

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



(第2版)

Copyright © 2009, ALAXALA Networks Corporation. All rights reserved.



### はじめに

AX シリーズ 認証ソリューションガイド(RSA SecurID<sup>®</sup> 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<sup>®</sup> Appliance 2.0 オーナー ガイド
- RSA SecurID<sup>®</sup> Appliance 3.0 オーナー ガイド
- RSA Authentication Manager<sup>®</sup> 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	Ι	2009.4.21	初版発行	
第2版	-	2009.8.19	使用機器の追加	本ガイド
			・RSA SecurID Appliance 3.0 を追加。	全般
			・認証スイッチとして AX2430S を追加。	
			AX シリーズの OS のバージョンアップに対応	
			・AX1240S(Ver2.0)から(Ver2.1)	
			・AX3630S(Ver10.1)から(Ver11.1.A)	
			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	122
			り入れ「1.2.2 特徴」を一部追加。	1.2.2
			  「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。	3章
			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。	3.5、3.6
			「4.4 Next token モード時の認証手順」を一部変更。	4.4
			「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	付録

# 目次

1. 概要
1.1 RSA SecurIDについて
1.2.6 AXシリースの認証モート 14
<ul> <li>2.1 サポート状況</li></ul>
<b>3.</b> システム構築例(固定VLANモード)16
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 スイッチの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       20         3.3.3 AX3630Sのコンフィグレーション       22         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
4. クライアント認証手順	48
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
F	
3. 動作確認方法	56
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
6. 注意事項	58
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
付録. コンフィグレーション	58

### 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。



#### 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。

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.	は <b>1.1.4 トークン</b> を参照して下さい。				

表 1.1-1 RSA SecurID のコード名称

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 Wndows 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。



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 Applience3.0 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 Applience2.0 ユーザ も対象に、RSA SecurID Applience2.0 及び、RSA SecurID Applience3.0 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 Applience3.0 の他の新機能については、 RSA SecurID Applience 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 $\pm - \ddagger$

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。

- 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。





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

AX シリーズ認証ソリューションガイド (RSA SecurID 編)

#### 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1.2.6AX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	0	0	
New PIN モード	0	_	
Next token モード	0	_	

(凡例) 〇: 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2.1.1AX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4.3New 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 単位にアクセスり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。

認証方式	AX1230S	AX1240S	AX2400S、 AX3600S	AX6300S、 AX6700S		
802.1X 認証	—	—	—	_		
Web 認証	Δ	0	0	Δ		
MAC 認証	—	—	—	-		

表 2.1-1 連携可能な AX シリーズ

(凡例) O: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。
 一: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。

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

#### 表 2.2-1 認証モードごとの最大認証端末数

(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。



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。

役割	製品名		バージョン	備考	
	1	RSA SecurID Appliance 100		2.0	BSA Securito Appliance けいージョンに応
		ソフトウェア	RSA Authentication Manager	6.1.2	じて使用する機器が変わります。
RSA SecurID			RSA RADIUS Server	6.1	
Appliance	٢	RSA SecurID	Appliance 130	3.0	RSA Authentication Manage7.1 から RSA
	۷.	ソフトウェア	RSA Authentication Manager	7.1	RADIUS Sever を統合しています。
	<u>ハ</u> ー	ドウェア	RSA SecurID SID700	_	
トークン	トー	クン			トークンについては <b>1.1.4トークン</b> を参照し
	ソフトウェア トークン		RSA SecurID Token for Windows Desktops	4.0	て下さい。
コアスイッチ	AX3630S			11.1.A	   本システムで使用する DHCP サーバ
DHCPサーバ					
認証スイッチ	AX1240S、 AX2430S		40S.		Web 認証を行う
				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					MAC 認証用 RADIUS サーバ
DNS サーバ	OS		Windows Server 2003	SP1	本システムで使用する DNS サーバ
サーバ操作端末					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。

表 3.1-1 認証システム構成機器一覧

(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。

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
				20	MAC 認証
	アップリンク接続	トランクポート	100、1000	23~24	—
AX1240S	認証用	アクセスポート	100	1~10	Web 認証
				24	MAC 認証
	アップリンク接続	トランクポート	100、1000	25~26	—

表 3.1-2 認証スイッチのポート構成

#### 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。

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 3.1-3 VLAN 定義

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	0	0
	認証前、及び認証失敗端末	×	Δ
151	<u>ヽ ゞにっと ぃ ゞにてっ</u>	· · · · · · · · · · · · · · · · · · ·	

(凡例)〇:通信可能 ×:通信不可 Δ: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 のコンフィグ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。

- 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ができない機器(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ができない機器(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

AX シリーズ認証ソリューションガイド (RSA SecurID 編)

#### 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	
事前設定	
(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。
VLAN の定義	
(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。
スパニングツリーの設定	
(config)# spanning-tree disable	スパニングツリーを無効にします。
インターフェイスの設定	
物理ポートの設定	
<ul> <li>●認証用         <ul> <li>(config)# interface range gigabittethernet 0/1-10</li> <li>(config-if-range)# switchport access vlan 100</li> <li>(config-if-range)# web-authentication port</li> <li>(config-if-range)# authentication ip access-group</li></ul></li></ul>	<ul> <li>認証ポートの設定 ポート0/1~10をアクセスポートのVLAN100に設定します。</li> <li>Web認証対象ポートの設定をします。</li> <li>認証前アクセスリスト "WebAuth"を設定します。</li> <li>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。</li> <li>ポート0/20をアクセスポートのVLAN100に設定します。</li> <li>MAC認証対象ポートの設定をします。</li> <li>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。</li> <li>アップリンクポートの設定</li> <li>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。</li> </ul>
LAN インターフェイスの設定	
(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。
デフォルトルートの設定	
(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。

アクセスリストの作成	
ip access-list extended "WebAuth" 10 permit udp any any eq bootps 20 permit udp any any eq domain	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) 「認証前アクセスリストの設定」
Web 認証の設定	
<pre>(config)# web-authentication system-auth-control (config)# web-authentication ip address 1.1.1.1 (config)# aaa authentication web-authentication</pre>	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。
MAC 認証の設定	
<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>	MAC認証を有効にします。 MAC認証専用に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)
	「MAG認証の設定」
RADIUS サーバの設定	
(config)# radius-server host 10.51.0.3 key "alaxala"	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。

