# eduroam による大学間無線 LAN 連携と国内外の動向

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：** 欧州で高等教育・研究機関の無線 LAN の相互利用環境が構築されたことに端を発する eduroam (エデュローム) は、現在では欧州 36 か国の他、アジア太平洋地域にも普及してきている．日本では、国立情報学研究所の主導による全国大学共同電子認証基盤構築事業 (UPKI) における認証連携のアプリケーションの一つとして、eduroam JP の名で運用されている．本稿では、eduroam によるキャンパスユビキタス環境実現の概要を述べ、国内外における動向を紹介する．また、一千規模の多数の機関を効率的に eduroam に接続し、安定なシステムを実現するための技術開発を、併せて紹介する．

## 1　はじめに

近年、無線 LAN システムを既に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、ネットワーク管理の立場からは、このような新しい授業方法を支援していく必要もある．

従来のキャンパス無線 LAN(あるいは有線ポート) のシステムは、機関ごとに構築され、基本的に機関内の者だけが利用できるシステムがほとんどである．しかし、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キャンパスで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、現地で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 はアジア太平洋地域にも普及してきており、現在、日本でも eduroam JP の名で運用されている [1, 2, 3]．一方、日本には 1,200 をこ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 の認証連携の仕組みのままでは大規模な展開・導入が難しく、何らかの対策が必要である．

本稿では、eduroam によるキャンパスユビキタスネットワーク環境の実現の概要を述べ、国内外における動向を紹介する．機関の eduroam 導入のしきいを大幅に下げ、大規模な無線 LAN ローミング基盤を安定に運用するための技術開発も、併せて紹介する．

## 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 はヨーロッパの 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る [1, 2]．2009 年 9 月の時点で、欧州 36 か国が eduroam に加盟している．

欧州で eduroam が急速に発展した背景として、欧州では国内に限らず隣接諸国の大学等とも教育・研究交流が盛んであり、機関や国をまたがっても利用できるネットワークアクセス手段が切望されていたことが挙げられる．商用無線 LAN サービスの普及率や、相互運用性、利用料金なども、eduroam 普及の大きな要因と言われている．

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．

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、カナダが加盟済みである．

### 2.2 eduroam の仕組み

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

基本的な eduroam では、IEEE802.1X に基づいたユーザ認証が行われる．図 1 には、日本 (jp) の機関 D のユーザがオーストラリア (au) の機関 A において無線 LAN を使おうとしているシナリオが描かれている．アクセスポイントには、オーセンティケータと呼ばれる仕組みが備わっており、ユーザ認証が成功しなければ、利用者の端末はネットワークに接続することができない．

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．認証情報はオーセンティケータの上位の RADIUS プロキシに転送され、さらに複数の RADIUS 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．機関 D 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．

なお、認証情報のやりとりは、所属機関の RADIUS サーバと端末をエンドポイントとする暗号化されたトンネルを介して行われる．従って、アクセスポイントや中間の RADIUS プロキシでは、利用者のパスワードを盗み見ることはできない．

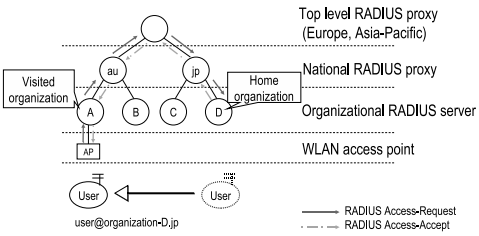


図 1: eduroam のしくみ

### 2.3 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 [4]．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 月に東北大学がオーストラリアにある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．UPKI 事業の参加機関を中心に eduroam に接続、実証実験を行った後、eduroam JP の名で国内運用を開始した．

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．2009 年 9 月の時点で国立情報学研究所、北海道大学、東北大学、山形大学、尚絅学院大学、高エネルギー加速器研究機構、名古屋大学、京都大学、京都教育大学、大阪大学、九州大学の計 11 機関が eduroam に接続済みである．

図 2 に加盟機関のマップを、図 3 にネットワーク図を示す．日本のトップレベルのサーバは、プライマリ (NII) とセカンダリ (東北大学) の二台あり、冗長構成により可用性を高めている．

## 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、以下の二つの機能を統合して導入することはもちろん可能であるが、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
- 認証情報の管理 (アカウント管理、認証連携)

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

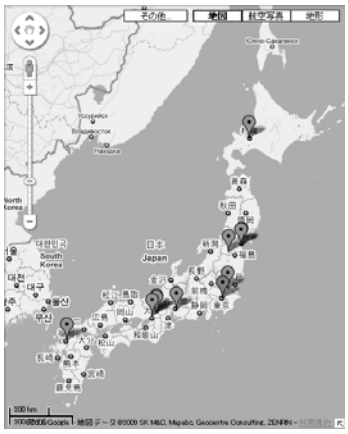

図 2: eduroam JP 加盟機関マップ (2009 年 9 月現在, Google Maps にて)

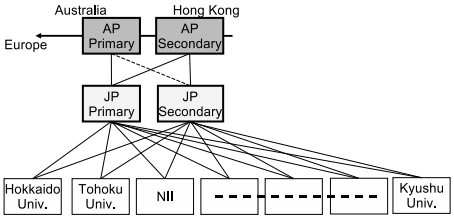


図 3: eduroam JP ネットワーク

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、認証連携の仕組み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 に加入するためには、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. ハードウェアとしては PC サーバ程度、あるいは小型アプライアンスの規模で十分である. アクセスポイントが必要ならば、一台だけでも eduroam の運用は開始できる. しかしながら、教職員・学生にアカウントを発行することを考えると、運用の手間が意外に大きいことがわかる.

