ACS 5.x ポリシー モデル

ACS 5.x は、ポリシーベースのアクセス コントロール システムです。ACS 5.x での*ポリシー モデル*という用語は、ポリシー管理者のポリシー要素、ポリシー オブジェクト、およびポリシー規則を表しています。ACS 5.x では、4.x バージョンで使用されていたグループベースのモデルの代わりに、ルール ベース ポリシー モデルが使用されています。

ここでは、次の内容について説明します。

（注） ACS 4.x および ACS 5.8 での概念の対応については、ACS 4.x から ACS 5.8 への機能マッピング（2-5 ページ）を参照してください。

ACS 5.x ポリシー モデルの概要

ACS 5.x のルール ベース ポリシー モデルを使用すると、以前のグループベースの手法よりも強力で柔軟なアクセス コントロールを実現できます。

以前のグループベース モデルでは、*グループ*を使用してポリシーを定義していました。これは、グループに次の 3 つのタイプの情報が結合されていたためです。

- 識別情報：この情報は、AD グループまたは LDAP グループでのメンバーシップ、または ACS 内部ユーザの静的割り当てに基づいています。
- その他の制約事項または条件：時間の制限、デバイスの制限など。
- 権限：VLAN または Cisco IOS の特権レベル。

ACS 5.x ポリシー モデルは、次の形式の*規則*に基づいています。

If *condition* then *result*

たとえば、グループベース モデルに関して記述されている次の情報を使用します。

If *identity-condition, restriction-condition* then *authorization-profile*

ACS 5.8 では、条件および結果をグローバルな共有オブジェクトとして定義します。これらを定義しておくと、規則を作成するときに参照できます。ACS 5.8 では、これらの共有オブジェクトに対して*ポリシー要素*という用語を使用しています。ポリシー要素は、規則を作成するための構築ブロックとなります。

表 3-1 に、以前のグループに含まれていたすべての情報をさまざまなポリシー要素によって定義する方法を示します。

表 3-1　　ポリシー要素の情報

ACS 4.x グループの情報	ACS 5.8 ポリシー要素の情報
識別情報	• AD グループ メンバーシップおよび属性 • LDAP グループ メンバーシップおよび属性 • ACS 内部 ID グループおよび属性
その他のポリシー条件	• 時刻と日付の条件 • カスタム条件
権限	認可プロファイル

*ポリシー*は、アクセス要求を評価して決定を返すために ACS 5.x で使用される規則セットです。規則セットの例は次のとおりです。

- *認可ポリシー*の規則セットでは、任意のアクセス要求に関する認可の決定が返されます。
- *ID ポリシー*では、任意のアクセス要求の ID 属性の認証方法および取得方法が決定されます。

ACS 5.x では、独立したポリシーの順序（ポリシー ワークフロー）が*アクセス サービス*に編成され、アクセス要求を処理するために使用されます。複数のアクセス サービスを作成して、異なる種類のアクセス要求を処理できます。たとえば、デバイス管理アクセスやネットワーク アクセスなどです。詳細については、アクセス サービス（3-5 ページ）を参照してください。

単純なポリシーおよびルール ベース ポリシーを定義できます。ルール ベース ポリシーは、さまざまな条件をテストする複雑なポリシーです。単純なポリシーでは、条件なしですべての要求に対して単一の結果を適用します。

さまざまなタイプのポリシーがあります。

さまざまなタイプのポリシーの詳細については、ポリシーのタイプ（3-5 ページ）を参照してください。

ポリシー モデルの用語の詳細については、ポリシーの用語（3-3 ページ）を参照してください。

関連項目

- ポリシーおよび ID 属性（3-17 ページ）
- サービスおよびポリシーの設定フロー（3-19 ページ）

ポリシーの用語

表 3-2 に、ルール ベース ポリシーの用語を示します。

表 3-2　ルール ベース ポリシーの用語

用語	説明
アクセス サービス	アクセス要求の処理に使用される一連のポリシー セット。ACS 5.x を使用すると、複数のアクセス サービスを定義して、独立および分離された複数のポリシー セットを単一の ACS システムでサポートできます。 2 つのデフォルト アクセス サービスがあります。1 つはデバイス管理用（デバイス シェルまたは CLI への TACACS+ ベースのアクセス）であり、もう一つはネットワーク アクセス用（ネットワーク接続への RADIUS ベースのアクセス）です。
ポリシー要素	ポリシー条件（たとえば、時刻や日付、またはユーザ選択属性に基づくカスタム条件）および権限（許可プロファイルなど）を定義するグローバルな共有オブジェクト。ポリシー要素は、ポリシー規則を作成するときに参照されます。
認可プロファイル	RADIUS ベースのネットワーク アクセス サービス用の基本的な権限コンテナであり、ネットワーク アクセス要求に許可するすべての権限を定義します。 VLAN、ACL、URL リダイレクト、セッション タイムアウト、再認可タイマー、または応答で返されるその他のあらゆる RADIUS 属性が、認可プロファイルで定義されます。
シェル プロファイル	TACACS+ ベースのデバイス管理ポリシー用の基本的な権限コンテナであり、シェル アクセス要求に許可する権限を定義します。 IOS 特権レベル、セッション タイムアウトなどがシェル プロファイルで定義されます。
コマンド セット	TACACS+ ベースの許可コマンドのセットがコマンド認可単位で格納されます。
ポリシー	特定のポリシー決定に到達するために使用される規則セット。たとえば、認証方法や許可する認可。デフォルト規則を持つポリシーの場合、ポリシーは、ユーザ作成規則と一致しない要求に対するデフォルト規則を持つ最初の一致規則テーブルになります。
ID ポリシー	任意の要求の ID 属性を認証および取得する方法を選択するための ACS 5.8 ポリシー。ACS 5.8 では、2 つのタイプの ID ポリシーを使用できます。1 つは単純で静的なポリシーで、もう 1 つはより複雑な状況で使用するルール ベース ポリシーです。
ID グループ マッピング ポリシー	ID ストアから収集された識別情報（グループ メンバーシップ、ユーザ属性など）を、単一の ACS ID グループにマッピングするための任意のポリシー。 このポリシーは、識別情報を標準化し、単なるタグまたは識別分類である単一の ID グループに要求をマッピングする場合に役立ちます。必要に応じて、ID グループを認可ポリシーの条件として使用できます。
認可ポリシー	アクセス要求に認可属性を割り当てるための ACS 5.8 ポリシー。認可ポリシーによって単一の規則が選択されたあと、その規則の結果として参照される認可プロファイルの内容が応答に読み込まれます。
例外ポリシー	認可ポリシーの特別なオプション。例外ポリシーを使用すると、認可ポリシーの例外と免除に対して使用する条件と認可の結果セットを別個に定義できます。例外ポリシーが定義されている場合は、主要な（標準）認可ポリシーの前にチェックされます。
デフォルト規則	ACS 5.8 ポリシーのキャッチオール規則。この規則を編集して、デフォルトの結果または認可アクションを指定できます。この規則は、特定の要求が、ユーザ作成規則で指定されている条件と一致しなかった場合のポリシー決定として使用できます。

