無線 LAN の
セキュリティ設定マニュアル

第 4 版

2007 年 4 月

はじめに

このマニュアルは、無線 LAN（IEEE 802.11a 準拠、IEEE 802.11b 準拠、IEEE 802.11g 準拠）通信のセキュリティ環境の構築方法について説明しています。

2007 年 4 月

このマニュアルの表記について

■本文中の記号

表：本文中の記号

記号	意味
重要	お使いになるときに注意していただきたいことや、してはいけないことを記述しています。必ずお読みください。
POINT	操作に関連することを記述しています。必要に応じてお読みください。

■画面例およびイラスト

表記されている画面およびイラストは一例です。お使いの機種や状況によって、画面およびイラストが一部異なることがあります。

■製品の呼び方

本文中の製品名称を、次のように略して表記します。
なお、このマニュアルではお使いの OS 以外の情報もありますが、ご了承ください。

表：製品名称などの表記

製品名称	本書での表記	
Windows Vista™ Ultimate	Windows Vista	Windows
Windows Vista™ Enterprise		
Windows Vista™ Business		
Windows Vista™ Home Premium		
Windows Vista™ Home Basic		
Microsoft® Windows® XP Professional	Windows XP	
Microsoft® Windows® XP Home Edition		
Microsoft® Windows® XP Media Center Edition 2004		
Microsoft® Windows® XP Media Center Edition 2005		
Microsoft® Windows® XP Tablet PC Edition		
Microsoft® Windows® XP Tablet PC Edition 2005		
Microsoft® Windows® 2000 Professional	Windows 2000	
Microsoft® Windows® 2000 Server	Windows 2000 Server	
Microsoft® Windows Server™ 2003, Standard Edition	Windows Server 2003	

表：製品名称などの表記

製品名称	本書での表記	
ワイヤレス LAN ステーション FMWT-56AG	FMWT-56AG	無線LANアクセスポイント
ワイヤレス LAN ステーション FMWT-55AG	FMWT-55AG	
ワイヤレス LAN ステーション FMWT-54AG	FMWT-54AG	
ワイヤレス LAN ステーション FMWT-53A	FMWT-53 シリーズ	
ワイヤレス LAN ステーション FMWT-53G		
ワイヤレス LAN ステーション FMWT-52A	FMWT-52 シリーズ	
ワイヤレス LAN ステーション FMWT-52B		
ワイヤレス LAN ステーション FMWT-52AB		
ワイヤレス LAN ステーション FMWT-52BB		
ワイヤレスブロードバンドルータ FMWBR-201	FMWBR-201	
ワイヤレスブロードバンドルータ FMWBR-102	FMWBR-102	
ワイヤレスブロードバンドルータ FMWBR-101	FMWBR-101	
ワイヤレス LAN ステーション FMWT-501	FMWT-501	
ワイヤレス LAN カード FMV-JW482	FMV-JW482	
ワイヤレス LAN カード FMV-JW481	FMV-JW481	
ワイヤレス LAN カード FMV-JW183	FMV-JW183	

■商標について

セキュリティの表記について

このマニュアルではセキュリティの設定に関する表記を、次の表のように記載します。

表：このマニュアルのセキュリティの設定に関する表記

本書での表記	製品で使用されている表記 または『無線 LAN のセキュリティ設定マニュアル 第３版』での表記
WPA-PSK	WPA-PSK WPA- パーソナル
WPA2-PSK	WPA2-PSK 802.11i (WPA2)-PSK WPA2- パーソナル
WPA-PSK ／ WPA2-PSK	WPA/WPA2 パスフレーズ
WPA	WPA WPA-RADIUS WPA- エンタープライズ
WPA2	WPA2 802.11i (WPA2) WPA2- エンタープライズ
WPA ／ WPA2	WPA ／ WPA2
EAP-TLS	スマートカードまたはその他の証明書 EAP-TLS TLS
PEAP-MSCHAPv2	セキュリティで保護されたパスワード（EAP-MSCHAP v2） PEAP（EAP-MSCHAP V2） PEAP-MSCHAP-V2 PEAP［注 1］
PEAP-TLS	PEAP（EAP-TLS）

注 1　認証に TLS を使用する PEAP-TLS 以外

無線 LAN 製品ご使用時におけるセキュリティに関するご注意

重要

・お客様の権利（プライバシー保護）に関する重要な事項です。

無線 LAN では、LAN ケーブルを使用する代わりに、電波を利用してパソコンなどと無線 LAN アクセスポイント（ワイヤレス LAN ステーション、ワイヤレスブロードバンドルータ、ファミリーネットワークステーションなど）間で情報のやり取りを行うため、電波の届く範囲であれば自由に LAN 接続が可能であるという利点があります。
その反面、電波はある範囲内であれば障害物（壁など）を越えてすべての場所に届くため、セキュリティに関する設定を行っていない場合、以下のような問題が発生する可能性があります。

・通信内容を盗み見られる
悪意ある第三者が、電波を故意に傍受し、
- ID やパスワード又はクレジットカード番号などの個人情報
- メールの内容

などの通信内容を盗み見られる可能性があります。

・不正に侵入される
悪意ある第三者が、無断で個人や会社内のネットワークへアクセスし、
- 個人情報や機密情報を取り出す（情報漏洩）
- 特定の人物になりすまして通信し、不正な情報を流す（なりすまし）
- 傍受した通信内容を書き換えて発信する（改ざん）
- コンピュータウィルスなどを流しデータやシステムを破壊する（破壊）

などの行為をされてしまう可能性があります。

本来、無線 LAN カードや無線 LAN アクセスポイントは、これらの問題に対応するためのセキュリティの仕組みを持っていますので、無線 LAN 製品のセキュリティに関する設定を行って製品を使用することで、その問題が発生する可能性は少なくなります。
無線 LAN 製品は、購入直後の状態においては、セキュリティに関する設定が施されていない場合があります。
したがって、お客様がセキュリティ問題発生の可能性を少なくするためには、無線 LAN カードや無線 LAN アクセスポイントをご使用になる前に、必ず無線 LAN 製品のセキュリティに関するすべての設定を取扱説明書に従って行ってください。
なお、無線 LAN の仕様上、特殊な方法によりセキュリティ設定が破られることもあり得ますので、ご理解のうえ、ご使用ください。
セキュリティの設定などについて、お客様ご自身で対処できない場合には、「富士通パーソナル製品に関するお問合せ窓口」までお問い合わせください。
当社では、お客様がセキュリティの設定を行わないで使用した場合の問題を充分理解したうえで、お客様自身の判断と責任においてセキュリティに関する設定を行い、製品を使用することをお奨めします。
セキュリティ対策を施さず、あるいは、無線 LAN の仕様上やむを得ない事情によりセキュリティの問題が発生した場合、当社は、これによって生じた損害に対する責任を負いかねます。

目次

1

第 1 章

概要

無線 LAN のセキュリティを設定する前に、ご確認いただきたいことを説明します。

1 無線 LAN のセキュリティについて

無線 LAN の通信は、ユーザー認証とデータの暗号化によって、セキュリティを守ります。ユーザー認証とデータの暗号化にはそれぞれいくつか種類があります。

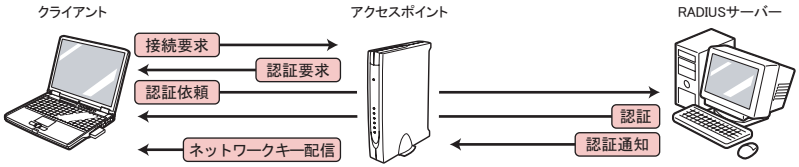
認証方式と暗号化

認証方式とデータの暗号化について説明します。

従来の WEP では、無線 LAN アクセスポイントとクライアントに設定した固定のネットワークキーを使用してデータを暗号化することで、無線 LAN 通信のデータを第三者に解読されないようにしています。しかし、固定のネットワークキーを使用するため、同じキーを長い間使い続けていると、ネットワークキーの値を解読されてしまう恐れがあります。また、キーの値を変更する場合は、無線 LAN アクセスポイントとすべてのクライアントのパソコンの設定を手動で変更しなければならないため、大規模なネットワークの場合は大変な労力を必要とします。

そこで、IEEE 802.1X や WPA では、ネットワークに接続を要求するクライアントの認証を行い、認証に成功したクライアントだけに、無線 LAN アクセスポイントが自動生成したネットワークキーを配信する、という方法を使っています。また、そのネットワークキーの値を一定の間隔で変更することもできます。認証に成功し、ネットワークキーを受け取ったクライアントだけが、無線 LAN アクセスポイントを介したネットワークと通信が行えるようになります。こうして、無線 LAN のセキュリティレベルをより高くしています。

次の図は、セキュリティの方法に IEEE 802.1X や WPA を使用した場合に、クライアントがネットワークに接続要求をしてから、ネットワークキーを受け取るまでの大まかな流れです。



■認証方式について

認証方式には、いくつかの種類があります。認証方式によって証明書を使う方法や、ユーザー名／パスワードを使用する方法などがあります。

・EAP-TLS

EAP-TLS では、RADIUS サーバーとクライアントの相互で証明書による認証を行います。

RADIUS サーバーが、証明書を取得したときのユーザー名と証明書の情報をクライアントに送信します。クライアントは、RADIUS サーバーから送られてきた情報が、クライアント自身の持つ証明機関の情報と一致するか確認します。これが RADIUS サーバーの認証になります。

次に、クライアントは、証明書を取得したときのユーザー名と証明書の情報を RADIUS サーバーに送信します。RADIUS サーバーは、クライアントから送られてきた情報が、RADIUS サーバー自身の持つ証明機関の情報と一致するか確認します。これがクライアントの認証になります。

・PEAP-MSCHAPv2

PEAP-MSCHAPv2 では、認証に証明書とユーザー名／パスワードを使用します。

RADIUS サーバーがクライアントを認証する時はユーザー名／パスワードを使用します。

ユーザー名／パスワードの情報は、EAP-MSCHAP v2 で暗号化されます。

クライアントが RADIUS サーバーを認証するときは証明書を使用します。

・PEAP-TLS

PEAP-TLS では、EAP-TLS と同様に、RADIUS サーバーとクライアントの相互で証明書による認証を行います。

PEAP-TLS では暗号化情報がカプセル化されるため、EAP-TLS よりセキュリティレベルが高くなります。

■クライアント証明書の種類について

クライアント証明書には、ユーザーアカウントごとに発行される「ユーザー証明書」と、コンピューターアカウントに発行される「コンピューター証明書」の 2 種類があります。

EAP-TLS や PEAP-TLS などクライアントの認証に証明書を使用する認証方式で、ドメインログオンなど、ユーザーが Windows にログオンする前から通信する必要がある場合には、コンピューター証明書が必要になります。

・ユーザー証明書

コンピューターを使用する 1 ユーザーアカウントに対して発行される証明書です。同じコンピューターを別のユーザーアカウントで使用する場合は、再度ユーザー証明書を取得する必要があります。

・コンピューター証明書

コンピューターに対して発行される証明書です。同じコンピューターを使用する場合、異なるユーザーアカウントでも利用できます。

■シングルサインオンについて

Windows にログオンするユーザー名とパスワード、またはドメインにログオンするユーザー名とパスワードを無線 LAN の認証に使用します。PEAP-MSCHAPv2 など、認証にユーザー名とパスワードを使用する認証方式で使用できます。

■データの暗号化について

データの暗号化には、通常ネットワークキーを使用します。ネットワークキーを使ってデータの暗号化と復号化を行うため、通信を行う者同士でネットワークキーが一致していないと通信が行えないようになっています。従来の WEP は、この値を固定で設定していましたが、セキュリティの種類によってこの値を可変にすることでセキュリティレベルを高くしています。

IEEE 802.1X では、ネットワークキーの値を一定間隔で自動的に変更することができます。これにより、ネットワークキーに固定値を使用している場合より解読されにくくしています。

WPA では、暗号化方式に TKIP（Temporal Key Integrity Protocol）を使用し、1 パケットごとにネットワークキーを変更します。これによりネットワークキーを解読されにくくしています。また、WPA に対応した製品の中には TKIP よりセキュリティレベルの高い AES という暗号化方式を使用できるものもあります。

セキュリティパターンの種類

ユーザー認証方式と通信データの暗号化方式の組み合せによって、次のようなセキュリティのパターンがあります。それぞれのセキュリティパターンの特長と認証の流れを説明します。

- IEEE 802.1X ＋ EAP-TLS
  認証に RADIUS サーバーを使用します。認証方式は EAP-TLS、通信データの暗号化方式は WEP となります。
  特長と認証の流れは、「IEEE 802.1X ＋ EAP-TLS」（→ P.16）をご覧ください。
- IEEE 802.1X ＋ PEAP-MSCHAPv2
  認証に RADIUS サーバーを使用します。認証方式は PEAP-MSCHAPv2、通信データの暗号化方式は WEP となります。
  特長と認証の流れは、「IEEE 802.1X ＋ PEAP-MSCHAPv2」（→ P.17）をご覧ください。
- IEEE 802.1X ＋ PEAP-TLS
  認証に RADIUS サーバーを使用します。認証方式は PEAP-TLS、通信データの暗号化方式は WEP となります。
  特長と認証の流れは、「IEEE 802.1X ＋ PEAP-TLS」（→ P.18）をご覧ください。
- WPA ＋ EAP-TLS ／ WPA2 ＋ EAP-TLS
  認証に RADIUS サーバーを使用します。認証方式は EAP-TLS、通信データの暗号化方式は TKIP または AES となります。
  特長と認証の流れは、「WPA ＋ EAP-TLS ／ WPA2 ＋ EAP-TLS」（→ P.19）をご覧ください。
- WPA ＋ PEAP-MSCHAPv2 ／ WPA2 ＋ PEAP-MSCHAPv2
  認証に RADIUS サーバーを使用します。認証方式は PEAP-MSCHAPv2、通信データの暗号化方式は TKIP または AES となります。
  特長と認証の流れは、「WPA ＋ PEAP-MSCHAPv2 ／ WPA2 ＋ PEAP-MSCHAPv2」（→ P.20）をご覧ください。

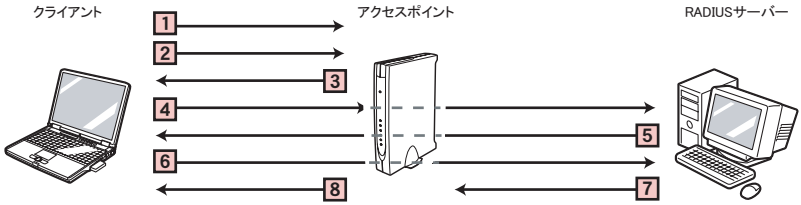
・WPA ＋ PEAP-TLS ／ WPA2 ＋ PEAP-TLS
認証に RADIUS サーバーを使用します。認証方式は PEAP-TLS、通信データの暗号化方式は TKIP または AES となります。
特長と認証の流れは、「WPA ＋ PEAP-TLS ／ WPA2 ＋ PEAP-TLS」（→P.21）をご覧ください。
・WPA-PSK ／ WPA2-PSK
無線 LAN アクセスポイントが認証を行う家庭向け簡易認証方式で、RADIUS サーバーを使用しません。通信データの暗号化方式は TKIP または AES となります。
特長と認証の流れは、「WPA-PSK ／ WPA2-PSK」（→ P.22）をご覧ください。
・従来の WEP
認証は行いません。無線 LAN アクセスポイントとクライアントそれぞれにネットワークキーを手動で設定します。クライアントは、無線 LAN アクセスポイントとネットワークキーが一致すれば通信を行うことができます。通信データの暗号化方式は WEP となります。

■IEEE 802.1X + EAP-TLS

EAP-TLS を使用したユーザー認証を行うために、あらかじめ接続するクライアントに対してクライアント証明書を準備し、インストールします。また、クライアントが RADIUS サーバーを認証するためにも別の証明書（サーバー証明書）を準備し、RADIUS サーバーにインストールします（クライアントを認証する証明書を共用することもできますが、それぞれを別々に準備したほうがより安全になります）。

一般的な証明書のインストール方法については、「クライアント証明書（ユーザー証明書）のインストール」（→ P.336）をご覧ください。

また、暗号化には、WEP を使用します。認証に成功したクライアントに対して無線 LAN アクセスポイントが生成したネットワークキーを配布します。ネットワークキーの値を定期的に変更することでより安全になります。



1 **クライアントが無線 LAN アクセスポイントに接続を要求します。**

2 **クライアントは無線 LAN アクセスポイントに対して認証を行うように要求します。**

3 **無線 LAN アクセスポイントはクライアントに対してクライアントの ID 情報を要求します。**

4 **クライアントは無線 LAN アクセスポイントに ID 情報を送信し、無線 LAN アクセスポイントは RADIUS サーバーに対して認証を行うことを通知します。**

5 **RADIUS サーバーはサーバー証明書をクライアントに送信するとともに、クライアント証明書を要求します。**

6 **クライアントは RADIUS サーバーにクライアント証明書を送信します。**

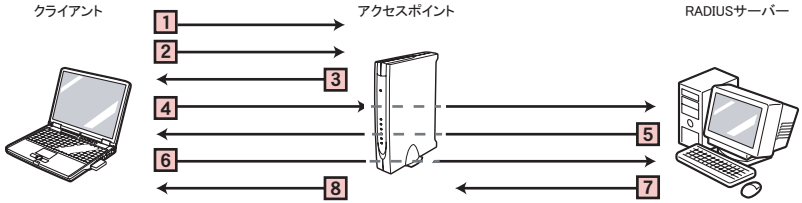
7 **認証が成功したら、RADIUS サーバーは無線 LAN アクセスポイントに対して認証に成功したことを通知します。**

8 **無線 LAN アクセスポイントはネットワークキーを生成し、それを自身に登録した後、クライアントにネットワークキーを通知します。**

クライアントは通知されたネットワークキーを使用して無線LANアクセスポイント経由のネットワークにアクセスできるようになります。

■IEEE 802.1X + PEAP-MSCHAPv2

PEAP-MSCHAPv2 を使用したユーザー認証の場合、RADIUS サーバーがクライアントを認証するときは、ユーザー名／パスワードを PEAP-MSCHAP v2 で暗号化して使用します。また、クライアントが RADIUS サーバーを認証するために RADIUS サーバーに、サーバー証明書をインストールする必要があります。
一般的な証明書のインストール方法については、「クライアント証明書（ユーザー証明書）のインストール」（→ P.336）をご覧ください。
また、暗号化には、WEP を使用します。認証に成功したクライアントに対して無線 LAN アクセスポイントが生成したネットワークキーを配布します。ネットワークキーの値を定期的に変更することでより安全になります。



1 **クライアントが無線 LAN アクセスポイントに接続を要求します。**

2 **クライアントは無線 LAN アクセスポイントに対して認証を行うように要求します。**

3 **無線 LAN アクセスポイントはクライアントに対してクライアントの ID 情報を要求します。**

4 **クライアントは無線 LAN アクセスポイントに ID 情報を送信し、無線 LAN アクセスポイントは RADIUS サーバーに対して認証を行うことを通知します。**

5 **RADIUS サーバーはサーバー証明書をクライアントに送信するとともに、クライアントの認証情報を要求します。**

6 **クライアントは RADIUS サーバーに認証情報を送信します。**

7 **認証が成功したら、RADIUS サーバーは無線 LAN アクセスポイントに対して認証に成功したことを通知します。**

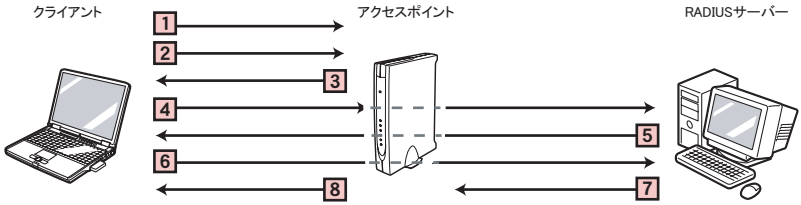
8 **無線 LAN アクセスポイントはネットワークキーを生成し、それを自身に登録した後、クライアントにネットワークキーを通知します。**
クライアントは通知されたネットワークキーを使用して無線LANアクセスポイント経由のネットワークにアクセスできるようになります。

■IEEE 802.1X + PEAP-TLS

PEAP-TLS を使用したユーザー認証を行うために、あらかじめ接続するクライアントに対してクライアント証明書を準備し、インストールします。また、クライアントが RADIUS サーバーを認証するためにも別の証明書（サーバー証明書）を準備し、RADIUS サーバーにインストールします（クライアントを認証する証明書を共用することもできますが、それぞれを別々に準備したほうがより安全になります）。

一般的な証明書のインストール方法については、「クライアント証明書（ユーザー証明書）のインストール」（→ P.336）をご覧ください。

また、暗号化には、WEP を使用します。認証に成功したクライアントに対して無線 LAN アクセスポイントが生成したネットワークキーを配布します。ネットワークキーの値を定期的に変更することでより安全になります。



1 **クライアントが無線 LAN アクセスポイントに接続を要求します。**

2 **クライアントは無線 LAN アクセスポイントに対して認証を行うように要求します。**

3 **無線 LAN アクセスポイントはクライアントに対してクライアントの ID 情報を要求します。**

4 **クライアントは無線 LAN アクセスポイントに ID 情報を送信し、無線 LAN アクセスポイントは RADIUS サーバーに対して認証を行うことを通知します。**

5 **RADIUS サーバーはサーバー証明書をクライアントに送信するとともに、クライアント証明書を要求します。**

6 **クライアントは RADIUS サーバーにクライアント証明書を送信します。**

7 **認証が成功したら、RADIUS サーバーは無線 LAN アクセスポイントに対して認証に成功したことを通知します。**

8 **無線 LAN アクセスポイントはネットワークキーを生成し、それを自身に登録した後、クライアントにネットワークキーを通知します。**

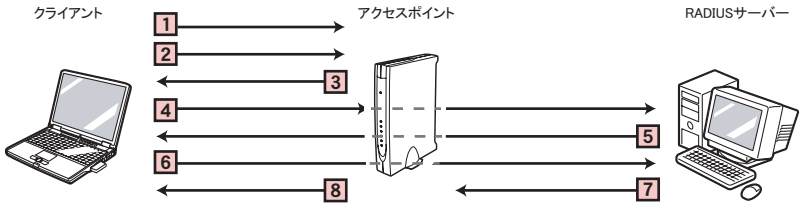
クライアントは通知されたネットワークキーを使用して無線LANアクセスポイント経由のネットワークにアクセスできるようになります。

■WPA ＋ EAP-TLS ／ WPA2 ＋ EAP-TLS

EAP-TLS を使用したユーザー認証を行うために、あらかじめ接続するクライアントに対してクライアント証明書を準備し、インストールします。また、クライアントが RADIUS サーバーを認証するためにも別の証明書（サーバー証明書）を準備し、RADIUS サーバーにインストールします（クライアントを認証する証明書を共用することもできますが、それぞれを別々に準備したほうがより安全になります）。

一般的な証明書のインストール方法については、「クライアント証明書（ユーザー証明書）のインストール」（→ P.336）をご覧ください。

WPA ではデータの暗号化に TKIP を使用します。これは、パケットごとに暗号化に使用するネットワークキーを変更します。また、より強固な AES という暗号化方式を使用することもできます。



1 **クライアントが無線 LAN アクセスポイントに接続を要求します。**

2 **クライアントは無線 LAN アクセスポイントに対して認証を行うように要求します。**

3 **無線 LAN アクセスポイントはクライアントに対してクライアントの ID 情報を要求します。**

4 **クライアントは無線 LAN アクセスポイントに ID 情報を送信し、無線 LAN アクセスポイントは RADIUS サーバーに対して認証を行うことを通知します。**

5 **RADIUS サーバーはサーバー証明書をクライアントに送信するとともに、クライアント証明書を要求します。**

6 **クライアントは RADIUS サーバーにクライアント証明書を送信します。**

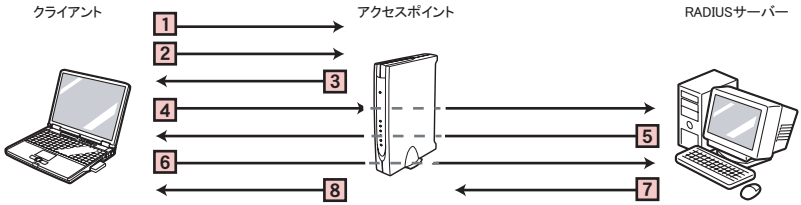
7 **認証が成功したら、RADIUS サーバーは無線 LAN アクセスポイントに対して認証に成功したことを通知します。**

8 **無線 LAN アクセスポイントはネットワークキーを生成し、それを自身に登録した後、クライアントにネットワークキーを通知します。**

クライアントは通知されたネットワークキーを使用して無線LANアクセスポイント経由のネットワークにアクセスできるようになります。

■WPA ＋ PEAP-MSCHAPv2 ／ WPA2 ＋ PEAP-MSCHAPv2

PEAP-MSCHAPv2 を使用したユーザー認証の場合、RADIUS サーバーがクライアントを認証するときは、ユーザー名／パスワードを PEAP-MSCHAP v2 で暗号化して使用します。また、クライアントが RADIUS サーバーを認証するために RADIUS サーバーに、サーバー証明書をインストールする必要があります。
一般的な証明書のインストール方法については、「クライアント証明書（ユーザー証明書）のインストール」（→ P.336）をご覧ください。
WPA ではデータの暗号化に TKIP を使用します。これは、パケットごとに暗号化に使用するネットワークキーを変更します。また、より強固な AES という暗号化方式を使用することもできます。



1 **クライアントが無線 LAN アクセスポイントに接続します。**

2 **クライアントは無線 LAN アクセスポイントに対して認証を行うように要求します。**

3 **無線 LAN アクセスポイントはクライアントに対してクライアントの ID 情報を要求します。**

4 **クライアントは無線 LAN アクセスポイントに ID 情報を送信し、無線 LAN アクセスポイントは RADIUS サーバーに対して認証を行うことを通知します。**

5 **RADIUS サーバーはサーバー証明書をクライアントに送信するとともに、クライアントの認証情報を要求します。**

6 **クライアントは RADIUS サーバーに認証情報を暗号化して送信します。**

7 **認証が成功したら、RADIUS サーバーは無線 LAN アクセスポイントに対して認証に成功したことを通知します。**

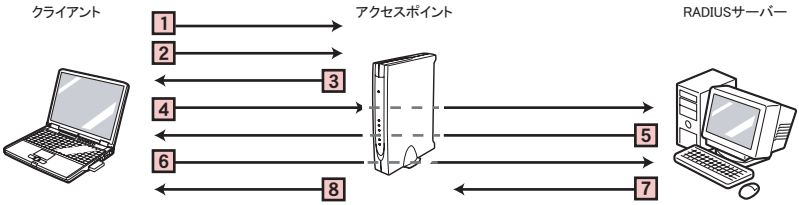
8 **無線 LAN アクセスポイントはネットワークキーを生成し、それを自身に登録した後、クライアントにネットワークキーを通知します。**
クライアントは通知されたネットワークキーを使用して無線LANアクセスポイント経由のネットワークにアクセスできるようになります。

■WPA ＋ PEAP-TLS ／ WPA2 ＋ PEAP-TLS

PEAP-TLS を使用したユーザー認証を行うために、あらかじめ接続するクライアントに対してクライアント証明書を準備し、インストールします。また、クライアントが RADIUS サーバーを認証するためにも別の証明書（サーバー証明書）を準備し、RADIUS サーバーにインストールします（クライアントを認証する証明書を共用することもできますが、それぞれを別々に準備したほうがより安全になります）。

一般的な証明書のインストール方法については、「クライアント証明書（ユーザー証明書）のインストール」（→ P.336）をご覧ください。

WPA ではデータの暗号化に TKIP を使用します。これは、パケットごとに暗号化に使用するネットワークキーを変更します。また、より強固な AES という暗号化方式を使用することもできます。



1 **クライアントが無線 LAN アクセスポイントに接続を要求します。**

2 **クライアントは無線 LAN アクセスポイントに対して認証を行うように要求します。**

3 **無線 LAN アクセスポイントはクライアントに対してクライアントの ID 情報を要求します。**

4 **クライアントは無線 LAN アクセスポイントに ID 情報を送信し、無線 LAN アクセスポイントは RADIUS サーバーに対して認証を行うことを通知します。**

5 **RADIUS サーバーはサーバー証明書をクライアントに送信するとともに、クライアント証明書を要求します。**

6 **クライアントは RADIUS サーバーにクライアント証明書を送信します。**

7 **認証が成功したら、RADIUS サーバーは無線 LAN アクセスポイントに対して認証に成功したことを通知します。**

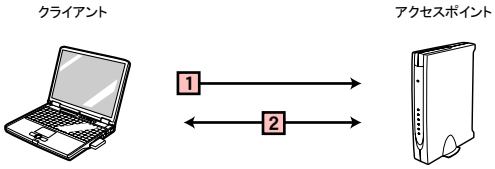
8 **無線 LAN アクセスポイントはネットワークキーを生成し、それを自身に登録した後、クライアントにネットワークキーを通知します。**

クライアントは通知されたネットワークキーを使用して無線LANアクセスポイント経由のネットワークにアクセスできるようになります。

■WPA-PSK ／ WPA2-PSK

WPA-PSK はクライアント認証を無線 LAN アクセスポイントが行うため、RADIUS サーバーが不要です。

WPA ではデータの暗号化に TKIP を使用します。これは、パケットごとに暗号化に使用するネットワークキーを変更します。また、より強固な AES という暗号化方式を使用することもできます。



1 クライアントが無線 LAN アクセスポイントに接続します。

2 クライアントと無線 LAN アクセスポイントの間で、PSK による認証を行います。

クライアントは無線LANアクセスポイント経由のネットワークにアクセスできるようになります。

2 セキュリティパターンの選択

セキュリティ環境の構築にあたっては、各セキュリティパターンのセキュリティレベルや、導入に必要な環境、作業、コストなど、ネットワークの規模などに合わせて導入するパターンを検討する必要があります。

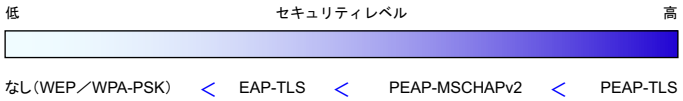
■セキュリティレベル

セキュリティのパターンは、RADIUS サーバーを使用する場合と使用しない場合に分けることができます。RADIUS サーバーを使用する環境の方が、セキュリティレベルは高くなりますが、RADIUS サーバーの導入、管理には、それなりのコストがかかるため、ネットワークの規模などに合わせて導入を検討する必要があります。
ユーザー認証と暗号化方式のそれぞれでセキュリティレベルを比較すると次のようになります。

□ ユーザー認証

ユーザー認証をセキュリティレベルの高い順に並べると次のようになります。

・PEAP-TLS
・PEAP-MSCHAPv2
・EAP-TLS
・なし（WEP ／ WPA-PSK）

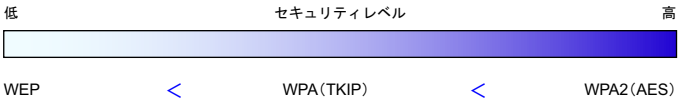


ただし、運用方法によっては、この図式が当てはまらない場合があります。

□ 暗号化方式

暗号化方式をセキュリティレベルの高い順に並べると次のようになります。

・WPA2（AES）
・WPA（TKIP）
・WEP



■導入に必要な環境と準備作業

セキュリティのパターンによって、必要な環境と準備作業は次の通りです。

表：セキュリティパターンによる必要な環境と準備作業

セキュリティパターン	必要な環境	クライアントで必要な準備作業
IEEE 802.1X ＋ EAP-TLS	・証明機関（CA 局） ・RADIUS サーバー［注 1］ ・無線 LAN アクセスポイント	・信頼する証明機関の登録 ・クライアント証明書のインストール
IEEE 802.1X ＋ PEAP-MSCHAP v2	・証明機関（CA 局） ・RADIUS サーバー［注 1］ ・無線 LAN アクセスポイント	・信頼する証明機関の登録
IEEE 802.1X ＋ PEAP-TLS	・証明機関（CA 局） ・RADIUS サーバー［注 1］ ・無線 LAN アクセスポイント	・信頼する証明機関の登録 ・クライアント証明書のインストール
WPA ＋ EAP-TLS	・証明機関（CA 局） ・RADIUS サーバー［注 1］ ・WPA または WPA2 に対応した無線 LAN アクセスポイント［注 2］	・信頼する証明機関の登録 ・クライアント証明書のインストール
WPA ＋ PEAP-MSCHAPv2	・証明機関（CA 局） ・RADIUS サーバー［注 1］ ・WPA または WPA2 に対応した無線 LAN アクセスポイント［注 2］	・信頼する証明機関の登録
WPA ＋ PEAP-TLS	・証明機関（CA 局） ・RADIUS サーバー［注 1］ ・WPA または WPA2 に対応した無線 LAN アクセスポイント［注 2］	・信頼する証明機関の登録 ・クライアント証明書のインストール
WPA-PSK	・WPA または WPA2 に対応した無線 LAN アクセスポイント［注 2］	
WPA2 ＋ EAP-TLS	・証明機関（CA 局） ・RADIUS サーバー［注 1］ ・WPA2 に対応した無線 LAN アクセスポイント［注 2］	・信頼する証明機関の登録 ・クライアント証明書のインストール
WPA2＋PEAP-MSCHAPv2	・証明機関（CA 局） ・RADIUS サーバー［注 1］ ・WPA2 に対応した無線 LAN アクセスポイント［注 2］	・信頼する証明機関の登録
WPA2 ＋ PEAP-TLS	・証明機関（CA 局） ・RADIUS サーバー［注 1］ ・WPA2 に対応した無線 LAN アクセスポイント［注 2］	・信頼する証明機関の登録 ・クライアント証明書のインストール
WPA2-PSK	・WPA2 に対応した無線 LAN アクセスポイント［注 2］	
従来の WEP	・無線 LAN アクセスポイント	特になし

注 1　RADIUS サーバーの準備作業として、信頼する証明機関の登録とサーバー証明書のインストールを行う必要があります。

注 2　WPA2 の認証（RADIUS 認証、WPA2 エンタープライズ）に対応している必要があります。

Memo

2

第 2 章

無線 LAN アクセスポイントの設定

無線 LAN アクセスポイントの設定について説明します。

1 FMWBR-201 の設定

FMWBR-201 の設定方法を説明します。
このマニュアルでは暗号化と認証方式の設定についてのみ説明します。その他の設定については製品に添付のマニュアルをご覧ください。
設定方法は、次のパターンで異なります。

・「IEEE 802.1X」（→ P.28）
・「WPA」（→ P.30）
・「WPA-PSK」（→ P.32）

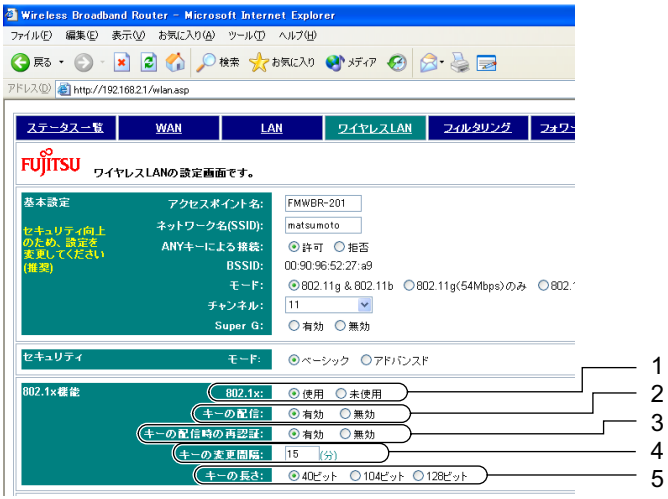
IEEE 802.1X

FMWBR-201 の Web ブラウザの設定画面にログインし、次のようにセキュリティの設定を行います。

1 トップメニューの「ワイヤレス LAN」をクリックします。

2 「セキュリティ」カテゴリの「モード」で、「ベーシック」をクリックして ◉ にします。

3 「802.1x 機能」カテゴリで、次のように設定します。



1. 802.1x
「使用」をクリックして ◉ にします。

2. **キーの配信**
「有効」をクリックして◉にします。
3. **キーの配信時の再認証**
一定間隔で再認証処理を行うかどうか選択します。
4. **キーの変更間隔**
「キーの配信時の再認証」を有効にした場合、設定します。設定された時間ごとにキーの変更を行います。
5. **キーの長さ**
ネットワークキーの長さを選択します。
ネットワークキーの長さは、クライアントの無線 LAN 機能の仕様を考慮する必要があります。
詳しくは、「各製品の対応状況」（→ P.356）、または各製品のマニュアルをご覧ください。

4 「RADIUS 機能」カテゴリで、RADIUS サーバーの情報を設定します。

1. RADIUS サーバー 1
「使用」をクリックして◉にし、次のように入力します。
・「IP アドレス」に RADIUS サーバーの IP アドレスを入力します。
・「ポート」に、使用するポート番号を入力します。通常は変更する必要はありません。
・「共有シークレット」に、RADIUSサーバーの共有シークレットを入力します。
2. RADIUS サーバー 2
バックアップ用の RADIUS サーバーがある場合は、RADIUS サーバー 1 と同様に設定します。バックアップ用の RADIUS サーバーがない場合は、「未使用」をクリックして◉にします。
3. **キーマスク**
共有シークレットの値を確認する場合は、「有効」をクリックして☐にします。
4. **リトライ間隔**
RADIUS サーバーに認証要求をリトライするときの間隔を秒で指定します。通常は変更する必要はありません。
5. **リトライ回数 / サーバー**
サイクルごとに何回リトライを行うかを指定します。通常は変更する必要はありません。
6. **サイクル数**
それぞれのサーバーに対して、「リトライ回数 / サーバー」で指定した回数のリトライを行うことを 1 サイクルといいます。何サイクル試行したら認証要求を停止するかを指定します。通常は変更する必要はありません。

5 **「ワイヤレス　LAN」メニュー画面で必要な項目を設定したら、「設定」をクリックします。**

「設定を保存しています。」という画面が終了すると、設定が完了します。

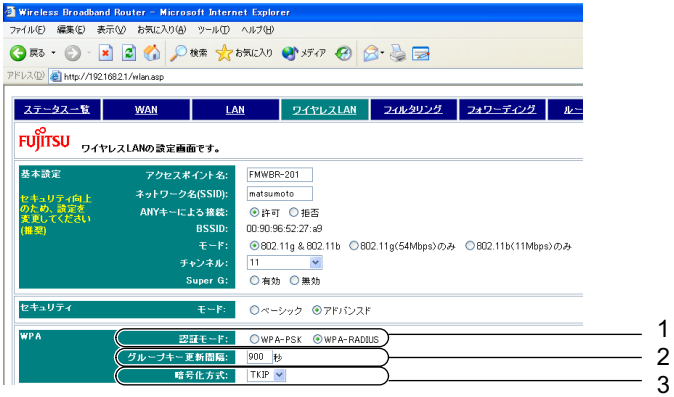
WPA

FMWBR-201 の Web ブラウザの設定画面にログインし、次のようにセキュリティの設定を行います。

1 **トップメニューの「ワイヤレス LAN」をクリックします。**

2 **「セキュリティ」カテゴリの「モード」で、「アドバンスド」をクリックして◉にします。**

3 **「WPA」カテゴリで、次のように設定します。**



1. **認証モード**

   「WPA-RADIUS」をクリックして◉にします。

2. **グループキー更新間隔**

   グループキーの更新間隔を設定します。通常は変更する必要はありません。

3. **暗号化方式**

   ▼をクリックして「TKIP」、「AES」、「自動」のいずれかを選択します。

   クライアントの無線 LAN 機能によっては、AES に対応していないものがあります。

   詳しくは、「各製品の対応状況」（→ P.356）、または各製品のマニュアルをご覧ください。

   ・「TKIP」

   TKIP で暗号化を行います。クライアントの暗号化方式を TKIP に設定する必要があります。

   ・「AES」

AES で暗号化を行います。クライアントの暗号化方式を AES に設定する必要があります。

・「自動」
クライアントの暗号化方式を自動判別し、TKIP、または AES で暗号化を行います。

4 「RADIUS 機能」カテゴリで、RADIUS サーバーの情報を設定します。

1. RADIUS サーバー 1
「使用」をクリックして◉にし、次のように入力します。
・「IP アドレス」に RADIUS サーバーの IP アドレスを入力します。
・「ポート」に、使用するポート番号を入力します。通常は変更する必要はありません。
・「共有シークレット」に、RADIUS サーバーで指定されている共有シークレットを指定します。
2. RADIUS サーバー 2
バックアップ用の RADIUS サーバーがある場合は、RADIUS サーバー 1 と同様に設定します。バックアップ用の RADIUS サーバーがない場合は、「未使用」をクリックして◉にします。
3. **キーマスク**
共有シークレットの値を確認する場合は、「有効」をクリックして☐にします。
4. **リトライ間隔**
RADIUS サーバーに認証要求をリトライするときの間隔を秒で指定します。通常は変更する必要はありません。
5. **リトライ回数 / サーバー**
サイクルごとに何回リトライを行うかを指定します。通常は変更する必要はありません。
6. **サイクル数**
それぞれのサーバーに対して、「リトライ回数 / サーバー」で指定した回数のリトライを行うことを 1 サイクルといいます。何サイクル試行したら認証要求を停止するかを指定します。通常は変更する必要はありません。

5 「ワイヤレス　LAN」メニュー画面で必要な項目を設定したら、「設定」をクリックします。

「設定を保存しています。」という画面が終了すると、設定が完了します。

WPA-PSK

FMWBR-201 の Web ブラウザの設定画面にログインし、次のようにセキュリティの設定を行います。

1 **トップメニューの「ワイヤレス LAN」をクリックします。**

2 **「セキュリティ」カテゴリの「モード」で、「アドバンスド」をクリックして◉にします。**

3 **「WPA」カテゴリで、次のように設定します。**

1. **認証モード**
   「WPA-PSK」をクリックして◉にします。
2. **PSK 入力**
   PSK の入力方法を選択し、PSK を入力します。
   ・PSK をパスフレーズで入力する場合
   「パスフレーズ」をクリックして◉にします。「パスフレーズ」項目が表示されるので、PSK を ASCII 文字 8 ～ 63 文字の範囲で入力します。使用できる文字は、半角英数字、半角記号です。
   ・PSK を 16 進数で入力する場合
   「16 進数」をクリックして◉にします。「PSK」項目が表示されるので、PSK を 16 進数 64 文字で入力します。使用できる文字は、0 ～ 9、A ～ F、a ～ f です。
3. **キーマスク**
   パスフレーズまたは PSK の値を確認する場合は、「有効」をクリックして□にします。
4. **グループキー更新間隔**
   グループキーの更新間隔を設定します。通常は変更する必要はありません。短くすることで、外部からの暗号の解読が困難になります。

5. **暗号化方式**

をクリックして「TKIP」、「AES」、「自動」のいずれかを選択します。
クライアントの無線 LAN 機能によっては、AES に対応していないものがあります。
詳しくは、「各製品の対応状況」(→ P.356)、または各装置のマニュアルをご覧ください。

・「TKIP」
TKIP で暗号化を行います。クライアントの暗号化方式を TKIP に設定する必要があります。

・「AES」
AES で暗号化を行います。クライアントの暗号化方式を AES に設定する必要があります。

・「自動」
クライアントの暗号化方式を自動判別し、TKIP、または AES で暗号化を行います。

4 「ワイヤレス　LAN」メニュー画面で必要な項目を設定したら、「設定」をクリックします。

「設定を保存しています。」という画面が終了すると、設定が完了します。

2 FMWT-56AG ／ FMWT-55AG ／ FMWT-54AG の設定

FMWT-56AG ／ FMWT-55AG ／ FMWT-54AG の設定方法を説明します。
このマニュアルでは暗号化と認証方式の設定についてのみ説明します。その他の設定については製品に添付のマニュアルをご覧ください。
設定方法は、次のパターンで異なります。
・「IEEE 802.1X」（→ P.34）
・「WPA ／ WPA2」（→ P.37）
・「WPA-PSK ／ WPA2-PSK」（→ P.41）

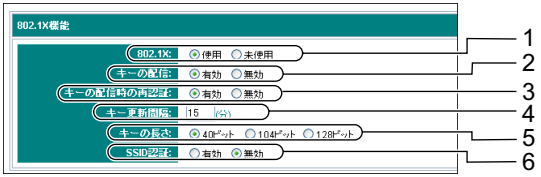
IEEE 802.1X

FMWT-56AG ／ FMWT-55AG ／ FMWT-54AG の Web ブラウザの設定画面にログインし、次のようにセキュリティの設定を行います。

1 左側のメニューから「セキュリティポリシー」をクリックします。

2 「セキュリティ」カテゴリの「モード」で、「ベーシック」をクリックして ◉ にします。

3 「802.1X 機能」カテゴリで次のように設定します。



1. 802.1X
   「使用」をクリックして ◉ にします。
2. **キーの配信**
   「有効」をクリックして ◉ にします。
3. **キーの配信時の再認証**
   一定間隔で再認証処理を行うかどうか選択します。
4. **キー更新間隔**
   「キーの配信時の再認証」を有効にした場合、設定します。設定された時間ごとにキーの変更を行います。

5. キーの長さ
   暗号化に使用するキーの長さを設定します。
   ネットワークキーの長さは、クライアントの無線 LAN 機能の仕様を考慮する必要があります。
   詳しくは、「各製品の対応状況」(→ P.356)、または各製品のマニュアルをご覧ください。
6. SSID 認証
   SSID 認証を行うかどうか選択します。SSID 認証については、FMWT-56AG ／ FMWT-55AG ／ FMWT-54AG のマニュアルをご覧ください。

4 「設定」ボタンをクリックします。

再起動の確認画面が表示されます。

5 「OK」をクリックします。

「設定を保存しています。」という画面が終了すると、「セキュリティポリシー」設定が完了します。

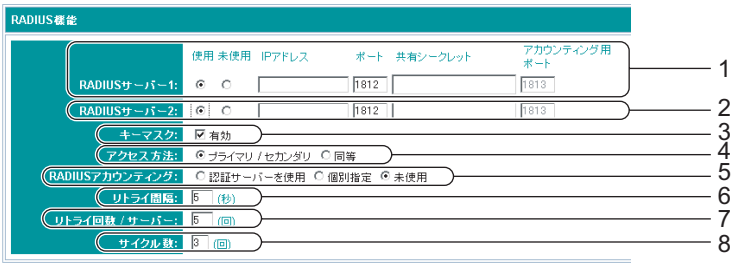
重要

・「RADIUS　サーバーの設定」ボタンをクリックする前に、必ず「セキュリティポリシー」画面の「設定」ボタンをクリックしてください。
「セキュリティポリシー」画面の「設定」ボタンをクリックせずに「RADIUS サーバーの設定」ボタンをクリックすると、「セキュリティポリシー」画面で変更した内容が反映されません。

6 「RADIUS 機能」カテゴリの「RADIUS サーバーの設定」ボタンをクリックします。

「RADIUS サーバーの設定」画面が表示されます。

7 RADIUS サーバーの情報を次のように設定します。



1. RADIUS サーバー 1
   「使用」をクリックして◉にし、次のように入力します。
   ・「IP アドレス」に RADIUS サーバーの IP アドレスを入力します。
   ・「ポート」に使用するポート番号を入力します。通常は変更する必要はありません。
   ・「共有シークレット」に RADIUS サーバーの共有シークレットを入力します。
   ・「アカウンティング用ポート」に RADIUS アカウンティングで使用するポート番号を入力します。

「RADIUS アカウンティング」項目を「認証サーバーを使用」に設定したときに設定可能な詳細項目です。

2. **RADIUS サーバー 2**

   RADIUS サーバー 1 以外に RADIUS サーバーがある場合は、「使用」をクリックして◉にし、「RADIUS サーバー 1」と同様に設定します。

   RADIUS サーバー 1 以外に RADIUS サーバーがない場合は、「未使用」をクリックして◉にします。

3. **キーマスク**

   共有シークレットを確認する場合は、「有効」をクリックして☐にします。

4. **アクセス方法**

   「RADIUS サーバー 1」と「RADIUS サーバー 2」の両方が「使用」のときに表示される項目です。「RADIUS サーバー 1」と「RADIUS サーバー 2」の使い方を設定します。

   ・プライマリ／セカンダリ

   「RADIUS サーバ 1」を優先サーバー、「RADIUS サーバー 2」をバックアップサーバーとして使用します。再認証時には、必ず「RADIUS サーバー 1」にアクセスし、「RADIUS サーバー 1」からの応答がない場合、「RADIUS サーバー 2」にアクセス先を切り替えます。

   ・同等

   「RADIUS サーバー 1」と「RADIUS サーバー 2」を同じ優先度で使用します。再認証時には、前回の認証に成功したサーバーにアクセスします。RADIUS サーバーからの応答がない場合、アクセス先を切り替えます。

5. **RADIUS アカウンティング**

   RADIUS アカウンティングを使用するかどうか、また使用する場合は、アカウンティングサーバーの指定方法を選択します。

   ・認証サーバーを使用

   RADIUS アカウンティングを使用します。RADIUS サーバー 1（および RADIUS サーバー 2）を、アカウンティングサーバーとして併用します。「RADIUS サーバー 1」（および「RADIUS サーバー 2」）の詳細項目で、「アカウンティング用ポート」を設定する必要があります。

   ・個別指定

   RADIUS アカウンティングを使用します。アカウンティングサーバーを、RADIUS サーバー 1（および RADIUS サーバー 2）とは別に指定します。

   「個別指定」に設定すると、「アカウンティングサーバー」項目が表示されるので、詳細項目を次のように設定します。

   - 「IP アドレス」にアカウンティングサーバーの IP アドレスを入力します。
   - 「ポート」に RADIUS アカウンティングで使用するポート番号を入力します。
   - 「共有シークレット」にアカウンティングサーバーの共有シークレットを入力します。

   ・未使用

   RADIUS アカウンティングを使用しません。

6. **リトライ間隔**
   RADIUS サーバーに認証要求をリトライするときの間隔を 1 ～ 60（秒）の範囲で指定します。通常は変更する必要はありません。
7. **リトライ回数／サーバー**
   サイクルごとに何回リトライを行うかを、1 ～ 10（回）の範囲で指定します。通常は変更する必要はありません。
8. **サイクル回数**
   それぞれのサーバーに対して、「リトライ回数 / サーバー」で指定した回数のリトライを行うことを 1 サイクルといいます。何サイクル試行したら認証要求を停止するかを、1 ～ 5（回）の範囲で指定します。通常は変更する必要はありません。

8 「RADIUS サーバーの設定」画面で必要な設定が終わったら、「設定」ボタンをクリックします。
再起動の確認画面が表示されます。

9 「OK」をクリックします。
「設定を保存しています。」という画面が終了すると、RADIUS サーバーの設定が完了します。

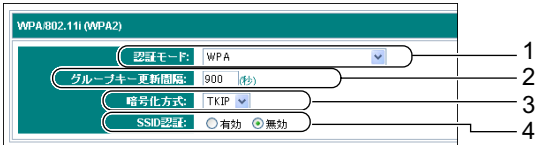
WPA ／ WPA2

FMWT-56AG ／ FMWT-55AG ／ FMWT-54AG の Web ブラウザの設定画面にログインし、次のようにセキュリティの設定を行います。

1 左側のメニューから「セキュリティポリシー」をクリックします。

2 「セキュリティ」カテゴリの「モード」で、「アドバンスド」をクリックして◉にします。

3 「WPA/802.11i (WPA2)」カテゴリで次のように設定します。



1. **認証モード**
   WPA のみ使用する場合は「WPA」を選択します。
   IEEE 802.11i (WPA2) のみ使用する場合は「802.11i (WPA2)」を選択します。
   WPA と IEEE 802.11i (WPA2) の両方を使用する場合は「WPA/802.11i (WPA2)」を選択します。
2. **グループキー更新間隔**
   グループキーの更新間隔を設定します。通常は変更する必要はありません。

3. 暗号化方式

をクリックして、「TKIP」、「AES」、「自動」のいずれかを選択します。
クライアントの無線 LAN 機能によっては、AES に対応していないものがあります。
詳しくは、「各製品の対応状況」(→ P.356)、または各製品のマニュアルをご覧ください。

・「TKIP」
TKIP で暗号化を行います。クライアントの暗号化方式を TKIP に設定する必要があります。

・「AES」
AES で暗号化を行います。クライアントの暗号化方式を AES に設定する必要があります。

・「自動」
クライアントの暗号化方式を自動判別し、TKIP、または AES で暗号化を行います。

4. SSID 認証

SSID 認証を行うかどうか選択します。SSID 認証については、FMWT-56AG ／ FMWT-55AG ／ FMWT-54AG のマニュアルをご覧ください。

4 「設定」ボタンをクリックします。

再起動の確認画面が表示されます。

5 「OK」をクリックします。

「設定を保存しています。」という画面が終了すると、「セキュリティポリシー」設定が完了します。

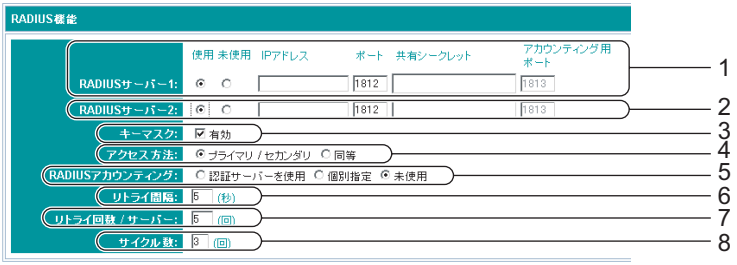
重要

・「RADIUS サーバーの設定」ボタンをクリックする前に、必ず「セキュリティポリシー」画面の「設定」ボタンをクリックしてください。
「セキュリティポリシー」画面の「設定」ボタンをクリックせずに「RADIUS サーバーの設定」ボタンをクリックすると、「セキュリティポリシー」画面で変更した内容が反映されません。

6 「RADIUS 機能」カテゴリの「RADIUS サーバーの設定」ボタンをクリックします。

「RADIUS サーバーの設定」画面が表示されます。

7 RADIUS サーバーの情報を次のように設定します。



1. RADIUS サーバー 1

   「使用」をクリックして◉にし、次のように入力します。

   ・「IP アドレス」に RADIUS サーバーの IP アドレスを入力します。

   ・「ポート」に使用するポート番号を入力します。通常は変更する必要はありません。

   ・「共有シークレット」に RADIUS サーバーの共有シークレットを入力します。

   ・「アカウンティング用ポート」に RADIUS アカウンティングで使用するポート番号を入力します。

   「RADIUS アカウンティング」項目を「認証サーバーを使用」に設定したときに設定可能な詳細項目です。

2. RADIUS サーバー 2

   RADIUS サーバー 1 以外に RADIUS サーバーがある場合は、「使用」をクリックして◉にし、「RADIUS サーバー 1」と同様に設定します。

   RADIUS サーバー 1 以外に RADIUS サーバーがない場合は、「未使用」をクリックして◉にします。

3. キーマスク

   共有シークレットを確認する場合は、「有効」をクリックして□にします。

4. アクセス方法

   「RADIUS サーバー 1」と「RADIUS サーバー 2」の両方が「使用」のときに表示される項目です。「RADIUS サーバー 1」と「RADIUS サーバー 2」の使い方を設定します。

   ・プライマリ／セカンダリ

   「RADIUS サーバ 1」を優先サーバー、「RADIUS サーバー 2」をバックアップサーバーとして使用します。再認証時には、必ず「RADIUS サーバー 1」にアクセスし、「RADIUS サーバー 1」からの応答がない場合、「RADIUS サーバー 2」にアクセス先を切り替えます。

   ・同等

   「RADIUS サーバー 1」と「RADIUS サーバー 2」を同じ優先度で使用します。再認証時には、前回の認証に成功したサーバーにアクセスします。RADIUS サーバーからの応答がない場合、アクセス先を切り替えます。

5. RADIUS アカウンティング

   RADIUS アカウンティングを使用するかどうか、また使用する場合は、アカウンティングサーバーの指定方法を選択します。

   ・認証サーバーを使用

RADIUSアカウンティングを使用します。RADIUSサーバー1(およびRADIUSサーバー 2）を、アカウンティングサーバーとして併用します。「RADIUSサーバー 1」（および「RADIUS サーバー 2」）の詳細項目で、「アカウンティング用ポート」を設定する必要があります。

・個別指定
RADIUS アカウンティングを使用します。アカウンティングサーバーを、RADIUS サーバー 1（およびRADIUS サーバー 2）とは別に指定します。
「個別指定」に設定すると、「アカウンティングサーバー」項目が表示されるので、詳細項目を次のように設定します。
  ・「IP アドレス」にアカウンティングサーバーの IP アドレスを入力します。
  ・「ポート」に RADIUS アカウンティングで使用するポート番号を入力します。
  ・「共有シークレット」にアカウンティングサーバーの共有シークレットを入力します。

・未使用
RADIUS アカウンティングを使用しません。

6. **リトライ間隔**
RADIUS サーバーに認証要求をリトライするときの間隔を 1 ～ 60（秒）の範囲で指定します。通常は変更する必要はありません。
7. **リトライ回数／サーバー**
サイクルごとに何回リトライを行うかを、1 ～ 10（回）の範囲で指定します。通常は変更する必要はありません。
8. **サイクル回数**
それぞれのサーバーに対して、「リトライ回数 / サーバー」で指定した回数のリトライを行うことを 1 サイクルといいます。何サイクル試行したら認証要求を停止するかを、1 ～ 5（回）の範囲で指定します。通常は変更する必要はありません。

8 「RADIUS サーバーの設定」画面で必要な設定が終わったら、「設定」ボタンをクリックします。
再起動の確認画面が表示されます。

9 「OK」をクリックします。
「設定を保存しています。」という画面が終了すると、RADIUS サーバーの設定が完了します。

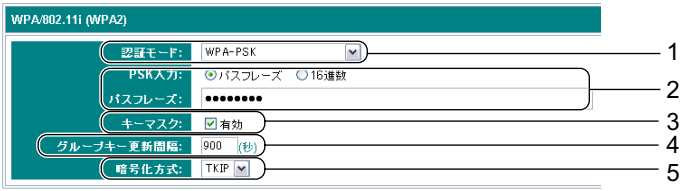
WPA-PSK ／ WPA2-PSK

FMWT-56AG ／ FMWT-55AG ／ FMWT-54AG の Web ブラウザの設定画面にログインし、次のようにセキュリティの設定を行います。

1 **左側のメニューから「セキュリティポリシー」をクリックします。**

2 **「セキュリティ」カテゴリの「モード」で、「アドバンスド」をクリックして◉にします。**

3 **「WPA/802.11i (WPA2)」カテゴリで次のように設定します。**



1. **認証モード**
   無線 LAN のセキュリティを WPA-PSK で設定する場合は、「WPA-PSK」を選択します。
   無線 LAN のセキュリティを IEEE 802.11i (WPA2)-PSK で設定する場合は、「802.11i (WPA2)-PSK」を選択します。
   無線 LAN クライアントの認証モードを WPA-PSK と IEEE 802.11i (WPA2)-PSK のいずれかで自動判別し、認証を行う場合は、「WPA-PSK/802.11i (WPA2)-PSK」を選択します。
2. **PSK 入力**
   PSK の入力方法を選択し、PSK を入力します。
   ・PSK をパスフレーズで入力する場合
   「パスフレーズ」をクリックして◉にします。「パスフレーズ」項目が表示されるので、PSK を ASCII 文字 8 ～ 63 文字の範囲で入力します。使用できる文字は、半角英数字、半角記号です。
   ・PSK を 16 進数で入力する場合
   「16 進数」をクリックして◉にします。「PSK」項目が表示されるので、PSK を 16 進数 64 文字で入力します。使用できる文字は、0 ～ 9、A ～ F、a ～ f です。
3. **キーマスク**
   パスフレーズまたは PSK を確認する場合は、「有効」をクリックして☐にします。
4. **グループキー更新間隔**
   グループキーの更新間隔を設定します。通常は変更する必要はありません。

5. 暗号化方式

をクリックして、「TKIP」、「AES」、「自動」のいずれかを選択します。
クライアントの無線 LAN 機能によっては、AES に対応していないものがあります。
詳しくは、「各製品の対応状況」(→ P.356)、または各製品のマニュアルをご覧ください。

・「TKIP」
TKIP で暗号化を行います。クライアントの暗号化方式を TKIP に設定する必要があります。

・「AES」
AES で暗号化を行います。クライアントの暗号化方式を AES に設定する必要があります。

・「自動」
クライアントの暗号化方式を自動判別し、TKIP、または AES で暗号化を行います。

4 「設定」ボタンをクリックします。

再起動の確認画面が表示されます。

5 「OK」をクリックします。

「設定を保存しています。」という画面が終了すると、「セキュリティポリシー」設定が完了します。

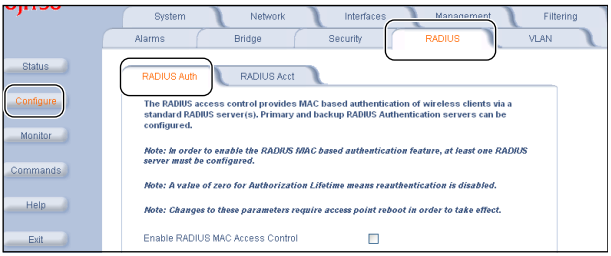
3 FMWT-53 シリーズの設定

FMWT-53 シリーズの設定方法を説明します。
このマニュアルでは暗号化と認証方式の設定についてのみ説明します。その他の設定については製品に添付のマニュアルをご覧ください。
設定方法は、次のパターンで異なります。
・「IEEE 802.1X」（→ P.43）
・「WPA」（→ P.45）
・「WPA-PSK」（→ P.48）

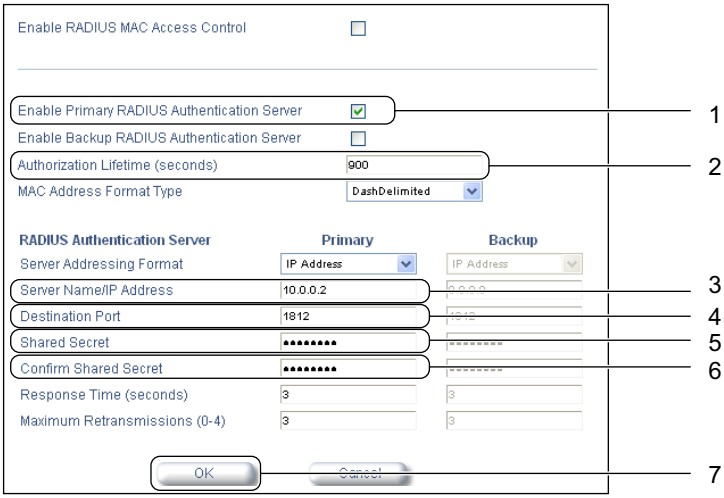
IEEE 802.1X

Web ブラウザの「HTTP インターフェース設定画面」で次のようにセキュリティの設定を行います。

1 「Configure」メニュー→「RADIUS」タブ→「RADIUS Auth」タブの順にクリックします。



2 次のように、RADIUS サーバーの情報を設定します。



1. Enable Primary RADIUS Authentication Server

   クリックして☑にします。
2. Authorization Lifetime

   無線 LAN クライアントの再認証時間（秒）の間隔を 7200 ～ 43200 の範囲で設定します。
3. Server Name/IP Address

   RADIUS サーバーの IP アドレスを入力します。
4. Destination Port

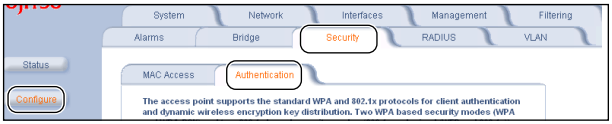
   RADIUS サーバーの認証ポートを入力します。
5. Shared Secret

   RADIUS サーバーの共有シークレットを入力します。
6. Confirm Shared Secret

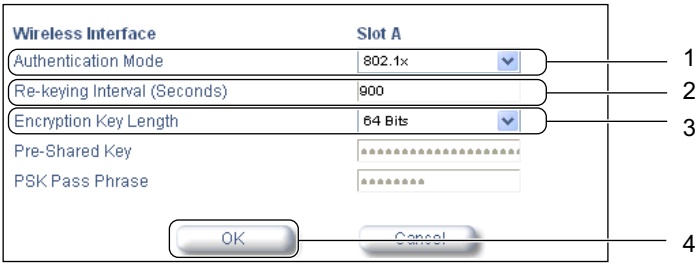
   確認のため、「Shared Secret」と同じ値を入力します。
7. OK

   この画面の設定が完了したら、クリックします。

3 「Configure」メニュー→「Security」タブ→「Authentication」タブの順にクリックします。



4 **次のように、IEEE 802.1X の設定をします。**



1. Authentication Mode

   をクリックして「802.1x」を選択します。
2. Re-Keying Interval

   ネットワークキーの再配布時間(秒)の間隔を 60 ～ 65535 の範囲で設定します。
3. Encryption Key Length

   自動生成するネットワークキーの長さを選択します。

   ネットワークキーの長さは、クライアントの無線 LAN 機能の仕様を考慮する必要があります。

   詳しくは、「各製品の対応状況」(→ P.356)、または各製品のマニュアルをご覧ください。
4. OK

   この画面の設定が完了したら、クリックします。

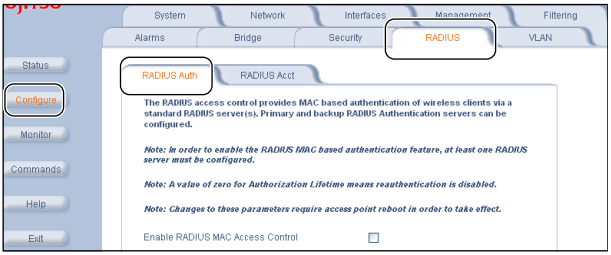
5 **必要な項目をすべて設定したら、「Commands」メニュー→「Reboot」タブの順にクリックします。**

6 **「Reboot」をクリックして、無線 LAN アクセスポイントを再起動します。**

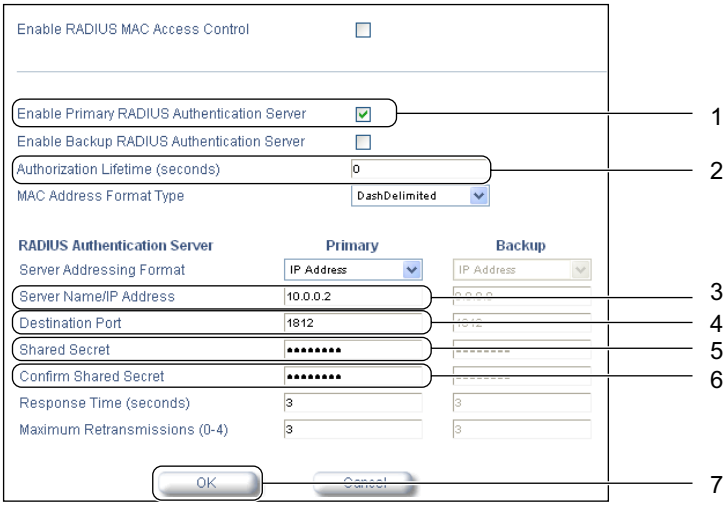
WPA

Web ブラウザの「HTTP インターフェース設定画面」で、次のようにセキュリティの設定を行います。

1 **「Configure」メニュー→「RADIUS」タブ→「RADIUS Auth」タブの順にクリックします。**

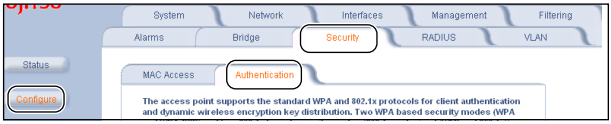


2 次のように、RADIUS サーバーの情報を設定します。

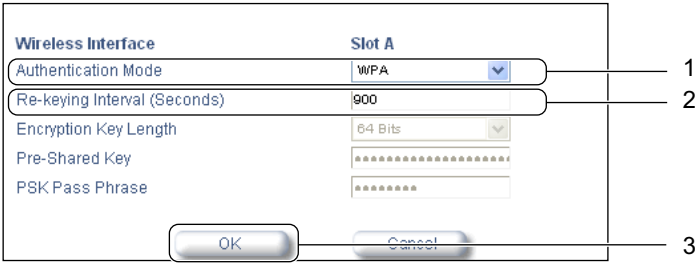


1. Enable Primary RADIUS Authentication Server
   クリックして☑にします。
2. Authorization Lifetime
   0 を入力します。
3. Server Name/IP Address
   RADIUS サーバーの IP アドレスを入力します。
4. Destination Port
   RADIUS サーバーの認証ポートを入力します。
5. Shared Secret
   RADIUS サーバーの共有シークレットを入力します。
6. Confirm Shared Secret
   確認のため、「Shared Secret」と同じ値を入力します。
7. OK
   この画面の設定が完了したら、クリックします。

3 「Configure」メニュー→「Security」タブ→「Authentication」タブの順にクリックします。



4 次のように、WPA の設定をします。



1. Authentication Mode

   をクリックして「WPA」を選択します。
2. Re-Keying Interval

   ネットワークキーの再配布時間(秒)の間隔を 60 ～ 65535 の範囲で設定します。
3. OK

   この画面の設定が完了したら、クリックします。

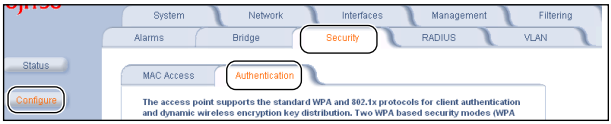
5 必要な項目をすべて設定したら、「Commands」メニュー→「Reboot」タブの順にクリックします。

6 「Reboot」をクリックして、無線 LAN アクセスポイントを再起動します。

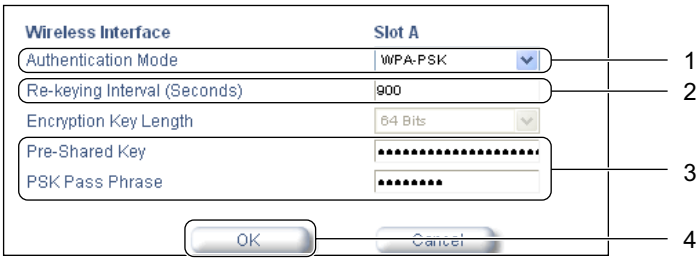
WPA-PSK

Web ブラウザの「HTTP インターフェース設定画面」で、次のようにセキュリティの設定を行います。

1 「Configure」メニュー→「Security」タブ→「Authentication」タブの順にクリックします。



2 次のように、WPA-PSK の設定をします。



1. Authentication Mode

   をクリックして「WPA-PSK」を選択します。
2. Re-Keying Interval

   ネットワークキーの再配布時間（秒）の間隔を 60 ～ 65535 の範囲で設定します。
3. Pre-Shared Key ／ PSK Pass Phrase

   認証キーを設定します。

   ・認証キーを 16 進数で設定する場合

   「Pre-Shared Key」に 16 進数（0 ～ 9、A ～ F、a ～ f）64 文字で入力します。

   ・認証キーをパスフレーズで設定する場合

   「PSK Pass Phrase」に ASCII 文字 8 ～ 63 文字で入力します。
4. OK

   この画面の設定が完了したら、クリックします。

3 必要な項目をすべて設定したら、「Commands」メニュー→「Reboot」タブの順にクリックします。

4 「Reboot」をクリックして、無線 LAN アクセスポイントを再起動します。

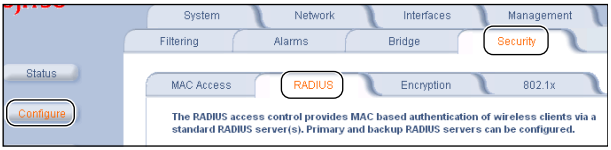
4 FMWT-52 シリーズの設定

FMWT-52 シリーズの設定方法を説明します。
このマニュアルでは暗号化と認証方式の設定についてのみ説明します。その他の設定については製品に添付のマニュアルをご覧ください。
FMWT-52 シリーズは、「IEEE 802.1X」（→ P.49）のみサポートしています。

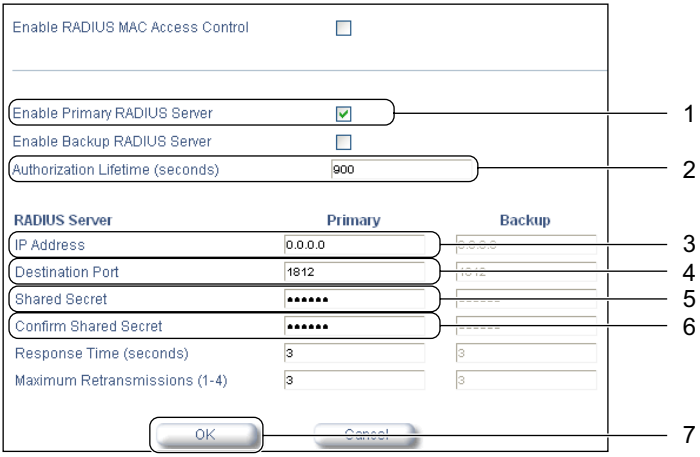
IEEE 802.1X

Web ブラウザの「HTTP インターフェース設定画面」で次のようにセキュリティの設定を行います。

1 「Configure」メニュー→ 「Security」タブ→「RADIUS」タブの順にクリックします。



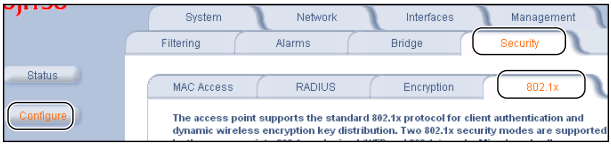
2 次のように RADIUS サーバーの情報を設定します。



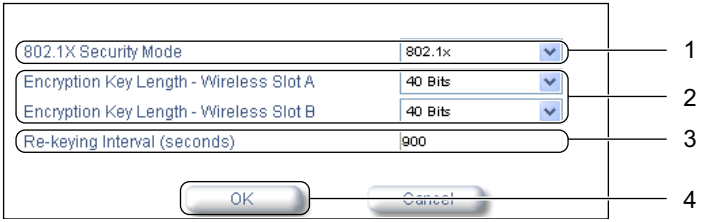
1. Enable Primary RADIUS Server
   クリックして☑にします。

2. Authorization Lifetime
   無線 LAN クライアントの再認証時間（秒）の間隔を 60 ～ 43200 の範囲で設定します。
3. IP Address
   RADIUS サーバーの IP アドレスを入力します。
4. Destination Port
   RADIUS サーバーの認証ポートを入力します。
5. Shared Secret
   RADIUS サーバーの共有シークレットを入力します。
6. Confirm Shared Secret
   確認のため、「Shared Secret」と同じ値を入力します。
7. OK
   この画面の設定が完了したら、クリックします。

3 「Configure」メニュー→「Security」タブ→「802.1x」タブの順にクリックします。



4 次のように、IEEE 802.1X の設定をします。



1. 802.1X Security Mode
   をクリックして「802.1x」を選択します。
2. Encryption Key Length - Wireless Slot A ／ Encryption Key Length - Wireless Slot B
   自動生成するネットワークキーの長さを選択します。
   ネットワークキーの長さは、クライアントの無線 LAN 機能の仕様を考慮する必要があります。
   詳しくは、「各製品の対応状況」（→ P.356）、または各製品のマニュアルをご覧ください。
3. Re-Keying Interval
   ネットワークキーの再配布時間（秒）の間隔を 60 ～ 65535 の範囲で設定します。
4. OK
   この画面の設定が完了したら、クリックします。

5 必要な項目をすべて設定したら、「Commands」メニュー→「Reboot」タブをクリックします。

6 「Reboot」をクリックして、無線 LAN アクセスポイントを再起動します。

Memo

3

第 3 章

クライアントの設定

クライアントの無線 LAN の設定について説明します。

1 クライアントの無線 LAN について

セキュリティの設定方法は搭載されている無線 LAN の種類やパソコンに搭載されている OS によって異なります。

Windows Vista をお使いの場合

パソコンに搭載されている OS が Windows Vista の場合、無線 LAN の設定には、Plugfree NETWORK または Windows Vista 標準の無線 LAN 機能（WLAN Auto Config）をお使いください。
設定方法については、それぞれ次の該当個所をご覧ください。

- Plugfree NETWORK を使って無線 LAN の設定を行う場合は、「Plugfree NETWORK を使った設定」（→ P.265）をご覧ください。
- Windows Vista 標準の無線 LAN 機能を使って無線 LAN の設定を行う場合は、「Windows Vista 標準の無線 LAN 機能を使った設定」（→ P.282）をご覧ください。

Windows XP をお使いの場合

パソコンに搭載されている OS が Windows XP の場合、無線 LAN の設定方法には、各デバイス固有のユーティリティをお使いになる方法と、Mr.WLANner または Windows XP 標準の無線 LAN 機能（Wireless Zero Configuration）をお使いになる方法があります。
Mr.WLANner または Windows XP 標準の無線 LAN 機能（Wireless Zero Configuration）をお使いになる場合は、それぞれ次の該当箇所をご覧ください。

- Mr.WLANner を使って無線 LAN の設定を行う場合は、「Mr.WLANner を使った設定」（→ P.231）をご覧ください。
- Windows XP 標準の無線 LAN 機能を使って無線 LAN の設定を行う場合は、「Windows XP 標準の無線 LAN 機能を使った設定」（→ P.249）をご覧ください。

各デバイス固有のユーティリティをお使いになる場合は、お使いのデバイスと、ユーティリティを確認する必要があります。確認方法については、「デバイス固有のユーティリティで無線 LAN の設定を行う場合」（→ P.54）をご覧ください。

デバイス固有のユーティリティで無線 LAN の設定を行う場合

■ ワイヤレス LAN カードを増設している場合

パソコンにワイヤレス LAN カードを増設してお使いになっている場合は、ワイヤレス LAN カードの裏面ラベルで製品名を確認することができます。このマニュアルでは、次の製品のセキュリティの設定方法について説明しています。

・ラベルに「FMV-JW183 ワイヤレス LAN カード」と記載されている場合
設定方法は、「FMV-JW183 の設定」（→ P.300）をご覧ください。
・ラベルに「FMV-JW481 ワイヤレス LAN カード」または「FMV-JW482 ワイヤレス LAN カード」と記載されている場合
ユーティリティのバージョンによって設定方法が異なります。「Atheros 無線 LAN 搭載モデルのユーティリティバージョン確認方法」（→ P.56）をご覧になり、ユーティリティのバージョンをご確認ください。

■無線 LAN 標準搭載のパソコンをお使いの場合

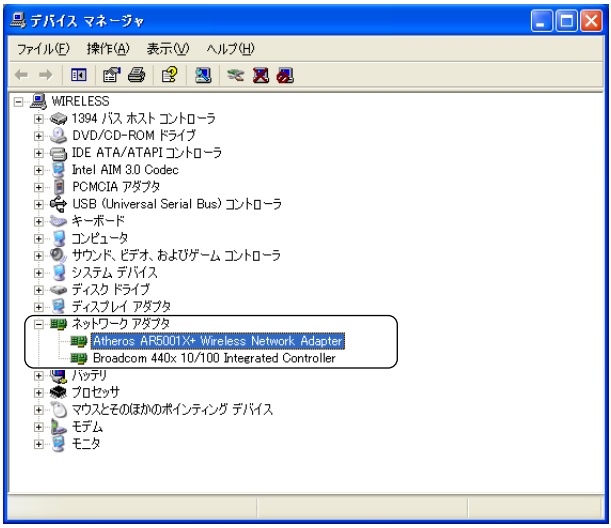
パソコンに無線 LAN 機能が標準搭載されている場合は、次の手順でお使いのパソコンに搭載されている無線 LAN の種類をご確認ください。

1 次のように操作します。

・Windows XP の場合
「スタート」ボタンをクリックして表示されるメニューから「マイコンピュータ」を右クリックし、表示されるメニューから「プロパティ」をクリックします。
・Windows 2000 の場合
デスクトップ画面の「マイコンピュータ」を右クリックし、表示されるメニューから「プロパティ」をクリックします。
「システムのプロパティ」ウィンドウが表示されます。

2 「ハードウェア」タブをクリックして、「デバイス マネージャ」をクリックします。

3 「ネットワークアダプタ」の「+」をクリックして、搭載されている無線 LAN のデバイス名を確認します。



■ 次のいずれかが表示されている場合
・「Atheros AR5001X+ Wireless Network Adapter」

・「Atheros AR5006X+ Wireless Network Adapter」
・「Atheros AR5006EXS Wireless Network Adapter」
「Atheros 無線 LAN 搭載モデル」（本書での表記）です。
このモデルでは、ユーティリティのバージョンにより設定方法が異なりますので、「Atheros 無線 LAN 搭載モデルのユーティリティバージョン確認方法」（→ P.56）でユーティリティのバージョンを確認してください。

■ 次のいずれかが表示されている場合

・「Intel(R) PRO/Wireless 3945ABG Network Connection」
・「Intel(R) PRO/Wireless LAN 2915ABG Network Connection」
・「Intel(R) PRO/Wireless LAN 2200BG Network Connection」
・「Intel(R) PRO/Wireless LAN 2100 3B Mini PCI Adapter」
「Intel 無線 LAN 搭載モデル」（本書での表記）です。
Intel 無線 LAN 搭載モデルでは、ユーティリティのバージョンにより設定方法が異なりますので、「Intel 無線 LAN 搭載モデルのユーティリティバージョン確認方法」（→ P.57）でユーティリティのバージョンを確認してください。

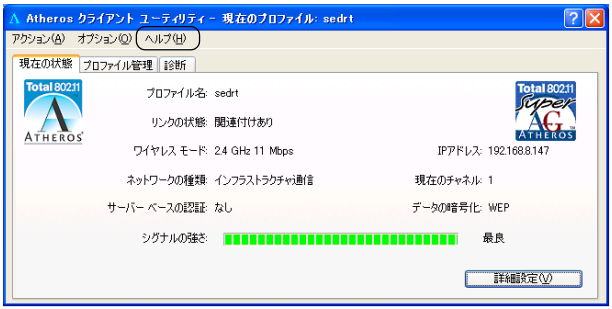
■「Broadcom BCM4306 Wireless LAN Adapter」と表示されている場合
「Broadcom 無線 LAN 搭載モデル」（本書での表記）です。
設定方法は、「Broadcom 無線 LAN 搭載モデルの設定」（→ P.315）をご覧ください。

■「Intersil PRISM Wireless LAN PCI Card」と表示されている場合
「Intersil 無線 LAN 搭載モデル」（本書での表記）です。
設定方法は、「Intersil 無線 LAN 搭載モデルの設定」（→ P.325）をご覧ください。

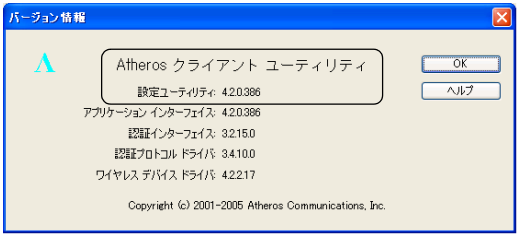
■Atheros 無線 LAN 搭載モデルのユーティリティバージョン確認方法

1 デスクトップ右下の通知領域からユーティリティアイコンを右クリックし、表示されるメニューから「Atheros クライアント ユーティリティを開く」をクリックします。
「Atheros クライアントユーティリティ」ウィンドウが表示されます。

2 「ヘルプ」→「バージョン情報」の順にクリックします。



3 **「バージョン情報」ウィンドウでユーティリティのバージョンを確認します。**



次の説明に記載されている「n」は任意の数字です。

・バージョンが「4.0.n.n」／「4.1.n.n」／「4.2.n.n」の場合
設定方法は、「Atheros 無線 LAN 搭載モデル／ FMV-JW481 ／ FMV-JW482 v4.x 系の設定」（→ P.59）をご覧ください。

・バージョンが「3.1.n.n」の場合
設定方法は、「Atheros 無線 LAN 搭載モデル／ FMV-JW481 v3.x 系の設定」（→ P.74）をご覧ください。

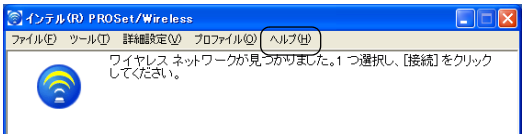
・バージョンが「2.4.n.n」の場合
設定方法は、「Atheros 無線 LAN 搭載モデル／ FMV-JW481 v2.x 系の設定」（→ P.84）をご覧ください。

■Intel 無線 LAN 搭載モデルのユーティリティバージョン確認方法

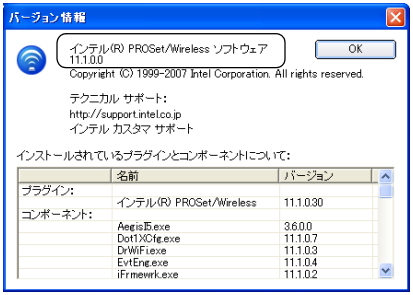
1 **「スタート」ボタン→「すべてのプログラム」→「Intel PROSet Wireless」→「Intel PROSet Wireless」の順にクリックします。**

「インテル (R) PROSet/Wireless」ウィンドウが表示されます。

2 **「ヘルプ」→「バージョン情報」の順にクリックします。**



3 「バージョン情報」ウィンドウでユーティリティのバージョンを確認します。



次の説明に記載されている「n」は任意の数字です。

- バージョンが「11.n.n.n」／「10.5.n.n」の場合
  設定方法は、「Intel 無線 LAN 搭載モデル v11.x 系／ v10.5.x 系の設定」（→ P.94）をご覧ください。
- バージョンが「10.1.n.n」の場合
  設定方法は、「Intel 無線 LAN 搭載モデル v10.1.x 系の設定」（→ P.140）をご覧ください。
- バージョンが「9.0.n.n」の場合
  設定方法は、「Intel 無線 LAN 搭載モデル v9.x 系の設定」（→ P.175）をご覧ください。
- バージョンが「8.1.n.n」／「8.0.n.n」／「7.1.n.n」／「7.0.n.n」の場合
  設定方法は、「Intel 無線 LAN 搭載モデル v8.x 系／ v7.x 系の設定」（→ P.202）をご覧ください。

2 Atheros 無線 LAN 搭載モデル／FMV-JW481 ／ FMV-JW482 v4.x 系の設定

クライアントのパソコンが、Atheros 無線 LAN 搭載モデル、または FMV-JW481 または FMV-JW482 v4.x 系の場合の設定方法を説明します。

重要

Windows XP をお使いのお客様へ

無線 LAN の設定、通信に Atheros クライアントユーティリティをお使いになることをお勧めします。

Atheros クライアントユーティリティで無線 LAN の設定、通信を行う場合、Windows XP の無線 LAN 機能が有効になっていると、通信に支障がありますので、次の手順で Windows XP の無線 LAN 機能を無効にしてください。

1. 「スタート」ボタン→「コントロールパネル」の順にクリックします。
2. 「ネットワークとインターネット接続」をクリックします。
3. 「ネットワーク接続」をクリックします。
   現在インストールされているネットワークの一覧が表示されます。
4. 一覧から「ワイヤレスネットワーク接続」を右クリックして、表示されるメニューから「プロパティ」をクリックします。
   「ワイヤレス ネットワーク接続のプロパティ」ウィンドウが表示されます。
5. 「ワイヤレス ネットワーク」タブをクリックします。
6. 「Windows を使ってワイヤレス ネットワークの設定を構成する」を☑ から☐ にし、「OK」をクリックします。
7. 「ネットワーク接続」ウィンドウの ✕ をクリックします。

POINT

・無線 LAN ネットワークへの接続は、Windows によって起動されるサービスである、Atheros Configuration Service が起動してから開始されます。ドメイン環境で使用する場合は、ネットワーク接続が確立するのを待ってからログオンする必要があります。

