
# Account@Adapter+
# 認証連携設定例

エイチ・シー・ネットワークス株式会社

BUFFALO

（2023/5/17 作成）

SE23-Adapter-002

# 本資料の構成

- 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。

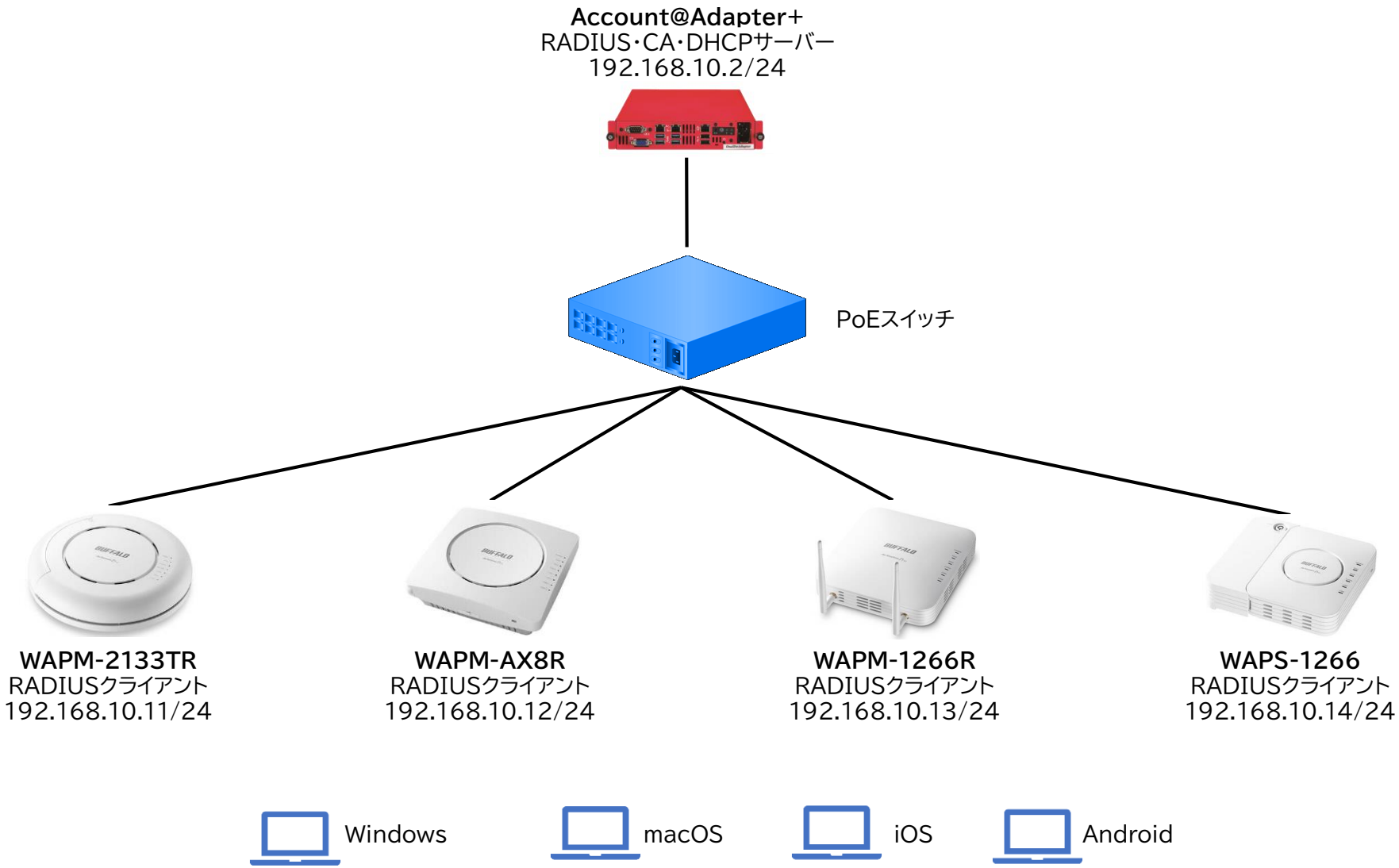
# 目次

# 1. 構成

# 1-1 構成図



- 以下の環境を構成します。



# 1-2 環境



## 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<br>DHCPサーバー<br>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<br>22H2 |
| MacBook Air | Apple | 802.1Xクライアント端末 | macOS Ventura<br>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 環境



