

The Guaranteed Network いちばん近くで、もっと先へ。

RADIUS サーバー設定ガイド NetAttest EPS 編



資料 No. NTS-07-R-042

アラクサラネットワークス株式会社

はじめに

RADIUSサーバー設定ガイドNetAttest EPS編は、アラクサラの認証スイッチでサポートしている認証 機能を用いたシステム構築において、RADIUSサーバーに株式会社ソリトンシステムズの NetAttest EPSを使用する場合の設定方法を示します。

関連資料

- ・AXシリーズ 認証ソリューションガイド
- ・AXシリーズ製品マニュアル(<u>http://www.alaxala.com/jp/techinfo/manual/index.html</u>)
- ・NetAttest EPS V4.8 管理者ガイド 第6版

本ガイド使用上の注意事項

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

本資料の内容は、改良のため予告なく変更する場合があります。

輸出時の注意

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

商標一覧

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

改訂履歴

版数	rev.	日付	変更内容	変更箇所
初版	—	2007.11.29	初版発行	—
第2版	—	2008.4.17	MAC 認証におけるユーザー名、パスワード設定	5.1.1
			について AX スイッチのバージョン UP に対応	
			しました。	
			AX1200S(1.3.B),	
			AX2400S(10.6.C),	
			AX3600S(10.6.C)	
第3版	—	2017.3.24	・NetAttest EPS の使用バージョンを Ver.4.8	全面改訂
			に更新しました。	
			・認証クライアント端末の OS、ブラウザを変	
			更しました。	
			・付録にマルチステップ認証とダイナミック	
			ACL/QoS の設定例を追加しました。	

目次

1.	概要	Ę	5
1	.1.	概要	5
1	.2.	設定例環境	6
	1.2.	1. 使用機器一覧とコンフィグレーション	6
	1.2.	2. 設定例のネットワーク構成図	7
2.	Net	Attest EPS の初期設定	8
2	2.1.	準備	8
2	2.2.	システム初期設定	8
2	2.3.	サービス初期設定1	1
2	2.4.	DHCP サーバーの設定1	5
3.	IEE	E 802.1X 認証1	6
3	5.1.	NetAttest EPS の設定1	6
	3.1.	1. ユーザー情報の登録1	6
	3.1.	2. ユーザー証明書の発行1	8
3	5.2.	認証クライアントの設定2	0
	3.2.	1. ユーザー証明書のインストール2	0
	3.2.	2. PEAP の設定と認証確認2	2
	3.2.	3. TLS の設定と認証確認2	4
4.	Wel	b 認証2	6
4	.1.	NetAttest EPS の設定	6
	4.1.	1. ユーザー情報の登録	6
4	.2.	認証クライアントの設定2	8
	4.2.	1. Web 認証の設定と認証確認2	8
5.	MA	C 認証3	0
5	5.1.	NetAttest EPS の設定	0
	5.1.	1. ユーザー情報の登録	0
5	.2.	MAC 認証の確認	2
付爹	录1.	マルチステップ認証3	3
付釒	录 2.	ダイナミック ACL/QoS	5

1. 概要

1.1. 概要

本資料では認証スイッチにアラクサラの AX シリーズ、クライアントコンピュータに Windows 8.1、 Windows 10、NetAttest EPS を RADIUS サーバー、ユーザーデータベースとして下記の認証方式を使用 したシステムを構築するための設定方法を記載しています。

認証方式

- ・IEEE802.1X 認証 (PEAP、TLS)
- ・Web 認証
- ・MAC 認証

使用方法

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

認証スイッチのコンフィグレーションに関して本資料では詳細な説明は記載していません。認証スイ ッチの設定は完了している事を前提にサーバー、クライアントの設定方法を記載しています。各認証方 式に関連するコンフィグレーションはアラクサラの「製品マニュアル」や「認証ソリューションガイド」 を参照してください。

1.2. 設定例環境

1.2.1. 使用機器一覧とコンフィグレーション

使用機器一覧

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

コンフィグレーション設定例

AX1240S のコンフィグレーション interface vlan 100 hostname "AX1240S" ip address 192.168.100.12 255.255.255.0 vlan 1 name "VLAN0001" interface vlan 200 ip address 192.168.200.12 255.255.255.0 vlan 30 interface vlan 1000 vlan 100 mac-based ip address 172.16.0.12 255.255.255.0 vlan 200 mac-based ip route 0.0.0.0 0.0.0.0 172.16.0.254 vlan 1000 ■ip access-list extended "auth" 10 permit udp any any eq bootps spanning-tree disable 20 permit udp any any eq bootpc spanning-tree mode pvst ■ 30 permit udp any host 192.168.1.2 eq domain interface fastethernet 0/1 • dot1x system-auth-control switchport mode mac-vlan switchport mac vlan 100,200 ▲mac-authentication system-auth-control switchport mac native vlan 30 ▲mac-authentication id-format 1 mac-authentication password "alaxala" Odt1x port-control auto • dot1x multiple-authentication • dot1x supplicant-detection auto web-authentication system-auth-control web-authentication port web-authentication ip address 1.1.1.1 ▲mac-authentication port authentication ip access-group "auth" service dhcp vlan 30 ■authentication arp-relay ■ip dhcp pool "V30" network 192.168.30.0/24 ~未使用インターフェイスは省略~ ■lease 0 0 0 10 default-router 192.168.30.254 interface gigabitethernet 0/25 ! ★radius-server host 192.168.1.2 key "alaxala" media-type auto switchport mode trunk ★radius-server dead-interval 0 switchport trunk allowed vlan 30,100,200,1000 I eaaa authentication dot1x default group radius interface vlan 1 ▲aaa authentication mac-authentication default group radius interface vlan 30 ip address 192.168.30.12 255.255.255.0 aaa authentication web-authentication default group radius ●IEEE802.1X 認証を行うためのコンフィグレーション Web 認証を行うためのコンフィグレーション

