CHAPTER 4

# ACS を使用した一般的なシナリオ

ネットワーク コントロールとは、ネットワークへのアクセスを制御するプロセスのことです。従来は、ネットワークに対するユーザの認証には、ユーザ名とパスワードが使用されていました。近年の急速な技術の進歩により、ユーザ名とパスワードによる従来のネットワーク アクセス管理方式では不十分となっています。

ユーザによるネットワークへのアクセス方法およびユーザのアクセス対象は、大きく変化しています。したがって、ネットワークへのアクセスを制御するには、複雑でダイナミックなポリシーを定義する必要があります。

たとえば、これまでは、ユーザは自分が所属するグループに基づいてネットワークへのアクセスを許可され、特定のアクションの実行を認可されていました。現在では、ユーザが所属するグループに加えて、次のような他の要素も考慮する必要があります。

- アクセスが勤務時間内か勤務時間外か
- リモート アクセスかどうか
- サービスおよびリソースへのアクセスがフル アクセスか制限付きアクセスか

ユーザ以外に、各種のデバイスもネットワークへの接続を試みます。

ユーザやデバイスがネットワーク アクセス サーバ（無線アクセス ポイント、802.1x スイッチ、VPN サーバなど）を介してネットワークに接続する場合は、ACS によってその要求が認証および認可され、接続が確立されます。

認証とは、ネットワークへの接続を試みるユーザまたはデバイスの ID を確認するプロセスのことです。ACS は、クレデンシャルという形式でユーザまたはデバイスの ID 証明を受け取ります。認証には、次のような 2 つの異なる方式があります。

- パスワードベースの認証：より単純なユーザ認証方式です。ユーザが入力するのは、ユーザ名とパスワードです。サーバが内部または外部のデータベースでユーザ名とパスワードをチェックし、それらが登録されていれる場合、そのユーザはアクセスを許可されます。アクセスのレベル（認可）は作成済みの規則と条件によって定義されます。
- 証明書ベースの認証：ACS は、Extensible Authentication Protocol-Transport Level Security（EAP-TLS）と Protected Extensible Authentication Protocol-Transport Level Security（PEAP-TLS）を使用した証明書ベースの認証をサポートします。これらはサーバによるクライアント認証とクライアントによるサーバ認証に証明書を使用します。

  証明書ベースの認証方式は、パスワードベースの認証方式と比べて強力なセキュリティを備えているため、この方式を推奨します。

認可では、ユーザまたはデバイスに許可するアクセスのレベルを決定します。ACS 5.x のルール ベースのポリシー モデルを使用すると、規則の中に複雑な条件を定義できます。ACS は規則（ポリシー）のセットを使用してアクセス要求を評価し、判断を返します。

個別のポリシーからなる順序をアクセス サービスにまとめ、これを使用してアクセス要求を処理します。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。

Cisco Secure Access Control System（ACS）を使用すると、ネットワークのサービスおよびリソース（IP 電話やプリンタなどのデバイスも含む）へのアクセスを一元的に管理できます。ACS 5.4 はポリシーベースのアクセス コントロール システムであり、複雑なポリシー条件を作成できるだけでなく、政府によるさまざまな規制に準拠することもできます。

ネットワークに ACS を展開する場合は、ネットワークへのアクセスを決定する適切な認証方式を選択する必要があります。

この章では、一般的ないくつかのシナリオについてのガイドラインを示します。この章の内容は、次のとおりです。



# デバイス管理の概要

デバイス管理を使用すると、ネットワーク デバイスに対して実行される管理操作を ACS で制御および監査できます。デバイス管理には次の方法を使用します。

- セッション管理：ネットワーク デバイスへのセッション認可要求により、ACS 応答が発生します。この応答には、ネットワーク デバイスにより解釈されるトークンが含まれています。ネットワーク デバイスにより、セッション期間中に実行できるコマンドが制限されます。セッション管理（4-3 ページ）を参照してください。
- コマンド認可：管理者がネットワーク デバイスに対して操作コマンドを発行すると、その管理者がコマンドの発行を認可されているかどうかを判定する問い合わせが ACS に行われます。コマンド認可（4-4 ページ）を参照してください。

デバイス管理の結果は、シェル プロファイルまたはコマンド セットにすることができます。

シェル プロファイルでは、セッション認可要求への応答で返される属性を選択できます。最も一般的に使用される属性は特権レベルです。シェル プロファイルには、シェル アクセス セッションに使用する共通属性と、その他のタイプのセッションに使用するユーザ定義属性があります。

ACS 5.4 では、カスタム TACACS+ 認可サービスおよび属性を作成できます。次のことを定義できます。

- 上記属性の任意の A-V ペア
- 任意または必須の属性
- 同じ名前を持つ複数の A-V ペア（マルチパート属性）

また、ACS では、タスク固有の事前定義済みシェル属性がサポートされています。TACACS+ シェル プロファイルを使用すると、シェル認可応答で返されるカスタム属性を指定できます。TACACS+ のカスタム サービスおよび属性（4-5 ページ）を参照してください。

コマンド セットでは、許可または拒否されるコマンドのセットおよびコマンド引数を定義します。認可を要求するコマンドを受信すると、認可結果に含まれている使用可能なコマンド セット内のコマンドと比較されます。

コマンドがコマンド セットに一致すると、そのコマンドに対応する許可または拒否の設定が取得されます。一致した規則の中で複数の結果が該当する場合は、その結果が統合され、コマンドに対する単一の許可または拒否の結果が返されます。その条件は次のとおりです。

- コマンド セット内に明示的な deny-always 設定が存在する場合、コマンドは拒否される。
- コマンド セット内に明示的な deny-always 設定が存在せず、すべてのコマンド セットが許可の結果を返す場合、コマンドは許可される。
- 上記 2 つの条件のどちらにも当てはまらない場合、コマンドは拒否される。

許可および拒否の設定は、デバイス管理規則テーブルで設定します。デバイス管理規則テーブル内では、一致する条件または一致しない条件としてポリシー要素を設定します。この規則テーブルにより、マッチング プロセスを通じて特定の要求条件がデバイス管理結果にマップされます。規則テーブルで処理された結果は、要求の種類に応じてシェル プロファイルまたはコマンド セットとなります。

セッション管理要求にはシェル プロファイル結果が含まれています。この中には、セッションのプロビジョニングで使用される属性の値が入っています。コマンド認可要求にはコマンド認可結果が含まれています。この中には、コマンドおよび引数の確認に使用されるコマンド セットのリストが入っています。

このモデルを使用すると、特定のデバイスを管理できるように管理者レベルを設定できます。たとえば、あるユーザに Network Device Administrator のロールを割り当てるとデバイス管理機能にフル アクセスできますが、Read Only Admin の場合は管理機能を実行できません。

# セッション管理

次の手順では、管理者がネットワーク デバイスとのセッション（通信する機能）を確立するためのフローについて説明します。

1. 管理者がネットワーク デバイスにアクセスします。
2. ネットワーク デバイスから、RADIUS または TACACS+ のアクセス要求が ACS に送信されます。
3. ACS は ID ストア（外部 LDAP、Active Directory、RSA、RADIUS ID サーバ、または内部 ACS ID ストア）を使用して、管理者のクレデンシャルを検証します。
4. RADIUS 応答または TACACS+ 応答（accept または reject）がネットワーク デバイスに送信されます。accept 応答には管理者の最大特権レベルも含まれており、セッション期間中の管理者のアクセス レベルはこの値によって決定されます。

セッション管理ポリシー（デバイス管理規則テーブル）を設定して通信を許可するには、次の手順を実行します。

**ステップ 1**　TACACS+ プロトコルのグローバル設定およびユーザ認証オプションを設定します。TACACS+ の設定（18-2 ページ）を参照してください。

**ステップ 2**　ネットワーク リソースを設定します。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。

**ステップ 3**　ユーザおよび ID ストアを設定します。内部 ID ストアの管理（8-4 ページ）または外部 ID ストアの管理（8-22 ページ）を参照してください。

**ステップ 4**　必要に応じてシェル プロファイルを設定します。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（9-24 ページ）を参照してください。

**ステップ 5**　アクセス サービス ポリシーを設定します。アクセス サービス ポリシーの作成（10-4 ページ）を参照してください。

**ステップ 6**　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 ポリシーの作成（10-4 ページ）を参照してください。

**ステップ 7**　認可ポリシー（規則テーブル）を設定します。ネットワーク アクセス用セッション認可ポリシーの設定（10-29 ページ）を参照してください。

# コマンド認可

ここでは、管理者がネットワーク デバイスにコマンドを発行するためのフローについて説明します。

**（注）**　このデバイス管理コマンド フローが対応しているのは、TACACS+ プロトコルだけです。

1. 管理者がネットワーク デバイスにコマンドを発行します。
2. ネットワーク デバイスから、アクセス要求が ACS に送信されます。
3. ACS が任意で ID ストア（外部 Lightweight Directory Access Protocol [LDAP]、Active Directory、RADIUS ID サーバ、または内部 ACS ID ストア）を使用して、ポリシー処理に含まれるユーザ属性を取得します。
4. 応答には、管理者がコマンドの発行を認可されているかどうかが示されています。

コマンド認可ポリシー（デバイス管理規則テーブル）を設定して、管理者がネットワーク デバイスにコマンドを発行できるようにするには、次の手順を実行します。

**ステップ 1**　TACACS+ プロトコルのグローバル設定およびユーザ認証オプションを設定します。TACACS+ の設定（18-2 ページ）を参照してください。

**ステップ 2**　ネットワーク リソースを設定します。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。

**ステップ 3**　ユーザおよび ID ストアを設定します。内部 ID ストアの管理（8-4 ページ）または外部 ID ストアの管理（8-22 ページ）を参照してください。

**ステップ 4**　必要に応じてコマンド セットを設定します。デバイス管理用のコマンド セットの作成、複製、および編集（9-29 ページ）を参照してください。

**ステップ 5**　アクセス サービス ポリシーを設定します。アクセス サービス ポリシーの作成（10-4 ページ）を参照してください。

**ステップ 6**　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 ポリシーの作成（10-4 ページ）を参照してください。

**ステップ 7**　認可ポリシー（規則テーブル）を設定します。デバイス管理のシェル/コマンド認可ポリシーの設定（10-35 ページ）を参照してください。

**関連項目**

- 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）
- システム管理者およびアカウントの設定（16-3 ページ）

