TACACS の設定

この章では、詳細なアカウンティング情報を提供し、認証および許可プロセスを柔軟に管理できるようにするために、TACACS+ をイネーブルにして設定する方法について説明します。TACACS+は、AAA を介して実装され、AAA コマンドを使用してのみイネーブルにできます。

TACACS に関する情報

TACACS+は、ユーザーによるルータまたはネットワーク アクセス サーバーへのアクセス試行の集中的な確認を可能にするセキュリティアプリケーションです。TACACS+ サービスは、通常 UNIX または Windows NT ワークステーション上で動作する TACACS+ デーモンのデータベースで管理されます。ネットワーク アクセス サーバーに設定した TACACS+ 機能を使用可能にするには、TACACS+ サーバーにアクセスして TACACS+ サーバーを設定しておく必要があります。

TACACS+ では、独立したモジュラ型の認証、許可、アカウンティング機能が提供されます。TACACS+ を使用すると、単一のアクセス コントロール サーバー（TACACS+ デーモン）で、各サービス（認証、許可、アカウンティング）を個別に提供できます。各サービスを固有のデータベースに結合し、デーモンの機能に応じてそのサーバーまたはネットワークで使用できる他のサービスを提供できます。

TACACS+の目的は、単一の管理サービスから複数のネットワーク アクセス ポイントを管理する方法を提供することです。アクセス サーバーおよびルーティングのシスコ ファミリおよび（ルータとアクセス サーバー両方の）Cisco IOS および Cisco IOS XE ユーザー インターフェイスは、ネットワーク アクセス サーバーにすることができます。

ネットワーク アクセス ポイントによって、従来の「低機能な」端末、端末エミュレータ、ワークステーション、パーソナル コンピュータ（PC）、およびルータと、適切なアダプタ（たとえば、モデムまたは ISDN アダプタ）を併用して、Point-to-Point Protocol（PPP）、Serial Line Internet Protocol（SLIP）、Compressed SLIP（CSLIP）、または AppleTalk Remote Access（ARA）

プロトコルを使用する通信が可能になります。つまり、ネットワーク アクセス サーバーは、単一のユーザー、ネットワークまたはサブネットワーク、および相互接続したネットワークに対して、接続を提供できます。ネットワーク アクセス サーバーを介して接続されているエンティティは、ネットワーク アクセス クライアントと呼ばれます。たとえば、音声グレードの回路で PPP を実行する PC は、ネットワーク アクセス クライアントです。AAA セキュリティ サービスを介して管理される TACACS+ は、次のサービスを提供できます。

- 認証：ログインとパスワードのダイアログ、チャレンジ/レスポンス、メッセージングのサポートを介して、認証を詳細に制御できます。

認証機能には、ユーザーに任意のダイアログを実行する機能があります（たとえば、ログインとパスワードの指定後に、自宅住所、母親の旧姓、サービス タイプ、社会保険番号などの複数の質問をユーザーに試行する機能）。さらに、TACACS+ 認証サービスは、ユーザー画面へのメッセージ送信をサポートします。たとえば、会社のパスワード有効期間ポリシーに従い、パスワードの変更の必要があることをユーザーに通知することもできます。

- 認可：autocommand、アクセス コントロール、セッション期間、プロトコル サポートの設定といった、ユーザー セッション時のユーザー機能についてきめ細かく制御します。また、TACACS+ 認可機能を使用して、ユーザーが実行できるコマンドを制限することもできます。
- アカウンティング：課金、監査、およびレポートに使用する情報を収集して TACACS+ デーモンに送信します。ネットワークの管理者は、アカウンティング機能を使用して、セキュリティ監査のためにユーザの活動状況をトラッキングしたり、ユーザ課金用の情報を提供したりできます。アカウンティング レコードには、ユーザ ID、開始時刻および終了時刻、実行されたコマンド（PPP など）、パケット数、およびバイト数が含まれます。

