AlaxalA

The Guaranteed Network
いちばん近くで、もっと先へ。

RADIUS サーバー設定ガイド
NetAttest EPS 編

第 3 版

資料 No. NTS-07-R-042

アラクサラネットワークス株式会社

はじめに

RADIUSサーバー設定ガイドNetAttest EPS編は、アラクサラの認証スイッチ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サーバーに株式会社ソリトンシステムズの NetAttest 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/techinfo/manual/index.html）
・NetAttest EPS V4.8 管理者ガイド　第6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

・NetAttest EPSは、株式会社ソリトンシステムズの商標または登録商標です。
・Ethernetは、富士ゼロックス（株）の登録商標です。
・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。

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ー名、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
第 3 版	ー	2017.3.24	・NetAttest EPS の使用バージョンを Ver.4.8 に更新しました。 ・認証クライアント端末の OS、ブラウザを変更しました。 ・付録にマルチステップ認証とダイナミック ACL/QoS の設定例を追加しました。	全面改訂

目次

1. 概要

1.1. 概要

本資料では認証スイッチにアラクサラの AX シリーズ、クライアントコンピュータに Windows 8.1、Windows 10、NetAttest EPS を RADIUS サーバー、ユーザーデータベースとして下記の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

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。

認証スイッチ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。認証スイッチの設定は完了している事を前提にサーバー、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アラクサラの「製品マニュアル」や「認証ソリューションガイド」を参照してください。

1.2. 設定例環境

1.2.1. 使用機器一覧とコンフィグレーション

使用機器一覧

- RADIUS サーバー：NetAttest EPS-ST05-A (Ver.4.8)
- 認証端末：Windows 8.1 , Windows 10
- 認証スイッチ：AX1240S (Ver.2.5) / AX2530S(Ver.4.6)
- L3 スイッチ：AX3640S（Ver.11.14）
- HUB：EAPOL 透過機能有り

コンフィグレーション設定例

AX1240S のコンフィグレーション

```
hostname "AX1240S"
!
vlan 1
   name "VLAN0001"
!
vlan 30
!
vlan 100 mac-based
!
vlan 200 mac-based
!
vlan 1000
!
spanning-tree disable
spanning-tree mode pvst
!
interface fastethernet 0/1
   switchport mode mac-vlan
   switchport mac vlan 100,200
   switchport mac native vlan 30
   ●dot1x port-control auto
   ●dot1x multiple-authentication
   ●dot1x supplicant-detection auto
   ■web-authentication port
   ▲mac-authentication port
   ■authentication ip access-group "auth"
   ■authentication arp-relay
!
～未使用インターフェイスは省略～
!
interface gigabitethernet 0/25
   media-type auto
   switchport mode trunk
   switchport trunk allowed vlan 30,100,200,1000
!
interface vlan 1
!
interface vlan 30
   ip address 192.168.30.12 255.255.255.0
!
interface vlan 100
   ip address 192.168.100.12 255.255.255.0
!
interface vlan 200
   ip address 192.168.200.12 255.255.255.0
!
interface vlan 1000
   ip address 172.16.0.12 255.255.255.0
!
ip route 0.0.0.0 0.0.0.0 172.16.0.254
!
■ip access-list extended "auth"
   ■10 permit udp any any eq bootps
   ■20 permit udp any any eq bootpc
   ■30 permit udp any host 192.168.1.2 eq domain
!
●dot1x system-auth-control
!
▲mac-authentication system-auth-control
▲mac-authentication id-format 1
▲mac-authentication password "alaxala"
!
■web-authentication system-auth-control
■web-authentication ip address 1.1.1.1
!
■service dhcp vlan 30
■ip dhcp pool "V30"
   ■network 192.168.30.0/24
   ■lease 0 0 0 10
   ■default-router 192.168.30.254
!
★radius-server host 192.168.1.2 key "alaxala"
★radius-server dead-interval 0
!
●aaa authentication dot1x default group radius
!
▲aaa authentication mac-authentication default group radius
!
■aaa authentication web-authentication default group radius
```

●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

★RADIUS サーバー関連のコンフィグレーション（各認証方式共通）

※上記コンフィグレーションは AX1240S の設定コンフィグです。同等の設定を AX2530S に定義する場合は関連資料の「認証ソリューションガイド」を参照して下さい。

1.2.2. 設定例のネットワーク構成図

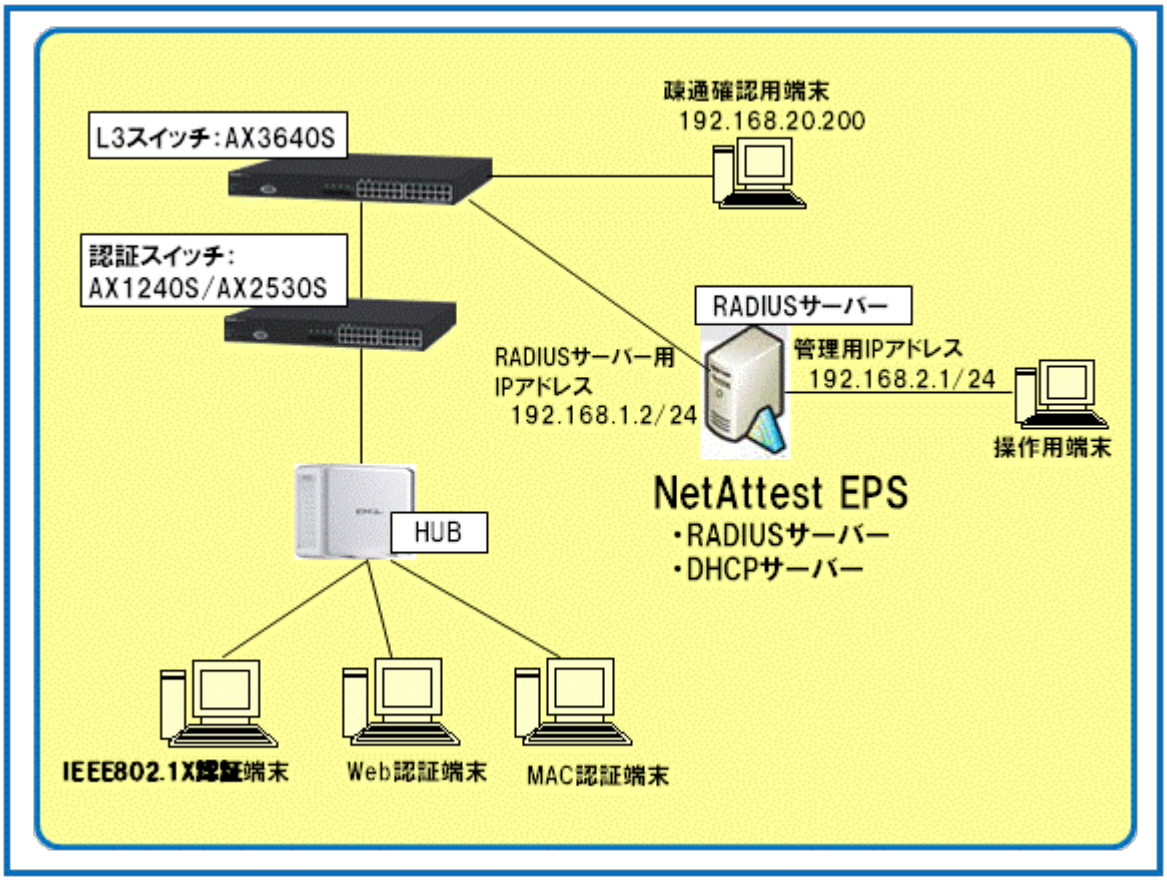


図 1.2-1 構成図

アラクサラの認証スイッチでは、MAC VLAN を使用した動的な VLAN 切り替えを構成しています。認証に成功した端末は、RADIUS サーバーからの VLAN 情報（MAC VLAN の VLAN ID）に従い、動的に VLAN の切り替えを行います。

設定例では、ユーザーID に付属させる各情報について以下のように設定します。認証方式によって認証後に所属させる VLAN を分けています。VLAN ID や認証方式による所属 VLAN の振り分けはネットワーク構成に沿って変更してください。

表 1.2-1 各認証方式のユーザー情報

認証方式	ユーザーID	認証前に所属する VLAN	認証後に所属する VLAN
IEEE802.1X 認証	user01	30	100
Web 認証	user02	30	200
MAC 認証	[MAC アドレス]	30	200

2. NetAttest EPS の初期設定

NetAttest EPS の初期設定を以下の順序でおこないます。なお NetAttest EPS の初期設定は、各認証方式で共通の設定のため、1 回設定すれば再度設定する必要はありません。

2.1. 準備

① 電源スイッチを ON にして、電源投入後 本体の電源 LED が点灯していることを確認します。
② 数十秒後、本体の LCD コンソールパネルに「NetAttest EPS Starting up…」と表示され、起動が完了すると、本体前面の LCD コンソールパネルに「NetAttest EPS System Ready.」と表示されます。
③ 操作用端末を準備し、管理用インタフェース(LAN2)に LAN ケーブルを接続します。
※ 工場出荷時設定では、管理インターフェイス(LAN2)のIP アドレスは、「192.168.2.1/24」に設定されています。セットアップのため、操作用端末にはこのアドレスにアクセス可能なIP アドレスを設定し、管理ネットワークに接続してください。(例：192.168.2.201/24)

2.2. システム初期設定

ホスト名やネットワークの設定など、初回セットアップ時の必須項目の設定を行います。

① 操作端末から Web ブラウザ(Internet Explorer)を起動し、NetAttest EPS の管理 IP アドレスにポート番号を加えアクセス(`http://192.168.2.1:2181/`)し、「初期設定ウィザード」－「システム初期設定」をクリックします。

② ID、パスワードを入力して、ログオンします。
(デフォルト設定　　アカウント,パスワード：`admin`)

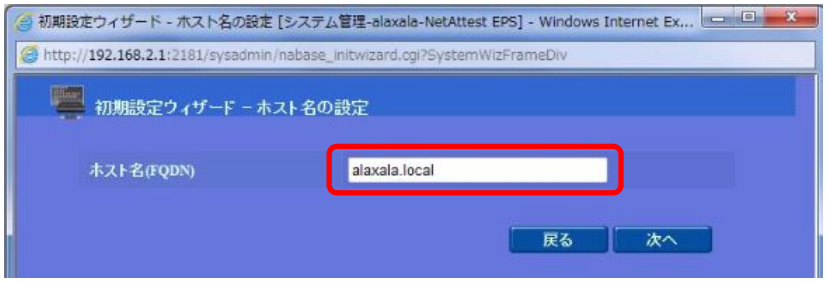
③ <次へ>ボタンをクイックして、システム初期設定をおこないます。システム初期設定ウィザードでは、ホスト名やネットワークの設定など、初回セットアップ時の設定をおこないます。本内容は必要に応じて設定してください。

＜設定内容＞

- タイムゾーンと日付・時刻の設定
- 管理者アカウントの設定
- ホスト名の設定
- インタフェースの設定
- ドメインネームサーバーの設定
- ライセンスの設定

