アクセス ポイント / ブリッジの管理

この章では、アクセス ポイント / ブリッジを管理する方法について説明します。この章の内容は、次のとおりです。

アクセス ポイント / ブリッジへの不正アクセスの防止

権限のないユーザがアクセス ポイント / ブリッジ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のアクセス ポイント / ブリッジ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からのアクセスは制限します。

アクセス ポイント / ブリッジ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。

- アクセス ポイント / ブリッジに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、各ユーザはアクセス ポイント / ブリッジにアクセスする前に認証されます。また、特定の特権レベル（読み取り専用または読み取り / 書き込み）をユーザ名とパスワードのそれぞれの組み合わせに指定できます。詳細は、「ユーザ名とパスワードの組み合わせの設定」の項（P. 5-6）を参照してください。

（注）　デフォルトのユーザ名は *Cisco*、デフォルトのパスワードは *Cisco* です。
ユーザ名とパスワードでは、大文字と小文字が区別されます。

- セキュリティ　サーバのデータベースに集中的に保存されたユーザ名とパスワードの組み合わせ。詳細は、「RADIUS によるアクセス ポイント / ブリッジへのアクセスの制御」の項（P. 5-9）を参照してください。

特権 EXEC コマンドへのアクセス防止

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

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

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

デフォルト パスワードと特権レベルの設定

表 5-1 は、デフォルト パスワードと特権レベルの設定を示しています。

表 5-1　デフォルト パスワードと特権レベル

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

静的イネーブル パスワードの設定または変更

イネーブル パスワードは、特権 EXEC モードへのアクセスを制御します。

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

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

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**enable password** *password*	特権 EXEC モードにアクセスするための新しいパスワードを定義するか、既存のパスワードを変更します。 デフォルトのパスワードは *Cisco* です。 *password* には 1 ～ 25 文字の英数字からなる文字列を指定します。文字列を数字で始めることはできず、大文字と小文字は区別されます。また、スペースを使用できますが、先頭のスペースは無視されます。パスワードに疑問符（?）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+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.** **Crtl+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+V キーを押す必要はありません。パスワード プロンプトで単純に abc?123 と入力します。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show running-config**	入力内容を確認します。
ステップ 5	**copy running-config startup-config**	（オプション）コンフィギュレーション ファイルに入力内容を保存します。 イネーブル パスワードは暗号化されず、アクセス ポイント / ブリッジのコンフィギュレーション ファイルで読み取ることができます。

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

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

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

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

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

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

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

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**enable password** [**level** *level*] {*password* | *encryption-type encrypted-password*}	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。これは非可逆的暗号化方式を使用して保存されます。 • （オプション）*level* の指定範囲は 0 ～ 15 です。レベル 1 は通常のユーザ EXEC モードの特権です。デフォルトのレベルは 15（特権 EXEC モードの特権）です。 • *password* には 1 ～ 25 文字の英数字からなる文字列を指定します。文字列を数字で始めることはできず、大文字と小文字は区別されます。また、スペースを使用できますが、先頭のスペースは無視されます。デフォルトでは、パスワードは定義されていません。 • （オプション）*encryption-type* には、タイプ 5（シスコ独自の暗号化アルゴリズム）だけが指定できます。暗号化タイプを指定する場合は、別のアクセス ポイント / ブリッジの設定からコピーした暗号化パスワードを指定する必要があります。 （注）　暗号化タイプを指定し、クリア テキスト パスワードを入力すると、特権 EXEC モードを再開できません。失われた暗号化パスワードはどのような方法でも復元できません。
ステップ 3	**service password-encryption**	（オプション）パスワードの定義時または設定の書き込み時にパスワードを暗号化します。 暗号化により、パスワードをコンフィギュレーション ファイルで読み取ることができなくなります。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**copy running-config startup-config**	（オプション）コンフィギュレーション ファイルに入力内容を保存します。

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

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

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

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

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

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

ユーザ名とパスワードの組み合わせの設定

ユーザ名とパスワードの組み合わせを設定できます。これは、アクセス ポイント / ブリッジに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、各ユーザがアクセス ポイント / ブリッジにアクセスする際の認証に使用されます。特権レベルを定義している場合、ユーザ名とパスワードのそれぞれの組み合わせに特定の特権レベル（関連する権利と特権を含む）を割り当てることができます。

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

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

	コマンド	目的
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	入力内容を確認します。
ステップ 6	**copy running-config startup-config**	（オプション）コンフィギュレーション ファイルに入力内容を保存します。

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

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

（注）　ユーザ名は 1 つ以上設定しなければなりません。また、login local をアクセス ポイント / ブリッジとの Telnet セッションを開くように設定する必要があります。ユーザ名が 1 つだけの場合にそのユーザ名を入力しないと、アクセス ポイント / ブリッジからロックアウトされることがあります。

複数の特権レベルの設定

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

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

この項では設定情報を扱います。

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

コマンドに対する特権レベルの設定

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

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**privilege** *mode* **level** *level command*	コマンドに特権レベルを設定します。 • *mode* には、グローバル コンフィギュレーション モードの場合は **configure** を、EXEC モードの場合は **exec** を、インターフェイス設定モードの場合は **interface** を、回線設定モードの場合は **line** を入力します。 • *level* の指定範囲は 0 ～ 15 です。レベル 1 は通常のユーザ EXEC モードの特権です。レベル 15 は**イネーブル** パスワードで許可されるアクセス レベルです。 • *command* にはアクセスを制限するコマンドを指定します。

	コマンド	目的
ステップ 3	**enable password level** *level password*	特権レベルにイネーブル パスワードを指定します。 • *level* の指定範囲は 0 ～ 15 です。レベル 1 は通常のユーザ EXEC モードの特権です。 • *password* には 1 ～ 25 文字の英数字からなる文字列を指定します。文字列を数字で始めることはできず、大文字と小文字は区別されます。また、スペースを使用できますが、先頭のスペースは無視されます。デフォルトでは、パスワードは定義されていません。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** または **show privilege**	入力内容を確認します。 最初のコマンドは、パスワードとアクセス レベルの設定を表示します。2 番目のコマンドは、特権レベルの設定を表示します。
ステップ 6	**copy running-config startup-config**	（オプション）コンフィギュレーション ファイルに入力内容を保存します。

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

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

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

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

特権レベルへのログインと終了

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

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

RADIUS によるアクセス ポイント / ブリッジへのアクセスの制御

この項では、Remote Authentication Dial-In User Service（RADIUS）を使用してアクセス ポイント / ブリッジ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アクセス ポイント / ブリッジを設定する手順の詳細は、第 12 章「RADIUS 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 Authentication, Authorization, and Accounting（AAA; 認証、認可、アカウンティング）を通じて効率化され、AAA コマンドでのみ有効に設定できます。

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

次の各項で RADIUS の設定について説明します。

デフォルトの RADIUS 設定

RADIUS と AAA は、デフォルトでは無効になっています。

セキュリティ上の危険を回避するため、ネットワーク管理アプリケーションから RADIUS を設定することはできません。RADIUS を有効にすると、Command-Line Interface（CLI; コマンドライン インターフェイス）を通じてアクセス ポイント / ブリッジにアクセスするユーザを認証できます。

