CHAPTER 1

802.11 ネットワーク セキュリティの基本

この章は、802.11 ネットワーク セキュリティの機能の概要について説明しており、次の項で構成されています。

概要

この項は、企業内に無線 LAN の導入を計画しているシステム管理者を対象としており、現在利用可能な 802.11 セキュリティの主な機能の概要について説明しています。この章では、Wi-Fi Protected Access（WPA）および WPA2 を中心に説明し、Wired Equivalent Privacy（WEP）機能についても簡単に説明します。

WEP はオリジナルの 802.11 規格で規定された最初のセキュリティ メカニズムですが、新しい 802.11i 規格によって置き換えられました。当初、802.11 規格には脆弱性がありましたが、新しい 802.11i 規格の導入によりその脆弱性が解決されました。これらの新しいセキュリティの強化は、認証および暗号化の使用による機密通信への企業要求に対応しています。

用語

このガイドでは、無線システムの基本的な物理コンポーネントに多くの一般用語を使用しています。図 1-1 は、これらのコンポーネントである無線 LAN クライアント、アクセス ポイント、無線 LAN コントローラ（WLC）、および AAA（認証、認可、アカウンティング）サーバ間のシステム トポロジを示しています。

図 1-1　安全な無線トポロジ

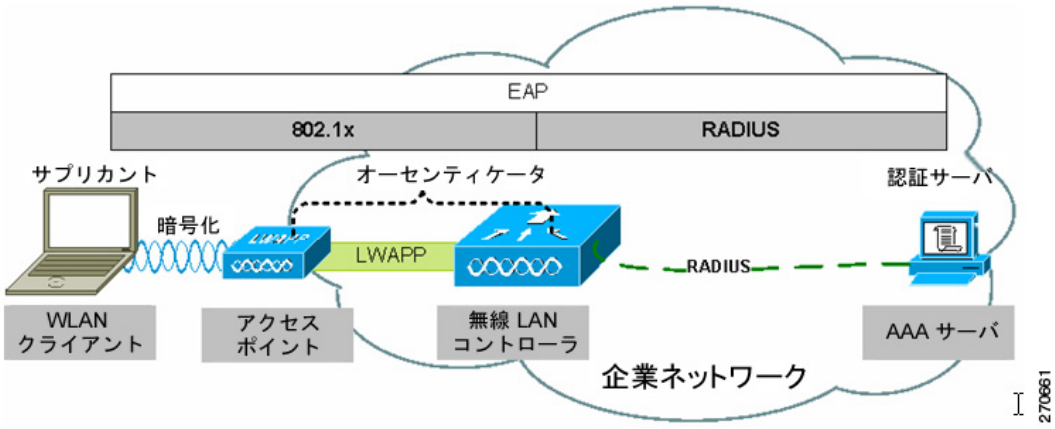


図 1-1 は、802.1X 認証プロセスの基本的な役割および関係も示しています。802.1X サプリカント（Cisco Secure Services Client）は無線 LAN クライアント上に存在します。アクセス ポイントと WLC は、スプリット MAC アーキテクチャによって 802.1X オーセンティケータとして機能します。AAA サーバは認証サーバです。また、この図は、クライアントと認証サーバ間の EAP（拡張認証プロトコル）パケットの送信における 802.1X および RADIUS プロトコルの役割も示しています。802.1X の詳細については、「IEEE 802.1X」の項（P.1-8）を参照してください。EAP の詳細については、「EAP」の項（P.1-9）を参照してください。

IEEE 802.11 の基本

802.11 無線 LAN は、次の基本コンポーネントが動作しています。

- ビーコン：無線 LAN ネットワークの存在を示すために使用されます。
- プローブ：無線 LAN クライアントがネットワークを見つけるために使用します。
- 認証：従来の 802.11 規格で定義された機能です。
- アソシエーション：アクセス ポイントと無線 LAN クライアント間のリンクを確立するプロセスです。

ビーコンは、アクセス ポイントによって定期的にブロードキャストされますが、プローブ、認証、およびアソシエーションの各フレームは、通常、アソシエーションおよび再アソシエーション プロセスでのみ使用されます。

ビーコン

無線 LAN ビーコン フレームには、SSID サービスセット ID、またはネットワーク名とも呼ばれます)、サポートされているビット レート、およびその無線 LAN のセキュリティ設定など、アクセス ポイントについての設定情報が含まれます。

ビーコンの主な目的は、無線 LAN クライアントが周囲にどのような利用可能なネットワークがあるのかを識別できるようにすることです。これにより、無線 LAN クライアントは、アソシエーションを試行するネットワークを選択できます。

多くの 無線 LAN のセキュリティ マニュアルでは、SSID を含めないでビーコンを送信することが、SSID をハッカーに知られないようにするためのセキュリティ上のベスト プラクティスであるとして推奨されています。すべての企業向け無線 LAN ソリューションでは、この機能をオプションとして提供していますが、SSID はアソシエーションの試行中に簡単に特定できるため、このオプションはある程度の効果しかありません。また、無線 LAN クライアントには、ビーコンに含まれる SSID 情報を必要とするものもあり、SSID 情報をアドバタイズしない無線 LAN との確実なアソシエーションを確保できません。これらの理由により、SSID 情報をビーコンに含んでブロードキャストするのが最善です。

