CHAPTER 8

ワイヤレス デバイスの基本設定

このモジュールは、次の Integrated Services Routers（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。

- Cisco 860 シリーズ
- Cisco 880 シリーズ
- Cisco 890 シリーズ

（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 ソフトウェアのアップグレード」（P.8-9）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。

ワイヤレス 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。

ルータの Cisco IOS コマンドライン インターフェイス（CLI）から次のコマンドをグローバル コンフィギュレーション モードで入力します。

	コマンド	目的

ステップ 1	**interface wlan-ap0**
	
	例：
	`router(config)# interface wlan-ap0`
	`router(config-if)#`
		ルータのコンソール インターフェイスをワイヤレス デバイスに定義します。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 を使用してください。
		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`
		インターフェイスの IP アドレスおよびサブネット マスクを指定します。
		
		（注）　**ip unnumbered vlan1** コマンドを使用すると、IP アドレスをシスコ サービス統合型ルータに割り当てられている IP アドレスと共用できます。

ステップ 3	**no shut** **例：** `router(config-if)# no shut`	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。
ステップ 4	**interface vlan1** **例：** `router(config-if)# interface vlan1`	内部ギガビット イーサネット 0（GE 0）ポートから他のインターフェイスへのデータ通信に、仮想 LAN インターフェイスを使用するように指定します。 Cisco 860 シリーズ、Cisco 880 シリーズ、および Cisco 890 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。

	コマンド	目的
ステップ 5	**ip address** *subnet mask* **例：** `router(config-if)# ip address 10.10.0.30 255.255.255.0`	インターフェイスの IP アドレスおよびサブネット 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で接続を開きます。

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。このコマンドを入力すると、Cisco IOS ソフトウェアの **dot11 radio** レベルに自動的にスキップします。

セッションを閉じる

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. **Control-Shift-6 x**

ルータ

2. 通信を切断します。
3. **Enter** キーを 2 回押します。

ワイヤレス設定

（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。「ワイヤレス コンフィギュレーション セッションの開始」（P.8-2）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 IOS コマンドライン インターフェイス」（P.8-4）：自律ソフトウェア
- 「Cisco Express のセットアップ」（P.8-4）：ユニファイド ソフトウェア

（注）　Autonomous 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 ソフトウェアのアップグレード」（P.8-9）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終了後、Web ブラウザのインターフェイスでデバイスを設定します。手順については次の URL を参照してください。
http://cisco.com/en/US/docs/wireless/access_point/12.4_10b_JA/configuration/guide/scg12410b-chap2-gui.html

Cisco Express のセットアップ

Unified 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、Bridge-Group Virtual Interface（BVI; ブリッジ グループ仮想インターフェイス）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 キーを押します。[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。デフォルトのユーザ名は *Cisco* 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に関する詳細については、次の URL を参照してください。
http://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.8-5）
- 「ワイヤレス セキュリティの設定」（P.8-5）
- 「ワイヤレス サービス品質の設定」（P.8-8）（任意）

無線の設定

Autonomous 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、第 9 章「無線の設定」を参照してください。

ワイヤレス セキュリティの設定

認証の設定

認証のタイプは、アクセス ポイントに設定される Service Set Identifiers（SSID; サービス セット ID）に対応しています。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、公開鍵または共用鍵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、次のシスコの URL で Cisco.com の『*Authentication Types for Wireless Devices*』の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/SecurityAuthenticationTypes.html

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 Cisco.com で『*RADIUS and TACACS+ Servers in a Wireless Environment*』のマニュアルを参照してください。

ローカル オーセンティケータとしてのアクセス ポイントの設定

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。アクセス ポイントは毎秒最大 5 回の認証を行います。

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 のリストも設定可能です。

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 Cisco.com で『*Using the Access Point as a Local Authenticator*』のマニュアル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。ワイアレス デバイスとそのワイヤレス クライアント デバイスは同じ WEP キーを使用してデータの暗号化と復号化を行います。WEP キーはユニキャスト と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 メッセージは、ネットワーク上の 1 つのデバイスだけに送信されます。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、ワイヤレス LAN 上の無線通信を保護するように設計された暗号化と安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）を有効にするには、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ワイヤレス LAN にとって最適な安全性を提供します。WEP だけを含む暗号スイートは、安全性が最も劣ります。

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 Cisco.com で『*Configuring WEP and Cipher Suites*』のマニュアルを参照してください。

