



TACACS の設定

この章では、詳細なアカウント情報を提供し、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 コマンドを使用するのみイネーブルにできます。

- [機能情報の確認](#) (1 ページ)
- [TACACS に関する情報](#) (1 ページ)
- [TACACS の設定方法](#) (4 ページ)
- [TACACS の設定例](#) (10 ページ)
- [その他の参考資料](#) (15 ページ)
- [TACACS の設定に関する機能情報](#) (16 ページ)

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。最新の機能情報および警告については、「[Bug Search Tool](#)」およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

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。

TACACS に関する情報

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+ 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 サーバに設定した TACACS+ 機能を使用可能にするには、TACACS+ サーバにアクセスして TACACS+ サーバ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、アカウントिंग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 (TACACS+ デーモン) で、各サービス (認証、許可、アカウントिंग) 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両方の) Cisco IOS および Cisco IOS XE ユーザインターフェイスは、ネットワークアクセスサーバ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は、単一のユーザ、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に試行する機能)。さらに、TACACS+ 認証サービスは、ユーザ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、ユーザセッション時のユーザ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、アカウント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。アカウントングレコードには、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興味があるユーザ向けに、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

ユーザが TACACS+ を使用してネットワーク アクセス サーバ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 サーバは TACACS+ デーモンに接続してユーザ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に表示されます。ユーザがユーザ名を入力すると、ネットワーク アクセス サーバは 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 サーバはユーザに対してパスワードプロンプトを表示します。ユーザ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、デーモンとユーザとの間で対話できるようになり、デーモンはユーザ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 : ユーザは認証に失敗しました。ユーザ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 サーバはユーザを認証する代替方式を使用しようとします。
 4. CONTINUE : ユーザは、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、ユーザによる入力ではなく、PAP プロトコルパッケージでユーザ名とパスワードがネットワーク アクセス サーバに到達するため、ユーザにはプロンプトが表示されません。PPP CHAP ログインは、原則もにしています。

ネットワーク アクセス サーバで認可をイネーブリングしている場合、認証の後に、ユーザは追加の認可段階を実行する必要があります。ユーザは 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



- (注) Cisco IOS XE リリース 3.2S では、**tacacs-server host** コマンドは **tacacs server** コマンドに置き換えられました。**tacacs server** コマンドの詳細については、『*Security Command Reference*』を参照してください。

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。
- **tacacs-server host** 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。**tacacs-server key** コマンドを使用して、ネットワーク アクセス サーバと 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+ 接続のアカウントिंग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、「アカウントिंगの設定」の章を参照してください。

TACACS サーバホストの指定

tacacs-server host コマンドを使用すると、TACACS+ サーバを保守する 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。



(注) **tacacs-server host** コマンドは、間もなく廃止される予定です。**tacacs-server host** コマンドの代わりに **server** コマンドを使用できます。

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
<pre>Router(config)# tacacs-server host hostname [single-connection] [port integer] [timeout integer] [key string]</pre>	TACACS+ホストを指定します。

tacacs-server host 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を使用される 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) **tacacs-server host** コマンドによるタイムアウト値の指定は、このサーバに関する **tacacs-server timeout** 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) **tacacs-server host** コマンドによる暗号キーの指定は、このサーバに関するグローバルコンフィギュレーションの **tacacs-server key** 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。

tacacs-server host コマンドのパラメータの一部は、**tacacs-server timeout** コマンドおよび **tacacs-server key** 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) # tacacs-server key 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 サーバグループの設定

AAA サーバ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。サーバグループは、グローバルサーバホストリストと併せて使用されます。サーバグループには、選択したサーバホストの IP アドレスが一覧表示されます。

サーバ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（アカウントिंगなど）に設定されている場合、設定されている 2 番目のホスト 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トिंगサービスの提供に失敗すると、2 番目のホスト エントリを使用してアカウント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 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）。

