# 「世界でつながるキャンパス無線LAN」
## ～認証連携が切り拓く、新時代の教育・研究環境～

大学には、教育や研究を支えるさまざまな情報システムがあります。その中のキャンパス無線LAN（ラン）について、特色や課題、先端の環境、そしてインフラ開発の様子を、ちょっと覗いてみましょう。

### デジタルキャンパスへの入口「キャンパス無線LAN」

高等教育と最先端の研究を支える大学の情報システムは、近年大幅に進化しています。学生は大学のウェブサイトで授業概要を確認し、履修登録を行い、講義資料を取り寄せ、教務電子掲示板を閲覧し、自宅からインターネット経由でレポートを提出するといったことを、日常的に行っています。調べ物にもネットが便利な時代です。2000年頃はまだ冊子体が多かった論文誌（ジャーナル）は、現在では電子ジャーナルが一般的です。会議資料も電子ファイルで配られます。今や大学キャンパスの機能の多くがネット上にあり、「デジタルキャンパス」とみなすことができます。学生や教職員のノートパソコン（PC）やスマートフォン、タブレットなどの携帯情報機器（以下、端末と呼ぶ）を大学のネットワークに接続したいという要望が出てくるのは当然でしょう。デジタルキャンパスへの入口が必要で、その一つが「キャンパス無線LAN」です。大学では講義・演習や学会などで百人規模の利用者が集まることもあり、強力な無線LANインフラが必要になります。

### 認証、暗号化、偽基地局対策で安全・安心なネット利用環境

キャンパス無線LANと家庭用無線LANの違いは何でしょうか。キャンパス無線LANのように大勢が共用するシステムでは、個人ごとの通信を暗号化する仕組みが必要です。電波を傍受（盗聴）されることは避けられないので、暗号化によって通信内容を保護します。この暗号化のために、「キー（鍵）」と呼ばれる短い秘密のデータを使います。一方、家庭では一つのキーを家族で共有する使い方が一般的です。もし大学でも同じような運用をすれば、何千人、何万人という学生のうち、誰か一人でもキーを他に漏らしてしまうと、全員の通信内容が危険に曝されます。

もう一つの重要な機能が「ユーザ認証」です。もし大学の無線LANに誰でも自由に接続できたら、何者かが学内外の情報システムに攻撃を仕掛けたとしても、犯人がわかりません。また、大学が個別に契約している電子ジャーナルを学外者が閲覧することは、問題になるのが一般的です。このようなことを避けるため、正規の利用者であることを確認した上で、無線LANの利用を許可する仕組みが必要です。

偽の基地局への対策も欠かせません。悪意を持った人が、他人のID・パスワードなどを不正入手する目的で、本物の基地局を模した偽物を設置する恐れがあります。偽基地局に誤って接続しないようにする仕組みが必要です。

安全・安心な無線LANシステムを作るためには、ユーザ認証、通信の暗号化、偽基地局対策がすべて揃う必要があります。

### 認証連携で世界中をキャンパスに

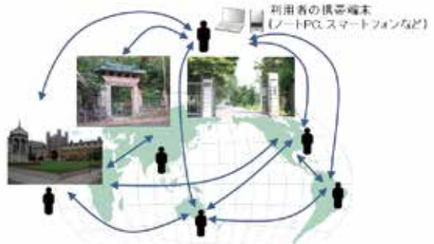
大学では、教員が非常勤講師として他大学の授業に通ったり、学会活動や共同研究などで他機関を頻繁に訪問したりすることがあります。近年では単位互換制度による学生の交流も盛んになりつつあります。欧州の大学では、他大学でのインターンシップ研修が義務づけられているケースもあります。このような環境で、訪問先ごとにIDを発行してもらうのは、利用者にも管理者にも多大な手間がかかります。世界中の大学で無線LANを相互利用できたら――それを実現したのが2003年に欧州で開発された「eduroam（エデュローム）」で、現在約60か国が参加する世界標準になっています。eduroamは、先に述べたユーザ認証、通信の暗号化、偽基地局対策のすべてを備えています。日本では、東北大学が2006年に国内初の参加機関となり、2013年12月時点で57機関が参加しています。

eduroamは「認証連携」という仕組みを無線LANに導入したものです。認証連携とは、異なる機関やサービスの間で、IDやその属性（IDに付随する情報）を関連付け、利用できるようにするための技術で、既に多くのサービスに導入されています。例えばツイッターやGoogleなどのIDを利用して写真共有などの外部サービスを利用できるのは、認証連携の例です。

