RADIUS サーバ設定ガイド

Net'Attest® EPS編

for the Guaranteed Network

第 2 版

Copyright © 2007,2008, ALAXALA Networks Corporation. All rights reserved.

はじめに

RADIUSサーバ設定ガイドNet’Attest EPS編は、AXシリーズでサポートしている認証機能を用いたシステム構築において、RADIUSサーバに株式会社ソリトンシステムズ Net’Attest EPSを使用する場合の設定方法を示します。

関連資料

・AXシリーズ 認証ソリューションガイド
・AXシリーズ製品マニュアル（http://www.alaxala.com/jp/support/manual/index.html）
・Net’Attest EPS V3.2 管理者ガイド　第１版

本ガイド使用上の注意事項

本資料に記載の内容は、弊社が特定の環境において、基本動作や接続動作を確認したものであり、すべての環境で機能・性能・信頼性を保証するものではありません。弊社製品を用いたシステム構築の一助としていただくためのものとご理解いただけますようお願いいたします。
Windows製品に関する詳細はマイクロソフト株式会社のドキュメント等を参照下さい。

本資料の内容は、改良のため予告なく変更する場合があります。

輸出時の注意

本ガイドを輸出される場合には、外国為替および外国貿易法ならびに米国の輸出管理関連法規などの規制をご確認の上、必要な手続きをお取り下さい。

商標一覧

・Net’Attestは株式会社ソリトンシステムズの登録商標です。
・Ethernetは、米国Xerox Corp.の商品名称です。
・イーサネットは、富士ゼロックス（株）の商品名称です。
・Microsoftは、米国およびその他の国における米国Microsoft Corp.の登録商標です。
・Windowsは、米国およびその他の国における米国Microsoft Corp. の登録商標です。
・そのほかの記載の会社名、製品名は、それぞれの会社の商標もしくは登録商標です。

Copyright © 2007,2008, ALAXALA Networks Corporation. All rights reserved

改訂履歴

版数	rev.	日付	変更内容	変更箇所
初版	ー	2007.11.29	初版発行	ー
第 2 版	ー	2008.4.17	MAC 認証におけるユーザ名、パスワード設定について AX スイッチのバージョン UP に対応しました。 AX1200S(1.3.B), AX2400S(10.6.C), AX3600S(10.6.C)	5.1.1

Copyright © 2007,2008, ALAXALA Networks Corporation. All rights reserved

目次

1. 概要 5

1.1. 概要 5
1.2. 設定例環境 6
1.2.1. 使用機器一覧とAXコンフィグレーション 6
1.2.2. 設定例のネットワーク構成図 7

2. Net'Attest EPSの構成 8

2.1. 準備 8

3. IEEE802.1X認証の設定 9

3.1. Net'Attest EPSの設定 9
3.1.1. RADIUSクライアントの作成 11
3.1.2. ユーザの作成 13
3.1.3. PEAP、TLSの設定 16
3.2. Windows XP / Vistaの設定 17
3.2.1. 証明書作成 17
3.2.2. PEAP設定、認証の確認 25
3.2.3. TLS設定、認証の確認 29

4. Web認証の設定 34

4.1. Net'Attest EPSの設定 34
4.1.1. ユーザの作成 34
4.2. Windows XP/Vistaの設定 34
4.2.1. クライアントの設定 34
4.3. Web認証の確認 35

5. MAC認証の設定 37

5.1. Net'Attest EPSの設定 37
5.1.1. ユーザの作成 37
5.2. MAC認証の確認 39

6. ログイン認証 40

6.1. RADIUS サーバによる認証の設定 40

7. Windows Vista PEAP 設定の際の注意点 41

Copyright © 2007,2008, ALAXALA Networks Corporation. All rights reserved

1. 概要

1.1. 概要

本資料では認証スイッチにAXシリーズ、クライアントコンピュータにWindows XP、Windows Vista、Net’Attest EPS を RADIUS、ユーザデータベースとして下記認証方式を使用したシステムを構築するための設定方法を記載しています。

認証方式

- IEEE802.1X 認証 （PEAP、TLS）
- Web 認証
- MAC 認証
- ログイン認証

使用方法

本資料は、認証方式毎に設定方法を記載しています。目次を参照して構成する認証方式の項目から設定してください。

AX のコンフィグレーションに関して本資料では詳細な説明は記載していません。AX の設定は完了している事を前提にサーバ、クライアントの設定方法を記載しています。各認証方式に関連するコンフィグレーションは AX のマニュアルや認証ソリューションガイド_3 章(認証ネットワークの構築編)を参照してください。

Copyright © 2007,2008, ALAXALA Networks Corporation. All rights reserved

1.2. 設定例環境

1.2.1. 使用機器一覧と AX コンフィグレーション

使用機器一覧

RADIUS：Net'Attest EPS-SX01 Ver3.4.2

Supplicant：Windows XP , Windows Vista Ultimate

Authenticator：AX1230S(Ver1.3.B) / AX2430S(Ver10.6.C)

L3switch：AX3630S（Ver10.6.C）

HUB：EAPOL 透過機能有り

AX コンフィグレーション設定例

AX1230S のコンフィグレーション

```
hostname "AX1230S"
!
vlan 1
   name "VLAN0001"
!
vlan 10 mac-based
!
vlan 20 mac-based
!
vlan 100
!
spanning-tree disable
spanning-tree mode pvst
!
interface fastethernet 0/24
   switchport mode mac-vlan
   switchport mac vlan 30-31
   switchport mac native vlan 100
!
interface gigabitethernet 0/25
   media-type auto
   switchport mode trunk
   switchport trunk allowed vlan 30-31,200
!
interface vlan 1
!
interface vlan 30
   ip address 192.168.30.253 255.255.255.0
!
interface vlan 31
   ip address 192.168.31.253 255.255.255.0
!
interface vlan 100
   ip address 192.168.100.253 255.255.255.0
!
interface vlan 200
   ip address 192.168.200.253 255.255.255.0
!
   ip route 0.0.0.0 0.0.0.0 192.168.200.254
   !
●dot1x vlan dynamic enable
●dot1x vlan dynamic radius-vlan 30-31
●dot1x vlan dynamic reauthentication
   !
●dot1x system-auth-control
   !
▲mac-authentication system-auth-control
▲mac-authentication vlan 30
▲mac-authentication vlan 31
▲mac-authentication interface fastethernet 0/24
▲mac-authentication id-format 1
   !
■web-authentication system-auth-control
■web-authentication vlan 30
■web-authentication vlan 31
   !
   service dhcp vlan 100
   !
   ip dhcp pool "before"
      network 192.168.100.0
      lease 0 0 0 10
   !
★radius-server host 192.168.10.1 key "alaxala"
●aaa authentication dot1x default group radius
◆aaa authentication login default group radius local
▲aaa authentication mac-authentication default group radius
■aaa authentication web-authentication default group radius
   !
★aaa authorization network default group radius
   !
   line vty 0 0
   !
```

●IEEE802.1X 認証を行うためのコンフィグレーション

■Web 認証を行うためのコンフィグレーション

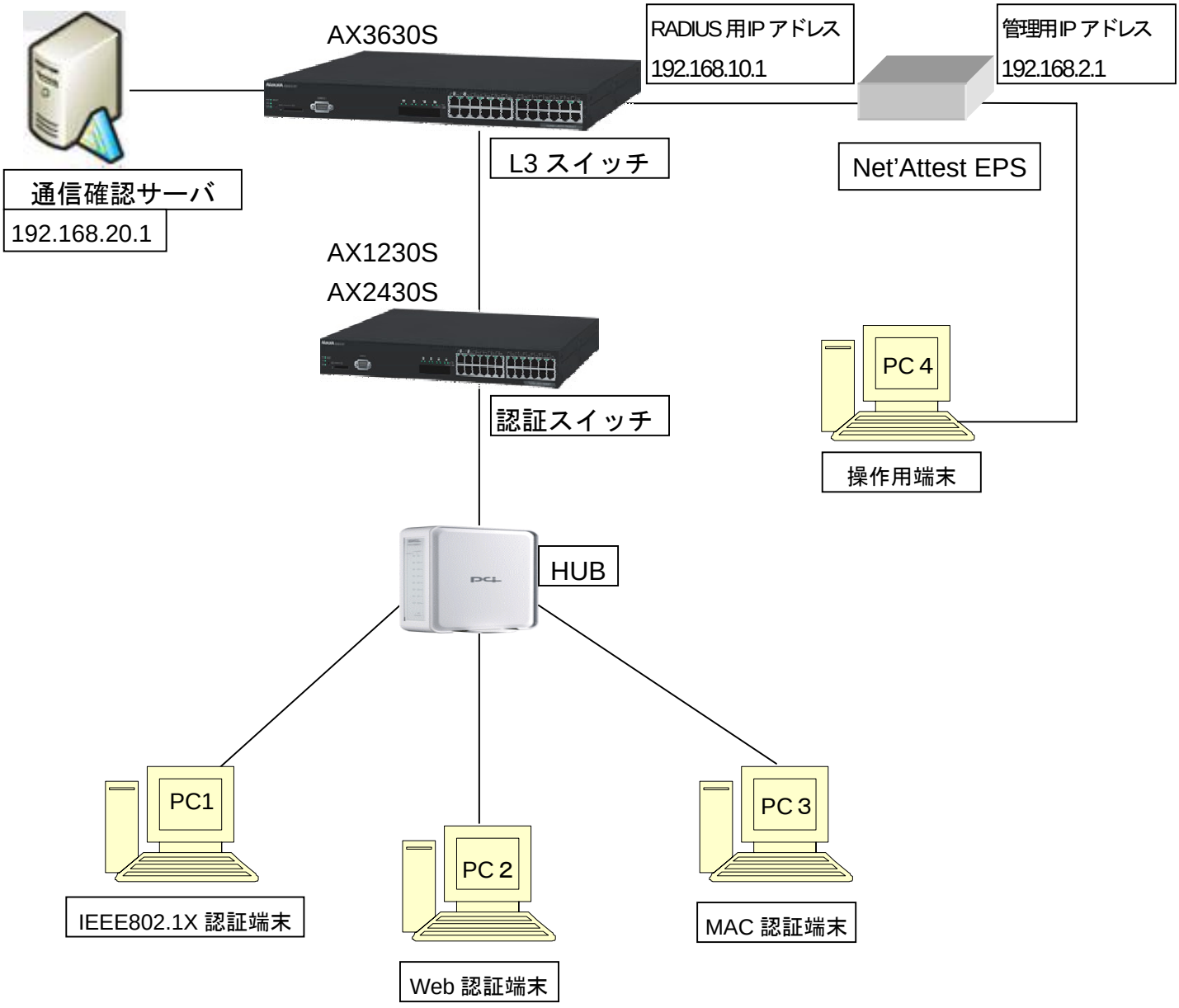
▲MAC 認証を行うためのコンフィグレーション

◆ログイン認証を行うためのコンフィグレーション

★RADIUS サーバ関連のコンフィグレーション（各認証方式共通）

Copyright © 2007,2008, ALAXALA Networks Corporation. All rights reserved

1.2.2. 設定例のネットワーク構成図



※認証する際の構成

ユーザ名：user01・user02

認証後の VLAN：VLAN30、31

Windows XP

Windows Vista

Copyright © 2007,2008, ALAXALA Networks Corporation. All rights reserved

2. Net’Attest EPS の構成

2.1. 準備

①: 電源を入れ、本体後ろのポート２(管理用インタフェース)に LAN ケーブル（クロス）を接続。
操作端末から Web ブラウザを起動し HTTP アクセス「http://192.168.2.1:2181」する。

