NetAttest EPS 設定例

連携機器:

ACERA800ST

Case: TLS 方式での認証

Version 1.0

株式会社ソリトンシステムズ



NetAttest®は、株式会社ソリトンシステムズの登録商標です。

その他、本書に掲載されている会社名、製品名は、それぞれ各社の商標または登録商標です。 本文中に ™、®、©は明記していません。

Copyright © 2012, Soliton Systems K.K. , All rights reserved.



はじめに

本書について

本書は CA 内蔵 RADIUS サーバープライアンス NetAttest EPS と FURUNOS YSTEMS 社製 無線アクセスポイント ACERA800ST の 802.1X 環境での接続 について、設定例を示したものです。

各機器の管理 IP アドレス設定など、基本設定は既に完了しているものとします。 設定例は管理者アカウントでログインし、設定可能な状態になっていることを 前提として記述します。

表記方法

表記方法	説明
ABCDabcd1234	コマンド名、ファイル名、ディレクトリ名、画面上のコンピュータ出力、
(normal)	コード例を示します。
ABCDabcd1234	ユーザーが入力する文字を、画面上のコンピュータ出力と区別して示しま
(bold)	す。
ABCDabcd1234	亦物をテレキオ、実際に使用する特定の名前キたけ値で署き換うキオ
(italic)	支奴で小しより。天际に使用りる村庄の石削よには他し自己換えより。

表記方法			
ſ J	参照するドキュメントを示します。		
٢J	参照する章、節、ボタンやメニュー名、強調する単語を示します。		
[‡-]	キーボード上のキーを表します。		
[‡-1]+[‡-	「七」11を押したがら「七」21を押すことを手します		
2]			

表記方法(コマンドライン)

表記方法	説明
%, \$, >	一般ユーザーのプロンプトを表します。
#	特権ユーザーのプロンプトを表します。
[filename]	[] は省略可能な項目を示します。この例では、filename は省略してもよ
[menane]	いことを示しています。

アイコンについて

アイコン	説明
٤	利用の参考となる補足的な情報をまとめています。
<u>.</u>	注意事項を説明しています。場合によっては、データの消失、機器の破損 の可能性があります。

画面表示例について

このマニュアルで使用している画面(画面キャプチャ)やコマンド実行結 果は、実機での表示と若干の違いがある場合があります。

ご注意

本書は、当社での検証に基づき、NetAttest EPS 及び ACERA800ST の 操作方法を記載したものです。すべての環境での動作を保証するもので はありません。



目次

1	構成.		. 6
	1-1	構成図	. 6
	1-2	環境	. 7
2	NetA	ttest EPS	. 8
	2-1	NetAttest EPS 設定の流れ	. 8
	2-2	システム初期設定ウィザードの実行	. 9
	2-3	サービス初期設定ウィザードの実行	10
	2-4	Authenticator(RADIUS Client)の登録	11
	2-5	RADIUS サーバー基本設定	12
	2-6	ユーザーの登録	13
	2-7	ユーザー証明書の発行	13
3	ACE	RA800ST	15
	3-1	ACERA800ST 設定の流れ	15
	3-2	ACERA800STのESSIDの設定	16
	3-3	ACERA800ST の再起動	18
4	クラ・	イアント PC の設定	19
	4-1	クライアント PC 設定の流れ	19
	4-2	ワイヤレスネットワーク接続先の登録	20
	4-3	ユーザー証明書のインポート	22
	4-4	インポートされたユーザー証明書の確認	25



1構成

1-1 構成図

- ・有線 LAN と無線 LAN は同一セグメント
- ・無線 LAN で接続するクライアント PC の IP アドレスは、
 NetAttest EPS-ST04 の DHCP サーバーから配付
- ・RADIUS の通信は、ACERA800ST と EPS 間で行われる