RADIUS ログイン認証の設定

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

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

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

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**aaa new-model**	AAA を有効にします。
ステップ 3	**aaa authentication login** {**default** | *list-name*} *method1* [*method2...*]	ログイン認証方式リストを作成します。 • **login authentication** コマンドで名前付きリストの指定をしない場合に使用されるデフォルトのリストを作成する場合は、**default** キーワードの後に、デフォルトで使用する方式を指定します。デフォルトの方式リストは、自動的にすべてのインターフェイスに適用されます。 • *list-name* には、作成するリストに付ける名前の文字列を指定します。 • *method1...* には、認証アルゴリズムが試行する実際の方式を指定します。2 番目以降の認証方式が使用されるのは、その前の方式からエラーが返された場合に限られます。前の方式が失敗した場合ではありません。 次のいずれかの方式を選択します。 • **local**：認証にローカル　ユーザ名データベースを使用します。データベースにユーザ名情報を入力する必要があります。これには、グローバル設定コマンド **username** *password* を使用します。 • **radius**：RADIUS 認証を使用します。この認証方式を使用するには、事前に RADIUS サーバを設定しておく必要があります。詳細は、「RADIUS サーバ ホストの識別」の項（P. 12-5）を参照してください。
ステップ 4	**line** [**console** | **tty** | **vty**] *line-number* [*ending-line-number*]	回線設定モードを開始し、認証リストを適用する回線を設定します。
ステップ 5	**login authentication** {**default** | *list-name*}	認証リストを 1 つまたは複数の回線に適用します。 • **default** を指定すると、**aaa authentication login** コマンドで作成したデフォルトのリストが使用されます。 • *list-name* には、**aaa authentication login** コマンドで作成したリストを指定します。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show running-config**	入力内容を確認します。
ステップ 8	**copy running-config startup-config**	（オプション）コンフィギュレーション ファイルに入力内容を保存します。

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

AAA サーバ グループの定義

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

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

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

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

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**aaa new-model**	AAA を有効にします。
ステップ 3	**radius-server host** {*hostname* | *ip-address*} [**auth-port** *port-number*] [**acct-port** *port-number*] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*]	リモート RADIUS サーバ ホストの IP アドレスまたはホスト名を指定します。 • （オプション）**auth-port** *port-number* には、認証要求の UDP 宛先ポートを指定します。 • （オプション）**acct-port** *port-number* には、アカウンティング要求の UDP 宛先ポートを指定します。 • （オプション）**timeout** *seconds* には、アクセス ポイント / ブリッジが RADIUS サーバの返答を待ち、再送信するまでの時間を指定します。指定範囲は 1 ～ 1000 です。この設定はグローバル設定コマンド **radius-server timeout** の設定よりも優先されます。**radius-server host** コマンドでこのタイムアウトを設定しない場合は、**radius-server timeout** コマンドの設定が使用されます。 • （オプション）**retransmit** *retries* には、サーバが応答しない場合または応答が遅い場合に、RADIUS 要求をサーバに再送信する回数を指定します。範囲は 1 ～ 1000 です。**radius-server host** コマンドでこの再送回数を設定しない場合は、グローバル設定コマンド **radius-server retransmit** の設定が使用されます。 • （オプション）**key** *string* には、RADIUS サーバで動作するアクセス ポイント / ブリッジと RADIUS デーモンの間で使用される認証と暗号キーを指定します。

	コマンド	目的
		（注）　このキーはテキスト文字列で、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。キーは必ず **radius-server host** コマンドの最後に設定してください。先頭の空白は無視されますが、キー内およびキーの末尾の空白は有効です。キーに空白を使用する場合、引用符がキーの一部である場合を除き、キーを引用符で囲まないでください。 アクセス ポイント / ブリッジが単一の IP アドレスと関連付けられた複数のホスト エントリを認識するように設定するには、このコマンドを必要な数だけ入力します。その際、各 UDP ポート番号が異なっていることを確認してください。アクセス ポイント/ブリッジソフトウェアは、指定された順序でホストを検索します。個々の RADIUS ホストで使用するタイムアウト、再送信、暗号キーの値を設定します。
ステップ 4	**aaa group server radius** *group-name*	AAA サーバ グループをグループ名で定義します。 このコマンドを実行すると、アクセス ポイント / ブリッジはサーバ グループ設定モードへ移行します。
ステップ 5	**server** *ip-address*	特定の RADIUS サーバを定義されたサーバ グループにアソシエートします。この手順を、AAA サーバ グループの各 RADIUS サーバについて繰り返します。 グループ内の各サーバは、ステップ 2 であらかじめ定義されている必要があります。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show running-config**	入力内容を確認します。
ステップ 8	**copy running-config startup-config**	（オプション）コンフィギュレーション ファイルに入力内容を保存します。
ステップ 9		RADIUS ログイン認証を有効にします。「RADIUS ログイン認証の設定」の項（P. 5-9）を参照してください。

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

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

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

ユーザ特権アクセスとネットワーク サービスの RADIUS 許可の設定

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

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

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

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

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

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

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**aaa authorization network radius**	ネットワーク関連のすべてのサービス要求に対して、ユーザが RADIUS 許可を受けるようにアクセス ポイント / ブリッジを設定します。
ステップ 3	**aaa authorization exec radius**	ユーザの RADIUS 許可でユーザの特権 EXEC アクセス権の有無を判断するように、アクセス ポイント / ブリッジを設定します。 **exec** キーワードを指定すると、ユーザ プロファイル情報（**autocommand** 情報など）が返される場合があります。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	入力内容を確認します。
ステップ 6	**copy running-config startup-config**	（オプション）コンフィギュレーション ファイルに入力内容を保存します。

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

RADIUS 設定の表示

RADIUS 設定を表示するには、**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 / ブリッジへのアクセスの制御

この項では、Terminal Access Controller Access Control System Plus（TACACS+）を使用してアクセス ポイント / ブリッジ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アクセス ポイント / ブリッジを設定する手順の詳細は、第 12 章「RADIUS と TACACS+ サーバの設定」を参照してください。

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

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

次の項で TACACS+ の設定について説明します。

デフォルト TACACS+ 設定

TACACS+ と AAA は、デフォルトでは無効になっています。

セキュリティ上の危険を回避するため、ネットワーク管理アプリケーションから TACACS+ を設定することはできません。TACACS+ を有効にすると、CLI 経由でアクセス ポイント / ブリッジにアクセスする管理者を認証できます。

TACACS+ ログイン認証の設定

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

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

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

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**aaa new-model**	AAA を有効にします。
ステップ 3	**aaa authentication login** {**default** | *list-name*} *method1* [*method2...*]	ログイン認証方式リストを作成します。 • **login authentication** コマンドで名前付きリストの指定をしない場合に使用されるデフォルトのリストを作成する場合は、**default** キーワードの後に、デフォルトで使用する方式を指定します。デフォルトの方式リストは、自動的にすべてのインターフェイスに適用されます。 • *list-name* には、作成するリストに付ける名前の文字列を指定します。 • *method1...* には、認証アルゴリズムが試行する実際の方式を指定します。2 番目以降の認証方式が使用されるのは、その前の方式からエラーが返された場合に限られます。前の方式が失敗した場合ではありません。 次のいずれかの方式を選択します。 • **local**：認証にローカル ユーザ名データベースを使用します。データベースにユーザ名情報を入力する必要があります。これには、グローバル設定コマンド **username** *password* を使用します。 • **tacacs+**：TACACS+ 認証を使用します。この認証方式を使用するには、事前に TACACS+ サーバを設定しておく必要があります。
ステップ 4	**line** [**console** | **tty** | **vty**] *line-number* [*ending-line-number*]	回線設定モードを開始し、認証リストを適用する回線を設定します。
ステップ 5	**login authentication** {**default** | *list-name*}	認証リストを 1 つまたは複数の回線に適用します。 • **default** を指定すると、**aaa authentication login** コマンドで作成したデフォルトのリストが使用されます。 • *list-name* には、**aaa authentication login** コマンドで作成したリストを指定します。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show running-config**	入力内容を確認します。
ステップ 8	**copy running-config startup-config**	（オプション）コンフィギュレーション ファイルに入力内容を保存します。

