにアクセスする特定のユーザおよびグループの許可ポリシーを定義し、許可プロファイルを設定することができます。

許可ポリシーには条件付きの要件を含めることができ、この要件では、1 つ以上の許可プロファイルを返すことができる許可チェックを含む複合条件を使用して、1 つ以上の ID グループを組み合わせます。また、特定の ID グループを使用しない条件付きの要件が存在する場合もあります（デフォルトの「Any」の使用など）。

関連項目

- エンドポイント ID グループの詳細については、「エンドポイント ID グループでグループ化された識別済みエンドポイント」（P.21-44）を参照してください。

Cisco ISE 許可プロファイル

ネットワーク許可ポリシーは、特定のユーザおよびグループの ID にルールを関連付け、対応するプロファイルを作成します。これらのルールが設定された属性と一致する場合は、常に、権限を付与する、対応する許可プロファイルがポリシーおよびによって返され、ネットワーク アクセスがこれに応じて許可されます。

たとえば、許可プロファイルには、次のタイプに含まれるさまざまな権限を含めることができます。

- 標準プロファイル
- 例外プロファイル
- デバイスベースのプロファイル

プロファイルは、ディクショナリに保存されているリソース セットから選択された属性で構成され、特定の許可ポリシーの複合条件が一致したときに返されます。許可ポリシーには単一のネットワーク サービス ルールにマッピングする複合条件を含めることができるため、許可チェックのリストを含めることもできます。

単純なシナリオでは、すべての許可チェックがルール内で AND ブール演算子を使用して作成されます。高度なシナリオでは、任意のタイプの許可確認式を使用できますが、これらのすべての許可確認は、返される許可プロファイルに準拠する必要があります。許可確認は、通常、ライブラリに追加できるユーザ定義名を含む 1 つ以上の条件から構成され、他の許可ポリシーで再利用できます。

関連項目

- 「許可ポリシーの用語」（P.20-2）
- 「許可ポリシーとサポートされているディクショナリ」（P.20-4）
- 「許可ポリシーの設定」（P.20-8）
- 第 18 章「ポリシー条件の設定」
- 「許可プロファイルの権限の設定」（P.20-10）
- 「ダウンロード可能 ACL の権限の設定」（P.20-12）

許可ポリシーの用語

Cisco ISE 許可ポリシーおよびプロファイルに使用される基本的な用語は、次のとおりです。

- 「許可プロファイル」（P.20-3）
- 「許可ポリシー」（P.20-3）
- 「アクセス コントロール リスト」（P.20-4）
- 「ネットワーク許可」（P.20-2）
- 「ポリシー要素」（P.20-2）

ネットワーク許可

許可は、いずれのユーザが Cisco ISE ネットワークおよびそのリソースにアクセスできるかを保証するための重要な要件です。ネットワーク許可は、ネットワークおよびそのリソースへのユーザ アクセスならびに各ユーザがシステム上でこれらのリソースに対して実行できることを制御します。Cisco ISE ネットワークは、読み取り、書き込み、実行の権限を許可する権限セットを定義します。Cisco ISE では、ネットワークのニーズに合わせて、多数のさまざまな許可ポリシーを作成できます。このリリースでは、Cisco ISE ネットワークとリソースへの RADIUS アクセスだけをサポートします。

ポリシー要素

ポリシー要素は認可ポリシーを定義するコンポーネントであり、次の物があります。

- ルール名

- ID グループ
- 条件（Conditions）
- 権限

これらのポリシー要素は、ポリシー ルールを作成したときに参照され、条件および属性の選択によって、特定のタイプの許可プロファイルを作成できます。

許可プロファイル

許可プロファイルは、多数の特定の権限によって一連のネットワーク サービスへのアクセスが許可されるコンテナとして機能します。許可プロファイルには、ネットワーク アクセス要求に付与される権限セットを定義し、次のものを含めることができます。

