



## 認証タイプの設定

---

この章では、アクセス ポイントで認証タイプを設定する手順について説明します。この章では、次の項目について説明します。

- [認証タイプの概要 \(10-2 ページ\)](#)
- [認証タイプの設定 \(10-6 ページ\)](#)
- [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的一致 \(10-9 ページ\)](#)

## 認証タイプの概要

ここでは、アクセスポイントで設定できる認証タイプを説明します。認証タイプは、アクセスポイント用に設定する SSID に関連付けられています。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提供したい場合、複数の SSID を設定できます。複数の SSID の設定については、[第 8 章「複数の SSID の設定」](#)を参照してください。

ワイヤレス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 Key 認証を使って、アクセスポイントで認証を得る必要があります。最大限のセキュリティのために、クライアントデバイスは MAC アドレスか EAP 認証を使って、ネットワーク上の認証サーバに基づく認証タイプを、ネットワークで認証する必要があります。

アクセスポイントは、次の 4 つの認証メカニズム (タイプ) を使用します。同時に複数の認証メカニズムを使用することもできます。ここでは、各認証タイプについて説明します。

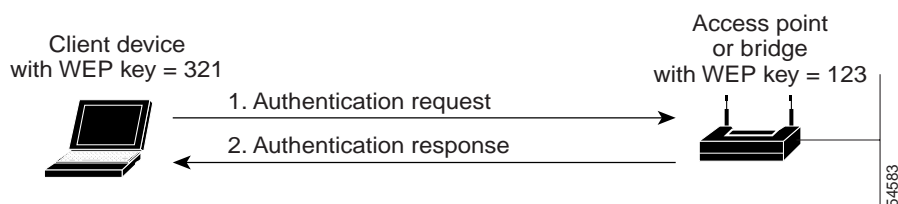
- [アクセスポイントへの Open 認証 \(10-2 ページ\)](#)
- [アクセスポイントへの Shared Key 認証 \(10-3 ページ\)](#)
- [ネットワークへの EAP 認証 \(10-3 ページ\)](#)
- [ネットワークへの MAC アドレス認証 \(10-5 ページ\)](#)
- [MAC ベースの認証、EAP 認証、および Open 認証の組み合わせ \(10-5 ページ\)](#)

### アクセスポイントへの Open 認証

Open 認証は、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 認証を使用して、ワイヤレスデバイスは、アクセスポイントとの認証ができますが、WEP キーがアクセスポイントのキーと一致する場合に限り、通信できます。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との認証を試みません。Open 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 10-1](#) 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 10-1 Open 認証のシーケンス



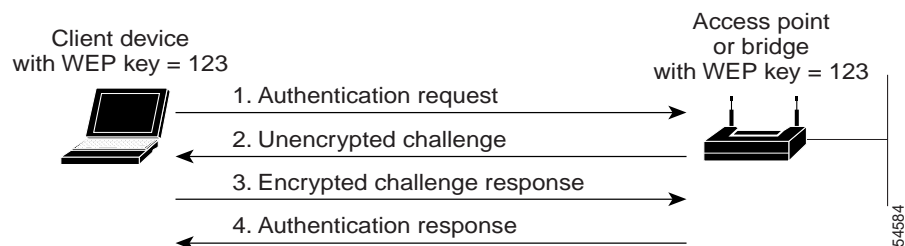
## アクセス ポイントへの Shared Key 認証

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文字列を送信します。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、どちらも監視することができます。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 キーを割り出す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 10-2 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 10-2 Shared Key 認証のシーケンス



## ネットワークへの EAP 認証

この認証タイプは、ワイヤレス 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。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、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 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 キーと共に暗号化して、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 10-3 に示す手順で実行されます。

