Cisco Unified Wireless Network アーキテクチャ：基本セキュリティ機能

Cisco Unified Wireless Network ソリューションは、Wireless Local Area Network（WLAN）エンドポイント、WLAN インフラストラクチャおよびクライアント通信を保護するアーキテクチャと製品セキュリティ機能を使用するエンドツーエンドのセキュリティを提供します。

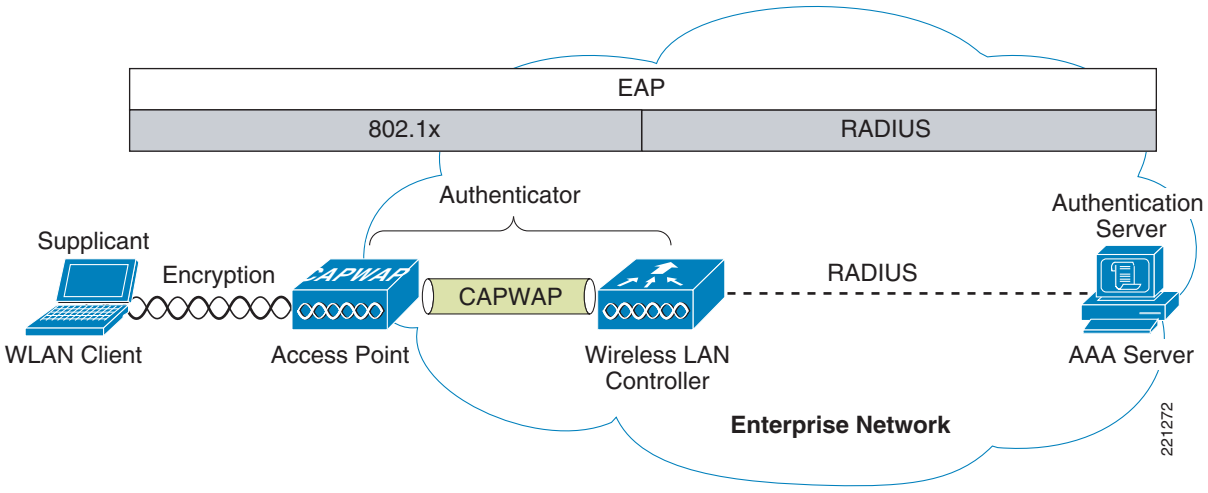
Cisco Unified Wireless Network ソリューションは、IEEE 802.11-2012 標準の基本セキュリティ機能を基盤としています。無線周波数（RF）とネットワーク ベースのセキュリティ機能を強化して全体的なセキュリティを保証します。

セキュアなワイヤレス トポロジ

図 4-1 では、セキュアなワイヤレス トポロジについて説明します。このトポロジは、802.1X 認証プロセスの基本的な役割を持つ次のコンポーネントで構成されます。

- クライアント上に 802.1x サプリカント（無線ソフトウェア）を持つ WLAN クライアント
- 無線アクセスポイント（CAPWAP）プロトコルの管理とプロビジョニングを使用するアクセス ポイント（AP）およびワイヤレス LAN コントローラ（WLC）
- クライアントと認証サーバの間で Extensible Authentication Protocol（EAP）パケットを送受信する RADIUS プロトコル
- 認証サーバとしての AAA（認証、許可、アカウンティング）サーバ

図 4-1　セキュアなワイヤレス トポロジ



WLAN のセキュリティ メカニズム

セキュリティは WLAN ネットワークの認証および暗号化を使用して実行されます。WLAN ネットワークのセキュリティ メカニズムは次のとおりです。

- オープン認証（暗号化なし）
- Wired Equivalent Privacy（WEP）
- シスコの WEP 拡張（Cisco Key Integrity Protocol + Cisco Message Integrity Check）
- Wi-Fi Protected Access（WPA）
- Wi-Fi Protected Access 2（WPA2）
- 拡張ローカル モード（ELM）の Cisco Adaptive Wireless Intrusion Prevention System（wIPS）

シスコの Wired Equivalent Privacy（WEP）Extension

元の 802.11 セキュリティ メカニズムである WEP は*何らかのレベルのセキュリティを適用するスタティック暗号化方式セキュリティであり、ビジネス コミュニケーションを保証するには不十分である*と一般的には見られています。Cisco WLAN 製品では、次のように WEP を拡張することで、その不足に対応しました。

- Cisco Key Integrity Protocol（CKIP）
- Cisco Message Integrity Check（CMIC）

シスコによる WEP の拡張は、Cisco WEP Extension と総称されています。

Wi-Fi Protected Access（WPA）

802.11 の WEP 標準が、暗号化キーの管理方法の問題の処理に失敗しました。暗号化メカニズム自体に問題があることがわかったため、クライアントのトラフィックを監視するだけで WEP キーが獲得できました。IEEE 802.11i 標準は、元の 802.11 WEP の標準に見つかったこれらのセキュリティの問題に対処します。

WPA および WPA2 は Wi-Fi Alliance で定義された 802.11i ベースのセキュリティ ソリューションです。Wi-Fi Alliance は IEEE 802.11 製品の相互運用性を証明し、あらゆる市場セグメントにわたって無線 LAN の標準を推進します。Wi-Fi Alliance の一連のテストでは、他の Wi-Fi 認定製品との相互運用性の認定を取得するために製品をテストする方法を定義します。

WPA は Temporal Key Integrity Protocol（TKIP）を使用して、事前共有キーまたは RADIUS/802.1x ベースの認証による暗号化とダイナミックな暗号キーの生成を行います。WPA で導入されたメカニズムは、ハードウェアをアップグレードしなくても、より堅牢なセキュリティを WEP ソリューションに提供するように設計されています。

Wi-Fi Protected Access 2（WPA2）

WPA2 は、承認された IEEE 802.11i 標準を基礎とする次世代の Wi-Fi セキュリティであり、802.11i 標準の Wi-Fi Alliance の相互運用性を実装することによって認証されます。WPA2 は、企業と個人の分類の両方で認証を行います。

企業の分類には、RADIUS/802.1x ベースの認証と事前共有キーへの対応が必要となります。個人の分類にはクライアントと AP で共有する共通キーのみ必要です。

WPA2 で導入された Advanced Encryption Standard（AES）の新しいメカニズムでは、一般的に WLAN クライアントと AP のハードウェアのアップグレードが必要となります。ただし、すべてのシスコ CAPWAP ハードウェアは WPA2 に対応しています。

802.1X

802.1X は、802.11i のセキュリティ ワーク グループによって採用された、ポート ベースのアクセス コントロール用 IEEE フレームワークです。このフレームワークは、WLAN ネットワークに認証されたアクセスを提供します。

- 802.11 アソシエーション プロセスは、AP の各 WLAN クライアントに対する「仮想」ポートを作成します。
- この AP により、802.1X ベースのトラフィックを除くすべてのデータ フレームがブロックされます。
- 802.1X フレームは EAP 認証パケットを伝送します。EAP 認証パケットはそこから AP によって AAA サーバに渡されます。
- EAP 認証に成功すると、AAA サーバは AP に EAP 成功メッセージを送信します。その後 AP によって、WLAN クライアントから仮想ポートへデータ トラフィックが渡されることが許可されます。
- 仮想ポートを開く前に、WLAN クライアントと AP の間にデータ リンク暗号化が確立されます。これは、クライアントを認証するように設定されたポートに他の WLAN クライアントがアクセスできないようにするためです。

認証および暗号化

Cisco Wireless Security Suite は、必須または既存の認証、プライバシー、クライアント インフラストラクチャを基礎とするセキュリティのアプローチのオプションを提供します。Cisco Wireless Security Suite では、ELM 機能を含む WPA、WPA2、WEP Extesion および wIPS をサポートします。

次のオプションを使用できます。

- 次の EAP 方式を使用した 802.1X に基づく認証：
  - Cisco LEAP、すなわち Secure Tunneling（EAP-FAST）を介した EAP-Flexible Authentication
  - PEAP - Generic Token Card（PEAP-GTC）
  - PEAP - Microsoft Challenge Authentication Protocol Version 2（PEAP-MSCHAPv2）
  - EAP-Transport Layer Security（EAP-TLS）
  - EAP-Subscriber Identity Module（EAP-SIM）
- 暗号化：
  - AES-CCMP Encryption WPA2
  - TKIP 暗号化の拡張：WPA/WPA2 または WEP TKIP Cisco Key Integrity Protocol（CKIP）、および Cisco Message Integrity Check（CMIC）を介したキー ハッシング（パケットごとのキーイング）およびブロードキャスト キー ローテーション

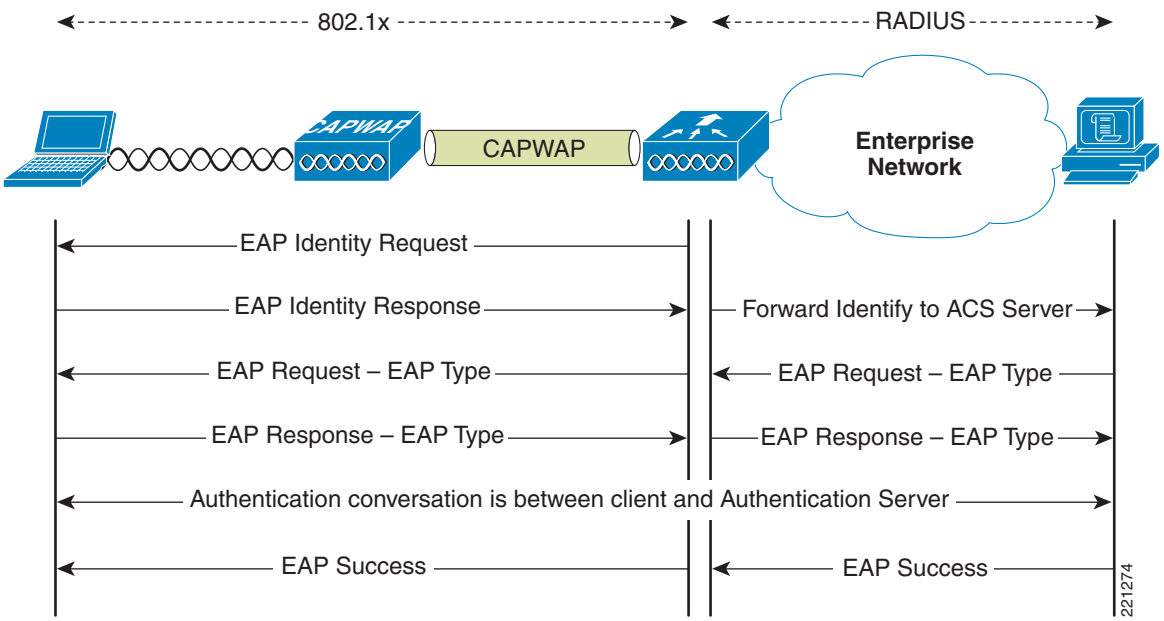
Extensible Authentication Protocol（拡張認証プロトコル）

Extensible Authentication Protocol（EAP）は、転送プロトコルから認証プロトコルを分離する必要があることを規定する IETF RFC です。これにより、802.1X や UDP、RADIUS などのトランスポート プロトコルによって EAP プロトコルを伝送できるようになります。認証プロトコル自体は変わりません。基本の EAP プロトコルには次の 4 種類のパケット タイプが含まれます。

- EAP 要求：要求パケットがオーセンティケータによってサプリカントに送信されます。各要求には type フィールドがあり、要求されている内容を示します。これには、使用されるサプリカント アイデンティティや EAP タイプなどが含まれます。シーケンス番号により、オーセンティケータおよびピアは、各 EAP 要求に対応する EAP 応答を一致できます。
- EAP 応答：応答パケットがサプリカントによってオーセンティケータに送信された後、シーケンス番号を使用して最初の EAP 要求と照合します。EAP 応答のタイプは通常 EAP 要求と一致しますが、応答が否定応答（NAK）の場合は除きます。
- EAP 成功：認証の成功が発生すると、成功パケットがオーセンティケータからサプリカントへ送信されます。
- EAP 失敗：認証の失敗が発生すると、失敗パケットがオーセンティケータからサプリカントへ送信されます。

EAP を 802.11i 準拠のシステムで使用すると、AP は EAP パススルー モードで動作します。パススルー モードではコード ID と長さフィールドを検査し、その後受信した EAP パケットをクライアント サプリカントから AAA に転送します。AAA サーバからオーセンティケータによって受信された EAP パケットが、サプリカントに転送されます。図 4-2 では、EAP プロトコルのフローの例を示します。

図 4-2　EAP プロトコルのフロー



認証

要件に応じて、安全な無線の展開には PEAP や EAP-TLS、EAP-FAST などのさまざまな認証プロトコルが使用されます。プロトコルに関係なく、無線の展開には 802.1X、EAP および RADIUS が基本的な伝送手段としてかならず使用されます。

これらのプロトコルにより、WLAN クライアントの認証の成功に基づいたネットワーク アクセス コントロールが可能になります。その逆も同様です。このソリューションでは、RADIUS プロトコルによって伝送されるポリシーを介した承認のほか、RADIUS アカウンティングも提供します。

認証の実行に使用する EAP の種類については、以降で詳しく説明します。EAP プロトコルの選択に影響する主な要因は、現在使用されている認証システム（AAA）です。理想的には、セキュアな WLAN を展開するために新しい認証システムを導入する必要はありませんが、すでに使用されている認証システムを活用する必要があります。

サプリカント

市場で入手可能なさまざまな EAP サプリカントには、使用可能な認証ソリューションと顧客の要望の多様性が反映されています。

表 4-1 では、一般的な EAP サプリカントの概要を示します。

- EAP-FAST：EAP-Flexible Authentication via Secured Tunnel。PEAP で使用されているものと類似したトンネルを使用しますが、公開キー インフラストラクチャ（PKI）を使用する必要はありません。
- PEAP MSCHAPv2：Protected EAP MSCHAPv2。Transport Layer Security（TLS）トンネル（SSL の IETF 標準）を使用して、WLAN クライアントと認証サーバ間でのカプセル化された MSCHAPv2 の交換を保護します。

- PEAP GTC：Protected EAP Generic Token Card（GTC）。TLS トンネルを使用して、Generic Token Card の交換（ワンタイム パスワードや LDAP 認証など）を保護します。
- EAP-TLS：EAP Transport Layer Security。PKI を使用して、WLAN ネットワークと WLAN クライアントの両方を認証します。クライアント証明書および認証サーバの証明書が必要となります。

表 4-1　一般的なサプリカントの比較

	Cisco EAP-FAST	PEAP MS-CHAPv2	PEAP EAP-GTC	EAP-TLS
シングル サインオン（MSFT AD のみ）	あり	あり	あり[1]	あり
ログイン スクリプト（MSFT AD のみ）	あり	あり	一部	あり[2]
パスワード変更（MSFT AD）	あり	あり	あり	該当なし
Microsoft AD データベース サポート	あり	あり	あり	あり
ACS ローカル データベース サポート	あり	あり	あり	あり
LDAP データベース サポート	あり[3]	なし	あり	あり
OTP 認証サポート	あり[4]	なし	あり	なし
RADIUS サーバ証明書は必要か？	なし	あり	あり	あり
クライアント証明書は必要か？	なし	なし	なし	あり
匿名	あり	あり[5]	あり[6]	なし

1. サプリカントに依存
2. マシン アカウントとマシン認証はスクリプトをサポートするために必要です。
3. 自動プロビジョニングは、LDAP データベースではサポートされていません。
4. サプリカントに依存
5. サプリカントに依存
6. サプリカントに依存

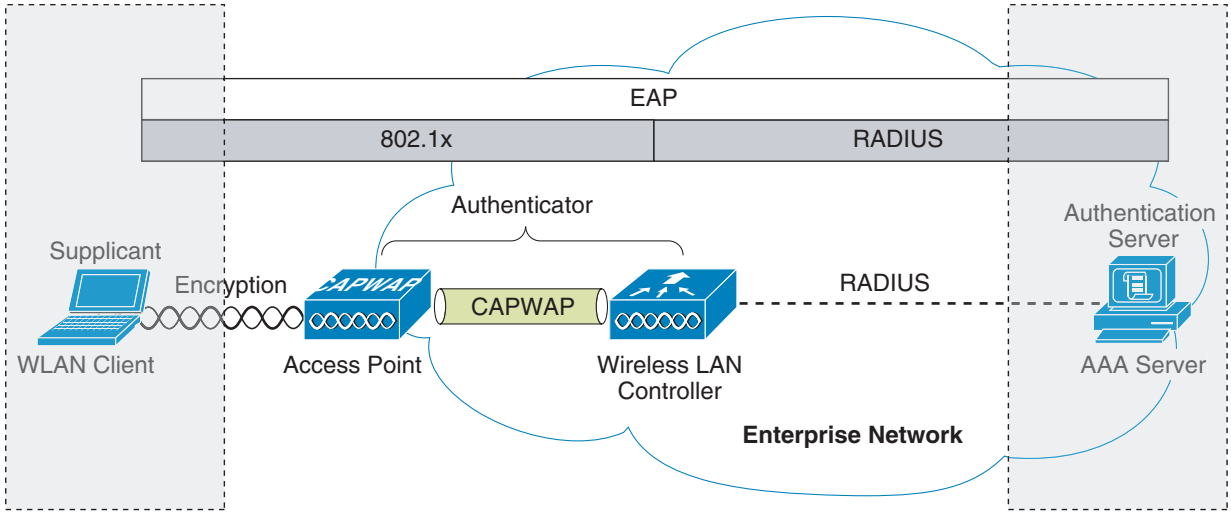
オーセンティケータ

WLC は、802.1X ベースのサプリカントと RADIUS 認証サーバ間で交換される EAP メッセージのリレーとして機能するオーセンティケータです。認証が正常に完了した場合、WLC は次のものを獲得します。

- EAP 成功メッセージを含む RADIUS パケット
- EAP 認証中に認証サーバで生成される暗号化キー
- 通信ポリシーの RADIUS ベンダー固有の属性（VSAs）

