RADIUS サーバと TACACS+ サーバの設定

この章では、Remote Authentication Dial-In User Service（RADIUS）と Terminal Access Controller Access Control System Plus（TACACS+）を有効にして設定する方法について説明します。これは、認証プロセスと許可プロセスに詳細なアカウンティング情報と柔軟な管理制御を提供します。RADIUS と TACACS+ は AAA を通じて効率化され、AAA コマンド以外では有効に設定できません。

（注） アクセス ポイントは、メイン サーバをバックアップするローカル認証サーバとして、または RADIUS サーバの存在しないネットワークで認証サービスを提供するローカル認証サーバとして設定できます。アクセス ポイントをローカル認証サーバとして設定する方法の詳細は、第 8 章「ローカル認証サーバとしてのアクセス ポイントの設定」を参照してください。

（注） この章で使用されるコマンドの構文と使用方法の詳細は、リリース 12.2 の『Cisco IOS Security Command Reference』を参照してください。

この章の内容は、次のとおりです。

RADIUS の設定と有効化

この項では、RADIUS を設定して有効にする方法について説明します。次の各項で RADIUS の設定について説明します。

RADIUS の概要

RADIUS はネットワークを不正アクセスから保護する、分散型クライアント / サーバ システムです。RADIUS クライアントは RADIUS をサポートするシスコ デバイス上で動作し、中央 RADIUS サーバに認証要求を送信します。RADIUS サーバには、ユーザ認証情報とネットワーク サービス アクセス情報がすべて格納されます。通常、RADIUS ホストは、RADIUS サーバ ソフトウェアを実行するマルチユーザ システムです。RADIUS サーバ ソフトウェアは、シスコ（Cisco Secure Access Control Server バージョン 3.0）、Livingston、Merit、Microsoft、その他のソフトウェア プロバイダーから提供されています。詳細は、RADIUS サーバの資料を参照してください。

RADIUS は、次のようなアクセス セキュリティを必要とするネットワーク環境で使用します。

- それぞれが RADIUS をサポートするマルチ ベンダー アクセス サーバを含むネットワーク。たとえば、複数のベンダーのアクセス サーバは単一の RADIUS サーバ ベースのセキュリティ データベースを使用します。マルチ ベンダーのアクセス サーバを使用する IP ベースのネットワークでは、ダイヤルイン ユーザは Kerberos セキュリティ システムを使用するようにカスタマイズされた RADIUS サーバを通じて認証されます。
- アプリケーションが RADIUS プロトコルをサポートするターンキー ネットワーク セキュリティ環境。これは、*スマート カード*アクセス制御システムを使用するようなアクセス環境です。その例として、ユーザの検証とネットワーク リソースへのアクセス許可に、RADIUS が Enigma のセキュリティ カードとともに使用されています。
- すでに RADIUS を使用しているネットワーク。ネットワークには、RADIUS クライアントを含むシスコ アクセス ポイントを追加できます。
- リソース アカウンティングを必要とするネットワーク。RADIUS アカウンティングは、RADIUS 認証または許可とは無関係に使用できます。RADIUS アカウンティング機能により、サービスの開始および終了時に、セッションの間に使用されるリソース（時間、パケット、バイトなど）の量を示すデータを送信できます。インターネット サービス プロバイダーは、特別なセキュリティと課金のニーズを満たすために、フリーウェア版の RADIUS アクセス制御およびアカウンティング ソフトウェアを使用することがあります。

RADIUS は、次のようなネットワーク セキュリティ状況には適していません。

- マルチプロトコル アクセス環境。RADIUS は AppleTalk Remote Access（ARA）、NetBIOS Frame Control Protocol（NBFCP）、NetWare Asynchronous Services Interface（NASI）、または X.25 PAD 接続をサポートしません。
- スイッチ間またはルータ間の状況。RADIUS は双方向認証を提供しません。シスコ以外のデバイスが認証を要求する場合、RADIUS を使用して、あるデバイスからシスコ以外のデバイスに対して認証を実行できます。
- 各種サービスを使用するネットワーク。一般に RADIUS は、ユーザを 1 つのサービス モデルにバインドします。

RADIUS の操作

無線ユーザが、RADIUS サーバによってアクセス制御されるアクセス ポイントにログインして認証を試行する場合、ネットワークの認証は図 12-1 に示す手順で実行されます。

図 12-1　EAP 認証のシーケンス

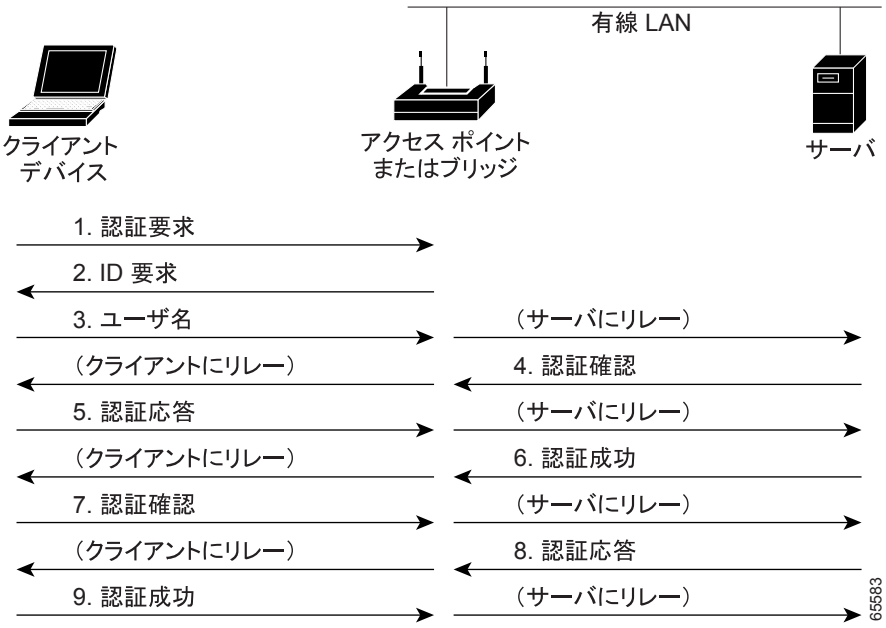

図 12-1 の 1 ～ 9 では、有線 LAN 上の無線クライアント デバイスと RADIUS サーバが、802.1x および Extensible Authentication Protocol（EAP; 拡張認証プロトコル）を使用して、アクセス ポイント経由で相互認証を行っています。RADIUS サーバは、認証身元証明要求をクライアントに送信します。クライアントはユーザが入力したパスワードを一方向暗号化し、認証身元証明要求に対する応答を生成して RADIUS サーバに送信します。RADIUS サーバは、サーバ自体のユーザ データベースの情報から独自の応答を生成し、それをクライアントからの応答と比較します。RADIUS サーバがクライアントを認証すると、同じ処理が逆方向から繰り返され、今度はクライアントが RADIUS サーバを認証します。

相互認証が終了すると、RADIUS サーバとクライアントは、クライアントに固有の、クライアントに適切なレベルのネットワーク アクセスを提供する Wired Equivalent Privacy（WEP）キーを決定します。これにより、有線のスイッチド セグメントのセキュリティ レベルは、デスクトップのレベルに近づきます。クライアントはこのキーをロードして、ログオン セッションでの使用に備えます。

ログオン セッションでは、RADIUS サーバが *セッション キー*と呼ばれる WEP キーを暗号化して、有線 LAN 経由でアクセス ポイントに送信します。アクセス ポイントは、セッション キーを使用してブロードキャスト キーを暗号化し、クライアントに送信します。クライアントは、送信されてきたキーを、セッション キーを使用して復号化します。クライアントとアクセス ポイントは WEP を有効にし、セッション キーとブロードキャスト WEP キーを残りのセッションの間、すべての通信に対して使用します。