TACACS+ プロトコルは、ネットワーク アクセス サーバーと TACACS+ デーモンの間に認証機能を提供します。また、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プロトコル交換は暗号化されるため、機密性を確保できます。

TACACS+ デーモン ソフトウェアを実行するシステムで、ネットワーク アクセス サーバーで TACACS+ 機能を使用する必要があります。

独自の TACACS+ ソフトウェアを開発することに関心があるユーザー向けに、シスコでは、TACACS+ プロトコル仕様をドラフトの RFC として使用できるようにしています。

TACACS の動作

ユーザーが TACACS+ を使用してネットワーク アクセス サーバーに対して認証を受けることで、単純な ASCII ログインを試行すると、一般的に、次のプロセスが発生します。

1. 接続が確立すると、ネットワーク アクセス サーバーは TACACS+ デーモンに接続してユーザー名のプロンプトをを取得します。また、そのプロンプトはユーザーに表示されます。ユーザーがユーザー名を入力すると、ネットワーク アクセス サーバーは TACACS+ デーモンに接続し、パスワード プロンプトを取得します。ネットワーク アクセス サーバーはユーザーに対してパスワードプロンプトを表示します。ユーザーがパスワードを入力すると、パスワードは TACACS+ デーモンに送信されます。

（注） TACACS+によって、デーモンとユーザーとの間で対話できるようになり、デーモンはユーザーの認証に必要な情報を取得できるようになります。通常、この処理は、ユーザー名とパスワードの組み合わせのプロンプトを表示することで完了しますが、TACACS+デーモンの制御下で、母親の旧姓など、他のアイテムを含めることができます。

1. ネットワーク アクセス サーバーは、最終的に TACACS+ デーモンから次のいずれかの応答を得ます。
    1. ACCEPT：ユーザーは認証され、サービスを開始できます。認可を必須にするようにネットワーク アクセス サーバーが設定されている場合、この時点で認可が開始されます。
    2. REJECT：ユーザーは認証に失敗しました。ユーザーは以降のアクセスを拒否される可能性があります。または、TACACS+ デーモンに応じてログイン シーケンスを再試行するようにプロンプトが表示されます。
    3. ERROR：認証中のある時点でエラーが発生しました。エラーは、デーモン、またはデーモンとネットワーク アクセス サーバー間のネットワーク接続で発生する可能性があります。ERROR 応答を受信すると、通常、ネットワーク アクセス サーバーはユーザーを認証する代替方式を使用しようとします。
    4. CONTINUE：ユーザーは、さらに認証情報の入力を求められます。
2. PAP ログインは、ASCII ログインに似ていますが、ユーザーによる入力ではなく、PAP プロトコル パケットでユーザー名とパスワードがネットワーク アクセス サーバーに到達するため、ユーザーにはプロンプトが表示されません。PPP CHAP ログインは、原則もにています。

ネットワーク アクセス サーバーで認可をイネーブルにしている場合、認証の後に、ユーザーは追加の認可段階を実行する必要があります。ユーザーは TACACS+ 許可に進む前に、まず TACACS+ 認証を正常に完了する必要があります。

1. TACACS+ の認可が必要な場合も、TACACS+ デーモンに接続します。また、TACACS+ デーモンは、ACCEPT または REJECT 認可応答を返します。ACCEPT 応答が返される場合、この応答には、そのユーザーに関する EXEC または NETWORK セッションを指示するために使用される属性の形式のデータが含まれます。これによって、ユーザーがアクセスできるサービスを判断します。この場合のサービスは次のとおりです。
    1. Telnet、rlogin、ポイントツーポイント プロトコル（PPP）、シリアル ライン インターネット プロトコル（SLIP）、EXEC サービス
    2. 接続パラメータ（ホストまたはクライアントの IP アドレス、アクセス リスト、およびユーザ タイムアウトを含む）

