

# Alaxala

## AX シリーズ 認証ソリューションガイド (RSA SecurID®編)

for  
the  
Guaranteed  
Network

(第2版)

## はじめに

AX シリーズ 認証ソリューションガイド(RSA SecurID® 編)は、AX シリーズと RSA SecurID のワンタイム・パスワード認証機能を連携したシステムを構築するための基本的な技術情報をシステムエンジニアの方へ提供し、各機能の動作概要の把握、システムの構築および安定稼動を目的として書かれています。

なお本書では RSA SecurID Appliance のバージョン 2.0 と 3.0 の両方の設定方法をそれぞれ解説しています。

### 関連資料

#### AX シリーズ

- AX シリーズ製品マニュアル
- AX シリーズ認証ソリューションガイド
- AX シリーズ認証ソリューションガイド マルチステップ認証編
- RADIUS サーバ設定ガイド(Windows Server 2003 編)
- AX1240S オプションライセンス設定ガイド
- AX3600S・AX2400S オプションライセンス設定ガイド

#### RSA SecurID

- RSA SecurID® Appliance 2.0 オーナー ガイド
- RSA SecurID® Appliance 3.0 オーナー ガイド
- RSA Authentication Manager® 6.1 管理者ガイド
- RSA Authentication Manager® 7.1 管理者ガイド
- RSA RADIUS Server 6.1 管理者ガイド
- RSA Authentication Manager® 7.1 RADIUS リファレンスガイド

### 本資料使用上の注意事項

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を確認したものであり、機能・性能・信頼性についてあらゆる環境条件すべてにおいて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。

本資料作成時の OS ソフトウェアバージョンは特記の無い限り以下となっております。

AX1240S      Ver2.1      ソフトウェアオプションライセンス (OP-OTP)

AX2430S      Ver11.1.A      ソフトウェアオプションライセンス (OP-OTP)

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

本資料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ください。

### 商標一覧

- アラクサラの名称およびロゴマークは、アラクサラネットワークス株式会社の商標および商登録です。
- RSA、SecurID は、RSA Security Inc. の登録商標です。
- 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。
- 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。
- 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。

### 使用機器一覧

- AX1240S (Ver2.1)
- AX2430S (Ver11.1.A)
- AX3630S (Ver11.1.A)
- Windows XP SP2
- Windows Vista SP1
- RSA SecurID Appliance 3.0
- RSA SecurID Appliance 2.0
- RSA SecurID SID700
- RSA SecurID Token for Windows Desktops Ver4.0

### 改訂履歴

版数	rev.	日付	変更内容	変更箇所
初版	—	2009.4.21	初版発行	—
第 2 版	—	2009.8.19	<p>使用機器の追加</p> <ul style="list-style-type: none"> <li>・RSA SecurID Appliance 3.0 を追加。</li> <li>・認証スイッチとして AX2430S を追加。</li> </ul> <p>AX シリーズの OS のバージョンアップに対応</p> <ul style="list-style-type: none"> <li>・AX1240S (Ver2.0) から (Ver2.1)</li> <li>・AX3630S (Ver10.1) から (Ver11.1.A)</li> </ul> <p>AX シリーズのバージョンアップによりサポートされた機能を取り入れ「1.2.2 特徴」を一部追加。</p> <p>「3 章」プリンタ等の非認証端末の扱いを変更。 認証除外端末として登録する方法から MAC 認証を行うシステム構築例に変更。</p> <p>Appliance の追加に伴い「RSA SecurID Appliance の設定」を「3.5 RSA SecurID Appliance 2.0 の設定」と「3.6 RSA SecurID Appliance 3.0 の設定」に変更。</p> <p>「4.4 Next token モード時の認証手順」を一部変更。</p> <p>「付録：コンフィグレーションファイル」にて AX2430S のコンフィグレーションを追加</p>	<p>本ガイド 全般</p> <p>1.2.2</p> <p>3 章</p> <p>3.5、3.6</p> <p>4.4</p> <p>付録</p>

# 目次

<b>1. 概要</b> .....	<b>6</b>
1.1 RSA SecurIDについて .....	6
1.1.1 特徴 .....	6
1.1.2 ワンタイム・パスワード .....	6
1.1.3 二要素による本人認証 .....	7
1.1.4 トークン .....	8
1.1.5 RSA SecurID Appliance .....	9
1.1.6 ネットワーク認証に関連するRSA SecurIDの機能 .....	9
1.2 AXシリーズとの連携 .....	10
1.2.1 動作概要 .....	10
1.2.2 特徴 .....	11
1.2.3 AXシリーズのソフトウェアオプションライセンスについて .....	12
1.2.4 New PINモード対応シーケンス .....	12
1.2.5 Next tokenモード対応シーケンス .....	13
1.2.6 AXシリーズの認証モード .....	14
<b>2. サポート状況と収容条件</b> .....	<b>15</b>
2.1 サポート状況 .....	15
2.1.1 AXシリーズのRSA SecurID連携サポート状況 .....	15
2.2 収容条件 .....	15
2.2.1 最大認証端末数 .....	15
<b>3. システム構築例（固定VLANモード）</b> .....	<b>16</b>
3.1 認証システム構成機器一覧 .....	16
3.1.1 ネットワーク構成図（詳細） .....	17
3.1.2 認証スイッチのポート構成 .....	17
3.1.3 スwitchのVLAN定義 .....	18
3.2 設定ポイント .....	18
3.3 AXシリーズのコンフィグレーション .....	20
3.3.1 AX2430Sのコンフィグレーション .....	20
3.3.2 AX1240Sのコンフィグレーション .....	22
3.3.3 AX3630Sのコンフィグレーション .....	24
3.4 DNSサーバの設定 .....	25
3.5 RSA SecurID Appliance 2.0 の設定 .....	26
3.5.1 初期設定 .....	26
3.5.2 RSA Authentication Managerの設定 .....	27

3.5.3 RSA RADIUS Serverの設定 .....	35
3.6 RSA SecurID Appliance 3.0 の設定 .....	38
3.6.1 初期設定 .....	38
3.6.2 RSA RADIUS Serverの設定 .....	40
3.6.3 RSA Authentication Managerの設定 .....	43
3.7 MAC認証用RADIUSサーバの設定 .....	47
3.8 クライアント端末の設定 .....	47
3.8.1 ハードウェアトークン .....	47
3.8.2 ソフトウェアトークン .....	47
<b>4. クライアント認証手順 .....</b>	<b>48</b>
4.1 ハードウェアトークンを使用した認証手順 .....	48
4.2 ソフトウェアトークンを使用した認証手順 .....	50
4.3 New PINモード時の認証手順 .....	52
4.4 Next tokenモード時の認証手順 .....	55
<b>5. 動作確認方法 .....</b>	<b>56</b>
5.1 AXシリーズにおける確認方法 .....	56
5.1.1 #show web-authentication login .....	56
5.1.2 #show web-authentication logging .....	56
5.2 RSA Authentication Managerにおける確認方法 .....	56
5.2.1 リアルタイムログ (RSA SecurID Appliance 2.0) .....	56
5.2.2 リアルタイムログ (RSA SecurID Appliance 3.0) .....	57
<b>6. 注意事項 .....</b>	<b>58</b>
6.1 ソフトウェアオプションライセンス (OP-OTP) 無効時の注意事項 .....	58
<b>付録. コンフィグレーション .....</b>	<b>58</b>

# 1. 概要

## 1.1 RSA SecurID について

RSA SecurID とは、RSA セキュリティ株式会社が提供するワンタイム・パスワードによる認証システムです。専用のサーバソフトウェア「RSA Authentication Manager」と同期した「RSA SecurID 認証トークン」(以下トークンと略します)によって 60 秒ごとに生成されるランダムな数字(トークンコード)と本人だけが知る暗証番号(PIN)の二つの要素を組み合わせたワンタイム・パスワードによって本人認証を行います。

### 1.1.1 特徴

以下に RSA SecurID の特徴を示します。

- (1) 有効なパスワードは 60 秒ごとに変更されるため、パスワードの推測や盗聴などの不正行為に対して強力な本人認証を実現します。(ワンタイム・パスワード)
- (2) 本人だけが知る暗証番号(PIN)と自動的にパスワードを生成する機器とを組み合わせる二要素認証を採用しているため、パスワードや暗証番号などのように利用者が暗記しているだけの固定パスワードに比べてよりセキュアな認証を実現します。
- (3) 様々な環境に応じて形式を使い分けることが可能なトークンと、トークンに表示される数字を入力するシンプルな使い勝手。

### 1.1.2 ワンタイム・パスワード

RSA SecurID では認証のために一度しか使用できない使い捨てのパスワード(ワンタイム・パスワード)を利用します。トークンに表示される数字の羅列は 60 秒ごとに変化するため悪意のある第三者にパスワードを不正搾取されても一度使用したパスワードは無効となるので悪用されることはありません。図 1.1-1 にて時間により変化するトークンの使用イメージを示します。

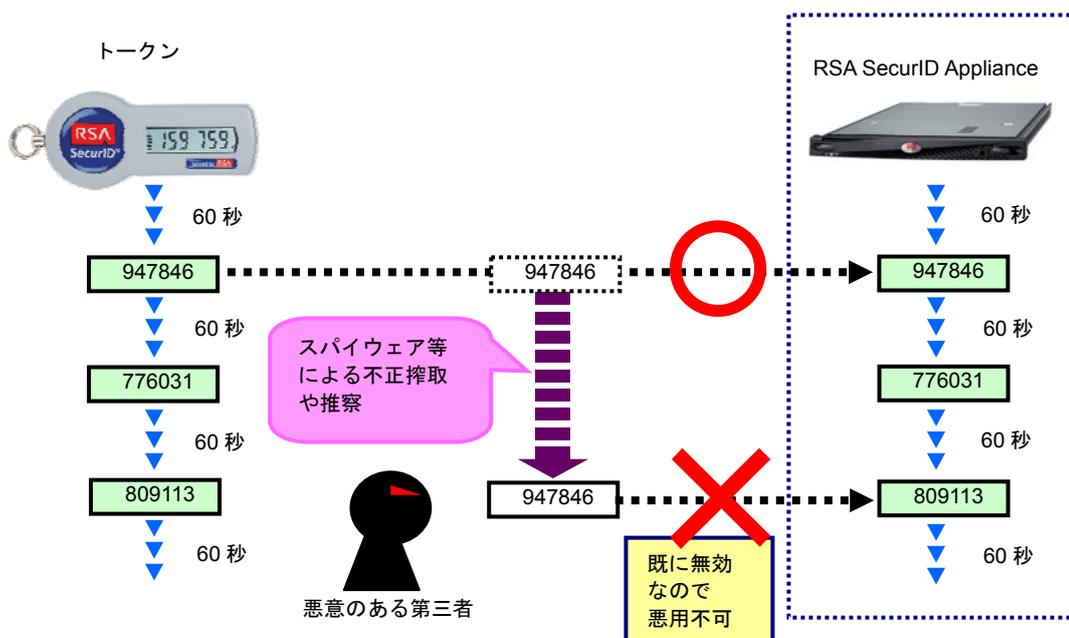


図 1.1-1 ワンタイム・パスワード

### 1.1.3 二要素による本人認証

RSA SecurID では本人だけが知る暗証番号 (PIN) とトークンにより 60 秒ごとに生成されるランダムな数字を組み合わせた二要素認証を採用しています。二要素を組み合わせて生成されるコードをパスコードと呼び認証時のパスワードとして使用します。

表 1.1-1 に二要素認証を構成するコードの名称と説明を示します。

表 1.1-1 RSA SecurID のコード名称

名称	説明
PIN	ユーザー本人だけが知る暗証番号。(4~8 桁の英数字)
トークンコード	トークンに表示され 60 秒経過すると変更されるランダムな数字。
パスコード	PIN コードとトークンコードの 2 つの要素の組み合わせ。(※1)

※1…トークンの種別によりパスコードの生成方法は複数あります。トークン種別に関しては 1.1.4 トークンを参照して下さい。

以下の図 1.1-2 にユーザーがトークンを使用して二要素認証を行う場合のパスコード (パスワード) 生成手順を簡単に解説します。

- ① ユーザー「USER01」の PIN は「8984」で登録されています。
- ② トークンに表示されている 6 桁のトークンコード「159759」を確認します。
- ③ ユーザーの PIN+トークンコードの計 10 桁がパスコード「8984159759」となります。
- ④ 認証時にユーザーID「USER01」とパスコードである「8984159759」を入力します。

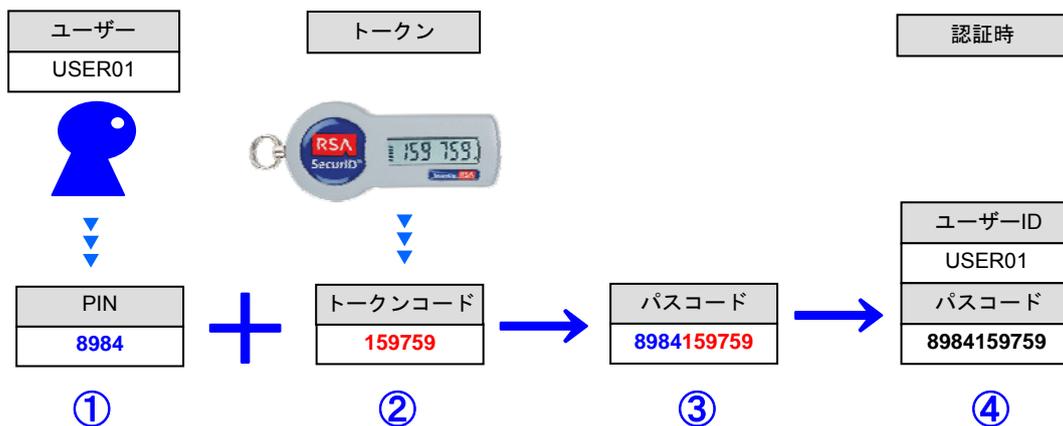


図 1.1-2 トークン使用時の二要素認証の例

### 1.1.4 トークン

トークンは利用者の環境に応じて複数の形式がラインナップされています。大きく別けて以下の2種類になります。本ガイド3章ではハードウェアトークンに「RSA SecurID SID700」、ソフトウェアトークンに「RSA SecurID Token for Windows Desktops Ver4.0」を使用した認証システムの構築方法を紹介しています。他の形式のトークンにつきましてはRSA セキュリティ (株) のホームページを参照して下さい。

#### (4) ハードウェアトークン

小型軽量タイプやデジタル証明書を格納した USB 接続タイプやクレジットカードサイズのカードタイプなどがあります。



図 1.1-3 RSA SecurID SID700

#### (5) ソフトウェアトークン

Windows 端末にインストールするタイプや携帯電話にインストールするタイプなどがあります。

 A screenshot of the RSA SecurID software token interface. It shows a window titled "My Token" with a dropdown menu and an "Options" button. The main area displays "Passcode:" followed by the number "7082 6883". Below the passcode are two buttons: "Re-enter PIN" and "Copy". The RSA SecurID logo is visible in the bottom left corner of the window.	<p>サポート OS</p> <ul style="list-style-type: none"><li>• Windows 2000 Professional(SP4 以降)</li><li>• Windows XP Professional(SP2 以降)</li><li>• Windows Vista Business</li><li>• Windows Vista Enterprise</li></ul>
--	--

図 1.1-4 RSA SecurID Token for Windows Desktops Ver4.0

### 1.1.5 RSA SecurID Appliance

RSA SecurID Appliance は、ワンタイム・パスワードのデファクト・スタンダードである SecurID による二要素認証が簡単に導入できるラックマウント型アプライアンス・サーバー製品です。

RSA SecurID Appliance には、認証サーバソフトウェアの RSA Authentication Manager がプリインストールされており、Windows デスクトップ認証を始めとする社内ネットワークの認証や VPN などのリモートアクセス認証、Web サービスの認証など、企業が求められるユーザー認証に幅広く対応します。

RSA SecurID Appliance のバージョンによりインストールできる RSA Authentication Manager のバージョンが変わります。本ガイドでは、RSA SecurID Appliance2.0 に RSA Authentication Manager6.1 を使用し、RSA SecurID Appliance3.0にはRSA Authentication Manager7.1を使用しています。

RSA SecurID Appliance3.0 では、RSA RADIUS Server が RSA Authentication Manager に統合されたことにより操作性が向上していますが、本ガイドでは既存の RSA SecurID Appliance2.0 ユーザーも対象に、RSA SecurID Appliance2.0 及び、RSA SecurID Appliance3.0 の設定方法を記載しています。

なお、本ソリューションガイドと関係しない Appliance3.0 の他の新機能については、RSA SecurID Appliance のマニュアル又は、RSA セキュリティ社のホームページを参照してください。

### 1.1.6 ネットワーク認証に関連する RSA SecurID の機能

ネットワーク認証を行う際に利用できる RSA SecurID の機能にて本ガイドで使用する機能を以下に紹介します。

#### (1) New PIN モード

New PIN モードとは認証時に使用する暗証番号 (PIN) をユーザが初めてアクセスする際に自身で登録することが出来る機能です。トークンを所持する利用者に PIN を登録してもらうことにより導入時の管理者の作業を軽減することができます。

#### (2) Next token モード

RSA SecurID はログインに 3 回失敗すると不正ログインがあるとみなし、Next token モードに移行します。Next token モードでは正しいパスワードで認証が成功しても 1 回では認証許可を出さずに次ぎのトークンコードの入力を要求します。

## 1.2 AX シリーズとの連携

AX シリーズのネットワーク認証と RSA SecurID のワンタイム・パスワードによる認証システムを連携する事により、通常のネットワーク認証よりもさらにセキュアな認証ネットワークを構築することができます。以下に AX シリーズの Web 認証と RSA SecurID のワンタイム・パスワードを連携させた認証システムの概要を紹介します。

### 1.2.1 動作概要

以下に AX シリーズの Web 認証と RSA SecurID のワンタイム・パスワードが連携した認証システムの動作概要と認証シーケンスを示します。ユーザーが Web 認証を行い認証成功後、業務サーバにアクセスする例の操作手順を解説します。

- ① ユーザーは認証スイッチ (AX シリーズ) 配下のクライアント端末からブラウザを起動し業務サーバなどに Web アクセスを行います。(任意の URL にアクセス)
- ② 認証スイッチ (AX シリーズ) は HTTP リダイレクト機能によりクライアント端末に Web 認証ログイン画面を表示します。ユーザーは自身のユーザーID とトークンを使用して生成されたパスコードを入力しログイン認証を実行します。
- ③ RSA SecurID Appliance は入力されたユーザーID とパスコードが正しかった場合認証スイッチを経由してクライアント端末に認証成功を通知します。
- ④ 認証に成功した端末は業務サーバにアクセス可能となります。

