Windows XP オペレーティング システムでのクライアント アダプタの設定

この付録では、Windows XP でのクライアント アダプタの設定および使用方法について説明します。

この付録では、次の項目について説明します。

概要

この付録では、ACU ではなく Windows XP でクライアント アダプタに対して最小限の設定を行い、Windows XP 用に用意されている 4 つのセキュリティ オプションのうち 1 つを有効にする方法について説明します。次の「セキュリティ機能の概要」の項では、十分に情報を得てから設定プロセスを開始できるよう、これらの各オプションについて説明します。

この付録ではさらに、クライアント アダプタがアソシエートされるネットワークを指定したり、クライアント アダプタの現在のステータスを表示したりする場合に Windows XP を使用する際の基本情報も提供します。

（注）　Windows XP でのクライアント アダプタの設定または使用に関するさらに詳細な情報が必要な場合は、Microsoft の Windows XP に関する資料を参照してください。

セキュリティ機能の概要

Windows XP でクライアント アダプタを使用するときは、WEP（Wired Equivalent Privacy）暗号キーを使用してデータを暗号化することで、無線ネットワーク経由で転送するデータを保護できます。WEP 暗号化では、送信側のデバイスが WEP キーで各パケットを暗号化し、受信側のデバイスが同じキーを使用して各パケットを復号化します。

転送データの暗号化および復号化に使用される WEP キーは、アダプタに静的に関連付けることも、EAP 認証プロセスの一部として動的に作成することもできます。使用する WEP キーの種類は、次の「静的 WEP キー」および「EAP（動的 WEP キーを使用）」の項を参考に決めてください。EAP を使用する動的 WEP キーでは、静的 WEP キーよりも強固なセキュリティが確保されます。

WEP キーの長さは、静的または動的のいずれの場合も、40 ビットまたは 128 ビットです。128 ビットの WEP キーでは、40 ビットのキーよりもセキュリティ レベルが高くなります。

静的 WEP キー

無線ネットワーク内の各デバイスには、最大 4 個の静的な WEP キーを指定できます。適切なキー（相互通信を行うすべてのデバイスで同一の WEP キー）で暗号化されていないパケットを受信すると、デバイスはそのパケットを廃棄し、宛先に送信しません。

静的 WEP キーは、書き込み専用の一時的なキーなので、クライアント アダプタから再び読み取ることはできず、クライアント アダプタの電源が切られたり Windows デバイスがリブートされると失われます。静的キーは一時的なものですが、クライアント アダプタを挿入するたび、あるいは Windows デバイスをリブートするたびに入力し直す必要はありません。これは、WEP キーが Windows デバイスのレジストリに保存されるためです。このキーは、セキュリティ上の理由により、暗号化された形で保存されます。ドライバは、クライアント アダプタのレジストリ パラメータをロードして読み取ると、静的 WEP キーを検出し、復号化して、アダプタの揮発性メモリに保存します。

EAP（動的 WEP キーを使用）

無線 LAN のセキュリティに関する新しい規格は、米国電気電子技術者協会（IEEE）で定義されているように、*802.1X for 802.11*、または簡単に *802.1X* と呼ばれています。802.1X とそのプロトコルである Extensible Authentication Protocol（EAP; 拡張認証プロトコル）をサポートしているアクセス ポイントは、無線クライアントと Remote Authentication Dial-In User Service（RADIUS）サーバなどの認証サーバ間のインターフェイスとして機能します。アクセス ポイントは、この認証サーバと有線ネットワークを介して通信します。

Windows XP でクライアント アダプタを設定する場合、次の 3 つの 802.1X 認証タイプを使用できます。

- **EAP-TLS**：この認証タイプは、オペレーティング システムを介して有効または無効にされ、動的でセッションベースの WEP キーを使用してデータを暗号化します。このキーは、クライアント アダプタおよび RADIUS サーバから得られます。

  EAP-TLS をサポートする RADIUS サーバには、Cisco Secure ACS バージョン 3.0 以降、Cisco Access Registrar バージョン 1.8 以降などがあります。

  （注）　EAP-TLS では、証明書を使用する必要があります。証明書のダウンロードとインストールについては、Microsoft の資料を参照してください。

- **Protected EAP**（または **PEAP**）：PEAP 認証は、無線 LAN 経由で One-Time Password（OTP）、Windows NT または 2000 ドメイン、LDAP ユーザ データベースをサポートするように設計されています。EAP-TLS 認証がベースとなっていますが、認証にクライアント証明書ではなくパスワードまたは PIN を使用します。また、オペレーティング システムにより有効または無効にされ、クライアント アダプタおよび RADIUS サーバから取り出された動的セッションベース WEP キーを使用してデータを暗号化します。PEAP 認証を使用する場合、ネットワークで OTP ユーザ データベースが使用されているときには、ハードウェア トークン パスワードまたはソフトウェア トークン PIN を入力し、EAP 認証プロセスを開始してネットワークにアクセスする必要があります。ネットワークで Windows NT または 2000 のドメイン ユーザ データベースあるいは LDAP ユーザ データベース（NDS など）が使用されている場合は、ユーザ名、パスワード、およびドメイン名を入力して認証プロセスを開始する必要があります。

  PEAP 認証をサポートする RADIUS サーバには、Cisco Secure ACS バージョン 3.1 以降、Cisco Access Registrar バージョン 3.5 以降などがあります。

  （注）　PEAP 認証を使用するには、インストールの際に PEAP サプリカントをインストールするか、Windows XP の Service Pack 1 をインストールする必要があります。この Service Pack には、Microsoft の PEAP サプリカントが収められています。このサプリカントは Windows のユーザ名とパスワードのみをサポートし、シスコの PEAP サプリカントとは相互運用性がありません。シスコの PEAP サプリカントを使用する場合、Service Pack 1 for Windows XP の後に ACU をインストールします。この順序でインストールしなければ、PEAP サプリカントは Microsoft の PEAP サプリカントで上書きされます。

- **EAP-SIM**：EAP-SIM 認証は、公衆無線 LAN で使用できるように設計されており、PCSC 準拠のスマートカード リーダーが装備されているクライアントが必要です。Install Wizard ファイルに含まれる EAP-SIM サプリカントがサポートするのは Gemplus SIM+ カードだけですが、標準の GSM-SIM カードや最新バージョンの EAP-SIM プロトコルをサポートする最新のサプリカントも使用できます。新しいサプリカントは、次の URL の Cisco.com からダウンロードできます。

  http://www.cisco.com/cgi-bin/tablebuild.pl/access-registrar-encrypted

  EAP-SIM 認証を正常に実行するためには上記の要件を満たす必要がありますが、それだけでは不十分です。通常は、ネットワーク内で EAP-SIM 認証をサポートする WLAN サービス プロバイダとサービス契約を結ぶ必要もあります。また、PCSC スマートカード リーダーは標準 GSM-SIM カードまたはチップを読み取ることができる場合もありますが、通常、EAP-SIM 認証では、サービス プロバイダが WLAN サービス用の GSM 携帯電話のアカウントを提供する必要があります。

