



【連携機器】アイ・オー・データ機器 BSH-GM シリーズ/BSH-GP08 【Case】IEEE802.1X EAP-PEAP(MS-CHAP V2)/EAP-TLS

Rev2.0

株式会社ソリトンシステムズ



はじめに

本書について

本書はオールインワン認証アプライアンス NetAttest EPS と、アイ・オー・データ機器社製 L2 ス イッチ BSH-GM シリーズ/BSH-GP08 の IEEE802.1X EAP-PEAP(MS-CHAP V2)/EAP-TLS 環境で の接続について設定例を示したものです。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。 Seliton Pracour

アイコン	説明
(پ	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 BSH-G08M 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。

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。

<u>Saliton</u>

1.	構成	.1
	1-1 構成図	1
	1-2 環境	2
	1-2-1 機器	. 2
	1-2-2 認証方式	. 2
	1-2-3 ネットワーク設定	. 2
2.	NetAttest EPS の設定	. 3
	2-1 初期設定ウィザードの実行	3
	2-2 システム初期設定ウィザードの実行	4
	2-3 サービス初期設定ウィザードの実行	5
	2-4 ユーザーの登録	6
	2-5 クライアント証明書の発行	7
3.	BSH-GM シリーズ/BSH-GP08の設定	. 8
3.	BSH-GM シリーズ/BSH-GP08 の設定 3-1 IP アドレスの設定	. 8 9
3.	BSH-GM シリーズ/BSH-GP08 の設定 3-1 IP アドレスの設定 3-2 RADIUS サーバーの設定1	.8 9 10
3. 4.	BSH-GM シリーズ/BSH-GP08の設定 3-1 IP アドレスの設定 3-2 RADIUS サーバーの設定1 Windows 10 のクライアント設定1	.8 9 10
3. 4.	BSH-GM シリーズ/BSH-GP08 の設定 3-1 IP アドレスの設定	.8 9 10 13
3. 4.	BSH-GM シリーズ/BSH-GP08 の設定 3-1 IP アドレスの設定	.8 9 10 13 13
3.	BSH-GM シリーズ/BSH-GP08 の設定 3-1 IP アドレスの設定	.8 9 10 13 13
3. 4.	BSH-GM シリーズ/BSH-GP08 の設定	.8 9 10 13 13 14 14
 3. 4. 5. 	BSH-GM シリーズ/BSH-GP08 の設定	.8 9 10 13 14 14 16
3. 4. 5.	BSH-GM シリーズ/BSH-GP08 の設定	.8 9 10 13 13 14 14 16



<u>Seliton</u> 1. 構成

1-1 構成図

以下の環境を構成します。

- 有線 LAN で接続する機器は L2 スイッチに収容
- 有線 LAN で接続するクライアント PC の IP アドレスは、NetAttest D3-SX04 の
 DHCP サーバーから払い出す



S≎liton®

1-2 環境

1-2-1 機器

製品名	メーカー	役割	バージョン	
NetAttest EPS-ST05	ソリトンシステムズ	RADIUS/CA サーバー	4.10.3	
BSH-G08M	アイ・オー・データ機器	RADIUS クライアント (L2 スイッチ)	2.1.0	
VAIO Pro PB	VAIO	802.1X クライアント (Client PC)	Windows 10 64bit Windows 標準サプリカント	
NetAttest D3-SX04	ソリトンシステムズ	DHCP/DNS サーバー	4.2.16	

1-2-2 認証方式

IEEE802.1X EAP-PEAP(MS-CHAP V2)/EAP-TLS

1-2-3 ネットワーク設定

機器	IP アドレス	RADIUS port (Authentication)	RADIUS Secret (Key)	
NetAttest EPS-ST05	192.168.1.2/24	1913	secret	
BSH-G08M	192.168.1.1/24	UDF 1612	secret	
Client PC	DHCP	-	-	

<u>Seliton</u>

2. NetAttest EPS の設定

2-1 初期設定ウィザードの実行

NetAttest EPS の初期設定は LAN2(管理インターフェイス)から行います。初期の IP アドレスは 「192.168.2.1/24」です。管理端末に適切な IP アドレスを設定し、Internet Explorer から 「http://192.168.2.1:2181/」にアクセスしてください。