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

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

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

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

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

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

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

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

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**aaa authorization network tacacs+**	ネットワーク関連のすべてのサービス要求に対して、ユーザが TACACS+ 許可を受けるようにアクセス ポイント / ブリッジを設定します。
ステップ 3	**aaa authorization exec tacacs+**	ユーザの TACACS+ 許可でユーザの特権 EXEC アクセス権の有無を判断するように、アクセス ポイント / ブリッジを設定します。 **exec** キーワードを指定すると、ユーザ プロファイル情報（**autocommand** 情報など）が返される場合があります。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	入力内容を確認します。
ステップ 6	**copy running-config startup-config**	（オプション）コンフィギュレーション ファイルに入力内容を保存します。

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

TACACS+ 設定の表示

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

イーサネット速度と二重設定の設定

アクセス ポイント/ブリッジ パワー インジェクタは、設定することができない組み込み 10/100baseT スイッチを含みます。スイッチのポートは、自動速度および自動二重、および自動 MDIX に設定されます。スイッチのポート 0 はブリッジへの同軸リンクに、スイッチのポート 1 はパワー インジェクタの RJ-45 ジャックに使用されます。他のスイッチ ポートは使用されません。

ブリッジ ファストイーサネット 0 インターフェイスの速度と二重設定は、パワー インジェクタ スイッチのブリッジ ポートとポート 0 の間のリンクにのみ適用されます。これらの設定は、パワー インジェクタの RJ-45 ポートに使用される速度やデュプレックスには依存しません。このため、最高のパフォーマンスを発揮するために、ブリッジ ファストイーサネットは常に自動速度および自動二重に設定する必要があります。この設定により、ブリッジとパワー インジェクタの間のリンクに 100 megabits per second（Mbps; メガビット / 秒）全二重が使用されます。

Fast Ethernet Settings ページには次の注意が記載されています。

注意　インライン パワーを使用中に「要求された二重」または「要求された速度」を修正しないでください。インライン パワーを使用中にこれらの設定を変更すると、デバイスがリブートする場合があります。詳細は、資料を参照してください。

イーサネット速度とデュプレックスを設定するための次のガイドラインを常に守る必要があります。

- パワー インジェクタの外部 LAN ポート（接続ポート）が接続されるデバイスの設定にかかわらず、内部ファストイーサネット 0 インターフェイスは、常に自動速度と自動二重に設定する必要があります。
- 接続ポートは常に次のいずれかに設定する必要があります。
  - 100Mbps、自動二重（推奨）
  - 100Mbps、半二重
  - 10Mbps、自動二重
  - 10Mbps、半二重

（注）　ポートを 10Mbps に設定すると、スループットが低下する可能性があります。

- 接続ポートは絶対に全二重に設定しないでください。

これらのガイドラインに従わないと、レイト コリジョン、Cycle Redundancy Check（CRC; 巡回冗長検査）エラーなどによりデータが失われます。

アクセス ポイント / ブリッジのローカル認証および許可の設定

ローカル モードで AAA を実装するようにアクセス ポイント / ブリッジを設定すると、サーバを使用せずに作動するように AAA を設定できます。アクセス ポイント / ブリッジは認証と許可を処理します。この設定ではアカウンティングは使用できません。

特権 EXEC モードからローカル AAA にアクセス ポイント / ブリッジを設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**aaa new-model**	AAA を有効にします。
ステップ 3	**aaa authentication login default local**	ローカル ユーザ名データベースを使用するログイン認証を設定します。**default** キーワードにより、ローカル ユーザ データベース認証がすべてのインターフェイスに適用されます。
ステップ 4	**aaa authorization exec local**	ローカル データベースをチェックして、ユーザが EXEC シェルの実行を許可されているかどうかを判断するようにユーザ AAA 許可を設定します。
ステップ 5	**aaa authorization network local**	ネットワーク関連のすべてのサービス要求に対してユーザ AAA 許可を設定します。
ステップ 6	**username** *name* [**privilege** *level*] {**password** *encryption-type password*}	ローカル データベースを入力し、ユーザ名ベースの認証システムを設定します。 このコマンドを各ユーザについて繰り返します。 • *name* には、ユーザ ID を 1 ワードで指定します。空白と引用符は使用できません。 • （オプション）*level* には、ユーザがアクセス後に取得する特権レベルを指定します。指定範囲は 0 ～ 15 です。レベル 15 は特権 EXEC モードのアクセスを許可します。レベル 0 はユーザ EXEC モードのアクセスを許可します。 • *encryption-type* には、後ろに暗号化されていないパスワードが続くことを指定する場合は **0** を入力します。非表示のパスワードが続くことを指定するには **7** を入力します。 • *password* には、アクセス ポイント / ブリッジにアクセスするためにユーザが入力しなければならないパスワードを指定します。パスワードは 1 ～ 25 文字の間で指定します。空白を入れることもできます。また、パスワードは必ず **username** コマンドの最後のオプションとして指定してください。
ステップ 7	**end**	特権 EXEC モードに戻ります。
ステップ 8	**show running-config**	入力内容を確認します。
ステップ 9	**copy running-config startup-config**	（オプション）コンフィギュレーション ファイルに入力内容を保存します。

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

Dynamic Host Configuration Protocol（DHCP）サービスを提供するためのアクセス ポイント / ブリッジの設定

次の項では、DHCP サーバとしてアクセス ポイント / ブリッジを設定する方法について説明します。

DHCP サーバの設定

デフォルトでは、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アクセス ポイントが設定されます。DHCP サーバとしてアクセス ポイントを設定し、有線と無線 LAN 上の両方のデバイスに IP 設定を割り当てることもできます。

アクセス ポイントとして設定した場合、デフォルト値に設定されると、アクセス ポイント / ブリッジはデフォルトでミニ DHCP サーバになり、DHCP サーバから IP 設定を受信することはできません。ミニ DHCP サーバとして、アクセス ポイント / ブリッジは 10.0.0.11 ～ 10.0.0.30 の 20 個までの IP アドレスをイーサネット ポートに接続された PC および SSID を使用しないか、SSID として *tsunami* を使用するように設定され、すべてのセキュリティ設定が無効にされた無線クライアント デバイスに提供します。静的な IP アドレスを アクセス ポイント / ブリッジに割り当てると、ミニ DHCP サーバ機能は自動的に無効になります。

DHCP 関連コマンドとオプションの詳細は、『Cisco IOS IP Configuration Guide, Release 12.3』の「Configuring DHCP」の章を参照してください。次の URL をクリックすると、「Configuring DHCP」の章を参照できます。

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

特権 EXEC モードからアクセス ポイントを設定し、DHCP サービスを提供する手順は、次のとおりです。

	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	**ip dhcp excluded-address** *low_address* [*high_address*]	アクセス ポイント / ブリッジの IP アドレスを無線デバイスが割り当てるアドレスの範囲から除外します。IP アドレスを 10.91.6.158 などのように 4 つのグループの文字で入力します。 アクセス ポイント / ブリッジは、DHCP アドレス プール サブネットのすべての IP アドレスが DHCP クライアントに割り当てるために使用可能であることを前提とします。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。 （オプション）除外されるアドレスの範囲を入力するには、範囲の下限値のアドレスを入力してから、範囲の上限値のアドレスを入力します。
ステップ 3	**ip dhcp pool** *pool_name*	DHCP 要求への応答として無線デバイスが割り当てる IP アドレスのプールの名前を作成し、DHCP コンフィギュレーション モードに移行します。