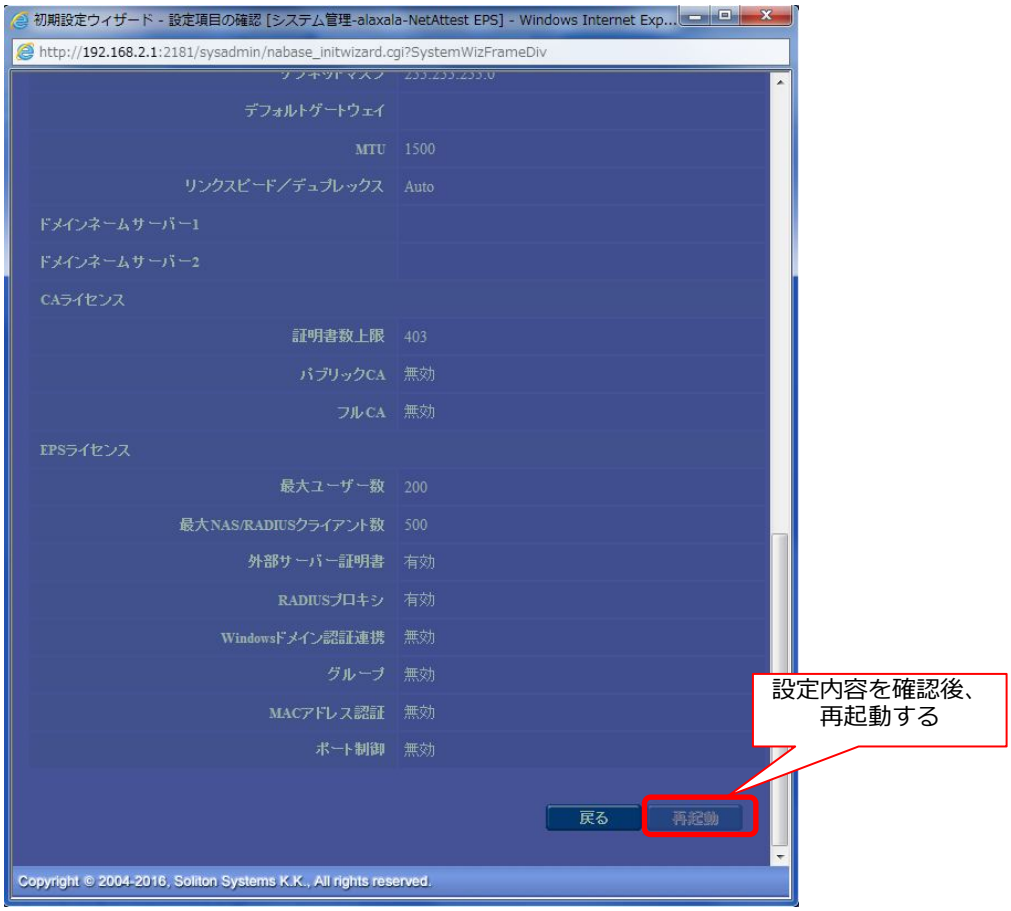
内容の詳細については、「NetAttest EPS V4.8 管理者ガイド」を参照ください。
本例では、「ホスト名の設定」と「インタフェース(LAN1)の設定」の設定を変更／追加しています。ここでは、その変更箇所のみ説明します。

- ホスト名(FQDN)の設定をします。



- レイヤ 3 での中継をするため、 サービスインタフェースの設定の「編集対象 : LAN1」の[デフォルトゲートウェイ]を設定します。

④ 設定を保存・反映するには、設定項目の確認画面で、「再起動」ボタンをクリックしてください。



2.3. サービス初期設定

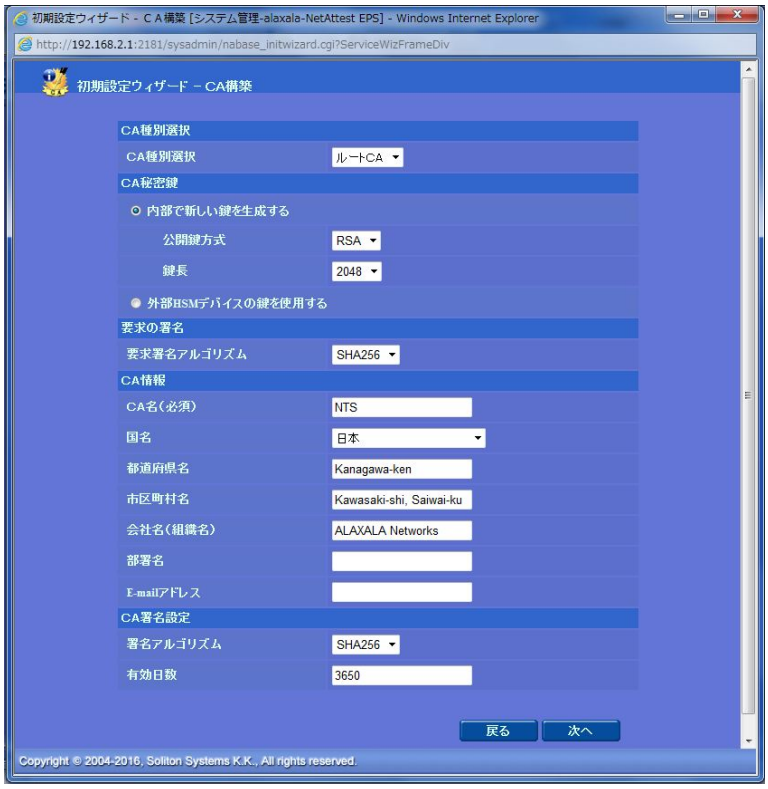
サービス初期設定ウィザードでは、証明機関の構築、ローカルLDAP データベースの構築、RADIUS サーバーの設定など、ローカルLDAPデータベースのユーザー情報によるRADIUS 認証をおこなうための必須項目を設定します。

「初期設定ウィザードー設定項目の確認」ページで<再起動>ボタンをクリックしてシステムを再起動すると、再起動後の管理ページへのリンクが表示されます。このリンクをクリックすると「サービス初期設定」の最初のページが表示されます。<次へ>ボタンをクリックしてサービス初期設定ウィザードを開始してください。

(1) CA構築とサーバー証明書のセットアップ

① CA種別選択：＜ルートCA＞、CA秘密鍵、およびCA情報を設定して、<次へ>ボタンをクリックします。

※本資料の設定例は「ルートCA として構築／サーバー証明書は自身のCA で発行」のパターンの一例となります



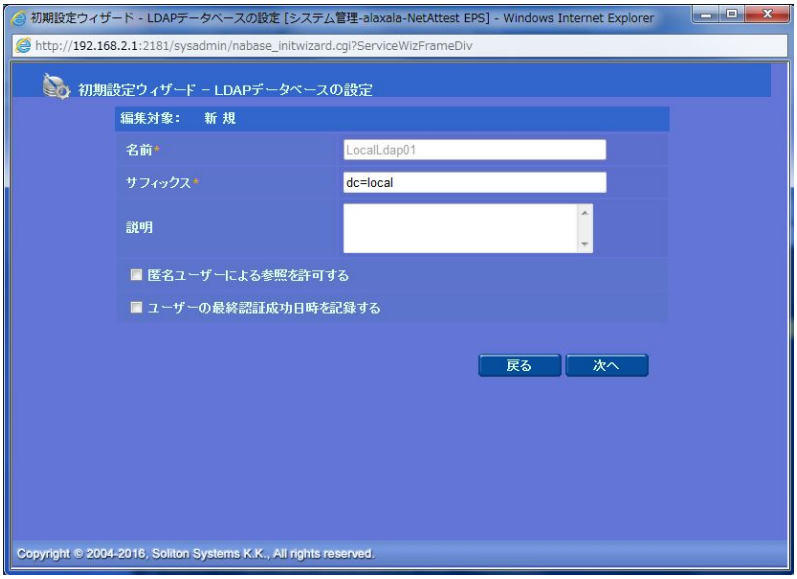
② CA情報が正常に終了すると「CA情報」ページが表示されるので、内容を確認後 <次へ>ボタンをクリックします。

③「サーバー証明書発行」で[このCAでサーバー証明書を自動発行する]を選択し、[署名アルゴリズム][有効日数]を指定します。さらに「鍵パラメータ」では サーバー証明書の[公開鍵方式]と[鍵長]を指定して、<次へ>ボタンをクリックします。

※ CA 構築とサーバー証明書のセットアップについては、別途「NetAttest EPS V4.8 管理者ガイド」を参照してください。

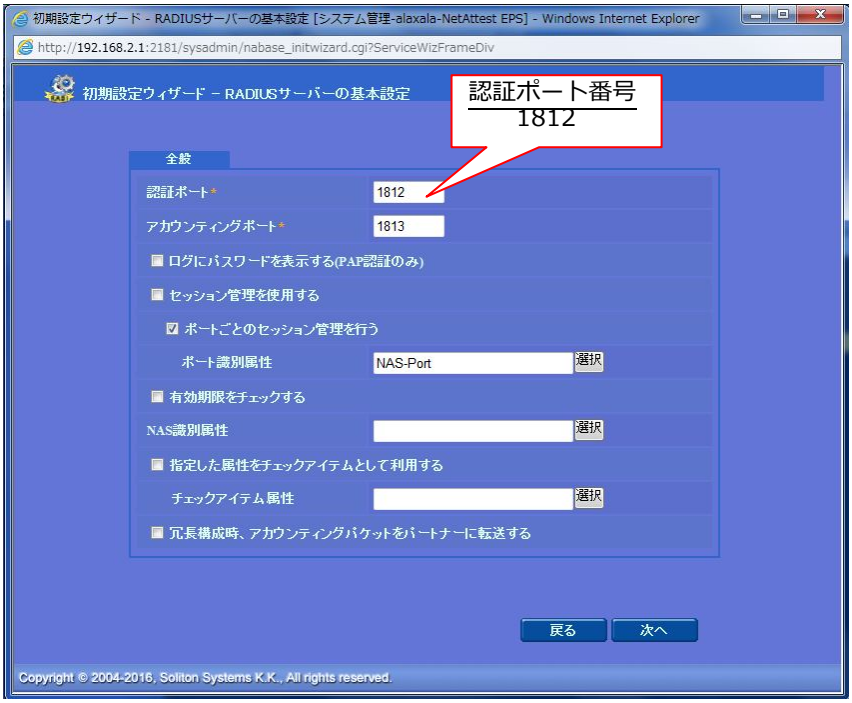
(2) LDAPデータベースを構築

① [サフィックス]、[説明]、[匿名ユーザーによる参照を許可する]および[ユーザーの最終認証成功日時を記録する]を必要に応じて設定し、<次へ>ボタンをクリックするとローカルデータベースが構築されます。正常に構築されるとLDAPサービスが起動され、次のページに進みます。

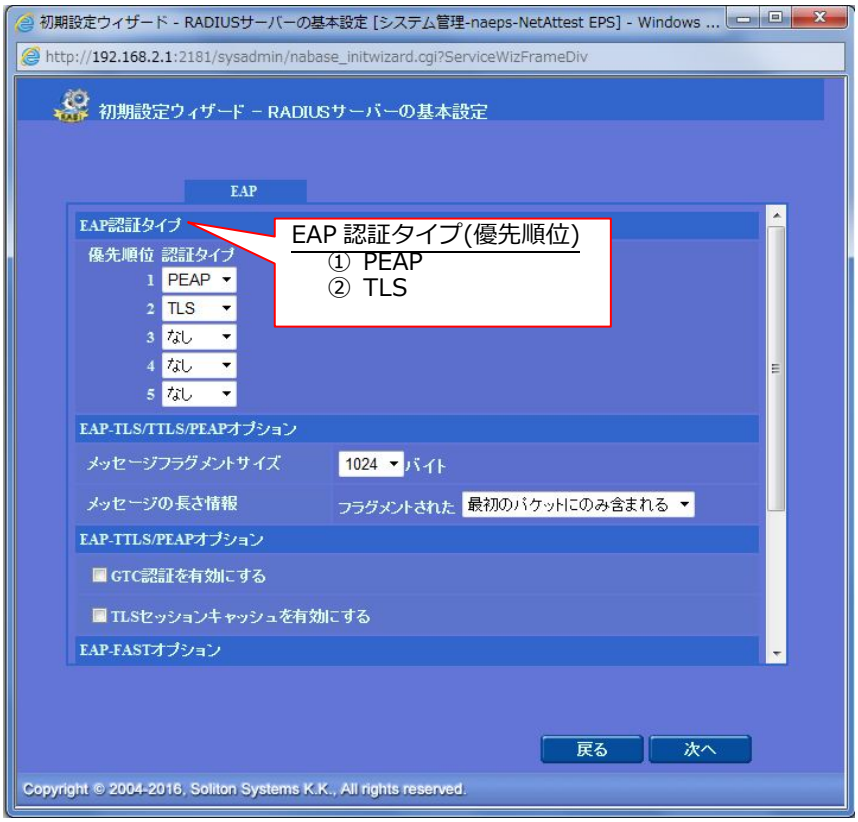


(3) RADIUSサーバーの基本設定

①[認証ポート]、[アカウンティングポート]などを設定します。
認証ポートの値はコンフィグレーション「radius-server host」コマンドの[auth-port]の値を設定します。設定を省略した場合はデフォルト設定「1812」のままにしてください。
設定後、<次へ>ボタンをクリックします。



