CHAPTER 10

無線デバイスの管理

このモジュールでは、次のワイヤレス デバイス管理タスクについて説明します。

無線デバイスへのアクセスのセキュリティ保護

アクセス ポイントのハードウェアおよびソフトウェアの管理

無線デバイスの通信管理

モード ボタン機能のディセーブル化

無線デバイスの MODE ボタンをディセーブルにするには、**[no] boot mode-button** コマンドを使用します。

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でアクセス 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。

（注）　無線デバイスをリブートするには、ルータの Cisco IOS CLI から **service-module wlan-ap reset** コマンドを使用してください。このコマンドの詳細については、「無線デバイスのリブート」（P.10-22）を参照してください。

MODE ボタンはデフォルトでイネーブルに設定されています。アクセス ポイントの MODE ボタンをディセーブルにするには、特権 EXEC モードで開始し、次のステップに従います。

手順の概要

1. **configure terminal**
2. **no boot mode-button**
3. **end**

手順の詳細

	コマンドまたはアクション	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**	特権 EXEC モードに戻ります。 **（注）**　この設定は保存する必要はありません。

モード ボタンのステータスを確認するには、特権 EXEC モードで **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** および **show boot mode-button** コマンドを実行すると、通常は次のような応答が表示されます。

```
ap# show boot
BOOT path-list: flash:/c1200-k9w7-mx-v123_7_ja.20050430/c1200-k9w7-mx.v123_7_ja.20050430
Config file: flash:/config.txt
Private Config file: flash:/private-config
Enable Break: no
Manual boot:no
Mode button:on
Enable IOS break: no
HELPER path-list:
NVRAM/Config file
    buffer size: 32768

ap# show boot mode-button
on
ap#
```

（注）　特権 EXEC パスワードがわかっていれば、**boot mode-button** コマンドを使用して、モード 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を制限します。

ワイヤレス デバイスへの不正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。このペアによって、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」（P.10-8）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、パスワードに無効な文字です。

- ユーザ名とパスワードのペアは、セキュリティ サーバのデータベースに一元的に保管されます。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」（P.10-11）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。特権レベルにより、ユーザがネットワーク装置にログインした後に発行できるコマンドが定義されます。

（注）　ここで使用す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 for Release 12.4*』を参照してください。

ここでは、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 10-1 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 10-1　デフォルト パスワードと特権レベル

権限レベル	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 モードで **no enable password** コマンドを実行すると、enable パスワードが削除されますが、このコマンドを使用する場合は十分な注意が必要です。enable パスワードを削除すると、特権 EXEC モードからロックアウトされます。

特権 EXEC モードから静的 enable パスワードを設定または変更するには、次のステップを実行します。

手順の概要

1. **configure terminal**
2. **enable password** *password*
3. **end**
4. **show running-config**
5. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	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* : 1 ～ 25 文字の英数字の文字列。文字列を数字で始めることはできません。大文字と小文字が区別されます。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。パスワードには疑問符（?）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に、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** と入力します。 2. Crtl+V キーを押します。 3. **?123** と入力します。 • イネーブル パスワードを入力するよう求められた場合は Ctrl+V キーを入力する必要はありません。パスワード プロンプトで **abc?123** と入力します。 **（注）** TAB、?、$、+、および [は、パスワードに無効な文字です。
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。

次の例は、enable パスワードを *l1u2c3k4y5* に変更する方法を示しています。このパスワードは暗号化されず、レベル 15 へのアクセス（標準の特権 EXEC モード 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およびイネーブル シークレット パスワードの保護

特にネットワーク間を行き交う、または TFTP サーバに保存されるパスワードに対してセキュリティ レイヤを追加するには、グローバル コンフィギュレーション モードで **enable password** コマンドまたは **enable secret** コマンドのいずれかを使用できます。いずれのコマンドを使用しても、ユーザが特権 EXEC モード（デフォルト）にアクセスするために、または指定した特権レベルにアクセスするために入力が必要な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。これら 2 つのコマンドを同時に有効にすることはできません。

enable パスワードおよび enable secret パスワードに暗号化を設定するには、特権 EXEC モードで開始し、次のステップに従います。

手順の概要

1. **configure terminal**
2. **enable password** [**level** *level*] {*password* | *encryption-type encrypted*-**password**}
   または
   enable secret [**level** *level*] {*password* | *encryption-type encrypted*-**password**}
3. **service password-encryption**
4. **end**
5. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	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。

	コマンドまたはアクション	目的
ステップ 2	**enable password** [**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	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ます。これは非可逆的な暗号化方式を使用して保存されます。 • *level*：（任意）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*：1 ～ 25 文字の英数字の文字列。文字列を数字で始めることはできません。大文字と小文字が区別されます。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。 • *encryption-type*：（任意）5 だけを入力してください。シスコ独自の暗号化アルゴリズムを使用できます。暗号化タイプを指定する場合は、別のアクセス ポイントの無線デバイス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 パスワードを入力した場合は特権 EXEC モードを再開できません。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 パスワードおよびイネーブル 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ら、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。さまざまなレベルにアクセス可能なコマンドを指定する場合は、グローバル コンフィギュレーション モードで **privilege level** 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」（P.10-9）を参照してください。

