



# Account@Adapter + 認証連携設定例

**HCNET** エイチ・シー・ネットワークス株式会社

**BUFFALO**™

(2023/5/17 作成)

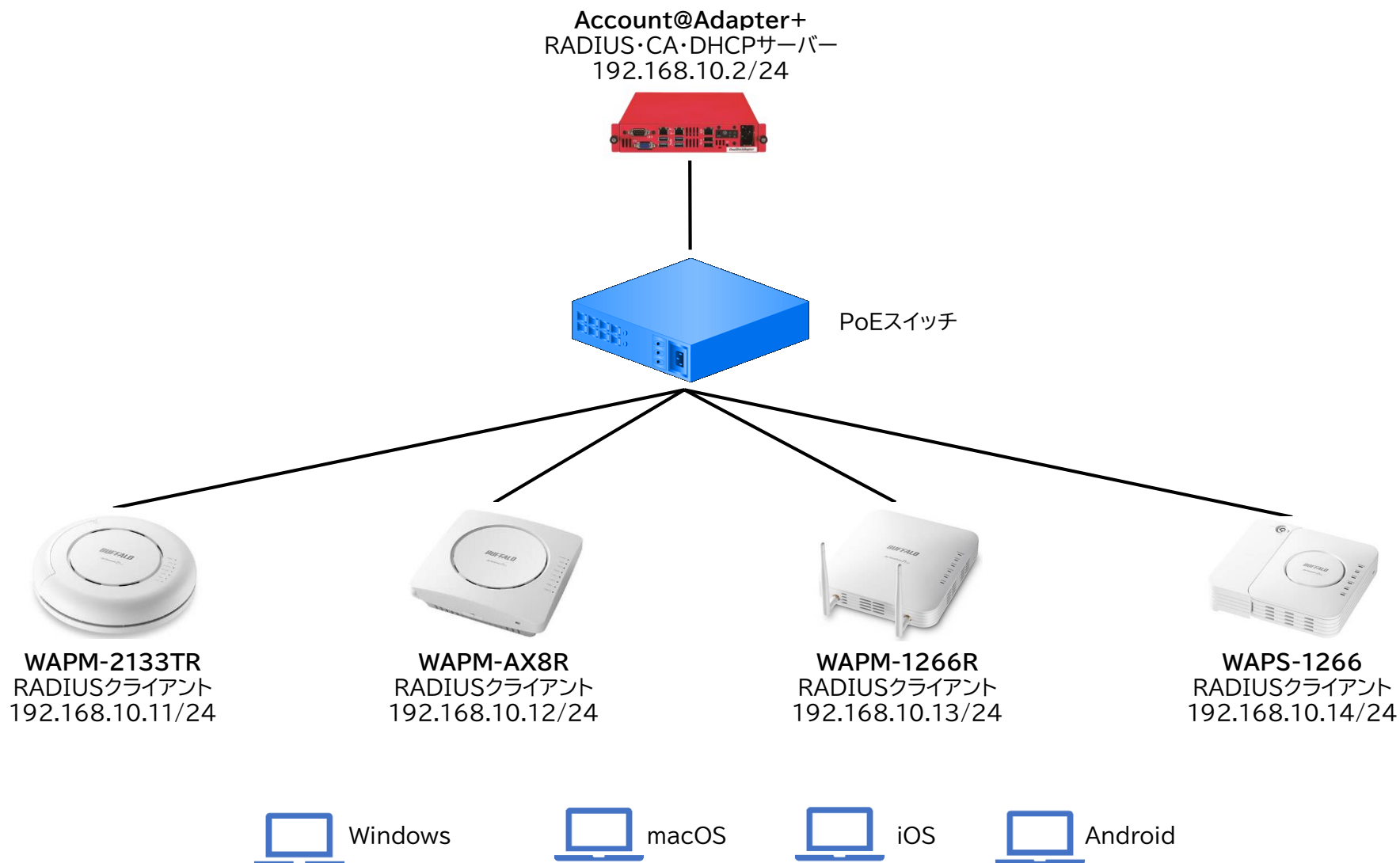
- ▶ 本資料では、RADIUS認証アプライアンス Account@Adapter+ と、バッファロー社製アクセスポイント WAPM-2133TR/WAPM-AX8R/WAPM-1266R/WAPS-1266 のIEEE802.1X EAP-TLS および EAP-PEAP 環境での接続に関する設定について説明します。
- ▶ 設定例ではバッファロー社製無線アクセスポイント WAPM-2133TR/WAPM-AX8R/WAPM-1266R/WAPS-1266 のWi-Fi機能のための基本設定が完了していることを前提とし、IEEE802.1X EAP-TLS および EAP-PEAP に必要な設定のみを説明します。
- ▶ 本資料は、現時点の最新バージョン(Ver.6.18.00)の仕様に従って記述したものになります。使用している画面等は、環境により表示される内容に若干の差異が発生する場合がありますのでご注意ください。
- ▶ 本資料は、当社での検証に基づき、RADIUS認証アプライアンス Account@Adapter+ およびバッファロー社製アクセスポイント WAPM-2133TR/WAPM-AX8R/WAPM-1266R/WAPS-1266 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のでご注意ください。

