Windows Server2003 を用いた
IEEE802.1X 認証環境の構築

株式会社バッファロー

2007 年 4 月

［準備編］

■IEEE802.1X 認証システムによるユーザ認証環境の構築

- 本マニュアルで用いるシステム構成
- ActiveDirectory の構築
- 証明機関（CA）の構築
  - ―．インターネットインフォメーションサービス（IIS）のインストール
  - ―．証明機関（CA）のインストール
- RADIUS サーバー（IAS）の構築
  - ―．IAS のインストール
  - ―．RADIUS クライアント（AirStationPro 及び BusinessSwitch）の登録
  - ―．リモートアクセスポリシーの設定
- ユーザアカウント（クライアント PC）の登録
- RADIUS クライアントの設定
  - ―．AirStation（無線アクセスポイント）の設定―WAPM/WAPS シリーズ
  - ―．BusinessSwitch（有線スイッチ）の設定―BS/BSL シリーズ

［端末設定編］

■各認証方式の設定

- EAP-PEAP 認証を行う為の設定（無線及び有線）
  - ―．ルート証明書のインストール
  - ―．EAP-PEAP 認証を行う為の IAS の設定
  - ―．認証端末でのサプリカント設定
- EAP-TLS 認証を行う為の設定（無線及び有線）
  - ―．ルート証明書及びコンピュータ証明書のインストール
  - ―．EAP-TLS 認証を行う為の IAS の設定
  - ―．認証端末でのサプリカント設定

＜注意＞

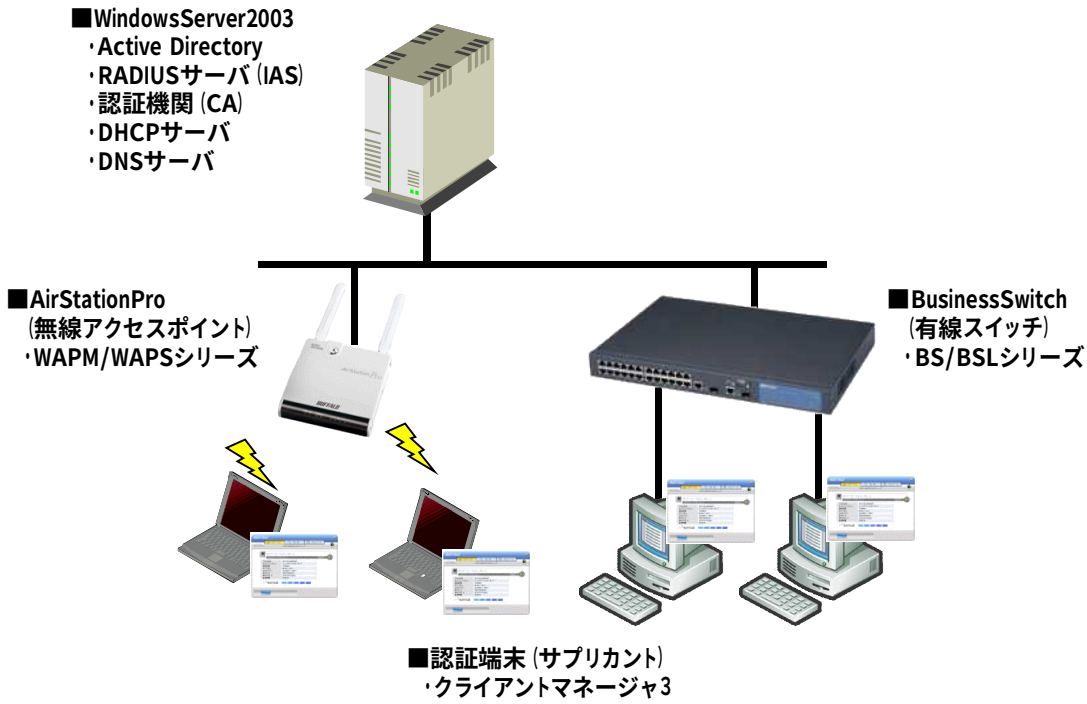
※本マニュアルに掲載されている各製品名は一般的に各社の商標または登録商標です。

※本マニュアルはバッファロー製無線アクセスポイント及び有線スイッチを IEEE802.1X 認証環境にて用いる際の設定情報提供を目的として作成されております。従って、本マニュアルに記載されている内容について、いかなるサポート及び保証をするものではありません。

※本マニュアルに記載されて内容によって生じた損害について、一切の責任を負いません。

[準備編]

●本マニュアルで用いるシステム構成



本マニュアルではWindowsServer2003がインストールされたコンピュータに各種サーバ機能をインストールする構成となります。また、その他の構成条件は以下を想定しています。

■RADIUS クライアント：

バッファロー製無線アクセスポイント（WAPM/WAPS シリーズ）、有線スイッチ（BS/BSL シリーズ）

■サプリカント：

バッファロー製クライアントマネージャ３

■IP アドレス/DNS サーバ：

DHCP サーバより自動取得

上記以外の RADIUS クライアントやサプリカントを使用される場合は各メーカ提供のマニュアルを参考に設定してください。

Active Directory の構築

まず、最初に RADIUS サーバ（IAS）として用いるコンピュータに Active Directory をセットアップします。本マニュアルでは［サーバの構成ウィザード］を用いて Active Directory を構成します。

1. ［スタート］－[管理ツール]－[サーバの役割管理]をクリックし、[サーバの役割管理]を開きます。
2. ［サーバの役割管理］で［役割を追加または削除する］をクリックします。

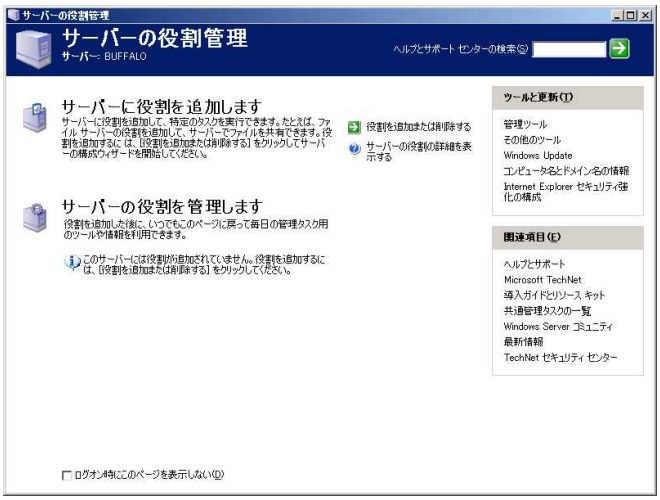


図１：サーバの役割管理画面

3. ［準備作業］で作業内容を確認し、［次へ］をクリックします。

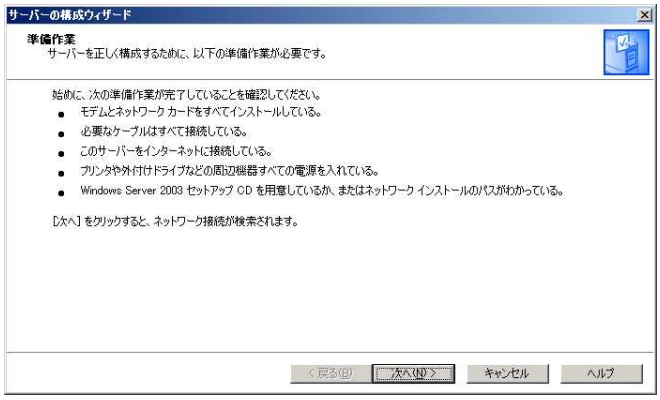


図２：役割構成の準備作業

4. ［構成オプション］で［最初のサーバの標準構成］を選択し、［次へ］をクリックします。

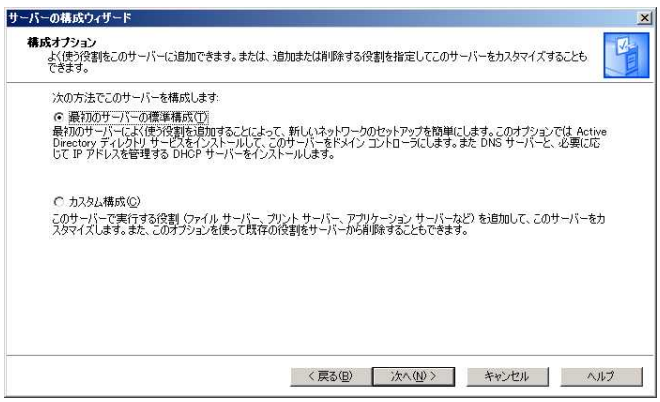


図３：構成オプション

［最初のサーバーの標準構成］を選択した場合、ActiveDirectory のほかに DNS サーバー及び DHCP サーバーなどもインストールされます。使用環境において、これらのサーバー機能が不要な場合は［カスタム構成］を選択し、必要なサーバー機能だけをインストールしてください。

5. 「ActiveDirectory ドメイン名」を入力し、［次へ］をクリックします。

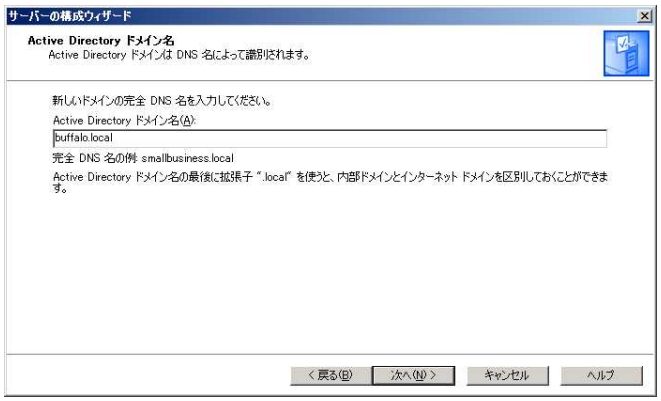


図４：ActiveDirectory ドメイン名の入力

6. **既定の NetBIOS 名を変更する際には［NetBIOS ドメイン名］を入力し、[次へ]をクリックします**

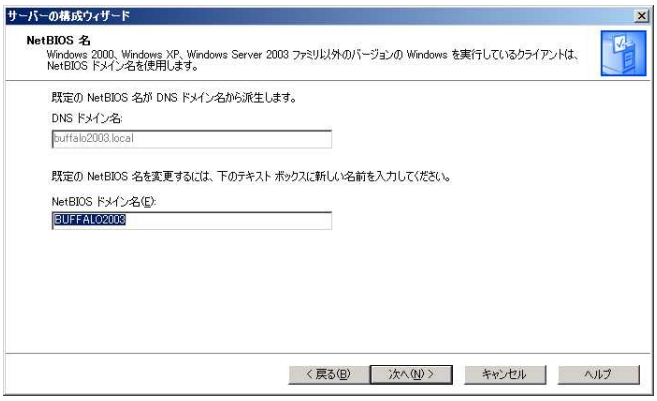


図５：NetBIOS ドメイン名の入力

7. **DNS クエリの転送を行う場合はクエリの転送先サーバ IP アドレスを入力します。ここでは[いいえ、クエリ転送しません]を選択し、[次へ]をクリックします。**

