アクセス ポイントの管理

この章では、ワイヤレス デバイスの管理方法について説明します。

MODE ボタンの無効化

コンソール ポートを搭載したアクセス ポイントの MODE ボタンは、**[no] boot mode-button** グローバル コンフィギュレーション コマンドで無効にできます。このコマンドを使用するとパスワードによるリカバリを防ぎ、権限のないユーザがアクセス ポイントの CLI にアクセスできないようにします。

注意 このコマンドは、パスワードによるリカバリを無効にします。このコマンドを入力した後、アクセス ポイントの特権 EXEC モードのパスワードを紛失してしまうと、アクセス ポイントの CLI にアクセスし直すには、シスコの Technical Assistance Center（TAC）に連絡する必要があります。

MODE ボタンはデフォルトで有効に設定されています。特権 EXEC モードから、次の手順に従ってアクセス ポイントの MODE ボタンを無効にします。

	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	**no boot mode-button**	アクセス ポイントの MODE ボタンを無効にします。
ステップ 3	**end**	(注)　この設定は保存する必要はありません。

MODE ボタンのステータスをチェックするには、特権 EXEC モードから **show boot** または **show boot mode-button** コマンドを実行します。設定の実行時には、ステータスが表示されません。**show boot** と **show boot mode-button** コマンドを実行すると、通常次のような応答が表示されます。

```
ap#show boot
BOOT path-list:      flash:/ap3g2-k9w7-mx.152-4.JA1/ap3g2-k9w7-mx.152-4.JA1
Config file:         flash:/config.txt
Private Config file: flash:/private-config
Enable Break:        yes
Manual Boot:         no
Enable IOS Break:    no
HELPER path-list:
NVRAM/Config file
      buffer size:   32768
      Mode Button:    on
Radio Core TFTP:
ap#
```

(注)　特権 EXEC のパスワードがわかっていれば、グローバル コンフィギュレーション コマンド **boot mode-button** を使用して、MODE ボタンを通常動作に復旧できます。

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ワイヤレス 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ワイヤレス 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。

ワイヤレス 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。

- ワイヤレス 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、各ユーザはワイヤレス 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。詳細については、「ユーザ名とパスワードのペアの設定」セクション（5-6 ページ）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。

(注)　TAB、?、$、+、および [は、パスワードには無効な文字です。

- RADIUS または TACACS+ 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。詳細については、「RADIUS によるアクセス ポイントへのアクセスの制御」セクション（5-11 ページ）および「TACACS+ によるアクセス ポイントへのアクセスの制御」セクション（5-16 ページ）を参照してください。

特権 EXEC コマンドへのアクセスの保護

ネットワークで端末のアクセス コントロールを行う簡単な方法は、パスワードを使用して権限レベルを割り当てることです。パスワード保護によって、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が制限されます。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については、リリース 12.3 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。

デフォルトのパスワードおよび権限レベル設定

表 5-1 に、デフォルトのパスワードおよび権限レベル設定を示します。

表 5-1　　デフォルトのパスワードおよび権限レベル設定

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 パスワードおよび権限レベル	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 です（特権 EXEC レベル）。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 パスワードおよび権限レベル	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 です（特権 EXEC レベル）。パスワードは、暗号化されてからコンフィギュレーション ファイルに書き込まれます。
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。

スタティック 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 コンフィギュレーション 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。

スタティック イネーブル パスワードを設定または変更するには、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	**enable password** *password*	特権 EXEC モードへのアクセス用に、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 文字の英数字のストリングを指定します。ストリングを数字で始めることはできません。大文字と小文字を区別し、スペースを使用できますが、先行スペースは無視されます。パスワードに疑問符(?)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、疑問符を入力する前に Ctrl キーを押した状態で 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。 2. **Ctrl+V** を入力します。 3. **?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、疑問符の前で Ctrl キー、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。 (注)　TAB、?、$、+、および [は、パスワードには無効な文字です。
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**	(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。 イネーブル パスワードは暗号化されず、ワイヤレス 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。

次に、イネーブル パスワードを*l1u2c3k4y5* に変更する例を示します。パスワードは暗号化されておらず、レベル 15 のアクセスが与えられます(従来の特権 EXEC モード アクセス)。

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

暗号化によるイネーブルおよびイネーブル 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超えるパスワードや 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 コンフィギュレーション コマンド **enable password** または **enable secret** を使用できます。コマンドの作用はどちらも同じです。このコマンドにより、暗号化されたパスワードを設定できます。特権 EXEC モード(デフォルト設定)または特定の権限レベルにアクセスするユーザは、このパスワードを入力する必要があります。

より高度な暗号化アルゴリズムが使用されるので、**enable secret** コマンドを使用することを推奨します。

enable secret コマンドを設定した場合、このコマンドは **enable password** コマンドよりも優先されます。同時に 2 つのコマンドを有効にはできません。

イネーブルおよびイネーブル シークレット パスワードに暗号化を設定するには、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	**enable password** [**level** *level*] {*password* | *encryption-type encrypted-password*}	特権 EXEC モードへのアクセス用に、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	または
	enable secret [**level** *level*] {*password* | *encryption-type encrypted-password*}	シークレット パスワードを定義し、非可逆暗号方式を使用して保存します。 • （任意）*level* に指定できる範囲は 0 ～ 15 です。レベル 1 が通常のユーザ EXEC モード権限です。デフォルト レベルは 15 です（特権 EXEC モード権限）。 • *password* には、1 ～ 25 文字の英数字のストリングを指定します。ストリングを数字で始めることはできません。大文字と小文字を区別し、スペースを使用できますが、先行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ません。 • （任意）*encryption-type* には、タイプ 0 とタイプ 7 の両方を使用できます。暗号化タイプ 0 では、パスワードが暗号化されません。暗号化タイプ 7 では、パスワードが暗号化されます。両方のタイプが指定されると、パスワード文字列は暗号化タイプ 5 に変換されます。これは、シスコ独自の暗号化アルゴリズムです。. **（注）** 暗号化タイプを指定してクリア テキスト パスワードを入力した場合は、再び特権 EXEC モードを開始することはできません。暗号化されたパスワードが失われた場合は、どのような方法でも回復することはできません。
ステップ 3	**service password-encryption**	（任意）パスワードを定義するとき、または設定を保存するときに、パスワードを暗号化します。 暗号化を行うと、コンフィギュレーション ファイル内でパスワードが読み取り可能な形式になるのを防止できます。
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**	（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。