1. 構成
  - 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. Account@Adapter+の設定
  - 2-1 管理画面へのアクセス
  - 2-2 ネットワーク設定
  - 2-3 CA設定
  - 2-4 RADIUS設定
    - 2-4-1 RADIUS設定
    - 2-4-2 RADIUSクライアント登録
  - 2-5 アカウント登録
    - 2-5-1 EAP-TLS認証用 証明書アカウント登録
    - 2-5-2 EAP-PEAP認証用 ユーザーアカウント登録
  - 2-6 DHCP設定
    - 2-6-1 サーバグループ設定
    - 2-6-2 スコープ設定
  - 2-7 証明書発行/ダウンロード
    - 2-7-1 EAP-TLS認証用 クライアント証明書発行/ダウンロード
    - 2-7-2 EAP-PEAP認証用 CA証明書ダウンロード
3. RADIUSクライアントの設定
  - 3-1 管理画面へのアクセス
  - 3-2 IPアドレス設定
  - 3-3 RADIUS設定
  - 3-4 SSID設定
4. EAP-TLS認証でのクライアント設定
  - 4-1 Windows 11でのEAP-TLS認証
  - 4-2 macOSでのEAP-TLS認証
  - 4-3 iOSでのEAP-TLS認証
  - 4-4 AndroidでのEAP-TLS認証
5. EAP-PEAP認証でのクライアント設定
  - 5-1 Windows 11でのEAP-PEAP認証
  - 5-2 macOSでのEAP-PEAP認証
  - 5-3 iOSでのEAP-PEAP認証
  - 5-4 AndroidでのEAP-PEAP認証

# 1. 構成



- ▶ 以下の環境を構成します。



## ▶ 1-2-1 機器

製品名	メーカー	役割	バージョン
Account@Adapter+	エイチ・シー・ネットワークス	RADIUSサーバー DHCPサーバー CA	6.18.00
WAPM-2133TR	バッファロー	RADIUSクライアント	1.27
WAPM-AX8R	バッファロー	RADIUSクライアント	1.27
WAPM-1266R	バッファロー	RADIUSクライアント	1.28
WAPS-1266	バッファロー	RADIUSクライアント	1.27
ThinkPad X13 Yoga Gen 1	Lenovo	802.1Xクライアント端末	Windows 11 Pro 22H2
MacBook Air	Apple	802.1Xクライアント端末	macOS Ventura バージョン13.2.1
iPad	Apple	802.1Xクライアント端末	16.3.1
Lenovo Tab K10	Lenovo	802.1Xクライアント端末	Android11

※動作検証を行った時点の製品やOSのバージョンを記載しています。

※製品やOSを実際にご利用いただく際には脆弱性などの問題が対策されたバージョンを選定いただくようにしてください。

- ▶ 1-2-2 認証方式
- ▶ 以下の認証方式について、検証を実施しました。
  - ▶ IEEE802.1X EAP-TLS
  - ▶ IEEE802.1X EAP-PEAP

## ▶ 1-2-3 ネットワーク設定

製品名	IPアドレス	RADIUSポート	シークレットキー
Account@Adapter+	192.168.10.2/24	1812	buffalo
WAPM-2133TR	192.168.10.11/24	1812	buffalo
WAPM-AX8R	192.168.10.12/24	1812	buffalo
WAPM-1266R	192.168.10.13/24	1812	buffalo
WAPS-1266	192.168.10.14/24	1812	buffalo
ThinkPad X13 Yoga Gen 1	DHCP	-	-
MacBook Air	DHCP	-	-
iPad	DHCP	-	-
Lenovo Tab K10	DHCP	-	-



## 2. Account@Adapter+の設定

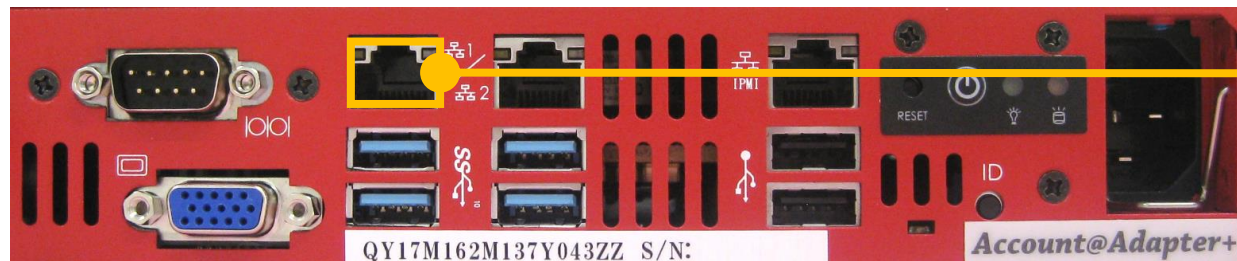
下記の流れでセットアップを行います。

1. 管理画面へのアクセス
2. ネットワーク設定
3. CA設定
4. RADIUS設定
5. アカウント登録
6. DHCP設定
7. 証明書発行/ダウンロード



## 2-1 管理画面へのアクセス

- ▶ Account@Adapter+の設定を行うため、管理画面にアクセスします
  - ▶ Account@Adapter+の初期IPアドレスは「192.168.0.1/24」となります  
設定を行う際は、クライアント端末のIPアドレスを同じセグメントに設定の上実施願います
  - ▶ クライアント端末とAccount@Adapter+のLAN1(左側)をLANケーブルで直接接続します



LAN1

- ▶ Microsoft Edgeを起動し、下記URLにアクセスします
  - ▶ <http://192.168.0.1:8080/manager/>
- ▶ 管理者IDとパスワードを入力し、管理画面にログインします
  - ▶ ログインID:naadmin
  - ▶ パスワード:naadmin



Account  Adapter

Ver. 6.18.00

ログインID

パスワード

ログイン

Copyright (C) 2006 HC Networks, Ltd. All Rights Reserved.