パスワード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、特権コマンド パスワード、コンソール パスワード、および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 コンフィギュレーション モードで **no enable password** [**level** *level*] コマンドまたは **no enable secret** [**level** *level*] コマンドを使用します。パスワード暗号化をディセーブルにするには、グローバル コンフィギュレーション モードで **no service password-encryption** 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

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を設定します。ユーザ名とパスワードのペアは回線またはインターフェイスに割り当てられ、これらのペアにより、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。特権レベルを定義したら、ユーザ名とパスワードの各ペアに特定の特権レベルを（対応する権限とともに）指定します。

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するには、特権 EXEC モードで開始し、次のステップに従います。

手順の概要

1. **configure terminal**
2. **username** *name* [**privilege** *level*] {**password** *encryption-type password*}
3. **login local**
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	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、およびパスワードを入力します。 • *name*：1 語でユーザ ID を指定します。スペースや引用符は使用できません。 • *level*：（任意）ユーザがアクセス権を取得した後に持つ特権レベルを指定します。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*：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。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*：ワイヤレス デバイスにアクセスするためにユーザが入力する必要があるパスワード。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 3	**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 4	**end**	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 5	**show running-config**	入力を確認します。
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。

特定のユーザに対してユーザ名認証をディセーブルにするには、グローバル コンフィギュレーション モードで **no username** *name* 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、パスワードを指定しない接続を許可するには、回線コンフィギュレーション モードで **no login** 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 デバイスとの 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。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、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。

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。各モードには、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。**configure** コマンドへのアクセスを制限する場合は、レベル 3 のセキュリティを割り当て、制限されたユーザのグループにそのパスワードを配布できます。

この項では、設定情報について説明します。

- 「コマンドの特権レベルの設定」（P.10-9）
- 「特権レベルへのログインと終了」（P.10-11）

コマンドの特権レベルの設定

コマンド モードに特権レベルを設定するには、特権 EXEC モードで開始し、次のステップに従います。

手順の概要

1. **configure terminal**
2. **privilege** *mode* **level** *level command*
3. **enable password level** *level password*
4. **end**
5. **show running-config**
   または
   show privilege
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	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*	コマンドの特権レベルを設定します。 • *mode*：グローバル コンフィギュレーション モードの場合は **configure**、EXEC モードの場合は **exec**、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**、ライン コンフィギュレーション モードの場合は **line** と入力します。 • *level*：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*：アクセスが制限されるコマンドを指定します。
ステップ 3	**enable password level** *level password*	特権レベルの enable パスワードを指定します。 • *level*：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*：1 ～ 25 文字の英数字の文字列。文字列を数字で始めることはできません。大文字と小文字が区別されます。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。 **（注）** TAB、?、$、+、および [は、パスワードに無効な文字です。
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**	入力を確認します。 **show running-config** コマンドを実行すると、パスワードとアクセス レベルの設定が表示されます。 **show privilege** コマンドを実行すると、特権レベルの設定が表示されます。
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特権レベル 15 に設定されます。

特定のコマンドの特権をデフォルトに戻すには、グローバル コンフィギュレーション モードで **no privilege** *mode* **level** *level command* コマンドを使用します。

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

指定された特権レベルにログインする、あるいは指定された特権レベルを終了するには、特権 EXEC モードで開始し、次のステップに従います。

手順の概要

1. **enable** *level*
2. **disable** *level*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** *level*	指定された特権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*	指定した特権レベルを終了します。 *level* に指定できる範囲は 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

ここでは、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方法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については、『*Cisco IOS Software Configuration Guide for Cisco Aironet Access Points*』の「Configuring Radius and TACACS+ Servers」の章を参照してください。

RADIUS を使用すると、アカウンティングの詳細を取得したり、認証および許可プロセスの柔軟な管理制御を実現できます。RADIUS は、Authentication, Authorization, Accounting（AAA; 認証、許可、アカウンティング）を通じて効率化され、AAA コマンドでだけイネーブルにできます。

（注）　ここで使用す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」（P.10-12）
- 「RADIUS ログイン認証の設定」（P.10-12）（必須）
- 「AAA サーバ グループの定義」（P.10-14）（任意）
- 「ユーザの特権アクセスとネットワーク サービスに対する RADIUS 許可の設定」（P.10-16）（任意）
- 「RADIUS の設定の表示」（P.10-17）

RADIUS のデフォルト設定

RADIUS および AAA は、デフォルトでディセーブルです。

セキュリティの失効を防止するため、ネットワーク管理アプリケーションを使用して RADIUS を設定することはできません。RADIUS を有効にすると、CLI を通じてワイヤレス デバイスにアクセスしてい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ます。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（「default」という名前が指定されています）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、ユーザの認証に使用する、順序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、最初の方式が失敗した場合に認証用のバックアップ システムが確実に機能します。ソフトウェアは、リストの最初の方式を使用してユーザを認証します。この方式が応答しない場合、ソフトウェアは、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。このサイクルのいずれかの時点で認証に失敗した場合、つまりセキュリティ サーバまたはローカル ユーザ名データベースからユーザ アクセスを拒否する応答があった場合には、許可プロセスが停止し、それ以上の認証方式は試行されません。