3.3.2 AX1240S のコンフィグレーション

edge#1 (AX1240S)の設定	
事前設定	
(config)# system function filter extended-authentication	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。
	※設定後は、装直の再起動が必要です。
(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。
VLAN の定義	
(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。
スパニングツリーの設定	
(config)# spanning-tree disable	スパニングツリーを無効にします。
物理ポートの設定	
<ul> <li>●認証用         <ul> <li>(config) # interface range fastethernet 0/1-10</li> <li>(config-if-range) # switchport access vlan 100</li> <li>(config-if-range) # web-authentication port</li> <li>(config-if-range) # authentication ip access-group</li></ul></li></ul>	<ul> <li>認証ポートの設定 ポート0/1~0/10をアクセスポートのVLAN100に設定 します。</li> <li>Web認証対象ポートの設定をします。</li> <li>認証前アクセスリスト "WebAuth"を設定します。</li> <li>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。</li> <li>ポート0/24をアクセスポートのVLAN100に設定しま す。</li> <li>MAC認証対象ポートの設定をします。</li> <li>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。</li> <li>アップリンクポートの設定 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。</li> </ul>
VLAN インターフェイスの設定	
(config)# interface vlan 100 (config-if)# ip address 192.168.100.12 255.255.255.0	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 172.16.0.12 255.255.255.0	管理用VLAN1000にインタフェースIPアドレスを設定 します。
デフォルトルートの設定	
(config)# ip route 0.0.0.0 0.0.0 172.16.0.1	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。

アクセスリストの作成	
ip access-list extended "WebAuth" 10 permit udp any any eq bootps 20 permit udp any any eq domain	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) 「認証前アクセスリストの設定」
Web 認証の設定	
(config)# web-authentication system-auth-control (config)# web-authentication ip address 1.1.1.1 (config)# aaa authentication web-authentication default group radius	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。
MAC 認証の設定	
<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>	<ul> <li>MAC認証を有効にします。</li> <li>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。</li> <li>MAC認証専用に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。</li> <li>RADIUSサーバでMAC認証を行うことを設定します。</li> <li>設定ポイント(3)</li> </ul>
	「MAC認証の設定」
RADIUS サーバの設定	
(config)# radius-server host 10.51.0.3 key "alaxala"	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。

#### 3.3.3 AX3630S のコンフィグレーション

core#1 (AX3630S)の設定	
事前設定	
(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。
VLAN の定義	-
(config)# vlan 1 (config-vlan)# state suspend	VLAN1 は使用しないため、無効にします。
(config)# vlan 50,51,100,1000 (config-vlan)# state active	各 VLAN50,51,100,1000 を作成します。
スパニングツリーの設定	
(config)# spanning-tree disable	スパニングツリーを無効にします。
インターフェイスの設定	•
物理ポートの設定	
●業務サーバ用 (config)# interface gigabitethernet 0/1 (config-if-range)# switchport access vlan 50	<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。
●認証サーバ (RSA SecurID) 用 (config)# interface range gigabitethernet 0/2-3 (config-if-range)# switchport access vlan 51	<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。
●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	<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。
VLAN インターフェイスの設定	•
(config)# interface vlan 50 (config-if)# ip address 10.50.0.1 255.255.255.0	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。
(config)# interface vlan 51 (config-if)# ip address 10.51.0.1 255.255.255.0	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。
(config)# interface vlan 100 (config-if)# ip address 192.168.100.1 255.255.255.0	   認証用 VLAN100 にインタフェース IP アドレスを設定し   ます。
(config-if)# ip address 172.16.0.1 255.255.255.0	   管理用 VLAN1000 にインタフェース IP アドレスを設定し   ます。
DHCP サーバの設定	
<pre>(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</pre>	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。
(config)# service dhcp vlan 100	   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。

AX シリーズ認証ソリューションガイド (RSA SecurID 編)

#### 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3.6RSA 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用端末を 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<sup>®</sup> 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) ヘトークン割り当て
  - 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。

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

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

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用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 ございません。引き続き RSA Authentication Manager の設定を進めて下さい。

#### (1) Agent Host の登録

①操作用端末から 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

項 番	項目	值	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	

表	3.5-2	Agent	Host	の設定
---	-------	-------	------	-----

※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「Defailt 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。)

		-
Default Login: user0	1	
Default Shell:		
€ Local User ○ Remote Us	ser	
Serial Number Tol	ken Type/Auth With Statu	s
okens:		A
		<b>*</b>
O: Original token R:	Replacement for previous token	
iole: <none> ssigned Profile:</none>		
lole: <none> ssigned Profile:</none>		
iole: <none> ssigned Profile: Temporary User</none>		
iole: <none> ssigned Profile: Temporary User Start Date: 81/81/1986</none>	89:88 End Date: 81/81/198	6 89:88
iole: <none> ssigned Profile: Temporary User Start Date: 01/01/1986 7 Allowed to Create a PIN</none>	09:00 End Date: 01/01/198 ┌─ Required to Create	6 89:00 : a PIN
lole: <none> ssigned Profile: Temporary User Start Date: 01/01/1986 7 Allowed to Create a PIN Assign Token</none>	09:00 End Date: 01/01/198 ☐ Required to Create Edit Assigned Token	6 09∶00 ≥ a PIN Administrative Role
lale: <none> ssigned Profile: Temporary User Start Date: 01/01/1986 7 Allowed to Create a PIN Assign Token Group Memberships</none>	99:00 End Date: 01/01/198 Required to Create Edit Assigned Token Agent Host Activations	6 09:00 a PIN Administrative Role Edit User Extension Data
lale: <none> ssigned Profile: Temporary User Start Date: 01/01/1986 7 Allowed to Create a PIN Assign Token Group Memberships SetyChange User Password</none>	99:00 End Date: 01/01/198 F Required to Create Edit Assigned Token Agent Host Activations Remove User Password	6 09:00 a PIN Administrative Role Edit User Extension Data Edit Access Times
lale: <none> ssigned Profile: Temporary User Start Date: 01/01/1986 / Allowed to Create a PIN Assign Token Group Memberships Set/Change User Password Assign Profile</none>	09:00 End Date: 01/01/198 Required to Creat Edit Assigned Token Agent Host Activations Remove User Password Remove Profile Assignment	6 09:00 a PIN Administrative Role Edit User Extension Data Edit Access Times Delete User
lale: <none> ssigned Profile: Temporary User Start Date: 01/01/1986 7 Allowed to Create a PIN Assign Token Group Memberships SetyChange User Password Assign Profile</none>	99:00 End Date: 01/01/198 F Required to Creat Edit Assigned Token Agent Host Activations Remove User Password Remove Profile Assignment	6 09:00 a PIN Administrative Role Edit User Extension Data. Edit Access Times Delete User

