



【連携機器】BUFFALO BS-GS2016 【Case】IEEE802.1X EAP-PEAP(MS-CHAP V2)/ EAP-TLS/EAP-TLS+ダイナミック VLAN 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、BUFFALO 社製 L2 スイッチ BS-GS2016 の IEEE802.1X EAP-PEAP(MS-CHAP V2)/EAP-TLS/EAP-TLS+ダイナミック VLAN 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。

アイコンについて

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
<u>.</u>	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 BS-GS2016 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。

1.構成

<mark>Seliton</mark> 目次

1 構成 2
1-1 構成図
1-2 環境
1-2-1 機器
1-2-2 認証方式
1-2-3 ネットワーク設定
2. NetAttest EPS の設定4
2-1 初期設定ウィザードの実行
2-2 システム初期設定ウィザードの実行5
2-3 サービス初期設定ウィザードの実行6
2-4 ユーザーの登録7
2-5 ユーザーのリプライアイテムの設定8
2-6 クライアント証明書の発行9
3. BS-GS2016の設定10
3-1 IP アドレスの設定11
3-2 VLAN の設定12
3-2-1 VLAN10 の作成12
3-2-2 VLAN20 の作成13
3-2-3 PVID の設定14
3-2-4 VLAN 1 を修正 14
3-3 RADIUS サーバーの設定15
3-3-1 RADIUS サーバーの IP アドレス設定
3-3-2 認証ポートの設定16
4. Windows 10 のクライアント設定17
4-1 EAP-PEAP 認証17
4-2 EAP-TLS 認証
4-2-1 クライアント証明書のインポート18
4-2-2 サプリカント設定 20
5. 動作確認結果
5-1 EAP-PEAP 認証21

<u>Seliton</u>



1-1 構成図

以下の環境を構成します。

- ・L3 スイッチには VLAN1、VLAN10、VLAN20 の 3 つの VLAN を作成する
- ・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
- ・各 VLAN の設計および用途は以下とする。
 - VLAN1 : 192.168.1.0/24 (EPS、D3、認証のみ/user03用)
 - VLAN10 : 192.168.10.0/24 (ダイナミック VLAN/user01 用)
- VLAN20 : 192.168.20.0/24 (ダイナミック VLAN/user02 用)



Seliton®

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	4.10.4
BS-GS2016	BUFFALO	RADIUS クライアント (L2 スイッチ)	1.0.3.43
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	4.2.17

1-2-2 認証方式

IEEE802.1X EAP-PEAP(MS-CHAP V2)/EAP-TLS/EAP-TLS+ダイナミック VLAN

1-2-3 ネットワーク設定

機器	IP アドレス RADIUS port (Authentica		RADIUS Secret (Key)
NetAttest EPS-ST05	192.168.1.2/24	1912	secret
BS-GS2016	192.168.10.1/24	UDF 1612	secret
Client PC	DHCP	-	-

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

Seliton

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

CARMENT			
CAMERINA	B-NGA M		
CAREEN			
• PRECEDUARS THE IS			
200005535	RSA 🛩		
REF.	2048 🛩		
● 3HB05Mデバイスの開始8			
₹.R0₩4.			
要求著名フルゴリズム	SHA296 🛩		
CA1166			
	TeetCA		
	日本	~	
初期用品書	Takya		
市区町村名	Shinjuku		
\$8.500B(5)	Soliton Systems		
878-8			
E-mat2PD-2			
CARGUT			





