認証タイプの設定

この章では、アクセス ポイントに認証タイプを設定する方法について説明します。

認証タイプの概要

この項ではアクセス ポイントに設定できる認証タイプについて詳しく説明します。認証タイプはアクセス ポイントに設定する Service Set Identifier（SSID; サービス セット ID）に関連付けられます。認証タイプが関連付けられた SSID は、有効な暗号化メカニズムが設定された VLAN または無線インターフェイスに関連付けられます。したがって、SSID に設定する認証方式が、SSID が関連付けられている VLAN または無線インターフェイスに設定されている暗号化方式と互換性を持っていることを確認してください。

詳細については、第 10 章「認証および暗号化メカニズムについて」の項を参照してください。同じアクセス ポイントで異なるタイプのクライアント デバイスを使用する場合は、複数の SSID を設定します。複数の SSID の設定手順の詳細は、第 7 章「複数の SSID の設定」を参照してください。

無線クライアント デバイスがアクセス ポイントを介してネットワークで通信を行うには、Open または Shared キー認証を使用してアクセス ポイントから認証を得る必要があります。最大限のセキュリティを確保するには、MAC アドレス認証または EAP 認証を使用して、ネットワークに対してクライアント デバイスを認証する必要もあります。MAC アドレス認証と EAP 認証は、いずれもネットワーク上の認証サーバに依存します。

認証サーバは AP に設定することも、外部サーバに設定することもできます。クライアント認証プロセスは、次のように設定できます。

1. クライアントの認証は、アクセス ポイントに対して行うことができます（公開キーまたは共有キーを使用）。
2. アソシエーション フェーズでは、オプションで、クライアントの MAC アドレスを使用してクライアントを認証できます。
3. AP とのアソシエーションが完了した後は、オプションで、RADIUS サーバに対してクライアントを認証できます。
4. 個々のクライアント キーの生成および管理には、EAP/802.1x.EAP/802.1x メカニズムを使用できます。

（注） デフォルトでは、アクセス ポイントは service-type 属性を authenticate-only に設定した再認証要求を認証サーバに送信します。ただし、Microsoft IAS サーバの中には、authenticate-only の service-type 属性をサポートしていないものがあります。ユーザの要件に応じて、service-type 属性を **dot11 aaa authentication attributes service-type login-user** または **dot11 aaa authentication attributes service-type framed-user** に設定してください。デフォルトでは、アクセス要求に応じてサービス タイプ「login」が送信されます。

アクセス ポイントは、複数の認証メカニズム（タイプ）を同時に使用することができます。次の項でそれぞれの認証タイプについて説明します。

- アクセス ポイントに対する Open 認証（11-2 ページ）
- アクセス ポイントに対する WEP Shared Key 認証（11-2 ページ）
- ネットワークに対する EAP 認証（11-3 ページ）
- ネットワークに対する MAC アドレス認証（11-5 ページ）
- MAC ベースの認証、EAP 認証、および Open 認証の組み合わせ（11-6 ページ）
- 認証されたクライアントの CCKM の利用（11-6 ページ）
- WPA キー管理の使用（11-7 ページ）

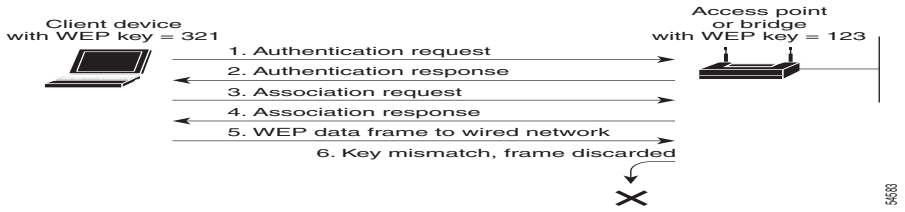
アクセス ポイントに対する Open 認証

Open 認証では、すべてのデバイスに認証およびアクセス ポイントとの通信の試みを許可します。Open 認証を使用すると、すべてのワイヤレス デバイスをアクセス ポイントで認証できます。Open 認証はネットワーク上の RADIUS サーバに依存しません。

Open 認証と WEP 暗号化を使用するシナリオでは、クライアントと AP の WEP が一致しなくても認証は成功します。Open 認証が完了した後は、クライアントはデータ（DHCP 要求を含む）を送信できません。ただし、Open 認証を使用し、暗号化を使用しない場合、ワイヤレス クライアントはアソシエーション フェーズが完了した直後からデータを送信できます。

図 11-1 は、認証を試みるデバイスと、Open 認証を使用しているアクセス ポイントとの認証シーケンスを示しています。この例では、デバイスの WEP キーがアクセス ポイントのキーと一致しないため、認証はできても、データを転送できません。

図 11-1　Open 認証のシーケンス



アクセス ポイントに対する WEP Shared Key 認証

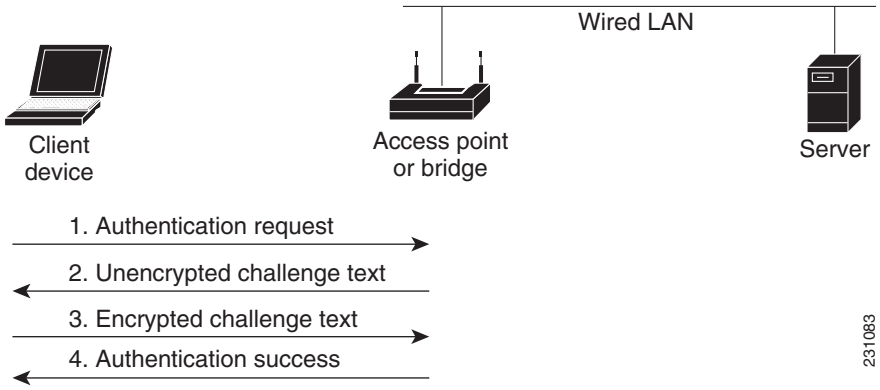
シスコでは、802.11 標準で規定されている WEP 認証に準拠するために、Shared Key 認証を提供しています。ただし、Shared Key のセキュリティ上の欠点により、WEP は非推奨となっています。IEEE およびシスコでは、WEP 認証を使用しないよう推奨しています。

Shared Key 認証では、アクセス ポイントが、アクセス ポイントとの通信を試みるすべてのデバイスに、暗号化されていない身元証明要求テキスト ストリングを送信します。認証を求めるデバイスは身元証明要求テキストを暗号化して、アクセス ポイントに返送します。身元証明要求テキストが正しく暗号化されていれば、アクセス ポイントはそのデバイスに認証を許可します。暗号化されていない身元証明要求も暗号化された身元証明要求もモニタできます。しかしそのために、アクセス ポイントは、暗号化前のテキストと暗号化後のテキストを比較して WEP キーを計算す

る不正侵入者の攻撃に対し、無防備な状態になります。このような弱点により、Shared Key 認証は Open 認証よりも安全性が劣る場合があります。Open 認証と同様に、Shared Key 認証ではネットワーク上の RADIUS サーバは使用されません。

図 11-2 は、認証を試みるデバイスと、Shared Key 認証を使用しているアクセス ポイントとの認証シーケンスを示しています。この例では、デバイスの WEP キーがアクセス ポイントのキーと一致しているため、認証を受けて通信できます。

図 11-2　Shared Key 認証のシーケンス



ネットワークに対する EAP 認証

この認証タイプは、無線ネットワークに最高レベルのセキュリティを提供します。拡張可能認証プロトコル（EAP）を使用して EAP 対応の RADIUS サーバと対話することにより、アクセス ポイントは、ワイヤレス クライアント デバイスと RADIUS サーバが相互認証を行って動的なユニキャスト キーを派生できるよう支援します。RADIUS サーバはこのキーをアクセス ポイントに送ります。アクセス ポイントはこのキーを、クライアントに対して送受信するすべてのユニキャスト データ信号に使用します。また、アクセス ポイントは、クライアントのユニキャスト キーを使用してブロードキャスト キーを暗号化し、その暗号化したブロードキャスト キーをクライアントに送信します。

このキーは、基礎となるセキュリティ フレームワーク（動的 WEP、WPA または WPA 2 による 802.1X）に応じて、次のように使用されます。

- WEP の場合：アクセス ポイントはこのキーを、クライアントとの間で送受信するすべてのユニキャスト データ信号に直接使用します。
- WPAv1/v2 の場合：このキーは、クライアントとの間で送受信するすべてのユニキャスト データ信号に使用するユニキャスト キーを派生させるために使用されます。