- ユーザおよび ID ストアの管理（8-1 ページ）
- 外部 ID ストアの管理（8-22 ページ）
- ポリシー条件の管理（9-1 ページ）
- アクセス ポリシーの管理（10-1 ページ）

## TACACS+ のカスタム サービスおよび属性

ここでは、TACACS+ のカスタム属性およびサービスを定義する設定フローについて説明します。

**ステップ 1**　要求に応じて TACACS+ サービスに移行するためのカスタム TACACS+ 条件を作成します次の手順を実行します。

a. [Policy Elements] > [Session Conditions] > [Custom] に移動し、[Create] をクリックします。

b. カスタム TACACS+ 条件を作成します。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 2**　TACACS+ シェル プロファイルを結果として使用し、デバイス管理用のアクセス サービスを作成します。デバイス管理のシェル/コマンド認可ポリシーの設定（10-35 ページ）を参照してください。

**ステップ 3**　カスタム TACACS+ 属性を作成します。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（9-24 ページ）を参照してください。

# パスワードベースのネットワーク アクセス

ここでは、次の内容について説明します。

- パスワードベースのネットワーク アクセスの概要（4-5 ページ）
- パスワードベースのネットワーク アクセスの設定フロー（4-7 ページ）

パスワードベースのプロトコルの詳細については、付録 B「ACS 5.4 での認証」を参照してください。

## パスワードベースのネットワーク アクセスの概要

単純で暗号化されていないユーザ名とパスワードの使用は確実な認証メカニズムではありませんが、インターネット アクセスのように認可レベルまたは特権レベルが低い場合は十分です。

暗号化を使用すると、ネットワーク上でパスワードが不正に取得されるリスクが小さくなります。RADIUS などのクライアント/サーバ アクセス コントロール プロトコルでは、パスワードを暗号化することにより、ネットワーク内でパスワードが不正に取得される事態を防止します。ただし、RADIUS は AAA クライアントと ACS 間でだけ動作します。認証プロセスにおけるこの時点の前の段階で、認可されていないユーザが暗号化されていないパスワードを入手する可能性があります。たとえば、次のような場合です。

- 電話回線を介してダイヤルアップ接続を行うエンドユーザ クライアントとの間の通信
- ネットワークアクセス サーバで終端する ISDN 回線
- エンドユーザ クライアントとホスティング デバイスの間の Telnet セッションを介して行われる通信

ACS はさまざまな認証方式をサポートしており、ACS のサポートする各種 ID ストアに対する認証を行います。認証プロトコルと ID ストアの互換性の詳細については、認証プロトコルと ID ストアの互換性（B-37 ページ）を参照してください。

パスワードの処理は、使用するセキュリティ制御プロトコル（RADIUS など）のバージョンと種類、および AAA クライアントとエンドユーザ クライアントの設定に基づいて、上記のパスワード認証プロトコルを使用して行うことができます。

ACS では、異なるセキュリティ レベルを同時に使用して、さまざまな要件に対応できます。基本的なセキュリティ レベルは、Password Authentication Protocol（PAP; パスワード認証プロトコル）によって確保されます。PAP で得られるセキュリティ レベルはごく基本的なレベルですが、クライアントにとってはシンプルで有用なプロトコルです。エンドユーザ クライアントから AAA クライアントに通信するときに MSCHAPv2 を使用すると、パスワードが暗号化されるため、暗号化しない場合よりも高いセキュリティ レベルを確保できます。

（注）　パスワードベースのアクセス（または証明書ベースのアクセス）では、ACS の設定に応じてユーザの認証だけでなく *認可* も行われます。さらに、NAS によってアカウンティング要求が送信される場合は、ユーザのアカウンティングも行われます。

ACS では、次に示すパスワードベースの認証方式がサポートされています。

- プレーンな RADIUS パスワード認証方式
  - RADIUS-PAP
  - RADIUS-CHAP
  - RADIUS-MSCHAPv1
  - RADIUS-MSCHAPv2
- RADIUS EAP ベースのパスワード認証方式
  - PEAP-MSCHAPv2
  - PEAP-GTC
  - EAP-FAST-MSCHAPv2
  - EAP-FAST-GTC
  - EAP-MD5
  - LEAP

認証方式は、次の要素に基づいて選択する必要があります。

- ネットワーク アクセス サーバ：無線アクセス ポイント、802.1X 認証スイッチ、VPN サーバなど
- クライアント コンピュータおよびソフトウェア：EAP サプリカント、VPN クライアントなど
- ユーザの認証に使用する ID ストア：内部または外部（AD、LDAP、RSA トークン サーバ、または RADIUS ID サーバ）

**関連項目**

- ACS 5.4 での認証（B-1 ページ）
- パスワードベースのネットワーク アクセスの設定フロー（4-7 ページ）
- 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）
- アクセス ポリシーの管理（10-1 ページ）

# パスワードベースのネットワーク アクセスの設定フロー

ここでは、パスワードベースのネットワーク アクセスに関してエンドツーエンドのフローについて説明し、実行が必要なタスクを示します。タスクを設定する方法に関する情報は、該当するタスクの章にあります。

パスワードベースのネットワーク アクセスを設定するには、次の手順を実行します。

**ステップ 1**　ネットワーク デバイスおよび AAA クライアントを設定します。

a. 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）で、[Authentication Setting] を [RADIUS] に設定します。

b. 共有秘密を入力します。

詳細については、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。

**ステップ 2**　ユーザおよび ID ストアを設定します。詳細については、第 8 章「ユーザおよび ID ストアの管理」を参照してください。

**ステップ 3**　ポリシー条件および認可プロファイルを定義します。詳細については、第 9 章「ポリシー要素の管理」を参照してください。

**ステップ 4**　アクセス サービスを定義します。詳細については、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。

a. [Access Service Type] を [Network Access] に設定します。

b. [Allowed Protocols] ページで ACS 対応プロトコルのいずれかを選択し、表 4-1 の処理カラムの手順を実行します。

**ステップ 5**　アクセス サービスをサービス セレクション ポリシーに追加します。詳細については、サービス セレクション ルールの作成、複製、および編集（10-8 ページ）を参照してください。

**ステップ 6**　作成したサービスに戻り、[Authorization Policy] ページで認可規則を定義します。詳細については、アクセス サービス ポリシーの設定（10-21 ページ）を参照してください。

*表 4-1　ネットワーク アクセス認証プロトコル*

| プロトコル | Action |
|---|---|
| Process Host Lookup（MAB） | [Allowed Protocols] ページで [Process Host Lookup] を選択します。 |
| RADIUS PAP | [Allowed Protocols] ページで [Allow PAP/ASCII] を選択します。 |
| RADIUS CHAP | [Allowed Protocols] ページで [Allow CHAP] を選択します。 |
| RADIUS MSCHAPv1 | [Allowed Protocols] ページで [Allow MS-CHAPv1] を選択します。 |
| RADIUS MSCHAPv2 | [Allowed Protocols] ページで [Allow MS-CHAPv2] を選択します。 |
| EAP-MD5 | [Allowed Protocols] ページで [Allow EAP-MD5] を選択します。 |
| LEAP | [Allowed Protocols] ページで [Allow LEAP] を選択します。 |
| PEAP | [Allowed Protocols] ページで [PEAP] を選択します。PEAP 内部方式の場合は、[EAP-MSCHAPv2] か [EAP-GTC]、またはその両方を選択してください。 |

*表 4-1　ネットワーク アクセス認証プロトコル（続き）*

| プロトコル | Action |
|---|---|
| EAP-FAST | 1. [Allowed Protocols] ページで [Allow EAP-FAST] を選択し、EAP-FAST 設定をイネーブルにします。<br>2. EAP-FAST 内部方式の場合は、[EAP-MSCHAPv2] か [EAP-GTC]、またはその両方を選択してください。<br>3. [Allow Anonymous In-Band PAC Provisioning] か [Allow Authenticated In-Band PAC Provisioning]、またはその両方を選択します。<br>Windows マシンで Microsoft AD に対する認証を行う場合、およびパスワード変更機能の場合は、次の手順を実行します。<br>1. [Use PACS] オプション ボタンをクリックします。PAC の詳細については、PAC について（B-23 ページ）を参照してください。<br>2. [Allow Authenticated In-Band PAC Provisioning] をオンにします。<br>3. [Allow Machine Authentication] をオンにします。<br>4. [Machine PAC Time to Live] を入力します。<br>5. [Enable Stateless Session Resume] をオンにします。<br>6. [Authorization PAC Time to Live] を入力します。<br>7. [Preferred EAP Protocol] をオンにしてリストから優先プロトコルを設定します。 |

RADIUS、EAP 以外の認証方式（RADIUS/PAP、RADIUS/CHAP、RADIUS/MS-CHAPv1、RADIUS/MSCHAPv2）、および単純な EAP 方式（EAP-MD5 と LEAP）の場合は、表 4-1 に定義されている [Allowed Protocols] ページのプロトコルだけを設定する必要があります。

一部の複雑な EAP プロトコルでは、次に示す追加設定が必要です。

- EAP-TLS の場合は、次の設定も行う必要があります。
  - EAP-TLS 設定（[System Administration] > [Configuration] > [EAP-TLS Settings]）。
  - ローカル サーバ証明書（[System Administration] > [Configuration] > [Local Server Certificates] > [Local Certificates]）。
  - CA 証明書（[Users and Identity Stores] > [Certificate Authorities]）。
- PEAP の場合は、次の設定も行う必要があります。
  - [Allowed Protocols] ページの内部方式。さらに、パスワード変更が許可されるかどうかを指定します。
  - PEAP 設定（[System Administration] > [Configuration] > [PEAP Settings]）。
  - ローカル サーバ証明書（[System Administration] > [Configuration] > [Local Server Certificates] > [Local Certificates]）。
- EAP-FAST の場合は、次の設定も行う必要があります。
  - [Allowed Protocols] ページの内部方式。さらに、パスワード変更が許可されるかどうかを指定します。
  - PAC を使用するかどうか。さらに、PAC を使用する場合は In-Band PAC Provisioning を許可する方法を指定します。
  - EAP-FAST 設定（[System Administration] > [Configuration] > [EAP-FAST] > [Settings]）。