②Net’Attest EPS V3.2 管理者ガイドに従い、

- タイムゾーンと日付・時刻の設定
- ライセンス情報の設定
- ホスト名の設定
- ベース DN の設定
- 認証用インタフェースの設定
- 管理用インタフェースの設定
- 証明機関の設定
- RADIUS の設定
- RADIUS クライアントの追加
- SNMP 設定（必要な場合のみ）
- NTP 設定（必要な場合のみ）

を設定して下さい。

Copyright © 2007,2008, ALAXALA Networks Corporation. All rights reserved

3. IEEE802.1X 認証の設定

3.1. Net'Attest EPS の設定

①：電源を入れ、本体後ろのポート 2 に LAN ケーブルを接続。

②：ご使用の Web ブラウザを起動し、サーバの IP アドレスにポート番号を加えアクセス。

③：下記画面で管理ツールを選択。

④：ログイン ID を入力。デフォルトは admin。

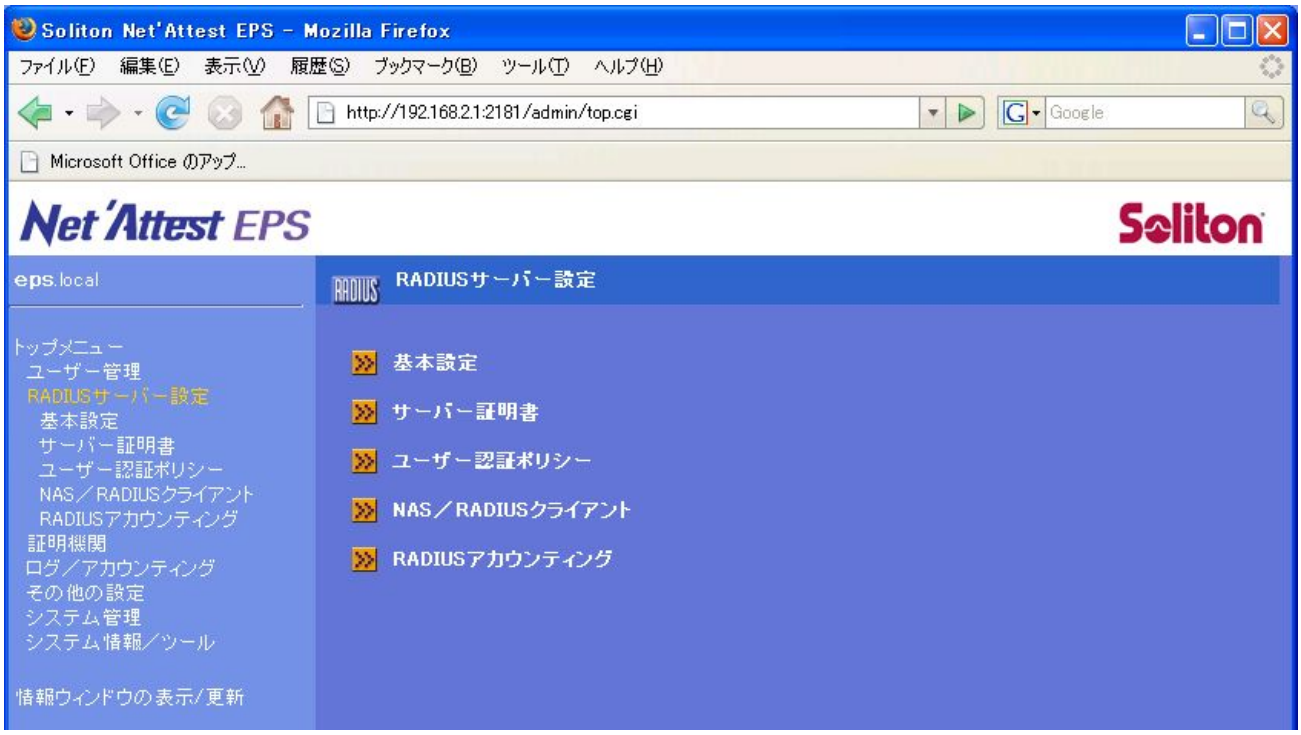
Copyright © 2007,2008, ALAXALA Networks Corporation. All rights reserved

⑤：下記画面が表示されればログイン成功。

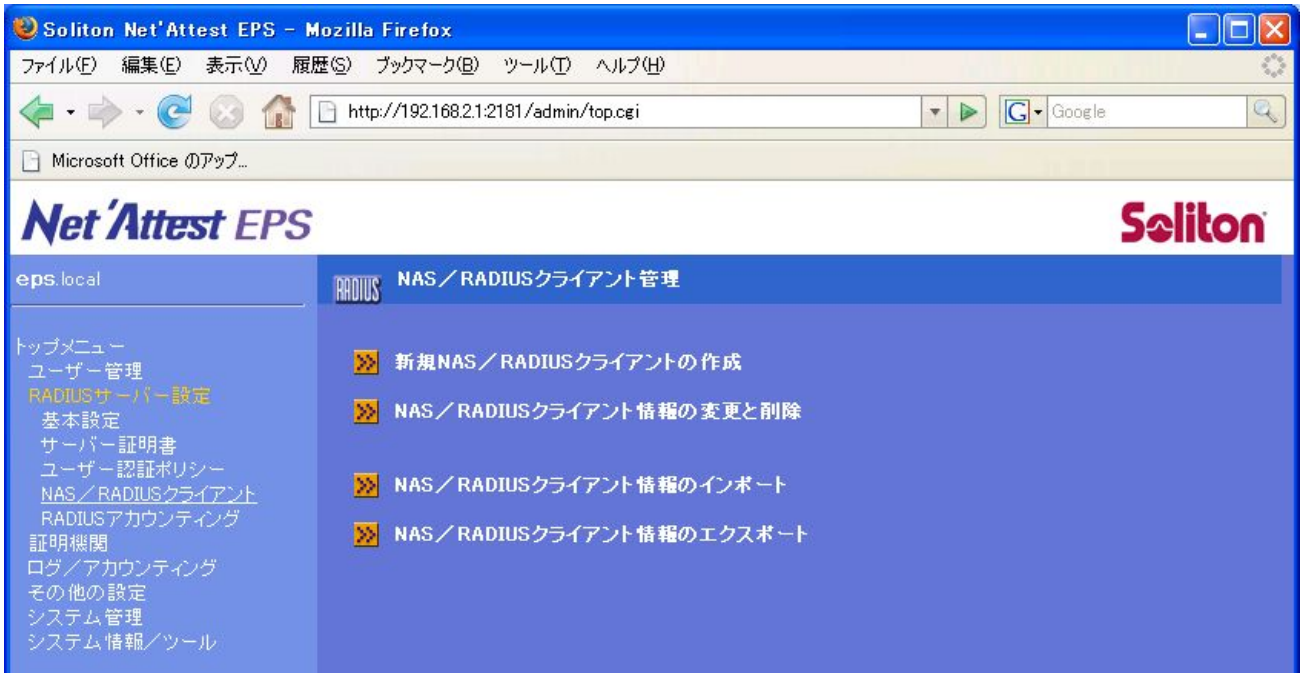
Copyright © 2007,2008, ALAXALA Networks Corporation. All rights reserved

3.1.1. RADIUS クライアントの作成

①：トップメニューから RADIUS サーバ設定を選択。



②：更に新規 NAS／RADIUS クライアントの作成を選択。



Copyright © 2007,2008, ALAXALA Networks Corporation. All rights reserved

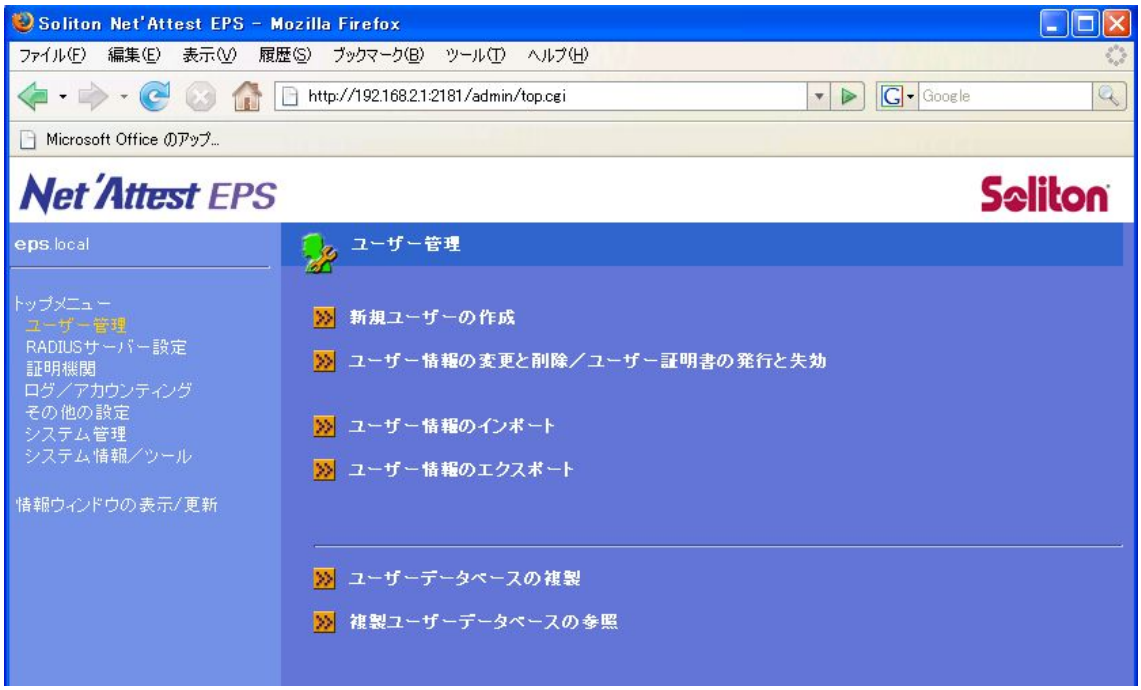
③：認証スイッチの情報（名前、IP アドレス、共有鍵（AX に設定した RADIUS 鍵））を入力し保存。