EAP-SIM は、オペレーティング システムにより有効または無効にされ、クライアント アダプタおよび RADIUS サーバから取り出された動的セッションベース WEP キーを使用してデータを暗号化します。EAP-SIM は、SIM カードとの通信について、ユーザ検証コード、または PIN を入力することを要求します。PIN を、コンピュータに格納する、またはリブート後または認証が試行されるたびに入力が要求されるように選択できます。

EAP-SIM をサポートする RADIUS サーバには、Cisco Access Register バージョン 3.0 以降があります。

アクセス ポイントで Require EAP を有効にし、Windows XP を使用して EAP-TLS、PEAP、または EAP-SIM 向けにクライアント アダプタを設定すると、ネットワークに対する認証は、次の手順で実行されます。

1. クライアント アダプタがアクセス ポイントとアソシエートし、認証プロセスを開始します。

（注）　クライアントと　RADIUS　サーバの間で認証が成功するまで、クライアントはネットワークにフル アクセスできません。

2. クライアントと RADIUS サーバは、アクセス ポイント経由で通信し、認証用の共有秘密情報を使用して認証プロセスを実行します。この共有秘密情報とは、PEAP ではパスワード、EAP-TLS では証明書、EAP-SIM では SIM カードおよびサービス プロバイダの Authentication Center に保存されている内部キーです。パスワードまたは内部キーはプロセス中には送信されません。
3. 認証が成功すると、クライアントと RADIUS サーバは、クライアントに固有の動的なセッションベース WEP キーを取り出します。
4. RADIUS サーバは、有線 LAN 上の安全なチャネルを使用してアクセス ポイントにキーを送信します。
5. セッションの間、アクセス ポイントとクライアントはこのキーを使用して、相互に伝送するすべてのユニキャスト パケットの暗号化または復号化を行います。また、アクセス ポイントにブロードキャストが設定されている場合は、パケットをブロードキャストします。

（注）　802.1X 認証の詳細は、IEEE 802.11 規格を参照してください。RADIUS サーバの詳細は、次の URL を参照してください。
http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/secur_c/scprt2/scrad.htm

Wi-Fi Protected Access（WPA）

Wi-Fi Protected Access（WPA）は、従来または将来の無線 LAN システムのデータ保護やアクセス制御などのレベルを大幅に向上させた、規格ベースの相互運用可能なセキュリティの強化版です。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）やメッセージ完全性チェック（MIC）を使用し、認証済みキー管理に 802.1X を使用しています。

WPA では、WPA と WPA-Pre-shared key（WPA-PSK）の 2 種類の相互に排他的なキー管理がサポートされています。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。

WPA を使用するには、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。これらは次の URL からダウンロードできます。

- Service Pack 1：http://www.microsoft.com/WindowsXP/pro/downloads/servicepacks/sp1/default.asp
- 修正プログラム 815485：http://www.microsoft.com/downloads/details.aspx?FamilyID=009d8425-ce2b-47a4-abec-274845dc9e91&DisplayLang=en

EAP 認証を実行できる 350 シリーズと CB20A カードだけで WPA を使用できます。WPA はアクセス ポイントでも有効にする必要があります。

（注）　アクセス ポイントでは、Cisco IOS リリース 12.2(11)JA 以降を使用して WPA を有効化している必要があります。この機能を有効にする手順については、アクセス ポイントの資料を参照してください。

クライアント アダプタの設定

Windows XP でクライアント アダプタを設定する手順は、次のとおりです。

（注）　ACU をインストールしているにもかかわらず Windows XP を使用してクライアント アダプタを設定する場合は、ACU を起動して、Select Profile 画面で **Use Another Application To Configure My Wireless Network Settings** オプションが選択されていることを確認します。

（注）　これらの手順は、次のものを使用していることを想定しています。
- Windows XP Service Pack 1 および Microsoft サポート用修正プログラム 815485
- Windows XP のカテゴリ表示ではなくクラシック表示

Windows XP Service Pack 1 およびサポート用修正プログラム 815485 を使用していない場合、表示される画面がこの項で示されているものと異なる場合があります。これらのソフトウェアへのアップグレードを行わずに Windows XP でクライアント アダプタを設定する手順については、このマニュアルの OL-1394-06 バージョンを参照してください。

ステップ 1　クライアント アダプタのファームウェアおよびドライバがインストールされており、クライアント アダプタが Windows XP デバイスに挿入されていることを確認します。

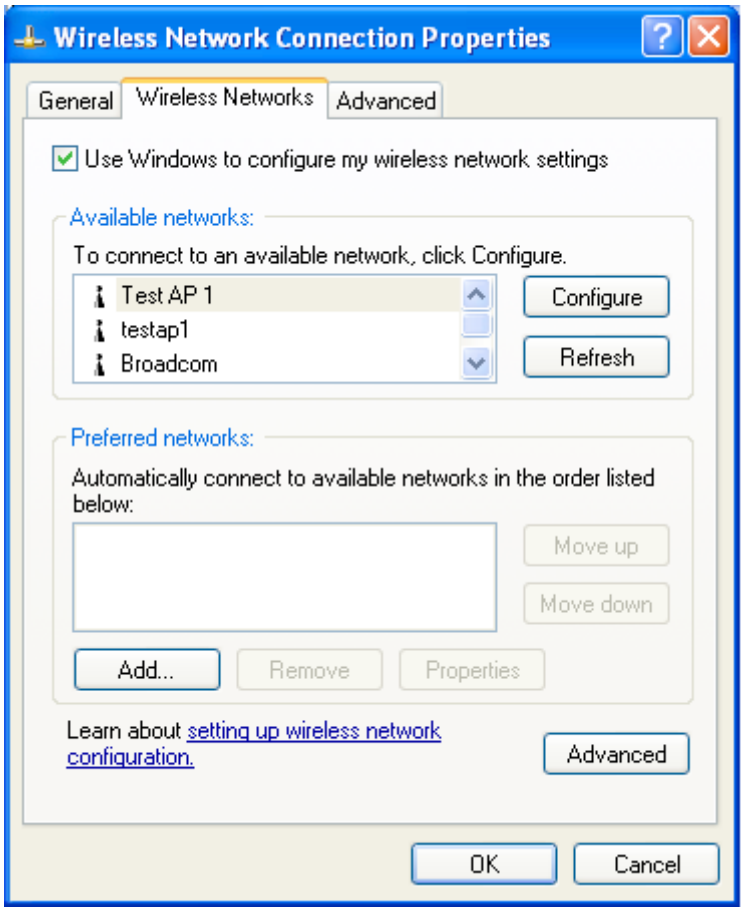
ステップ 2　**My Computer**、**Control Panel**、および **Network Connections** をダブルクリックします。