EAP 認証には複数のタイプがありますが、アクセス ポイントはどのタイプについても同じように機能します。アクセス ポイントは、無線クライアント デバイスと RADIUS サーバ間の認証メッセージを中継します。RADIUS サーバを使用したクライアント認証の設定方法の詳細は、「SSID への認証タイプの割り当て」の項（P.10-10）を参照してください。

RADIUS の設定

この項では、RADIUS をサポートするアクセス ポイントの設定方法について説明します。ユーザは最低でも、RADIUS サーバ ソフトウェアを実行するホストを識別し、RADIUS の認証方式リストを定義する必要があります。オプションで、RADIUS 認証とアカウンティングの方式リストを定義できます。

方式リストは、ユーザ アカウントの認証、許可、管理に使用される手順と方法を定義します。方式リストを使用して 1 つまたは複数のセキュリティ プロトコルを指定できるので、先頭の方式が失敗してもバックアップ システムが確実に機能できます。ソフトウェアは、リストの先頭の方式を使用してユーザ アカウントの認証、許可、管理をします。その方式が応答しない場合には、リストの次の方式が選択されます。このプロセスは、リスト内の方式との通信に成功するか、または方式リストをすべて試行するまで続けられます。

アクセス ポイントに RADIUS 機能を設定する前に、RADIUS サーバにアクセスして設定する必要があります。

この項で説明する設定の内容は次のとおりです。

（注）　RADIUS サーバの Command-Line Interface（CLI; コマンドライン インターフェイス）コマンドは、**aaa new-model** コマンドを入力するまで無効になっています。

デフォルトの RADIUS 設定

RADIUS と AAA は、デフォルトでは無効になっています。

セキュリティ上の危険を回避するため、ネットワーク管理アプリケーションから RADIUS を設定することはできません。RADIUS を有効にすると、CLI を通じてアクセス ポイントにアクセスするユーザを認証できます。

RADIUS サーバ ホストの識別

アクセス ポイントと RADIUS サーバ間の通信には、次のいくつかのコンポーネントを使用します。

- ホスト名または IP アドレス
- 認証先ポート
- アカウンティング宛先ポート
- キー文字列
- タイムアウト期間
- 再送信値

RADIUS セキュリティ サーバは、ホスト名と IP アドレス、ホスト名と特定の User Datagram Protocol（UDP; ユーザ データグラム プロトコル）ポート番号、IP アドレスと特定の UDP ポート番号により識別されます。IP アドレスと UDP ポート番号の組み合わせから一意の識別子が作成され、異なるポートを特定の AAA サービスを提供する RADIUS ホストとして個別に定義できます。この一意の識別子を使用すると、サーバ上の同じ IP アドレスを持つ複数の UDP ポートに RADIUS 要求を送信できます。

（注）　Cisco IOS リリース 12.2(8)JA 以降では、RADIUS サーバとアクセス ポイントとの通信に、21645 ～ 21844 の範囲で無作為に選択された UDP ソース ポート番号が使用されます。

同一の RADIUS サーバにアカウンティングなど同じサービスを実行する 2 つのホスト エントリを設定すると、2 番目に設定されたホスト エントリは最初のホスト エントリの故障時のバックアップとして機能します。この例では、最初に設定されたホスト エントリがアカウンティング サービスに失敗すると、アクセス ポイントは同じデバイスに設定された 2 番目のホスト エントリにアカウンティング サービスの提供を求めます。（RADIUS ホスト エントリは、設定された順序で試行されます）。

RADIUS サーバとアクセス ポイントは、共有の身元証明要求テキスト文字列を使用して、パスワードを暗号化して応答を交換します。RADIUS で AAA セキュリティ コマンドを使用するように設定するには、RADIUS サーバ デーモンを実行しているホストと、アクセス ポイントと共有する身元証明要求テキスト（キー）文字列を指定する必要があります。

タイムアウト、再送信、暗号キーの値は、すべての RADIUS サーバに対してグローバルに設定することも、またはグローバル設定とサーバ単位の設定を組み合わせることも可能です。アクセス ポイントと通信するすべての RADIUS サーバにこれらの設定をグローバルに適用するには、3 つの一意なグローバル設定コマンド、**radius-server timeout**、**radius-server retransmit**、**radius-server key** を使用します。特定の RADIUS サーバにこれらの値を適用するには、グローバル設定コマンド **radius-server host** を使用します。

（注）　アクセス ポイントにグローバル機能とサーバ単位の機能（タイムアウト、再送信、キー コマンド）を同時に設定する場合、サーバ単位のタイマ、再送信、キー値のコマンドがグローバルなタイマ、再送信、キー値のコマンドに優先します。すべての RADIUS サーバに対するこれら設定の実行については、「すべての RADIUS サーバの設定」の項（P.12-13）を参照してください。

認証時用に AAA サーバ グループを使用して既存のサーバ ホストをグループ化するようアクセス ポイントを設定できます。詳細は、「AAA サーバ グループの定義」の項（P.12-9）を参照してください。

特権 EXEC モードから、次の手順に従ってサーバ単位の RADIUS サーバ通信を設定します。この手順は必須です。

	コマンド	目的
ステップ 1	**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 2	**aaa new-model**	AAA を有効にします。
ステップ 3	**radius-server host** {*hostname* | *ip-address*} [**auth-port** *port-number*] [**acct-port** *port-number*] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*]	リモート RADIUS サーバ ホストの IP アドレスまたはホスト名を指定します。 • （オプション）**auth-port** *port-number* には、認証要求の UDP 宛先ポートを指定します。（オプション）**acct-port** *port-number* には、アカウンティング要求の UDP 宛先ポートを指定します。 • （オプション）**timeout** *seconds* には、アクセス ポイントが再送信する前に RADIUS サーバの返信を待機する時間を指定します。指定範囲は 1 ～ 1000 です。この設定は、グローバル設定コマンド **radius-server timeout** の設定よりも優先されます。**radius-server host** コマンドにタイムアウトが設定されていない場合、**radius-server timeout** コマンドの設定が使用されます。 • （オプション）**retransmit** *retries* には、サーバが応答しないか応答が遅い場合に、RADIUS 要求をサーバに再送信する回数を指定します。範囲は 1 ～ 1000 です。**radius-server host** コマンドでこの再送回数を設定しない場合は、グローバル設定コマンド **radius-server retransmit** の設定が使用されます。 • （オプション）**key** *string* には、アクセス ポイントと RADIUS サーバ上の RADIUS デーモンの間で使用される認証と暗号キーを指定します。 （注）　このキーはテキスト文字列で、その文字列は　RADIUS サーバで使用される暗号キーと一致しなければなりません。キーは常に **radius-server host** コマンドの最後の項目として設定します。先頭の空白は無視されますが、キー内およびキーの末尾の空白は有効です。キーに空白を使用する場合、引用符がキーの一部である場合を除き、キーを引用符で囲まないでください。 アクセス ポイントが単一の IP アドレスと関連付けられた複数のホスト エントリを認識するように設定するには、このコマンドを必要な数だけ入力します。その際、各 UDP ポート番号が異なっていることを確認してください。アクセス ポイントのソフトウェアは、指定された順序でホストを検索します。個々の RADIUS ホストで使用するタイムアウト、再送信、暗号キーの値を設定します。
ステップ 4	**dot11 ssid** *ssid-string*	アカウンティングを有効にする必要がある、Service Set Identifier（SSID; サービス セット ID）の SSID 設定モードを入力します。SSID には、最大 32 文字の英数字を使用できます。SSID では、大文字と小文字が区別されます。

