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

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： 欧州発祥の学術無線 LAN ローミング基盤 eduroam (エデュローム) は、欧州 40 か国以上のほか、アジア太平洋地域、カナダ、US にも普及しつつあり、国内では 15 機関が参加するに至っている．商用無線 LAN サービスとの連携により首都圏の市街地でも利用可能になったのに加え、学術認証フェデレーション (GakuNin) との連携強化や代理認証システムの提供により、大学への導入が格段に容易になった．本講演では、eduroam の国内外における動向を紹介し、様々な導入形態を紹介・提案する．

1 はじめに

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 に接続したり、学生が持ち込みの PC を使って演習や自習を行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．さらに、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．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、ネットワーク管理者にとっても、ゲスト用アクセスポイントの一時的設置や、ID 発行といった手間から解放されるという利点がある．

以上のような背景のもと、大学等の高等教育機関の無線 LAN システムを接続し、相互利用を可能とする、無線 LAN ローミングの実現が望まれるようになった．欧州で運用が始まった無線 LAN ローミング基盤である eduroam (エデュローム) はアジア太平洋地域や北米にも普及してきており、日本でも eduroam JP の名で運用されている [1, 2, 3, 4].

欧州各国とは異なり、日本には 1,200 を超える非常に多くの高等教育機関が存在するため、従来の eduroam の仕組みでは大規模な展開・導入が難しい．我々は、機関の eduroam 参加の障壁を取り除き、運用コストも下げられるような仕組みについて技術開発を行っている [4]．既報告の代理認証システムに加えて、本年は国内の認証連携基盤である「学術認証フェデレーション (GakuNin)」[5] との連携が可能となり、さらに商用無線 LAN サービスとの連携も実現したことによって、格段に容易に eduroam を導入する下地が整ってきた．

本稿では、eduroam の国内外における動向を紹介し、様々な導入形態を紹介・提案するほか、キャンパスネットワーク全体のアウトソース化や、商用無線 LAN のキャンパス導入、携帯電話網の負荷軽減を実現する 3G オフロードも視野に入れた導入形態を紹介する．

2 国際無線 LAN ローミング基盤 eduroam

2.1 eduroam とその国際的動向

無線 LAN ローミングとは、「認証連携技術により、利用者が所属機関のアカウントを使って他機関の無線 LAN インフラを利用できる仕組み」である．eduroam は TERENA (Trans-European Research and Education Networking Association) において開発され、欧州内の教育研究機関ごとの無線 LAN システムを相互接続したことに端を発する無線 LAN ローミング基盤であり、2010 年 10 月の時点で、欧州では 40 か国以上が加盟している [1, 2].

欧州の一部の国々では、教育研究機関以外でも、eduroam の利用が可能な無線 LAN アクセスポイントが設置されている例がある．例えば、大学の近所のパブや、街中のカフェ等においても、eduroam 対応のアクセスポイント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 のアクセスポイントで eduroam が利用可能となっている．

アジア太平洋地区では、2004 年にオーストラリアが eduroam に接続したのを皮切りに、現在では中国、香港、台湾、日本、ニュージーランド、カナダ、US が加盟済みである．

eduroam では、参加機関の間で認証連携を実現するために、図 1 に示すような世界規模の RADIUS サーバ (Remote Authentication Dial-In User Ser-

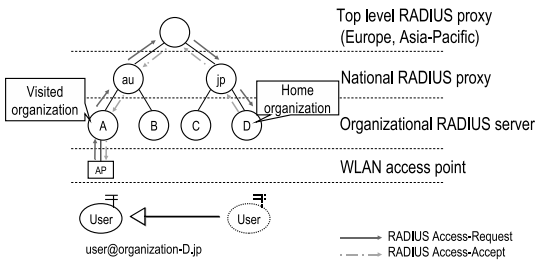

図 1: eduroam のしくみ

vice Servers) の階層的ネットワークを用いる．欧州とアジア太平洋地区に世界のトップレベルサーバが設置されている．RADIUS サーバの役割は、認証情報の提供と、隣接サーバへの認証情報・結果の転送の、二種類がある．ユーザ情報を持たないサーバは、特にプロキシサーバと呼ばれる．