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

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。

NetAttest	EPS				(h-1-1-1	ページ 6 設定保存	ログオン中: admin
 naepsexample.com システム設定 システム管理 和目標明 		<u> こーザー 覧</u>	● 一部 ● 完全	グルーナ 💙	ユーザーまで 検索		
■ all-y No(K) ■ DHCPサーバー ■ LDAPサーバー ■ RADIUSサーバー ■ ユーザー ■ ユーザー ■ ユーザー ■ ユーザー			ĺ.	<u>ユーザーD</u>	品総認証成功日時	ザー削除時の証明 新田明書	道加
 ■ エクスポート ■ インポート ■ ユーザーバスワー ■ デフォルトユーザー ■ ゲスト 	ドボリシー ープロファイル		ser	1051 上一 編集対象	・ザー設定 :: 新規	£1T £ 9	
				ユーザ 基本情 女 E-Mai 詳細情	14種 チェックアイテム リナライアイ 使 し し 一 税 税 1 税 1 1 1 1 1 1 1 1 1 1 1 1 1	754 ОТР	
項目	値			認証情	版 一D use	vr01	
姓	user01	user02	user03			~	
ユーザーID	user01	user02	user03		叶 种贝相学 止		
パスワード	password	password	password			ОК ++	ンセル 道用
NetAttest	EPS				مخود با	▼-ジ) □ 読定保存	ログオン中: admin 10 ログオフ
 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 		ユーザー ユーザー 詳細 <u>オブションの設定</u> エクスポート	● 一部 ● 完全	ヴルーナ 💙	ユーザーまで 検索		道加
■ RADIUSサーバー ■ ユーザー ■ ユーザー一覧			ά.	<u>ユーザーID</u>	日本の日本の日本の日本の日本の日本の日本の日本の日本の日本の日本の日本の日本の日	ザー削除時の証明 証明書	<u>書失効オブション</u> タスク
■ エクスポート ■ インポート ■ ユーザーバフロー	-ドボリシー		ol	<u>test</u> <u>user01</u>		発行 変 到 発行 変 列	
■ デフォルトユーザ・ ■ ゲスト	ープロファイル						

2-5 ユーザーのリプライアイテムの設定

ダイナミック VLAN で接続先を制御したいユーザーにリプライアイテムを設定します。 対象のユーザーの「変更」ボタンよりユーザー設定画面に進み、「リプライアイテム」タブにて 「VLAN ID」と「タグ」を指定します。

Not Attact FPS	a de la companya de l			ログオン中: admin	
NetAllest LI O				パページ 😢 ログオフ	
■ naeps.example.com	🔰 ユーザーー覧				
■ システム設定 ■ システム管理	ユーザー • -	一部 🔍 完全 グループ 🔽	ユーザーまで 検索		
■ 証明機関	詳細オプションの設定				
■ DHCPサーバー	<u>エクスポート</u>			24 to	
■ EADIUSサーバー			<u>ユーザー削除</u>	<u>増加</u> 時の証明書失効オブション	
= ユーザー	■ 名前	<u>ユーザーID</u>	<u>最終認証成功</u> 日時 証明書	タスク	
■ ユーザー一覧 ■ エクフポート	test user			で更 削除	
■ エンスホート ■ インボート	user01	user01		西加除	
■ ユーザーバスワードポリシー		<u>useror</u>	7613	C	
			٩	♥	
Net Attest EPS				ログオン中: admin	
Nothitoot El O				プページ) 🕑 ログオフ)	
■ naeps.example.com	📃 🚨 ユーザー設定				
■ システム設定 ■ システム管理	編集対象: user01				
■ 証明機関	ユーザー情報 チェックアイテム リプライアイテム OTP				
■ DHCPサーバー	標準のリプライアイテム				
■ ELAPサーバー ■ RADIUSサーバー	SessionTimeout	1800			
■ ユーザー	VLAN ID	10	タグ 0		
■ ユーザー一覧 ■ エクコポート	Filter ID				
■ エジスホート ■ インポート	任意のリプライアイテム				
■ ユーザーバスワードボリシー	アトリピュー	ト オペレーター	値		
■ デフォルトユーザープロファイル = ゲフィ		選択 = 🗸	+ -		
■ クスト					
		ОК	キャンセル 適用		

