キャンパス無線 eduroam の国内外の最新動向 ― 利便性と耐障害・耐災害性の向上 ―

後藤 英昭, 曽根 秀昭

東北大学 サイバーサイエンスセンター
{hgot,sone}@isc.tohoku.ac.jp

概要： 学術系の無線 LAN ローミング基盤である eduroam は，国内では 2012 年度末の 43 機関から 56 機関 (2013 年 10 月現在) に成長し，国際的にも新規参加国が相次いでいる．欧州では大学以外にも病院，空港・駅，博物館などでサービス提供される例が見られ，応用が広がってきている．また，端末の設定を自動化するツールや，世界の eduroam 基地局マップの開発など，利便性の改善も進められている．本報告では，eduroam の最新状況を概説するとともに，利便性の向上策と，耐障害・耐災害性を実現する新しい認証サービスの開発状況を紹介する．

1 はじめに

国際的な学術無線 LAN ローミング基盤である eduroam (エデュローム) は，世界中の大学や研究所等において，キャンパス無線 LAN の相互利用を実現する [1]．日本では，2006 年の eduroam 参加以来，東北大学がその運用の責任校として，国立情報学研究所 (NII) と共同で運用および研究開発を行っている．2013 年 10 月時点での国内の参加機関数は 56 であり，順調に増加している．大学 ICT 推進協議会年次大会 [2, 3] を始め，各種研究会や学会などにおける広報により，eduroam の知名度も高くなってきており，参加に向けて準備中あるいは検討中の機関も少なくない．しかしながら，日本国内には 1,200 を超える高等教育機関があり，普及率では約 4.7%に留まっている．eduroam 導入の障壁を緩和するために，eduroam の運用主体である eduroam JP では,「eduroam 代理認証システム」(東北大学) や「仮名アカウント発行システム」(京都大学, NII), SINET を利用したゲストネットワークなどを開発・提供してきた．

世界に目を向けると，2010 年に eduroam 開発元の TERENA で GeGC (Global eduroam Governance Committee) が組織され，国際的な運用体制が整備されて以来，新規参加国が相次いでいる．[2] で既報のとおり，市街地の公衆無線 LAN による eduroam サービスも一部で行われているが，近年では空港や駅に導入される例も見られる．

一方，eduroam の利便性にはまだ改善の余地が多く残されており，利便性改善のための様々な開発も進められるようになった．安定性の改善も必要とされているが，特に耐障害性については，東日本大震災の経験を生かして，我々の研究グループが重点的な研究開発を行っている [3]．

本報告では，eduroam の国内外の最新状況を概説するとともに，利便性の向上策と，耐障害・耐災害性を実現する新しい認証サービスの開発状況を紹介する．

2 国内外の eduroam の動向

2.1 国内の状況

eduroam の国内基盤である eduroam JP は，2006 年に日本が eduroam に参加して以来，徐々に参加機関が増え，国内の機関数は 2011 年末に 27，2012 年末には 43 となり，2013 年 10 月現在で 56 機関に至っている．しかしながら，国内には約 1,200 の高等教育機関があり，普及率はまだ 4.7%に過ぎない．eduroam 導入の障壁を緩和するために，eduroam JP では,「eduroam 代理認証システム」(東北大学) や「仮名アカウント発行システム」(京都大学, NII), SINET を利用したゲストネットワークなどを開発・提供してきた．代理認証システムは，各機関の RADIUS IdP (ID プロバイダ) の機能を代行するウェブサービスであり，機関の管理者用アカウントをオンラインサインアップで取得するだけで，機関内の利用者のための eduroam アカウントを随時取得できるようになる．現在，20 機関がこのシステムを利用しており，機関のメインの eduroam IdP として利用するほか，機関内に構築した IdP の補助として利用する例や，学会等のゲスト用アカウントの発行に利用している例が見られる．

仮名アカウント発行システムは，学術認証フェデレーション (学認, GakuNin)[4] の ID を用いて，各利用者が自分の eduroam アカウントを取得できるようにするウェブサービスである．既に学認に参加している機関では，eduroam IdP を機関に導入する必要がなくなり，システム構築でも運用面でも利

点がある．

キャリア/ISP と eduroam の連携は，残念ながら進んでいない状況である．eduroam JP では，2010 年に旧ライブドア社と連携し，同社の公衆無線 LAN サービスである livedoor Wireless の基地局を利用して，関東地区の市街地 (屋外) やカフェ，貸し会議室などでの eduroam サービスを実現した [2]．同社の改組・事業移管に伴い，livedoor Wireless は 2013 年 4 月にサービス終息し，屋外 (柱上) 基地局も停波することになったが，約 130 の屋内基地局については eduroam 連携が継続している．