	コマンド	目的
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。アクセス ポイント/ブリッジはこのサブネット内で IP アドレスを割り当てます。 （オプション）アドレス プールにサブネット マスクを割り当てるか、アドレス 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、サブネット マスクを割り当てるための代替方法です。プレフィクス長さの前にスラッシュ（/）を付ける必要があります。
ステップ 5	**lease** { *days* [*hours*] [*minutes*] | **infinite** }	無線デバイスによって割り当てられた IP アドレスのリースの期間を設定します。 • 日：リース期間を日数で設定します。 • （オプション）時間：リース期間を時間単位で設定します。 • （オプション）分：リース期間を分単位で設定します。 • 無限：リース期間を無限に設定します。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show running-config**	入力内容を確認します。
ステップ 8	**copy running-config startup-config**	（オプション）コンフィギュレーション ファイルに入力内容を保存します。

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

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

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

DHCP サーバ アクセス ポイントのモニタリングおよび維持

次の項では、DHCP サーバ アクセス ポイントを監視し、維持するために使用できるコマンドについて説明します。

- 表示コマンド（P. 5-21）
- クリア コマンド（P. 5-21）
- デバッグ コマンド（P. 5-21）

表示コマンド

Exec モードで、表 5-2 に示すコマンドを入力し、DHCP サーバとしてアクセス ポイント / ブリッジに関する情報を表示します。

表 5-2　DHCP サーバ用の表示コマンド

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たすべてのアドレス競合のリストを表示します。アクセス ポイント / ブリッジの IP アドレスを入力し、アクセス ポイント / ブリッジによって記録された競合を表示します。
show ip dhcp database [*url*]	DHCP データベースの最新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 モードで使用します。
show ip dhcp server statistics	サーバ統計情報と送受信メッセージに関するカウント情報を表示します。

クリア コマンド

特権 EXEC モードで、表 5-3 に示すコマンドを使用して DHCP サーバ変数をクリアします。

表 5-3　DHCP サーバ用のクリア 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。アドレス引数を指定すると、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クリアされます。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クリアされます。
clear ip dhcp conflict { *address* | * }	DHCP データベースからアドレス競合をクリアします。アドレス引数を指定すると、特定の IP アドレスの競合がクリアされます。アスタリスク（*）を指定すると、すべてのアドレスの競合がクリアされます。
clear ip dhcp server statistics	すべての DHCP サーバ カウンタを 0 にリセットします。

デバッグ コマンド

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

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

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

アクセス ポイント / ブリッジの Secure Shell の設定

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

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

SSH の概要

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

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

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

SSH の詳細は、リリース 12.3 の『Cisco IOS Security Configuration Guide』の「Configuring Secure Shell」の項を参照してください。

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

SSH の設定

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

（注）　SSH の設定と SSH 設定の表示については、リリース 12.3 の『Cisco IOS Security Configuration Guide』の「Configuring Secure Shell」の項を参照してください。

クライアント アドレス レゾリューション プロトコル（ARP）キャッシングの設定

アクセス ポイント / ブリッジを設定し、関連クライアント デバイスの ARP キャッシュを維持することができます。アクセス ポイント / ブリッジで ARP キャッシュを維持すると、無線 LAN のトラフィック負荷が低減されます。ARP キャッシングはデフォルトで無効に設定されています。

この項で説明する内容は次のとおりです。

クライアント ARP キャッシングの概要

アクセス ポイント / ブリッジの ARP キャッシングは、無線デバイスにおけるクライアント デバイスの ARP 要求を停止することにより無線 LAN のトラフィックを低減します。クライアント デバイスに ARP 要求を転送するのではなく、アクセス ポイント / ブリッジは関連するクライアント デバイスの代わりに応答します。

ARP キャッシングを無効にすると、アクセス ポイント / ブリッジは無線ポートを介してすべての ARP 要求を関連クライアントに転送し、ARP 要求が誘導されるクライアントが応答します。ARP キャッシングを有効にすると、アクセス ポイント / ブリッジは関連クライアントに対する ARP 要求に応答し、クライアントに要求を転送しません。アクセス ポイント / ブリッジがキャッシュにない IP アドレスへの ARP 要求を受信した場合、その要求をドロップし、転送しません。そのビーコンで、アクセス ポイント / ブリッジには、バッテリ寿命を伸ばすためブロードキャスト メッセージを無視することができることをクライアント デバイスに警報する情報要素が含まれます。

オプションの ARP キャッシング

非シスコ クライアント デバイスがアクセス ポイントに関連付けられ、データを渡していない場合、アクセス ポイント / ブリッジはクライアントの IP アドレスを知らないことがあります。この状況が無線 LAN で頻繁に発生する場合、オプションの ARP キャッシングを有効にすることができます。ARP キャッシングがオプションである場合、アクセス ポイント / ブリッジは、アクセス ポイント / ブリッジに知られている IP アドレスを使用してクライアントの代わりに応答しますが、未知のクライアントへアドレス指定された ARP 要求を無線ポートから転送します。アクセス ポイント / ブリッジがすべての関連クライアントの IP アドレスを認識すると、関連クライアントに誘導されない ARP 要求をドロップします。

ARP キャッシングの設定

特権 EXEC モードからアクセス ポイント / ブリッジを設定し、関連するクライアントの ARP キャッシュを維持する手順は、次のとおりです。

	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	**dot11 arp-cache** [**optional**]	無線デバイスで ARP キャッシングを有効にします。 • （オプション）**オプション**のキーワードを使用して、IP アドレスがアクセス ポイント / ブリッジに知られているクライアント デバイスにのみ ARP キャッシングを有効にします。
ステップ 3	**end**	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 4	**show running-config**	入力内容を確認します。
ステップ 5	**copy running-config startup-config**	（オプション）コンフィギュレーション ファイルに入力内容を保存します。

この例は、アクセス ポイントに ARP キャッシングを設定する方法を示しています。

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

システムの日時の管理

アクセス ポイント / ブリッジのシステム時刻と日付は、Network Time Protocol（NTP; ネットワーク タイム プロトコル）を使用して自動的に管理することも、アクセス ポイント / ブリッジに時刻と日付を設定して手動で管理することもできます。

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

この項で説明する設定の内容は次のとおりです。

システム クロックの概要

時刻サービスの核になるのはシステム クロックです。このクロックはシステムの起動時に始動し、日付と時刻を常時監視します。

システム クロックは次の方法で設定できます。

- Network Time Protocol
- 手動設定

システム クロックは次のサービスに時刻を提供します。

- ユーザ **show** コマンド
- メッセージのロギングとデバッグ

システム クロックは、Greenwich Mean Time（GMT; グリニッジ標準時）として知られる、Coordinated Universal Time（UTC; 世界標準時）を基準にして内部的に時刻を決定します。ローカル タイム ゾーンの時刻が正しく表示されるように、ローカル タイム ゾーンとサマー タイム（夏時間）の情報を設定できます。

システム クロックは、時間が*信頼できる*か否か（つまり、信頼性のある時刻ソースから設定されたかどうか）を追跡します。信頼できない場合、時刻は表示のみに使用され、再配布はされません。設定情報については、「時刻と日付の手動設定」の項（P. 5-35）を参照してください。

Network Time Protocol の概要

NTP はデバイスのネットワークで時刻を同期させるためのプロトコルです。NTP は IP 上で動作する User Datagram Protocol（UDP; ユーザ データグラム プロトコル）上で実行されます。NTP は RFC 1305 で規定されています。

