アクセス ポイントの管理

この章では、無線デバイスの管理方法について説明します。この章の内容は、次のとおりです。

アクセス ポイントへの不正アクセスの防止

権限のないユーザが無線デバイスの設定を変更したり、設定情報を表示したりするのを防ぐことができます。通常は、ネットワーク管理者から無線デバイスへのアクセスを許可し、ローカル ネットワーク内の端末またはワークステーションから接続するユーザのアクセスは制限します。

無線デバイスへの不正なアクセスを防ぐには、次のいずれかのセキュリティ機能を設定してください。

- 無線デバイスでローカルに保存されるユーザ名とパスワードの組み合わせ。この組み合わせによって、各ユーザは無線デバイスにアクセスする前に認証されます。また、特定の特権レベル（読み取り専用または読み取り / 書き込み）をユーザ名とパスワードのそれぞれの組み合わせに指定できます。詳細は、「ユーザ名とパスワードの組み合わせの設定」の項（P.5-6）を参照してください。デフォルトのユーザ名は *Cisco*、デフォルトのパスワードは *Cisco* です。ユーザ名とパスワードでは、大文字と小文字が区別されます。
- セキュリティ　サーバのデータベースに集中的に保存されたユーザ名とパスワードの組み合わせ。詳細は、「RADIUS によるアクセス ポイントへのアクセスの制御」の項（P.5-9）を参照してください。

特権 EXEC コマンドへのアクセス防止

ネットワークで端末のアクセスを制御する簡単な方法として、パスワードの使用と特権レベルの割り当てがあります。パスワード保護は、ネットワークまたはネットワーク デバイスへのアクセスを制限します。特権レベルは、ユーザがネットワーク デバイスにログインした後に発行できるコマンドを定義します。

（注）　この項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。

この項では、コンフィギュレーション ファイルと特権 EXEC コマンドへのアクセスを制御する方法について説明します。内容は次のとおりです。

デフォルト パスワードと特権レベルの設定

表 5-1 にデフォルト パスワードと特権レベルの設定を示します。

表 5-1　デフォルト パスワードと特権レベル

機能	デフォルト設定
ユーザ名とパスワード	デフォルトのユーザ名は *Cisco*、デフォルトのパスワードは *Cisco* です。
イネーブル パスワードと特権レベル	デフォルトのパスワードは *Cisco* です。デフォルトはレベル 15（特権 EXEC レベル）です。パスワードはコンフィギュレーション ファイルで暗号化されます。
イネーブル シークレット パスワードと特権レベル	デフォルトのイネーブル パスワードは *Cisco* です。デフォルトはレベル 15（特権 EXEC レベル）です。パスワードはコンフィギュレーション ファイルに書き込まれる前に暗号化されます。
回線パスワード	デフォルトのパスワードは *Cisco* です。パスワードはコンフィギュレーション ファイルで暗号化されます。

静的イネーブル パスワードの設定または変更

イネーブル パスワードは、特権 EXEC モードへのアクセスを制御します。

（注）　グローバル設定コマンド **no enable password** は、イネーブル パスワードを削除しますが、このコマンドを使用する場合は十分な注意が必要です。イネーブル パスワードを削除すると、EXEC モードからロックアウトされます。

特権 EXEC モードから、次の手順に従って静的イネーブル パスワードを設定または変更します。

	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	**enable password** *password*	特権 EXEC モードにアクセスするための新しいパスワードを定義するか、既存のパスワードを変更します。 デフォルトのパスワードは *Cisco* です。 *password* には 1 ～ 25 文字の英数字からなる文字列を指定します。文字列を数字で始めることはできず、大文字と小文字は区別されます。また、スペースを使用できますが、先頭のスペースは無視されます。パスワードにクエスチョン マーク（?）を含めることができます。その場合はパスワードを作成するとき、クエスチョン マークを入力する前に Ctrl+V キーを押してください。たとえば、パスワード abc?123 を作成する場合は、次のように入力します。 **1.** **abc** を入力します。 **1.** **Crtl+V** を入力します。 **2.** **?123** を入力します。 イネーブル パスワードの入力を求められたときは、クエスチョン マークの前で Ctrl+V キーを押す必要はありません。パスワード プロンプトで単純に abc?123 と入力します。
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**	（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。 イネーブル パスワードは暗号化されず、無線デバイスのコンフィギュレーション ファイルで読み取ることができます。

次の例は、イネーブル パスワードを *l1u2c3k4y5* に変更する方法を示しています。パスワードは暗号化されず、レベル 15 へのアクセス（従来の特権 EXEC モードへのアクセス）を可能にします。

```
AP(config)# enable password l1u2c3k4y5
```

暗号化によるイネーブル パスワードとイネーブル シークレット パスワードの保護

セキュリティ レベルを強化するために、特にネットワークを越えるパスワードや Trivial File Transfer Protocol（TFTP; 簡易ファイル転送プロトコル）サーバに保存されたパスワードについて、グローバル設定コマンド **enable password** または **enable secret** を使用できます。どちらのコマンドを使っても、ユーザが特権 EXEC モード（デフォルト）または指定した特権レベルにアクセスする場合に入力が要求される暗号化パスワードを設定できます。

より高度な暗号化アルゴリズムを使用しているので、**enable secret** コマンドの使用をお勧めします。

enable secret コマンドを設定する場合、**enable password** コマンドよりも優先されます。2 つのコマンドを同時に有効にはできません。

特権 EXEC モードから、次の手順に従ってイネーブル パスワードとイネーブル シークレット パスワードに暗号化を設定します。

	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	**enable password** [**level** *level*] {*password* | *encryption-type encrypted-password*} または **enable secret** [**level** *level*] {*password* | *encryption-type encrypted-password*}	特権 EXEC モードにアクセスするための新しいパスワードを定義するか、既存のパスワードを変更します。 または シークレット パスワードを定義します。これは非可逆的暗号化方式を使用して保存されます。 • （オプション）*level* の指定範囲は 0 ～ 15 です。レベル 1 は通常のユーザ EXEC モードの特権です。デフォルトのレベルは 15（特権 EXEC モードの特権）です。 • *password* には 1 ～ 25 文字の英数字からなる文字列を指定します。文字列を数字で始めることはできず、大文字と小文字は区別されます。また、スペースを使用できますが、先頭のスペースは無視されます。デフォルトでは、パスワードは定義されていません。 • （オプション）*encryption-type* には、タイプ 5（シスコ独自の暗号化アルゴリズム）だけが指定できます。暗号化タイプを指定する場合は、別のアクセス ポイントの設定からコピーした暗号化パスワードを指定する必要があります。 （注）　暗号化タイプを指定し、クリア テキスト パスワードを入力すると、特権 EXEC モードを再開できません。失われた暗号化パスワードはどのような方法でも復元できません。
ステップ 3	**service password-encryption**	（オプション）パスワードの定義時または設定の書き込み時にパスワードを暗号化します。 暗号化により、パスワードをコンフィギュレーション ファイルで読み取ることができなくなります。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**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。