アクセス ポイントとクライアント デバイスで EAP を有効にすると、ネットワークに対する認証は、図 11-3 に示す手順で実行されます。

図 11-3　EAP 認証のシーケンス

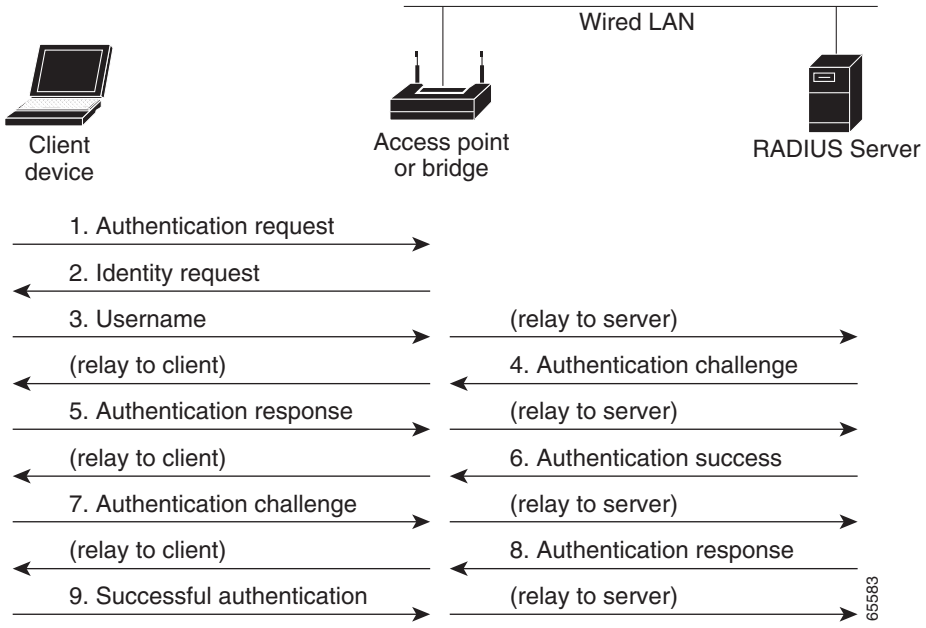


図 11-3 の手順 1 ～ 9 では、無線クライアント デバイスと有線 LAN 上の RADIUS サーバが 802.1x および EAP を使用して、アクセス ポイント経由で相互認証を実行します。RADIUS サーバは、認証身元証明要求をクライアントに送信します。クライアントはユーザまたはマシンによって提供されたクレデンシャルを一方向で暗号化して、認証身元証明要求に対する応答を生成し、その応答を RADIUS サーバに送信します。RADIUS サーバは、サーバ自体のユーザ データベースの情報から独自の応答を生成し、クライアントからの応答と比較します。RADIUS サーバがクライアントを認証すると、同じ処理が逆方向から繰り返され、今度はクライアントが RADIUS サーバを認証します。

相互認証が完了すると、RADIUS サーバとクライアントは、クライアントに固有の適切なレベルのネットワーク アクセスを提供する WEP キーまたは Pairwise Master Key（PMK）を決定します。これにより、有線のスイッチド セグメントのセキュリティ レベルは、デスクトップのレベルに近づきます。クライアントはこのキーをロードして、ログイン セッションでの使用に備えます。

ログイン セッション中に、RADIUS サーバは WEP キー（または WPAv1/v2 Pairwise Master Key）を暗号化し、有線 LAN 経由でアクセス ポイントに送信します。AP はこのキーを使用してブロードキャスト キーを暗号化し、暗号化後のブロードキャスト キーをクライアントに送信します。クライアントはこのブロードキャスト キーを同一のユニキャスト キーを使用して復号化します。クライアントとアクセス ポイントは暗号化を有効にし、ユニキャスト キーとブロードキャスト キーを残りのセッションの間、すべての通信に対して使用します。

EAP 認証には複数のタイプがありますが、アクセス ポイントはどのタイプについても同じように機能します。つまり、アクセス ポイントは、無線クライアント デバイスと RADIUS サーバ間の認証メッセージを中継します。アクセス ポイントで EAP を設定する方法の詳細は、「SSID への認証タイプの割り当て」セクション（11-9 ページ）を参照してください。

(注)　EAP 認証を使用する場合は、Open 認証または Shared Key 認証を選択できますが、この選択は必須ではありません。EAP 認証は、アクセス ポイントとネットワークの両方に対する認証を制御します。

ネットワークに対する MAC アドレス認証

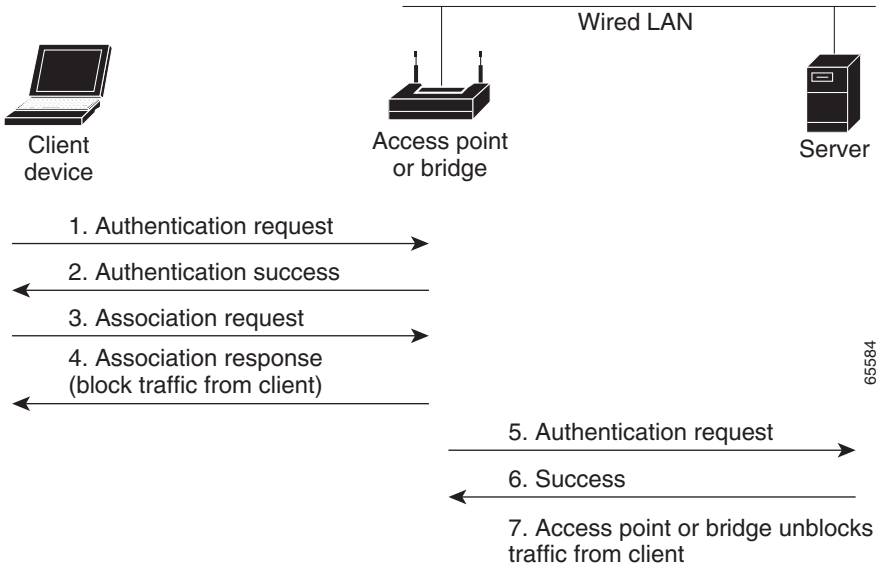
アクセス ポイントは、無線クライアント デバイスの MAC アドレスをネットワーク上の RADIUS サーバに中継します。サーバはそのアドレスを、許可される MAC アドレスのリストと照合します。MAC アドレスは不正侵入者でも偽造できるため、MAC ベースの認証は EAP 認証より安全性が劣ります。ただし、EAP 機能を持たないクライアント デバイスにとって、MAC ベースの認証は 1 つの代替認証方式となります。MAC ベースの認証の有効化の詳細は、「SSID への認証タイプの割り当て」セクション（11-9 ページ）を参照してください。

ヒント　ネットワークに RADIUS サーバがない場合は、許可される MAC アドレスのリストをアクセス ポイントの [Advanced Security: MAC Address Authentication] ページで作成できます。このリストにない MAC アドレスを持つデバイスは、認証されません。

ヒント　無線 LAN 上の MAC 認証クライアントが頻繁にローミングする場合、アクセス ポイント上で MAC 認証キャッシュを有効にすることができます。MAC 認証キャッシングを使用すると、アクセス ポイントは認証サーバに要求を送信することなく MAC アドレス キャッシュ内のデバイスを認証するため、オーバーヘッドが軽減されます。この機能を有効にする手順の詳細は、「MAC 認証キャッシングの設定」セクション（11-15 ページ）を参照してください。

図 11-4 は、MAC ベースの認証のシーケンスを示しています。

図 11-4　MAC ベースの認証のシーケンス



MAC ベースの認証、EAP 認証、および Open 認証の組み合わせ

MAC ベースの認証と EAP 認証を組み合わせてクライアント デバイスを認証するように、アクセス ポイントを設定できます。この機能を有効にした場合、まず、802.11 Open 認証を使用してアクセス ポイントにアソシエートするクライアント デバイスが MAC 認証を行います。MAC 認証が成功すると、クライアント デバイスはネットワークに接続されます。MAC 認証が失敗した場合、EAP 認証を行います。このような認証の組み合わせを設定する方法の詳細は、「SSID への認証タイプの割り当て」セクション（11-9 ページ）を参照してください。