- プロファイル名
- プロファイルの説明
- 関連 DACL
- 関連 VLAN
- 関連 SGACL
- 任意の数の他のディクショナリベースの属性

許可ポリシー

許可ポリシーは、ユーザ定義の単一のルールまたはルールのセットで構成できます。これらのルールは、特定のポリシーを作成するために機能します。たとえば、標準ポリシーは、ID グループ用に入力した値と特定の条件または属性をリンクする If-Then 表記法を使用するルール名を含め、一意の許可プロファイルを作成する特定の権限セットを生成できます。設定できる許可ポリシー オプションは 2 つあります。

- 最初に一致したルールの適用（First Matched Rules Apply）
- 複数の一致するルールが適用されます。

これら 2 つのオプションは、ユーザの権限セットと一致したときに、標準ポリシー テーブルにリストされている最初に一致したルール タイプの使用または複数の一致したルール タイプの使用のいずれかを Cisco ISE に指示します。設定できる許可ポリシーには、次の 2 つのタイプがあります。

- 標準：標準ポリシーは、長期間有効なままにし、ユーザ、デバイス、またはグループの大規模なグループに適用し、特定またはすべてのネットワーク エンドポイントへのアクセスを許可するために作成されるポリシーです。標準ポリシーは変更しないようにし、権限の共通セットを共有するユーザ、デバイス、グループの大規模なグループに適用します。

  標準ポリシーは、特定の条件または権限を使用する特定の ID グループに使用するために変更したり、新しい事業部門、ユーザ グループ、デバイス、ネットワーク グループのニーズを満たすための別のタイプの標準ポリシーを作成したりするためのテンプレートとして使用できます。

- 例外：これとは対照的に、例外ポリシーは、標準ポリシーの例外として機能するタイプのポリシーであるため、適切な名前を付けられます。例外ポリシーは、短期間のポリシー期間、特定のタイプのネットワーク デバイス、ネットワーク エンドポイントまたはグループ、特別な条件や権限を満たすニーズ、あるいは即時要件などのさまざまな要因に基づく制限されたアクセスを許可することを目的としています。

  例外ポリシーは、制限された数のユーザ、デバイス、またはグループにネットワーク リソースへのアクセスを許可するなどの、即時または短期間のニーズを満たすために作成します。例外ポリシーを使用すると、1 人のユーザまたはユーザのサブセットに合わせて調整された、ID グループ、

条件、または権限に対する、カスタマイズされた値の特定のセットを作成できます。これにより、さまざまな、またはカスタマイズされたポリシーを作成し、企業、グループ、またはネットワークのニーズを満たすことができます。

アクセス コントロール リスト

Cisco ISE システムのアクセス コントロール リスト（ACL）は、特定のオブジェクトまたはネットワーク リソースに接続する権限のリストです。ACL は、いずれのユーザまたはグループがオブジェクトへのアクセス権を付与されるか、および指定されたオブジェクトまたはネットワーク リソースでどの操作が許可されるかを指定します。一般的な ACL の各エントリは、サブジェクトおよび操作を指定するか、または状態（許可または拒否など）を提供します。Cisco ISE は、Downloadable ACL（DACL）も使用します。

許可ポリシーとサポートされているディクショナリ

簡易および複合両方の許可ポリシーのタイプで、確認は返される許可プロファイルに準拠する必要があります。

確認には、通常、ライブラリに追加して他のポリシーで再利用できるユーザ定義名を含む 1 つ以上の条件が含まれます。条件は、Cisco ISE ディクショナリからの属性を使用して条件を定義します。ディクショナリには、次の物があります。

- システム定義されたディクショナリ：
  - RADIUS
- RADIUS ベンダ ディクショナリ
  - Airespace
  - Cisco
  - Cisco BBSM
  - Cisco VPN3000
  - Microsoft

詳細は、Cisco ISE ディクショナリの「ディクショナリおよびディクショナリ属性」（P.10-1）を参照してください。

認可ポリシーおよびプロファイル設定のガイドライン

許可ポリシーおよびプロファイルを管理または運用する場合、次のガイドラインに従ってください。

- 作成するルール名は、サポートされている次の文字のみを使用する必要があります。
  - 記号：プラス（+）、ハイフン（-）、アンダースコア（_）、ピリオド（.）、およびスペース（ ）。
  - アルファベット文字：A ～ Z、a ～ z。
  - 数字：0 ～ 9。
- ID グループのデフォルトは「Any」です（このグローバル デフォルトを使用してすべてのユーザに適用できます）。
- 条件では、1 つ以上のポリシー値を設定することが許可されています。ただし、条件はオプションであり、許可ポリシーを作成する場合に必須ではありません。次に、条件を作成する 2 つの方法を示します。

