CHAPTER 4

ワイヤレス デバイスの基本設定

この章では、Cisco 880 Series Integrated Services Router（ISR; サービス統合型ルータ）での自律ワイヤレス デバイスの設定方法について説明します。

（注） 自律ソフトウェアを組み込みワイヤレス デバイス上で Cisco Unified ソフトウェアにアップグレードするには、「Cisco Unified ソフトウェアへのアップグレード」（P.4-9）で手順を参照してください。

ワイヤレス デバイスは組み込み型で、接続用の外部コンソール ポートはありません。ワイヤレス デバイスを設定するには、コンソール ケーブルでパーソナル コンピュータをホスト ルータのコンソール ポートに接続して次の手順に従って接続を確立し、ワイヤレス設定を行います。

無線コンフィギュレーション セッションの開始

（注） ルータのセットアップでワイヤレス デバイスを設定する*前*に、後述の手順に従ってルータとアクセス ポイントとの間でセッションを開く必要があります。

以下のコマンドを、グローバル コンフィギュレーション モードでルータの Cisco IOS CLI 上に入力します。

手順の概要

1. **interface wlan-ap0**
2. **ip address *subnet mask***
3. **no shutdown**
4. **interface vlan1**
5. **ip address *subnet mask***
6. **exit**
7. **exit**
8. **service-module wlan-ap 0 session**

手順の詳細

	コマンド	目的

ステップ 1	**interface wlan-ap0**
	
	例：
	`router(config)# interface wlan-ap0`
	`router(config-if)#`
		ワイヤレス デバイスへの、ルータのコンソール インターフェイスを定義します。このインターフェイスは、ルータのコンソールとワイヤレス デバイス間の通信に使用します。
		常にポート 0 を使用します。
		次のメッセージが表示されます。
		
		`The wlan-ap 0 interface is used for managing the embedded AP. Please use the` **`service-module wlan-ap 0 session`** `command to console into the embedded AP.`

ステップ 2	**ip address *subnet mask***
	
	例：
	`router(config-if)# ip address 10.21.0.20 255.255.255.0`
	
	`or`
	`router(config-if)# ip unnumbered vlan1`
		インターフェイス IP アドレスとサブネット マスクを指定します。
		（注） この IP アドレスは、**ip unnumbered vlan1** コマンドを使用することで、Cisco ISR に割り当てられた IP アドレスと共有できます。

ステップ 3	**no shutdown** **例：** `router(config-if)# no shutdown`	内部インターフェイス接続を開いた状態を維持するように指定します。

	コマンド	目的
ステップ 4	**interface vlan1** **例：** `router(config-if)# interface vlan1`	データ通信のために、内部 Gigabit Ethernet（GE0; ギガビット イーサネット）0 ポート上で仮想 LAN インターフェイスを別のインターフェイスに指定します。 • Cisco 880 シリーズの ISR では、すべてのスイッチ ポートがデフォルトの vlan1 インターフェイスを継承します。
ステップ 5	**ip address** ***subnet mask*** **例：** `router(config-if)# ip address 10.10.0.30 255.255.255.0`	インターフェイス IP アドレスとサブネット マスクを指定します。

ステップ 6	**exit**
	
	例：
	`router(config-if)# exit`
	`router(config)#`
		インターフェイス コンフィギュレーション モードを終了します。

ステップ 7	**exit**
	
	例：
	`router(config)# exit`
	`router#`
		グローバル コンフィギュレーション モードを終了します。

ステップ 8	**service-module wlan-ap 0 session**
	
	例：
	`router# service-module wlan-ap0 session`
	`Trying 10.21.0.20, 2002 ... Open`
	
	`ap>`
		ワイヤレス デバイスとルータのコンソール間の接続をオープンにします。

ヒント　ワイヤレス デバイスとのセッションを開始するコンソールに Cisco IOS ソフトウェア エイリアスを作成する場合は、EXEC プロンプトから **alias exec dot11radio service-module wlan-ap 0 session** コマンドを入力します。