サーバグループ名を使用してサーバ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。

手順の概要

1. Router(config)# **tacacs-server host name** [**single-connection**] [**port integer**] [**timeout integer**] [**key string**]
2. Router(config-if)# **aaa group server**{radius | tacacs+} *group-name*
3. Router(config-sg)# **server ip-address** [**auth-port port-number**] [**acct-port port-number**]

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)# tacacs-server host name [single-connection] [port integer] [timeout integer] [key string]	サーバホストの IP アドレスを指定および定義してから、AAA サーバグループを設定します。 tacacs-server host コマンドの詳細については、この章の「TACACS サーバホストの指定」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+} <i>group-name</i>	グループ名を指定して AAA サーバ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+ サーバを定義済みのサーバ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、アカウント専用 UDP ポートを設定します。 AAA サーバグループの TACACS+ サーバごとに、このステップを繰り返します。 (注) グループの各サーバは、 tacacs-server host 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 サーバグループに対してユーザを認証できます。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）。さらに、サーバグループを使用して、複数の AAA サービスに同じサーバ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トサービスと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 サーバ上のすべてのインターフェイスに、一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またはサーバ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 サーバグループの選択を設定する前に、各 AAA サーバ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を設定する必要があります。「TACACS サーバホストの指定」および「AAA サーバグループの設定」を参照してください。

サーバグループの DNIS に基づいて、特定の AAA サーバ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。

手順の概要

1. Router(config)# **aaa dnis map enable**
2. Router(config)# **aaa dnis map dnis-number authentication ppp group server-group-name**
3. Router(config)# **aaa dnis map dnis-number accounting network [none | start-stop | stop-only] group server-group-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 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 サーバグループにマッピングします。このサーバグループのサーバは、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 サーバグループにマッピングします。このサーバグループのサーバは、アカウント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 認可により、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+ を介する認可は、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+ 認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、ユーザがアクセスしているサービスや、ユーザ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 サーバが TACACS+ 認可機能およびアカウントリング機能を実装するには、各ユーザセッションで 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
tacacs-server host 10.1.2.3
tacacs-server 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。
- **tacacs-server host** 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。**tacacs-server key** 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
tacacs-server host 10.1.2.3
tacacs-server 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。
- **tacacs-server host** 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。**tacacs-server key** 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
tacacs-server host 10.1.2.3
tacacs-server 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。
- **tacacs-server host** 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。**tacacs-server key** 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
tacacs-server host 10.2.3.4
tacacs-server 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。
- **tacacs-server host** 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。**tacacs-server key** 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認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+
tacacs-server host 10.1.2.3
tacacs-server 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認可を設定します。認証リストとは異なり、この認可リストは、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。

- **tacacs-server host** 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。**tacacs-server key** 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+
tacacs-server host 10.1.2.3
tacacs-server 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。
- **tacacs-server host** 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。**tacacs-server key** 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 サーバグループの例

次に、3つの異なる TACACS+ サーバメンバを使用してサーバ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.
tacacs-server host 172.16.0.1
tacacs-server host 172.17.0.1
tacacs-server host 172.18.0.1
tacacs-server host 172.19.0.1
tacacs-server host 172.20.0.1
tacacs-server 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 igmp 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規格または変更された規格はありません。また、既存の規格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。	<p>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。</p> <p>http://www.cisco.com/go/mibs</p>

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。	--

テクニカル サポート

説明	Link
<p>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。</p> <p>お使いの製品のセキュリティ情報や技術情報入手するために、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。</p> <p>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。</p>	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+		<p>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。</p> <p>TACACS+ は、認証および認可プロセスについて詳細なアカウント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 コマンドを使用するのみインネーブルにできます。</p> <p>次のコマンドが導入または変更されました：tacacs-server host、tacacs-server key、aaa authentication、aaa accounting、aaa group server tacacs+。</p>
DNIS に基づく AAA サーバグループ		<p>DNIS に基づく AAA サーバ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 サーバグループに対してユーザを認証できます。</p> <p>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</p>