- 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 環境



## 1-2-3 ネットワーク設定

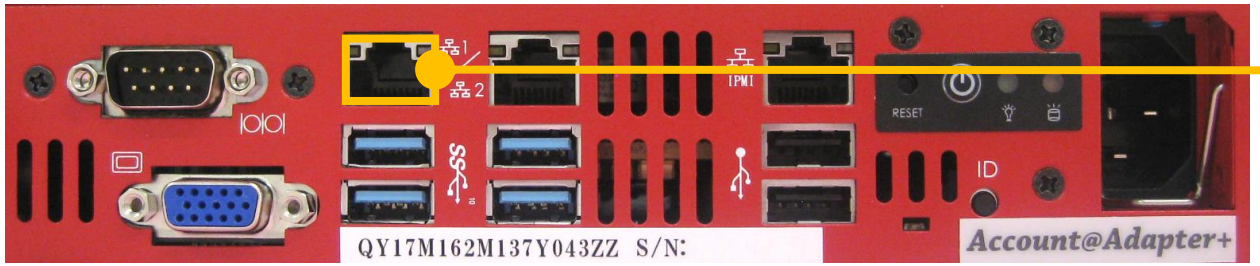
| 製品名 | IPアドレス | RADIUSポート | シークレットキー |
|---|---|---|---|
| Account@Adapter+ | 192.168.10.2/24 | 1812 | buffalo |
| WAPM-2133TR | 192.168.10.11/24 | 1812 | buffalo |
| WAPM-AX8R | 192.168.10.12/24 | 1812 | buffalo |
| WAPM-1266R | 192.168.10.13/24 | 1812 | buffalo |
| WAPS-1266 | 192.168.10.14/24 | 1812 | 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




  - 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

# 2-2 ネットワーク設定

- 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

| 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

# 2-3 CA設定

- 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


■ 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 |
| ⑤CRL配布ポイント | 使用しない |
| ⑥OCSP 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 RADIUS設定