1-2 環境

1-2-1 機器

役割 メーカー		製品名	SW バージョン
Authentication Server (認証サーバー)	Soliton Systems	NetAttest EPS ST-04	Ver. 4.4.1
無線 Access Point	泉 Access Point FURUNOSYSTEMS		07.04
Client PC / Supplicant (802.1x クライアント)	HP Microsoft	ProBook 5220m	Windows 7 SP1 Windows 標準サプリカント

1-2-2 認証方式

IEEE 802.1x TLS

1-2-3 ネットワーク設定

	EPS-ST04	ACERA800ST	Client PC
IP アドレス	192.168.1.2/24	192.168.1.103/24	192.168.1.110 (DHCP)
RADIUS port (Authentication)	UDP 1812		
RADIUS port (Accounting)	UDP 1813		
RADIUS Secret (Key)	soliton		



2 NetAttest EPS

2-1 NetAttest EPS 設定の流れ

設定の流れ

- 1. システム初期設定ウィザードの実行
- 2. サービス初期設定ウィザードの実行
- 3. RADIUS クライアントの登録
- 4. 認証ユーザーの追加登録
- 5. 証明書の発行



2-2 システム初期設定ウィザードの実行

システム初期設定ウィザードを使用し、以下の項目を設定します。

- ◆ タイムゾーンと日付・時刻の設定
- ◆ ホスト名の設定
- ◆ サービスインターフェイスの設定
- ◆ 管理インターフェイスの設定
- ◆ ドメインネームサーバーの設定

	▼ 🗟 49 ×	
🖕 お気に入り 🏾 🏉 システム管理-Net'Attest EPS 🛛 👘 🔹 🗔 🔹	□ 鳥・ページ(P)・セーフティ(S)・ ツール(O)・ @・	
Net Attest EPS		
でた。 知識設定ウレザード		
	設定	
 サービス初期 	設定	
▲ システム管理ページ		
	初期設定ウィザードー設定項目の確認	2
<u>V3.x 設定/テータ</u>	ホスト名	naeps.na-labo.soliton.jp
Copyright © 2004-2010, Soliton Systems K.K., All rights reserved.	サービスインターフェイス	
	IPアドレス	192.168.1.2
	サブネットマスク	255.255.255.0
	デフォルトゲートウェイ	
	管理インターフェイス	
	IPアドレス	192.168.2.1
	サブネットマスク	255.255.255.0
	デフォルトゲートウェイ	
	ドメインネームサーバー1	192.168.1.100
	ドメインネームサーバー2	
	設定内容を確認して下さい。 この設定を保存・反映するには「再起	動」ボタンをクリックして下さい。
		反る 再起動
	Copyright © 2004-2010, Soliton Systems K	.K., All rights reserved.



2-3 サービス初期設定ウィザードの実行

サービス初期設定ウィザードを実行します。

本書では、下記項目を図のように設定しました。

- ◆ CA 構築
- ◆ LDAP データベースの設定
- ◆ RADIUS サーバーの基本設定(全般)

初期設定ウィザード - CA構築				
CA種別選択				
CA種別選択	ルートCA 💌			
CA秘密鍵生成				
公開鍵方式	RSA			
鍵長	2048 💌			
CA情報				
CA名(必須)	na-labo CAD1			
国名	日本			
都道府県名	Tokyo			
市区町村名	Shinjuku			
会社名(組織名)	Soliton Systems K.K.			
部署名	Mktg			
E-mailアドレス	na-admin@na-labo.soliton			
CA署名設定				
ダイジェストアルゴリズム	SHA1 🔽			
有効日数	3650			
		初期設定ウィザード - LDA	APデータペースの設定	
	戻る	編集対象: 新規		
Copyright © 2004-2010, Soliton System	s K.K., All rights reserved.	名前*	LocalLdap01	
		サフィックス*	dc=na-labo,dc=solitor	n,dc=jp
初期設定ウィザード - RADIUSサー	バーの基本設定	説明		
全般				戻る次へ
認証ボート*	1812			
アカウンティングポート*	1813			
□ ログにバスワードを表示する(PA	P認証のみ)			
□ セッション管理を使用する				
■ 冗長構成時、アカウンティングル	「ケットをパートナーに転送する 			



