認可の設定

AAA 認可を使用すると、ユーザーが利用できるサービスを制限できます。AAA 認可をイネーブルにすると、ネットワーク アクセス サーバーはユーザーのプロファイルから取得した情報を使用して、ユーザーの設定を設定します。このプロファイルは、ローカル ユーザー データベースまたはセキュリティ サーバーにあります。認可が完了すると、ユーザー 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、ユーザー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。

AAA 認可の前提条件

名前付き方式リストを使用して認証を設定する前に、まず、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。AAA 認証の設定方法については、「認証の設定」モジュールを参照してください。
- RADIUS または TACACS+ 認可を発行している場合、RADIUS または TACACS+ セキュリティ サーバーの特性を定義します。シスコのネットワーク アクセス サーバーを設定して RADIUS セキュリティ サーバーと通信する方法の詳細については、「RADIUS の設定」の章を参照してください。シスコのネットワーク アクセス サーバーを設定して TACACS+ セキュリティ サーバーと通信する方法の詳細については、「TACACS+ の設定」モジュールを参照してください。

- ローカル認可を発行している場合、**username** コマンドを使用して、特定のユーザーに関連付けられている権限を定義します。**username** コマンドの詳細については、『*Cisco IOS Security Command Reference*』を参照してください。

認可の設定の概要

認可の名前付き方式リスト

許可方式リストによって、許可の実行方法とこれらの方式の実行順序が定義されます。方式リストは、順に照会する認可方式（RADIUS または TACACS+ など）を記述した指定リストです。方式リストを使用すると、許可に使用するセキュリティプロトコルを1つ以上指定できるため、最初の方式が失敗した場合のバックアップシステムを確保できます。Cisco IOS XE 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ーを許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、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 XE 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、リストの次の許可方式が試行されます。このサイクルの任意の時点で許可が失敗した場合（つまり、セキュリティサーバーまたはローカル ユーザー名データベースからユーザー サービスの拒否応答が返される場合）、許可プロセスは停止し、その他の許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。

- Commands：ユーザが実行する EXEC モード コマンドに適用されます。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属性に適用されます。
- Network：ネットワーク接続に適用されます。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。

方式の指定リストを作成すると、指定した許可タイプに対して特定の許可方式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）です。名前付き方式リストを指定せずに、特定の許可タイプ用の **aaa authorization** コマンドが発行されると、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いて、すべてのインターフェイスまたは回線にデフォルトの方式リストが自動的に適用されます。（定義

済みの方式リストは、デフォルトの方式リストに優先します）。デフォルトの方式リストが定義されていない場合、デフォルトでローカル認可が実行されます。

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、属性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。属性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ーは、**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、たとえばユーザーに固有の権限を許可します。ローカルデータベースを介して制御できるのは、一部の機能だけです。
- 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、属性を関連付けることでユーザーに固有の権限を定義します。属性は適切なユーザーとともにRADIUSサーバー上のデータベースに保存されます。

（注） CSCuc32663 では、パスワードおよび認可ログは、TACACS+、LDAP、または RADIUS セキュリティ サーバーへ送信される前にマスクされます。マスクされていない情報を TACACS+、LDAP または RADIUS セキュリティサーバーに送信するには、**aaa authorization commands visible-keys** コマンドを使用します。

認可方式

ネットワークアクセスサーバーから TACACS+ セキュリティサーバー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 サーバーを使用して認可を設定する詳細な方法については、「TACACS+ の設定」の章を参照してください。TACACS+ サーバーが、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 認可の例」を参照してください。

ユーザー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、認証済みユーザー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たくない場合があります。指定した回線またはインターフェイスで許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。

ローカル許可を選択するには（つまり、ルータまたはアクセスサーバーがローカルユーザーデータベースに問い合わせて、ユーザー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。ローカル許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、「認証の設定」の章を参照してください。

ネットワークアクセスサーバーからRADIUSセキュリティサーバーを介して許可を要求するには、**radius** *method* キーワードを使用します。RADIUS セキュリティ サーバーを使用して認可を設定する詳細な方法については、「RADIUS の設定」の章を参照してください。