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

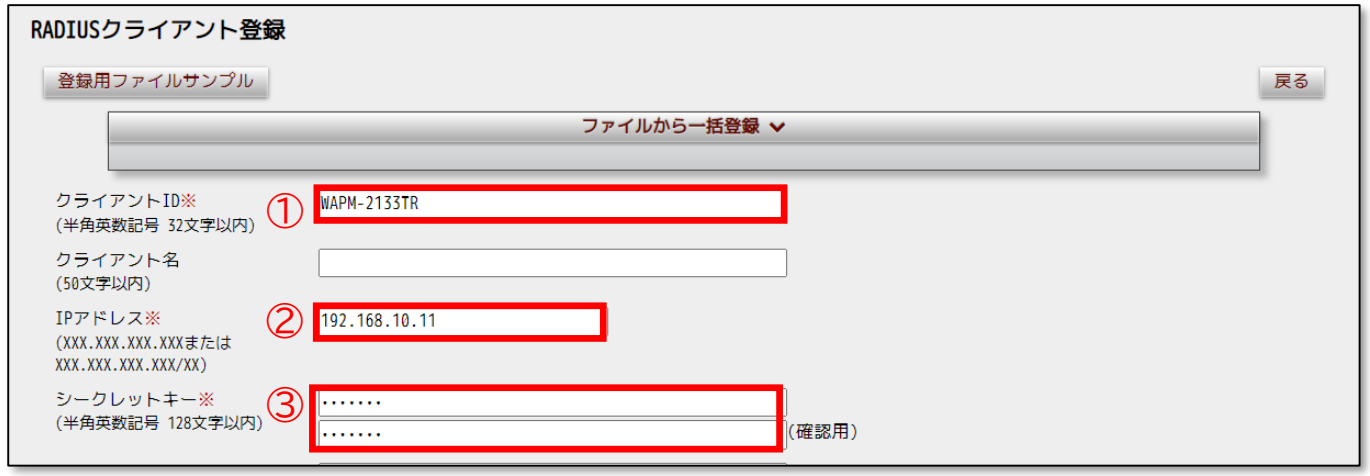

■ RADIUS設定

| 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 RADIUS設定

- 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



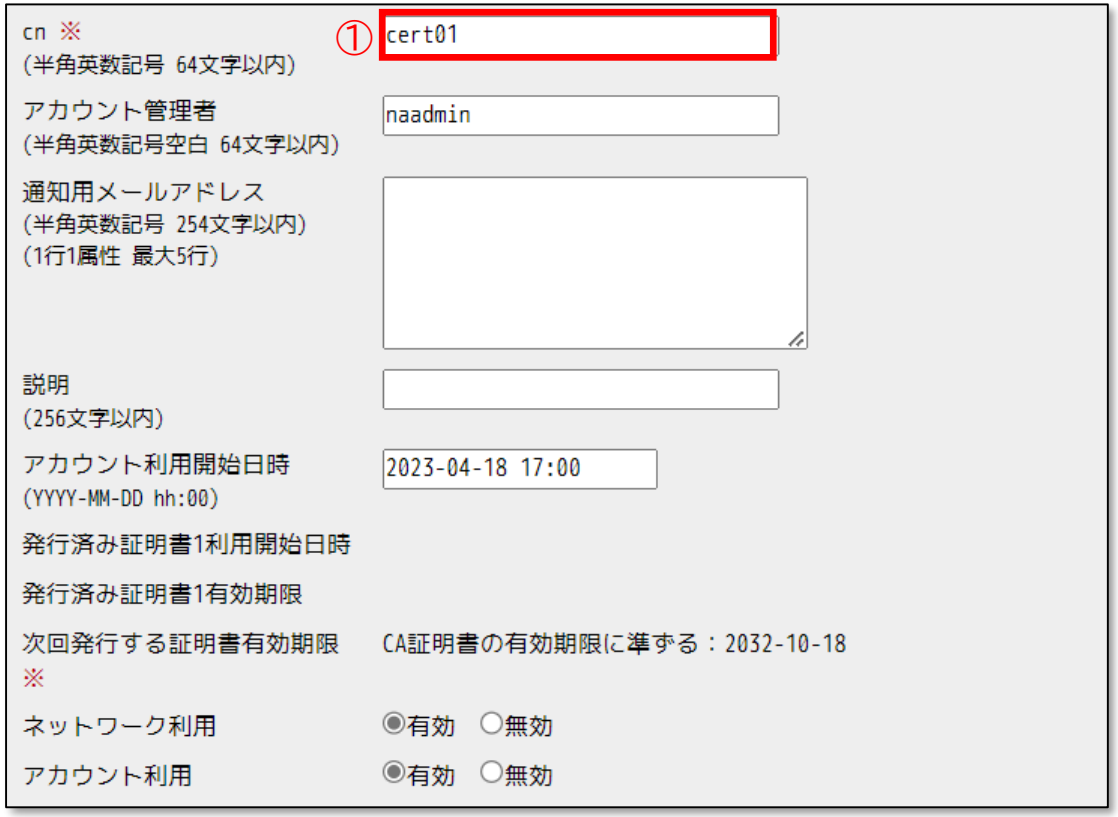

■ RADIUSクライアント登録

| 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 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
  - 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



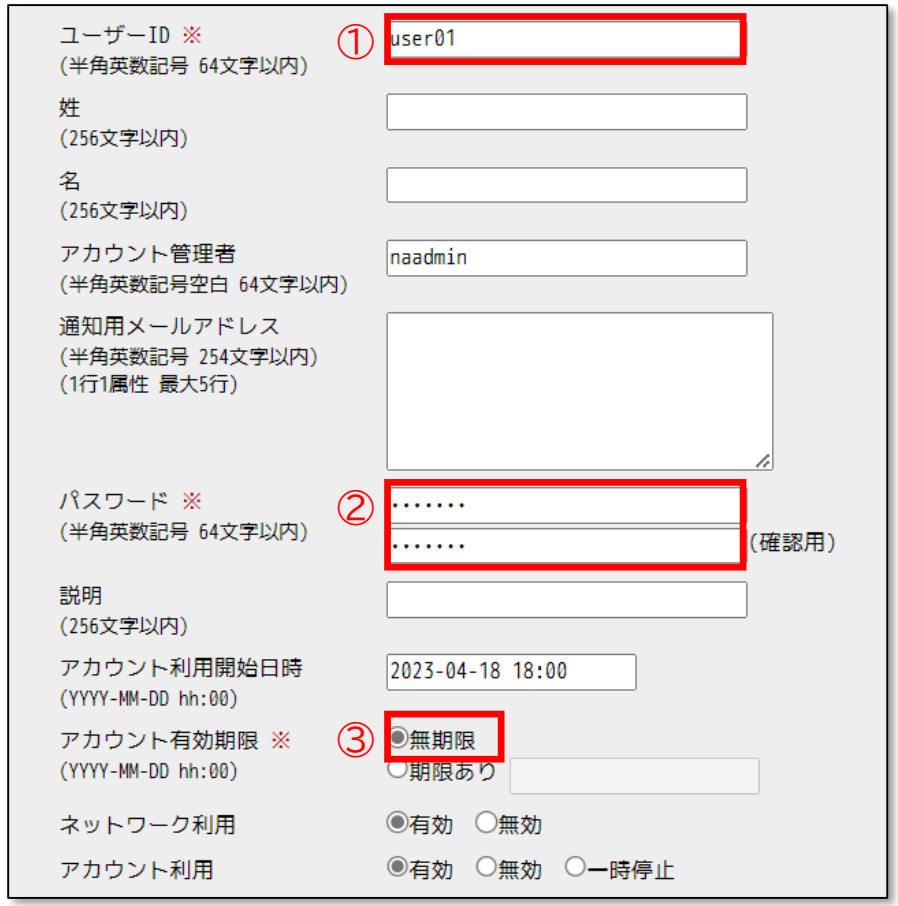

■ 証明書アカウント登録

| 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 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
  - 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