	コマンド	目的
ステップ 5	**accounting** *list-name*	この SSID の RADIUS アカウンティングを有効にします。*list-name* には、アカウンティング方式のリストを指定します。方式のリストの詳細は、次の URL をクリックしてください。 http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fibm_c/bcfpart1/bcftb.htm （注）　SSID のアカウンティングを有効にするには、SSID 設定に **accounting** コマンドを含める必要があります。URL をクリックすると、SSID 設定モード **accounting** コマンドの詳細が表示されます。 http://www.cisco.com/en/US/products/hw/wireless/ps4570/products_command_reference_chapter09186a008041757f.html#wp2449819
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show running-config**	入力内容を確認します。
ステップ 8	**copy running-config startup-config**	（オプション）コンフィギュレーション ファイルに入力内容を保存します。

特定の RADIUS サーバを削除するには、グローバル設定コマンド **no radius-server host** *hostname* | *ip-address* を使用します。

次の例は、認証に使用される RADIUS サーバと、アカウンティングに使用される別の RADIUS サーバの設定方法を示しています。

```
AP(config)# radius-server host 172.29.36.49 auth-port 1612 key rad1
AP(config)# radius-server host 172.20.36.50 acct-port 1618 key rad2
```

次の例は、RADIUS アカウンティング用に SSID を設定する方法を示しています。

```
AP(config)# dot11 ssid batman
AP(config-ssid)# accounting accounting-method-list
```

次の例は、RADIUS サーバとして *host1* を設定して、認証とアカウンティングの両方にデフォルトポートを使用する方法を示しています。

```
AP(config)# radius-server host host1
```

（注）　RADIUS サーバにはほかにも複数の設定が必要です。その設定には、アクセス ポイントの IP アドレスおよびサーバとアクセス ポイントで共有するキー文字列が含まれます。詳細は、RADIUS サーバの資料を参照してください。

RADIUS ログイン認証の設定

AAA 認証を設定するには、認証方式の名前付きリストを定義し、そのリストを各種のインターフェイスに適用します。この方式リストは、実行される認証のタイプと実行順序を定義したものです。定義されたいずれかの認証方式が実行されるようにするには、この方式リストを特定のインターフェイスに適用しておく必要があります。唯一の例外は、デフォルトの方式リスト（名前は、*default*）です。デフォルトの方式リストは、明示的に定義された名前付きの方式リストを持つインターフェイスを除くすべてのインターフェイスに自動的に適用されます。

方式リストには、ユーザの認証時に照会されるシーケンスと認証方式が記述されています。認証に使用するセキュリティ プロトコルを 1 つまたは複数指定できるため、最初の方法が失敗した場合でも認証のバックアップ システムが確実に機能します。ソフトウェアは、まずリストの最初の方式を使用してユーザを認証します。その方式が応答しなければ、方式リストの次の認証方式を選択します。このプロセスは、リスト内の認証方式との通信が成功するか、定義済みの方式をすべて試行するまで続けられます。このサイクルのどの認証にも失敗する場合、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がユーザ アクセスの拒否を応答した場合、認証プロセスは停止して、他の認証方式は試行されません。

特権 EXEC モードから、次の手順に従ってログイン認証を設定します。この手順は必須です。

	コマンド	目的
ステップ 1	**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 2	**aaa new-model**	AAA を有効にします。
ステップ 3	**aaa authentication login** {**default** | *list-name*} *method1* [*method2...*]	ログイン認証方式リストを作成します。 • **login authentication** コマンドで名前付きのリストが指定されていない場合に使用するデフォルトのリストを作成するには、**default** キーワードの後にデフォルトで使用する方式を指定します。デフォルトの方式リストは、自動的にすべてのインターフェイスに適用されます。リスト名の詳細は、次のリンクをクリックしてください。http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/fsaaa/scfathen.htm#xtocid2 • *method1...* には、認証アルゴリズムが試行する実際の方式を指定します。2 番目以降の認証方式が使用されるのは、その前の方式からエラーが返された場合に限られます。前の方式が失敗した場合ではありません。 次のいずれかの方式を選択します。 • **line**：認証に回線パスワードを使用します。この認証方式を使用する前に、回線パスワードを定義する必要があります。回線設定コマンド **username** *password* を使用します。 • **local**：認証にローカル　ユーザ名データベースを使用します。データベースにユーザ名情報を入力する必要があります。グローバル設定コマンド **username** *password* を使用します。 • **radius**：RADIUS 認証を使用します。この認証方式を使用するには、事前に RADIUS サーバを設定しておく必要があります。詳細は、「RADIUS サーバ ホストの識別」の項（P.12-5）を参照してください。
ステップ 4	**line** [**console** | **tty** | **vty**] *line-number* [*ending-line-number*]	回線設定モードを開始し、認証リストを適用する回線を設定します。

	コマンド	目的
ステップ 5	**login authentication** {**default** | *list-name*}	認証リストを 1 つまたは複数の回線に適用します。 • **default** を指定すると、**aaa authentication login** コマンドで作成したデフォルト リストを使用します。 • *list-name* には、**aaa authentication login** コマンドで作成したリストを指定します。
ステップ 6	**radius-server attribute 32 include-in-access-req format %h**	認証時に NAS_ID 属性でシステム名を送信するようにアクセスポイントを設定します。
ステップ 7	**end**	特権 EXEC モードに戻ります。
ステップ 8	**show running-config**	入力内容を確認します。
ステップ 9	**copy running-config startup-config**	（オプション）コンフィギュレーション ファイルに入力内容を保存します。

AAA を無効にするには、グローバル設定コマンド **no aaa new-model** を使用します。AAA 認証を無効にするには、グローバル設定コマンド **no aaa authentication login** {**default** | *list-name*} *method1* [*method2...*] を使用します。ログインの RADIUS 認証を無効にするか、デフォルト値に戻すには、回線設定コマンド **no login authentication** {**default** | *list-name*} を使用します。

AAA サーバ グループの定義

認証時用に AAA サーバ グループを使用して既存のサーバ ホストをグループ化するようアクセスポイントを設定できます。設定されたサーバ ホストのサブセットを選択して、特定のサービスに使用します。このサーバ グループは、グローバル サーバ ホスト リストで使用されます。このリストには、選択されたサーバ ホストの IP アドレスのリストが示されています。

各ホスト エントリが一意の識別子（IP アドレスと UDP ポート番号の組み合わせ）を持っていれば、同一サーバに対する複数のホスト エントリをサーバ グループに含めることも可能です。それによって、特定の AAA サービスを提供する RADIUS ホストとして、異なるポートを個別に定義できます。同一の RADIUS サーバにアカウンティングなど同じサービスを実行する 2 つのホスト エントリを設定すると、2 番目に設定されたホスト エントリは最初のホスト エントリの故障時のバックアップとして機能します。

特定のサーバに定義済みグループ サーバをアソシエートするには、グループ サーバ設定コマンド **server** を使用します。IP アドレスでサーバを特定するか、オプションの **auth-port** および **acct-port** キーワードを使用して複数のホスト インスタンスまたはエントリを特定できます。

特権 EXEC モードから、次の手順に従って、AAA サーバ グループを定義し、特定の RADIUS サーバをそのグループにアソシエートします。

	コマンド	目的
ステップ 1	**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 2	**aaa new-model**	AAA を有効にします。

