概要

この章では、Cisco Wireless LAN Solution のコンポーネントと特長について説明します。この章の内容は、次のとおりです。

Cisco Wireless LAN Solution の概要

Cisco Wireless LAN Solution は、企業およびサービス プロバイダーに 802.11 無線ネットワーキング ソリューションを提供するように設計されています。Cisco Wireless LAN Solution を使用すると、大規模無線 LAN の展開および管理が簡素化され、他に類のないクラス最高のセキュリティ インフラストラクチャを実現できます。オペレーティング システムによって、すべてのデータ クライアント、通信、およびシステム管理機能の管理、Radio Resource Management（RRM）機能の実行、オペレーティング システム Security ソリューションを使用したシステム全体のモビリティ ポリシーの管理、およびオペレーティング システム Security フレームワークを使用したすべてのセキュリティ機能の調整が行われます。

Cisco Wireless LAN Solution は、Cisco Wireless LAN Controller とそのアソシエートされている Lightweight アクセス ポイントから構成されます。これらは、オペレーティング システムで制御され、次のいずれかまたはすべてのオペレーティング システム ユーザ インターフェイスによってすべて同時に管理されます。

- Cisco Wireless LAN Controller によってホストされる、HTTP または HTTPS あるいはその両方の全機能を備えた Web ユーザ インターフェイス。個々のコントローラを設定して監視するときに使用できます。「Web ユーザ インターフェイスと CLI」の項（P.1-53）を参照してください。
- 全機能を備えた Command-line Interface（CLI; コマンドライン インターフェイス）。個々の Cisco Wireless LAN Controller を設定して監視するときに使用できます。「Web ユーザ インターフェイスと CLI」の項（P.1-53）を参照してください。
- 「Cisco Wireless Control System」の項（P.1-54）では、1 つ以上の Cisco Wireless LAN Controller とアソシエート先のアクセス ポイントを設定し監視するために使用する、Cisco Wireless Control System（WCS）について説明しています。WCS には、大規模システムの監視と制御を容易にするツールが備わっています。WCS は、Windows 2000、Windows Server 2003、および Red Hat Enterprise Linux ES サーバ上で動作します。
- 業界標準の SNMP V1、V2c、および V3 インターフェイスであれば、SNMP 準拠のサードパーティ製ネットワーク管理システムと併用できます。

Cisco Wireless LAN Solution は、クライアント データ サービス、クライアントの監視と制御、およびすべての不正なアクセス ポイントの検出、監視、および阻止機能をサポートします。Cisco Wireless LAN Solution では、Lightweight アクセス ポイント、Cisco Wireless LAN Controller、およびオプションの Cisco WCS を使用して、企業とサービス プロバイダーに無線サービスを提供します。

Cisco WCS アプリケーションには次の 2 つのバージョンがあります。

- Cisco WCS Base：最も近い Lightweight アクセス ポイントに対する、クライアント、不正なアクセス ポイント、不正なアクセス ポイント クライアント、Radio Frequency ID（RFID; 無線周波数 ID）タグ ロケーションもサポートします。
- Cisco WCS Location：10m 以内のクライアント、不正なアクセス ポイント、不正なアクセス ポイント クライアント、RFID タグ ロケーションもサポートします。

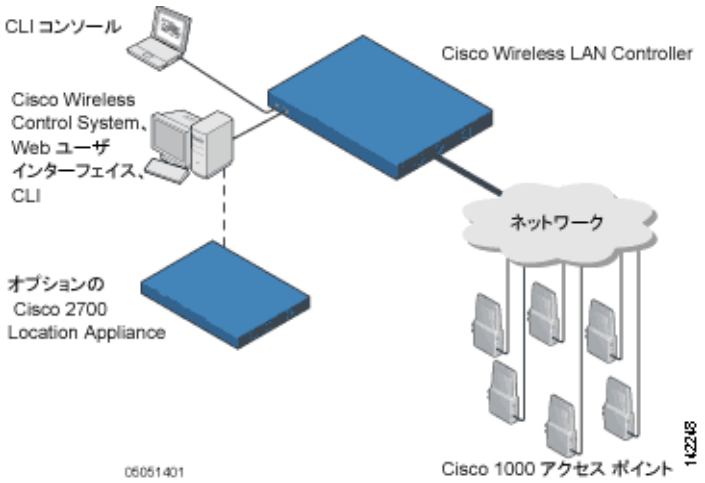
詳細は、「Cisco WCS Base」の項（P.1-55）と「Cisco WCS Location」の項（P.1-56）を参照してください。

Cisco WCS Location を使用している場合、Cisco Wireless LAN Solution のエンド ユーザは、Cisco 2700 シリーズ Location Appliance を展開することもできます。これについては、第 10 章「Location Appliance を設定および使用する方法」を参照してください。Location Appliance は、履歴ロケーション データを計算、収集、および格納し、このデータを Cisco WCS に表示することにより、高精度な組み込み Cisco WCS Location 機能を拡張します。この場合、Location Appliance は 1 つまたは複数の Cisco WCS サーバに対するサーバとして機能し、そのアソシエートされているコントローラのデータを収集、格納、および受け渡しします。

（注）　本書では、Cisco Wireless LAN Controller 全体を説明します。特に記載されていない限り、本書の説明は、Cisco 2000 シリーズ Wireless LAN Controller、Cisco 4100 シリーズ Wireless LAN Controller、Cisco 4400 シリーズ Wireless LAN Controller などの、すべての Cisco Wireless LAN Controller に適用されます。

図 1-1 は、複数のフロアとビルディングに同時に展開できる Cisco Wireless LAN Solution コンポーネントを示しています。

図 1-1　Cisco WLAN Solution コンポーネント



シングルコントローラ展開

スタンドアロンの Cisco Wireless LAN Controller では、複数のフロアとビルディングに配置されている Lightweight アクセス ポイントを同時にサポートすることができます。サポートされている機能は、次のとおりです。

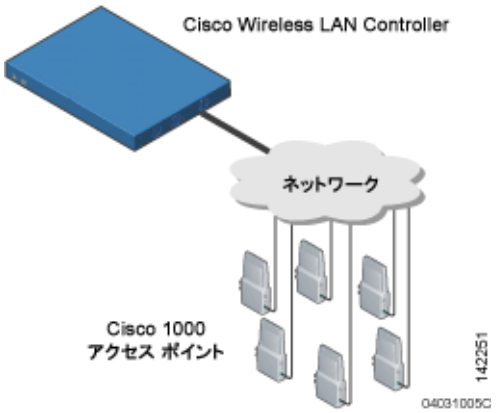
- ネットワークに追加された Lightweight アクセス ポイントの自動検出と自動設定。
- Lightweight アクセス ポイントの完全制御。
- 最大 16 までの Lightweight アクセス ポイント無線 LAN（SSID）ポリシーの完全制御。
- ネットワークを介したコントローラへの Lightweight アクセス ポイントの接続。ネットワーク機器では、アクセス ポイントに Power over Ethernet を提供してもしなくてもかまいません。

一部の Cisco Wireless LAN Controller では、1 つのネットワークに障害が発生した場合、冗長ギガビット イーサネット接続を使用してこれを迂回します。常に 1 つの冗長ギガビット イーサネット接続がアクティブで、もう一方はパッシブです。ネットワークに障害が発生すると、アクティブな接続がパッシブになり、パッシブな接続がアクティブになります。

（注）　一部のコントローラは、複数の物理ポートを使用して、ネットワークの複数のサブネットに接続できます。この機能は、Cisco WLAN Solution オペレータが複数の VLAN を別々のサブネットに限定する場合などに役立ちます。

図 1-2 は、一般的なシングルコントローラ展開を示しています。

図 1-2　シングルコントローラ展開



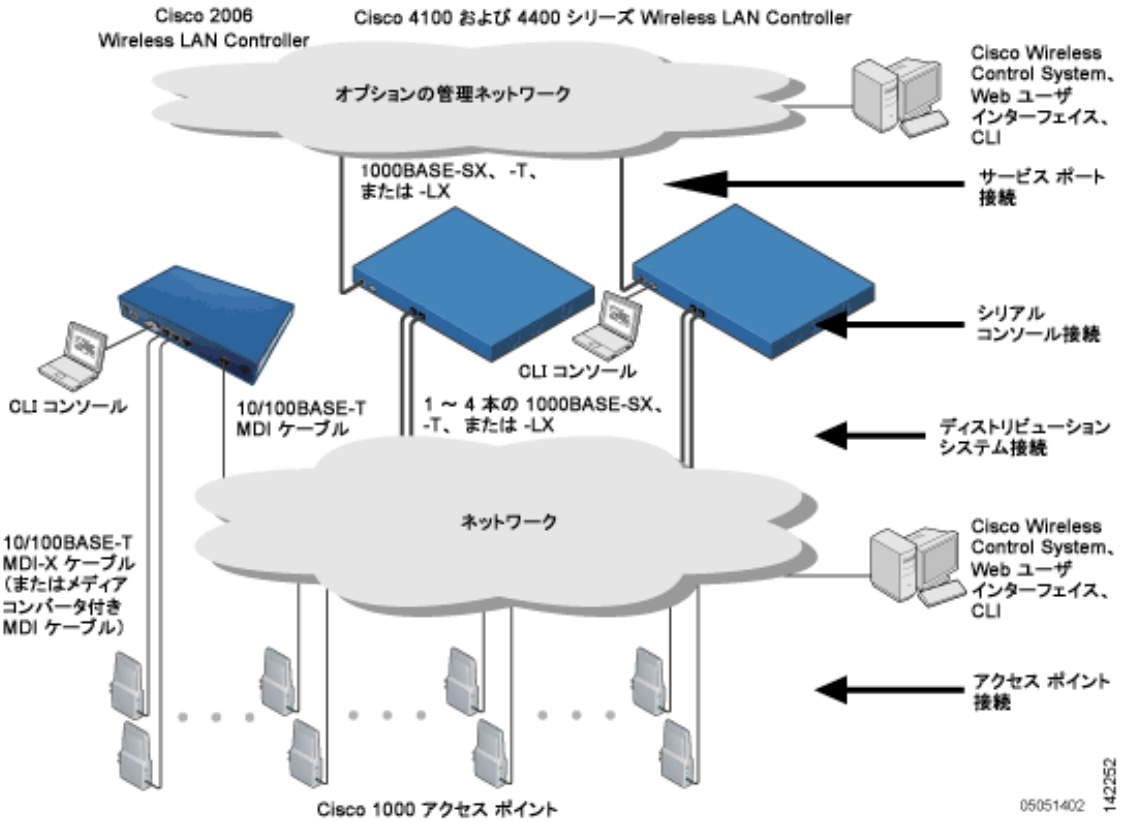
マルチコントローラ展開

すべての Cisco Wireless LAN Controller は、複数のフロアとビルディングに配置されている Lightweight アクセス ポイントを同時にサポートできます。ただし、Cisco Wireless LAN Solution の全機能が実現されるのは、複数のコントローラが使用されている場合です。マルチ Cisco Wireless LAN Controller システムには、次の追加の機能があります。

- ネットワークに追加された Cisco Wireless LAN Controller の RF パラメータの自動検出と自動設定。
- 同一コントローラ（レイヤ 2）でのローミングとサブネット間（レイヤ 3）でのローミング。
- 未使用ポートがある任意の冗長コントローラへのアクセス　ポイントの自動フェールオーバー（「Cisco Wireless LAN Controller のフェールオーバーの保護」の項（P.1-33）を参照）。

次の図は、一般的なマルチコントローラ展開を示しています。また、この図では、オプションの専用管理ネットワークと、ネットワークとコントローラ間の 3 つの物理接続タイプも示しています。

図 1-3　一般的なマルチコントローラ展開



オペレーティング システム ソフトウェア

オペレーティング システム ソフトウェアは、Cisco Wireless LAN Controller と Cisco 1000 シリーズ Lightweight アクセス ポイントを制御します。このソフトウェアには、オペレーティング システムのセキュリティ機能と Radio Resource Management（RRM）機能がすべて組み込まれています。

オペレーティング システムのセキュリティ

オペレーティング システムのセキュリティ機能により、レイヤ 1、レイヤ 2、およびレイヤ 3 のセキュリティ コンポーネントを、Cisco WLAN Solution 全体の簡単な Policy Manager に組み込みます。この Policy Manager は、最大 16 の無線 LAN それぞれに対して、独立したセキュリティ ポリシーを作成する管理ツールです（「Cisco WLAN Solution 無線 LAN」の項（P.1-18）を参照してください）。

802.11 静的 WEP の脆弱性は、次のような強化された業界標準のセキュリティ ソリューションを使用することで克服できます。

- Extensible Authentication Protocol（EAP; 拡張認証プロトコル）使用による 802.1X 動的キー。
- Wi-Fi Protected Access（WPA）動的キー。Cisco WLAN Solution の WPA 実装には、次のものが含まれます。
  - Temporal Key Integrity Protocol（TKIP）+ Message Integrity Code Checksum（Michael）動的キー、または
  - WEP キー（事前共有キーのパスフレーズの有無を問わない）
- RSN（事前共有キーの有無を問わない）
- Cranite FIPS140-2 準拠パススルー
- Fortress FIPS140-2 準拠パススルー
- オプションの MAC フィルタリング

WEP 問題は、次のような業界標準のレイヤ 3 セキュリティ ソリューションを使用すると、さらに進んだ解決が可能です。

- 終端されるパススルー VPN
- 終端されるパススルー Layer Two Tunneling Protocol（L2TP; レイヤ 2 トンネリング プロトコル）。L2TP は IP Security（IPSec; IP セキュリティ）プロトコルを使用します。
- 終端されるパススルー IPSec プロトコル。終端される Cisco WLAN Solution の IPSec 実装には、次のものが含まれます。
  - Internet Key Exchange（IKE; インターネット キー エクスチェンジ）
  - Diffie-Hellman（D-H; ディッフィーヘルマン）グループ
  - ANSI X.3.92 Data Encryption Standard（データ暗号規格 ; ANSI X.3.92 データ暗号化規格）、ANSI X9.52-1998 Data Encryption Standard（3DES; ANSI X9.52-1998 データ暗号化規格）、または Advanced Encryption Standard/Cipher Block Chaining（AES/CBC; 高度暗号化規格 / 暗号ブロック連鎖）の 3 つのオプション レベルの暗号化。

  Cisco WLAN Solution IPSec 実装には、次のアルゴリズムを使用した業界標準認証も含まれます。
  - Message Digest 5（MD5; メッセージ ダイジェスト 5）アルゴリズム
  - Secure Hash Algorithm-1（SHA-1）
- Cisco Wireless LAN Solution では、ローカルおよび RADIUS Media Access Control（RADIUS MAC; RADIUS メディア アクセス制御）アドレス フィルタリングがサポートされています。
- Cisco Wireless LAN Solution は、ローカルおよび RADIUS ユーザ / パスワード認証をサポートします。

- また、Cisco Wireless LAN Solution は、手動および自動による無効化を使用して、ネットワーク サービスへのアクセスをブロックします。手動で無効化するときは、オペレータがクライアントの MAC アドレスを使用してアクセスをブロックします。自動による無効化は常にアクティブであり、クライアントが一定の回数の認証を繰り返し試みて失敗すると、オペレーティング システム ソフトウェアにより、オペレータが設定した時間だけネットワーク サービスへのアクセスが自動的にブロックされます。この無効化を使用すると、Brute-Force ログイン アタックを阻止できます。

これらとその他のセキュリティ機能は、業界標準の許可および認証方式を使用して、ビジネスクリティカルな無線 LAN トラフィックに対する最高のセキュリティを実現します。

Cisco WLAN Solution の有線セキュリティ

従来のアクセス ポイント ベンダーの多くは、「オペレーティング システムのセキュリティ」の項（P.1-6）で説明したような無線インターフェイスのセキュリティ対策に集中しています。ただし、オペレーティング システムには、Cisco Wireless LAN Controller サービス インターフェイス、アクセス ポイントに対する Cisco Wireless LAN Controller のセキュリティ、デバイス サービシング時とクライアントのローミング時の Cisco Wireless LAN Controller 間通信のセキュリティを確保するためのセキュリティ機能が組み込まれています。

製造されるすべての Cisco Wireless LAN Controller と Cisco 1000 シリーズ Lightweight アクセス ポイントには、固有の署名付き X.509 証明書が添付されます。この証明書は、デバイス間の IPSec トンネルの認証に使用されます。認証された IPSec トンネルにより、モビリティおよびデバイス サービシングでの安全な通信が保証されます。

また、Cisco Wireless LAN Controller と Cisco 1000 シリーズ Lightweight アクセス ポイントは、署名付き証明書を使用して、ダウンロードしたコードを読み込む前に確認することで、ハッカーによって Cisco Wireless LAN Controller や Cisco 1000 シリーズ Lightweight アクセス ポイントに悪意のあるコードがダウンロードされないようにしています。

レイヤ 2 およびレイヤ 3 の Lightweight Access Point protocol（LWAPP）動作

Cisco Wireless LAN Controller と Cisco 1000 シリーズ Lightweight アクセス ポイント間の LWAPP 通信は、ISO データリンク レイヤ 2 またはネットワーク レイヤ 3 で実行されます。

動作上の要件

レイヤ 2 LWAPP 通信の要件として、Cisco Wireless LAN Controller と Cisco 1000 シリーズ Lightweight アクセス ポイントは同一サブネット上のレイヤ 2 デバイスを使用して相互接続されている必要があります。これが、Cisco Wireless LAN Solution のデフォルトの操作モードです。Cisco Wireless LAN Controller と Cisco 1000 シリーズ Lightweight アクセス ポイントが異なるサブネット上にあるときは、デバイスはレイヤ 3 モードで動作しなければならないことに注意してください。

レイヤ 3 LWAPP 通信の要件として、Cisco Wireless LAN Controller と Cisco 1000 シリーズ Lightweight アクセス ポイントは、同一サブネットではレイヤ 2 デバイスを使用して接続し、異なるサブネット間ではレイヤ 3 デバイスを使用して接続する必要があります。

1 つのモビリティ グループに含まれる Cisco Wireless LAN Controller はすべて、同じ LWAPP レイヤ 2 またはレイヤ 3 モードを使用する必要があり、使用しないと、モビリティ ソフトウェアのアルゴリズムが無効になります。

設定上の要件

レイヤ 2 モードで Cisco Wireless LAN Solution を稼働している場合は、レイヤ 2 通信を制御するよう管理インターフェイスを設定する必要があります。

レイヤ 3 モードで Cisco Wireless LAN Solution を稼働している場合は、レイヤ 2 通信を制御するよう管理インターフェイスを設定し、Cisco 1000 シリーズ Lightweight アクセス ポイントと Cisco Wireless LAN Controller 間のレイヤ 3 通信を制御するよう AP マネージャ インターフェイスを設定する必要があります。

Radio Resource Management（RRM）

Radio Resource Management（RRM）を使用すると、Cisco Wireless LAN Controller は、次の情報についてそのアソシエートされている Cisco 1000 シリーズ Lightweight アクセス ポイントを継続的に監視することができます。

- トラフィックの負荷：トラフィックの送受信に使用される帯域幅の合計量。これにより、無線 LAN 管理者は、クライアントの需要よりも先に、ネットワークの成長を追跡して計画を立てることができます。
- 干渉：他の 802.11 発信元から送られてくるトラフィック量。
- ノイズ：現在割り当てられているチャネルと干渉している 802.11 以外のノイズ量。
- カバレッジ：すべてのクライアントの Received Signal Strength Indicator（RSSI; 受信信号強度インジケータ）と Signal to Noise Ratio（SNR; 信号対雑音比）。
- 近くにあるアクセス ポイント。

RRM は、収集した情報を使用して、オペレータが定義した制限内で、最も効率が良くなるように 802.11 RF ネットワークを定期的に再設定できます。そのために、RRM では次の処理を行います。