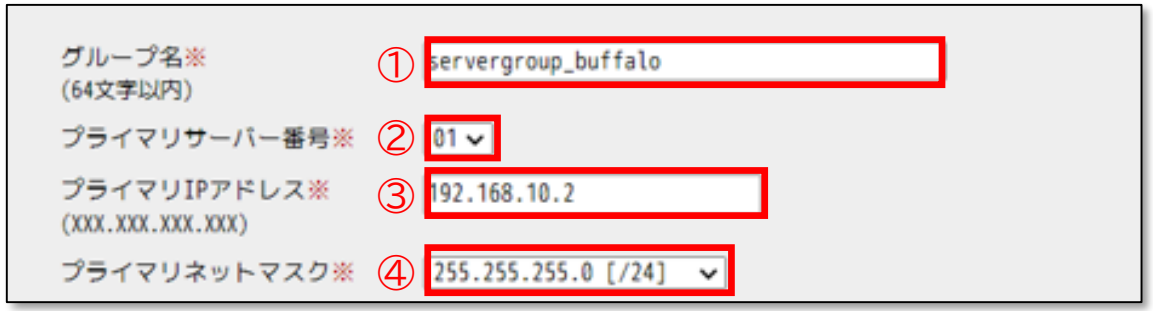

■ ユーザーアカウント登録

| 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 DHCP設定

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



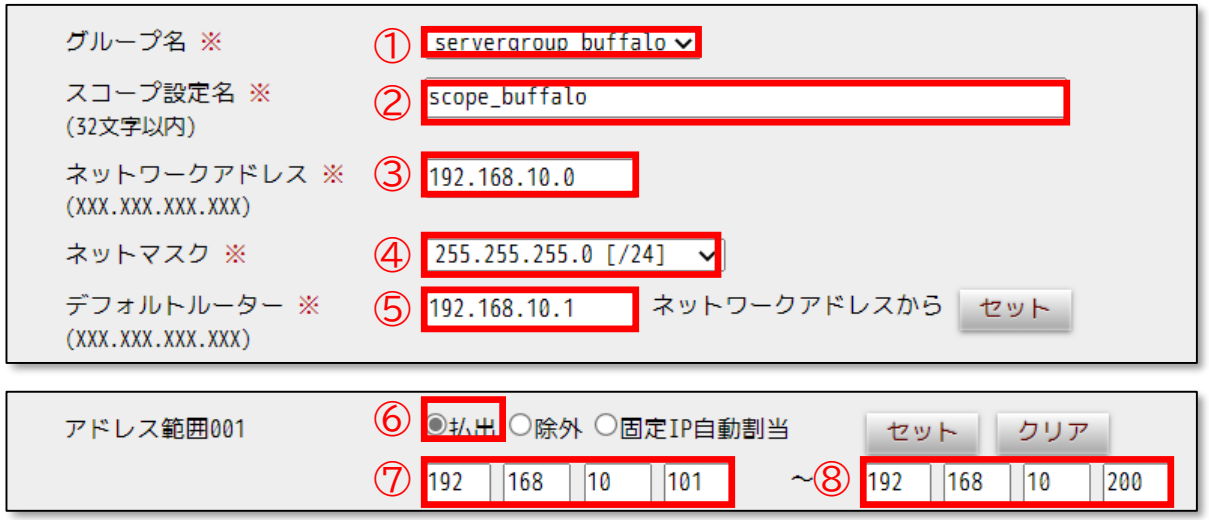

■ サーバーグループ登録

| 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 DHCP設定

- 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



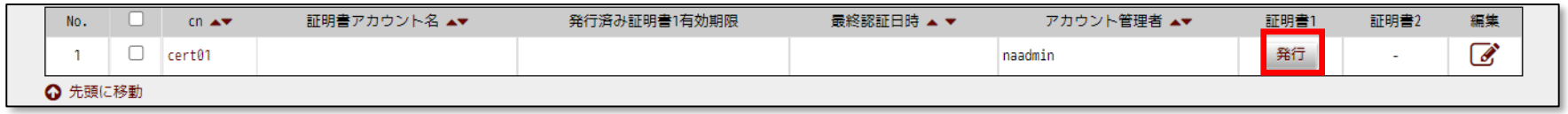

■ スコープ設定登録

| 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

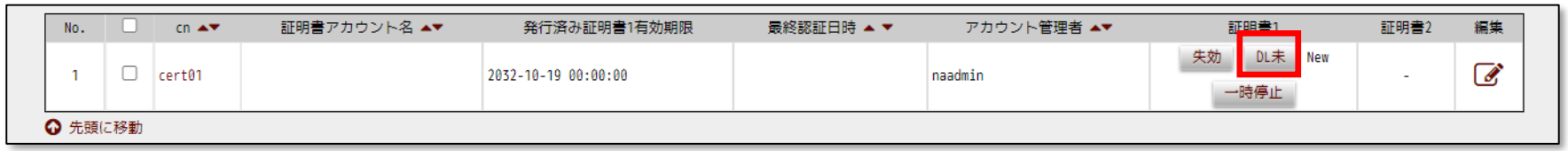
# 2-7 証明書発行/ダウンロード

- 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
  - 2-5-1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