	コマンド	目的
ステップ 3	**radius-server host** {*hostname* | *ip-address*} [**auth-port** *port-number*] [**acct-port** *port-number*] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*]	リモート RADIUS サーバ ホストの IP アドレスまたはホスト名を指定します。 • （オプション）**auth-port** *port-number* には、認証要求の UDP 宛先ポートを指定します。 • （オプション）**acct-port** *port-number* には、アカウンティング要求の UDP 宛先ポートを指定します。 • （オプション）**timeout** *seconds* には、アクセス ポイントが再送信する前に RADIUS サーバの返信を待機する時間を指定します。指定範囲は 1 ～ 1000 です。この設定は、グローバル設定コマンド **radius-server timeout** の設定よりも優先されます。**radius-server host** コマンドにタイムアウトが設定されていない場合、**radius-server timeout** コマンドの設定が使用されます。 • （オプション）**retransmit** *retries* には、サーバが応答しないか応答が遅い場合に、RADIUS 要求をサーバに再送信する回数を指定します。範囲は 1 ～ 1000 です。**radius-server host** コマンドでこの再送回数を設定しない場合は、グローバル設定コマンド **radius-server retransmit** の設定が使用されます。 • （オプション）**key** *string* には、アクセス ポイントと RADIUS サーバ上の RADIUS デーモンの間で使用される認証と暗号キーを指定します。 （注）　このキーはテキスト文字列で、その文字列は　RADIUS サーバで使用される暗号キーと一致しなければなりません。キーは常に **radius-server host** コマンドの最後の項目として設定します。先頭の空白は無視されますが、キー内およびキーの末尾の空白は有効です。キーに空白を使用する場合、引用符がキーの一部である場合を除き、キーを引用符で囲まないでください。 アクセス ポイントが単一の IP アドレスと関連付けられた複数のホスト エントリを認識するように設定するには、このコマンドを必要な数だけ入力します。その際、各 UDP ポート番号が異なっていることを確認してください。アクセス ポイントのソフトウェアは、指定された順序でホストを検索します。個々の RADIUS ホストで使用するタイムアウト、再送信、暗号キーの値を設定します。
ステップ 4	**aaa group server radius** *group-name*	AAA サーバ グループをグループ名で定義します。 このコマンドを実行すると、アクセス ポイントはサーバ グループ設定モードへ移行します。
ステップ 5	**server** *ip-address*	特定の RADIUS サーバを定義されたサーバ グループにアソシエートします。この手順を、AAA サーバ グループの各 RADIUS サーバについて繰り返します。 グループ内の各サーバは、ステップ 2 であらかじめ定義されている必要があります。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show running-config**	入力内容を確認します。
ステップ 8	**copy running-config startup-config**	（オプション）コンフィギュレーション ファイルに入力内容を保存します。
ステップ 9		RADIUS ログイン認証を有効にします。「RADIUS ログイン認証の設定」の項（P.12-8）を参照してください。

特定の RADIUS サーバを削除するには、グローバル設定コマンド **no radius-server host** *hostname* | *ip-address* を使用します。設定リストからサーバ グループを削除するには、グローバル設定コマンド **no aaa group server radius** *group-name* を使用します。RADIUS サーバの IP アドレスを削除するには、サーバ グループ設定コマンド **no server** *ip-address* を使用します。

次の例では、アクセス ポイントは異なる 2 つの RADIUS グループ サーバ（*group1* と *group2*）を認識するように設定されます。group1 には、同じ RADIUS サーバで同じサービス用に設定された異なる 2 つのホスト エントリがあります。2 番目のホスト エントリは、最初のエントリに対して故障時のバックアップとして機能します。

```
AP(config)# aaa new-model
AP(config)# radius-server host 172.20.0.1 auth-port 1000 acct-port 1001
AP(config)# radius-server host 172.10.0.1 auth-port 1645 acct-port 1646
AP(config)# aaa group server radius group1
AP(config-sg-radius)# server 172.20.0.1 auth-port 1000 acct-port 1001
AP(config-sg-radius)# exit
AP(config)# aaa group server radius group2
AP(config-sg-radius)# server 172.20.0.1 auth-port 2000 acct-port 2001
AP(config-sg-radius)# exit
```

ユーザ特権アクセスとネットワーク サービスの RADIUS 許可の設定

AAA 許可は、ユーザが使用できるサービスを制限します。AAA 許可が有効の場合、アクセス ポイント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セッションを設定します。ユーザのプロファイルは、ローカル ユーザ データベースかセキュリティ サーバにあります。ユーザが要求したサービスへのアクセスを許可されるのは、ユーザ プロファイル内の情報により許可された場合だけです。

（注）　この項では、アクセス　ポイント管理者向けの許可の設定について説明します。無線クライアント デバイス向けの許可の設定は説明しません。

グローバル設定コマンド **aaa authorization** と **radius** キーワードを使用すると、ユーザのネットワーク アクセスを特権 EXEC モードに制限するパラメータを設定できます。

これらの許可パラメータは、**aaa authorization exec radius local** コマンドで設定します。

- 認証に RADIUS が使用された場合は、特権 EXEC アクセス許可に RADIUS を使用します。
- 認証に RADIUS が使用されなかった場合は、ローカル データベースを使用します。

（注）　CLI を通してログインした認証済みユーザは、許可が設定されていても許可が省略されます。

特権 EXEC モードから、次の手順に従って特権 EXEC アクセスとネットワーク サービスに RADIUS 許可を指定します。

	コマンド	目的
ステップ 1	**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 2	**aaa authorization network radius**	ネットワーク関連のすべてのサービス要求に対して、ユーザが RADIUS 許可を受けるようにアクセス ポイントを設定します。

	コマンド	目的
ステップ 3	**aaa authorization exec radius**	ユーザの RADIUS 許可でユーザの特権 EXEC アクセス権の有無を判断するように、アクセス ポイントを設定します。 **exec** キーワードにより、ユーザ プロファイル情報（**autocommand** 情報など）が返される場合があります。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	入力内容を確認します。
ステップ 6	**copy running-config startup-config**	（オプション）コンフィギュレーション ファイルに入力内容を保存します。

許可を無効にするには、グローバル設定コマンド **no aaa authorization** {**network** | **exec**} *method1* を使用します。

RADIUS アカウンティングの起動

AAA アカウンティング機能は、ユーザがアクセスしているサービスと、サービスが消費しているネットワーク リソースの量を追跡します。AAA アカウンティングが有効の場合、アクセス ポイントはアカウンティングの記録の形式でユーザ アクティビティを RADIUS セキュリティ サーバに報告します。各アカウンティングの記録にはアカウンティング属性と値のペア（AV）が含まれており、セキュリティ サーバに保存されます。その後このデータは、ネットワーク管理、クライアントへの課金、または監査のために分析されます。アクセス ポイントに送信される属性の完全なリストについては、「アクセス ポイントが送信する RADIUS 属性」の項（P.12-18）を参照してください。

特権 EXEC モードから、次の手順に従って Cisco IOS 特権レベルとネットワーク サービスに RADIUS アカウンティングを有効にします。

	コマンド	目的
ステップ 1	**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 2	**aaa accounting network start-stop radius**	ネットワーク関連のすべてのサービス要求に、RADIUS アカウンティングを有効にします。
ステップ 3	**ip radius source-interface bvi1**	アカウンティングの記録として BVI IP アドレスを NAS_IP_ADDRESS 属性で送信するようにアクセス ポイントを設定します。
ステップ 4	**aaa accounting update periodic** *minutes*	アカウンティングの更新間隔を分で入力します。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show running-config**	入力内容を確認します。
ステップ 7	**copy running-config startup-config**	（オプション）コンフィギュレーション ファイルに入力内容を保存します。

アカウンティングを無効にするには、グローバル設定コマンド **no aaa accounting** {**network** | **exec**} {**start-stop**} *method1...* を使用します。

CSID 形式の選択

Called-Station-ID（CSID）内の Media Access Control（MAC; メディア アクセス制御）アドレスの形式と RADIUS パケット内の CSID 属性を選択できます。グローバル設定コマンド **dot11 aaa csid** を使用して、CSID 形式を選択します。表 12-1 は、形式オプションと対応する MAC アドレスの例を示しています。

表 12-1　CSID 形式オプション

オプション	MAC アドレスの例
default	0007.85b3.5f4a
ietf	00-07-85-b3-5f-4a
unformatted	000785b35f4a

デフォルトの CSID 形式に戻すには、**dot11 aaa csid** コマンドで **no** を指定するか、**dot11 aaa csid default** と入力します。

