認可の設定

AAA 認可機能を使用して、ユーザができることとできないことを定義します。AAA 認可をイネーブルにすると、ネットワーク アクセス サーバはユーザのプロファイルから取得した情報を使用して、ユーザの設定を設定します。このプロファイルは、ローカル ユーザ データベースまたはセキュリティ サーバにあります。認可が完了すると、ユーザ プロファイルの情報で許可されているサービスであれば、ユーザは要求したサービスに対するアクセス権を付与されます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。この章に記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「認可の設定に関する機能情報」（P.16）を参照してください。

プラットフォーム サポートと Cisco IOS および Catalyst OS ソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

この章の構成

前提条件

名前付き方式リストを使用して認可を設定する前に、次のタスクを実行する必要があります。

- ネットワーク アクセス サーバで AAA をイネーブルにします。
- AAA 認証を設定します。一般的に、認可は認証後に実行し、認証が適切に動作することに依存します。
- RADIUS または TACACS+ の認可が発行された場合、シスコ ネットワーク アクセス サーバが RADIUS または TACACS+ セキュリティ サーバと通信できるように、Lightweight Directory Access Protocol（LDAP）、RADIUS、または TACACS+ セキュリティ サーバの特性を定義します。
- ローカル認可が発行された場合、**username** コマンドを使用して、特定のユーザに関連付けられている権限を定義します。
- これらの前提条件に関連するマニュアルの詳細については、「関連資料」（P.14）を参照してください。

認可の設定の概要

ここでは、認可機能を設定する方法について説明します。

認可の名前付き方式リスト

認可の方式リストでは、認可の実行方法と、その方式を実行する順序を定義します。方式リストは、シーケンスで照会される認可方式（LDAP、RADIUS、TACACS+ など）を説明する単なる名前付きリストです。方式リストを使用すると、1 つまたは複数のセキュリティ プロトコルを認可に使用できるため、最初の方式が失敗した場合に備えて認可のバックアップ システムを確保できます。Cisco IOS ソフトウェアでは、特定のネットワーク サービスについてユーザを認可するために最初の方式が使用されます。その方式が応答しない場合、方式リストの次の方式が選択されます。このプロセスは、リストのいずれかの認可方式と通信に成功するか、定義されているすべての方式が試行されるまで継続されます。

（注） Cisco IOS ソフトウェアでは、前の方式からの応答がない場合にのみ、リストの次の認可方式が試行されます。このサイクルの任意の時点で認可が失敗した場合（つまり、セキュリティ サーバまたはローカル ユーザ名データベースからユーザ サービスの拒否応答が返される場合）、認可プロセスは停止し、その他の認可方式は試行されません。

方式リストは、要求した認可タイプに固有です。

- **Auth-proxy**：ユーザ別に特定のセキュリティ ポリシーを適用します。認証プロキシのコンフィギュレーション マニュアルの詳細については、「関連資料」（P.14）を参照してください。

- **Commands**：ユーザが発行する EXEC モード コマンドに適用します。コマンドの認可は、特定の特権レベルに関連付けられた、グローバル コンフィギュレーション コマンドなどのすべての EXEC モード コマンドについて、認可を試行します。
- **EXEC**：ユーザ EXEC ターミナル セッションに関連付けられたアトリビュートに適用します。
- **Network**：ネットワーク接続に適用します。これには、PPP、SLIP、または ARAP 接続が含まれます。
- **Reverse Access**：リバース Telnet セッションに適用されます。

名前付き方式リストが作成されると、指定した認可タイプに固有の認可方式のリストが定義されます。

定義されると、方式リストを特定の回線またはインターフェイスに適用してから、定義済み方式のいずれかを実行する必要があります。唯一の例外は、デフォルトの方式リスト（「default」という名前が指定されています）です。特定の認可タイプ用の **aaa authorization** コマンドが、名前付き方式リストを指定せずに発行されると、デフォルトの方式リストは、名前付き方式リストが明示的に定義されている場合を除き、すべてのインターフェイスまたは回線へ自動的に適用されます（定義した方式リストは、デフォルトの方式リストよりも優先されます）。デフォルトの方式リストが定義されていない場合、デフォルトで認可は実行されません。

