CHAPTER 13

RADIUS サーバと TACACS+ サーバの設定

この章では、リモート認証ダイヤルイン ユーザ サービス（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 ポイントをローカル認証サーバとして設定し、メイン サーバのバックアップとして使用したり、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したりできます。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については、第 11 章「認証タイプの設定」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については、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、不正なアクセスからネットワークのセキュリティを保護する分散クライアント/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。RADIUS ホストは、通常、シスコ（Cisco Secure Access Control Server バージョン 3.0）、Livingston、Merit、Microsoft などのソフトウェア プロバイダーの RADIUS サーバ ソフトウェアが稼働しているマルチユーザ システムです。詳細については、RADIUS サーバのマニュアル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 サーバによるネットワーク。たとえば、複数のベンダーのアクセス サーバが、1 つの RADIUS サーバベース 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 コントロール 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 を使用中のネットワーク。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 アカウンティングが必要なネットワーク。RADIUS 認証または許可とは別個に RADIUS アカウンティングを使用できます。RADIUS アカウンティング機能によって、サービスの開始および終了時点でデータを送信し、このセッション中に使用されるリソース（時間、パケット、バイトなど）の量を表示できます。インターネット サービス プロバイダーは、RADIUS アクセス コントロールおよびアカウンティング ソフトウェアのフリーウェア バージョンを使用して、特殊なセキュリティおよび課金に対するニーズを満たすこともできます。

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状態。RADIUS は、双方向認証を行いません。RADIUS は、他社製のデバイスが認証を必要とする場合に、あるデバイスから他社製のデバイスへの認証に使用できます。

- 各種のサービスを使用するネットワーク。RADIUS は、一般に 1 人のユーザを 1 つのサービス モデルにバインドします。

RADIUS の動作

無線ユーザが、RADIUS サーバによってアクセス コントロールされるアクセス 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 13-1 に示す手順で実行されます。

図 13-1　EAP 認証のシーケンス

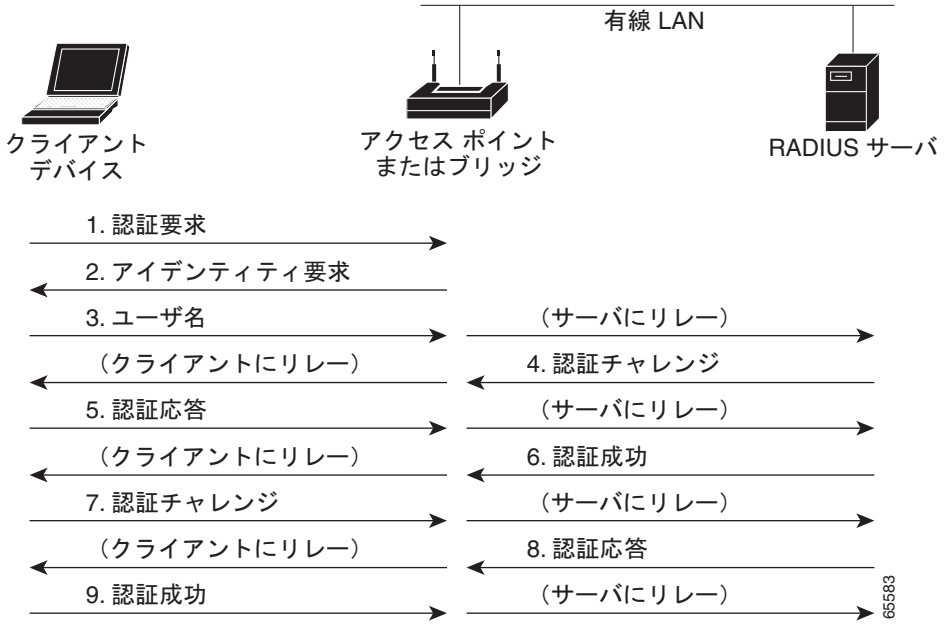

図 13-1 の手順 1 ～ 9 では、無線クライアント デバイスと有線 LAN 上の RADIUS サーバが 802.1x および EAP を使用して、アクセス ポイント経由で相互認証を実行します。RADIUS サーバは、認証身元証明要求をクライアントに送信します。クライアントはユーザが入力したパスワードを一方向暗号化し、認証身元証明要求に対する応答を生成して RADIUS サーバに送信します。RADIUS サーバは、サーバ自体のユーザ データベースの情報から独自の応答を生成し、クライアントからの応答と比較します。RADIUS サーバがクライアントを認証すると、同じ処理が逆方向から繰り返され、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 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、ログイン セッションでの使用に備えます。