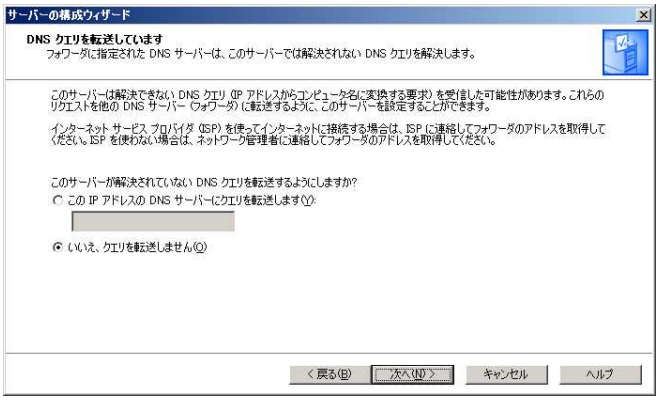


図６：DNS クエリの転送設定

8. **設定内容を確認し、[次へ]をクリックします。**

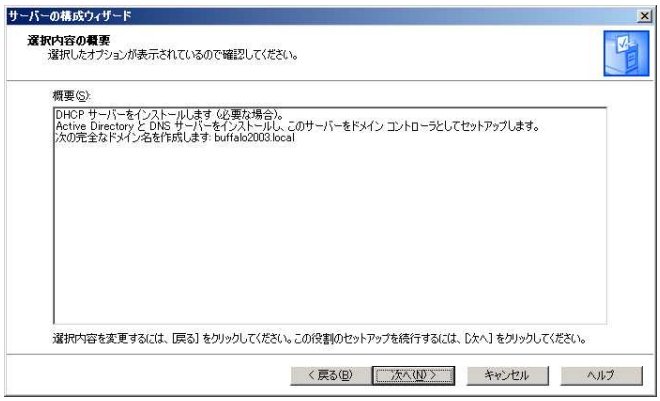


図７：選択内容の確認

9. **選択したサーバーの役割の追加が実行されます。**

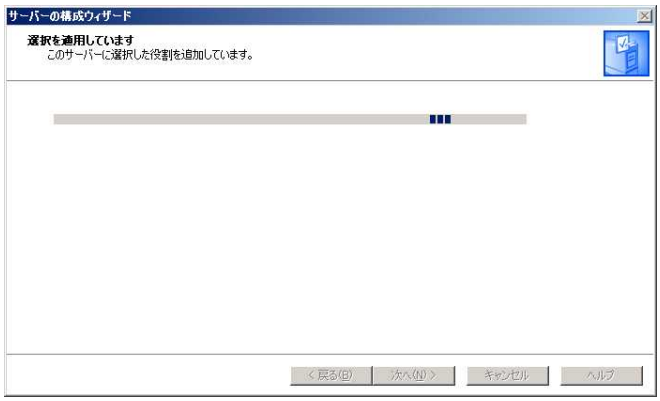


図８：役割の追加

10. **サーバーの構成が完了したことを示す画面が表示されたら[次へ]をクリックします。**

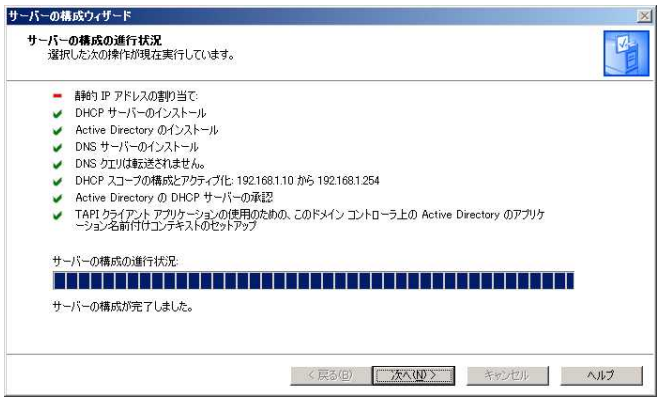


図９：サーバーの構成の完了

11. **サーバーの構成が完了したことを確認するメッセージが表示されます。[完了]をクリックし、[サーバー構成ウィザード]を終了します。**

図１０：サーバー構成完了の確認画面

以上で Active Directory **のセットアップは完了です。**
引き続き証明機関（CA**）の構築を行ってください。**

証明機関 (CA) の構築

Active Directory をセットアップしたコンピュータに証明機関（CA）をセットアップします。

■インターネットインフォメーションサービス（以下 IIS）のインストール

まず、WEB ブラウザを用いて証明書の取得が出来るように IIS をセットアップします。

1. ［スタート］－［設定］－［コントロールパネル］－［プログラムの追加と削除］を選択します。
2. ［Windows コンポーネントの追加と削除］をクリックします。

図１：プログラムの追加と削除

3. ［Windows コンポーネント］にて［アプリケーションサーバー］にチェックを入れ、［次へ］をクリックします。

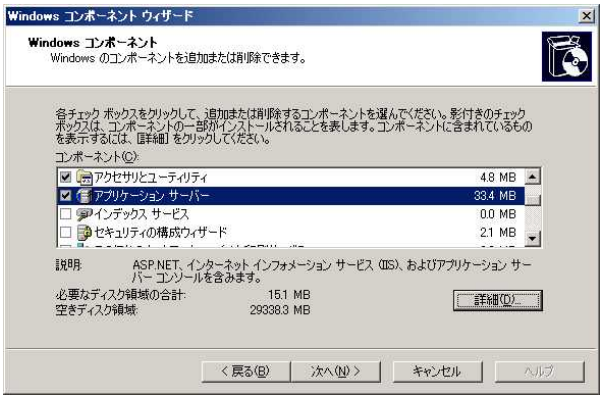


図２：Windows コンポーネントウィザード

4. IIS のインストールが開始されます。

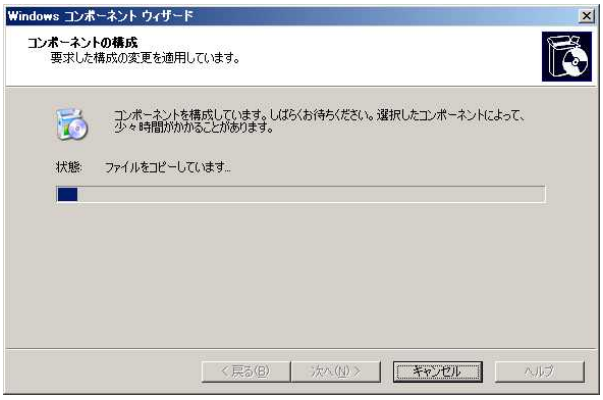


図３：コンポーネントの構成

5. **コンポーネントの構成が完了したことを確認するメッセージが表示されます。［完了］をクリックし、［Windows コンポーネントウィザード］を終了します。**

図４：Windows コンポーネントウィザードの完了

以上で IIS のセットアップは完了です。
引き続き証明機関（CA）のセットアップを行ってください。

■証明機関（CA）のインストール

次に電子証明書の発行が出来るように証明機関（CA）をセットアップします。

1. **［スタート］－［設定］－［コントロールパネル］－［プログラムの追加と削除］を選択します。**
2. **［Windows コンポーネントの追加と削除］をクリックします。**

図１：プログラムの追加と削除

3. ［Windows コンポーネント］にて［証明書サービス］にチェックを入れ、［次へ］をクリックします。

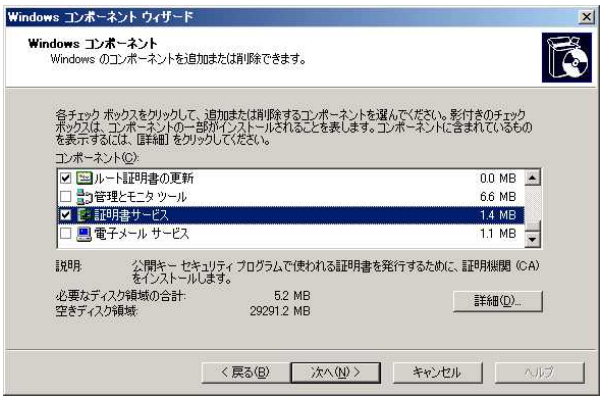


図２：Windows コンポーネントの選択

4. 次のようなメッセージが表示されるので内容を確認して［はい］をクリックします。

図３：バインドに関する確認画面

5. ［証明書サービス］にチェックが入っていることを確認し、［次へ］をクリックします。
6. ［CA の種類］にて［エンタープライズ CA］を選択します。

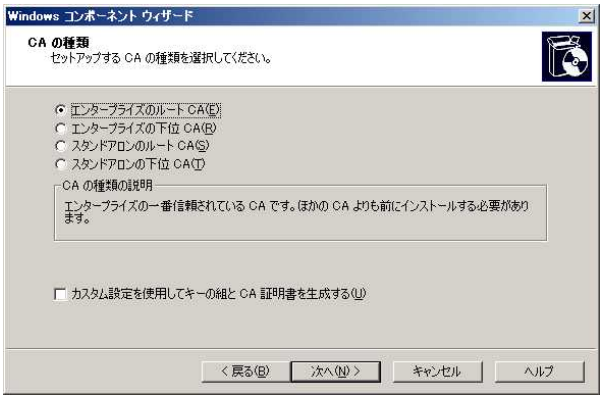


図４：CA の種類の選択

7. ［CA 識別情報］にて［この CA の共通名］に任意の値を入力し、［次へ］をクリックします。

図５：CA 識別情報の入力

8. ［証明書データベースの設定］にて証明書データベースとデータベースログの保存場所を指定し、［次へ］をクリックします。

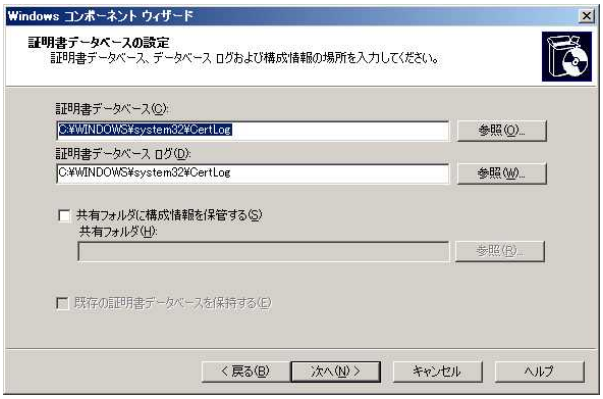


図６：証明書データベースの設定

9. IISが動作している場合、IISサービスの一時停止を必要とするメッセージが表示されるので、［はい］をクリックします。

図７：IIS サービスの一時停止

10. 証明書サービスのインストールが開始されます。

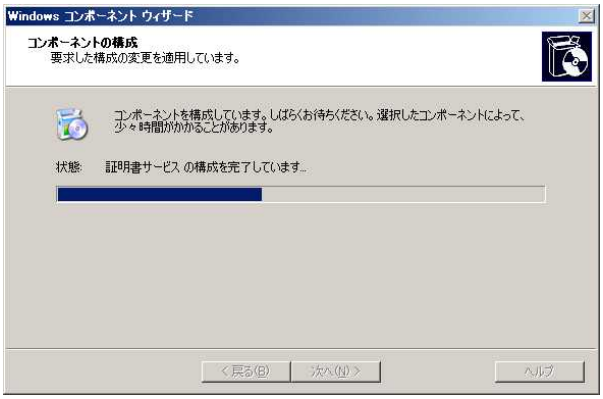


図８：証明書サービスのインストール

11. Active Server Page(ASP)を有効にする旨のメッセージが表示されるので、［はい］をクリックします。

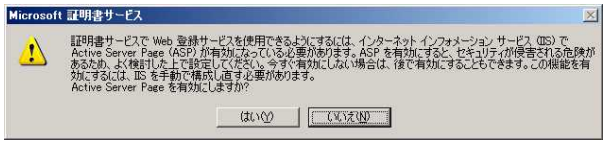


図９：ASP 有効の選択メッセージ

12. **コンポーネントの構成が完了したことを確認するメッセージが表示されます。［完了］をクリックし、［Windows コンポーネントウィザード］を終了します。**

図１０：Windows コンポーネントウィザードの完了

以上で証明機関（CA）のセットアップは完了です。
引き続き RADIUS サーバー（IAS）のセットアップを行ってください。

RADIUS サーバーの構築

Active Directory をセットアップしたコンピュータに RAIDUS サーバーをセットアップします。
本マニュアルでは Windows Server2003 の標準 RADIUS サーバー機能であるインターネット認証サービス（IAS）を用います。

■インターネット認証サービス（以下 IAS）のインストール

IEEE802.1X 認証に用いる RADIUS サーバーとして IAS をセットアップします。

1. ［スタート］－［設定］－［コントロールパネル］－［プログラムの追加と削除］を選択します。
2. ［Windows コンポーネントの追加と削除］をクリックします。

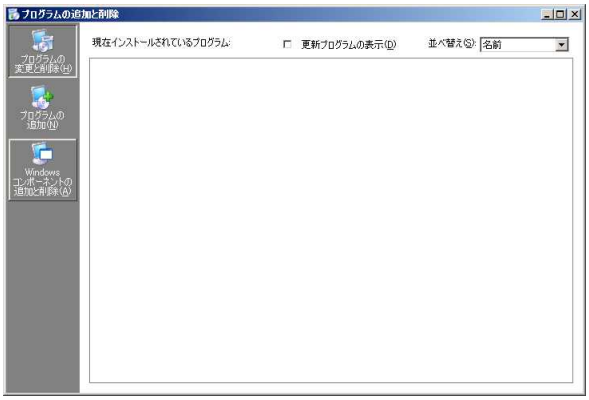


図１：プログラムの追加と削除

3. ［Windows コンポーネント］にて［ネットワークサービス］にチェックを入れ、［詳細］をクリックします。

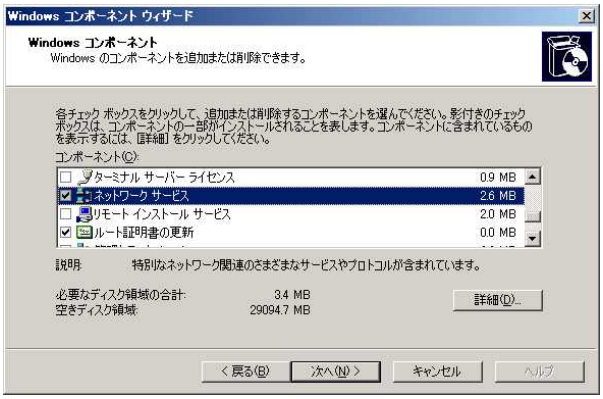


図２：Windows コンポーネントの選択

4. ［ネットワークサービスのサブコンポーネント］で［インタネット認証サービス］にチェックを入れ、［OK］をクリックします。

図３：ネットワークサービスの選択

5. ［Windows コンポーネント］にて［ネットワークサービス］にチェックが入っていることを確認し、［次へ］をクリックします。

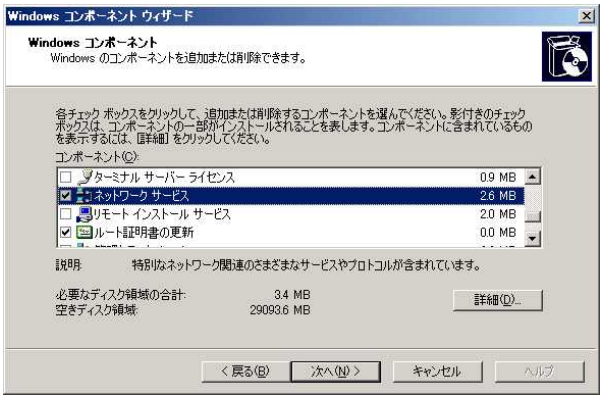


図４：Windows コンポーネントの選択

6. IAS のインストールが開始されます。

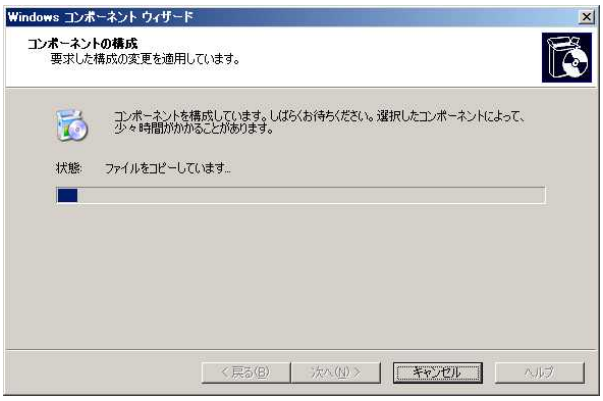


図５：IAS のインストール

7. **コンポーネントの構成が完了したことを確認するメッセージが表示されます。［完了］をクリックし、［Windows コンポーネントウィザード］を終了します。**

