[全国共同利用情報基盤センター研究開発論文集 No.28]より

Eduroam の導入と日本版アレンジ

今井 哲郎　　後藤 英昭　　曽根 秀昭
東北大学情報シナジーセンター

1. はじめに

近年，ノート PC 等のモバイルデバイスの普及により，無線 LAN の利用がますます増大している．無線 LAN のユーザは，どこでもネットワークアクセスを望むようになり，駅や学術機関においても無線アクセスの需要は拡大している．特に学術機関においては，教授同士の相互訪問や交換学生などの学術機関間の交流が盛んで，訪問先においても自分のホームと同等の環境で仕事をしたいという事例が増えており，訪問先における無線あるいは有線のネットワークアクセスをローミング技術で実現することの需要が高まってきている．

本報告では，国際研究機関間のローミング方式である Eduroam について紹介し，また日本へ導入した際の運用方式について報告する．

2．Eduroam

TERENA Task Force on Mobility[1] は教育機関のための新しいローミング基盤を策定した．この基盤は Eduroam と呼ばれ，ヨーロッパの多くの国といくつかのアジア大洋州の国に広がっている．Eduroam の参加国を図 1 に示す．

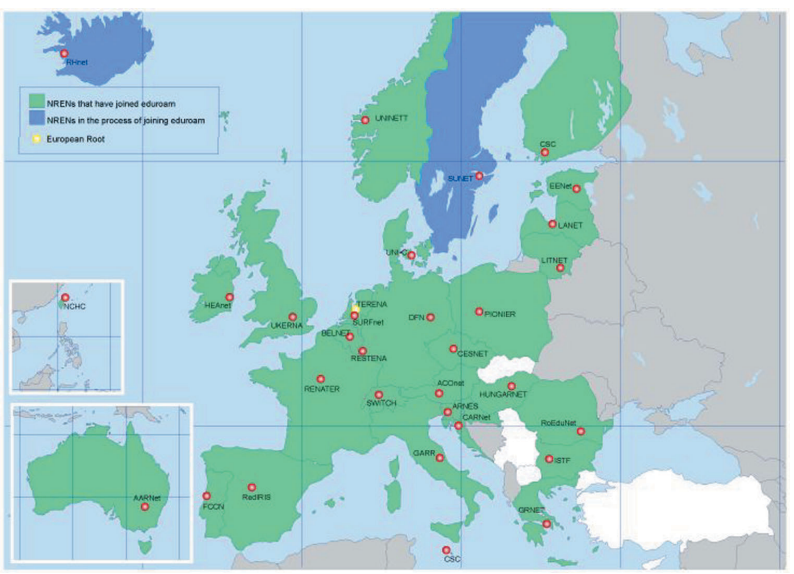

図 1　Eduroam 参加国
(http://www.eduroam.org/より引用)

TERENA は Eduroam のための技術的候補として以下の 3 つの手法をピックアップした．[2][3][4]

- RADIUS を活用した Web ベースの認証
- VPN ベースの認証
- IEEE802.1X ベースの認証

これらは以下の特徴を持つとまとめられる．

- Web：スケーラブル，セキュアでない，既に広く展開されている
- VPN：スケーラブルでない，セキュア，既に広く展開されている
- IEEE802.1X：スケーラブル，セキュア，新しい

以上のことから，TERENA では IEEE802.1X ベースの認証技術を採用することになった．IEEE802.1X は無線アクセスポイントや LAN スイッチでユーザを認証するための仕組みである．

Eduroam の技術は IEEE802.1X と RADIUS サーバのプロキシツリー構造とをベースとしている．IEEE802.1X では，EAP-TTLS[5]が推奨されている．図 2 に EAP-TTLS の概要と特徴を示す．

