CHAPTER 1

概要

この章では、コントローラのコンポーネントと機能について説明します。この章の内容は、次のとおりです。

Cisco Unified Wireless Network Solution の概要

Cisco Unified Wireless Network（Cisco UWN）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 UWN 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 システムは、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を管理し、Radio Resource Management（RRM）機能を実行します。また、オペレーティング システム セキュリティ ソリューションを使用してシステム全体のモビリティ ポリシーを管理したり、オペレーティング システムのセキュリティ フレームワークを使用してすべてのセキュリティ機能を調整することもできます。

Cisco UWN Solution は、Cisco Wireless LAN Controller とそれにアソシエートされている Lightweight アクセス ポイントで構成されます。これらはオペレーティング システムによって制御され、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。

- HTTP、HTTPS、またはこれら両方の機能をすべて備えた Web ユーザ インターフェイス。Cisco Wireless LAN Controller によってホストされるこのインターフェイスは、個々のコントローラを設定および監視するときに使用できます。第 2 章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 を設定および監視するときに使用できます。第 2 章を参照してください。
- Cisco Wireless Control System（WCS）。1 つ以上の Cisco Wireless LAN Controller とアソシエートされているアクセス ポイントを設定、監視する場合に使用します。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 2003、および Red Hat Enterprise Linux ES サーバ上で動作します。

（注）　WCS ソフトウェア リリース 4.1 は、コントローラ ソフトウェア リリース 4.1 を実行しているコントローラとともに使用する必要があります。前のバージョンの WCS は、コントローラ ソフトウェア リリース 4.1 を実行しているコントローラとともに使用しないでください。

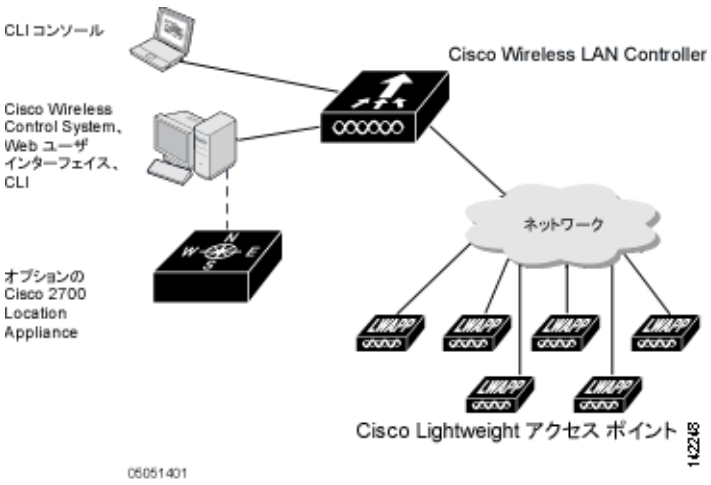
- 業界標準の SNMP V1、V2c、および V3 インターフェイスであれば、SNMP 準拠のサードパーティ製ネットワーク管理システムと併用できます。

Cisco UWN 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 UWN 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。

（注）　特に記載されていない限り、以降では、Cisco Wireless LAN Controller を *コントローラ*と呼び、すべての Cisco Lightweight アクセス ポイントを *アクセス ポイント*と呼びます。

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 UWN Solution コンポーネント



シングルコントローラ展開

スタンドアロンのコントローラでは、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。
- Cisco 1000 シリーズ アクセス ポイントに対する最大 16 までの無線 LAN（SSID）ポリシーの完全制御。

（注）　LWAPP 有効化アクセス ポイントは、最大 8 つまでの無線 LAN（SSID）ポリシーをサポートします。

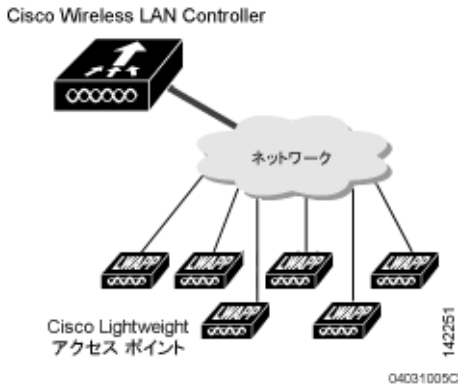
- ネットワークを介したコントローラへの Lightweight アクセス ポイントの接続。ネットワーク機器では、アクセス ポイントに Power over Ethernet を提供してもしなくてもかまいません。