  - 選択肢の対応するディクショナリから既存の条件または属性を選択します。
  - 推奨値を選択またはテキスト ボックスを使用してカスタム値を入力できるカスタム条件を作成します。
- 作成する条件名は、サポートされている次の文字のみを使用する必要があります。
  - 記号：ハイフン（-）、アンダースコア（_）、およびピリオド（.）。
  - アルファベット文字：A ～ Z、a ～ z。
  - 数字：0 ～ 9。
- 権限は、ポリシーに使用する許可プロファイルを選択するときに重要です。権限は、特定のリソースへのアクセス権を付与したり、特定のタスクの実行を可能にしたりできます。たとえば、あるユーザが特定の ID グループ（デバイス管理者など）に属しており、そのユーザが定義済みの条件（サイトがボストンにあるなど）を満たしている場合、このユーザは、そのグループに関連付けられた権限（特定のネットワーク リソースのセットへのアクセス権、デバイスへの特定の操作を実行する権限など）を付与されます。
- 必ず [保存（Save）] をクリックして、新規または変更したポリシーやプロファイルを Cisco ISE データベースに保存します。

デフォルトの許可ポリシー、ルール、プロファイル設定

Cisco ISE ソフトウェアには、共通設定を提供する多数のデフォルトの条件、ルール、プロファイルが事前インストールされているため、Cisco ISE 許可ポリシーおよびプロファイルで必要なルールおよびポリシーを容易に作成できます。これらの組み込み設定のデフォルトには、表 20-1 で説明されている指定された値が含まれています。

表 20-1　許可ポリシー、プロファイル、およびルールの設定のデフォルト

名前	ユーザ インターフェイスのパス	説明	その他の情報
許可ポリシーのデフォルト			
許可ポリシーのデフォルトの複合条件	**[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [許可（Authorization）]**	これらは、許可ポリシーで使用される条件、ルール、およびプロファイルの事前インストールされた設定のデフォルトです。	許可ポリシーを作成するために、次の関連属性を使用できます。 • 有線 802.1x • 有線 MAB • 無線 802.1x • Catalyst スイッチ ローカル Web 認証 • WLC Web 認証
有線 MAB 複合条件	**[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [許可（Authorization）] > [複合条件（Compound Conditions）] を選択します。**	この複合条件は次の属性と値をチェックします。 • RADIUS:Service-Type = Call-Check • RADIUS:NAS-Port-Type = Ethernet	この複合条件は、有線 MAB 許可ポリシーで使用されます。 このポリシーで指定された基準に一致する要求は、有線 MAB 許可ポリシーに基づいて評価されます。

表 20-1　許可ポリシー、プロファイル、およびルールの設定のデフォルト （続き）

名前	ユーザ インターフェイスのパス	説明	その他の情報
無線 802.1X 複合条件	**[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [許可（Authorization）] > [複合条件（Compound Conditions）] を選択します。**	この複合条件は次の属性と値をチェックします。 • RADIUS:Service-Type = Framed • RADIUS:NAS-Port-Type = Wireless-IEEE802.11	この複合条件は、無線 802.1X 許可ポリシーで使用されます。 このポリシーで指定された基準に一致する要求は、無線 802.1X 許可ポリシーに基づいて評価されます。
許可プロファイル設定のデフォルト			
Blacklist_Access	**[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [許可プロファイル（Authorization Profiles）] > [Blacklist_Access]**	この許可プロファイルは、ブラックリストに登録されているデバイスへのアクセスを拒否します。ブラックリストに登録されているデバイスはすべて、次の URL にリダイレクトされます。 url-redirect=https://ip:port/mydevices/blackhole.jsp	このデフォルトの許可プロファイルは、デバイス ポータルで「失われた」として宣言されているすべてのエンドポイントに適用されます。
Cisco_IP_Phones	**[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [許可プロファイル（Authorization Profiles）] > [Cisco_IP_Phones]**	この許可プロファイルでは、次の値の設定デフォルト プロファイルを使用します。 • [名前（Name）] : [Cisco IP Phone] • [DACL] : [PERMIT_ALL_TRAFFIC] • [VSA] : [cisco:av-pair:device-traffic-class=voice] このプロファイルは、このプロファイルで指定された基準に一致する要求を評価します。	このデフォルトの許可プロファイルは、DACL およびベンダー固有属性（VSA）を使用して、すべての「音声」トラフィックを許可します（PERMIT_ALL_TRAFFIC）。