IEEE 802.1X ＋ EAP-TLS ／ WPA ＋ EAP-TLS ／ WPA2 ＋ EAP-TLS

次のセキュリティパターンの場合の設定方法を説明します。

・IEEE 802.1X ＋ EAP-TLS
・WPA ＋ EAP-TLS
・WPA2 ＋ EAP-TLS

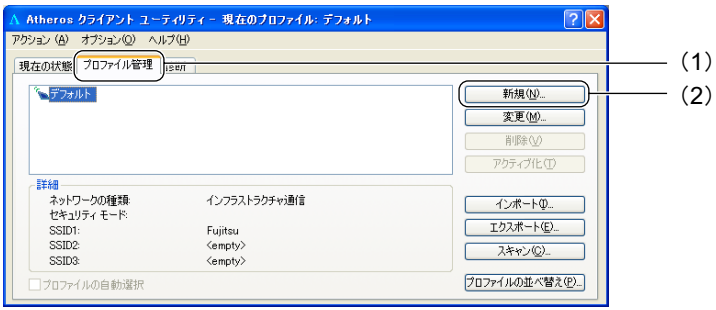
重要

・事前にユーザー認証に使用する電子証明書を、ユーザーごとにインストールする必要があります。
・複数ユーザーで運用する場合は、ユーザーごとにプロファイルを作成し、ログオン後にプロファイルを切り替えてお使いください。なお、コンピューター起動時にアクティブになるプロファイルは、シャットダウンおよび再起動前にアクティブだったプロファイルです。

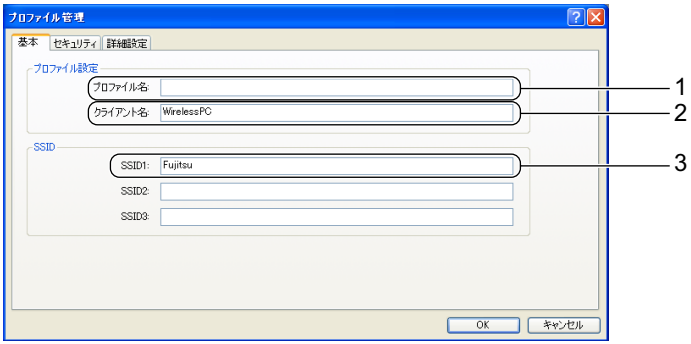
1 デスクトップ右下の通知領域からユーティリティアイコンを右クリックし、表示されるメニューから「Atheros クライアント ユーティリティを開く」をクリックします。

「Atheros クライアントユーティリティ」ウィンドウが表示されます。

2 (1)「プロファイル管理」タブをクリックし、(2)「新規」をクリックします。



3「プロファイル管理」ウィンドウで次のように設定します。

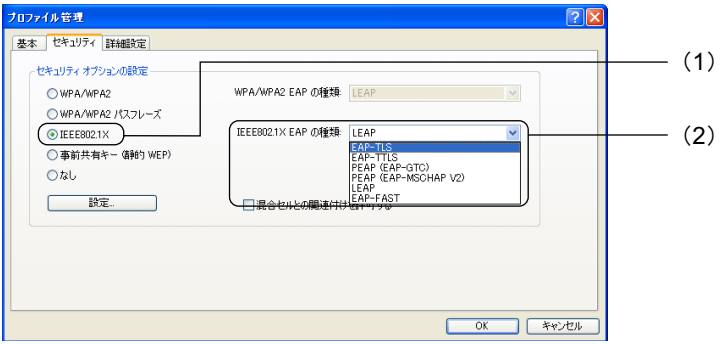


1. プロファイルを識別するためのプロファイル名を設定します。
   半角英数字、半角記号、および全角文字(日本語)で入力できます(32 文字以内)。
2. 「クライアント名」は変更する必要はありません。
3. 「SSID1」を入力します。
   ネットワーク名（SSID）を接続する無線 LAN アクセスポイントに合わせて設定します。
   「SSID2」／「SSID3」は、使用できません。設定を行わないでください。

4 「セキュリティ」タブをクリックし、次のように設定します。

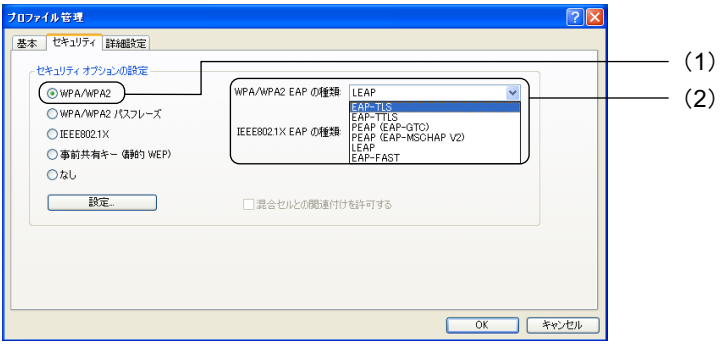
■ IEEE 802.1X の場合

1. (1)「IEEE802.1X」をクリックして にし、(2)「IEEE802.1X EAP の種類」の をクリックして「EAP-TLS」を選択します。



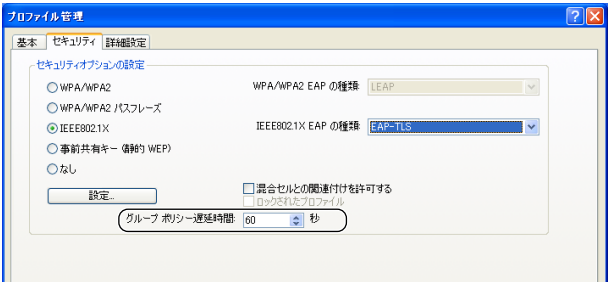
■ WPA ／ WPA2 の場合

1. (1)「WPA/WPA2」をクリックして にし、(2)「WPA/WPA2 EAP の種類」の をクリックして「EAP-TLS」を選択します。



POINT

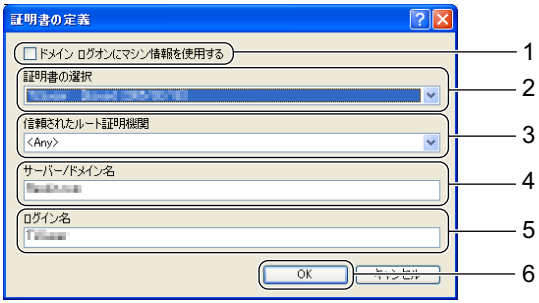
・v4.2.x.x を使用している場合に表示される「グループ ポリシー遅延時間」の機能は未サポートです。



5 「設定」をクリックします。

「証明書の定義」ウィンドウが表示されます。

6 次の設定を行います。



1. ドメイン環境で使用する場合は、「ドメイン ログオンにマシン情報を使用する」をクリックして☑にします。
   ドメイン環境で使用する場合は、本設定のほかに「ドメイン環境で使用する場合」（→ P.62）の設定を行う必要があります。
2. 「証明書の選択」の ⌄ をクリックして、インストールしたクライアントの証明書を選択します。
3. 「信頼されたルート証明機関」の ⌄ をクリックして、インストールした RADIUS サーバーの証明書の証明機関を選択します。
4. 「サーバー／ドメイン名」を入力します。
   RADIUS サーバーのフルコンピューター名または、RADIUS サーバーのドメイン名を入力します。
   自動的に検出される場合もあります。
5. 「ログイン名」を入力します。
   セキュリティグループに登録された、認証用のユーザー名を入力します。
   自動的に検出される場合もあります。
6. 設定が終わったら、「OK」をクリックします。

POINT

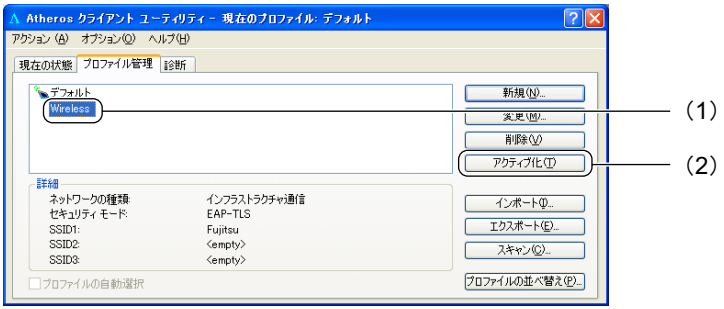
ドメイン環境で使用する場合

「ドメイン ログオンにマシン情報を使用する」の設定のほかに、お使いになるパソコンで次の設定をする必要があります。

- ログオン前に通信を行うために、コンピューター証明書をインストールします。
- ドメインログオンに使用するドメインユーザーアカウントに対して、ローカルコンピューターの管理者権限を設定します。
- シングルサインオンを無効にします。シングルサインオンを有効にしている場合は、ドライバをインストールし直す必要があります。

7 **「プロファイル管理」ウィンドウで「OK」をクリックします。**

8 **「Atheros クライアントユーティリティ」ウィンドウの「プロファイル管理」タブの画面で、(1) 作成したプロファイルを選択して、(2)「アクティブ化」をクリックします。**



IEEE 802.1X ＋ PEAP-MSCHAPv2 ／ WPA ＋ PEAP-MSCHAPv2 ／ WPA2 ＋ PEAP-MSCHAPv2

次のセキュリティパターンの場合の設定方法を説明します。

・IEEE 802.1X ＋ PEAP-MSCHAPv2
・WPA ＋ PEAP-MSCHAPv2
・WPA2 ＋ PEAP-MSCHAPv2

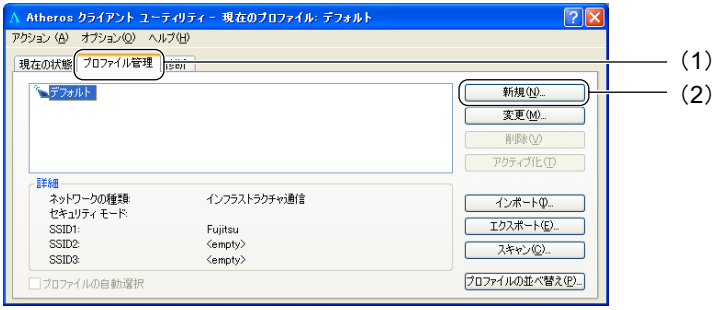
POINT

・双方向認証のみサポートしています。事前にサーバー認証に使用する電子証明書をインストールする必要があります。

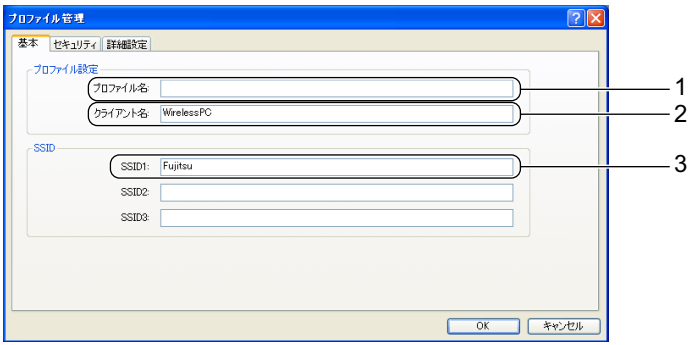
1 **デスクトップ右下の通知領域からユーティリティアイコンを右クリックし、表示されるメニューから「Atheros クライアント ユーティリティを開く」をクリックします。**

「Atheros クライアントユーティリティ」ウィンドウが表示されます。

2 (1)「プロファイル管理」タブをクリックし、(2)「新規」をクリックします。



3 「プロファイル管理」ウィンドウで次のように設定します。

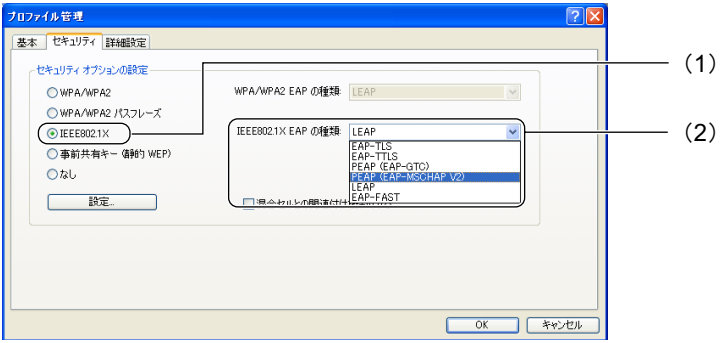


1. プロファイルを識別するための「プロファイル名」を入力します。
   半角英数字、半角記号、および全角文字(日本語)で入力できます(32 文字以内)。
2. 「クライアント名」は変更する必要はありません。
3. 「SSID1」を入力します。
   ネットワーク名（SSID）を接続する無線 LAN アクセスポイントに合わせて設定します。
   「SSID2」／「SSID3」は、使用できません。設定を行わないでください。

4 「セキュリティ」タブをクリックし、次のように設定します。

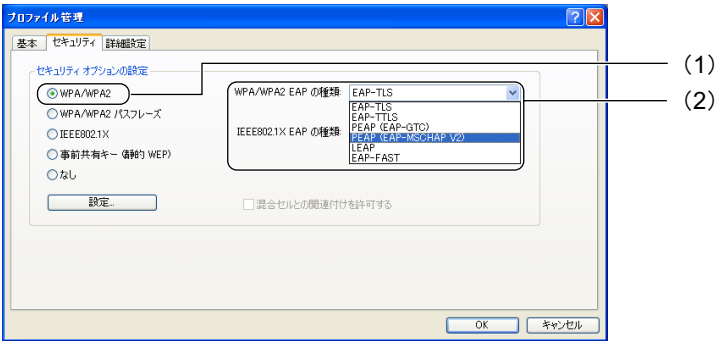
■ IEEE 802.1X の場合

1. (1)「IEEE802.1X」をクリックして にし、(2)「IEEE802.1X EAP の種類」の をクリックして「PEAP (EAP-MSCHAP V2)」を選択します。



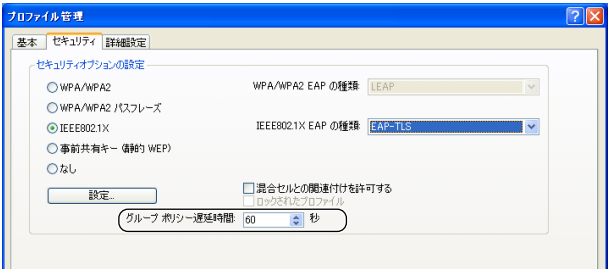
■ WPA ／ WPA2 の場合

1. (1)「WPA/WPA2」をクリックして にし、(2)「WPA/WPA2 EAP の種類」の をクリックして「PEAP (EAP-MSCHAP V2)」を選択します。



POINT

・v4.2.x.x を使用している場合に表示される「グループ ポリシー遅延時間」の機能は未サポートです。

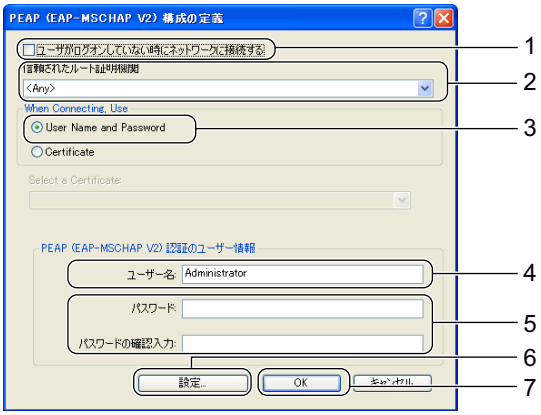


5 「設定」をクリックします。

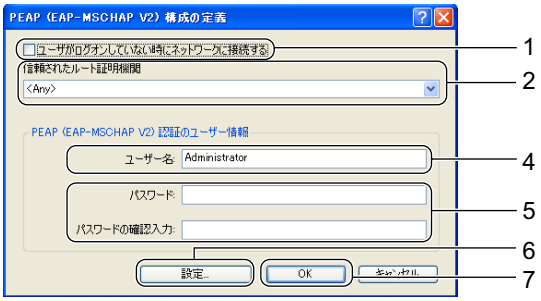
「PEAP (EAP-MSCHAP V2) 構成の定義」ウィンドウが表示されます。

6 次の設定を行います。

■ v4.2.2.7 以降をご使用の場合

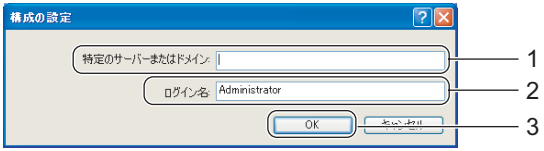


■ 上記以前の版数をご使用の場合



1. ドメイン環境で使用する場合は、「ユーザがログオンしていない時にネットワークに接続する」をクリックして☑にします。
   Windows にログオンしていない状態でも、Atheros クライアントユーティリティに設定したユーザー情報を使用してネットワークに接続できるようになります。
   Atheros クライアントユーティリティに設定した固定のユーザー名とパスワードで無線 LAN 認証を行うことにより、ドメインユーザーでログオンすることができます。
2. 「信頼されたルート証明機関」の ⌄ をクリックして、インストールした RADIUS サーバーの証明書の証明機関を選択します。
3. v4.2.2.7 以降をご使用の場合は、「User Name and Password」を選択します。
   上記以前の版数をご使用の場合は、本項目の設定はありません。
4. 「ユーザー名」に認証に使用するユーザー名を入力します。
   自動的に検出される場合もあります。

5. 「パスワード」と「パスワードの確認入力」に、認証に使用するユーザーのパスワードを入力します。
6. 「設定」をクリックして、認証ユーザーの詳細を設定します。
「構成の設定」ウィンドウで設定を行います。

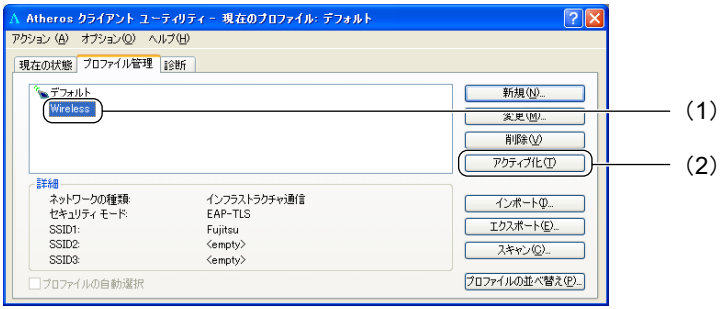


1. 「特定のサーバーまたはドメイン」
RADIUS サーバーのフルコンピューター名または、RADIUS サーバーのドメイン名を入力します。
2. 「ログイン名」
認証に使用するユーザー名を入力します。「PEAP (EAP-MSCHAP V2) の設定」ウィンドウで設定した内容と同じものです。
自動的に検出される場合もあります。
3. 「OK」
設定が終了したら「OK」をクリックします。

7. 設定が終了したら、「OK」をクリックします。

7 「プロファイル管理」ウィンドウで「OK」をクリックします。

8 「Atheros クライアントユーティリティ」ウィンドウの「プロファイル管理」タブの画面で、(1) 作成したプロファイルを選択して、(2)「アクティブ化」をクリックします。



IEEE 802.1X-PEAP-TLS ／ WPA-PEAP-TLS ／ WPA2-PEAP-TLS

次のセキュリティパターンの場合の設定方法を説明します。

- IEEE 802.1X ＋ PEAP-TLS
- WPA ＋ PEAP-TLS
- WPA2 ＋ PEAP-TLS

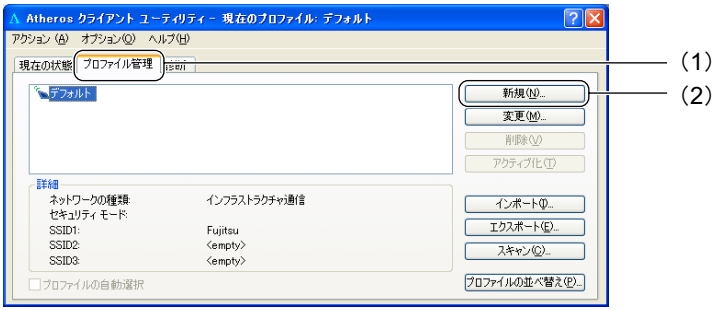
重要

・この認証方式が使用できるのは、v4.2.x.x 以降のユーティリティになります。
・ユーザー証明書を使用する場合は、ユーザー認証に使用する電子証明書を、事前に認証するユーザーごとにインストールする必要があります。
・複数ユーザーで運用する場合は、ユーザーごとにプロファイルを作成し、ログオン後にプロファイルを切り替えてお使いください。なお、コンピューター起動時にアクティブになるプロファイルは、シャットダウンおよび再起動前にアクティブだったプロファイルです。
・ドメイン環境での運用は未サポートです。

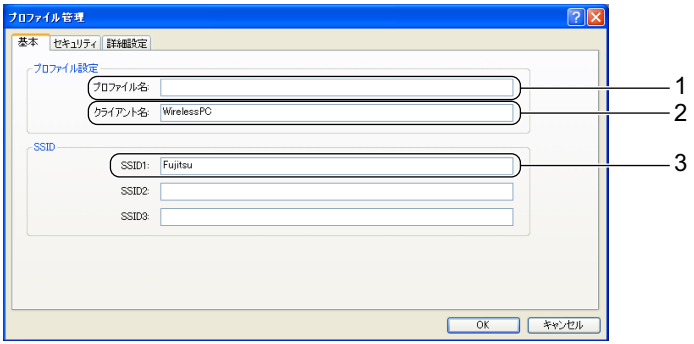
1 **デスクトップ右下の通知領域からユーティリティアイコンを右クリックし、表示されるメニューから「Atheros クライアント ユーティリティを開く」をクリックします。**

「Atheros クライアントユーティリティ」ウィンドウが表示されます。

2 **(1)「プロファイル管理」タブをクリックし、(2)「新規」をクリックします。**



3 **「プロファイル管理」ウィンドウで次のように設定します。**



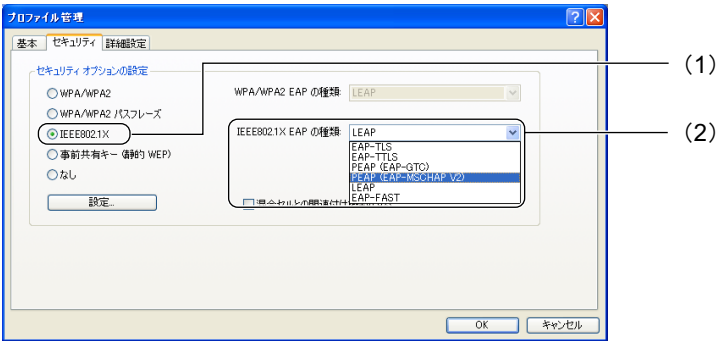
1. プロファイルを識別するための「プロファイル名」を入力します。
   半角英数字、半角記号、および全角文字(日本語)で入力できます(32 文字以内)。
2. 「クライアント名」は変更する必要はありません。

3.「SSID1」を入力します。
ネットワーク名（SSID）を接続する無線 LAN アクセスポイントに合わせて設定します。
「SSID2」／「SSID3」は、使用できません。設定を行わないでください。

4 「セキュリティ」タブをクリックし、次のように設定します。

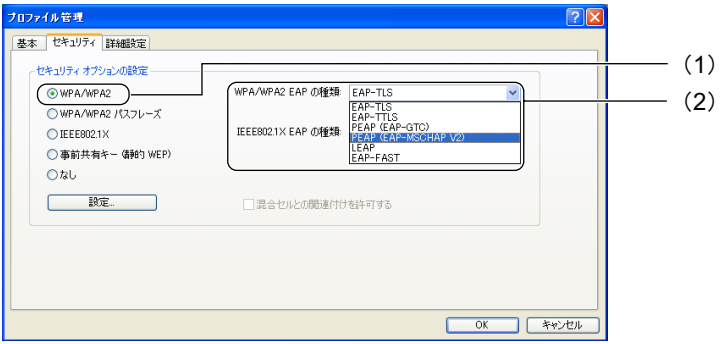
■ IEEE 802.1X の場合

1.（1）「IEEE802.1X」をクリックして にし、（2）「IEEE802.1X EAP の種類」の をクリックして「PEAP (EAP-MSCHAP V2)」を選択します。



■ WPA ／ WPA2 の場合

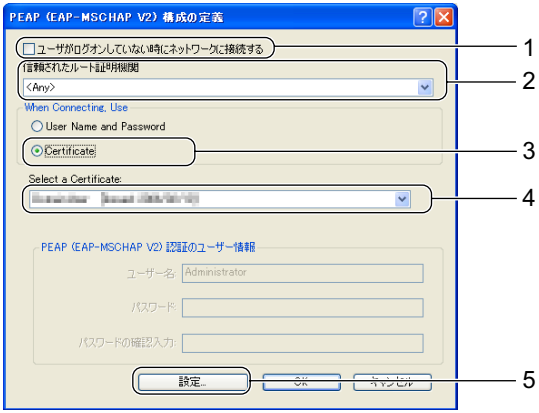
1.（1）「WPA/WPA2」をクリックして にし、（2）「WPA/WPA2 EAP の種類」の をクリックして「PEAP (EAP-MSCHAP V2)」を選択します。



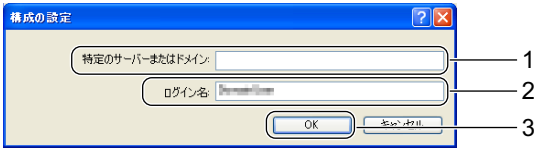
5 「設定」をクリックします。

「PEAP (EAP-MSCHAP V2) 構成の定義」ウィンドウが表示されます。

6 次の設定を行います。



1. 「ユーザがログオンしていない時にネットワークに接続する」をクリックして☐にします。
2. 「信頼されたルート証明機関」の をクリックして、インストールしたRADIUSサーバーの証明書の証明機関を選択します。
3. 「Certificate」をクリックして◉にします。
4. 「Select a Certificate:」の をクリックして、インストールしたクライアントの証明書を選択します。
5. 「設定」をクリックして、次のように設定します。

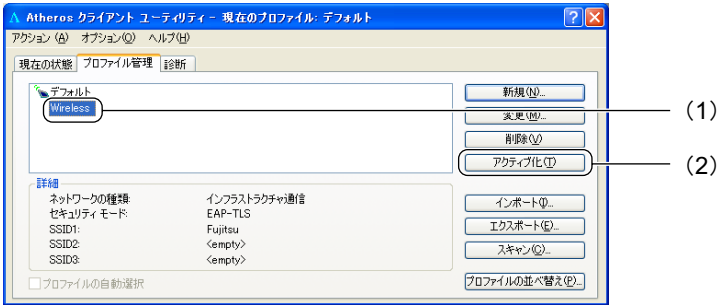


1. 「特定のサーバーまたはドメイン」を入力します。
   RADIUS サーバーのフルコンピューター名または、RADIUS サーバーのドメイン名を入力します。自動的に検出される場合もあります。
2. 「ログイン名」を入力します。
   「ログイン名」を入力します。セキュリティグループに登録された、認証用のユーザー名を入力します。自動的に検出される場合もあります。
3. 設定が終わったら「OK」をクリックします。

7 **設定が終わったら、「PEAP (EAP-MSCHAP V2) 構成の定義」ウィンドウで「OK」をクリックします。**

8 **「プロファイル管理」ウィンドウで「OK」をクリックします。**

9 **「Atheros クライアントユーティリティ」ウィンドウの「プロファイル管理」タブの画面で、(1) 作成したプロファイルを選択して、(2)「アクティブ化」をクリックします。**



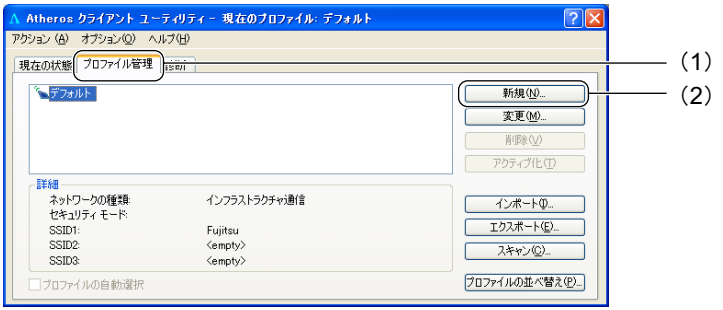
WPA-PSK ／ WPA2-PSK

WPA-PSK ／ WPA2-PSK の場合の設定方法を説明します。

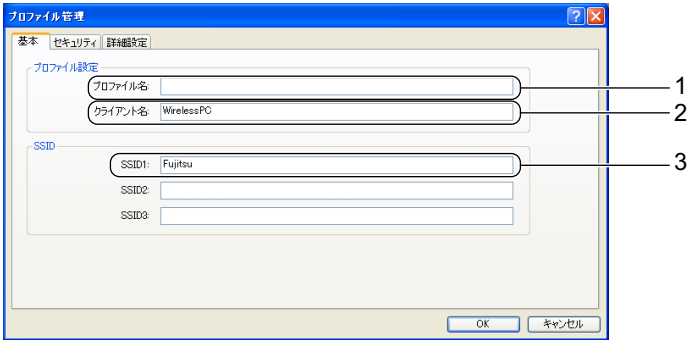
1 **デスクトップ右下の通知領域からユーティリティアイコンを右クリックし、表示されるメニューから「Atheros クライアント ユーティリティを開く」をクリックします。**

「Atheros クライアントユーティリティ」ウィンドウが表示されます。

2 **(1)「プロファイル管理」タブをクリックし、(2)「新規」をクリックします。**

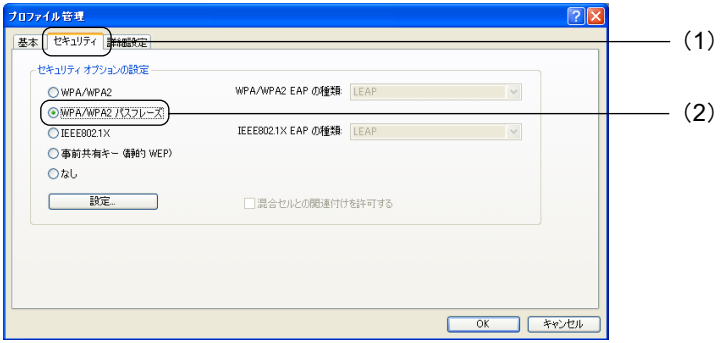


3 「プロファイル管理」ウィンドウで次のように設定します。



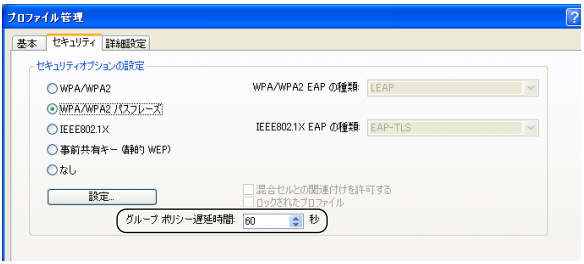
1. プロファイルを識別するための「プロファイル名」を入力します。
   半角英数字、半角記号、および全角文字（日本語）で入力できます（32 文字以内）。
2. 「クライアント名」は変更する必要はありません。
3. 「SSID1」を入力します。
   ネットワーク名（SSID）を接続する無線 LAN アクセスポイントに合わせて設定します。
   「SSID2」／「SSID3」は、使用できません。設定を行わないでください。

4 (1)「セキュリティ」タブをクリックし、(2)「WPA/WPA2 パスフレーズ」をクリックして◉にします。



POINT

・v4.2.x.x を使用している場合に表示される「グループ ポリシー遅延時間」の機能は未サポートです。

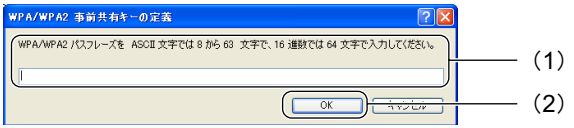


5 **「設定」をクリックします。**

「WPA/WPA2 事前共有キーの定義」ウィンドウが表示されます。

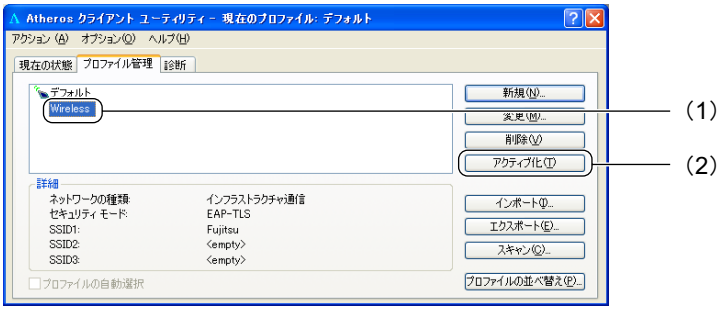
6 **(1)PSK(WPA/WPA パスフレーズ)を設定し、(2)「OK」をクリックします。**

無線 LAN アクセスポイントと同じ値を設定してください。8 文字以上 63 文字以下は ASCII 文字、64 文字は 16 進数での入力になります。



7 **「プロファイル管理」ウィンドウで「OK」をクリックします。**

8 **「Atheros クライアントユーティリティ」ウィンドウの「プロファイル管理」タブの画面で、(1) 作成したプロファイルを選択して、(2)「アクティブ化」をクリックします。**



3 Atheros 無線 LAN 搭載モデル／FMV-JW481 v3.x 系の設定

クライアントのパソコンが、Atheros 無線 LAN 搭載モデル、または FMV-JW481 v3.x 系の場合の設定方法を説明します。

重要

Windows XP をお使いのお客様へ

無線 LAN の設定、通信に Atheros Client Utility をお使いになることをお勧めします。
Atheros Client Utility で無線 LAN の設定、通信を行う場合、Windows XP の無線 LAN 機能が有効になっていると、通信に支障がありますので、次の手順で Windows XP の無線 LAN 機能を無効にしてください。

1. 「スタート」ボタン→「コントロールパネル」の順にクリックします。
2. 「ネットワークとインターネット接続」をクリックします。
3. 「ネットワーク接続」をクリックします。
   現在インストールされているネットワークの一覧が表示されます。
4. 一覧から「ワイヤレスネットワーク接続」を右クリックして、表示されるメニューから「プロパティ」をクリックします。
   「ワイヤレス ネットワーク接続のプロパティ」ウィンドウが表示されます。
5. 「ワイヤレス ネットワーク」タブをクリックします。
6. 「Windows を使ってワイヤレス ネットワークの設定を構成する」を☑から☐にし、「OK」をクリックします。
7. 「ネットワーク接続」ウィンドウの  をクリックします。

IEEE 802.1X ＋ EAP-TLS ／ WPA ＋ EAP-TLS

次のセキュリティパターンの場合の設定方法を説明します。

- IEEE 802.1X ＋ EAP-TLS
- WPA ＋ EAP-TLS

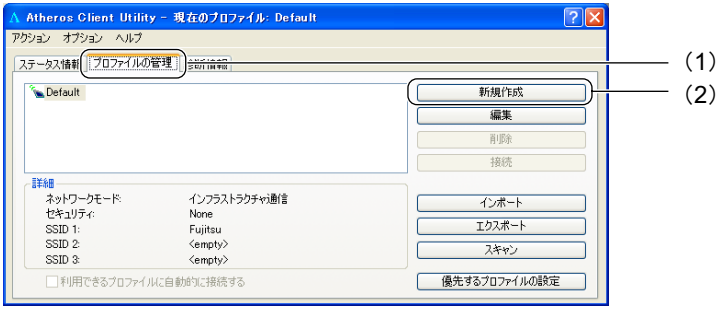
重要

- 事前にユーザー認証に使用する電子証明書を、ユーザーごとにインストールする必要があります。
- 複数ユーザーで運用する場合は、ユーザーごとにプロファイルを作成し、ログオン後にプロファイルを切り替えてお使いください。なお、コンピューター起動時にアクティブになるプロファイルは、シャットダウンおよび再起動前にアクティブだったプロファイルです。
- ドメイン環境での運用は未サポートです。

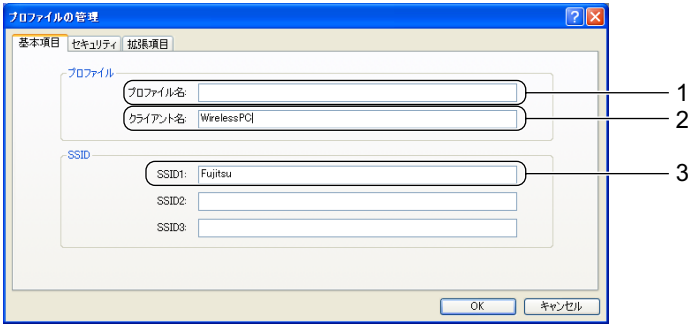
1 デスクトップ右下の通知領域からユーティリティアイコンを右クリックし、表示されるメニューから「ユーティリティを開く」をクリックします。

「Atheros Client Utility」ウィンドウが表示されます。

2 (1)「プロファイルの管理」タブをクリックし、(2)「新規作成」をクリックします。



3 「プロファイルの管理」ウィンドウで次のように設定します。

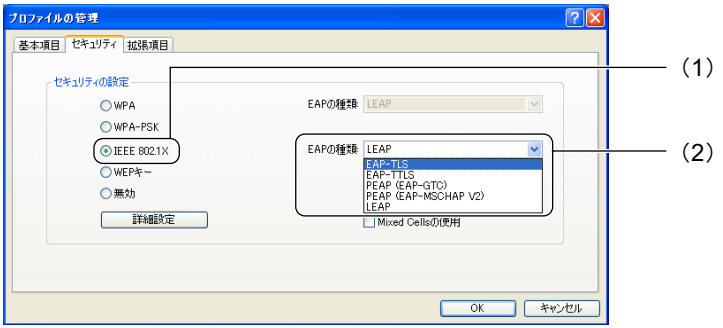


1. 「プロファイル名」を入力します。
   半角英数字、および半角記号 32 文字以内で入力します。
2. 「クライアント名」は変更する必要はありません。
3. 「SSID1」を入力します。
   ネットワーク名（SSID）を接続する無線 LAN アクセスポイントに合わせて設定します。
   「SSID2」／「SSID3」は、使用できません。設定を行わないでください。

4 「セキュリティ」タブをクリックし、次のように設定します。

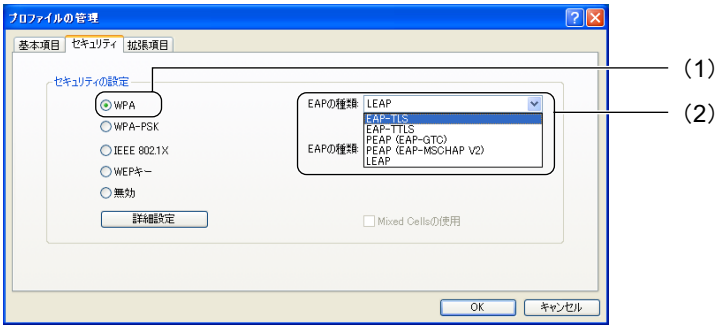
■ IEEE 802.1X の場合

1. (1)「IEEE 802.1X」をクリックして にし、(2)「EAP の種類」の をクリックして「EAP-TLS」を選択します。



■ WPA の場合

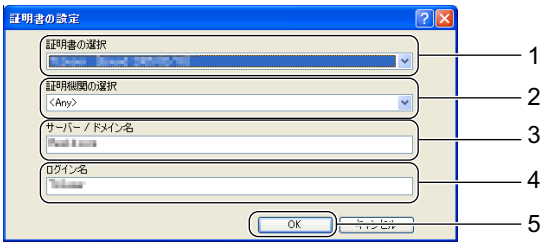
1. (1)「WPA」をクリックして にし、(2)「EAP の種類」の をクリックして「EAP-TLS」を選択します。



5 「詳細設定」をクリックします。

「証明書の設定」ウィンドウが表示されます。

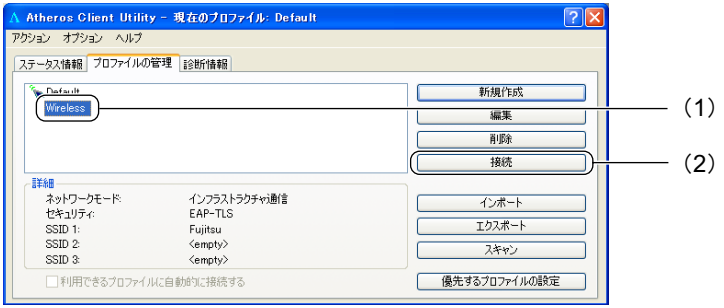
6 次の設定を行います。



1. 「証明書の選択」の をクリックして、インストールしたクライアントの証明書を選択します。
2. 「証明機関の選択」の をクリックして、インストールした RADIUS サーバーの証明書の証明機関を選択します。
3. 「サーバー／ドメイン名」を入力します。
   RADIUS サーバーのフルコンピューター名または、RADIUS サーバーのドメイン名を入力します。
   自動的に検出される場合もあります。
4. 「ログイン名」を入力します。
   セキュリティグループに登録された、認証用のユーザー名を入力します。
   自動的に検出される場合もあります。
5. 以上の設定が終わったら、「OK」をクリックします。

7 「プロファイルの管理」ウィンドウで「OK」をクリックします。

8 「Atheros Client Utility」ウィンドウの「プロファイルの管理」タブの画面で、(1)作成したプロファイルを選択して、(2)「接続」をクリックします。



IEEE 802.1X ＋ PEAP-MSCHAPv2 ／ WPA ＋ PEAP-MSCHAPv2

次のセキュリティパターンの場合の設定方法を説明します。

- IEEE 802.1X ＋ PEAP-MSCHAPv2
- WPA ＋ PEAP-MSCHAPv2

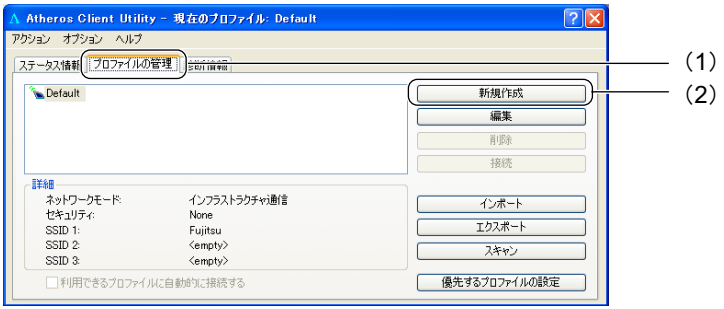
重要

- 双方向認証のみサポートしています。事前にサーバー認証に使用する電子証明書をインストールする必要があります。
- 複数ユーザーで運用する場合は、ユーザーごとにプロファイルを作成し、ログオン後にプロファイルを切り替えてお使いください。なお、コンピューター起動時にアクティブになるプロファイルは、シャットダウンおよび再起動前にアクティブだったプロファイルです。
- ドメイン環境での運用は未サポートです。

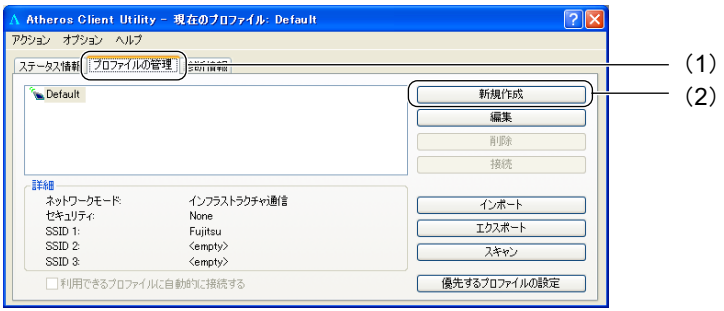
1 **デスクトップ右下の通知領域からユーティリティアイコンを右クリックし、表示されるメニューから「ユーティリティを開く」をクリックします。**

「Atheros Client Utility」ウィンドウが表示されます。

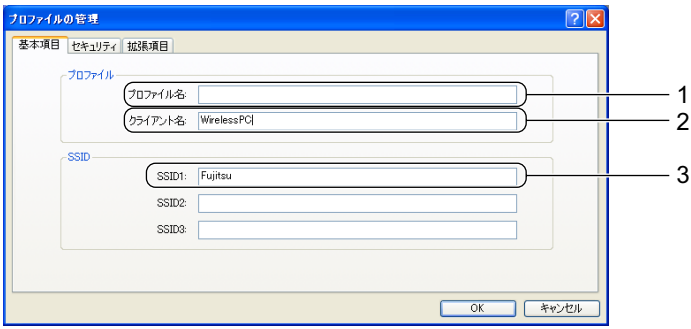
2 **(1)「プロファイルの管理」タブをクリックし、(2)「新規作成」をクリックします。**



3 **(1)「プロファイルの管理」タブをクリックし、(2)「新規作成」をクリックします。**



4 **「プロファイルの管理」ウィンドウで次のように設定します。**



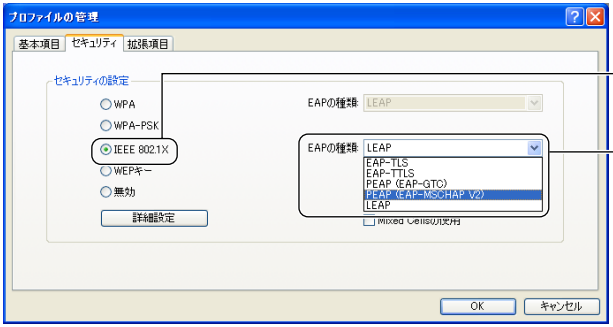
1. 「プロファイル名」を入力します。
   半角英数字、および半角記号 32 文字以内で入力します。

2.「クライアント名」は変更する必要はありません。
3.「SSID1」を入力します。
ネットワーク名（SSID）を接続する無線 LAN アクセスポイントに合わせて設定します。
「SSID2」／「SSID3」は、使用できません。設定を行わないでください。

5 「セキュリティ」タブをクリックし、次のように設定します。

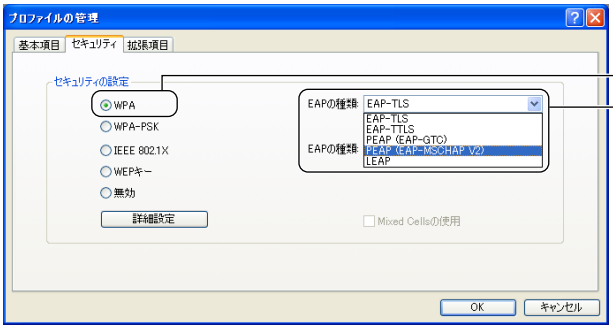
■ IEEE 802.1X の場合

1.（1）「IEEE 802.1X 」をクリックして にし、（2）「EAP の種類」の をクリックして「PEAP (EAP-MSCHAP V2)」を選択します。



■ WPA の場合

1.（1）「WPA」をクリックして にし、（2）「EAP の種類」の をクリックして「PEAP (EAP-MSCHAP V2)」を選択します。

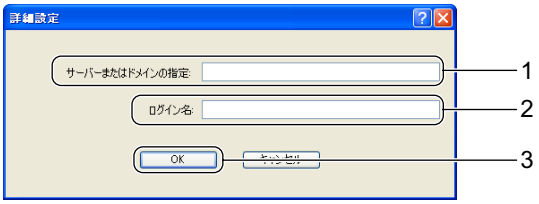


6 「詳細設定」をクリックします。

「PEAP (EAP-MSCHAP V2) の設定」ウィンドウが表示されます。

7 次の設定を行います。

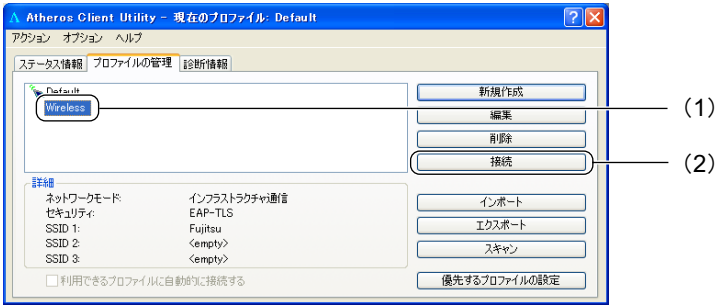
1. 「証明機関の選択」の をクリックして、インストールしたクライアントの証明書を選択します。
2. 「ユーザー名」に、認証に使用するユーザー名を入力します。
   自動的に検出される場合もあります。
3. 「パスワード」と「パスワードの確認」に、認証に使用するユーザーのパスワードを入力します。
4. 「詳細設定」をクリックして、認証ユーザーの詳細を設定します。
   「詳細設定」ウィンドウで設定を行います。



   1. 「サーバーまたはドメインの指定」
      RADIUS サーバーのフルコンピューター名または、RADIUS サーバーのドメイン名を入力します。
   2. 「ログイン名」
      認証に使用するユーザー名を入力します。「PEAP (EAP-MSCHAP V2) の設定」ウィンドウで設定した内容と同じものです。
   3. 「OK」
      設定が終了したら、「OK」をクリックします。
5. 設定が終了したら、「OK」をクリックします。

8 **「プロファイルの管理」ウィンドウで「OK」をクリックします。**

9 **「Atheros Client Utility」ウィンドウの「プロファイルの管理」タブの画面で、(1)作成したプロファイルを選択して、(2)「接続」をクリックします。**



WPA-PSK

WPA-PSK の場合の設定方法を説明します。

重要

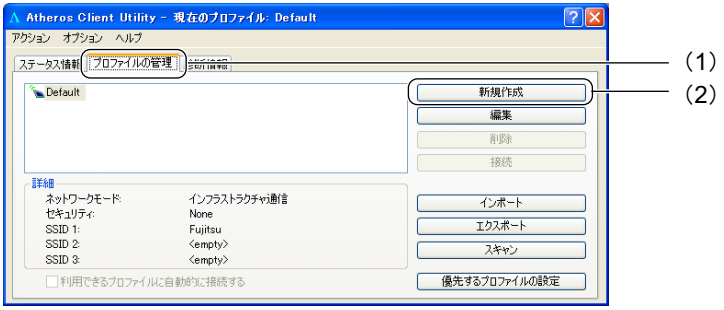
ドメインログオンを使用する場合

v3.1.2.40 以降のバージョンのドライバでは、Windows へのログオン前およびログオフ後も無線 LAN ネットワークに接続されますので、ドメイン環境での運用が可能です。ただし、無線 LAN ネットワークへの接続は、Windows によって起動されるサービスである、Atheros Configuration Service が起動してから開始されますので、ログオンする場合には、ネットワーク接続が確立するのを待つ必要があります。

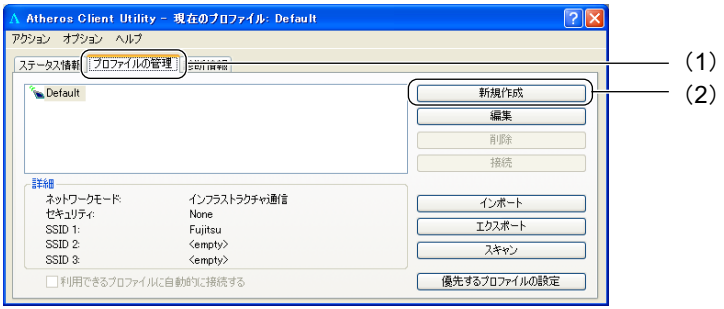
1 **デスクトップ右下の通知領域からユーティリティアイコンを右クリックし、表示されるメニューから「ユーティリティを開く」をクリックします。**

「Atheros Client Utility」ウィンドウが表示されます。

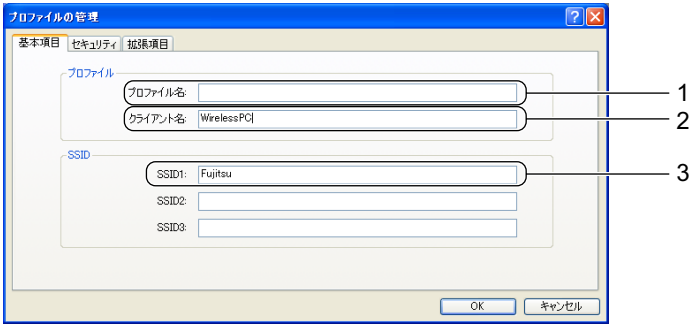
2 (1)「プロファイルの管理」タブをクリックし、(2)「新規作成」をクリックします。



3 (1)「プロファイルの管理」タブをクリックし、(2)「新規作成」をクリックします。

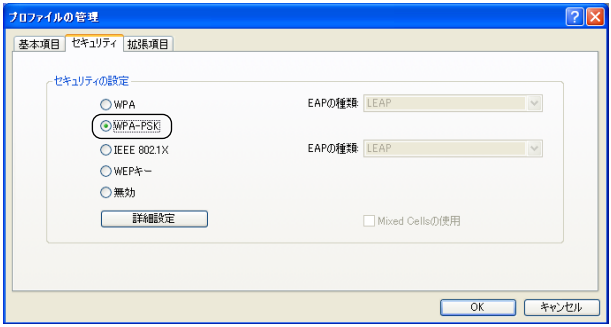


4 「プロファイルの管理」ウィンドウで次のように設定します。



1. 「プロファイル名」を入力します。
   半角英数字、および半角記号 32 文字以内で入力します。
2. 「クライアント名」は変更する必要はありません。
3. 「SSID1」を入力します。
   ネットワーク名（SSID）を接続する無線 LAN アクセスポイントに合わせて設定します。「SSID2」／「SSID3」は、使用できません。設定を行わないでください。

5 **(1)「WPA-PSK」をクリックして◉にします。**

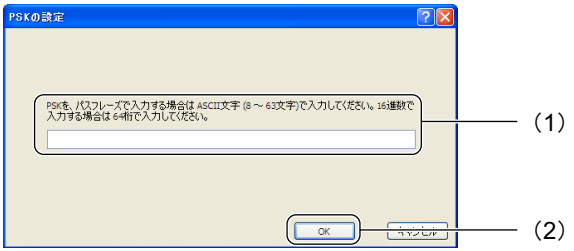


6 **「詳細設定」をクリックします。**

「PSK の設定」ウィンドウが表示されます。

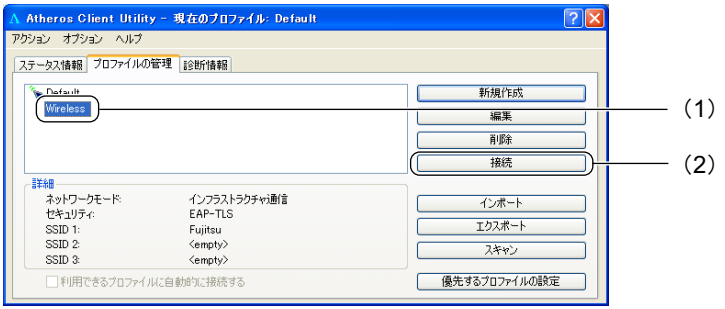
7 **(1) PSK を設定し、(2)「OK」をクリックします。**

無線 LAN アクセスポイントと同じ値を設定してください。8 文字以上 63 文字以下は ASCII 文字、64 文字は 16 進数での入力になります。



8 **「プロファイルの管理」ウィンドウで「OK」をクリックします。**

9 **「Atheros Client Utility」ウィンドウの「プロファイルの管理」タブの画面で、(1) 作成したプロファイルを選択して、(2)「接続」をクリックします。**



4 Atheros 無線 LAN 搭載モデル／FMV-JW481 v2.x 系の設定

クライアントのパソコンが、Atheros 無線 LAN 搭載モデル、または FMV-JW481 v2.x 系の場合の設定方法を説明します。

重要

Windows XP をお使いのお客様へ

無線 LAN の設定、通信に Atheros Client Utility をお使いになることをお勧めします。
Atheros Client Utility で無線 LAN の設定、通信を行う場合、Windows XP の無線 LAN 機能が有効になっていると、通信に支障がありますので、次の手順で Windows XP の無線 LAN 機能を無効にしてください。

1. 「スタート」ボタン→「コントロールパネル」の順にクリックします。
2. 「ネットワークとインターネット接続」をクリックします。
3. 「ネットワーク接続」をクリックします。
   現在インストールされているネットワークの一覧が表示されます。
4. 一覧から「ワイヤレスネットワーク接続」を右クリックして、表示されるメニューから「プロパティ」をクリックします。
   「ワイヤレス ネットワーク接続のプロパティ」ウィンドウが表示されます。
5. 「ワイヤレス ネットワーク」タブをクリックします。
6. 「Windows を使ってワイヤレス ネットワークの設定を構成する」を☑から☐にし、「OK」をクリックします。
7. 「ネットワーク接続」ウィンドウの  をクリックします。

IEEE 802.1X ＋ EAP-TLS ／ WPA ＋ EAP-TLS

次のセキュリティパターンの場合の設定方法を説明します。

- IEEE 802.1X ＋ EAP-TLS
- WPA ＋ EAP-TLS

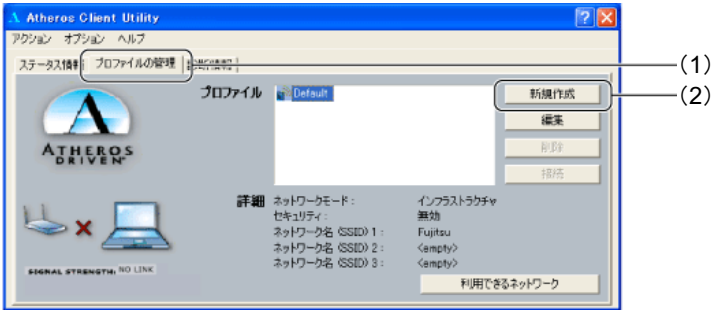
重要

- 事前にユーザー認証に使用する電子証明書を、ユーザーごとにインストールする必要があります。
- 複数ユーザーで運用する場合は、ユーザーごとにプロファイルを作成し、ログオン後にプロファイルを切り替えてお使いください。なお、コンピューター起動時にアクティブになるプロファイルは、シャットダウンおよび再起動前にアクティブだったプロファイルです。
- ドメイン環境での運用は未サポートです。

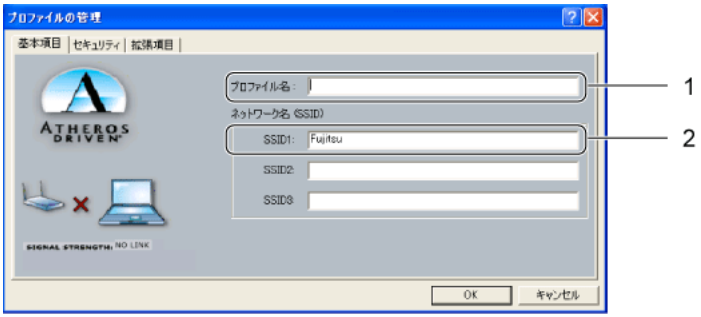
1 デスクトップ右下の通知領域からユーティリティアイコン（  ）を右クリックし、表示されるメニューから「ユーティリティを開く」をクリックします。

「Atheros Client Utility」ウィンドウが表示されます。

2 (1)「プロファイルの管理」タブをクリックし、(2)「新規作成」をクリックします。



3 「プロファイルの管理」ウィンドウで次のように設定します。



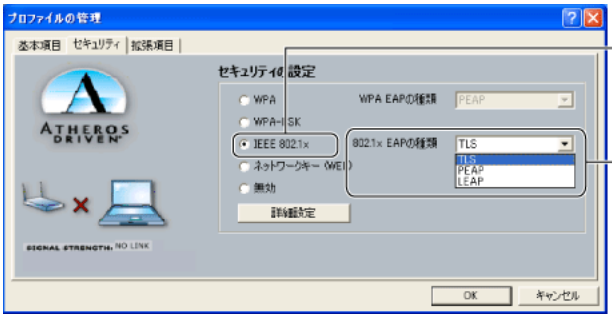
1. 「プロファイル名」を入力します。
   半角英数字、および半角記号 32 文字以内で入力します。
2. 「SSID1」を入力します。
   ネットワーク名（SSID）を接続する無線 LAN アクセスポイントに合わせて設定します。
   「SSID2」／「SSID3」は、使用できません。設定を行わないでください。

4 「セキュリティ」タブをクリックします。

5 次のように操作します。

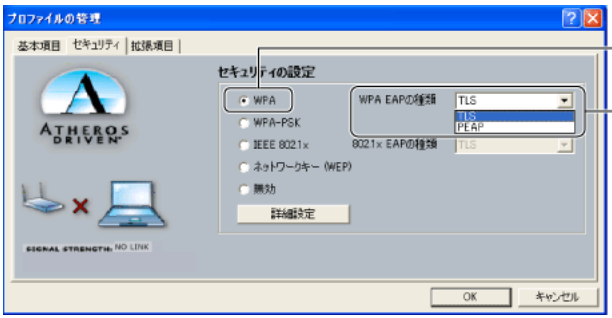
■ IEEE 802.1X の場合

1. (1)「IEEE 802.1x」をクリックして にし、(2)「802.1x EAP の種類」の をクリックして、「TLS」を選択します。



■ WPA の場合

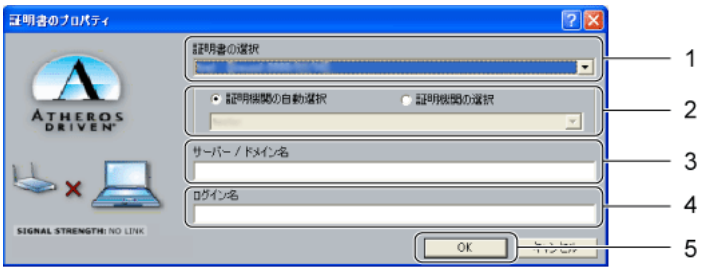
1. (1)「WPA」をクリックして にし、(2)「WPA EAP の種類」の をクリックして、「TLS」を選択します。



6 「詳細設定」をクリックします。

「証明書のプロパティ」ウィンドウが表示されます。

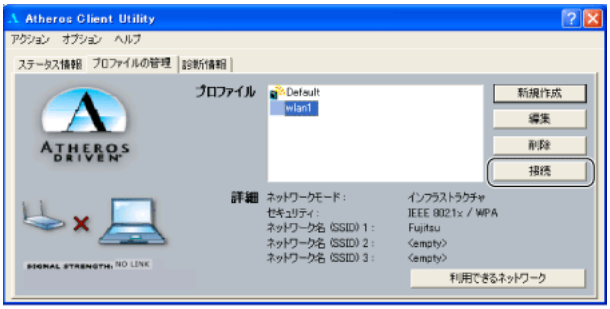
7 次の設定を行います。



1. 「証明書の選択」の▼をクリックして使用する証明書を選択します。
2. 証明機関を選択します。
   通常は、「証明機関の自動選択」をクリックして◉にします。
   証明機関を特定する必要がある場合には、「証明機関の選択」をクリックして◉にし、▼をクリックして使用する証明機関を選択します。
3. 「サーバー / ドメイン名」を入力します。
   RADIUS サーバーのフルコンピューター名を入力します。
4. 「ログイン名」を入力します。
   セキュリティグループに登録された、認証用のユーザー名を入力します。
5. 以上の設定が終わったら、「OK」をクリックします。

8 **「プロファイルの管理」ウィンドウで、「OK」をクリックします。**

9 **「Atheros Client Utility」ウィンドウの「プロファイルの管理」タブで、作成したプロファイルを選択して、「接続」をクリックします。**



IEEE 802.1X ＋ PEAP-MSCHAPv2 ／ WPA ＋ PEAP-MSCHAPv2

次のセキュリティパターンの場合の設定方法を説明します。

・IEEE 802.1X ＋ PEAP-MSCHAPv2
・WPA ＋ PEAP-MSCHAPv2

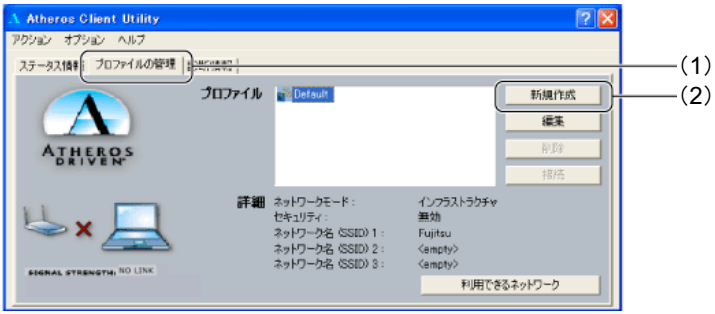
重要

・双方向認証のみサポートしています。事前にサーバー認証に使用する電子証明書をインストールする必要があります。
・複数ユーザーで運用する場合は、ユーザーごとにプロファイルを作成し、ログオン後にプロファイルを切り替えてお使いください。なお、コンピューター起動時にアクティブになるプロファイルは、シャットダウンおよび再起動前にアクティブだったプロファイルです。
・ドメイン環境での運用は未サポートです。

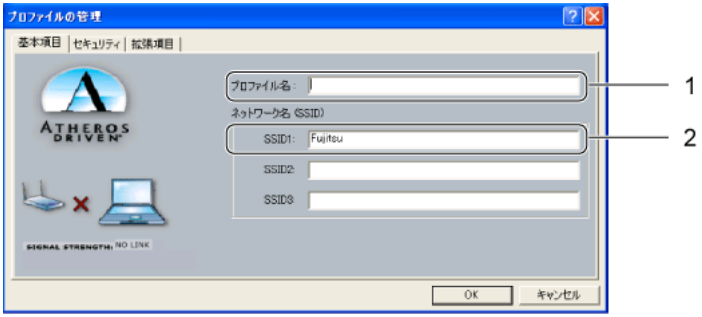
1 **デスクトップ右下の通知領域からユーティリティアイコン（ ）を右クリックし、表示されるメニューから「ユーティリティを開く」をクリックします。**

「Atheros Client Utility」ウィンドウが表示されます。

2 **(1)「プロファイルの管理」タブをクリックし、(2)「新規作成」をクリックします。**



3 **「プロファイルの管理」ウィンドウで次のように設定します。**



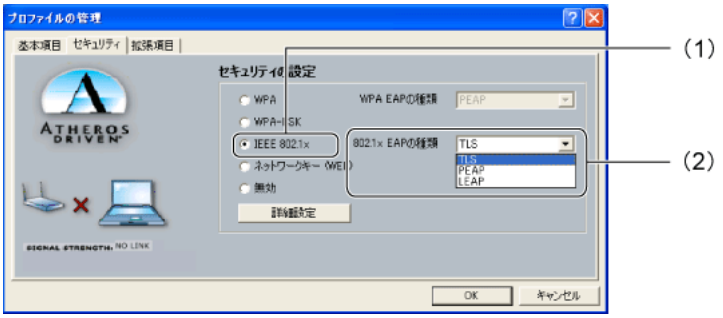
1. 「プロファイル名」を入力します。
   半角英数字、および半角記号 32 文字以内で入力します。
2. 「SSID1」を入力します。
   ネットワーク名（SSID）を接続する無線 LAN アクセスポイントに合わせて設定します。
   「SSID2」／「SSID3」は、使用できません。設定を行わないでください。

4 「セキュリティ」タブをクリックします。

5 次のように操作します。

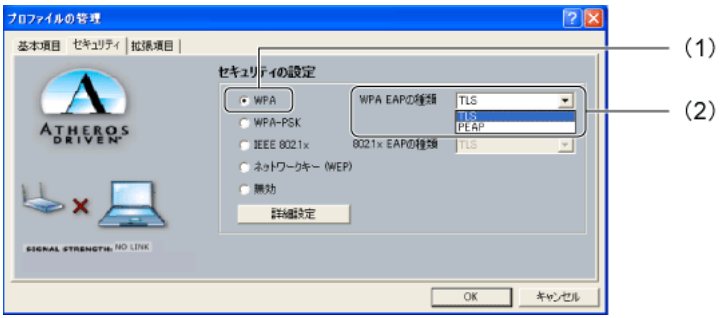
■ IEEE 802.1X の場合

1. (1)「IEEE 802.1x」をクリックして にし、(2)「802.1x EAP の種類」の をクリックして、「PEAP」を選択します。



■ WPA の場合

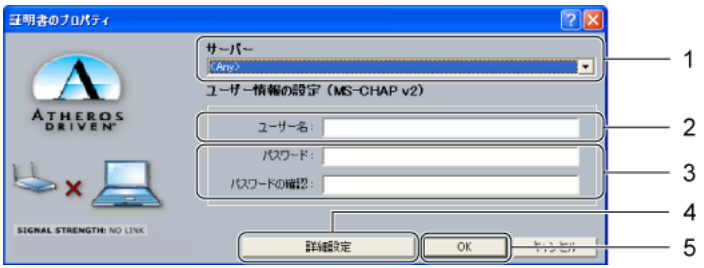
1. (1)「WPA」をクリックして にし、(2)「WPA EAP の種類」の をクリックして、「PEAP」を選択します。



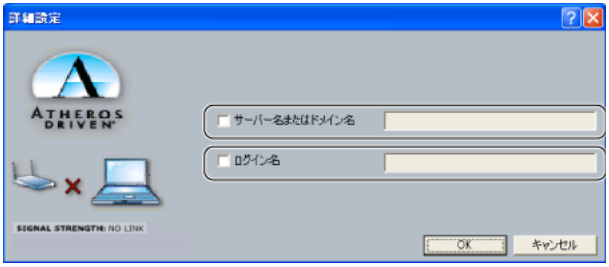
6 「詳細設定」をクリックします。

「証明書のプロパティ」ウィンドウが表示されます。

7 次の設定を行います。



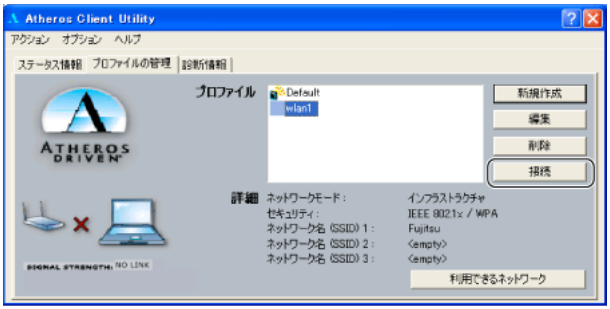
1. 「サーバー」の▼をクリックして、インストールした RADIUS サーバーの証明書の証明機関を選択します。
2. 「ユーザー名」に、認証に使用するフルユーザー名を入力します。（例：TLSuser@wireless.local.com）
   UPN サフィックスをつけて設定してください。
3. 「パスワード」と「パスワードの確認」に、認証に使用するユーザーのパスワードを設定します。
4. 「詳細設定」をクリックし、証明書の詳細設定をします。
   「詳細設定」ウィンドウで設定を行います。



   - 「サーバー名またはドメイン名」を設定します。
     RADIUS サーバーのフルコンピューター名を設定します。
   - 「ログイン名」を設定します。
     認証に使用するフルユーザー名を設定します。「証明書のプロパティ」画面で設定した内容と同じものです。
     設定したら、「OK」をクリックします。
5. 設定が終わったら、「OK」をクリックします。

8 「プロファイルの管理」ウィンドウで、「OK」をクリックします。

9 「Atheros Client Utility」ウィンドウの「プロファイルの管理」タブで、作成したプロファイルを選択して、「接続」をクリックします。



WPA-PSK

WPA-PSK の場合の設定方法を説明します。

重要

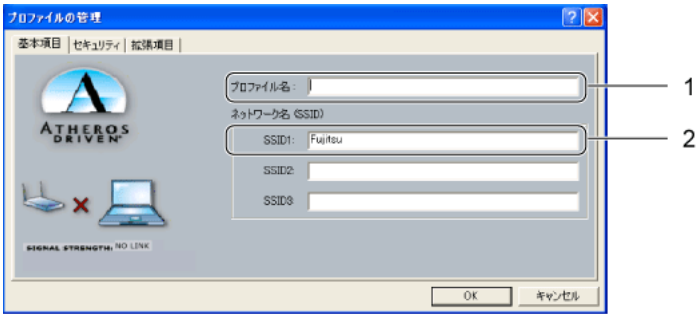
・無線 LAN ネットワークへの接続は、ユーザーがログオンした後、Atheros Client Utility が起動してから開始されます。ログオフ時は無線 LAN ネットワークに接続されません。

1 **デスクトップ右下の通知領域からユーティリティアイコン（ ）を右クリックし、表示されるメニューから「ユーティリティを開く」をクリックします。**

「Atheros Client Utility」ウィンドウが表示されます。

2 **(1)「プロファイルの管理」タブをクリックし、(2)「新規作成」をクリックします。**

3 **「プロファイルの管理」ウィンドウで次のように設定します。**

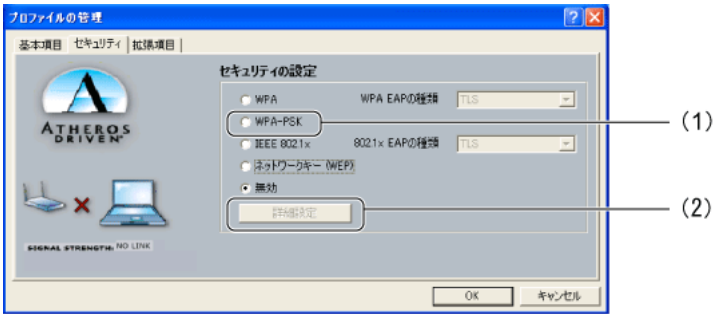


1. 「プロファイル名」を入力します。
   半角英数字、および半角記号 32 文字以内で入力します。

2.「SSID1」を入力します。
ネットワーク名（SSID）を接続する無線 LAN アクセスポイントに合わせて設定します。
「SSID2」／「SSID3」は、使用できません。設定を行わないでください。

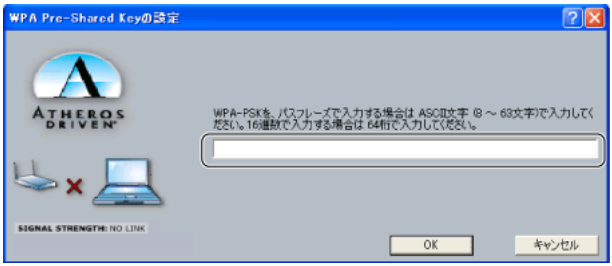
4 「セキュリティ」タブをクリックします。

5 (1)「WPA-PSK」をクリックして◉にし、(2)「詳細設定」をクリックします。



「WPA Pre-Shared Key の設定」ウィンドウが表示されます。

6 PSK を設定し、「OK」をクリックします。
無線 LAN アクセスポイントと同じ値を設定してください。8 文字以上 63 文字以下は ASCII 文字、64 文字は 16 進数での入力になります。

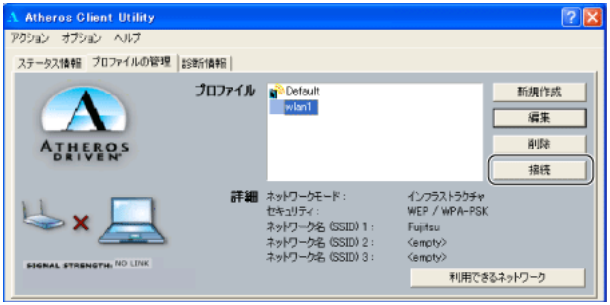


POINT

・16 進数を使用する場合、A ～ F の入力には大文字を使用してください。

7 「プロファイルの管理」ウィンドウで、「OK」をクリックします。

8 「Atheros Client Utility」ウィンドウの「プロファイルの管理」タブで、作成したプロファイルを選択して、「接続」をクリックします。



5 Intel 無線 LAN 搭載モデル v11.x 系／ v10.5.x 系の設定

クライアントのパソコンが、Intel 無線 LAN 搭載モデル v11.x 系／ v10.5.x 系の場合の設定方法を説明します。

重要

シングルサインオン／ドメインログオンを使用する場合

プログラムの追加が必要です。追加方法については、「シングルサインオン／ドメインログオンを使用する場合のプログラムの追加」（→ P.94）をご覧ください。

シングルサインオン／ドメインログオンを使用する場合のプログラムの追加

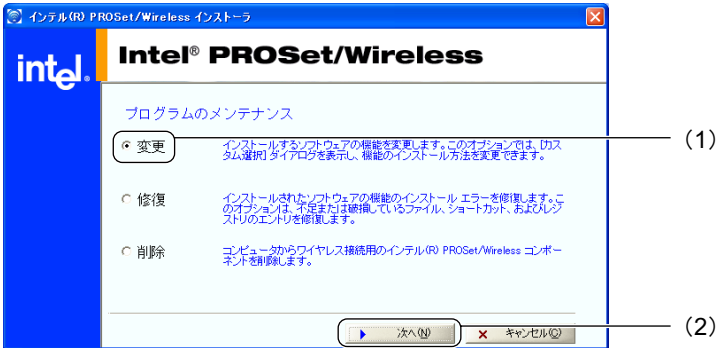
シングルサインオンやドメインログオンを使用する場合は、次の手順に従って、プログラムを追加してください。

1. **「スタート」ボタン→「コントロールパネル」または、「スタート」ボタン→「設定」→「コントロールパネル」の順にクリックします。**
   「コントロールパネル」ウィンドウが表示されます。

2. **Windows XP の場合は「プログラムの追加と削除」、Windows 2000 の場合は「アプリケーションの追加と削除」をクリックします。**

3. **「現在インストールされているプログラム」の一覧から、「インテル (R) PROSet/Wireless ソフトウェア」を選択し、「変更と削除」をクリックします。**
   「インテル (R) PROSet/Wireless インストーラ」ウィンドウが表示されます。

4 **(1)「変更」を◉にして、(2)「次へ」をクリックします。**



5 **「シングルサインオン」の✕▾をクリックし、表示されるメニューから「この機能と、すべてのサブ機能をインストールする」を選択します。**

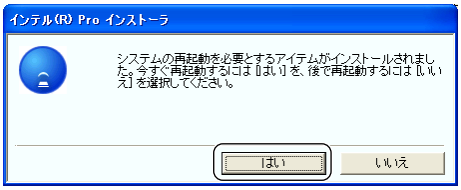
6 **「管理者ツールキット」(または「管理者ツール」)の✕▾をクリックし、表示されるメニューから「この機能と、すべてのサブ機能をインストールする」を選択します。**

7 **「編集」をクリックします。**
追加するプログラムがインストールされます。

8 **「インテル (R) PROSet/Wireless インストーラ」ウィンドウで「コンポーネントの変更を完了しました。」と表示されたら、次のように操作します。**

1. 「シングルサインオン」、「ログオン前接続」、「管理者ツールキット」（または「管理者ツール」）に ✔ がついていることを確認します。
2. 「OK」をクリックします。

9 **システムの再起動について確認のメッセージが表示されたら、「はい」をクリックして、パソコンを再起動します。**



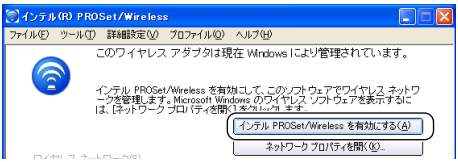
IEEE 802.1X ＋ EAP-TLS ／ WPA ＋ EAP-TLS ／ WPA2 ＋ EAP-TLS

次のセキュリティパターンの場合の設定方法を説明します。
- IEEE 802.1X ＋ EAP-TLS
- WPA ＋ EAP-TLS（WPA エンタープライズ EAP-TLS）
- WPA2 ＋ EAP-TLS（WPA2 エンタープライズ EAP-TLS）

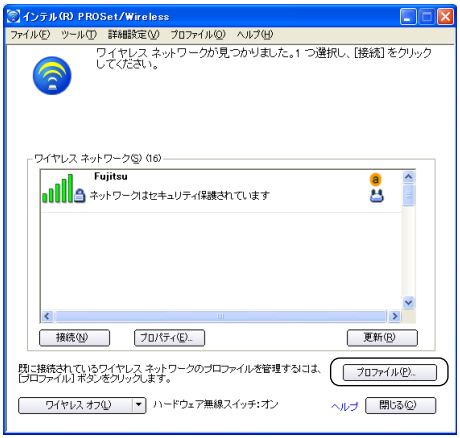
1 **「スタート」ボタン→「すべてのプログラム」→「Intel PROSet Wireless」→「Intel PROSet Wireless」の順にクリックします。**
「インテル (R) PROSet/Wireless」ウィンドウが表示されます。

POINT

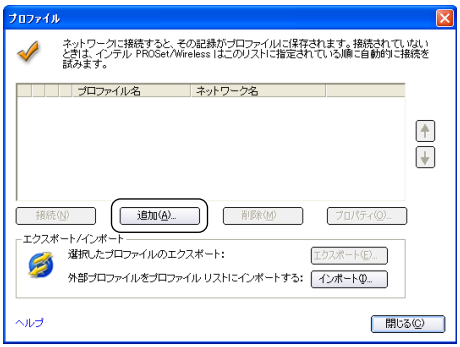
・Windows XP 標準の無線 LAN 機能が有効になっている場合は、「インテル PROSet/Wireless を有効にする」をクリックしてください。



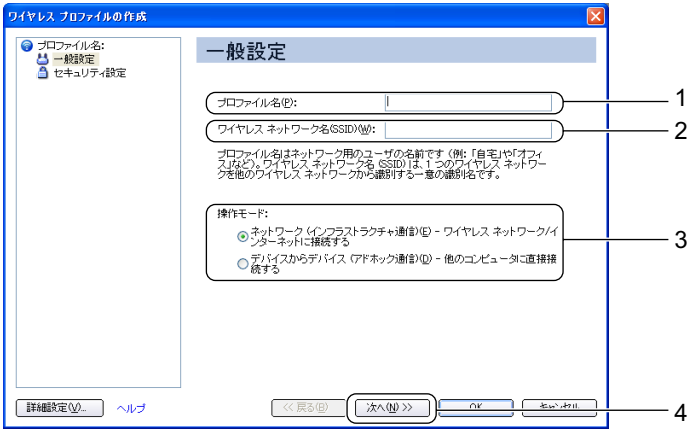
2 「プロファイル」をクリックします。



3 「追加」をクリックします。



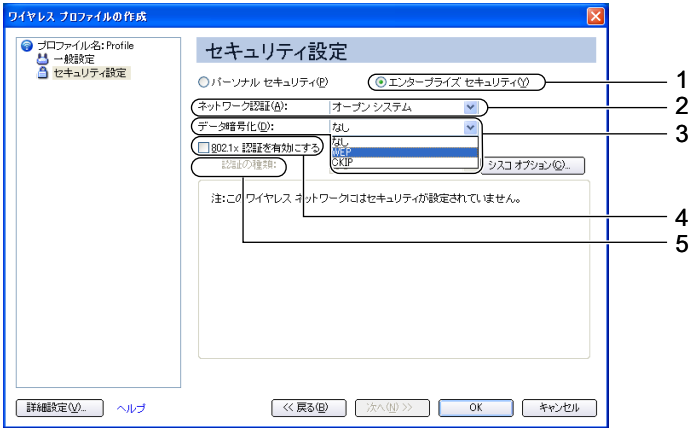
4 無線 LAN のネットワークへ接続するための情報を設定します。



1. 「プロファイル名」を入力します。
   設定するパラメータ情報を保存するシステムファイルの名前を入力します。プロファイル名は半角英数字および、日本語（全角文字）を 32 文字以内で入力できます。
2. 「ワイヤレスネットワーク名（SSID)」を入力します。
   お使いになる環境に合わせてネットワーク名を入力します。ネットワーク名は、半角英数字 32 文字以内で入力してください。
3. 「操作モード」の「ネットワーク（インフラストラクチャ通信）- ワイヤレスネットワーク / インターネットに接続する」をクリックして◉にします。
4. 「次へ」をクリックします。

5 セキュリティを設定します。

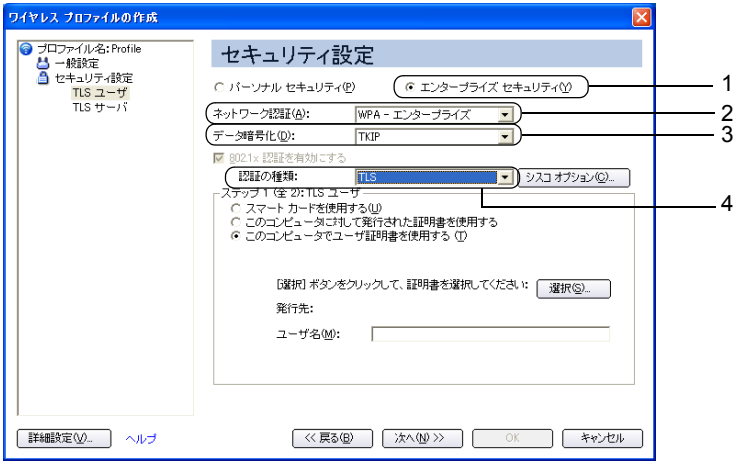
■ IEEE 802.1X の場合



1. 「エンタープライズ セキュリティ」の◯をクリックして◉にします。
2. 「ネットワーク認証」の ⌄ をクリックし、「オープン システム」を選択します。

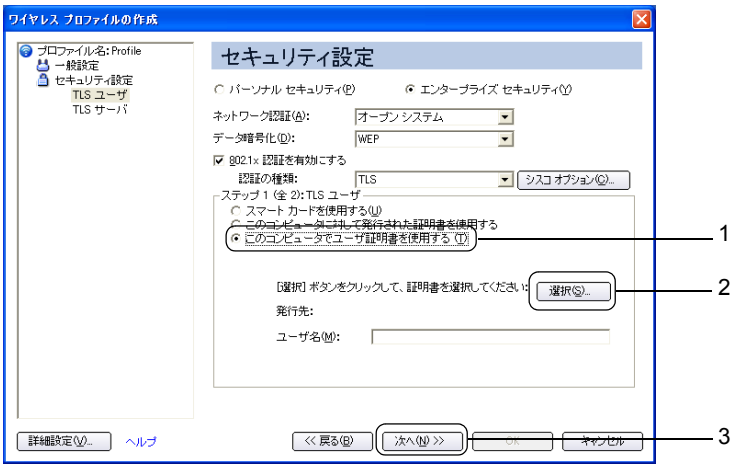
3. 「データ暗号化」の をクリックし、「WEP」を選択します。
4. 「802.1x 認証を有効にする」の をクリックして にします。
5. 「認証の種類」の をクリックして、「TLS」を選択します。

■ WPA ／ WPA2 の場合



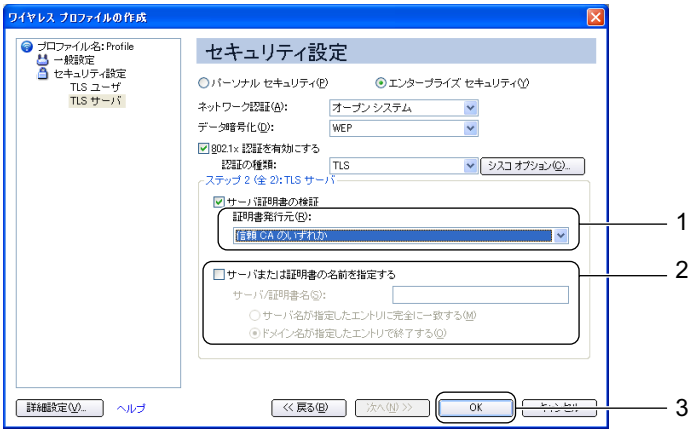
1. 「エンタープライズ セキュリティ」の をクリックして にします。
2. 「ネットワーク認証」の をクリックし、「WPA - エンタープライズ」または「WPA2 - エンタープライズ」を選択します。
   お使いになる環境、無線 LAN アクセスポイントに合わせて設定してください。
3. 「データ暗号化」の をクリックし、「TKIP」または、「AES - CCMP」を選択します。
   お使いになる環境、無線 LAN アクセスポイントに合わせて設定してください。
4. 「認証の種類」の をクリックして、「TLS」を選択します。

6 認証の設定（ステップ 1）をします。



1.「このコンピュータでユーザ証明書を使用する」をクリックして◉にします。
2.「選択」をクリックし、使用する証明書を選択します。
3.「次へ」をクリックします。