一部のコントローラでは、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。

（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、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



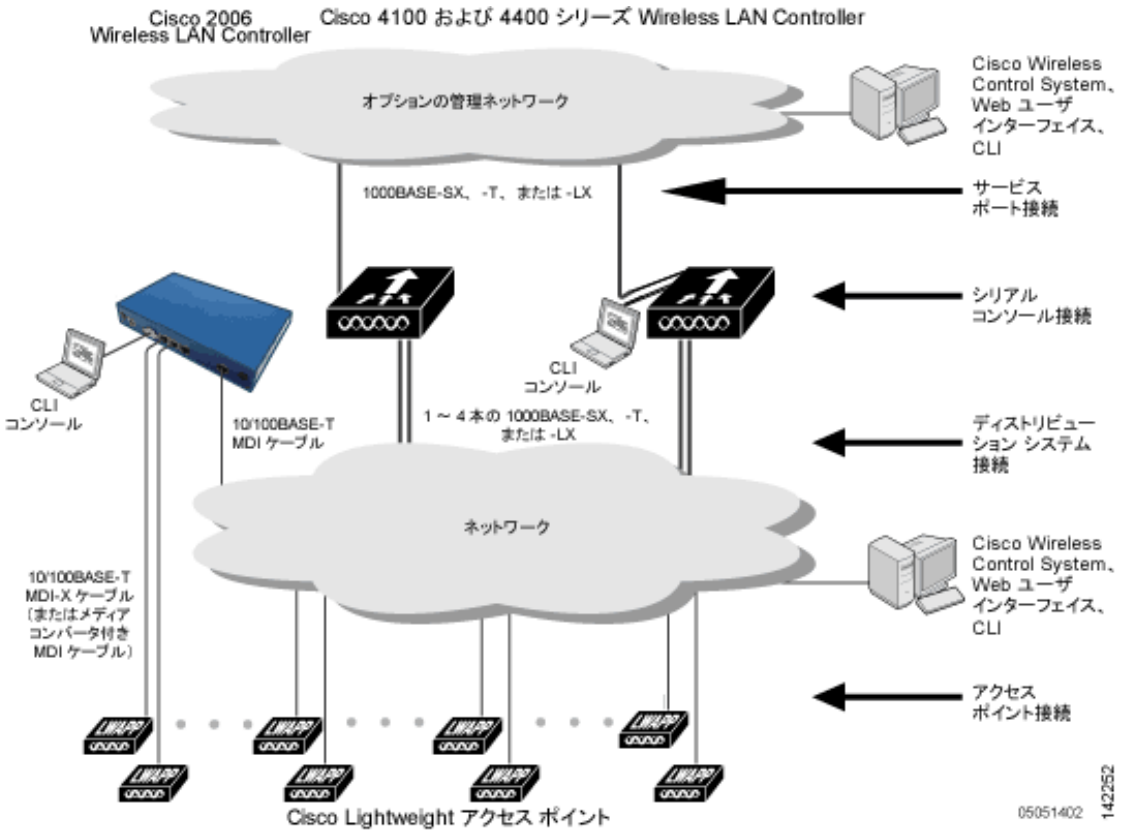
マルチコントローラ展開

すべてのコントローラは、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 コントローラ 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 コントローラ の RF パラメータの自動検出と自動設定。
- 同一サブネット（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。
- アクセス　ポイントの負荷を減らした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. 1-17）を参照）。

図 1-3 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 および 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は、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 全体を対象とするシンプルな Policy Manager に統合したものです。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 UWN Solution 無線 LAN」の項（P. 1-12）を参照）。

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
  - 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。

- パススルー VPN
- 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。一方、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 ポイントに接続する Cisco Wireless LAN Controller、デバイス サービシング時とクライアント ローミング時の Cisco Wireless LAN Controller 間通信をセキュリティで保護するためのセキュリティ機能が組み込まれています。

Cisco Wireless LAN Controller と Cisco 1000 シリーズ Lightweight アクセス ポイントの各製品には、それぞれ固有の署名付き X.509 証明書が添付されます。この署名付き証明書は、ダウンロードしたコードを読み込む前の検証に使用されます。このようにして、悪意のあるコードがハッカーによって Cisco Wireless LAN Controller や Cisco 1000 シリーズ Lightweight アクセス ポイント にダウンロードされることを防ぎます。