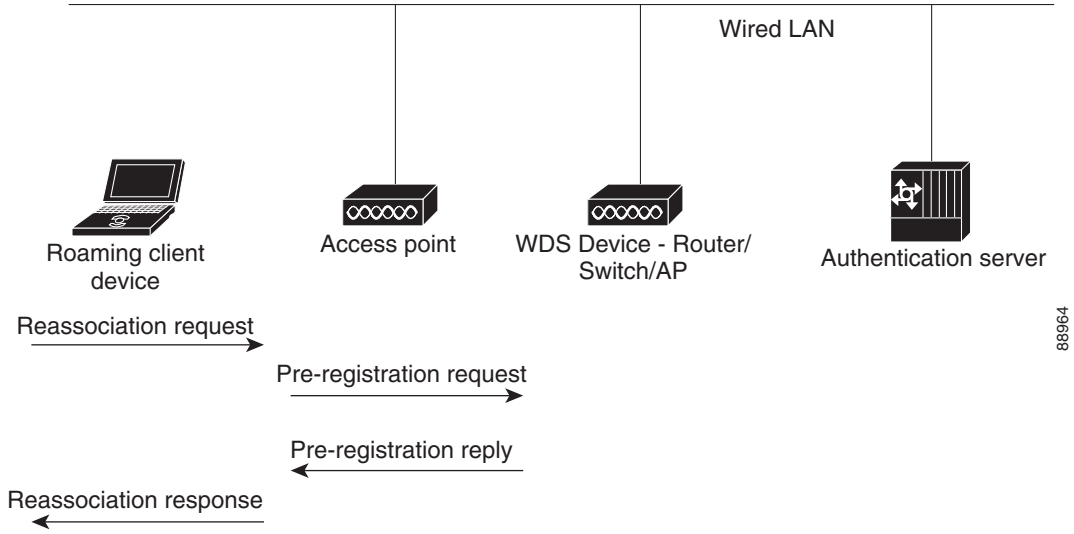
認証されたクライアントの CCKM の利用

Cisco Centralized Key Management（CCKM）を使うと、認証されたクライアント デバイスは、1 つのアクセス ポイントから別のアクセス ポイントへ、再アソシエーションの際にほとんど遅延することなくローミングできます。ネットワーク上のアクセス ポイントは、Wireless Domain Service（WDS; 無線ドメイン サービス）を提供し、サブネット上の CCKM 対応クライアント デバイスに対してセキュリティ クレデンシャルのキャッシュを生成します。WDS アクセス ポイントのクレデンシャルのキャッシュは、CCKM 対応クライアント デバイスが新しいアクセス ポイントにローミングする際、再アソシエーションに必要な時間を大幅に短縮します。クライアント デバイスがローミングすると、WDS アクセス ポイントがクライアントのセキュリティ クレデンシャルを新しいアクセス ポイントに転送し、再アソシエーション プロセスが短縮されて、ローミングするクライアントと新しいアクセス ポイント間での 2 つのパケット交換だけになります。ローミングするクライアントは非常にすばやく再アソシエートするため、音声やその他の時間に敏感なアプリケーションで、知覚できるほどの遅延は生じません。アクセス ポイントで CCKM を有効にする方法の詳細は、「SSID への認証タイプの割り当て」セクション（11-9 ページ）を参照してください。無線 LAN 上にある WDS アクセス ポイントの設定の詳細は、「アクセス ポイントを潜在的な WDS デバイスとして設定する」セクション（12-6 ページ）を参照してください。

（注）　RADIUS サーバによる VLAN 割り当て機能は、CCKM を利用した SSID グループのクライアント デバイスに対してはサポートされません。

図 11-5 は、CCKM を使用した再アソシエーション プロセスを示しています。

図 11-5　CCKM を使用したクライアント再アソシエーション



WPA キー管理の使用

WPAv1 は、802.11i 改訂の初期ドラフトに基づく Wi-Fi Alliance 認定です。WPAv1 ではデータ保護に TKIP（Temporal Key Integrity Protocol）を使用します。WPAv2 は、2004 年に発行された 802.11i の最終改訂に基づく Wi-Fi Alliance 認定です。WPAv2 では、AES（Advanced Encryption Standard）と Counter-Mode Cipher Block Chaining（CBC）Message Authentication Code（MAC）プロトコルを使用します。WPAv1 および WPAv2 はいずれも、ホーム タイプの導入には事前共有キー（PSK）を使用した認証を許可し、企業タイプの導入での認証キー管理には 802.1X の使用を許可します。

（注）　WPA では、TKIP の使用を推奨し、AES の使用を許可しています。WPA2 では、AES-CCMP の使用を推奨し、後方互換性を確保するために TKIP の使用を許可しています。シスコおよび Wi-Fi Alliance では、AES と WPAv1 または TKIP と WPAv2 を使用しないよう推奨しています。最も強力なセキュリティは、WPAv2 と AES-CCMP を使用することにより実現できます。クライアントが AES-CCMP で WPAv2 をサポートしていないネットワークでは、WPAv1 と TKIP を使用できます。

クライアントと認証サーバは、WPA（WPAv1 または WPAv2）キー管理を使用して EAP 認証方式で相互認証を行い、Pairwise Master Key（PMK）を生成します。サーバは WPA を使用し、PMK を動的に生成してアクセス ポイントに渡します。ただし、そのためには、WPA-PSK を使用してクライアントとアクセス ポイントの両方で事前共有キーを設定し、事前共有キーが PMK として使用されるように設定してください。

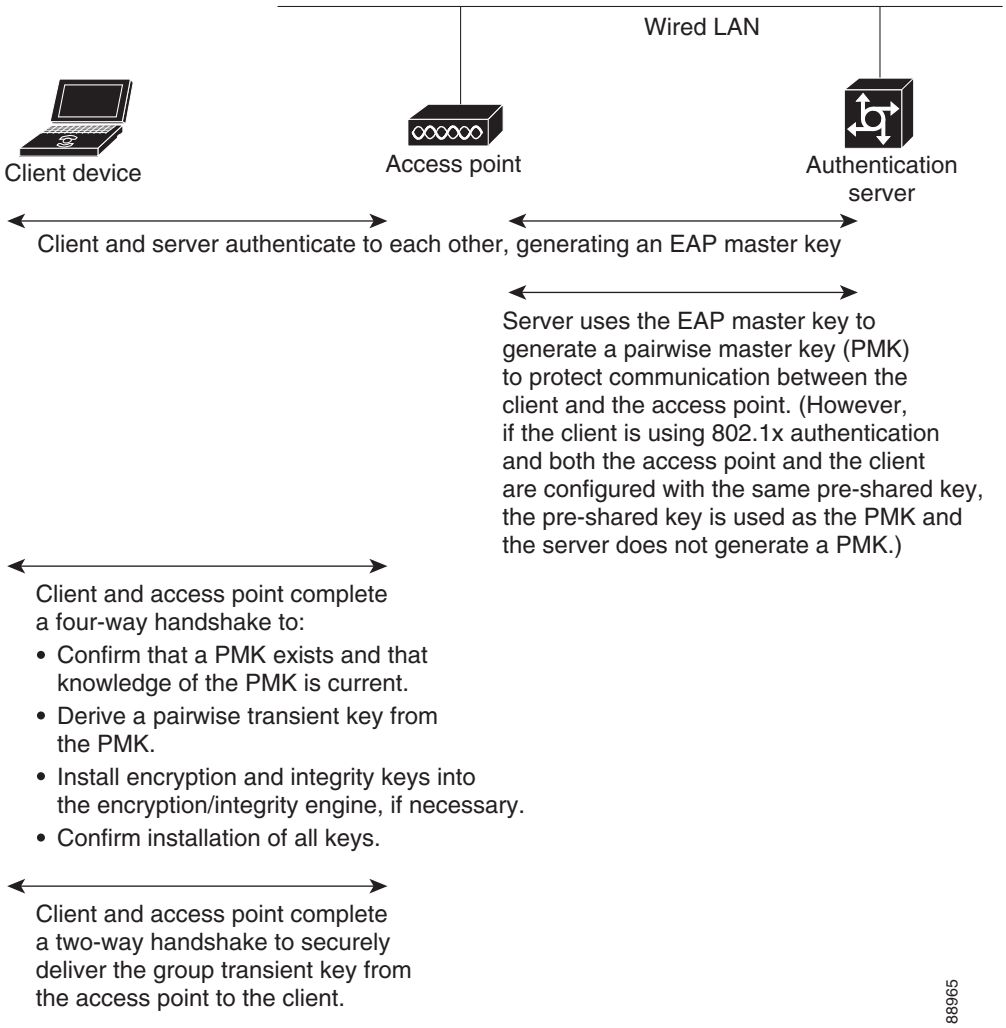
WPA キー管理は、WPA および WPA-Pre-Shared Key（WPA-PSK）の相互に排他的な 2 つの管理タイプをサポートしています。クライアントと認証サーバは、WPA を使用してキーを管理し、EAP 認証方式で相互認証を行い、Pairwise Master Key（PMK）を生成します。サーバは WPA を使用し、PMK を動的に生成してアクセス ポイントに渡します。ただし、そのためには、WPA-PSK を使用してクライアントとアクセス ポイントの両方で事前共有キーを設定し、事前共有キーが PMK として使用されるように設定してください。

