サイエンティフィック・システム研究会
システム技術分科会 2008 年度第 2 回会合資料

2009 年 1 月 29 日

キャンパス無線 LAN における認証連携と国際ローミング基盤 eduroam

東北大学サイバーサイエンスセンター・准教授
後藤 英昭

[Abstract]

大学等のキャンパス無線 LAN には、認証の信頼性や運用面に関して、商用の公衆無線 LAN とは異なった問題が多数存在する。近年、授業・会議等における教職員・学生の大学間の移動に対応するために、キャンパス無線 LAN の相互利用環境が求められている。欧州で開発された eduroam は世界規模で利用されているローミングシステムであり、日本でも 2006 年に加盟した。現行の eduroam には幾つかの問題が指摘されており、ゲストネットワークの分離や利用者のロケーションプライバシーの問題などが最近の関心事である。

本講演では、キャンパス無線 LAN に特有の問題を紹介し、大規模ネットワークにおいて完全には信頼できない相手とローミングを実現する場合の問題点と対策例、およびネットワーク構成に対する要求を概説する。また、学内の部局が草の根的に無線 LAN システムを構築しながらも、安全で使いやすい無線 LAN ローミングを学内で実現できる、東北大学のユニークな取り組みを紹介する。

[Keyword]

キャンパス無線 LAN ローミング、eduroam (エデュローム)、認証連携、ロケーションプライバシー、VPN ローミング方式

1 はじめに

近年、授業や会議等において、教職員・学生の携帯端末を学内ネットワークに接続したいという要求が高まっており、キャンパスに無線 LAN システムを導入する事例も多い。従来は、機関ごとに構築され、基本的に機関内の者だけが利用できるシステムが多かった。しかし、近年では、教職員・学生の大学間の移動にも対応できるシステムが求められている。

認証連携技術を用いたネットワークローミングは、無線 LAN の相互利用にも有用であるが、現行のシステムにはまだセキュリティ上の問題が幾つか残っている。また、ユーザ認証や通信の効率化の点でも、更なる改善が必要である。

一方、大学等の教育研究機関における無線 LAN システムには、利用と管理の両面において、商用の公衆無線 LAN サービスとは異なった要求や条件が数多く存在する。このため、単純に商用サービスを導入するだけでは対応できない課題があり、教育研究機関での利用に適したネットワーク構成や認証システムを開発していく必要がある。

本講演では、上述の内容について概説するとともに、東北大学で行われている無線 LAN システムのユニークな構成方法について事例を紹介する。

2 キャンパス無線 LAN

国内・国際会議や研究会、各種集会において、教職員や研究者、学生のネットワーク利用が求められることが多く、キャンパスに有線のポートや無線 LAN を設置することが望まれている。大学等では、講師がプレゼンテーション用の PC を学内 LAN に接続したり、学生が持ち込みの PC を使って演習や自習を行ったりするなどの利用形態があり、ネットワーク管理の立場からは、このような新しい授業方法を支援していく必要がある。単位互換制度による大学間の学生の移動にも、対応が望まれている。教員や学生が国際会議などで渡航した際は、現地でインターネットに接続するのが難しいことが多い。もし現地の教育研究機関で自由にネットワーク接続が可能ならば、非常に便利である。

キャンパス無線 LAN には、商用の公衆無線 LAN サービスとは異なる要求が多々存在する（スライド 5, 6)。演習等で学生に PC を使わせようとすれば、受講者全員が無線 LAN を利用できる必要がある。システムの利

便性については、商用サービスのそれをはるかに越える、徹底的な対策が必要である。例えば、SSID のビーコンが出ていない(ステルス)環境では、多くの学生は SSID の手動登録でさえつまずくものである。また、教育機関では、何らかのインシデントが発生した場合に「教育的指導」が非常に重要である。

高い利便性を有し、十分なセキュリティを確保しつつ、数万人規模の利用者のサポートが可能で、かつ、管理やユーザサポートの手間がかからないシステムが望まれている。

3 大学間無線 LAN ローミング

3.1 国際無線 LAN ローミング基盤 eduroam

無線 LAN ローミングとは、「認証連携技術により、利用者が所属機関のアカウントを使って他機関の無線 LAN インフラを利用できる仕組み」である。国内では、国立情報学研究所(NII)と 7 大学、それに東京工業大学と高エネルギー加速器研究機構を加えた 10 機関が行っている「大学間連携のための全国共同電子認証基盤(UPKI)構築事業」の中で、大学間の無線 LAN ローミングを実現しようとするプロジェクトが走っている（スライド 9)。UPKI 構築事業は、最先端学術情報基盤(Cyber Science Infrastructure, CSI)の実現のうち、特に電子認証基盤に関わる研究開発や実証実験などを行う事業である。