下記のような流れでセットアップを行います。

- 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

NetAttest EPS の初期設定は LAN2(管理インターフェイス)から行います。初期の IP アドレスは「192.168.2.1/24」です。管理端末に適切な IP アドレスを設定し、Internet Explorer から「http://192.168.2.1:2181/」にアクセスしてください。

その後、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



項目	値
ホスト名	naeps.example.com
IP アドレス	デフォルト
ライセンス	なし

<u>Seliton</u>

2.NetAttest EPS の設定

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。

- 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

CA種別選択			
CANDERIN	"⊸⊦са ∨		
CANCER			
● 内部で新しい鍵を生成する			
公開減方式	RSA 🛩		
鍵長	2048 🗸		
○ 外部HSMデバイスの鍵を使	ยแฐอ		
要求の署名			
要求署名アルゴリズム	SHA256 V		
CA情報			
	TestCA		
国名	日本	~	
都道府积名	Tokyo		
市区町村名	Shinjuku		
会社名(組織名)	Soliton Systems		
部署名			
E-mailアドレス			
CA署名設定			





項目	値
CA 種別選択	ルート CA
公開鍵方式	RSA
鍵長	2048
CA名	TestCA

項目	値
優先順位	EAP 認証タイプ
1	TLS
2	PEAP

項目	値
NAS/RADIUS クライアント名	RadiusClient01
IPアドレス	192.168.10.1
シークレット	secret

Seliton 2-4 ユーザーの登録

NetAttest EPS の管理画面より、認証ユーザーの登録を行います。

[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行います。

Net Attest FPS			ログオン中: admin
	8		() トップページ) 🕒 設定保存) 🕚 ログオフ)
 Hadpstexample.com システム設定 システム管理 証明機関 DHCPサーバー 	 ユーザーー覧 ユーザー ユーザー ● 一部 ● 完全 詳細オブションの設定 エクスポート 	<i>グ</i> ループ <mark>∨</mark> コ	ーザーまで 検索
■ LDAPサーバー ■ RADIUSサーバー ■ ユーザー	● 2前	7 – ⁺f – m	道加 ユーザー削除時の証明書失効オフ 品後調査には10日時 (17日日本 タフク
■ ユーザー一覧 ■ エクスポート ■ インポート	test user	test	#X###################################
■ ユーザーバスワードポリシー ■ デフォルトユーザープロファイル ■ ゲスト		2-ザ- 編集対象:	設定
		ユーザー情報 基本情報	<u>チェックアイテム</u> リナライアイテム 0TP
		gf: 名 E-Mail	
		詳細情報 認証情報	
項目		ユーザーID パスワード	• user01
姓	user01	パスワード(
ユーザーID	user01		MIFY IL
パスワード	password		OK キャンセル 通用
			V ログオン中: admin
NetAttest EPS			(1) トップページ 白 読定保存 (1) ログオフ
 raepsexample.com システム設定 システム管理 証明機関 DHCPサーバー 	<u>ユーザー</u> 覧 ユーザー 詳細 <u>オブションの設定</u> エ <u>クスポート</u>	グループ 🔽 ニ	レーザーまで
■ LDAPサーバー ■ RADIUSサーバー			追加 ユーザー削除時の証明書失効オプション
■ ユーザー ■ ユーザー一覧	名前 test user	<u>ユーザーID</u> test	最終認証成功日時 証明書 タスク
■ エクスポート ■ インポート	user01	<u>user01</u>	9217 変更 削除 発行 変更 削除
■ 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 # ゲスト			



NetAttest EPS の管理画面より、クライアント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クライアント証明書を発行します。

(クライアント証明書は、user01.p12 という名前で保存)