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。

Confirmation		×
This user wil continue?	I be added to the database. Do you want to	
Yes	No	
<b>S</b> 0 0 0	DCA Authoritization Manage	- の乳白

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。

Serial Number:		
Select Token from Li	st	
Auto Select:		
Unassigned Token	Sorted by:	Token Import Date
		C Token Serial Number
		• Token Expiration Date

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。

Algorithm:	All Algorithm	is 💌	
Assigned Tok	ens		
✓ Unassigned <sup>¬</sup>	Fokens		
Serial Number	Expiration	Auth With	
000053844786	06/30/2010	Passcode	<b>[</b>
000053844788	06/30/2010	Passcode	
000053844789	06/30/2010	Passcode	
000055580485	06/30/2009	Passcode	
000055580486	06/30/2009	Passcode	
			-

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。

	la Lascidanici assess		alaxala		
	Default Login <sup>,</sup> user01		120		_
	Dendari Logini (				
	Default Shell:				
• Loca	al User 🔿 Remote Us	er			
:	Serial Number Tok	en Type/Auth With	Status		
okens:	000053844786 Key	Fob/Passcode	Enabled	;New PIN Mode	<u> </u>
					*
cianed	Drofile:				
ssigned	Profile:				
ssigned	Profile:				
ssigned Tempo	Profile: prary User	301-80 E-J D-4-1 8	1 / 84 / 1002	80.80	
ssigned Tempo Start Allowe	Profile: prary User Date: 01/01/1986 1 d to Create a PIN	89:00 End Date: 0 □ Require	1/81/1986 d to Create	a 99:00	
ssigned Tempo Start Allowe	Profile: prary User Date: 01/01/1986 d to Create a PIN	99:80 End Date: 8 Γ Require	1/01/1986 d to Create	a PIN	
ssigned Tempo Start Allowe A	Profile: orary User Date: 01/01/1986 Id to Create a PIN ssign Token	99:00 End Date:0 ☐ Require Edit Assigned Tol	1/01/1986 d to Create <en< td=""><td>6 89:00 a PIN Administrative</td><td>Role</td></en<>	6 89:00 a PIN Administrative	Role
ssigned Tempo Start Allowe A Grou	Profile: orary User Date: 01/01/1986 d to Create a PIN ssign Token p Memberships	99:00 End Date: 0 Require Edit Assigned Tol Agent Host Activat	1/81/1986 d to Create ken ions	a 09:00 a PIN Administrative Edit User Extensi	Role on Data
ssigned Tempo Start Allowe A Grou Set/Cha	Profile: arary User Date: 01/01/1986 1 d to Create a PIN ssign Token p Memberships nge User Password	99:00 End Date: 0 Require Edit Assigned Tol Agent Host Activat Remove User Pas	1/81/1986 d to Create ken ions sword	09:00 a PIN Administrative Edit User Extensi Edit Access Ti	Role on Data mes
ssigned Tempo Start Allowe A Grou Set/Chan	Profile: prary User Date: 01/01/1986 1 d to Create a PIN ssign Token p Memberships nge User Password ssign Profile	99:80 End Date: 0 Require Edit Assigned Tol Agent Host Activat Remove User Pas Remove Profile Ass	1/81/1986 d to Create ken ions sword ignment	a PIN Administrative Edit User Extensi Edit Access Ti Delete Us	Role on Data mes er
ssigned Tempo Start Allowe Grou Set/Chai A Viev	Profile: Date: 91/01/1986 1 d to Create a PIN ssign Token nge User Password ssign Profile w LDAP Source	19:00 End Date: 0	1/81/1986 d to Create ken ions sword ignment scode	69:88 a PIN Administrative Edit User Extensi Edit Access Ti Delete Us Clear Windows F	Role on Data mes er 2assword

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)

Available Agen	it Hosts	Agent Hosts Directly Activat	ed On
LAXALA-RSA	<u> </u>		1
X1240S			-
	-		
	×		• •
L	¥	<ul> <li>✓</li> <li>Edit Activation Data</li> </ul>	

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")

	te User
	Host: AX1240S
	ser: user01 alaxala
_	gin: user01
	ıell:
lser	OK Cancel Help Deactivat
	ok Cancel Help Deactivat

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。

dit User	
First and Last Name: user01	alaxala
Default Login: user01	
Default Shell:	
g Agent Hosts Activations	×
User: user01 alaxala	
tot	
Available Agent Hosts	Agent Hosts Directly Activated On
	AX1240S
51	
Activate On Agent Hosts	Edit Activation Data
Filter	Edit Agent Hosts
51	
ExitHelp	
OK Cancel Apply L/S Changes S	Set All L/S Help

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。

Serial Number:	0000538447	86
Algorithm:	All Algorithm	is 🔻
Assigned Tol	ens	
7 Unassigned	Tokens	
Serial Number	Expiration	Auth With
000053844786	06/30/2010	Passcode
000053844788	06/30/2010	Passcode
000053844789	06/30/2010	Passcode
000055580485	06/30/2009	Passcode
000055580486	06/30/2009	Passcode
		2
	- r	

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。

t Token	
Key Fob with 6 digits, changing every 60 se	conds. Algorithm is AES.
Serial Number: 000053844786	
Assigned to: user01 alaxala	
Next Tokencode Mode: Off	
Lost Status: Not Lost	
Last Login Date (UTC): 03/18/2009	08:41 🔽 Enabled
Token Start Date: 03/23/2007	09:00
Token Shutdown Date: 06/30/2010	09:00 🗵 New PIN mode
Token Assignment Date (UTC): 03/18/2009	07:28
Offline Auth. Expiration (UTC): 01/01/1986	00:00
User Authenticates With: 🖲 Passcode	C Tokencode Only
Resynchronize Token	Clear PIN
Set PIN to Next Tokencode	Edit Assigned User
Assign Token	Unassign Token
Delete Token	Edit Lost Status
Edit Token Extension Data	Assign Replacement Token
Re-Issue Software Token	View Emergency Tokencode
OK Cancel	Help