④：作成後 NAS／RADIUS クライアント一覧に戻り作成されていることを確認。

Copyright © 2007,2008, ALAXALA Networks Corporation. All rights reserved

3.1.2. ユーザの作成

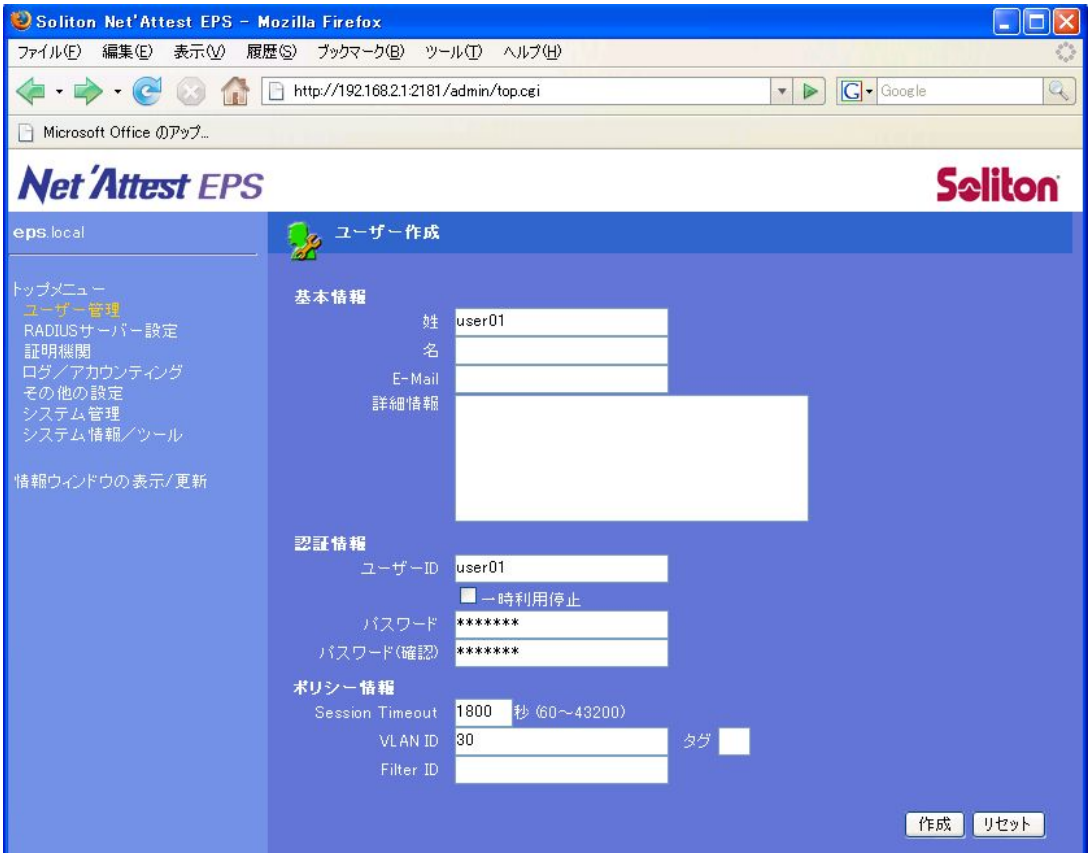
①：トップメニュー → ユーザ管理 → 新規ユーザの作成を選択。



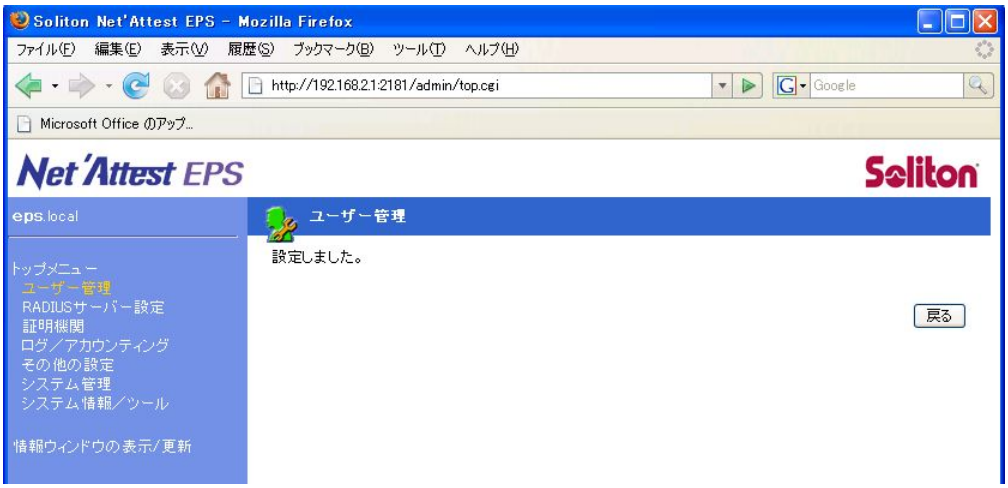
Copyright © 2007,2008, ALAXALA Networks Corporation. All rights reserved

②：ユーザ名、ユーザ ID、パスワード、VLAN ID を入力し、作成ボタンを押す。
　VLAN ID の入力は動的 VLAN 認証の場合のみ入力してください。固定 VLAN モードでは入力してもスイッチ側で無視されます。

　AX6700S,AX6300S,AX3630S,AX2430S の場合、AX のコンフィグレーションに認証済み端末の再認証を行う間隔(dot1x timeout reauth-period, dot1x vlan timeout reauth-period, dot1x vlan dynamic timeout reauth-period)を設定した場合でも、端末再認証時間は RADIUS サーバの設定(Session Timeout)に従います。Net'Attest EPS では本設定は必須項目となっていますので設定値にご注意願います。



③：情報に入力漏れがなければ、以下画面が表示される。



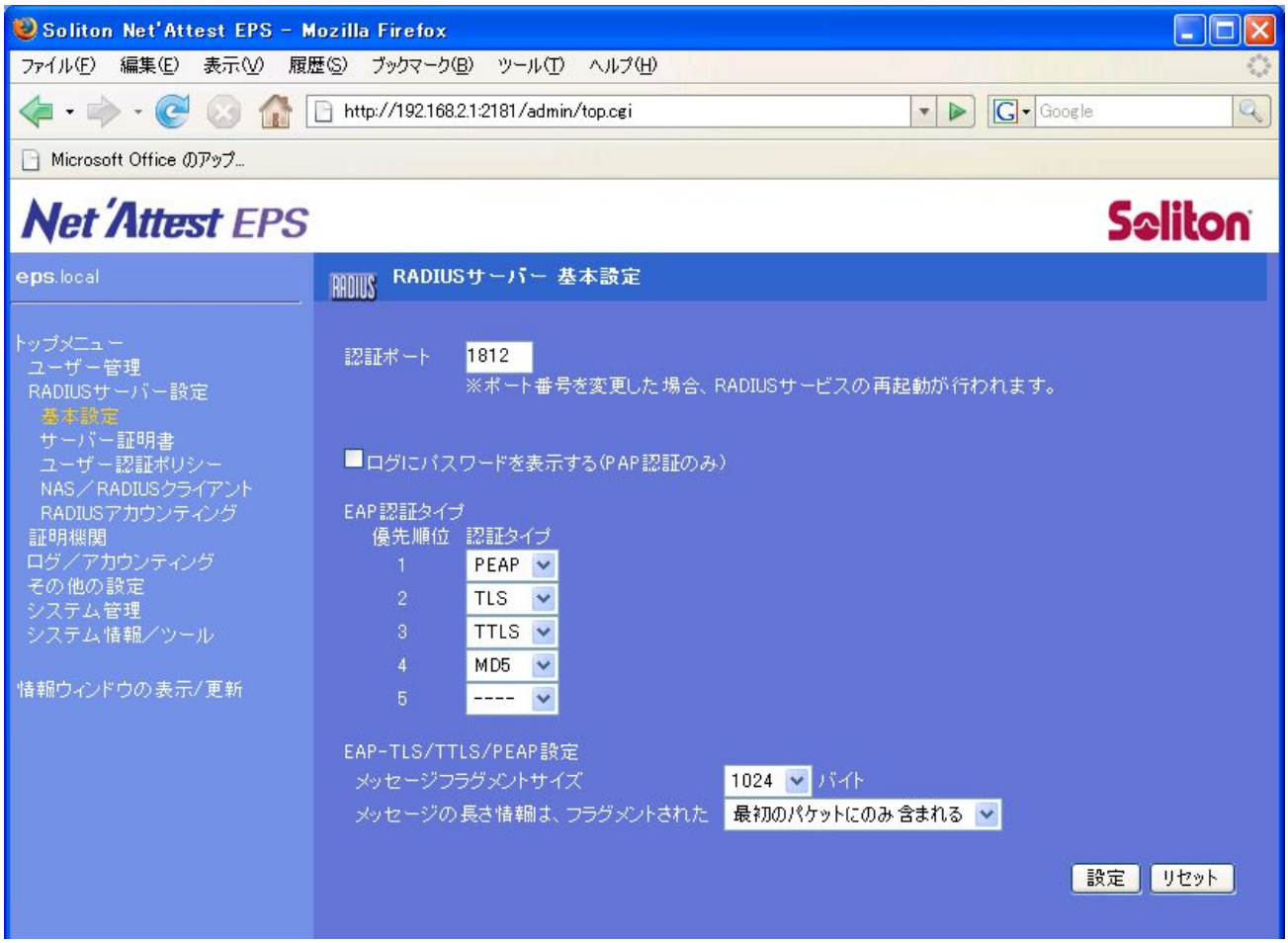
Copyright © 2007,2008, ALAXALA Networks Corporation. All rights reserved