						ヴォンロレッシー
NetAttest EPS					-ジ 合 設定保存	
■ naensexample rom	~					
■ システム設定	- <u>-</u> -					
■ システム管理	ユーザー	● 一部 ● 完全	グループ 💙 🔤	ユーザーまで 検索		
■ mu-ynxce ■ DHCPサーバー	詳細オフションの エクスポート					
■ LDAPサーバー						追加
■ RADIUSサーバー ■ ユーザー		A 34	- <i>4</i> - m	<u>2-</u>	-ザー削除時の証明書の	夫効オブション
■ ユーザー一覧		<u> </u>	<u>tort</u>	<u> </u>		
■エクスポート					発行 変更	
■ ユーザーパスワードポリシー		user01	<u>useru i</u>		第67 変更	削除
■ デフォルトユーザープロファイル						
■ ウスト 						
					1	
			编集対象: user01			
			基本情報			
			姓	user01		
			名			
			E-Mail			
			前关制作者转移		ć	
						<u>×</u>
			認計報	upor01		
			有効期限	usero i		
			● 日数 365		· 며 59 V 슈 59 V 원	***
			証明書ファイルオブション		or 0.0 10 10	
			パスワード			
		値	バスワード(確認)			
明書有効期限		365	※パスワードが空間の場合に	コム・ユーザーのバスワードを使用		
			✓ PKCS#12ファイルに証	明機関の証明書を含める		
(CS#12 ノアイルに証明機関	an	ナエック有			発行	キャンセル
					V	
		📕 ユーザー証明	書のダウンロード			
		ユーザー証明書ダウンズ	コードの準備が <u>できました。対</u>	 象をファイル <u>に保存して</u> つ	さい。 ダウ	<u>и-к</u>



3. BSH-GM シリーズ/BSH-GP08 の設定

アイ・オー・データ製 L2 インテリジェントスイッチの BSH-GM シリーズおよび BSH-GP08 は同 一の方法で設定が可能です。そのため本書では、代表して BSH-G08M を使用して設定を行います。 購入時の IP アドレスは DHCP 設定となっていますので、専用ツール「Magical Finder」を使います。 「Magical Finder」は下記 Web ページにアクセスし、お使いの OS を選んでダウンロードします。 http://www.iodata.jp/r/3022

Magical Finder を起動すると、下記のように対象製品が表示されます。

設定を行う機器を選択し、「Web 設定画面を開く」をクリックして設定画面を起動します。

Magical Finder		- 🗆 ×	🔎 Magical Finder		-		×
ネットワークデバイス一覧			< デバイス情報	R			
BSH-G08M MACアドレス ■ IPv4アドレス 192	2.168.0.7			BSH-G08M			
			ΜΑϹアドレス				
			IPv4 情報				
			IPアドレス割当設定	DHCP有効			
			IPv4アドレス	192.168.0.7			
			サブネットマスク	255.255.255.0			
			デフォルトゲートウェイ	192.168.0.1			
						_	
				Web設定画面を開く]	
				ネットワーク設定を変更]	
ヘルプ	更新	バージョン	ヘルプ	端末情報	バーミ	íзУ	

設定画面が起動したら、ユーザー名/パスワードを入力しログインします。

初期ユーザー名は admin(小文字) パスワードは IODATA(大文字)です

ログイン	
http://192.1 このサイトへの	68.0.3 接続ではプライバシーが保護されません
ユーザー名	admin
パスワード	
	ログイン キャンセル

BSH-G08Mのセットアップは下記の流れで行います。

- 1. IP アドレスの設定
- 2. RADIUS サーバーの設定

3-1 IP アドレスの設定

[ネットワーク]-[IP アドレス]にアクセスし IP アドレスを設定します。

IP アドレス設定画面を開いたら以下の項目を設定します

ログアウト	画面で見るマニュアル				
状態	>				
ネットワーク	~	8 port Gigabit			
IPアドレス					
時刻設定					
ポート	>	IPV47 PDA			
		アド	レスタイプ	 ダイナミック 	
VLAN	>	IPv	14アドレス	192.168.1.1	
		サブネッ	ットマスク	255.255.255.0	
		IPv4デフォルトゲ-	ートウェイ	192.168.1.254	
		DNS	5サーバー1		
		DNS	らサーバー2		
		IPv6アドレス			
			自動設定	□ 有効	
		DHCPv6ク	ライアント	□ 有効	
		IPv	/6アドレス		
		プレフ・	ィックス長	0	(0 - 128)
		IPv6デフォルトゲー	ートウェイ		
		DNS	5サーバー1		
		DNS	らサーバー2		
		現在のステータス			
		IPv	/4アドレス	192.168.0.3	
		IPv4デフォルトゲー	ートウェイ	192.168.0.1	
		IPv	/6アドレス	::	
		IPv6デフォルトゲー	ートウェイ	:: 	
		0500-50	ルアドレス	Te80::3676:c5tt:tett:3a1f/64	
		適用			

項目	値
アドレスタイプ	スタティック
IPv4 アドレス	192.168.1.1
サブネットマスク	255.255.255.0
IPv4 デフォルトゲートウェイ	192.168.1.254