図 4-3 では、全体的な認証アーキテクチャ内の*オーセンティケータ*の論理的ロケーションを示します。オーセンティケータは、802.1X プロトコルを使用してネットワーク アクセスを制御し、サプリカントと認証サーバの間で EAP メッセージをリレーします。

図 4-3　オーセンティケータの場所



EAP の交換の手順は次のとおりです。

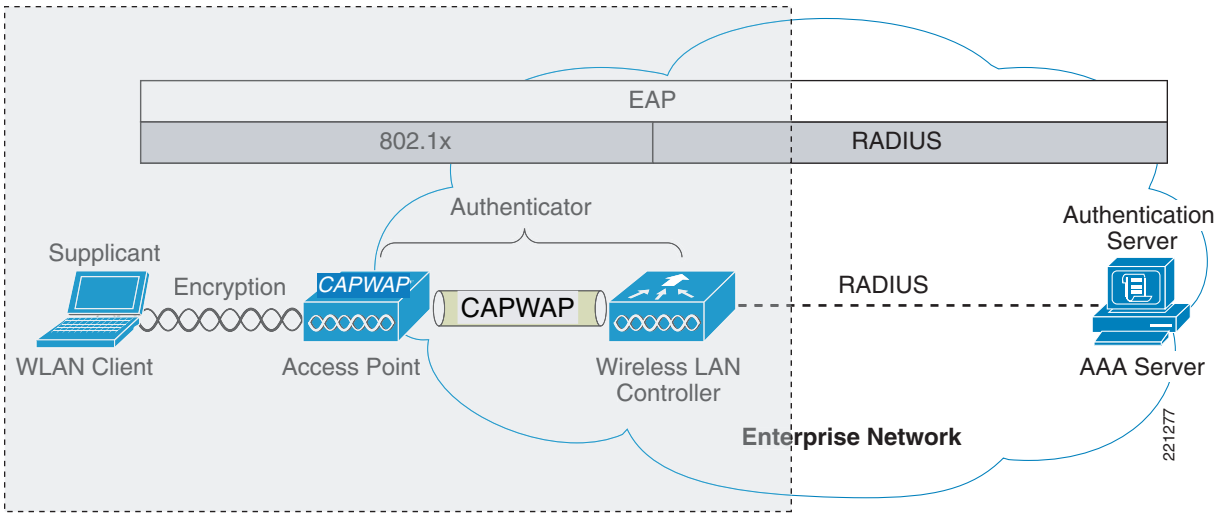
- パケット #1 が、AP によってクライアントに送信されます。このときクライアントの識別情報が要求されます。これにより、EAP 交換が開始されます。
- パケット #2 には、RADIUS サーバに転送されるクライアント ID が含まれています。パケット 2 内のクライアント ID に基づいて、EAP 認証を継続するかどうかを RADIUS サーバが判断します。
- パケット #3 には、認証のための EAP 方式として PEAP を使用する RADIUS サーバ要求が含まれます。実際の要求は、RADIUS サーバで設定された EAP の種類によって異なります。PEAP クライアントが要求を拒否すると、RADIUS サーバは別の種類の EAP を提示できます。
- パケット #4 ～ 8 は、PEAP の TLS トンネル セットアップです。
- パケット #9 ～ 16 は、PEAP 内の認証交換です。
- パケット #17 は、認証が成功したことをサプリカントとオーセンティケータに通知する EAP メッセージです。また、パケット #17 は暗号化キーと認証情報を RADIUS VSA の形式でオーセンティケータに伝送します。

認証サーバ

Cisco Secure Unified Wireless Network ソリューションで使用される認証サーバは、Cisco Access Control Server（ACS）および Cisco Identity Services Engine（ISE）です。ACS および ISE は、Windows 2000 以降のサーバにインストールされているソフトウェアとして、またはアプライアンスとして入手できます。逆に、認証サーバの役割は、IOS AP 上のローカル認証サービス、WLC 内のローカル EAP 認証のサポート、必要な EAP タイプをサポートする任意の AAA サーバに組み込まれた AAA サービスなど、特定の WLAN インフラストラクチャ内で実行できます。

図 4-4 では、RADIUS トンネルを介して EAP 認証を実行する、全体的な無線認証アーキテクチャ内の認証サーバの論理的ロケーションを示しています。

図 4-4　認証サーバのロケーション



EAP 認証が正常に完了すると、認証サーバからオーセンティケータに EAP 成功メッセージが送信されます。このメッセージは、EAP 認証プロセスが正常に行われたことをオーセンティケータに通知し、その結果として WLAN クライアントと AP の間の暗号化されたストリームを作成する際の基礎として使用される Pairwise Master Key（PMK）をオーセンティケータに渡します。

暗号化

暗号化は、ローカル RF ブロードキャスト ネットワーク上にプライバシーを提供する WLAN セキュリティの必須コンポーネントです。新しく展開を行う際は、TKIP（WPA/WPA2）または AES 暗号化を使用する必要があります。

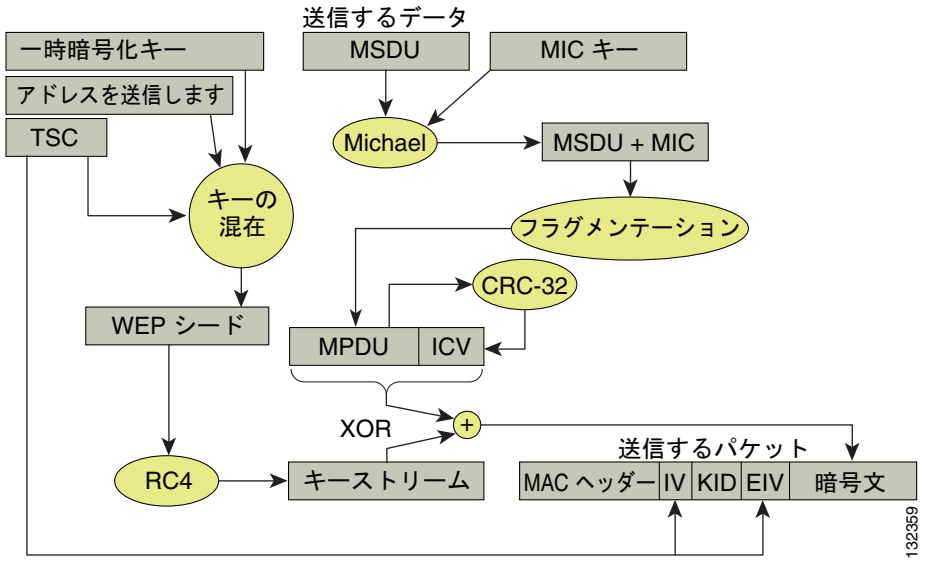
WPA および WPA2 では、暗号キーは Four-Way ハンドシェイク中に取得されます。Four-Way ハンドシェイクについてはこのセクションで後ほど説明します。

TKIP の暗号化

802.11i で指定されたエンタープライズ レベルの暗号化メカニズムは Wi-Fi Alliance による WPA/WPA2 および wIPS、すなわち Temporal Key Integrity Protocol（TKIP）、および Advanced Encryption Standard（AES）として認証されます。TKIP は認定された暗号化方式です。TKIP は、802.11 の WEP 暗号化方式に関連する元の欠点に対処することによって、旧式の WLAN 機器に対するサポートを提供します。TKIP ではこれを行うために、元の RC4 コア暗号化アルゴリズムを利用します。

WLAN クライアント デバイスのハードウェア更新サイクルから、数年間は TKIP が一般的な暗号化となりそうです。AES 暗号化によって、より幅広い IT 業界の標準やベスト プラクティスに沿った WLAN 暗号化規格がもたらされるため、AES 暗号化が望ましい方式です。図 4-5 では、基本的な TKIP のフロー チャートを表示します。

図 4-5　TKIP フロー チャート



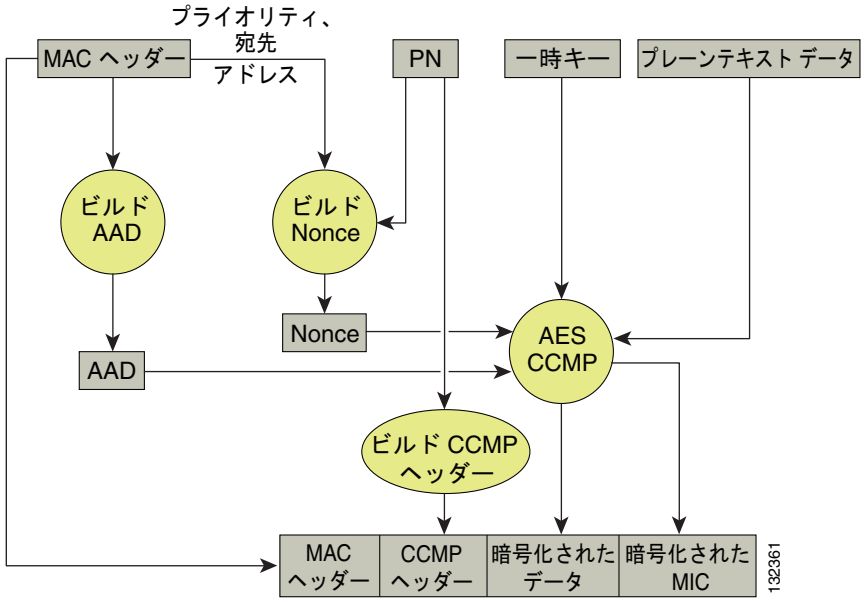
TKIP の主な 2 種類の機能は、MAC Service Data Unit（MSDU）の RC4 暗号化を使用するパケットごとのキーと、暗号化されたパケット内にメッセージ完全性チェック（MIC）を生成することです。パケットごとのキーは、送信アドレス、フレームの初期化ベクトル（IV）、および暗号キーのハッシュです。IV はそれぞれのフレーム送信に従って変化するため、RC4 暗号化に使用されるキーはフレームごとに固有のものです。

MIC は、ユーザ データと MIC キーを組み合わせるために Michael アルゴリズムを使用して生成されるものです。Michael アルゴリズムにはトレードオフがあり、演算のオーバーヘッドが少なくパフォーマンスは良いものの、アクティブな攻撃にさらされやすくなる可能性があります。この問題に対処するため、WPA には、一時的に WLAN クライアントが切断されたり、60 秒ごとに新しいキーのネゴシエーションを許可されないなどの攻撃を防御する対策が含まれます。しかし、この動作自体が一種の DoS 攻撃になる場合もあります。多くの WLAN 展開では、アンチウイルス機能を無効にすることができます。

AES の暗号化

図 4-6 では、基本的な AES カウンタ モード/CBC MAC Protocol（CCMP）のフロー チャートを示します。CCMP は、カウンタ モードが機密性を提供し、CBC MAC がメッセージの完全性を提供する AES 暗号化モードの 1 つです。

図 4-6　WPA2 AES CCMP



CCMP の手順では、追加の認証データ（AAD）は MAC ヘッダーから取り出され、CCM 暗号化プロセスに含まれます。これにより、フレームの暗号化されていない部分の変更からフレームを保護します。

リプレイ攻撃を防御するため、シーケンスト パケット番号（PN）は CCMP ヘッダーに含まれています。CCM 暗号化プロセスで順番に使用される nonce を生成するため、PN および MAC ヘッダーの一部が使用されます。

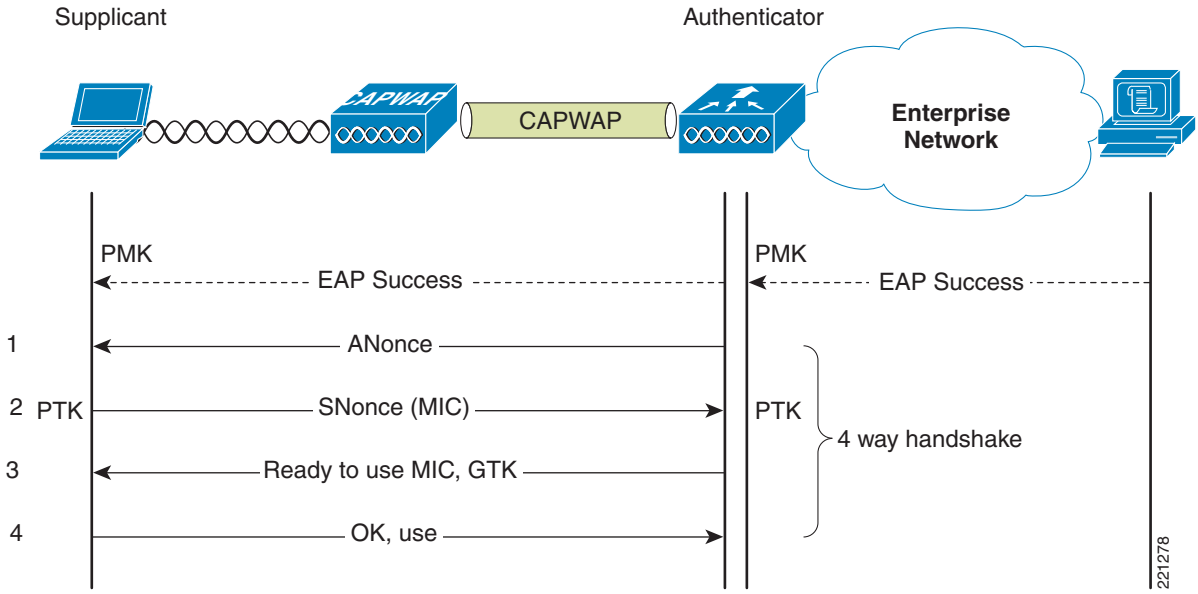
Four-Way ハンドシェイク

Four-Way ハンドシェイクは、無線データ フレームを暗号化するための暗号化キーを取得するために使用される方式です。図 4-7 では、暗号化キーを生成するために使用されるフレーム交換を図示します。これらのキーを一時キーと呼びます。

暗号化キーは、EAP 認証中に相互に取得される PMK から取得されます。この PMK は EAP 成功メッセージの中でオーセンティケータに送信されますが、サプリカントには転送されません。これは、サプリカントが PMK の自分のコピーを生成しているためです。

1. オーセンティケータは、オーセンティケータの nonce（ANonce）を含む EAPOL-Key フレームを送信します。ANonce はオーセンティケータによって生成される乱数です。
   a. サプリカントは、ANonce とサプリカントの nonce（SNonce）から PTK を取得します。SNonce は、クライアント/サプリカントによって生成される乱数です。
2. サプリカントは、SNonce、（再）アソシエーション要求フレームの RSN 情報要素および MIC を含む EAPOL-Key フレームを送信します。
   a. オーセンティケータは、ANonce および SNonce から PTK を取得し、EAPOL-Key フレーム内の MIC を検証します。
3. オーセンティケータは、ANonce、ビーコンまたはプローブ応答メッセージの RSN 情報要素、一時キーをインストールするかどうかを判断する MIC、カプセル化されたグループ一時キー（GTK）であるマルチキャスト暗号キーを含む EAPOL-Key フレームを送信します。
4. サプリカントは、一時キーがインストールされていることを確認するための EAPOL-Key フレームを送信します。

図 4-7　Four-Way ハンドシェイク

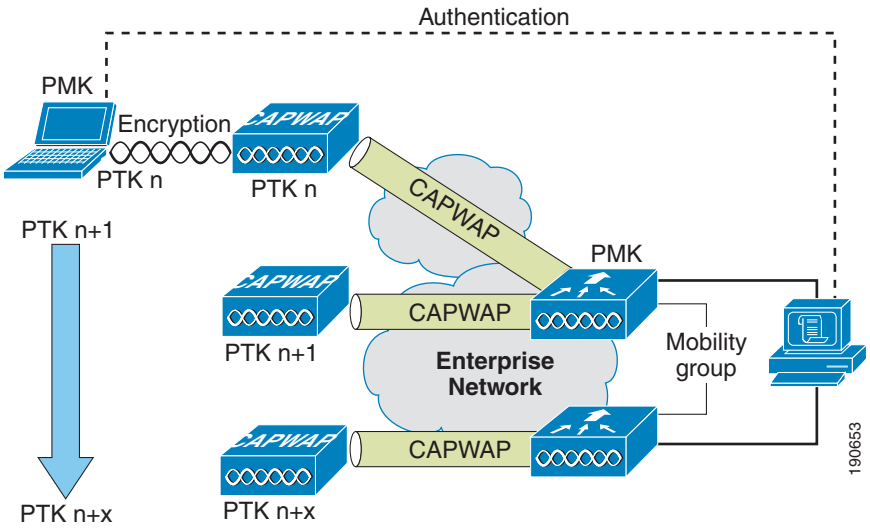


Proactive Key Caching と CCKM

Proactive Key Caching（PKC）は、AP クライアント 802.1x/EAP 認証中に生成される PMK に対して予防的なキャッシング（クライアント ローミング イベントの前）を許可する 802.11i 拡張機能です（図 4-8 を参照）。クライアントがローミングしようとしている AP で（所定の WLAN クライアントの）PMK があらかじめキャッシュされている場合、完全な 802.1x/EAP 認証は必要ではありません。代わりに、WLAN クライアントが WPA Four-Way ハンドシェイク プロセスを使用して、その AP との通信のための新しいセッション暗号化キーを安全に取得することができます。

これらのキャッシュされた PMK の AP への配信は、Cisco Unified Wireless Network の展開では大幅に簡略化されています。PMK は単純にコントローラにキャッシュされるため、接続するすべての AP で使用可能になります。PMK は、アンカー コントローラを含むモビリティ グループを構成する他のすべてのコントローラと共有されます。

図 4-8　Proactive Key Caching のアーキテクチャ



Cisco Centralized Key Management（CCKM）は、高速セキュア ローミング（FSR）を提供する Cisco Compatible Extensions クライアントでサポートされるシスコの標準です。ローミング処理を促進するための基本的なメカニズムは PKC と同じで、PMK キャッシュを使用します。ただし、CCKM の実装が少々異なるため、2 つのメカニズムの間に互換性はありません。

