

# RADIUS サーバ設定ガイド fullflexEG7 編



第2版



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

#### はじめに

RADIUSサーバ設定ガイドfullflexEG7編は、AXシリーズでサポートしている認証機能を用いたシステム構築において、RADIUSサーバに株式会社アクセンス・テクノロジー 社のfullflexEG7を使用する場合の設定方法を示します。

#### 関連資料

- ・AXシリーズ 認証ソリューションガイド
- ・AXシリーズ製品マニュアル(<u>http://www.alaxala.com/jp/support/manual/index.html</u>)
- ・fullflexEG7 ユーザーズガイド
- ・アクセンス・テクノロジー社ウェブサイト(<u>http://accense.com/</u>)

#### 本ガイド使用上の注意事項

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

本資料の内容は、改良のため予告なく変更する場合があります。

#### 輸出時の注意

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

#### 商標一覧

- ・fullflexは株式会社アクセンス・テクノロジーの登録商標です。
- ・Ethernetは、米国Xerox Corp.の商品名称です。
- ・イーサネットは、富士ゼロックス(株)の商品名称です。
- ・Microsoftは、米国およびその他の国における米国Microsoft Corp.の登録商標です。
- ・Windowsは、米国およびその他の国における米国Microsoft Corp. の登録商標です。
- ・そのほかの記載の会社名、製品名は、それぞれの会社の商標もしくは登録商標です。

# 改訂履歴

版数	rev.	日付	変更内容	変更箇所
初版	—	2007.10.31	初版発行	—
第2版	—	2008.4.17	MAC 認証におけるユーザ名、パスワード設定に	5.1.1
			ついて AX スイッチのバージョン UP に対応し	
			ました。	
			AX1200S(1.3.B),	
			AX2400S(10.6.C),	
			AX3600S(10.6.C)	

# 目次

1	概要	6
1	.1. 概要	6
1	.2. 設定例環境	7
	1.2.1. 使用機器一覧とAXコンフィグレーション	7
	1.2.2. 設定例のネットワーク構成図	8
2.	fullflexEG7 の構成	9
2	.1.	
2	.2. サーバへのインストール	9
3.	IEEE802.1X認証の設定	9
3	.1. fullflexEG7 の設定	9
	3.1.1. RADIUSクライアントの設定	11
	3.1.2. ユーザの作成	13
	3.1.3. PEAP、TLSの設定	17
	3.1.4. IEEE802.1x認証時の端末再認証設定に関して	18
3	.2. Windows XP / Vistaの設定	19
	3.2.1. ユーザ証明書/ルート証明書の作成	19
	3.2.2. PEAP設定、認証の確認	25
	3.2.3. TLS設定、認証の確認	29
4.	Web認証の設定	32
4	.1. fullflexEG7 の設定	32
	4.1.1. ユーザの作成	32
4	.2. Windows XP / Vista の設定	32
	4.2.1. クライアントの設定	32
4	.3. Web認証の確認	33
5.	MAC認証の設定	36
5	.1. fullflexEG7 の設定	36
	5.1.1. ユーザの作成	36
5	.2. MAC認証の確認	39
6.	ログイン認証	40
6	.1. RADIUS サーバによる認証の設定	40

7.	認証ログの詳細な表示	に関して41	I
7.1	. fullflexEG7での認証ロ	グの詳細表示41	I
8.	Windows Vista PEAP	設定の際の注意点42	2

#### 1 概要

#### 1.1. 概要

本資料では認証スイッチにAXシリーズ、クライアントコンピュータにWindows XP, Windows Vista、 fullflexEG7をRADIUS、ユーザデータベースとして下記認証方式を使用したシステムを構築するための 設定方法を記載しています。

認証方式

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

使用方法

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

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

#### 1.2. 設定例環境

#### 1.2.1. 使用機器一覧と AX コンフィグレーション

使用機器一覧

RADIUS : fullflexEG7 Ver2.7.0 Supplicant : Windows XP SP2, Windows Vista Ultimate Authenticator : AX1230S(Ver1.3.B) / AX2430S(Ver10.6.C) L3switch : AX3630S (Ver10.6.C) HUB : EAPOL 透過機能有り

#### AX コンフィグレーション設定例

AX1230S の :	コンフィグレーション
hostname "AX1230S"	ip route 0.0.0.0 0.0.0.0 192.168.200.254
!	!
vlan 1	•dot1x vlan dynamic enable
name "VLAN0001"	• dot1x vlan dynamic radius-vlan 30-31
!	Odt1x vlan dynamic reauthentication
vlan 10 mac-based	!
!	dot1x system-auth-control
vlan 20 mac-based	!
!	mac-authentication system-auth-control
vlan 100	▲mac-authentication vlan 30
!	▲mac-authentication vlan 31
spanning-tree disable	mac-authentication interface fastethernet 0/24
spanning-tree mode pvst	mac-authentication id-format 1
!	!
interface fastethernet 0/24	web-authentication system-auth-control
switchport mode mac-vlan	web-authentication vlan 30
switchport mac vlan 30-31	web-authentication vlan 31
switchport mac native vlan 100	!
!	service dhcp vlan 100
interface gigabitethernet 0/25	!
media-type auto	ip dhcp pool "before"
switchport mode trunk	network 192.168.100.0
switchport trunk allowed vlan 30-31,200	lease 0 0 0 10
!	!
interface vlan 1	★radius-server host 192.168.10.2 key "alaxala"
!	aaa authentication dot1x default group radius
interface vlan 30	aaa authentication login default group radius local
ip address 192.168.30.253 255.255.255.0	▲aaa authentication mac-authentication default group radius
!	aaa authentication web-authentication default group radius
interface vlan 31	!
ip address 192.168.31.253 255.255.255.0	★aaa authorization network default group radius
interface vlan 100	line vty 0 0
ip address 192.168.100.253 255.255.255.0	!
interface vlan 200	
ip address 192.168.200.254 255.255.255.0	
!	