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。

Set PIN to Next Tokencode
Serial Number: 000053844786
Enter the code displaying on the token.
685623
OK Cancel Help

図 3.5-12 RSA Authentication Manager の設定 12

④PIN 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。)
-------	---------	------------	------	--------	------------	---------

Set PIN to Next Tokencode
Serial Number: 000053844786
Enter the code displaying on the token.
685623
The PIN will be the first 4 digits of the next tokencode.
Cancel Help

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。

Al a saith as t		
Algorium.	All Algorium	
Assigned Tok	ens	
🔽 Unassigned	Fokens	
Serial Number	Expiration	Auth With
000053844786	06/30/2010	Passcode
000053844788	06/30/2010	Passcode
000053844789	06/30/2010	Passcode
000055580485	06/30/2009	Passcode
000055580486	06/30/2009	Passcode

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。

Edit Token	×			
Key Fob with 6 digits, changing ev	every 60 seconds. Algorithm is AES.			
Serial Number: 000053844786				
Assigned to: user01 alaxala				
Next Tokencode Mode: Off				
Lost Status: Not Lost	ist			
Last Login Date (UTC): 03/	9/18/2009 10:35 🔽 Enabled			
Token Start Date: 03/23/2007 09:00				
Token Shutdown Date: 06/30/2010 09:00 🗖 New PIN mode				
Token Assignment Date (UTC): 03/18/2009 07:28				
Offline Auth. Expiration (UTC): 01/	1/01/1986 00:00			
User Authenticates With: 💿 P	Passcode O Tokencode Only			
Resynchronize Token	Clear PIN			
Set PIN to Next Tokencode	Edit Assigned User			
Assign Token	Unassign Token			
Delete Token	Edit Lost Status			
Edit Token Extension Data	Assign Replacement Token			
Re-Issue Software Token	View Emergency Tokencode			
OK Cancel	Нер			

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。

dit Token	
Key Fob with 6 digits, changing every 60	) seconds. Algorithm is AES.
Serial Number: 000053844786	3
Assigned to: user01 alaxala	a
Next Tokencode Mode: Off	
Lost Status: Not Lost	
Last Login Date (UTC): 03/18/20	109 10:35 🗹 Enabled
Token Start Date: 03/23/20	07 09:00
Token Shutdown Date: 06/30/20	10 09:00 🗹 New PIN mode
Token Assignment Date (UTC): 03/18/20	09 07:28
Offline Auth. Expiration (UTC): 01/01/19	86 00:00
User Authenticates With: 💿 Passco	de 🔿 Tokencode Only
Resynchronize Token	Clear PIN
Set PIN to Next Tokencode	Edit Assigned User
Assign Token	Unassign Token
Delete Token	Edit Lost Status
Edit Token Extension Data	Assign Replacement Token
Re-Issue Software Token	View Emergency Tokencode
OK Cancel	Help

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。

RSA RADIUS Po	wered by Steel-Belted Radius (RSA-ALAXALA)
Page         Web         He           Image         Meb         He           Image         Meb	np 🕒 👌 Edit 🔇 Cut 😜 Copy 🎧 Paste 🐼 Delete
RSA RADIUS Server     RADIUS Clie     Profiles     Replication     Statistics	Administration nts At1230S 172.16.0.12 - Standard Radius - AX2430S 172.16.0.11 - Standard Radius -
Edit RADIUS Client	×
Name:	AX1240S
Description:	
IP Address:	172.16.0.12
Shared secret:	ו••••
Make/model:	Standard Radius -
Advanced Use differe	nt shared secret for Accounting Edt
Assume do	wm if no keepaive packets after j seconds

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。

Stee RSA RADIUS Powered by Stee	I-Belted Radius (RSA-ALAXALA)	<u>_     ×</u>
Open Failer         web         Open Failer           Image: Sector	iait 🚯 Cut 😜 Copy 🌑 Pasta 🐼 Delete	,
RSA RADIUS Server Administration     RADIUS Clients     Profiles     Participa	Name         Description           FOR_VLAN90         staticvlan           YLAN100	
Statistics	ofile ame: VLAN100	×
Đ	Attributes Check list Return list	
	Attribute Value Default User-Name user01	
	•	
	Add Edit Delete	
	<u>O</u> K <u>Cancel</u>	

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

Edit Profile					×
Name: Description:	VLAN300				0
Attributes					
Check list	Return list				_
	Attribute	Valu	e	Echo	
Tunnel	-Medium-Type	802			
Tunnel	-Private-Group-ID	300			
Tunnel	-Туре	VLAN			
Add	Edit	Dejete			
	Se	ve <u>C</u> anc	el		



#### (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。

<b>à</b> 1	RSA Auth	ientica	tion Ma	nager	6.1.2 Admin	istratio	n RSA	-ALAXAL	A					- O ×
Eile	<u>S</u> ystem	User	<u>T</u> oken	Group	Agent Host	<u>R</u> ealm	Sįte	RA <u>D</u> IUS	Log	R <u>e</u> port	Help			
		Add P	rofile										×	
		Ente		ufile na	me The n	ame n	et i	natch th		nfile na	me in :	vour	_	
		RAD	IUS se	erver d	atabase a	nd ma	y con	tain up	to 48	chara	cters,	your	_	
		inclu	ıding l	etters,	spaces, a	nd syr	nbols	3.					_	
													_	
		Prof	ile Nai	ne: VL	AN100								_	
													_	
			04		anaal				Ца	- 1			_	
			UK		ancer			_	пе	Р			_	
			_	_		_	_	_	_	_	_	_		
														_

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。

Edit User		×
First and Last Name: RSA	Alaxal	a
Default Login: user01		
Sele	ect Profile	×
Default Shell:	lame:	
💿 Local User 🔿 Remote		
Serial Number Tokens: 000053088864	/LAN100	<u>~</u>
0: Original token		
Role: <none></none>		
Assigned Profile:		
🗆 Temporary User		*
Start Date: 01/01/1986		
Allowed to Create a PIN	OK Cancel He	:lp
Assign Token		
Group Memberships	Agent Host Activations	Edit User Extension Data
Set/Change User Password	Remove User Password	Edit Access Times
Assign Profile	Remove Profile Assignment	Delete User
View LDAP Source	View Emergency Passcode	Clear Windows Password
OK Cancel Apply L/S	Changes Set All L/S	lelp