イネーブル パスワードとイネーブル シークレット パスワードが両方とも定義されている場合、ユーザはイネーブル シークレット パスワードの方を入力する必要があります。

特定の特権レベル用のパスワードを定義するには、**level** キーワードを指定します。レベルを指定し、パスワードを設定した後、このレベルでアクセスする必要のあるユーザだけにパスワードを与えてください。任意のレベルでアクセスできるコマンドを指定する場合は、グローバル設定コマンド **privilege level** を使用します。詳細は、「複数の特権レベルの設定」の項（P.5-7）を参照してください。

パスワードの暗号化を有効にすると、ユーザ名パスワード、認証キー パスワード、特権コマンド パスワード、コンソールと仮想端末の回線パスワードを含むすべてのパスワードに適用されます。

パスワードとレベルを削除するには、グローバル設定コマンド **no enable password** [**level** *level*] または **no enable secret** [**level** *level*] を使用します。パスワードの暗号化を無効にするには、グローバル設定コマンド **no service password-encryption** を使用します。

次の例は、特権レベル 2 の暗号化パスワード *1FaD0$Xyti5Rkls3LoyxzS8* を設定する方法を示しています。

```
AP(config)# enable secret level 2 5 $1$FaD0$Xyti5Rkls3LoyxzS8
```

ユーザ名とパスワードの組み合わせの設定

ユーザ名とパスワードの組み合わせを設定できます。これは、無線デバイスでローカルに保存されます。ユーザ名とパスワードの組み合わせは、回線またはインターフェイスに割り当てられ、各ユーザが無線デバイスにアクセスする際の認証に使用されます。特権レベルを定義している場合、ユーザ名とパスワードのそれぞれの組み合わせに特定の特権レベル（アソシエートされている権利と特権を含む）を割り当てることができます。

特権 EXEC モードから、次の手順に従って、ログイン ユーザ名とパスワードを要求するユーザ名ベースの認証システムを設定します。

	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	**username** *name* [**privilege** *level*] {**password** *encryption-type password*}	各ユーザのユーザ名、特権レベル、パスワードを入力します。 • *name* には、ユーザ ID を 1 ワードで指定します。空白と引用符は使用できません。 • （オプション）*level* には、ユーザがアクセス後に取得する特権レベルを指定します。指定範囲は 0 ～ 15 です。レベル 15 は特権 EXEC モードのアクセスを許可します。レベル 1 はユーザ EXEC モードのアクセスを許可します。 • *encryption-type* には、後ろに暗号化されていないパスワードが続くことを指定する場合は 0 を入力します。非表示のパスワードが続くことを指定するには 7 を入力します。 • *password* には、無線デバイスへアクセスするためにユーザが入力しなければならないパスワードを指定します。パスワードは 1 ～ 25 文字の間で指定します。空白を入れることもできます。また、パスワードは必ず **username** コマンドの最後のオプションとして指定してください。
ステップ 3	**login local**	ログイン時にローカル パスワードのチェック機能を有効にします。認証はステップ 2 で指定したユーザ名に基づいて実行されます。
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。

特定のユーザに対してユーザ名の認証を無効にするには、グローバル設定コマンド **no username** *name* を使用します。

パスワード チェック機能を無効にし、パスワードを指定しない接続を許可する場合は、回線設定コマンド **no login** を使用します。

（注）　ユーザ名は 1 つ以上設定しなければなりません。また、login local を無線デバイスとの Telnet セッションを開くように設定する必要があります。ユーザ名が 1 つだけの場合にそのユーザ名を入力しないと、無線デバイスからロックアウトされることがあります。

複数の特権レベルの設定

デフォルトでは、Cisco IOS ソフトウェアにはユーザ EXEC モードと特権 EXEC モードという 2 つのパスワード セキュリティのモードがあります。各モードにコマンドの階層を最大 16 レベルまで設定できます。複数のパスワードを設定すると、ユーザ グループ別に特定のコマンド群へのアクセスを許可できます。

たとえば、**clear line** コマンドへのアクセスを多くのユーザに許可する場合は、このコマンドにレベル 2 のセキュリティを指定し、レベル 2 のパスワードを広く配布します。一方、**configure** コマンドについては、アクセスをもう少し制限する場合、このコマンドにレベル 3 のセキュリティを指定し、より限られたユーザ グループにレベル 3 のパスワードを配布します。

この項では設定情報を扱います。

- コマンドに対する特権レベルの設定（P. 5-7）
- 特権レベルへのログインと終了（P. 5-8）

コマンドに対する特権レベルの設定

特権 EXEC モードから、次の手順に従って特定のコマンド モードに特権レベルを設定します。

	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	**privilege** *mode* **level** *level command*	コマンドに特権レベルを設定します。 • *mode* には、グローバル コンフィギュレーション モードの場合は **configure** を、EXEC モードの場合は **exec** を、インターフェイス設定モードの場合は **interface** を、回線設定モードの場合は **line** を入力します。 • *level* の指定範囲は 0 ～ 15 です。レベル 1 は通常のユーザ EXEC モードの特権です。レベル 15 は**イネーブル** パスワードで許可されるアクセス レベルです。 • *command* にはアクセスを制限するコマンドを指定します。
ステップ 3	**enable password level** *level password*	特権レベルにイネーブル パスワードを指定します。 • *level* の指定範囲は 0 ～ 15 です。レベル 1 は通常のユーザ EXEC モードの特権です。 • *password* には 1 ～ 25 文字の英数字からなる文字列を指定します。文字列を数字で始めることはできず、大文字と小文字は区別されます。また、スペースを使用できますが、先頭のスペースは無視されます。デフォルトでは、パスワードは定義されていません。
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** または **show privilege**	入力内容を確認します。 最初のコマンドは、パスワードとアクセス レベルの設定を表示します。2 番目のコマンドは、特権レベルの設定を表示します。
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。