（注）　また **wlccp wds aaa csid** コマンドを使用しても CSID 形式を選択できます。

すべての RADIUS サーバの設定

特権 EXEC モードから、次の手順に従ってアクセス ポイントとすべての RADIUS サーバ間のグローバル通信設定を実行します。

	コマンド	目的
ステップ 1	**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 2	**radius-server key** *string*	アクセス ポイントとすべての RADIUS サーバ間で使用する共有の身元証明要求テキスト文字列を指定します。 （注）　このキーはテキスト文字列で、その文字列は RADIUS サーバで使用される暗号キーと一致しなければなりません。先頭の空白は無視されますが、キー内およびキーの末尾の空白は有効です。キーに空白を使用する場合、引用符がキーの一部である場合を除き、キーを引用符で囲まないでください。
ステップ 3	**radius-server retransmit** *retries*	アクセス ポイントが RADIUS 要求をサーバに送信して、中止するまでの回数を指定します。デフォルトは 3、範囲は 1 ～ 1000 です。
ステップ 4	**radius-server timeout** *seconds*	アクセス ポイントが RADIUS 要求を再送する前に、要求への応答を待機する時間を秒数で指定します。デフォルトは 5、範囲は 1 ～ 1000 です。

	コマンド	目的
ステップ 5	**radius-server deadtime** *minutes*	このコマンドは、Cisco IOS ソフトウェアで認証要求に応答しない RADIUS サーバを「dead」とマークして、要求の待機がタイムアウトになる前に、設定された次のサーバを試行する場合に使用します。dead とマークされている RADIUS サーバでは、指定する時間の間（最大 1440 分、24 時間）、追加の要求はスキップされます。 （注）　複数の RADIUS サーバを設定した場合、パフォーマンスの最適化のために RADIUS サーバのデッドタイムを設定する必要があります。
ステップ 6	**radius-server attribute 32 include-in-access-req format %h**	認証時に NAS_ID 属性でシステム名を送信するようにアクセスポイントを設定します。
ステップ 7	**end**	特権 EXEC モードに戻ります。
ステップ 8	**show running-config**	設定内容を確認します。
ステップ 9	**copy running-config startup-config**	（オプション）コンフィギュレーション ファイルに入力内容を保存します。

再送信、タイムアウト、デッドタイムをデフォルトの設定に戻すには、それぞれのコマンドで **no** を指定します。

ベンダー固有の RADIUS 属性を使用するアクセス ポイントの設定

Internet Engineering Task Force（IETF）のドラフト規格では、アクセス ポイントと RADIUS サーバ間で、ベンダー固有の属性（属性 26）を使用してベンダー固有の情報をやり取りする方法を指定しています。ベンダーは、Vendor-Specific Attributes（VSA; ベンダー固有の属性）を使用することで、汎用には適していない各社固有の拡張属性に対応できます。シスコの RADIUS 実装では、仕様で推奨される形式を使用することで、ベンダー固有オプションを 1 つサポートします。シスコのベンダー ID は 9 です。サポートされるオプションはベンダータイプ 1 であり、*cisco-avpair* という名前が付けられています。この値は、次の形式の文字列です。

```
protocol : attribute sep value *
```

potocol は特定の許可を受けるためのシスコ プロトコル属性の値です。*attribute* と *value* は、Cisco TACACS+ 仕様で定義された該当 AV ペアです。*sep* には、必須属性の場合は = を、オプション属性の場合はアスタリスク（*）を指定します。このコマンドにより、TACACS+ 許可で使用できる全機能が RADIUS でも使用できます。

たとえば、次の AV ペアは IP 許可の際（PPP の IPCP アドレス割り当ての際）、シスコの *multiple named ip address pools* 機能を有効にします。

```
cisco-avpair= "ip:addr-pool=first"
```

次の例は、特権 EXEC コマンドへの即時アクセスを使用して、ユーザにアクセス ポイントからログインする方法を示しています。

```
cisco-avpair= "shell:priv-lvl=15"
```

他のベンダーには、そのベンダー固有の ID、オプション、関連 VSA があります。ベンダーの ID と VSA についての詳細は、RFC 2138「Remote Authentication Dian-In User Service（RADIUS）」を参照してください。

特権 EXEC モードから、次の手順に従って、VSA を認識して使用するようにアクセス ポイントを設定します。

	コマンド	目的
ステップ 1	**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 2	**radius-server vsa send** [**accounting** | **authentication**]	アクセス ポイントが RADIUS IETF 属性 26 で定義された VSA を認識して使用できるようにします。 • （オプション）認識されたベンダー固有の属性セットをアカウンティング属性だけに制限するには、**accounting** キーワードを使用します。 • （オプション）認識されたベンダー固有の属性セットを認証属性だけに制限するには、**authentication** キーワードを使用します。 キーワードを指定しないでこのコマンドを入力すると、アカウンティングと認証の両方のベンダー固有属性が使用されます。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show running-config**	設定内容を確認します。
ステップ 5	**copy running-config startup-config**	（オプション）コンフィギュレーション ファイルに入力内容を保存します。

RADIUS 属性の完全なリスト、または VSA 26 の詳細は、リリース 12.2 の『Cisco IOS Security Configuration Guide』の付録「RADIUS Attributes」を参照してください。

ベンダー専用の RADIUS サーバ通信用アクセス ポイントの設定

IETF の RADIUS ドラフト規格では、アクセス ポイントと RADIUS サーバの間でベンダー専用の情報を通信する方法を指定していますが、一部のベンダーは RADIUS 属性セットを独自の方法で拡張しています。Cisco IOS ソフトウェアは、ベンダー専用の RADIUS 属性のサブセットをサポートします。

すでに説明したように、ベンダー専用または IETF ドラフト準拠の RADIUS を設定するには、RADIUS サーバ デーモンを実行しているホストと、そのホストがアクセス ポイントを共有する身元証明要求テキストを指定する必要があります。RADIUS ホストと身元証明要求テキストは、グローバル設定コマンド **radius-server** を使用して指定します。

特権 EXEC モードから、次の手順に従ってベンダー専用の RADIUS サーバ ホストおよび共有の身元証明要求テキストを指定します。

	コマンド	目的
ステップ 1	**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 2	**radius-server host** {*hostname* | *ip-address*} **non-standard**	リモート RADIUS サーバ ホストの IP アドレスまたはホスト名を指定し、ホストがベンダー専用の RADIUS 実装を使用していることを識別します。

	コマンド	目的
ステップ 3	**radius-server key** *string*	アクセス ポイントとベンダー専用の RADIUS サーバ間で使用する共有の身元証明要求テキスト文字列を指定します。アクセス ポイントと RADIUS サーバは、このテキスト文字列を使用して、パスワードを暗号化し応答を交換します。 （注）　このキーはテキスト文字列で、その文字列は RADIUS サーバで使用される暗号キーと一致しなければなりません。先頭の空白は無視されますが、キー内およびキーの末尾の空白は有効です。キーに空白を使用する場合、引用符がキーの一部である場合を除き、キーを引用符で囲まないでください。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	設定内容を確認します。
ステップ 6	**copy running-config startup-config**	（オプション）コンフィギュレーション ファイルに入力内容を保存します。

ベンダー専用の RADIUS ホストを削除するには、グローバル設定コマンド **no radius-server host** {*hostname* | *ip-address*} **non-standard** を使用します。キーを無効にするには、グローバル設定コマンド **no radius-server key** を使用します。

次の例は、ベンダー専用の RADIUS ホストを指定して、アクセス ポイントとサーバ間で秘密鍵 *rad124* を使用する方法を示しています。

```
AP(config)# radius-server host 172.20.30.15 nonstandard
AP(config)# radius-server key rad124
```

WISPr RADIUS 属性の設定

Wi-Fi アライアンスのドキュメント『WISPr Best Current Practices for Wireless Internet Service Provider (WISP) Roaming』には、アクセス ポイントが RADIUS アカウンティングおよび認証要求とともに送信しなければならない RADIUS 属性が示されています。現在アクセス ポイントは、WISPr ロケーション名、ISO と International Telecommunications Union（ITU）の国番号とエリア コード属性だけをサポートしています。**snmp-server location** コマンドと **dot11 location isocc** コマンドを使用して、アクセス ポイントでこれらの属性を設定します。