ログイン 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。つまり、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」（P.11-10）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。最低限、RADIUS サーバ ソフトウェアが稼働するホスト（1 つまたは複数）を特定し、RADIUS 認証の方式リストを定義する必要があります。また、任意で RADIUS 許可およびアカウンティングの方式リストを定義できます。

方式リストによって、ユーザの認証、許可、またはアカウント維持のための順序と方式を定義します。方式リストを使用して、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ので、最初の方式が失敗した場合のバックアップ システムが確保されます。ソフトウェアは、リスト内の最初の方式を使用してユーザの認証、許可、アカウントの維持を行います。その方式で応答が得られなかった場合、ソフトウェアはそのリストから次の方式を選択します。このプロセスは、リスト内の方式による通信が成功するか、方式リストの方式をすべて試し終わるまで続きます。

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。

ここでは、次の設定情報について説明します。

- 「RADIUS のデフォルト設定」（P.13-4）
- 「RADIUS サーバ ホストの識別」（P.13-5）（必須）
- 「RADIUS ログイン認証の設定」（P.13-7）（必須）
- 「AAA サーバ グループの定義」（P.13-9）（任意）
- 「ユーザ特権アクセスおよびネットワーク サービスに関する RADIUS 許可の設定」（P.13-11）（任意）
- 「パケット オブ ディスコネクトの設定」（P.13-12）（任意）
- 「RADIUS アカウンティングの開始」（P.13-13）（任意）
- 「CSID 形式の選択」（P.13-14）（任意）
- 「すべての RADIUS サーバの設定」（P.13-15）（任意）
- 「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」（P.13-16）（任意）
- 「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」（P.13-17）（任意）
- 「WISPr RADIUS 属性の設定」（P.13-18）（任意）

（注）　RADIUS サーバの CLI 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。

RADIUS のデフォルト設定

RADIUS および AAA は、デフォルトではディセーブルに設定されています。

セキュリティの失効を防止するため、ネットワーク管理アプリケーションを使用して 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
- 認証の宛先ポート
- アカウンティングの宛先ポート
- キー文字列
- タイムアウト時間
- 再送信回数

RADIUS セキュリティ サーバは、ホスト名または IP アドレス、ホスト名と特定のユーザ データグラム プロトコル（UDP）ポート番号、または 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 ID を使用することによって、同じ IP アドレスにあるサーバ上の複数の UDP ポートに、RADIUS 要求を送信できます。

（注）　Cisco IOS Release 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 エントリのフェールオーバー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、設定した順序に従って試行されます）。

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 ストリングを使用して、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）ストリング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 コンフィギュレーション コマンド（**radius-server timeout**、**radius-server retransmit**、**radius-server key**）を使用します。これらの設定を特定の RADIUS サーバに適用するには、**radius-server host** グローバル コンフィギュレーション コマンドを使用します。

（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ー、再送信、キー値のコマンドがグローバルなタイマー、再送信、キー値のコマンドに優先します。すべての RADIUS サーバに対してこれらの値を設定するには、「すべての RADIUS サーバの設定」（P.13-15）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。詳細については、「AAA サーバ グループの定義」（P.13-9）を参照してください。