AAA 認可方式

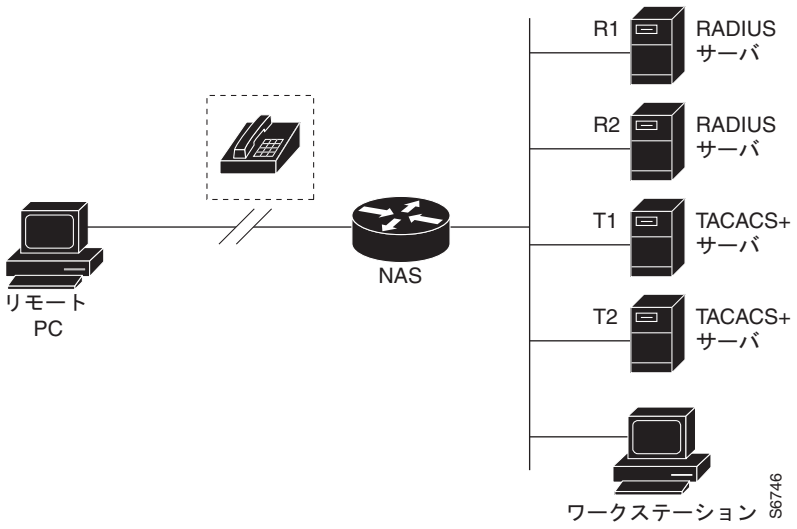
AAA は 5 種類の認可方式をサポートしています。

- TACACS+：ネットワーク アクセス サーバは、TACACS+ セキュリティ デーモンと認可情報を交換します。TACACS+ 認可は、アトリビュート値ペアを関連付けることでユーザに特定の権限を定義します。アトリビュートペアは適切なユーザとともに TACACS+ セキュリティ サーバのデータベースに保存されます。
- If-Authenticated：ユーザが認証に成功した場合、ユーザは要求した機能にアクセスできます。
- **None**：ネットワーク アクセス サーバは、認可情報を要求しません。認可は、この回線/インターフェイスで実行されません。
- Local：ルータまたはアクセス サーバは、**username** コマンドの定義に従って、ローカル データベースに問い合わせて、たとえばユーザに固有の権限を認可します。ローカル データベースでは制御できるのは、一部の機能だけです。
- LDAP：ネットワーク アクセス サーバは RADIUS セキュリティ サーバからの認可情報を要求します。LDAP 認可では、アトリビュートを関連付けることでユーザに固有の権限を定義します。アトリビュートは適切なユーザとともに LDAP サーバ上のデータベースに保存されます。
- RADIUS：ネットワーク アクセス サーバは RADIUS セキュリティ サーバからの認可情報を要求します。RADIUS 認可では、アトリビュートを関連付けることでユーザに固有の権限を定義します。アトリビュートは適切なユーザとともに RADIUS サーバ上のデータベースに保存されます。

方式リストとサーバ グループ

サーバ グループは、方式リストに使用する既存の LDAP、RADIUS、または TACACS+ サーバ ホストをグループ化する方法の 1 つです。図 1 に、4 台のセキュリティ サーバ（R1 と R2 は RADIUS サーバ、T1 と T2 は TACACS+ サーバ）が設置された一般的な AAA ネットワーク設定を示します。R1 と R2 で RADIUS サーバのグループを構成します。T1 と T2 で TACACS+ サーバのグループを構成します。

図 1　一般的な AAA ネットワーク設定



サーバ グループを使用して、設定したサーバ ホストのサブセットを指定し、特定のサービスに使用します。たとえば、サーバ グループを使用すると、R1 および R2 を 1 つのサーバ グループとして定義し、T1 および T2 を別のサーバ グループとして定義できます。R1 と T1 を方式リストに指定することや、R2 と T2 を方式リストに指定することができます。そのため、RADIUS および TACACS+ のリソースを割り当てる場合の柔軟性が高くなります。

サーバ グループには、1 台のサーバに対して複数のホスト エントリを含めることができます。エントリごとに固有の識別情報を設定します。固有の識別情報は、IP アドレスと UDP ポート番号の組み合わせで構成されます。これにより、RADIUS ホストとして定義されているさまざまなポートが、固有の AAA サービスを提供できるようになります。つまり、この固有識別情報を使用して、ある IP アドレスに位置する 1 台のサーバ上に複数の UDP ポートが存在する場合、それぞれの UDP ポートに対して RADIUS 要求を送信できます。1 台の RADIUS サーバ上にある異なる 2 つのホスト エントリが 1 つのサービス（認可など）に設定されている場合、設定されている 2 番めのホスト エントリは最初のホスト エントリのフェールオーバー バックアップとして動作します。この例の場合、最初のホスト エントリがアカウンティング サービスの提供に失敗すると、同じデバイスに設定されている 2 番めのホスト エントリを使用してアカウンティング サービスを提供するように、ネットワーク アクセス サーバが試行します（試行される RADIUS ホスト エントリの順番は、設定されている順序に従います）。