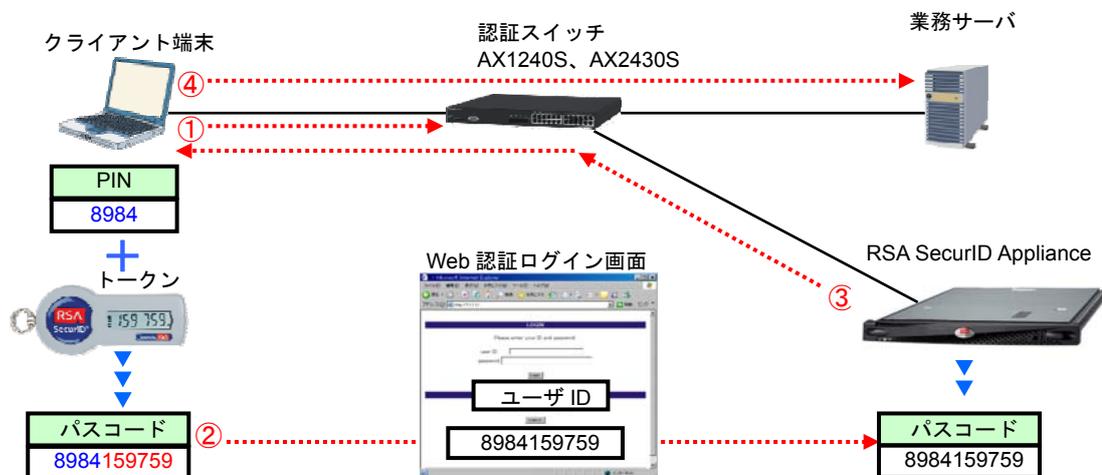


図 1.2-1 AX シリーズと RSA SecurID の動作概要

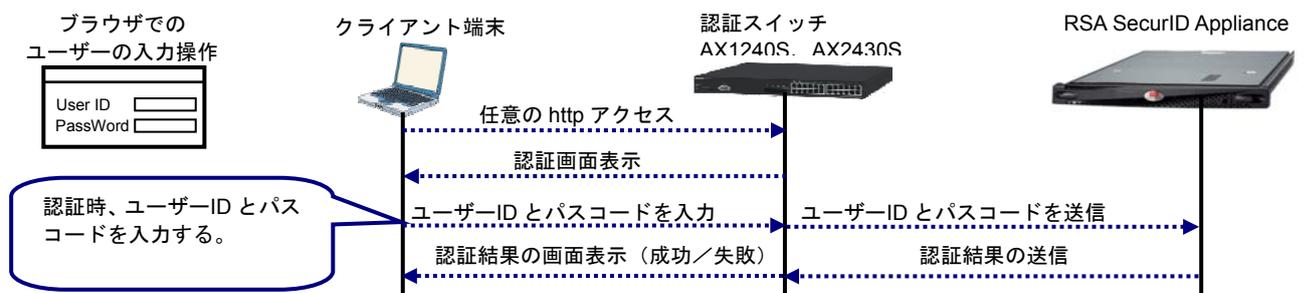


図 1.2-2 AX シリーズと RSA SecurID の Web 認証シーケンス

## 1.2.2 特徴

以下に AX シリーズの Web 認証と RSA SecurID が連携した認証システムの特徴を示します。

### (1) RSA SecurID が持つ独自の認証機能をサポート

- ユーザーが自身で PIN を登録できるため管理者の作業軽減が可能になる New PIN モードをサポート。
- ログインに 3 回失敗すると不正ログオンがあるとみなし、正しいパスコードで認証が成功しても 1 回では認証許可を出さずに次のトークンコードの入力を要求する Next token モードをサポート。

### (2) 認証モードの選択により導入環境に適した認証ネットワークを構築可能

- AX シリーズがサポートする 2 つの認証モード (固定 VLAN モード、動的 VLAN モード) それぞれにて RSA SecurID との連携が可能です。認証モードに関しては 1.2.6 AX シリーズの認証モードを参照して下さい。

### (3) ネットワーク認証環境下での RSA SecurID クライアントライセンス有効活用

- プリンタなどトークンを使用できない機器を AX シリーズにて認証除外端末として設定することで RSA SecurID のクライアントライセンスを消費することなくシステムを構築することができます。
- AX シリーズは認証方式毎に RADIUS サーバを指定する機能をサポートしています。プリンタなどトークンを使用できない機器を RSA SecurID とは別の RADIUS サーバで認証 (MAC 認証) することで RSA SecurID のクライアントライセンスを消費することなくシステムを構築することができます。

### (4) マルチステップ認証との併用が可能

- AX1240S がサポートするマルチステップ認証を組み合わせることにより機器認証 (MAC 認証) とユーザー認証 (ワンタイムパスワードを用いた Web 認証) の両方に成功した端末のみ通信を許可するため、より強固な認証システムの構築が可能です。  
構築の際は本書とあわせて「AX シリーズ認証ソリューションガイド マルチステップ認証編」を参照して下さい。

### 1.2.3 AX シリーズのソフトウェアオプションライセンスについて

RSA SecurID には、表 1.2-1 に示すようにトークンを使用したワンタイム・パスワード機能、New PIN モード、Next token モードの 3 つの機能があります。これら 3 つの機能と AX シリーズの Web 認証を連携させるためには、AX シリーズのワンタイム・パスワード認証機能 (OP-OTP) のソフトウェアオプションライセンスを購入し装置で有効にする必要があります。

なお、RSA SecurID のトークンを使用したワンタイム・パスワード機能と AX シリーズの Web 認証を連携させるだけなら、ソフトウェアオプションライセンスは無効でも動作します。

表 1.2-1 ワンタイム・パスワード認証機能 (OP-OTP) のサポートする機能範囲

機能内容	ソフトウェアオプションライセンス (OP-OTP)	
	有効	無効
ログイン時のトークンコード、PIN 入力	○	○
New PIN モード	○	—
Next token モード	○	—

(凡例) ○ : サポート — : 未サポート

AX シリーズごとの本ソフトウェアオプションライセンスのサポート状況は **2.1.1 AX シリーズの RSA SecurID 連携サポート状況** を参照して下さい。以降、本ガイドでは AX シリーズにワンタイム・パスワード認証機能 (OP-OTP) のソフトウェアオプションライセンスが有効になっていることを前提に書かれています。

### 1.2.4 New PIN モード対応シーケンス

図 1.2-2 にて AX シリーズの Web 認証と RSA SecurID の New PIN モードが連携する際の動作シーケンスを示します。ブラウザでの実際の画面遷移と操作手順は **4.3 New PIN モード時の認証手順** を参照して下さい。

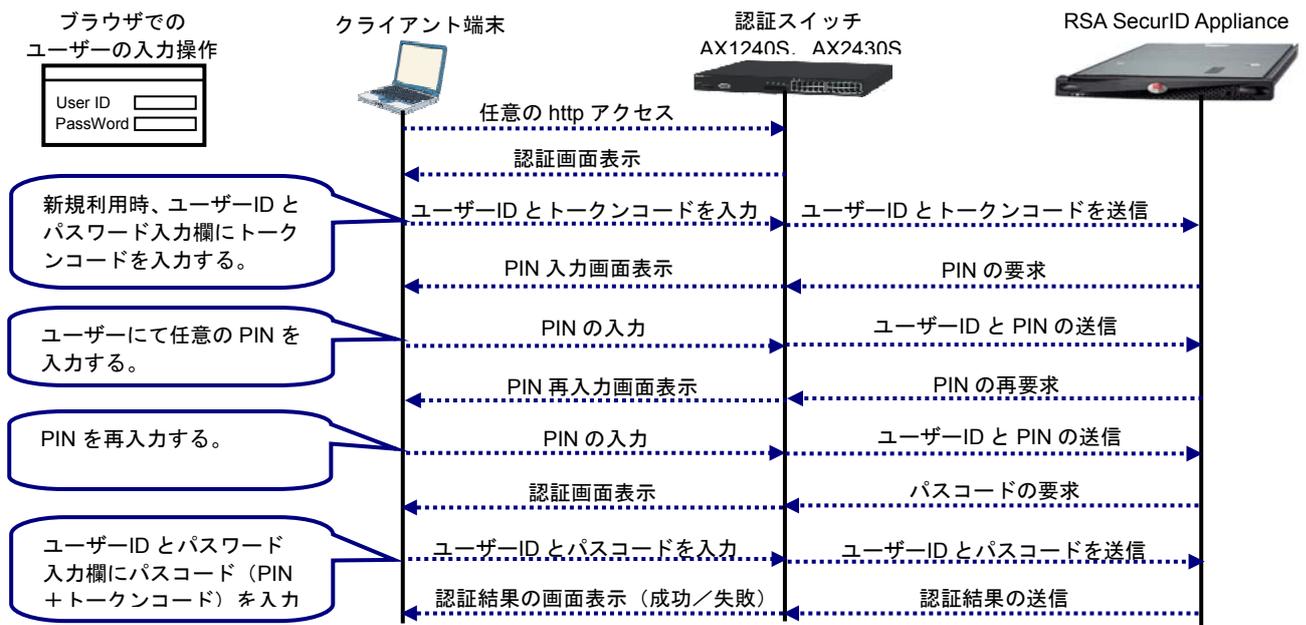


図 1.2-3 New PIN モード動作概要

### 1.2.5 Next token モード対応シーケンス

図 1.2-3 にてAXシリーズのWeb認証とRSA SecurIDのNext tokenモードが連携する際の動作シーケンスを示します。ブラウザでの実際の画面遷移と操作手順は4.4Next tokenモード時の認証手順を参照して下さい。

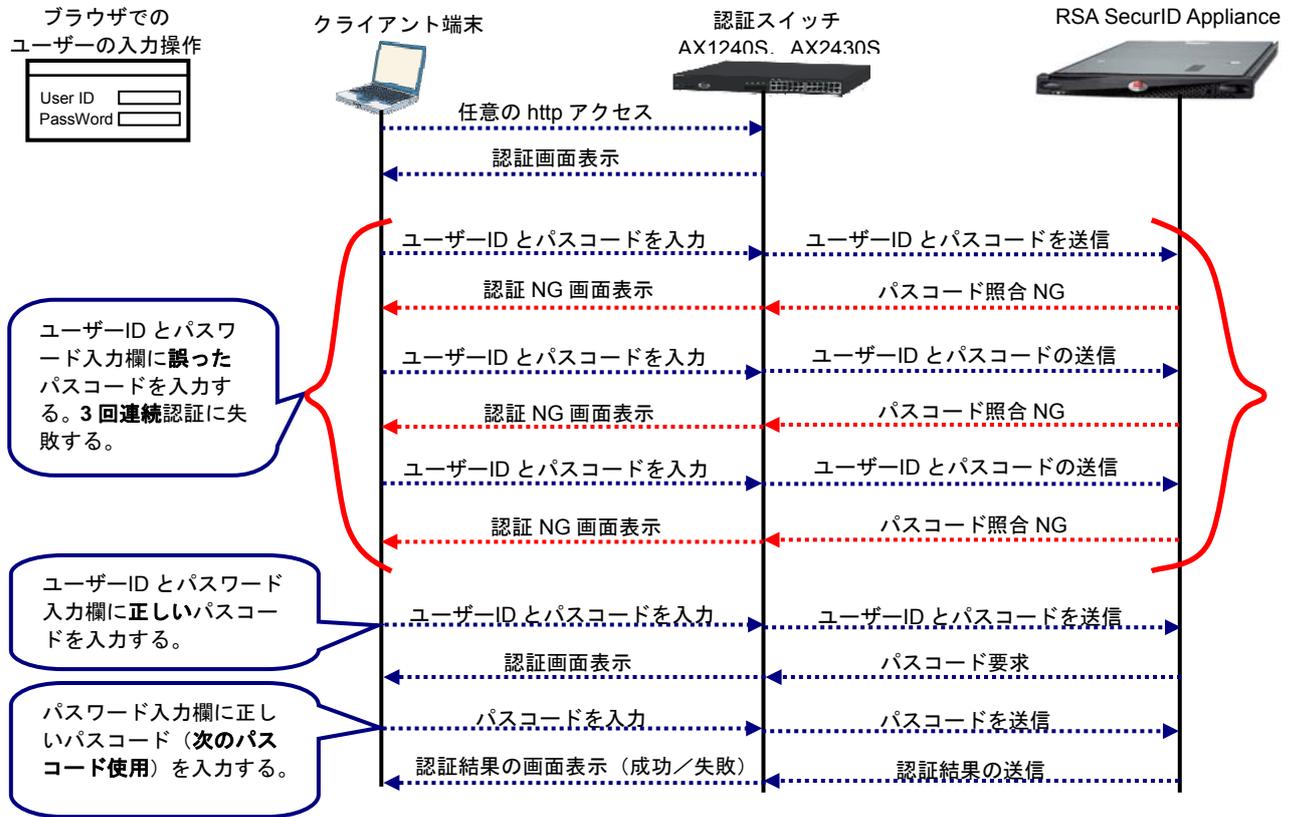


図 1.2-4 Next token モード動作概要

## 1.2.6 AX シリーズの認証モード

AX シリーズのネットワーク認証にはクライアント端末が認証成功後所属する VLAN (ネットワーク) に応じて、以下 2 種類の認証モードが存在します。RSA SecurID と連携する場合どちらの認証モードでも連携が可能です。認証モードの詳細な説明につきましては「AX シリーズ認証ソリューションガイド」や AX シリーズのマニュアルを参照して下さい。

### (1) 固定 VLAN モード

認証成功後もクライアント端末が所属する VLAN が変更しない認証モード。

AX シリーズがサポートする認証前アクセスリストを用いて認証可否に応じて通信を制御します。VLAN(ネットワーク)や IP アドレスの変更が発生しないため単純なネットワーク構築が可能です、そのため既存の環境に導入しやすいなどのメリットがあります。

⇒ 本ガイド 3 章にてシステム構築例を記載しています。

### (2) 動的 VLAN モード

認証成功時 RADIUS サーバの指示によりクライアント端末の所属する VLAN が変更する認証モード。

AX シリーズの MACVLAN を用いてユーザーごとに所属する VLAN を制御することが可能です。また所属する VLAN 単位にアクセスリストを設定することでよりきめ細かい認証ネットワークが構築可能です。

⇒ 動的 VLAN モードを構築する場合は本ガイドの「3.5.4 RSA RADIUS Server の設定」の (2) ポリシーの作成にて「動的 VLAN モードを使用する場合は…」を参照して RADIUS サーバの設定を追加してください。また AX シリーズの構成定義やネットワーク構築方法に関しては「AX シリーズ認証ソリューションガイド」の「3.3 動的 VLAN モードのネットワーク構築例」を参照して下さい。

## 2. サポート状況と収容条件

### 2.1 サポート状況

AX シリーズにて RSA SecurID と連携する際に関連する機能のサポート状況を以下に示します。

#### 2.1.1 AX シリーズの RSA SecurID 連携サポート状況

表 2.1-1 に RSA SecurID と連携する認証方式とソフトウェアオプションライセンス (OP-OTP) のサポート状況を AX シリーズごとに示します。

表 2.1-1 連携可能な AX シリーズ

認証方式	AX1230S	AX1240S	AX2400S、 AX3600S	AX6300S、 AX6700S
802.1X 認証	—	—	—	—
Web 認証	△	○	○	△
MAC 認証	—	—	—	—

(凡例) ○：連携可能、ソフトウェアオプションライセンス (OP-OTP) の購入が必要。

△：ログイン時のトークンコード、PIN 入力のみ連携可能。

—：連携不可

### 2.2 収容条件

AX シリーズにて RSA SecurID と連携する際に関連する収容条件を以下に示します。

#### 2.2.1 最大認証端末数

AX シリーズのサポートする各認証モードごとの最大認証端末数を以下に示します。RSA SecurID との連携に関しては赤枠で囲んだ Web 認証を確認してください。

表 2.2-1 認証モードごとの最大認証端末数

認証モード	認証方式	AX1200S		AX2400S、AX3600S		AX6300S、AX6700S	
		64/ポート 256/装置	合計 1024/ 装置	64/ポート 256/VLAN	合計 1024/ 装置	256/ポート 256/VLAN	合計 4096/ 装置
固定 VLAN モード	IEEE802.1X 認証	1024/装置		1024/装置		4096/装置	
	MAC 認証	1024/装置		1024/装置		4096/装置	
	Web 認証	1024/装置		1024/装置		4096/装置	
動的 VLAN モード	IEEE802.1X 認証	256/装置	合計 256/装置	256/装置 (*1)	合計 256/装置 (*1)	—	
	MAC 認証	256/装置		256/装置 (*1)		—	—
	Web 認証	256/装置		256/装置 (*1)		—	

(凡例) —：未サポート

(\*1) AX3640S では 1024/装置となります

### 3. システム構築例 (固定 VLAN モード)

本章ではAXシリーズのWeb認証(固定VLANモード)とRSA SecurIDのワンタイム・パスワードを連携させた認証システムの構築例をもとにAXシリーズのコンフィグレーション、RSA SecurIDやクライアント端末の設定などを解説しています。なおRSA SecurID Applianceの設定に関してはバージョンごとに設定方法を解説しています。使用するバージョンがRSA SecurID Appliance 2.0 の場合は3.5章を、RSA SecurID Appliance 3.0 の場合は3.6章を参照してください。

#### 3.1 認証システム構成機器一覧

以下に本章にて構築する認証システムの基本的なネットワーク構成図と構成機器一覧表を示します。

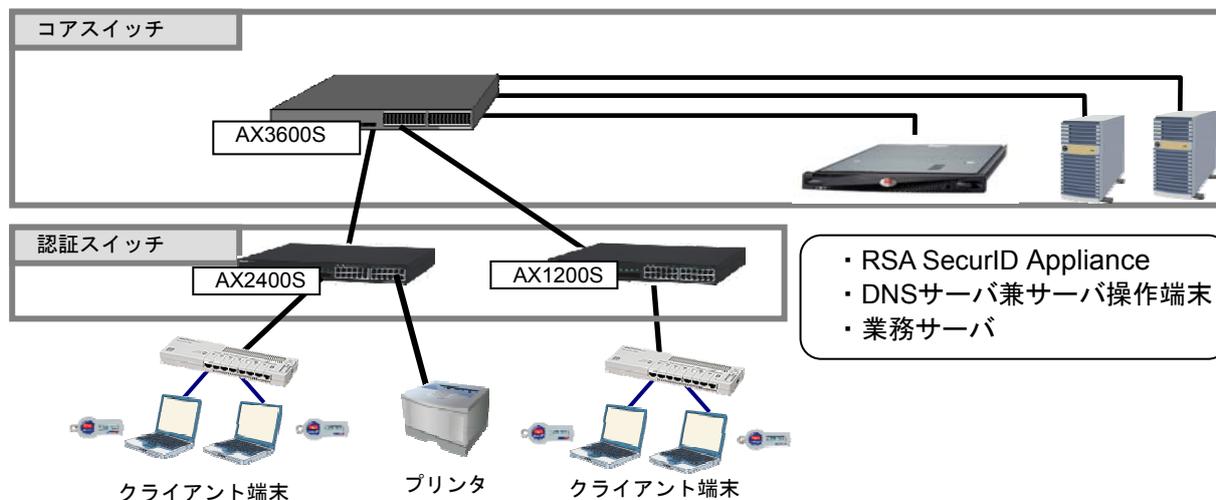


図 3.1-1 認証システム基本構成

本認証システムを構成する機器の用途と製品名及び使用バージョンを以下の表に示します。

表 3.1-1 認証システム構成機器一覧

役割	製品名		バージョン	備考
RSA SecurID Appliance	①	RSA SecurID Appliance 100	2.0	RSA SecurID Appliance はバージョンに応じて使用する機器が変わります。 RSA Authentication Manager 7.1 から RSA RADIUS Server を統合しています。
		ソフトウェア	RSA Authentication Manager	
	②	RSA SecurID Appliance 130	3.0	
		ソフトウェア	RSA Authentication Manager	
トークン	ハードウェアトークン	RSA SecurID SID700	—	トークンについては1.1.4トークンを参照して下さい。
	ソフトウェアトークン	RSA SecurID Token for Windows Desktops	4.0	
コアスイッチ DHCP サーバ	AX3630S		11.1.A	本システムで使用する DHCP サーバ
認証スイッチ	AX1240S、		2.1	Web 認証を行う
	AX2430S		11.1.A	
業務サーバ	—		—	認証に成功したクライアント端末のみ通信可能なサーバ
RADIUS サーバ DNS サーバ サーバ操作端末	OS	Windows Server 2003	SP1	MAC 認証用 RADIUS サーバ 本システムで使用する DNS サーバ RSA SecurID Appliance 操作端末
		Windows XP	SP2	
クライアント端末	OS	Windows Vista	SP1	
		—	—	
プリンタ	—		—	MAC 認証を行う。

