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

サーバーの構成ウィザード	×
NetBIOS 名 Windows 2000、Windows XP、Windows Server 2003 フェミリ以外のバージョンの Windows を実行しているクライアントは、 NetBIOS ドメイン名を使用します。	ST.
既定の NetBIOS 名が DNS ドメイン名がら派生します。	
DNS ドメイン名:	
buffalo2003.local	
NetBIOS ドメイン名(E):	
RUEFAL02008	
〈戻る(風) 〉 キャンセル	ヘルプ

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。

DNS クエリを転送しています フォワーダに指定された DNS サーバーは、こ	のサーバーでは解決されない DNS クエリを解決します。	Z
このサーバーは解決できない DNS クエリ ロ リクエストを他の DNS サーバー(フォワーダ)	P アドレスからコンピュータ名に変換する要求)を受信した可能1 (こ転送するように、このサーバーを設定することができます。	生があります。これらの
インターネット サービス プロバイダ (ISP) を(ください。ISP を使わない場合は、ネットワー	要ってインターネットに接続する場合は、ISP に連絡してフォワータ ク管理者に連絡してフォワーダのアドレスを取得してください。	のアドレスを取得して
このサーバーが解決されていない DNS クエ	りを転送するようにしますか?	
○ この IP アドレスの DNS サーバー(こうエ)	Jを転送します(Y):	
① いいえ、クエリを転送しません(Q)		
	and the Construction Construction	

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。

サーバーの構成ウィザード		×
選択を通用しています このサーバーに選択した役割を追加しています。		15 million
	(記5(日) たい(4)) キャン(77)()	A.1.7

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。

ndows コンポーネント Windows のコンポーネントを追り	加または削除できます。	
各チェック ボックスをクリックして、 ボックスは、コンボーネントの一番 を表示するには、 [詳細] をクリ・ コンボーネント(C)	追加または削除するコンポーネントを 部がインストールされることを表します。 っりしてください。	選んでください。 影付きのチェック コンボーネントに含まれているもの
アクセサリとユーティリテ	4	4.8 MB
☑ (■アプリケーション サーバ		33.4 MB
□ ��インデックス サービス		0.0 MB
□ りセキュリティの構成ウィ	ザード	2.1 MB 🚽
INB ASPNET	パターネット インフォメーション サービス	(IIS)、およびアプリケーション サー

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。

CA の種類				æ
セットアップする CA の種類を	選択してください。			U
◎ エンターフライスのルート	CA(E)			
○ エンタープライズの下位 (DA(<u>R</u>)			
C スタンドアロンのルート Ci	A(<u>S</u>)			
○ スタンドアロンの下位 CA	Ð			
CA の種類の説明				
エンカニペニイブのニー来(言)	順されている こみ です	(FI)/D CA HIER	前にインストールする。必要	更があり
ます。	active office	5 (a)) (0) (1) (3) (1)		A13077
57. STAN	active on co	5 660 00 00 65 01		4.007
193 - 991 All arian		s lauros on assor	nici 2711 7670423	
193 - 991 × 00 - 19184				
ます。 していたい しんしょう しんしょう しんしょう しんかく しょう しんかく します しんかく します しんかく します しんかく しょう しんかく しゅう	キーの組と CA 証明書	また生成する①		
ます。 「カスタム設定を使用して3	キーの組と CA 証明者	また生成する(U)		
100 971人の Wrat	キーの組と CA 証明書	またしていたい。 また生成する(<u>U</u>)		
まごう ファイスの 留信4	キーの約1と CA 証明書	************************************		

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。

aows ቧጋሎ ተፈንኮ ባብታት	
CA 識別情報 この CA を識別する情報を	入力してください。
この CA の共通名(<u>C</u>):	
CAL	
識別名のサフィックス(型):	
DC=buffalo2003,DC=local	
識別名のブレビュー(P):	
CN=CA,DC=buffalo2003,DC	Flocal
	1月37月9月8日 2012/01/22 21:07
P 14 1	
	〈戻る(日) 次へ(N) > キャンセル ヘルプ

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。

arena) - X/ - X/0/		
C:¥WINDOWS¥system32¥CertI	Log	参照(Q)_
証明書データベース ログ(D):		
C:¥WINDOWS¥system32¥CertI	Log	参照(₩)
共有フォルダ(<u>H</u>): 共有フォルダ(<u>H</u>):	B 2 9 Q	参照(6)

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。

Microsof	t 証明書サービス	×
1	インストールを完了するには、証明書サービスによりインターネットインフォメーション サービスを一時的に停止する必要が ります。このサービスを今ずく停止しますが? 	あ

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。

dows コンポ コンポーネン 要求した	ー ネント ウィザード トの構成 傷成の変更を適用しています。	Ē
6	コンボーネントを構成しています。しばらくお待ちください。選択したコンボーネントによって、 少々時間がかかることがあります。	
状態	証明書サービスの構成を完了しています_	
	< 戻る(8) 次へ(10) > へ	ルブ

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。

יעב vindows Windows ወ	ドーネント コンポーネントを追加	ロまたは削除できます。		
各チェックオ ボックスは、 を表示する コンポーネン	∜ックスをクリックして、 コンポーネントの一音 には、『詳細』 をクリッ 小ト(℃):	追加または削除するコンポーネントを述 防インストールされることを表します。コ クしてください。	置んでください。影付きのチェック コンボーネントに含まれているも	5
1 2/2-	ミナル サーバー ライ	センス	0.9 MB	٠
	・トワーク サービス		2.6 MB	
🗆 🚚 y t	ート インストール サ	ービス	2.0 MB	(test
V 🖾 //~	ート証明書の更新		0.0 MB	-
脱明	特別なネットワ	ーク関連のさまざまなサービスやブロトコ	ルが含まれています。	
必要なディ	スク領域の合計:)領域:	3.4 MB 29094.7 MB		