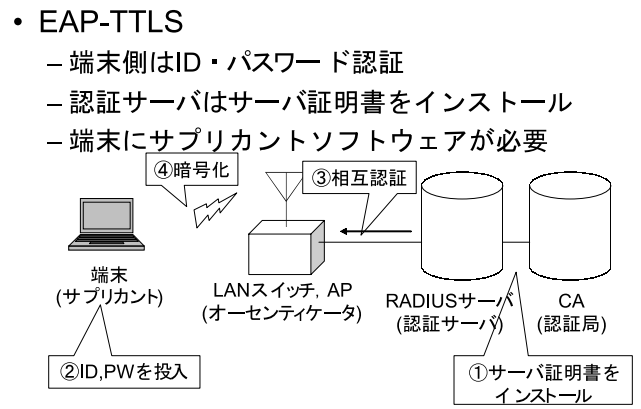

図 2　EAP-TTLS の概要

図 3 に Eduroam システムの処理を示す．ユーザが自分のホーム機関と異なる機関においてレルム名つきの ID とパスワードを入力すると，訪問先の RADIUS サーバではレルム名を参照してそれが自サーバの処理範囲にないことを確認する．そして，そのユーザの認証要求を上位のナショナル RADIUS プロキシサーバに転送し，ナショナル RADIUS サーバではレルム名を見てユーザのホーム機関の RADIUS サーバに要求を転送する(もしユーザが異なる国から認証要求を出したとすると，さらに上位のインターナショナル RADIUS プロキシサーバを介して転送される)．Ack メッセージがホーム機関の RADIUS サーバから発行されると，要求を転送したのと同じルートで訪問先の RADIUS サーバまで転送されて返ってきて，最後に Authenticator(無線 LAN アクセスポイントや LAN スイッチ)がユーザの接続を許可してユーザの認証が完了する．

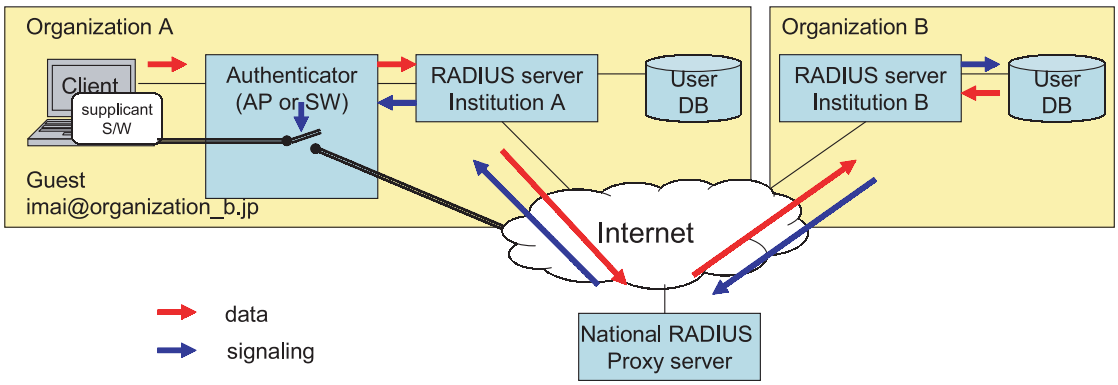

図 3　Eduroam の処理

3．Eduroam の日本への導入

3.1　導入

日本における Eduroam 導入の動きは我々が先行して行っている．8 月 31 日に RADIUS プロキシサーバの連携が完了して，実運用が開始された．図 4 に関連する RADIUS プロキシサーバを示す．

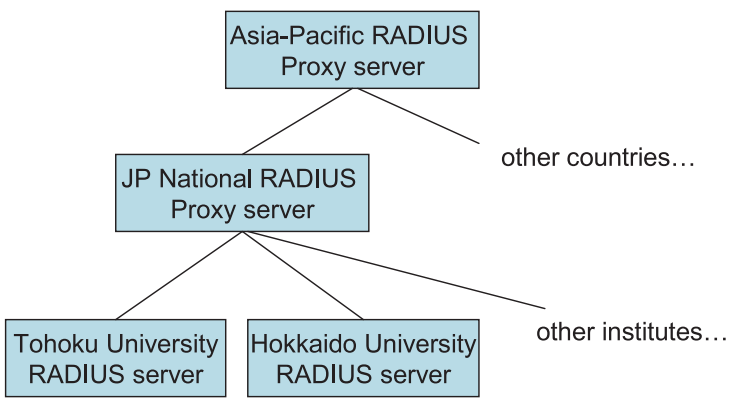

図 4　RADIUS 階層構造

今回我々が構築した東北大 RADIUS サーバと JP-RADIUS サーバは，共にハードウェアとして NEC 製の Express5800/110Gc-S を利用し，RADIUS サーバソフトウェアとして FreeRADIUS1.1.3[6]を利用しており，またこれには proxy.conf の記述において正規表現を許容するためのパッチを当てている．さらに IEEE802.1X では，我々は EAP-TTLS を採用し，サプリカントソフトウェアとして SecureW2[7]を採用した．また我々は Eduroam 対応の無線アクセスポイントとして NEC 製の AP-E201 を使った．