また、ドキュメント『WISPr Best Current Practices for Wireless Internet Service Provider (WISP) Roaming』には、RADIUS 認証応答とアカウンティング要求でクラス属性をアクセス ポイントに加えることも指示されています。アクセス ポイントは自動的にクラス属性を加えるので、それを設定する必要はありません。

ISO と ITU の国番号とエリア コードのリストは、ISO と ITU の Web サイトにあります。Cisco IOS ソフトウェアは、アクセス ポイントで設定された国番号とエリア コードの有効性を確認しません。

特権 EXEC モードから、次の手順に従ってアクセス ポイントに WISPr RADIUS 属性を指定します。

	コマンド	目的
ステップ 1	**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 2	**snmp-server location** *location*	WISPr の場所名属性を指定します。ドキュメント『WISPr Best Current Practices for Wireless Internet Service Provider (WISP) Roaming』では、次の形式で場所名を入力することを推奨しています。 *hotspot_operator_name*,*location*
ステップ 3	**dot11 location isocc** *ISO-country-code* **cc** *country-code* **ac** *area-code*	アクセス ポイントがアカウンティング要求と認証要求に加える ISO と ITU の国番号とエリア コードを指定します。 • **isocc** *ISO-country-code*：アクセス ポイントが RADIUS 認証とアカウンティング要求に加える ISO 国番号を指定します。 • **cc** *country-code*：アクセス ポイントが RADIUS 認証とアカウンティング要求に加える ITU 国番号を指定します。 • **ac** *area-code*：アクセス ポイントが RADIUS 認証とアカウンティング要求に加える ITU エリア コードを指定します。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	設定内容を確認します。
ステップ 6	**copy running-config startup-config**	（オプション）コンフィギュレーション ファイルに入力内容を保存します。

次の例は、WISPr の場所名属性を設定する方法を示しています。

```
ap# snmp-server location ACMEWISP,Gate_14_Terminal_C_of_Newark_Airport
```

次の例は、アクセス ポイントで ISO と ITU のロケーション コードを設定する方法を示しています。

```
ap# dot11 location isocc us cc 1 ac 408
```

次の例は、アクセス ポイントがクライアント デバイスの使用する SSID を追加して場所 ID 文字列をフォーマットする方法を示しています。

```
isocc=us,cc=1,ac=408,network=ACMEWISP_NewarkAirport
```

RADIUS 設定の表示

RADIUS 設定を表示するには、特権 EXEC コマンド **show running-config** を使用します。

（注）　アクセス ポイントで DNS が設定されている場合、**show running-config** コマンドはサーバのホスト名の代わりに IP アドレスを表示することがあります。

アクセス ポイントが送信する RADIUS 属性

表 12-2 から表 12-6 は、アクセス要求、アクセス許可、アカウンティング要求パケットの中でアクセス ポイントがクライアントに送信する属性を示しています。

（注）　Wi-Fi アライアンスのドキュメント『WISPr Best Current Practices for Wireless Internet Service Provider (WISP) Roaming』で推奨されているように、RADIUS アカウンティング要求と認証要求の属性に加えるように、アクセス ポイントを設定できます。詳細は、「ベンダー固有の RADIUS 属性を使用するアクセス ポイントの設定」の項（P.12-14）を参照してください。

表 12-2　アクセス要求パケットで送信される属性

属性 ID	説明
1	User-Name
4	NAS-IP-Address
5	NAS-Port
12	Framed-MTU
30	Called-Station-ID（MAC アドレス）
31	Calling-Station-ID（MAC アドレス）
32	NAS-Identifier[1]
61	NAS-Port-Type
79	EAP-Message
80	Message-Authenticator

1. 属性 32（include-in-access-req）が設定されている場合、アクセス ポイントは NAS-Identifier を送信します。

表 12-3　アクセス許可パケットで送信される属性

属性 ID	説明
25	Class
27	Session-Timeout
64	Tunnel-Type[1]
65	Tunnel-Medium-Type[1]
79	EAP-Message
80	Message-Authenticator
81	Tunnel-Private-Group-ID[1]
VSA（属性 26）	LEAP session-key
VSA（属性 26）	auth-algo-type
VSA（属性 26）	SSID

1. RFC2826、VLAN オーバーライド番号を定義

表 12-4　アカウンティング要求（開始）パケットで送信される属性

属性 ID	説明
1	User-Name
4	NAS-IP-Address
5	NAS-Port
6	Service-Type
25	Class
41	Acct-Delay-Time
44	Acct-Session-ID
61	NAS-Port-Type
VSA（属性 26）	SSID
VSA（属性 26）	NAS-Location
VSA（属性 26）	Cisco-NAS-Port
VSA（属性 26）	Interface

表 12-5　アカウンティング要求（更新）パケットで送信される属性

属性 ID	説明
1	User-Name
4	NAS-IP-Address
5	NAS-Port
6	Service-Type
25	Class
41	Acct-Delay-Time
42	Acct-Input-Octets
43	Acct-Output-Octets
44	Acct-Session-ID
46	Acct-Session-Time
47	Acct-Input-Packets
48	Acct-Output-Packets
61	NAS-Port-Type
VSA（属性 26）	SSID
VSA（属性 26）	NAS-Location
VSA（属性 26）	VLAN-ID
VSA（属性 26）	Connect-Progress
VSA（属性 26）	Cisco-NAS-Port
VSA（属性 26）	Interface

表 12-6　アカウンティング要求（終了）パケットで送信される属性

属性 ID	説明
1	User-Name
4	NAS-IP-Address
5	NAS-Port
6	Service-Type
25	Class
41	Acct-Delay-Time
42	Acct-Input-Octets
43	Acct-Output-Octets
44	Acct-Session-ID
46	Acct-Session-Time
47	Acct-Input-Packets
48	Acct-Output-Packets
49	Acct-Terminate-Cause
61	NAS-Port-Type
VSA（属性 26）	SSID
VSA（属性 26）	NAS-Location
VSA（属性 26）	Disc-Cause-Ext
VSA（属性 26）	VLAN-ID
VSA（属性 26）	Connect-Progress
VSA（属性 26）	Cisco-NAS-Port
VSA（属性 26）	Interface
VSA（属性 26）	auth-algo-type

（注）　デフォルトでは、アクセス ポイントは service-type 属性を authenticate-only に設定した状態で、再認証要求を認証サーバに送信します。ただし、Microsoft IAS サーバの中には、authenticate-only の service-type 属性をサポートしていないものがあります。service-type 属性を login-only に変更することで、Microsoft IAS サーバがアクセス ポイントからの再認証要求を認識できるようになります。再認証要求の service-type 属性を login-only に変更するには、グローバル設定コマンド **dot11 aaa authentication attributes service-type login-only** を使用します。

TACACS+ の設定と有効化

この項で説明する設定の内容は次のとおりです。

TACACS+ の概要

TACACS+ は、アクセス ポイントにアクセスしようとするユーザを集中的に検証するセキュリティ アプリケーションです。RADIUS とは異なり、TACACS+ はアクセス ポイントにアソシエートされたクライアント デバイスを認証しません。

TACACS+ サービスは、通常 UNIX または Windows NT ワークステーションで動作する TACACS+ デーモンのデータベース内で管理されます。アクセス ポイントに TACACS+ 機能を設定する前に、TACACS+ サーバにアクセスして設定する必要があります。

TACACS+ には独立したモジュール式の認証、許可、およびアカウンティング機能が備わっています。TACACS+ によって、単一のアクセス制御サーバ（TACACS+ デーモン）が、認証、許可、アカウンティングの各サービスを個別に提供できます。各サービスを独自のデータベースと関連付けて、デーモンの機能に応じて、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利用することができます。