サーバ グループの設定および DNIS 番号に基づくサーバ グループの設定の詳細については、「Configuring LDAP」、「Configuring RADIUS」、または「Configuring TACACS+」の各フィーチャ モジュールを参照してください。

AAA 認可タイプ

Cisco IOS ソフトウェアは、5 種類の認可をサポートしています。

- **Auth-proxy**：ユーザ別に特定のセキュリティ ポリシーを適用します。認証プロキシのコンフィギュレーション マニュアルの詳細については、「関連資料」（P.14）を参照してください。
- **Commands**：ユーザが発行する EXEC モード コマンドに適用します。コマンドの認可は、特定の特権レベルに関連付けられた、グローバル コンフィギュレーション コマンドなどのすべての EXEC モード コマンドについて、認可を試行します。
- **EXEC**：ユーザ EXEC ターミナル セッションに関連付けられたアトリビュートに適用します。

- **Network**：ネットワーク接続に適用します。これには、PPP、SLIP、または ARAP 接続が含まれます。
- **Reverse Access**：リバース Telnet セッションに適用されます。
- Configuration：AAA サーバからのコンフィギュレーションのダウンロードに適用されます。
- IP Mobile：IP モバイル サービスの認可に適用されます。

認可のアトリビュート値ペア

RADIUS および TACACS+ の認可はいずれも、セキュリティ サーバのデータベースに保存されているアトリビュートを処理することで、ユーザに固有の権限を定義します。RADIUS と TACACS+ のいずれも、アトリビュートはセキュリティ サーバに定義され、ユーザに関連付けられ、ユーザの接続に適用されるネットワーク アクセス サーバに送信されます。

サポートされる RADIUS アトリビュートと TACACS+ アトリビュート値のペアの詳細については、「関連資料」（P.14）を参照してください。

認可の設定方法

ここでは、次の設定手順について説明します。

- 「名前付き方式リストによる AAA 認可の設定」
- 「グローバル コンフィギュレーション コマンドの認可のディセーブル化」
- 「リバース Telnet の認可の設定」

詳細については、「認可設定の例」（P.8）を参照してください。

名前付き方式リストによる AAA 認可の設定

名前付き方式リストを使用して AAA 認可を設定するには、次のタスクを実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa authorization** {**auth-proxy** | **network** | **exec** | **commands** *level* | **reverse-access** | **configuration** | **ipmobile**} {**default** | *list-name*} [*method1* [*method2...*]]
4. **line** [**aux** | **console** | **tty** | **vty**] *line-number* [*ending-line-number*]
5. **authorization** {**arap** | **commands** *level* | **exec** | **reverse-access**} {**default** | *list-name*}

手順の詳細

	コマンド	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	`Router(config)# aaa authorization {auth-proxy | network | exec | commands level | reverse-access | configuration | ipmobile} {default | list-name} [method1 [method2...]]`	特定の認可タイプの認可方式リストを作成し、認可をイネーブルにします。

ステップ 4	`Router(config)# line [aux | console | tty | vty] line-number [ending-line-number]`
	
	または
	
	`Router(config)# interface interface-type interface-number`
		認可方式リストを適用する回線について、ライン コンフィギュレーション モードを開始します。
		
		または、認可方式リストを適用するインターフェイスについて、インターフェイス コンフィギュレーション モードを開始します。

ステップ 5	`Router(config-line)# authorization {arap | commands level | exec | reverse-access} {default | list-name}`
	
	または
	`Router(config-line)# ppp authorization {default | list-name}`
		1 つの回線または複数回線に認可リストを適用します。
		
		または、1 つのインターフェイスまたは複数インターフェイスに認可リストを適用します。

ここでは、次の内容について説明します。

- 「認可タイプ」
- 「認可方式」

認可タイプ

名前付き認可方式リストは、指定される認可の種類によって変わります。

ユーザ別に固有のセキュリティ ポリシーを適用する認可をイネーブルにする方式リストを作成するには、**auth-proxy** キーワードを使用します。認証プロキシのコンフィギュレーション マニュアルの詳細については、「関連資料」（P.14）を参照してください。