表 20-1　許可ポリシー、プロファイル、およびルールの設定のデフォルト （続き）

名前	ユーザ インターフェイスのパス	説明	その他の情報
許可ポリシーのデフォルト			
有線 802.1X 複合条件	**[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [許可（Authorization）] > [複合条件（Compound Conditions）] を選択します。**	この複合条件は次の属性と値をチェックします。 • RADIUS:Service-Type = Framed • RADIUS:NAS-Port-Type = Ethernet	この複合条件は、有線 802.1X 許可ポリシーで使用されます。 このポリシーで指定された基準に一致する要求は、有線 802.1X 許可ポリシーに基づいて評価されます。
Catalyst スイッチのローカル Web 認証複合条件	**[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [許可（Authorization）] > [複合条件（Compound Conditions）] を選択します。**	この複合条件は次の属性と値をチェックします。 • RADIUS:Service-Type = Outbound • RADIUS:NAS-Port-Type = Ethernet	この複合条件を使用するには、この条件を確認する許可ポリシーを作成する必要があります。
ワイヤレス LAN コントローラ（WLC）ローカル Web 認証複合条件（Wireless Lan Controller (WLC) Local Web Authentication Compound Condition）	**[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [許可（Authorization）] > [複合条件（Compound Conditions）] を選択します。**	この複合条件は次の属性と値をチェックします。 • RADIUS:Service-Type = Outbound • RADIUS:NAS-Port-Type = Wireless-IEEE802.11	この複合条件を使用するには、この条件を確認する許可ポリシーを作成する必要があります。
ブラックリストのデフォルトの許可ルール	**[ポリシー（Policy）] > [許可ポリシー（Authorization Policy）]**	この許可プロファイルでは、次の値の設定デフォルト ルールを使用します。 • [ルール名（Rule Name）]：[ブラックリストのデフォルト（Black List Default）] • [エンドポイント ID グループ（Endpoint Identity Group）]：[ブラックリスト（Blacklist）] • 条件：すべて • 権限/許可プロファイル：Blacklist_Access	このデフォルト ルールは、「失われた」ユーザ デバイスがシステムから削除されるか、または「元に戻される」まで、このようなデバイスを適切にプロビジョニングするように設計されています。

表 20-1　許可ポリシー、プロファイル、およびルールの設定のデフォルト （続き）

名前	ユーザ インターフェイスのパス	説明	その他の情報
プロファイリングされた Cisco IP Phone 許可ルール	**[ポリシー（Policy）] > [許可ポリシー（Authorization Policy）]**	この許可プロファイルでは、次の値の設定デフォルト ルールを使用します。 • [ルール名（Rule Name）] : [プロファイリングされた Cisco IP Phone（Profiled Cisco IP Phones）] • [エンドポイント ID グループ（Endpoint Identity Group）] : [Cisco-IP-Phones] • 条件：すべて • [権限/許可プロファイル（Permissions/Authorization Profile）] : [Cisco_IP_Phones]	このデフォルト ルールは、デフォルトのエンドポイント ID グループとして Cisco IP Phone を使用し、このテーブルにリストされている値を使用します。
許可ルール設定のデフォルト			
デフォルトの許可ルール	**[ポリシー（Policy）] > [許可ポリシー（Authorization Policy）]**	この許可プロファイルでは、次の値の設定デフォルト ルールを使用します。 • [ルール名（Rule Name）] : [デフォルト（Default）] • [エンドポイント ID グループ（Endpoint Identity Group）] : [任意（Any）] • 条件：すべて • [許可プロファイル（Authorization Profile）] : [PermitAccess]	このデフォルト ルールは、デフォルトのエンドポイント ID グループとして [任意（Any）] を使用し、このテーブルにリストされている値を使用します。