コマンドに特権レベルを設定すると、そのコマンドの一部を構文とするコマンドもすべてそのレベルに設定されます。たとえば、**show ip route** コマンドをレベル 15 に設定すると、個別に異なるレベルに設定しない限り、**show** コマンドと **show ip** コマンドも自動的にレベル 15 に設定されます。

特定のコマンドについてデフォルトの特権に戻すには、グローバル設定コマンド **no privilege** *mode* **level** *level command* を使用します。

次の例は、**configure** コマンドを特権レベル 14 に設定し、ユーザがレベル 14 のコマンドを使用する場合に入力するパスワードとして *SecretPswd14* を定義する方法を示しています。

```
AP(config)# privilege exec level 14 configure
AP(config)# enable password level 14 SecretPswd14
```

特権レベルへのログインと終了

特権 EXEC モードから、次の手順に従って、指定された特権レベルにログインし、指定された特権レベルに出ます。

	コマンド	目的
ステップ 1	**enable** *level*	指定した特権レベルにログインします。 *level* の指定範囲は 0 ～ 15 です。
ステップ 2	**disable** *level*	指定した特権レベルに出ます。 *level* の指定範囲は 0 ～ 15 です。

RADIUS によるアクセス ポイントへのアクセスの制御

この項では、Remote Authentication Dial-In User Service（RADIUS）を使用して、無線デバイスの管理者アクセス権を制御する手順について説明します。RADIUS をサポートするように無線デバイスを設定する手順の詳細は、第12章「RADIUS サーバと TACACS+ サーバの設定」を参照してください。

RADIUS は詳細なアカウンティング情報を提供し、認証と許可のプロセスを柔軟に管理します。RADIUS は AAA を通じて効率化され、AAA コマンドでのみ有効に設定できます。

（注）　この項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。

次の各項で RADIUS の設定について説明します。

- デフォルトの RADIUS 設定（P. 5-9）
- RADIUS ログイン認証の設定（P. 5-9）（必須）
- AAA サーバ グループの定義（P. 5-11）（オプション）
- 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（P. 5-13）（オプション）
- RADIUS 設定の表示（P. 5-13）

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、Command-Line Interface（CLI; コマンドライン インターフェイス）経由で無線デバイスにアクセスするユーザを認証できます。

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リストの指定をしない場合に使用されるデフォルトのリストを作成する場合は、**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。 • **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。これには、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。
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のリストが使用されます。 • **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に無線デバイスを設定できます。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。

特定のサーバを定義済みグループ サーバに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。
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 User Datagram Protocol（UDP; ユーザ データグラム プロトコル）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、無線デバイスが RADIUS サーバの返答を待ち、再送信するまでの時間を指定します。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** コマンドでこの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。 • （オプション）**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。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、無線デバイスと RADIUS サーバで動作する 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。

	コマンド	目的
		（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。キーは必ず **radius-server host** コマンドの最後に設定してください。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。 無線デバイスが単一の 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回数だけ入力します。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。無線デバイス 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、無線デバイスはサーバ 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場合は、グローバル設定コマンド **no aaa group server radius** *group-name* を使用します。また、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、無線デバイスは異なる 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、無線デバイスは、ローカル ユーザ データベースまたはセキュリティ サーバ上にある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。

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。

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。

- 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無線デバイスを設定します。
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、無線デバイスを設定します。 **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**	（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 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。

TACACS+ によるアクセス ポイントへのアクセスの制御

この項では、Terminal Access Controller Access Control System Plus（TACACS+）を使用して無線デバイスの管理者アクセス権を制御する手順について説明します。TACACS+ をサポートするように無線デバイスを設定する手順の詳細は、第 12 章「RADIUS サーバと TACACS+ サーバの設定」を参照してください。

TACACS+ は詳細なアカウンティング情報を提供し、認証と許可のプロセスを柔軟に管理します。TACACS+ は AAA を通じて効率化され、AAA コマンドでのみ有効に設定できます。

（注）　この項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。

次の項で TACACS+ の設定について説明します。

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 TACACS+ を設定することはできません。TACACS+ を有効にすると、CLI 経由で無線デバイスにアクセスする管理者を認証できます。

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、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リストの指定を*しない*場合に使用されるデフォルトのリストを作成する場合は、**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。 • **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。これには、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。
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のリストが使用されます。 • **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、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、無線デバイスは、ローカル ユーザ データベースかセキュリティ サーバ上にある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。

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。

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。

- 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 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、ユーザが TACACS+ 許可を受けるように無線デバイスを設定します。
ステップ 3	**aaa authorization exec tacacs+**	ユーザの TACACS+ 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、無線デバイスを設定します。 **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**	（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+ 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。

イーサネットの速度およびデュプレックスの設定

無線デバイスのイーサネット ポートに速度およびデュプレックスの設定を割り当てることができます。無線デバイスのイーサネット ポート上の速度設定とデュプレックス設定のどちらについても、デフォルト設定の **auto** を使用することをお勧めします。無線デバイスがスイッチからインライン電源を受け取ったときに、速度設定またはデュプレックス設定が変更されるとイーサネット リンクがリセットされ、無線デバイスがリブートします。無線デバイスの接続先のスイッチのポートが **auto** に設定されていない場合、無線デバイスのポートを **half** または **full** に変更してデュプレックスの不一致を修正することができます。これによってイーサネット リンクはリセットされなくなります。ただし、**half** または **full** から **auto** に戻すと、リンクがリセットされ、無線デバイスがスイッチからインライン電源を受け取ると、その無線デバイスはリブートします。

（注）　無線デバイスのイーサネット ポート上の速度およびデュプレックスの設定は、無線デバイスの接続先のポート上のイーサネット設定と一致させる必要があります。無線デバイスの接続先のポート上の設定を変更する場合は、これと一致するように無線デバイスのイーサネット ポート上の設定も変更します。

イーサネットの速度とデュプレックスは、デフォルトでは **auto** に設定されています。特権 EXEC モードから、次の手順に従ってイーサネットの速度とデュプレックスを設定します。

	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	**interface fastethernet0**	インターフェイス設定モードを開始します。
ステップ 3	**speed** { **10** | **100** | **auto** }	イーサネット速度を設定します。デフォルト設定の **auto** を使用することをお勧めします。
ステップ 4	**duplex** { **auto** | **full** | **half** }	デュプレックス設定を行います。デフォルト設定の **auto** を使用することをお勧めします。
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。