単純なポリシー

すべての ACS ポリシーをルール ベース ポリシーとして設定できます。ただし、場合によっては、条件なしですべての要求に適用する単一の結果を選択する単純なポリシーを設定することもできます。

たとえば、さまざまな条件の規則セットを含むルール ベースの認証ポリシーを定義できます。または、内部データベースをすべての認証に使用する場合は、単純なポリシーを定義できます。

表 3-3 は、各ポリシー タイプが単純なポリシーとして設定できるかどうかを判断する場合に役立ちます。

- 単純なポリシーを作成および保存してからルール ベースのポリシーに変更すると、単純なポリシーはルール ベースのポリシーのデフォルト規則になります。
- ルール ベース ポリシーを保存してから単純なポリシーに変更した場合、ACS ではデフォルト規則が単純なポリシーとして自動的に使用されます。

関連項目

- ポリシーのタイプ（3-5 ページ）

ルール ベース ポリシー

ルール ベース ポリシーは、ID ベース ポリシーでの課題を克服するために導入されました。以前のバージョンの ACS では、ユーザ グループのメンバーシップによってメンバーにアクセス権が付与されていましたが、特定の制限も課されていました。

ユーザがアクセスを要求すると、ID ストアを使用してそのユーザのクレデンシャルが認証され、そのユーザは適切なユーザ グループに関連付けられます。認可はユーザ グループと関連付けられているため、ユーザ グループのすべてのメンバーは常に同じアクセス制限と権限を持ちます。

このタイプのポリシー（単純なポリシー）では、権限は特定のユーザ グループとのユーザの関連付けに基づいて付与されます。これは、ユーザの ID だけが主要な条件である場合に役立ちます。ただし、さまざまな条件下で異なる権限が必要なユーザの場合、このポリシーは機能しません。

ACS 5.x では、ID に関係なくさまざまな条件に基づく規則を作成できます。ユーザ グループにすべての情報が含まれるわけではありません。

たとえば、従業員がキャンパスで勤務しているときにはフル アクセスを許可し、リモートで勤務しているときにはアクセスを制限する場合は、ACS 5.8 でルール ベース ポリシーを使用してこれを実現できます。

ID 以外のさまざまな条件に基づいて権限を設定することができ、権限はユーザ グループに関連付けられなくなりました。セッション属性および環境属性（アクセス場所、アクセス タイプ、端末の健全性、日付、時刻など）を使用して、許可するアクセスのタイプを決定できます。

認可は、次のように規則セットに基づいています。

If *conditions* then *apply the respective permissions*

ルール ベース ポリシーでは、条件は使用可能なセッション属性の任意の組み合わせで構成可能であり、権限は認可プロファイルで定義されます。VLAN、ダウンロード可能 ACL、QoS 設定、および RADIUS 属性を含めるように認可プロファイルを定義します。

ポリシーのタイプ

表 3-3 に、ACS で設定可能なポリシーのタイプを示します。

ポリシーは評価順に示されています。あるポリシーで取得された属性は、そのポリシー以降のすべてのポリシーで使用できます。唯一の例外は、ID ストアからの属性だけを使用する ID グループ マッピング ポリシーです。

表 3-3　　ACS ポリシー タイプ

ポリシー	例外ポリシーを含めることができるかどうか	単純[1] およびルール ベースのポリシー	条件に使用できるディクショナリ	使用可能な結果タイプ	取得される属性
サービス セレクション 着信要求に適用するアクセス サービスを決定します。	いいえ	はい	ID ストア関連以外すべて	アクセス サービス	—
ID 認証用の ID ソースを決定します。	いいえ	はい	ID ストア関連以外すべて	ID ソース、エラー オプション	ID 属性、内部 ID ストアの ID グループ
ID グループ マッピング 外部 ID ストアから ACS ID グループへの属性およびグループのマッピングを定義します。	いいえ	はい	ID ストア ディクショナリだけ	IDグループ	外部 ID ストアの ID グループ
ネットワーク アクセス認可 ネットワーク アクセス用の認可および権限を決定します。	はい	ルール ベースだけ	すべてのディクショナリ	認可プロファイル、セキュリティ グループ アクセス	—
デバイス管理の認可 デバイス管理用の認可および権限を決定します。	はい	ルール ベースだけ	すべてのディクショナリ	シェル プロファイル、コマンド セット	—

1. 単純なポリシーでは、ACS がすべての要求に適用する単一の結果セットを指定します。つまり、実際には単一規則ポリシーです。

アクセス サービス

アクセス サービスは、ACS 5.x での不可欠な構成要素です。アクセス サービスを使用すると、ネットワークに接続するユーザとデバイス、およびネットワーク デバイスを管理する管理者用のアクセス ポリシーを設定できます。

ACS 5.x では、認証要求および認可要求はアクセス サービスによって処理されます。アクセス サービスは、次の要素で構成されています。

- ID ポリシー：ユーザの認証方法を指定します。パスワードの確認に使用される、許可された認証プロトコルおよびユーザ リポジトリが含まれています。
- グループ マッピング ポリシー：ユーザの ACS ID グループが、外部 ID ストアのユーザ属性またはグループ メンバーシップに基づいてダイナミックに設定されるかどうかを指定します。ユーザの ID グループをユーザの認可の一部として使用できます。
- 認可ポリシー：ユーザの認可規則を指定します。

アクセス サービスは、アクセス要求の処理に使用される、独立したポリシー セットです。

ACS 管理者は、さまざまな種類のアクセス要求の処理を明確に区別および分離するために、複数のアクセス サービスを作成できます。ACS では、次の 2 つのデフォルト アクセス サービスが提供されています。

- Default Device Admin：デバイス CLI への TACACS+ ベースのアクセスに使用
- Default Network Access：ネットワーク接続への RADIUS ベースのアクセスに使用

これらのアクセス サービスをそのまま使用したり、必要に応じて変更または削除したりできます。追加のアクセス サービスを作成することもできます。

TACACS+ プロトコルによって、認証が認可から分離されます。つまり、ACS では、TACACS+ 認証要求と認可要求が個別に処理されます。表 3-4 に、RADIUS アクセス サービスと TACACS+ アクセス サービスのその他の相違点を示します。

表 3-4　RADIUS アクセス サービスと TACACS+ アクセス サービス

ポリシー タイプ	TACACS+	RADIUS
Identity	任意[1]	必須
Group Mapping	任意	任意
Authorization	任意[1]	必須

1. TACACS+ の場合、ID または認可を選択する必要があります。

TACACS+ の場合、すべてのポリシー タイプが任意ですが、1 つのサービスで少なくとも 1 つのポリシー タイプを選択する必要があります。TACACS+ の ID ポリシーを定義していない場合は、ACS によって認証要求に対して認証エラーが返されます。