- 同じ Cisco Wireless LAN Controller 内と、複数の Cisco Wireless LAN Controller 間の双方において、動的なチャネルの再割り当てを行い、キャパシティを増大させてパフォーマンスを向上させます。
- 同じ Cisco Wireless LAN Controller 内と、複数の Cisco Wireless LAN Controller 間の双方において、送信電力を調整して、カバレッジとキャパシティのバランスを取ります。
- オペレータが近くの Cisco 1000 シリーズ Lightweight アクセス ポイントをグループに割り当てて、Radio Resource Management アルゴリズムの処理を効率的に行えるようにします。
- 各 Cisco Wireless LAN Controller にレポートするグループ化された Cisco 1000 シリーズ Lightweight アクセス ポイント間で新しいクライアントをロード バランシングします。RRM は自動的に一部の登録者を近くのアクセス ポイントにアソシエートして、すべてのクライアントのスループットを高めることができるので、多数のクライアントが 1 個所にコンバージしている場合に（会議室や講堂など）、この処理が特に重要になります。
- 新しい Cisco 1000 シリーズ Lightweight アクセス ポイント がネットワークに追加されると、自動的に検出して設定を行います。RRM は、アソシエートされている Cisco 1000 シリーズ Lightweight アクセス ポイントを自動的に分散して、カバレッジとキャパシティを最大限に活用します。
- 新しい Cisco Wireless LAN Controller がネットワークに追加されると、自動的に検出して設定を行います。RRM は、アソシエートされている Cisco 1000 シリーズ Lightweight アクセス ポイントを自動的に分散して、カバレッジとキャパシティを最大限に活用します。
- クライアントが非常に低い信号強度で Cisco 1000 シリーズ Lightweight アクセス ポイントに常時接続しているカバレッジ ホールを検出してレポートします。
- オペレータが定義したモビリティ グループ内で、自動的に Cisco Wireless LAN Controller グループを定義します。

このように、RRM ソリューションを使用すると、オペレータは、面倒な履歴データの解釈と個々の Cisco 1000 シリーズ IEEE 802.11a/b/g Lightweight アクセス ポイントの再設定にかかる負担を避けることができます。RRM の電力制御機能によってクライアントの要望が満たされ、Cisco 1000 シリーズ Lightweight アクセス ポイントを追加（または再配置）する必要があることがカバレッジ ホール検出機能によってオペレータにアラートされます。

RRM では展開されているネットワーク 802.11a および 802.11b/802.11g のそれぞれに対して、別々の監視と制御を使用します。また、RRM は自動的に有効になりますが、個々の Cisco 1000 シリーズ Lightweight アクセス ポイントについてカスタマイズしたり無効にしたりすることも可能です。

さらに、簡単な手動による設定を希望するオペレータに対して、RRM では最適な Cisco Radio 設定を推奨し、これらの設定をオペレータ コマンドに割り当てることができます。

RRM の制御によって、最適なキャパシティ、パフォーマンス、および信頼性を備えたネットワークが構築されます。また、RRM 機能により、オペレータは、一過性でトラブルシューティングが困難なノイズおよび干渉問題の発生を確認するために常時ネットワークを監視する必要から開放されます。最終的に、RRM の制御によって、クライアントは Cisco WLAN Solution 802.11 ネットワーク経由による、シームレスで円滑な接続を利用できるようになります。

Cisco Wireless LAN Controller

Cisco 1000 シリーズ Lightweight アクセス ポイントをマルチ Cisco Wireless LAN Controller 展開ネットワークに追加する場合、すべての Cisco 1000 シリーズ Lightweight アクセス ポイントを、同一サブネット上の 1 つのマスター コントローラにアソシエートすると便利です。こうすると、オペレータは複数のコントローラにログインして、新たに追加された Cisco 1000 シリーズ Lightweight アクセス ポイントがアソシエートしているコントローラを検索する必要はありません。

Lightweight アクセス ポイントを追加するとき、各サブネット内の 1 つのコントローラをマスター コントローラとして割り当てることができます。同一サブネット上のマスター コントローラがアクティブである限り、プライマリ、セカンダリ、ターシャリ コントローラが割り当てられていない新しいアクセス ポイントはすべて、マスター Cisco Wireless LAN Controller とのアソシエートを自動的に試みます。このプロセスについては、「Cisco Wireless LAN Controller のフェールオーバーの保護」の項（P.1-33）を参照してください。

オペレータは、WCS Web ユーザ インターフェイスを使用して、マスター コントローラを監視し、アクセス ポイントがマスター コントローラにアソシエートするのを確認できます。そして、オペレータは、アクセス ポイント設定を確認して、プライマリ、セカンダリ、ターシャリ コントローラをアクセス ポイントに割り当てて、プライマリ、セカンダリ、またはターシャリ コントローラに再アソシエートするように、アクセス ポイントを再度ブートします。

（注）　Lightweight アクセス ポイントでは、プライマリ、セカンダリ、またはターシャリ コントローラが割り当てられていない場合、リブート時には必ずマスター コントローラが最初に検索されます。マスター コントローラ経由による Lightweight アクセス ポイントを追加したら、プライマリ、セカンダリ、またはターシャリ コントローラを各アクセス ポイントに割り当ててください。シスコでは、初期設定後にすべてのコントローラのマスター設定を無効にすることを推奨しています。

プライマリ、セカンダリ、ターシャリ コントローラ

マルチコントローラ ネットワークでは、Lightweight アクセス ポイントは同じサブネット上の任意のコントローラにアソシエートできます。確実にすべてのアクセス ポイントを特定のコントローラにアソシエートするために、オペレータは、プライマリ、セカンダリ、およびターシャリ コントローラをアクセス ポイントに割り当てることができます。

アクセス ポイントはネットワークに追加されると、プライマリ、セカンダリ、およびターシャリ コントローラをまず検索してから、使用可能なアクセス ポイント ポートを持つ、最も負荷の少ないコントローラを検索します。詳細は、「Cisco Wireless LAN Controller のフェールオーバーの保護」の項（P.1-33）を参照してください。

クライアント ローミング

Cisco Wireless LAN Solution は、同じ Cisco Wireless LAN Controller で管理されている Cisco 1000 シリーズ Lightweight アクセス ポイント間、同一サブネット上の同じ Cisco WLAN Solution モビリティ グループに属している Cisco Wireless LAN Controller 間、および異なるサブネット上の同じモビリティ グループに属しているコントローラ間での、シームレスなクライアント ローミングをサポートします。

同一コントローラ（レイヤ 2）でのローミング

すべての Cisco Wireless LAN Controller は、同じコントローラで管理されているアクセス ポイント間での同一コントローラ クライアント ローミングをサポートします。セッションはそのまま持続され、クライアントは同じ DHCP 割り当てまたはクライアント割り当て IP アドレスを引き続き使用するため、このローミングはクライアントには透過的に行われます。コントローラには、リレー機能を備えている DHCP 機能があります。同一コントローラ ローミングは、シングルコントローラ展開とマルチコントローラ展開でサポートされています。

コントローラ間（レイヤ 2）ローミング

同様に、マルチコントローラ展開の Cisco Wireless LAN Solution では、同一モビリティ グループ内および同一サブネット上のコントローラによって管理されるアクセス ポイント間のクライアント ローミングをサポートします。セッションがアクティブである限り、セッションはそのまま持続され、コントローラ間のトンネルによって、クライアントは同じ DHCP 割り当てまたはクライアント割り当て IP アドレスを引き続き使用できるため、このローミングもクライアントには透過的に行われます。クライアントが 0.0.0.0 というクライアント IP アドレス、または 169.254.*.* というクライアント 自動 IP アドレスを持つ DHCP Discover を送信するか、オペレータが設定したセッションのタイムアウトが過ぎた場合には、トンネルがティアダウンし、クライアントは再認証を行わなければなりません。

リモート ロケーションにある Cisco 1030 リモート エッジ Lightweight アクセス ポイントがローミングをサポートするには、同一サブネット上になければならないことに注意してください。

サブネット間（レイヤ 3）でのローミング

同様に、マルチコントローラ展開の Cisco Wireless LAN Solution では、異なるサブネット上の同一モビリティ グループ内のコントローラによって管理されるアクセス ポイント間のクライアント ローミングをサポートします。セッションがアクティブである限り、セッションはそのまま持続され、コントローラ間のトンネルによって、クライアントは同じ DHCP 割り当てまたはクライアント割り当て IP アドレスを引き続き使用できるため、このローミングはクライアントには透過的に行われます。クライアントが 0.0.0.0 というクライアント IP アドレス、または 169.254.*.* というクライアント 自動 IP アドレスを持つ DHCP Discover を送信するか、オペレータが設定したセッションのタイムアウトが過ぎた場合には、トンネルがティアダウンし、クライアントは再認証を行わなければなりません。

リモート ロケーションにある Cisco 1030 リモート エッジ Lightweight アクセス ポイントがローミングをサポートするには、同一サブネット上になければならないことに注意してください。

特殊なケース：VoIP による通話ローミング

802.11 VoIP 通話は、積極的に最強の RF 信号とのアソシエーションを見つけ出すことで、最適な QoS（Quality of Service）と最高のスループットを約束します。Cisco Wireless LAN Solution の平均ハンドオーバー遅延時間は 9 ミリ秒以下なので、20 ミリ秒という最短の VoIP 通話要件や、ローミング ハンドオーバーの遅延時間の短縮は簡単に実現されます。

この短い遅延時間は、個々のアクセス ポイントにローミング ハンドオーバーのネゴシエートを許可せずに、Cisco Wireless LAN Controller によって制御されます。

Cisco Wireless LAN Solution では、Cisco Wireless LAN Controller が同一のモビリティ グループに属している場合、異なるサブネット上のコントローラによって管理される Cisco 1000 シリーズ Lightweight アクセス ポイント間での 802.11 VoIP 通話ローミングをサポートします。セッションがアクティブである限り、セッションはそのまま持続され、コントローラ間のトンネルによって、VoIP 通話は同じ DHCP 割り当て IP アドレスを引き続き使用できるため、このローミングはクライアントには透過的に行われます。クライアントが 0.0.0.0 という VoIP 通話 IP アドレス、または 169.254.*.* という VoIP 通話自動 IP アドレスを持つ DHCP Discover を送信するか、オペレータが設定したセッションのタイムアウトが過ぎた場合には、トンネルがティアダウンして、VoIP クライアントは再認証を行わなければならないことに注意してください。

クライアント ロケーション

Cisco Wireless LAN Solution では、クライアント、不正なアクセス ポイント、不正なアクセス ポイント クライアント、無線周波数 ID（RFID）タグ ロケーションを定期的に特定し、Cisco WCS データベースにそのロケーションを保存します。クライアントのロケーション履歴を表示するには、Cisco WCS Monitor Client < クライアント > - < ベンダーの MAC アドレス > ページを参照して、Recent Map（High Resolution）または Present Map（High Resolution）を選択します。Cisco WCS Base では、最も近いアクセス ポイントへのロケーションをサポートします。Cisco WCS Location では、10m 以内のロケーションをサポートします。

Cisco WCS Location を使用している場合、Cisco Wireless LAN Solution のエンド ユーザは、Cisco 2700 シリーズ Location Appliance（Location Appliance）を展開することもできます。これについては、「Cisco 2700 シリーズ Location Appliance」の項（P.1-59）を参照してください。Location Appliance は、履歴ロケーション データを計算、収集、および格納することで、高精度な組み込み Cisco WCS Location 機能を拡張して、このデータを Cisco WCS に表示することができます。この場合、Location Appliance は 1 つまたは複数の Cisco WCS サーバに対するサーバとして機能し、そのアソシエートされているコントローラのデータを収集、格納、および受け渡しします。

外部 DHCP サーバ

オペレーティング システムは、ネットワークに対しては DHCP リレーとして、そして業界標準の外部 DHCP サーバが DHCP リレーをサポートする場合は、クライアントに対する DHCP サーバとして表示されるように設計されています。つまり、各 Cisco Wireless LAN Controller は、DHCP サーバに対する DHCP リレー エージェントとして表示されます。これは、Cisco Wireless LAN Controller が、無線クライアントに対しては、仮想 IP アドレスにある DHCP サーバとして表示されることも意味します。

Cisco Wireless LAN Controller は DHCP サーバから取得したクライアント IP アドレスをキャプチャするので、同一 Cisco Wireless LAN Controller、Cisco Wireless LAN Controller 間、およびサブネット間でのクライアント ローミング時に、そのクライアントの同一 IP アドレスを保持します。

無線 LAN ごとの割り当て

Cisco WLAN Solution 無線 LAN はすべて、同じ DHCP サーバまたは異なる DHCP サーバを使用するか、または DHCP サーバを使用しないようにするかを設定できます。これにより、オペレータはかなり柔軟に無線 LAN を設定できるようになります。詳細は、「Cisco WLAN Solution 無線 LAN」の項（P.1-18）を参照してください。

無線による管理をサポートする Cisco WLAN Solution の無線 LAN では、管理（デバイス サービシング）クライアントが DHCP サーバから IP アドレスを取得できるようにする必要があります。無線による管理の設定方法は、「無線による管理の使用」の項（P.3-17）を参照してください。

インターフェイスごとの割り当て

個々のインターフェイスに DHCP サーバを割り当てることができます。

- レイヤ 2 管理インターフェイスは、プライマリおよびセカンダリ DHCP サーバに設定できます。管理インターフェイスの詳細は、「管理インターフェイスについて」の項（P.1-29）を参照してください。
- レイヤ 3 AP マネージャ インターフェイスは、プライマリおよびセカンダリ DHCP サーバに設定できます。AP マネージャ インターフェイスの詳細は、「AP マネージャ インターフェイス」の項（P.1-30）を参照してください。
- 各オペレータ定義インターフェイスは、プライマリおよびセカンダリ DHCP サーバに設定できます。オペレータ定義インターフェイスの詳細は、「オペレータ定義インターフェイス」の項（P.1-30）を参照してください。
- 仮想インターフェイスは、DHCP サーバを使用しません。仮想インターフェイスの詳細は、「仮想インターフェイス」の項（P.1-31）を参照してください。
- サービス ポート インターフェイスは、DHCP サーバを有効または無効にするように設定できます。サービス ポート インターフェイスの詳細は、「サービス ポート」の項（P.1-31）を参照してください。

セキュリティ上の考慮事項

高度なセキュリティが必要な場合は、すべてのクライアントに対して DHCP サーバの IP アドレスの取得を要求することを推奨します。この要件を適用するためには、すべての無線 LAN を、DHCP Required に設定して、有効な DHCP サーバの IP アドレスを入力するように設定し、クライアントの固定 IP アドレスが禁止されるようにします。DHCP Required に設定されている 無線 LAN にアソシエートするクライアントは、指定した DHCP サーバの IP アドレスを取得しないと、どのネットワーク サービスへのアクセスも許可されません。

DHCP Required が選択されている場合、クライアントは DHCP を使って IP アドレスを取得しなければならないことに注意してください。固定 IP アドレスを持つクライアントはすべて、ネットワーク上で許可されなくなります。クライアントの DHCP プロキシとして動作する Cisco Wireless LAN Controller が、DHCP トラフィックを監視します。

セキュリティが多少劣ってもかまわない場合は、DHCP Required を無効に設定し、有効な DHCP サーバの IP アドレスを指定して、無線 LAN を作成することができます。その後クライアントは、固定 IP アドレスを使用するか、指定された DHCP サーバの IP アドレスを取得するかを選択できます。

また、オペレータは、DHCP Required を無効に設定し、DHCP サーバの IP アドレス を 0.0.0.0 に指定した無線 LAN を別に作成することもできます。このような無線 LAN では、すべての DHCP 要求がドロップするため、クライアントは固定 IP アドレスを使用しなければなりません。これらの無線 LAN は、無線接続による管理をサポートしていないことに注意してください。

Cisco WLAN Solution のモビリティ グループ

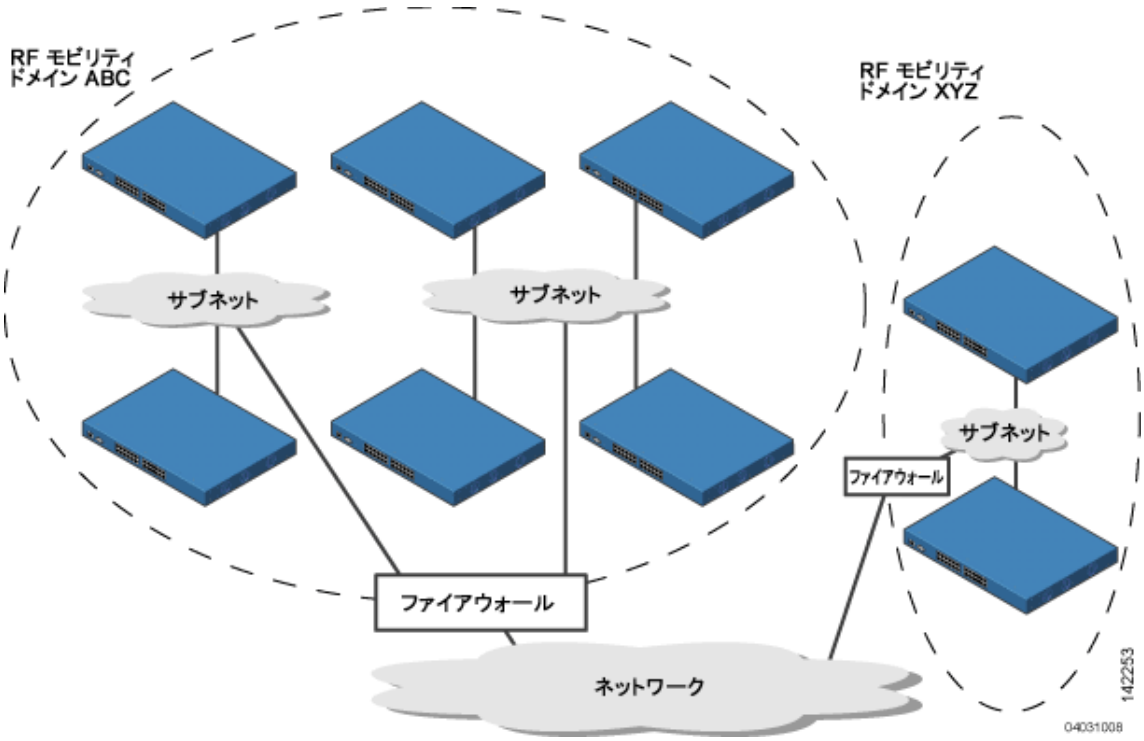
Cisco Wireless LAN Solution オペレータは、コントローラのグループ間でのクライアント ローミングを許可するようモビリティ グループを定義できます。マルチコントローラ展開のコントローラは、ネットワーク全体および無線で相互検出を行うことができるため、企業、公共機関、および無線インターネット サービス プロバイダーは、使用しているコントローラを切り離すことが重要です。オペレーティング システムでは、オペレータがコントローラにモビリティ グループ名を割り当てることで、この切り離しを簡単に実行できるようにしています。この割り当てを実行するには、Web ユーザ インターフェイス、WCS、または CLI を使用できます。

クライアントは、本来の、つまりアンカーである Cisco Wireless LAN Controller に自動的にアソシエートされた後で、ローミングできるようになります。このアンカーの Cisco Wireless LAN Controller は、クライアント セッション期間中、クライアント情報を保持し、クライアントがすべてのハンドオフにおいて同じ IP アドレスで接続された状態を維持するようにします。

モビリティ グループに含まれるすべてのコントローラでは、同一のレイヤ 2 および レイヤ 3 LWAPP 動作を使用する必要があり、使用しないと、モビリティ ソフトウェア アルゴリズムを無視することになるので注意が必要です。