(注)　WPA 情報エレメントでアドバタイズされる（さらに 802.11 でのアソシエーション中に決定される）ユニキャストとマルチキャストの暗号スイートは、明示的に割り当てられた VLAN でサポートされている暗号スイートと一致しない可能性があります。RADIUS サーバにより、以前決定された暗号スイートとは別の暗号スイートを使用する、新規の VLAN ID が割り当てられた場合、アクセス ポイントとクライアントは、この新たな暗号スイートに切り替えることができなくなります。現在、WPA プロトコルと CCKM プロトコルでは、最初の 802.11 暗号ネゴシエーション フェーズ以降での暗号スイートの変更は許可されていません。このような場合、クライアント デバイスと無線 LAN とのアソシエーションが解除されてしまいます。

WPA キー管理をアクセス ポイントで設定する方法の詳細は、「SSID への認証タイプの割り当て」セクション（11-9 ページ）を参照してください。

図 11-6 は、WPA キー管理プロセスを示しています。

図 11-6　WPA キー管理プロセス



認証タイプの設定

この項では、認証タイプを設定する方法について説明します。設定タイプはアクセス ポイントの SSID に割り当てます。複数の SSID の設定の詳細は、「複数の SSID の設定」セクション（7-2 ページ）を参照してください。ここでは、次の内容について説明します。

- SSID への認証タイプの割り当て（11-9 ページ）
- 認証のホールドオフ、タイムアウト、間隔の設定（11-16 ページ）
- 802.1X サプリカントの EAP 方式プロファイルの作成と適用（11-18 ページ）

SSID への認証タイプの割り当て

設定する SSID は、VLAN または無線インターフェイスにマッピングされます。したがって、SSID に定義する認証タイプが、SSID に関連付ける VLAN または無線インターフェイスに定義されている暗号化方式と互換性を持つことを確認してください。詳細については、第 10 章「認証および暗号化メカニズムについて」を参照してください。

特権 EXEC モードから、次の手順に従って SSID に認証タイプを設定します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**dot11 ssid** *ssid-string*	SSID を作成し、新しい SSID の SSID コンフィギュレーション モードを入力します。SSID には、最大 32 文字の英数字を使用できます。SSID では、大文字と小文字が区別されます。 一部のクライアントでは、SSID 文字列での特殊文字の使用をサポートしていません。シスコでは、SSID 文字列では文字 !、#、;、+、\、/、" を使用しないよう推奨しています。

	コマンド	目的
ステップ 3	**authentication open** [**mac-address** *list-name* [**alternate**]] [[**optional**] **eap** *list-name*]	(任意)この SSID の認証タイプを Open に設定します。Open 認証では、すべてのデバイスに認証およびアクセス ポイントとの通信の試みを許可します。 • (任意)SSID の認証タイプを MAC アドレス認証を使用する Open に設定します。アクセス ポイントは、すべてのクライアント デバイスに対して、ネットワーク接続を許可される前に MAC アドレス認証の実行を強制します。*list-name* には、認証方式リストを指定します。 • クライアント デバイスが MAC 認証か EAP 認証を使用してネットワークに接続するのを許可する場合は、**alternate** キーワードを使用します。いずれかの認証を得たクライアントはネットワークとの接続を許可されます。 • (任意)SSID の認証タイプを EAP 認証を使用する Open に設定します。アクセス ポイントは、すべてのクライアント デバイスに対して、ネットワーク接続を許可される前に EAP 認証の実行を強制します。*list-name* には、認証方式リストを指定します。 クライアント デバイスが Open 認証か EAP 認証を使用してアソシエートおよび認証されるのを許可する場合は、**optional** キーワードを使用します。この設定は、特殊なクライアント アクセシビリティを必要とするサービス プロバイダーが主に使用します。 (注)　EAP 認証が設定されたアクセス ポイントは、アソシエートするすべてのクライアント デバイスに対して EAP 認証の実行を強制します。EAP を使用しないクライアント デバイスはアクセス ポイントを使用できません。
ステップ 4	**authentication shared** [**mac-address** *list-name*] [**eap** *list-name*]	(任意)SSID の認証タイプを Shared Key に設定します。 (注)　WEP Shared Key にはセキュリティ上の欠陥があるため、使用しないことを推奨します。 • (任意)SSID の認証タイプを MAC アドレス認証を使用する Shared Key に設定します。list-name には、認証方式リストを指定します。 • (任意)SSID の認証タイプを EAP 認証を使用する Shared Key に設定します。list-name には、認証方式リストを指定します。このモードは、EAP に段階的に移行するネットワーク向けに設計されています。EAP をサポートするクライアントは個々のクライアント認証と個々のクライアント キー管理を使用する一方、静的 WEP のみをサポートするクライアントには、静的 WEP を使用したアソシエーションが許可されます。

	コマンド	目的
ステップ 5	**authentication network-eap** *list-name* [**mac-address** *list-name*]	（任意）SSID の認証タイプを Network-EAP に設定します。拡張認証プロトコル（EAP）を使用して、Cisco LEAP をサポートする EAP 互換の RADIUS サーバと対話することにより、アクセス ポイントは、無線クライアント デバイスと RADIUS サーバが相互認証を行って動的なユニキャスト WEP キーを派生できるよう支援します。 • （任意）SSID の認証タイプを MAC アドレス認証を使用する Network-EAP に設定します。アクセス ポイントにアソシエートするすべてのクライアント デバイスは、MAC アドレス認証の実行が要求されます。list-name には、認証方式リストを指定します。

	コマンド	目的
ステップ 6	**authentication key-management** { [**wpa** [**version** *versionnumber*]] | [**cckm**] } [**optional**]	(任意)SSID の認証タイプを WPA または CCKM、あるいはその両方に設定します。**optional** キーワードを指定すると、WPA(WPAv1 または WPAv2)および CCKM クライアント以外のクライアント デバイスもこの SSID を使用できます。**optional** キーワードを指定しない場合、この SSID を使用できるのは WPA(WPAv1 または WPAv2)または CCKM クライアント デバイスだけになります。 SSID で CCKM を有効にするには、EAP 認証(EAP および/または Network EAP による Open 認証)形式も有効にする必要があります。SSID で CCKM と EAP を有効にすると、LEAP、EAP-FAST、PEAP/GTC、MSPEAP、EAP-TLS、および EAP-FAST を使用するクライアント デバイスは、SSID を使用して認証を行うため、CCKM を使用した高速ローミングによるメリットがもたらされます。 (WPAv1 または WPAv2 による)SSID の WPA キー管理を有効にするには、(さらに MAC 認証を使用するかどうかに関係なく)EAP または Network EAP あるいはその両方による Open 認証も有効にする必要があります。この場合、個々のクライアント認証は EAP を使用して行われ、個々のクライアント Pairwise Master Key(PMK)が定義されます。あるいは、Open 認証を有効にして、WPA 事前共有キーを定義することもできます。この場合、AP およびワイヤレス クライアントは事前共有キーを Pairwise Master Key (PMK)として使用します。 **(注)** CLI から SSID に対して WPA と CCKM の両方を有効にする場合、最初に WPA を入力し、次に CCKM を入力する必要があります(ただし、Web UI では、単純に両方のオプションをオンにします)。WPA ではどのクライアントも認証を試行できますが、CCKM では音声クライアントだけが認証を試行できます。 **(注)** CCKM または WPA を有効にするには、SSID の VLAN に対する暗号化モードを、いずれかの暗号スイート オプションに設定する必要があります。VLAN 暗号化モードの設定方法の詳細は、第 10 章「暗号化モードの設定」を参照してください。 **(注)** 事前共有キーなしで SSID の WPA を有効にすると、キー管理タイプは WPA になります。事前共有キーを設定して SSID の WPA を有効にすると、キー管理タイプは WPA-PSK になります。事前共有キーの設定方法の詳細は、追加の WPA の設定を参照してください。 CCKM およびサブネット コンテキスト マネージャを使うように無線 LAN を設定する方法の詳細については第 12 章「その他のサービスの設定」を参照してください。 (任意)WPA を使用する場合は、サポートする WPA のバージョン(WPAv1 または WPAv2)を指定できます。

	コマンド	目的
ステップ 7	**end**	特権 EXEC モードに戻ります。
ステップ 8	**copy running-config startup-config**	(任意)コンフィギュレーション ファイルに設定を保存します。

SSID を無効にする場合、または SSID 機能を無効にする場合は、SSID コマンドの **no** 形式を使用します。

次の例では、SSID *batman* の認証タイプを、CCKM 認証済みキー管理を使用した Network-EAP に設定します。batman SSID を使用するクライアント デバイスは、adam サーバ リストを使って認証します。認証後、CCKM 対応クライアントは CCKM を使って迅速に再アソシエートできます。

```
ap1200# configure terminal
ap1200(config-if)# ssid batman
ap1200(config-ssid)# authentication network-eap adam
ap1200(config-ssid)# authentication key-management cckm optional
ap1200(config)# interface dot11radio 0
ap1200(config-if)# ssid batman
ap1200(config-ssid)# end
```