ステップ 3　**Wireless Network Connection** を右クリックします。

ステップ 4　**Properties** をクリックします。Wireless Network Connection Properties 画面が表示されます。

ステップ 5　**Wireless Networks** タブを選択します。次の画面が表示されます（図 D-1 を参照）。

図 D-1　Wireless Network Connection Properties 画面（Wirelss Networks タブ）



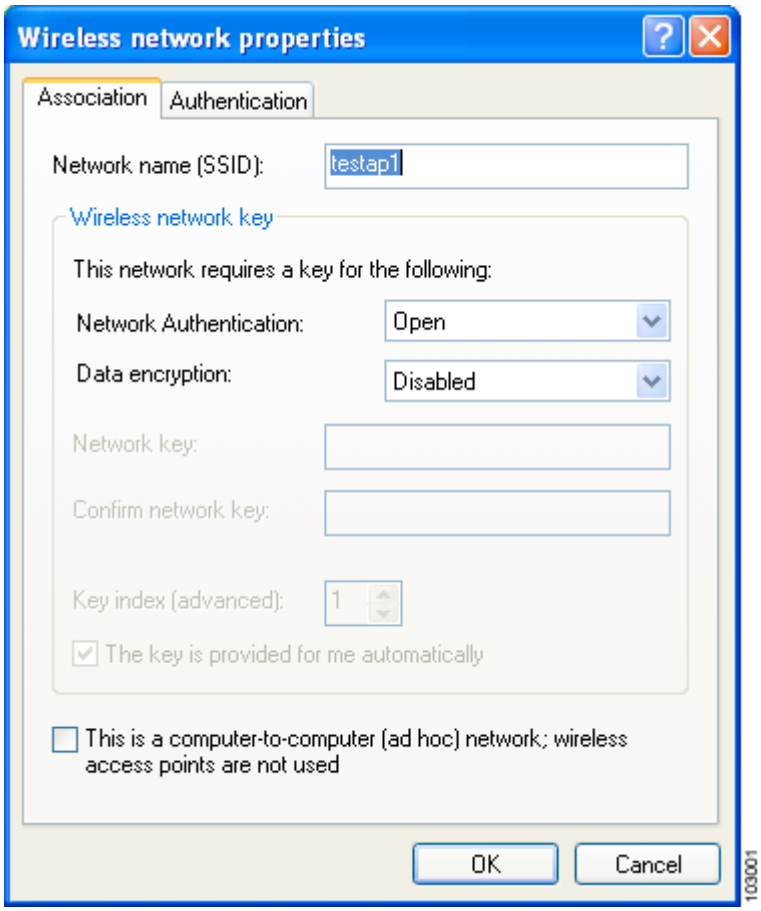
ステップ 6　**Use Windows to configure my wireless network settings** チェックボックスがオンになっていることを確認します。

ステップ 7　使用可能なネットワークのリストから、クライアント アダプタをアソシエートするアクセス ポイントの SSID をクリックし、**Configure** をクリックします。使用するアクセス ポイントの SSID がリストにない場合や、*アドホック ネットワーク*（アクセス ポイントを使用しない、一対一のコンピュータ間ネットワーク）でクライアント アダプタを使用する場合は、**Add** をクリックします。

（注）　使用可能なネットワークのリストに SSID を表示するには、該当のアクセス ポイントで Allow Broadcast SSID to Associate オプションを有効にする必要があります。

Wireless Network Properties 画面が表示されます（図 D-2 を参照）。

図 D-2　Wireless Network Properties 画面（Association タブ）



ステップ 8　次のいずれかを実行します。

- 使用可能なネットワークのリストから SSID を選択した場合は、SSID が Network name（SSID）フィールドに表示されることを確認します。
- Add をクリックした場合は、アクセス ポイントまたはクライアント アダプタをアソシエートするアドホック ネットワークの大文字と小文字を区別した SSID を Network name（SSID）フィールドに入力します。

ステップ 9　アドホック ネットワークでクライアント アダプタを使用する場合は、画面下部にある **This is a computer-to-computer (ad hoc mode) network; wireless access points are not used** チェックボックスをオンにします。

ステップ 10　Network Authentication ドロップダウン リストから、次のいずれかのオプションを選択します。

- **Open** : WEP の設定に関係なく、クライアント アダプタは、アクセス ポイントとの認証を行い、通信を試みることができます。静的な WEP を使用する場合、または WPA なしで EAP 認証を行う場合は、このオプションを選択することをお勧めします。
- **Shared** : クライアント アダプタは同じ WEP キーを持つアクセス ポイントだけと通信することができます。Shared Key 認証は、セキュリティ上のリスクが伴うので、使用しないことをお勧めします。

（注）　Shared key 認証では WEP キーが必要とされるにもかかわらず、EAP 認証が完了しないと EAP-TLS に対する WEP キーが設定されないので、EAP-TLS では Shared Key 認証を使用できません。

- **WPA**：WPA を有効にします。これにより、WPA を使用してクライアント アダプタをアクセス ポイントにアソシエートできます。
- **WPA-PSK**：WPA-PSK（WPA-Pre-shared key）を有効にします。これにより、WPA-PSK を使用してクライアント アダプタをアクセス ポイントにアソシエートできます。
- **WPA-None**：クライアントがアド ホック モードに設定されている場合に、クライアント アダプタの WPA を有効にします。

（注）　WPA および WPA-PSK の詳細は、「Wi-Fi Protected Access（WPA）」の項（P.D-4）を参照してください。

ステップ 11　Data encryption ドロップダウン リストから、次のいずれかのオプションを選択します。

- **Disabled**：クライアント アダプタでデータの暗号化を使用できません。Network Authentication で Open または Shared が選択されている場合だけこのオプションを選択できます。
- **WEP**：クライアント アダプタで静的または動的な WEP を使用できます。Open 認証の場合、このオプションを選択することをお勧めします。
- **TKIP**：クライアント アダプタで Temporal Key Integrity Protocol（TKIP）を使用できます。WPA または WPA-PSK の場合、このオプションを選択することをお勧めします。

ステップ 12　静的 WEP を使用する場合は、次の手順に従って、静的 WEP キーを入力します。

（注）　動的 WEP を使用する EAP-TLS、PEAP、または EAP-SIM 認証を使用する予定の場合は、ステップ 13 に進みます。

a. **The key is provided for me automatically** チェックボックスがオフになっていることを確認します。

b. アクセス ポイント（インフラストラクチャ ネットワーク内）またはその他のクライアント（アドホック ネットワーク内）の WEP キーをシステム管理者から取得し、Network key フィールドと Confirm network key フィールドの両方に入力します。新しい静的 WEP キーを入力するには、次のガイドラインに従ってください。

- WEP キーは、次の文字数で構成する必要があります。
  －40 ビットのキーでは 10 個の 16 進数または 5 個の ASCII テキスト文字
  　例：5A5A313859（16 進数）または ZZ18Y（ASCII 文字）
  －128 ビットのキーでは 26 個の 16 進数または 13 個の ASCII テキスト文字
  　例：5A5831353335545955493335 34（16 進数）または ZX1535TYUI354（ASCII 文字）

（注）　Cisco Aironet 1200 シリーズ アクセス ポイントで 5GHz クライアント アダプタを使用する場合、それらのアダプタに対して 16 進数を入力する必要があります。