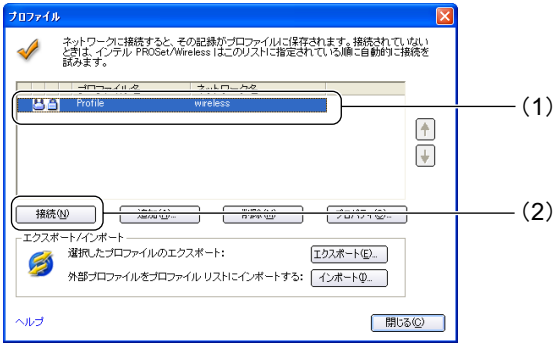
7 認証の設定（ステップ 2）をします。



1.「証明書発行元」の⌄をクリックして、使用する証明書の発行元を選択するか、「信頼 CA のいずれか」を選択します。
2. サーバー／証明書を指定する場合は、「サーバまたは証明書の名前を指定する」の☐をクリックして☑にし、RADIUS サーバーに合わせて次のように設定します。
   サーバー名が、証明書のサーバー名と完全に一致する場合、「サーバ名が指定したエントリに完全に一致する」を◉にし、「サーバ／証明書名」にサーバー名を入力します。
   証明書にこのドメインまたは、このドメインのサブドメインに属するサーバー名が指定されている場合は、「ドメイン名が指定したエントリで終了」を◉にし、「サーバ／証明書名」にドメイン名を入力します。
3. 設定が終了したら、「OK」をクリックします。

「プロファイルウィザード」が終了し、「プロファイル」に作成したプロファイルが追加されます。

8 **(1)「プロファイル」のリストから作成したプロファイルを選択し、(2)「接続」をクリックします。**



IEEE 802.1X ＋ PEAP-MSCHAPv2 ／ WPA ＋ PEAP-MSCHAPv2 ／ WPA2 ＋ PEAP-MSCHAPv2

次のセキュリティパターンの場合の設定方法を説明します。

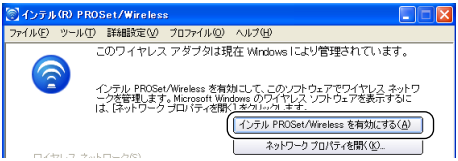
- IEEE 802.1X ＋ PEAP-MSCHAPv2
- WPA ＋ PEAP-MSCHAPv2（WPA エンタープライズ PEAP-MSCHAP-V2）
- WPA2 ＋ PEAP-MSCHAPv2（WPA2 エンタープライズ PEAP-MSCHAP-V2）

1 **「スタート」ボタン→「すべてのプログラム」→「Intel PROSet Wireless」→「Intel PROSet Wireless」の順にクリックします。**

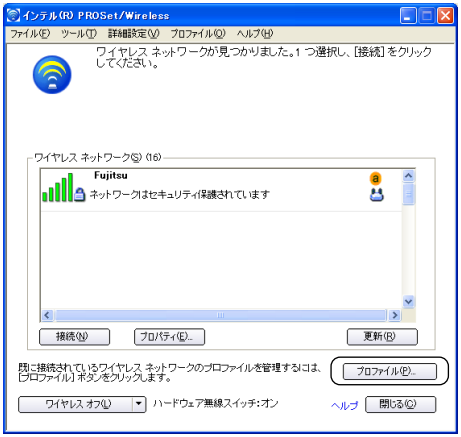
「インテル (R) PROSet/Wireless」ウィンドウが表示されます。

POINT

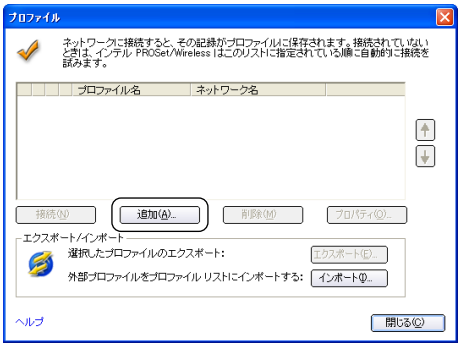
- Windows XP 標準の無線 LAN 機能が有効になっている場合は、「インテル PROSet/Wireless を有効にする」をクリックしてください。



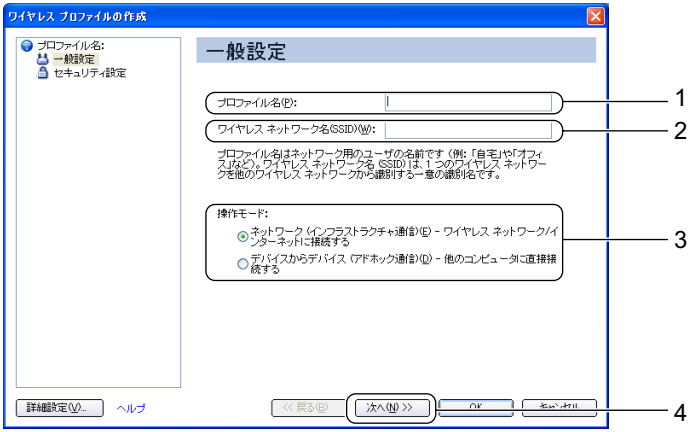
2 「プロファイル」をクリックします。



3 「追加」をクリックします。



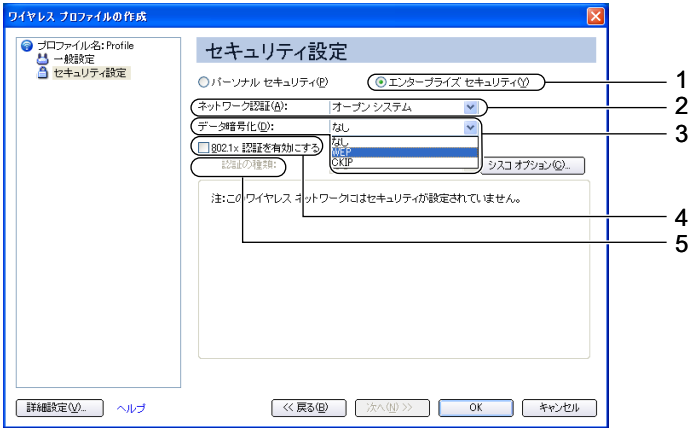
4 無線 LAN のネットワークへ接続するための情報を設定します。



1. 「プロファイル名」を入力します。
   設定するパラメータ情報を保存するシステムファイルの名前を入力します。プロファイル名は半角英数字および、日本語（全角文字）を 32 文字以内で入力できます。
2. 「ワイヤレスネットワーク名（SSID)」を入力します。
   お使いになる環境に合わせてネットワーク名を入力します。ネットワーク名は、半角英数字 32 文字以内で入力してください。
3. 「操作モード」の「ネットワーク（インフラストラクチャ通信）- ワイヤレスネットワーク / インターネットに接続する」をクリックして◉にします。
4. 「次へ」をクリックします。

5 セキュリティを設定します。

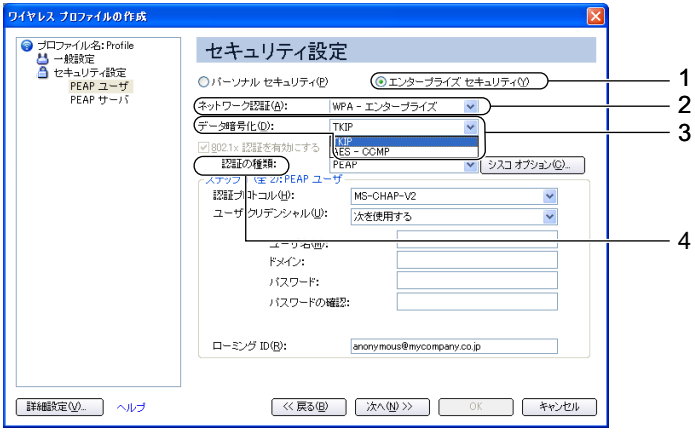
■ IEEE 802.1X の場合



1. 「エンタープライズ セキュリティ」の○をクリックして◉にします。
2. 「ネットワーク認証」の ▼ をクリックし、「オープン システム」を選択します。

3.「データ暗号化」の をクリックし、「WEP」を選択します。
4.「802.1x 認証を有効にする」の をクリックして にします。
5.「認証の種類」の をクリックして、「PEAP」を選択します。

■ WPA ／ WPA2 の場合



1.「エンタープライズ セキュリティ」の をクリックして にします。
2.「ネットワーク認証」の をクリックし、「WPA - エンタープライズ」または「WPA2 - エンタープライズ」を選択します。
お使いになる環境、無線 LAN アクセスポイントに合わせて設定してください。
3.「データ暗号化」の をクリックし、「TKIP」または、「AES - CCMP」を選択します。
お使いになる環境、無線 LAN アクセスポイントに合わせて設定してください。
4.「認証の種類」の をクリックして、「PEAP」を選択します。

6 認証の設定（ステップ 1）を行います。

1.「認証プロトコル」の をクリックして、「MS-CHAP-V2」を選択します。
2.「ユーザクリデンシャル」を選択します。

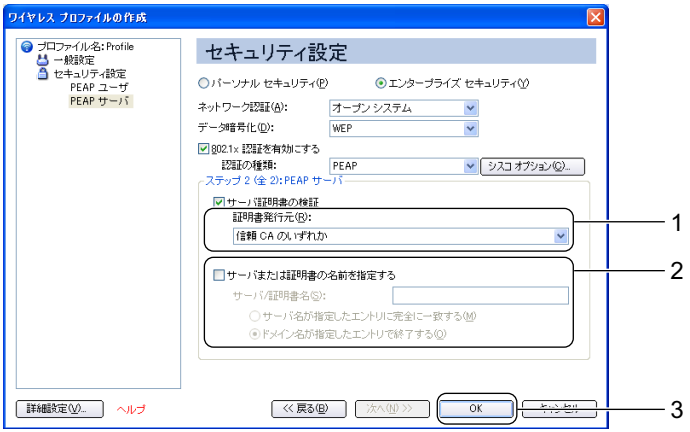
・接続のたびに認証情報を入力する場合は、をクリックして「接続するたびにプロンプトを表示する」を選択します。
・シングルサインオンを使用する場合は、をクリックして「Windows ログオンを使用する」を選択します。
シングルサインオンを使用する場合は、プログラムを追加する必要があります。
プログラムの追加方法については、「シングルサインオン／ドメインログオンを使用する場合のプログラムの追加」（→ P.140）をご覧ください。
・認証情報を保存する場合は、をクリックして「次を使用する」を選択し、次のように入力します。

表：「次を使用する」を選択した場合の設定

項目	説明
ユーザ名	認証に使用するユーザー名を入力します。
ドメイン	ドメインに参加しているネットワークに接続する場合は、RADIUS サーバーのドメイン名を入力します。
パスワード	認証に使用するユーザーのパスワードを入力します。
パスワードの確認	確認のため、「パスワード」と同じ値を入力します。

3. 「ローミング ID」に、認証に使用するユーザー名を入力します。
4. 「次へ」をクリックします。

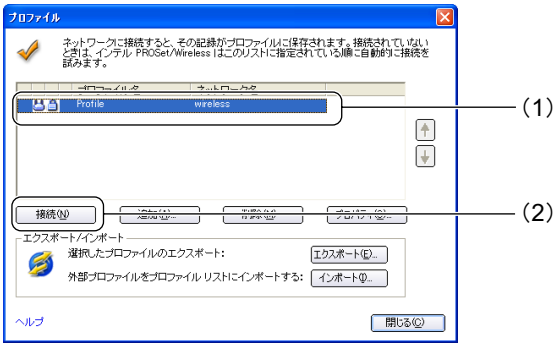
7 認証の設定（ステップ 2）をします。



1. 「証明書発行元」の をクリックして、使用する証明書の発行元を選択するか、「信頼 CA のいずれか」を選択します。
2. サーバー／証明書を指定する場合は、「サーバまたは証明書の名前を指定する」の をクリックして にし、RADIUS サーバーに合わせて次のように設定します。
   サーバー名が、証明書のサーバー名と完全に一致する場合、「サーバ名が指定したエントリに完全に一致する」を にし、「サーバ／証明書名」にサーバー名を入力します。
   証明書にこのドメインまたは、このドメインのサブドメインに属するサーバー名が指定されている場合は、「ドメイン名が指定したエントリで終了」を にし、「サーバ／証明書名」にドメイン名を入力します。
3. 設定が終了したら、「OK」をクリックします。

「プロファイルウィザード」が終了し、「プロファイル」に作成したプロファイルが追加されます。

8 (1)「プロファイル」のリストから作成したプロファイルを選択し、(2)「接続」をクリックします。



IEEE 802.1X ＋ PEAP-TLS ／ WPA ＋ PEAP-TLS ／ WPA2 ＋ PEAP-TLS

次のセキュリティパターンの場合の設定方法を説明します。

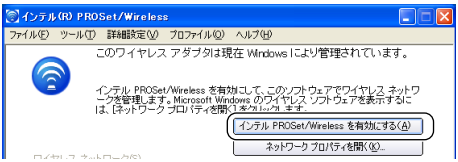
- IEEE 802.1X ＋ PEAP-TLS
- WPA ＋ PEAP-TLS（WPA エンタープライズ PEAP-TLS）
- WPA2 ＋ PEAP-TLS（WPA2 エンタープライズ PEAP-TLS）

1 「スタート」ボタン→「すべてのプログラム」→「Intel PROSet Wireless」→「Intel PROSet Wireless」の順にクリックします。

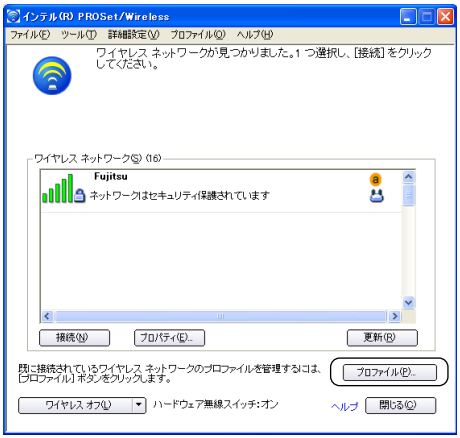
「インテル (R) PROSet/Wireless」ウィンドウが表示されます。

POINT

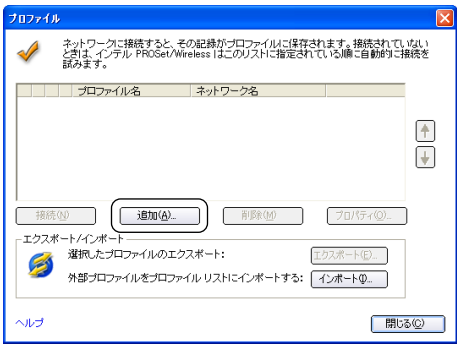
・Windows XP 標準の無線 LAN 機能が有効になっている場合は、「インテル PROSet/Wireless を有効にする」をクリックしてください。



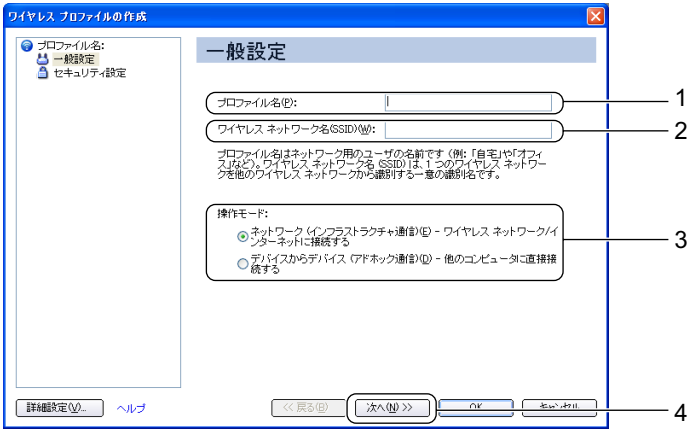
2 「プロファイル」をクリックします。



3 「追加」をクリックします。



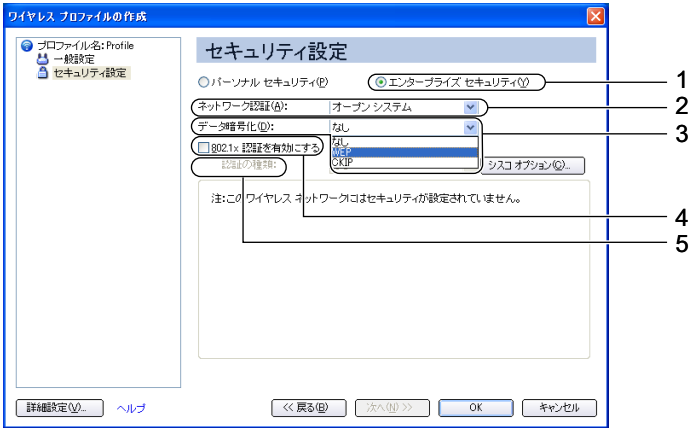
4 無線 LAN のネットワークへ接続するための情報を設定します。



1. 「プロファイル名」を入力します。
   設定するパラメータ情報を保存するシステムファイルの名前を入力します。プロファイル名は半角英数字および、日本語（全角文字）を 32 文字以内で入力できます。
2. 「ワイヤレスネットワーク名（SSID)」を入力します。
   お使いになる環境に合わせてネットワーク名を入力します。ネットワーク名は、半角英数字 32 文字以内で入力してください。
3. 「操作モード」の「ネットワーク（インフラストラクチャ通信）- ワイヤレスネットワーク / インターネットに接続する」をクリックして◉にします。
4. 「次へ」をクリックします。

5 セキュリティを設定します。

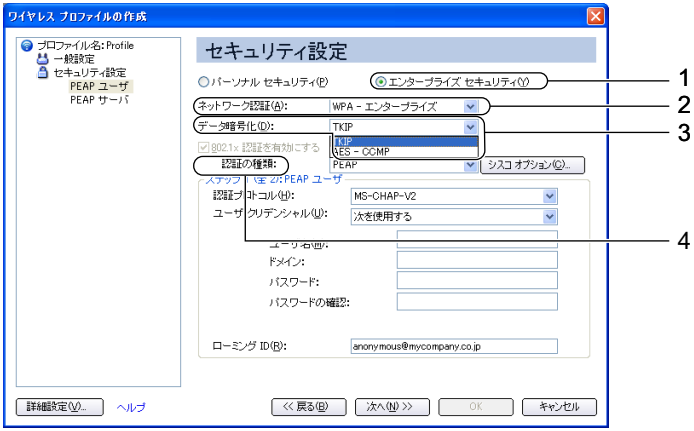
■ IEEE 802.1X の場合



1. 「エンタープライズ セキュリティ」の○をクリックして◉にします。
2. 「ネットワーク認証」の ▼ をクリックし、「オープン システム」を選択します。

3.「データ暗号化」の をクリックし、「WEP」を選択します。
4.「802.1x 認証を有効にする」の をクリックして にします。
5.「認証の種類」の をクリックして、「PEAP」を選択します。

■ WPA ／ WPA2 の場合

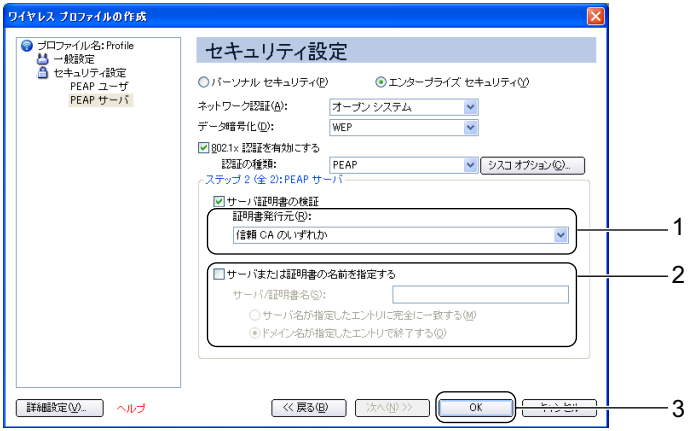


1.「エンタープライズ セキュリティ」の をクリックして にします。
2.「ネットワーク認証」の をクリックし、「WPA - エンタープライズ」または「WPA2 - エンタープライズ」を選択します。
お使いになる環境、無線 LAN アクセスポイントに合わせて設定してください。
3.「データ暗号化」の をクリックし、「TKIP」または、「AES - CCMP」を選択します。
お使いになる環境、無線 LAN アクセスポイントに合わせて設定してください。
4.「認証の種類」の をクリックして、「PEAP」を選択します。

6 認証の設定（ステップ 1）を行います。

1. 「認証プロトコル」の をクリックして、「TLS」を選択します。
2. 「このコンピュータ上のユーザ証明書を使用する」をクリックして にします。
3. 「選択」をクリックし、使用する証明書を選択します。
4. 「ローミング ID」に、認証に使用するユーザー名を入力します。
5. 「次へ」をクリックします。

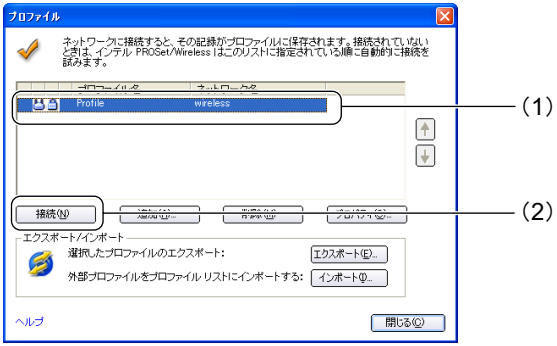
7 認証の設定（ステップ 2）をします。



1. 「証明書発行元」の をクリックして、使用する証明書の発行元を選択するか、「信頼 CA のいずれか」を選択します。
2. サーバー／証明書を指定する場合は、「サーバまたは証明書の名前を指定する」の をクリックして にし、RADIUS サーバーに合わせて次のように設定します。
   サーバー名が、証明書のサーバー名と完全に一致する場合、「サーバ名が指定したエントリに完全に一致する」を にし、「サーバ／証明書名」にサーバー名を入力します。
   証明書にこのドメインまたは、このドメインのサブドメインに属するサーバー名が指定されている場合は、「ドメイン名が指定したエントリで終了」を にし、「サーバ／証明書名」にドメイン名を入力します。
3. 設定が終了したら、「OK」をクリックします。

「プロファイルウィザード」が終了し、「プロファイル」に作成したプロファイルが追加されます。

8 **(1)「プロファイル」のリストから作成したプロファイルを選択し、(2)「接続」をクリックします。**



WPA-PSK ／ WPA2-PSK

次のセキュリティパターンの場合の設定方法を説明します。

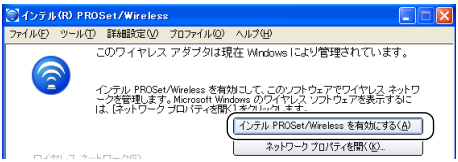
・WPA-PSK（WPA パーソナル）
・WPA2-PSK（WPA2 パーソナル）

1 **「スタート」ボタン→「すべてのプログラム」→「Intel PROSet Wireless」→「Intel PROSet Wireless」の順にクリックします。**

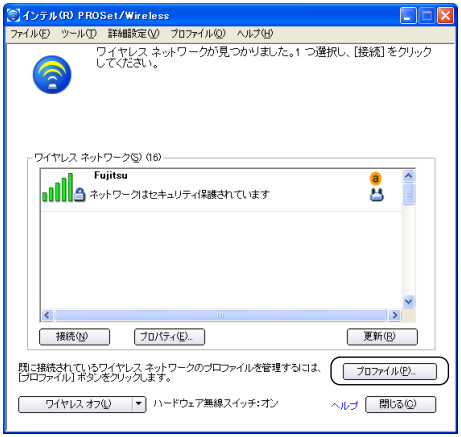
「インテル (R) PROSet/Wireless」ウィンドウが表示されます。

POINT

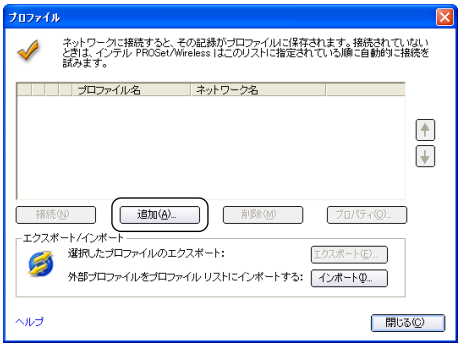
・Windows XP 標準の無線 LAN 機能が有効になっている場合は、「インテル PROSet/Wireless を有効にする」をクリックしてください。



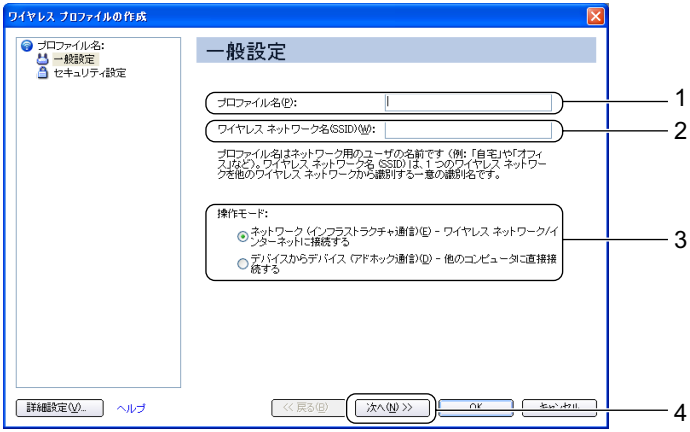
2 「プロファイル」をクリックします。



3 「追加」をクリックします。

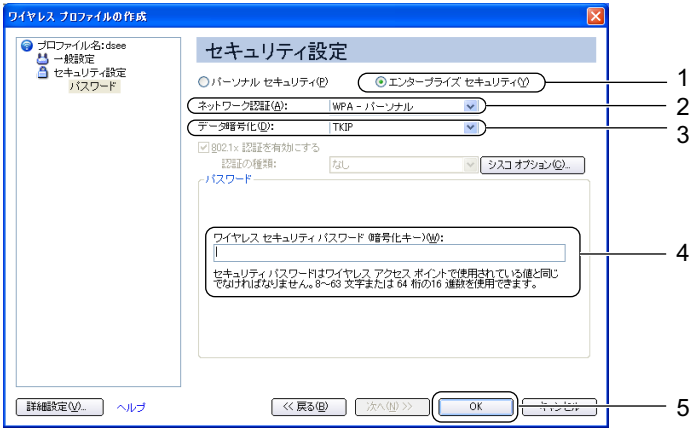


4 無線 LAN のネットワークへ接続するための情報を設定します。



1. 「プロファイル名」を入力します。
   設定するパラメータ情報を保存するシステムファイルの名前を入力します。プロファイル名は半角英数字および、日本語（全角文字）を 32 文字以内で入力できます。
2. 「ワイヤレスネットワーク名（SSID)」を入力します。
   お使いになる環境に合わせてネットワーク名を入力します。ネットワーク名は、半角英数字 32 文字以内で入力してください。
3. 「操作モード」の「ネットワーク（インフラストラクチャ通信）- ワイヤレスネットワーク / インターネットに接続する」をクリックして◉にします。
4. 「次へ」をクリックします。

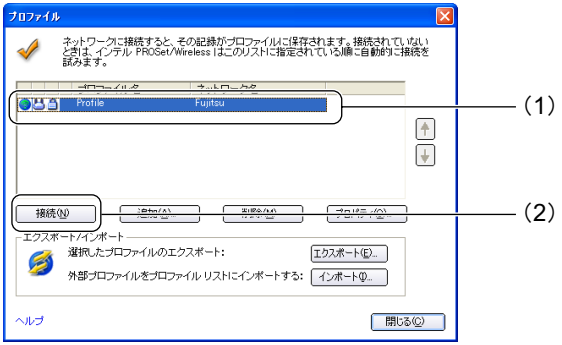
5 セキュリティを設定します。



1. 「エンタープライズセキュリティ」を選択します。
2. 「ネットワーク認証」の をクリックし、「WPA - パーソナル」または「WPA2 - パーソナル」を選択します。
   お使いになる環境、無線 LAN アクセスポイントに合わせて設定してください。
3. 「データ暗号化」を選択します。
   お使いになる環境、無線 LAN アクセスポイントの設定に合わせて設定してください。
4. お使いになる接続方法に合わせて「ワイヤレスセキュリティパスワード（暗号化キー）」を入力します。
   パスフレーズまたは 16 進数で入力します。無線 LAN アクセスポイントの設定に合わせて設定してください。
5. 設定が終了したら、「OK」をクリックします。

「プロファイルウィザード」が終了し、「プロファイル」に作成したプロファイルが追加されます。

6 (1)「プロファイル」のリストから作成したプロファイルを選択し、(2)「接続」をクリックします。



ドメインログオン使用：IEEE 802.1X ＋ EAP-TLS ／ WPA ＋ EAP-TLS ／ WPA2 ＋ EAP-TLS

次のセキュリティパターンでドメインログオンをお使いになる場合の設定方法を説明します。

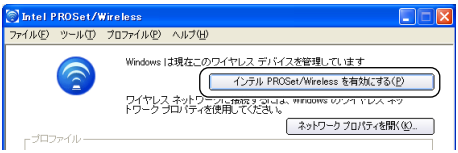
- IEEE 802.1X ＋ EAP-TLS
- WPA ＋ EAP-TLS
- WPA2 ＋ EAP-TLS

1 「スタート」ボタン→「すべてのプログラム」→「Intel PROSet Wireless」→「Intel PROSet Wireless」の順にクリックします。

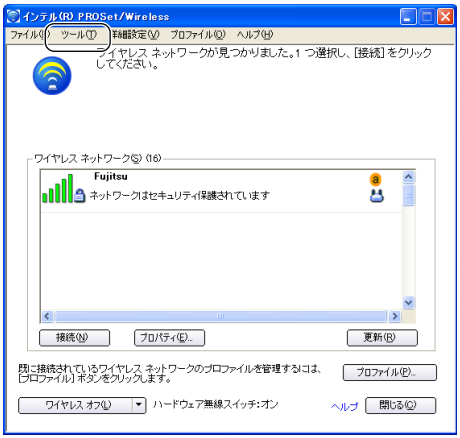
「インテル (R) PROSet ／ Wireless」ウィンドウが表示されます。

POINT

・Windows XP 標準の無線 LAN 機能が有効になっている場合は、「インテル PROSet/Wireless を有効にする」をクリックしてください。



2 「ツール」メニュー→「管理ツール」の順にクリックします。



「パスワードの作成」ウィンドウが表示されます。

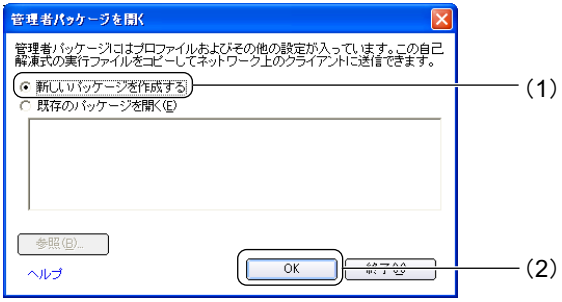
POINT

・ドメインログオンをする場合は、「管理ツール」で設定する必要があります。

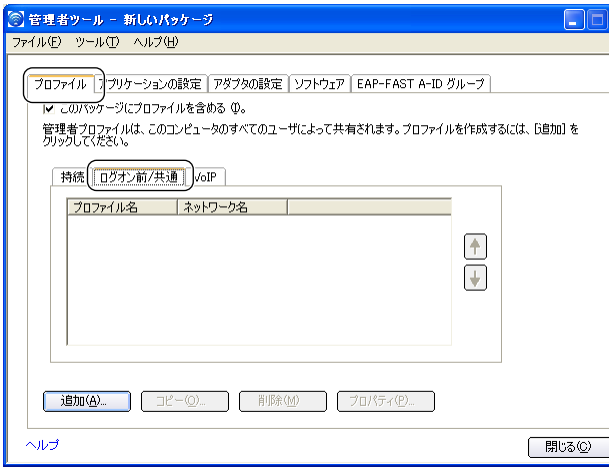
3 プロファイルを保護するためのパスワードを設定し、「OK」をクリックします。

「管理者パッケージを開く」ウィンドウが表示されます。

4 **(1)「新しいパッケージを作成する」をクリックして◉にし、(2)「OK」をクリックします。**



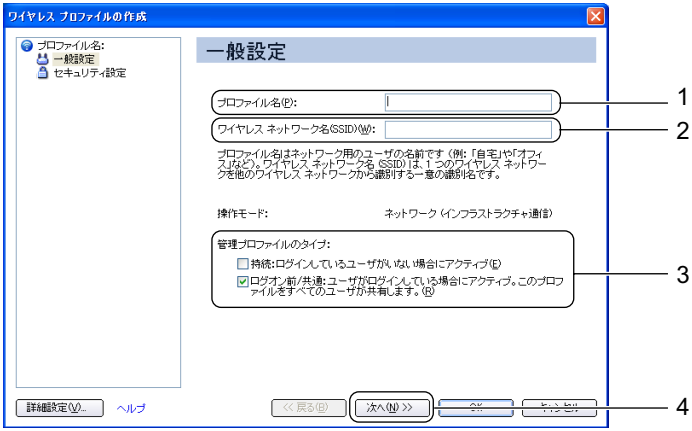
5 **「プロファイル」タブの「ログオン前 / 共通」タブをクリックします。**



6 **「追加」をクリックします。**

「ワイヤレスプロファイルの作成」ウィザードが表示されます。

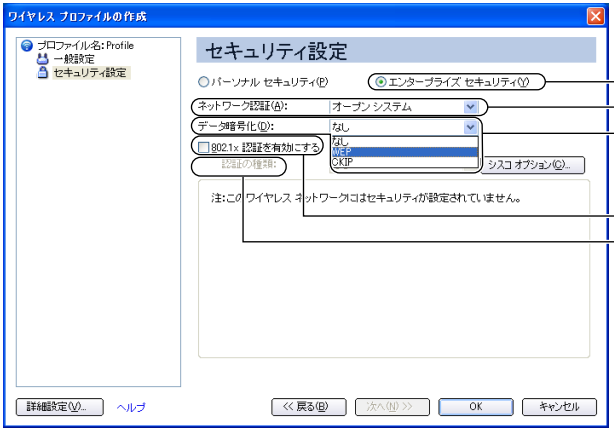
7 無線 LAN のネットワークへ接続するための情報を設定します。次のように設定します。



1. 「プロファイル名」を入力します。
   設定するパラメータ情報を保存するプロファイルの名前を入力します。半角英数字、および日本語（全角文字）32 文字以内で入力できます。
2. 「ワイヤレスネットワーク名（SSID)」を入力します。
   お使いになる環境に合わせてネットワーク名を入力します。ネットワーク名は、半角英数字 32 文字以内で入力してください。
3. 「管理プロファイルのタイプ」を設定します。
   - 持続
     「持続」を☑にすると、起動時およびコンピューターにログオンしているユーザーがいない場合でも、プロファイルが有効になります。
   - ログオン前 / 共通
     「ログオン前 / 共通」を☑にすると、ユーザーがコンピューターにログオンすると同時に接続が行われます。
4. 設定が終わったら「次へ」をクリックします。

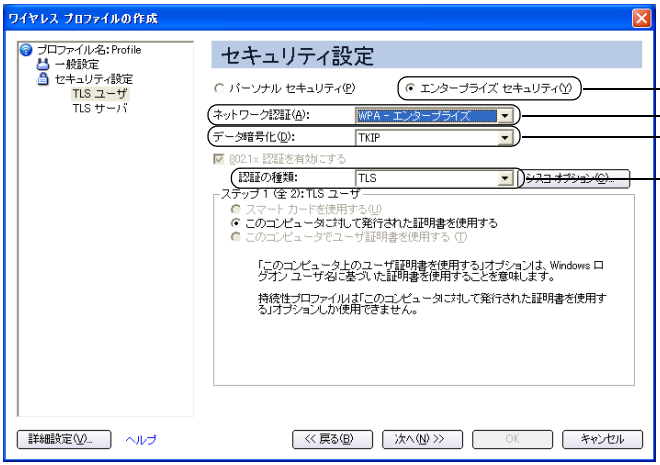
8 セキュリティを設定します。

■ IEEE 802.1X の場合



1. 「エンタープライズ セキュリティ」の◯をクリックして◉にします。
2. 「ネットワーク認証」の ⌄ をクリックし、「オープン システム」を選択します。
3. 「データ暗号化」の ⌄ をクリックし、「WEP」を選択します。
4. 「802.1x 認証を有効にする」の☐ をクリックして☑ にします。
5. 「認証の種類」の ⌄ をクリックして、「TLS」を選択します。

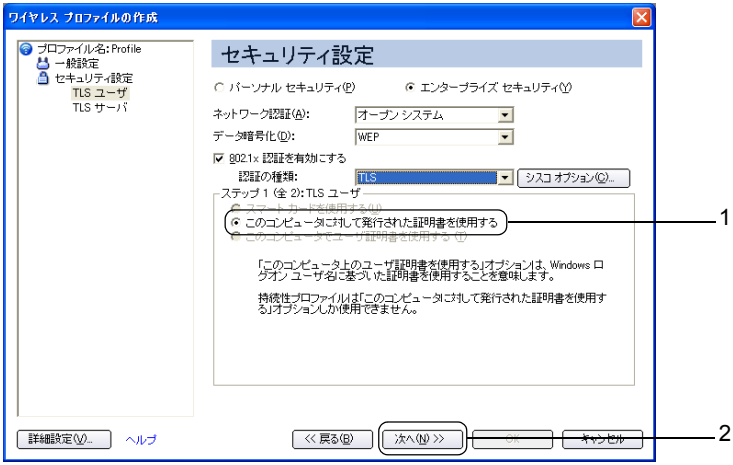
■ WPA ／ WPA2 の場合



1. 「エンタープライズ セキュリティ」の◯をクリックして◉にします。
2. 「ネットワーク認証」の ⌄ をクリックし、「WPA - エンタープライズ」または「WPA2 - エンタープライズ」を選択します。
   お使いになる環境、無線 LAN アクセスポイントに合わせて設定してください。
3. 「データ暗号化」の ⌄ をクリックし、「TKIP」または、「AES - CCMP」を選択します。
   お使いになる環境、無線 LAN アクセスポイントに合わせて設定してください。

4.「認証の種類」の をクリックして、「TLS」を選択します。

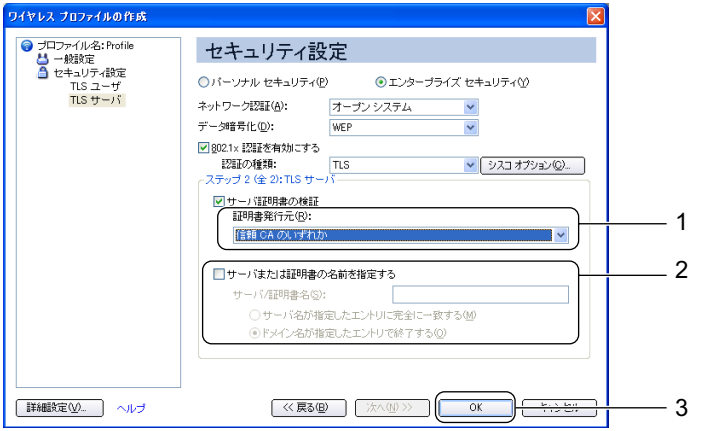
9 認証の設定（ステップ 1）をします。



1.「このコンピュータに対して発行された証明書を使用する」をクリックして にします。

2.「次へ」をクリックします。

10 認証の設定（ステップ 2）をします。



1. 必要に応じて、「証明書発行元」の をクリックして使用する証明書の発行元を選択するか、「信頼 CA のいずれか」を選択します。
2. サーバー／証明書を指定する場合は、「サーバまたは証明書の名前を指定する」の をクリックして にし、RADIUS サーバーに合わせて次のように設定します。
   サーバー名が、証明書のサーバー名と完全に一致する場合、「サーバ名が指定したエントリに完全に一致する」を にし、「サーバ／証明書名」にサーバー名を入力します。
   証明書にこのドメインまたは、このドメインのサブドメインに属するサーバー名が指定されている場合は、「ドメイン名が指定したエントリで終了」を にし、「サーバ／証明書名」にドメイン名を入力します。
3. 設定が終了したら、「OK」をクリックします。

「プロファイルウィザード」が終了し、「プロファイル」に作成したプロファイルが追加されます。

11 「ファイル」メニュー→「パッケージを保存する」の順にクリックします。

「名前を付けて保存」ウィンドウが表示されます。作成したプロファイルを実効ファイル形式で保存します。

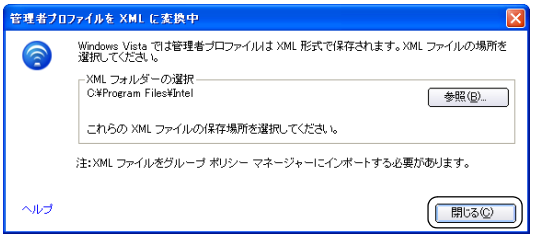
POINT

・管理者ツールで作成したパッケージを他のパソコンに適用することができます。

12 ファイル名を入力して「保存」をクリックします。

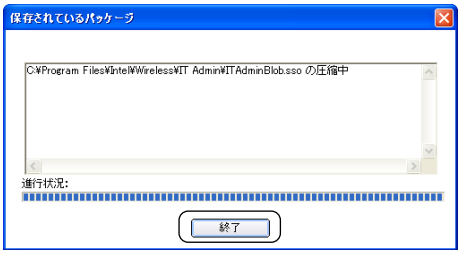
「管理者プロファイルを XML に変換中」ウィンドウが表示されます。

13 「閉じる」をクリックします。

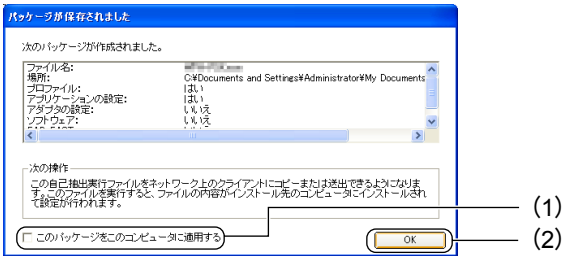


「保存されているパッケージ」ウィンドウが表示されます。

14 「終了」をクリックします。



15 **(1)「このパッケージをこのコンピュータに適用する」にチェックを入れ、(2)「OK」をクリックします。**



16 **「閉じる」をクリックします。**
作成したプロファイルが適用されます。

17 **「閉じる」をクリックします。**

ドメインログオン使用：IEEE 802.1X ＋ PEAP-MSCHAPv2 ／ WPA ＋ PEAP-MSCHAPv2 ／ WPA2 ＋ PEAP-MSCHAPv2

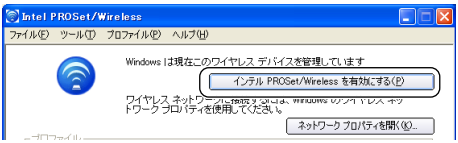
次のセキュリティパターンでドメインログオンをお使いになる場合の設定方法を説明します。

・IEEE 802.1X ＋ PEAP-MSCHAPv2
・WPA ＋ PEAP-MSCHAPv2（WPA エンタープライズ PEAP-MSCHAP-V2）
・WPA2 ＋ PEAP-MSCHAPv2（WPA2 エンタープライズ PEAP-MSCHAP-V2）

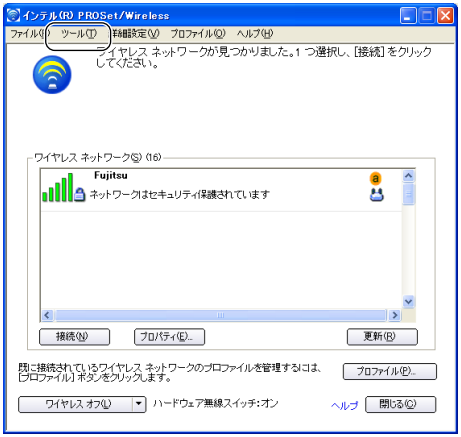
1 **「スタート」ボタン→「すべてのプログラム」→「Intel PROSet Wireless」→「Intel PROSet Wireless」の順にクリックします。**
「インテル (R) PROSet ／ Wireless」ウィンドウが表示されます。

POINT

・Windows XP 標準の無線 LAN 機能が有効になっている場合は、「インテル PROSet/Wireless を有効にする」をクリックしてください。



2 「ツール」メニュー→「管理ツール」の順にクリックします。



「パスワードの作成」ウィンドウが表示されます。

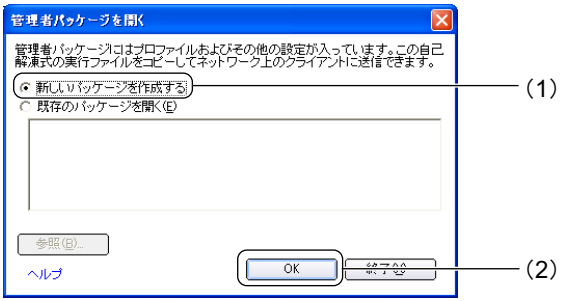
POINT

・ドメインログオンをする場合は、「管理ツール」で設定する必要があります。

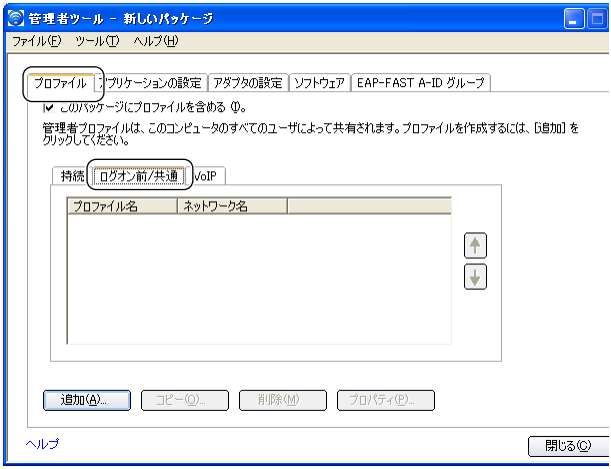
3 プロファイルを保護するためのパスワードを設定し、「OK」をクリックします。

「管理者パッケージを開く」ウィンドウが表示されます。

4 (1)「新しいパッケージを作成する」をクリックして●にし、(2)「OK」をクリックします。



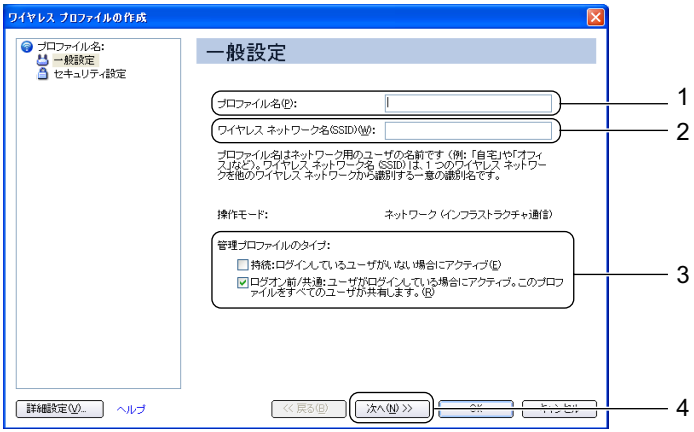
5 「プロファイル」タブの「ログオン前 / 共通」タブをクリックします。



6 「追加」をクリックします。

「ワイヤレスプロファイルの作成」ウィザードが表示されます。

7 無線 LAN のネットワークへ接続するための情報を設定します。次のように設定します。



1. 「プロファイル名」を入力します。
   設定するパラメータ情報を保存するプロファイルの名前を入力します。半角英数字、および日本語（全角文字）32 文字以内で入力できます。
2. 「ワイヤレスネットワーク名（SSID）」を入力します。
   お使いになる環境に合わせてネットワーク名を入力します。ネットワーク名は、半角英数字 32 文字以内で入力してください。
3. 「管理プロファイルのタイプ」を設定します。
   ・持続

「持続」を☑にすると、起動時およびコンピューターにログオンしているユーザーがいない場合でも、プロファイルが有効になります。この場合は認証情報を保存する必要があります。

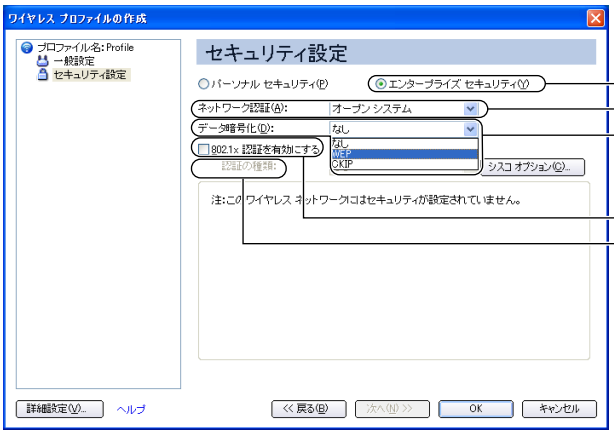
・ログオン前 / 共通

「ログオン前 / 共通」を☑にすると、ユーザーがコンピューターにログオンすると同時に接続が行われます。

4. 設定が終わったら「次へ」をクリックします。

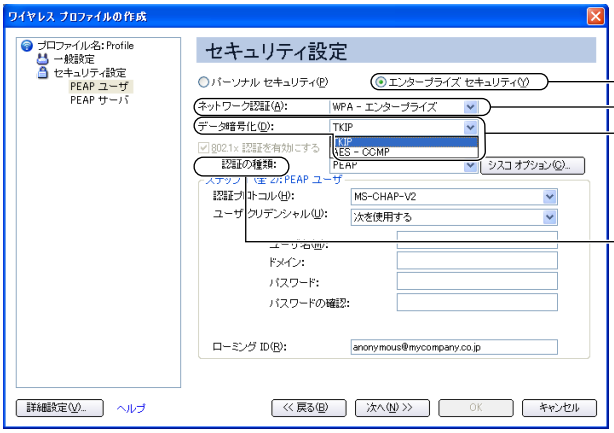
8 セキュリティを設定します。

■ IEEE 802.1X の場合



1. 「エンタープライズ セキュリティ」の◯をクリックして◉にします。
2. 「ネットワーク認証」の⌄をクリックし、「オープン システム」を選択します。
3. 「データ暗号化」の⌄をクリックし、「WEP」を選択します。
4. 「802.1x 認証を有効にする」の☐をクリックして☑にします。
5. 「認証の種類」の⌄をクリックして、「PEAP」を選択します。

■ WPA ／ WPA2 の場合



1. 「エンタープライズ セキュリティ」の○をクリックして◉にします。
2. 「ネットワーク認証」の▼をクリックし、「WPA - エンタープライズ」または「WPA2 - エンタープライズ」を選択します。
   お使いになる環境、無線 LAN アクセスポイントに合わせて設定してください。
3. 「データ暗号化」の▼をクリックし、「TKIP」または、「AES - CCMP」を選択します。
   お使いになる環境、無線 LAN アクセスポイントに合わせて設定してください。
4. 「認証の種類」の▼をクリックして、「PEAP」を選択します。

9 認証の設定（ステップ 1）を行います。

1. 「認証プロトコル」の▼をクリックして、「MS-CHAP-V2」を選択します。
2. 「ユーザクリデンシャル」を選択します。
   - 接続のたびに認証情報を入力する場合は、▼をクリックして「接続するたびにプロンプトを表示する」を選択します。
   - シングルサインオンを使用する場合は、▼をクリックして「Windows ログオンを使用する」を選択します。
   - 認証情報を保存する場合は、▼をクリックして「次を使用する」を選択し、次のように入力します。

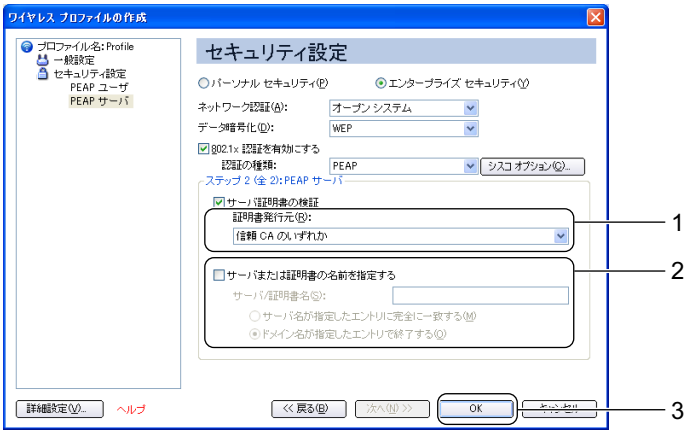
     手順 7 の「管理プロファイルのタイプ」で「持続」を☑にした場合は、この設定だけが選択できます。

表：「次を使用する」を選択した場合の設定

項目	説明
ユーザ名	認証に使用するユーザー名を入力します。
ドメイン	ドメインに参加しているネットワークに接続する場合は、RADIUS サーバーのドメイン名を入力します。
パスワード	認証に使用するユーザーのパスワードを入力します。
パスワードの確認	確認のため、「パスワード」と同じ値を入力します。

3.「ローミング ID」に、認証に使用するユーザー名を入力します。
4.「次へ」をクリックします。

10 認証の設定（ステップ 2）をします。



1.「証明書発行元」の をクリックして、使用する証明書の発行元を選択するか、「信頼 CA のいずれか」を選択します。
2. サーバー／証明書を指定する場合は、「サーバまたは証明書の名前を指定する」の をクリックして にし、RADIUS サーバーに合わせて次のように設定します。
   サーバー名が、証明書のサーバー名と完全に一致する場合、「サーバ名が指定したエントリに完全に一致する」を にし、「サーバ／証明書名」にサーバー名を入力します。
   証明書にこのドメインまたは、このドメインのサブドメインに属するサーバー名が指定されている場合は、「ドメイン名が指定したエントリで終了」を にし、「サーバ／証明書名」にドメイン名を入力します。
3. 設定が終了したら、「OK」をクリックします。

「プロファイルウィザード」が終了し、「プロファイル」に作成したプロファイルが追加されます。

11 「ファイル」メニュー→「パッケージを保存する」の順にクリックします。

「名前を付けて保存」ウィンドウが表示されます。作成したプロファイルを実効ファイル形式で保存します。

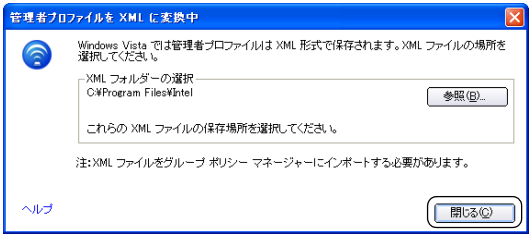
POINT

・管理者ツールで作成したパッケージを他のパソコンに適用することができます。

12 ファイル名を入力して「保存」をクリックします。

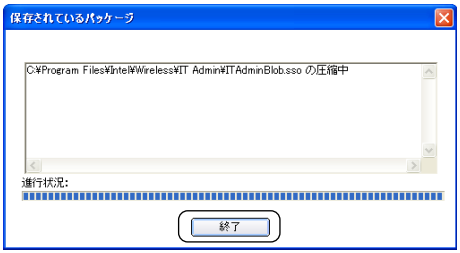
「管理者プロファイルを XML に変換中」ウィンドウが表示されます。

13 「閉じる」をクリックします。

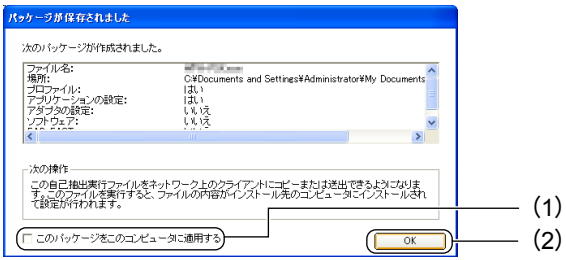


「保存されているパッケージ」ウィンドウが表示されます。

14 「終了」をクリックします。



15 (1)「このパッケージをこのコンピュータに適用する」にチェックを入れ、(2)「OK」をクリックします。



16 「閉じる」をクリックします。

作成したプロファイルが適用されます。

17 「閉じる」をクリックします。

ドメインログオン使用：IEEE 802.1X ＋ PEAP-TLS ／ WPA ＋ PEAP-TLS ／ WPA2 ＋ PEAP-TLS

次のセキュリティパターンでドメインログオンをお使いになる場合の設定方法を説明します。

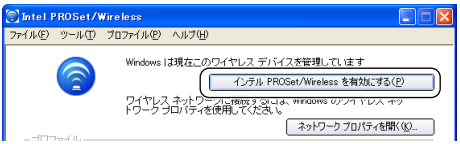
・IEEE 802.1X ＋ PEAP-TLS
・WPA ＋ PEAP-TLS（WPA エンタープライズ PEAP-TLS）
・WPA2 ＋ PEAP-TLS（WPA2 エンタープライズ PEAP-TLS）

1 「スタート」ボタン→「すべてのプログラム」→「Intel PROSet Wireless」→「Intel PROSet Wireless」の順にクリックします。

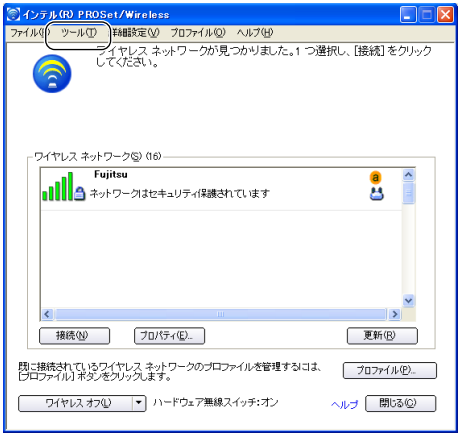
「インテル (R) PROSet ／ Wireless」ウィンドウが表示されます。

POINT

・Windows XP 標準の無線 LAN 機能が有効になっている場合は、「インテル PROSet/Wireless を有効にする」をクリックしてください。



2 「ツール」メニュー→「管理ツール」の順にクリックします。



「パスワードの作成」ウィンドウが表示されます。

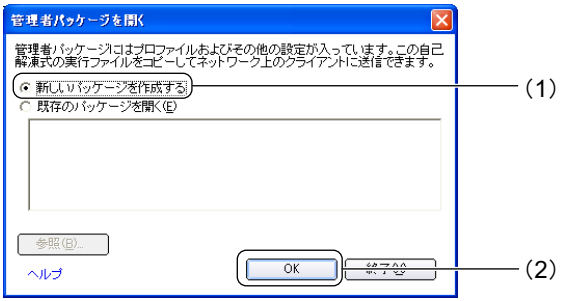
POINT

・ドメインログオンをする場合は、「管理ツール」で設定する必要があります。

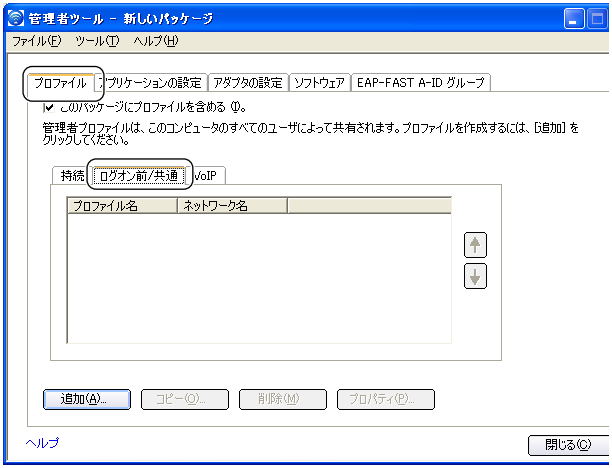
3 **プロファイルを保護するためのパスワードを設定し、「OK」をクリックします。**

「管理者パッケージを開く」ウィンドウが表示されます。

4 **(1)「新しいパッケージを作成する」をクリックして◉にし、(2)「OK」をクリックします。**



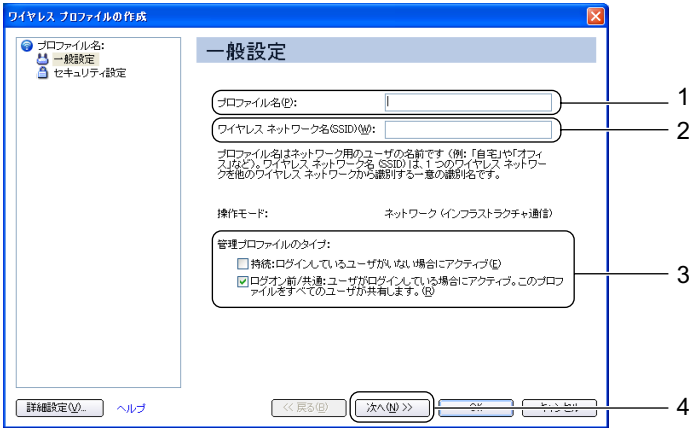
5 **「プロファイル」タブの「ログオン前 / 共通」タブをクリックします。**



6 **「追加」をクリックします。**

「ワイヤレスプロファイルの作成」ウィザードが表示されます。

7 無線 LAN のネットワークへ接続するための情報を設定します。次のように設定します。



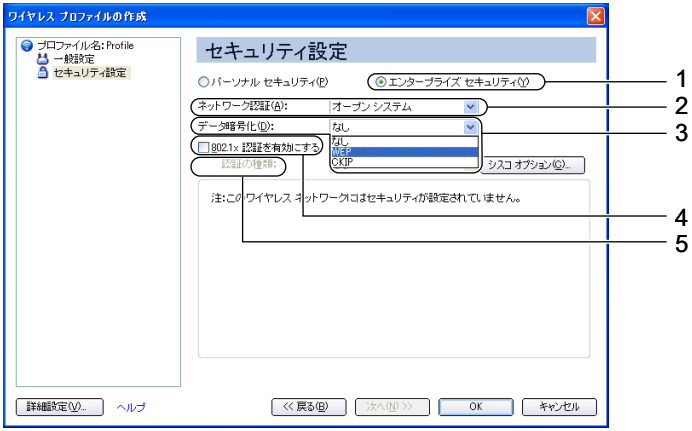
1. 「プロファイル名」を入力します。
   設定するパラメータ情報を保存するプロファイルの名前を入力します。半角英数字、および日本語（全角文字）32 文字以内で入力できます。
2. 「ワイヤレスネットワーク名（SSID）」を入力します。
   お使いになる環境に合わせてネットワーク名を入力します。ネットワーク名は、半角英数字 32 文字以内で入力してください。
3. 「管理プロファイルのタイプ」を設定します。
   - 持続

     「持続」を☑にすると、起動時およびコンピューターにログオンしているユーザーがいない場合でも、プロファイルが有効になります。この場合は認証情報を保存する必要があります。
   - ログオン前 / 共通

     「ログオン前 / 共通」を☑にすると、ユーザーがコンピューターにログオンすると同時に接続が行われます。
4. 設定が終わったら「次へ」をクリックします。

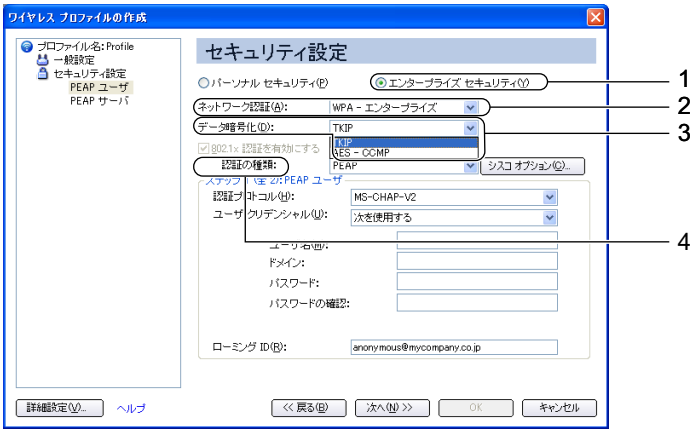
8 セキュリティを設定します。

■ IEEE 802.1X の場合



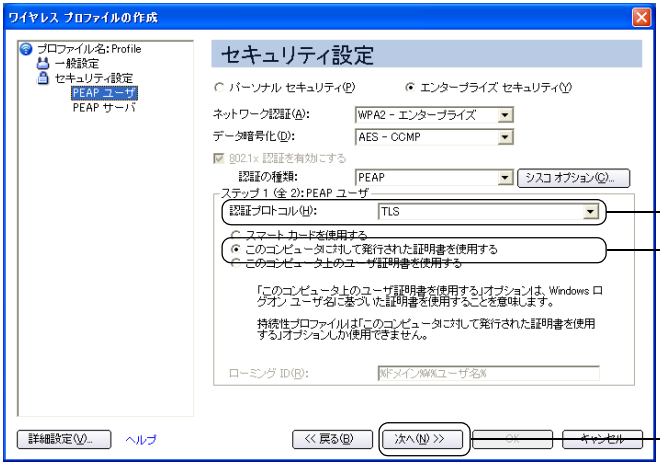
1. 「エンタープライズ セキュリティ」の ○ をクリックして ◉ にします。
2. 「ネットワーク認証」の ⌄ をクリックし、「オープン システム」を選択します。
3. 「データ暗号化」の ⌄ をクリックし、「WEP」を選択します。
4. 「802.1x 認証を有効にする」の ☐ をクリックして ☑ にします。
5. 「認証の種類」の ⌄ をクリックして、「PEAP」を選択します。

■ WPA ／ WPA2 の場合



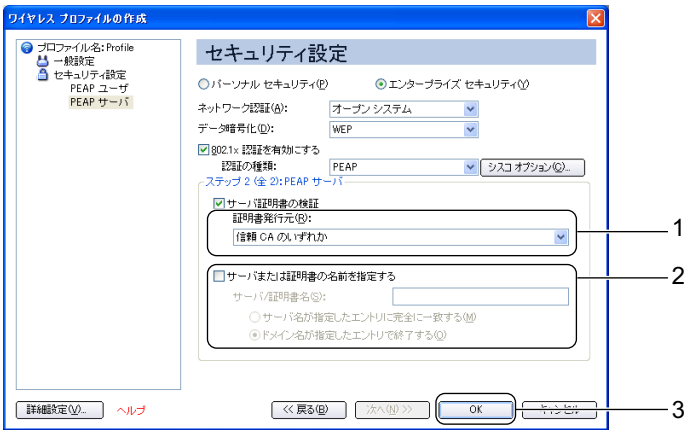
1. 「エンタープライズ セキュリティ」の ○ をクリックして ◉ にします。
2. 「ネットワーク認証」の ⌄ をクリックし、「WPA - エンタープライズ」または「WPA2 - エンタープライズ」を選択します。
   お使いになる環境、無線 LAN アクセスポイントに合わせて設定してください。
3. 「データ暗号化」の ⌄ をクリックし、「TKIP」または、「AES - CCMP」を選択します。
   お使いになる環境、無線 LAN アクセスポイントに合わせて設定してください。
4. 「認証の種類」の ⌄ をクリックして、「PEAP」を選択します。

9 認証の設定（ステップ 1）を行います。



1. 「認証プロトコル」の をクリックして「TLS」を選択します。
2. 「このコンピュータに対して発行された証明書を使用する」をクリックして にします。
3. 「次へ」をクリックします。

10 認証の設定（ステップ 2）をします。



1. 「証明書発行元」の をクリックして、使用する証明書の発行元を選択するか、「信頼 CA のいずれか」を選択します。
2. サーバー／証明書を指定する場合は、「サーバまたは証明書の名前を指定する」の をクリックして にし、RADIUS サーバーに合わせて次のように設定します。
   サーバー名が、証明書のサーバー名と完全に一致する場合、「サーバ名が指定したエントリに完全に一致する」を にし、「サーバ／証明書名」にサーバー名を入力します。
   証明書にこのドメインまたは、このドメインのサブドメインに属するサーバー名が指定されている場合は、「ドメイン名が指定したエントリで終了」を にし、「サーバ／証明書名」にドメイン名を入力します。
3. 設定が終了したら、「OK」をクリックします。

「プロファイルウィザード」が終了し、「プロファイル」に作成したプロファイルが追加されます。

11 「ファイル」メニュー→「パッケージを保存する」の順にクリックします。

「名前を付けて保存」ウィンドウが表示されます。作成したプロファイルを実効ファイル形式で保存します。

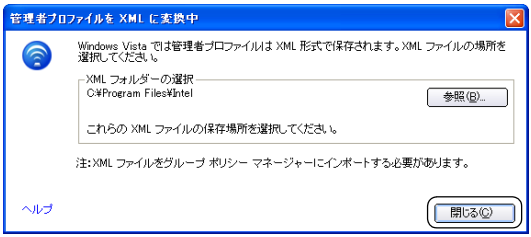
POINT

・管理者ツールで作成したパッケージを他のパソコンに適用することができます。

12 ファイル名を入力して「保存」をクリックします。

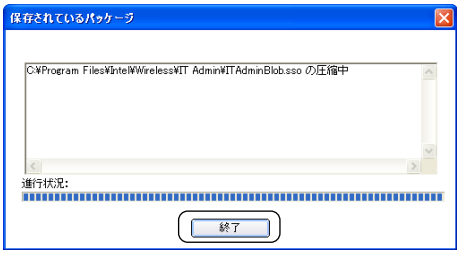
「管理者プロファイルを XML に変換中」ウィンドウが表示されます。

13 「閉じる」をクリックします。

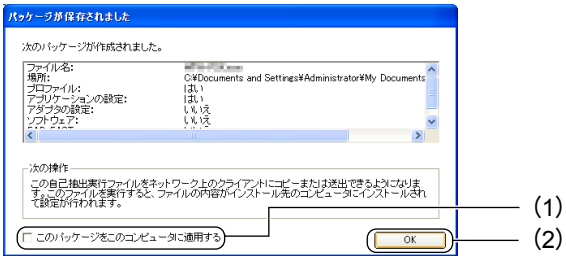


「保存されているパッケージ」ウィンドウが表示されます。

14 「終了」をクリックします。



15 **(1)「このパッケージをこのコンピュータに適用する」にチェックを入れ、(2)「OK」をクリックします。**



16 **「閉じる」をクリックします。**
作成したプロファイルが適用されます。

17 **「閉じる」をクリックします。**

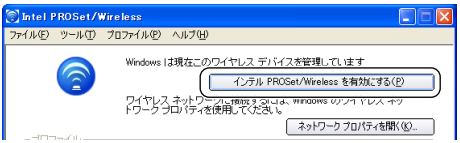
ドメインログオン使用：WPA-PSK

WPA-PSK でドメインログオンをお使いになる場合の設定方法を説明します。

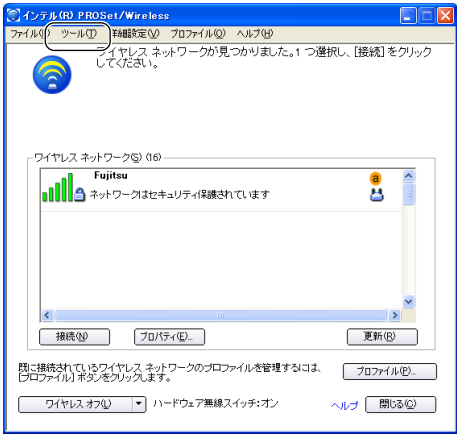
1 **「スタート」ボタン→「すべてのプログラム」→「Intel PROSet Wireless」→「Intel PROSet Wireless」の順にクリックします。**
「インテル (R) PROSet ／ Wireless」ウィンドウが表示されます。

POINT

・Windows XP 標準の無線 LAN 機能が有効になっている場合は、「インテル PROSet/Wireless を有効にする」をクリックしてください。



2 「ツール」メニュー→「管理ツール」の順にクリックします。



「パスワードの作成」ウィンドウが表示されます。

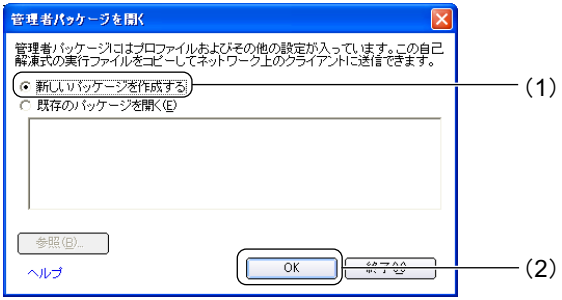
POINT

・ドメインログオンをする場合は、「管理ツール」で設定する必要があります。

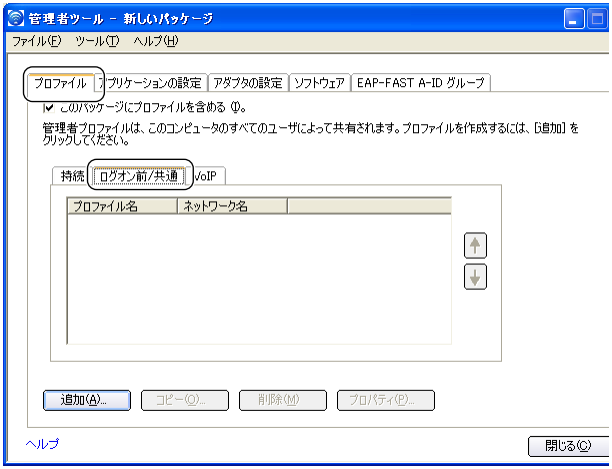
3 プロファイルを保護するためのパスワードを設定し、「OK」をクリックします。

「管理者パッケージを開く」ウィンドウが表示されます。

4 (1)「新しいパッケージを作成する」をクリックして◉にし、(2)「OK」をクリックします。



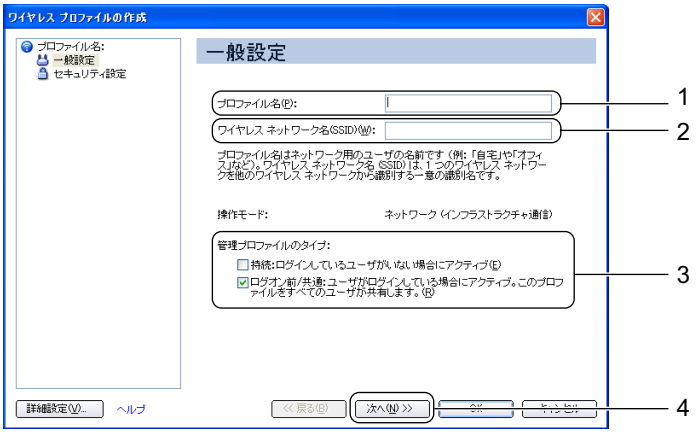
5 「プロファイル」タブの「ログオン前 / 共通」タブをクリックします。



6 「追加」をクリックします。

「ワイヤレスプロファイルの作成」ウィザードが表示されます。

7 無線 LAN のネットワークへ接続するための情報を設定します。次のように設定します。



1. 「プロファイル名」を入力します。
   設定するパラメータ情報を保存するプロファイルの名前を入力します。半角英数字、および日本語（全角文字）32 文字以内で入力できます。
2. 「ワイヤレスネットワーク名（SSID）」を入力します。
   お使いになる環境に合わせてネットワーク名を入力します。ネットワーク名は、半角英数字 32 文字以内で入力してください。
3. 「管理プロファイルのタイプ」を設定します。
   ・持続

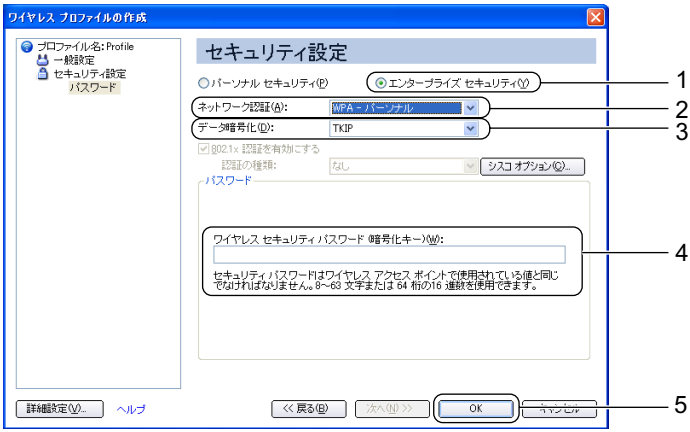
「持続」を☑にすると、起動時およびコンピューターにログオンしているユーザーがいない場合でも、プロファイルが有効になります。

・ログオン前 / 共通

「ログオン前 / 共通」を☑にすると、ユーザーがコンピューターにログオンすると同時に接続が行われます。

4. 設定が終わったら「次へ」をクリックします。

8 セキュリティの設定をします。次のように設定します。



1. 「エンタープライズ セキュリティ」の◯をクリックして◉にします。
2. 「ネットワーク認証」の ⌄ をクリックし、「WPA - パーソナル」または「WPA2 - パーソナル」を選択します。

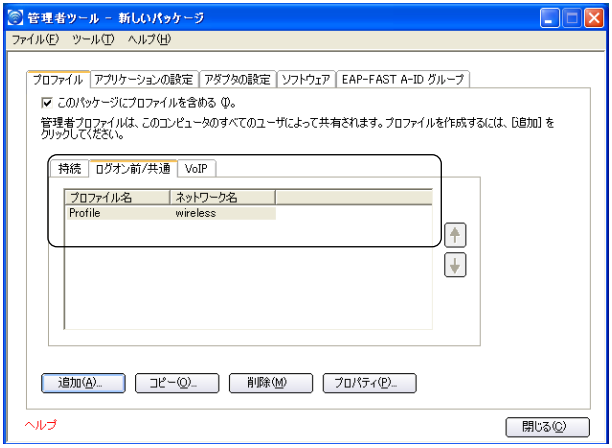
   お使いになる環境、無線 LAN アクセスポイントに合わせて設定してください。
3. 「データ暗号化」を選択します。

   お使いになる環境、無線 LAN アクセスポイントに合わせて設定してください。
4. お使いになる接続方法に合わせて「ワイヤレスセキュリティパスワード（暗号化キー）」を入力します。

   パスフレーズまたは 16 進数で入力します。お使いになる環境、無線 LAN アクセスポイントに合わせて設定してください。

5. 設定が終了したら、「OK」をクリックします。

「ワイヤレス プロファイルの作成」ウィザードが終了し、「ログオン前 / 共通」に作成したプロファイルが追加されます。



9 **「ファイル」メニュー→「パッケージを保存する」の順にクリックします。**

「名前を付けて保存」ウィンドウが表示されます。作成したプロファイルを実効ファイル形式で保存します。

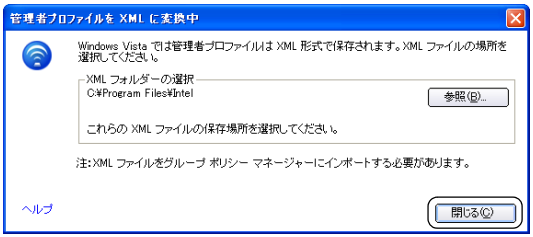
POINT

・管理者ツールで作成したパッケージを他のパソコンに適用することができます。

10 **ファイル名を入力して「保存」をクリックします。**

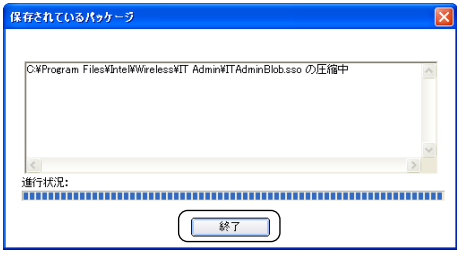
「管理者プロファイルを XML に変換中」ウィンドウが表示されます。

11 **「閉じる」をクリックします。**

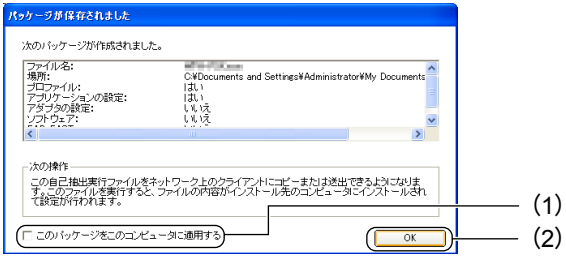


「保存されているパッケージ」ウィンドウが表示されます。

12 「終了」をクリックします。



13 (1)「このパッケージをこのコンピュータに適用する」にチェックを入れ、(2)「OK」をクリックします。



14 「閉じる」をクリックします。

作成したプロファイルが適用されます。

15 「閉じる」をクリックします。

6 Intel 無線 LAN 搭載モデル v10.1.x 系の設定

クライアントのパソコンが、Intel 無線 LAN 搭載モデル v10.1.x 系の場合の設定方法を説明します。

重要

シングルサインオン／ドメインログオンを使用する場合

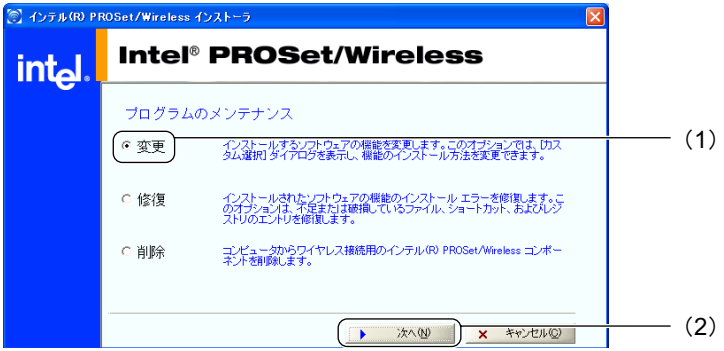
プログラムの追加が必要です。追加方法については、「シングルサインオン／ドメインログオンを使用する場合のプログラムの追加」（→ P.140）をご覧ください。

シングルサインオン／ドメインログオンを使用する場合のプログラムの追加

シングルサインオンやドメインログオンを使用する場合は、次の手順に従って、プログラムを追加してください。

1. **「スタート」ボタン→「コントロールパネル」または、「スタート」ボタン→「設定」→「コントロールパネル」の順にクリックします。**
   「コントロールパネル」ウィンドウが表示されます。
2. **Windows XP の場合は「プログラムの追加と削除」、Windows 2000 の場合は「アプリケーションの追加と削除」をクリックします。**
3. **「現在インストールされているプログラム」の一覧から、「インテル (R) PROSet/Wireless ソフトウェア」を選択し、「変更と削除」をクリックします。**
   「インテル (R) PROSet/Wireless インストーラ」ウィンドウが表示されます。

4 **(1)「変更」を◉にして、(2)「次へ」をクリックします。**



5 **「シングルサインオン」の✕をクリックし、表示されるメニューから「この機能と、すべてのサブ機能をインストールする」を選択します。**

6 **「管理者ツールキット」の✕をクリックし、表示されるメニューから「この機能と、すべてのサブ機能をインストールする」を選択します。**

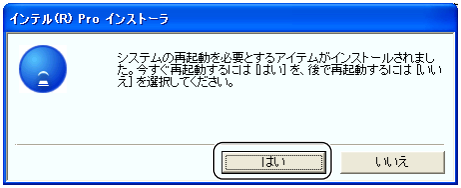
7 **「編集」をクリックします。**

追加するプログラムがインストールされます。

8 **「インテル (R) PROSet/Wireless インストーラ」ウィンドウで「コンポーネントの変更を完了しました。」と表示されたら、次のように操作します。**

1. 「シングルサインオン」、「ログオン前接続」、「管理者ツールキット」に✔がついていることを確認します。
2. 「OK」をクリックします。

9 **システムの再起動について確認のメッセージが表示されたら、「はい」をクリックして、パソコンを再起動します。**



IEEE 802.1X ＋ EAP-TLS ／ WPA ＋ EAP-TLS ／ WPA2 ＋ EAP-TLS

次のセキュリティパターンの場合の設定方法を説明します。

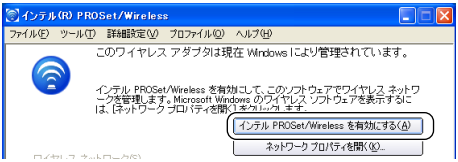
- IEEE 802.1X ＋ EAP-TLS
- WPA ＋ EAP-TLS
- WPA2 ＋ EAP-TLS

1 **「スタート」ボタン→「すべてのプログラム」→「Intel PROSet Wireless」→「Intel PROSet Wireless」の順にクリックします。**

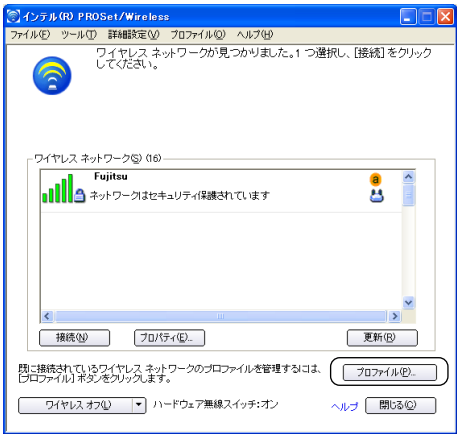
「インテル (R) PROSet/Wireless」ウィンドウが表示されます。

POINT

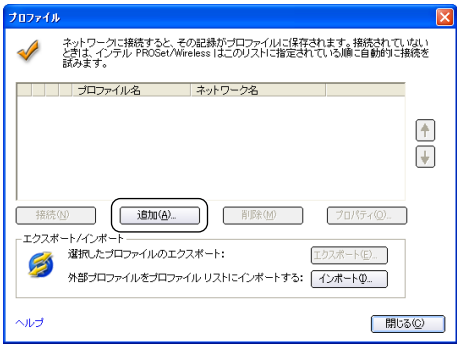
- Windows XP 標準の無線 LAN 機能が有効になっている場合は、「インテル PROSet/Wireless を有効にする」をクリックしてください。



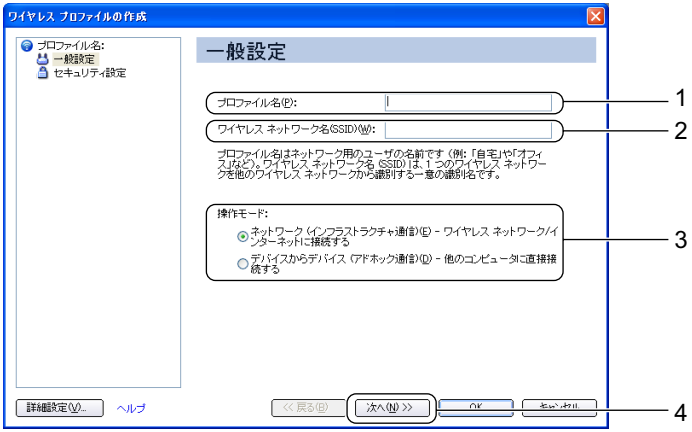
2 「プロファイル」をクリックします。



3 「追加」をクリックします。



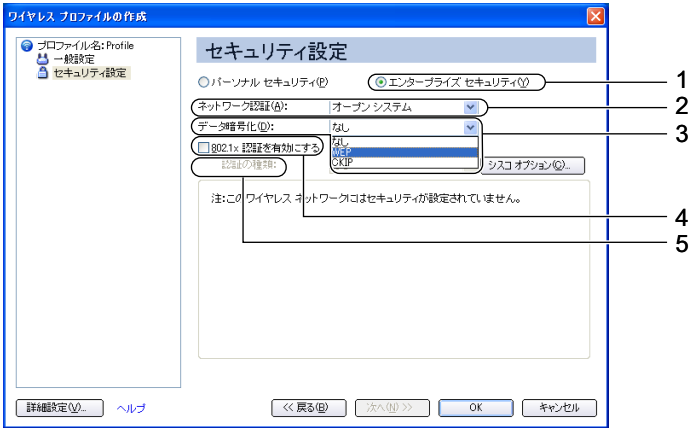
4 無線 LAN のネットワークへ接続するための情報を設定します。



1. 「プロファイル名」を入力します。
   設定するパラメータ情報を保存するシステムファイルの名前を入力します。プロファイル名は半角英数字および、日本語（全角文字）を 32 文字以内で入力できます。
2. 「ワイヤレスネットワーク名（SSID)」を入力します。
   お使いになる環境に合わせてネットワーク名を入力します。ネットワーク名は、半角英数字 32 文字以内で入力してください。
3. 「操作モード」の「ネットワーク（インフラストラクチャ通信）- ワイヤレスネットワーク / インターネットに接続する」をクリックして◉にします。
4. 「次へ」をクリックします。