TACACS の設定方法

TACACS+ をサポートするようにルータを設定するには、次のタスクを実行する必要があります。

- **aaa new-model** 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、AAA をイネーブルにします。TACACS+ を使用する予定がある場合、AAA を設定する必要があります。**aaa new-model** コマンドの使用の詳細については、「AAA の概要」の章を参照してください。
- コマンドを使用して、1 つ以上の TACACS+ デーモンの IP アドレスを指定します。 コマンドを使用して、ネットワーク アクセス サーバーと TACACS+ デーモンの間のすべてのやり取りを暗号化するために使用する暗号化キーを指定します。TACACS+デーモンでも、この同じキーを設定する必要があります。
- **aaa authentication** 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、認証に TACACS+ を使用する方式リストを定義します。**aaa authentication** コマンドの使用の詳細については、「認証の設定」の章を参照してください。
- line および interface コマンドを使用して、定義済みの方式リストを多様なインターフェイスに適用します。詳細については、「認証の設定」の章を参照してください。
- 必要に応じて、**aaa authorization** グローバル コマンドを使用して、ネットワーク アクセス サーバーの認可を設定します。回線またはインターフェイスごとに設定できる認証とは異なり、認可は、ネットワーク アクセス サーバー全体のグローバル設定です。**aaa authorization** コマンドの使用の詳細については、「認可の設定」の章を参照してください。
- 必要に応じて、**aaa accounting** コマンドを使用して TACACS+ 接続のアカウンティングをイネーブルにします。**aaa accounting** コマンドの使用の詳細については、「アカウンティングの設定」の章を参照してください。

TACACS サーバー ホストの指定

コマンドを使用すると、TACACS+ サーバーを保守する 1 つまたは複数の IP ホストの名前を指定できます。TACACS+ ソフトウェアは、指定した順序でホストを検索するため、この機能は、希望のデーモン リストを設定する場合に役立ちます。

TACACS+ホストを指定するには、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。

コマンド	目的
`Router(config)# hostname [single-connection] [port integer] [timeout integer] [key string]`	TACACS+ ホストを指定します。

コマンドを使用して、次のオプションも設定できます。

- **single-connection** キーワードを使用して、単一接続を指定します。通信が必要になるたびに、ルータの接続を開き、TCP 接続を閉じるのではなく、single-connection オプションによって、ルータとデーモン間の単一のオープンな接続を保守します。この方法はデーモンが処理できる TACACS 操作数が多くなるため、効率的です。

（注） この処理を有効にするには、デーモンが single-connection モードをサポートする必要があります。サポートしていない場合、ネットワーク アクセス サーバーとデーモン間の接続が動作しなくなるか、不要なエラーを受信します。

- **port** *integer* 引数を使用して、TACACS+ デーモンに接続するときに使用される TCP ポート番号を指定します。デフォルト ポート番号は 49 です。
- **timeout** *integer* 引数を使用して、ルータがタイムアウトしてエラー宣言するまで、デーモンからの応答を待つ期間（秒）を指定します。

（注） コマンドによるタイムアウト値の指定は、このサーバーに関するコマンドで設定されたデフォルトのタイムアウト値よりも優先されます。

- **key** *string* 引数を指定して、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トラフィックを暗号化および復号化するための暗号キーを指定します。

（注） コマンドによる暗号キーの指定は、このサーバーに関するグローバル コンフィギュレーションの コマンドで設定されたデフォルト キーよりも優先されます。

コマンドのパラメータの一部は、 コマンドおよび コマンドによるグローバル設定よりも優先されるため、このコマンドを使用して個別の TACACS+ 接続を一意に設定することで、ネットワークのセキュリティを強化できます。

TACACS 認証キーの設定

グローバル TACACS+ 認証キーおよび暗号化キーを設定するには、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。

コマンド	目的
`Router(config)# key`	TACACS+ デーモンで使用する、一致する暗号キーを設定します。

（注） 暗号化が成功するには、TACACS+ デーモンに同じキーを設定する必要があります。

AAA サーバー グループの設定

AAA サーバー グループを使用するようにルータを設定すると、既存のサーバー ホストをグループ化できます。これによって、設定したサーバーホストのサブセットを選択し、それを特定のサービスに使用できます。サーバー グループは、グローバル サーバー ホスト リストと併せて使用されます。サーバー グループには、選択したサーバー ホストの IP アドレスが一覧表示されます。