イネーブルおよびイネーブル シークレット パスワードの両方が定義されている場合、ユーザはイネーブル シークレット パスワードを入力する必要があります。

特定の権限レベルのパスワードを定義する場合は、**level** キーワードを使用します。レベルを指定してパスワードを設定したあと、特権レベルにアクセスする必要のあるユーザだけに、パスワードを通知してください。さまざまなレベルでアクセス可能なコマンドを指定する場合は、**privilege level**

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。詳細については、「複数の特権レベルの設定」セクション（5-7 ページ）を参照してください。

パスワードの暗号化をイネーブルにすると、ユーザ名パスワード、認証キー パスワード、イネーブル コマンド パスワード、コンソールおよび仮想端末回線パスワードなど、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、**no enable password** [**level** *level*] または**no enable secret** [**level** *level*] 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。パスワードの暗号化をディセーブルにするには、**no service password-encryption** 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、権限レベル 2 に対して暗号化パスワード *1FaD0$Xyti5Rkls3LoyxzS8* を設定する例を示します。

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

ユーザ名とパスワードのペアの設定

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、ワイヤレス 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、各ユーザがワイヤレス デバイスにアクセスする際の認証に使用されます。権限レベルを定義している場合は、ユーザ名とパスワードの各ペアに特定の権限レベルを、対応する権利および権限とともに割り当てることもできます。

ユーザ名ベースの認証システムを設定するには、特権 EXEC モードで次の手順を実行します。この認証システムでは、ログイン ユーザ名とパスワードが要求されます。

	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	**login local**	ログイン時のローカル パスワード チェックをイネーブルにします。認証は、ステップ 2 で指定されたユーザ名に基づきます。
ステップ 3	**username** *name* [**privilege** *level*] {**password** *encryption-type password*}	各ユーザのユーザ名、権限レベル、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。スペースと引用符は使用できません。 • （任意）*level* には、アクセス権を得たユーザに設定する権限レベルを指定します。指定できる範囲は 0 ～ 15 です。レベル 15 では特権 EXEC モードでのアクセスが可能です。レベル 1 では、ユーザ EXEC モードでのアクセスとなります。 • *encryption-type* には、暗号化されていないパスワードが後ろに続く場合は 0 を、暗号化されたパスワードが後ろに続く場合は 7 を指定します。 • *password* には、ワイヤレス 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 文字で、埋め込みスペースを使用でき、**username** コマンドの最後のオプションとして指定します。
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**	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。

特定ユーザのユーザ名認証をディセーブルにするには、**no username** *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。

パスワード チェックをディセーブルにし、パスワードなしでの接続を可能にするには、**no login** ライン コンフィギュレーション コマンドを使用します。

(注)　ユーザ名は少なくとも 1 つ設定する必要があります。また、ワイヤレス デバイスに対して Telnet セッションを開くように login local を設定する必要があります。**no username** コマンドでユーザ名だけを入力すると、ワイヤレス デバイスからロックアウトされることがあります。

あるいは、ライン コンフィギュレーション コマンド **no login** を使用して、Telnet でのユーザ名の検証を無効にすることもできます。その場合、ユーザ検証を行う AP にログインしてから、**enable password**（または **enable secret**）コマンドで特権 EXEC レベルを取得する必要があります。このレベルを Telnet ラインに対してデフォルトで取得することもできます。それには、コマンド **privilege level 15** を使用します。

(注)　no login コマンドと privilege level 15 コマンドの両方を使用すると、AP に接続するすべての Telnet クライアントに AP に対する完全な特権アクセスが割り当てられることになります。

```
ap(config)# line vty 0 4
ap(config-line)# no login
ap(config-line)# privilege level 15
```

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、最大 16 個の階層レベルからなるコマンドを設定できます。複数のパスワードを設定することにより、ユーザ グループ別に特定のコマンドへのアクセスを許可することができます。

たとえば、多くのユーザに **clear line** コマンドへのアクセスを許可する場合、レベル 2 のセキュリティを割り当て、レベル 2 のパスワードを広範囲のユーザに配布できます。また、**configure** コマンドへのアクセス制限を強化する場合は、レベル 3 のセキュリティを割り当て、そのパスワードを限られたユーザ グループに配布することもできます。

この項では設定情報を扱います。

- コマンドの特権レベルの設定（5-8 ページ）
- 権限レベルへのログインおよび終了（5-9 ページ）

コマンドの特権レベルの設定

コマンド モードの権限レベルを設定するには、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	**privilege** *mode* **level** *level command*	コマンドの権限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 コンフィギュレーション モードの場合は **interface** を、ライン コンフィギュレーション モードの場合は **line** をそれぞれ入力します。 • *level* に指定できる範囲は 0 ～ 15 です。レベル 1 が通常のユーザ EXEC モード権限です。レベル 15 は、**enable** パスワードによって許可されるアクセス レベルです。 • *command* には、アクセスを制限したいコマンドを指定します。
ステップ 3	**enable password level** *level password*	権限レベルに対応するイネーブル パスワードを指定します。 • *level* に指定できる範囲は 0 ～ 15 です。レベル 1 が通常のユーザ EXEC モード権限です。 • *password* には、1 ～ 25 文字の英数字のストリングを指定します。ストリングを数字で始めることはできません。大文字と小文字を区別し、スペースを使用できますが、先行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ません。 (注)　TAB、?、$、+、および [は、パスワードには無効な文字です。
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** 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**	(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。