ワイヤレス VLAN の設定

ワイヤレス LAN で VLAN を使用し、SSID を VLAN に割り当てると、「セキュリティ タイプ」（P.8-7）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、定義済みのスイッチ セット内のブロードキャスト 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。このブリッジング ドメインはネットワーク装置のさまざまな部分でサポートされています。たとえば、相互にブリッジング プロトコルを稼動する LAN スイッチは、VLAN ごとに個別のプロトコル グループが 1 つあります。

ワイヤレス 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
Cisco.com で『*Configuring Wireless VLANs*』のマニュアルを参照してください。

（注） ワイヤレス 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
Cisco.com で『*Service Set Identifiers*』のマニュアルを参照してください。

お読みください VLAN を使用しない場合は、2.4-GHz 無線などのインターフェイスに暗号化設定（WEP および暗号）が適用されます。1 つのインターフェイスに複数の暗号化設定を使用できません。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。SSID のセキュリティ設定が他の SSID の設定と競合する場合は、SSID を 1 つまたは複数削除して競合が生じないようにします。

セキュリティ タイプ

表 8-1 に、SSID に割り当てることができる 4 つのセキュリティ タイプを示します。

表 8-1　SSID セキュリティのタイプ

セキュリティ タイプ	説明	イネーブル化されたセキュリティ機能
セキュリティなし	セキュリティが一番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。	なし。
スタティック WEP キー	セキュリティなしよりもセキュリティが高いオプションです。ただし、スタティック WEP キーは攻撃に対して脆弱です。このオプションを設定する場合は、MAC アドレスに基づいてワイヤレス デバイスとのアソシエーションを制限することを検討してください。設定の手順については、http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/SecurityCipherSuitesWEP.html の Cisco.com で『*Cipher Suites and WEP*』のマニュアルを参照してください。 または ネットワークに RADIUS サーバが配置されていない場合は、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こと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 Cisco.com で『*Using the Access Point as a Local Authenticator*』のマニュアルを参照してください。	必須の WEP。クライアント デバイスは、ワイヤレス デバイス キーに一致する WEP キーなしでは、この SSID を使用して対応付けできません。

表 8-1　SSID セキュリティのタイプ （続き）

セキュリティ タイプ	説明	イネーブル化されたセキュリティ機能
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、鍵管理なしで RADIUS サーバ認証ポート 1645 を使用します。 ネットワークの認証サーバ（サーバ認証ポート 1645）に関する IP アドレスおよび共有シークレットの入力が必要となります。802.1X 認証ではダイナミック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。クライアント デバイスがこの SSID を使用して対応付けを行う場合、802.1X 認証を実行する必要があります。 EAP-FAST を使用して無線クライアントが認証されるように設定している場合、EAP のオープン認証も設定する必要があります。オープン認証を EAP で設定しないと、次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 認証と同様、ネットワークの認証サーバ（サーバ認証ポート 1645）に IP アドレスおよび共有シークレットを入力する必要があります。	必須の WPA 認証。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。 EAP-FAST を使用して無線クライアントが認証されるように設定している場合、EAP のオープン認証も設定する必要があります。オープン認証を EAP で設定しないと、次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

ワイヤレス サービス品質の設定

サービス品質（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 を設定しない場合、デバイスは、パケットのコンテンツやサイズに関係なくすべてのパケットにベストエフォートのサービスを提供します。この場合のパケット送信では、信頼性、遅延限度、スループットのいずれも保証されません。ワイヤレス デバイスのサービス品質（QoS）に設定するには、URL http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/QualityOfService.html の『*Quality of Service in a Wireless Environment*』のマニュアルを参照してください。

ホット スタンバイ モードのアクセス 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。このスタンバイ アクセス ポイントは、監視するアクセス ポイントの近くに配置され、監視対象のアクセス ポイントとまったく同じ設定が行われます。スタンバイ アクセス ポイントは監視対象のアクセス ポイントに対するクライアントとして対応付けられ、イーサネットと無線ポートを介して 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）要求を送信します。監視対象のアクセス ポイントが応答に失敗した場合は、スタンバイ アクセス ポイントがオンラインになり、監視対象のアクセス ポイントのネットワークでの立場を引き継ぎます。