アソシエーション - 接続プロセス

高速ローミングを除いて、802.11 クライアントは、無線 LAN ネットワーク上にデータを送信する前に次の 3 段階のプロセスを踏む必要があります。

1. 適切な無線 LAN ネットワークを見つける：企業での展開の場合、適切なネットワークの検索で、複数のチャネルにプローブ要求を送信し、ネットワーク名（SSID）、ビット レート要件、および必要なセキュリティ設定を指定する必要があります。
2. 802.11 認証：802.11 は、オープン認証および共有キー認証の 2 種類の認証メカニズムをサポートしています。オープン認証は、基本的にヌル認証であり、クライアントが認証要求を送信すれば、アクセス ポイントは必ず認証応答（許可）を返します。802.11 共有 WEP キー認証の実装には欠点がありますが、規格に適合するためには実装する必要があります。共有キー認証は推奨されていませんので、使用しないでください。

   オープン認証が、企業向けの無線 LAN 展開で使用される唯一のメカニズムです。前述のとおり、オープン認証は基本的にヌル認証であるため、802.1X および EAP 認証メカニズムによるアソシエーションの後で、実際の認証が発生します。
3. 802.11 アソシエーション：この段階では、セキュリティ オプションおよびビット レート オプションを確定し、無線 LAN クライアントとアクセス ポイント間のデータリンクを確立します。セキュリティで保護された企業向けの無線 LAN アクセス ポイントは、802.1X 認証が成功するまで、すべての無線 LAN クライアント トラフィックをアクセス ポイントでブロックします。クライアントがネットワークに接続し、あるアクセス ポイントから別のネットワークにローミ

ングする場合、そのアソシエーションは*再アソシエーション*と呼ばれます。アソシエーションと再アソシエーションの主な違いは、再アソシエーションでは、新しいネットワークにローミング情報を提供するために、以前のアクセス ポイントの基本 MAC アドレス（BSSID）を再アソシエーション要求に格納して送信することです。

プローブ要求およびプローブ応答

無線 LAN ネットワークに SSC を設定できます。これにより、無線 LAN クライアントは、目的の無線 LAN ネットワークの SSID を含んだプローブ要求を送信できるようになります。

無線 LAN クライアントが利用可能な無線 LAN ネットワークの検出を試みている場合には、SSID を含めないでプローブ要求を送信することもできます。この場合、このタイプのクエリーに応答するように設定されたすべてのアクセス ポイントが、プローブ応答を送信します。ブロードキャスト SSID がイネーブルになっていない無線 LAN は応答しません。

アソシエーション

アソシエーション フレームおよびアソシエーション応答フレームは、データ レートおよびセキュリティの設定に対して最終的な許可を提供します。このプロセスが完了すると、無線 LAN クライアントと無線 LAN アクセス ポイント間で 802.11 データ フレームの送信が可能になります。企業向け無線 LAN の展開では、802.1X 認証または EAP 認証が完了および成功するまでは、これらのデータ フレームは無線 LAN クライアントとアクセス ポイント間の 802.1X フレームに限定されます。

また、このアソシエーション プロセスには、無線 LAN クライアントをそのアクセス ポイントから接続解除するために使用される、関連するアソシエーション解除フレームがあります。アソシエーション解除フレームは、必ずユニキャスト フレームです。

再アソシエーション

再アソシエーションは、無線クライアントが一時的にアクセス ポイントの範囲外に移動、または別のアクセス ポイントにローミングする場合に発生します。再アソシエーション プロセスは、アソシエーション プロセスと似ていますが、ローミングが行われるときに新しいアクセス ポイントと以前のアクセス ポイントが有線ネットワーク上で通信し、無線クライアント情報をやり取りする点で異なります。

無線クライアントが新しいアクセス ポイントにローミングするときに、クライアントが新しいロケーションに移動したことを 802.11 ネットワークに知らせるために、再アソシエーション プロセスが使用されます。無線クライアントは、再アソシエーション フレームを新しいアクセス ポイントに発行し、新しいアクセス ポイントは、以前のアクセス ポイントを特定します。新しいアクセス ポイントは以前のアクセス ポイントと有線リンクで通信し、無線クライアントが前回アソシエートされていたことを確認します。無線クライアントが前回アソシエートされていた場合、新しいアクセス ポイントは無線クライアントに再アソシエーション応答フレームを発行します。アソシエートされていなかった場合には、アソシエーション解除フレームを発行します。再アソシエーション応答の送信後、新しいアクセス ポイントは以前のアクセス ポイントと有線リンクで通信し、再アソシエーション プロセスを完了します。以前のアクセス ポイントでバッファされていたフレームは、新しいアクセス ポイントにすべて転送されます。再アソシエーション プロセスが完了すると、新しいアクセス ポイントは、無線クライアントからのフレームの処理を開始します。

認証

前述のとおり、802.11 認証モードにはオープン モードと共有モードの 2 つのモードがあります。802.11 認証は、単独ではセキュリティ効果が低く、ネットワーク セキュリティがあまり問題にならないホーム無線ネットワークで主に使用されます。802.1X 用に設定されていないアクセス ポイントを使用して企業ネットワークに接続する必要のあるホーム ユーザは、SSC を使用して VPN 接続を確立する必要があります。VPN の詳細については、「VPN 統合」の項（P.2-32）を参照してください。