同様に、認可ポリシーを定義していない場合に、ACS がセッションまたはコマンドの認可要求を受信すると、その要求は失敗します。RADIUS アクセス サービスと TACACS+ アクセス サービスの両方で、サービスの作成後、ポリシーを追加するためにサービスを変更できます。

（注） アクセス サービスにはサービス セレクション ポリシーは含まれていません。サービス セレクション規則は独立して定義されています。

複数のアクセス サービス（さまざまな使用例、ネットワーク、地域、管理ドメイン用のサービスなど）を保持および管理できます。サービス セレクション ポリシーを設定します。サービス セレクション ポリシーとは、各新規アクセス要求を適切なアクセス サービスに送信するサービス セレクション規則セットのことです。

表 3-5 に、アクセス サービス セットの例を示します。

表 3-5　アクセス サービス リスト

アクセス サービス A（デバイス管理用）	アクセス サービス B（802.1X エージェントレス ホストへのアクセス用）	アクセス サービス C（802.1X 有線および無線デバイスからのアクセス用）
ID ポリシー A	ID ポリシー B	ID ポリシー C
シェル/コマンド認可ポリシー A	セッション認可ポリシー B	セッション認可ポリシー C

表 3-6 に、サービス セレクション ポリシーを示します。

表 3-6　　サービス セレクション ポリシー

ルール名	条件	結果
DevAdmin	protocol = TACACS+	アクセス サービス A
Agentless	Host Lookup = True	アクセス サービス C
Default	—	アクセス サービス B

ACS 5.8 は、TACACS+ アクセス要求を受信すると、ID ポリシー A に従って要求を認証するアクセス サービス A を適用したあと、シェル/コマンド認可ポリシーに従って認可および権限を適用します。このサービスによって、すべての TACACS+ 要求が処理されます。

ACS 5.8 は、ホスト ルックアップであると判断した RADIUS 要求（たとえば、RADIUS の service-type 属性が *call-check* と同一）を受信すると、ID ポリシー C に従って認証するアクセス サービス C を適用します。次いで、セッション認可ポリシー C に従ってセッション認可プロファイルを適用します。このサービスはホスト ルックアップのすべての要求（MAC Auth Bypass 要求としても知られている）を処理します。

アクセス サービス B によって、その他の RADIUS 要求が処理されます。このアクセスサービスは、ID ポリシー B に従って認証し、セッション認証ポリシー B を適用します。このサービスによって、上記の規則で処理されるホスト ルックアップを除き、すべての RADIUS 要求が処理されます。

アクセス サービス テンプレート

ACS では、新しいサービスを作成するときにテンプレートとして使用できる定義済みのアクセス サービスが提供されています。アクセス サービス テンプレートを選択すると、ACS によって、ポリシー セットが含まれたアクセス サービスが作成され、それぞれのサービスにカスタマイズされた条件セットが設定されます。

サービスにポリシーを追加したり、サービスからポリシーを削除したりすることにより、アクセス サービスの構造を変更できます。また、ポリシー条件セットを変更することにより、ポリシーの構造を変更することもできます。アクセス サービス テンプレートおよび説明のリストについては、アクセス サービス テンプレートの設定（10-22 ページ）を参照してください。

RADIUS および TACACS+ プロキシ サービス

ACS 5.8 は、RADIUS、RADIUS プロキシまたは TACACS+ プロキシ サーバとして機能できます。

- RADIUS プロキシ サーバとしての場合、ACS は NAS から認証要求およびアカウンティング要求を受信し、これらの要求を外部 RADIUS サーバに転送します。
- TACACS+ プロキシ サーバとしての場合、ACS は NAS から認証、許可、およびアカウンティング要求を受信し、これらの要求を外部 TACACS+ サーバに転送します。

ACS は要求の結果を受け入れて NAS に返します。ACS で RADIUS および TACACS+ サーバに要求が転送されるように、外部 RADIUS および TACACS+ サーバを ACS で設定する必要があります。タイムアウト時間および接続試行回数を定義できます。

ACS プロキシのリモート ターゲットは、次のパラメータを含むリモート RADIUS および TACACS+ サーバのリストです。

- IP
- 認証ポート
- アカウンティング ポート

- 共有秘密キー
- 応答タイムアウト
- リトライ回数
- 接続ポート
- ネットワーク タイムアウト

プロキシ サービスでは次の情報を使用できます。

- リモート RADIUS または TACACS+ サーバ リスト
- アカウンティング プロキシ ローカル/リモート/両方
- ユーザ名からのプレフィックス/サフィックスのストリッピング

RADIUS プロキシ サーバは、要求を受信すると、リスト内の最初のリモート RADIUS または TACACS+ サーバにその要求を転送します。プロキシ サーバは、指定されたタイムアウト間隔および試行回数内に応答を受信しない場合、その要求をリスト内の次の RADIUS または TACACS+ サーバに転送します。

最初の応答をリスト内のいずれかのリモート RADIUS または TACACS+ サーバから受信すると、プロキシ サービスによってその応答が処理されます。応答が有効な場合は、ACS によってその応答が NAS に戻されます。

表 3-7に、ACS 4.2 リリースと 5.8 リリース間での RADIUS プロキシ サービスの相違点を示します。

表 3-7　　ACS 4.2 と 5.8 間での RADIUS および TACACS+ プロキシ サービスの相違点

機能	ACS 5.8	ACS 4.2
設定可能なタイムアウト（RADIUS）	はい	いいえ
設定可能な再試行カウント（RADIUS）	はい	いいえ
ネットワーク タイムアウト（TACACS+）	はい	いいえ
認証ポートおよびアカウンティング ポート（RADIUS）	はい	はい
接続ポート（TACACS+）	はい	いいえ
プロキシ サイクルの検出	はい（RADIUS の場合のみ）	いいえ
ユーザ名のストリッピング	はい	はい
アカウンティング プロキシ（ローカル、リモート、または両方）	はい	はい
アカウント遅延タイムアウトのサポート（RADIUS）	いいえ	いいえ

ACS は、複数の外部 RADIUS および TACACS+ サーバへのプロキシ サーバとして同時に機能できます。ACS がプロキシ サーバとして機能するには、ACS で RADIUS または TACACS+ プロキシ サービスを設定する必要があります。RADIUS プロキシ サービスの設定方法については、アクセスサービスの一般プロパティの設定（10-13 ページ）を参照してください。

RADIUS および TACACS+ 要求のプロキシ処理の詳細については、RADIUS および TACACS+ プロキシ要求（4-29 ページ）を参照してください。