セッションの終了

ワイヤレス デバイスとルータのコンソールとの間のセッションを閉じるには、次の手順に従います。

ワイヤレス デバイス

1. **Ctrl+Shift+6**、**x**

ルータ

1. **disconnect** コマンドを入力します。
2. Enter を押します。

無線環境の設定

（注） ワイヤレス デバイスを初めて設定する場合は、基本のワイヤレス設定の前に、アクセス ポイントとルータとの間でコンフィギュレーション セッションを開始する必要があります。「無線コンフィギュレーション セッションの開始」（P.4-2）を参照してください。

ワイヤレス デバイスのソフトウェアに適合するツールを使用してデバイスを設定します。

- 「Cisco Express 設定」（P.4-4）：ユニファイド ソフトウェア
- 「Cisco IOS コマンドライン インターフェイス」（P.4-5）：自律ソフトウェア

（注） 自律モードでワイヤレス デバイスを実行していて Unified モードにアップグレードするには、「Cisco Unified ソフトウェアへのアップグレード」（P.4-9）でアップグレードの手順を参照してください。

Cisco Unified Wireless ソフトウェアへのアップグレード後、次の URL で Web ブラウザ インターフェイスを使用してデバイスを設定します。
http://cisco.com/en/US/docs/wireless/access_point/12.4_10b_JA/configuration/guide/scg12410b-chap2-gui.html

Cisco Express 設定

自律ワイヤレス デバイスを設定するには、次の手順に示すように、Web ブラウザ ツールを使用します。

ステップ 1　ワイヤレス デバイスとのコンソール接続を確立し、**show interface bvi1** Cisco IOS コマンドを入力して、ブリッジ グループ仮想インターフェイス（BVI）IP アドレスを取得します。

ステップ 2　ブラウザのウィンドウを開き、ブラウザ ウィンドウのアドレス行にこの BVI IP アドレスを入力します。Enter を押します。[Enter Network Password] ウィンドウが表示されます。

ステップ 3　ユーザ名を入力します。*Cisco* はデフォルトのユーザ名です。

ステップ 4　ワイヤレス デバイスのパスワードを入力します。デフォルトのパスワードは *Cisco* です。[Summary Status] ページが表示されます。Web ブラウザの設定ページの使用方法の詳細については、次の URL を参照してください。
http://www.cisco.com/en/US/docs/wireless/access_point/12.4_10b_JA/configuration/guide/scg12410b-chap4-first.html#wp1103336

Cisco IOS コマンドライン インターフェイス

自律ワイヤレス デバイスを設定するには、Cisco IOS CLI ツールを使用して次の作業を行います。

- 「無線の設定」（P.4-5）
- 「無線セキュリティ設定の実行」（P.4-5）
- 「無線 QoS の設定」（P.4-8）（任意）

無線の設定

自律モードまたは Cisco Unified モードで信号を伝送するために、ワイヤレス デバイスの無線パラメータを設定します。特定の設定手順については、「無線の設定」（P.5-1）を参照してください。

無線セキュリティ設定の実行

- 「認証の設定」（P.4-5）
- 「ローカル認証システムとしてのアクセス ポイント設定」（P.4-6）
- 「WEP および暗号スイートの設定」（P.4-6）
- 「無線 VLAN の設定」（P.4-6）
- 「SSID の割り当て」（P.4-7）

認証の設定

認証の種類は、Service Set Identifiers（SSID; サービス セット識別子）に準拠します。SSID はアクセス ポイントに設定されます。同一のアクセス ポイントを持つ複数の種類のクライアント デバイスで使用するために、複数の SSID を設定します。

アクセス ポイントを介したワイヤレス クライアント デバイスとネットワークとの通信を開始する前に、クライアント デバイスは、公開キーまたは共用キーによる認証によってアクセス ポイントを認証する必要があります。安全性を最大限にするために、クライアント デバイスは MAC アドレスまたは Extensible Authentication Protocol（EAP; 拡張認証プロトコル）認証を使用してネットワークも認証する必要があります。いずれの認証タイプもネットワークの認証サーバを信頼します。

認証タイプを選択するには、
http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/SecurityAuthenticationTypes.html の『*Authentication Types for Wireless Devices*』を参照してください。

最大限のセキュリティ環境を設定するには、
http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/SecurityRadiusTacacs_1.html の『*RADIUS and TACACS+ Servers in a Wireless Environment*』を参照してください。