図 10-3 EAP 認証のシーケンス

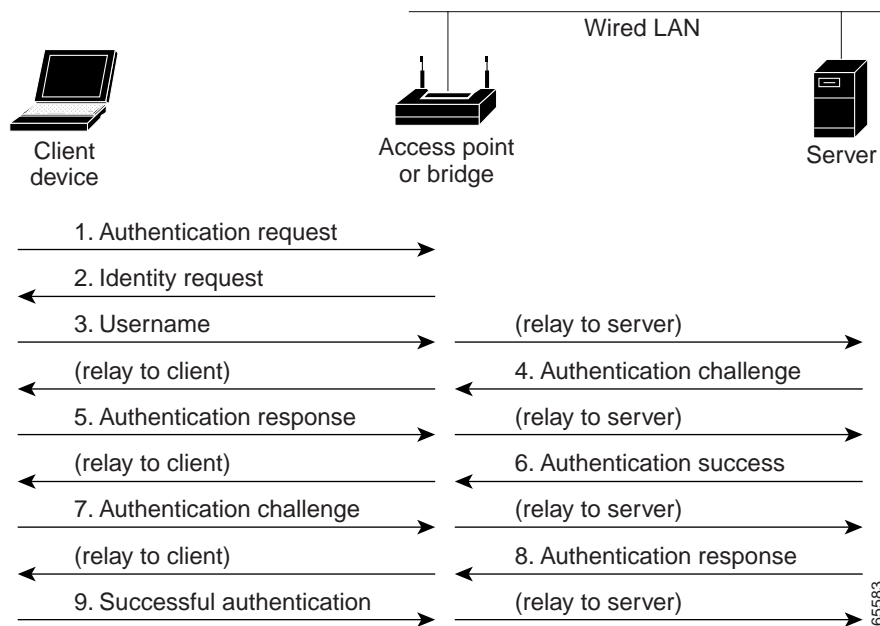


図 10-3 の 1 ~ 9 では、ワイヤード LAN 上のワイヤレス クライアント デバイスと RADIUS サーバが、802.1x および EAP を使用して、アクセス ポイント経由で相互認証を行っています。RADIUS サーバは、認証身元証明要求をクライアントに送信します。クライアントはユーザが入力したパスワードを一方暗号化し、身元証明要求に対する応答を生成して、それを RADIUS サーバに送信します。RADIUS サーバは、サーバ自体のユーザ データベースの情報から独自の応答を生成し、それをクライアントからの応答と比較します。RADIUS サーバがクライアントを認証すると、同じ処理が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、クライアント固有の WEP キーを特定して、適切なレベルのネットワーク アクセスを提供します。これにより、ワイヤードスイッチドセグメントのセキュリティ レベルは、個々のデスクトップのレベルまで近づきます。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、ワイヤード 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ブロードキャストキーをセッションキーを使って暗号化し、クライアントに送信します。クライアントはセッションキーを使用してキーを復号化します。クライアントとアクセスポイントは WEP を有効にして、セッションおよびブロードキャスト WEP キーを残りのセッションのすべての通信に使用します。

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、ワイヤレスクライアントデバイスから RADIUS サーバに、RADIUS サーバからワイヤレスクライアントデバイスに、認証メッセージを中継します。アクセスポイントでの EAP の設定方法については、10-6 ページの「SSID への認証タイプの割り当て」を参照してください。



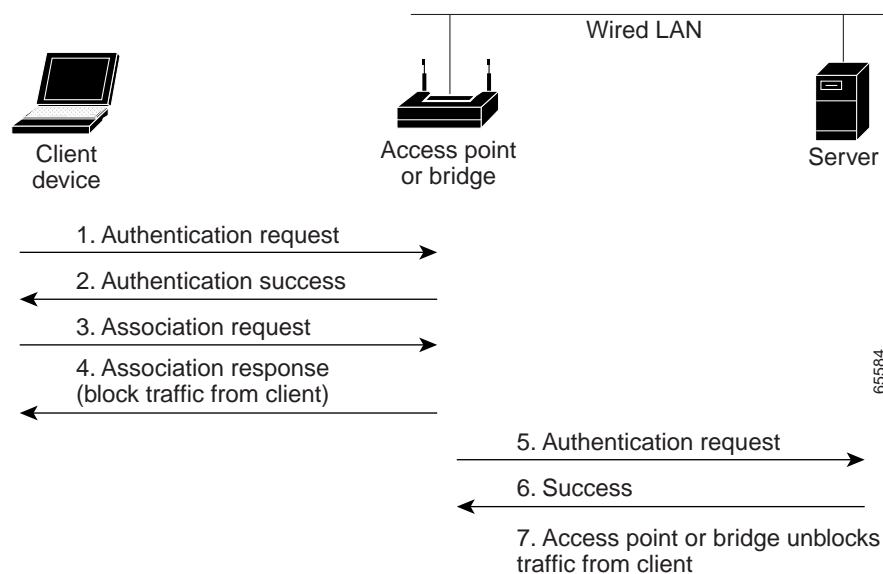
(注) EAP 認証を使用する場合は、Open または Shared Key 認証を選択できますが、これは必須ではありません。EAP 認証は、アクセスポイントとネットワークの両方に対する認証を制御します。

