［大学 ICT 推進協議会 2014 年度 年次大会論文集より転載］

キャンパス無線 eduroam の最新動向と国内機関向け新サービス

後藤英昭 [1]，　新妻 共 [2]，　中村素典 [3]，　曽根秀昭 [1]

[1] 東北大学サイバーサイエンスセンター
[2] 東北大学大学院 情報科学研究科
[3] 国立情報学研究所
hgot@cc.tohoku.ac.jp

概要： 学術系の無線 LAN ローミング基盤である eduroam は，世界 70 か国，国内 86 機関 (2014 年 10 月現在) に成長し，大学キャンパス以外にも様々な施設でサービス展開が進んでいる．本報告では，eduroam の国内外の最新状況を概説するとともに，国内の参加機関および学術団体のための新しい認証サービスとして，(1) 国内で開催される国際会議・国内会議等のための期間限定 eduroam アカウント発行，(2) 所属機関発行の電子メールアカウントを間接的な認証に利用するオンラインサインアップシステム，(3) EAP-TLS 認証を実現するクライアント証明書発行システムの 3 種類を紹介する．

1　はじめに

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) は，世界中の大学や研究所等において，キャンパス無線 LAN の相互利用を実現する．世界ではこの一年ほどで南米やアジア，アフリカで展開が進んでいる．[1] で既報のように，病院や空港・鉄道駅，博物館などの公共施設におけるサービスも各地で見られるようになり，eduroam サービスの厚みが増してきている．2014 年 10 月時点での国内の参加機関数は 86 であり，国内の認証基盤として，学術認証フェデレーション (学認，GakuNin)[2] と並んで近年成長が著しい．

日本国内には 1,200 を超える高等教育機関があることから，eduroam 導入の障壁を緩和し，また，利用者・管理者双方の利便性を改善することを目的として，eduroam JP では「代理認証システム」や「仮名アカウント発行システム」，SINET を利用したゲストネットワークなどを開発・提供してきた．一方，国内で eduroam サービスが利用できる大学施設や会議場が増加したのに伴い，会場の無線 LAN サービスを国際会議や学会，研究会等の参加者に提供するというニーズも見えてきた．本稿では，この需要に応えるための「会議向け期間限定 eduroam アカウントの試行」を紹介する．

eduroam JP では，eduroam インフラの利便性と耐障害性の向上のための技術開発・実証実験も継続している．本稿では，代理認証システムの拡張機能として新規開発した，「eduroam オンラインサインアップシステム」と「クライアント証明書発行システム」を紹介する．

2　国内外の eduroam の動向

2.1　国内の状況

eduroam JP の参加機関数は 2014 年 10 月時点で 86 となり，高等教育機関における普及率は約 7.2% である．機関数の推移を見ると，2006 年の日本導入以来，2011 年末 27 機関，2012 年末 43 機関，2013 年 10 月時点で 56 機関であり，この一年間で大幅に増えたことがわかる．知名度の高まりや，キャンパス無線 LAN のシステム更新時期に合わせて導入が進んでいること，教育・研究の現場における携帯端末利用の増加などが，この背景にあると考えられる．

2014 年度は，専門学校から初の問い合わせがあった．eduroam JP の正式な実施要領・運用基準はまだ策定中であるが，従来は大学・短期大学・高等専門学校が漠然と想定されていたことから，国立情報学研究所内のネットワーク運営・連携本部・認証作業部会で専門学校 (学校教育法の分類) の eduroam 参加可否について審議し，参加を認めることとした．

eduroam の利便性を向上させるために，eduroam 基地局マップのデータ提供を参加機関に呼び掛けている [1]．しかしながら，あまり協力が得られていない．現在は提出データが XML 形式のため，その編集が障害になっている可能性が高く，管理者にとって利便性の高いデータ提供手段を探っている．

2.2　世界の状況

執筆時点で世界の参加国 (地域) 数は 70 であり，大きな変化はないものの，南米やアジアの各国内での展開が進んでいる．アジア地域ではマレーシアが参加し，12 か国 (地域) に至っている．特にインドの 64 機関とタイの 18 機関 (いずれも予定を含む) は，国内展開の速さを見せている．

新興国では電源やネットワークが不安定なところもあり，そのような地域に eduroam を展開する場合，再認証を減らすことのできる安定な認証基盤が必要である．我々が開発してきた耐障害・耐災害 eduroam のアーキテクチャ[1] が応用できる可能性があるが，現時点では導入未定である．

キャンパス外の eduroam サービスとしては，ミュンヘン中心部の広場で基地局が設置されるなど，世界各地で様々な試みが見られる．スウェーデンの空港におけるサービスは今年も継続中であり，SNS 上で称賛の声を多数見ることができる．ノルウェーの空港では，2013 年に試験運用が行われていたが，2014 年 1 月に UNINETT の正式サービスとなった．

