

キャンパス外 eduroam と大学における OpenRoaming 導入

後藤英昭¹⁾, 原田寛之²⁾, 漆谷重雄³⁾

1) 東北大学 サイバーサイエンスセンター

2) 札幌学院大学 情報処理課

3) 国立情報学研究所

Off-campus eduroam and Deployment of OpenRoaming at Universities

Hideaki Goto¹⁾, Hiroyuki Harada²⁾, Shigeo Urushidani³⁾

1) Cyberscience Center, Tohoku University

2) Information Processing Division, Sapporo Gakuin University

3) National Institute of Informatics

概要

学生や生徒、教職員の学習・教育・研究環境を改善するために、キャンパスのみならず市街地でも eduroam のサービスを提供したいという要求があり、各国が様々な枠組みで対応してきた。これと反対に、他大学からの訪問者に限らず、より広く、市民の学習環境の改善のために、キャンパスに公衆無線 LAN を導入する事例も増えてきている。筆者らは、社会全体の ICT 対応推進という側面を踏まえて、従来型のキャンパス無線 LAN と公衆無線 LAN の間の垣根を減らした、新しい無線 LAN インフラのあり方を提唱してきた。Wireless Broadband Alliance (WBA) により運用が始まった OpenRoaming は、同組織の次世代ホットスポットのコンセプトを具現化した無線 LAN ローミング基盤であり、筆者らもその初期の開発段階から参画している。eduroam と OpenRoaming の連携のために、eduroam の運用母体である GÉANT において相互運用の検討が進められ、試験運用ができる状態になった。本報告では、OpenRoaming 基地局で eduroam を有効にする方法と、キャンパスに OpenRoaming を導入する方法について、最新動向と実践的な技術情報の提供を行う。

1 はじめに

教育・研究機関向けの無線 LAN ローミング基盤である eduroam (エデュローム) は、執筆時点 (2021 年 9 月) で世界 106 か国 (地域)、国内 313 機関に導入されるに至っている [1]。初等・中等教育機関についても、海外では既にいくつかの国で導入が進み、社会全体の学習・教育環境の ICT 対応が進められている [2]。学生や生徒、教職員の学習・教育・研究環境を改善するために、キャンパスのみならず市街地でも eduroam のサービスを提供したいという要求があり、各国が様々な枠組みで対応してきた [3, 4]。この種のサービスは、ここ数年でよく“off-campus eduroam”と呼ばれるようになった。これと反対に、他大学からの訪問者に限らず、より広く、市民の学習環境の改善のために、キャンパスに公衆無線 LAN を導入する事例も増えてきている。2020 年度年次大会 [2] で既

報のとおり、筆者らは、社会全体の ICT 対応推進という側面を踏まえて、従来型のキャンパス無線 LAN と公衆無線 LAN の間の垣根を減らした、新しい無線 LAN インフラのあり方を提唱している。Wireless Broadband Alliance (WBA) により運用が始まった OpenRoaming [5] は、同組織の次世代ホットスポットのコンセプトを具現化した無線 LAN ローミング基盤であり、筆者らもその初期の開発段階から参画している。また、国内では、eduroam と OpenRoaming を包含する形の、Cityroam [6] と呼ぶローミング基盤を開発・運用している (図 1)。eduroam の運用母体である GÉANT において、OpenRoaming との相互運用の検討が進められ、試験運用ができる状態になった。本報告では、各機関が市街地等の OpenRoaming 基地局からの eduroam 接続を受け入れる方法と、自機関のキャンパスに OpenRoaming を導入する方法の二点について、最新動向と実践的な技術情報の提供を行う。



図1 Cityroam ウェブサイト (2021年9月).