レガシー WEP SSID の WPA 移行モードの設定

WPA 移行モードは、レガシー WEP クライアント タイプをサポートする必要がある一方、よりセキュアな認証および暗号化を使用できるようにするための SSID 専用のモードです。この特定のモードでは、次のタイプのクライアント デバイスを使用できます。

- TKIP と認証済みキー管理に対応した WPA クライアント
- 認証済みキー管理には対応しているが TKIP には対応していない 802.1X-2001 クライアント（従来の LEAP クライアント、TLS を使うクライアントなど）
- TKIP にも認証済みキー管理にも対応してない静的 WEP クライアント

これら 3 つのタイプすべてのクライアントが同じ SSID を使用してアソシエートする場合、SSID 用のマルチキャスト暗号スイートは WEP でなければなりません。最初の 2 つのタイプのクライアントだけが同じ SSID を使用する場合、マルチキャスト キーは動的でもかまいませんが、静的 WEP クライアントが SSID を使用する場合、キーは静的でなければなりません。アクセス ポイントは自動的に静的グループ キーおよび動的グループ キー間を切り替えて、アソシエートされているクライアント デバイスに対応することができます。同じ SSID で 3 つのすべてのタイプのクライアントをサポートするには、キー スロット 2 または 3 に静的キーを設定する必要があります。

WPA 移行モードに SSID を設定するには、次の設定を行います。

- WPA（オプション）
- TKIP および 40 ビットまたは 128 ビット WEP を含む暗号スイート
- キー スロット 2 または 3 内の静的 WEP キー

次の例では、WPA 移行モードに移行するために SSID を設定します。

```
ap1200# configure terminal
ap1200(config-if)# ssid migrate
ap1200(config-if)# encryption mode cipher tkip wep128
ap1200(config-if)# encryption key 3 size 128 12345678901234567890123456 transmit-key
ap1200(config-ssid)# authentication open
ap1200(config-ssid)# authentication network-eap adam
ap1200(config-ssid)# authentication key-management wpa optional
ap1200(config-ssid)# wpa-psk ascii batmobile65
ap1200(config)# interface dot11radio 0
ap1200(config-if)# ssid migrate
ap1200(config-ssid)# end
```

追加の WPA の設定

2 つのオプションの設定を使ってアクセス ポイントに事前共有キーを設定し、グループ キーの更新頻度を調整します。

事前共有キーの設定

8021X/EAP ベース認証を使用できないワイヤレス LAN 上の WPA（WPAv1 または WPAv2）をサポートするには、アクセス ポイント上に事前共有キーを設定する必要があります。事前共有キーを ASCII 文字または 16 進数として入力できます。キーを ASCII 文字として入力する場合は、8 ～ 63 文字を入力します。アクセス ポイントはこのキーを、『*Password-based Cryptography Standard*（RFC2898）』に記載されているプロセスを使用して展開します。キーを 16 進数として入力する場合は、64 桁の 16 進数を入力する必要があります。

グループ キー更新の設定

WPA プロセスの最後の段階で、アクセス ポイントは認証されたクライアント デバイスにグループ キーを配布します。次のオプションの設定を使って、クライアントのアソシエーションとアソシエーション解除をベースにして、グループ キーを変更、配布するようにアクセス ポイントを設定できます。

- Membership-termination：アクセス ポイントは、任意の認証されたデバイスがアクセス ポイントからアソシエーションを解除するときに、新しいグループ キーを生成、配布します。この機能は、アソシエートされているデバイスに対してグループ キーを秘匿しますが、ネットワーク上のクライアントがアクセス ポイント間を頻繁にローミングする場合、オーバーヘッド トラフィックを生む可能性があります。
- 機能の変更：セルのクライアント機能が変更されると、アクセス ポイントは動的グループ キーを生成して配布します。たとえば、AES、TKIP、および WEP を許可するセル内に、現在 AES クライアントだけが含まれている場合、ブロードキャスト キーは AES を使用します。アクセス ポイントは、このセルに初めて TKIP クライアントが参加すると TKIP を使用して新しいブロードキャスト キーを生成し、初めて WEP クライアントが参加すると新しいブロードキャスト キーをブロードキャスト キーを生成します。対称的に、アクセス ポイントは最後の WEP クライアントがセルを離れると新しいブロードキャスト キーを生成します。その時点ですべてのクライアントが AES をサポートしている場合、新しいブロードキャスト キーでは AES が使用されます。一部のクライアントが TKIP を使用し、その他のクライアントが AES を使用する場合（AES クライアントも TKIP をサポートします）、新しいブロードキャスト キーでは TKIP が使用されます。最後の TKIP クライアントがセルを離れ、セル内に AES クライアントだけが残されると、アクセス ポイントは AES を使用して新しいブロードキャスト キーを生成します。

特権 EXEC モードから、次の手順に従って、WPA 事前共有キーとグループ キー更新オプションを設定します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ssid** *ssid-string*	SSID の SSID コンフィギュレーション モードを開始します。
ステップ 3	**wpa-psk** { **hex** | **ascii** } [**0** | **7**] *encryption-key*	クライアント デバイス用の事前共有キーを、静的 WEP キーも利用する WPA を使って入力します。 PSK 認証で WPAv1 または WPAv2 を使用するクライアント デバイスの事前共有キーを入力します。16 進数を使用する場合は、256 ビット キーを完成するために 64 桁の 16 進数を入力する必要があります。ASCII を使用する場合、アクセス ポイントでキーが拡張されるように最低 8 文字の英数字または記号を入力する必要があります。ASCII 文字は 63 文字まで入力できます。
ステップ 4	**interface dot11radio** { **0** | **1** }	無線インターフェイスのインターフェイス コンフィギュレーション モードを開始します。 2.4GHz 無線および 2.4GHz 802.11n 無線は 0 です。 5GHz 無線および 5GHz 802.11n 無線は 1 です。
ステップ 5	**ssid** *ssid-string*	ステップ 2 で定義した SSID を入力して、選択した無線インターフェイスに SSID を割り当てます。
ステップ 6	**exit**	特権 EXEC モードに戻ります。
ステップ 7	**broadcast-key** [**vlan** *vlan-id*] { **change** *seconds* } [**membership-termination**] [**capability-change**]	**broadcast key rotation** コマンドを使用して、WPA グループ キーの追加の更新を設定します。
ステップ 8	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

次の例は、WPA および静的 WEP を使用するクライアント用の事前共有キーを、グループ キー更新オプションとともに設定する方法を示しています。

```
ap# configure terminal
ap(config-if)# ssid batman
ap(config-ssid)# wpa-psk ascii batmobile65
ap(config)# interface dot11radio 0
ap(config-ssid)# ssid batman
ap(config-if)# exit
ap(config)# broadcast-key vlan 87 membership-termination capability-change
```

MAC 認証キャッシングの設定

無線 LAN 上の MAC 認証クライアントが頻繁にローミングする場合、アクセス ポイント上で MAC 認証キャッシュを有効にすることができます。MAC 認証キャッシングを使用すると、アクセス ポイントは認証サーバに要求を送信することなく MAC アドレス キャッシュ内のデバイスを認証するため、オーバーヘッドが軽減されます。クライアント デバイスが認証サーバに対する MAC 認証を実行すると、アクセス ポイントがクライアントの MAC アドレスをキャッシュに追加します。

特権 EXEC モードから、次の手順に従って MAC 認証キャッシングを有効にします。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**dot11 aaa authentication mac-authen filter-cache** [**timeout** *seconds*]	アクセス ポイントでの MAC 認証キャッシングを有効にします。 **timeout** オプションを使用して、キャッシュ内の MAC アドレスのタイムアウト値を設定します。値を 30 ～ 65555 秒の範囲で入力します。デフォルト値は 1800（30 分）です。タイムアウト値を入力すると、MAC 認証キャッシングが自動的に有効になります。
ステップ 3	**exit**	特権 EXEC モードに戻ります。
ステップ 4	**show dot11 aaa authentication mac-authen filter-cache** [*address*]	MAC 認証キャッシュ内のエントリを表示します。特定のクライアントのエントリを表示するには、クライアントの MAC アドレスを追加します。
ステップ 5	**clear dot11 aaa authentication mac-authen filter-cache** [*address*]	キャッシュ内のすべてのエントリをクリアします。キャッシュから特定のクライアントをクリアするには、クライアントの MAC アドレスを追加します。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

次の例は、タイムアウトを 1 時間に設定して MAC 認証キャッシングを有効にする方法を示しています。

```
ap# configure terminal
ap(config)# dot11 aaa authentication mac-authen filter-cache timeout 3600
ap(config)# end
```

MAC 認証キャッシングを無効にするには、**no** 形式の **dot11 aaa authentication mac-authen filter-cache** コマンドを使用します。次に例を示します。

```
no dot11 aaa authentication mac-authen filter-cache
```