また，我々は日本における Eduroam の Web サイトを立ち上げた[8]．2006 年 9 月 29 日現在，お知らせがあるだけの簡素なサイトであるが，順次，Eduroam の参加方法や

freeRADIUS の設定方法，利用可能な無線アクセスポイントなどの情報を載せていく予定である．

3.2　IP アドレス付与時の問題

Eduroam では通常，訪問先のアクセスポイントによって認証されたユーザは，訪問先の IP アドレスを付与してもらうことでインターネットへのアクセスを実現する．ここでは，訪問先の IP アドレスを利用させることのリスクについて述べる．

インターネットのコミュニティでは，通常 IP アドレスは組織の情報として扱われる．すなわち，訪問先の IP アドレスを利用しているユーザは，訪問先の組織の人間だとして扱われる．したがって，例えば訪問先の IP アドレスを利用しているユーザが不正アクセスなどの攻撃を行った場合には，攻撃を受けたネットワークの管理者はログを調べ，訪問先の IP アドレスを持ったユーザが攻撃を行ったことを特定し，訪問先の組織のネットワーク管理者に対して苦情を訴えることになる．このように，ユーザに訪問先の組織が自前の IP アドレスを使わせることは，ユーザ行動に対する責任をも担うことになるのである．

また，訪問先の IP アドレスを利用するので，例えば自分のホーム機関に IP アドレスによるフィルタリングを施したリソースが存在した場合には，そこへはアクセスできない．アクセス制御装置は，ユーザが訪問先の IP アドレスをつけていることによって，訪問先の組織のユーザと判断してしまうからである．これらの IP アドレス付与の問題を，図 5 に示す．

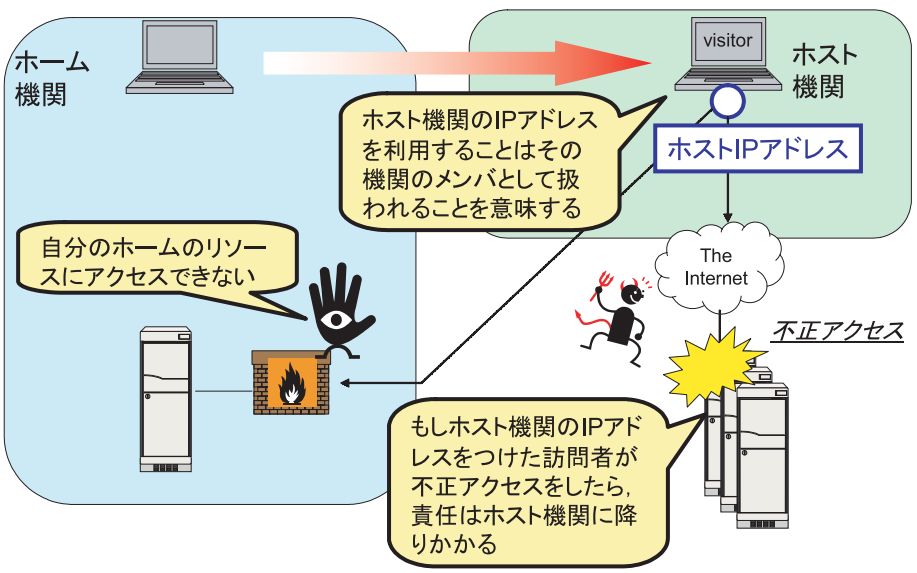

図 5　付与された IP アドレスに関する問題

我々は上記の問題を解決するために，Eduroam で認証を行ったユーザに対して，VPN サーバに対する VPN 接続確立要求のパケットと VPN パケットのみを通すようなアクセ