項目	値			
ユーザーID	user01	user02	user03	
VLAN ID	10	20	-	
タグ	0	0	-	



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)

						da sere
NetAttest EPS						中: admi
E mane example com	~					1717
■ システム設定	ユーザ・	──覧				
 ■ システム管理 ■ 50日番切 	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	非細オフションの設 エクスポート	ĨĒ.				
■ LDAPサーバー					i i	追加
+ RALIUS リーバー = ユーザー		夕箭	ว – +f∽m		-ザー削除時の証明書失効オン 	<u> ジョン</u>
■ ユーザー一覧		test user	test	AVESSAND USP/11-14-1		1 18全
■ エクスホート ■ インポート		11serf)1				
■ ユーザーパスワードポリシー		ustivi	<u>ustror</u>			3.64
■ デフォルトユーザープロファイル ■ ゲスト						
					↓	
			編集対象: user01			
			基本情報			
			姓	userU1		
			To F. Mail			
			≣¥¥ÐI¶∰₽₽		0	
			認計報			
			ユーザーID	user01		
			有効期限 日数 365			
			●日付 2016 ♥	年 7 💙月 9 🌱 日 23 🕯	✔ 時 <mark>59 ♥</mark> 分 <mark>59 ♥</mark> 秒まで	
			パスワード			
18		値	パスワード(確認)			
		265	※パスワードが空間の場合に			
:明書有効期限		365	✓ PKCS#12ファイルに証明	明機関の証明書を含める		
KCS#12 ファイルに証明機関	の・・・	チェック有			発行 キャン1	セル
		@			• •	
		- 二一ザー証明	唐のタワンロード			
		ユーザー証明書ダウン	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	象をファイルに保存して	Fðu。 ダウンロー	۴



3. BS-GS2016の設定

BUFFALO 社製レイヤー2 スマートスイッチ BS-GS20 シリーズ(BS-GS20, BS-GS20P)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 BS-GS2016 を使用し、WebGUI から各種設定を実施する方法を紹介します。

購入時の BS-GS2016 は、IP アドレスが 192.168.1.254 に設定されています。端末に適切な IP アドレスを設定して Web ブラウザより管理画面にアクセスし、設定を開始します。 初期のユーザー名/パスワードは admin/password です。

ユーザー名	admin
パスワード	•••••
	ログイン

セットアップは以下の流れで行います。

- 1. IP アドレスの設定
- 2. VLAN の設定
- 3. RADIUS サーバーの設定

ここでは、

Port1,4をVLAN10

Port2 を VLAN20

に設定します。



3-1 IP アドレスの設定

トップページより[基本設定]-[VLAN]-[VLAN 設定]をクリックします。

<u>システム</u>
▼ 基本設定
システム情報設定
- VLAN
VLAN設定
VLAN#-ト
▶ルーティング
▶ SNMP
▶ LLDP
▶MACアドレス
▶ポート設定
▶システムセキュリティ
日付と時刻
▶詳細設定
▶管理

VLAN1を選択し、「編集」ボタンをクリックします。



以下の画面から IPv4 アドレス、デフォルトゲートウェイを設定します。

IPv4アドレス設定			
IPv4アドレス	192.168.10.1		1
サブネットマスク	255.255.255.0	項目	
デフォルトゲートウェイ	102 169 10 254	IPv 4アドレス	192.168.10.1
7 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7	192.108.10.254	デフォルトゲートウェイ	192.168.10.254

一番下にある「適用」ボタンをクリックします。

Untagged	All	\bigcirc	\bigcirc	۲	\bigcirc
Not Member	All	۲	۲	\bigcirc	۲
適用リセッ	۱ ‡+	ァンt	71		
	<u> </u>				
	Untagged Not Member 適用	Untagged All Not Member All 適用 リセット キャ	Untagged All ○ Not Member All ◎ 適用 リセット キャンt	Untagged All O O Not Member All O O	Untagged All ○ ○ ● Not Member All ● ● ○ 適用 リセット キャンセル

Seliton

3-2 VLANの設定

3-2-1 VLAN10の作成

[基本設定]-[VLAN]-[VLAN 設定]をクリックし VLAN の追加を行います。

「VLAN の追加/編集」の VLAN ID に「10」を入力し、VLAN 名に「VLAN10」を入力します。管理 VLAN の欄にチェックを入れます。

VLANの追加/編集			
VLAN ID	10 (2-4094)	項目	値
VLAN名	VLAN10	VLAN ID	10
管理VLAN		VLAN 名	VLAN10
		管理 VLAN	チェックあり

