



【連携機器】BUFFALO WAPM-1166D 【Case】IEEE802.1x EAP-TLS, EAP-PEAP(MS-CHAPv2)認証

Rev1.0

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 CA 内蔵 RADIUS サーバーアプライアンス NetAttest EPS と BUFFALO 社製無線アクセス ポイント WAPM-1166D の IEEE802.1x EAP-TLS, EAP-PEAP(MS-CHAPv2)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
•	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、
<u>.</u>	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 WAPM-1166D 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
1-1 構成図5
1-2 環境6
1-1-1 機器6
1-1-2 認証方式6
1-1-3 ネットワーク設定6
2. NetAttest EPS の設定7
2-1 システム初期設定ウィザードの実行7
2-2 システム初期設定ウィザードの実行8
2-3 サービス初期設定ウィザードの実行9
2-4 ユーザーの登録10
2-5 クライアント証明書の発行11
3. BUFFALO WAPM-1166D12
3-1 BUFFALO WAPM-1166D 設定の流れ12
3-1-1 RADIUS サーバーの登録 13
3-1-2 無線基本設定 14
3-1-3 無線セキュリティー設定 15
4. EAP-TLS 認証でのクライアント設定16
4-1 Windows 8.1 での EAP-TLS 認証16
4-1-1 デジタル証明書のインポート16
4-2 iOS (iPad)での EAP-TLS 認証19
4-2-1 デジタル証明書のインポート19
4-3 Android (Galaxy S5)での EAP-TLS 認証
4-3-1 デジタル証明書のインポート
4-3-2 サプリカント設定 22
5. EAP-PEAP 認証でのクライアント設定23
5-1 Windows 8.1 のサプリカント設定
5-2 iOS のサプリカント設定 24
5-3 Android のサプリカント設定25

<mark>Seliton</mark> 構成

1-1 構成図

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。

- 有線 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-ST04 の DHCP サーバーから払い出す



環境

1-1-1機器

製品名	メーカー	役割	バージョン
NetAttest EPS-ST04	Soliton Systems	RADIUS/CA サーバー	Ver. 4.8.1
WAPM-1166D	BUFFALO	RADIUS クライアント	Ver. 1.2.7
Surface Pro	Microsoft	Client PC (802.1x クライアント)	Windows 8.1 64bit Windows 標準サプリカント
iPad	Apple	Client Tablet (802.1x クライアント)	Ver. 8.0.2
Galaxy S5 Google		Client Phone (802.1x クライアント)	Ver. 5.0

1-1-2 認証方式

IEEE802.1x EAP-TLS 認証, IEEE802.1x EAP-MS-PEAP 認証

1-1-3 ネットワーク設定

	IP アドレス	RADIUS port (Authentication)	RADIUS Secret (Key)
NetAttest EPS-ST04	192.168.1.2/24	1912	secret
WAPM-1166D	192.168.1.1/24	0DF 1612	secret
Client PC	DHCP	-	-
Client Tablet	DHCP	-	-
Client Phone	DHCP	-	-

NetAttest EPS の設定

2-1 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、インターネットエクスプロー ラーから「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、インターネットエクスプロー ラーから「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.local
IP アドレス	デフォルト
ライセンス	なし

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

CANNER		
CANDERIN	л–нса ♥	
CANCER		
● 内部で新しい鍵を生成する		
公開鍵方式	RSA 🛩	
10.K	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		
	TestCA]
	日本	×
都通府県名	Tekyo	
市区町村名	Shinjuku	
会社名(組織名)	Soliton Systems	
部署名		
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
EAP 認証タイプ	
1	TLS
2	PEAP

	RadiusClient01	
🖬 このNAS/RADIUSクライアント	を有効にする	
	● NAS/RADIUSクライアント ● NASのみ ● RADIUSクライアントのみ	
1993		$\hat{}$
	192.168.1.1	
NAS\$\$\$10		
	原山	次 へ

項目	値
NAS/RADIUS クライアント名	RadiusClient
IP アドレス	192.168.1.1
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。