●IEEE802.1X 認証を行うためのコンフィグレーション ■Web 認証を行うためのコンフィグレーション ▲MAC 認証を行うためのコンフィグレーション ◆ログイン認証を行うためのコンフィグレーション ★RADIUS サーバ関連のコンフィグレーション(各認証方式共通) 1.2.2. 設定例のネットワーク構成図



#### ※認証する際の構成

ユーザ名:user03・user04・user05・user06 認証後の VLAN:VLAN30、31

Windows XP Windows Vista

# 2. fullflexEG7の構成

#### 2.1. 準備

インストールするサーバを用意してください。

なお、fullflexEG7の対応OSおよびハードウェアはfullflexEG7ユーザーズガイド,アクセンス・テクノロジー社ウェブサイト(<u>http://accense.com/</u>)を確認してください。

#### 2.2. サーバへのインストール

インストール方法については、fullflexEG7 のユーザーズガイド 2.インストール 2.1 準備をご参照ください。

なお、インストール時、管理者画面にアクセスするユーザ名とパスワードが表示されます。 以降の操作で必要になりますので忘れないようご注意願います。

# 3. IEEE802.1X 認証の設定

#### 3.1. fullflexEG7の設定

①:ご使用の Web ブラウザを起動し、サーバの IP アドレスに、fullflexEG7 インストール時に設定した管理画面表示用の HTTPS(SSL)ポート番号(標準:892)を付け足してアクセス。

#### ②:下記画面に移動したら、管理者用ページを選択。



Copyright @ 2001, 2002, 20

③:管理者用ページに入るには fullflexEG7 インストール時に表示されたユーザ名、パスワードを入力。

ユーザネ	ムンパスワードが必要です
3	https://192.168.10.2:892 の Privileged Area に対するユーザ名とパスワードを入力してください ユーザ名:
	admin
	パスワード
	*****
	OK キャンセル

#### ④:下記に示す管理者用ページが表示されます。



RADIUSクライアントを登録しましょう

#### 3.1.1. RADIUS クライアントの設定

#### ①: 左側メニューから、基本設定を選択。その中から RADIUS クライアントの設定を選択。



#### ②:RADIUS クライアントの追加を選択



③:認証スイッチの情報(クライアント名、IP アドレス、共有鍵(AX に設定した RADIUS 鍵))を入 カし保存。



#### ④:一覧に戻り、RAIDUS クライアントが作成されていることを確認。



# 3.1.2. ユーザの作成

# ①:管理者用ページのユーザ設定を選択し、下記画面を表示する。

LLDV/NA	アクセスを許可するユーザの設定 アクセスを許可するユーザを設定します。あるユー 報を元にキーワード検索や表示ユーザの叙込みも ドとアッフロード(の)で行ってください。	ザを一時的に無効、 5できます。新規ユーザ (F)	自幼にする、また 「のう追加は、 <u>ユ・</u>	<del>こ情報を削除、修 ーザの追加(A)</del> で彳	正するときは、下のユ テってください。CSVフ	ーザー覧から該当す iァイルによるアップロ
<ul> <li>その他の設定と操作</li> <li>●設定状態のバックアップとリストア</li> <li>●ログの表示         <ul> <li>●「ullflex EG(こついて</li> <li>パージョン2.0からの移行</li> </ul> </li> </ul>	前のページ       泣のページ         ユーザ名	-ジ -ジ -ジ -ジ -ジ -ジ -ジ -ジ -ジ -ジ	第二次目前的目标。	有効期限	<b>証明書</b>	

# ②:ユーザの追加を選択し、下記画面へ。ユーザ名、パスワードを入力。

🎢 fullflex EG	
<ul> <li>         fullflex EG 上のレベルへ     </li> <li>         管理者用ページ ①</li></ul>	新しいユーザを追加します。「基本情報」の内容を記入し、必要に応じて他の箇所も記入を行い、保存ボタンをクリックしてください。         新しいユーザを追加します。「基本情報」の内容を記入し、必要に応じて他の箇所も記入を行い、保存ボタンをクリックしてください。         基本情報         ユーザ名       user03         1文字以上、256文字以下で、大文字小文字のアルファペットあよび数字、空白(1,1)・(7)ン(-)、アットマーウ(@)、ピリオ K(1,25ッシュングンプーラインンが利用でき はないたい、         パスワード       11方込んだ文字が不のまま示されるので注意してください。         イスワード       11方込んだ文字が不のまま示されるので注意してください。         マンドレ、センジマンダーラインンが利用できます。       2011年1月1日         認証方法       標準         回時接続セッション数       □         このユーザを無効にする。       有効期限

③:証明書の発行のため、「このユーザが使用するクライアント証明書を作成する」にチェックを入れ、 一般名等の設定を行う。

		[]		
<ul> <li>〒型者用ページ ①</li> <li>□ ユーザの設定</li> <li>□ ユーザの追加</li> <li>- ダウンロードとアップロード</li> <li>- ユーザの共通設定</li> <li>- ユーザ同期の設定</li> <li>ユーザ同期の実行</li> <li>● 基本設定</li> <li>● 802.1Xを使う</li> <li>● プロキシを行う</li> <li>● 他システムとの連携を行う</li> <li>● その他の設定と操作</li> <li>● 設定状態のパックアップとリストア</li> <li>● ログの表示</li> <li>- fullflex EG[2017</li> <li>- パージョン2.0からの移行</li> </ul>	<ul> <li>         正明書         <ul> <li></li></ul></li></ul>	使用するクライアント証明書を作成3 ライアント証明書を使用ない場合は、チェッ 出本語を除く文字のうち、アスタリスク(4)、ス ロックロン 回り書を作成する場合は必須です。1~ BMG alaxala kawasaki kanagawa JP 日本 間 975 日1~7306日 定する・必要がある場合は以下に指う べるときの・必要条件 定できます。 うときに、追加する属性	tる。 >を外してください。 ラッシュ(ノ、イコール(=)以外の文字が利用できます。 64文字 1 ~~64文字 1 ~~128文字 1 ~~128文字 至してください。	
<b>完</b> 了				

④:動的 VLAN の場合には、アクセス許可を行う時に追加する属性を入力。完了したら、保存ボタンを

# 二回押す。

上のレベルへ		証明書を作成する場合は必須です。1~64文字	
5理者用ページ @)	部署名	BMG	1~64文字
コーザの設定	組織名	alaxala	1~64文字
ー <u>ユーリの通加</u> -ダウンロードとアップロード	市町村名	kawasaki	1~128文字
-ユーザの共通 <mark>設定</mark>	都道府県名	kanagawa	1~128文字
ーユーザ同期の設定 コーザ同期の実行	国名	JP 日本	~
→基本設定 -802.1×を使う	証明書の有効期	間 976 日1~7306日	
ブロキシを行う (他システルとの)連携を行う	一属性を個別に設	定する必要がある場合は以下に指定してくださ	()。———
その他の設定と操作	アクセス要求を調	べるときの必要条件	
設定状態のバックアップとリストア			
ログの表示			
-fullflex EGについて			
-バージョン2.0からの移行			
	100項目(100行)まで語 アクセス 誕生可を行	設定できます。 こうときに 追加する 属性	
		= VIAN	
	renner ispe		
	Tunnel-Mediu	m-Type - IEEE-802	
	Tunnel-Mediu Tunnel-Priva	te-Group-ID = "VLAN0031"	
	Tunnel-Mediu Tunnel-Priva	m=Type - IEEE-802 te-Group-ID = "YLAN0081"	
	Tunne I-Mediu Tunne I-Priva 100项目(100行)法で言	m=Type - IEEE-002 te-Group-ID = "VLAN0031" 設定できます。	