④：戻って作成したユーザがユーザー覧にあることを確認。

Copyright © 2007,2008, ALAXALA Networks Corporation. All rights reserved

3.1.3. PEAP、TLS の設定

①：RADIUS サーバ設定から基本設定を選択。認証ポートの値は AX のコンフィグレーション radius-server host コマンドの auth-port の値を設定。auth-port の設定を省略した場合は、デフォルト値(1812)のままとしてください。プルダウンメニューより使用する EAP 認証タイプを選択し、設定を押す。



Copyright © 2007,2008, ALAXALA Networks Corporation. All rights reserved

3.2. Windows XP / Vista の設定

3.2.1. 証明書作成

3.2.1.1. ユーザ証明書

①：トップメニュー → ユーザ管理 → ユーザ情報の変更と削除／ユーザ証明書の発行と失効を選択する。

②：下記画面で、ダウンロードしたいユーザの証明書のボタンを押す。

③：発行ボタンを押す。

Copyright © 2007,2008, ALAXALA Networks Corporation. All rights reserved

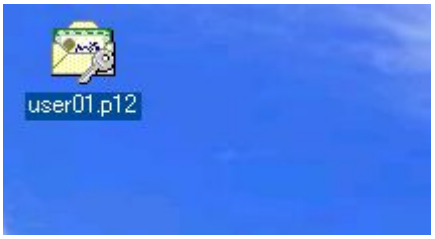
④：必要な情報を入力し、発行ボタンを押す。

⑤：ダウンロードボタンを押して、証明書を保存する。

Copyright © 2007,2008, ALAXALA Networks Corporation. All rights reserved

⑥：ディスクに保存する。

⑦：任意のディレクトリに保存されていることを確認。



Copyright © 2007,2008, ALAXALA Networks Corporation. All rights reserved

3.2.1.2. ルート証明書の作成

①：トップメニュー　→　証明機関の証明書のダウンロードを選択。

②：証明機関の証明書（DER 形式）をダウンロードする。

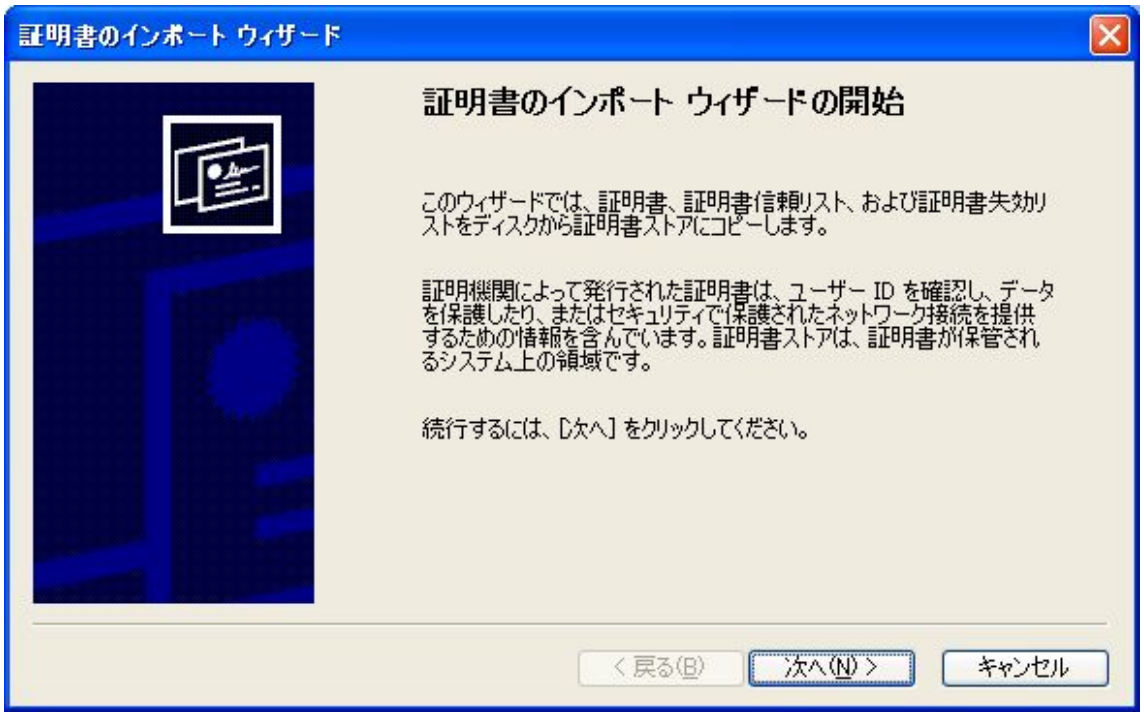
Copyright © 2007,2008, ALAXALA Networks Corporation. All rights reserved

③：ディスクに保存するを選択。

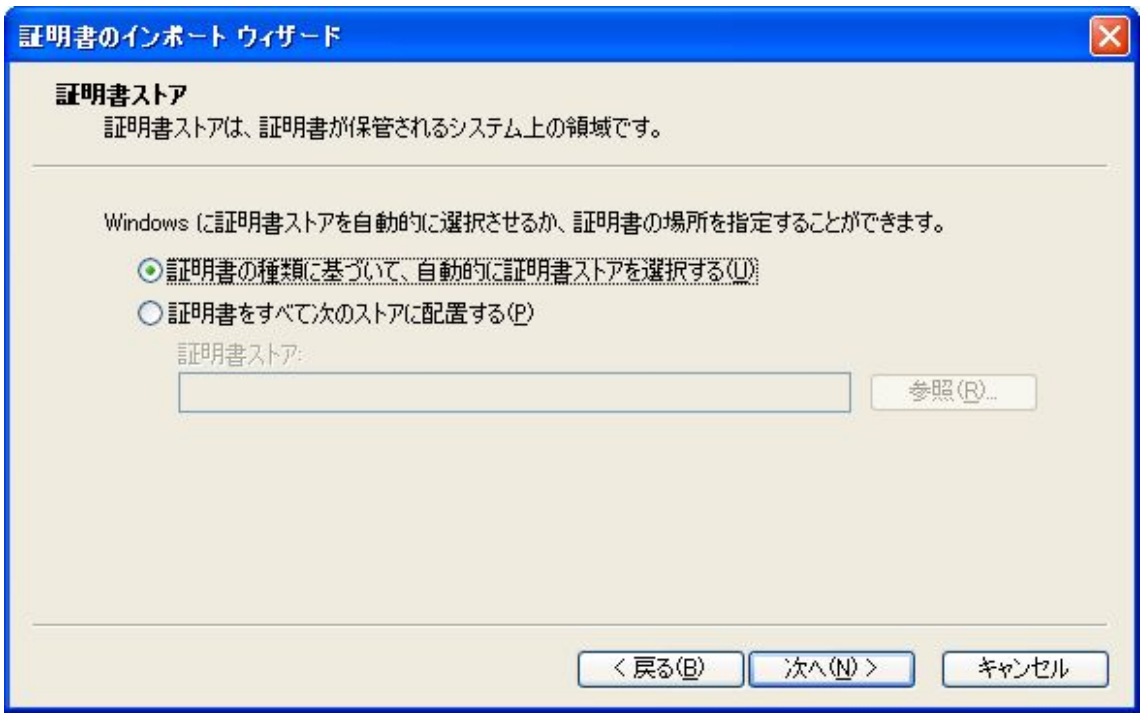
④：任意のディレクトリに保存した証明書をダブルクリックし、インストールの手順を開始。

