Passpoint 対応アクセスポイント設定手順書

暫定 2023/03 版

国立情報学研究所

1. アクセスポイントの選定における注意事項

OpenRoaming においては、eduroam と同様に IEEE802.1X 認証を利用が前提となっています。その他に、自動ローミングを有効とするために、Wi-Fi CERTIFIED Passpoint®への対応など、若干の拡張が加えられています。

アクセスポイントの仕様として、以下の要件を満たす必要があります。

- IEEE802.1X 認証に対応していること。
- WPA2(WPA/AES)の無線暗号化に対応していること。
- SSID ごとに異なる RADIUS サーバに接続できること。
- Wi-Fi CERTIFIED Passpoint®に対応していること。

実際には、上記に対応していながら OpenRoaming の認証基盤との相性問題が発生することがあります。導入機材が実際に利用可能は、日本において認証連携基盤を運用する Cityroam より提供される情報を参照することを薦めます。

2. RADIUS Proxy の設定

RADIUS ツリーの構造は eduroam と同様です。設定においては、eduroam と基本的に同一ですので、RADIUS サーバの導入方法においては、eduroam JP 事務局の提供する「Free RADIUS 3 による RADIUS サーバを構築する場合」を参考に構築を行ってください。eduroam で使用する RADIUS サーバをそのまま利用することも可能です。

eduroam と OpenRoaming の設定での差異として、accounting 設定があります。各機関の RADIUS Proxy から OpenRoaming の Hub に向けて acct パケットの送出が必要になります。

例）FreeRADIUS における eduroam 設定との差異点

[proxy.conf]

home_server セクションで、type=auth+acct とする必要があります。eduroam においては、acct は不要と指定されているので、混同しないよう注意が必要です。

設定例

```
home_server JPhub1 {
type = auth+acct
```

```
ipaddr = [JP Hub プライマリ IP アドレス]
port = 1812
secret = <シークレットキー>
status_check = status-server
}

home_server JPhub2 {
type = auth+acct
ipaddr = [JP Hub セカンダリ IP アドレス]
port = 1812
secret = <シークレットキー>
status_check = status-server
}

home_server_pool JPhub-pool {
type = fail-over
home_server = JPhub1
home_server = JPhub2
}

realm DEFAULT {
auth_pool = JPhub-pool
acct-pool = JPhub-pool
nostrip
}
```

なお、OpenRoaming のハブ間の接続においては、TLS を使用する RADIUS クライアント/サーバ接続である RadSec を使用しています。

現在は機関に設置する RADIUS Proxy において、RadSec は必須とされていませんが、新規に立ち上げる場合は将来的な移行を踏まえ、RADIUS Proxy においても RadSec に対応しておくことが望ましいです。

3. アクセスポイントの設定

基本的な設定

eduroam で行っている設定を参考に、WPA2 Enterprise の設定を行ってください。

- IEEE802.1X 認証（エンタープライズ認証）

- SSID は Cityroam を推奨（Cityroam 経由で OpenRoaming に参加する場合）
  ※ Cityroam では、Passpoint 非対応機での接続を確保するために、なるべく同一の SSID を使うことを推奨しています。
- RADIUS サーバのホスト IP もしくは FQDN、ポート番号、シークレットキーをアクセスポイント側に入力

Called-Station-Id の設定

Cityroam 経由で OpenRoaming に参加する場合は、Called-Station-Id 属性の末尾に SSID を含む必要があります。Cisco Meraki を使用する場合は、自動的に付与されますが、ArubaOS など明示的な設定が必要なアクセスポイントもあります。

ArubaOS におけるコマンド入力例
called-station-id include-ssid delimiter :