5 セキュリティを設定します。

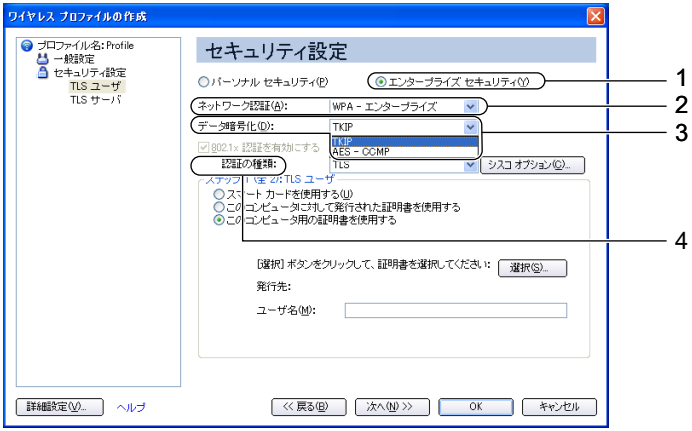
■ IEEE 802.1X の場合



1. 「エンタープライズ セキュリティ」の○をクリックして◉にします。
2. 「ネットワーク認証」の ▼ をクリックし、「オープン システム」を選択します。

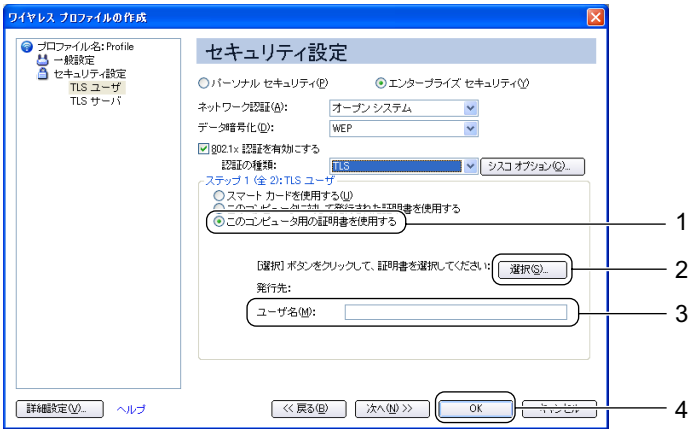
3. 「データ暗号化」の をクリックし、「WEP」を選択します。
4. 「802.1x 認証を有効にする」の をクリックして にします。
5. 「認証の種類」の をクリックして、「TLS」を選択します。

■ WPA ／ WPA2 の場合



1. 「エンタープライズ セキュリティ」の をクリックして にします。
2. 「ネットワーク認証」の をクリックし、「WPA - エンタープライズ」または「WPA2 - エンタープライズ」を選択します。
   お使いになる環境、無線 LAN アクセスポイントに合わせて設定してください。
3. 「データ暗号化」の をクリックし、「TKIP」または、「AES - CCMP」を選択します。
   お使いになる環境、無線 LAN アクセスポイントに合わせて設定してください。
4. 「認証の種類」の をクリックして、「TLS」を選択します。

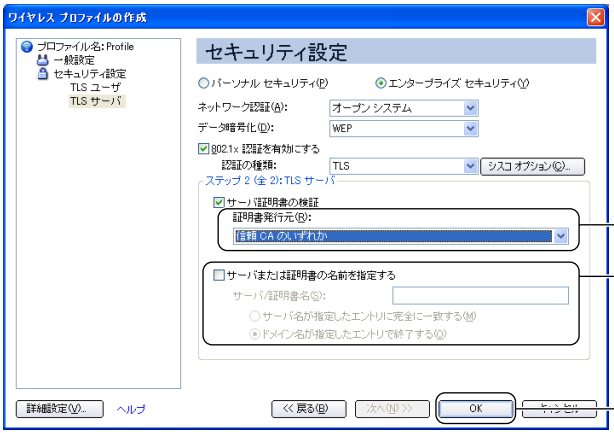
6 認証の設定（ステップ 1）をします。



1. 「このコンピュータ用の証明書を使用する」をクリックして にします。
2. 「選択」をクリックし、使用する証明書を選択します。

3.「ユーザ名」に、認証に使用するユーザー名を入力します。
4.「次へ」をクリックします。

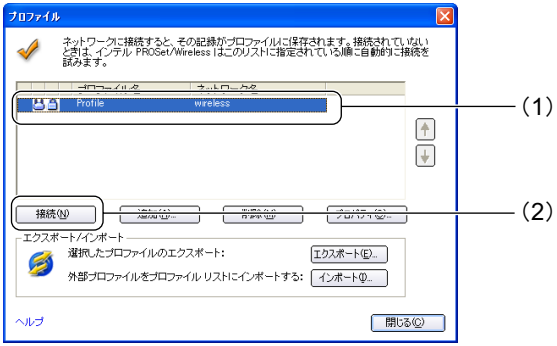
7 認証の設定（ステップ 2）をします。



1.「証明書発行元」の をクリックして、使用する証明書の発行元を選択します。
2. サーバー／証明書を指定する場合は、「サーバまたは証明書の名前を指定する」の をクリックして にし、RADIUS サーバーに合わせて次のように設定します。
   サーバー名が、証明書のサーバー名と完全に一致する場合、「サーバ名が指定したエントリに完全に一致する」を にし、「サーバ／証明書名」にサーバー名を入力します。
   証明書にこのドメインまたは、このドメインのサブドメインに属するサーバー名が指定されている場合は、「ドメイン名が指定したエントリで終了」を にし、「サーバ／証明書名」にドメイン名を入力します。
3. 設定が終了したら、「OK」をクリックします。

「プロファイルウィザード」が終了し、「プロファイル」に作成したプロファイルが追加されます。

8 **(1)「プロファイル」のリストから作成したプロファイルを選択し、(2)「接続」をクリックします。**



IEEE 802.1X ＋ PEAP-MSCHAPv2 ／ WPA ＋ PEAP-MSCHAPv2 ／ WPA2 ＋ PEAP-MSCHAPv2

次のセキュリティパターンの場合の設定方法を説明します。

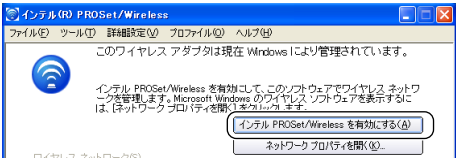
- IEEE 802.1X ＋ PEAP-MSCHAPv2
- WPA ＋ PEAP-MSCHAPv2
- WPA2 ＋ PEAP-MSCHAPv2

1 **「スタート」ボタン→「すべてのプログラム」→「Intel PROSet Wireless」→「Intel PROSet Wireless」の順にクリックします。**

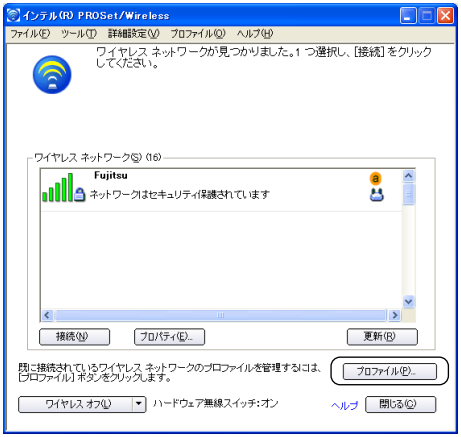
「インテル (R) PROSet/Wireless」ウィンドウが表示されます。

POINT

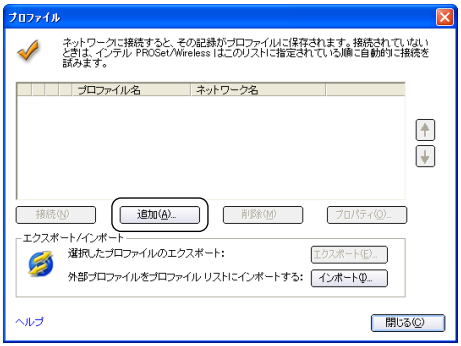
- Windows XP 標準の無線 LAN 機能が有効になっている場合は、「インテル PROSet/Wireless を有効にする」をクリックしてください。



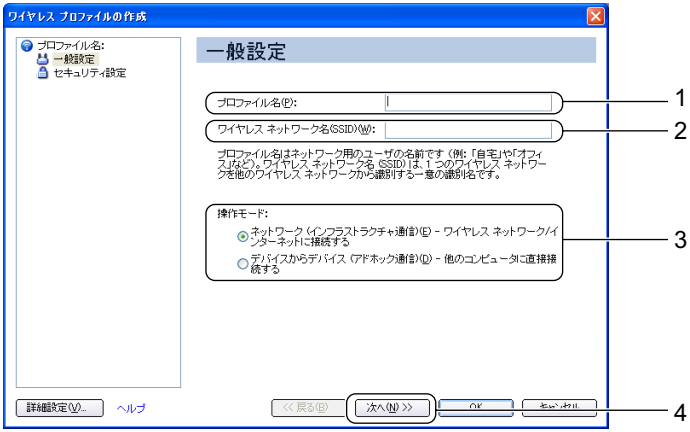
2 「プロファイル」をクリックします。



3 「追加」をクリックします。



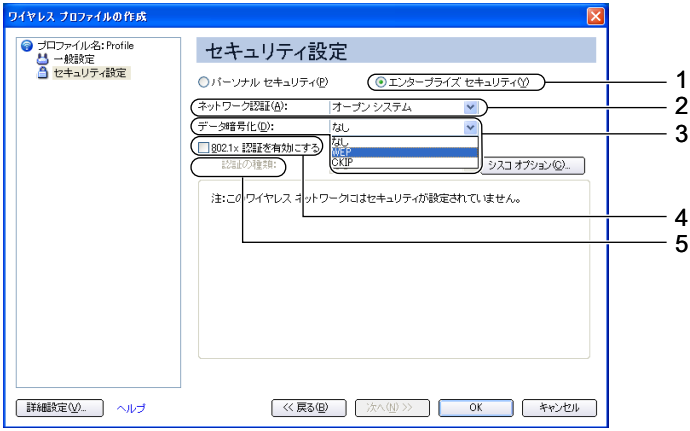
4 無線 LAN のネットワークへ接続するための情報を設定します。



1. 「プロファイル名」を入力します。
   設定するパラメータ情報を保存するシステムファイルの名前を入力します。プロファイル名は半角英数字および、日本語（全角文字）を 32 文字以内で入力できます。
2. 「ワイヤレスネットワーク名（SSID)」を入力します。
   お使いになる環境に合わせてネットワーク名を入力します。ネットワーク名は、半角英数字 32 文字以内で入力してください。
3. 「操作モード」の「ネットワーク（インフラストラクチャ通信）- ワイヤレスネットワーク / インターネットに接続する」をクリックして◉にします。
4. 「次へ」をクリックします。

5 セキュリティを設定します。

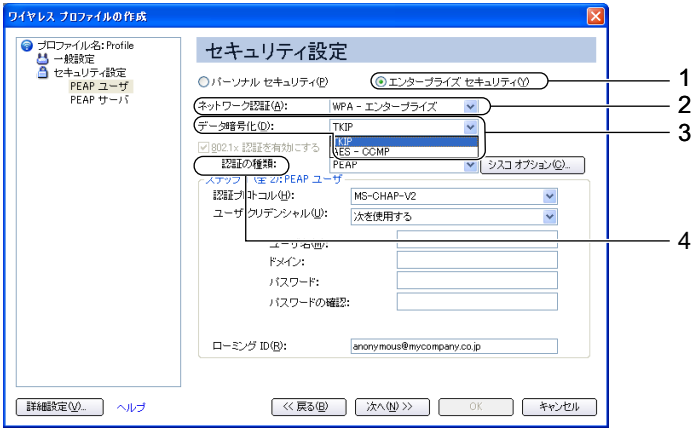
■ IEEE 802.1X の場合



1. 「エンタープライズ セキュリティ」の○をクリックして◉にします。
2. 「ネットワーク認証」の ⌄ をクリックし、「オープン システム」を選択します。

3.「データ暗号化」の をクリックし、「WEP」を選択します。
4.「802.1x 認証を有効にする」の をクリックして にします。
5.「認証の種類」の をクリックして、「PEAP」を選択します。

■ WPA ／ WPA2 の場合



1.「エンタープライズ セキュリティ」の をクリックして にします。
2.「ネットワーク認証」の をクリックし、「WPA - エンタープライズ」または「WPA2 - エンタープライズ」を選択します。
お使いになる環境、無線 LAN アクセスポイントに合わせて設定してください。
3.「データ暗号化」の をクリックし、「TKIP」または、「AES - CCMP」を選択します。
お使いになる環境、無線 LAN アクセスポイントに合わせて設定してください。
4.「認証の種類」の をクリックして、「PEAP」を選択します。

6 認証の設定（ステップ 1）を行います。

1.「認証プロトコル」の をクリックして、「MS-CHAP-V2」を選択します。
2.「ユーザクリデンシャル」を選択します。

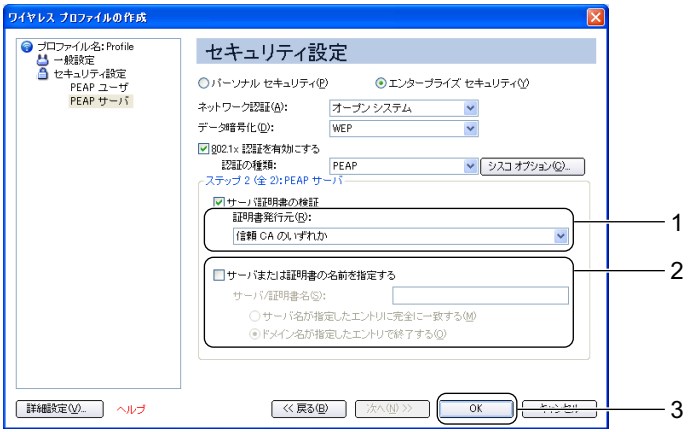
・接続のたびに認証情報を入力する場合は、をクリックして「接続するたびにプロンプトを表示する」を選択します。
・シングルサインオンを使用する場合は、をクリックして「Windows ログオンを使用する」を選択します。
シングルサインオンを使用する場合は、プログラムを追加する必要があります。
プログラムの追加方法については、「シングルサインオン／ドメインログオンを使用する場合のプログラムの追加」（→ P.140）をご覧ください。
・認証情報を保存する場合は、をクリックして「次を使用する」を選択し、次のように入力します。

表：「次を使用する」を選択した場合の設定

項目	説明
ユーザ名	認証に使用するユーザー名を入力します。
ドメイン	ドメインに参加しているネットワークに接続する場合は、RADIUS サーバーのドメイン名を入力します。
パスワード	認証に使用するユーザーのパスワードを入力します。
パスワードの確認	確認のため、「パスワード」と同じ値を入力します。

3. 「ローミング ID」に、認証に使用するユーザー名を入力します。
4. 「次へ」をクリックします。

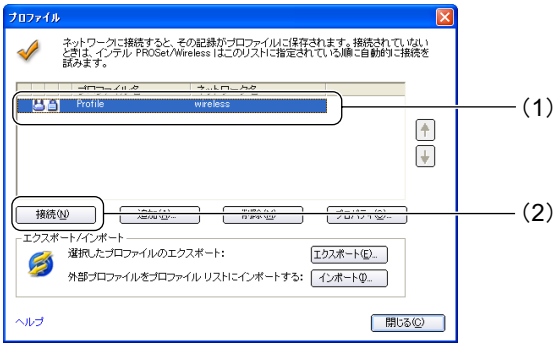
7 認証の設定（ステップ 2）をします。



1. 「証明書発行元」の をクリックして、使用する証明書の発行元を選択します。
2. サーバー／証明書を指定する場合は、「サーバまたは証明書の名前を指定する」の をクリックして にし、RADIUS サーバーに合わせて次のように設定します。
   サーバー名が、証明書のサーバー名と完全に一致する場合、「サーバ名が指定したエントリに完全に一致する」を にし、「サーバ／証明書名」にサーバー名を入力します。
   証明書にこのドメインまたは、このドメインのサブドメインに属するサーバー名が指定されている場合は、「ドメイン名が指定したエントリで終了」を にし、「サーバ／証明書名」にドメイン名を入力します。
3. 設定が終了したら、「OK」をクリックします。

「プロファイルウィザード」が終了し、「プロファイル」に作成したプロファイルが追加されます。

8 (1)「プロファイル」のリストから作成したプロファイルを選択し、(2)「接続」をクリックします。



IEEE 802.1X ＋ PEAP-TLS ／ WPA ＋ PEAP-TLS ／ WPA2 ＋ PEAP-TLS

次のセキュリティパターンの場合の設定方法を説明します。

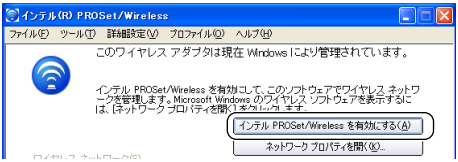
- IEEE 802.1X ＋ PEAP-TLS
- WPA ＋ PEAP-TLS
- WPA2 ＋ PEAP-TLS

1 「スタート」ボタン→「すべてのプログラム」→「Intel PROSet Wireless」→「Intel PROSet Wireless」の順にクリックします。

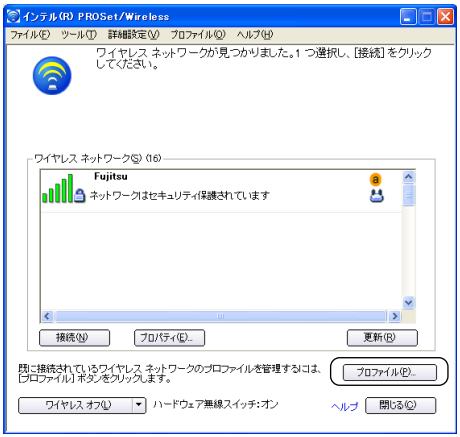
「インテル (R) PROSet/Wireless」ウィンドウが表示されます。

POINT

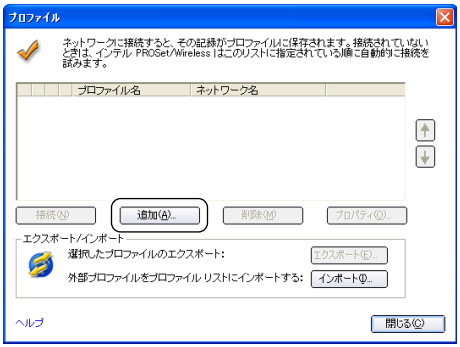
- Windows XP 標準の無線 LAN 機能が有効になっている場合は、「インテル PROSet/Wireless を有効にする」をクリックしてください。



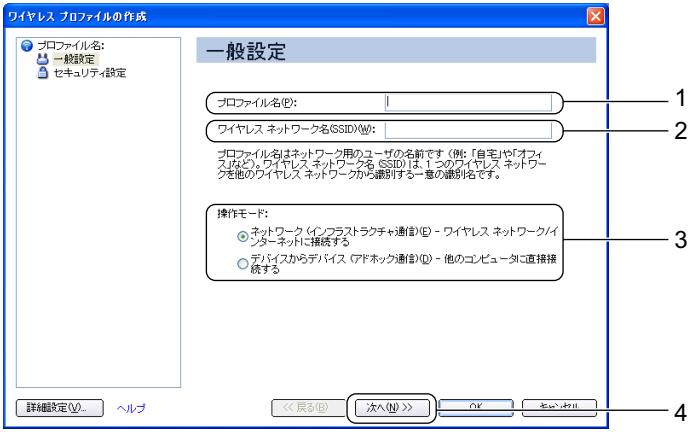
2 「プロファイル」をクリックします。



3 「追加」をクリックします。



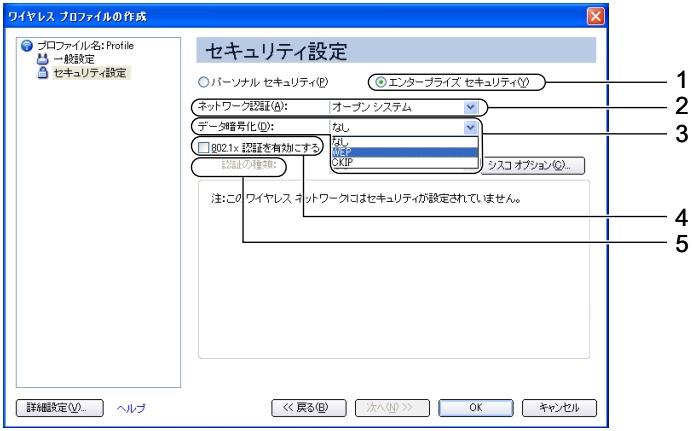
4 無線 LAN のネットワークへ接続するための情報を設定します。



1. 「プロファイル名」を入力します。
   設定するパラメータ情報を保存するシステムファイルの名前を入力します。プロファイル名は半角英数字および、日本語（全角文字）を 32 文字以内で入力できます。
2. 「ワイヤレスネットワーク名（SSID）」を入力します。
   お使いになる環境に合わせてネットワーク名を入力します。ネットワーク名は、半角英数字 32 文字以内で入力してください。
3. 「操作モード」の「ネットワーク（インフラストラクチャ通信） - ワイヤレスネットワーク / インターネットに接続する」をクリックして◉にします。
4. 「次へ」をクリックします。

5 セキュリティを設定します。

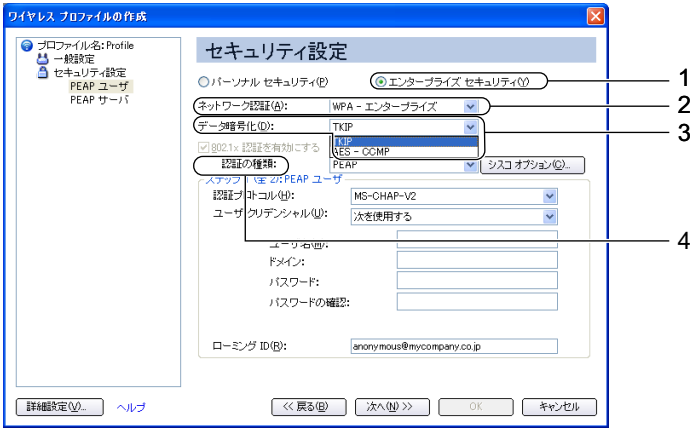
■ IEEE 802.1X の場合



1. 「エンタープライズ セキュリティ」の○をクリックして◉にします。
2. 「ネットワーク認証」の ▼ をクリックし、「オープン システム」を選択します。

3. 「データ暗号化」の をクリックし、「WEP」を選択します。
4. 「802.1x 認証を有効にする」の をクリックして にします。
5. 「認証の種類」の をクリックして、「PEAP」を選択します。

■ WPA ／ WPA2 の場合



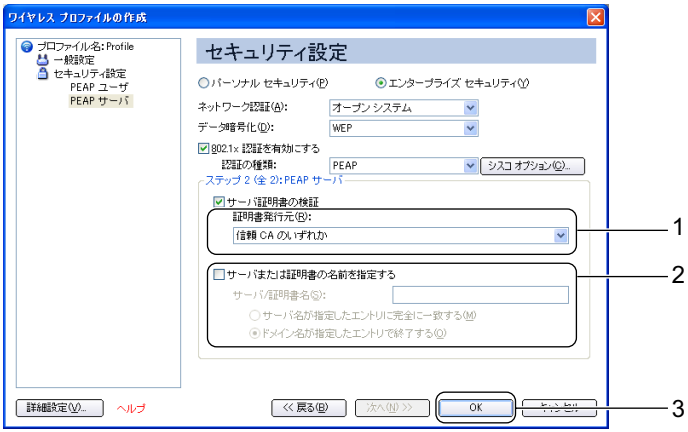
1. 「エンタープライズ セキュリティ」の をクリックして にします。
2. 「ネットワーク認証」の をクリックし、「WPA - エンタープライズ」または「WPA2 - エンタープライズ」を選択します。
   お使いになる環境、無線 LAN アクセスポイントに合わせて設定してください。
3. 「データ暗号化」の をクリックし、「TKIP」または、「AES - CCMP」を選択します。
   お使いになる環境、無線 LAN アクセスポイントに合わせて設定してください。
4. 「認証の種類」の をクリックして、「PEAP」を選択します。

6 認証の設定（ステップ 1）を行います。

1. 「認証プロトコル」の をクリックして、「TLS」を選択します。
2. 「このコンピュータ用の証明書を使用する」をクリックして にします。

3. 「選択」をクリックし、使用する証明書を選択します。
4. 「ユーザ名」に、認証に使用するユーザー名を入力します。
5. 「次へ」をクリックします。

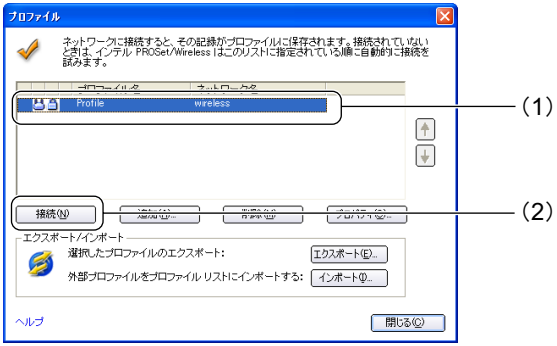
7 認証の設定（ステップ 2）をします。



1. 「証明書発行元」の をクリックして、使用する証明書の発行元を選択します。
2. サーバー／証明書を指定する場合は、「サーバまたは証明書の名前を指定する」の をクリックして にし、RADIUS サーバーに合わせて次のように設定します。
   サーバー名が、証明書のサーバー名と完全に一致する場合、「サーバ名が指定したエントリに完全に一致する」を にし、「サーバ／証明書名」にサーバー名を入力します。
   証明書にこのドメインまたは、このドメインのサブドメインに属するサーバー名が指定されている場合は、「ドメイン名が指定したエントリで終了」を にし、「サーバ／証明書名」にドメイン名を入力します。
3. 設定が終了したら、「OK」をクリックします。

「プロファイルウィザード」が終了し、「プロファイル」に作成したプロファイルが追加されます。

8 **(1)「プロファイル」のリストから作成したプロファイルを選択し、(2)「接続」をクリックします。**



WPA-PSK ／ WPA2-PSK

WPA-PSK ／ WPA2-PSK の場合の設定方法は、Intel 無線 LAN 搭載モデル v11.x 系／ v10.5.x 系と同じです。「WPA-PSK ／ WPA2-PSK」（→ P.111）をご覧ください。

ドメインログオン使用：IEEE 802.1X ＋ EAP-TLS ／ WPA ＋ EAP-TLS ／ WPA2 ＋ EAP-TLS

次のセキュリティパターンでドメインログオンをお使いになる場合の設定方法を説明します。

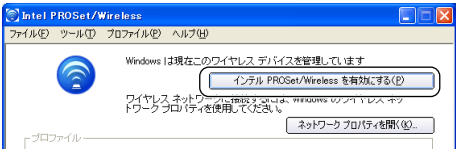
・IEEE 802.1X ＋ EAP-TLS
・WPA ＋ EAP-TLS
・WPA2 ＋ EAP-TLS

1 **「スタート」ボタン→「すべてのプログラム」→「Intel PROSet Wireless」→「Intel PROSet Wireless」の順にクリックします。**

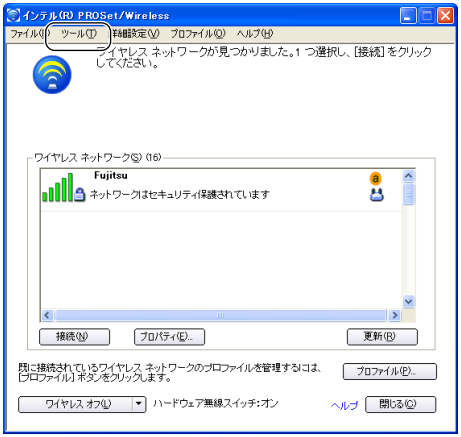
「インテル (R) PROSet ／ Wireless」ウィンドウが表示されます。

POINT

・Windows XP 標準の無線 LAN 機能が有効になっている場合は、「インテル PROSet/Wireless を有効にする」をクリックしてください。



2 「ツール」メニュー→「管理ツール」の順にクリックします。



「パスワードの作成」ウィンドウが表示されます。

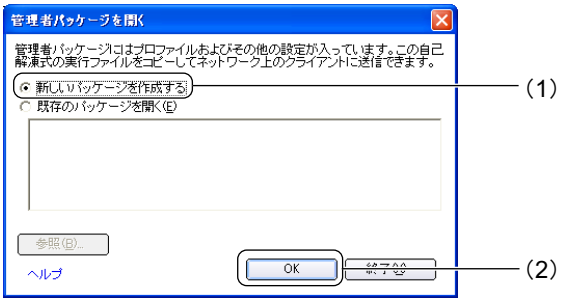
POINT

・ドメインログオンをする場合は、「管理ツール」で設定する必要があります。

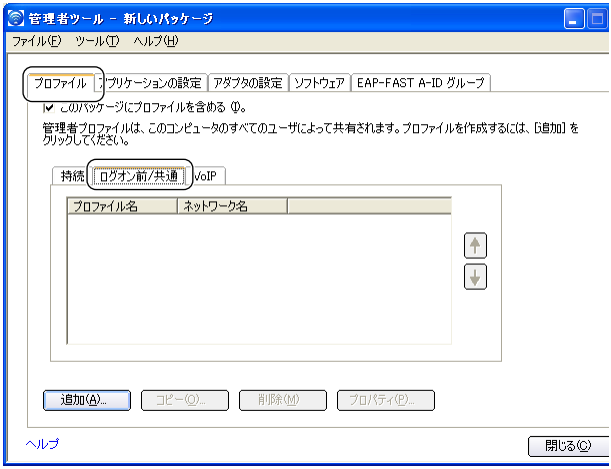
3 プロファイルを保護するためのパスワードを設定し、「OK」をクリックします。

「管理者パッケージを開く」ウィンドウが表示されます。

4 (1)「新しいパッケージを作成する」をクリックして●にし、(2)「OK」をクリックします。



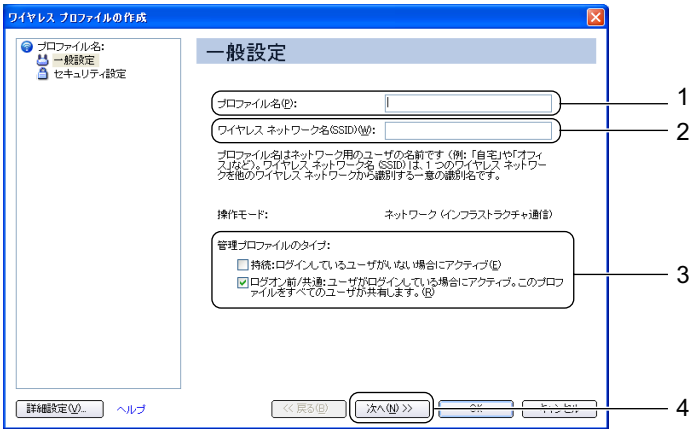
5 「プロファイル」タブの「ログオン前 / 共通」タブをクリックします。



6 「追加」をクリックします。

「ワイヤレスプロファイルの作成」ウィザードが表示されます。

7 無線 LAN のネットワークへ接続するための情報を設定します。次のように設定します。



1. 「プロファイル名」を入力します。
   設定するパラメータ情報を保存するプロファイルの名前を入力します。半角英数字、および日本語（全角文字）32 文字以内で入力できます。
2. 「ワイヤレスネットワーク名（SSID）」を入力します。
   お使いになる環境に合わせてネットワーク名を入力します。ネットワーク名は、半角英数字 32 文字以内で入力してください。
3. 「管理プロファイルのタイプ」を設定します。
   ・持続

「持続」を☑にすると、起動時およびコンピューターにログオンしているユーザーがいない場合でも、プロファイルが有効になります。

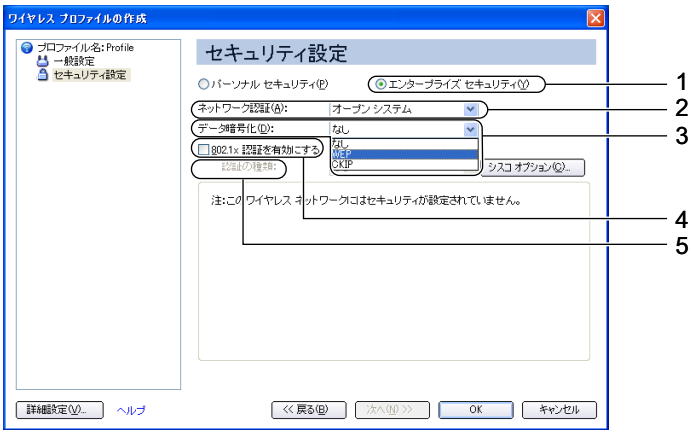
・ログオン前 / 共通

「ログオン前 / 共通」を☑にすると、ユーザーがコンピューターにログオンすると同時に接続が行われます。

4. 設定が終わったら「次へ」をクリックします。

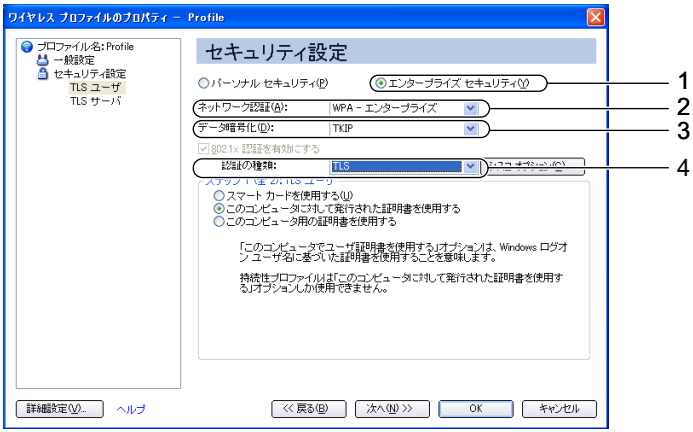
8 セキュリティを設定します。

■ IEEE 802.1X の場合



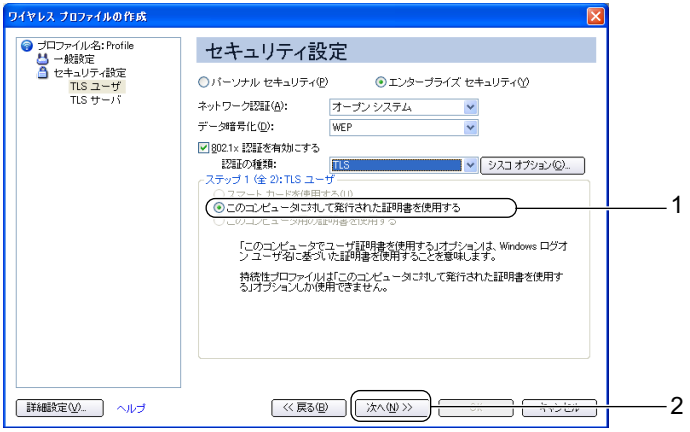
1. 「エンタープライズ セキュリティ」の◯をクリックして◉にします。
2. 「ネットワーク認証」の⌄をクリックし、「オープン システム」を選択します。
3. 「データ暗号化」の⌄をクリックし、「WEP」を選択します。
4. 「802.1x 認証を有効にする」の☐をクリックして☑にします。
5. 「認証の種類」の⌄をクリックして、「TLS」を選択します。

■ WPA ／ WPA2 の場合



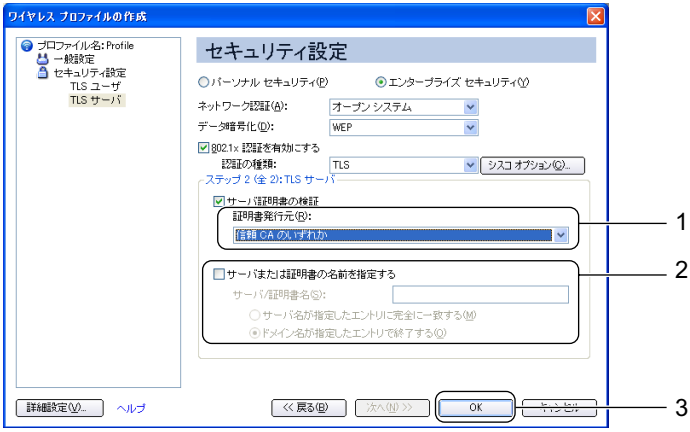
1. 「エンタープライズ セキュリティ」の○をクリックして◉にします。
2. 「ネットワーク認証」の > をクリックし、「WPA - エンタープライズ」または「WPA2 - エンタープライズ」を選択します。
   お使いになる環境、無線 LAN アクセスポイントに合わせて設定してください。
3. 「データ暗号化」の をクリックし、「TKIP」または、「AES - CCMP」を選択します。
   お使いになる環境、無線 LAN アクセスポイントに合わせて設定してください。
4. 「認証の種類」の をクリックして、「TLS」を選択します。

9 認証の設定（ステップ 1）をします。



1. 「このコンピュータ用の証明書を使用する」をクリックして◉にします。
2. 「次へ」をクリックします。

10 認証の設定（ステップ 2）をします。



1. 必要に応じて、「証明書発行元」の をクリックして使用する証明書の発行元を選択します。
2. サーバー／証明書を指定する場合は、「サーバまたは証明書の名前を指定する」の をクリックして にし、RADIUS サーバーに合わせて次のように設定します。
   サーバー名が、証明書のサーバー名と完全に一致する場合、「サーバ名が指定したエントリに完全に一致する」を にし、「サーバ／証明書名」にサーバー名を入力します。
   証明書にこのドメインまたは、このドメインのサブドメインに属するサーバー名が指定されている場合は、「ドメイン名が指定したエントリで終了」を にし、「サーバ／証明書名」にドメイン名を入力します。
3. 設定が終了したら、「OK」をクリックします。

「プロファイルウィザード」が終了し、「プロファイル」に作成したプロファイルが追加されます。

11 「ファイル」メニュー→「パッケージを保存する」の順にクリックします。

「名前を付けて保存」ウィンドウが表示されます。作成したプロファイルを実効ファイル形式で保存します。

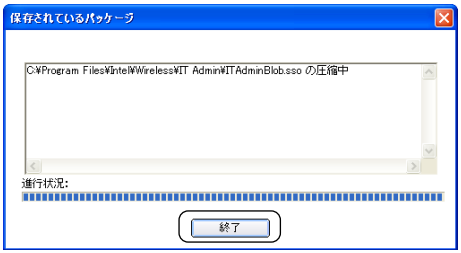
POINT

・管理者ツールで作成したパッケージを他のパソコンに適用することができます。

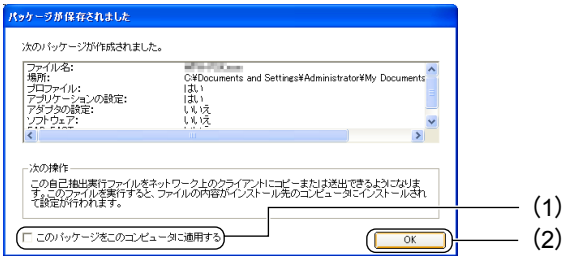
12 ファイル名を入力して「保存」をクリックします。

「保存されているパッケージ」ウィンドウが表示されます。

13 「終了」をクリックします。



14 **(1)「このパッケージをこのコンピュータに適用する」にチェックを入れ、(2)「OK」をクリックします。**



15 **「閉じる」をクリックします。**
作成したプロファイルが適用されます。

16 **「閉じる」をクリックします。**

ドメインログオン使用：IEEE 802.1X ＋ PEAP-MSCHAPv2 ／ WPA ＋ PEAP-MSCHAPv2 ／ WPA2 ＋ PEAP-MSCHAPv2

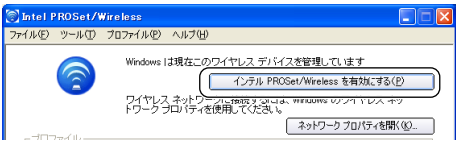
次のセキュリティパターンでドメインログオンをお使いになる場合の設定方法を説明します。

・IEEE 802.1X ＋ PEAP-MSCHAPv2
・WPA ＋ PEAP-MSCHAPv2
・WPA2 ＋ PEAP-MSCHAPv2

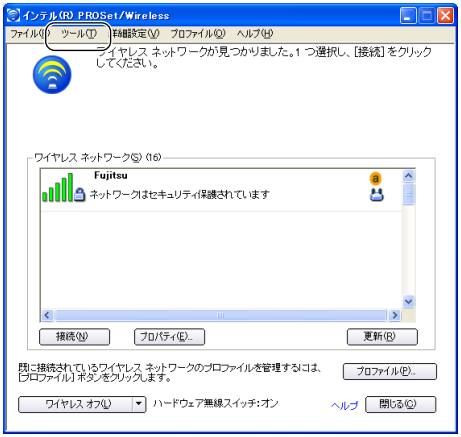
1 **「スタート」ボタン→「すべてのプログラム」→「Intel PROSet Wireless」→「Intel PROSet Wireless」の順にクリックします。**
「インテル (R) PROSet ／ Wireless」ウィンドウが表示されます。

POINT

・Windows XP 標準の無線 LAN 機能が有効になっている場合は、「インテル PROSet/Wireless を有効にする」をクリックしてください。



2 「ツール」メニュー→「管理ツール」の順にクリックします。



「パスワードの作成」ウィンドウが表示されます。

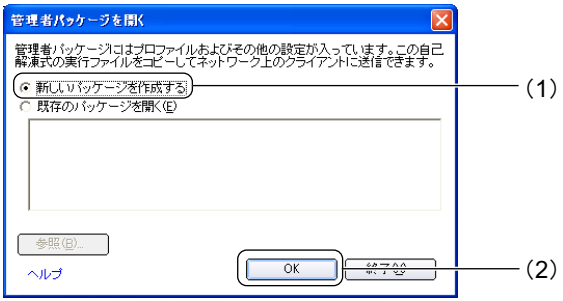
POINT

・ドメインログオンをする場合は、「管理ツール」で設定する必要があります。

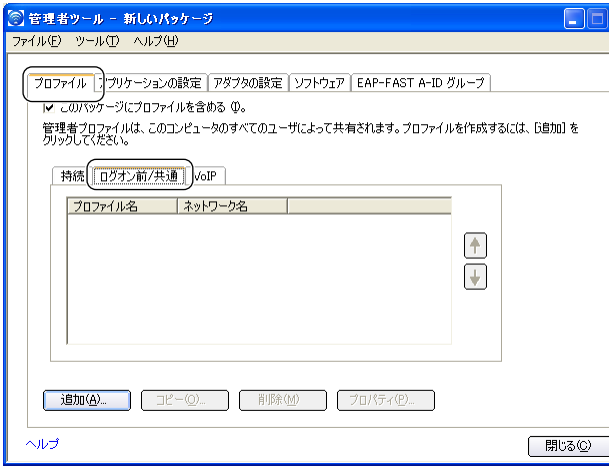
3 プロファイルを保護するためのパスワードを設定し、「OK」をクリックします。

「管理者パッケージを開く」ウィンドウが表示されます。

4 (1)「新しいパッケージを作成する」をクリックして●にし、(2)「OK」をクリックします。



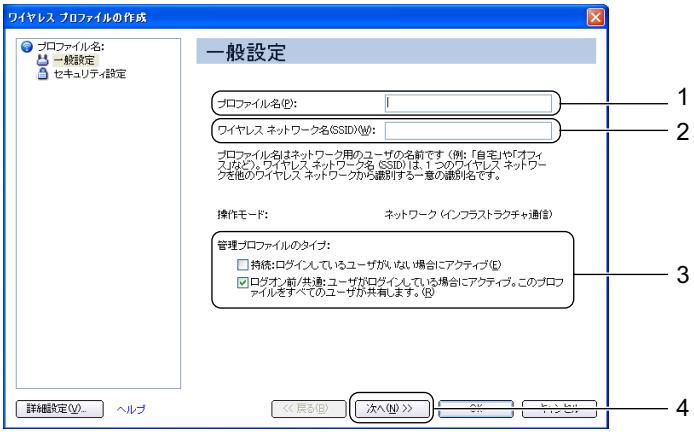
5 「プロファイル」タブの「ログオン前 / 共通」タブをクリックします。



6 「追加」をクリックします。

「ワイヤレスプロファイルの作成」ウィザードが表示されます。

7 無線 LAN のネットワークへ接続するための情報を設定します。次のように設定します。



1. 「プロファイル名」を入力します。
   設定するパラメータ情報を保存するプロファイルの名前を入力します。半角英数字、および日本語（全角文字）32 文字以内で入力できます。
2. 「ワイヤレスネットワーク名（SSID）」を入力します。
   お使いになる環境に合わせてネットワーク名を入力します。ネットワーク名は、半角英数字 32 文字以内で入力してください。
3. 「管理プロファイルのタイプ」を設定します。
   ・持続

「持続」を☑にすると、起動時およびコンピューターにログオンしているユーザーがいない場合でも、プロファイルが有効になります。この場合は認証情報を保存する必要があります。

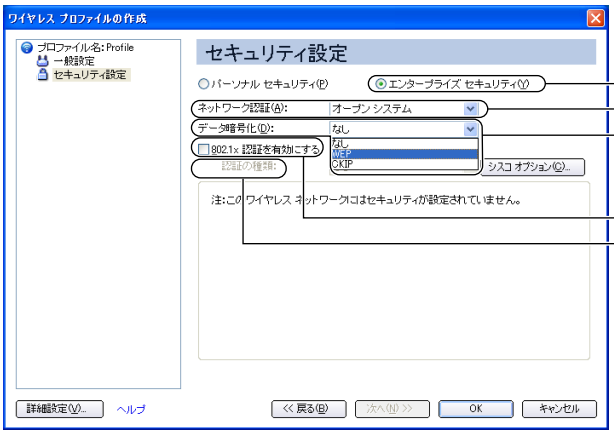
・ログオン前 / 共通

「ログオン前 / 共通」を☑にすると、ユーザーがコンピューターにログオンすると同時に接続が行われます。

4. 設定が終わったら「次へ」をクリックします。

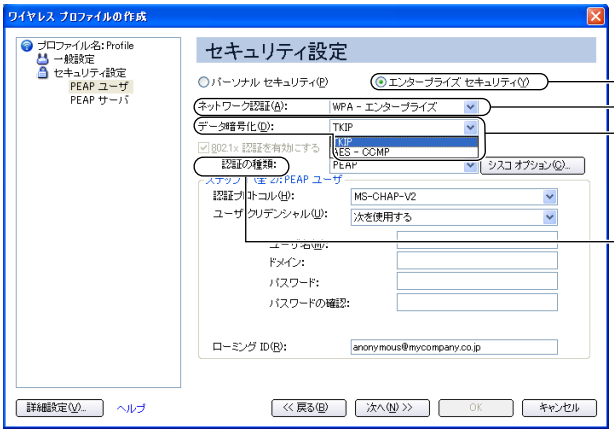
8 セキュリティを設定します。

■ IEEE 802.1X の場合



1. 「エンタープライズ セキュリティ」の◯をクリックして◉にします。
2. 「ネットワーク認証」の⌄をクリックし、「オープン システム」を選択します。
3. 「データ暗号化」の⌄をクリックし、「WEP」を選択します。
4. 「802.1x 認証を有効にする」の☐をクリックして☑にします。
5. 「認証の種類」の⌄をクリックして、「PEAP」を選択します。

■ WPA ／ WPA2 の場合



1. 「エンタープライズ セキュリティ」の○をクリックして◉にします。
2. 「ネットワーク認証」の▼をクリックし、「WPA - エンタープライズ」または「WPA2 - エンタープライズ」を選択します。
   お使いになる環境、無線 LAN アクセスポイントに合わせて設定してください。
3. 「データ暗号化」の▼をクリックし、「TKIP」または、「AES - CCMP」を選択します。
   お使いになる環境、無線 LAN アクセスポイントに合わせて設定してください。
4. 「認証の種類」の▼をクリックして、「PEAP」を選択します。

9 認証の設定（ステップ 1）を行います。

1. 「認証プロトコル」の▼をクリックして、「MS-CHAP-V2」を選択します。
2. 「ユーザクリデンシャル」を選択します。
   - 接続のたびに認証情報を入力する場合は、▼をクリックして「接続するたびにプロンプトを表示する」を選択します。
   - シングルサインオンを使用する場合は、▼をクリックして「Windows ログオンを使用する」を選択します。
   - 認証情報を保存する場合は、▼をクリックして「次を使用する」を選択し、次のように入力します。

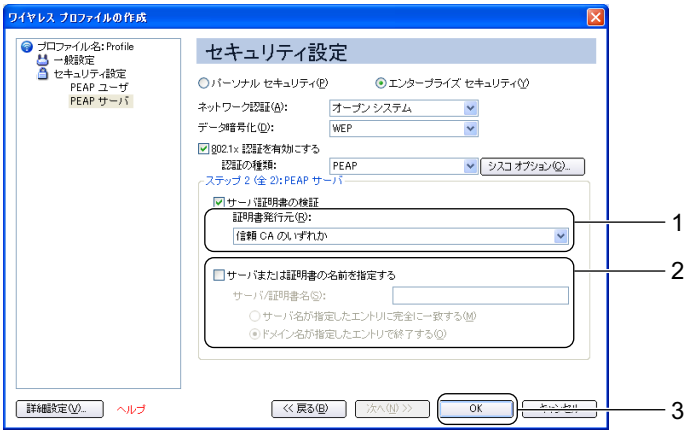
     手順 7 の「管理プロファイルのタイプ」で「持続」を☑にした場合は、この設定だけが選択できます。

表：「次を使用する」を選択した場合の設定

項目	説明
ユーザ名	認証に使用するユーザー名を入力します。
ドメイン	ドメインに参加しているネットワークに接続する場合は、RADIUS サーバーのドメイン名を入力します。
パスワード	認証に使用するユーザーのパスワードを入力します。
パスワードの確認	確認のため、「パスワード」と同じ値を入力します。

3.「ローミング ID」に、認証に使用するユーザー名を入力します。
4.「次へ」をクリックします。

10 認証の設定（ステップ 2）をします。



1.「証明書発行元」の をクリックして、使用する証明書の発行元を選択します。
2. サーバー／証明書を指定する場合は、「サーバまたは証明書の名前を指定する」の をクリックして にし、RADIUS サーバーに合わせて次のように設定します。
   サーバー名が、証明書のサーバー名と完全に一致する場合、「サーバ名が指定したエントリに完全に一致する」を にし、「サーバ／証明書名」にサーバー名を入力します。
   証明書にこのドメインまたは、このドメインのサブドメインに属するサーバー名が指定されている場合は、「ドメイン名が指定したエントリで終了」を にし、「サーバ／証明書名」にドメイン名を入力します。
3. 設定が終了したら、「OK」をクリックします。

「プロファイルウィザード」が終了し、「プロファイル」に作成したプロファイルが追加されます。

11 「ファイル」メニュー→「パッケージを保存する」の順にクリックします。

「名前を付けて保存」ウィンドウが表示されます。作成したプロファイルを実効ファイル形式で保存します。

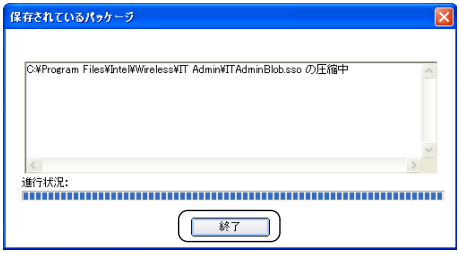
POINT

・管理者ツールで作成したパッケージを他のパソコンに適用することができます。

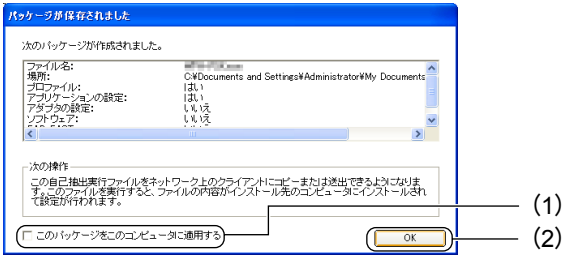
12 ファイル名を入力して「保存」をクリックします。

「保存されているパッケージ」ウィンドウが表示されます。

13 **「終了」をクリックします。**



14 **(1)「このパッケージをこのコンピュータに適用する」にチェックを入れ、(2)「OK」をクリックします。**



15 **「閉じる」をクリックします。**
作成したプロファイルが適用されます。

16 **「閉じる」をクリックします。**

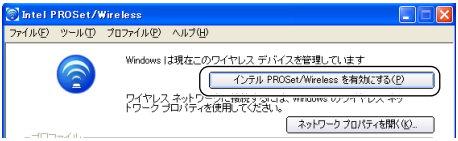
ドメインログオン使用：WPA-PSK ／ WPA2-PSK

WPA-PSK ／ WPA2-PSK でドメインログオンをお使いになる場合の設定方法を説明します。

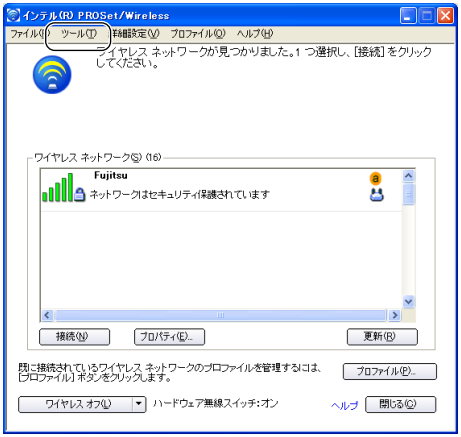
1 **「スタート」ボタン→「すべてのプログラム」→「Intel PROSet Wireless」→「Intel PROSet Wireless」の順にクリックします。**
「インテル (R) PROSet ／ Wireless」ウィンドウが表示されます。

POINT

・Windows XP 標準の無線 LAN 機能が有効になっている場合は、「インテル PROSet/Wireless を有効にする」をクリックしてください。



2 「ツール」メニュー→「管理ツール」の順にクリックします。



「パスワードの作成」ウィンドウが表示されます。

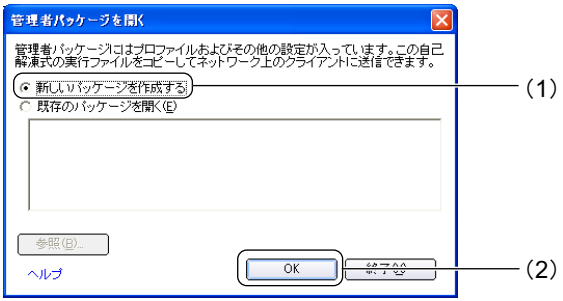
POINT

・ドメインログオンをする場合は、「管理ツール」で設定する必要があります。

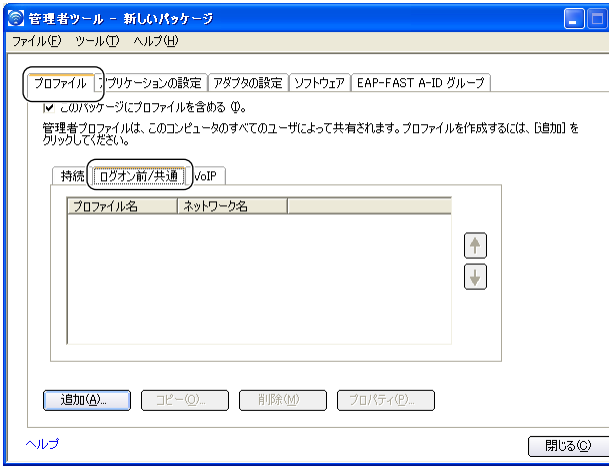
3 プロファイルを保護するためのパスワードを設定し、「OK」をクリックします。

「管理者パッケージを開く」ウィンドウが表示されます。

4 (1)「新しいパッケージを作成する」をクリックして●にし、(2)「OK」をクリックします。



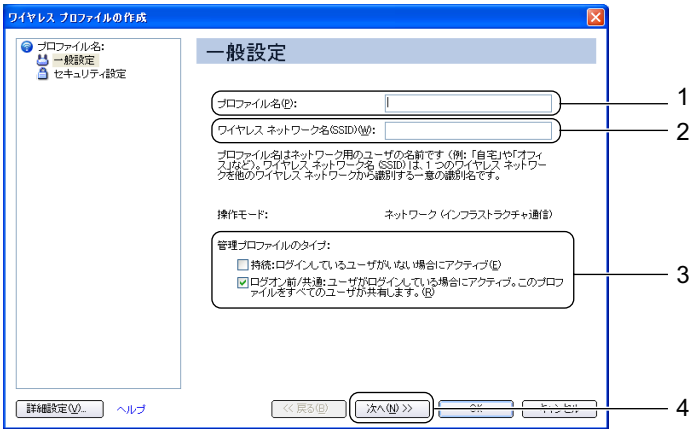
5 「プロファイル」タブの「ログオン前 / 共通」タブをクリックします。



6 「追加」をクリックします。

「ワイヤレスプロファイルの作成」ウィザードが表示されます。

7 無線 LAN のネットワークへ接続するための情報を設定します。次のように設定します。



1. 「プロファイル名」を入力します。
   設定するパラメータ情報を保存するプロファイルの名前を入力します。半角英数字、および日本語（全角文字）32 文字以内で入力できます。
2. 「ワイヤレスネットワーク名（SSID）」を入力します。
   お使いになる環境に合わせてネットワーク名を入力します。ネットワーク名は、半角英数字 32 文字以内で入力してください。
3. 「管理プロファイルのタイプ」を設定します。
   ・持続

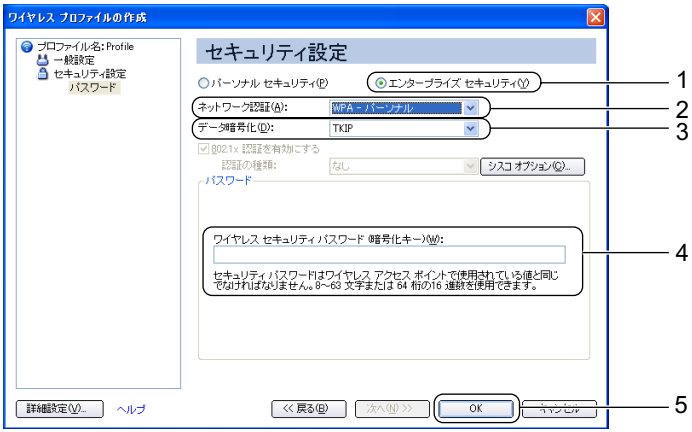
「持続」を☑にすると、起動時およびコンピューターにログオンしているユーザーがいない場合でも、プロファイルが有効になります。

・ログオン前 / 共通

「ログオン前 / 共通」を☑にすると、ユーザーがコンピューターにログオンすると同時に接続が行われます。

4. 設定が終わったら「次へ」をクリックします。

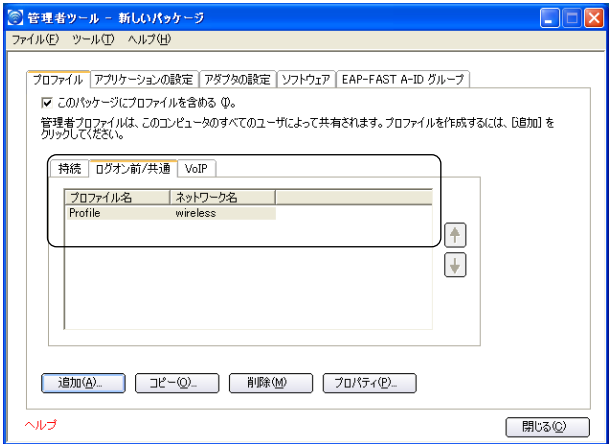
8 セキュリティの設定をします。次のように設定します。



1. 「エンタープライズ セキュリティ」の◯をクリックして◉にします。
2. 「ネットワーク認証」の⌄をクリックし、「WPA - パーソナル」または「WPA2 - パーソナル」を選択します。
   お使いになる環境、無線 LAN アクセスポイントに合わせて設定してください。
3. 「データ暗号化」を選択します。
   お使いになる環境、無線 LAN アクセスポイントに合わせて設定してください。
4. お使いになる接続方法に合わせて「ワイヤレスセキュリティパスワード（暗号化キー）」を入力します。
   パスフレーズまたは 16 進数で入力します。お使いになる環境、無線 LAN アクセスポイントに合わせて設定してください。

5. 設定が終了したら、「OK」をクリックします。

「ワイヤレス プロファイルの作成」ウィザードが終了し、「ログオン前 / 共通」に作成したプロファイルが追加されます。



9 **「ファイル」メニュー→「パッケージを保存する」の順にクリックします。**

「名前を付けて保存」ウィンドウが表示されます。作成したプロファイルを実効ファイル形式で保存します。

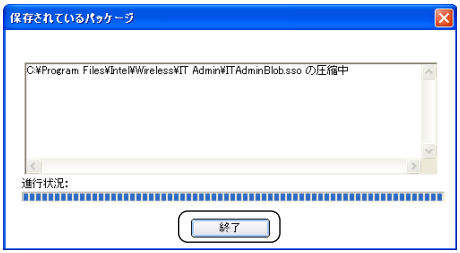
POINT

・管理者ツールで作成したパッケージを他のパソコンに適用することができます。

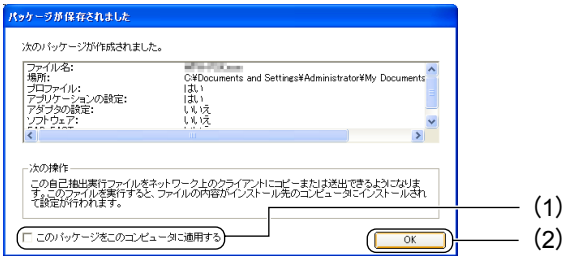
10 **ファイル名を入力して「保存」をクリックします。**

「保存されているパッケージ」ウィンドウが表示されます。

11 **「終了」をクリックします。**



12 **(1)「このパッケージをこのコンピュータに適用する」にチェックを入れ、(2)「OK」をクリックします。**



13 **「閉じる」をクリックします。**
作成したプロファイルが適用されます。

14 **「閉じる」をクリックします。**

7 Intel 無線 LAN 搭載モデル v9.x 系の設定

クライアントのパソコンが、Intel 無線 LAN 搭載モデル v9.x 系の場合の設定方法を説明します。

重要

シングルサインオン／ドメインログオンを使用する場合

プログラムの追加が必要です。追加方法については、「シングルサインオン／ドメインログオンを使用する場合のプログラムの追加」（→ P.175）をご覧ください。

シングルサインオン／ドメインログオンを使用する場合のプログラムの追加

シングルサインオンやドメインログオンを使用する場合は、次の手順に従って、プログラムを追加してください。

1. **「スタート」ボタン→「コントロールパネル」または、「スタート」ボタン→「設定」→「コントロールパネル」の順にクリックします。**
   「コントロールパネル」ウィンドウが表示されます。
2. **Windows XP の場合は「プログラムの追加と削除」、Windows 2000 の場合は「アプリケーションの追加と削除」をクリックします。**
3. **「現在インストールされているプログラム」の一覧から、「Intel(R) PROSet/Wireless Software」を選択し、「変更と削除」をクリックします。**
   「インテル (R) PROSet/Wireless インストーラ」ウィンドウが表示されます。

4 (1)「変更」を◉にして、(2)「次へ」をクリックします。

5 「シングルサインオン」の✕▾をクリックし、表示されるメニューから「この機能と、すべてのサブ機能をインストールする」を選択します。

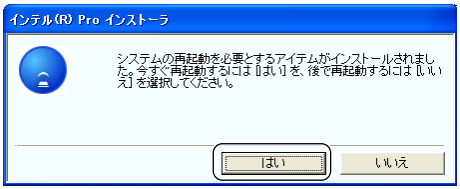
6 「管理ツール」の✕▾をクリックし、表示されるメニューから「この機能と、すべてのサブ機能をインストールする」を選択します。

7 **「編集」をクリックします。**
追加するプログラムがインストールされます。

8 **「インテル (R) PROSet/Wireless インストーラ」ウィンドウで「コンポーネントの変更を完了しました。」と表示されたら、次のように操作します。**

1. 「シングルサインオン」、「ログオン前接続」、「管理ツール」に ✔ がついていることを確認します。
2. 「OK」をクリックします。

9 **システムの再起動について確認のメッセージが表示されたら、「はい」をクリックして、パソコンを再起動します。**



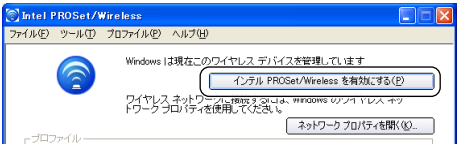
IEEE 802.1X ＋ EAP-TLS ／ WPA ＋ EAP-TLS ／ WPA2 ＋ EAP-TLS

次のセキュリティパターンの場合の設定方法を説明します。
・IEEE 802.1X ＋ EAP-TLS
・WPA ＋ EAP-TLS
・WPA2 ＋ EAP-TLS

1 **「スタート」ボタン→「すべてのプログラム」（「プログラム」）→「Intel PROSet Wireless」→「Intel PROSet Wireless」の順にクリックします。**
「Intel PROSet ／ Wireless」ウィンドウが表示されます。

POINT

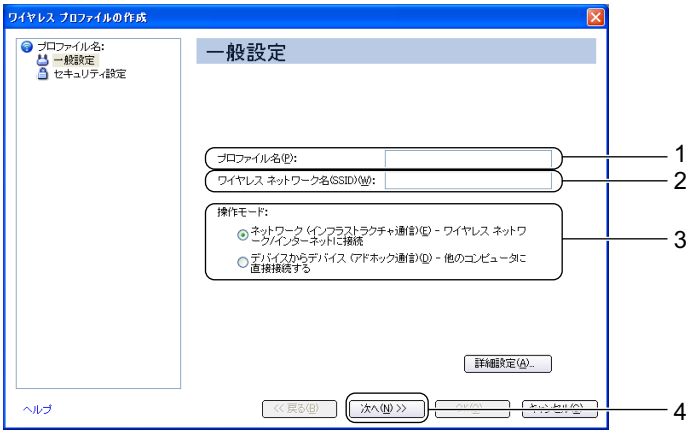
・OS が Windows XP の場合、Wireless Zero Configuration が有効になっていると次のような画面が表示されます。この場合は、「インテル PROSet/Wireless を有効にする」をクリックしてください。



2 「追加」をクリックします。

「ワイヤレスプロファイルの作成」ウィンドウが表示されます。

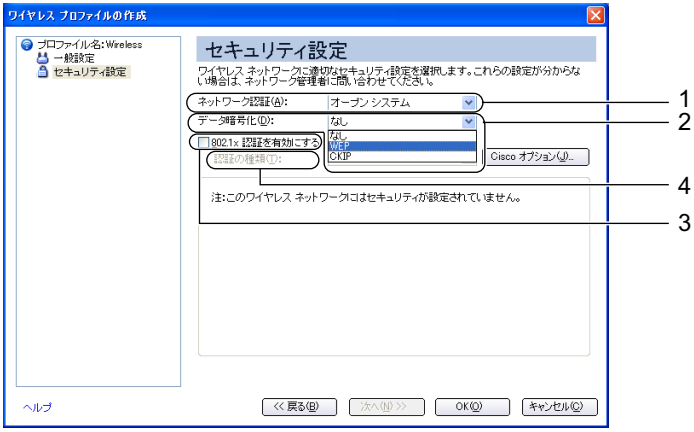
3 無線 LAN のネットワークへ接続するための情報を設定します。次のように設定します。



1. 「プロファイル名」を入力します。
   設定するパラメータ情報を保存するプロファイルの名前を入力します。半角英数字、および日本語（全角文字）32 文字以内で入力できます。空白文字は使用できません。
2. 「ワイヤレスネットワーク名（SSID）」を入力します。
3. 「操作モード」の「ネットワーク（インフラストラクチャ通信）」をクリックして◉にします。
4. 設定が終わったら「次へ」をクリックします。

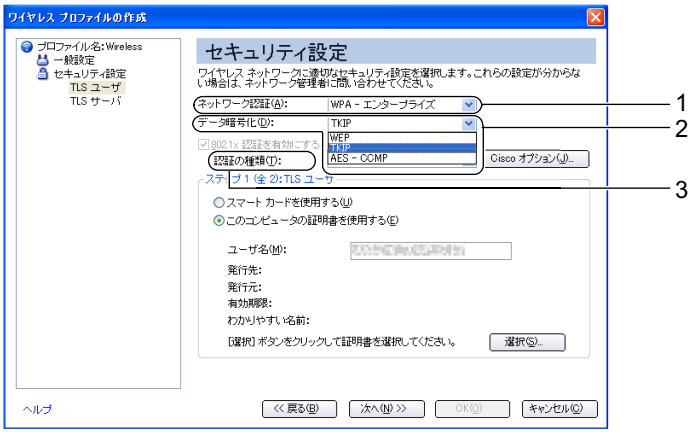
4 セキュリティの設定をします。次のように設定します。

■ IEEE 802.1X の場合



1. 「ネットワーク認証」の ▼ をクリックし、「オープン システム」を選択します。
2. 「データ暗号化」の ▼ をクリックし、「WEP」を選択します。
3. 「802.1x 認証を有効にする」の ☐ をクリックして ☑ にします。
4. 「認証の種類」の ▼ をクリックして、「TLS」を選択します。

■ WPA ／ WPA2 の場合

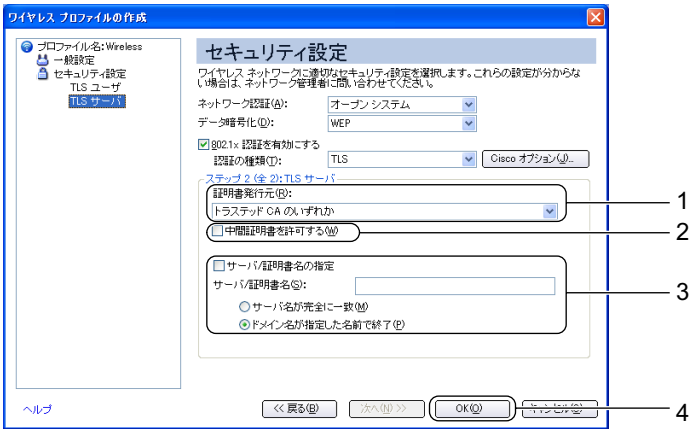


1. 「ネットワーク認証」の をクリックし、「WPA - エンタープライズ」または「WPA2 - エンタープライズ」を選択します。
   無線 LAN アクセスポイントに合わせて設定してください。
2. 「データ暗号化」の をクリックし、「TKIP」または、「AES - CCMP」を選択します。
   無線 LAN アクセスポイントに合わせて設定してください。
3. 「認証の種類」の をクリックして、「TLS」を選択します。

5 認証の設定（ステップ 1）を行います。

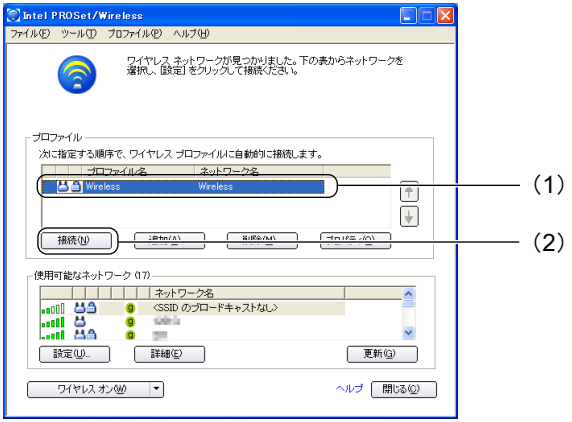
1. 「このコンピュータの証明書を使用する」をクリックして にします。
2. 「選択」をクリックし、使用する証明書を選択します。
3. 「ユーザ名」に、認証に使用するユーザー名を入力します。
4. 「次へ」をクリックします。

6 認証の設定（ステップ 2）を行います。



1. 「証明書発行元」の をクリックして、使用する証明書の発行元を選択します。
2. 「中間証明書を許可する」を設定します。
   証明機関から直接クライアント証明書を発行した場合は、 にします。
   中間証明機関の 1 つから発行された場合は、 にします。
3. サーバ／証明書を指定する場合は、「サーバ／証明書名の指定」の をクリックして にし、RADIUS サーバーに合わせて次のように設定します。
   サーバー名が、証明書のサーバー名と完全に一致する場合、「サーバ名が完全に一致」を にし、「サーバ／証明書名」にサーバー名を入力します。
   証明書にこのドメインまたは、このドメインのサブドメインに属するサーバー名が指定されている場合は、「ドメイン名が指定した名前で終了」を にし、「サーバ／証明書名」にドメイン名を入力します。
4. 設定が終了したら、「OK」をクリックします。

7 (1)「プロファイル」のリストから作成したプロファイルを選択し、(2)「接続」をクリックします。



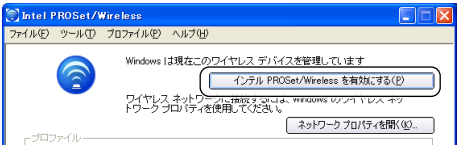
IEEE 802.1X ＋ PEAP-MSCHAPv2 ／ WPA ＋ PEAP-MSCHAPv2 ／ WPA2 ＋ PEAP-MSCHAPv2

次のセキュリティパターンの場合の設定方法を説明します。
- IEEE 802.1X ＋ PEAP-MSCHAPv2
- WPA ＋ PEAP-MSCHAPv2
- WPA2 ＋ PEAP-MSCHAPv2

1 「スタート」ボタン→「すべてのプログラム」(「プログラム」) →「Intel PROSet Wireless」→「Intel PROSet Wireless」の順にクリックします。
「Intel PROSet ／ Wireless」ウィンドウが表示されます。

POINT

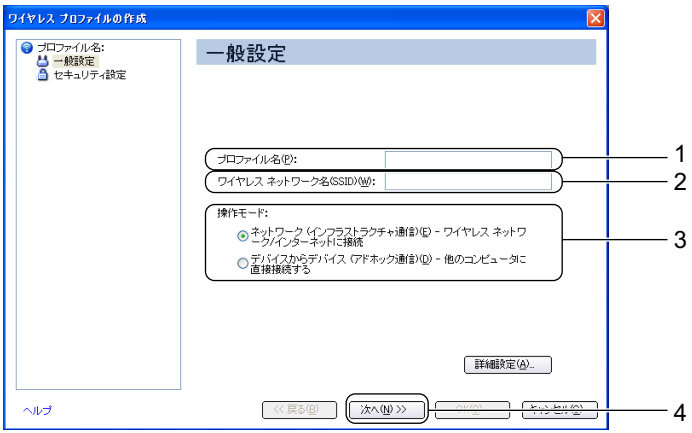
・OS が Windows XP の場合、Wireless Zero Configuration が有効になっていると次のような画面が表示されます。この場合は、「インテル PROSet/Wireless を有効にする」をクリックしてください。



2 「追加」をクリックします。

「ワイヤレスプロファイルの作成」ウィンドウが表示されます。

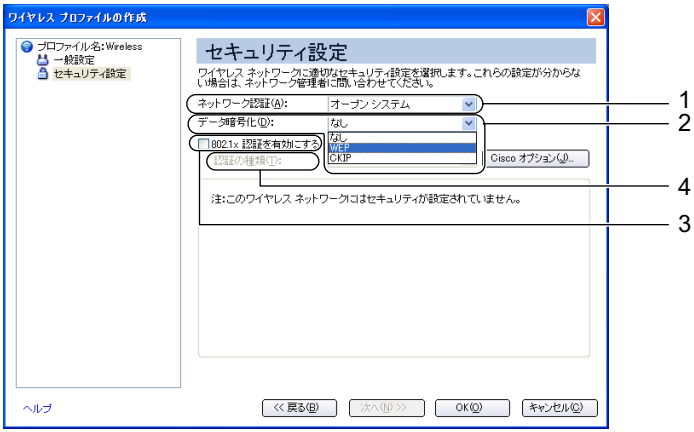
3 無線 LAN のネットワークへ接続するための情報を設定します。次のように設定します。



1. 「プロファイル名」を入力します。
   設定するパラメータ情報を保存するプロファイルの名前を入力します。半角英数字、および日本語（全角文字）32 文字以内で入力できます。空白文字は使用できません。
2. 「ワイヤレスネットワーク名（SSID）」を、半角英数字 32 文字以内で入力します。
3. 「操作モード」の「ネットワーク（インフラストラクチャ通信）」をクリックして◉にします。
4. 設定が終わったら「次へ」をクリックします。

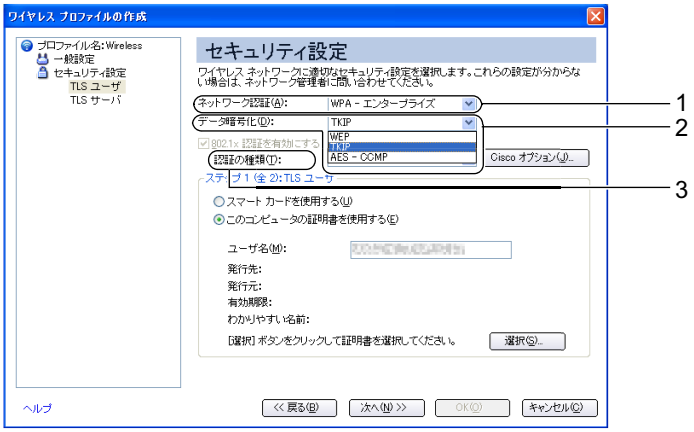
4 セキュリティの設定をします。次のように設定します。

■ IEEE 802.1X の場合



1. 「ネットワーク認証」の▼をクリックし、「オープン システム」を選択します。
2. 「データ暗号化」の▼をクリックし、「WEP」を選択します。
3. 「802.1x 認証を有効にする」の☐をクリックして☑にします。
4. 「認証の種類」の▼をクリックして、「PEAP」を選択します。

■ WPA ／ WPA2 の場合



1. 「ネットワーク認証」の をクリックし、「WPA - エンタープライズ」または「WPA2 - エンタープライズ」を選択します。
   無線 LAN アクセスポイントに合わせて設定してください。
2. 「データ暗号化」の をクリックし、「TKIP」または、「AES - CCMP」を選択します。
   無線 LAN アクセスポイントの設定に合わせて設定してください。
3. 「認証の種類」の をクリックして、「PEAP」を選択します。

5 認証の設定（ステップ 1）を行います。

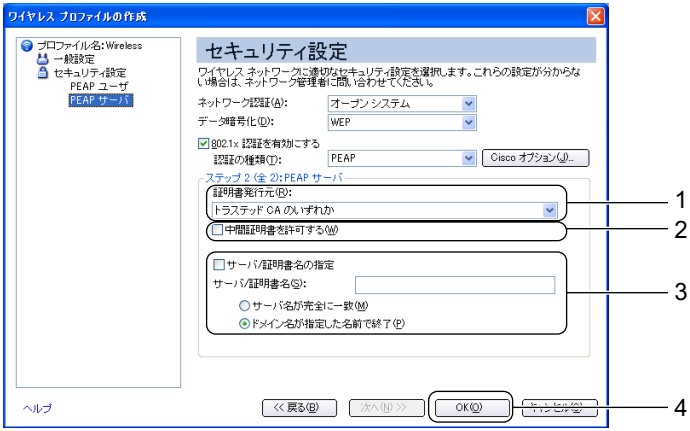
1. 「認証プロトコル」の をクリックして、「MS-CHAP-V2」を選択します。
2. 「ユーザクリデンシャル」を選択します。
   - 接続のたびに認証情報を入力する場合は、 をクリックして「接続するたびにプロンプトを表示する」を選択します。
   - シングルサインオンを使用する場合は、 をクリックして「Windows ログオンを使用する」を選択します。
     シングルサインオンを使用する場合は、プログラムを追加する必要があります。
     プログラムの追加方法については、「シングルサインオン／ドメインログオンを使用する場合のプログラムの追加」（→ P.175）をご覧ください。
   - 認証情報を保存する場合は、 をクリックして「次を使用する」を選択し、次のように入力します。

表：「次を使用する」を選択した場合の設定

項目	説明
ユーザ名	認証に使用するユーザー名を入力します。
ドメイン	ドメインに参加しているネットワークに接続する場合は、RADIUS サーバーのドメイン名を入力します。
パスワード	認証に使用するユーザーのパスワードを入力します。
パスワードの確認	確認のため、「パスワード」と同じ値を入力します。

3. クライアント証明書を使用する場合は、「このワイヤレスネットワークでクライアント証明書を使用する」を☐から☑にして、「選択」をクリックして使用する証明書を選択します。
4. 「ローミング ID」に、認証に使用するユーザー名を入力します。
5. 「次へ」をクリックします。

6 認証の設定（ステップ 2）を行います。



1. 「証明書発行元」の⌄をクリックして、使用する証明書の発行元を選択します。
2. 「中間証明書を許可する」を設定します。

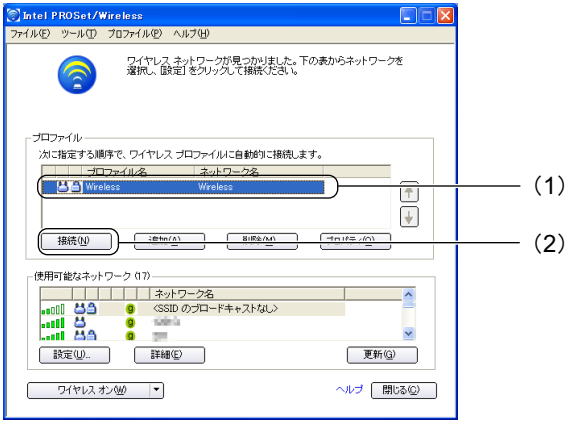
   証明機関から直接クライアント証明書を発行した場合は、☐にします。

   中間証明機関の 1 つから発行された場合は、☑にします。
3. サーバ／証明書を指定する場合は、「サーバ／証明書名の指定」の☐をクリックして☑にし、RADIUS サーバーに合わせて次のように設定します。

   サーバー名が、証明書のサーバー名と完全に一致する場合、「サーバ名が完全に一致」を◉にし、「サーバ／証明書名」にサーバー名を入力します。

   証明書にこのドメインまたは、このドメインのサブドメインに属するサーバー名が指定されている場合は、「ドメイン名が指定した名前で終了」を◉にし、「サーバ／証明書名」にドメイン名を入力します。
4. 設定が終了したら、「OK」をクリックします。

7 **(1)「プロファイル」のリストから作成したプロファイルを選択し、(2)「接続」をクリックします。**



IEEE 802.1X ＋ PEAP-TLS ／ WPA ＋ PEAP-TLS ／ WPA2 ＋ PEAP-TLS

次のセキュリティパターンの場合の設定方法を説明します。

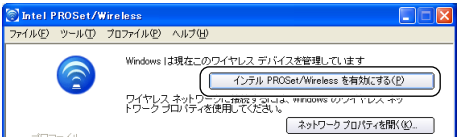
- IEEE 802.1X ＋ PEAP-TLS
- WPA ＋ PEAP-TLS
- WPA2 ＋ PEAP-TLS

1 **「スタート」ボタン→「すべてのプログラム」(「プログラム」)→「Intel PROSet Wireless」→「Intel PROSet Wireless」の順にクリックします。**

「Intel PROSet ／ Wireless」ウィンドウが表示されます。

POINT

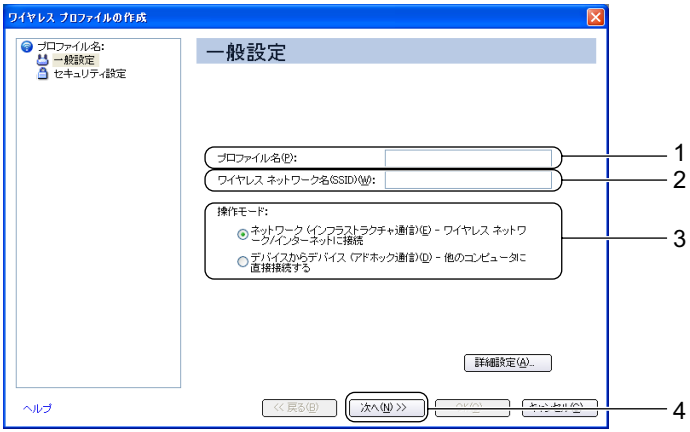
- OS が Windows XP の場合、Wireless Zero Configuration が有効になっていると次のような画面が表示されます。この場合は、「インテル PROSet/Wireless を有効にする」をクリックしてください。



2 「追加」をクリックします。

「ワイヤレスプロファイルの作成」ウィンドウが表示されます。

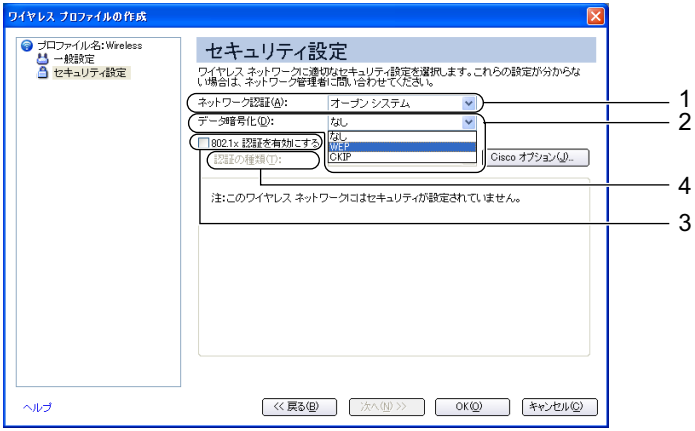
3 無線 LAN のネットワークへ接続するための情報を設定します。次のように設定します。



1. 「プロファイル名」を入力します。
   設定するパラメータ情報を保存するプロファイルの名前を入力します。半角英数字、および日本語（全角文字）32 文字以内で入力できます。空白文字は使用できません。
2. 「ワイヤレスネットワーク名（SSID）」を、半角英数字 32 文字以内で入力します。
3. 「操作モード」の「ネットワーク（インフラストラクチャ通信）」をクリックして◉にします。
4. 設定が終わったら「次へ」をクリックします。

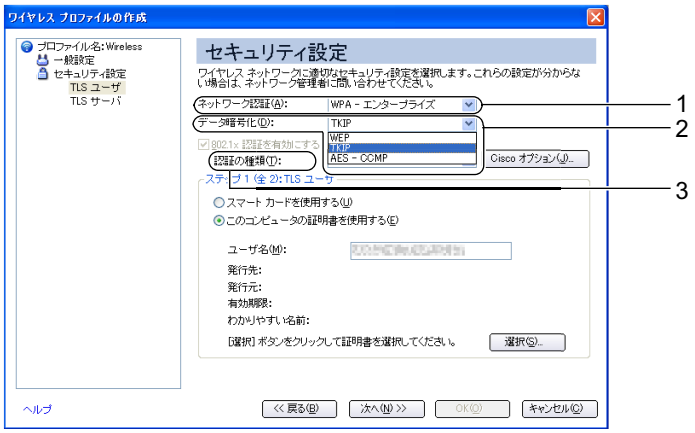
4 セキュリティの設定をします。次のように設定します。

■ IEEE 802.1X の場合



1. 「ネットワーク認証」の をクリックし、「オープン システム」を選択します。
2. 「データ暗号化」の をクリックし、「WEP」を選択します。
3. 「802.1x 認証を有効にする」の をクリックして にします。
4. 「認証の種類」の をクリックして、「PEAP」を選択します。

■ WPA ／ WPA2 の場合

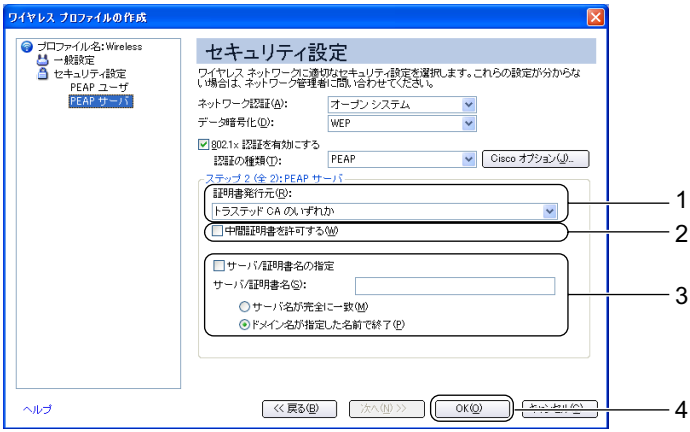


1. 「ネットワーク認証」の をクリックし、「WPA - エンタープライズ」または「WPA2 - エンタープライズ」を選択します。
   無線 LAN アクセスポイントに合わせて設定してください。
2. 「データ暗号化」の をクリックし、「TKIP」または、「AES - CCMP」を選択します。
   無線 LAN アクセスポイントの設定に合わせて設定してください。
3. 「認証の種類」の をクリックして、「PEAP」を選択します。