- ▶ IPアドレスの設定
  - ▶ 管理ツール [環境設定] - [ネットワーク設定] - 《メンテナンスメニュー》に遷移します

ネットワーク設定

ネットワーク設定

---

eth0

IPアドレス※ ① 192.168.10.2  
(XXX.XXX.XXX.XXX)

ネットマスク※ ② 255.255.255.0  
(XXX.XXX.XXX.XXX)

---

eth1

IPアドレス   
(XXX.XXX.XXX.XXX)

ネットマスク ③   
(XXX.XXX.XXX.XXX)

---

デフォルトゲートウェイ※   
(XXX.XXX.XXX.XXX)

### ■ ネットワーク設定

設定項目	設定値
①IPアドレス	192.168.10.2
②ネットマスク	255.255.255.0
③デフォルトゲートウェイ	192.168.10.1

- ▶ 設定後、画面下部の[登録]をクリックします

- ▶ CA設定
  - ▶ 管理ツール [CA] – [CA設定]を開き、CAの[設定]をクリックします

CA設定

認証局 ①  自己認証局  下位認証局

---

自己認証局情報設定

名前 (cn)※ ②   
(半角英数記号 64文字以内)

国 (c) ③   
(半角英数記号 2文字以内)

都道府県 (st)※ ④   
(半角英数記号 128文字以内)

市区町村 (l)

組織名 (o)

部署 (ou)

メールアドレス (E-mail)

有効期限

フレンドリー名

Basic Constraints  non-critical  critical

CRL配布ポイント ⑤  使用する  使用しない  
(半角英数記号 1024文字以内)

OCSP URI ⑥  使用する  使用しない  
(半角英数記号 1024文字以内)

---

暗号アルゴリズム

署名アルゴリズム

鍵長

### ■ 自己認証局情報設定

設定項目	設定値
① 認証局	自己認証局
② 名前 (cn)	ca_buffalo
③ 国 (c)	日本 (JP)
④ 都道府県 (st)	Tokyo
⑤ CRL配布ポイント	使用しない
⑥ OCSP URI	使用しない

- ▶ 設定後、画面下部の[登録]をクリックします
- ▶ [登録]をクリック後、画面左上の[RADIUS設定反映]をクリックします

- ▶ 2-4-1 RADIUS設定
  - ▶ 管理ツール [RADIUS] – [RADIUS設定]を開きます

### RADIUS設定

RADIUSポート番号※  
(半角数字 1~65535) **①**

RADIUS Accounting※  
(半角数字 1~65535) **②** 使用する 使用しない  
ポート番号

接続状況 **③** 記録する 記録しない

二重ログイン 許可する 許可しない

認証サーバー証明書 **④** 使用しない 内部サーバー証明書 外部サーバー証明書

認証局 **⑤** 内部認証局 外部認証局

IEEE 802.1X認証 **⑥** EAP-TLS PEAP EAP-TTLS EAP-MD5 EAP-MSCHAPv2  
PEAPの対応inner-tunnel認証方式:EAP-MSCHAPv2,EAP-TLS  
TTLSの対応inner-tunnel認証方式:PAP,CHAP,MSCHAPv2,EAP-MSCHAPv2,EAP-TLS  
outer-tunnel認証のAccess-AcceptにReply-Message属性を含める

内部アカウント 使用する 使用しない

認証失敗アカウントロック 使用する 使用しない  
認証連続失敗回数

最終認証日時記録 内部アカウント 外部LDAP/ADアカウント

NAS-IP-Address属性 パケットソースIPアドレスで書きこむ

MACアドレスの区切り文字 無視する 無視しない

### ■ RADIUS設定

設定項目	設定値
①RADIUSポート番号	1812
②RADIUS Accounting	使用する
③接続状況	記録する
④認証サーバー証明書	内部サーバー証明書
⑤認証局	内部認証局
⑥IEEE 802.1X認証	EAP-TLS/PEAP

- ▶ 設定後、画面下部の[登録]をクリックします
- ▶ [登録]をクリック後、画面左上の[RADIUS設定反映]をクリックします

- ▶ 2-4-2 RADIUSクライアント
  - ▶ 管理ツール [RADIUS] – [RADIUSクライアント]を開きます
  - ▶ 画面上部の[新規登録]をクリックします

**RADIUSクライアント登録**

登録用ファイルサンプル 戻る

ファイルから一括登録 ▼

クライアントID※ ① WAPM-2133TR  
(半角英数記号 32文字以内)

クライアント名   
(50文字以内)

IPアドレス※ ② 192.168.10.11  
(XXX.XXX.XXX.XXXまたは  
XXX.XXX.XXX.XXX/XX)

シークレットキー※ ③ .....  
..... (確認用)  
(半角英数記号 128文字以内)

### ■ RADIUSクライアント登録

設定項目	設定値①	設定値②	設定値③	設定値④
①クライアントID	WAPM-2133TR	WAPM-AX8R	WAPM-1266R	WAPS-1266
②IPアドレス	192.168.10.11	192.168.10.12	192.168.10.13	192.168.10.14
③シークレットキー	buffalo	buffalo	buffalo	buffalo