Copyright © 2007,2008, ALAXALA Networks Corporation. All rights reserved

⑤：次へ。



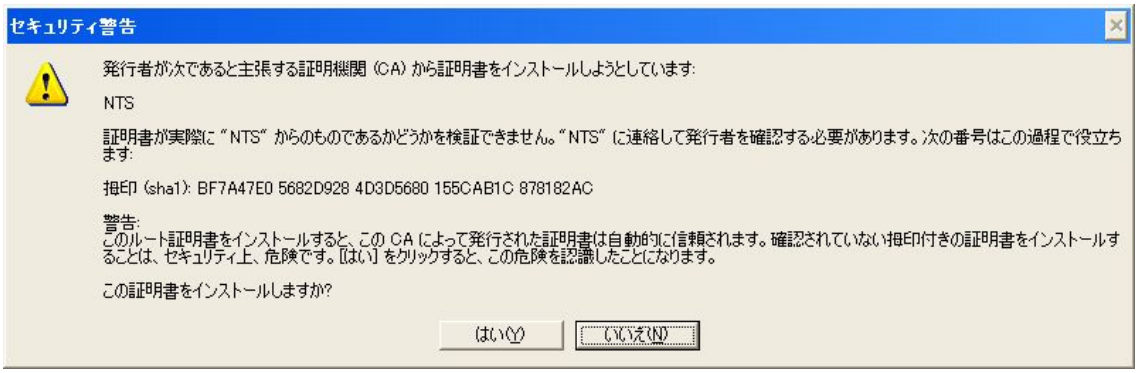
⑥：自動的に適切なストアに振り分けられる。次へ。



Copyright © 2007,2008, ALAXALA Networks Corporation. All rights reserved

⑦：選択した内容を確認する。完了。

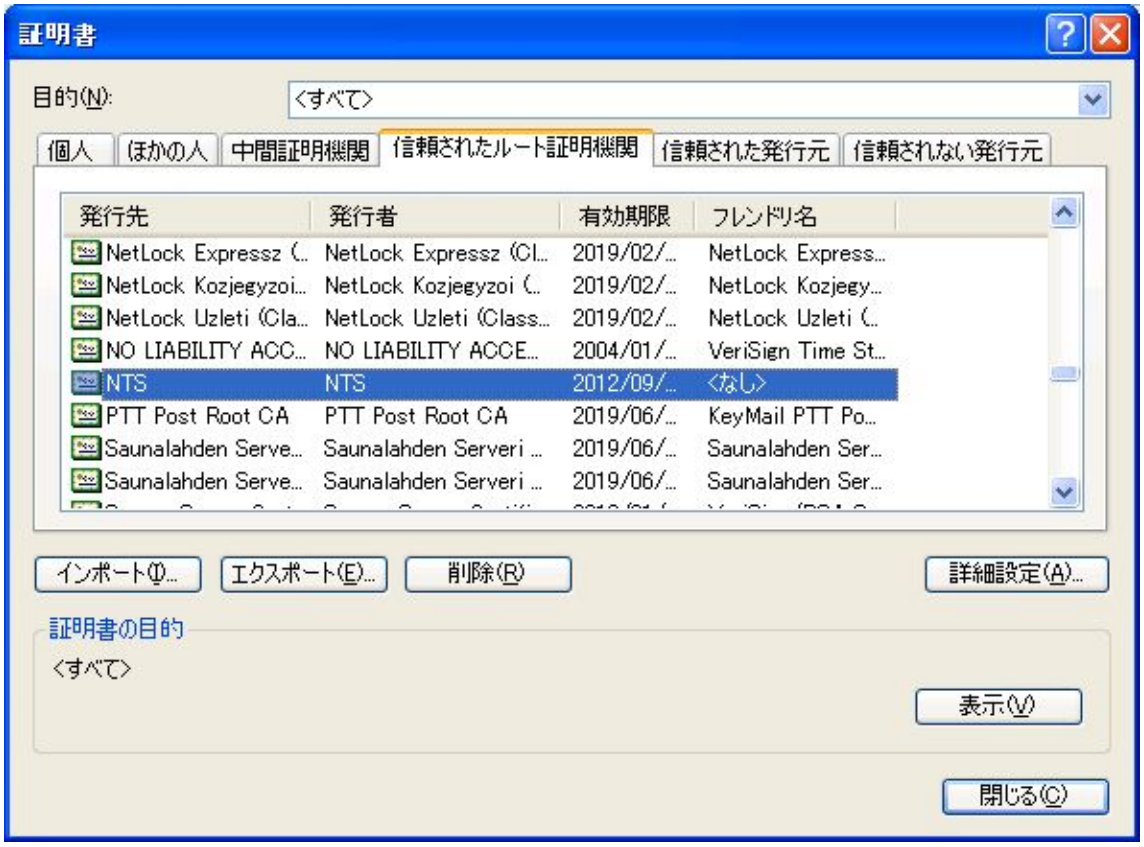
⑧：はいを選択する。



⑨：正しくインポートされました。

Copyright © 2007,2008, ALAXALA Networks Corporation. All rights reserved

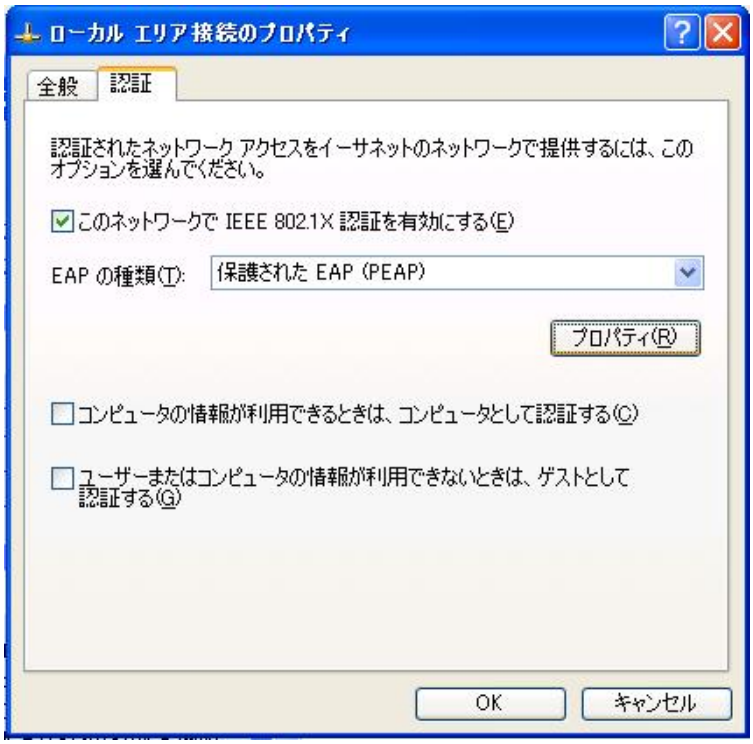
⑩：ルート証明書のストアに正しくインポートされていること確認。



Copyright © 2007,2008, ALAXALA Networks Corporation. All rights reserved

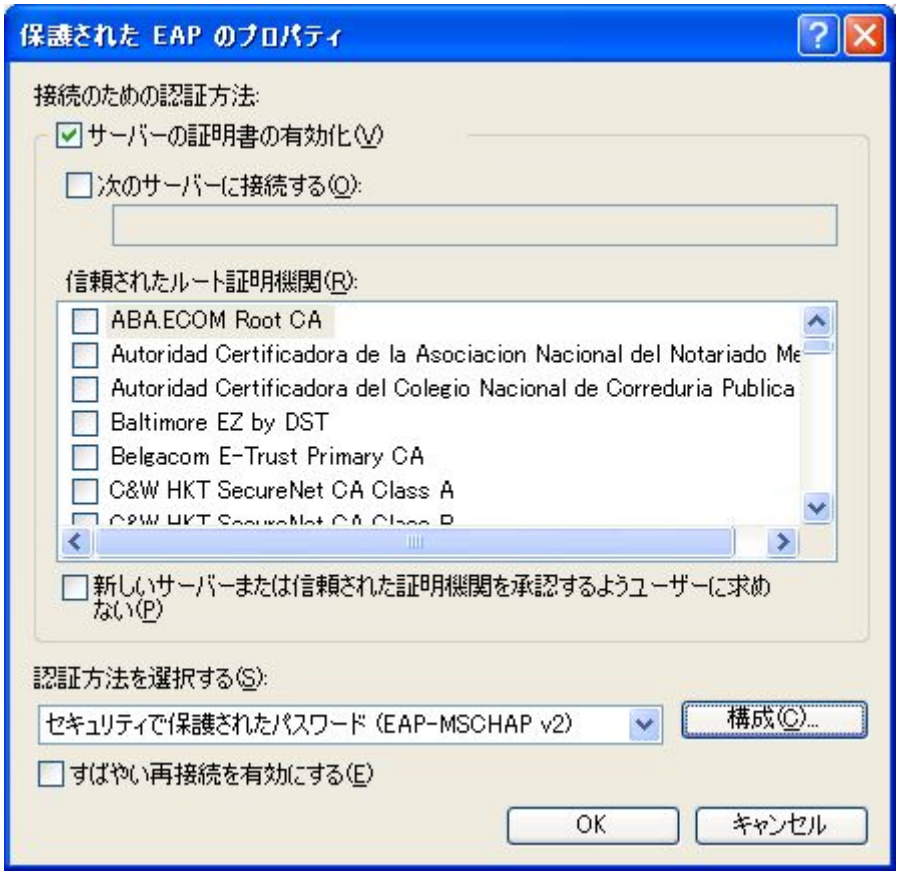
3.2.2. PEAP 設定、認証の確認

①：サプリカントで使用する EAP の設定をする。
スタート→コントロールパネル→ネットワーク接続→該当のローカルエリア接続を
右クリックプロパティ→認証タブを開き、EAP の種類に保護された EAP(PEAP)を選択、
プロパティをクリックする。