機関の eduroam システムの構築を支援する機器が，幾つかの国内企業で開発されるようになった．eduroam の仕様に合わせた RADIUS サーバ/プロキシ機能を有するアプライアンス製品が市販されており，煩雑なインストール作業や設定を行わずに，eduroam 対応のキャンパス無線 LAN システムを構築できる．

2.2 世界の状況

世界的にも eduroam の参加国 (地域) が徐々に増加しており，2013 年現在で 70 弱となっている．この二年ほどで，南アフリカ共和国やロシア，南米各国が参加し，南極を除くすべての大陸に一通り行き渡ったことになる．アジア地域では，シンガポールやタイ，韓国が参加し，11 か国 (地域) に至っている．

カナダや US，シンガポール，タイなどは，国内の普及が比較的速いが，国によっては立ち上がりの遅い所もある．これは国内事情に依るので，国外からの支援は基本的に困難であるが，日本の「代理認証システム」のような IdP ウェブサービスが有効と考えられるケースもあり，実際に TERENA の会議においても注目されるようになった．欧米においても，小さな機関などのサポートや，ゲストアカウント発行の問題が顕在化してきており，集中型のアカウント発行システムの検討が始まっている．

市街地における eduroam サービスについては，[2] でもルクセンブルク市の例などが既報であるが，最近目立ったところでは，北欧の空港等におけるサービスがある．スウェーデンでは，国内の学術ネットワーク SUNET のプロジェクトにより，駅や空港をはじめ，The Cloud が提供する市街地の一部のアクセスポイントで eduroam が利用できるようになった．ノルウェーの UNINETT でも類似のプロジェクトがあり，2013 年に，国内の 19 の空港において eduroam の試験運用が行われている．

大学のみならず，病院や博物館において eduroam サービスを提供する例も見られるようになった．例えば，ロンドン自然史博物館にも eduroam の基地局を見つけることができる．

2.3 利便性の改善

eduroam の利便性を改善するためのツールやサービスの開発が進められているので，代表的なものを紹介する．

eduroam で採用されている IEEE802.1X に基づく認証方式は，世界標準として広く採用されており，Windows シリーズを始め，MacOS，Android，iOS などの様々なオペレーティングシステム (OS) が対応している．しかしながら，一部の OS では無線 LAN に接続するための設定が煩雑で，多くの利用者にとって難解であるという問題があった．eduroam を利用しやすくするために，設定を容易に行うためのツール “eduroam CAT (Configuration Assistant Tool” が欧州の DANTE によって開発された [5]．現在，eduroam CAT は以下の OS に対応している．

- Microsoft Windows 8, 7, Vista, XP
- Apple OS X (Mountain Lion, Lion)
- Apple iOS (iPhone, iPad, iPod touch)
- Linux (多くの主要ディストリビューション)

日本の機関はまだ eduroam CAT に情報を提供していないので，これを利用できない状況である．また，ユーザインタフェースが日本語に対応していないため，国内の多くの利用者には利用しにくいだろう．今後の機能拡張あるいは類似ツールの提供が望まれる．

もう一つの便利なサービスが，eduroam 基地局マップである．長距離用に特別に設計された基地局を用いる場合を除いて，一般に無線 LAN の電波の到達範囲はそれほど広くない．eduroam を利用する場合は，基地局の概ねの位置を知る必要がある．自分の所属する機関においても，初めて利用する場合は eduroam 対応の基地局を探す必要がある．訪問先で eduroam を利用しようとすれば，よほど密に基地局が設置された機関でない限り，利用できる場所を探し出すのが難しいことも多い．慣れない外国の地で eduroam のある最寄りのキャンパスを探し出そうとすれば，面倒はなおさらのことである．

世界の eduroam サービス状況のモニタリングを行ったり，統計情報，参加機関情報などをとりまとめるための，“eduroam database” の構築が進められている．このデータベースには，各国の基地局の位置情報も登録されており，ウェブ上で地図の上に位置を表示できるサービスが提供されている．さらに，The JNT Association (英国) で開発された “eduroam Companion” を利用すると，eduroam database の登録情報を元にして，Android や iOS で動作するスマートフォン，タブレットなどの携

帯端末でも eduroam 基地局マップを見ることができる．

日本はまだモニタリングのための情報を eduroam database に提供していないが，基地局マップに必要な最低限のデータのみ，2013 年 7 月より提供開始した．執筆時点で一部の先行機関のみが詳細な位置データを提供しているが，ほとんどの機関は本部位置が暫定的に登録されている．基地局の位置データは各機関より提供してもらうほかないので，そのデータの収集方法について現在検討中である．