- ▶ 設定後、画面下部の[登録]をクリックします
- ▶ [登録]をクリック後、画面左上の[RADIUS設定反映]をクリックします

- ▶ 2-5-1 EAP-TLS認証用 証明書アカウント登録
  - ▶ ディレクトリペインの任意のディレクトリー [証明書] タブを開きます
  - ▶ [新規登録] をクリックします

cn ※ (半角英数記号 64文字以内)	<input type="text" value="cert01"/>
アカウント管理者 (半角英数記号空白 64文字以内)	<input type="text" value="naadmin"/>
通知用メールアドレス (半角英数記号 254文字以内) (1行1属性 最大5行)	<input type="text"/>
説明 (256文字以内)	<input type="text"/>
アカウント利用開始日時 (YYYY-MM-DD hh:00)	<input type="text" value="2023-04-18 17:00"/>
発行済み証明書1利用開始日時	
発行済み証明書1有効期限	
次回発行する証明書有効期限	CA証明書の有効期限に準ずる: 2032-10-18
※	
ネットワーク利用	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
アカウント利用	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効

### ■ 証明書アカウント登録

設定項目	設定値
①cn	cert01

- ▶ 設定後、画面下部の[登録]をクリックします

- ▶ 2-5-2 EAP-PEAP認証用 ユーザーアカウント登録
  - ▶ ディレクトリペインの任意のディレクトリー[ユーザー]タブを開きます
  - ▶ [新規登録]をクリックします

ユーザーID ※ (半角英数記号 64文字以内)	① user01
姓 (256文字以内)	<input type="text"/>
名 (256文字以内)	<input type="text"/>
アカウント管理者 (半角英数記号空白 64文字以内)	naadmin
通知用メールアドレス (半角英数記号 254文字以内) (1行1属性 最大5行)	<input type="text"/>
パスワード ※ (半角英数記号 64文字以内)	② ..... ..... (確認用)
説明 (256文字以内)	<input type="text"/>
アカウント利用開始日時 (YYYY-MM-DD hh:00)	2023-04-18 18:00
アカウント有効期限 ※ (YYYY-MM-DD hh:00)	③ <input checked="" type="radio"/> 無期限 <input type="radio"/> 期限あり <input type="text"/>
ネットワーク利用	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
アカウント利用	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効 <input type="radio"/> 一時停止

### ■ ユーザーアカウント登録

設定項目	設定値
①ユーザーID	user01
②パスワード	buffalo
③アカウント有効期限	無期限

- ▶ 設定後、画面下部の[登録]をクリックします



- ▶ 2-6-1 サーバグループ設定
  - ▶ 管理ツール [DHCP]-[サーバグループ]を開きます
  - ▶ [サーバグループ登録]をクリックします

グループ名※ (64文字以内)	①	<input type="text" value="servergroup_buffalo"/>
プライマリサーバー番号※	②	<input type="text" value="01"/>
プライマリIPアドレス※ (XXX.XXX.XXX.XXX)	③	<input type="text" value="192.168.10.2"/>
プライマリネットマスク※	④	<input type="text" value="255.255.255.0 [/24]"/>

### ■ サーバグループ登録

設定項目	設定値
①グループ名	servergroup_buffalo
②プライマリサーバー番号	01
③プライマリIPアドレス	192.168.10.2
④プライマリネットマスク	255.255.255.0[/24]

- ▶ 設定後、画面下部の[登録]をクリックします
- ▶ [登録]をクリック後、画面左上の[DHCP設定反映]をクリックします

- ▶ 2-6-2 スコープ設定
  - ▶ 管理ツール [DHCP] – [スコープ設定] – [スコープ設定]タブを開きます
  - ▶ 画面上部の[新規登録]をクリックします


グループ名 ※	①	servergroup buffalo		
スコープ設定名 ※ (32文字以内)	②	scope_buffalo		
ネットワークアドレス ※ (XXX.XXX.XXX.XXX)	③	192.168.10.0		
ネットマスク ※	④	255.255.255.0 [/24]		
デフォルトルーター ※ (XXX.XXX.XXX.XXX)	⑤	192.168.10.1	ネットワークアドレスから	セット
アドレス範囲001	⑥	<input checked="" type="radio"/> 払出 <input type="radio"/> 除外 <input type="radio"/> 固定IP自動割当	セット	クリア
	⑦	192   168   10   101	~	⑧ 192   168   10   200

### ■ スコープ設定登録

設定項目	設定値
①グループ名	(サーバーグループを選択)
②スコープ設定名	scope_buffalo
③ネットワークアドレス	192.168.10.0
④ネットマスク	255.255.255.0[/24]
⑤デフォルトルーター	192.168.10.1
⑥アドレス範囲001	払出
⑦アドレス範囲	192.168.10.101
⑧アドレス範囲	192.168.10.200

- ▶ 設定後、画面下部の[登録]をクリックします
- ▶ [登録]をクリック後、画面左上の[DHCP設定反映]をクリックします

- ▶ 2-7-1 EAP-TLS認証用 クライアント証明書発行/ダウンロード
  - ▶ 2-5-1で証明書アカウントを作成したディレクトリの[証明書]タブを開きます
  - ▶ 「証明書1」列の[発行]をクリックします

No.	<input type="checkbox"/>	cn ▼	証明書アカウント名 ▼	発行済み証明書1有効期限	最終認証日時 ▲ ▼	アカウント管理者 ▼	証明書1	証明書2	編集
1	<input type="checkbox"/>	cert01				naadmin	発行	-	