一方、国のトップレベル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、日本には国公立・私立を含めて約 760 の大学がある (2008 年調べ) ことから、その手間も相当に大きいものとなる. 短大等を含めると日本には 1,200 以上の高等教育機関が存在するが、この数は欧州の諸外国と比べて桁違いに大きい. 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.

様々な要素が eduroam 普及の障壁になっていると考えられるが、それらを取り払うか軽減するための技術開発や環境整備が、海外では TERENA を

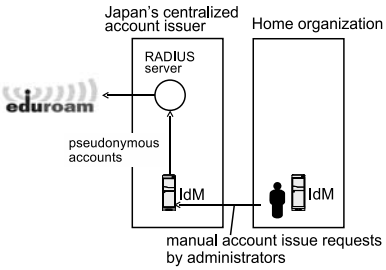


図 4: 代理認証システム

はじめ各国の NREN (National Research and Education Network) で、国内では国立情報学研究所、東北大学、京都大学などで行われている. eduroam の大規模展開に向けた取り組みの一部を、以下の節で紹介する.

## 3.2 代理認証システム

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.

解決策の一つとしては、Shibboleth SSO (Single Sign-On) [5] のように、共同電子認証基盤で今後普及が期待される汎用的な認証連携の仕組みを使い、eduroam を利用できるようにすることが考えられる. Shibboleth によって eduroam の一時アカウントを発行するシステムが、実用化に向けて京都大学および東北大学で開発中である. このシステムでは、利用者個人が Shibboleth でユーザ認証を受け、条件を満たしていれば個人用の eduroam 一時アカウントが発行される. eduroam のユーザ認証は、日本のトップレベル RADIUS サーバに直結された代理認証サーバによって行われる. 従って、当システムを利用する機関では Shibboleth の IdP (Identity Provider) を立てるだけでよい.

二つ目の解決策として、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システムが考えられる. この方法では、学内の統合認証基盤などが構築中や計画中、あるいは Shibboleth SSO の実現が難しい場合であっても、すぐに eduroam が利用可能になる. 概要を図 4 に示す.

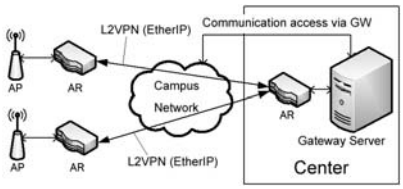


図 5: EtherIP を用いた可搬型アクセスポイント

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．

この代理認証システムは、既に実証実験として提供中である [3]．当システムでは、1 名からでも eduroam を容易に試すことができるほか、各機関の責任の下でゲスト用のアカウントを配布することも可能である．

以上の二種類の代理認証の仕組みは、eduroam の RADIUS プロキシネットワークの構造が単純になり、eduroam の可用性の向上にも貢献すると考えられる．

### 3.3 可搬型 eduroam アクセスポイント

大規模な機関では、建物内のネットワークがキャンパスネットワーク (幹線) とは別の業者によって導入・管理されていることがあり、学内共用の無線 LAN アクセスポイントの設置が容易ではないことがある．また、学外の会議場などでアクセスポイントを立てる場合、その都度の機材の設定変更は面倒である．特に、IEEE802.1X によるユーザ認証は、アクセスポイントの設定項目が多く、上位の RADIUS サーバの設定変更も必要になるため、実用的ではなかった．

学内外の eduroam 対応アクセスポイントの設置条件を大幅に緩和できるものとして、可搬型のアクセスポイントシステムを開発した．図 5 にネットワーク構成を示す．

アクセスポイント (AP) にアクセスルーター (AR) を抱き合わせて、学内 LAN などに接続する．学内の情報基盤センターなどに対向の AR を設置して、これに複数のアクセスポイントを収容する．AP の通信はすべて、AR で作られた L2VPN (EtherIP) のトンネルを介して、センターのゲートウェイに届けられる．これにより、端末とゲートウェイの間の通信もすべて学内 LAN から隔離される．AP が置かれる場所のネットワークから見ると、AR の上流のポートだけが見え、帯域を消費される以外は、利用者端末からの影響は一切受けない．

AP を別のネットワークに移動した場合でも、AR の IP アドレスを変更するだけでよく、AP は自動的にセンターのゲートウェイに収容される．もし設置場所のネットワークで DHCP (Dynamic Host Configuration Protocol) が利用できるならば、AR の IP アドレスも自動的に設定されるので、手作業の設定変更は一切不要である．AP の設定はセンターで一度行っておくだけでよい．

試作システムでは、AP にはアライドテレシス AT-TQ2403、AP 側のルーターに NEC IX2005、センター側のルーターに NEC IX3010 を用いた．

この可搬型アクセスポイントは、学内 LAN のみならず、インターネットを経由しても利用可能である．IPsec の通信が透過するならば、NAPT (Network Address/Port Translation) の裏側に AR を置いても動作する．

## 4 まとめ

eduroam による大学間無線 LAN 連携によって、教職員・学生の大学間移動に対応し、先進的な教育・研究環境の創成が期待されている．キャンパス無線 LAN システムの構築や更新は一朝一夕にはできないため、近々新設あるいは更新の予定がある機関には、eduroam にも対応したシステムを構築することを奨めたい．

eduroam の大規模な展開に備えて、認証連携を容易にする代理認証システムと、設置条件を大幅に緩和できるアクセスポイントを開発した．代理認証システムの一部は、既に実証実験として提供中であり、学術情報ネットワーク (SINET) に加入機関から利用可能である．

## 参考文献

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

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

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

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

[5] Shibboleth: http://shibboleth.internet2.edu/