図 3.5-21 RSA RADIUS Server の設定 5

③以上で設定は終了です。

AX シリーズ認証ソリューションガイド (RSA SecurID 編)

#### 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3.5RSA 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 Appliance3.0 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 Appliance3.0 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
- ① 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
- (1) 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。

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

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

#### 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。

🚈 RSA Security Console: - Welcome Administrator - Microsoft Internet Explorer	
ファイル(E) 編集(E) 表示(V) お気に入り(A) ツール(T) ヘルプ(H)	an a
🔇 戻る • 🕞 - 💌 😰 🏠 🔎 検索 🣩 お気に入り 🚱	» アドレス(2) (塗) https://securid.example.co.jp:7004/console-ims/Home.do 💽 💽 移動
リンク 🥑【価格.com】 🥑 CSEWeb 🥑 NAVITIME 🍓 SNB-SHOP 🥑 リシテフ	P 🥑 リモート デスクトップ 🥑 駅探 🥑 国語辞書 🎒 天気予報 🍪 日情動怠 🍪 翻訳@nifty 🤍 🎽
RSA Security Console	Logged on as: nts001 <u>My Permissions</u>   <u>My Preferences</u>   <u>Log Off</u> Realm: SystemDomain   <u>Configuration</u>
Home Identity  Authentication  Access  Reporting  RADIUS	Administration      Setup      Help
🗋 🛛 Realm: SystemDomain	I Help on this page *
Welcome nts001. You logged on: Monday, June 15, 2009 5:43 PM .	
My Console	About Console
My Permissions	* All Help Topics
My Preferences	Online Support at RSA SecurCare Online
	Software Version Information
	Check License Status
Copyright @2007 -	2008 RSA Security Inc. All rights reserved.
	* *
ē	

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。操作用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。

me	Identity 💌	Authenticat	on 🔻	Access 🔻	Reporting 🔻	RADIUS 🔻	Administration 🔻	Setup 🔻	Help 💌	
						RADIUS Ser	vers		1	
Add New Authentication Agent				RADIUS Clients		Manage Existing		Li Help on this page ▼		
	Authentication	agents provid	le a sec	ure two-way	communication p	RADIUS Profiles		Add New		ser attempts to gain access to a network resource, the
	agent receives	s the authentio	ation re	equest and s	ubmits it over a s	RADIUS Use	r Attribute Definition:	;		-
	Cancel		ave	57		RADIUS Stat	tistics	•		

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。

* Required field	
RADIUS Client Settings	
I Client Name: * AX24305	
ANY Client:	
IP Address: * 172.16.0.11	
👔 Make / Model: 👘 - Standard Radius -	
i Shared Secret: *	
Accounting:     Use different shared secret for Accounting	
Client Status:     Assume down if no keepalive packets are sent in the specified inact	tivity time.
Notes:	

図 3.6-3 RADIUS Client の設定 2

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

#### 表 3.6-2 RADIUSClient 設定

※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。

Confirmation	Required			
The hostname or	IP address you have entered ca	annot be resolved.		
IP Address:	172.16.0.11			
Hostname:	AX24305			

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。

Add RADIUS Profi	le		i Help on this page ▼
Add RADIUS Profile Properties.			
Cancel 🔀 Save	Σ		
14	* Required field		
<b>RADIUS Profile Basics</b>			
i Profile Name:	* WebAuth		
Notes:			
Return List Attributes			
These attributes are returned you do not want to specify a	by the RADIUS server to the RADIUS client in an accept me articular value but want to make sure the attribute value in	ssage when the server authenticates the user. You the request is echoed to the RADIUS client.	may select <b>Echo</b> for an attribute i
🚺 Return List Attributes:	Attribute Service-Type 🔹	Add <b>&gt;</b> Update <b>&gt;</b>	

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。)

RADIUS Profiles Add New D	I Help on this page *
RADIUS profile is used to customize a user's session and authentication requirements.	
Added 1 Radius profile.	
1 items found.	
Show 25 🔽 per page	
Profile Name	Notes
WEBAUTH →	
Profile Name	Notes
Show 25 💌 per page	
1 items found.	



※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

These attributes are returned	by the RADIUS server to the RADIUS client in an accep	t message when the server authenticates the user. You may select <b>Echo</b> for an attribute il
you do not want to specify a p	particular value but want to make sure the attribute val	Je in the request is echoed to the RADIUS client.
1 Return List Attributes:	Attribute Service-Type Value  Echo Tunnel-Medium-Type:802:NoEcho Tunnel-Private-Group-ID:300:NoEcho Tunnel-Type:VLAN:NoEcho	Add Dupdate Down

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。 3.6.2RSA RADIUS Serverの設定と同様に操作用端末のブラウザよりRSA SecurID Appliance3.0 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。

RS	🔨 Secu	rity Console		Logged on as: nts001 <u>My Permissions</u>   <u>My Preferences</u>   Realm: SystemDomain   <u>Conf</u>	Log Ol iguratio
Home	Identity 🔻	Authentication 🔻 🛛 Access 👻	Reporting - RADIUS - Ad	Administration • Setup • Help •	
		Policies •			
	Realm:	SecurID Tokens	Manage Existing	Left Point Help on this page 1	
	Welcome ntsO(	On-Demand Tokencodes	Statistics		
		Software Token Device Types 🕨	Import Tokens Job	Manage Existing	
	My Conso	Token Attribute Definitions	Distribute Software Tokens Job	ionsole	

#### 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。

t SecurID Tokens Job	Help on this page *
mport, specify options, and click Import.	
* Required field	
* ImportTokens_20090616_1637PM	
trol	
SystemDomain 💌	
* D:¥評価¥検疫認証¥認証¥Radius¥RSASecurID¥Applian 1996日	
(Required only if file is password-protected.)	
Ignore all duplicate tokens     Orverweite all duplicate tokens	

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。

🚵 🛛 Import SecurID Tol	ken Jobs 🛛 Refresh 🚺			i Hel	p on this page 🔻
In Progress Completed	ss that you can cancel. When an import token job is comp	lete, you can view	, the results summary from th	e Completed tab.	
Where:	1 items found.				
	0 selected: Cancel Job >			Sł	now 25 💽 per page
	Distance Job Name	Status	Submitted On	Submitted By	<u>% Complete</u>
	□ http://www.commonstance.com/commonstance.com/commonstance.com/commonstance.com/commonstance.com/commonstance.com/com/com/com/com/com/com/com/com/com/	In Progress	6/16/09 4:39:33 PM JST	nts001	0
Search 2	Dob Name	<u>Status</u>	Submitted On	Submitted By	% Complete
	0 selected: Cancel Job <b>&gt;</b>	20		Sł	now 25 💽 per page
	1 items found.				