3-2 RADIUS サーバーの設定

認証サーバーの設定をします。設定画面より[RADIUS 認証]-[認証サーバー設定]を選択します。 認証サーバーテーブルの設定画面が表示されるので「追加」を選択します。

STP	>	入1 設
ループ検知	>	
LLDP	>	MACP
マルチキャスト	>	IPv472 IPv672
RADIUS認証	~	527
認証サーバー設定		
オーセンティケータ	設定 >	認証サーバーテーブル
EAPOL透過		All ▼ エントリを表示
ACL	>	■ 認証サーバーアドレス ポート番号 優先度 再送回数 タイムアウト
QoS	>	
		道加編集創開除

認証サーバーの追加画面が表示されるので必要項目を入力します。

認証サーバーを追加					
アドレスタイプ	 ○ ホストậ ● IPv4 ● IPv6 	名			
認証サーバーアドレス	192.168.1.2	2]		
ポート番号	1812] (0 - 65535, デフォル	ト 1812)	
優先度	1		(0 - 65535)		
認証キー	■ デフォル secret	レト値を使用]		
再送回数		レト値を使用	(1 - 10, デフォルト 3)	
カイレアウト	🕑 デフォノ	レト値を使用			
914791	3	項目		値	
適用 閉じる]	認証サール	バーアドレス	192.168.1.2	
	·	ポート番	号	1812	
		=刃=エ→		デフォルト値を使用:チ	エックなし
		ãØā∐+		secret	

Seliton®

設定画面より[RADIUS 認証]-[オーセンティケータ設定]-[プロパティ]を選択します。 ポートモードテーブルの設定画面が表示されるので「802.1x 認証」にチェックを付け適用します。 認証対象の端末を接続するポートを選択し、「編集」をクリックします。

ループ検知		liiit t								
LLDP	 19 38: 	92.1								
マルチキャスト		и								
RADIUS認証					002 175	ÐET				
認証サーバー設定	認証方法 認証方法									
オーセンティケータ設定、	定 MACアドレスフォーマット XXXXXXXXXX ▼									
プロパティ										
ポート設定	Ĺ	箇用								
	ポー	トモ	ードテー	ーブル						
EAPOL透過										
ACL										
QoS	_	No	ポート	認証	法	ホフトモード	盾失盾位			
				802.1X認証	MAC認証					
		1	GE1	無効	無効	マルチ認証	802.1X認証			
		2	GE2	無効	無効	マルチ認証	802.1X認証			
		3	GE3	無効	無効	マルチ認証	802.1X認証			
		4	GE4	無効	無効	マルチ認証	802.1X認証			
		5	GE5	無効	無効	マルチ認証	802.1X認証			
		6	GE6	無効	無効	マルチ認証	802.1X認証			
		7	GE7	無効	無効	マルチ認証	802.1X認証			
		8	GE8	無効	無効	マルチ認証	802.1X認証			
		(= #								

編集をクリックするとポートモードの編集画面が表示されるので、認証方法の「802.1x 認証」にチェックを付けます。優先順位の適用一覧に「802.1x 認証」が入っていることを確認し、適用します。

ポートモードを編集	ŧ			
ポート	GE7			
波江古社	@ 802.1X認	E		
BOPE/J/A				
ホストモード	 マルチ認識 シングルオ 	E tスト		
優先順位	候補一覧 MAC認証	適用一5 802.1X	2 認証 ▲ 高 → 但	抑重位
適用	閉じる			