ローカル認証システムとしてのアクセス ポイント設定

ローカルの認証サービスまたはバックアップ認証サービスを障害が発生した WAN リンクまたはサーバに提供するために、アクセス ポイントをローカルの認証サーバとして機能するように設定できます。アクセス ポイントは、Lightweight Extensible Authentication Protocol（LEAP）認証、Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling（EAP-FAST）認証または MAC ベースの認証を使用して最大 50 のワイヤレス クライアント デバイスを認証することができます。このアクセス ポイントは毎秒最大 5 つの認証を実行できます。

ローカル オーセンティケータでのアクセス ポイントの設定は、クライアントのユーザ名とパスワードを使用して手動で行います。これは、ローカル オーセンティケータのデータベースが RADIUS サーバと同期化されないためです。クライアントが使用できる VLAN および SSID のリストを指定できます。

ワイヤレス デバイスにこの機能をセットアップする詳細については、http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/SecurityLocalAuthent.html の『*Using the Access Point as a Local Authenticator*』を参照してください。

WEP および暗号スイートの設定

Wired Equivalent Privacy（WEP）暗号はワイヤレス デバイス間での伝送データをスクランブルして、通信機密を保持します。ワイヤレス デバイスおよびそのワイヤレス クライアント デバイスは、同一の WEP キーを使用してデータの暗号化および複合化を行います。WEP キーは、ユニキャストおよびマルチキャストの両方のメッセージを暗号化します。ユニキャスト メッセージとは、ネットワーク上の 1 個のデバイスに向けて送信されるメッセージです。マルチキャスト メッセージは、ネットワーク上の複数のデバイスに送信されます。

暗号スイートは、無線 LAN 上の無線通信を保護するように設計された暗号と完全性アルゴリズムのセットです。Wi-Fi Protected Access（WPA）または Cisco Centralized Key Management（CCKM）をイネーブルにするには、暗号スイートを使用する必要があります。

Temporal Key Integrity Protocol（TKIP）を含む暗号スイートは無線 LAN にとって最適な安全性を提供します。WEP だけしか含まない暗号化スイートでは、最低限のセキュリティしかありません。

暗号化の手順については、http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/SecurityCipherSuitesWEP.html の『*Configuring WEP and Cipher Suites*』を参照してください。

無線 VLAN の設定

無線 LAN で VLAN を使用し、SSID を VLAN に割り当てると、「セキュリティの種類」（P.4-7）で定義されている 4 種類のセキュリティ設定のいずれかを使用して複数の SSID を作成できます。VLAN は、定義されたスイッチのセット内に存在するブロードキャスト ドメインと考えることができます。VLAN は、単一のブリッジング ドメインに接続されている複数のエンド システム（ホスト、またはブリッジやブリッジやルータなどのネットワーク装置）で構成されます。ブリッジング ドメインは、さまざまなネットワーク機器によりサポートされます。ネットワーク機器には、各 VLAN 用の別個のプロトコル グループとともに、ブリッジング プロトコルをそれらの間で動作させる LAN スイッチなどがあります。

無線 VLAN アーキテクチャの詳細については、http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/wireless_vlans.html の『*Configuring Wireless VLANs*』を参照してください。

（注） 無線 LAN で VLAN を使用*しない*と、SSID に割り当てることができるセキュリティ オプションが制限されます。これは、Express Security ページで暗号化設定と認証タイプが対応付けられているためです。

SSID の割り当て

アクセス ポイントとして機能するワイヤレス デバイスには最大 16 個の SSID を設定できます。また、SSID ごとに一意のパラメータ セットを設定できます。たとえば、ある SSID ではネットワーク アクセスだけを利用者に許可し、別の SSID では認証したユーザであれば機密データへのアクセスを許可するといった利用法が可能です。

複数の SSID の作成の詳細については、
http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/ServiceSetID.html の『*Service Set Identifiers*』を参照してください。

（注） VLAN を使用しない場合、暗号化設定（WEP と暗号）が 2.4GHz 無線などのインターフェイスに適用されるため、1 つのインターフェイスで複数の暗号化設定を使用することはできません。たとえば、VLAN がディセーブルの状態でスタティック WEP を使用する SSID を作成した場合は、WPA 認証を使用する SSID を別途作成できません。使用される暗号化設定が異なるためです。ある SSID のセキュリティ設定と、別の SSID の設定が競合していた場合、1 つ以上の SSID を削除して競合を解消できます。