ログイン認証を設定するには、特権 EXEC モードで開始し、次のステップに従います。この手順は必須です。

手順の概要

1. **configure terminal**
2. **aaa new-model**
3. **aaa authentication login** {**default** | *list-name*} *method1* [*method2...*]
4. **line** [**console** | **tty** | **vty**] *line-number* [*ending-line-number*]
5. **login authentication** {**default** | *list-name*}
6. **end**
7. **show running-config**
8. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**aaa new-model**	AAA をイネーブルにします。

	コマンドまたはアクション	目的
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*：作成するリストの名前を指定する文字列。 • *method1...*：認証アルゴリズムが試み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、『*Cisco IOS Software Configuration Guide for Cisco Aironet Access Points*』の「Configuring Radius and TACACS+ Servers」の章にある「Identifying the RADIUS Server Host」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、認証リストを適用する回線を設定します。
ステップ 5	**login authentication** {**default** | *list-name*}	1 つの回線または複数回線に認証リストを適用します。 • **default** を指定すると、**aaa authentication login** コマンドで作成したデフォルト リストが使用されます。 • *list-name* : **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、グローバル コマンド モードで **no aaa new-model** 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、グローバル コマンド モードで **no aaa authentication login** {**default** | *list-name*} *method1* [*method2...*] コマンドを使用します。ログインの RADIUS 認証をディセーブルにするか、デフォルト値に戻すには、回線コンフィギュレーション モードで **no login authentication** {**default** | *list-name*} 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 ホストの一部を選択して、それら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。

各ホストのエントリが一意の識別情報（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、同一の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ができます。これにより、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。同じ RADIUS サーバに同一のサービス（アカウンティングなど）を実行する 2 つの異なるホスト エントリを設定すると、2 番目に設定されたホスト エントリが最初のホスト 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 アドレスで特定したり、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したりできます。

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。

手順の概要

1. **configure terminal**
2. **aaa new-model**
3. **radius-server host** {***hostname*** | *ip-address*} [**auth-port** *port-number*] [**acct-port** *port-number*] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*]
4. **aaa group server radius** *group-name*
5. **server** *ip-address*
6. **end**
7. **show running-config**
8. **copy running-config startup-config**
9. RADIUS ログイン認証をイネーブルにします。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**aaa new-model**	AAA をイネーブルにします。

	コマンドまたはアクション	目的
ステップ 3	**radius-server host** {*hostname* | *ip-address*} [**auth-port** *port-number*] [**acct-port** *port-number*] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*]	リモート RADIUS サーバ ホストの IP アドレスまたはホスト名を指定します。 • **auth-port** *port-number*：（任意）認証要求用のユーザ データグラム プロトコル（UDP）の宛先ポートを指定します。 • **acct-port** *port-number*：（任意）アカウンティング要求のための UDP 宛先ポートを指定します。 • **timeout** *seconds*：（任意）再送信する前に、ワイヤレス デバイスが RADIUS サーバの応答を待機する間隔。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。 • **retransmit** *retries*：（任意）サーバが応答しない、または応答が遅い場合に RADIUS の要求をサーバに再送信する回数。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。 • **key** *string*：（任意）ワイヤレス デバイスと RADIUS サーバで実行されている RADIUS デーモン間で使用される認証および暗号キーを指定します。 **（注）** このキーはテキスト文字列で、RADIUS サーバで使用される暗号キーと一致する必要があります。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 アドレスに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、および暗号キーをそれぞれ設定してください。
ステップ 4	**aaa group server radius** *group-name*	グループ名を指定して AAA サーバ グループを定義します。 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。

	コマンドまたはアクション	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 グループと関連付けます。 • 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。	『*Cisco IOS Software Configuration Guide for Cisco Aironet Access Points*』の「Configuring Radius and TACACS+ Servers」の章にある「Configuring RADIUS Login Authentication」を参照してください。