利用者は、ネットワークへの接続にあたって、DNS (Domain Name System) のドメイン名に似た “レルム名” を含むユーザ ID と、パスワード (または証明書) をアクセスポイントに提示する．ユーザ ID は “ユーザ識別子@レルム名” の構造をとる．また、レルム名は eduroam のネットワーク構造を反映した階層構造を持っている．認証情報はアクセスポイントの上流の RADIUS プロキシに転送され、さらに複数のプロキシを経由して、最終的には利用者の所属機関の RADIUS サーバまで届けられる．所属機関のサーバは、送られてきた認証情報をデータベースのエントリと比較し、正しく認証されれば Accept の応答を、誤っている場合は Reject を返す．

RADIUS は、パケットロスの多い通信経路や、大陸間の遠距離通信では、たまに不安定になることが運用経験上知られている．この問題に対処し、また、ツリーを使わずに機関どうしで直接通信を実現できるようにするために、RadSec と呼ばれる通信プロトコルが開発されている [6]．しかし、各機関で RADIUS に加えて RadSec に関する知識も必要となり、これは新たな導入障壁となる可能性がある．eduroam の大規模展開という観点では、機関参加の容易化には寄与しない．

2.2 日本における eduroam

日本の eduroam への加盟は、全国共同電子認証基盤 (UPKI) 構築事業のプロジェクトの一つとして実現した [7]．UPKI 構築事業は、国立情報学研究所 (NII) と 8 大学 1 機関によって平成 17 年度より開始された事業であり、認証連携技術によって大学等を相互接続し、全国大学共同電子認証基盤を実現しようとするものである．eduroam による無線 LAN ローミングは、認証連携のアプリケーションの一つとして位置付けられた．2006 年 8 月に東北大学がアジア太平洋地区のサーバに接続し、これにより日本の eduroam 加盟が実現した．

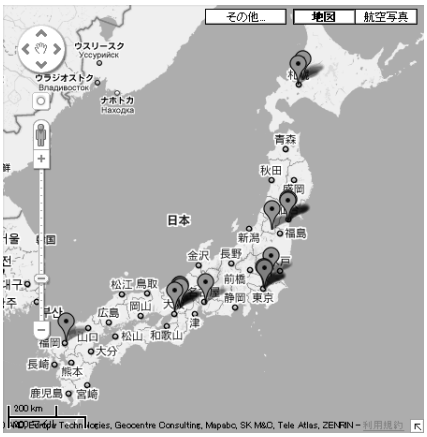

図 2: eduroam JP 参加機関マップ (2010 年 10 月現在, Google Maps にて)

現在、eduroam JP は国立情報学研究所の正式なサービスの一部であり、国内の高等教育研究機関は申請により随時加入できる．2010 年 10 月の時点で計 15 機関が eduroam に参加している．図 2 に参加機関のマップを示す．

3 大規模展開への取り組み

3.1 eduroam 普及の障壁とその対策

eduroam の導入においては、二つの機能を明確に意識すると見通しがよくなる．

- 無線 LAN アクセスポイントシステム
  – eduroam SP (Service Provider)
- 認証サーバ (アカウント管理、認証連携)
  – eduroam IdP (ID Provider)

例えば、貸し会議場・会議室のような場所では、アクセスポイントの提供だけでよい．また、大学等においてアクセスポイントの整備が時期的に遅れるような場合は、学外 (特に海外) で eduroam 利用の便を図るために、eduroam IdP だけでも先に整備することはメリットが大きい．

機関として eduroam に参加するためには、技術的にはその機関の代表の RADIUS サーバを立てるだけでよい．アクセスポイント一台だけでも、eduroam の運用は開始できる．しかし、ネットワーク技術者にとっても RADIUS の知識は一般的ではなく、学習の手間がかかる．また、ネットワークに詳しい職員がいない機関もあり、無線 LAN のためだけに RADIUS サーバを導入するのは難しい．

eduroam JP のサーバに各大学のサーバを接続し、認証連携のテストを行うことを考えると、日本には 1,200 以上の高等教育機関がある (2008 年調べ) ことから、その手間も相当に大きいものとなる．

