無線デバイスの設定

次の項では、ワイヤレス デバイスを Cisco 1941W サービス統合型ルータ（ISR）に設定する方法について説明します。

（注） デバイス上のソフトウェアを Cisco Unified ソフトウェアにアップグレードできます。「Cisco Unified ソフトウェアへのアップグレード」（P.9）を参照してください。

（注） 無線デバイスはルータに埋め込まれており、接続のための外部コンソール ポートがありません。ワイヤレス デバイスを設定するときは、コンソール ケーブルを使用してパーソナル コンピュータをホスト ルータのコンソール シリアル ポートに接続した後、指示に従ってコンフィギュレーション セッションを確立します。

無線コンフィギュレーション セッションの開始

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 コマンドライン インターフェイス（CLI）に入力します。

手順の概要

1. **interface wlan-ap0**
2. **ip address** ***subnet mask***
3. **no shut**
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。これはルータのコンソール デバイスとワイヤレス デバイス間の通信に使用されます。
		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`
	
	例：
	`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 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 GE0[1] ポートでデータ通信の仮想 LAN インターフェイスを他のインターフェイスに指定します。

	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 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)#`
		このモードを終了します。

ステップ 7	**exit**
	
	例：
	`router(config)# exit`
	`router#`
		この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。

1. GE0 = ギガビット イーサネット 0

ヒント IOS ソフトウェアのエイリアスを作成してコンソールと無線デバイス間でセッションを開始したい場合、**alias exec dot11radio service-module wlan-ap 0 session** コマンドを EXEC プロンプトで入力します。このコマンドを入力すると、自動的に IOS の **dot11 radio** レベルにスキップします。

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間のセッションを終了するには、次の 2 つの手順を両方実行します。

ワイヤレス デバイス

1. **Ctrl+Shift+6、x**

ルータ

2. **disconnect**
3. Enter キーを 2 回押します。

無線環境の設定

（注） 初めて自律無線デバイスを設定する場合、まずルータとアクセス ポイント間でコンフィギュレーション セッションを開始してから、基本となる無線設定のコンフィギュレーションを実行します。「無線コンフィギュレーション セッションの開始」（P.1）を参照してください。

適切なソフトウェア ツールを使用して無線デバイスを設定します。

- ユニファイド ソフトウェア：「Cisco Express 設定」（P.4）
- 自律ソフトウェア：「Cisco IOS CLI」（P.4）

Cisco Express 設定

Cisco Unified ワイヤレス デバイスを設定するには、Web ブラウザの Cisco Express 設定ツールを使用します。

ステップ 1 コンソールと無線デバイス間に接続を確立し、**show interface bvi1 IOS** コマンドを入力して、BVI IP アドレスを取得します。

ステップ 2 ブラウザ ウィンドウを開き、ブラウザウィンドウ アドレス ラインに BVI IP アドレスを入力します。Enter キーを押すと 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 CLI

自律無線デバイスの設定は、まずルータとアクセス ポイント間に接続を確立し、その後 Cisco IOS CLI ツールを使用して行います。

- 「無線の設定」（P.4）
- 「無線セキュリティ設定の実行」（P.5）
- 「無線 QoS の設定」（P.8）（任意）
- 「ホット スタンバイ モードでのアクセス ポイントの設定」（P.9）（任意）

無線の設定

無線デバイスに無線パラメータを設定し、シグナルを発信します。特定の設定手順については、第 3 章「無線の設定」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

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。同じアクセス ポイントで別の種類のクライアント デバイスをサポートしたい場合、複数の SSID を設定します。

無線クライアント デバイスがアクセス ポイントを通してユーザのネットワーク上で通信を行うためには、オープン キーまたは共有キーを使ってアクセス ポイントに認証する必要があります。セキュリティを最も高く設定するには、MAC アドレスか Extensible Authentication Protocol（EAP; 拡張認証プロトコル）認証を使用して、ユーザのネットワークに対してもクライアント デバイスを認証する必要があります。これらの認証の種類はいずれも、ユーザのネットワークの認証サーバによって決まります。

認証タイプを選択するには、Cisco.com の『*Authentication Types for Wireless Devices*』（http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/SecurityAuthenticationTypes.html）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、Cisco.com の『*RADIUS and TACACS+ Servers in a Wireless Environment*』（http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/SecurityRadiusTacacs_1.html）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

アクセス ポイントをローカル認証サーバとして動作するよう設定することで、WAN リンク障害またはサーバ障害が発生したときに、ローカル認証サービスかバックアップ認証サービスを提供できます。アクセス ポイントでは、Lightweight Extensible Authentication Protocol（LEAP; Lightweight 拡張認証プロトコル）、Extensible Authentication Protocol-Flexible Authentication Secure Tunneling（EAP-FAST）あるいは MAC ベース認証を使用して無線クライアント デバイスを 50 まで認証できます。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。