	1 550				ログオン中: admin
NetAttes	st EPS			(1) トップページ) 🕒 設定(森 🖲 ログオフ)
naeps.local		💄 ユーザー一覧			
■ システム設定 ■ システム管理		フー#C	完全 万山,寸 ▼	コーザーまで 検索	
■ 証明機関		14 り 詳細オブションの設定			
■ DHCPサーバー ■ I DAPサーバー		<u>エクスポート</u>			
■ RADIUSサーバ				<u>ユーザー削除時の言</u>	明書失効オブョン
■ ユーザー	1	名前	<u>ユーザーID</u>	最終認証成功 日時証明書	タスク
■ エクスポート	,	test user	test	発行	変更 削 :
■ インボート ■ フ ー ザーパフ	ロニビポルシー				
■エーケーバス ■デフォルトユー	・ブードホッシー -ザーブロファイル				
			ユーザー情報 チ 基本情報		
			姓	user01	
			名		
			E-Mani ≣¥án⊀≾öR		^
	項目	値	認正情報		<u> </u>
	<u>t</u>	user01	ユーザーID*	user01	
			バスワード・	••••••	
	ユーサーID	user01	■ 一時利用停止		
	パスワード	password			
				ОК	キャンセル 道用
				*	
Not Atta	t EDC	保存されていたい部ウナナリー	データがあります!		ログオン中: admin
NetAttes	Stero)	MITCHLUS PAUEDEA/LIA	1 200026.9 1	1 トップページ 🇅 設定	森 📵 ログオフ
■ naeps.local		💄 ユーザー一覧			
■システム設定 ■システム管理				フーザーまで 検索	
■ 証明機関					
■ DHCPサーバー		エクスポート			
■ RADIUSサーバ				ユーザー削除時の調	追加 神書失効オプション
■ユーザー	_		<u>ユーザーID</u>	最終認証成功	タスク
■ ユーサーー覧 ■ エクスポート	Ĺ	test user	test		変更 削除
■インポート			user()1		変 面
■ ユーザーパス	ワードポリシー	userv1		9 87	<u>灵史</u> 刑际



2-5 クライアント証明書の発行

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_02.p12 という名前で保存)



Seliton BUFFALO WAPM-1166D

3-1 BUFFALO WAPM-1166D 設定の流れ

BUFFALO 社製無線アクセスポイント WAPM-1166D を設定するためには、専用の設定・管理ツール「AirStation Admin Tools」やシリアルコンソールを利用する方法、管理 WebGUI を利用する方法 法などが存在しますが、本書では、管理 WebGUI から各種設定を実施する方法を紹介します。

設定の流れ

- 1. RADIUS サーバーの登録
- 2. 無線基本設定
- 3. 無線セキュリティー設定



3-1-1 RADIUS サーバーの登録

RADIUS サーバーの設定をします。

TOP ページの [詳細設定] リンクをクリックします。 [無線設定] メニューを展開し、 [RADIUS] リンクをクリックします。右側に RADIUS 設定項目が表示されますので、プライマリーサーバーの 項目に値を入力します。

3	11401	設定	システム情報	Log Out	
5°	- 7		₩ 10	2	
BUFFALO	R/DIUS 設	定			
disStation Dec	7				
C Home C Log Out	RADIUSサーバ	-(11g)			
WAPM-1166D			ブライマリーRADI	USサーバー	
い設備設定	- サーバー	〇内蔵RADIUS+	ナーバー ® 外部RADIUSサー	11-	
▲ 無線セキュリティー	RADIUSサーバー	192.168.1.2			
	認証ポート	1812			
L wds	Shared Secret				
RADIUS	Session Timeout	3600	þ		
HADIUS BR	Accounting	●有効 ○無効			
- 内裁RADIUSサーバー	Accountingボート	1813			-
し ユーザー教理			セカンダリーRAD	USサーバー	
MACマクセス制度	サーバー	○ 内蔵RADIUS*	ナーバー ® 外部RADIUSサー	11-	
WMM	RADIUS				
無線環境干二ター	1211年末一下	1812			
スケジュール	Shared Secret	-			
▼ 你把给宝	Session Timeout	3600 \$	•		
T IS TRACE	Accounting	◎ 有効 ○ 無効			
本体パスワード	Accountingボート	1813			
<u>時刻設定</u> 口付け現在送(andor)	RADIUS	-(11a)			
Relation Tople		1.000			
設定保存健元	#-15-	O data paper 10+	項目	値	
西起動	RADIUS# -15-	192.168.1.2			
設定初期化	認識ポート	1812		۲ 102 169 1 2	
ファームウェア更新	Shared Secret		KAD105 9-7	192.108.1.2	
1 P 10 25	chared Secret		=≂ ===================================	1010	
				1012	
			Shared secre	t secret	
				1	