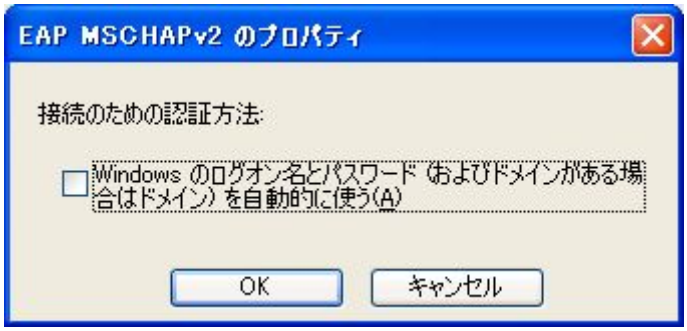


Copyright © 2007,2008, ALAXALA Networks Corporation. All rights reserved

②：下記画面で、セキュリティで保護されたパスワード（EAP-MSCHAPv2）を選択し構成ボタンを押す。



③：EAP MSCHAPv2 のプロパティにて下記のチェックをはずす。
OK を 3 回クリックしローカルエリア接続のプロパティを閉じる



Copyright © 2007,2008, ALAXALA Networks Corporation. All rights reserved

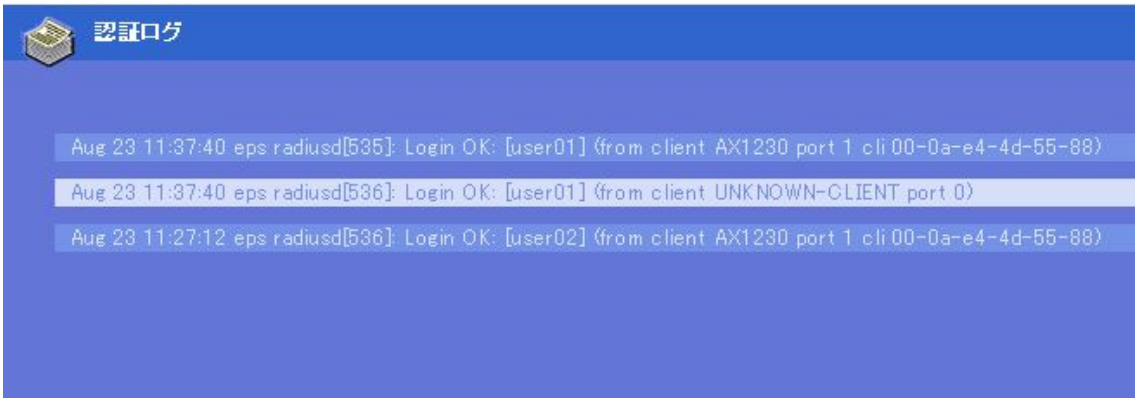
④：PEAP 認証の確認

サプリカントをケーブルに接続すると、資格情報の入力画面が現れる。

正しいユーザ名とパスワードを入力。

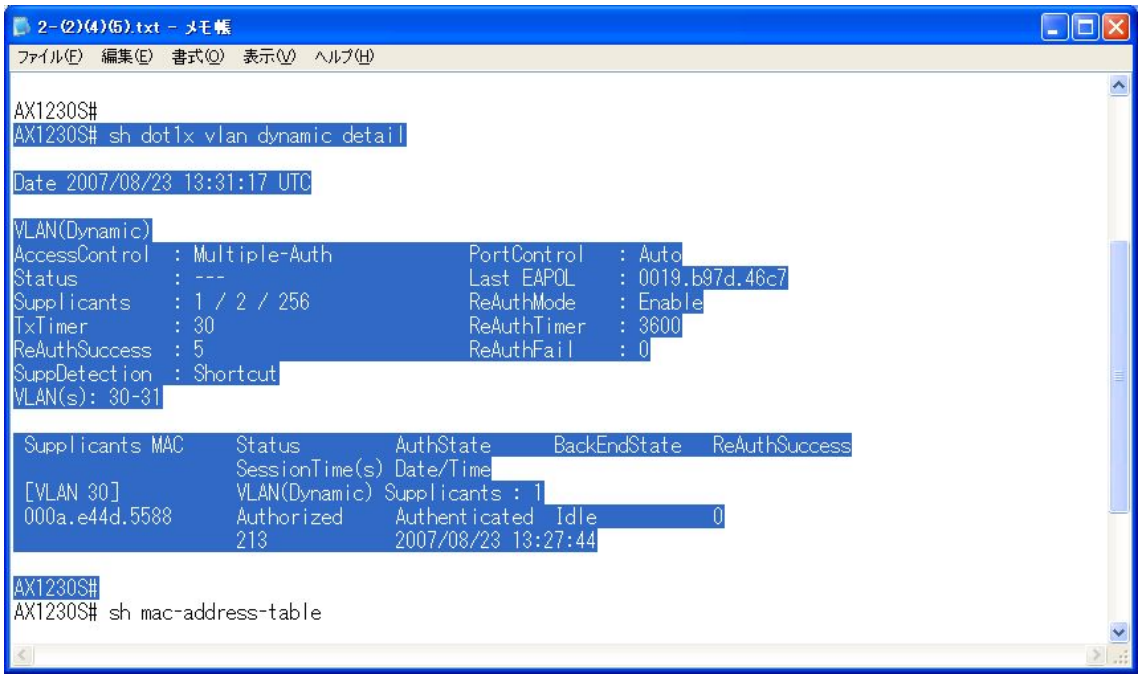
⑤：認証に成功したことを、サーバーログで確認する。

トップメニュー　→　ログ／アカウンティング　→認証ログの表示　を選択。



Copyright © 2007,2008, ALAXALA Networks Corporation. All rights reserved

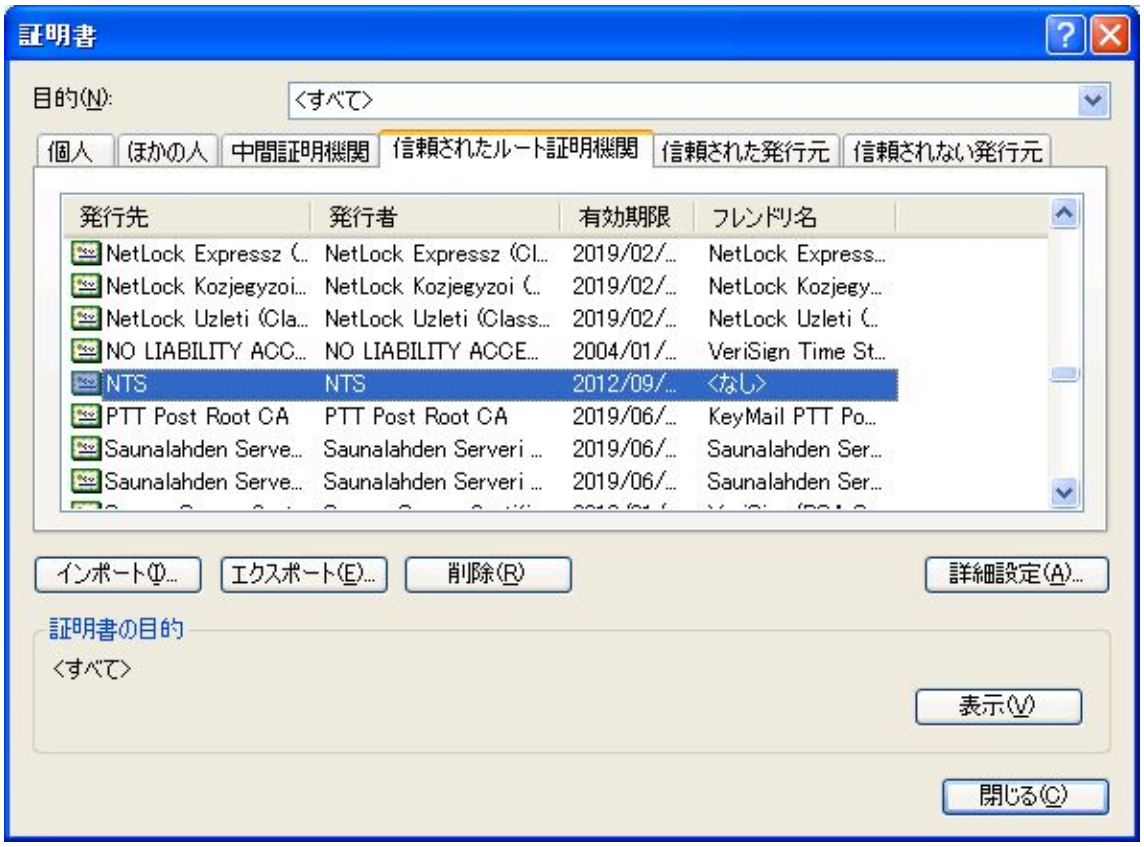
⑥：AX（Authenticator）では show dot1x vlan dynamic detail コマンドにて認証に成功していることを確認。



Copyright © 2007,2008, ALAXALA Networks Corporation. All rights reserved

3.2.3. TLS 設定、認証の確認

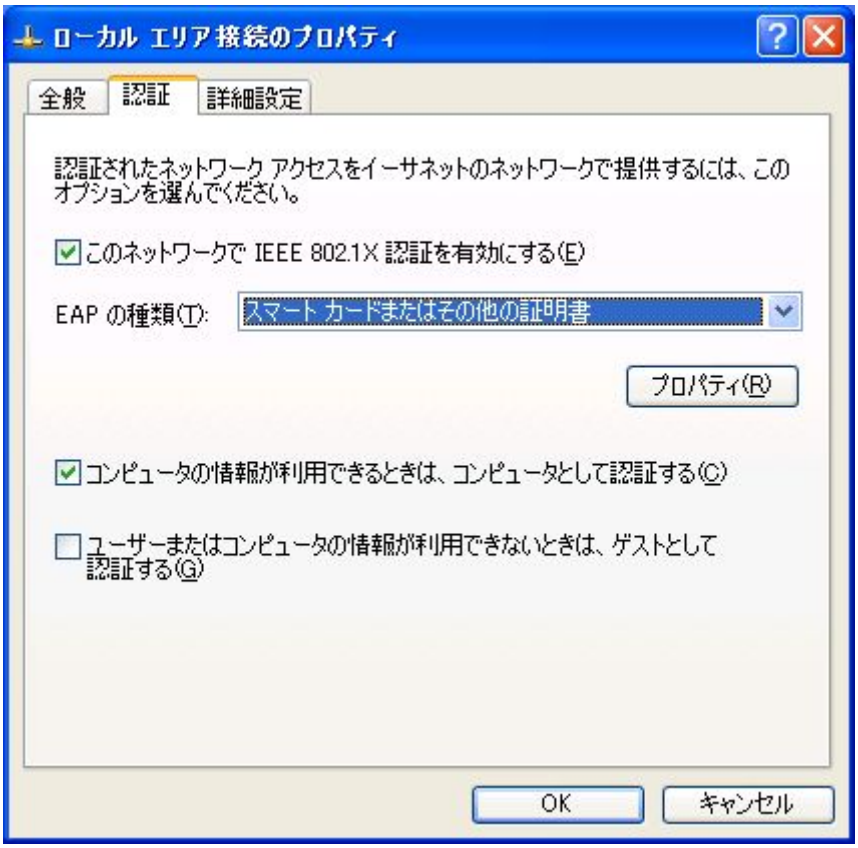
①：ユーザ証明書の確認
スタート→コントロールパネル→インターネットオプション→コンテンツタブ→
証明書→個人タブをクリック。発行者 NTS の証明書を確認する。



Copyright © 2007,2008, ALAXALA Networks Corporation. All rights reserved

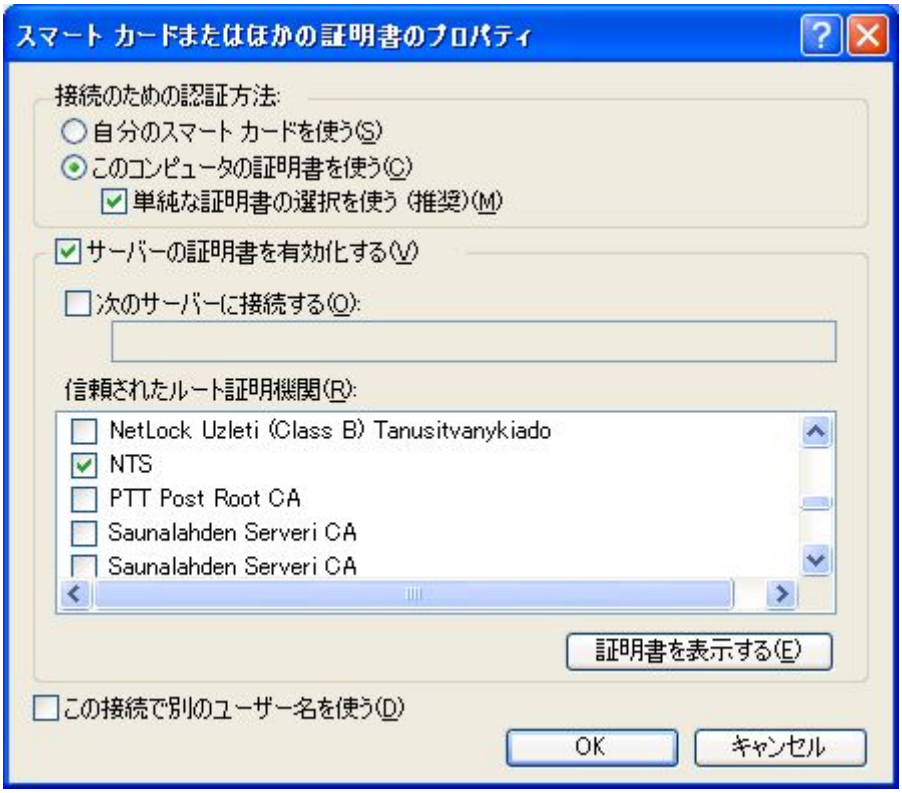
②：サプリカントで使用する EAP の設定をする。

スタート→コントロールパネル→ネットワーク接続→該当のローカルエリア接続を右クリックプロパティ→認証タブを開き、EAP の種類に“スマートカードまたはその他の証明書”を選択、プロパティをクリックする。