■ web 認証を行っためのコンフィクレーンヨン ▲MAC 認証を行うためのコンフィグレーション ★RADIUS サーバー関連のコンフィグレーション(各認証方式共通) ※上記コンフィグレーションは AX1240S の設定コンフィグです。同等の設定を AX2530S に定義す る場合は関連資料の「認証ソリューションガイド」を参照して下さい。

1.2.2. 設定例のネットワーク構成図



図 1.2-1 構成図

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

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

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

表 1.2-1 各認証方式のユーザー情報

2. NetAttest EPS の初期設定

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

2.1. 準備

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

2.2. システム初期設定

- ホスト名やネットワークの設定など、初回セットアップ時の必須項目の設定を行います。
 - 操作端末から Web ブラウザ(Internet Explorer)を起動し、NetAttest EPS の管理 IP アドレスに ポート番号を加えアクセス(http://192.168.2.1:2181/)し、「初期設定ウィザード」-「シ ステム初期設定」をクリックします。

★ ② ● Inter/1922.08.2.4.2181 月 - GX ● (2.5.7.4 日本 - dotte - h x) NetAttest EFG ★ 10588257 x 5 - F ● 2.5.7.6 1058252 ● 2.5.7.6 105825 ● 2.5.7.6 105825 ● 2.5.7.6 1058252 ● 2.5.7.6 1058252 ● 2.5.7.6 1058252 ● 2.5.7.6 1058252 ● 2.5.7.6 105825 ● 2.5.7.6 105825 ● 2.5.7.6 105825 ● 2.5.7.6 105825 ● 2.5.7.6 105825 ● 2.5.7.6 105825 ● 2.5.7.6 105825 ● 2.5.7.6 105825 ● 2.5.7.6 105825 ● 2.5.7.6 1058252 ● 2.5.7.6 105825		C 0 X
NetAttest EFS	G ● http://192.168.2.1:2181 P + C × G 「システム管理-alexala-N x	
MERARCEST CON → 22.5 ADMARE → 2.75 ADMARE → 2.75 ADMARE → 2.75 ADMARE ADMARC-2A	Alet Attest FTF	
● ● ● ● ● ● ● ● ● ● ● ● ● ●	NetArtest Ero	
 第第第第三クィゾード ● システム計算算定 ● システム管理ページへ ● CA管理ページへ 		
 ○○ 22五ム田周辺定 ○○ 22五ム田周辺定 ○○ 2二乙ス田周辺定 ○○ 2二乙ス田周辺定 ○○ 2二乙ス田周辺定 ○○ 2二乙田周辺定 ○○ 2二〇二 ○○ 2二〇二 ○○ 21〇二 		
CATHRAGE ZZ F A THRAGE → ZZ F A THRAGE → ZZ F A THRAGE CATHRAGE ZA CATHRAGE ZA	te annibito at -s	
© 227400000 227400000 2274000000 2274000000 2274000000 2274000000 2274000000 2274000000 2274000000 2274000000 22740000000 22740000000 22740000000 22740000000 22740000000 227400000000000000000000000000000000000		
©/ 2221198852 ↔ 2274897<20 State=-20	Or 237140mage	
	◎ ゲービス初期設定	
ea管理ページへ	▲■ システム管理ページへ	
	🥰 ca管理ページへ	
	31	
Copyright © 2004-2016, Soliton Systems K.K., All rights reserved	Copyright # 2004-2016, Soliton Systems K.K., All rights reserved.	

② ID、パスワードを入力して、ログオンします。

デフォルト設定 ア	カウント,パスワード : admin
システム管	き理ページログオン
管理者アカウ	リントの認証が必要です。
アカウント:	admin
パスワード:	•••••
	ログオン

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

初期設定ウィザー	F	
	システム初期設定を行うには、「次へ」をクリックして下さい。	
	*^	

<設定内容>

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

内容の詳細については、「NetAttest EPS V4.8 管理者ガイド」を参照ください。

本例では、「ホスト名の設定」と「インタフェース(LAN1)の設定」の設定を変更/追加しています。ここでは、その変更箇所のみ説明します。

● ホスト名(FQDN)の設定をします。

初期設定ウィザード - ホスト名の設定 新ttp://192.168.2.1:2181/sysadmin/	[システム管理-alaxala-NetAttest EPS] - Windows Internet Ex 📼 💷 🗙
🧱 初期設定ウィザード – ホン	スト名の設定
ホスト名(FQDN)	alaxala.local
	屋る 次へ

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

🍘 初期設定ウィザード - サービスインター	フェイスの設定 [システム管理-alaxala-NetAttest EPS] - Wind 💶 💷 🗮 🌉
Attp://192.168.2.1:2181/sysadmin/n	abase_initwizard.cgi?SystemWizFrameDiv
📕 初期設定ウィザード – サー	ビスインターフェイスの設定
編集対象: LAN1	
P設定 デバイス設定	a
🗾 この設定を有効にする	
IP7Fレス	192.168.1.2
サブネットマスク	255.255.265.0 (24)
デフォルトゲートウェイ	192.168.1.254
мти	1500

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

初期設定ウィザード - 設定項目の確認 [システム管理-alaxal	a-NetAttest EPS] - Windows Internet Exp	
http://192.168.2.1:2181/sysadmin/nabase_initwizard.c	gi?SystemWizFrameDiv	
ን ጋተማኮ ‹አጋ	233.233.233.0	*
デフォルトゲートウェイ		
	1500	
リンクスピード/デュプレックス	Auto	
ドメインネームサーバー1		
ドメインネームサーバー2		
CAライセンス		
証明書数上限	403	
パブリックCA	無効	
フルCA	無効	
IPSライセンス		
最大ユーザー数	200	
最大NAS/RADIUSクライアント数	500	
外部サーバー証明書	有効	
RADIUSプロキシ	有効	
Windowsドメイン認証連携	無効	
 グループ	無効	
MACアドレス認証		設正内谷を唯認後
	戻る 再起動	
pyright © 2004-2016, Soliton Systems K.K., All rights res	erved.	

