CHAPTER 11

認証タイプの設定

この章では、アクセス ポイントに無線デバイスに認証タイプを設定する方法について説明します。この章で説明する内容は、次のとおりです。

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。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ために、クライアント デバイスは Media Access Control（MAC; メディア アクセス コントロール）アドレス認証または Extensible Authentication Protocol（EAP; 拡張認証プロトコル）認証を使用してネットワークから認証を得る必要もあります。これらの認証タイプではネットワーク上の認証サーバが使用されます。

（注）　デフォルトでは、アクセス ポイントは service-type 属性を authenticate-only に設定した状態で、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。service-type 属性を login-only に変更することで、Microsoft IAS サーバがアクセス ポイントからの再認証要求を確実に認識できるようになります。再認証要求の service-type 属性を login-only に変更するには、グローバル コンフィギュレーション コマンド **dot11 aaa authentication attributes service-type login-only** を使用します。

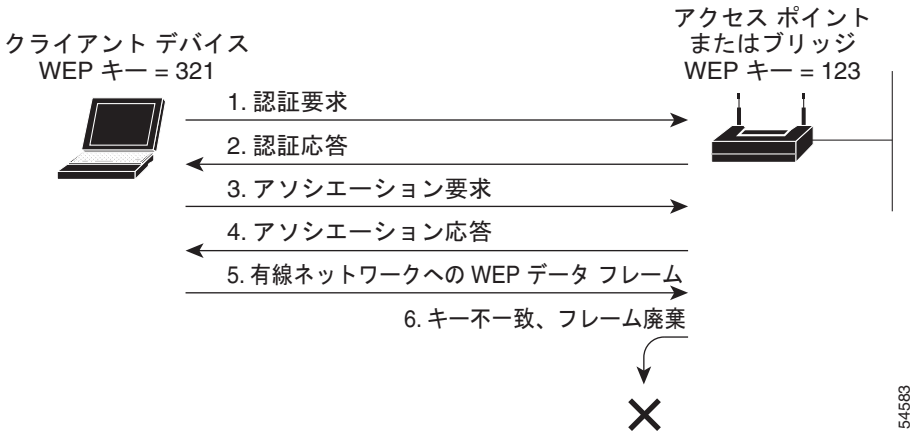
アクセス ポイントは、複数の認証メカニズム（タイプ）を同時に使用することができます。次の項でそれぞれの認証タイプについて説明します。

アクセス ポイントに対する Open 認証

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、すべての無線デバイスがアクセス ポイントから認証を受けられますが、デバイスが通信できるのは Wired Equivalent Privacy（WEP）キーがアクセス ポイントの WEP キーに一致する場合だけです。WEP を使用しないデバイスは WEP を使用しているアクセス ポイントに対して認証を試みません。Open 認証では、ネットワーク上の Remote Authentication Dial-In User Service（RADIUS）サーバは使用されません。

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、データを転送することができません。

図 11-1　Open 認証のシーケンス



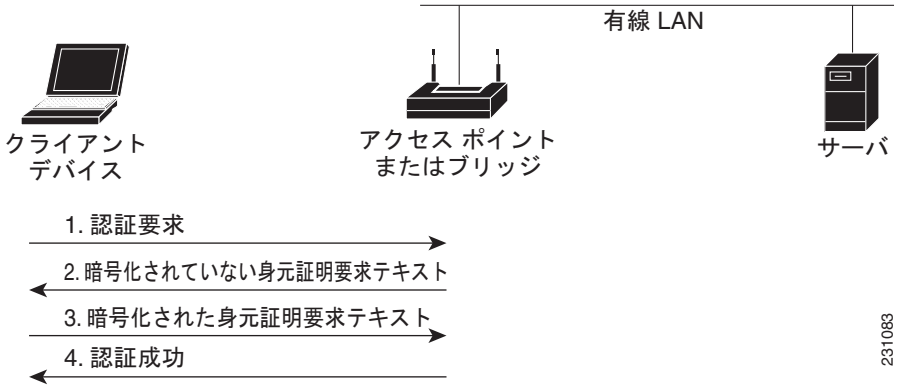
アクセス ポイントに対する Shared Key 認証

シスコでは、IEEE 802.11b 規格に準拠するために、Shared Key 認証も採用しています。ただし、Shared Key 認証にはセキュリティ上の弱点があるため、なるべく使用しないようにしてください。