コマンドをある権限レベルに設定すると、構文がそのコマンドのサブセットであるコマンドはすべて、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特権レベル 15 に設定されます。

特定のコマンドについて、デフォルトの権限に戻すには、**no privilege** *mode* **level** *level command* 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。

configure コマンドを権限レベル 14 に設定し、レベル 14 のコマンドを使用する場合にユーザが入力するパスワードとして *SecretPswd14* を定義する例を示します。

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

権限レベルへのログインおよび終了

指定した権限レベルにログインする、または指定した権限レベルを終了するには、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	**enable** *level*	指定した権限レベルにログインします。 *level* に指定できる範囲は 0 ～ 15 です。
ステップ 2	**disable***level*	指定した権限レベルを終了します。 *level* に指定できる範囲は 0 ～ 15 です。

[Easy Setup] の設定

[Easy Setup] を使用すると、一つの画面でネットワークと無線を設定できます。

ネットワーク設定

ネットワーク設定を使用してアクセス ポイントを設定するには、次のフィールドに値を入力します。

- Hostname
- Server protocol（DHCP / Static）
- IP Address
- IP Subnet
- デフォルト ゲートウェイ
- IPv6 Protocol（DHCP / Autoconfig / Static IP）
- IPV6 address
- Username
- Password
- SNMP Community
- Current SSID list（アクセス ポイントに設定された SSID リスト）

無線設定

無線設定を使用してアクセス ポイントを設定するには、次のフィールドを設定します。

- [SSID]：32 バイト文字列。
- ビーコン内に指定された [Broadcast SSID]
- セキュリティ
- 無線ネットワークでの役割
  - [Access point]：ルート デバイス。この設定は、どのアクセス ポイントにも適用できます。
  - [Repeater]：非ルート デバイス。この設定も、どのアクセス ポイントにも適用できます。
  - [Root Bridge]：この設定は、どのアクセス ポイントにも適用できます。
  - [Non-Root Bridge]：この設定は、どのアクセス ポイントにも適用できます。

  - [Workgroup Bridge]：この設定は、どのアクセス ポイントにも適用できます。
  - ユニバーサル ワークグループ ブリッジ
  - [Scanner]：アクセス ポイントはネットワーク モニタリング デバイスとして機能します。継続的にスキャンを行い、このモードで無線 LAN に接続中の他の無線デバイスから検出した無線トラフィックをレポートします。すべてのアクセス ポイントは、スキャナとして設定できます。
  - [Spectrum]：Spectrum Expert モードの設定を参照してください。
- [Optimize Radio Network]：無線デバイスの無線に対する事前設定を選択するか、設定をカスタマイズできます。
- [Aironet Extensions]：無線 LAN 上に Cisco Aironet 無線デバイスがある場合にのみ、この設定を有効にできます。
- チャネル
- 電源

工場出荷時設定にアクセス ポイントをリセットするには、[Factory Reset] をクリックします。アクセス ポイントのイメージをリロードするには、[Reboot AP] をクリックします。

Spectrum Expert モードの設定

Spectrum Expert モードは、AP3500、AP3600、AP2600、AP1550 シリーズなどのすべての CleanAir 対応のアクセス ポイントでサポートされます。専用スペクトル センサーとして設定すると、Spectrum Expert Connect 自律アクセス ポイントは Cisco Spectrum Expert に接続できます。Spectrum Expert モードは、独立したモードであり、モニタ モードのサブセットではありません。

Spectrum Expert モードを有効にするには、次の手順を実行します。

ステップ 1　[Spectrum Expert] アイコンをクリックします。

ステップ 2　[Network] > [Network Interface] を選択します。

ステップ 3　[Radio0-802.11n 2G.Hz] または [Radio0-802.11n 5G.Hz] をクリックします。

ステップ 4　[Enable] をクリックします。

ステップ 5　[Spectrum] オプション ボタンをクリックします。

ステップ 6　[Apply] をクリックします。

Spectrum Expert モードは、AP3500、AP3600、AP2600、AP1550 シリーズなどのすべての CleanAir 対応のアクセス ポイントでサポートされます。

Spectrum Expert の接続の設定

アクセス ポイントを Spectrum Expert として設定するには、次のコマンドを使用します。

- AP(config)#**interface dot11Radio 0**
- AP(config-if)#**station-role spectrum**
- AP(config-if)# **no shutdown**
- AP# **show spectrum status**

Spectrum Expert は、Internet Explorer でのみサポートされます。Spectrum Expert を起動にする前に、次の設定を変更します。

ステップ 1　[Tools] > [Internet options] > [Security] > [custom level] > [ActiveX Controls & plug-ins] > [Initialize and script ActiveX controls not marked as safe for scripting] を選択します。

ステップ 2　[Enable] オプション ボタンをクリックします。

次のポップアップ メッセージは無視できます。

```
Your current security settings put computer at risk.
```

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、ワイヤレス 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ワイヤレス デバイスを設定する手順の詳細は、第 13 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 を介して実装され、AAA コマンドを使用してのみイネーブルにできます。

（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については、リリース 12.3 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。

- RADIUS のデフォルト設定（5-11 ページ）
- RADIUS ログイン認証の設定（5-12 ページ）（必須）
- AAA サーバ グループの定義（5-13 ページ）（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（5-15 ページ）（任意）
- RADIUS の設定の表示（5-16 ページ）