2.3. サービス初期設定

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

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

(1) CA構築とサーバー証明書のセットアップ

 CA種別選択: <ルートCA>、CA秘密 鍵、およびCA情報を設定して、<次ヘ>ボ タンをクリックします。
 ※本資料の設定例は「ルートCA として構 築/サーバー証明書は自身のCA で発 行」のパターンの一例となります

初期設定ウィザード - CA構築		
CA種別選択		
CA種別選択	JU-FCA ▼	
CA秘密鍵		
◎ 内部で新しい鍵を生成す		
公開鍵方式	RSA -	
鍵長	2048 -	
◎ 外部HSMデバイスの鍵を	使用する	
要求の署名		
要求署名アルゴリズム	SHA256 -	
CA情報		
CA名(必須)	NTS	-
国名	日本	
都道府県名	Kanagawa-ken	
市区町村名	Kawasaki-shi, Saiwai-ku	
会社名(組織名)	ALAXALA Networks	
部署名		
E-mailアドレス		
CA署名設定		
署名アルゴリズム	SHA256 -	
有効日数	3650	

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

発行者	CN=NTS,O=ALAXALA Networks,L=Kawasaki-shi, Saiwa i-ku,ST=Kanagawa-ken,C=JP
所有者	CN=NTS,O=ALAXALA Networks,L=Kawasaki-shi, Saiwa i-ku,ST=Kanagawa-ken,C=JP
有効期間開始	
有効期間終了	
CA設定	
CRL更新間隔	
LDAPサーバー連携	
LDAPサーバー	localhost
連携	ユーザー証明書登録連携 CRL登録連携

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

の明色空白 オードーサーバー 祭司	1 de		
の別設定ワイケート・ケーハー証明	18		
サーバー証明書発行			
○ このCAでサーバー証明書を自動発行:	13	a second and a second	
著名アルコリスム		SHA256 -	
有効日数		730	
🔽 国名/繆道府県名/市日	(町村名/会社名(狙織名)	/認署名は CAと同じ値を使用する	
▶ サーバー証明書要求を発行する			
表求 パラメータ			
サーバー情報			
20		alaxala.local	
国名			
都道府県名		Kanagawa-ken	
市区町村名		Kawasaki-shi, Saiwai-ku	
会社名(組織名)		ALAXALA Networks	
部署名			
E-Mail			
別名	DNS名	🖾 白身のホスト名	
		□ 冗長構成時パートナーホスト名	
	197ドレス	LANI LAN2 LAN3 LAN4	
	1 M W III. 49 1	□ 九長福族時サービスIPアトレス	
	(日本設定)		
通ハウメータ の 市地 大部 しい物を生きする			
公開課方式			
鏡長		2048 -	
要求著名アルコリスム		SHA256 -	
		展る次へ	J

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

(2) LDAPデータベースを構築

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

編集対象: 新規						
名前*	LocalLdap01					
<u>武</u> 明	uc-iocal	* *				
■ 匿名ユーザーによる参	■ 匿名ユーザーによる参照を許可する ■ ユーザーの最終認証成功日時を記録する					
反3 次へ						

(3) RADIUSサーバーの基本設定

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



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

まま、<次へ>ボタンをクリックします。

9 初期設定ワイザート - RADIUSサーバーの基本	設定[システム言理-naeps-iverAttest EPS] - Windows C
http://192.168.2.1:2181/sysadmin/nabase	e_initwizard.cgi?ServiceWizFrameDiv
🍰 初期設定ウィザード – RADIUS*	サーバーの基本設定
EAP	
EAP認証タイプ 優先順位 認証タイプ 1 PEAP ・ 2 TLS ・ 3 なし ・ 4 なし ・ 5 なし ・	認証タイプ(優先順位) 1) PEAP 2) TLS
EAP-TLS/TTLS/PEAPオプション	
メッセージフラグメントサイズ	1024 * /지구ト
メッセージの長さ情報	フラグメントされた 最初のパケットにのみ含まれる 🔻 📃
EAP-TTLS/PEAPオプション	
🔤 GTC認証を有効にする	
TLSセッションキャッシュを有効に	
EAP-FASTオプション	•
	戻る次へ
Copyright © 2004-2016, Soliton Systems K.K.,	All rights reserved.

(4) RADIUSクライアントの設定

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

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

設定が完了したら<次へ>ボタン をクリックしてください NAS/RADIUS クライアントが登 録され、RADIUS サービスが開始 されます。

正常に終了すると次のページに 進みます。

NAS/RADIUSクライアント名・	AX1240S	
☑ このNAS/RADIUSクライアント?	を有効にする	
タイプ	⊙ NAS/RADIUSクライアント ⊙ NASのみ ⊙ RADIUSクライアントのみ	認証スイッチの IP アドレス (例) 1/2.16.0.12
説明		
IPアドレス*	172.16.0.12	
シークレット*		認証スイッチに設定した RADIUS
NAS識別値		(例) alaxala
	L	
		7 Ma
	, K	

(5) サービス初期設定の完了

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



2.4. DHCP サーバーの設定

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

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

NetAttest EPS		<u></u>	E
= alaxala.local	いけいでは、 しけいでは、 しけいでは、 したいで したいででいで したいででいで したいで、 したいででいで したいで したいでいで したいでいで したいでいで したいでいで	[サブネッ	ト](例) 192.168.100.0
 システム設定 システム管理 証明機関 	編集対象: 新規		ナブネットマスク] (例) 255.255.255.0 (24)
■ DHCPサーバー ■ 起動/停止 = PLNPH+ い、部中		初時書り当 C Welter 192.168.100.0	
■ DHCPサーハー設定 ■ DHCPスコーブ ■ DHCPリース情報	サブネットマスク 図 このスコープを有効にする	255.255.255.0 (24) 🔻	[テフォルトクートウエイ] (例) 192.168.100.254
■ LDAPサーバー ■ RADIUSサーバー ■ フーザー	デフォルトゲートウェイ	192.168.100.254	
	DNSサーバー1 DNSサーバー2		
	ドメイン名 デフォルトリース時間	43200 秒(60~86400秒)	
	最大リース時間	86400 秒(60~86400秒)	
		ок + +ури	· 通用