(凡例) — : 特に指定しないもしくは指定が無い事を示します。

### 3.1.1 ネットワーク構成図(詳細)

AX シリーズの Web 認証 (固定 VLAN モード) と RSA SecurID のワンタイム・パスワードを連携した認証システムの詳細なネットワーク構成図を以下に示します。

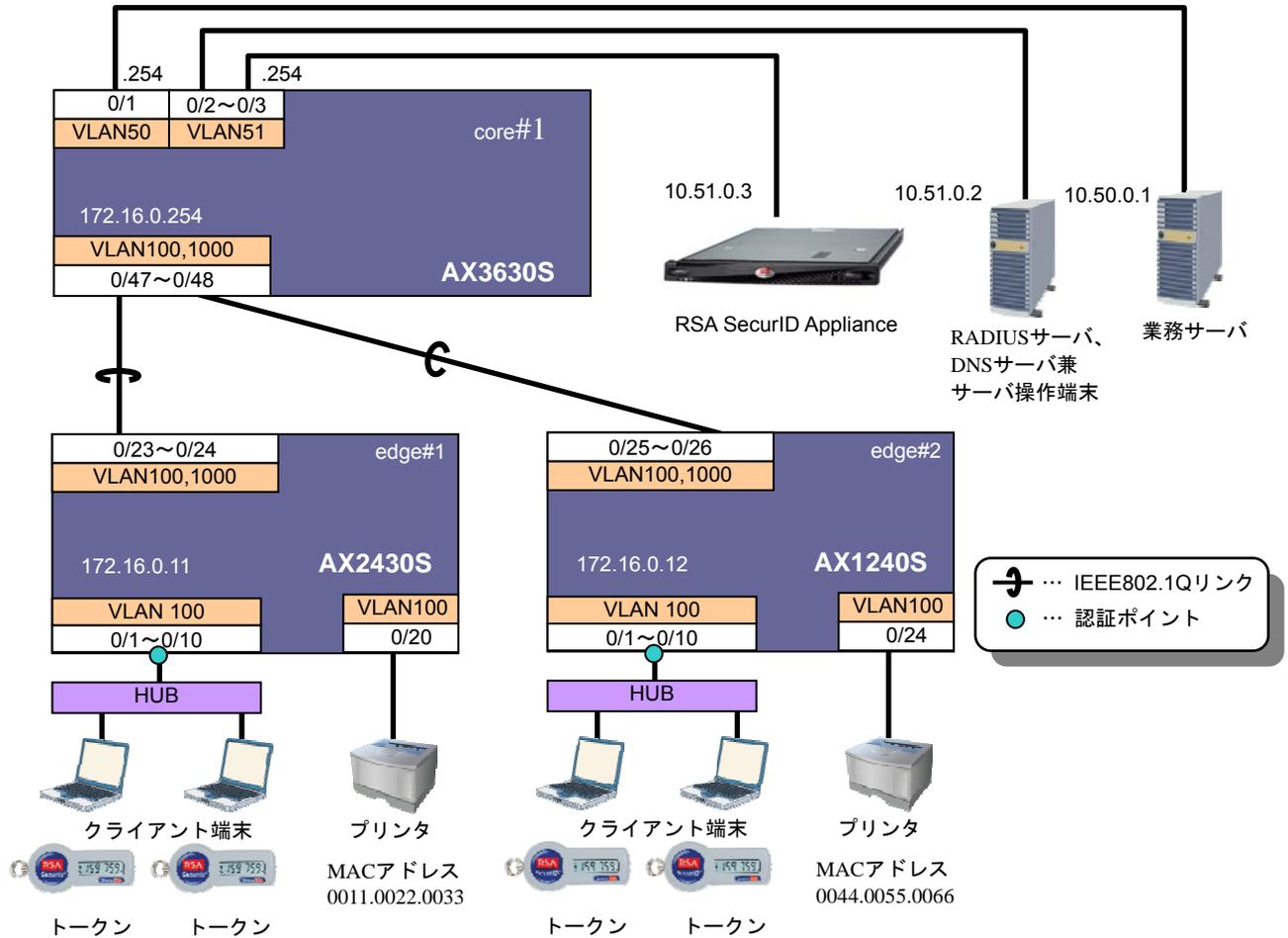


図 3.1-2 ネットワーク構成図 (詳細)

### 3.1.2 認証スイッチのポート構成

ここで、認証スイッチのポートを以下のように設定します。本構築例ではプリンタなどトークンを使用できない機器はMAC認証を行う設定としています。MAC認証の設定に関しては[3.2設定ポイント](#)を参照して下さい。

表 3.1-2 認証スイッチのポート構成

認証スイッチ	用途	ポート種別	VLAN	ポート番号	認証方式
AX2430S	認証用	アクセスポート	100	1~10	Web 認証
		アップリンク接続		トランクポート	20
AX1240S	認証用	アクセスポート	100	1~10	Web 認証
		アップリンク接続		トランクポート	25~26

### 3.1.3 スイッチの VLAN 定義

本構築例にて使用する VLAN の定義情報を表 3.2-3 に、クライアント端末の認証状態に応じた通信可否を表 3.2-4 に示します。

表 3.1-3 VLAN 定義

VLAN 名	VLAN-ID	ネットワーク IP アドレス	用途	設置サーバ
業務サーバ VLAN	50	10.50.0.0/24	認証が成功した端末と通信可能なサーバが所属する VLAN。(社内ネットワークなど)	業務サーバ
認証サーバ VLAN	51	10.51.0.0/24	RSA SecurID が所属する VLAN。	RSA SecurID
認証 VLAN	100	192.168.100.0/24	クライアント端末が所属する VLAN。	
管理用 VLAN	1000	172.16.0.0/24	各装置を管理するための VLAN。	

表 3.1-4 クライアント端末の認証状態に応じた通信可否

	業務サーバ	DHCP、DNS サーバ
認証成功端末	○	○
認証前、及び認証失敗端末	×	△

(凡例) ○：通信可能 ×：通信不可 △：一部プロトコル (DHCP、DNS) のみ通信可能

## 3.2 設定ポイント

図 3.1-2 のネットワーク構成図にて AX のコンフィギュレーションで設定のポイントを以下に示します。

### (1) オプションライセンスの確認

本ガイドでは New PIN モードと Next token モードを利用します。

AX シリーズの `#show license`(運用コマンド)にてソフトウェアオプションライセンス (OP-OTP) が有効であることを確認して下さい。

### (2) 認証前 ACL の作成

クライアント端末の認証前及び認証失敗時に以下 2 つの通信を許可するため、認証スイッチに認証前アクセスリストを定義します。

- ① 本ガイドではクライアント端末の IP アドレスを DHCP サーバより配布しています。そのためクライアント端末からの DHCP パケットを許可します。(クライアント端末の IP アドレスを固定する環境では本定義は不要です。)
- ② 認証前にクライアント端末からの名前解決を可能にします。クライアント端末から DNS サーバ宛、DNS クエリパケットを許可します。

### (3) トークンを使用したパスワード入力できない機器 (プリンタなど) の接続

トークンを使用したパスワード入力できない機器 (プリンタなど) の接続方法には以下の 2 種類あります。環境に合わせて選択して下さい。なお本ガイドでは①の MAC 認証を使用する方法を解説しています。

#### ①MAC 認証を使用する方法

トークンを使用できないプリンタなどを RSA SecurID とは別の RADIUS サーバで認証 (MAC 認証) します。3.3 AX シリーズのコンフィグレーションに MAC 認証のコンフィグレーションを記載しています。

#### ②認証除外端末を設定する方法

トークンを使用できないプリンタなどを認証除外端末として設定します。認証スイッチに以下のコマンドを設定してください。

```
(config)# mac-address-table static (端末のMACアドレス) vlan 100 interface fastethernet 0/24
```

### 3.3 AX シリーズのコンフィグレーション

本構成における、AXシリーズのコンフィグレーションの解説を下記に示します。またコンフィグレーションはテキストファイルにて添付しています。**付録**を参照して下さい。

#### 3.3.1 AX2430S のコンフィグレーション

edge#1 (AX2430S)の設定	
<b>事前設定</b>	
(config)# hostname "edge#1" (config)# clock timezone "JST" +9 0	ホスト名の設定をします。 タイムゾーンの設定をします。
<b>VLAN の定義</b>	
(config)# vlan 1 (config-vlan)# state suspend (config)# vlan 100,1000 (config-vlan)# state active	VLAN1は使用しないため、無効にします。  認証VLANとしてVLAN100を、管理用VLANとしてVLAN1000を作成します。
<b>スパンニングツリーの設定</b>	
(config)# spanning-tree disable	スパンニングツリーを無効にします。
<b>インターフェイスの設定</b>	
<b>物理ポートの設定</b>	
<ul style="list-style-type: none"> <li>● 認証用 (config)# interface range gigabitethernet 0/1-10 (config-if-range)# switchport access vlan 100 (config-if-range)# web-authentication port (config-if-range)# authentication ip access-group "WebAuth" (config-if-range)# authentication arp-relay</li> <li> </li> <li>(config)# interface gigabitethernet 0/20 (config-if-range)# switchport access vlan 100 (config-if-range)# mac-authentication port (config-if-range)# authentication arp-relay</li> <li> </li> <li>● アップリンク用 (config)# interface range gigabitethernet 0/23-24 (config-if-range)# switchport mode trunk (config-if-range)# switchport trunk allowed vlan 100, 1000</li> </ul>	<b>認証ポートの設定</b> ポート0/1~10をアクセスポートのVLAN100に設定します。 Web認証対象ポートの設定をします。 認証前アクセスリスト"WebAuth"を設定します。 認証前の端末から送信される他宛てARP パケットを認証対象外のポートへ出力させます。  ポート0/20をアクセスポートのVLAN100に設定します。 MAC認証対象ポートの設定をします。 認証前の端末から送信される他宛てARP パケットを認証対象外のポートへ出力させます。
<b>アップリンクポートの設定</b>	
ポート0/23~24をトランクポートに設定し、VLAN100、1000を設定します。	
<b>LAN インターフェイスの設定</b>	
(config)# interface vlan 100 (config-if)# ip address 192.168.100.11 255.255.255.0	認証用VLAN100にインタフェースIPアドレスを設定します。
(config)# interface vlan 1000 (config-if)# ip address 172.16.0.11 255.255.255.0	管理用VLAN1000にインタフェースIPアドレスを設定します。
<b>デフォルトルートの設定</b>	
(config)# ip default-gateway 172.16.0.1	RADIUSサーバと通信を行うため、デフォルトルートを設定します。

<b>アクセスリストの作成</b>	
<pre>ip access-list extended "WebAuth"  10 permit udp any any eq bootps  20 permit udp any any eq domain</pre>	<p>認証前アクセスリストとして定義する“WebAuth”を作成します。 DHCPパケットの許可を設定します DNSパケットの許可を設定します 設定ポイント (2)</p> <p>「認証前アクセスリストの設定」</p>
<b>Web 認証の設定</b>	
<pre>(config)# web-authentication system-auth-control (config)# web-authentication ip address 1.1.1.1  (config)# aaa authentication web-authentication default group radius</pre>	<p>Web認証を有効にします。 Web認証専用IPアドレスを設定します。本ガイドでは「1.1.1.1」としています。 RADIUSサーバでWeb認証を行うことを設定します。</p>
<b>MAC 認証の設定</b>	
<pre>(config)# mac-authentication system-auth-control (config)# mac-authentication radius-server host 10.51.0.2 key "alaxala" (config)# aaa authentication mac-authentication default group radius</pre>	<p>MAC認証を有効にします。 MAC認証専用RADIUSサーバのIPアドレスとシークレットキーを入力します。 RADIUSサーバでMAC認証を行うことを設定します。 設定ポイント (3)</p> <p>「MAC認証の設定」</p>
<b>RADIUS サーバの設定</b>	
<pre>(config)# radius-server host 10.51.0.3 key "alaxala"</pre>	<p>RADIUSサーバのIPアドレス、認証ポート番号およびキーを設定します。</p>

## 3.3.2 AX1240S のコンフィグレーション

edge#1 (AX1240S)の設定	
<b>事前設定</b>	
<pre>(config)# system function filter extended-authentication  (config)# hostname "edge#1" (config)# clock timezone "JST" +9 0</pre>	<p>フィルタ機能と拡張認証機能を使用するため、システムファンクションリソース配分を変更します。</p> <p><b>※設定後は、装置の再起動が必要です。</b></p> <p>ホスト名の設定をします。 タイムゾーンの設定をします。</p>
<b>VLAN の定義</b>	
<pre>(config)# vlan 1 (config-vlan)# state suspend (config)# vlan 100,1000 (config-vlan)# state active</pre>	<p>VLAN1は使用しないため、無効にします。</p> <p>認証VLANとしてVLAN100を、管理用VLANとしてVLAN1000を作成します。</p>
<b>スパンニングツリーの設定</b>	
<pre>(config)# spanning-tree disable</pre>	<p>スパンニングツリーを無効にします。</p>
<b>インターフェイスの設定</b>	
<b>物理ポートの設定</b>	
<p>●認証用</p> <pre>(config)# interface range fastethernet 0/1-10 (config-if-range)# switchport access vlan 100 (config-if-range)# web-authentication port (config-if-range)# authentication ip access-group "WebAuth" (config-if-range)# authentication arp-relay  (config)# interface fastethernet 0/24 (config-if-range)# switchport access vlan 100 (config-if-range)# mac-authentication port (config-if-range)# authentication arp-relay</pre> <p>●アップリンク用</p> <pre>(config)# interface range gigabitethernet 0/25-26 (config-if-range)# switchport mode trunk (config-if-range)# switchport trunk allowed vlan 100,1000</pre>	<p><b>認証ポートの設定</b></p> <p>ポート0/1~0/10をアクセスポートのVLAN100に設定します。</p> <p>Web認証対象ポートの設定をします。 認証前アクセスリスト“WebAuth”を設定します。 認証前の端末から送信される他宛てARP パケットを認証対象外のポートへ出力させます。</p> <p>ポート0/24をアクセスポートのVLAN100に設定します。</p> <p>MAC認証対象ポートの設定をします。 認証前の端末から送信される他宛てARP パケットを認証対象外のポートへ出力させます。</p> <p><b>アップリンクポートの設定</b></p> <p>ポート0/25~0/26をトランクポートに設定し、VLAN100、1000を設定します。</p>
<b>VLAN インターフェイスの設定</b>	
<pre>(config)# interface vlan 100 (config-if)# ip address 192.168.100.12 255.255.255.0  (config)# interface vlan 1000 (config-if)# ip address 172.16.0.12 255.255.255.0</pre>	<p>認証用VLAN100にインターフェイスIPアドレスを設定します。</p> <p>管理用VLAN1000にインターフェイスIPアドレスを設定します。</p>
<b>デフォルトルートの設定</b>	
<pre>(config)# ip route 0.0.0.0 0.0.0.0 172.16.0.1</pre>	<p>RADIUSサーバと通信を行うため、デフォルトルートを設定します。</p>

<b>アクセスリストの作成</b>	
<pre>ip access-list extended "WebAuth"  10 permit udp any any eq bootps  20 permit udp any any eq domain</pre>	<p>認証前アクセスリストとして定義する“WebAuth”を作成します。 DHCPパケットの許可を設定します DNSパケットの許可を設定します 設定ポイント (2)</p> <p>「認証前アクセスリストの設定」</p>
<b>Web 認証の設定</b>	
<pre>(config)# web-authentication system-auth-control (config)# web-authentication ip address 1.1.1.1  (config)# aaa authentication web-authentication default group radius</pre>	<p>Web認証を有効にします。 Web認証専用IPアドレスを設定します。本ガイドでは「1.1.1.1」としています。 RADIUSサーバでWeb認証を行うことを設定します。</p>
<b>MAC 認証の設定</b>	
<pre>(config)# mac-authentication system-auth-control (config)# mac-authentication id-format 1  (config)# mac-authentication radius-server host 10.51.0.2 key "alaxala"  (config)# aaa authentication mac-authentication default group radius</pre>	<p>MAC認証を有効にします。 RADIUSサーバへ認証要求する際のMACアドレス形式を1に設定します。 MAC認証専用RADIUSサーバのIPアドレスとシークレットキーを入力します。</p> <p>RADIUSサーバでMAC認証を行うことを設定します。 設定ポイント (3)</p> <p>「MAC認証の設定」</p>
<b>RADIUS サーバの設定</b>	
<pre>(config)# radius-server host 10.51.0.3 key "alaxala"</pre>	<p>RADIUSサーバのIPアドレス、およびシークレットキーを設定します。</p>

## 3.3.3 AX3630S のコンフィグレーション

core#1 (AX3630S)の設定	
<b>事前設定</b>	
(config)# hostname "core#1" (config)# clock timezone JST +9 0	ホスト名の設定をします。 タイムゾーンの設定をします。
<b>VLAN の定義</b>	
(config)# vlan 1 (config-vlan)# state suspend (config)# vlan 50,51,100,1000 (config-vlan)# state active	VLAN1 は使用しないため、無効にします。 各 VLAN50,51,100,1000 を作成します。
<b>スパンニングツリーの設定</b>	
(config)# spanning-tree disable	スパンニングツリーを無効にします。
<b>インターフェイスの設定</b>	
<b>物理ポートの設定</b>	
<ul style="list-style-type: none"> <li>●業務サーバ用 (config)# interface gigabitethernet 0/1 (config-if-range)# switchport access vlan 50</li> <li>●認証サーバ (RSA SecurID) 用 (config)# interface range gigabitethernet 0/2-3 (config-if-range)# switchport access vlan 51</li> <li>●認証スイッチ用 (config)# interface range gigabitethernet 0/47-48 (config-if-range)# switchport mode trunk (config-if-range)# switchport trunk allowed vlan 100,1000</li> </ul>	<b>業務サーバ用ポートの設定</b> ポート 0/1 をアクセスポートの VLAN50 に設定します。  <b>認証サーバ (RSA SecurID) 用ポートの設定</b> ポート 0/2~0/3 をアクセスポートの VLAN51 に設定します。  <b>認証スイッチ用ポートの設定</b> ポート 0/47~0/48 をトランクポートに設定し、VLAN100、1000 を設定します。
<b>VLAN インターフェイスの設定</b>	
(config)# interface vlan 50 (config-if)# ip address 10.50.0.1 255.255.255.0  (config)# interface vlan 51 (config-if)# ip address 10.51.0.1 255.255.255.0  (config)# interface vlan 100 (config-if)# ip address 192.168.100.1 255.255.255.0  (config)# interface vlan 1000 (config-if)# ip address 172.16.0.1 255.255.255.0	業務サーバ用 VLAN50 にインタフェース IP アドレスを設定します。  認証サーバ (RSA SecurID) 用 VLAN51 にインタフェース IP アドレスを設定します。  認証用 VLAN100 にインタフェース IP アドレスを設定します。  管理用 VLAN1000 にインタフェース IP アドレスを設定します。
<b>DHCP サーバの設定</b>	
(config)# ip dhcp pool VLAN100 (dhcp-config)# network 192.168.100.0/24 (dhcp-config)# lease 0 8 0 0 (dhcp-config)# dns-server 10.51.0.2 (dhcp-config)# default-router 192.168.100.1  (config)# service dhcp vlan 100	DHCP アドレスプール "VLAN100" を設定します。 配布するネットワーク IP アドレスを設定します。 リース時間を 8 時間に設定します。 配布する DNS サーバの IP アドレスを設定する 配布するデフォルトルートを設定します。  VLAN100 で DHCP サービスを開始します。