3-1-2 無線基本設定

無線 LAN 端末が接続する無線ネットワークの名前を設定します。 左側のメニューから [無線設定] を展開し、802.11gの [無線基本] リンクをクリックします。 右側の無線基本(11g)にて設定します。

	Anne de de Halle - La cata a la		
BUFFALU	無線基本 (11g)		_
AirStation P_{ro}	無線LAN	● 有効 ○ 無効	٦
e Home e Los Out	無線モード	11b/g/n ▼	
WAPM-1166D	有効 SSID#	1.*	
	* # SS	ID VLANモード VLAN ID 治がIVLAN ID	
▼ ネットワーク設定	1 Soliton-BUFFA	LO_TEST_G Untagged 1	
Proxy ARP	オートチャンクル	(++++ = = =+++	
<u> ブリッジ</u>	チャンネル	Ch1 .	
Link Integrity	チャンネルモード	20 MHz	
▼ 無線設定	BSS BasicRateSet	1.2.5.11 Mbps	
WPS	Multicast Rate	Auto	
802. Vig			
└─ 無錢基本		設定 キャンセ	IL
→ 詳細造定			
▲ 無線セキュリティー			
2ライアントモニター			
L WDS			
802.11a			
- 無線基本			
▶ 詳細設定			
▲ 無線セキュリティー			
L クライアントモニター			
LA WDS			
RADIUS			
LA RADIUS 設定			

項目	値
無線 LAN	有効にチェック
SSID	Soliton-BUFFALO_TEST_G

i

3-1-3 無線セキュリティー設定

「無線セキュリティー設定」では、認証方法と無線の暗号化方式を設定します。 左側のメニューから [無線設定] を選択し、802.11gの [無線セキュリティー] をクリックします。 右側の無線セキュリティー(11g)にて設定します。

BUFFALO	無線セキュリティー (11g)			
lirStation P_{ro}	SSID	Soliton-BUFFALO_TES	T_G ▼	
Home CLog Out	VLAN設定	VLANE-F Untagged •	VLAN ID	追加VLAN ID
<u>ネットワーク設定</u>	次の場合に有効にする	通常時と緊急時 ▼		
Proxy ARP	ANY接続	有効 ▼		
ブリッジ	ブライバシーセパレーター	使用しない ・		
Link Integrity	ロードバランス(同時接続台数制限)	100 /100		
「 無線設定	初起在去	140A 540		
WPS	agair カメ、	WPA-EAP *		
802.11g	WFAシリン 暗号化方式	MFA2-EAF		
- 無読基本	土工商新用服用	AL3 .		
山計測設定	Management Frame Protection			
→ 無路をキュリティー	iehniter	流の	•	
クライアンナチニター	Jar Jones Ser	120105051-01117-851		
L WDS				設定キャンセノ
802.11a		тар		店
▲ <u>無猿並本</u>		現日		16
→ 詳細設定		詞をす		
無機をキュリティー				WFA-LAF
<u>クラ-イアントモニター</u>		WPA タイプ		WPA2-EAP
RADIUS		暗号化方式		AES
In the object				追加認証を行わない

NetAttest EPS による RADIUS 認証を行うためには、「EAP」がついている方式を選択します。 また、選択した認証方式により設定可能な [無線の暗号化] も決定されます。

<mark>S₂liton</mark> EAP-TLS 認証でのクライアント設定

4-1 Windows 8.1 での EAP-TLS 認証

4-1-1 デジタル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_02.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_02.p12	
 ご 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、および証明書先効リストをディスクから証明書ストアにコピー します。 証明倫欄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 課されたキットフーが競売を提供するための情報を含んています。証明書ストアは、証明書が保留されるシス テム上の参考です。	
保存場所 ● 現在のユーザー(C) ○ ローカル コンピューター(L)	
ズへ(N) キャンセル	
▲ 正明書のインボート ウィザード ● 季 証明書のインボート ウィザード ● 読む日本の意識	
 NORT COLOR ALL AND COMMENT OF COMMENT. 	【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フ