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

※動的 VLAN の設定を行うため、「アクセス許可を行う時に追加する属性」に

Tunnel-Type = VLAN

Tunnel-Medium-Type = IEEE-802

Tunnel-Private-Group-ID = "認証後所属する VLANID"

を設定してください。

VLANID は、ダブルコーテーションで括ってください。

上記設定は、Web 認証、MAC 認証共に共通で、認証モードに差異はありません。

なお、全てのユーザが同じ設定の場合、ユーザの共通設定で設定が可能です。

# ⑤: 3.1.2の①の画面に戻り、設定したユーザが作成されていることを確認する。

<ul> <li>fullflex EG</li> <li>上レのレベルへ</li> <li>管理者用ページ (0)</li> <li>コーザの設定</li> <li>基本設定</li> <li>802.1Xを使う</li> <li>プロキシを行う</li> <li>他システムとの連携を行う</li> <li>その他の設定と操作</li> <li>設定状態のバックアップとリストア</li> <li>ログの表示</li> <li>-fullflex EG(こついて</li> </ul>	アクセスを許可するユーザを設定します。あるユーザを一時的に無効、有効にする、また情報を削除、修正するときは、下のユーザー覧から該当す 報を元にキーワード検索や表示ユーザの絞込みもできます。新規ユーザの追加は、 <u>ユーザの追加(A)</u> で行ってください。CSVファイルによるアップロ・ <u>ドレアップロード(C)</u> で行ってください。						
└バージョン2.0からの移行	最初のページ 前のページ 次 ユーザ名 user03	0ページ 最後のペー 記証方法 標準	-ジ <b>無効</b> 〇有効	有効期限	<b>証明書</b> O.あり		

#### 3.1.3. PEAP、TLSの設定

①:管理者用ページの「802.1Xを使う」,「認証手順の選択」を選択し、右側のメニューから、「受け付ける認証手順」を選択する。

②:下記画面にて、認証手順に使用する PEAP、TLS にチェックを入れる。

🍠 fullflex EG	
≜上のレベルへ	
管理者用ページ ①           ウユーザの設定           ユーザの追加           ダウンロードとアップロード           ユーザの規約定           ユーザ同期の設定           ユーザ同期の設定           ユーザ同期の設定           ユーザ同期の設定           ユーザ同期の設定           ユーザ同期の設定           クライアントの再認証           EAPプロトコルの動作の調整           EAP-TLSの動作の調整           ロクキシを行う           他の設定と棟作           設定状態のパックアップとリストア           ログの表示	
<ul> <li>その他の設定と操作</li> <li>設定状態のパックアップとリストア</li> <li>ログの表示         <ul> <li>fullflex EG(こついて</li> <li>パージョン2.0からの移行</li> </ul> </li> </ul>	【保存(S) 

メモ・・・「要求する認証手順」は、認証開始の順番を変更します。特に設定の必要はありません。

③:設定を保存し、完了する。

#### 3.1.4. IEEE802.1x 認証時の端末再認証設定に関して

AX6700S,AX6300S,AX3630S,AX2400Sの再認証時間は、RADIUS サーバの設定に従うため、RADIUS サーバ, AX のどちらで再認証時間を決定するか決めて、設定して下さい。

AX にて、設定する場合は下記画面、クライアントの再認証を〇〇秒ごとに要求するのチェックをはず して下さい。

AX1200Sは、上記設定にチェックがある場合でもAXのコンフィグレーション設定に従います。



Copyright @ 2001, 2002, 2003, 2004, 2005, 2006, 2007 by Accense Technology, Inc. All rights reserved.

RADIUS サーバ設定ガイド fullflexEG7 編(第2版)

#### 3.2. Windows XP / Vista の設定

#### 3.2.1. ユーザ証明書/ルート証明書の作成

※fullflexEG7 での CA 機能に関する注意点。

今回、簡易 CA 機能付きの fullflexEG7 を使用し、以下説明しておりますが fullflexEG7 は、原則として CA 機能(証明書発行機能)を付加されておりません。 IEEE802.1X による認証を行う場合には、認証機関(CA)から必要な証明書を別途入手してご使用して 頂くか、簡易 CA 機能の付加についてアクセンス・テクノロジー社へご相談してください。

①:サーバ(fullflexEG7)への通信が可能なポートに認証対象にしたい PC を接続。サーバの IP アドレスに、fullflexEG7 インストール時に設定した管理画面表示用の HTTPS(SSL)ポート番号(標準:892)を付け足してアクセス。

②:一般ユーザ用ページを選択。

❷ fullflex EG - fullflex EGトゥプメニュー - Mozilla Firefox
ファイル(E) 編集(E) 表示(V) 履歴(G) ブックマーク(B) ツール(T) ヘルプ(H)
🕒 Microsoft Office שאיש איש איש איש איש איש איש איש איש אי
🎢 fullflex EG
fullflex EGトップメニュー
<u> 一般ユーザ用ページ(U)</u>
一般ユーザ自身によるパスワードの変更および証明書のダウンロードを行うことができます。一般ユーザはこのページにだけアクセスができます。このページにアクセスするには、 パスワードが必要です。
▲ <u>管理者用ページ(A)</u>

fullflex EGの動作の設定と、利用者の管理を行うことができます。このページにアクセスするには、管理者のユーザ名とパスワードが必要です。

Copyright @ 2001, 2002, 2(

③:ユーザ名,パスワードの入力を促されるので、

3.1.2 で作成したユーザ情報を入力。

(例:ユーザ名:user03、パスワード:alaxala)

④:入力した情報に誤りがなければ、下記画面が表示。

🍠 fullf	lex EG	
د 🔏	ーザ情報	報の管理(user03)
パスワードの	変更	
現在のパスワ	- K	
新しいパスワー	-ド	た文字がそのまま表示されるので注意してください。
パスワー	ドを変更す	- ろ (X)
■ T 明まのガ	AND. R	
IEEE 802.1X() を要求されます <u>802.1Xの設定</u>	はる認証を す。このパスフ <u>「方法</u> を参考	利用する場合には、各利用者端末(パソコン)にクライアント証明書をインストールする必要があります。以下の証明書をダウン クレーズとしては、この画面を利用する際に入力したパスワードを入力してください。証明書のインストールの方法は端末のOSによ ftcしてください。
国名	JP	
都道府県名	kanagawa	
市町村名	kawasaki	
組織名	alaxala	
部署名	BMG	
一般名	user03	
有効期間	975日	
この証明 トップページに	書をダウン 戻る(B)	ロードする (W)