関連項目

- ポリシーの用語（3-3 ページ）
- ポリシーのタイプ（3-5 ページ）
- サービスおよびポリシーの設定フロー（3-19 ページ）

ID ポリシー

次の 2 つの主要メカニズムによって、要求の認証に使用されるメカニズムとソースが定義されます。

- パスワードベース：ユーザがユーザ名とパスワードを入力したあと、データベースに照らして認証が実行されます。MAC アドレスを指定することにより、ホストでこの認証をバイパスできます。ただし、ID ポリシー認証の場合は、ホスト ルックアップもパスワードベースであると見なされます。
- 証明書ベース：クライアントがセッション認証用の証明書を提示します。ACS 5.8 では、証明書ベースの認証は、PEAP-TLS または EAP-TLS プロトコルを選択した場合に発生します。

また、要求内のプリンシパルの属性を取得するためにデータベースを使用できます。

ID ソースは、ID ポリシーの 1 つの結果であり、次のいずれかのタイプになります。

- アクセス拒否：ユーザへのアクセスは拒否され、認証は実行されません。
- ID データベース：単一の ID データベース。ID ポリシーの結果として単一の ID データベースが選択された場合、外部データベース（LDAP や AD）または内部データベース（ユーザやホスト）のいずれかが結果として選択されます。

  選択されたデータベースを使用してユーザ/ホストの認証が行われ、そのユーザ/ホストに関してデータベースに格納されている定義済み属性が取得されます。
- 証明書認証プロファイル：証明書の構造および内容が含まれており、具体的には証明書属性を内部ユーザ名にマッピングします。証明書ベースの認証の場合は、証明書認証プロファイルを選択する必要があります。

  証明書ベースの要求の場合、証明書を使用して自身を特定するエンティティは、証明書に格納されている公開キーに関連付けられている秘密キーを保持します。証明書認証プロファイルでは、次のことを定義することにより、基本的な PKI 処理が拡張されています。
  - ユーザ名の定義に使用される証明書属性。証明書属性のサブセットを選択して、要求のコンテキストにユーザ名フィールドを読み込むことができます。このユーザ名は、要求の残りのユーザを識別する場合に使用されます。ログで使用される識別情報にも使用されます。
  - 証明書の失効ステータスの確認に使用される LDAP または AD データベース。LDAP または AD データベースを選択すると、証明書データが LDAP または AD データベースから取得され、クライアントが入力したデータに照らして比較されて、クライアント証明書の追加確認が行われます。
- ID 順序：ID データベースの順序。この順序は認証に使用されます。追加の順序が指定されている場合は、その追加順序を使用して属性だけが取得されます。ID ポリシーの結果として複数の ID 方式を選択できます。ID 方式を ID 順序オブジェクトで定義します。ID 順序には任意のタイプの方式を含めることができます。

  ID 順序には 2 つのコンポーネントがあります。1 つは認証用であり、もう一つは属性取得用です。管理者は、証明書および ID データベースのいずれか、またはその両方に基づいて認証を実行できます。
  - 証明書に基づいて認証を実行する場合は、ACS によって単一の証明書認証プロファイルが選択されます。
  - ID データベースに基づいて認証を実行する場合は、認証が成功するまで順番にアクセスされるデータベースのリストを定義する必要があります。認証が成功すると、データベース内の定義済み属性が取得されます。

また、任意のデータベース リストを定義して、そこから追加属性を取得することもできます。これらの追加データベースには、使用された認証がパスワードベースであるか証明書ベースであるかに関係なく、アクセスできます。

証明書ベースの認証が使用された場合、ユーザ名フィールドは、証明書属性から読み込まれ、属性の取得に使用されます。リストで定義されているすべてのデータベースにアクセス可能であり、ユーザに一致するレコードが見つかった場合は、対応する属性が取得されます。

ユーザのパスワードに要変更のマークが付いている場合でも、またはユーザ アカウントがディセーブルになっている場合でも、そのユーザの属性を取得できます。ユーザのアカウントをディセーブルにした場合でも、そのユーザの属性は属性ソースとして引き続き使用できます。ただし、認証には使用できません。

エラー オプション

ID ポリシーの処理中にエラーが発生した場合、そのエラーは次の 3 つの主要タイプのいずれかになります。

- Authentication failed：ACS は、認証が失敗したことを示す明示的な応答を受信します。たとえば、正しくないユーザ名やパスワードが入力された場合、またはユーザがディセーブルにされた場合があります。
- User/host not found：指定されたユーザ/ホストが認証データベースで見つかりませんでした。
- Process failed：定義されたデータベースへのアクセス中にエラーが発生しました。

ID データベースから返されたすべてのエラーは、上記のいずれかのタイプになります。各エラー タイプに対して、次のオプションを設定できます。

- Reject：ACS によって拒否応答が送信されます。
- Drop：応答は返されません。
- Continue：ACS によって、サービスで定義されている次のポリシーに対して処理が続行されます。

認証ステータス システム属性で、ID ポリシー処理の結果が保持されます。エラーの発生時にポリシー処理の続行を選択した場合は、後続のポリシー処理でこの属性を条件として参照して、ID ポリシー処理が成功しなかった場合を区別できます。

使用される基本プロトコルでの制限が原因で、[Continue] オプションを選択しても処理を続行できない場合があります。このことは PEAP、LEAP、および EAP-FAST の場合に該当し、[Continue] オプションを選択しても要求は拒否されます。

規則を作成する場合、次のデフォルト値をエラー オプションに使用できます。

- Authentication failed：デフォルトは *reject* です。
- User/host not found：デフォルトは *reject* です。
- Process failure：デフォルトは *drop* です。

グループ マッピング ポリシー

ID グループ マッピング ポリシーは、標準ポリシーです。条件は、外部属性ストアだけ、または証明書から取得される属性またはグループに基づきます。結果は ID グループ階層内の ID グループになります。

ID ポリシーが内部ユーザまたはホスト ID ストアにアクセスすると、対応するユーザまたはホスト レコードから ID グループが直接設定されます。この処理は、グループ マッピング ポリシーの暗黙的な処理部分です。

したがって、このデフォルト規則は、グループ マッピング ポリシーの処理の一部として、次の条件が両方とも満たされる場合にだけ適用されます。

- グループ マッピング テーブル内のいずれの規則も一致しない。
- ID グループが内部ユーザまたはホスト レコードから設定されていない。

グループ マッピング ポリシーの結果は、システム ディクショナリ内の **IdentityGroup** 属性に格納され、ID グループ条件を選択することにより、ポリシーにこの属性を含めることができます。

デバイス管理用の認可ポリシー

シェル プロファイルによってデバイス CLI へのアクセスが決まります。コマンド セットによってコマンド認可ごとの TACACS+ が決まります。デバイス管理アクセス サービス用の認可ポリシーでは、単一のシェル プロファイルおよび複数のコマンド セットを含めることができます。

複数のコマンド セットを持つ規則の処理

認可ポリシーに複数のコマンド セットを持つ規則が含まれている場合は、ACS によってアクセス要求内のコマンドが処理される方法を理解することが重要です。規則の結果に複数のコマンド セットが含まれており、その規則の条件がアクセス要求に一致した場合、ACS では、その規則内の各コマンド セットに照らしてアクセス要求内のコマンドが処理されます。