先頭に移動

- ▶ [OK]をクリックします

accountadapter.example.com:8080 の内容

証明書を発行します。  
よろしいですか？

- ▶ 「証明書1」列の[DL未]をクリックします

No.	<input type="checkbox"/>	cn ▼	証明書アカウント名 ▼	発行済み証明書1有効期限	最終認証日時 ▲ ▼	アカウント管理者 ▼	証明書1	証明書2	編集
1	<input type="checkbox"/>	cert01		2032-10-19 00:00:00		naadmin	失効 DL未 New 一時停止	-	

先頭に移動

- ▶ [インポートパスワード]に任意の値を入力し、[実行]をクリックします

インポートパスワード入力

インポートパスワード ※  
(半角英数字記号 30文字以内)

(確認用)

- ▶ 証明書ファイルがダウンロードされたことを確認します

- ▶ 2-7-2 EAP-PEAP認証用 CA証明書ダウンロード
  - ▶ 管理ツール [CA]－[CA設定]を開き、CAの[p12]をクリックします



- ▶ 証明書ファイルがダウンロードされたことを確認します

### 3. RADIUSクライアントの設定

下記の流れでセットアップを行います。

1. 管理画面へのアクセス
2. IPアドレス設定
3. RADIUS設定
4. SSID設定



- ▶ バッファロー社製無線アクセスポイントWAPM-2133TR、WAPM-AX4R、WAPM-1266R、WAPS-1266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WAPM-2133TRを使用して設定を行います。
- ▶ 無線アクセスポイントの設定を行うため、管理画面にアクセスします
  - ▶ バッファロー社製無線アクセスポイントのIPアドレスは、初期設定がDHCPから自動取得となっています。
  - ▶ DHCPサーバーがない環境の場合、IPアドレスは「192.168.11.100/24」となります。そのため設定を行う際は、クライアント端末のIPアドレスを同じセグメントに設定の上実施願います
  - ▶ クライアント端末と無線アクセスポイントのLAN1(左側)をLANケーブルで直接接続します



- ▶ Microsoft Edgeを起動し、下記URLにアクセスします
  - ▶ 192.168.11.100
- ▶ 管理者IDとパスワードを入力し、管理画面にログインします
  - ▶ ログインID:admin
  - ▶ パスワード:password

The image shows the management interface of the Buffalo AirStation Pro WAPM-2133TR. The interface is displayed on a light gray background. At the top, the Buffalo logo is shown in red, followed by 'AirStation Pro' in a serif font and 'WAPM-2133TR Version 1.27' in a smaller font. Below this, there are two input fields: 'ユーザー名' (Username) with 'admin' entered, and 'パスワード' (Password) with 'password' entered. A red rectangular border highlights these two input fields. At the bottom of the form, there is a dark gray button with the text 'ログイン' (Login) in white.

- ▶ IPアドレスの設定
  - ▶ 詳細設定 [LAN設定] – [IPアドレス]に遷移します

**LAN側IPアドレス設定**

IPアドレス ①

IPアドレスの取得方法 ① 手動設定 ▼

IPアドレス ② 192.168.10.11

サブネットマスク ③ 255.255.255.0 ▼

デフォルトゲートウェイ

DNSサーバー

プライマリー

セカンダリー

DHCPサーバー

DHCPサーバー機能 使用しない ▼

**設定**

### ■ ネットワーク設定

設定項目	設定値
①IPアドレスの取得方法	手動設定
②IPアドレス	192.168.10.11
③サブネットマスク	255.255.255.0

- ▶ 上記設定後、画面下部の[登録]をクリックします
- ▶ IPアドレス変更後、Microsoft Edgeを起動し、下記URLにアクセスし直します
  - ▶ 192.168.10.11

- ▶ RADIUS設定
  - ▶ 詳細設定 [ネットワーク設定] – [RADIUS設定]タブを開きます

**RADIUS設定**

**RADIUSサーバー**

プライマリ-RADIUSサーバー

サーバー	① <input type="radio"/> 内蔵 <input checked="" type="radio"/> 外部
サーバー名	② 192.168.10.2
認証ポート	③ 1812
Accounting	<input checked="" type="checkbox"/> 使用する
Accountingポート	1813
Shared Secret	④ buffalo
Session-Timeout	3600 秒

セカンダリ-RADIUSサーバー

サーバー	<input type="radio"/> 内蔵 <input checked="" type="radio"/> 外部
サーバー名	
認証ポート	1812
Accounting	<input checked="" type="checkbox"/> 使用する
Accountingポート	1813
Shared Secret	
Session-Timeout	3600 秒