各ポートの設定を行います。

例:ポート1番と4番をUntaggedに選択。

ポート 10 番を Tagged に選択

最後に「適用」ボタンをクリックします。



Seliton

3-2-2 VLAN20の作成

[基本設定]-[VLAN]-[VLAN 設定]をクリックし、「VLAN の追加/編集」より VLAN20 の追加を行い ます。

VLANの追加/編集	
VLAN ID	20 (2-4094)
VLAN名	VLAN20
管理VLAN	

項目	値
VLAN ID	20
VLAN 名	VLAN20

各ポートの設定を行います。

例:ポート2番をUntagged に選択。

ポート 10 番を Tagged に選択

最後に「適用」ボタンをクリックします。

ポート		1	2	3	4	5	6	7	9	0	10	11	12	13	14	15	16
<u>М</u> -Т.		1	2	2	-	<u> </u>	0		•	3	10		12	13	14	15	10
Tagged		\bigcirc	۲	\bigcirc	\bigcirc	\bigcirc	\bigcirc	\bigcirc	۲								
Untagged	All	\bigcirc	۲	\bigcirc													
Not Member		۲	\bigcirc	۲	۲	۲	۲	۲	۲	۲	\bigcirc	۲	۲	۲	۲	۲	0

3. BS-GS2016 の設定

Seliton

3-2-3 PVID の設定

[基本設定]-[VLAN]-[VLAN ポート]をクリックし、各ポートの PVID を変更します。



項目	値
ポート 1 の PVID	10
ポート 2 の PVID	20
ポート3のPVID	1
ポート 4 の PVID	10

「適用」をクリックします。



Olucion All C C

3-2-4 VLAN1を修正 必要に応じて VLAN 1 を修正してください。[基本設定]-[VLAN]-[VLAN 設定]をクリックします。 「VLAN ステータス」の VLAN ID 1 を選択し、「編集」 ボタンをクリックします。

VLA	Nステータス	
	VLAN ID	IPv4アドレス
	1	192.168.10.1
	10	-
	20	-
	PVID	
	プロテクトポート	
T:Sta	atic Tagged U:Static	Untagged -:Not
編集	削除	

各ポートの設定を行って、最後に「適用」ボタンをクリックします。

ポート		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Tagged	All	\odot	\bigcirc	۲	\bigcirc	\bigcirc	\bigcirc	\bigcirc	\bigcirc	\bigcirc							
Untagged	All	\odot	\bigcirc	۲	\bigcirc	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲
Not Member									\bigcirc	\bigcirc	\bigcirc				\bigcirc	\bigcirc	

3-3 RADIUS サーバーの設定

Spliton

3-3-1 RADIUS サーバーの IP アドレス設定

[詳細設定]-[認証]-[RADIUS]をクリックし、認証サーバーを指定します。

認証サーバーIPv4 アドレスに EPS の IP アドレスを指定し、共通暗号化キーに EPS で設定した キー(シークレット)を入力します。

ダイナミック VLAN を行う場合は、詳細設定のダイナミック VLAN にチェックを入れます。 最後に「適用」ボタンをクリックし、設定を保存します。

システム ▶基本設定	RADIUS	
▼詳細設定 ▶OoS	プライマリー認証サーバー	
▶ セキュリティ	認証	☑有効
▼認証	認証サーバーIPv4アドレス	192.168.1.2
ステータス	認証サーバーポート	1812
	共有暗号化キー	[]
ポートトランク	セカンダリー認証サーバー	
トラフィック制御	認証	有效
ミラーリング	認証サーバーIPv4アドレス	1.1.1.1
> STP	認証サーバーポート	1812
MLD	共有暗号化丰一	
► ACL	詳細設定	
ループ防止機能	リセットタイマー	3600 秒
▶管理	拡張設定	■Accounting ■Termination-Action ▼ダイナミックVLAN
	適用	