または

```
no wlccp wds aaa authentication mac-authen filter-cache
```

認証のホールドオフ、タイムアウト、間隔の設定

特権 EXEC モードから、次の手順に従って、アクセス ポイントを介して認証を行うクライアント デバイスにホールドオフ時間、再認証間隔、認証タイムアウトを設定します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**dot11 holdoff-time** *seconds*	クライアント デバイスが認証失敗の後に次の認証を試みるまでに待機する時間を、秒数で入力します。ホールドオフ期間は、クライアントがログインに 3 回失敗したとき、つまりアクセス ポイントからの認証要求に 3 回応答できなかったときに開始されます。値を 1 ～ 65555 秒の範囲で入力します。
ステップ 3	**dot1x timeout supp-response** *seconds* [local]	認証に失敗するまでにアクセス ポイントがクライアントの EAP/dot1x メッセージ返答を待つ時間を秒数で入力します。値を 1 ～ 120 秒の範囲で入力します。 すでに設定されているタイムアウト値とは別のタイムアウト値を優先して送信するように RADIUS サーバを設定できます。アクセス ポイントが RADIUS サーバの値を無視して、設定された値を使用するように設定するには、**local** キーワードを入力します。 オプションの **no** キーワードを使用すると、タイムアウトが 30 秒のデフォルト状態にリセットされます。
ステップ 4	**interface dot11radio** { **0** | **1** }	無線インターフェイスのインターフェイス コンフィギュレーション モードを開始します。 2.4GHz 無線および 2.4GHz 802.11n 無線は 0 です。 5GHz 無線および 5GHz 802.11n 無線は 1 です。
ステップ 5	**dot1x reauth-period** { *seconds* | **server** }	認証されたクライアントに対して再認証するように強制する前に、アクセス ポイントが待つ間隔を秒数で入力します。 認証サーバが指定した再認証間隔を使用するようにアクセス ポイントを設定する場合は、**server** キーワードを入力します。このオプションを使用する場合は、認証サーバを RADIUS 属性 27、Session-Timeout に設定します。この属性により、セッションまたはプロンプトが終了するまでにクライアントに提供されるサービスの最大秒数が設定されます。サーバは、クライアント デバイスが EAP 認証を実行するときにこの属性をアクセス ポイントに送信します。 （注）　SSID に MAC アドレス認証と EAP 認証を両方設定した場合、サーバからクライアント デバイスの MAC 認証と EAP 認証両方の Session-Timeout 属性が送信されます。アクセス ポイントでは、クライアントが最後に実行した認証の Session-Timeout 属性が使用されます。たとえば、クライアントが MAC アドレス認証を実行し、次に EAP 認証を実行した場合、アクセス ポイントではサーバの EAP 認証の Session-Timeout 値が使用されます。いずれの Session-Timeout 属性を使用するのかという混乱を避けるため、認証サーバで MAC 認証と EAP 認証の両方に同じ Session-Timeout 値を設定します。

	コマンド	目的
ステップ 6	**countermeasure tkip hold-time** *seconds*	TKIP MIC 障害保持時間を設定します。保持時間は、0 ～ 65535 秒の範囲で指定できます。デフォルトは 60 秒です。 アクセス ポイントが、たとえば 60 秒以内に 2 度の MIC 障害を検出した場合、そのインターフェイス上のすべての TKIP クライアントを保持時間だけブロックします。
ステップ 7	**end**	特権 EXEC モードに戻ります。
ステップ 8	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

値をデフォルトに戻すには、各コマンドの **no** 形式を使用します。

802.1X サプリカントの EAP 方式プロファイルの作成と適用

この項では、802.1X サプリカントに対応した EAP 方式リストのオプション設定について説明します。EAP 方式プロファイルを設定すると、サプリカントで利用可能な EAP 方式でも、サプリカントがその一部を確認応答しないようにできます。たとえば、RADIUS サーバが EAP-FAST と LEAP をサポートしている場合に、特定の設定下において、サーバは安全性の高い方式ではなく、LEAP を最初に使用する場合があります。優先される EAP 方式リストが定義されていない場合、サプリカントは LEAP をサポートしますが、EAP-FAST などの安全性の高い方式をサプリカントに強制するほうが有益です。

802.1X サプリカントの詳細については、クレデンシャル プロファイルの作成（4-25 ページ）を参照してください。

EAP 方式プロファイルの作成

特権 EXEC モードから、次の手順に従って新しい EAP プロファイルを定義します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**eap profile** *profile name*	プロファイル名を入力します
ステップ 3	**description**	（任意）EAP プロファイルの説明を入力します
ステップ 4	**method** {**fast** | **gtc** | **leap** | **md5** | **mschapv2** | **peap** | **tls**}	許可する 1 つまたは複数の EAP 方式を入力します。 （注）　EAP-GTC、EAP-MD5、および EAP-MSCHAPV2 は、サブパラメータとして表示されますが、トンネル型 EAP 認証の内部方式として使用され、プライマリ認証方式としては使用されません。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**copy running config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

コマンドを無効にする、またはデフォルトに設定するには、**no** コマンドを使用します。

現在利用可能な（登録済み）EAP 方式を表示するには、**show eap registrations method** コマンドを使用します。

```
ap#show eap registrations method
Registered EAP Methods:
  Method  Type            Name
    4     Auth and Peer   MD5
    6     Auth and Peer   GTC
    13    Auth and Peer   TLS
    17    Auth and Peer   LEAP
    25    Auth and Peer   PEAP
    26    Auth and Peer   MSCHAPV2
    43    Auth and Peer   FAST
```

既存の EAP セッションを表示するには、**show eap sessions** コマンドを使用します。

ファストイーサネットインターフェイスに対する EAP プロファイルの適用

この操作は通常、RADIUS サーバに対して認証する必要があるアクセス ポイントが、接続デバイスの 802.1x 認証を行うように設定されたスイッチ ポートに接続される際に、それらのアクセス ポイントに適用されます。この場合、AP は 802.1X クライアントとして機能するため、認証するクレデンシャルを提供する必要があります。

特権 EXEC モードから、次の手順に従って EAP プロファイルをファストイーサネットインターフェイスに適用します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface gigabitethernet 0**	アクセス ポイントのファスト イーサネット ポートのインターフェイス コンフィギュレーション モードを開始します。 **interface g0** を使用してファスト イーサネット コンフィギュレーション モードを開始することもできます。
ステップ 3	**dot1x eap profile** *profile*	プロファイルの事前設定プロファイル名を入力します。
ステップ 4	**end**	インターフェイス コンフィギュレーション モードを終了します。

アップリンク SSID に対する EAP プロファイルの適用

この操作は通常、無線リンクを介してルート アクセス ポイントまたはルート ブリッジに対して認証される必要がある非ルート ブリッジおよびワークグループ ブリッジに適用されます。特権 EXEC モードから、次の手順に従って EAP プロファイルをアップリンク SSID に適用します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface dot11radio** {**0** | **1**}	無線インターフェイスのインターフェイス コンフィギュレーション モードを開始します。 2.4GHz 無線および 2.4GHz 802.11n 無線は 0 です。 5GHz 無線および 5GHz 802.11n 無線は 1 です。
ステップ 3	**ssid** *ssid*	アップリンク SSID を無線インターフェイスに割り当てます。

	コマンド	目的
ステップ 4	**dot1x** {**credentials** | **default** | **eap**}	次のいずれかの値を指定できます。 • credentials：クレデンシャル プロファイルの設定 • default：この SSID のデフォルト値で Dot1x を設定します。 • eap：EAP 固有のパラメータを設定します。
ステップ 5	**dot1x eap profile** *profilename*	プロファイルの事前設定プロファイル名を入力します。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**copy running config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

アクセス ポイントとクライアント デバイスの認証タイプのマッチング

この項で説明する認証タイプを使用する場合は、アクセス ポイントの認証設定がアクセス ポイントにアソシエートするクライアント アダプタの認証設定に一致している必要があります。アクセス ポイントに暗号スイートおよび WEP を設定する手順の詳細は、暗号化モードの設定（10-7 ページ）を参照してください。

表 11-1 は、各認証タイプに必要なクライアントとアクセス ポイントの設定を示しています。

（注）　Cisco Aironet 以外のクライアント アダプタの中には、**Open 認証 + EAP** を設定しないと、アクセス ポイントに対して 802.1X 認証を実行しないものもあります。LEAP を使用する Cisco Aironet クライアントと LEAP を使用する Cisco Aironet 以外のクライアントの両方が同じ SSID を使用してアソシエートできるようにするには、その SSID を **Network EAP** 認証と **Open 認証 + EAP** の両方に対応するように設定することが必要な場合があります。