2 OpenRoaming 基地局からの eduroam 利用の有効化

2.1 概要

本章では、利用者が eduroam のアカウントを用いて OpenRoaming の基地局に接続できるようにするための、各機関で必要な対応方法を示す。従来の eduroam では、“eduroam” という共通の SSID (Service Set Identifier) が用いられており、この SSID を吹いている基地局ではすべての eduroam アカウントが利用できるように、eduroam Compliance Statement に規定がある。これに対して、OpenRoaming 上で eduroam アカウントを使う場合は、ID プロバイダ (IdP) となる各機関で、オプトインが必要である。

eduroam 参加機関が、OpenRoaming 上での eduroam 利用を有効化するには、OpenRoaming からの認証要求が自機関の ID プロバイダ (IdP) まで届くように、認証経路を設定する必要がある。図2に、eduroam と OpenRoaming の認証連携の様子を示す。左図が、OpenRoaming からの認証要求を受け付ける様子であり、上部の雲の中にある IdP が各機関に相当する。OpenRoaming の認証連携では、全面的に RadSec [7] を用いた Peer-to-Peer 的なルーティングが行われるが、各機関の IdP 自身、または、その途中にあるゲートウェイ (プロキシ) が RadSec エンドポイントになる必要がある。RadSec エンドポイントにはサーバ証明書が必要であり、これは OpenRoaming

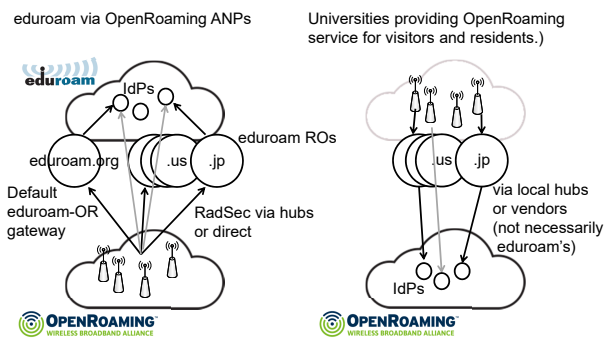


図2 eduroam と OpenRoaming の認証連携.

のブローカーとなる組織から発行される。

2.2 eduroam の基盤を用いた接続

eduroam の国際的な運用母体である GÉANT と、国内のセキュア公衆無線 LAN ローミング基盤である Cityroam は、2020 年春に、OpenRoaming に初期サポートメンバーとして参加した。現在、GÉANT は WBA の Contributor Member であり、OpenRoaming においてブローカーの権限も有している。このため、国際的な eduroam としては、そのメンバーに対して RadSec 用電子証明書の発行も可能である。eduroam メンバーの具体的な OpenRoaming 参加方法はまだ Global eduroam Governance Committee (GeGC) で検討中であるが、各国のオペレータが希望すれば、国単位で大学等の OpenRoaming 利用が可能なる段階にある。

国内の eduroam 参加機関が、OpenRoaming からの接続を受け入れたい場合、RadSec エンドポイントとして、以下のような選択肢が考えられる。

- 自機関の proxy を使う。(証明書の取得が必要)
- eduroam (国際) の proxy を使う。
- 国内の eduroam proxy を使う。
- その他の事業者の proxy を使う。

現在、国内の eduroam 運用組織である eduroam JP (国立情報学研究所) では、OpenRoaming の扱いが決まっていない。また、各機関が証明書を取得するためには、eduroam の国際運用組織への申請が必要となるが、これには各国の代表組織による取次が必要となる。その他の事業者として、現在、国内では Cityroam が eduroam JP 宛ての認証要求を中継できる。従って、現時点で利用できるのは、eduroam (国際) 経由、または、Cityroam 経由の接続のみである。

OpenRoaming 上で eduroam アカウントを有効にしたい機関は、RadSec で利用される NAPTR

(Naming Authority Pointer) レコードを自機関の DNS (Domain Name System) サーバに追加する必要がある。OpenRoaming の ANP (Access Network Provider. eduroam の SP に相当) は、認証要求に含まれるレルムを元に DNS で名前解決を行い、実際にサービスを提供しているサーバのアドレス (ここではプロキシの IP アドレス) を求める。