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、認証が成立し、通信が許可されます。

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。拡張認証プロトコル（EAP）を使用して 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 キーを引き出す補助をします。RADIUS サーバはアクセス ポイントに WEP キーを送ります。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。さらに、アクセス ポイントはブロードキャスト WEP キー（アクセス ポイントの WEP キー スロット 1 に入力されたキー）をクライアントのユニキャスト キーとともに暗号化して、クライアントに送信します。

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

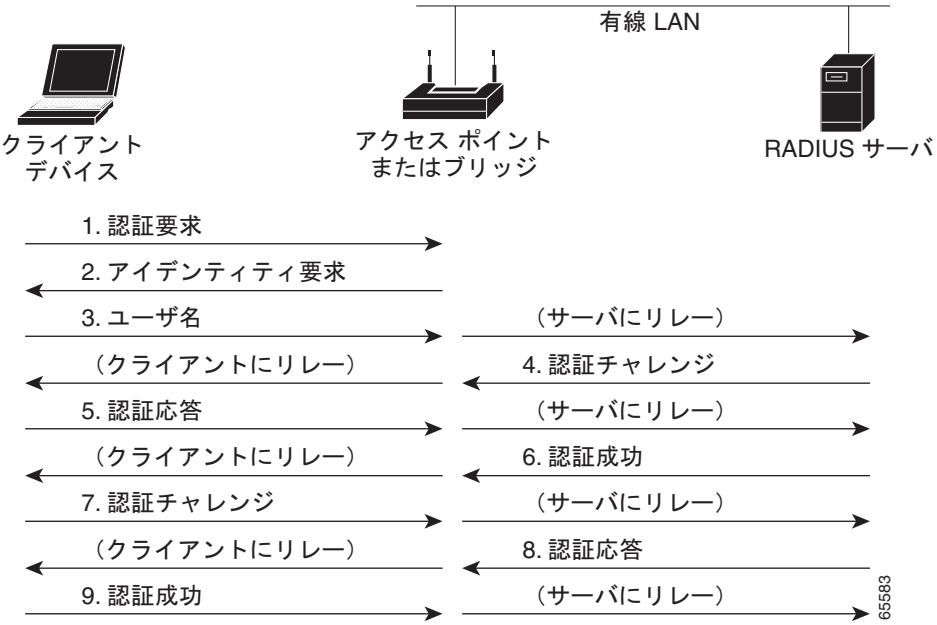


図 11-3 の手順 1 ～ 9 では、無線クライアント デバイスと有線 LAN 上の RADIUS サーバが 802.1x および EAP を使用して、アクセス ポイント経由で相互認証を実行します。RADIUS サーバは、認証身元証明要求をクライアントに送信します。クライアントはユーザが入力したパスワードを一方向暗号化し、認証身元証明要求に対する応答を生成して RADIUS サーバに送信します。RADIUS サーバは、サーバ自体のユーザ データベースの情報から独自の応答を生成し、クライアントからの応答と比較します。RADIUS サーバがクライアントを認証すると、同じ処理が逆方向から繰り返され、今度はクライアントが RADIUS サーバを認証します。

相互認証が終了すると、RADIUS サーバとクライアントは、クライアントに固有の、クライアントに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 セッションでは、RADIUS サーバが *セッション* キーと呼ばれる WEP キーを暗号化して、有線 LAN 経由でアクセス ポイントに送信します。アクセス ポイントは、セッション キーを使用してブロードキャスト キーを暗号化し、クライアントに送信します。クライアントは、送信されてきたキー

を、セッション 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 WEP を有効にし、セッション キーとブロードキャスト WEP 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」（P.11-10）を参照してください。

（注）　EAP 認証を使用する場合は、Open または Shared Key 認証を選択できますが、これ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