指定された RADIUS サーバを削除するには、グローバル コンフィギュレーション モードで **no radius-server host** *hostname* | *ip-address* コマンドを使用します。設定リストからサーバ グループを削除するには、グローバル コンフィギュレーション モードで **no aaa group server radius** *group-name* 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、sg-radius コンフィギュレーション モードで **no server** *ip-address* 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 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フェールオーバー 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
```

ユーザの特権アクセスとネットワーク サービスに対する 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の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。ユーザが要求したサービスにアクセスを許可されるのは、ユーザ プロファイルによって許可された場合だけです。

グローバル コンフィギュレーション モードで **aaa authorization** コマンドに **radius** キーワードを使用すると、特権 EXEC モードへのユーザのネットワーク アクセスを制限するパラメータを設定できます。

aaa authorization exec radius コマンドを実行すると、次の許可パラメータが設定されます。

- 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、許可が省略されます。

特権 EXEC アクセスおよびネットワーク サービスに RADIUS 許可を指定するには、特権 EXEC モードで開始し、次のステップに従います。

手順の概要

1. **configure terminal**
2. **aaa authorization network radius**
3. **aaa authorization exec radius**
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	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ワイヤレス 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、ユーザが特権 EXEC アクセスを持っているかどうか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、グローバル コンフィギュレーション モードで **no aaa authorization** {**network** | **exec**} *method1* コマンドを使用します。

RADIUS の設定の表示

RADIUS 設定を表示するには、特権 EXEC モードで **show running-config** 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については、『*Cisco IOS Software Configuration Guide for Cisco Aironet Access Points*』の「Configuring Radius and TACACS+ Servers」の章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。AAA により TACACS+ が容易になります。また、TACACS+ をイネーブルにするには AAA コマンドを実行する必要があります。

（注）　ここで使用す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。

次の各項で TACACS+ の設定について説明します。

- 「TACACS+ のデフォルト設定」（P.10-18）
- 「TACACS+ ログイン認証の設定」（P.10-18）
- 「特権 EXEC アクセスおよびネットワーク サービスに対する TACACS+ 許可の設定」（P.10-20）
- 「TACACS+ 設定の表示」（P.10-21）

TACACS+ のデフォルト設定

TACACS+ と AAA は、デフォルトでディセーブルに設定されます。

セキュリティの失効を防止するため、ネットワーク管理アプリケーションを使用して TACACS+ を設定することはできません。TACACS+ を有効にすると、CLI を通じてワイヤレス デバイスにアクセスしてい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ます。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（*default* という名前）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、ユーザの認証に使用する、順序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、最初の方式が失敗した場合に認証用のバックアップ システムが確実に機能します。ソフトウェアは、リストの最初の方式を使用してユーザを認証します。この方式が応答しない場合、ソフトウェアは、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。このサイクルのいずれかの時点で認証に失敗した場合、つまりセキュリティ サーバまたはローカル ユーザ名データベースからユーザ アクセスを拒否する応答があった場合には、許可プロセスが停止し、それ以上の認証方式は試行されません。

ログイン認証を設定するには、特権 EXEC モードで開始し、次のステップに従います。この手順は必須です。

手順の概要

1. **configure terminal**
2. **aaa new-model**
3. **aaa authentication login** {**default** | *list-name*} *method1* [*method2...*]
4. **line** [**console** | **tty** | **vty**] *line-number* [*ending-line-number*]
5. **login authentication** {**default** | *list-name*}
6. **end**
7. **show running-config**
8. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	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*：作成するリストの名前を指定する文字列。 • *method1...*：認証アルゴリズムが試み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。グローバル コンフィギュレーション モードで **username** *password* 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、認証リストを適用する回線を設定します。
ステップ 5	**login authentication** {**default** | *list-name*}	1 つの回線または複数回線に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* : **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。

	コマンドまたはアクション	目的
ステップ 7	**show running-config**	入力を確認します。
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、グローバル コンフィギュレーション モードで **no aaa new-model** 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、グローバル コンフィギュレーション モードで **no aaa authentication login** {**default** | *list-name*} *method1* [*method2...*] コマンドを使用します。ログインの TACACS+ 認証をディセーブルにするか、デフォルト値に戻すには、回線コンフィギュレーション モードで **no login authentication** {**default** | *list-name*} 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 サービスに対する 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 モードで **aaa authorization** コマンドに **tacacs+** キーワードを使用すると、特権 EXEC モードへのユーザ ネットワーク アクセスを制限するパラメータを設定できます。

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

- TACACS+ を使用して認証を行った場合は、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、許可が省略されます。

TACACS+ 許可を特権 EXEC アクセスおよびネットワーク サービスに指定するには、特権 EXEC モードで開始し、次のステップに従います。

手順の概要

1. **configure terminal**
2. **aaa authorization network tacacs+**
3. **aaa authorization exec tacacs+**
4. **end**
5. **show running-config**
6. **show running-config**

手順の詳細

	コマンドまたはアクション	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ワイヤレス 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、ユーザが特権 EXEC アクセスを持っているかどうか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、グローバル コンフィギュレーション モードで **no aaa authorization** {**network** | **exec**} *method1* コマンドを使用します。

TACACS+ 設定の表示

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

ワイヤレス ハードウェアおよびソフトウェアの管理

ここでは、次のタスクを実行するための手順について説明します。

- 「無線デバイスの工場出荷時のデフォルト設定へのリセット」（P.10-21）
- 「無線デバイスのリブート」（P.10-22）
- 「無線デバイスのモニタリング」（P.10-22）

無線デバイスの工場出荷時のデフォルト設定へのリセット

無線デバイスのハードウェアおよびソフトウェアを工場出荷時のデフォルト設定にリセットするには、ルータの Cisco IOS 特権 EXEC モードで **service-module wlan-ap0 reset default-config** コマンドを使用します。

注意　データを紛失することがあるため、シャットダウンまたは障害状態から回復する場合は、**service-module wlan-ap0 reset** コマンドだけを使用してください。

無線デバイスのリブート

グレースフル シャットダウンを実行し、無線デバイスをリブートするには、ルータの Cisco IOS 特権 EXEC モードで **service-module wlan-ap0 reload** コマンドを使用します。確認プロンプトで、**Enter** キーを押してアクションを確認するか、**n** と入力してキャンセルします。

自律モードでリロード コマンドを実行すると、リブートする前に設定が保存されます。リブートの試行が成功しない場合は、次のメッセージが表示されます。

