eduroamで作る災害に強い大学間連携キャンパス無線LAN

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： 学術無線 LAN ローミング基盤である eduroam(エデュローム) は，国内の参加機関数が昨年末の 27 機関から 43 機関 (2012 年 11 月現在) まで増加した．この成長には，我々が開発しサービス提供している「代理認証システム」も貢献している．2011 年の東日本大震災では，eduroam に限らず大学の情報インフラの抱える問題が明らかになり，防災・減災に関する様々な知見がもたらされた．本報告では，被災時における eduroam 利用・運用の経験を紹介し，無線 LAN ローミングの有用性を示すとともに，災害に強いキャンパス無線 LAN システムの構築を提案する．また，クラウド型で耐災害性・耐障害性を向上させた新しい代理認証システムを紹介する．

1 はじめに

2011 年 3 月 11 日に発生した東北地方太平洋沖地震では，揺れの最中に広域停電が発生し，仙台市中心部においても電源復帰 (復電) まで 1〜2 日間を要した．大学のネットワークやサーバ類も数時間でバックアップ電池が尽きて 2 日間以上停止した．この災害は，大学の情報インフラの抱える問題をあぶり出し，防災・減災に関する様々な知見をもたらした [1].

筆者らは国立情報学研究所 (NII) と共同で，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) の国内運用・展開を行っている [2]. eduroam は，2006 年に日本が参加して以来，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 11 月現在では 43 となり，順調な増加傾向にある．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 3.5%に留まっている．eduroam 導入の障壁として，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，筆者らは「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であるが，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，実際に東日本大震災では広域停電の影響を受けた [1].

本報告では，被災時における eduroam 利用・運用の経験を紹介し，無線 LAN ローミングの有用性を示すとともに，災害に強いキャンパス無線 LAN システムの構築を提案する．また，IdP を地理的分散させ，クラウド型で耐災害性・耐障害性を向上させた新しい代理認証システムを紹介する．

2 東日本大震災における eduroam

2.1 大地震直後のネットワーク利用環境

回線の混雑と利用制限により，大規模災害時に電話がつながりにくくなることはよく知られている．東日本大震災においても，地震発生から間もなく通話がほとんどできない状態になった．データ通信に関しては，キャリアメールや 3G データ通信/WiMAX が辛うじて利用可能であったが，この 2 年間でスマートフォンが急速に普及したこともあり，現在でも同様に利用できる保証はない．また，3G や WiMAX のいずれか一方，あるいは，両方とも利用できない地域もあった．家庭のネットワーク環境は，光/VDSL/ADSL ルータなどの電源喪失により，有線接続は一般に利用不可能となる．複数種類の無線接続手段を確保しておくのが有効なことは自明である．

大学においては，広域で長時間停電したことにより，研究室の PC やネットワーク機器はもちろん，構内電話も使えなくなり，特に市内に点在するキャンパスの間で連絡に支障が生じた．ただし，幹線ネットワークはバックアップ電源により一定時間利用可能な状況にあり，特に，一部の無線 LAN 基地局が被災直後の重要な時間帯に生き残っていたことは注目に値する．

総務省の検討資料 [4] によれば，災害時の音声通話以外の通信手段の充実・改善や，インターネット接続機能の確保，IP ネットワークの耐災害性向上などが,「今後取り組むべき事項」に挙げられてい

る．無線 LAN を含め，キャンパスネットワークの構築においても，耐災害性と減災の考えを取り入れておくことが望ましい．

2.2 被災時の eduroam の運用・利用状況

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 が非常通信手段として有効だったことが判明している．この時の様子を以下に事例紹介する．

1. サーバのログの分析から，無停電電源装置 (UPS) と PoE (Power over Ethernet) のおかげで，一部の eduroam 対応アクセスポイントが大地震発生からしばらくの間正常動作しており，停電下でも何人かが正常にネットワーク利用できていたことが判明.
   電話網が麻痺している状況で，非常通信手段として有効.
   (ただし，RADIUS サーバの自動シャットダウンが早すぎたという反省がある．)
2. サーバのログの分析から，日本を訪れていた海外の人々が，3 月 11 日の地震発生から夜間にかけて，eduroam を正常に利用できていたことが判明.
   国際的な無線 LAN ローミング基盤が役立った．電話網が利用できない環境下で，eduroam は強力な代替通信手段として機能する可能性がある．
3. 出張していたと思われる人々が，大地震の直後から，訪問先の機関で eduroam を正常に利用できていた.
   大学間無線 LAN ローミングが有効に機能した.
4. 東北大学において，まだ有線ネットワークが復旧していない館内で，復旧作業の過程で最寄りの建物からの eduroam の電波を利用していたという事例があった.

