

[解 説]

OpenVPN を用いた eduroam/Cityroam/Passpoint 対応
可搬型基地局の開発

後藤英昭

東北大学サイバーサイエンスセンター クラウドサービス基盤研究室

1 はじめに

教育・研究機関向けの国際無線 LAN ローミング基盤である eduroam（エデュローム）は、日本導入から 2019 年 8 月をもって 13 年目を迎えた [1]。現在、国内 260 機関が参加しているが、未参加の大学も多数ある。一方で、国内外ともに、カフェや博物館、空港・鉄道駅などの市街地・公共施設への eduroam 基地局導入が進められている。学術会議が催される会議施設への要望が少なくないものの、なかなか導入が進まないという問題がある。

eduroam 対応基地局のない会議施設や、未参加の大学、未導入部局での一時的利用、試用、デモなどのために、可搬型の eduroam 対応基地局があると便利だと考えられる。しかし、eduroam では利用者認証が必須のため、アクセスポイント (AP) から最寄りの参加機関の認証サーバ (プロキシ) に RADIUS (Remote Authentication Dial In User Service) 連携のための接続が必要であり、基地局の暫定設置には専門知識とネットワーク管理権限が必要になる。このような問題に対処するために、筆者らは 2008 年にセンター管理型キャンパス無線 LAN システムを開発し、図 1 のような可搬型の eduroam 基地局を実現した [2]。この基地局は、DHCP (Dynamic Host Configuration Protocol) とインターネット接続が可能な回線があれば、イーサネットと電源のケーブルを接続するだけで、現地での設定なしに eduroam サービスを提供できる。

このシステムは、学内で全学の eduroam システムが整備される以前の実証実験の段階や、eduroam 基地局が配置されなかった施設での、暫定サービスに用いられた。また、会議におけるデモにも利用された。しかしながら、使用機材の老朽化による故障が目立ってきたことや、Passpoint [3] などの最新技術に対応できないこと、現場のネットワークの制約によって IPsec の通信がブロックされやすいといった問題があった。今回、現代的な技術への対応と可用性の向上、小型化を目指して、後継の可搬型基地局システムを開発した。新しいシステムは、eduroam のみならず、一般市民も利用できるセキュアな無線 LAN ローミング基盤で



図 1 EtherIP 方式可搬型基地局 (2008 年版)

ある Cityroam [4] に対応し、国内外の携帯電話会社 (キャリア) や無線インターネットサービスプロバイダ (ISP) とのローミングにも対応している。通信内容の保護とセンターへの収容には、従来の EtherIP/IPsec に代わり、現地のネットワークでブロックされにくい OpenVPN [5] を採用した。

本稿では、従来の可搬型基地局の概要とユースケースを示した後、新しい可搬型基地局の構成を説明する。なお、この基地局はクラウドサービス基盤研究室で開発し、使用しているものであり、サイバーサイエンスセンターのサービスとして貸出を行っているものではない。従って、本稿の内容は技術紹介に留まる。

2 可搬型基地局とユースケース

2.1 EtherIP 方式の可搬型基地局

SENAC Vol.42 の記事 [2] で既報のとおり、筆者らは EtherIP を利用したセンター管理型のキャンパス無線 LAN システムを開発した。このシステムでは、無線 LAN アクセスポイント (AP) の通信はすべて IPsec で保護された EtherIP のトンネルを通じてセンターのアクセスルータに収容される。AP 側のシステムは、図 1 のように、無線 LAN AP とアクセスルータをセットにしたものである。利用者認証に必要な RADIUS の通信に加えて、利用者の通信も暗号化されてセンターに運ばれるため、設置場所のネットワークにおける盗聴に関して安全である。ただし、AP とア

アクセスルータを結ぶイーサネットケーブルは、通信が暗号化されていないため、利用者が抜き差しできないように物理的な保護が必要である。

AP はイーサネットのレイヤ 2 (L2) でセンターに収容されているため、アクセスルータの EtherIP の接続が確立している状態ならば、センターからウェブブラウザで設定変更も可能である。このため、仮想ネットワークと SSID の追加・削除などもセンターから容易に実施でき、現地に赴く必要がないという利点があった。