AAA セキュリティ サービスを通じて管理される TACACS+ は、次のようなサービスを提供します。

- 認証：ログインとパスワードのダイアログ、身元証明要求と応答、メッセージのサポートを通じて管理者の認証を完全に制御します。

  認証機能は、管理者との対話を実行できます（たとえば、ユーザ名とパスワードが入力された後に、自宅住所、母親の旧姓、サービス タイプ、社会保険番号など、複数の質問でユーザの身元を確認します）。また TACACS+ 認証サービスは、管理者の画面にメッセージを送信できます。たとえば、会社のパスワード エージング ポリシーのため、パスワードを変更する必要があることをメッセージで管理者に通知することができます。
- 許可：管理者のセッション期間中の管理機能を詳細に制御します。これには自動コマンドの設定、アクセス制御、セッション期間、またはプロトコル サポートなどが含まれますが、それに限定されません。また、管理者が TACACS+ 許可機能で実行できるコマンドを強制的に制限できます。
- アカウンティング：課金、監査、報告に使用される情報を収集して、TACACS+ デーモンに送信します。ネットワーク マネージャはアカウンティング機能を使用して、セキュリティ監査時に管理者アクティビティを追跡したり、またはユーザの課金時に情報を提供できます。アカウンティング レコードには、管理者 ID、開始時間と終了時間、実行されたコマンド（PPP など）、パケット数、バイト数が含まれます。

TACACS+ プロトコルは、アクセス ポイントと TACACS+ デーモンの間で認証を実行します。アクセス ポイントと TACACS+ デーモンの間で実行されるすべてのプロトコル交換が暗号化されるので、認証の機密性を保証します。

アクセス ポイントで TACACS+ を使用するには、TACACS+ デーモン ソフトウェアを実行するシステムが必要です。

TACACS+ の操作

管理者が TACACS+ を使用してアクセス ポイントの認証を受け、簡単な ASCII ログインを試行した場合、次のプロセスが発生します。

1. 接続が確立されると、アクセス ポイントは TACACS+ デーモンに連絡してユーザ名プロンプトを取得し、このプロンプトが管理者に表示されます。管理者がユーザ名を入力すると、アクセス ポイントは TACACS+ デーモンにアクセスしてパスワード プロンプトを取得します。アクセス ポイントは管理者にパスワード プロンプトを表示し、管理者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。

   TACACS+ を使用してデーモンと管理者との間で会話が続けられ、デーモンは管理者の認証に必要な情報を取得します。デーモンはユーザ名とパスワードの組み合わせの入力を要求しますが、ユーザの母親の旧姓など、他の項目が含まれる場合があります。

2. アクセス ポイントは最終的に、TACACS+ デーモンから次に示す応答のいずれかを受信します。
   - ACCEPT：管理者が認証され、サービスが開始します。許可を要求するようにアクセス ポイントが設定されている場合、この時点で許可が開始します。
   - REJECT：管理者は認証されません。管理者は TACACS+ デーモンに従ってアクセスが拒否されるか、ログイン シーケンスを再試行するように要求されます。
   - ERROR：デーモンによる認証のある時点、またはデーモンとアクセス ポイント間のネットワーク接続のある時点で、エラーが発生しています。ERROR 応答を受信した場合、通常、アクセス ポイントは、別の方法で管理者の認証を試行します。
   - CONTINUE：管理者は追加の認証情報を要求されます。

   認証の後、アクセス ポイントで許可が有効になっている場合、管理者はさらに許可フェーズに進みます。管理者は TACACS+ 許可に進む前に、まず TACACS+ 認証を完了する必要があります。

3. TACACS+ 許可が要求される場合、再び TACACS+ デーモンにアクセスします。TACACS+ デーモンは ACCEPT か REJECT の許可応答を返します。ACCEPT 応答が返された場合、この応答には属性の形でその管理者に EXEC または NETWORK セッションを指示するデータが含まれており、管理者がアクセスできる下記のサービスを決定できます。
   - Telnet、rlogin、または特権 EXEC サービス
   - 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、管理者のタイムアウトが含まれます。

TACACS+ の設定

この項では、TACACS+ をサポートするアクセス ポイントの設定方法について説明します。ユーザは最低でも TACACS+ デーモンを実行するホストを識別して、TACACS+ 認証の方式リストを定義する必要があります。オプションで、TACACS+ 認証とアカウンティングの方式リストを定義できます。方式リストは管理者アカウントの認証、許可、管理に使用される手順と方法を定義します。方式リストを使用して 1 つまたは複数のセキュリティ プロトコルを指定できるので、先頭の方式が失敗してもバックアップ システムが確実に機能できます。ソフトウェアは、リストの先頭の方式を使用して管理者のアカウントの認証、許可、管理をします。その方式が応答しない場合には、リストの次の方式が選択されます。このプロセスは、リスト内の方式との通信に成功するか、または方式リストをすべて試行するまで続けられます。

この項で説明する設定の内容は次のとおりです。

- デフォルトの TACACS+ 設定（P. 12-23）
- TACACS+ サーバ ホストの識別と認証キーの設定（P. 12-23）
- TACACS+ ログイン認証の設定（P. 12-24）
- 特権 EXEC アクセスとネットワーク サービスの TACACS+ 許可の設定（P. 12-25）
- TACACS+ アカウンティングの起動（P. 12-26）

デフォルトの TACACS+ 設定

TACACS+ と AAA は、デフォルトでは無効になっています。

セキュリティの失効を防止するために、ネットワーク管理アプリケーションを通じて TACACS+ を設定することはできません。TACACS+ を有効にすると、CLI を通じてアクセス ポイントにアクセスする管理者を認証できます。

TACACS+ サーバ ホストの識別と認証キーの設定

認証時に単一サーバまたは AAA サーバ グループを使用して既存のサーバ ホストをグループ化するようにアクセス ポイントを設定できます。サーバをグループ化し、設定されたサーバ ホストのサブセットを選択して特定のサービスに使用できます。このサーバ グループは、グローバル サーバ ホスト リストで使用され、選択されたサーバ ホストの IP アドレスのリストが含まれます。

特権 EXEC モードから、次の手順に従って TACACS+ サーバを実行する IP ホストを識別し、オプションで暗号キーを設定します。

	コマンド	目的
ステップ 1	**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 2	**tacacs-server host** *hostname* [**port** *integer*] [**timeout** *integer*] [**key** *string*]	TACACS+ サーバを管理している IP ホストを識別します。このコマンドを数回入力して、優先されるホストのリストを作成します。ソフトウェアは、指定された順序でホストを検索します。 • *hostname* には、ホストの名前または IP アドレスを指定します。 • （オプション）**port** *integer* には、サーバのポート番号を指定します。デフォルトはポート 49、範囲は 1 ～ 65535 です。 • （オプション）**timeout** *integer* には、タイム アウトになってアクセス ポイントがエラーを宣言するまでにデーモンからの応答を待機する時間を秒数で指定します。デフォルト設定は 5 秒です。範囲は 1 ～ 1000 秒です。 • （オプション）**key** *string* には、アクセス ポイントと TACACS+ デーモンの間の全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。正常に暗号化するために、同じキーを TACACS+ デーモンに設定する必要があります。
ステップ 3	**aaa new-model**	AAA を有効にします。
ステップ 4	**aaa group server tacacs+** *group-name*	（オプション）AAA サーバ グループをグループ名で定義します。 このコマンドは、アクセス ポイントをサーバ グループサブ設定モードに移行します。
ステップ 5	**server** *ip-address*	（オプション）特定の TACACS+ サーバを定義されたサーバ グループにアソシエートします。この手順を、AAA サーバ グループの各 TACACS+ サーバについて繰り返します。 グループ内の各サーバは、ステップ 2 であらかじめ定義されている必要があります。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show tacacs**	入力内容を確認します。
ステップ 8	**copy running-config startup-config**	（オプション）コンフィギュレーション ファイルに入力内容を保存します。