ANQP Venue 情報の入力

Passpoint においては、ANQP で出力する要素として以下の項目が必要です。

- Operator name（オペレーター名） - 運用事業者名を入力
  例）alansmith university
- Venue name（会場名） - 場所の名称を入力
  言語コードを指定し日本語等で入力することも可能です。ただし、ユーザーは日本語話者とは限りませんので、そこを留意することも必要です。
  例）Research Bldg. 3F
- Venue Group / Venue type（会場タイプ） - 設置場所の種類を選択
  入れ子構造になっており、Cisco Meraki のように Venue type のみの入力で済むものもあります。
- Network type（ネットワークの種類）- 有料、無料、テストなど運用種別を選択
- Domain List
  特定の Wi-Fi ネットワークへの接続を試みることができることをユーザーデバイスに通知するために使用されます。Cityroam 経由で接続する場合は、cityroam.jp を入力してください。

Cisco Meraki における設定例
HotSpot2.0（ホットスポット 2.0）のタブで設定を行います。

- OpenRoaming で使用する SSID を選択

- ホットスポット 2.0 を「有効」
- オペレーター名、会場名を入力
- 会場タイプ、ネットワークの種類を選択
- ドメインリストを入力

Venue Group/Venue type、Network type は決められた数値または表記を入れる必要がありますが、コマンドラインによる設定の場合、選択項目がありません。International Building Code が元になっており、IEEE 802.11-2012 Table 8-52 and 8-53 にて参照できますが、機器によっては設定できる値が限られています。
参考までに下記に ArubaOS 8 における記述例を記載します。なお、バージョンによって Venue-Type の記載名に違いがあります。Venue-Type の詳細は各アクセスポイントに搭載されている OS のマニュアルにて確認してください。

Venue Group
- assembly
- business
- educational

- factory-or-industrial
- institutional
- mercantile
- outdoor
- reserved
- residential
- storage
- unspecified
- utility-misc
- vehicular

Venue Type（一例）
- educational-primary-school
- educational-secondary-school
- educational-university
- educational-unspecified
- assembly-library
- assembly-museum
- assembly-restaurant
- business-research-and-development
- institutional-hospital
- residential-boarding-house
- residential-dormitory
- outdoor-bus-stop

ArubaOS 8 におけるコマンド入力例
(host) [md] (config)# wlan anqp-venue-name-profile cityroam
(host) [md] (ANQP Venue Name Profile "cityroam")# venue-name “Research Bldg. 3F”
(host) [md] (ANQP Venue Name Profile "cityroam")# venue-group educational
(host) [md] (ANQP Venue Name Profile "cityroam")# venue-type educational-university
(host) [md] (ANQP Venue Name Profile "cityroam")# venue-lang-code EN

※Operator name は wlan hotspot h2qp-operator-friendly-name-profile で記載します。

(host) [md] (config) #wlan hotspot h2qp-operator-friendly-name-profile cityroam

(host) [md] (H2QP Operator Friendly Name Profile "cityroam") #op-fr-name alansmith university
(host) [md] (H2QP Operator Friendly Name Profile "cityroam") #op-lang-code EN

ローミングコンソーシアム OI の入力
アクセス可能なローミングコンソーシアムと通信事業者の組織識別子を指定します。
WBA OpenRoaming - 5A03BA000
Cisco OpenRoaming - 004096
将来的には WBA OpenRoaming に統一されますが、2022 年現在では旧 Cisco OpenRoaming も使用されていますので、当面の間は入れておいた方がよいです。
eduroam もローミングコンソーシアム OI（001BC50460）を持っていますが、SSID: eduroam を同時に吹いている場合は入力しないでください。

Cisco Meraki における設定例
HotSpot2.0（ホットスポット 2.0）のタブにあるローミングコンソーシアム OI を 1 行毎に改行して入力します。