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。

（注）　IPv4 ネットワーク レイヤ プロトコルでは、LWAPP コントローラ システムによる転送がサポートされています。IPv6（クライアント用のみ）と Appletalk もサポートされていますが、4400 シリーズ コントローラと Cisco WiSM でのみのサポートとなります。他のレイヤ 3 プロトコル（IPX、DECnet Phase IV、OSI CLNP など）およびレイヤ 2（ブリッジ）プロトコル（LAT および NetBeui など）はサポートされていません。

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 通信を行うには、Cisco Wireless LAN Controller と Cisco 1000 シリーズ Lightweight アクセス ポイントが同一サブネットにある場合はレイヤ 2 デバイスを使用してこれらを接続し、異なるサブネットにある場合はレイヤ 3 デバイスを使用して接続します。また、アクセス ポイントの IP アドレスが外部 DHCP サーバを介して静的または動的に割り当てられていることも必要です。

モビリティ グループに属するすべての Cisco Wireless LAN Controller は、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ます。それ以外の場合は、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、Cisco 1000 シリーズ Lightweight アクセス ポイントおよびレイヤ 2 モード用に設定された管理インターフェイスを制御するよう AP 管理インターフェイスを設定する必要があります。

Cisco Wireless LAN Controller

Cisco Wireless LAN Controller マルチ展開ネットワークに Cisco 1000 シリーズ Lightweight アクセス ポイントを追加する場合、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. 1-17）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。次に、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 ポイントをリブートします。

（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。

用意したアクセス 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. 1-17）を参照してください。

クライアント ロケーション

Cisco Wireless LAN Solution で Cisco WCS を使用する場合、コントローラは、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チェックし、そのロケーションを Cisco WCS データベースに保存します。ロケーション ソリューションに関する詳細は、『Cisco Wireless Control System Configuration Guide』および『Cisco Location Appliance Configuration Guide』を参照してください。これらのガイドの URL は次のとおりです。

『Cisco Wireless Control System Configuration Guide』

http://www.cisco.com/en/US/products/ps6305/products_installation_and_configuration_guides_list.html

『Cisco Location Appliance Configuration Guide』

http://www.cisco.com/en/US/products/ps6386/products_installation_and_configuration_guides_list.html

コントローラ プラットフォーム

コントローラは、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コントローラ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 UWN Solution が実現されます。コントローラは、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。

ソフトウェア リリース 4.1 との使用がサポートされているコントローラは、次のとおりです。

- Cisco 2000 シリーズ コントローラ
- Cisco 2100 シリーズ コントローラ
- Cisco 4400 シリーズ コントローラ
- Catalyst 6500 シリーズ ワイヤレス サービス モジュール（WiSM）
- コントローラ ネットワーク モジュール内蔵の Cisco 28/37/38xx シリーズ サービス統合型ルータ
- Catalyst 3750G Integrated Wireless LAN Controller Switch

最初の 3 つのコントローラはスタンドアロン プラットフォームです。その他の 3 つのコントローラは、シスコのスイッチおよびルータ製品に統合されています。

Cisco 2000 および 2100 シリーズ コントローラ

Cisco 2000 および 2100 シリーズ Wireless LAN Controller は、Cisco Lightweight アクセス ポイントおよび Cisco Wireless Control System（WCS）と組み合わせて使用することで、システム全体での無線 LAN 機能を実現します。2000 および 2100 シリーズ コントローラはそれぞれ最大 6 個の Lightweight アクセス ポイントを制御し、企業の支社展開に一般的なマルチコントローラ アーキテクチャに適しています。小規模から中規模の環境のためのシングル コントローラ展開にも使用できます。

注意　コントローラのコンソール ポートに Power over Ethernet（PoE）ケーブルを接続しないでください。接続すると、コントローラが損傷するおそれがあります。

（注）　アクセス ポイントをコントローラに再接続するときは、20 秒以上待ってから接続してください。待たずに接続すると、コントローラがデバイスを検出できないことがあります。

サポートされない機能

次に示すハードウェア機能は、2000 および 2100 シリーズ コントローラではサポートされません。

- Power over Ethernet（PoE）[2000 シリーズ コントローラのみ]