アクセス ポイントの無線ネットワーク管理の設定

無線デバイスを無線ネットワーク管理に対して有効にできます。Wireless Network Manager（WNM; 無線ネットワーク マネージャ）は無線 LAN 上のデバイスを管理します。

無線デバイスが WNM と対話するように設定するには、次のコマンドを入力します。

```
AP(config)# wlccp wnm ip address ip-address
```

WDS アクセス ポイントと WNM の間の認証ステータスをチェックするには、次のコマンドを入力します。

```
AP# show wlccp wnm status
```

not authenticated、*authentication in progress*, *authentication fail*、*authenticated*、*security keys setup* のいずれかのステータスをとります。

アクセス ポイントのローカル認証および許可の設定

サーバを介さずに AAA を操作できるように設定するには、ローカル モードで AAA を実装するように無線デバイスを設定します。無線デバイスは、認証と許可を処理します。この設定ではアカウンティングは使用できません。

（注）　無線デバイスを 802.1x 対応のクライアント デバイス用の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を提供したり、RADIUS サーバのないネットワーク上で認証サービスを提供したりできます。無線デバイス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。

特権 EXEC モードから、次の手順に従ってローカル AAA に無線デバイスを設定します。

	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 local**	ローカル ユーザ名データベースを使用するログイン認証を設定します。**default** キーワードにより、ローカル ユーザ データベース認証がすべてのインターフェイスに適用されます。
ステップ 4	**aaa authorization exec local**	ローカル データベースをチェックして、ユーザが EXEC シェルの実行を許可されているかどうかを判断するようにユーザ AAA 許可を設定します。
ステップ 5	**aaa authorization network local**	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 AAA 許可を設定します。
ステップ 6	**username** *name* [**privilege** *level*] {**password** *encryption-type password*}	ローカル データベースを入力し、ユーザ名ベースの認証システムを設定します。 このコマンドを各ユーザについて繰り返します。 • *name* には、ユーザ ID を 1 ワードで指定します。空白と引用符は使用できません。 • （オプション）*level* には、ユーザがアクセス後に取得する特権レベルを指定します。指定範囲は 0 ～ 15 です。レベル 15 は特権 EXEC モードのアクセスを許可します。レベル 0 はユーザ EXEC モードのアクセスを許可します。 • *encryption-type* には、後ろに暗号化されていないパスワードが続くことを指定する場合は **0** を入力します。非表示のパスワードが続くことを指定するには **7** を入力します。 • *password* には、無線デバイスへアクセスするためにユーザが入力しなければならないパスワードを指定します。パスワードは 1 ～ 25 文字の間で指定します。空白を入れることもできます。また、パスワードは必ず **username** コマンドの最後のオプションとして指定してください。
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。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。

DHCP サービスを提供するためのアクセス ポイントの設定

次の項では、無線デバイスを DHCP サーバとして機能させる方法について説明します。

DHCP サーバの設定

デフォルトでは、アクセス ポイントは、ネットワーク上の DHCP サーバから IP 設定を受信するように設定されています。アクセス ポイントを DHCP サーバとして機能するように設定し、IP 設定を、有線 LAN と無線 LAN 両方のデバイスに割り当てることもできます。

1100 シリーズのアクセス ポイントは、デフォルト設定ではミニ DHCP サーバとして機能し、DHCP サーバから IP 設定を受信できません。ミニ DHCP サーバとして、1100 シリーズのアクセス ポイントは、そのイーサネット ポートに接続されている 1 台の PC と無線クライアント デバイスに 10.0.0.11 ～ 10.0.0.30 の範囲の最大 20 個の IP アドレスを提供します。無線クライアント デバイスについては、Service Set Identifier（SSID; サービス セット ID）を使用しないか、SSID に *tsunami* を使用するように設定され、すべてのセキュリティ設定が無効になるものが対象となります。このミニ DHCP サーバの機能は、1100 シリーズのアクセス ポイントに静的 IP アドレスを割り当てると、自動的に無効になります。初期セットアップを簡単にするためのコンソール ポートがあるので、1200 シリーズのアクセス ポイントは自動的に DHCP サーバにはなりません。

DHCP 関連のコマンドとオプションの詳細は、リリース 12.2 の『Cisco IOS IP Configuration Guide』の「Configuring DHCP」の章を参照してください。次のリンクをクリックすると、「Configuring DHCP」の章を参照できます。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fipr_c/ipcprt1/1cfdhcp.htm

特権 EXEC モードから、次の手順に従って、アクセス ポイントが DHCP サービスを提供するように設定します。

	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	**ip dhcp excluded-address** *low_address* [*high_address*]	無線デバイスが割り当てるアドレス範囲から、無線デバイスの IP アドレスを除外します。アドレスを、10.91.6.158 のように 4 つのグループに区切って入力します。 無線デバイスでは、DHCP アドレス プール サブネット中のすべての IP アドレスを DHCP クライアントへの割り当てに使用できると仮定されます。DHCP サーバがクライアントに割り当てるべきでない IP アドレスを指定する必要があります。 （オプション）除外するアドレスの範囲を指定するには、範囲の下限のアドレスの後に、範囲の上限のアドレスを入力します。
ステップ 3	**ip dhcp pool** *pool_name*	DHCP 要求に応じて無線デバイスが割り当てる IP アドレスのプールの名前を生成し、DHCP 設定モードを開始します。
ステップ 4	**network** *subnet_number* [*mask* | *prefix-length*]	アドレス プールにサブネット番号を割り当てます。無線デバイスは、このサブネット内の IP アドレスを割り当てます。 （オプション）アドレス プールにサブネット マスクを割り当てるか、アドレス接頭辞を構成するビット数を指定します。接頭辞はネットワーク マスクを割り当てる代替法です。接頭辞の長さの前には必ずスラッシュ（/）を入力してください。

	コマンド	目的
ステップ 5	**lease** { *days* [*hours*] [*minutes*] | **infinite** }	無線デバイスによって割り当てられた IP アドレスのリース期間を設定します。 • days：日数でリース期間を設定します。 • （オプション）hours：時間数でリース期間を設定します。 • （オプション）minutes：分数でリース期間を設定します。 • infinite：リース期間を無限に設定します。
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。

デフォルト設定に戻すには、これらのコマンドの **no** フォームを使用します。

次の例は、無線デバイスを DHCP サーバとして設定する方法を示しています。

```
AP# configure terminal
AP(config)# ip dhcp excluded-address 172.16.1.100 172.16.1.117
AP(config)# ip dhcp pool wishbone
AP(dhcp-config)# network 172.16.1.0 255.255.255.0
AP(dhcp-config)# lease 10
AP(dhcp-config)# end
```