図６：Windows コンポーネントウィザードの完了

8. **［スタート］－［管理ツール］－［インターネット認証サービス］を選択します。**
9. **［インターネット認証サービス］画面において左枠内の［インターネット認証サービス（ローカル）］を右クリックし、［Active Directory にサーバーを登録］を選択します。**

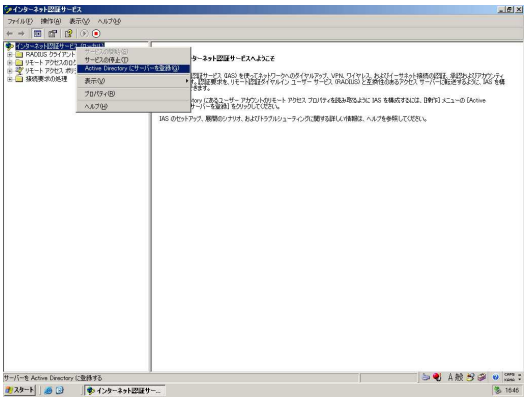


図７：インターネット認証サービス

10. **IAS にダイヤルインプロパティの読み取り権限を与える旨のメッセージが表示されるので、［OK］をクリックします。**

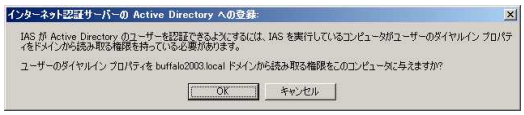


図８：読み取り権限に関するメッセージ

11. **IAS がダイヤルインプロパティの読み取り権限を取得した旨のメッセージが表示されるので、［OK］をクリックします。**

図９：読み取り権限取得のメッセージ

以上で IAS のセットアップは完了です。
引き続き RADIUS クライアントの登録を行ってください。

■RADIUS クライアント（AirStationPro 及び BusinessSwitch）の登録

IAS に AirStationPro 及び BusinessSwitch などの RADIUS クライアントを登録します。

1. ［スタート］－［管理ツール］－［インターネット認証サービス］を選択します。
2. ［インターネット認証サービス］画面において左枠内の［RADIUS クライアント］を右クリックし、［新しい RADIUS クライアント］を選択します。

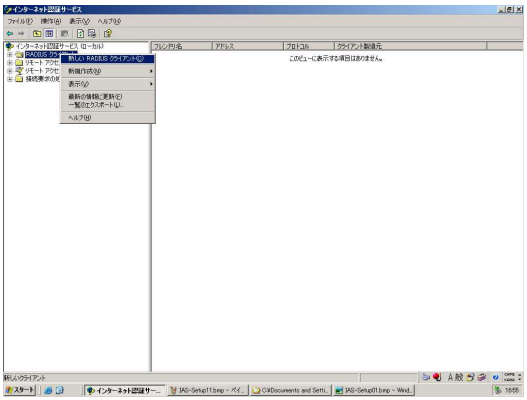


図１：RADIUS クライアントの登録選択

3. ［新しいクライアント］画面で［フレンドリ名］と［クライアントのアドレス（IP または DNS)］を入力します。

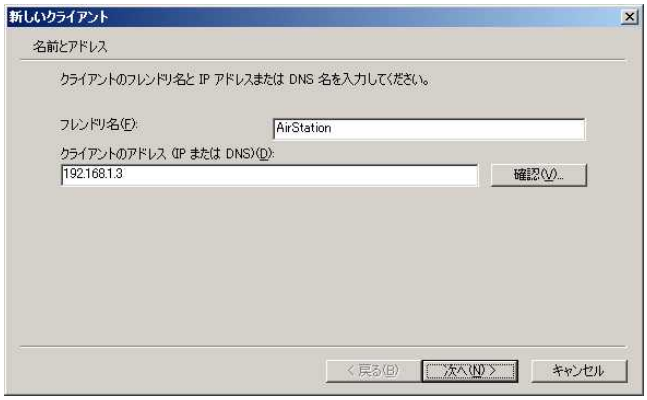


図２：RADIUS クライアント情報の入力

4. **［追加情報］画面で必要な値を入力します。ここでは［クライアントベンダ］に「**RADIUS Standard**」が選択されていることを確認し、［共有シークレット］を入力します。入力したら［完了］をクリックします。**

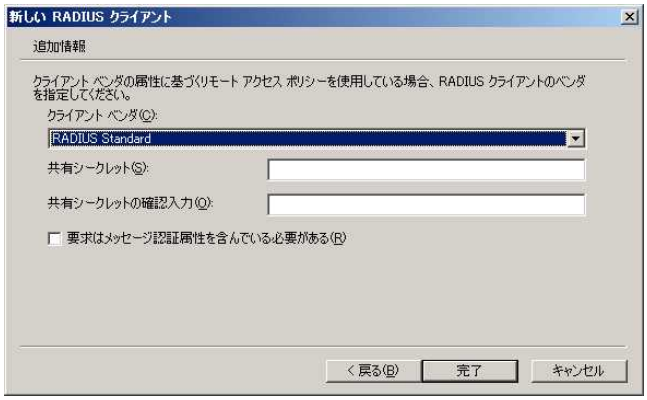


図３：追加情報の入力

以上で RADIUS **クライアントの登録は完了です。**
複数の RADIUS **クライアントの登録を行う場合は上記の設定を繰り返してください。**
引き続きリモートアクセスポリシーの設定を行ってください。

■リモートアクセスポリシーの設定

無線接続用及び有線接続用にリモートアクセスポリシーを登録します。

1. ［スタート］－［管理ツール］－［インターネット認証サービス］を選択します。
2. ［インターネット認証サービス］画面において左枠内の［リモートアクセスポリシー］を右クリックし、［新しいリモートアクセスポリシー］を選択します。

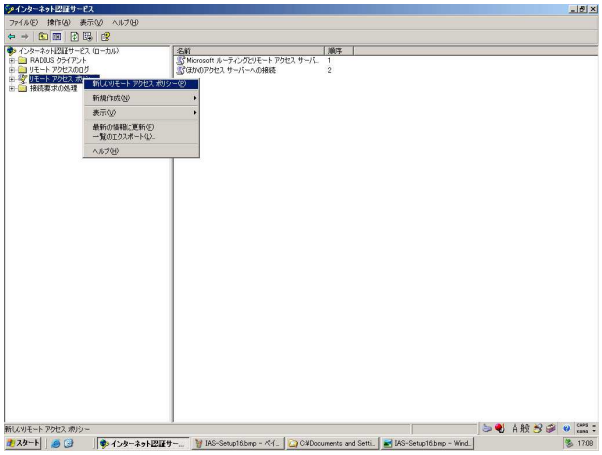


図１：リモートアクセスポリシーの追加

3. リモートアクセスポリシーウィザードが起動しますので［次へ］をクリックします。

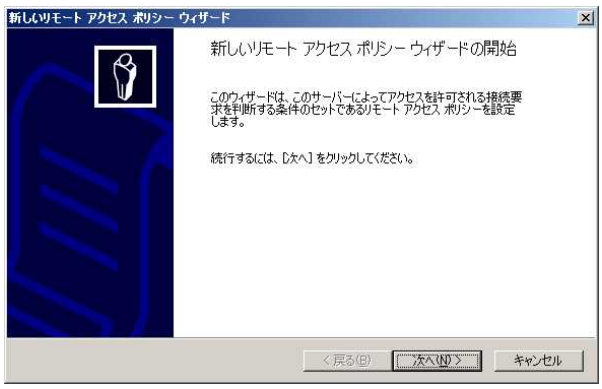


図２：リモートアクセスポリシーウィザード

4. ［ポリシーの構成方法］の選択画面が表示されるので「ウィザードを使って共有シナリオの標準ポリシーを設定する」を選択し、［ポリシー名］を入力します。入力したら、［次へ］をクリックします。

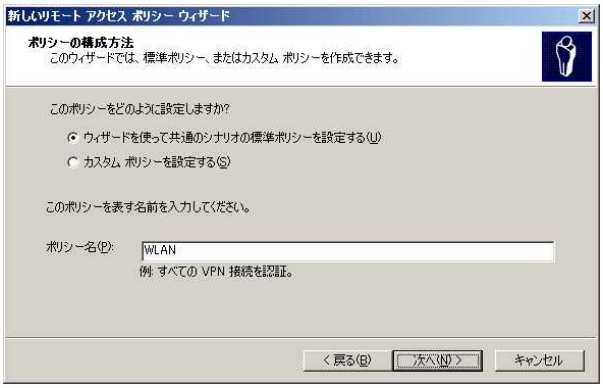


図３：ポリシーの構成方法

5. ［アクセス方法］の選択画面で接続方法に応じてポリシーを作成する為のアクセス方法を選択します。アクセス方法に「ワイヤレス」（無線の場合）もしくは「イーサネット」（有線の場合）を選択し、［次へ］をクリックします。

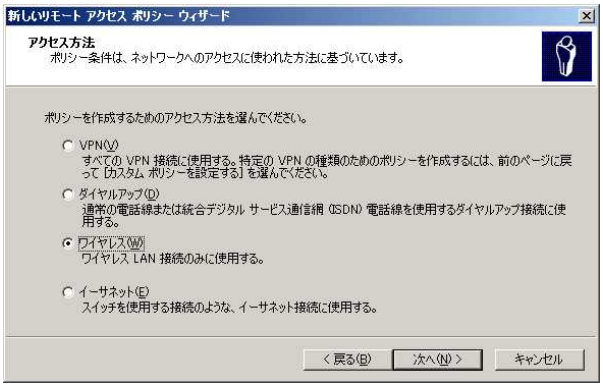


図４：アクセス方法の選択（無線の場合）

6. ［ユーザーまたはグループアクセス］設定画面でアクセス許可の基準を設定します。ここでは「ユーザ」を選択し、［次へ］をクリックします。

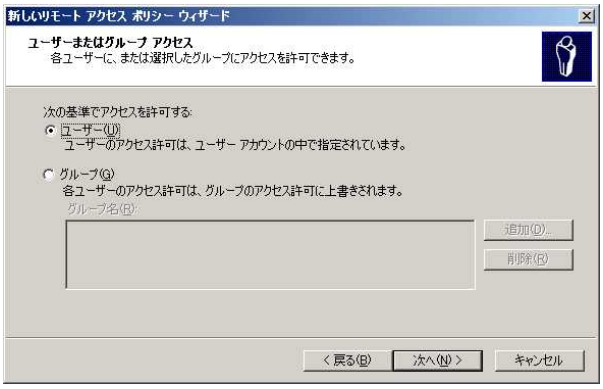


図５：アクセス許可の設定

7. ［認証方法］の設定画面で使用する認証方法を選択します。EAP-PEAP を用いる場合は「保護された EAP（PEAP）」、EAP-TLS を用いる場合は「スマートカードまたはその他の証明書」を選択し、［次へ］をクリックします。

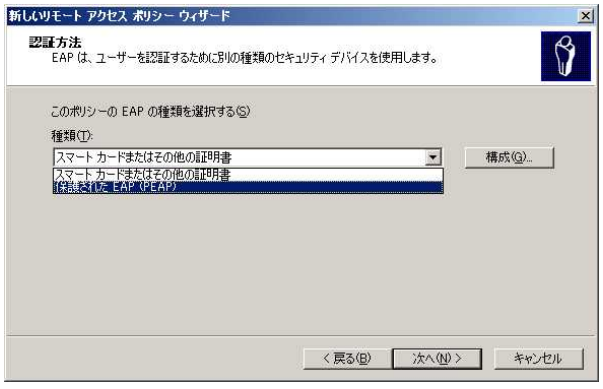


図６：認証方法の選択（EAP-PEAP の場合）

8. リモートアクセスポリシーの作成が完了したことを確認するメッセージが表示されます。［完了］をクリックし、［新しいリモートアクセスポリシーウィザード］を終了します。