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



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



3. IEEE 802.1X 認証

3.1. NetAttest EPS の設定

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

3.1.1. ユーザー情報の登録

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

表 3.1-1 IEEE802.1)	、 認証で使用す	「るユーザー情報
--------------------	----------	----------

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

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

NetAttest EPS		BUITI	↑トッブページ) ロ 設定的	ログオン中:admir 森) 📵 ログオフ
 alaxala local システム設定 システム管理 証明機関 DH2Pサーバー 	<u>ユーザー一覧</u> ユーザー 0 一部 © 完全 エ <u>クスポート</u>	グループ 💌 📑	ローザーまで 検索	jê Ju
■ EDAP9ーバー ■ RADIUSサーバー ■ スーポー	名前	<u>ユーザーID</u>	<u>ユーザー削除時の</u> 計 証明書	19月書 天効オブション タスク
 ユージー・覧 エクスポート エクスポート ユンポート ユーザーパスワードボリシー 				

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

NetAttest EPS		((トップページ)
■ alaxala.local	🚨 ユーザー設定		
■ システム管理	編集対象: 新規		[旌] (例) user01
■ 証明機関 ■ DHCPサーバー	ユーザー情報 チェックアイテム リブライアイテム 012		
■ LDAPサーバー	基本情報		
■ RADIUSサーバー	姓*	user01	
■ ユーザー一覧			
■ エクスポート	E-Mail	[7-	-ザーID] (例) user()1
■ 1 ンホート ■ ユーザーパスワードポリシー	詳細情報		
■ デフォルトユーザーブロファイル	認証情報		
		user01	
	パスワード*		
	パスワード(確認)*		
	🔳 一時利用停止		
		OK +	マンセル 適用

NetAttest EPS			(●トッブページ)● 設定(
 alaxala local システム設定 システム管理 証明機関 DHOPサーバー LDAPサーバー 	ユーザー設定 編集対象:新規 ユーザー情報 チェックアイラ 標準のリプライアイテム	та ијјјита о тр	認証後に所属 [VLAN ID]	する VLAN (例) 100
 ■ RADUCS ワーハー = ユーザー = ユーザー 重 ムウスボート = ユーザーパスワードボリシー ■ デフォルトユーザープロファイ) 	SesionTimeout VLAN ID Filter ID 任意のリプライアイテム アトリビュート	1800 100 オペレーター 選択 = -	95 値	
		ОК	キャンセル 適用	

<session timeout に関する注意事項>

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

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

NetAttest EPS				(a	ログオンマ	Þ
 alaxala.local システム設定 システム管理 証明機関 DHCPサーバー LDAPサーバー 	- <u>-</u>	-ザ覧 ○ 一部 ● 完全	グループ 🔹 🗖 ユ	-ザーまで <u>検索</u> ユ <u>ーザ</u> -	 ● 該定体件 ● 該 ● is ● 該 ● is ● is	クロション
■ RADIUSサーハー ■ ユーザー		名前	<u>ユーザーID</u>	証明書	タスク	
■ ユーザー一覧			user01	発行	支更 削除	
■ エクスポート ■ インポート		user02	<u>user02</u>	発行	支更 削除	

3.1.2. ユーザー証明書の発行

認証クライアントにインストールするためのユーザー証明書を発行します。

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

NetAttest EPS				(Alustan 21)		ブオン中:admin
 alaxala.local システム設定 システム管理 証明機関 DHOPサーバー LDAPサーバー 	<u>ユ</u> ーザー ユーザー エクスポート	『覧 ○ 一部 ● 完全	<i>Ğ</i> ル−J ▼	ユーザーまで 検索 ユーザーまで 検索	1 設定は44	 ビロタイプ 送加 夫効オブション
■ RADIOS 9 - ハー = ユーザー		名前	<u>ユーザー</u> I	D at	明書 ら	スク
■ ユーザー一覧		user01	<u>user01</u>		発行 変更	削除
■ エクスポート ■ インポート ■ ユーザーパスワードポリシー ■ デフォルトユーザープロファイル	-	user02	<u>user02</u>	3	能行 変更	削除

② <発行>ボタンをクリックするとユーザー証明書を発行します。

NetAttest EPS		●トップページ ● 設定保存					
■ alaxala.local	🔔 ユーザー証明書発行						
■ システム管理	編集対象: user01	編集対象: user01					
■ 証明機関	基本情報	基本情報					
■ DHCPサーバー ■ LDAPサーバー	姓	user01					
■ RADIUSサーバー	名						
	E-Mail						
■ エーリー一員 ■ エクスポート							
■ インポート	詳細情報	A					
■ ユーザーバスワードボリシー ■ デフォルトユーザーブロファイル							
	認証情報						
	ユーサー田	user01 証明書のインポートをおこないたい場合は、					
	● 日数 <mark>365</mark> 日	ここにパスワードを入力します。					
	◎ 日付 2018 👻 年 2 👻 月						
	証明書ファイルオプション						
	パスワード						
	パスワード(確認)						
		ーのパスワードを使用します。					
	☑ PKCS#12ファイルに証明機関の証明	月書を含める					
	a in reasonance and a fabrication with constitution	発行 キャンセル					

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



ユーザー証明書ファイル : user01_02.p12

3.2. 認証クライアントの設定

3.2.1. ユーザー証明書のインストール

PC にユーザー証明書をインストールします。 ① <u>「3.1.2 ユーザー証明書の発行」</u>でダウ ンロードしておいたユーザー証明書 (uer01_05.p12)をダブルクリックすると、証 明書インポートウィザードが実行されます。