- クライアント アダプタの WEP キーは、インフラストラクチャ モードの場合は通信先のアクセス ポイントと同じキーに、アドホック モードの場合は通信先のクライアントと同じキーに設定する必要があります。

c. Key index (advanced) フィールドで、作成する WEP キーの番号を選択します（1、2、3、または 4）。

（注）　クライアント アダプタとアクセス ポイント（インフラストラクチャ ネットワーク内）またはその他のクライアント（アドホック ネットワーク内）の両方に、同じ番号の WEP キーを割り当てる必要があります。

d. **OK** をクリックして設定を保存し、この SSID を Preferred networks（図 D-1 を参照）のリストに追加します。静的な WEP の設定はこれで完了です。クライアント アダプタは、ネットワークへのアソシエーションを、示された順序で自動的に試みます。

ステップ 13　WPA-PSK または WPA-None オプションを選択した場合、アクセス ポイント（インフラストラクチャ ネットワーク内）またはその他のクライアント（アドホック ネットワーク内）の事前共有キーをシステム管理者から取得し、Network key フィールドと Confirm network key フィールドの両方に入力します。次のガイドラインに従って事前共有キーを入力します。

- 事前共有キーには、8 ～ 63 文字の ASCII テキスト、または 64 桁の 16 進数が含まれている必要があります。

（注）　Cisco Aironet 1200 シリーズ アクセス ポイントで 5GHz クライアント アダプタを使用する場合、それらのアダプタに対して 16 進文字を入力する必要があります。

- お使いのクライアント アダプタの事前共有キーは、通信する予定のアクセス ポイント（インフラストラクチャ ネットワーク内）またはその他のクライアント（アドホック ネットワーク内）で使用されている事前共有キーと一致している必要があります。

ステップ 14　動的な WEP を使用する EAP-TLS、PEAP、または EAP-SIM 認証を使用する場合は、**The key is provided for me automatically** チェックボックスをオンにします。

（注）　WPA または WPA-PSK を選択している場合、このパラメータは使用できません。

ステップ 15　EAP 認証を使用する場合は、次のいずれかを実行します。

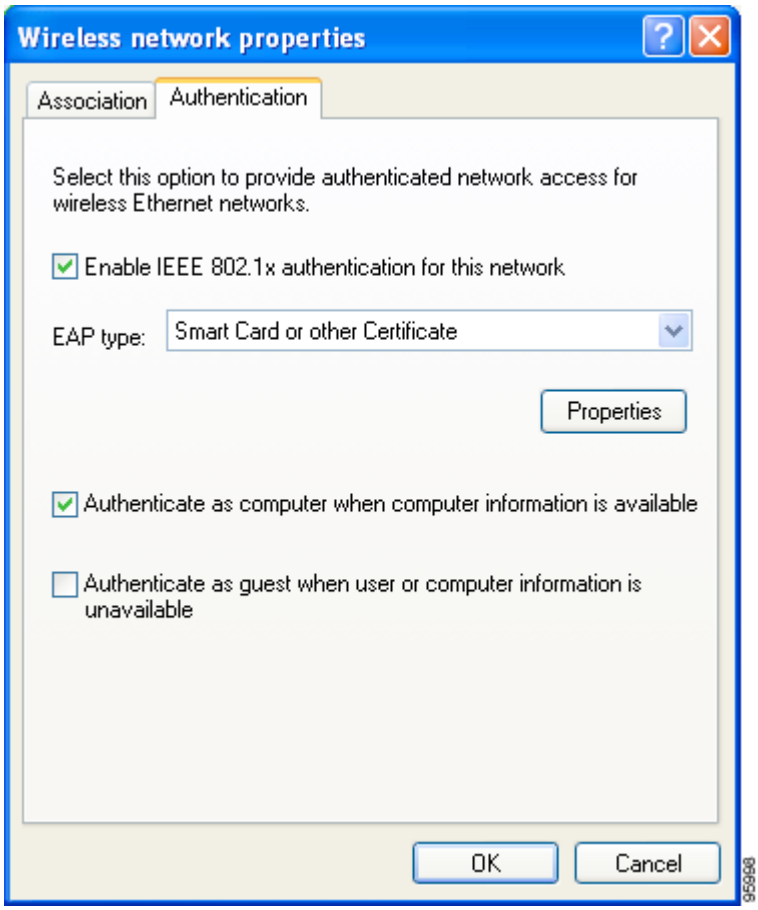
- EAP-TLS 認証を使用する予定の場合は、次の「EAP-TLS 認証の有効化」の項の手順に従ってください。
- PEAP 認証を使用する予定の場合は、「PEAP 認証の有効化」の項（P.D-14）の手順に従ってください。
- EAP-SIM 認証を使用する予定の場合は、「EAP-SIM 認証の有効化」の項（P.D-17）の手順に従ってください。

EAP-TLS 認証の有効化

初期設定が完了した後、次の手順に従って、クライアント アダプタが EAP-TLS 認証を使用するための準備を行います。

ステップ 1　Wireless Network Properties 画面で **Authentication** タブをクリックします。次の画面が表示されます（図 D-3 を参照）。

図 D-3　Wireless Network Properties 画面（Authentication タブ）

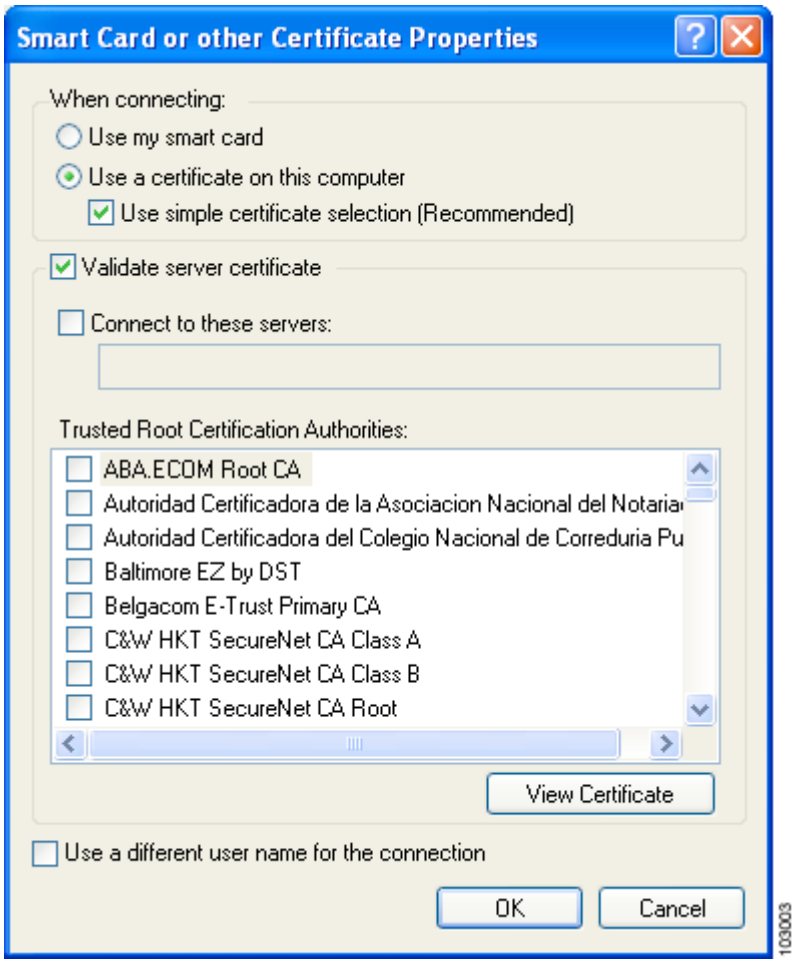


ステップ 2　Association 画面で WPA または WPA-PSK オプションを選択していない場合は、**Enable IEEE 802.1x authentication for this network** チェックボックスをオンにします。