ネットワークアクセスサーバーからRADIUSセキュリティサーバーを介して許可を要求するには、**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 サーバーを使用して認可を設定する詳細な方法については、「RADIUSの設定」の章を参照してください。RADIUSサーバーがサービスを認可できるようにする例については、「RADIUS 認可の例」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。

方式リストとサーバ グループ

サーバー グループは、方式リストに使用する既存の RADIUS または TACACS+ サーバー ホストをグループ化する方法の 1 つです。次の図に、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。

サーバー グループを使用して、設定したサーバー 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、サーバーグループを使用すると、R1およびR2を別のサーバーグループとして定義し、T1およびT2を別のサーバーグループとして定義できます。つまり、R1 と T1 を方式リストに指定できるか、または R2 と T2 を方式リストに指定できます。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 サーバー上にある異なる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 サーバーが試行します（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）。

サーバー グループの設定および DNIS 番号に基づくサーバー グループの設定の詳細については、「RADIUS の設定」または「TACACS+ の設定」の章を参照してください。

AAA 認可タイプ

Cisco IOS XE ソフトウェアは、5 種類の認可をサポートしています。

- Commands：ユーザが実行する EXEC モード コマンドに適用されます。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属性に適用されます。
- Network：ネットワーク接続に適用されます。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。

承認タイプ

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。

ユーザー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。認証プロキシ機能の詳細については、このガイドの「Traffic Filtering and Firewalls」の部の「Configuring Authentication Proxy」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）について認可を有効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。

ユーザーが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有効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。これにより、指定されたコマンド レベル（0 ～ 15）に関連付けられている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有効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。

Cisco IOS XE ソフトウェアでサポートされている認可のタイプの詳細については、「AAA 認可タイプ」を参照してください。

認可の属性値ペア

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

サポートされる RADIUS 属性のリストについては、「RADIUS 属性の概要および RADIUS IETF 属性」の章を参照してください。サポートされる TACACS+ の AV ペアのリストについては、「TACACS+ の設定」の章を参照してください。

認可の設定方法

この章のコマンドを使用した認可の設定例については、「認可の設定例」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、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。

手順の概要

1. Router(config)# **aaa authorization** {**auth-proxy** | **network** | **exec** | **commands** *level* | **reverse-access** | **configuration** | **ipmobile**} {**default** | *list-name*} [*method1* [*method2...*]]
2. 次のいずれかを実行します。
   - Router(config)# **line** [**aux** | **console** | **tty** | **vty**] *line-number* [*ending-line-number*]
   -
   -
   - Router(config)# **interface** *interface-type interface-number*
3. 次のいずれかを実行します。
   - Router(config-line)# **authorization**{**arap** | **commands** *level* | **exec** | **reverse-access**} {**default** | *list-name*}
   -
   -
   - Router(config-line)# **ppp authorization**{**default** | *list-name*}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	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 2	次のいずれかを実行します。 • Router(config)# **line** [**aux** | **console** | **tty** | **vty**] *line-number* [*ending-line-number*] • • • 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 3	次のいずれかを実行します。 • Router(config-line)# **authorization**{**arap** | **commands** *level* | **exec** | **reverse-access**} {**default** | *list-name*} • • • 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。

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）に対して許可が試行されます。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 サーバー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
`Device(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。

コンソール上で 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。

（注） デフォルトでコンソールの AAA 認可はディセーブルです。コンソールで AAA 許可が有効になっている場合は、AAA の設定段階で **no aaa authorization console** コマンドを設定して無効にします。ユーザー認証用のコンソールでは AAA をディセーブルにする必要があります。