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

★ 愛 証明書のインポート ウイザード	★ 愛 証明者の1ンポートウイザード
証明書のインボート ウィザードの開始	インボートする証明者ファフル インボートする正明者ファフル インボートするファイルを指定してください。
このウイザードでは、証明會、証明會重額リスト、および証明會失効リストをデイスクから証明會ストアにコピー します。	77イル名(F): <u>CivUsersYntstPCesktopYnewtYuset01_65p12</u> 注意: 次の形式を使うと1つのファイルに複数の証明豊を保管できます: Personal Information Exchange- PKCS #12 (.PFX, P12) Cryptographic Message Syntax Standard - PKCS #7 証明豊 (.P78) Microsoft シリフル化された証明豊ストア (.SST)
次へ(N) キャンセル	次へ(N) キャンセル

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

★ 愛短明色の12ポートウイザード	★ 愛照●のインポート ウイザード
NET-06日 パスワード入力	^{転用書 ストッ} 「証明書の種類に基づいて、・・・」を選択
セキュリティを推持するために、秘密キーはパスワートで保護され 秘密キーのパスワードを入力してください。 パスワード(P): ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	証明会がよりは、証明会が保管されるシステム上の領域 Windows に証明会ストアを自動的に選択 証明会の場所を指定することができます。 ● 証明会の運転に基づいて、自動的に証明会ストアを選択する(U) ● 証明会の運転に基づいて、自動的に証明会ストアを選択する(U) ● 証明会をすべて次のストアに配置する(P) 証明台ストア: 参照(R)
インボートオプシン(0): 	70.00 247/01

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



3.2.2. PEAP の設定と認証確認

- ① サプリカントで使用するEAPの設定をおこないます。
- [イーサネットのプロパティ]の[認証]タブから以下設定をおこないます。

イーサネット 2のプロパティ	×	保護された EAP のプロパティ チェックを入れる ×
ネットワーク 認証 共有	有効にする	接続のための認証方法:
/		□ ご明書を検証してサーバーの ID を検証する(V)
このイーサネット アダプターに認証済みのネットワ は、このオプションを選択してください。	アクセスを提供するに	□ 次のサーバーに接続する (例: srv1、srv2、.*¥.srv3¥.com)(O):
✓ IEEE 802.1X 認証を有効にする(N)	「EAP(PEAP)」を選択	
ネットロークの認証大法の避担(小小)		信頼されたルート証明機関(R):
ネットワークの設証方法の選択(M): Microsoft 保護された FAD (DEAD)	→ 設定(5) ◆	□ Microsoft Root Authol □ Microsoft Root Certific □ Microsoft Root Certific □ L Microsoft Root Certific
MICIOSOIL (A DAT)	BXX2(0)	Microsoft Root Certific Microsoft Root Certific Microsoft Root Certific
□ ログオンするたびに、この接続用の資格情報を修	吏用する(R)	Starfield Services Root Certificate Authority
□ 承認されていたいえwトローク マクセフトコ+ール	パックオスに	Symantic: Enterprise Mobile Root for Microsoft TestCA
	(1)23.9(1)	接続前の通知(T):
追加の設定(D)		サーバー名またはルート証明書が指定されなかった場合にユーザーに通知します >
		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) V 構成(C)
		 ✓ 高速再接続を有効にする(F) □ サーバーに暗号化パインドの TLV がない場合は切断する(D)
		ID プライバシーを有効にする(!)
	ОК ++775h	
		OK キャンセル
		EAP MSCHAPV2 00 / 01/71
		接続のための認証方法:
	ナエックをはすす	
		□ 合はドメイン)を自動的に使う(A)
		OK キャンセル

_

② 認証を開始します。

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

Windows セキュリティ	× ユーザー名を入力 : (例) user01
user01	パスワードを入力
624.2:	OK キャンセル

- ③認証に成功したことを、以下の方法で確認します。
 - (1) NetAttest EPSの認証ログで確認
 NetAttest EPSでは、[RADIUSサーバー] [RADIUSサーバー管理] [認証ログ] [表示]で
 以下のようなログが表示されます。
 <RADIUS認証ログの表示>

🏴 RADIUS認	証ログの表示		
			更新
日時	種別	Priority	ተለንት
Feb 27 11:21:24	radiusd[8550]	notice	2017/02/27 11:21:24 Login OK: [user01] (from client AX1240S port 10 cli 00-01-8e-b7-88-11)
Feb 27 11:21:24	radiusd[8550]	notice	2017/02/27 11:21:24 Login OK: [user01] (from client AX1240S port 10 cli 00-01-8e-b7-88-11 via proxy to virtual server)

(2) 認証スイッチの運用コマンドで確認

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

AX1240S# show dot1x port 0/1 detail				
Date 2017/02/27 11:21	:32 JST			
Port 0/1 (Dynamic)				
AccessControl : Multi	ple-Auth	PortContr	ol : Auto	
Status :		Last EAP	OL : 0001.8e	b7.8811
Supplicants : 1 / 3	/ 64	ReAuthMod	de : Disable	
TxTimer : 30		ReAuth	Timer : 3600	
ReAuthSuccess : 8		ReAut	hFail : 6	
SuppDetection : Auto)			
VLAN(s): 30,100,200				
Supplicants MAC F	Status	AuthState	BackEndState	ReAuthSuccess
	SessionTime(s)	Date/Time		SubState
[VLAN 100]	[VLAN 100] Port(Dynamic) Supplicants : 1			
0001.8eb7.8811	Authorized	Authenticated	Idle	0
	8	2017/02/27 11:	21:24	Full