ステップ 3　EAP タイプには、**Smart Card or other Certificate** を選択します。

ステップ 4　**Properties** をクリックします。Smart Card or Other Certificate Properties 画面が表示されます（図 D-4 を参照）。

図 D-4　Smart Card or Other Certificate Properties 画面



ステップ 5　**Use a certificate on this computer** オプションを選択します。

ステップ 6　**Use simple certificate selection (Recommended)** チェックボックスをオンにします。

ステップ 7　サーバの証明書評価が必要な場合は、**Validate server certificate** チェックボックスをオンにします。

ステップ 8　接続するサーバ名を指定する場合は、**Connect to these servers** チェックボックスをオンにし、チェックボックス内のフィールドに適切なサーバ名を入力します。

（注）　サーバ名を入力し、入力したサーバ名と一致しないサーバにクライアント アダプタが接続した場合、認証プロセスの間に接続の受け付けまたはキャンセルを選択するプロンプトが表示されます。

（注）　このフィールドを空白にすると、サーバ名が確認されず、証明書が有効な間は接続が設定されます。

ステップ 9　Trusted Root Certification Authorities フィールドで、サーバ証明書をダウンロードした認証局の名前の隣にあるチェックボックスをオンにします。

（注）　このチェックボックスがオフのままの場合、認証プロセス中に、ルート証明機関への接続を承認するように指示されます。

ステップ 10　**OK** を 3 回クリックして、設定を保存します。これで、設定は完了です。

ステップ 11　「EAP 認証プロセスを開始するには証明書の受け入れが必要である」という意味のポップアップ メッセージがシステム トレイの上に表示された場合は、メッセージをクリックし、その指示に従って証明書を受け入れます。

（注）　以後は、認証の際に証明書を受け入れるように指示されることはありません。1 つを受け入れると、次から同じ証明書が使用されます。

ステップ 12　サーバの証明書用のルート証明機関を示すメッセージが表示されるので、それが正しい認証機関の場合は、**OK** をクリックして接続を受け付けます。そうでない場合は、**Cancel** をクリックしてください。

ステップ 13　クライアント アダプタが接続されるサーバを示すメッセージが表示されるので、それが正しい接続先サーバの場合は、**OK** をクリックして接続を受け付けます。そうでない場合は、**Cancel** をクリックしてください。

これで、クライアント アダプタは EAP 認証を行います。

（注）　コンピュータをリブートして Windows ユーザ名およびパスワードを入力するたびに、EAP 認証プロセスが自動的に開始され、クライアント アダプタは EAP 認証を行います。

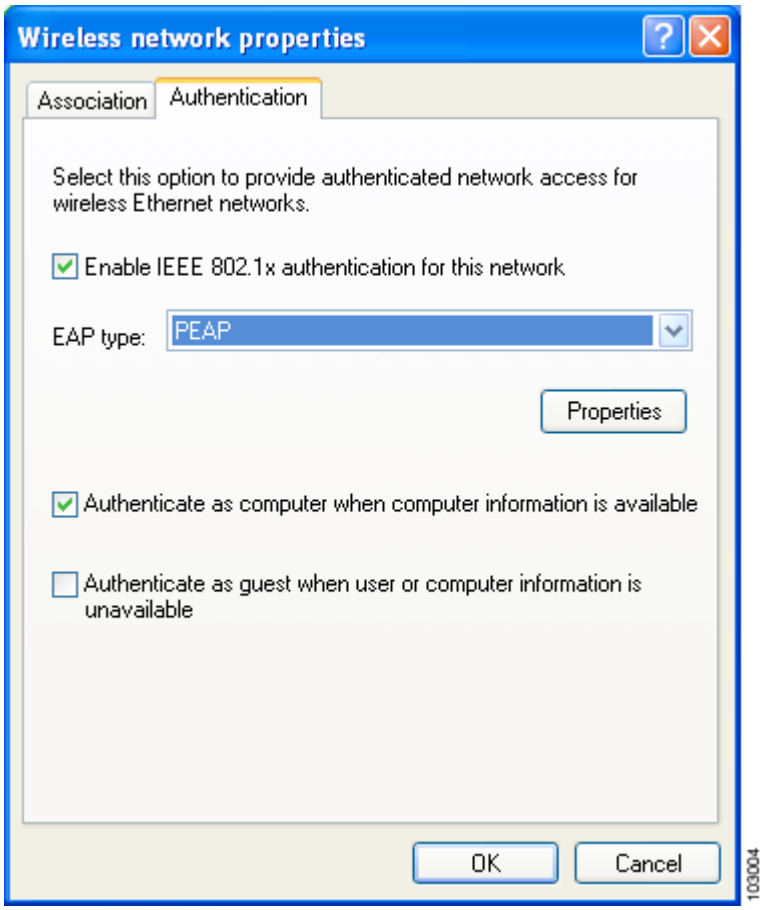
ステップ 14　認証を検証するには、**My Computer**、**Control Panel**、**Network Connections** の順にダブルクリックします。ステータスが Wireless Network Connection の右側に表示されます。**View** および **Refresh** をクリックして、現在のステータスを取得してください。クライアント アダプタが認証された場合、ステータスは *Authentication succeeded* になります。

PEAP 認証の有効化

初期設定が完了したら、次の手順に従って、クライアント アダプタが PEAP 認証を使用するための準備をします。

ステップ 1　Wireless Network Properties 画面で **Authentication** タブをクリックします。次の画面が表示されます（図 D-5 を参照）。

