NetAttest EPS 設定例

連携機器:

Alcatel-Lucent Omni Access WLAN Case:TLS方式での認証

Version 1.1

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 \odot 2011, Soliton Systems K.K. , All rights reserved.



はじめに

本書について

本書は CA 内蔵 RADIUS サーバーアプライアンス NetAttest EPS とアルカテ ル・ルーセント社製 無線 LAN スイッチ Omni Access WLAN における 802. 1X 認証環境の構築について、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)	इ.
ABCDabcd1234	
(italic)	

表記方法	説明
ſ]	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]+[‡- 2]	[キー1]を押しながら[キー2]を押すことを表します。

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 いことを示しています。

アイコンについて

アイコン	説明
•	利用の参考となる補足的な情報をまとめています。
•	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 Omni Switch 6 850,Omni Access WLAN 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	6
2NetAttest EPS	8
2-1 NetAttest EPS 設定の流れ	
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 ユーザーの登録	11
2-5 ユーザー証明書の発行	13
3 Alcatel-Lucent	
3-1 設定の流れ	
3-2 Switch 側設定項目	15
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 Windows XP での設定	20
4-3 Windows 7 での設定	25
4-4 インポートされたユーザー証明書の確認	



1 構成

1-1 構成図

- ・無線 LAN で接続する機器は L2 スイッチに収容
- ・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-ST03 の DHCP サーバーから払い出す





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-ST03	Ver. 4.2.3
Authenticator	Alcatel Lucent	Omni Switch 6850	
Access WLAN (RADIUS クライアント)	Alcatel Lucent	Omni Access WLAN	
無線 Access Point	Alcatel Lucent	OmniAccess WirelessLAN Access Points	
Client PC / Supplicant	Panasonic Microsoft	Let's note CF-W7	Windows XP SP3 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-ST03	Omni Access W LAN	OmniAccess WirelessLAN Access Points	Client PC		
IP アドレス	192.168.1.2	192.168.1.251	192.168.1.250	192.168.1.112 (DHCP)		
RADIUS port (Authentication)		UDP 1812				
RADIUS port (Accounting)		_				
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
- ◆ メインネームサーバーの設定

	💽 🗟 🍫 🗙	
😭 お気に入り 🏾 🏉 システム管理-Net'Attest EPS 🛛 👘 🔹 🕤 🗸	🖃 🚔 • ページ(P) • セーフティ(S) • ツール(O) • 🕡 •	
Net Attest EPS		
「● 初期設定ウィザード		
 システム初期 サービス知識 	設定	
	INX.JE	
	ネーー 初期設定ウスザード - 設定項日の確認	2
¹ 0 1 日 4 1 2 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1		
	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	
	₽₽₣₽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	
	₽₽₣₽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。
		戻る再起動
	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、黒文字の項目のみ、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)
- ◆ RADIUS サーバーの基本設定(EAP)
- ◆ RADIUS サーバーの基本設定(証明書検証)
- ◆ NAS/RADIUS クライアント設定

初期設定ウィザード-○△描築			1	
Manxe 717 F CAma				
CA種別選択				
CA種別選択				
CA秘密鍵生成		初期設定ウィザード – L DAE	データペーフの設定	
公開鍵方式	RSA 💌			
鍵長	2048 💌	編集対象:新規		
CA情報		名前*	LocalLdap01	
CA名(必須)	na-labo CAD1	サフィックス*	dc=na-labo,dc=s	oliton,dc=jp
国名	日本			
都道府県名	Tokyo	説明		-
市区町村名	Shinjuku			_
会社名(組織名)	Soliton Systems K.K.			戻る次へ
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 - RAD	IUSサーバーの基本設定	
		ł		
Copyright © 2004-2010, Soliton Syst	ems K.K., All rights reserved.	全般		
		認証ボート*	1812	
		アカウンティングポート*	1813	
		□ ログにパスワードを表示	示する(PAP認証のみ)	
		□ セッション管理を使用で	ta	
		■ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □	ティングバケットをバートナー	こ転送する



