D10-6

キャンパス無線 eduroam 導入のメリットと国内外の動向

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： 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，この一年で国内の参加機関数が約 7 割も増加し，2011 年 9 月現在 24 機関で利用されるに至った．参加に向けて準備中の機関も少なくない．しかし，eduroam の導入を検討している幾つかの機関からは，機関内で導入のメリットを理解してもらうのが難しいといった声も聞かれる．本発表では，導入説明の一助となるように，eduroam 導入の様々なメリットについてまとめる．

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)[1] は，2006 年に日本が参加して以来，国内でも次第に参加機関が増え，2011 年 9 月時点で 24 機関が利用している [2]．この数は前年同月比で約 7 割増であり，順調な増加傾向である．また，情報教育研究集会 [3] を始め，各種研究会や講習会，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．国内の eduroam は，eduroam JP の名前で，国立情報学研究所と東北大学が中心となって運用されている．国際的には，北米 (カナダ，アメリカ合衆国) における普及ペースが速いこともあって，国際的な無線 LAN ローミング基盤としての地位は確実なものとなった．

日本国内には 1,200 を超える高等教育機関があり，普及率ではまだ 2.0%とまだまだ低い．eduroam の導入を検討している幾つかの機関からは，学内において eduroam 導入のメリットを理解してもらうのが難しいといった声も聞かれる．従来，広報において国際性を前面に出していたことが影響してか,「海外との交流が少ないのでメリットがない」と思われているケースも見られた．しかし，eduroam の導入は，国内や学内といった範囲でも様々なメリットがあり，さらには，今後来るであろうキャンパスユビキタス時代に適した学術ネットワークアクセス環境を提供し，教育・研究環境の改善や開拓が期待される．

本稿では，各機関における導入説明の一助となるように，eduroam 導入の様々なメリットについてまとめる．

2 キャンパス無線 eduroam 導入のメリット

eduroam は，以下に示すような特徴を有する．これらを踏まえた上で，eduroam 導入の様々なメリットについて述べる．

(1) 商用公衆無線 LAN でも利用されている，標準的な IEEE802.1X 方式を採用し，安全なユーザ認証を実現．(技術的には何ら特殊なところは無い．)

(2) Windows PC や Mac はもちろん，iPhone や Android などのスマートフォン，タブレット，Linux など，幅広い端末および環境で利用可能．

(3) 学術系の無線 LAN システムとして，国際的なデファクトスタンダード．

(4) エンドユーザに対して課金しない．ローミングしている機関どうしや，国の間でも，利用料金のバランス (支払い) などは行わず，サービスの無償相互提供が原則．

(5) 全世界どこでも，ほぼ同じ接続手順．端末の多くは，一度の初期設定のみで良く，サービスエリア内に入ると自動的にネットワークに接続される．

(6) 不正利用時のインシデント対応 (端末の追跡・特定など) が可能．

(7) 認証 VLAN の機能によって，学内 LAN とゲストネットワークの安全な分離が可能．(来訪者の端末をゲストネットワークに収容．)