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 経由でワイヤレス 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（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。 • *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。 • **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」セクション（13-5 ページ）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。

	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 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にワイヤレス デバイスを設定できます。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。
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、ワイヤレス 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、ワイヤレス 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。 **（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。 ワイヤレス 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。ワイヤレス 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。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、ワイヤレス デバイスはサーバ グループ コンフィギュレーション モードへ移行します。

	コマンド	目的
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。
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」セクション（5-12 ページ）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、ワイヤレス 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 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 1812 acct-port 1813
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 1812 acct-port 1813
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 認証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 許可がイネーブルの場合、ワイヤレス 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 プロファイルから取得した情報を使用して、ユーザ セッションを設定します。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。

グローバル コンフィギュレーション 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 group 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 group 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ワイヤレス デバイスを設定します。
ステップ 3	**aaa authorization exec group 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、ワイヤレス 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**	（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。

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。

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+）を使用してワイヤレス 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ワイヤレス デバイスを設定する手順の詳細は、第 13 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 を介して実装され、AAA コマンドを使用してのみ有効にできます。

（注）　この項で使用されるコマンドの構文および使用方法の詳細については、『*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。

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 経由でワイヤレス 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（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、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。その方式が失敗すれば、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。 • *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。 • **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。
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 認証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 許可がイネーブルの場合、ワイヤレス 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 プロファイルから取得した情報を使用して、ユーザ セッションを設定します。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。

グローバル コンフィギュレーション 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 group 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） 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 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 group 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ワイヤレス デバイスを設定します。
ステップ 3	**aaa authorization exec group 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、ワイヤレス 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**	（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+ 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。

イーサネットの速度およびデュプレックスの設定

ワイヤレス 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。ワイヤレス 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** を使用することを推奨します。ワイヤレス 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、ワイヤレス デバイスがリブートします。ワイヤレス 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、ワイヤレス 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、ワイヤレス デバイスがスイッチからインライン電源を受け取ると、そのワイヤレス デバイスはリブートします。

(注)　ワイヤレス 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、ワイヤレス 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。ワイヤレス 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ワイヤレス 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 gigabitethernet0**	インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**speed** {**10** | **100** | **1000** | **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**	(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。

アクセス ポイントの無線ネットワーク管理の設定

ワイヤレス 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。無線ネットワーク マネージャ(WNM)は無線 LAN 上のデバイスを管理します。

ワイヤレス 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 を実装するようにワイヤレス デバイスを設定します。ワイヤレス 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機能は使用できません。

(注)　ワイヤレス 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。ワイヤレス 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 9 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 にワイヤレス 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 をイネーブルにします。
ステップ 3	**aaa authentication login default local**	ローカルのユーザ名データベースを使用するように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 default 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 default local**	ネットワーク関連のすべてのサービス要求に対するユーザ AAA 認証を設定します。
ステップ 6	**username** *name* [**privilege** *level*] {**password** *encryption-type password*}	ローカル データベースを使用し、ユーザ名ベースの認証システムを設定します。 ユーザごとにコマンドを繰り返し入力します。 • *name* には、ユーザ ID を 1 ワードで指定します。スペースと引用符は使用できません。 • (任意) *level* には、アクセス権を得たユーザに設定する権限レベルを指定します。指定できる範囲は 0 ～ 15 です。レベル 15 では特権 EXEC モードでのアクセスが可能です。レベル 0 では、ユーザ EXEC モードでのアクセスとなります。 • *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、ワイヤレス 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 文字で、埋め込みスペースを使用でき、**username** コマンドの最後のオプションとして指定します。 (注)　TAB、?、$、+、および [は、パスワードには無効な文字です。
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。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。

認証キャッシュとプロファイルの設定

認証キャッシュとプロファイル機能を使用すると、アクセス ポイントがユーザのために認証/許可応答をキャッシュできるようになります。このため、次回の認証/許可要求を AAA サーバに送信しなくて済むようになります。

(注)　この機能は、アクセス ポイントの Admin 認証だけにサポートされています。

この機能をサポートする次のコマンドが、Cisco IOS Release 12.3(7) に用意されています。

```
cache expiry
cache authorization profile
cache authentication profile
aaa cache profile
```

(注)　これらのコマンドについては、『*Command Reference for Cisco Aironet Access Points and Bridges*』を参照してください。