図2:Windows コンポーネントの選択

[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。

ネットワーク サービス			×
各チェック ボックスをクリックしつ ボックスは、コンボーネントの一 を表示するには、ほ羊細1 をク ネットワーク サービス のサブコ	、、追加また(肖明徐するコンボ・ ・部がインストールされることをま リックしてください。 ンボーネント(Q)	ーネントを選んでください。影付きのチェック 表します。コンボーネントに含まれているもの	
🗆 🌉 HTTP プロキシを経	自した RPC	0.0 MB 🔺	
🗌 🚚 Windows インターネ	ットネーム サービス (WINS)	0.9 MB	
🔽 🖳 インターネット認証サ	-ëz	0.0 MB	
🛛 🛃 ドメイン ネーム シス	FL (DNS)	1.6 MB	
🗌 🚚 リモート アクセス検疫	サービス	0.1 MB	1
🗌 🚚 簡易 TCP/IP サービ	え	00 MB 👻	1
説明: ダイヤルアップと V ット認証サービス	PN ユーザーの認証、承認お。 IAS) (‡ RADIUS プロトコルを	はびアカウンティングを有効にします。インターネ サポートします。	
必要なディスク領域の合計: 空きディスク領域:	3.4 MB 29094.0 MB		
		OK キャンセル	

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。

a construction of the second	
各チェックボックスをクリックして、追加または算明除するコンボーネントを選ん ボックスは、コンボーネントの一部がインストールされることを表します。コン を表示するには、国新聞をクリックしてください。	んでください。 影付きのチェック /ボーネントに含まれているもの
コンボーネント©> コンボーネント©> コンボーネント©> コンボーネント©> コンボーネント©> コンボーネント©> コンボーネント©> コンボーネント©> コンボーネント©> コンボーネント©> コンボーネント©> コンボーネント©> コンボーネント©>	0.9 MB 🔺
☑ 書コネットワーク サービス	2.6 MB
🗆 🚚リモート インストール サービス	2.0 MB
■ ルート証明書の更新	0.0 MB 🚽
説明 特別なネットワーク関連のさまざまなサービスやプロトコル	が含まれています。
必要なディスク領域の合計: 3.4 MB 空きディスク領域: 29093.6 MB	詳細(<u>D</u>)

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

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。



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。
- [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。

(シターネット記録)	t~E2 (0~b/l)	212月名	7562	701-26	クライアント製造元		2
リモート アウセ	MUCH RADIUS OPH 75 M	<u></u>		2063-636	示する項目は取りません。		
リモートアクロ	MURITER QD	•					
	表示(2)	•					
	最新の情報に更新を) 一覧のエクスポートUL						
	ヘルプ(日)						

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。

	DYENS REVISER
フレンドリ名(E):	AirStation
クライアントのアドレス (IP または Df	NS)(D):
192.168.1.3	· · · · · · · · · · · · · · · · · · ·

図 2: RADIUS クライアント情報の入力

 [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。

RADIUS Stendard ▼ ▼	1アンドヘンダの腐住に奉うくりモー! 第定してください。 1ライアント ベンダ(C):	、アクセスボリンーを使用している場合、RADIUS クライアンドのヘンタ
キ有シークレット(S): キ有シークレットの確認入力(Q): 「要求はメッセージ記証漏性を含んでいる必要がある(R)	RADIUS Standard	
キ有シークレットの確認入力(Q):	共有シークレット(<u>S</u>):	
一要求はメッセージ認証属性を含んでいる必要がある(B)	共有シークレットの確認入力(の):	
	- 要求はメッセージ認証属性を含/	いでいる必要がある(<u>R</u>)

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。
- [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。

ペリシーの構成方 に このウィザードで	ま は、標準ポリシー、またはカスタム ポリシーを作成できます。
このポリシーをど	のように設定しますか?
© ウィザート	を使って共通のシナリオの標準ポリシーを設定する(U)
C ታሪቃሪ	ポリシーを設定する(<u>6</u>)
このポリシーを表	す名前を入力してください。
ポリシー名(P):	WLAN
	例: すべての VPN 接続を認証。
	〈戻る(B) 【次へ(10)>】 キャンセル

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)

 [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。

次の基準でアク	セスを許可する:				
・ ユーザー(U ユーザーの	」 アクセス許可は、ユー	-ザー アカウントの・	中で指定されています	•	
C グループ(G)					
各ユーザー	のアクセス許可は、グ	ループのアクセス影	「可に上書きされます。		
グループ名	AB):				ietn(0)
					削除(包)

図5:アクセス許可の設定

 [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。

しいリモート アクセス ポリシー ウィザード		
EAPは、ユーザーを認証するために別の種類のセ	キュリティデバイスを使用します。	Ø
このポリシーの EAP の種類を選択する(S)		
種類①		
スマート カードまたはその他の証明書	•	構成(G)
スマート カードまたはその他の証明書		
(朱護された EAP (PEAP)		
	11 12 12 -	11 (11 - 11 - 11
	く 戻る(<u>B</u>) 次へ(<u>N</u>)	> キャンセル

図6:認証方法の選択(EAP-PEAPの場合)

 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。

インターネット以降サービス			_151×
• → 🗈 🖩 🗙 📽 🛱 😵 + +			
(-)シースト(1)(-)・(-)、(-)、(-)、(-)、(-)、(-)、(-)、(-)、(-)、(-)、	Edit Stati Stati<	1 18 / - 1 	

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。

	ジェッキスタリナキ			
接続要求加減たり。 地球ー条件の)	と要りのる余件を指.	走していたらい。		
NAS-Port-Type /	が次のものと一致: "	ワイヤレス - その1	也 OR ワイヤレ	ス - IEEE 802.
•				•
ishn(D)	編集(F)	賀北徐(R)	1	
		を満たした場合	」 明谊するプロフ・	マルガ接続に
適用されます。	> Clarcococi i			17073300000
	i(P)			
プロファイルの編集				
プロファイルの編集	」 、で個々のアクセス詳	可が指定されたい	服り このポリト	ノーガネットワー
プロファイルの編集 ユーザー プロファイル フへのアクセスを制徒	 いで個々のアクセス許 Pします。	可が指定されない	い限り、このポリシ	ノーがネットワー
プロファイルの編集 ユーザー プロファイル アへのアクセスを制徒 接続要求が指定の	ーーーー」 いで個々のアクセス許 叩します。 条件を満たした場合	可が指定されない	1限り、このポリシ	ノーがネットワー
プロファイルの編集 ユーザー プロファイル かへのアクセスを制徒 接続要求が指定の C リモート アクセス	 いで個々のアクセス許 叩します。 条件を満たした場合 許可を拒否する(<u>N</u>)	可が指定されない	略り、このポリシ	ノーがネットワー

