セキュリティ ソリューションの設定

この章では、無線 LAN のセキュリティ ソリューション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 セキュリティ

Cisco Wireless LAN Solution セキュリティ ソリューションは、802.11 アクセス ポイントのセキュリティを構成する潜在的に複雑なレイヤ 1、レイヤ 2、およびレイヤ 3 を 1 つの単純なポリシー マネージャにまとめたもので、システム全体のセキュリティ ポリシーを無線 LAN 単位でカスタマイズできます。これは、単純で、統一された、体系的なセキュリティ管理ツールを提供します。

企業での無線 LAN 展開の最も大きな障害の 1 つが、脆弱な独立型の暗号化方式である Wired Equivalent Privacy（WEP）です。低価格のアクセス ポイントの登場も新たな問題で、企業ネットワークに接続して man-in-the-middle アタックおよび DoS 攻撃（サービス拒絶攻撃）に利用される可能性があります。また、次々に追加されるセキュリティ ソリューションの複雑さから、多くの IT マネージャが無線 LAN セキュリティの最新技術を採用することをためらっています。

レイヤ 1 ソリューション

Cisco Wireless LAN Solution オペレーティング システムのセキュリティ ソリューションによって、すべてのクライアントはアクセスの試行回数を、オペレータが設定した回数までに制限されます。クライアントがその制限回数内にアクセスできなかった場合、オペレータが設定したタイマーが切れるまでそのクライアントは自動的に除外（アクセスをブロック）されます。そのオペレーティング システムは、無線 LAN ごとに SSID ブロードキャストを無効にすることもできます。

レイヤ 2 ソリューション

上位レベルのセキュリティと暗号化が必要な場合、ネットワーク管理者は、Extensible Authentication Protocol（EAP; 拡張認証プロトコル）を使用する 802.1X 動的キーや Wi-Fi Protected Access（WPA）動的キーなど業界標準のセキュリティ ソリューションも実装できます。Cisco Wireless LAN Solution の WPA 実装には、Advanced Encryption Standard（AES）動的キー、Temporal Key Integrity Protocol + Message Integrity Code Checksum（TKIP + Michael）動的キー、または WEP 静的キーが含まれます。無効化も使用され、オペレータが設定した回数だけ認証の試行に失敗すると、自動的にレイヤ 2 アクセスがブロックされます。

どの無線セキュリティ ソリューションを採用した場合も、コントローラとアクセス ポイントとの間のすべてのレイヤ 2 有線通信は、Lightweight Access Point Protocol（LWAPP;Lightweight アクセス ポイント プロトコル）トンネルを使用してデータを渡すことにより保護されます。

レイヤ 3 ソリューション

WEP の問題は、Virtual Private Network（VPN; バーチャル プライベート ネットワーク）、Layer Two Tunneling Protocol（L2TP; レイヤ 2 トンネリング プロトコル）、および IP security（IPSec）プロトコルなどの業界標準のレイヤ 3 セキュリティ ソリューションを使用して解決できます。Cisco Wireless LAN Solution の L2TP 実装には IPsec が含まれており、その IPSec 実装には、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、および 3 つのオプション レベルの暗号化である DES（ANSI X.3.92 データ暗号規格）、3DES（ANSI X9.52-1998 データ暗号規格）、または AES/CBC（Advanced Encryption Standard/Cipher Block Chaining）が含まれています。無効化も使用され、オペレータが設定した回数だけ認証の試行に失敗すると、自動的にレイヤ 3 アクセスがブロックされます。

Cisco WLAN Solution の IPSec 実装には、Message Digest Algorithm（MD5）や Secure Hash Algorithm-1（SHA-1）を使用した業界標準の認証も含まれています。

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）フィルタリングがサポートされています。このフィルタリングは、802.11 アクセス カード MAC アドレスの既知のリストがある小規模のクライアント グループに適しています。Cisco Wireless LAN Solution は、ローカルおよび RADIUS ユーザ / パスワード認証もサポートします。この認証は、小規模から中規模のクライアント グループに適しています。

シングル ポイントでの設定ポリシー マネージャのソリューション

Cisco Wireless LAN Solution に WCS を装備した場合、システム全体のセキュリティ ポリシーを無線 LAN ごとに設定できます。スモール オフィス、ホームオフィス（SOHO）のアクセス ポイントでは、アクセス ポイントごとにセキュリティ ポリシーを個別に設定する必要があります。また、複数のアクセス ポイントにわたってセキュリティ ポリシーを設定するには、サードパーティのアプライアンスを使用する必要があります。Cisco Wireless LAN Solution セキュリティ ポリシーは WCS からシステム全体に適用できるため、エラーを除去することができ、全体的な作業量が大幅に減少します。