（注）　2100 シリーズ コントローラのポート 7 および 8 は PoE ポートです。

- サービス ポート（専用の帯域外管理 10/100 Mbps イーサネット インターフェイス）

次に示すソフトウェア機能は、2000 および 2100 シリーズ コントローラではサポートされません。

- VPN 終端（IPSec、L2TP など）
- ゲスト コントローラ トンネルの終端（ゲスト コントローラ トンネルの起点は可能）
- 外部 Web 認証 Web サーバ リスト
- レイヤ 2 LWAPP
- スパニング ツリー
- ポートのミラーリング
- Cranite
- Fortress
- AppleTalk
- QoS ユーザごと帯域幅コントラクト
- IPv6 パススルー
- リンク集約（LAG）

Cisco 4400 シリーズ コントローラ

Cisco 4400 シリーズ Wireless LAN Controller には、4402 と 4404 の 2 つのモデルがあります。4402 では最大 50 個、4404 では最大 100 個の Lightweight アクセス ポイントがサポートされ、大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。

4400 シリーズ コントローラには、1 つまたは 2 つの Cisco 4400 シリーズ電源を装着できます。4400 シリーズ コントローラに 2 つの Cisco 4400 シリーズ電源を装着して冗長構成にしておけば、一方の電源に障害が発生した場合でも、他方の電源から引き続きコントローラに電力を供給できます。

Catalyst 6500 シリーズ ワイヤレス サービス モジュール

Catalyst 6500 シリーズ Wireless Services Module（WiSM; ワイヤレス サービス モジュール）は、Catalyst 6500 スイッチと 2 つの Cisco 4404 コントローラが統合されたもので、最大 300 個の Lightweight アクセス ポイントをサポートします。スイッチには、スイッチとコントローラを接続する内部ギガバイト イーサネット ポートが 8 個装備されています。スイッチと内部コントローラではそれぞれ異なるソフトウェア バージョンが実行されており、これらのソフトウェア バージョンは個別にアップグレードする必要があります。

（注）　Catalyst 6500 シリーズ スイッチのシャーシは、他のサービス モジュールがインストールされていなければ最大 5 個の Cisco WiSM をサポートできます。サービス モジュールが 1 つ以上インストールされている場合、シャーシがサポート可能なサービス モジュールの数は最大 4 個となります（WiSM を含む）。

詳細は、次のドキュメントを参照してください。

- 『Catalyst 6500 Series Switch Installation Guide』
- 『Catalyst 6500 Series Switch Wireless Services Module Installation and Configuration Note』
- 『Release Notes for Catalyst 6500 Series Switch Wireless LAN Services Module』

これらのドキュメントには、次の URL からアクセスできます。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

Cisco 28/37/38xx シリーズ サービス統合型ルータ

Cisco 28/37/38xx シリーズ サービス統合型ルータは、28/37/38xx ルータと Cisco コントローラ ネットワーク モジュールを統合したもので、ネットワーク モジュールのバージョンに応じて最大 6 個、8 個、または 12 個の Lightweight アクセス ポイントをサポートします。8 個または 12 個のアクセス ポイントをサポート可能なバージョンは、高速プロセッサと大容量のオンボード メモリを備えています。内部ファスト イーサネット ポート（6 アクセス ポイント バージョン）または内部ギガビット イーサネット ポート（8 アクセス ポイントおよび 12 アクセス ポイント バージョン）によって、ルータと統合コントローラが接続されます。ルータと内部コントローラではそれぞれ異なるソフトウェア バージョンが実行されており、これらのソフトウェア バージョンは個別にアップグレードする必要があります。詳細は、次のドキュメントを参照してください。

- 『Cisco Wireless LAN Controller Network Module Feature Guide』
- 『Cisco 28/37/38xx Series Hardware Installation Guide』

これらのドキュメントには、次の URL からアクセスできます。

http://www.cisco.com/en/US/products/hw/wireless/index.html

（注）　Cisco 2801 サービス統合型ルータでは、コントローラ ネットワーク モジュールはサポートされません。

Catalyst 3750G Integrated Wireless LAN Controller Switch

Catalyst 3750G Integrated Wireless LAN Controller Switch は、Catalyst 3750 スイッチと Cisco 4400 シリーズ コントローラが統合されたもので、最大 25 個または 50 個の Lightweight アクセス ポイントをサポートします。スイッチには、スイッチとコントローラを接続する内部ギガバイト イーサネット ポートが 2 個装備されています。スイッチと内部コントローラではそれぞれ異なるソフトウェア バージョンが実行されており、これらのソフトウェア バージョンは個別にアップグレードする必要があります。詳細は、次のドキュメントを参照してください。