2.1 キャンパスの仮想的拡大

現在，無線 LAN システムをキャンパスに導入済みの教育・研究機関は少なくない．大学等では，講師がプレゼンテーション用の PC を学内 LAN に接

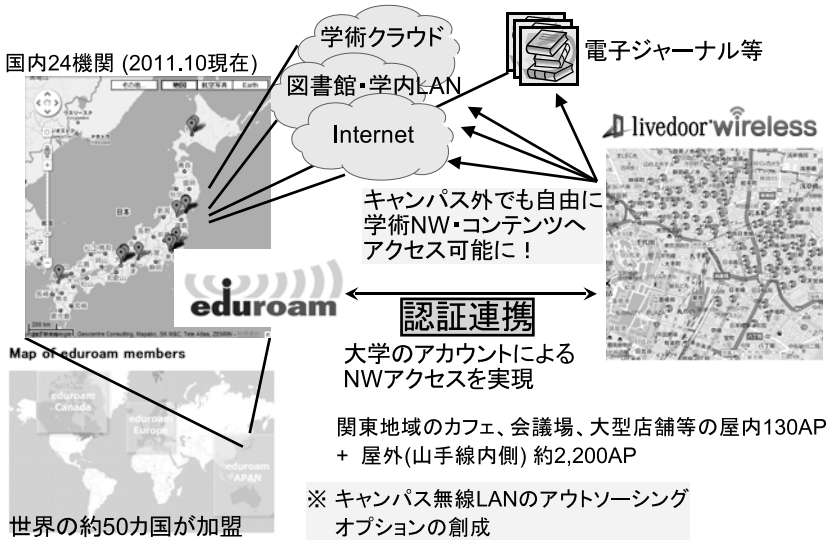

図 1: キャンパスの仮想的拡大

続したり，学生が持ち込みの PC を使って演習や自習を行なったりするなどの利用形態があり，キャンパスネットワークはこのような新しい授業方法を支援していく必要がある．これらのことは従来の無線 LAN システムでも実現可能に見えるが，実際は利便性に問題を抱えている機関も少なくない．例えば，大きな大学では部局ごとに無線 LAN システムを整備することがあるが，全学で相互利用できるようなローミング対応のシステムをわざわざ設計・構築しない限り，無線 LAN システムは部局ごとに閉じたものになってしまう．その結果，教員や学生にとっては他学部での講義・演習に支障があり，教職員にとっては移動先の会議室において不便を強いられる．全学で共通の無線 LAN システムを構築すれば，このような問題は解決できるだろうが，機関内に閉じていることに変わりはない．

近年では，教職員・学生の大学間の移動にも対応できるシステムが求められている．単位互換制度により他校の講義や演習に出席する学生にとっては，現地でのネットワーク接続が必要になる．大学間の協定が進んで，各大学に閉じたシステムでは教育・研究を十分にサポートできなくなってくることは想像に難くない．

eduroam は国際標準の IEEE802.1X に基づいたネットワークローミングシステムであり，学内の部局間での無線 LAN ローミングにも応用できるうえに，国立情報学研究所にあるサーバに登録するだけで，他機関との認証連携が有効になり，無線 LAN の相互利用環境を実現できる．

教員や学生が国際会議などで海外渡航した際は，インターネットに接続するのが難しいことが多い．もし現地の教育・研究機関で自由にネットワーク接続が可能ならば，利用者にとって非常に便利なことはもちろん，利用コストの面でもメリットが非常に大きい．例えばヨーロッパにおいて，ホテルの公衆無線 LAN が利用できたとしても，一日あたりの利用料金は 20 ユーロといった相場であり，値下げ傾向ではあるがまだ相当な負担となる．日本のプロバイダ (ISP) のアカウントを利用したローミング利用も考えられるが，料金的には同様に高額である．eduroam を利用すれば，現地で端末の電源を入れるだけで，多くの場合は自動的にネットワークに接続され，無料で高速なインターネット利用が可能である．

以上のように，eduroam では部局間から大学間，さらに国をまたいでも，シームレスでスケーラブルな無線 LAN 相互利用環境が実現できる．言い換えれば，従来は学内に閉じていたキャンパスネットワークが，仮想的に拡大するとも言える．電子化された教材はもちろんのこと，国内外を問わずに電子ジャーナルや学術クラウドなどへのアクセスが可能となることから，ネットワークへの依存度が高まった現代の教育・研究環境では，「キャンパスの仮想的拡大」と見ることもできるだろう (図 1)．

さらに近年では，公衆無線 LAN の提供業者や自治体と協力して，教育研究機関以外でも eduroam 対応のアクセスポイント (AP) が利用できるような環境の構築が進められている．例えば欧州では，大学の近所のパブや，街なかのカフェ等においても，eduroam 対応の AP を設置する動きがある．ルクセンブルクでは，地方自治体が運営する市街地無線 LAN サービス HotCity の AP で eduroam が利用可能となっている．日本においては，今のところ関東地区限定ではあるが，ライブドア社が市街地やカ

フェ，大型店舗で運用している公衆無線LANサービスにおいて，約2,500基のAPでeduroamが利用可能となっている[4]．このように，キャンパス無線LANシステムにeduroamを採用するだけで，他に特別な契約もなく，キャンパスを大幅に拡大できることになる．