設定画面より[RADIUS 認証]-[オーセンティケータ設定]-[ポート設定]を選択します。

LLDP			>	<u>192</u> . 追加	1								
マルチキャスト			>										
RADIUS認証													
認証サーバー設定	Ē												
オーセンティケー	一夕詞	安定											
プロパティ													
ポート設定]										
EAPOL透過	ポー	ト設が	ミテーフ	ブル									
ACI													
, IOE													
		No	#b	ポート4個	कञ्च	尽士まてし物		一般タイマー			802.1x	パラメーター	
	•	No.	ポート	术	再認証	最大ホスト数	再認証	ー般タイマー 非アクティブ	待機時間	TX期間	802.1x サプリカントタイムアウト	パラメーター サーバータイムアウト	最大リクエスト数
		No.	ポート GE1	ポート制御 無効	再認証	最大ホスト数 256	再認証 3600	ー般タイマー 非アクティブ 60	待機時間 60	TX期間 30	802.1x サプリカントタイムアウト 30	パラメーター サーバータイムアウト 30	最大リクエスト数 2
		No.	ポート GE1 GE2	ポート制御 無効 無効	再認証 無効	最大ホスト数 256 256	再認証 3600 3600	一般タイマー 非アクティブ 60	待機時間 60 60	TX期間 30 30	802.1x サプリカントタイムアウト 30 30	パラメーター サーバータイムアウト 30 30	最大リクエスト数 2 2
		No. 1 2 3	ポート GE1 GE2 GE3	ポート制御 無効 無効	再認証 無効 無効	最大ホスト数 256 256 256	再認証 3600 3600 3600	-般タイマー 非アクティブ 60 60	待機時間 60 60	TX期間 30 30 30	802.1x サプリカントタイムアウト 30 30 30	パラメーター サーバータイムアウト 30 30 30	最大リクエスト数 2 2 2
		No. 1 2 3 4	ポート GE1 GE2 GE3 GE4	ポート制御 無効 無効 無効	再認証 無効 無効 無効	<mark>最大ホスト数</mark> 256 256 256 256	中認証 3600 3600 3600 3600	- 般タイマー 非アクティブ 60 60 60 60	待機時間 60 60 60 60	TX期間 30 30 30 30	802.1x サブリカントタイムアウト 30 30 30	<mark>パラメーター</mark> サーバータイムアウト 30 30 30 30	最大リクエスト数 2 2 2 2 2
		No. 1 2 3 4 5	ポート GE1 GE2 GE3 GE4 GE5	ポート制御 無効 無効 無効 気効	再認証 無効 無効 無効 無効	最大ホスト数 256 256 256 256 256 256	月記記 3600 3600 3600 3600 3600	- 般タイマ 非アクティブ 60 60 60 60 60	符機時間 60 60 60 60 60	TX期間 30 30 30 30 30 30	802.1x サブリカントタイムアウト 30 30 30 30 30	<mark>パラメーター</mark> サーバータイムアウト 30 30 30 30 30 30	最大リクエスト数 2 2 2 2 2 2 2 2 2
		No. 1 1 2 3 4 5 6 7	ポート GE1 GE2 GE3 GE4 GE5 GE6 GE7	ポート44御 無効 無効 無効 気効 気効 の の の の の の の の の の の の の の の の	再認証 無効 無効 無効 無効 無効	最大ホスト数 256 256 256 256 256 256 256 256	1250 3600 3600 3600 3600 3600 3600	- 般タイマー 非アクティブ 60 60 60 60 60 60 60 60 60 60	待機時間 60 60 60 60 60 60 60 60	TX期間 30 30 30 30 30 30 30 30	802.1x サブリカントタイムアウト 30 30 30 30 30 30 30 30	<mark>パラメーター サーバータイムアウト</mark> 30 30 30 30 30 30 30	最大リクエスト数 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2
		No. 1 2 3 4 5 6 7 8	ポート GE1 GE2 GE3 GE4 GE5 GE6 GE7 GE8	ポート制御 無効 無効 無効 無効 無効 無効	再認証 無効 無効 無効 無効 無効 無効	最大木スト数 256 256 256 256 256 256 256 256 256 256	中記 3600 3600 3600 3600 3600 3600 3600 360	 一般タイマー 非アクティブ 60 60	待機時間 60 60 60 60 60 60 60 60 60 60	 エメ期間 30 30	802.1x サプリカントタイムアウト 30 30 30 30 30 30 30 30 30 30 30 30 30	<mark>パラメーター サーバータイムアウト</mark> 30 30 30 30 30 30 30 30 30 30 30 30	最大リクエスト数 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2

表示されるポート設定テーブルにて認証対象の端末を接続するポートを選択し、「編集」をクリック します。ポート設定の編集画面が表示されるので、ポート制御の「自動」を選択し適用します。

ポート	GE7	
ボート制御	 無効 強制的に認証する 強制的に認証しない 自動 	
再認証	□ 有効	
最大ホスト数	256	」 (1 - 256, デフォルト 256)
一般タイマー		
再認証	3600] 秒 (300 - 4294967294, デフォルト 3600)
非アクティブ	60] 秒 (60 - 65535, デフォルト 60)
待機時間	60] 秒 (0 - 65535, デフォルト 60)
802.1xパラメーター		
TX期間	30] 秒 (1 - 65535, デフォルト 30)
サプリカントタイムアウト	30] 秒 (1 - 65535, デフォルト 30)
サーバータイムアウト	30] 秒 (1 - 65535, デフォルト 30)
最大リクエスト数	2	(1 - 10, デフォルト 2)