2-4 Authenticator(RADIUS Client)の登録

WebGUI より、RADIUS Client の登録を行います。

「RADIUS サーバー設定」→「NAS/RADIUS クライアント追加」から、RAD IUS Client の追加を行います。

Net Attest EPS			存)
 naeps 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 足動/停止 RADIUSサーバー設定 	NAS/RADIUSクライアント一覧 S/RADIUSクライアント名 IPアドレス		F
 RADIUSサーバー管理 ライセンス NAS/PADIUSクライアンホー覧 NAS/RADIUSクライアンホー覧 	NAS/RADIUSクライアント設定 編集対象: ACERA800ST		
■ インボート ■ ユーザー	NAS/RADIUSクライアント名*	ACERA800ST	
	☑ このNAS/RADIUSクライアントマ	を有効にする	
	説明	スタンドアローン	
	IP7Fレス*	192.168.1.103	
	シークレット*	•••••	
	所属するNASグループ	•	
S/RADIUS クライアントタ1			
アドレス(Authenticator)】			
92.168.1.103			
- ク レット]			
oliton			

2-5 RADIUS サーバー基本設定

WebGUI より、RADIUS サーバーの基本設定を行います。

「RADIUS サーバー」→「RADIUS サーバー設定」→「基本設定」→「EAP」から設定を行います。







2-6 ユーザーの登録

WebGUI より、ユーザー登録を行います。

「ユーザー」→「ユーザー一覧」から、『追加』ボタンでユーザー登録を始め ます。



ユーザー証明書の発行

WebGUI より、ユーザー証明書の発行を行います。

「ユーザー」→「ユーザー一覧」から、該当するユーザーの「証明書」の欄の 『発行』ボタンでユーザー証明書の発行を始めます。

Net Attest EPS				①トップページ 〇 読定保存 〇 ログオフ
≡ naeps na−labo soliton jp	💄 ユーザー一覧			
■システム設定 ■システム管理	ユーザー 👥 🔹 一部 💿 完全	グループ • 1000 ユー*	ザーまで 被索	
■証明機関 ■ DHCP# ーパー	名前		<u>ユーザーID</u> 17881	道加 ▶ タスク
■ LDAPサーバー			soliton_user Rfi	
■ RADIUSサーハー				
 ユーザー一覧 エクラポート 				
 インボート 		基本情報		
■ ユーザーハスワートホリシー ■ デフォルトユーザープロファイル		姓	シリトン	
		名	一郎	
		E-Mail		
		詳細情報		*
【 訨 明 書 有 幼 期 限 】		刻証権も		
· 365			soliton usor	
		▲ 5 D 有効期限*	soliton_user	
【証明書ノアイルオノショ	ヨンハスリート」	◎ 日数 365	8	
• password		● 日付 201 で	1 ▼ 年 10 ▼ 月 22 ▼ 日 23 ▼	時 <mark>59 ▼</mark> 分 <mark>59 ▼</mark> 秒ま
		証明書ファイルオフ	プション	
	証明機関の・・・】	パスワード	•••••	
・チェッ ク 有		パスワード(確認)	••••••	
		※バスワードが空傷		を使用します。
		▼ PKCS#12ファイ	/ ルに証明機関の証明書を含める	5
				発行 キャンセル
				3613 1 7 2 70
Net Attest EPS				
■ naeps.na−labo.soliton.jp	ユーザー証明書の)ダウンロード		
●システム設定				
 システム管理 	ユーザー証明書ダウ	ワンロードの準備ができま	ました。対象をファイルに保存して下す	い。 ダウンロード
* 証明機図 ■ DHCPサーバー				
■ LDAPサーバー				
■ RADIUSサーバー				
 ユーサー フーザー→ 				
■ エクスポート				
■ インポート				
■ ユーザーパスワードポリシー ■ デフォルトフ ーザープロファイル				
■ デフォルトエーリーフロファイル				