5 認証の設定（ステップ 1）を行います。

1. 「認証プロトコル」の をクリックして、「TLS」を選択します。
2. 「このコンピュータの証明書を使用する」をクリックして にします。
3. 「選択」をクリックし、使用する証明書を選択します。
4. 「ユーザ名」に、認証に使用するユーザー名を入力します。
5. 「次へ」をクリックします。

6 認証の設定（ステップ 2）を行います。



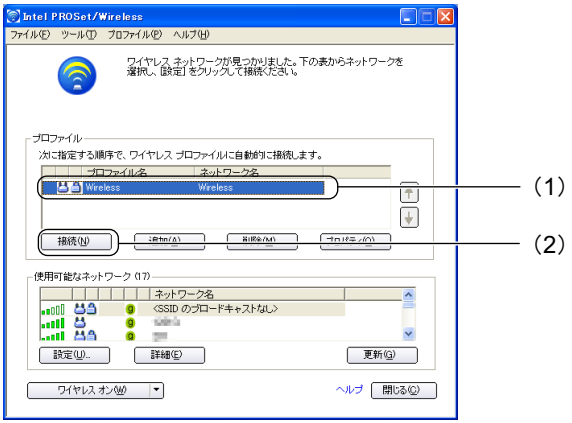
1. 「証明書発行元」の をクリックして、使用する証明書の発行元を選択します。
2. 「中間証明書を許可する」を設定します。

   証明機関から直接クライアント証明書を発行した場合は、 にします。

   中間証明機関の 1 つから発行された場合は、 にします。

3. サーバ／証明書を指定する場合は、「サーバ／証明書名の指定」の☐をクリックして☑にし、RADIUS サーバーに合わせて次のように設定します。
   サーバー名が、証明書のサーバー名と完全に一致する場合、「サーバ名が完全に一致」を◉にし、「サーバ／証明書名」にサーバー名を入力します。
   証明書にこのドメインまたは、このドメインのサブドメインに属するサーバー名が指定されている場合は、「ドメイン名が指定した名前で終了」を◉にし、「サーバ／証明書名」にドメイン名を入力します。
4. 設定が終了したら、「OK」をクリックします。

7 (1)「プロファイル」のリストから作成したプロファイルを選択し、(2)「接続」をクリックします。



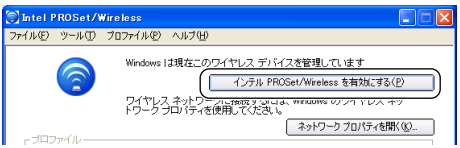
WPA-PSK ／ WPA2-PSK

WPA-PSK ／ WPA2-PSK の場合の設定方法を説明します。

1 「スタート」ボタン→「すべてのプログラム」(「プログラム」) →「Intel PROSet Wireless」→「Intel PROSet Wireless」の順にクリックします。
「Intel PROSet ／ Wireless」ウィンドウが表示されます。

POINT

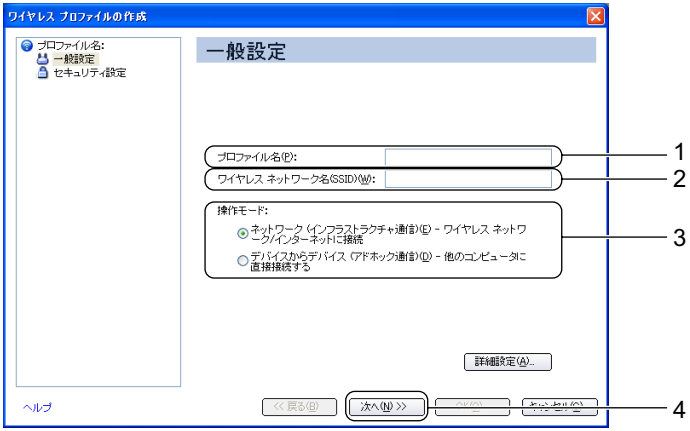
・OS が Windows XP の場合、Wireless Zero Configuration が有効になっていると次のような画面が表示されます。この場合は、「インテル PROSet/Wireless を有効にする」をクリックしてください。



2 「追加」をクリックします。

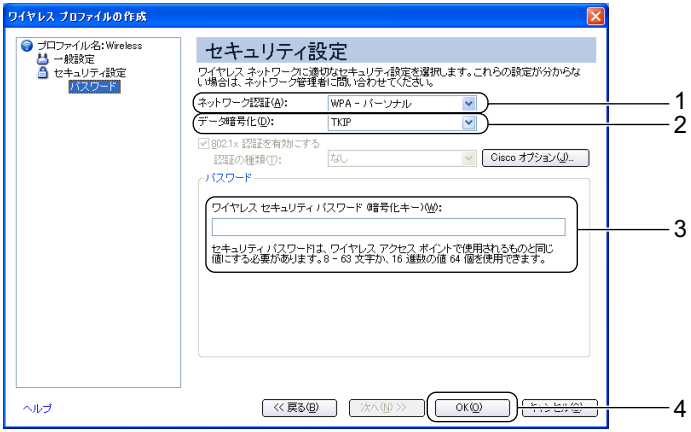
「ワイヤレスプロファイルの作成」ウィンドウが表示されます。

3 無線 LAN のネットワークへ接続するための情報を設定します。次のように設定します。



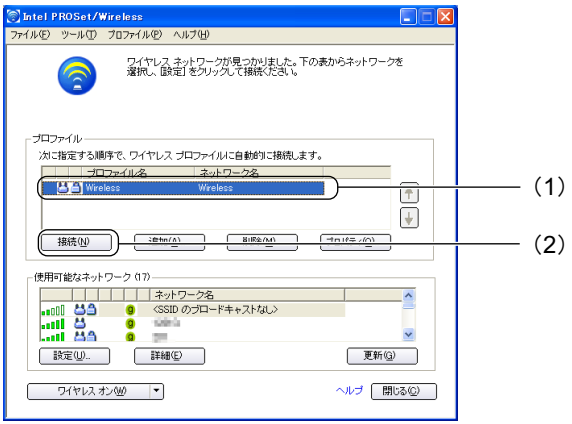
1. 「プロファイル名」を入力します。
   設定するパラメータ情報を保存するプロファイルの名前を入力します。半角英数字、および日本語（全角文字）32 文字以内で入力できます。空白文字は使用できません。
2. 「ワイヤレスネットワーク名（SSID）」を、半角英数字 32 文字以内で入力します。
3. 「操作モード」の「ネットワーク（インフラストラクチャ通信）」をクリックして◉にします。
4. 設定が終わったら「次へ」をクリックします。

4 セキュリティの設定をします。次のように設定します。



1. 「ネットワーク認証」の をクリックし、「WPA - パーソナル」または「WPA2 - パーソナル」を選択します。
   無線 LAN アクセスポイントに合わせて設定してください。
2. 「データ暗号化」の をクリックし、「TKIP」または、「AES - CCMP」を選択します。
   無線 LAN アクセスポイントの設定に合わせて設定してください。
3. 「ワイヤレスセキュリティパスワード」に WPA-PSK を入力します。
   パスフレーズまたは 16 進数で入力します。無線 LAN アクセスポイントの設定に合わせて設定してください。
4. 設定が終了したら、「OK」をクリックします。

5 (1)「プロファイル」のリストから作成したプロファイルを選択し、(2)「接続」をクリックします。



ドメインログオン使用：IEEE 802.1X ＋ PEAP-MSCHAPv2 ／ WPA ＋ PEAP-MSCHAPv2 ／ WPA2 ＋ PEAP-MSCHAPv2

次のセキュリティパターンでドメインログオンをお使いになる場合の設定方法を説明します。

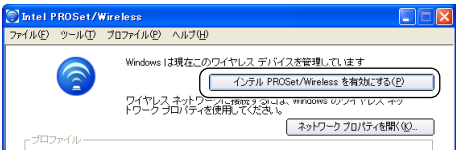
・IEEE 802.1X ＋ PEAP-MSCHAPv2
・WPA ＋ PEAP-MSCHAPv2
・WPA2 ＋ PEAP-MSCHAPv2

1 「スタート」ボタン→「すべてのプログラム」（「プログラム」）→「Intel PROSet Wireless」→「Intel PROSet Wireless」の順にクリックします。

「Intel PROSet ／ Wireless」ウィンドウが表示されます。

POINT

・OS が Windows XP の場合、Wireless Zero Configuration が有効になっていると次のような画面が表示されます。この場合は、「インテル PROSet/Wireless を有効にする」をクリックしてください。



2 「ツール」→「管理ツール」の順にクリックします。

「パスワードの作成」ウィンドウが表示されます。

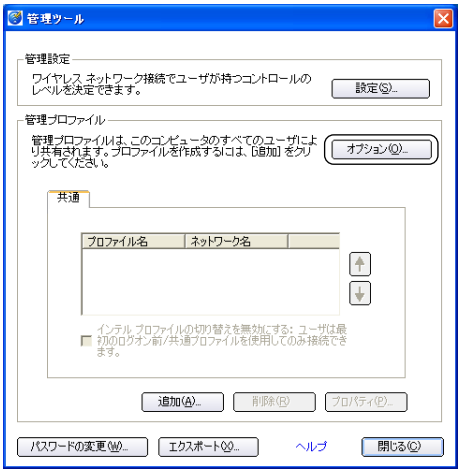
POINT

・ドメインログオンをする場合は、「管理ツール」で設定する必要があります。

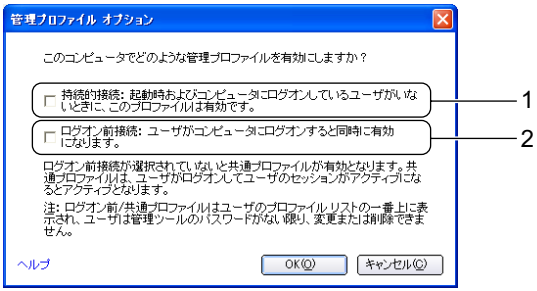
3 **プロファイルを保護するためのパスワードを設定し、「OK」をクリックします。**

「管理ツール」ウィンドウが表示されます。

4 **「オプション」をクリックします。**



5 **「管理プロファイル オプション」を設定し、「OK」をクリックします。**



1. **持続的接続**

   「持続的接続」を☑にすると、起動時およびコンピューターにログオンしているユーザーがいない場合でも、プロファイルが有効になります。

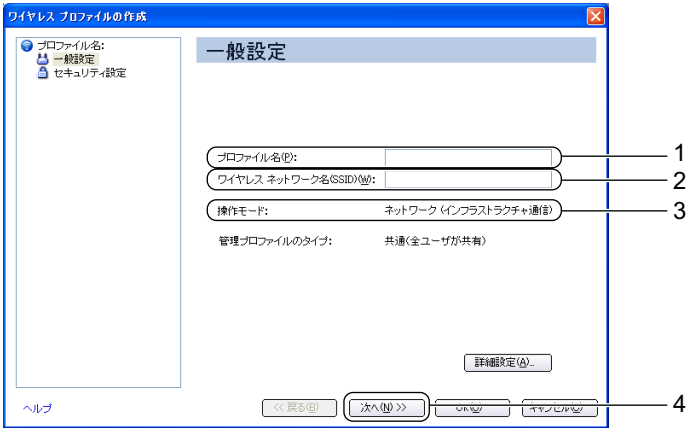
2. **ログオン前接続**

   「ログオン前接続」を☑にすると、ユーザーがコンピューターにログオンすると同時に接続が行われます。

6 **「管理ツール」ウィンドウで、「追加」をクリックします。**

「ワイヤレスプロファイルの作成」ウィンドウが表示されます。

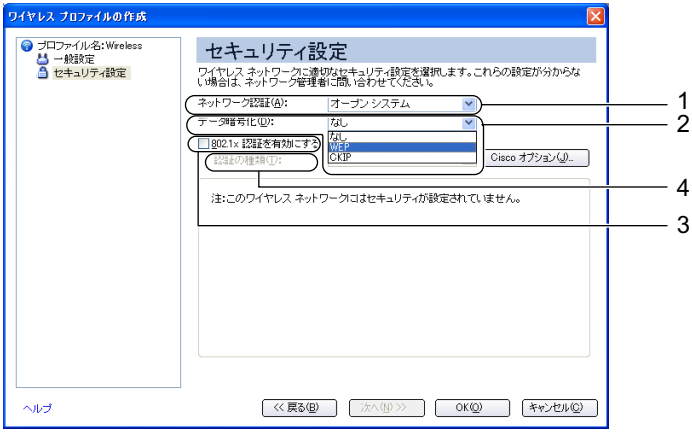
7 無線 LAN のネットワークへ接続するための情報を設定します。次のように設定します。



1. 「プロファイル名」を入力します。
   設定するパラメータ情報を保存するプロファイルの名前を入力します。半角英数字、および日本語（全角文字）32 文字以内で入力できます。空白文字は使用できません。
2. 「ワイヤレスネットワーク名（SSID）」を、半角英数字 32 文字以内で入力します。
3. 「操作モード」の「ネットワーク（インフラストラクチャ通信）」をクリックして◉にします。
4. 設定が終わったら「次へ」をクリックします。

8 セキュリティの設定をします。次のように設定します。

■ IEEE 802.1X の場合



1. 「ネットワーク認証」の ⌄ をクリックし、「オープン システム」を選択します。
2. 「データ暗号化」の ⌄ をクリックし、「WEP」を選択します。
3. 「802.1x 認証を有効にする」の☐をクリックして☑にします。

4.「認証の種類」の をクリックして、「PEAP」を選択します。

■ WPA ／ WPA2 の場合

1.「ネットワーク認証」の をクリックし、「WPA - エンタープライズ」または「WPA2 - エンタープライズ」を選択します。

無線 LAN アクセスポイントに合わせて設定してください。

2.「データ暗号化」の をクリックし、「TKIP」または、「AES - CCMP」を選択します。

無線 LAN アクセスポイントの設定に合わせて設定してください。

3.「認証の種類」の をクリックして、「PEAP」を選択します。

9 認証の設定（ステップ 1）を行います。

1. 「認証プロトコル」の をクリックして、「MS-CHAP-V2」を選択します。
2. 「ユーザクリデンシャル」を選択します。

   接続のたびに認証情報を入力する場合は、 をクリックして「接続するたびにプロンプトを表示する」を選択します。

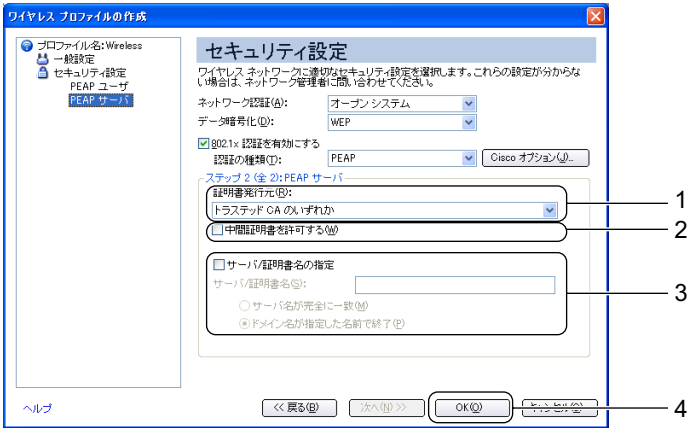
   認証情報を保存する場合は、 をクリックして「次を使用する」を選択し、次のように入力します。

表：「次を使用する」を選択した場合の設定

項目	説明
ユーザ名	認証に使用するユーザー名を入力します。
ドメイン	ドメインに参加しているネットワークに接続する場合は、RADIUS サーバーのドメイン名を入力します。
パスワード	認証に使用するユーザーのパスワードを入力します。
パスワードの確認	確認のため、「パスワード」と同じ値を入力します。

3. クライアント証明書を使用する場合は、「このワイヤレスネットワークでクライアント証明書を使用する」を から にし、「選択」をクリックして使用する証明書を選択します。
4. 「ローミング ID」に、認証に使用するユーザー名を入力します。
5. 「次へ」をクリックします。

10 認証の設定（ステップ 2）を行います。



1. 「証明書発行元」の をクリックして、使用する証明書の発行元を選択します。
2. 「中間証明書を許可する」を設定します。

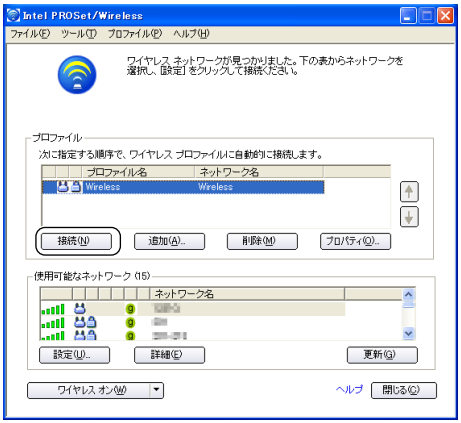
   証明機関から直接クライアント証明書を発行した場合は、 にします。

   中間証明機関の 1 つから発行された場合は、 にします。

3. サーバ／証明書を指定する場合は、「サーバ／証明書名の指定」の☐をクリックして☑にし、RADIUS サーバーに合わせて次のように設定します。
   サーバー名が、証明書のサーバー名と完全に一致する場合、「サーバ名が完全に一致」を◉にし、「サーバ／証明書名」にサーバー名を入力します。
   証明書にこのドメインまたは、このドメインのサブドメインに属するサーバー名が指定されている場合は、「ドメイン名が指定した名前で終了」を◉にし、「サーバ／証明書名」にドメイン名を入力します。
4. 設定が終了したら、「OK」をクリックします。

11 **「管理ツール」ウィンドウで「閉じる」をクリックします。**

12 **「Intel PROSet/Wireless」ウィンドウで「接続」をクリックします。**



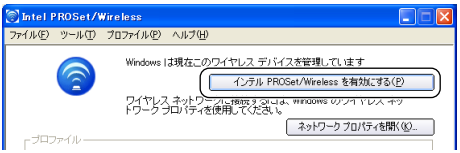
ドメインログオン使用：WPA-PSK ／ WPA2-PSK

WPA-PSK ／ WPA2-PSK でドメインログオンをお使いになる場合の設定方法を説明します。

1 **「スタート」ボタン→「すべてのプログラム」（「プログラム」）→「Intel PROSet Wireless」→「Intel PROSet Wireless」の順にクリックします。**
「Intel PROSet ／ Wireless」ウィンドウが表示されます。

POINT

・OS が Windows XP の場合、Wireless Zero Configuration が有効になっていると次のような画面が表示されます。この場合は、「インテル PROSet/Wireless を有効にする」をクリックしてください。



2 「ツール」→「管理ツール」の順にクリックします。

「パスワードの作成」ウィンドウが表示されます。

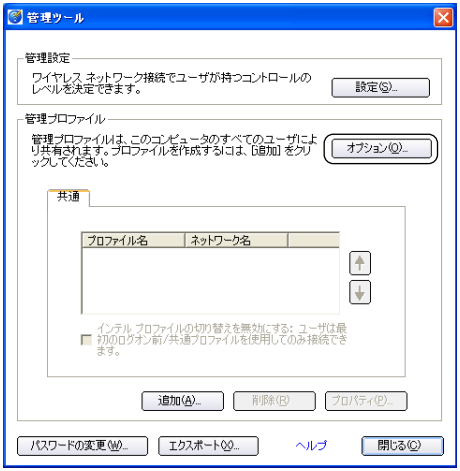
POINT

・ドメインログオンをする場合は、「管理ツール」で設定する必要があります。

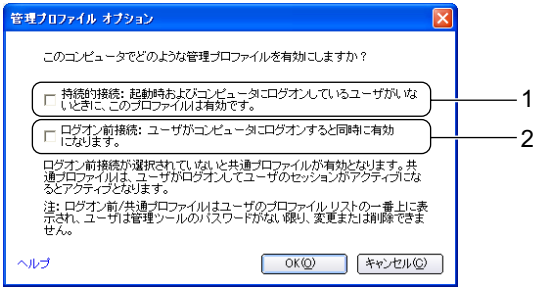
3 プロファイルを保護するためのパスワードを設定し、「OK」をクリックします。

「管理ツール」ウィンドウが表示されます。

4 「オプション」をクリックします。



5 「管理プロファイル オプション」を設定し、「OK」をクリックします。

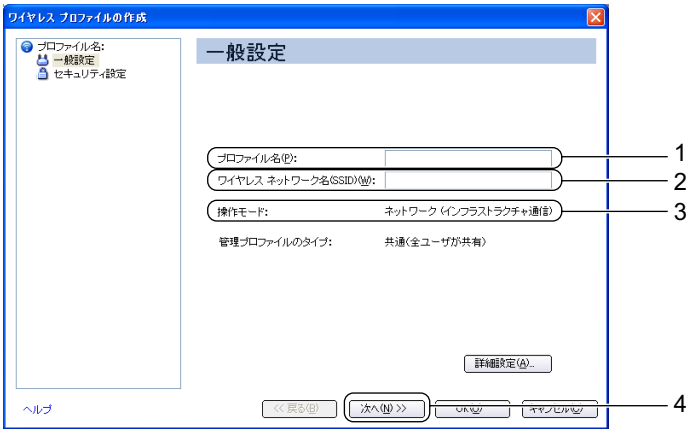


1. **持続的接続**
   「持続的接続」を☑にすると、起動時およびコンピューターにログオンしているユーザーがいない場合でも、プロファイルが有効になります。
2. **ログオン前接続**
   「ログオン前接続」を☑にすると、ユーザーがコンピューターにログオンすると同時に接続が行われます。

6 「管理ツール」ウィンドウで、「追加」をクリックします。

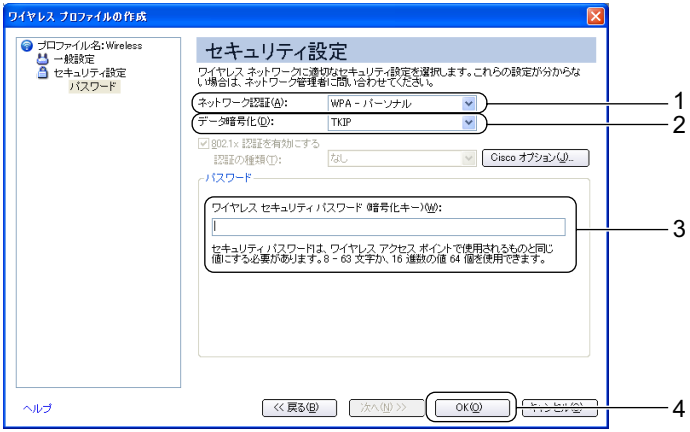
「ワイヤレスプロファイルの作成」ウィンドウが表示されます。

7 無線 LAN のネットワークへ接続するための情報を設定します。次のように設定します。



1. 「プロファイル名」を入力します。
   設定するパラメータ情報を保存するプロファイルの名前を入力します。半角英数字、および日本語（全角文字）32 文字以内で入力できます。空白文字は使用できません。
2. 「ワイヤレスネットワーク名（SSID）」を、半角英数字 32 文字以内で入力します。
3. 「操作モード」の「ネットワーク（インフラストラクチャ通信）」をクリックして◉にします。
4. 設定が終わったら「次へ」をクリックします。

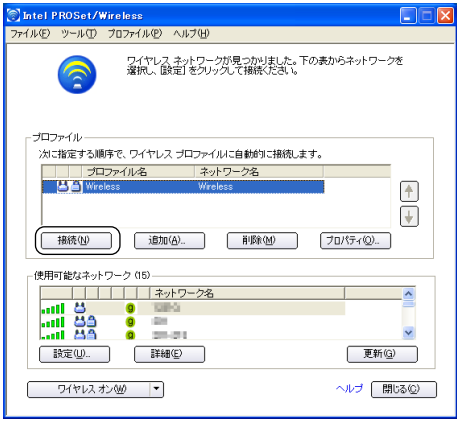
8 セキュリティの設定をします。次のように設定します。



1. 「ネットワーク認証」の をクリックし、「WPA - パーソナル」または「WPA2 - パーソナル」を選択します。
   無線 LAN アクセスポイントに合わせて設定してください。
2. 「データ暗号化」の をクリックし、「TKIP」または、「AES - CCMP」を選択します。
   無線 LAN アクセスポイントの設定に合わせて設定してください。
3. 「ワイヤレスセキュリティパスワード」に WPA-PSK を入力します。
   パスフレーズまたは 16 進数で入力します。無線 LAN アクセスポイントの設定に合わせて設定してください。
4. 設定が終了したら、「OK」をクリックします。

9 「管理ツール」ウィンドウで「閉じる」をクリックします。

10 「Intel PROSet/Wireless」ウィンドウで「接続」をクリックします。



8 Intel 無線 LAN 搭載モデル v8.x 系／v7.x 系の設定

クライアントのパソコンが、Intel 無線 LAN 搭載モデル v8.x 系または v7.x 系の場合の設定方法を説明します。

重要

シングルサインオン／ドメインログオンを使用する場合

プログラムの追加が必要です。追加方法については、「シングルサインオン／ドメインログオンを使用する場合のプログラムの追加」（→ P.202）をご覧ください。

Windows XP をお使いのお客様へ

ユーティリティで各種セキュリティ機能をお使いになる場合、Windows XP で提供される無線 LAN の機能を無効にする必要があります。

次の手順で Windows の機能を無効にしてください。

1. 「スタート」ボタン→「コントロールパネル」の順にクリックします。
2. 「ネットワークとインターネット接続」をクリックします。
3. 「ネットワーク接続」をクリックします。
   現在インストールされているネットワークの一覧が表示されます。
4. 一覧から「ワイヤレスネットワーク接続」を右クリックして、表示されるメニューから「プロパティ」をクリックします。
   「ワイヤレス ネットワーク接続のプロパティ」ウィンドウが表示されます。
5. 「ワイヤレス ネットワーク」タブをクリックします。
6. 「Windows を使ってワイヤレス ネットワークの設定を構成する」を☑から☐にし、「OK」をクリックします。
7. 「ネットワーク接続」ウィンドウの❌をクリックします。

シングルサインオン／ドメインログオンを使用する場合のプログラムの追加

シングルサインオンやドメインログオンを使用する場合は、次の手順に従って、プログラムを追加してください。

1 「スタート」ボタン→「コントロールパネル」または、「スタート」ボタン→「設定」→「コントロールパネル」の順にクリックします。

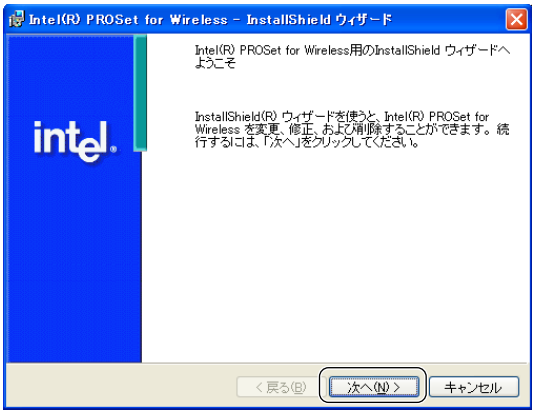
「コントロールパネル」ウィンドウが表示されます。

2 **Windows XP の場合は「プログラムの追加と削除」、Windows 2000 の場合は「アプリケーションの追加と削除」をクリックします。**

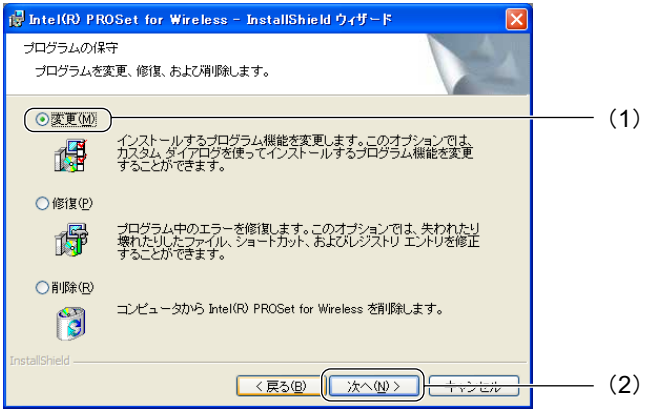
3 **「現在インストールされているプログラム」の一覧から、「Intel(R) PROSet for Wireless」を選択し、「変更」をクリックします。**

「インテル (R) PROSet for Wireless InstallShield ウィザード」ウィンドウが表示されます。

4 **「次へ」をクリックします。**



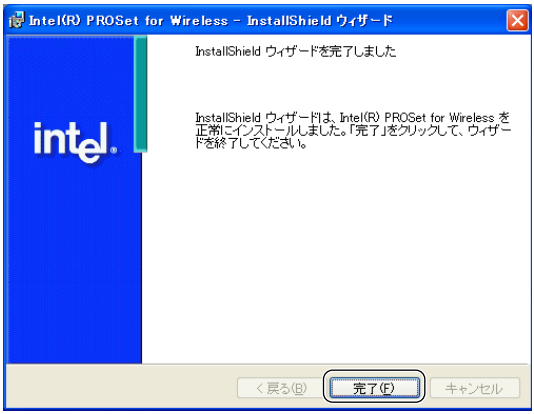
5 **(1)「変更」をクリックして◉にし、(2)「次へ」をクリックします。**



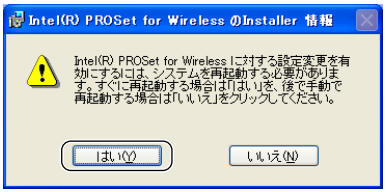
6 **「シングルサインオン機能セット」の[×]をクリックし、表示されるメニューから「この機能およびすべてのサブ機能をローカルのハードディスク ドライブにインストールします」を選択し、「次へ」をクリックします。**

7 **「インストール」をクリックします。**
追加するプログラムがインストールされます。

8 **インストールが完了したら、「完了」をクリックします。**



9 **システムの再起動について確認のメッセージが表示されたら、「はい」をクリックして、パソコンを再起動します。**



10 **再起動後、「スタート」ボタン→「すべてのプログラム」（「プログラム」）→「Intel Network Adapters」→「Intel（R）PROSet for Wireless」の順にクリックします。**

「インテル（R）PROSet for Wireless」ウィンドウが表示されます。

IEEE 802.1X ＋ EAP-TLS ／ WPA ＋ EAP-TLS

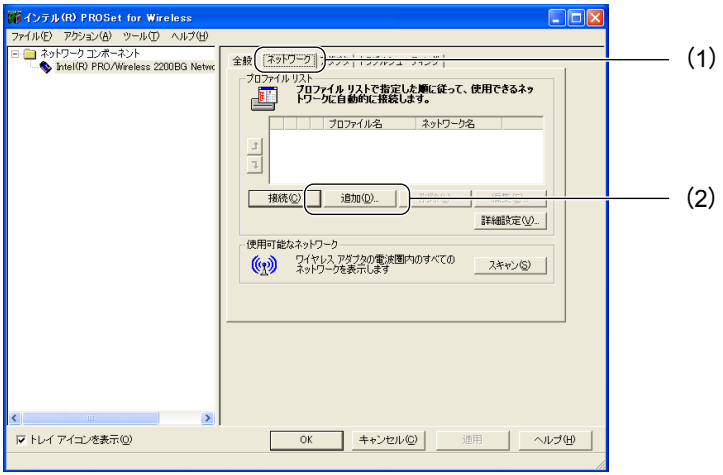
次のセキュリティパターンの場合の設定方法を説明します。

・IEEE 802.1X ＋ EAP-TLS
・WPA ＋ EAP-TLS

1 **「スタート」ボタン→「すべてのプログラム」（「プログラム」）→「Intel Network Adapters」→「Intel（R）PROSet for Wireless」の順にクリックします。**

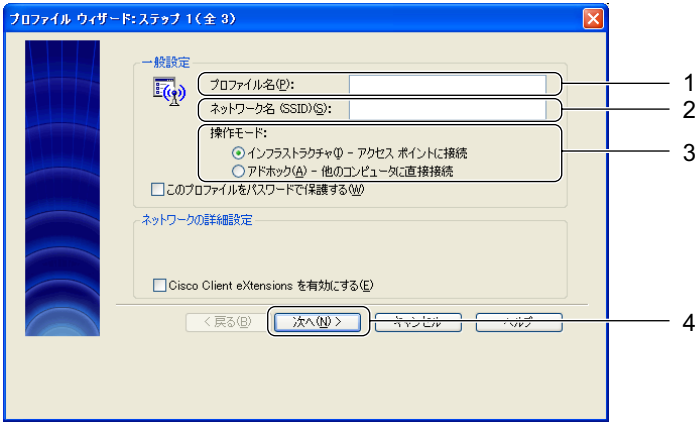
「インテル（R）PROSet for Wireless」ウィンドウが表示されます。

2 **(1)「ネットワーク」タブをクリックし、(2)「追加」をクリックします。**



「プロファイルウィザード」ウィンドウが表示されます。

3 無線 LAN のネットワークへ接続するための情報を設定します。次のように設定します。



1. 「プロファイル名」を入力します。
   設定するパラメータ情報を保存するプロファイル名を入力します。半角英数字 40 文字以内で、任意の文字列を入力してください。空白文字は使用できません。
2. 「ネットワーク名（SSID）」を入力します。
   ネットワーク名（SSID）は、半角英数字 32 文字以内で入力してください。
3. 「操作モード」の「インフラストラクチャ」をクリックして◉にします。
4. 設定が終わったら「次へ」をクリックします。

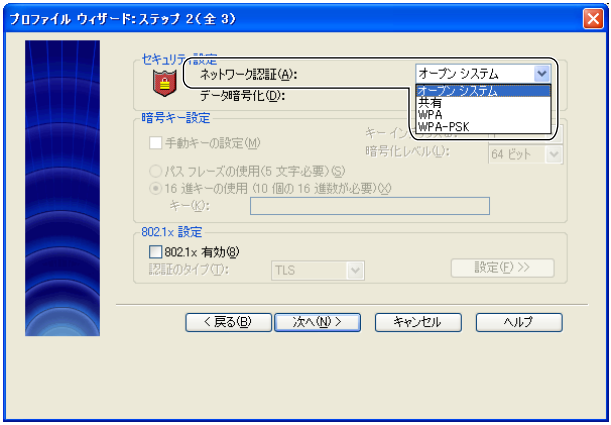
POINT

・「このプロファイルをパスワードで保護する」について
設定しているプロファイルをパスワードで保護することができます。パスワード保護を有効にしたい場合には、「このプロファイルをパスワードで保護する」を☑にします。

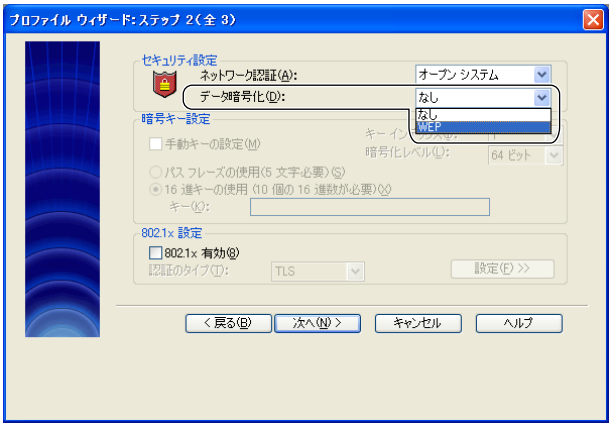
4 セキュリティの設定をします。次のように設定します。

■ IEEE 802.1X の場合

1. 「ネットワーク認証」の をクリックし、「オープンシステム」を選択します。

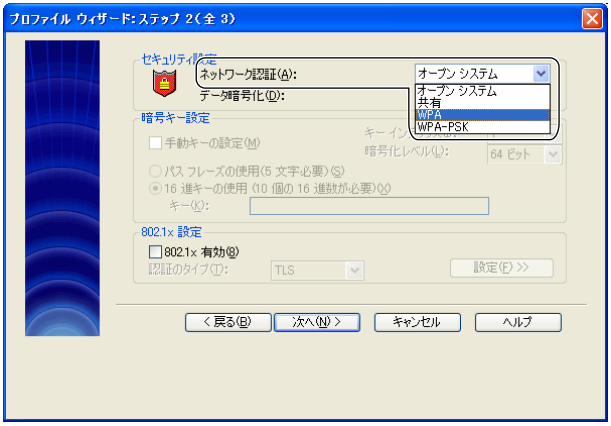


2. 「データ暗号化」の をクリックし、「WEP」を選択します。

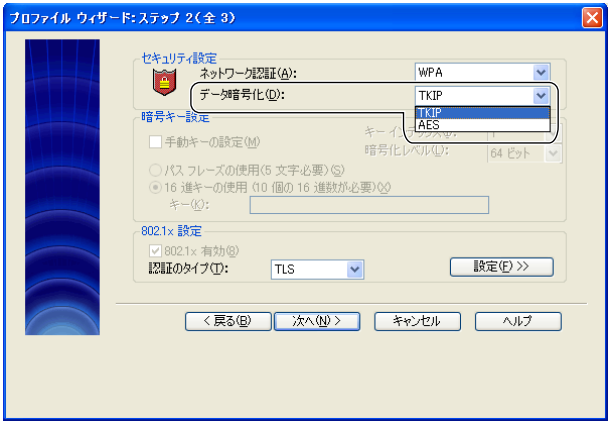


■ WPA の場合

1.「ネットワーク認証」の をクリックし、「WPA」を選択します。



2.「データ暗号化」の をクリックし、「TKIP」または「AES」を選択します。
接続する無線 LAN アクセスポイントに合わせて設定してください。



5 「802.1x 設定」の設定をします。

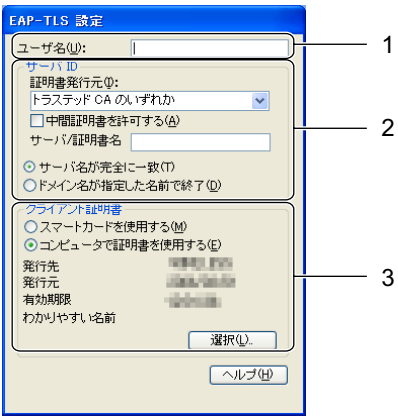
1.「802.1x 有効」を □ から ☑ にします。

「認証のタイプ」の をクリックし、「TLS」を選択します。

2.「設定 >>」をクリックします。

「EAP-TLS 設定」ウィンドウが表示されます。

3. パラメータを指定します。



1. ユーザ名
   認証のためのユーザー名を設定します。
2. サーバ ID
   - 証明書発行元

     「証明書発行元」の をクリックすると、証明書のリストが表示されます。リスト内から使用する証明書を選択します。
   - 中間証明書を許可する

     証明機関から直接発行された場合は、 にします。

     中間証明機関の 1 つから発行された場合は、 にします。

・サーバ / 証明書名
サーバ／証明書名を指定する場合は、サーバー名またはドメイン名をRADIUS サーバーの設定に合わせて入力します。
サーバー名が、証明書のサーバー名と完全に一致する場合、「サーバ名が完全に一致」を◉にし、サーバー名を入力します。
証明書にこのドメイン名、またはこのドメインのサブドメインに属するサーバー名が指定されていない場合は、「ドメイン名が指定した名前で終了」を◉にし、ドメイン名を入力します。

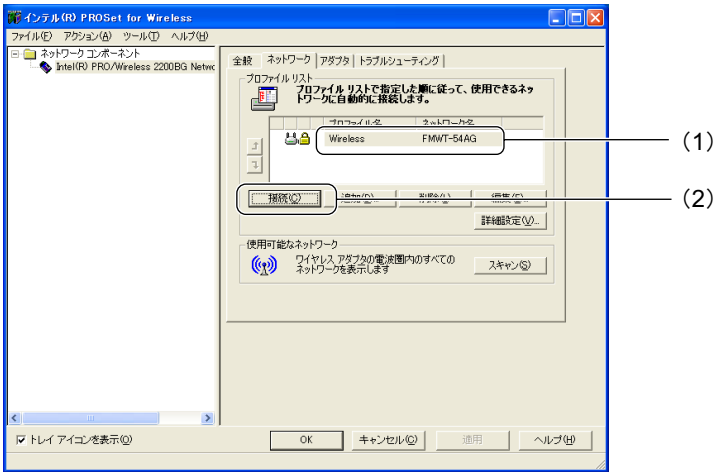
3. クライアント証明書
「選択」をクリックして証明書を選択します。

6 設定したら、プロファイルウィザードの「閉じる <<」をクリックします。

7 「次へ」をクリックします。

8 「プロファイルウィザード：ステップ 3（全 3)」ウィンドウで「完了」をクリックします。

9 (1)「プロファイルリスト」から作成したプロファイルを選択し、(2)「接続」をクリックします。



IEEE 802.1X ＋ PEAP-MSCHAPv2 ／ WPA ＋ PEAP-MSCHAPv2

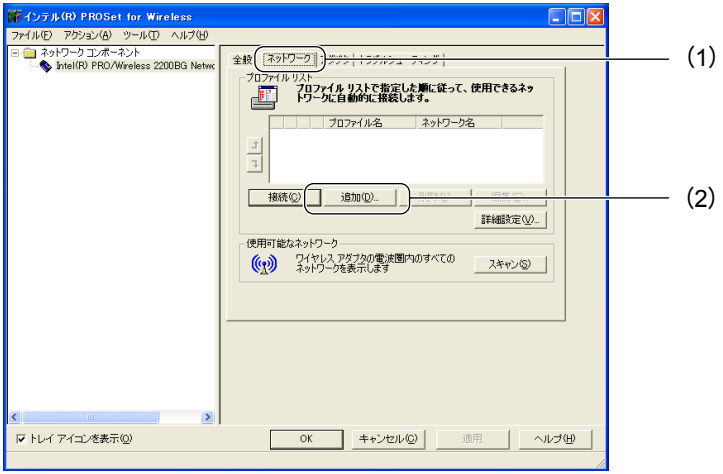
次のセキュリティパターンの場合の設定方法を説明します。

・IEEE 802.1X ＋ PEAP-MSCHAPv2
・WPA ＋ PEAP-MSCHAPv2

1 「スタート」ボタン→「すべてのプログラム」（「プログラム」）→「Intel Network Adapters」→「Intel（R）PROSet for Wireless」の順にクリックします。

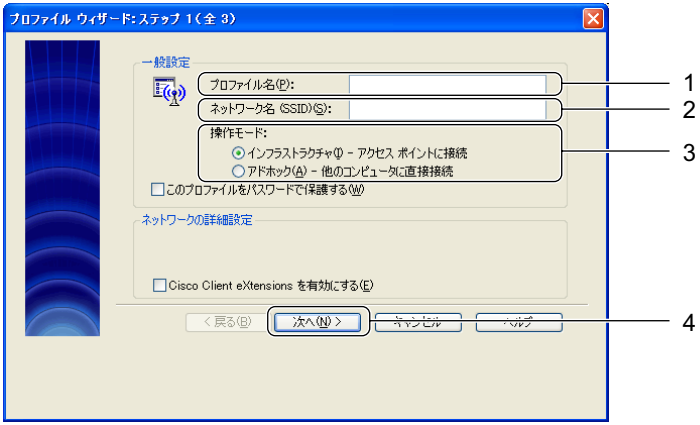
「インテル（R）PROSet for Wireless」ウィンドウが表示されます。

2 (1)「ネットワーク」タブをクリックし、(2)「追加」をクリックします。



「プロファイルウィザード」ウィンドウが表示されます。

3 無線 LAN のネットワークへ接続するための情報を設定します。次のように設定します。



1. 「プロファイル名」を入力します。
   設定するパラメータ情報を保存するプロファイル名を入力します。半角英数字 40 文字以内で、任意の文字列を入力してください。空白文字は使用できません。
2. 「ネットワーク名（SSID）」を入力します。
   ネットワーク名（SSID）は、半角英数字 32 文字以内で入力してください。
3. 「操作モード」の「インフラストラクチャ」をクリックして◉にします。
4. 設定が終わったら「次へ」をクリックします。

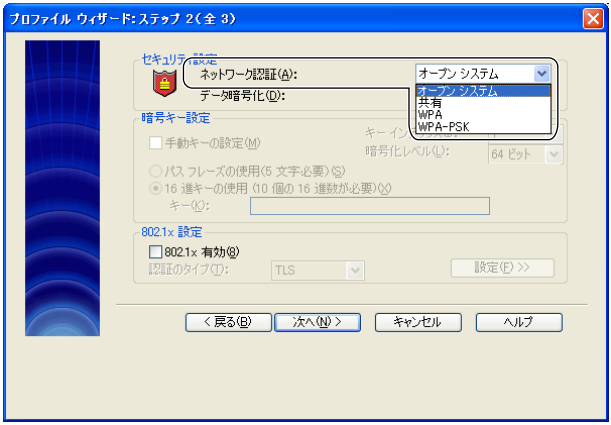
POINT

・「このプロファイルをパスワードで保護する」について
設定しているプロファイルをパスワードで保護することができます。パスワード保護を有効にしたい場合には、「このプロファイルをパスワードで保護する」を☑にします。

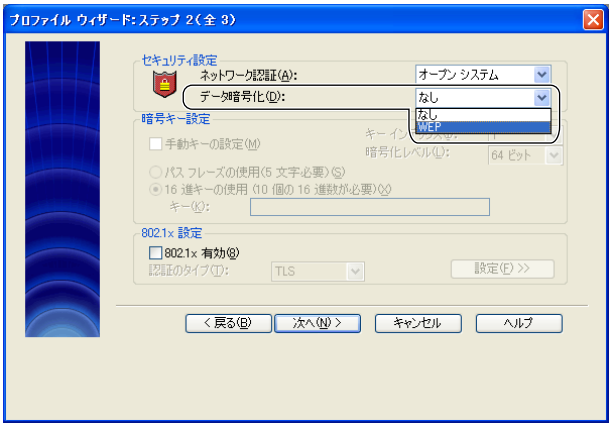
4 セキュリティの設定をします。次のように設定します。

■ IEEE 802.1X の場合

1. 「ネットワーク認証」の をクリックし、「オープンシステム」を選択します。

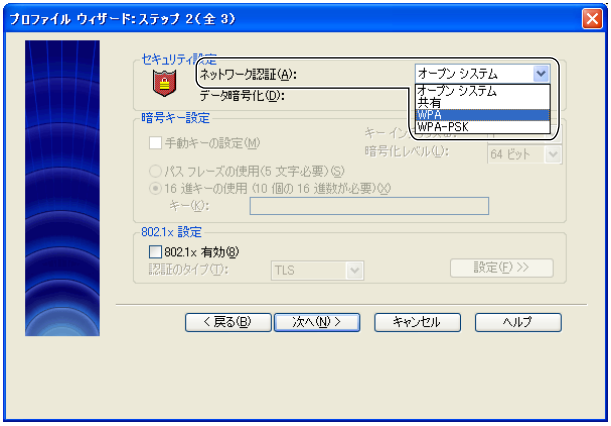


2. 「データ暗号化」の をクリックし、「WEP」を選択します。

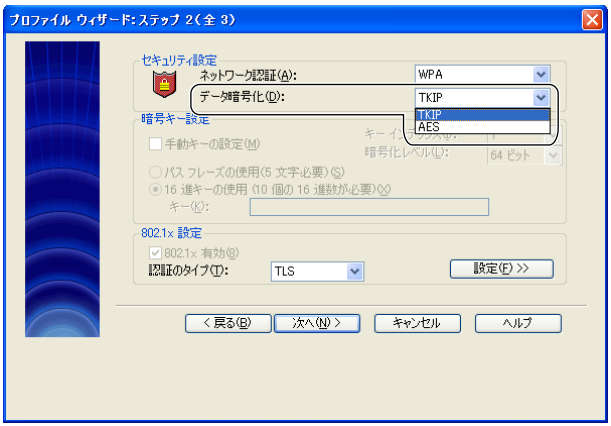


■ WPA の場合

1.「ネットワーク認証」の をクリックし、「WPA」を選択します。



2.「データ暗号化」の をクリックし、「TKIP」、または「AES」を選択します。
接続する無線 LAN アクセスポイントに合わせて設定してください。



5 「802.1x 設定」の設定をします。

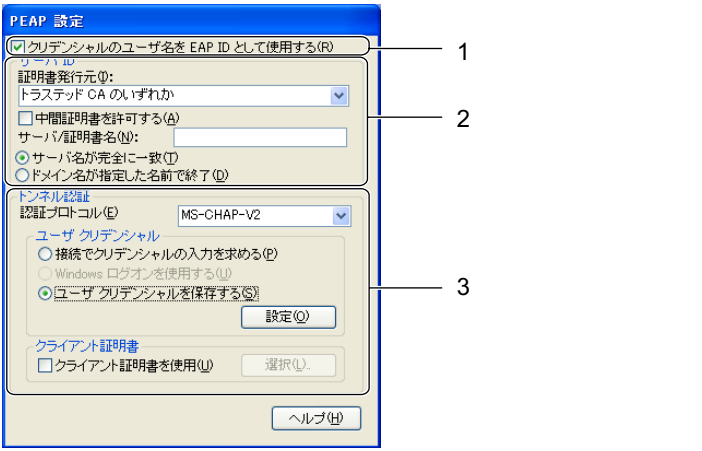
1.「802.1x 有効」を から にします。

「認証のタイプ」の をクリックし、「PEAP」を選択します。

2.「設定 >>」をクリックします。

「PEAP 設定」ウィンドウが表示されます。

3. パラメータを指定します。



1. クリデンシャルのユーザ名を EAP ID として使用する

   「クリデンシャルのユーザ名を EAP ID として使用する」が☑になっていることを確認します。

2. サーバ ID

   ・証明書発行元

   「証明書発行元」の⌄をクリックすると、証明書のリストが表示されます。リストの中から使用する証明書を選択します。

   ・中間証明書を許可する

   証明機関から直接発行された場合は、☐にします。

   中間証明機関の 1 つから発行された場合は、☑にします。

・サーバ / 証明書名

サーバ／証明書名を指定する場合は、サーバー名またはドメイン名をRADIUS サーバーの設定に合わせて入力します。

サーバー名が証明書のサーバー名と完全に一致する場合、「サーバ名が完全に一致」を◉にし、サーバー名を入力します。

証明書にこのドメイン名、またはこのドメインのサブドメインに属するサーバー名が指定されていない場合は、「ドメイン名が指定した名前で終了」を◉にし、ドメイン名を入力します。

3. トンネル認証

・認証プロトコル

「認証プロトコル」の ⌄ をクリックして「MS-CHAP-V2」を選択します。

・ユーザクリデンシャル

認証に使用するユーザーの情報を入力します。

接続するたびに入力する場合

「接続でクリデンシャルの入力を求める」をクリックして◉にします。

シングルサインオンを使用する場合

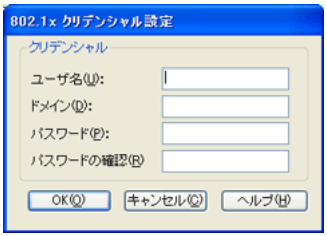
「Windows ログオンを使用する」をクリックして◉にします。

シングルサインオンを使用する場合は、プログラムを追加する必要があります。

プログラムの追加方法については、「シングルサインオン／ドメインログオンを使用する場合のプログラムの追加」(→ P.202) をご覧ください。

あらかじめ設定しておく場合

「ユーザクリデンシャルを保存する」をクリックして◉にし、「設定」をクリックします。「802.1x クリデンシャル設定」ウィンドウで次の項目を設定し、「OK」をクリックします。



表：「802.1x クリデンシャル設定」画面の設定項目について

項目名	説明
ユーザ名	認証に使用するユーザー名を入力します。

表：「802.1x クリデンシャル設定」画面の設定項目について

項目名	説明
ドメイン	ドメインに参加しているネットワークに接続する場合は、RADIUS サーバーのドメイン名を入力します。
パスワード	認証に使用するユーザーのパスワードを入力します。
パスワードの確認	確認のため、「パスワード」と同じ値を入力します。

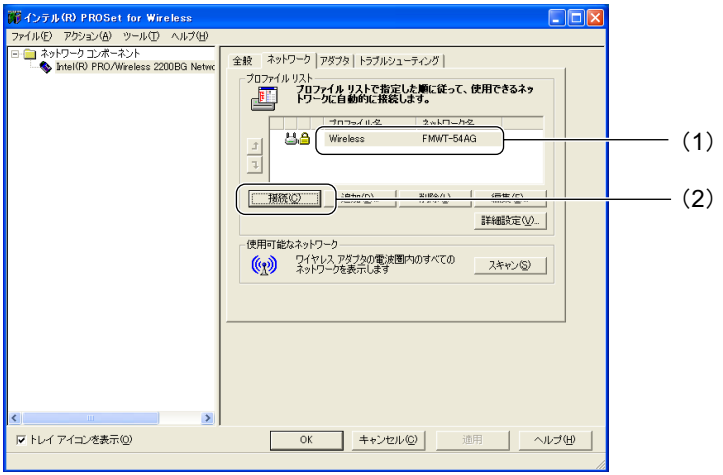
・クライアント証明書
使用しません。

6 **設定したら、プロファイルウィザードの「閉じる <<」をクリックします。**

7 **「次へ」をクリックします。**

8 **「プロファイルウィザード：ステップ 3（全 3)」ウィンドウで「完了」をクリックします。**

9 **(1)「プロファイルリスト」から作成したプロファイルを選択し、(2)「接続」をクリックします。**



IEEE 802.1X ＋ PEAP-TLS ／ WPA ＋ PEAP-TLS

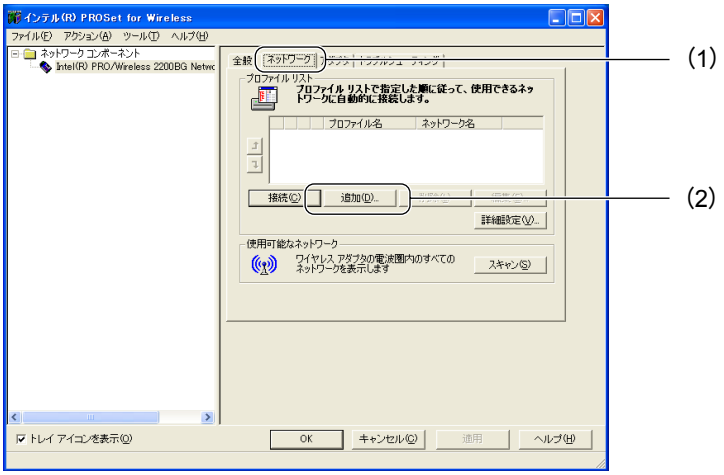
次のセキュリティパターンの場合の設定方法を説明します。

・IEEE 802.1X ＋ PEAP-TLS
・WPA ＋ PEAP-TLS

1 **「スタート」ボタン→「すべてのプログラム」（「プログラム」）→「Intel Network Adapters」→「Intel（R）PROSet for Wireless」の順にクリックします。**

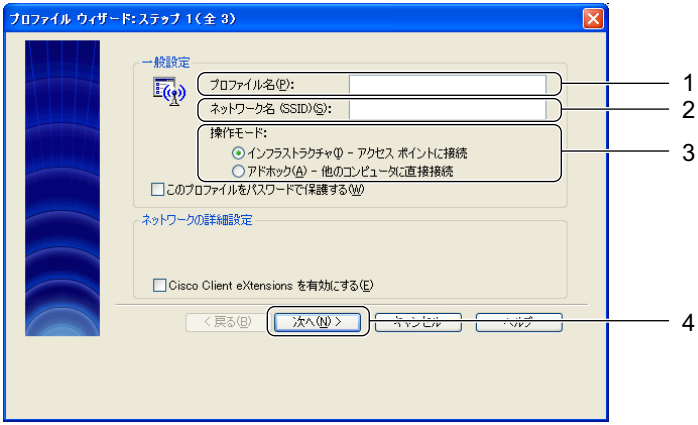
「インテル（R）PROSet for Wireless」ウィンドウが表示されます。

2 **(1)「ネットワーク」タブをクリックし、(2)「追加」をクリックします。**



「プロファイルウィザード」ウィンドウが表示されます。

3 無線 LAN のネットワークへ接続するための情報を設定します。次のように設定します。



1. 「プロファイル名」を入力します。
   設定するパラメータ情報を保存するプロファイル名を入力します。半角英数字 40 文字以内で、任意の文字列を入力してください。空白文字は使用できません。
2. 「ネットワーク名（SSID）」を入力します。
   ネットワーク名（SSID）は、半角英数字 32 文字以内で入力してください。
3. 「操作モード」の「インフラストラクチャ」をクリックして◉にします。
4. 設定が終わったら「次へ」をクリックします。

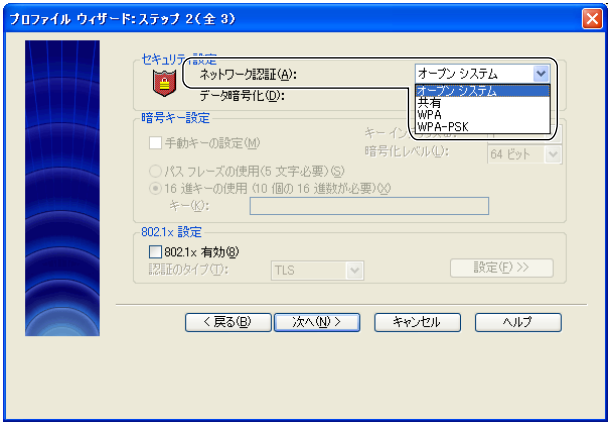
POINT

・「このプロファイルをパスワードで保護する」について
設定しているプロファイルをパスワードで保護することができます。パスワード保護を有効にしたい場合には、「このプロファイルをパスワードで保護する」を☑にします。

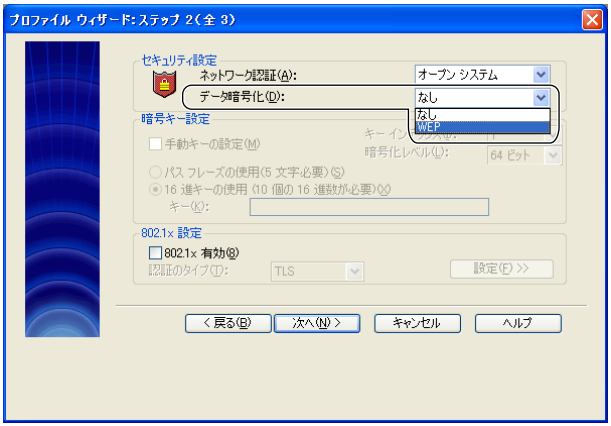
4 セキュリティの設定をします。次のように設定します。

■ IEEE 802.1X の場合

1. 「ネットワーク認証」の をクリックし、「オープンシステム」を選択します。

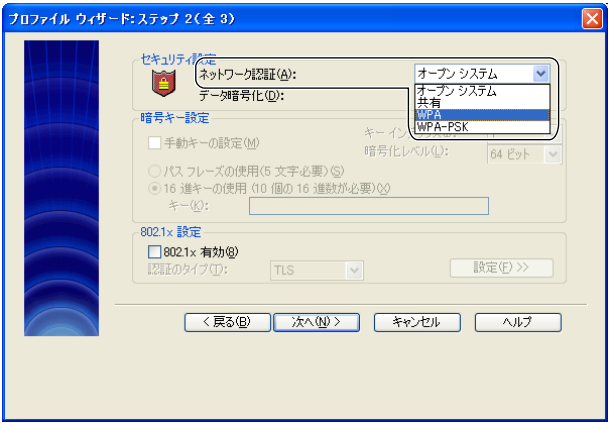


2. 「データ暗号化」の をクリックし、「WEP」を選択します。

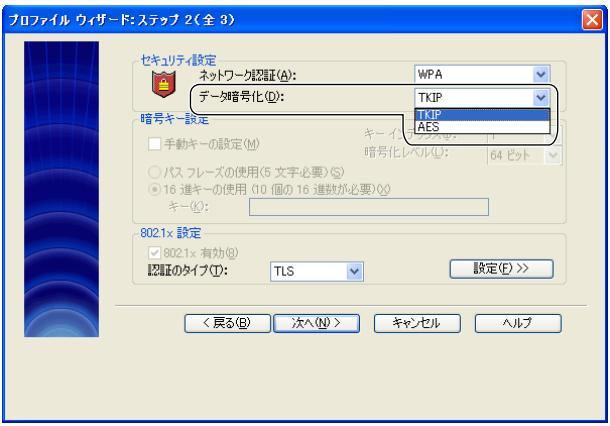


■ WPA の場合

1. 「ネットワーク認証」の をクリックし、「WPA」を選択します。



2. 「データ暗号化」の をクリックして「TKIP」、または「AES」を選択します。
接続する無線 LAN アクセスポイントに合わせて設定してください。



5 「802.1x 設定」の設定をします。

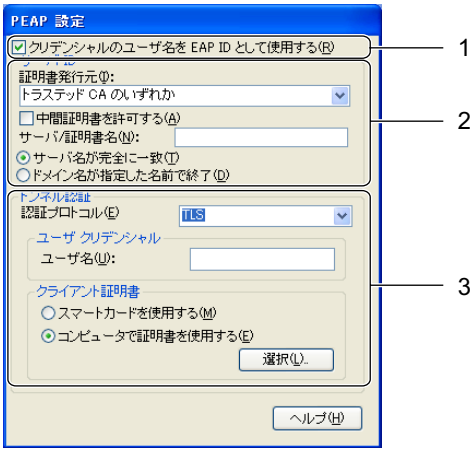
1. 「802.1x 有効」を☐から☑にします。

「認証のタイプ」の をクリックし、「PEAP」を選択します。

2.「設定 >>」をクリックします。

「PEAP 設定」ウィンドウが表示されます。

3. パラメータを指定します。



1. クリデンシャルのユーザ名を EAP ID として使用する

   「クリデンシャルのユーザ名を EAP ID として使用する」が☑になっていることを確認します。

2. サーバ ID

   ・証明書発行元

   「証明書発行元」の⌄をクリックすると、証明書のリストが表示されます。リストの中から使用する証明書を選択します。

   ・中間証明書を許可する

   証明機関から直接発行された場合は、☐にします。

   中間証明機関の 1 つから発行された場合は、☑にします。

・サーバ / 証明書名

サーバ／証明書名を指定する場合は、サーバー名またはドメイン名をRADIUS サーバーの設定に合わせて入力します。

サーバー名が、証明書のサーバー名と完全に一致する場合、「サーバ名が完全に一致」を◉にし、サーバー名を入力します。

証明書にこのドメイン名、またはこのドメインのサブドメインに属するサーバー名が指定されている場合は、「ドメイン名が指定した名前で終了」を◉にし、ドメイン名を入力します。

3. トンネル認証

・認証プロトコル

「認証プロトコル」の⌄をクリックし、「TLS」を選択します。

・ユーザクリデンシャル

認証に使用するユーザーの情報を入力します。

・クライアント証明書

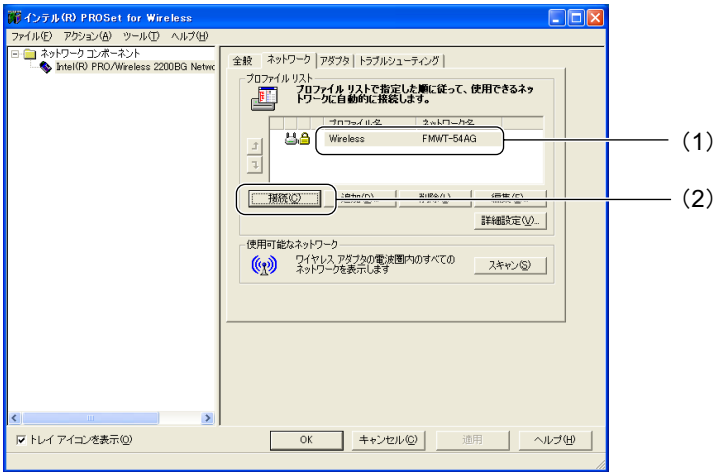
「コンピュータで証明書を使用する」をクリックして◉にし、「選択」をクリックして使用する証明書を選択します。

6 設定したら、プロファイルウィザードの「閉じる <<」をクリックします。

7 「次へ」をクリックします。

8 「プロファイルウィザード：ステップ 3（全 3)」ウィンドウで「完了」をクリックします。

9 (1)「プロファイルリスト」から作成したプロファイルを選択し、(2)「接続」をクリックします。



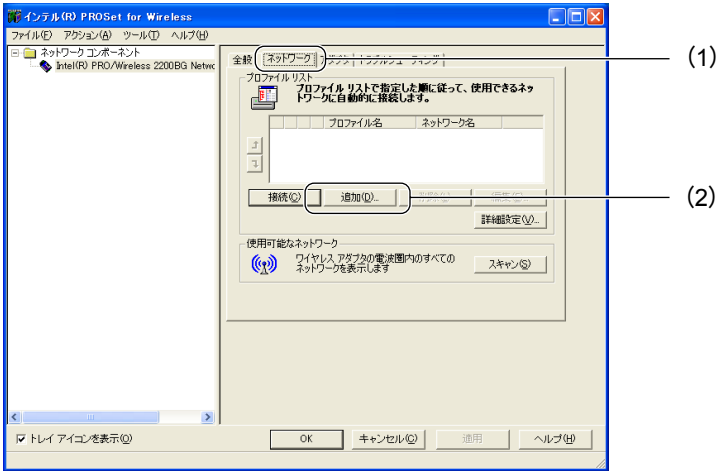
WPA-PSK

WPA-PSK の場合の設定方法を説明します。

1 **「スタート」ボタン→「すべてのプログラム」（「プログラム」）→「Intel Network Adapters」→「Intel（R）PROSet for Wireless」の順にクリックします。**

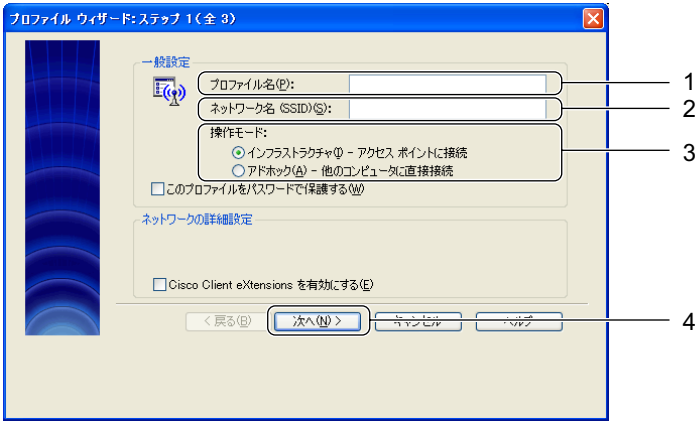
「インテル（R）PROSet for Wireless」ウィンドウが表示されます。

2 **(1)「ネットワーク」タブをクリックし、(2)「追加」をクリックします。**



「プロファイルウィザード」ウィンドウが表示されます。

3 **無線 LAN のネットワークへ接続するための情報を設定します。次のように設定します。**



1.「プロファイル名」を入力します。
設定するパラメータ情報を保存するプロファイル名を入力します。半角英数字40 文字以内で、任意の文字列を入力してください。空白文字は使用できません。
2.「ネットワーク名（SSID）」を入力します。
ネットワーク名（SSID）は、半角英数字 32 文字以内で入力してください。
3.「操作モード」の「インフラストラクチャ」をクリックして にします。
4. 設定が終わったら「次へ」をクリックします。

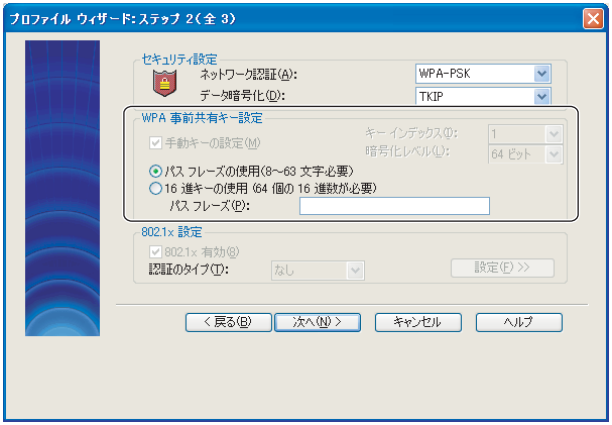
POINT

・「このプロファイルをパスワードで保護する」について
設定しているプロファイルをパスワードで保護することができます。パスワード保護を有効にしたい場合には、「このプロファイルをパスワードで保護する」を にします。

4 セキュリティの設定をします。次のように設定します。

1.「ネットワーク認証」の をクリックし、「WPA-PSK」を選択します。
2.「データ暗号化」の をクリックして「TKIP」、または「AES」を選択します。
接続する無線 LAN アクセスポイントに合わせて設定してください。

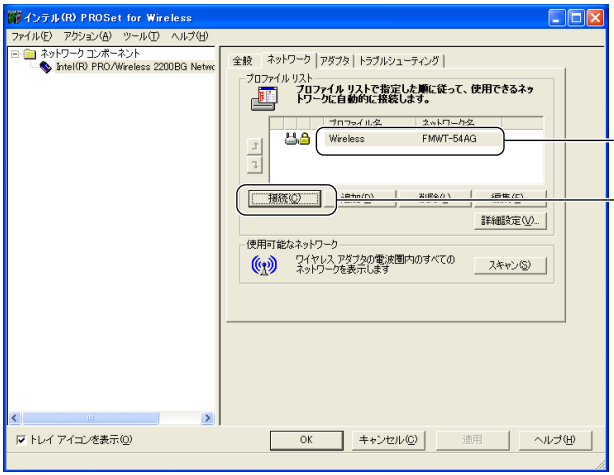
5 「WPA 事前共有キー設定」を設定します。無線 LAN アクセスポイントと同じ入力形式を選択して、値を入力してください。



6 「次へ」をクリックします。

7 「プロファイルウィザード：ステップ 3（全 3)」ウィンドウで「完了」をクリックします。

8 (1)「プロファイルリスト」から作成したプロファイルを選択し、(2)「接続」をクリックします。



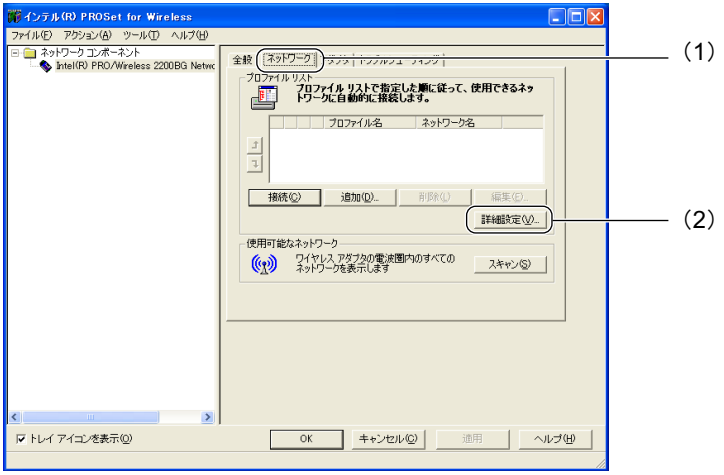
ドメインログオン使用：WPA-PSK

WPA-PSK でドメインログオンをお使いになる場合の設定方法を説明します。

1 **「スタート」ボタン→「すべてのプログラム」（「プログラム」）→「Intel Network Adapters」→「Intel（R）PROSet for Wireless」の順にクリックします。**

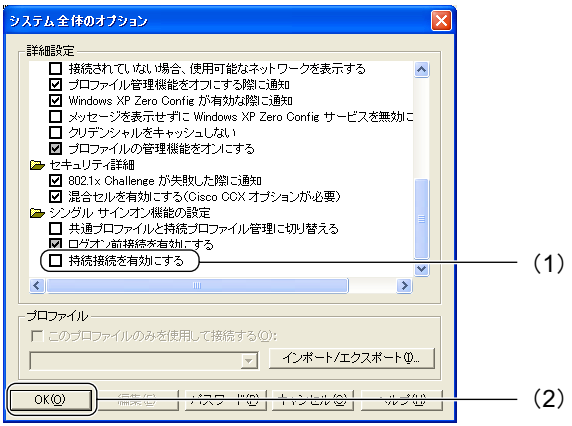
「インテル（R）PROSet for Wireless」ウィンドウが表示されます。

2 **(1)「ネットワーク」タブをクリックし、(2)「詳細設定」をクリックします。**

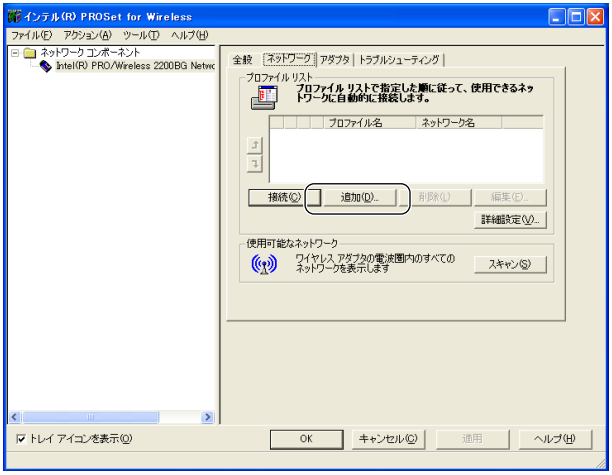


「システム全体のオプション」ウィンドウが表示されます。

3 **(1) 一覧から「持続接続を有効にする」をクリックして☑にし、(2)「OK」をクリックします。**

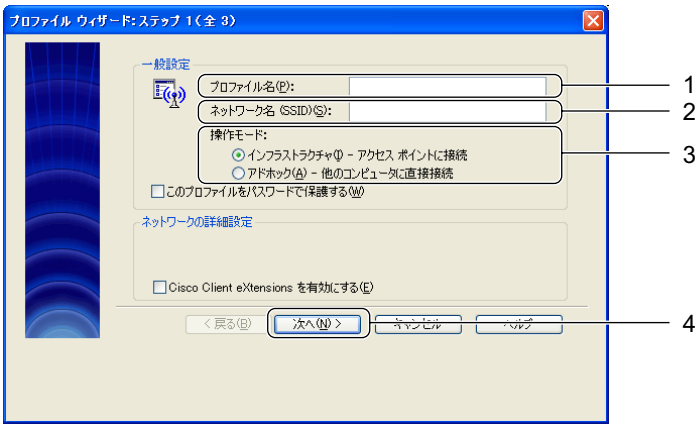


4 「追加」をクリックします。



「プロファイルウィザード」ウィンドウが表示されます。

5 無線 LAN のネットワークへ接続するための情報を設定します。次のように設定します。

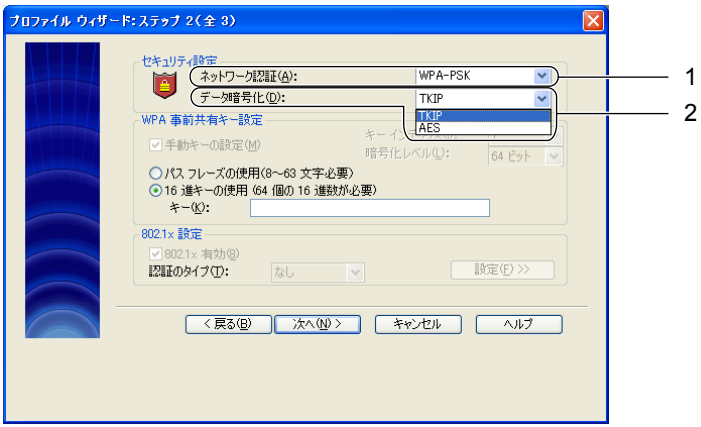


1. 「プロファイル名」を入力します。
   設定するパラメータ情報を保存するプロファイル名を入力します。半角英数字 40 文字以内で、任意の文字列を入力してください。空白文字は使用できません。
2. 「ネットワーク名（SSID）」を入力します。
   ネットワーク名（SSID）は、半角英数字 32 文字以内で入力してください。
3. 「操作モード」の「インフラストラクチャ」をクリックして◉にします。
4. 設定が終わったら「次へ」をクリックします。

POINT

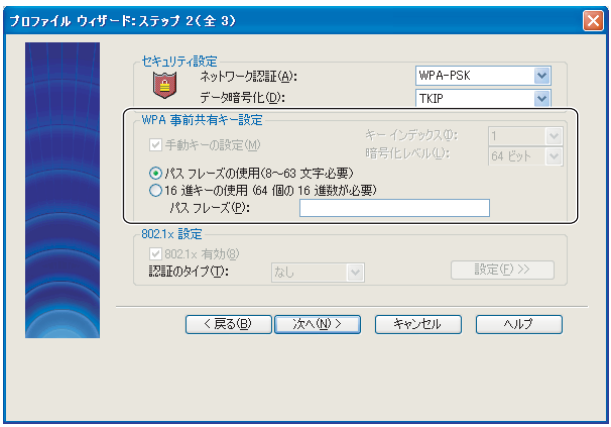
・「このプロファイルをパスワードで保護する」について
設定しているプロファイルをパスワードで保護することができます。パスワード保護を有効にしたい場合には、「このプロファイルをパスワードで保護する」を☑にします。

6 セキュリティの設定をします。次のように設定します。



1. 「ネットワーク認証」の▼をクリックし、「WPA-PSK」を選択します。
2. 「データ暗号化」の▼をクリックして「TKIP」、または「AES」を選択します。
接続する無線 LAN アクセスポイントに合わせて設定してください。

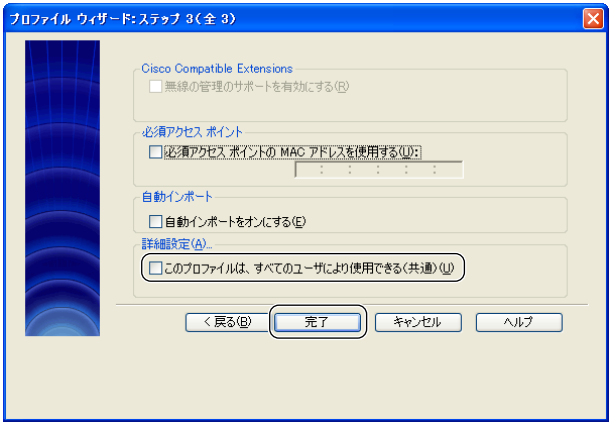
7 「WPA 事前共有キー設定」を設定します。無線 LAN アクセスポイントと同じ入力形式を選択して、値を入力してください。



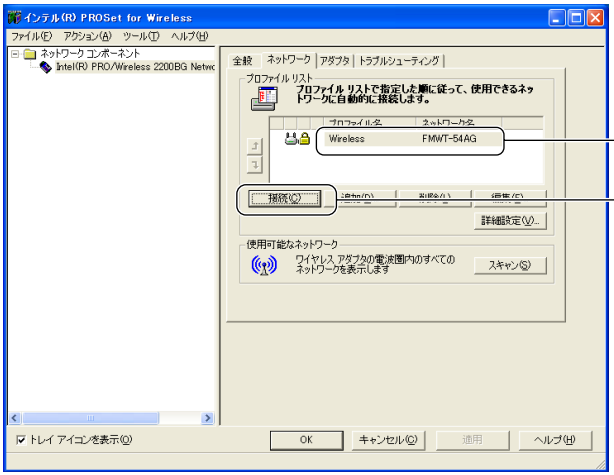
8 **「次へ」をクリックします。**

9 **「プロファイルウィザード：ステップ 3（全 3)」ウィンドウで「完了」をクリックします。**

ドメインログオンを使用する場合は、「このプロファイルは、すべてのユーザにより使用できる（共通)」をクリックして☑にし、「完了」をクリックします。



10 **(1)「プロファイルリスト」から作成したプロファイルを選択し、(2)「接続」をクリックします。**



9 Mr.WLANner を使った設定

無線 LAN の設定に、無線 LAN 設定ユーティリティ「Mr.WLANner」を使用する場合の設定方法を説明します。

IEEE 802.1X ＋ EAP-TLS ／ WPA ＋ EAP-TLS ／ WPA2 ＋ EAP-TLS

次のセキュリティパターンの場合の設定方法を説明します。

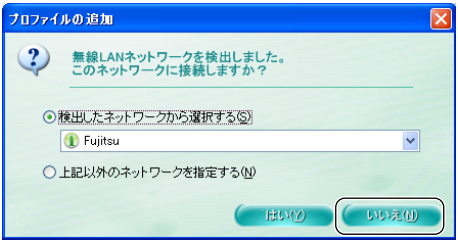
・IEEE 802.1X ＋ EAP-TLS
・WPA ＋ EAP-TLS
・WPA2 ＋ EAP-TLS

1 デスクトップ右下の通知領域からユーティリティアイコン（）を右クリックし、「設定」をクリックします。

「Mr.WLANner」ウィンドウが表示されます。

POINT

・「プロファイルの追加」ウィンドウが表示された場合、「いいえ」をクリックしてください。

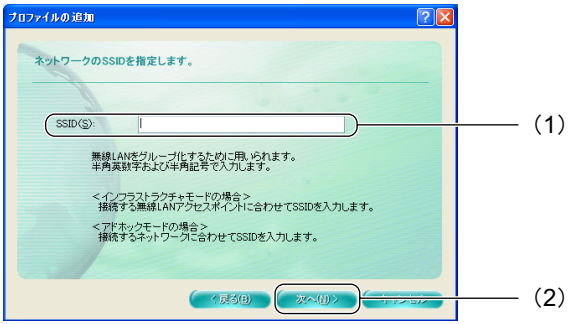


2 「プロファイルの追加」をクリックします。

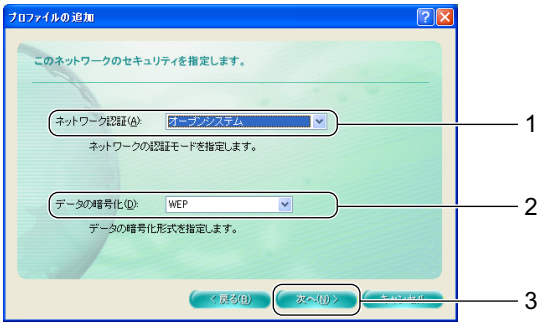
「プロファイルの追加」ウィンドウが表示されます。

3 (1)「インフラストラクチャモード」を選択して、(2)「次へ」をクリックします。

4 (1) 接続する無線 LAN アクセスポイントに合わせて「SSID」を入力し、(2)「次へ」をクリックします。



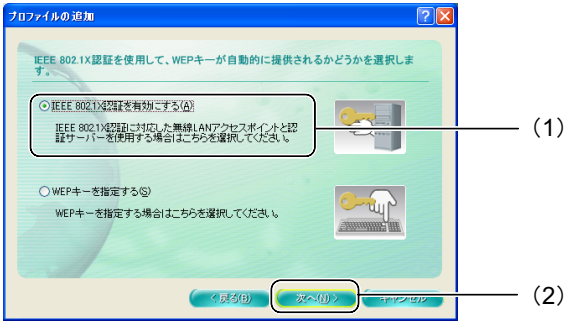
5 セキュリティの設定をします。



■ IEEE 802.1X の場合

1. 「ネットワーク認証」の をクリックし、「オープンシステム」を選択します。
2. 「データの暗号化」の をクリックし、「WEP」を選択します。
3. 「次へ」をクリックします。

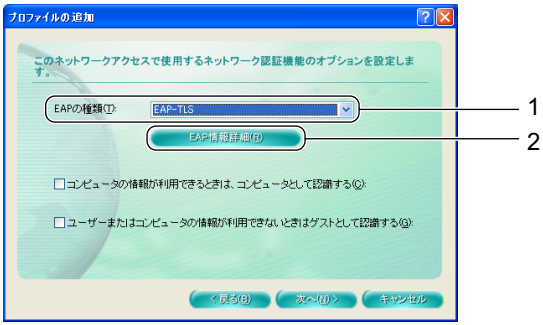
4. （1）「「IEEE 802.1X 認証を有効にする」をクリックして◉にし、（2）「次へ」をクリックします。



■ WPA ／ WPA2 の場合

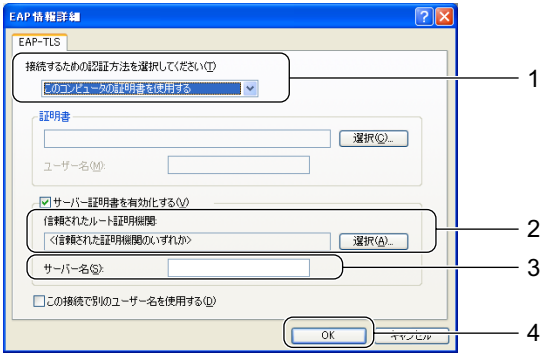
1. 「ネットワーク認証」の をクリックし、「WPA」または「WPA2」を選択します。
   無線 LAN アクセスポイントに合わせて設定してください。
2. 「データの暗号化」の をクリックし、「TKIP」または「AES」を選択します。
   無線 LAN アクセスポイントに合わせて設定してください。
3. 「次へ」をクリックします。

6 認証の設定をします。



1. 「EAP の種類」の をクリックし、「EAP-TLS」を選択します。
2. 「EAP 情報詳細」をクリックします。
   「EAP 情報詳細」ウィンドウが表示されます。

7 次のように設定します。



1. 「接続するための認証方法を選択してください」の をクリックし、「このコンピュータの証明書を使用する」を選択します。
2. 「証明機関」の「選択」をクリックして、表示されるリストから使用する証明機関を選択します。
3. 「サーバー名」に認証サーバーのサーバー名を入力します。
4. 「OK」をクリックします。

8 「プロファイルの追加」ウィンドウで「次へ」をクリックします。

9 (1)「プロファイル名」と「シールアイコン」を設定し、(2)「次へ」をクリックします。

10 設定内容を確認し、「完了」をクリックします。

ネットワークに接続されます。

POINT

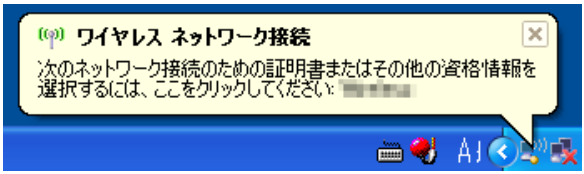
ネットワークに接続されない場合

ネットワークに接続されない場合は、作成したプロファイルをクリックし、「接続」をクリックしてください。

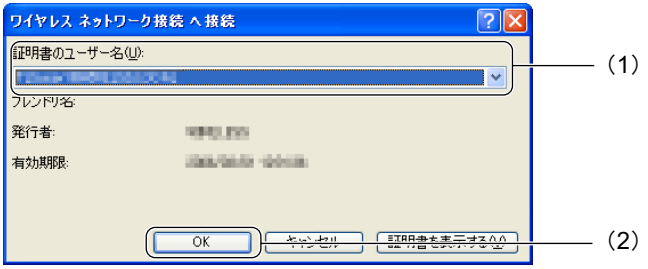
パソコンに複数の証明書をインストールしている場合

デスクトップ右下の通知領域に、メッセージが表示されるので、次のように操作してください。

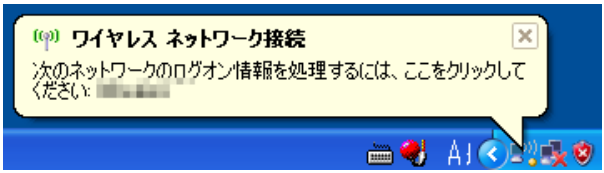
1. メッセージをクリックします。



2. （1）証明書のユーザー名を選択して、（2）「OK」をクリックします。

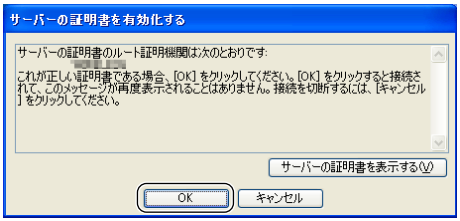


11 デスクトップ右下の通知領域に表示されるメッセージをクリックします。



「サーバーの証明書を有効化する」ウィンドウが表示されます。

12 「OK」をクリックします。



IEEE 802.1X ＋ PEAP-MSCHAPv2 ／ WPA ＋ PEAP-MSCHAPv2 ／ WPA2 ＋ PEAP-MSCHAPv2

次のセキュリティパターンの場合の設定方法を説明します。

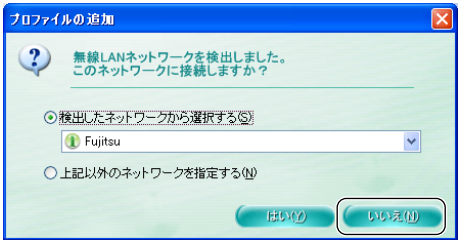
・IEEE 802.1X ＋ PEAP-MSCHAPv2
・WPA ＋ PEAP-MSCHAPv2
・WPA2 ＋ PEAP-MSCHAPv2