許可ポリシーの設定

[許可ポリシー（Authorization Policy）] ページでは、許可ポリシーを表示、作成、複製/変更、削除できます。次の許可ポリシー プロファイルの各項には、標準許可ポリシーで指示されるアクションの例が示されています。同じプロセスに従って例外許可ポリシーを管理できます。

はじめる前に

この手順を開始する前に、管理者ポータルで使用される管理およびルール ベース条件、ID グループ、状態、権限の基本構成要素と利用方法の基本を理解しておく必要があります。

ステップ 1　[ポリシー（Policy）] > [許可（Authorization）] > [標準（Standard）] を選択します。

ステップ 2　右端にある下矢印をクリックし、[新規ルールを上に挿入（Insert New Rule Above）] または [新規ルールを下に挿入（Insert New Rule Below）] のどちらかを選択します。

ステップ 3　ルール名を入力し、許可ポリシーの ID グループ、条件、属性、権限を [Identity] を選択します。

選択したすべての属性に [等しい（Equals）]、[等しくない（Not Equals）]、[一致（Matches）]、[次で始まる（Starts With）]、または [次で始まらない（Not Starts With）] の演算子オプションが含まれているとは限りません。

「Match」オペレータは、ワイルドカードのなしの正規表現（REGEX）をサポートし、使用します。

ステップ 4　[完了（Done）] をクリックします。

ステップ 5　[保存（Save）] をクリックして、変更を Cisco ISE システム データベースに保存し、この新しい許可ポリシーを作成します。

許可ポリシー条件を作成するときに、有効な属性を再利用するには、サポートされている属性を含むディクショナリから選択します。たとえば、Cisco ISE は、AuthenticationIdentityStore という属性を提供しています。これは NetworkAccess ディクショナリにあります。この属性は、ユーザの認証中にアクセスされた最後の ID ソースを識別します。

- 認証中に単一の ID ソースが使用されると、この属性には認証が成功した ID ストアの名前が含まれます。
- 認証中に ID ソース順序を使用する場合、この属性にはアクセスされた最後の ID ソースの名前が含まれます。

AuthenticationStatus 属性を AuthenticationIdentityStore 属性と組み合わせて使用し、ユーザが正常に認証された ID ソースを識別する条件を定義できます。たとえば、許可ポリシーで LDAP ディレクトリ（LDAP13）を使用してユーザが認証された条件をチェックするために、次の再利用可能な条件を定義できます。

```
If NetworkAccess.AuthenticationStatus EQUALS AuthenticationPassed AND
NetworkAccess.AuthenticationIdentityStore EQUALS LDAP13
```

（注）　AuthenticationIdentityStore は、条件にデータを入力できるテキストフィールドを表します。このフィールドには、名前を必ず正しく入力またはコピーします。ID ソースの名前が変更された場合は、ID ソースの変更と一致するように、この条件を変更する必要があります。

以前認証されたエンドポイント ID グループに基づく許可条件を定義するために、Cisco ISE では、エンドポイント ID グループ 802.1X 認証ステータスの間に定義された許可をサポートしています。Cisco ISE では、802.1X 認証を実行するとき、RADIUS 要求の「Calling-Station-ID」フィールドから MAC アドレスを抽出し、この値を使用して、デバイスのエンドポイント ID グループ（endpointIDgroup 属性として定義）のセッション キャッシュを検索して読み込みます。

このプロセスによって、許可ポリシー条件の作成に endpointIDgroup 属性を使用できるようになり、ユーザ情報に加えてこの属性を使用して、エンドポイント ID グループ情報に基づく許可ポリシーを定義できます。