② [EAP認証タイプ]に使用するEAPタイプを設定します。
設定が完了したら、<次へ>ボタンをクリックします。
証明書検証に関する設定は、そのまま、<次へ>ボタンをクリックします。



(4) RADIUSクライアントの設定

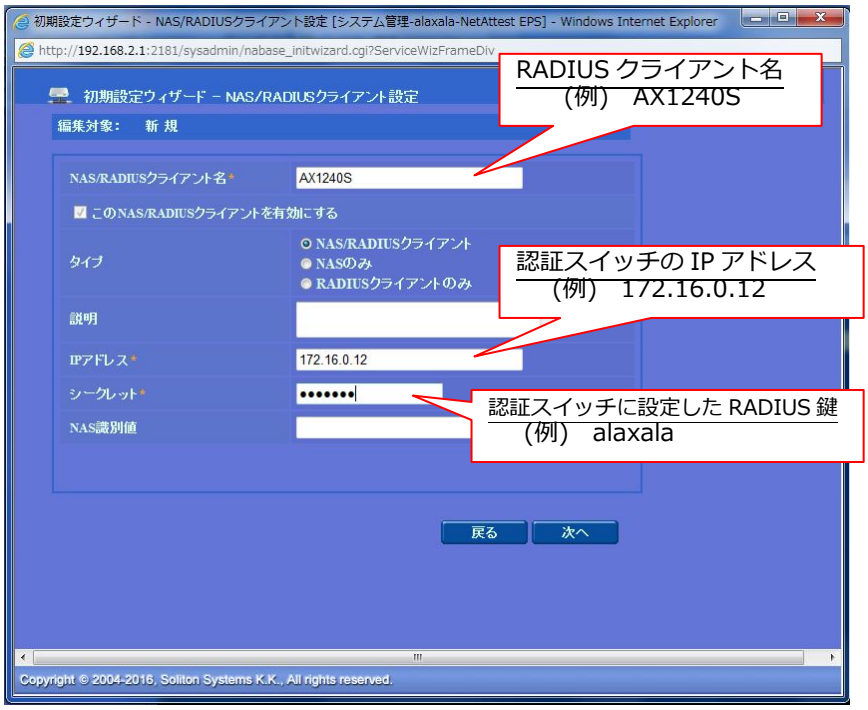
最初の NAS/RADIUS クライアントを登録します。RADIUS サーバーが起動するためには、少なくとも 1 つの NAS/RADIUS クライアントの登録が必要です。

[NAS/RADIUS クライアント名]と[IP アドレス]およびアクセスを許可するための[シークレット]を設定します。

設定が完了したら<次へ>ボタンをクリックしてください

NAS/RADIUS クライアントが登録され、RADIUS サービスが開始されます。

正常に終了すると次のページに進みます。



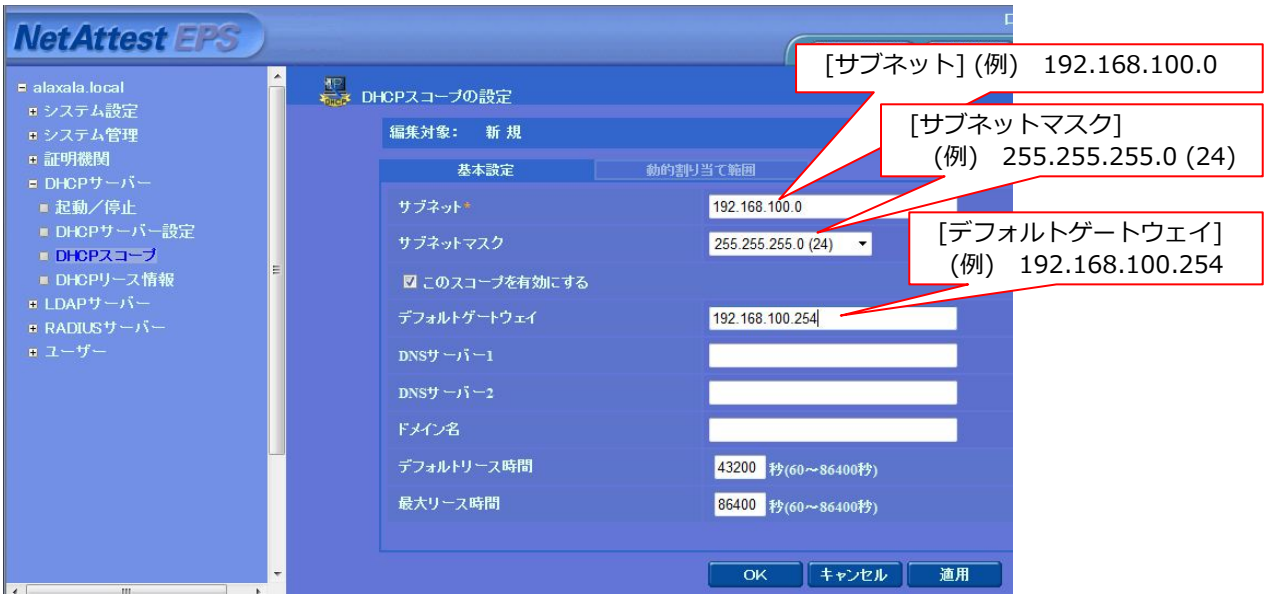
(5) サービス初期設定の完了

「初期設定ウィザード – NAS/RADIUS クライアントの設定」ページの<次へ>ボタンをクリックすると、サービス初期設定の完了メッセージが表示されます。<OK>ボタンをクリックするとシステム管理ページが開きます。

2.4. DHCP サーバーの設定

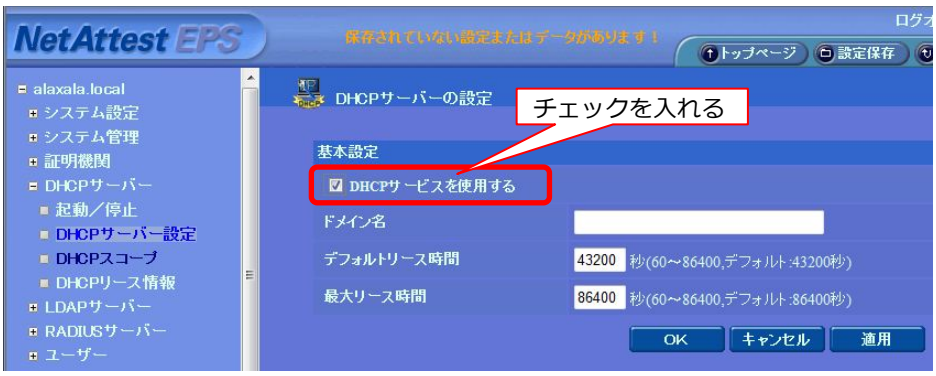
本例では、NetAttest EPS の DHCP サービス機能を使用します。他の DHCP サーバーを使用する場合は設定不要です。

① DHCP サービスを有効にするには、DHCP スコープを設定します。「基本設定」タブで [サブネット]、[サブネットマスク]、[デフォルトゲートウェイ]を設定します。



②「動的割り当て範囲」タブで、DHCP クライアントに割り当てる IP アドレス範囲を設定し、<OK>, または<適用>ボタンをクリックすると DHCP スコープが設定されます。

③ [DHCP サーバー] － [DHCP サーバー設定] をクリックして [DHCP サービスを使用する]オプションをチェックして、<OK>, または<適用>ボタンをクリックすると DHCP サービスが開始されます。



3. IEEE 802.1X 認証

3.1. NetAttest EPS の設定

NetAttest EPS の初期設定を実施していない場合は、先に**「2 章　NetAttest EPS の初期設定」**を実施してから、以下をおこなってください。なお NetAttest EPS の初期設定は、各認証方式で共通の設定のため、1 回設定すれば再度設定する必要はありません。

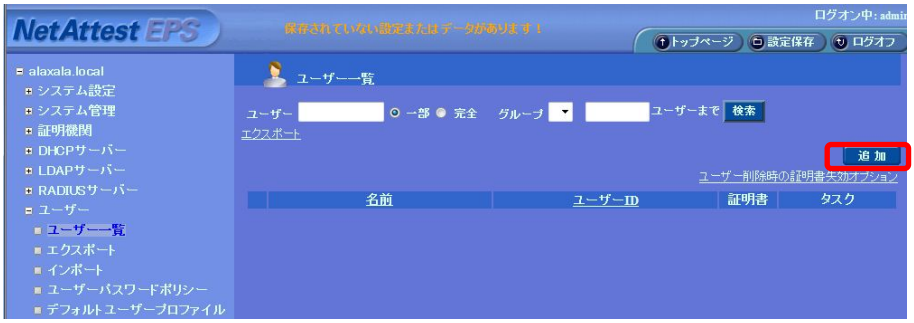
3.1.1. ユーザー情報の登録

IEEE802.1X 認証で使用するユーザー情報は、以下の例とします。これに従い NetAttest EPS に登録してください。

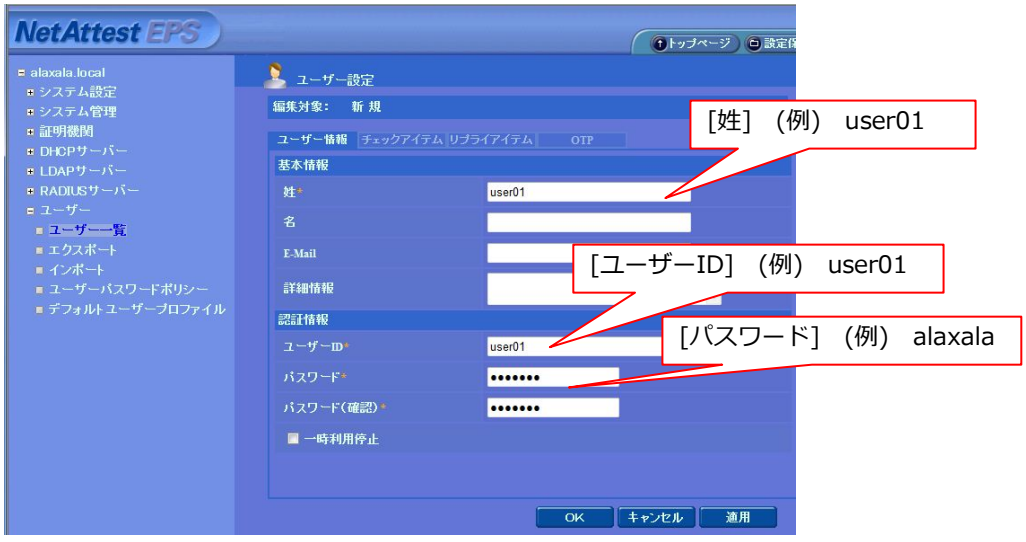
表 3.1-1　IEEE802.1X 認証で使用するユーザー情報

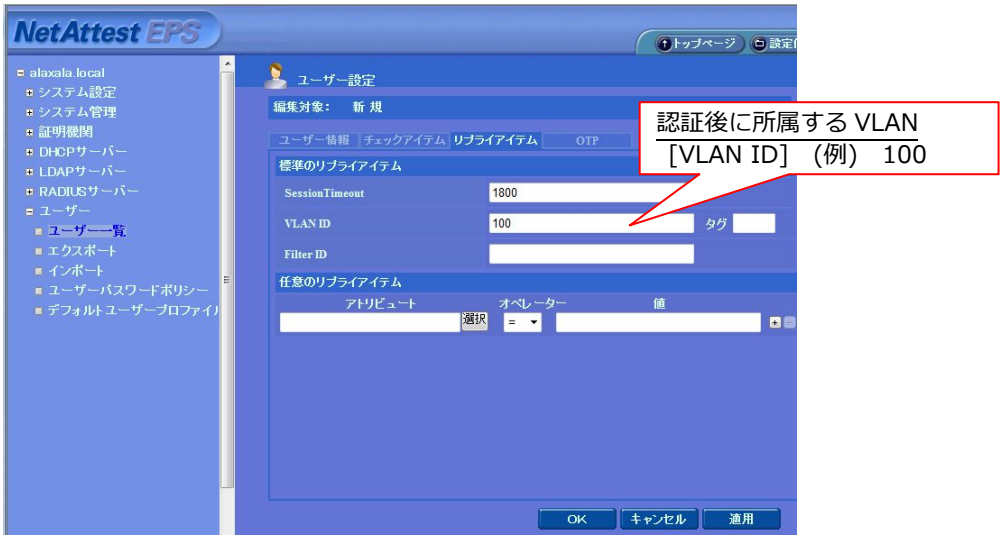
ユーザーID	パスワード	認証後に所属する VLAN
user01	alaxala	100