⑤:この証明書をダウンロードするを選択し、接続しているサプリカントに証明書をダウンロードする。

⑥:任意のディレクトリに保存した証明書をダブルクリックし、インストールの手順を開始。



⑦:次へ。

証明書のインボート ウィザード		×
	証明書のインボート ウィザートの開始	
	このウィザードでは、証明書、証明書信頼リスト、および証明書失効リ ストをディスクから証明書ストアにコピーします。	
	証明機関によって発行された証明書は、ユーザー ID を確認し、データ を保護したり、またはセキュリティで保護されたネットワーク接続を提供 するための情報を含んでいます。証明書ストアは、証明書が保管され るシステム上の領域です。	
	続行するには、[次へ] をクリックしてください。	
	< 戻る(B) 次へ(N)> キャンセル	

# ⑧:参照しているファイルが正しいことを確認。次へ。

	ポートするファイルを指定してください。
77	(ル名(E):
C:¥	Documents and Settings¥Administrator¥デスクトップ¥clcert.p12 参照(R)
注意	ま、次の形式を使うと1 つのファイルに複数の証明書を保管できます:
1	Personal Information Exchange- PKCS #12 (PFX,P12)
(	Cryptographic Message Syntax Standard- PKCS #7 証明書(P7B)
	Microsoft シリアル化された証明書ストア(SST)
	< 戻る(B) 次へ(N) > キャンセル

⑨:ユーザの作成手順で設定したパスワードを、秘密キーのパスワードへ入力。次へ。

証明書のインポート ウィザード	$\mathbf{X}$
<b>パスワード</b> セキュリティを維持するために、秘密キーはパスワードで保護されていました。	
秘密キーのパスワードを入力してください。	
******** *******	
□ 秘密キーの保護を強力にする(E) このオブションを有効にすると、秘密キーがアブリケーションで使われるたびに確認を求められます。	
<ul> <li>このキーをエクスポート可能にする(M)</li> <li>キーのバックアップやトランスポートを可能にします。</li> </ul>	
< 戻る(8) 次へ(10) > キャンセル	

#### 10:自動的に適切なストアに振り分けられる。次へ。

明書のインボート ウィザード	
証明書ストア 証明書ストアは、証明書が保管されるシス	₹テム上の領域です。
Windows (ご証明書ストアを自動的に選択	させるか、証明書の場所を指定することができます。
⊙証明書の種類に基づいて、自動的	っに証明書ストアを選択する(U)
○証明書をすべて次のストアに配置す	≠る( <u>P</u> )
証明書ストア	
	< 戻る(B) 次へ(N) > キャンセル

# ⑪:選択した内容を確認する。完了。

証明書のインボート ウィザード		×
	証明書のインポート ウィザードの完了	
	証明書のインボートウィザードが正常に完了しました。	
	)次の設定が指定されました:	
	選択された証明書ストア ウィザードで自動的に決定されます 内容 PFX ファイル名 C:¥Documents and Settings¥Administr	
	く戻る(B) 完了 キャンセル	

# 12:はいを選択する。

セキュリティ	/警告
•	発行者が次であると主張する証明機関(CA)から証明書をインストールしようとしています:
-	fullflex EG internal CA 20070802190213
	証明書が実際に "fullflex EG internal CA 20070802190213" からのものであるかどうかを検証できません。"fullflex EG internal CA 20070802190213" に連絡して発行者を確認する必要があります。次の番号はこの過程で役立ちます:
	損印 (sha1): E3F7E0BF 1373C12C 2D8993FF 965A4B95 C4E96DCA
	警告: このルート証明書をインストールすると、この CA によって発行された証明書は自動的に信頼されます。確認されていない拇印付きの証明書をインストールす ることは、セキュリティ上、危険です。[はい] をクリックすると、この危険を認識したことになります。
	この証明書をインストールしますか?
	はい公 (ごびびえ)(2001)

13:正しくインポートされました。



(1): ユーザ証明書のストアに正しくインポートされていること確認。

証明書				? 🛛
目的(N): 個人 ほかの人	ズすべて>     「     中間語     印根関     「     信頼     れた     ルート	<b>亚月機関 (言</b> 類	順された発行元	€頼されない発行元
発行先	発行者	有効期限	フレンドリ名	
user03	fullflex EG internal C	2010/05/	くなし>	
インボートΦ	[エクスポート(E)] [前除(B)			[詳細設定( <u>A</u> )
\				表示①
				閉じる(©)

15: ルート証明書のストアに正しくインポートされていること確認。

明書				?
的( <u>N</u> ):	すべて>			
個人 (ほかの人)中間証明	月機関 信頼されたルート語	山明鴉関(言語	順された発行元 信頼	されない発行元
発行先	発行者	有効期限	フレンドリ名	^
🔛 FESTE, Verified Ce	FESTE, Verified Certs	2020/01/	FESTE, Verified	
🔛 First Data Digital	First Data Digital Cer	2019/07/	First Data Digita	
FNMT Clase 2 CA	FNMT Clase 2 CA	2019/03/	Fabrica Nacional	
fullflex EG internal	fullflex EG internal C	2010/04/	くなし〉	
GlobalSign Root CA	GlobalSign Root CA	2014/01/	GlobalSign Root	
GTE Cyber Trust GL.	GTE Cyber Trust Glob	2018/08/	GTE Cyber Trust	
GTE CyberTrust R	GTE CyberTrust Root	2004/04/	GTE CyberTrust	
		2000/02/		~
インポートロ エクスポー	-ト( <u>E</u> ) 削除( <u>R</u> )	ר		詳細設定(A)
		-		
証明書の日町				
<বৃশ্7>				( まテ0.0
				\$0100
				開じる(C)

Copyright  $\ensuremath{\textcircled{O}}$  2007, 2008, ALAXALA Networks Corporation. All rights reserved.

●証明書の確認

<Windows XP の場合>

スタート→設定→コントロールパネル→インターネットオプション→インターネットのプロパティ コンテンツタブ→証明書→信頼された証明機関に fullflexEG7 のサーバ証明書がインストール されていることを確認する。

<Windows Vista の場合>

スタート→設定→コントロールパネル→インターネットオプション→インターネットのプロパティ コンテンツタブ→証明書→信頼された証明機関に fullflexEG7 のサーバ証明書がインストール されていることを確認する。

#### 3.2.2. PEAP 設定、認証の確認

①:サプリカントで使用する EAP の設定をする。

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

🔸 ローカル エリア接続のプロパティ 🛛 🕐 🔀
全般認証
認証されたネットワーク アクセスをイーサネットのネットワークで提供するには、この オプションを選んでください。 マニのネットワークで IEEE 802.1X 認証を有効にする(E)
EAP の種類(I): 保護された EAP (PEAP)
プロパティ(R)  コンピュータの情報が利用できるときは、コンピュータとして認証する(C)  ユーザーまたはコンピュータの情報が利用できないときは、ゲストとして 認証する(G)
OK キャンセル