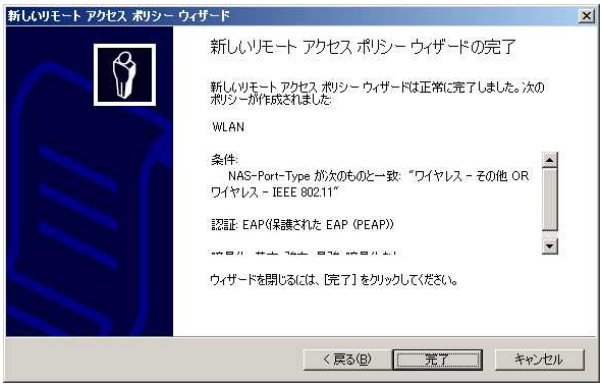


図７：リモートアクセスポリシーウィザードの完了

9. ［インターネット認証サービス］画面において、右枠内からいま作成したリモートアクセスポリシーを選択し、ダブルクリックします。

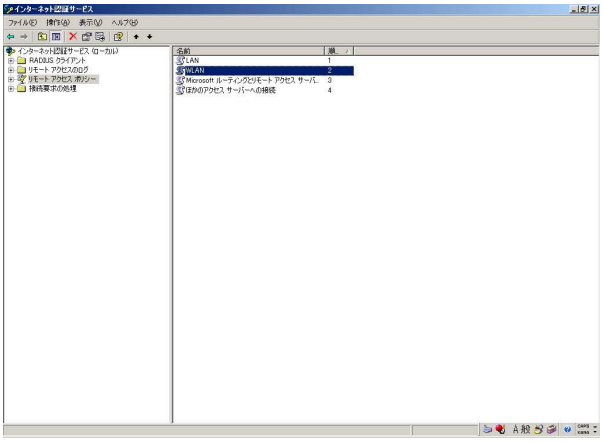


図８：リモートアクセスポリシーの選択

10. ［リモートアクセスポリシー］プロパティで、［接続要求が指定の条件を満たした場合］の欄に［リモートアクセス許可を与える］を選択し、［プロファイルの編集］をクリックします。

図９：リモートアクセスポリシーのプロパティ

11. **［ダイヤルインプロファイルの編集］画面で［認証］タブを選択します。［認証］設定画面が表示されたら許可する認証方法を選択します。**EAP-PEAP **を用いる場合は「**Microsoft **暗号化認証バージョン** 2（MS-CHAP v2)」**にチェックを入れ、**EAP-TLS **を用いる場合はどこにもチェックが入っていないことを確認し、**［OK］**をクリックします。**

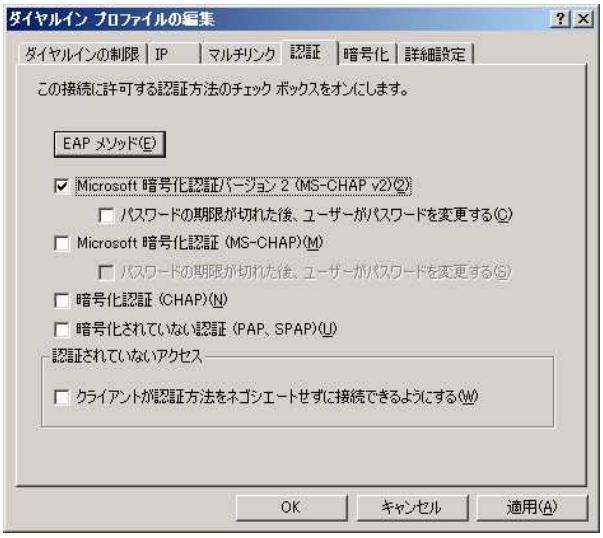


図１０：ダイヤルインプロファイルの編集（EAP-PEAP **の場合）**

12. **［リモートアクセスポリシー］プロパティで、［接続要求が指定の条件を満たした場合］の欄に「リモートアクセス許可を与える」が選択させていることを確認し、**［OK］**をクリックします。**

図１１：リモートアクセスポリシーのプロパティ

以上で RADIUS **サーバーのセットアップは完了です。**
詳細設定については環境に応じて設定をおこなってください。

ユーザアカウントの登録

IEEE802.1X 認証において認証へ用いるユーザアカウントを Active Directory に登録します。

■Active Directory へのユーザアカウントの登録

IEEE802.1X 認証にて認証されるようにユーザアカウントを設定します。

1. ［スタート］－［管理ツール］－［Active Directory ユーザーとコンピュータ］を選択します。
2. 左枠内のユーザーアカウントを登録するドメインをクリックして展開します。

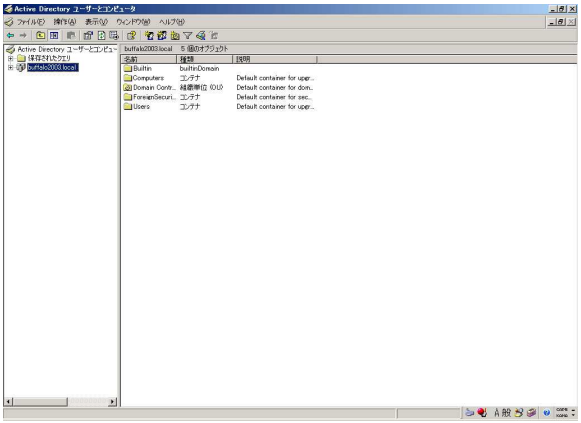


図１：Active Directory ユーザーとコンピュータ

3. ［Users］コンテナを右クリックし、［新規作成］－［ユーザー］を選択します。

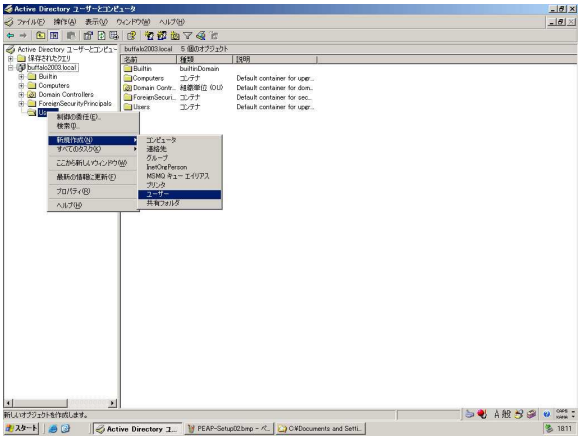


図２：ユーザーの新規作成

4. ユーザー情報に必要事項を入力します。

図３：ユーザー情報の入力

5. ［パスワード］を設定します。ここではパスワードのポリシーとして［ユーザーはパスワードを変更できない］にチェックを入れ、［次へ］をクリックします。

図４：パスワードの設定

6. 作成ユーザーの情報が表示されるので内容を確認し、［完了］をクリックします。

図５：作成ユーザー情報の確認

7. ［Active Directory ユーザーとコンピュータ］画面の右枠内から、いま作成したユーザー名を選択し、ダブルクリックします。

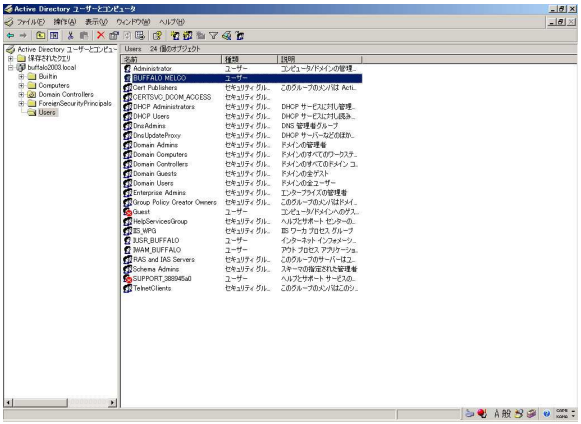


図６：Active Directory ユーザーとコンピュータ

8. **［ユーザーのプロパティ］画面から［ダイヤルイン］タブを選択し、［リモートアクセス許可（ダイヤルインまたは VPN)］で［アクセス許可］を選択します。選択したら［OK］をクリックします。**

図７：ユーザーのダイヤルイン設定

以上でユーザーアカウントの登録は完了です。
複数のユーザーを登録する場合は上記の設定を繰り返してください。
引き続き RADIUS クライアント（AirStationPro 及び BusinessSwitch）の設定を行ってください。

RADIUS クライアントの設定

IEEE802.1X 認証にあわせ、無線アクセスポイントやスイッチの設定を行います。

■AirStationPro（無線アクセスポイント）の設定－WAPM/WAPS シリーズ

ここでは無線アクセスポイントとして BUFFALO 製 WAPM/WAPS シリーズの設定方法を説明します。

1. WAPM/WAPS シリーズのマニュアルを参考に設定画面を開きます。
2. 設定画面が開いたら［詳細設定］をクリックします。

図１：WAPM/WAPS シリーズ設定画面

3. 左側の選択項目から［無線設定］をクリックします。

図２：詳細設定画面

4. ［無線設定］が開いたら、「無線セキュリティ」を設定します。ここでは IEEE802.11g のセキュリティ設定を行いますので［無線セキュリティ設定（11g）］をクリックします。

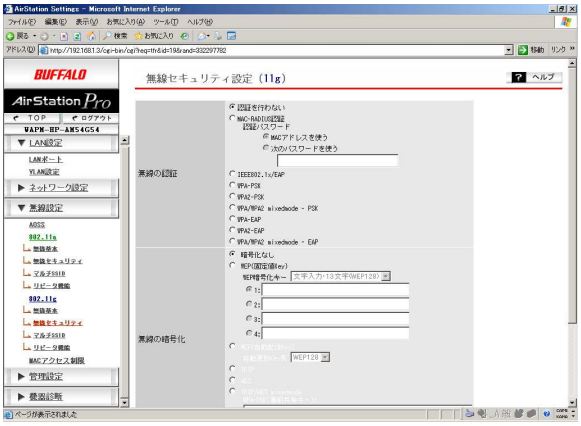


図３：無線セキュリティ設定（802.11g の場合）

5. ［無線の認証］と［無線の暗号化］を設定します。ここでは以下の値を設定しますので該当項目を選択し、［設定］をクリックします。

●無線の認証：WPA/WPA2 mixedmode-EAP

●無線の暗号化：AES

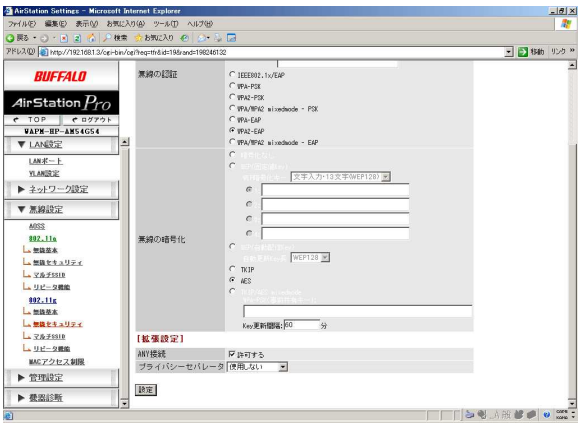


図４：無線の認証と暗号化の設定

6. 設定の内容が表示されるのでメッセージを確認し、［設定］をクリックします。その後、再スタートするのでしばらくしてから再度、設定画面を開き、［詳細設定］をクリックします。

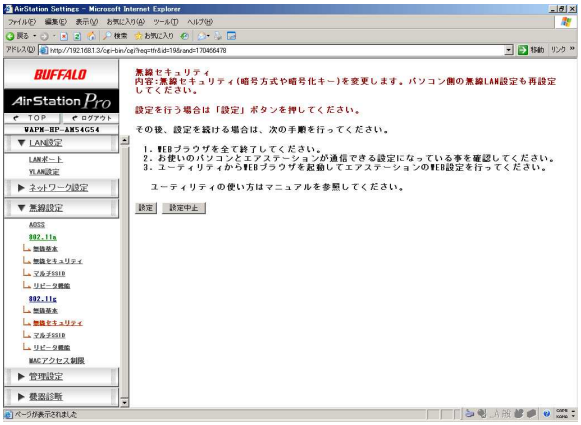


図５：設定内容の確認メッセージ

7. 再スタートしますので、しばらくしたら左側の選択項目から［ネットワーク設定］をクリックします。

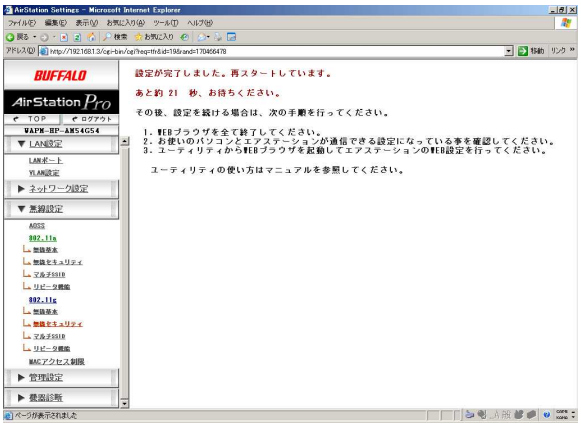


図６：再起動メッセージ

8. [RADIUS 設定]を選択し、RADIUS サーバの設定をおこないます。ここでは以下の値にて設定しますが環境に合わせて設定をしてください。値を入力したら[設定]をクリックします。