図 1-4 は、2 つのグループの Cisco Wireless LAN Controller について、モビリティ グループ名を作成した結果を示しています。ABC モビリティ グループの Cisco Wireless LAN Controller は、そのアクセス ポイントと共有サブネットを経由して、互いに認識し、相互通信を行いますが、ABC モビリティ グループは、XYZ アクセス ポイントを不正なアクセス ポイントとしてタグ付けします。同様に、XYZ モビリティ グループのコントローラは、ABC モビリティ グループのコントローラを認識せず、通信を行いません。この機能により、ネットワークでのモビリティ グループの切り離しが確実に行われます。

図 1-4　一般的なモビリティ グループ名の適用



（注）　コントローラが正常に VLAN トラフィックをルーティングするように、無線 LAN と管理インターフェイスにはそれぞれ別の VLAN セットを割り当てることをお勧めします。

Cisco WLAN Solution モビリティ グループ機能を使用して、異なるモビリティ グループ名を同じ無線ネットワーク内の異なる Cisco Wireless LAN Controller に割り当て、1 つの企業内の異なるフロア、ビルディング、キャンパス間でのローミングを制限することもできます。

Radio Resource Management（RRM）動作は、有効の場合、個々の Cisco WLAN Solution モビリティ グループ内に制約されます。RRM の詳細は、「Radio Resource Management（RRM）」の項（P.1-9）を参照してください。

（注）　コントローラは同じモビリティ　グループ内で相互通信を行うため、ネットワーク上の不要なトラフィックを増やさないように、シスコでは、物理的に分離されているコントローラを同じスタティック モビリティ グループに追加しないようにすることを推奨しています。

Cisco WLAN Solution の有線接続

Cisco Wireless LAN Solution コンポーネントは、業界標準のイーサネット ケーブルとコネクタを使用して相互に通信します。次の項では、Cisco WLAN Solution の有線接続について説明します。

- Cisco 2000 シリーズ Wireless LAN Controller をネットワークに接続するときは、1 ～ 4 本の 10/100BASE-T イーサネット ケーブルを使用します。
- Cisco 4100 シリーズ Wireless LAN Controller をネットワークに接続するときは、1 ～ 2 本の光ファイバ ギガビット イーサネット ケーブルを使用します。2 つの冗長ギガビット イーサネット接続によって、1 つのネットワークに発生した障害を迂回することができます。常に 1 つの Cisco 4100 シリーズ Wireless LAN Controller ギガビット イーサネット接続がアクティブで、もう一方はパッシブです。ネットワークに障害が発生すると、アクティブな接続がパッシブになり、パッシブな接続がアクティブになります。
- 4402 Cisco 4400 シリーズ Wireless LAN Controller をネットワークに接続するときは、1 ～ 2 本の光ファイバ ギガビット イーサネット ケーブルを使用し、4404 Cisco 4400 シリーズ Wireless LAN Controller をネットワークに接続するときは、1 ～ 4 本の光ファイバ ギガビット イーサネット ケーブルを使用します。2 つの冗長ギガビット イーサネット接続によって、1 つのネットワークに発生した障害を迂回することができます。常に各ペアの 1 つの Cisco 4400 シリーズ Wireless LAN Controller ギガビット イーサネット接続がアクティブで、もう一方はパッシブです。ネットワークに障害が発生すると、アクティブな接続がパッシブになり、パッシブな接続がアクティブになります。
- Cisco 1000 シリーズ Lightweight アクセス ポイントをネットワークに接続するときは、10/100BASE-T イーサネット ケーブルを使用します。Power over Ethernet（PoE）機能が搭載されているネットワーク デバイスから Cisco 1000 シリーズ Lightweight アクセス ポイントの電力を供給するときは、標準の CAT-5 ケーブルを使用することもできます。この電源分配プランを使用すると、個々の AP 電源供給と接続用ケーブルにかかるコストを軽減できます。

Cisco WLAN Solution 無線 LAN

Cisco Wireless LAN Solution では、Lightweight アクセス ポイントについて、最大 16 の無線 LAN を制御できます。各無線 LAN は、別々の無線 LAN ID（1 ～ 16）、別々の無線 LAN SSID（無線 LAN 名）を持ち、固有のセキュリティ ポリシーを割り当てることができます。

Cisco 1000 シリーズ Lightweight アクセス ポイントは、すべてのアクティブな Cisco WLAN Solution 無線 LAN SSID をブロードキャストし、各無線 LAN に定義されているポリシーを適用します。

（注）　コントローラが正常に VLAN トラフィックをルーティングするように、無線 LAN と管理インターフェイスにはそれぞれ別の VLAN セットを割り当てることをお勧めします。

Cisco Wireless LAN Solution で無線による管理を有効にすると、オペレータは CLI と Telnet、http/https、および SNMP を使用して、有効になった無線 LAN 全体のシステムを管理できるようになります。

Cisco WLAN Solution 無線 LAN を設定するには、第 5 章「無線 LAN の設定」を参照してください。

アクセス コントロール リスト

オペレーティング システムでは、標準的なでは、標準的なファイアウォールのアクセス コントロール リストと同様に、64 個までの Access Control List（ACL; アクセス コントロール リスト）を定義できます。各 ACL には、64 個までのルール（フィルタ）を含めることができます。

オペレータは、ACL を使用して、指定した無線 LAN 内の複数の VPN サーバにアクセスするようクライアントを制御できます。無線 LAN 上のすべてのクライアントが 1 つの VPN サーバにアクセスする必要がある場合は、「セキュリティ概要」の項（P.3-2）に示す IPSec または VPN ゲートウェイのパススルー設定を使用してください。

定義した ACL は、管理インターフェイス、AP マネージャ インターフェイス、または任意のオペレータ定義インターフェイスに適用できます。

アクセス コントロール リストの設定方法は、『Web User Interface Online Help』の Access Control Lists > New を参照してください。

ID ネットワーキング

Cisco Wireless LAN Controller では、次のパラメータを、特定の無線 LAN にアソシエートしているすべてのクライアントに適用させることができます。適用可能なパラメータは、QoS、グローバルまたはインターフェイス固有の DHCP サーバ、レイヤ 2 と レイヤ 3 のセキュリティ ポリシー、およびデフォルトのインターフェイス（物理ポート、VLAN、および ACL 割り当てを含む）です。

ただし、Cisco Wireless LAN Controller では、MAC Filtering を使用するか、または AAA Override パラメータを許可することによって、個々のクライアント（MAC アドレス）にプリセットされている無線 LAN パラメータを無効にすることもできます。たとえば、この設定を使用すると、社内の全クライアントを会社の無線 LAN にログインさせてから、MAC アドレスごとに、異なる QoS、DHCP サーバ、レイヤ 2 とレイヤ 3 のセキュリティ ポリシー、およびインターフェイス設定を使用して、クライアントを接続させることができます。

Cisco Wireless LAN Solution オペレータはクライアントに MAC Filtering を設定すると、異なる VLAN を MAC アドレスに割り当てることができます。この MAC アドレスは、オペレーティング システムでクライアントを管理インターフェイス、またはいずれかのオペレータ定義インターフェイスに自動的に再ルーティングさせるときに使用できます。どちらのインターフェイスにも、独自の VLAN、ACL、DHCP サーバ、および物理ポート割り当てがあります。この MAC Filtering は、おおまかな AAA Override として使用でき、通常はすべての AAA（RADIUS その他の）Override よりも優先されます。

ただし、Allow AAA Override が有効である場合は、MAC アドレスごとに QoS と ACL を返すように、RADIUS（またはその他の AAA）サーバを設定することもできます。Allow AAA Override が有効であるときは、Cisco Wireless LAN Controller に設定されている MAC Filtering パラメータよりも AAA Override が優先されます。特定の MAC アドレスに使用できる AAA Override がない場合は、すでに Cisco Wireless LAN Controller にある MAC Filtering パラメータを使用します。この AAA（RADIUS その他の）Override は、詳細な AAA Override として使用できますが、Allow AAA Override が有効であるときにのみ、MAC Filtering よりも優先されます。

すべての場合において、Override パラメータ（たとえば、オペレータ定義インターフェイスや QoS）は、Cisco Wireless LAN Controller 設定であらかじめ定義しておく必要があります。

いずれの場合も、使用されているのがレイヤ 2 認証であるか、レイヤ 3 認証であるかにかかわらず、オペレーティング システムでは AAA サーバまたは MAC Filtering で指定されている QoS と ACL が使用されます。

また、MAC フィルタリング、802.1X、または WPA レイヤ 2 認証について設定されている場合、オペレーティング システム では、クライアントをデフォルトの Cisco WLAN Solution 無線 LAN VLAN から別の VLAN に移動するだけであることに注意してください。

Cisco WLAN Solution 無線 LAN を設定するには、「無線 LAN の設定」の項（P.5-2）を参照してください。

Cisco Secure ACS との統合の強化

ID ベースのネットワーキング機能は、認証、認可、アカウンティング（AAA）Override を使用します。次のベンダー固有属性が RADIUS アクセス ポイント メッセージに存在する場合は、値が無線 LAN プロファイルで指定された値を上書きします。

- QoS レベル
- 802.1p 値
- VLAN インターフェイス名
- アクセス コントロール リスト（ACL）名

このリリースでは、IETF RFC 2868（トンネル プロトコル サポートの RADIUS 属性）で定義されている標準の「VLAN 名 / 番号を割り当てられた RADIUS」機能を使用して AAA サーバが VLAN の番号または名前を返すサポートが追加されています。無線クライアントを特定の VLAN に割り当てるために、AAA サーバはアクセス ポイント メッセージ内で次の属性をコントローラに送信します。

- IETF 64（トンネル タイプ）：VLAN
- IETF 65（トンネル メディア タイプ）：802
- IETF 81（トンネル プライベート グループ ID）：VLAN # または VLAN 名文字列

これにより、Cisco Secure ACS はポスチャ分析の結果となりえる VLAN の変更を通信できるようになります。この機能の利点は、次のとおりです。

- Cisco Secure ACS との統合により、インストールとセットアップ時間が短縮されます。
- Cisco Secure ACS は、有線および無線ネットワーク上で円滑に動作します。

この機能は、2000、4100、4400 シリーズ コントローラ、および、1000、1130、1200、1500 シリーズ Lightweight アクセス ポイントをサポートします。

動的周波数選択

Cisco Wireless LAN Solution は、無線デバイスがレーダー信号を検出して干渉しないようにする Dynamic Frequency Selection（DFS; 動的周波数選択）の使用を必須とする欧州とシンガポールの規制に準拠しています。

5GHz の無線を使用する Lightweight アクセス ポイントが表 1-1 に示す 15 チャネルのいずれかで動作している場合、アクセス ポイントがアソシエートするコントローラは、自動的に DFS を使用して動作周波数を設定します。

DFS 対応の 5GHz 無線用のチャネルを手動で選択した場合、コントローラはそのチャネルでのレーダー アクティビティを 60 秒間チェックします。レーダー アクティビティが検出されない場合、アクセス ポイントは選択されたチャネル上で動作します。選択されたチャネルでレーダー アクティビティが検出された場合、コントローラは自動的に別のチャネルを選択し、30 分後にアクセス ポイントは選択されたチャネルを再試行します。

（注）　Rogue Location Detection Protocol（RLDP; 不正ロケーション検出プロトコル）は、表 1-1 に示すチャネルではサポートされていません。

（注）　一部の 5GHz チャネルの有効な最大送信電力は、他のチャネルよりも大きくなります。電力が制限されている 5GHz チャネルをランダムに選択した場合、コントローラはそのチャネルの電力制限に合うように送信電力を下げます。

表 1-1　DFS が自動的に有効にされる 5GHz チャネル

52（5260MHz）	104（5520MHz）	124（5620MHz）
56（5280MHz）	108（5540MHz）	128（5640MHz）
60（5300MHz）	112（5560MHz）	132（5660MHz）
64（5320MHz）	116（5580MHz）	136（5680MHz）
100（5500MHz）	120（5600MHz）	140（5700MHz）

DFS の使用時、コントローラはレーダー信号の動作周波数を監視します。チャネルでレーダー信号が検出された場合、コントローラは次の手順を実行します。

- アクセス ポイント チャネルを、レーダー アクティビティが見られないチャネルに変更します。コントローラは、ランダムにチャネルを選択します。
- 選択されたチャネルが表 1-1 に示したチャネルのいずれかである場合、新しいチャネルでレーダー信号を 60 秒間スキャンします。新しいチャネルでレーダー信号が検出されない場合、コントローラはクライアントのアソシエーションを承認します。
- レーダー アクティビティが見られたチャネルをレーダー チャネルとして記録し、そのチャネルでのアクティビティを 30 秒間回避します。
- トラップを生成し、ネットワーク マネージャに警告します。

ファイル転送

Cisco Wireless LAN Solution オペレータは、CLI コマンド、Web ユーザ インターフェイス コマンド、または Cisco WCS コマンドを使用して、オペレーティング システムのコード、設定、および証明書ファイルを Cisco Wireless LAN Controller にアップロードすること、およびそこからダウンロードすることができます。

- CLI コマンドを使用するには、「コントローラとのファイルのやり取り」の項（P.6-2）を参照してください。
- Cisco WCS コマンドを使用するには、「Cisco WCS を使ってシステム ソフトウェアを更新する方法」の項（P.9-22）を参照してください。

Power over Ethernet

Lightweight アクセス ポイントは、イーサネット ケーブルを使用して、802.3af 準拠の Power over Ethernet (PoE) デバイスから電力供給を受けることができます。これにより、個々のデバイスへの電力供給や、余分な配線、コンジット、コンセントにかかるコストが軽減され、設置時間を短縮できます。PoE 機能を使用すると、設置担当者は、AC コンセントの近くに Cisco 1000 シリーズ Lightweight アクセス ポイントやその他の電力供給を要する装置を取り付ける必要がなくなるため、最大カバレッジが得られるように Cisco 1000 シリーズ Lightweight アクセス ポイントをより柔軟に配置できるようになります。

PoE を使用している場合、1 本の CAT-5 ケーブルを各 Lightweight アクセス ポイントから PoE 機能が搭載されているネットワーク要素（PoE 電源ハブや、Cisco WLAN Solution シングルライン PoE インジェクタなど）に接続します。PoE 機器で Lightweight アクセス ポイントが PoE 対応であると判断された場合は、使用されていないイーサネット ケーブル ペアを使って、48 VDC の電力が Lightweight アクセス ポイントに供給されます。

PoE ケーブルの長さは、100BASE-T 仕様では 100m に、10BASE-T 仕様では 200m にそれぞれ制限されています。

Lightweight アクセス ポイントは、802.3af 準拠デバイスまたは外部電源装置から電力供給を受けることができます。

ピコ セル機能

ピコ セル機能には、オペレーティング システムの最適化が含まれています。この機能は次のようにサポートされます。

- Cisco WCS Pico Cell Mode パラメータで オペレーティング システム パラメータを再設定し、ピコ セル展開で オペレーティング システム が効率的に機能するようにします。オペレータがピコ セル ネットワークを展開しているときは、オペレーティング システム では、**config database size 2048** CLI コマンドを使用して、割り当てメモリを 512MB から 2048MB に増やす必要があります。
- 複数のモビリティ　ドメインが存在する場合は、そのドメイン間でクライアントを移動できます。
- WPA2 VFF 拡張が追加されているため、アソシエートするたびにキーを再生成する必要はありません。これにより、既存の PTK と GTK の再使用が可能です。
- WPA2 PMK キャッシングと VFF では、認証段階の前にコンテキスト転送の一部として PMK キャッシュが転送されます。これにより、Cisco Wireless LAN Controller 内と Cisco Wireless LAN Controller 間での双方のローミング イベントに対して機能する、迅速なハンドオフが可能となります。
- ビーコン / プローブ応答によって、Cisco 1000 シリーズ Lightweight アクセス ポイントが、接続先となる Cisco Wireless LAN Controller を指定できるため、必要な場合にのみ再許可イベントが発生するようになり、その結果、Cisco Wireless LAN Controller 間のハンドオフが最小限に抑えられて、CPU 使用率が低下します。
- ピコ セルに対する Cisco 1000 シリーズ Lightweight アクセス ポイントの感度を変更できます。
- Cisco 1000 シリーズ Lightweight アクセス ポイント フォールバック動作を制御して、ピコ セル使用を最適化することができます。
- 方向性アンテナのヒート マップをサポートします。
- ブラックリストに載っているイベントに対して特別の制御を行うことができます。
- Cisco 1000 シリーズ Lightweight アクセス ポイントの CLI を使用して、基本の LWAPP 設定を作成して表示することができます。

Intrusion Detection Service（IDS; 侵入検知サービス）

侵入検知サービスには次のものがあります。

- 「ANY」SSID のクライアント プローブの感知
- Cisco 1000 シリーズ Lightweight アクセス ポイントの有無の感知
- MiM 攻撃、NetStumbler、Wellenreiter の通知
- 管理フレーム検出と RF 妨害検出
- スプーフィングされた許可解除検出（エアジャックなど）
- ブロードキャスト許可解除検出
- ヌル プローブ応答検出
- 擬似 AP 検出
- 脆弱な WEP 暗号化の検出
- MAC スプーフィング検出
- AP なりすまし検出
- ハニーポット AP 検出
- 有効なステーションの保護
- 正しく設定されていない AP の保護
- 不正なアクセス ポイントの検出
- アドホック検出と保護
- 無線ブリッジ検出
- 休眠状態の検出 / 保護

Cisco Wireless LAN Controller

Cisco Wireless LAN Controller は、802.11a プロトコルおよび 802.11b/802.11g プロトコルをサポートする、企業向けの高性能無線スイッチング プラットフォームです。Radio Resource Management（RRM）機能が搭載されているオペレーティング システムの制御下でこの製品を稼働することにより、802.11 RF 環境でのリアルタイムの変化に自動対応する Cisco WLAN Solution が実現されます。Cisco Wireless LAN Controller は、高性能なネットワークおよびセキュリティ ハードウェアを中心に構築されており、他に例のないセキュリティを備えた信頼性の高い 802.11 企業ネットワークが実現します。

Cisco 2000 シリーズ Wireless LAN Controller

Cisco 2000 シリーズ Wireless LAN Controller は、Cisco Wireless LAN Solution を構成するコンポーネントの 1 つです。すべての Cisco 2000 シリーズ Wireless LAN Controller は、最大 6 の Cisco 1000 シリーズ Lightweight アクセス ポイントを制御し、小規模企業と低密度アプリケーションに理想的な LAN 環境を作り出します。

Cisco 2000 シリーズ Wireless LAN Controller は、241 x 152 x 41mm のスリムなシャーシを持ち、デスクトップとシェルフに取り付けることができます。Cisco 2000 シリーズ Wireless LAN Controller の前面パネルには、電源 LED が 1 つと、イーサネット LAN ポートのステータス LED が 4 つ付いており、このステータス LED は、対応する 4 つの背面パネルのイーサネット LAN コネクタの 10MHz または 100MHz 接続と送受信アクティビティを示します。Cisco 2000 シリーズ Wireless LAN Controller には、デスクトップとシェルフ取り付け用ゴム脚が 4 つ付属しています。

Cisco 4100 シリーズ Wireless LAN Controller

Cisco 4100 シリーズ Wireless LAN Controller は、Cisco Wireless LAN Solution を構成するコンポーネントの 1 つです。すべての Cisco 4100 シリーズ Wireless LAN Controller は、最大 36 の Cisco 1000 シリーズ Lightweight アクセス ポイントを制御し、中規模企業と中密度アプリケーションに理想的な LAN 環境を作り出します。