次の例は、Admin 認証用に設定したアクセス ポイントの設定例です。認証キャッシュを有効に設定した状態の TACACS+ を使用しています。この例では TACACS サーバを使用していますが、アクセス ポイントは RADIUS を使用して Admin 認証用に設定できます。

```
version 12.3
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname ap
!
!
username Cisco password 7 123A0C041104
username admin privilege 15 password 7 01030717481C091D25
ip subnet-zero
!
!
aaa new-model
!
!
aaa group server radius rad_eap
server 192.168.134.229 auth-port 1645 acct-port 1646
!
aaa group server radius rad_mac
server 192.168.134.229 auth-port 1645 acct-port 1646
!
aaa group server radius rad_acct
server 192.168.134.229 auth-port 1645 acct-port 1646
!
aaa group server radius rad_admin
server 192.168.134.229 auth-port 1645 acct-port 1646
cache expiry 1
cache authorization profile admin_cache
```

```
cache authentication profile admin_cache
!
aaa group server tacacs+ tac_admin
server 192.168.133.231
cache expiry 1
cache authorization profile admin_cache
cache authentication profile admin_cache
!
aaa group server radius rad_pmip
!
aaa group server radius dummy
!
aaa authentication login default local cache tac_admin group tac_admin
aaa authentication login eap_methods group rad_eap
aaa authentication login mac_methods local
aaa authorization exec default local cache tac_admin group tac_admin
aaa accounting network acct_methods start-stop group rad_acct
aaa cache profile admin_cache
all
!
aaa session-id common
!
!
!
bridge irb
!
!
interface Dot11Radio0
no ip address
no ip route-cache
shutdown
speed basic-1.0 basic-2.0 basic-5.5 6.0 9.0 basic-11.0 12.0 18.0 24.0 36.0 48.0 54.0
station-role root
bridge-group 1
bridge-group 1 subscriber-loop-control
bridge-group 1 block-unknown-source
no bridge-group 1 source-learning
no bridge-group 1 unicast-flooding
bridge-group 1 spanning-disabled
!
interface Dot11Radio1
no ip address
no ip route-cache
shutdown
speed basic-6.0 9.0 basic-12.0 18.0 basic-24.0 36.0 48.0 54.0
station-role root
bridge-group 1
bridge-group 1 subscriber-loop-control
bridge-group 1 block-unknown-source
no bridge-group 1 source-learning
no bridge-group 1 unicast-flooding
bridge-group 1 spanning-disabled
!
interface FastEthernet0
no ip address
no ip route-cache
duplex auto
speed auto
bridge-group 1
no bridge-group 1 source-learning
bridge-group 1 spanning-disabled
!
interface BVI1
ip address 192.168.133.207 255.255.255.0
```

```
no ip route-cache
!
ip http server
ip http authentication aaa
no ip http secure-server
ip http help-path http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag
ip radius source-interface BVI1
!
tacacs-server host 192.168.133.231 key 7 105E080A16001D1908
tacacs-server directed-request
radius-server attribute 32 include-in-access-req format %h
radius-server host 192.168.134.229 auth-port 1645 acct-port 1646 key 7 111918160405041E00
radius-server vsa send accounting
!
control-plane
!
bridge 1 route ip
!
!
!
line con 0
transport preferred all
transport output all
line vty 0 4
transport preferred all
transport input all
transport output all
line vty 5 15
transport preferred all
transport input all
transport output all
!
end
```

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、ワイヤレス 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（5-24 ページ）
- DHCP サーバ アクセス ポイントのモニタリングと維持（5-26 ページ）

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。

（注）　アクセス ポイントを DHCP サーバとして設定すると、IP アドレスがそのサブネット上のデバイスに割り当てられます。このデバイスは、サブネット上の他のデバイスと通信しますが、それ以上先とは通信しません。サブネットより先にデータを送信する必要がある場合は、デフォルトのルータを割り当てる必要があります。デフォルト ルータの IP アドレスには、DHCP サーバとして設定したアクセス ポイントと同じサブネット上のものを設定してください。

DHCP 関連のコマンドとオプションの詳細は、リリース 12.3 の『*Cisco IOS IP Configuration Guide*』の「Configuring DHCP」の章を参照してください。「Configuring DHCP」の章を参照するには、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/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、デフォルト ルータを指定します。

	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	**ip dhcp excluded-address** *low_address* [*high_address*]	ワイヤレス デバイスが割り当てるアドレス範囲から、ワイヤレス デバイスの IP アドレスを除外します。IP 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。 ワイヤレス 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。 (任意)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 要求に応じてワイヤレス 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 コンフィギュレーション 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。ワイヤレス 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。 (任意)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。プレフィックス長は、スラッシュ (/) で開始する必要があります。
ステップ 5	**lease** { *days* [*hours*] [*minutes*] | **infinite** }	ワイヤレス 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。 • (任意)hours: 時間数でリース期間を設定します。 • (任意)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	**default-router** *address* [*address2 ... address 8*]	サブネット上の DHCP クライアントに対し、デフォルト ルータの IP アドレスを指定します。求められるのは 1 つの IP アドレスですが、コマンド行 1 行につき最大 8 つまでのアドレスを指定できます。
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。

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

この例では、ワイヤレス 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。IP アドレスの範囲は省略し、デフォルト ルータを割り当てています。

```
AP# configure terminal
AP(config)# ip dhcp excluded-address 172.16.1.1 172.16.1.20
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)# default-router 172.16.1.1
AP(dhcp-config)# end
```

DHCP サーバ アクセス ポイントのモニタリングと維持

次の項では、DHCP サーバ アクセス ポイントのモニタ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（5-26 ページ）
- clear コマンド（5-27 ページ）
- debug コマンド（5-27 ページ）

show コマンド

DHCP サーバとしてのワイヤレス 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。ワイヤレス デバイスの IP アドレスを入力すると、ワイヤレス 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 データベースのアドレス競合をクリアします。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** }

ワイヤレス 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** 形式を使用します。

アクセス ポイントのセキュア シェルの設定

この項では、セキュア シェル（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、『*Cisco IOS Security Command Reference for Release 12.3*』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 リリースでは、どちらの SSH バージョンもサポートします。バージョン番号を指定しないと、アクセス ポイントがデフォルトのバージョン 2 になります。

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（詳細については、「RADIUS によるアクセス ポイントへのアクセスの制御」セクション（5-11 ページ）を参照してください）
- ローカル認証および許可（詳細については、「アクセス ポイントのローカル認証および許可の設定」セクション（5-21 ページ）を参照）

SSH の詳細については、次の URL にある『*Secure Shell Configuration Guide*』を参照してください。
http://www.cisco.com/en/US/docs/ios-xml/ios/security/config_library/12-4t/secuser-12-4t-library.html

（注）　このソフトウェア リリースの SSH 機能は IP Security（IPsec）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 の設定方法と SSH 設定の表示方法の詳細については、次の URL にある『*Secure Shell Configuration Guide*』を参照してください。
http://www.cisco.com/en/US/docs/ios-xml/ios/security/config_library/12-4t/secuser-12-4t-library.html