3.2.3. TLS の設定と認証確認

- ① サプリカントで使用するTLSの設定をおこないます。
- [イーサネットのプロパティ]の[認証]タブから以下設定をおこないます。

イーサネット 2のプロパティ	×	
ネットワーク 認証 共有 有 このイーサネット アダブターに認証済みのネットワーム、このオプションを選択してください。 ア レービービービービービービービービービービービービービービービービービービービ	i効にする ⁷ セスを提供するに 「スマートカードまたは その他の証明書」を選択 ✓ 設定(5) ◆	接続のための認証方法: ○ 自分のスマートカードを使う(S) ③ このコンピューターの証明書を使う(C) ☑ 単純な証明書の選択を使う (推奨)(M) ☑ 証明書を検証してサーバーの ID を検証する(V) □ 次のサーバーに接続する (例: srv1, srv2, :*4.srv34.com)(O): (次のサーバーに接続する (例: srv1, srv2, :*4.srv34.com)(O): (京のサーバーに接続する (の: srv1, srv2, :*4.srv34.com)(O): (京のサーバーに接続する (の: srv1, srv2, :*4.srv34.com)(O): (京のサーバーに接続する (の: srv1, srv2, :*4.srv34.com)(O): (京のサーバーに接続する (の: srv1, srv2, :*4.srv34.com)(O): (京のサーバーになり、 (家のサービー) (京のサービー)
	OK キャンセル	□この接続で別のユーザー名を使う(D) ○K キャンセル

② 認証を開始します。

認証クライアントにケーブルを接続すると、認証が開始されます。

③ 認証に成功したことを、以下の方法で確認します。

(1) NetAttest EPSの認証ログで確認

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

<RADIUS認証ログの表示>

	証ログの表示		
日時	種別	Priority	ተላንት
Feb 27 11:38:51	radiusd[8550]	notice	2017/02/27 11:38:51 Login OK: [user01] (from client AX1240S port 10 cli 00-01-8e-b7-88-11)

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

AX1240S# show dot1x port 0/1 detail				
Date 2017/02/27 11:41	:00 JST			
Port 0/1 (Dynamic)				
AccessControl : Multi	ple-Auth	PortContr	ol : Auto	
Status :		Last EAP	OL : 0001.8el	b7.8811
Supplicants : 1 / 1	/ 64	ReAuthMod	de : Disable	
TxTimer : 30		ReAuth	Timer : 3600	
ReAuthSuccess : 9		ReAuth	hFail : 7	
SuppDetection : Auto	1			
VLAN(s): 30,100,200				
Supplicants MAC F	Status	AuthState	BackEndState	ReAuthSuccess
	SessionTime(s)	Date/Time		SubState
[VLAN 100]	Port(Dynamic) Supplicants : 1			
0001.8eb7.8811	Authorized	Authenticated	ldle	1
	273	2017/02/27 11:	:36:28	Full

4. Web 認証

4.1. NetAttest EPS の設定

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

4.1.1. ユーザー情報の登録

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

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

表 4.1-1 Web 認証で使用するユーザー情報

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

Mad Address FING				ログオン中: admir
NetAttest EPS			(1トップページ) 回設	定保存 📵 ログオフ
■ alaxala.local ■ システム設定 ■ システム管理 ■ 2018/08/19	ユーザー→覧 ユーザー 0 ー部 ● 完全	グルーナ	ユーザーまで 検索	
■ DHCPサーバー ■ LDAPサーバー ■ RADILSサーバー			<u>ユーザー削除時</u>	<u>追加</u> の証明書矢効オブション
■ ユーザー ■ ユーザー ■ ユーザー覧 ■ エクフポート	名前	<u>ユーザーID</u>	証明書	タスク
 ■ インボート ■ ユーザーバスワードボリシー ■ デフォルトユーザーブロファイル 				

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

NetAttest EPS		(●トッブページ) ● 該近
■ alaxala.local	🔔 ユーザー設定	
 ■ システム設定 ■ システム管理 	編集対象: 新規	[旌] (例) user02
■ 証明機関	ユーザー情報 チェックアイティ	
■ DHCPサーハー ■ LDAPサーバー	基本情報	
■ RADIUSサーバー	姓*	user02
 ユーザー ユーザー 		
■ エクスポート	E-Mail	
■ インボート ■ ユーザーバスワードボリシー	詳細情報	[ユーザーID] (例) user02
■ デフォルトユーザープロファイル	認証情報	[パフワード] (例) alavala
	ユーザーD*	user02
	パスワード*	
	バスワード(確認)*	•••••
	🔲 一時利用停止	
		OK キャンセル 適用

Copyright © 2007,2017, ALAXALA Networks Corporation. All rights reserved

NetAttest EPS	●トップページ) ● 設定的
 ■ alaxala.local ● システム設定 ● システム管理 ■ 証明機関 ■ DHOPサーバー ■ LDAPサーバー ■ RADIUSサーバー ■ ユーザー ■ ユーザー ■ エクスポート ■ インボート ■ ユーザーパスワードボリシー ■ デフォルトユーザーブロファイJ 	● トゥオページ ● 歳年 ▲ 集対象: 新規 ユーザー協程 チェックアイテム リブライアイテム 標準のリブライアイテム VLAN ID (例) 200 SessionTimeout 1800 VLAN ID 200 Filter ID ff 窓のリブライアイテム アトリビュート オペレーター 値 一 厳訳 = ▼
	OK キャンセル 連用

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

NetAttest EPS				t)トップページ)	ログオン	ノ中 ログ
 alaxala local システム設定 システム管理 証明機関 DHOPサーバー LDAPサーバー 	- 	-ザー→覧 ○ -部 ● 完	全 <i>ヴルー</i> ブ ▼ ユーザー	まで <u>検索</u> ユ <u>ーザー</u>	削狩時の証明書失効才	<u>追</u> 1ブ2
■ RADIOS 7 - 7 - = 7 - ザー		名煎	<u>ユーザーID</u>	証明書	タスク	
■ ユーザー一覧			user01	発行	支更 削除	
■ エクスポート ■ インポート		user02	user02	発行	夹更 削除	

4.2. 認証クライアントの設定

4.2.1. Web 認証の設定と認証確認

① 認証の設定をおこないます。

[イーサネットのプロパティ]の[認証]タブから以下設定をおこないます。

イーサネット 2のプロパティ	×
キットワーク 認証 共有	
このイーサネット アダプターに認証済みのネットワーク アクセスを提供するに は、このオプションを選択してください。	チェックが入っている ⁵ チェックをはずす
□ IEEE 802.1X 認証を有効にする(N)	
ネットワークの認証方法の選択(M):	
Microsoft: スマートカードまたはその他の証明書 💛 設定(S)	
ログオンするたびに、この接続用の資格情報を使用する(R)	
□ 承認されていないネットワーク アクセスにフォールバックする(F)	
追加の設定(D)	
OK キャン1	2.11

② 認証を開始します。

ブラウザからWeb認証専用IPアドレス(1.1.1)にHTTPアクセスをして ログイン画面が表示されたら、 ユーザーIDおよび パスワードを入力します。

	🎯 ۲۰۹	- □ × × 命☆隠ಅ
		ユーザー名を入力 : (例) user02
	LOGIN	
user ID	Please enter your ID and pass	word. パスワードを入力
passwo		
	Login	ーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーー
	LOGOUT	
	Please push the following but	ton.