ス制御を行う．このようにすることによって，ユーザに自分のホームの VPN サーバへアクセスさせ，自分のホームの IP アドレスを利用してインターネットへアクセスをさせることができる．ただしこの場合，ホームの場合と同様，訪問先のアクセス制限のあるリソースにはアクセスできなくなる．図 6 に，Eduroam の日本での運用でとった対策を示す．東北大では，日本ではこの Eduroam を VPN 限定で運用する方式を推奨する．なおこの VPN 限定方式は，日本独自の方式ではなく，実際に Eduroam を VPN だけで運用している例も既に存在している．また，この運用が Eduroam の仕様上も問題がないことが確認されている．

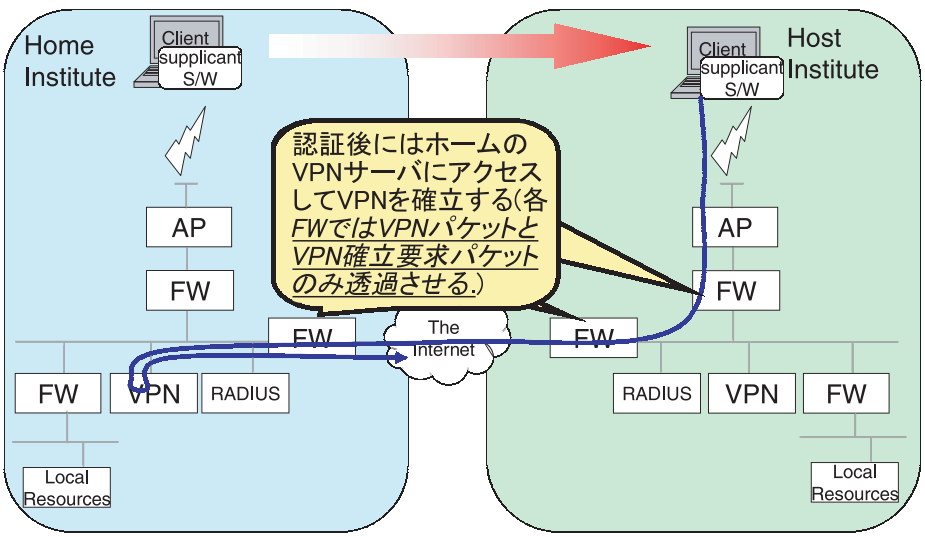

図 6　Eduroam の日本での運用

3.3　議論

前述のように，Eduroam のコミュニティでは，VPN を利用した認証方式はスケーラブルでないとしている[3]．これは，ネットワーク管理者がアクセス制限を行う際にはアクセス制御装置で透過させる全ての IP アドレスを設定する必要があり，その数は数千にも及ぶからであるとされる．しかし，我々の方式では，透過させるポート番号のみを記述することによって，この問題を回避している．例えば，ユーザが VPN として PPTP を利用する場合には，ファイアウォールなどのアクセス制御装置には，PPTP パケット 1723 と GRE パケット 47 のみを透過させると設定するだけでよい．こうすることによって，ユーザは VPN パケットであれば世界中の VPN サーバに送ることができてしまうが，我々はそれでも本手法は十分なセキュリティを保っていると考える．

4. まとめ

本稿では，Eduroam の紹介と日本への導入と Eduroam の日本版アレンジについて述べた．今後は，ユーザに自分のホームの IP アドレスを使わせるだけでなく，訪問先の IP

アドレスをも利用させることによって，訪問先のリソースへの接続性を確保するなど，日本独自の改良を加えた東北大方式を提案していく予定である．

[参考文献]
[1] TERENA Task Force on Mobility, http://www.terena.nl/activities/tf-mobility/
[2] "Inventory of web-based solution for inter-NREN roaming," http://www.terena.nl/activities/tf-mobility/deliverables/delF/DelF-f.pdf
[3] "Inventory of VPN-based Solutions for Inter-NREN Roaming," http://www.terena.nl/activities/tf-mobility/deliverables/delE/DeliEv4.4-np.pdf
[4] "Inventory of 802.1X-based solutions for inter-NRENs roaming," http://www.terena.nl/activities/tf-mobility/deliverables/delD/DelD_v1.2-f.pdf
[5] EAP-TTLS, http://tools.ietf.org/wg/eap/draft-funk-eap-ttls-v1-01.txt
[6] FreeRADIUS, http://www.freeradius.org/
[7] SecureW2, http://www.securew2.com/
[8] Eduroam-JP website http://www.eduroam.jp/