セキュア コピー プロトコルのサポート

セキュア コピー プロトコル（SCP）は、セキュリティのためにセキュア シェル（SSH）を使用してネットワーク上のホスト間のファイル転送をサポートします。Cisco IOS リリース 15.2(2)JB は、アクセス ポイント自体へのログイン中に、アクセス ポイントとの間の SCP ファイル転送をサポートします。

AAA 認証を使用してデータ転送が制限されます。SCP では、AAA 認証を使用してユーザ名とパスワードを確認して、転送中のデータの完全性と機密性を確保できます。

SSH を設定するには、次のコマンドを使用します。

- **ip hostname**
- **ip domain-name**
- **crypto key generate rsa (512, 1024,2048)**
- **ip SSH version**
- **aaa new-model**
- **aaa authentication login default local**
- **aaa authorization exec default local**
- **username cisco privilege 15 password 0 cisco**

SCP を実行するには、**copy run scp://url** コマンドを使用します。

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、ワイヤレス デバイスを設定できます。ワイヤレス 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。

ここでは、次の情報について説明します。

クライアント ARP キャッシングの概要

ワイヤレス 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 要求をワイヤレス 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。ワイヤレス 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、ワイヤレス 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、ワイヤレス 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。ワイヤレス デバイスがキャッシュにない IP アドレスに向けた ARP 要求を受け取ると、ワイヤレス デバイスはその要求をドロップして転送しません。ワイヤレス 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、ワイヤレス 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、ワイヤレス デバイスはワイヤレス デバイスに既知の 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、ワイヤレス 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 要求をドロップします。

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ワイヤレス 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**]	ワイヤレス デバイスでの ARP キャッシングを有効にします。 • （任意）ワイヤレス 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。

	コマンド	目的
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。

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
```

システム日時の管理

ワイヤレス デバイスのシステムの時刻と日付は、Simple Network Time Protocol(SNTP)を使用して自動的に管理することも、ワイヤレス 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 12.3 の『*Cisco IOS Configuration Fundamentals Command Reference*』を参照してください。

ここでは、次の設定情報について説明します。

- Simple Network Time Protocol の概要(5-30 ページ)
- SNTP の設定(5-31 ページ)
- 手動での日時の設定(5-31 ページ)

Simple Network Time Protocol の概要

簡易ネットワーク タイム プロトコル(SNTP)とは、クライアント専用バージョンの簡易版 NTP です。SNTP は、NTP サーバから時間を受信するだけで、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。通常、SNTP は 100 ミリ秒以内の精度で時刻を提供しますが、NTP のような複雑なフィルタリングや統計メカニズムは提供しません。

SNTP は、設定済みのサーバからパケットを要求して受け入れるように設定するか、任意の送信元から NTP ブロードキャスト パケットを受け入れるように設定できます。複数の送信元が NTP パケットを送信している場合、最適な層にある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。これらの両方を満たすサーバが複数ある場合は、時刻パケットを最初に送信したサーバが選択されます。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

SNTP は、デフォルトでディセーブルになっています。アクセス ポイントで SNTP をイネーブルにするには、表 5-4 に示すコマンドのいずれか、または両方をグローバル コンフィギュレーション モードで使用します。

表 5-4　SNTP コマンド

コマンド	目的
sntp server {*address* | *hostname*} [**version** *number*]	NTP サーバからの NTP パケットを要求するように SNTP を設定します。
sntp broadcast client	任意の NTP ブロードキャストからの NTP パケットを受け入れるように SNTP を設定します。

各 NTP サーバについて、**sntp server** コマンドを 1 回入力します。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。

手動での日時の設定

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、次にシステムを再起動するまで正確です。手動設定は最後の手段としてのみ使用することを推奨します。ワイヤレス 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。

ここでは、次の設定情報について説明します。

- システム クロックの設定（5-31 ページ）
- 日時設定の表示（5-32 ページ）
- タイム ゾーンの設定（5-32 ページ）
- 夏時間の設定（5-33 ページ）

システム クロックの設定

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

システム クロックを設定するには、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	**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、時刻を時間（24 時間形式）、分、秒で指定します。指定された時刻は、設定されたタイム ゾーンに基づきます。 • *day* には、当月の日付で日を指定します。 • *month* には、月を名前で指定します。 • *year* には、年を指定します（常に 4 桁で指定）。
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**	（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。

次に、システム クロックを手動で 2001 年の 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
```

日時設定の表示

日時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、信頼性がある（正確であると信じられる）かどうかを示す *authoritative* フラグを維持します。システム クロックがタイミング ソースによって設定されている場合は、フラグを設定します。時刻が信頼性のないものである場合は、表示目的でのみ使用されます。クロックが信頼できず、*authoritative* フラグも設定されていなければ、ピアの時刻が無効でも、フラグはピアがクロックと同期しないようにします。

show clock の表示の前にある記号は、次の意味があります。

- *:時刻は信頼できません。
- （空白）:時刻は信頼できます。
- .:時刻は信頼できますが、NTP は同期していません。

タイム ゾーンの設定

手動でタイム ゾーンを設定するには、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	**clock timezone** *zone hours-offset* [*minutes-offset*]	タイム ゾーンを設定します。 ワイヤレス デバイスは内部時間を協定世界時（UTC）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だけに使用されます。 • *zone* には、標準時間が施行されているとき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 からの時差を入力します。 • （任意）*minutes-offset* には、UTC からの分差を入力します。