– ローカル サーバ証明書（[System Administration] > [Configuration] > [Local Server Certificates] > [Local Certificates]、Authenticated PAC Provisioning がイネーブルの場合にかぎります）。

**関連項目**

- ACS 5.4 での認証（B-1 ページ）
- 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）
- アクセス ポリシーの管理（10-1 ページ）
- アクセス サービスの作成、複製、および編集（10-12 ページ）
- PAC について（B-23 ページ）

# 証明書ベースのネットワーク アクセス

ここでは、次の内容について説明します。

- 証明書ベースのネットワーク アクセスの概要（4-9 ページ）
- ACS で証明書を使用する方法（4-10 ページ）
- 証明書ベースのネットワーク アクセス（4-10 ページ）

証明書ベースのプロトコルの詳細については、以下を参照してください。付録 B「ACS 5.4 での認証」

## 証明書ベースのネットワーク アクセスの概要

EAP-TLS を使用するには、ACS のコンピュータ証明書をインストールする必要があります。インストールされるコンピュータ証明書は、アクセス クライアントが信頼するルート CA まで証明書チェーンをたどることができる CA によって発行される必要があります。

さらに、ACS でアクセス クライアントのユーザ証明書またはコンピュータ証明書を確認するには、そのアクセス クライアントにユーザ証明書またはコンピュータ証明書を発行したルート CA の証明書をインストールしておく必要があります。

ACS では、EAP-TLS プロトコルを使用する証明書ベースのネットワーク アクセスがサポートされています。このプロトコルでは、クライアントによるサーバ認証およびサーバによるクライアント認証に証明書を使用します。

PEAP、または EAP-FAST の authenticated-provisioning モードなどの他のプロトコルでもクライアントによるサーバ認証に証明書を利用しますが、これらは証明書ベースのネットワーク アクセスとは見なされません。これは、サーバがクライアント認証に証明書を使用しないためです。

ACS 公開キー インフラストラクチャ（PKI）の証明書ベース認証は、X509 証明書 ID に基づいています。証明書によって自分自身を識別するエンティティでは、証明書に格納された公開キーに対応する秘密キーを保持します。

証明書は自己署名することも、別の CA に署名してもらうこともできます。証明書の階層を作成すると、その CA に対する各エンティティの信頼関係を構築できます。信頼できるルート CA とは、他のすべての CA の証明書に署名し、結果として階層内の各証明書に署名するエンティティのことです。

ACS は、自分自身の証明書を使用して ACS 自身を識別します。Certificate Trust List（CTL; 証明書信頼リスト）をサポートしており、接続証明書を認可します。また、チェーン証明書のすべてが提示された場合は、アイデンティティ証明書を認可する複雑な階層もサポートします。

証明書で使用する、複数の RSA キー サイズ（512、1024、2048、または 4096 ビット）をサポートしています。その他のキーサイズを使用することもできます。ACS 5.4 では RSA がサポートされています。ACS はデジタル署名アルゴリズム（DSA）をサポートしません。ただし、一部の使用例では、ACS は DSA 暗号スイートが証明書ベースの認証に使用されないようにしません。

ネットワーク アクセス認証に使用するすべての証明書は、X.509 証明書の要件を満たし、SSL/TLS を使用する接続で動作する必要があります。この最小要件を満たしたうえで、クライアントおよびサーバの証明書には追加の要件があります。

ACS では次の 2 種類の証明書を設定できます。

- 信頼証明書：CA 証明書とも呼ばれます。CTL 信頼階層を形成し、リモート証明書の確認に使用します。
- ローカル証明書：ローカル サーバ証明書とも呼ばれます。クライアントは、ローカル証明書をさまざまなプロトコルとともに使用し、ACS サーバを認証します。この証明書は秘密キーと関連付けて保持され、秘密キーは証明書を所持していることの証明に利用されます。

（注）　証明書ベースのアクセス（またはパスワードベースのアクセス）では、ACS の設定に応じてユーザの認証だけでなく*認可*も行われます。さらに、NAS によってアカウンティング要求が送信される場合は、ユーザのアカウンティングも行われます。

**関連項目**

- CA 証明書の設定（8-73 ページ）
- ローカル サーバ証明書の設定（18-14 ページ）
- ACS で証明書を使用する方法（4-10 ページ）

# ACS で証明書を使用する方法

次に、ACS 5.4 における証明書の使用例を 3 つ示します。

- 証明書ベースのネットワーク アクセス（4-10 ページ）
- 証明書によるブラウザからの ACS Web インターフェイスの認可（4-12 ページ）
- LDAP セキュア認証接続の確認（4-12 ページ）

## 証明書ベースのネットワーク アクセス

TLS 関連の EAP および PEAP プロトコルの場合は、ローカル証明書ストアからサーバ証明書をセットアップし、クライアントを認証する信頼証明書リストを設定する必要があります。信頼証明書は、ローカル証明書ストアにある任意の証明書から選択できます。

EAP-TLS または PEAP（EAP-TLS）を使用するには、信頼証明書を入手してインストールする必要があります。タスクを実行する方法に関する情報は、該当するタスクの章にあります。

**始める前に**

次を設定してサーバをセットアップします。

- EAP-TLS または PEAP（EAP-TLS）
- ローカル証明書。ローカル サーバ証明書の設定（18-14 ページ）を参照してください。

EAP-TLS または PEAP（EAP-TLS）の証明書ベースのネットワーク アクセスを設定するには、次の手順を実行します。

**ステップ 1**　信頼証明書リストを設定します。詳細については、CA 証明書の設定（8-73 ページ）を参照してください。

**ステップ 2**　LDAP 外部 ID ストアを設定します。LDAP に格納された証明書に対して証明書を確認するときに、この設定が必要となる場合があります。詳細については、外部 LDAP ID ストアの作成（8-27 ページ）を参照してください。

**ステップ 3**　証明書認証プロファイルをセットアップします。詳細については、証明書認証プロファイルの設定（8-77 ページ）を参照してください。

**ステップ 4**　ポリシー要素を設定します。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。

カスタム条件を作成すると、証明書の属性をポリシー条件として使用できます。詳細については、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 5**　アクセス サービスを作成します。詳細については、アクセス サービスの設定（10-11 ページ）を参照してください。

**ステップ 6**　[Allowed Protocols] ページで、[EAP-TLS or PEAP (EAP-TLS) as inner method] を選択します。

**ステップ 7**　アクセス サービスの ID ポリシーおよび認可ポリシーを設定します。詳細については、アクセス サービス ポリシーの設定（10-21 ページ）を参照してください。

**（注）**　ID ポリシーの規則を作成した結果、証明書認証プロファイルまたは ID 順序が作成される場合があります。詳細については、ID ポリシーの表示（10-22 ページ）を参照してください。

**ステップ 8**　認可ポリシーを設定します。ネットワーク アクセス用セッション認可ポリシーの設定（10-29 ページ）を参照してください。

**ステップ 9**　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 ポリシーの設定（10-5 ページ）を参照してください。

*表 4-2　ネットワーク アクセス認証プロトコル*

| プロトコル | Action |
|---|---|
| EAP-TLS | [Allowed Protocols] ページで [Allow EAP-TLS] を選択し、EAP-TLS 設定をイネーブルにします。<br>• [Enable Stateless Session resume]：アクセス サービスごとにステートレス セッション再開機能をイネーブルにするには、このチェックボックスをオンにします。この機能では、次のオプションを設定することが可能です。<br>– [Proactive Session Ticket update]：セッション チケットが更新される前に経過する必要がある存続可能時間の量を示すパーセント値を入力します。たとえば、値 10 を入力した場合、セッション チケットの更新は存続可能時間の 10 パーセントが過ぎた後に実行されます。<br>– [Session ticket Time to Live]：正の整数を使用して日、週、月、および年に対応する最大値を入力します。 |
| PEAP | [Allowed Protocols] ページで [PEAP] を選択します。PEAP 内部方式の場合、[EAP-TLS] または [PEAP Cryptobinding TLV] を選択します。 |

**関連項目**

- ローカル サーバ証明書の設定（18-14 ページ）
- CA 証明書の設定（8-73 ページ）
- ACS 5.4 での認証（B-1 ページ）
- EAP-TLS の概要（B-6 ページ）

## 証明書によるブラウザからの ACS Web インターフェイスの認可

ブラウザを使用して ACS に接続する場合は、HTTPS 証明書ベースの認証を使用します。ブラウザから ACS Web インターフェイスを認可するときは、ACS のローカル サーバ証明書が使用されます。ACS ではブラウザ認証がサポートされていません（相互認証はサポートされていません）。

ACS にはデフォルトのローカル サーバ証明書がインストールされているため、ブラウザから ACS に接続できます。デフォルト証明書は自己署名証明書であり、インストール時にこの証明書は変更できません。

**関連項目**

- ACS で証明書を使用する方法（4-10 ページ）
- ローカル サーバ証明書の設定（18-14 ページ）

## LDAP セキュア認証接続の確認

LDAP 外部 ID ストア用にセキュアな外部認証接続を定義するには、CA 証明書を使用して接続を確認します。

証明書を使用して LDAP セキュア認証接続を確認するには、次の手順を実行します。

**ステップ 1**　LDAP 外部 ID ストアを設定します。外部 LDAP ID ストアの作成（8-27 ページ）を参照してください。

**ステップ 2**　[LDAP Server Connection] ページで [Use Secure Authentication] をオンにします。

**ステップ 3**　ドロップダウン メニューから [Root CA] を選択して ACS 用の LDAP 設定を続行します。

**関連項目**

- ACS で証明書を使用する方法（4-10 ページ）
- ローカル サーバ証明書の設定（18-14 ページ）
- 外部 ID ストアの管理（8-22 ページ）

# エージェントレス ネットワーク アクセス

ここでは、次の内容について説明します。

- エージェントレス ネットワーク アクセスの概要（4-13 ページ）
- ホスト ルックアップ（4-13 ページ）
- エージェントレス ネットワーク アクセスのフロー（4-16 ページ）