認証フレームに関連するもう 1 つのフレーム タイプは、認証解除フレームです。無線 LAN クライアントが認証解除フレームを受信した場合、そのクライアントはアクセス ポイントから接続解除されます。この場合、無線 LAN クライアントは、もう一度最初からプローブ要求プロセスをやり直すか、認証アソシエーション プロセスをやり直さなければならない場合があります。認証解除フレームは、ブロードキャスト MAC アドレス宛てに送信できます。

無線ネットワーク セキュリティの概念

セキュリティは、ネットワーク設計コンポーネントの 1 つと見なし、後から付け加えるのではなく、最初から組み込んでおく必要があります。また、セキュリティは、他のネットワーク コンポーネントと同じ費用便益分析およびユーザビリティの検討が必要です。

企業セキュリティの説明では、無線 LAN の RF 信号は、通常、展開されたビルディングの境界を越えた範囲に届くということが一貫して示されています。これにより、外部からのネットワークの監視および攻撃を受ける危険性があります。しかし、このタイプの攻撃は非常に限られています。どのような攻撃を実行するにも、適切な技能を備えた攻撃者が、無線 LAN に物理的に近接した場所で作業を行う必要があります。このため、攻撃者は適切な無線 LAN を探して広範囲のエリアをローミングしなければなりません。アクセス コントロール用の 802.1X フレームワークと他の無線環境管理ツールを組み合せることにより、このような攻撃の可能性を厳しく制限できます。企業のロケーションおよびその企業が運営するビジネス タイプにより、ネイティブの無線 LAN セキュリティへの推奨される増強方法が決まります。

物理的セキュリティ

どのようなネットワークにも、敵対行為が加えられる可能性はあります。敵対行為は、大まかに次のように分類できます。

- 機密情報収集：一般に、企業リソースへの不正アクセスに役立てられますが、重要な個人や事業のロケーションを確認するためなど、他の理由を目的とすることもあります。認証およびサプリカントの設定で使用される EAP タイプの選択で、認証中にユーザ名情報が漏えいする可能性が決まります。
- 不正アクセス：802.11 セキュリティでの認証および暗号化により、セッションを保護できますが、機器やパスワードの盗難を保護するポリシーやプロセスを適切に配備する必要があります。これには通常、次の 2 つの方法で対処します。
  - エンドノード セキュリティ。無線 LAN に直接関連付けられていないモバイル デバイスを保護します。このタイプのセキュリティは、エンドノードのモビリティを理解して評価される必要があります。
  - WPA または WPA2。無線 LAN クライアントに採用します。ユーザ認証機能や無線 LAN 上のユーザ通信の機密保持を提供します。
- サービス拒絶：正規のユーザがネットワーク上の情報やサービスにアクセスするのを妨害する無線 LAN ネットワーク攻撃です。この攻撃は通常、802.11 管理フレーム、または無線 LAN ネットワークと同じスペクトラムでの電波干渉を利用します。このタイプの攻撃には、RF 管理および 無線 IDS 機能（WIDS）で対処します。

規制、規格、および業界認証

ネットワーク システム規格のほとんどは、通常、Institute of Electrical and Electronic Engineers（IEEE; 米国電気電子学会）および Internet Engineering Task Force（IETF; インターネット技術特別調査委員会）によって策定されたものです。安全な無線 LAN 展開において導入された 2 つの中心的な規格が、IEEE が定めた 802.11 規格と、IETF が定めた EAP 規格です。

IEEE

IEEE は、一連の 802.11 規格シリーズを定めている団体です。最初の 802.11 規格は 1999 年に策定され、その後、多くの修正が加えられてきました。これらの修正では、さまざまな物理レイヤの実装が追加され、より高いビット レート（802.11b、802.11a、および 802.11g）、Quality of Service（QoS）の拡張（802.11e）、およびセキュリティの強化（802.11i）が実現されました。

また、IEEE は、ポート セキュリティのための 802.1X 規格も定めており、802.11i において無線 LAN クライアントの認証に使用されます。

IETF

IETF の主な Request For Comments（RFC; コメント要求）および無線 LAN に関連する草案は、Extensible Authentication Protocol（EAP; 拡張認証プロトコル）に基づいています。EAP の利点は、認証プロトコルをその転送メカニズムから分離することです。EAP は、802.1X フレーム、PPP フレーム、UDP パケット、および RADIUS パケットで送信可能です。

EAP は、無線 LAN 上で 802.1X フレームに含まれ、アクセス ポイントと AAA サーバ間で RADIUS パケットに含まれて送信されます。これは、無線 LAN クライアントと AAA サーバ間で、エンドツーエンドの EAP 認証を提供します。「EAP」の項（P.1-9）を参照してください。

Wi-Fi 構成

有線ネットワークでは、デバイスは同じベンダーのものが使用されるのが一般的で、統合は製品試験の一部です。異なるベンダー製のデバイスを同じネットワークで組み合わせて使用すると、使用するデバイスおよびその相互作用を理解したネットワーク専門家のグループによる、相互運用性および統合性の管理および制御が必要になります。