表 11-1　クライアントとアクセス ポイントのセキュリティ設定

セキュリティ機能	クライアントの設定	アクセス ポイントの設定
静的 WEP（Open 認証）	WEP キーを作成し、Use Static WEP Keys と Open Authentication を有効化	WEP を設定して有効化し、SSID に対して Open 認証を有効化。
静的 WEP（Shared Key 認証）	WEP キーを作成し、Use Static WEP Keys と Shared Key Authentication を有効化	WEP を設定して有効化し、SSID に対して Shared Key 認証を有効化。
LEAP 認証	LEAP を有効化	WEP を設定して有効化し、SSID に対して Network-EAP を有効化。[1]

表 11-1　クライアントとアクセス ポイントのセキュリティ設定(続き)

セキュリティ機能	クライアントの設定	アクセス ポイントの設定
EAP-FAST 認証	EAP-FAST を有効化し、自動プロビジョニングを有効化または Protected Access Credential (PAC) ファイルをインポート	WEP を設定して有効化し、SSID[1] に対して Network-EAP を有効化。 ワイヤレス クライアントで EAP-FAST を使用する認証が設定されている場合は、Open 認証 + EAP も設定する必要があります。EAP を使用したオープン認証を設定しないと、次の GUI 警告メッセージが表示されます。 「WARNING: Network EAP is used for LEAP authentication only.If radio clients are configured to authenticate using EAP-FAST, Open Authentication with EAP should also be configured.」 CLI を使用している場合は、次の警告メッセージが表示されます。 「SSID CONFIG WARNING: [SSID]: If radio clients are using EAP-FAST, AUTH OPEN with EAP should also be configured.」
WPA による EAP-FAST 認証	EAP-FAST および Wi-Fi Protected Access (WPA) を有効化し、自動プロビジョニングを有効化または PAC ファイルをインポート。 WPA アクセス ポイントと非 WPA アクセス ポイントの両方にクライアントをアソシエートできるようにするには、両方のアクセス ポイントに対して Allow Association を有効にします。	TKIP を含む暗号スイートの選択、WEP の設定および有効化、SSID に対する Network EAP および WPA の有効化。 (注)　WPA クライアントおよび非 WPA クライアントの両方で SSID を使用できるようにするには、オプションの WPA を有効にします。
802.1X 認証と CCKM	LEAP を有効化	暗号スイートを選択し、SSID に対して EAP および/または Network EAP による Open 認証および CCKM を有効にします。 (注)　802.1X クライアントおよび非 802.1X クライアントの両方で SSID を使用できるようにするには、オプションの CCKM を有効にします。

表 11-1　クライアントとアクセス ポイントのセキュリティ設定(続き)

セキュリティ機能	クライアントの設定	アクセス ポイントの設定
802.1X 認証と WPA	いずれかの 802.1X 認証方式を有効化	暗号スイートを選択し、SSID に対して EAP と WPA による Open 認証を有効化します(EAP による Open 認証に加えて、またはその代わりに Network EAP 認証を有効にすることもできます)。 (注)　WPA クライアントと非 WPA クライアントの両方が SSID を利用できるようにするには、オプションの WPA を有効にします。
802.1X 認証と WPA-PSK	いずれかの 802.1X 認証方式を有効化	暗号スイートを選択し、SSID に対してオプション EAP および WPA による Open 認証を有効化します(オプション EAP による Open 認証に加えて、またはその代わりに、Network-EAP 認証を有効にすることもできます)。WPA 事前共有キーを入力。 802.1x/EAP を使用するクライアントは、個々の WPA PMK を生成します。WPA-PSK を使用するクライアントは、PSK を PMK として使用します。 (注)　WPA クライアントと非 WPA クライアントの両方が SSID を利用できるようにするには、オプションの WPA を有効にします。
動的 WEP 暗号化による EAP-TLS 認証		
Windows を使用してカードを設定する場合	EAP タイプとして Enable network access control using IEEE 802.1X および Smart Card or other Certificate を選択	WEP を設定して有効化し、SSID に対して EAP と EAP による Open 認証を有効化
動的 WEP 暗号化による EAP-MD5 認証		
Windows XP を使用してカードを設定する場合	EAP タイプとして Enable network access control using IEEE 802.1X および MD5-Challenge を選択	WEP を設定して有効化し、SSID に対して EAP と Open Authentication を有効化
動的 WEP 暗号化による PEAP 認証		
Windows を使用してカードを設定する場合	EAP タイプとして Enable network access control using IEEE 802.1X および PEAP を選択	WEP を設定して有効化し、SSID に対して必須 EAP と EAP による Open 認証を有効化

表 11-1　クライアントとアクセス ポイントのセキュリティ設定(続き)

セキュリティ機能	クライアントの設定	アクセス ポイントの設定
動的 WEP 暗号化による EAP-SIM 認証		
Windows を使用してカードを設定する場合	EAP タイプとして Enable network access control using IEEE 802.1X および SIM 認証を選択	完全暗号化による WEP をセットアップして有効化し、SSID に対して必須 EAP と EAP による Open 認証を有効化

1. Cisco Aironet 以外のクライアント アダプタの中には、**Open 認証 + EAP** の両方に対応するように設定することが必要な場合があります。LEAP を使用する Cisco Aironet クライアントと LEAP を使用する Cisco Aironet 以外のクライアントの両方が同じ SSID を使用してアソシエートできるようにするには、その SSID を **Network EAP** 認証と **Open 認証 + EAP** の両方に対応するように設定することが必要な場合があります。

ゲスト アクセス管理

ゲスト アクセスでは、ゲストはインターネットと、ホスト エンタープライズのセキュリティを損なうことなくゲスト独自のエンタープライズにアクセスできます。

ゲスト アクセスは、次の方法で許可されます。

- Web 認証
- Web パススルー

Web 認証

Web 認証を使用すると、ゲストが有効なユーザ名とパスワードを入力するまで Autonomous AP は IP トラフィック（DHCP および DNS 関連のパケット以外）をブロックできます。

Web 認証では、各ゲスト用に異なるユーザ名とパスワードを定義する必要があります。ユーザ名とパスワードを使用して、ゲストはローカル RADIUS サーバまたは外部 RADIUS サーバによって認証されます。

Web 認証は、Open、dot1x、および PSK 認証タイプでサポートされます。すべての暗号化タイプを使用できます。

Web 認証の設定（GUI）

Web 認証を有効にするには、次の手順を実行します。

ステップ 1　アクセス ポイントの GUI で [Secuirty] ページを表示します。

ステップ 2　[SSID Manager] を選択します。

ステップ 3　[Web Authentication] チェックボックスをオンにします。

Web 認証の設定（CLI）

特権 EXEC モードから、次のコマンドを使用して Open 認証による Web 認証を有効にします。

- Open 認証による Web 認証を設定するには、次のコマンドを使用します。
  - ap(config)# **dot11 ssid guestssid**
  - ap(config-ssid)# **web-auth**
  - ap(config-ssid)# **authentication open**
  - ap(config-ssid)# **exit**
- Web 認証を有効にする場合は、次のようにします。
  - ap(config)# **ip admission name Web_auth proxy http**
  - ap(config)# **interface dot11Radio 0**
  - ap(config-if)# **ip admission Web_auth**

特権 EXEC モードから、次のコマンドを使用して dot1x 認証による Web 認証を有効にします。

- Web 認証による Web 認証を設定するには、次のコマンドを使用します。
  - ap(config)# **dot11 ssid guestssid**
  - ap(config-ssid)# **web-auth**
  - ap(config-ssid)# **authentication open eap eap_methods**
  - ap(config-ssid)# **authentication network-eap eap_methods**
  - ap(config-ssid)# **authentication key-management wpa version 2**
  - ap(config-ssid)# **exit**
- Web 認証を有効にする場合は、次のようにします。
  - ap(config)# **ip admission name Web_auth proxy http**
  - ap(config)# **interface dot11Radio 0**
  - ap(config-if)# **ip admission Web_auth**
  - ap(config-if)# encryption mode ciphers aes-ccm

次に、dot1x 認証による Web 認証の設定例を示します。

```
configure terminal
aaa new-model
aaa authentication login webauth group radius
aaa authorization auth-proxy default group radius

radius-server local
nas 192.168.8.100 key 0 cisco
user cisco password cisco

radius-server host 192.168.8.100 auth-port 1812  acct-port 1813 key 0 cisco
aaa group server radius  rad_eap
server 192.168.8.100 auth-port 1812 acct-port 1813
exit
```

```
aaa authentication login eap_methods group rad_eap
ip admission name webauth proxy http
ip admission name webauth method-list authentication webauth

dot11 guest
username guest-use  lifetime 350 password cisco123
exit


dot11 ssid dxwbssid
authentication open eap eap_methods
authentication network-eap eap_methods
authentication key-management wpa version 2
web-auth
guest-mode
exit

int d0
encryption mode ciphers aes-ccm
ssid dxwbssid
ip admission webauth
no shut
exit
```