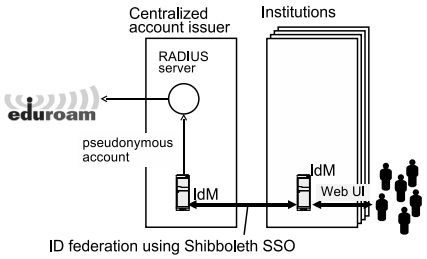

図 3: eduroam 仮名アカウント発行システム

国内で eduroam を普及させるためには、機関の加入や接続の技術サポートにおいても、大幅な省力化が必要不可欠である．

3.2 eduroam 仮名アカウント発行システム

eduroam の大規模展開の一助となるように、eduroam JP では「eduroam 仮名アカウント発行システム」を構築し、2010 年 6 月より全国の高等教育機関に対してサービスを開始した．このシステムは、京都大学で開発・構築された．学術認証フェデレーション (GakuNin)[5] の Shibboleth SSO (Single Sign-On) を利用することによって、学術認証フェデレーションの参加機関の教職員・学生は、利用者個人が Shibboleth でユーザ認証を受け、利用条件を満たしていれば個人用の eduroam 一時アカウントを随時取得できる (図 3).

各機関において、無線 LAN 連携のために新たに専用のユーザデータベースを構築することは、数千〜数万人の学生を擁する大学はもちろん、たとえ数百人の機関であっても現実的ではない．もし、統合認証基盤やそれに類する認証システムが構築済みで、認証情報を RADIUS プロトコルに変換する仕組みを用意できるのであれば、比較的容易に利用者に eduroam のアカウントを配布できる．しかし、RADIUS サーバの立ち上げでさえも、運用コスト等の制約により難しいことがある．前述の「eduroam 仮名アカウント発行システム」では、今後普及が期待される汎用的な認証連携システムである学術認証フェデレーションさえ導入すれば、機関の eduroam IdP を省略しつつ、eduroam の利用環境を整えることができる．

さらに、このシステムでは、日本のトップレベル RADIUS サーバに直結された共用認証サーバによってユーザ認証が行われるため、プロキシの段数を減らすことができ、eduroam の安定化も期待できる．

3.3 代理認証システム

平成 21 年度に既報のとおり、eduroam JP では、一時アカウントを自動発行し eduroam のユーザ認証を代行する「代理認証システム」のサービスも提供している [3, 4]．当システムでは、学内の統合認証基盤などが構築中や計画中であっても、管理者アカウントの申請だけですぐに eduroam が利用可能になる．学術認証フェデレーションに未参加でも利用できるため、eduroam 導入の敷居を大幅に下げることができる．

当システムを利用しようとする機関では、管理者と責任者を定め、システムのウェブサイトから利用申請を行う．機関用の管理アカウントが発行されるので、管理者はこれを用いて、必要な数の一時アカウントをシステムから随時ダウンロードできる (バルク発行)．機関におけるアカウントの配布・管理は、管理者が責任を持って行う．この部分は、学内で自動化されていても手動でも構わない．なお、利用者の故意あるいは無意識の不正利用に備えて、一時アカウントと利用者の紐付けが必要であるが、これはアカウントを請求した機関が責任を持って行う．

4 商用無線 LAN サービスとの連携

4.1 市街地における eduroam サービス

大学間の無線 LAN ローミングが実現すると、次の段階として、キャンパスを越えて市街地でも eduroam を利用したいという要望が出てくるのは当然のことと考えられる．2.1 で述べたように、海外では地元のプロバイダ (ISP) や地方自治体の協力により、大学の近所のカフェや市街地において eduroam のサービスが展開されている例がある．しかし、規模としてはまだまだ限定的である．

eduroam JP では、商用無線 LAN サービスとの国内初の連携として、国立情報学研究所と株式会社ライブドアによって 2010 年 3 月に「国際学術無線 LAN ローミング基盤 eduroam の共同実証実験」が開始した [8]．この実証実験では、ライブドア社が運営する公衆無線 LAN サービス「livedoor Wireless」のアクセスポイントで eduroam のサービスを提供することで、新規にアクセスポイントを設置することなしに、市街地での eduroam 利用を可能としている．実験開始の 3 月の時点では、同社が関東地域のカフェや会議場、大型店舗に所有する約 130 基の屋内アクセスポイントで eduroam が利用可能となった．7 月には東京・山手線内側の約 2,200 基の屋外アクセスポイントにもサービスが拡大された．

商用無線 LAN サービスとの連携のイメージを図 4 に示す．このような連携は、技術的には市街地での eduroam サービスを実現したということに過ぎないが、そのインパクトとしては「キャンパスの仮想的拡大」と見なすことができる．従来は図書館、学術クラウドなどへの自由なアクセスがキャンパス内に限定されていたものが、大学の所属メンバーであれば市街地でもこれらに容易にアクセスできることになり、キャンパスの垣根を越えて教育・研究・