  - [OK]をクリックします


  - 「証明書1」列の[DL未]をクリックします

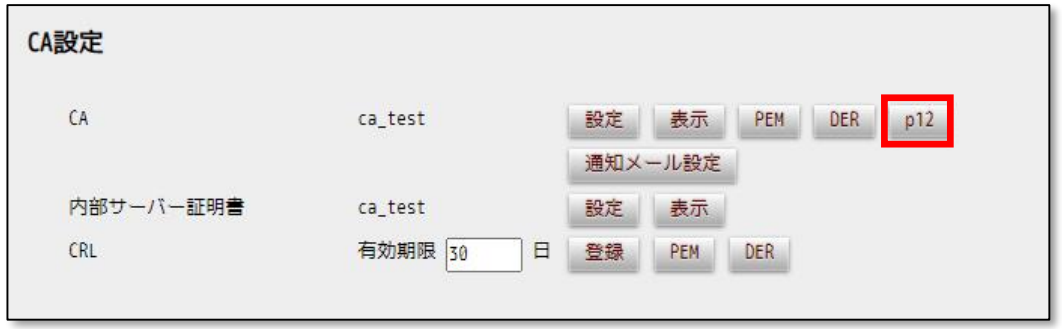



  - [インポートパスワード]に任意の値を入力し、[実行]をクリックします


  - 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 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
  - 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