サーバー グループには複数のホスト エントリを含めることができます。ただし、各エントリの IP アドレスが一意である必要があります。そのサーバー グループにある異なる 2 つのホストエントリが 1 つのサービス（アカウンティングなど）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、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 TACACS+ 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 グループ名を使用してサーバーホストを定義するには、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。一覧のサーバーは、グローバル コンフィギュレーション モードに存在します。

ステップ 1 Router(config)# *name* [**single-connection**] [**port** *integer*] [**timeout** *integer*] [**key** *string*]

サーバー ホストの IP アドレスを指定および定義してから、AAA サーバー グループを設定します。 コマンドの詳細については、この章の「TACACS サーバー ホストの指定」セクションを参照してください。

ステップ 2 Router(config-if)# **aaa group server**{**radius** | **tacacs+**} *group-name*

グループ名を指定して AAA サーバー グループを定義します。グループのすべてのメンバは、タイプを同じにする必要があります。つまり、RADIUS または TACACS+ です。このコマンドでは、サーバー グループのサブコンフィギュレーション モードにルータを配置します。

ステップ 3 Router(config-sg)# **server** *ip-address* [**auth-port** *port-number*] [**acct-port** *port-number*]

特定の TACACS+ サーバーを定義済みのサーバー グループと関連付けます。**auth-port** *port-number* オプションを使用して、認証専用の UDP ポートを設定します。**acct-port** *port-number* オプションを使用して、アカウンティング専用の UDP ポートを設定します。

AAA サーバー グループの TACACS+ サーバーごとに、このステップを繰り返します。

（注） グループの各サーバーは、 コマンドを使用して事前に定義する必要があります。

DNIS に基づく AAA サーバー グループの選択の設定

Cisco IOS XE ソフトウェアを使用すると、セッションの Dialed Number Identification Service（DNIS）番号に基づき、特定の AAA サーバー グループに対してユーザーを認証できます。すべての電話回線（通常の自宅電話または商用の T1/PRI 回線）を、複数の電話番号と関連付けることができます。DNIS 番号は、ユーザー宛てに発信された番号を示します。

たとえば、複数の顧客で同じ電話番号を共有する場合に、電話を受ける前に発信元を知りたいことがあります。DNIS を使用すると、応答するときに発信元の顧客がわかるため、電話に応答する方法をカスタマイズできます。

ISDN または内部モデムと接続する Cisco ルータは、DNIS 番号を受信できます。この機能を使用すると、顧客ごとに異なる TACACS+ サーバー グループを割り当て可能です（つまり、DNIS 番号ごとに異なる TACACS+ サーバー）。さらに、サーバー グループを使用して、複数の AAA サービスに同じサーバー グループを指定できます。また、各 AAA サービスに個別のサーバー グループを指定できます。

Cisco IOS XE ソフトウェアには、認証サービスとアカウンティング サービスを複数の方法で実装できる柔軟性があります。

- グローバル：AAA サービスは、グローバル コンフィギュレーション アクセス リスト コマンドを使用して定義され、特定のネットワーク アクセス サーバー上のすべてのインターフェイスに、全般的に適用されます。
- インターフェイス別：AAA サービスは、インターフェイス コンフィギュレーション コマンドを使用して定義され、特定のネットワーク アクセス サーバーに設定されているインターフェイスにだけ適用されます。
- DNIS マッピング：DNIS を使用して、AAA サーバーが AAA サービスを提供するように指定します。

複数の AAA コンフィギュレーション方式を同時に設定できるため、シスコでは、AAA サービスを提供するサーバーまたはサーバー グループを決定するために、優先順位を設定しました。優先順位は次のとおりです。