多くのベンダー製のデバイスを含む無線ネットワークでは、複数の無線規格によりさまざまな解釈およびオプション機能を展開することが可能でした。そこで、業界の企業および団体のグループは、Wi-Fi Alliance（www.wi-fi.org）を設立し、WPA、WPA2、および Wi-Fi Multimedia（WMM）認証プログラムによる無線 LAN の相互運用性の認証を開始しました。

WPA 規格は、802.11i ワーク グループの規格の承認に先立って WEP 暗号化プロセスの脆弱性に対処するために策定されました。策定の主な目的の 1 つは、WEP 対応機器への下位互換性を保つことでした。ここでは、WEP で使用される基本の RC4 暗号化のサポートを継続することを可能とする一方で、WEP 暗号化の脆弱性に対処するキーの生成手順の改良、およびメッセージ整合性チェックの改善が加えられています。

WPA2 は、批准された 802.11i 規格に基づいており、AES-CCMP 暗号化を使用します。この暗号化では、クライアントおよびアクセス ポイントのハードウェアを新しく用意する必要があります。ラップトップおよびクライアント デバイスのアップグレード サイクルが長いため、WPA および WPA2 が混在する環境はしばらくの間は続くと考えられます。無線 LAN をまだ導入していない（既存の実装環境による制約がない）企業での展開では、最初から WPA2 を使用できると想定されます。

Cisco Compatible Extensions

Cisco Compatible ExtensionsCCX プログラムは、シスコの無線 LAN インフラストラクチャと互換性があり、セキュリティ、モビリティ、Quality of Service、およびネットワーク管理を強化するためのシスコの技術革新を利用した、無線クライアント デバイスの幅広い可用性を確保します。

IEEE 802.1X

IEEE 802.1X は、ポート ベースのアクセス コントロールを行うための IEEE 規格のフレームワークです。無線 LAN ネットワークへの認証済みのアクセスを提供する手段として、802.11i セキュリティ ワーク グループによって採択されました。

- 802.11 アソシエーション プロセスは、アクセス ポイントに無線 LAN クライアント用の仮想ポートを作成します。
- アクセス ポイントは、802.1X トラフィック以外のすべてのデータ フレームをブロックします。
- 802.1X フレームは EAP 認証パケットを送信し、それらのパケットはアクセス ポイントによって AAA サーバに転送されます。
- EAP 認証が成功の場合、AAA サーバは EAP 成功メッセージをアクセス ポイントに送信します。そうすると、アクセス ポイントは、仮想 ポートを介した無線 LAN クライアントからのデータ トラフィックの送信を許可します。
- 仮想ポートを開く前に、データ リンク暗号化が無線 LAN クライアントおよびアクセス ポイント間で確立されます。これにより、他の無線 LAN クライアントが認証済みクライアント用に開かれたポートにアクセスできないようにします。

EAP

EAP は IEFT の RFC の 1 つです。認証プロトコルがそれを送信する転送プロトコルから分離するという要求に対処しています。これにより、認証プロトコルを変更することなく、802.1X、UDP、または RADIUS などの転送プロトコルによって EAP プロトコルを送信することが可能になります。

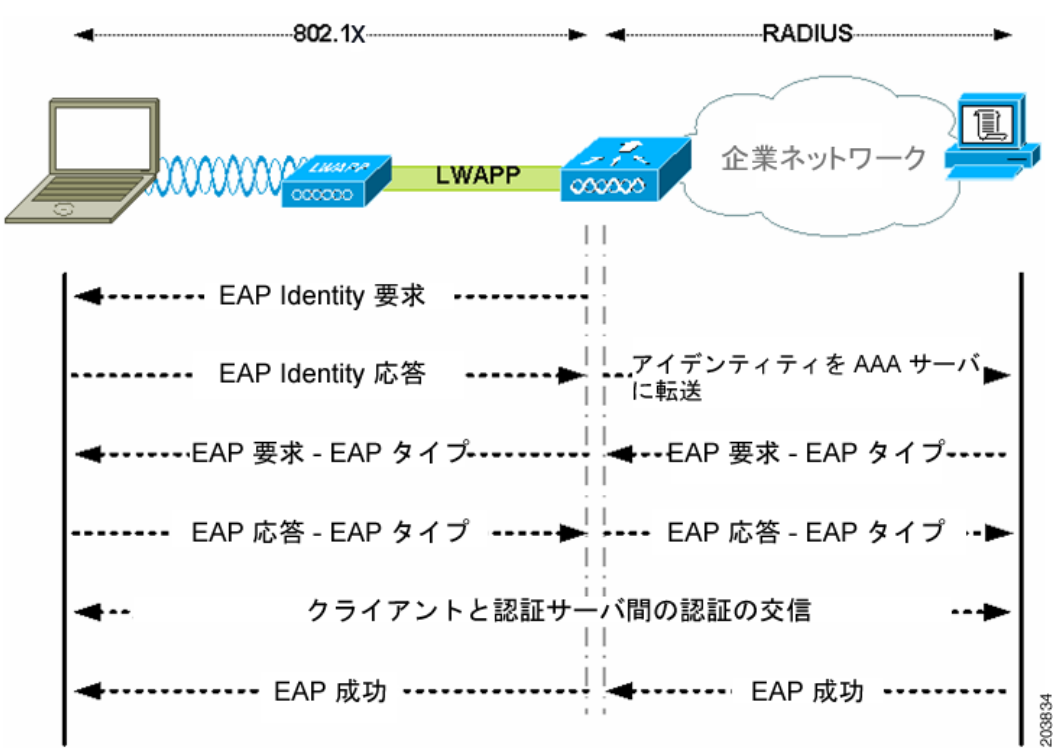
基本的な EAP プロトコルは比較的単純で、次の 4 つのパケット タイプで構成されます。