- 『Catalyst 3750G Integrated Wireless LAN Controller Switch Getting Started Guide』
- 『Catalyst 3750 Switch Hardware Installation Guide』
- 『Release Notes for the Catalyst 3750 Integrated Wireless LAN Controller Switch, Cisco IOS Release 12.2(25)FZ』

これらのドキュメントには、次の URL からアクセスできます。

http://www.cisco.com/en/US/products/hw/switches/ps5023/tsd_products_support_series_home.html

Cisco UWN Solution の有線接続

Cisco UWN Solution のコンポーネントは、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。ここでは、有線接続について説明します。

- 2000 シリーズ コントローラ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。
- 2100 シリーズ コントローラをネットワークに接続するときは、1 ～ 6 本の 10/100BASE-T イーサネット ケーブルを使用します。
- 4402 コントローラ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。4404 コントローラをネットワークに接続するときは、最大 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。ギガビット イーサネット接続を冗長化しておけば、ネットワーク上のいずれかの箇所で障害が発生した場合でも、それを迂回できます。
- Cisco Catalyst 6500 シリーズ スイッチにインストールされた Wireless Services Module（WiSM）内のコントローラをネットワークに接続するときは、スイッチのスイッチ ポートを使用します。
- Cisco サービス統合型ルータにインストールされている Wireless LAN Controller ネットワーク モジュールをネットワークに接続するときは、ルータのポートを使用します。
- Catalyst 3750G Integrated Wireless LAN Controller Switch のコントローラをネットワークに接続するときは、スイッチのポートを使用します。
- Cisco 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。標準の CAT-5 ケーブルを使用して、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 ポイントへ電力を供給することもできます。この電源分配プランを使用すると、個々のアクセス ポイント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 UWN Solution 無線 LAN

Cisco UWN 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 WLAN には、それぞれ異なる WLAN ID（1 ～ 16）と WLAN SSID（WLAN 名）が割り当てられます。また、一意のセキュリティ ポリシーを割り当てることもできます。ソフトウェア リリース 3.2 以降を使用すると、同じ無線 LAN 上で静的 WEP と動的 WEP の両方を設定できます。

Lightweight アクセス ポイントでは、すべてのアクティブな Cisco UWN 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）　コントローラが最適な性能と容易な管理で動作できるよう、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 UWN 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。

無線 LAN の設定については、第 6 章を参照してください。

ID ネットワーキング

コントローラでは、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、MAC フィルタリングを使用するか、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 UWN Solution オペレータがクライアントに対して MAC フィルタリングを設定するときに、別の VLAN を MAC アドレスに割り当てることができます。このことを使用して、クライアントをオペレーティング システムによって自動的に管理インターフェイスまたはオペレータ定義インターフェイスに再ルーティングすることができます。インターフェイスはそれぞれ、独自の VLAN、ACL、DHCP サーバ、および物理ポート割り当てが設定されています。この MAC フィルタリングはおおまかな AAA Override として使用でき、通常、いずれも AAA（RADIUS またはその他の）Override より優先されます。

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 が有効な場合は、コントローラで設定されている MAC フィルタリング パラメータよりも AAA Override が優先されます。特定の MAC アドレスで使用できる AAA Override がない場合は、コントローラの既存の MAC フィルタリング パラメータがオペレーティング システムによって使用されます。この AAA（RADIUS またはその他の）Override は詳細な AAA Override として使用できますが、Allow AAA Override が有効な場合のみ、MAC フィルタリングより優先されます。

どのような場合でも、Override パラメータ（オペレータ定義のインターフェイスや QoS など）をコントローラの設定で事前に定義しておく必要があります。

いずれの場合も、レイヤ 2 認証が使用されるかレイヤ 3 認証が使用されるかにかかわらず、AAA サーバまたは MAC フィルタリングで指定されている QoS と ACL がオペレーティング システムによって使用されます。

また、MAC フィルタリング、802.1X、または WPA レイヤ 2 認証を行うように設定されている場合、オペレーティング システムが行うのはクライアントをデフォルトの Cisco UWN Solution 無線 LAN VLAN から別の VLAN に移動することだけです。無線 LAN の設定については、第 6 章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 サポートのための RADIUS 属性）で定義されている標準の「RADIUS による VLAN 名 / 番号の割り当て」機能を使用して AAA サーバが VLAN の番号または名前を返せるようにするための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）FVLAN
- 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、2100、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。