図9:リモートアクセスポリシーのプロパティ

[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。

ポリシー条件(<u>C</u>): NAS=Port=Type /	が欠のものと一致: "	(01762-20)他 OR ワイヤ	7レス - IEEE 802
▲ ·追加(D) (編集(E)	賞	1	<u>)</u>
接続要求がこのポリ 適用されます。	シーで指定した条件	を満たした場合、	 関連するプロ	ファイルが接続に
(ブロファイルの編集	(P)			
ユーザー プロファイル クヘのアクセスを制徒	 っで個々のアクセス許 叩きす。	可が指定されな	い限り、このポ	リシーがネットワー
> >>>> >				

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。

and the second sec	rectory 1-9-2102	1-9			2
s smaller	牌作(A) 表示(公)	パンドウ酸 ヘルク	(B)		-0
> 🗈		8 226	274 k		
Active Dir	ectory ユーザーとコンピュー	buffalo2003.local	5 個のオブジェクト		
🗉 🦲 保存さ	れたウエリ	之前	種類	1388	
B D Durisio	2003 local ittin mouters	Builtin Computers	builtinDomain コンテナ	Default container for uppr	
1 (0) Do	main Controllers	Domin Cont.		Default container for sec	
🕀 🦲 For	reignSecurityPrincipals	Ciliars.	Tret	Default container for uner	
	制御の委任(E) 検索印				
		 エバュータ 連絡先 	2		
	ここから新しいウィンドウ	ガループ InetOrePe	rson		
	最新の情報に更新任	MSMQ #:	1-14072		
	プロパティ(8)	2-#-			
	AJL700	共有フォル	5		

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。

独生(上):	BUFFALO			1
名(E):	MELCO		イニシャルΦ	
フル ネーム(<u>A</u>):	BUFFALO MEL	.00		
ユーザー ログオン名(<u>U</u>):			
buffalo		@buffalo20	103.local	•
ユーザー ログオン名	(Windows 2000 以前:)∰:		
BUFFAL02003¥		buffalo		

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。

**		
フード変更が必要(M)		
<u>(2713</u>)		
1. T.	からしていた。 ない(S)	5000 (1997) 5000 (1997)

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。

完了]を	クリックすると、〉次(Dオブジェクト <u>た</u>	が作成されます:	
フルネー	L: BUFFALO M	ELCO		<u>_</u>
ユーザー	ログオン名: buffa	lo@buffalo20)03.local	
ユーザー(おパスワードを変す	更できない		

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。

委Active Directory ユーザーとコンピュ	1-2						_ 8
3 2m(ルE) 操作(A) 表示(2) り	シャンドウ国 ヘルプ田						- 8
	0	63 m					
Active Directory Turfful Tulfau	Hears 24 (Bittet TO yok	~ ~					
+ () 保存されたクエリ	久約	5625	1488				
E Duffalo2003.local	C Administrator	7-#-	コンピュータ/ドメインの管理。				
🕀 🦲 Builtin	BUFFALO MELCO	7-tf-					
🕀 🦲 Computers	Cort Publishers	ヤキョリティグル。	このグループのメンバは Acti				
🗄 🧕 Domain Controllers	CERTSVC DOOM ACCESS	セキュリティ グルー					
ForeignSecurityPrincipals	DHCP Administrators	セキュリティ グルー	DHOPサービスに対し管理。				
Users	DHCP Users	セキュリティ グルー	DHOP サービスに対し読み				
	Dra Admina	セキュリティグルー	DNS 管理者グループ				
	Dns Update Proxy	セキュリティ グルー	DHOP サーバーなどのほか				
	Domain Admins	セキュリティ グルー	ドメインの管理者				
	Domain Computers	セキュリティ グルー	ドメインのすべてのワークステー				
	Domain Controllers	セキュリティ グルー	ドメインのすべてのドメインコー				
	Domain Guests	セキュリティ グルー	ドメインの全ゲスト				
	Domain Users	セキュリティ グルー	ドメインの全ユーザー				
	Enterprise Admins	セキュリティ グルー	エンターブライズの管理者				
	Group Policy Creator Owners	セキュリティ グルー	このグループのメンパはドメイニ				
	Guest	ユーザー	コンピュータ/ドメインへのゲス。				
	HelpServicesGroup	セキュリティ グルー	ヘルプとサポート センターの				
	TILS_WPG	セキュリティ グルー	IIS ワーカ プロセス グループ				
	1 JUSR BUFFALO	ユーザー	インターネット インフォメーシー				
	MAN_BUFFALO	ユーザー	アウト プロセス アプリケーショー				
	RAS and IAS Servers	セキュリティグルー	このグループのサーバーはユー				
	Scheme Admins	セキュリティグル。	スキーマの指定された管理者				
	SUPPORT_38894540	ユーザー	ヘルプとサポート サービスのニ				
	TelnetGlients	セキュリティ グルー	このグループのメンパはこのシュ				
				20	A 99	30	() COPE