17月2日文正フィンニト ニ RADIUS ワー。	バーの基本設定				
EAP					
EAP認証タイブ					
優先順位 認証タイブ					
2 PEAP -					
3 <mark>なし →</mark>					
4 <mark>なし ▼</mark> 5 なし ▼					
EAP-TLS/TTLS/PEAPオプション					
メッセージフラグメントサイズ	1024 - バイト				
メッセージの長さ情報	フラグメントされた 最初の)バ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	有効にする				
		展るとなって			
					1
		初期設定ウィザー	- RADIUSサーバー	-の基本設定	
opyright © 2004-2011, Soliton Systems	K.K., All rights reserved.				
				=ToFI++++++=T	
		四	コリニトス 投資すたたい	aL約音(次aL	
		ロテカリ	ストによる快証で有X別 約つ証明機関素		~ プラール - (は 4)は 4) 日本
			5 I J 61. 77 J 105 (94) 	◎ 階増まで(1~	9, テノオルト進:りは 9と回尽)
		CNJ 1.99	* 1		<u>∠</u> _¥
				例:%{Use	r-Name}
		サラジェク	⊦チェック条件	例:%{Use 例:O=Co	r-Name) た含む npany/OU-Branch
		サラジェク	↓チェック条件	691: 94(Use	r-Aame) た会む npany/OU-Branch
設定ウィザード – NAS/RADIUSクラ	ライアント設定	サ <i>ラジェ</i> ク	テェック条件	691: 96(Use	r-Aame) 加pany/OU=Branch
設定ウィザード – NAS/RADIUSク . 冨茱対象: 新 規	ライアント設定	<i>ل</i> ±עּדָ ז	トチェック条件	β¶: 9%(Use β¶: Ο=Co	r-Aame) を含む apany/OU-Branch
設定ウィザード – NAS/RADIUSク= 霍集対象: 新 規 NAS/RADIUSクライアント名	ライアント設定 TestClient	9 <i>39±</i> 9	トチェック条件	691: 9%(Use	r-Aame) た合む apany/OU=Branch
設定ウィザード – NAS/RADIUSク= 電集対象: 新規 NAS/RADIUSクライアント名。 図 このNAS/RADIUSクライアントを約	ライアント設定 TestClient 自効にする	9 <i>99</i> 2	+チェック条件	β¶: 9%(Use β¶: Ο=Co	F-A ane) を含む npany/OU=Branch 更る 次へ
設定ウィザード – NAS/RADIUSク= 冨集対象: 新規 NAS/RADIUSクライアント名・ ■ このNAS/RADIUSクライアントを引 EV時	ライアント設定 TestClient 有効にする		+ チェック条件	691: 96(Use	FAme) を含む mpany/OU=Branch 展る 次へ
設定ウィザード – NAS/RADIUSクラ 電集対象: 新規 NAS/RADIUSクライアント名 ごのNAS/RADIUSクライアントを 説明	ライアント設定 TestClient 自効にする	1955 tr	トチェック条件 n Systems K.K	ලිබ්: 96(Use	FAme) を含む mpany/OU=Branch 更る 次へ
設定ウィザード - NAS/RADIUSクラ ■集対象: 新規 NAS/RADIUSクライアント名* 図 このNAS/RADIUSクライアントを 説明 IPアドレス*	ライアント設定 TestClient 自効にする 192.168.1.100		トチェック条件 in Systeme K-K	βi : %(Use βij : O=Co βij : O=Co	F-Aane) を含む apaany/OU=Branch 更る 次へ
設定ウィザード - NAS/RADIUSク= 富集対象: 新規 NAS/RADIUSクライアント名 ☑ このNAS/RADIUSクライアント名 説明 IPアドレス。 シークレット	ライアント 設定 TestClient 有効にする 192.168.1.100		トチェック条件 in Systems K.K	ි වි: %(Use (වි]: O=Co	F-Ame) を含む mpany/OU=Branch 戻る 次へ
設定ウィザード - NAS/RADIUSクラ 編集対象: 新規 NAS/RADIUSクライアンド名。 望 このNAS/RADIUSクライアンド名。 説明 IPアドレス。 シークレット・ 所属するNASグループ	ライアント 設定 TestClient 自効にする 192.168.1.100		トチェック条件 Jin Systeme K.K	fil: %(Use	F-Ame) Real Carlos F-Ame) Carlos F-Ame) Carlos
 設定ウィザード - NAS/RADIUSクラ 編集対象: 新規 NAS/RADIUSクライアント名 ごのNAS/RADIUSクライアント名 説明 ピアドレス シークレット・ 所属するNASグルーブ 	ライアント設定 TestClient 自効にする 192.168.1.100 ・・・・・・		+チェック条件	ØI : %(Use ØI : %(Use ØI : % ØI : % <t< td=""><td>F-Ame) Appany/OU=Branch 戻る 次へ</td></t<>	F-Ame) Appany/OU=Branch 戻る 次へ