- EAP 要求：オーセンティケータがサプリカントに要求パケットを送信します。それぞれの要求には、サプリカントの識別情報や使用される EAP タイプなどの要求内容を示すタイプ フィールドが含まれます。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、EAP 応答とそれぞれの EAP 要求を照合できます。
- EAP 応答：サプリカントは応答パケットをオーセンティケータに送信し、元の EAP 要求と照合するためにシーケンス番号を使用します。EAP 応答のタイプは、応答が NAK（否定応答）でない限り、通常 EAP 要求と一致します。
- EAP 成功：認証成功の場合、オーセンティケータは成功パケットをサプリカントに送信します。
- EAP 失敗：認証失敗の場合、オーセンティケータは失敗パケットをサプリカントに送信します。

EAP が 802.11i システムで使用されている場合、アクセス ポイントは EAP パススルー モードで動作します。このモードでは、アクセス ポイントはコード、ID、および長フィールドを確認し、次にサプリカントから受信した EAP パケットを AAA サーバに転送します。オーセンティケータで AAA サーバから受信したパケットは、サプリカントに転送されます。

図 1-2 は、EAP プロトコルでやり取りされるメッセージを示しています。

図 1-2　EAP プロトコルのフロー



EAP-FAST

EAP-FAST は、シスコの専用 802.1X 認証タイプであり、柔軟で簡単な展開および管理を提供し、さまざまなユーザおよびパスワード データベースのタイプをサポートするとともに、サーバによって実行されるパスワードの失効および変更、ならびにデジタル証明書（オプション）をサポートしています。

EAP-FAST は、証明書を使用せず、辞書攻撃からの保護を提供する、802.1X EAP タイプの展開を検討しているお客様のために開発されました。

EAP-FAST は、EAP 内に TLS メッセージを カプセル化します。そのプロトコルは次の 3 つのフェーズで構成されています。

1. プロビジョニング フェーズ。Authenticated Diffie-Hellman Protocol（ADHP）を使用して、Protected Access Credential（PAC）と呼ばれる共有秘密クレデンシャルでクライアントをプロビジョニングします。
2. トンネル確立フェーズ。このフェーズでは、PAC を使用してトンネルを確立します。
3. 認証フェーズ。このフェーズでは、認証サーバがユーザのクレデンシャル（トークン、ユーザ名 / パスワード、またはデジタル証明書）を認証します。

EAP-TLS

EAP-Transport Level SecurityEAP-TLS は、TLS プロトコル（RFC 2246）に基づいた 802.1X EAP 認証アルゴリズムです。TLS は、X.509 デジタル証明書に基づいた相互認証を使用します。EAP-TLS メッセージ交換により、相互認証、暗号スイートのネゴシエーション、ならびにクライアントと認証サーバ間の秘密鍵の交換および検証を提供します。

下記のリストは、EAP-TLS クライアント証明書の使用が、無線接続の強化認証を提供する主な理由を示しています。

- 認証は自動で行われ、通常、ユーザの操作は必要ありません。
- ユーザ パスワードに依存する必要がありません。
- 認証保護の強化のためにデジタル証明書を使用します。
- 公開鍵の暗号化で、メッセージ交換が保護されます。
- 辞書攻撃に対応しています。
- 認証プロセスでは、最終的にデータを暗号化して署名を作るための、相互に取り決められたキーが使用されます。

EAP-TTLS

EAP-Tunnelled Transport Layer Security（EAP-TTLS）は、2 つのフェーズから構成されるプロトコルで、EAP-TLS の機能を拡張しています。フェーズ 1 では、完全な TLS セッションを実行し、フェーズ 2 で使用される セッション キーを導出して、サーバおよびクライアント間で安全にアトリビュートをトンネルします。フェーズ 2 でトンネルされたアトリビュートは、多くの異なるメカニズムを使用する追加認証を実行するために使用できます。

フェーズ 2 で使用できる認証メカニズムには、次のプロトコルが含まれます。

- PAP（パスワード認証プロトコル）: 2 方向ハンドシェイクを使用して、ピアが最初のリンク確立時にアイデンティティを確立するための簡単な方式を提供します。認証が承認されるまで、または接続が終了するまで、ピアは ID/ パスワードのペアをオーセンティケータに繰り返し送信します。
- CHAP（チャレンジ ハンドシェーク認証プロトコル）: 3 方向ハンドシェイクを使用して定期的にピアのアイデンティティを確認します。

- MS-CHAP（Microsoft CHAP）：3 方向ハンドシェイクを使用して定期的にピアのアイデンティティを確認します。
- MS-CHAPv2：応答パケットにピア チャレンジ、成功パケットにオーセンティケータ応答を含むことにより、ピア間の相互認証を提供します。
- EAP 次の EAP 方式の使用を可能にします。
  - EAP MD5（EAP メッセージ ダイジェスト 5）：EAP-MD5 は、EAP セキュリティ アルゴリズムで、128 ビットの生成された数字文字列、またはハッシュを使用して、データ パケットの信頼性を確認します。
  - EAP MSCHAPv2：3 方向ハンドシェイクを使用して定期的にピアのアイデンティティを確認します。