すべてのネットワーク関連サービス要求（SLIP、PPP、PPP NCP、ARAP などのプロトコル）について認可をイネーブルにする方式リストを作成するには、**network** キーワードを使用します。

ユーザが EXEC シェルを実行できるかどうかを認可で決定できるように方式リストを作成するには、**exec** キーワードを使用します。

特定の特権レベルに関連付けられた個々の EXEC コマンドについて認可をイネーブルにする方式リストを作成するには、**commands** キーワードを使用します（これによって、0 ～ 15 の指定したコマンド レベルに関連付けられたすべてのコマンドを認可できます）。

リバース Telnet 機能について認可をイネーブルにする方式リストを作成するには、**reverse-access** キーワードを使用します。

認可方式

ネットワーク アクセス サーバから TACACS+ セキュリティ サーバを介して認可情報を要求するには、**group tacacs+** *method* キーワードを指定して **aaa authorization** コマンドを使用します。TACACS+ セキュリティ サーバを使用して認可を設定する詳細な方法については、「Configuring TACACS+」フィーチャ モジュールを参照してください。TACACS+ サーバが、PPP や ARA などのネットワーク サービスの使用を認可できるようにする例については、「TACACS+ 認可：例」（P.10）を参照してください。

ユーザが認証済みであれば、要求した機能へのアクセスを許可するには、**if-authenticated** *method* キーワードを指定して **aaa authorization** コマンドを使用します。この方式を選択する場合、すべての要求した機能は、認証済みユーザに自動的に許可されます。

特定のインターフェイスまたは回線から認可を実行しない方がよい場合があります。指定した回線またはインターフェイスで認可動作を停止するには、**none** *method* キーワードを使用します。この方式を選択すると、すべてのアクションについて認可はディセーブルになります。

ローカル認可を選択するには（つまり、ルータまたはアクセス サーバがローカル ユーザ データベースに問い合わせて、ユーザが使用可能な機能を決定する場合）、**local** *method* キーワードを指定して **aaa authorization** コマンドを使用します。ローカル認可に関連する機能は、**username** グローバル コンフィギュレーション コマンドを使用して定義します。許可されている機能のリストについては、「Configuring Authentication」を参照してください。

ネットワーク アクセス サーバから LDAP セキュリティ サーバを介して認可を要求するには、**ldap** *method* キーワードを使用します。RADIUS セキュリティ サーバを使用して認可を設定する詳細な方法については、「Configuring RADIUS」フィーチャ モジュールを参照してください。

ネットワーク アクセス サーバから RADIUS セキュリティ サーバを介して認可を要求するには、**radius** *method* キーワードを使用します。RADIUS セキュリティ サーバを使用して認可を設定する詳細な方法については、「Configuring RADIUS」フィーチャ モジュールを参照してください。

ネットワーク アクセス サーバから RADIUS セキュリティ サーバを介して認可情報を要求するには、**group** *radius* method キーワードを指定して **aaa authorization** コマンドを使用します。RADIUS セキュリティ サーバを使用して認可を設定する詳細な方法については、「Configuring RADIUS」フィーチャ モジュールを参照してください。RADIUS サーバがサービスを認可できるようにする例については、「RADIUS 認可：例」（P.11）を参照してください。

（注） SLIP の認可方式リストは、関連インターフェイスで PPP に設定されているすべての方式に従います。特定のインターフェイスに定義および適用されるリストがない場合（または PPP 設定が指定されていない場合）、認可のデフォルト設定が適用されます。

グローバル コンフィギュレーション コマンドの認可のディセーブル化

commands キーワードを指定して **aaa authorization** コマンドを使用すると、その特権レベルに関連付けられているすべての EXEC モード コマンド（グローバル コンフィギュレーション コマンドを含む）に対して認可が試行されます。一部の EXEC レベル コマンドと同じコンフィギュレーション コマンドもあるため、認可プロセスが混乱する可能性があります。**no aaa authorization config-commands** を使用すると、ネットワーク アクセス サーバがコンフィギュレーション コマンド認可の試行を停止します。

すべてのグローバル コンフィギュレーション コマンドについて AAA 認可をディセーブルにするには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
Router(config)# **no aaa authorization config-commands**	すべてのグローバル コンフィギュレーション コマンドについて認可をディセーブルにします。