設定ウィザード - NAS/RADIUSクラ 編集対象: 新規 NAS/RADIUSクライアント名* 図 このNAS/RADIUSクライアントを 説明 IPアドレス* シークレット* 所属するNASグルーブ	ライアント設定 TestClient 有効にする 192.168.1.100 ・・・・・・ ▼		トチェック条件 on Systems K.K	fil: ۹ه(Use	F-Aane) を含む npany/OU=Branch 戻る 次へ
設定ウィザード - NAS/RADIUSクラ 編集対象: 新規 NAS/RADIUSクライアント名 ご このNAS/RADIUSクライアント名 説明 IPアドレス シークレット 所属するNASグループ	ライアント設定 TestClient 有効にする 192.168.1.100 ・・・・・・		+チェック条件 In Systems K.K	ر البالي (بالع البالي البالي البالي (بالبالي البالي	F-Aane) Reference for the second se
設定ウィザード – NAS/RADIUSクラ 編集対象: 新規 NAS/RADIUSクライアント名 ご このNAS/RADIUSクライアント名 説明 IPアドレス シークレット 所属するNASグルーブ	ライアント 設定 TestClient 自効にする 192.168.1.100 ・・・・・・ ▼		トチェック条件 Jin Systeme K.K	() I ights reserved.	Frame) mpany/OU=Branch 展る 次へ
設定ウィザード - NAS/RADIUSクラ 編集対象: 新規 NAS/RADIUSクライアント名 ご このNAS/RADIUSクライアント名 説明 IPアドレス シークレット・ 所属するNASグループ	ライアント設定 TestClient 耳効にする 192.168.1.100 	サ ブジェク ・ ・ 、 、 、 、 、 、 、 、 、 、 、 、 、	Fチェック条件 in Systeme K K	() () <td< td=""><td>F-Aane) mpany/OU=Branch 戻る 次へ</td></td<>	F-Aane) mpany/OU=Branch 戻る 次へ
 設定ウィザード - NAS/RADIUSクラ 編集対象: 新規 NAS/RADIUSクライアント名 コ このNAS/RADIUSクライアント名 説明 IPアドレス シークレット・ 所属するNASグループ 	ライアント設定 TestClient 自効にする 192.168.1.100 ・・・・・・ ・	サブジェグ ・ ・ ・ 、 、 、 、 、 、 、 、 、 、 、 、 、 、 、 、	▶ チェック条件 In Systems K.K	fil: ۹ه(Use (۶۹): O=Co	FAIRE) mpany/OU-Branch 戻る 次へ
設定ウィザード - NAS/RADIUSク 編集対象: 新規 NAS/RADIUSクライアント名・ 図 このNAS/RADIUSクライアント名・ 説明 IPアドレス・ シークレット・ 所属するNASグルーブ	ライアント設定 「TestClient 有効にする 192.168.1.100 ・・・・・・ ▼	サナジェク ・ ・ 、 、 、 、 、 、 、 、 、 、 、 、 、	FJエック条件 >n Systems K.K	ØI : %(Use ØI : %(Use ØI : % ØI : % <t< td=""><td>Frame) Real Carlos Real 次へ</td></t<>	Frame) Real Carlos Real 次へ
設定ウィザード - NAS/RADIUSクラ 編集対象: 新規 NAS/RADIUSクライアント名 ご このNAS/RADIUSクライアント名 説明 IPアドレス シークレット 所属するNASグループ	ライアント 設定 TestClient 自効にする 192.168.1.100 ・・・・・・ ・		トチェック条件 Jin Systems K.K	C, All rights reserved.	rAnne) mpany/OU=Branch 戻る 次へ
設定ウィザード - NAS/RADIUSクラ 編集対象: 新規 NAS/RADIUSクライアント名 ご このNAS/RADIUSクライアント名 説明 IPアドレス シークレット 所属するNASグループ	ライアント設定 TestClient 自効にする 192.168.1.100 ・・・・・・ ▼	サ ブジェグ	Fチェック条件 In Systems K.K	()) ()) ()) ()) ()) ()) (), All rights reserved.	FAIRE) mpany/OU=Branch 更る 次へ
設定ウィザード - NAS/RADIUSク 電集対象: 新規 NAS/RADIUSクライアント名 ご このNAS/RADIUSクライアント名 説明 IPアドレス シークレット 所属するNASグループ	ライアント設定 TestClient 192.168.1.100 	サ ブジェク サ ブジェク ・ ・ 、 、 、 、 、 、 、 、 、 、 、 、 、	FJエック条件	ر بالعالي (Use) (بالعالي) (ب العالي) () () () () () () () () () () () () ()	FAIRE) mpany/OU-Branch 戻る 次へ