図 1-5 は、前面パネルに 2 つの冗長 SX/LC ジャックが付いている Cisco 4100 シリーズ Wireless LAN Controller を示しています。1000BASE-SX 回線は、LC 物理コネクタを使用した 850nM（SX）光ファイバ リンクで 100Mbps または 1000Mbps の有線接続をネットワークに提供します。

図 1-5　4100 シリーズ コントローラ

Cisco 4100 シリーズ Wireless LAN Controller は、製造段階で発注があれば、VPN、IPSec などのプロセッサ集中型タスクをサポートする VPN/ 拡張セキュリティ モジュール（Crypto Card）を搭載することができます。また、Cisco 4100 シリーズ Wireless LAN Controller には、2 つの（Cisco 4100 シリーズ Wireless LAN Controller）1000BASE-SX ネットワーク コネクタが装備されており、これを使用すると、ギガビット イーサネット速度でネットワークとの通信が可能になります。1000BASE-SX ネットワーク コネクタは、LC 物理コネクタを使用した 850nM（SX）光ファイバ リンクで 100Mbps または 1000Mbps の有線接続をネットワークに提供します。

Cisco 4100 シリーズ Wireless LAN Controller の 2 つの冗長ギガビット イーサネット接続を使用すると、1 つのネットワークに発生した障害を迂回することができます。常に 1 つの Cisco 4100 シリーズ Wireless LAN Controller ギガビット イーサネット接続がアクティブで、もう一方はパッシブです。ネットワークに障害が発生すると、アクティブな接続がパッシブになり、パッシブな接続がアクティブになります。

Cisco 4400 シリーズ Wireless LAN Controller

Cisco 4400 シリーズ Wireless LAN Controller は、Cisco Wireless LAN Solution を構成するコンポーネントの 1 つです。すべての Cisco 4400 シリーズ Wireless LAN Controller は、最大 100 の Cisco 1000 シリーズ Lightweight アクセス ポイントを制御し、大規模企業と高密度アプリケーションに理想的な LAN 環境を作り出します。

4402 Cisco 4400 シリーズ Wireless LAN Controller には、2 つの冗長前面パネル SX/LC/T SFP モジュール（SFP トランシーバ、または小型フォーム ファクタ プラグイン）が 1 セット装備されており、4404 Cisco 4400 シリーズ Wireless LAN Controller には、2 つの冗長前面パネル SX/LC/T SFP モジュールが 2 セット装備されています。

- 1000BASE-SX SFP モジュールは、LC 物理コネクタを使用した 850nM（SX）光ファイバ リンクで 1000Mbps の有線接続をネットワークに提供します。
- 1000BASE-LX SFP モジュールは、LC 物理コネクタを使用した 1300nM（LX/LH）光ファイバ リンクで 1000Mbps の有線接続をネットワークに提供します。
- 1000BASE-T SFP モジュールは、RJ-45 物理コネクタを使用した銅線リンクで 1000Mbps の有線接続をネットワークに提供します。

Cisco 4400 シリーズ Wireless LAN Controller の 1 または 2 セットの冗長ギガビット イーサネット接続を使用すると、Cisco 4400 シリーズ Wireless LAN Controller は 1 つのネットワークに発生した障害を迂回することができます。常に 1 つの Cisco 4400 シリーズ Wireless LAN Controller ギガビット イーサネット接続がアクティブで、もう一方はパッシブです。ネットワークに障害が発生すると、アクティブな接続がパッシブになり、パッシブな接続がアクティブになります。

Cisco 4400 シリーズ Wireless LAN Controller には、1 つまたは 2 つの Cisco 4400 シリーズ電源を装着することができます。Cisco Wireless LAN Controller に 2 つの Cisco 4400 シリーズ電源を装着すると、電源が冗長構成になるため、一方の電源に障害が発生しても、他方の電源で電力の供給を続けることができます。

Cisco Wireless LAN Controller には、標準で 1 つの Cisco 4400 シリーズ電源が工場出荷時にスロット 1 に装着されています。冗長性のために、製造段階で Cisco 4400 シリーズ電源をもう 1 つ発注して、スロット 2 に取り付けることができます。同じ電源がスロット 1 にも装着されているので、故障した電源と現場で交換することができます。

Cisco 2000 シリーズ Wireless LAN Controller の型番

Cisco 2000 シリーズ Wireless LAN Controller の型番は、次のとおりです。

- AIR-WLC2006-K9：Cisco 2000 シリーズ Wireless LAN Controller は、最大 6 つの Cisco 1000 シリーズ Lightweight アクセス ポイントと通信します。

（注）　Cisco 2000 シリーズ Wireless LAN Controller には、卓上用取り付け脚が付属しています。

Cisco 4100 シリーズ Wireless LAN Controller の型番

Cisco 4100 シリーズ Wireless LAN Controller の型番は、次のとおりです。

- AIR-WLC4112-K9：Cisco 4100 シリーズ Wireless LAN Controller は、2 つの冗長ギガビット イーサネット接続を使用して 1 つのネットワークに発生した障害を迂回し、最大 12 の Cisco 1000 シリーズ Lightweight アクセス ポイントと通信します。つまり、常に 1 つの Cisco 4100 シリーズ Wireless LAN Controller ギガビット イーサネット接続がアクティブで、もう一方はパッシブです。ネットワークに障害が発生すると、アクティブな接続がパッシブになり、パッシブな接続がアクティブになります。1000BASE-SX ネットワーク アダプタは、LC 物理コネクタを使用した 850nM（SX）光ファイバ リンクで 100Mbps または 1000Mbps の有線接続をネットワークに提供します。
- AIR-WLC4124-K9：Cisco 4100 シリーズ Wireless LAN Controller は、2 つの冗長ギガビット イーサネット接続を使用して 1 つのネットワークに発生した障害を迂回し、最大 24 の Cisco 1000 シリーズ Lightweight アクセス ポイントと通信します。
- AIR-WLC4136-K9：Cisco 4100 シリーズ Wireless LAN Controller は、2 つの冗長ギガビット イーサネット接続を使用して 1 つのネットワークに発生した障害を迂回し、最大 36 の Cisco 1000 シリーズ Lightweight アクセス ポイントと通信します。

（注）　すべての Cisco 4100 シリーズ Wireless LAN Controller モデルには、19 インチ EIA 装置ラック用フラッシュ マウント金具が付属しています。

次のアップグレード モデルも提供されています。

- AIR-VPN-4100：VPN/ 拡張セキュリティ モジュール。VPN、L2TP、IPSec などのプロセッサ集中型セキュリティ オプションをサポートします。これは、すべての Cisco 4100 シリーズ Wireless LAN Controller 用の、現場でインストール可能なオプションです。

Cisco 4400 シリーズ Wireless LAN Controller の型番

Cisco 4400 シリーズ Wireless LAN Controller の型番は、次のとおりです。

- AIR-WLC4402-12-K9：4402 Cisco 4400 シリーズ Wireless LAN Controller は、2 つの冗長ギガビット イーサネット接続を使用して 1 つのネットワークに発生した障害を迂回し、最大 12 の Cisco 1000 シリーズ Lightweight アクセス ポイントと通信します。つまり、常に 1 つの Cisco 4400 シリーズ Wireless LAN Controller ギガビット イーサネット接続がアクティブで、もう一方はパッシブです。ネットワークに障害が発生すると、アクティブな接続がパッシブになり、パッシブな接続がアクティブになります。
- AIR-WLC4402-25-K9：4402 Cisco Wireless LAN Controller は、2 つの冗長ギガビット イーサネット接続を使用して 1 つのネットワークに発生した障害を迂回し、最大 25 の Cisco 1000 シリーズ Lightweight アクセス ポイントと通信します。
- AIR-WLC4402-50-K9：4402 Cisco Wireless LAN Controller は、2 つの冗長ギガビット イーサネット接続を使用して 1 つのネットワークに発生した障害を迂回し、最大 50 の Cisco 1000 シリーズ Lightweight アクセス ポイントと通信します。
- AIR-WLC4404-100-K9：4404 Cisco Wireless LAN Controller は、4 つの冗長ギガビット イーサネット接続を使用して 1 つまたは 2 つのネットワークに発生した障害を迂回し、最大 100 の Cisco 1000 シリーズ Lightweight アクセス ポイントと通信します。

（注）　すべての Cisco 4400 シリーズ Wireless LAN Controller モデルには、19 インチ EIA 装置ラック用フラッシュ マウント金具が付属しています。

4402 Cisco 4400 シリーズ Wireless LAN Controller は、2 つの冗長前面パネル SX/LC/T SFP モジュール（SFP トランシーバ、または小型フォーム ファクタ プラグイン）を 1 セット使用し、4404 Cisco 4400 シリーズ Wireless LAN Controller は、2 つの冗長前面パネル SX/LC/T SFP モジュールを 2 セット使用します。

- 1000BASE-SX SFP モジュールは、LC 物理コネクタを使用した 850nM（SX）光ファイバ リンクで 1000Mbps の有線接続をネットワークに提供します。
- 1000BASE-LX SFP モジュールは、LC 物理コネクタを使用した 1300nM（LX/LH）光ファイバ リンクで 1000Mbps の有線接続をネットワークに提供します。
- 1000BASE-T SFP モジュールは、RJ-45 物理コネクタを使用した銅線リンクで 1000Mbps の有線接続をネットワークに提供します。

次の電源モジュールも提供されています。

- AIR-PWR-4400-AC：すべての Cisco 4400 シリーズ電源。1 台の Cisco 4400 シリーズ電源で複数の Cisco 4400 シリーズ電源への電力供給が可能で、Cisco 4400 シリーズ電源は冗長構成です。

ディストリビューション システム ポート

Distribution System（DS; ディストリビューション システム）ポートは、コントローラがネットワーク全域のアクセス ポイントと通信するときに使用する物理ポートです。DS ポートは、Cisco Wireless LAN Solution 無線 LAN とその他のネットワークとの間でパケットを交換する場所です。

（注）　DS ポートを専用のコントローラ サービス ポートに割り当てることはできません。

「レイヤ 2 およびレイヤ 3 の Lightweight Access Point protocol（LWAPP）動作」の項（P.1-8）で説明したように、LWAPP 通信がレイヤ 2（同一サブネット）動作に設定されている場合、ディストリビューション システムには、物理ディストリビューション システム ポートの数に関係なく、コントローラ間の全通信と、コントローラとアクセス ポイント間の全通信を制御する 1 つの管理インターフェイスがなければなりません。

また、「レイヤ 2 およびレイヤ 3 の Lightweight Access Point protocol（LWAPP）動作」の項（P.1-8）で説明したように、LWAPP 通信がレイヤ 3（異なるサブネット）動作に設定されている場合、ディストリビューション システムには、物理ディストリビューション システム ポートの数に関係なく、コントローラ間の全通信を制御する 1 つの管理インターフェイスと、コントローラとアクセス ポイント間の全通信を制御する 1 つの AP マネージャ インターフェイスがなければなりません。

また、個々の物理ディストリビューション システム ポートでは、1 ～ 512 個のオペレータ定義インターフェイスを割り当てることができます。オペレータ定義インターフェイスは個々に設定して、ディストリビューション システム ポート上での VLAN 通信を許可します。

管理インターフェイスについて

論理管理インターフェイスは、Cisco Wireless LAN Controller と Cisco 1000 シリーズ Lightweight アクセス ポイント間のレイヤ 2 通信を制御します。

（注）　コントローラが正常に VLAN トラフィックをルーティングするように、無線 LAN と管理インターフェイスにはそれぞれ別の VLAN セットを割り当てることをお勧めします。

管理インターフェイスには 1 つの物理ポートが割り当てられ、これを使用して、他のネットワーク デバイスおよびアクセス ポイントとの通信を行います。ただし、管理インターフェイスは、次のように、サービス ポート以外の他のすべての物理ポートを使用して通信することも可能です。

- レイヤ 2 ネットワークでメッセージを送信し、サービス ポート以外のすべての物理ポートを使用して他の Cisco Wireless LAN Controller を自動検出して通信を行います。
- レイヤ 2 ネットワークで Cisco 1000 シリーズ Lightweight アクセス ポイント LWAPP ポーリング メッセージを受信し、可能な限り多くの Cisco 1000 シリーズ Lightweight アクセス ポイントを自動検出して、アソシエートし、通信を行います。

（注）　コントローラが故障した場合、ドロップした Lightweight アクセス ポイントは、別のコントローラのネットワークをポーリングします。オンラインのコントローラに Lightweight アクセス ポイントのポートが残っている場合、管理インターフェイスはそのネットワークで Lightweight アクセス ポイント ポーリング メッセージを受信し、可能な限り多くのアクセス ポイントを自動検出して、アソシエートし、通信を行います。詳細は、「Cisco Wireless LAN Controller のフェールオーバーの保護」の項（P.1-33）を参照してください。

（注）　管理インターフェイスを専用のコントローラ サービス ポートに割り当てることはできません。

管理インターフェイスでは、バーンドイン Cisco Wireless LAN Controller ディストリビューション システム MAC アドレスを使用し、さらに、次の項目について設定する必要があります。

- VLAN 割り当て
- 固定 IP アドレス、IP ネットマスク、デフォルト ゲートウェイ
- 物理ポート割り当て
- プライマリ DHCP サーバとセカンダリ DHCP サーバ
- アクセス コントロール リスト（必要な場合）

設定方法は、「管理インターフェイスの確認と変更」の項（P.7-3）を参照してください。

AP マネージャ インターフェイス

論理 AP マネージャ インターフェイスは、Cisco Wireless LAN Controller と Lightweight アクセス ポイント間のレイヤ 3 通信を制御します。

AP マネージャ インターフェイスは、1 つの物理ポートに割り当てられて、管理インターフェイスと同じサブネットおよび物理ポート上に存在することができます。AP マネージャ インターフェイスは、次のように、サービス ポート以外の任意の物理ポートを使用して通信することができます。

- ネットワーク経由でレイヤ 3 メッセージを送信し、他の Cisco Wireless LAN Controller を自動検出して通信を行います。
- レイヤ 3 ネットワークで Lightweight アクセス ポイント LWAPP ポーリング メッセージを受信し、可能な限り多くの Lightweight アクセス ポイントを自動検出して、アソシエートし、通信を行います。

（注）　AP マネージャ インターフェイスを専用のコントローラ サービス ポートに割り当てることはできません。

AP マネージャ インターフェイスでは、次の項目を設定する必要があります。

- VLAN 割り当て
- 固定 IP アドレス（管理インターフェイスの IP アドレスとは別の IP アドレスであるが、管理インターフェイスと同じサブネット上になければならない）、IP ネットマスク、デフォルト ゲートウェイ
- 物理ポート割り当て
- プライマリ DHCP サーバとセカンダリ DHCP サーバ
- アクセス コントロール リスト（必要な場合）

設定方法は、「AP マネージャ インターフェイスの作成および割り当て」の項（P.7-4）を参照してください。

オペレータ定義インターフェイス

すべての Cisco Wireless LAN Controller は、最大 512 のオペレータ定義インターフェイスをサポートできます。各オペレータ定義インターフェイスでは、個々の物理ポートに接続されている Cisco Wireless LAN Controller とその他の全ネットワーク デバイス間の、VLAN とその他の通信を制御します。1 ～ 512 個のオペレータ定義インターフェイスを、無線 LAN、物理ディストリビューション システム ポート、レイヤ 2 管理インターフェイス、およびレイヤ 3 AP マネージャ インターフェイスに割り当てることができます。

（注）　AP マネージャ インターフェイスを専用のコントローラ サービス ポートに割り当てることはできません。

（注）　オペレータ定義インターフェイス名にスペースを含めることはできません。オペレータ定義インターフェイス名にスペースが含まれていると、CLI を使用して設定を編集できなくなる可能性があります。

各オペレータ定義インターフェイスでは、次の項目を設定する必要があります。

- VLAN 番号
- 固定 IP アドレス、IP ネットマスク、デフォルト ゲートウェイ
- 物理ポート割り当て
- プライマリ DHCP サーバとセカンダリ DHCP サーバ
- アクセス コントロール リスト（必要な場合）

設定方法は、「オペレータ定義インターフェイスの作成、割り当て、および削除」の項（P.7-5）を参照してください。

仮想インターフェイス

仮想インターフェイスは、Cisco Wireless LAN Controller のレイヤ 3 Security Manager 通信と Mobility Manager 通信を制御します。このインターフェイスは、DNS ゲートウェイ ホスト名を管理します。このホスト名は、レイヤ 3 Web Auth が有効なときに、レイヤ 3 の Security Manager と Mobility Manager が、証明書の発信元を確認するために使用するものです。

仮想インターフェイスでは、次の項目を設定する必要があります。

- 任意の架空、未割り当て、未使用のゲートウェイ IP アドレス
- DNS ゲートウェイ ホスト名

設定方法は、「仮想インターフェイスの確認と変更」の項（P.7-6）を参照してください。

サービス ポート

Cisco Wireless LAN Controller の物理サービス ポートは、オペレーティング システム デバイス サービス専用の 10/100BASE-T イーサネット ポートで、以前は管理ポートと呼ばれていたものです。サービス ポートは、サービス ポート インターフェイスによって制御されます。

サービス ポートには、管理インターフェイスとは異なる、IP アドレス、サブネット マスク、および IP 割り当てプロトコルを設定します。これにより、オペレータは Cisco Wireless LAN Controller を直接管理したり、10.1.2.x などの専用オペレーティング システム サービス ネットワーク経由で管理できるようになり、ネットワークダウンタイム時のオペレーティング システム デバイス サービスのアクセスが保証されます。

ネットワーク データ ストリームから Cisco Wireless LAN Controller デバイス サービスを削除して、セキュリティを向上させ、より安全なサービス接続を提供するために、Cisco WLAN Solution ではサービス ポートが作成されました。

ゲートウェイをサービス ポートに割り当てることはできないので、サービス ポートはルーティングできないことに注意してください。ただし、ネットワーク管理デバイスへの専用ルートを設定することはできます。

また、サービス ポートは自動認識しません。適切なストレートまたはクロス イーサネット ケーブルを使用して、サービス ポートと通信する必要があります。

サービス ポートの設定方法は、「サービス ポートの設定」の項（P.4-12）を参照してください。

サービス ポート インターフェイス

サービス ポート インターフェイスは、専用 Cisco Wireless LAN Controller サービス ポートを使用した通信を制御します。サービス ポートの詳細は、「サービス ポート」の項（P.1-31）を参照してください。

（注）　サービス ポート インターフェイスは、専用のコントローラ サービス ポートにのみ割り当てることができます。

サービス ポート インターフェイスは、バーンドイン Cisco Wireless LAN Controller サービス ポート MAC アドレスを使用し、さらに、次の項目について設定する必要があります。

- DHCP プロトコルがアクティブ化されているかどうか
- IP アドレスと IP ネットマスク

設定方法は、「サービス ポートの設定」の項（P.4-12）を参照してください。

Startup Wizard

工場出荷の新しいオペレーティング システム ソフトウェアをロードしたときや、工場出荷時のデフォルトにリセットした後で Cisco Wireless LAN Controller の電源を投入すると、起動スクリプトにより Startup Wizard が実行され、初期設定を行うようプロンプトが表示されます。Startup Wizard では、次のことを行います。