③ 認証が成功すると「Login success」画面が表示されます。



- ④ 認証に成功したことを、以下の方法で確認します。
 - (1) NetAttest EPSの認証ログで確認
 NetAttest EPSでは、[RADIUSサーバー] [RADIUSサーバー管理] [認証ログ] [表示]で
 以下のようなログが表示されます。
 <RADIUS認証ログの表示>

🏁 RADIUS認	証ログの表示		
日時	種別	Priority	イベント
Feb 27 15:25:47	radiusd[8550]	notice	2017/02/27 15:25:47 Login OK: [user02] (from client AX1240S port 10 cli 00-01-8e-b7-88-11)

(2) 認証スイッチの運用コマンドで確認

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

AX1240S# show web-authentication login		
Date 2017/02/27 15:27:01 JST		
Dynamic VLAN mode total login counts(Logi	n/Max): 1 / 256	
Authenticating client counts : 0		
Port roaming : Disable		
No F User name	Port VLAN Login time Lin	nit
1 user02	0/1 200 2017/02/27 15:25:47 00:5	58:45

5. MAC 認証

5.1. NetAttest EPS の設定

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

5.1.1. ユーザー情報の登録

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

表 5.1-1 MAC 認証で使用するユーザー情報

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

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

NetAttest EPS		NUET I	●トップページ ● 設定	ログオン中:admir 保存 📵 ログオフ
 alaxala.local システム設定 システム管理 証明機関 DHOPサーバー LDAPサーバー 	▲ ユーザー一覧 ユーザー 0 一部 ● 完全 エクスポート	グループ 🔹	ユーザーまで 検索 ユーザー削除時の)	<u>追加</u> 通用書矢307フション
 RADUSワーハー ユーザー ユーザー エクスポート インポート ユーザーパスワードボリシー デフォルトユーザープロファイル 	名前	<u>1-1-1-10</u>	証明書	タスク

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

ユーザー情報 チェックアイティ	A リプライアイテム OTP	
基本情報		
姓*	00018eb78811	
名		
E-Mail		
詳細情報	[ユーザーID] MAC フ	アドレス
認証情報		 (例) alaval
ユーザーD*	00018eb78811	
パスワード*		
パスワード(確認)*	•••••	
🔲 一時利用停止		

<注意事項>

ユーザーIDとパスワードの入力形式について

AX1200S, AX2200S, AX2500Sシリーズでは、デフォルトのMACアドレス設定形式が00-11-22-33-44-55 の形式となりますが、コンフィグレーションコマンド(mac-authentication id-format)で001122334455や 00:11:22:33:44:55などの形式及び英字の大文字小文字が変更可能となっています。またパスワードはコンフ ィグレーションコマンド(mac-authentication password)で装置ごとに統一する事が可能です。

NetAttest EPS	● トップページ ● 設定的
 ■ alaxala.local ■ システム設定 ■ システム管理 ■ 証明機関 ■ DHCPサーバー ■ LDAPサーバー ■ RADIUSサーバー 	 ユーザー設定 編集対象: 新規 ユーザー情報 チェックアイテム リプライアイテム 認証後に所属する VLAN [VLAN ID] (例) 200 Session Timeout
 □ ユーザー □ ユーザー-覧 □ エクスポート □ インボート □ ユーザーパスワードボリシー □ デフォルトユーザーブロファイノ 	VLAN ID 200 タグ Filter ID 任意のリブライアイテム アトリビュート オペレーター 値 選択 = ▼ ●

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

Not Attact EBC					ログオン	ノ中: admin
INCLALIEST EPS			(●トップページ ● 設定(保存 📵 🛙	ログオフ)
= naeps.local	🙎 ユーザ-					
■ システム設定						
 システム管理 新明機関 	ユーザー	◎ 一部 ◎ 完全 グループ	▼ ユーザーまで 検索			
■ DHCPサーバー	<u>12245</u> F					is to
■ LDAPサーバー				ユーザー削除時の	证明書失効才	サブション
■ RADIUSサーバー		名前	ユーザーID	証明書	タス	5
- ユーザー - コーザー一覧		user01	user01	訂明書	क म	育川 路余
 ■ エクスポート 						
			<u>user02</u>	証明書	发史	削除
■ ユーザーバスワードポリシー		00018eb78811	00018eb78811	発行	変更	削除
■ デフォルトユーザープロファイル						

5.2. MAC 認証の確認

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

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

<RADIUS認証ログの表示>

	証ログの表示		
日時	種別	Priority	ተላንት
Feb 27 17:25:50	radiusd[8550]	notice	2017/02/27 17:25:50 Login OK: [00018eb78811] (from client AX1240S port 10 cli 00-01-8e-b7-88-11)

(2) 認証スイッチの運用コマンドで確認

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

AX1240S# show mac-authentication auth-state						
Date 2017/02/27 17:26:13 JST						
Dynamic VLAN mode total client counts(Login/Max): 1 / 256						
Authenticating client counts : 0						
Hold down client counts : 0						
Port roaming : Disable						
No F MAC address Port VLAN Login time Limit Real	uth					
1 0001.8eb7.8811 0/1 200 2017/02/27 17:25:49 infinity 3575						