3 会議向け期間限定 eduroam アカウントの試行

国際会議では，参加者がネットワークを利用できるように，一時的に基地局を設置したり，既設の基地局のためのゲストアカウントを用意するのが通例である．このようなサービスは，外国からの参加者など，現地の携帯電話網を利用しにくい人々にとって重要である．会議情報やプロシーディングス等を閲覧する目的でも，高速な無線 LAN は利便性が高い．大規模なイベントでは，参加者が持ち込むモバイルルータによる混信が原因で，大勢がネットワークを利用できなくなる問題がある．より快適な基地局を会場で提供し，それに誘導することが望ましい．

会議ごとに基地局を立てる方法は，機材の調達や技術者の確保はもちろん，会場との調整も必要になり，実現にかかるコストが大きい．会場に大容量の基地局が既設であれば，混信等のトラブルも少なく，安定なサービスを提供しやすい．国内で eduroam サービスが利用できる大学施設や会議場が増加したのに伴って，会場の無線 LAN サービスを会議参加者に提供するというニーズが見えてきた．

会場に eduroam 対応の基地局がある場合，参加機関の利用者は各自のアカウントでそのままネットワークが利用できる．しかし，国内外ともに eduroam に未参加の機関もまだ多く， 企業の研究所のように eduroam に参加できない機関からの参加者も多い．会議運営者が eduroam 参加機関の構成員であるとは限らず，参加機関であってもアカウントの発行には責任が伴い，ゲスト用に発行するのが難しいという側面もある．会議で eduroam 対応基地局を利用するためには，会議運営者が自身の責任の下でゲストアカウントを容易に取得，配布できる仕組みが必要である．eduroam JP ではこれを実現するための技術と実施要項を検討し，7 月に「会議向け期間限定 eduroam アカウントの試行」を開始した．

ゲストアカウントの発行には，我々が開発して 2008 年より実証実験として eduroam 参加機関に提供している，「代理認証システム」を用いた．会議主催者を仮想的な機関とみなして，同システムの「機関」として一時的に登録し，アカウント発行権限を会議運営者に渡す仕組みである．なお，機能的な拡張は一切行っていない．代理認証システムの利用者 ID には，通常は “< 大学名 >.eduroam.jp” の形式のレルム名が付くが，ゲストアカウントを一般の機関のものと区別するために，会議名と年を基本とする会議略称に comf/symp/mtg などを付加したものをレルム名とするルールを課した．例えば会議略称が EMC14 の場合，レルム名を “emc14-conf.eduroam.jp” のようにする．会議主催者が事前に，会議の正式名称，主催者名，責任者名，実務担当者，会議ウェブサイト，会議期間，アカウント有効期限と発行見込み数などの情報を記入した申請書を代理認証システム管理者に送付し，承認を受けることにより，当サービスを利用できるものとした．

eduroam のアカウント発行はその主体となる機関の責任の下で行われるが，国内の eduroam 運用については eduroam JP にも部分的に責任が及ぶ．このため，当サービスの利用は国内の会議施設・大学施設などで開催される国際会議・国内会議を当面の主な対象として，以下の提供条件を定めた．

- 代理認証システムの登録と同様に，会議名 (システム上は機関名)，責任者 (会議代表者)，実務担当者を登録すること．
- 会議主催者は SINET 加入機関または学術団体 (学振認定) であること．
- 実務担当者は SINET 加入機関 (eduroam 参加機関が望ましい) の職員であること．

実務担当者は，以下に従う必要があるものとした．

- 当サービスの利用が許可された後，会議期間の前々日までに代理認証システムを操作して，アカウントのリストを得る．必要に応じてテスト用のアカウントを別途生成し，会場または最寄りの eduroam 参加機関で動作確認を行う．
- 提供条件，使用方法ガイド，アカウント情報を記したアカウント通知を利用者へ渡す．
- 不正利用などにおける責任の明確化のために，アカウントを渡す参加登録者について，妥当な身元把握をすること．例えば，事前に有料参加登録した者については，参加登録をもって身元情報として，一律に配布することができる．当日に参加登録する者や無料 (および少額参加費) の会議では，身元確認をしてアカウントを渡すこと．

- 会議主催者が利用者から設定と利用の方法の問い合わせに対応する (会場の基地局運用者に負担をかけない) こと.
- 利用者対し，サービス提供条件を知らせて，順守させること.
- アカウント有効期間中および以後半年間は，利用者の特定を求める照会に回答すること.

当サービスの利用者に対しては，アカウントの利用に際し，以下の提供条件への同意を求めている.