3 ACERA800ST

3-1 ACERA800ST 設定の流れ

設定の流れ

- 1. ACERA800STのESSIDの設定
- 2. ACERA800STの再起動

3-2 ACERA800STのESSIDの設定

ACERA800ST に ESSID を設定します。

ACERA800ST では複数 ESSID を設定できますが、ESSID 毎にセキュリティを 変更できますので、RADIUS サーバーを登録する場合も ESSID 毎に登録しま す。ここでは以下のパラメータを設定しています。

- ◆ESSIDの有効/無効 ◆ESSID
- ◆ステルスモードの有効/無効 ◆暗号方式
- ◆WPA 固有設定
- ◆WPA、802.1x 共通設定 (RADIUS サーバーの登録)

保存 変更を適用して再起動				
無線LAN1 セキュリテ	ィ設定 ESSID 1			
設定のコピー	ESSID 1 🗸 へ下記設定内容を	<u>ב הקר (</u>		
2 <u></u>				
設定	◎有效 ○無效	0		
ESSID	TLS	0		
VLAN ID		0		
DTIMインターバル	1 💌	0		
ステルスモード	○有効 🗿 無効	e		
any拒否	●有効 ●無効	0		
無線セパレータ	◯ 有效 ⊙ 無效	0		
無線セバレータポリシー	④ 通過 〇 進町	0		
無線セバレータ例外アドレン	z	0		
MACアドレスフィルタリング	◯有效 ⑧無效			
対象MACアドレス		Ø		
暗号化設定				
暗号方式	WPA2-Enterprise 🗸		0	
WEP語定			_	
BAR	モード:		0	
	+-		0	
WPA固有設定				
5	略号化方式	O TKIP OAES	e	
	パスフレーズ	TESTSAMPLE	0	
	GTK更新圓圓	7200	Ø	
	事前認証	◯ 有効 ⊙ 無効	0	
WPA,802.1x共通設定			_	
	ブライマリ思証サーバ	192.168.1.2	Ø	
1	ブライマリ恩証サーバボート	1812	0	
2	プライマリ恩証サーバクレデンシャル	secret	0	
	セカンダリ問題サーバ		0	
	セカンダリ問題サーバポート	1812	0	
	セカンダリ問題サーバクレデンシャル		0	



・暗号方式

暗号方式には以下の方式を選択頂けますが、RADIUS サーバーをご利用頂く場合は WP A2-Enterprise(暗号化が TKIP/AES の場合)もしくは IEEE802.1x(暗号化が WEP の場合)を選択ください。ここでは WAP2-Enterprise を選択しています。

なし
WEP
WPA-PSK
WPA2-Personal
WPA2-Enterprise
IEEE802.1×

・WPA 固有設定

WPA 固有設定では、WPA2-Enterprise で利用する暗号化方式を設定します。TKIP/AE S から選択します。ここでは AES を選択しています。パスフレーズは自動的に配信され るため入力する必要はありません。必要に応じて事前認証なども選択頂けます。

WPA固有設定			
	略号化方式	O TKIP OAES	Ø
	パスフレーズ	TESTSAMPLE	e
	GTK更新間隔	7200	0
	事前認証	○ 有効 ④ 無効	0

・WPA、802.1x 共通設定 (RADIUS サーバーの登録)

RADIUS サーバーは、プライマリ・セカンダリを登録頂けます。

【ホスト名】RADIUS サーバー NetAttest EPS を指定(FQDN もしくは IP アドレス)

【ポート番号】1812 (RADIUS サーバーで利用するポート番号)