エンドポイント ID グループの条件は、[許可ポリシー設定（authorization policy configuration）] ページの [ID グループ（ID Groups）] カラムで定義できます。ユーザ関連情報に基づく条件は、許可ポリシーの [その他の条件（Other Conditions）] のセクションで定義する必要があります。ユーザ情報が内部ユーザ属性に基づいている場合は、内部ユーザ ディクショナリの ID グループ属性を使用します。たとえば、「User Identity Group:Employee:US」のような値を使用して、ID グループに完全な値のパスを入力できます。

関連項目

- 「許可ポリシーの設定」（P.B-4）
- 「単純および複合条件」（P.18-1）
- 「単純条件の作成」（P.18-2）
- 「複合条件の作成」（P.18-3）

時刻と日付の条件

[ポリシー要素条件（Policy Elements Conditions）] ページを使用して、時刻と日付のポリシー要素条件を表示、作成、変更、削除、複製、および検索します。ポリシー要素は、設定した特定の時刻と日付の属性設定に基づく条件を定義する共有オブジェクトです。

時刻と日付の条件を使用すると、Cisco ISE システム リソースにアクセスする権限を、作成した属性設定で指定された特定の時刻と日付に設定または制限できます。

関連項目

- 「時刻と日付の条件の作成」（P.18-8）
- 「時刻と日付の条件の設定」（P.B-18）

許可プロファイルの権限の設定

許可プロファイルの権限設定を開始する前に、以下を確認します。

- 認可ポリシーおよび許可プロファイル間の関係を理解している
- [許可プロファイル（Authorization Profile）] ページをよく理解している
- ポリシーおよびプロファイルを設定する場合に必要な基本ガイドラインを知っている
- 認可プロファイルの権限の構成を理解している
- 次のトピックで説明されている設定のデフォルト値に注意してください。
  - 「許可ポリシーとサポートされているディクショナリ」（P.20-4）
  - 「認可ポリシーおよびプロファイル設定のガイドライン」（P.20-4）
  - 「デフォルトの許可ポリシー、ルール、プロファイル設定」（P.20-5）

ネットワークでさまざまなタイプの許可プロファイルのポリシー要素権限を表示、作成、変更、削除、複製、または検索するプロセスの開始点として [結果（Results）] ナビゲーション ペインを使用します。[結果（Results）] ペインには、最初 [認証（Authentication）]、[許可（Authorization）]、[プロファイリング（Profiling）]、[ポスチャ（Posture）]、[クライアント プロビジョニング（Client Provisioning）]、および [セキュリティ グループ アクセス（Security Group Access）] のオプションが表示されています。

許可プロファイルでは、RADIUS 要求が受け入れられたときに返される属性を選択できます。Cisco ISE では、[共通タスク（Common Tasks）] 設定を設定して共通に使用される属性をサポートできるメカニズムが提供されます。Cisco ISE が基盤となる RADIUS 値に変換する [共通タスク（Common Tasks）] 属性の値を入力する必要があります。

関連項目

「新しい標準許可プロファイル の権限の設定」（P.20-11）

新しい標準許可プロファイル の権限の設定

新しい許可プロファイル ページを使用して、新しい標準許可プロファイルを作成し、その権限を設定します。

ステップ 1　[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [許可（Authorization）] > [許可プロファイル（Authorization Profiles）] を選択します。

ステップ 2　[追加（Add）] をクリックします。

ステップ 3　必要に応じて値を入力して、新しい許可プロファイルを設定します。[名前（name）] フィールドでサポートされる文字は次のとおりです：スペース、!# $ % & " （）* + , - ./ ; = ?@ _ {.

ステップ 4　[送信（Submit）] をクリックして変更を Cisco ISE システム データベースに保存し、許可プロファイルを作成します。

関連項目

「許可プロファイルの設定」（P.B-25）

ダウンロード可能 ACL

DACL 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 DACL は、許可プロファイルに追加できます。その後、これらの許可プロファイルを許可ポリシーの結果として指定できます。

既存の DACL と同じか、または類似する新しい DACL 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、各 DACL（元の DACL および複製された DACL）に個別にアクセスして、編集または削除します。

（注）　DACL 作成中は、キーワード *Any* が DACL のすべての ACE のソースである必要があります。DACL がプッシュされると、ソースの *Any* がスイッチに接続されているクライアントの IP アドレスで置き換えられます。