リバース Telnet の認可の設定

Telnet は、リモート ターミナル接続に使用される標準ターミナル エミュレーション プロトコルです。通常、ネットワーク アクセス サーバにログインし、そのネットワーク アクセス サーバから Telnet を使用して他のネットワーク デバイスにアクセスします。ただし、場合によっては、リバース Telnet セッションを確立する必要があります。リバース Telnet セッションでは、反対方向の Telnet 接続（つまり、ネットワーク内部から、ネットワーク周辺にあるネットワーク アクセス サーバに対する接続）が確立されます。その接続によって、ネットワーク アクセス サーバに接続しているモデムや他のデバイスへのアクセスを取得します。リバース Telnet は、ユーザがネットワーク アクセス サーバに接続されているモデム ポートに Telnet を送信できるようにすることで、ユーザにダイヤルアウト機能を提供します。

リバース Telnet を介してアクセスできるポートのアクセス権を制御することが重要です。適切に制御しないと、たとえば、不正ユーザがモデムに自由にアクセスし、着信コールをトラップして迂回させたり、不正な宛先にコールを送信したりする可能性があります。

リバース Telnet 時の認証は、Telnet 用の標準の AAA ログイン手順を介して実行されます。通常、Telnet またはリバース Telnet セッションを確立するには、ユーザはユーザ名とパスワードを指定する必要があります。リバース Telnet 認可は、認証に加えて認可を必須にすることで、追加（オプション）レベルのセキュリティを提供します。リバース Telnet 認可をイネーブルにすることで、標準の Telnet ログイン手順を介してユーザ認証を完了した後に、RADIUS または TACACS+ を使用して、そのユーザが非同期ポートにリバース Telnet アクセスを実行できるかどうかを認可できます。

リバース Telnet 認可には次の利点があります。

- リバース Telnet アクティビティを実行しているユーザに、リバース Telnet を使用して特定の非同期ポートにアクセスする権限を付与することで、追加レベルの保護を実現しています。
- リバース Telnet 認可を管理できる（アクセス リスト以外の）代替方式があります。

ネットワーク アクセス サーバが TACACS+ または RADIUS サーバからの認可情報を要求するように設定してから、ユーザによるリバース Telnet セッションの確立を許可するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
Router(config)# **aaa authorization reverse-access** *method1* [*method2 ...*]	ネットワーク アクセス サーバが認可情報を要求するように設定してから、ユーザによるリバース Telnet セッションの確立を許可します。

この機能によって、ネットワーク アクセス サーバは、セキュリティ サーバ（RADIUS または TACACS+）からリバース Telnet 認可情報を要求できます。セキュリティ サーバ上のユーザに固有のリバース Telnet 特権を設定する必要があります。

認可設定の例

ここでは、認可設定の例を紹介します。

名前付き方式リストの設定：例

次に、RADIUS サーバから AAA サービスを提供するために Cisco AS5300（AAA および RADIUS セキュリティ サーバとの通信で有効）を設定する例を示します。RADIUS サーバが応答に失敗すると、認証情報と認可情報についてローカル データベースへの照会が行われ、アカウンティング サービスは TACACS+ サーバによって処理されます。

```
aaa new-model
aaa authentication login admins local
aaa authentication ppp dialins group radius local
aaa authorization network scoobee group radius local
aaa accounting network charley start-stop group radius

username root password ALongPassword

radius-server host alcatraz
radius-server key myRaDiUSpassWoRd

interface group-async 1
 group-range 1 16
 encapsulation ppp
 ppp authentication chap dialins
 ppp authorization scoobee
 ppp accounting charley

line 1 16
 autoselect ppp
 autoselect during-login
 login authentication admins
 modem dialin
```

この RADIUS AAA 設定のサンプル行は、次のように定義されます。

- **aaa new-model** コマンドは、AAA ネットワーク セキュリティ サービスをイネーブルにします。
- **aaa authentication login admins local** コマンドは、ログイン認証の方式リスト「admins」を定義します。
- **aaa authentication ppp dialins group radius local** コマンドで、RADIUS 認証を示す認証方式リスト「dialins」を定義します。次に、（RADIUS サーバが応答しない場合）PPP を使用するシリアル回線にはローカル認証が使用されます。
- **aaa authorization network scoobee group radius local** コマンドで、「scoobee」というネットワーク認可方式リストを定義します。その際、PPP を使用するシリアル回線に RADIUS 認可を使用するように指定します。RADIUS サーバが応答に失敗すると、ローカル ネットワークの認可が実行されます。
- **aaa accounting network charley start-stop group radius** コマンドで、charley というネットワーク アカウンティング方式リストを定義します。その際、PPP を使用するシリアル回線に RADIUS アカウンティング サービス（この場合、特定のイベントに対する開始レコードと終了イベント）を使用するように指定します。