ファイル転送

Cisco UWN Solution オペレータは、GUI、CLI コマンド、または Cisco WCS 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コントローラにアップロードしたり、コントローラからダウンロードしたりできます。

- CLI コマンドの使用方法については、「コントローラとのファイルのやり取り」の項（P. 8-7）を参照してください。
- Cisco WCS を使用してソフトウェアをアップグレードする方法については、『Cisco Wireless Control System Configuration Guide』を参照してください。以下の URL をクリックすると、このガイドを参照できます。

  http://www.cisco.com/en/US/products/ps6305/products_installation_and_configuration_guides_list.html

Power over Ethernet

Lightweight アクセス ポイントは、イーサネット ケーブルを介して、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、10BASE-T 仕様では 200m に制限されています。

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。

スタートアップ ウィザード

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り、工場出荷時のデフォルトにリセットした後でコントローラの電源を入れると、起動スクリプトによりスタートアップ ウィザードが実行され、初期設定を要求するプロンプトが表示されます。スタートアップ ウィザードでは次のことを行います。

- コントローラに 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）。
- コントローラがサービス ポートを使用して GUI、CLI、または Cisco WCS（直接的にまたは間接的に）と通信できるように設定します。この設定を行うには、有効な IP 設定プロトコル（none または DHCP）を入力し、none の場合は IP アドレスとネットマスクを入力します。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。
- コントローラ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 アドレスを入力ます。これは、クライアント、コントローラ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 転送モードを入力します。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. 1-7）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 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します。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。
- スタートアップ ウィザードから RADIUS サーバを設定する場合は、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要求します。
- 国コードを収集します。
- 802.11a、802.11b、および 802.11g 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。

スタートアップ ウィザードの使用方法については、「設定 ウィザードの使用方法」の項（P. 4-2）を参照してください。

Cisco Wireless LAN Controller のメモリ

コントローラには 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コントローラ設定が保持され、NVRAM （非揮発性 RAM）にはリブート設定が保持されます。コントローラのオペレーティング システムを設定すると、揮発性 RAM の内容が変更されます。したがって、揮発性 RAM の設定を NVRAM に保存し、コントローラが現在の設定でリ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。

- 設定 ウィザードの使用方法
- コントローラ設定のクリア
- Saving Configurations
- Resetting the Controller
- 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

各コントローラには、定義された数の Lightweight アクセス ポイント用通信ポートが装備されています。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。
- 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 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 コントローラが割り当てられておらず、アクティブなマスター コントローラがない場合、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コントローラにアソシエートを試み、未使用ポートを使用してそのディスカバリ 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 へのネットワーク接続

すべてのコントローラは、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。コントローラは、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コントローラ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 および 2100 シリーズ Wireless LAN Controller（P. 1-18）
- Cisco 4400 シリーズ Wireless LAN Controller（P. 1-19）