### 3.4 DNS サーバの設定

本ガイドでは DNS サーバの設定方法の記載を省いています。構築環境で以下の動作となるように DNS サーバのセットアップをしてください。

本構築例では AX シリーズの Web 認証で HTTP リダイレクト機能を使用しています。クライアント端末からの任意の Web アクセスに対し認証画面を表示させるため、認証前のクライアント端末から名前解決が成功する環境にしてください。

### 3.5 RSA SecurID Appliance 2.0 の設定

本環境を構築するためにRSA SecurID Appliance 2.0 で必要な設定を以下の3つのステップに別け設定方法を順に紹介します。なおRSA SecurID Appliance 3.0 を使用して本環境を構築する場合は**3.6 RSA SecurID Appliance 3.0 の設定**を参照して下さい。

#### (1) 初期設定

ライセンスの割り当てやシステムに関する初期設定、DNS サーバの設定を行います。

#### (2) RSA Authentication Manager の設定

本環境で認証に使用するユーザー登録やトークンの設定を行います。

#### (3) RSA RADIUS Server の設定

本認証ネットワークにて RADIUS サーバの設定を示します。

#### 3.5.1 初期設定

- RSA SecurID Appliance 2.0 の設定をするためにはまず初期設定が必要です。初期設定はサーバ操作端末を RSA SecurID Appliance 2.0 に接続し、ブラウザから Web 画面を操作して以下の設定を行います。設定手順は RSA SecurID® Appliance 2.0 オーナー ガイド「第2章：セットアップと構成」の「Appliance のセットアップ」を参照して下さい。

- ① 時刻設定
- ② 管理者 (administrator) のパスワード設定
- ③ ネットワーク情報の設定
- ④ ライセンスファイルのアップロード
- ⑤ トークンレコードのインポート
- ⑥ 管理者 (administrator) へトークン割り当て
- ⑦ RSA RADIUS Server のインストール

##### ①について

時刻設定に関して本構成ではインターネット接続を想定していない為 NTP を使用していません。可能であれば time.nist.gov などのインターネットタイムサーバを利用することをお勧めします。

##### ③について

本構築例のネットワーク設定を表 3.5-1 に示します。構築する環境に合わせて設定をして下さい。

表 3.5-1 RSA SecurID Appliance ネットワーク設定

項番	項目	設定値	備考
1	IP アドレス	10.51.0.3	本装置の IP アドレス
2	サブネットマスク	255.255.255.0	
3	デフォルトゲートウェイ	10.51.0.1	本構築例では L3 スイッチの IP アドレス
4	DNS サーバ	10.51.0.2	
5	ホスト名	Securid.example.co.jp	任意のホスト名

##### ⑦について

本構築例では RADIUS サーバとして RSA SecurID Appliance 2.0 に RSA RADIUS Server をインストールしています。インストール方法に関しましては「RSA RADIUS Server 6.1 管理者ガイド」第2章「RSA RADIUS Server のインストール」を参照してください。

### 3.5.2 RSA Authentication Manager の設定

本環境を構築するためのAuthentication Managerで行う設定を以下に示します。本ガイドでは**3.6.1初期設定**と同様に操作端末のブラウザからRSA SecurID Appliance2.0 にリモートデスクトップWeb接続にてサーバの設定を行っています。

- **(1)Agent Hostの登録**  
認証スイッチを Agent Host として登録します。
- **(2)認証ユーザーの作成**  
認証ユーザーを登録します。
- **(3)トークンの割り当て**  
認証ユーザーにトークンを割り当てます。
- **(4)Agent Hostの割り当て**  
認証ユーザーに Agent Host を割り当てます。
- **(5)認証ユーザーのPIN登録**  
認証ユーザーの PIN を登録します。  
※ New PIN モードを使用して認証ユーザーの PIN を登録する場合は本設定を行う必要はありません。引き続き RSA Authentication Manager の設定を進めて下さい。

#### (1) Agent Host の登録

①操作端末から RSA SecurID Appliance2.0 にリモートデスクトップ Web 接続を行い、RSA SecurID Appliance2.0 上の Windows Server 2003 にて「スタート」→「RSA Authentication Manager Host Mode」を起動します。メインメニューから「Agent Host」を展開し「Add Agent Host」をクリックします。「Add Agent Host」画面にて表 3.4-2 を参照して項目の入力、または選択します。



図 3.5-1 RSA Authentication Manager の設定 1

表 3.5-2 Agent Host の設定

項番	項目	値	備考
1	Name	AX1240S	任意の名前
2	Network address	172.16.0.12	認証スイッチの IP アドレス
3	Agent type	Communication Server	

※上記設定と同じ手順で AX2430S も追加してください。

②その他の項目はデフォルトのまま「OK」ボタンをクリックし閉じます。

## (2) 認証ユーザーの作成

①メインメニューから「User」を展開し「Add User」をクリックします。「Add User」画面で「First and Last Name:」と「Default Login:」の項目を入力して下さい。

(本構築例では図 3.4-2 のように「user01」「alaxala」を登録しています。)

図 3.5-2 RSA Authentication Manager の設定 2

## (3) トークンの割り当て

①「Add User」画面にてユーザー名を入力後「Assign Token」ボタンをクリックして下さい。するとデータベースに対するユーザー登録の確認画面が表示されますので「OK」クリックして下さい。

図 3.5-3 RSA Authentication Manager の設定 3

②次に「Select Token」画面が表示されます。「Select Token from List」ボタンをクリックしてください。



図 3.5-4 RSA Authentication Manager の設定 4

③続けて新しい「Select Token」画面が表示されます。リスト表示されているトークンからユーザーに割り当てるトークンのシリアル番号を選択し「OK」ボタンをクリックします。

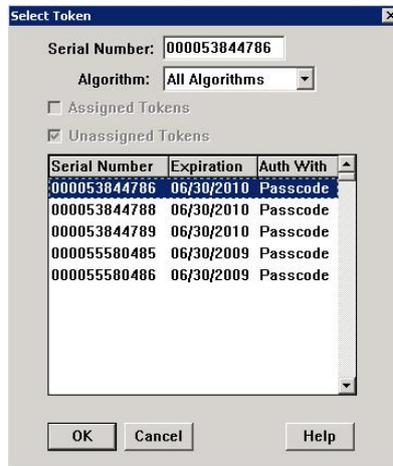


図 3.5-5 RSA Authentication Manager の設定 5

④戻ると「Edit User」画面になっています、中央の「Tokens : 」に選択したトークンが割り当てられたことを確認します。



図 3.5-6 RSA Authentication Manager の設定 6

#### (4) Agent Host の割り当て

- ① トークンの割り当てが完了したら「Edit User」画面の「Agent Hosts Activations」ボタンをクリックします。「Agent Hosts Activations」画面左に**(1)Agent Hostの登録**にて作成したAgent Host名を選択して「Activate On Agent Host」ボタンをクリックして下さい。  
 (本構築例では“AX1240S”という名前のAgent Hostを割り当てます)

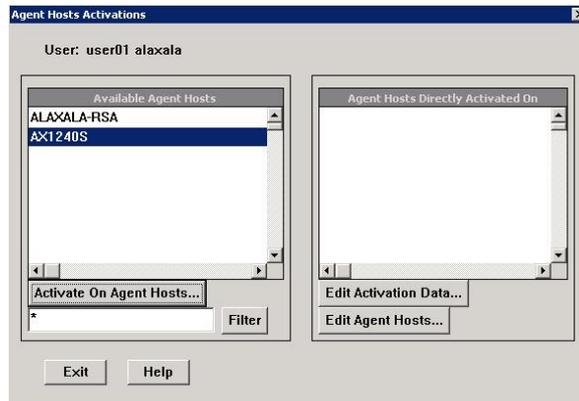


図 3.5-7 RSA Authentication Manager の設定 7

- ② 「Activate User」画面の「Login:」に割り当てるユーザーが選択されている事を確認して「OK」ボタンをクリックします。(本構築例では“User01”)

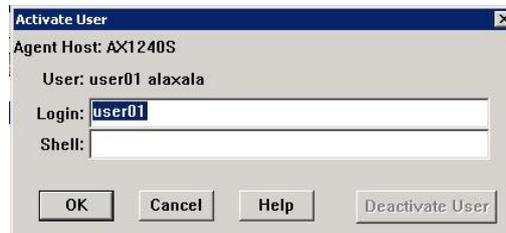


図 3.5-8 RSA Authentication Manager の設定 8

- ③ 「Agent Hosts Activations」の右画面にAgent Hostが追加されていることを確認して左下の「Exit」ボタンで閉じます。「Edit User」画面も左下「OK」ボタンで閉じてください。

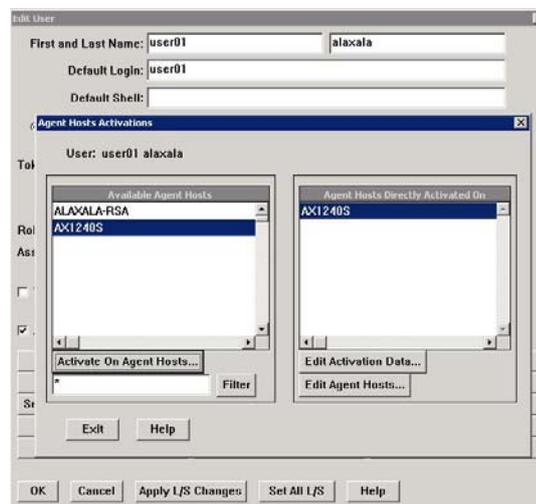


図 3.5-9 RSA Authentication Manager の設定 9

## (5) 認証ユーザーの PIN 登録

- トークンを割り当てた認証ユーザーに対して PIN の登録を行います。本ガイドでは認証ユーザーの PIN の登録方法を以下 2 種類示しています。構築する環境や運用ルールに応じて登録方法を選択して下さい。PIN の登録やオプションに関しては「RSA Authentication Manager 6.1 管理者ガイド」の第 6 章「PIN に関するオプション」を参照して下さい。

### (1) システム管理者が認証ユーザーの PIN を登録する方法

### (2) New PIN モードを使用して認証ユーザーが自身で PIN を登録する方法

#### (1) システム管理者が認証ユーザーの PIN を登録する方法

管理者がユーザーの PIN を登録することにより、トークンを渡されたユーザーはすぐに認証を行うことができます。New PIN モードを使用できない環境ではこの方法を選択して下さい。以下に設定手順を示します。

- ①メインメニュー「token」を展開して「Edit Token」をクリックしてください。続けて新しい「Select Token」画面が表示されます。リスト表示されているトークンから PIN を登録するユーザーに割り当てたトークンのシリアル番号を選択し「OK」ボタンをクリックします。

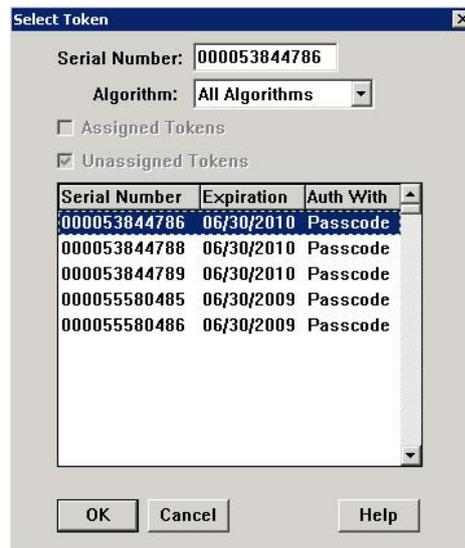


図 3.5-10 RSA Authentication Manager の設定 10

② 「Edit Token」画面が表示されたら「Set PIN to Next Tokencode...」をクリックして下さい。

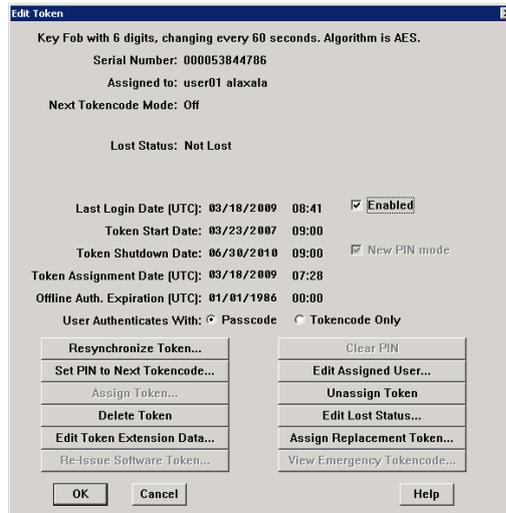


図 3.5-11 RSA Authentication Manager の設定 11

③ 「Set PIN to Next Tokencode」画面の入力欄にシリアル NO に該当するトークンのトークンコードを入力して「OK」ボタンをクリックして下さい。



図 3.5-12 RSA Authentication Manager の設定 12

④ PIN の登録が完了し以下の画面が表示されます。登録された PIN はトークンに表示される次のトークンコードの最初の 4 桁の数字です。

(例、次のトークンコードが“032843”であれば“0328”がユーザーの PIN となります。)



図 3.5-13 RSA Authentication Manager の設定 13

⑤ 以上で認証ユーザーの PIN の登録は完了です。「OK」ボタンで画面を閉じて下さい。

## (2) New PIN モードを使用して認証ユーザーが自身で PIN を登録する方法

本システムではトークンが割り当てられたユーザーはデフォルトで「New PIN モード」となります。New PIN モードを使用して認証ユーザーが自身の PIN を登録する場合 RSA Authentication Manager では特別な設定はございません。

→4.3New PINモード時の認証手順を参照してユーザー自身でPINを登録して下さい。

なお一度 PIN を登録したユーザーが New PIN モードを使用して PIN の再登録を行うには以下の設定を行って下さい。

①メインメニュー「token」を展開して「Edit Token」をクリックしてください。続けて新しい「Select Token」画面が表示されます。リスト表示されているトークンから PIN を登録するユーザーに割り当てたトークンのシリアル番号を選択し「OK」ボタンをクリックします。

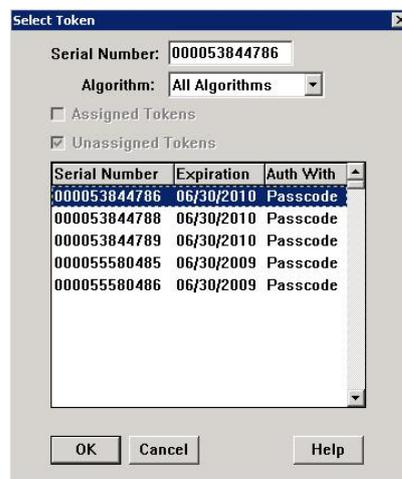


図 3.5-14 RSA Authentication Manager の設定 14

②「Edit Token」画面が表示されたら「New PIN mode」のチェックが外れていることを確認して「Clear PIN」をクリックして下さい。

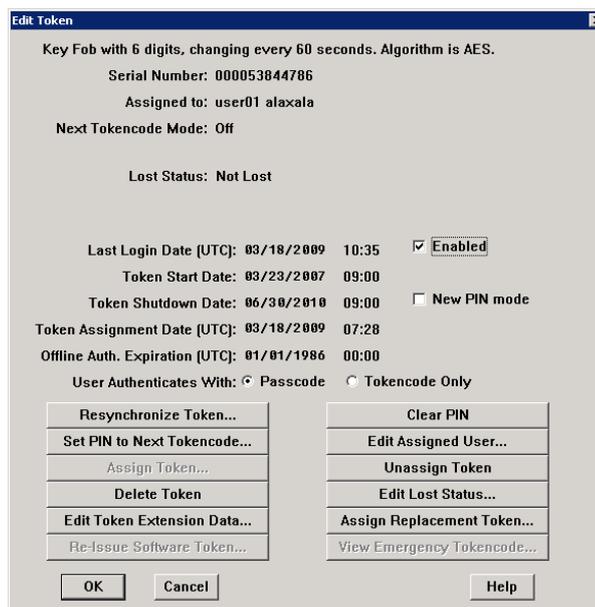


図 3.5-15 RSA Authentication Manager の設定 15

③ 「Clear PIN」がグレイアウト、「New PIN mode」にチェックが入りグレイアウトしている事を確認して「OK」ボタンで閉じて下さい。この状態でユーザーはNew PINモードを使用してPINの登録が可能です。**4.3New PINモード時の認証手順**を参照して下さい。

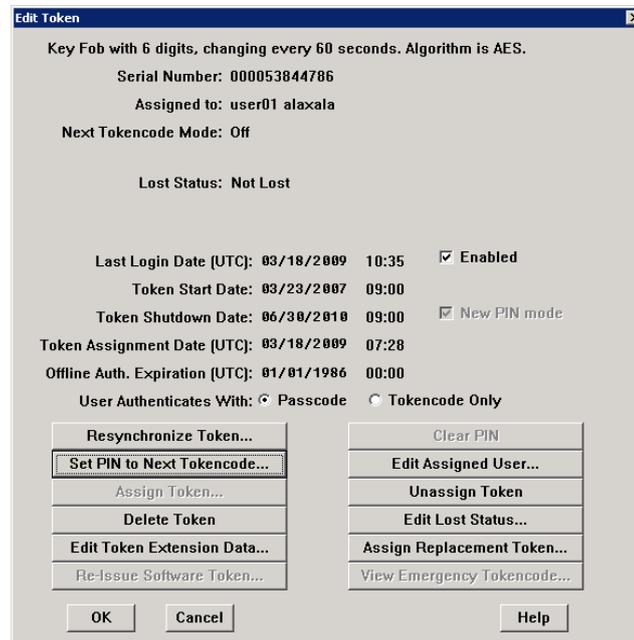


図 3.5-16 RSA Authentication Manager の設定 16

### 3.5.3 RSA RADIUS Server の設定

本構築例での RSA RADIUS Server の設定を以下に示します。RSA SecurID Appliance 2.0 にアクセスして RSA RADIUS Server の設定を行います。

- **(1)RADIUSクライアントの登録**  
認証スイッチを RADIUS クライアントとして登録します。
- **(2)認証ポリシーの作成**  
本システムで使用するポリシーを作成します。
- **(3)認証ポリシーの割り当て**  
作成したポリシーをユーザーに割り当てます。

#### (1) RADIUS クライアントの登録

①「スタート」→「RSA Authentication Manager Host Mode」を起動。メインメニューから「RADIUS」を展開し「Manage RADIUS Server」をクリック、「RSA RADIUS」設定画面を表示します。左画面「RADIUS Clients」を選択し上部にある操作メニューから「Add」をクリックし表 3.4-3 の情報を入力します。

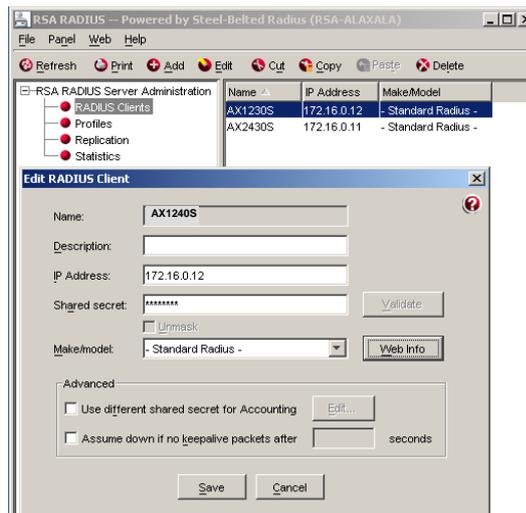


図 3.5-17 RSA RADIUS Server の設定 1

表 3.5-3 RADIUS クライアント設定

項番	項目	値	備考
1	Name	AX1240S	任意の名前
2	IP Address	172. 16. 0. 12	認証スイッチの IP アドレス
3	Shared secret	alaxala	シークレットキー