```
Failed to save service module configuration.
```

通常、リロード機能は、Lightweight Access Point Protocol（LWAPP）モードで動作しているときには、Wireless LAN Controller（WLC; ワイヤレス LAN コントローラ）で処理されます。**service-module wlan-ap0 reload** コマンドを入力すると、次のメッセージと共にプロンプトが表示されます。

```
The AP is in LWAPP mode. Reload is normally handled by WLC controller.

Still want to proceed? [yes]
```

無線デバイスのモニタリング

ここでは、ルータのハードウェアをモニタリングするためのコマンドについて説明します。

- 「無線デバイスの統計情報の表示」（P.10-22）
- 「無線デバイスのステータスの表示」（P.10-22）

無線デバイスの統計情報の表示

無線デバイスの統計情報を表示するには、特権 EXEC モードで **service-module wlan-ap0 statistics** コマンドを使用します。コマンドの出力例を示します。

```
  CLI reset count = 0
  CLI reload count = 1
  Registration request timeout reset count = 0
  Error recovery timeout reset count = 0
  Module registration count = 10

The last IOS initiated event was a cli reload at *04:27:32.041 UTC Fri Mar 8 2007
```

無線デバイスのステータスの表示

無線デバイスのステータスおよび設定情報を表示するには、特権 EXEC モードで **service-module wlan-ap0 status** コマンドを使用します。コマンドの出力例を示します。

```
Service Module is Cisco wlan-ap0
Service Module supports session via TTY line 2
Service Module is in Steady state
Service Module reset on error is disabled
Getting status from the Service Module, please wait..

Image path = flash:c8xx_19xx_ap-k9w7-mx.acregr/c8xx_19xx_ap-k9w7-mx.acre
gr
System uptime = 0 days, 4 hours, 28 minutes, 5 seconds
Router#d was introduced for embedded wireless LAN access points on Integrated Services
Routers.
```

システム日時の管理

ワイヤレス デバイスのシステムの日付と時刻は、Simple Network Time Protocol（SNTP）を使用して自動的に管理する、あるいはワイヤレス デバイスに日付と時刻を設定して手動で管理できます。

（注）　ここで使用す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 Configuration Fundamentals Command Reference for Release 12.4*』を参照してください。

この項で説明する設定情報は次のとおりです。

簡易ネットワーク タイム プロトコルの概要

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ネットワーク タイム プロトコル（NTP）です。SNTP は、NTP サーバから時間だけを受信します。他のシステムに時刻サービスを提供できません。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、最適なストラタム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/docs/ios/12_1/configfun/configuration/guide/fcd303.html#wp1001075

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。クライアントが現在選択されているサーバからパケットの受信を停止している場合や、上記の基準に基づいてより最適なサーバが検出された場合に限り、SNTP は新しいサーバを選択します。

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 10-2 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 10-2　SNTP コマンド

コマンド	目的
sntp server {*address* | *hostname*} [**version** *number*]	NTP サーバから 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 サーバからの 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入れますが、ストラタムが等しい場合は、設定済みのサーバからの時間を優先します。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

時間の他のソースが利用できない場合は、システムの再起動後に時刻と日付を手動で設定できます。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」（P.10-24）
- 「日時設定の表示」（P.10-25）
- 「タイム ゾーンの設定」（P.10-25）
- 「夏時間の設定」（P.10-26）

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 モードで開始し、次のステップに従います。

手順の概要

1. **clock set** *hh*:*mm*:*ss day month year*
   または
   clock set *hh*:*mm*:*ss month day year*
2. **show running-config**
3. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	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*	次のいずれかの形式を使用して、システム クロックを手動で設定します。 • *hh*:*mm*:*ss*：時間（24 時間形式）、分、秒を指定します。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*：月の日で日付を指定します。 • *month*：フル ネームで月を指定します。 • *year*：4 桁（短縮なし）で年を指定します。
ステップ 2	**show running-config**	入力を確認します。
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

時刻と日付の設定を表示するには、特権 EXEC モードで **show clock** [**detail**] 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 NTP などのタイミング 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い場合は、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

タイム ゾーンを手動で設定するには、特権 EXEC モードで開始し、次のステップに従います。

手順の概要

1. **configure terminal**
2. **clock timezone** *zone hours-offset* [*minutes-offset*]
3. **end**
4. **show running-config**
5. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	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*]	時間帯を設定します。 **（注）** ワイヤレス デバイスは、協定世界時（UTC）で内部時刻を保持します。このコマンドは、手動で時刻を設定したときに表示目的でだけ使用します。 • *zone*：標準時が適用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。デフォルトの設定は UTC です。 • *hours-offset*：UTC からのオフセット時間数を入力します。 • *minutes-offset*：（任意）UTC からのオフセット分数を入力します。
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。

グローバル コンフィギュレーション モードでの *clock timezone* コマンドの **minutes-offset** 変数は、ローカル タイム ゾーンの UTC との時差が 1 時間のパーセンテージである場合に使用できます。たとえば、大西洋沿岸の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% 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、グローバル コンフィギュレーション モードで **no clock timezone** コマンドを使用します。

夏時間の設定

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）を設定するには、特権 EXEC モードで開始し、次のステップに従います。

手順の概要

1. **configure terminal**
2. **clock summer-time** *zone* **recurring** [*week day month hh*:*mm week day month hh*:*mm* [*offset*]]
3. **end**
4. **show running-config**
5. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	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*]]	毎年指定された日に開始および終了する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*：夏時間が有効な場合に表示される時間帯名（PDT など）を指定します。 • *week*：（任意）月の週（1 ～ 5 または **last**）を指定します。 • *day*：（任意）曜日（日曜日など）を指定します。 • *month*：（任意）月（January など）を指定します。 • *hh*:*mm*：（任意）時間と分で時刻（24 時間形式）を指定します。 • *offset*：（任意）夏時間中に追加する分数を指定します。デフォルト値は 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 番め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も後の場合は、南半球にいるものと想定されます。

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サマー タイムが定期的なパターンで実施されていない場合は、特権 EXEC モードでから、次のステップを実行して、次回のサマー タイム イベントの正確な日付と時刻を設定してください。

手順の概要

1. **configure terminal**
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*]]
3. **end**
4. **show running-config**

5. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	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*：夏時間が有効な場合に表示される時間帯名（PDT など）を指定します。 • *week*：（任意）月の週（1 ～ 5 または **last**）を指定します。 • *day*：（任意）曜日（日曜日など）を指定します。 • *month*：（任意）月（January など）を指定します。 • *hh*:*mm*：（任意）時間と分で時刻（24 時間形式）を指定します。 • *offset*：（任意）夏時間中に追加する分数を指定します。デフォルト値は 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 番め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も後の場合は、南半球にいるものと想定されます。

サマー タイムをディセーブルにするには、グローバル コンフィギュレーション モードで **no clock summer-time** コマンドを使用します。

次に、夏時間が 2000 年 10 月 12 日の 2 時に始まり、2001 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 2000 2:00 26 April 2001 2:00
```