【クレデンシャル(Secret)】 最大16桁となります。

WPA,802.1x共通設定		
ブライマリ想証サーバ	192.168.1.2	0
ブライマリ思証サーバボート	1812	0
プライマリ想証サー バクレデンシャル	se (soliton	0
セカンダリ恩証サーバ		0
セカンダリ問題サーバボート	1812	0
セカンダリ問証サー バクレデンシャル		0



3-3 ACERA800ST の再起動

変更した設定内容を保存し、変更を適用するために再起動を行います。

ACERA800ST の設定は以上となります。

保存 変更を適用して再起動 無線 LAN1 セキュリティ設定 ESSID 1			
設定のコピー	ESSID 1 🗸 へ下記設定内容を	: <u> </u>	
-			
設定	◎有効 〇無効	(2)	
ESSID	TLS	0	
VLAN ID		0	
DTIMインターバル	1 💌	0	
ステルスモード	○有効 ◎無効	0	
any拒否	● 有効 ● 無効	0	
無線セパレータ	◯有効 ④無効	0	
無線セバレータポリシー	 通過 連時 	0	
無線セパレータ例外アドレス		0	
MACZRL フラマルカルング			
MACTEDX 24/03922	●有効 ●無効		
対象MACアドレス		•	
暁星ル熱ウ			
唱与北越走			
暗号方式	WPA2-Enterprise 🔽		0
WEP設定 -			_
	-F:	Open O Shared	0
4	-		0
WPA固有設定 -			
	得化方式	O TKIP O AES	0
,	「スフレーズ	TESTSAMPLE	0
G	TK更新圓隔	7200	0
4	「前書記	○ 有効 ④ 無効	0
WPA,802.1x共通設定-			
7	ライマリ思証サーバ	192.168.1.2	0
7	ライマリ恩証サーバボート	1812	0
7	ライマリ恩証サーバクレデンシャル	secret	0
ŧ	カンダリ思証サーバ		0
t	カンダリ副語サーバボート	1812	0
ŧ	カンダリ思証サーバクレデンシャル		0



4 クライアント PC の設定

4-1 クライアント PC 設定の流れ

設定の流れ

- 1. ワイヤレスネットワーク接続先の登録
- 2. ユーザー証明書のインポート



4-2 ワイヤレスネットワーク接続先の登録

ワイヤレスネットワーク接続先の登録を行います。

👍 ワイヤレス ネットワーク接続のフロパティ	
全般 ワイヤレス ネットワーク 詳細設定	
 全般 ワイヤレスネットワーク 詳細設定 ✓ Windows でワイヤレスネットワークの設定を構成する 利用可能なネットワーク(N): 範囲にあるワイヤレスネットワークに接続、切断またはは、下のボタンをクリックしてください。 ワイヤレス 優先ネットワーク(P): 下(こ一覧表示された順に、利用可能なネットワークに 	☆ W) 詳細を表示するに 、ネットワークの表示 自動的に接続します: 上へ(U)
<u>追加(A)</u> <u>ワイヤレス ネットワーク構成の設立</u> についての詳細を表示します。	►ヘロ
【ネットワーク名(SSID)】 ・TLS 【ネットワーク認証】 ・WPA2 【データの暗号化】 ・AES	ネットワーク名 (SSID)(N): TLS 「このネットワークがブロードキャストしていない場合でも接続する(N) ワイヤレス ネットワーク キー このネットワークでは)次のためのキーが必要: ネットワーク認証(A): WPA2 データの暗号(L(D): ネットワーク キーの 確認入力(Q): キーのインデックス (詳細)公: 1 ↓ 「キーは自動的に提供される(H)
	これはコンピュータ相互 (ad hoc) のネットワークで、ワイヤレス アクセス ポイ ントを使用しない(C) OK キャンセル