スタンバイ アクセス ポイントの設定は、監視対象のアクセス ポイントの設定と IP アドレス以外は同一にする必要があります。監視対象のアクセス ポイントがオフラインになり、ネットワークでの立場をスタンバイ アクセス ポイントが引き継いだ場合、両者の設定が同じであるため、クライアント デバイスはスタンバイ アクセス ポイントに容易にスイッチできます。詳細については、Cisco.com の http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/RolesHotStandby.html で『*Hot Standby Access Points*』のマニュアルを参照してください。

Cisco Unified ソフトウェアのアップグレード

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.8-9）
- 「アップグレードの実行」（P.8-11）
- 「アクセス ポイントでのソフトウェアのダウングレード」（P.8-12）
- 「アクセス ポイントでのソフトウェアの回復」（P.8-12）

ソフトウェアの前提条件

- アクセス ポイントが組み込まれた Cisco 890 シリーズ ISR は、ルータが IP Base 機能セットと Cisco IOS 12.4(22)YB ソフトウェア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。
- 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 機能セットと Cisco IOS 12.4(20)T ソフトウェア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 アーキテクチャの中で組み込み型アクセス ポイントを使用するには、バージョン 5.1 以降のシスコ Wireless LAN Configuration（WLC）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.8-10）
- 「モード設定がイネーブルになっていることの確認」（P.8-10）

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 ポイントに DHCP サーバ機能を提供します。次に、アクセス ポイントは WLC と通信を行って、DHCP プール設定でオプション 43 をコントローラの IP アドレスにセットアップします。設定例は次のとおりです。

```
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.com で『*Cisco Wireless LAN Configuration Guide*』のマニュアル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

次の手順を行います。

1. ルータから WLC に ping を送信して IP 接続が確立されていることを確認します。
2. **service-module wlan-ap 0 session** コマンドを入力してアクセス ポイントへのセッションを確立します。
3. アクセス ポイントで自律起動イメージを実行していることを確認します。
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、このコマンドの出力例を示します。

```
Autonomous-AP#show boot
BOOT path-list:      flash:ap801-k9w7-mx.124-10b.JA3/ap801-k9w7-mx.124-10b.JA3
Config file:         flash:/config.txt
Private Config file: flash:/private-config
Enable Break:        yes
Manual Boot:         yes
HELPER path-list:
NVRAM/Config file
buffer size:   32768
Mode Button:    on
```

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（*回復イメージ*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# conf terminal
Router(config)# service-module wlan-ap 0 bootimage unified
Router(config)# end
```

（注）　**service-module wlan-ap 0 bootimage unified** コマンドを実行しても正しく処理されない場合は、ソフトウェア ライセンスがまだ有効であるか確認してください。