EAP-PEAP

EAP-PEAP は、802.1X EAP 認証タイプの 1 つです。サーバ側の EAP-TLS を利用し、証明書、トークン、ログイン パスワード、およびワンタイム パスワード（OTP）などの、さまざまな異なる認証方式をサポートしています。

EAP-PEAP は、次のサービスを提供することによって EAP 方式を保護します。

- EAP パケット用の TLS トンネルの作成
- メッセージ認証
- メッセージ暗号化
- クライアントへのサーバの認証
- 鍵交換によるダイナミック WEP キーまたは TKIP キーの確立

これらの認証メカニズムは、以下で使用できます。

- パスワード
  - EAP MSCHAPv2：3 方向ハンドシェイクを使用して定期的にピアのアイデンティティを確認します。
  - EAP GTC（EAP Generic Token Card）：EAP エンベロープを定義して、ユーザ パスワードを送信します。
- トークン
  - EAP GTC：EAP エンベロープを定義して、トークン カード生成のユーザ OTP を送信します。
- 証明書
  - EAP TLS：EAP エンベロープを定義して、ユーザ証明書を送信します。

認証

お客様の要望に応じて安全なモビリティ環境でさまざまな認証メカニズムをご使用いただけますが、すべてのメカニズムはサポート プロトコルとして 802.1X、EAP、および RADIUS を使用します。これらのプロトコルを使用することにより、ユーザは無線 LAN の正常な認証に基づいてアクセスを制御し、LAN ネットワークを認証できます。

また、このシステムは、AAA の他の要素である許可およびアカウンティングを、RADIUS および RADIUS アカウンティングを介してやり取りされるポリシーによって提供しています。

認証を実行するメカニズムの詳細は以降の項で説明しますが、認証プロトコルの選択に影響する主な要素は、既存のクライアント認証データベースとの統合です。ユーザは認証システムを新たに構築することなく、安全な無線 LAN を展開できる必要があります。

サプリカント

802.1X 認証に使用されるソフトウェア クライアントは、通常、802.1X の用語に基づいて *サプリカント*と呼ばれます。SSC は有線および無線ネットワーク用のサプリカントです。お客様のさまざまな認証システムへの要望に適切にマップする、多くの異なる EAP 方式をサポートしています。SSC がサポートする一般的な EAP 方式は、次のとおりです。

- Protected EAP（PEAP）MSCHAPv2：Transport Layer Security（TLS）トンネルを使用して、無線 LAN クライアントと認証サーバ間のカプセル化された MSCHAPv2 の送受信を保護します。
- PEAP GTC（Generic Token Card）：TLS トンネルを使用して、Generic Token Card の送受信を保護します。
- EAP-Flexible Authentication via Secured Tunnel（FAST）：トンネルを使用して送受信を保護します。
- EAP-TLS：X.509 デジタル証明書に基づいた相互認証を使用します。

表 1-1 は、一般的な EAP メソッドの要約を示しています。

表 1-1　Cisco SSC と EAP 方式の機能比較

機能	Cisco EAP-FAST	PEAP MS-CHAP v2	PEAP EAP-GTC	EAP-TLS
シングル サインオン（Microsoft Active Directory のみ）	あり	あり	あり	あり
ログイン スクリプト（Microsoft Active Directory のみ）	あり	あり	一部	あり
パスワード変更（Microsoft Active Directory のみ）	あり	あり	あり	–
Microsoft Active Directory データベース サポート	あり	あり	あり	あり
Access Control ServerACS ローカル データベース サポート	あり	あり	あり	あり
Lightweight Directory Access ProtocolLDAP データベース サポート	なし	なし	あり	あり
ワンタイム パスワード（OTP）認証サポート	なし	なし	あり	なし
RADIUS サーバ証明書の必要性	あり	あり	あり	あり
クライアント証明書の必要性	なし	なし	なし	あり
匿名性	あり	あり	あり	なし

オーセンティケータ

Cisco Secure Mobility Solution のオーセンティケータは、無線 LAN アクセス ポイントからの着信 802.1X フレームを処理する WLC であり、EAP パススルー モードで動作して、EAP パケットを 802.1X フレームから RADIUS パケットへ、RADIUS パケットから 802.1X フレームへとリレーします。

認証が成功すると、WLC は EAP 成功メッセージ、EAP 認証時に認証 サーバで生成された暗号キー、および通信ポリシーのための RADIUS 拡張を含む RADIUS パケットを受信します。

認証プロセス全体におけるオーセンティケータの位置については、図 1-1 を参照してください。オーセンティケータは、802.1X メカニズムによってネットワーク アクセスを制御し、サプリカントと認証サーバ間で EAP メッセージをリレーします。

認証サーバ

Cisco Secure Mobility Solution で使用される認証サーバは、Cisco Access Control Server（ACS）です。Cisco ACS は、Windows 2000 または 2003 サーバ上にインストール可能な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。また、認証サーバを、無線 LAN インフラストラクチャ デバイスに組み込むこともできます。たとえば、Cisco IOS ソフトウェアを実行するアクセス ポイント上のローカル認証サービス、または Cisco WLSExpress に含まれる AAA サービスなどが当てはまります。