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。

IFFALO MELOOU/U/J/	?
全般 住所 アカウント プロファイル ダイヤルイン 環境 セッション リモート制能	↓ 電話 組織 所属するグループ 卸 ターミナル サービスのプロファイル COM
「リモート アクセス許可 (ダイヤルインまたは VF	N)
 アクセスを許可(W) 	
○ アクセスを拒否(①)	
€ リモート アクセス ポリシーでアクセスを制徒	印(户)
▶ 発信者番号を確認(型)	-
「コールバック オプション	,
☞ コールバックしない(©)	
○ 呼び出し元による設定 (ルーティングとり)	Eート アクセス サービスのみ)(<u>S</u>)
○ 常に次の電話番号にコールバック(⊻)	
一 静的 IP アドレスを割り当てる(G)	()
┏ 静的ルートを適用(E)	,
このダイヤルイン接続に対して有効にするル 義してください。	卜を定

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。

bWL入り ④ g=th&tag=bridge LANポート	Jan						💌 🛃 1540	1)29 ×
a=th&tag=bridge LANポート	Jan .	12			_		💌 💽 1540	リンク >>
LANボート	=martin						and the second second	
	設正						7 11	ブ
W御IIPアドレ	a	C DMCPサーバからJPアドレス の 手動設定 JPアドレス 192.168 サブキットマスク[265.265	*自動取得 1.3 5255.0 ▼					_
は張設定]								
・フォルトゲー	トウェイ							
107-5. 1.1++.	1.000.000	プライマリ:						
10(x-4))	-/// / /	レス セカンダリ: [
SEEVLAN ID		1						
線LANボー	ト設定							
調出ポート	有効	YLANモー F	通信方式					
線ボート(目)	有効王	Untassed Port 💌 VLAN ID 1	inteing	6M 👱	M01	自動		
「線水ート(#2)	有効・	Untagged Port VLAN ID 1	通信速度	自動 👱	MOI	自動・		
線ボート(お)	有效主	Untagged Port VLAN ID 1	通信速度	自動 💌	MOI	自動 💌		
16泉水ート(\$4)	有效。	Untagged Port • VLAN ID 1	incient	840 <u>-</u>	101	自動・		
定								
	N例JPアドレ: 立張設定 フォルトゲー S(ネーム)サ・ 禁ULAN ID 終しんN ポート 線ポート(和) 線ポート(和) 連 変	N間IPアドレス な変換定] フォルドグートウェイ S(ネーム)サーバアド TEVLAN ID 酸LANKモート酸定 酸体モート物の 酸ポート(4) 有効子 酸ポート(4) 有効子 酸ポート(4) 有効子 変	Representation Repres	ROD = 100-517 として名称的時	C D07-30-3077 2.52 名助約7 4		C 100-100-100-177 F2.52 80000 #	C D07-305-077-F2-52 名紙約7 F402g P77-F2-52 名紙約7 F402g P77-F2-52 名 P77-F2-52 名 P7-F2-52 名 P7-F2-52 名 P7-F2-52 P7-F2-52

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。

	AirStation Settings - Microsoft Internet Exp	orer	_18 ×
QB = 0 · (g) (g) (g) (g) BUFFALD Image: Status (g) (g) (g) (g) BUFFALD Maket = 1 ∪ 5 < (g) £ (l1g) (g) (g) <th>ファイル(E) 編集(E) 表示(y) お気に入り(A) ツー</th> <th>L① ヘルプ密</th> <th></th>	ファイル(E) 編集(E) 表示(y) お気に入り(A) ツー	L① ヘルプ密	
P#2.00 @ P#x7/702.0013/sector/or/preprint-del/del/del/2027/702 BUFFALD Ain Station P Ain Station P VEX.002 VEX.	🔾 戻る • 🕤 - 💽 😦 🐔 🔎 検索 🤹 お死に2	0 🐵 😥 🔓 🕞	
BUFFALD #Material D < 4 (2):21 12 < >>> >>>>>> AllinStation Pro- verset @ (2):22 @ (2):22 >>>>>>>>>>>>>>>>>>>>>>>>>>>>	アドレス(2) 👩 http://1921681.3/cgi-bin/ogi?teg=tfr&id	=19&rand=332297782	 Nation (1) (1) (1) (1) (1) (1) (1) (1) (1) (1)
▲IDStation Pro- ■ 000000000000000000000000000000000000	BUFFALO ###	セキュリティ設定 (11g)	? ヘルブ
□ blask @ ##ft/c/u. □ blask @ #ft/c/u. □ stastanta 000000000000000000000000000000000000	AIDSTALLON Pro	Ф (2014) Структ С 100-000 (2017) ВИС С 110-000 (2017) С 100-000 (2017) С 100-0000 (2017) С 100-0	
	□ BLAS - SUE_C ■ BLAS - SUE_C	P 単有にな C 単式開発的(m) 2013年1000年10月1日日日 SU目着的(AC 見早入7)11日年96((7)11日) C 計 C 計	

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

AirStation Settings - Microsoft	t Internet Explorer	_ 8 2
ファイル(2) 編集(2) 表示(2) お気	起入り(例) ツール(1) ヘルプ(19)	1
🔾 戻る • 🕤 · 💽 😰 🐔 🔑 機	en 🏫 890220 🐵 🎰 📓 🔤	
РРЬДФ 👔 нар//1921681.3/сеньі	in/og/heq=th&id=198/and=198246132	 Nab リンク ×
BUFFALD AirStation Pro top e 02701- VAPK-BP-ARS4654 VI LANGE	70,800 LEEE C ILEEDIS, 1/4/4P C WHY PCR C WHY PCR	
 ▲ SANGEL ▲ SANG	第項の通路化 「日本市中市 「日本 「日本	
▲ 3及F8910 ▲ 9ビータ開始 MACTクセス制限 ▶ 管理設定 ▶ 登録設施	検索設定] AN(設計 F (An)+5 プライバシーセバレータ (使用4.1 ■) ■ ■	
8	1	

図4:無線の認証と暗号化の設定

 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。

AirStation Settings - Microsoft Int	ternet Explorer	_ 8 ×
ファイル(E) 編集(E) 表示(y) お気に入	カ(金) ツール① ヘルプ(金)	1
🔾 戻る • 🕥 - 💽 😦 🐔 🔎 検索	👷 8902A0 🐵 🌛 🕞	
アドレスの 👩 http://1921681.3/cgi+bin/o	g/Treq=tfr&id=19&rand=170426478 💽 🛃 1940	リンク ×
BUFFALD AlipStation Pro ▼ 109 € 027701 Vare-H-ASS(25) ▼ AASS(2) ■ 2012 - 7052 ▼ 2012 - 705 ▼ 2012 - 705 ■	設定が完てしました。再スタートしています。 あと約 打	•