ローカル認証アクセス ポイントは、クライアント ユーザ名およびパスワードとともに手動で設定します。これは、そのデータベースと Remote Authentication Dial-In User Service（RADIUS; リモート認証ダイヤルイン ユーザ サービス）サーバが同期しないためです。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。

この役割のワイヤレス デバイス設定の詳細については、Cisco.com の『*Using the Access Point as a Local Authenticator*』（http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/SecurityLocalAuthent.html）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。

TKIP を含んでいる暗号化スイートにより、ユーザの無線 LAN に最高のセキュリティを提供できます。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、『*Configuring WEP and Cipher Suites*』（http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/SecurityCipherSuitesWEP.html）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.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、1 つのブリッジング ドメインによって接続された、ホストかネットワーク機器（ブリッジやルータなど）のいずれかに該当する複数のエンド システムで構成されます。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。

ワイヤレス VLAN アーキテクチャの詳細については、Cisco.com の『*Configuring Wireless VLANs*』（http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/wireless_vlans.html）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

SSID は、ワイヤレス デバイス上に 16 個まで設定できます。これはアクセス ポイントのロール内の作業です。また各 SSID に一意のパラメータ セットを設定することもできます。たとえば、1 個の SSID を使用してゲストにネットワークへの制限されたアクセス権を付与し、それとは別の SSID を使用して認証済みのユーザにセキュアなデータへのアクセス権を付与できます。

複数の SSID を作成する方法の詳細については、Cisco.com の『*Service Set Identifiers*』（http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/ServiceSetID.html）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 2.4 GHz 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 をディセーブルにした状態で SSID を静的な WEP とともに作成する場合、追加 SSID は、Wi-Fi 保護アクセス（WPA）認証とともに作成できません。その SSID では別の暗号化設定を使用しているためです。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 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 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
No Security	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 スペースで使用されている SSID だけに使用し、ネットワークへのアクセスを制限している VLAN に割り当てる必要があります。	なし。
Static WEP Key	このオプションは、「セキュリティなし」よりは安全です。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。設定手順については、Cisco.com の『*Cipher Suites and WEP*』（http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/SecurityCipherSuitesWEP.html）を参照してください。 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。 指示については Cisco.com の『*Using the Access Point as a Local Authenticator*』（http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/SecurityLocalAuthent.html）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 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 認証[1]	このオプションを選択すると、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。 この設定では、暗号化必須、WEP、Open 認証 + EAP、ネットワーク EAP 認証、キー管理なし、RADIUS サーバ認証ポート 1645 を選択します。 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がありません。	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]	このオプションを選択すると、データベースに対する認証を（認証サーバを通して）済ませたユーザは無線でアクセスできるようになります。その後、ユーザの IP トラフィックは WEP で使用されていたアルゴリズムよりも強いアルゴリズムで暗号化されます。 この設定では、暗号化、TKIP[10]、オープン認証 + EAP、ネットワーク EAP 認証、必須キー管理 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 を使用してアソシエートするクライアント 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 = 拡張認証プロトコル - トランスポート層セキュリティ
5. EAP-FAST = 拡張認証プロトコル - セキュアトンネル経由の柔軟な認証
6. EAP-TTLS = 拡張認証プロトコル - トンネル方式トランスポート層セキュリティ
7. EAP-GTC = 拡張認証プロトコル - 汎用トークン カード
8. EAP-SIM = 拡張認証プロトコル - 加入者認証モジュール
9. WA = Wi-Fi 保護アクセス
10. TKIP = Temporal Key Integrity Protocol

無線 QoS の設定

Quality of Service（QoS）を設定することで、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、パケットを送信します。ワイヤレス デバイスに Quality of Service（QoS）を設定するには、『*Quality of Service in a Wireless Environment*』（http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/QualityOfService.html）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、それをモニタします（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モニタ対象のアクセス ポイントとアソシエートします。またモニタ対象のアクセス 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、Cisco.com の『*Hot Standby Access Point*』（http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/RolesHotStandby.html）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

Cisco Unified モードでアクセス ポイントを動作させるには、以下の手順（概略）に従ってソフトウェアをアップグレードします。

- 「アップグレードの準備」（P.9）
- 「アップグレードの実行」（P.10）
- 「アクセス ポイントへのソフトウェアのダウンロード」（P.11）
- 「アクセス ポイントでのソフトウェア リカバリ」（P.11）

ソフトウェア前提条件

- IP ベース フィーチャ セットおよび Cisco IOS Release 15.0(1)M がルータにより動作している場合、Cisco 1941W ISR が、Cisco Unified ソフトウェアへのアップグレードに適当です。
- Cisco Unified アーキテクチャに組み込まれたアクセス ポイントを使用するには、Cisco wireless LAN controller（WLC）がバージョン 5.1 以降で動作している必要があります。