サーバ単位で RADIUS サーバとの通信を設定するには、特権 EXEC モードで次の手順を実行します。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 をイネーブルにします。
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。 • （任意）**auth-port** *port-number* には、認証要求の UDP 宛先ポートを指定します。このパラメータがない場合、デフォルトのポート番号は 1645 です。 • （任意）**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。このパラメータがない場合、デフォルトのポート番号は 1646 です。 • （任意）**timeout***seconds* には、アクセス ポイントが再送信する前に RADIUS サーバの応答を待つ時間を指定します。指定できる範囲は 1 ～ 1000 です。この設定は、**radius-server timeout** グローバル コンフィギュレーション コマンドによる設定を上書きします。**radius-server host** コマンドでタイムアウトを設定しない場合は、**radius-server timeout** コマンドの設定が使用されます。 • （任意）**retransmit** *retries* には、サーバが応答しない場合、または応答が遅い場合に、RADIUS 要求をサーバに再送信する回数を指定します。指定できる範囲は 1 ～ 1000 です。**radius-server host** コマンドで再送信回数を指定しない場合、**radius-server retransmit** グローバル コンフィギュレーション コマンドの設定が使用されます。 • （任意）**key** *string* には、アクセス ポイントと RADIUS サーバで稼働中の 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）** キーは、RADIUS サーバで使用する暗号化キーに一致するテキスト ストリングでなければなりません。キーは常に **radius-server host** コマンドの最後のアイテムとして設定してください。先頭のスペースは無視されますが、キーの中間および末尾のスペースは使用されます。キーにスペースを使用する場合は、引用符がキーの一部分である場合を除き、引用符でキーを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。各 RADIUS ホストで使用するタイムアウト、再送信回数、および暗号キーの値をそれぞれ設定してください。
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 コンフィギュレーション モードを開始します。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/en/US/docs/ios/12_2/security/configuration/guide/scfacct.html **（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 コンフィギュレーション モード **accounting** コマンドの詳細が表示されます。 http://www.cisco.com/en/US/docs/ios/wlan/command/reference/wl_book.html
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**	（任意）コンフィギュレーション ファイルに設定を保存します。

特定の RADIUS サーバを削除するには、**no radius-server host** {*hostname* | *ip-address*} グローバル コンフィギュレーション コマンドを使用します。

次に、1 つの RADIUS サーバを認証用に、もう 1 つの RADIUS サーバをアカウンティング用に設定する例を示します。

```
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
```

次に、*host1* を RADIUS サーバとして設定し、認証およびアカウンティングの両方にデフォルトのポートを使用するように設定する例を示します。

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

（注） RADIUS サーバ上でも、いくつかの値を設定する必要があります。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 ストリングが含まれます。詳細については、RADIUS サーバのマニュアル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（偶然に *default* と名前が付けられている）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。

方式リストは、ユーザ認証のためクエリ送信を行う手順と認証方式を記述したものです。認証に使用する 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、最初の方式が失敗した場合のバックアップ システムが確保されます。ソフトウェアは、リスト内の最初の方式を使用してユーザを認証し

ます。その方式で応答が得られなかった場合、ソフトウェアはそのリストから次の方式を選択します。このプロセスは、リスト内の認証方式による通信が成功するか、定義された方式をすべて試し終わるまで繰り返されます。この処理のある時点で認証が失敗した場合（つまり、セキュリティ サーバまたはローカルのユーザ名データベースがユーザ アクセスを拒否すると応答した場合）、認証プロセスは停止し、それ以上認証方式が試行されることはありません。

ログイン認証を設定するには、特権 EXEC モードで次の手順を実行します。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 をイネーブルにします。
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** コマンドに名前付きリストが指定*されなかった*場合に使用されるデフォルトのリストを作成するには、**default** キーワードの後ろにデフォルト状況で使用する方式を指定します。デフォルト認証方式リストは、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。追加の認証方式は、その前の方式でエラーが返された場合に限り使用されます。前の方式が失敗した場合は使用されません。 次のいずれかの方式を選択します。 • **line**：回線パスワードを認証に使用します。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。**password** *password* ライン コンフィギュレーション コマンドを使用します。 • **local**：ローカル ユーザ名データベースを認証に使用します。データベースにユーザ名情報を入力しておく必要があります。**username** *password* グローバル コンフィギュレーション コマンドを使用します。 • **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。詳細については、「RADIUS サーバ ホストの識別」（P.13-5）を参照してください。
ステップ 4	**line** [**console** | **tty** | **vty**] *line-number* [*ending-line-number*]	ライン コンフィギュレーション モードを開始し、認証リストの適用対象とする回線を設定します。
ステップ 5	**login authentication** {**default** | *list-name*}	回線または回線セットに対して、認証リストを適用します。 • **default** を指定する場合は、**aaa authentication login** コマンドで作成したデフォルトの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**	（任意）コンフィギュレーション ファイルに設定を保存します。

AAA をディセーブルにするには、**no aaa new-model** グローバル コンフィギュレーション コマンドを使用します。AAA 認証をディセーブルにするには、**no aaa authentication login** {**default** | *list-name*} *method1* [*method2...*] グローバル コンフィギュレーション コマンドを使用します。ログインに関する RADIUS 認証をディセーブルにする、あるいはデフォルト値に戻すには、**no login authentication** {**default** | *list-name*} ライン コンフィギュレーション コマンドを使用します。