ステップ 1　コマンド セットにコマンドとその引数との一致が含まれる場合、その一致が *Deny Always* であると、ACS によってそのコマンド セットは *Commandset-DenyAlways* として指定されます。

ステップ 2　コマンド セット内のコマンドの一致に *Deny Always* がない場合は、最初の一致が見つかるまで、コマンド セット内のすべてのコマンドが順番にチェックされます。

- 最初の一致が *Permit* である場合、そのコマンド セットは *Commandset-Permit* として指定されます。
- 最初の一致が *Deny* である場合、そのコマンド セットは *Commandset-Deny* として指定されます。

ステップ 3　ACS は、すべてのコマンド セットを分析したあと、コマンドを次のように認可します。

a. コマンド セットが *Commandset-DenyAlways* として指定された場合、ACS によってそのコマンドは拒否されます。

b. *Commandset-DenyAlways* がない場合、コマンド セットが *Commandset-Permit* である場合はそのコマンドが許可されます。そうでない場合、そのコマンドは拒否されます。

関連項目

- ポリシーの用語（3-3 ページ）
- ネットワーク アクセスの認可プロファイル（3-17 ページ）

認可ポリシーの例外規則

現実世界での一般的な問題は、日々の運用で、ポリシーの免除または例外を許可する必要が頻繁に発生することです。特定のユーザが、特殊なアクセスを短期間必要とする場合があります。または、あるユーザが休暇中の他のユーザの代理を務めるために追加のユーザ権限を必要とする場合があります。

ACS では、認可ポリシーの例外ポリシーを定義できます。例外ポリシーには、ポリシーの例外および免除用の個別のポリシー セットが含まれています。これらは、通常、臨時および一時的なものです。例外規則は、主要規則テーブルの規則よりも優先されます。

例外規則では、主要ポリシーとは異なる条件および結果セットを使用できます。たとえば、主要ポリシーでは条件として ID グループと場所を使用し、関連する例外ポリシーでは異なる条件を使用することがあります。

デフォルトでは、例外ポリシーは複合条件および時刻と日付の条件を使用します。時刻と日付の条件は、例外規則に明確な開始時刻と終了時刻を設定する必要がある場合は特に重要となります。

例外ポリシーは、主要ポリシーよりも優先されます。例外ポリシーには、例外ポリシー独自のデフォルト規則は必要ありません。例外ポリシーで一致が見つからなかった場合は、独自のデフォルト規則を持つ主要ポリシーが適用されます。

例外を使用すると、標準ポリシーの一時的変更に対処できます。たとえば、あるグループの管理者 *John* が休暇中で、別のグループの管理者 *Bob* がその代理を務める場合、*John* と同じアクセス権を休暇の間 *Bob* に付与する例外規則を作成できます。

関連項目

- ポリシーの用語（3-3 ページ）
- ポリシーの条件（3-16 ページ）
- ポリシーの結果（3-16 ページ）
- ポリシーおよび ID 属性（3-17 ページ）

サービス セレクション ポリシー

ACS では、さまざまなアクセス要求を受信すると、サービス セレクション ポリシーを使用してこれらの要求が処理されます。次の 2 つのモードのサービス セレクションが提供されています。

- 単純なサービス セレクション（3-12 ページ）
- ルール ベースのサービス セレクション（3-13 ページ）

単純なサービス セレクション

単純なサービス セレクション モードでは、ACS によってすべての AAA 要求が 1 つのアクセス サービスを使用して処理されます。実際にはサービスは選択されません。

ルール ベースのサービス セレクション

ルール ベースのサービス セレクション モードでは、さまざまな設定可能オプションに基づいて、使用するアクセス サービスが決定されます。オプションの一部を次に示します。

- AAA Protocol：要求に使用されるプロトコル。TACACS+ または RADIUS です。
- Request Attributes：要求内の RADIUS 属性または TACACS+ 属性。
- Date and Time：ACS が要求を受信した日付および時刻。
- Network Device Group：AAA クライアントが属しているネットワーク デバイス グループ。
- ACS Server：要求を受信する ACS サーバ。
- AAA Client：要求を送信した AAA クライアント。
- Network condition objects：ネットワーク条件の基になるもの。
  - End Station：接続を開始および終了する端末。
  - Device：要求を処理する AAA クライアント。
  - Device Port：この条件では、デバイス以外に、端末が関連付けられているポートもチェックされます。

ポリシー条件の詳細については、ポリシー条件の管理（9-1 ページ）を参照してください。

ACS は、2 つのデフォルト アクセス サービス（Default Device Admin および Default Network Access）を使用して事前設定されています。ルール ベースのサービス セレクション モードは、AAA プロトコルを選択基準として使用するように設定されています。このため、TACACS+ 要求を受信した場合は Default Device Admin サービスが使用され、RADIUS 要求を受信した場合は Default Network Access サービスが使用されます。

アクセス サービスおよびサービス セレクションのシナリオ

ACS を使用すると、組織では、複数のシナリオ（有線、無線、リモート VPN、デバイス管理など）で ID 要件およびアクセス コントロール要件を管理できます。アクセス サービスは、これらのさまざまなシナリオをサポートする場合に主要な役割を果たします。

アクセス サービスを使用すると、独立した個別のネットワーク アクセス ポリシーを作成して、さまざまなネットワーク アクセス シナリオにおける固有のポリシー要件に対処できます。さまざまなシナリオに対して個別のポリシーを使用すると、組織のネットワークをより適切に管理できます。

たとえば、デバイス管理とネットワーク アクセスに使用するデフォルトのアクセス サービスには、ネットワーク デバイスにアクセスするネットワーク管理者と、企業のネットワークにアクセスする組織のスタッフとの典型的な区別がポリシーに反映されています。

ただし、複数のアクセス サービスを作成すると、さまざまな管理ドメインを区別できます。たとえば、アジア太平洋地域での無線アクセスを、ヨーロッパのユーザによる無線アクセスを管理しているチームとは異なるチームが管理できます。この場合、次のアクセス サービスが必要となります。

- APAC ワイヤレス：アジア太平洋地域のワイヤレス ユーザ用のアクセス サービス。
- ヨーロッパ ワイヤレス：ヨーロッパ諸国のワイヤレス ユーザ用のアクセス サービス。

追加のアクセス サービスを作成することにより、単一のアクセス サービス内に複数のポリシーが存在する複雑な状況を軽減できます。このためには、複数のアクセス サービス間で複合ポリシーを作成します。たとえば、大規模な組織で 802.1x ネットワーク アクセスを展開する場合、次のアクセス サービスが可能となります。

