

キャンパス無線 eduroam と次世代ホットスポットの最新動向

後藤英昭¹⁾, 原田寛之²⁾, 中村素典^{3,4)}

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) 京都大学 情報環境機構

4) 国立情報学研究所

Updates on eduroam and the Next Generation Hotspot

Hideaki Goto¹⁾, Hiroyuki Harada²⁾, Motonori Nakamura^{3,4)}

1) Cyberscience Center, Tohoku University

2) Information Processing Division, Sapporo Gakuin University

3) Institute for Information Management and Communication, Kyoto University

4) National Institute of Informatics

概要

教育・研究機関向けの無線 LAN ローミング基盤である eduroam は、2019 年 9 月時点で世界 101 か国(地域)、国内 263 機関に導入されるに至っている。学生の学習・研究環境の充実のために、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 導入も進められている。国内では、2010 年に関東地域の貸し会議施設やカフェなどで市街地 eduroam サービスの実証実験が行なわれ、近年では一般市民向けの次世代ホットスポット (NGH) と融合する形で、eduroam 対応基地局の設置が各地で進められている。現在、世界では NGH によるフリー Wi-Fi の国際ローミング基盤の立ち上げが進められており、筆者らもプロジェクトに参画している。その準備として開催されてきた City Wi-Fi Roaming トライアルに、2018 年も参加することで、eduroam サービスの連携技術を確認するとともに、連携の有効性を確認した。

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、2019 年 9 月時点で世界 101 か国(地域)、国内 263 機関に導入されるに至っている [1]。2017 年度年次大会 [2] で既報のとおり、学生の学習・研究環境の充実のために、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 導入も進められている。国内では、2010 年に関東地域の貸し会議施設やカフェなどで市街地 eduroam サービスの実証実験が行なわれ [3]、企業の社会貢献の一環として現在でもその一部が継続し、利用者から好評を博している。近年では一般市民向けの次世代ホットスポット (NGH) と融合する形で、eduroam 対応基地局の設置が各地で進められている [2]。

筆者らは、2017 年に Wireless Broadband Alliance (WBA) による City Wi-Fi Roaming トライアル [4] に参加することで、世界で初めて eduroam を NGH

と接続し、公衆無線 LAN に eduroam サービスを容易に乗せられるような枠組みとその有効性を示した。また、2018 年度年次大会 [5] で一部報告したが、2018 年のトライアルにも参加して、NGH における eduroam の実用化を推進した。

本稿では、2018 年から 2019 年にかけての次世代ホットスポットの最新動向を紹介する。また、eduroam の市街地サービスが、大学におけるサービスと同様のセキュリティを有していることを解説する。

2 セキュア無線 LAN ローミング基盤 Cityroam

公衆無線 LAN で広く用いられているオープン Wi-Fi やキャプティブポータルには、セキュリティ上の重大な問題が多数あることから、海外ではフリー Wi-Fi であっても IEEE 802.1X (以下、1X 認証) や Passpoint によるセキュア接続オプションを併設する例が見られる。Passpoint にローミングを組み合わせた全体的なコンセプト仕様が、次世代ホットスポット



図 1 Cityroam 基地局マップ (2019 年 9 月)

(Next Generation Hotspot, NGH)) と呼ばれる。

国内の公衆無線 LAN のセキュア化と NGH 導入を推進する目的で、第一著者が発起人となり、2017 年 1 月に「セキュア公衆無線 LAN ローミング研究会 (NGHSIG)」が発足した [6]。2018 年度、当研究会では、参加企業や開発者を増やししながら複数の通信事業者と協働で国内各地に次世代フリー Wi-Fi の整備を進めた。このローミング基盤を Cityroam と命名し、国内外で広報及び技術紹介を行った。Cityroam の基地局マップを図 1 に示す。Cityroam の認証連携基盤は eduroam にも接続されており、いずれの基地局においても eduroam の SSID を吹くことを標準仕様としている。これにより、大規模ショッピングモールやホテル、北九州モノレールの各駅、スキーリゾートなどで、eduroam 及び Cityroam の両サービスが実現した。

3 City Wi-Fi Roaming trial 2018

現在、世界では NGH によるフリー Wi-Fi の国際ローミング基盤の立ち上げが進められており、WBA によるものや、Cisco OpenRoaming [7] などがある。筆者らはこれまで、WBA のプロジェクトに参画してきた。WBA で NGH ベースのローミング基盤の準備として開催されてきた City Wi-Fi Roaming トライアルに、2018 年も NGHSIG 名義で参加することで、eduroam サービスの連携技術を確立するとともに、連携の有効性を確認した。また、世界の通信事業者及び都市と協働で、NGH 基盤の構築に貢献した。同トライアルへの参加は、GÉANT と WBA の間の MoU (Memorandum of Understanding) を利用したものであり、eduroam を Passpoint/NGH に対応させ、世界のフリー Wi-Fi に乗せるための技術・運用開発を、世界の eduroam コミュニティをリードする形