各 WLAN クライアントのキーのキャッシュの状態は、`show pmk-cache all` コマンドで確認できます。このコマンドにより、キーをキャッシュしているクライアントと、使用されているキー キャッシング メカニズムを識別します。802.11r ワーク グループは、802.11 向けの FSR メカニズムの標準化を担当します。

WLC は次の例に示すように、WLAN -802.1x+CCKM の CCKM と PKC の両方をサポートします。

```
WLAN Identifier.................................. 1
Network Name (SSID).............................. wpa2
…
Security
   802.11 Authentication:........................ Open System
   Static WEP Keys.............................. Disabled
   802.1X....................................... Disabled
   Wi-Fi Protected Access (WPA/WPA2)............. Enabled
      WPA (SSN IE)............................... Disabled
      WPA2 (RSN IE).............................. Enabled
         TKIP Cipher............................. Disabled
         AES Cipher.............................. Enabled
   Auth Key Management
         802.1x.................................. Enabled
         PSK..................................... Disabled
         CCKM.................................... Enabled
…
(Cisco Controller) >show pmk-cache all
PMK-CCKM Cache
                              Entry
Type        Station           Lifetime   VLAN Override        IP Override
------    --------------      --------   ------------------   ---------------
CCKM    00:12:f0:7c:a3:47     43150                             0.0.0.0
RSN     00:13:ce:89:da:8f     42000                            0.0.0.0
```

Cisco Unified Wireless Network アーキテクチャ

図 4-9 では、CAPWAP AP やメッシュ CAPWAP、管理システム（WCS/NCS/PI）、およびワイヤレス LAN コントローラ（WLC）を含む Cisco Unified Wireless Network アーキテクチャの高レベルのトポロジを示します。

Cisco Access Control Server（ACS）*または* Identity Services Engine（ISE）および AAA 機能は、ソリューションを実現するため、無線ユーザの認証および許可をサポートする RADIUS サービスを提供します。

図 4-9　Cisco Unified Wireless Network アーキテクチャ

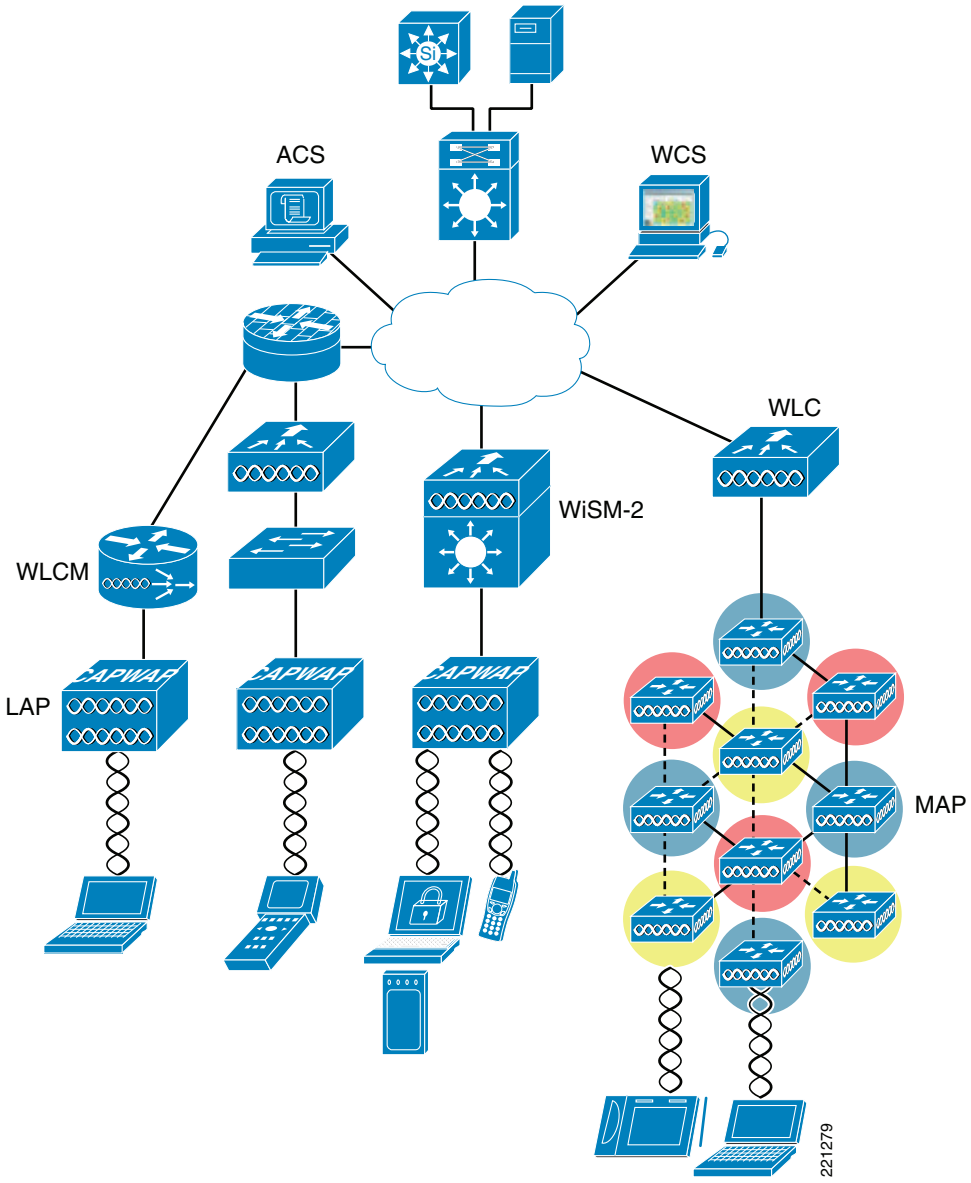
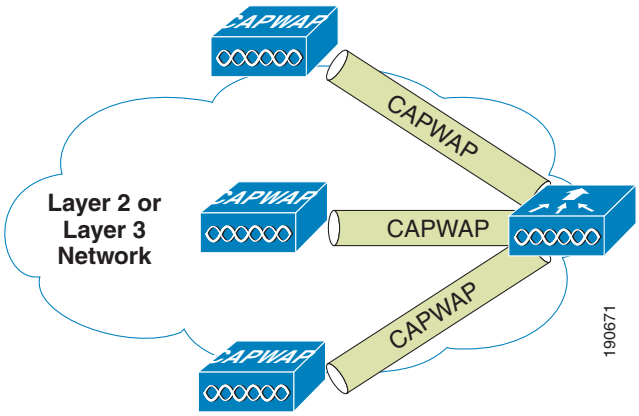


図 4-10 では、アーキテクチャの主要機能の 1 つである、AP がどのように CAPWAP プロトコルを使用して WLC へのトンネル トラフィックと通信するのかについて説明します。

図 4-10　CAPWAP AP と WLC の接続



CAPWAP には次の 3 つの基本機能があります。

- AP の制御と管理
- WLC からの WLAN クライアント トラフィックのトンネリング
- Cisco Unified Wireless Network の管理に関する 802.11 データの収集

CAPWAP の機能

Control and Provisioning of Wireless Access Points（CAPWAP）は、Lightweight Access Point Protocol（LWAPP）に対する更新です。CAPWAP は多くの AP の管理を WLC でできるようにする、標準かつ相互運用可能なプロトコルです。CAPWAP の機能は次のとおりです。

- シスコの LWAPP 製品から、CAPWAP を使用する次世代のシスコ製品へのアップグレード パス
- RFID リーダーおよび類似のデバイスを管理する機能
- サードパーティのアクセス ポイントと相互運用するコントローラ

LWAPP 対応の AP では、CAPWAP コントローラの discover と join が可能で、CAPWAP コントローラへの移行はシームレスに行われます。たとえば、WLC ディスカバリ処理とファームウェアのダウンロード処理は、CAPWAP および LWAPP で同じです。

覚えておく必要のある重要なポイント

- LWAPP を使用する AP からのトラフィックのみを許容するようにファイアウォールが設定されている場合、CAPWAP を使用する AP からのトラフィックを許容するようにファイアウォールのルールを変更する必要があります。
- CAPWAP UDP ポート 5246 と 5247（LWAPP UDP ポート 12222 と 12223 のように）がイネーブルになっていて、AP のコントローラへの join を妨げる可能性のある中継デバイスによりブロックされていないことを確認してください。
- コントローラと AP 間のコントロール パスにアクセス コントロール リスト（ACL）がある場合、新しいプロトコル ポートをオープンして、アクセス ポイントが阻止されるのを防ぐ必要があります。

AP は、コントローラの宛先ポートに到達するために任意の UDP 送信元ポートを使用します。新しく開封したばかりの AP がある場合、コントローラから CAPWAP イメージをダウンロードする前に LWAPP を使用してコントローラに接続しようとすることがあります。AP は、コントローラから CAPWAP イメージをダウンロードしたら、CAPWAP のみを使用して、コントローラとやり取りします。

（注）　CAPWAP を使用してコントローラへの join を 60 秒間試行した後、AP は LWAPP の使用にフォールバックします。AP は、LWAPP を使用してコントローラを 60 秒以内に検出できないと、CAPWAP を使用してコントローラへの join を再度試行します。AP は、コントローラに join できるまで、CAPWAP と LWAPP を 60 秒ごとに切り替えるこのサイクルを繰り返します。

Cisco Unified Wireless Network のセキュリティ機能

ネイティブの 802.11 セキュリティ機能が、物理的なセキュリティや CAPWAP アーキテクチャの展開の容易さと組み合わさることで、WLAN の導入全体のセキュリティの向上に役立ちます。CAPWAP プロトコルに固有のセキュリティ上の利点に加えて、Cisco Unified Wireless Network ソリューションには次のようなセキュリティ機能もあります。

- 強化された WLAN セキュリティ オプション
- ACL およびファイアウォール機能
- Dynamic Host Configuration Protocol（DHCP）および Address Resolution Protocol（ARP）の保護
- ピアツーピア ブロック
- ワイヤレス侵入防御システム（wIPS）
  - クライアント除外
  - 不正 AP 検出
- 管理フレーム保護
- 動的 RF 管理
- アーキテクチャの統合
- IDS 統合

強化された WLAN セキュリティ オプション

Cisco Unified Wireless Network ソリューションでは、複数の WLAN セキュリティ オプションを同時にサポートします。たとえば、1 つの WLC 上に複数の WLAN を作成し、それぞれの WLAN に、オープンなゲスト WLAN ネットワークやレガシー プラットフォーム用の WEP のネットワークから WPA や WPA2 セキュリティ設定の組み合わせまで対応可能な独自の WLAN セキュリティを設定することができます。

それぞれの WLAN SSID は、WLC 上の同じ、または異なる dot1q インターフェイスにマッピングすることも、モビリティ アンカー（オート アンカー モビリティ）接続を介して別のコントローラにトンネリングされた IP（EoIP）上のイーサネットにマッピングすることもできます。

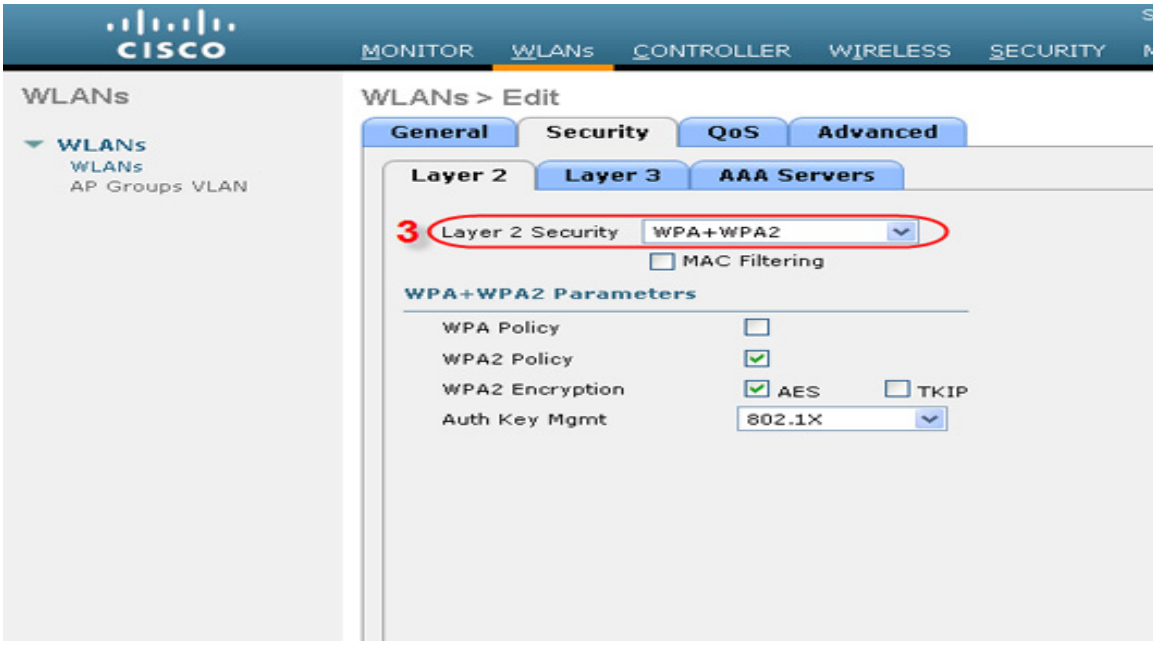
WLAN クライアントが 802.1X を介して認証する場合、dot1q VLAN の割り当ては、認証成功時に WLC に渡される RADIUS 属性を使用して制御されます。

図 4-11 および図 4-12 では、Unified Wireless Network WLAN 設定画面のサブセットを示します。これらの設定画面に表示される主な設定項目は次の 3 つです。

- WLAN SSID
- WLAN がマッピングされている WLC インターフェイス
- セキュリティ方式（図 4-12）

図 4-11　WLAN の [General] タブ

図 4-12　WLAN の [Layer 2 Security] タブ



ローカル EAP 認証

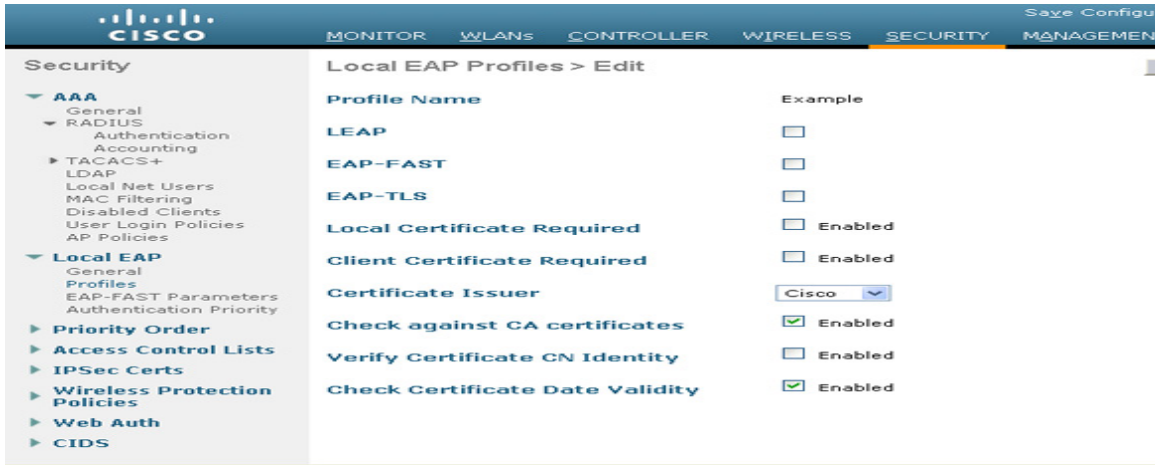
WLC ソフトウェアは、外部 RADIUS サーバが使用可能でない場合や使用不可になった場合に使用できる、ローカル EAP 認証機能を提供します。ローカル認証への切替えが設定されるまでの遅延は、図 4-13 で示したとおりに設定します。RADIUS サーバの可用性が復旧されると、WLC は自動的にローカル認証から RADIUS サーバ認証へ再び切り替えます。

図 4-13　ローカル認証のタイムアウト

WLC 上でローカルでサポートされる EAP の種類は、LEAP、EAP-FAST、EAP-TLS および PEAP です。

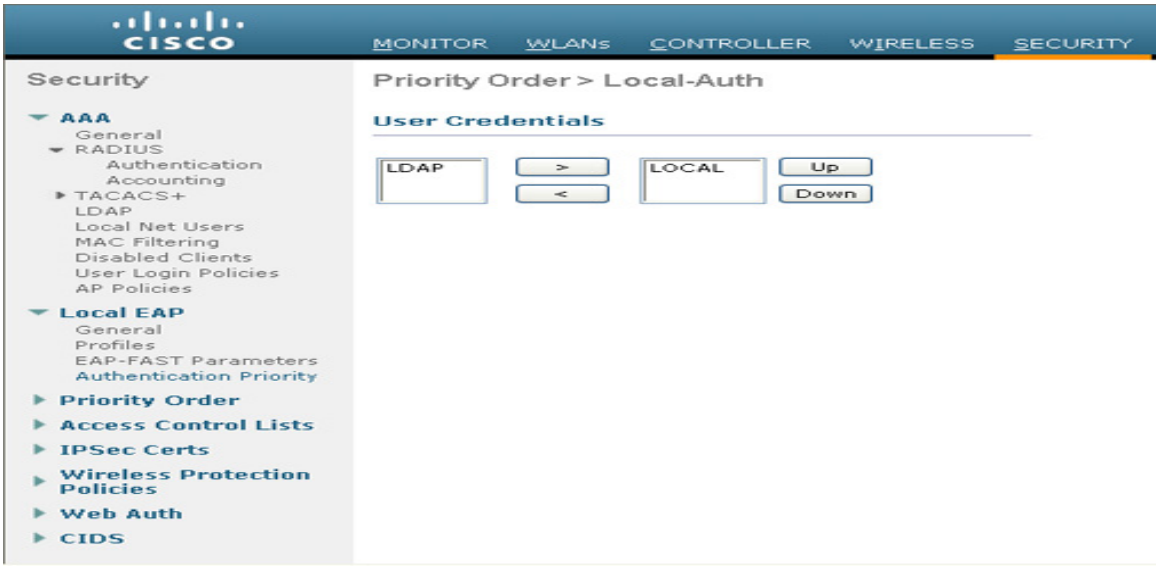
図 4-14 では、ローカル EAP のプロファイルを選択するウィンドウを示します。