（注）　コントローラのポートの設定とインターフェイスへの割り当てについては、第 3 章を参照してください。

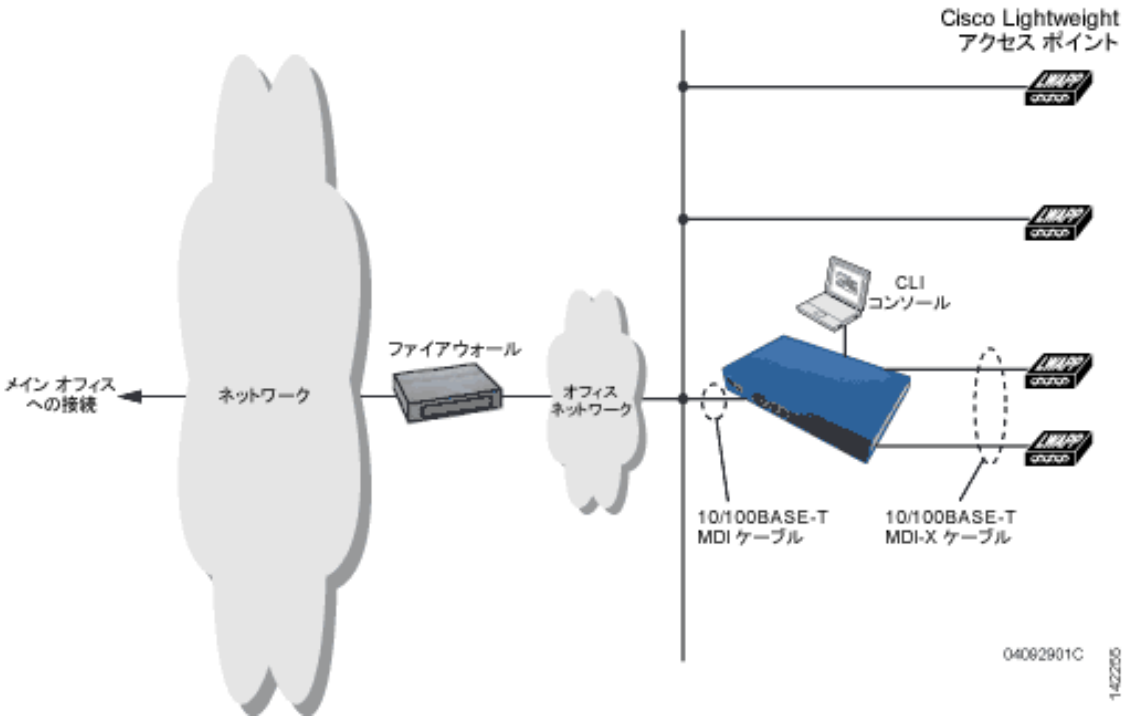
Cisco 2000 および 2100 シリーズ Wireless LAN Controller

Cisco 2000 および 2100 シリーズ コントローラでは、ネットワークとの通信には任意の物理データ ポートを 1 つ使用できます。また、ポートの 1 つに論理管理インターフェイスを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。

- 最大 4 つの 10/100BASE-T ケーブルを、2000 シリーズ コントローラ シャーシの 4 つの背面パネル データ ポートに接続できます。
- 最大 6 本の 10/100BASE-T ケーブルを 2100 シリーズ コントローラ シャーシの 6 つの背面パネル データ ポートに接続できます。2100 シリーズには、2 個の PoE ポートもあります（ポート 7 および 8）。

図 1-4 は、2000 および 2100 シリーズ コントローラへの接続を示しています。

図 1-4　2000 および 2100 シリーズ コントローラへの物理ネットワーク接続



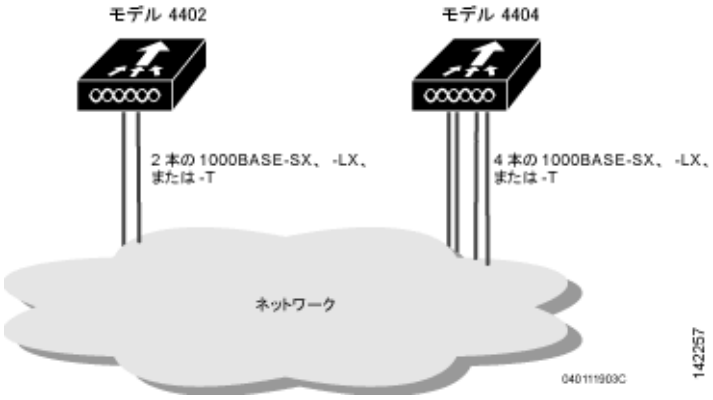
Cisco 4400 シリーズ Wireless LAN Controller

Cisco 4400 シリーズ コントローラは、1 つまたは 2 つの物理データ 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 コントローラでは、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 コントローラでは、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 1-5 は、4400 シリーズ コントローラへの接続を示しています。

図 1-5　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



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 に接続して、アドホック無線ネットワークを確立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。

スキャナを使用して不正なアクセス ポイントを手動で検出しなくても、Cisco UWN Solution では、MAC アドレスと IP アドレスに基づいて、管理対象のアクセス ポイントに不正なアクセス ポイントを検出させ、その情報を自動的に収集することによって、システム オペレータは不正なアクセス ポイントを特定してタグ付けし、監視することができます。また、オペレーティング システムを使用し、4 つの 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 ポイントの検出、タギング、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 ポイントを見つけます。詳細は、『Cisco Wireless Control System Configuration Guide』を参照してください。
- 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 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 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、不正なアクセス ポイントに関するレポートをコントローラから定期的に受け取り、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、コントローラから受信した MAC アドレスが一致していることがわかると、コントローラに対して不正なアクセス 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 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。