国際学術無線 LAN ローミング基盤「eduroam」について

第２技術班　中 原 勝 俊

１．はじめに

eduroam （エデュローム）とは、国の内外の機関で、いつでも自由に無償で利用できる、無線 LAN のローミング基盤である。国際学術という名称からも eduroam は、ほとんどの場合で大学等の研究機関で利用されている。しかし、現在では、空港やホテルといったパブリックスペースでも利用できるようになってきており、今後利用の場はますます広がってくることが予想される。2016 年 3 月現在、国内 137 機関、世界約 75 か国(地域)で利用可能となっており、無線 LAN のデファクト・スタンダードとなってきている。佐世保高専でも昨年より eduroam が利用できるようになった。一方全国の高専では、現在本校以外に仙台高専、香川高専のまだ３校だけでしか利用できないが、平成 30 年度の高専統一ネットワークでは、全高専が eduroam に参加することが検討されている。

ここでは、eduroam の概要と、eduroam に参加するにあたり実施したネットワークの設定、およびクライアントを eduroam に接続する方法等について説明する。

図１． eduroam ロゴ

２.eduroam でできること

eduroam では、以下のようなことができる（eduroam のリーフレットより)。

■ 自機関はもちろん、国内外の訪問先機関の無線 LAN が利用できます。
- 現地スタッフの手を借りずに、無線 LAN による高速ネットワークがいつでも自由に無償で利用できます。
- 認証連携により，所属機関で発行された ID がそのまま使えます。
- 接続設定が共通なので、訪問先ごとに設定を変更する必要がありません (共通 ESSID: eduroam)。

■ ユーザ認証および通信内容の高いセキュリティが確保できます
- 802.1X 方式による安全なユーザ認証を利用しており、偽基地局の対策が可能です。
- WPA2/AES による強力な暗号通信を利用します。

■ 様々な端末が使えます
- Windows や Mac はもちろんのこと、iPhone や Android など様々な端末に対応しています。

■ 訪問者のためのネットワーク環境を毎回準備する必要がなくなります
- 学会等で訪問者が来るたびに基地局を設置・変更しなくても済みます。
- eduroam 用のネットワークを分離しておくことで，訪問者が学内システムに不正にアクセスすることを防止できます.

・SINET 接続機関は eduroam 用アドレスの割り当てが受けられます。

■ 学術認証フェデレーションとも連携できます（オプション）

・NII が運用している「学術認証フェデレーション(学認)」に参加機関は、RADIUS サーバを用意しなくとも、機関のアカウントを用いて eduroam 用アカウントの発行が可能です。

３．eduroam への参加

eduroam に参加するために以下のような点に留意した。

・インターネット接続では、既存接続と eduroam 接続を分ける

・eduroam 側から学内 LAN へのアクセスができないようにする

・SINET の eduroam アクセスネットワーク収容を利用する（専用 IP アドレスを付与）

・eduroam 仮名アカウント発行システム（学術認証フェデレーション Shibboleth 連携)を利用する

3.1 学外接続の設定

学外接続の設定では、eduroam との連携を実現するために、eduroam JP 事務局に申請し、eduroam 接続用として新規に IP アドレスを付与してもらった。その IP アドレスを利用して、すでに本校で利用している SINET 接続とは別に eduroam に接続するための新たなルートを追加した。追加したといっても新規に回線を引いたのではなく、既存の SINET 接続を VLAN 多重化接続に切り替えることで実現できる。これにより、１つの回線を論理的に 2 つに分離し、その後本校の受け側の設定に既存接続用と eduroam 接続用の２つの VLAN を構築し、学内 LAN 向けと eduroam 向けの設定を行った。