NTP ネットワークは通常、ラジオ クロックやタイム サーバに付属するアトミック クロックなどの信頼できる時刻ソースから時刻を取得します。NTP はこの時刻をネットワーク全体に配布します。NTP はきわめて効率的で、2 台のデバイスを 1 ミリ秒以内の誤差で同期するのに、毎分 1 パケットしか必要としません。

NTP は*ストラタム（層）*の概念を使って、デバイスが信頼できる時刻ソースからどれだけ離れているかを NTP ホップ数で示します。ストラタム 1 のタイム サーバにはラジオ クロックまたはアトミック クロックが直接接続されており、ストラタム 2 のタイム サーバは NTP を通じてストラタム 1 のタイム サーバから時刻を受信します。同様に、以降のストラタムも時刻を受信します。NTP を実行するデバイスは、NTP で通信するデバイスのうち最もストラタム番号の小さいものを、時刻ソースとして自動的に選択します。この方式により、NTP スピーカの自動編成型ツリーが効果的に構築されます。

NTP は同期化されていないデバイスとの同期化は決して行わず、時刻が正確でない可能性のあるデバイスとの同期を回避します。また、複数のデバイスから報告された時刻を比較し、ストラタムが低くても、他のデバイスと時刻が大きくずれているデバイスとの同期は行いません。

NTP を実行するデバイス間の通信は、*アソシエーション*と呼ばれ、通常は静的に設定されます。つまり、アソシエーションを形成するすべてのデバイスの IP アドレスが各デバイスに割り当てられます。2 台のデバイス間の NTP メッセージをアソシエーションと交換することで、正確な時刻が維持されます。ただし、LAN 環境では、NTP メッセージの代わりに IP ブロードキャスト メッセージを使用するように NTP を設定することができます。この方法では、単純にブロードキャスト メッセージを送受信するように各デバイスを設定できるため、設定が複雑になるのが抑えられます。ただし、その場合、情報の流れは一方向に限定されます。

デバイスで維持される時刻は重要なリソースです。NTP のセキュリティ機能を使用して、間違った時刻が誤って、または悪意を持って設定されるのを防ぐ必要があります。アクセス リスト ベースの制限方式と暗号化認証メカニズムの 2 種類のメカニズムを使用できます。

シスコの NTP の実装では、ストラタム 1 サービスをサポートしていません。したがって、ラジオ クロックまたはアトミック クロックには接続できません。ネットワークの時刻サービスは、IP インターネット上で利用できる一般の NTP サーバから取得することをお勧めします。図 5-1 は、NTP を使用した一般的なネットワークの例を示しています。

インターネットからネットワークが切り離されている場合、シスコの NTP 実装では、各デバイスが NTP を通じて同期されているかのように振る舞いますが、実際には他の方法で時間を判断しています。他のデバイスは NTP を通じてそのデバイスと同期をとります。

複数の時刻ソースが使用できる場合、常に NTP がより信頼性の高いソースと見なされます。NTP の時刻は他の方法で設定される時刻よりも優先されます。

一部のホスト システムには NTP ソフトウェアが組み込まれています。また、UNIX および UNIX 系を実行するシステムの場合は、一般に利用できる NTP ソフトウェアも入手できます。こうした NTP ソフトウェアを使って、ホスト システムの時刻を同期化することもできます。

図 5-1　一般的な NTP ネットワークの構成

NTP の設定

Cisco Aironet 1300 シリーズのアクセス ポイント / ブリッジはハードウェア クロックを持っていません。また、外部 NTP ソースが使用できないときにピアが同期をとるのに使用する NTP マスター クロックとしては機能しません。これらのアクセス ポイント / ブリッジは、カレンダーのハードウェアによるサポートもありません。このため、グローバル設定コマンド **ntp update-calendar** および **ntp master** は使用できません。

この項で説明する設定の内容は次のとおりです。

デフォルトの NTP 設定

表 5-4 は、デフォルトの NTP 設定を示しています。

表 5-4　デフォルトの NTP 設定

機能	デフォルト設定
NTP 認証	無効。認証キーが指定されていません。
NTP ピアまたはサーバ アソシエーション	設定されていません。
NTP ブロードキャスト サービス	無効。NTP ブロードキャスト パケットを送受信するインターフェイスはありません。
NTP アクセス制限	アクセス制限は指定されていません。
NTP パケットの送信元 IP アドレス	送信元アドレスは発信側インターフェイスで判断されます。

デフォルトでは、NTP は無効に設定されています。

NTP 認証の設定

この手順は NTP サーバの管理者と調整する必要があります。この手順で設定する情報は、アクセス ポイント / ブリッジが NTP サーバと時刻を同期するために使うサーバと照合されていなければなりません。

特権 EXEC モードから、次の手順に従って、セキュリティのために他のデバイスとのアソシエーション（NTP を実行するデバイス間の、正確な時間維持のための通信）を認証します。

	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	**ntp authenticate**	NTP 認証機能を有効にします。デフォルトでは無効に設定されています。
ステップ 3	**ntp authentication-key** *number* **md5** *value*	認証キーを定義します。デフォルトでは定義されていません。 • *number* には、キー番号を指定します。範囲は 1 ～ 4294967295 です。 • **md5** を指定すると、Message Digest 5（MD5）を使用したメッセージ認証がサポートされます。 • *value* には、キーに使用する 8 文字までの任意の文字列を入力します。 ブリッジとデバイスの双方がこれらの認証キーのいずれかを保有していなければ、アクセス ポイント / ブリッジはデバイスと同期をとりません。キー番号は **ntp trusted-key** *key-number* コマンドで指定します。

	コマンド	目的
ステップ 4	**ntp trusted-key** *key-number*	アクセス ポイント / ブリッジが同期をとるためにピア NTP デバイスが NTP パケットで指定しなければならないキー番号（ステップ 3 で定義したキー番号）を 1 つまたは複数指定します。 デフォルトでは、信頼するキーは定義されていません。 *key-number* には、ステップ 3 で定義したキーを指定します。 このコマンドは、誤ってアクセス ポイント / ブリッジが信頼できないデバイスに同期されるのを防ぎます。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show running-config**	入力内容を確認します。
ステップ 7	**copy running-config startup-config**	（オプション）コンフィギュレーション ファイルに入力内容を保存します。

NTP 認証を無効にするには、グローバル設定コマンド **no ntp authenticate** を使用します。認証キーを削除するには、グローバル設定コマンド **no ntp authentication-key** *number* を使用します。デバイスの ID の認証を無効にするには、グローバル設定コマンド **no ntp trusted-key** *key-number* を使用します。

次の例は、NTP パケットで認証キー 42 を提供するデバイスのみと同期をとるようにアクセス ポイント / ブリッジを設定する手順を示しています。

```
ap(config)# ntp authenticate
ap(config)# ntp authentication-key 42 md5 aNiceKey
ap(config)# ntp trusted-key 42
```

NTP アソシエーションの設定

NTP アソシエーションには、ピア アソシエーション（アクセス ポイント / ブリッジを他のデバイスに同期させることも、他のデバイスをブリッジに同期させることも可能）またはサーバ アソシエーション（アクセス ポイント / ブリッジを他のデバイスに同期させることのみが可能、その逆は不可）のいずれかを指定できます。