ワイヤレス ネットワークのプロパティ	
アソシェーション認証 接続	
認証されたネットワーク アクセスをワイヤレスのイーサネットのネットワークで提供 するには、このオブションを選んでください。	【EAP の種類】
✓このネットワークで IEEE 802.1× 認証を有効にする(E)	・スマートカードまたはその他の証明書
EAP の種類(T): スマートカードまたはその他の証明書	【コンピュータの情報が利用できる・・・】
プロパティ(<u>R</u>)	・チェック有
▶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())	
□ 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(<u>G</u>)	
OK Fャンセル	
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:	【接続のにめの認証方法】
	・このコノヒユータの証明者を使う
□ 単純な証明書の選択を使う(推奨/M)	「単純な証明者の選択を使う」
□ 次のサーバー(ご接続する(Q):	・テエック有
信頼されたルート記印用機関(R): AddTrust External CA Root	
America Online Root Certification Authority 1 GA 1 Certificate Classe A Recommender	
Certiposte Serveur	
証明書を表示する(E)	
 この接続で別のユーザー名を使う(D) OK キャンセル 	



4-3 ユーザー証明書のインポート

NetAttest EPS からダウンロードしたユーザー証明書をインポートします。

本書では、デスクトップ上に保存されている「soliton_user_0E.p12」 アイコンをダブルクリックします。

soliton user (DE p12	
証明書のインボート ウィザード	
	証明書のインボート ウィザードの開始
	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。
証明書のインボート ウィザード	
インボートする証明書ファイル インボートするファイルを指定してください。	
ファイル名(E): Ci¥Documents and Settings¥takabashi洋デスクトップ¥soliton user 0Ep	
注意: 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: Personal Information Exchange- PKCS #12 (PFX,P12) Cryptographic Message Syntax Standard- PKCS #7 証明書(P7E Microsoft シリアル化された証明書ストア(SST)	3)
	次へ(10) > キャンセル
次ペ-	ジヘ



パスワード セキュリティを維持するため(こ 秘密をに付けのコードでの保護されていました
ビイユリティを推行するのと思え、他立て「はハスン」として読みでいていないと。
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、秘密キーがアプリケーションで使われるたびに確認を求められます。
□ このキーをエクスポート可能にする(M) キーのバックアップやトランスポートを可能にします。
< 戻る(B) 次へ(M) > キャンセル
NetAttest EPS にてユーザー証明書を発行した
際に設定したパスワードを入力します。
[パスワード]
• password
証明書のインボート 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 (ご評明書ストアを自動的に選択させるか、評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(₽)
aliun者ストル: 参照(R)
〈戻る(B) 次へ(N) 〉 キャンセル
【証明書の種類に基づいて・・・】
・チェック有 次ページへ
•

Seliton





4-4 インポートされたユーザー証明書の確認

Internet Explorer より、「ツール」→「インターネットオプション」→ 「コンテンツ」タブを開きます。

インターネット オブション	? 🔀
全般 セキュリティ プライバシー コンテンツ 接続 プログラム 詳細設定	
コンテンツ アドバイザー	
「「「「「「「「」」」」「「「」」」」「「「」」」」「「」」」」「「」」」」「「」」」」	
有効にする(2)	
■ 10月香 ■ 暗号化された接続と識別のための証明書を設定します。	
	_
SSL 状態のグリア(S) 証明書(C) 発行元(B) オートマングリート	
あ Tユンフリー テ オートコンプリートによって、Web ページで前回	
1002年 入力した内容を、入力中に補完できます。 1002年	
フィードと Web スライス	
0 キャンセル 適用	
証明書	?
目的(N): < <すべて>	
個人 ほかの人 中間証明機関 信頼されたルート証明機関 信頼さ	「約1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
eps-st03.soliton_t.com 2011/10/ <	ない
インポートした	ト証明書
インボートロ エクスボート(E)」 削除(R)	詳細設定(<u>A</u>)
~証明書の目的	



改訂履歴

日付	版	改訂内容
2012/9/28	1.0	初版作成