以上のような経験から，学内の部局間のみならず，大学間でも無線 LAN をローミング対応にしておくことは，平時の利便性ばかりではなく，被災時にも非常に有益であると言える．

大規模災害時には，人々が他部局の建物に避難したり，研究室のネットワークが長期に利用不可能になることもある．被災時に自分の所属大学に居るとは限らず，自宅に近い他校が避難所となることもあるだろう．また，建物が無事であっても，大地震の場合は書籍や機材の散乱，家具の転倒，照明器具やエアコンなどの落下により，有線ポートに容易に手が届かないといった状況が少なくない．前述のケース 4 のように，最寄りのネットワークが使用不可能でも，隣接する建物の無線 LAN を利用できる可能性がある．

以上の経験および考察より，キャンパス無線 LAN システムの構築にあたって，以下のことを提言したい．

- eduroam によって他機関とローミング
- 上記が不可能な場合，最低限，全学対応または学内部局間でローミング
- 平常時と同じ設定で利用可能にしておく
  (災害時に最大限に有効活用できるように)

3 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 (Delegate Authentication System, DEAS) 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．代理認証システムによる eduroam システムの簡素化の様子を図 1 に示す．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 11 月現在，代理認証システムは 15 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．5 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 2 機関は近い将来に自前の RADIUS

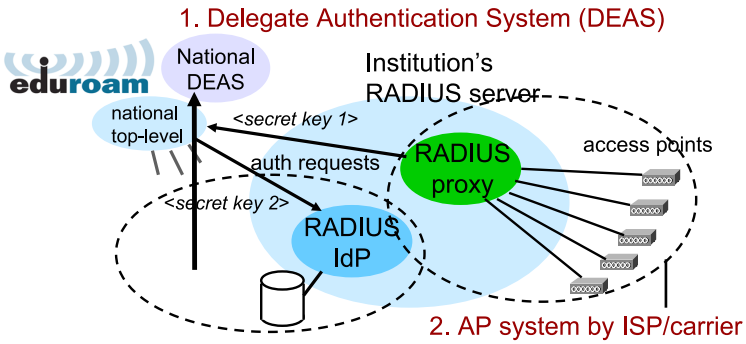

図 1: 代理認証システム (DEAS) による eduroam システムの簡素化

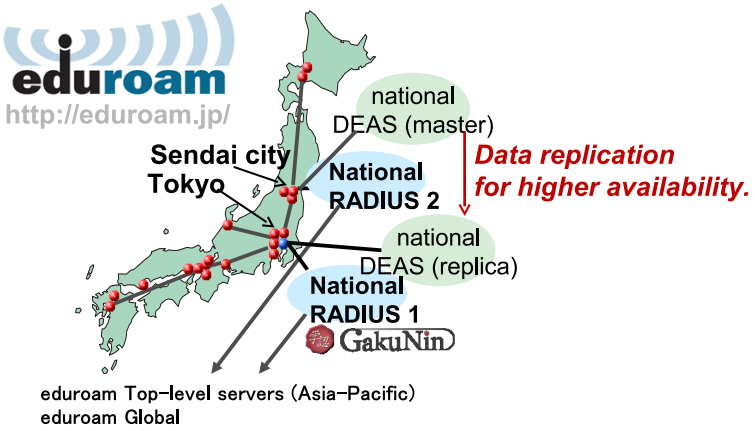

図 2: クラウド型代理認証システムにおけるデータベースの冗長構成

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．

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，東日本大震災が発生した当時はまだ，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 [5]．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 (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 つである．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 2 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，一方向の同期で十分である．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 1.0 秒に設定した．

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 [6] 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．

4 むすび

東日本大震災における eduroam 利用・運用の経験を紹介し，被災時の緊急通信手段としての有用性を示した．また，耐災害性・耐障害性を向上させた新しい代理認証システムを紹介した．

eduroam に限らず，大学の情報インフラにおいて被災時にも IdP が利用可能なことは，耐災害性の観点で重要であり，何らかの備えが必要と考えられる．機関が独自に運用している IdP の耐災害性・耐障害性の向上についても，その実現方法を今後検討していく予定である．

参考文献

[1] 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.

[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] “大規模災害等緊急事態における通信確保の在り方について最終取りまとめ (案),” 総務省・大規模災害等緊急事態における通信確保の在り方に関する検討会 (第 8 回会合) 配付資料, 平成 23 年 12 月 27 日, http://www.soumu.go.jp/main_sosiki/kenkyu/saigai/02kiban02_03000140.html (2012.11.12 参照).

[5] プレスリリース「データホテルと東北大学、学術無線 LAN ローミング eduroam JP においてクラウド型大規模 eduroam 認証サービスの産学連携提供を開始。–キャンパス無線 LAN を始めとする教育機関向け IT インフラソリューション展開を強化–」, http://www.datahotel.co.jp/release/detail/?nid=26 , 2012.10.

[6] 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.