アップグレードの準備

以下の作業を行い、アップグレードの準備をします。

- 「アクセス ポイントの IP アドレスの保護」（P.10）
- 「アップグレードに備えて」（P.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 アドレスを保護して WLC との通信、起動時におけるユニファイド イメージのダウンロードを可能にします。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、Cisco.com の『*Cisco Wireless LAN Configuration Guide*』（http://www.cisco.com/en/US/docs/wireless/controller/4.0/configuration/guide/ccfig40.html）を参照してください。

アップグレードに備えて

次のステップを実行します。

1. ルータから WLC サーバに ping を実行し、接続を確認します。
2. **service-module wlan-ap 0 session** コマンドを実行し、アクセス ポイントとのセッションを確立します。
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。
4. アクセス ポイントで **show boot** コマンドを入力して、モード設定がイネーブルになっているか確認します。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

Unified ソフトウェアへのアップグレードは、以下の手順で実行します。

ステップ 1　**service-module wlan-ap 0 bootimage unified** コマンドを発行してアクセス ポイント起動イメージをユニファイド アップグレード イメージに変更します。これは*リカバリ イメージ*とも呼ばれます。

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

（注）　**service-module wlan-ap 0 bootimage unified** コマンドがうまく機能しない場合、ソフトウェア ライセンスが現在も適切なものであるかチェックします。

アクセス ポイント コンソールで **show boot** コマンドを使用して、アクセス ポイントの起動イメージ パスを特定します。

```
autonomous-AP# show boot
BOOT path-list:      flash:/ap801-rcvk9w8-mx/ap801-rcvk9w8-mx
```

ステップ 2 **service-module wlan-ap 0 reload** コマンドを発行して正常にシャットダウンし、次にアクセス ポイントを再起動してアップグレード プロセスを完了します。アクセス ポイントでセッションを開始して、アップグレード プロセスを監視します。

Web ベースのコンフィギュレーション ページを使用した無線デバイス設定の詳細については、「Cisco Express 設定」（P.4）を参照してください。

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. アクセス ポイントを、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しようとしたのですが失敗しました。リカバリ モードでスタックが発生したようです。どうすればいいでしょうか。

A. 以下の項目をチェックしてください。

- IP アドレスが、WLC と同一のサブネット上にある BVI インターフェイス上にあるか。
- ルータまたはアクセス ポイントから WLC を ping して、接続状態を確認できるか。
- アクセス ポイントのデータおよび時間が現在に設定されているか。**show clock** コマンドを使用してこれらの情報を確認します。

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 ポイントがリカバリ モードでスタックしているときは、**service-module wlan-ap0 reset bootloader** コマンドを使用してアクセス ポイントをブートローダに戻し、手動でイメージをリカバリしてください。

アクセス ポイントへのソフトウェアのダウンロード

service-module wlan-ap0 bootimage autonomous コマンドを使用してアクセス ポイントをリセットし、再起動して直前の自律イメージに戻ります。**service-module wlan-ap 0 reload** コマンドを使用してアクセス ポイントを自律ソフトウェア イメージとともに再ロードします。

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、**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当たっては、十分注意してください。このコマンドは、シャットダウンまたは障害が発生した状態から回復する場合にだけ使用します。

関連資料

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

- 「独立したマニュアル」—表 2
- 「Unified 関連のマニュアル」—表 3

表 2　　独立したマニュアル

ネットワーク デザイン	リンク	説明
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。
設定	**リンク**	
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	**リンク**	
『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。
『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 と TACACS+ は AAA を通じて効率化され、AAA コマンド以外では有効に設定できません。
『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。ローカル認証を担当するアクセス ポイントは、LEAP、EAP-FAST および MAC ベースの認証を最大 50 個のクライアント デバイスに対して実行します。
『Cipher Suites and WEP』	http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/SecurityCipherSuitesWEP.html	WPA[3] および CCKM[4]、WEP[5]、および WEP 機能（AES[6]、MIC[7]、TKIP[8]、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。
『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。
『Configuring Wireless VLANs』	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[9] 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。
管理	**リンク**	**説明**
アクセス ポイントの管理	「無線デバイスの管理」	ネットワークのワイヤレス デバイスを管理する方法について説明します。

表 2　独立したマニュアル （続き）

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[10] 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、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. WPA = Wireless Protected Access（ワイヤレス保護アクセス）
4. CCKM = Cisco Centralized Key Management
5. WEP = Wired Equivalent Privacy（有線と同等のプライバシー）
6. AES = Advanced Encryption Standard
7. MIC = Message Integrity Check
8. TKIP = Temporal Key Integrity Protocol
9. SSID = Service Set Identifiers
10. QoS = Quality of Service

表 3　Unified 関連のマニュアル

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
『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