2-4 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。



2-5 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			0	●トッフページ ● 読定保存) ● ロジオフ)
■ 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 🔹 🔹 🔹 完全	グループ 🔹 1000 ユーザー	まで「検索」	-
■証明機関 ■ DHCPサーバー	名前		<u>2-4-10</u>	28 Mar タスク
■ LDAPサーバー ■ DADUCH - バー			soliton_user Rfi	天王 利用
* RADIOS 9 - A-				
■ ユーザー一覧 ■ エムマポート		-		-
■ インボート		基本情報		
■ユーリーバスフードホララー ■デフォルトユーザープロファイル		姓	ソリトン	
		名	一郎	
		E-Mail		
		訐粬 憜報		~
		認証情報		
		ユーザーID	soliton_user	
		有効期限		
		◎日数 365		ま 50 - 八 50 - 秋 末
		7		т <mark>33 т</mark> јј <mark>33 т</mark> ју а.
		証明書ファイルオブシ	עצי	
		パスワード	•••••	
		バスワード(確認)	•••••	
		※バスワードが空棚の		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	
				発行キャンセル
·				
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し	た。対象をファイルに保存して下さ	い。 ダウンロード
● 証明機関 ● DHCP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				
■ インポート				
■ ユーザーパスワードポリシー				
■ テフォルトエーザーブロファイル				



3 Omni Access WLAN

3-1 設定の流れ

Alcatel-Lucent 社製スイッチ Omni Access WLAN を設定するためには、W ebGUI または CLI を用います。本書では WebGUI を用いて各種設定を実施す る方法を紹介します。



3-2 Switch 側設定項目

3-2-1 Radius サーバーの登録

RADIUS サーバーとして NetAttest EPS を登録します。

[SECURITY]メニューを展開し、[Servers]リンクをクリックします。

「Summary」項目の中「RADIUS Servers」欄の[Name]の下の[Empty]