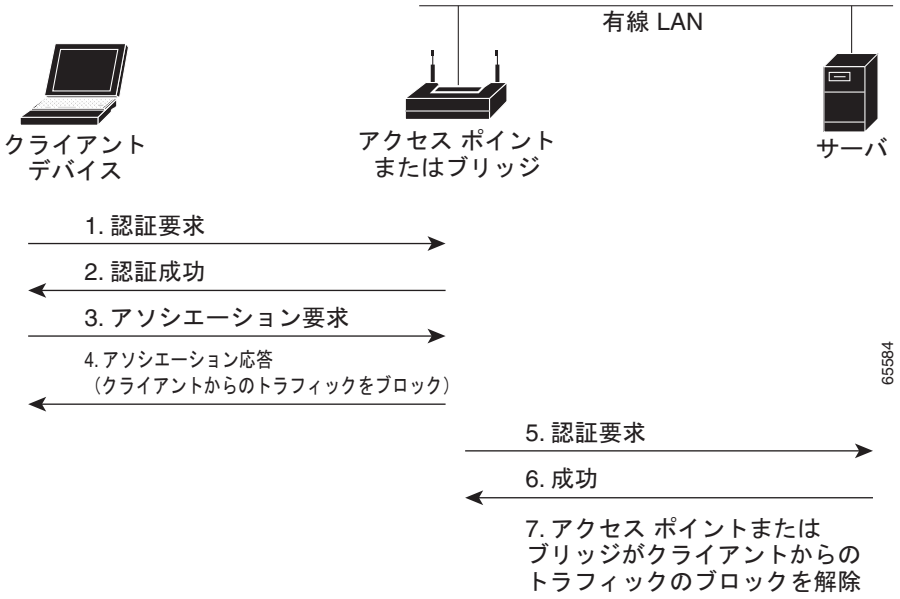
アクセス ポイントは、無線クライアント デバイスの MAC アドレスをネットワーク上の RADIUS サーバに中継します。サーバはそのアドレスを、許可された MAC アドレスのリストと照合します。MAC アドレスは不正侵入者でも偽造できるため、MAC ベースの認証は EAP 認証より安全性が劣ります。ただし、EAP 機能を持たないクライアント デバイスにとって、MAC ベースの認証は 1 つの代替認証方式となります。MAC ベースの認証の有効化の詳細は、「SSID への認証タイプの割り当て」（P.11-10）を参照してください。

ヒント　ネットワークに RADIUS サーバが使用されていない場合は、アクセス ポイントの [Advanced Security: MAC Address Authentication] ページで、許可される MAC アドレスのリストを作成できます。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」（P.11-16）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」（P.11-10）を参照してください。