図 4-14　ローカル EAP のプロファイル



WLC ではローカル データベースを使用してデータ認証を行うことができます。また、LDAP ディレクトリにアクセスして EAP-FAST または EAP-TLS 認証に関するデータを提供することもできます。ユーザ クレデンシャル データベースのプライオリティ（LDAP かローカルか）は、図 4-15 で示すとおりに設定可能です。

図 4-15　ローカル EAP のプライオリティ



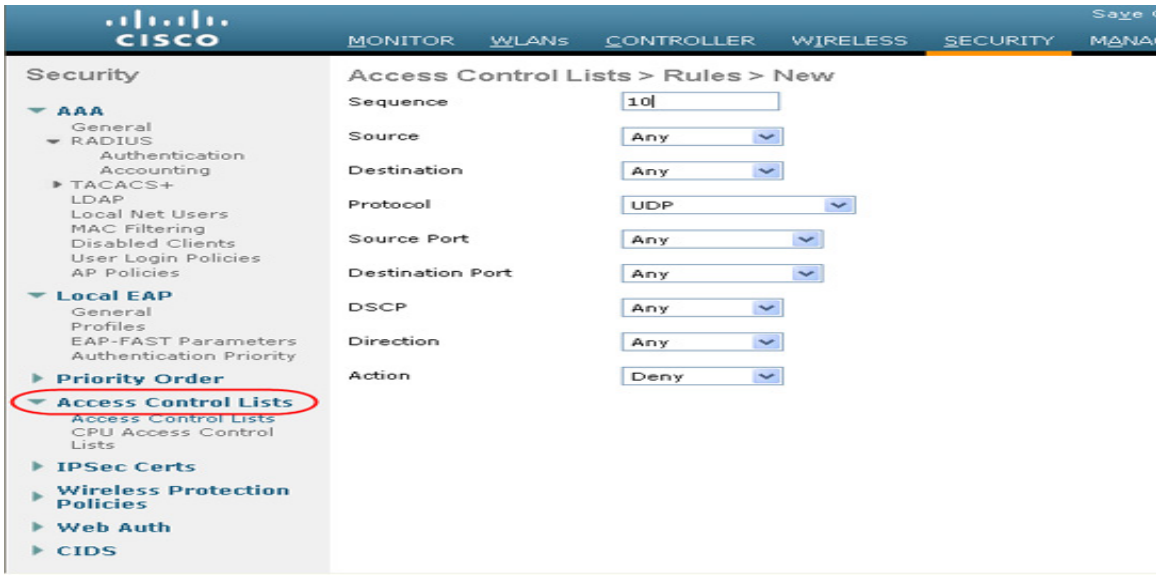
ACL およびファイアウォール機能

WLC では、WLC 上で設定されている任意のインターフェイス用にアクセス コントロール リスト（ACL）を定義できます。また、WLC 自体の CPU 用に ACL を定義することもできます。これらの ACL を使用することで、特定の WLAN にポリシーを適用し、特定のアドレスやプロトコルへのアクセスを制限したり、WLC 自体に追加保護を行ったりすることができます。

インターフェイス ACL は、ACL が適用されているインターフェイスに出入りする WLAN クライアント トラフィックに作用します。CPU ACL は WLC インターフェイスに依存しないため、WLC システムに送受信されるすべてのトラフィックに適用されます。

図 4-16 では、[ACL Configuration] ページを示します。ACL では、発信元アドレスと送信先アドレスの範囲、プロトコル、送信元ポートと宛先ポート、DSCP、および ACL が適用される方向を指定できます。ACL は、さまざまな規則の順序で作成できます。

図 4-16　[ACL Configuration] ページ



DHCP および ARP 保護

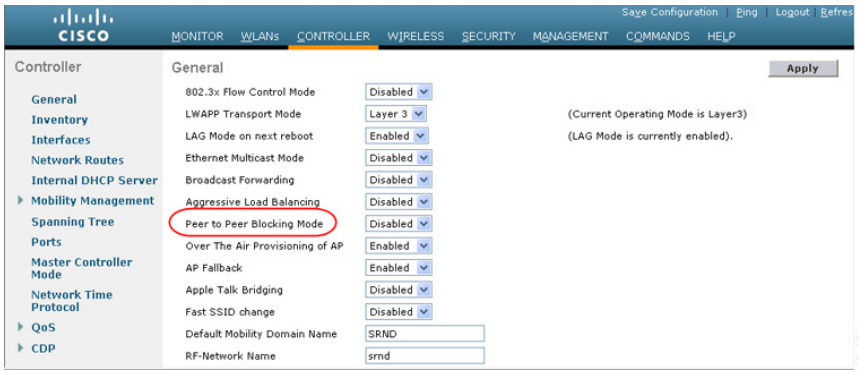
WLC は、WLAN クライアントの DHCP 要求のリレー エージェントとして動作します。その際、WLC は DHCP インフラストラクチャを保護するために、いくつかのチェックを実行します。最も重要なチェックは、DHCP 要求に含まれている MAC アドレスが、要求を送信する WLAN クライアントの MAC アドレスに一致することを確認することです。これにより、WLC 自体のインターフェイスに対する 1 つの DHCP 要求（IP アドレス）に WLAN クライアントを制限し、それによって DHCP 枯渇攻撃を防御します。WLC は、デフォルトでは WLAN クライアントからのブロードキャスト メッセージを WLAN に再転送しないため、WLAN が DHCP サーバとして動作したり、誤った DHCP 情報をスプーフィングしたりすることが防止されます。

WLC は MAC アドレスと IP アドレスの関係を維持することで、WLAN クライアントの ARP プロキシとして機能します。これにより、重複した IP アドレスおよび ARP スプーフィング攻撃を WLC がブロックできるようになります。WLC は、WLAN クライアント間の直接的な ARP 通信を許可しません。これにより、WLAN クライアント デバイス宛ての ARP スプーフィング攻撃も防止できます。

ピアツーピア ブロック

WLC は、同じ WLAN のクライアント同士の通信をブロックするように設定できます。ルータを介して通信するように強制することで、同じサブネットのクライアント同士で見込まれる攻撃を防止します。図 4-17 は、WLC 上でのピアツーピア ブロックの設定画面です。これは WLC のグローバル設定であり、WLC に設定されているすべての WLAN に適用されることに注意してください。

図 4-17　ピアツーピア ブロック



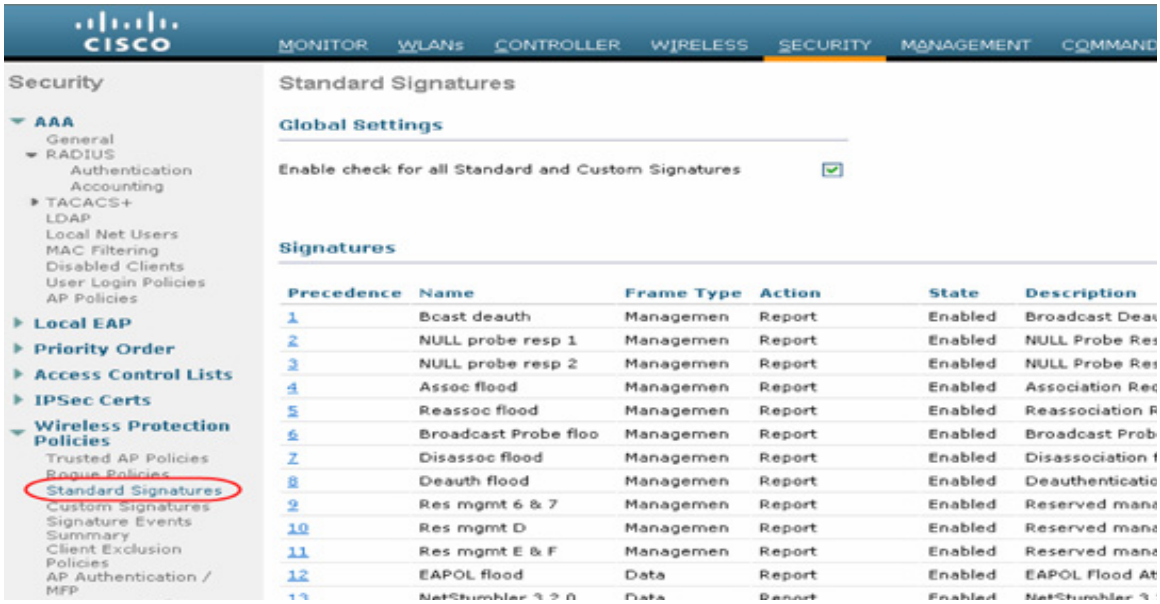
無線 IDS

WLC は、接続された AP すべてから取得した情報を使用して WLAN の IDS 分析を行い、WLC のほか WCS に対して検出された攻撃も報告します。無線 IDS 分析は、有線ネットワーク IDS システムで実行できる分析を補完するものです。WLC の組み込み無線 IDS 機能では、有線ネットワーク IDS システムから見ることのできない、または使用できない 802.11 および WLC 固有の情報を分析します。

WLC によって使用される無線 IDS シグニチャ ファイルは WLC ソフトウェア リリースに含まれています。ただし、別のシグニチャ ファイルを使用して個別に更新することが可能です。カスタム シグニチャは、[Custom Signatures] ウィンドウに表示されます。

図 4-18 は、WLC の [Standard Signatures] ウィンドウです。

図 4-18　標準の WLAN IDS シグニチャ



Cisco Adaptive Wireless Intrusion Prevention System

ELM 機能を備えた Cisco Adaptive Wireless Intrusion Prevention System（wIPS）を使用すれば、モニタリング専用モードまたはオーバーレイ ネットワークを必要とすることなく、展開された AP に総合的なセキュリティ保護を提供できます（図 4-19 を参照）。AP は、セキュリティへの不正なアクセスや侵入、攻撃を防御する必要があります。ネットワーク AP で ELM 機能がイネーブルになっているシスコの wIPS を使用すれば、効果的かつ簡単に無線セキュリティを実装できます。

図 4-19　拡張ローカル モード（ELM）での AP の展開

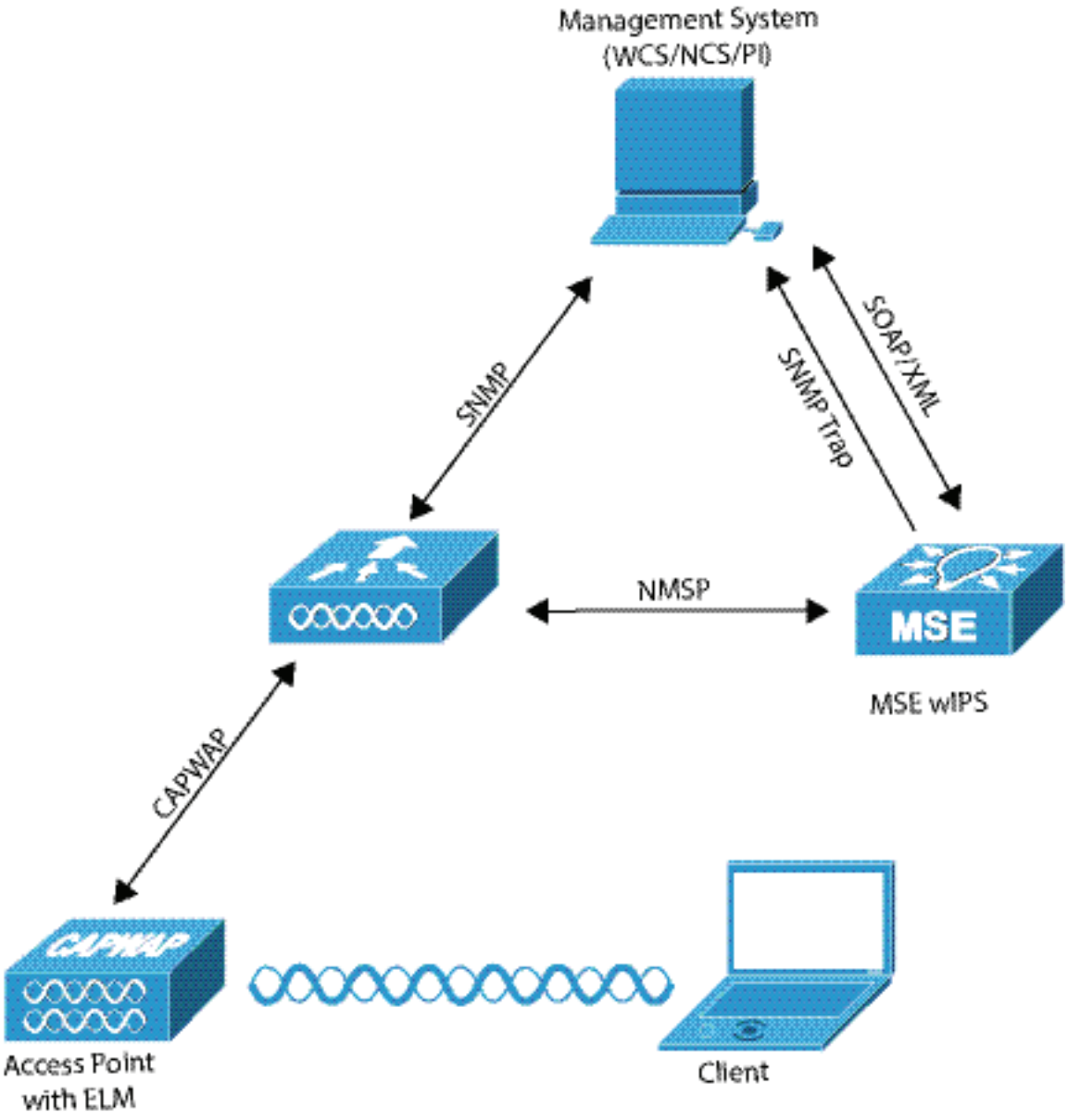


図 4-19 の wIPS 通信プロトコルは次のとおりです。

- CAPWAP：これは、Lightweight Access Point Protocol（LWAPP）の後継プロトコルであり、ELM AP と WLC の間の通信に使用されます。WLC と wIPS との間でアラーム情報が送受信され、他の Cisco Prime Infrastructure 管理システムの構成情報が AP にプッシュされる双方向トンネルを提供します。

（注）　Cisco Prime Infrastructure 管理システムは、以前は Wireless Control System（WCS）と呼ばれていましたが、その後 Network Control System（NCS）に進化しました。わかりやすくするため、これら 3 つすべてを *管理システム（WCS/NCS/PI）* と呼びます。

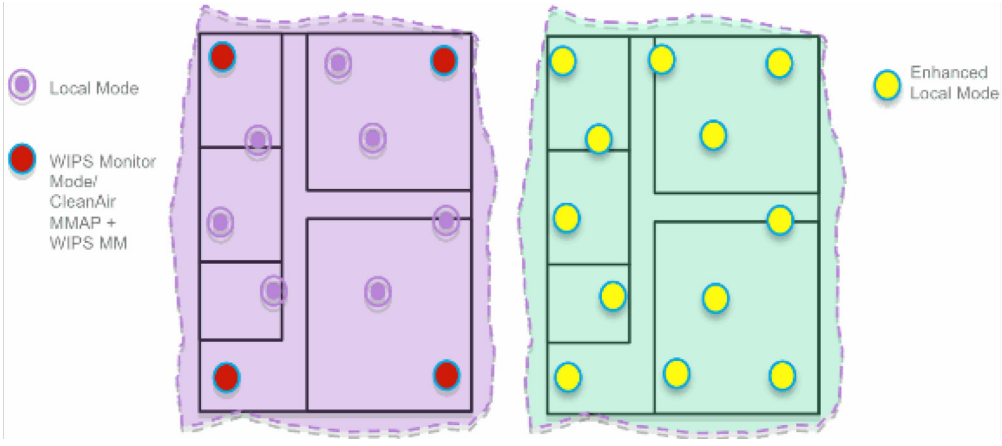
- Network Mobility Services Protocol（NMSP）：この暗号化されたプロトコルは、WLC と管理システム（WCS/NCS/PI）間で通信を行います。wIPS の展開において、このプロトコルは、WLC から wIPS（およびその他の動作しているサービス）へ集約するアラーム情報および、wIPS の設定情報をコントローラにプッシュする経路を提供します。
- SOAP/XML（Simple Object Access Protocol）：管理システム（WCS/NCS/PI）への通信方式。このプロトコルは、モビリティ サービス エンジン（MSE）で稼働する wIPS やその他のサービスに設定パラメータを配布するために使用します。
- SNMP（簡易ネットワーク管理プロトコル）：MSE から管理システム（WCS/NCS/PI）へ wIPS のアラーム情報を転送するために使用されます。また、WLC から管理システム（WCS/NCS/PI）に不正 AP の情報を伝えるためにも使用されます。

モニタ専用モードと ELM

図 4-20 では、wIPS モニタ モードの標準的な展開と ELM 機能を持つ AP の比較を示します。両方のモードの一般的な対象範囲は次のようになっています。

- wIPS のモニタ専用モードの AP（図 4-20 では赤色で表示）は、一般的に 15,000 ～ 35,000 平方フィートを対象範囲とします。
- ELM 機能を持つ AP（図 4-20 では黄色で表示）は、一般的に 3,000 ～ 5,000 平方フィートを対象範囲とします。