ネットワーク アクセスに使用するプロトコルの詳細については、ACS 5.4 での認証（B-1 ページ）を参照してください。

# エージェントレス ネットワーク アクセスの概要

エージェントレス ネットワーク アクセスとは、ホスト デバイスに適切なエージェント ソフトウェアがない場合に、ポートベースの認証および認可を実行するメカニズムのことです。

たとえば、802.1x サプリカントのないホスト デバイスやサプリカントがディセーブルにされているホスト デバイスなどです。

ホスト デバイス、およびそのデバイスが接続するスイッチでは、802.1x をイネーブルにする必要があります。802.1x サプリカントのないホストまたはデバイスが、802.1x がイネーブルなポートに接続しようとすると、デフォルト セキュリティ ポリシーの対象となります。

デフォルト セキュリティ ポリシーによって、802.1x 認証が成功してからネットワークへのアクセスを許可する必要があることが通知されます。したがって、デフォルトでは 802.1x 非対応のデバイスは 802.1x で保護されたネットワークにアクセスできません。

802.1x をサポートするデバイスの数は増加していますが、ネットワーク接続が必要なデバイスには、802.1x をサポートしない、またはサポートできないデバイスが常に存在します。このようなデバイスの例としては、ネットワーク プリンタ、バッジ リーダー、およびレガシー サーバなどを挙げることができます。これらのデバイスについては、何らかのプロビジョニングを行う必要があります。

非 802.1x デバイスに対応するために、シスコでは 2 つの機能を提供しています。たとえば、MAC Authentication Bypass（ホスト ルックアップ）および Web 認証を使用したゲスト VLAN アクセスです。

ACS 5.4 では、802.1x サプリカントが存在しない場合にホスト ルックアップ フォールバック メカニズムがサポートされます。ホスト ルックアップが設定されている場合、ポートで 802.1x がタイムアウトしたあとにホスト ルックアップに成功すると、ポートはオープン ステートに移行できます。

**関連項目**

- ホスト ルックアップ（4-13 ページ）
- エージェントレス ネットワーク アクセスのフロー（4-16 ページ）

# ホスト ルックアップ

ACS は、クレデンシャル（パスワードや証明書など）に従って ID を認証できない場合の検証方法として、ホスト ルックアップを使用します。ID の検証には、ID ストアのルックアップを行う必要があります。

ホスト ルックアップを使用する例としては、ネットワーク デバイスが MAC 認証バイパス（MAB）を要求するように設定されている場合があります。これは、ポートで 802.1x がタイムアウトしたあと、または認証バイパスを実行するようにポートが明示的に設定されている場合に発生します。MAB を適用すると、ホストはネットワーク アクセス デバイスに接続します。

デバイスは適切なソフトウェア エージェントがホストに存在しないことを検出すると、MAC アドレスによってホストを識別する必要があると判断します。*service-type=10* およびホストの MAC アドレスを含む RADIUS 要求を Calling-Station-Id 属性で ACS に送信します。

一部のデバイスで、PAP 認証または EAP-MD5 認証を送信して MAB 要求を実行するように設定されている場合があります。このとき、ユーザ名、ユーザ パスワード、および CallingStationID 属性にホストの MAC アドレスが含まれますが、*service-type=10* 属性は含まれません。

ホスト ルックアップのほとんどの使用例は MAC アドレスの取得ですが、デバイスが個別のパラメータ検証を要求する場合や、MAC アドレスの代わりにこの値が Calling-Station-Id 属性に含まれる場合など、その他のシナリオも考えられます。たとえば、レイヤ 3 での使用例では IP アドレスとなります。

表 4-3 に、ホスト ルックアップの使用例に必要な RADIUS パラメータを示します。

*表 4-3　　ホスト ルックアップの使用例に対する RADIUS 属性*

| | 使用例 | | |
|---|---|---|---|
| **属性** | **PAP** | **802.1x** | **EAP-MD5** |
| **RADIUS::ServiceType** | — | コール チェック（PAP または EAP-MD5 を使用） | — |
| **RADIUS::UserName** | MAC address | 任意の値（通常は MAC アドレス） | MAC address |
| **RADIUS::UserPassword** | MAC address | 任意の値（通常は MAC アドレス） | MAC address |
| **RADIUS::CallingStationID** | MAC address | MAC address | MAC address |

ACS では、次の ID ストアのホスト ルックアップがサポートされています。

- 内部ホスト
- 外部 LDAP
- 内部ユーザ
- Active Directory

Active Directory には LDAP API 経由でアクセスできます。

内部ユーザ ID ストアに関連ホストがすでにリストされていて、内部ホスト ID ストアにデータを移動しない場合は、ホスト ルックアップに内部ユーザ ID ストアを使用できます。

ACS が使用するのは MAC 形式（XX-XX-XX-XX-XX-XX）であり、その他の形式に変換することはできません。User-Name 属性（xx:xx:xx:xx:xx:xx など）を使用して内部ユーザ ID ストアを検索するには、[Process Host Lookup] オプションをオフにしておく必要があります。ACS では要求を PAP 要求として処理します。

ホスト ルックアップ設定によって、PAP または EAP-MD5 上での MAC アドレス認証が検出されない場合、認証および認可は通常の PAP または EAP-MD5 のユーザ認証と同様に実行されます。ID ストアには、これらの認証プロトコルをサポートする任意のストアを使用できます。ACS は、RADIUS User-Name 属性で示した MAC アドレス形式を使用します。

**関連項目**

- ホスト ルックアップ用アクセス サービスの作成（4-19 ページ）
- 内部 ID ストア ホストの一括操作の表示および実行（8-19 ページ）
- ユーザおよび ID ストアの管理（8-1 ページ）
- コール チェックを使用する認証（4-15 ページ）

# コール チェックを使用する認証

Call Check 属性を含むネットワーク アクセス要求をホスト ルックアップ（RADIUS::ServiceType = 10）として識別する場合、ACS は認証ポリシーに従って、設定された ID ストアで Calling-Station-ID 属性（MAC アドレスなど）の値をルックアップし、ホストを認証（確認）および認可します。

ACS は RADIUS メッセージを受信すると、基本的な分析と確認を実行し、Call Check 属性（RADIUS ServiceType(6)）の値が 10 に等しいかどうかを確認します。RADIUS ServiceType が 10 に等しい場合は、システム ディクショナリ属性 UseCase をホスト ルックアップの値に設定します。

ACS のパケット処理フローでは、Call Check service-type によるホスト ルックアップの検出はサービス セレクション ポリシーの前に実行されます。サービス セレクション ポリシーでは条件 *UseCase equals Host Lookup* を使用できます。

RADIUS 要求の処理では、まず RADIUS User-Name 属性が System UserName 属性にコピーされます。RADIUS Service-Type が 10 の場合は、RADIUS Calling-Station-ID 属性が System User-Name 属性にコピーされ、RADIUS User-Name 属性の値が上書きされます。

ACS では、次の 4 つの MAC アドレス形式がサポートされています。

- ハイフンで区切られた 6 グループの 2 桁 16 進数字：01-23-45-67-89-AB
- コロンで区切られた 6 グループの 2 桁 16 進数字：01:23:45:67:89:AB
- ドットで区切られた 3 グループの 4 桁 16 進数字：0123.4567.89AB
- 区切り文字なしの連続する 12 桁の 16 進数字：0123456789AB

Calling-Station-ID 属性が、サポートされている上記 4 つの MAC アドレス形式のいずれかである場合は、ACS によって XX-XX-XX-XX-XX-XX の形式で User-Name 属性にコピーされます。MAC アドレスが上記 4 つ以外の形式である場合は、ストリングがそのままコピーされます。

## Service-Type Call Check の処理

CallingStationID 属性値を System UserName 属性値にコピーしない場合があります。[Process Host Lookup] オプションがオンの場合、ACS は RADIUS User-Name 属性からコピーされた System UserName 属性を使用します。

[Process Host Lookup] オプションがオフの場合は、[HostLookup] フィールドは無視され、元の System UserName 属性の値を使用して認証および認可が行われます。要求の処理は、メッセージ プロトコルに従って続行されます。たとえば、PAP の RADIUS User-Name や User-Password の属性などに従います。

[Process Host Lookup] オプションの設定については、ホスト ルックアップ用アクセス サービスの作成（4-19 ページ）を参照してください。

# PAP/EAP-MD5 認証

MAC アドレス認証に PAP または EAP-MD5 を使用するようにデバイスを設定してある場合は、ネットワーク アクセス サービス内で要求をホスト ルックアップ要求として検出するように、ACS を設定できます。デバイスは、User-Name、User-Password、および Calling-Station-ID の各属性にホストの MAC アドレスを含む要求を送信します。

ホスト ルックアップを検出するように ACS を設定しない場合、アクセス要求は通常の PAP または EAP-MD5 認証要求として処理されます。

[Process HostLookup] フィールドをオンにし、PAP または EAP-MD5 を選択すると、ACS::UseCase 属性に HostLookup 値が設定されます。User-Password 属性は、検出アルゴリズムで無視されます。

ACS は、要求が Call Check 属性を使用している場合と同様に認証プロセスを継続し、その要求をホスト ルックアップ（Service-Type=10）要求として処理します。RADIUS ディクショナリ属性 ACS::UseCase は HostLookup の値に設定されます。

PAP および EAP-MD5 MAC 認証の [Detect Host Lookup] オプションは、サービス セレクション ポリシーのあとに実行されます。サービス セレクション規則が ACS::UseCase = Host Lookup に一致するように設定されている場合、要求はホスト ルックアップ カテゴリに分類されます。

PAP 認証または EAP-MD5 認証を MAC 認証フローとして検出するように ACS が設定されていない場合、ACS では [Detect Host Lookup] オプションが考慮されません。これらの要求は通常のユーザ認証要求と同様に処理され、選択されている ID ストア内でユーザ名とパスワードが検索されます。