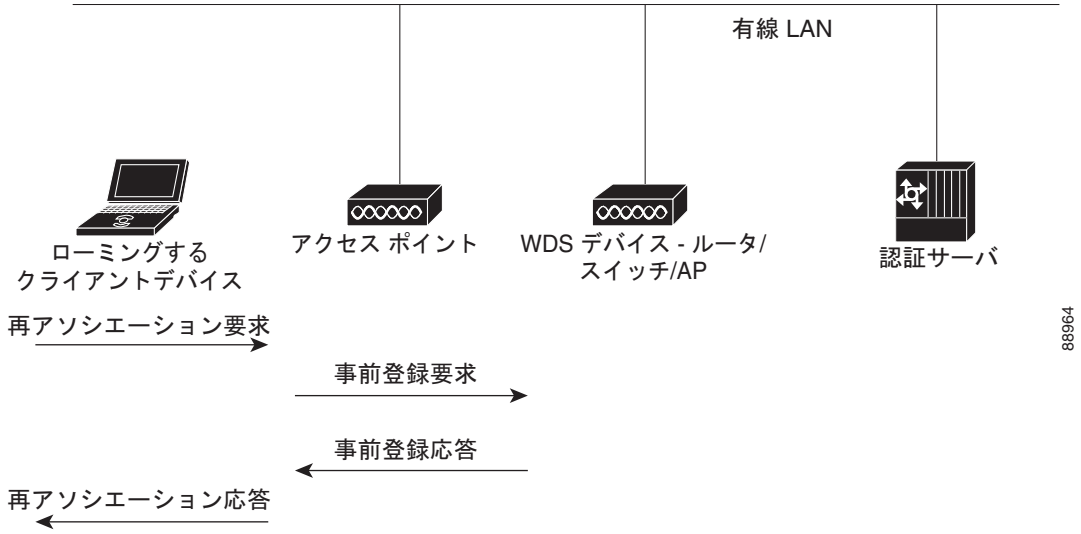
認証されたクライアントの CCKM の利用

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により、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に発生する再アソシエーションに必要な時間が大幅に短縮されます。クライアント デバイスがローミングする場合、WDS のアクセス ポイントは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 プロセスは、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」（P.11-10）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」（P.12-9）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

Wi-Fi Protected Access（WPA）は、既存および将来の無線 LAN システムのデータ保護とアクセス コントロールの水準を大幅に向上させる、標準規格に基づく相互運用性のあるセキュリティ拡張です。WPA は、現在策定中の IEEE 802.11i 規格のサブセットで、この規格と互換性があります。WPA では、データ保護に Temporal Key Integrity Protocol（TKIP）を使用し、認証済みキー管理に 802.1X を使用しています。

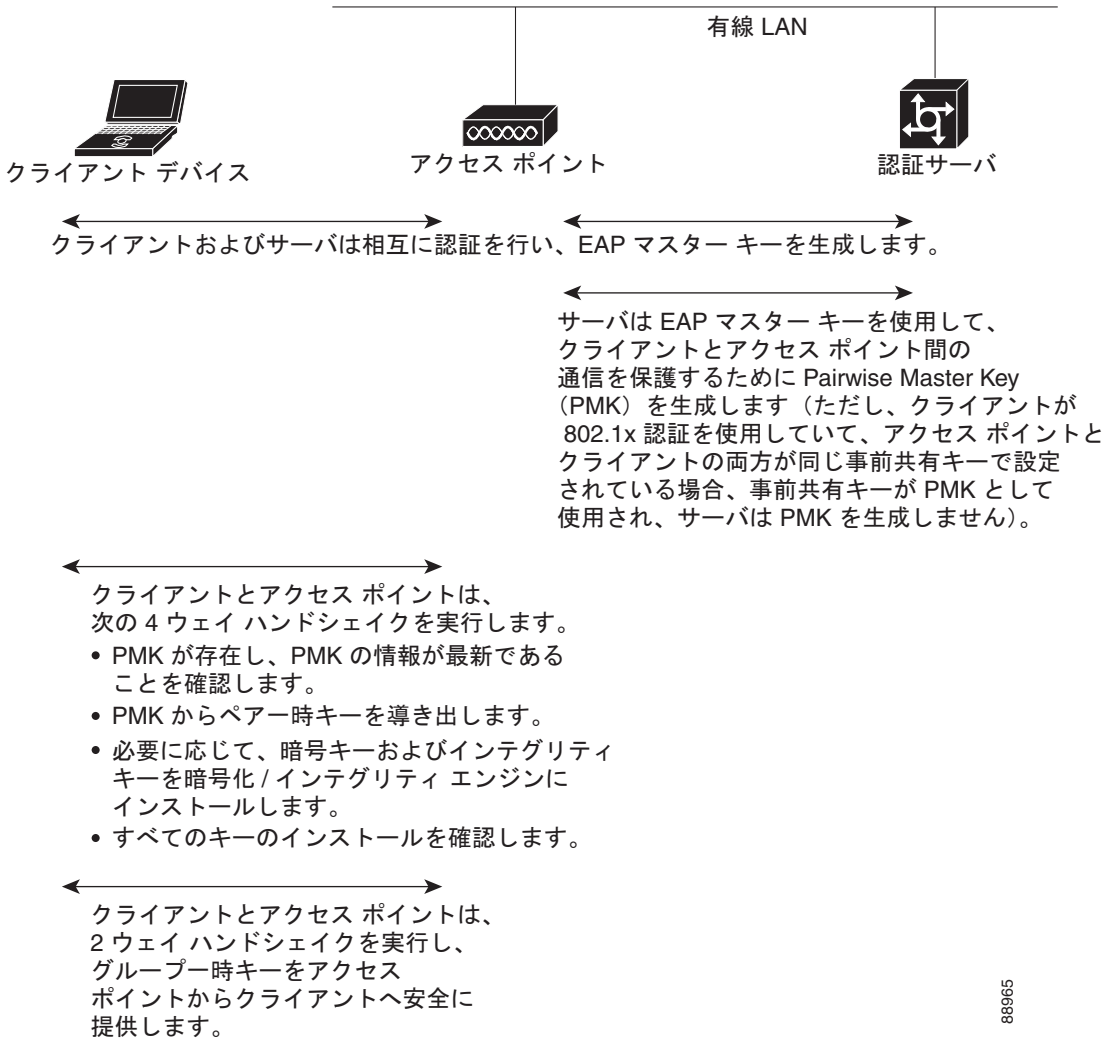
WPA キー管理は、2 つの相互排他的な管理タイプである WPA および WPA-Pre-shared key（WPA-PSK）をサポートしています。クライアントと認証サーバは、WPA を使用してキーを管理し、EAP 認証方式で相互認証を行い、Pairwise Master Key（PMK）を生成します。サーバは WPA を使用し、PMK を動的に生成してアクセス ポイントに渡します。ただし、そのためには、WPA-PSK を使用してクライアントとアクセス ポイントの両方で事前共有キーを設定し、事前共有キーが PMK として使用されるように設定してください。

