[全国共同利用情報基盤センター研究開発論文集 No. 34 より]

キャンパス無線 eduroam の耐災害性・耐障害性向上と高機能化

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

1　はじめに

2006 年に日本が国際的な学術無線 LAN ローミング基盤である eduroam (エデュローム)[1]に参加して以来, 徐々に参加機関が増え, 2011 年末に 27 だった国内の機関数は 2012 年 9 月現在では 39 となり, 順調な増加傾向にある[2]. 大学 ICT 推進協議会年次大会[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 3.1%に留まっている. 機関への eduroam 導入の障壁の一つとして, 機関ごとの RADIUS サーバの導入・管理にかかる労力および経費の高さが考えられ, この問題に対処するために, サイバーサイエンスセンターでは「eduroam 代理認証システム」を開発して, 2008 年よりサービス提供してきた.

代理認証システムは, 低い導入・管理コストと高い安定性を実現する eduroam の新しいアーキテクチャとして世界的にも注目されているが, 従来の実装では IdP (ID プロバイダ)の機能が単一故障点となる問題があり, 実際に 2011 年の東日本大震災では広域停電の影響を受けた[4]. 当システムの耐災害性および耐障害性を向上させるために, IdP を地理的分散させたクラウド型の認証基盤を構築したので, 本稿で紹介する.

一方, eduroam には機能の高度化の要求もある. サイバーサイエンスセンターCSI 研究室では, OpenFlow 技術を用いて, 機関のポリシーと利用者の属性情報に基づいたアクセス制御を実現する方式を開発した. 詳細は参考文献[4],[5]で示したが, 本稿ではその概略を述べる.

2　eduroam 代理認証システムの耐災害性・耐障害性の向上

代理認証システムは, eduroam の認証基盤をウェブサービスとして代行・提供するものであり, 各機関の管理者はウェブ画面から必要数の eduroam アカウント(ID とパスワードのペア)を随時請求, 取得できる. eduroam のユーザ認証は, 機関ごとの RADIUS IdP ではなく代理認証システムによって行われる. 本システムを利用することにより, 各機関で RADIUS IdP を導入・運用する必要がなくなり, 機関管理者のサインアップのみで eduroam を利用開始できるようになる. もし機関が無線 LAN 基地局の運用をシステムインテグレータやインターネットサービスプロバイダ(ISP)などに委託すれば, 基地局を収容する RADIUS proxy の管理も不要となる.

2012 年 9 月現在, 代理認証システムは 13 機関に利用されている. このうち 2 機関は, 代理認証システムを当初利用していたが, 学内のインフラ整備に伴って RADIUS IdP を構築し, 補助用として代理認証システムの利用を継続している. 4 機関は主システムとして日常的に代理認証システムを利用しており, 他の 1 機関は数か月内に自前の RADIUS IdP を立ち上げるとされる. その他の機関は補助用の IdP として利用している. このように, 代理認証システムは機関の eduroam 参加の障壁を下げるのに役立っている.

2011 年 3 月 11 日に発生した東北地方太平洋沖地震では, 地震の揺れの最中から東日本で大規模な停電が発生し, 数時間後に無停電電源装置のバッテリが切れた後は, 東北大学に設置されていた eduroam 関係のサーバ群も停止した. サイバーサイエンスセンターは学内の情報インフラの拠点であり, 優先的に電源復旧作業が進められたが, それでも再通電まで約 2 日間を要した. 日本国内のインフラである eduroam JP では, トップレベル RADIUS proxy のプライマリサーバが国立情報学研究所(東京都), セカンダリサーバが東北大学(仙台市)に設置されていたが, このような冗長構成が功を奏して, 国内の eduroam が停止することは避けられた. 大地震の直後から初期の復旧作業にかけて, 部分的ではあるものの, eduroam が緊急連絡手段として有効に使われたことが判明している. この時の様子は文献[6]で報告済みである.