③その他の項目はデフォルトのまま「OK」ボタンをクリックし RADIUS クライアントが追加されていることを確認します。

## (2) 認証ポリシーの作成

① 「RSA RADIUS」設定画面の「Profiles」を選択し、操作メニュー「Add」をクリックし、「Name」には任意の名前（本例では“VLAN100”）を入力します。Attributes 項目の「Check list」タブを選択、「Add」をクリックし「User-Name」を選択、Value には「user01」を入力、「OK」をクリックし追加します。

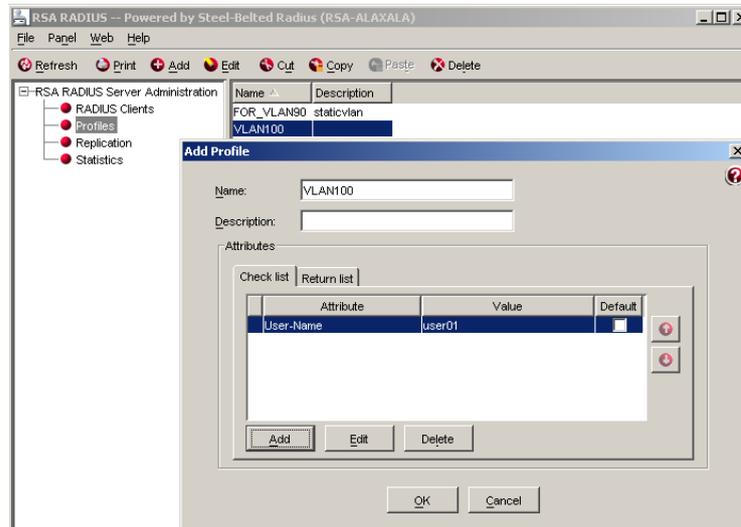


図 3.5-18 RSA RADIUS Server の設定 2

② 「OK」ボタンで「Add Profile」画面を閉じ作成したプロファイルが追加されていることを確認します。

※AX シリーズの認証モードに動的 VLAN モードを使用した場合は①の「Check list」の設定に以下の設定を追加して下さい。

「Return list」タブをクリックして以下のアトリビュートを追加して下さい。

(以下の設定では動的 VLAN300 を使用した場合の例です。)

- ・Attribute : Tunnel-Medium-Type、Value : “802”
- ・Attribute : Tunnel-Type、Value : “VLAN”
- ・Attribute : Tunnel-Private-Group-ID、Value : 300

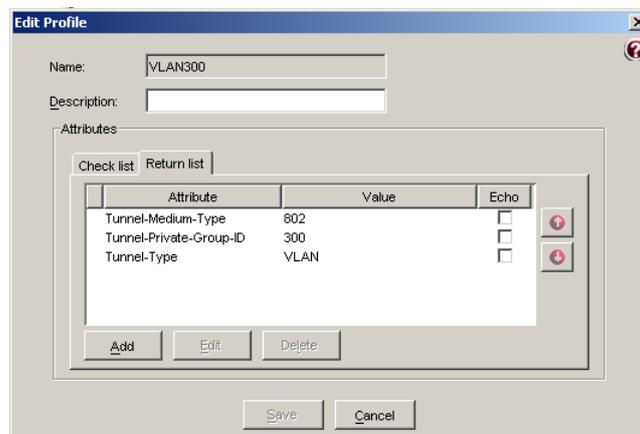


図 3.5-19 RSA RADIUS Server の設定 3

### (3) 認証ポリシーの割り当て

- ① 「RSA RADIUS」設定画面を閉じメインメニューから「RADIUS」を展開し「Add Profile」をクリックします。「Profile Name」にRSA RADIUS の Profile で指定した名前を入力します。(本構築例では“VLAN100”)入力後「OK」で閉じます。

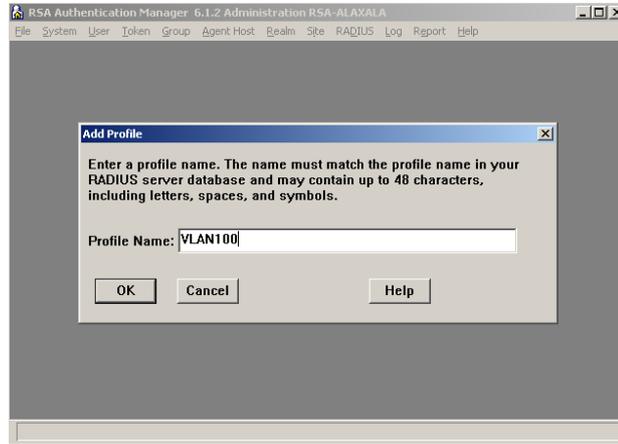


図 3.5-20 RSA RADIUS Server の設定 4

- ②次にメインメニュー「User」を展開し「Edit User」をクリックします。既に登録済みのユーザ（本例では“user01”）を指定し「Edit User」画面を表示します。画面左下の「Assign Profile」をクリックし、先程作成したプロファイル（本例では“VLAN100”）を選択したら「OK」で閉じます。

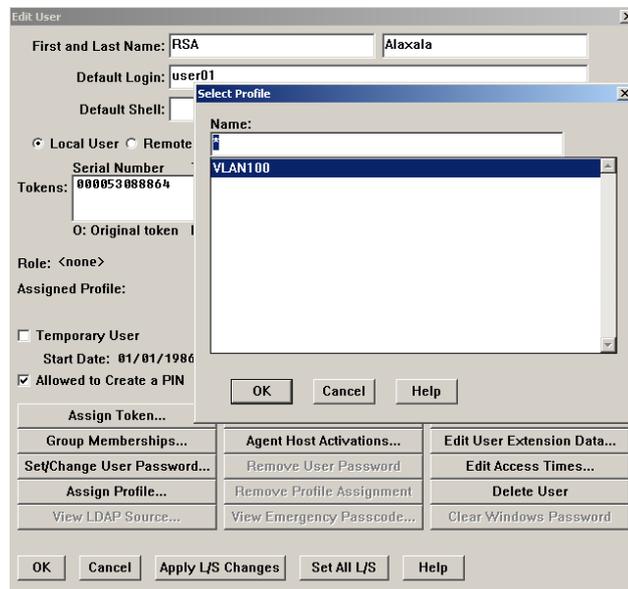


図 3.5-21 RSA RADIUS Server の設定 5

- ③以上で設定は終了です。

### 3.6 RSA SecurID Appliance 3.0 の設定

本環境を構築するためにRSA SecurID Appliance 3.0 で必要な設定を以下の3つのステップに別け設定方法を順に紹介します。なおRSA SecurID Appliance 2.0 を使用して本環境を構築する場合は**3.5 RSA SecurID Appliance 2.0 の設定**を参照して下さい。

#### (1) 初期設定

ライセンスの割り当てやシステムに関する初期設定、DNS サーバの設定を行います。

#### (2) RSA RADIUS Serverの設定

本認証ネットワークにて RADIUS サーバの設定を示します。

#### (3) RSA Authentication Managerの設定

本環境で認証に使用するユーザー登録やトークンの設定を行います。

#### 3.6.1 初期設定

RSA SecurID Appliance 3.0 の設定をするためにはまず初期設定が必要です。初期設定はサーバ操作用端末を RSA SecurID Appliance 3.0 に接続し、ブラウザから Web 画面を操作して以下の設定を行います。設定手順は RSA SecurID Appliance 3.0 オーナー ガイド「第3章：Appliance プライマリの設定方法」を参照して Quick Setup (以下①～④に該当) を実行して下さい。

- ⑧ ライセンスファイルのアップロード
- ⑨ 時刻設定
- ⑩ オペレーティング・システム・パスワードとスーパー管理者のパスワード設定
- ⑪ ネットワーク情報の設定
- ⑫ 本ネットワークシステム内の DNS サーバの設定
- ⑬ セキュリティコンソールへのログオン方法について

#### ②について

時刻設定に関して本構成ではインターネット接続を想定していない為 NTP を使用していません。可能であれば time.nist.gov などのインターネットタイムサーバを利用することをお勧めします。

#### ④について

本構築例のネットワーク設定を表 3.4-1 に示します。構築する環境に合わせて設定をして下さい。

表 3.6-1 RSA SecurID Appliance ネットワーク設定

項番	項目	設定値	備考
1	IP アドレス	10.51.0.3	本装置の IP アドレス
2	サブネットマスク	255.255.255.0	
3	デフォルトゲートウェイ	10.51.0.1	本構築例では L3 スイッチの IP アドレス
4	DNS サーバ	10.51.0.2	
5	ホスト名	Securid.example.co.jp	任意のホスト名

## ⑤について

本ガイドでは DNS サーバの設定手順の記載を省いています。以下の要件を満たす設定を行って下さい。

Quick Setup 完了後、操作用端末のブラウザから RSA SecurID Appliance3.0 の管理コンソールに SSL で接続して設定を行います。操作用端末から RSA SecurID Appliance3.0 のホスト名が解決ができるように本システム内の DNS サーバを設定してください。

また本構築例では AX シリーズの Web 認証で HTTP リダイレクト機能を使用しています。クライアント端末からの任意の Web アクセスに対し認証画面を表示させるため、認証前に名前解決が可能な環境となるように設定してください。

## ⑥について

Quick Setup 完了後、本書では RSA RADIUS Sever と RSA Authentication Manager の設定を行うため操作用端末のブラウザから RSA SecurID Appliance3.0 のセキュリティコンソールに SSL で接続して設定を行います。セキュリティコンソールへの接続方法は RSA SecurID® Appliance 3.0 オーナー ガイド「第 4 章 RSA 管理コンソールの構成と使用」を参照して下さい。

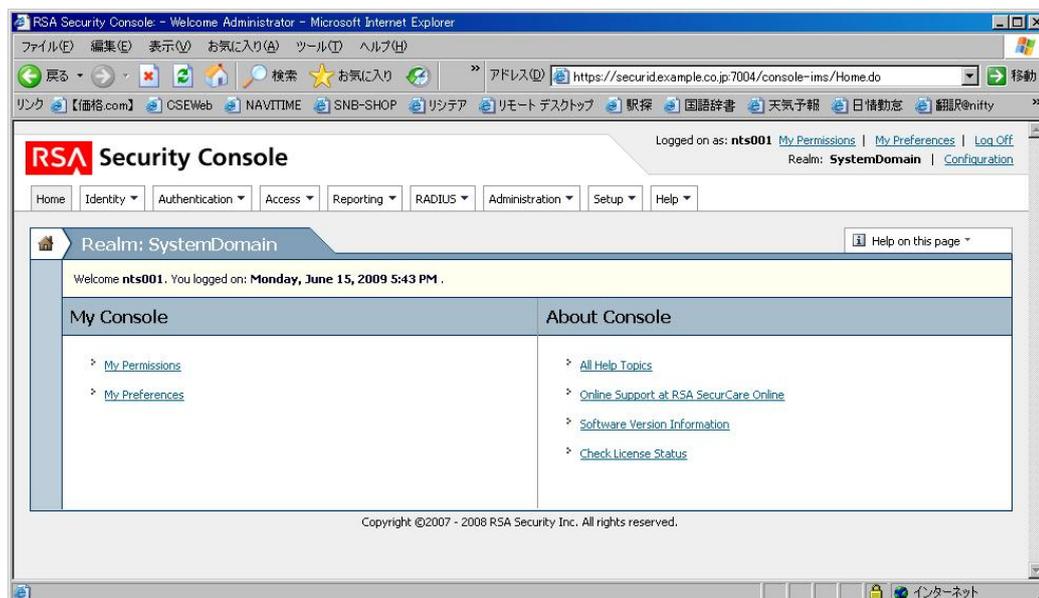


図 3.6-1 セキュリティコンソールのトップ画面

### 3.6.2 RSA RADIUS Server の設定

RSA RADIUS Server の設定を以下に示します。操作端末のブラウザより RSA SecurID Appliance のセキュリティコンソールにアクセスして RSA RADIUS Server の設定を行います。

- **(1) RADIUSクライアントの登録**  
認証スイッチを RADIUS クライアントとして登録します。  
同時に AgentHost としての登録も行います。
- **(2) RADIUSプロファイルの作成**  
本システムで使用する RADIUS のプロファイルを作成します。

#### (1) RADIUS クライアントの登録

- ①セキュリティコンソールのトップ画面から「RADIUS」→「RADIUS Clients」→「Add New」をクリックして下さい。

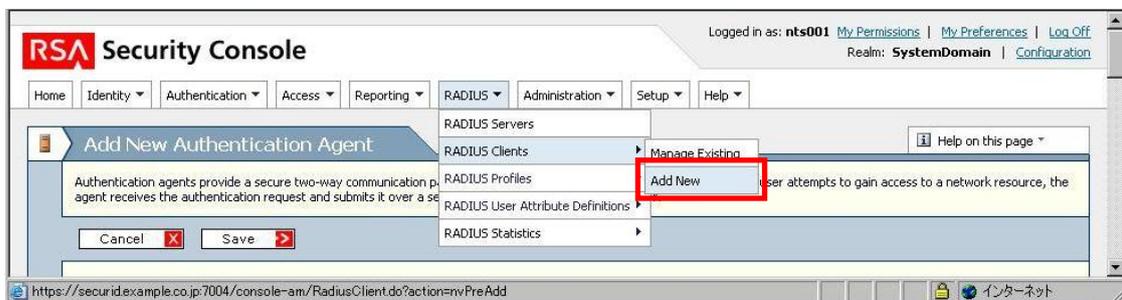


図 3.6-2 RADIUS Client の設定 1

- ②「Add RADIUS Client」画面にて「Client Name」、「IP Address」、「Shared Secret」を表 3.4-3 を参照しそれぞれ入力して下さい。  
入力後は右下の「Save and Create Associated RSA Agent」をクリックして下さい。

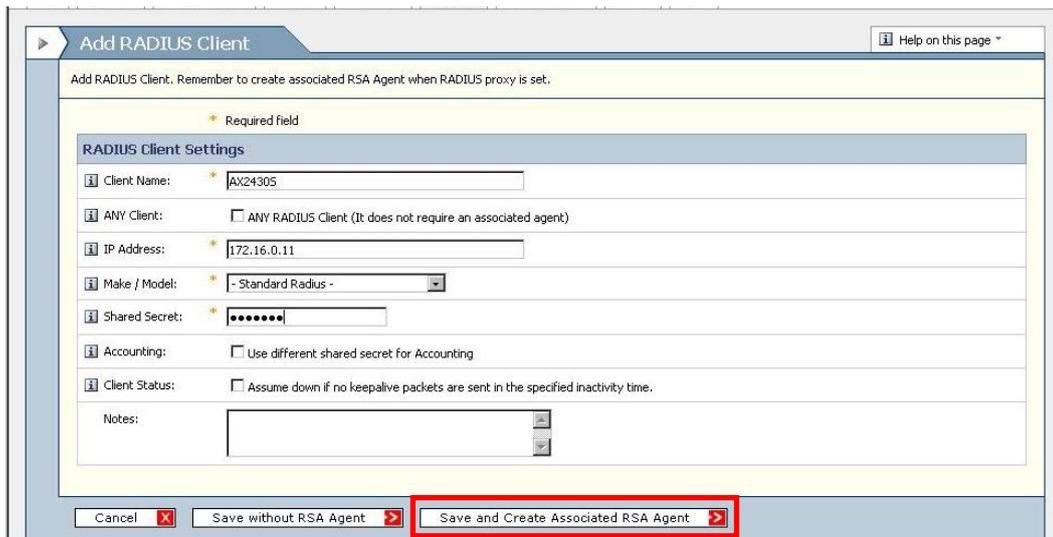


図 3.6-3 RADIUS Client の設定 2

表 3.6-2 RADIUSClient 設定

認証スイッチ	Name	IP Address	Shared Secret
AX2430S	AX2430S	172.16.0.11	alaxala
AX1240S	AX1240S	172.16.0.12	alaxala

※本ガイドでは認証スイッチ 2 台分の登録を行います。

- ③ 「Add New Authentication Agent」画面が表示されたらそのまま「Save」ボタンをクリックします。「Confirmation Required」画面が表示されたら右下「Yes, Save Agent」ボタンをクリックしエージェントホストの登録を完了させます。



図 3.6-4 Agent Host の登録

## (2) RADIUS プロファイルの作成

- ① セキュリティコンソールのトップ画面から「RADIUS」→「RADIUS Profile」→「Add New」をクリックして「Add RADIUS Profile」画面を表示して下さい。「Profile Name:」に任意の名前（本ガイドでは“WebAuth”を使用）を入力し「Seve」ボタンをクリックして下さい。

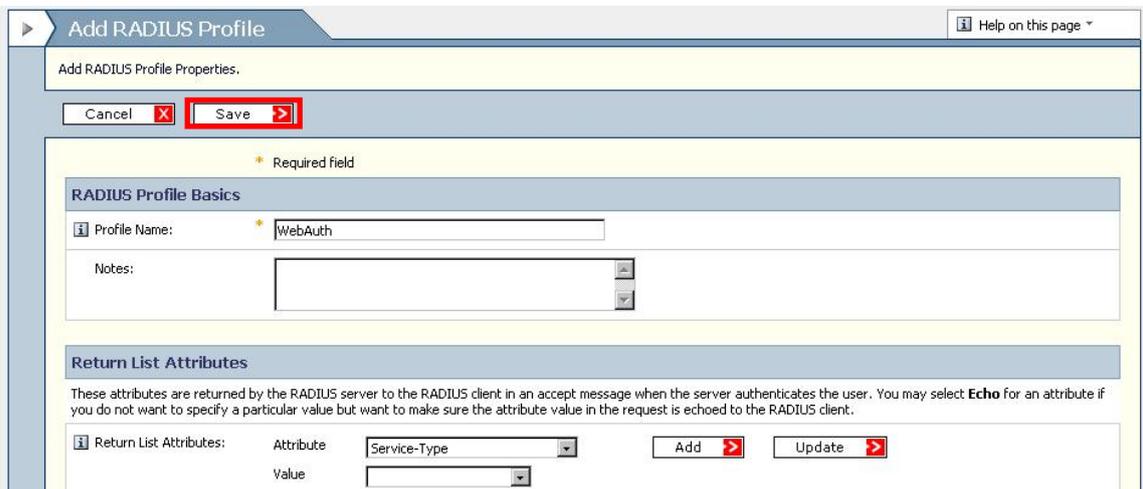


図 3.6-5 RADIUS Profile の作成 1

- ②RADIUS Profiles 画面にて作成した“WEBAUTH”という名前のプロファイルが登録されていることを確認する。(※登録後のプロファイル名は大文字表示となります。)

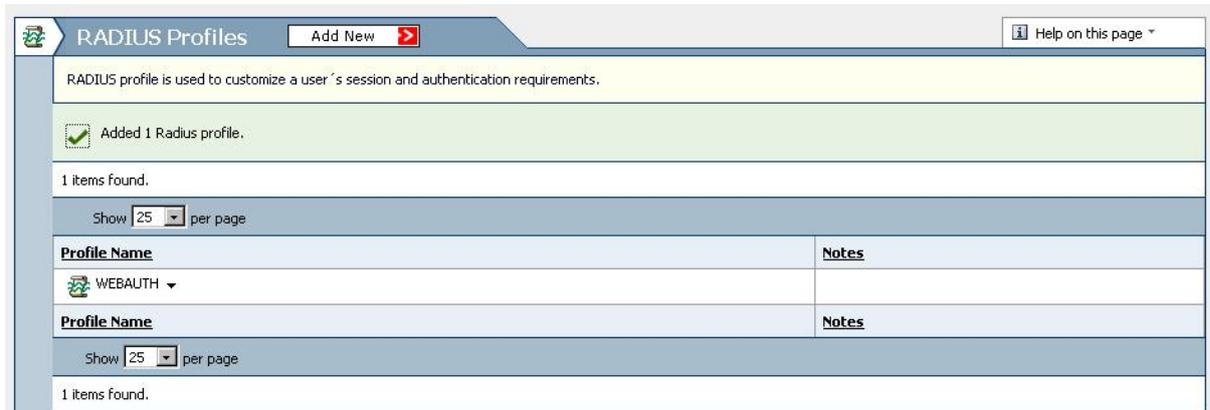


図 3.6-6 RADIUS Profile の作成 2

※AXシリーズの認証モードに動的VLANモードを使用した場合は①の「Add RADIUS Profile」画面内の「Check list」設定に以下の設定を追加して下さい。AXシリーズの認証モードに関しては**1.2.6 AXシリーズの認証モード**を参照して下さい。  
(以下の設定では動的 VLAN300 を使用した場合の例です。)