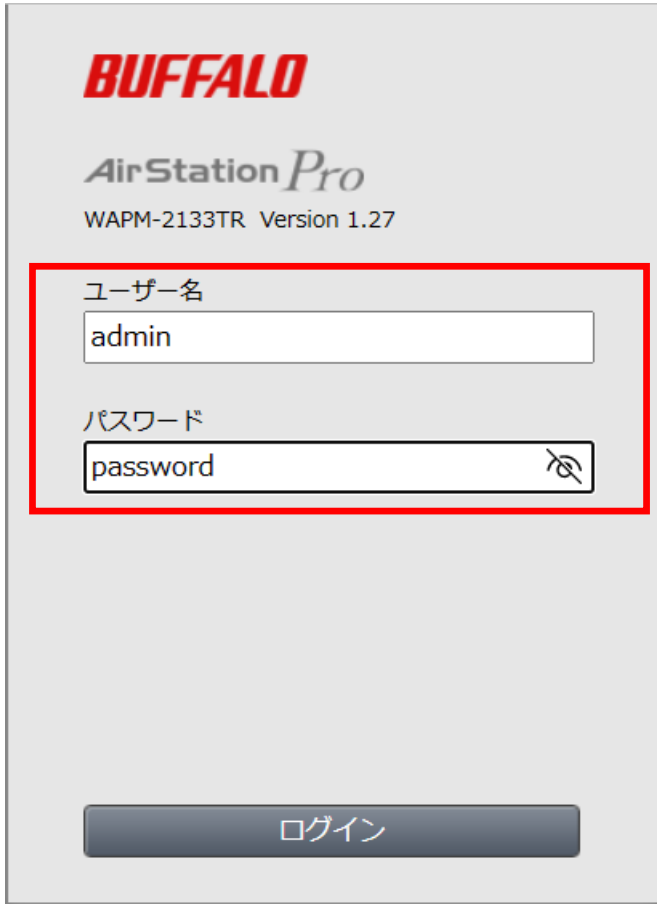
# 3. RADIUSクライアントの設定

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

# 3-1 管理画面へのアクセス

- 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



# 3-2 IPアドレス設定

- 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

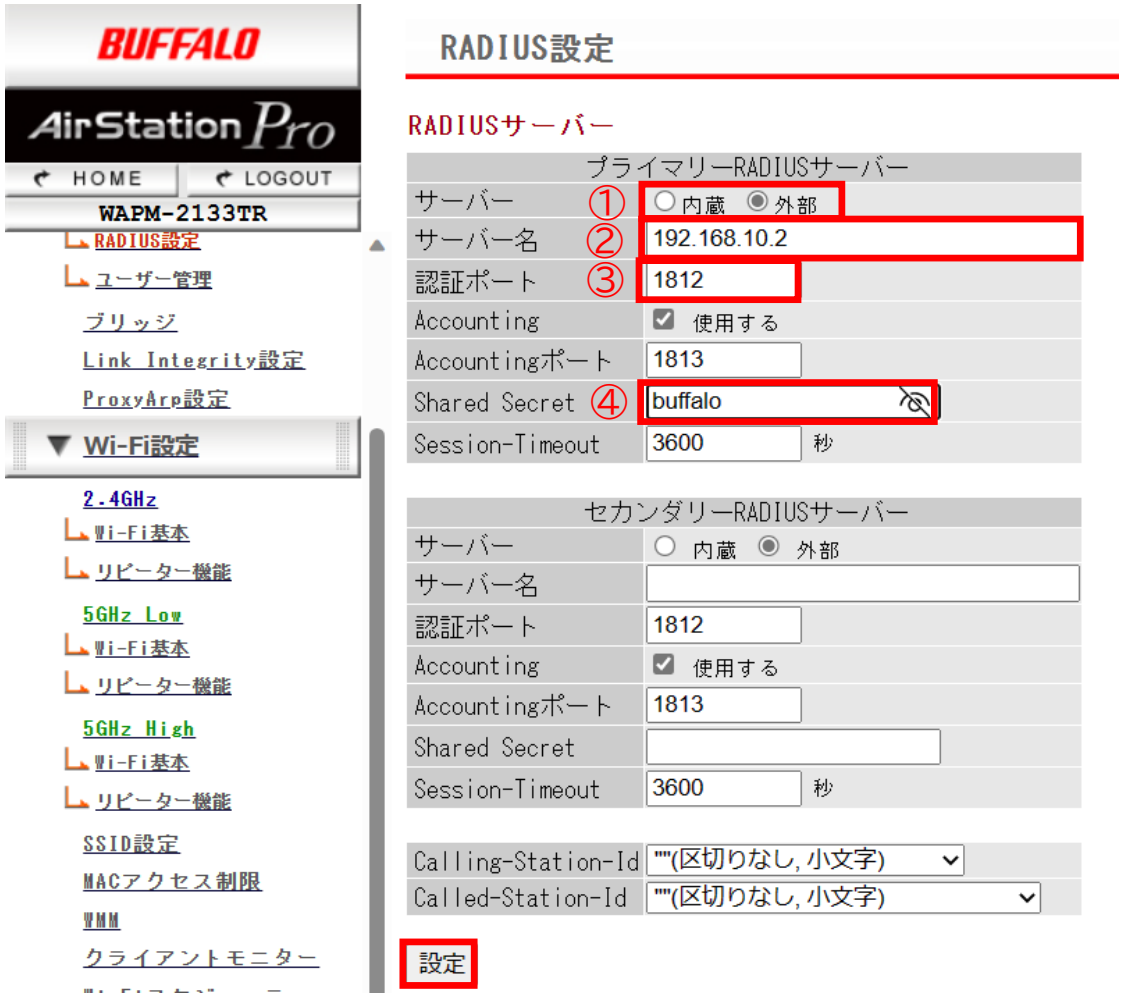

■ ネットワーク設定

| 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

# 3-3 RADIUS設定

- 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




- 上記設定後、画面下部の［設定］をクリックします

■ 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 |

# 3-4 SSID設定



- 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


  - 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<br>(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

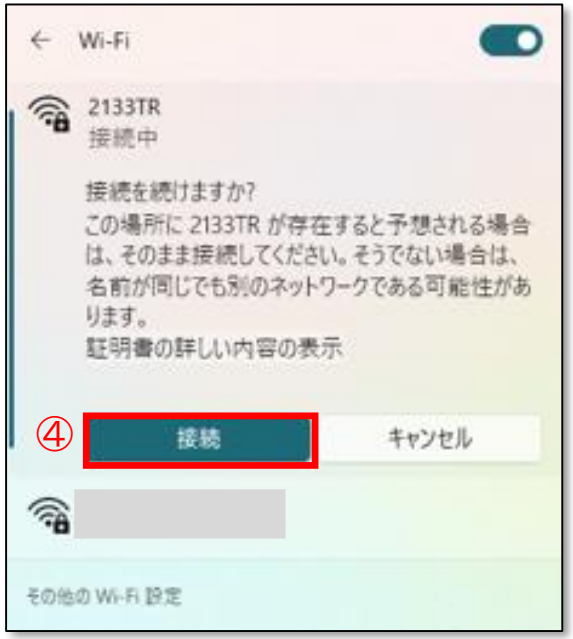
※代表として、RADIUSクライアント『WAPM-2133TR』を経由したEAP-TLS認証について記載しておりますが、
その他のRADIUSクライアント（WAPM-AX8R/WAPM-1266R/WAPS-1266）についても手順は同様となります。