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。

Smart Secure Switch - Microsoft Internet Explorer		
ファイルビ 編集(2) 表示(2) お気に入り(3) ツール(1) ヘルプ(3)		1
🔾 戻る + 🕥 · 💌 😰 🐔 🔎 検索 🤹 約5002入0 🐵 🔝 - 🛬 🗔		
7Kb2@ http://1921681.2/top_index.asp		
7912/2010 (Control 1911/2/10, unknow) FITUAL STATUS	Avora :: ELLONGORDENTI EM-A JAR-OR BOOMING TO COMPANY	2 6 6 6 6 7 2 9 7
Done Done		ana ・)信頼i高みサイト

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

■ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○	7(小空) 編集(E) 表示(E) お気に入り	@ 9-#0 AN7@		4
(arth) = 1022 (ar) 戻る • 〇) - 💽 💽 🏠 🎾 検索 81,200 🖾 http://doi.io/1.0/1.4	2 8902A0 🐵 🔎 🖟 🗔	- 15 1745	112.21
100-12-02 20-15-02 20-15-02 20-15-02 20 20-15-02 20 20-15-02 20 20-15-02 20 20-15-02 20 20-15-02 20 20-15-0 20 20 20 20 20 20 20 20 20 20 20 20 20	UFFALO	SIL65200M		
	Image: A_2-J'\$\end{tabular} -2-J'\$\end{tabular} -2-J'\$\end{tabular} -2-J'\$\end{tabular} -12-J'\$\end{tabular} -332-J'\$\end{tabular} -1-1232 -1-1232 -1-1232 > 1-1232 > 0-05282 > 1-12	調査サーバ (現在サーバ)P. 1932 (1941) 調査ポート 9932 Shared Secret: ●●●●● Tereout: P 29(1-10) 有効時間 P 3/2 P 3/2 ア 3/2 P		

図3:認証サーバ設定

- 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)

PLACED 開催(1) まテハ おぼに3の			-1013
PFL/200 10 http://1921681.2/advance_m	initial	- 🛃 \$54b	150
BUFFALO	LinkUp-1212:3 LinkUp-#1212 LinkUp-1212.Jati LinkDown BSL SERIES		
TOPへ戻る	ポートの設定		
▼ <u>2</u> - <i>t</i> ' gata bit 2 - <i>t</i> ' gata λ ₂ − 5 ∧ 2 - gat b - <i>t</i> ' bit - <i>t</i> - bit - <i>t</i> - bit > <i>t</i> - bit <	1K−+1 2 20 3 4 5 6 7 8 2822 78 0 200 (L60 ♥ (L60		
	4		
		λ ap 😜 🚙 .	0004

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。

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。

 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。

叠 Microsoft 証明書サービス - Microsoft Internet Explorer		_ 8 ×
ファイルモン 編集モン 表示(ジ) お気に入り(金) ツール(① ヘルプ(ピ)		1
Q 展5 • ○ · ≥ 2 🐔 🔑 検索 ☆ 8502A0 🐵 🐊 • 🖟 📨		
PFU2@ antp://19216811/certsrv/certcarc.asp	- 🛃 移動	150 ×
47		1
ancrosore generation of the	45	-
CA 証明書、証明書チェーン、または CRL のダウンロード		_ 1
コンピュータがこの証明機関から発行されている証明書を信頼できるようにするために、 この CA 証明書チェーンをインストールしてください。		
CA 証明書、証明書チェーン、または CRL をダウンロードするために、証明書とエンコード方式を選択してください。		
CA 证明書:		
現在 [CA]		
エンコード方式		
@ DER		
C Base 64		
CA 如明書フェースのパリノロート		
最新の delta CRL のダウンロード		
		_ 1
	the second se	~
	方服 🂕 🏓 🐧	KOPE -

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。

	証明書の	情報
この CA この証明: さい。	ルート証明 書を信頼	明書は信頼されていません。信頼を有効にするには されたルート証明機関のストアにインストールしてくだ
発行	亍先 :	CA
発行	う者:	CA
有	幼期間 2	2007/01/22 から 2012/01/22

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。

明書ストア 証明書ストアは、証明書が保管され。	るシステム上の領域です。
Windows (Z証明書ストアを自動的に)	選択させるか、証明書の場所を指定することができます。
○証明書の種類に基づいて、自	動的に証明書ストアを選択する(U)
◎証明書をすべて次のストア(酒	(置する(P))
証明書ストア:	
	参照(<u>R</u>)_
	< 戻る(B) 次へ(N) > キャン

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。

証明書ストアの選択	? 🔀
使用する証明書ストアを選択してください(の)	
 個人 信頼されたルート証明機関 レジストリ ローカルコンピュータ エンタープライズの信頼 中間証明機関 	*
✓物理ストアを表示する(S) OK	キャンセル

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。

証明書ストア	は、証明書が保管され	るシステム上の	領域です。		
Windows (20)	[明書ストアを自動的に	選択させるか、	証明書の場所を	指定することが	できます。
	の種類に基づいて、自	動的に証明書	ストアを選択する	U)	
⊙証明書	をすべて次のストアに遭	2置する(<u>P</u>)			
訂正日月	書ストア:				
信頼	されたルート証明機関	¥ローカル コンビ	2-9		参照(<u>R</u>)_

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。

(i)	正しくインボートされました。
~	

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。
- [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。

有線用リモートアクセスポリシー(例:LAN)