項目	値
認証	有効
認証サーバーIPv4 アドレス	192.168.1.2
共通暗号化キー	secret
ダイナミック VLAN	有効

Seliton

3-3-2 認証ポートの設定

[詳細設定]-[認証]-[ポート認証]ページにて認証ポートを選択し、「適用」クリックします。

システム ▶基本設定	ポート認識	E															
 ¥ 詳細設定 > QoS 	[注意]トランク	ポー	トに	指定す	<u>t</u> nt	เกล	ポー	トも、	MA	יבא	11	ターた	が設定	され	τιι	るポ-	- ト(お
 セキュリティ ▼認証 	ポート	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
ステータス	802.1Xポート	1	1	1	1												
	802.1X MAC																
ボートトランク	MAC認証																
トラフィック制御 ミラーリング	適用																



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。



項目	値
認証モードを指定する	ユーザー認証

項目	値
接続のための認証方法	
- サーバー証明書の検証をする	On
- 信頼されたルート認証機関	TestCA
- Windows のログオン名と・・・	Off

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。





※ 証明書のインポート ウィザード ※ 証明書のインポート ウィザード RE#= の病気 セキュリティを推持す 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。 パスワード(P): ●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●
Wæ年-の保護 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。 パスワード(P): ●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●
kez ← 006個 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。 パスワード(P): ●●●●●●●●●●● 」パスワードの表示(D)
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): ●●●●●●●●●●●● □ パスワードの表示(D)
- パスワード(P): ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・
●●●●●●●● □ パスワードの表示(D)
 パスワードの表示(D)
インポートオブション(I):
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。
□ このイービュンスパート N 細にする(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
¥
☞ 証明書のインポート ウィザード
石松豊ストッ
証明書ストアは、証明書が保留されるシステム上の領域です。
Windows 「好明曲?」とであた動物に考切させみか、好明曲の後部を指示すスペンドできます

(● 虹内田の運用に登ついて、日都町に虹内田AF/を満れずな(0) ○ 証明音をすべて次のストアに配置する(P)
征明音入下?:
E ant the
次へ(N) キャンセル
¥
● 証明書のインポート ウィザード
証明書のインポートウィザードの完了
(完了)をクリックすると、証明書がインポートされます。
次の設定が確定されました。
湿沢された証明書ストア ウイザードで自動的に決定されます 内容 PFX
77代ル名 Ci¥Users¥soliton¥Desktop¥user01.p12