- DNIS 別：AAA サービスを提供するサーバー グループを DNIS によって指定するようネットワーク アクセス サーバーを設定している場合、この方式がその他の AAA 選択方式よりも優先されます。
- インターフェイス別：サーバーから AAA サービスを提供する方法をアクセス リストによって決定するように、インターフェイスごとにネットワーク アクセス サーバーを設定している場合、この方式が他のグローバル コンフィギュレーション AAA アクセス リストよりも優先されます。
- グローバル：セキュリティ サーバーが AAA サービスを提供する方法を決定するために、グローバル AAA アクセス リストを使用してネットワーク アクセス サーバーを設定する場合、この方式には最も低い優先度が使用されます。

（注） DNIS に基づいて AAA サーバー グループの選択を設定する前に、各 AAA サーバー グループに関連付けられたリモートセキュリティ サーバーを設定する必要があります。「TACACS サーバー ホストの指定」および「AAA サーバー グループの設定」を参照してください。

サーバー グループの DNIS に基づいて、特定の AAA サーバー グループを選択するようにルータを設定するには、DNIS マッピングを設定します。DNIS 番号を使用して、サーバー グループをグループ名とマッピングするには、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。

ステップ 1 Router(config)# **aaa dnis map enable**

DNIS マッピングをイネーブルにします。

ステップ 2 Router(config)# **aaa dnis map** *dnis-number* **authentication ppp group** *server-group-name*

DNIS 番号を定義済みの AAA サーバー グループにマッピングします。このサーバー グループのサーバーは、認証に使用されます。

ステップ 3 Router(config)# **aaa dnis map** *dnis-number* **accounting network** [**none** | **start-stop** | **stop-only**] **group** *server-group-name*

DNIS 番号を定義済みの AAA サーバー グループにマッピングします。このサーバー グループのサーバーは、アカウンティングに使用されます。

TACACS 認証の指定

TACACS+ デーモンを指定し、関連する TACACS+ 暗号キーを定義したら、TACACS+ 認証の方式リストを定義する必要があります。TACACS+ 認証は AAA を介して実行されるため、認証方式として TACACS+ を指定して、**aaa authentication** コマンドを発行する必要があります。詳細については、「認証の設定」の章を参照してください。

TACACS 認可の指定

AAA 許可により、ユーザによるネットワーク アクセスを制限するパラメータを設定することができます。TACACS+ を介する許可は、コマンド、ネットワーク接続、および EXEC セッションに適用できます。AAA によって TACACS+ 許可が容易になるため、認可方式として TACACS+ を指定して、**aaa authorization** コマンドを発行する必要があります。詳細については、「認可の設定」の章を参照してください。

TACACS アカウンティングの指定

AAA アカウンティングを使用すると、ユーザーがアクセスしているサービスや、ユーザーが消費しているネットワーク リソース量を追跡できます。AAA によって TACACS+ アカウンティングは容易になるため、アカウンティング方式として TACACS+ を指定して、**aaa accounting** コマンドを発行する必要があります。詳細については、「アカウンティングの設定」の章を参照してください。

TACACS の AV ペア

ネットワーク アクセス サーバーが TACACS+ 認可機能およびアカウンティング機能を実装するには、各ユーザー セッションで TACACS+ の属性と値（AV）ペアを送受信します。サポートされる TACACS+ の AV ペアのリストについては、「TACACS 属性値ペア」の章を参照してください。

TACACS の設定例

TACACS 認証の例

次に、PPP 認証に使用するセキュリティ プロトコルとして TACACS+ を設定する例を示します。

```
aaa new-model
aaa authentication ppp test group tacacs+ local
 10.1.2.3
 key goaway
interface serial 0
 ppp authentication chap pap test
```

前述の設定例の回線は、次のように定義されます。

- **aaa new-model** コマンドは、AAA セキュリティ サービスをイネーブルにします。
- **aaa authentication** コマンドにより、PPP を実行するシリアル インターフェイスに使用する方式リスト「test」を定義します。キーワード **group tacacs+** は、TACACS+ を介して認証を実行することを示します。認証中に TACACS+ から何らかのエラーが返される場合、キーワード **local** は、ネットワーク アクセス サーバ上のローカル データベースを使用して認証が試行されることを示します。
- コマンドにより、TACACS+ デーモンが 10.1.2.3 という IP アドレスを持っていると指定します。 コマンドにより、共有暗号キーを「goaway」に定義します。
- **interface** コマンドで回線を選択します。**ppp authentication** コマンドは、テスト方式リストをこの回線に適用します。