1 デスクトップ右下の通知領域からユーティリティアイコン（ ）を右クリックし、「設定」をクリックします。

「Mr.WLANner」ウィンドウが表示されます。

POINT

・「プロファイルの追加」ウィンドウが表示された場合、「いいえ」をクリックしてください。

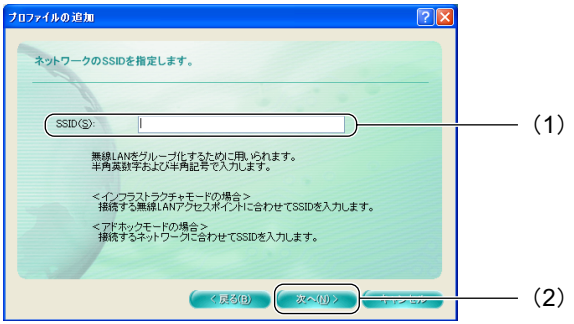


2 「プロファイルの追加」をクリックします。

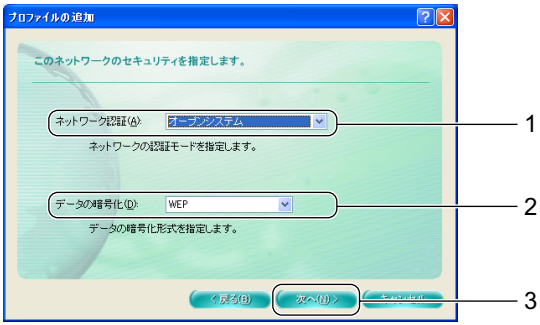
「プロファイルの追加」ウィンドウが表示されます。

3 (1)「インフラストラクチャモード」を選択して、(2)「次へ」をクリックします。

4 (1) 接続する無線 LAN アクセスポイントに合わせて「SSID」を入力し、(2)「次へ」をクリックします。



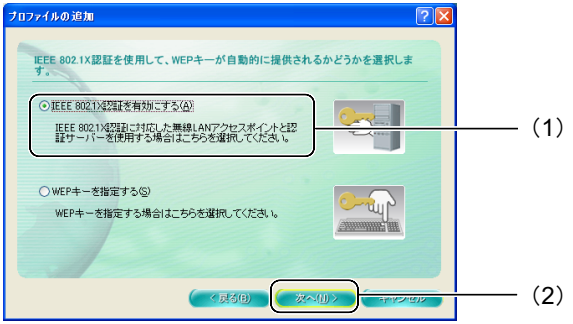
5 セキュリティの設定をします。



■ IEEE 802.1X の場合

1. 「ネットワーク認証」の をクリックし、「オープンシステム」を選択します。
2. 「データの暗号化」の をクリックし、「WEP」を選択します。
3. 「次へ」をクリックします。

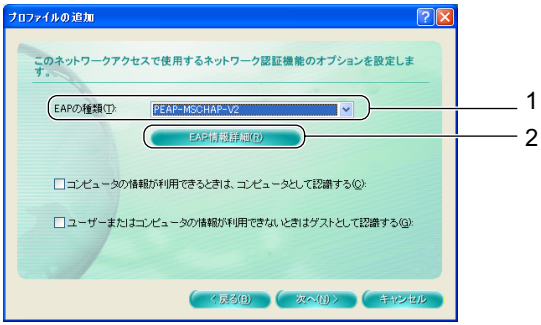
4. (1)「IEEE 802.1X 認証を有効にする」をクリックして◉にし、(2)「次へ」をクリックします。



■ WPA ／ WPA2 の場合

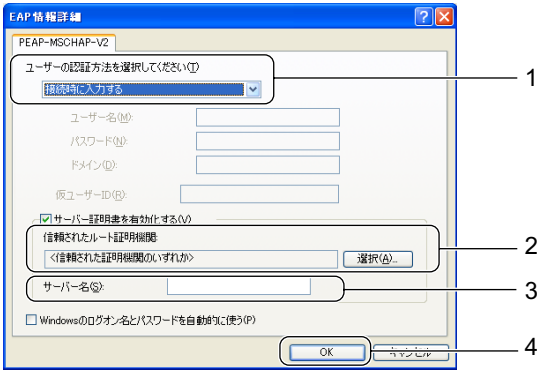
1. 「ネットワーク認証」の をクリックし、「WPA」または「WPA2」を選択します。
   無線 LAN アクセスポイントに合わせて設定してください。
2. 「データの暗号化」の をクリックし、「TKIP」または「AES」を選択します。
   無線 LAN アクセスポイントに合わせて設定してください。
3. 「次へ」をクリックします。

6 認証の設定をします。



1. 「EAP の種類」の をクリックし、「PEAP-MSCHAP-V2」を選択します。
2. 「EAP 情報詳細」をクリックします。
   「EAP 情報詳細」ウィンドウが表示されます。

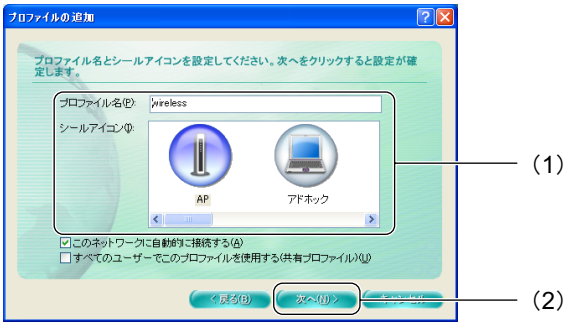
7 次のように設定します。



1. 「ユーザーの認証方法を選択してください」の をクリックし、「接続時に入力する」を選択します。
2. 「証明機関」の「選択」をクリックして、表示されるリストから使用する証明機関を選択します。
3. 「サーバー名」に認証サーバーのサーバー名を入力します。
4. 「OK」をクリックします。

8 「プロファイルの追加」ウィンドウで「次へ」をクリックします。

9 (1)「プロファイル名」と「シールアイコン」を設定し、(2)「次へ」をクリックします。



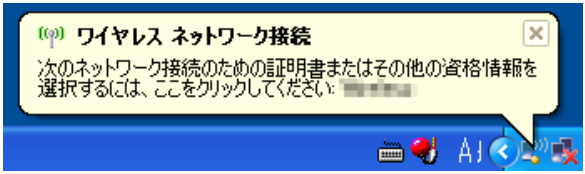
10 設定内容を確認し、「完了」をクリックします。

ネットワークに接続されます。

POINT

・ネットワークに接続されない場合は、作成したプロファイルをクリックし、「接続」をクリックしてください。

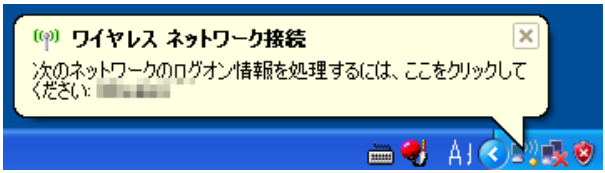
11 デスクトップ右下の通知領域にされるメッセージをクリックします。



12 (1) ユーザー名、パスワード、ログオンドメインを入力して、(2)「OK」をクリックします。

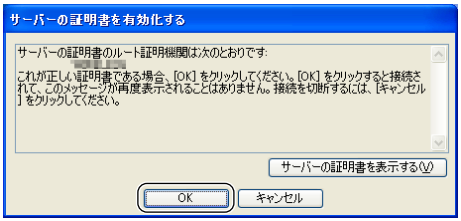
ユーザー名、パスワード、ログオンドメインは、ネットワーク管理者にご確認ください。

13 デスクトップ右下の通知領域に表示されるメッセージをクリックします。



「サーバーの証明書を有効化する」ウィンドウが表示されます。

14 「OK」をクリックします。



IEEE 802.1X ＋ PEAP-TLS ／ WPA ＋ PEAP-TLS ／ WPA2 ＋ PEAP-TLS

次のセキュリティパターンの場合の設定方法を説明します。

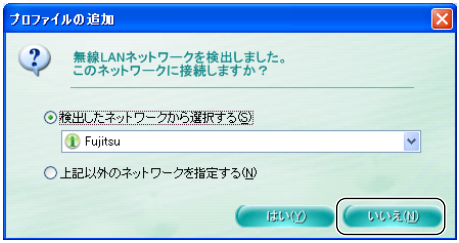
・IEEE 802.1X ＋ PEAP-TLS
・WPA ＋ PEAP-TLS
・WPA2 ＋ PEAP-TLS

1 デスクトップ右下の通知領域からユーティリティアイコン（  ）を右クリックし、「設定」をクリックします。

「Mr.WLANner」ウィンドウが表示されます。

POINT

・「プロファイルの追加」ウィンドウが表示された場合、「いいえ」をクリックしてください。

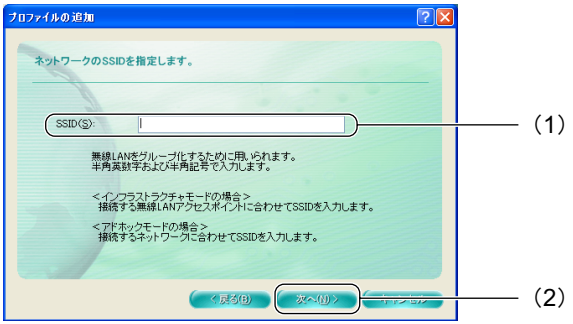


2 「プロファイルの追加」をクリックします。

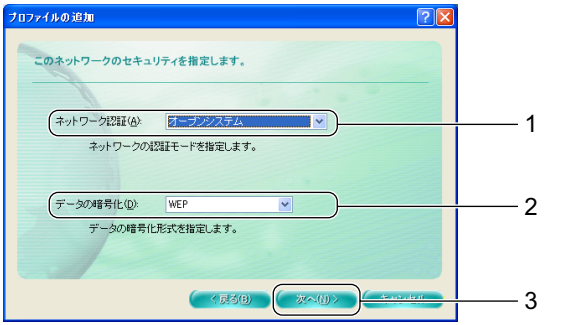
「プロファイルの追加」ウィンドウが表示されます。

3 (1)「インフラストラクチャモード」を選択して、(2)「次へ」をクリックします。

4 (1) 接続する無線 LAN アクセスポイントに合わせて「SSID」を入力し、(2)「次へ」をクリックします。



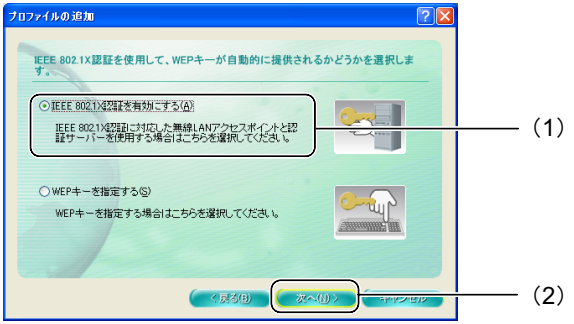
5 セキュリティの設定をします。



■ IEEE 802.1X の場合

1. 「ネットワーク認証」の をクリックし、「オープンシステム」を選択します。
2. 「データの暗号化」の をクリックし、「WEP」を選択します。
3. 「次へ」をクリックします。

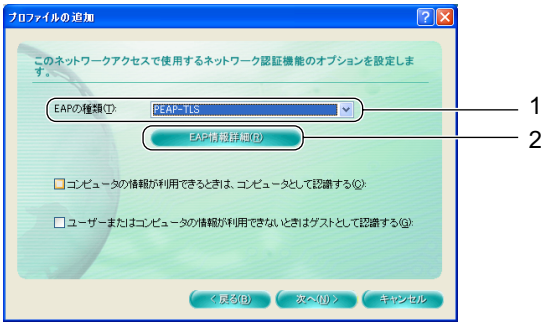
4. （1）「IEEE 802.1X 認証を有効にする」をクリックして◉にし、（2）「次へ」をクリックします。



■ WPA ／ WPA2 の場合

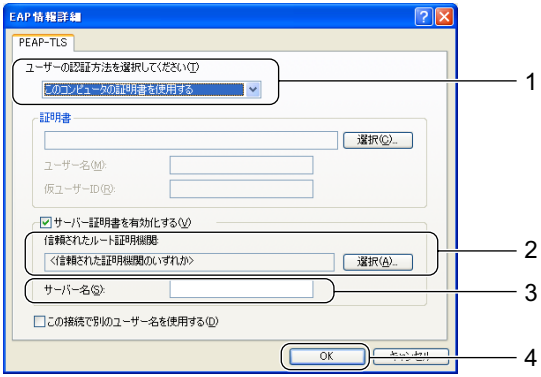
1. 「ネットワーク認証」の をクリックし、「WPA」または「WPA2」を選択します。
   無線 LAN アクセスポイントに合わせて設定してください。
2. 「データの暗号化」の をクリックし、「TKIP」または「AES」を選択します。
   無線 LAN アクセスポイントに合わせて設定してください。
3. 「次へ」をクリックします。

6 認証の設定をします。



1. 「EAP の種類」の をクリックし、「PEAP-TLS」を選択します。
2. 「EAP 情報詳細」をクリックします。
   「EAP 情報詳細」ウィンドウが表示されます。

7 次のように設定します。



1. 「ユーザーの認証方法を選択してください」の をクリックし、「このコンピュータの証明書を使用する」を選択します。
2. 「証明機関」の「選択」をクリックして、表示されるリストから使用する証明機関を選択します。
3. 「サーバー名」に認証サーバーのサーバー名を入力します。
4. 「OK」をクリックします。

8 「プロファイルの追加」ウィンドウで「次へ」をクリックします。

9 (1)「プロファイル名」と「シールアイコン」を設定し、(2)「次へ」をクリックします。

10 設定内容を確認し、「完了」をクリックします。

ネットワークに接続されます。

POINT

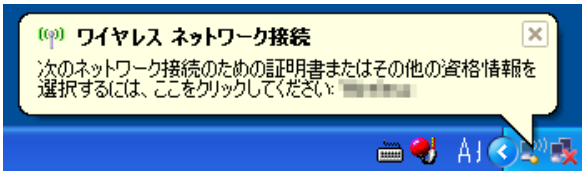
ネットワークに接続されない場合

ネットワークに接続されない場合は、作成したプロファイルをクリックし、「接続」をクリックしてください。

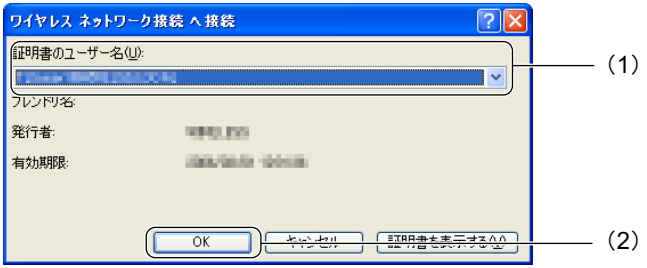
パソコンに複数の証明書をインストールしている場合

デスクトップ右下の通知領域に、メッセージが表示されるので、次のように操作してください。

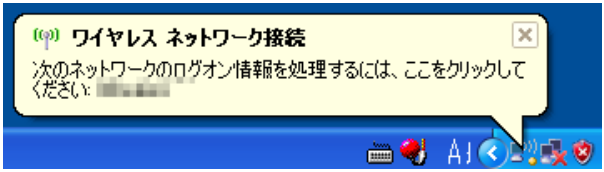
1. メッセージをクリックします。



2. （1）証明書のユーザー名を選択して、（2）「OK」をクリックします。

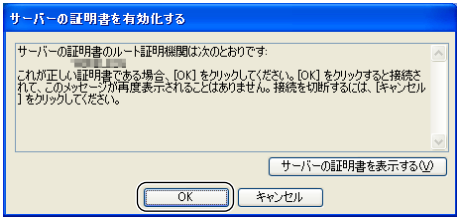


11 デスクトップ右下の通知領域に表示されるメッセージをクリックします。



「サーバーの証明書を有効化する」ウィンドウが表示されます。

12 「OK」をクリックします。



WPA-PSK ／ WPA2-PSK

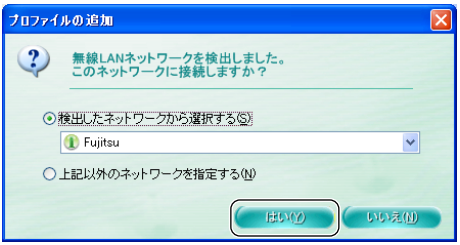
WPA-PSK ／ WPA2-PSK の場合の設定方法を説明します。

1 デスクトップ右下の通知領域からユーティリティアイコン（ ）を右クリックし、「設定」をクリックします。

「Mr.WLANner」ウィンドウが表示されます。

POINT

・「プロファイルの追加」ウィンドウが表示された場合、接続する無線 LAN アクセスポイントに設定された SSID（または ESSID）を選択して「はい」をクリックします。その後、手順 6 にお進みください。

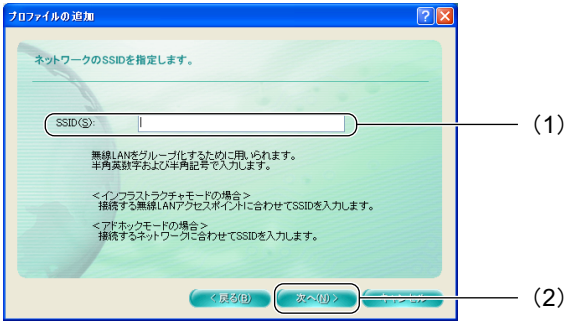


2 「プロファイルの追加」をクリックします。

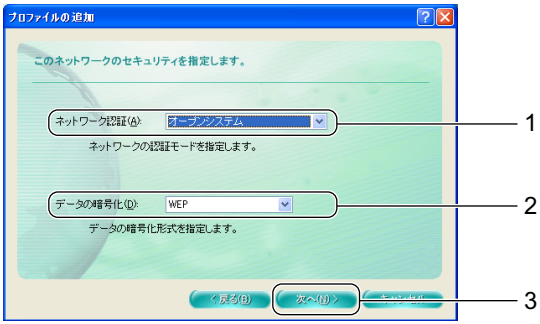
「プロファイルの追加」ウィンドウが表示されます。

3 (1)「インフラストラクチャモード」を選択して、(2)「次へ」をクリックします。

4 (1) 接続する無線 LAN アクセスポイントに合わせて「SSID」を入力し、(2)「次へ」をクリックします。

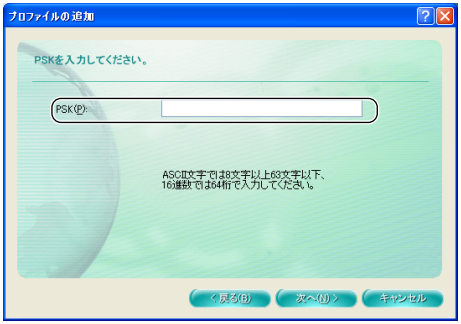


5 セキュリティの設定をします。



1. 「ネットワーク認証」の をクリックし、「WPA-PSK」または「WPA2-PSK」を選択します。
   無線 LAN アクセスポイントに合わせて設定してください。
2. 「データの暗号化」の をクリックし、「TKIP」または「AES」を選択します。
   無線 LAN アクセスポイントに合わせて設定してください。
3. 「次へ」をクリックします。

6 「PSK」に、無線 LAN アクセスポイントと同じ値を入力します。



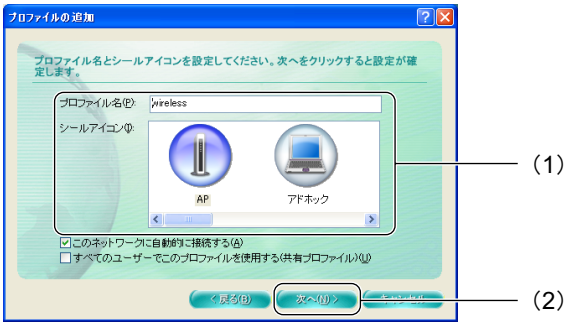
次のいずれかで入力します。

・ASCII 文字を、8 ～ 63 文字の範囲で入力します。使用できる文字は次の通りです。
0 ～ 9、a ～ z、A ～ Z、(アルファベットの大文字・小文字を区別します)、半角記号

・16 進数を、64 文字で入力します。使用できる文字は次の通りです。
0 ～ 9、A ～ F、a ～ f（アルファベットの大文字・小文字を区別しません）

7 「次へ」をクリックします。

8 (1)「プロファイル名」と「シールアイコン」を設定し、(2)「次へ」をクリックします。



9 設定内容を確認し、「完了」をクリックします。

ネットワークに接続されます。

POINT

・ネットワークに接続されない場合は、作成したプロファイルをクリックし、「接続」をクリックしてください。

10 Windows XP 標準の無線 LAN 機能を使った設定

無線 LAN の設定に、Windows XP 標準の無線 LAN 機能（Wireless Zero Configuration）を使用する場合の設定方法を説明します。

IEEE 802.1X ＋ EAP-TLS ／ WPA ＋ EAP-TLS ／ WPA2 ＋ EAP-TLS

次のセキュリティパターンの場合の設定方法を説明します。

- IEEE 802.1X ＋ EAP-TLS
- WPA ＋ EAP-TLS
- WPA2 ＋ EAP-TLS

POINT

WPA2 をお使いになる場合

WPA2 の機能を使用するには Microsoft から提供されている WPA2 機能に関するプログラムが適用されている必要があります。

1 「スタート」ボタン→「コントロールパネル」の順にクリックします。

2 「ネットワークとインターネット接続」をクリックします。

3 「ネットワーク接続」をクリックします。

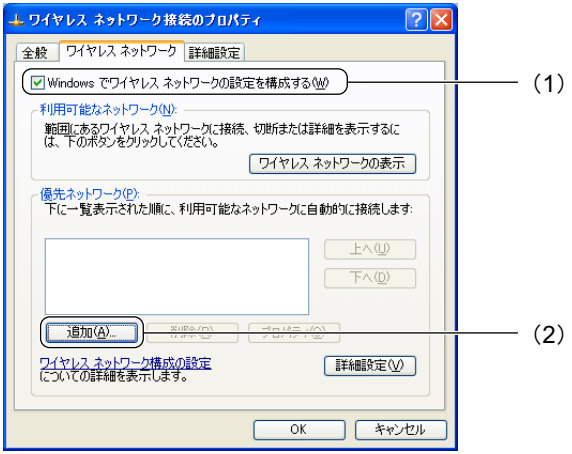
現在インストールされているネットワークの一覧が表示されます。

4 「ワイヤレスネットワーク接続」を右クリックして、表示されるメニューから「プロパティ」をクリックします。

「ワイヤレスネットワーク接続のプロパティ」ウィンドウが表示されます。

5 「ワイヤレスネットワーク」タブをクリックします。

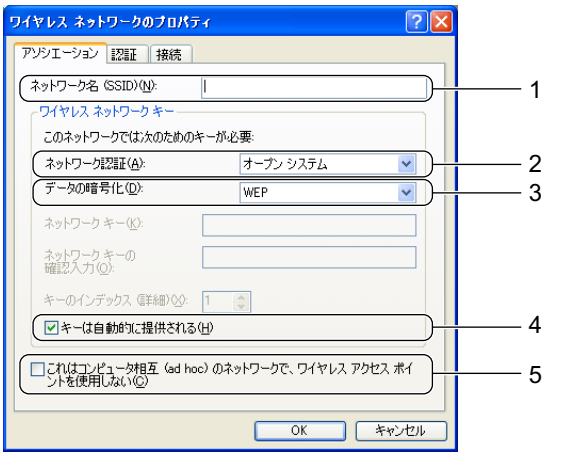
6 (1)「Windows でワイヤレス　ネットワークの設定を構成する」が☑になっていることを確認し、(2)「追加」をクリックします。



「ワイヤレス ネットワークのプロパティ」ウィンドウが表示されます。

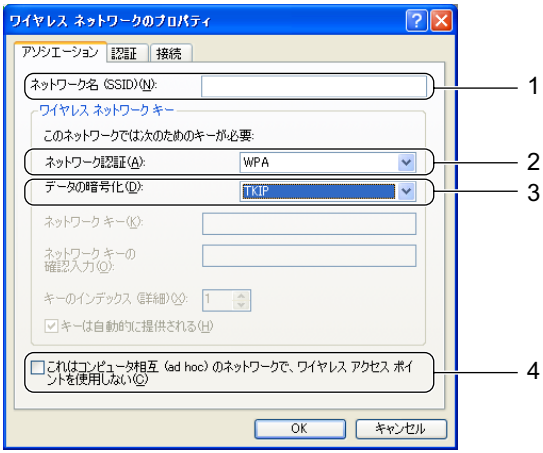
7 「アソシエーション」タブの画面で、次のように設定します。

■ IEEE 802.1X の場合



1. 「ネットワーク名（SSID)」を、接続する無線 LAN アクセスポイントに合わせて設定します（アルファベットの大文字・小文字を区別します)。
2. 「ネットワーク認証」の ⌄ をクリックして「オープンシステム」を選択します。
3. 「データの暗号化」の ⌄ をクリックして「WEP」を選択します。
4. 「キーは自動的に提供される」をクリックして☑にします。
5. 「これはコンピュータ相互（ad hoc）のネットワークで、ワイヤレス アクセス ポイントを使用しない」をクリックして☐にします。

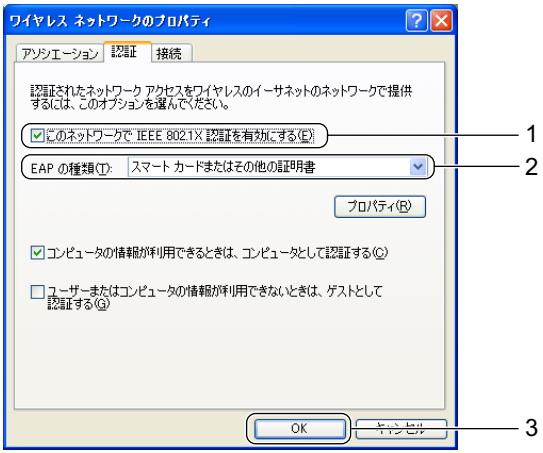
■ WPA ／ WPA2 の場合



1. 「ネットワーク名（SSID)」を、接続する無線 LAN アクセスポイントに合わせて設定します（アルファベットの大文字・小文字を区別します)。
2. 「ネットワーク認証」で、▼ をクリックして「WPA」を選択します。
3. 「データの暗号化」で、▼ をクリックして「TKIP」または「AES」を選択します。
   無線 LAN アクセスポイントに合わせて設定してください。
4. 「これはコンピュータ相互（ad hoc）のネットワークで、ワイヤレス アクセス ポイントを使用しない」をクリックして☐にします。

8 「認証」タブをクリックします。

9 次のように設定します。



1. IEEE 802.1X の場合は、「このネットワークで IEEE 802.1X を有効にする」をクリックして☑にします。
   WPA の場合、この項目は☑の状態でグレイアウト表示になっています。

2. 「EAPの種類」の から「スマートカードまたはその他の証明書」を選択します。
3. 「OK」をクリックします。
「ワイヤレス ネットワーク接続のプロパティ」ウィンドウに戻ります。

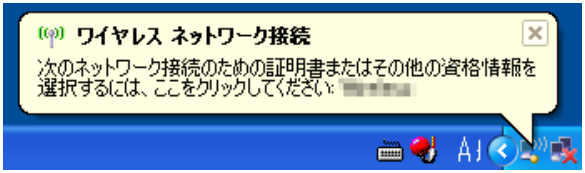
10 「優先ネットワーク」に、「ネットワーク名（SSID）」に入力したネットワーク名が追加されたことを確認して、「OK」をクリックします。

POINT

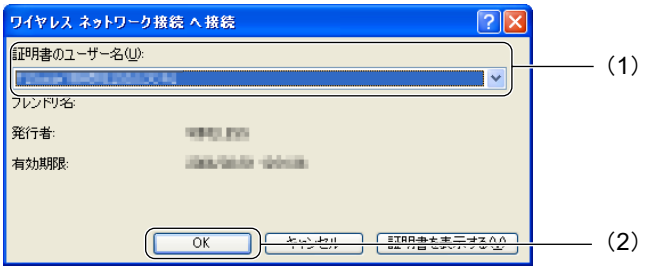
パソコンに複数の証明書をインストールしている場合

デスクトップ右下の通知領域に、メッセージが表示されるので、次のように操作してください。

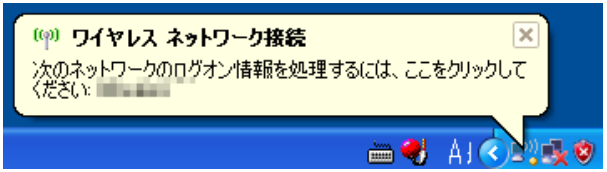
1. メッセージをクリックします。



2. （1）証明書のユーザー名を選択して、（2）「OK」をクリックします。

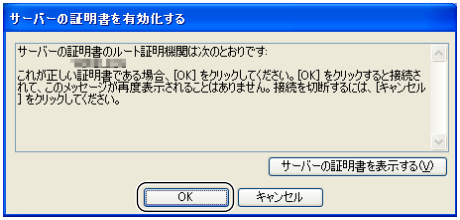


11 デスクトップ右下の通知領域に表示されるメッセージをクリックします。



「サーバーの証明書を有効化する」ウィンドウが表示されます。

12 **「OK」をクリックします。**



IEEE 802.1X ＋ PEAP-MSCHAPv2 ／ WPA ＋ PEAP-MSCHAPv2 ／ WPA2 ＋ PEAP-MSCHAPv2

次のセキュリティパターンの場合の設定方法を説明します。

・ IEEE 802.1X ＋ PEAP-MSCHAPv2
・ WPA ＋ PEAP-MSCHAPv2
・ WPA2 ＋ PEAP-MSCHAPv2

POINT

WPA2 をお使いになる場合

WPA2 の機能を使用するには Microsoft から提供されている WPA2 機能に関するプログラムが適用されている必要があります。

1 **「スタート」ボタン→「コントロールパネル」の順にクリックします。**

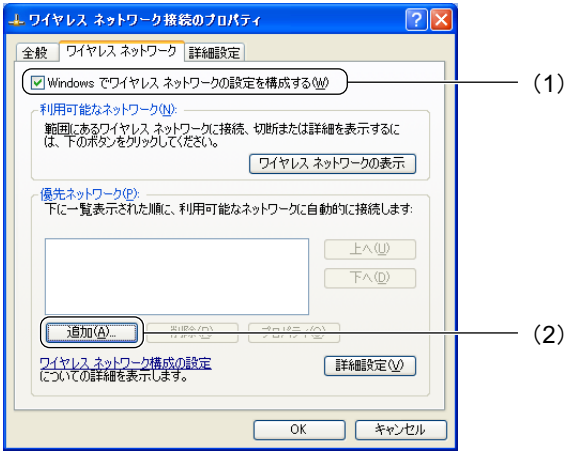
2 **「ネットワークとインターネット接続」をクリックします。**

3 **「ネットワーク接続」をクリックします。**
現在インストールされているネットワークの一覧が表示されます。

4 **「ワイヤレスネットワーク接続」を右クリックして、表示されるメニューから「プロパティ」をクリックします。**
「ワイヤレスネットワーク接続のプロパティ」ウィンドウが表示されます。

5 「ワイヤレスネットワーク」タブをクリックします。

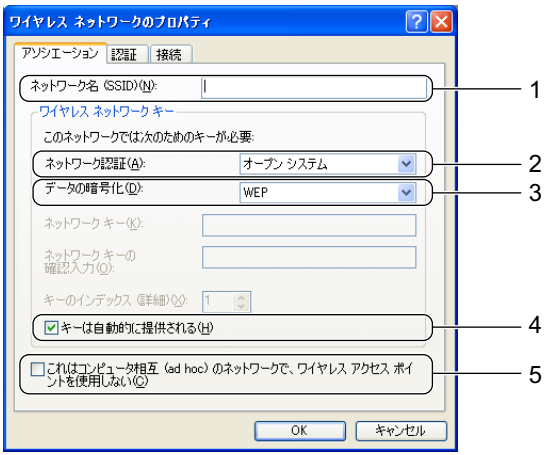
6 (1)「Windows でワイヤレス　ネットワークの設定を構成する」が☑になっていることを確認し、(2)「追加」をクリックします。



「ワイヤレス ネットワークのプロパティ」ウィンドウが表示されます。

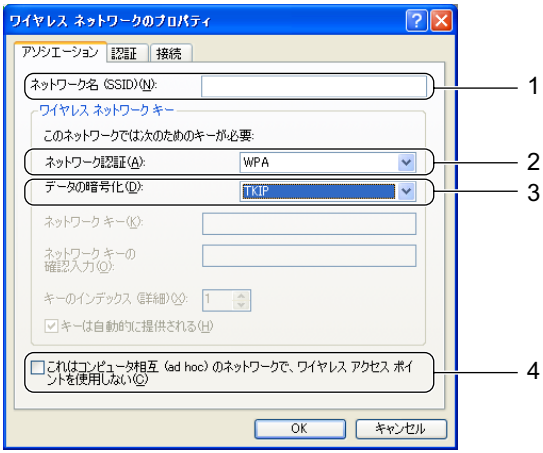
7 「アソシエーション」タブの画面で、次のように設定します。

■ IEEE 802.1X の場合



1. 「ネットワーク名（SSID)」を、接続する無線 LAN アクセスポイントに合わせて設定します（アルファベットの大文字・小文字を区別します)。
2. 「ネットワーク認証」の ⌄ をクリックして「オープンシステム」を選択します。
3. 「データの暗号化」の ⌄ をクリックして「WEP」を選択します。
4. 「キーは自動的に提供される」をクリックして☑にします。
5. 「これはコンピュータ相互（ad hoc）のネットワークで、ワイヤレス アクセスポイントを使用しない」をクリックして☐にします。

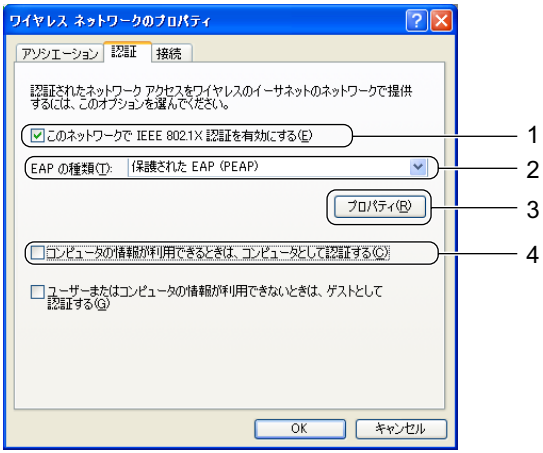
■ WPA ／ WPA2 の場合



1. 「ネットワーク名（SSID)」を、接続する無線 LAN アクセスポイントに合わせて設定します（アルファベットの大文字・小文字を区別します)。
2. 「ネットワーク認証」で、▼ をクリックして「WPA」を選択します。
3. 「データの暗号化」で、▼ をクリックして「TKIP」または「AES」を選択します。
   無線 LAN アクセスポイントに合わせて設定してください。
4. 「これはコンピュータ相互（ad hoc）のネットワークで、ワイヤレス アクセス ポイントを使用しない」をクリックして☐にします。

8 「認証」タブをクリックします。

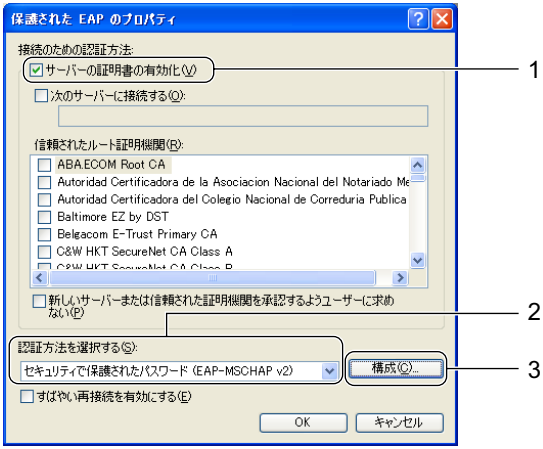
9 次のように設定します。



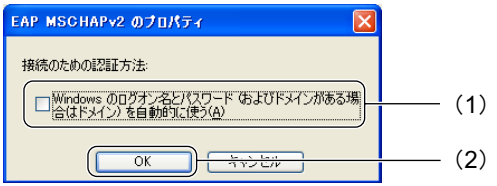
1. IEEE 802.1X の場合は、「このネットワークで IEEE 802.1X を有効にする」をクリックして☑にします。
   WPA の場合、この項目は☑の状態でグレイアウト表示になっています。

2. 「コンピュータの情報が利用できるときは、コンピュータとして認証する」をクリックして☐にします。
3. 「EAP の種類」の ⌄ をクリックして、「保護された EAP（PEAP）」を選択します。
4. 「プロパティ」をクリックします。
   「保護された EAP のプロパティ」ウィンドウが表示されます。

10 次のように操作します。



1. 「サーバーの証明書を有効化する」が☑になっていることを確認します。
2. 「認証方法を選択する」で、「セキュリティで保護されたパスワード（EAP-MSCHAP v2）」が選択されていることを確認します。
3. 「構成」をクリックします。
   「EAP MSCHAPv2 のプロパティ」ウィンドウが表示されます。
4. 接続時にユーザー名とパスワードの入力を行う場合は、（1）「Windows のログオン名とパスワード（およびドメインがある場合はドメイン）を自動的に使う」をクリックして☐にし、（2）「OK」をクリックします。



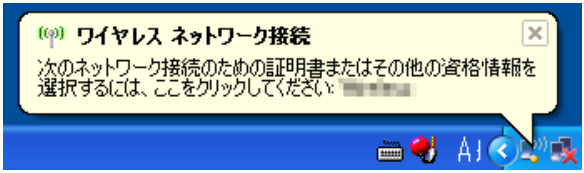
11 「保護された EAP のプロパティ」ウィンドウで「OK」をクリックします。

12 「ワイヤレス ネットワークのプロパティ」ウィンドウで「OK」をクリックします。

「ワイヤレス ネットワーク接続のプロパティ」ウィンドウに戻ります。

13 **「優先ネットワーク」に、「ネットワーク名（SSID）」に入力したネットワーク名が追加されたことを確認して、「OK」をクリックします。**

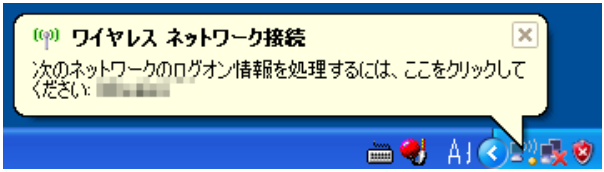
14 **デスクトップ右下の通知領域にされるメッセージをクリックします。**



15 **（1）ユーザー名、パスワード、ログオンドメインを入力して、（2）「OK」をクリックします。**

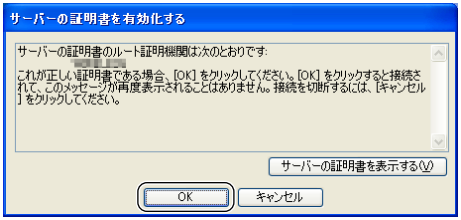
ユーザー名、パスワード、ログオンドメインは、ネットワーク管理者にご確認ください。

16 **デスクトップ右下の通知領域に表示されるメッセージをクリックします。**



「サーバーの証明書を有効化する」ウィンドウが表示されます。

17 **「OK」をクリックします。**



IEEE 802.1X ＋ PEAP-TLS ／ WPA ＋ PEAP-TLS ／ WPA2 ＋ PEAP-TLS

次のセキュリティパターンの場合の設定方法を説明します。

・IEEE 802.1X ＋ PEAP-TLS
・WPA ＋ PEAP-TLS
・WPA2 ＋ PEAP-TLS

POINT

WPA2 をお使いになる場合

WPA2 の機能を使用するには Microsoft から提供されている WPA2 機能に関するプログラムが適用されている必要があります。

1 **「スタート」ボタン→「コントロールパネル」の順にクリックします。**

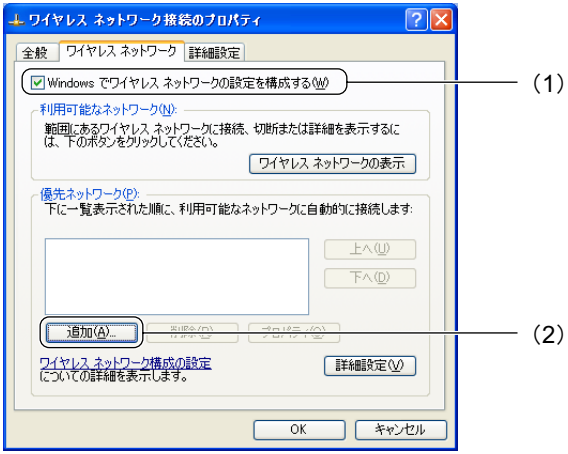
2 **「ネットワークとインターネット接続」をクリックします。**

3 **「ネットワーク接続」をクリックします。**
現在インストールされているネットワークの一覧が表示されます。

4 **「ワイヤレスネットワーク接続」を右クリックして、表示されるメニューから「プロパティ」をクリックします。**
「ワイヤレスネットワーク接続のプロパティ」ウィンドウが表示されます。

5 「ワイヤレスネットワーク」タブをクリックします。

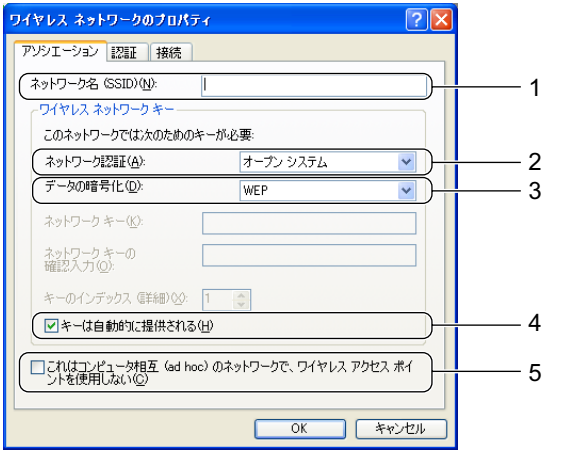
6 (1)「Windows でワイヤレス　ネットワークの設定を構成する」が☑になっていることを確認し、(2)「追加」をクリックします。



「ワイヤレス ネットワークのプロパティ」ウィンドウが表示されます。

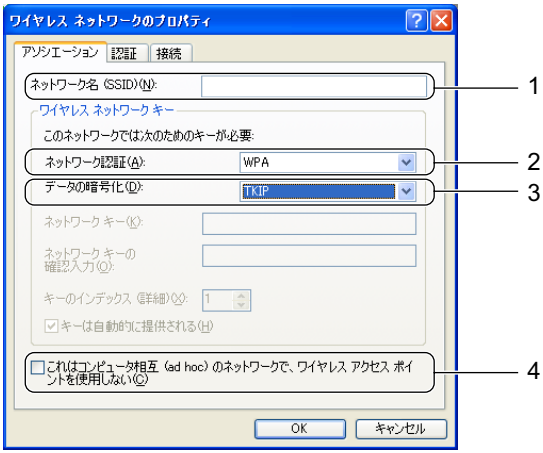
7 「アソシエーション」タブの画面で、次のように設定します。

■ IEEE 802.1X の場合



1. 「ネットワーク名（SSID)」を、接続する無線 LAN アクセスポイントに合わせて設定します（アルファベットの大文字・小文字を区別します)。
2. 「ネットワーク認証」の ⌄ をクリックして「オープンシステム」を選択します。
3. 「データの暗号化」の ⌄ をクリックして「WEP」を選択します。
4. 「キーは自動的に提供される」をクリックして☑にします。
5. 「これはコンピュータ相互（ad hoc）のネットワークで、ワイヤレス アクセス ポイントを使用しない」をクリックして☐にします。

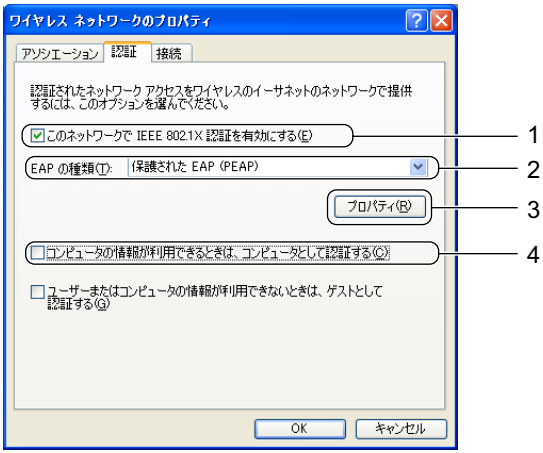
■ WPA ／ WPA2 の場合



1. 「ネットワーク名（SSID)」を、接続する無線 LAN アクセスポイントに合わせて設定します（アルファベットの大文字・小文字を区別します)。
2. 「ネットワーク認証」で、 をクリックして「WPA」を選択します。
3. 「データの暗号化」で、 をクリックして「TKIP」または「AES」を選択します。
   無線 LAN アクセスポイントに合わせて設定してください。
4. 「これはコンピュータ相互（ad hoc）のネットワークで、ワイヤレス アクセス ポイントを使用しない」をクリックして☐にします。

8 「認証」タブをクリックします。

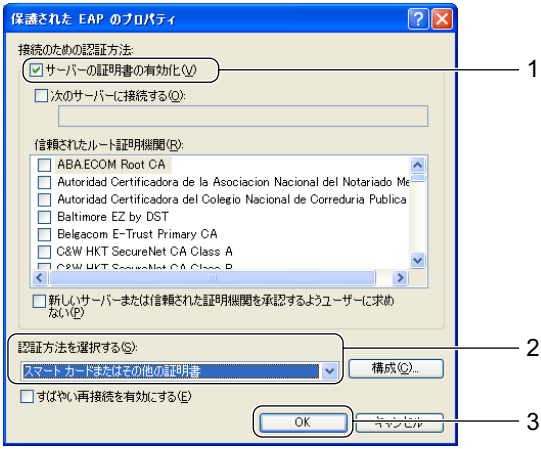
9 次のように設定します。



1. IEEE 802.1X の場合は、「このネットワークで IEEE 802.1X を有効にする」をクリックして☑にします。
   WPA の場合、この項目は☑の状態でグレイアウト表示になっています。

2. 「コンピュータの情報が利用できるときは、コンピュータとして認証する」をクリックして☐にします。
3. 「EAP の種類」の⌄をクリックして、「保護された EAP (PEAP)」を選択します。
4. 「プロパティ」をクリックします。
「保護された EAP のプロパティ」ウィンドウが表示されます。

10 次のように操作します。



1. 「サーバーの証明書を有効化する」が☑になっていることを確認します。
2. 「認証方法を選択する」の⌄をクリックして、「スマートカードまたはその他の証明書」を選択します。
3. 「OK」をクリックします。

11 「ワイヤレス ネットワークのプロパティ」ウィンドウで「OK」をクリックします。

「ワイヤレス ネットワーク接続のプロパティ」ウィンドウに戻ります。

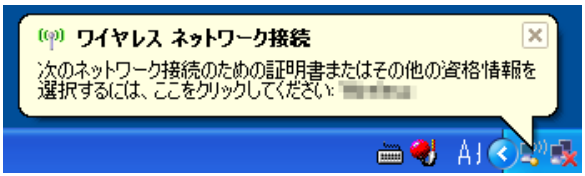
12 「優先ネットワーク」に、「ネットワーク名 (SSID)」に入力したネットワーク名が追加されたことを確認して、「OK」をクリックします。

POINT

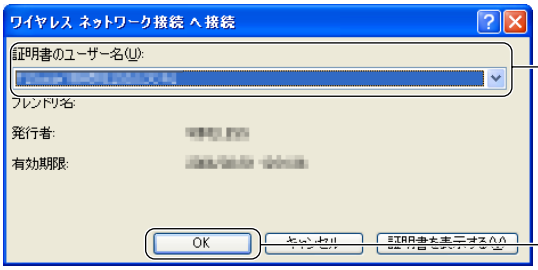
パソコンに複数の証明書をインストールしている場合

デスクトップ右下の通知領域に、メッセージが表示されるので、次のように操作してください。

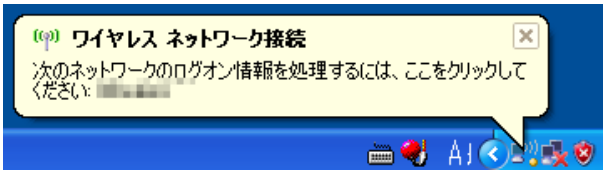
1. メッセージをクリックします。



2. (1) 証明書のユーザー名を選択して、(2)「OK」をクリックします。

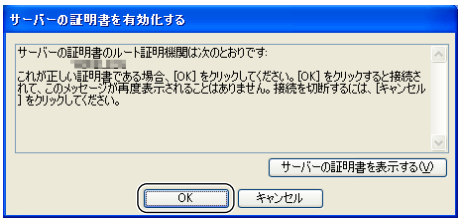


13 **デスクトップ右下の通知領域に表示されるメッセージをクリックします。**



「サーバーの証明書を有効化する」ウィンドウが表示されます。

14 **「OK」をクリックします。**



WPA-PSK ／ WPA2-PSK

WPA-PSK ／ WPA2-PSK の場合の設定方法を説明します。

POINT

WPA2 をお使いになる場合

WPA2 の機能を使用するには Microsoft から提供されている WPA2 機能に関するプログラムが適用されている必要があります。

1 **「スタート」ボタン→「コントロールパネル」の順にクリックします。**

2 **「ネットワークとインターネット接続」をクリックします。**

3 **「ネットワーク接続」をクリックします。**

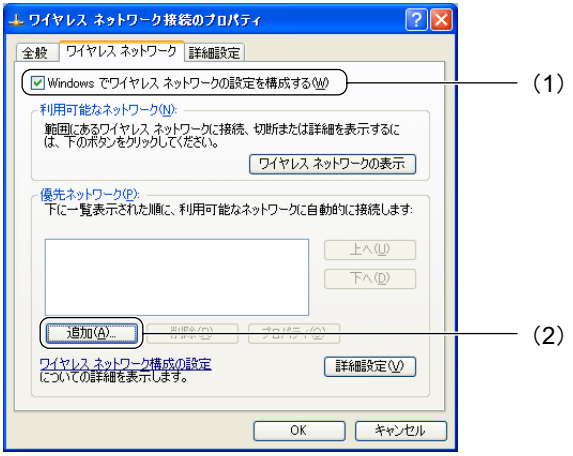
現在インストールされているネットワークの一覧が表示されます。

4 **「ワイヤレスネットワーク接続」を右クリックして、表示されるメニューから「プロパティ」をクリックします。**

「ワイヤレスネットワーク接続のプロパティ」ウィンドウが表示されます。

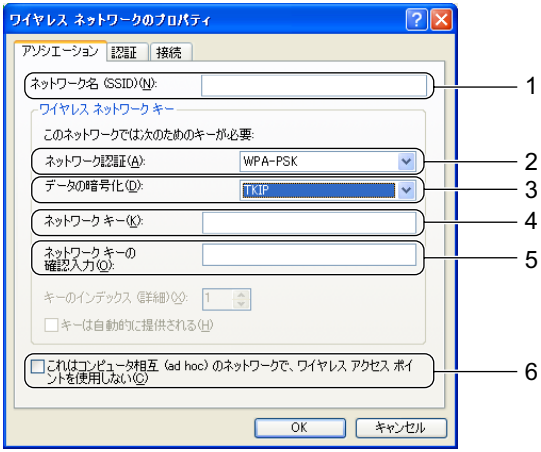
5 **「ワイヤレスネットワーク」タブをクリックします。**

6 **(1)「Windows でワイヤレス　ネットワークの設定を構成する」が☑になっていることを確認し、(2)「追加」をクリックします。**



「ワイヤレス ネットワークのプロパティ」ウィンドウが表示されます。

7 **「アソシエーション」タブの画面で、次のように設定します。**



1. 「ネットワーク名（SSID)」を接続する無線 LAN アクセスポイントに合わせて設定します（アルファベットの大文字・小文字を区別します)。
2. 「ネットワーク認証」で、▼をクリックして「WPA-PSK」を選択します。

3. 「データの暗号化」で、 をクリックして「TKIP」または「AES」を選択します。
   無線 LAN アクセスポイントに合わせて設定してください。
4. 「ネットワークキー」に、無線 LAN アクセスポイントと同じ WPA-PSK の値を入力します。
   次のいずれかで入力します。
   ・ASCII 文字を、8 ～ 63 文字の範囲で入力します。使用できる文字は次の通りです。
   0～9、a～z、A～Z（アルファベットの大文字・小文字を区別します）、半角記号
   ・16 進数を、64 文字で入力します。使用できる文字は次の通りです。
   0 ～ 9、A ～ F、a ～ f（アルファベットの大文字・小文字を区別しません）
5. 「ネットワークキーの確認入力」に、確認のため、「ネットワークキー」に入力した値と同じ値を入力します。
6. 「これはコンピュータ相互（ad hoc）のネットワークで、ワイヤレス アクセスポイントを使用しない」をクリックして☐にします。

8 **「OK」をクリックします。**

9 **(1)「優先ネットワーク」に、「ネットワーク名（SSID)」に入力したネットワーク名が追加されたことを確認して、(2)「OK」をクリックします。**

11 Plugfree NETWORK を使った設定

無線 LAN の設定に、Plugfree NETWORK を使用する場合の設定方法を説明します。

IEEE 802.1X ＋ EAP-TLS ／ WPA ＋ EAP-TLS ／ WPA2 ＋ EAP-TLS

次のセキュリティパターンの場合の設定方法を説明します。

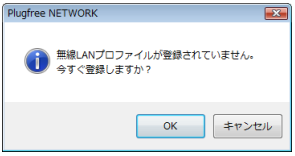
・IEEE 802.1X ＋ EAP-TLS
・WPA ＋ EAP-TLS（WPA エンタープライズ EAP-TLS）
・WPA2 ＋ EAP-TLS（WPA2 エンタープライズ EAP-TLS）

1 画面右下の通知領域にある Plugfree NETWORK のアイコンをダブルクリックします。

「使用場所管理」画面が表示されます。

POINT

・画面右下の通知領域にある Plugfree NETWORK のアイコンを右クリックして表示されるメニューから「管理画面」をクリックしても「使用場所管理」画面が表示されます。
・次の画面が表示された場合は「OK」をクリックして、手順 4 へお進みください。



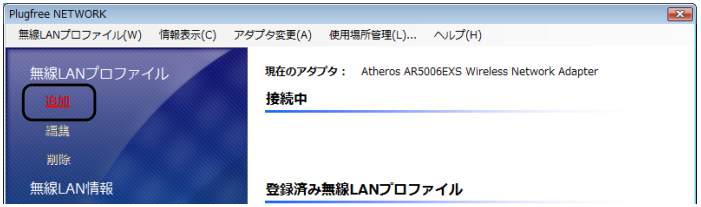
2 「使用場所管理」画面で「無線 LAN 管理」をクリックします。

「無線 LAN 管理」画面が表示されます。

3 次のように操作します。

■ 新規作成の場合

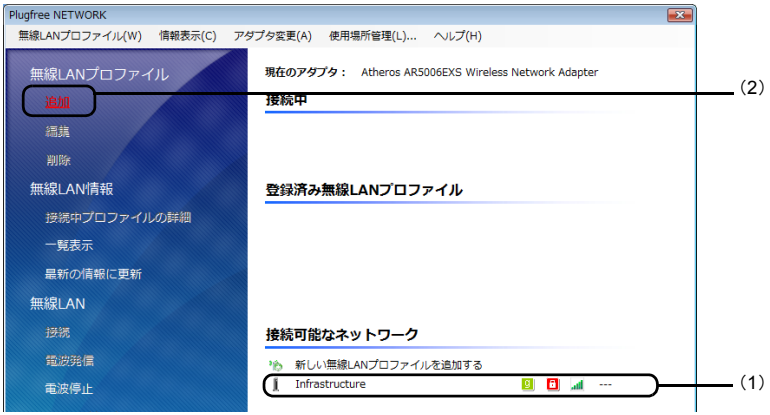
「無線 LAN 管理」画面で「追加」をクリックします。



手順 4 に進みます。

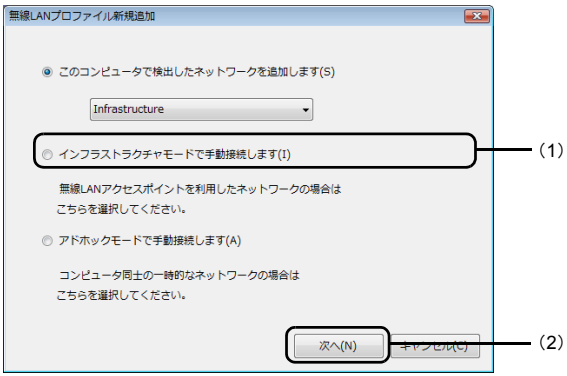
■「接続可能なネットワーク」から追加する場合

(1)「無線 LAN 管理」画面の右ペインの「接続可能なネットワーク」から、追加する無線 LAN プロファイルを選択して、(2)「追加」をクリックします。

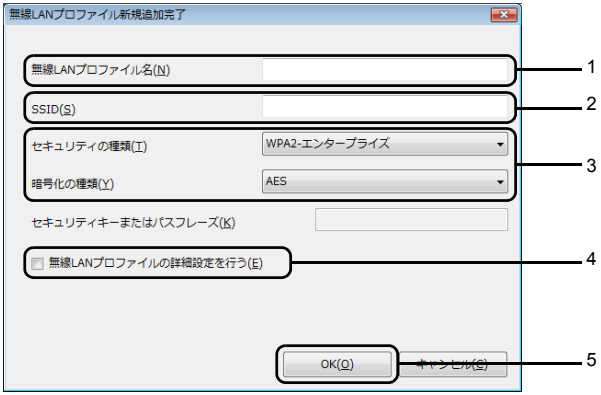


手順 5 に進みます。

4 (1)「インフラストラクチャモードで手動接続します」を選択して、(2)「次へ」をクリックます。



5 無線 LAN プロファイルのセキュリティを設定します。

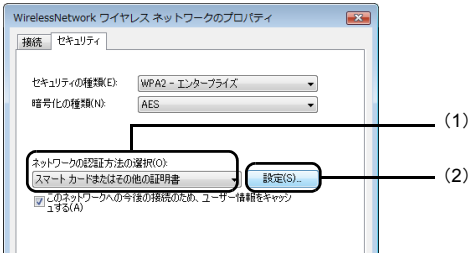


手順 3 で「接続可能なネットワーク」から追加した場合は、一部、設定済みの項目があります。

1. **「無線 LAN プロファイル名」を設定します。**
   このネットワーク設定の識別名を 1 ～ 128 文字で設定します。
   使用できる文字は、全角文字、全角記号、全角スペース、半角英数カナ文字、半角スペース、半角のハイフン（-）、アンダーバー（_）です。
2. **「SSID」を設定します。**
   インフラストラクチャモードの場合は、接続する無線 LAN アクセスポイントに設定されている SSID（または ESSID）と同じ値を設定します。
3. **「セキュリティの種類」と「暗号化の種類」を設定します。**
   お使いになる環境、無線 LAN アクセスポイントに合わせて設定してください。
   IEEE 802.1X の場合
   1. 「セキュリティの種類」で「802.1x」を選択します。
      「暗号化の種類」は自動的に「WEP」が選択されます。

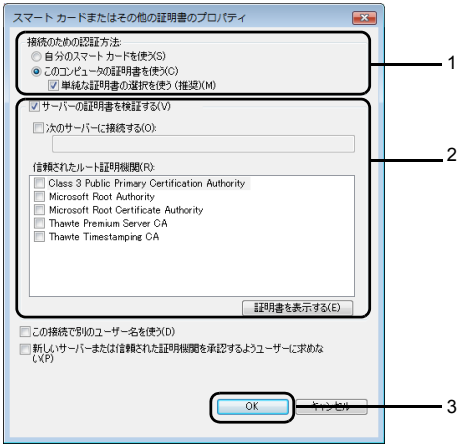
   WPA ／ WPA2 の場合
   1. 「セキュリティの種類」で「WPA- エンタープライズ」または「WPA2 エンタープライズ」を選択します。
   2. 「暗号化の種類」で「TKIP」または「AES」を選択します。
4. **「無線 LAN プロファイルの詳細設定を行う」の☐をクリックして☑にします。**
5. **「OK」をクリックします。**

6 (1)「ネットワークの認証方法の選択」で「スマートカードまたはその他の証明書」を選択し、(2)「設定」をクリックします。



「スマートカードまたはその他の証明書のプロパティ」ウィンドウが表示されます。

7 詳細設定を行います。



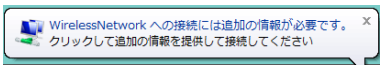
1. 認証方法を選択します。
2. 必要に応じて認証サーバの設定をします。
3. 「OK」をクリックします。

8 「ワイヤレスネットワークのプロパティ」ウィンドウで「OK」をクリックします。

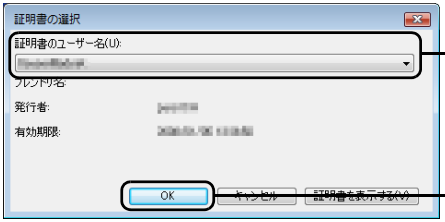
POINT

パソコンに複数の証明書をインストールしている場合

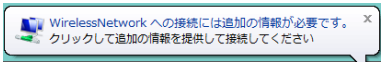
1. デスクトップ右下の通知領域に表示されるメッセージをクリックします。



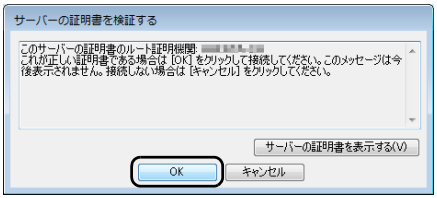
2. (1) 証明書のユーザー名を選択して、(2)「OK」をクリックします。



9 **デスクトップ右下の通知領域に表示されるメッセージをクリックします。**



10 **「OK」をクリックします。**



使用場所情報の追加などについては、「Plugfree NETWORK」のヘルプをご覧ください。

IEEE 802.1X ＋ PEAP-MSCHAPv2 ／ WPA ＋ PEAP-MSCHAPv2 ／ WPA2 ＋ PEAP-MSCHAPv2

次のセキュリティパターンの場合の設定方法を説明します。

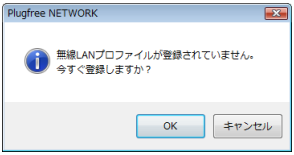
- IEEE 802.1X ＋ PEAP-MSCHAPv2
- WPA ＋ PEAP-MSCHAPv2（WPA エンタープライズ PEAP-MSCHAP v2）
- WPA2 ＋ PEAP-MSCHAPv2（WPA2 エンタープライズ PEAP-MSCHAP v2）

1 **画面右下の通知領域にある Plugfree NETWORK のアイコンをダブルクリックします。**

「使用場所管理」画面が表示されます。

POINT

- 画面右下の通知領域にある Plugfree NETWORK のアイコンを右クリックして表示されるメニューから「管理画面」をクリックしても「使用場所管理」画面が表示されます。
- 次の画面が表示された場合は「OK」をクリックして、手順 4 へお進みください。



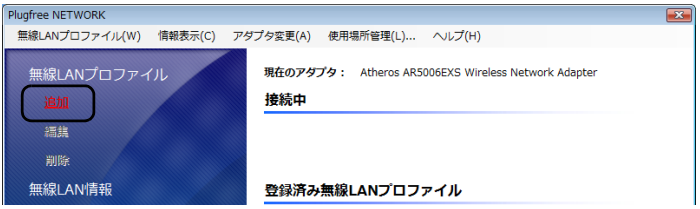
2 「使用場所管理」画面で「無線 LAN 管理」をクリックします。

「無線 LAN 管理」画面が表示されます。

3 次のように操作します。

■ 新規作成の場合

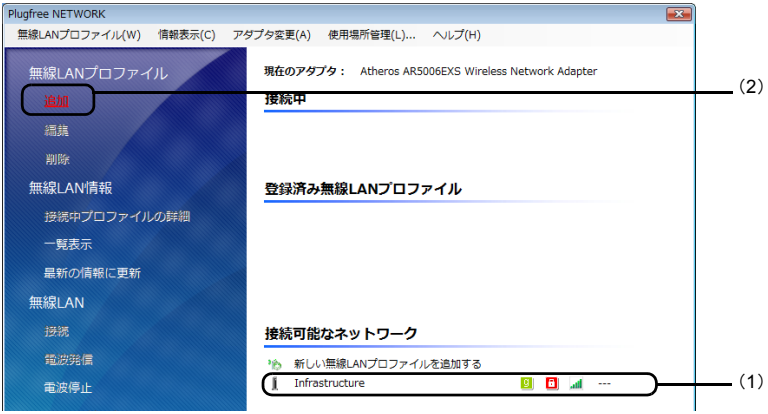
「無線 LAN 管理」画面で「追加」をクリックします。



手順 4 に進みます。

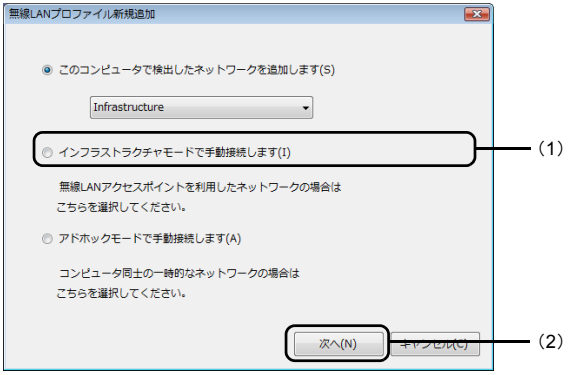
■「接続可能なネットワーク」から追加する場合

(1)「無線 LAN 管理」画面の右ペインの「接続可能なネットワーク」から、追加する無線 LAN プロファイルを選択して、(2)「追加」をクリックします。

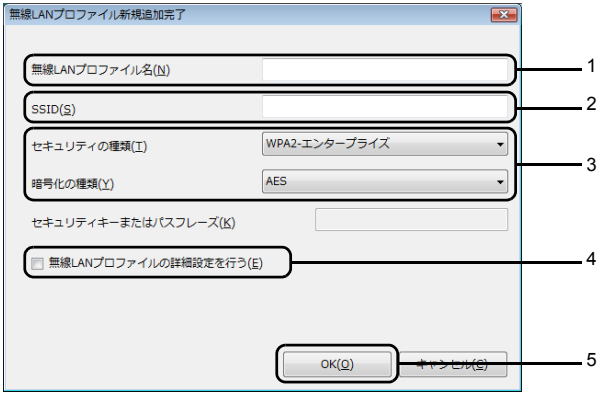


手順 5 に進みます。

4 (1)「インフラストラクチャモードで手動接続します」を選択して、(2)「次へ」をクリックます。



5 無線 LAN プロファイルのセキュリティを設定します。



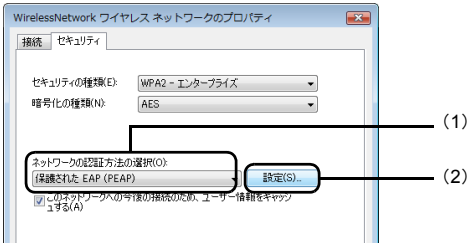
手順 3 で「接続可能なネットワーク」から追加した場合は、一部、設定済みの項目があります。

1. **「無線 LAN プロファイル名」を設定します。**
   このネットワーク設定の識別名を 1 ～ 128 文字で設定します。
   使用できる文字は、全角文字、全角記号、全角スペース、半角英数カナ文字、半角スペース、半角のハイフン（-）、アンダーバー（_）です。
2. **「SSID」を設定します。**
   インフラストラクチャモードの場合は、接続する無線 LAN アクセスポイントに設定されている SSID（または ESSID）と同じ値を設定します。
3. **「セキュリティの種類」と「暗号化の種類」を設定します。**
   お使いになる環境、無線 LAN アクセスポイントに合わせて設定してください。
   IEEE 802.1X の場合
   1. 「セキュリティの種類」で「802.1x」を選択します。
      「暗号化の種類」は自動的に「WEP」が選択されます。
   WPA ／ WPA2 の場合

1.「セキュリティの種類」で「WPA- エンタープライズ」または「WPA2 エンタープライズ」を選択します。
2.「暗号化の種類」で「TKIP」または「AES」を選択します。

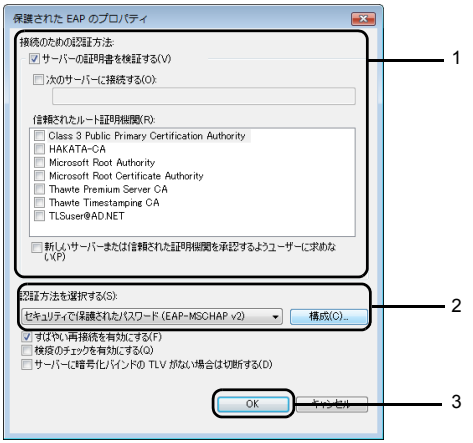
4.「無線 LAN プロファイルの詳細設定を行う」の☐をクリックして☑にします。
5.「OK」をクリックします。

6 (1)「ネットワークの認証方法の選択」で「保護された EAP（PEAP)」を選択し、(2)「設定」をクリックします。



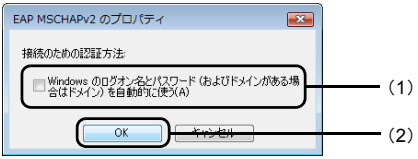
「保護された EAP のプロパティ」ウィンドウが表示されます。

7 詳細設定を行います。



1. 必要に応じて認証サーバーの設定をします。
2.「認証方法を選択する」で「セキュリティで保護されたパスワード（EAP-MSCHAP v2)」を選択し、「構成」をクリックします。
「EAP MSCHAPv2 のプロパティ」ウィンドウが表示されます。

3. (1)「Windows のログオン名とパスワード（およびドメインがある場合はドメイン）を自動的に使う」をクリックして にし、(2)「OK」をクリックします。

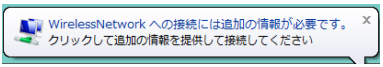


注 1　シングルサインオンを使用する場合は、パソコンをドメインに参加させたうえでこのチェックをつけた無線LANのプロファイルを共有プロファイルとして作成してください。

4.「保護された EAP のプロパティ」ウィンドウで「OK」をクリックします。

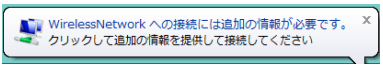
8「ワイヤレスネットワークのプロパティ」ウィンドウで「OK」をクリックします。

9 デスクトップ右下の通知領域に表示されるメッセージをクリックします。

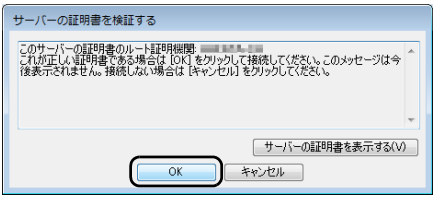


10 (1)「ユーザー名」と「パスワード」を入力し、(2)「OK」をクリックします。

11 デスクトップ右下の通知領域に表示されるメッセージをクリックします。



12「OK」をクリックします。



使用場所情報の追加などについては、「Plugfree NETWORK」のヘルプをご覧ください。

IEEE 802.1X ＋ PEAP-TLS ／ WPA ＋ PEAP-TLS ／ WPA2 ＋ PEAP-TLS

次のセキュリティパターンの場合の設定方法を説明します。

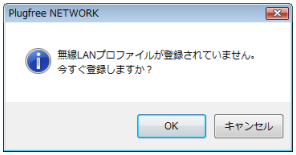
- IEEE 802.1X ＋ PEAP-TLS
- WPA ＋ PEAP-TLS（WPA エンタープライズ PEAP-TLS）
- WPA2 ＋ PEAP-TLS（WPA2 エンタープライズ PEAP-TLS）

1 画面右下の通知領域にある Plugfree NETWORK のアイコンをダブルクリックします。

「使用場所管理」画面が表示されます。

POINT

- 画面右下の通知領域にある Plugfree NETWORK のアイコンを右クリックして表示されるメニューから「管理画面」をクリックしても「使用場所管理」画面が表示されます。
- 次の画面が表示された場合は「OK」をクリックして、手順 4 へお進みください。



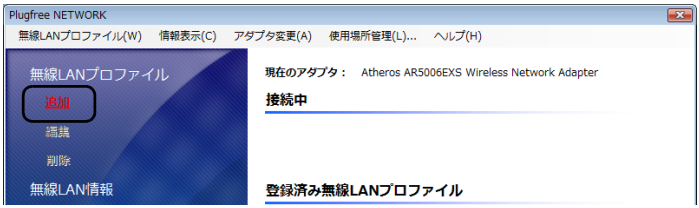
2 「使用場所管理」画面で「無線 LAN 管理」をクリックします。

「無線 LAN 管理」画面が表示されます。

3 次のように操作します。

■ 新規作成の場合

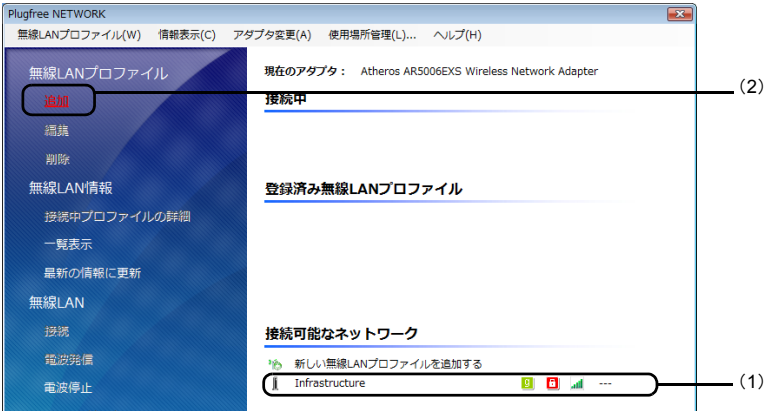
「無線 LAN 管理」画面で「追加」をクリックします。



手順 4 に進みます。

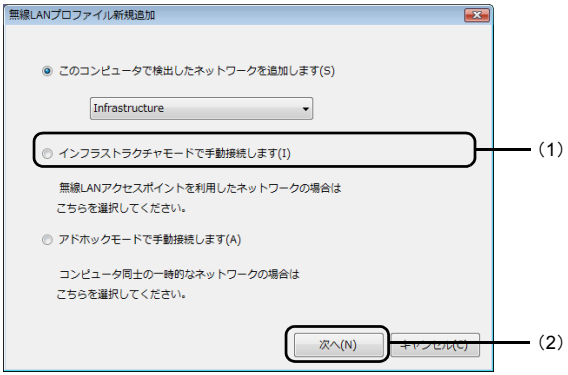
■「接続可能なネットワーク」から追加する場合

(1)「無線 LAN 管理」画面の右ペインの「接続可能なネットワーク」から、追加する無線 LAN プロファイルを選択して、(2)「追加」をクリックします。

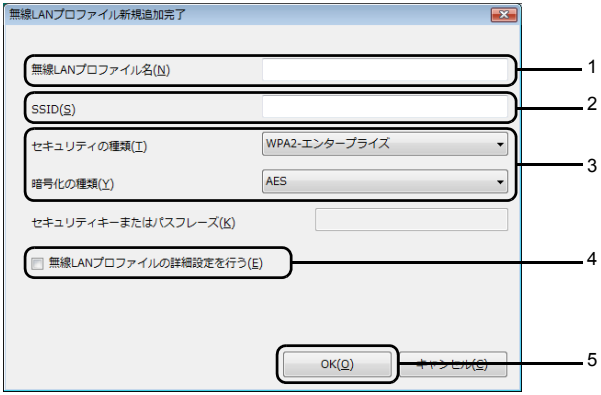


手順 5 に進みます。

4 (1)「インフラストラクチャモードで手動接続します」を選択して、(2)「次へ」をクリックます。



5 無線 LAN プロファイルのセキュリティを設定します。

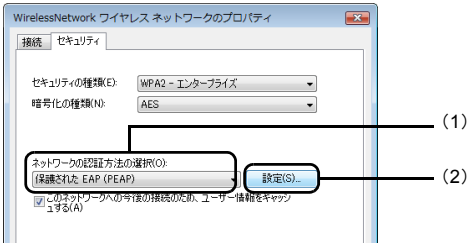


手順 3 で「接続可能なネットワーク」から追加した場合は、一部、設定済みの項目があります。

1. **「無線 LAN プロファイル名」を設定します。**
   このネットワーク設定の識別名を 1 ～ 128 文字で設定します。
   使用できる文字は、全角文字、全角記号、全角スペース、半角英数カナ文字、半角スペース、半角のハイフン（-）、アンダーバー（_）です。
2. **「SSID」を設定します。**
   インフラストラクチャモードの場合は、接続する無線 LAN アクセスポイントに設定されている SSID（または ESSID）と同じ値を設定します。
3. **「セキュリティの種類」と「暗号化の種類」を設定します。**
   お使いになる環境、無線 LAN アクセスポイントに合わせて設定してください。
   IEEE 802.1X の場合
   1. 「セキュリティの種類」で「802.1x」を選択します。
      「暗号化の種類」は自動的に「WEP」が選択されます。

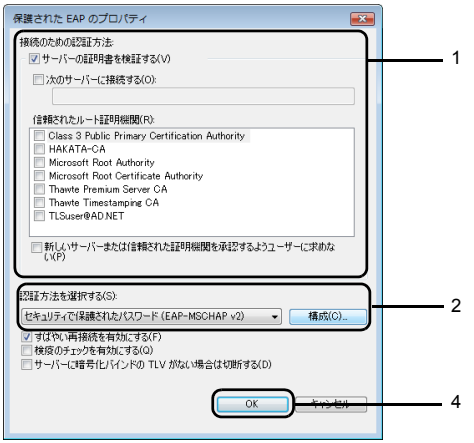
   WPA ／ WPA2 の場合
   1. 「セキュリティの種類」で「WPA- エンタープライズ」または「WPA2 エンタープライズ」を選択します。
   2. 「暗号化の種類」で「TKIP」または「AES」を選択します。
4. **「無線 LAN プロファイルの詳細設定を行う」の☐をクリックして☑にします。**
5. **「OK」をクリックします。**

6 (1)「ネットワークの認証方法の選択」で「保護された EAP（PEAP)」を選択し、(2)「設定」をクリックします。



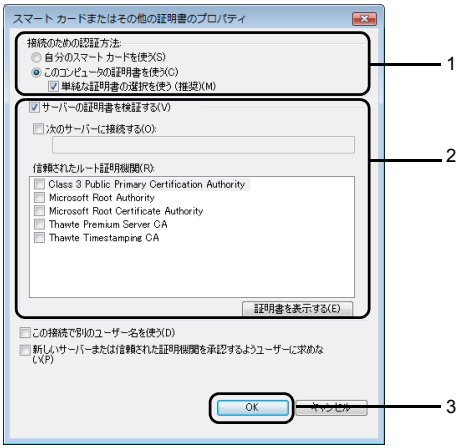
「保護された EAP のプロパティ」ウィンドウが表示されます。

7 詳細設定を行います。



1. 必要に応じて認証サーバーの設定をします。
2. 「認証方法を選択する」で「スマートカードまたはその他の証明書」を選択し、「構成」をクリックします。
   「スマートカードまたはその他の証明書のプロパティ」ウィンドウが表示されます。

3. 詳細設定を行います。



1. 認証方法を選択します。
2. 必要に応じて認証サーバーの設定をします。
3. 「OK」をクリックします。

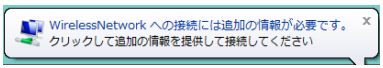
4. 「保護された EAP のプロパティ」ウィンドウで「OK」をクリックします。

8 「ワイヤレスネットワークのプロパティ」ウィンドウで「OK」をクリックします。

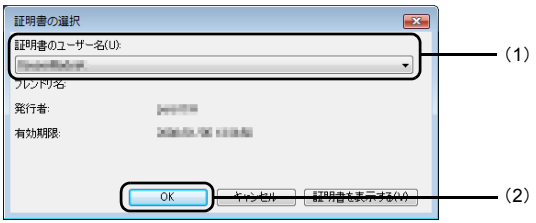
POINT

パソコンに複数の証明書をインストールしている場合

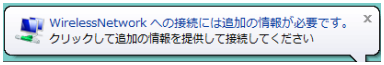
1. デスクトップ右下の通知領域に表示されるメッセージをクリックします。



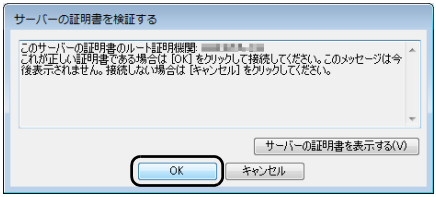
2. (1) 証明書のユーザー名を選択して、(2)「OK」をクリックします。



9 デスクトップ右下の通知領域に表示されるメッセージをクリックします。



10 **「OK」をクリックします。**



使用場所情報の追加などについては、「Plugfree NETWORK」のヘルプをご覧ください。

WPA-PSK ／ WPA2-PSK

次のセキュリティパターンの場合の設定方法を説明します。

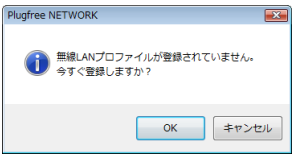
・WPA-PSK（WPA パーソナル）
・WPA2-PSK（WPA2 パーソナル）

1 **画面右下の通知領域にある Plugfree NETWORK のアイコンをダブルクリックします。**

「使用場所管理」画面が表示されます。

POINT

・画面右下の通知領域にある Plugfree NETWORK のアイコンを右クリックして表示されるメニューから「管理画面」をクリックしても「使用場所管理」画面が表示されます。
・次の画面が表示された場合は「OK」をクリックして、手順 4 へお進みください。



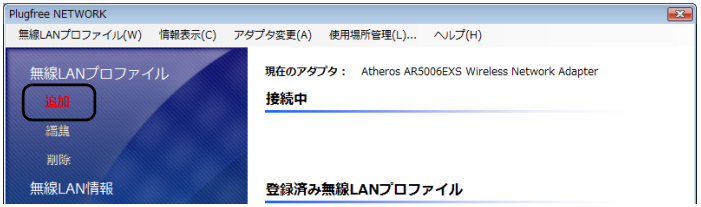
2 **「使用場所管理」画面で「無線 LAN 管理」をクリックします。**

「無線 LAN 管理」画面が表示されます。

3 次のように操作します。

■ 新規作成の場合

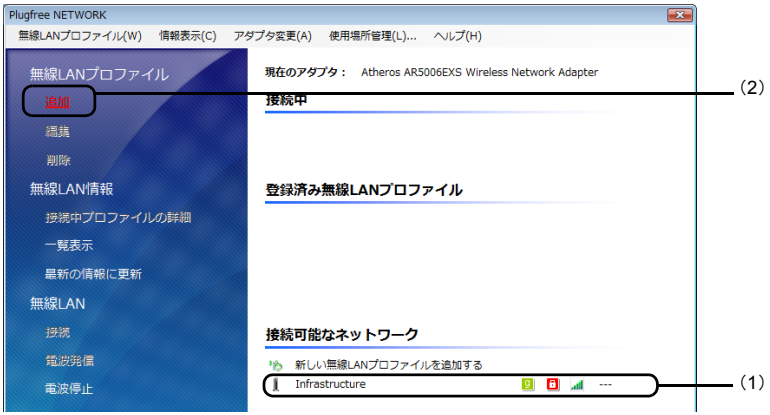
「無線 LAN 管理」画面で「追加」をクリックします。



手順 4 に進みます。

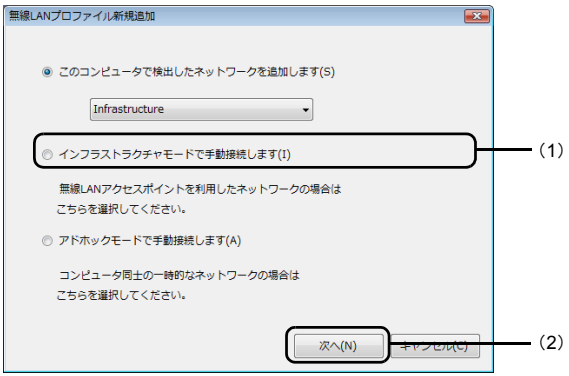
■「接続可能なネットワーク」から追加する場合

(1)「無線 LAN 管理」画面の右ペインの「接続可能なネットワーク」から、追加する無線 LAN プロファイルを選択して、(2)「追加」をクリックします。

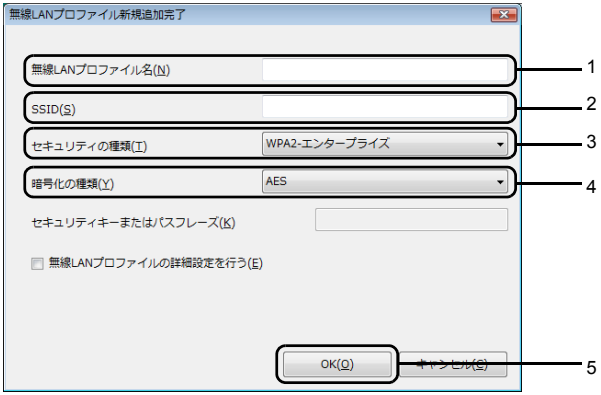


手順 5 に進みます。

4 (1)「インフラストラクチャモードで手動接続します」を選択して、(2)「次へ」をクリックます。



5 無線 LAN プロファイルのセキュリティを設定します。



手順 3 で「接続可能なネットワーク」から追加した場合は、一部、設定済みの項目があります。

1. **「無線 LAN プロファイル名」を設定します。**
   このネットワーク設定の識別名を 1 ～ 128 文字で設定します。
   使用できる文字は、全角文字、全角記号、全角スペース、半角英数カナ文字、半角スペース、半角のハイフン（-）、アンダーバー（_）です。
2. **「SSID」を設定します。**
   インフラストラクチャモードの場合は、接続する無線 LAN アクセスポイントに設定されている SSID（または ESSID）と同じ値を設定します。
3. **「セキュリティの種類」を設定します。**
   「WPA パーソナル」または「WPA2 パーソナル」を選択します。
   お使いになる環境、無線 LAN アクセスポイントに合わせて設定してください。
4. **「暗号化の種類」を選択します。**
   「TKIP」または「AES」を選択します。
   お使いになる環境、無線 LAN アクセスポイントに合わせて設定してください。
5. **「OK」をクリックします。**

使用場所情報の追加などについては、「Plugfree NETWORK」のヘルプをご覧ください。

12 Windows Vista 標準の無線 LAN 機能を使った設定

無線 LAN の設定に、Windows Vista 標準の無線 LAN 機能（WLAN Auto Config）を使用する場合の設定方法を説明します。

IEEE 802.1X ＋ EAP-TLS ／ WPA ＋ EAP-TLS ／ WPA2 ＋ EAP-TLS

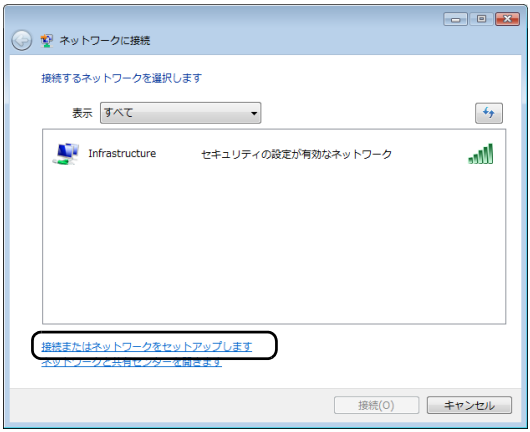
次のセキュリティパターンの場合の設定方法を説明します。

- IEEE 802.1X ＋ EAP-TLS
- WPA ＋ EAP-TLS（WPA エンタープライズ EAP-TLS）
- WPA2 ＋ EAP-TLS（WPA2 エンタープライズ EAP-TLS）