DHCP サーバ アクセス ポイントの監視と維持

次の項では、DHCP サーバ アクセス ポイントの監視と維持に使用できるコマンドについて説明します。

- Show コマンド（P. 5-20）
- Clear コマンド（P. 5-21）
- Debug コマンド（P. 5-21）

Show コマンド

DHCP サーバとしての無線デバイスに関する情報を表示するには、EXEC モードで 表 5-2 中のコマンドを入力します。

表 5-2　DHCP サーバ用の Show コマンド

コマンド	目的
show ip dhcp conflict [*address*]	特定の DHCP サーバによって記録されているすべてのアドレス競合のリストを表示します。無線デバイスの IP アドレスを入力すると、無線デバイスによって記録されている競合が表示されます。
show ip dhcp database [*url*]	DHCP データベースでの最近のアクティビティを表示します。 （注）　このコマンドは特権 EXEC モードで使用してください。
show ip dhcp server statistics	送受信されたサーバの統計情報やメッセージに関するカウント情報を表示します。

Clear コマンド

DHCP サーバ変数を消去するには、特権 EXEC モードで 表 5-3 中のコマンドを使用します。

表 5-3　DHCP サーバ用の Clear コマンド

コマンド	目的
clear ip dhcp binding { *address* | * }	DHCP データベースから自動アドレス バインディングを削除します。address 引数を指定すると、特定の（クライアント）IP アドレスの自動バインディングが消去されます。アスタリスク（*）を指定すると、すべての自動バインディングが消去されます。
clear ip dhcp conflict { *address* | * }	DHCP データベースからアドレス競合を消去します。address 引数を指定すると、特定の IP アドレスの競合が消去されます。アスタリスク（*）を指定すると、すべてのアドレスの競合が消去されます。
clear ip dhcp server statistics	すべての DHCP サーバのカウンタを 0 にリセットします。

Debug コマンド

DHCP サーバのデバッグを有効にするには、特権 EXEC モードで次のコマンドを使用します。

debug ip dhcp server { **events** | **packets** | **linkage** }

無線デバイス DHCP サーバのデバッグを無効にするには、このコマンドの **no** フォームを使用します。

アクセス ポイントの Secure Shell の設定

この項では、Secure Shell（SSH）機能の設定方法について説明します。

（注）　この項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』の「Secure Shell Commands」の項を参照してください。

SSH の概要

SSH は、レイヤ 2 デバイスまたはレイヤ 3 デバイスに安全なリモート接続を提供するプロトコルです。SSH には、SSH バージョン 1 と SSH バージョン 2 の 2 種類のバージョンがあります。このソフトウェア リリースは SSH バージョン 1 のみをサポートしています。

SSH はデバイスの認証時に強力な暗号化を行うため、Telnet よりもリモート接続の安全性が高くなります。SSH 機能では SSH サーバと SSH 統合クライアントを使用します。クライアントは次のユーザ認証方式をサポートしています。

- RADIUS（詳細は、「RADIUS によるアクセス ポイントへのアクセスの制御」の項（P.5-9）を参照）
- ローカル認証と許可（詳細は、「アクセス ポイントのローカル認証および許可の設定」の項（P.5-18）を参照）

SSH の詳細は、リリース 12.2 の『Cisco IOS Security Configuration Guide』の「Configuring Secure Shell」の項を参照してください。

（注）　このソフトウェア リリースの SSH 機能は IP Security（IPSec;IP セキュリティ）をサポートしていません。

SSH の設定

SSH を設定する前に、Cisco.com から暗号ソフトウェア イメージをダウンロードします。詳細は、このリリースのリリース ノートを参照してください。

SSH の設定と SSH 設定の表示については、リリース 12.2 の『Cisco IOS Security Configuration Guide』の「Configuring Secure Shell」の項を参照してください。

クライアント ARP キャッシングの設定

アソシエートされたクライアント デバイスの Address Resolution Protocol（ARP; アドレス レゾリューション プロトコル）キャッシュを保持するように、無線デバイスを設定できます。無線デバイスで ARP キャッシュを保持すると、無線 LAN のトラフィック負荷が軽減されます。ARP キャッシングはデフォルトで無効に設定されています。

この項で説明する内容は次のとおりです。

クライアント ARP キャッシングの概要

無線デバイスでの ARP キャッシングは、クライアント デバイスへの ARP 要求を無線デバイスで止めることによって、無線 LAN 上のトラフィックを軽減します。無線デバイスは、ARP 要求をクライアント デバイスへ転送する代わりに、アソシエートされたクライアント デバイスに代わって ARP 要求に応答します。

ARP キャッシングを無効にすると、無線デバイスはすべての ARP 要求をアソシエートされたクライアントに無線ポート経由で転送し、ARP 要求を受け取ったクライアントが応答します。一方、ARP キャッシングを有効にすると、無線デバイスはアソシエートされたクライアントに代わって ARP 要求に応答し、クライアントへは要求を転送しません。キャッシュにない IP アドレスに向けた ARP 要求を受け取ると、無線デバイスはその要求を廃棄して転送しません。無線デバイスは、ビーコンに情報エレメントを追加して、バッテリの寿命を延ばすためのブロードキャスト メッセージを安全に無視できることをクライアント デバイスに通知します。

オプションの ARP キャッシング

アクセス ポイントにシスコ製以外のクライアント デバイスがアソシエートされ、そのデバイスがデータを通さない場合、無線デバイスがそのクライアントの IP アドレスを認識していない可能性があります。無線 LAN でこの状況が頻発する場合は、オプションの ARP キャッシングを有効にできます。ARP キャッシングがオプションの場合、無線デバイスは既知の IP アドレスのクライアントについては、その代理として応答しますが、不明なクライアント宛ての ARP 要求はすべて無線ポートから転送します。アソシエートされた全クライアントの IP アドレスを記憶すると、無線デバイスはそれらのアソシエートされたクライアント以外に対する ARP 要求を廃棄します。

ARP キャッシングの設定

特権 EXEC モードから、次の手順に従って、アソシエートされたクライアントの ARP キャッシュを保持するように無線デバイスを設定します。

	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	**dot11 arp-cache** [**optional**]	無線デバイスでの ARP キャッシングを有効にします。 • （オプション）無線デバイスが認識している IP アドレスのクライアント デバイスに限って ARP キャッシングを有効にするには、**optional** キーワードを使用します。
ステップ 3	**end**	特権 EXEC モードに戻ります。