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。設定済みのサーバ ホストのサブセットを選択して、それを特定のサービスに使用します。サーバ グループは、選択されたサーバ ホストの IP アドレスのリストを含むグローバルなサーバ ホスト リストとともに使用されます。

サーバ グループには、同じサーバの複数のホスト エントリを含めることもできますが、各エントリが一意の ID（IP アドレスと UDP ポート番号の組み合わせ）を持っていることが条件です。この場合、個々のポートをそれぞれ特定の AAA サービスを提供する RADIUS ホストとして定義できます。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 エントリのフェールオーバー時のバックアップとして機能します。

定義したグループ サーバに特定のサーバを対応付けるには、**server** グループ サーバ コンフィギュレーション コマンドを使用します。サーバを IP アドレスで特定することもできますし、任意指定の **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することもできます。

AAA サーバ グループを定義し、そのグループに特定の RADIUS サーバを対応付けるには、特権 EXEC モードで次の手順を実行します。

	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	**aaa new-model**	AAA をイネーブルにします。

	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。 • （任意）**auth-port** *port-number* には、認証要求の UDP 宛先ポートを指定します。 • （任意）**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。 • （任意）**timeout***seconds* には、アクセス ポイントが再送信する前に RADIUS サーバの応答を待つ時間を指定します。指定できる範囲は 1 ～ 1000 です。この設定は、**radius-server timeout** グローバル コンフィギュレーション コマンドによる設定を上書きします。**radius-server host** コマンドでタイムアウトを設定しない場合は、**radius-server timeout** コマンドの設定が使用されます。 • （任意）**retransmit** *retries* には、サーバが応答しない場合、または応答が遅い場合に、RADIUS 要求をサーバに再送信する回数を指定します。指定できる範囲は 1 ～ 1000 です。**radius-server host** コマンドで再送信回数を指定しない場合、**radius-server retransmit** グローバル コンフィギュレーション コマンドの設定が使用されます。 • （任意）**key** *string* には、アクセス ポイントと RADIUS サーバで稼働中の 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）** キーは、RADIUS サーバで使用する暗号化キーに一致するテキスト ストリングでなければなりません。キーは常に **radius-server host** コマンドの最後のアイテムとして設定してください。先頭のスペースは無視されますが、キーの中間および末尾のスペースは使用されます。キーにスペースを使用する場合は、引用符がキーの一部分である場合を除き、引用符でキーを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。各 RADIUS ホストで使用するタイムアウト、再送信回数、および暗号キーの値をそれぞれ設定してください。
ステップ 4	**aaa group server radius** *group-name*	AAA サーバ グループを、特定の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 コンフィギュレーション モードへ移行します。
ステップ 5	**server** *ip-address*	特定の RADIUS サーバを定義済みのサーバ グループに対応付けます。AAA サーバ グループの RADIUS サーバごとに、このステップを繰り返します。 グループの各サーバは、ステップ 2 で定義済みのものでなければなりません。
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。

	コマンド	目的
ステップ 8	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。
ステップ 9		RADIUS ログイン認証をイネーブルにします。「RADIUS ログイン認証の設定」（P.13-7）を参照してください。

特定の RADIUS サーバを削除するには、**no radius-server host** {*hostname* | *ip-address*} グローバル コンフィギュレーション コマンドを使用します。サーバ グループをコンフィギュレーション リストから削除するには、**no aaa group server radius** *group-name* グローバル コンフィギュレーション コマンドを使用します。RADIUS サーバの IP アドレスを削除するには、**no server** *ip-address* サーバ グループ コンフィギュレーション コマンドを使用します。