- **username** コマンドはユーザ名とパスワードを定義します。これらの情報は、PPP Password Authentication Protocol（PAP; パスワード認証プロトコル）認証での発信元の身元確認に使用されます。
- **radius-server host** コマンドは RADIUS サーバ ホストの名前を定義します。
- **radius-server key** コマンドはネットワーク アクセス サーバと RADIUS サーバ ホスト間の共有秘密テキスト ストリングを定義します。
- **interface group-async** コマンドは非同期インターフェイス グループを選択して定義します。
- **group-range** コマンドはインターフェイス グループのメンバの非同期インターフェイスを定義します。
- **encapsulation ppp** コマンドは指定のインターフェイスに使用される PPP をカプセル化方式として設定します。
- **ppp authentication chap dialins** コマンドは ppp 認証方式として Challenge Handshake Authentication Protocol（CHAP; チャレンジ ハンドシェーク認証プロトコル）を選択し、特定のインターフェイスに「ダイヤルイン」方式リストを適用します。
- **ppp authorization scoobee** コマンドによって、scoobee ネットワーク認可方式リストは指定したインターフェイスに適用されます。
- **ppp accounting charley** コマンドによって、charley ネットワーク アカウンティング方式リストは指定したインターフェイスに適用されます。
- **line** コマンドはコンフィギュレーション モードをグローバル コンフィギュレーションからライン コンフィギュレーションに切り替え、設定対象の回線を指定します。
- **autoselect ppp** コマンドは、選択した回線上で PPP セッションを自動的に開始できるように Cisco IOS ソフトウェアを設定します。
- **autoselect during-login** コマンドを使用して、Return キー押さずにユーザ名およびパスワードのプロンプトを表示します。ユーザがログインすると、autoselect 機能（この場合は PPP）が開始します。
- **login authentication admins** コマンドは、ログイン認証の admins 方式リストを適用します。
- **modem dialin** コマンドは選択した回線に接続されているモデムを設定し、着信コールだけを受け入れるようにします。

TACACS+ 認可：例

次に、TACACS+ サーバを使用して、PPP や ARA などのネットワーク サービスの使用を認可する例を示します。TACACS+ サーバが使用不能の場合、または認可プロセス中にエラーが発生した場合、フォールバック方式（none）はすべての認可要求を許可することです。

```
aaa authorization network default group tacacs+ none
```

次に、TACACS+ を使用してネットワークの認可を許可する例を示します。

```
aaa authorization network default group tacacs+
```

次に、同じ認可を提供し、mci と att というアドレス プールも作成する例を示します。

```
aaa authorization network default group tacacs+
ip address-pool local
ip local-pool mci 172.16.0.1 172.16.0.255
ip local-pool att 172.17.0.1 172.17.0.255
```

これらのアドレス プールは、TACACS デーモンによって選択できます。デーモンの設定例を次に示します。

```
user = mci_customer1 {
    login = cleartext "some password"
    service = ppp protocol = ip {
        addr-pool=mci
    }
}

user = att_customer1 {
    login = cleartext "some other password"
    service = ppp protocol = ip {
        addr-pool=att
     }
```

RADIUS 認可：例

次に、RADIUS を使用して認可を行うようにルータを設定する方法の例を示します。

```
aaa new-model
aaa authorization exec default group radius if-authenticated
aaa authorization network default group radius
radius-server host ip
radius-server key
```

この RADIUS 認可設定のサンプル行は、次のように定義されます。

- **aaa authorization exec default group radius if-authenticated** コマンドで、ネットワーク アクセス サーバが RADIUS サーバに接続して、ユーザのログイン時にユーザが EXEC シェルを起動する権限があるかどうかを決定するように設定します。ユーザが適切に認証されていて、ネットワーク アクセス サーバが RADIUS サーバに接続するときにエラーが発生する場合、フォールバック方式は CLI の起動を許可することです。

  返される RADIUS 情報を使用して、その接続に適用される autocommand または接続アクセス リストを指定できます。

- **aaa authorization network default group radius** コマンドで、RADIUS を回するネットワーク認可を設定します。この操作は、アドレス割り当ての管理、アクセス リストのアプリケーション、および他の多様なユーザ別の数量に使用できます。