指定された TACACS+ サーバ名またはアドレスを削除するには、グローバル設定コマンド **no tacacs-server host** *hostname* を使用します。設定リストからサーバ グループを削除するには、グローバル設定コマンド **no aaa group server tacacs+** *group-name* を使用します。TACACS+ サーバの IP アドレスを削除するには、サーバ グループ サブ設定コマンド **no server ip-address** を使用します。

TACACS+ ログイン認証の設定

AAA 認証を設定するには、認証方式の名前付きリストを定義し、そのリストを各種のインターフェイスに適用します。この方式リストは、実行される認証のタイプと実行順序を定義したものです。定義されたいずれかの認証方式が実行されるようにするには、この方式リストを特定のインターフェイスに適用しておく必要があります。唯一の例外は、デフォルトの方式リスト（名前は、*default*）です。デフォルトの方式リストは、明示的に定義された名前付きの方式リストを持つインターフェイスを除くすべてのインターフェイスに自動的に適用されます。定義された方式リストは、デフォルトの方式リストよりも優先されます。

方式リストには、管理者を認証するクエリーのシーケンスと認証方式が記述されています。認証に使用するセキュリティ プロトコルを 1 つまたは複数指定できるため、最初の方法が失敗した場合でも認証のバックアップ システムが確実に機能します。ソフトウェアは、まずリストの最初の方式を使用してユーザを認証します。その方式が応答しなければ、方式リストの次の認証方式を選択します。このプロセスは、リスト内の認証方式との通信が成功するか、定義済みの方式をすべて試行するまで続けられます。このサイクルのどの認証にも失敗する場合、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が管理者のアクセスの拒否を応答した場合、認証プロセスは停止して、他の認証方式は試行されません。

特権 EXEC モードから、次の手順に従ってログイン認証を設定します。

	コマンド	目的
ステップ 1	**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 2	**aaa new-model**	AAA を有効にします。
ステップ 3	**aaa authentication login** {**default** | *list-name*} *method1* [*method2...*]	ログイン認証方式リストを作成します。 • **login authentication** コマンドで名前付きのリストが指定されていない場合に使用するデフォルトのリストを作成するには、**default** キーワードの後にデフォルトで使用する方式を指定します。デフォルトの方式リストは、自動的にすべてのインターフェイスに適用されます。 • *list-name* には、作成するリストに付ける名前の文字列を指定します。 • *method1...* には、認証アルゴリズムが試行する実際の方式を指定します。2 番目以降の認証方式が使用されるのは、その前の方式からエラーが返された場合に限られます。前の方式が失敗した場合ではありません。 次のいずれかの方式を選択します。 • **line**：認証に回線パスワードを使用します。この認証方式を使用する前に、回線パスワードを定義する必要があります。回線設定コマンド **username** *password* を使用します。 • **local**：認証にローカル ユーザ名データベースを使用します。データベースにユーザ名情報を入力する必要があります。グローバル設定コマンド **username** *password* を使用します。 • **tacacs+**：TACACS+ 認証を使用します。この認証方式を使用するには、事前に TACACS+ サーバを設定しておく必要があります。

	コマンド	目的
ステップ 4	**line** [**console** | **tty** | **vty**] *line-number* [*ending-line-number*]	回線設定モードを開始し、認証リストを適用する回線を設定します。
ステップ 5	**login authentication** {**default** | *list-name*}	認証リストを 1 つまたは複数の回線に適用します。 • **default** を指定すると、**aaa authentication login** コマンドで作成したデフォルト リストを使用します。 • *list-name* には、**aaa authentication login** コマンドで作成したリストを指定します。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show running-config**	入力内容を確認します。
ステップ 8	**copy running-config startup-config**	（オプション）コンフィギュレーション ファイルに入力内容を保存します。

AAA を無効にするには、グローバル設定コマンド **no aaa new-model** を使用します。AAA 認証を無効にするには、グローバル設定コマンド **no aaa authentication login** {**default** | *list-name*} *method1* [*method2...*] を使用します。ログイン時の TACACS+ 認証を無効にするか、デフォルト値に戻すには、回線設定コマンド **no login authentication** {**default** | *list-name*} を使用します。

特権 EXEC アクセスとネットワーク サービスの TACACS+ 許可の設定

AAA 許可は、管理者が使用できるサービスを制限します。AAA 許可が有効の場合、アクセス ポイントは管理者のプロファイルから取得した情報を使用して管理者のセッションを設定します。管理者のプロファイルは、ローカル ユーザ データベースかセキュリティ サーバにあります。管理者が要求したサービスへのアクセスが許可されるのは、管理者プロファイル内の情報により許可された場合だけです。

グローバル設定コマンド **aaa authorization** と **tacacs+** キーワードを使用すると、ユーザのネットワーク アクセスを特権 EXEC モードに制限するパラメータを設定できます。

これらの許可パラメータは、**aaa authorization exec tacacs+ local** コマンドで設定します。

- 認証に TACACS+ が使用された場合は、特権 EXEC アクセス許可に TACACS+ を使用します。
- 認証に TACACS+ を使用していない場合、ローカル データベースを使用します。

（注）　CLI を通してログインした認証済み管理者は、許可が設定されていても許可が省略されます。

特権 EXEC モードから、次の手順に従って特権 EXEC アクセスとネットワーク サービスに TACACS+ 許可を指定します。

	コマンド	目的
ステップ 1	**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 2	**aaa authorization network tacacs+**	ネットワーク関連のすべてのサービス要求に対して、管理者の TACACS+ 許可が受け入れられるようにアクセス ポイントを設定します。

	コマンド	目的
ステップ 3	**aaa authorization exec tacacs+**	管理者の TACACS+ 許可に管理者が特権 EXEC アクセス権を持っているかどうかを判断するように、アクセス ポイントを設定します。 **exec** キーワードにより、ユーザ プロファイル情報（**autocommand** 情報など）が返される場合があります。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	入力内容を確認します。
ステップ 6	**copy running-config startup-config**	（オプション）コンフィギュレーション ファイルに入力内容を保存します。

許可を無効にするには、グローバル設定コマンド **no aaa authorization** {**network** | **exec**} *method1* を使用します。

TACACS+ アカウンティングの起動

AAA アカウンティング機能は、管理者がアクセスしているサービスと、サービスが消費しているネットワーク リソースの量を追跡します。AAA アカウンティングが有効の場合、アクセス ポイントはアカウンティングの記録の形で管理者のアクティビティを TACACS+ セキュリティ サーバに報告します。各アカウンティングの記録にはアカウンティング属性と値のペア（AV）が含まれており、セキュリティ サーバに保存されます。その後このデータは、ネットワーク管理、クライアントへの課金、または監査のために分析されます。

特権 EXEC モードから、次の手順に従って Cisco IOS 特権レベルとネットワーク サービスに TACACS+ アカウンティングを有効にします。

	コマンド	目的
ステップ 1	**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 2	**aaa accounting network start-stop tacacs+**	ネットワーク関連のすべてのサービス要求に対して、TACACS+ アカウンティングを有効にします。
ステップ 3	**aaa accounting exec start-stop tacacs+**	TACACS+ アカウンティングを有効にして、特権 EXEC プロセスの開始時に start-record アカウンティング通知を送信し、終了時に stop-record アカウンティング通知を送信します。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	入力内容を確認します。
ステップ 6	**copy running-config startup-config**	（オプション）コンフィギュレーション ファイルに入力内容を保存します。

アカウンティングを無効にするには、グローバル設定コマンド **no aaa accounting** {**network** | **exec**} {**start-stop**} *method1...* を使用します。

TACACS+ 設定の表示

TACACS+ サーバ統計を表示するには、特権 EXEC コマンド **show tacacs** を使用します。