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 では、同じ RADIUS サーバ上の異なる 2 つのホスト エントリを、同じサービス用に設定しています。2 番目のホスト エントリが、最初の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。

```
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およびネットワーク サービスに関する RADIUS 許可の設定

AAA 許可によってユーザが使用できるサービスが制限されます。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。ユーザは、ユーザ プロファイル内の情報で認められている場合に限り、要求したサービスのアクセスが認可されます。

（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。

特権 EXEC モードへのユーザのネットワーク アクセスを制限するパラメータを設定するには、**radius** キーワードを指定して **aaa authorization** グローバル コンフィギュレーション コマンドを使用します。

aaa authorization exec radius local コマンドは、次の許可パラメータを設定します。

- RADIUS を使用して認証を行った場合は、RADIUS を使用して特権 EXEC アクセスを許可します。
- 認証に RADIUS を使用しなかった場合は、ローカル データベースを使用します。

（注）　許可が設定されていても、CLI を使用してログインし、認証されたユーザに対しては、許可は省略されます。

特権 EXEC アクセスおよびネットワーク サービスに関する RADIUS 許可を指定するには、特権 EXEC モードで次の手順を実行します。

	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	**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。
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** キーワードを指定すると、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**	（任意）コンフィギュレーション ファイルに設定を保存します。

許可をディセーブルにするには、**no aaa authorization** {**network** | **exec**} *method1* グローバル コンフィギュレーション コマンドを使用します。

パケット オブ ディスコネクトの設定

Packet of Disconnect（PoD; パケット オブ ディスコネクト）は、ディスコネクト メッセージとも呼ばれています。PoD の詳細は、Internet Engineering Task Force（IETF; インターネット技術特別調査委員会）Internet Standard RFC 3576 で参照できます。

パケット オブ ディスコネクトは、検出されたセッションを終了させる方式で構成されています。PoD は RADIUS Disconnect_Request パケットであり、RADIUS access_accept パケットによりセッションが承認された後、認証するエージェント サーバがユーザを接続解除するときに使用されるようになっています。これが必要な場合としては、少なくとも次の 2 つの状況が考えられます。

- 不正使用の検出。これは、コールを承認後でなければ実行できません。
- プリペイド アクセス時間が切れたホット スポット ユーザの切断。

セッションが終了すると、RADIUS サーバは Network Access Server（NAS; ネットワーク アクセス サーバ）（WDS またはアクセス ポイント）に切断メッセージを送信します。802.11 セッションには、Pod 要求で Calling-Station-ID [31] RADIUS 属性（クライアントの MAC アドレス）を指定する必要があります。アクセス ポイントまたは WDS は、関連するセッションのアソシエーションを解除しようとし、次に接続解除応答メッセージを RADIUS サーバに返送します。メッセージ タイプは次のとおりです。

- 40：切断要求
- 41：切断：ACK
- 42：切断：NAK

（注） PoD 要求の設定法については、ご使用の RADIUS サーバ アプリケーションの資料を参照してください。

（注）　アクセス ポイントは、再アソシエートしようとするクライアントの次の試みを妨害しません。PoD 要求を発行する前にクライアントのアカウントを無効にするのは、セキュリティ管理者の責任です。

（注）　WDS を設定すると、PoD 要求は WDS に対して発行されます。WDS はアソシエーション解除の要求を親アクセス ポイントに転送してから、そのセッションを自身の内部テーブルから削除します。

（注）　PoD は Cisco CNS Access Registrar（CAR）RADIUS サーバでサポートされていますが、Cisco Secure ACS Server v4.0 以前ではサポートされていません。