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

保護された EAP のフロパティ ? 🔀
接続のための認証方法
▼サーバーの証明書の有効化(型)
□ 次のサーバーに接続する(Q):
信頼されたルート証明機関(R):
ABA.ECOM Root CA
🔲 Autoridad Certificadora de la Asociacion Nacional del Notariado Me
🔄 Autoridad Certificadora del Colegio Nacional de Correduria Publica
Baltimore EZ by DST
🔲 Belgacom E-Trust Primary CA
🔄 🖸 C&W HKT SecureNet CA Class A
■新しいサーバーまたは信頼された証明機関を承認するようユーザーに求めない(P)
認証方法を選択する(S):
セキュリティで保護されたパスワード (EAP-MSCHAP v2) 🛛 構成(C)
□ すばやい再接続を有効にする(E)
OK キャンセル

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

EAP MSCHAPv2 のプロパティ 🛛 🔀
接続のための認証方法:
ー Windows のログオン名とパスワード (およびドメインがある場)
UN 47701

RADIUS サーバ設定ガイド fullflexEG7 編(第2版)

④: PEAP 認証の確認

サプリカントをケーブルに接続すると、資格情報の入力画面が現れる。 正しいユーザ名とパスワードを入力。

資格情報の入力		
ユーザー名(山):	user03	
パスワード(P):	****	
ログオン ドメイン(止):		
	OK (*State)	
	UN +77/2/1	

⑤:認証に成功したことを、サーバーログで確認する。

管理者画面 → ログの表示 →認証ログの表示 を選択

認証ログの表示

ユーザ登録をしたユーザの認証処理が、期待した通りに実行されているかどうかを調べる場合は、検索キーワードにユーザ名を指定して調べます。また、認証かログの内容に含まれているAcceptedのキーワードを指定します。

付と時刻の範囲 20	070827	7183141. <b>"</b> M6200	70827	まで
※キーリート 表示				
20070827183141.3	728755	[eap-tls:1812]	user01:	unknown CA
20070827183241.3	713403	[eap-tls:1812]	user01:	unknown CA
20070827183701.	332547	[eap-tls:1812]	user05:	Accepted /C=JP/ST=kanagawa/L=kawasaki/O=alaxala/OU=BMG/CN=user05
20070827183948.0	603827	[eap-tls:1812]	user05:	Accepted /C=JP/ST=kanagawa/L=kawasaki/O=alaxala/OU=BMG/CN=user05
20070827184414.4	406583	[eap-tls:1812]	user06:	Accepted /C=JP/ST=kanagawa/L=kawasaki/O=alaxala/OU=BMG/CN=user06
20070827184418.	560983	[eap-tls:1812]	user05:	Accepted /C=JP/ST=kanagawa/L=kawasaki/O=alaxala/OU=BMG/CN=user05
20070827184436.	568146	[eap-tls:1812]	user06:	Accepted /C=JP/ST=kanagawa/L=kawasaki/O=alaxala/OU=BMG/CN=user06
20070827184506.4	486774	[eap-tls:1812]	user06:	Accepted /C=JP/ST=kanagawa/L=kawasaki/O=alaxala/OU=BMG/CN=user06
20070827184536.4	477534	[eap-tls:1812]	user06:	Accepted /C=JP/ST=kanagawa/L=kawasaki/O=alaxala/OU=BMG/CN=user06
20070027104000	470571	[con+10.1012]		Appended (CT IR/ST-kepseewe/L-keweekki/Ote Levele/OU-PNC/CN-uperOF

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

▶ 2-(2)(4)(5).txt - メモ帳		
ファイル(E) 編集(E) 書式(Q) 表示(V) ヘルプ(H)		
AX1230S# show dot1× vlan dynamic d	etail	
Date 2007/08/27 19:58:36 UTC		
VLAN(Dynamic) AccessControl : Multiple-Auth Status : Supplicants : 2 / 2 / 256 TxTimer : 30 ReAuthSuccess : 211 SuppDetection : Shortcut VLAN(s): 30-31	PortControl : Auto Last EAPOL : 0019.b970 ReAuthMode : Enable ReAuthTimer : 3600 ReAuthFail : 7	7d.46c7
Supplicants MAC Status SessionTime(s [VLAN 30] VLAN(Dynamic) 000a.e44d.5588 Authorized 493 [VLAN 31] VLAN(Dynamic) 0019.b97d.46c7 Authorized 104	AuthState BackEndState Re Date/Time Supplicants : 1 Authenticated Idle 1 2007/08/27 19:50:23 Supplicants : 1 Authenticated Idle 3 2007/08/27 19:56:52	ReAuthSuccess
AX1230S#		

# 3.2.3. TLS 設定、認証の確認

①:ユーザ証明書の確認

スタート→コントロールパネル→インターネットオプション→コンテンツタブ→

証明書→個人タブをクリック。発行者 fullflex EG internalCA(CA)発行先がユーザ ID の証明書を確認 する。

証明書					? 🛛
目的(N) 個人	ほかの人中間調	<すべて> 晒月機関   信頼されたルート語	四月機関 (言類	順された発行元	● 信頼されない発行元
発行	行先 user05	発行者 fullflex EG internal C	有効期限	フレンドリ名	
	<b>トロ</b> ) エクスオ	ペート(E)) [ 削除( <u>R</u> )			詳細設定(A)
証明書	の目的				
					表示──
					開じる(©)

②:サプリカントで使用する EAP の設定をする。

スタート→コントロールパネル→ネットワーク接続→該当のローカルエリア接続を

右クリックプロパティ→認証タブを開き、EAP の種類に"スマートカードまたはその他の証明書"を選 択、プロパティをクリックする。 ③:スマートカードまたはほかの証明書のプロパティにて、接続のための認証方法に

"このコンピュータの証明書を使う"を選択。サーバ証明書を有効化するにチェックし

信頼されたルート証明機関から fullflex EG internalCA をチェックする。OK を2回クリックし閉じる。

スマート カードまたはほかの証明書のブロパティ	? 🔀
接続のための認証方法: <ul> <li>自分のスマートカードを使う(S)</li> <li>このコンピュータの証明書を使う(C)</li> <li>単純な証明書の選択を使う(推奨)(M)</li> </ul>	
┌──サーバーの証明書を有効化する♡♡	
□次のサーバーに接続する(0):	
(言頼されたルート証明機関( <u>R</u> ):	
FNMT Clase 2 CA	~
💟 fullflex EG internal CA 20070802190213	
GlobalSign Root CA	
GTE CyberTrust Global Root	100
Hitachi Internal Class1 CA3	
<u>&lt;</u>	
証明書を表示する(	E)
<ul> <li>この接続で別のユーザー名を使う(D)</li> <li>OK</li> <li>キャン</li> </ul>	也儿