	コマンド	目的
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。

clock timezone グローバル コンフィギュレーション コマンドの**minutes-offset** 変数は、現地のタイム ゾーンと UTC との時差が分単位である場合に使用できます。たとえば、カナダ大西洋沿岸のある区域のタイム ゾーン(大西洋標準時(AST))は UTC-3.5 です。この場合、3 は 3 時間、.5 は 50% を意味します。この場合、必要なコマンドは**clock timezone AST -3 30** です。

時刻を UTC に設定するには、**no clock timezone** 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。

夏時間の設定

毎年特定の曜日に夏時間が開始して終了する地域に夏時間を設定するには、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	**clock summer-time** *zone* **recurring** [*week day month hh*:*mm week day month hh*:*mm* [*offset*]]	毎年指定した日に開始および終了するように夏時間を設定します。 夏時間はデフォルトでディセーブルに設定されています。パラメータなしで**clock summer-time** *zone* **recurring** を指定すると、夏時間のルールは米国のルールをデフォルトにします。 • *zone* には、夏時間が施行されているときに表示されるタイム ゾーンの名前(たとえば PDT)を入力します。 • (任意)*week* には、月の何週目かを指定します(1 ～ 5、または **last**)。 • (任意)*day* には、曜日を指定します(Sunday、Monday など)。 • (任意)*month* には、月を指定します(January、February など)。 • (任意)*hh*:*mm* には、時刻を時間(24 時間形式)と分で指定します。 • (任意)*offset* には、夏時間の間、追加する分の数を指定します。デフォルトは 60 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**	(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。

clock summer-time グローバル コンフィギュレーション コマンドの最初の部分では夏時間の開始時期を、2 番目の部分では終了時期を指定します。すべての時刻は、現地のタイム ゾーンを基準にしています。開始時間は標準時を基準にしています。終了時間は夏時間を基準にしています。開始月が終了月より後の場合は、システムでは南半球にいると見なされます。

次に、夏時間が 4 月の第一日曜の 2 時に始まり、10 月の最終日曜の 2 時に終わるように指定する例を示します。

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

ユーザの居住地域の夏時間が定期的なパターンに従わない（次の夏時間のイベントの正確な日時を設定する）場合は、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	**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*]]	最初の日付で夏時間開始の日付を、2 番めの日付で終了の日付を設定します。 夏時間はデフォルトでディセーブルに設定されています。 • *zone* には、夏時間が施行されているときに表示されるタイム ゾーンの名前（たとえば PDT）を入力します。 • （任意）*week* には、月の何週目かを指定します（1 ～ 5、または **last**）。 • （任意）*day* には、曜日を指定します（Sunday、Monday など）。 • （任意）*month* には、月を指定します（January、February など）。 • （任意）*hh*:*mm* には、時刻を時間（24 時間形式）と分で指定します。 • （任意）*offset* には、夏時間の間、追加する分の数を指定します。デフォルトは 60 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**	（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。

clock summer-time グローバル コンフィギュレーション コマンドの最初の部分では夏時間の開始時期を、2 番目の部分では終了時期を指定します。すべての時刻は、現地のタイム ゾーンを基準にしています。開始時間は標準時を基準にしています。終了時間は夏時間を基準にしています。開始月が終了月より後の場合は、システムでは南半球にいると見なされます。

夏時間をディセーブルにするには、**no clock summer-time** 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、夏時間が 2013 年 10 月 12 日の 2 時に始まり、2014 年 4 月 26 日の 2 時に終わるように設定する例を示します。

```
AP(config)# clock summer-time pdt date 12 October 2013 2:00 26 April 2014 2:00
```

HTTP アクセスの定義

デフォルトでは、80 が HTTP アクセスに使用され、ポート 443 が HTTPS アクセスに使用されます。この値は、ユーザがカスタマイズできます。GUI を使用して HTTP アクセスを定義するには、次の手順に従います。

ステップ 1　アクセス ポイントの GUI から、[Services] > [HTTP] の順にクリックします。[Service: HTTP-Web server] 画面が表示されます。

ステップ 2　この画面に、目的の HTTP と HTTPS のポート番号を入力します。このポート番号フィールドに値を入力しないと、デフォルト値が使用されます。

ステップ 3　[Apply] をクリックします。

CLI を使用して HTTP アクセスを定義するには、次の手順に従います。

ステップ 1　AP(config)# **conf t**

ステップ 2　AP(config)# **ip http port** *value*

ステップ 3　AP(config)# **ip http secure-port** *value*

システム名とプロンプトの設定

ワイヤレス 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ていない場合は、システム名の最初の 20 文字をシステム プロンプトとして使用します。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 コンフィギュレーション 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については、『*Cisco IOS Configuration Fundamentals Command Reference*』および『*Cisco IOS IP and IP Routing Command Reference*』ガイドを参照してください。

ここでは、次の設定情報について説明します。

- デフォルトのシステム名およびプロンプトの設定(5-35 ページ)
- システム名の設定(5-35 ページ)
- DNS の概要(5-36 ページ)

デフォルトのシステム名およびプロンプトの設定

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

手動でシステム名を設定するには、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	**hostname** *name*	手動でシステム名を設定します。 デフォルト設定は *ap* です。 (注)　システム名を変更する場合、ワイヤレス 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、ワイヤレス 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 ポイントを区別することが重要な場合、システム名の一意の部分を最初の 15 文字に含めてください。
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**	(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。

システム名を設定すると、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 コンフィギュレーション コマンド **no hostname** を使用します。

DNS の概要

ドメイン ネーム システム(DNS)プロトコルは、DNS 分散型データベースを制御し、これによりホスト名を IP アドレスに対応付けできます。ワイヤレス デバイスに DNS を設定すると、**ping**、**telnet**、**connect**、などすべての IP コマンドおよび関連する 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 によって定義される階層型の命名方式では、デバイスを場所またはドメインで特定できます。ドメイン名は、ピリオド(.)を区切り文字として使用して構成されています。たとえば、シスコは、IP で *com* というドメイン名に分類される商業組織なので、ドメイン名は *cisco.com* となります。このドメイン内の File Transfer Protocol(FTP)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。