2.2 eduroam 基地局の暫定設置

EtherIP 方式では、アクセスルータを接続したネットワークと EtherIP トンネル内のネットワークが論理的に分離されている。このため、前述のように利用者の通信が保護されるのと同様に、トンネル外のネットワークの通信も無線 LAN 利用者から保護される。トンネリング機能のないアクセスポイントを設置する場合は、通常のローカルエリアネットワーク (LAN) とは物理的に独立した、専用の通信ケーブルを敷設するのが一般的である。これに対して、EtherIP 方式では既存のネットワークにアクセスルータを接続しても、通信の安全性が保たれる。この性質を利用して、東北大学では、eduroam に対応した「TAINS 無線 LAN システム」(2010 年) の整備の前後、数年間に渡り、希望する部局に基地局を設置して、eduroam の暫定サービスと試用に役立てた。

実際に基地局が設置された建物は、サイバーサイエンスセンターの他に、附属図書館 (川内)、情報科学研究科、電気通信研究所、マルチメディア教育棟 (川内)、工学部 (電気系) であった。

2.3 会議場における eduroam サービス・デモ

会議場等での暫定サービスに用いられることを想定して、センターでは常に一台の可搬型基地局を「おでかけ用」としてリザーブしていた。しかし、手提げ一つ分の大きさと重量があること、2 系統の AC 電源が必要なことなど、扱いやすいと言えるほどのものではなかった。

また、この基地局を実際に会議場などに持ち込んで利用しようとする、会議場やホテルのネットワークで厳しいアクセス制限がかけられていることがあり、IPsec NAT traversal の通信が透過できず、EtherIP の接続が確立できない問題が時折見られた。このため、関係者以外に利用を呼び掛けることが難しく、利用促進できなかった。

この基地局は会議のために何度か持ち出されたが、

あまり活躍しないまま、休眠状態となった。

2.4 市街地 eduroam 基地局の実証実験

キャンパス外で学生が集まるようなカフェや、博物館、図書館、空港・鉄道駅などの公共施設に eduroam 基地局を設置し、社会全体の教育・研究環境の充実に役立てようという動きが、国内外で活発化している [6]。日本では、2010 年 3 月にライブドア社と国立情報学研究所の共同実証実験として、関東地区の貸し会議施設やカフェの公衆無線 LAN 基地局で eduroam サービスを提供開始した。これは世界の先進事例の一つになり、後継のサービスが現在でも提供されている。2017 年には、公衆無線 LAN のセキュア化と利便性の向上、および、eduroam の市街地展開の推進を目的として、著者が筆頭となって「セキュア公衆無線 LAN ローミング研究会 (NGHSIG)」を立ち上げた [7]。NGHSIG では、一般に「フリー Wi-Fi」と呼ばれる無償の公衆無線 LAN サービスを整備・提供する通信事業者を募り、Cityroam と呼ぶローミング基盤を運営することで、国内各所の民間施設などに eduroam 対応の基地局を整備している。NGHSIG では、国内外の携帯電話会社 (キャリア) や ISP とのローミングも推進しており、参加事業者の基地局ではこれらのアカウントも利用できるようになる。フリー Wi-Fi の永続的な国際ローミング基盤は、執筆時点でまだ立ち上げの段階であるが、Wireless Broadband Alliance (WBA) が過去に実施した City Wi-Fi Roaming trial に NGHSIG も参加し、AT&T や T-Mobile US、Boingo などのアカウントが利用できることを確認済みである。

市街地の eduroam サービスを充実させていく上で、どのような場所に基地局を設置するのが有効かという問いがあった。一方で、ロケーションオーナー (基地局を置く場所の管理人) の協力なくしては、基地局を運用できない。仙台市内で実証実験ができそうな場所を探していたところ、コワーキングスペースが候補に挙がった。利用者に無線 LAN サービスも提供しているということで、第三者利用可能な回線も既にあり、学生や教員も出入りがあるということで、実証実験には最適と思われた。コワーキングスペースとしては、eduroam サービスがあることが集客につながるという期待があった。そこで、仙台市内のコワーキングスペース「ノラヤ」にて実証実験を行うことにした (図 2)。Passpoint 対応の最新仕様の基地局を置きたい気持ちは山々であったが、まだ利用できそうな手頃な製品がなかったことから、学内で回収していた基地局をそのまま流用した。実証実験は 2017 年 3 月から 2019



図2 コワーキングスペースにおける eduroam サービス (2017 年 3 月, ノラヤ様ご協力による)

年 6 月まで実施したが、大学関係者の出入りの多い店舗だったこともあり、eduroam が有効に活用された。期間内に認証 OK になった端末は、ユニーク端末数にして 517 台であった。この数には、店舗前の通行人の分も含まれる。なお、eduroam にはプライバシー保護の仕組みがあり、基地局の管理者は真の利用者を知ることができない。