Copyright © 2007,2008, ALAXALA Networks Corporation. All rights reserved

③：スマートカードまたはほかの証明書のプロパティにて、接続のための認証方法に“このコンピュータの証明書を使う”を選択。サーバ証明書を有効化するにチェックし信頼されたルート証明機関から NTS をチェックする。OK を 2 回クリックし閉じる。



Copyright © 2007,2008, ALAXALA Networks Corporation. All rights reserved

④TLS 認証の確認

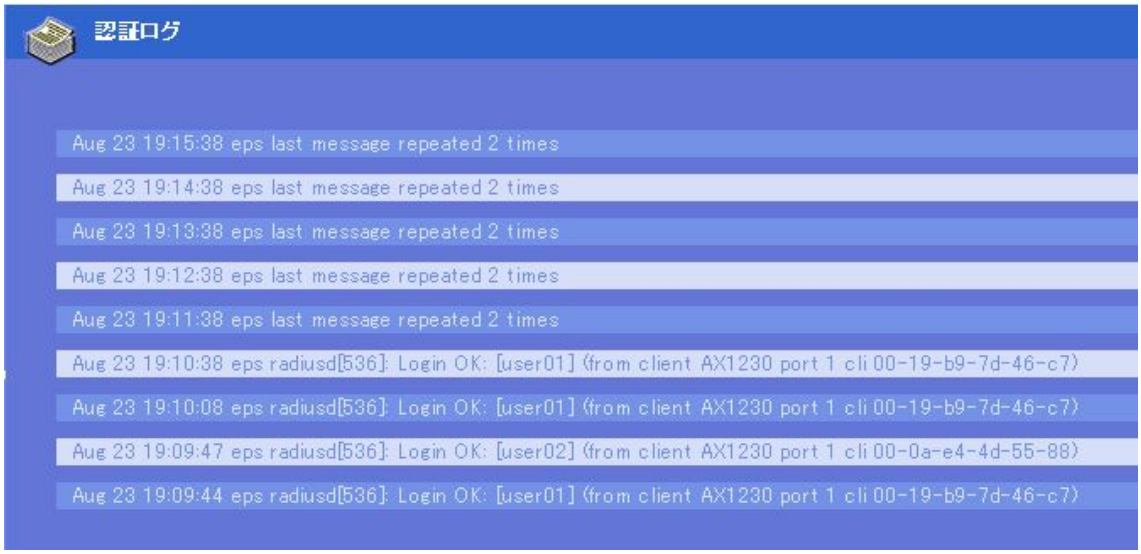
サプリカントをケーブルに接続すると、認証します。

なお、証明書を持つユーザが複数いる場合は、下記に示す画面が出ます。

認証させたいユーザを選択し、OK をクリック。

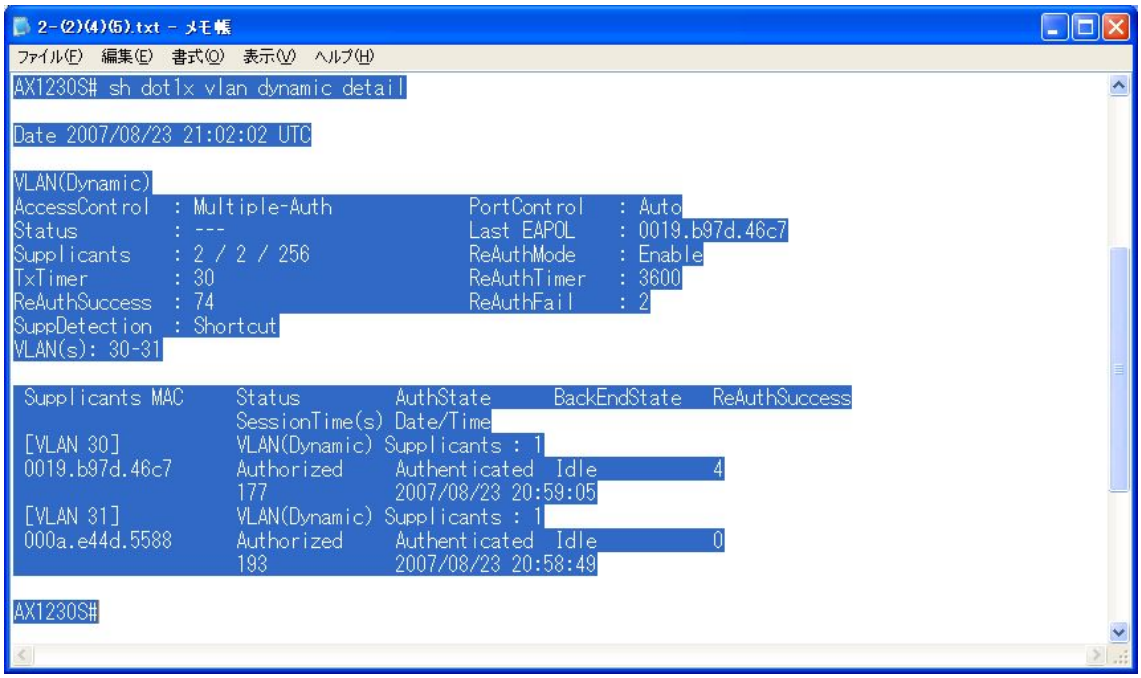
⑤：認証に成功したことを、サーバーログで確認する。

トップメニュー　→　ログ／アカウンティング　→認証ログの表示　を選択。



Copyright © 2007,2008, ALAXALA Networks Corporation. All rights reserved

⑥：AX（Authenticator）では show dot1x vlan dynamic detail コマンドにて、認証に成功していることを確認する。



Copyright © 2007,2008, ALAXALA Networks Corporation. All rights reserved

4. Web 認証の設定

4.1. Net'Attest EPS の設定

Net'Attest EPS の設定は、「**2　IEEE802.1X 認証の設定**」を参照して下さい。

4.1.1. ユーザの作成

①：ユーザの作成は 3.1.2 の手順で、設定画面にアクセス。
Web 認証用にユーザを作る。

4.2. Windows XP/Vista の設定

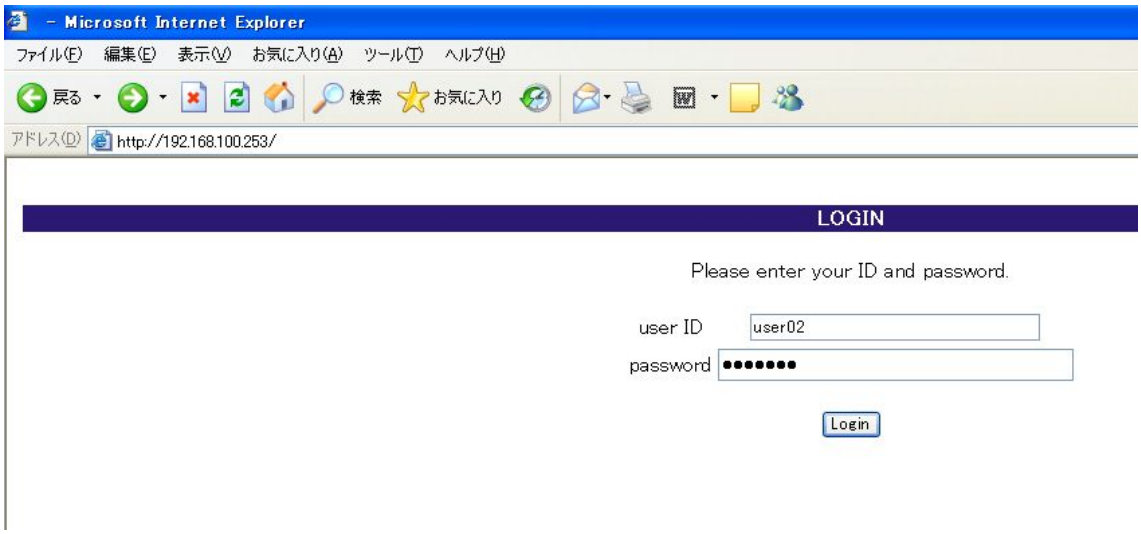
4.2.1. クライアントの設定

①：サプリカントにて、スタート→コントロールパネル→ネットワーク接続→
該当のローカルエリア接続を右クリックプロパティ→認証タブを開くと、一番上にある、
このネットワークで IEEE 802.1X 認証を有効にするにチェックが入っている場合は、チェックを外す。

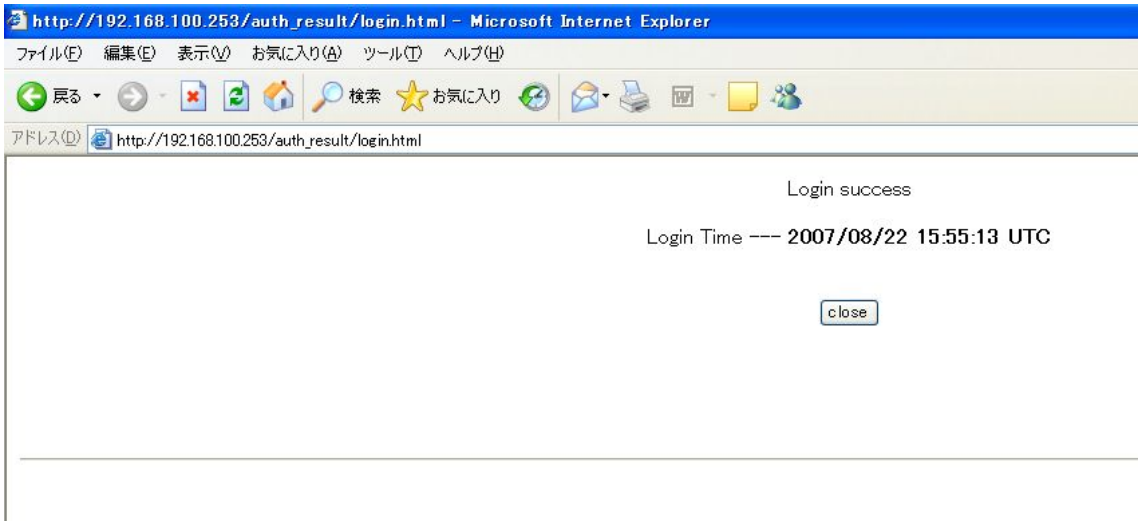
Copyright © 2007,2008, ALAXALA Networks Corporation. All rights reserved