2.2 安全なユーザ認証

現在，キャンパス無線LANでも商用の公衆無線LANサービスでも，ウェブブラウザの画面にID・パスワードを入力する，いわゆる「ウェブ認証」と呼ばれる方式が広く用いられている．しかし，付録Aに示すように，ウェブ認証は偽AP問題に対処できず，ID・パスワードの盗難に関して大変危険であることが知られている．もし，教職員の業務や学生の履修登録などの重要な用途で使われるID・パスワードと同一のものがウェブ認証でも用いられているならば，それはセキュリティ上の大変な脅威である．

eduroamで利用されている1X認証では，偽AP問題への対策が可能であり，端末の初期設定で正しい認証方式(MS-CHAPv2など)が選択されていれば，ID・パスワード盗難のリスクは非常に低くなる．また，本章の冒頭でも挙げたように，一度設定を行なっておけば，サービスエリア内に入ると端末は自動的にネットワークに接続される．1X認証では，正しいかどうかわからない認証画面の指示に利用者が従うような危険性は排除できる．また，eduroamの端末設定は一部の値を除いて世界共通なので，周囲の人の援助を受けやすいという利点もある．

日本のeduroamでは，「学術認証フェデレーション(学認)[5]」を利用してエンドユーザがeduroam用のアカウントを取得できる「仮名アカウント発行システム」が提供されている．もし機関が学認に参加し，このシステムを利用すれば，eduroam用のユーザデータベースを別途構築しなくて済む．また，配布されるのは一時アカウントであるので，万一の盗難の際にも被害範囲を小さく抑えることができる．

2.3 安全なネットワーク構成

キャンパス無線LANでは，学内利用者の端末は学内LANに接続させ，高度なネットワークサービスを提供し，一方で来訪者の端末はゲスト用のネットワークに収容し，学内LANへの干渉を避けたいというニーズがある．ウェブ認証方式で，このような利用者IDに基づくネットワークの分離を行うことも不可能ではないが，セッションハイジャックにも耐性のある仕組みを作り込むことは難しい．eduroamでは，1X認証において認証VLANを利用することで，安全なネットワーク分離が可能である．

ローミング環境では，大学が契約している電子ジャーナルなどに来訪者がアクセスできるようでは，ライセンス違反となる．認証VLANを利用することで，このような問題にも対処が可能である．

2.4 導入と運用の簡略化，低コスト化

従来のキャンパス無線LANシステム構築では，大学とシステムインテグレータ(SIer)が，認証方式の選定からシステム設計を行うケースも少なくなかった．1X認証がまだあまり普及しておらず，Windowsのサポートも弱く，実績が少なかったことなども影響していたと思われる．

eduroamは世界標準の1X認証方式を採用しており，近年では様々なオペレーティングシステムで1Xのサポートが強化されたこともあり，無線LANの安全な認証方式としてはごく標準的なものになっている．このため，キャンパス無線LANにeduroamを採用する場合，極端に言えば調達における文書に「eduroamに対応すること」の一文を入れることで，仕様策定の大幅な簡略化が期待できる．APまわりもごくありふれた機器構成・ネットワーク構成になるので，経験のあるSIerやプロバイダ(ISP)では設計が容易になり，初期導入コストの低減が期待される．

従来はスモールオフィス向けの安価なスタンドアロン型のAPを並べることも多かったが，キャンパスに数十〜数百といった数のAPを設置すると，その管理・運用コストが意外に高くなる．コントローラ型のAPシステムは，初期導入費用が割高になるものの，死活監視や設定変更などの手間が大幅に減るので，少ない人数で運用でき，長期運用ではトータルコストの低減につながると考えられる．また，ハードウェアの高い安定性も期待できる．

eduroamは，ネットワーク管理者の運用負担の観点でもメリットがある．大学で学会などが開催される場合，従来は既設APの設定変更やゲスト用APの一時的設置などの作業が必要だった．独自の認証方式を採用している場合は，接続のサポートも必要である．eduroamを導入すれば，eduroamのアカウントを持っている来訪者はそのまま無線LANが利用でき，アカウントのない人にはゲストIDを配るだけで済む．小規模な会議で従来はゲスト用APの設置を諦めていたケースでも，容易に無線LANサービスを提供できるようになると思われる．

2.5 海外の研究機関との交流促進・支援

2.1で述べたように，日本の教員や研究者が海外の教育・研究機関を訪れた際にeduroamが利用できることは非常に大きなメリットである．当然ながら，海外から見れば，日本でも各所でeduroamが