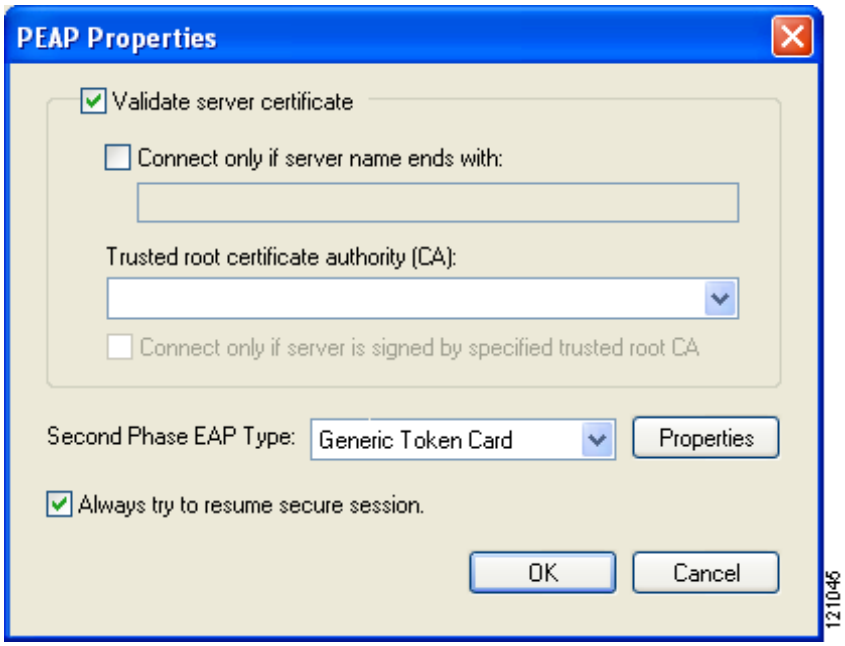
図 D-5　Wireless Network Properties 画面（Authentication タブ）



ステップ 2　Association 画面で WPA または WPA-PSK オプションを選択していない場合は、**Enable IEEE 802.1x authentication for this network** チェックボックスをオンにします。

ステップ 3　EAP タイプの場合は、**PEAP** を選択します。**Properties** をクリックします。PEAP Properties 画面が表示されます（図 D-6 を参照）。

図 D-6　PEAP Properties 画面



ステップ 4　サーバの証明書評価が必要な場合は **Validate server certificate** チェックボックスをオンにします（推奨）。

ステップ 5　接続するサーバ名を指定する場合は、**Connect only if server name ends with** チェックボックスをオンにし、チェックボックスの下にあるフィールドに該当サーバ名の接尾辞を入力します。

（注）　サーバ名を入力し、入力したサーバ名と一致しないサーバにクライアント アダプタが接続した場合、認証プロセスの間に接続の受け付けまたはキャンセルを選択するプロンプトが表示されます。

（注）　このフィールドを空白にすると、サーバ名が確認されず、証明書が有効な間は接続が設定されます。

ステップ 6　サーバ証明書をダウンロードした認証機関の名前が Trusted root certificate authority（CA）フィールドに表示されていることを確認します。必要に応じて、ドロップダウン メニューで矢印をクリックして適切な名前を選択します。

（注）　このフィールドが空白の場合、認証プロセス中に、ルート証明機関への接続を承認するように指示されます。

ステップ 7　上記のフィールドで指定した信頼できるルート証明書を証明サーバが必ず使用するようにするには、**Connect only if server is signed by specified trusted root CA** チェックボックスをオンにします。これによって、クライアントと不正なアクセス ポイントとの接続を防止できます。

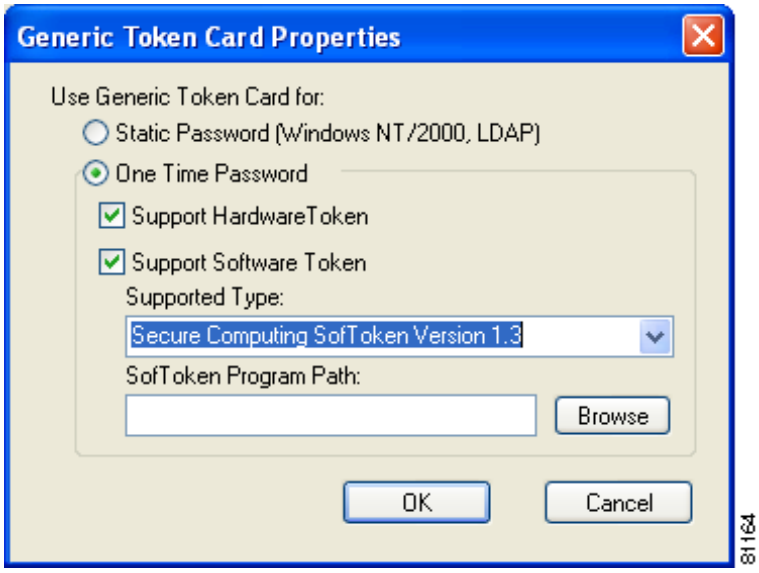
ステップ 8　次のいずれかを実行します。

- PEAP プロトコルがユーザにクレデンシャルの再入力を要求する前に常に以前のセッションの再開を試みるようにする場合は、**Always try to resume secure session** チェックボックスをオンにします。
- クライアント アダプタの無線のアソシエーション解除時（カードが取り出される、無線がオフになる、アクセス ポイントの範囲外になる、プロファイルを切り替えるなどの場合）にユーザ名とパスワードの再入力が要求されるようにする場合は、**Always try to resume secure session** チェックボックスをオフにします。

（注）　このチェックボックスをオンにすると、クライアント アダプタのアソシエーションが一時的に解除されたときに、ユーザ名とパスワードを再入力する手間が省けます。Cisco Secure ACS System Configuration - Global Authentication Setup 画面の PEAP Session Timeout の設定によって、レジューム機能を有効にする期間（ユーザ クレデンシャルを再入力しなくても PEAP セッションをレジュームできる期間）が制御されます。このタイムアウト期間中にデバイスから離れると、他のユーザが PEAP セッションをレジュームしてネットワークにアクセス可能になるので注意してください。

ステップ 9　現在、使用可能な第 2 フェーズの EAP タイプは、Generic Token Card だけです。**Properties** をクリックします。Generic Token Card Properties 画面が表示されます（図 D-7 を参照）。

図 D-7　Generic Token Card Properties 画面



ステップ 10　ユーザ データベースに応じて、**Static Password (Windows NT/2000, LDAP)** または **One Time Password** オプションを選択します。

ステップ 11　次のいずれかを実行します。

- ステップ 10 で **Static Password (Windows NT/2000, LDAP)** オプションを選択した場合は、ステップ 12 に進みます。
- ステップ 10 で **One Time Password** オプションを選択した場合、次のチェックボックスのいずれか、または両方をオンにし、1 回限りのパスワードでサポートされるトークンの種類を指定します。

- **Support Hardware Token**：ハードウェア トークン デバイスは 1 回限りのパスワードを取得します。各自のハードウェア トークン デバイスを使用して 1 回限りのパスワードを取得し、ユーザ クレデンシャルの入力が要求された場合はそのパスワードを入力する必要があります。
- **Support Software Token**：PEAP サプリカントは、ソフトウェア トークン プログラムで動作して、1 回限りのパスワードを取得します。1 回限りのパスワードではなく、PIN だけを入力します。このチェックボックスをオンにした場合、Supported Type ドロップダウン ボックスから、クライアントにインストールされているソフトウェア トークン ソフトウェア（Secure Computing SofToken バージョン 1.3、Secure Computing SofToken II 2.0、RSA SecurID Software Token v 2.5 など）も選択する必要があります。ここで Secure Computing SofToken バージョン 1.3 を選択した場合は、Browse ボタンを使用してソフトウェア プログラムのパスを見つける必要があります。