セキュリティの種類

表 4-1 は、SSID に割り当てられる 4 つのセキュリティ タイプについて説明しています。

表 4-1　SSID セキュリティの種類

セキュリティ タイプ	説明	有効になるセキュリティ機能
セキュリティなし	これは安全性が最も低いオプションです。このオプションは、パブリック スペースで SSID を使用する場合に限定して使用し、ネットワークへのアクセスを制限する VLAN に割り当てる必要があります。	—
スタティック WEP キー	このオプションは、[No Security] よりは安全です。ただし、静的 WEP キーは攻撃に対して脆弱です。この設定を選択する場合は、MAC アドレス ベースのワイヤレス デバイスへのアソシエートを制限するかどうかを検討してください。詳細については、次の URL の『*Cipher Suites and WEP*』を参照してください。 http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/SecurityCipherSuitesWEP.html または ネットワーク内に RADIUS サーバがない場合、アクセス ポイントをローカル認証サーバとして使用するかを検討してください。 手順については、
http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/SecurityLocalAuthent.html の『*Using the Access Point as a Local Authenticator*』を参照してください。	WEP が必須。ワイヤレス デバイス キーに合う WEP キーがないと、この SSID を使用してもクライアント デバイスをアソシエートできません。

表 4-1　SSID セキュリティの種類 （続き）

セキュリティ タイプ	説明	有効になるセキュリティ機能
EAP[1] 認証	このオプションは、802.1X 認証（LEAP[2]、PEAP[3]、EAP-TLS[4]、EAP-FAST[5]、EAP-TTLS[6]、EAP-GTC[7]、EAP-SIM[8]、およびその他の 802.1X/EAP ベースの製品）がイネーブルになります。 この設定は、必須の暗号化、WEP、オープン認証プラス EAP、ネットワーク EAP 認証を使用し、キー管理なしで RADIUS サーバ認証ポート 1645 を使用します。 ネットワーク上の認証サーバの IP アドレスと共有秘密キーを入力する必要があります（サーバ認証ポート 1645）。802.1X 認証によって動的暗号キーが提供されるため、WEP キーを入力する必要はありません。	必須の 802.1X 認証。この SSID を使用してアソシエートするクライアント デバイスは、802.1X 認証を実行する必要があります。 ワイヤレス クライアントで EAP-FAST を使用する認証が設定されている場合は、Open 認証 + EAP も設定する必要があります。EAP によるオープン認証を設定していない場合、以下の警告メッセージが表示されます。 `SSID CONFIG WARNING: [SSID]: If radio clients are using EAP-FAST, AUTH OPEN with EAP should also be configured.`
WPA[9]	このオプションは、データベース認証されたユーザにワイヤレス アクセスを許可します。アクセスは認証サーバのサービスを通じて行います。ユーザの IP トラフィックは WEP で使用されるものより強力なアルゴリズムで暗号化されます。 この設定では暗号キー、TKIP[10]、オープン認証プラス EAP、ネットワーク EAP 認証、必須のキー管理 WPA、および RADIUS サーバ認証ポート 1645 を使用します。 EAP 認証の場合と同じように、ネットワーク上の認証サーバの IP アドレスと共有秘密キーを入力する必要があります（サーバ認証ポート 1645）。	WPA 認証が必須。この SSID を使用して対応付けを行うクライアント デバイスは WPA 対応でなければなりません。 ワイヤレス クライアントで EAP-FAST を使用する認証が設定されている場合は、Open 認証 + EAP も設定する必要があります。EAP によるオープン認証を設定していない場合、以下の警告メッセージが表示されます。 `SSID CONFIG WARNING: [SSID]: If radio clients are using EAP-FAST, AUTH OPEN with EAP should also be configured.`