- 会議主催者が参加登録者へ，個人を特定して無償で割り当てるアカウントであること.
- 有効期間中だけ有効であること．有効期間終了後はすみやかにこのアカウントの設定を削除すること (端末の無線 LAN プロファイル “eduroam” を削除).
- 会場内での利用のために提供されていること．国内の会場外の eduroam 基地局でも使えるかもしれないが，保証されないこと．日本国外の eduroam 基地局で使用しないこと.
- 電気通信法規，会場のネットワーク運用規則を順守し，学術研究活動目的で利用すること．(商用利用や，著作権を侵害するコンテンツの送受信は，禁止)
- 利用に障害が生じても無保証・現状提供であること．(利用者から設定と利用の方法の問い合わせは，会議主催者で対応する)
- 会場管理者や eduroam サービス提供者が会議主催者に対し，運用上の理由で利用者の個人情報を求め得ること.
- 以上の提供条件を記したフォームを受け取り，同意・承諾したうえで，利用すること.

これまでの運用で，会議主催者が学会のような組織ではなく，実行委員会という一時的な組織である例も多いことが判っており，提供条件緩和の声も聞かれる．現在，試行期間として様子を見ながら，提供条件等について検討を続けている段階である.

国外で開催される会議については，現時点で有効なゲストアカウント配布の仕組みはない．会議用ゲストアカウントは国内独自の運用であり，eduroam の責任分界の観点でも，会議開催地で発行するのが妥当と考えられる．早期に eduroam が行き渡った欧州をはじめ，世界のほとんどの国々では，集中型アカウントサービスを持っていない．このため，ゲストアカウントを発行する仕組みをどのようにするかについて，TERENA(eduroam の開発元) の関係者などで議論が行われている段階である.

4　代理認証システムの拡張

4.1　eduroam オンラインサインアップシステム

eduroam JP では,「代理認証システム」と「仮名アカウント発行システム」の二種類の集中型アカウントサービスを提供している．後者は学認 [2] と連携しており，利用者が学認のアカウントを使ってシステムにログインし，eduroam のアカウントを取得できる仕組みである．前者の「代理認証システム」は，機関内の認証システムや学認との連携がなくても eduroam アカウントが利用できることを目標としている．2014 年 10 月現在，eduroam に参加している国内 86 機関のうち約 1/3 にあたる 29 機関が代理認証システムをメインまたは補助的な eduroam IdP (ID Provider) として利用しており，そのうち約 55%が学認に未参加である.

従来の代理認証システムでは，機関管理者がアカウントを希望数だけ発行要求し，ID とパスワードの一覧を CSV 形式などでダウンロードしてから，利用者に配布する必要があった．この方式は，小規模の大学では運用可能な範囲と考えられるが，利用者にアカウントを直接配布する手段が実現できれば，管理者の負担が減り，大人数を擁する大学でも当システムを採用しやすくなるものと考えられる.

ほとんどの機関の学生や教職員は，機関発行のメールアドレスを持っている．我々はこの点に着目し，メールアドレスを間接的に個人認証に利用するオンラインサインアップ機能を開発，付加した [3].

eduroam の利用を希望する者 (以下，利用者) は，eduroam 以外のいずれかのネットワークに接続された端末からサインアップのためのウェブサイトにアクセスし，メールアドレスや本名，メールの到達性を確認するための一時的なパスワードを入力する．メールアドレスは，機関管理者が予め設定したドメイン名 (例えば “< 大学名 >.ac.jp”) に末尾が一致するものだけが利用できる．このように所属機関で発行されたメールアドレスに限定することで，部外者からの不正な申請を抑制している．利用者が申請ボタンをクリックすると，入力されたメールアドレスに対して，本人確認のためのメールが自動的に送られる．この様子を図 1 に示した．メールに記載のリンクをウェブブラウザで開き，先に入力したパスワードを入力することで本人確認が完了し，申請内容が機関管理者に通知される．このとき，どの機関の管理者に通知メールが送られるかは，登録されたドメイン名 (部分) によってシステムが自動的に判断する．利用者はこの時点で ID・パスワードを得るが，機関管理者によってロックが解除されるまでは，実際に使うことはできない.