認証サーバは、RADIUS トンネル上で EAP 認証を実行します。

EAP 認証が成功すると、認証サーバは EAP 成功メッセージをオーセンティケータに送信します。このメッセージは、オーセンティケータに EAP 認証プロセスが成功したことを通知し、Pairwise Master Key を渡します。マスター キーは、無線 LAN クライアントとアクセス ポイント間の暗号化ストリームを作成します。

暗号化

802.11i では、WPA および WPA2 の 2 つの企業レベル暗号化メカニズムが規定されています。これらの暗号化タイプは、Temporal Key Integrity Protocol（TKIP）および Advanced Encryption Standard（AES）です。

TKIP は WPA で認証されている暗号化で、中心的な暗号化アルゴリズム（RC4）のサポートを継続する一方で、WEP の欠点に対処することによって、従来の無線 LAN 機器へのサポートを提供します。クライアント デバイスのハードウェア リフレッシュ サイクルを考えると、TKIP が一般的な暗号化メカニズムとしてしばらくの間は使用される可能性が高いと考えられます。TKIP は、WEP の既知の脆弱性にすべて対処していますが、WPA2 の AES 暗号化は、従来の暗号化のベスト プラクティスと無線 LAN 暗号化を調和させることができるため、推奨される暗号化メカニズムです。

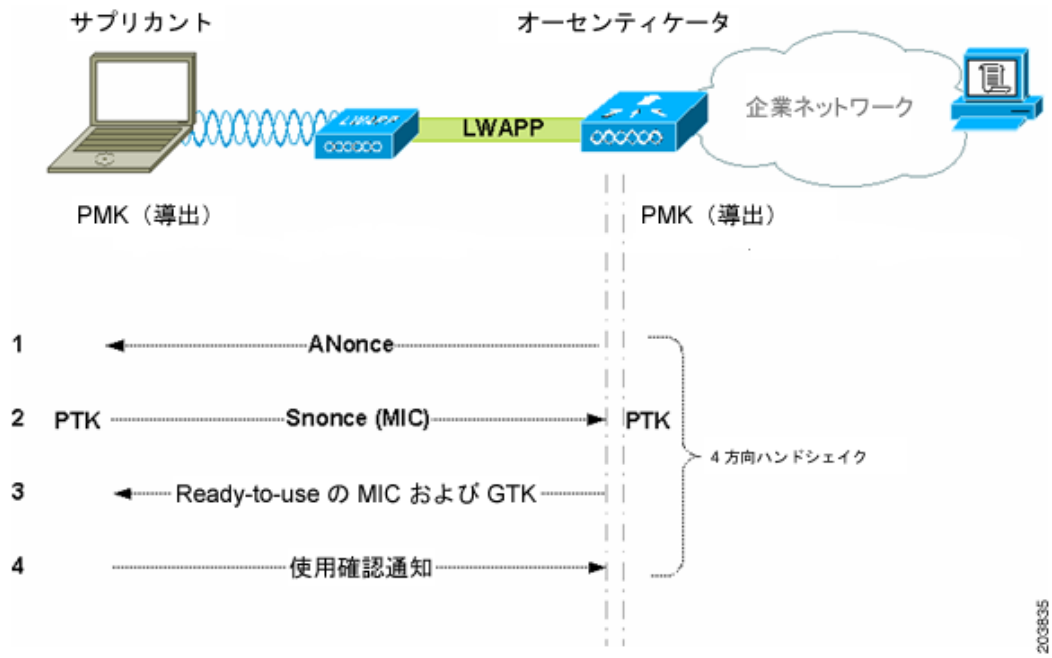
TKIP の 2 つの主なメカニズムは、MSDU（MAC Service Data Unit）の RC4 暗号化用のパケットごとのキー生成、および追加された暗号化パケットの Message Integrity Check（MIC）です。

AES Counter Mode/CBC MAC Protocol（CCMP）は、802.11i で使用される AES 暗号化モードで、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します。

4 方向ハンドシェイク

4 方向ハンドシェイクは、無線データ フレームの暗号化のための暗号キーの導出に使用されるメカニズムを表します。図 1-3 は、暗号キーを生成するために使用されるフレーム交換の概略図です。これらのキーは*一時*キーと呼ばれます。

図 1-3　4 方向ハンドシェイク



暗号化に使用されるキーは、EAP 認証セクションで相互に導出された Pairwise Master Key（PMK）から導出されます。PMK は、オーセンティケータに送信されます。オーセンティケータに送信された PMK は、サプリカントには転送されません。サプリカントではすでに PMK のコピーを独自に導出しているためです。

4 方向ハンドシェイクは次のイベントで構成されています。

1. オーセンティケータは ANonce（Authenticator Nonce：オーセンティケータによって生成される乱数）を含む EAPOL-Key フレームを送信します。
   - サプリカントは、ANonce および SNonce（Supplicant Nonce：オーセンティケータによって導出される乱数）から Pairwise Temporal Key（PTK）を導出します。
2. サプリカントは、SNonce、再アソシエーション要求フレームからの RSN 情報要素、および Message Integrity Check（MIC）を含む EAPOL-Key フレームを送信します。
   - オーセンティケータは、ANonce および SNonce から PTK を導出し、EAPOLKey フレーム内の MIC を検証します。
3. オーセンティケータは、一時キーをインストールするかを決める ANonce、ビーコンまたはプローブ応答メッセージからの RSN 情報要素、および MIC、ならびにカプセル化された Group Temporal Key（GTK：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、EAPOL-Key フレームを送信し、一時キーをインストールしたことを通知します。