（注） この例ではフォールバック方式を指定していないため、何らかの理由で認可に失敗すると、RADIUS サーバからの応答はありません。

LDAP 認可：例

次に、LDAP を使用して認可を行うようにルータを設定する方法の例を示します。

```
aaa new-model
aaa authorization exec default group ldap if-authenticated
aaa authorization network default group ldap
```

この RADIUS 認可設定のサンプル行は、次のように定義されます。

- **aaa authorization exec default group ldap if-authenticated** コマンドで、ネットワーク アクセス サーバが LDAP サーバに接続して、ユーザのログイン時にユーザが EXEC シェルを起動する権限があるかどうかを決定するように設定します。ユーザが適切に認証されていて、ネットワーク アクセス サーバが LDAP サーバに接続するときにエラーが発生する場合、フォールバック方式は CLI の起動を許可することです。

返される LDAP 情報を使用して、その接続に適用される autocommand または接続アクセス リストを指定できます。

aaa authorization network default group ldap コマンドで、LDAP を回するネットワーク認可を設定します。このコマンドは、アドレス割り当ての管理、アクセス リストのアプリケーション、および他の多様なユーザ別の数量に使用できます。

リバース Telnet 認可：例

次に、ネットワーク アクセス サーバが TACACS+ セキュリティ サーバから認可情報を要求してから、ユーザによるリバース Telnet セッションの確立を許可する例を示します。

```
aaa new-model
aaa authentication login default group tacacs+
aaa authorization reverse-access default group tacacs+
!
tacacs-server host 172.31.255.0
tacacs-server timeout 90
tacacs-server key goaway
```

この TACACS+ リバース Telnet 認可設定のサンプル行は、次のように定義されます。

- **aaa new-model** コマンドは AAA をイネーブルにします。
- **aaa authentication login default group tacacs+** コマンドで、ログイン時のユーザ認証のデフォルト方式として TACACS+ を指定します。
- リバース Telnet セッションを確立しようとしているときに、**aaa authorization reverse-access default group tacacs+** コマンドで、ユーザ認可の方式として TACACS+ を指定します。
- **tacacs-server host** コマンドで、TACACS+ サーバを指定します。
- **tacacs-server timeout** コマンドで、ネットワーク アクセス サーバが TACACS+ サーバの応答を待機する期間を設定します。
- **tacacs-server key** コマンドで、ネットワーク アクセス サーバと TACACS+ デーモン間のすべての TACACS+ 通信に使用される暗号化キーを定義します。

次に、ネットワーク アクセス サーバ「maple」上のポート tty2、およびネットワーク アクセス サーバ「oak」上のポート tty5 に対するリバース Telnet アクセス権をユーザ pat に付与する汎用の TACACS+ サーバを設定する例を示します。

```
user = pat
  login = cleartext lab
  service = raccess {
    port#1 = maple/tty2
    port#2 = oak/tty5
```

（注） この例では、「maple」と「oak」には、DNS 名またはエイリアスではなく、ネットワーク アクセス サーバのホスト名が設定されています。

次に、TACACS+ サーバ（CiscoSecure）を設定して、ユーザ pat にリバース Telnet アクセス権を付与する例を示します。

```
user = pat
profile_id = 90
profile_cycle = 1
member = Tacacs_Users
service=shell {
default cmd=permit
}
```

```
service=raccess {
allow ”c2511e0” ”tty1” ”.*”
refuse ”.*” ”.*” ”.*”
password = clear “goaway”
```

（注） CiscoSecure は、バージョン 2.1（*x*）～ バージョン 2.2（1）のコマンドライン インターフェイスを使用して、リバース Telnet だけをサポートしています。

空の「service=raccess {}」句は、リバース Telnet のネットワーク アクセス サーバ ポートに対して無条件のアクセス権をユーザに許可しています。「service=raccess」句が存在しない場合、ユーザはリバース Telnet のすべてのポートに対してアクセスを拒否されます。

次に、ネットワーク アクセス サーバが RADIUS セキュリティ サーバから認可を要求してから、ユーザによるリバース Telnet セッションの確立を許可する例を示します。

```
aaa new-model
aaa authentication login default group radius
aaa authorization reverse-access default group radius
!
radius-server host 172.31.255.0
radius-server key go away
auth-port 1645 acct-port 1646
```