Calling-Station-Id ""(区切りなし, 小文字) ▼

Called-Station-Id ""(区切りなし, 小文字) ▼

**設定**

### ■ スコープ設定登録

設定項目	設定値
①サーバー	外部
②サーバー名	192.168.10.2
③認証ポート	1812
④Shared Secret	buffalo

- ▶ 上記設定後、画面下部の[設定]をクリックします



## ▶ SSIDの設定

- ▶ 詳細設定 [Wi-Fi設定] – [SSID設定]タブを開きます
- ▶ 画面中央の[新規作成]をクリックします

## SSID設定 - SSIDの編集

## ステアリング ポリシー設定

ステアリング ポリシー 無効

## SSID編集

Index	状態	SSID	VLAN ID	2.4GHz	5GHz Low	5GHz High	ステアリング	Wi-Fiの認証	暗号化
SSIDの設定は登録されていません									
使用可能SSID				2.4GHz 16 / 16	5GHz Low 16 / 16	5GHz High 16 / 16			
Wi-Fi	①	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効							
SSID	②	2133TR							
次の場合に有効にする		通常時と緊急時							
使用デバイス	③	<input checked="" type="checkbox"/> 2.4GHz <input checked="" type="checkbox"/> 5GHz Low <input checked="" type="checkbox"/> 5GHz High							
ステアリング		無効							
優先制御		優先							
VLAN ID		VLANモード	VLAN ID	追加VLAN ID					
		Untagged Port	1						
ANY接続		<input checked="" type="checkbox"/> 許可する							
プライバシーセパレーター		使用しない							
ロードバランス(同時接続台数制限)		2.4GHz 128 / 128	5GHz Low 128 / 128	5GHz High 128 / 128					
Wi-Fiの認証	④	WPA2 Enterprise							
暗号化方式		AES							
キー更新間隔		60 分							
Management Frame Protection		無効							
追加認証		追加認証を行わない							
RADIUS	⑤	ネットワーク設定内のRADIUSサーバー設定を使用する							

修正保存 編集を終了して前の画面へ戻る

- ▶ 設定後、画面下部の[修正保存]をクリックします

## ■ スコープ設定登録

	設定値
①Wi-Fi	有効
②SSID	2133TR
③使用デバイス	2.4GHz、5GHz Low、5GHz High (WAPM-2133TR以外では、2.4GHzと5GHz)
④Wi-Fiの認証	WPA2 Enterprise
⑤RADIUS	ネットワーク設定内のRADIUSサーバー設定を使用する

## 4. EAP-TLS認証でのクライアント設定

下記のOSにおけるEAP-TLS認証手順を記載します。

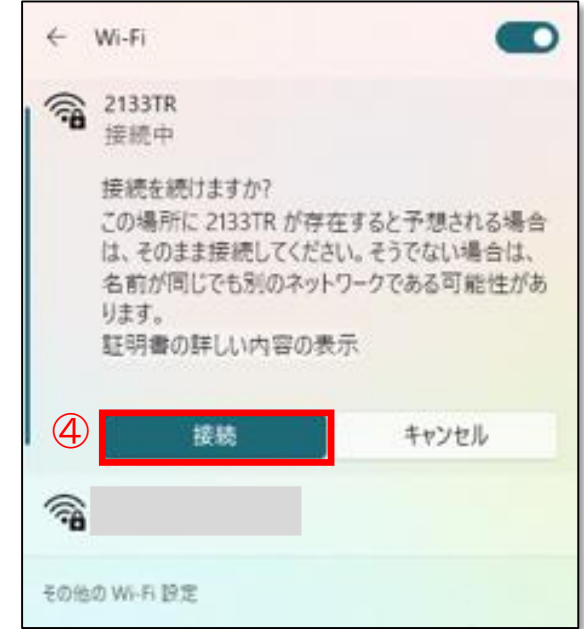
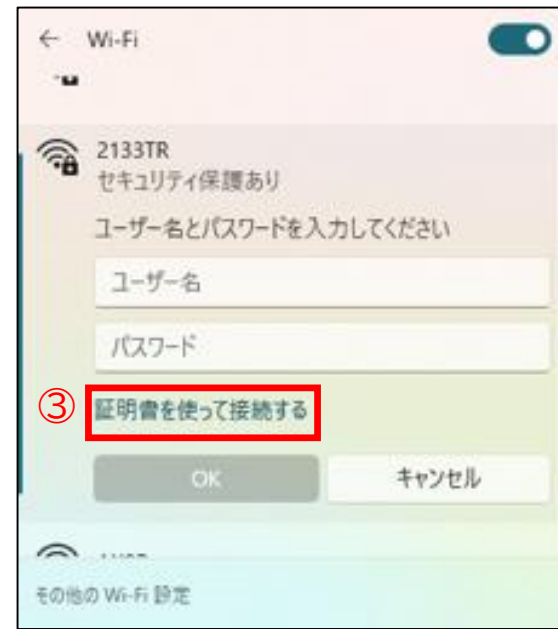
1. Windows 11でのEAP-TLS認証
2. macOSでのEAP-TLS認証
3. iOSでのEAP-TLS認証
4. AndroidでのEAP-TLS認証

※代表として、RADIUSクライアント『WAPM-2133TR』を経由したEAP-TLS認証について記載しておりますが、その他のRADIUSクライアント(WAPM-AX8R/WAPM-1266R/WAPS-1266)についても手順は同様となります。