図 4-20　　モニタ モードと ELM の比較



従来の Adaptive wIPS 展開の場合、5 つそれぞれのローカル モード AP に対して 1 つのモニタ モード AP という比率を推奨します。これは、最適なカバレッジ範囲を実現するネットワーク設計や専門知識により異なる場合があります。ELM により、既存のすべての AP で ELM ソフトウェア機能を有効にするだけで、パフォーマンスを維持しつつ、モニタ モード wIPS 操作をローカル データ サービス モード AP に効果的に追加できます。

On-Channel および Off-Channel のパフォーマンス

AP がチャネルにアクセスしたときに、攻撃を検出および分類するためそのチャネルに*留まる*時間を、*一時停止*時間といいます。ELM の主機能は、データ、音声およびビデオ クライアント、サービスのパフォーマンスに影響を与えることなく、On-Channel 攻撃で効果的に機能します。これに対し、ローカル モードでは、攻撃を検出および分類するための最低限の滞留時間を提供する Off-Channel スキャンは場合によって変化します。

たとえば、音声クライアントが AP に関連づけられている場合、無線リソース管理（RRM）により、サービスが影響を受けないことを保証するため、音声クライアントがアソシエート解除されるまでスキャンが延期されます。この例では、オフチャネル中の ELM による検出はベスト エフォート型と見なされます。すべてのチャネル、カントリー チャネルまたは DCA チャネルで近隣の ELM AP が動作することで効果が増します。したがって、カバレッジの保護を最大にするためにすべてのローカル モードの AP で ELM を有効にすることが推奨されます。すべてのチャネルでのフルタイムの専用スキャニングが必要な場合、シスコではモニタ モードの AP を展開することを推奨します。

通常、ローカル モードとモニタ モードの AP の相違点は以下のとおりです。

- ローカル モード AP：WLAN クライアントにタイム スライシング Off-Channel スキャニングを提供し、各チャネルで 50 ミリ秒間リスニングして、設定によりすべてのチャネル、カントリー チャネルまたは DCA チャネルのスキャニングを実行します。
- モニタ モード AP：WLAN クライアントにサービスを提供せず、スキャニングだけを行い、各チャネルで 1.2 秒間リスニングして、すべてのチャネルをスキャンします。

WAN リンクをまたぐ ELM

シスコは、低帯域幅 WAN リンクでの ELM AP の展開など、困難なトポロジにおける機能の最適化に努めてきました。ELM 機能は、AP での攻撃シグニチャの判別のための事前処理を行い、低速リンクで機能するように最適化されています。シスコでは、ベスト プラクティスとして、WAN 経由の ELM のパフォーマンスを検証する基準をテストおよび測定することを推奨します。

CleanAir 統合

Cisco CleanAir テクノロジーは、ワイヤレス干渉の影響を緩和して 802.11n ネットワークに対しパフォーマンスの保護を提供する、セルフ ヒーリングと自己最適化が可能なスペクトラム対応の無線ネットワークです。

ELM 機能は、CleanAir 操作を補完し、同様のパフォーマンスを実現して、次の既存の CleanAir スペクトラム対応のメリットをモニタ モード AP の展開に提供します。

- 専用シリコン レベル RF インテリジェンス
- スペクトラム対応、セルフ ヒーリングおよび自己最適化
- 非標準のチャネル脅威および干渉の検出および緩和
- Bluetooth、マイクロ波、コードレス電話などの非 Wi-Fi 検出
- RF ジャマーなどの RF 層 DOS 攻撃の検出および特定

ELM wIPS アラーム フロー

攻撃は、*信頼できる* AP で発生した場合にのみ該当します。図 4-21 で示すとおり、ELM AP は攻撃を検出した後、管理システム（WCS/NCS/PI）に攻撃を通知し、関連付けて、報告します。アラーム フローの一般的なプロセスは次のとおりです。

1. 攻撃が、*信頼できる* AP に対して発生する
2. ELM 機能を持つ AP の検出が CAPWAP を介して WLC に通知される
3. NMSP を介して MSE に透過的に渡される
4. MSE 上の wIPS データベースにログインし、SNMP トラップを介して、管理システム（WCS/NCS/PI）に送信する
5. 管理システム（WCS/NCS/PI）に表示される

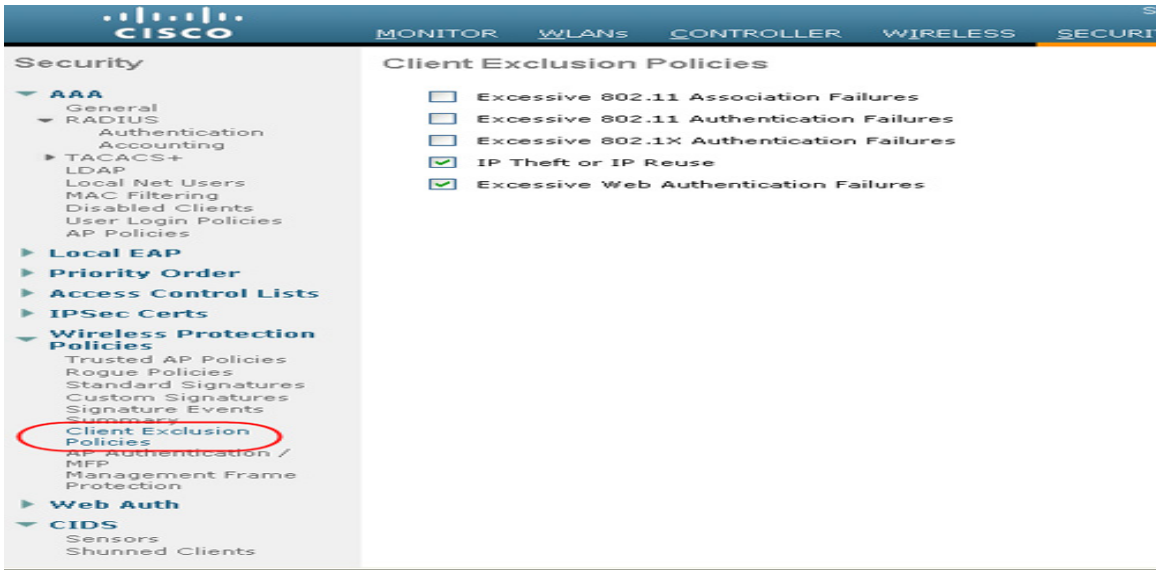
図 4-21　　脅威検出のアラーム フロー

クライアント除外

無線 IDS 以外に、WLC では追加の手順で WLAN インフラストラクチャと WLAN クライアントを保護することができます。WLC は、動作が脅威または不適切と見なされる WLAN クライアントを除外するポリシーを実行できます。図 4-22 では、現在サポートされている次のクライアント除外ポリシーを含む [Exclusion Policies] ウィンドウを示します。

- Excessive 802.11 association failures：可能性のある不正なクライアントまたは DoS 攻撃
- Excessive 802.11 authentication failures：可能性のある不正なクライアントまたは DoS 攻撃
- Excessive 802.1X authentication failures：可能性のある不正なクライアントまたは DoS 攻撃
- IP theft or IP reuse：可能性のある不正なクライアントまたは DoS 攻撃
- Excessive web authentication failures：可能性のある DoS またはパスワード クラッキング攻撃

図 4-22　クライアント除外ポリシー

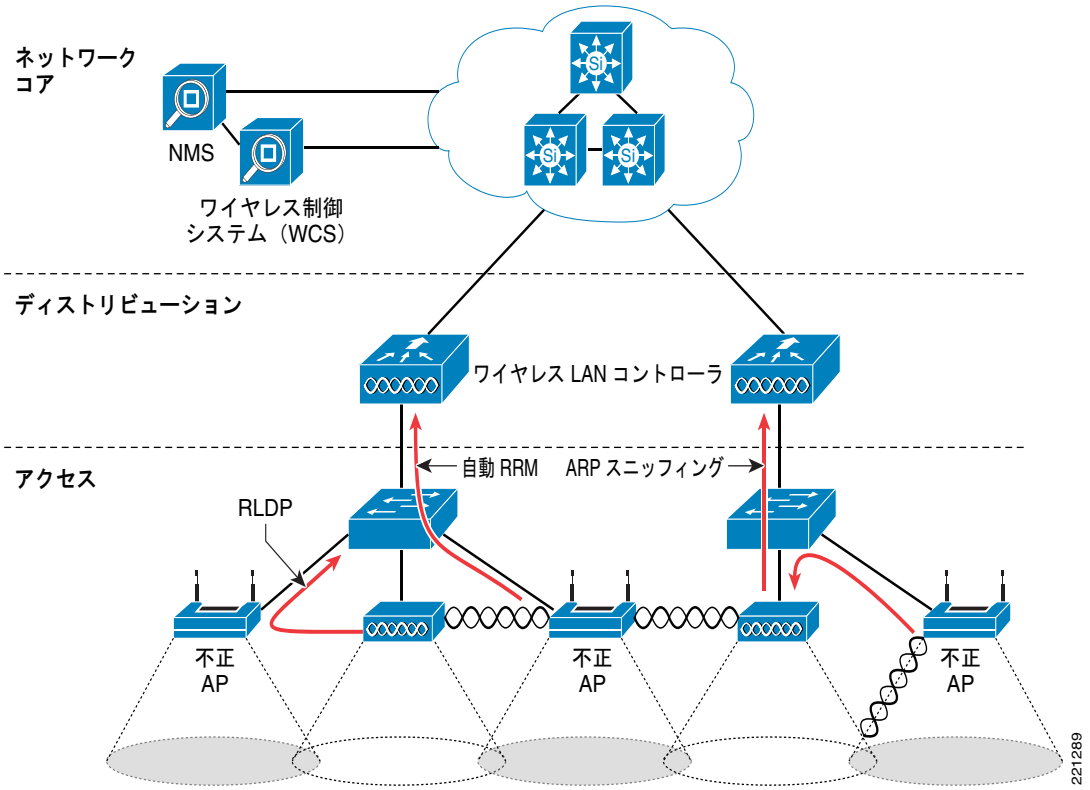


不正 AP

図 4-23 で示したとおり、Cisco Unified Wireless Network ソリューションは不正 AP に完全なソリューションを提供します。このソリューションが提供する機能は次のとおりです。

- Air/RF の検出：ビーコンと 802.11 プローブの応答を検出またはスニッフィングすることによる不正なデバイスを検出すること。
- 不正 AP の検索：検出された RF 特性および管理された RF ネットワークの既知の特性を使用して、不正なデバイスを見つけること。
- 有線の検出：有線ネットワークに不正デバイスを関連付けたり追跡したりするためのメカニズム。
- 不正 AP の分離：不正 AP へのクライアント接続を防ぐメカニズム。

図 4-23　Unified Wireless Network での不正 AP 検出



Air/RF 検出

2 台の AP の RF 検出の導入モデルは次のとおりです。

- 標準の AP 導入
- モニタ モードの AP 導入

これらの導入モデルはいずれも RF の検出をサポートするため、不正 AP に限定されませんが、アドホック クライアントや不正なクライアント（不正 AP のユーザ）の検出が検出されたときにも情報を把握できます。モニタ モード用に設定された AP は RF チャネルのスキャン専用であり、クライアント アソシエーションやデータ伝送はサポートしていません。

不正 AP を検索すると、AP は 50 ミリ秒間オフチャネルになって、不正なクライアントをリッスンし、ノイズやチャネルの干渉を監視します。スキャンされたチャネルは 802.11a および 802.11b/g のグローバル WLAN ネットワーク パラメータで設定されます。

検出された不正と思われるクライアントやアクセス ポイントは、次の情報を収集するためコントローラに送信されます。

- 不正 AP の MAC アドレス
- 不正 AP 名
- 不正に接続されたクライアントの MAC アドレス
- WPA、WEP または WEP2 でフレームが保護されているかどうか
- プリアンブル
- 信号対雑音比（SNR）

- 受信信号強度表示（RSSI）
- スイッチポート トレース

WLC が信頼済み AP から別のレポートを受け取るか、2 回目の検出サイクルが完了するまで、不正と思われるクライアントやアクセス ポイントは不正に分類されません。信頼済み AP は不正と思われるクライアントや AP のチャネルに移動して、不正なクライアントや AP、ノイズ、干渉を監視します。同じクライアントや AP がもう一度検出されると、WLC 上で*不正*として分類されます。

いったん不正デバイスとして分類されると、WLC はこの不正 AP がローカルネットワークに接続されているか、または単に近接 AP であるかを確認します。いずれの場合でも、管理対象の Cisco Unified Wireless Network 外部の AP は不正として見なされます。

モニタ モードでは、信頼済み AP はユーザ トラフィックを伝送しないため、チャネルのスキャン専用です。顧客が特定のサービス エリアの WLAN をサポートしたくないが、そのエリアで 不正 AP および不正なクライアントを監視したい場合に、最も一般的に使用されるのがモニタ モードです。

ロケーション

Cisco Prime Infrastructure のロケーション機能を使用して、不正 AP のおおよその場所を示す間取り図を提示することができます。間取り図にはすべての正規の AP の場所が表示され、不正 AP の場所がドクロのアイコンで強調表示されます。Cisco Unified Wireless Network のロケーション機能の詳細については、次の Web ページを参照してください。
http://www.cisco.com/en/US/products/ps6386/index.html

有線の検出

AP の数が少ない支社や、間取り図情報が利用可能でないなど、不正な AP の場所を示す Cisco Prime Infrastructure の機能が有効でない場合があります。このような場合、Cisco Unified Wireless Network ソリューションでは 2 種類の有線ベースの検出オプションを使用できます。

- Rogue Detector AP
- Rogue Location Discovery Protocol（RLDP）

AP が Rogue Detector として設定されている場合、その AP の無線はオフになり、AP の役割は有線ネットワークをリッスンして不正 AP に関連付けられたクライアント、すなわち*不正なクライアント*の MAC アドレスを検出することになります。Rogue Detector は、不正なクライアントの MAC アドレスを含む ARP パケットをリッスンします。そのような ARP が検出されると、AP はその旨を WLC に報告し、Cisco Unified Wireless Network と同じネットワークに 不正 AP が接続されているかどうかを検証します。

ARP 情報をとらえる可能性を最大まで上げるため、Rogue AP Detector は Switched Port Analyzer（SPAN）ポートを使用しているすべての使用可能なブロードキャスト ドメインに接続されます。一般的なネットワークに存在するさまざまな集約ブロードキャスト ドメインを把握するため、複数の Rogue AP Detector を展開することができます。

不正なクライアントが無線ルータ（共通のホーム WLAN デバイス）の背後にある場合、ARP 要求は有線ネットワークに認識されないため、不正な AP 検知器に代わる手段が必要となります。また、監視すべきブロードキャスト ドメインが大量にあるような一部の展開（メイン キャンパス ネットワークなど）については、Rogue Detector AP が実用的でない場合もあります。

このような状況では RLDP オプションが役立ちます。この場合、不正 AP が検出されると、標準の AP はその不正 AP にクライアントとしてアソシエートし、コントローラにテストパケットを送信しようとします。このとき、AP は標準 AP としての動作を停止して、一時的にクライアントモードに移行する必要があります。この動作によって、不正 AP がネットワーク上に実際に存在していることが確認され、当該の不正 AP のネットワーク上での論理的な場所を示す IP アドレス情報が提示されます。支社

内のロケーション情報を取得する難しさと、マルチテナントの建物内で不正 AP が検出される可能性を組み合わせて考えると、Rogue AP Detector と RLDP はロケーション ベースの不正 AP 検出を強化する便利なツールです。

スイッチ ポート トレース

Cisco Prime Infrastructure では、コントローラから情報を取得することによって、不正アクセス ポイントを検出できます。不正アクセス ポイント表には、*ネイバー リスト*にないフレームから検出された BSSID アドレスが記載されています。ネイバー リストには、確認済み AP または*ネイバー*の既知の BSSID アドレスが含まれます。指定された期間の終わりに、不正アクセス ポイント表の内容が、CAPWAP Rogue AP Report メッセージでコントローラに送信されます。この方法では、Cisco Prime Infrastructure はコントローラから受け取った情報を単純に収集します。さらに、有線の不正アクセス ポイントのスイッチ ポートの自動または手動スイッチ ポート トレース（SPT）も組み込むことができます。自動 SPT は、大規模なワイヤレス ネットワークに適しています。

不正 AP が Cisco Prime Infrastructure に報告されると、自動 SPT が自動的に起動します。自動 SPT は、不正 AP の有線のロケーションの関連付けを基礎とする、より高速なスキャン方法です。トレースを実行し、回線上で検出された不正アクセス ポイントを封じ込められるようにするために、Cisco Prime Infrastructure を使用して、自動 SPT および自動封じ込めの基準を設定できます。

不正 AP を自動的に封じ込める必要があることを複数のコントローラが報告した場合、Cisco Prime Infrastructure は最も強い RSSI を報告したコントローラを検出し、そのコントローラに封じ込め要求を送信します。

不正 AP の封じ込め

不正 AP に接続されたクライアント、または不正なアドホックに接続されたクライアントは、近隣の AP から 802.11 認証解除パケットを送信することによって封じ込めることができます。近隣の WLAN 内にある正規の AP にこの作業を行うことは違法であるため、当該の AP が本当に不正 AP であることを確認する手順を行ってから作業する必要があります。シスコがソリューションから不正 AP の自動封じ込め機能を削除したのは、これが理由です。