【パスワード】

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

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。

4-มหาวารายานี้ 1-มหาวารายานี้ 1-มหาวารายาน 1-มหาวารายานี้ 1-มหาวารายานี้ 1-มหาวารายานี้ 1-มหาวารายานี้ 1-มหาวารายานี้ 1-มหาวารายานี้ 1-มหาวารายานี้ 1-มหาวา 1-มหาวารายานี้ 1-มหาวารายานี้ 1-มหาวารายานี้ 1-มหาวารายานี้ 1-มหาวารายานี้ 1-มหาวารายานี้ 1-มหาวารายานี้ 1-มหาวา 1-มหาวารายานี้ 1-มหาวารายานี้ 1-มหาวารายานี้ 1-มหาวารายานี้ 1-มหาวารายานี้ 1-มหาวารายานี้ 1-มหาวารายานี้ 1-มหาวา 1-มหาวารายานี้ 1-มหาวารายานี้ 1-มหาวารายานี้ 1-มหาวารายานี้ 1-มหาวารายานี้ 1-มหาวารายานี้ 1-มหาวารายานี้ 1-มหาว 1-มหาวารายานี้ 1-มหาวารายานี้ 1-มหาวารายานี้ 1-มหาวารายานี้ 1-มหาวารายานี้ 1-มหาวารายานี้ 1-มหาวารายานี้ 1-มหาวารายานี้ 1-มหาวารายานี้ 1-มหาวารายานี้ 1-มหาว 1-มหาวารายานี้ 1-มหาวารายานี้ 1-มหาวารายานี้ 1-มหาวารายานี้ 1-มหาวารา 1-มหาวารายานี้ 1-มหาวารายานี้ 1-มหาวารายานี้ 1-มหาวารายานี้ 1-มหาวารายานี้ 1-มหาวารายานี้ 1-มหาวารายานี้ 1-มหาว 1-มหาวารายานี้ 1-มหาวารายานี้ 1-มหาวารายานี้ 1-มหาวารายานี้ 1-มหาวารายานี้ 1-มหาวารายานี้ 1-มหาวารายานี้ 1-มหาว 1-มหาวารายานี้ 1-มหาวารายานี้ 1-มหาวารายานี้ 1-มหาวารายานี้ 1-มหาวารายานี้ 1-มหาวารายานี้ 1-มหาวารา 1-มหาวารายานี้ 1-มหาวารายานี้ 1-มหาวารายานี้ 1-มหาวารายานี้ 1-มหาวารา 1-มหาวารายานี้ 1-มหาวารายานี้ 1-มหาวารายานี้ 1-มหาวารายานี้ 1-มหาวารายานี้ 1-มหาวารายานี้ 1-มหาวารายานี้ 1-มหาวา		
ネットワーク 認証 共有		
このイーサネット アダブターに認証済みのネットワーク アクセスを提供するに は、このオブションを選択してください。	項目	
☑ IEEE 802.1X 認証を有効にする(N)	TFFF 802.1X 認証を	
ネットワークの認証方法の選択(M):	有効	
Microsoft:スマートカードまたはその他の証明書 〜 設定(S) 🔵	1月20169 つ	
	Microsoft:ス ⁻ ネットワークの認証方式の選択	マートカード
□ ロクオンするたひに、この接続用の資格情報を使用する(R)	またはその他	の証明書
□ 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)		
違加の設定(D)	スマートカードまたはその他の証明書のプロパティ × 接続のための認証方法:	
	 ○ 目分のスマートカードを使う(5) ○ このコンピューターの証明書を使う(C) ○ 単純な証明書の違択を使う(推奨)(M) ○ 証明書を検証してサーバーの ID を検証する(V) 	
UK TTZEN	□ 次のサーバーに接続する (例: srv1、srv2、.*¥.srv3¥.com)(O):	
÷		
詳細設定 802.1X の設定 802.11 の設定 ② 認証モーを指定する(P): <u>ーザー認証</u> 」「「」」「一切一記」」」」」」」」」」 ③ マイてのユーザーの資格情報を削除する(D) □ このネットワークに対するシングル サインオンを有効にする(S) ③ ユーザー ログオンの直前に実行する(F) ③ ユーザー ログオンの直範に実行する(F) ○ スーザー ログオンの直範に実行する(F) ○ スーザー ログオンの直範に実行する(F) ○ スーザー ログオンの直範に実行する(F) ○ スーゲールグスクロビック表示を許可する(L) ○ このネットワーケでは、コンビューターとユーザーの認証に別の仮想 LAN を使用する(V)	個親されたルート証明機関(R): Microsoft Root Certificate Authority 2010 Microsoft Root Certificate Authority 2011 ✓ TestCA thawte Primary Root CA Thawte Timestamping CA UTN - DATACOP SGC UTN - DATACOP SGC VeriSign Class 3 Public Primary Certification Authority - GS Coll Coll Coll Coll Coll Coll Coll Coll	
	項目	値
 OK キャンヤル	接続のための認証方法	
	- このコンピューターの証明書を使う	On
	- 単純な証明書の選択を使う(推奨)	On

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

On

TestCA

項目	値
認証モードを指定する	ユーザー認証

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: [user03] (from client RadiusClient01 port 1 cli CC-30-80-32-8B-AF via proxy to
NetAllest LI 5	Login OK: [user03] (from client RadiusClient01 port 1 cli CC-30-80-32-8B-AF)
BS-GS2016	Port authentication is passed on port 1