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

27-462 前199 美術会 A299 ● (26) 王文 (19) [19] ● ● ● (26) - A299 [19] ● (26) = A299 [19] ● ● (26) - A299 [19] ● (26) = A299 [19] ● ● (26) - A299 [19] ● (26) = A299 [19] ● ● (26) - A299 [19] ● (26) = A299 [19] ● ● (26) - A299 [19] ● (26) = A299 [19] ● ● (26) - A299 [19] ● (26) = A299 [19] ● ● (26) - A299 [19] ● (26) = A299 [19] ● ● (26) - A299 [19] ● (26) = A299 [19] ● ● (26) - A299 [19] ● (26) = A299 [19] ● ● (26) - A299 [19] ● (26) = A299 [19] ● ● (26) - A29	タインターネット認証サービス				_8×
4 → 1 ○ □ ▼ 2 □ ▼ 2 541 ■ 1 → 1 □ ▼ 2 → 10 544 1 2 → 1 □ ○ □ → 10 544 1 2 → 1 □ ○ □ → 10 544 1 2 → 1 □ ○ □ → 10 544 1 2 → 1 □ ○ □ → 10 544 1 2 → 1 □ ○ □ → 10 544 1 2 → 1 □ ○ □ → 10 544 1 2 → 1 □ ○ □ → 10 544 1 2 → 1 □ ○ □ → 10 3 3 2 → 1 □ ○ □ → 10 3 3 2 → 1 □ ○ □ ○ □ ○ □ ○ □ 3 3 3 □ □ ○ □ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○	ファイル(E) 操作(A) 表示(V) ヘルナ(E)				
	⇔ → 🗈 🖬 🗙 🖻 🖫 🔮 + +				
	◆ (2)	Fat STAN STAN	1 - 1 - 1 - 2 - 1 - 1 - 2022 + - 1 - 3 - 1 - 2022 + - 1 - 3 - 888 - 4		

図1:リモートアクセスポリシーの選択

 [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。

検結面電台が差たすが	、西小なる名供た地	テレア/ポネ()		
接続要求が両に900 ポリシー条件(<u>C</u>):	0要ののの余叶を指	走ししい/2011。		
NAS-Port-Type か	り次のものと一致: "	ワイヤレス - そ(D他 OR ワイヤレ	ス – IEEE 802. ⁻
•			1	•
追加(D)	編集(<u>E</u>)	削除(<u>R</u>)	1	
接続要求がこのポリシ	シーで指定した条件	を満たした場合	、関連するブロファ	イルが接続に
	(n)			
フロファイルの編集	<u>(P).</u>			
クヘのアクセスを制御	ご個々のアクセス計 します。	可加指定される	にゆぼり、このポリン	ノーカルネットワー
	条件を満たした場合			
接続要求が指定の多	the state of the s			
接続要求が指定の美 C リモート アクセス語	キ可を拒否する(N)			
接続要求が指定のま C リモート アクセス語 ・ リモート アクセス語	キ可を拒否する(N) キ可を与える(<u>G)</u>			

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。

1 ドルコブ ブロブアコルの編集	?
ダイヤルインの制限 IP マルチリンク 認証 暗号化 詳細設定	
この接続に許可する認証方法のチェックボックスをオンにします。	
EAP メゾッド(E)	
✓ Microsoft 暗号化認証パージョン 2 (MS-CHAP v2)②)	
□ パスワードの期限が切れた後、ユーザーがパスワードを変更す	5(<u>C</u>)
厂 Microsoft 暗号化認証 (MS-CHAP)(M)	
📕 パスワードの期限が切れた後、ユーザーがパスワードを変更す	5(<u>G</u>)
□ 暗号化認証 (CHAP)(N)	
□ 暗号化されていない認証 (PAP、SPAP)(U)	
「認証されていないアクセス――	
□ クライアントが認想証方法をネゴシエートせずに接続できるようにする(W)	

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。

AP の種類は表示	されている順序でネゴシエートされます。	
AP の種類化が 発調された EAP ・	PEAP)	上八移動(山)
		下八移動位)

図4:EAP プロバイダの選択

 [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。

¥護された EAP	(PEAP)		上八移動(
			下八移動(

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

 [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。

が作モード(M) ホームモード	
ジネスモードは802.1	
-Cい。 プロファイル	
現在プロファイルはロックされていません。	
	ロック心
プロファイルのエクスボー	~(E)
プロファイルのインポート	Φ
プロファイルの初期化(>
使用するアダプター	
次のネットワークアダプタを使用します。(A)	
無線アダプタ自動選択	
▼ プロファイルを使用して自動的に接続す	3(P)

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。

認証プロファイル名	
	編集任

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)

.P/T)插*首(E)	EAP-PEAP
	EAP-PEAP 💌
クライアント設定	
C Windowsのログイン情報	を使用して認証する₩
C SecureLockKeyを使用す	r5(5)
● 認証開始時にユーザ名	とパスワードを入力する(M)
○ 入力した値を使用する(D
ユーザ名(<u>U</u>)	
バスワード(P)	
┏ ユーザ証明書を使用し	ロダインする回
	[[]]][]]][]]][]]]][]]]]]]]]]]]]]]]]]]]
▼ サーバ証明書の有効化	.₩
┌ 次のサーバに接続する	◎ 「サーハ名ボメインの一部①
1言頼されたルート証明機関	
人下ア されいこ証明書を目	朝時期にはた
詳細設定	
詳細設定 内部認証プロトコル 🛛	MS-CHAP-V2

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-EAPAES(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。

認証情報を入力	してください	
ユーザ名(山)	buffalo	
バスワード(P)	*****	_
[ок	

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。

4ir5tal	tion		0	
umit us	niagan.	現住の旅院仏殿を表示します。	ヘルプ	
	Wireless-	PEAP	1	
	SSID RUSE ALO			
	COLONNALO	5011 F 1		
	アダプタ名	WLI-CB-G54HP		
	ネットワークタイプ	インフラストラクチャモード		
	通信速度	48.0Mbps		
	チャンネル	9 チャンネル		
	セキュリティ	WPA-EAP(AES)		
	IPアドレス	192.168.1.11		
	MACアドレス	00.0D.0B.97.42.DA		
	経過時間	00.00.15		
	一一一電波受信強度			
	平命電波受信強度			