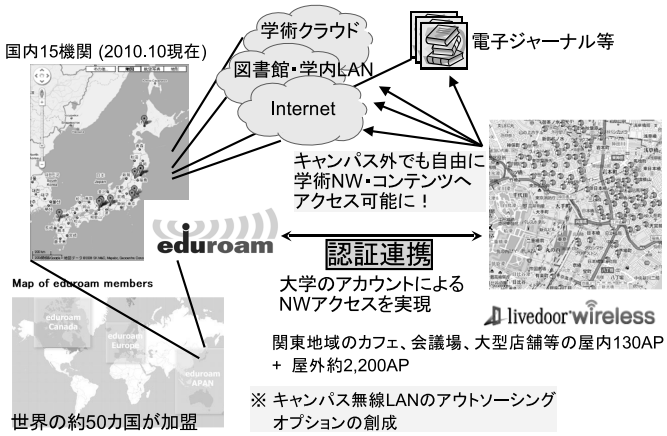

図 4: eduroam と商用無線 LAN サービスの連携

学習の場が広がることになる．

4.2 通信事業者によるアクセスポイント整備

大学によっては、自前で無線 LAN システムの設計から構築までが可能なこともあるが、アクセスポイントの死活監視などの手間を含めた運用のコストは意外に高い．特に、スタンドアロン型のアクセスポイントを自前で大量導入することは避けるべきである．実際に、欧州の多くの機関でコントローラ型のアクセスポイントシステムに置き換えが進んでいることが報告されている．

各機関で設計・構築の手間を極力かけずにアクセスポイントシステムを整備する方法としては、通信事業者に委託するのが最も有望と考えられる．すなわち、システム構築から運用・管理までアウトソーシングすることである．機関はアカウント発行とユーザサポートに注力できるようになる．

もし無線 LAN システムを含むキャンパスネットワーク全体を、通信事業者に整備・運用を委託できれば、キャンパス内で商用無線 LAN サービスの提供も可能となり、企業からの出席者の多い学会の場や、市民の出入りの多い図書館などにおいて、ネットワークアクセスの便を図ることが可能となるだろう．大学等から見れば、アウトソーシングによる効率化、低コスト化が期待できる．また、通信事業者がシステム構築を行うことで、システムの安定運用も期待できる．

一方、携帯電話のコンテンツのリッチ化やスマートフォンの隆盛、PC 用 3G モデムの普及によって、小規模な集会でさえも、キャンパス内で携帯電話網が容易に飽和することが現在問題となっている．通信事業者によるキャンパス無線 LAN の整備は、データ通信を無線 LAN に逃がす、いわゆる「3G オフロード」の観点でも有望である．通信事業者から見れば、大学構内へのサービスエリア拡大や、携帯電話・スマートフォンのサービス向上、設備投資の低コスト化などのメリットがあると考えられる．

5 まとめ

「eduroam 仮名アカウント発行システム」や「代理認証システム」の提供により、各機関では eduroam のアカウントを容易に取得できるようになった．商用無線 LAN サービスとの連携も始まり、関東地区では市街地でも eduroam が利用可能となった．学内の無線 LAN システムをアウトソーシングできれば、通信事業者の整備による安定したキャンパス無線 LAN サービスを実現しつつ、機関における eduroam 導入の手間と運用コストを抑えられる可能性がある．

近々無線 LAN システムの新設あるいは更新の予定がある機関には、新世代のキャンパスネットワークの構築を目指して、eduroam に対応したシステムの導入を奨めたい．

参考文献

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

[2] eduroam (world site) : http://www.eduroam.org/

[3] eduroam JP: http://www.eduroam.jp/

[4] 後藤英昭, 曽根秀昭, “eduroam による大学間無線 LAN 連携と国内外の動向,” 平成 21 年度 情報教育研究集会 講演論文集, 2009.

[5] 学術認証フェデレーション (GakuNin): https://upki-portal.nii.ac.jp/docs/fed

[6] TLS encryption for RADIUS: http://tools.ietf.org/html/draft-ietf-radext-radsec-07

[7] UPKI イニシアティブ: https://upki-portal.nii.ac.jp/

[8] 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.