# 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

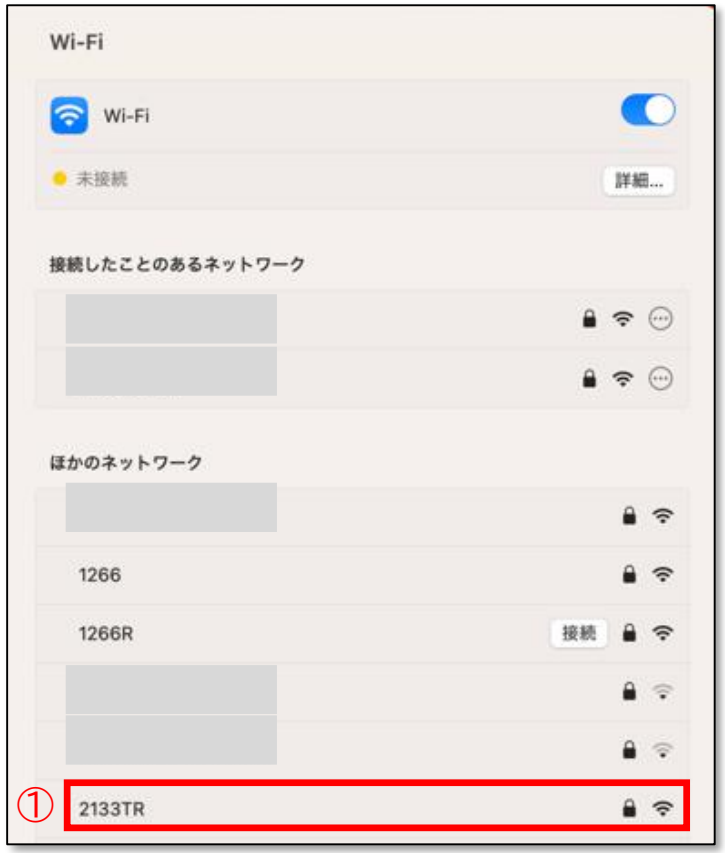


# 4-2 macOSでのEAP-TLS認証



- 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



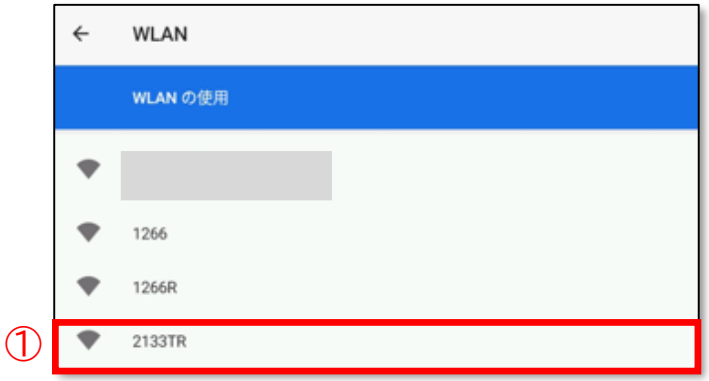
- 事前準備：PCにクライアント証明書をインポートしておきます。
- EAP-TLS認証の実施
  - ① SSID「2133TR」をクリックします
  - ② [モード]をクリックし、[EAP-TLS]を選択します
  - ③ [ID]をクリックし、[cert01]を選択します
  - ④ [接続]をクリックします
  - ⑤ [信頼]をクリックします