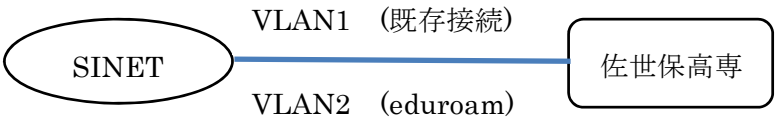

図２．学外接続の VLAN 多重化

また、eduroam に接続する際に必要となるユーザ認証には、IEEE802.1X の PEAP が利用されるので、そのためのアカウントが必要となる。今回このアカウントの発行には、学認の「eduroam 仮名アカウント発行システム」を利用することとした。そのため、eduroam JP 側の RADIUS サーバと同期をとるための RADIUS プロキシを設置して運用している。

3.2 学内接続の設定

学内の設定では、eduroam 接続のための学内用 VLAN を新たに作成し、eduroam 接続が可能な部屋（場所）までその VLAN を延ばした。その後、既存の AP に ESSID：eduroam を追加して運用したが、設定直後から通常の学内の無線 LAN 接続が非常に不安定になり、設定を元に戻さざるを得なくなった。ベンダーに相談したところ、本校の場合、既存の無線 LAN の環境に eduroam 用の設定を追加するには、認証系やその他に大幅な変更が伴い、無線 LAN 環境を再設計しなければならないということで、既存の AP に eduroam の設定を追加する方法は断念した。そこで、eduroam 専用の基地局（AP）を設置することにした。現在、大会議室、多目的室、情報処理センターに eduroam 専用の AP を設置しており、この場所で設定確認、疎通確認ができるようになっている。また、eduroam

接続のための VLAN は、学内 LAN のスイッチに収容できるため、今後 eduroam を利用したい場所の拡大にも対応できる。しかし、eduroam からの接続は、明示的に学内 LAN と切り離してルートを構成しているので、eduroam 側から学内 LAN にはアクセスできないようになっている。

４．クライアントの設定

eduroam に接続できるクライアントは、Windows、Android、MacOS、iOS とほぼすべてのクライアントが利用できる。また、その設定方法も eduroam JP の web サイトに詳しく掲載されているのでここでは割愛する。以下にクライアントを eduroam に接続するための手順を示す。

①eduroam 接続用アカウントの発行

eduroam JP のサイトから「eduroam 仮名アカウント発行システム」を利用してアカウントとパスワードを発行する。アカウントは利用者自身で発行することができるが、アカウントには有効期限が定められており、１日～１年の期限を設定するようになっている。目的に応じて各自で設定する必要がある。

②クライアントへの認証設定

仮名アカウント発行システムで発行したアカウントとパスワードを各クライアントに設定する。ユーザ認証は 802.1X 認証、認証方式は PEAP、暗号化は WPA2/AES を用いる。

③eduroam 用 AP での接続確認

クライアントの設定が完了したら、eduroam の基地局（AP）に接続できるか確認する。AP を設置している部屋は現在、大会議室、多目的室、情報処理センターなので、このいずれかで行う必要がある。なお、この設定が完了し、eduroam への接続が確認できたなら、その設定を一切変更することなく、全世界の eduroam 参加機関（場所）で無線 LAN が利用できるようになる。

４．おわりに

以上、説明したように eduroam は、組織にとっても個人にとっても大変大きなメリットがある。私自身昨年末に東京に出張した際、本校で設定した eduroam の設定を何の変更することもなく、出張先の無線 LAN が利用でき、その利便性を実感した。今後、空港などのパブリックスペースでの利用が可能となってくれば、その利便性がますます向上するのは間違いない。もちろん、現在はフリーの Wi-Fi スポットやスマートフォンのテザリングでも無線 LAN が利用できるが、eduroam の最大のメリットは、リーフレットにもあるように「ユーザ認証および通信内容の高いセキュリティ」が担保されているため、安心して利用することができ、しかも「全世界で利用できる」ということである。

なお、eduroam の詳細や基地局の設置状況、各クライアントの詳細な設定方法については、以下のサイトを参考にされたい。

参考

eduroam JP web サイト　　http://www.eduroam.jp/

TERENA eduroam web サイト　　https://www.eduroam.org/