**関連項目**

- ホスト ルックアップ用アクセス サービスの作成（4-19 ページ）
- アクセス ポリシーの管理（10-1 ページ）
- 内部 ID ストア ホストの一括操作の表示および実行（8-19 ページ）
- ユーザおよび ID ストアの管理（8-1 ページ）

# エージェントレス ネットワーク アクセスのフロー

ここでは、エンドツーエンドのエージェントレス ネットワーク アクセス フローについて説明し、実行が必要なタスクを示します。タスクを設定する方法に関する情報は、該当するタスクの章にあります。

ACS でエージェントレス ネットワーク アクセスを設定するには、リストされた順序で次の手順を実行します。

**ステップ 1**　ネットワーク デバイスおよび AAA クライアントを設定します。

これは、ACS でネットワーク デバイスおよび AAA クライアントを設定する一般的なタスクです。エージェントレス ネットワーク アクセスに固有のタスクではありません。[Network Resources] > [Network Devices and AAA Clients] を選択し、[Create] をクリックします。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。

**ステップ 2**　内部ホストの ID ストアを設定します。

- 内部 ID ストアを設定します。内部 ID ストアへのホストの追加（4-17 ページ）を参照してください。

  または

- 外部 ID ストアを設定します。LDAP 外部 ID ストアのホスト ルックアップ用の設定（4-18 ページ）を参照してください。

詳細については、第 8 章「ユーザおよび ID ストアの管理」を参照してください。

**ステップ 3**　ID グループを設定します。ホスト ルックアップ ネットワーク アクセス要求用の ID グループの設定（4-18 ページ）を参照してください。

詳細については、第 8 章「ユーザおよび ID ストアの管理」を参照してください。

**ステップ 4**　ホスト ルックアップ要求用のポリシー要素および認可プロファイルを定義します。

詳細については、第 9 章「ポリシー要素の管理」を参照してください。

**ステップ 5**　ホスト ルックアップ用のアクセス サーバを定義することによって、空のサービスを作成します。詳細については、ホスト ルックアップ用アクセス サービスの作成（4-19 ページ）を参照してください。

**ステップ 6**　作成したサービスに戻ります。

a. ID ポリシーを定義します。詳細については、ホスト ルックアップ要求用の ID ポリシーの設定（4-19 ページ）を参照してください。

   ACS には、複数の ID ストアでホスト MAC アドレスを検索するオプションがあります。

   たとえば、MAC アドレスは、内部ホスト ID ストア、設定済みの LDAP ID ストアのいずれか、または内部ユーザ ID ストア内に格納されている可能性があります。

   MAC アドレス ルックアップは設定済みの ID ストアのいずれかで行い、MAC 属性は ID 順序で設定した別の ID ストアから取り出すことができます。

   ID ストアで MAC アドレスが検出されなかった場合でも、ホスト ルックアップ要求の処理を続行するように、ACS を設定できます。管理者は、MAC アドレスが検出されたかどうかに関係なく、イベントに基づいて認可ポリシーを定義できます。

   ACS::UseCase 属性は認証ポリシーの選択に使用できますが、ホスト ルックアップのサポートには必須ではありません。

b. 作成したサービスに戻ります。

c. 認可ポリシーを定義します。詳細については、ホスト ルックアップ要求用の認可ポリシーの設定（4-20 ページ）を参照してください。

**ステップ 7**　サービス セレクションを定義します。

**ステップ 8**　アクセス サービスをサービス セレクション ポリシーに追加します。詳細については、サービス セレクション ルールの作成、複製、および編集（10-8 ページ）を参照してください。

**関連項目**

- ユーザおよび ID ストアの管理（8-1 ページ）
- アクセス ポリシーの管理（10-1 ページ）

# 内部 ID ストアへのホストの追加

ホスト ルックアップ用の内部 ID ストアを設定するには、次の手順を実行します。

**ステップ 1**　[Users and Identity Store] > [Internal Identity Stores] > [Hosts] を選択し、[Create] をクリックします。

詳細については、内部 ID ストア ホストの一括操作の表示および実行（8-19 ページ）を参照してください。

**ステップ 2**　[Users and Identity Stores] > [Internal Identity Store] > [Hosts] > [Create] ページの説明に従って、フィールドに入力します。

**ステップ 3**　[Submit] をクリックします。

**前の手順：**

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）

**次の手順：**

ホスト ルックアップ ネットワーク アクセス要求用の ID グループの設定（4-18 ページ）

# LDAP 外部 ID ストアのホスト ルックアップ用の設定

ホスト ルックアップ用に LDAP 外部 ID ストアを設定するには、次の手順を実行します。

**ステップ 1**　[Users and Identity Stores] > [External Identity Stores] > [LDAP] を選択し、[Create] をクリックします。詳細については、外部 LDAP ID ストアの作成（8-27 ページ）を参照してください。

**ステップ 2**　LDAP データベース作成の手順を実行します。

[LDAP: Directory Organization] ページで MAC アドレス形式を選択します。

MAC アドレスは、選択した形式で LDAP 外部 ID ストアに保存されます。

**ステップ 3**　[Finish] をクリックします。

**前の手順：**

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）

**次の手順：**

ホスト ルックアップ ネットワーク アクセス要求用の ID グループの設定（4-18 ページ）

**関連項目**

- 外部 LDAP ID ストアの作成（8-27 ページ）
- 外部 LDAP ID ストアの削除（8-33 ページ）

# ホスト ルックアップ ネットワーク アクセス要求用の ID グループの設定

ホスト ルックアップ ネットワーク アクセス要求用に ID グループを設定するには、次の手順を実行します。

**ステップ 1**　[Users and Identity Store] > [Identity Groups] を選択し、[Create] をクリックします。

詳細については、ID 属性の管理（8-7 ページ）を参照してください。

**ステップ 2**　必要に応じてフィールドに入力します。

ID グループには、プリンタや電話機など、任意のエージェントレス デバイスを指定できます。

**ステップ 3**　[Submit] をクリックします。

**前の手順：**

- 内部 ID ストアへのホストの追加（4-17 ページ）
- LDAP 外部 ID ストアのホスト ルックアップ用の設定（4-18 ページ）

**次の手順：**

- ホスト ルックアップ用アクセス サービスの作成（4-19 ページ）

**関連項目**

- ID 属性の管理（8-7 ページ）

# ホスト ルックアップ用アクセス サービスの作成

アクセス サービスを作成してから、エージェントレス ホストの処理をイネーブルにします。

ホスト ルックアップ用にアクセス サービスを作成するには、次の手順を実行します。

**ステップ 1**　[Access Policies] > [Access Service] を選択し、[Create] をクリックします。詳細については、アクセス サービスの設定（10-11 ページ）を参照してください。

**ステップ 2**　[Access Service Properties - General] ページの説明に従って、フィールドに入力します。

a. [Service Structure] セクションで [User Selected Policy Structure] を選択します。

b. [Access Service Type] を [Network Access] に設定し、ポリシー構造を定義します。

c. [Network Access] を選択し、[Identity] および [Authorization] をオンにします。

グループ マッピングおよび [External Policy] オプションは任意です。

d. [Process Host Lookup] を選択する必要があります。

ACS で PAP 認証または EAP-MD5 認証を検出して MAC アドレスを取得し（PAP/EAP-MD5 認証（4-15 ページ）を参照）、ホスト ルックアップ要求（MAB 要求など）と同様に処理する場合は、次の手順を実行します。

e. [Allowed Protocols] ページで、ACS がサポートしている MAB 用のプロトコルのいずれか（EAP-MD5 または PAP）を選択します。

f. ホスト ルックアップとして [Detect PAP/EAP-MD5] を選択します。

**関連項目**

- アクセス ポリシーの管理（10-1 ページ）
- ACS 5.4 での認証（B-1 ページ）
- コール チェックを使用する認証（4-15 ページ）
- Service-Type Call Check の処理（4-15 ページ）

## ホスト ルックアップ要求用の ID ポリシーの設定

ホスト ルックアップ要求用に ID ポリシーを設定するには、次の手順を実行します。

**ステップ 1**　[Access Policies] > [Access Services] > [<access_servicename> Identity] を選択します。

詳細については、ID ポリシーの表示（10-22 ページ）を参照してください。

**ステップ 2**　[Customize] を選択し、認可ポリシー条件をカスタマイズします。

条件のリストが表示されます。このリストには、ID 属性、システム条件、およびカスタム条件が含まれています。詳細については、ポリシーのカスタマイズ（10-4 ページ）を参照してください。

**ステップ 3**　[Available] カスタマイズ条件から [Use Case] を選択し、[Selected] 条件に移動します。

**ステップ 4**　[Identity Policy] ページで [Create] をクリックします。

**a.** 規則の [Name] を入力します。

**b.** [Conditions] 領域で [Use Case] をオンにし、値が一致する必要があるかどうかを確認します。

**c.** [Host Lookup] を選択し、[OK] をクリックします。

この属性選択によって、アクセス要求の処理中に、ACS によって IP アドレスではなくホストが検索されます。

**d.** 使用する [Identity Source] として、ホスト ルックアップをサポートする ID ストアのいずれかを選択します。

**e.** [OK] をクリックします。

**ステップ 5**　[Save Changes] をクリックします。

**関連項目**

- アクセス ポリシーの管理（10-1 ページ）

## ホスト ルックアップ要求用の認可ポリシーの設定

ホスト ルックアップ要求用に認可ポリシーを設定するには、次の手順を実行します。

**ステップ 1**　[Access Policies] > [Access Services] > [<access_servicename> Authorization] を選択します。

詳細については、ネットワーク アクセス用セッション認可ポリシーの設定（10-29 ページ）を参照してください。

**ステップ 2**　[Customize] を選択し、認可ポリシー条件をカスタマイズします。

条件のリストが表示されます。このリストには、ID 属性、システム条件、およびカスタム条件が含まれています。

詳細については、ポリシーのカスタマイズ（10-4 ページ）を参照してください。

**ステップ 3**　[Available] カスタマイズ条件から [Use Case] を選択し、[Selected] 条件に移動します。

**ステップ 4**　カスタマイズ結果から [Authorization Profiles] を選択し、[Selected] 条件に移動して [OK] をクリックします。

**ステップ 5**　[Authorization Policy] ページで [Create] をクリックします。

**a.** 規則の [Name] を入力します。

**b.** [Conditions] 領域で [Use Case] をオンにし、値が一致する必要があるかどうかを確認します。

**c.** [Host Lookup] を選択し、[OK] をクリックします。

この属性選択によって、アクセス要求の処理中に、ACS によって IP アドレスではなくホストが検索されます。

**d.** 認可プロファイルから [Authorization Profile] を選択し、[Selected] 結果カラムに移動します。

**e.** [OK] をクリックします。

ステップ 6　[Save Changes] をクリックします。

**関連項目**

- アクセス ポリシーの管理（10-1 ページ）

# VPN リモート ネットワーク アクセス

リモート アクセス バーチャル プライベート ネットワーク（VPN）を使用すると、パブリックなインターネットからプライベートな企業ネットワークに安全に接続できます。自宅またはその他の場所から、自社のネットワークにアクセスすることも可能です。この VPN は、自社の境界ネットワーク（DMZ）に接続されます。VPN ゲートウェイでは同時 VPN 接続を管理できます。