システム名およびプロンプトの設定

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 モードで **prompt** コマンドを使用して、手動でプロンプトを設定しないと更新されません。

（注）　ここで使用す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 Configuration Fundamentals Command Reference*』および『*Cisco IOS IP Addressing Services 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。

デフォルトのシステム名とプロンプトの設定

デフォルトのアクセス ポイン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

システム名を手動で設定するには、特権 EXEC モードで開始し、次のステップに従います。

手順の概要

1. **configure terminal**
2. **hostname** *name*
3. **end**
4. **show running-config**
5. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	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。装置同士を区別することがクライアント ユーザにとって重要な場合、システム名の一意の部分が最初の 15 文字に表示されるようにしてください。

	コマンドまたはアクション	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、その名前がシステムプロンプトとしても使用されます。

ホスト名をデフォルトに戻すには、グローバル コンフィギュレーション モードで **no hostname** コマンドを使用します。

DNS の概要

DNS プロトコルは、ドメイン ネーム システム（DNS）を制御します。DNS とは分散型データベースであり、ホスト名を IP アドレスにマッピングできます。ワイヤレス デバイス に DNS を設定すると、**ping**、**telnet**、**connect**、および関連する Telnet サポート操作などの、すべての IP コマンドでホスト名の代わりに IP アドレスを使用できます。

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 では *com* ドメイン名で識別される民間組織です。このためドメイン名は *cisco.com* です。このドメイン内にあるファイル転送プロトコル（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、まずホスト名を明示し、ネットワーク上に存在するネーム サーバを指定し、DNS をイネーブルにします。

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」（P.10-30）
- 「DNS の設定」（P.10-31）
- 「DNS 設定の表示」（P.10-32）

DNS のデフォルト設定

表 10-3 に、デフォルトの DNS 設定を示します。

表 10-3　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 サーバのアドレスは未設定

DNS の設定

DNS を使用するようにワイヤレス デバイスを設定するには、特権 EXEC モードで開始し、次のステップに従います。

手順の概要

1. **configure terminal**
2. **ip domain-name** *name*
3. **ip name-server** *server-address1* [*server-address2 ... server-address6*]
4. **ip domain-lookup**
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	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*	非完全修飾ホスト名（ドット付き 10 進表記ドメイン名のない名前）を完成させるためにソフトウェアが使用する、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が設定されませんが、ワイヤレス デバイスの設定が BOOTP または DHCP サーバから行われている場合、デフォルトのドメイン名前が BOOTP あるいは DHCP サーバによって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イネーブルにします。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。