3　耐障害・耐災害性向上のための研究開発

eduroam は世界の無線 LAN ローミングのデファクトスタンダードとなり，既に世界中で便利に利用されているが，その安定性と効率にはまだ解決すべき課題が残されている．eduroam の耐障害・耐災害性を向上させるための，最近の研究開発を紹介する．

3.1　背景

例えば，日本で発行されたアカウントを持って外国を訪れた場合や，その逆に，外国からの訪問者が日本で eduroam を利用する場合，ユーザ認証が安定せず，認証成功までに数分かかったり，無線 LAN の利用中に突然ネットワークが切断されることがある．このような不安定性は，他の国でも同様に発生し，国内のローミングでも発生することがある．

2013 年 3〜5 月には，アジア太平洋地域のトップレベル RADIUS サーバの障害が相次ぎ，完全な復旧までにかなりの日数がかかった．eduroam の標準的な構成では，世界のトップレベルの RADIUS サーバや各国，各機関のサーバが，ツリー状の階層的な認証ネットワークで結ばれている．そのため，上位のサーバに障害が発生すると，広域に影響がある．また，多くの RADIUS サーバを中継するほど，認証処理が不安定になることが経験的に知られている．

eduroam の安定性を向上させるために，RadSec と呼ばれる通信方式が開発され，一部の国々では既に利用されている [6]．RadSec は eduroam の安定性向上に効果的であるが，DNSSEC が必要になることから，導入のしきいが高くなるという欠点がある．また，前述したようなサーバ障害には対応できない．

eduroam の信頼性を高めていくためには，耐災害性・強靭性に関する取り組みが必要である．

3.2　研究開発の状況

筆者らは，東日本大震災の経験を受けて，災害に強いキャンパス無線 LAN を実現するために，eduroam の耐災害性向上についての研究を遂行してきた．クラウド型代理認証システムによる耐災害性向上については，[3] で既報のとおりである．さらに，公衆無線 LAN への応用も想定して，被災地の避難所などで利用できるような，耐災害無線 LAN システムについての研究を進めてきた [7]．後者の研究では，ネットワークインフラの被災や広域停電などで広域ネットワーク (WAN) が利用できない場合を想定し，そのような場合でもユーザ認証を可能とする，ローカル認証方式を開発した．クライアント証明書を利用したローカル認証の様子を図 1 に示す．

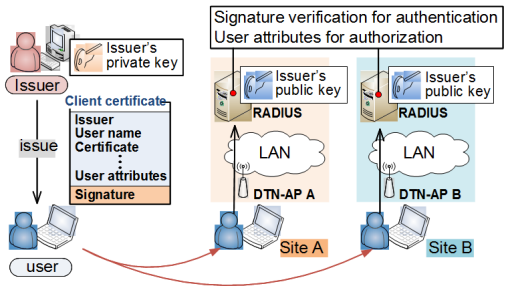

図 1: クライアント証明書を利用したローカル認証

このローカル認証方式は，eduroam でも利用されている IEEE802.1X に基づいている．eduroam では様々な EAP(拡張認証プロトコル, Extensible Authentication Protocol) が利用できるが，ここでは EAP-TLS (〜Transport Layer Security) を利用しており，プロトタイプシステムは実際に eduroam システム上に構築された．

eduroam で EAP-TLS に基づくユーザ認証を行う場合，一般的には RADIUS ツリーを利用し，認証リクエストは利用者の所属機関にある RADIUS IdP まで届けられる．一方，ローカル認証方式では，eduroam アカウントを発行する機関がクライアント証明書に署名し，その際に利用される秘密鍵とペアになる公開鍵を他機関に配布しておく．無線 LAN 基地局を収容する RADIUS サーバに予めこの公開鍵を導入しておくことで，WAN を介さないで認証処理が完結する．この耐災害無線 LAN システムでは，各都道府県がアカウントの発行に責任を持つという運用を想定したので，47 個の公開鍵を事前に RADIUS サーバに登録しておけばよい．

eduroam にこのローカル認証方式を応用することで，RADIUS サーバやネットワークの障害にも強いシステムが実現できると考えられる [8]．さらに，WAN を介して認証リクエストを多段にリレーする必要もなくなるので，認証の安定化や高速化にも寄与できる．ただし，eduroam の標準の構成では世界中の参加機関がアカウント発行機関となることから，図 1 の構成ではすべての RADIUS サーバに世界中の公開鍵をインストールする必要があり，