- Cisco Wireless LAN Controller に 32 文字以下のシステム名が付いていることを確認します。
- 管理ユーザ名とパスワードを追加します（それぞれ 24 文字以下）。
- Cisco Wireless LAN Controller が、（直接的にまたは間接的に）サービス ポートを使用して、CLI、Cisco WCS、または Web ユーザ インターフェイスと通信可能であることを確認します。これは、有効な IP 設定プロトコル（none または DHCP）を受け取ることで、また none の場合は、IP アドレスとネットマスクを受け取ることで確認します。サービス ポートを使用しない場合、IP アドレスおよびネットマスクは 0.0.0.0 と入力します。
- Cisco Wireless LAN Controller が管理インターフェイスでネットワーク（802.11 ディストリビューション システム）と通信できることを確認します。これは、有効な固定 IP アドレス、ネットマスク、デフォルトのルータ IP アドレス、VLAN 識別子、および物理ポート割り当てを収集することで確認します。
- DHCP サーバの IP アドレスを入力するよう求めます。これは、クライアント、Cisco Wireless LAN Controller 管理インターフェイス、およびオプションでサービス ポート インターフェイスに IP アドレスを指定する際に使用されます。
- LWAPP 転送モードを問い合わせます。これについては、「レイヤ 2 およびレイヤ 3 の Lightweight Access Point protocol（LWAPP）動作」の項（P.1-8）を参照してください。
- 仮想ゲートウェイ IP アドレスを収集します。これは、任意の架空、未割り当てのゲートウェイ IP アドレス（1.1.1.1 など）で、レイヤ 3 Security Manager と Mobility Manager で使用されます。
- ユーザがモビリティ グループ（RF グループ）名を入力できるようにします。
- 無線 LAN 1 802.11 SSID またはネットワーク名を収集します。
- クライアントが固定 IP アドレスを使用できるようにするかどうかを指定するよう求めます。Yes に設定すると使い勝手は良くなりますが、セキュリティが低下します（セッションがハイジャックされる可能性がある）。クライアントが自分自身の IP アドレスを指定できるので、DHCP を使用できないデバイスに適した設定です。No に設定すると使い勝手は悪くなりますが、セキュリティが向上します。クライアントが IP アドレスの DHCP を指定する必要があるため、Windows XP デバイスに適した設定です。

- Startup Wizard から RADIUS サーバを設定する必要がある場合は、RADIUS サーバの IP アドレス、通信ポート、および秘密鍵の入力を求めます。
- 国番号を収集します
- 802.11a、802.11b、および 802.11g Cisco 1000 シリーズ Lightweight アクセス ポイント ネットワークを有効または無効にします。
- Radio Resource Management（RRM）を有効または無効にします。

Startup Wizard の使用方法は、「Configuration Wizard の使用方法」の項（P.4-2）を参照してください。

Cisco Wireless LAN Controller のメモリ

Cisco Wireless LAN Controller には 2 種類のメモリがあります。揮発性 RAM には、現在のアクティブな Cisco Wireless LAN Controller 設定が保持され、NVRAM にはリブート設定が保持されます。Cisco Wireless LAN Controller のオペレーティング システムを設定している場合は、揮発性 RAM を編集しているため、その設定を揮発性 RAM から NVRAM に保存して、確実に Cisco Wireless LAN Controller が現在の設定で再度ブートされるようにする必要があります。

次の処理を行うときは、どちらのメモリを編集しているか理解していることが重要となります。

- Configuration Wizard の使用方法
- コントローラ設定のクリア
- 設定の保存
- コントローラのリセット
- CLI からのログアウト

Cisco Wireless LAN Controller のフェールオーバーの保護

すべての Cisco Wireless LAN Controller には、Cisco 1000 シリーズ Lightweight アクセス ポイント用の通信ポートが、定義された数だけ装備されています。つまり、未使用のアクセス ポイント ポートがある複数のコントローラが同じネットワーク上に展開されている場合、1 つのコントローラが故障すると、ドロップしたアクセス ポイントは、自動的に未使用のコントローラ ポートをポーリングして、そのポートにアソシエートします。

インストール時に、すべての Lightweight アクセス ポイントを専用のコントローラに接続して、最終的な作業として各 Lightweight アクセス ポイントを設定することをお勧めします。この手順では、プライマリ、セカンダリ、ターシャリ コントローラについてそれぞれの Lightweight アクセス ポイントを設定し、設定した WLAN Solution モビリティ グループ情報を格納できるようにします。

フェールオーバー回復時に、設定した Lightweight アクセス ポイントが、ローカル DHCP サーバから IP アドレスを取得し（レイヤ 3 動作でのみ）、プライマリ、セカンダリ、ターシャリ コントローラへの接続を試み、次にモビリティ グループ内のその他のコントローラの IP アドレスへの接続を試みます。これにより、アクセス ポイントがブラインド ポーリング メッセージを送信する時間が必要なくなるため、結果的に回復期間が短縮されます。

マルチコントローラ展開では、1 つのコントローラが故障すると、ドロップしたアクセス ポイントが再度ブートされて、Radio Resource Management（RRM）の指示の下で次の処理が行われます。

- ローカル DHCP サーバ（ローカル サブネット上にあるサーバ）の IP アドレスを取得します。
- Cisco 1000 シリーズ Lightweight アクセス ポイントは、プライマリ、セカンダリ、またはターシャリ コントローラが割り当てられている場合、そのコントローラにアソシエートを試みます。

- アクセス ポイントにプライマリ、セカンダリ、ターシャリ コントローラが割り当てられていない場合、またはプライマリ、セカンダリ、ターシャリ コントローラが使用できない場合には、同一サブネット上のマスター コントローラにアソシエートを試みます。
- アクセス ポイントが同一サブネット上でマスター コントローラを検出できなかった場合は、格納されているモビリティ グループ メンバに IP アドレスで接続を試みます。
- 使用できるモビリティ グループ メンバがない場合、および Cisco 1000 シリーズ Lightweight アクセス ポイントにプライマリ、セカンダリ、ターシャリ Cisco Wireless LAN Controller が割り当てられておらず、アクティブなマスター Cisco Wireless LAN Controller がない場合には、Cisco 1000 シリーズ Lightweight アクセス ポイントは、同一サブネット上で最も負荷の少ない Cisco Wireless LAN Controller にアソシエートを試みて、未使用ポートを使ったそのディスカバリ メッセージに応答します。

つまり、十分なコントローラが展開されている場合には、1 つのコントローラが故障したとしても、アクティブなアクセス ポイントのクライアント セッションがただちにドロップする一方で、ドロップしたアクセス ポイントが別のコントローラの未使用ポートにアソシエートするため、クライアント デバイスはすぐに再アソシエートと再認証を行うことができます。

Cisco Wireless LAN Controller の自動時刻設定

すべてのコントローラは、手作業で時刻を設定したり、1 つまたは複数の Network Time Protocol（NTP; ネットワーク タイム プロトコル）サーバから現在時刻を取得するよう設定することができます。各 NTP サーバの IP アドレスは、コントローラ データベースに追加されています。すべてのコントローラは NTP サーバを検索して、リブート時およびユーザ定義ポーリング間隔ごとに（毎日から毎週）、現在時刻を取得できます。

Cisco Wireless LAN Controller の時間帯

すべての Cisco Wireless LAN Controller は、手作業で時間帯を設定したり、1 つまたは複数の ネットワーク タイム プロトコル（NTP）サーバから現在の時間帯を取得するよう設定することができます。各 NTP サーバの IP アドレスは、Cisco Wireless LAN Controller データベースに追加されています。すべての Cisco Wireless LAN Controller は、NTP サーバを検索して、リブート時およびユーザ定義ポーリング間隔ごとに（毎日から毎週）、現在の時間帯を取得できます。

Cisco Wireless LAN Controller へのネットワーク接続

すべての Cisco Wireless LAN Controller は、動作モードに関係なく、ネットワークを 802.11 ディストリビューション システムとして使用します。Cisco Wireless LAN Controller は、イーサネット ポートのタイプや速度に関係なく、関連付けられている Cisco Wireless LAN Controller の監視と通信をネットワークを使用して行います。以降の項では、次のネットワーク接続について説明します。

- Cisco 2000 シリーズ Wireless LAN Controller（P. 1-25）
- Cisco 4100 シリーズ Wireless LAN Controller（P. 1-25）
- Cisco 4400 シリーズ Wireless LAN Controller（P. 1-26）

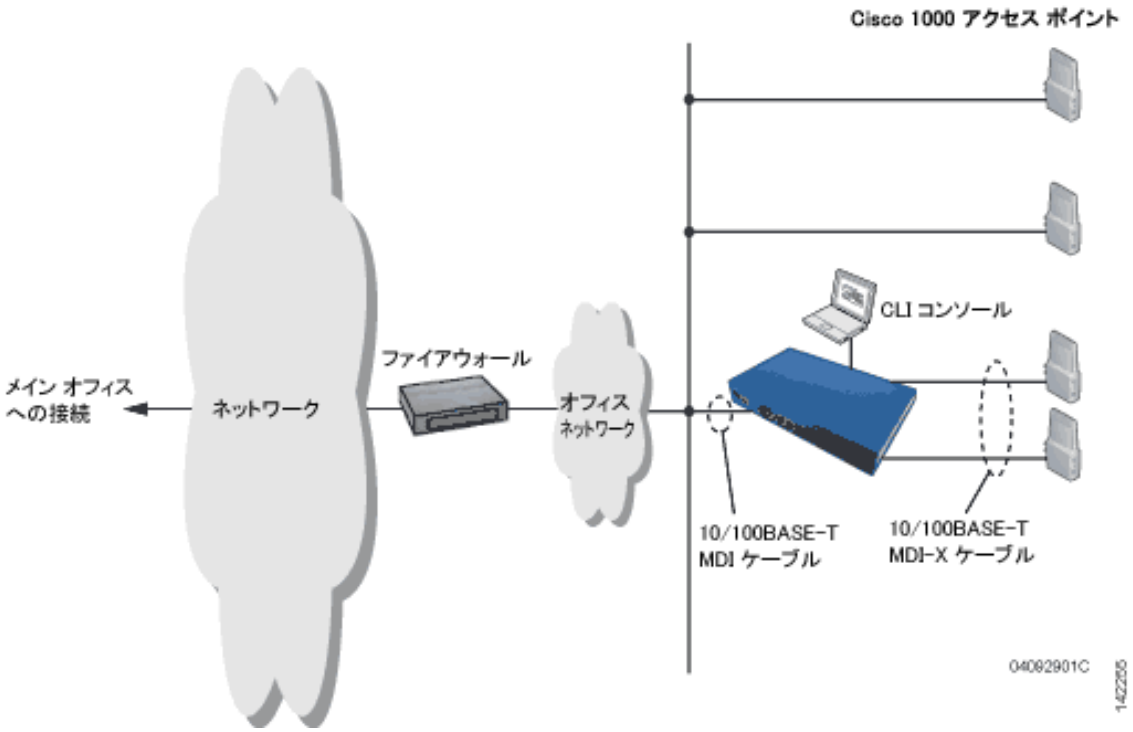
Cisco 2000 シリーズ Wireless LAN Controller

論理管理インターフェイスは 1 つの物理ポートに割り当てることができるため、Cisco 2000 シリーズ Wireless LAN Controller は、いずれか 1 つの物理ポートを使用してネットワークと通信できます。物理ポートの説明は次のとおりです。

- 最大 4 つの 10/100BASE-T ケーブルを、Cisco 2000 シリーズ Wireless LAN Controller シャーシの 4 つの背面パネル コネクタに接続できます。

図 1-6 は、2000 シリーズ コントローラへの接続を示しています。

図 1-6　2000 シリーズ コントローラへの物理ネットワーク接続



Cisco 4100 シリーズ Wireless LAN Controller

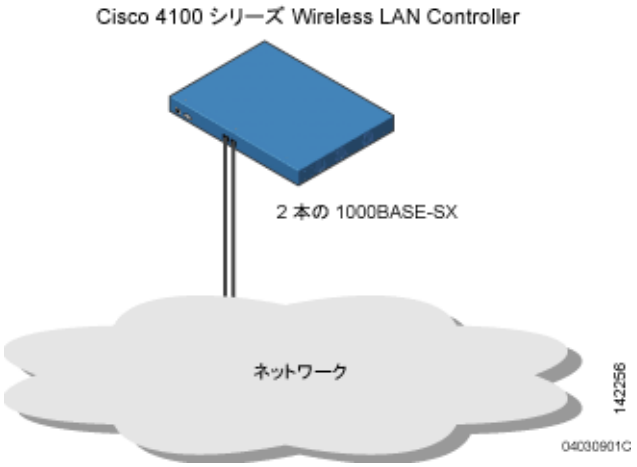
Cisco 4100 シリーズ Wireless LAN Controller は、１ つまたは 2 つの物理ポートを使ってネットワークと通信でき、論理管理インターフェイスを １ つまたは 2 つの物理ポートに割り当てることができます。物理ポートの説明は次のとおりです。

- 2 本のギガビット イーサネット 1000BASE-SX 光ファイバ ケーブルを Cisco 4100 シリーズ Wireless LAN Controller 前面の LC コネクタに接続できます。これは、同一サブネットに接続しなければなりません。2 つのギガビット イーサネット ポートは冗長構成になっており、最初にアクティブになるポートがマスターで、他方のポートがバックアップ ポートになります。最初の接続に失敗すると、スタンバイ接続がマスター ポートになり、失敗した接続がバックアップ ポートになります。

（注）　1000BASE-SX 回線は、LC 物理コネクタを使用した 850nM（SX）光ファイバ リンクで 100Mbps または 1000Mbps の有線接続をネットワークに提供します。

図 1-7 は、4100 シリーズ コントローラへの接続を示しています。

図 1-7　4100 シリーズ コントローラへの物理ネットワーク接続



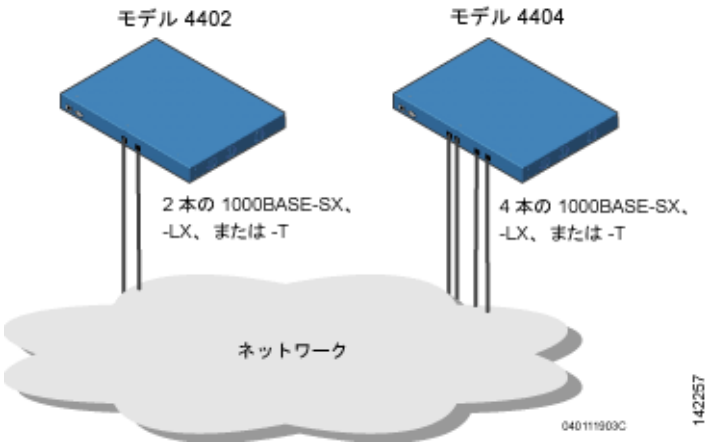
Cisco 4400 シリーズ Wireless LAN Controller

Cisco 4400 シリーズ Wireless LAN Controller は、1 つまたは 2 つの物理ポート ペアを使ってネットワークと通信でき、論理管理インターフェイスを物理ポートに割り当てることができます。物理ポートの説明は次のとおりです。

- 4402 Cisco Wireless LAN Controller では、次の接続のうち、2 つまでの接続が任意の組み合わせでサポートされます。
  - 1000BASE-T（ギガビット イーサネット、前面パネル、RJ-45 物理ポート、UTP ケーブル）
  - 1000BASE-SX（ギガビット イーサネット、前面パネル、LC 物理ポート、LC 物理コネクタを使用したマルチモード 850nM（SX）光ファイバ リンク）
  - 1000BASE-LX（ギガビット イーサネット、前面パネル、LC 物理ポート、LC 物理コネクタを使用したマルチモード 1300nM（LX/LH）光ファイバ リンク）
- 4404 Cisco Wireless LAN Controller では、次の接続のうち、4 つまでの接続が任意の組み合わせでサポートされます。
  - 1000BASE-T（ギガビット イーサネット、前面パネル、RJ-45 物理ポート、UTP ケーブル）
  - 1000BASE-SX（ギガビット イーサネット、前面パネル、LC 物理ポート、LC 物理コネクタを使用したマルチモード 850nM（SX）光ファイバ リンク）
  - 1000BASE-LX（ギガビット イーサネット、前面パネル、LX 物理ポート、LC 物理コネクタを使用したマルチモード 1300nM（LX/LH）光ファイバ リンク）

図 1-8 は、4400 シリーズ コントローラへの接続を示しています。

図 1-8　4402 および 4404 シリーズ コントローラへの物理ネットワーク接続



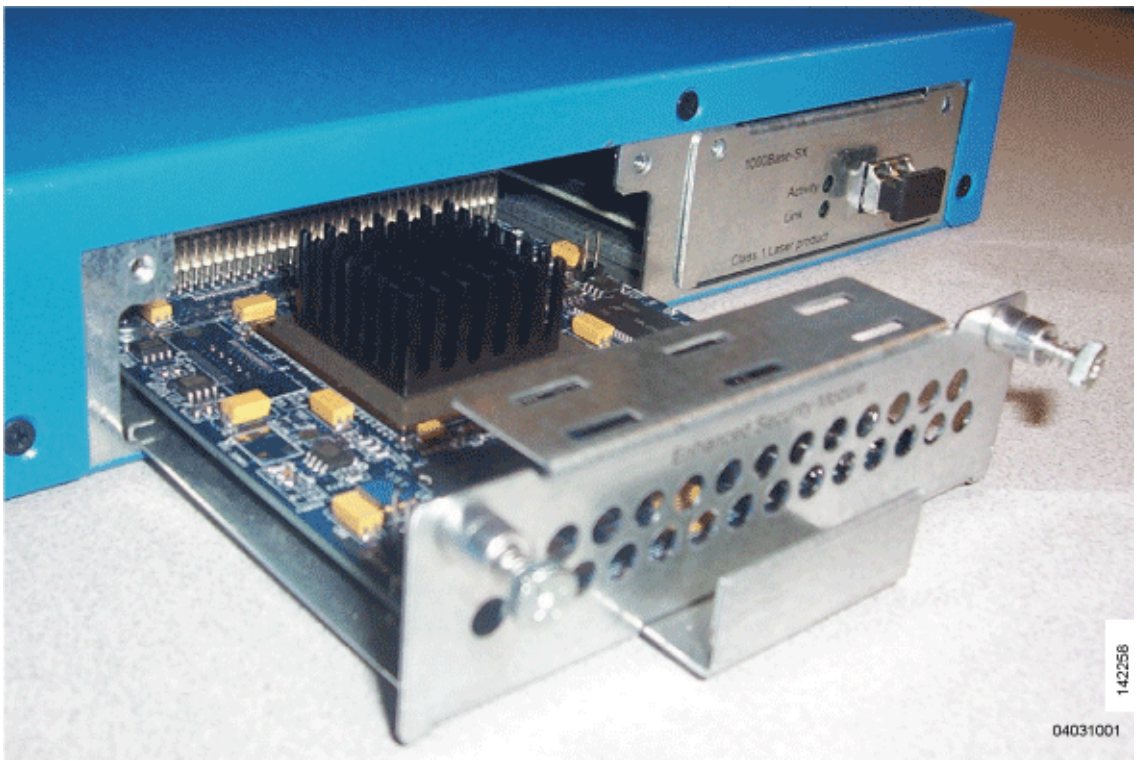
Cisco 4100 シリーズ Wireless LAN Controller VPN/ 拡張セキュリティ モジュール

すべての Cisco 4100 シリーズ Wireless LAN Controller には、オプションの VPN/ 拡張セキュリティ モジュール（AIR-VPN-4100）を、背面パネルに装着することができます。VPN/ 拡張セキュリティ モジュールにより、Cisco 4100 シリーズ Wireless LAN Controller のハードウェア暗号化が大幅に加速され、管理インターフェイスを使用して次の操作が可能になります。

- 組み込み VPN サーバでのミッションクリティカルなトラフィックの実行
- レイヤ 2 およびレイヤ 3 暗号化を有効にした状態での、最大 1Gbps のスループットの維持
- 高速なプロセッサ集中型暗号化（L2TP、IPSec、3DES など）のサポート

図 1-9 は、Cisco 4100 シリーズ Wireless LAN Controller の背面に VPN/ 拡張セキュリティ モジュールをスライドさせて装着しているところを示しています。