## ネットワークへの MAC アドレス認証

アクセス ポイントは、ワイヤレス 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らし合わせます。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 [ Address Filters ] 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。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 つの代替認証手段となります。MAC ベースの認証の有効化については、10-6 ページの「SSID への認証タイプの割り当て」を参照してください。

図 10-4 は、MAC ベースの認証のシーケンスを示しています。

図 10-4 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 認証を組み合わせることでクライアント 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 ポイントに結合するクライアント 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、アクセス ポイントはクライアント デバイスによる EAP 認証の試行を待ちます。このような認証の組み合わせを設定する方法については、10-6 ページの「SSID への認証タイプの割り当て」を参照してください。

## 認証タイプの設定

ここでは、認証タイプの設定方法について説明します。アクセス ポイントの SSID に設定タイプを添付します。複数の SSID の設定については、第 8 章「複数の SSID の設定」を参照してください。ここでは、次の事柄を取り上げます。

- 認証のデフォルト設定 (10-6 ページ)
- SSID への認証タイプの割り当て (10-6 ページ)
- 認証のホールドオフ、タイムアウト、間隔の設定 (10-8 ページ)

### 認証のデフォルト設定

アクセス ポイントのデフォルトの SSID は tsunami です。表 10-1 に、デフォルトの SSID に対するデフォルトの認証設定を示します。




表 10-1 認証のデフォルト設定

機能	デフォルト設定
SSID	tsunami
ゲスト モード SSID	tsunami (アクセス ポイントはビーコン中のこの SSID をブロードキャストして、SSID のないクライアントデバイスが結合できるようにします)
tsunami に割り当てられている認証タイプ	open

### SSID への認証タイプの割り当て

SSID 用の認証タイプを設定するには、イネーブル EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードに入ります。
ステップ 2	<code>interface dot11radio 0</code>	無線インターフェイス用のインターフェイス コンフィギュレーション モードに入ります。
ステップ 3	<code>ssid ssid-string</code>	SSID を生成し、新しい SSID 用の SSID コンフィギュレーション モードに入ります。SSID には、最大 32 桁の英数字を使用できます。SSID では大文字 / 小文字が区別されます。

コマンド	目的
<b>ステップ 4</b> <b>authentication open</b> <b>[mac-address list-name [alternate]]</b> <b>[eap list-name]</b>	<p>(任意) この SSID に対して、認証タイプを Open に設定します。Open 認証は、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。</p> <ul style="list-style-type: none"> <li>(任意) SSID の認証タイプを MAC アドレス認証で 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、ネットワークに参加を許可する前に MAC アドレス認証を実行することを強制します。 <i>list-name</i> には、認証方式リストを指定します。方式リストの詳細は、次のリンクをクリックしてください。 <a href="http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/fsaaa/scfathen.htm#xtocid2">http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/fsaaa/scfathen.htm#xtocid2</a></li> <li><b>alternate</b> キーワードを使用して、クライアント デバイスが MAC または EAP 認証を使ってネットワークに参加することを許可し、いずれかの認証を正常に完了したクライアントが、ネットワークへの参加を許可されます。</li> <li>(任意) SSID の認証タイプを EAP 認証で 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、ネットワークに参加を許可する前に EAP 認証を実行することを強制します。<i>list-name</i> には、認証方式リストを指定します。</li> </ul> <p> (注) EAP 認証用に設定されているアクセスポイントは、すべての結合しているクライアント デバイスに、EAP 認証を実行することを強制します。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。</p>
<b>ステップ 5</b> <b>authentication shared [mac-address list-name][eap list-name]</b>	<p>(任意) この SSID に対して、認証タイプを Shared Key に設定します。</p> <p> (注) 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。</p> <p> (注) Shared Key 認証は、たった 1 つの SSID だけに割当てできます。</p> <ul style="list-style-type: none"> <li>(任意) SSID の認証タイプを MAC アドレス認証で Shared Key に設定します。<i>list-name</i> には、認証方式リストを指定します。</li> <li>(任意) SSID の認証タイプを EAP 認証で Shared Key に設定します。<i>list-name</i> には、認証方式リストを指定します。</li> </ul>