2.3 Cityroam 経由の接続

執筆時点で、Cityroam は OpenRoaming に接続済みであり、eduroam JP の参加機関もトライアルが可能である。Cityroam を中継点とする場合、具体的には、以下のようなレコードを登録すればよい。(機関側で SRV レコードの登録は不要)

```
<レルム> IN NAPTR 50 50 "s"
      "aaa+auth:radius.tls.tcp" ""
      _radiustls._tcp.idp.cityroam.jp.
```

どのようにしてプロキシのアドレスが取得されるのか、dig コマンドを用いて具体例を見ることができる。

```
$ dig naptr cityroam.jp
$ dig srv _radiustls._tcp.jpgw.cityroam.jp
```

Cityroam 経由の接続を行う場合、事前の報告は不要であるが、長期間利用にはご一報いただきたい。

2.4 接続用プロファイル

OpenRoaming の利用には、Passpoint [8] に対応した端末と、Passpoint プロファイルが必要である。各機関でこのプロファイルを発行するシステムを用意するのは難しいと考えられるが、幸いなことに、eduroam CAT (Configuration Assistant Tool) が既に対応しており、従来の eduroam のプロファイルに加えて、OpenRoaming 用のプロファイルも端末に同時インストール可能となっている。

2.5 サービスエリア

Cityroam では eduroam の SSID も併設することを基本としているため、Cityroam 基地局で OpenRoaming 経由の接続を試すには、eduroam SSID 用のプロファイルを削除する必要がある。もちろん、実際の利用については eduroam SSID の方が簡便なため、わざわざ OpenRoaming 経由で利用する必要はないと言える。

国際的にも OpenRoaming は黎明期にあり、サービスエリアが少ない。今後、観光の復活に伴って徐々に対応基地局が増えることが期待されている。国内でも、Cityroam 以外の基地局が増えてくれば、OpenRoaming 経由の接続が有用になってくると予想さ



図 3 新宿中央公園の Cityroam 対応スマートポール (東京都デジタルサービス局)。

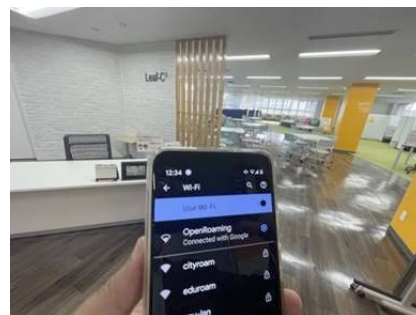


図 4 札幌学院大学における OpenRoaming。

れる。

図 3 は、東京都が実証実験中のスマートポールの例で、eduroam と Cityroam に加えて、OpenRoaming にも対応した基地局が内蔵されている。国際ローミングに対応したこのような公衆無線 LAN サービスが、国内外で普及することを願っている。

3 自機関への OpenRoaming 導入

大学等が OpenRoaming 対応の基地局を導入して市民向けの公衆無線 LAN サービスを提供する方法を紹介する。図 2 の右側に、機関が OpenRoaming ANP となる場合の認証連携の様子を示す。左図の上部の雲は eduroam の基盤を表しているが、右上の雲は eduroam ではなく、OpenRoaming のものである。OpenRoaming のサービスを提供する機関は、OpenRoaming に参加する必要がある。

前章で述べたように、eduroam は全体として既に OpenRoaming に参加している。しかしながら、各国のオペレータは eduroam の運用組織であり、市民一般を受け入れるような OpenRoaming 基地局の運用は管轄外である。eduroam の認証連携ネットワークに、OpenRoaming の認証要求をそのまま重畳させることは、技術的に困難である。

現在、大学等が OpenRoaming の基地局を導入するには、以下のような方法がある。

- ハブ事業者経由で OpenRoaming の認証連携基盤に接続する。
- OpenRoaming に対応した無線 LAN 事業者 (通信事業者) に基地局システムの運用を委託する。
- 機関自身が OpenRoaming に参加する。
- Cisco DNA Spaces のような、OpenRoaming が統合された無線 LAN システムを導入する。