① 新規ユーザーを登録するには、システム管理ページで[ユーザー] – [ユーザー一覧]を選択して <追加>ボタンをクイックします。



② 「ユーザー情報」タブで、[ユーザーID]、[パスワード]などの認証情報、および [姓]、[名]、[E-Mail]などの基本情報を設定します。また「サプライアイテム」タブでは、[VLAN ID]に認証後に所属する VLAN ID を設定して、<OK>または<適用ボタン>をクリックします。





＜session timeout に関する注意事項＞

認証スイッチが AX6000S,AX4600S,AX3800S,AX3600S,AX2400S の場合、コンフィグレーションに認証済み端末の再認証をおこなう間隔(dot1x timeout reauth-period, dot1x vlan timeout reauth-period, dot1x vlan dynamic timeout reauth-period)を設定した場合でも、再認証時間は RADIUS サーバーの設定[session timeout]に従います。

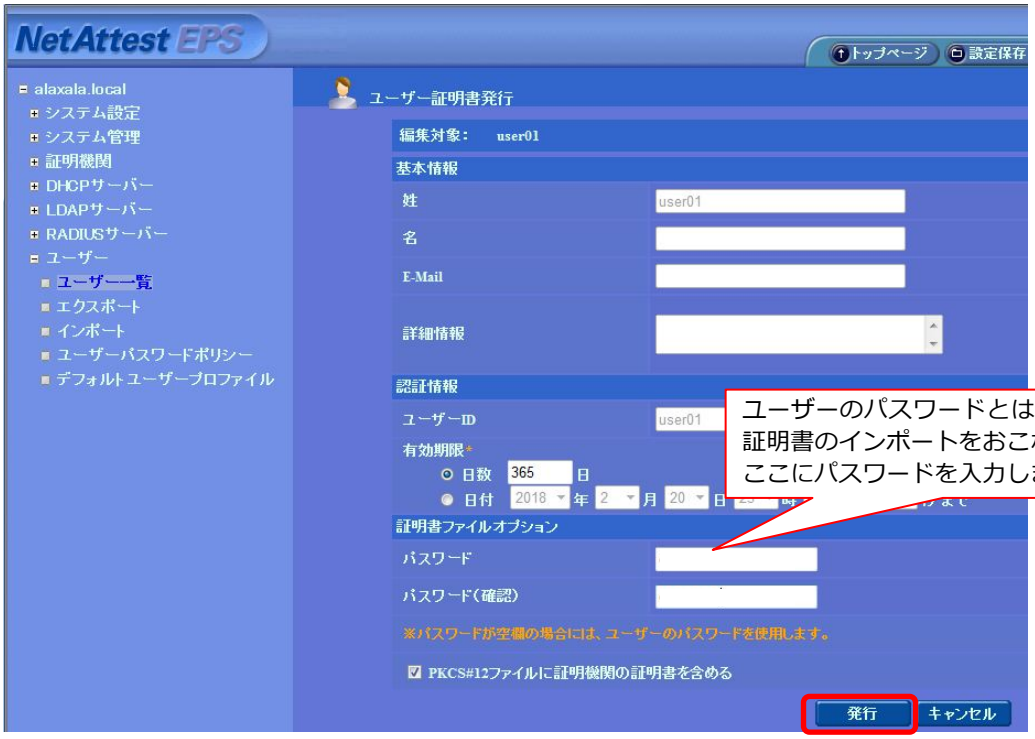
③ システム管理ページで [ユーザー] – [ユーザー一覧]に追加したユーザーが登録されていることを確認します。

3.1.2. ユーザー証明書の発行

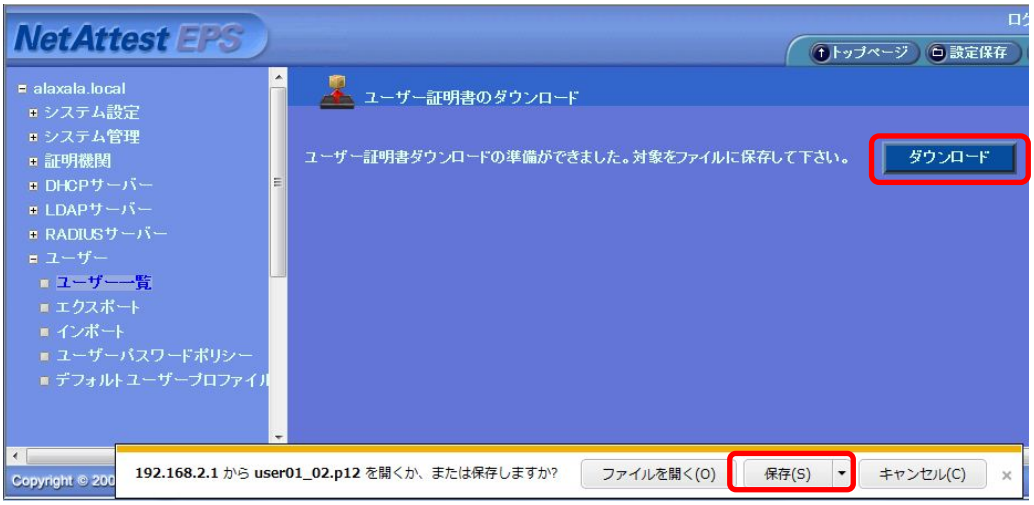
認証クライアントにインストールするためのユーザー証明書を発行します。

①「ユーザー一覧」ページの証明書欄の<発行>ボタンをクリックすると、「ユーザー証明書発行」ページが表示されます。

② <発行>ボタンをクリックするとユーザー証明書を発行します。



③ ユーザー証明書の発行が正常におこなわれると、「ユーザー証明書のダウンロード」ページが表示されます。<ダウンロード>ボタンをクリックして証明書ファイルをダウンロードしてください。



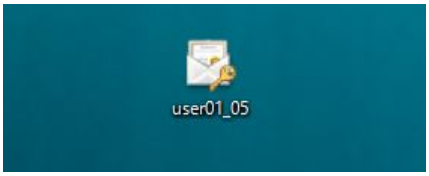
ユーザー証明書ファイル ： user01_02.p12

3.2. 認証クライアントの設定

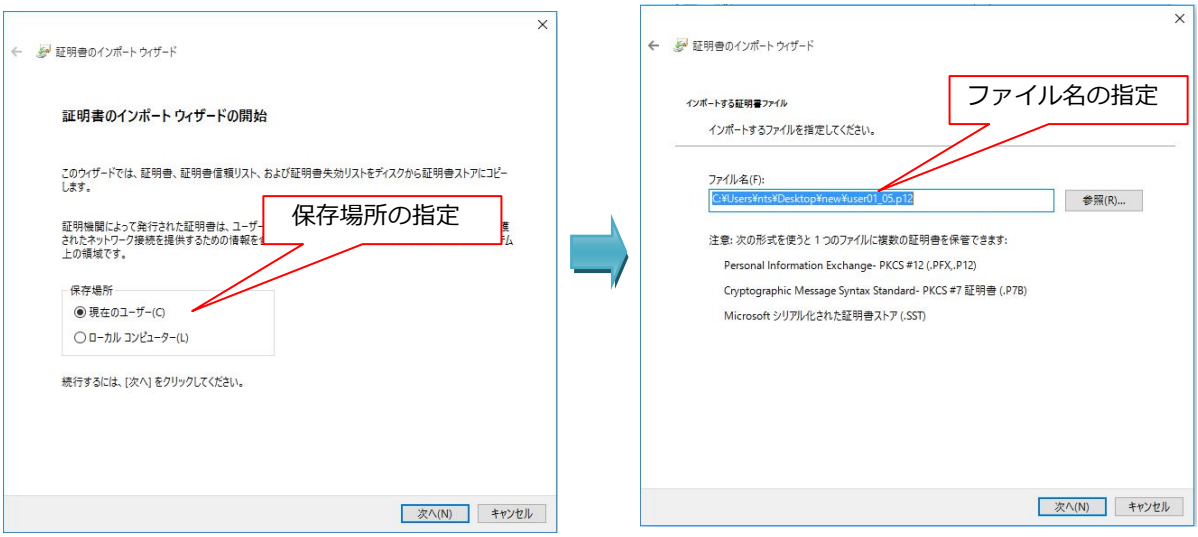
3.2.1. ユーザー証明書のインストール

PC にユーザー証明書をインストールします。

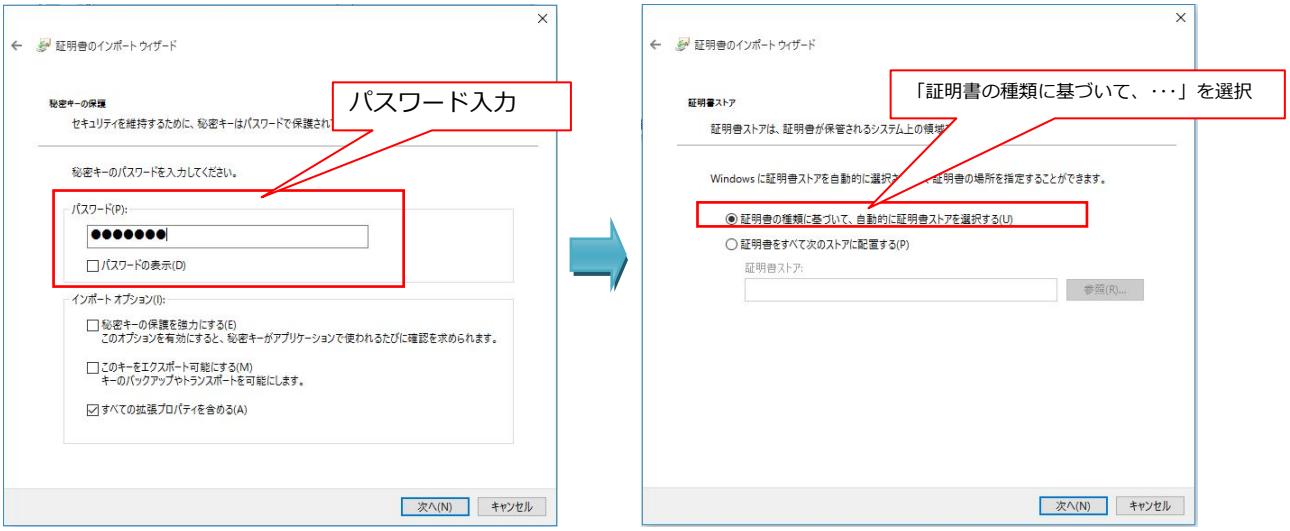
① 「3.1.2 ユーザー証明書の発行」でダウンロードしておいたユーザー証明書(uer01_05.p12)をダブルクリックすると、証明書インポートウィザードが実行されます。