	コマンド	目的
ステップ 6	<b>authentication network-eap</b> <i>list-name</i> [ <i>mac-address list-name</i> ]	(任意) この SSID に対して、認証タイプを Network-EAP に設定します。Extensible Authentication Protocol (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、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 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 EAP 認証を実行するように強制しません。  <ul style="list-style-type: none"> <li>(任意) SSID の認証タイプを MAC アドレス認証で Network-EAP に設定します。アクセス ポイントに結合するすべてのクライアント デバイスは、MAC アドレス認証を実行するように要求されます。list-name には、認証方式リストを指定します。</li> </ul>
ステップ 7	<b>end</b>	イネーブル EXEC モードに戻ります。
ステップ 8	<b>copy running-config startup-config</b>	(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 を無効にするか、SSID 機能を無効にするには、no 形式の SSID コマンドを使用します。

MAC アドレスと EAP 認証の組み合わせで、SSID batman 用の認証タイプを Open に設定する例を示します。batman SSID を使用するクライアント デバイスは、最初、adam という名前のサーバを使って MAC アドレス認証を試みます。MAC 認証が成功したら、そのデバイスはネットワークに参加しますが、失敗した場合は、同じサーバを使用する EAP 認証を試みます。

```
ap1100# configure terminal
ap1100(config)# configure interface dot11radio 0
ap1100(config-if)# ssid batman
ap1100(config-ssid)# authentication open mac adam alternate eap adam
ap1100(config-ssid)# end
```

## 認証のホールドオフ、タイムアウト、間隔の設定

アクセス ポイントを通じて認証するクライアント デバイス用に、ホールドオフ タイム、再認証間隔、認証タイムアウトを設定するには、イネーブル EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<b>configure terminal</b>	グローバル コンフィギュレーション モードに入ります。
ステップ 2	<b>dot11 holdoff-time</b> <i>seconds</i>	クライアント デバイスが、認証失敗後に、認証を再試行できるようになるまで待たなければならない秒数を入力します。値を 1 ~ 65555 秒の範囲で入力します。
ステップ 3	<b>interface dot11radio 0</b>	無線インターフェイス用のインターフェイス コンフィギュレーション モードに入ります。
ステップ 4	<b>dot1x client-timeout</b> <i>seconds</i>	アクセス ポイントが、認証を放棄する前に、認証を試みるクライアントからの応答を待つ時間 (秒数) 入力します。値を 1 ~ 65555 秒の範囲で入力します。

	コマンド	目的
ステップ 5	<code>dot1x reauth-period seconds [server]</code>	<p>認証されたクライアントに再認証を強制するまでのアクセス ポイントの待ち時間 (秒数) を入力します。</p> <ul style="list-style-type: none"> <li>(任意) <code>server</code> キーワードを入力して、認証サーバによって指定されている再認証期間を使用するように設定します。このオプションを使う場合、認証サーバを RADIUS attribute 27、Session-Timeout に設定します。この属性は、セッションまたはプロンプトの終了までにクライアントに提供されるサービスの最長時間 (秒数) を設定します。クライアント デバイスが EAP 認証を実行する場合、アクセス ポイントにこの属性を送信します。</li> </ul>
ステップ 6	<code>end</code>	イネーブル EXEC モードに戻ります。
ステップ 7	<code>copy running-config startup-config</code>	(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。