- ・Attribute : Tunnel-Medium-Type、Value : “802”
- ・Attribute : Tunnel-Type、Value : “VLAN”
- ・Attribute : Tunnel-Private-Group-ID、Value : 300

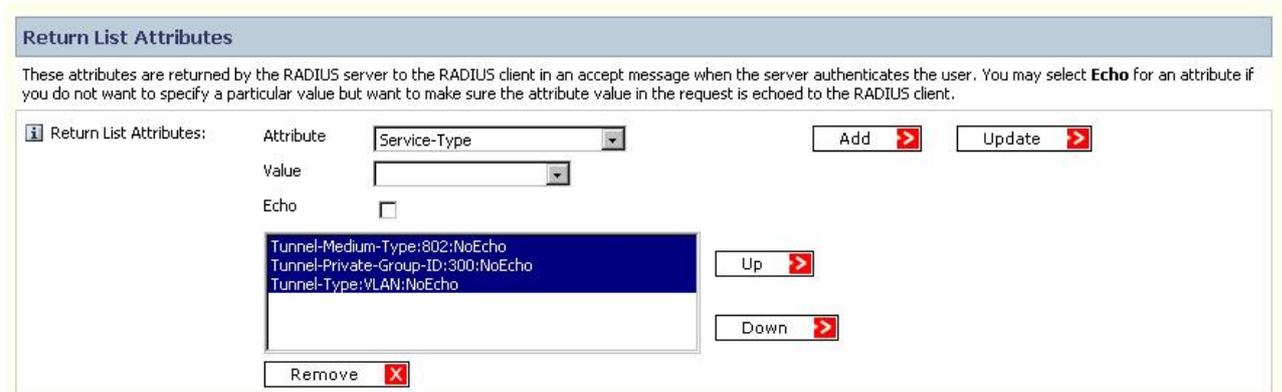


図 3.6-7 RADIUS Profile の作成 3

### 3.6.3 RSA Authentication Manager の設定

本環境を構築するための Authentication Manager で行う設定を以下に示します。

**3.6.2 RSA RADIUS Server の設定**と同様に操作端末のブラウザより RSA SecurID Appliance 3.0 のセキュリティコンソールにアクセスして RSA RADIUS Server の設定を行います。

- **(1) トークンレコードのインポート**  
Authentication Manager にトークンレコード(※1)をインポートしてトークンを使用できる状態にします。(※1 … トークンの情報が記載された XML 形式のファイル)
- **(2) 認証ユーザーの作成**  
トークンを使用するユーザーを作成します。
- **(3) トークンの割り当て**  
認証ユーザーにトークンを割り当てます。
- **(4) RADIUS プロファイルの割り当て**  
認証ユーザーに本システムで使用する RADIUS プロファイルを割り当てます。

#### (1) トークンレコードのインポート

- ①セキュリティコンソールのトップ画面から「Authentication」→「SecurID Tokens」→「Import Token Job」→「Add New」をクリックして下さい。

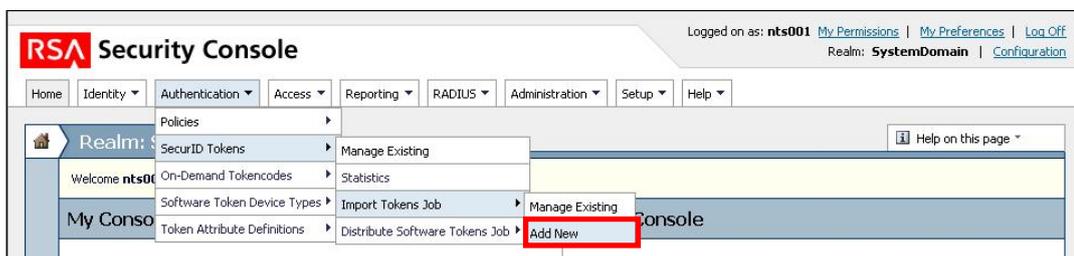


図 3.6-8 Token Import1

- ②「Add New Import SecurID Tokens Job」画面の「Import File:」にトークンレコード (XML 形式のファイル) をセットし「Submit Job」ボタンをクリックして下さい。

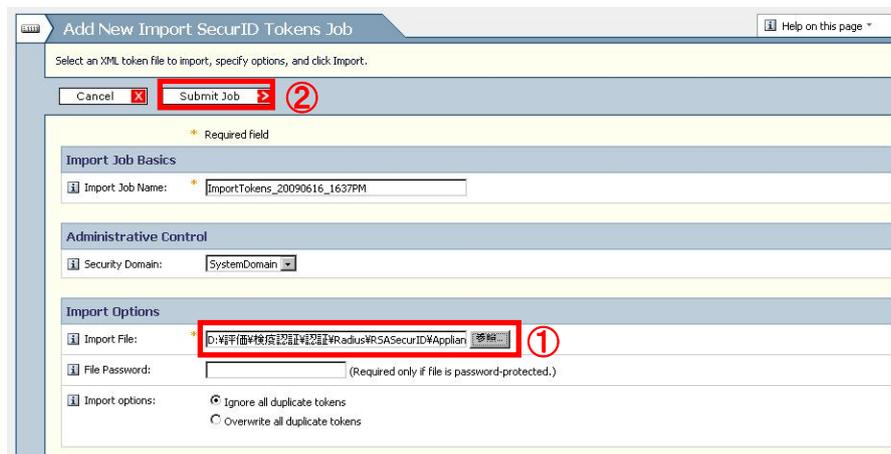


図 3.6-9 Token Import2

- ③ トークンレコードが正しくインポートされた事を確認します。

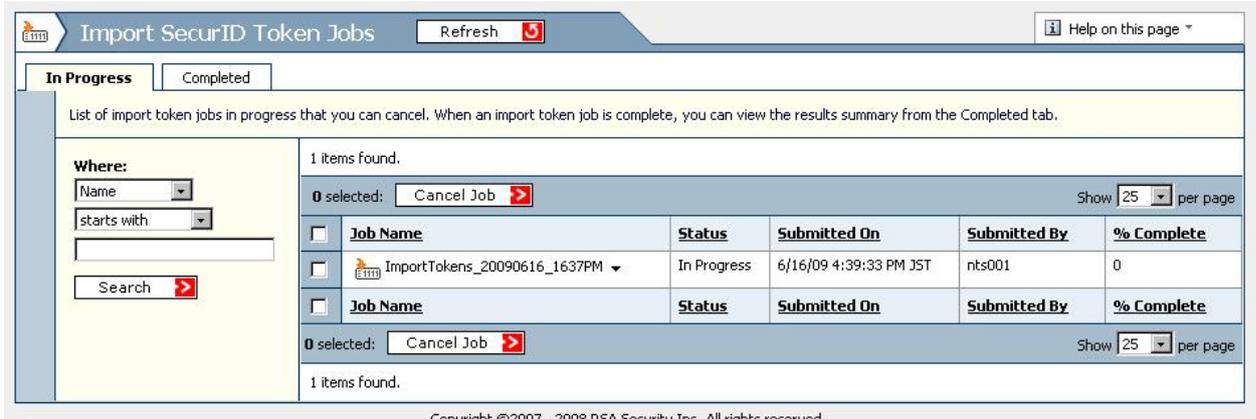


図 3.6-10 Token Import3

※ トークンのインポート方法についての詳細は RSA SecurID® Appliance 3.0 オーナー ガイド「第 5 章ユーザーとトークンの管理」を参照して下さい。

## (2) 認証ユーザーの作成

- ① セキュリティコンソールのトップ画面から「Identity」→「Users」→「Add New」をクリックし「Add New User」画面を表示します。「User Name:」、「User ID:」、「Password:」、「Confirm Password:」を入力し「Save」ボタンをクリックして下さい。  
 (本構築例では図 3.4-11 のように「User Name:」と「User ID:」に“user01”、「Password:」には“alaxala\_abc1”と設定。また「Force Password Change」のチェックを外します。)

**Administrative Control**

Identity Source: Internal Database  
 Security Domain: SystemDomain administrators manage this user

**User Basics**

First Name: user01  
 Middle Name:  
 Last Name: user01  
 User ID: user01  
 Email:  
 Certificate DN:  
 Notes:

**Password**

Password: [masked] What's a valid password?  
 Confirm Password: [masked]  
 Force Password Change:  Require user to change password at next login

図 3.6-11 Add User1

- ② 「Users」画面が表示され作成したユーザー（本例では「User01」）が登録されていることを確認します。

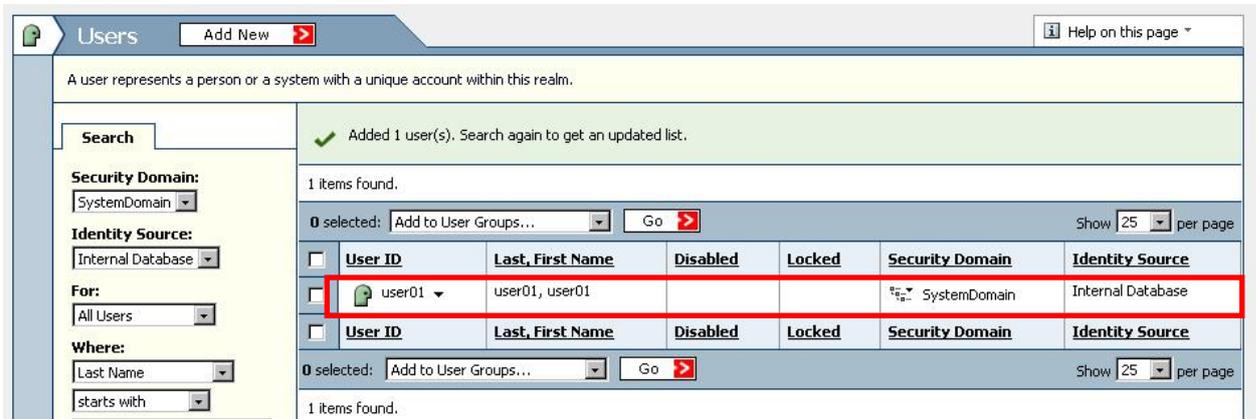


図 3.6-12 Add User2

### (3) トークンの割り当て

- ① 「Users」画面から先程作成した「User01」をクリックし操作メニューを開きます。「SecurID Tokens」をクリックして下さい。

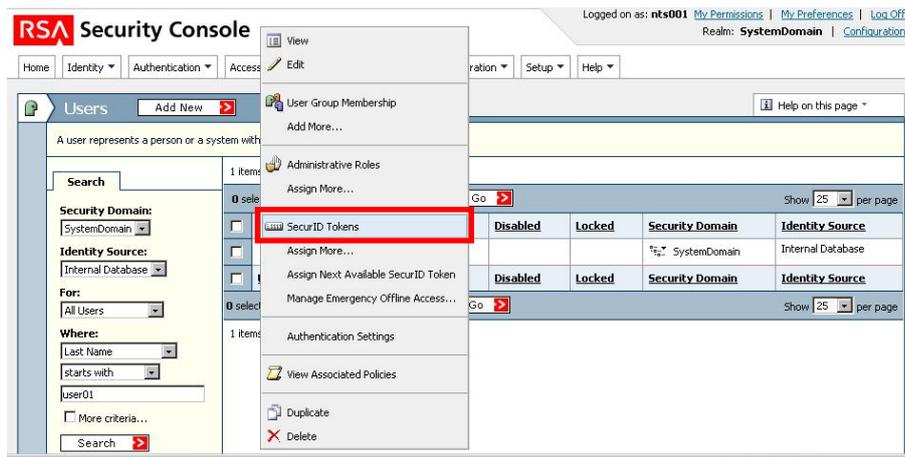


図 3.6-13 トークンの割り当て 1

- ② 「Assigned SecurID Tokens」画面が表示されたらそのまま「Assign Token」ボタンをクリックして下さい。

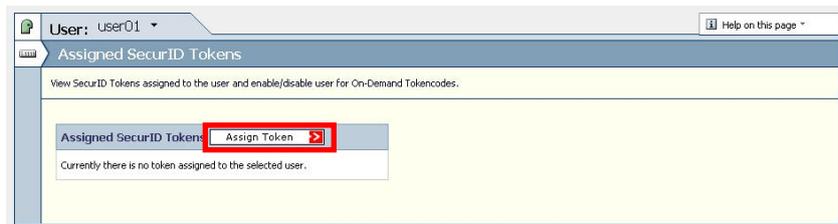


図 3.6-14 トークンの割り当て 2

- ③ 「Assigned SecurID Tokens」の画面が変わり、インポートされたトークン一覧が表示されます。本ユーザーが使用するトークンのシリアルナンバーの左にチェックをいれ「Assign」ボタンをクリックしてください。

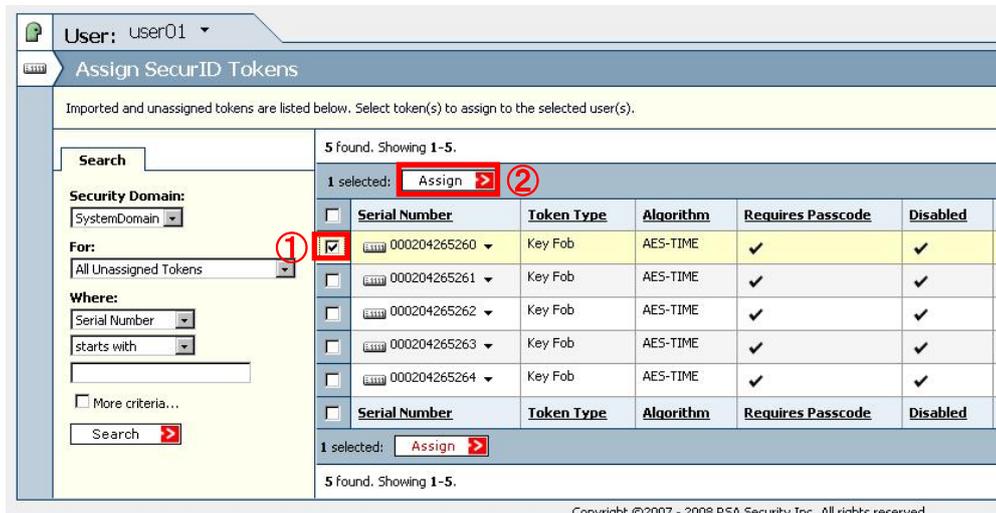


図 3.6-15 トークンの割り当て 3

- ④以上でユーザーに対するトークンの割り当ては完了です。

#### (4) RADIUS プロファイルの割り当て

- ① 「Users」画面から先程作成した「User01」をクリックし操作メニューを開きます。「Authentication Settings」をクリックして下さい。

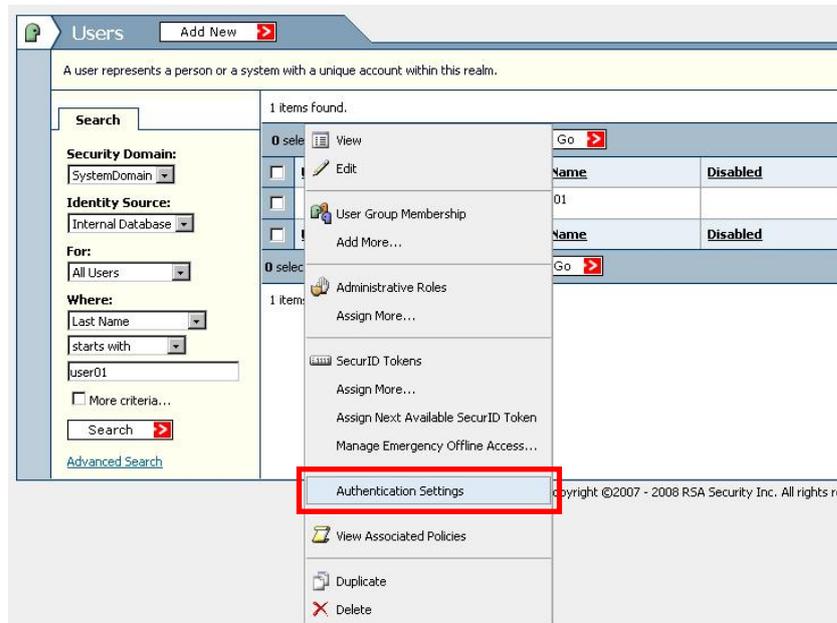


図 3.6-16 RADIUS Profile の割り当て 1

- ②「User01」の「Authentication Settings」画面が表示されたら「RADIUS」設定の項目にて「User RADIUS Profile:」を“WEBAUTH”に設定して画面下にある「Save」ボタンをクリックして下さい。

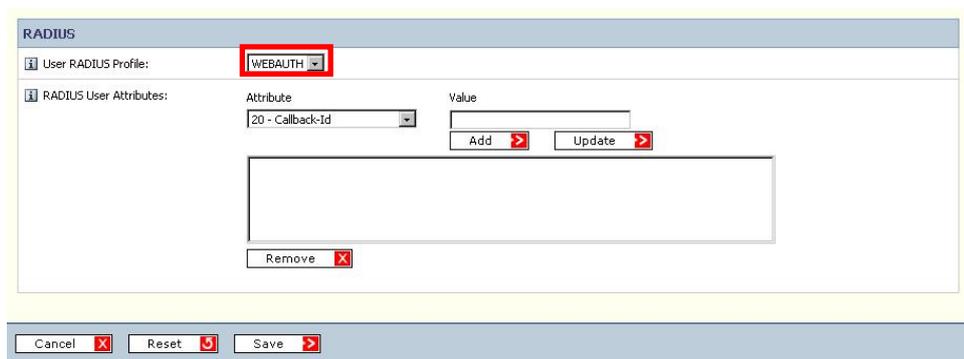


図 3.6-17 RADIUS Profile の割り当て 2

- ③以上でユーザーに対する RADIUS プロファイルの割り当ては完了です。

※本ガイドではユーザー単体に RADIUS プロファイルを割り当てしていますが、ユーザーが所属するグループ単体に RADIUS プロファイルを割り当てることも可能です。  
 詳細な設定方法は「RSA SecurID® Appliance 3.0 オーナー ガイド」を参照して下さい。

### 3.7 MAC 認証用 RADIUS サーバの設定

本構築例ではトークンを使用したパスワード入力ができない機器（プリンタなど）の接続に MAC 認証を使用しています。RADIUS サーバ設定ガイド(Windows Server 2003 編)の「5 章 MAC 認証の設定」を参照して、本環境用に MAC 認証専用の RADIUS サーバの設定を行ってください。

### 3.8 クライアント端末の設定

本構築例でのクライアント端末に必要な設定を以下に示します。

#### 3.8.1 ハードウェアトークン

本システムでハードウェアトークン（RSA SecurID SID700）を使用する場合、クライアント端末に特別な設定を行う必要は無くトークンを使用した Web 認証を行う事が可能です。