	コマンドまたはアクション	目的
ステップ 6	**show running-config**	入力を確認します。
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 クエリは発生しません。ピリオド（.）なしでホスト名を設定すると、ピリオドと、それに続くデフォルトのドメイン名がホスト名に追加され、その後で DNS クエリが行われて、名前が IP アドレスにマッピングされます。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 モードで **ip domain-name** コマンドによって設定される値です。ホスト名にピリオド（.）が含まれている場合は、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 コンフィギュレーション モードで **no ip domain-name** *name* コマンドを使用します。ネーム サーバ アドレスを削除するには、グローバル コンフィギュレーション モードで **no ip name-server** *server-address* コマンドを使用します。ワイヤレス デバイスで DNS をディセーブルにするには、グローバル コンフィギュレーション モードで **no ip domain-lookup** コマンドを使用します。

DNS 設定の表示

DNS 設定情報を表示するには、特権 EXEC モードで **show running-config** 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ます。

バナーの作成

今日のお知らせ（MOTD）バナーおよびログイン 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） ここで使用す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 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」（P.10-32）
- 「MOTD ログイン バナーの設定」（P.10-33）
- 「ログイン バナーの設定」（P.10-34）

バナーのデフォルト設定

MOTD およびログイン バナーは設定されていません。

MOTD 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 行または複数行のメッセージ 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 モードで開始し、次のステップに従います。

手順の概要

1. **configure terminal**
2. **banner motd** *c message c*
3. **end**
4. **show running-config**
5. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	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 を指定します。 • *c*：ポンド記号（#）など、目的の区切り文字を入力して **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*：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、グローバル コンフィギュレーション モードで **no banner motd** コマンドを使用します。

次の例は、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。ポンド記号（#）は開始および終了の区切り文字として次のように使用されています。

```
AP(config)# banner motd #
This is a secure site. Only authorized users are allowed.
For access, contact technical support.
#
AP(config)#
```

次の例では、直前の設定のバナーを示します。

```
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。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。

ログイン バナーを設定するには、特権 EXEC モードで開始し、次のステップに従います。

手順の概要

1. **configure terminal**
2. **banner login** *c message c*
3. **end**
4. **show running-config**
5. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	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* : ポンド記号（#）など、目的の区切り文字を入力して **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* : 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、グローバル コンフィギュレーション モードで **no banner login** コマンドを使用します。

次の例は、開始および終了の区切り文字としてドル記号（$）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)#
```

イーサネットの速度およびデュプレックスの設定

Cisco 1941-W ISR インターフェイスは、デフォルトで 1000Mbps の速度とデュプレックス設定だけをサポートし、このインターフェイスは常にアップになっています。ワイヤレス デバイスがスイッチからインライン パワー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。

（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。イーサネット速度およびデュプレックスを設定するには、特権 EXEC モードから、次の手順を実行します。

手順の概要

1. **configure terminal**
2. **interface fastethernet0**
3. **speed {10 | 100 | auto}**
4. **duplex {auto | full | half}**
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	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**	設定インターフェイス 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。 **（注）** 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設定します。 **（注）** 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。

WNM と対話するようにワイヤレス デバイスを設定するには、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詳細な手順については、Cisco.com の『*Using the Access Point as a Local Authenticator*』マニュアルを参照してください。

http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/SecurityLocalAuthent.html

ワイヤレス デバイスをローカル AAA に設定するには、特権 EXEC モードで開始し、次のステップに従います。

手順の概要

1. **configure terminal**
2. **aaa new-model**
3. **aaa authentication login default local**
4. **aaa authorization exec local**
5. **aaa authorization network local**
6. **username** *name* [**privilege** *level*] {**password** *encryption-type password*}
7. **end**
8. **show running-config**
9. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	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 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。 このコマンドをユーザごとに繰り返し入力します。 • *name*：1 語でユーザ ID を指定します。スペースや引用符は使用できません。 • *level*：（任意）ユーザがアクセス権を取得した後に持つ特権レベルを指定します。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*：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。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*：ワイヤレス デバイスへのアクセス権を取得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 文字で指定し、スペースを含めることができます。また、パスワードは、**username** コマンドの最後のオプションとして指定する必要があります。 **（注）** TAB、?、$、+、および [は、パスワードに無効な文字です。
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、グローバル コンフィギュレーション モードで **no aaa new-model** コマンドを使用します。許可をディセーブルにするには、グローバル コンフィギュレーション モードで **no aaa authorization** {**network** | **exec**} *method1* 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により、アクセス ポイントがユーザの認証応答および許可応答をキャッシュできるようになります。このため、これ以降認証および許可要求を AAA サーバに送信しなくても済みます。

（注）　この機能は、アクセス ポイントの Admin 認証にだけ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、『*Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges, Versions 12.4(10b)JA and 12.3(8)JEC*』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。許可キャッシュをイネーブルにした状態で 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 サーバとして機能するように設定する方法について説明します。

- 「DHCP サーバの設定」（P.10-40）
- 「DHCP サーバ アクセス ポイントのモニタリングと維持」（P.10-42）

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 の両方の装置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については、次の URL で『*Cisco IOS IP Addressing Services Configuration Guide, Release 12.4*』の DHCP の部分を参照してください。

http://www.cisco.com/en/US/docs/ios/ipaddr/configuration/guide/iad_dhcp_rdmp_ps6350_TSD_Products_Configuration_Guide_Chapter.html