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:/ap801-rcvk9w8-mx/ap801-rcvk9w8-mx
```

ステップ 2　正規の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、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 reload** コマンドを実行します。その後、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。

GUI の設定ページを使用したワイヤレス デバイスのセットアップの詳細については、「Cisco Express のセットアップ」（P.8-4）を参照してください。

アップグレードのトラブルシューティングまたは AP の Autonomous モードへの復帰

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、回復モードに陥ったままになっているようです。次にどのような作業が必要でしょうか。

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。

- 回復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. 私のアクセス ポイントでは、何度試みても起動できません。何が原因でしょうか。
私のアクセス ポイントは回復イメージのままになってしまい、Unified ソフトウェアにアップグレードできません。何が原因でしょうか。

A. アクセス ポイントでは、起動を試みて失敗したり、回復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。

アクセス ポイントでのソフトウェアのダウングレード

アクセス ポイント BOOT を直前の自律イメージにリセットするには、グローバル コンフィギュレーション モードで **service-module wlan-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。

アクセス ポイントでのソフトウェアの回復

アクセス ポイントにイメージを回復するには、グローバル コンフィギュレーション モードで **service-module wlan-ap0 reset bootloader** コマンドを使用します。このコマンドは手動でイメージを回復するためにアクセス ポイントをブートローダに戻します。

注意　このコマンドを使用するときは注意が必要です。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回復する目的に限り使用してください。

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。

- シスコの自律ソフトウェアのマニュアル—表 8-2
- Cisco Unified ソフトウェアのマニュアル—表 8-3

表 8-2　シスコの自律ソフトウェアのマニュアル

ネットワーク設計	リンク先
ワイヤレスの概要	第 2 章「ワイヤレス デバイスの概要」
設定	**リンク先**
無線の設定	第 9 章「無線の設定」
セキュリティ	**リンク先**
『Authentication Types for Wireless Devices』	このマニュアルは、アクセス ポイントに設定する認証タイプについて解説します。 http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/SecurityAuthenticationTypes.html
『RADIUS and TACACS+ Servers in a Wireless Environment』	このマニュアルは、RADIUS および TACACS+ 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[1] 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。 http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/SecurityRadiusTacacs_1.html

表 8-2　シスコの自律ソフトウェアのマニュアル （続き）

ネットワーク設計	リンク先
『Using the Access Point as a Local Authenticator』	このマニュアルは、アクセス ポイントを小規模のワイヤレス LAN に対するスタンドアロンのオーセンティケータとして使用したり、バックアップ認証サービスを提供したりといった、ローカル オーセンティケータとして機能するようにワイヤレス デバイスを使用する方法について解説します。アクセス ポイントはローカル オーセンティケータとして、最大 50 のクライアント デバイスに対し、LEAP 認証、EAP-FAST 認証、および MAC ベースの認証を実施します。 http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/SecurityLocalAuthent.html
『Cipher Suites and WEP』	このマニュアルは、WPA および CCKM[2]、WEP、および WEP 機能（AES[3]、MIC[4]、TKIP、およびブロードキャスト鍵のローテーションなど）を使用するために必要な暗号スイートの設定方法について解説します。 http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/SecurityCipherSuitesWEP.html
『Hot Standby Access Points』	このマニュアルは、ワイヤレス デバイスをホットスタンバイ ユニットとして設定する方法について解説します。 http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/RolesHotStandby.html
『Configuring Wireless VLANs』	このマニュアルは、ワイヤード LAN に設定された VLAN とともにアクセス ポイントを使用するための設定方法について解説します。 http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/wireless_vlans.html
『Service Set Identifiers』	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 をサポートできます。このマニュアルは、ワイヤレス デバイスで SSID を設定および管理する方法について解説します。 http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/ServiceSetID.html
管理	**リンク先**
アクセス ポイントの管理	第 10 章「ワイヤレス デバイスの管理」
『Quality of Service』	このマニュアルは、ユーザのシスコ ワイヤレス インターフェイスでの QoS の設定方法について解説します。この機能を使用すると、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 を設定しない場合、デバイスは、パケットのコンテンツやサイズに関係なくすべてのパケットにベストエフォートのサービスを提供します。この場合のパケット送信では、信頼性、遅延限度、スループットのいずれも保証されません。 http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/QualityOfService.html

表 8-2　シスコの自律ソフトウェアのマニュアル （続き）

ネットワーク設計	リンク先
『Regulatory Domains and Channels』	このマニュアルは、シスコのアクセス製品でサポートされている世界の規制区域内の無線チャネルを一覧表示します。 http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/RadioChannelFrequencies.html
『System Message Logging』	このマニュアルは、ワイヤレス デバイスへのシステム メッセージ ロギングの設定方法について解説します。 http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/SysMsgLogging.html

1. AAA = Authentication, Authorization, and Accounting
2. CCKM = Cisco Centralized Key Management
3. AES = Advanced Encryption Standard
4. MIC = Message Integrity Check

表 8-3　Cisco Unified ソフトウェアのマニュアル

ネットワーク設計	リンク先
『Why Migrate to the Cisco Unified Wireless Network?』	http://www.cisco.com/en/US/prod/collateral/wireless/ps5679/ps6548/prod_white_paper0900aecd804f19e3_ps6305_Products_White_Paper.html
『LWAPP[1] Wireless LAN Controllers』	http://www.cisco.com/en/US/products/ps6366/index.html
『LWAPP Wireless LAN Access Points』	http://www.cisco.com/en/US/prod/collateral/wireless/ps5678/ps6306/prod_white_paper0900aecd802c18ee_ps6366_Products_White_Paper.html
『Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges, versions 12.4(10b) JA and 12.3(8) JEC』	http://www.cisco.com/en/US/docs/wireless/access_point/12.4_10b_JA/command/reference/cr2410b.html
『Cisco Aironet 1240AG Access Point Support Documentation』	http://www.cisco.com/en/US/docs/wireless/access_point/1240/quick/guide/ap1240qs.html
『Cisco 4400 Series Wireless LAN Controllers Support Documentation』	http://www.cisco.com/en/US/products/ps6366/tsd_products_support_series_home.html

1. LWAPP = Lightweight Access Point Protocol