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。

- . 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
- . 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

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 ヘ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。

💁 Microsoft 証明書サービス - Microsoft Internet Explorer	E E 🛛
ファイルビン 編集化)表示(2) お気に入り(8) ツール① ヘルプ(9)	At
🔇 R5 · 🔘 · 🖹 📓 🐔 🔎 H# 📩 8941230 🚱 🎯 🍓 🖼 🍇	
7F0.2(0) (a) http://19216811/certsrv/certigus.asp	🖌 🔁 移動 リンク 🎽
Microsoft 証明書サービス CA	<u>م الم الم الم الم الم الم الم الم الم ال</u>
証明書の要求	
証明書の種類の選択 ユーザー証明書 福見書の選択の詳細設定を送信する。	
創パータが表示されました	 1>9-ネット

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

[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



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。

Microsoft 証明書サービス - Microsoft Internet Explorer	
イルモン 編集モン 表示(の) お気に入り(の) ツール(ロ) ヘルブ(の)	4
) Ro - 💿 - 🖹 📓 🟠 🔎 888 📌 896020 🚱 🎯 🎯 🖓 🖼	
67.00 a) http://192168111/certsrv/certmpn.asp	💌 🔁 移動 リンク
Merosoft 証明書サービス CA	*
2.7ト さわた 経明中	
ノスドールとすめに証明音	
しい証明書は正しくインストールされました。	

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)

キット記録サービス			×
操作(A) 表示(V) ヘルナ(D)			
🖻 🕅 🗙 📽 👒 😵 🔸 🔸			
ネット認証サービス(ローカル)	名前	M. 7	
DIUS クライアント	S LAN	1	
ート アクセスのログ	SWLAN	2	
ート アクセス ポパシー	S Microsoft ルーティングとリモート アクセス サーバー	3	
要求の処理	「愛信かのアクセス サーバーへの接続	-4	
	Contraction in according to the second		

5 - AL 3 00 AD - 42 - 50 000 -

図1:リモートアクセスポリシーの選択

 [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。

ポリシーを件の	2,200,000,00,00,000,000,000,000,000,000	目していたさい。	
ホリジー条件(C): NAS-Port-Type	が次のものと一致: "「	ワイヤレス - その他 OR S	バヤレス - IEEE 802.1
4			,
追加(<u>D</u>)	編集(E)	削除(<u>R</u>)	
1+++	シーで指定した条件	と満たした場合、関連する	ジョファイルが接続に
接続要求からのボ			
接続要求からのボ 適用されます。			
接続要求からのボ 適用されます。 プロファイルの編集	€(<u>P)</u>	7-5740	5 M 5 1 5
接続要求かしのボ 適用されます。 フロファイルの編集 ユーザー プロファイ クへのアクセスを制作	<u>長(P)</u> ルで個々のアクセス許す 卸します。	可が指定されない限り、こ	のポリシーがネットワー
接続要求が、のボ 適用されます。 プロファイルの編集 ユーザープロファイ、 クへのアクセスを制作 接続要求が指定の	E(P)… Lで個々のアクセス許可します。 かくになった場合: シューム シュー	可が指定されない限り、こ	のポリシーがネットワー

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。

	-
『イヤルインの制限 IP マルチリンク 認証 暗号化 詳細設定	
この接続に許可する認証方法のチェックボックスをオンにします。	
[EAP 379862]	
■ Microsoft 暗号化認証パージョン 2 (MS-CHAP v2)(2)	
▶ パスワードの期限が切れた後、ユーザーがパスワードを変更する	(<u>C</u>)
□ Microsoft 暗号化認証 (MS-CHAP)(M)	
┏ パスワードの期限が切れた後、ユーザーがパスワードを変更する	(S)
□ 暗号化認証 (CHAP)(N)	
□ 暗号化されていない認証 (PAP、SPAP)(U)	
一認証されていないアクセス	
□ クライアントが認証方法をネゴシエートせずに接続できるようにする 🖤	
2	

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。

AP の種類(<u>P</u>):	(05.40)		1.5.7620.000
KBBC4V2 EAF	VEAD		上八移動(D) 下八移動(D)

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。

忍証方法:		
スマート カードまたはその他の言 (岩腹された EAP (PEAP) MD5-Challenge	此明書	
MDUFUNANENSE		

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)

スマート カードまたはほか(の証明書のプロパティ	<u>? ×</u>
このサーバーは、接続が完 書を選択してください。	了する前に呼び出し側に識別されます。識別	の証拠として使う証明
証明書の発行先の	buffalo.buffalo2003.local	.
フレンドリ名		
発行者:	CA	
有効期限:	2008/01/22 23:13:01	
	ОК	**ンセル

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

 [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。

オプション	
動作モード(M) ホームモード ビジネスモードは8021	
-7077110	
現在プロファイルはロックされていません	ロック(L)
ー プロファイルのエクスポート	(E)
プロファイルのインポート(Ø I
プロファイルの初期化(E	
使用するアダプター	
次のネットワークアダブタを使用します。(A)	
無線アダプタ自動選択	*
▶ プロファイルを使用して自動的に接続する	5(<u>P</u>)
ОК	キャンセル

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。

MA ユテータス Q 検 索 E プロファイル Citeret Manager プロファイルの作成と鏡紙類位を表示します。 3 プロファイル名	×						UFFALO	BU
))	ブロファイル	<u></u> を表示しま 名	Q 検 索 イルの作成と接続順位 プロファイル:	、 ステータス プロファ・	Station nt Manager	AirS
H)							כ	
)	
								_