Convrint @2007 - 2008 RSA Security Inc. All rights reserved.

#### 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。)

Cancel 🔀 Sa	ve 🔰 🛛 Save & Add Another 🄁
	* Required field
Administrative Contr	ol
i Identity Source:	* Internal Database 💌
i Security Domain:	SystemDomain 💌 administrators manage this user
User Basics	
First Name:	user01
Middle Name:	
Last Name:	* user01
i User ID:	* user01
Email:	
i Certificate DN:	
Notes:	A.
Password	
i Password:	* What's a valid password?

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。

Users Add Ne	w <b>&gt;</b>					i Help on this page *		
A user represents a person or	a system with a unique accou	nt within this realm.						
Search	Added 1 user(s)	). Search again to get an updat	ed list.					
Security Domain:	1 items found.	1 items found.						
Identity Source:	0 selected: Add to U	lser Groups	Go 🔁			Show 25 💌 per p		
Internal Database 💌	User ID	Last, First Name	Disabled	Locked	Security Domain	Identity Source		
For:	🗖 🔐 user01 🗸	user01, user01			°্≣ SystemDomain	Internal Database		
All Users	User ID	Last, First Name	Disabled	Locked	Security Domain	Identity Source		
Last Name	0 selected: Add to Us	ser Groups 🗾 🗌	Go 🔁			Show 25 💌 per p		
starts with	1 items found.							

図 3.6-12 Add User2

- (3) トークンの割り当て
  - 「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。

Necurity Co	nsole	II View	1			Realm: Sy	stemDomain   <u>Con</u> l
Identity	n 🕶 Access	🧨 Edit	ratio	Setup 🔻	Help 🔻		
Users Add Ne	w 🔰 (	Na User Group Membership Add More					I Help on this page
Search	1 item: 0	Administrative Roles Assign More	Go	D			Show 25 💌 p
SystemDomain 💌		SecurID Tokens		<u>Disabled</u>	Locked	Security Domain	Identity Source
Identity Source:		Assign More				°ন্≓ SystemDomain	Internal Database
Internal Database 💌		Assign Next Available SecurID Token		Disabled	Locked	Security Domain	Identity Source
For:	0 select	Manage Emergency Offline Access	Go	Σ			Show 25 💌 p
Where:	1 items	Authentication Settings					
starts with	_	📿 View Associated Policies					
user01		j) Duplicate					
		× Delete					

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。

3	User: User01 •	i Help on this page *
	Assigned SecurID Tokens	
	View SecurID Tokens assigned to the user and enable/disable user for On-Demand Tokencodes.	
	Assigned SecurID Tokens Assign Token	
	Currently there is no token assigned to the selected user.	
- 33		

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。

User: user01 •						
Imported and unassigned tokens are list	ed below. Select token(s) to assign t	o the selected user(:	s).			
Search	5 found. Showing 1-5.	2				
SystemDomain	Serial Number	Token Type	Algorithm	Requires Passcode	Disabled	E
For:	000204265260 -	Key Fob	AES-TIME	1	1	2
All Unassigned Tokens	000204265261 🗸	Key Fob	AES-TIME	1	~	2
Where:	□ 000204265262 -	Key Fob	AES-TIME	~	~	2
starts with	☐ 000204265263	Key Fob	AES-TIME	<b>v</b>	~	2
	D 000204265264 -	Key Fob	AES-TIME	~	~	2
More criteria	Serial Number	Token Type	Algorithm	Requires Passcode	Disabled	E
Search 🔁	1 selected: Assign 🔰					
	5 found. Showing 1-5.					_
	1	Convrigh	ዜ @2007 - 2008 R	SA Security Inc. All rights re-	served	

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

「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。

Search	1 items f	ound.		
Fecurity Domain:	0 sele	II View	Go 🔁	
SystemDomain 💌		🧨 Edit	Name	Disabled
Identity Source:		🗐 Harr Course Marshaushin	01	
Internal Database 💌	<b> </b>	Add More	Name	Disabled
For:	0 selec	Hadrorom	Go 🔁	
Where: Last Name	1 item:	Administrative Roles Assign More		
starts with view of the starts		SecurID Tokens Assign More		
Search  Advanced Search		Manage Emergency Offline Access		
		Authentication Settings	opyright ©2007 -	2008 RSA Security Inc. All r
	14			

図 3.6-16 RADIUS Profaile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。

RADIUS			
i User RADIUS Profile:	WEBAUTH -		
RADIUS User Attributes:	Attribute 20 - Callback-Id  Remove	Value Add 2 Update 2	
Cancel 🗙 Reset 🕻	Save D		

図 3.6-17 RADIUS Profaile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位に 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位に 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

ベートウェアトークン(RSA Security SiD700)を使用してAX シリースの 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。

🥖 - Windows Internet Explorer	
	- 🍫 🗙 Live Search 🖉 -
ファイル(E) 編集(E) 表示(Y) お気に入り(A) ツール(I)	~ レプ(圧)
* * @	
	LOGIN
Please ente	er your ID and password.
	- 5992 A.
user ID	E
password	
	Login
	LOGOUT
Please pu	sh the following button.
	Logout
ページが表示されました	😱 😜 インターネット   保護モード: 無効 🔍 100% 👻

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コード(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

🧀 - Windows Internet Explorer	
ⓒ	↓ ↓ ↓ Live Search      ♀      ✓
ファイル(E) 編集(E) 表示(V) お気に入り(A) ツール(I) ヘルプ(H)	
* * 6	
LOGIN	
Please enter vour ID and p	assword.
user ID user01	E
password	
Login	
LOGOUT	
Please push the following	button.
Logout	
	▼ - ネットし保護エード・無効 ● 10004 ■
L.9 😽 1.25	100% *