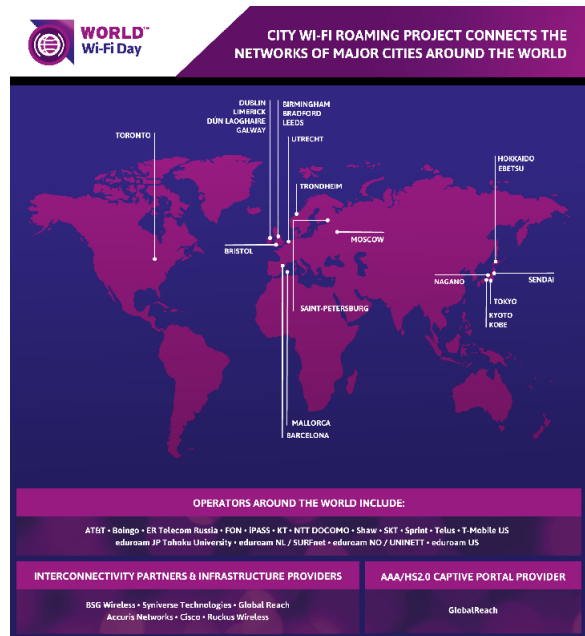


図 2 WBA City Wi-Fi Roaming 2018 (©Wireless Broadband Alliance)

で NGHSIG が実施したものである。前年度のトライアルの実績に基づいて、2018 年には他国にも参加を呼びかけ、ノルウェーとオランダ、米国の参加が実現した。

同トライアルの参加都市のマップを図 2 に示す。前年には国内に実験的な基地局を数か所しか用意できなかったが、2018 年には Cityroam の基地局も充実してきており、世界的に見ても最先端のサービスを多数のサービスエリアで提供することができた。

Cityroam の基地局では、常設している eduroam と国内ローミングに加えて、同トライアルの期間内には AT&T、T-Mobile US などの SIM 認証、及び、Boingo のローミングが利用可能であった。

現在、永続的な NGH 対応国際ローミングのフェデレーションが WBA において準備中であり、2019 年内に立ち上がる見込みである。この準備に位置付けられていた City Wi-Fi Roaming トライアルは、第 3 回となる 2018 年をもって終了することとなった。

4 Cityroam を利用した会議用無線 LAN と可搬型基地局

Cityroam の認証連携基盤は eduroam を統合する形で開発されている。同基盤に無線 LAN 基地局を接続することで、eduroam を含む NGH の各種ローミングサービスを、利用者に容易に提供できる。この仕組みを利用して、大学 ICT 推進協議会年次大会 (AXIES)

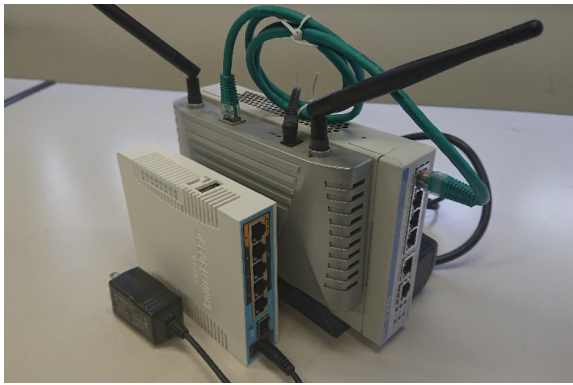


図3 左：OpenVPN方式可搬型基地局(2019年版)
と右：EtherIP方式可搬型基地局(2008年版) ([9]
より)

や Internet Week 2018 などの会議を支援した。これにより、一時的に設置する基地局でも様々な通信事業者のアカウントを受け入れられるローミング環境を容易に実現できる仕組みを実現し、その有用性を確認した。

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 3 (右) のような可搬型の eduroam 基地局を実現した [8]。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。

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/NGH 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。そこで、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 [9]。図 3 に、新旧の可搬型基地局の様子を示す。新型では MikroTik 製の小型ルータ hAP ac を使用しており、本体 (114 × 137 × 29mm)・AC アダプタとも小さく、軽量で、旧型より携帯性が大

幅に向上した。

新しいシステムは、Cityroam の認証連携基盤を利用することで、一般市民も利用できるようになり、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 を採用した。ただし、OpenVPN とハードウェアの性能がボトルネックとなり、通信速度は実測値で下り 20 ~ 28Mbps 程度であった。10 台程度の端末数ならば実用になると思われるが、大人数での利用には別方式も検討が必要である。