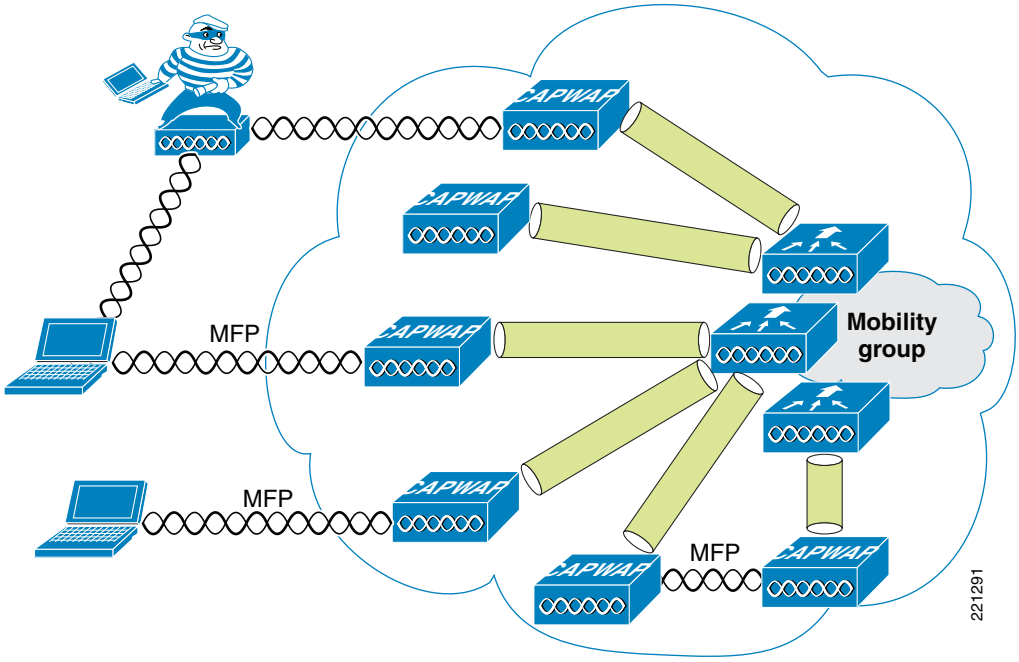
企業の WLAN にも不正 AP クライアントが存在するかどうかを判断するには、クライアントの MAC アドレスと、802.1X 認証中に AAA によって収集された MAC アドレスを比較します。これにより、改ざんされた可能性のある WLAN クライアントやセキュリティ ポリシーに従っていないユーザの識別が可能になります。

管理フレーム保護

802.11 の課題の 1 つは、暗号化や Message integrity check のない平文で管理フレームが送信され、そのためにスプーフィング攻撃に対して脆弱であるということです。WLAN 管理フレームのスプーフィングが WLAN ネットワークの攻撃に使用される可能性があります。この問題に対処するため、シスコでは 802.11 管理フレームに Message Integrity Check（MIC）を挿入するためのデジタル署名メカニズムを作成しました。これにより、WLAN の展開の正規のメンバを識別できるほか、不正なインフラストラクチャ デバイスや、有効な MIC の不足によりスプーフィングされたフレームを識別できます。

Management Frame Protection（MFP）で使用される MIC はメッセージの簡単な CRC ハッシュですが、デジタル署名のコンポーネントも含みます。MFP の MIC コンポーネントによってフレームが改竄されていないことが確認され、デジタル署名コンポーネントによって MIC が WLAN ドメインの正規メンバーによって生成されたことが確認されます。MFP で使用されるデジタル署名キーはモビリティ グループのすべてのコントローラ間で共有されます。したがって、異なるモビリティ グループのキーがそれぞれ異なるため、すべての WLAN 管理フレームはそのモビリティ グループ内の WLC によって検証できます（図 4-24）。

図 4-24　管理フレーム保護



現在はインフラストラクチャ側とクライアント MFP の両方が可能ですが、クライアント MFP の場合は、Cisco Compatible Extension v5 クライアントが、無効なフレームを検出および拒否する前にモビリティ グループの MFP キーを *学習*する必要があります。

MFP は、次のような利点を提供します。

- WLAN ネットワーク インフラストラクチャによって生成された 802.11 管理フレームを認証する
- 不正 AP や中間者攻撃の一部として検出されないように有効な AP MAC または SSID をスプーフィングする悪意のある不正の検出を可能にする
- ソリューションの不正 AP と WLAN IDS シグニチャ検出の効率を上げる
- Cisco Compatible Extensions v5 を使用するクライアント デバイスの保護を提供する
- バージョン 12.3(8)/v2.13 のスタンドアロン AP/WDS/WLSE でサポートされる

MFP を有効にするには 2 つの手順が必要です。まず WLC の [Security] タブで MFP を有効にし（図 4-25）、モビリティ グループ内の WLAN で MFP をイネーブルにします（図 4-26）。

図 4-25　コントローラの MFP のイネーブル化

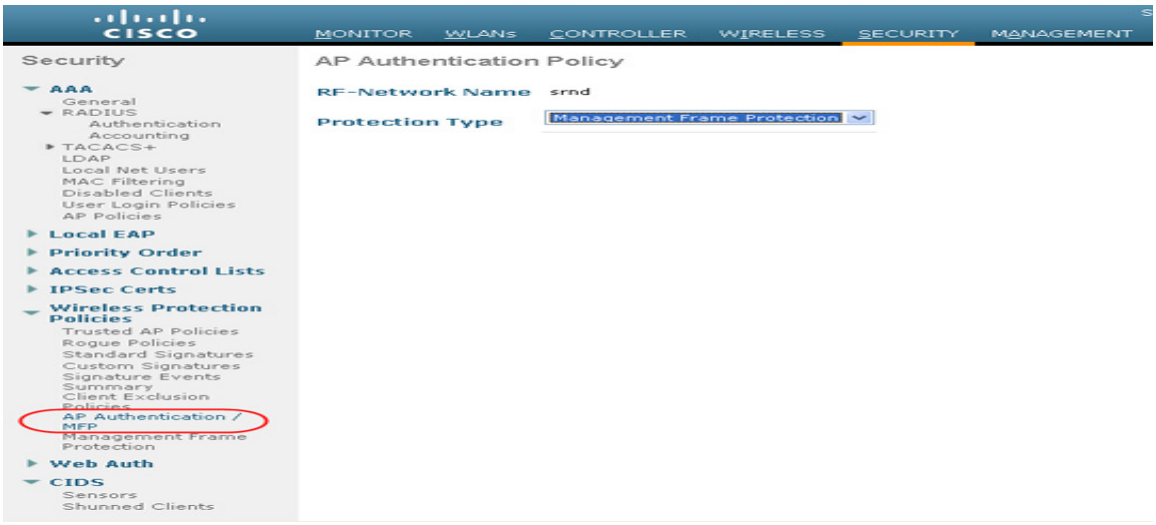
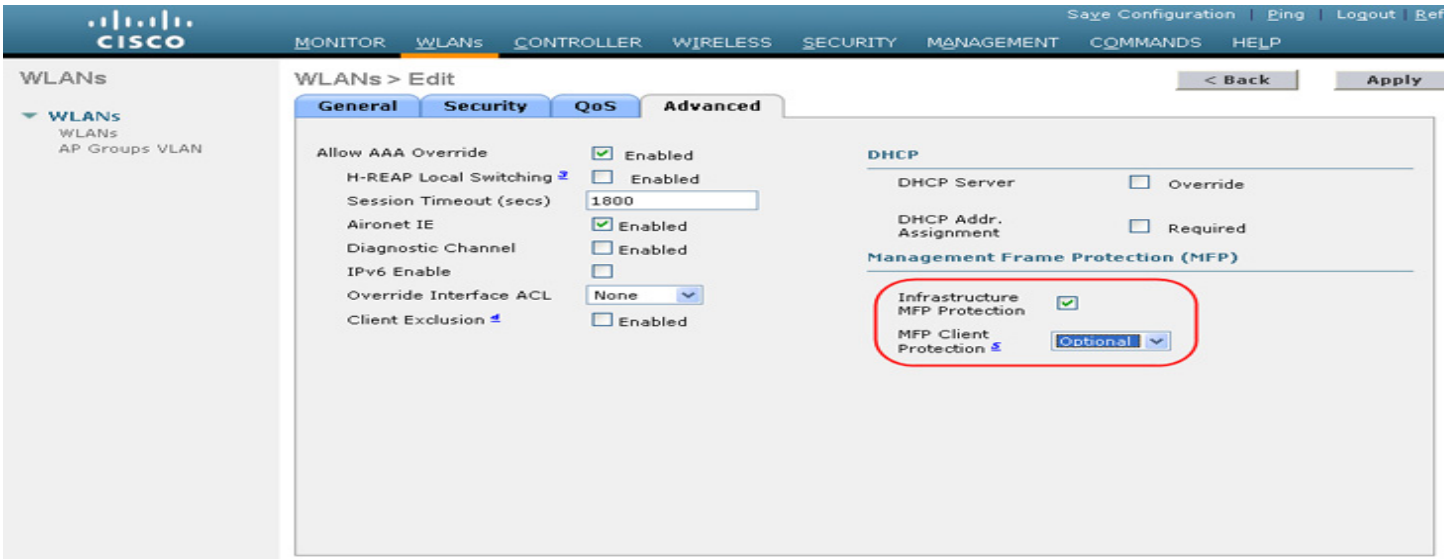


図 4-26　WLAN ごとの MFP のイネーブル化



クライアント管理フレーム保護

Cisco Compatible Extensions v5 の WLAN クライアントでは、MFP をサポートしています。上記の 図 4-26 で示したとおり、MFP は WLAN ごとにイネーブルにできます。

WLAN クライアントに MFP を提供する方式は管理フレームで MIC を使用するものであり、AP に使用する方式と基本的に同じです。これにより、信頼済みの管理フレームがクライアントによって識別できるようになります。MIC の暗号キーは、WPA2 認証プロセス中にクライアントに渡されます。クライアント MFP は、WPA2 に対してのみ使用できます。WPA および WPA2 クライアントが同じ WLAN を共有する場合、クライアント MFP は「Optional」に設定する必要があります。

管理システムのセキュリティ機能

不正 AP 検出に対するロケーション機能のサポート以外に、管理システム（WCS/NCS/PI）には Unified Wireless Network セキュリティに関する 2 つの機能があります。1 つは WLC 設定の確認管理、もう 1 つはアラームおよびレポート発行インターフェイスです。

設定の確認

管理システム（WCS/NCS/PI）には設定の監査レポートをオンデマンドまたは定期的に発行する機能があります。このレポートでは、WLC の現在稼働している完全な設定と、管理システム（WCS/NCS/PI）データベースに保存されている既知の有効な設定を比較します。現在稼働している設定と保存されているデータベース設定の間にある例外が明記され、画面のレポートを介してネットワーク管理者に通知されます（図 4-27）。

図 4-27　監査レポートの例

171.71.128.75 >Audit Report

Device name	171.71.128.75	**Time of Audit**	1:00:23
Report ID	68	**Synchronization Status**	Different In WCS And Controller

Object name	802.11 171.71.128.75
Synchronization Status	Different In WCS And Controller

<

Attribute	Value In WCS	Value In Device
bridgingSharedSecretKey	*****	*****

Object name	Known Rogues 171.71.128.75 00:01:64:45:b9:b8
Synchronization Status	Not Present In Controller
Object name	Known Rogues 171.71.128.75 00:02:8a:0e:37:bf
Synchronization Status	Not Present In Controller
Object name	Known Rogues 171.71.128.75 00:02:8a:1f:93:f9
Synchronization Status	Not Present In Controller
Object name	Known Rogues 171.71.128.75 00:02:8a:1f:94:15
Synchronization Status	Not Present In Controller
Object name	Known Rogues 171.71.128.75 00:02:8a:5b:40:4d
Synchronization Status	Not Present In Controller
Object name	Known Rogues 171.71.128.75 00:02:8a:5b:41:01
Synchronization Status	Not Present In Controller
Object name	Known Rogues 171.71.128.75 00:02:8a:5b:46:f0
Synchronization Status	Not Present In Controller
Object name	Known Rogues 171.71.128.75 00:02:8a:5b:46:f1
Synchronization Status	Not Present In Controller

190735

アラームおよびレポート

WLC から直接生成され、エンタープライズ ネットワーク管理システム（NMS）に送信できるアラームのほか、管理システムではアラーム通知の送信も可能です。さまざまなコンポーネントによって送信されるアラームのタイプとは別に、アラーム通知方法の主な違いは、WLC が Simple Network Management Protocol（SNMP）のトラップを使用してアラーム（NMS システムでしか解釈できない）を送信する一方で、管理システム（WCS/NCS/PI）は SMTP 電子メールを使用して管理者にアラーム メッセージを送信することです。

管理システム（WCS/NCS/PI）ではリアルタイムのレポートと定期的なレポートが提供されます。これらのレポートはエクスポートや電子メールによる送信が可能です。管理システム（WCS/NCS/PI）から提供されるレポートの内容は次のようなものです。

- アクセス ポイント
- 監査
- クライアント
- インベントリ
- メッシュ
- パフォーマンス
- セキュリティ

アーキテクチャの統合

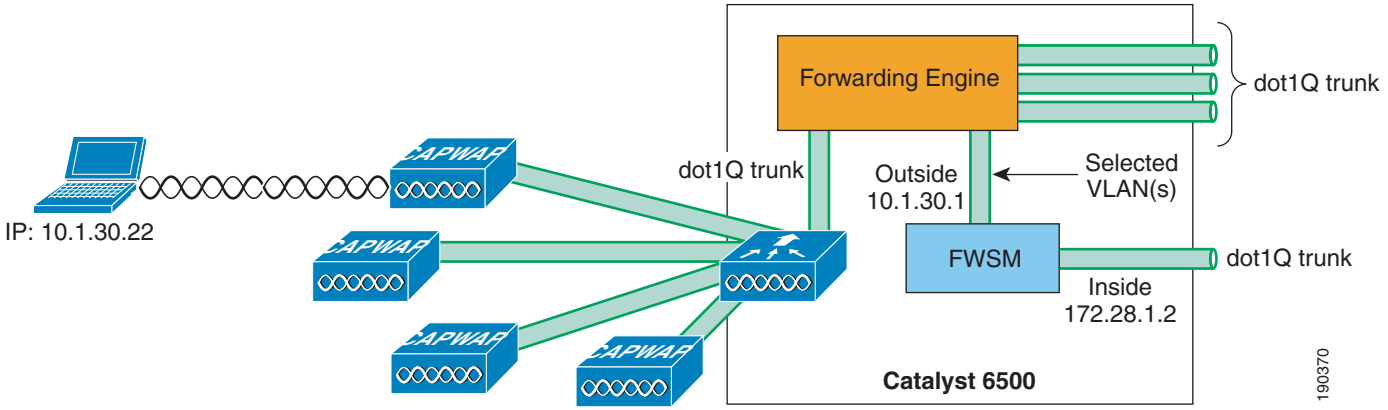
シスコでは、Cisco IOS に組み込まれたもの、サービスまたはネットワーク モジュールに統合されたもの、独立型アプライアンスとして提供されるもの、ソフトウェアとして提供されるものなど、さまざまなセキュリティ サービスを提供しています。

Cisco Unified Wireless Network アーキテクチャでは WLAN クライアントとアップストリームの有線ネットワーク間のレイヤ 2 接続を提供するため、ソリューションへのこれらのセキュリティ サービスの統合が容易になります。これは、クライアント トラフィックと「直列」に並ぶことで機能するアプライアンスやモジュールを、WLAN クライアントと有線ネットワーク間に容易に挿入できることを意味します。たとえば、古い WLSM ベースの展開では、Cisco Firewall Services Module（FWSM）を WLAN が通過するように Cisco 6500 に VRF-Lite を実装する必要がありますが、Cisco Unified WLAN の展開では、WiSM で簡単に WLAN クライアントの VLAN を直接 FWSM にマッピングできます。シスコ ワイヤレス製品の WLAN コントローラのうち、レイヤ 2 で物理/論理インターフェイスに直接 WLAN トラフィックをマッピングできないのは、ISR ベースの WLC モジュールのみです。ISR WLAN モジュールは ISR で利用可能なすべての IOS および IPS 機能にアクセスできますが、ルータの IOS VRF 機能を使用して、WLAN クライアントからの IP トラフィックを特定の ISR サービス モジュールのインターフェイスに送受信する必要があります。

図 4-28 では、WiSM と FWSM モジュールの間でのアーキテクチャの統合の例を示します。この例では、WLAN クライアントは外部ファイアウォール インターフェイスと同じサブネット上にあります。WLAN クライアント トラフィックが両方の方向でファイアウォールを通過することを保証するための、ルーティング ポリシーや VRF 設定は必要ありません。

WLAN の展開と組み合わせて Cisco Network Admission Control（NAC）アプライアンス（旧称 Cisco Clean Access）を実装することで、ネットワークに接続するエンド デバイスが、最新のセキュリティ ソフトウェア要件およびオペレーティング システムのパッチによってコンプライアンスに関する企業ポリシーに従っていることを保証できます。前述した FWSM モジュールのように、Cisco NAC アプライアンスもレイヤ 2 で Cisco Unified Wireless Network アーキテクチャに統合できます。これにより、無線ユーザの VLAN に NAC ポリシーを適用する厳密な管理が可能になります。

図 4-28　ファイアウォール モジュールの統合の例



ネットワーク層との統合が簡単であること以外に、Cisco Unified Wireless Network ソリューションは Cisco IDS の展開と統合されています。これにより、Cisco IDS によってブロックされているクライアントを、Cisco Unified Wireless Network から除外することができます。

Cisco Integrated Security Features

Cisco Integrated Security Features（CISF）は Cisco Catalyst スイッチに入っている機能です。悪意のあるユーザがネットワークへの無線アクセスを取得した後に実行するおそれのあるさまざまな攻撃を防御することができます。このセクションでは、これらの攻撃や、WLC がどのようにこれらの攻撃を防御するか、アクセス スイッチで CISF がイネーブルになっている場合に CISF がどのようにネットワークを保護するかついて説明します。

（注）　ここで述べる攻撃は、CISF がアクセス スイッチでイネーブルになっている場合に防御できるもののみであり、無線ネットワーク上に存在しうるすべての攻撃を総合的に分析することは意図していません。

攻撃のタイプ

攻撃は、有線ネットワークでも無線ネットワークでも発生することがあります。ただし、無線ネットワーク接続の場合、攻撃者はネットワークに物理的に接続しなくても攻撃を確立することができます。WLC および CISF には、次のような攻撃を防ぐために特別に設計された機能があります。