代理認証システムのサーバは東北大学に設置されており，当時はまだセカンダリサーバの構築は計画段階であった．このため，3 月の大地震の際には広域停電の影響を受け，停電のなかった関東地区の大学においても，2 日間に渡って eduroam が利用できなくなるという問題があった．これは被災時のネットワーク利用環境を維持するという観点でも問題であり，改善が急務であった．2012 年に入り，株式会社データホテル(旧ライブドア)より同社クラウドサービス「EX-CLOUD」のサーバ無償提供の申し出があり，今回これを利用して代理認証システムを冗長化し，クラウド型の代理認証システムを構築した．システム構成を以下に説明する．

代理認証システムの構成要素は大きく分けて，(1) ウェブユーザインタフェース(CGI プログラム群)，(2) SQL データベース(PostgreSQL DB)，(3) RADIUS インタフェース(FreeRADIUS) の 3 つがある．ウェブインタフェースの機能を冗長化するには，データ変更の同期や排他制御の処理が複雑となり，システムの大幅な変更が必要である．しかし，被災時に eduroam の認証処理が継続できることが最も重要であり，新規ユーザ作成などのアカウント管理はそれほど緊急性を要しないとみなせる．そこで，主システムの復旧にはそれほど日数を要しないという前提で，ウェブインタフェースの冗長化は今回見送った．

図 1 に，代理認証システムの冗長化の様子を示す．主システムであるマスタサーバは従来どおり東北大学に設置，運用継続する．東京にある EX-CLOUD の仮想マシン上に PostgreSQL DB と FreeRADIUS をインストールして，レプリカサーバを構築した．SQL データベースには，ウェブインタフェース用の管理者アカウント情報と，RADIUS 認証に必要な eduroam アカウント情報が格納されているが，後者のみを同期すれば十分である．eduroam JP のトップレベル RADIUS proxy には，代理認証システムのマスタサーバをプライマリサーバ，レプリカサーバをセカンダリサーバとしてそれぞれ登録し，代理認証システム用のレルム名を持つアカウントの認証要求を，これらのサーバに転送するように設定した．通常はマスタサーバのみに認証要求が転送されるが，例えば東北大学の停電や，何らかの障害によってマスタサーバが応答できない場合は，転送先が自動的にレプリカサーバに切り替わる．

マスタサーバとレプリカサーバのデータの同期には Slony-I (2.x 系)を用い，マスタからレプリカへの一方向の同期とした．アカウント管理の機能がマスタ側にしかないので，一方向で十分である．また，アカウントの作成，削除，一時停止などの操作は頻繁に行われるものではなく，多少の遅れがあっても実用上問題がないため，同期確認間隔は Slony-I の最大値である 1.0 秒に設定した．