1. EAP = Extensible Authentication Protocol
2. LEAP = Lightweight Extensible Authentication Protocol
3. PEAP = Protected Extensible Authentication Protocol
4. EAP-TLS = Extensible Authentication Protocol-Transport Layer Security
5. EAP-FAST = Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling
6. EAP-TTLS = Extensible Authentication Protocol-Tunneled Transport Layer Security
7. EAP-GTC = Extensible Authentication Protocol-Generic Token Card
8. EAP-SIM = Extensible Authentication Protocol-Subscriber Identity Module
9. WPA = Wi-Fi Protected Access
10. TKIP = Temporal Key Integrity Protocol

無線 QoS の設定

Quality of Service（QoS）を設定すると、特定のトラフィックを他のトラフィックよりも優先的に処理できます。QoS がない場合、デバイスは各パケットに最善のサービスを提供します（パケットの内容やサイズは問いません）。信頼性、遅延限度、またはスループットに関して保証することなく、スイッチはパケットを送信します。ワイヤレス デバイスに QoS を設定するには、http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/QualityOfService.html の『*Quality of Service in a Wireless Environment*』を参照してください。

ホット スタンバイ モードでのアクセス ポイントの設定

ホット スタンバイ モードでは、アクセス ポイントは別のアクセス ポイントのバックアップとして指定されます。スタンバイ アクセス ポイントは、アクセス ポイントのそばに配置され、それを監視します（設定は、このアクセス ポイントとまったく同じにします）。スタンバイ アクセス ポイントは、クライアントとして監視対象のアクセス ポイントとアソシエートします。また監視対象のアクセス ポイントに、イーサネットおよび無線ポートを通して Internet Access Point Protocol（IAPP; インターネット アクセス ポイント プロトコル）クエリを送信します。モニタするアクセス ポイントから応答がない場合、スタンバイ アクセス ポイントはオンラインに切り替わり、そのアクセス ポイントの役割をネットワーク上で引き継ぎます。

スタンバイ アクセス ポイントの設定は、IP アドレスを除き、モニタするアクセス ポイントの設定と一致している必要があります。モニタ対象アクセス ポイントがオフラインになり、スタンバイ アクセス ポイントがそれを引き継いだ場合、両アクセス ポイントの設定が同一であれば、クライアント デバイスは簡単かつ確実にスタンバイ アクセス ポイントに切り替わることができます。詳細については、http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/RolesHotStandby.html の『*Hot Standby Access Points*』を参照してください。

Cisco Unified ソフトウェアへのアップグレード

アクセス ポイントを Cisco Unified モードで実行するには、次の手順に従ってソフトウェアをアップグレードする必要があります。

- 「アップグレードの準備」（P.4-9）
- 「アップグレードの実行」（P.4-11）
- 「AP ブートローダのアップグレード」（P.4-12）
- 「アクセス ポイントへのソフトウェアのダウンロード」（P.4-12）
- 「アクセス ポイントでのソフトウェア リカバリ」（P.4-13）

ソフトウェア前提条件

- アクセス ポイントが組み込まれた Cisco 880 シリーズ ISR は、ルータが advipservices フィーチャセットと Cisco IOS Release15.2(4)M1 またはそれ以降のバージョンを実行している場合、自律ソフトウェアから Cisco Unified ソフトウェアにアップグレードできます。
- Cisco Unified アーキテクチャの組み込み型アクセス ポイントを使用するには、Cisco Wireless LAN Configuration（WLC）が、シングル無線（Cisco IOS Release 7.0.116.0 またはそれ以降のバージョン）とデュアル無線（Cisco IOS Release 7.2.110.0 またはそれ以降のバージョン）の最小バージョンを実行している必要があります。

アップグレードの準備

アップグレードを準備するには次の作業を行います。

- 「アクセス ポイントの IP アドレスの保護」（P.4-10）
- 「モード設定がイネーブルになっていることの確認」（P.4-10）

アクセス ポイントの IP アドレスの保護

アクセス ポイントの IP アドレスを保護することにより、アクセス ポイントは WLC と通信でき、起動時に Unified イメージをダウンロードできます。ホスト ルータは、DHCP プールを通じてアクセス ポイント DHCP サーバ機能を提供します。このアクセス ポイントは WLC と通信し、DHCP プール コンフィギュレーションのコントローラ IP アドレスのオプション 43 を設定します。以下に設定サンプルを示します。

```
ip dhcp pool embedded-ap-pool
network 60.0.0.0 255.255.255.0
dns-server 171.70.168.183
default-router 60.0.0.1
option 43 hex  f104.0a0a.0a0f   (single WLC IP address(10.10.10.15) in hex format)
int vlan1
ip address 60.0.0.1 255.255.255.0
```