コマンド	目的
`Device(config)# no aaa authorization console`	コンソールでの認証を無効にします。

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 サーバーに（主にダイヤルアップ接続経由で）ログインし、Telnet を使用してそのネットワーク アクセス サーバーから他のネットワーク 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 サーバーに対する接続）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 サーバー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、ユーザーがネットワーク アクセス サーバー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、ユーザー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、不正ユーザー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、ユーザーはユーザー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（任意）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ー認証を完了した後に、RADIUS または TACACS+ を使用して、そのユーザー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ーに、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 サーバーが TACACS+ または RADIUS サーバーからの認可情報を要求するように設定してから、ユーザーによるリバース 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 サーバーが認可情報を要求するように設定してから、ユーザーによるリバース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 サーバーは、セキュリティ サーバー（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 サーバー上のユーザーに固有のリバース Telnet 特権を設定する必要があります。

認可設定の例

TACACS 認可の例

次に、TACACS+ サーバーを使用して、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+ サーバーが使用不能の場合、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 認可の例

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ーが RADIUS サーバーに接続して、ユーザーのログイン時にユーザーが 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。ネットワークアクセスサーバーが RADIUS サーバーに接続するときにエラーが発生した場合、フォールバック方式は、ユーザーが適切に認証されていると CLI の起動を許可します。

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** コマンドにより、RADIUS を介するネットワーク許可を設定します。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ー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 サーバーからの応答はありません。

リバース Telnet 認可の例

次に、ネットワーク アクセス サーバーが TACACS+ セキュリティ サーバーから認可情報を要求してから、ユーザーによるリバース 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 を有効にします。
- **aaa authentication login default group tacacs+** コマンドで、ログイン時のユーザー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、ユーザー認可の方式として TACACS+ を指定します。
- **tacacs-server host** コマンドで、TACACS+ サーバーを指定します。

- **tacacs-server timeout** コマンドで、ネットワークアクセスサーバーが TACACS+ サーバー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ーと TACACS+ デーモン間のすべての TACACS+ 通信に使用される暗号キーを定義します。

次に、ネットワーク アクセス サーバー「maple」上のポート tty2、およびネットワーク アクセス サーバー「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ー pat に付与する汎用の TACACS+ サーバー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 サーバーのホスト名が設定されています。

次に、TACACS+ サーバー（CiscoSecure）を設定して、ユーザー 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 サーバー ポートに対して無条件のアクセス権をユーザーに許可しています。「service=raccess」句が存在しない場合、ユーザーはリバース Telnet のすべてのポートに対してアクセスを拒否されます。

TACACS+の設定の詳細については、「TACACS+の設定」の章を参照してください。CiscoSecure の設定の詳細については、『*CiscoSecure Access Control Server User Guide*』の version 2.1(2) 以降を参照してください。

次に、ネットワーク アクセス サーバーが RADIUS セキュリティ サーバーから認可を要求してから、ユーザーによるリバース 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 を有効にします。
- **aaa authentication login default group radius** コマンドで、ログイン時のユーザー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、ユーザー認可の方式として RADIUS を指定します。
- **radius-server host** コマンドで、RADIUS サーバーを指定します。
- **radius-server key** コマンドで、ネットワークアクセスサーバーと RADIUS デーモン間のすべての RADIUS 通信に使用される暗号キーを定義します。

次に、ネットワーク アクセス サーバー「maple」上のポート tty2 で、ユーザー「pat」にリバース Telnet アクセス権を付与する RADIUS サーバー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 サーバー ポートに対して無条件のアクセス権をユーザーに許可します。「raccess:port={*nasname* }/{*tty number* }」句がユーザー プロファイルにない場合、ユーザー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。

RADIUS の設定の詳細については、「RADIUS の設定」の章を参照してください。

その他の参考資料

関連資料

関連項目	マニュアル タイトル
セキュリティ コマンド	『Cisco IOS Security Command Reference』
IPSec	IPsec 仮想トンネル インターフェイス機能のドキュメント

MIB

MIB	MIB のリンク
なし	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ 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

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。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。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

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

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
AAA 認可およびアカウンティングの名前付き方式リスト	Cisco IOS XE Release 2.1	許可方式リストによって、許可の実行方法とこれらの方式の実行順序が定義されます。方式リストは、順に照会する認可方式（RADIUS または TACACS+ など）を記述した指定リストです。 Cisco IOS XE Release 2.1 では、Cisco ASR 1000 シリーズ Aggregation Services Router にこの機能が実装されました。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。