●サーバ名：192.168.1.1

●Shared Secret：IAS の項で設定した「共有シークレット」と同じ値

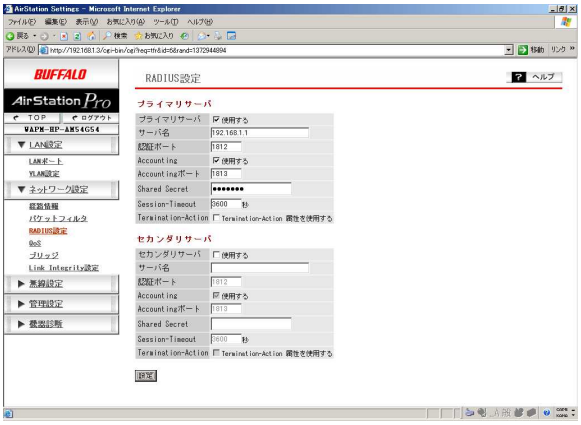


図７：RADIUS 設定

以上で AirStationPro（無線アクセスポイント）の設定は完了です。

IEEE802.11a 側の設定を行う場合は 4.で［セキュリティ設定(11a)］を選択して、同様に設定を行ってください。複数の AirStationPro の設定を行う場合も上記の設定を繰り返してください。

また、BusinessSwitch（有線スイッチ）の設定を行う場合は次項の設定方法を参考に設定を行ってください。

■BusinessSwitch（有線スイッチ）の設定－BS/BSL スイッチ

ここでは有線スイッチとして BUFFALO 製 BSL シリーズの設定方法を参考に説明します。

BS シリーズの設定画面は若干異なりますが設定手順は同様となります。

1. BS/BSL シリーズのマニュアルを参考に設定画面を開きます。
2. 設定画面が開いたら［詳細設定］をクリックします。

図１：BSL シリーズ設定画面

3. [ユーザ認証設定]から[認証サーバ設定]を選択します。

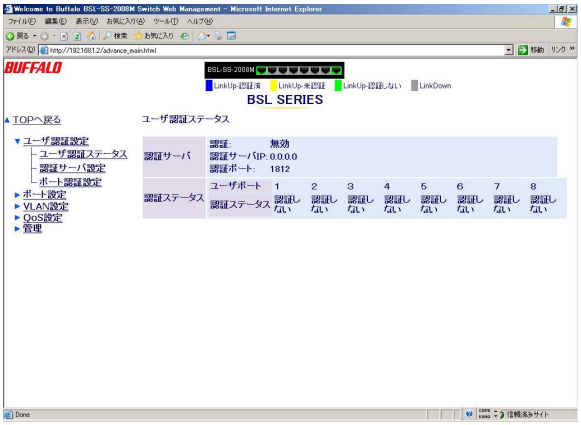


図２：詳細設定画面

4. ［認証サーバ設定］を開いたら、「認証サーバ（RADIUS サーバ）」の設定をします。ここでは以下の値にて設定しますが環境に合わせて設定をしてください。値を入力したら[設定]をクリックします。

●認証サーバ IP：192.168.1.1

●Shared Secret：IAS の項で設定した「共有シークレット」と同じ値

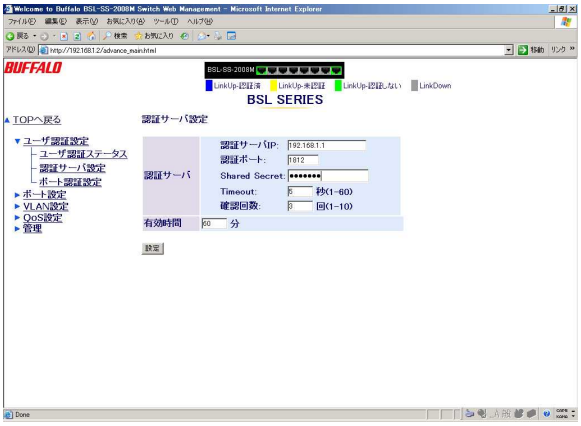


図３：認証サーバ設定

5. **次に［ポート認証設定］を選択し、 認証するポートを設定します。ここでは以下の値で設定します。認証サーバ（RADIUS サーバ）へ接続するポートは必ず「認証しない」に設定してください。設定したら、[設定]をクリックします。**

●ポート１～７：認証する

●ポート８：認証しない（デフォルト）

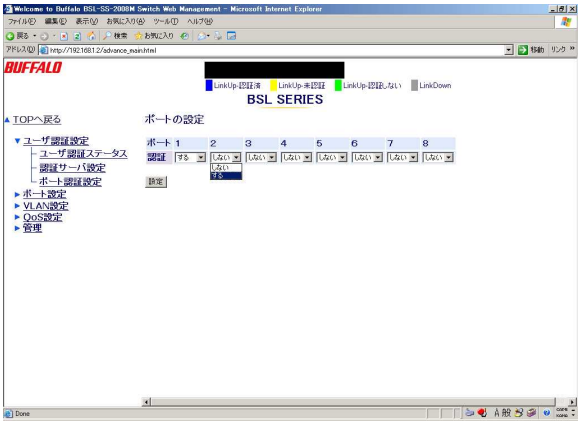


図４：認証ポートの設定

以上で BusinessSwitch**（有線スイッチ）の設定は完了です。**

複数の BusinessSwitch **の設定を行う場合は上記の設定を繰り返してください。**

[端末設定編]

各認証方式におけるクライアントコンピュータの設定

■EAP-PEAP 認証を行う為の設定（無線及び有線）

以下では EAP-PEAP 認証を行うために次の手順で設定を行います。

－．認証されるクライアントコンピュータ（以下、認証端末）へのルート証明書のインストール

－．EAP-PEAP 認証を行う為の IAS の設定

－．認証端末でのサプリカント設定

●ルート証明書のインストール

EAP-PEAP 認証で用いるルート証明書の発行及びインストールを行います。

1. Active Directory をセットアップしたコンピュータで WWW ブラウザを立ち上げ、URL 入力欄に「http：//（証明機関の IP アドレス）/certsrv」を入力します。認証画面が開いたら、CA に対する管理者権限を有する「ユーザー名」と「パスワード」を入力し、[OK]をクリックします。

   ●ユーザー名：管理者のユーザー名

   ●パスワード：ユーザー名に対応したパスワード

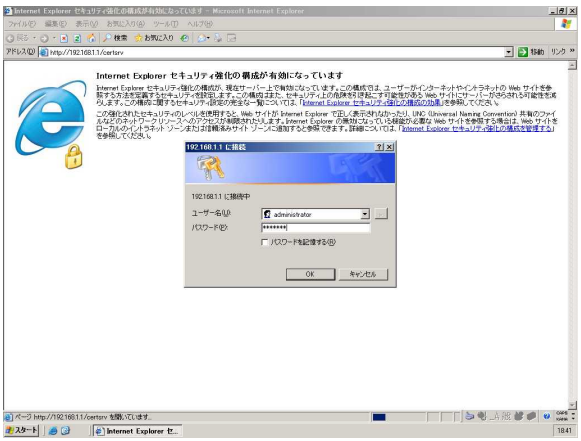


図１：証明機関へのアクセス

2. [Microsoft 認証サービス―CA]の画面が表示されたら、「CA 証明書、証明書チェーン、または CRL のダウンロード」をクリックします。

図２：タスクの選択

3. [CA 証明書、証明書チェーン、または CRL のダウンロード]画面が表示されたら、[CA 証明書のダウンロード]をクリックします。

図３：証明書の選択

4. [ファイルのダウンロード]画面が表示されたら[保存]をクリックし、適切な場所へファイルを保存します。ここではデスクトップ上に保存します。

図４：証明書のダウンロード

5. 保存した証明書をフロッピーやフラッシュメモリなどを用いて、認証端末へコピーします。

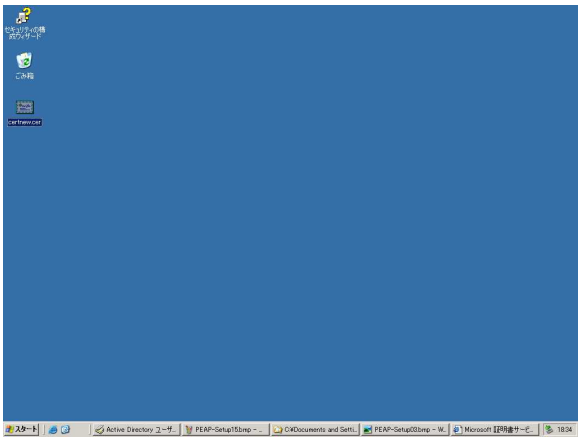


図５：証明書の保存

本マニュアルでは認証端末として WindowsXP での手順を示します。
その他の OS をお使いの場合は各 OS のメーカーへ設定方法をご確認願います。

---

6. 保存した証明書をダブルクリックすると以下の画面が表示されるので[証明書のインストール]をクリックします。

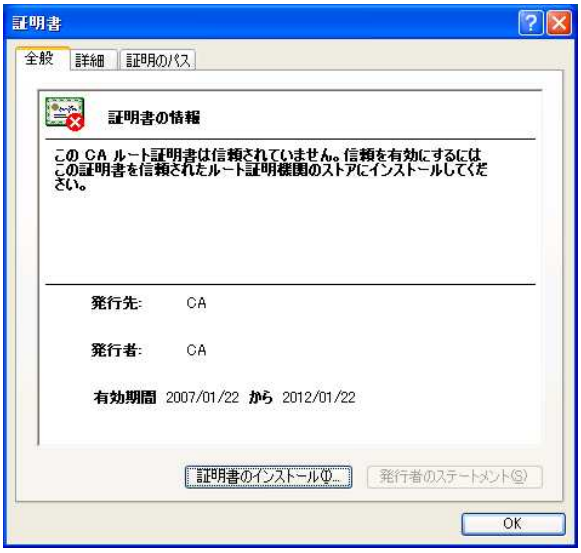


図６：証明書の情報

7. [証明書のインポートウィザード]が起動するので[次へ]をクリックして進めます。

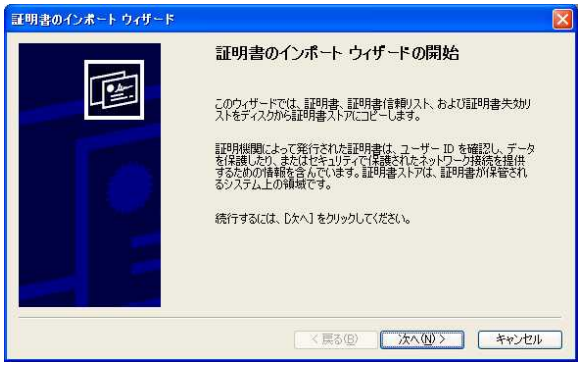


図７：証明書インポートウィザード

8. [証明書ストア]の選択方法画面が表示されるので、[証明書をすべて次のストアに配置する]を選択し、[参照]をクリックします。

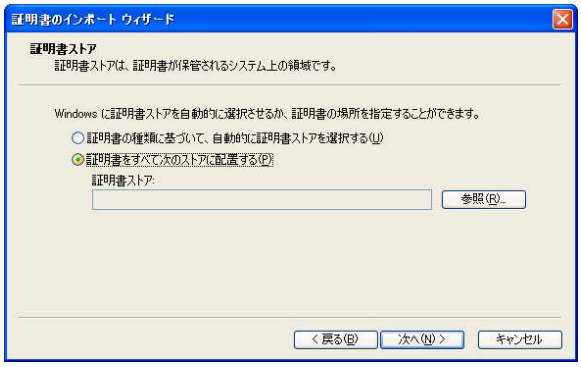


図８：証明書ストアの選択方法

9. [証明書ストアの選択]画面が表示されたら、[物理ストアを表示する]にチェックをいれ、[信頼されたルート証明機関]－[ローカルコンピュータ]を選択し、[OK]をクリックします。

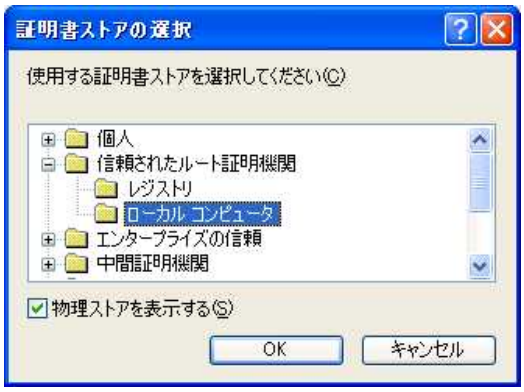


図９：証明書ストアの選択

10. [証明書ストア]の選択方法画面に戻ったら、[証明書ストア]に「信頼されたルート証明機関¥ローカルコンピュータ」と入力されていることを確認し、[次へ]をクリックします。