図 1-9　4100 シリーズ コントローラの VPN/ 拡張セキュリティ モジュール ロケーション



Lightweight アクセス ポイント

この項では、Cisco Lightweight アクセス ポイントについて説明します。

Cisco 1000 シリーズ IEEE 802.11a/b/g Lightweight アクセス ポイント

Cisco 1000 シリーズ Lightweight アクセス ポイントは、革新的な Cisco Wireless LAN Solution を構成するコンポーネントの 1 つです。Cisco 1000 シリーズ Lightweight アクセス ポイントは、以降で説明するようにコントローラとアソシエートすると、見た目も美しいプレナム定格の筐体 1 つで、高度な 802.11a と 802.11b/g アクセス ポイント機能を提供します。図 1-10 は、外部アンテナ用のコネクタが装着されているタイプと装着されていないタイプの 2 種類の Cisco 1000 シリーズ IEEE 802.11a/b/g Lightweight アクセス ポイントを示しています。

図 1-10　1000 シリーズ Lightweight アクセス ポイント

Cisco WLAN Solution では、802.11a/b/g Cisco 1030 リモート エッジ Lightweight アクセス ポイントも提供しています。これは、リモート展開用、つまり WAN リンクによる Radio Resource Management（RRM）制御のために設計されている Cisco 1000 シリーズ Lightweight アクセス ポイントであり、外部アンテナ用のコネクタが付属しています。

Cisco 1000 シリーズ Lightweight アクセス ポイントは、ほとんどの環境に溶け込む中間色仕上げになっていますが、塗装することもできます。また、Cisco 1000 シリーズ Lightweight アクセス ポイントには、単方向性（180 度）または全方向性（360 度）カバレッジ用の高ゲイン内部アンテナがペアで付属しており、天井裏に取り付ける場合のプレナム定格にも適合しています。

Cisco Wireless LAN Solution では、従来 SOHO（スモール オフィス、ホームオフィス）のアクセス ポイントで行わなければならなかった処理の大部分を Cisco Wireless LAN Controller に任せます。

Cisco 1030 リモート エッジ Lightweight アクセス ポイント

Cisco Wireless LAN Controller が継続して制御する Lightweight アクセス ポイントの一般ルールで唯一の例外は、Cisco 1030 IEEE 802.11a/b/g リモート エッジ Lightweight アクセス ポイントです（Cisco 1030 リモート エッジ Lightweight アクセス ポイント）。Cisco 1030 リモート エッジ Lightweight アクセス ポイントはリモート サイトでの設置を目的としており、Cisco Wireless LAN Controller で初期設定され、通常は Cisco Wireless LAN Controller で制御されます。

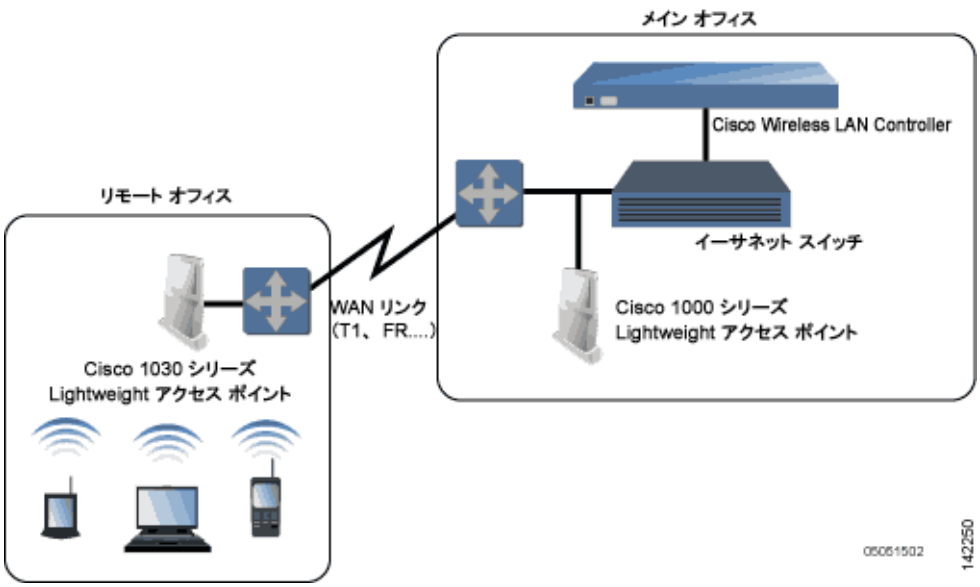
ただし、Cisco 1030 リモート エッジ Lightweight アクセス ポイントはクライアント データをブリッジするので（すべてのクライアント データをそれぞれの Cisco Wireless LAN Controller 経由で受け渡しする他の Cisco 1000 シリーズ Lightweight アクセス ポイントと比較して）、Cisco 1030 リモート エッジ Lightweight アクセス ポイントとその Cisco Wireless LAN Controller 間で WAN リンクが切断された場合、Cisco 1030 リモート エッジ Lightweight アクセス ポイント は、ローカル サブネット上の他の Cisco 1030 リモート エッジ Lightweight アクセス ポイントを経由して無線 LAN 1 クライアント データの送信を続けます。また、通信が再び確立されるまで、VLAN の新規設定などの Cisco Wireless LAN Controller からアクセスする機能は利用できません。

Cisco 1030 リモート エッジ Lightweight アクセス ポイントには、従来の SOHO（スモール オフィス、ホームオフィス）AP 処理能力が搭載されているので、そのアソシエートされている Cisco Wireless LAN Controller への WAN リンクに失敗した場合も、継続して動作することができます。Cisco 1030 リモート エッジ Lightweight アクセス ポイントは、そのアソシエートされている Cisco Wireless LAN Controller によって設定されるため、他の Cisco Wireless LAN Solution と同じ無線 LAN 設定になります。Cisco Wireless LAN Controller に接続されている間は、RRM の制御下で転送出力とチャネル選択を変更し、他の Cisco 1000 シリーズ Lightweight アクセス ポイントと同じ不正なアクセス ポイントのロケーションを実行します。

Cisco 1030 リモート エッジ Lightweight アクセス ポイントは、Cisco Wireless LAN Controller に接続されている間は、複数の無線 LAN をサポートできます。ただし、Cisco Wireless LAN Controller との接続を失うと、サポートするのは、ローカル サブネット上の 1 つの無線 LAN のみになります。

図 1-11 は、一般的な Cisco 1030 リモート エッジ Lightweight アクセス ポイント設定を示しています。

図 1-11　一般的な 1030 シリーズ Lightweight アクセス ポイントの設定



Cisco 1030 リモート エッジ Lightweight アクセス ポイントは、リブート時に IP アドレスを取得できるように、ローカル サブネット上の DHCP サーバを使用可能にしておく必要があります。また、リモート ロケーションにある Cisco 1030 リモート エッジ Lightweight アクセス ポイントがクライアント ローミングを行うには、同一サブネット上になければならないことにも注意してください。

Cisco 1000 シリーズ Lightweight アクセス ポイントの製品番号

Cisco 1000 シリーズ Lightweight アクセス ポイントには、802.11a と 802.11b/g の無線機能がそれぞれ 1 つ搭載されています。Cisco 1000 シリーズ Lightweight アクセス ポイントは、次の設定で提供されています。

- AIR-AP1010-A-K9、AIR-AP1010-C-K9、AIR-AP1010-E-K9、AIR-AP1010-J-K9、AIR-AP1010-N-K9、および AIR-AP1010-S-K9：AP1010 Cisco 1000 シリーズ Lightweight アクセス ポイントに高ゲイン内部アンテナが 4 つ付属し、外部アンテナ アダプタは含まれていません。
- AIR-AP1020-A-K9、AIR-AP1020-C-K9、AIR-AP1020-E-K9、AIR-AP1020-J-K9、AIR-AP1020-N-K9、および AIR-AP1020-S-K9：AP1020 Cisco 1000 シリーズ Lightweight アクセス ポイントに高ゲイン内部アンテナが 4 つ、5GHz 外部アンテナ アダプタが 1 つ、2.4GHz 外部アンテナ アダプタが 2 つ付属しています。
- AIR-AP1030-A-K9、AIR-AP1030-C-K9、AIR-AP1030-E-K9、AIR-AP1030-J-K9、AIR-AP1030-N-K9、および AIR-AP1030-S-K9：AP1030 Cisco 1000 シリーズ Lightweight アクセス ポイント（Cisco 1030 リモート エッジ Lightweight アクセス ポイント）に高ゲイン内部アンテナが 4 つ、5GHz 外部アンテナ アダプタが 1 つ、2.4GHz 外部アンテナ アダプタが 2 つ付属しています。

サポート対象の規制区域は、付録 D 「Cisco WLAN Solution でサポートされている国番号」を参照してください。

Cisco 1000 シリーズ Lightweight アクセス ポイントには、カラーコーディネートされた天井マウント ベースおよび天井吊り下げレール クリップが付属しています。プロジェクション マウントおよびフラッシュ マウント用シート メタル壁面取り付けブラケット キットを別途注文することもできます。ベース、クリップ、およびオプションのブラケットを使用すると、簡単に天井や壁に取り付けできます。

Cisco 1000 シリーズ Lightweight アクセス ポイントは、Power Over Ethernet や外部電源装置から電源供給を受けることができます。外部電源モデルには次のものがあります。

- AIR-PWR-1000：すべての Cisco 1000 シリーズ Lightweight アクセス ポイントに対応する、オプションの外部電源装置（110 ～ 220VAC から 48VDC）

シングル インライン PoE インジェクタ モデルには次のものがあります。

- AIR-PWRINJ-1000AF：すべての Cisco 1000 シリーズ Lightweight アクセス ポイントに対応し、90 ～ 250VAC の電源で稼働する、オプションのシングル 802.3af インライン Power over Ethernet インジェクタ

プロジェクションおよびフラッシュ シート メタル壁面取り付けブラケット モデルには次のものがあります。

- AIR-ACC-WBRKT1000：すべての Cisco 1000 シリーズ Lightweight アクセス ポイントに対応する、オプションのシート メタル壁面取り付けブラケット キット。キットには、プロジェクション マウント用とフラッシュ マウント用のブラケットが 1 つずつ入っています。

Cisco 1000 シリーズ Lightweight アクセス ポイントの外部アンテナと内部アンテナ

Cisco 1000 シリーズ Lightweight アクセス ポイントの筐体には、1 つの 802.11a または 802.11b/g 無線、4 つの高ゲイン アンテナ（802.11a と 802.11b/g それぞれ 2 つ）が装備されています。これらは、別々に有効または無効にして、180 度のセクター化カバレッジ領域または 360 度の全方向性カバレッジ領域を生成することができます。

（注）　Cisco 1000 シリーズ Lightweight アクセス ポイントでは、FCC 要件に違反して、機器を操作するユーザの権利が無効になることがないように、付属している内部アンテナまたは外部アンテナを使用してください。

無線 LAN オペレータは、Cisco 1000 シリーズ Lightweight アクセス ポイントの内部アンテナ ペアのいずれか 1 つを無効にすれば、180 度のセクター化カバレッジ領域を生成することができます。たとえば、ビルディング内部のみにカバレッジが求められる屋外壁面取り付け場所や、ある一定の領域で 2 倍のクライアントを許可できるバックツーバック配置で、この機能は役立ちます。

アンテナ パターンは、付録 E 「1000 シリーズ アクセス ポイントのアンテナ パターン」を参照してください。

外部アンテナ コネクタ

AP1020 および AP1030 Cisco 1000 シリーズ Lightweight アクセス ポイントには、オスの逆極性 TNC ジャックが装備されており、これは付属している外部方向アンテナまたは高ゲイン アンテナを設置する際に必要となります。外部アンテナ オプションを使用すると、Cisco 1000 シリーズ Lightweight アクセス ポイントのアンテナをより柔軟に配置できます。

（注）　AP1010 Cisco 1000 シリーズ Lightweight アクセス ポイントは内部高ゲイン アンテナに限定して使用するよう設計されているため、外部アンテナ用ジャックは付いていません。

802.11b/g 2.4GHz の Left 外部アンテナ コネクタは、内部 Side A アンテナに対応し、2.4GHz の Right 外部アンテナ コネクタは、内部 Side B アンテナに対応しています。802.11b/g ダイバーシティを有効にした場合、Left 外部アンテナや Side A 内部アンテナは、Right 外部アンテナや Side B 内部アンテナと異なることに注意してください。

また、802.11a 5GHz の Left 外部アンテナ コネクタは、内部アンテナとは分離しており、802.11a の送受信パスにダイバーシティを追加することにも注意してください。外部 802.11a アンテナは、FCC 規制領域で認可されていませんが、他の国での使用が認可される可能性があります。

アンテナのセクター化

Cisco WLAN Solution は、アンテナのセクター化をサポートしています。これは、所定の空間で、クライアント数やクライアントのスループットを増大させるときに使用できます。設置担当者が 2 つの Cisco 1000 シリーズ Lightweight アクセス ポイントをバックツーバックで取り付けて、ネットワーク オペレータが両方のアクセス ポイントの 2 つ目のアンテナを無効にすると、2 つのセクターを持つ 360 度のカバレッジ領域を作成できます。

設置担当者は、ビルディングの周辺に Cisco 1000 シリーズ Lightweight アクセス ポイントを取り付けて、Side B 内部アンテナを無効にすることもできます。この設定を使用すると、内部アンテナのダイバーシティ機能を削除するだけで、カバレッジを駐車場にまで拡張することなく、ビルディング内部に対してサービスを提供できます。

1000 シリーズ Lightweight アクセス ポイントの内部アンテナの輻射パターンは、内部アンテナ パターンに関する付録 E を参照してください。

Cisco 1000 シリーズ Lightweight アクセス ポイント の LED

すべての Cisco 1000 シリーズ Lightweight アクセス ポイントの本体上部に 4 つの LED が取り付けられています。これらの LED は、ほぼどの角度からも確認できます。LED は、電源と障害のステータス、2.4GHz（802.11b/g）Cisco Radio アクティビティ、および 5GHz（802.11a）Cisco Radio アクティビティを示します。

この LED 表示によって、無線 LAN 管理者は簡単に Cisco 1000 シリーズ Lightweight アクセス ポイントのステータスを監視できます。トラブルシューティング方法の詳細は、エラー メッセージとアクセス ポイントの LED に関する付録を参照してください。

Cisco 1000 シリーズ Lightweight アクセス ポイントのコネクタ

AP1020 および AP1030 Cisco 1000 シリーズ Lightweight アクセス ポイントには、次の外部コネクタが付いています。

- RJ-45 イーサネット ジャック 1 つ。Cisco 1000 シリーズ Lightweight アクセス ポイントをネットワークに接続するときに使用します。
- 48VDC 電源入力ジャック 1 つ。付属しているオプションの外部電源アダプタを接続するときに使用します。
- オスの逆極性 TNC アンテナ ジャック 3 つ。オプションの外部アンテナを Cisco 1000 シリーズ Lightweight アクセス ポイントに接続するときに使用します。2 つが 802.11b/g 無線用で、1 つが 802.11a 無線用です。

（注）　AP1010 Cisco 1000 シリーズ Lightweight アクセス ポイントは内部高ゲイン アンテナに限定して使用するよう設計されているため、外部アンテナ用ジャックは付いていません。

Cisco 1000 シリーズ Lightweight アクセス ポイントは、標準の CAT-5（カテゴリ 5）以上の 10/100Mbps ツイストペア ケーブルを RJ-45 コネクタに接続して、Cisco Wireless LAN Controller と通信します。CAT-5 ケーブルは、Cisco 1000 シリーズ Lightweight アクセス ポイント側面の RJ-45 ジャックに差し込んでください。

Cisco 1000 シリーズ Lightweight アクセス ポイントは、CAT-5 ケーブルを使ってネットワーク機器から電力を受け取ることができます。このオプションの詳細は、Power over Ethernet を参照してください。

Cisco 1000 シリーズ Lightweight アクセス ポイントは、付属しているオプションの外部電源アダプタ（AC から 48 VDC）から電力供給を受けることができます。外部アダプタを使用して Cisco 1000 シリーズ Lightweight アクセス ポイントに電力を供給する場合は、電源アダプタを Cisco 1000 シリーズ Lightweight アクセス ポイント側面の 48VDC 電源ジャックに差し込んでください。

Cisco 1000 シリーズ Lightweight アクセス ポイントには、全方向性カバレッジを提供する、それぞれ 2 つの 802.11a と 802.11b/g 高ゲイン内部アンテナが装備されています。しかし、一部の Cisco 1000 シリーズ Lightweight アクセス ポイントでは、付属しているオプションの高ゲイン アンテナや

方向性アンテナを使用することもできます。外部アンテナを使用している場合は、AP1020 および AP1030 Cisco 1000 シリーズ Lightweight アクセス ポイントの側面にあるオスの逆極性 TNC ジャックに接続します。

（注）　Cisco 1000 シリーズ Lightweight アクセス ポイントでは、FCC 要件に違反して、機器を操作するユーザの権利が無効になることがないように、付属している内部アンテナまたは外部アンテナを使用してください。

Cisco 1000 シリーズ Lightweight アクセス ポイントの所要電力

すべての Cisco 1000 シリーズ Lightweight アクセス ポイントには、7W の電力供給が可能な公称 48VDC（38 ～ 57VDC）電源が必要です。Cisco 1000 シリーズ Lightweight アクセス ポイントでは公称電源 +48VDC と -48 VDC の両方を使用できるため、DC 電源の極性はどちらでもかまいません。

Cisco 1000 シリーズ Lightweight アクセス ポイントは、アクセス ポイント本体の側面に接続された外部電源装置 (110-220 VAC 電源より給電)、または Power over Ethernet から電力供給を受けることができます。

Cisco 1000 シリーズ Lightweight アクセス ポイントの外部電源装置

Cisco 1000 シリーズ Lightweight アクセス ポイントは、外部電源装置（110 ～ 220VAC、48VDC）、または Power Over Ethernet 機器から電力供給を受けることができます。

外部電源装置（AIR-PWR-1000）は、安全な 110 ～ 220VAC コンセントに接続します。コンバータを使用すると、Cisco 1000 シリーズ Lightweight アクセス ポイントに必要な 48VDC の出力が得られます。コンバータの出力は、48VDC ジャックを通して Cisco 1000 シリーズ Lightweight アクセス ポイント側面コネクタに送られます。

AIR-PWR-1000 外部電源は、国別仕様に適合した電源コードとともに別途ご注文いただけます。適合する電源コードを注文されるときは、シスコにお問い合わせください。

Cisco 1000 シリーズ Lightweight アクセス ポイントの取り付けオプション

Cisco 1000 シリーズ Lightweight アクセス ポイント取り付けオプションは、『Internal-Antenna AP1010 Cisco 1000 シリーズ IEEE 802.11a/b/g Lightweight アクセス ポイント Quick Start Guide』または『External-Antenna AP1020 and AP1030 Cisco 1000 シリーズ IEEE 802.11a/b/g Lightweight アクセス ポイント Quick Start Guide』を参照してください。

Cisco 1000 シリーズ Lightweight アクセス ポイントの物理的なセキュリティ

Cisco 1000 シリーズ Lightweight アクセス ポイントの筐体側面には、Kensington MicroSaver セキュリティ ケーブル用のスロットが付いています。Kensington 社製セキュリティ製品の詳細は、Kensington の Web サイトを参照してください。取り付け方法は、『Internal-Antenna AP1010 Cisco 1000 シリーズ IEEE 802.11a/b/g Lightweight アクセス ポイント Quick Start Guide』または『External-Antenna AP1020 and AP1030 Cisco 1000 シリーズ IEEE 802.11a/b/g Lightweight アクセス ポイント Quick Start Guide』を参照してください。