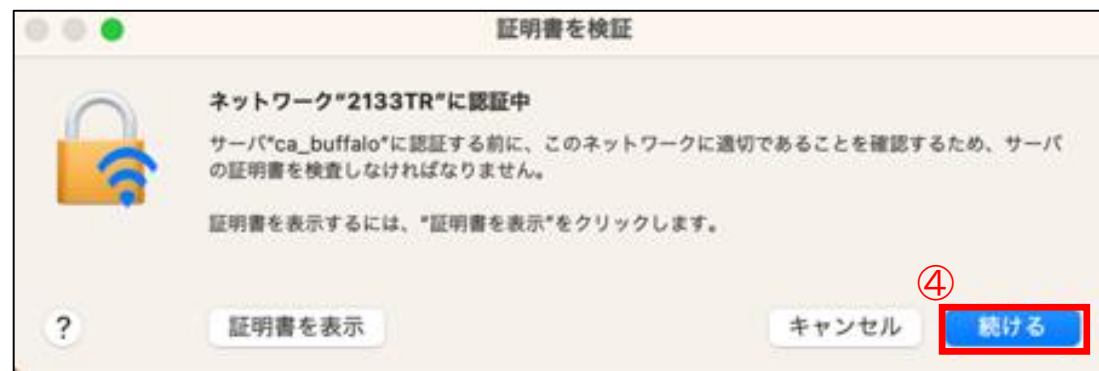
## 4-1 Windows 11でのEAP-TLS認証

- ▶ 事前準備: PCにクライアント証明書をインポートしておきます。
- ▶ EAP-TLS認証の実施
  - ▶ ① SSID「2133TR」をクリックします
  - ▶ ② [接続]をクリックします
  - ▶ ③ [証明書を使って接続する]をクリックします
  - ▶ ④ [接続]をクリックします



## 4-2 macOSでのEAP-TLS認証

- ▶ 事前準備: PCにクライアント証明書をインポートしておきます。
- ▶ EAP-TLS認証の実施
  - ▶ ① SSID「2133TR」をクリックします
  - ▶ ② プルダウンから[cert01]を選択します
  - ▶ ③ [OK]をクリックします
  - ▶ ④ [続ける]をクリックします



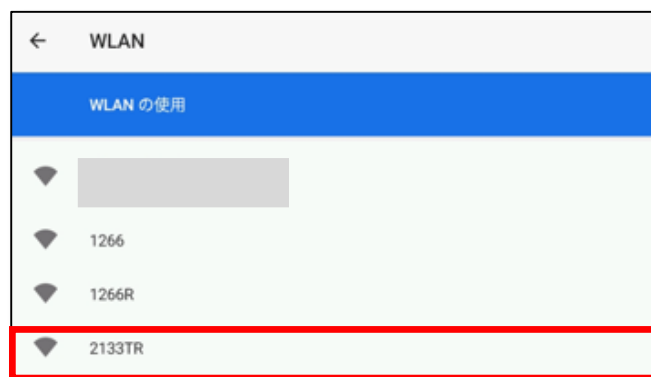
## 4-3 iOSでのEAP-TLS認証

- ▶ 事前準備: PCにクライアント証明書をインポートしておきます。
- ▶ EAP-TLS認証の実施
  - ▶ ① SSID「2133TR」をクリックします
  - ▶ ② [モード]をクリックし、[EAP-TLS]を選択します
  - ▶ ③ [ID]をクリックし、[cert01]を選択します
  - ▶ ④ [接続]をクリックします
  - ▶ ⑤ [信頼]をクリックします



## 4-4 AndroidでのEAP-TLS認証

- ▶ 事前準備: PCにクライアント証明書をインポートしておきます。
- ▶ EAP-TLS認証の実施
  - ▶ ① SSID「2133TR」をクリックします
  - ▶ ②～⑦ 表に記載の値を入力/選択します
  - ▶ ⑧ [接続]をクリックします



## ■ 認証設定

設定項目	設定値
②EAP方式	TLS
③CA証明書	ca_buffalo
④オンライン認証ステータス	検証しない
⑤ドメイン	ca_buffalo
⑥ユーザー証明書	(クライアント証明書を選択)
⑦ID	cert01

## 5. EAP-PEAP認証でのクライアント設定

下記のOSにおけるEAP-PEAP認証手順を記載します。

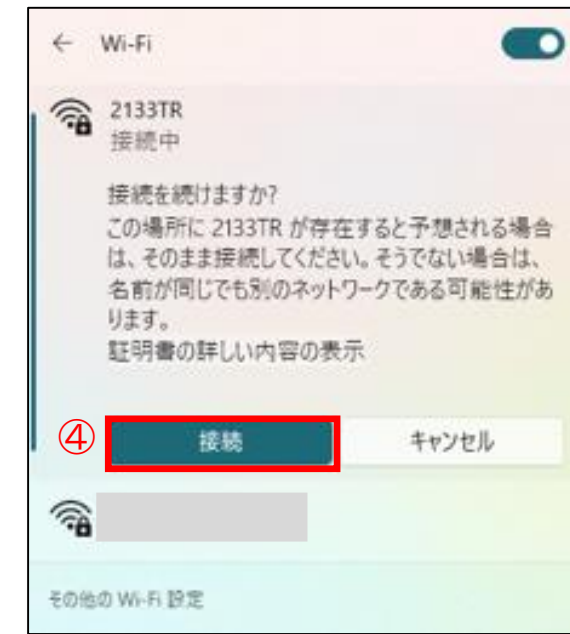
1. Windows 11でのEAP-PEAP認証
2. macOSでのEAP-PEAP認証
3. iOSでのEAP-PEAP認証
4. AndroidでのEAP-PEAP認証

※代表として、RADIUSクライアント『WAPM-2133TR』を経由したEAP-PEAP認証について記載しておりますが、その他のRADIUSクライアント(WAPM-AX8R/WAPM-1266R/WAPS-1266)についても手順は同様となります。