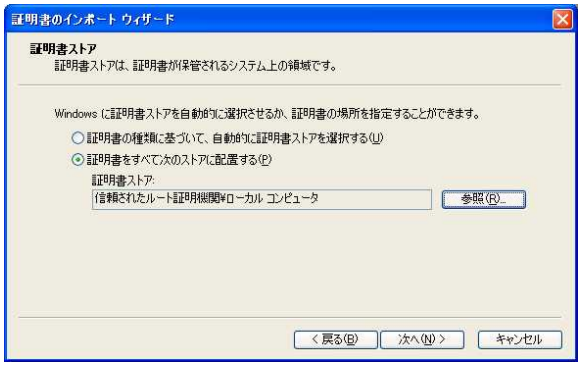


図１０：証明書ストアの選択方法

11. [証明書のインポートウィザード]の完了確認画面が表示されるので、内容を確認して[完了]をクリックします。

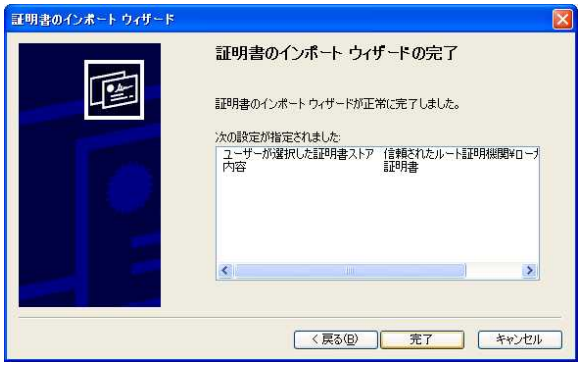


図１１：証明書インポートウィザードの完了確認

12. [証明書のインポートウィザード]の完了画面が表示されるので[OK]をクリックします。

図１２：インポート完了メッセージ

以上でルート証明書のインストールは完了です。
複数のパソコンにルート証明書をインストールする場合は同様の操作を行ってください。
引き続き EAP-PEAP 認証の為に IAS の設定を行います。

●EAP-PEAP 認証を行う為の IAS の設定

[準備編]でセットアップした IAS を EAP-PEAP 認証を行うために設定します。

1. ［スタート］－［管理ツール］－［インターネット認証サービス］を選択します。
2. ［インターネット認証サービス］画面において左枠内の［リモートアクセスポリシー］を選択し、右枠内のリモートアクセスポリシーから認証される端末に該当するリモートアクセスポリシーを選択し、ダブルクリックします。本マニュアルでは以下のリモートアクセスポリシーを選択します。
   ●無線接続パソコン　→　無線用リモートアクセスポリシー（例：WLAN）
   ●有線接続パソコン　→　有線用リモートアクセスポリシー（例：LAN）

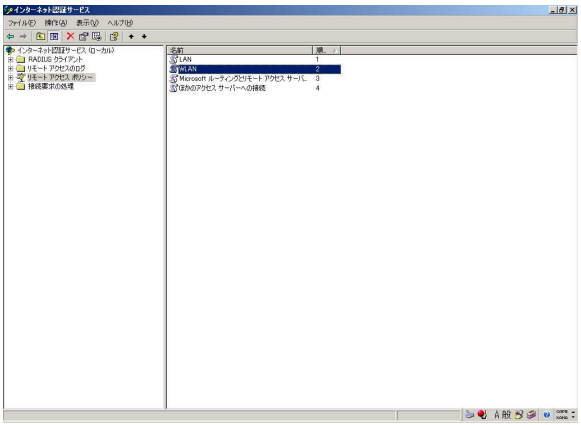


図１：リモートアクセスポリシーの選択

3. ［リモートアクセスポリシー］プロパティで、［接続要求が指定の条件を満たした場合］の欄に［リモートアクセス許可を与える］が選択されていることを確認し、［プロファイルの編集］をクリックします。

図２：リモートアクセスポリシーのプロパティ

4. ［ダイヤルインプロファイルの編集］画面で［認証］タブを選択します。［認証］設定画面が表示されたら、「Microsoft 暗号化認証バージョン 2（MS-CHAP v2）」にチェックが入っていることを確認し、［EAP メソッド］をクリックします。

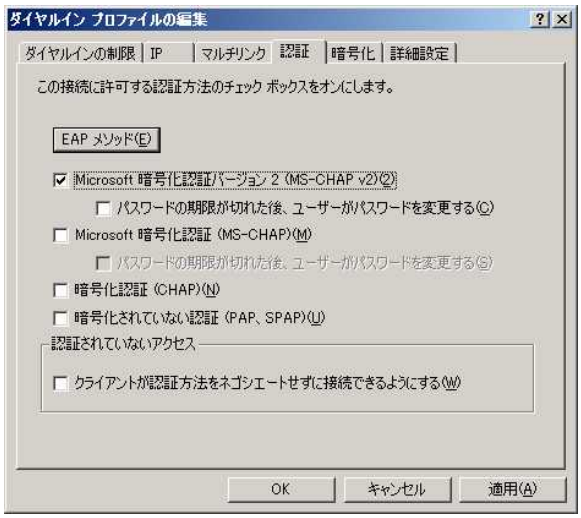


図３：ダイヤルインプロパティの編集

5. ［EAP プロバイダの選択］画面で［保護された EAP（PEAP）］を選択し、［編集］をクリックします。EAP の種類に［保護された EAP（PEAP）］の表示がない場合は［追加］をクリックし、EAP を追加します。

図４：EAP プロバイダの選択

6. ［保護された EAP のプロパティ］画面で、［証明書の発行先］及び［EAP の種類］に適切なものが選択されていることを確認します。本マニュアルでは以下の値を用います。設定できたら［OK］をクリックします。

●証明書の発行先：証明機関（CA）のコンピュータ名（例：buffalo.buffalo2003.local）

●EAP の種類：セキュリティで保護されたパスワード（EAP-MSCHAP v2）

図５：保護された EAP のプロパティ

7. これまで表示された画面において［OK］をクリックし、［インターネット認証サービス］画面まで戻ります。

図６：EAP プロバイダの選択

●認証端末でのサプリカント設定

最後に認証端末でのサプリカントを設定します。

ここではサプリカントとして BUFFALO 製クライアント接続ツール「クライアントマネージャー３」を用いた設定方法を説明します。

1. BUFFALO 製無線 LAN 製品に添付されているエアナビゲーターのウィザードに従い、「クライアントマネージャー３」をインストールします。
2. タスクバーの右下にあるクライアントマネージャー３のアイコンを右クリックし、［オプション］を選択します。

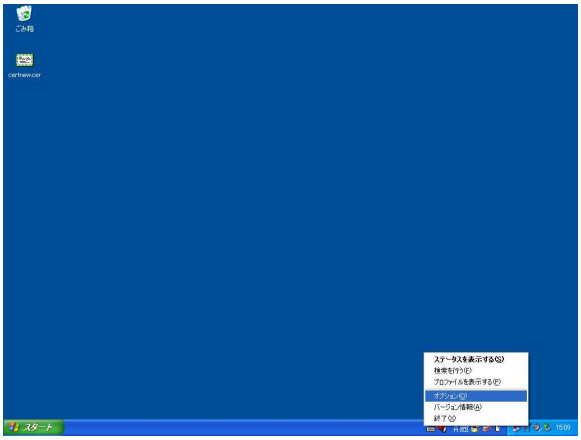


図１：オプションの選択

3. ［オプション］画面が表示されたら、［動作モード］に［ビジネスモード］を選択します。［使用するアダプタ］欄においては無線 LAN アダプタを使用する場合は、［無線アダプタ自動選択］が選択されていることを確認します。有線で接続する場合には有線 LAN アダプタを直接指定します。設定できたら［OK］をクリックします。

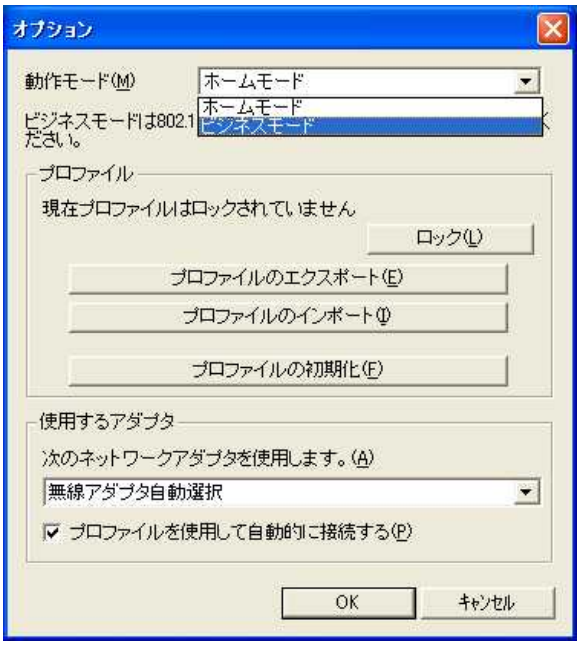


図２：オプション画面

4. タスクバーの右下にあるクライアントマネージャー３のアイコンを右クリックし、［プロファイルを表示する］を選択します。

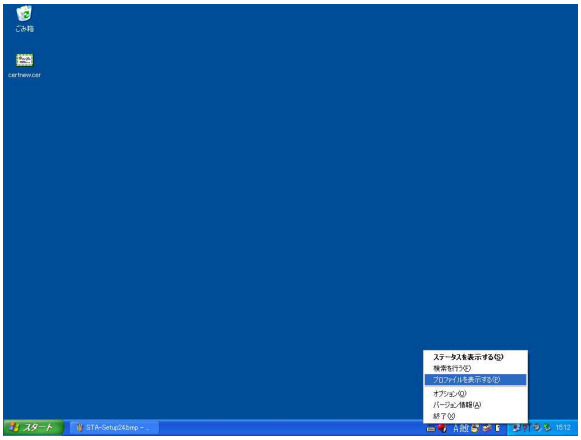


図３：プロファイルの選択

5. ［プロファイル］画面が表示されたら、画面右下の［802.1x プロファイル］をクリックします。

図４：プロファイル画面

6. ［認証プロファイル一覧］画面が表示されたら、［新規］をクリックします。

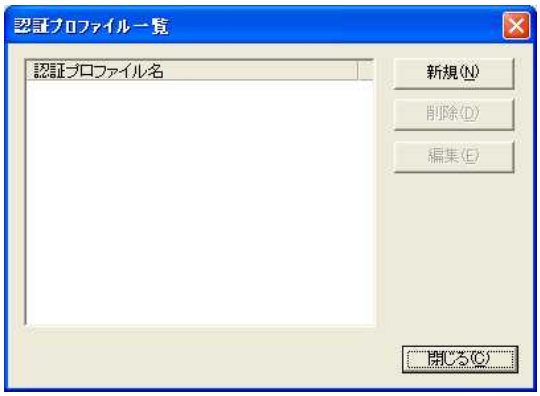


図５：認証プロファイル一覧

7. ［認証プロファイル］画面が表示されたら、EAP-PEAP 認証にあわせて、適切な値を設定します。ここでは以下の値を設定します。設定したら［OK］をクリックします。

●プロファイル名：任意の名称（例：EAP-PEAP）

●EAP の種類：EAP-PEAP

●クライアント設定：認証開始時にユーザ名とパスワードを入力する（使用環境に合わせます）

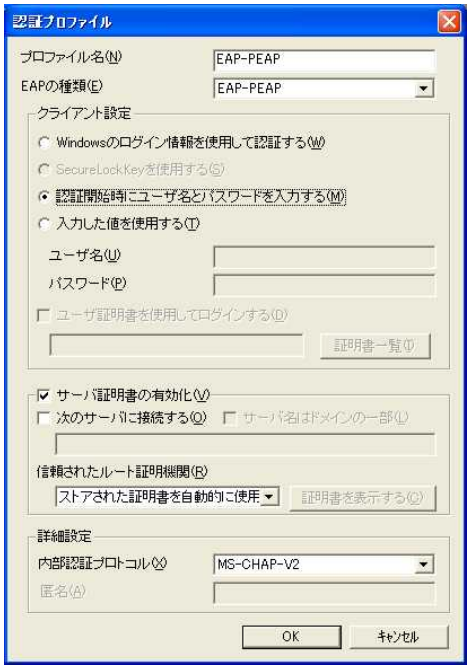


図６：認証プロファイル

8. ［認証プロファイル一覧］画面に戻ったら、［閉じる］をクリックします。

図７：認証プロファイル一覧

9. ［プロファイル］画面に戻ったら、画面左下の［追加］をクリックします。

図８：プロファイル画面

10. ［プロファイル情報］画面が表示されたら、［基本設定］タブを選択し、プロファイルの設定を行います。ここでは以下の値を設定します。設定したら[OK]をクリックします。

●プロファイル選択：無線

●プロファイル名：Wireless-PEAP

●ネットワークタイプ：インフラストラクチャモード

●SSID：BUFFALO2003**（お使いの無線** LAN **環境に合わせます）**

●暗号化方式：WPA-EAP AES**（お使いの無線** LAN **環境に合わせます）**

●認証プロファイル：EAP-PEAP

図９：プロファイル情報

有線用にプロファイル設定する際には以下の項目を設定します。

●プロファイル選択：有線

●プロファイル名：Wired-PEAP

●認証プロファイル：EAP-PEAP

---

11. **次に［ネットワーク］タブを選択し、**

12. **［ブラウザ］タブを選択し、**

13. **プロファイルが登録されたら、選択して[接続]をクリックします。**

図１０：プロファイル画面

14. **無線 AP への接続と認証が開始されますので完了するまでしばらく待ちます。**

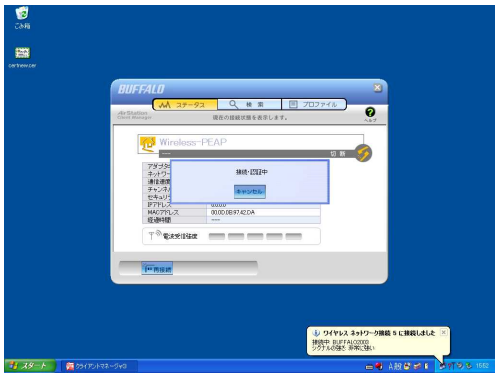


図１１：接続中画面

15. **[認証情報を入力してください]の画面が表示されたら、[準備編]の[ユーザアカウントの登録]で登録した[ユーザ名]と[パスワード]を入力します。**

図１２：認証情報入力画面

16. **[認証完了]のメッセージが表示されたら接続完了です。**

図１３：認証完了画面

■EAP-TLS 認証を行う為の設定（無線及び有線）

以下では EAP-TLS 認証を行うために次の手順で設定を行います。

一．認証されるクライアントコンピュータ（以下、認証端末）へのルート証明書及びユーザー証明書のインストール

一．EAP-TLS 認証を行う為の IAS の設定

一．認証端末でのサプリカント設定

●ルート証明書とユーザー証明書のインストール

EAP-TLS 認証で用いるルート証明書とユーザー証明書の発行及びインストールを行います。

1. 認証端末で WWW ブラウザを立ち上げ、URL 入力欄に「http：//（証明機関の IP アドレス）/certsrv」を入力します。認証画面が開いたら認証端末で認証に用いる「ユーザー名」と「パスワード」を入力し、[OK]をクリックします。