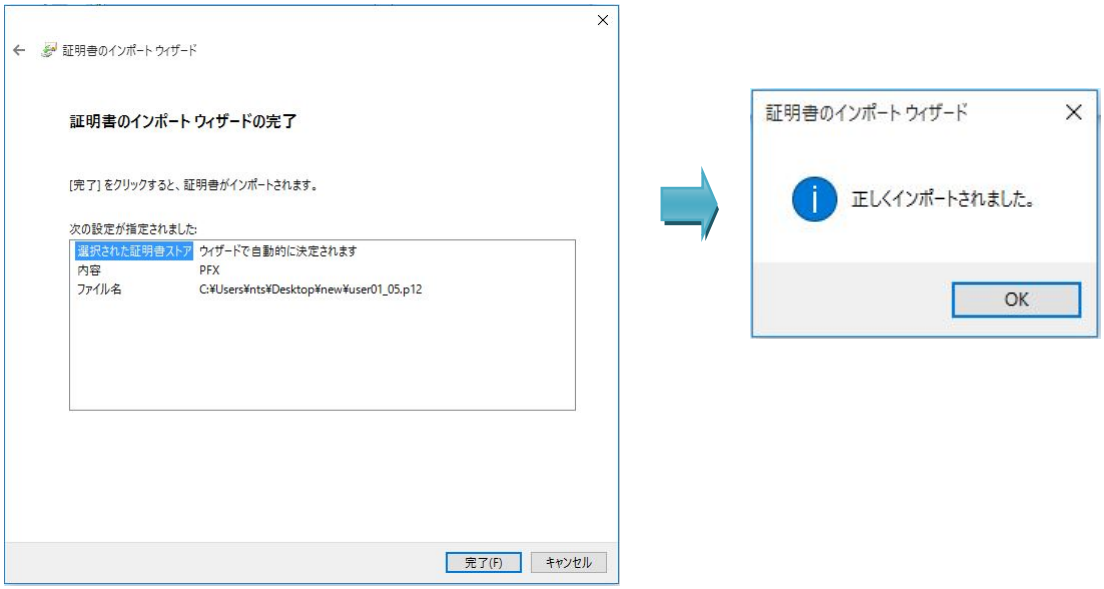
②「証明書のインポートウィザードの開始」で、保存場所の指定 ⇒ 証明書ファイルの指定をして次に進みます。



③ NetAttest EPSで証明書を発行した際に設定したパスワードを入力し、証明書ストアを自動的に選択するを選びます。



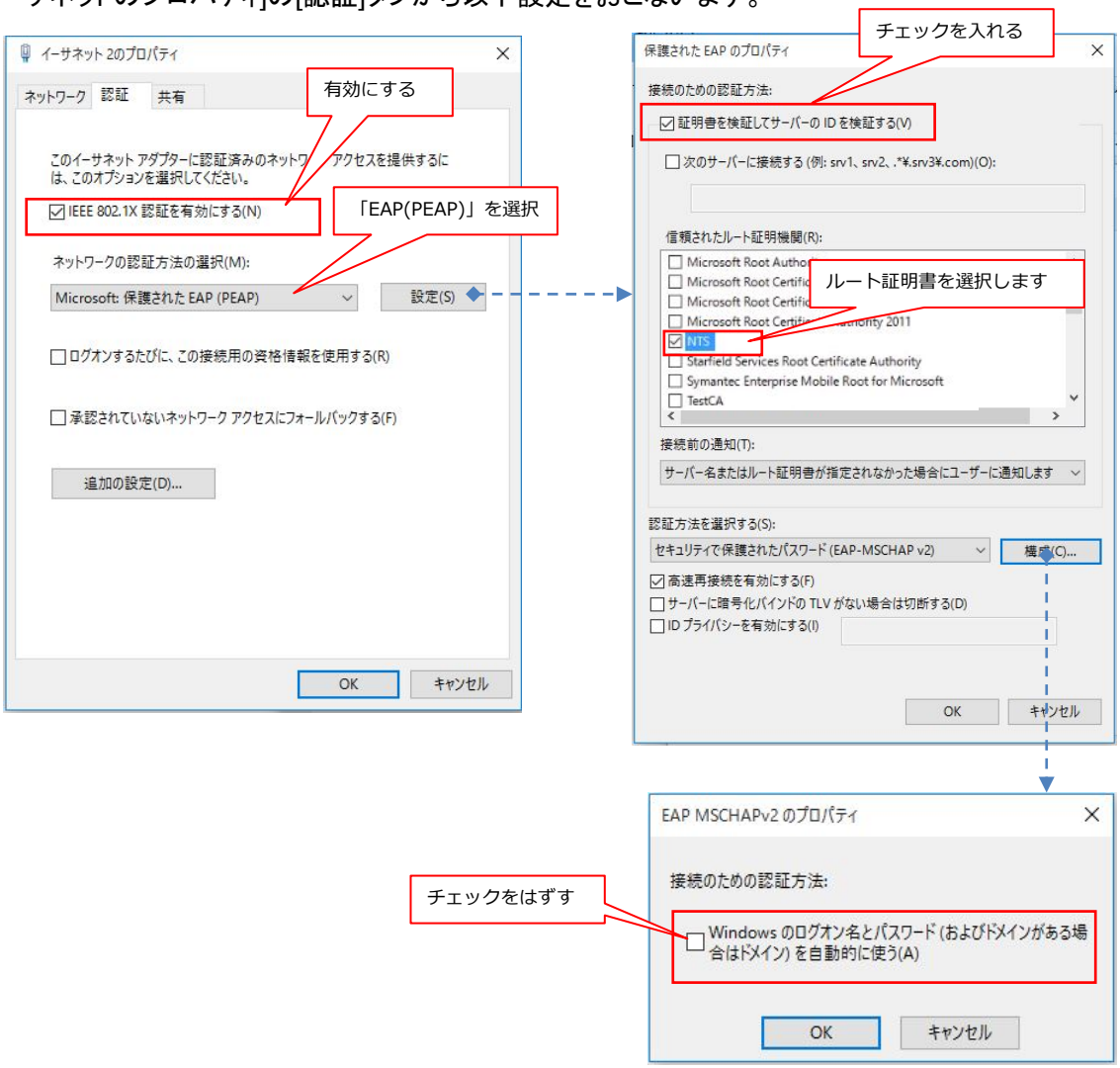
④「証明書のインポートウィザードの完了」の画面で<完了>ボタンをクリックすると、証明書がインポートされ、正常にインポートされるとメッセージが出力されます。



3.2.2. PEAP の設定と認証確認

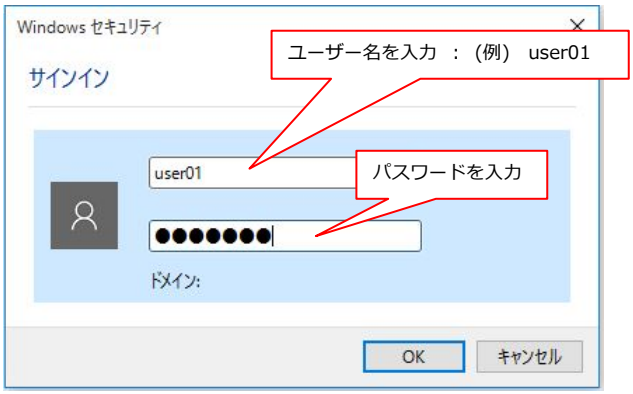
① サプリカントで使用するEAPの設定をおこないます。

[イーサネットのプロパティ]の[認証]タブから以下設定をおこないます。



② 認証を開始します。

認証クライアントにケーブルを接続すると、「サインイン」の入力画面が表示されるので、ユーザー名とパスワードを入力します。

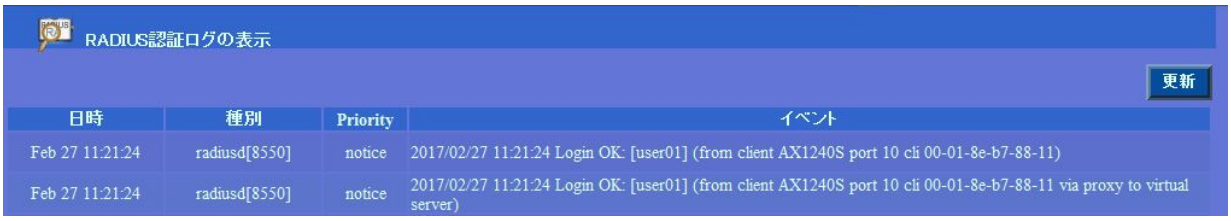


③ 認証に成功したことを、以下の方法で確認します。

(1) NetAttest EPSの認証ログで確認

NetAttest EPSでは、[RADIUSサーバー] – [RADIUSサーバー管理] – [認証ログ] – [表示]で以下のようなログが表示されます。

＜RADIUS認証ログの表示＞



(2) 認証スイッチの運用コマンドで確認

ALAXALAの認証スイッチ(AX1240S)では、運用コマンドで認証ステータスを確認できます。

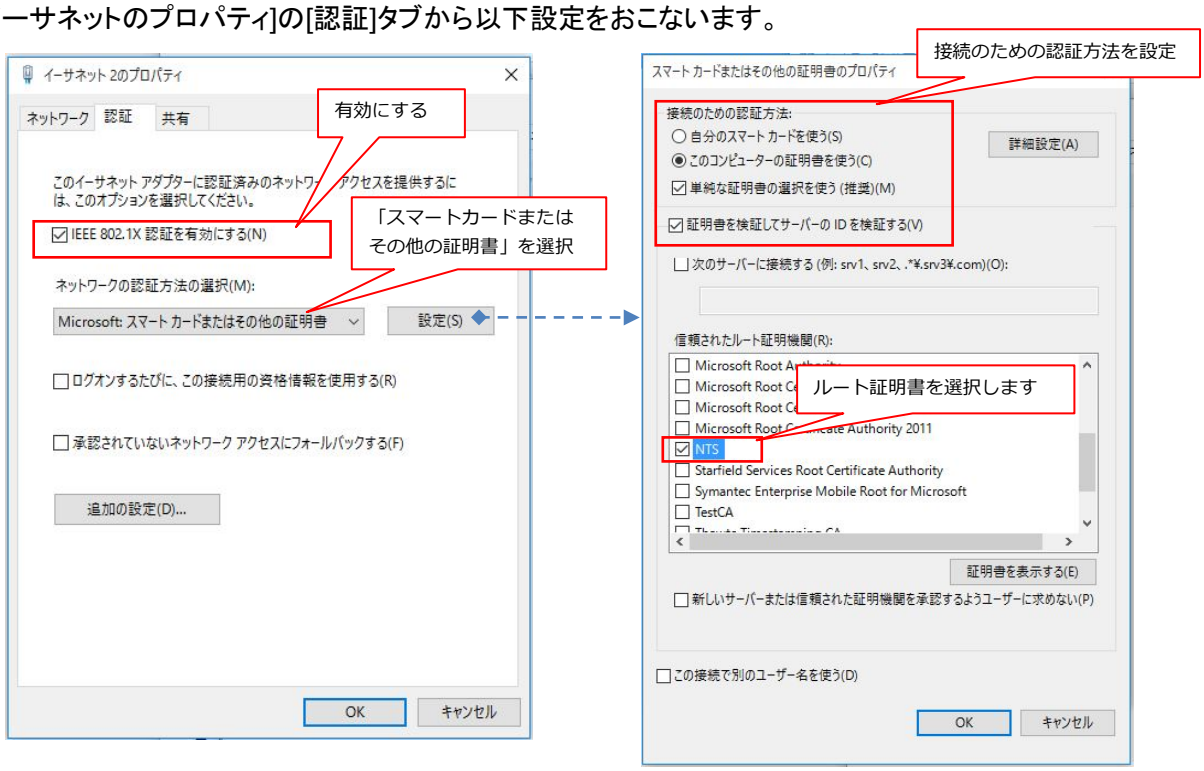
＜認証スイッチでの表示＞

```
AX1240S# show dot1x port 0/1 detail

Date 2017/02/27 11:21:32 JST
Port 0/1 (Dynamic)
AccessControl    : Multiple-Auth              PortControl     : Auto
Status           : ---                        Last EAPOL      : 0001.8eb7.8811
Supplicants      : 1 / 3 / 64                 ReAuthMode      : Disable
TxTimer          : 30                         ReAuthTimer     : 3600
ReAuthSuccess    : 8                          ReAuthFail      : 6
SuppDetection    : Auto
VLAN(s): 30,100,200

 Supplicants MAC   F  Status          AuthState       BackEndState    ReAuthSuccess
                      SessionTime(s) Date/Time                       SubState
 [VLAN 100]           Port(Dynamic) Supplicants : 1
 0001.8eb7.8811       Authorized      Authenticated   Idle            0
                      8               2017/02/27 11:21:24            Full
```