#### ④: TLS 認証の確認

サプリカントをケーブルに接続すると、認証します。

なお、証明書を持つユーザが複数いる場合は、下記に示す画面が出ます。 認証させたいユーザを選択し、OK をクリック。



⑤認証に成功したことを、サーバーログで確認する。

管理者画面 → ログの表示 →認証ログの表示 を選択。

蒙認証ログの表示	<del>.</del>		
ユーザ登録をしたユーザの認証処理	が、期待した通りにま	€行されている# まま	かどうかを調べる場合は、検索キーワードにユーザ名を指定して調べます。また、認証か
ロクの1415日まれにいるAccepted	ロのキーワートを指定し	Jæ 9 °	
日付と時刻の範囲 200708271	83141. <u></u> から20070	827	うま
検索キーワード			
表示			
20070827183141.728755 [e	eap-tls:1812] us	er01: unkn	own CA
20070827183241.713403 [e	eap-tls:1812] us	er01: unkn	own CA
20070827183701.932547 [e	eap-tls:1812] us	er05: Acce	oted /C=JP/ST=kanagawa/L=kawasaki/O=alaxala/OU=BMG/CN=user05
20070827183948.603827 [e	eap-tls:1812] us	er05: Acce	oted /C=JP/ST=kanagawa/L=kawasaki/O=alaxala/OU=BMG/CN=user05
20070827184414.406583 [e	eap-tls:1812] us	er06: Acce	oted /C=JP/ST=kanagawa/L=kawasaki/O=alaxala/OU=BMG/CN=user06
20070827184418.560983 [@	eap-tls:1812] us	er05: Acce	oted /C=JP/ST=kanagawa/L=kawasaki/O=alaxala/OU=BMG/CN=user05
20070827184436.568146 6	eap-tls:1812] us	er06: Acce	oted /C=JP/ST=kanagawa/L=kawasaki/O=alaxala/OU=BMG/CN=user06
20070827184506.486774 [6	eap-tls:18121 us	er06: Acce	oted /C=JP/ST=kanagawa/L=kawasaki/O=alaxala/OU=BMG/CN=user06
20070827184536.477534	ap-tls:1812] us	er06: Acce	oted /C=JP/ST=kanagawa/L=kawasaki/O=alaxala/OU=BMG/CN=user06
20070827184606.470571	eap-tls:1812] us	er06: Acce	oted /C=JP/ST=kanagawa/L=kawasaki/O=alaxala/OU=BMG/CN=user06

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

▶ 2-(2)(4)(5).txt - メモ帳	
ファイル(E) 編集(E) 書式(Q) 表示(V) ヘルプ(H)	
AX1230S# show dot1x vlan dynamic detail	^
Date 2007/08/27 20:38:43 UTC	
VLAN(Dynamic) AccessControl : Multiple-Auth PortControl : Auto Status : Last EAPOL : 0019.b97d.46c7 Supplicants : 2 / 2 / 256 ReAuthMode : Enable TxTimer : 30 ReAuthTimer : 3600 ReAuthSuccess : 231 ReAuthFail : 8 SuppDetection : Shortcut VLAN(s): 30-31	
Supplicants MAC     Status     AuthState     BackEndState     ReAuthSuccess       SessionTime(s)     Date/Time       [VLAN 30]     VLAN(Dynamic)     Supplicants : 1       000a     c44d 5588     Authorized     Juthorized	
OutrainedAuthon rizedAuthon rizedAuthon rizedAuthon rized7072007/08/2720:26:56[VLAN 31]VLAN(Dynamic)Supplicants: 10019.b97d.46c7Authon rizedAuthon ticated1962007/08/2720:35:28	
AX1230S#	<b>▼</b> .::

# 4. Web 認証の設定

#### 4.1. fullflexEG7の設定

fullflexEG7の設定は、「2 IEEE802.1X 認証の設定」を参照して下さい。 なお、Web 認証では、EAP の種類で、PAP を使用しますが fullflexEG7 ではデフォルトで 認証が許可されているため、別途設定の必要はありません。 802.1x を使うのメニューのところで、内部認証手順の選択の、EAP-TTLS の内部認証手順の 中に PAP の設定がありますが、変更しても Web 認証に問題はありません。

#### 4.1.1. ユーザの作成

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

#### 4.2. Windows XP / Vista の設定

#### 4.2.1. クライアントの設定

① : PC の設定は、スタート→コントロールパネル→ネットワーク接続→

該当のローカルエリア接続を右クリックプロパティ→認証タブを開くと、一番上にある、

このネットワークで IEEE 802.1X 認証を有効にするにチェックが入っている場合は、チェックを外す。

🕹 ローカル エリア接続のプロパティ	? 🛛
全般認証詳細設定	
認証されたネットワーク アクセスをイーサネットのネットワークで提供する オプションを選んでください。	には、この
□このネットワークで IEEE 802.1X 認証を有効にする(E)	
EAP の種類(T): スマートカードまたはその他の証明書	~
וסל	(ティ( <u>R</u> )
☑コンピュータの情報が利用できるときは、コンピュータとして認証する	0
<ul> <li>ユーザーまたはコンピュータの情報が利用できないときは、ゲストとし</li> <li>認証する(G)</li> </ul>	π
ОК	キャンセル

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

# 4.3. Web 認証の確認

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

🕘 – Microsoft Internet Explorer
ファイル(E) 編集(E) 表示(M) お気に入り(A) ツール(T) ヘルプ(H)
③ 戻る · ● · ▲ ② 《 → 検索 ☆ お気に入り ④ ② · → ◎ 図 · → 3
アドレス(1) (192.168.100.253/
LOGIN
Please enter your ID and password.
user ID user03
password
Login

②: "Login success"と認証成功画面が表示される。

🚰 http://192.168.100.253/auth_result/login.html - Microsoft Internet Explorer
ファイル(E) 編集(E) 表示(V) お気に入り(A) ツール(D) ヘルプ(H)
🕞 戻る 🔹 💿 - 💽 🛃 🏠 🔎 検索 👷 お気に入り 🚱 🚖 🥁 🔟 - 🔜 🍪
アドレス(1) 🗃 http://192.168.100.253/auth_result/login.html
Login success
Login Time 2007/08/28 18:19:52 UTC
close

③:認証に成功したことを、サーバーログで確認する。
 管理者画面 → ログの表示 →認証ログの表示 を選択。

<b>家</b> 証(	コグの表示
ユーザ登録をしたユー の内容に含まれてい	-ザの認証処理が、期待した通りに実行されているかどうかを調べる場合は、検索キーワードにユーザ名を指定し S Acceptedのキーワードを指定します。
日付と時刻の範囲 検索キーワード <del>表示</del>	20070828162147.から20070828 まで
2007082816214 2007082816214 2007082816282 2007082816282 2007082816282	7.511025 [auth:1812] user02: Unknown user 8.877468 [auth:1812] user01: Unknown user 9.364889 [auth:1812] user03: Accepted 9.728456 [auth:1812] user04: Accepted