	コマンド	目的
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**	（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。

次の例に、アクセス ポイントで ARP キャッシングを設定する方法の例を示します。

```
AP# configure terminal
AP(config)# dot11 arp-cache
AP(config)# end
```

システムの日時の管理

無線デバイスのシステムの時刻と日付は、Simple Network Time Protocol（SNTP; 簡易ネットワーク タイム プロトコル）を使用して自動的に管理することも、無線デバイスに時刻と日付を設定して手動で管理することもできます。

（注）　この項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 Configuration Fundamentals Command Reference』を参照してください。

この項で説明する設定の内容は次のとおりです。

Simple Network Time Protocol の概要

Simple Network Time Protocol（SNTP）とは、クライアント専用バージョンの簡易版 Network Time Protocol（NTP; ネットワーク タイム プロトコル）です。SNTP は、NTP サーバから時間を受信のみできます。他のシステムに時刻サービスを提供することはできません。SNTP は通常、100 ミリ秒単位で正確な時間を提供しますが、NTP のように複雑なフィルタリングや統計メカニズムはありません。

SNTP は、設定済みサーバからパケットを要求して受け付けるよう設定することも、任意のソースからの NTP ブロードキャスト パケットを受け付けるよう設定することもできます。複数のソースから NTP パケットが送信された場合は、ストラタムが最良のサーバが選択されます。NTP とストラタムの詳細は、次の URL をクリックしてください。

http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_configuration_guide_chapter09186a00800ca66f.html#1001131

複数のサーバのストラタムが同じだった場合は、ブロードキャスト サーバよりも設定済みサーバが優先されます。基準を両方とも満たすサーバが複数ある場合は、最初に時間パケットを送信する方が選択されます。現在選択中のサーバからパケット受信が途絶えたり、または上記の基準に基づいてより最適なサーバが検出されたりしない限り、SNTP が新たにサーバを選択することはありません。

SNTP の設定

デフォルトでは、SNTP は無効に設定されています。アクセス ポイントで SNTP を有効にするには、グローバル コンフィギュレーション モードで次のいずれかまたは両方のコマンドを使用します。

表 5-4　SNTP コマンド

コマンド	目的
sntp server { *アドレス* | *ホスト名* } [**version** *番号*]	NTP サーバから NTP パケットを要求するよう SNTP を設定します。
sntp broadcast client	どの NTP ブロードキャスト サーバからも NTP パケットを受け付けるよう SNTP を設定します。

NTP サーバごとに **sntp server** コマンドを 1 回ずつ入力してください。NTP サーバは、アクセス ポイントからの SNTP メッセージに応答できるよう設定しておく必要があります。

sntp server コマンドと **sntp broadcast client** コマンドの両方を入力した場合、アクセス ポイントはブロードキャスト サーバからの時間を受け付けますが、同一のストラタムと判断して設定済みサーバからの時間の方を優先します。SNTP に関する情報を表示するには、**show sntp** EXEC コマンドを使用します。

時刻と日付の手動設定

時刻ソースが利用できない場合は、システムの再起動後に手動で時刻と日付を設定できます。時刻は次回のシステム再起動まで正確に維持されます。手動設定は最後の手段として行うことをお勧めします。無線デバイスが同期できる外部ソースがある場合は、システム クロックを手動で設定する必要はありません。

この項で説明する設定の内容は次のとおりです。

システム クロックの設定

ネットワークに NTP サーバなどの時刻サーバを提供する外部ソースがある場合は、システム クロックを手動で設定する必要はありません。

特権 EXEC モードから、次の手順に従ってシステム クロックを設定します。

	コマンド	目的
ステップ 1	**clock set** *hh*:*mm*:*ss day month year* または **clock set** *hh*:*mm*:*ss month day year*	次のいずれかの書式を使ってシステム クロックを手動で設定します。 • *hh*:*mm*:*ss* には、時間（24 時間形式）、分、秒を指定します。設定されたタイム ゾーンを基準に時間を指定します。 • *day* には、日にちを指定します。 • *month* には、月を名前で指定します。 • *year* には、年を 4 桁で指定します。
ステップ 2	**show running-config**	入力内容を確認します。
ステップ 3	**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。

次に、システム クロックを手動で 2001 年 7 月 23 日 午後 1 時 32 分に設定する例を示します。

```
AP# clock set 13:32:00 23 July 2001
```

時刻と日付の設定の表示

日付と時刻の設定を表示するには、**show clock** [**detail**] 特権 EXEC コマンドを使用します。

システム クロックは、時間の信頼性（正確性）を示す *authoritative* フラグを表示し続けます。システム クロックが NTP などの時刻ソースで設定されている場合は、このフラグが設定されます。信頼できない場合、時刻は表示のみに使用されます。ピアの時刻が無効になった場合、クロックが信頼でき、*authoritative* フラグが設定されるまで、このフラグがピアのクロックとの同期を防ぎます。

show clock の前に表示される記号には次のような意味があります。

- *****：時刻が信頼できません。
- （空白）：時刻が信頼できます。
- .：時刻は信頼できますが、NTP は同期が行われていません。

タイム ゾーンの設定

特権 EXEC モードから、次の手順に従ってタイム ゾーンを手動で設定します。

	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	**clock timezone** *zone hours-offset* [*minutes-offset*]	タイム ゾーンを設定します。 無線デバイスは内部時間を Universal Time Coordinated（UTC; 協定世界時）で維持するため、このコマンドは表示専用で、時刻を手動で設定するときにのみ使用されます。 • *zone* には、標準時間が有効な場合に表示されるタイム ゾーンの名前を入力します。デフォルトは UTC です。 • *hours-offset* には、UTC との時差を時間単位で入力します。 • （オプション）*minutes-offset* には、UTC との時差を分単位で入力します。
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**	（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。

グローバル設定コマンド **clock timezone** の *minutes-offset* 変数は、ローカル タイム ゾーンの UTC との時差が 1 時間未満の単位である場合に使用できます。たとえば、大西洋沿岸カナダの一部地域のタイム ゾーン（AST）は UTC-3.5 です。3 は 3 時間を、5 は 50 パーセントを意味します。この場合、コマンドを **clock timezone AST -3 30** と指定することになります。