から RADIUS の登録をします。

Alcatel-Lucent	0			T			vx ⁻	Target (192.168.1.254)		Options
Physical	Server	RADIUS	LDAP	ACE	TACACS+	Authentication	Accounting	Certificate		
Layer 2										
Networking										
Policy		-								
Security	Secu	urity Se	rvers	Hom	e					
	About	Security S	ervers							
AVLAN	The Se	curity Serve	rs feature	is used	to configure	the switch to comn	nunicate with au	uthentication servers.	These servers are used for storing inform	mation abo
	(Authe	nticated Swit	ch Access In User S	;) and us ervice (I	sers who nee: RADIUS), Lia	d access to a partion htweight Directory	ular VLAN or V Access Protoco	LANs (Authenticated V I (LDAP), SecurID痴 A	LANs or 802.1X Port-Based Network Acc CE/Server, and Terminal Access Contro	ess Contro ller Access
<u>i</u> e								. (, ,),,,,,,,		
ASA	More									
	Sumn	arv								
									1949.0	
Servers	RADIU	S Servers							LDAP Servers	
a	Name	V Host Nar	ne IP	Address	: <u>5</u>				Name Host Name IP Address	
	NetAtt	est		192.168	.1.2 =				[EnibrA]	
	ACES	ervers							TACACS+ Servers	
i c	Name	Host Name	IP Addres	35					Name Host IP Address Port	
	[Empty]							[Empty]	
Network Security										



RADIUS Servers 登録ページが開くので[Add]ボタンをクリックし下記値を入力する。

Alcatel·Lucent						vxTa	rget (192.168.1.254)		Options Save	Configuration Help		₩ = 🗗 t Log Out
Physical	Server R	ADIUS LD	AP ACE	TACACS+ A	Authentication	Accounting	Certificate					
Layer 2												
Networking Policy Security	RADIU	S Serve	rs									
8. 2 ⁴ 2		Server Name V	Host Name	IP Address	Backup Host Name	Backup IF Address	Authentication Retries	Authentication Timeout (sec)	Authentication Port	Accounting Port	VRF Name	S
AVLAN		VetAttest		192.168.1.2		0.0.0.0	3	2	1812	1813	default	
ASA Servers	Add	Modify	Dele	te Refr	esh Help]						
Access Guardian												
Network Security												

入力値

[Server Name] NetAttest

[IP Adress] 192.168.1.2

[Backup Host Name] 0.0.0.0

[Authentication Retries] 3

[Authentication Timeout (sec)] 2

[Authentication Port] 1812

[Accounting Port] 1813

[VRF Name] default



3-3 Omni Access WLAN 側設定項目

3-3-1 Radius サーバーの登録

Radius サーバーとして NetAttest EPS を登録します。

[Configuration]タブをクリックします。[Security]メニューの[Authenticat ion]リンクをクリックし、右ペインの[Server]タブの中の[RADIUS Server] リンクをクリックします。その後、Radius サーバー名を入力して[Add]ボタ ンをクリックし、登録します。



[Host] 192.168.1.2 [Key] Soliton

> [Retype] soliotn



3-3-2 SSID の設定

SSID の設定を行います。

[Configuration]タブをクリックします。[Wireless]メニューの[AP Configuration]リンクをクリックします。

[Profiles]欄から[Wireless LAN]-[Virtual AP]と進めていき、[SSID Profile]

から[Profile Details]を設定します。

Network 欄の[Network Name]と[802.11 Security]を認証方式を設定します。

Monitoring Configura	tion Diagnostics Maintenance Plan	Events Report	ts Save Configuration			Logout adm
Wizards AP Wizard	Configuration > AP Group	o > Edit "de	efault"			
Switch Wizard						
WLAN/LAN Wizard	Profiles			Profile	Details	
License Wizard	E Wireless LAN		SSID Profile > wyse-test-s	ssid prof 💌	Show Reference	Save As Reset
Network	 Virtual AP 					
UI Mia	wyse-test-vap_prof		Basic Advanced			
Ports	🛨 AAA Profile	wyse-test- aaa_prof	Network			
Cellular Profile	802.11K Profile	default	Network Name (SSID)		wyse-test	
IP Security Authentication	SSID Profile ssid_prof	802.11 Security				
Access Control	EDCA Parameters Station profile		Network Authentication	C None C 802.1x/WEP C	O wpa O wpa-psk 👁 wpa	2 C WPA2-PSK
Wireless	EDCX Parameters XP pronie			C Mixed		
AP Configuration AP Installation	High-throughput SSID Profile	wyse-test- htssid_prof	Encryption			
Management General	WMM Traffic Management Profile		Keys			
Administration	RF Management					
Certificates	AP OOS					
SNMP	IDS					
Logging	💽 Mesh					