以上で BSH-G08M の設定は完了です。



4. Windows 10 のクライアント設定

4-1 EAP-PEAP 認証

Windows 標準サプリカントで PEAP の設定を行います。

- ※ 本設定を行う前に「Wired AutoConfig」サービスが起動されていることをご確認下さい。
- [イーサネットのプロパティ]の [認証] タブから以下の設定を行います。



- サーバー証明書の検証をする

- Windows のログオン名と・・・

- 信頼されたルート認証機関

項目	値
認証モードを指定する	ユーザー認証

On

Off

TestCA

4-2 EAP-TLS 認証

4-2-1 クライアント証明書のインポート

PC にクライアント証明書をインポートします。ダウンロードしておいたクライアント証明書 (user01.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。

user01.p12	
← → 証明書のインボートウイザード	×
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 します。	トアにコピー
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 されたネットワーク発展を提供するための優報を含んでいます。証明書ストアは、証明書が保管さ 上の様域です。	Jティで保護 れるシステム
保存場所 ● 現在のユーザー(○) ○ ローカル コンドコーター(1)	
そうまるには、[次へ]をクリックしてください。	
	キャンセル
◆ 夢 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 インボートするコアイルを指定してくだちい。	
774/1.2.(F)	
C:WUsers¥solitonWDesktop¥user01.p12	₩(B)
注書: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 証明會 (.P7B)	
Microsoft シリアル化された証明書ストア (.SST)	
次へ(<u>N</u>)	キャンセル



\checkmark	
× ← <i>W</i> 証明豊のインボート ウイザード	
時度年-0月間 セキュリティを総持するために、私宅キーはバ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。	
/(スワード(P):	
□ パスワードの表示(D)	
- インボートオブション(I):	
□ 秘密モーの保護を強力にする(E) 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) キーのパックアップ 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)	
次へ(N) キャンセル	「2-4 ユーザーの登録」 で設定したバスワードを入力
×	
← ジジ 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 に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 証明書の憧憬に基づいて、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:	
参照(R)	
次へ(N) キャンセル	
×	
←	
証明書のインポートウィザードの完了	
[元了]をクリックすると、証明書がインホートされます。 この時間が低声されました。	
ベリビスをプロたとくなした 選択された証明者ストア ウイザードで自動的に決定されます 内錠 PFX	
ファイル名 Ci¥Users¥soliton¥Desktop¥user01.p12	
完了(F) キャンセル	

Seliton

4-2-2 サプリカント設定

Windows 標準サプリカントで TLS の設定を行います。

※ 本設定を行う前に「Wired AutoConfig」サービスが起動されていることをご確認下さい。

[イーサネットのプロパティ]の [認証] タブから以下の設定を行います。



証明書を検証してサーバーの ID を検証する

信頼されたルート証明機関

項目	値
認証モードを指定する	ユーザー認証

On

TestCA

5. 動作確認結果

5-1 EAP-PEAP 認証

EAP-PEAP 認証が成功した場合のログ表示例

製品名	ログ表示例	
NetAttest EPS	Login OK: [user01] (from client RadiusClient01 port 1 cli CC-30-80-32-8B-AF via proxy to virtual server)	
	Login OK: [user01] (from client RadiusClient01 port 1 cli CC-30-80-32-8B-AF)	
BSH-GM シリーズ/	802 1y authentication successful for client CC120,00122,0014E on CisabitEthernot7	
BSH-GP08	002.1X authentication succession of client CC.30.00.32.0B.AF of Gigabitethemet/	

5-2 EAP-TLS 認証

EAP-TLS 認証が成功した場合のログ表示例

製品名	ログ表示例	
NetAttest EPS	Login OK: [user01] (from client RadiusClient01 port 1 cli CC-30-80-32-8B-AF)	
BSH-GM シリーズ/	802.1x authentication successful for client CC:30:80:32:8B:AF on GigabitEthernet7	
BSH-GP08		

<u>Seliton</u>®

改訂履歴

日付	版	改訂内容
2018/10/31	1.0	初版作成
2019/03/19	2.0	ロゴ画像差し替え