- 802.1x：常勤スタッフのマシン、ユーザ パスワード、および証明書ベースの認証用。
- エージェントレス デバイス：電話やプリンタなど、EAP サプリカントを持たないデバイス用。
- ゲスト アクセス：ゲスト無線ネットワークにアクセスするユーザ用。

この例では、802.1x、エージェントレス デバイス、およびゲスト アクセス用のネットワーク アクセス ポリシーを 1 つのアクセス サービスで作成する代わりに、このポリシーを 3 つのアクセス サービスに分割します。

最初の一致規則テーブル

ACS 5.8 では、規則セットを評価するための最初の一致規則テーブルを使用してポリシーを決定できます。規則テーブルには条件および結果が含まれています。条件は、単純または複合のいずれかとなります。単純な条件は、属性演算子値で構成され、True または False のいずれかとなります。複合条件には、AND または OR 演算子で結合された、より複雑な条件が含まれています。詳細については、「ポリシーの条件（3-16 ページ）」を参照してください。

管理者は、ポリシーに含める単純な条件を選択します。これらの条件は規則テーブルでカラムとして表示されます。規則テーブルでは、カラム見出しは条件の名前になり、通常は属性の名前です。

規則はカラム見出しの下に表示され、各セルには、条件を形成するために属性と結合される演算子および値が表示されます。[ANY] の場合、図 3-1（14 ページ）に定義済みの条件タイプが含まれているカラムベースの規則テーブルを示します。

図 3-1　　ポリシー規則テーブルの例

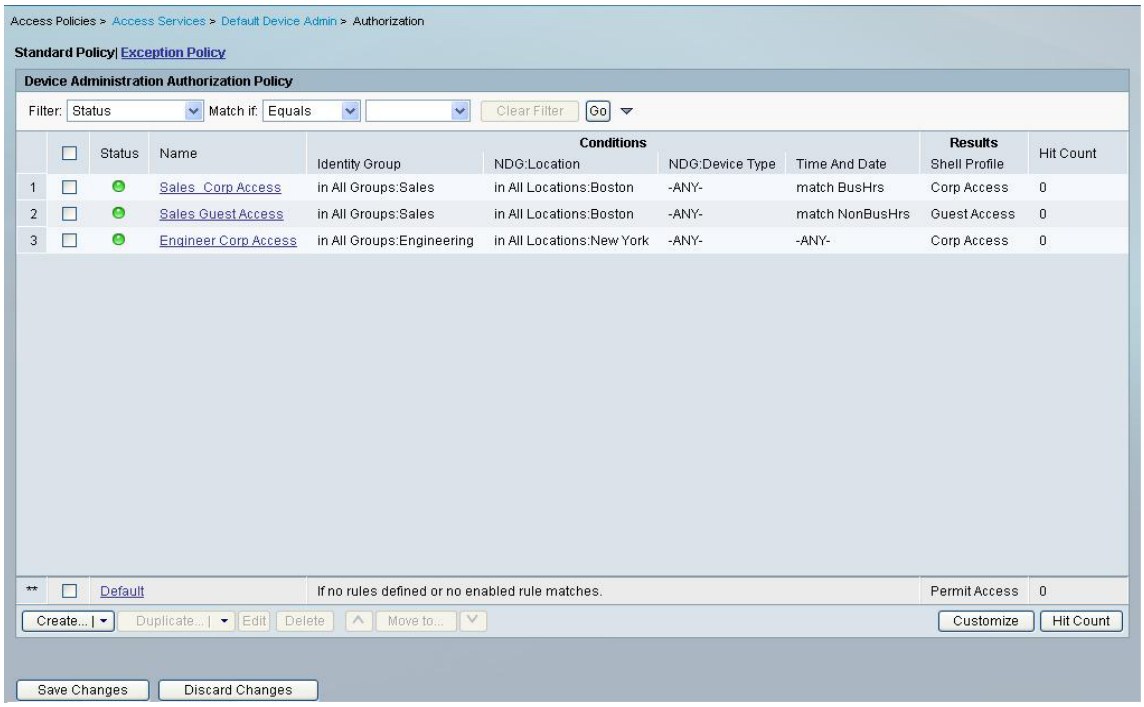


表 3-8　ポリシー規則の例

カラム	説明
Status	規則のステータスを、次のようにイネーブル、ディセーブル、または監視対象として定義できます。 • Enabled：ACS は、イネーブルにされた規則を評価し、規則の条件がアクセス要求に一致すると、規則の結果を適用します。 • Disabled：規則が規則テーブルに表示されますが、ACS はその規則をスキップし、評価しません。 • Monitor Only：ACS は監視対象の規則を評価します。規則の条件がアクセス要求と一致すると、ACS は、その一致に関する情報を含むログ レコードを作成します。 結果は適用しないで、以降の規則に対して処理を続行します。規則の使用開始時にこのステータスを使用して、その規則が必要であるかどうかを確認します。
Name	説明的な名前。規則の目的を示す任意の名前を指定できます。デフォルトでは、ACS によって規則名ストリング [rule-number] が生成されます。
条件	
Identity Group	この例では、内部 ID グループの 1 つと照合されます。
NDG: Location	Location ネットワーク デバイス グループ。2 つの事前定義済みの NDG は、Location および Device Type です。
結果	
Shell Profile	デバイス管理タイプのポリシーに使用され、TACACS+ シェル アクセス要求用の権限（Cisco IOS 特権レベルなど）が含まれています。
Hit Counts	ポリシーのヒット カウンタの最後のリセット以降、規則が着信要求と一致した回数が表示されます。ACS では、監視対象の規則またはイネーブルになっている規則に関して、すべての条件が着信要求と一致した場合に、ヒットをカウントします。次にヒット カウントの説明を示します。 • イネーブルになっている規則のヒット カウントは、ACS が要求を処理するときに発生した一致を示します。 • 監視対象の規則のヒット カウントは、ACS が要求を処理するときに規則がイネーブルになっていた場合に、それらの規則の結果となるカウントを示します。 ACS 展開内のプライマリ サーバによってヒット カウントが表示されます。このカウントは、ACS 展開でのすべてのサーバにおける各規則の一致合計を示しています。セカンダリ サーバでは、ポリシー テーブルのすべてのヒット カウントはゼロと表示されます。

デフォルト規則では、他の規則が存在しないか、またはアクセス要求内の属性値が規則と一致しない場合に ACS で使用されるポリシー結果が指定されています。

ACS は、現在のアクセス要求に関連付けられている属性値を、規則で表されている条件セットと比較することによって、最初の一致規則テーブル内の規則セットを評価します。

- 属性値が条件に一致しない場合、ACS は規則テーブル内の次の規則に進みます。
- 属性値が条件と一致すると、その規則で指定されている結果が ACS によって適用され、残りの規則はすべて無視されます。
- 属性値がいずれの条件とも一致しない場合は、ポリシーのデフォルト規則で指定されている結果が適用されます。