   ●ユーザー名：Active Directory に登録されたユーザー名

   ●パスワード：ユーザー名に対応したパスワード

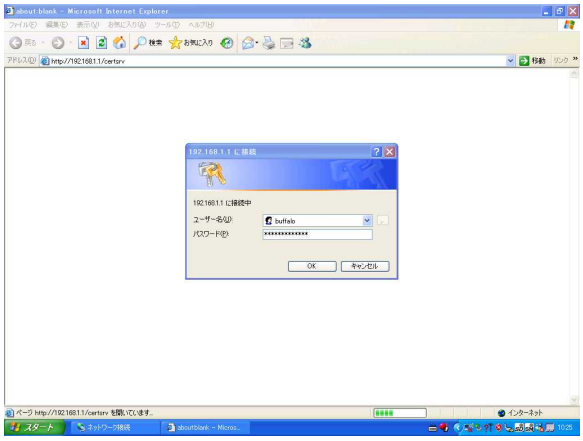


図１：証明機関へのアクセス

証明書のインストールにあたり、まず初めに認証機関(CA)へは EAP-TLS 認証なしでアクセスする必要があります。有線による接続などの任意の方法で CA へアクセスしてください。

---

2. [Microsoft 認証サービス－CA]の画面が表示されたら、「証明書を要求する」をクリックします。

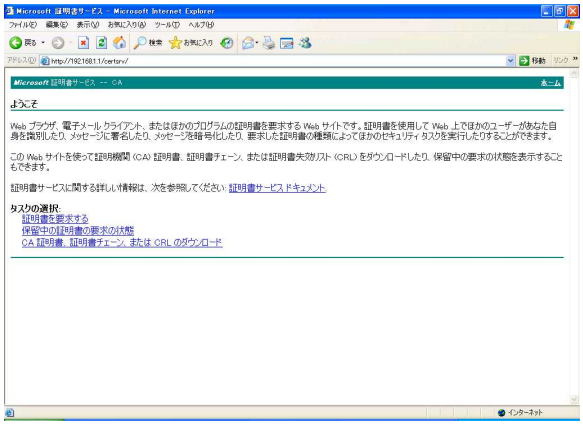


図２：タスクの選択

3. [証明書の要求]画面が表示されたら、[証明書の種類の選択]で[ユーザー証明書]をクリックします。

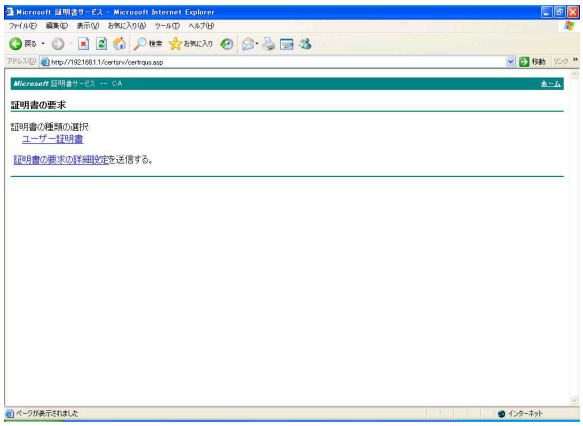


図３：証明書の選択

4. [ユーザー証明書－識別情報]の画面が表示されたら、[送信]をクリックします。

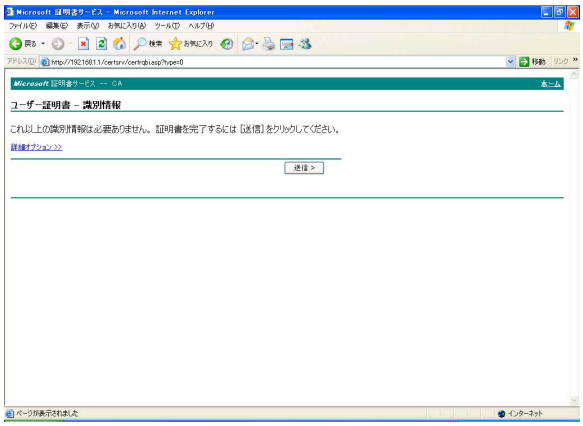


図４：証明書のダウンロード

5. [潜在するスクリプト違反]のメッセージが表示されますので、[はい]をクリックします。

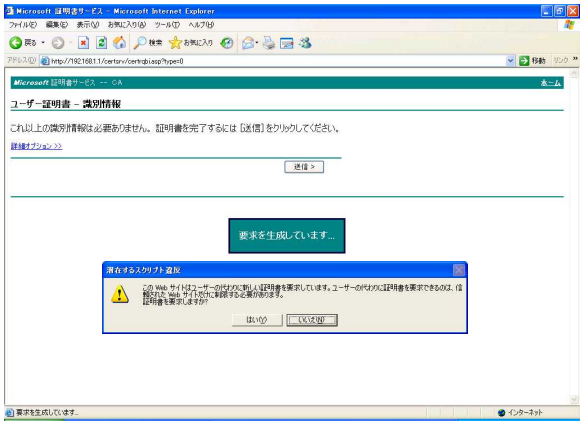


図５：証明書の要求

6. [証明書は発行されました]の表示がされますので、[この証明書のインストール]をクリックします。
その際[潜在するスクリプト違反]のメッセージが表示されるので、[はい]をクリックします。

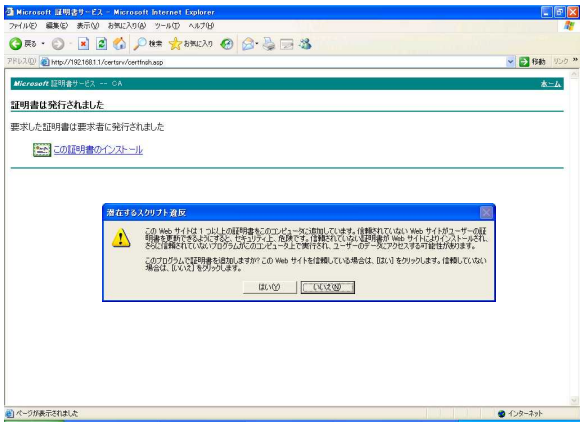


図６：証明書の発行

ルート証明書がインストールされていない場合、上記メッセージの前にルート証明書をインストールする旨のメッセージが表示されますので、[はい]をクリックします。

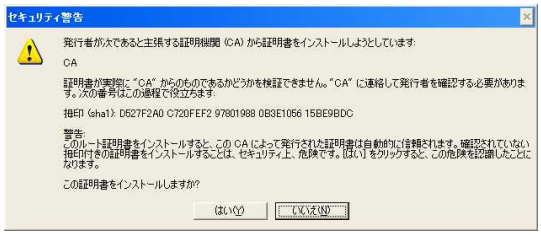


図７：ルート証明書のインストール

---

7. 証明書のインストールが完了した旨のメッセージが表示されれば、証明書のインストール作業は終了です。

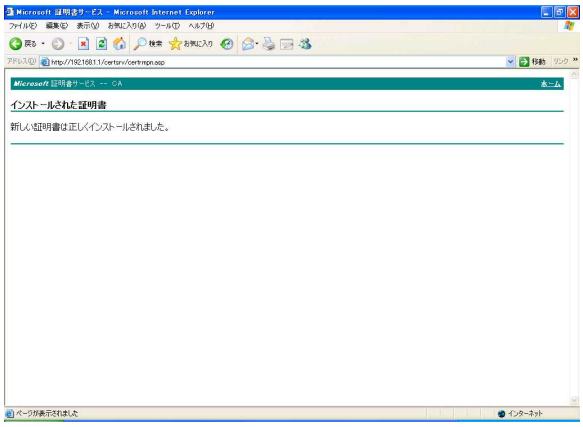


図８：証明書のインストールの完了

以上でルート証明書及びユーザー証明書のインストールは完了です。
複数のパソコンにルート証明書及びユーザー証明書をインストールする場合は同様の操作を行ってください。
引き続き EAP-TLS 認証の為に IAS の設定を行います。

●EAP-TLS 認証を行う為の IAS の設定

[準備編]でセットアップした IAS を EAP-TLS 認証を行うために設定します。

1. ［スタート］－［管理ツール］－［インターネット認証サービス］を選択します。
2. ［インターネット認証サービス］画面において左枠内の［リモートアクセスポリシー］を選択し、右枠内のリモートアクセスポリシーから認証される端末に該当するリモートアクセスポリシーを選択し、ダブルクリックします。本マニュアルでは以下のリモートアクセスポリシーを選択します。

●無線接続パソコン　→　無線用リモートアクセスポリシー（例：WLAN）

●有線接続パソコン　→　有線用リモートアクセスポリシー（例：LAN）

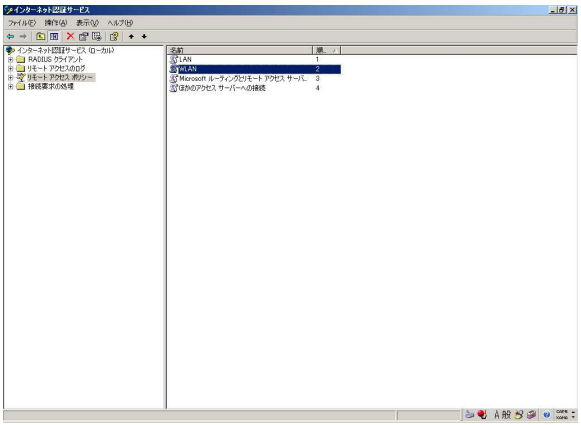


図１：リモートアクセスポリシーの選択

3. ［リモートアクセスポリシー］プロパティで、［接続要求が指定の条件を満たした場合］の欄に［リモートアクセス許可を与える］が選択されていることを確認し、［プロファイルの編集］をクリックします。

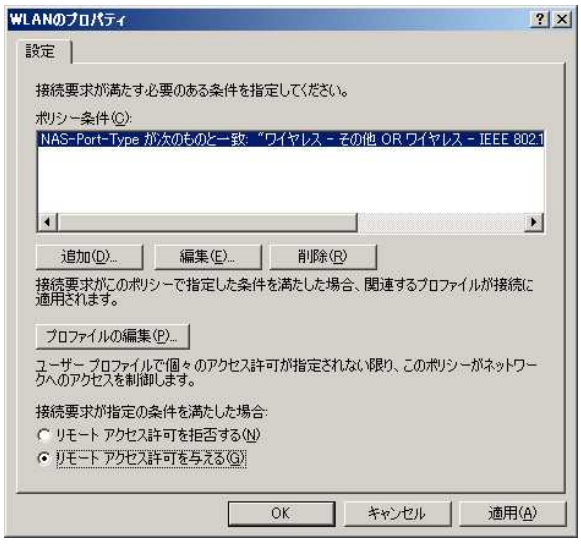


図２：リモートアクセスポリシーのプロパティ

4. ［ダイヤルインプロファイルの編集］画面で［認証］タブを選択します。［認証］設定画面が表示されたら、「Microsoft 暗号化認証バージョン 2（MS-CHAP v2)」のチェックをはずし、［EAP メソッド］をクリックします。

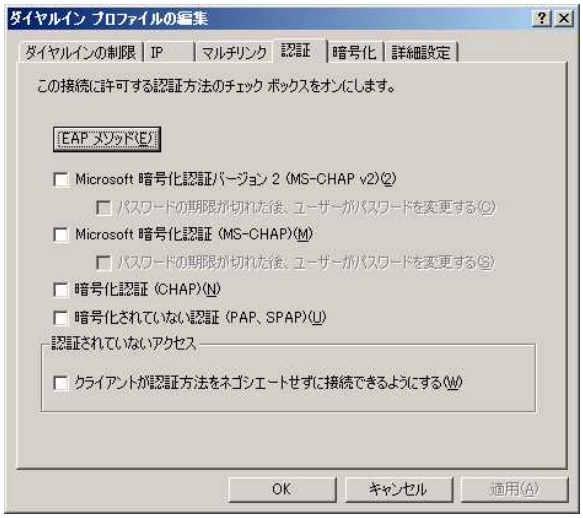


図３：ダイヤルインプロパティの編集

5. ［EAP プロバイダの選択］画面で［保護された EAP（PEAP)］を選択し、［削除］をクリックします。

図４：EAP プロバイダの選択

6. ［EAP の種類］に［スマートカードまたはその他の証明書］が表示されていない場合は、［追加］をクリックし、［スマートカードまたはその他の証明書］を追加します。