時刻を UTC に設定するには、グローバル設定コマンド **no clock timezone** を使用します。

サマー タイム（夏時間）の設定

特権 EXEC モードから、次の手順に従って、毎年、特定の日付（曜日）に開始および終了するサマータイム（夏時間）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	**clock summer-time** *zone* **recurring** [*week day month hh*:*mm week day month hh*:*mm* [*offset*]]	毎年指定された日付に開始および終了するサマー タイムを設定します。 サマー タイムはデフォルトでは無効になっています。パラメータを指定しないで **clock summer-time** *zone* **recurring** を指定した場合、サマー タイムのルールは米国のルールをデフォルトとします。 • *zone* には、サマー タイムが有効なときに表示されるタイムゾーンの名前（PDT など）を指定します。 • （オプション）*week* には、月の第何週かを指定します（1 ～ 5 または **last**）。 • （オプション）*day* には、曜日を指定します（Sunday、Monday など）。 • （オプション）*month* には、月を名前で指定します（January、February など）。 • （オプション）*hh*:*mm* には、時刻（24 時間形式）を時間と分の単位で指定します。 • （オプション）*offset* には、サマー タイム期間中に追加する時間を分単位で指定します。デフォルトは 60 分です。
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**	（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。

グローバル設定コマンド **clock summer-time** の最初の部分は、サマー タイムの開始時を、2 番目の部分は終了時を指定します。すべての時間は ローカル タイム ゾーンを基準にします。開始時間は標準時が基準になります。終了時間はサマー タイムが基準になります。開始月が終了月より後の場合、自動的に南半球であると解釈されます。

次の例では、4 月の第 1 日曜日の 02:00 に開始し、10 月の最終日曜日の 02:00 に終了するサマー タイムの指定方法を示します。

```
AP(config)# clock summer-time PDT recurring 1 Sunday April 2:00 last Sunday October
2:00
```

ユーザ居住地域のサマー タイムが定期的なパターンに従わない場合、特権 EXEC モードから、次の手順に従って、次のサマー タイム イベントの日付と時間を正確に設定します。

	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	**clock summer-time** *zone* **date** [*month date year hh*:*mm month date year hh*:*mm* [*offset*]] または **clock summer-time** *zone* **date** [*date month year hh*:*mm date month year hh*:*mm* [*offset*]]	最初の日付に開始し、2 番目の日付に終了するサマー タイムを設定します。 サマー タイムはデフォルトでは無効になっています。 • *zone* には、サマー タイムが有効なときに表示されるタイム ゾーンの名前（PDT など）を指定します。 • （オプション）*week* には、月の第何週かを指定します（1 ～ 5 または **last**）。 • （オプション）*day* には、曜日を指定します（Sunday、Monday など）。 • （オプション）*month* には、月を名前で指定します（January、February など）。 • （オプション）*hh*:*mm* には、時刻（24 時間形式）を時間と分の単位で指定します。 • （オプション）*offset* には、サマー タイム期間中に追加する時間を分単位で指定します。デフォルトは 60 分です。
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**	（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。

グローバル設定コマンド **clock summer-time** の最初の部分は、サマー タイムの開始時を、2 番目の部分は終了時を指定します。すべての時間は ローカル タイム ゾーンを基準にします。開始時間は標準時が基準になります。終了時間はサマー タイムが基準になります。開始月が終了月より後の場合、自動的に南半球であると解釈されます。

サマー タイムを無効にするには、グローバル設定コマンド **no clock summer-time** を使用します。

次の例では、2000 年 10 月 12 日 02:00 に開始し、2001 年 4 月 26 日 02:00 に終了するサマー タイムの設定方法を示します。

```
AP(config)# clock summer-time pdt date 12 October 2000 2:00 26 April 2001 2:00
```

システム名とプロンプトの設定

無線デバイスを識別するシステム名を設定します。デフォルトでは、システム名とプロンプトは *ap* です。

システム プロンプトを設定しない場合、システム名の最初の 20 文字がシステム プロンプトとして使用されます。大なり記号（>）が追加されます。プロンプトは、システム名が変更されると必ず更新されますが、グローバル設定コマンド **prompt** を使用して手動でプロンプトを設定している場合は更新されません。

（注）　この項で使用されるコマンドの構文と使用方法の詳細は、『Cisco IOS Configuration Fundamentals Command Reference』、およびリリース 12.3 の『Cisco IOS IP and IP Routing Command Reference』を参照してください。

この項で説明する設定の内容は次のとおりです。

デフォルトのシステム名とプロンプトの設定

アクセス ポイントのデフォルトのシステム名とプロンプトは *ap* です。

システム名の設定

特権 EXEC モードから、次の手順に従ってシステム名を手動で設定します。

	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	**hostname** *name*	システム名を手動で設定します。 デフォルト設定は *ap* です。 （注）　システム名を変更する場合、無線デバイスの無線はリセットされ、アソシエートしているクライアント デバイスはアソシエーションが解除され、ただちに再アソシエートされます。 （注）　システム名には、63 文字まで入力することができます。しかし、無線デバイスでは、クライアント デバイスに自分自身を識別させる際に、システム名の最初の 15 文字だけを使用します。クライアント ユーザがアクセス ポイントどうしを区別することが重要な場合、システム名の一意の部分が最初の 15 文字に現れるようにしてください。
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**	（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。

システム名を設定すると、その名前がシステム プロンプトとしても使用されます。

デフォルトのホスト名に戻すには、グローバル設定コマンド **no hostname** を使用します。

DNS の概要

DNS プロトコルは DNS を制御します。これはホスト名を IP アドレスにマッピングする際に使用する分散型データベースです。無線デバイスに DNS を設定すると、**ping**、**telnet**、**connect**、および関連する Telnet サポート操作で、IP アドレスの代わりにホスト名を使用できます。

IP は階層命名方式を定義します。この方式では場所またはドメインでデバイスを特定することができます。ドメイン名はピリオド（.）を区切り文字として連結できます。たとえば、シスコ システムズは IP ではドメイン名 *com* で特定される民間組織です。このためドメイン名は *cisco.com* になります。このドメイン内の File Transfer Protocol（FTP; ファイル転送プロトコル）システムなどの個々のデバイスは *ftp.cisco.com* のように識別されます。

ドメイン名を追跡するために、IP は IP アドレスにマッピングされた名前のキャッシュ（またはデータベース）を保持するドメイン ネーム サーバの概念を定義しています。ドメイン名を IP アドレスにマッピングするには、まずホスト名を特定し、ネットワーク上に存在するネーム サーバを特定し、DNS を有効にします。