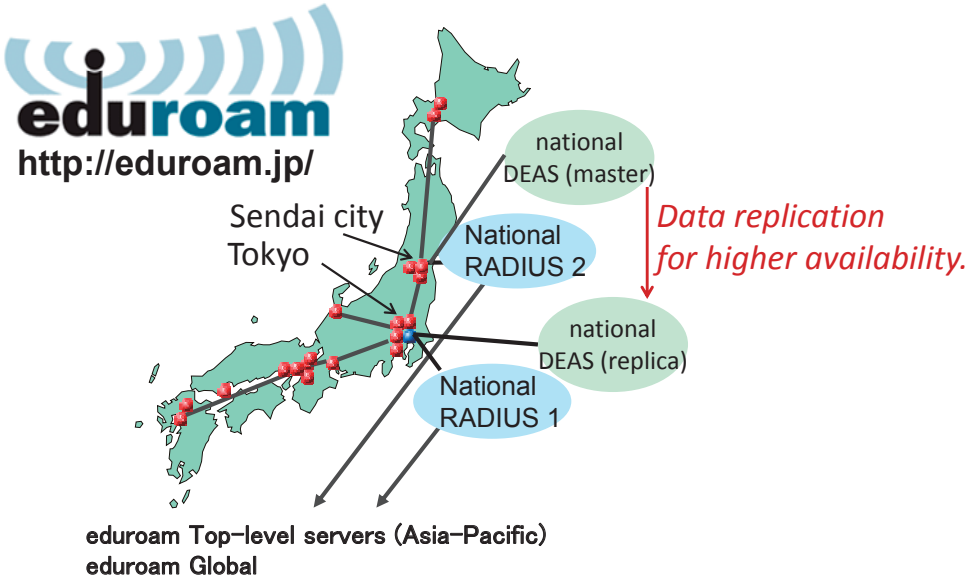

図 1. クラウド型代理認証システムにおけるデータベースの冗長構成

株式会社データホテルでは，公衆無線 LAN サービス livedoor Wireless における eduroam サービスの提供[7]に加えて，各大学のキャンパス無線 LAN システムの構築も手掛けている．同社の顧客の多くが代理認証システムを利用していることから，同社の基地局を利用する学内利用者の認証リクエストの多くが日本のトップレベル RADIUS proxy を通過することになり，混雑による性能低下の懸念があること，および，各大学に RADIUS IdP を設置する従来方法と比べて RADIUS proxy のホップ数が多くなり，安

定性が低下する恐れがある．これら問題は，基地局を設置した業者に代理認証システムのレプリカサーバを持たせることで解決できると考えられる．今回構築したシステムでは，同社がレプリカサーバの方をプライマリ IdP とみなして認証要求を転送するように設定することで，RADIUS 認証のバイパス経路を構成でき，安定性の向上が期待できる．このような構成による運用は執筆時点において検討中であるが，負荷分散の有効な手段になると考えられる．

3　利用者の属性情報に基づく eduroam のアクセス制御の高度化

eduroam の運用の現場では，ID のレルムを見て機関のメンバーとゲストの端末を区別し，異なるサブネットに収容するといった単純なアクセス制御は従来も可能であったが，より高度なアクセス制御を実現する標準的な仕組みは存在しない．利用者の種別に応じた詳細なネットワークアクセス制御が可能になれば，利便性やセキュリティの向上につながると考えられる．

利用者の所属機関と訪問先機関では，それぞれがアクセス制御のポリシーを有する．一例を以下に示す．

所属機関のポリシー(例)：

- 自機関の教職員・学生のネットワーク利用に特にアクセス制限は設けないが，ファイアウォールを通して，アクセスログを採取する．
- 学生にはトラブルの生じがちな特定のウェブ掲示板やファイル交換サイトを訪問先機関で利用させないようにしたい．利用帯域も制限したい．(訪問先に対するリクエスト)
- 教職員には訪問先でも比較的自由なネットワークアクセスを許可したい．(訪問先に対するリクエスト)
- 訪問先機関が許可した場合，教職員については訪問先のファイルサーバやプリンタなどの利用を許可する．(訪問先に対するリクエスト)

訪問先機関のポリシー(例)：

- 訪問者の学生には特定のウェブ掲示板やファイル交換サイトを利用させないようにする．利用帯域も制限する．
- 訪問者の学内サーバへのアクセスは原則禁止とするが，非常勤講師には許可する．
- 会議等において，その場で利用権限を付与して，訪問者にファイルサーバやプリンタなどのローカルサービスの利用を許可する．

このような複雑なポリシーを元にアクセス制御を行うには，ポリシーやルールの記述方法の標準化が必要である．しかし，汎用的な記述方法を設計するのは大変難しいと考えられる．そこでまず初めに，ポリシーおよびルールを単純化したモデルを採用することとし，機関のポリシーと利用者の属性情報に基づいたアクセス制御を実現する方式を開発した[4][5]．ローカルサービス(リソース)の利用の可否はネットワークのアクセス制御によって行う．システムの概要を図 2 に示す．