**関連項目**

- サポートされている認証プロトコル（4-21 ページ）
- サポートされる ID ストア（4-21 ページ）
- サポートされている VPN ネットワーク アクセス サーバ（4-22 ページ）
- サポートされている VPN クライアント（4-22 ページ）
- VPN リモート アクセス サービスの設定（4-23 ページ）

## サポートされている認証プロトコル

ACS 5.4 では、VPN トンネル内の内部認証用に次のプロトコルがサポートされています。

- RADIUS/PAP
- RADIUS/CHAP
- RADIUS/MS-CHAPv1
- RADIUS/MS-CHAPv2

MS-CHAPv1 プロトコルまたは MS-CHAPv2 プロトコルを使用すると、作成されるトンネルを暗号化するための MPPE キーを ACS で生成できます。

**関連項目**

- VPN リモート ネットワーク アクセス（4-21 ページ）
- サポートされる ID ストア（4-21 ページ）
- サポートされている VPN ネットワーク アクセス サーバ（4-22 ページ）
- サポートされている VPN クライアント（4-22 ページ）
- VPN リモート アクセス サービスの設定（4-23 ページ）

## サポートされる ID ストア

ACS は、次の ID ストアに対する VPN 認証を実行できます。

- ACS 内部 ID ストア：RADIUS/PAP、RADIUS/CHAP、RADIUS/MS-CHAP-v1、および RADIUS/MS-CHAP-v2
- Active Directory：RADIUS/PAP、RADIUS/MS-CHAP-v1、および RADIUS/MS-CHAP-v2
- LDAP：RADIUS/PAP
- RSA SecurID サーバ：RADIUS/PAP
- RADIUS トークン サーバ：RADIUS/PAP（ダイナミック OTP）

**関連項目**

- VPN リモート ネットワーク アクセス（4-21 ページ）
- サポートされている認証プロトコル（4-21 ページ）
- サポートされている VPN ネットワーク アクセス サーバ（4-22 ページ）
- サポートされている VPN クライアント（4-22 ページ）
- VPN リモート アクセス サービスの設定（4-23 ページ）

# サポートされている VPN ネットワーク アクセス サーバ

ACS 5.4 では、次の VPN ネットワーク アクセス サーバがサポートされています。

- Cisco ASA 5500 シリーズ
- Cisco VPN 3000 シリーズ

**関連項目**

- VPN リモート ネットワーク アクセス（4-21 ページ）
- サポートされている認証プロトコル（4-21 ページ）
- サポートされる ID ストア（4-21 ページ）
- サポートされている VPN クライアント（4-22 ページ）
- VPN リモート アクセス サービスの設定（4-23 ページ）

# サポートされている VPN クライアント

ACS 5.4 では、次の VPN クライアントがサポートされています。

- Cisco VPN Client 5.0 シリーズ
- Cisco Clientless SSL VPN（WEBVPN）
- Cisco AnyConnect VPN クライアント 2.3 シリーズ
- MS VPN クライアント

**関連項目**

- VPN リモート ネットワーク アクセス（4-21 ページ）
- サポートされている認証プロトコル（4-21 ページ）
- サポートされる ID ストア（4-21 ページ）
- サポートされている VPN ネットワーク アクセス サーバ（4-22 ページ）
- VPN リモート アクセス サービスの設定（4-23 ページ）

# VPN リモート アクセス サービスの設定

VPN リモート アクセス サービスを設定するには、次の手順を実行します。

**ステップ 1**　デフォルト ネットワーク アクセス サービスの [Allowed Protocols] ページで、VPN プロトコルを設定します。詳細については、アクセス サービスの許可されたプロトコルの設定（10-16 ページ）を参照してください。

**ステップ 2**　ディクショナリ タイプ、および Tunneling-Protocols 属性のタイプと値を選択して、VPN の認可プロファイルを作成します。詳細については、認可プロファイルの RADIUS 属性の指定（9-22 ページ）を参照してください。

**ステップ 3**　[Submit] をクリックし、VPN 認可プロファイルを作成します。

**関連項目**

- VPN リモート ネットワーク アクセス（4-21 ページ）
- サポートされている認証プロトコル（4-21 ページ）
- サポートされる ID ストア（4-21 ページ）
- サポートされている VPN ネットワーク アクセス サーバ（4-22 ページ）
- サポートされている VPN クライアント（4-22 ページ）
- VPN リモート アクセス サービスの設定（4-23 ページ）

# ACS と Cisco Security Group Access

（注）　ACS は、Security Group Access 機能をイネーブルにするために追加機能ライセンスが必要です。

Cisco Security Group Access（以後、Security Group Access と呼ぶ）は、シスコ製品の新しいセキュリティ アーキテクチャです。ネットワーク トラフィックの機密保持、メッセージ認証、整合性、アンチリプレイ保護を提供する信頼できるネットワーク ファブリックを作成するために Security Group Access を使用できます。

Security Group Access では、すべてのネットワーク デバイスに ID を設定し、それらのデバイスがネットワーク内で動作を開始する前に認証および認可を行う必要があります。この対策により、セキュアなネットワーク内に不適切なネットワーク デバイスが接続されることを予防できます。

これまで、ACS はユーザおよびホストだけを認証し、ネットワークへのアクセスを許可していました。Security Group Access により、ACS は、名前とパスワードを使用して、ルータやスイッチなどのデバイスも認証します。ネットワーク インターフェイス カード（NIC）が取り付けられているすべてのデバイスは、デバイス自身を認証するか、または信頼ネットワークには接続しないようにする必要があります。

IP アドレスではなく名前によってデバイスを識別できるため、セキュリティが向上し、デバイス管理が簡素化されます。

（注）　Cisco IOS 12.2(33) SXI が稼働する Cisco Catalyst 6500 および DataCenter 3.0 (Nexus 7000) NX-OS 4.0.3 デバイスは Security Group Access をサポートしています。Cisco Catalyst 6500 では Security Group Tag（SGT）がサポートされていますが、このリリースでは Security Group Access Control List（SGACL）はサポートされていません。

Security Group Access 用に ACS を設定するには、次の手順を実行します。

1. ユーザの追加

   これは、ACS でユーザを追加する一般的なタスクです。Security Group Access に固有ではありません。[Users and Identity Stores] > [Internal Identity Store] > [Users] を選択し、[Create] をクリックします。詳細については、内部ユーザの作成（8-12 ページ）を参照してください。
2. Security Group Access 用デバイスの追加。
3. セキュリティ グループの作成。
4. SGACL の作成。
5. NDAC ポリシーの設定。
6. Security Group Access 用の EAP-FAST 設定の構成。
7. Security Group Access アクセス用のアクセス サービスの作成。
8. エンドポイント アドミッション コントロール ポリシーの作成。
9. 出力ポリシーの作成。
10. デフォルト ポリシーの作成。

# Security Group Access 用デバイスの追加

RADIUS プロトコルには、AAA クライアントとサーバ間の共有秘密情報が必要です。ACS では、RADIUS 要求が既知の AAA クライアントから送信された場合にだけ、この要求が処理されます。共有秘密情報を使用して ACS の AAA クライアントを設定する必要があります。

Security Group Access デバイスは、同じ共有秘密を使用して設定する必要があります。Security Group Access では、すべてのデバイスが、セキュア ネットワークに参加する新しいデバイスに対して AAA クライアントとして動作できる必要があります。

すべての Security Group Access デバイスは、EAP Flexible Authentication via Secured Tunnel（EAP-FAST）プロトコルの一部として、Protected Access Credential（PAC）を所有しています。PAC は、AAA クライアントの識別に使用されます。RADIUS 共有秘密情報は、この PAC から取得できます。

ネットワーク デバイスを追加するには、次の手順を実行します。

**ステップ 1**　[Network Resources] > [Network Devices and AAA Client] を選択し、[Create] をクリックします。詳細については、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。

**ステップ 2**　[Network Devices and AAA Clients] ページのフィールドに入力します。

- デバイスをシード Security Group Access デバイスとして追加するには、[RADIUS] および [Security Group Access] をオンにし、Security Group Access クライアントとしてデバイスを追加するには、[Security Group Access] のみをオンにします。

  RADIUS クライアントとしてデバイスを追加する場合は、[IP Address] および [RADIUS/Shared Secret] を入力します。

Security Group Access デバイスとしてデバイスを追加する場合は、[Security Group Access] セクションのフィールドに入力します。

- [Advanced Settings] をオンにして、Security Group Access デバイス設定の詳細設定を表示し、デフォルト設定を修正できます。