利用できることが期待されている．日本の公衆無線LANサービスが欧米に比べて安いといっても，契約が必要になるか，割高な一日利用権を購入する手間がかかる．さらに，多くの大学等のキャンパスには公衆無線LANが導入されていないため，商用サービスが利用できないという根本的な問題がある．

eduroamを導入することによって，海外の研究者に無償でネットワーク利用環境を提供することができ，会議も誘致しやすくなると考えられる．小規模で頻繁な打ち合わせでは特に，ゲストIDの取得なしに自由にネットワークが利用できることの恩恵は大きい．eduroamサービスの提供は，相互に恩恵を与えあうという観点では義務であるが，海外機関にとっての「おもてなし」の意思の表れでもある．国際的な教育・研究環境をうたう機関であればなおさら，交流促進・支援の観点でeduroamの存在意義は大きいものとなるはずである．

3 eduroamの国内外の動向

3.1 普及近況

eduroamは欧州のTERENA(Trans-European Research and Education Networking Association)で開発され，2011年10月現在，欧州圏では37か国(地域)が参加している．一部の国を除いて，ほぼどの国でも利用できるほどに普及している．

アジア太平洋地域では，オーストラリアが欧州外で最初にeduroamを導入して以来，香港，台湾，日本などが接続しており，中国も正式な国内展開に向けて準備中とのことである．他国にホスティングされている国を含めると，8地域がeduroamに参加している．

カナダとアメリカ合衆国は，正式なeduroam参加は日本より遅かったが，それぞれ34機関と32機関が既にeduroamのサービスを提供しており，日本よりも普及ペースが速い．北米がeduroamに参加したことによって，eduroamの国際的なデファクトスタンダードの地位は確実なものとなったと言える．現在，アジアの一部の国や南米諸国の参加に向けて，準備や交渉が進められている．

3.2 eduroamの運用ルールと技術要件

eduroamは実証実験的なプロジェクトからスタートしており，欧州やオーストラリアではそれぞれ独自に運用ルールが定められてきた．最近，北米を含めアジア太平洋州への普及が進んできたことから，世界のeduroamを実証実験的な運用から正式なものにするために，2010年11月にTERENAを中心にGlobal eduroam Governance Committee (GeGC)が組織された．GeGCは世界各地から選出された7名の委員(投票権を持ち，任期二年間)で構成され，アジア太平洋地域からはオーストラリアと日本が代表となり，日本では著者の後藤が委員となっている．

この一年間に，GeGCではeduroamサービスの定義や技術要件を示したeduroam Compliance Statementの作成を行ってきた．その第一版が2011年10月に完成し，発行された．eduroamの運用にあたって，参加機関はこの文書の規定に従う必要がある．

以前は国際的な公式ルールが存在しなかったことから，国内のeduroamも実証実験的な運用がなされてきたが，日本でも正式なルールの作成が必要であり，事務局ではeduroam Compliance Statementを元にしてその準備を行っているところである．

3.3 eduroam JPの大規模化へ向けた取り組み

eduroamの基本的な構成では，各機関にRADIUSサーバが設置される．しかし，このようなネットワーク構成では，数百〜千規模の機関が存在すると，新規接続に加えて，日常の機材トラブルや不正利用時におけるeduroam JP事務局の負担が非常に大きくなることが問題である．また，各機関においては，eduroam用のIDデータベースの構築や，既存の認証システムと連携する機構の作り込みが困難なことがある．また，東日本大震災以降，大学の情報インフラを学内からデータセンターやクラウドサービスに移す流れが加速していることから，eduroamにもそれに見合う仕組みが必要と考えられる．

低い導入・管理コストでeduroamを運用できるようにするため，国立情報学研究所と東北大学では，大規模化に適したeduroamの新しいアーキテクチャの研究開発を行ってきた．その成果の一部として，現在，以下に示す二種類のサービスが提供されている．

- eduroam仮名アカウント発行システム
- eduroam代理認証システム

「eduroam仮名アカウント発行システム」は，2.2に示したように，学術認証フェデレーションと連携したシステムであり，これを利用することで，各機関にRADIUS IdP (IDプロバイダ)の機能を置く必要がなくなる．

「eduroam代理認証システム」は，従来は各機関に置かれていたRADIUS IdPの機能を代行するものであり，各機関からはアカウント発行のウェブサービスとして利用できる．利用を希望する機関は，オンラインで管理者のアカウントを申請するだけでよく，その管理者がeduroamのアカウントを必要な数だけ随時，自由に取得できる．取得したアカウントのエンドユーザへの配布が手動であること

から，大人数向けの利用には向かないが，機材等の準備がまったく要らないという点で，eduroam 参加へのしきいを大きく下げることが可能である．

なお，機関の管理者の負担を低減させ，中規模の機関でも利用できるようにするために，「eduroam 代理認証システム」に改良を加え，エンドユーザ向けのインタフェースを追加する準備が進められている．