WLC 検出プロセスの詳細については、
http://www.cisco.com/en/US/docs/wireless/controller/4.0/configuration/guide/ccfig40.html の『*Cisco Wireless LAN Configuration Guide*』を参照してください。

モード設定がイネーブルになっていることの確認

モード設定がイネーブルになっていることを確認するには、次の手順に従います。

ステップ 1　ルータから WLC サーバに ping を実行し、接続を確認します。

ステップ 2　**service-module wlan-ap 0 session** コマンドを実行し、アクセス ポイントへのセッションを確立します。

ステップ 3　アクセス ポイントが自律起動イメージを動作させているか確認します。

ステップ 4　**show boot** コマンドを入力してアクセス ポイントのモード設定がイネーブルになっていることを確認します。次に、コマンドの出力例を示します。

```
# show boot
BOOT path-list:      flash:ap802-k9w7-mx.124/ap802-k9w7-mx.124
Config file:         flash:/config.txt
Private Config file: flash:/private-config
Enable Break:          no
Manual Boot:         yes
HELPER path-list:    no
NVRAM/Config file
buffer size:   32768
Mode Button:    on
Radio Core TFTP:
ap#
```

アップグレードの実行

自律ソフトウェアを Cisco Unified ソフトウェアにアップグレードするには、次の手順に従います。

ステップ 1　アクセス ポイントの起動イメージを Cisco Unified アップグレード イメージ（*リカバリ イメージ*とも呼びます）に変更するには、グローバル コンフィギュレーション モードで **service-module wlan-ap 0 bootimage unified** コマンドを実行します。

```
Router# configure terminal
Router(config)# service-module wlan-ap 0 bootimage unified
Router(config)# end
```

（注）　**service-module wlan-ap 0 bootimage unified** コマンドが実行されない場合、advipservices または advipsevices_npe ソフトウェア ライセンスがイネーブルになっているかどうかを確認してください。

アクセス ポイントの起動イメージのパスを識別するには、アクセス ポイントのコンソールから EXEC モードで **show boot** コマンドを使用します。

```
autonomous-AP# show boot
BOOT path-list: flash:/ap802-rcvk9w8-mx/ap802-rcvk9w8-mx
```

ステップ 2　正規の手順でシャットダウンを行ってアクセス ポイントをリブートし、アップグレード プロセスを完了するには、特権 EXEC モードで **service-module wlan-ap 0 reload** コマンドを実行します。アクセス ポイントとのセッションを確立し、アップグレード プロセスを監視します。

AP から自律モードへアップグレードまたは復帰する際のトラブルシューティング

Q. 私のアクセス ポイントでは、自律ソフトウェアから Cisco Unified ソフトウェアへのアップグレードに失敗し、リカバリ モードに陥ったままになっているようです。どうすればいいでしょうか。

A. アクセス ポイントで自律ソフトウェアから Unified ソフトウェアにアップグレードできなかった場合は、次の操作を実行してください。

- リカバリ イメージを起動する前に、自律アクセス ポイントのスタティック IP アドレスが BVI インターフェイスに設定されていないことを確認します。
- ルータ / アクセス ポイントと WLC 間で ping を実行して、接続が確立されているか確認します。
- アクセス ポイントと WLC クロック（時刻と日付）が正しく設定されているか確認します。

Q. アクセス ポイントが起動を試行しているのですが、何度やってもうまくいきません。どうしてですか。
またアクセス ポイントがリカバリ イメージでスタックしたまま、Unified ソフトウェアにアップグレードしません。どうしてですか。

A. アクセス ポイントでは、起動を試みて失敗したり、リカバリ モードに陥ってしまい、Unified ソフトウェアにアップグレードできない場合があります。このいずれかの状態になった場合は、**service-module wlan-ap0 reset bootloader** コマンドを実行してアクセス ポイントをブートローダに戻し、手動でイメージを復帰させてください。