（注）　SofToken Program Path フィールドは、Secure Computing SofToken バージョン 1.3 以外のソフトウェア トークン プログラムを選択した場合は使用できません。

ステップ 12　**OK** を 4 回クリックして、設定を保存します。これで、設定は完了です。

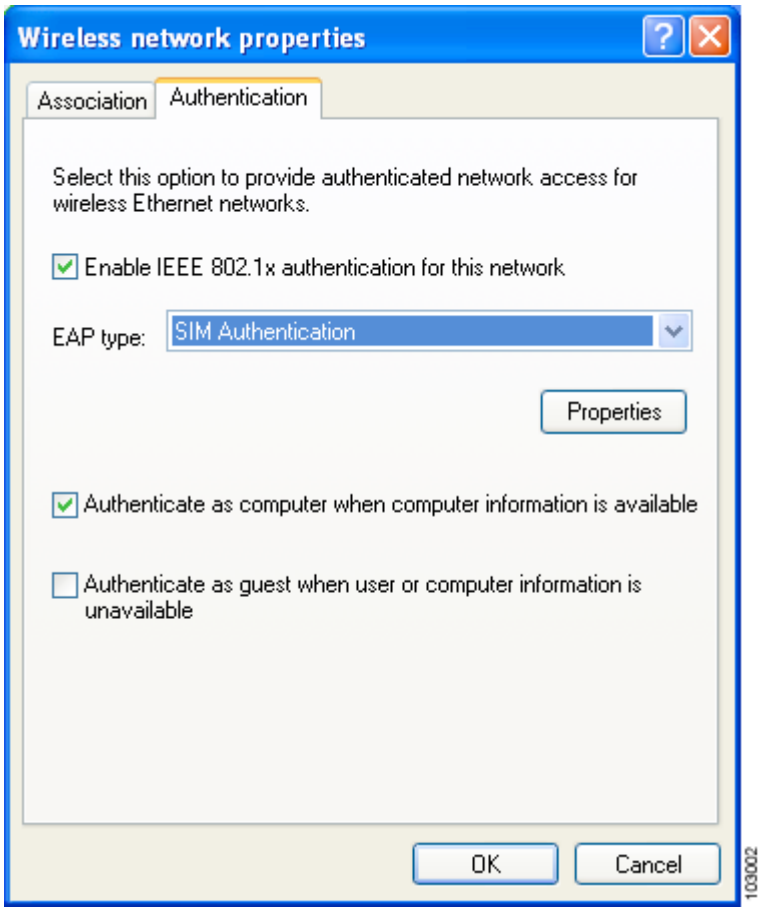
ステップ 13　PEAP による認証手順については、「PEAP の使用方法」の項（P.6-23）を参照してください。

EAP-SIM 認証の有効化

初期設定が完了した後、次の手順に従って、クライアント アダプタが EAP-SIM 認証を使用するための準備を行います。

ステップ 1　Wireless Network Properties 画面で **Authentication** タブをクリックします。次の画面が表示されます（図 D-8 を参照）。

図 D-8　Wireless Network Properties 画面（Authentication タブ）

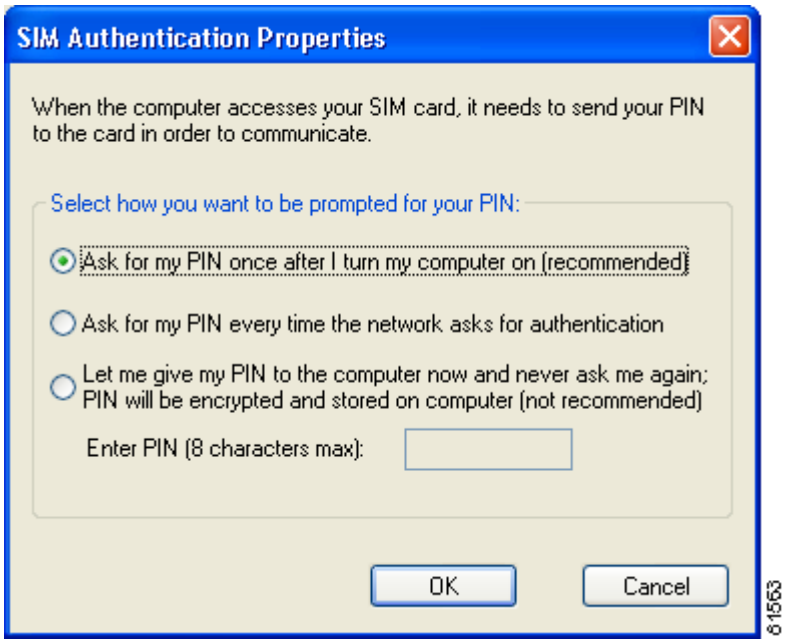


ステップ 2　Association 画面で WPA または WPA-PSK オプションを選択していない場合は、**Enable IEEE 802.1x authentication for this network** チェックボックスをオンにします。

ステップ 3　EAP タイプの場合は、**SIM Authentication** を選択します。

ステップ 4　**Properties** をクリックします。SIM Authentication Properties 画面が表示されます（図 D-9 を参照）。

図 D-9　SIM Authentication Properties 画面



ステップ 5　SIM のリソース（データまたはコマンド）にアクセスする場合は、EAP-SIM サプリカントから SIM カードに有効な PIN が提供されなければなりません。この PIN は SIM に保存された PIN と一致する必要があります。次のオプションのいずれかを選択し、EAP-SIM サプリカントが SIM カードの PIN を処理する方法を指定します。

- **Ask for my PIN once after I turn my computer on（recommended）**：ソフトウェアは PIN を永続的に保存しません。各セッションの最初の認証で、ソフトウェアから PIN の入力が 1 度要求されます。セッションは起動からシャットダウンまたはリブートまでの時間として定義されます。
- **Ask for my PIN every time the network asks for authentication**：ソフトウェアは PIN を保存しません。EAP-SIM 認証が実行されるたびに PIN の入力が要求されます。クライアントがアクセス ポイント間をローミングする場合、またはセッションのタイムアウトが指定されている場合（アカウンティングおよびセキュリティを目的とした場合など）は、このオプションの選択はお勧めできません。
- **Let me give my PIN to the computer now and never ask me again; PIN will be encrypted and stored on computer (not recommended)**：このオプションの下の Enter PIN 編集ボックスに、PIN を 1 回だけ入力する必要があります。ソフトウェアはレジストリに PIN を保存し、要求された場合にレジストリからその PIN を取り出します。このオプションを選択した場合、この時点で PIN を入力する必要があります。PIN は認証が試みられたときに評価されます。