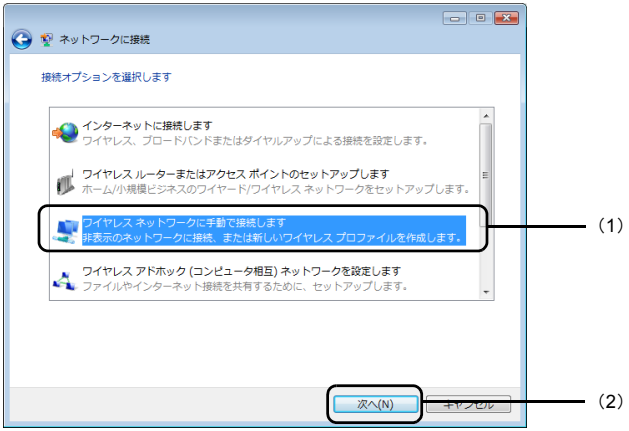
1 **（スタート）→「接続先」の順にクリックします。**

「ネットワークに接続」ウィンドウが表示されます。

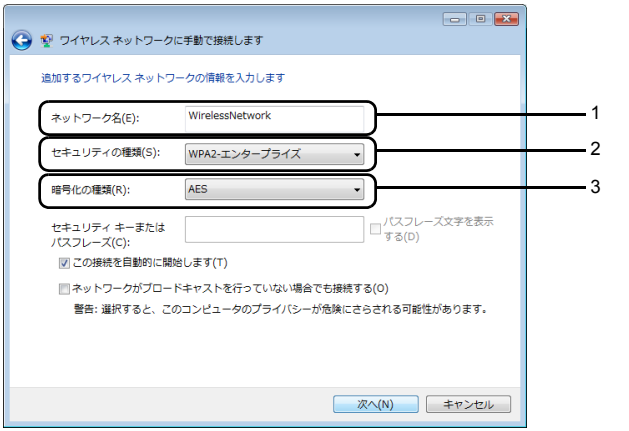
2 **「接続またはネットワークをセットアップします」をクリックします。**



3 (1)「ワイヤレスネットワークに手動で接続します」を選択し、(2)「次へ」をクリックします。



4 接続する無線 LAN アクセスポイントに合わせて、無線 LAN の情報を入力します。



POINT

・接続先の無線 LAN アクセスポイントがブロードキャストを行っていない場合は、「ネットワークがブロードキャストを行っていない場合でも接続する」をクリックして☑にしてください。
詳細についてはネットワーク管理者に確認してください。

■ WPA ／ WPA2 の場合

1. ネットワーク名
接続する無線 LAN アクセスポイントに合わせてネットワーク名（SSID）を入力します。

2. セキュリティの種類
「WPA2-エンタープライズ」「WPA-エンタープライズ」のいずれかを選択します。
3. 暗号化の種類
「AES」「TKIP」のいずれかを選択します。

■ IEEE 802.1X の場合

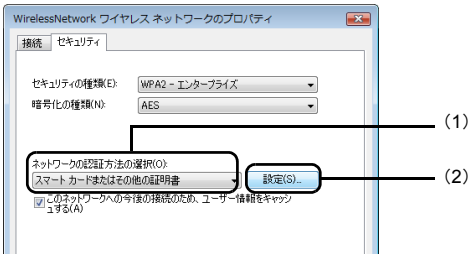
1. ネットワーク名
接続する無線 LAN アクセスポイントに合わせてネットワーク名（SSID）を入力します。
2. セキュリティの種類
「802.1 x 」を選択します。

5 「次へ」をクリックします。

6 「接続の設定を変更します」をクリックします。

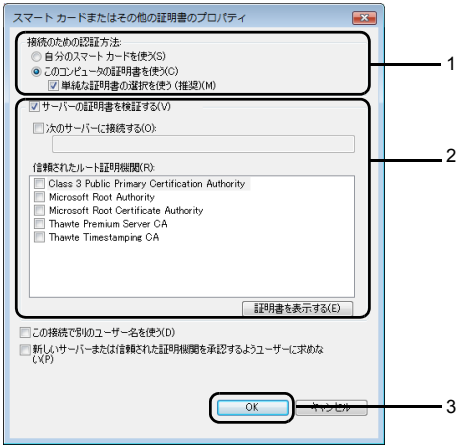
7 「ワイヤレスネットワークのプロパティ」ウィンドウの「セキュリティ」タブをクリックします。

8 (1)「ネットワークの認証方法の選択」で「スマートカードまたはその他の証明書」を選択し、(2)「設定」をクリックします。



「スマートカードまたはその他の証明書のプロパティ」ウィンドウが表示されます。

9 詳細設定を行います。



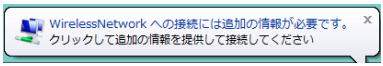
1. 認証方法を選択します。
2. 必要に応じて認証サーバの設定をします。
3. 「OK」をクリックします。

10 「ワイヤレスネットワークのプロパティ」ウィンドウで「OK」をクリックします。

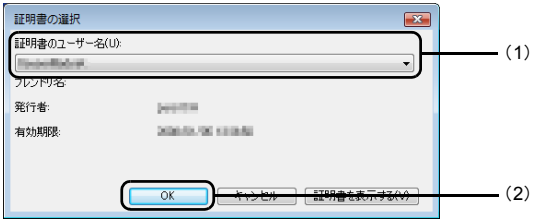
POINT

パソコンに複数の証明書をインストールしている場合

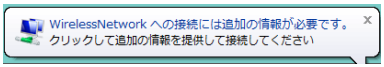
1. デスクトップ右下の通知領域に表示されるメッセージをクリックします。



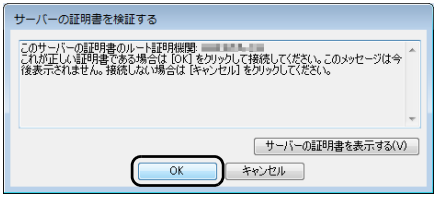
2. (1) 証明書のユーザー名を選択して、(2)「OK」をクリックします。



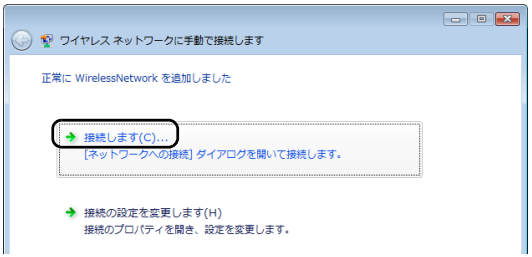
11 デスクトップ右下の通知領域に表示されるメッセージをクリックします。



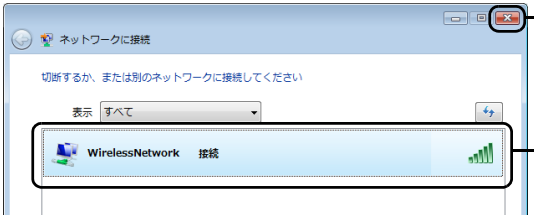
12 「OK」をクリックします。



13 「ワイヤレスネットワークに手動で接続します」ウィンドウで「接続します」をクリックします。



14 (1)ネットワークに接続されたことを確認して、(2) をクリックします。



「ネットワークに接続」ウィンドウが閉じます。

IEEE 802.1X ＋ PEAP-MSCHAPv2 ／ WPA ＋ PEAP-MSCHAPv2 ／ WPA2 ＋ PEAP-MSCHAPv2

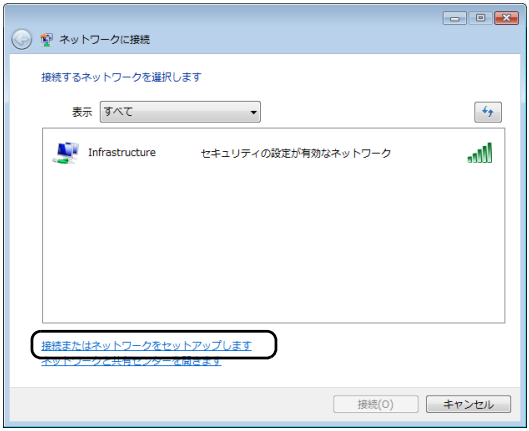
次のセキュリティパターンの場合の設定方法を説明します。

- IEEE 802.1X ＋ PEAP-MSCHAPv2
- WPA ＋ PEAP-MSCHAPv2（WPA エンタープライズ PEAP-MSCHAP v2）
- WPA2 ＋ PEAP-MSCHAPv2（WPA2 エンタープライズ PEAP-MSCHAP v2）

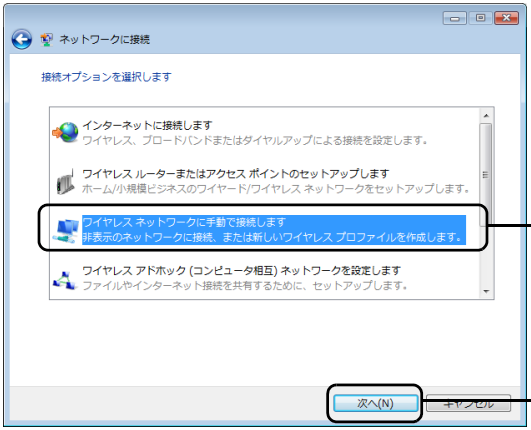
1 (スタート) →「接続先」の順にクリックします。

「ネットワークに接続」ウィンドウが表示されます。

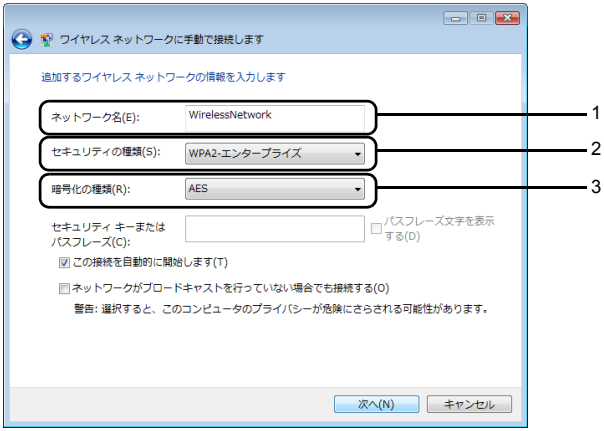
2 「接続またはネットワークをセットアップします」をクリックします。



3 (1)「ワイヤレスネットワークに手動で接続します」を選択し、(2)「次へ」をクリックします。



4 接続する無線 LAN アクセスポイントに合わせて、無線 LAN の情報を入力します。



POINT

・接続先の無線 LAN アクセスポイントがブロードキャストを行っていない場合は、「ネットワークがブロードキャストを行っていない場合でも接続する」をクリックして☑にしてください。
詳細についてはネットワーク管理者に確認してください。

■ WPA ／ WPA2 の場合

1. **ネットワーク名**
   接続する無線 LAN アクセスポイントに合わせてネットワーク名（SSID）を入力します。
2. **セキュリティの種類**
   「WPA2-エンタープライズ」「WPA-エンタープライズ」のいずれかを選択します。
3. **暗号化の種類**
   「AES」「TKIP」のいずれかを選択します。

■ IEEE 802.1X の場合

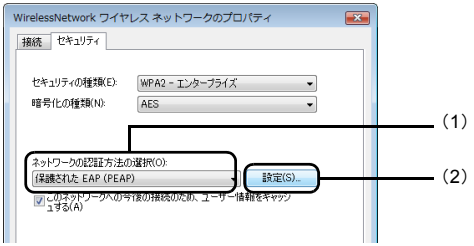
1. **ネットワーク名**
   接続する無線 LAN アクセスポイントに合わせてネットワーク名（SSID）を入力します。
2. **セキュリティの種類**
   「802.1 x 」を選択します。

5 **「次へ」をクリックします。**

6 **「接続の設定を変更します」をクリックします。**

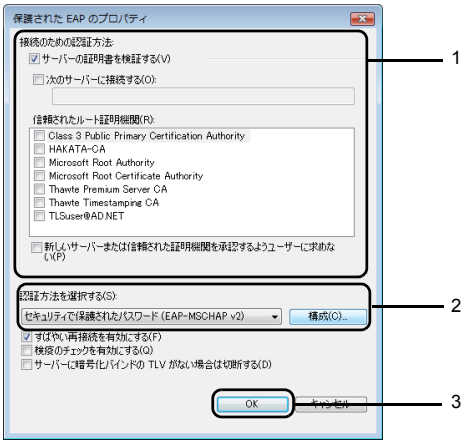
7 **「ワイヤレスネットワークのプロパティ」ウィンドウの「セキュリティ」タブをクリックします。**

8 **(1)「ネットワークの認証方法の選択」で「保護された EAP（PEAP)」を選択し、(2)「設定」をクリックします。**



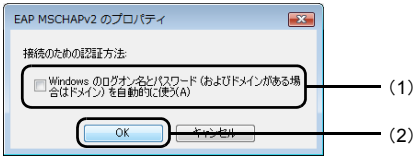
「保護された EAP のプロパティ」ウィンドウが表示されます。

9 **詳細設定を行います。**



1. 必要に応じて認証サーバーの設定をします。
2. 「認証方法を選択する」で「セキュリティで保護されたパスワード（EAP-MSCHAP v2)」を選択し、「構成」をクリックします。
   「EAP MSCHAPv2 のプロパティ」ウィンドウが表示されます。

3. (1)「Windows のログオン名とパスワード（およびドメインがある場合はドメイン）を自動的に使う」をクリックして にし、(2)「OK」をクリックします。

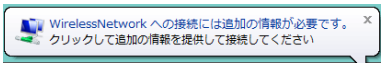


注 1　シングルサインオンを使用する場合は、パソコンをドメインに参加させた上でこのチェックをつけた無線LANのプロファイルを共有プロファイルとして作成してください。

4.「保護された EAP のプロパティ」ウィンドウで「OK」をクリックします。

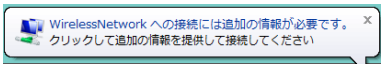
10 「ワイヤレスネットワークのプロパティ」ウィンドウで「OK」をクリックします。

11 デスクトップ右下の通知領域に表示されるメッセージをクリックします。

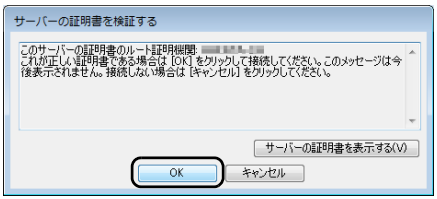


12 (1)「ユーザー名」と「パスワード」を入力し、(2)「OK」をクリックします。

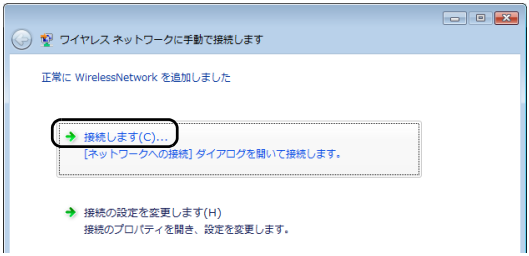
13 デスクトップ右下の通知領域に表示されるメッセージをクリックします。



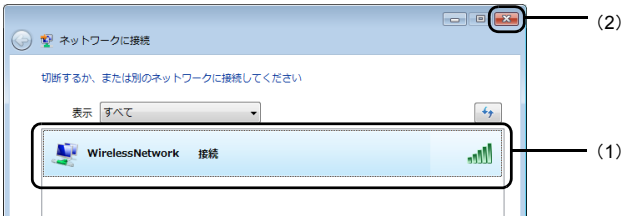
14 「OK」をクリックします。



15 **「ワイヤレスネットワークに手動で接続します」ウィンドウで「接続します」をクリックします。**



16 **(1)ネットワークに接続されたことを確認して、(2)をクリックします。**



「ネットワークに接続」ウィンドウが閉じます。

IEEE 802.1X ＋ PEAP-TLS ／ WPA ＋ PEAP-TLS ／ WPA2 ＋ PEAP-TLS

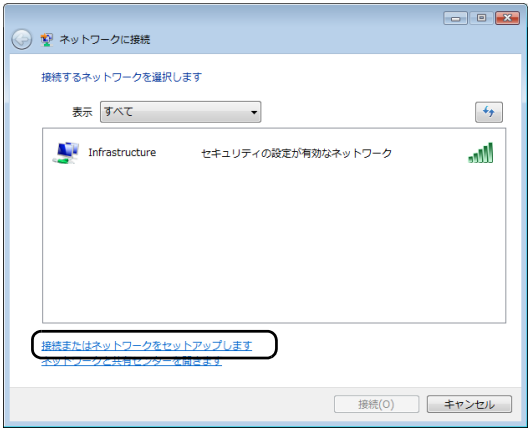
次のセキュリティパターンの場合の設定方法を説明します。

・IEEE 802.1X ＋ PEAP-TLS
・WPA ＋ PEAP-TLS（WPA エンタープライズ PEAP-TLS）
・WPA2 ＋ PEAP-TLS（WPA2 エンタープライズ PEAP-TLS）

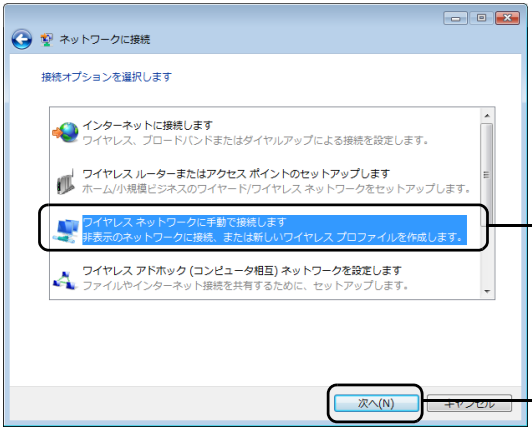
1 **(スタート)→「接続先」の順にクリックします。**

「ネットワークに接続」ウィンドウが表示されます。

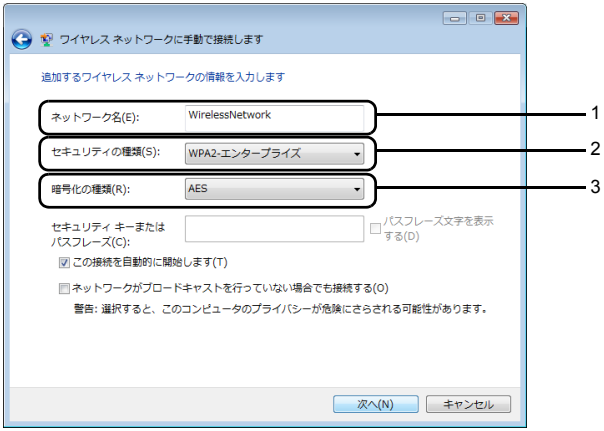
2 「接続またはネットワークをセットアップします」をクリックします。



3 (1)「ワイヤレスネットワークに手動で接続します」を選択し、(2)「次へ」をクリックします。



4 接続する無線 LAN アクセスポイントに合わせて、無線 LAN の情報を入力します。



POINT

・接続先の無線 LAN アクセスポイントがブロードキャストを行っていない場合は、「ネットワークがブロードキャストを行っていない場合でも接続する」をクリックして☑にしてください。
詳細についてはネットワーク管理者に確認してください。

■ WPA ／ WPA2 の場合

1. **ネットワーク名**
   接続する無線 LAN アクセスポイントに合わせてネットワーク名（SSID）を入力します。
2. **セキュリティの種類**
   「WPA2-エンタープライズ」「WPA-エンタープライズ」のいずれかを選択します。
3. **暗号化の種類**
   「AES」「TKIP」のいずれかを選択します。

■ IEEE 802.1X の場合

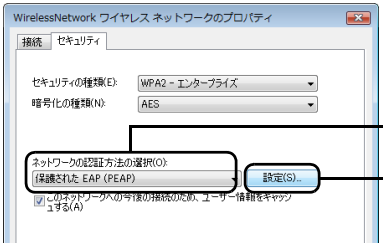
1. **ネットワーク名**
   接続する無線 LAN アクセスポイントに合わせてネットワーク名（SSID）を入力します。
2. **セキュリティの種類**
   「802.1 x 」を選択します。

5 「次へ」をクリックします。

6 「接続の設定を変更します」をクリックします。

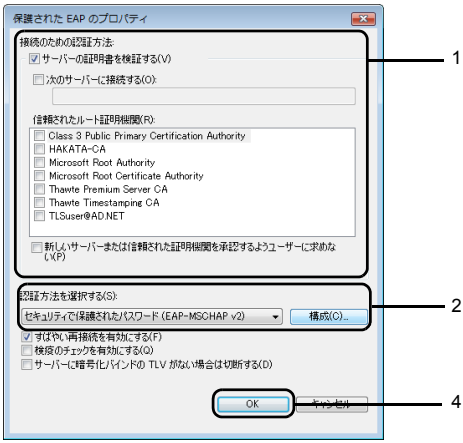
7 「ワイヤレスネットワークのプロパティ」ウィンドウの「セキュリティ」タブをクリックします。

8 (1)「ネットワークの認証方法の選択」で「保護された EAP（PEAP)」を選択し、(2)「設定」をクリックします。



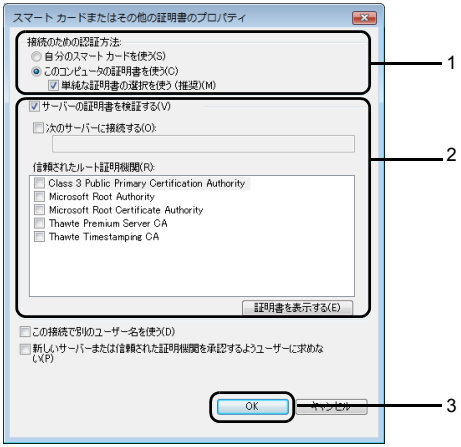
「保護された EAP のプロパティ」ウィンドウが表示されます。

9 詳細設定を行います。



1. 必要に応じて認証サーバーの設定をします。
2. 「認証方法を選択する」で「スマートカードまたはその他の証明書」を選択し、「構成」をクリックします。
   「スマートカードまたはその他の証明書のプロパティ」ウィンドウが表示されます。

3. 詳細設定を行います。



1. 認証方法を選択します。
2. 必要に応じて認証サーバーの設定をします。
3. 「OK」をクリックします。

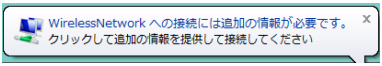
4. 「保護された EAP のプロパティ」ウィンドウで「OK」をクリックします。

10 「ワイヤレスネットワークのプロパティ」ウィンドウで「OK」をクリックします。

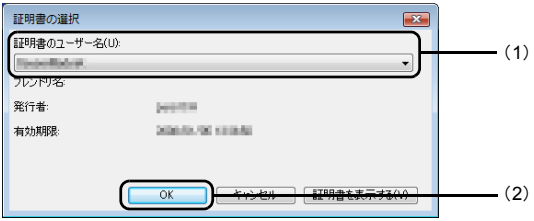
POINT

パソコンに複数の証明書をインストールしている場合

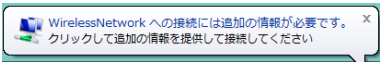
1. デスクトップ右下の通知領域に表示されるメッセージをクリックします。



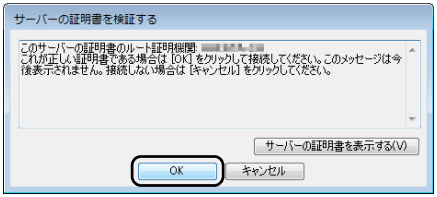
2. (1) 証明書のユーザー名を選択して、(2)「OK」をクリックします。



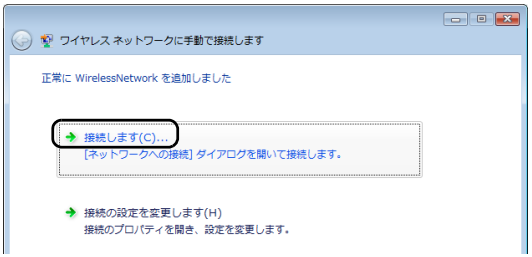
11 デスクトップ右下の通知領域に表示されるメッセージをクリックします。



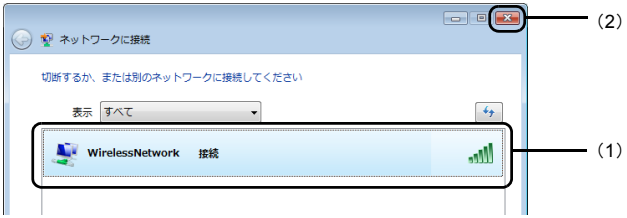
12 「OK」をクリックします。



13 「ワイヤレスネットワークに手動で接続します」ウィンドウで「接続します」をクリックします。



14 (1)ネットワークに接続されたことを確認して、(2) をクリックします。



「ネットワークに接続」ウィンドウが閉じます。

WPA-PSK ／ WPA2-PSK

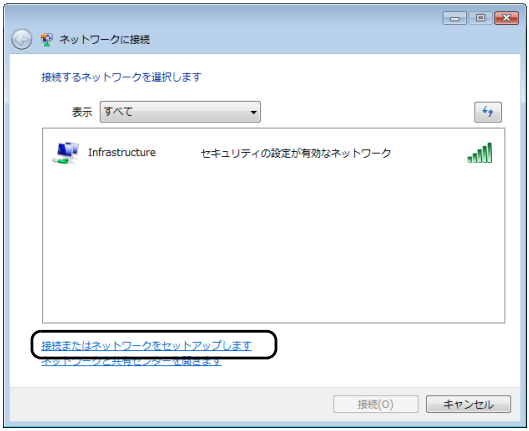
次のセキュリティパターンの場合の設定方法を説明します。

・WPA-PSK（WPA パーソナル）
・WPA2-PSK（WPA2 パーソナル）

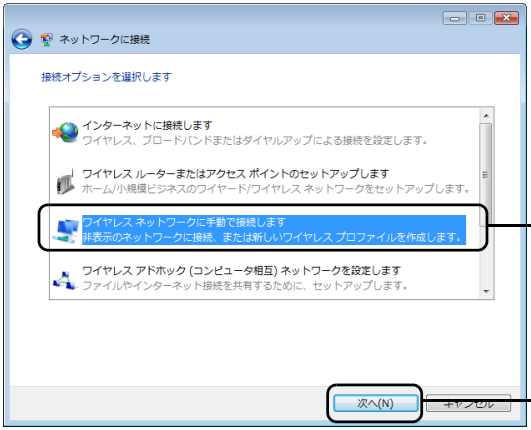
1 (スタート) →「接続先」の順にクリックします。

「ネットワークに接続」ウィンドウが表示されます。

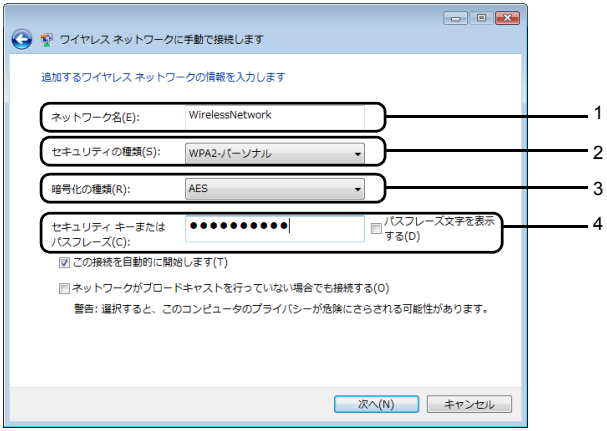
2 「接続またはネットワークをセットアップします」をクリックします。



3 (1)「ワイヤレスネットワークに手動で接続します」を選択し、(2)「次へ」をクリックします。



4 無線 LAN の情報を、接続する無線 LAN アクセスポイントに合わせて入力します。



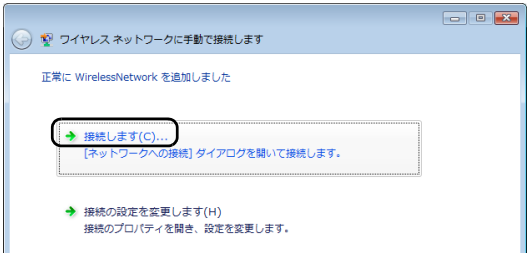
POINT

・接続先の無線 LAN アクセスポイントがブロードキャストを行っていない場合は、「ネットワークがブロードキャストを行っていない場合でも接続する」をクリックして☑にしてください。
詳細についてはネットワーク管理者に確認してください。

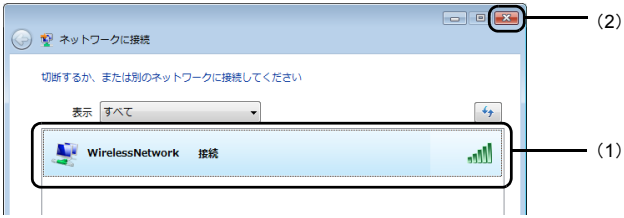
1. **ネットワーク名**
   接続する無線 LAN アクセスポイントに合わせてネットワーク名（SSID）を入力します。
2. **セキュリティの種類**
   「WPA2- パーソナル」「WPA- パーソナル」のいずれかを選択します。
3. **暗号化の種類**
   「AES」「TKIP」のいずれかを選択します。
4. **セキュリティキーまたはパスフレーズ**
   接続する無線 LAN アクセスポイントに合わせて、PSK（パスフレーズ）を入力します。

5 「次へ」をクリックします。

6 「ワイヤレスネットワークに手動で接続します」ウィンドウで「接続します」をクリックします。



7 (1)ネットワークに接続されたことを確認して、(2) をクリックします。



「ネットワークに接続」ウィンドウが閉じます。

13 FMV-JW183 の設定

クライアントのパソコンに搭載されている無線 LAN のデバイスが、FMV-JW183 の場合の設定方法を説明します。
なお、ここでは OS が Windows 2000 の場合の設定方法を説明します。OS が Windows XP の場合は、「Windows XP 標準の無線 LAN 機能を使った設定」（→ P.249）をご覧ください。

POINT

・Windows 2000 Service Pack 4 以降が必要です。
・無線 LAN の設定を行う前に、Windows 2000 が提供する無線 LAN の機能が有効になっている必要があります。次の手順で確認してください。
1. 「スタート」ボタン→「設定」→「コントロールパネル」の順にクリックします。
2. 「管理ツール」をクリックします。
3. 「サービス」をクリックします。
4. 「名前」の一覧で「Wireless Configuration」の「スタートアップの種類」が「自動」になっているかどうか確認します。
「スタートアップの種類」が「手動」や「無効」の場合は、次の手順で「自動」に設定してください。
   1. 「Wireless Configuration」を右クリックし、「プロパティ」をクリックします。
   2. 「スタートアップの種類」で「自動」を選択し、「適用」をクリックします。
   3. 「サービスの状態」で、「開始」をクリックします。
   4. 「OK」をクリックします。
5. 「サービス」ウィンドウ、および「管理ツール」ウィンドウを閉じます。

IEEE 802.1X ＋ EAP-TLS

IEEE 802.1X ＋ EAP-TLS の場合の設定方法を説明します。

1 デスクトップ右下の通知領域からクライアントマネージャのアイコン（ ）をクリックします。

POINT

・アイコンの状態は、接続状態などにより異なります。
・通知領域にクライアントマネージャのアイコンが表示されていない場合は、「スタート」ボタン→「プログラム」→「Wireless」→「Client Manager」の順にクリックします。

「Wireless クライアントマネージャ」ウィンドウが表示されます。

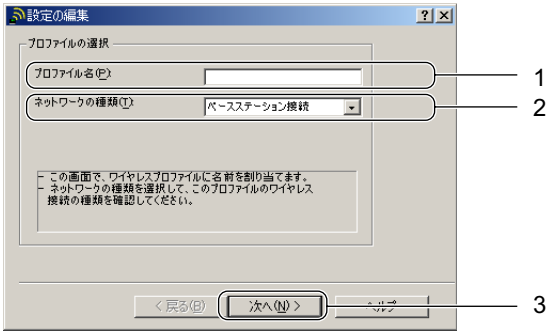
2 「アクション」メニュー→「設定プロファイルの追加 / 編集」の順にクリックします。

「設定プロファイルの追加 / 編集」ウィンドウが表示されます。

3 「プロファイルの選択」で「追加」をクリックします。

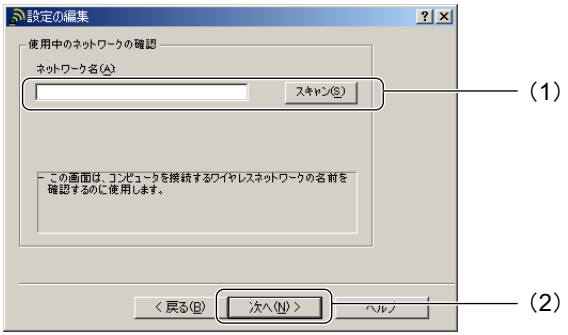
「設定の編集」ウィンドウが表示されます。

4 「プロファイルの選択」で、次のように設定します。



1. 「プロファイル名」に設定内容を保存するプロファイル名を設定します。任意の文字列を、半角英数字、および半角記号 32 文字以内で入力します。
2. 「ネットワークの種類」の▼から「ベースステーション接続」を選択します。
3. 「次へ」をクリックします。

5 「使用中のネットワークの確認」で、(1)「ネットワーク名」に接続する無線 LAN アクセスポイントのネットワーク名（SSID）を入力し、(2)「次へ」をクリックします。



重要

・接続する無線 LAN アクセスポイントと同じネットワーク名（SSID）を設定したアドホックの無線 LAN が、近くにないことを確認してください。
近くにある場合は、正常に通信が行えない可能性があります。どちらかのネットワーク名（SSID）を変更してください。

POINT

・「スキャン」をクリックすると、利用可能なネットワークの一覧が表示されます。

6 「セキュリティの設定」で通信データを暗号化するための設定をします。次のように設定します。

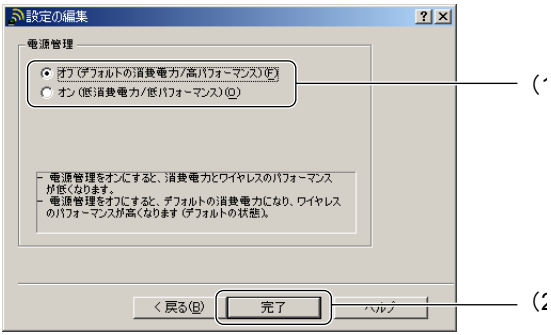
1. 「データセキュリティの有効化」をクリックして☑にします。
2. 「英数字を使用」をクリックして◉にします。
3. 「キー 1」に、仮の文字列「guest」と入力します。
4. 「データの暗号化」で▼をクリックして、「キー 1」を選択します。
5. 「共有キー認証」をクリックして☐にします。
6. 「次へ」をクリックします。

POINT

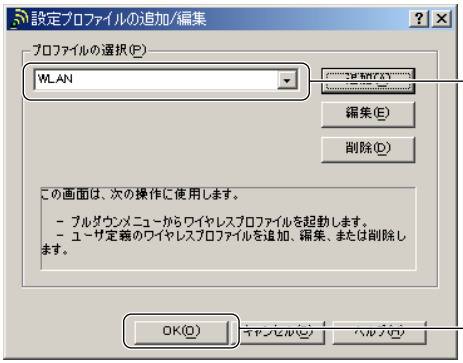
・キー1 に入力する文字列は仮の設定です。実際の暗号化には無線 LAN アクセスポイントから通知を受けた文字列を使用します。

7 (1)「電源管理」で、「オフ」をクリックして◉にし、(2)「完了」をクリックします。

「オン」はお使いになれません。「オン」をクリックして◉にすると、無線 LAN アクセスポイントと通信できなくなる場合があります。



8 **「設定プロファイルの追加 / 編集」ウィンドウで、(1)「プロファイルの選択」に設定したプロファイル名が選択されていることを確認し、(2)「OK」をクリックします。**



9 **「Wireless クライアントマネージャ」ウィンドウで「OK」をクリックします。**

10 **デスクトップの「マイ ネットワーク」を右クリックして、表示されるメニューから「プロパティ」をクリックします。**

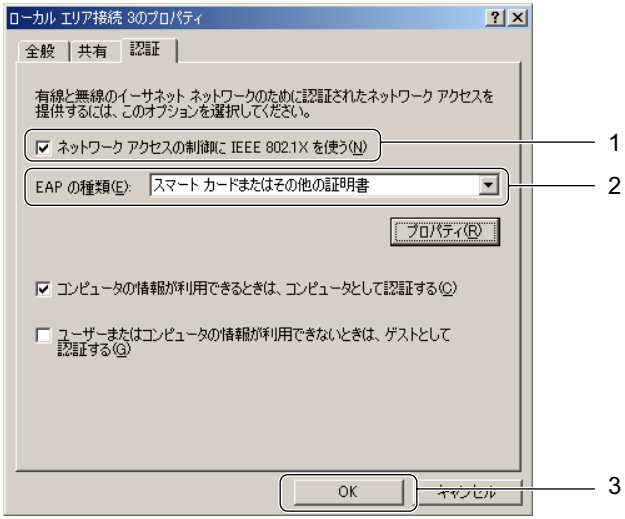
「ネットワークとダイヤルアップ接続」ウィンドウに、現在インストールされているネットワークの一覧が表示されます。

11 **一覧に表示されているアイコンにマウスポインタを重ねて「802.11b Wireless LAN Adapter (A)」と表示されるアイコンを右クリックし、表示されるメニューから「プロパティ」をクリックします。**

「ローカル エリア接続のプロパティ」ウィンドウが表示されます。

12 「認証」タブをクリックします。

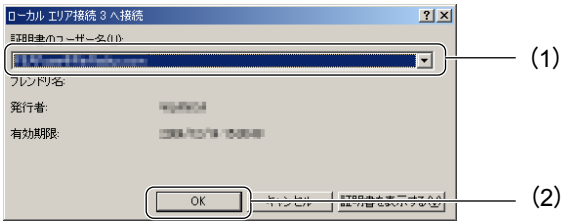
13 次のように設定します。



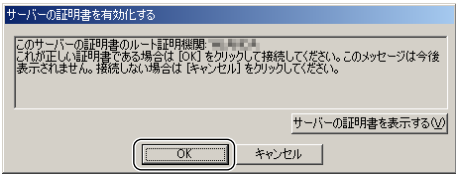
1. 「ネットワークアクセスの制御に IEEE 802.1X を使う」をクリックして☑にします。
2. 「EAP の種類」の▼をクリックして「スマートカードまたはその他の証明書」を選択します。
3. 「OK」をクリックします。

POINT

・パソコンに複数の証明書をインストールしている場合は次の画面が表示されますので、(1)「証明書のユーザー名」を選択して、(2)「OK」をクリックします。



14 **「サーバーの証明書を有効化する」ウィンドウが表示されますので、「OK」をクリックします。**



IEEE 802.1X + PEAP-MSCHAPv2

IEEE 802.1X + PEAP-MSCHAPv2 の場合の設定方法を説明します。

1 **デスクトップ右下の通知領域からクライアントマネージャのアイコン（ ）をクリックします。**

POINT

・アイコンの状態は、接続状態などにより異なります。
・通知領域にクライアントマネージャのアイコンが表示されていない場合は、「スタート」ボタン→「プログラム」→「Wireless」→「Client Manager」の順にクリックします。

「Wireless クライアントマネージャ」ウィンドウが表示されます。

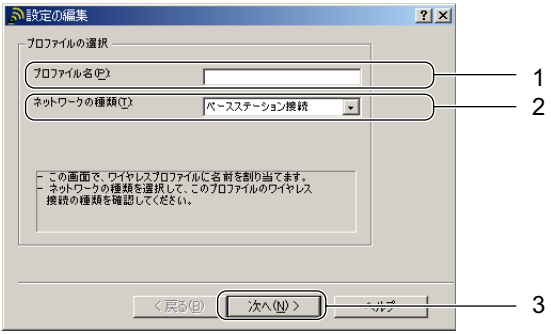
2 **「アクション」メニュー→「設定プロファイルの追加 / 編集」の順にクリックします。**

「設定プロファイルの追加 / 編集」ウィンドウが表示されます。

3 **「プロファイルの選択」で「追加」をクリックします。**

「設定の編集」ウィンドウが表示されます。

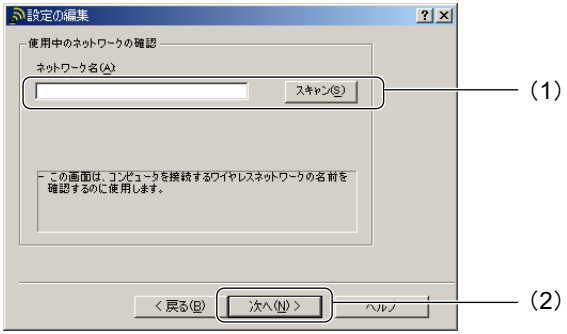
4 **「プロファイルの選択」で、次のように設定します。**



1. 「プロファイル名」に設定内容を保存するプロファイル名を設定します。任意の文字列を、半角英数字、および半角記号 32 文字以内で入力します。
2. 「ネットワークの種類」の から「ベースステーション接続」を選択します。

3.「次へ」をクリックします。

5 「使用中のネットワークの確認」で、(1)「ネットワーク名」に接続する無線 LAN アクセスポイントのネットワーク名（SSID）を入力し、(2)「次へ」をクリックします。



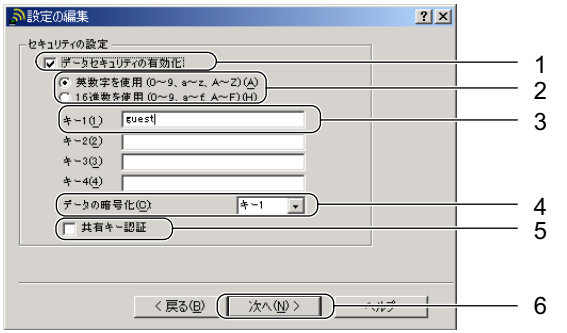
重要

・接続する無線 LAN アクセスポイントと同じネットワーク名（SSID）を設定したアドホックの無線 LAN が、近くにないことを確認してください。
近くにある場合は、正常に通信が行えない可能性があります。どちらかのネットワーク名（SSID）を変更してください。

POINT

・「スキャン」をクリックすると、利用可能なネットワークの一覧が表示されます。

6 「セキュリティの設定」で通信データを暗号化するための設定をします。次のように設定します。



1.「データセキュリティの有効化」をクリックして☑にします。
2.「英数字を使用」をクリックして◉にします。
3.「キー 1」に、仮の文字列「guest」と入力します。
4.「データの暗号化」の▼をクリックし「キー 1」を選択します。
5.「共有キー認証」をクリックして☐にします。

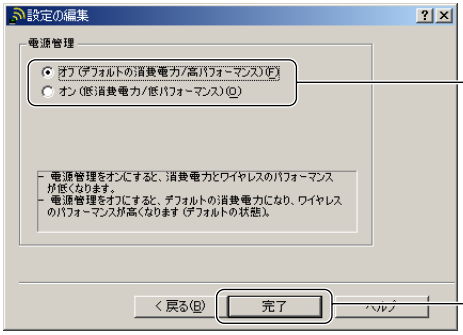
6.「次へ」をクリックします。

POINT

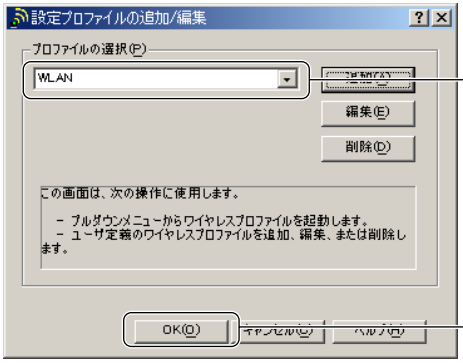
・キー1に入力する文字列は仮の設定です。実際の暗号化には無線 LAN アクセスポイントから通知を受けた文字列を使用します。

7 (1)「電源管理」で、「オフ」をクリックして○にし、(2)「完了」をクリックします。

「オン」はお使いになれません。「オン」をクリックして○にすると、無線 LAN アクセスポイントと通信できなくなる場合があります。



8「設定プロファイルの追加 / 編集」ウィンドウで、(1)「プロファイルの選択」に設定したプロファイル名が選択されていることを確認し、(2)「OK」をクリックします。



9「Wireless クライアントマネージャ」ウィンドウで「OK」をクリックします。

10 デスクトップの「マイ ネットワーク」を右クリックして、表示されるメニューから「プロパティ」をクリックします。

「ネットワークとダイヤルアップ接続」ウィンドウに、現在インストールされているネットワークの一覧が表示されます。

11 一覧に表示されているアイコンにマウスポインタを重ねて「802.11b Wireless LAN Adapter（A）」と表示されるアイコンを右クリックし、表示されるメニューから「プロパティ」をクリックします。

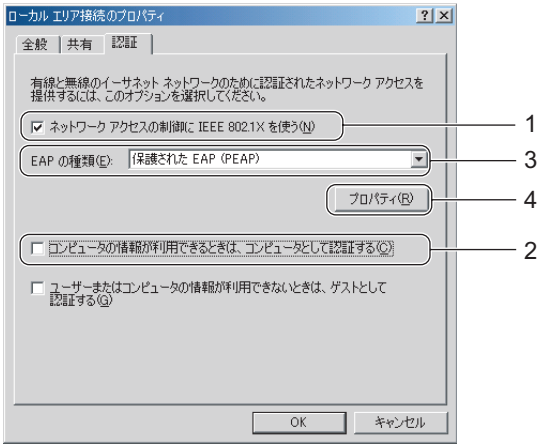
「ローカル エリア接続のプロパティ」ウィンドウが表示されます。

12 「認証」タブをクリックします。

13 次のように設定します。

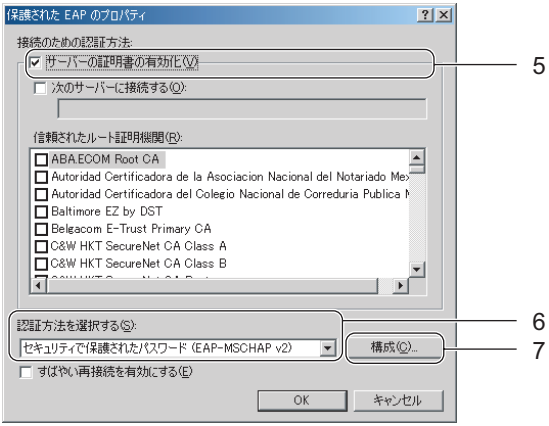
1. 「ネットワーク アクセスの制御に IEEE 802.1X を使う」をクリックして☑にします。
2. 「コンピュータの情報が利用できるときは、コンピュータとして認証する」をクリックして☐にします。
3. 「EAP の種類」の▼をクリックし、「保護された EAP（PEAP）」を選択します。
4. 「プロパティ」をクリックします。

   「保護された EAP のプロパティ」ウィンドウが表示されます。



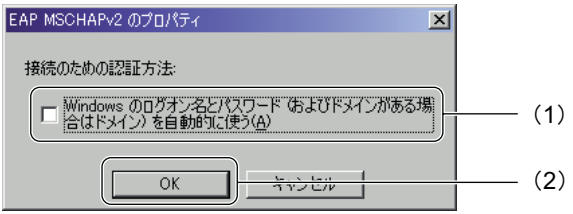
5. 「サーバーの証明書の有効化」が☑になっていることを確認します。
6. 「認証方法を選択する」で、「セキュリティで保護されたパスワード（EAP-MSCHAP v2）」が選択されていることを確認します。

7.「構成」をクリックします。



「EAP MSCHAPv2 のプロパティ」ウィンドウが表示されます。

8.（1）「Windows のログオン名とパスワード（およびドメインがある場合はドメイン）を自動的に使う」をクリックして☐にし、（2）「OK」をクリックします。

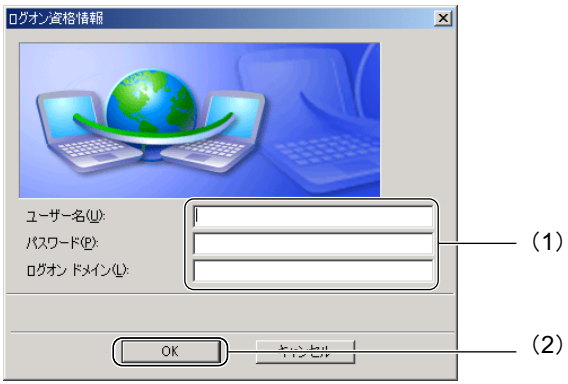


9.「保護された EAP のプロパティ」ウィンドウで「OK」をクリックします。

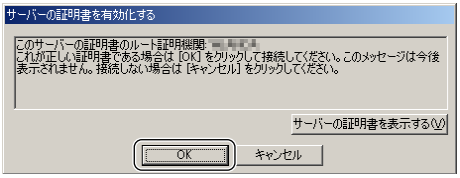
10.「ローカル エリア接続のプロパティ」ウィンドウで「OK」をクリックします。

14 「ログオン資格情報」ウィンドウが表示されますので、（1）ユーザー名、パスワード、ログオンドメインを入力して、（2）「OK」をクリックします。

ユーザー名、パスワード、ログオンドメインは、ネットワーク管理者にご確認ください。



15 **「サーバーの証明書を有効化する」ウィンドウが表示されますので、「OK」をクリックします。**



IEEE 802.1X + PEAP-TLS

IEEE 802.1X + PEAP-TLS の場合の設定方法を説明します。

1 **デスクトップ右下の通知領域からクライアントマネージャのアイコン（ ）をクリックします。**

POINT

- アイコンの状態は、接続状態などにより異なります。
- 通知領域にクライアントマネージャのアイコンが表示されていない場合は、「スタート」ボタン→「プログラム」→「Wireless」→「Client Manager」の順にクリックします。

「Wireless クライアントマネージャ」ウィンドウが表示されます。

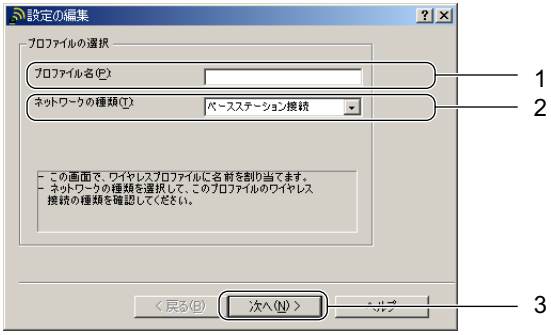
2 **「アクション」メニュー→「設定プロファイルの追加 / 編集」の順にクリックします。**

「設定プロファイルの追加 / 編集」ウィンドウが表示されます。

3 **「プロファイルの選択」で「追加」をクリックします。**

「設定の編集」ウィンドウが表示されます。

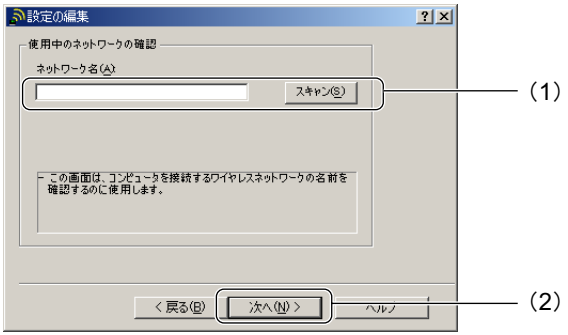
4 **「プロファイルの選択」で、次のように設定します。**



1. 「プロファイル名」に設定内容を保存するプロファイル名を設定します。任意の文字列を、半角英数字、および半角記号 32 文字以内で入力します。
2. 「ネットワークの種類」の から「ベースステーション接続」を選択します。

3.「次へ」をクリックします。

5 「使用中のネットワークの確認」で、(1)「ネットワーク名」に接続する無線 LAN アクセスポイントのネットワーク名（SSID）を入力し、(2)「次へ」をクリックします。



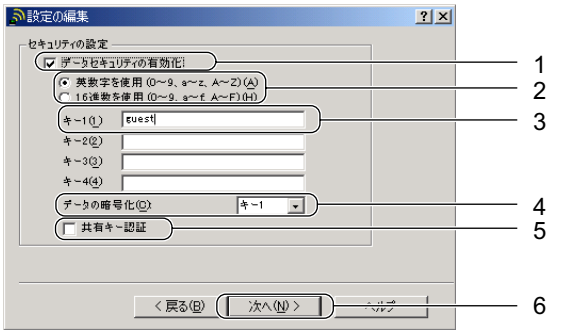
重要

・接続する無線 LAN アクセスポイントと同じネットワーク名（SSID）を設定したアドホックの無線 LAN が、近くにないことを確認してください。
近くにある場合は、正常に通信が行えない可能性があります。どちらかのネットワーク名（SSID）を変更してください。

POINT

・「スキャン」をクリックすると、利用可能なネットワークの一覧が表示されます。

6 「セキュリティの設定」で通信データを暗号化するための設定をします。次のように設定します。



1.「データセキュリティの有効化」をクリックしてにします。
2.「英数字を使用」をクリックしてにします。
3.「キー 1」に、仮の文字列「guest」と入力します。
4.「データの暗号化」のをクリックし「キー 1」を選択します。
5.「共有キー認証」をクリックしてにします。

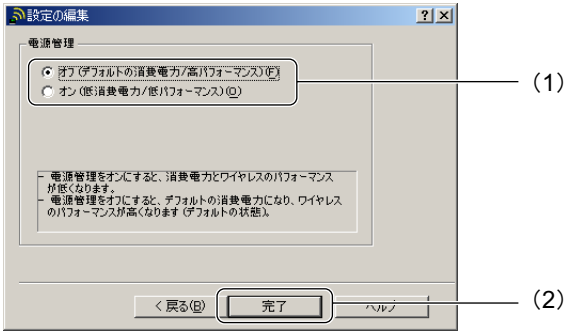
6.「次へ」をクリックします。

POINT

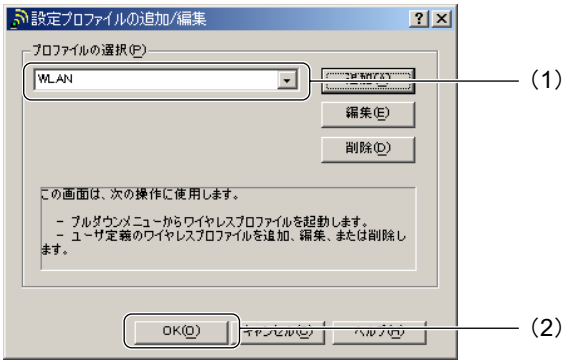
・キー1 に入力する文字列は仮の設定です。実際の暗号化には無線 LAN アクセスポイントから通知を受けた文字列を使用します。

7 (1)「電源管理」で、「オフ」をクリックして にし、(2)「完了」をクリックします。

「オン」はお使いになれません。「オン」をクリックして にすると、無線 LAN アクセスポイントと通信できなくなる場合があります。



8「設定プロファイルの追加 / 編集」ウィンドウで、(1)「プロファイルの選択」に設定したプロファイル名が選択されていることを確認し、(2)「OK」をクリックします。



9 **「Wireless クライアントマネージャ」ウィンドウで「OK」をクリックします。**

10 **デスクトップの「マイ ネットワーク」を右クリックして、表示されるメニューから「プロパティ」をクリックします。**

「ネットワークとダイヤルアップ接続」ウィンドウに、現在インストールされているネットワークの一覧が表示されます。

11 **一覧に表示されているアイコンにマウスポインタを重ねて「802.11b Wireless LAN Adapter（A）」と表示されるアイコンを右クリックし、表示されるメニューから「プロパティ」をクリックします。**

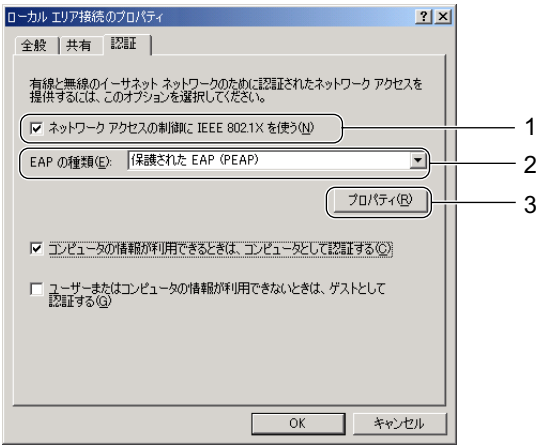
「ローカル エリア接続のプロパティ」ウィンドウが表示されます。

12 **「認証」タブをクリックします。**

13 **次のように設定します。**

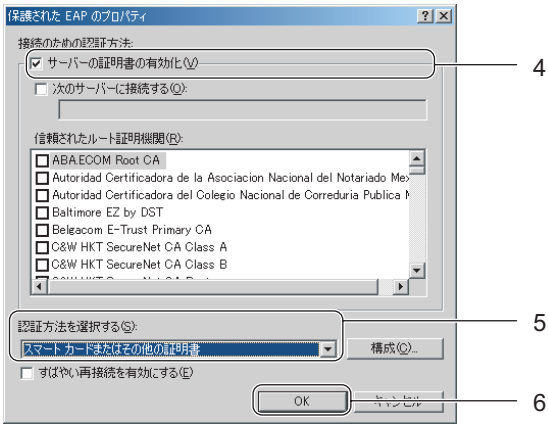
1. 「ネットワーク アクセスの制御に IEEE 802.1X を使う」をクリックして☑にします。
2. 「EAP の種類」の▼をクリックし、「保護された EAP（PEAP）」を選択します。
3. 「プロパティ」をクリックします。

   「保護された EAP のプロパティ」ウィンドウが表示されます。



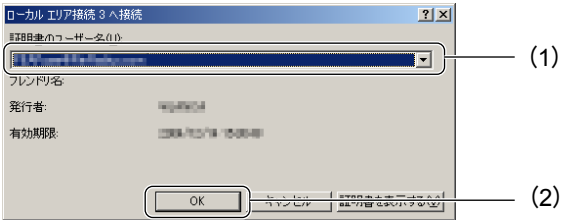
4. 「サーバーの証明書の有効化」が☑になっていることを確認します。
5. 「認証方法を選択する」で、▼をクリックして「スマートカードまたはその他の証明書」を選択します。

6.「OK」をクリックします。

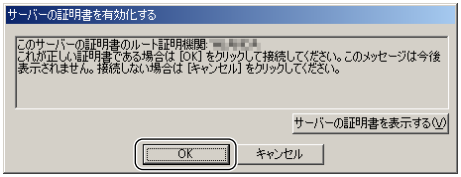


POINT

・パソコンに複数の証明書をインストールしている場合は次の画面が表示されますので、(1)「証明書のユーザー名」を選択して、(2)「OK」をクリックします。



14 「サーバーの証明書を有効化する」ウィンドウが表示されますので、「OK」をクリックします。



14 Broadcom 無線 LAN 搭載モデルの設定

クライアントのパソコンに搭載されている無線 LAN のデバイスが、Broadcom 無線 LAN 搭載モデルの場合の設定方法を説明します。
なお、ここでは OS が Windows 2000 の場合の設定方法を説明します。OS が Windows XP の場合は、「Windows XP 標準の無線 LAN 機能を使った設定」（→ P.249）をご覧ください。

POINT

・Windows 2000 Service Pack 4 以降が必要です。
・無線 LAN の設定を行う前に、Windows 2000 が提供する無線 LAN の機能が有効になっている必要があります。次の手順で確認してください。
1. 「スタート」ボタン→「設定」→「コントロールパネル」の順にクリックします。
2. 「管理ツール」をクリックします。
3. 「サービス」をクリックします。
4. 「名前」の一覧で「Wireless Configuration」の「スタートアップの種類」が「自動」になっているかどうか確認します。
「スタートアップの種類」が「手動」や「無効」の場合は、次の手順で「自動」に設定してください。
   1. 「Wireless Configuration」を右クリックし、「プロパティ」をクリックします。
   2. 「スタートアップの種類」で「自動」を選択し、「適用」をクリックします。
   3. 「サービスの状態」で、「開始」をクリックします。
   4. 「OK」をクリックします。
5. 「サービス」ウィンドウ、および「管理ツール」ウィンドウを閉じます。

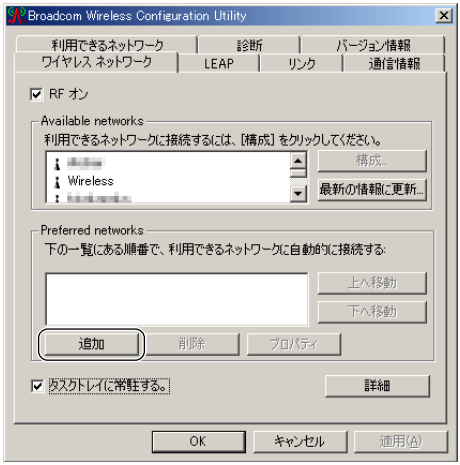
IEEE 802.1X ＋ EAP-TLS

IEEE 802.1X ＋ EAP-TLS の場合の設定方法を説明します。

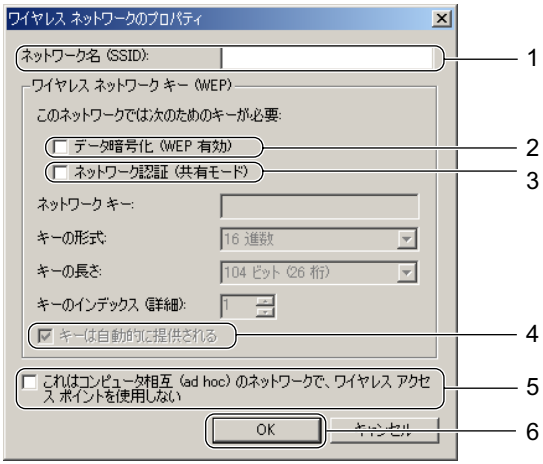
1 デスクトップ右下の通知領域からユーティリティアイコン（  ）を右クリックし、表示されるメニューから「ユーティリティを開く」をクリックします。

「Broadcom Wireless Configuration Utility」ウィンドウが表示されます。

2 「追加」をクリックします。



3 「ワイヤレス ネットワークのプロパティ」ウィンドウで次のように設定します。



1. 「ネットワーク名（SSID）」を、接続する無線 LAN アクセスポイントに合わせて設定します。
2. 「データ暗号化 (WEP 有効)」をクリックして☑にします。
3. 「ネットワーク認証 (共有モード)」をクリックして☐にします。
4. 「キーは自動的に提供される」をクリックして☑にします。
5. 「これはコンピュータ相互（ad hoc）のネットワークで、ワイヤレス アクセスポイントを使用しない」をクリックして☐にします。
6. 「OK」をクリックします。

4 **「Preferred Networks」に、「ネットワーク名（SSID）」に入力したネットワーク名が追加されたことを確認して、「OK」をクリックします。**

5 **デスクトップの「マイ　ネットワーク」を右クリックして、表示されるメニューから「プロパティ」をクリックします。**

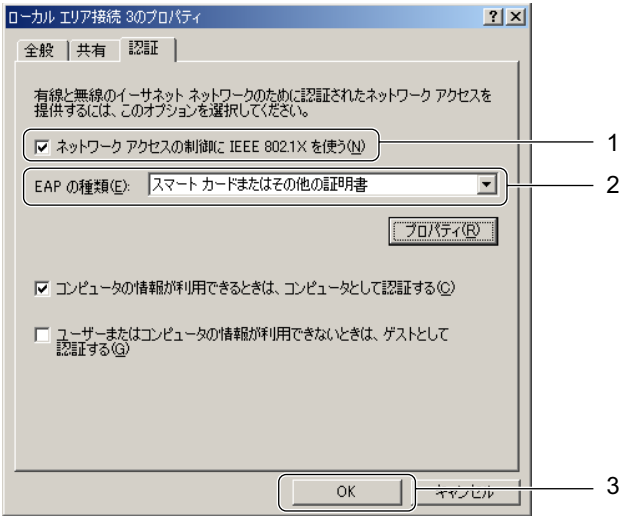
「ネットワークとダイヤルアップ接続」ウィンドウに、現在インストールされているネットワークの一覧が表示されます。

6 **一覧に表示されているアイコンにマウスポインタを重ねて「Broadcom BCM4306 Wireless LAN Adapter」と表示されるアイコンを右クリックし、表示されるメニューから「プロパティ」をクリックします。**

「ローカル エリア接続のプロパティ」ウィンドウが表示されます。

7 **「認証」タブをクリックします。**

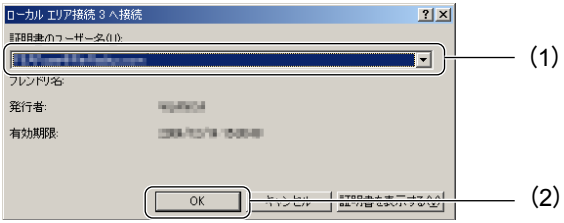
8 **次のように設定します。**



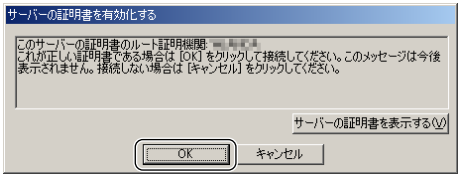
1. 「ネットワークアクセスの制御に IEEE 802.1X を使う」をクリックして☑にします。
2. 「EAP の種類」の▼をクリックして「スマートカードまたはその他の証明書」を選択します。
3. 「OK」をクリックします。

POINT

・パソコンに複数の証明書をインストールしている場合は次の画面が表示されますので、(1)「証明書のユーザー名」を選択して、(2)「OK」をクリックします。



9 **「サーバーの証明書を有効化する」ウィンドウが表示されますので、「OK」をクリックします。**



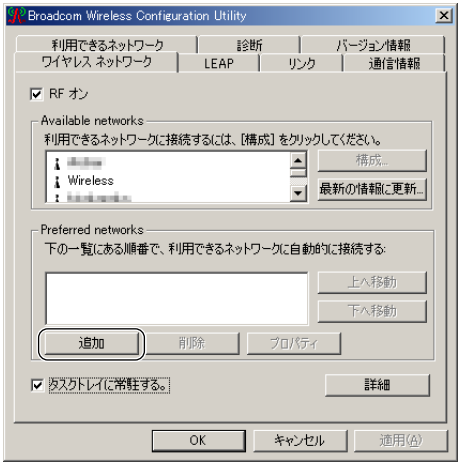
IEEE 802.1X + PEAP-MSCHAPv2

IEEE 802.1X + PEAP-MSCHAPv2 の場合の設定方法を説明します。

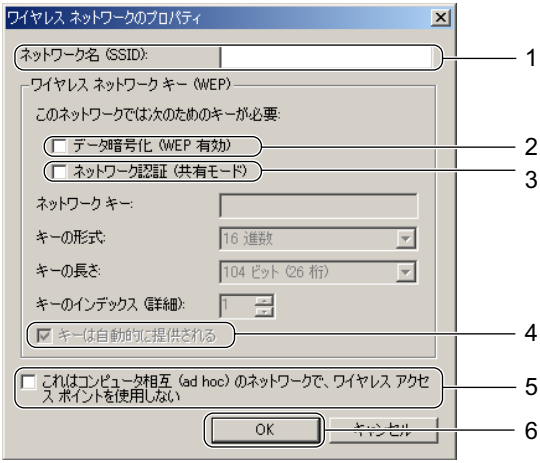
1 **デスクトップ右下の通知領域からユーティリティアイコン（ ）を右クリックし、表示されるメニューから「ユーティリティを開く」をクリックします。**

「Broadcom Wireless Configuration Utility」ウィンドウが表示されます。

2 **「追加」をクリックします。**



3 「ワイヤレス ネットワークのプロパティ」ウィンドウで次のように設定します。



1. 「ネットワーク名（SSID)」を、接続する無線 LAN アクセスポイントに合わせて設定します。
2. 「データ暗号化 (WEP 有効)」をクリックして☑にします。
3. 「ネットワーク認証 (共有モード)」をクリックして☐にします。
4. 「キーは自動的に提供される」をクリックして☑にします。
5. 「これはコンピュータ相互（ad hoc）のネットワークで、ワイヤレス アクセス ポイントを使用しない」をクリックして☐にします。
6. 「OK」をクリックします。

4 「Preferred Networks」に、「ネットワーク名（SSID）」に入力したネットワーク名が追加されたことを確認して、「OK」をクリックします。

5 デスクトップの「マイ　ネットワーク」を右クリックして、表示されるメニューから「プロパティ」をクリックします。

「ネットワークとダイヤルアップ接続」ウィンドウに、現在インストールされているネットワークの一覧が表示されます。

6 一覧に表示されているアイコンにマウスポインタを重ねて「Broadcom BCM4306 Wireless LAN Adapter」と表示されるアイコンを右クリックし、表示されるメニューから「プロパティ」をクリックします。

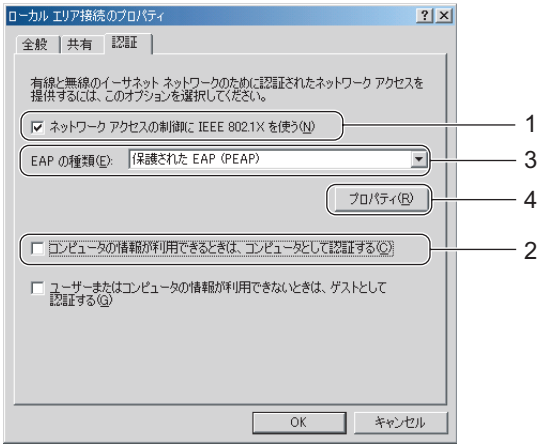
「ローカル エリア接続のプロパティ」ウィンドウが表示されます。

7 「認証」タブをクリックします。

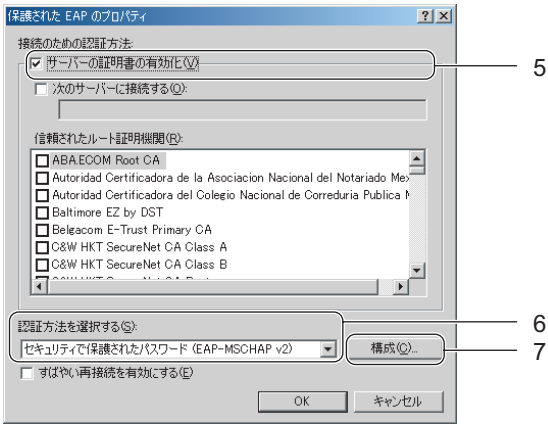
8 次のように設定します。

1. 「ネットワーク アクセスの制御に IEEE 802.1X を使う」をクリックして☑にします。
2. 「コンピュータの情報が利用できるときは、コンピュータとして認証する」をクリックして☐にします。

3.「EAP の種類」の▼をクリックし、「保護された EAP（PEAP）」を選択します。
4.「プロパティ」をクリックします。
「保護された EAP のプロパティ」ウィンドウが表示されます。

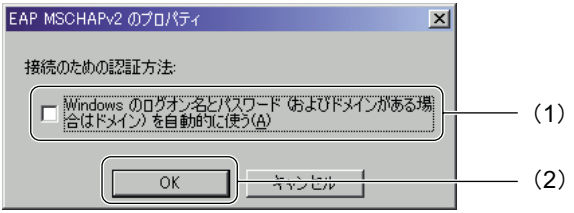


5.「サーバーの証明書の有効化」が☑になっていることを確認します。
6.「認証方法を選択する」で、「セキュリティで保護されたパスワード（EAP-MSCHAP v2）」が選択されていることを確認します。
7.「構成」をクリックします。



「EAP MSCHAPv2 のプロパティ」ウィンドウが表示されます。

8. （1）「Windows のログオン名とパスワード（およびドメインがある場合はドメイン）を自動的に使う」をクリックしてにし、（2）「OK」をクリックします。

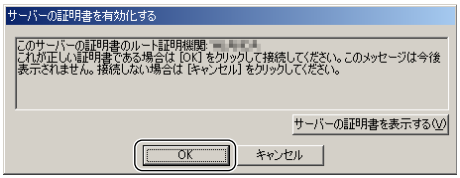


9. 「保護された EAP のプロパティ」ウィンドウで「OK」をクリックします。
10. 「ローカル エリア接続のプロパティ」ウィンドウで「OK」をクリックします。

9 「ログオン資格情報」ウィンドウが表示されますので、（1）ユーザー名、パスワード、ログオンドメインを入力して、（2）「OK」をクリックします。

ユーザー名、パスワード、ログオンドメインは、ネットワーク管理者にご確認ください。

10 「サーバーの証明書を有効化する」ウィンドウが表示されますので、「OK」をクリックします。



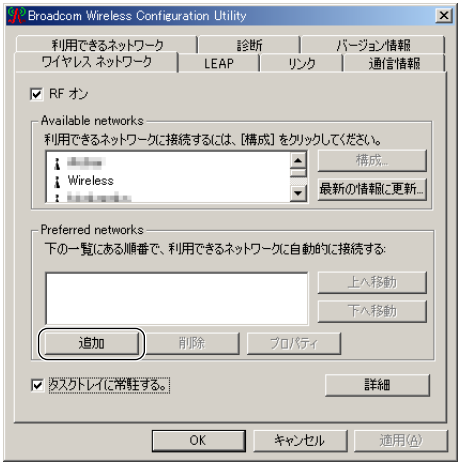
IEEE 802.1X ＋ PEAP-TLS

IEEE 802.1X ＋ PEAP-TLS の場合の設定方法を説明します。

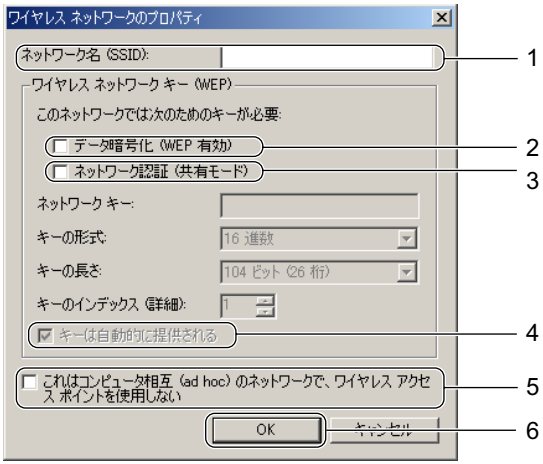
1 **デスクトップ右下の通知領域からユーティリティアイコン（ ）を右クリックし、表示されるメニューから「ユーティリティを開く」をクリックします。**

「Broadcom Wireless Configuration Utility」ウィンドウが表示されます。

2 **「追加」をクリックします。**



3 **「ワイヤレス ネットワークのプロパティ」ウィンドウで次のように設定します。**



1. 「ネットワーク名（SSID）」を、接続する無線 LAN アクセスポイントに合わせて設定します。
2. 「データ暗号化 (WEP 有効)」をクリックして☑にします。
3. 「ネットワーク認証 (共有モード)」をクリックして☐にします。
4. 「キーは自動的に提供される」をクリックして☑にします。
5. 「これはコンピュータ相互（ad hoc）のネットワークで、ワイヤレス アクセスポイントを使用しない」をクリックして☐にします。
6. 「OK」をクリックします。

4 「Preferred Networks」に、「ネットワーク名（SSID）」に入力したネットワーク名が追加されたことを確認して、「OK」をクリックします。

5 デスクトップの「マイ　ネットワーク」を右クリックして、表示されるメニューから「プロパティ」をクリックします。

「ネットワークとダイヤルアップ接続」ウィンドウに、現在インストールされているネットワークの一覧が表示されます。

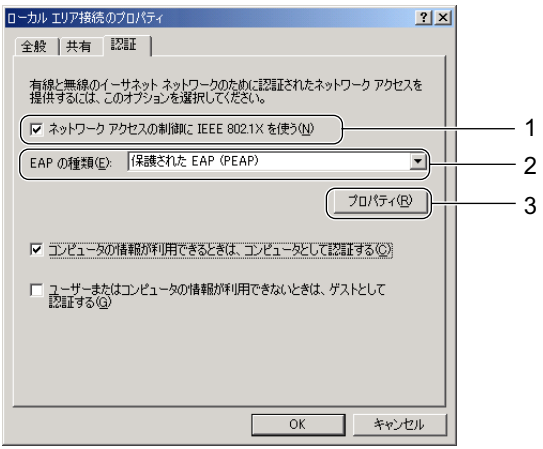
6 一覧に表示されているアイコンにマウスポインタを重ねて「Broadcom BCM4306 Wireless LAN Adapter」と表示されるアイコンを右クリックし、表示されるメニューから「プロパティ」をクリックします。

「ローカル エリア接続のプロパティ」ウィンドウが表示されます。

7 「認証」タブをクリックします。

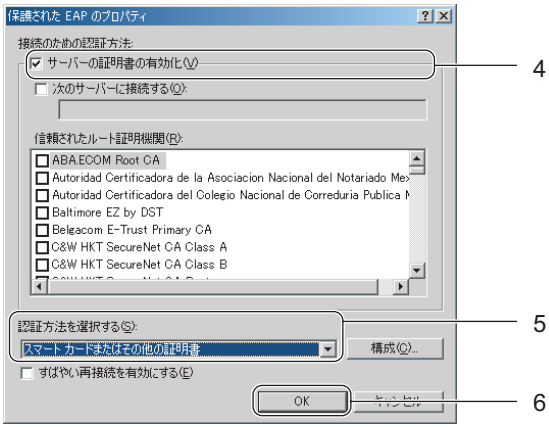
8 次のように設定します。

1. 「ネットワーク アクセスの制御に IEEE 802.1X を使う」をクリックして☑にします。
2. 「EAP の種類」の▼をクリックし、「保護された EAP（PEAP）」を選択します。
3. 「プロパティ」をクリックします。
   「保護された EAP のプロパティ」ウィンドウが表示されます。



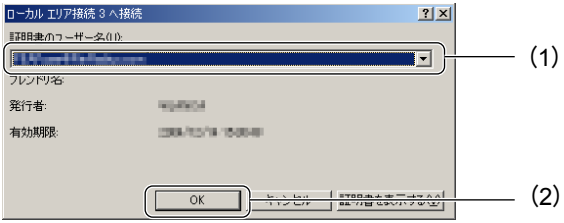
4. 「サーバーの証明書の有効化」が☑になっていることを確認します。

5. 「認証方法を選択する」で、▼をクリックして「スマートカードまたはその他の証明書」を選択します。
6. 「OK」をクリックします。

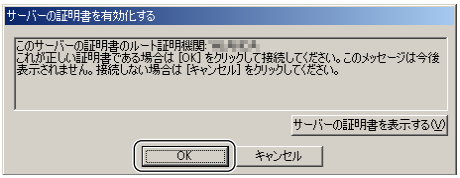


POINT

・パソコンに複数の証明書をインストールしている場合は次の画面が表示されますので、(1)「証明書のユーザー名」を選択して、(2)「OK」をクリックします。



9 「サーバーの証明書を有効化する」ウィンドウが表示されますので、「OK」をクリックします。



15 Intersil 無線 LAN 搭載モデルの設定

クライアントのパソコンに搭載されている無線 LAN のデバイスが、Intersil 無線 LAN 搭載モデルの場合の設定方法を説明します。
なお、ここでは OS が Windows 2000 の場合の設定方法を説明します。OS が Windows XP の場合は、「Windows XP 標準の無線 LAN 機能を使った設定」（→ P.249）をご覧ください。

POINT

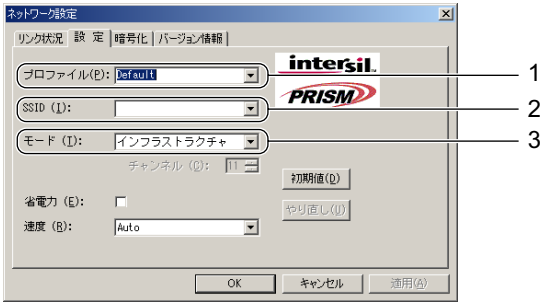
・Windows 2000 Service Pack 4 以降が必要です。
・無線 LAN の設定を行う前に、Windows 2000 が提供する無線 LAN の機能が有効になっている必要があります。次の手順で確認してください。
1. 「スタート」ボタン→「設定」→「コントロールパネル」の順にクリックします。
2. 「管理ツール」をクリックします。
3. 「サービス」をクリックします。
4. 「名前」の一覧で「Wireless Configuration」の「スタートアップの種類」が「自動」になっているかどうか確認します。
「スタートアップの種類」が「手動」や「無効」の場合は、次の手順で「自動」に設定してください。
    1. 「Wireless Configuration」を右クリックし、「プロパティ」をクリックします。
    2. 「スタートアップの種類」で「自動」を選択し、「適用」をクリックします。
    3. 「サービスの状態」で、「開始」をクリックします。
    4. 「OK」をクリックします。
5. 「サービス」ウィンドウ、および「管理ツール」ウィンドウを閉じます。

IEEE 802.1X ＋ EAP-TLS

IEEE 802.1X ＋ EAP-TLS の場合の設定方法を説明します。

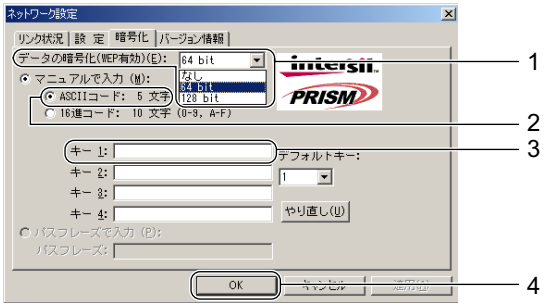
1 「スタート」ボタン→「プログラム」→「PRISM Wireless LAN Configuration」の順にクリックします。
「ネットワーク設定」ウィンドウが表示されます。

2 次のように設定します。



1. 「プロファイル」にプロファイル名を入力します。
2. 「SSID」を、接続する無線 LAN アクセスポイントに合わせて設定します。
3. 「モード」の▼をクリックして、「インフラストラクチャ」を選択します。

3 「暗号化」タブをクリックし、次のように設定します。



1. 「データの暗号化（WEP 有効）」の▼をクリックし、「64 bit」または「128 bit」を選択します。
   無線 LAN アクセスポイントの設定に合わせて設定してください。
   「64 bit」または「128 bit」について
   製品によっては、64 ビットは 40 ビット、128 ビットは 104 ビットと表記されている場合があります。
2. 「ASCII コード」をクリックして◉にします。
3. 「キー 1」に仮の文字列を入力します。「64 bit」の場合は 5 文字、「128 bit」の場合は 13 文字入力します。
   キー1 に入力する文字列は仮の設定です。実際の暗号化には無線 LAN アクセスポイントから通知を受けた文字列を使用します。
4. 「OK」をクリックします。

4 デスクトップの「マイ ネットワーク」を右クリックして、表示されるメニューから「プロパティ」をクリックします。

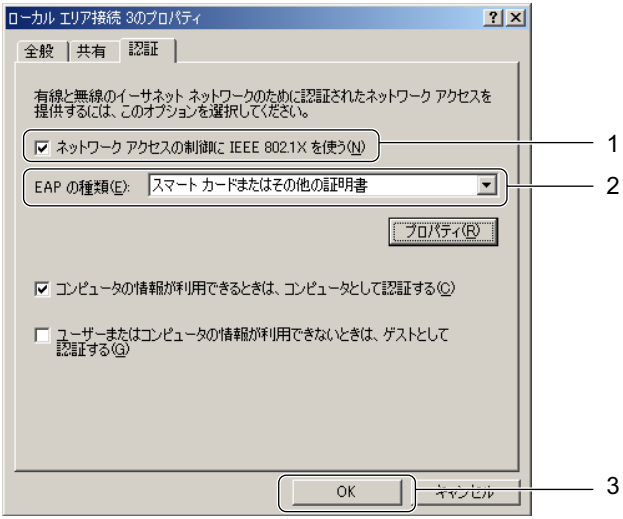
「ネットワークとダイヤルアップ接続」ウィンドウに、現在インストールされているネットワークの一覧が表示されます。

5 **一覧に表示されているアイコンにマウスポインタを重ねて「Intersil PRISM Wireless LAN PCI Card」と表示されるアイコンを右クリックし、表示されるメニューから「プロパティ」をクリックします。**

「ローカル エリア接続のプロパティ」ウィンドウが表示されます。

6 **「認証」タブをクリックします。**

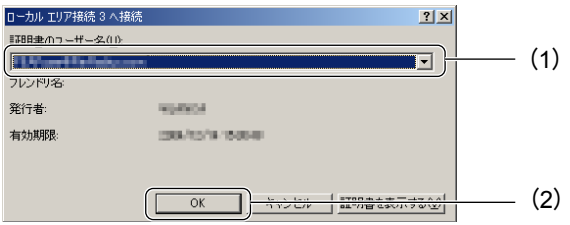
7 **次のように設定します。**



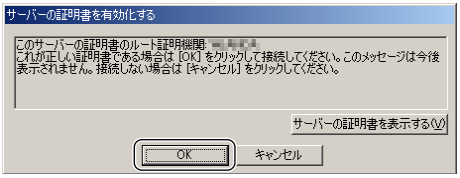
1. 「ネットワークアクセスの制御に IEEE 802.1X を使う」をクリックして☑にします。
2. 「EAP の種類」の▼をクリックして「スマートカードまたはその他の証明書」を選択します。
3. 「OK」をクリックします。

POINT

・パソコンに複数の証明書をインストールしている場合は次の画面が表示されますので、(1)「証明書のユーザー名」を選択して、(2)「OK」をクリックします。



8 **「サーバーの証明書を有効化する」ウィンドウが表示されますので、「OK」をクリックします。**



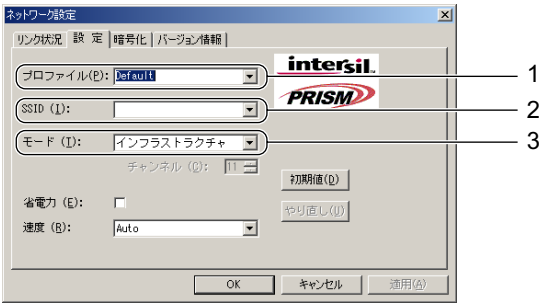
IEEE 802.1X ＋ PEAP-MSCHAPv2 の場合

IEEE 802.1X ＋ PEAP-MSCHAPv2 の場合の設定方法を説明します。

1 **「スタート」ボタン→「プログラム」→「PRISM Wireless LAN Configuration」の順にクリックします。**

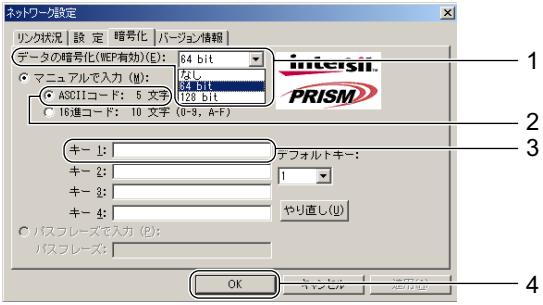
「ネットワーク設定」ウィンドウが表示されます。

2 **次のように設定します。**



1. 「プロファイル」にプロファイル名を入力します。
2. 「SSID」を、接続する無線 LAN アクセスポイントに合わせて設定します。
3. 「モード」の▼をクリックして、「インフラストラクチャ」を選択します。

3 **「暗号化」タブをクリックし、次のように設定します。**



1. 「データの暗号化（WEP 有効）」の▼をクリックし、「64 bit」または「128 bit」を選択します。
   無線 LAN アクセスポイントの設定に合わせて設定してください。
   「64 bit」または「128 bit」について
   製品によっては、64 ビットは 40 ビット、128 ビットは 104 ビットと表記されている場合があります。
2. 「ASCII コード」をクリックして◉にします。
3. 「キー 1」に仮の文字列を入力します。「64 bit」の場合は 5 文字、「128 bit」の場合は 13 文字入力します。
   キー 1 に入力する文字列は仮の設定です。実際の暗号化には無線 LAN アクセスポイントから通知を受けた文字列を使用します。
4. 「OK」をクリックします。

4 デスクトップの「マイ　ネットワーク」を右クリックして、表示されるメニューから「プロパティ」をクリックします。

「ネットワークとダイヤルアップ接続」ウィンドウに、現在インストールされているネットワークの一覧が表示されます。

5 一覧に表示されているアイコンにマウスポインタを重ねて「Intersil PRISM Wireless LAN PCI Card」と表示されるアイコンを右クリックし、表示されるメニューから「プロパティ」をクリックします。