特権 EXEC モードから、次の手順に従って PoD 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 pod server** [**port** *port number*] [**auth-type** {**any** | **all** | **session-key**}] [**clients** *client 1...*] [**ignore** {**server-key** *string...*| **session-key** }] | **server-key** *string...*]}	特定のセッション属性が提供されると、RADIUS サーバからの要求により切断されるユーザ セッションを有効にします。 **port** *port number*：（任意）アクセス ポイントが PoD 要求をリッスンする UDP ポート。デフォルト値は 1700 です。 **auth-type**：このパラメータは、802.11 セッションに対してはサポートされません。 **clients**（任意）：4 台までの RADIUS サーバをクライアントとして指名できます。この設定が存在し、リストにないデバイスからの PoD 要求が発信される場合、拒否されます。 **ignore**（任意）：*server_key* に設定すると、PoD 要求を受信したときに共有の身元証明要求は検証されません。 **session-key**：802.11 セッションに対してはサポートされません。 **server-key**：共有秘密テキスト ストリングを設定します。 *string*：ネットワーク アクセス サーバとクライアント ワークステーション間で共有される事前共有キー。この共有身元証明要求は両方のシステムで同一である必要があります。 （注）　このパラメータ以降に入力されたデータは、共有の身元証明要求ストリングとして扱われます。
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**	入力内容を確認します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

RADIUS アカウンティングの開始

AAA アカウンティング機能は、ユーザがアクセスしたサービスと、消費したネットワーク リソース量をトラッキングします。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 レコードにはアカウンティングの Attribute-Value（AV）ペアが含まれ、レコードはセキュリティ サーバに格納されます。このデータを、ネットワーク管理、クライアント請求、または監査のために分

析できます。アクセス ポイントに送信される属性の詳細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」（P.13-20）を参照してください。

Cisco IOS の権限レベルおよびネットワーク サービスに関する RADIUS アカウンティングをイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	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	**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ついて、RADIUS アカウンティングをイネーブルにします。
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**	（任意）コンフィギュレーション ファイルに設定を保存します。

アカウンティングをディセーブルにするには、**no aaa accounting** {**network** | **exec**} {**start-stop**} *method1...* グローバル コンフィギュレーション コマンドを使用します。

CSID 形式の選択

RADIUS パケット内の Called-Station-ID（CSID）および Calling-Station-ID 属性に対する MAC アドレスの形式を選択できます。**dot11 aaa csid** 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 CSID 形式を選択します。表 13-1 は、対応する MAC アドレスの例付きで示した形式のオプションです。

表 13-1　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 ストリングを指定します。 **（注）** キーは、RADIUS サーバで使用する暗号化キーに一致するテキスト ストリングでなければなりません。先頭のスペースは無視されますが、キーの中間および末尾のスペースは使用されます。キーにスペースを使用する場合は、引用符がキーの一部分である場合を除き、引用符でキーを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 です。指定できる範囲は 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 秒です。指定できる範囲は 1 ～ 1000 です。
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）** このコマンドは、複数の RADIUS サーバを定義するときに必要な設定です。設定しない場合、クライアントの認証が行われません。定義される RADIUS サーバが 1 台の場合、このコマンドはオプションです。
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**	設定値を確認します。
ステップ 9	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

次の例では、2 つのメイン サーバとローカル認証サーバについて、サーバのデッド タイムを 10 分間に設定する方法を示します。