シームレスな接続

無線モビリティを達成するために、ネットワーク管理者はサイト調査を行って、企業構内に適切な無線カバレッジがあることを確認する必要があります。シスコは、バランスのとれた適切に設計された無線インフラストラクチャを実現するための、無線スペクトラム分析ツールおよびアプリケーションを提供しています。

企業ネットワーク インフラストラクチャは、有線および無線メディアの両方に基づいており、無線メディアはモビリティを提供し、有線メディアは多くの場合より高い速度とスループットを提供します。有線および無線接続の両方が、マップされたネットワーク ドライブの復元、ログイン スクリプトの実行、コンピュータのグループ ポリシー オブジェクト（GPO）およびユーザの GPO の実行、ならびに無線 LAN クライアント コンピュータへのログインまたはリブート時にネットワーク接続の必要なタスクの実行ができる必要があります。また、無線 LAN クライアントは、クライアントの停止または休止状態からの回復後に、接続を復元できる必要があります。

ほとんどの企業環境で、エンド ユーザは、ワークステーションを切り離したり、イーサネット ケーブルを取り外して会議室などの別の場所に移動する場合でも、ネットワークに接続できる必要があります。一般的な企業では、ユーザが移動中には接続を欠くことは許容されています。しかし、次の場所に到着すれば、簡単に接続を回復できる必要があります。他の企業では、ユーザが Voice-over-IP（VoIP）などの継続的な接続を必要とするアプリケーションを使用している場合には、移動中であっても接続を保つ必要がある場合もあります。無線ローミングは、無線ネットワーク インフラストラクチャでのこれらの問題に対処します。

ローミング

エンド ユーザは、次のことができる必要があります。

- 有線接続から無線接続に、またその逆に、簡単に切り替えできる。
- 信号強度の低いアクセス ポイントから、同じ SSID を持つより信号強度の高いアクセス ポイントにローミングできる。

別のアクセス ポイントにローミングするには、現在のアクセス ポイントとのアソシエーションを解除し、新しいアクセス ポイントとアソシエーションを確立する必要あります。このプロセスによって、特に 802.1X を必要とする企業では、既存のネットワーク接続を終了する必要が出てきます。ローミングは、802.1X 認証後に行われます。すべてのプロセスには、30 秒以上かかる場合があります。

EAP-TLS、EAP-FAST、または EAP-PEAP が、展開されている認証方式である場合、セッション再開により、802.1X 認証中の再接続時間が短縮されます。

セッション再開

一般的な EAP-TLS ハンドシェイクでは、EAP 成功メッセージが生成されるまでに、多くのパケット交換が行われます。その後、4 方向ハンドシェイクが実行され、暗号キーが確立されます。集中化されたバックエンド認証サーバを使用している場合には、セッション再開により、ユーザの前回の認証セッションからのセッション ステート情報を利用することによって、新しいアクセス ポイントにローミングする場合の認証ハンドシェイクが簡単になります。これにより、ハンドシェイク パケット交換の回数を減らすことができます。

しかし、この処理で再接続の時間を短縮することはできますが、これではまだ無線 LAN クライアント上で起動されている Voice-over-IPVoIP などのリアルタイム アプリケーションに対応できません。その再接続時間は 50 ～ 200 ミリ秒である必要があります。

無線ネットワークのフレームワークは、認証済みのクライアント デバイスが再アソシエーションに伴う遅延を認識することなく、あるアクセス ポイントから別のアクセス ポイントに安全にローミングできる高速セキュア ローミングをサポートしています。また、高速セキュアローミングは、無線 VoIP などの遅延に敏感なアプリケーションもサポートしています。

高速セキュア ローミング

高速ローミングは、リアルタイム データを処理する Wi-Fi アプリケーションを使用するハンドヘルド型のデバイスに最適です。高速ローミングを達成するための主な技術は、シスコの CCKM および 802.11i PMKID キャッシングの 2 つです。

両方のアプローチでは、無線インフラストラクチャが、隣接アクセス ポイントに対して、802.1X 認証から以前に導出された必要なキー関連情報を事前に確立します。

あるアクセス ポイントに接続すると、802.11i PMKID キャッシングにより、隣接アクセス ポイントのリストが無線 LAN クライアントに共有され、802.11i PMKID は、事前認証と呼ばれる 802.1X 認証を、他のアクセスポイントと無線 LAN クライアント間で現在の無線接続を介してトンネルします。無線 LAN クライアントが実際に別のアクセス ポイントにローミングするときに、隣接アクセス ポイントを検索し、適合する PMK を使用して、4 方向ハンドシェイクのみを行い、アソシエーション後の接続を確立します。

CCKM は、異なる方式を使用します。無線ネットワーク インフラストラクチャがシスコのアクセス ポイントに基づいている場合には、無線 LAN クライアントは事前認証および 4 方向ハンドシェイクを省略でき、別のシスコ製アクセス ポイントへの再アソシエーション時に高速ローミングを達成できます。