（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」（P.11-10）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



WPA、CCKM、CKIP、および WPA-TKIP のソフトウェアおよびファームウェア要件

表 11-1 は、アクセス ポイントと Cisco Aironet クライアント デバイスが WPA および CCKM キー管理、Cisco Key Integrity Protocol（CKIP）および WPA-TKIP 暗号化プロトコルをサポートするために必要なファームウェアとソフトウェアの要件を示しています。

表 11-1 に挙げたセキュリティの組み合わせをサポートするには、Cisco Aironet アクセス ポイントおよび Cisco Aironet クライアント デバイスで、次のバージョンのソフトウェアとファームウェアを実行する必要があります。

- アクセス ポイント：Cisco IOS Release 12.2(13)JA 以降
- 340、350、および CB20A クライアント デバイス：次のコンポーネントを含むインストール ウィザード バージョン 1.2
  - PC、LM、および PCI カード ドライバ バージョン 8.4
  - mini-PCI および CardBus PC カード ドライバ バージョン 3.7
  - Aironet Client Utility（ACU）バージョン 6.2
  - クライアント ファームウェア バージョン 5.30.13

表 11-1　WPA、CCKM、CKIP、WPA-TKIP のソフトウェアおよびファームウェア要件

キー管理/暗号化プロトコル	サードパーティ製ホスト サプリカント[1] の要/不要	サポートされているプラットフォーム OS
LEAP/CKIP **（注）** このセキュリティの組み合わせには 12.2(11)JA 以降が必要です。	No	Windows 95/98、Me、NT、2000、XP、Windows CE、Mac OS X、Linux、DOS
LEAP/CCKM + CKIP **（注）** このセキュリティの組み合わせには 12.2(11)JA 以降が必要です。	No	Windows 98、Me、NT、2000、XP、Windows CE
LEAP/CCKM + WPA-TKIP	No	Windows XP および 2000
LEAP/WPA（CCKM なし）	No	Windows XP および 2000
ホスト ベース EAP（PEAP、EAP-SIM、EAP-TLS など）/WPA（CCKM なし）	No[2]	Windows XP
ホスト ベース EAP（PEAP、EAP-SIM、EAP-TLS など）/WPA（CCKM なし）	Yes	Windows 2000
WPA-PSK モード	No [2]	Windows XP
WPA-PSK モード	Yes	Windows 2000

1. Funk Odyssey Client サプリカント バージョン 2.2、Meetinghouse Data Communications Aegis Client バージョン 2.1 など
2. Windows XP ではサードパーティ製のサプリカントは必要ありませんが、Windows XP Service Pack 1 および Microsoft サポート用修正プログラム 815485 をインストールする必要があります。