IP ではドメイン名をトラッキングするために、ドメイン ネーム サーバという概念が定義されています。ドメイン ネーム サーバの役割は、名前から IP アドレスへのマッピングをキャッシュ(またはデータベース)に保存することです。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 サーバを指定し、DNS を有効にします。

ここでは、次の設定情報について説明します。

- DNS のデフォルト設定(5-37 ページ)
- DNS の設定(5-37 ページ)
- DNS の設定の表示(5-38 ページ)

DNS のデフォルト設定

表 5-5 に、DNS のデフォルト設定を示します。

表 5-5　DNS のデフォルト設定

機能	デフォルト設定
DNS イネーブル ステート	ディセーブル
DNS デフォルト ドメイン名	未設定
DNS サーバ	ネーム サーバのアドレスが未設定

DNS の設定

特権 EXEC モードから、次の手順に従って DNS を使用するようにワイヤレス 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）を作成するときに使用するデフォルトのドメイン名を定義します。 ドメイン名を未修飾の名前から区切るために使用される最初のピリオドは入れないでください。 ブート時にはドメイン名は設定されていませんが、ワイヤレス 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*]	1 つまたは複数のネーム サーバのアドレスを指定して、名前およびアドレスの解決に使用します。 最大 6 つのネーム サーバを指定できます。各サーバ アドレスはスペースで区切ります。最初に指定されたサーバが、プライマリ サーバです。ワイヤレス 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は、バックアップ サーバにクエリが送信されます。
ステップ 4	**ip domain-lookup**	（任意）ワイヤレス 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、デフォルトでイネーブルにされています。 ユーザのネットワークデバイスが、名前の割り当てを制御できないネットワーク内のデバイスと接続する必要がある場合、グローバルなインターネットのネーミング方式（DNS）を使用して、ユーザの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**	（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。

ワイヤレス 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 コンフィギュレーション 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、**no ip domain-name** *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。ネームサーバのアドレスを削除するには、**no ip name-server** *server-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。ワイヤレス デバイスで DNS を無効にするには、グローバル コンフィギュレーション コマンド **no ip domain-lookup** を使用します。

DNS の設定の表示

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)　ワイヤレス デバイスに DNS が設定されている場合、**show running-config** コマンドを実行すると、サーバの名前ではなく IP アドレスが表示される場合があります。

バナーの作成

今日のお知らせ(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。表示されるのは、MoTD バナーの後で、ログイン プロンプトが表示される前です。

(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 12.3 の『*Cisco IOS Configuration Fundamentals Command Reference*』を参照してください。

ここでは、次の設定情報について説明します。

- バナーのデフォルト設定(5-38 ページ)
- Message-of-the-Day ログイン バナーの設定(5-38 ページ)
- ログイン バナーの設定(5-39 ページ)

バナーのデフォルト設定

MoTD およびログイン バナーは設定されません。

Message-of-the-Day ログイン バナーの設定

ワイヤレス デバイスにログインしたときに画面に表示される 1 行以上の行のメッセージ バナーを作成できます。

MoTD ログイン バナーを設定するには、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	**banner motd** *c message c*	MoTD バナーを指定します。 *c* にはポンド記号(#)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 テキストの始まりと終わりを表します。終わりの区切り文字の後ろの文字は廃棄されます。 *message* には、255 文字までのバナー メッセージを入力します。メッセージ内には区切り文字を使用できません。
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**	(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。

MoTD バナーを削除するには、**no banner motd** 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、開始および終了区切り文字にポンド記号(#)を使用して、ワイヤレス 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 #
This is a secure site.Only authorized users are allowed.
For access, contact technical support.
#
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 '^]'.

This is a secure site.Only authorized users are allowed.
For access, contact technical support.

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。バナーが表示されるのは、MoTD バナーの後で、ログイン プロンプトが表示される前です。

ログイン バナーを設定するには、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	**banner login** *c message c*	ログイン メッセージを指定します。 *c* にはポンド記号(#)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 テキストの始まりと終わりを表します。終わりの区切り文字の後ろの文字は廃棄されます。 *message* には、255 文字までのログイン メッセージを入力します。メッセージ内には区切り文字を使用できません。
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**	(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。

ログイン バナーを削除するには、**no banner login** 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、開始および終了区切り文字にドル記号($)を使用して、ワイヤレス 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 $
Access for authorized users only.Please enter your username and password.
$
AP(config)#
```

自律 Cisco Aironet アクセス ポイントを Lightweight モードにアップグレードする方法

(注)　GUI または CLI を使用して自律アクセス ポイントの Cisco IOS イメージのみをアップグレードする方法については、次の URL を参照してください。
http://www.cisco.com/en/US/tech/tk722/tk809/technologies_configuration_example09186a00809f0e94.shtml.

ネットワーク上で無線 LAN コントローラと通信できるよう、自律 Cisco Aironet アクセス ポイントを Lightweight モードにアップグレードするユーティリティが用意されています。アップグレード ユーティリティの使用方法の詳細については、次の URL にある『*Upgrading Autonomous Cisco Aironet Access Points to Lightweight Mode* 』を参照してください。

http://www.cisco.com/en/US/docs/wireless/access_point/conversion/lwapp/upgrade/guide/lwapnote.html

自律アクセス ポイントを Lightweight モードに変換するには、アクセス ポイントに Telnet し、次のコマンドを実行します。

archive download-sw {/overwrite | /reload} tftp: //location/image-name