関連項目

- ポリシーの用語（3-3 ページ）
- ポリシーの条件（3-16 ページ）
- ポリシーの結果（3-16 ページ）
- 認可ポリシーの例外規則（3-12 ページ）

ポリシーの条件

次の条件内の属性に基づいて、単純な条件を規則テーブルに定義できます。

- Customizable conditions：ACS が認識するプロトコル ディクショナリおよび ID ディクショナリに基づいたカスタム条件を作成できます。ポリシー規則ページでカスタム条件を定義します。個別の条件オブジェクトとして定義することはできません。
- Standard conditions：デバイス IP アドレス、プロトコル、ユーザ名関連のフィールドなど、常に使用可能な属性に基づいた標準条件を使用できます。

関連項目

- ポリシーの用語（3-3 ページ）
- ポリシーの結果（3-16 ページ）
- 認可ポリシーの例外規則（3-12 ページ）
- ポリシーおよび ID 属性（3-17 ページ）

ポリシーの結果

ポリシー規則には、ポリシーのタイプに応じた結果情報が含まれています。独立した共有オブジェクトとしてポリシーの結果を定義します。ポリシーの結果はユーザまたはユーザ グループの定義には関連付けられません。

たとえば、認可ポリシー用の認可結果と権限結果を定義するポリシー要素を次に示します。

- ID ポリシーの結果としての ID ソースおよびエラー オプション。ネットワーク アクセスの認可プロファイル（3-17 ページ）を参照してください。
- グループ マッピングの ID グループ。グループ マッピング ポリシー（3-10 ページ）を参照してください。
- ネットワーク アクセスの認可プロファイル（3-17 ページ）。
- デバイス管理用の認可ポリシー（3-11 ページ）。
- Cisco Security Group Access のセキュリティ グループおよびセキュリティ グループ アクセス コントロール リスト（ACL）。ACS とシスコ セキュリティ グループ アクセス（4-24 ページ）を参照してください。

その他のポリシー結果については、認可および権限の管理（9-18 ページ）を参照してください。

関連項目

- ポリシーの用語（3-3 ページ）
- ポリシーの条件（3-16 ページ）
- 認可ポリシーの例外規則（3-12 ページ）
- ポリシーおよび ID 属性（3-17 ページ）

ネットワーク アクセスの認可プロファイル

認可プロファイルでは、認可の成功後に ACS によってユーザに返される RADIUS 属性セットを定義します。アクセス認可情報には、認可特権と権限、およびダウンロード可能 ACL などのその他の情報が含まれています。

複数の認可プロファイルをネットワーク アクセス ポリシー結果として定義できます。この方法では、規則の結果として認可プロファイルを組み合わせて使用できるため、個々のプロファイルで組み合わせ自体をすべて保持するよりも、保持する認可プロファイルの数が少なくなります。

複数の認可プロファイルを含む規則の処理

セッション認可ポリシーには、複数の認可プロファイルを持つ規則を含めることができます。認可プロファイルには、一般情報（名前と説明）および RADIUS 属性だけが含まれています。複数の認可プロファイルを使用した場合は、ACS によってそれらのプロファイルが単一の属性セットにマージされます。特定の属性の出現状況によって、次のように処理されます。

- 結果として生成される認可プロファイルの 1 つだけに出現する場合、属性はその認可結果に含められます。
- 結果プロファイルに複数回出現する場合は、結果セットで最初に出現したプロファイル内の属性値に基づいて、認可結果の属性値が決定されます。

  たとえば、VLAN が最初のプロファイルに出現する場合、リスト内の 2 番めまたは 3 番めのプロファイルに出現する VLAN よりも優先されます。

（注） 複数の認可プロファイルを使用する場合は、優先順位の高い順に並べる必要があります。

プロトコル ディクショナリ内の RADIUS 属性定義では、属性が応答で 1 回だけ出現するか、または複数回出現するかを指定します。いずれの場合も、応答で属性値が何回出現するかにかかわらず、ACS によって、1 つのプロファイルだけから任意の属性の値が取得されます。唯一の例外は、Cisco Attribute Value（AV）ペアです。このペアは、結果に含まれるすべてのプロファイルから取得されます。

関連項目

- ポリシーの用語（3-3 ページ）
- デバイス管理用の認可ポリシー（3-11 ページ）

ポリシーおよび ID 属性

ID ストアには、ポリシー条件の一部として、認可結果で使用できる ID 属性が含まれています。ポリシーを作成するときに、ID 属性およびユーザ属性を参照できます。

これにより、認可規則内の権限にグループを直接マッピングする際の柔軟性が高まります。ACS がユーザまたはホストの要求を処理するときに、ID 属性が取得され、認可ポリシー条件で使用できるようになります。

たとえば、ACS 内部ユーザの ID ストアを使用する場合、その内部ユーザの ID グループを参照したり、その内部ユーザの属性を参照したりできます（ACS では、内部 ID ストア レコード用に追加のカスタム属性を作成できることに注意してください）。

外部 Active Directory（AD）を使用している場合は、AD グループを認可規則で直接参照できます。また、AD ユーザ属性を認可規則で直接参照できます。ユーザ属性には、ユーザの部門またはマネージャの属性が含まれている場合があります。

関連項目

- ユーザおよび ID ストアの管理（8-1 ページ）
- ポリシーの用語（3-3 ページ）
- ポリシーのタイプ（3-5 ページ）

ポリシーおよびネットワーク デバイス グループ

ネットワーク デバイス グループ（NDG）をポリシー条件として参照できます。ACS では、デバイスの要求を受信すると、そのデバイスと関連付けられている NDG が取得され、ポリシー テーブルの NDG に照らして比較されます。この方法を使用すると、複数のデバイスをグループ化し、同じポリシーを割り当てることができます。たとえば、特定の場所にあるすべてのデバイスをグループ化して、同じポリシーを割り当てることができます。

ネットワーク デバイスからネットワークへのアクセス要求を受信すると、ACS はネットワーク デバイス リポジトリを検索して、IP アドレスが一致するエントリを見つけます。その IP アドレスを使用して ACS が識別したデバイスから要求を受信した場合、ACS はそのデバイスに関連付けられているすべての NDG を取得します。

関連項目

- ユーザおよび ID ストアの管理（8-1 ページ）
- ポリシーの用語（3-3 ページ）
- ポリシーのタイプ（3-5 ページ）

ルール ベース ポリシーの例

次の例に、ポリシー要素を使用してポリシー規則を作成する方法を示します。

ある企業では、ネットワークを 2 つの地域（East および West）に分割しており、各地域にネットワーク操作エンジニアが常駐しています。エンジニアは、次のことを可能にするアクセス ポリシーを作成します。