通知メールを受信した機関管理者は，管理用のウェブサイトにログインして申請内容を調べ，アカ

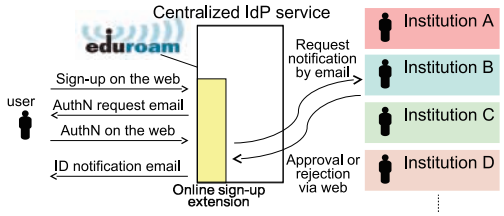

図 1: eduroam オンラインサインアップシステム

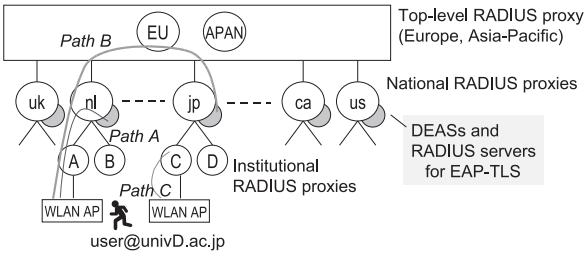

図 2: 耐障害・耐災害 eduroam のアーキテクチャ

ウントの有効期間を設定して承認するか，理由を記入して拒否の操作を行う．この承認結果は，申請者のメールアドレスに送付される．

4.2 クライアント証明書発行システム

eduroam は IEEE802.1X に基づく認証方式を採用しており，PEAP や EAP-TTLS，EAP-TLS などの様々な方式が利用できる．このうち PEAP は，Windows を始め，MacOS，Android，iOS，Linux など幅広いオペレーティングシステム (OS) が対応しており，eduroam では世界的に主流となっている．代理認証システムでも PEAP を採用している．

PEAP では ID・パスワードのペアがアカウントとして利用されるが，運用方法や利用場面によっては，電子証明書を用いる EAP-TLS 方式が適している場合がある．我々が開発している耐障害・耐災害 eduroam のアーキテクチャ[1] では，EAP-TLS 方式によって耐障害性と効率的な認証処理を実現している．例えば，図 2 において，日本 (jp) の代理認証システムの CA 証明書を機関 C が事前に取得しておけば，端末の認証を *Path C* の経路のみで効率的に行うことができる．将来的にこのようなシステムを実現する準備に加えて，現在の eduroam の構成のままで EAP-TLS 方式を利用したいという機関もあることから，これをサポートするための「クライアント証明書発行システム」を代理認証システムに追加した [3]．

クライアント認証のための電子証明書はデータが大きく，パスワードのような手入力は事実上困難である．そのため，利用者自身が証明書を端末にダウンロードできる手段を提供する必要がある．開発したクライアント証明書発行システムでは，eduroam アカウントとして PEAP 用に発行された ID・パスワードのペアをシステムの利用者認証に流用した．

利用者は，eduroam アカウントからレルム部分を除いた ID を用いて，同システムのウェブサイトにログインする．端末に証明書をインストールするのに必要なパスフレーズを入力し，証明書発行のボタンをクリックする．システム内部で PKCS#12 形式の証明書ファイルが生成され，ダウンロードのためのリンクがウェブ画面に表示される．利用者はこの証明書ファイルを端末にダウンロードし，先に入力したパスフレーズを用いてインストールする．

クライアント証明書がインストールできることは，Windows, OS X, iOS で確認した．Android については，ベンダやバージョンによるばらつきが大きく，導入を簡略化するツールの開発が望まれる．

このクライアント証明書発行システムは，機関管理者がその利用可否を選択できる．初期状態では利用不可に設定されており，利用者は証明書を取得できない．また，万一の悪用に備えて，機関管理者は証明書失効権限を有しており，不正利用が発覚した場合は当該証明書を CRL(Certificate Revocation List) に加え，また，再発行の操作を禁止できる．

5 むすび

eduroam の国内外の最新状況を概説した．国内ではキャンパス無線 LAN の更新時に eduroam を導入する例が多く見られるようになっている．

国内で開催される会議等のために，会議向け機関限定 eduroam アカウントの試行を開始した．eduroam 基地局の整備された大学施設・会議場であれば，会議主催者が主体となってゲストアカウントを発行し，利用者の便宜を図ることができる．

また，代理認証システムの拡張として，「eduroam オンラインサインアップシステム」と「クライアント証明書発行システム」を開発した．国内機関の eduroam 参加の加速と，耐障害性・耐災害性を有する eduroam システムの開発に貢献が期待される．

参考文献

[1] 後藤英昭, 曽根秀昭, “キャンパス無線 eduroam の国内外の最新動向 – 利便性と耐障害・耐災害性の向上 –,” 大学 ICT 推進協議会 2013 年度年次大会 論文集 W3E-5, pp.122–125, 2013.

[2] 西村 健, 中村素典, 山地一禎, 大谷 誠, 岡部寿男, 曽根原 登, “日本における学術認証フェデレーション “学認” の展開,” 大学 ICT 推進協議会 2011 年度年次大会 論文集, 2011.

[3] T. Niizuma and H. Goto, “Centralized Online Sign-up and Client Certificate Issuing System for eduroam,” COMPSAC Workshop MidArch 2014, pp.174–179, 2014 (Västerås, Sweden).