3 OpenVPN を用いた可搬型基地局

3.1 システム設計の方針

可搬型基地局システムを新規に設計するにあたり、基本的には従来のユースケースを網羅するものの、特に以下を重視することにした。

- 会議における eduroam/Cityroam/Passpoint の一時サービスやデモ。
- 市街地における実証実験のため、店舗などに貸出・設置。

また、従来の仕様を網羅しつつ、特に以下の性質を重視することにした。

- 次世代ホットスポット (NGH) に対応するため、Passpoint (Hotspot 2.0) が利用できること。
- 現場のネットワークで通信がブロックされにくいこと。
- 利用者の通信が、暗号化された状態でセンターにトンネルされること。これにより、基地局の運用者 (ロケーションオーナーなど) が盗聴などの不正行為を働いた場合であっても、サービス利用者の通信が漏洩しないこと (従来同様)。
- センターから基地局の設定変更が可能なこと (従来同様)。
- 台数を増やせること、および、貸出中の紛失・破損の可能性を考慮し、ハードウェアが安価で、で

きればライセンス料が不要であること。

- できれば、有線のイーサネット回線ばかりではなく、携帯データ通信 (LTE) や公衆無線 LAN も上流回線として利用できること。

従来の可搬型基地局では、有線接続しか対応していなかったことから、無線 LAN の設備しかない会場・ホテルなどで利用できないという制約があった。また、無線 LAN の設備すらない会議室もあり、その場合は LTE 回線を利用したいこともある。

価格とライセンス料の制約さえ緩和できるならば、コントローラ型あるいはクラウド型の AP を利用することが考えられる。例えば、Meraki の AP ならば、ネットワークを移動してもクラウドコントローラに自動接続され、どこからでもコントローラのウェブ画面を介して設定変更が可能である。筆者は、実際に何度か Meraki の AP を会議場に持ち込み、デモを行った。Aruba の Remote Access Point (RAP) の場合、現場のネットワークで 443/tcp のポートさえ開いていれば、可搬型基地局として使用できる可能性がある。443/tcp はウェブサイトの HTTPS (Hypertext Transfer Protocol Secure) で広く用いられていることから、インターネット接続を前提とした回線でブロックされることはまずない。コントローラ型のため、AP を一括管理できることや、同じ会場に複数の AP を配置できるという利点もある。しかしながら、エンタープライズ向けの AP は一般に年間ライセンスなどの費用が必要であり、貸出用のように稼働率の低い機器では費用対効果が低くなる。このため、複数台設置による高いスケーラビリティと一括管理を諦めつつ、できるだけ安価な構成を探ることにした。

3.2 使用機材とネットワーク構成

高価なコントローラやライセンス費用が必要ないこと、および、技術基準適合証明等があり国内で使用可能という条件の下、Passpoint (Hotspot 2.0) に対応した AP を探した。Passpoint の動作に定評があり、安価な製品として、Ubiquiti Networks UAP-AC-PRO がある。しかし、同社の製品は同一サブネット内にコントローラとなるコンピュータ、または、Cloud Key と呼ばれる小型デバイスが必要である。このため、一か所に少数台の AP しか置かない場合には、センターからのリモート管理の実現にコストがかかる問題があった。

UAP-AC-PRO と小型アクセッスルータを組み合わせ、L2 でセンターに収容する方式も、実際に組み立て



図3 UAP-AC-PRO を用いた可搬型基地局の試作機



図5 hAP ac を利用した可搬型基地局 (2019 年版)

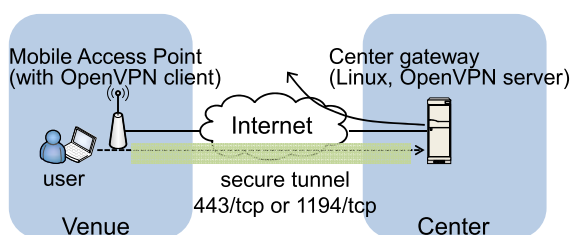


図4 OpenVPN による基地局収容

て評価を行った。必要な機能は実現できたものの、図3のように筐体が複数でケーブルも多くなることから、利便性・携帯性の観点で少し難があった。

もう一つの候補として、MikroTik hAP ac があった。同製品の Passpoint 機能は、設定のためのインタフェースがまだ洗練されておらず、試験的なレベルと言える [8]。しかしながら、2018 年の City Wi-Fi Roaming で運用実績ができたことから、今回はこちらを採用することにした。