UPKI 構築事業では、独自のローミング方式を一から開発することも検討されていた。しかし、既にヨーロッパ方面で広く利用されている eduroam というローミング基盤があり、国内のみならず国際的にも無線 LAN ローミングで連携できることが望ましいことから、まずは eduroam を国内導入するところから始めることになった。2006 年にアジア太平洋地域の eduroam コミュニティと調整を行い、日本地区のトップレベルのサーバを東北大学に設置して、東北大学が初めて eduroam に加盟した。また、同年中に NII を含む 4 機関が加盟して、国内でも無線 LAN ローミング基盤が立ち上がった。日本の eduroam は、eduroam JP と呼ばれている。

2009 年 1 月現在の eduroam JP は、NII による正式サービスであり、NII と東北大学が管理実務を担当している。eduroam JP では、国内の高等教育機関等に参加を呼び掛けており、現時点で 10 機関が接続している（スライド 12)。

3.2 IP アドレスのゲスト利用の問題

eduroam に限らず、無線 LAN や有線ポートの機関間ローミングでは、ゲストに訪問機関の IP アドレスを貸し出して、機関の内外のサービスを利用させる形態(オープンアクセス)が一般的である（スライド 15)。このような利用形態は、プロバイダが提供する商用サービスとしての無線 LAN ローミングではあまり問題を生じないが、大学等ではセキュリティ上の大きな問題を生じることがある。

一般に個々の大学では、出版社と契約して、多数の電子ジャーナルを購読している。電子ジャーナルの閲覧にあたっては、教員や学生の個人を認証できることが望ましい。しかしながら、まだ大多数の大学では電子認証基盤が整備されていないため、大学の IP アドレスを利用してユーザ認証の代用としているのが一般的である[1]。ゲストが訪問機関の IP アドレスを利用できると、電子ジャーナルの閲覧が可能となり、これは契約違反とみなせる。

大学内にある、学内利用に限定されたサービスでも、IP アドレス範囲によるアクセス制限が用いられていることが多い。訪問機関の IP アドレスを自由に利用させることは、学内リソースの保護の観点でも、セキュリティ上の問題がある。

ゲストが故意に、あるいはコンピュータウィルスの感染などによって無意識のうちに、学外のサーバやネットワークに攻撃を仕掛けてしまうこともある。学外から見ると、攻撃元は訪問先機関になるので、苦情等は訪問先機関に寄せられることになる。もし重大なインシデントが発生すれば、ゲスト利用者の些細な不注意によって、訪問先機関全体が処罰される危険性もある。

3.2.1 解決策 1

電子ジャーナルと契約しておらず、学内ともみなさない IP アドレス範囲に、ゲスト専用のネットワークを構築することによって、上述の問題の一部を解決することは可能である（スライド 16)。このようなネットワーク構成では、電子ジャーナルや内部リソースへのアクセスを遮断することができる。しかしなが

---

1 いくつかの出版社や大学では、Shibboleth/SAML を用いてシングルサインオン(SSO)によるユーザ認証の仕組みが整備されてきている。

ら、利用者が自分の所属するホーム機関で無線 LAN を利用しているのに学内サービスを自由に利用できない、といった問題が新たに生じる。認証 VLAN などを用いてこの問題は技術的に解決可能であるが、ネットワーク構成が複雑になるという欠点がある。また、専用ネットワークの契約者が自機関である以上、ゲストの学外への不正アクセスに関しては対策にならない。

大学の入り口に VPN サーバを設置すれば、他機関の無線 LAN を利用している場合でも、学内リソースや所属機関が購読している電子ジャーナルへのアクセスが可能となり、サービスの利便性を向上させることができる（スライド 16)。

3.2.2 解決策 2

eduroam に参加している機関の中には、eduroam の無線 LAN アクセスポイントからの通信を主要な VPN プロトコルに限定している所がある。端末からの通信を VPN に限定することにより、利用者が eduroam の IEEE802.1X によるユーザ認証を通っただけではネットワーク上の様々なサービスを直接に利用することはできなくなる。利用者は、所属機関などの VPN サーバに接続することによって、ネットワーク上の様々なサービスが利用可能になる。このような運用ポリシーは、「VPN-only ポリシー」と呼ばれている(スライド 18)。