```
AP(config)# aaa new-model

AP(config)# radius-server host 172.20.0.1 auth-port 1000 acct-port 1001 key 77654

AP(config)# radius-server host 172.10.0.1 auth-port 1645 acct-port 1646 key 77654

AP(config)# radius-server host 10.91.6.151 auth-port 1812 acct-port 1813 key 110337

AP(config)# radius-server deadtime 10
```

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** 形式を使用します。

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; インターネット技術特別調査委員会）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。各ベンダーは、Vendor-Specific Attribute（VSA）を使用することによって、一般的な用途には適さない独自の拡張属性をサポートできます。シスコが実装する RADIUS では、この仕様で推奨されるフォーマットを使用して、ベンダー固有のオプションを 1 つサポートしています。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、次のフォーマットのストリングです。

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

protocol は、特定の許可タイプに使用するシスコの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、ユーザがアクセス 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 の詳細については、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。 • （任意）認識されるベンダー固有属性の集合をアカウンティング属性だけに限定するには、**accounting** キーワードを使用します。 • （任意）認識されるベンダー固有属性の集合を認証属性だけに限定するには、**authentication** キーワードを使用します。 キーワードを指定せずにこのコマンドを入力すると、アカウンティングおよび認証のベンダー固有属性の両方が使用されます。
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**	設定値を確認します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

RADIUS 属性の詳細なリスト、または VSA 26 の詳細については、『*Cisco IOS Security Configuration Guide for Release 12.2*』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、ベンダー独自仕様の RADIUS 属性のサブセットをサポートしています。

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 ホストおよびシークレット テキスト ストリングを指定するには、**radius-server** グローバル コンフィギュレーション コマンドを使用します。

ベンダー独自仕様の RADIUS サーバ ホスト、および共有されるシークレット テキスト ストリングを指定するには、特権 EXEC モードで次の手順を実行します。

	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 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 ストリングを指定します。アクセス ポイントと RADIUS サーバは、このテキスト ストリングを使用して、パスワードを暗号化し応答を交換します。 **（注）** キーは、RADIUS サーバで使用する暗号化キーに一致するテキスト ストリングでなければなりません。先頭のスペースは無視されますが、キーの中間および末尾のスペースは使用されます。キーにスペースを使用する場合は、引用符がキーの一部分である場合を除き、引用符でキーを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**	設定値を確認します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

ベンダー独自仕様の RADIUS ホストを削除するには、**no radius-server host** {*hostname* | *ip-address*} **non-standard** グローバル コンフィギュレーション コマンド を使用します。キーをディセーブルにするには、**no radius-server key** グローバル コンフィギュレーション コマンドを使用します。

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キー *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 アライアンスの資料である『*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; 国際電気通信連合）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、『*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ため、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。『*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**	設定値を確認します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

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 ストリング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 の設定の表示

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

（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 13-2 から 表 13-6 は、アクセス ポイントがクライアントに送信するアクセス要求、アクセス許可、アカウンティング要求パケット中の属性を示しています。

（注）　Wi-Fi アライアンスの資料『*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、「WISPr RADIUS 属性の設定」（P.13-18）を参照してください。

表 13-2　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 13-3　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. RFC2868、VLAN オーバーライド番号を定義

表 13-4　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 13-5　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 13-6　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確実に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 コンフィギュレーション 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

ここでは、次の設定情報について説明します。

- 「TACACS+ の概要」（P.13-23）
- 「TACACS+ の動作」（P.13-23）
- 「TACACS+ の設定」（P.13-24）
- 「TACACS+ 設定の表示」（P.13-28）

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上で稼働する TACACS+ デーモンのデータベースで管理されます。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+ 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+ では、単一のアクセス コントロール サーバ（TACACS+ デーモン）が各サービス（認証、許可、およびアカウンティング）を別個に提供します。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使用できます。

TACACS+ は、AAA セキュリティ サービスによって管理され、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 コントロール、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、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 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ため、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+ の動作

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を入力するよう求めますが、ユーザの母親の旧姓など、その他の項目を含めることもできます。

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+ 許可が必要な場合は、再び TACACS+ デーモンに接続し、デーモンが ACCEPT または 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。最低限、TACACS+ デーモンを維持するホスト（1 つまたは複数）を特定し、TACACS+ 認証の方式リストを定義する必要があります。また、任意で TACACS+ 許可および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、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ので、最初の方式が失敗した場合のバックアップ システムが確保されます。このソフトウェアは、リストの先頭の方式を使用して管理者のアカウントを認証、許可、または管理します。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、リスト内の方式による通信が成功するか、方式リストの方式をすべて試し終わるまで続きます。

ここでは、次の設定情報について説明します。

- 「TACACS+ のデフォルト設定」（P.13-24）
- 「TACACS+ サーバ ホストの特定および認証キーの設定」（P.13-25）
- 「TACACS+ ログイン認証の設定」（P.13-26）
- 「特権 EXEC アクセスおよびネットワーク サービス用の TACACS+ 許可の設定」（P.13-27）
- 「TACACS+ アカウンティングの起動」（P.13-28）

TACACS+ のデフォルト設定

TACACS+ および AAA は、デフォルトではディセーブルに設定されています。

セキュリティの失効を防止するため、ネットワーク管理アプリケーションを使用して 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 ホストの特定および認証キーの設定