特権 EXEC モードから、次の手順に従って他のデバイスと NTP アソシエーションを形成します。

	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	**ntp peer** *ip-address* [**version** *number*] [**key** *keyid*] [**source** *interface*] [**prefer**] または **ntp server** *ip-address* [**version** *number*] [**key** *keyid*] [**source** *interface*] [**prefer**]	ブリッジがピアに同期するか、ピアがブリッジに同期するように、アクセス ポイント / ブリッジのシステム クロックを設定します（ピア アソシエーション）。 または アクセス ポイント / ブリッジのシステム クロックをタイム サーバに同期するように設定します（サーバ アソシエーション）。 デフォルトではピア アソシエーションもサーバ アソシエーションも定義されていません。 • *ip-address* には、ピア アソシエーションの場合はクロック同期をとるピアの IP アドレスを指定します。サーバ アソシエーションの場合は、クロック同期をとるタイム サーバの IP アドレスを指定します。 • （オプション）*number* には NTP バージョン番号を指定します。指定範囲は 1 ～ 3 です。デフォルトではバージョン 3 が選択されています。 • （オプション）*keyid* には、グローバル設定コマンド **ntp authentication-key** で定義した認証キーを入力します。 • （オプション）*interface* には、送信元 IP アドレスを取得するインターフェイスを指定します。デフォルトでは、送信元 IP アドレスは発信側インターフェイスから取得されます。 • （オプション）このピアまたはサーバを優先的に同期をとるピアまたはサーバとして指定する場合は、**prefer** キーワードを入力します。このキーワードを指定すると、ピア間またはサーバ間の切り替えが減少します。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show running-config**	入力内容を確認します。
ステップ 5	**copy running-config startup-config**	（オプション）コンフィギュレーション ファイルに入力内容を保存します。

アソシエーションは一方のデバイスのみ設定してください。もう一方のデバイスは自動的にアソシエーションを確立します。デフォルトの NTP バージョン（バージョン 3）を使用していて NTP 同期が実行されない場合は、NTP バージョン 2 を使用してみてください。インターネット上の多くの NTP サーバはバージョン 2 を実行しています。

ピア アソシエーションまたはサーバ アソシエーションを削除するには、グローバル設定コマンド **no ntp peer** *ip-address* または **no ntp server** *ip-address* を使用します。

次の例は、NTP バージョン 2 を使用して、IP アドレス 172.16.22.44 のピアのクロックにシステム クロックが同期するように、アクセス ポイント / ブリッジを設定する方法を示しています。

```
ap(config)# ntp server 172.16.22.44 version 2
```

NTP ブロードキャスト サービスの設定

NTP を実行するデバイス間の通信は、*アソシエーション*と呼ばれ、通常は静的に設定されます。つまり、アソシエーションを形成するすべてのデバイスの IP アドレスが各デバイスに割り当てられます。2 台のデバイス間の NTP メッセージをアソシエーションと交換することで、正確な時刻が維持されます。ただし、LAN 環境では、NTP メッセージの代わりに IP ブロードキャスト メッセージを使用するように NTP を設定することができます。この方法では、単純にブロードキャスト メッセージを送受信するように各デバイスを設定できるため、設定が複雑になるのが抑えられます。ただし、その場合、情報の流れは一方向に限定されます。

時刻情報をネットワーク上にブロードキャストするルータのような NTP ブロードキャスト サーバが存在する場合、アクセス ポイント / ブリッジはインターフェイス単位で NTP ブロードキャスト パケットを送受信します。アクセス ポイント / ブリッジは、ピアに NTP ブロードキャスト パケットを送信して、ピアがそのパケットと同期をとれるようにできます。また、アクセス ポイント / ブリッジは、NTP ブロードキャスト パケットを受信して内蔵クロックを同期することもできます。この項では、NTP ブロードキャスト パケットを送信および受信する手順について説明します。

特権 EXEC モードから、次の手順に従って、NTP ブロードキャスト パケットをピアに送信するようにアクセス ポイント / ブリッジを設定します。これにより、ピアはアクセス ポイント / ブリッジとクロックの同期をとることができます。

	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** *interface-id*	インターフェイス設定モードを開始し、NTP ブロードキャスト パケットを送信するインターフェイスを指定します。
ステップ 3	**ntp broadcast** [**version** *number*] [**key** *keyid*] [*destination-address*]	インターフェイスが NTP ブロードキャスト パケットをピアに送信できるようにします。 デフォルトでは、この機能はすべてのインターフェイスで無効になっています。 • （オプション）*number* には NTP バージョン番号を指定します。指定範囲は 1 ～ 3 です。バージョンの指定を省略すると、バージョン 3 が使用されます。 • （オプション）*keyid* には、ピアにパケットを送信するときに使用する認証キーを指定します。 • （オプション）*destination-address* には、クロックをこのアクセス ポイント / ブリッジに同期しているピアの IP アドレスを指定します。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	入力内容を確認します。
ステップ 6	**copy running-config startup-config**	（オプション）コンフィギュレーション ファイルに入力内容を保存します。
ステップ 7		次の手順で説明するように、接続されたピアが NTP ブロードキャスト パケットを受信するように設定します。

インターフェイスの NTP ブロードキャスト パケットの送信を無効にするには、インターフェイス設定コマンド **no ntp broadcast** を使用します。

次の例では、NTP バージョン 2 パケットを送信するインターフェイスの設定手順を示します。

```
ap(config)# interface gigabitethernet0/1
ap(config-if)# ntp broadcast version 2
```

特権 EXEC モードから、接続されたピアから NTP ブロードキャスト パケットを受信するようにアクセス ポイント / ブリッジを設定する手順は、次のとおりです。

	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	**interface** *interface-id*	インターフェイス設定モードを開始し、NTP ブロードキャスト パケットを受信するインターフェイスを指定します。
ステップ 3	**ntp broadcast client**	インターフェイスが NTP ブロードキャスト パケットを受信できるようにします。 デフォルトでは、どのインターフェイスも NTP ブロードキャスト パケットを受信しません。
ステップ 4	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 5	**ntp broadcastdelay** *microseconds*	（オプション）アクセス ポイント / ブリッジと NTP ブロードキャスト サーバ間の推定されるラウンドトリップ遅延を変更します。 デフォルト値は 3000 マイクロ秒です。指定範囲は 1 ～ 999999 です。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show running-config**	入力内容を確認します。
ステップ 8	**copy running-config startup-config**	（オプション）コンフィギュレーション ファイルに入力内容を保存します。

インターフェイスの NTP ブロードキャスト パケットの受信を無効にするには、インターフェイス設定コマンド **no ntp broadcast client** を使用します。推定されるラウンドトリップ遅延をデフォルト値に戻すには、グローバル設定コマンド **no ntp broadcastdelay** を使用します。

次の例では、NTP バージョン 2 パケットを受信するインターフェイスの設定手順を示します。

```
ap(config)# interface gigabitethernet0/1
ap(config-if)# ntp broadcast client
```

NTP アクセス制限の設定

NTP アクセスは次の項で説明するように、2 つのレベルで制御できます。

- アクセス グループの作成と基本的な IP アクセス リストの指定（P. 5-32）
- 特定のインターフェイスでの NTP サービスの無効化（P. 5-34）