J,
€ 参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。
 ・ ・ ・
 証明書ストア:
参照(R)
ガス (N) まや^オフリー
● 参証明書のインポート ウィザード
証明書のインボート ウィザードの完了
[完了]をクリックすると、証明書がインボートされます。
次の設定が指定されました。
□ 3.000kk201日にといいといい。 □ 3.000k201日によります。 □ 3.000k201日によります。
内容 PFX アイル名 C:¥Users¥soliton¥AppData¥Local¥Microsoft¥Windows¥INetCach
٢



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。

※本項では TLS の設定のみを記載します。その他の認証方式の設定に関しては付録を

ご参照ください。

[ワイヤレスネットワークのプロパティ]の[セキュリティ]タブから以下の設定を行います。



4-2 iOS (iPad)での EAP-TLS 認証

4-2-1 デジタル証明書のインポート

NetAttest EPS から発行したデジタル証明書を iOS デバイスにインポートする方法として、 下記の方法などがあります。

1) Mac OS を利用して Apple Configurator を使う方法

2) デジタル証明書をメールに添付し iOS デバイスに送り、インポートする方法

3) SCEP で取得する方法 (NetAttest EPS-ap を利用できます)

いずれかの方法で CA 証明書とクライアント証明書をインポートします。本書では割愛します。



サプリカント設定

WAPM-1166D で設定した SSID をタップし、サプリカントの設定を行います。 ※本項では TLS の設定のみを記載します。その他の認証方式の設定に関しては付録を ご参照ください。

まず、「ユーザー名」には証明書を発行したユーザーアカウントの ID を入力します。次に「モード」 より「EAP-TLS」を選択します。その後、「ユーザー名」の下の「ID」よりインポートされたユーザ ー証明書を選択します。





4-3 Android (Galaxy S5)での EAP-TLS 認証

4-3-1 デジタル証明書のインポート

NetAttest EPS から発行したデジタル証明書を Android デバイスにインポートする方法として、 下記 3 つの方法等があります。いずれかの方法で CA 証明書とユーザー証明書をインポートします。 手順については、本書では割愛します。

- 1) SD カードにデジタル証明書を保存し、インポートする方法※1
- 2) デジタル証明書をメールに添付し Android デバイスに送り、インポートする方法※2
- 3) SCEP で取得する方法 (NetAttest EPS-ap を利用できます)※3

※1 メーカーや OS バージョンにより、インポート方法が異なる場合があります。事前にご検証ください。

※2 メーカーや OS バージョン、メーラーにより、インポートできない場合があります。事前にご検証ください。

※3 メーカーや OS バージョンにより、Soliton KeyManager が正常に動作しない場合があります。事前にご検証ください。

Android 5.0 では証明書インポート時に用途別に証明書ストアが選択できますが、本書では無線 LAN 接続を行うため「Wi-Fi」を選択しています。





4-3-2 サプリカント設定

WAPM-1166D で設定した SSID をタップし、サプリカントの設定を行います。

※本項では TLS の設定のみを記載します。その他の認証方式の設定に関しては付録を ご参照ください。

「ID」には証明書を発行したユーザーアカウントの ID を入力します。CA 証明書とユーザー証明書は、インポートした証明書を選択して下さい。



項目	値
セキュリティ	802.1X EAP
EAP 方式	TLS
CA 証明書	user01_02
ユーザー証明書	user01_02
ID	user01

<mark>S≎liton</mark> EAP-PEAP 認証でのクライアント設定

5-1 Windows 8.1 のサプリカント設定

[ワイヤレスネットワークのプロパティ]の[セキュリティ]タブから以下の設定を行います。





5-2 iOS のサプリカント設定

WAPM-1166D で設定した SSID をタップし、サプリカントの設定を行います。

「ユーザー名」、「パスワード」 には"2-4 ユーザー登録" で設定したユーザーID、 パスワードを入力してください。



項目	値
ユーザー名	user01
パスワード	password
モード	自動



5-3 Android のサプリカント設定

WAPM-1166D で設定した SSID をタップし、サプリカントの設定を行います。

「ユーザー名」、「パスワード」 には"2-4 ユーザー登録"で設定したユーザーID、パスワードを入力し てください。「CA 証明書」には、インポートした CA 証明書を選択してください。



改訂履歴

日付	版	改訂内容
2015/09/30	1.0	初版作成