BS-GS2016の設定画面でも確認ができます。

[詳細設定]-[認証]-[ステータス]の画面で「認証済み」と表示されていれば認証成功です。

認証状態					
ポート	認証設定	認証状態			
1	802.1Xポート	認証済み			
2	802.1Xポート	無効			
3	802.1Xポート	無効			
4	802.1Xポート	無効			

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: [user03] (from client RadiusClient01 port 1 cli CC-30-80-32-8B-AF)
BS-GS2016	Port authentication is passed on port 1

BS-GS2016の設定画面でも確認ができます。

[詳細設定]-[認証]-[ステータス]の画面で「認証済み」と表示されていれば認証成功です。

認証状態					
ポート	認証設定	認証状態			
1	802.1Xポート	認証済み			
2	802.1Xポート	無効			
3	802.1Xポート	無効			
4	802.1Xポート	無効			



5-3 EAP-TLS+ダイナミック VLAN 認証

EAP-TLS 認証+ダイナミック VLAN 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)								
BS-GS2016	Port authentication is passed on port 3								

ダイナミック VLAN が成功した場合の BS-GS2016 の VLAN 割当状態の表示例

[基本設定]-[VLAN]-[VLAN 設定]を参照



VLAN10 が割り当てられた場合

VL	ANステータス																																		
	VLAN ID	IPv4アドレス	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	VLA	名	管理	VLAN	a												
	1	192.168.10.1	-	-	U		U	U	U	U	U	U	U	U	U	U	U	U			τ	Up													
	10		U	-	÷	U	-	÷	-	÷	÷	т	÷	-	-	-	-	÷	VLN/	A10	τ	Up													
	20	-	-	U		-	-	-	-	-	-	т	-	-	-	-	-	-	VLA	N20	D	own													
	PVID		10	20	1	10	1	1	1	1	1	1	1	1	1	1	1	1																	
	プロテクトポート		-	-	F	-	-	-	-	-	-	-	-	-	-	-	-	-																	
T:S	tatic Tagged U:Static	: Untagged -:No	et Men	nber	3:有	効				VI	AN	ステ	-9	ג																					
編集	_集 削除				L					E			.AN	D		IPv4	アドレ	ス		2 3	4						10			13	14			VLAN名	管理VLAN
					T					E	1		1			192.	168.1	0.1			•	U	U	U	U	U	U	U	U	U	U	U	U		Up
					L				-	E)		10						U I	• •	U	J -	-	-	-	-	Т	-	-	-	-	÷	-	VLNA10	Up
										E	1		20				-		- 1	JU		-	-	-	-	-	Т	•	-	-	-	-	-	VLAN20	Down
												I	PVIE)					10 2	0 20	10	0 1	1	1	1	1	1	1	1	1	1	1	1		
											7	'D₹	クト	ポー	ト				-	•		-	-	-	-	-	-	-	-	-	-	-	-		
										T	Stati	: Tagį	ged	U:Sta	tic U	Jntag	ged	-:Not	Memb	er X:	有効														
										Ņ	集	削除																							

VLAN20 が割り当てられた場合

BS-GS2016 の設定画面でも確認ができます。

[詳細設定]-[認証]-[ステータス]の画面で「動的 VLAN」と表示されていれば認証成功です。

認証状態									
ポート	認証設定	認証状態							
1	802.1Xポート	無効							
2	802.1Xポート	無効							
3	802.1Xポート	動的VLAN							
4	802.1Xポート	無効							

Seliton 付録 L3 スイッチの設定

ポート設定、DHCP リレー設定

下記のようにポートの設定をします。

ポート	VLAN ID	ネットワーク	スイッチ IP アドレス	備考
1-5	1	192.168.1.0/255.255.255.0	192.168.1.254	
6-9	10	192.168.10.0/255.255.255.0	192.168.10.254	
10	10.20			VLAN10とVLAN20の
10	10,20			トランクポート
11-14	20	192.168.20.0/255.255.255.0	192.168.20.254	

DHCP リレー設定にて、「192.168.1.3」を指定します。



改訂履歴

日付	版	改訂内容
2019/02/04	1.0	初版作成
2019/03/19	2.0	ロゴ画像差し替え