図５：EAP の追加

7. ［EAP プロバイダの選択］画面で［スマートカードまたはその他の証明書］を選択し、［編集］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］画面において、［証明書の発行先］に適切なものが選択されていることを確認します。本マニュアルでは以下の値を用います。適切に設定できたら［OK］をクリックします。

●証明書の発行先：証明機関（CA）のコンピュータ名（例：buffalo.buffalo2003.local）

図６：保護された EAP のプロパティ

8. これまで表示された画面において［OK］をクリックし、［インターネット認証サービス］画面まで戻ります。

図７：EAP プロバイダの選択

●認証端末でのサプリカント設定

最後に認証端末でのサプリカントを設定します。

ここではサプリカントとして BUFFALO 製クライアント接続ツール「クライアントマネージャー３」を用いた設定方法を説明します。

1. BUFFALO 製無線 LAN 製品に添付されているエアナビゲーターのウィザードに従い、「クライアントマネージャー３」をインストールします。
2. タスクバーの右下にあるクライアントマネージャー３のアイコンを右クリックし、［オプション］を選択します。

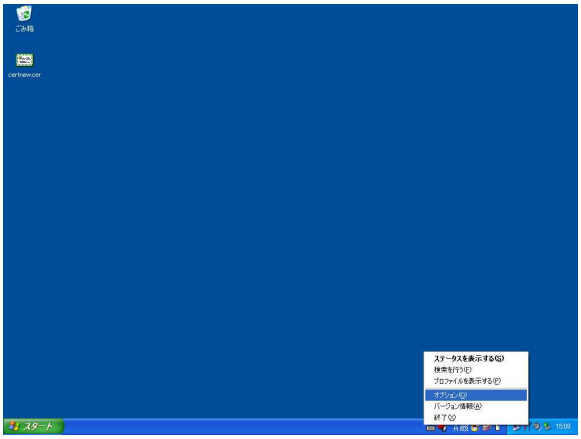


図１：オプションの選択

3. ［オプション］画面が表示されたら、［動作モード］に［ビジネスモード］を選択します。［使用するアダプタ］欄においては無線 LAN アダプタを使用する場合は、［無線アダプタ自動選択］が選択されていることを確認します。有線で接続する場合には有線 LAN アダプタを直接指定します。設定できたら［OK］をクリックします。

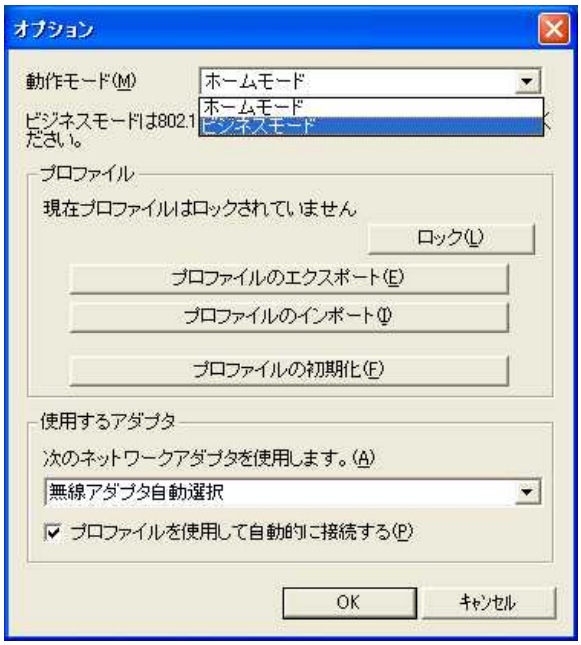


図２：オプション画面

4. タスクバーの右下にあるクライアントマネージャー３のアイコンを右クリックし、［プロファイルを表示する］を選択します。

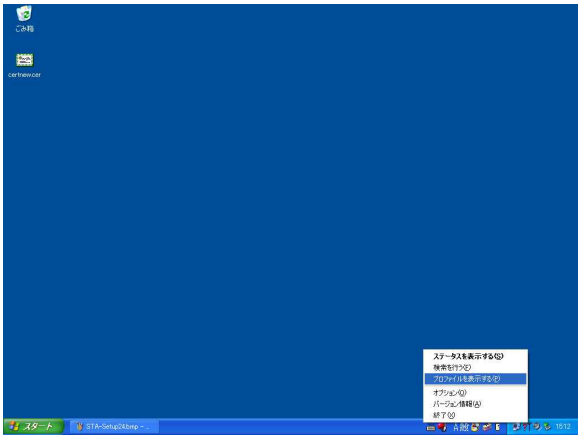


図３：プロファイルの選択

5. ［プロファイル］画面が表示されたら、画面右下の［802.1x プロファイル］をクリックします。

図４：プロファイル画面

6. ［認証プロファイル一覧］画面が表示されたら、［新規］をクリックします。

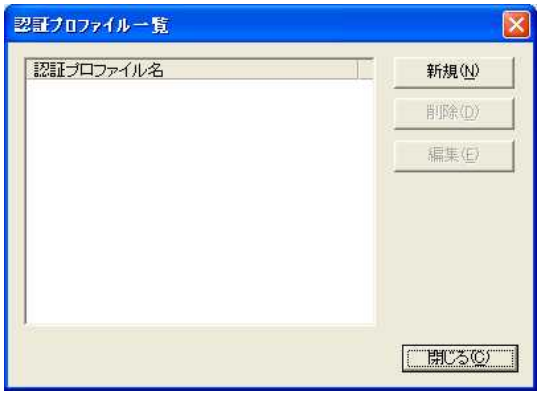


図５：認証プロファイル一覧

7. ［認証プロファイル］画面が表示されたら、EAP-TLS 認証にあわせて、適切な値を設定します。ここでは以下の値を設定します。設定したら［OK］をクリックします。

●プロファイル名：任意の名称（例：EAP-TLS）

●EAP の種類：EAP-TLS

●クライアント設定：入力した値を使用する（例：bufflo）

※ユーザー証明書発行時に使用したユーザー名

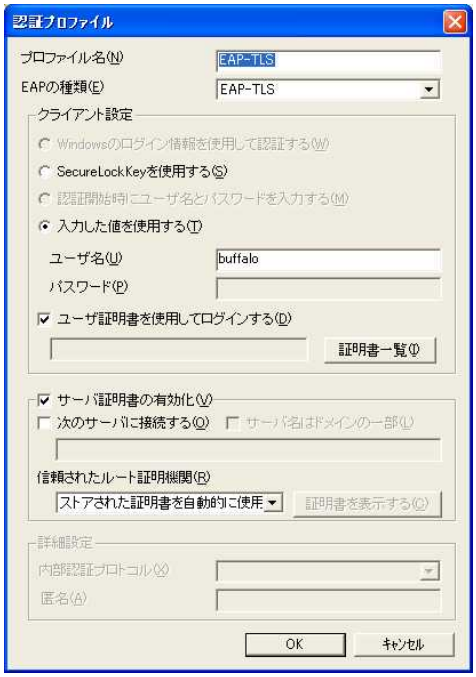


図６：認証プロファイル

ユーザ証明書の設定については、［証明書一覧］をクリックし、［証明書一覧］画面からユーザ名に対応したユーザ証明書を指定します。

図７：ユーザ証明書一覧

［ユーザ名の不一致］のメッセージが表示されたら［キャンセル］をクリックします。

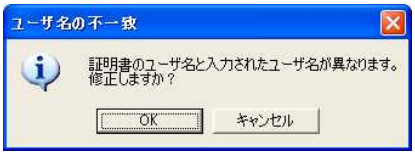


図８：ユーザ名の不一致

---

8. ［認証プロファイル］の設定を行ったら、［OK］をクリックし［認証プロファイル一覧］に戻ります。

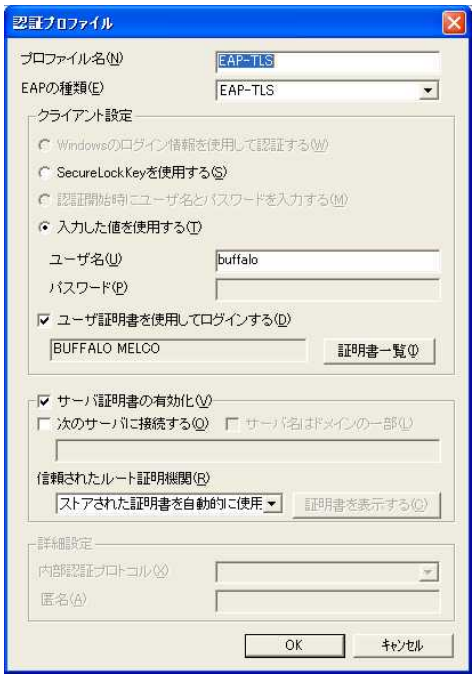


図９：認証プロファイル

9. ［認証プロファイル一覧］画面に戻ったら、［閉じる］をクリックします。

図１０：認証プロファイル一覧

10. ［プロファイル］画面に戻ったら、画面左下の［追加］をクリックします。

図１１：プロファイル画面

11. ［プロファイル情報］画面が表示されたら、［基本設定］タブを選択し、プロファイルの設定を行います。ここでは以下の値を設定します。

●プロファイル選択：無線

●プロファイル名：Wireless-TLS

●ネットワークタイプ：インフラストラクチャモード

●SSID：BUFFALO2003**（お使いの無線 LAN 環境に合わせます）**

●暗号化方式：WPA-EAP AES**（お使いの無線 LAN 環境に合わせます）**

●認証プロファイル：EAP-TLS

図１２：基本設定

有線用にプロファイル設定する際には以下の項目を設定します。

●プロファイル選択：有線

●プロファイル名：Wired-TLS

●認証プロファイル：EAP-TLS

---

12. ［ネットワーク］タブを選択し、IP アドレス及び DNS サーバの設定を行います。ここではどちらとも［自動的に取得する］に設定します。［ブラウザ］及び［プリンタ］も環境に合わせ設定します。

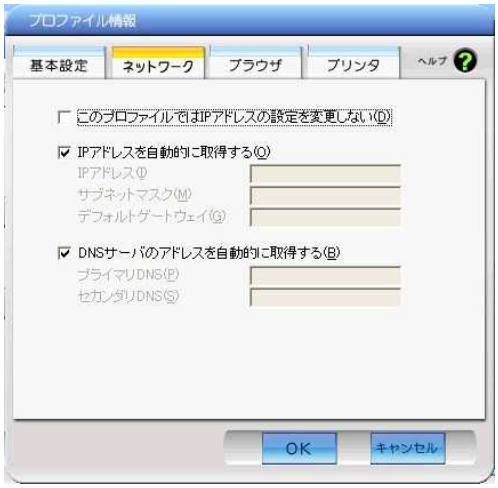


図１３：ネットワーク設定

13. **プロファイルが登録されたら、選択して[接続]をクリックします。**

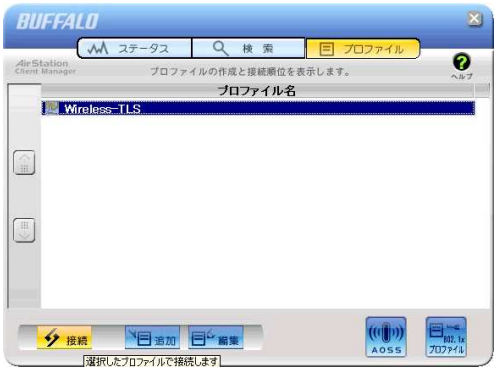


図１４：プロファイル画面

14. **無線 AP への接続と認証が開始されますので完了するまでしばらく待ちます。**

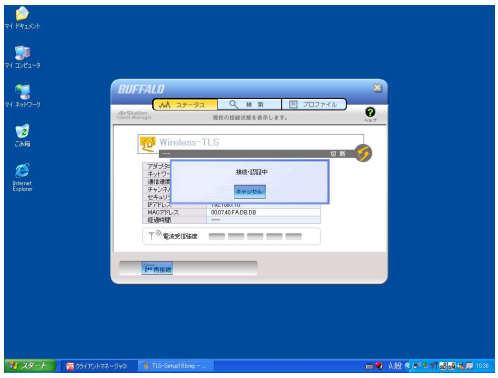


図１５：接続中画面

15. **[認証完了]のメッセージが表示されたら接続完了です。**

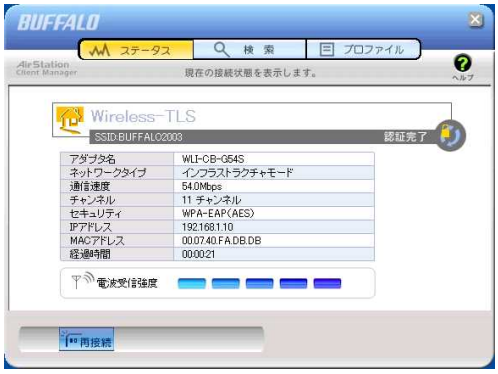


図１６：認証完了画面

■改版履歴

・2007 年 4 月 27 日　　初版作成・発行