値をデフォルト設定にリセットするには、これらのコマンドの `no` 形式を使用します。

## 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的一致

ここで説明する認証タイプを使用するには、アクセス ポイント認証設定がアクセス ポイントに結合するクライアント アダプタでの認証設定に一致する必要があります。ワイヤレス クライアント アダプタに認証タイプを設定する手順については、『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 ポイントで WEP を設定する手順については、第 9 章「WEP および WEP 機能の設定」を参照してください。

表 10-2 に、各認証タイプに必要なクライアントとアクセス ポイントの設定を一覧表示します。

表 10-2 クライアントおよびアクセス 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
静的な WEP キー (Open 認証)	WEP キーを生成し、静的な WEP キーの使用と Open 認証を有効にする。	WEP を設定して有効にし、Open 認証を有効にする。
静的な WEP キー (Shared Key 認証)	WEP キーを生成し、静的な WEP キーの使用と Shared Key 認証を有効にする。	WEP を設定して有効にし、Shared Key 認証を有効にする。
LEAP 認証	LEAP を有効にする。	WEP を設定して有効にし、EAP と Open 認証を有効にする。
EAP-TLS 認証		
ACU を使用してカードを設定する場合	[ Host Based EAP ] および ACU の [ Use Dynamic WEP Keys ] を有効にし、[ Enable network access control using IEEE 802.1X ] を選択して、Windows 2000 (サービスパック 3) または Windows XP における EAP タイプとして、[ スマート カードまたはその他の証明書 ] を選択する。	WEP を設定して有効にし、EAP と Open 認証を有効にする。
Windows XP を使用してカードを設定する場合	[ Enable network access control using IEEE 802.1X ] を選択して、EAP タイプとして、[ スマートカードまたはその他の証明書 ] を選択する。	WEP を設定して有効にし、EAP と Open 認証を有効にする。

表 10-2 クライアントおよびアクセス 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 キーを生成し、[ Host Based EAP ] を有効にし、ACU で [ Use Dynamic WEP Keys ] を有効にし、[ Enable network access control using IEEE 802.1X ] を選択して、Windows 2000 ( サービス パック 3 ) または Windows XP における EAP タイプとして、[ MD5-Challenge ] を選択する。	WEP を設定して有効にし、EAP と Open 認証を有効にする。
Windows XP を使用してカードを設定する場合	[ Enable network access control using IEEE 802.1X ] を選択して、EAP タイプとして、[ MD5-Challenge ] を選択する。	WEP を設定して有効にし、EAP と Open 認証を有効にする。
PEAP 認証		
ACU を使用してカードを設定する場合	[ Host Based EAP ] および ACU の [ Use Dynamic WEP Keys ] を有効にし、[ Enable network access control using IEEE 802.1X ] を選択して、Windows 2000 ( サービス パック 3 ) または Windows XP における EAP タイプとして、[ PEAP ] を選択する。	WEP を設定して有効にし、EAP と Open 認証を有効にする。
Windows XP を使用してカードを設定する場合	[ Enable network access control using IEEE 802.1X ] および EAP タイプとして [ PEAP ] を選択する。	WEP を設定して有効にし、Require EAP と Open 認証を有効にする。
EAP-SIM 認証		
ACU を使用してカードを設定する場合	[ Host Based EAP ] および ACU の [ Use Dynamic WEP Keys ] を有効にし、[ Enable network access control using IEEE 802.1X ] を選択して、Windows 2000 ( サービス パック 3 ) または Windows XP における EAP タイプとして、[ SIM Authentication ] を選択する。	WEP を [ Full Encryption ] に設定して有効にし、EAP と Open 認証を有効にする。
Windows XP を使用してカードを設定する場合	[ Enable network access control using IEEE 802.1X ] および EAP タイプとして [ SIM Authentication ] を選択する。	WEP を [ Full Encryption ] に設定して有効にし、Require EAP と Open 認証を有効にする。