VPN-only の場合は、学外から見るとアクセス元が常に利用者の所属機関(アカウントのある機関)になるので、インシデント発生時の対応が容易になる。また、所属機関の内部リソースの利用も自然に行える。

VPN-only の場合、解決策 1 のように無線 LAN 専用のサブネットを用意する必要はなく、ネットワーク構成は単純になる。しかし、アクセスポイントからの通信を VPN に限定するためのファイアウォールやパケットフィルタが必要になる。

一方で、この方式の欠点の一つとして、二重のログイン操作が必要になることが挙げられる。eduroam の 1X 認証に加えて、VPN 接続のためのユーザ認証が必要であり、接続の操作が煩雑になる。端末に VPN クライアントソフトウェアが必要な点や、VPN 接続の効率や安定性の問題も残されている。

東北大学の我々の研究グループでは、利用者に VPN の利用を意識させず、eduroam のユーザ認証の手続きだけで自動的に端末が所属機関に仮想的に属し、さらに訪問先のローカルリソース(例えば会議室のプリンタやファイルサーバ)にも効率的なアクセスを実現できるようなネットワーク制御技術を開発中である。

3.3 ロケーションプライバシーと Pseudonymous ID

eduroam では、世界規模で構築された階層的な RADIUS プロキシサーバを介してアカウント情報をリレーすることによって、認証連携を実現している。そのため、経路上のプロキシサーバのログに残されたアカウント情報を見れば、「どこの、誰が、どのあたりで」無線 LAN を利用したのかを知ったり、推測できることがある。利用者の識別や行動調査も可能になることから、「ロケーションプライバシー」の侵害の危険性があることが、最近認知され始めた。

1X 認証の Outer Identity の仕組みを用いることで、プロキシサーバ上のログに匿名 ID を残すことが可能である。しかし、すべてのサプリカント(端末側のソフトウェア)が Outer Identity をサポートしているわけではなく、サポートされていても、利用者が明示的に設定しなければならない。

通常、1X 認証では EAP によるトンネルを通してユーザ認証が行われるため、プロキシサーバ上のログにパスワードが記録されることはない。しかしながら、サプリカントの設定を誤ると、パスワードが平文でネットワークを流れ、ログに記録されることがある。万一、プロキシサーバのログが流出した場合は、重大な情報漏洩問題となる。利用者の不注意であっても、パスワードが漏洩しやすいシステムは安全であるとは言えない。プロキシサーバの管理者が互いに「完全には信頼できない」ならば、プロキシサーバのログにクリティカルな情報が残らないように、何らかの対策が必要である。

eduroam に限らず、ローミングにおいて有用と考えられている技術の一つに、Pseudonymous ID の利用が挙げられる。完全に匿名な Anonymous ID と違い、Pseudonymous ID は準匿名の扱いとなる。通常の利用においては、利用者は匿名でいられる。何らかのインシデントが発生した場合に、認証連携の境界で管理者が協力することによって、利用者追跡を可能にしようとするものである。

4 キャンパス無線 LAN の構成方法

キャンパス無線 LAN を整備する方法として、大きく二種類が考えられる。一つは、情報基盤センターに相当するセンターが中心となって全学にアクセスポイントを設置し、一元管理する方法である。もう一方

は、学内部局が個別に無線LANシステムを構築する方法である。どちらにも得失があり、一概にどちらが良いとも言えないだろう。大規模な大学では、前者は予算や管理の面で実現が難しいことがある。一方、後者の場合、部局が独自のシステムを導入したのでは部外者の利用が不便になるので、学内でローミングを実現できるようなシステムを導入するのが望ましい。

近年では、複数のSSIDを同時利用できるアクセスポイントが普及してきているので、部局独自の方式と学内ローミング、eduroamなどの複数方式を同時サポートするシステムの構築はそれほど難しくはない。ただし、マルチSSID機能への対応が不十分な製品がまだ多いため、アクセスポイントの選定にあたっては十分な検討が必要である。

5 東北大学の無線LANシステム

5.1 ボトムアップなシステム構築

東北大学では、全学的な無線LANシステムの整備はこれまでに行われていない。学内の各部局が独自に無線LANシステムを導入してきた。しかし、部局独自の方式が乱立しては、学内での無線LAN相互利用が困難になる。そこで、2004年より学内ローミングに関する検討を始め、設置の主体は部局や研究室のままで、学内ネットワークTAINS(テインズ)上で無線LAN相互利用を実現するための方式として「どこでもTAINS」方式を開発した。