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。

🧭 - Windows Internet Explorer			×
G + https://1.1.1.1/cgi-bin/Process.cg	1	🕶 🔒 🍫 🗙 Live Search	o 🗸
**		🗿 🔻 🗟 👻 🖶 👻 🔂 ページ(P) 🔻 🎯 ツール(Q)	• »
	Login success		*
	Login_Time 2009/06/22 17:49	:39 JST	
	Logout_Time 2009/06/22 18:49	:39 JST	
	close		
	LOGOUT		
	Please push the following butto	on.	
	Logout		

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。

000	055580487 Optio	ns 💙 🗖 🏹
C	Passcode:	
	8250 499	4
	Re-enter PI	N Copy
RSA	SecuriD*	

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。

🧀 - Windows Internet Explorer	x
ⓒ ◯ ▽ 🖻 http://1.1.1.1/	> +
ファイル(E) 編集(E) 表示(V) お気に入り(A) ツール(I) ヘルプ(H)	
☆	• **
	Â
LOGIN	
Please enter your ID and password.	
	m
publicity	
Login	
LOGOUT	2
Please push the following button.	
Logout	_
ページが表示されました 🛛 🔓 🥥 インターネット   保護モード: 無効 🔍 100% 🔹	•

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

🍘 - Windows Internet Explorer	
• • • http://1.1.1/	<ul> <li>→ × Live Search</li> <li>P →</li> </ul>
ファイル(E) 編集(E) 表示(V) お気に入り(A) ツール(I) ヘルプ(H)	
	$\bigcirc \bullet \bullet \bigcirc \bullet \bullet \bullet \bigcirc \bullet \bullet \circ \bigcirc \bullet \circ \bullet \circ ) \bullet \circ \bigcirc \bullet \circ \circ$
	<u>^</u>
LOGIN	
Please enter your ID and pa	assword.
	=
passworu	
Login	
LOGOUT	
Please push the following	putton.
Logout	
	ーネット   保護モード: 無効 🔍 100% 👻

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。

🧀 - Windows Internet Explorer	
	✓ 4 × Live Search
ファイル(E) 編集(E) 表示(Y) お気に入り(A) ツール(I) ヘルプ(H)	
* * 6	
	·
LOGIN	
Please enter your ID a	and password.
user ID	=
password	
Login	
LOGOU	Г
Please push the follo	wing button.
Logaut	
ページか表示されました	インターネット   保護モート: 無効 € 100% ▼

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。

🤌 - Windows Internet Explorer			
		- + X Live Search	+ ۹
ファイル(E) 編集(E) 表示(V) お気に入り(A) ツー	·ル(エ) ヘルプ(H)		
* * 🔾		🏠 ▼ 🗟 ▼ 🖶 ▼ 🔂 ページ(P) ▼	() ッール( <u>0</u> ) ▼ <sup>≫</sup>
			<u>^</u>
	LOGIN		
Pleas	e enter vour ID an	d password.	
user ID	user01		E
password ••	••••		
	(Login)		
	LOGOUT		
Plea	se push the follow	ng button.	
(*************************************			+
存機中: http://1.1.1.1/cgi-bin/Login.cgi	Lø 😝 1	ンターネット   保護モート: 無効	≪ 100% ▼

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。

🤌 - Windows Internet Explorer	
🚱 🔵 🗸 🙋 http://1.1.1.1/cgi-bin/Login.cgi	✓ 47 × Live Search
ファイル(E) 編集(E) 表示(Y) お気に入り(A) ツール(I)	~レプ(圧)
* * @	
	*
R	eply Message
Enter a new PIN	having from 4 to 8 digits:
	Enter
	▼ □ 4ンターネット   保護モード: 無効

図 4.3-3 New PIN モード認証 3

④PIN の再入力が要求されますので同じ PIN を再び入力し「Enter」をクリックする。

🧀 - Windows Internet Explorer		
CO v Attp://1.1.1.1/cgi-bin/Process.cgi	✓ 4 Live Search	• ۹
ファイル(E) 編集(E) 表示(Y) お気に入り(A) ツール(I) ヘルプ(H)		
* * (2)	💧 🔹 🗟 🔹 🖶 🔹 📴 ページ(Ⴒ) 👻 🍈 ツール	ν( <u>ο)</u> ▼ <sup>≫</sup>
		*
Reply Message		
Please re-enter new H	PIN:	
••••	Enter	
		-
		-
	ターネット   保護モード: 無効 🔍 100	% 🔻 🔐

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。

🧀 - Windows Internet Explorer	
🚱 🔵 👻 http://1.1.1.1/cgi-bin/Process.cgi	
ファイル(E) 編集(E) 表示(Y) お気に入り(A) ツール(I) ヘルプ(H)	
* * @	$ \stackrel{\bullet}{} \bullet \boxtimes \bullet \stackrel{\bullet}{\twoheadrightarrow} \stackrel{\bullet}{} \bullet \stackrel{\bullet}{} \stackrel{\bullet}{$
Reply Message	
PIN Accepted. Wait for the token code to then enter the new passcode	change, 9: Enter
ページが表示されました 🛛 🐻 インタ	ーネット丨保護モード: 無効 🔍 100% 🔻

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、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、値が切り換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 sucess 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コードどちらでも入力可能です。

🥖 - Windows Internet Explorer		
🚱 💭 🗢 🖻 http://1.1.1.1/cgi-bin/Login.cgi	- 🍕 🗙 Live Search	P -
ファイル(F) 編集(E) 表示(V) お気に入り(A)	ツール(T) ヘルプ(H)	
* * @	🏠 ▼ 🗟 ▼ 🖶 ⊀−ジ(P) ▼	· ۞ ツール(0) ▼ <sup>≫</sup>
		*
	Reply Message	
	Wait for token to change, then enter the new tokencode: Enter	
, ページが表示されました	🎲 🍚 インターネット   保護モード: 無効	🔍 100% 🔻

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コ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。

l.	✓ ♣ ↔ × Live Search	<del>ب</del> ۾
	🟠 🔹 🔝 🔹 🖶 🔹 🔂 🗠 = 5(P) 🕶 🎯	ツール(0) ▼ <sup>≫</sup>
		*
Reply Message		
Access Denied		
Enter PASSCODE:		
	Enter	
	i Reply Message Access Denied Enter PASSCODE:	i