Cisco Aironet クライアント デバイスのセキュリティ設定の詳細については、『*Cisco Aironet 340, 350, and CB20A Wireless LAN Client Adapters Installation and Configuration Guide for Windows*』を参照してください。次の URL をクリックすると、『*Cisco Aironet 340, 350, and CB20A Wireless LAN Client Adapters Installation and Configuration Guide for Windows*』を参照できます。

http://www.cisco.com/en/US/products/hw/wireless/ps4555/products_installation_and_configuration_guides_list.html

（注）　いずれかの無線インターフェイスまたは VLAN で、（**TKIP + WEP 128** または **TKIP + WEP 40** のような組み合わせではなく）**TKIP** だけの暗号スイートを設定する場合は、この無線または VLAN 上のすべての SSID を、WPA または CCKM のキー管理を使用するように設定する必要があります。無線または VLAN に対して TKIP を設定する場合、SSID にキー管理を設定しないと、SSID に対するクライアント認証が失敗します。

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、第 7 章「複数の SSID の設定」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」（P.11-10）
- 「認証のホールドオフ、タイムアウト、間隔の設定」（P.11-17）
- 「802.1X サプリカントの EAP 方式プロファイルの作成と適用」（P.11-18）

（注）　ワイヤレス ルータのデフォルトの認証 SSID はありません。

SSID への認証タイプの割り当て

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。 SSID には、最大 32 文字の英数字を使用でき、大文字と小文字が区別されます。 最初の文字に次の文字は使用できません。 • 感嘆符（!） • ポンド記号（#） • セミコロン（;） 次の文字は無効とされ、SSID には使用できません。 • プラス記号（+） • 閉じ大カッコ（]） • スラッシュ（/） • 引用符（"） • Tab • 末尾のスペース

	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。方式のリストの詳細は、次のリンクをクリックしてください。http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/fsaaa/scfathen.htm#xtocid2 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）** ただし、Shared Key 認証にはセキュリティ上の弱点があるため、なるべく使用しないようにしてください。 **（注）** Shared Key 認証を割り当てることが可能な SSID は 1 つに限られます。 • （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。

	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 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 キーを引き出す補助をします。ただし、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 EAP 認証を強制しません。 • （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**] [**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 または 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と、この SSID を使用できるのは WPA または CCKM クライアント デバイスだけになります。 SSID の CCKM 機能を有効にするには、Network-EAP 認証も有効にする必要があります。CCKM と Network EAP が SSID で有効な場合、クライアント デバイスが LEAP、EAP-FAST、PEAP/GTC、MSPEAP、EAP-TLS、および EAP-FAST を使用していれば SSID で認証できます。 また、SSID の WPA 機能を有効にするには、Open 認証または Network-EAP 認証、あるいはその両方を有効にする必要があります。 **（注）** 1 つの SSID で WPA と CCKM を両方とも有効にするには、**wpa** を先に入力し、次に **cckm** を入力します。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。CCKM と WPA の両方を有効にするには、暗号化モードを、TKIP を含む暗号スイート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、「暗号スイートと WEP の設定」（P.10-3）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」（P.11-15）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「WDS、高速安全ローミング、無線管理、および Wireless Intrusion Detection Service の設定」を参照してください。
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
```

WPA 移行モードの設定

WPA 移行モードにより、次に挙げるタイプのクライアント デバイスを、同じ SSID を使用してアクセス ポイントにアソシエートさせることができます。

- 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

802.1X ベースの認証を使用できない無線 LAN 上の WPA 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。
- Capability change：アクセス ポイントは、最後の非キー管理（静的 WEP）クライアントがアソシエーションを解除されたときに、動的グループ キーを生成、配布します。また、最初の非キー管理（静的 WEP）クライアントが認証するときに、静的に設定された WEP キーを配布します。WPA 移行モードでは、アクセス ポイントにアソシエートしている静的 WEP クライアントが存在しない場合は、この機能により、キー管理が可能なクライアントのセキュリティが大幅に向上します。

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。 16 進数または ASCII 文字を使用して、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。

	コマンド	目的
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して 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 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 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 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。

	コマンド	目的
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。

MAC 認証キャッシングを無効にするには、**dot11 aaa mac-authen filter-cache** コマンドの **no** 形式を使用します。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 mac-authen filter-cache timeout 3600
ap(config)# end
```