DHCP サービスを提供するようにアクセス ポイントを設定し、デフォルトのルータを指定するには、特権 EXEC モードで開始し、次のステップに従います。

手順の概要

1. **configure terminal**
2. **ip dhcp excluded-address** *low_address* [*high_address*]
3. **ip dhcp pool** *pool_name*
4. **network** *subnet_number* [*mask* | *prefix-length*]
5. **lease** {*days* [*hours*] [*minutes*] | **infinite**}
6. **default-router** *address* [*address2 ... address 8*]
7. **end**
8. **show running-config**
9. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** **例**： `AP# 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 デバイスは、DHCP アドレス プール サブネット内のすべての 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します。DHCP サーバがクライアントに割り当てない 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入力するには、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作成して、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 プールのサブネットマスクを割り当てるか、アドレス プレフィクスを構成するビット数を指定します。プレフィクスはネットワーク マスクを割り当てる代替法です。プレフィクス長は、スラッシュ（/）で開始する必要があります。

	コマンドまたはアクション	目的
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*：リース期間（日数）。 • *hours*：（任意）リース期間（時間数）。 • *minutes*：（任意）リース期間（分数）。 • **infinite**：リース期間を無期限に設定します。
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てデフォルト ルータの IP アドレスを指定します。 **（注）** 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。

次の例では、ワイヤレス デバイスを DHCP サーバとして設定し、IP アドレスの範囲を除外し、さらにデフォルト ルータを割り当てる方法を示します。

```
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 ポイントのモニタおよび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.10-42）
- 「clear コマンド」（P.10-43）
- 「debug コマンド」（P.10-43）

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、特権 EXEC モードで表 10-4 のコマンドを入力します。

表 10-4　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 IP アドレスを入力して、ワイヤレス デバイスにより記録される衝突を表示します。
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 10-5 のコマンドを使用します。

表 10-5　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 デバッグをイネーブルにするには、次のコマンドを特権 EXEC モードで使用します。

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

ここでは、セキュア シェル（SSH）機能を設定する方法について説明します。

（注）　この章で使用す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 for Release 12.4*』の「Secure Shell Commands」を参照してください。

SSH の概要

SSH は、レイヤ 2 またはレイヤ 3 の装置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」（P.10-11）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」（P.10-36）を参照してください）

SSH に関する詳細については、『*Cisco IOS Security Configuration Guide for Release 12.4*』のパート 5「Other Security Features」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）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。詳細については、このリリースのリリース ノートを参照してください。

SSH を設定し、SSH の設定を表示する方法については、次の URL で『*Cisco IOS Security Configuration Guide for Release 12.4*』のパート 6「Other Security Features」を参照してください。

http://www.cisco.com/en/US/docs/ios/security/configuration/guide/12_4/sec_12_4_book.html

クライアント ARP キャッシングの設定

関連付けられたクライアント装置のアドレス解決プロトコル（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」（P.10-45）
- 「ARP キャッシングの設定」（P.10-45）

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 キャッシングをディセーブルにすると、ワイヤレス デバイスはすべての ARP 要求を関連付けられたクライアントに無線ポート経由で転送します。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

シスコ製以外のクライアント装置がアクセス ポイントに関連付けられ、その装置にデータを渡していない場合、ワイヤレス デバイスがクライアント 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 アドレスを持つクライアントに代わって応答しますが、不明なクライアント宛ての ARP 要求を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

関連付けら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 デバイスを設定するには、特権 EXEC モードで開始し、次のステップに従います。

手順の概要

1. **configure terminal**
2. **dot11 arp-cache** [**optional**]
3. **end**
4. **show running-config**
5. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	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 キャッシングをイネーブルにします。 （任意）ワイヤレス デバイスが IP アドレスを認識しているクライアント 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。
ステップ 4	**show running-config**	入力を確認します。
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。

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

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

ポイントツーマルチポイント ブリッジングにおける複数の VLAN とレート制限の設定

この機能は、ポイントツーマルチポイント ブリッジングを変更したもので、複数の VLAN で動作しながら、各 VLAN のトラフィック レートを制御できるように設定するものです。

（注） レート制限ポリシーは、非ルート ブリッジでのファスト イーサネット入力ポートにだけ適用できます。

通常、複数の VLAN をサポートしていると、別々の VLAN 上にある各リモート サイトで、ポイントツーマルチポイント ブリッジリンクを設定できます。この設定では、各サイトへのトラフィックを分離して制御することができます。レート制限機能により、リモート サイトがリンク帯域幅全体のうち指定された量を超える帯域幅が消費されないようになります。アップリンク トラフィックだけは、非ルート ブリッジのファスト イーサネット入力ポートを使用して管理できます。

クラスベースのポリシング機能を使用すると、レート制限を指定して、これを非ルート ブリッジのイーサネット インターフェイスの入力に適用できます。イーサネット インターフェイスの入力にレートを適用すると、すべての受信イーサネット パケットが設定したレートに適合します。