付録1. マルチステップ認証

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

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

(1) マルチステップ認証を設定

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

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

(config)# interface fastethernet 0/1 (config-if)# switchport mode mac-vlan (config-if)# switchport mac vlan 100,200 (config-if)# switchport mac native vlan 30 (config-if)# dot1x port-control auto (config-if)# dot1x multiple-authentication (config-if)# dot1x supplicant-detection auto (config-if)# dot1x supplicant-detection auto (config-if)# mac-authentication port (config-if)# mac-authentication port (config-if)# authentication ip access-group "a (config-if)# authentication arp-relay	auth"	
(config if) # durichlication alphenergy		
	マルチステップ認証の設定	

(2) RADIUS サーバーの設定

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

Not Attest EDG					ログオン	/中:admin
NetAttestEPS			((●トップページ) 🕒 設定	保存) 📵 🕻	ログオフ)
■ naeps.local = システム設定 = システム管理 = 証明観関	ב - ש ב-ש- <u>ב-ש-</u>	ザー→覧 ○ →部 ● 完全 グルーナ	▼ ユーザーまで 検索			
 ■ DHCPサーバー ■ LDAPサーバー ■ RADIUSサーバー ■ ユーザー ■ ユーザー 		名前	7-#-m	<u>ユーザー削除時の</u> 証明書	証明書失効オ シス	追加 Iブション ク
		user01	user01	証明書	変更	削除
■ エクスポート ■ インポート		user02	<u>user02</u>	証明書	変更	削除
■ ユーザーバスワードポリシー ■ デフォルトユーザーブロファイル	-	00018eb78811	<u>00018eb78811</u>	発行	· 変更	削除
		MAC 認証用のユー	ザーID <変更	>ボタンをクリック		

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

標準のリプライアイテム	1000		
Session I imeout	1800		
VLAN ID	200	タグ	0
Filter ID			
任意のリプライアイテム			
アトリビュート	オペレーター	値	
Filter-la	= • @@vveb-+	Auth@@	• e
「Filter-Id」を選択		[@@Web-Auth@@	』」と入力」
「Filter-Id」を選択		「@@Web-Auth@@	』」と入け

(3) マルチステップ認証の確認

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

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

AX1240S# show authentication multi-step					
Date 2017/03/02 15:56:20 JST					
Port 0/1 : multi-step					
< Supplicant information > <authentic method=""></authentic>					
No MAC address State VLAN F Type Last (first step)					
1 0001.8eb7.8811 pass 200 multi web (mac)					

付録 2. ダイナミック ACL/QoS

アラクサラの認証スイッチ AX2500S シリーズでは、ダイナミック ACL/QoS 機能を実装してい ます。ダイナミック ACL/QoS 機能は、認証時に RADIUS サーバーによるクラス情報配布と 付与 されたクラス情報を使用して、アクセス制御を ACL(フィルタ)/QoS 機能で実現します。 ここでは一例として、ダイナミック ACL の設定、および手順について紹介します。

(1) ACL の作成

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

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

表 付録 2-1 ダイナミック ACL で制御するネットワーク

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

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

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

(2) RADIUS サーバーの設定

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

NetAttest EPS				()トップページ	ログオン中
 alaxala.local システム設定 システム管理 証明機関 DHOPサーバー LDAPサーバー 	ב <u>\$</u> ב- יי - בסגא-ד	ザ覧 ○ -部 ● 完全	<i>グループ</i> ▼ 2 コ <変更>ボタンをクリック	ーザーまで 検索	je je
■ RADIUSサーバー ■ ユーザー		名前	<u>ユーザーID</u>	い明書	92.0
■ ユーザー一覧 ■ エクスポート ■ インボート		user01 user02	user01 user02	発行 発行	支更 削除 支更 削除

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

設定例:「user01」:	Class 1,「user02」: Cla	ass 2 を指定
● 「user01」		
🤔 ユーザー設定		
編集対象: user01		
ユーザー情報 チェックアイテ	ム リプライアイテム OTP	
標準のリプライアイテム		
SessionTimeout	1800	
VLAN ID	100	タグ 0
Filter ID		
任意のリプライアイテム		
アトリビュート	オペレーター 選択 = VClass=1	值
T III.el-Iu		
	「Filter-Id」を選択	「/Class=1」と入力」
● 「user02」		
👆 ユーザー設定		
編集対象: user02		
ユーザー情報 チェックアイティ	ム リプライアイテム OTP	
標準のリプライアイテム		
SessionTimeout	1800	
VLAN ID	200	タグ <mark>0</mark>
Filter ID		
任意のリプライアイテム		1.00
アトリビュート Filter-Id	オペレーター 選択 = ▼ /Class=2	
L F		「/Class=2」と入力」

(3) ダイナミック ACL の確認

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

AX2530S# show access-filter	
Date 2017/03/06 16:40:12 JST Using Interface:vlan 100 in VLAN100 : fuser01」 Extended IP access-list:DynamicACL 10 permit ip any 192.168.5.0 0.0.0.255 class 1 Matched packets : 4 20 deny ip any 192.168.5.0 0.0.0.255 Matched packets : 0 30 permit ip any 192.168.6.0 0.0.0.255 class 2 Matched packets : 0 40 deny ip any 192.168.6.0 0.0.0.255 Matched packets : 4 50 permit ip any any Matched packets : 153 Implicitly denied packets : 0	
Using Interface:vlan 200 in VLAN 200 : Fuser0 2 J Extended IP access-list:DynamicACL 10 permit ip any 192.168.5.0 0.0.0.255 class 1 Matched packets : 0 20 deny ip any 192.168.5.0 0.0.0.255 Matched packets : 4 30 permit ip any 192.168.6.0 0.0.0.255 class 2 Matched packets : 4 40 deny ip any 192.168.6.0 0.0.0.255 Matched packets : 4 40 deny ip any 192.168.6.0 0.0.0.255 Matched packets : 0 50 permit ip any any Matched packets : 120 Implicitly denied packets : 0	



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

アラクサラネットワークス株式会社 ネットワークテクニカルサポート

〒212-0058

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