アクセス グループの作成と基本的な IP アクセス リストの指定

特権 EXEC モードから NTP サービスへのアクセスをアクセス リストで制御する手順は、次のとおりです。

	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	**ntp access-group** {**query-only** | **serve-only** | **serve** | **peer**} *access-list-number*	アクセス グループを作成し、基本的な IP アクセス リストを適用します。 キーワードには、それぞれ次のような意味があります。 • **query-only**：NTP 制御クエリのみを許可します。 • **serve-only**：時間要求のみを許可します。 • **serve**：時間要求と NTP 制御クエリを許可しますが、アクセス ポイント / ブリッジのリモート デバイスとの同期を許可しません。 • **peer**：時間要求と NTP 制御クエリを許可し、アクセス ポイント / ブリッジのリモート デバイスとの同期も許可します。 *access-list-number* には、1 ～ 99 までの標準的な IP アクセス リスト番号を指定します。
ステップ 3	**access-list** *access-list-number* **permit** *source* [*source-wildcard*]	アクセス リストを作成します。 • *access-list-number* には、ステップ 2 で指定した番号を入力します。 • 条件が一致すればアクセスを許可する場合は、**permit** キーワードを入力します。 • *source* には、アクセス ポイント / ブリッジへのアクセスを許可するデバイスの IP アドレスを入力します。 • （オプション）*source-wildcard* には、ソースに適用されるワイルドカード ビットを入力します。 （注） アクセス リストを作成する場合は、デフォルトで、すべてのパケットに対する暗黙拒否ステートメントがアクセス リストの末尾に組み込まれていることに注意してください。アクセス リストの最後まで一致するアドレスが見つからないと、この拒否ステートメントが適用されます。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	入力内容を確認します。
ステップ 6	**copy running-config startup-config**	（オプション）コンフィギュレーション ファイルに入力内容を保存します。

アクセス グループのキーワードは、次のように制限が弱いものから強いものの順にスキャンされます。

1. **peer**：時間要求と NTP 制御クエリを許可し、アドレスがアクセス リストの基準を満たすデバイスとの同期をアクセス ポイント / ブリッジに許可します。
2. **serve**：時間要求と NTP 制御クエリを許可しますが、アドレスがアクセス リストの基準を満たすデバイスとの同期はアクセス ポイント / ブリッジに許可しません。
3. **serve-only**：アドレスがアクセス リストの基準を満たすデバイスからの時間要求のみ受け付けます。
4. **query-only**：アドレスがアクセス リストの基準を満たすデバイスからの NTP 制御クエリのみ受け付けます。

送信元 IP アドレスがアクセス リストの複数のアクセス タイプに一致する場合は、最初のタイプが許可されます。アクセス グループが指定されていない場合は、すべてのデバイスにすべてのアクセス タイプが許可されます。また、アクセス グループが指定されている場合は、指定されたアクセス タイプだけが許可されます。

アクセス ポイント / ブリッジの NTP サービスに対するアクセス制御を削除するには、グローバル設定コマンド **no ntp access-group** {**query-only** | **serve-only** | **serve** | **peer**} を使用します。

次の例は、アクセス リスト 99 のピアとの同期を許可するようにアクセス ポイント / ブリッジを設定する手順を示しています。ただし、このアクセス ポイント / ブリッジはアクセス リスト 42 の時間要求のみを受け付けるようにアクセスを制限します。

```
ap# configure terminal
ap(config)# ntp access-group peer 99
ap(config)# ntp access-group serve-only 42
ap(config)# access-list 99 permit 172.20.130.5
ap(config)# access list 42 permit 172.20.130.6
```

特定のインターフェイスでの NTP サービスの無効化

デフォルトでは、NTP サービスはすべてのインターフェイスで有効になっています。

特権 EXEC モードから、次の手順に従ってインターフェイスでの NTP パケットの受信を無効にします。

	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	**interface** *interface-id*	インターフェイス設定モードを開始し、無効にするインターフェイスを指定します。
ステップ 3	**ntp disable**	インターフェイスでの NTP パケットの受信を無効にします。 デフォルトでは、すべてのインターフェイスで NTP パケットが受信されます。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	入力内容を確認します。
ステップ 6	**copy running-config startup-config**	（オプション）コンフィギュレーション ファイルに入力内容を保存します。

インターフェイスで NTP パケットの受信を再び有効にするには、インターフェイス設定コマンド **no ntp disable** を使用します。

NTP パケットの送信元 IP アドレスの設定

アクセス ポイント / ブリッジが NTP パケットを送信する場合、通常、送信元 IP アドレスは NTP パケットを送信するインターフェイスのアドレスに設定されます。すべての NTP パケットに特定の送信元 IP アドレスを使用する場合は、グローバル設定コマンド **ntp source** を使用します。これにより、指定したインターフェイスのアドレスが使用されます。このコマンドは、あるインターフェイス上のアドレスを応答パケットの宛先として使用できない場合に便利です。

特権 EXEC モードから、次の手順に従って、送信元 IP アドレスとして使用する特定のインターフェイスを設定します。

	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	**ntp source** *type number*	送信元 IP アドレスとして使用するインターフェイスのタイプと番号を指定します。 デフォルトでは、送信元アドレスは発信側インターフェイスで判断されます。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show running-config**	入力内容を確認します。
ステップ 5	**copy running-config startup-config**	（オプション）コンフィギュレーション ファイルに入力内容を保存します。

指定したインターフェイスは、すべての宛先に送信されるすべてのパケットの送信元アドレスとして使用されます。送信元アドレスを特定のアソシエーションに使用する場合は、「NTP アソシエーションの設定」の項（P. 5-29）で説明するように、グローバル設定コマンド **ntp peer** または **ntp server** で **source** キーワードを指定します。

NTP 設定の表示

次の 2 つの特権 EXEC コマンドを使って NTP 情報を表示できます。

- **show ntp associations** [**detail**]
- **show ntp status**

これらのコマンドで表示されるフィールドについては、リリース 12.3 の『Cisco IOS Configuration Fundamentals Command Reference』を参照してください。

時刻と日付の手動設定

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

この項で説明する設定の内容は次のとおりです。

システム クロックの設定

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

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

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

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

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

時刻と日付の設定の表示

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

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

show clock の前に表示される記号には次のような意味があります。

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

タイム ゾーンの設定

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

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**clock timezone** *zone hours-offset* [*minutes-offset*]	タイム ゾーンを設定します。 アクセス ポイント / ブリッジは内部時間を Universal Time Coordinated（UTC; 協定世界時）で維持するため、このコマンドは表示専用で、時刻を手動で設定するときにのみ使用されます。 • *zone* には、標準時間が有効な場合に表示されるタイム ゾーンの名前を入力します。デフォルトは UTC です。 • *hours-offset* には、UTC との時差を時間単位で入力します。 • （オプション）*minutes-offset* には、UTC との時差を分単位で入力します。
ステップ 3	**end**	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 4	**show running-config**	入力内容を確認します。
ステップ 5	**copy running-config startup-config**	（オプション）コンフィギュレーション ファイルに入力内容を保存します。

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

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

サマー タイム（夏時間）の設定

特権 EXEC モードから、次の手順に従って、毎年、特定の日付（曜日）に開始および終了するサマータイム（夏時間）を設定します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**clock summer-time** *zone* **recurring** [*week day month hh*:*mm week day month hh*:*mm* [*offset*]]	毎年指定された日付に開始および終了するサマー タイムを設定します。 サマー タイムはデフォルトでは無効になっています。パラメータを指定しないで **clock summer-time** *zone* **recurring** を指定した場合、サマー タイムのルールは米国のルールをデフォルトとします。 • *zone* には、サマー タイムが有効なときに表示されるタイム ゾーンの名前（PDT など）を指定します。 • （オプション）*week* には、月の第何週かを指定します（1 ～ 5 または **last**）。 • （オプション）*day* には、曜日を指定します（Sunday、Monday など）。 • （オプション）*month* には、月を名前で指定します（January、February など）。 • （オプション）*hh*:*mm* には、時刻（24 時間形式）を時間と分の単位で指定します。 • （オプション）*offset* には、サマー タイム期間中に追加する時間を分単位で指定します。デフォルトは 60 分です。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show running-config**	入力内容を確認します。
ステップ 5	**copy running-config startup-config**	（オプション）コンフィギュレーション ファイルに入力内容を保存します。