不正アクセス ポイントのソリューション

この項では、不正アクセス ポイントに対するセキュリティ ソリューションについて説明します。

不正アクセス ポイントの問題

不正アクセス ポイントは、正規のクライアントをハイジャックし、プレーン テキストまたは他の DoS 攻撃や man-in-the-middle アタックを使用することによって、無線 LAN の運用を妨害します。つまり、ハッカーは不正アクセス ポイントを使用して、パスワードやユーザ名などの機密情報を取得できるのです。すると、ハッカーは一連の Clear To Send（CTS; クリア ツー センド）フレームを送信できるようになります。このフレームはアクセス ポイントを模倣し、特定の無線 LAN クライアント アダプタに伝送して、他のすべてのアダプタには待機するように指示します。その結果、正規のクライアントは、無線 LAN リソースに接続できなくなります。したがって、無線 LAN サービス プロバイダーは、空間からの不正アクセス ポイントの締め出しに強い関心を持っています。

オペレーティング システムのセキュリティ ソリューションでは、「不正アクセス ポイントのタギングと阻止」の説明にあるように、Radio Resource Management（RRM）機能を使用して、すべての近隣アクセス ポイントを継続的に監視し、不正アクセス ポイントを自動的に検出し、それらを特定します。

不正アクセス ポイントのタギングと阻止

WCS を使用して Cisco Wireless LAN Solution を監視している場合、不正アクセス ポイントが検出されるとフラグが生成され、既知の不正アクセス ポイントが MAC アドレスで表示されます。オペレータは、それぞれの不正アクセス ポイントに最も近いアクセス ポイントの場所を示すマップを表示できます。その後、それらを Known または Acknowledged 不正アクセス ポイントとしてマークする（追加の処置はなし）、それらを Alert 不正アクセス ポイントとしてマークする（監視し、アクティブになったときに通知）、それらを Contained 不正アクセス ポイントとしてマークする（1 つから 4 つのアクセス ポイントに対して、不正アクセス ポイントのクライアントが不正アクセス ポイントとアソシエートするたびにそれらの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によって阻止する）のいずれかを実行します。

統合されたセキュリティ ソリューション

Cisco Wireless LAN Solution では、次の統合されたセキュリティ ソリューションも用意されています。

- Cisco Wireless LAN Solution オペレーティング システムのセキュリティは、堅牢な 802.1X AAA（認証、認可、アカウンティング）エンジンを中心に構築されており、オペレータは、Cisco Wireless LAN Solution 全体にわたってさまざまなセキュリティ ポリシーを迅速に設定および適用できます。
- コントローラおよびアクセス ポイントには、システム全体の認証および認可プロトコルがすべてのポートおよびインターフェイスに装備され、最大限のシステム セキュリティが実現されています。
- オペレーティング システムのセキュリティ ポリシーは個別の無線 LAN に割り当てられ、アクセス ポイントは設定されたすべての無線 LAN（最大 16）に同時にブロードキャストします。このポリシーにより、干渉を増加し、システム スループットを低下するアクセス ポイントの追加が不要になる場合があります。
- コントローラは、安全に IPSec VPN クライアントを終了し、これにより中央の VPN コンセントレータの負荷を軽減できます。
- オペレーティング システムのセキュリティは、RRM 機能を使用して、干渉およびセキュリティ侵犯がないか継続的に空間を監視し、それらを検出したときはオペレータに通知します。
- オペレーティング システムのセキュリティは、業界標準の AAA サーバで動作し、システム統合が単純で簡単です。
- オペレーティング システムのセキュリティ ソリューションは、通常、高い処理能力を必要とする、包括的なレイヤ 2 およびレイヤ 3 の暗号化アルゴリズムを実現します。コントローラに VPN/ 拡張セキュリティ モジュールを装備することで、高度なセキュリティ設定に必要なハードウェアとしての機能も実現でき、暗号化を別のサーバで行う必要はありません。

WCS を使用して Cisco Wireless LAN Solution のレイヤ 2 モードからレイヤ 3 モードへの変換

WCS ユーザ インターフェイスを使用して、Cisco Wireless LAN Solution をレイヤ 2 モードからレイヤ 3 LWAPP 転送モードに変換する手順は、次のとおりです。

（注） この手順を実行すると、コントローラが再度ブートしてアクセス ポイントがコントローラと再アソシエートするまで、アクセス ポイントはオフラインになります。

（注） レイヤ 3 モードでは、コントローラが接続されているすべてのサブネットに、少なくとも 1 台の DHCP サーバが必要です。この手順を完了すると、コントローラにアソシエートしているアクセス ポイントにコントローラの IP アドレスが保存されます。各アクセス ポイントは、電源の投入と同時にローカル DHCP サーバから IP アドレスを取得し、プライマリ、セカンダリ、またはターシャリ コントローラに接続します。