場所またはデバイス タイプは、NDAC ポリシー規則を設定するための条件として使用できます。

**ステップ 3**　[Submit] をクリックします。

# セキュリティ グループの作成

Security Group Access は、入力でパケットにタグを付加するためにセキュリティ グループを使用して、あとで出力時にフィルタできるようにします。セキュリティ グループを使用した結果、セキュリティ グループ タグが付加されます。これは、ネットワーク デバイスに送信される 4 バイトのストリング ID です。

Web インターフェイスでは 10 進数および 16 進数で表示されます。SGT の値は一意です。セキュリティ グループを編集するときに、名前は変更できますが SGT ID は変更できません。

セキュリティ グループ名 *Unknown* および *Any* は予約されています。この予約名は、出力ポリシー マトリクスで使用します。出力ポリシーが変更されると、生成 ID が変更されます。

デバイスで考慮されるのは SGT の値だけです。セキュリティ グループの名前および説明は管理上の便宜のためのものであり、デバイスには伝達されません。したがって、セキュリティ グループの名前と説明を変更しても、SGT の生成 ID には影響ありません。

セキュリティ グループを作成するには、次の手順を実行します。

**ステップ 1**　[Policy Elements] > [Authorizations and Permissions] > [Network Access] > [Security Groups] を選択し、[Create] をクリックします。

**ステップ 2**　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（9-34 ページ）の説明に従って、フィールドに入力します。

**ヒント**　セキュリティ グループを編集すると、セキュリティ グループ タグおよび生成 ID が表示されます。

**ステップ 3**　[Submit] をクリックします。

# SGACL の作成

Security Group Access Control List（SGACL）は、標準的な IP ベースの ACL によく似ており、TCP、ユーザ データグラム プロトコル（UDP）、およびポートまでのトランスポート プロトコル、FTP、または Secure Shell Protocol（SSH）の通信を許可または拒否するかどうかを指定できます。

セキュリティ グループ間の通信に適用する SGACL も作成できます。ACS で Security Group Access ポリシー管理を適用するには、カスタマイズ可能な出力マトリクス ビューを使用して送信元および宛先のセキュリティ グループの共通部分、または個々の送信元および宛先のセキュリティ グループ ペアにこれらの SGACL を設定します。

SGACL を作成するには、次の手順を実行します。

ステップ 1　[Policy Elements] > [Authorizations and Permissions] > [Named Permissions Objects] > [Security Group ACLs] を選択し、[Create] をクリックします。

ステップ 2　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（9-34 ページ）の説明に従って、フィールドに入力します。

ステップ 3　[Submit] をクリックします。

# NDAC ポリシーの設定

Network Device Admission Control（NDAC; ネットワーク デバイス アドミッション コントロール）ポリシーでは、デバイスに送信されるセキュリティ グループを定義します。NDAC ポリシーを設定する場合は、NDG など、あらかじめ定義されている条件を使用して規則を作成します。

NDAC ポリシーは単一のサービスで、1 つ以上の規則が定義された単一のポリシーが含まれます。認証、ピア認可、および環境の各要求に対する応答の設定には同じポリシーが使用されるため、同じデバイスに適用した場合は、すべての要求タイプについて同じ SGT が返されます。

（注）　サービス セレクション ポリシーのサービスとして NDAC ポリシーを追加できません。ただし、NDAC ポリシーは Security Group Access デバイスに自動的に適用されます。

デバイスに NDAC ポリシーを設定するには、次の手順を実行します。

ステップ 1　[Access Policies] > [Security Group Access Control] > [Security Group Access] > [Network Device Access] > [Authorization Policy] を選択します。

ステップ 2　[Customize] をクリックし、NDAC ポリシー規則で使用する条件を選択します。

[Default Rule] は、一致する規則がない場合、または規則が定義されていない場合のデフォルト規則となります。[Default Rule] 結果のデフォルト セキュリティ グループ タグは [Unknown] です。

ステップ 3　[Create] をクリックし、新しい規則を作成します。

ステップ 4　[NDAC Policy Properties] ページのフィールドに入力します。

ステップ 5　[Save Changes] をクリックします。

# Security Group Access 用の EAP-FAST 設定の構成

RADIUS 情報は PAC から取得されるため、EAP-FAST トンネル PAC の存続時間を定義する必要があります。アクティブな PAC の存続可能時間を更新することもできます。

トンネル PAC の EAP-FAST 設定を行うには、次の手順を実行します。

ステップ 1　[Access Policies] > [Security Group Access Control] > [Network Device Access] を選択します。

ステップ 2　[Network Device Access EAP-FAST Settings] ページのフィールドに入力します。

ステップ 3　[Submit] をクリックします。

# Security Group Access アクセス用のアクセス サービスの作成

エンドポイント デバイスに対するエンドポイント アドミッション コントロール ポリシー用のアクセス サービスを作成し、サービス セレクション ポリシーにそのサービスを追加できます。

（注）　NDAC ポリシーは Security Group Access デバイスに自動的に適用されるサービスです。Security Group Access デバイス用のアクセス サービスを作成する必要はありません。

アクセス サービスを作成するには、次の手順を実行します。

**ステップ 1**　[Access Policies] > [Access Service] を選択し、[Create] をクリックします。詳細については、アクセス サービスの設定（10-11 ページ）を参照してください。

**ステップ 2**　必要に応じて、[Access Service Properties - General] ページのフィールドに入力します。

**ステップ 3**　[Service Structure] セクションで [User selected policy structure] を選択します。

**ステップ 4**　[Network Access] を選択し、[Identity] および [Authorization] をオンにします。

**ステップ 5**　[Next] をクリックします。

[Access Services Properties] ページが表示されます。

**ステップ 6**　[Authentication Protocols] 領域で、使用するアクセス サービスに関連するプロトコルのチェックボックスをオンにします。

**ステップ 7**　[Finish] をクリックします。

# エンドポイント アドミッション コントロール ポリシーの作成

サービスを作成したあとに、エンドポイント アドミッション コントロール ポリシーを設定します。エンドポイント アドミッション コントロール ポリシーは、エンドポイントに対する SGT および認可プロファイルを返します。複数のポリシーを作成し、デフォルト規則ポリシーを設定できます。デフォルトは Deny Access および Unknown セキュリティ グループです。

アクセス サービスにセッション認可ポリシーを追加するには、次の手順を実行します。

**ステップ 1**　[Access Policies] > [Access Services] > ***service*** > [Authorization] を選択します。

**ステップ 2**　認可ポリシーを設定します。ネットワーク アクセス用セッション認可ポリシーの設定（10-29 ページ）を参照してください。

**ステップ 3**　[Network Access Authorization Rule Properties] ページのフィールドに入力します。

[Default Rule] は、一致する規則がない場合、または規則が定義されていない場合のデフォルト規則となります。デフォルト規則結果のデフォルトは [Deny Access] です。この設定ではネットワークへのアクセスが拒否されます。セキュリティ グループ タグは [Unknown] です。

セキュリティ グループは、Security Group Access のセッション認可ポリシー作成時に変更できます。

**ステップ 4**　[OK] をクリックします。

**ステップ 5**　[Access Policies] > [Service Selection Policy] を選択し、エンドポイント ポリシーに追加するサービスを選択します。詳細については、サービス セレクション ポリシーの設定（10-5 ページ）を参照してください。

**ステップ 6**　[Service Select Policy] ページのフィールドに入力します。

**ステップ 7**　[Save Changes] をクリックします。

# 出力ポリシーの作成

出力ポリシー（SGACL ポリシーとも呼ばれます）によって、送信元および宛先の SGT に基づいてネットワークの出力ポイントで適用される SGACL が決定されます。出力ポリシーはマトリクスで表現され、X 軸および Y 軸がそれぞれ宛先 SGT および送信元 SGT を表します。また、各セルにはこれら 2 つの SGT の共通部分に適用される SGACL のセットが入ります。

この SGT を伝送するエンドポイント（または Security Group Access デバイス）がパケットを送信する場合は、任意のセキュリティ グループが送信元 SGT の役割を果たすことができます。パケットが、この SGT を伝送するエンドポイント（または Security Group Access デバイス）を宛先とする場合は、任意のセキュリティ グループが宛先 SGT の役割を果たすことができます。したがって、出力マトリクスには既存のセキュリティ グループが両方の軸にすべてリストされ、SGT セットとその SGT セット自身のデカルト積（SGT x SGT）となります。

マトリクスの先頭行（最上部）にはカラム ヘッダーがあり、ここには宛先 SGT が表示されます。先頭列（左端）には行タイトルがあり、送信元 SG が表示されます。これらの軸の共通部分が原点セル（左上隅）で、軸のタイトル、つまり宛先および送信元が入ります。

他のすべてのセルは、定義済みの SGACL が含まれる内部マトリクス セルです。行および列は、SGT 名に従ってアルファベット順に並べられます。SGACL ごとに、200 個の ACE を保持できます。

最初のうち、マトリクスには未知の送信元 SG および未知の宛先 SG が入っています。*未知*というのは、事前に定義された SG のことであり、この値は変更できません。SG を追加すると、新しい行と新しい列がマトリクスに追加されます。新規に追加されるセルの内容は空です。

出力ポリシーを追加して出力マトリクスにデータを入力するには、次の手順を実行します。

**ステップ 1**　[Access Policies] > [Security Group Access Control] > [Egress Policy] を選択します。

出力マトリクスが表示されます。セキュリティ グループは定義した順序で表示されます。

**ステップ 2**　セルをクリックして [Edit] をクリックします。

**ステップ 3**　必要に応じてフィールドに入力します。

**ステップ 4**　セルに適用する SGACL のセットを選択し、選択したセットを [Selected] カラムに移動します。

この ACL は、セルの座標に一致する送信元および宛先の SGT の出力ポイントで使用されます。SGACL は表示される順序で適用されます。

**ステップ 5**　[Up] および [Down] の矢印を使用し、順序を変更します。デバイスは、設定された順序でポリシーを適用します。選択したセキュリティ グループのパケットに SGACL が適用されます。

**ステップ 6**　[Submit] をクリックします。

# デフォルト ポリシーの作成

出力マトリクスで送信元 SG および宛先 SG の出力ポリシーを設定したあとに、デフォルト出力ポリシーを設定することを推奨します。デフォルト ポリシーは、SGT が割り当てられていないデバイスに適用されます。デフォルト ポリシーは、ネットワーク デバイスによって、セルに定義されている特定のポリシーに追加されます。デフォルト ポリシーの初期設定は *Permit All* です。