機関自身がブローカーを通じて OpenRoaming に参加する方法がある。しかし、現時点でこれに対応できる国内のブローカーは知られていない。ブローカーとしての eduroam から RadSec の証明書を取得することも考えられるが、現時点ではまだ eduroam に運用の枠組みがなく、計画も未定である。

もし、機関自身が運用している基地局に OpenRoaming のサービスを追加するのであれば、Cityroam 経由で OpenRoaming に接続するのが最も簡便と考えられる。この場合、Cityroam がハブ事業者として機能する。自前で基地局を運用する必要がないのであれば、通信事業者に業務委託する方法が、安定性でも管理・運用面でもメリットがあると考えられる。

図 4 は、札幌学院大学のキャンパスに導入した OpenRoaming の例である。認証連携には、Cityroam の基盤を利用している。OpenRoaming では様々な機関のアカウントが利用できるが、最近よく利用されているのは、Google や Apple, Samsung のアカウントを用いてサインアップできる、OpenRoaming 用アカウントである。

OpenRoaming に使うバックホール回線には、市民のトラフィックを流せるものが必要となる。詳しくは 2020 年度の報告 [2] をご覧いただきたい。

4 むすび

本報告では、OpenRoaming 基地局で eduroam を有効にする方法と、キャンパスに OpenRoaming を導入する方法について、最新動向と実践的な技術情報を示した。市民向けの国際無線 LAN ローミング基盤である OpenRoaming を用いると、eduroam のアカウントを用いて、市街地等の基地局で安全な無線 LAN 利用が可能となる。これを実現するためには、機関ごとのオプトインが必要である。キャンパス内に OpenRoaming 対応の基地局を導入する場合、各機関は OpenRoaming の認証連携ネットワークに参加する

必要がある。筆者らが開発・運用している Cityroam 基盤では、eduroam と OpenRoaming を統合した認証連携基盤を提供しており、eduroam JP の参加機関であれば、OpenRoaming の試行も可能である。

地域社会への貢献や災害対応などの観点で、学校や図書館等公共施設への安全な公衆無線 LAN の導入が望まれている。今後、国内外の通信事業者とのローミングを充実させ、利用できるアカウントとサービスエリアの拡充を図っていく予定である。

本研究の一部は、令和 3 年度国立情報学研究所公募型共同研究の助成を受けた。

参考文献

- [1] eduroam JP: <https://www.eduroam.jp/> (2021 年 9 月 27 日参照)
- [2] 後藤英昭, 原田寛之, 漆谷重雄, “キャンパス無線 LAN と公衆無線 LAN の統合 – eduroam と Cityroam, OpenRoaming –,” 大学 ICT 推進協議会 2020 年度年次大会 論文集 WA2-1, 2020.
- [3] GÉANT NETWORKS, “eduroam: Bringing City-Wide Wi-Fi Roaming Access to Cape Town.” https://impact.geant.org/portfolio/eduroam_capetown/ (2021 年 9 月 27 日参照)
- [4] eduroam Everywhere: <https://www.heanet.ie/services/connectivity/eduroam-everywhere> (2021 年 9 月 27 日参照)
- [5] WBA OpenRoaming: <https://wballiance.com/openroaming/> (2021 年 9 月 27 日参照)
- [6] Cityroam: <https://cityroam.jp/> (2021 年 9 月 27 日参照)
- [7] S. Winter and M. McCauley, “Dynamic Peer Discovery for RADIUS/TLS and RADIUS/DTLS Based on the Network Access Identifier (NAI),” IETF RFC7585, 2015. <https://tools.ietf.org/html/rfc7585> (2021 年 9 月 27 日参照)
- [8] 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/> (2021 年 9 月 27 日参照)