3.2.3. TLS の設定と認証確認

① サプリカントで使用するTLSの設定をおこないます。

[イーサネットのプロパティ]の[認証]タブから以下設定をおこないます。



② 認証を開始します。

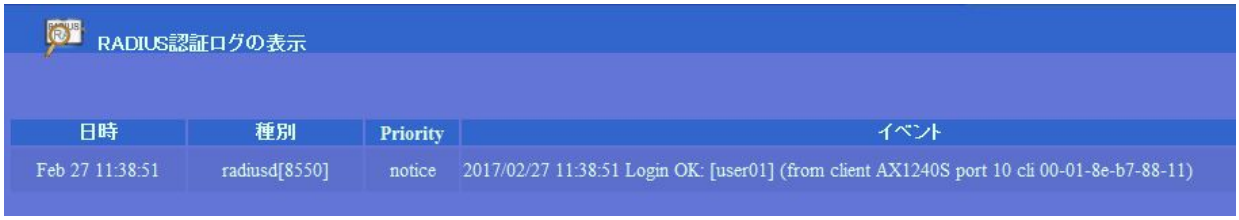
認証クライアントにケーブルを接続すると、認証が開始されます。

③ 認証に成功したことを、以下の方法で確認します。

(1) NetAttest EPSの認証ログで確認

NetAttest EPSでは、[RADIUSサーバー] – [RADIUSサーバー管理] – [認証ログ] – [表示]で以下のようなログが表示されます。

＜RADIUS認証ログの表示＞



(2) 認証スイッチの運用コマンドで確認

アラクサラの認証スイッチ(AX1240S)では、運用コマンドで認証ステータスを確認できます。

＜認証スイッチの表示＞

```
AX1240S# show dot1x port 0/1 detail

Date 2017/02/27 11:41:00 JST
Port 0/1 (Dynamic)
AccessControl    : Multiple-Auth                PortControl     : Auto
Status           : ---                          Last EAPOL      : 0001.8eb7.8811
Supplicants      : 1 / 1 / 64                   ReAuthMode      : Disable
TxTimer          : 30                           ReAuthTimer     : 3600
ReAuthSuccess    : 9                            ReAuthFail      : 7
SuppDetection    : Auto
VLAN(s): 30,100,200

 Supplicants MAC   F  Status          AuthState       BackEndState    ReAuthSuccess
                      SessionTime(s) Date/Time                       SubState
 [VLAN 100]           Port(Dynamic) Supplicants : 1
 0001.8eb7.8811       Authorized      Authenticated   Idle            1
                      273             2017/02/27 11:36:28            Full
```

4. Web 認証

4.1. NetAttest EPS の設定

NetAttest EPS の初期設定を実施していない場合は、先に**「2 章　NetAttest EPS の初期設定」**を実施してから、以下をおこなってください。なお NetAttest EPS の初期設定は、各認証方式で共通の設定のため、1 回設定すれば再度設定する必要はありません。

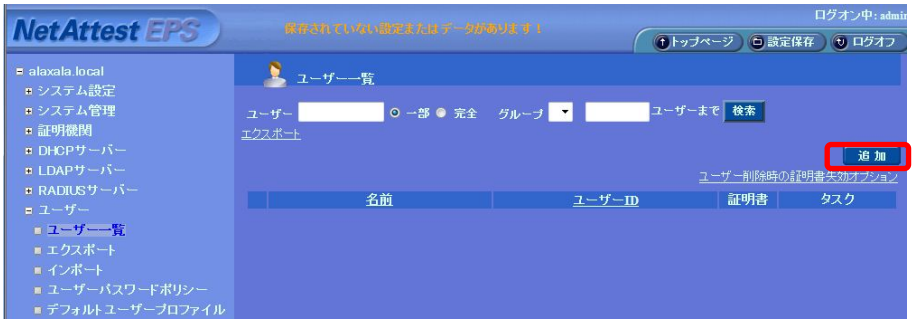
4.1.1. ユーザー情報の登録

Web 認証で使用するユーザー情報は、以下の例とします。これに従い NetAttest EPS に登録してください。

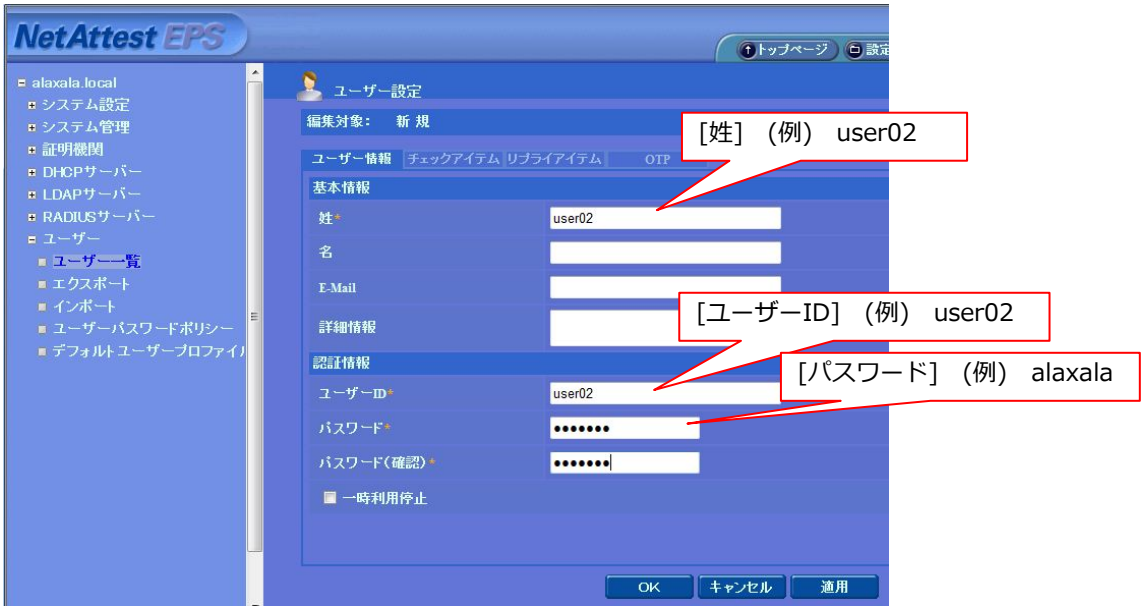
表 4.1-1　Web 認証で使用するユーザー情報

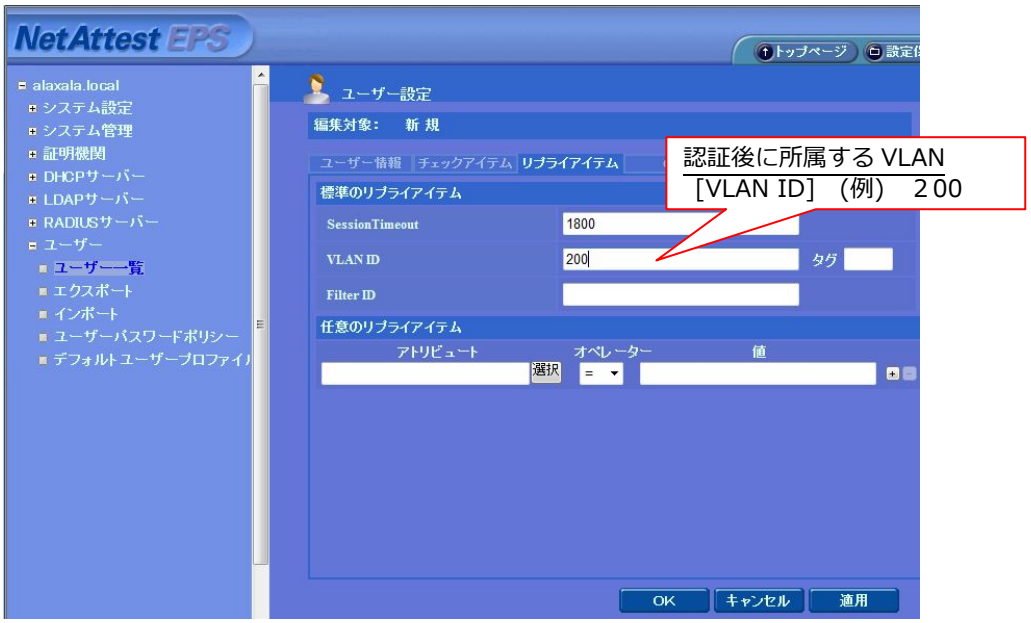
ユーザーID	パスワード	認証後に所属する VLAN
user02	alaxala	200

① 新規ユーザーを登録するには、システム管理ページで[ユーザー] – [ユーザー一覧]を選択して<追加>ボタンをクイックします。



② 「ユーザー情報」タブで、[ユーザーID]、[パスワード]などの認証情報、および [姓]、[名]、[E-Mail]などの基本情報を設定します。また「サプライアイテム」タブでは、[VLAN ID]に認証後に所属する VLAN ID を設定して、<OK>または<適用ボタン>をクリックします。





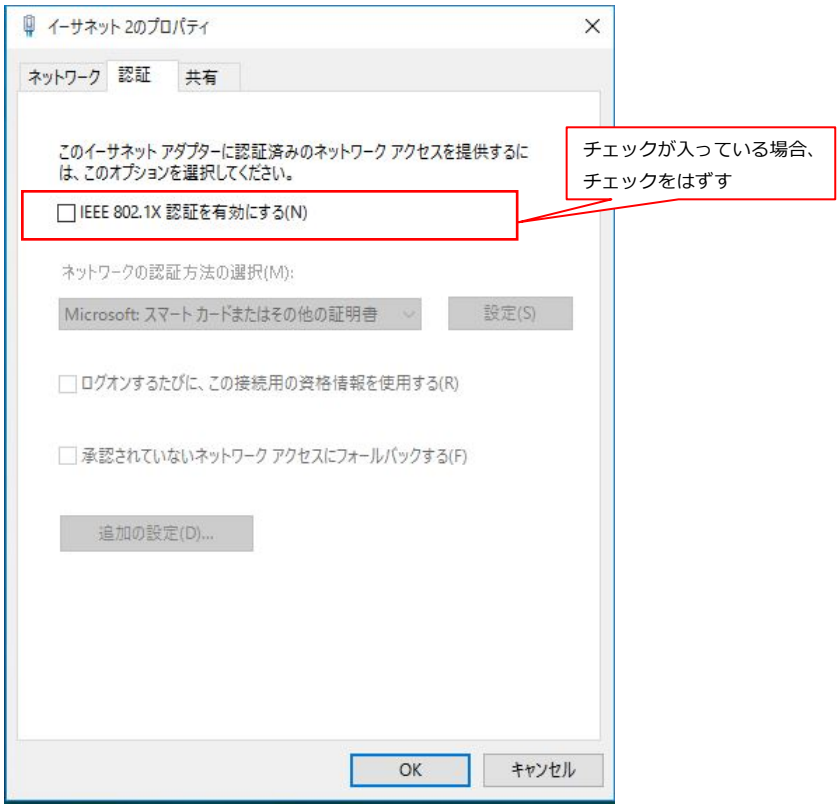
③ システム管理ページで [ユーザー] – [ユーザー一覧]に追加したユーザーが登録されていることを確認します。