次に、PPP 認証のセキュリティ プロトコルとして TACACS+ を設定する例を示します。ただし、「test」方式リストの代わりに、「default」方式リストが使用されます。

```
aaa new-model
aaa authentication ppp default if-needed group tacacs+ local
 10.1.2.3
 key goaway
interface serial 0
 ppp authentication chap default
```

前述の設定例の回線は、次のように定義されます。

- **aaa new-model** コマンドは、AAA セキュリティ サービスをイネーブルにします。
- **aaa authentication** コマンドにより、PPP を実行するシリアル インターフェイスに使用する方式リスト「default」を定義します。キーワード **default** は、デフォルトですべてのインターフェイスに PPP 認証が適用されることを示します。**if-needed** キーワードは、ユーザが ASCII ログイン手順を介してすでに認証済みの場合には PPP 認証が不要なのでスキップできることを示します。認証が必要な場合、キーワード **group tacacs+** は、TACACS+ を介して認証が実行されることを示します。認証中に TACACS+ から何らかのエラーが返される場合、キーワード **local** は、ネットワーク アクセス サーバ上のローカル データベースを使用して認証が試行されることを示します。
- コマンドにより、TACACS+ デーモンが 10.1.2.3 という IP アドレスを持っていると指定します。 コマンドにより、共有暗号キーを「goaway」に定義します。
- **interface** コマンドで回線を選択します。**ppp authentication** コマンドは、デフォルト方式リストをこの回線に適用します。

次に、PAP に同じ認証アルゴリズムを作成し、「default」ではなく「MIS-access」の方式リストを呼び出す例を示します。

```
aaa new-model
aaa authentication pap MIS-access if-needed group tacacs+ local
 10.1.2.3
 key goaway
interface serial 0
 ppp authentication pap MIS-access
```

前述の設定例の回線は、次のように定義されます。

- **aaa new-model** コマンドは、AAA セキュリティ サービスをイネーブルにします。
- **aaa authentication** コマンドにより、PPP を実行するシリアル インターフェイスに使用する方式リスト「MIS-access」を定義します。方式リスト「MIS-access」は、PPP 認証がすべてのインターフェイスに適用されることを示します。**if-needed** キーワードは、ユーザが ASCII ログイン手順を介してすでに認証済みの場合には PPP 認証が不要なのでスキップできることを示します。認証が必要な場合、キーワード **group tacacs+** は、TACACS+ を介して認証が実行されることを示します。認証中に TACACS+ から何らかのエラーが返される場合、キーワード **local** は、ネットワーク アクセス サーバ上のローカル データベースを使用して認証が試行されることを示します。
- コマンドにより、TACACS+ デーモンが 10.1.2.3 という IP アドレスを持っていると指定します。 コマンドにより、共有暗号キーを「goaway」に定義します。

- **interface** コマンドで回線を選択します。**ppp authentication** コマンドは、デフォルト方式リストをこの回線に適用します。

次に、IP アドレスが 10.2.3.4 である TACACS+ デーモンと暗号キー「apple」の設定の例を示します。

```
aaa new-model
aaa authentication login default group tacacs+ local
 10.2.3.4
 key apple
```

前述の設定例の回線は、次のように定義されます。

- **aaa new-model** コマンドは、AAA セキュリティ サービスをイネーブルにします。
- **aaa authentication** コマンドで、デフォルトの方式リストを定義します。すべてのインターフェイスでの着信 ASCII ログイン（デフォルト）では、認証に TACACS+ を使用します。応答する TACACS+ サーバがない場合、ネットワーク アクセス サーバは、認証用のローカル ユーザ名データベースに含まれる情報を使用します。
- コマンドにより、TACACS+ デーモンが 10.2.3.4 という IP アドレスを持っていると指定します。 コマンドにより、共有暗号キーが「apple」になるように定義します。