（注） レイヤ 3 モードでは、コントローラおよびアクセス ポイントを含むすべてのサブネットが互いにルーティング可能である必要があります。

ステップ 1　レイヤ 3 モードで Cisco Wireless LAN Solution を使用するには、アクセス ポイント マネージャ インターフェイスを作成し、各コントローラとコントローラにアソシエートしているアクセス ポイントとの間の通信を管理する必要があります。このインターフェイスには、固定 IP アドレスが必要です。IP アドレスは、管理インターフェイスの IP アドレスとは異なる必要がありますが、管理インターフェイスと同じサブネットにあってもかまいません。

ステップ 2　コントローラとアクセス ポイントはすべて同じサブネット上に配置し、レイヤ 2 のデバイス経由でのみ接続するようにします。

（注） 変換を実行する前に、コントローラおよびアソシエートしているアクセス ポイントをレイヤ 3 モードで動作するように設定する必要があります。

ステップ 3　WCS ユーザ インターフェイスにログインします。

ステップ 4　**Configure > Access Points** の順にクリックし、All Access Points ページに移動します。

ステップ 5　各アクセス ポイントに対して、アクセス ポイント名をクリックして プライマリ、セカンダリ、およびターシャリ コントローラの名前が正しいことを確認します。これらの名前を変更した場合、**Save** をクリックして変更を保存します。

ステップ 6　All Access Points ページでは、アクセス ポイントがコントローラにアソシエートしていることを確認してから次の手順に進みます。

（注）　この手順を実行しないと、変換を完了した後にアクセス ポイントがコントローラにアソシエートできなくなる場合があります。

ステップ 7　LWAPP 転送モードをレイヤ 2 からレイヤ 3 に変更する手順は、次のとおりです。

a. **Configure > Controllers** の順にクリックし、All Controllers ページに移動します。
b. 目的のコントローラの IP アドレスをクリックして、*IP Address* > Controller Properties ページを表示します。
c. サイドバーで、**System > General** の順にクリックして、*IP Address* > General ページを表示します。
d. LWAPP 転送モードを **Layer3** に変更し、**Save** をクリックします。次のメッセージが表示されます。

```
Please reboot the system for the LWAPP Mode change to take effect.
```

e. **OK** をクリックします。

ステップ 8　新しいアクセス ポイント マネージャ インターフェイスを作成する手順は、次のとおりです。

a. **Configure > Controllers** の順にクリックし、All Controllers ページに移動します。
b. 目的のコントローラの IP アドレスをクリックして、*IP Address* > Controller Properties ページを表示します。
c. サイドバーで、**System > Interfaces** の順にクリックして、*IP Address* > Interface ページを表示します。
d. Select a Command ドロップダウン メニューから、**Add Interface** を選択し、**GO** をクリックします。
e. *IP Address* > Interface ページで次の情報を入力します。
   - ap-manager インターフェイス名
   - VLAN 識別子（必要な場合）
   - ステップ 1 で取得した access point manager IP address
   - gateway IP address
   - コントローラへのディストリビューション システム接続の physical port number
   - primary DHCP server IP address
   - secondary DHCP server IP address

（注）　このサブネット上に 2 番目の DHCP サーバがない場合、これは primary DHCP server IP address と同じになります。

f. 必要に応じて、アクセス コントロール リスト（ACL）名をドロップダウン メニューから選択します。
g. **Save** をクリックし、アクセス ポイント マネージャ インターフェイスをインターフェイスのリストに追加します。
h. *IP Address* > Interface ページで、WCS によって ap-manager インターフェイス名がインターフェイスのリストに追加されていることを確認します。
i. また、management インターフェイスが ap-manager インターフェイスとは異なる IP アドレスで適切に設定されていることを確認します。

ステップ 9　新しい設定を保存してコントローラを再起動する手順は、次のとおりです。

a. **Configure > Controllers** の順にクリックし、All Controllers ページに移動します。

b. 目的のコントローラの IP アドレスをクリックして、*IP Address* > Controller Properties ページを表示します。

c. サイドバーで、**System > Commands** の順にクリックして、*IP Address* > Controller Commands ページを表示します。

d. Administrative Commands の下で、**Save Config To Flash** を選択し **GO** をクリックして、変更した設定をコントローラに保存します。

e. Administrative Commands の下で、**Reboot** を選択し **GO** をクリックして、コントローラをリブートします。

f. **OK** をクリックし、保存して再度ブートすることを確認します。

ステップ 10　コントローラが再度ブートした後で LWAPP 転送モードがレイヤ 3 になっていることを確認する手順は、次のとおりです。

a. **Monitor > Devices** > **Controllers** の順にクリックし、Controllers > Search Results ページに移動します。