例として、東北大学の学生であるXさんが外国のA大学を訪問して無線LANを利用するというシナリオを考えます。Xさんは、無線LANを利用するためのID（アカウントと呼ばれることがある）を自分の大学で取得しておきます。認証に必要なパスワードなどの情報も併せて、所属大学の認証サーバ（認証機能を提供するコンピュータ）にアカウントが保存されます。

Xさんが無線LANを使おうとしても、最初は基地局が通信を阻止しており、ネットワークに接続できません。標準的なeduroamの構成では、階層的な構造をした認証用のネットワークを介して認証情報が送られます。基地局はXさんの端末から送られてきたIDをA大学の認証サーバに送ります。IDに含まれるレルム名（所属を表す住所のようなもの）より学外の利用者だとわかるので、認証要求は国の代表のサーバに送られます。レルム名の末尾を見ると国外の利用者だとわかるので、認証要求は世界のトップレベルのサーバに転送されます。レルム名の末尾が日本（jp）なので、認証要求は日本のサーバに送られ、最終的には東北大学の認証サーバに届けられます。認証の結果、正しい利用者と判れば「受理」のメッセージが返送され、基地局が通信を許可します。

eduroamは、大学キャンパスの外にも広がってきています。日本では、通信事業者との協同により、東京中心部の貸会議室やカフェなどでもeduroamが利用できます。スウェーデンでは空港・駅などでeduroamが使えますし、ルクセンブルクでは市街地でも利用できます。世界のさまざまな場所にキャンパスが拡大していると見ることができ、今後の教育・研究のスタイルにも、大きな影響を与える可能性があります。



世界中の大学でキャンパス無線LANを相互利用
（キャンパス無線LANローミング）

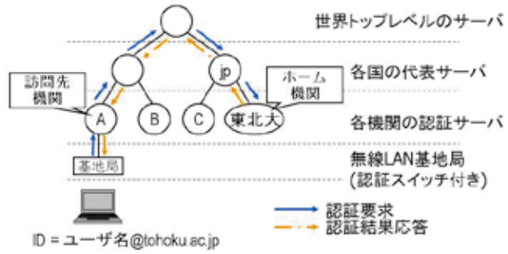
日本における国際学術無線LANローミング基盤eduroam

### 災害に強い無線LANインフラの実現に向けて

日本には1200以上の高等教育機関があります。大規模なeduroamシステムを低い導入コストで構築し、各機関および事務局の運用の手間を削減しつつ、安定に運用するための技術の開発が、課題となっています。私たちが開発した「代理認証システム」は、各大学の認証サーバの機能を国の中央のサーバで代行することで、個々の大学のサーバを不要とするものです。各大学では管理用のログインIDを取得するだけでeduroamが利用開始できるようになり、これによって参加の敷居が大幅に下がりました。

2011年の東日本大震災では、予期せずeduroamが災害時にも有効なことが明らかになりました。他大学を訪問中の人や、来日していた外国人が、大地震の直後にeduroamを利用していました。電話網が混雑して使えない状況でも、大学の無線LANが連携していたお陰で、連絡手段が一つ手元に残っていたのです。

大規模災害時には、連絡手段の確保が重要です。現在、部分的なネットワークの障害や、大人数の同時利用にも耐えられるような、災害に強い無線LANインフラの実現をめざして、さまざまな大学と企業、政府が連携して、研究開発が進められています。



eduroamの認証連携のしくみ（標準構成）

**後藤 英昭**（ごとう ひであき）
1967年生まれ
現職／東北大学サイバーサイエンスセンター
准教授
専門／ネットワークセキュリティパターン認識、
画像認識
関連ホームページ／http://www.imglab.org/