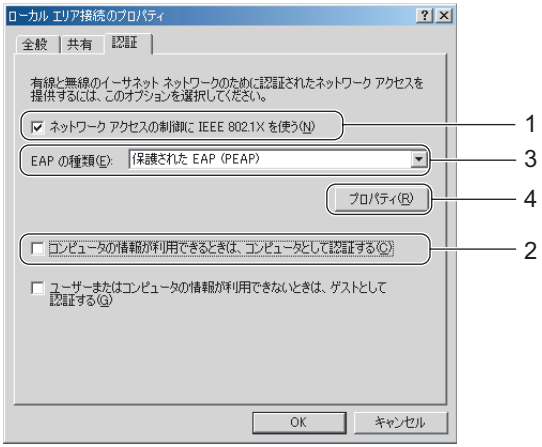
「ローカル エリア接続のプロパティ」ウィンドウが表示されます。

6 「認証」タブをクリックします。

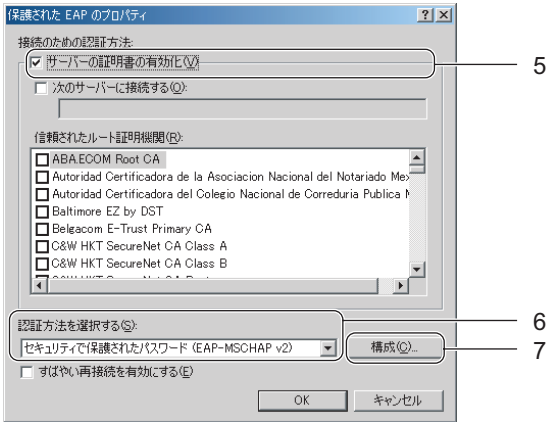
7 次のように設定します。

1. 「ネットワーク アクセスの制御に IEEE 802.1X を使う」をクリックして☑にします。
2. 「コンピュータの情報が利用できるときは、コンピュータとして認証する」をクリックして☐にします。
3. 「EAP の種類」の▼をクリックし、「保護された EAP（PEAP）」を選択します。

4.「プロパティ」をクリックします。
「保護された EAP のプロパティ」ウィンドウが表示されます。

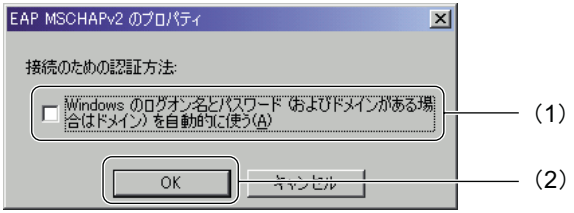


5.「サーバーの証明書の有効化」が☑になっていることを確認します。
6.「認証方法を選択する」で、「セキュリティで保護されたパスワード（EAP-MSCHAP v2）」が選択されていることを確認します。
7.「構成」をクリックします。



「EAP MSCHAPv2 のプロパティ」ウィンドウが表示されます。

8. (1)「Windows のログオン名とパスワード（およびドメインがある場合はドメイン）を自動的に使う」をクリックして☐にし、(2)「OK」をクリックします。

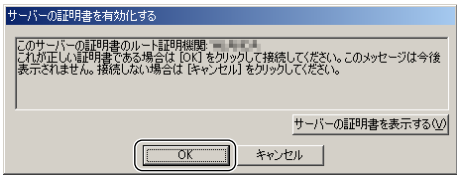


9. 「保護された EAP のプロパティ」ウィンドウで「OK」をクリックします。
10. 「ローカル エリア接続のプロパティ」ウィンドウで「OK」をクリックします。

8 「ログオン資格情報」ウィンドウが表示されますので、(1) ユーザー名、パスワード、ログオンドメインを入力して、(2)「OK」をクリックします。

ユーザー名、パスワード、ログオンドメインは、ネットワーク管理者にご確認ください。

9 「サーバーの証明書を有効化する」ウィンドウが表示されますので、「OK」をクリックします。



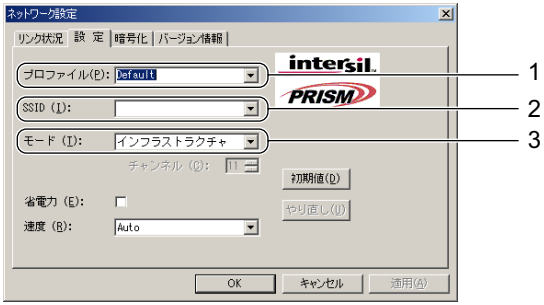
IEEE 802.1X ＋ PEAP-TLS

IEEE 802.1X ＋ PEAP-TLS の場合の設定方法を説明します。

1 「スタート」ボタン→「プログラム」→「PRISM Wireless LAN Configuration」の順にクリックします。

「ネットワーク設定」ウィンドウが表示されます。

2 次のように設定します。



1. 「プロファイル」にプロファイル名を入力します。
2. 「SSID」を、接続する無線 LAN アクセスポイントに合わせて設定します。
3. 「モード」の▼をクリックして、「インフラストラクチャ」を選択します。

3 「暗号化」タブをクリックし、次のように設定します。

1. 「データの暗号化（WEP 有効）」の▼をクリックし、「64 bit」または「128 bit」を選択します。
   無線 LAN アクセスポイントの設定に合わせて設定してください。
   「64 bit」または「128 bit」について
   製品によっては、64 ビットは 40 ビット、128 ビットは 104 ビットと表記されている場合があります。
2. 「ASCII コード」をクリックして◉にします。

3. 「キー 1」に仮の文字列を入力します。「64 bit」の場合は 5 文字、「128 bit」の場合は 13 文字入力します。
   キー1 に入力する文字列は仮の設定です。実際の暗号化には無線 LAN アクセスポイントから通知を受けた文字列を使用します。
4. 「OK」をクリックします。

4 デスクトップの「マイ　ネットワーク」を右クリックして、表示されるメニューから「プロパティ」をクリックします。

「ネットワークとダイヤルアップ接続」ウィンドウに、現在インストールされているネットワークの一覧が表示されます。

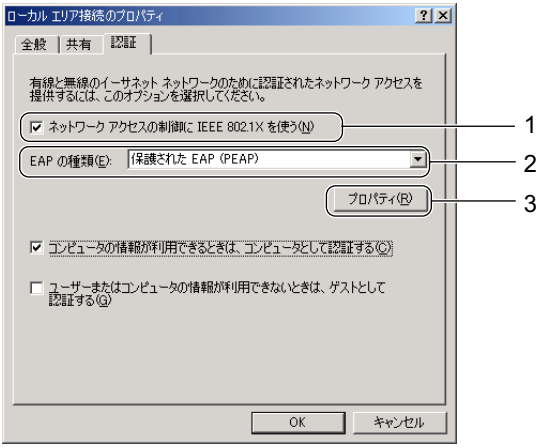
5 一覧に表示されているアイコンにマウスポインタを重ねて「Intersil PRISM Wireless LAN PCI Card」と表示されるアイコンを右クリックし、表示されるメニューから「プロパティ」をクリックします。

「ローカル エリア接続のプロパティ」ウィンドウが表示されます。

6 「認証」タブをクリックします。

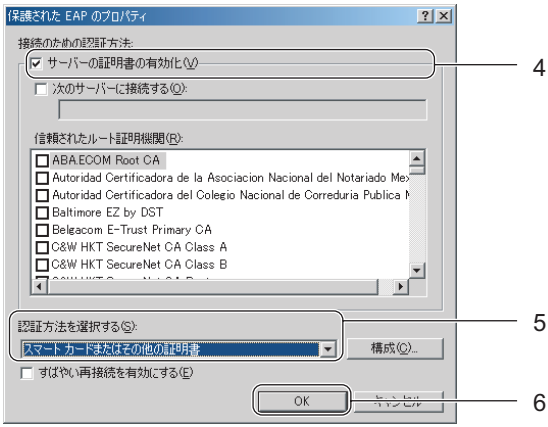
7 次のように設定します。

1. 「ネットワーク アクセスの制御に IEEE 802.1X を使う」をクリックして☑にします。
2. 「EAP の種類」の▼をクリックし、「保護された EAP（PEAP）」を選択します。
3. 「プロパティ」をクリックします。
   「保護された EAP のプロパティ」ウィンドウが表示されます。



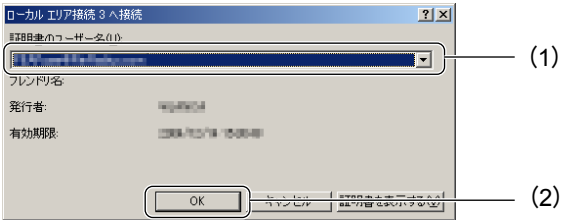
4. 「サーバーの証明書の有効化」が☑になっていることを確認します。
5. 「認証方法を選択する」で、▼をクリックして「スマートカードまたはその他の証明書」を選択します。

6.「OK」をクリックします。

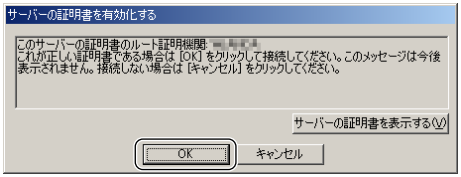


POINT

・パソコンに複数の証明書をインストールしている場合は次の画面が表示されますので、(1)「証明書のユーザー名」を選択して、(2)「OK」をクリックします。



8 「サーバーの証明書を有効化する」ウィンドウが表示されますので、「OK」をクリックします。



4

第 4 章

付録

証明書のインストール方法や、各製品のセキュリティの対応状況、本マニュアルに関連した用語について説明します。

1 その他の設定

ユーザー証明書のインストール方法について説明します。

クライアント証明書（ユーザー証明書）のインストール

ここでは、Windows 2000 Server または Windows Server 2003 を使用して構築された証明機関から有線 LAN 経由でクライアント証明書（ユーザー証明書）をインストールする方法を説明します。
これ以外の証明機関を使用する場合は、それぞれの証明機関のマニュアルなどをご覧ください。
また、Web ブラウザ以外の方法でクライアント証明書をインストールする場合は、使用する証明機関のマニュアルなどをご覧ください。

POINT

Windows Vista をお使いの場合

Windows Vista をお使いの場合は、Web ブラウザ経由でクライアント証明書（ユーザー証明書）をインストールできない場合があります。

1 証明機関が設置されているネットワークにクライアントのパソコンを有線 LAN 経由で接続し、IP アドレスを設定または取得します。

2 Web ブラウザを起動し、アドレスに以下のように入力します。

http://[証明機関の IP アドレス]/certsrv/
例）証明機関の IP アドレスが、192.168.1.5 の場合
http://192.168.1.5/certsrv/

3 ログインメニューが表示されたら、それぞれのユーザー名 / パスワードでログインします。

Microsoft 証明書サービスが表示されます。

4 「タスクの選択」の中から、「証明書を要求する」をクリックします。

5 「証明書の種類の選択」の中から、「ユーザー証明書」をクリックします。

6 「送信」をクリックします。

POINT

・「潜在するスクリプト違反」などのメッセージが表示される場合があります。このような場合には、「はい」をクリックしてください。

7 「証明書は発行されました」と表示されたら、「この証明書のインストール」をクリックします。

POINT

・「潜在するスクリプト違反」などのメッセージが表示される場合があります。このような場合には、「はい」をクリックしてください。

「インストールされた証明書」に「新しい証明書は正しくインストールされました。」と表示されたら、証明書のインストールは終了です。

2 サーバーの設定

サーバーの設定例について説明します。

Windows 2000 Server の設定

Windows 2000 Server を RADIUS サーバーとして使用する場合の設定方法を説明します。
Windows 2000 Server にあらかじめ「インターネット認証サービス」から新しいリモートアクセスポリシーを作成し、無線 LAN アクセスポイントをクライアントとして登録してください。その後、次の項目について確認してください。
詳しい設定方法については、OS のマニュアルをご覧ください。

重要

Windows 2000 Server の事前設定について

Windows 2000 Server には、あらかじめ以下の設定を行ってください。設定方法は、OS のマニュアルをご覧ください。

- Windows 2000 Service Pack 4 を適用する。
- Active Directory へ追加する。
- 認証用のユーザー登録と認証用のセキュリティグループを登録する。
- RADIUS サーバー用のアカウントで証明機関より証明書を発行してもらい、証明書をインストールする。
- インターネット認証サービスをインストールする。

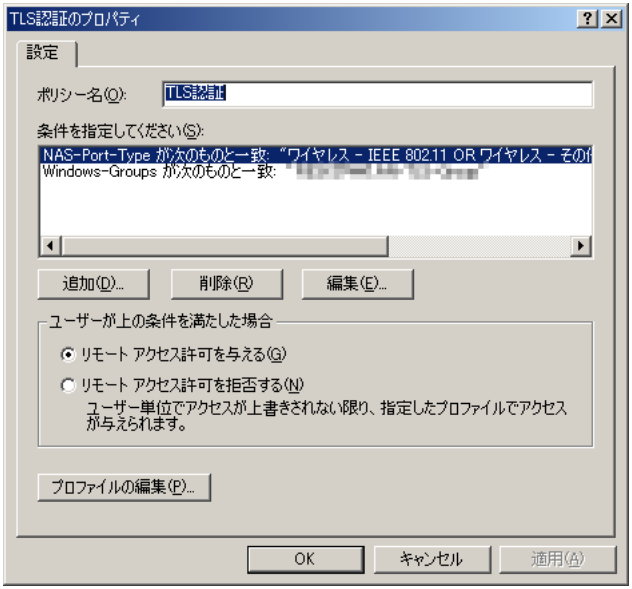
サーバーの設定は、認証方式の種類によって異なります。認証方式の種類によって、次をご覧ください。

- 「認証方式が EAP-TLS の場合」（→ P.338）
- 「認証方式が PEAP-MSCHAPv2 の場合」（→ P.340）
- 「認証方式が PEAP-TLS の場合」（→ P.343）

■ 認証方式が EAP-TLS の場合

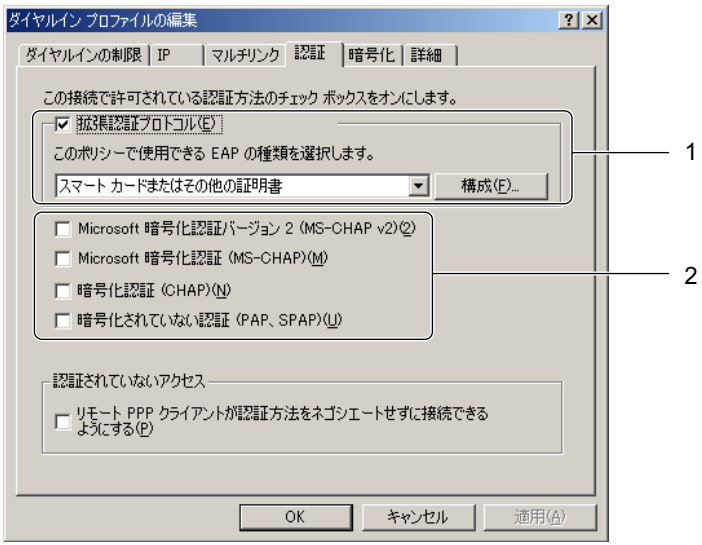
□ 作成したプロファイルのプロパティの設定

「リモートアクセスポリシー」の中から、作成したプロファイルのプロパティが次の図のように設定されているか確認します。



□ ポリシー条件の設定

作成したプロファイルのプロパティ画面で「プロファイルの編集」をクリックして、「認証」タブの画面で確認します。



1 拡張認証プロトコル

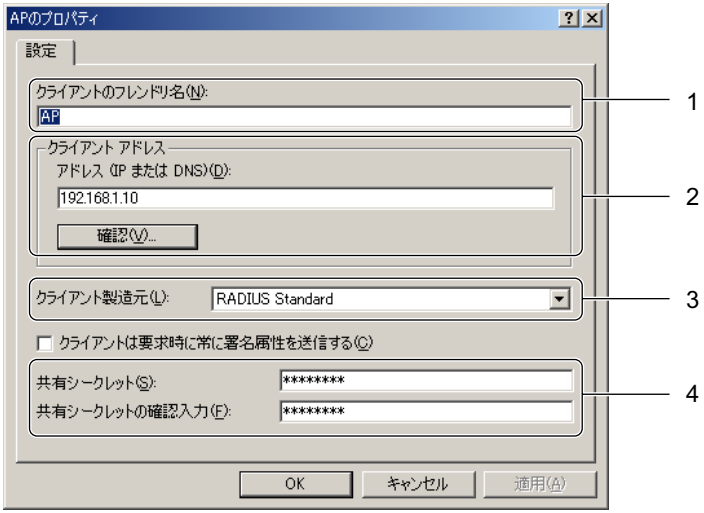
「スマートカードまたはその他の証明書」が選択されていることを確認し、「構成」をクリックして使用する証明機関が選択されていることを確認してください。

2 その他の認証方法

チェックボックスが☐になっていることを確認してください。

☐ RADIUS クライアントのプロパティの設定

RADIUS クライアントのプロパティの設定を確認します。



1 クライアントのフレンドリ名

無線 LAN アクセスポイントの識別名が入力されていることを確認してください。

2 クライアントアドレス

無線 LAN アクセスポイントの IP アドレスが入力されていることを確認してください。

3 クライアント製造元

「RADIUS Standard」が選択されていることを確認してください。

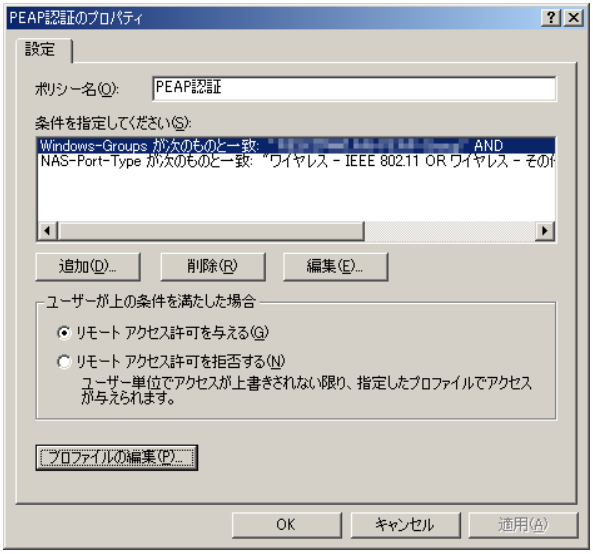
4 共有シークレット／共有シークレットの確認入力

無線 LAN アクセスポイントと共通の値を入力したか確認してください。

■ 認証方式が PEAP-MSCHAPv2 の場合

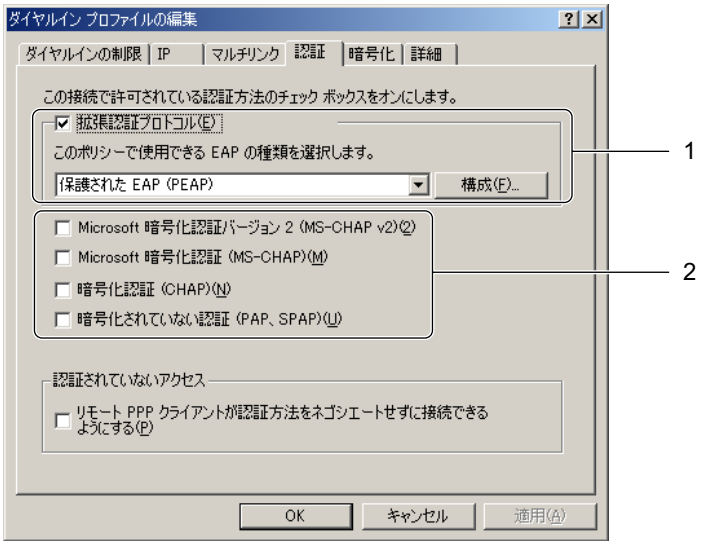
☐ 作成したプロファイルのプロパティの設定

「リモートアクセスポリシー」の中から、作成したプロファイルのプロパティが次の図のように設定されているか確認します。



□ ポリシー条件の設定

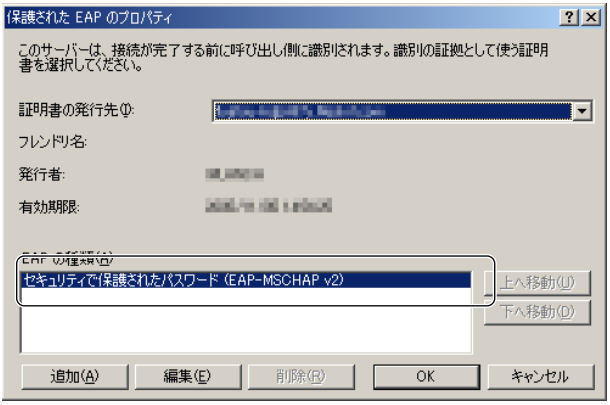
作成したプロファイルのプロパティ画面で「プロファイルの編集」をクリックして、「認証」タブの画面が次のように設定されているか確認します。



1 拡張認証プロトコル

「保護された EAP（PEAP）」が選択されていることを確認します。

また、「構成」をクリックし、「EAP の種類」に「セキュリティで保護されたパスワード（EAP-MSCHAP v2）」が登録されていることを確認してください。

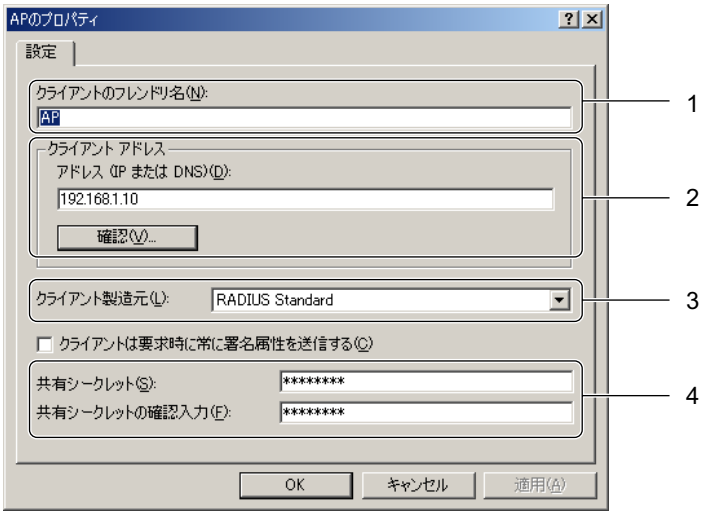


2 その他の認証方法

チェックボックスが☐になっていることを確認してください。

☐ RADIUS クライアントのプロパティの設定

RADIUS クライアントから作成した RADIUS クライアントのプロパティの設定を確認します。



1 クライアントのフレンドリ名

無線 LAN アクセスポイントの識別名が入力されていることを確認してください。

2 クライアントアドレス

無線 LAN アクセスポイントの IP アドレスが入力されていることを確認してください。

3 クライアント製造元

「RADIUS Standard」が選択されていることを確認してください。

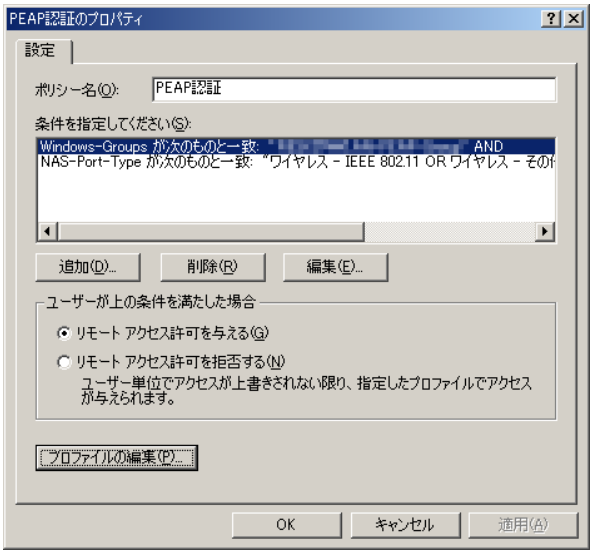
4 共有シークレット／共有シークレットの確認入力

無線 LAN アクセスポイントと共通の値を入力したか確認してください。

■認証方式が PEAP-TLS の場合

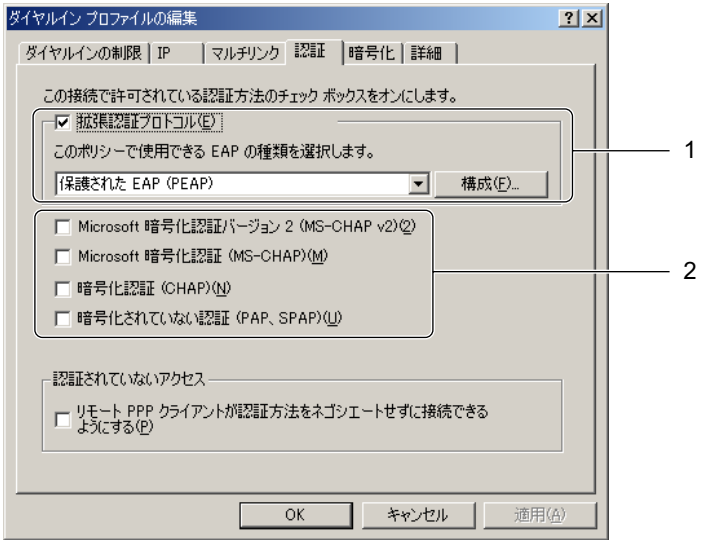
□ 作成したプロファイルのプロパティの設定

「リモートアクセスポリシー」の中から、作成したプロファイルのプロパティが次の図のように設定されているか確認します。



□ ポリシー条件の設定

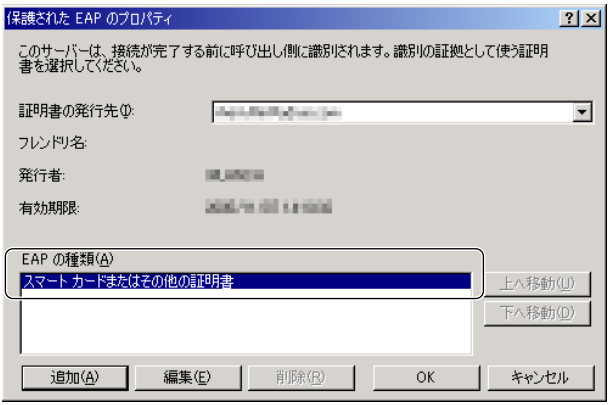
作成したプロファイルのプロパティ画面で「プロファイルの編集」をクリックして、「認証」タブの画面が次のように設定されているか確認します。



1 拡張認証プロトコル

「保護された EAP（PEAP)」が選択されていることを確認します。

また、「構成」をクリックし、「EAP の種類」に「スマートカードまたはその他の証明書」が登録されていることを確認してください。

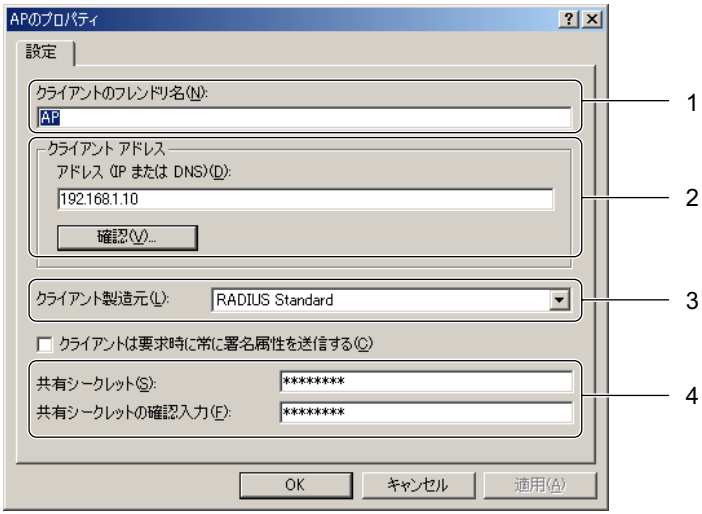


2 その他の認証方法

チェックボックスが□になっていることを確認してください。

□ RADIUS クライアントのプロパティの設定

RADIUS クライアントから作成した RADIUS クライアントのプロパティの設定を確認します。



1 クライアントのフレンドリ名

無線 LAN アクセスポイントの識別名が入力されていることを確認してください。

2 クライアントアドレス

無線 LAN アクセスポイントの IP アドレスが入力されていることを確認してください。

3 クライアント製造元

「RADIUS Standard」が選択されていることを確認してください。

4 共有シークレット／共有シークレットの確認入力

無線 LAN アクセスポイントと共通の値を入力したか確認してください。

Windows Server 2003 の設定

Windows Server 2003 を RADIUS サーバーとして使用する場合の設定方法を説明します。
Windows Server 2003 にあらかじめ「インターネット認証サービス」から新しいリモートアクセスポリシーを作成し、無線 LAN アクセスポイントをクライアントとして登録してください。その後、次の項目について設定を確認してください。
詳しい設定方法については、OS のマニュアルをご覧ください。

重要

Windows Server 2003 の事前設定について

Windows Server 2003 には、あらかじめ次の設定を行ってください。設定方法は、OS のマニュアルをご覧ください。

- **Active Directory へ追加する。**
- **認証用のユーザー登録と認証用のセキュリティグループを登録する。**
- **RADIUS サーバー用のアカウントで証明機関より証明書を発行してもらい、証明書をインストールする。**
- **インターネット認証サービスをインストールする。**

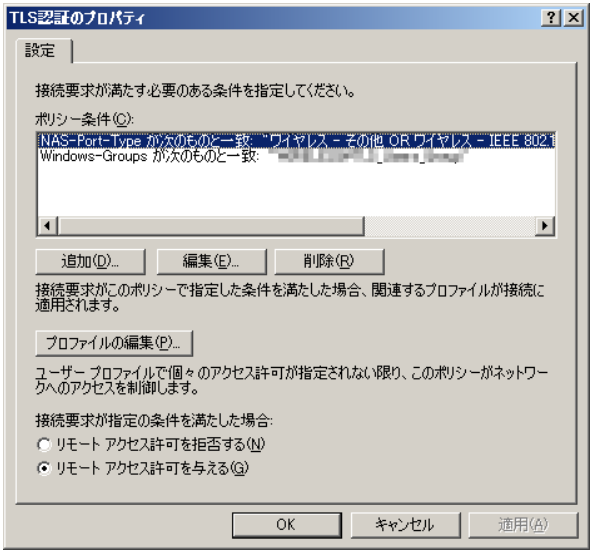
サーバーの設定は、認証方式の種類によって異なります。認証方式の種類によって、次をご覧ください。

・「認証方式が EAP-TLS の場合」(→ P.346)
・「認証方式が PEAP-MSCHAPv2 の場合」(→ P.349)
・「認証方式が PEAP-TLS の場合」(→ P.353)

■ 認証方式が EAP-TLS の場合

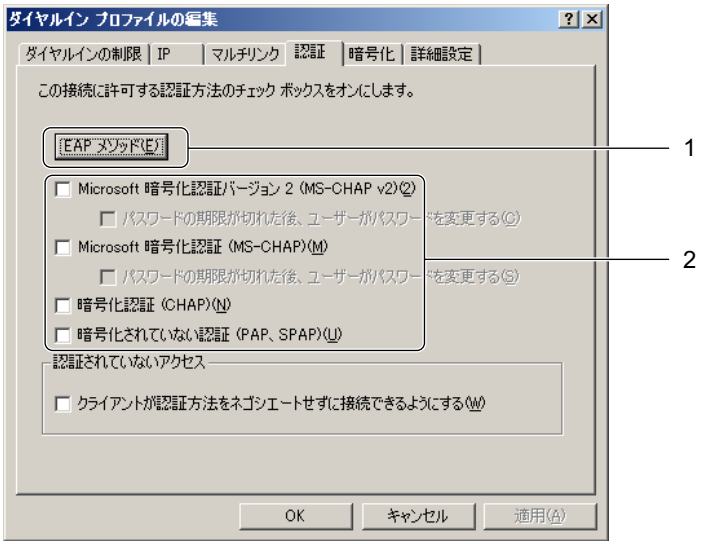
□ 作成したプロファイルのプロパティの設定

「リモートアクセスポリシー」の中から、作成したプロファイルのプロパティが次の図のように設定されているか確認します。



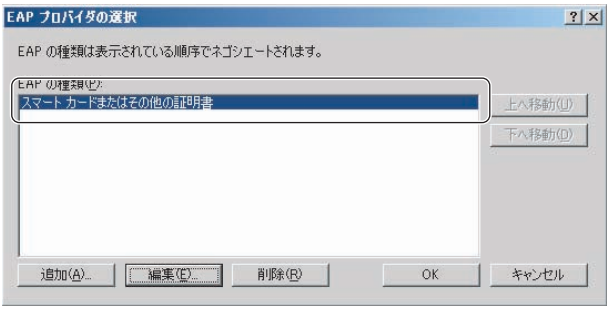
□ ポリシー条件の設定

作成したプロファイルのプロパティ画面で「プロファイルの編集」をクリックして、「認証」タブの画面が次のようになっているか確認します。



1 EAP メソッド

「EAP メソッド」をクリックし、「EAP の種類」に「スマート カードまたはその他の証明書」が登録されていることを確認してください。

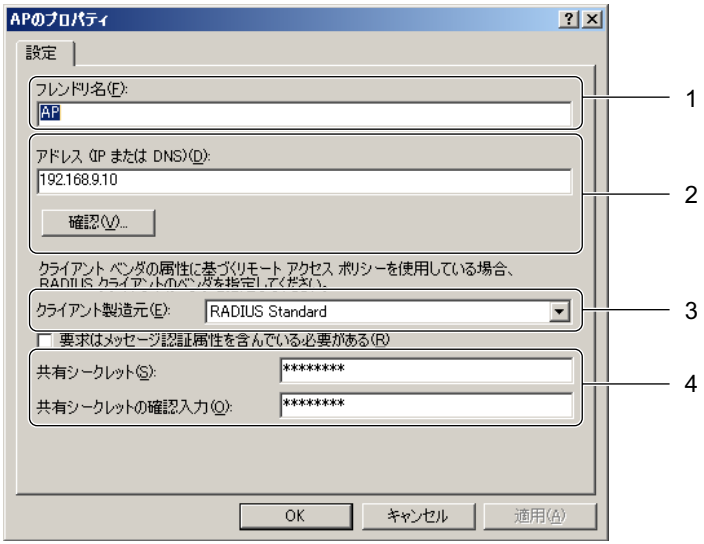


2 その他の認証方法

チェックボックスが☐になっていることを確認してください。

☐ RADIUS クライアントのプロパティの設定

RADIUS クライアントから作成した RADIUS クライアントのプロパティの設定を確認します。



1 フレンドリ名

無線 LAN アクセスポイントの識別名が入力されていることを確認してください。

2 アドレス（IP または DNS）

無線 LAN アクセスポイントの IP アドレスが入力されていることを確認してください。

3 クライアント製造元

「RADIUS Standard」が選択されていることを確認してください。

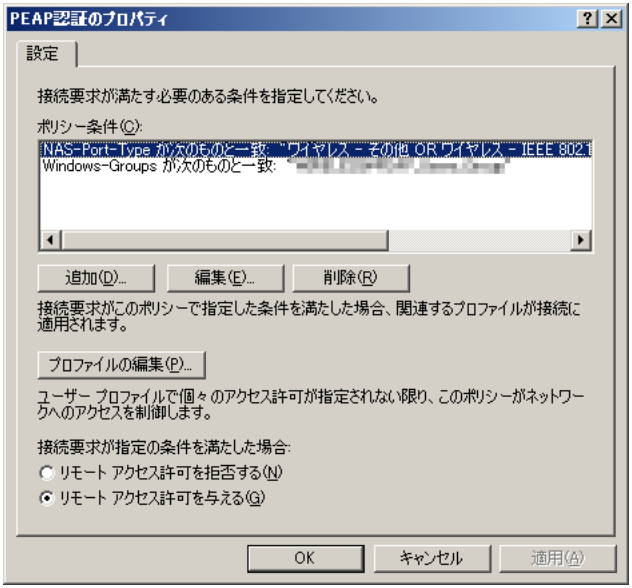
4 共有シークレット／共有シークレットの確認入力

無線 LAN アクセスポイントと共通の値を入力したか確認してください。

■認証方式が PEAP-MSCHAPv2 の場合

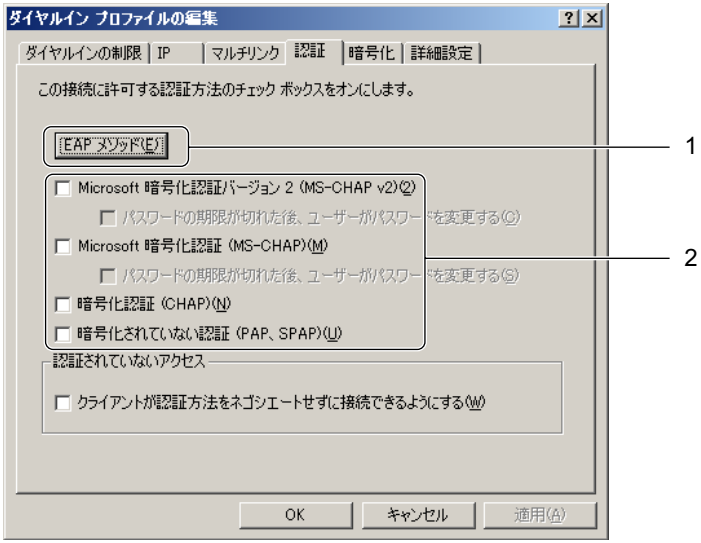
□ 作成したプロファイルのプロパティの設定

「リモートアクセスポリシー」の中から、作成したプロファイルのプロパティが次の図のように設定されているか確認します。



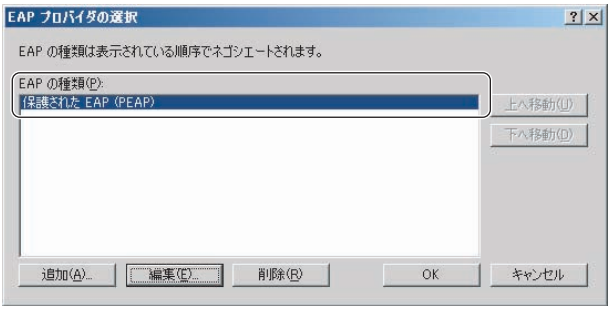
□ ポリシー条件の設定

作成したプロファイルのプロパティ画面で「プロファイルの編集」をクリックして、「認証」タブの画面が次のようになっているか確認します。

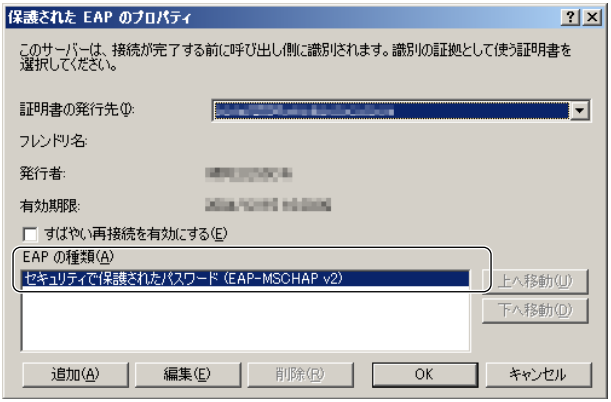


1 EAP メソッド

「EAP メソッド」をクリックし、「EAP の種類」に「保護された EAP（PEAP)」が登録されていることを確認してください。



また、「編集」をクリックし、「EAP の種類」に「セキュリティで保護されたパスワード（EAP-MSCHAP v2)」が登録されていることを確認してください。

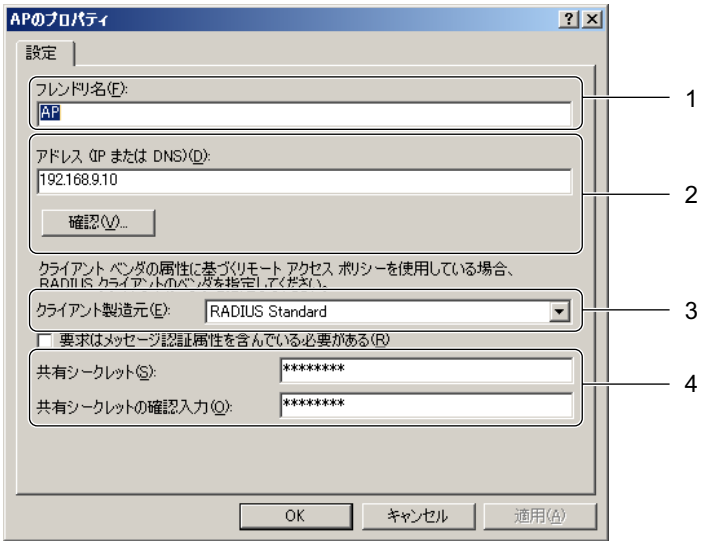


2 その他の認証方法

チェックボックスが☐になっていることを確認してください。

□ RADIUS クライアントのプロパティの設定

RADIUS クライアントから作成した RADIUS クライアントのプロパティの設定を確認します。



1 フレンドリ名

無線 LAN アクセスポイントの識別名が入力されていることを確認してください。

2 アドレス（IP または DNS）

無線 LAN アクセスポイントの IP アドレスが入力されていることを確認してください。

3 クライアント製造元

「RADIUS Standard」が選択されていることを確認してください。

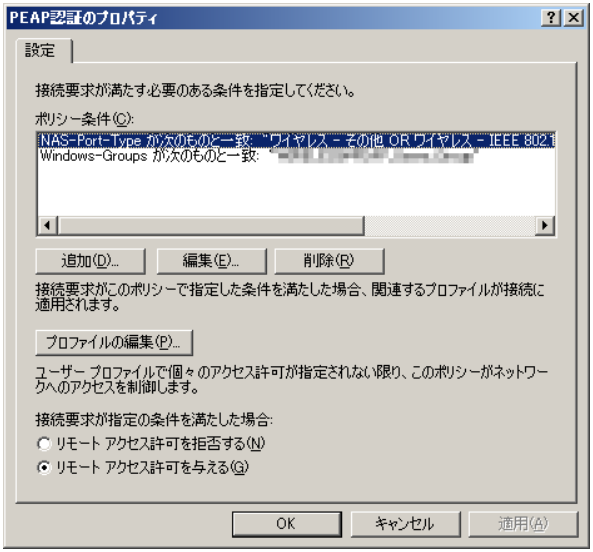
4 共有シークレット／共有シークレットの確認入力

無線 LAN アクセスポイントと共通の値を入力したか確認してください。

■認証方式が PEAP-TLS の場合

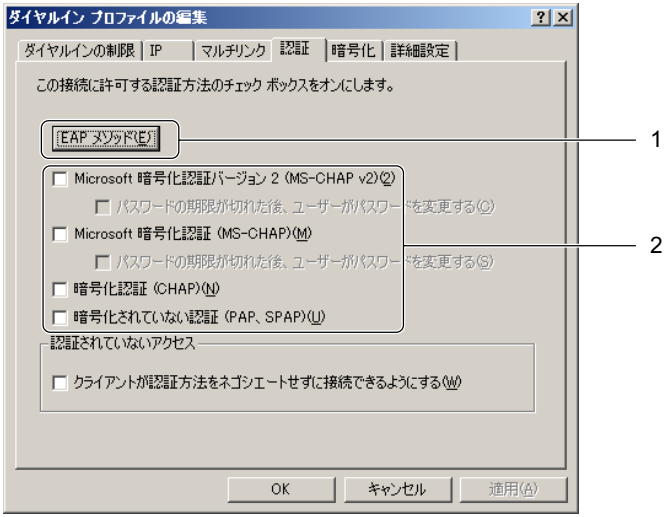
□ 作成したプロファイルのプロパティの設定

「リモートアクセスポリシー」の中から、作成したプロファイルのプロパティが次の図のように設定されているか確認します。



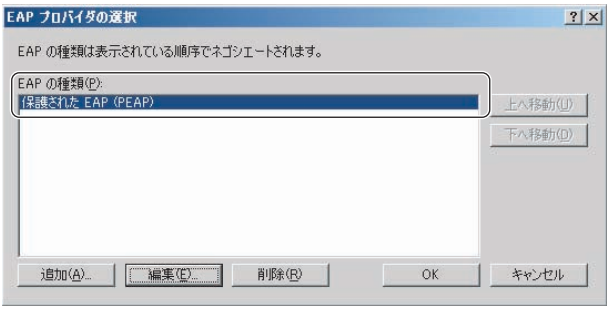
□ ポリシー条件の設定

作成したプロファイルのプロパティ画面で「プロファイルの編集」をクリックして、「認証」タブの画面が次のようになっているか確認します。

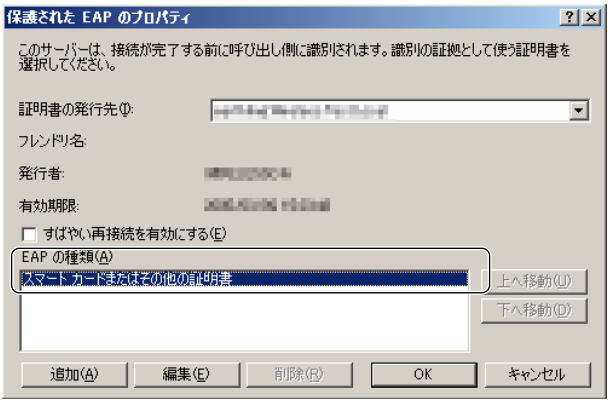


1 EAP メソッド

「EAP メソッド」をクリックし、「EAP の種類」に「保護された EAP（PEAP)」が登録されていることを確認してください。



「編集」をクリックし、「EAP の種類」に「スマートカードまたはその他の証明書」が登録されていることを確認してください。

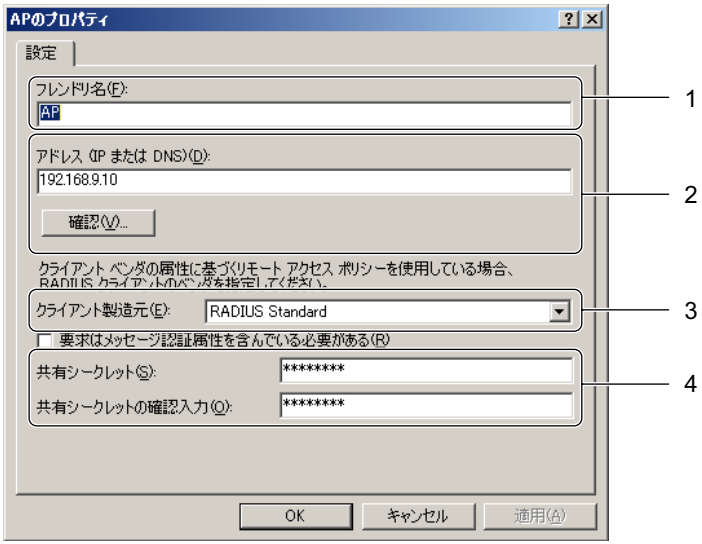


2 その他の認証方法

チェックボックスが☐になっていることを確認してください。

□ RADIUS クライアントのプロパティの設定

RADIUS クライアントから作成した RADIUS クライアントのプロパティの設定を確認します。



1 フレンドリ名

無線 LAN アクセスポイントの識別名が入力されていることを確認してください。

2 アドレス（IP または DNS）

無線 LAN アクセスポイントの IP アドレスが入力されていることを確認してください。

3 クライアント製造元

「RADIUS Standard」が選択されていることを確認してください。

4 共有シークレット／共有シークレットの確認入力

無線 LAN アクセスポイントと共通の値を入力したか確認してください。

3 各製品の対応状況

無線 LAN アクセスポイントおよび無線 LAN クライアントのセキュリティの対応状況は、次のとおりです。

無線 LAN アクセスポイントの対応状況

無線 LAN アクセスポイントのセキュリティの対応状況は次のとおりです。

凡例 ■：対応 □：未対応

表：無線 LAN アクセスポイントの対応状況

製品	対応状況				
	IEEE 802.1X	WEP キー	WPA		認証方式
FMWT-56AG ／ FMWT-55AG ／ FMWT-54AG	対応済	■ 40bit ■ 104bit ■ 128bit	■ WPA ■ WPA2	暗号化方式 ■ TKIP ■ AES	■ EAP-TLS ■ PEAP-MSCHAPv2 ■ PEAP-TLS □ LEAP
FMWT-53 シリーズ	対応済	■ 40bit ■ 104bit ■ 128bit	■ WPA □ WPA2	暗号化方式 ■ TKIP □ AES	■ EAP-TLS ■ PEAP-MSCHAPv2 ■ PEAP-TLS □ LEAP
FMWT-52 シリーズ	対応済	■ 40bit ■ 104bit □ 128bit	□ WPA □ WPA2	―	■ EAP-TLS ■ PEAP-MSCHAPv2 ■ PEAP-TLS □ LEAP
FMWBR-201	対応済	■ 40bit ■ 104bit ■ 128bit	■ WPA □ WPA2	暗号化方式 ■ TKIP ■ AES	■ EAP-TLS ■ PEAP-MSCHAPv2 ■ PEAP-TLS □ LEAP
FMWBR-102	対応済	■ 40bit ■ 104bit □ 128bit	□ WPA □ WPA2	―	■ EAP-TLS ■ PEAP-MSCHAPv2 ■ PEAP-TLS □ LEAP
FMWBR-101	未対応	■ 40bit ■ 104bit □ 128bit	□ WPA □ WPA2	―	□ EAP-TLS □ PEAP-MSCHAPv2 □ PEAP-TLS □ LEAP
FMWT-501	対応済	■ 40bit □ 104bit □ 128bit	□ WPA □ WPA2	―	□ EAP-TLS □ PEAP-MSCHAPv2 □ PEAP-TLS □ LEAP

無線 LAN クライアントの対応状況

無線 LAN クライアントのセキュリティの対応状況は次のとおりです。

凡例 ■: 対応 □: 未対応

表：無線 LAN クライアントの対応状況

無線 LAN 搭載モデル名または製品名（デバイス名）	ドライババージョン	対応状況				
		IEEE 802.1X	WEP キー	WPA		認証方式
Atheros 無線 LAN 搭載モデル （Atheros AR5001X ＋ Wireless Network Adapter） （Atheros AR5006X ＋ Wireless Network Adapter） （Atheros AR5006EXS Wireless Network Adapter） （Atheros AR5007EG Wireless Network Adapter） （Atheros AR5008X Wireless Network Adapter） ワイヤレス LAN カード FMV-JW482 ワイヤレス LAN カード FMV-JW481	v7.x	対応済	■ 40bit ■ 104bit □ 128bit	■ WPA ■ WPA2	暗号化方式 ■ TKIP ■ AES	■ EAP-TLS ■ PEAP-MSCHAPv2 ■ PEAP-TLS ■ LEAP
	v4.x	対応済	■ 40bit ■ 104bit ■ 128bit	■ WPA ■ WPA2	暗号化方式 ■ TKIP ■ AES	■ EAP-TLS ■ PEAP-MSCHAPv2 ■ PEAP-TLS［注 1］ ■ LEAP
	v3.x	対応済	■ 40bit ■ 104bit ■ 128bit	■ WPA □ WPA2	暗号化方式 ■ TKIP ■ AES	■ EAP-TLS ■ PEAP-MSCHAPv2 □ PEAP-TLS ■ LEAP
	v2.x	対応済	■ 40bit ■ 104bit ■ 128bit	■ WPA □ WPA2	暗号化方式 ■ TKIP ■ AES	■ EAP-TLS ■ PEAP-MSCHAPv2 □ PEAP-TLS ■ LEAP
Intel 無線 LAN 搭載モデル （Intel(R) Wireless WiFi Link 4965AG） （Intel(R) PRO/Wireless 3945ABG Network Connection） （Intel(R) PRO/Wireless LAN 2915ABG Network Connection） （Intel(R) PRO/Wireless LAN 2200BG Network Connection） （Intel(R) PRO/Wireless LAN 2100 3B Mini PCI Adapter）	v11.x	対応済	■ 40bit ■ 104bit □ 128bit	■ WPA ■ WPA2	暗号化方式 ■ TKIP ■ AES	■ EAP-TLS ■ PEAP-MSCHAPv2 ■ PEAP-TLS ■ LEAP
	v10.x	対応済	■ 40bit ■ 104bit □ 128bit	■ WPA ■ WPA2	暗号化方式 ■ TKIP ■ AES	■ EAP-TLS ■ PEAP-MSCHAPv2 ■ PEAP-TLS ■ LEAP
	v9.x	対応済	■ 40bit ■ 104bit □ 128bit	■ WPA ■ WPA2	暗号化方式 ■ TKIP ■ AES	■ EAP-TLS ■ PEAP-MSCHAPv2 ■ PEAP-TLS ■ LEAP
	v8.x	対応済	■ 40bit ■ 104bit □ 128bit	■ WPA □ WPA2	暗号化方式 ■ TKIP ■ AES	■ EAP-TLS ■ PEAP-MSCHAPv2 ■ PEAP-TLS ■ LEAP
	v1.x	対応済	■ 40bit ■ 104bit □ 128bit	■ WPA ■ WPA2［注 1］	暗号化方式 ■ TKIP □ AES	■ EAP-TLS ■ PEAP-MSCHAPv2 ■ PEAP-TLS ■ LEAP
Broadcom 無線 LAN 搭載モデル （Broadcom BCM4306 Wireless LAN Adapter）	―	対応済	■ 40bit ■ 104bit □ 128bit	■ WPA［注 2］ □ WPA2	暗号化方式 ■ TKIP □ AES	■ EAP-TLS ■ PEAP-MSCHAPv2 ■ PEAP-TLS □ LEAP

表：無線 LAN クライアントの対応状況

無線 LAN 搭載モデル名または製品名（デバイス名）	ドライババージョン	対応状況				
		IEEE 802.1X	WEP キー	WPA		認証方式
Intersil 無線 LAN 搭載モデル （Intersil PRISM Wireless LAN PCI Card） ワイヤレス LAN カード FMV-W182	―	対応済	■ 40bit ■ 104bit □ 128bit	■ WPA［注 2］ □ WPA2	暗号化方式 ■ TKIP □ AES	■ EAP-TLS ■ PEAP-MSCHAPv2 ■ PEAP-TLS □ LEAP
ワイヤレス LAN カード FMV-JW381	―	未対応	■ 40bit ■ 104bit ■ 128bit	□ WPA □ WPA2	―	□ EAP-TLS □ PEAP-MSCHAPv2 □ PEAP-TLS □ LEAP
ワイヤレス LAN カード FMV-JW183	―	対応済	■ 40bit ■ 104bit □ 128bit	■ WPA［注 2］ □ WPA2	暗号化方式 ■ TKIP □ AES	■ EAP-TLS ■ PEAP-MSCHAPv2 ■ PEAP-TLS □ LEAP
ワイヤレス LAN カード FMV-JW182	―	未対応	■ 40bit ■ 104bit □ 128bit	□ WPA □ WPA2	―	□ EAP-TLS □ PEAP-MSCHAPv2 □ PEAP-TLS □ LEAP
ワイヤレス LAN カード FMV-JW181 ワイヤレス LAN カード FMV-W181	―	未対応	■ 40bit □ 104bit □ 128bit	□ WPA □ WPA2	―	□ EAP-TLS □ PEAP-MSCHAPv2 □ PEAP-TLS □ LEAP

注 1　富士通製品情報ページに公開されている最新版のドライバをインストールする必要があります。
注 2　Windows XP のみ対応。

無線 LAN クライアントのシングルサインオン動作確認情報

シングルサインオンを使用した Windows ログオンの動作が確認されているのは、次の標準搭載モデルのデバイス、およびワイヤレス LAN カードです。

・Atheros 無線 LAN 搭載モデル
・Intel 無線 LAN 搭載モデル
・ワイヤレス LAN カード FMV-JW481
・ワイヤレス LAN カード FMV-JW482

POINT

シングルサインオンを使用した Windows ログオン機能をお使いになる場合

・Atheros 無線 LAN 搭載モデル、FMV-JW481、および FMV-JW482 でシングルサインオンを使用する場合は、ドライバの再インストールが必要になります。
インストール手順は、それぞれ次をご覧ください。
  ・Atheros 無線 LAN 搭載モデルの場合
  パソコンに添付の「ドライバーズディスク」に格納されている、無線 LAN ドライバの「Install.txt」をご覧ください。
  ・FMV-JW481 ／ FMV-JW482 の場合
  製品に添付のマニュアルをご覧ください。
・Intel 無線 LAN 搭載モデルでシングルサインオンを使用する場合は、初期設定が必要です。
初期設定については、ユーティリティバージョンによって、それぞれ次の該当する項目をご覧ください。
  ・ユーティリティバージョンが v 10.5.x ／ v11.x の場合
  「シングルサインオン／ドメインログオンを使用する場合のプログラムの追加」（→ P.94）
  ・ユーティリティバージョンが v10.1.x の場合
  「シングルサインオン／ドメインログオンを使用する場合のプログラムの追加」（→ P.140）
  ・ユーティリティバージョンが v9.x の場合
  「シングルサインオン／ドメインログオンを使用する場合のプログラムの追加」（→ P.175）
  ・ユーティリティバージョンが v8.x ／ v7.x の場合
  「シングルサインオン／ドメインログオンを使用する場合のプログラムの追加」（→ P.202）

シングルサインオンを使用した Windows ログオン機能に対応していないデバイス

次の標準搭載モデル、およびワイヤレス LAN カードではシングルサインオンを使用した Windows ログオンに対応していません。

・Broadcom 無線 LAN 搭載モデル
・Intersil 無線 LAN 搭載モデル
・FMV-JW381
・FMV-JW183
・FMV-JW182
・FMV-JW181
・FMV-W182
・FMV-W181

■動作確認情報

デバイスやドライババージョンによって、シングルサインオン機能をどの認証方式で使用できるかが異なります。以下のシングルサインオンを使用した Windows ログオンの動作確認情報の表をご確認ください。
なお、「PEAP-GTC」、「EAP-FAST」、「TTLS」については、動作確認のみです。

POINT

- **富士通製品情報ページに公開されている最新版のドライバをインストールする必要があります。**

凡例　■：該当の機能の動作を確認しています。
　　□：該当の機能は動作しません。

表：シングルサインオンを使用した Windows ログオンの動作確認情報

無線 LAN 搭載モデル名または製品名 （デバイス名）	ドライババージョン	シングルサインオン可能な認証方式
Atheros 無線 LAN 搭載モデル （Atheros AR5001X ＋ Wireless Network Adapter） （Atheros AR5006X ＋ Wireless Network Adapter） （Atheros AR5006EXS Wireless Network Adapter） （Atheros AR5007EG Wireless Network Adapter） （Atheros AR5008X Wireless Network Adapter） ワイヤレス LAN カード FMV-JW482 ワイヤレス LAN カード FMV-JW481	v7.x ／ v4.x ／ v3.x	■ PEAP-MSCHAPv2 ■ LEAP ■ PEAP-GTC □ EAP-FAST ■ TTLS
	v2.x	□ PEAP-MSCHAPv2 □ LEAP □ PEAP-GTC □ EAP-FAST □ TTLS
Intel 無線 LAN 搭載モデル （Intel(R) Wireless WiFi Link 4965AG） （Intel(R) PRO/Wireless 3945ABG Network Connection） （Intel(R) PRO/Wireless LAN 2915ABG Network Connection） （Intel(R) PRO/Wireless LAN 2200BG Network Connection） （Intel(R) PRO/Wireless LAN 2100 3B Mini PCI Adapter）	v11.x ／ v10.x ／ v9.x ／ v1.x	■ PEAP-MSCHAPv2 ■ LEAP ■ PEAP-GTC ■ EAP-FAST ■ TTLS
	v8.x	■ PEAP-MSCHAPv2 ■ LEAP ■ PEAP-GTC □ EAP-FAST ■ TTLS

無線 LAN クライアントのドメインログオン動作確認情報

ドメインログオンに対応しているのは、次の標準搭載モデルのデバイス、およびワイヤレス LAN カードです。

・Atheros 無線 LAN 搭載モデル
・Intel 無線 LAN 搭載モデル
・ワイヤレス LAN カード FMV-JW481
・ワイヤレス LAN カード FMV-JW482

POINT

ドメインログオン機能をお使いになる場合

・Intel 無線 LAN 搭載モデルでドメインログオンを使用する場合は、初期設定が必要です。
初期設定については、ユーティリティバージョンによって、それぞれ次の該当する項目をご覧ください。
・ユーティリティバージョンが v 10.5.x ／ v11.x の場合
「シングルサインオン／ドメインログオンを使用する場合のプログラムの追加」（→ P.94）
・ユーティリティバージョンが v10.1.x の場合
「シングルサインオン／ドメインログオンを使用する場合のプログラムの追加」（→ P.140）
・ユーティリティバージョンが v9.x の場合
「シングルサインオン／ドメインログオンを使用する場合のプログラムの追加」（→ P.175）
・ユーティリティバージョンが v8.x ／ v7.x の場合
「シングルサインオン／ドメインログオンを使用する場合のプログラムの追加」（→ P.202）

ドメインログオン機能に対応していないデバイス

次の標準搭載モデル、および無線 LAN カードではドメインログオンを使用した Windows ログオンに対応していません。

・Broadcom 無線 LAN 搭載モデル
・Intersil 無線 LAN 搭載モデル
・FMV-JW381
・FMV-JW183
・FMV-JW182
・FMV-JW181
・FMV-W182
・FMV-W181

■動作確認情報

デバイスやドライババージョンによって、ドメインログオン機能をどの認証方式で使用できるかが異なります。以下のドメインログオンの動作確認情報の表をご確認ください。
なお、ネットワーク環境によっては、表のとおりに動作しない場合があります。

□「動作確認済みの機能」について

ドメインログオンの動作確認情報の表にある「動作確認済みの機能」欄の項目について説明します。

・ログオン前の通信
Windows（ドメイン）にログオンをする前に、パソコンに保存された情報で通信できる機能です。

・ファーストログオン
ログオンしようとするパソコンで初めて使用されるユーザー情報でのログオンが可能な機能です。証明書を使用する認証では、ログオンした後のユーザーに対する証明書が用意されていないため、使用することができません。
・ログオン後の認証
ログオン処理開始後に無線 LAN の認証処理が行われます。ログオン前に通信している場合は、一旦接続が切れますので、移動プロファイルや、グループポリシーなどが使用できません。
・ログオフ後の通信
Windows ログオフを選択した後も、通信が可能な機能です。
・シングルサインオン
ドメインにログオンするユーザー名／パスワードを無線 LAN の認証に使用します。この機能を使用する場合は、ログオン前／ログオフ後は通信できません。

□ Windows Vista 搭載のパソコン

POINT

・富士通製品情報ページに公開されている最新版のドライバをインストールする必要があります。

凡例　■：該当の機能の動作を確認しています。

□：該当の機能は動作しません。

表：ドメインログオンの動作確認情報（Windows Vista 搭載パソコン）

ユーティリティ	ドメインログオン可能な認証方式	動作確認済みの機能
WLAN Auto Config	■ EAP-TLS	■ ログオン前の通信 □ ファーストログオン［注 1］ ■ ログオン後の認証 ■ ログオフ後の通信 □ シングルサインオン
	■ PEAP-MSCHAPv2	■ ログオン前の通信 ■ ファーストログオン ■ ログオン後の認証 ■ ログオフ後の通信 ■ シングルサインオン
	■ PEAP-TLS	■ ログオン前の通信 □ ファーストログオン［注 1］ ■ ログオン後の認証 ■ ログオフ後の通信 □ シングルサインオン
	■ WPA-PSK ／ WEP	■ ログオン前の通信 ■ ファーストログオン ■ ログオフ後の通信 □ シングルサインオン
Plugfree NETWORK	■ EAP-TLS	■ ログオン前の通信 □ ファーストログオン［注 1］ ■ ログオン後の認証 ■ ログオフ後の通信 □ シングルサインオン
	■ PEAP-MSCHAPv2	■ ログオン前の通信 ■ ファーストログオン ■ ログオン後の認証 ■ ログオフ後の通信 ■ シングルサインオン
	■ PEAP-TLS	■ ログオン前の通信 □ ファーストログオン［注 1］ ■ ログオン後の認証 ■ ログオフ後の通信 □ シングルサインオン
	■ WPA-PSK ／ WEP	■ ログオン前の通信 ■ ファーストログオン ■ ログオフ後の通信 □ シングルサインオン

注 1　ファーストログオンは、ログオン自体は成功しますが、ログオン後の環境にユーザー認証用の証明書がインストールされていないため、通信できません。

□ Windows XP ／ Windows 2000 搭載のパソコン

POINT

・富士通製品情報ページに公開されている最新版のドライバをインストールする必要があります。

凡例　■：該当の機能の動作を確認しています。
□：該当の機能は動作しません。

表：ドメインログオンの動作確認情報（Windows XP ／ Windows 2000 搭載のパソコン）

無線 LAN 搭載モデル名または製品名（デバイス名）	ドライババージョン	ドメインログオン可能な認証方式	動作確認済みの機能
Atheros 無線 LAN 搭載モデル （Atheros AR5001X ＋ Wireless Network Adapter） （Atheros AR5006X ＋ Wireless Network Adapter） （Atheros AR5006EXS Wireless Network Adapter） （Atheros AR5007EG Wireless Network Adapter） （Atheros AR5008X Wireless Network Adapter） ワイヤレス LAN カード FMV-JW482 ワイヤレス LAN カード FMV-JW481	v4.x	■ EAP-TLS	■ ログオン前の通信 □ ファーストログオン ■ ログオン後の認証 ■ ログオフ後の通信 □ シングルサインオン
		■ PEAP-MSCHAPv2	■ ログオン前の通信 ■ ファーストログオン ■ ログオン後の認証 ■ ログオフ後の通信 ■ シングルサインオン
		□ PEAP-TLS	□ ログオン前の通信 □ ファーストログオン □ ログオン後の認証 □ ログオフ後の通信 □ シングルサインオン
		■ WPA-PSK ／ WEP	■ ログオン前の通信 ■ ファーストログオン ■ ログオフ後の通信 □ シングルサインオン
		■ LEAP ［注］Gina のインストールが必要	□ ログオン前の通信 ■ ファーストログオン □ ログオン後の認証 □ ログオフ後の通信 ■ シングルサインオン
		□ PEAP-GTC	□ ログオン前の通信 □ ファーストログオン □ ログオン後の認証 □ ログオフ後の通信 □ シングルサインオン
		■ EAP-FAST ［注］Gina のインストールが必要	□ ログオン前の通信 ■ ファーストログオン □ ログオン後の認証 □ ログオフ後の通信 ■ シングルサインオン
		□ TTLS	□ ログオン前の通信 □ ファーストログオン □ ログオン後の認証 □ ログオフ後の通信 □ シングルサインオン

表：ドメインログオンの動作確認情報（Windows XP ／ Windows 2000 搭載のパソコン）

無線 LAN 搭載モデル名または製品名（デバイス名）	ドライババージョン	ドメインログオン可能な認証方式	動作確認済みの機能
Atheros 無線 LAN 搭載モデル （Atheros AR5001X ＋ Wireless Network Adapter） （Atheros AR5006X ＋ Wireless Network Adapter） （Atheros AR5006EXS Wireless Network Adapter） （Atheros AR5007EG Wireless Network Adapter） （Atheros AR5008X Wireless Network Adapter） ワイヤレス LAN カード FMV-JW482 ワイヤレス LAN カード FMV-JW481	v3.x	□ EAP-TLS	□ ログオン前の通信 □ ファーストログオン □ ログオン後の認証 □ ログオフ後の通信 □ シングルサインオン
		□ PEAP-MSCHAPv2	□ ログオン前の通信 □ ファーストログオン □ ログオン後の認証 □ ログオフ後の通信 □ シングルサインオン
		□ PEAP-TLS	□ ログオン前の通信 □ ファーストログオン □ ログオン後の認証 □ ログオフ後の通信 □ シングルサインオン
		■ WPA-PSK ／ WEP	■ ログオン前の通信 ■ ファーストログオン ■ ログオフ後の通信 □ シングルサインオン
		■ LEAP	■ ログオン前の通信 ■ ファーストログオン ■ ログオン後の認証 ■ ログオフ後の通信 □ シングルサインオン
		□ PEAP-GTC	□ ログオン前の通信 □ ファーストログオン □ ログオン後の認証 □ ログオフ後の通信 □ シングルサインオン
		□ EAP-FAST	□ ログオン前の通信 □ ファーストログオン □ ログオン後の認証 □ ログオフ後の通信 □ シングルサインオン
		□ TTLS	□ ログオン前の通信 □ ファーストログオン □ ログオン後の認証 □ ログオフ後の通信 □ シングルサインオン

表：ドメインログオンの動作確認情報（Windows XP ／ Windows 2000 搭載のパソコン）

無線 LAN 搭載モデル名または製品名（デバイス名）	ドライババージョン	ドメインログオン可能な認証方式	動作確認済みの機能
Atheros 無線 LAN 搭載モデル （Atheros AR5001X ＋ Wireless Network Adapter） （Atheros AR5006X ＋ Wireless Network Adapter） （Atheros AR5006EXS Wireless Network Adapter） （Atheros AR5007EG Wireless Network Adapter） （Atheros AR5008X Wireless Network Adapter） ワイヤレス LAN カード FMV-JW482 ワイヤレス LAN カード FMV-JW481	v2.x	☐ EAP-TLS	☐ ログオン前の通信 ☐ ファーストログオン ☐ ログオン後の認証 ☐ ログオフ後の通信 ☐ シングルサインオン
		☐ PEAP-MSCHAPv2	☐ ログオン前の通信 ☐ ファーストログオン ☐ ログオン後の認証 ☐ ログオフ後の通信 ☐ シングルサインオン
		☐ PEAP-TLS	☐ ログオン前の通信 ☐ ファーストログオン ☐ ログオン後の認証 ☐ ログオフ後の通信 ☐ シングルサインオン
		☐ WPA-PSK ／ WEP	☐ ログオン前の通信 ☐ ファーストログオン ☐ ログオン後の認証 ☐ ログオフ後の通信 ☐ シングルサインオン
		☐ LEAP	☐ ログオン前の通信 ☐ ファーストログオン ☐ ログオン後の認証 ☐ ログオフ後の通信 ☐ シングルサインオン
		☐ PEAP-GTC	☐ ログオン前の通信 ☐ ファーストログオン ☐ ログオン後の認証 ☐ ログオフ後の通信 ☐ シングルサインオン
		☐ EAP-FAST	☐ ログオン前の通信 ☐ ファーストログオン ☐ ログオン後の認証 ☐ ログオフ後の通信 ☐ シングルサインオン
		☐ TTLS	☐ ログオン前の通信 ☐ ファーストログオン ☐ ログオン後の認証 ☐ ログオフ後の通信 ☐ シングルサインオン

表：ドメインログオンの動作確認情報（Windows XP ／ Windows 2000 搭載のパソコン）

無線 LAN 搭載モデル名または製品名（デバイス名）	ドライババージョン	ドメインログオン可能な認証方式	動作確認済みの機能
Intel 無線 LAN 搭載モデル （Intel(R) Wireless WiFi Link 4965AG） （Intel(R) PRO/Wireless 3945ABG Network Connection） （Intel(R) PRO/Wireless LAN 2915ABG Network Connection） （Intel(R) PRO/Wireless LAN 2200BG Network Connection） （Intel(R) PRO/Wireless LAN 2100 3B Mini PCI Adapter）	v11.x ／ v10.x	■ EAP-TLS	■ ログオン前の通信 □ ファーストログオン ■ ログオン後の認証 ■ ログオフ後の通信 □ シングルサインオン
		■ PEAP-MSCHAPv2	■ ログオン前の通信 ■ ファーストログオン ■ ログオン後の認証 ■ ログオフ後の通信 ■ シングルサインオン
		□ PEAP-TLS	□ ログオン前の通信 □ ファーストログオン □ ログオン後の認証 □ ログオフ後の通信 □ シングルサインオン
		■ WPA-PSK ／ WEP	■ ログオン前の通信 ■ ファーストログオン ■ ログオフ後の通信 □ シングルサインオン
		■ LEAP	■ ログオン前の通信 ■ ファーストログオン ■ ログオン後の認証 ■ ログオフ後の通信 ■ シングルサインオン
		■ PEAP-GTC	■ ログオン前の通信 ■ ファーストログオン ■ ログオン後の認証 ■ ログオフ後の通信 □ シングルサインオン
		■ EAP-FAST	■ ログオン前の通信 ■ ファーストログオン ■ ログオン後の認証 ■ ログオフ後の通信 ■ シングルサインオン
		■ TTLS	■ ログオン前の通信 ■ ファーストログオン ■ ログオン後の認証 ■ ログオフ後の通信 ■ シングルサインオン

表：ドメインログオンの動作確認情報（Windows XP ／ Windows 2000 搭載のパソコン）

無線 LAN 搭載モデル名または製品名（デバイス名）	ドライババージョン	ドメインログオン可能な認証方式	動作確認済みの機能
Intel 無線 LAN 搭載モデル （Intel(R) Wireless WiFi Link 4965AG） （Intel(R) PRO/Wireless 3945ABG Network Connection） （Intel(R) PRO/Wireless LAN 2915ABG Network Connection） （Intel(R) PRO/Wireless LAN 2200BG Network Connection） （Intel(R) PRO/Wireless LAN 2100 3B Mini PCI Adapter）	v9.x	□ EAP-TLS	□ ログオン前の通信 □ ファーストログオン □ ログオン後の認証 □ ログオフ後の通信 □ シングルサインオン
		■ PEAP-MSCHAPv2	■ ログオン前の通信 ■ ファーストログオン ■ ログオン後の認証 ■ ログオフ後の通信 ■ シングルサインオン
		□ PEAP-TLS	□ ログオン前の通信 □ ファーストログオン □ ログオン後の認証 □ ログオフ後の通信 □ シングルサインオン
		■ WPA-PSK ／ WEP	■ ログオン前の通信 ■ ファーストログオン ■ ログオフ後の通信 □ シングルサインオン
		■ LEAP	■ ログオン前の通信 ■ ファーストログオン ■ ログオン後の認証 ■ ログオフ後の通信 ■ シングルサインオン
		■ PEAP-GTC	■ ログオン前の通信 ■ ファーストログオン ■ ログオン後の認証 ■ ログオフ後の通信 □ シングルサインオン
		■ EAP-FAST	■ ログオン前の通信 ■ ファーストログオン ■ ログオン後の認証 ■ ログオフ後の通信 ■ シングルサインオン
		■ TTLS	■ ログオン前の通信 ■ ファーストログオン ■ ログオン後の認証 ■ ログオフ後の通信 ■ シングルサインオン

表：ドメインログオンの動作確認情報（Windows XP ／ Windows 2000 搭載のパソコン）

無線 LAN 搭載モデル名または製品名（デバイス名）	ドライババージョン	ドメインログオン可能な認証方式	動作確認済みの機能
Intel 無線 LAN 搭載モデル （Intel(R) Wireless WiFi Link 4965AG） （Intel(R) PRO/Wireless 3945ABG Network Connection） （Intel(R) PRO/Wireless LAN 2915ABG Network Connection） （Intel(R) PRO/Wireless LAN 2200BG Network Connection） （Intel(R) PRO/Wireless LAN 2100 3B Mini PCI Adapter）	v8.x	□ EAP-TLS	□ ログオン前の通信 □ ファーストログオン □ ログオン後の認証 □ ログオフ後の通信 □ シングルサインオン
		□ PEAP-MSCHAPv2	□ ログオン前の通信 □ ファーストログオン □ ログオン後の認証 □ ログオフ後の通信 □ シングルサインオン
		□ PEAP-TLS	□ ログオン前の通信 □ ファーストログオン □ ログオン後の認証 □ ログオフ後の通信 □ シングルサインオン
		■ WPA-PSK ／ WEP	■ ログオン前の通信 □ ファーストログオン □ ログオフ後の通信 □ シングルサインオン
		■ LEAP	■ ログオン前の通信 □ ファーストログオン □ ログオン後の認証 □ ログオフ後の通信 □ シングルサインオン
		□ PEAP-GTC	□ ログオン前の通信 □ ファーストログオン □ ログオン後の認証 □ ログオフ後の通信 □ シングルサインオン
		□ EAP-FAST	□ ログオン前の通信 □ ファーストログオン □ ログオン後の認証 □ ログオフ後の通信 □ シングルサインオン
		□ TTLS	□ ログオン前の通信 □ ファーストログオン □ ログオン後の認証 □ ログオフ後の通信 □ シングルサインオン

表：ドメインログオンの動作確認情報（Windows XP ／ Windows 2000 搭載のパソコン）

無線 LAN 搭載モデル名または製品名（デバイス名）	ドライババージョン	ドメインログオン可能な認証方式	動作確認済みの機能
Intel 無線 LAN 搭載モデル （Intel(R) Wireless WiFi Link 4965AG） （Intel(R) PRO/Wireless 3945ABG Network Connection） （Intel(R) PRO/Wireless LAN 2915ABG Network Connection） （Intel(R) PRO/Wireless LAN 2200BG Network Connection） （Intel(R) PRO/Wireless LAN 2100 3B Mini PCI Adapter）	v1.x	□ EAP-TLS	□ ログオン前の通信 □ ファーストログオン □ ログオン後の認証 □ ログオフ後の通信 □ シングルサインオン
		■ PEAP-MSCHAPv2	■ ログオン前の通信 □ ファーストログオン □ ログオン後の認証 □ ログオフ後の通信 □ シングルサインオン
		□ PEAP-TLS	□ ログオン前の通信 □ ファーストログオン □ ログオン後の認証 □ ログオフ後の通信 □ シングルサインオン
		■ WPA-PSK ／ WEP	■ ログオン前の通信 ■ ファーストログオン ■ ログオフ後の通信 □ シングルサインオン
		■ LEAP	■ ログオン前の通信 □ ファーストログオン □ ログオン後の認証 □ ログオフ後の通信 □ シングルサインオン
		■ PEAP-GTC	■ ログオン前の通信 □ ファーストログオン □ ログオン後の認証 □ ログオフ後の通信 □ シングルサインオン
		■ EAP-FAST	■ ログオン前の通信 □ ファーストログオン □ ログオン後の認証 □ ログオフ後の通信 □ シングルサインオン
		■ TTLS	■ ログオン前の通信 □ ファーストログオン □ ログオン後の認証 □ ログオフ後の通信 □ シングルサインオン

4 用語解説

セキュリティの設定をするうえで参考となるネットワーク関連の用語について説明します。

AES（Advanced Encryption Standard）

現在用いられている DES、3DES に代わる次世代の標準暗号化方式で、強固な暗号化方式として無線 LAN への幅広い普及が見込まれています。暗号化アルゴリズムには、ベルギーの暗号開発者が開発した「Rijndael（ラインダール）」が採用され、データを固定のブロック長で区切ってそれぞれ暗号化を行います。データ長は 128、192、256 ビット、鍵の長さは 128、192、256 ビットがサポートされていて暗号強度は非常に高く設計されています。

DHCP（Dynamic Host Configuration Protocol）

IP アドレスなどの通信に関するパラメータを自動取得するために使用するプロトコルです。

IP アドレスを与える側を DHCP サーバー、IP アドレスを与えられる側を DHCP クライアントと呼びます。

DNS（Domain Name System）

パソコンに割り当てた IP アドレスと名前の対応を管理する機能です。

IP アドレスがわからないパソコンでも名前がわかっていれば、そのパソコンと通信できます。

EAP（Extensible Authentication Protocol）

リモートアクセスによるユーザー認証の際に使用されるプロトコルです。

電子証明書を使用する EAP-TLS などがあります。

EAP-TLS（Extensible Authentication Protocol-Transport Layer Security）

暗号化通信を行うためのプロトコルです。EAP-TLS では、電子証明書を使って認証を行います。

IEEE 802.11a

IEEE（米国電気電子学会）で LAN 技術の標準を策定している 802 委員会が定めた、無線 LAN の規格の 1 つです。5GHz 帯を使った高速無線 LAN の規格で、最大 54Mbps の通信が行えます。変調方式として、エラー訂正に優れた OFDM 方式を採用しています。

IEEE 802.11b

IEEE（米国電気電子学会）で LAN 技術の標準を策定している 802 委員会が定めた、無線 LAN の規格の 1 つです。無線免許なしで自由に使える 2.4GHz 帯の電波（ISM バンド）を使い、最大 11Mbps の速度で通信を行うことができます。

IEEE 802.11g

IEEE（米国電気電子学会）で LAN 技術の標準を策定している 802 委員会が定めた、無線 LAN の規格の 1 つです。現在最も普及している IEEE 802.11b と互換性を持ち、同じ 2.4GHz 帯を使いながら、最大で 54Mbps の通信が行えます。

IEEE 802.1X

ネットワークでのクライアント認証方式を定めた IEEE 標準プロトコルです。クライアントは、RADIUS サーバーとの認証が成功しない限り、ネットワークにアクセスすることはできません。クライアントと RADIUS サーバーで認証が成功するとセッションごとにネットワークキーが自動的に生成され、クライアントに配信されます。このため、無線 LAN クライアントで個々にネットワークキーを設定する必要がありません。また、通信中にもネットワークキーを自動的に変更するためセキュリティが高まります。認証の種類には電子証明書を使った EAP-TLS、電子証明書とユーザー名／パスワードを使用した PEAP などがあります。

IP アドレス（Internet Protocol Address）

TCP/IP 環境で、パソコンが通信するために使用するアドレスです。
現在使用されている IPv4（バージョン 4）では、0 から 255 までの、4 個の数値で表します（例：192.168.100.123）。
また、IP アドレスには、グローバルアドレスとプライベートアドレスがあります。
グローバルアドレスは、世界でただひとつのアドレスです。国内では、JPNIC（日本ネットワークインフォーメーションセンター）により管理されています。プライベートアドレスは、閉じたネットワークの中でひとつのアドレスです。

LAN（Local Area Network）

同一フロアやビルなどの比較的狭い範囲で、コンピューター同士を接続した環境をいいます。

MAC アドレス（Media Access Control Address）

ネットワークカードに固有の物理アドレスです。
Ethernet ならバイト長で、先頭の 3 バイトはベンダコードとして IEEE が管理／割り当てを行っています。残り 3 バイトは各ベンダで独自に（重複しないように）管理しているコードですので、結果として、世界中で同じ物理アドレスを持つ Ethernet カードは存在せず、すべて異なるアドレスが割り当てられていることになります。Ethernet ではこのアドレスを元にフレームの送受信を行っています。

PEAP-MSCHAPv2（Protected Extensible Authentication Protocol-MSCHAPv2）

IEEE 802.1X の認証プロトコルの 1 つです。電子証明書および ID ／パスワードを使って認証を行います。また、認証パケット自体をカプセル化するため、セキュリティレベルが高くなります。

PEAP-TLS（Protected Extensible Authentication Protocol-TLS）

IEEE 802.1X の認証プロトコルの 1 つです。電子証明書を使って認証を行います。また、認証パケット自体をカプセル化するため、セキュリティレベルが高くなります。

PING（Packet Internet Groper）

インターネットやイントラネットなどの TCP/IP ネットワークで、相手先のコンピューターと通信できているかや通信回線の状況を確認するコマンドです。

PSK（Pre-shared Key）

あらかじめ設定した文字列が無線 LAN アクセスポイントとクライアントで一致した場合、相互認証を行う簡易認証の方式です。

TCP/IP（Transmission Control Protocol/Internet Protocol）

インターネットの標準プロトコルであり、現在最も普及しているプロトコルです。

TKIP（Temporal Key Integrity Protocol）

WPA で使用される、ネットワークキーの 1 つです。暗号化アルゴリズムは、WEP と同じ RC4 ですが、1 パケットごとに暗号化に使用するネットワークキーを変更することで、セキュリティレベルが高くなっています。

WEP（Wired Equivalent Privacy）

無線 LAN で使用されるネットワークキーの 1 つです。データの暗号化／復号化ともに同一のネットワークキーを用いるため、通信する相手と同一の値を設定する必要があります。

Wi-Fi （Wireless Fidelity）CERTIFIED

無線 LAN の互換性接続を保証する団体「Wi-Fi Alliance®」の相互接続性テストに合格していることを示します。

WPA（Wi-Fi Protected Access）

Wi-Fi Alliance® が新たに策定したセキュリティ規格です。従来のネットワーク名（SSID）やネットワークキー（WEP）に加えて、ユーザー認証機能や暗号化プロトコルを採用して、セキュリティを強化しています。

WPA2（Wi-Fi Protected Access 2）

Wi-Fi Alliance® が新たに策定した WPA の新バージョンです。WPA と比べより強力な AES 暗号に対応しています。

オープンシステム認証

無線 LAN のネットワーク認証の 1 つです。認証の際にネットワークキーの確認を行わないため、クライアントは正しいネットワークキーを提示しなくても無線 LAN アクセスポイントと接続することができます。しかし、実際に通信を行う場合には同じネットワークキーが設定されている必要があります。オープンキー認証と呼ばれる場合もあります。

共有キー（シェアードキー）認証

無線 LAN のネットワーク認証の 1 つです。無線 LAN アクセスポイントは、クライアントに対し、同じネットワークキーが設定されているかどうかを認証する際に確認します。クライアントが誤ったネットワークキーを使用している場合や、ネットワークキー自体が設定されていない場合は認証に失敗し、無線 LAN アクセスポイントと通信できなくなります。

サブネットマスク

TCP/IP ネットワークは、複数の小さなネットワーク（サブネット）に分割されて管理されます。IP アドレスは、そのサブネットのアドレスと、個々のコンピューターのアドレスから構成されています。IP アドレスの何ビットがサブネットのアドレスかを定義するのが、サブネットマスクです。

シングルサインオン

無線 LAN の認証がユーザー名、パスワードを使用する方式の場合に、Windows にログオンするユーザー名とパスワードを、認証のユーザー ID、パスワードとして自動的に使用する機能です。この機能を使用すると、認証のためのユーザー ID とパスワードを、無線 LAN への接続時に別途入力する必要がありません。

チャンネル

無線 LAN カードや無線 LAN アクセスポイントで通信するために使用する、無線の周波数帯を表します。

ドメインログオン

無線 LAN でのドメインログオンを行う場合、有線 LAN と異なり、無線 LAN を接続するためのサービスが Windows へのログオン後にスタートする場合など、無線 LAN 経由でのドメインへログオンができない場合があります。いくつかの無線 LAN とドライバの組み合わせではこれらの問題を解決しています。

認証機関

インターネット上の電子資産を証明するために使用される電子証明書を発行する機関です。
電子証明書の所有者の身元を確認し、証明します。

認証サーバー

ユーザーのネットワークアクセスを許可するか否かを確認するサーバーのことです。
ソフトウェアでユーザーの名前やパスワードなどを一括管理します。暗号を利用した認証用のプロトコルを使い、ユーザーが「アクセスを許可された当人である」ことを認証します。RADIUS サーバーなどがこれに該当します。

ネットワークキー

無線 LAN でデータ通信を行う際にデータを暗号化するために使用する鍵情報です。
WEP や TKIP などがあります。

ネットワーク認証

無線 LAN クライアントが、無線 LAN アクセスポイントと接続する場合に行う認証方式を指します。オープンシステム認証と、共有キー（シェアードキー）認証があります。認証方法は、それぞれのクライアントに設定されていなければならず、通信したい無線 LAN アクセスポイントの設定とも一致している必要があります。認証モードと呼ばれる場合もあります。

ネットワーク名（SSID：Service Set Identifier）

無線 LAN を構成するとき、混信やデータの盗難などを防ぐために、グループ分けをします。このグループ分けをネットワーク名（SSID）で行います。さらにセキュリティ強化のためにネットワークキーを設定し、ネットワーク名（SSID）とネットワークキーが一致しないと通信できないようになっています。

パスフレーズ

WPA の認証方式の 1 つ、PSK 認証で使用するネットワークキーのことを指します。

索引

無線 LAN のセキュリティ設定マニュアル

第 4 版

発行日　2007 年 4 月
発行責任　富士通株式会社