東北大学では、サイバーサイエンスセンター(旧・情報シナジーセンター)が「どこでもTAINS」の共通仕様を広報誌等で提示し、賛同する部局がこれに対応した無線LANシステムを構築するという、ボトムアップ的なアプローチをとった。これにより、全学で巨大な経費を獲得しなくても、スモールスタートによって無線LANの整備が可能となった。また、部局によっては、館内ネットワークの一部として、無線LANシステムを望みの形で自由に整備することができるようになった。

5.2 「どこでもTAINS」方式

「どこでもTAINS」方式は、VPNを利用した学内ローミングシステムである（スライド29)。その大きな特長として「草の根的なシステム構築」が挙げられる。アクセスポイントとしては、エンタープライズ向けの製品はもちろん、家庭用の無線ブロードバンドルータも利用できる。学内LANに機材を接続できる権限のある人ならば、誰でも、アクセスポイントを随時、自由に設置できる。部局が建物の設備としてアクセスポイントを一括して設置するのに加えて、研究室という単位でも設置が可能である。

「どこでもTAINS」対応のアクセスポイントを利用するためには、VPNサーバを経由する必要がある。アクセスポイントと同様に、学内LANに機材を接続できる権限のある人ならば、VPNサーバを自由に設置できる。すなわち、部局でVPNサーバを設置してアカウント管理をしても良いし、研究室に自分専用のVPNサーバを置いても良い。

アクセスポイントもVPNサーバも、設置する際にセンターへの届け出は不要である。センターは共通仕様を提示するだけで、学内のどこにアクセスポイントやVPNサーバがあるのかをすべて把握しているわけではない。

「どこでもTAINS」の仕組みをスライド30に示す。各アクセスポイントでは、学内向けのVPNパケットのみを通過させるようなフィルタリングが行われる。宛先を学内に限定しているのは、部外者によって学外のVPNサーバを介してアクセスポイントを使われないようにするためである。TAINSのルールによって、学内LANにはユーザ認証のないVPNサーバ(踏み台サーバ)などは接続できない。すなわち、部外者の利用を排除できる。

外部への通信はこのVPNサーバを介して行われるので、何らかのインシデントが発生した場合は、VPNサーバの所在から、利用者や設置者を絞り込むことが可能となる。この性質は、責任の所在を明確にする上で有用である。

「どこでもTAINS」の大きな特長の一つに、その利便性が挙げられる。利用者は、適切なSSIDを選択して端末をアクセスポイントに接続した後、VPN接続の操作を行うだけで、ネットワーク利用が可能となる。Windowsに付属のPPTPクライアントでは、アカウント情報とサーバを登録しておけば、通常の利用においてはマウスボタンのわずか3クリック程度でVPN接続が完了する。

一方、eduroamなどの1X認証では、サプリカントの設定項目が多く、初期設定のしきいが高い。また、端末の無線LANドライバ、サプリカント、アクセスポイント、RADIUSサーバの間に相性問題が根強く残っ

ており、常用する場所では容易に接続できても、別のサイトではうまくつながらないなどのトラブルに見舞われることが多い。また、前述のようにeduroamにおいてもVPNを併用する場合があり、学内利用でも二回の認証を行うのは、利便性の低下につながる。

残念ながら「どこでもTAINS」の利用は学内限定[2]であるので、国内外のローミングのためにはeduroamも必要である。現在、東北大学では、「どこでもTAINS」とeduroamの両方式を展開している。

6 まとめ

キャンパス無線LANには、商用公衆無線LANと異なる要求が多々存在する。特に、高い利便性と教育・研究のサポートが重要である。

日本では2006年から国際無線LANローミング基盤eduroamが運用されている。eduroam対応の無線LANシステムを構築するには、セキュリティに配慮したネットワークの設計が必要である。また、現行のeduroamでは、ロケーションプライバシーの問題が認識されるようになってきた。Pseudonymous IDの利用は、プライバシー保護に有用と考えられている。

東北大学で行われている無線LANシステムのユニークな構成方法について説明した。「どこでもTAINS」はVPNを利用したローミング方式であり、草の根的にアクセスポイントを設置しながらも学内ローミングを実現できる。ネットワーク接続の操作も容易である。現在、東北大学では、学内ローミングには「どこでもTAINS」、学外ローミングにはeduroam というように、二種類の方式を展開している。

参考文献

スライド35を参照。

2 スケーラブルな方式も開発中である。