AP ブートローダのアップグレード

AP802 では、ホスト ルータ イメージの一部としてブートローダを使用できます。ブートローダをアップグレードするには、次の手順を実行します。

ステップ 1　**show platform version** コマンドを使用して、最初のコアで実行されているホスト ルータ イメージにバンドルされている WLAN AP ブートローダを確認します。

```
Router# show platform version
Platform Revisions/Versions :
.
WLAN AP Boot loader (bundled):
AP802 Boot Loader (AP802-BOOT-M) Version 12.4(25e)JA1, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Compiled Wed 30-May-12 03:46 by prod_rel_team
```

ステップ 2　ルータと WLAN AP の間でセッションを開きます。

ルータとアクセス ポイントの間でセッションを開く方法については、「無線コンフィギュレーション セッションの開始」（P.4-2）を参照してください。

ステップ 3　WLAN AP ブートローダのバージョンを確認します。

WLAN AP ブートローダでは、**version** コマンドを使用します。

```
ap: version
AP802 Boot Loader (AP802-BOOT-M) Version 12.4(25e)JA1, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Compiled Wed 30-May-12 03:46 by prod_rel_team
```

WLAN AP IOS で show version コマンドを使用します。

```
ap# show version
.
BOOTLDR: AP802 Boot Loader (AP802-BOOT-M) Version 12.4(25e)JA1, RELEASE SOFTWARE (fc1)
<snip>
Configuration register is 0xF
```

ステップ 4　次のコマンドを使用してブートローダをアップグレードします。

```
Router# service-module wlan-ap 0 upgrade bootloader
Router# service-module wlan-ap 0 reset
```

アクセス ポイントへのソフトウェアのダウンロード

直前の自律イメージにアクセス ポイントの起動をリセットするには、最初のコアで実行されているホスト ルータで、特権 EXEC モードで **service-module wlan-ap0 bootimage autonomous** コマンドを使用します。自律ソフトウェア イメージをアクセス ポイントにリロードするには、**service-module wlan-ap 0 reload** コマンドを使用します。

```
Router# configure terminal
Router(config)# service-module wlan-ap 0 bootimage autonomous
Router(config)# end
Router# write
Router# service-module wlan-ap 0 reload
```

アクセス ポイントでのソフトウェア リカバリ

アクセス ポイントのイメージをリカバリするには、特権 EXEC モードで **service-module wlan-ap0 reset bootloader** コマンドを使用します。このコマンドを使用すると、アクセス ポイントがブートローダに戻り、手動でイメージをリカバリできるようになります。

注意　このコマンドの使用には注意が必要です。この操作では通常のシャットダウンが実行*されない*ことから、実行中のファイル操作に影響が生じる場合があります。このコマンドは、シャットダウンまたは障害状態からリカバリする目的に限り使用してください。

サポートされるイメージ

Cisco ISR 880 シリーズでサポートされるイメージの詳細については、「サポートされるイメージ」（P.1-11）を参照してください。

関連資料

自律およびユニファイド設定手順の詳細については、次のマニュアルを参照してください。

- 「自律モードのマニュアル」—表 4-2
- 「Unified モードのマニュアル」—表 4-3

表 4-2　自律モードのマニュアル

自律モード	リンク	説明
ネットワーク デザイン		
ワイヤレスの概要	ワイヤレス デバイス概要	ネットワークのワイヤレス デバイスの役割について説明します。
『Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges Versions 12.4(25d)JA and 12.3(8)JEE』	http://www.cisco.com/en/US/docs/wireless/access_point/12.4.25d.JA/Command/reference/cr12425d-preface.html	Cisco Aironet アクセス ポイントとブリッジを設定するための Cisco IOS Release 12.4(25d)JA と Cisco IOS Release 12.3(8)JEE のコマンドについて説明します。
設定		
無線の設定	無線の設定	無線を設定する方法について説明します。
セキュリティ		
『Authentication Types for Wireless Devices』	http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/SecurityAuthenticationTypes.html	アクセス ポイントに設定されている認証タイプについて説明します。