4.2. 認証クライアントの設定

4.2.1. Web 認証の設定と認証確認

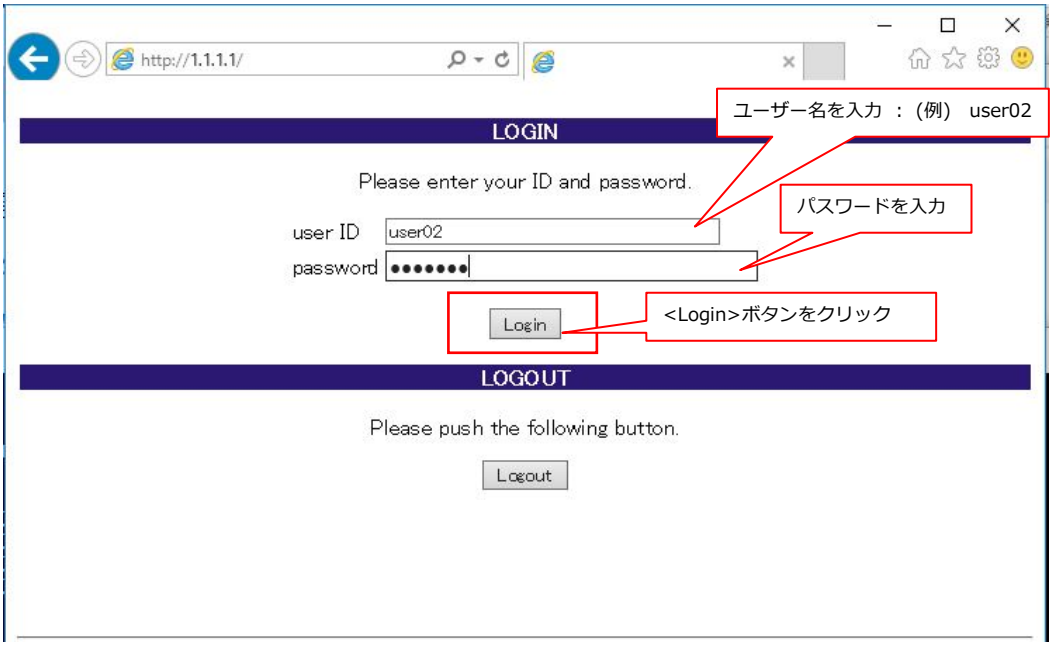
① 認証の設定をおこないます。

[イーサネットのプロパティ]の[認証]タブから以下設定をおこないます。

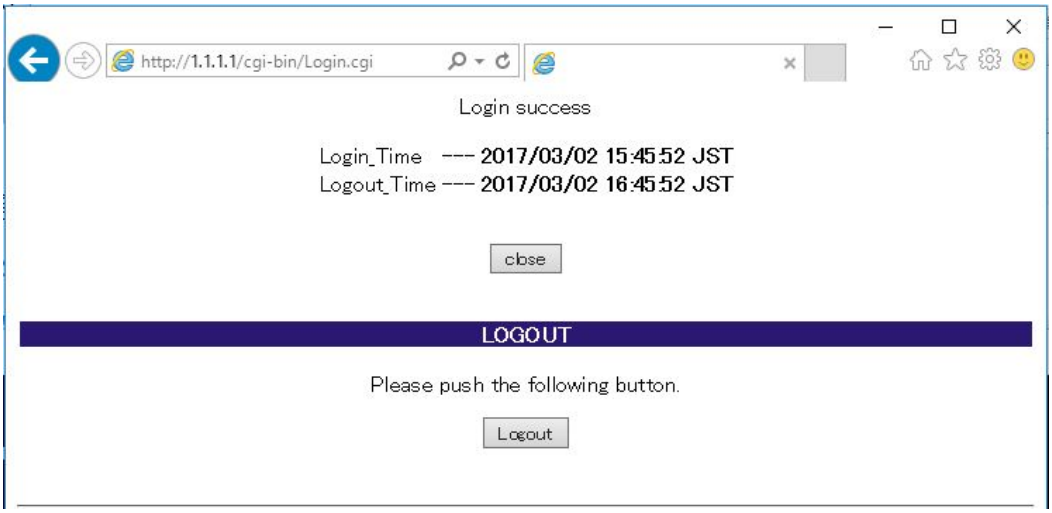


② 認証を開始します。

ブラウザからWeb認証専用IPアドレス(1.1.1.1)にHTTPアクセスをして ログイン画面が表示されたら、ユーザーIDおよび パスワードを入力します。



③ 認証が成功すると「Login success」画面が表示されます。

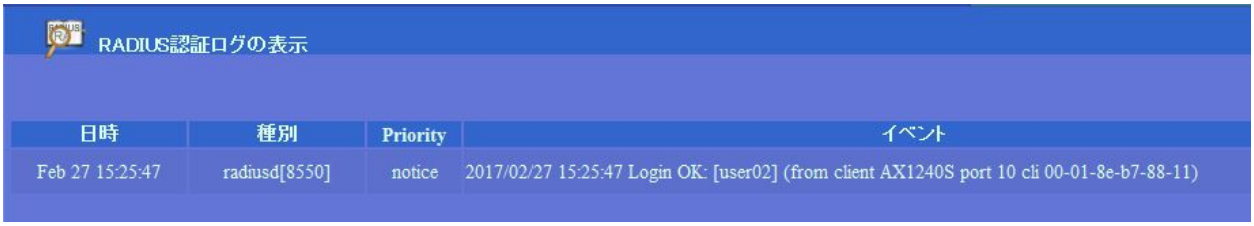


④ 認証に成功したことを、以下の方法で確認します。

(1) NetAttest EPSの認証ログで確認

NetAttest EPSでは、[RADIUSサーバー] – [RADIUSサーバー管理] – [認証ログ] – [表示]で以下のようなログが表示されます。

＜RADIUS認証ログの表示＞



(2) 認証スイッチの運用コマンドで確認

アラクサラの認証スイッチ(AX1240S)では、運用コマンドで認証ステータスを確認できます。

＜認証スイッチの表示＞

```
AX1240S# show web-authentication login

Date 2017/02/27 15:27:01 JST
 Dynamic VLAN mode total login counts(Login/Max):     1 / 256
  Authenticating client counts :       0
  Port roaming : Disable
   No F User name                              Port VLAN Login time              Limit
    1     user02                               0/1     200 2017/02/27 15:25:47 00:58:45
```

5. MAC 認証

5.1. NetAttest EPS の設定

NetAttest EPS の初期設定を実施していない場合は、先に**「2 章　NetAttest EPS の初期設定」**を実施してから、以下をおこなってください。なお NetAttest EPS の初期設定は、各認証方式で共通の設定のため、1 回設定すれば再度設定する必要はありません。

5.1.1. ユーザー情報の登録

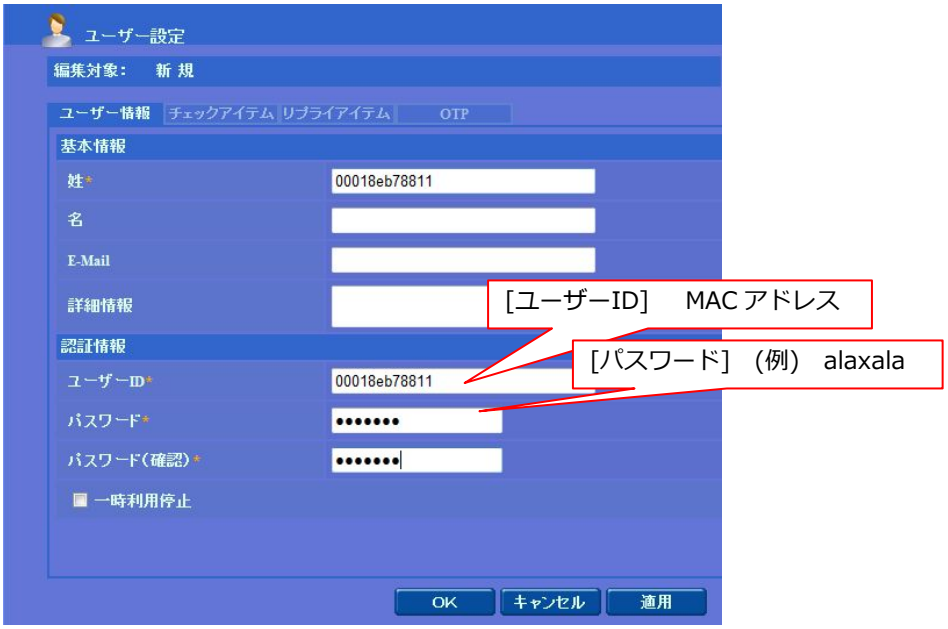
MAC 認証で使用するユーザー情報は、以下の例とします。これに従い NetAttest EPS に登録してください。

表 5.1-1　MAC 認証で使用するユーザー情報

ユーザーID (MAC)	パスワード	認証後に所属する VLAN
[MAC アドレス]	alaxala	200

① 新規ユーザーを登録するには、システム管理ページで[ユーザー] – [ユーザー一覧]を選択して<追加>ボタンをクイックします。

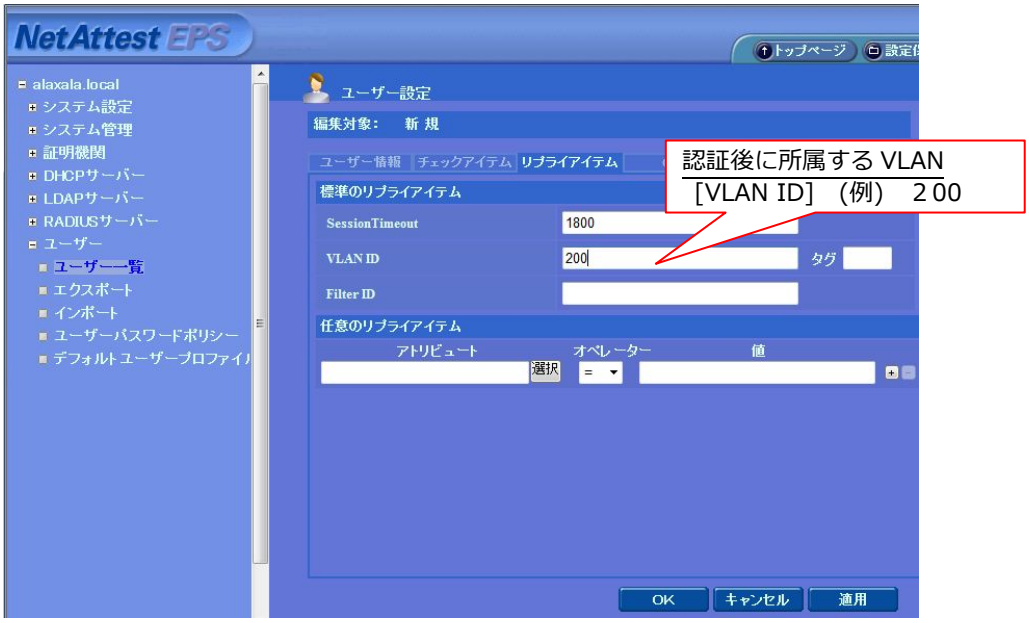
② 「ユーザー情報」タブで、[ユーザーID]、[パスワード]などの認証情報、および [姓]、[名]、[E-Mail]などの基本情報を設定します。また「サプライアイテム」タブでは、[VLAN ID]に認証後に所属する VLAN ID を設定して、<OK>または<適用ボタン>をクリックします。



＜注意事項＞

ユーザーIDとパスワードの入力形式について

AX1200S，AX2200S，AX2500Sシリーズでは、デフォルトのMACアドレス設定形式が**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。