hAP ac は、小型・高機能のルータが主機能で、これに 2.4GHz/5GHz デュアルバンドの無線 LAN 機能が搭載されている。家庭向けのルータと同様の使い方も可能であり、上流回線の接続には、PPPoE に加えて L2TP/IPsec や OpenVPN が利用できる。可搬型基地局では、現場のネットワークでブロックされにくいことを考慮して、OpenVPN を採用した。図4に、OpenVPN を利用した端末・AP のセンター収容の様子を示す。OpenVPN の標準的な構成では、ポート 1194/udp が用いられるが、hAP ac に搭載の RouterOS v6 で OpenVPN 機能が UDP に非対応のため、1194/tcp を用いる。また、アクセス制限されにくい 443/tcp を使うことも考慮する。

利用者の通信はすべて、OpenVPN の暗号化トンネルを通じてセンターのゲートウェイに接続され、そこで NAT (Network Address Port Translation) を介してインターネット上の様々なサイトに接続される。

可搬型基地局は、センター側で設定をすべて行った上でロケーションオーナーや会議運営者などの基地局運用者に貸し出し、管理権限は渡さない。このため、運用者が利用者の通信内容を盗み見ることは困難である。図5に、hAP ac による可搬型基地局の外観を示す。hAP ac では、平文の流れる通信線が外に出ていない点も、通信の保護の観点で有利である。

OpenVPN では、L2VPN によるブリッジ接続も可能であるが、この用途では L2 接続が必要ではないこと、および、スケーラビリティを優先させたいことから、L3VPN を採用した。利用者端末は hAP ac 内蔵の DHCP サーバから IP アドレスを取得し、内蔵の NAT を介して OpenVPN のトンネルに接続される。利用者認証のための内蔵 RADIUS クライアントも、同じ OpenVPN のトンネルを通じて、センターのゲートウェイに接続される。hAP ac の WAN 側端子は現場の LAN に接続され、DHCP により IP アドレスを取得するが、このアドレスが変わっても、内蔵 OpenVPN クライアントの設定変更は必要ない。

3.3 センター側の OpenVPN サーバ

複数台の可搬型基地局の通信を集約する、センター側のサーバは、PC と Linux を用いて構築した。サーバ上では、OpenVPN と RADIUS proxy を動かしている。RADIUS proxy は NGHSIG の JP hub に接続され、eduroam や Cityroam、キャリア/ISP と認証連携している。可搬型基地局は、OpenVPN クライアントに相当するが、個体ごとに個別のクライアント証明書を発行して、証明書認証を行うようにした。サーバ上にトンネル (tun) デバイスを設定し、24 ビットネットマスクのプライベートアドレスのサブネットを設けて、OpenVPN の複数のトンネルを収容している。すなわち、複数台の可搬型基地局がこの一つのサブネットに収容されることになる。

クライアント証明書のユーザ名ごとに、トンネルに

固定 IP アドレスを割り当てるようにした。これにより、可搬型基地局とその IP アドレスの対応が固定され、どこに設置された基地局から RADIUS の Access-Request メッセージが送られてきたのかを、サーバ側で容易に知ることができる。また、サーバ上のウェブブラウザや Secure Shell コマンドを用いて、特定の可搬型基地局をリモート操作できる。これらは、利用統計やシステム管理の観点で、大きな利点である。

参考までに、Code 1 に OpenVPN のサーバ側設定ファイルの例を示す。ccd ディレクトリの中には、ユーザ名をファイル名として、Code 2 のような内容のテキストファイルを置く。この例では、hAP ac にアドレス 172.30.2.14 が割り当てられる。

Code 1 tun.conf

```

1 dev tun0
2 proto tcp
3 port 1194
4 tun-mtu 1400
5
6 ca /etc/openvpn/keys/ca.crt
7 cert /etc/openvpn/keys/server.crt
8 key /etc/openvpn/keys/server.key
9 dh /etc/openvpn/keys/dh.pem
10
11 server 172.30.2.0 255.255.255.0
12 ifconfig-pool-persist ipp.txt
13
14 cipher AES-256-CBC
15 keepalive 10 60
16 #comp-lzo
17 persist-key
18 persist-tun
19
20 client-config-dir ccd
21 push "redirect-gateway"
22
23 verb 3