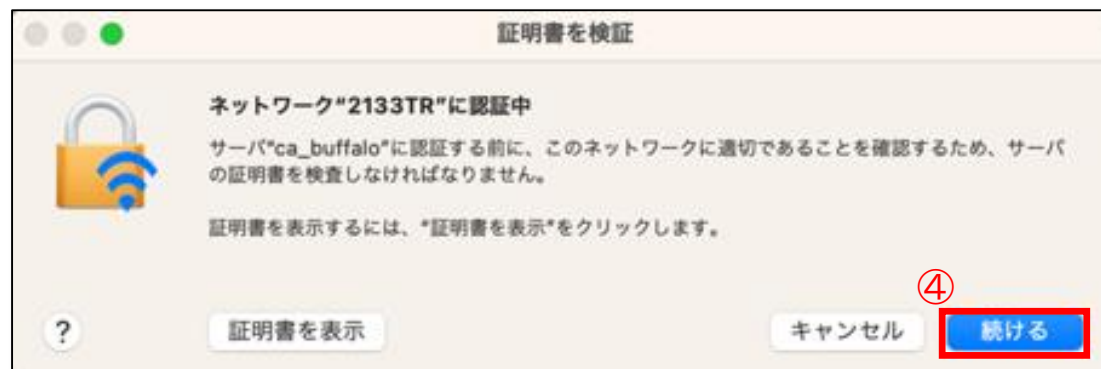
## 5-1 Windows 11でのEAP-PEAP認証

- ▶ 事前準備: PCにCA証明書をインポートしておきます。
- ▶ EAP-PEAP認証の実施
  - ▶ ① SSID「2133TR」をクリックします
  - ▶ ② [接続]をクリックします
  - ▶ ③ ユーザー名:user01 パスワード:buffalo を入力します
  - ▶ ④ [OK]をクリックします
  - ▶ ⑤ [接続]をクリックします



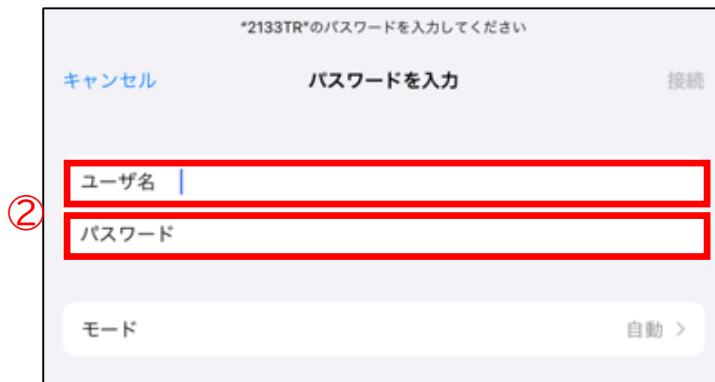


- ▶ 事前準備: PCにCA証明書をインポートしておきます。
- ▶ EAP-PEAP認証の実施
  - ▶ ① SSID「2133TR」をクリックします
  - ▶ ② アカウント名:user01 パスワード:buffalo を入力します
  - ▶ ③ [OK]をクリックします
  - ▶ ④ [続ける]をクリックします



## 5-3 iOSでのEAP-PEAP認証

- ▶ 事前準備: PCにCA証明書をインポートしておきます。
- ▶ EAP-PEAP認証の実施
  - ▶ ① SSID「2133TR」をクリックします
  - ▶ ② ユーザ名:user01 パスワード:buffalo を入力します
  - ▶ ③ [接続]をクリックします
  - ▶ ④ [信頼]をクリックします



## 5-4 AndroidでのEAP-PEAP認証

- ▶ 事前準備: PCにCA証明書をインポートしておきます。
- ▶ EAP-PEAP認証の実施
  - ▶ ① SSID「2133TR」をクリックします
  - ▶ ②～⑧ 表に記載の値を入力/選択します
  - ▶ ⑨ [接続]をクリックします

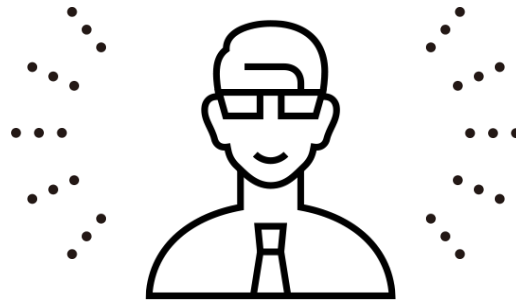


## ■ 認証設定

設定項目	設定値
②EAP方式	PEAP
③フェーズ2認証	MSCHAPV2
④CA証明書	ca_buffalo
⑤オンライン認証ステータス	検証しない
⑥ドメイン	ca_buffalo
⑦ID	user01
⑧パスワード	buffalo

## お問い合わせはこちら

お気軽に  
お問い合わせください



**HCNET** エイチ・シー・ネットワークス株式会社

〒111-0053 東京都台東区浅草橋1-22-16 ヒューリック浅草橋ビル 5F

<https://www.hcnet.co.jp/>

HCNET お問い合わせ



**BUFFALO**<sup>TM</sup>

〒460-8315 愛知県名古屋市中区大須三丁目30番20号 赤門通ビル

<https://www.buffalo.jp/>

バッファロー お問い合わせ



HCNETおよびそのロゴは、エイチ・シー・ネットワークス株式会社の登録商標です。記載されている社名および製品名は、各社の商標または登録商標です。掲載製品の写真の一部はイメージです。  
記載の製品を輸出される場合には、外国為替および外国貿易法の規制ならびに米国輸出管理規則などの外国の輸出関連法規をご確認のうえ、必要な手続きをお取りください。なお、ご不明な場合は、弊社担当営業にお問い合わせください。