#### 3.8.2 ソフトウェアトークン

ソフトウェアトークンを使用した Web 認証を行う場合はクライアント端末にソフトウェアトークンをインストールする必要があります。ソフトウェアトークンのインストールに関しては RSA SecurID® Appliance 3.0 オーナー ガイド「第 5 章ユーザーとトークンの管理」を参照して下さい

## 4. クライアント認証手順

本章ではクライアント端末でトークンを用いたワンタイム・パスワードによる Web 認証手順を以下の4つパターンで示します。

### (1) 4.1ハードウェアトークンを使用した認証手順

ハードウェアトークン (RSA SecurID SID700) を使用して AX シリーズの Web 認証を行う手順を以下に示します。認証ユーザーの PIN 登録が完了していない場合は **4.3New PIN モード時の認証手順**を先に参照してください。

### (2) 4.2ソフトウェアトークンを使用した認証手順

ソフトウェアトークン RSA SecurID Token for Windows Desktops Ver4.0 をを使用して AX シリーズの Web 認証を行う手順を以下に示します。認証ユーザーの PIN 登録が完了していない場合は **4.3New PIN モード時の認証手順**を先に参照してください。

### (3) 4.3New PINモード時の認証手順

ハードウェアトークン (RSA SecurID SID700) を使用して AX シリーズの Web 認証で New PIN モードを行う手順を以下に示します。ソフトウェアトークンを使用した場合も動作は同じです。

### (4) 4.4Next tokenモード時の認証手順

ハードウェアトークン (RSA SecurID SID700) を使用して AX シリーズの Web 認証で Next token モードを行う手順を以下に示します。ソフトウェアトークンを使用した場合も動作は同じです。

### 4.1 ハードウェアトークンを使用した認証手順

①クライアント端末を認証スイッチ (AX シリーズ) に接続し、ブラウザを起動します。すると AX シリーズの Web 認証リダイレクト機能により認証画面が表示されます。

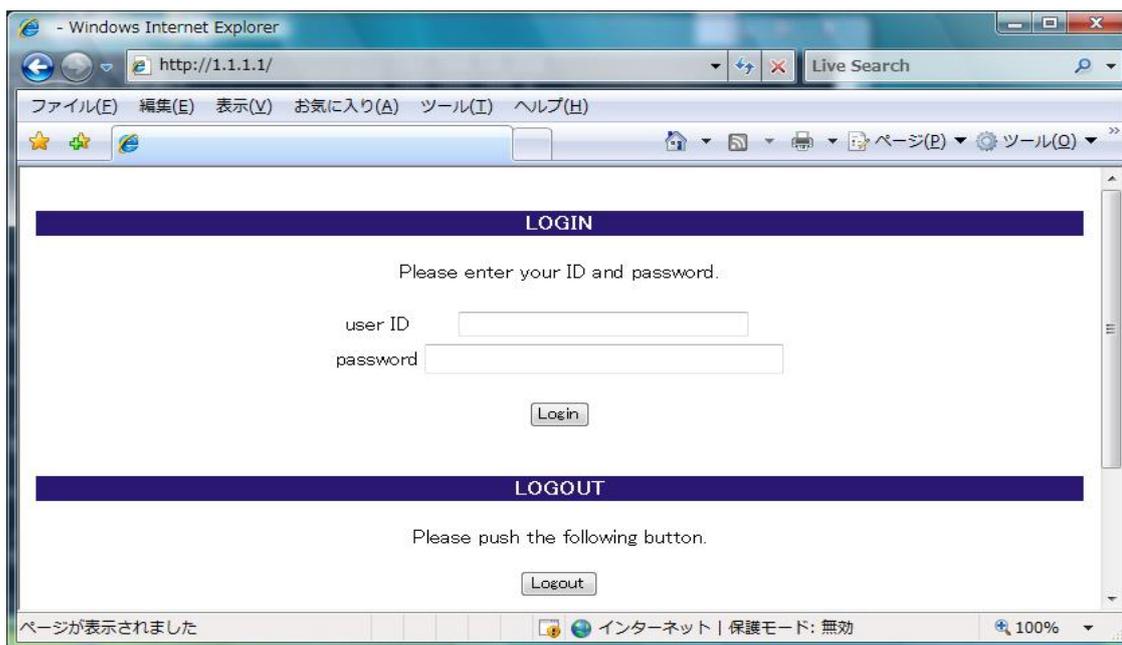


図 4.1-1 ハードウェアトークン認証 1

②UserID に認証ユーザーID を（本構築例では “user01”）password には認証ユーザーのパスワード（PIN+トークンに表示された6桁の数字）を入力し「Logon」ボタンをクリックして下さい。



図 4.1-2 ハードウェアトークン認証 2

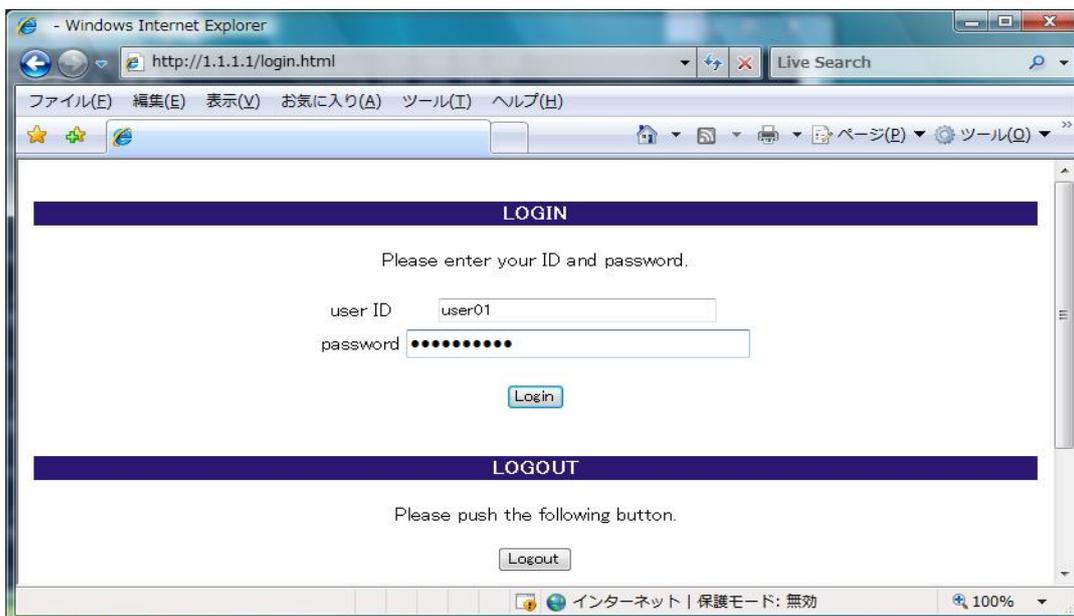


図 4.1-3 ハードウェアトークン認証 3

③認証成功時は Login success 画面が表示されます。

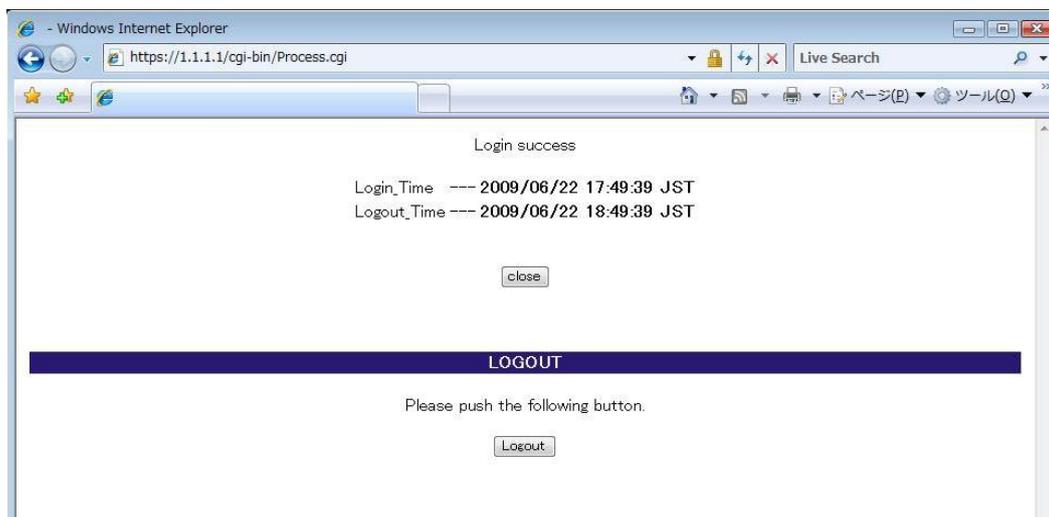


図 4.1-4 Login success 画面

## 4.2 ソフトウェアトークンを使用した認証手順

①クライアント端末にて RSA SecurID Token を起動します。  
(デフォルトでは C:/Program Files/RSA Security/RSA SecurID Software Token にインストールされます。)

②ソフトウェアトークンの Enter PIN に認証ユーザーの PIN を入力し図 4.3-1 のボタンをクリックする。

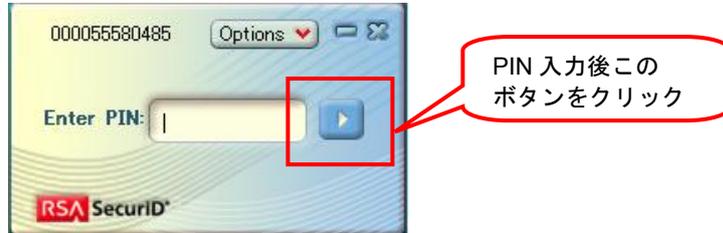


図 4.2-1 ソフトウェアトークン認証 1

③ソフトウェアトークンの画面では PIN 入力によりジェネレートされたパスコードが表示される。



図 4.2-2 ソフトウェアトークン認証 2

④クライアント端末を認証スイッチ (AX シリーズ) に接続し、ブラウザを起動します。すると AX シリーズの Web 認証リダイレクト機能により認証画面が表示されます。

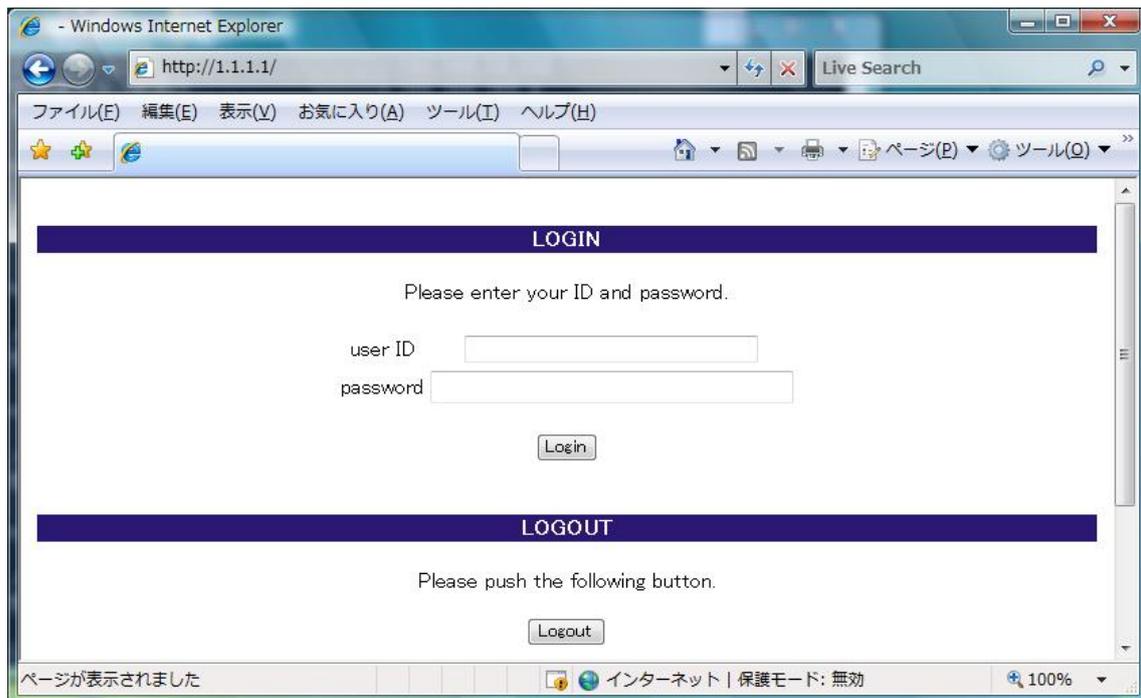


図 4.2-3 ソフトウェアトークン認証 3

- ⑤UserID に認証ユーザーID を（本構築例では “user01”）password にはソフトウェアトークンに表示されたをパスコード（8 桁）を入力し「Logon」ボタンをクリックして下さい

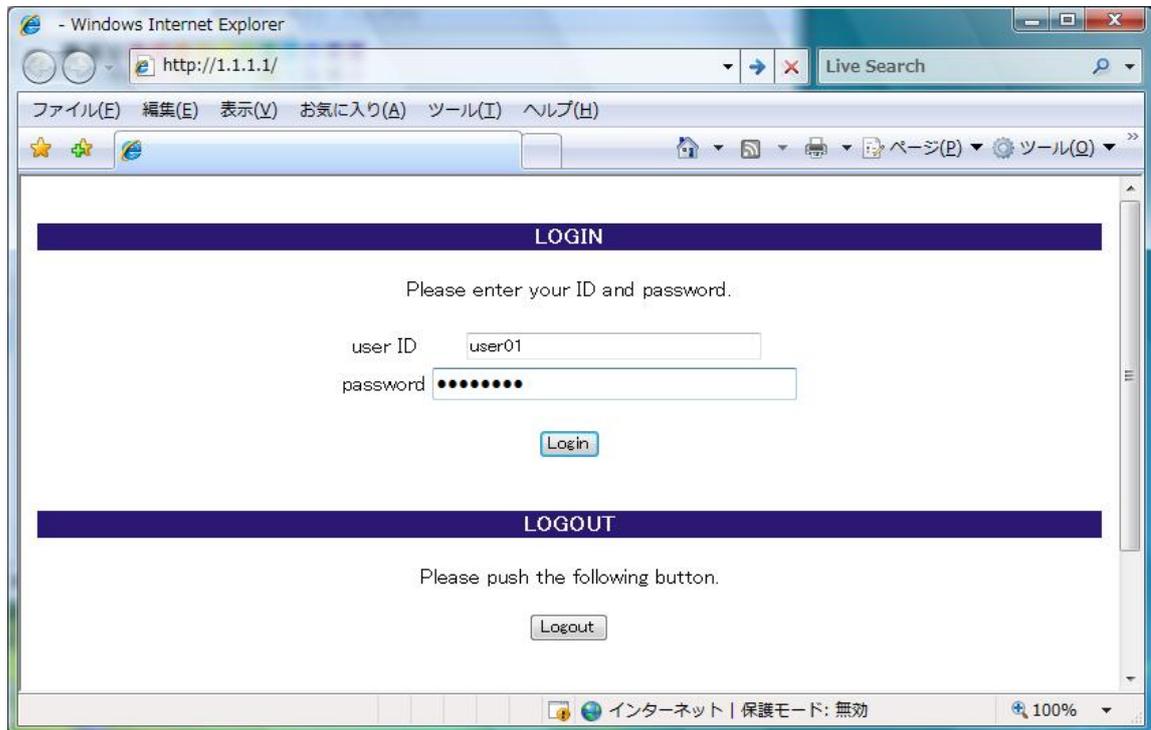


図 4.2-4 ソフトウェアトークン認証 4

- ⑥認証成功時は Login success 画面が表示されます。

### 4.3 New PIN モード時の認証手順

①クライアント端末を認証スイッチ (AX シリーズ) に接続し、ブラウザを起動します。すると AX シリーズの Web 認証リダイレクト機能により認証画面が表示されます。

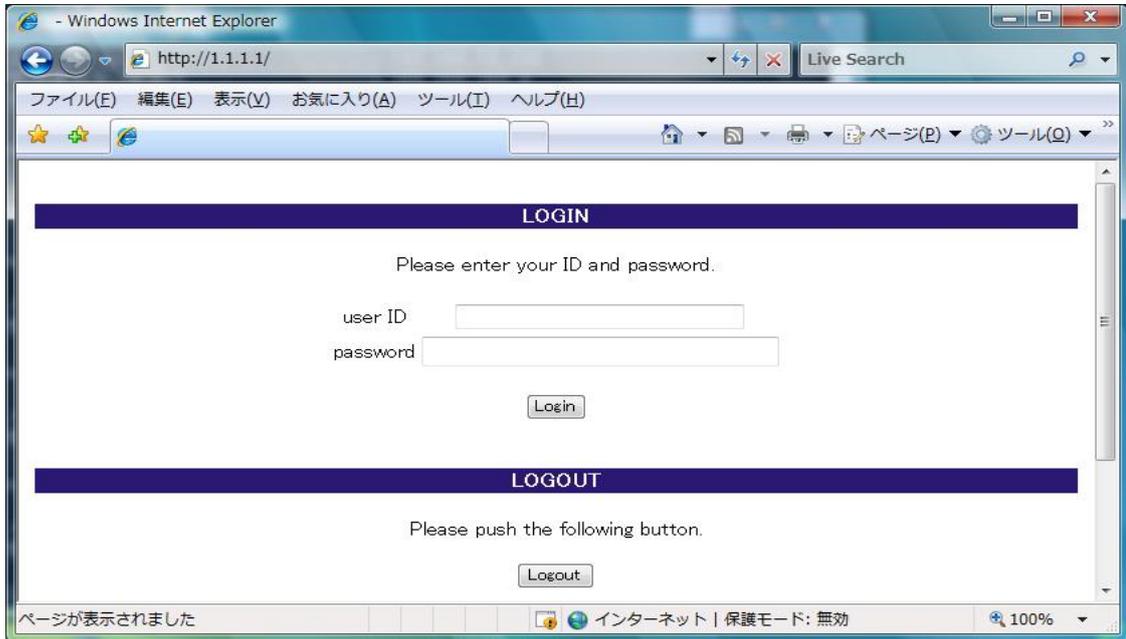


図 4.3-1 New PIN モード認証 1

②UserID に認証ユーザーID を (本構築例では “user01”) password にはトークンコード (ハードウェアトークンに表示された 6 桁の数字) を入力し「Logon」ボタンをクリックして下さい。



図 4.3-2 New PIN モード認証 2

- ③ユーザーID と入力されたトークンコードが正しい場合 New PIN モードに移行認証ユーザーの PIN 登録画面が表示されます。設定したい PIN を入力して「Enter」をクリックして下さい。