- MAC フラッディング攻撃
- DHCP 不正サーバ攻撃
- DHCP 枯渇攻撃
  - ARP スプーフィング攻撃
  - IP スプーフィング攻撃

MAC フラッディング攻撃

MAC フラッディング攻撃は、スイッチの Content-Addressable Memory（CAM）テーブルに情報を入力して、LAN トラフィックのフラッディングを開始させようとするものです。これらの攻撃は、macof（dsniff パッケージの一部）などのツールによって実行されます。macof は、任意の MAC および IP 送信元アドレスおよび宛先アドレスのフレームのフラッディングを生成するものです。

イーサネット スイッチのレイヤ 2 の学習メカニズムは、パケットの送信元 MAC アドレスに基づいています。ポートで受信した新規の送信元 MAC アドレスそれぞれについて、そのポートと、ポートが属する VLAN の CAM テーブル エントリがスイッチによって作成されます。macof ユーティリティは、これらのエントリを保存するために使用可能なスイッチ上のメモリが有限であれば、通常 10 秒未満で CAM テーブルを一杯にします。CAM テーブルのサイズは有限です。他のエントリが期限切れになる前に十分なエントリが CAM テーブルに入力されると、CAM テーブルが一杯になり、新しいエントリを受信できなくなります。

スイッチの CAM テーブルが一杯になると、CAM テーブルの特定の MAC アドレスのポート番号を特定できないため、着信トラフィックがあるポートすべてがフラッディングされます。スイッチは基本的に、パフォーマンスとセキュリティが損なわれたハブのように機能します。オーバーフローによりローカルの VLAN 内でトラフィックがあふれるため、そのユーザが接続された VLAN 内のトラフィックを侵入者側から見ることができます。

レイヤ 3 では、macof の対象となる任意の IP 送信先では、マルチキャスト アドレス空間も使用します。したがって、Protocol Independent Multicast（PIM）プロセスが偽のルートを処理しようとするため、マルチキャストがオンになっているディストリビューション レイヤ スイッチは高い CPU 利用率を経験することになります。

DHCP の不正サーバ攻撃

DHCP の不正サーバ イベントは、意図的な攻撃の結果である可能性と、ユーザが誤ってネットワーク セグメントに DHCP サーバを持ち込み、誤って IP アドレスを発行しようとした可能性があります。侵入者は DHCP サーバを持ち込み、DNS サーバを示す IP アドレスや、侵入者に制御されているコンピュータに疑いを持つことなくユーザのトラフィックをリダイレクトするデフォルトのゲートウェイを提示することができます。

DHCP 枯渇攻撃

DHCP 枯渇攻撃は、特定のセグメントの DHCP 範囲内にあるアドレスすべてを枯渇させることを意図しています。DHCP が枯渇すると、正規のユーザであっても DHCP を介して要求された IP アドレスが拒否されるため、ネットワークにアクセスできなくなります。Gobbler は、自動 DHCP 枯渇攻撃を実行するパブリック ドメインのハッキング ツールです。DHCP 枯渇は純粋な DoS メカニズムである場合もありますが、悪意のある不正なサーバ攻撃と組み合わせることで、トラフィックを傍受できる悪意のあるコンピュータへトラフィックの方向を変更するために使用される場合もあります。

ARP スプーフィング ベースの中間者攻撃

中間者（MIM）攻撃は、ネットワーク上を移動するデータを悪意のあるユーザが傍受する（あるいは変更する）ネットワーク セキュリティ侵害です。MIM 攻撃では ARP スプーフィングが使用されます。ARP スプーフィングでは、Gratuitous ARP（GARP）要求が悪用され、悪意のあるコンピュータにトラフィックが誤って転送されることで、そのコンピュータが特定の LAN セグメントの IP セッションの「中間者」となります。ARP スプーフィングの実行には、*ettercap*、*dsniff* および *arpspoof* というハッキング ツールが使用されます。特に ettercap は特定の LAN セグメントのすべてのステーションを表示する高度なユーザ インターフェイスであり、さまざまな種類の IP セッションのパスワードを取り込むための高度なパケット キャプチャ機能があります。

IP スプーフィング攻撃

IP スプーフィング攻撃は、他のユーザの IP アドレスをスプーフィングして DoS 攻撃を実行します。たとえば、送信元のセカンド パーティの IP アドレスが攻撃を受けている間に、攻撃者はサード パーティのシステムを ping することができます。ping の応答は、サードパーティ システムからセカンド パーティに転送されます。

無線展開トポロジに対する CISF

このセクションでは、さまざまな Cisco Unified Wireless Network 展開トポロジについて説明します。次のセクションでは、WLC または CISF 機能が無線攻撃をどのように防御するかについて説明します。

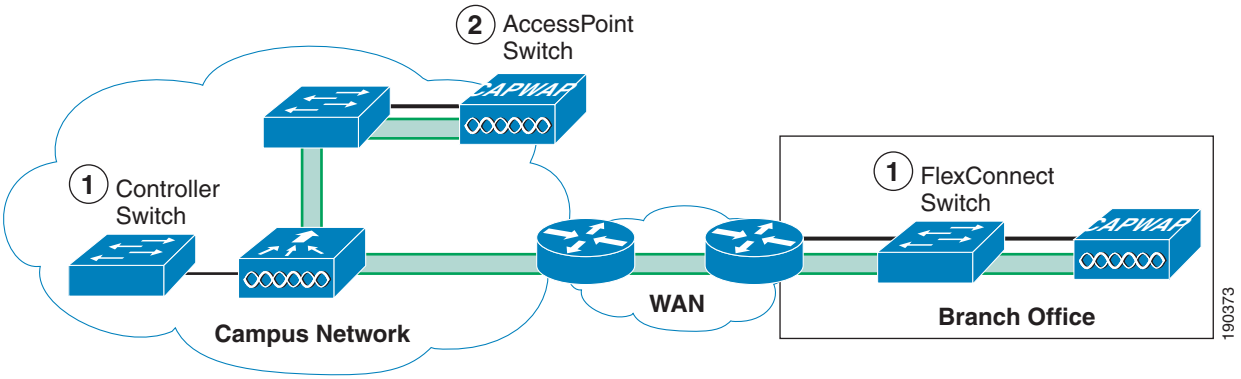
CISF は現在、アクセス ポイント（AP）から直接ではなくアクセス スイッチでのみ利用可能です。したがって、これらの機能の利点は、無線での攻撃者からのトラフィックがスイッチを通過している場合のみ有効です。

Unified Wireless Network ソリューションでは、3 か所をアクセス スイッチとみなすことができるため、アクセス スイッチの定義が若干異なります。

- コントローラ インターフェイスがネットワークで終端するポイント
- CAPWAP AP がネットワークで終端するポイント
- FlexConnect AP がネットワークで終端するポイント

これらのロケーションについて、図 4-29 で示します。

図 4-29　　アクセス スイッチ



CISF に関係する接続は、コントローラのスイッチおよび FlexConnect スイッチです。WLAN トラフィックは AP スイッチ上で終端せず、AP はそのスイッチ ポートに接続されている単一デバイスとして登場するだけで、セキュリティの観点からはアクセス クライアントとみなされるため、AP スイッチについては論じません。

（注）　CAPWAP AP と標準クライアントとの主な違いは、CAPWAP AP の Differentiated Services Code Point（DSCP）値が信頼済みであるという点です。

次のトポロジの対象範囲は、無線ユーザ間の攻撃に限定されています。これは、無線ユーザと有線ユーザが別々のサブネットでサポートされている（シスコのベスト プラクティスで推奨）ためであり、サブネット間の攻撃に関する議論はここの議論の範囲を超えているためです。

次の 3 つのトポロジについて考えます。

- トポロジ 1：攻撃者が接続されている AP と同じ AP にターゲットがアソシエートしている
- トポロジ 2：攻撃者とは別の AP にターゲットがアソシエートしている
- トポロジ 3：攻撃者とは別の AP にターゲットがアソシエートし、この AP が別のコントローラに接続される

1 つ目のトポロジでは、攻撃者とターゲットが両方とも同じ AP に関連付けられ、トラフィックは FlexConnect または WLC でローカルのままであるため、CISF は役に立ちませんが、Cisco Unified Wireless Network のネイティブのセキュリティでこれらの問題に対処できます。2 つ目と 3 つ目は CISF が有効なトポロジです。

さまざまなレベルの承認を必要とする企業の WLAN 展開では、一般的に SSID ごとに複数の VLAN が使用されます。これにより、FlexConnect AP または WLC 上のファスト イーサネット ポートと、アクセス スイッチの対応するポートの間に、802.1q のトランクを設定する必要があります。複数の VLAN が定義されるため、管理者はデータ トラフィックを AP と WLC の管理トラフィックから分離しておくことができます。

企業のセキュリティ ポリシーで、さまざまな種類のユーザに対してさまざまな種類の認証と暗号化が要求される（ゲスト アクセスに対してオープン認証は必要だが暗号化は行わない、従業員に dot1x 認証および強力な暗号化を行うなど）場合もあります。これは、FlexConnect AP または WLC にマルチ SSID および VLAN を定義することで達成されます。

上記の条件から、設定例で使用される設定は、WLC か FlexConnect AP とアクセス スイッチとの間のトランク接続を想定して行われます。

ポート セキュリティの使用による MAC フラッディング攻撃の軽減

ポート セキュリティでは、1 つのポートで許可される MAC アドレスの最大数を設定します。アドレス テーブルにアドレスを、手動、ダイナミックまたはその両方の組み合わせで追加できます。アドレス テーブル内の MAC アドレスの最大数に到達するとハードウェア内でパケットがドロップされ、アドレス テーブル内に MAC アドレスを持たないステーションがトラフィックを送信しようとします。

スイッチのアクセス ポートのポート セキュリティをイネーブルにすると、MAC フラッディング攻撃が停止されます。これは、そのポートで許容される MAC アドレスが制限されるためです。違反に対する対応が**シャットダウン**に設定されている場合、ポートはエラー ディセーブル状態になります。対応が*制限*に設定されている場合、送信元 MAC アドレスが未知のトラフィックはドロップされます。

ワイヤレス ネットワークでのポート セキュリティ

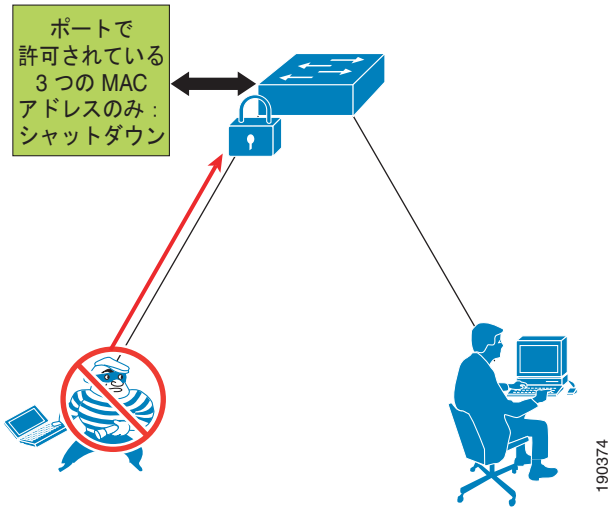
通常、FlexConnect AP や WLC に接続するスイッチ ポートでポート セキュリティをイネーブルにすることは推奨しません。ポート セキュリティを使用するということは、スイッチがそのポートから学習し、許可する MAC アドレスの正確な数が分かるということを暗に意味します。FlexConnect AP や WLC の場合、スイッチが学習したさまざまな送信元 MAC アドレスは通常、無線ユーザに対応します。スイッチ ポートでポート セキュリティを設定すると、有線ネットワーク上にいる特定の数のユーザだけが許可されます。

たとえば、一定の数の MAC しかアクセス ポイントを介してトラフィックを送信できないというセキュリティ ポリシーを設定している会社もあります。この場合、FlexConnect AP や WLC 上の MAC フィルタリングと、スイッチのポート セキュリティを組み合わせることで、選択されたユーザだけが有線ネットワークにアクセスできるようになります。

ただし、通常、会社が WLAN を展開するのは従業員の機動力を高めるためです。このことは、FlexConnect AP や WLC が、それ自体に関連付けられているユーザ数が常にあらかじめ決定されていないということを暗に意味しています。

したがって、AP に接続されているユーザ数を判断できない場合、スイッチ ポートのポート セキュリティをイネーブルにしても、メリットはありません。最悪の場合、違反が発生した場合にポートをシャット ダウンするようなポート セキュリティのポリシーが設定されると、強制的な DoS 攻撃が作成される場合があります。これが発生すると、その AP に接続されたユーザがすべてネットワークから切断されます。図 4-30 では、ポートをロックして SNMP トラップを送信することで無線 MAC フラッディング攻撃を制限するポート セキュリティの使用例を示します。

図 4-30　　ポート セキュリティの使用



ポート セキュリティの有効性

ポート セキュリティが攻撃を阻止するオプションでない場合、無線ユーザが MAC フラッディング攻撃を開始しても成功しません。その理由は、802.11 プロトコル自体にあります。AP とのアソシエーションは MAC ベースで行われます。このことは、AP ブリッジ（トランスレーショナル ブリッジ）のトラフィックが既知のユーザ（既知の MAC）との間で送受信されることを意味します。無線ユーザによって MAC フラッディング攻撃が開始された場合、ランダムに生成された MAC アドレスを持つ、AP に関連していないすべての 802.11 フレームはドロップされます。許可されるフレームは、スイッチがすでに学習していると思われる、悪意のあるユーザの MAC アドレスを持つフレームのみです。このため、アクセス ポイントの基本動作自体によって、スイッチが MAC フラッディング攻撃の被害に遭うことが防止されます。

ポート セキュリティの使用による DHCP 枯渇攻撃の軽減

有線アクセスの場合、ポート セキュリティでは現在、Gobbler などのツールを使用しているスイッチに接続された PC から実行される DHCP 枯渇攻撃を防止できます。攻撃が成功しないのは、ポート セキュリティによる軽減よりも、ツールの機能の制限によるものです。このような攻撃が失敗する理由は、Gobbler が別のソース MAC アドレスを使用して別の DHCP 要求を生成するからであり、ポートの保護によって攻撃を軽減できるからです。

ただし、攻撃者がイーサネット パケット内の MAC アドレスを使用でき、DHCP ペイロード内の MAC アドレス（chaddr フィールドという）を単純に変更した場合、ポート セキュリティでも攻撃は停止されません。この場合、現在可能な対策は、スイッチ ポートの DHCP レート リミッタを使用して攻撃を抑制することのみです。

無線 DHCP 枯渇攻撃

Unified Wireless Network 展開では、DHCP 枯渇攻撃に対する脆弱性は、ユーザ トラフィックを終端する WLC と、ユーザ トラフィックを終端する FlexConnect の間で異なります。

WLC は、DHCP 枯渇攻撃からネットワークを保護します。これは、DHCP 要求を確認することによってクライアントの MAC アドレスが chaddr に一致することが保証されるためです。アドレスが一致しない場合、DHCP 要求はドロップされます。

FlexConnect の場合、ユーザ VLAN はローカルで終端され、DHCP 要求はコントローラを通過せず、chaddr の分析は実行できません。この場合、このアクセス方法には、有線アクセスの場合と同じセキュリティ上の考慮事項が該当します。スマート（無線）攻撃者は、AP にアソシエートしている自分の MAC アドレスを使用してランダムな DHCP 要求を生成し、かどうかを AP に関連付けられただけを使用し、DHCP パケットのペイロード内で MAC アドレスの要求を単純に変更します。このとき、AP 側から見ると、パケットは有効に見えます。これは、信頼済み AP との関連付けに使用される MAC と送信元 MAC が同じであるためです。

DHCP スヌーピングによる不正な DHCP サーバ攻撃の軽減

DHCP スヌーピングは、DHCP スヌーピング バインディング テーブルを構築および維持し、信頼できない DHCP メッセージをフィルタリングすることでセキュリティを確保する DHCP セキュリティ機能です。この機能は、エンドユーザに接続する信頼できないインターフェイスと DHCP サーバまたは別のスイッチに接続する信頼できるインターフェイスとを区別することによって動作します。エンドユーザ ポートは、DHCP 要求のみを送信し、いかなる種類の DHCP トラフィックも送信しないように制限することができます。信頼済みポートではすべての DHCP メッセージの転送が許可されます。DHCP スヌーピング テーブルは VLAN ごとに構築され、クライアントの IP アドレスと MAC アドレスを信頼できないポートに関連付けます。DHCP スヌーピングをイネーブルにすると、非正規の DHCP サーバに接続しているユーザが信頼できない（ユーザ方向の）ポートに接続し、DHCP 要求に応答し始めるのを防止します。

ワイヤレス アクセスの DHCP スヌーピング

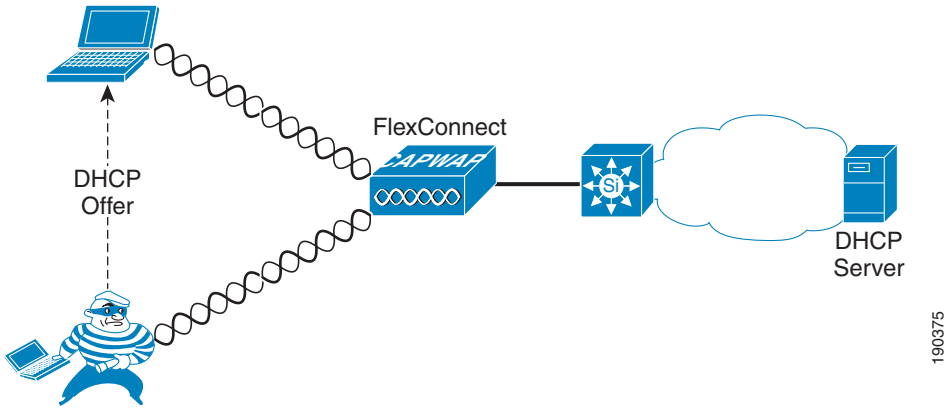
WLC はクライアントからのすべての DHCP 要求を管理し、DHCP リレー エージェントとして機能します。WLAN クライアントからの DHCP 要求は、WLAN に戻るブロードキャストではなく、WLC から設定済みの DHCP サーバへユニキャストされます。これにより、他の WLAN クライアントが不正な DHCP サーバ攻撃から WLC に接続することを防御します。