各機関の無線 LAN アクセスポイントを収容するために，RADIUS proxy の機能が必要である．この機能のために RADIUS サーバを設置する必要があるが，proxy は利用者のアカウント情報を持つ必要はないので，ネットワーク機器の一部とみなすことができる．アクセスポイントを設置する業者に，RADIUS proxy も合わせて導入してもらうことができる．

また，インターネットサービスプロバイダ (ISP) に依頼して商用公衆無線 LAN も同時に整備することも考えられ，現在ではこれが可能な業者は限られているものの，アウトソーシングによって，RADIUS proxy を含む無線 LAN システムが容易に導入できるようになる．ISP の利用により，アクセスポイントの死活監視などの労力も含めて，運用コストを下げられる可能性がある．

4 むすび

本稿では，eduroam 導入が機関にもたらす様々なメリットについてまとめた．また，国内外の動向と，eduroam の導入障壁と運用コストを下げる方法を紹介した．各機関における eduroam 導入の一助となれば幸いである．

参考文献

[1] L. Florio and K. Wierenga, “Eduroam, providing mobility for roaming users,” Proc. 11th International Conference EUNIS2005, 2005.

[2] eduroam JP ウェブサイト : http://www.eduroam.jp/

[3] 後藤英昭, 曽根秀昭, “大学間無線 LAN ローミング基盤 eduroam の動向と容易な導入方法,” 平成 22 年度 情報教育研究集会 講演論文集, 2010.

[4] プレスリリース「ライブドアと国立情報学研究所 (NII) 国際学術無線 LAN ローミング基盤 eduroam の共同実証実験を livedoor Wireless アクセスポイントにて開始」, http://corp.livedoor.com/press/2010/0308376, 2010.3.

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

付録 A ウェブ認証の危険性について

無線 LAN では，利用者が期待する正規のアクセスポイント (AP) に常に端末が接続されるとは限らない．悪意を持った者が ID とパスワードを盗み出すなどの目的で偽の AP を立てることも考えられる．このような「偽アクセスポイント (AP) 問題」への対策がない認証方式では，攻撃者に ID・パスワードなどを盗られることがある．

現在，キャンパス無線 LAN でも商用の公衆無線 LAN サービスでも，国内外を問わず，端末をアクセスポイントに接続するとウェブブラウザの画面に ID・パスワード入力画面が強制的に表示される，いわゆる「ウェブ認証」と呼ばれる方式が広く用いられている．しかし，ウェブ認証で偽 AP 問題に対処することは困難であり，ウェブ認証は大変危険であることが知られている．

ログイン画面で HTTP (HyperText Transfer Protocol) が使われている場合はもちろんであるが，例え HTTPS (HyperText Transfer Protocol over Secure Socket Layer) が使われていても，AP の背後にある認証サーバが正規のものである保障はなく，入力した ID・パスワードは暗号化無し (平文) で攻撃者に伝わってしまう．ウェブブラウザが警告を出さないような証明書は，条件さえ満たせば誰でも入手できることに注意が必要である．しかも，ユーザ認証がまだ済んでいない状態なので，端末はインターネットにアクセスできず，信頼できる機関を通してサーバ証明書の検証を行うこともできない．事前にウェブブラウザに機関独自のサーバ証明書を仕込んでおく手法も考えられるが，証明書の配布と導入サポートの手間がかかるという問題がある上に，ID 発行者と AP の管理者が異なるローミング環境では利用できない．

さらには，サーバ証明書を用いていたとしても，端末接続のたびに手動で入力操作を行う場合は，利用者が HTTPS の利用を意識せずに，攻撃者が用意した HTTP のページにうっかり ID・パスワードを入力してしまう危険性が排除できない．この時，当然ながらブラウザは一切警告を出さない．また，利用者の判断に頼るシステムである以上，攻撃者は偽の利用案内をブラウザに表示して，利用者を欺き，より重要な情報を聞き出すことも可能だろう．

商用サービスがウェブ認証を提供し続ける理由として，歴史的経緯とサービスの継続性，利用者にとって直観的で簡便な利用方法，低機能デバイスのサポートなどが考えられるが，ウェブブラウザを開くという簡単な操作で広告効果が得られる点も無視できないと思われる．一方で，1X 認証を利用した高セキュリティなプランを提供する公衆無線 LAN の業者も増えてきている．