この RADIUS リバース Telnet 認可設定のサンプル行は、次のように定義されます。

- **aaa new-model** コマンドは AAA をイネーブルにします。
- **aaa authentication login default group radius** コマンドで、ログイン時のユーザ認証のデフォルト方式として RADIUS を指定します。
- リバース Telnet セッションを確立しようとしているときに、**aaa authorization reverse-access default group radius** コマンドで、ユーザ認可の方式として RADIUS を指定します。
- **radius-server host** コマンドで、RADIUS サーバを指定します。
- **radius-server key** コマンドで、ネットワーク アクセス サーバと RADIUS デーモン間のすべての RADIUS 通信に使用される暗号化キーを定義します。

次に、ネットワーク アクセス サーバ「maple」上のポート tty2 で、ユーザ「pat」にリバース Telnet アクセス権を付与する RADIUS サーバに要求を送信する例を示します。

```
Username = ”pat”
Password = ”goaway”
User-Service-Type = Shell-User
cisco-avpair = ”raccess:port#1=maple/tty2”
```

構文「raccess:port=any/any」で、リバース Telnet のネットワーク アクセス サーバ ポートに対して無条件のアクセス権をユーザに許可します。「raccess:port={*nasname*}/{*tty number*}」句がユーザ プロファイルにない場合、ユーザはすべてのポートでリバース Telnet へのアクセスを拒否されます。

その他の参考資料

ここでは、認可機能に関する関連資料について説明します。

関連資料

内容	参照先
認可コマンド	『*Cisco IOS Security Command Reference*』
RADIUS	「Configuring RADIUS」フィーチャ モジュール
LDAP	「Configuring RADIUS」フィーチャ モジュール
RADIUS アトリビュート	「RADIUS Attributes Overview and RADIUS IETF Attributes」フィーチャ モジュール
TACACS+	「Configuring TACACS+」フィーチャ モジュール
TACACS+ アトリビュート値ペア	「TACACS+ Attribute-Value Pairs」フィーチャ モジュール
認証	「Configuring Authentication」フィーチャ モジュール
認証プロキシ	「Configuring Authentication Proxy」フィーチャ モジュール

規格

規格	タイトル
この機能がサポートする新しい規格または変更された規格はありません。また、この機能による既存規格のサポートに変更はありません。	—

MIB

MIB	MIB リンク
なし	選択したプラットフォーム、Cisco IOS リリース、および機能セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
この機能によってサポートされる新しい RFC や変更された RFC はありません。	—

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

認可の設定に関する機能情報

表 1 に、この機能のリリース履歴を示します。

ご使用の Cisco IOS ソフトウェア リリースによっては、コマンドの中に一部使用できないものがあります。特定のコマンドに関するリリース情報については、コマンド リファレンス マニュアルを参照してください。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、特定のソフトウェア リリース、機能セット、またはプラットフォームをサポートする Cisco IOS ソフトウェア イメージおよび Catalyst OS ソフトウェア イメージを確認できます。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp からアクセスできます。Cisco.com のアカウントは必要ありません。

（注） 表 1 には、一連の Cisco IOS ソフトウェア リリースのうち、特定の機能が初めて導入された Cisco IOS ソフトウェア リリースだけが記載されています。特に明記していないかぎり、その機能は、一連の Cisco IOS ソフトウェア リリースの以降のリリースでもサポートされます。

表 1　　認可の設定に関する機能情報

機能名	リリース	機能情報
認可の設定	10.0 Cisco IOS XE Release 2.1	AAA 認可機能を使用して、ユーザができることとできないことを定義します。AAA 認可をイネーブルにすると、ネットワーク アクセス サーバはユーザのプロファイルから取得した情報を使用して、ユーザの設定を設定します。このプロファイルは、ローカル ユーザ データベースまたはセキュリティ サーバにあります。認可が完了すると、ユーザ プロファイルの情報で許可されているサービスであれば、ユーザは要求したサービスに対するアクセス権を付与されます。 この機能は、Cisco IOS Release 10.0 で導入されました。 この機能は、Cisco ASR 1000 シリーズ ルータで導入されました。
LDAP の Active Directory との統合	15.1(1)T	LDAP はディレクトリへのアクセスに使用される標準ベースのプロトコルです。RADIUS に類似したクライアント サーバ モデルをベースとしています。LDAP はシスコ デバイス上で稼動し、ユーザ認証およびネットワーク サービス アクセスに関するすべての情報を保持する中央の LDAP サーバへ認証要求を送信します。 この機能は、AAA の認証および認可のサポートを提供します。 コマンド **aaa authorization** が変更されました。

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。