入力値

[Network Name(SSID)] wyse-test

[802.11 Security] WPA2

[Encryption] AES



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

Windows XP での設定

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

Windows 7 での設定

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



4-2 Windows XP での設定

4-2-1 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





証明書のインボート ウィザード 🛛 🕅
パスワード 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。 パスワード(<u>P</u>): 「******* 「秘密キーの保護を強力にする(<u>E</u>) このオプ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(N) > 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。
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。
< 戻る(B) 次へ(M) > キャンセル
【証明書の種類に基づいて・・・】 ・チェック有

Seliton



- 22 -

4-2-2 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				
✓ Windows でワイヤレス ネットワークの設定を構成す	3₩			
←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。	は詳細を表示するに			
7777	ス ネットワークの表示			
優先ネットワーク(P): 下に一覧表示された順に、利用可能なネットワーク(こ自動的に接続します:			
	<u>المراسم</u>			
	下へ(<u>D</u>)			
<u>追加(A)</u> 削除(R) プロパテ	· <u>r@</u>)			
ワイヤレスネットワーク構成の設定	[詳細設定(⊻)			
16.06.1CW5+###23877104.96	ワイヤレス ネットワー	クのプロパ	<u>∓</u> ∢	? 🗙
	アソシエーション 認識	正接続		
	ネットワーク名 (SSI))(<u>N</u>):	NA-Labo Wireless	
	🗹 このネットワー	ウがブロード ≯	トャストしていない場合でも接続す	する(<u>N</u>)
	-01762 ネットワ	-クキー		
	このネットワークで	よ)欠のための)キーが必要: 	
	ネットワーク認証	<u>A</u>):	WPA	×
	ナーダの増ち1日	<u>y</u>):	AES	×
	ネットワークキー	<u>(</u>):		
	ネットワークキー 確認入力(0):)		
	キーのインデックス	(言羊糸用)()())	1	
	- ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓	に提供される	5(H)	
			· <u></u>	
	 これはコンピュー・ ントを使用しない 	湘互 (ad hi (C)	oc) ወネットワークで、 ワイヤレス	アクセス ポイ
			ОК	キャンセル







4-3 Windows 7 での設定

4-3-1 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。

	 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、またはゼ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、Dたへ]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	× る(B) (N) > キャンセル
 C×Users¥nkubota¥Desktop¥soliton_user_0E.p12 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 Personal Information Exchange- PKOS #12 (PFX_P12) Cryptographic Message Syntax Standard- PKOS #7 証明 Microsoft シリアル化された証明書ストア (SST) 	参照(B)
証明書ファイルの形式の詳細について表示します。 	B) 次へ(N)> キャンセル