# ④:認証時のユーザ登録状況

🥹 fullflex EG – Mozilla Firefox								
ファイル(E) 編集(E) 表示(V) 履歴(S)	ブックマーク(B) ツール① ヘルプ(H)							
🗣 • 💽 📀 🏠 🖻 h	ttps://192.168.10.2:892/admin/frame.php?close=.1	&go=radius_users_list.php				🙆 v 🕨	G- Google	<b>Q</b> )
🗋 Microsoft Office のアップ								
🍠 fullflex EG							Accense Te	chnology,Inc.
土上のレベルへ	-0-							~
<ul> <li>▲ 2→10%</li> <li>● 2→10%</li> <li>● 2→10%</li> <li>● 2→10%</li> <li>● 2→12%</li> <li>● 2→12%</li></ul>	アクセスを許可するユーザを設定します。 報を元にキーワード検索や表示ユーザの前 ドとアップロード心で行ってください。 ユーザー覧 全4件のうち、1件目から表示しています 検索文字列(S) [2]	あるユーザを一時的に無効。 双込みもできます。新規ユー 。 双込み (P) 次のページ 最後のペー	有効にする、ま ザの追加は、 <u>-</u>	た情報を削除、 <u>ーザの追加(A)</u> で	修正するときは、下の 「行ってください。 CSY	ユーザー 覧から該当す /ファイルによるアップロ・	るユーザ名をクリックしてください ド、またはOSVファイルのダウン	N。様々な登録情 /□ - ドは、 <u>ダウン□ -</u>
	ユーザ名	逻证方法	無効	有効期限	証明書			
	user03	標準	〇有効	無期限	×なし			
	user04	標準	〇有効	無期限	×なし			
	user05	標準	〇有効	無期限	○あり			
	user06	標準	〇有効	無期限	Oあり			
				-				
1. <u></u>				c	opyright © 2001, 2002,	2003, 2004, 2005, 2006	, 2007 by Accense Technology, I	nc. All rights reserved. 💌
元了								192.168.10.2:892 📓

⑤: AX (Authenticator) では show web-authentication login コマンドで、認証に成功していることを確認。

🖡 2-(2)(6).txt - 以モ帳						
ファイル(E) 編集(E) 書式(Q)	表示⊙	ヘルプ(円)				
						^
Date 2007/08/28 18:20	:22 UTC					
No MAC address	VLAN	Type Port	ChGrp	MCast		
1 000a.e44d.5588	30	Dynamic 0/1	<b>H</b>	<del></del>		
2 0012.e208.20c8	30	Dynamic 0/25	-	-		
3 0012.e208.20c8	31	Dynamic 0/25	2	2		
4 0019.b97d.46c7	31	Dynamic 0/1	55			
5 000a.e44d.5588	100	Dynamic 0/1	<del></del>	H		
6 0019.b97d.46c7	100	Dynamic 0/1	-	-		
7 0100.5e00.0001	100	Snoop -	2	1		
8 0012.e208.20c8	200	Dynamic 0/25	55	5		
9 0100.5e00.0001	200	Snoop -	<del></del>	0		
AX1230S#						
AX1230S# show web-aut	hent i ca	tion login				
Date 2007/08/28 18:20	1:26 UTC					
lotal login user cou	ints: 2					
No User Name	VLAN	MAC address	Login tim		Limit time	
1 user03	30	000a.e44d.5588	2007/08/2	8 18:19:52	3566	
2 user04	- 31	0019.b9/d.46c/	2007/08/2	8 18:19:52	3566	
W/100000						
AXT2305#						×
<u>×</u>	_					≥

# 5. MAC 認証の設定

#### 5.1. fullflexEG7 の設定

fullflexEG7の設定は、「2 IEEE802.1X 認証の設定」を参照して下さい。

#### 5.1.1. ユーザの作成

#### ①:管理者用ページのユーザ設定を選択し、下記画面を表示。

✓ fullflex EG 上のレベルへ 管理者用ページ @) □ ユーザの設定 □ ユーザの追加 -ダウンロードとアップロード - ユーザの共通設定 - ユーザ同期の設定 2 ーザ同期の設定 - ジロドレックロード - ジロキシを行う ● 201×26(た) ● ブロキシを行う ● 201×26(た) ● ブロキシを行う ● 201×26(た) ● 201×26(t) ● 201	アクセスを許可するユーザを設定します。あるユーザを一時的に無効、有効にする、また情報を削除、修正するときは、下のユーザー覧から該当する:     報を元にキーワード検索や表示ユーザの叙込みもできます。新規ユーザの追加(A)で行ってください。 CSVファイルによるアップロード <u>ドとアップロード(C)</u> で行ってください。     ユーザー覧     全0件のうち、1 件目から表示しています。     検索文字列(S)     「放込み (F)     最初のページ 前のページ 次のページ 最後のページ							
<ul> <li>● 設定状態のバックアップとリストア</li> <li>● ログの表示</li> <li>● fullflex EG(こついて</li> <li>● パージョン2.0からの移行</li> </ul>	ユーザ名 	認証方法	<b>無効</b>	有効期限	<b>証明書</b>			

②: MAC 認証端末をユーザ登録します。ユーザ名とパスワードの入力形式は③を参照下さい。 また動的 VLAN の場合は 3.1.2 の④に示すアクセス許可を行う時に追加する属性を入力して下さい。

380 TH 101 HIS	
フーザ名	001122334455
1.1.1.0	1文字以上、250文字以下で、大文字小文字のアルファベットおよび数字、空白( )、ハイフン(-)、アットマーク(0)、ビリオド、)、スラッシュ(パンアンダーライン人)が利用できます。 
120-12	001122334455
NX9-F	↑打ち込んだ文字がそのまま表示されるので注意してください。  4文字以上、240文字以下で、すべての印字可能文字(日本語を除く)が利用できます。
認証方法	標準 ✓
同時接続セッショ	ン教 空白にした場合は共通設定に送います。
同時接続セッショ □このユーザを約 有効期限	ン数 空白にした場合は共通設定に送います。 風効にする。
同時接続セッショ □このユーザを 有効期限 時間帯による認問	ン数 空白にした場合は共通設定に送います。 無効にする。
同時接続セッショ □このユーザを 有効期限 時間帯による認問 時間帯指定 →	>数 空白CLC場合は共通設定C送います。 風効にする。 E 1100 通設定に従う ▼
同時接続セッショ □このユーザを 有効期限 時間帯による認い 時間帯指定 具 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	ン数 空白CLを場合は共通設定に送います。 無効にする。 ENIR 通設定に従う マ