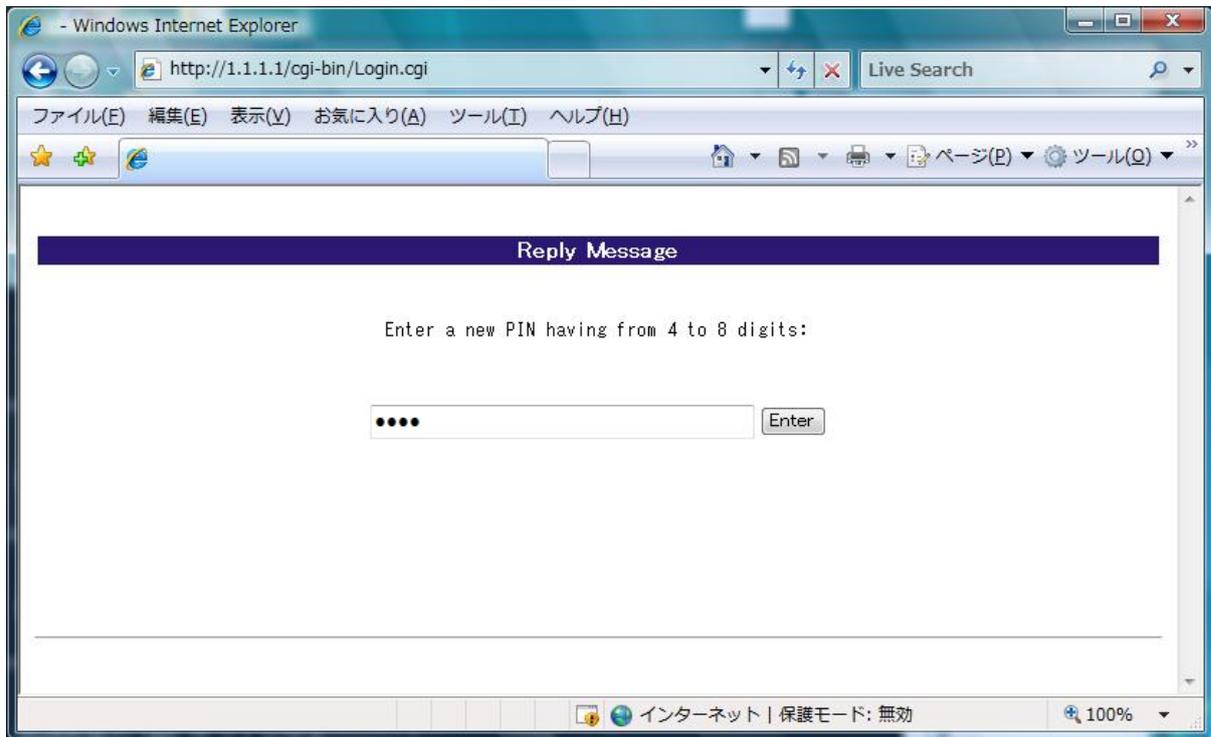


図 4.3-3 New PIN モード認証 3

- ④PIN の再入力が必要されますので同じ PIN を再び入力し「Enter」をクリックする。

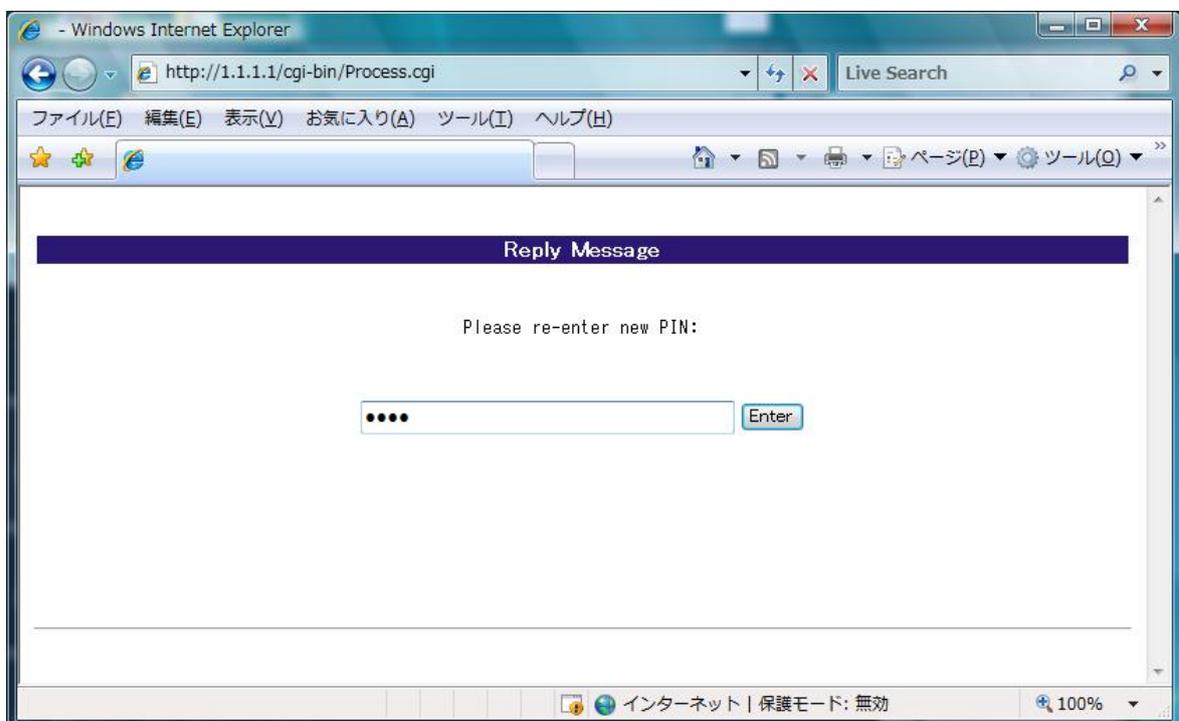


図 4.3-4 New PIN モード認証 4

⑤PIN の登録が完了した旨のメッセージが表示され、続けてパスコードの入力を行います。この時②で入力したトークンコードから 60 秒経過して次のトークンコードに変更している必要があります。

登録した PIN+トークンコード (6 桁) を入力し「Enter」ボタンをクリックします。

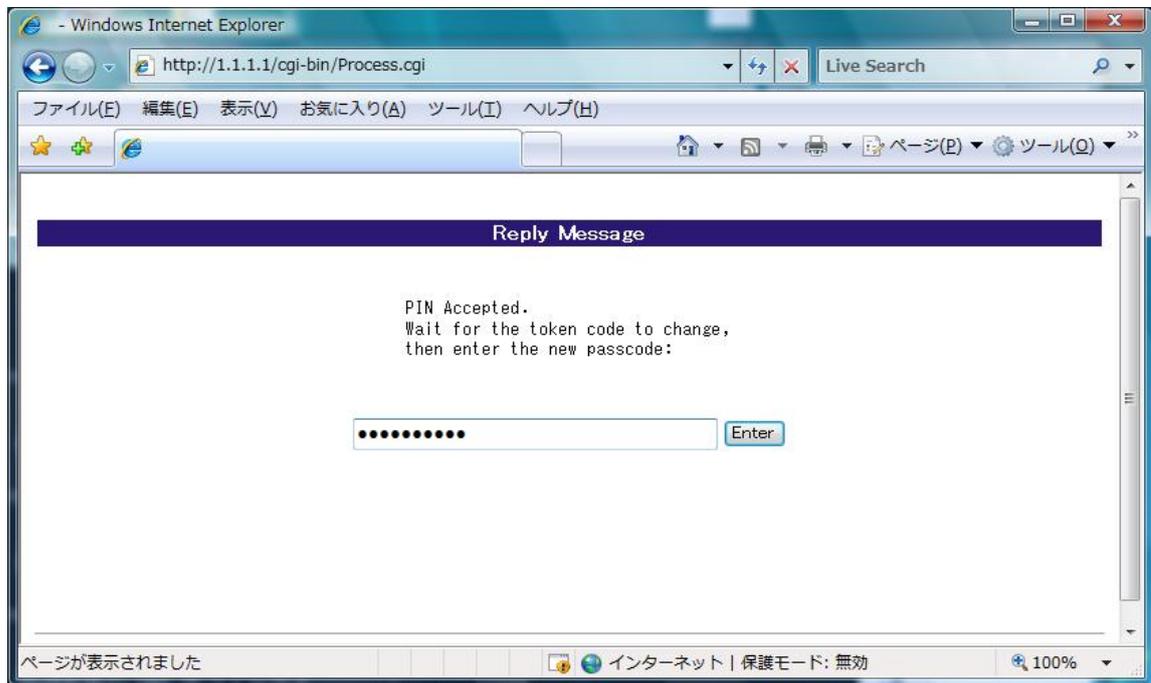


図 4.3-5 New PIN モード認証 5

※注意…ソフトウェアトークンを使用した場合、登録した PIN+トークンコード (8 桁) をパスコードに入力しても認証に成功しません。必ずソフトウェアトークンに PIN を入力しジェネレートされたパスコードを使用して下さい。

⑥認証成功時は Login success 画面が表示されます。

#### 4.4 Next token モード時の認証手順

①同じユーザーで3回（初期値）連続で認証に失敗するとそのユーザーは Next token モードとなります。Next token モードの状態では、図 4.1-1 に示す認証入力から認証に成功すると図 4.4-1 に示す Next token 入力画面が表示されます。この Next token 入力画面(※1)から入力するトークンコードは、認証成功時に使用したトークンコードではなく、新しいトークンコードになりますので、トークンを見て、値が切り変わったことを確認して入力してください。トークンコードの認証成功時は、図 4.1-4 の Login success 画面が表示されます。

※1 … 本入力項目ではトークンコード及びパスワードどちらでも入力可能です。

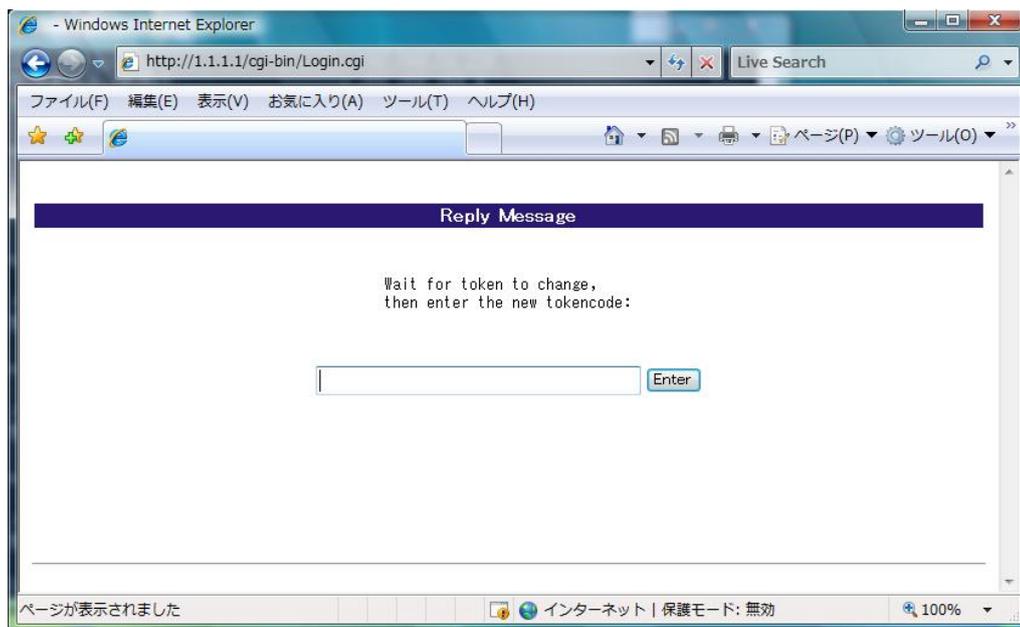


図 4.4-1 Next token 入力画面

②Next token入力画面から、間違ったトークンコードを入力してしまった場合、図4.4-2に示すPass code再入力画面が表示されます。本画面にて正しいパスワードを入力すると図4.4-1に示すNext token入力画面に戻ります。①の説明のとおり正しいトークンを入力して下さい。

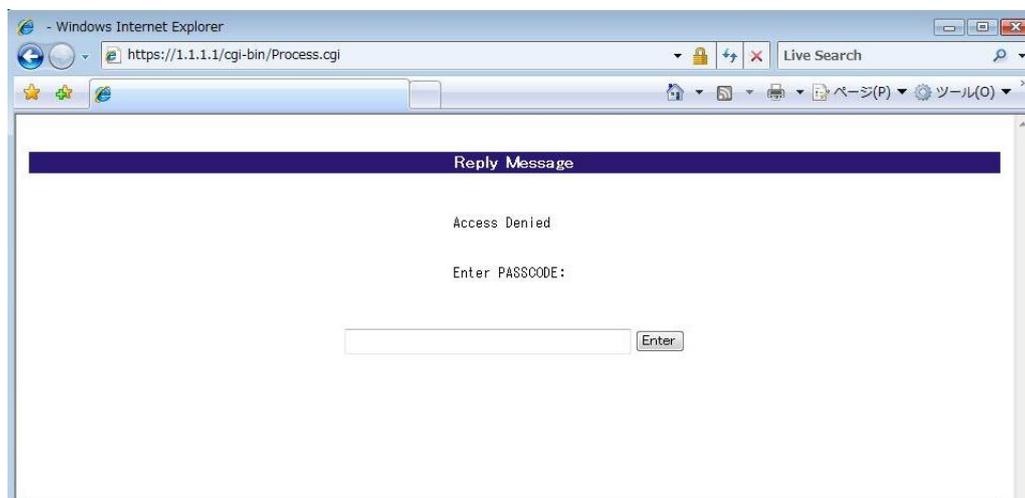


図 4.4-2 Passcode 再入力画面

## 5. 動作確認方法

### 5.1 AX シリーズにおける確認方法

AX シリーズの Web 認証に関する運用コマンドを以下に示します。

#### 5.1.1 #show web-authentication login

認証済みユーザの一覧が確認できます。また、ユーザごとに認証端末の MAC アドレス、ログイン時間、ログアウトまでの残り時間などが確認できます。

#### 5.1.2 #show web-authentication logging

Web 認証のログ表示コマンドです。

### 5.2 RSA Authentication Manager における確認方法

#### 5.2.1 リアルタイムログ (RSA SecurID Appliance 2.0)

ユーザのパスコード照合結果、認証結果、認証失敗時の失敗理由を RSA Authentication Manager で確認する操作手順を以下に示します。

- ① 「スタート」 → 「RSA Authentication Manager Host Mode」 を起動します。メインメニューから「Log」を展開し「Edit Log Extension Data」を選択し「Activity Log Extension」をクリックします。

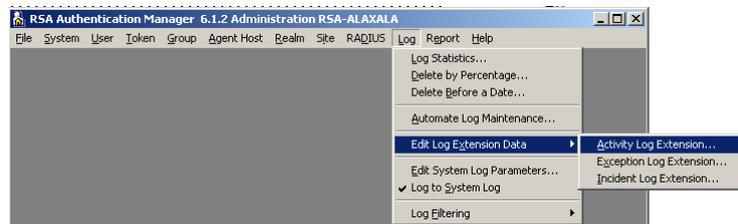


図 5.2-1 RSA Authentication Manager ログ 1

- ② [Log Entry Selection Criteria]画面にて「OK」ボタンをクリックします。



図 5.2-2 RSA Authentication Manager ログ 2

③認証ログが確認できます。

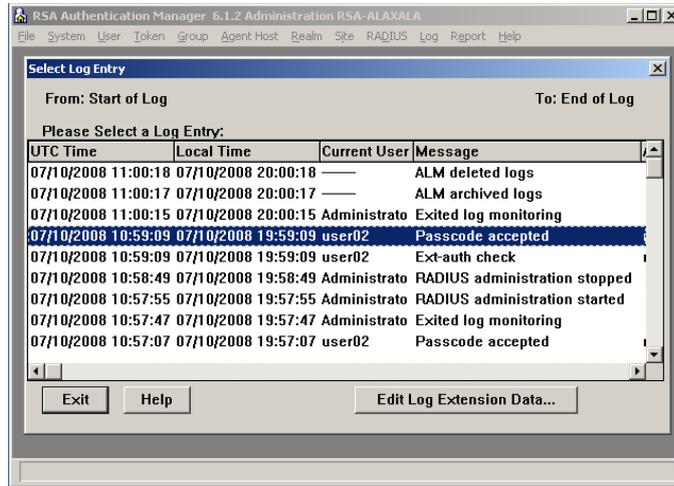


図 5.2-3 RSA Authentication Manager ログ 3

### 5.2.2 リアルタイムログ (RSA SecurID Appliance 3.0)

ユーザのパスコード照合結果、認証結果、認証失敗時の失敗理由をリアルタイムに RSA Authentication Manager で確認する操作手順を以下に示します。

①セキュリティコンソールのトップ画面から「Reporting」→「Real-time Activity Monitors」→「Authentication Active Monitor」をクリックして下さい。

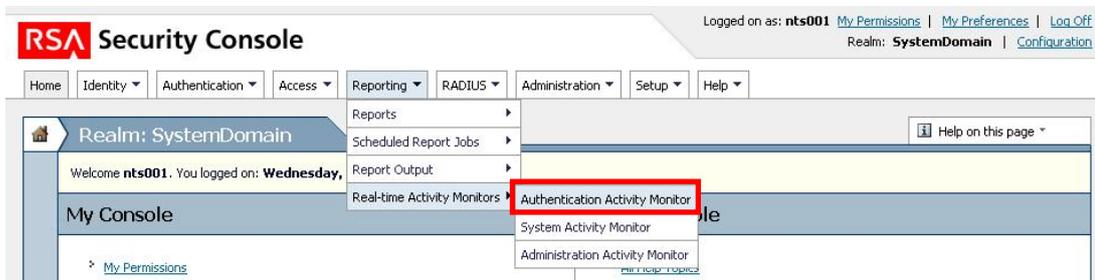


図 5.2-4 RSA Authentication Manager ログ 1

②左上の「Start Monitor」ボタンをクリックして、クライアント端末の認証操作を行います。すると以下の様に詳細なリアルタイムログが確認できます。

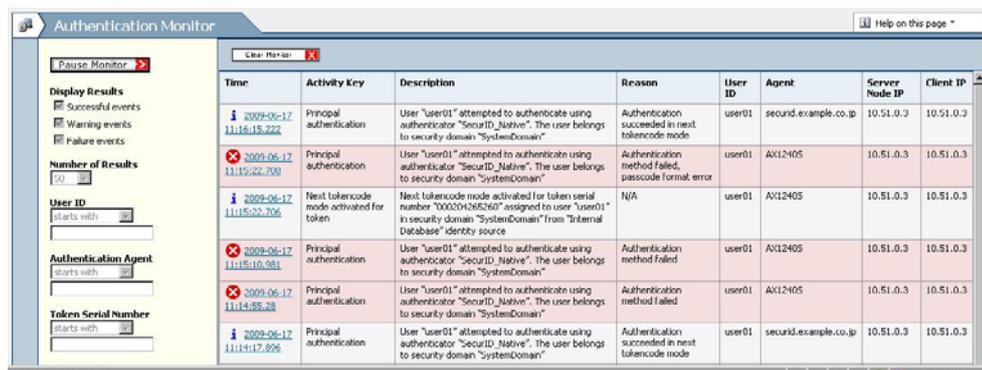


図 5.2-5 RSA Authentication Manager ログ 2

## 6. 注意事項

### 6.1 ソフトウェアオプションライセンス(OP-OTP)無効時の注意事項

ユーザが無効なパスワードを入力して連続3回ログインに失敗した場合、RSA SecurID ApplianceではデフォルトでユーザのNext tokenモードが有効となります。AXシリーズにソフトウェアオプションライセンス(OP-OTP)が有効化されていない認証ネットワーク環境ではユーザー自身でログインすることが出来なくなり、管理者にNext tokenモードの無効化を行ってもらう必要があります。

## 付録. コンフィグレーション

本ガイドにて紹介した構成のコンフィグレーション例です。

「3章 システム構築例」のネットワーク構成における各装置のコンフィグレーションをテキスト形式のファイルとして本ガイドに添付しております。(添付ファイルを抽出するには、Adobe Acrobat 5.0以降もしくはAdobe Reader 6.0以降が必要です。)

各コンフィグレーションについては、以下に示すファイル名と同じ名前の添付ファイルを参照下さい。

	装置名と対象装置	対象ファイル
L3 スイッチ	core#1(AX3630S)	core#1_config.txt
認証スイッチ	edge#1(AX2430S)	edge#1_config.txt
	edge#2(AX1240S)	edge#2_config.txt



# Alaxala

2009年8月26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  
<http://www.alaxala.com/>