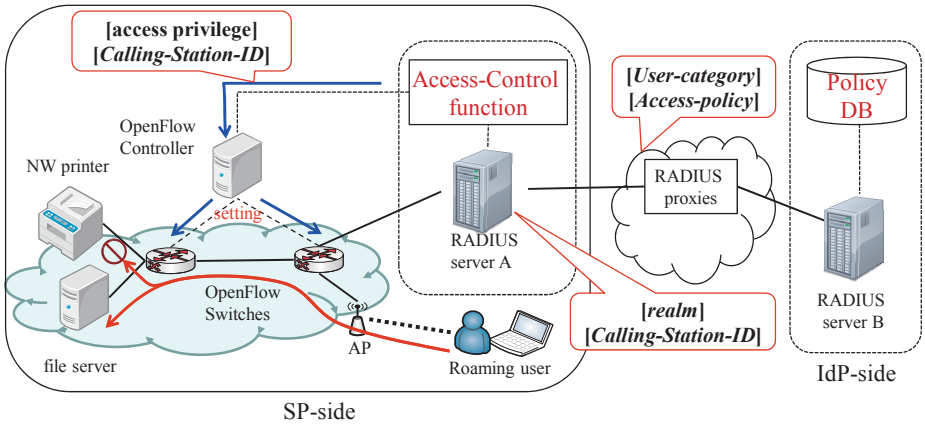

図 2. 属性情報に基づいたアクセス制御が可能な eduroam システム

IdP となる RADIUS サーバにはポリシーを格納したデータベースが接続される. 利用者ごとの eduroam アカウントには，利用者の種別やアクセス範囲を示す識別子が属性情報として付与されている．ある機関において訪問者がユーザ認証の手続きを開始すると，RADIUS プロトコルの通信パケットに埋め込まれた属性情報が訪問先機関の RADIUS サーバに届けられる．両機関のポリシーを突き合わせ，利用者の属性情報と組み合わせることによって，ネットワークアクセス制御のためのルールが生成される．このルールは OpenFlow コントローラに渡され，OpenFlow スイッチの動作が決定される．図 2 には，利用者がファイルサーバにアクセス可能だが，プリンタは利用できないというシナリオが例示されている．

ポリシーや属性情報が複雑になるにつれて，アクセス制御に必要な VLAN の数も非常に多くなることがある．OpenFlow 技術を用いることで，VLAN の総数に実用上制限のない dynamic VLAN が実現できる．また，システム内のすべての OpenFlow スイッチの制御を一台のコントローラで一括して行うことが可能である．このような OpenFlow の特長を生かして，eduroam のアクセス制御システムを構築することにより，単純なハードウェア構成で所望の機能を実装できた.

4 むすび

本稿では，平成 23〜24 年度にサイバーサイエンスセンターで実施した業務の成果として，耐災害性・耐障害性を向上させたクラウド型の代理認証システムと，利用者の属性情報に基づく eduroam のアクセス制御の高度化について紹介した. 両方とも，TF-MNM(モバイル通信とネットワークミドルウェアに関する TERENA のミーティング)や国際会議などで，国際的に方式提案を行なっている.

参考文献

[1] L. Florio, K. Wierenga, “Eduroam, providing mobility for roaming users,” EUNIS 2005, June 2005.

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

[3] 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.

[4] T. Watanabe, S. Kinoshita, J. Yamato, H. Goto, and H. Sone, “Flexible Access Control Framework Considering IdP-side’s Authorization Policy in Roaming Environment,” IEEE 36th International Conference on Computer Software and Applications Workshops, COMPSAC-MidArch 2012, pp.76-81, July 16-20, 2012 (Izmir).

[5] S. Kinoshita, T. Watanabe, J. Yamato, H. Goto, and H. Sone, “Implementation and Evaluation of an OpenFlow-based Access Control System for Wireless LAN Roaming,” IEEE 36th International Conference on Computer Software and Applications Workshops, COMPSAC-MidArch 2012, pp.82-87, July 16-20, 2012 (Izmir).

[6] 後藤英昭，曽根秀昭，“災害時における eduroam 全学無線 LAN の有効性とキャンパスアクセスネットワークの運用,” 電子情報通信学会 2012 年総合大会講演論文集 BS-6-1, pp.98-99, 2012.

[7] 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