Web パススルー

Web パススルーは、Web 認証と似ています。ただし、ゲストは認証情報を入力する必要はありません。

Web パススルーでは、ゲストがインターネットを初めて使用するとき、使用ポリシー ページにゲストをリダイレクトします。ポリシーを受け入れると、アクセスが許可されます。アクセス ポイントはゲストをポリシー ページにリダイレクトします。

Web 認証を有効にするには、次の手順を実行します。

ステップ 1　アクセス ポイントの GUI で [Secuirty] ページを表示します。

ステップ 2　[SSID Manager] を選択します。

ステップ 3　[Web Pass] チェックボックスをオンにします。

特権 EXEC モードから、次のコマンドを使用して、Web パススルーを有効にします。

- ap(config)# **ip admission name Web_passthrough consent**
- ap(config)# **interface dot11Radio 0**
- ap(config-if)# **ip admission Web_passthrough**

(注)　VLAN がない場合に限り、Web 認証または Web パススルーがインターフェイスで動作します。SSID が VLAN にマップされている場合、IP admission Web_auth または IP admission Web_passthrough を VLAN に設定する必要があります。

ゲスト アカウントの作成

新しいゲスト アカウントを作成するには、次の手順を実行します。

ステップ 1　GUI で、アクセス ポイントの [Management] > [Guest Management Services] ページを表示します。

ステップ 2　新しいゲスト アカウントを作成するには、[New] を選択します。

[Webauth] ページが表示されます。

ステップ 3　次の値を入力してください。

- Username
- Password
- Confirm Password
- Lifetime

ステップ 4　システムにパスワードとして自動的にランダム文字列を生成させるには、[Generate Password] チェックボックスをオンにします。または、手動でパスワード値を入力することもできます。

ステップ 5　[Apply] をクリックします。

既存のユーザを削除するには、次の手順を実行します。

ステップ 1　アクセス ポイントの GUI の [Guest Management Services] ページを表示します。

ステップ 2　削除するユーザ名を選択します。

ステップ 3　[Delete] をクリックします。

確認メッセージが表示されます。

ステップ 4　[OK] をクリックしてユーザを削除するか、[Cancel] をクリックして変更をキャンセルします。

特権 EXEC モードから、CLI コマンドを使用してゲスト アカウントを作成するには、次のコマンドを使用します。

- ap(config)# **dot11 guest**
- ap(config-guest-mode)# **username Gues-1 lifetime 40 password t_ksdgon**
- ap(config-guest-mode)# **username Gues-2 lifetime 35 password gp2**
- ap(config)# **exit**

ゲスト アクセスは最大で 24 日（35791 分）、最小で 5 分許可されます。

特権 EXEC モードから、ゲスト ユーザを削除するには、次のコマンドを使用します。

ap# **clear dot11 guest-user Gues-1**

特権 EXEC モードから、ゲスト ユーザを表示するには、次のコマンドを使用します。

ap# **show dot11 guest-users**

ゲスト アクセス ページのカスタマイズ

[Webauth Login] ゲスト アクセス ページをカスタマイズして、カスタム ロゴやその他のイメージを表示できます。[Login] ページ、[Success] ページ、[Failure] ページ、[Expired] ページをカスタマイズできます。ページをカスタマイズするには、次の手順に従います。

ステップ 1　カスタマイズしたページに表示するイメージを保存し、Web サーバ上で Web サーバの IP アドレスを ACL 入力/出力リスト許可されるように設定します。

ステップ 2　ページのデフォルト HTML コードをカスタマイズします。

ステップ 3　Web サーバ上のイメージ ファイルのフル パスを指定して、イメージを挿入するようにページのソース コードを編集します。例：<Body background="http://40.40.5.10/image.jpg" width="600" height="600">。ここで、image.jpg ファイルは IP アドレスが 40.40.5.10 の Web サーバ上にあります。

（注）　デフォルト ページの HTML コードを編集する際に、送信関数のコードとユーザ名とパスワードのフィールドのコードは変更しないでください。

ステップ 4　Web サーバにカスタマイズしたページを保存します。

ステップ 5　アクセス ポイントの GUI で、[Management] > [Guest Management Services] ページを表示します。

ステップ 6　[Webauth Login] を選択します。

ステップ 7　Web サーバから、次のページを参照してアップロードします

- [Login] ページ
- [Success] ページ
- [Failure] ページ
- [Expired] ページ

（注）　ゲスト アクセス ログインをカスタマイズする場合、[Login] ページ、[Success] ページ、[Failure] ページ、および [Expired] ページは必ずロードする必要があります。

ステップ 8　ファイル転送方式として FTP または TFTP を選択します。

ステップ 9　[Username] を入力します。

ステップ 10　[Password] を入力します。

ステップ 11　[Allowed-In ACL Name] と [Allowed-Out ACL Name] を入力します。

ステップ 12　変更を保存するには、[Close Window] をクリックします。

あるいは、次の CLI コマンドを使用して、カスタマイズされたゲスト アクセス ページを設定することもできます。編集したすべてのファイルをフラッシュ メモリにコピーします。次に、特権 EXEC モードで、次のコマンドを使用して、すべての編集済みファイルをフラッシュからロードします。

- ap(config)# **ip auth-proxy proxy http login page file flash:web_login.html**
- ap(config)# **ip auth-proxy proxy http success page file flash:web_success.html**
- ap(config)# **ip auth-proxy proxy http failure page file flash:web_fail.html**
- ap(config)# **ip auth-proxy proxy http login expired page file flash:web_logout.html**

ACL で Web サーバの IP アドレス（この場合の IP アドレスは 40.40.5.10）を設定するには、次のコマンドも必要です。特権 EXEC モードから、次の ACL コマンドを使用します。

- ap(config)# **dot11 webauth allowed incoming webauth_acl_in outgoing webaut_acl_out**
- ap(config)# **ip access-list extended webauth_acl_in**
- ap(config-ext-nacl)# **permit tcp any host 40.40.5.10 eq www**
- ap(config-ext-nacl)# **permit tcp any host 40.40.5.10 eq 443**
- ap(config-ext-nacl)# **permit tcp any host 40.40.5.10 eq 443**
- ap(config-ext-nacl)# **exit**
- ap(config)# **ip access-list extended webauth_acl_out**
- ap(config-ext-nacl)# **permit tcp any host 40.40.5.10 eq www**
- ap(config-ext-nacl)# **permit tcp any host 40.40.5.10 eq 443**
- ap(config-ext-nacl)# **exit**

（注）　上記のコマンドの acl-in および acl-out は、アクセス リストの名前です。これらの ACL を使用すると、マシンに保存されたイメージ ファイルをダウンロードして Web ページのカスタマイズに使用できます。

デフォルト ページには、ユーザ名、パスワード、[OK] ページだけが表示されます。

ゲスト アクセスは、次をサポートしていません。

- IPv6
- SNMP
- ローミング

キャプティブ ポータルのバイパス

Android、Apple、および Windows クライアントは、キャプティブ ポータルを使用して Wi-Fi ネットワークに接続します。これらのデバイスは、アソシエーションの時点でインターネット接続が使用できるかどうかを確認します。接続を使用できない場合、クライアントはワイヤレス ネットワークとアソシエートしません。これは、Web 認証または Web パススルーが強制される場合に、Autonomous AP ネットワークで問題になる可能性があります。

Web 認証または Web パススルーが強制される Autonomous AP ネットワークでは、ネットワーク接続は認証またはパススルーが成功した場合にのみ実現します。しかし、Web 認証または Web パススルーの前にキャプティブ ポータルが表示されるため、クライアントはネットワークへの接続に失敗します。

これを解決するために、Android および Windows クライアントでは、キャプティブ ポータルに障害が発生していても、ブラウザを使用して Web 認証または Web パススルーを実行できます。ただし、Apple クライアントでは、キャプティブ ポータルに障害が発生している場合、Web ブラウザを開くことはできません。これを解決するために、Apple クライアントでは、キャプティブ ポータル バイパス機能を設定できます。

Apple クライアントのキャプティブ ポータル バイパス（CLI）

Apple クライアントのキャプティブ ポータル機能をバイパスするには、コマンド **dot11 captive-portal-bypass** を使用します。

このコマンドは、Web 認証 と Web パススルーの両方に対応します。

このバイパスを無効にするには、コマンド **no dot11 captive-portal-bypass** を使用します。

Apple クライアントのキャプティブ ポータル バイパス（GUI）

Apple クライアントのキャプティブ ポータル機能をバイパスするには、[Management] > [Webauth Login] を選択します。

[Captive Portal Bypass] フィールド（Apple クライアントのみ）の対応するオプションをクリックすることによって、このバイパス機能を有効または無効にすることができます。