TACACS 認可の例

次に、デフォルトの方式リストを使用して、PPP 認証用のセキュリティ プロトコルとして、TACACS+ を設定する例を示します。また、TACACS+ を介してネットワークの許可を設定する方法も示します。

```
aaa new-model
aaa authentication ppp default if-needed group tacacs+ local
aaa authorization network default group tacacs+
 10.1.2.3
 key goaway
interface serial 0
 ppp authentication chap default
```

前述の設定例の回線は、次のように定義されます。

- **aaa new-model** コマンドは、AAA セキュリティ サービスをイネーブルにします。
- **aaa authentication** コマンドにより、PPP を実行するシリアル インターフェイスに使用する方式リスト「default」を定義します。キーワード **default** は、デフォルトですべてのインターフェイスに PPP 認証が適用されることを示します。**if-needed** キーワードは、ユーザが ASCII ログイン手順を介してすでに認証済みの場合には PPP 認証が不要なのでスキップできることを示します。認証が必要な場合、キーワード **group tacacs+** は、TACACS+ を介して認証が実行されることを示します。認証中に TACACS+ から何らかのエラーが返される場合、キーワード **local** は、ネットワーク アクセス サーバ上のローカル データベースを使用して認証が試行されることを示します。

- **aaa authorization** コマンドにより、TACACS+ を介するネットワークの許可を設定します。認証リストとは異なり、この許可リストは、ネットワーク アクセス サーバに対するすべての着信ネットワーク接続に常に適用されます。
- コマンドにより、TACACS+ デーモンが 10.1.2.3 という IP アドレスを持っていると指定します。 コマンドにより、共有暗号キーを「goaway」に定義します。
- **interface** コマンドで回線を選択します。**ppp authentication** コマンドは、デフォルト方式リストをこの回線に適用します。

TACACS アカウンティングの例

次に、デフォルトの方式リストを使用して、PPP 認証用のセキュリティ プロトコルとして、TACACS+ を設定する例を示します。また、TACACS+ を介してアカウンティングを設定する方法も示します。

```
aaa new-model
aaa authentication ppp default if-needed group tacacs+ local
aaa accounting network default stop-only group tacacs+
 10.1.2.3
 key goaway
interface serial 0
 ppp authentication chap default
```

前述の設定例の回線は、次のように定義されます。

- **aaa new-model** コマンドは、AAA セキュリティ サービスをイネーブルにします。
- **aaa authentication** コマンドにより、PPP を実行するシリアル インターフェイスに使用する方式リスト「default」を定義します。キーワード **default** は、デフォルトですべてのインターフェイスに PPP 認証が適用されることを示します。**if-needed** キーワードは、ユーザが ASCII ログイン手順を介してすでに認証済みの場合には PPP 認証が不要なのでスキップできることを示します。認証が必要な場合、キーワード **group tacacs+** は、TACACS+ を介して認証が実行されることを示します。認証中に TACACS+ から何らかのエラーが返される場合、キーワード **local** は、ネットワーク アクセス サーバ上のローカル データベースを使用して認証が試行されることを示します。
- **aaa accounting** コマンドにより、TACACS+ を介するネットワーク アカウンティングを設定します。この例では、ネットワーク接続が終了するたびに、終了したセッションについて説明するアカウンティング レコードが、TACACS+ デーモンに送信されます。
- コマンドにより、TACACS+ デーモンが 10.1.2.3 という IP アドレスを持っていると指定します。 コマンドにより、共有暗号キーを「goaway」に定義します。
- **interface** コマンドで回線を選択します。**ppp authentication** コマンドは、デフォルト方式リストをこの回線に適用します。

TACACS サーバー グループの例

次に、3 つの異なる TACACS+ サーバー メンバを使用してサーバー グループを作成する例を示します。

```
aaa group server tacacs tacgroup1
server 172.16.1.1
server 172.16.1.21
server 172.16.1.31
```