- 自分の地域のネットワーク デバイスへのフル アクセス。
- 自分の地域以外のデバイスへの読み取り専用アクセス。

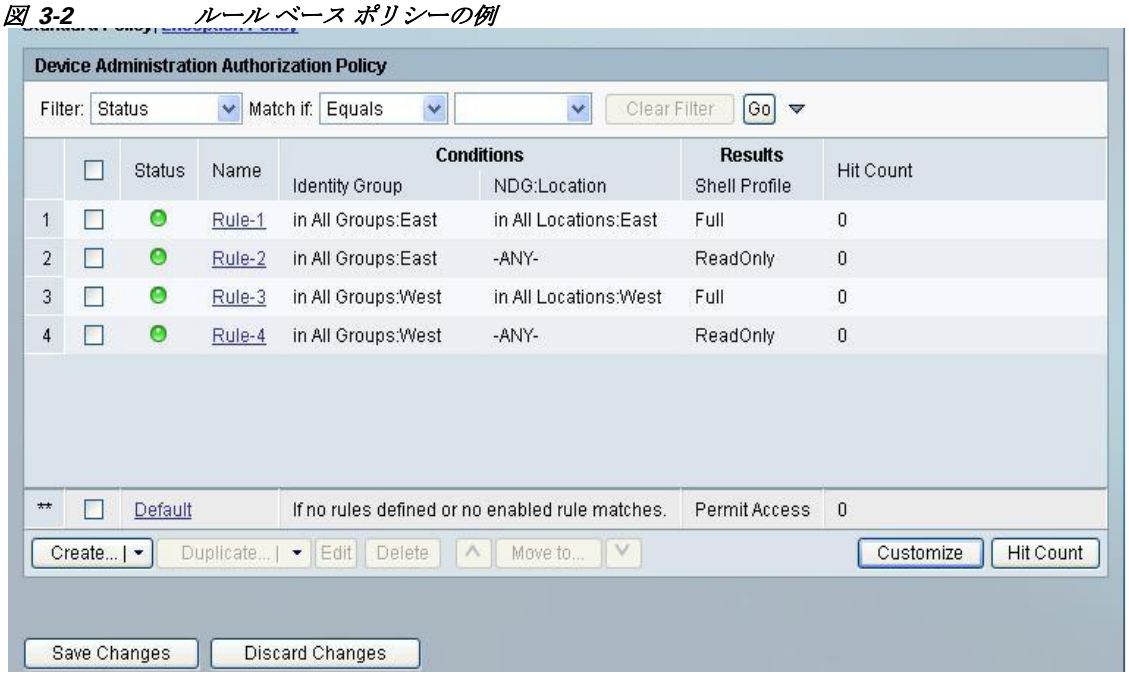
ACS 5.8 ポリシー モデルを次の目的のために使用できます。

- East および West のネットワーク デバイス グループを定義し、ネットワーク デバイスを該当するグループに割り当てる。
- East および West の ID グループを定義し、ユーザ（ネットワーク エンジニア）を該当するグループにマップする。
- フル アクセスまたは読み取り専用の認可プロファイルを定義する。
- ネットワーク デバイス グループの場所に応じて各 ID グループにフル アクセスまたは読み取り専用アクセスを許可する規則を定義する。

これを行う前に、2 つのユーザ グループ（エンジニアが常駐する場所ごとに 1 つのグループ。それぞれのグループに権限に関する個別の定義などが設定されます）を作成しておく必要があります。この定義では、ルール ベース モデルのような柔軟性や細かさは提供されません。

図 3-2 に、ポリシー規則テーブルの例を示します。

図 3-2　ルール ベース ポリシーの例



このポリシー テーブル内の各行は、単一の規則を表します。

最後のデフォルト規則を除き、各規則には 2 つの条件（ID グループと場所）および結果（認可プロファイル）が含まれています。ID グループは ID ベースの分類であり、場所は非 ID 条件です。認可プロファイルには、セッションの権限が含まれています。

ID グループ、場所、および認可プロファイルはポリシー要素です。

関連項目

- ポリシーの用語（3-3 ページ）
- ポリシーのタイプ（3-5 ページ）
- アクセス サービス（3-5 ページ）
- サービスおよびポリシーの設定フロー（3-19 ページ）

サービスおよびポリシーの設定フロー

表 3-9 に、サービスとポリシーを設定する場合の、推奨される基本フローを示します。このフローには、ユーザ定義の条件および属性の設定は含まれていません。このフローでは、NDG、ID グループ、および複合条件を規則で使用できます。

前提条件

サービスおよびポリシーを設定する前に、次のことを実行しておく必要があります。

- ACS へのネットワーク リソースの追加、およびネットワーク デバイス グループの作成。ネットワーク デバイス グループの作成、複製、および編集（7-2 ページ）およびネットワーク デバイスおよび AAA クライアント（7-5 ページ）を参照してください。
- 内部 ACS ID ストアへのユーザの追加、または外部 ID ストアの追加。内部ユーザの作成（8-14 ページ）、ID 属性の管理（8-8 ページ）、または外部 LDAP ID ストアの作成（8-35 ページ）を参照してください。

表 3-9　サービスおよびポリシーの設定手順

ステップ	アクション	Web インターフェイスのドロワ
ステップ 1	ポリシー結果を定義します。 • デバイス管理用の認可および権限：シェル プロファイルまたはコマンド セット。 • ネットワーク アクセス用の認可および権限：認可プロファイル。 次を参照してください。 • 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（9-25 ページ） • 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（9-30 ページ） • 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（9-19 ページ）	ポリシー要素
ステップ 2	（任意）カスタム条件をポリシー規則に定義します。このステップは、ステップ 6 でポリシー規則を定義する前に実行できます。つまり、規則の作成中にカスタム条件を定義できます。カスタム セッション条件の作成、複製、および編集（9-5 ページ）を参照してください。	—
ステップ 3	アクセス サービスを作成します。構造および許可プロトコルだけを定義します。ポリシーについてはまだ定義する必要はありません。アクセス サービスの作成、複製、および編集（10-12 ページ）を参照してください。	アクセス ポリシー
ステップ 4	要求に使用するアクセス サービスを決定するために、規則をサービス セレクション ポリシーに追加します。次を参照してください。 • ポリシーのカスタマイズ（10-4 ページ） • サービス セレクション規則の作成、複製、および編集（10-8 ページ）	アクセス ポリシー
ステップ 5	ID ポリシーを定義します。要求の認証に使用する ID ストアまたは順序を選択し、ID 属性を取得します。ユーザおよび ID ストアの管理（8-1 ページ）を参照してください。	ユーザおよび ID ストア
ステップ 6	認可規則を次のように作成します。 • デバイス管理：シェル/コマンド認可ポリシー。 • ネットワーク アクセス：セッション認可ポリシー。 次を参照してください。 • ポリシーのカスタマイズ（10-4 ページ） • アクセス サービス ポリシーの設定（10-23 ページ）	アクセス ポリシー

関連項目

- ポリシーの用語（3-3 ページ）
- ポリシーの条件（3-16 ページ）
- ポリシーの結果（3-16 ページ）
- ポリシーおよび ID 属性（3-17 ページ）