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

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

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

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

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**clock summer-time** *zone* **date** [*month date year hh*:*mm month date year hh*:*mm* [*offset*]] または **clock summer-time** *zone* **date** [*date month year hh*:*mm date month year hh*:*mm* [*offset*]]	最初の日付に開始し、2 番目の日付に終了するサマー タイムを設定します。 サマー タイムはデフォルトでは無効になっています。 • *zone* には、サマー タイムが有効なときに表示されるタイム ゾーンの名前（PDT など）を指定します。 • （オプション）*week* には、月の第何週かを指定します（1 ～ 5 または **last**）。 • （オプション）*day* には、曜日を指定します（Sunday、Monday など）。 • （オプション）*month* には、月を名前で指定します（January、February など）。 • （オプション）*hh*:*mm* には、時刻（24 時間形式）を時間と分の単位で指定します。 • （オプション）*offset* には、サマー タイム期間中に追加する時間を分単位で指定します。デフォルトは 60 分です。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show running-config**	入力内容を確認します。
ステップ 5	**copy running-config startup-config**	（オプション）コンフィギュレーション ファイルに入力内容を保存します。

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

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

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

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

システム名とプロンプトの設定

アクセス ポイント / ブリッジ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 *bridge* です。

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

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

この項で説明する設定の内容は次のとおりです。

デフォルトのシステム名とプロンプトの設定

アクセス ポイント / ブリッジのデフォルトのシステム名とプロンプトは *bridge* です。

システム名の設定

特権 EXEC モードから、次の手順に従ってシステム名を手動で設定します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**hostname** *name*	システム名を手動で設定します。 デフォルト設定は *bridge* です。 この名前は Advanced Research Projects Agency Network（ARPANET）ホスト名の規則に従っていなければなりません。すなわち、先頭は英字で、最後は英字または数字で終わります。その間の文字には英字、数字、ハイフンが使用できます。長さは 63 文字以内です。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show running-config**	入力内容を確認します。
ステップ 5	**copy running-config startup-config**	（オプション）コンフィギュレーション ファイルに入力内容を保存します。

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

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

DNS の概要

DNS プロトコルは Domain Name System（DNS; ドメイン ネーム システム）を制御します。これはホスト名を IP アドレスにマッピングする際に使用する分散型データベースです。アクセス ポイント / ブリッジに 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 は階層命名方式を定義します。この方式では場所またはドメインでデバイスを特定することができます。ドメイン名はピリオド（.）を区切り文字として連結できます。たとえば、シスコ システムズは IP ではドメイン名 *com* で特定される民間組織です。このためドメイン名は cisco.com になります。このドメイン内の File Transfer Protocol（FTP; ファイル転送プロトコル）システムなどの個々のデバイスは *ftp.cisco.com* のように識別されます。

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

この項で説明する設定の内容は次のとおりです。

デフォルトの DNS 設定

表 5-5 にデフォルトの DNS 設定を示します。

表 5-5　デフォルトの DNS 設定

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

DNS の設定

特権 EXEC モードから DNS を使用するようにアクセス ポイント / ブリッジを設定する手順は、次のとおりです。

	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	**ip domain-name** *name*	ソフトウェアが未修飾ホスト名（ドット付き 10 進ドメイン名を含まない名前）を作成する場合に使用するデフォルトのドメイン名を定義します。 未修飾名をドメイン名と区切るピリオドを先頭に使用しないでください。 ブート時にはドメイン名は設定されていませんが、アクセス ポイント / ブリッジの設定が Bootstrap Protocol（BOOTP; ブートストラップ プロトコル）または Dynamic Host Configuration Protocol（DHCP）サーバから行われている場合、BOOTP または DHCP サーバによってデフォルトのドメイン名が設定されることがあります（この情報がサーバに設定されている場合）。
ステップ 3	**ip name-server** *server-address1* [*server-address2 ... server-address6*]	名前とアドレスの解決に使用する 1 つまたは複数のネーム サーバのアドレスを指定します。 最大 6 つのネーム サーバを指定できます。各サーバのアドレスは空白で区切ります。最初に指定するサーバがプライマリ サーバになります。アクセス ポイント / ブリッジは最初にプライマリ サーバに DNS クエリを送信します。そのクエリが失敗した場合、バックアップ サーバが照会されます。
ステップ 4	**ip domain-lookup**	（オプション）アクセス ポイント / ブリッジで DNS ベースのホスト名からアドレスへの変換を有効にします。この機能はデフォルトで有効に設定されています。 ネットワークのデバイスが名前の割り当てを制御できないネットワークのデバイスとの接続を要求する場合、グローバル インターネット命名方式（DNS）を使用して、デバイスを一意に識別するデバイス名を動的に割り当てることができます。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show running-config**	入力内容を確認します。
ステップ 7	**copy running-config startup-config**	（オプション）コンフィギュレーション ファイルに入力内容を保存します。

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

ドメイン名を削除するには、グローバル設定コマンド **no ip domain-name** *name* を使用します。ネーム サーバ アドレスを削除するには、グローバル設定コマンド **no ip name-server** *server-address* を使用します。アクセス ポイント / ブリッジで DNS を無効にする場合は、グローバル設定コマンド **no ip domain-lookup** を使用します。

DNS 設定の表示

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

バナーの作成

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

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

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

この項で説明する設定の内容は次のとおりです。

- デフォルトのバナー設定（P. 5-42）
- Message-of-the-Day ログイン バナーの設定（P. 5-42）
- ログイン バナーの設定（P. 5-43）

デフォルトのバナー設定

デフォルトでは、MOTD バナーとログイン バナーは設定されていません。

Message-of-the-Day ログイン バナーの設定

アクセス ポイント / ブリッジにログインしたときに画面に表示される 1 行または複数行のメッセージ バナーを作成できます。

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

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**banner motd** *c message c*	message-of-the-day（今日のメッセージ）を指定します。 *c* にはシャープ記号（#）など希望する区切り文字を入力し、**Return** キーを押します。区切り文字は、バナー テキストの開始と終了を指定します。終了区切り文字より後の文字は破棄されます。 *message* には、最大 255 文字のバナー メッセージを入力します。メッセージ内で区切り文字は使用できません。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show running-config**	入力内容を確認します。
ステップ 5	**copy running-config startup-config**	（オプション）コンフィギュレーション ファイルに入力内容を保存します。

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

次の例は、開始および終了区切り文字にシャープ記号（#）を使用して、アクセス ポイント / ブリッジに MOTD バナーを設定する方法を示しています。

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

次の例は、上記の設定で表示されるバナーを示しています。

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

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

User Access Verification

Password:
```

ログイン バナーの設定

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

特権 EXEC モードから、次の手順に従ってログイン バナーを設定します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**banner login** *c message c*	ログイン メッセージを指定します。 *c* にはシャープ記号（#）など希望する区切り文字を入力し、**Return** キーを押します。区切り文字は、バナー テキストの開始と終了を指定します。終了区切り文字より後の文字は破棄されます。 *message* には、最大 255 文字のログイン メッセージを入力します。メッセージ内で区切り文字は使用できません。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show running-config**	入力内容を確認します。
ステップ 5	**copy running-config startup-config**	（オプション）コンフィギュレーション ファイルに入力内容を保存します。

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

次の例は、開始および終了区切り文字にドル記号（$）を使用して、アクセス ポイント / ブリッジにログイン バナーを設定する方法を示しています。

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