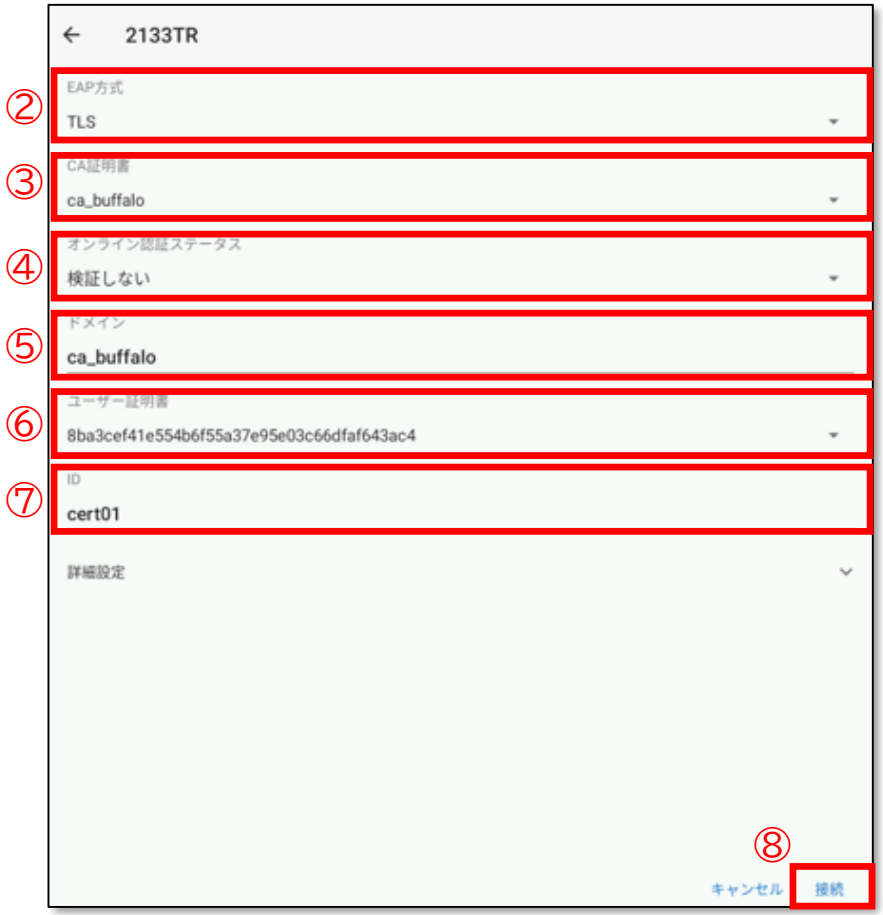




# 4-4 AndroidでのEAP-TLS認証

- 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

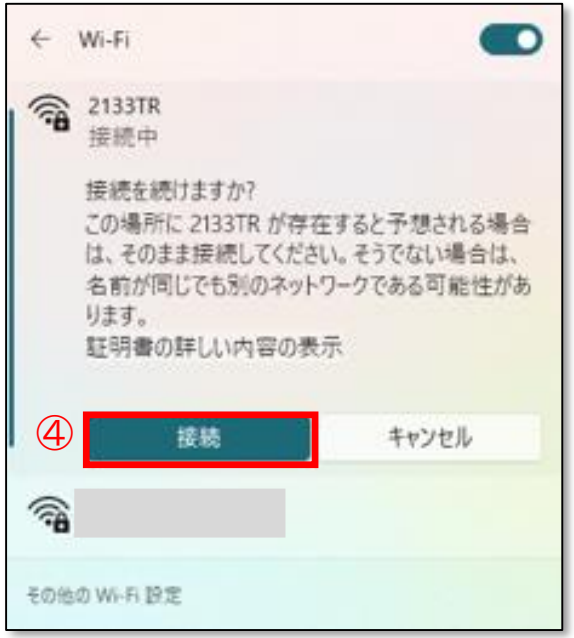
※代表として、RADIUSクライアント『WAPM-2133TR』を経由したEAP-PEAP認証について記載しておりますが、
その他のRADIUSクライアント（WAPM-AX8R/WAPM-1266R/WAPS-1266）についても手順は同様となります。

# 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



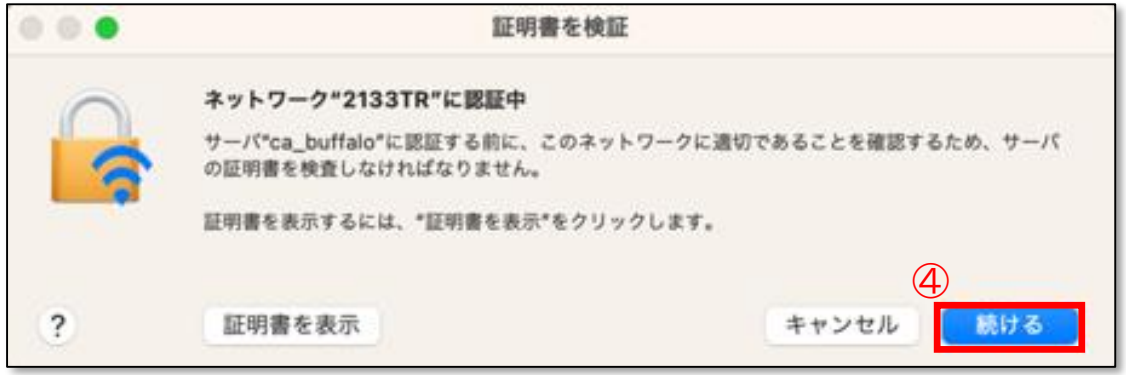



# 5-2 macOSでのEAP-PEAP認証



- 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 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

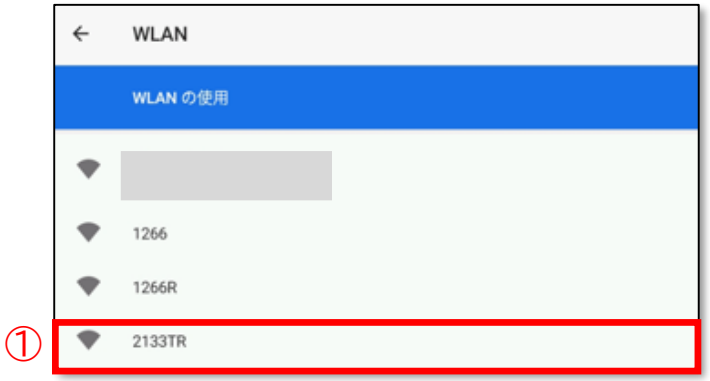


- 事前準備：PCにCA証明書をインポートしておきます。
- EAP-PEAP認証の実施
  - ① SSID「2133TR」をクリックします
  - ② ユーザ名：user01　パスワード：buffalo　を入力します
  - ③ [接続]をクリックします
  - ④ [信頼]をクリックします




# 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



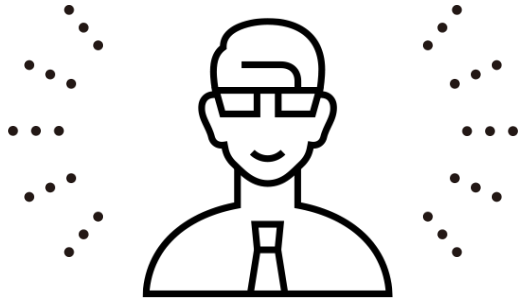


■ 認証設定

| 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™

〒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