Cityroam の認証連携基盤の枠組みは、会議等のイベントに限らず、災害時の避難所等の一時的な無線 LAN サービスの構築にも応用できると考えられる。

5 市街地 eduroam サービスのセキュリティ

国内外に限らず、大学キャンパス外の市街地・店舗などで eduroam が利用できることに気づいた利用者が、大学でもない所にあるのは正規の基地局だろうかとの不安を twitter などに書き込んでいることがある。盗聴や中間者攻撃などのセキュリティ問題を気にしているなら、このような疑問が生じることは自然であろう。

結論から述べると、教育・研究機関のキャンパス内とその外で、eduroam サービスのセキュリティに大差はない。eduroam や Cityroam では、1X 認証の EAP (Extensible Authentication Protocol) [10] が用いられており、認証の安全性はこれに基づいている。これらのサービスでは、利用者認証の実現のために、基地局が認証連携ネットワークに接続されている必要がある。この接続は誰でもできるようなものではなく、基地局の運用者が eduroam や Cityroam の運営者に対してまずローミング基盤への参加申請を行い、それが認められた上で、共通鍵ないし電子証明書を用いて基地局を認証連携ネットワークに接続する必要がある。大学であれば、大学の情報部門やそこから委託された業者が基地局の運用を行う。キャンパス外のサービスの場合は、通信事業者がこの役割を担っており、事業者ではない個人がローミング基盤に参加することは認められていない。すなわち、正規の運用者でなければ、正しく動作する eduroam 基地局を設置することはできない。

偽の基地局について、市街地の方が設置が容易と考えられるが、大学キャンパスであっても、立ち入りが

可能な場所であればそれほど難しいことではないと言える。もし利用者端末が偽基地局に接続させられるようなことがあれば、中間者攻撃などが可能となる。1X 認証では、利用者認証に先立ってサーバ証明書の検証が可能であり、この機能によって偽基地局を見破ることができ、端末を保護できる。偽基地局は、正規の認証連携ネットワークに接続されていないため、利用者の所属する機関の認証サーバに認証要求を送ることができず、端末にサーバ証明書の検証を成功させることができない。

ただし、現在の eduroam の運用では、端末の設定でサーバ証明書の検証を有効にしない利用方法も広く用いられている。iOS のように、明示的に有効にしないで、ある種の保護機能が働く環境もある。クライアント証明書を用いる EAP-TLS 方式では、攻撃者が正規利用者の認証情報を奪取することは困難である。一方、PEAP 方式には脆弱性が見つかっており、巧妙に細工された偽基地局によってパスワードが攻撃者に漏洩する恐れがある。従って、キャンパス内外を問わず、安全性の向上のために、サーバ証明書の検証を有効にすることが推奨される。

上記の脆弱性の影響範囲や、具体的な対策については、本稿のテーマを超えることから、eduroam JP 事務局から発行される情報などを参照していただきたい。

6 むすび

本稿では、eduroam を中心とした次世代ホットスポットの最新動向を紹介した。教育・研究関係以外の一般市民でも利用できるセキュアな無線 LAN ローミング基盤 Cityroam の展開が国内で進められており、これには eduroam も統合されていることから、eduroam の市街地サービスが充実してきている。

大学ではこれまで eduroam の導入が進められてきたが、eduroam のアカウントは教育・研究機関でしか発行できないことから、学術的な活動であるにも関わらず、企業の研究者や個人の学会員などが利用できないという問題があった。市民に開かれた大学として、生涯教育の環境改善を進めるという視点で、大学のキャンパス無線 LAN システムであっても、教育・研究機関以外の一般市民に利用を開放するという方向性も今後検討していく必要があると考えられる。

本研究の一部は、平成 30 年度、平成 31 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/> (2019 年 9 月 19 日参照)
- [2] 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.
- [3] “ライブドアと NII、学術無線 LAN ローミング基盤の共同実験を開始,” INTERNET Watch, 2010.3.9. <https://internet.watch.impress.co.jp/docs/news/353536.html> (2019 年 9 月 19 日参照)
- [4] City Wi-Fi Roaming: <http://worldwifiday.com/city-wi-fi-roaming/> (2019 年 9 月 19 日参照)
- [5] 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.
- [6] セキュア公衆無線 LAN ローミング研究会 (NGH-SIG): <https://nghsig.jp/> (2019 年 9 月 19 日参照)
- [7] Cisco OpenRoaming: <https://openroaming.org/> (2019 年 9 月 19 日参照)
- [8] 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.
- [9] 後藤英昭, “OpenVPN を用いた eduroam/Cityroam/Passpoint 対応可搬型基地局の開発,” 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.52, No.4, 2019.
- [10] B. Aboba, et al., “RFC3748: Extensible Authentication Protocol (EAP).” <https://tools.ietf.org/html/rfc3748> (2019 年 9 月 19 日参照)