Cisco 1000 シリーズ Lightweight アクセス ポイントの監視モード

Cisco 1000 シリーズ Lightweight アクセス ポイントと Cisco Wireless LAN Controller は、通常稼働中に、不正なアクセス ポイントを検出して阻止することができます。不正なアクセス ポイントの検出は、選択している国番号に関係なく、すべて 801.11 チャネルを使用して行われます（詳細は、付録 D 「Cisco WLAN Solution でサポートされている国番号」を参照してください）。

ただし、管理者が特定の Cisco 1000 シリーズ Lightweight アクセス ポイントの不正なアクセス ポイントの検出と阻止を実行したい場合は、個々の Cisco 1000 シリーズ Lightweight アクセス ポイントについて監視モードを有効にする必要があります。

監視機能は、Cisco Wireless LAN Controller ユーザ インターフェイスを使用して、アクセス ポイントごとにすべての 802.11 Cisco Radio に対して設定します。

コントローラ ディスカバリとしての DNS の使用

Cisco Wireless LAN Solution ソフトウェア リリース 3.0 以降では、アクセス ポイントは Domain Name Server（DNS; ドメイン ネーム サーバ）を介してコントローラを検出できます。この機能を使用するには、CISCO-LWAPP-CONTROLLER@< ローカル ドメイン > への応答としてコントローラの IP アドレスを返すように DNS を設定します。アクセス ポイントは DHCP サーバから IP アドレスと DNS 情報を受け取ると、DNS に問い合わせて CISCO-LWAPP-CONTROLLER@< ローカル ドメイン > を解決します。DNS がコントローラ IP アドレスのリストを送信すると、アクセス ポイントはディスカバリ要求をコントローラに送信します。

Autonomous アクセス ポイントの Lightweight モードへの変換

アップグレード変換ツールを使用して、Autonomous Cisco Aironet 1130AG、1200 および 1240AG シリーズ アクセス ポイントを Lightweight モードに変換することができます。これらのいずれかのアクセス ポイントを Lightweight モードに変換した場合、アクセス ポイントは無線 LAN コントローラと通信し、コントローラから設定とソフトウェア イメージを受信します。

Autonomous アクセス ポイントを Lightweight モードに変換する詳しい手順は、次のドキュメントを参照してください。

- *Release Notes for Cisco Aironet 1130AG, 1200, and 1240AG Series Access Points for Cisco IOS Release 12.3(7)JX*
- *Application Note: Upgrading Autonomous Cisco Aironet Access Points to Lightweight Mode*

Lightweight モードに変換したアクセス ポイントの使用に関するガイドライン

Autonomous アクセス ポイントを Lightweight モードに変換した場合に留意すべきガイドラインを次に示します。

- 変換したアクセス　ポイントは、2006 および　4400　コントローラのみをサポートします。Autonomous アクセス ポイントを Lightweight モードに変換した場合、アクセス ポイントは Cisco 2006 シリーズ無線 LAN コントローラおよび 4400 シリーズ コントローラとのみ通信できます。Cisco IOS ソフトウェアを実行するアクセス ポイントをサポートするのに必要なメモリが足りないため、Cisco 4100 シリーズ、Airespace 4012 シリーズ、および Airespace 4024 シリーズ コントローラはサポートされません。
- Lightweight モードに変換したアクセス ポイントは、Wireless Domain Service（WDS; 無線ドメイン サービス）をサポートしません。変換したアクセス ポイントは、Cisco 無線 LAN コントローラとのみ通信し、WDS デバイスとは通信できません。ただし、アクセス ポイントがコントローラにアソシエートする際、コントローラが WDS に相当する機能を提供します。
- LWAPP モードに変換したアクセス ポイントは、無線ごとに 8 の BSSID とアクセス ポイントごとに合計 8 の無線 LAN をサポートします（Cisco 1000 シリーズ アクセス ポイントは、無線ごとに 16 の BSSID とアクセス ポイントごとに 16 の無線 LAN をサポートします）。変換したアクセス ポイントがコントローラにアソシエートすると、1 から 8 の ID を持つ無線 LAN のみがアクセス ポイントにプッシュされます。
- Lightweight モードに変換したアクセス ポイントは、レイヤ 2 LWAPP をサポートしません。Lightweight モードに変換されたアクセス ポイントは、DHCP、DNS、または IP サブネット ブロードキャストを使用して IP アドレスを取得し、コントローラを検出する必要があります。
- アクセス ポイントが Lightweight モードに変換された後、コンソール ポートは装置への読み取り専用アクセスを提供します。

Lightweight モードから Autonomous モードへの復帰

アップグレード ツールで Autonomous アクセス ポイントを Lightweight モードに変換した後、Autonomous モードをサポートする Cisco IOS リリース（Cisco IOS リリース 12.3(7)JA 以前）をロードすることによって、アクセス ポイントを Lightweight 装置から Autonomous 装置に戻すことができます。アクセス ポイントがコントローラにアソシエートされている場合、コントローラを使用して Cisco IOS リリースをロードすることができます。アクセス ポイントがコントローラにアソシエートされていない場合、TFTP を使用して Cisco IOS リリースをロードすることができます。いずれの方法でも、ロードする Cisco IOS リリースを含む TFTP サーバにアクセス ポイントがアクセスできなければなりません。

コントローラを使用した前のリリースへの復帰

無線 LAN コントローラを使用して Lightweight モードから Autonomous モードに戻すには、次の手順を実行します。

ステップ 1　アクセス ポイントがアソシエートしているコントローラで CLI にログインします。

ステップ 2　次のコマンドを入力します。

config ap tftp-downgrade <TFTP サーバ IP アドレス > < ファイル名 > < アクセス ポイント名 >

ステップ 3　アクセス ポイントが再度ブートするまで待ち、CLI または GUI を使用してアクセス ポイントを再設定します。

MODE ボタンと TFTP サーバを使用した前のリリースへの復帰

アクセス ポイントの MODE（Reset）ボタンを使用して TFTP サーバから Cisco IOS リリースをロードし、Lightweight モードから Autonomous モードに戻すには、次の手順を実行します。

ステップ 1　TFTP サーバ ソフトウェアを実行している PC に、10.0.0.2 から 10.0.0.30 の範囲に含まれる静的 IP アドレスを設定する必要があります。

ステップ 2　PC の TFTP サーバ フォルダにアクセス ポイントのイメージ ファイル（1200 シリーズ アクセス ポイントの場合は、c1200-k9w7-tar.123-7.JA.tar など）があり、TFTP サーバがアクティブ化されていることを確認します。

ステップ 3　1200 シリーズ アクセス ポイントでは、TFTP サーバ フォルダにあるアクセス ポイントのイメージ ファイル名を **c1200-k9w7-tar.default** に変更します。

ステップ 4　カテゴリ 5（CAT5）イーサネット ケーブルを使用して PC をアクセス ポイントに接続します。

ステップ 5　アクセス ポイントから電源を抜きます。

ステップ 6　アクセス ポイントに電源を再接続しながら、**MODE** ボタンを押し続けます。

（注）　アクセス ポイントの MODE ボタンを有効にしておく必要があります。アクセス ポイントの MODE ボタンのステータスを確認するには、「Lightweight モードに変換したアクセス ポイントの Reset ボタンの無効化」の項（P.1-50）の手順に従ってください。

ステップ 7　**MODE** ボタンを押し続け、ステータス LED が赤に変わったら（約 20 ～ 30 秒）、MODE ボタンを放します。

ステップ 8　アクセス ポイントが再度ブートするまで待ちます（すべての LED が緑に変わった後、ステータス LED が緑に点滅します）。

ステップ 9　アクセス ポイントが再度ブートしたら、GUI または CLI を使用してアクセス ポイントを再設定します。

Lightweight モードに変換したアクセス ポイントから SSC を受け入れるコントローラ

Lightweight アクセス ポイント プロトコル（LWAPP）は、アクセス ポイントとコントローラの両方の X.509 証明書を必要とするセキュアな鍵配布によって、アクセス ポイントとコントロール間の制御通信を保護します。LWAPP は、X.509 証明書の事前プロビジョニングに依存しています。工場出荷時の証明書は、製造元がインストールした証明書（manufacturing-installed certificate）の頭字語である、*MIC* という言葉によって参照されます。2005 年 7 月 18 日より前に出荷された Cisco Aironet アクセス ポイントには MIC はありません。このため、これらのアクセス ポイントでは Lightweight モードで動作するようにアップグレードされた場合、自己署名証明書（SSC）を作成します。コントローラは、特定のアクセス ポイントの認証については SSC を受け入れるようにプログラムされています。

DHCP オプション 43 の使用

Cisco 1000 シリーズ アクセス ポイントは、DHCP オプション 43 に文字列形式を使用します。これに対し、Cisco Aironet アクセス ポイントは、DHCP オプション 43 に Type-Length-Value（TLV）を使用します。DHCP サーバはアクセス ポイントの DHCP Vendor Class Identifier（VCI; ベンダー クラス ID）文字列に基づいてオプションを返すようにプログラムされています（DHCP オプション 60）。表 1-2 は、Lightweight モードで動作可能な Cisco アクセス ポイントの VCI 文字列を示しています。

表 1-2　Lightweight アクセス ポイントの VCI 文字列

アクセス ポイント	**VCI** 文字列
Cisco 1000 シリーズ	Airespace 1200
Cisco Aironet 1130 シリーズ	Cisco AP c1130
Cisco Aironet 1200 シリーズ	Cisco AP c1200
Cisco Aironet 1240 シリーズ	Cisco AP c1240

TLV ブロックの形式は、次のとおりです。

- Type（タイプ）：0xf1（十進数 241）
- Length（長さ）：コントローラ IP アドレスの数 * 4
- Value（値）：コントローラの管理インターフェイスの IP アドレス リスト

DHCP オプション 43 の設定方法は、お使いの DHCP サーバの製品マニュアルを参照してください。『Application Note: Upgrading Autonomous Cisco Aironet Access Points To Lightweight Mode』には、DCHP サーバでオプション 43 を設定する手順の例が含まれています。

Lightweight モードに変換したアクセス ポイントへのコントローラを使用したデバッグ コマンドの送信

Lightweight モードに変換したアクセス ポイントにコントローラがデバッグ コマンドを送信できるようにするには、次のコマンドを入力します。

config ap remote-debug [**enable** | **disable** | **exc_command**] < アクセス ポイント名 >

この機能を有効にした場合、コントローラは変換したアクセス ポイントに文字列としてデバッグ コマンドを送信します。Cisco IOS ソフトウェアを Lightweight モードで実行する Cisco Aironet アクセス ポイントがサポートしている任意のデバッグ コマンドを送信することができます。

変換したアクセス ポイントからコントローラへのクラッシュ情報の送信

変換したアクセス ポイントが予期せず再度ブートした場合、アクセス ポイントではクラッシュ発生時にローカル フラッシュ メモリ上にクラッシュ ファイルを保存します。リブート後、アクセス ポイントはリブートの理由をコントローラに送信します。クラッシュにより装置が再度ブートした場合、コントローラは既存の LWAPP メッセージを使用してクラッシュ ファイルを取得し、コントローラのフラッシュ メモリにそれを保存します。クラッシュ情報コピーは、コントローラがアクセス ポイントからそれを取得した時点でアクセス ポイントのフラッシュ メモリから削除されます。

変換したアクセス ポイントからコントローラへの無線コア ダンプの送信

変換したアクセス ポイントの無線モジュールがコア ダンプを生成した場合、アクセス ポイントは無線クラッシュ発生時にローカル フラッシュ メモリ上に無線のコア ダンプ ファイルを保存します。また、無線がコア ダンプ ファイルを生成したことを知らせる通知メッセージをコントローラに送信します。コントローラはネットワーク管理者に警告するトラップを送信し、管理者はアクセス ポイントから無線コア ファイルを受信することができます。

アクセス ポイントからコア ファイルを取得するには、コントローラの CLI で、次のコマンドを入力します。

config ap get-radio-core-dump < スロット > < アクセス ポイント名 >

< スロット > には、アクセス ポイントの無線インターフェイス番号を入力します。

取得されたコア ファイルは、コントローラのフラッシュに保存され、その後、TFTP を通して外部サーバにアップロードし、分析に使用することができます。コア ファイルは、コントローラがアクセス ポイントからそれを取得した時点でアクセス ポイントのフラッシュ メモリから削除されます。

変換したアクセス ポイントからのメモリ コア ダンプの有効化

デフォルトでは、Lightweight モードに変換したアクセス ポイントは、コントローラにメモリ コア ダンプを送信しません。この機能を有効にするには、次のコマンドを入力します。

config ap core-dump enable <TFTP サーバ IP アドレス > < ファイル名 > {**compress** | **uncompress**} < アクセス ポイント名 > | **all**}

- <TFTP サーバ IP アドレス > には、アクセス ポイントがコア ファイルを送信する TFTP サーバの IP アドレスを入力します。アクセス ポイントは TFTP サーバに到達可能でなければなりません。
- < ファイル名 > には、アクセス ポイントがコア ファイルのラベル付けに使用するファイル名を入力します。

- 圧縮したコア ファイルを送信するようにアクセス ポイントを設定するには、**compress** を入力します。圧縮しないコア ファイルを送信するようにアクセス ポイントを設定するには、**uncompressed** を入力します。
- < アクセス ポイント名 > には、特定のアクセス ポイント名を入力します。Lightweight モードに変換したすべてのアクセス ポイントからのメモリ コア ダンプを有効にするには、**all** を入力します。

変換したアクセス ポイントの MAC アドレスの表示

コントローラが変換されたアクセス ポイントの MAC アドレスをコントローラ GUI の情報ページに表示する方法には違いがあります。

- コントローラでは、AP Summary ページに変換されたアクセス ポイントのイーサネット MAC アドレスのリストを表示します。
- AP Detail ページには、変換されたアクセス ポイントの BSS MAC アドレスとイーサネット MAC アドレスのリストを表示します。
- Radio Summary ページには、変換されたアクセス ポイントのリストを無線 MAC アドレスによって表示します。

Lightweight モードに変換したアクセス ポイントの Reset ボタンの無効化

Lightweight モードに変換したアクセス ポイントの Reset ボタンを無効化することができます。Reset ボタンは、アクセス ポイントの外面に MODE と書かれています。

次のコマンドを使用すると、あるコントローラにアソシエートしている変換されたアクセス ポイントの 1 つまたはすべての Reset ボタンを無効または有効にできます。

config ap reset-button {**enable** | **disable**} < アクセス ポイント名 > | **all**}

変換されたアクセス ポイントの Reset ボタンは、デフォルトでは有効になっています。

Lightweight モードに変換したアクセス ポイントの静的 IP アドレスの設定

Lightweight モードに変換したアクセス ポイントがコントローラにアソシエートした後、次のコマンドを入力してアクセス ポイントに静的 IP アドレスを設定します。

config ap static-ip enable < アクセス ポイント名 > <IP アドレス > < マスク > < ゲートウェイ >

不正なアクセス ポイント

安価で簡単に利用できることから、従業員は、IT 部門に知らせて同意を得ることなく、許可されていない不正なアクセス ポイントを既存の LAN やビルディング内のアドホック ネットワークに接続することがあります。

これらの不正なアクセス ポイントは、企業のファイアウォールの背後にあるネットワーク ポートに接続可能であるため、重大なネットワーク セキュリティ侵犯となることがあります。通常、従業員は不正なアクセス ポイントのセキュリティ設定を有効にしないので、権限のないユーザがこのアクセス ポイントを使って、ネットワーク トラフィックを傍受し、クライアント セッションをハイジャックすることは簡単です。さらに警戒すべきことは、無線ユーザとウォー チョーカーはセキュリティで保護されていないアクセス ポイントの場所を頻繁に公表するため、企業のセキュリティが侵害される可能性も増大します。

Cisco Wireless LAN Solution では、担当者がスキャナを持って不正なアクセス ポイントを手作業で検出するのではなく、管理対象のアクセス ポイントに MAC アドレスと IP アドレスによって不正なアクセス ポイントを検出させて、その情報を自動的に収集し、システム オペレータがその不正なアクセス ポイントを特定、タグ付け、および監視できるようにします。これについては、「不正なアクセス ポイントの検出と特定」の項（P.9-16）を参照してください。また、オペレーティング システムを使用し、4 つの Cisco 1000 シリーズ Lightweight アクセス ポイントの 1 つから、不正なアクセス ポイント クライアントに認証解除とアソシエート解除のメッセージを送信することで不正なアクセス ポイントを防ぐこともできます。最終的に、オペレーティング システムを使用すると、企業サブネット上のすべての不正なアクセス ポイントで認証を試みるクライアントすべてを自動的に防止できます。このリアルタイム検出は自動化されているため、LAN のセキュリティが大幅に向上する一方で、不正なアクセス ポイントの検出と監視にかかる人件費は節約されます。ピアツーピア（あるいは、アドホック）クライアントも、不正なアクセス ポイントと見られる可能性があることに注意してください。

不正なアクセス ポイントのロケーション、タギング、および阻止

この組み込み型の検出、タギング、監視、阻止機能を使用すると、システム管理者は、次に挙げる必要な処理を実行できます。

- 不正なアクセス ポイントを特定します（「不正なアクセス ポイントの検出と特定」の項（P.9-16）を参照）。
- 新しい不正なアクセス ポイントの通知を受け取ります（通路をスキャンして歩く必要はなくなります）。
- 不明の不正なアクセス ポイントが削除または認識されるまで監視します。
- 最も近い場所の認可済みアクセス ポイントを特定して、高速かつ効果的に誘導スキャンを行えるようにします。
- 1 ～ 4 つの Cisco 1000 シリーズ Lightweight アクセス ポイントで、不正なアクセス ポイント クライアントに認証解除とアソシエーション解除のメッセージを送信して、不正なアクセス ポイントを阻止します。この阻止は、MAC アドレスを使って個々の不正なアクセス ポイントに対して行うことも、企業サブネットに接続されているすべての不正なアクセス ポイントに対して要求することもできます。
- 不正なアクセス ポイントにタグを付けます。
  - 不正なアクセス ポイントが LAN 外部にあり、LAN または無線 LAN のセキュリティを脅かさない場合は承諾します。
  - 不正なアクセス ポイントが LAN または無線 LAN のセキュリティを脅かさない場合は容認します。
  - 不正なアクセス ポイントが削除または認識されるまで、不明なアクセス ポイントとしてタグ付けします。

- 不正なアクセス ポイントを阻止済みとしてタグ付けし、1 ～ 4 つの Cisco 1000 シリーズ Lightweight アクセス ポイントで、すべての不正なアクセス ポイント クライアントの認証解除およびアソシエーション解除メッセージを転送することにより、クライアントが不正なアクセス ポイントにアソシエートしないようにします。この機能には、同じ不正なアクセス ポイント上のアクティブなチャネルがすべて含まれます。

不正なアクセス ポイントが信頼されたネットワーク上にあるかどうかを検出するのは、Rogue Detector モードです。これは何らかの RF サービスを提供するのではなく、むしろ定期的に Cisco Wireless LAN Controller から不正なアクセス ポイントのレポートを受け取り、すべての ARP パケットをスニファするものです。このモードでは、ARP 要求と、Cisco Wireless LAN Controller から受信した MAC アドレスが一致していることが検出されると、Cisco Wireless LAN Controller に対する不正なアクセス ポイント アラートが生成されます。

混雑している RF 空間での不正なアクセス ポイントの自動検出を容易にするために、監視モードで動作するよう Cisco 1000 シリーズ Lightweight アクセス ポイントを設定しておくと、不要な干渉を生じずに監視を行えるようになります。

Web ユーザ インターフェイスと CLI

この項では、コントローラの GUI と CLI について説明します。

Web ユーザ インターフェイス

Web ユーザ インターフェイスは、各 Cisco Wireless LAN Controller に組み込まれています。Web ユーザ インターフェイスでは、最大 5 名のユーザが、組み込み Cisco Wireless LAN Controller http または https（http + SSL）Web サーバを同時に閲覧して、パラメータを設定し、Cisco Wireless LAN Controller とそのアソシエートされているアクセス ポイントの動作ステータスを監視することができます。