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。

💑 RSA Authentication Manager 6.1.2 Administration RSA-ALAXALA											<u> </u>				
Eile	System	User	<u>T</u> oken	Group	Agent Host	<u>R</u> ealm	Sįte	RADIUS	Log	Report	Help				
									Lo De De	g Statist slete by F slete <u>B</u> ef	ics Percenta ore a Dat	je e			
									A	utomate I	Log Mainl	enance			
									Ec	lit Log E <u>×</u>	tension (	)ata	•	Activity Lo	g Extension
									Ec	lit Syster	n Log Par	ameters.		Exception I Incident Lo	Log Extension og Extension
									Lo	g <u>F</u> ilterin	ig		•		



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

Log Entry Selection Criteria	×
Specify Log Entries by:	
C	
O Days Last: 1 day(s)	
C Date	
From Date: 06/10/2008 , 00:00:00	
To Date: 07/10/2008 , 23:59:59	
Filters:	
Current Login: *	Select
Affected User: *	Select
Affected Token: *	Select
Agent Host: *	Select
Group: *	Select
Server: *	
Site: *	Select
OK Clear Cancel Help	

図 5.2-2 RSA Authentication Manager ログ2

③認証ログが確認できます。

🚵 RSA Au	thentica	ation Ma	nager	6.1.2 Ad	ministrati	ion RSA	ALAXAL	A.				[	<u>-     ×</u>
<u>File</u> <u>Syste</u>	m <u>U</u> ser	<u>T</u> oken	Group	Agent H	lost <u>R</u> ealn	n Site	RA <u>D</u> IUS	Log	R <u>e</u> port	<u>H</u> elp			
Select L	og Entry	,											×
From	n: Start	of Log									To: En	d of Log	,
Pleas	se Sele	ect a Lo	g Entr	y:									
UTC Ti	me		Local	Time		Curre	nt User	Mes	sage				
07/10/	2008 1	1:00:18	07/10	/2008 2	20:00:18			ALM	delete	d log:	5		
07/10/	2008 1	1:00:17	07/10	/2008 2	20:00:17			ALM	archiv	ed log	gs		
07/10/	2008 1	1:00:15	07/10	/2008 2	20:00:15	Admir	nistrato	Exit	ed log i	monit	oring		
07/10/	2008 11	0:59:09	07/10	/2008 1	9:59:09	userO	2	Pas	scode a	ассер	ted		
07/10/	2008 10	0:59:09	07/10	/2008 1	9:59:09	userO	2	Ext-	auth ch	eck			
07/10/	2008 10	0:58:49	07/10	/2008 1	9:58:49	Admir	nistrato	RAD	IUS ad	minis	tration	stopped	
07/10/	2008 10	0:57:55	07/10	/2008 1	9:57:55	Admir	nistrato	RAD	IUS ad	minis	tration	started	
07/10/2	2008 10	0:57:47	07/10	/2008 1	9:57:47	Admir	nistrato	Exit	ed log i	monit	oring		
07/10/	2008 10	0:57:07	07/10	/2008 1	9:57:07	userO	2	Pas	scode a	ассер	ted		- L
•													
E	<b><it< b=""></it<></b>	Help					Edit I	.og E	xtensi	on Da	ta		
	-	-	-	-	-	-	-	-	-	-	-	-	
													_

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。

RS	🔨 Secu	rity Cons	ole	Logged on as: nts001 <u>My Permissions</u>   <u>My Preferences</u>   <u>Log</u> Realm: SystemDomain   <u>Configura</u>					
Home	Identity 🔻	Authentication 💌	Access 💌	Reporting 🔻	RADIUS 🔻	Administration	▼ Setup ▼	Help 🔻	
				Reports	•				
	🗃 🔪 Realm: SystemDomain			Scheduled Rep	port Jobs 🔹 🕨				i Help on this page *
	Welcome nts0	01. You logged on: V	Yednesday,	Report Outpu	t 🕨			_	
2				Real-time Acti	ivity Monitors 🕨	Authentication	Activity Monito	r .	
	My Conso	ble		3		System Activit	y Monitor	ble	
	2 Mu Down	in the second				Administration	Activity Monitor	r	
	• My Perm	ISSIONS					HITTOP TOP	<u>103</u>	

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。

۴)	Authentication Monitor							i Help on th	is page *			
	Pause Monitor	Cher Hankar 🔀										
	Display Results	Time	Activity Key	Description	Reason	User ID	Agent	Server Node IP	Client IP			
	Successful events Warning events Example avents	2009-06-17 11:16:15.222	Principal authentication	User "user01" attempted to authenticate using authenticator "SecurID_Native". The user belongs to security domain "SystemDomain"	Authentication succeeded in next tokencode mode	user01	securid.example.co.jp	10.51.0.3	10.51.0.3			
	Number of Results	8 2009-06-17 11:15:22.708	Principal authentication	User "user01" altempted to authenticate using authenticator "SecurID_Native". The user belongs to security domain "SystemDomain"	Authentication method failed, passcode format error	user01	AX12405	10.51.0.3	10.51.0.3			
	User ID starts with	1 2009-06-17 11:15:22.706	Next tokencode mode activated for token	Next tokencode mode activated for token serial number "000201265260" assigned to user "user01" in security domain "SystemDomain" from "Internal Database" identity source	N/A	user01	AX12405	10.51.0.3	10.51.0.3			
	Authentication Agent starts with	8 2009-06-17 11:15:10.981	Principal authentication	User "user01" attempted to authenticate using authenticator "SecurID_Native". The user belongs to security domain "SystemDomain"	Authentication method failed	user01	AX12405	10.51.0.3	10.51.0.3			
	Token Serial Number	8 2009-06-17 11:14:55.28	Principal authentication	User "user01" attempted to authenticate using authenticator "SecurID_Native". The user belongs to security domain "SystemDomain"	Authentication method failed	user01	AX12405	10.51.0.3	10.51.0.3			
	starts with	1 2009-06-17 11:14:17.896	Principal authentication	User "user01" attempted to authenticate using authenticator "SecurID_Native". The user belongs to security domain "SystemDomain"	Authentication succeeded in next tokencode mode	user01	securid.example.co.jp	10.51.0.3	10.51.0.3			

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ーの 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



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/