関連項目

「ダウンロード可能 ACL の権限の設定」（P.20-12）

ダウンロード可能 ACL の権限の設定

[ダウンロード可能 ACL（Downloadable ACLs）] ページを使用して、新しい DACL を作成し、権限を設定します。

ステップ 1　[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [許可（Authorization）] > [ダウンロード可能 ACL（Downloadable ACLs）] を選択します。

ステップ 2　**Action** アイコンをクリックし、[DACL の作成（Create DACL）] を選択するか、[DACL 管理ページ（DACL Management）] ページにある [追加（Add）] をクリックします。

ステップ 3　DACL に値を入力します。[名前（name）] フィールドでサポートされる文字は次のとおりです：スペース、!# $ % & " （） * + , - ./ ; = ?@ _ {.

ステップ 4　[送信（Submit）] をクリックします。

DACL では、次の形式がサポートされます。

- **ACTION PROTOCOL SOURCE_SUBNET WILDCARD_MASK** [**OPERATOR**[*PORT*]] **DEST_SUBNET WILDCARD_MASK** [**OPERATOR**[*PORT*]] [*ICMP_TYPE_CODE*]

表 20-2 は DACL 形式のオプションを示しています。

表 20-2　DACL 形式のオプション

オプション	説明
ACTION	ポリシー要素の権限が、アクセスを許可または拒否するべきかどうかを指定します。
PROTOCOL	次のプロトコルのどれかを指定します。 • ICMP • UDP • TCP • IP
SOURCE_SUBNET	次の送信元サブネット形式のどれかを指定します。 • 任意 • host x.x.x.x • <サブネット>
DEST_SUBNET	次の宛先サブネット形式のどれかを指定します。 • 任意 • host x.x.x.x • <サブネット>
WILDCARD_MASK	サブネット マスクのリバースを指定します。たとえば、0.0.0.255 と入力します。

表 20-2　DACL 形式のオプション

オプション	説明
OPERATOR	次の演算子のどれかを指定します。 • eq • lt • gt • neq • range
ポート	ポートを指定します。有効な範囲は 1 ～ 65535 です。
ICMP_TYPE_CODE	次の ICMP タイプ コードのどれかを指定します。 • 0：エコー応答 • 8：エコー要求 • 3：[0 ～ 15]：宛先到達不能 • 5：[0 ～ 3]：ICMP リダイレクト

関連項目

「ダウンロード可能 ACL」（P.20-11）

Active Directory ユーザ許可のためのマシン アクセス制限

Cisco ISE には、Microsoft Active Directory 認証ユーザの許可を制御する追加の方法を提供する、マシン アクセス制限（MAR）コンポーネントが含まれています。この形式の許可は、Cisco ISE ネットワークにアクセスするために使用されるコンピュータのマシン認証に基づきます。成功したマシン認証ごとに、Cisco ISE は、RADIUS Calling-Station-ID 属性（属性 31）で受信した値を、成功したマシン認証の証拠としてキャッシュします。

Cisco ISE は、[Active Directory の設定（Active Directory Settings）] ページの [存続可能時間（Time to Live）] パラメータで設定された時間が失効になるまで各 Calling-Station-ID 属性値をキャッシュに保持します。失効したパラメータは、Cisco ISE によってキャッシュから削除されます。

ユーザをエンドユーザ クライアントから認証する場合、Cisco ISE は、成功したマシン認証の Calling-Station-ID 値のキャッシュを検索して、ユーザ認証要求で受信した Calling-Station-ID 値を見つけようとします。Cisco ISE が一致するユーザ認証 Calling-Station-ID 値をキャッシュで見つけた場合、これは、次の方法で認証を要求するユーザに Cisco ISE が権限を割り当てる方法に影響します。

- Calling-Station-ID 値が Cisco ISE キャッシュで見つかった値と一致する場合、成功した許可の許可プロファイルを割り当てます。
- Calling-Station-ID 値が Cisco ISE キャッシュの値と一致しないことがわかった場合、マシン認証のない成功したユーザ認証の許可プロファイルを割り当てます。

関連項目

「Active Directory でのユーザとマシンの認証」（P.14-9）