（注）　このオプションは、他のユーザが PIN を知らなくても SIM を使用できるのでお勧めできません。

ステップ 6　**OK** を 3 回クリックして、設定を保存します。これで、設定は完了です。

コンピュータのレジストリに PIN を保存するように選択している場合、EAP 認証プロセスは自動的に開始し、クライアント アダプタは EAP 認証を行い、保存された PIN を使用して SIM カードにアクセスします。

（注）　保存された PIN が間違っているために、SIM で拒否された場合、EAP-SIM サプリカントは一時的にプロンプト モードをデフォルト設定（Ask for my PIN once after I turn my computer on）に変更し、SIM がロックアップするのを防ぎます。手動で変更している場合を除き、この設定はコンピュータの電源を切るまで継続します。SIM Authentication Properties 画面で保存された PIN を変更します。

電源投入またはリブート後、あるいは認証要求のたびに PIN の入力が要求される設定を選択した場合、Windows システム トレイの上に、ネットワークへのアクセスのためにクレデンシャルの入力を要求するポップアップ メッセージが表示されます。メッセージをクリックし、PIN を入力して **OK** をクリックします。これで、クライアント アダプタは EAP 認証を行います。

ステップ 7　認証を検証するには、**My Computer**、**Control Panel**、**Network Connections** の順にダブルクリックします。ステータスが Wireless Network Connection の右側に表示されます。**View** および **Refresh** をクリックして、現在のステータスを取得してください。クライアント アダプタが認証された場合、ステータスは *Authentication succeeded* になります。

（注）　認証がまだ保留状態にあるか、認証サーバが応答しない場合、ACU と Windows XP のシステム トレイ上の Windows Wireless Network Connection アイコンには接続ステータスが表示されます。

Wi-Fi Multimedia の有効化

Wi-Fi Multimedia（WMM）は、Quality of Service（QoS）のための IEEE 802.11e 無線 LAN 規格の一部です。プライオリティ タギングとキューイングをサポートします。QoS はアクセス ポイントの機能であり、ネットワークの専門家はこの機能を使用して、特定のトラフィックが他のトラフィックよりも優先的に処理されるようにできます。QoS を使用しない場合、アクセス ポイントは、パケットの内容やサイズに関係なく、各パケットにベストエフォート サービスを提供します。無線 LAN に QoS を実装すると、ネットワーク パフォーマンスの予測が容易になり、帯域幅を効果的に使用できます。

音声やビデオのような QoS 対応クライアント向けの時間依存のアプリケーション（Cisco IP SoftPhone など）がコンピュータで実行されている場合は、WMM を有効にすることをお勧めします。

QoS および WMM は、クライアントがアソシエートするアクセス ポイントで有効にする必要があります。これらの機能は、Cisco IOS リリース 12.3(2)JA 以降のアクセス ポイントでサポートされています。これらの機能を有効にする手順については、アクセス ポイントの資料を参照してください。

WMM は、クライアント アダプタ ファームウェア バージョン 5.60.08、PC/LM/PCI カード ドライバ バージョン 8.6、および mini PCI/CB20A カード ドライバ バージョン 3.9 で自動的にサポートされます。これらのソフトウェアは、Install Wizard バージョン 1.5 以降に付属しています。ただし、WMM のサポートを実現するには、Windows QoS パケット スケジューラを有効にする必要があります。

Windows XP が実行されているコンピュータで QoS Packet Scheduler を有効にする手順は、次のとおりです。

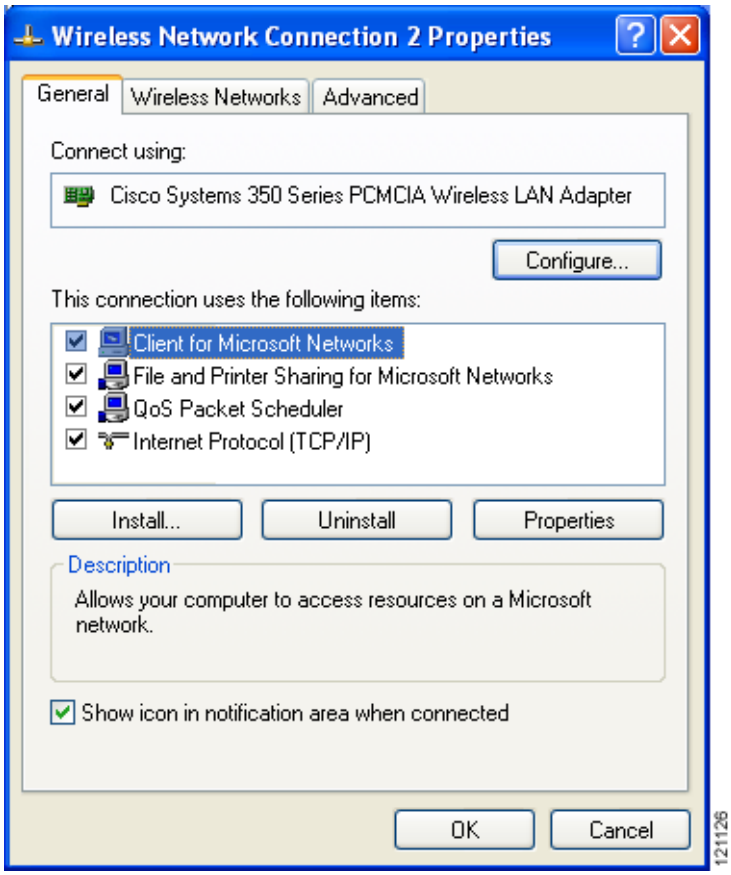
ステップ 1　**Control Panel** をダブルクリックします。

ステップ 2　**Network Connections** をクリックします。

ステップ 3　Wireless Network Connection を右クリックします。

ステップ 4　**Properties** をクリックします。Wireless Network Connection Properties 画面が表示されます（図 D-10 を参照）。

図 D-10　Wireless Network Connection Properties 画面



ステップ 5　その接続で使用される項目のリストに表示される **QoS Packet Scheduler** チェックボックスをオンにします。

ステップ 6　**OK** をクリックします。

Windows XP によるアクセス ポイントとのアソシエーション

Windows XP では、クライアント アダプタのドライバは、優先するネットワーク（図 D-1 を参照）のリスト内の最初のネットワークへのアソシエーションを自動的に試行します。アダプタがアソシエーションに失敗するか、アソシエーションが失われると、preferred networks のリスト内の次のネットワークに自動的に切り替わります。アクセス ポイントにアソシエートされている限り、アダプタはネットワークを切り替えません。クライアント アダプタを強制的に別のアクセス ポイントにアソシエートするには、使用可能なネットワークのリストから別のネットワークを選択する必要があります（**Configure** および **OK** をクリックします）。

クライアント アダプタの現在のステータスの表示

クライアント アダプタのステータスを表示するには、Windows のシステム トレイにある、2 台のコンピュータが接続されているアイコンをクリックします。Wireless Network Connection Status 画面が表示されます（図 D-11 を参照）。

図 D-11　Wireless Network Connection Status 画面