FlexConnect 802.1q トランク インターフェイスを介して VLAN に接続しているクライアントは、不正な DHCP サーバ攻撃から保護されません。

CISF 機能（この場合は DHCP スヌーピング）は AP でなくスイッチに対して実装されるため、不正なサーバからの悪意のあるメッセージを阻止する機能が働くのはスイッチからトラフィックが見える場合のみであることに注意してください。

図 4-31 で、不正な DHCP サーバの攻撃を軽減するための DHCP スヌーピングの使用例および、スイッチで DHCP を保護できるようになる前に攻撃がどのように発生するかを説明します。

図 4-31　不正な DHCP サーバ攻撃に対して使用されるセキュリティ



DHCP スヌーピングの有効性

DHCP スヌーピングは VLAN ごとにイネーブルになっているため、トランク ポートで動作します。異なる VLAN 内のクライアントの特定のトランク ポートで受信される DHCP 要求には、それぞれ異なる DHCP スヌーピング エントリが挿入されます。トランク ポートで DHCP スヌーピングが動作するという事実は非常に重要です。それは、この CISF 機能を、FlexConnect WLC のローカル インターフェイスに複数の SSID と VLAN が設定された WLAN 導入に応用できるためです。攻撃者が同じ WLAN/VLAN にターゲットとして関連付けられているが、経由する FlexConnect WLC は異なっている場合、スイッチによって DHCP スプーフィング攻撃を防御できます。ただし、攻撃者とターゲットが同じ FlexConnect WLC に関連付けられている場合、攻撃はアクセス スイッチを通過しないため、検出されません。

DHCP スヌーピングは、DHCP サーバに対する DHCP 要求を制限するレート制限によって、DHCP サーバ攻撃を防御します。

ダイナミック ARP インスペクションによる中間者攻撃の軽減

ダイナミック ARP インスペクション（DAI）は、アクセス スイッチで VLAN ごとにイネーブルになっています。これにより、ARP 要求や Gratuitous ARP（GARP）を含む応答を、DHCP バインディング テーブル内の DHCP スヌーピングが入力された MAC/IP エントリと比較します。スイッチが ARP メッセージを受信したときに、DHCP バインディング テーブルに一致するエントリがない場合、パケットは廃棄され、ログ メッセージがコンソールに送信されます。

DAI は、ettercap を使用して実行されるような中間者（MIM）攻撃につながる可能性のある ARP ポイズニング攻撃を防止します。ettercap は、悪意のあるユーザからターゲットへ送信された GARP メッセージを停止し、悪意のあるユーザのトラフィックを受信するように ARP テーブルを変更します。ARP メッセージは、攻撃者が接続しているポートで直接フィルタリングされます。

ワイヤレス アクセスに対する DAI

WLC は、WLC 自体に対する DAI と同様の機能を実行することで、MIM 攻撃を防御します。WLC に直接接続している VLAN のアクセス スイッチで DAI をイネーブルにしないでください。これは、WLC が GARP を使用してレイヤ 3 のクライアント ローミングをサポートしているためです。

FlexConnect とアクセス ポイントの間のトランクで設定された各 VLAN の DAI をイネーブルにできます。したがって、FlexConnect 上に複数の SSID と VLAN が存在する無線の展開において DAI は便利です。ただし、FlexConnect での WLC 展開では、DAI 機能の有効性に影響を与えるトポロジが 2 つあります。いずれのトポロジでも、両方の攻撃者が FlexConnect WLC に関連付けられていて、ターゲットにレイヤ 2 で隣接していると仮定しています。

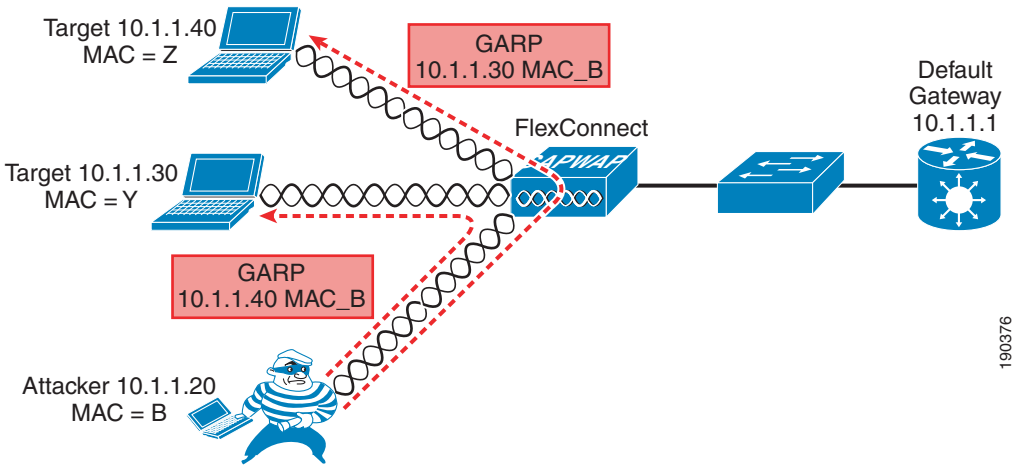
- トポロジ 1：一方のターゲットは無線接続されていて同じ AP に攻撃者として関連付けられているが、もう一方のターゲットはデフォルト ゲートウェイです。これが最も一般的な攻撃です。
- トポロジ 2：両方のターゲットが無線接続されています。

次の例では、攻撃がどのように開始され、停止されるかについて説明します。

- MIM は GARP を使用してデフォルト ゲートウェイと無線ターゲットの ARP テーブル エントリを変更し、攻撃者へトラフィックの方向を変更させようとします。DAI によってデフォルト ゲートウェイに対する GARP がブロックされる場合がありますが、無線ターゲットに対してスプーフィングされた GARP への DAI の影響はありません。これによって MIM 攻撃の影響は限定されますが、完全に MIM 攻撃の影響を防ぐことはできません。
- MIM 攻撃は無線クライアントに GARP を送信します。DAI を実装しているスイッチではこれらの GARP を認識しないため、攻撃を防止することはできません。

図 4-32 では、サブネット上の 2 つの IP 接続ノードに GARP を送信し、2 つのノードの間のトラフィックの方向を変えようとする攻撃メカニズムの例を示します。

図 4-32　　ダイナミック ARP インスペクション



DAI の影響

図 4-32 の例では、攻撃が完全に成功するのは、トラフィックが FlexConnect の WLC に対してローカルのままであり、スイッチを一度も移動しない場合のみです。通常、攻撃者の標的となるトラフィック（パスワードやアカウント情報など）は無線クライアントから有線ネットワーク（サーバまたはインターネット）に移動するため、それほど問題はありません。

デフォルト ゲートウェイと無線クライアントが攻撃対象である例を、半二重 MIM 攻撃と呼ぶことができます。ettercap により、すべてのトラフィックを侵入者に送信するように無線ユーザの ARP テーブルが変更される場合があります。ただし、次の例で示すように、デフォルト ゲートウェイへの GARP の送信はスイッチによって阻止されます。

```
4507-ESE#sh ip arp inspection log
Total Log Buffer Size : 32
```

```
Syslog rate : 5 entries per 1 seconds.
Interface Vlan Sender MAC Sender IP Num of Pkts Reason
---------- ---- -------------- --------------- ----------- ------
Fa3/26 20 00d0.5937.7acc 10.20.1.100 1(11:07:48 PDT Wed Oct 3 2012) DHCP
Deny
Fa3/26 20 00d0.5937.7acc 10.20.1.100 1(11:07:48 PDT Tue Oct 3 2012) DHCP
Deny
Fa3/26 20 00d0.5937.7acc 10.20.1.100 1(11:07:48 PDT Tue Oct 3 2012) DHCP
Deny
Fa3/26 20 00d0.5937.7acc 10.20.1.100 1(11:07:48 PDT Tue Oct 3 2012) DHCP
Deny
Fa3/26 20 00d0.5937.7acc 10.20.1.100 1(11:07:48 PDT Tue Oct 3 2012) DHCP
Deny
Fa3/26 20 00d0.5937.7acc 10.20.1.100 1(11:07:48 PDT Tue Oct 3 2012) DHCP
Deny
Fa3/26 20 00d0.5937.7acc 10.20.1.100 1(11:07:48 PDT Tue Oct 3 2012) DHCP
Deny
Fa3/26 20 00d0.5937.7acc 10.20.1.100 1(11:07:48 PDT Tue Oct 3 2012) DHCP
Deny
Fa3/26 20 00d0.5937.7acc 10.20.1.100 1(11:07:48 PDT Tue Oct 3 2012) DHCP
Deny
Fa3/26 20 00d0.5937.7acc 10.20.1.100 1(11:07:48 PDT Tue Oct 3 2012) DHCP
Deny
Interface Vlan Sender MAC Sender IP Num of Pkts Reason
---------- ---- -------------- --------------- ----------- ------
Fa3/26 20 00d0.5937.7acc 10.20.1.100 1(11:07:49 PDT Tue Oct 3 2012) DHCP Deny
```

MAC アドレスがログに記録されるため、管理者は攻撃者をアソシエート解除することによって、さらに確実なブロック アクションを実行できます。

DAI が VLAN に設定されている場合、ARP のレート リミッタは、特定のポートからの ARP 要求のフラッディングを防ぐようにグローバルで設定されています。レート リミッタのデフォルト値は 15 パケット/秒（pps）です。この上限に到達すると、スイッチは攻撃を防ぐためにポートをディセーブルにします。この場合、攻撃者が MIM 攻撃を実行するためには、まず他の誰が隣接するレイヤ 2 であるかを見つけ出す必要があります。そのために ettercap は一連の GARP を生成し、サブネット上の各 IP アドレスであると主張します。この方法では、そのアドレスの実際の所有者が応答し、ettercap がテーブルを作成する場合があります。

実験では、ettercap を使用すると即座にこの上限に達し、ポートがシャット ダウンしました。これは、有線トポロジにも当てはまります。無線トポロジでは、AP に接続されたポートをシャット ダウンすると、すべての無線ユーザと外部との接続が失われ、可能性のある MIM 攻撃が DoS 攻撃に変わります。

このような（強制的に DAI をイネーブルにすることで作成される）DoS を回避するため、シスコでは AP に接続されたスイッチのポートで ARP レート リミッタをオフにすることを推奨します。この操作は、次のインターフェイス レベルのコマンドで実行できます。

```
ip arp inspection limit none
```

そのほか、しきい値を 15 pps より大きい値に変更する方法もあります。ただし、攻撃を実行するために使用される特定のツールの実装によって方法が異なるため、これは一般的な解決策ではありません。

IP ソース ガードの使用による IP および MAC スプーフィングの軽減

アクセス スイッチのインターフェイスがイネーブルの場合、IP ソース ガードは、DHCP スヌーピング バインディング テーブルの内容に基づいて、Per-Port アクセス コントロール リスト（PACL）を動的に作成します。この PACL は、DHCP バインディング時に発行された IP アドレスからトラフィックを送信するように強制することで、スプーフィングされた他のアドレスによってトラフィックが転送されるのを防止します。またこれにより、攻撃者が、アドレスを手動で変更したり、アドレスのスプーフィングを行うように設計されたプログラム（hping2 など）を実行したりして、有効なアドレスを偽装す

ることを防止します。この機能には、着信アドレスをフィルタリングするオプション（ポート セキュリティ）があります。ここでも、DHCP スヌーピング バインディング テーブル内の MAC アドレスを使用します。

攻撃者は一般的に、スプーフィングされたアドレスを使用して自分の実際のアイデンティティを非表示にし、DoS 攻撃などのターゲットに対する攻撃を実行します。

無線アクセスに対する IP ソース ガード

無線アクセスの場合には、FlexConnect の WLC にアクセス スイッチを接続するトランク ポート上で IP ソース ガードをイネーブルにできます。これにより、DHCP バインディング テーブル内のエントリと一致しない無線ユーザからのトラフィックをスイッチでフィルタリングできます。

WLC の後ろに設定されている VLAN では、IP ソース ガードをイネーブルにする必要はありません。これは、WLC が同様の機能を実行して、クライアントで使用される IP アドレスが、そのクライアントに割り当てられた IP アドレスであることを保証しているためです。

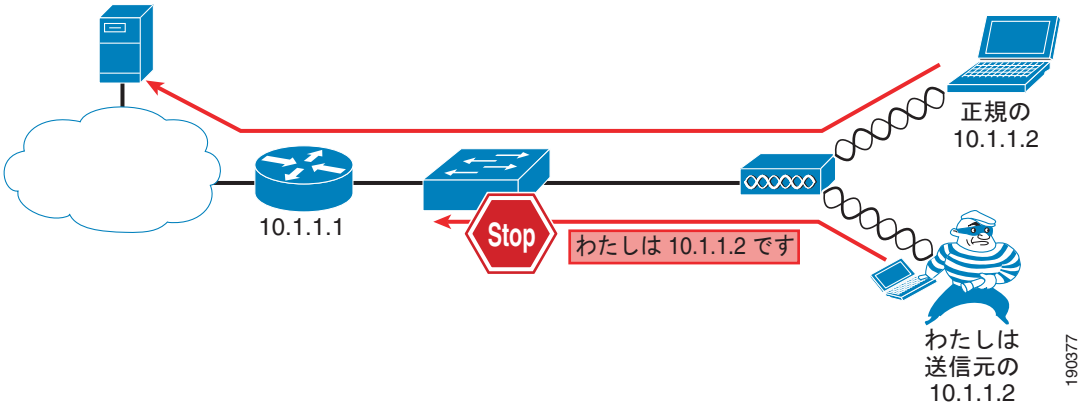
FlexConnect AP（標準の AP とは異なる）では WLAN クライアントの MAC アドレスと IP アドレスとのバインディング関係を検証できないため、FlexConnect の WLC 展開には IP ソース ガードが有利です。

テストでは、次の 2 つのトポロジが考慮されました。

- トポロジ 1：ターゲットが、同じ AP に関連付けられている他の無線ユーザによって表される。
- トポロジ 2：ターゲットが、別の AP に関連付けられた別の無線ユーザである。

図 4-33 は、IP および MAC スプーフィング攻撃を軽減するための IP ソース ガードの使用例です。

図 4-33　IP ソース ガードによる MIM の防止



IP ソース ガードの有効性

IP ソース ガード機能の有効性は、攻撃者がアドレスをどのようにスプーフィングするかと、どのトポロジがテストされるかという 2 つの要因に依存します。

AP へのアソシエーションはクライアントの MAC アドレスに基づくため、未知の送信元 MAC アドレスが指定されたフレームを受信すると、AP はそのフレームをドロップします。IP スプーフィング攻撃を実行する際、攻撃者にできる方法は、自分の MAC アドレスを使用するか、同じ AP に接続されている他のユーザからの MAC アドレスを使用するかです。他のすべての組み合わせ（ランダムな MAC アドレスを使用したり、別の AP に接続されたユーザの MAC アドレスを使用したりするなど）を使用すると、AP がフレームをドロップするため攻撃は失敗します。

攻撃者が自分の MAC アドレスを使用し、IP アドレスはスプーフィングした場合、スイッチでイネーブルになっている IP ソース ガードは、2 つ目トポロジではなく 1 つめのトポロジの攻撃を阻止します。1 つ目のトポロジでは、トラフィックは AP に対してローカルのままなので、CISF 機能は呼び出されません。2 つ目のトポロジでは、悪意のあるユーザによって送信された IP スプーフィングされたパケットのエントリが DHCP スヌーピング テーブルに存在しないため、CISF は正常に攻撃を阻止します。

ただし、攻撃者が同じ AP に接続された他の無線ユーザの MAC アドレスと IP アドレスの両方をスプーフィングできる場合、基本的には別のユーザのアイデンティティを想定しているため、攻撃はトポロジ 1 および 2 で成功します。MAC アドレスと IP アドレスの両方をスプーフィングすることは、暗号化が使用されていないホットスポット環境や、WEP の弱点を悪用した状況であれば現実に可能です。これが、可能な限り強力な暗号の使用をシスコが強く推奨する理由の 1 つです。

ターゲットへの攻撃の概要

表 4-2 では、該当するターゲットへの攻撃、考慮事項および解決策の簡単な要約を示します。

表 4-2　　調査結果の概要

ターゲットへの攻撃	適用性	考慮事項	ソリューション
MAC フラッディング	なし	Macof がランダムな MAC アドレスを送信元および宛先として使用する	アソシエーション テーブルに存在しない送信元 MAC からのフレームを AP が廃棄する
DHCP 枯渇	FlexConnect では、ありコントローラが不正な DHCP 要求を廃棄する	要求する MAC が DHCP ペイロード内で送信される	なし - レート制限
不良 DHCP サーバ	FlexConnect では、ありWLAN からの DHCP オファーをコントローラがブロックする	不正な DHCP サーバが無線であることを前提とする	なし
無線クライアント間の MIM	FlexConnect では、ありコントローラが GARP をブロックする	この場合、トラフィックはスイッチを通過しない	なし
異なる AP の無線クライアント間の MIM	FlexConnect では、ありコントローラが GARP をブロックする	ハッカーがトラフィックを妨害できるのは有線に対してのみである	違反のある DAI
無線クライアントと有線クライアントの間の MIM	FlexConnect では、ありサポートされていないコントローラ設定	ハッカーがトラフィックを妨害できるのは有線に対してのみである	違反のある DAI
IP スプーフィング	FlexConnect では、ありコントローラが IP アドレスと MAC アドレスのバインディングをチェックする	アイデンティティのスプーフィングを防止するために無線での暗号化が必要	IP ソース ガード

（注）　有線アクセス上に存在するのは CISF 機能の対象となる攻撃しかないので、攻撃者は常に無線であると想定されますが、ターゲットはそのとき関わっているトポロジによって有線の場合と無線の場合があります。