*デフォルト ポリシー*という用語は、すべてのセキュリティ グループ ポリシーのすべてのセキュリティ グループと関連しています。Security Group Access ネットワーク デバイスで、デフォルト ポリシーは特定セルのポリシーの最後に連結されます。

セルがブランクの場合は、デフォルト ポリシーだけが適用されます。セルにポリシーが含まれている場合、得られるポリシーはセル固有のポリシーのあとにデフォルト ポリシーを結合したものになります。

特定セルのポリシーとデフォルト ポリシーの結合方法は、デバイスで稼働しているアルゴリズムによって異なります。結果は、2 つのポリシーを連結した場合と同じになります。

最初にパケットが分析され、セルの SGACL によって定義された ACE に一致するかどうかが確認されます。一致しない場合、そのパケットでは不成立となり、デフォルト ポリシーの ACE と一致するかどうかが確認されます。

セル固有ポリシーとデフォルト ポリシーの結合は、ACS ではなく、Security Group Access ネットワーク デバイスによって行われます。ACS 側から見ると、セル固有ポリシーとデフォルト ポリシーは 2 組の異なる SGACL であり、2 つの別々なポリシー クエリーに対する応答でデバイスに送信されます。

デフォルト ポリシーを作成するには、次の手順を実行します。

**ステップ 1**　[Access Policies] > [Security Group Access Control] > [Egress Policy] を選択し、[Default Policy] を選択します。

**ステップ 2**　[Default Policy for Egress Policy] ページに従ってフィールドに入力します。

**ステップ 3**　[Submit] をクリックします。

# RADIUS および TACACS+ プロキシ要求

ネットワーク アクセス サーバ（NAS）から RADIUS 認証要求および認証/許可 TACACS+ 要求を受信してそれらの要求をリモート サーバに転送するプロキシ サーバとして機能するように ACS を使用できます。次に ACS は、リモート RADIUS または TACACS+ サーバから転送された各要求の応答を受信し、その応答をクライアントに返送します。

ACS ではサービス セレクション ポリシーを使用して、ローカル処理が必要な着信認証要求およびアカウンティング要求と、リモート RADIUS または TACACS+ サーバへの転送が必要な要求とを区別します。

ACS は NAS からプロキシ要求を受信すると、リストにある最初のリモート RADIUS または TACACS+ サーバにその要求を転送します。リモート RADIUS サーバから届いた最初の有効または無効な応答を処理し、次の処理を実行します。

- Access-Challenge、Access-Accept、または Access-Reject など、応答が RADIUS に有効な場合、ACS は NAS に応答を返します。
- ACS が指定された期間内に、応答を受信しない場合、ACS は指定した回数の再試行の後で、または指定されたネットワーク タイムアウト後に、リスト内の次のリモート RADIUS サーバへ要求を転送します。

- 応答が無効な場合、ACS プロキシは次のリモート RADIUS サーバへのフェールオーバーを実行します。リストの最後のフェールオーバー リモート RADIUS サーバまで応答を取得せずに到達すると、ACS は要求をドロップし、NAS に応答をまったく送信しません。

ACS は、リモート TACACS+ サーバから届いた最初の有効または無効な応答を処理し、次の処理を実行します。

- TAC_PLUS_AUTHEN (REPLY) または TAC_PLUS_AUTHOR(RESPONSE) など、応答が TACACS+ に有効な場合、ACS は NAS に応答を返します。
- ACS が指定された期間内に、応答を受信しない場合、ACS は指定した回数の再試行の後で、または指定されたネットワーク タイムアウト後に、リスト内の次のリモート TACACS+ サーバへ要求を転送します。
- 応答が無効な場合、ACS プロキシは次のリモート TACACS+ サーバへのフェールオーバーを実行します。リストの最後のフェールオーバー リモート TACACS+ サーバまで応答を取得せずに到達すると、ACS は要求をドロップし、NAS に応答をまったく送信しません。

ユーザ名（RADIUS）またはユーザ（TACACS+）からプレフィックス、サフィックス、およびその両方を削除するように ACS を設定できます。たとえば、ユーザ名 acme\smith@acme.com から、\ および @ をそれぞれプレフィックスおよびサフィックスの区切り文字として指定すると、ユーザの名前 smith だけを抽出するように ACS を設定できます。

ACS では、ローカル アカウンティング、リモート アカウンティング、またはその両方を実行できます。両方を選択した場合、ACS はローカル アカウンティングを実行してからリモート アカウンティングに進みます。ローカル アカウンティングで何らかのエラーがあった場合、ACS はそのエラーを無視してリモート アカウンティングに進みます。

プロキシ処理の実行中、ACS は次の処理を行います。

1. NAS から次のパケットを受信し、リモート RADIUS サーバに転送します。
- Access-Request
2. リモート RADIUS サーバから次のパケットを受信し、NAS に返送します。
- Access-Accept
- Access-Reject
- Access-Challenge
3. NAS から次のパケットを受信し、リモート TACACS+ サーバに転送します。
- TAC_PLUS_AUTHOR
- TAC_PLUS_AUTHEN
4. 次のパケットをリモート TACACS+ サーバから受信し、NAS に返送します。この動作は設定可能です。
- TAC_PLUS_ACCT

応答のない外部 RADIUS サーバをおよそ *タイムアウト* X *リトライ回数*秒間待機してから、フェールオーバーによって次のサーバに移行します。

最初に応答のあるサーバに到達するまでに、リストには応答のないサーバがいくつか存在する可能性があります。この場合、応答のある外部 RADIUS サーバに転送される各要求は、*以前に応答のなかったサーバ数* X *タイムアウト* X *リトライ回数*の間、遅延します。

この遅延は、EAP または RADIUS カンバセーションにおける 2 つのメッセージ間の外部 RADIUS サーバ タイムアウトよりも長くなる可能性があります。このような場合、外部 RADIUS サーバで要求がドロップされる場合があります。

フェールオーバーによって次のサーバに移行するまで無応答の外部 TACACS+ サーバが待機する秒数を設定できます。

ACS 5.4 は、RADIUS（IPv4）および TACACS+（IPv4 と IPv6）プロキシ用に複数のネットワーク インターフェイス コネクタをサポートします。仮想マシン、UCS、IBM、または CAM プラットフォームの ACS 5.4 には最大 4 つのネットワーク インターフェイス（イーサネット 0、イーサネット 1、イーサネット 2、およびイーサネット 3）が搭載されています。詳細については、『*Installation and Upgrade Guide for Cisco Secure Access Control System 5.4.*』の『Connecting the Network Interface』セクションにある『Multiple Network Interface Connector』を参照してください。

**関連項目**

- サポートされているプロトコル（4-31 ページ）
- サポートされている RADIUS 属性（4-31 ページ）
- プロキシ サービスの設定（4-32 ページ）

# サポートされているプロトコル

ACS の RADIUS プロキシ機能では、次のプロトコルがサポートされています。

- すべての RADIUS プロトコルの転送のサポート
- すべての EAP プロトコル
- ACS でサポートされていないプロトコル（ACS プロキシはプロトコルのカンバセーションに干渉せず、単に要求を転送するため）

(注)　ACS プロキシは暗号化された RADIUS 属性を使用するプロトコルをサポートできません。

ACS の TACACS+ プロキシ機能では、次のプロトコルがサポートされています。

- PAP
- ASCII
- CHAP
- MSCHAP 認証タイプ

**関連項目**

- RADIUS および TACACS+ プロキシ要求（4-29 ページ）
- サポートされている RADIUS 属性（4-31 ページ）
- プロキシ サービスの設定（4-32 ページ）

# サポートされている RADIUS 属性

サポートされている次の RADIUS 属性は暗号化されます。

- User-Password
- CHAP-Password
- Message-Authenticator
- MPPE-Send-Key および MPPE-Recv-Key
- Tunnel-Password
- LEAP セッション キー Cisco AV-Pair

# TACACS+ の本文の暗号化

NAS から暗号化された本文があるパケット（フラグ TAC_PLUS_UNECRYPTED_FLAG は 0x0）を受信すると、ACS は NAS と ACS 間の共有秘密および sessionID などの共通データで本文を復号化し、ACS および TACACS+ プロキシ サーバ間の共通データで本文を暗号化します。パケットの本文がクリア テキストの場合、ACS はクリア テキストでそれを TACACS+ サーバへ再送信します。

# TACACS+ サーバへの接続

ACS は別の TACACS+ サーバへの単一の接続をサポートします（フラグ TAC_PLUS_SINGLE_CONNECT_FLAG は 1）。リモート TACACS+ サーバが単一 TCP 接続による多重化 TACACS+ セッションをサポートしない場合、ACS はセッションごとに接続を開くか閉じます。

**関連項目**

- RADIUS および TACACS+ プロキシ要求（4-29 ページ）
- サポートされているプロトコル（4-31 ページ）
- プロキシ サービスの設定（4-32 ページ）

# プロキシ サービスの設定

プロキシ サービスを設定するには、次の手順を実行します。

**ステップ 1**　一連のリモート RADIUS および TACACS+ サーバを設定します。リモート サーバを設定する方法の詳細については、外部プロキシ サーバの作成、複製、および編集（7-21 ページ）を参照してください。

**ステップ 2**　外部プロキシ サービスを設定します。外部プロキシ サービスを設定する方法の詳細については、一般アクセス サービス プロパティの設定（10-13 ページ）を参照してください。

[User Selected Service Type] オプションを選択し、[Access Service Properties - General] ページで [Access Service Policy Structure] として [External proxy] を選択する必要があります。

**ステップ 3**　許可されるプロトコルを設定したら、[Finish] をクリックして外部プロキシ サービスの設定を完了します。

**関連項目**

- RADIUS および TACACS+ プロキシ要求（4-29 ページ）
- サポートされているプロトコル（4-31 ページ）
- サポートされている RADIUS 属性（4-31 ページ）