```

Code 2 ccd/map14-user

```

1 ifconfig-push 172.30.2.14 172.30.2.13

```

3.4 性能評価

実装した可搬型基地局 3 台を、研究室の別サブネットや、住宅の DSL (Digital Subscriber Line) に接続して、自動的に正しく OpenVPN の接続が完了し、利用者認証が正常に行われて端末から通信可能になることを確認した。いずれの場所でも下り 20～28Mbps の速度が得られた。無線 LAN 機能や DSL の



図6 新旧基地局のサイズ比較

速度からは見劣りするが、10 台程度の端末数ならば実用になると思われる。

同じハードウェア構成で OpenVPN の代わりに L2TP/IPsec による実装も試してみたが、速度が僅かに劣る上に、IPsec のトンネルが時折リンクダウンすること、その復旧に時間を要するという問題があった。従って、この用途とハードウェア構成では、OpenVPN の方が適切である。

図 6 に、新旧の可搬型基地局を並べて示す。新型は本体 (114 × 137 × 29mm) ・ AC アダプタともに小さく、軽量で、旧型より携帯性が大幅に向上した。なお、MikroTik hAP ac シリーズには、さらに小型の hAP ac lite があり、hAP ac の 3/5 程度のサイズであるが、執筆時点で技術基準適合証明等がなく、国内利用が難しい。

3.5 LTE や公衆無線 LAN の利用

hAP ac には USB2.0 ポートがあり、RNDIS (Remote Network Driver Interface Specification) に対応した機器ならば、ネットワーク機器として認識できることがある。モバイルルータ NEC MR05LN を接続してみたところ、自動的に lte1 デバイスとして認識されて、有線ネットワークの代わりに LTE 回線をバックホールとして利用できることが確認できた。ただし、可搬型基地局をこのような構成で不特定多数に使用させる場合は、SIM カード契約の利用条件に注意が必要である。

Android スマートフォンにも、同様にネットワーク機器として利用できるものがある。さらに、一部機種には Wi-Fi ブリッジなどの機能があり、現場の無線 LAN 設備の仕様によっては、無線 LAN を可搬型基地局のバックホールとして利用できることがある。

<https://pirosap.booth.pm/items/1217350>

4 むすび

従来の EtherIP 方式の可搬型 eduroam 基地局が老朽化したことから, eduroam/Cityroam/Passpoint に対応した新しい可搬型基地局のシステムを開発した. EtherIP/IPsec に代わり, OpenVPN を採用することで, 会議場やホテル, 店舗の DSL などの回線でブロックされにくいネットワーク構成とした. 新型の可搬型基地局は, 小型・軽量の無線 LAN 機能付きルータのみで構成されており, 携帯性が向上している. また, Cityroam を介して国内外のキャリア/ISP のローミングにも対応し, 会議などにおける利用者の幅を広げている.

開発した可搬型基地局は, センターの業務としての貸し出しは行っていないが, 筆者の研究プロジェクトの範囲内で, モニタのための貸し出しは可能である. 今後, 市街地の店舗などでも試用を行い, セキュアな公衆無線 LAN の普及のための技術・運用開発に役立てる予定である.

参考文献

- [1] eduroam JP, <https://www.eduroam.jp/>
- [2] 大和純一, 若山永哉, 後藤英昭, 曾根秀昭, “EtherIP を用いたセンター管理型キャンパス無線 LAN,” 東北大学サイバーサイエンスセンター大規模科学計算システム広報 SENAC Vol.42, No.1, pp.137–144, 2009.
- [3] Wi-Fi Alliance, “Passpoint – Wi-Fi ホットスポットネットワークへのシームレスでセキュアな接続を実現,” <https://www.wi-fi.org/ja/discover-wi-fi/passpoint/>
- [4] 原田寛之, 後藤英昭, “学術無線 LAN ローミング基盤 eduroam と次世代ホットスポット基盤 Cityroam のキャンパスへの展開,” 大学 ICT 推進協議会 2018 年度年次大会 論文集 MA1-5, 2018.
- [5] OpenVPN, <https://openvpn.net/>
- [6] 後藤英昭, 中村素典, 曾根秀昭, “デジタル時代の教育・研究を支える基盤としての eduroam と次世代ホットスポット,” 大学 ICT 推進協議会 2017 年度年次大会 論文集 TC2–5, 2017.
- [7] セキュア公衆無線 LAN ローミング研究会 (NGH-SIG), <https://nghsig.jp/>
- [8] Harada Hiroyuki, “Passpoint による Wi-Fi 環境の構築と運用– Passpoint (Hotspot 2.0) Knowledge Book –,” 2019.