（注）　Cisco WLAN Solution のセキュリティを強化するために、https: インターフェイスを有効にし、http: インターフェイスを無効にすることをお勧めします。

Web ユーザ インターフェイスは、同時に 1 つの Cisco Wireless LAN Controller と連携して動作するため、1 つの Cisco Wireless LAN Controller とそのアソシエートされている Cisco 1000 シリーズ Lightweight アクセス ポイントを設定または監視するときに特に便利です。

Web ユーザ インターフェイスの詳細は、「Web ブラウザ インターフェイスの使用方法」の項（P.2-2）を参照してください。

コマンドライン インターフェイス

Cisco Wireless LAN Solution Command Line Interface（CLI）は、各 Cisco Wireless LAN Controller に組み込まれています。CLI を使用すると、オペレータは VT-100 エミュレータを使用して、個々の Cisco Wireless LAN Controller をローカルまたはリモートで設定、監視、制御し、多数のデバッグ機能にアクセスすることができます。

CLI は同時に 1 つの Cisco Wireless LAN Controller と連携して動作するため、1 つの Cisco Wireless LAN Controller を設定または監視するときに特に便利です。

コマンドライン インターフェイス（CLI）を使用して、Cisco Wireless LAN Controller とそのアソシエートされている Cisco 1000 シリーズ Lightweight アクセス ポイントを設定および監視することができます。CLI は、簡単なテキストベースのツリー構造のインターフェイスであり、最大 5 名のユーザが Telnet 対応ターミナル エミュレータを使用して、Cisco Wireless LAN Controller とアソシエートされている Cisco 1000 シリーズ Lightweight アクセス ポイントのすべてを同時に設定および監視できます。

詳細は、「CLI の使用方法」の項（P.2-6）と『Cisco Wireless LAN Solution CLI Reference』を参照してください。

Cisco Wireless Control System

Cisco Wireless Control System（Cisco WCS）は、Cisco Wireless LAN Solution のネットワーク管理ツールです。Web ユーザ インターフェイスと CLI の機能が追加されており、個々のコントローラをコントローラ ネットワークに移行します。WCS は、Windows 2000、Windows 2003、および Red Hat Enterprise Linux ES サーバ上で動作します。

Cisco WCS には、Cisco Wireless LAN Controller レベルで使用されるのと同じ設定、パフォーマンス監視、セキュリティ、障害管理、およびアカウンティングのオプションが含まれていますが、複数のコントローラとその管理対象のアクセス ポイントをグラフィカルに表示するオプションも追加されています。

Cisco WCS には、サポートする機能レベルが異なる 2 つのバージョンが用意されています。

- Cisco WCS Base。無線クライアント データ アクセス機能、不正なアクセス ポイント阻止機能、Cisco Wireless LAN Solution の監視および制御機能が搭載され、最も近い Cisco 1000 シリーズ Lightweight アクセス ポイントへのクライアントと不正なアクセス ポイントのロケーションを実行できます。詳細は、「Cisco WCS Base」の項（P.1-55）を参照してください。
- Cisco WCS Location。WCS Base のすべての機能が搭載されていますが、10m 以内での高精度の不正なアクセス ポイントとクライアントのロケーションを実行できます。詳細は、「Cisco WCS Location」の項（P.1-56）を参照してください。

表 1-3 は、これらの機能のリストです。

表 1-3　WCS Base および WCS Location の機能

機能	Cisco WCS Base	Cisco WCS Location
ロケーションおよびトラッキング：		
• 低解像度のクライアントのロケーション	Yes	-
• 高解像度のクライアントのロケーション	-	Yes
• 低解像度の不正アクセス ポイントのロケーション	Yes	-
• 高解像度の不正アクセス ポイントのロケーション	-	Yes
クライアント データ サービス、セキュリティ、および監視：		
• Cisco 1000 シリーズ Lightweight アクセス ポイント経由のクライアント アクセス	Yes	Yes
• 複数の無線 LAN（個別の SSID およびポリシー）	Yes	Yes
Cisco 1000 シリーズ Lightweight アクセス ポイントを使用した、不正アクセス ポイントの検出と阻止	Yes	Yes
802.11a/b/g 帯域	Yes	Yes
Radio Resource Management（リアルタイムでのチャネル割り当て、不正なアクセス ポイントの検出と阻止）	Yes	Yes
Radio Resource Management（リアルタイムでの干渉の検出と無効化、送信電力の制御、チャネルの割り当て、クライアント モビリティの管理、クライアントの負荷分散、およびカバレッジ ホールの検出）	Yes	Yes
ソフトウェアと設定の更新の自動化	Yes	Yes
無線による侵入からの保護	Yes	Yes
グローバルおよび個別 AP のセキュリティ ポリシー	Yes	Yes
Cisco Wireless LAN Controller の制御	Yes	Yes
サポートされるワークステーション：		
• Windows 2000 または Windows 2003	Yes	Yes
• Red Hat Enterprise Linux ES サーバ	Yes	Yes

Cisco Wireless Control System は、Windows 2000、Windows 2003、および Red Hat Enterprise Linux ES サーバ上で動作します。Windows Cisco WCS は、通常の Windows アプリケーションとして実行することも、サービスとしてインストールすることもできます。サービスとしてインストールした場合は、継続的に実行され、リブート後に実行が再開されます。Linux Cisco WCS は、常に通常の Linux アプリケーションとして実行されます。

WCS ユーザ インターフェイスを使用すると、Cisco WCS オペレータは許可された Cisco WLAN Solution の設定、監視、制御機能のすべてを、Windows ワークステーションの Internet Explorer 6.0（またはその他の）Web ブラウザ ウィンドウから制御できるようになります。Cisco WCS オペレータのアクセス権は、Cisco WCS ユーザ インターフェイスの Admin タブを使用して、Cisco WCS 管理者が定義します。このタブで、Cisco WCS 管理者は、ユーザ アカウントを管理し、定期的なメンテナンス タスクをスケジュールすることができます。

Cisco WCS で Cisco WCS Cisco Wireless LAN Controller Autodiscovery アルゴリズムを使用すると、Cisco Wireless LAN Controller の設定と監視を簡単に行えると同時に、データ入力ミスも減少します。Cisco WCS は業界標準の SNMP プロトコルを使用して、Cisco Wireless LAN Controller と通信します。

また、Cisco WCS には Floor Plan Editor も搭載されています。これは、ビットマップ化されたキャンパス、フロア プラン、および屋外エリア マップをベクトル化し、ウォール タイプを追加および変更して、生成されたベクトル ウォール形式マップを Cisco WCS データベースにインポートすることができます。このベクトル ファイルを Cisco WCS RF Prediction Tool で使用すると、より正確な壁面および窓の RF 減衰値に基づいて、優れた RF 予測が生成されます。WCS のマップの詳細は、「マップの使用方法」の項（P.9-4）を参照してください。

Cisco WCS Base

Cisco WCS Base バージョンは、無線クライアント データ アクセス、不正アクセス ポイントの検出および阻止機能、Cisco WLAN Solution の監視と制御をサポートするとともに、次の機能をグラフィカル表示できます。

- コントローラにアソシエートしているアクセス ポイントの自動ディスカバリ
- 不正なアクセス ポイントの自動ディスカバリ、阻止、または通知
- 企業が複数の地理的領域にまたがっている場合、アクセス ポイントのカバレッジ領域をマップベース編成にすると便利です（詳細は、第 9 章「Cisco WCS の使用方法」と「Network Summary ページの確認」の項（P.9-2）を参照してください）。
- ユーザ指定のキャンパス、ビルディング、およびフロアのグラフィックス。次のものが表示されます。
  - 管理対象アクセス ポイントのロケーションとステータス（「Cisco WCS への Cisco Wireless LAN Controller の追加」の項（P.9-3）を参照してください）。
  - 最も近い管理対象の Cisco 1000 シリーズ Lightweight アクセス ポイントで受信する信号強度に基づいた、不正アクセス ポイントのロケーション（「不正なアクセス ポイントの検出と特定」の項（P.9-16）を参照してください）。
  - クライアントから受信する信号強度に基づいた、Cisco 1000 シリーズ Lightweight アクセス ポイントのカバレッジ ホールのアラーム情報。この情報は、マップ形式ではなく表形式で表示されます（「カバレッジ ホールの検索」の項（P.9-19）を参照してください）。
  - RF カバレッジ マップ
- システム全体の制御：
  - 顧客が定義したテンプレートを使用して簡素化されたネットワーク、Cisco Wireless LAN Controller、および管理対象の Cisco 1000 シリーズ Lightweight アクセス ポイントの設定
  - ネットワーク、Cisco Wireless LAN Controller、および管理対象の Cisco 1000 シリーズ Lightweight アクセス ポイントのステータスおよびアラームの監視
  - 自動および手動によるデータ クライアントの監視および制御機能

  - 自動監視：不正な AP、カバレッジ ホール、セキュリティ違反、Cisco Wireless LAN Controller、および Cisco 1000 シリーズ Lightweight アクセス ポイント
  - データ クライアント、不正なアクセス ポイント、カバレッジ ホール、セキュリティ違反、Cisco Wireless LAN Controller、および Cisco 1000 シリーズ Lightweight アクセス ポイントで使用可能なすべてのイベント ログ
  - Radio Resource Management（RRM）による、自動チャネルおよび電力レベルの割り当て
  - ユーザ定義の Cisco Wireless LAN Controller ステータスの自動監査、欠落したトラップ ポーリング、設定バックアップ、およびポリシー クリーンナップ
- 最も近い Cisco 1000 シリーズ Lightweight アクセス ポイントへの不正アクセス ポイントのリアルタイム ロケーション
- 最も近い Cisco 1000 シリーズ Lightweight アクセス ポイントへのクライアントのリアルタイムおよび履歴ロケーション
- Windows 2000、Windows 2003、および Red Hat Enterprise Linux ES Server ワークステーション上での実行

Cisco WCS Location

Cisco WCS Location では、「Cisco WCS Base」の項（P.1-55）に挙げられているグラフィカル表示に加えて、次の機能拡張も追加されています。

- 10m 以内の不正アクセス ポイントのオンデマンド ロケーション
- 10m 以内のクライアントのオンデマンド ロケーション
- Windows 2000、Windows 2003、および Red Hat Enterprise Linux ES サーバ上での実行
- Cisco WCS Location ユーザ インターフェイスで表示可能な履歴ロケーション データを収集および返すために、Location Appliance を使用する能力 Location Appliance の詳細は、「Cisco 2700 シリーズ Location Appliance」の項（P.1-59）を参照してください。

Cisco WCS ユーザ インターフェイス

ネットワーク オペレータは、Cisco WCS ユーザ インターフェイスのインターフェイスを使用すると、標準の HTTP または HTTPS ブラウザ ウィンドウを使用して、Cisco Wireless LAN Solution カバレッジ領域レイアウトの作成および設定、システム動作パラメータの設定、リアルタイムの Cisco Wireless LAN Solution 動作の監視、トラブルシューティング タスクの実行、を行うことができます。また、Cisco WCS 管理者は、Cisco WCS ユーザ インターフェイスのインターフェイスを使用すると、ユーザ アカウントの作成、編集、削除、パスワードの変更、アクセス権の割り当て、および定期的なメンテナンス タスクのスケジュールを行うことができます。

Cisco WCS のすべての機能を利用するためには、Windows ワークステーション ブラウザの Internet Explorer 6.0 またはそれ以降を使用することをお勧めします。

HTTPS（SSL を実装した HTTP）インターフェイスはデフォルトで有効になり、HTTP インターフェイスは、CLI、GUI、および WCS ユーザ インターフェイスで手動によりアクティブ化することができます。

Cisco WCS 管理者は、ユーザ名とパスワードを新規作成して、これを定義済みのアクセス権グループに割り当てます。

Cisco WCS ユーザ インターフェイス オペレータは、第 9 章「Cisco WCS の使用方法」に記載されている方法で、このタスクを実行します。

Floor Plan Editor

Cisco WCS には Floor Plan Editor が含まれています。これは、建築、機械、技術分野で使用されている図面、グラフィックス、マップ、およびその他の種類のライン アートワークを、ラスター ビットマップ形式から、ウォール（ベクトル）形式に変換するツールです。オペレータはスキャナを使用して図面をサポートされるファイル形式にデジタル化し、Cisco WCS にインポートすることができます。Floor Plan Editor は、Cisco WCS プログラムにインポートすることができる、ウォール形式のデータを自動的に認識して表示します。

まっすぐなアウトライン、角度のあるアウトライン、やや角度が付いたアウトラインを滑らかに作成することができるため、Floor Plan Editor は、フロア プラン図の変換、壁の特性の定義、生成されたベクトル ウォール形式マップの Cisco WCS データベースへのインポートに使用されます。ベクトル ファイルを Cisco WCS RF Prediction Tool で使用すると、Cisco 1000 シリーズ Lightweight アクセス ポイントの信号強度と、正確な壁、窓、および間仕切りの RF 減衰に基づいて、優れた RF 予測が生成されます。

それ以外の場合は、ラスター イメージを .BMP、.TIFF、.JPEG、または .PNG ラスター形式で保存してください。既存のベクトル マップ ファイルは編集することもできます。

出力ウォール ファイルは、ベクトル（Cisco WLAN Solution ウォール形式）で保存して、直接 Cisco WCS データベースにインポートできます。また、出力ウォール ファイルは、.DXF（AutoCAD）形式、.AI（Adobe Illustrator）形式、.EMF（拡張メタファイル）形式、.WMF（Windows メタファイル）形式、および .TXT（ASCII XY）形式で保存することもできますが、これらのファイル タイプは Cisco WCS では認識されません。

入力および出力イメージ サイズに対する制限はありません。

ヒント　データの解像度が高くなると、Floor Plan Editor の認識率も高くなります。可能な場合は、400 ～ 600dpi のスキャンを使用してください。

ヒント　Cisco WCS で最適な表示が得られるように、水平方向を長軸にして（ランドスケープ形式）イメージを作成することを強くお勧めします。

WCS でのマップの使用に関する詳細は、「マップの使用方法」の項（P.9-4）を参照してください。

Cisco WCS Cisco Wireless LAN Controller Autodiscovery

Cisco Wireless LAN Controller データを管理データベースに手動で追加すると、時間がかかり、データの入力ミスも多くなる可能性があります。Cisco WCS には Cisco Wireless LAN Controller 設定のアップロード機能が組み込まれており、これにより、データベース作成がスピードアップし、エラーも少なくなります。

Cisco Wireless LAN Controller Autodiscovery は、Cisco Wireless LAN Solution オペレータが定義したモビリティ グループサブネットに制限されます。

Cisco Wireless LAN Controller Autodiscovery を使用すると、オペレータは、IP アドレスで 1 つの Cisco Wireless LAN Controller を検索できます。Autodiscovery 機能は、指定した IP アドレスを持つネットワーク上の Cisco Wireless LAN Controller を検索し、検出された Cisco Wireless LAN Controller 情報を自動的に Cisco WCS データベースに保存します。

Lightweight アクセス ポイントがコントローラにアソシエートすると、コントローラは、ただちにアクセス ポイント情報を Cisco WCS に送信し、アクセス ポイントが Cisco WCS データベースに自動的に追加されます。

Cisco 1000 シリーズ Lightweight アクセス ポイント情報が Cisco WCS データベースに追加された後、空間のトポロジ マップが現在の状態を反映するように、オペレータは Cisco WCS ユーザ インターフェイス マップ上の適切なスポットにその Cisco 1000 シリーズ Lightweight アクセス ポイントを追加することができます。

Cisco WCS アラームの電子メール通知

Cisco WCS には、電子メールによる通知機能が組み込まれており、重大なアラームが発生したときにネットワーク オペレータに通知できます。

現在のアラーム通知設定を表示するには、Cisco WCS の Monitor All Alarms > Email Notification ページを参照してください。

Cisco WCS のロケーション キャリブレーション

Cisco WCS には、Cisco Wireless LAN Solution オペレータが RF カバレッジ領域の実際の信号強度と減衰を正確に測定し、Cisco WCS データベースに正確なキャリブレーション モデルを作成できる、キャリブレーション ツールが含まれています。キャリブレーションが完了すると、このキャリブレーション モデルは、クライアントと不正なアクセス ポイントのロケーションをより正確に行えるようになります。労力を省くために、同じ Cisco 1000 シリーズ Lightweight アクセス ポイント レイアウトと同じ壁レイアウトを持つ領域にキャリブレーション モデルを再利用することもできます。

キャリブレーション ツールはサイト調査ツールと同様に使用し、技術者は、Cisco WCS が搭載されているラップトップをフロアまたは屋外エリアの複数の場所に持って行き、そのフロアまたは屋外エリアのマップ上で選択した場所の実際の信号強度を測定することができます。そして、技術者は Cisco WCS でキャリブレーション ツールを使用して、フロアまたは屋外エリアの収集データ ポイントを処理します。

現在のキャリブレーション モデルを表示するには、Cisco WCS の Monitor RF Calibration Models ページを参照してください。

Cisco 2700 シリーズ Location Appliance

Cisco 2700 シリーズ Location Appliance（Location Appliance）は、履歴ロケーション データを計算、収集、および格納し、このデータを Cisco WCS に表示することにより、高精度な組み込み Cisco WCS Location 機能を拡張します。この場合、Location Appliance は 1 つまたは複数の Cisco WCS サーバに対するサーバとして機能し、そのサーバがアソシエートされている Cisco Wireless LAN Controller のデータを収集、格納、および受け渡しします。

コマンドライン インターフェイス（CLI）で簡単に設定した後、残りの Location Appliance の設定は Cisco WCS インターフェイスを使用して行えます。

設定された Location Appliance は、アソシエートされている Cisco Wireless LAN Controller と直接通信を行い、オペレータが定義したロケーション データを収集します。その後、アソシエートされている Cisco WCS サーバ のオペレータは、各 Location Appliance と通信して、選択したデータを転送して表示できます。

Location Appliance は、いつでもオペレータが指定した時間間隔で、任意の Cisco WCS サーバを指定した FTP フォルダにバックアップし、その Cisco WCS サーバから復元することができます。また、Location Appliance データベースは、いつでも Cisco WCS サーバ データベースと同期させることができます。

オペレータは Location Appliance の機能を使用して、Cisco WCS サーバ の新しいアプリケーション コードを、アソシエートされている Location Appliance すべてにダウンロードできます。

Location Appliance で Cisco WCS が拡張されている場合、Cisco Wireless LAN Solution の各 Location Appliance に対して、Cisco WCS は最大 1,500 のラップトップ クライアント、パームトップ クライアント、VoIP 通話クライアント、RFID（無線周波数 ID）アセット タグ、不正なアクセス ポイント、および不正なアクセス ポイント クライアントについて、履歴ロケーション データを表示できます。

オペレータは、異なるオペレータ定義間隔で、Cisco Wireless LAN Solution クライアント、不正なアクセス ポイントとクライアント、RFID アセット タグ、および統計情報のデータを収集するよう Location Appliance を設定することができます。

Location Appliance では、2 つの冗長背面パネル 10/100/1000BASE-T ポートを、1 つまたは 2 つのネットワーク セグメントに接続します。また、背面パネルには電源コードが、前面パネルには ON/OFF スイッチが付いています。Location Appliance には、CLI コンソールを使って初期設定を行うために、背面パネルに DB-9 コンソール ポートがあります。

Location Appliance は、アソシエートされている Cisco WCS サーバ および Cisco Wireless LAN Controller と通信できる、任意の Network Operations Center（NOC; ネットワーク オペレーション センター）またはワイヤリング クローゼットに装着することができます。