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。

	コマンド	目的
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て、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。
ステップ 6	**countermeasure tkip hold-time** *seconds*	TKIP MIC 障害保持時間を設定します。アクセス ポイントが 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期間の間ブロックします。
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。

（注） 8021X サプリカントは、1130AG シリーズ、1240AG シリーズ、1250 シリーズ、および 1300 シリーズのアクセス ポイントで利用できます。1100 シリーズおよび 1200 シリーズのアクセス ポイントでは利用できません。

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」（P.4-30）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**	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。

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

この操作は一般にルート アクセス ポイントに適用されます。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 fastethernet 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 fa0** 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

この操作は一般的にリピータ アクセス ポイントに適用されます。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。
ステップ 4	**exit**	configure terminal モードに戻ります。
ステップ 5	**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 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。無線クライアント アダプタの認証タイプの設定手順の詳細は、『*Cisco Aironet Wireless LAN Client Adapters Installation and Configuration Guide for Windows*』を参照してください。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、第 10 章「暗号スイートと WEP の設定」を参照してください。

表 11-2 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。
同様に、EAP-FAST を実行している Cisco Aironet 802.11a/b/g クライアント アダプタ（CB21AG および PI21AG）と EAP-FAST または 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。

（注） 802.11n アクセス ポイントを使用している場合、できるだけ 802.11n Wi-Fi カード ベンダーから使用中のカード向けの最新ドライバを入手してください。

表 11-2　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 キー（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 キー（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]
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。Open 認証 + EAP 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。

表 11-2　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 CCKM	LEAP を有効化	暗号スイートを選択し、SSID に対して Network-EAP と CCKM を有効化。 （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。
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 Open authentication と WPA を有効化（Open 認証に加えて、または Open 認証の代わりに 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 Open authentication と WPA を有効化（Open 認証に加えて、または Open 認証の代わりに 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。 （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。
EAP-TLS 認証		
ACU を使用してカードを設定する場合	Host Based EAP と Use Dynamic WEP Keys を有効化（ACU）、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（Windows 2000 Service Pack 3 または Windows XP）	WEP を設定して有効化し、SSID に対して EAP と Open authentication を有効化
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 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 Open Authentication を有効化

表 11-2　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-MD5 認証		
ACU を使用してカードを設定する場合	WEP キーを作成し、Host Based EAP と Use Static WEP Keys を有効化（ACU）、EAP タイプとして Enable network access control using IEEE 802.1X と MD5-Challenge を選択（Windows 2000 Service Pack 3 または Windows XP）	WEP を設定して有効化し、SSID に対して EAP と Open authentication を有効化
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
PEAP 認証		
ACU を使用してカードを設定する場合	Host Based EAP と Use Dynamic WEP Keys を有効化（ACU）、EAP タイプとして Enable network access control using IEEE 802.1X および PEAP を選択（Windows 2000 Service Pack 3 または Windows XP）	WEP を設定して有効化し、SSID に対して EAP と Open authentication を有効化
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 PEAP を選択	WEP を設定して有効化し、SSID に対して Require EAP と Open authentication を有効化
EAP-SIM 認証		
ACU を使用してカードを設定する場合	Host Based EAP と Use Dynamic WEP Keys を有効化（ACU）、EAP タイプとして Enable network access control using IEEE 802.1X および SIM Authentication を選択（Windows 2000 Service Pack 3 または Windows XP）	安全な暗号化の WEP を設定して有効化し、SSID に対して EAP と Open authentication を有効化
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 SIM 認証を選択	安全な暗号化の WEP を設定して有効化し、SSID に対して Require EAP と Open Authentication 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** 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。同様に、EAP-FAST を実行している Cisco Aironet 802.11a/b/g クライアント アダプタ（CB21AG および PI21AG）と EAP-FAST または 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。