4.3. Web 認証の確認

①：クライアント PC では認証前 VLAN 内で認証スイッチの IP アドレスに HTTP／HTTPS アクセスする。User ID、パスワードを入力し Login をクリックする。



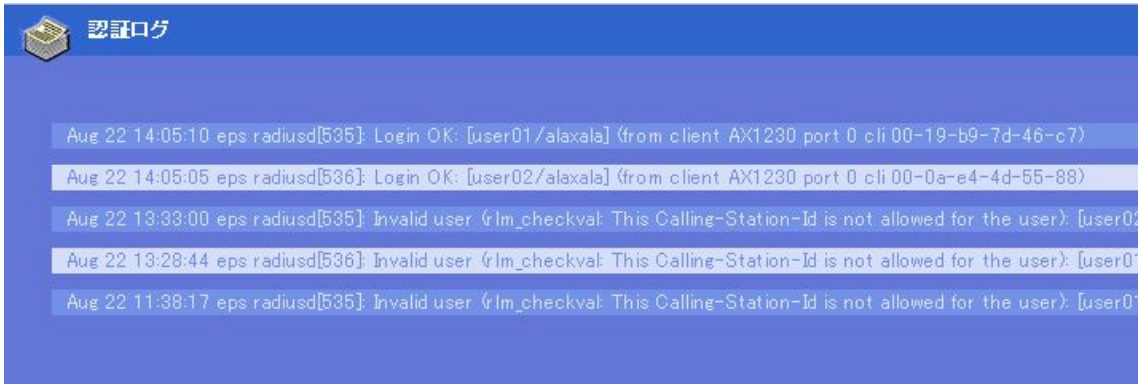
②：“Login success”と認証成功画面が表示される。



Copyright © 2007,2008, ALAXALA Networks Corporation. All rights reserved

③：認証に成功したことを、サーバーログで確認する。

トップメニュー　→　ログ／アカウンティング　→認証ログの表示　を選択。



④：AX（Authenticator）では show web-authentication login コマンドにて、認証に成功していることを確認する。

Copyright © 2007,2008, ALAXALA Networks Corporation. All rights reserved

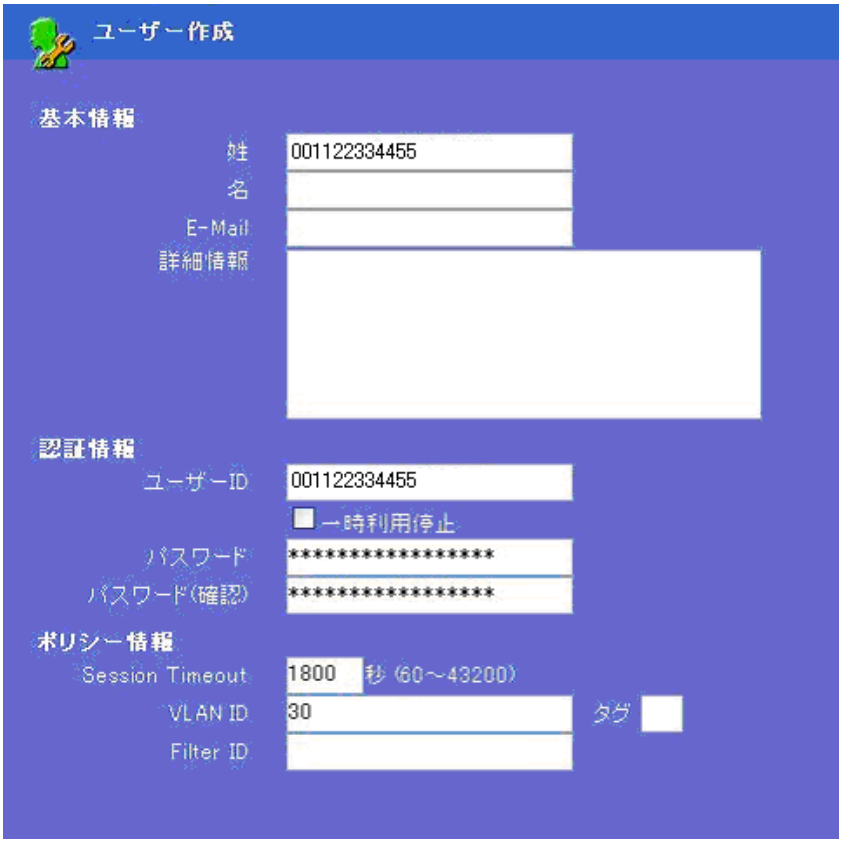
5. MAC 認証の設定

5.1. Net'Attest EPS の設定

Net'Attest EPS の設定は、「**2　IEEE802.1X 認証の設定**」を参照して下さい。

5.1.1. ユーザの作成

①：サーバでのユーザの作成は 3.1.2 の手順を参照して下さい。
ただしユーザ名、パスワードは認証したい端末の MAC アドレスを設定します。
固定 VLAN モードでは VLANID は入力不要です、入力しても無視されます。



②：ユーザ名パスワード入力形式

AX1200S シリーズは初期値の MAC アドレス設定形式はユーザ名とパスワードが **00-11-22-33-44-55** の形式となりますが、コンフィグレーションコマンド（mac-authentication id-format）で **001122334455** や **00:11:22:33:44:55** などの形式及び英字の大文字小文字が変更可能となっています。またパスワードはコンフィグレーションコマンド（mac-authentication password）で装置ごとに統一する事が可能です。省略時はユーザ名と同じフォーマットで MAC アドレスを問い合わせます。

AX2400S,AX3600S シリーズでは MAC アドレスは"-"や":"等の記号を含まない **001122334455** の 16 進数 12 桁（英字は小文字）の形式で登録してください。パスワードはコンフィグレーションコマンド（mac-authentication password）で装置ごとに統一する事が可能です。AX1200S と AX2400S シリーズ

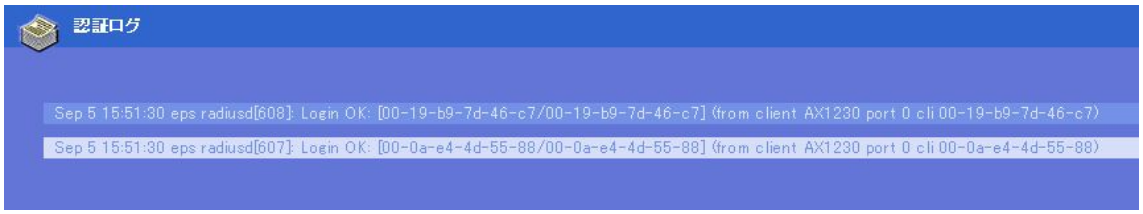
Copyright © 2007,2008, ALAXALA Networks Corporation. All rights reserved

混在環境では AX1200S 側のコンフィグレーションで **001122334455** の 16 進 12 桁（英字は小文字）の形式に統一してください。

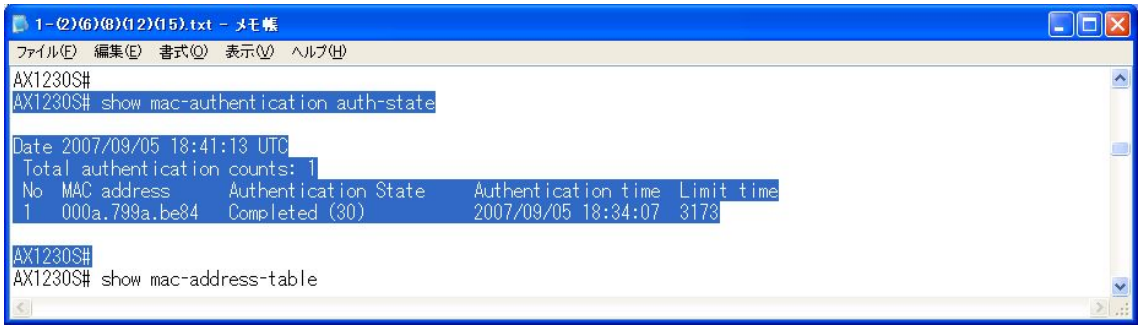
Copyright © 2007,2008, ALAXALA Networks Corporation. All rights reserved

5.2. MAC 認証の確認

①：認証ログにて MAC 認証の確認。



②：AX（Authenticator）では show mac-authentication auth-state コマンドにて認証に成功していることを確認。



Copyright © 2007,2008, ALAXALA Networks Corporation. All rights reserved

6. ログイン認証

6.1. RADIUS サーバによる認証の設定

［設定のポイント］
RADIUS サーバ，およびローカル認証を行う設定例を示します。RADIUS 認証に失敗した場合には，本装置によるローカル認証を行うように設定します。
あらかじめ，通常のリモートアクセスに必要な設定を行っておく必要があります。

［AXでの設定］
①： **(config)# aaa authentication login default group radius local**
使用するログイン認証方式をRADIUS 認証，ローカル認証の順に設定します。

②： **(config)# radius-server host 192.168.10.1 key "alaxala"**
RADIUS 認証に使用するサーバのIP アドレス(192.168.10.1)と共有鍵(alaxala)を設定します。

[Net’Attest EPS での設定]
3.1.2 の手順でログイン認証用のユーザ情報を Net’Attest EPS に登録して下さい。

詳細は、
AX1200S ソフトウェアマニュアル
コンフィグレーションガイド Vol. 1
８　ログインセキュリティと RADIUS
を参照して下さい。

Copyright © 2007,2008, ALAXALA Networks Corporation. All rights reserved

7. Windows Vista PEAP 設定の際の注意点

Windows Vista で PEAP 認証をご使用になる場合は、Net’Attest EPS をご使用の場合は ver3.4.2 以降をお使いください。

Copyright © 2007,2008, ALAXALA Networks Corporation. All rights reserved

2008 年 4 月 17 日　第 2 版発行

アラクサラネットワークス株式会社
ネットワークテクニカルサポート

〒212-0058
川崎市幸区鹿島田 890 番地 新川崎三井ビル西棟