b. 目的のコントローラの IP アドレスをクリックして、Controllers > *IP Address* > Summary ページを表示します。

c. General の下で、現在の LWAPP 転送モードが Layer3 になっていることを確認します。

ステップ 11　**Configure > Access Points** の順にクリックし、All Access Points ページに移動します。

ステップ 12　アクセス　ポイントがコントローラにアソシエートしていることを確認してから次の手順に進みます。

（注）　この手順を実行しないと、変換を完了した後にアクセス ポイントが目的のコントローラにアソシエートできなくなる場合があります。

ステップ 13　すべてのアクセス ポイントの電源を切り、レイヤ 3 設定を不揮発性メモリに保存します。

ステップ 14　各アクセス ポイントをネットワーク内の実際の位置に接続します。各アクセス ポイントがプライマリ、セカンダリ、またはターシャリ コントローラに接続し、最新のオペレーティング システム コードのコピーをダウンロードし、コントローラに対してステータスの報告を開始します。この処理には、各アクセス ポイントで数分かかる場合がある点に注意してください。

これで、レイヤ 2 からレイヤ 3 への LWAPP 転送モードの変換が完了しました。ap-manager インターフェイスによって、異なるサブネット上のコントローラとアクセス ポイントとの間におけるすべての通信が制御されます。

WCS を使用して Cisco Wireless LAN Solution のレイヤ 3 モードからレイヤ 2 モードへの変換

WCS ユーザ インターフェイスを使用して、Cisco Wireless LAN Solution をレイヤ 3 モードからレイヤ 2 LWAPP 転送モードに変換する手順は、次のとおりです。

（注）　この手順を実行すると、コントローラが再度ブートしてアクセス ポイントがコントローラと再アソシエートするまで、アクセス ポイントはオフラインになります。

ステップ 1　コントローラとアクセス ポイントはすべて同じサブネット上に配置するようにします。

（注）　変換を実行する前に、コントローラおよびアソシエートしているアクセス ポイントをレイヤ 2 モードで動作するように設定する必要があります。

ステップ 2　WCS ユーザ インターフェイスにログインします。LWAPP 転送モードをレイヤ 3 からレイヤ 2 に変換する手順は、次のとおりです。

a. **Configure > Controllers** の順にクリックし、All Controllers ページに移動します。
b. 目的のコントローラの IP アドレスをクリックして、*IP Address* > Controller Properties ページを表示します。
c. サイドバーで、**System > General** の順にクリックして、*IP Address* > General ページを表示します。
d. LWAPP 転送モードを **Layer2** に変更し、**Save** をクリックします。
e. WCS で次のメッセージが表示された場合、**OK** をクリックします。

```
Please reboot the system for the LWAPP Mode change to take effect.
```

ステップ 3　Cisco Wireless LAN Solution を再起動する手順は、次のとおりです。

a. *IP Address* > Controller Properties ページに戻ります。
b. **System > Commands** の順にクリックして、*IP Address* > Controller Commands ページを表示します。
c. Administrative Commands の下で、**Save Config To Flash** を選択し **GO** をクリックして、変更した設定をコントローラに保存します。
d. **OK** をクリックして、次に進みます。
e. Administrative Commands の下で、**Reboot** を選択し **GO** をクリックして、コントローラをリブートします。
f. **OK** をクリックし、保存して再度ブートすることを確認します。

ステップ 4　コントローラが再度ブートした後で LWAPP 転送モードがレイヤ 2 になっていることを確認する手順は、次のとおりです。

a. **Monitor > Devices** > **Controllers** の順にクリックし、Controllers > Search Results ページに移動します。

b. 目的のコントローラの IP アドレスをクリックして、Controllers > *IP Address* > Summary ページを表示します。

c. General の下で、現在の LWAPP 転送モードが Layer2 になっていることを確認します。

これで、レイヤ 3 からレイヤ 2 への LWAPP 転送モードの変換が完了しました。オペレーティング システムのソフトウェアによって、同じサブネット上のコントローラとアクセス ポイントとの間におけるすべての通信が制御されます。

WCS に対するファイアウォールの設定

WCS サーバと WCS ユーザ インターフェイスがファイアウォールの同じ側にない場合、ファイアウォール上の次のポートが双方向のトラフィックに対してオープンになっていない限り、これらは通信できません。

- ポート 21（FTP）
- ポート 69（TFTP）
- ポート 169（トラップ）
- ポート 443（HTTPS）

これらのポートをオープンにして、WCS サーバと WCS ユーザ インターフェイスとの間の通信を許可するようにファイアウォールを設定します。