③:ユーザ名パスワード入力形式

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

AX2400S,AX3600S シリーズでは MAC アドレスは"-"や":"等の記号を含まない **001122334455** の 16 進数 12 桁(英字は小文字)の形式で登録してください。パスワードはコンフィグレーションコマンド

(mac-authentication password) で装置ごとに統一する事が可能です。AX1200S と AX2400S シリーズ 混在環境では AX1200S 側のコンフィグレーションで **001122334455** の 16 進 12 桁(英字は小文字)の 形式に統一してください。 ④:MAC 認証時のユーザの登録状況。

ーザの設定 アクセスを許可するユーザを設定します。あるユーザを一時的に無効、有効にする、また情報を削除、修正するときは、下のユ 報を元にキーワード検索や表示ユーザの絞込みもできます。新規ユーザの追加は、ユーザの追加(A)で行ってください。CSV: <u>ドとアップロード(C)</u>で行ってください。 ユーザ'001122334455'を保存しました。 -ユーザー覧-全2件のうち、1件目から表示しています。 紋込み(F) 検索文字列(S) 前のページ 最初のページ 次のページ 最後のページ ユーザ名 忍証方法 無効 有効期限 証明書 標準 Xtab 001122334455 〇有効 無期限 000102030405 標準 〇有効 ×なし 無期限

# 5.2. MAC 認証の確認

①:認証に成功したことを、サーバーログで確認する。

管理者画面 → ログの表示 →認証ログの表示 を選択。

<b>7</b> 2110	コグの表	示				
ユーザ登録をしたユー ログの内容に含まれる	-ザの認証処 ているAccep	L理が、期待したi tedのキーワードを	動に実行されている 計定します。	かどうかを調べる場合は	、検索キーワードにユーザ名を指定し	って調べます。ま
日付と時刻の 範囲 検索キーワード 表示	20070829	9141135.m62	20070829	<b>5</b> ≴		
2007082914113 2007082914150	35.536419 )1.145075	[auth:1812] [auth:1812]	001122334455 : 000102030405 :	Accepted Accepted		
		24 	n ang sa			

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

📑 2-(3)(5).txt - メモ帳		
ファイル(E) 編集(E) 書式(Q) 表示(V) ヘルプ(H)		
AX1230S# show mac-address-table		^
Date         2007/08/29         16:20:54         UTC           No         MAC         address         VLAN         Type         Port           1         000a.e44d.5588         30         Dynamic         0/1           2         0012.e208.20c8         30         Dynamic         0/25           3         0012.e208.20c8         31         Dynamic         0/25           4         0019.b97d.46c7         31         Dynamic         0/1           5         000a.e44d.5588         100         Dynamic         0/1           6         0019.b97d.46c7         100         Dynamic         0/1           6         0019.b97d.46c7         100         Dynamic         0/1           7         0012.e208.20c8         200         Dynamic         0/25           8         0100.5e00.0001         200         Dynamic         0/25	ChGrp MCast        - 1	
AX1230S# AX1230S# show mac-authentication auth-state Date 2007/08/29 16:20:59 UTC Total authentication counts: 2 No MAC address Authentication State 1 0019.b97d.46c7 Completed (31) 2 000a.e44d.5588 Completed (30)	Authentication time Limit time 2007/08/29 16:20:20 3561 2007/08/29 16:20:23 3564	
<u>&lt;</u>		≥ .d

# 6. ログイン認証

# 6.1. RADIUS サーバによる認証の設定

[設定のポイント]

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

[AXでの設定]

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

#### ②: (config)# radius-server host 192.168.10.2 key "alaxala"

RADIUS 認証に使用するサーバのIP アドレス(192.168.10.2)と共有鍵(alaxala)を設定します。

[fullflexEG7 での設定]

3.1.2の手順でログイン認証用のユーザ情報を fullflexEG7 に登録して下さい。

詳細は、

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

# 7. 認証ログの詳細な表示に関して

#### 7.1. fullflexEG7での認証ログの詳細表示

詳細を確認する画面と、設定を行う画面は別のため、以下に設定方法を記載します。

#### ①:管理者画面の基本設定のメニューからログの記録を選択



# ②:パケット詳細ログを記録するにチェックを入れ設定を保存する。



パケット詳細ログの記録の有無を指定します。チェックボックスがチェックされている場合、記録を行います。記録したログはパケット詳細ログの表示で見ることができます。

③:ログの表示メニューからパケット詳細ログの表示を選択。

🛜 パケッ	ト詳細ログの	表示	
認証プロトコルの詳約 するの設定を有効に	細な内容を調べること しなければなりません	ができるパケットの詳細なP 。なお、パケット詳細ログを	勺容の表示おこないます。この機能を利用するためには、基本設定の <u>□グの記録</u> の排 出力するとディスクの消費量が多くなるため、プロトコル分析が必要なときにのみ利用 
日付と時刻の範囲	20070921	mら20070921	
検索キーワード			
表示			
id(13) : User-Nam User-Pas NAS-IP-A Service- Calling- NAS-Iden NAS-Iden 200709212007/	len(92) : authe e = "user03" sword = <a4 0d="" o<br="">ddress = 192.168 Type = Framed Station-Id = "00 tifier = "AX1230 -Type = Virtual 04.281788 [1812]</a4>	enticator(53122f601a c4 f6 7d Y 1d 7f ^ E 3.100.253 )-0a-e4-4d-55-88″ )S″ 1 192.168.200.253:65	067418725e52731e3c4677) 18 8e c6 ¥ 2c 1f 9>
id(13) :	len(48) : authe	nticator(944381f84c	Jab5c37bb7d5924f85eaaf5)
Tunnel-T Tunnel-M Tunnel-P	ype = YLAN edium-Type = IEB rivate-Group-ID	EE-802 = <e2 80="" 9c="" a="" l="" m<="" th="" v=""><th>V 0 0 3 0 e2 80 9d&gt;</th></e2>	V 0 0 3 0 e2 80 9d>
200709212008	18.031451 [1812]	] 192.168.200.253:65	i534 >> Access-Request
id(14) :	len(95) : authe	enticator(37417c3d1a	(943f4b27cc01651f280372)
User-Nam	e = ″aaaaaaaaa″		
User-Pas:	sword = <5 04 9	05 7e k p 97 0e 12	c2 8e 1e 94 L 0>
NAS-IP-A	ddress = 192.168	3.100.253	

# 8. Windows Vista PEAP 設定の際の注意点

Windows Vista で PEAP 認証をご使用になる場合は、fullflexEG7 ver2.7.0 以降をお使いください。



2008年4月17日 第2版発行

アラクサラネットワークス株式会社 ネットワークテクニカルサポート

〒212-0058

川崎市幸区鹿島田 890 番地 新川崎三井ビル西棟