証明書のインポート ウィザード	X
パスワード	
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す。 	
秘密キーのパスワードを入力してください。	
■ おがあた → の(兄妹たびた力)	
■ 祝田子一の「米酸を受力にすると、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 このオプ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	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。 	
▼ すべての拡張プロパティを含める(A)	
ヴェイベート なこの(兄妹の話名の(ついてまテレキオ	
	キャンセル
NetAttest EPS にてユーザー証明書を発行した	
正明書のインポート ウィザード	x
正明書のインボート ウィザード	X
正明書のインボート 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。	X
正明書のインボート ウィザード	
証明書のインボート ウィザード 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。 ・ 証明書の種業類に基づいて、自動的に証明書ストアを選択する(U) ・ 証明書ストア:	
 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。 証明書の種業類に基づいて、自動的に証明書ストアを選択する(U) 証明書の種業類に基づいて、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(P) 証明書ストア: 	<u>х</u>
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。 ・ ・ 証明書の種業類に基づいて、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(ご配置する(P) 証明書ストア:	Χ
証明書のインボート ウィザード 証明書ストア 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。 ④ 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)) ⑥ 証明書をすべて(次のストア(ご配置する(P)) 証明書ストア: 参照	χ
	★
	<u>х</u>
な明書のインボート ウィザード	<u>κ</u> (<u>B</u>)
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。	<u>κ</u> (B) (B)
ご明書のインボート ウィザード 「 ご明書ストアは、証明書が「保管されるシステム上の領域です。 「 いれdows (ご証明書ストアを自動的にご選択させるか、証明書の場所を指定することができます。 「 ご 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)」 「 ご 証明書をすべて、次のストアに配置する(P) 正明書ストアの詳細を表示します (く 戻る(B) 、 次へ(N) 【 証明書の種類に基づいて、・・】	χ (B)
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1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ご選択させるか、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、自動的に証明書ストアを選択する(U) ● 証明書の種類に基づいて、自動的にごご可用書ストアを選択する(U) ● 証明書ストア: ● 証明書ストアの詳細を表示します 【証明書の種類に基づいて・・・】 ・チェック有	R(B) *+νンセル
	χ R(B)





4-3-2 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。





) .血 ワイヤレス ネットワーク	に手動で接続します	
追加するワイヤレス ネットワ	ロークの情報を入力します	
ネットワーク名(E):	soliton	[ネットワーク名]
セキュリティの種類(S):	WPA2-エンタープライズ 🔹	Soliton
暗号化の種類(R):	AES	
セキュリティ キー(C):	文字を非表示にする(H)	[セキュリティの種類]
☑ この接続を自動的に開	始します(T)	WPA2-エンタープライズ
□ ネットワークがブロー	ドキャストを行っていない場合でも接続する(0)	
警告: 選択すると、このコン	ピューターのプライバシーが危険にさらされる可能性があります。	[暗号化の種類]
		AES
	次へ(N) キャンセル	

soliton ワイヤレス ネットワークのプロパティ	
接続 セキュリティ	
セキュリティの種類(E): WPA2 - エンタープライズ → 暗号化の種類(N): AES →	
ネットワークの認証方法の選択(O): 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)	
詳細設定(D)	[ネッ Micro その(
<u>ОК</u> <u></u>	

ネットワークの認証方式の選択] Microsoft スマートカードまたは その他の証明書



スマートカードまたはその他の証明書のプロパティ	
接続のための認知です注	
/ 自分のスマート カードを使う(S)	
◎ 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)	
☑ サーバーの証明書を検証する(V)	
□ 次のサーバー(は接続する(∩))	
naens local	
(hadpolloda)	「信柄大わたり」」と証明燃用)
信頼されたルート証明機関(R):	[16枚C1 いこルート証明機関]
🔲 GTE Cyber Trust Global Root	na-ens ca
Microsoft Root Authority	
Microsoft Root Certificate Authority	
🔽 na-ens ca	
Soliton Boot CA	
Thomas Promium Server CA	
Thawte Premium Server CA	
I Inawte Timestamping CA	
証明書を表示する(E)	
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)	
□この接続で別のユーザー名を使入り	



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。



目的(<u>N</u>): 個人 ほかの人 (ぼうべて> 中間証明機関 「信頼されたルート	証明機関「信頼された発行が	こ 信頼されない発行元
発行先		有効期限 フレンドリ名	
<u≌soliton_user< td=""><td>eps-st03.soliton.pt.com</td><td>n 2011/10/ <なし></td><td>></td></u≌soliton_user<>	eps-st03.soliton.pt.com	n 2011/10/ <なし>	>
インポートΦ	エクスポート(E) 削除(R)		
-証明書の目的――			
			===00

2



改訂履歴

日付	版	改訂内容
2012/2/1	1.0	初版作成
2012/9/10	1.1	RADIUS PortをTCPからUDPに修正