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 DNS 設定（P. 5-31）
- DNS の設定（P. 5-32）
- DNS 設定の表示（P. 5-33）

デフォルトの DNS 設定

表 5-5 にデフォルトの DNS 設定を示します。

表 5-5　デフォルトの DNS 設定

機能	デフォルト設定
DNS の有効 / 無効	無効
DNS デフォルト ドメイン名	設定されていません。
DNS サーバ	ネーム サーバ アドレスは設定されていません。

DNS の設定

特権 EXEC モードから、次の手順に従って DNS を使用するように無線デバイスを設定します。

	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	**ip domain-name** *name*	ソフトウェアが未修飾ホスト名（ドット付き 10 進ドメイン名を含まない名前）を作成する場合に使用するデフォルトのドメイン名を定義します。 未修飾名をドメイン名と区切るピリオドを先頭に使用しないでください。 ブート時にはドメイン名は設定されていませんが、無線デバイスの設定が BOOTP または Dynamic Host Configuration Protocol（DHCP）サーバから行われている場合、BOOTP または DHCP サーバによってデフォルトのドメイン名が設定されることがあります（この情報がサーバに設定されている場合）。
ステップ 3	**ip name-server** *server-address1* [*server-address2 ... server-address6*]	名前とアドレスの解決に使用する 1 つまたは複数のネーム サーバのアドレスを指定します。 最大 6 つのネーム サーバを指定できます。各サーバのアドレスは空白で区切ります。最初に指定するサーバがプライマリ サーバになります。無線デバイスは、最初にプライマリ サーバへ DNS クエリを送信します。そのクエリが失敗した場合、バックアップ サーバが照会されます。
ステップ 4	**ip domain-lookup**	（オプション）無線デバイスで DNS ベースのホスト名からアドレスへの変換を有効にします。この機能はデフォルトで有効に設定されています。 ネットワークのデバイスが名前の割り当てを制御できないネットワークのデバイスとの接続を要求する場合、グローバル インターネット命名方式（DNS）を使用して、デバイスを一意に識別するデバイス名を動的に割り当てることができます。
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。

無線デバイスの IP アドレスをホスト名として使用する場合、この IP アドレスが使用されるため DNS クエリは作成されません。ピリオド（.）を含まないホスト名を設定すると、名前を IP アドレスにマッピングする DNS クエリが作成される前に、ホスト名の後にピリオドとデフォルトのドメイン名が追加されます。デフォルトのドメイン名は、グローバル設定コマンド **ip domain-name** で設定される値です。ホスト名にピリオド（.）が含まれている場合、Cisco IOS ソフトウェアはホスト名にデフォルトのドメイン名を追加せずに、IP アドレスを検索します。

ドメイン名を削除するには、グローバル設定コマンド **no ip domain-name** *name* を使用します。ネーム サーバ アドレスを削除するには、グローバル設定コマンド **no ip name-server** *server-address* を使用します。無線デバイスで DNS を無効にする場合は、グローバル設定コマンド **no ip domain-lookup** を使用します。

DNS 設定の表示

DNS 設定情報を表示するには、**show running-config** 特権 EXEC コマンドを使用します。

（注）　無線デバイスで DNS が設定されていると、**show running-config** コマンドはサーバの名前でなく IP アドレスを表示することがあります。

バナーの作成

message-of-the-day（MOTD）バナーとログイン バナーを設定できます。MOTD バナーはログイン時に、接続されたすべての端末に表示されます。すべてのネットワーク ユーザに影響するメッセージ（差し迫ったシステム シャットダウンの通知など）を送信する場合に便利です。

ログイン バナーも接続されたすべての端末に表示されます。これは MOTD バナーの後、ログイン プロンプトの前に表示されます。

（注）　この項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 Configuration Fundamentals Command Reference』を参照してください。

この項で説明する設定の内容は次のとおりです。

デフォルトのバナー設定

デフォルトでは、MOTD バナーとログイン バナーは設定されていません。

Message-of-the-Day ログイン バナーの設定

無線デバイスにログインしたときに画面に表示される 1 行または複数行のメッセージ バナーを作成できます。

特権 EXEC モードから、次の手順に従って MOTD ログイン バナーを設定します。

	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	**banner motd** *c message c*	message-of-the-day（今日のメッセージ）を指定します。 *c* にはシャープ記号（#）など希望する区切り文字を入力し、**Return** キーを押します。区切り文字は、バナー テキストの開始と終了を指定します。終了区切り文字より後の文字は破棄されます。 *message* には、最大 255 文字のバナー メッセージを入力します。メッセージ内で区切り文字は使用できません。
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**	（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。

MOTD バナーを削除するには、グローバル設定コマンド **no banner motd** を使用します。

次の例は、開始および終了区切り文字にシャープ記号（#）を使用して、無線デバイスに MOTD バナーを設定する方法を示しています。

```
AP(config)# banner motd #
これは安全なサイトです。権限のあるユーザのみが許可されます。
アクセスに関しては、テクニカル  サポートにお問い合わせください。
#
AP(config)#
```

次の例は、上記の設定で表示されるバナーを示しています。

```
Unix> telnet 172.2.5.4
Trying 172.2.5.4...
Connected to 172.2.5.4.
Escape character is '^]'.

これは安全なサイトです。権限のあるユーザのみが許可されます。
アクセスに関しては、テクニカル  サポートにお問い合わせください。

User Access Verification

Password:
```

ログイン バナーの設定

接続したすべての端末に表示されるログイン バナーを設定できます。このバナーは MOTD バナーの後、ログイン プロンプトの前に表示されます。

特権 EXEC モードから、次の手順に従ってログイン バナーを設定します。

	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	**banner login** *c message c*	ログイン メッセージを指定します。 *c* にはシャープ記号 (#) など希望する区切り文字を入力し、**Return** キーを押します。区切り文字は、バナー テキストの開始と終了を指定します。終了区切り文字より後の文字は破棄されます。 *message* には、最大 255 文字のログイン メッセージを入力します。メッセージ内で区切り文字は使用できません。
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**	（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。

ログイン バナーを削除するには、グローバル設定コマンド **no banner login** を使用します。

次の例は、開始および終了区切り文字にドル記号 ($) を使用して、無線デバイスにログイン バナーを設定する方法を示しています。

```
AP(config)# banner login $
許可されたユーザのみアクセスできます。ユーザ名とパスワードを入力してください。
$
AP(config)#
```