③ システム管理ページで [ユーザー] – [ユーザー一覧]に追加したユーザーが登録されていることを確認します。

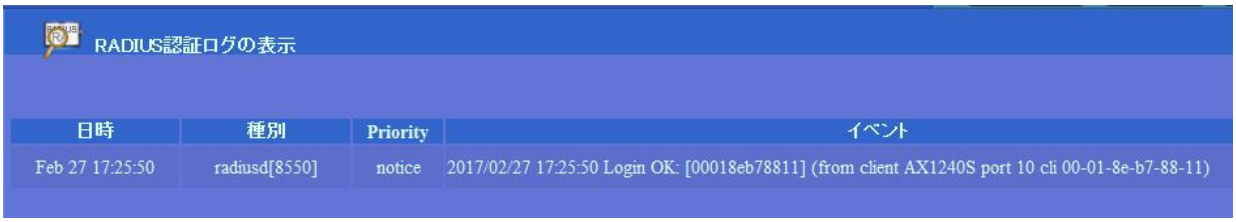
5.2. MAC 認証の確認

MAC認証を登録した端末をケーブルで接続して 認証に成功したことを、以下の方法で確認します。

(1) NetAttest EPSの認証ログで確認

NetAttest EPSでは、[RADIUSサーバー] – [RADIUSサーバー管理] – [認証ログ] – [表示]で以下のようなログが表示されます。

＜RADIUS認証ログの表示＞



(2) 認証スイッチの運用コマンドで確認

アラクサラの認証スイッチ(AX1240S)では、運用コマンドで認証ステータスを確認できます。

＜認証スイッチの表示＞

```
AX1240S# show mac-authentication auth-state

Date 2017/02/27 17:26:13 JST
 Dynamic VLAN mode total client counts(Login/Max):     1 / 256
  Authenticating client counts :       0
  Hold down client counts          :       0
  Port roaming : Disable
   No F MAC address        Port VLAN    Login time                Limit       Reauth
    1     0001.8eb7.8811    0/1     200    2017/02/27 17:25:49     infinity      3575
```

付録 1. マルチステップ認証

アラクサラの認証スイッチでは、マルチステップ認証をサポートしている装置があります。マルチステップ認証は、端末認証とユーザー認証を 2 段階で実施するため、より安全な認証システムを構築することができます。

ここでは、一例として ① 端末認証：MAC 認証 ⇒ ② ユーザー認証：Web 認証の組み合わせのマルチステップ認証の設定および手順について紹介します。

(1) マルチステップ認証を設定

認証スイッチの認証ポートにマルチステップ認証の設定を追加します。デフォルトではマルチステップ認証をおこないません。

以下の設定は、**「1.2.1 使用機器一覧と AX コンフィグレーション」**への追加設定となります。その他の設定は、コンフィグレーション設定例を参照ください。

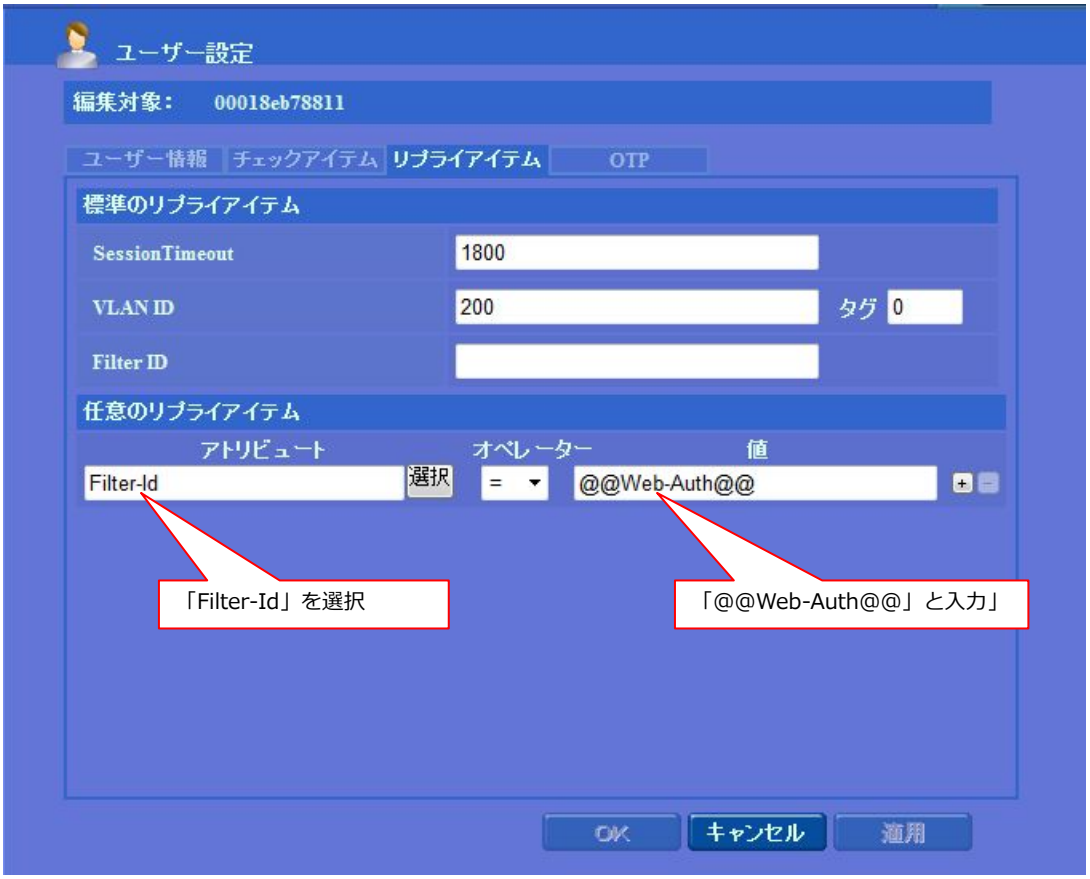
```
(config)# interface fastethernet 0/1
(config-if)# switchport mode mac-vlan
(config-if)# switchport mac vlan 100,200
(config-if)# switchport mac native vlan 30
(config-if)# dot1x port-control auto
(config-if)# dot1x multiple-authentication
(config-if)# dot1x supplicant-detection auto
(config-if)# web-authentication port
(config-if)# mac-authentication port
(config-if)# authentication ip access-group "auth"
(config-if)# authentication arp-relay
(config-if)# ★ authentication multi-step
```

マルチステップ認証の設定

(2) RADIUS サーバーの設定

① システム管理ページで[ユーザー] – [ユーザー一覧]を選択して、ユーザー一覧から MAC 認証用のユーザーから <変更>ボタンをクリックします。

② 「リプライアイテム」タブの[任意のリプライアイテム]欄で、アトリビュートに「Filter-Id」を選択し、値に「@@Web-Auth@@」を入力して <OK>ボタン、または<適用>ボタンをクリックします。



(3) マルチステップ認証の確認

① MAC 認証を登録した端末にケーブル接続すると、端末認証(MAC 認証)が開始されます。認証に成功したことを運用コマンドで確認します。

② ブラウザより、Web 認証専用 IP アドレスに HTTP アクセスして、ユーザー認証(Web 認証)を開始します。運用コマンドより、マルチステップ認証に成功したことを確認します。

```
AX1240S# show authentication multi-step

Date 2017/03/02 15:56:20 JST
Port 0/1    : multi-step
        <        Supplicant information        >    <Authentic method>
  No MAC address       State VLAN F Type       Last    (first step)
    1 0001.8eb7.8811 pass     200     multi     web     (mac)
```

付録 2. ダイナミック ACL/QoS

アラクサラの認証スイッチ AX2500S シリーズでは、ダイナミック ACL/QoS 機能を実装しています。ダイナミック ACL/QoS 機能は、認証時に RADIUS サーバーによるクラス情報配布と 付与されたクラス情報を使用して、アクセス制御を ACL(フィルタ)/QoS 機能で実現します。

ここでは一例として、ダイナミック ACL の設定、および手順について紹介します。

(1) ACL の作成

下記に示す一例は、クラス毎に保護したいネットワークを指定する例です。ユーザー認証後に 2 つのクラスに分けてそれぞれ違う宛先ネットワークに振り分けます。

表 付録 2-1 ダイナミック ACL で制御するネットワーク

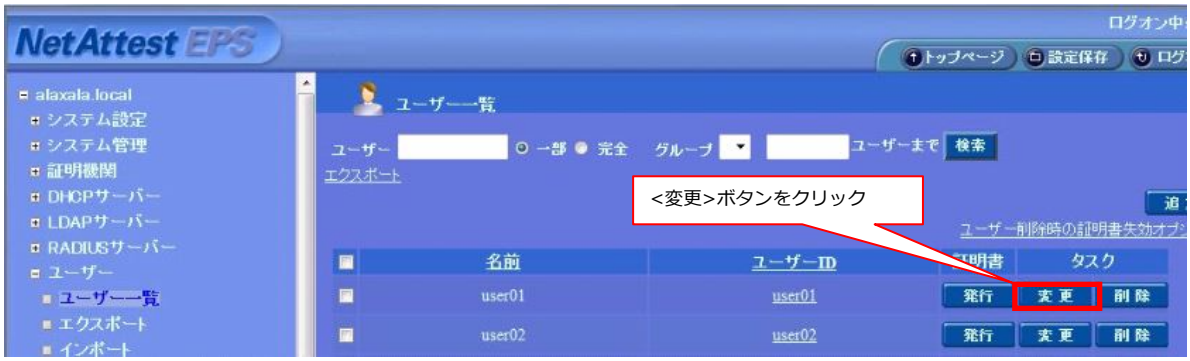
宛先ネットワーク	ネット A (192.168.5.0/24)	ネット B (192.168.6.0/24)	その他 (ANY)
通信可能なクラス	Class 1	Class 2	全クラス

ダイナミック ACL の設定例を以下に示します。以下の設定は、**「1.2.1 使用機器一覧と AX コンフィグレーション」**への追加設定となります。その他の設定は、コンフィグレーション設定例を参照ください。なお、ダイナミック ACL/QoS 機能は、AX2500S シリーズのみの機能となります。

```
(config)# ip access-list extended DynamicACL
(config-ext-nacl)# 10 permit ip any 192.168.5.0 0.0.0.255 class 1
(config-ext-nacl)# 20 deny ip any 192.168.5.0 0.0.0.255
(config-ext-nacl)# 30 permit ip any 192.168.6.0 0.0.0.255 class 2
(config-ext-nacl)# 40 deny ip any 192.168.6.0 0.0.0.255
(config-ext-nacl)# 50 permit ip any any

(config)# interface vlan 100
(config-if)# ip access-group DynamicACL in
(config)# interface vlan 200
(config-if)# ip access-group DynamicACL in
```

(2) RADIUS サーバーの設定

① システム管理ページで[ユーザー] – [ユーザー一覧]を選択して、ユーザー一覧から該当するユーザーID <変更>ボタンをクリックします。



② 「リプライアイテム」タブの[任意のリプライアイテム]欄で、アトリビュートに「Filter-Id」を選択し、値に「/Class=番号(1-63)」を入力して <OK>ボタン、または<適用>ボタンをクリックします。

設定例：「user01」： Class 1 ，「user02」： Class 2 を指定

- 「user01」

- 「user02」

(3) ダイナミック ACL の確認

ユーザー認証が完了後、宛先ネットワークへ疎通確認をおこない Class 単位で期待する統計カウンタとなっていることを確認します。

```
AX2530S# show access-filter

Date 2017/03/06 16:40:12 JST
Using Interface:vlan 100 in
Extended IP access-list:DynamicACL
   10 permit ip any 192.168.5.0 0.0.0.255 class 1
      Matched packets              :              4
   20 deny ip any 192.168.5.0 0.0.0.255
      Matched packets              :              0
   30 permit ip any 192.168.6.0 0.0.0.255 class 2
      Matched packets              :              0
   40 deny ip any 192.168.6.0 0.0.0.255
      Matched packets              :              4
   50 permit ip any any
      Matched packets              :            153
   Implicitly denied packets :              0

Using Interface:vlan 200 in
Extended IP access-list:DynamicACL
   10 permit ip any 192.168.5.0 0.0.0.255 class 1
      Matched packets              :              0
   20 deny ip any 192.168.5.0 0.0.0.255
      Matched packets              :              4
   30 permit ip any 192.168.6.0 0.0.0.255 class 2
      Matched packets              :              4
   40 deny ip any 192.168.6.0 0.0.0.255
      Matched packets              :              0
   50 permit ip any any
      Matched packets              :            120
   Implicitly denied packets :              0
```

VLAN100：「user01」

class 1 通過、class 2 廃棄

VLAN200：「user02」

class 2 通過、class 1 廃棄

2017 年 3 月 24 日　第 3 版発行
資料 No. NTS-07-R-042

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
川崎市幸区鹿島田一丁目 1 番 2 号 新川崎三井ビル西棟
http://www.alaxala.com/