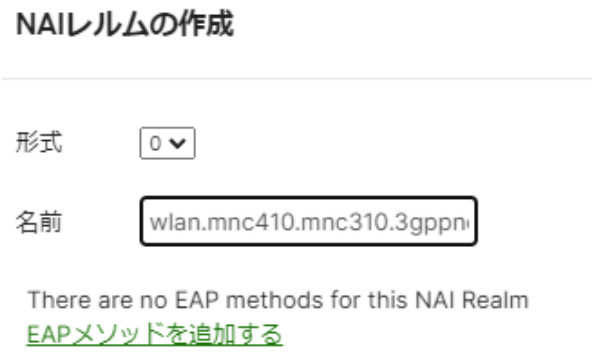
ArubaOS におけるコマンド入力例
※OI の長さを別途定義する必要があります
(host) [md] (config) #wlan hotspot anqp-roam-cons-profile cityroam
(host) [md] (ANQP Roaming Consortium Profile "cityroam") #roam-cons oi 5A03BA0000
(host) [md] (ANQP Roaming Consortium Profile "cityroam") #roam-cons-oi-len 5
(host) [md] (ANQP Roaming Consortium Profile "cityroam") #roam-cons oi 004096
(host) [md] (ANQP Roaming Consortium Profile "cityroam") #roam-cons-oi-len 3

NAI Realms と PLMN の入力
他のローミングプロバイダーやキャリア等と連携する場合に使用します。

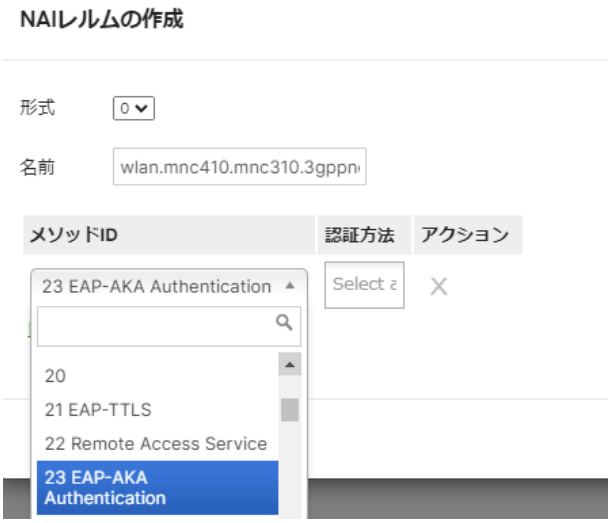
OpenRoaming では NAI Realms と PLMN の入力は必要ありません。

Cisco Meraki における設定例
HotSpot2.0（ホットスポット 2.0）のタブにある NAI Realms の項にある「Realm を作成」ボタンを押し、選択していきます。

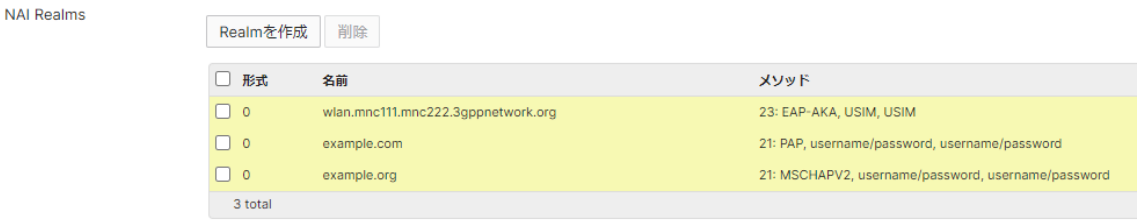
形式（Format）は 0 を選択、名前を入力し、「EAP メソッドを追加する」をクリック。



使用するメソッドの ID を選択します。
ID/Password での接続の場合は「21 EAP-TTLS」、SIM カードでの認証を用いる接続の場合は「23 EAP-AKA」を選択します。



続いて、認証方法を選択します。選択欄の横幅が狭く、選択肢が見づらいので、一度何かを選択し選択欄を広げてから選ぶことをお勧めします。必要のないものは×を押すと削除できます。



SIM カードでの認証を用いる場合は、MCC/MNCs の項目に 3GPP ネットワーク情報を入力します。複数ある場合は 1 行毎に改行します。