表 4-2　自律モードのマニュアル （続き）

自律モード	リンク	説明
『RADIUS and TACACS+ Servers in a Wireless Environment』	http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/SecurityRadiusTacacs_1.html	RADIUS[1] および TACACS+[2] のイネーブルと設定の方法、アカウンティング情報の詳細説明、さらに、管理側が行う認証と認証プロセスの柔軟な制御方法について説明します。RADIUS および TACACS+ は、AAA[3] を通じて活用され、AAA コマンドを使用する場合だけイネーブルにできます。
『Using the Access Point as a Local Authenticator』	http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/SecurityLocalAuthent.html	ローカル認証を担当するアクセス ポイントというロールにおいて、ワイヤレス デバイスを使用する方法について説明しています。アクセス ポイントは小規模無線 LAN のスタンドアロン認証システムとして機能するか、またはバックアップ認証サービスを提供します。アクセス ポイントはローカル認証サーバとして、最大 50 のクライアント デバイスに対して Light Extensible Authentication Protocol（LEAP; 拡張認証プロトコル）認証、Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling（EAP-FAST）認証、および Media Access Control（MAC; メディア アクセス コントロール）ベースの認証を実行します。
『Cipher Suites and WEP』	http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/SecurityCipherSuitesWEP.html	WPA[4] および CCKM[5]、WEP[6]、および WEP 機能（AES[7]、MIC[8]、TKIP[9]、およびブロードキャスト キーのローテーションなど）を使用するときに必要な暗号スイートの設定方法について解説します。
『Hot Standby Access Points』	http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/RolesHotStandby.html	ホット スタンバイ ユニットとしてワイヤレス デバイスを設定する方法について説明します。
無線 VLAN の設定	http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/wireless_vlans.html	アクセス ポイントが、有線 LAN 上に設定された VLAN と動作するよう設定する方法について説明しています。
『Service Set Identifier』	http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/ServiceSetID.html	ワイヤレス デバイスは、アクセス ポイントとして最大 16 の SSID[10] をサポートできます。本マニュアルでは、ワイヤレス デバイス上の SSID の設定および管理方法について説明します。

表 4-2　自律モードのマニュアル （続き）

自律モード	リンク	説明
管理		
Quality of Service	http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/QualityOfService.html	シスコのワイヤレス インターフェイスで QoS[11] を設定する方法について説明します。この機能により、別のトラフィックを犠牲にして特定のトラフィックを優先させることができます。QoS がない場合、デバイスは各パケットに最善のサービスを提供します（パケットの内容やサイズは問いません）。信頼性、遅延限度、またはスループットに関して保証することなく、スイッチはパケットを送信します。
『Regulatory Domains and Channels』	http://www.cisco.com/en/US/docs/routers/access/800/860-880-890/software/configuration/guide/scg_chanels.html	世界中の規制ドメイン内の Cisco アクセス製品でサポートしている無線チャネルが記載されています。
『System Message Logging』	http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/SysMsgLogging.html	ワイヤレス デバイスでシステム ロギング メッセージを設定する方法について説明します。

1. RADIUS = リモート認証ダイヤルイン ユーザ サービス
2. TACACS+ = Terminal Access Controller Access Control System Plus
3. AAA = Authentication, Authorization, and Accounting
4. WPA = Wireless Protected Access
5. CCKM = Cisco Centralized Key Management
6. WEP = Wired Equivalent Privacy
7. AES = Advanced Encryption Standard
8. MIC = Message Integrity Check
9. TKIP = Temporal Key Integrity Protocol
10. SSID = サービス セット ID
11. QoS = Quality of Service

表 4-3　Unified モードのマニュアル

ネットワーク デザイン	リンク
『Why Migrate to the Cisco Unified Wireless Network?』	http://www.cisco.com/en/US/solutions/ns175/networking_solutions_products_genericcontent0900aecd805299ff.html
『Wireless LAN Controller (WLC) FAQ』	http://www.cisco.com/en/US/products/ps6366/products_qanda_item09186a008064a991.shtml
シングル無線 AP802	
『Cisco Wireles LAN Controller Configuration Guide, Release 7.0.116.0』	http://www.cisco.com/en/US/docs/wireless/controller/7.0MR1/configuration/guide/cg_controller_setting.html
デュアル無線 AP802	
『Cisco Unified Wireless Network Software Release 7.2.110.0 （7.2 Maintenance Release 1）』	http://www.cisco.com/en/US/prod/collateral/wireless/ps6302/ps8322/ps10315/product_bulletin_c25-707629.html