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て設定済みサーバ ホストのサブセットを選択し、特定のサービスにそのサーバを使用できます。サーバ グループは、グローバル サーバ ホスト リストとともに使用され、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ています。

TACACS+ サーバを維持する IP ホストを特定し、任意で暗号キーを設定するには、特権 EXEC モードで次の手順を実行します。

	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	**tacacs-server host** *hostname* [**port** *integer*] [**timeout** *integer*] [**key** *string*]	TACACS+ サーバを維持する IP ホスト（1 つまたは複数）を特定します。このコマンドを複数回入力して、優先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。 • （任意）**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 です。指定できる範囲は 1 ～ 65535 です。 • （任意）**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。デフォルトは 5 秒です。指定できる範囲は 1 ～ 1000 秒です。 • （任意）**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。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。
ステップ 3	**aaa new-model**	AAA をイネーブルにします。
ステップ 4	**aaa group server tacacs+** *group-name*	（任意）AAA サーバ グループを、特定の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 グループサブコンフィギュレーション モードに移行します。
ステップ 5	**server** *ip-address*	（任意）特定の TACACS+ サーバを定義済みのサーバ グループに対応付けます。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。 グループの各サーバは、ステップ 2 で定義済みのものでなければなりません。
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**	（任意）コンフィギュレーション ファイルに設定を保存します。

指定された TACACS+ サーバ名またはアドレスを削除するには、**no tacacs-server host** *hostname* グローバル コンフィギュレーション コマンドを使用します。サーバ グループをコンフィギュレーション リストから削除するには、**no aaa group server tacacs+** *group-name* グローバル コンフィギュレーション コマンドを使用します。TACACS+ サーバの IP アドレスを削除するには、**no server ip-address** サーバ グループ サブコンフィギュレーション コマンドを使用します。

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（偶然に *default* と名前が付けられている）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。

方式リストには、管理者を認証するクエリ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 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、最初の方式が失敗した場合のバックアップ システムが確保されます。ソフトウェアは、リスト内の最初の方式を使用してユーザを認証します。その方式で応答が得られなかった場合、ソフトウェアはそのリストから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による通信が成功するか、定義された方式をすべて試し終わるまで繰り返されます。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アクセス権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。

ログイン認証を設定するには、特権 EXEC モードで次の手順を実行します。

	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	**aaa new-model**	AAA をイネーブルにします。
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** コマンドに名前付きリストが指定*されなかった*場合に使用されるデフォルトのリストを作成するには、**default** キーワードの後ろにデフォルト状況で使用する方式を指定します。デフォルト認証方式リストは、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、作成するリストの名前として使用する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。追加の認証方式は、その前の方式でエラーが返された場合に限り使用されます。前の方式が失敗した場合は使用されません。 次のいずれかの方式を選択します。 • **line**：回線パスワードを認証に使用します。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。**password** *password* ライン コンフィギュレーション コマンドを使用します。 • **local**：ローカル ユーザ名データベースを認証に使用します。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。**username** *password* グローバル コンフィギュレーション コマンドを使用します。 • **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。
ステップ 4	**line** [**console** | **tty** | **vty**] *line-number* [*ending-line-number*]	ライン コンフィギュレーション モードを開始し、認証リストの適用対象と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*}	回線または回線セットに対して、認証リストを適用します。 • **default** を指定する場合は、**aaa authentication login** コマンドで作成したデフォルトの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**	（任意）コンフィギュレーション ファイルに設定を保存します。

AAA をディセーブルにするには、**no aaa new-model** グローバル コンフィギュレーション コマンドを使用します。AAA 認証をディセーブルにするには、**no aaa authentication login** {**default** | *list-name*} *method1* [*method2...*] グローバル コンフィギュレーション コマンドを使用します。ログインに関する TACACS+ 認証をディセーブルにする、あるいはデフォルト値に戻すには、**no login authentication** {**default** | *list-name*} ライン コンフィギュレーション コマンドを使用します。

特権 EXEC アクセスおよびネットワーク サービス用の 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。

aaa authorization グローバル コンフィギュレーション コマンドと **tacacs+** キーワードを使用すると、管理者のネットワーク 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。

aaa authorization exec tacacs+ local コマンドは、次の許可パラメータを設定します。

- TACACS+ を使用して認証を行った場合は、TACACS+ を使用して特権 EXEC アクセスを許可します。
- 認証に TACACS+ を使用しなかった場合は、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 アクセスおよびネットワーク サービスに関する TACACS+ 許可を指定するには、特権 EXEC モードで次の手順を実行します。

	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	**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。
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** キーワードを指定すると、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。

	コマンド	目的
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**	（任意）コンフィギュレーション ファイルに設定を保存します。

許可をディセーブルにするには、**no aaa authorization** {**network** | **exec**} *method1* グローバル コンフィギュレーション コマンドを使用します。

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 レコードにはアカウンティングの Attribute-Value（AV）ペアが含まれ、レコードはセキュリティ サーバに格納されます。このデータを、ネットワーク管理、クライアント請求、または監査のために分析できます。

Cisco IOS の権限レベルおよびネットワーク サービスに関する TACACS+ アカウンティングをイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	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	**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ついて、TACACS+ アカウンティングをイネーブルにします。
ステップ 3	**aaa accounting exec start-stop tacacs+**	TACACS+ アカウンティングにより、特権 EXEC プロセスの最初に記録開始アカウンティング通知、最後に記録停止通知を送信するように設定します。
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**	入力内容を確認します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

アカウンティングをディセーブルにするには、**no aaa accounting** {**network** | **exec**} {**start-stop**} *method1...* グローバル コンフィギュレーション コマンドを使用します。

TACACS+ 設定の表示

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