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
---------------------	---

ロファイル名(N)	FARETIS
APの種類(F)	
カライア・ト設定	
C Walkington B Cold	
C Windowsoのロシイン信	HEREIRCHU CEZEE 9 ON <u>U</u> U Boot a Constantia a Const
C INTERPLOCKNEY 212H	ペトペンロ・トモナ サチエ (VV) H 3 の (D)
	46/17/2-LEV/19 2000
 ヘノリレルに置き使用する 	۵W
ユーザ名(凹)	buffalo
バスワード(<u>P</u>)	[:
	a second to the second second
▶ ユーリ証明書を実用	して山タインする型)
▶ ユーリ証明書を使用	してロクインする(型)
	してロクインする型
▶ ユーリ証明書を使用	UCU24ンする型 証明書一覧型 がとい
 ✓ ユーリ証明書を使用 ✓ サーバ証明書の有効 「 次のサーバに接続す 	UCU21ンする(型)
▼ ユーリ証明書を使用 ▼ サーバ証明書の有効 「 次のサーバに接続す	CCU21ンする ED Eま一覧 E E E E E E E E E E E E E E E E E E
 ✓ サーバ証明書の有効 ✓ サーバ証明書の有効 □ 次のサーバに接続す 「信頼されたルート証明機能」 	CCロクインする EIII書一覧 EIII書一覧 EIII書一覧 EIIII書一覧 EIIII書一覧 EIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII
 ✓ ユーリ証明書を使用 ✓ サーバ証明書の有効 ○ 次のサーバに接続す 「信頼されたルート証明概 (ストアされた証明書を) 	CCロクインする(型) IIII日書一覧(型) IIII日書一覧(型) IIII日書の表示する(公) IIII日書を表示する(公)
✓ サーバ証明書の有効 「次のサーバに接続す」 信頼されたルート証明機 「ストアされた証明書を	CCロクインする(型) IIIの目書一覧(型) IIIの目書一覧(型) IIIの目書一覧(型) IIIの目書の意味がないの一部(型) IIIの目書を表示する(型)
 ✓ サーバ証明書の有効 □ 次のサーバに接続す 「 次のサーバに接続す 「 (清頼されたルート証明機) 「ストアされた証明書を 「詳細訳定」 	CCロクインする(型) 証明書一覧(型) IIIの目書一覧(型) IIIの目書一覧(型) IIIの目書の意味の一部(型) IIIの目書を表示する(型)
 マ サーバ証明書の有効 一 次のサーバに接続す 「なのサーバに接続す 「信頼されたルート証明機」 「ストアされた証明書を 「詳編訳定 内的認証プロトコル※ 	C(ロクインする(型) IIIの目書一覧(型) IIIの目書一覧(型) IIIの目書一覧(型) IIIの目書の意味では「メインの一部(型) IIIの目書を表示する(型) IIIの目書を表示する(型) IIIの目書を表示する(型) IIIの目書を表示する(型)
 ✓ エーリ証明書の有効 □ 次のサーバに接続す 「次のサーバに接続す 「注頼されたルート証明機 「ストアされた証明書を 「詳細訳定 内部認証プロトコル公 (医名(A) 	CCLD7ノテな(型) 正明書一覧(型) 北(公) な(型) 「 サーバ名はドメインの一部(型) 関(R) 宮自動的に使用.▼] 証明書を表示する(型)

図6:認証プロファイル



図7:ユーザ証明書一覧

OK

キャンセル





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。

ロファイル名心	EAP-TLS
APの種類(E)	EAP-TLS
クライアント設定	
c Windowsのロジイン情	報を使用して認証する(W)
○ SecureLockKeyを使用	973(5)
€ 認証開始時にユーザ	名とパスワードを入力する(M)
◎ 入力した値を使用する	Ð
ユーザ名(U)	buffalo
パスワード(P)	
☑ ユーザ証明書を使用	してログインする(<u>D</u>)
BUFFALO MELCO	証明書一覧型
BUFFALO MELCO ・ サーバ証明書の有効 ・ 次のサーバに接続す (信頼されたルート証明規 「ストアされた証明書を	 証明書一覧① 化 ① る ② 「 サーバ るはドメインの一部 ① 切(B) 道動的に使用.▼ 証明書を表示する ②
BUFFALO MELCO	証明書一覧の 化の るの 「サーバるはボメインの一部の 関(B) 自動的に使用、 EIの用書を表示する(の)
BUFFALO MELCO 「サーパ証明書の有効 「次のサーパに接続す」 「 信頼されたルート証明規制 「ストアされた証明書を 一 ド料明定 内旧明記証プロトコル⊗	正明書一覧の 化 化 ひ ろ の 「 サーバるはドメインの一部 の 男 の 国 明書を表示する の 」 二 二 二 二 二 二 二 二 二

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。

証ブロファイル一覧	
認証プロファイル名	新規①
LMF-1LO	肖·『赤(<u>D</u>)
	編集(<u>E</u>)
	閉じる(<u>C</u>)

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。

			8
ステータス	Q検索	目 フロファイル	
プロファイ	(ルの作成と接続順位を	表示します。	~w7
	ブロファイル名		
追加	国会議策) = 802. 1x
	<u>>₹</u> -93 70774	<u>ステータス Q 検 寮</u> プロファイルの作点と接続裏位を プロファイル名	ステータス Q 検 変 E プロファイル プロファイルの作品と接続単位を表示します。 プロファイル名

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

基本設定			7779	
表示ノ プロファ	ビイコン)選択 イル選択		○ 有線(L)	
プロファ	イル名(12)	Wireless-TLS		
ネットワ	ークタイプ (N)	インフラストラクチャモード		
SSID(<u>S</u>)		BUFFALO200	13	
チャンネ	SNV(C)	自動設定チャ	シネル	*
暗号化力	方式(E)	WPA-EAP A	ES	•
送信卡	$-\Phi$	1		1
暗号牛	- <u>(IO</u>	1		
認証プロ	コファイル(<u>A</u>)	EAP-TLS		-
IT API	IANY拒否設定で	ある(<u>D</u>)		

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。

91 F410F		
94 ID-25-9		
94 #3+7-9	BUFFALD	0
<mark></mark>	Wireless-TLS	
journat Explorer	7分/50 第分/57 第 第 第 第 第 第 第 第 第 第 第 第 第	
	T . Carrier	
	(-Ban	
	-Sya 🍞 Tis-SetulBing	

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