DNIS に基づく AAA サーバー グループの選択の設定例

次に、特定の AAA サービスを提供するために、DNIS に基づいて TACACS+ サーバー グループを選択する例を示します。

```
! This command enables AAA.
aaa new-model
!
! The following set of commands configures the TACACS+ servers that will be associated
! with one of the defined server groups.
 172.16.0.1
 172.17.0.1
 172.18.0.1
 172.19.0.1
 172.20.0.1
 key abcdefg
! The following commands define the sg1 TACACS+ server group and associate servers
! with it.
aaa group server tacacs sg1
  server 172.16.0.1
  server 172.17.0.1
! The following commands define the sg2 TACACS+ server group and associate a server
! with it.
aaa group server tacacs sg2
  server 172.18.0.1
! The following commands define the sg3 TACACS+ server group and associate a server
! with it.
aaa group server tacacs sg3
  server 172.19.0.1
! The following commands define the default-group TACACS+ server group and associate
! a server with it.
aaa group server tacacs default-group
  server 172.20.0.1
!
! The next set of commands configures default-group tacacs server group parameters.
aaa authentication ppp default group default-group
aaa accounting network default start-stop group default-group
!
! The next set of commands enables DNIS mapping and maps DNIS numbers to the defined
! RADIUS server groups. In this configuration, all PPP connection requests using DNIS
! 7777 are sent to the sg1 server group. The accounting records for these connections
! (specifically, start-stop records) are handled by the sg2 server group. Calls with a
! DNIS of 8888 use server group sg3 for authentication and server group default-group
! for accounting. Calls with a DNIS of 9999 use server group default-group for
! authentication and server group sg3 for accounting records (stop records only). All
! other calls with DNIS other than the ones defined use the server group default-group
! for both authentication and stop-start accounting records.
aaa dnis map enable
aaa dnis map 7777 authentication ppp group sg1
```

```
aaa dnis map 7777 accounting network start-stop group sg2
aaa dnis map 8888 authentication ppp group sg3
aaa dnis map 9999 accounting network stop-only group sg3
```

TACACS デーモンの設定例

次に、TACACS+ デーモンの設定例を示します。実際に TACACS+ デーモンで使用する正確な構文は、この例の構文と異なる可能性があります。

```
user = mci_customer1 {
 chap = cleartext “some chap password”
 service = ppp protocol = ip {
inacl#1=”permit ip any any precedence immediate”
inacl#2=”deny igrp 0.0.1.2 255.255.0.0 any”
 }
```

その他の参考資料

ここでは、TACACS+ の設定機能に関する関連資料について説明します。

関連資料

関連項目	マニュアル タイトル
TACACS+ コマンド	『*Cisco IOS Security Command Reference*』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	--

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS XE ソフトウェア リリース、およびフィーチャ セットの MIB の場所を検索しダウンロードするには、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
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	--

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

TACACS 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 : TACACS+* の設定に関する機能情報

機能名	リリース	機能情報
TACACS+		TACACS+ は、ユーザによるルータまたはネットワーク アクセス サーバへのアクセス試行の集中的な確認を可能にするセキュリティ アプリケーションです。 TACACS+ は、認証および認可プロセスについて詳細なアカウンティング情報と柔軟な管理コントロールを提供します。TACACS+ は、AAA を介して実装され、AAA コマンドを使用してのみイネーブルにできます。 次のコマンドが導入または変更されました：、、**aaa authentication**、 **aaa accounting**、**aaa group server tacacs+**。
DNIS に基づく AAA サーバー グループ		DNIS に基づく AAA サーバー グループを使用すると、セッションの着信番号識別サービス（DNIS）番号に基づき、特定の AAA サーバー グループに対してユーザーを認証できます。 次のコマンドが導入または変更されました。**aaa dnis map enable**、**aaa dnis map authentication group**、**aaa dnis map accounting**

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。