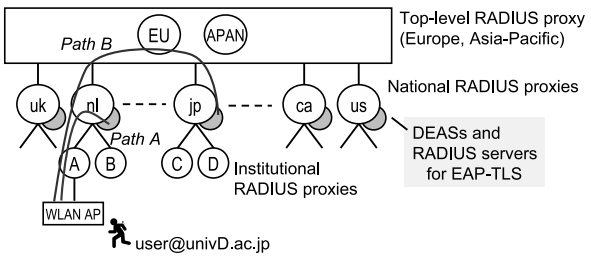

図 2: 耐障害・耐災害 eduroam のアーキテクチャ

現実的ではない．この問題に対処するために，代理認証システム (DEAS, Delegate Authentication System) のような集中型の IdP を併用する．耐障害・耐災害 eduroam のアーキテクチャを図 2 に示す．

このシステムを利用しようとする国は，集中型の IdP を用意し，また，国のトップレベルの RADIUS proxy にローカル認証の仕組みを付加し，他国の公開鍵を取り寄せて事前に登録するか，認証要求に応じて動的に公開鍵を取得できるようにしておく．世界の国数は 200 弱であるので，RADIUS proxy に登録される公開鍵の数も高々200 で済む．

利用者がある国を訪問し，eduroam を利用しようとする時，訪問国の RADIUS proxy が利用者の国の有効な公開鍵を利用できる場合は，図 2 の Path A が選択されて，認証が国のトップレベルで終端される．これにより，大陸をまたぐような長距離の通信を行うこと無しに認証が完結し，信頼性と速度の向上に寄与すると考えられる．

もし公開鍵の取り寄せが何らかの障害によって失敗した場合は，Path B が選択され，認証要求は利用者の国まで届けられる．本システムを導入していない国の場合は，利用者の所属機関の RADIUS IdP まで認証リクエストがリレーされる．これによって従来システムとの互換性が保たれる．

さらに効率的で安定な認証を実現するために，本システムを利用する国の各機関は，自国の公開鍵を基地局に最寄の RADIUS proxy に事前に登録しておく．これにより，自機関の利用者の認証は機関内のネットワークだけで完結することになり，国のプロキシの負荷を大幅に減らすことが可能である．

このシステムの基本的な認証処理は [7] で構築したプロトタイプで動作確認済みであるが，認証経路の自動切り替えや公開鍵の交換，不正利用等に対処するための CRL (Certificate Revocation List) の交換などの機能を含めたシステムの実装は，現在進行中である．機能と性能の評価が今後の課題である．

4 むすび

eduroam の国内外の最新状況を概説するとともに，利便性の向上策と，耐障害・耐災害性を実現する新しい認証サービスの開発状況を紹介した．eduroam の基本的な仕組みにはできるだけ手を付けずに，端末の設定を支援するツールや，基地局マップなど，利便性を向上させるためのツールやサービスが徐々に充実してきている．また，安定で高速な認証が行えるようにするための技術的な改良も進められている．これらは，導入に際して機関の管理者や利用者にできるだけ負担がかからないように配慮されているが，基地局マップのデータ作成のように若干の負担増もある．余力のある機関には，eduroam の利用環境の改善のために，データ提供や各種ツール/サービスの紹介などを行っていただけると幸いである．

参考文献

[1] eduroam JP: `http://www.eduroam.jp/`

[2] 後藤英昭, 曽根秀昭, “キャンパス無線 eduroam 導入のメリットと国内外の動向,” 大学 ICT 推進協議会 2011 年度年次大会 論文集 D10-6, pp.259-263, 2011.

[3] 後藤英昭, 曽根秀昭, “eduroam で作る災害に強い大学間連携キャンパス無線 LAN,” 大学 ICT 推進協議会 2012 年度年次大会 論文集 H9-3, pp.326-329, 2012.

[4] 学術認証フェデレーション (GakuNin): `https://www.gakunin.jp/`

[5] eduroam CAT: `https://cat.eduroam.org/`

[6] S. Winter, M. McCauley, S. Venaas, and K. Wierenga, “Transport Layer Security (TLS) Encryption for RADIUS,” IETF RFC6614, May 2012. Winter, S. et al., 2012.

[7] S. Kinoshita, T. Watanabe, Y. Yamasaki, H. Goto, and H. Sone, “Fault-Tolerant Wireless LAN Roaming System Using Client Certificates,” IEEE 37th International Conference on Computer Software and Applications (COMPSAC2013), pp.822–823, 2013 (Kyoto, Japan, July 22–26).

[8] H. Goto, H. Liu, S. Kinoshita, M. Nakamura, and H. Sone, “DISRUPTION-TOLERANT, LARGE-SCALE WIRELESS LAN ROAMING ARCHITECTURE FOR EDUROAM,” Proc. of IADIS International Conference Applied Computing 2013, pp.191–195, 2013 (Fort Worth, Texas, USA, Oct.23–25).