

大学における情報セキュリティ及び電子認証に関するワークショップ  
2007年2月26日



## Eduroamによる無線LAN国際連携について

後藤英昭 東北大学情報シナジー機構

今井哲郎 東北大学情報シナジー機構

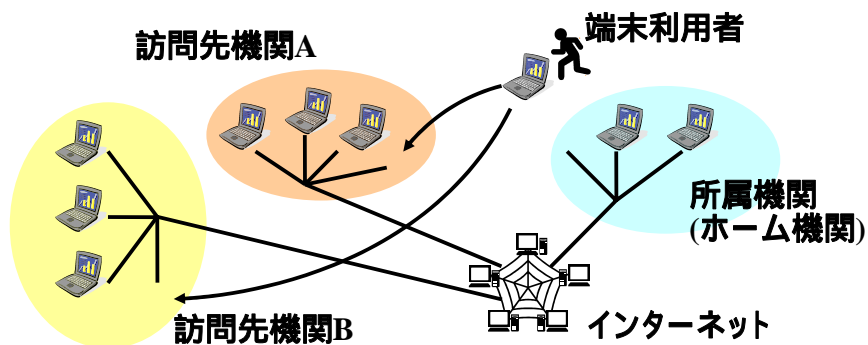
eduroam and the eduroam logo are trademarks  
or registered trademarks of TERENA.

## 発表内容

- 無線LANローミングとeduroamの紹介
- 日本へのeduroam導入
- eduroam.jpの現状
- 参加方法・利用方法
- 現行eduroamの問題と解決案
- キャンパスユビキタスネットワークの紹介

## 無線LANローミングとは

- 利用者が所属機関のアカウントだけで他機関の無線LANインフラを利用できる仕組み



## 無線LANローミングがもたらすもの

- 国内・国際会議，研究会，集会
  - 教職員、研究者、学生のネットワーク利用環境改善
  - 主催者側の準備負担軽減
- 講義など
  - 講師のネットワーク利用環境の改善
  - ネットワークを利用した新しい授業方法の推進
  - 単位互換制度による学生移動への対応
- その他
  - ブロードバンドサービスが普及していない地域におけるネットワーク利用手段の提供

# eduroamとは

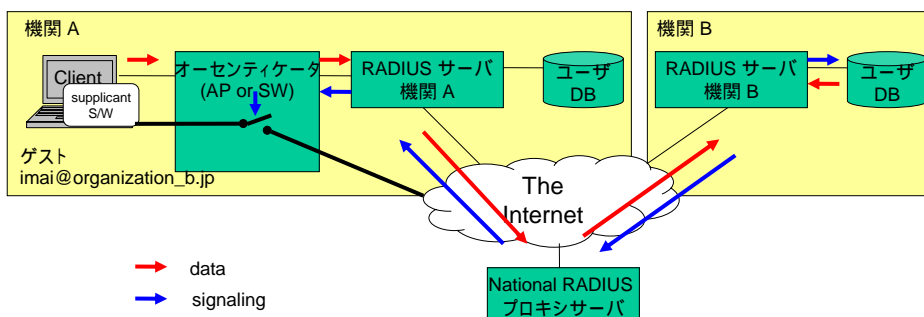


- ヨーロッパのTERENAで開発された、無線LANローミング基盤  
<http://www.eduroam.org/>
- ヨーロッパ29ヶ国の他、アジア太平洋地域ではオーストラリア、中国、台湾、香港、日本が参加  
(世界的なデファクトスタンダードに)
- RADIUSサーバの世界規模のツリーとIEEE802.1Xがベース



# eduroamの仕組み

- RADIUSツリーを介して認証情報を相互利用



## UPKI構築事業におけるeduroam

UPKI：大学間連携のための全国共同電子認証基盤

### ■UPKIにおける大学間無線LANローミング

- 目的：  
UPKIユーザが他のUPKI参加機関を訪問した際に、UPKIの仕様に基づく認証連携により、その機関が運用している無線LANインフラを利用してインターネットアクセスが可能となるような環境を構築する。
- 対象ユーザ：  
UPKI参加機関の教職員、学生、研究員等

## UPKI構築事業におけるeduroam

### ■UPKIにおける大学間無線LANローミング

- フェーズ1：  
国際的なデファクトスタンダードであるeduroamに日本も参加し、当初は6機関を接続して試験運用。他機関にも参加呼びかけ。
- フェーズ2：  
次世代ネットワークローミング方式 (仮称UPKI方式)の開発、試験運用。
- フェーズ3：  
UPKI方式の国内外展開

## 日本へのeduroam導入

- 2006年8月31日：東北大学情報シナジーセンターが先行してeduroam (Asia-Pacific) に接続
- 9月28日：eduroam.jp ウェブサイト開設
- 12月：APセカンダリサーバ(香港)と接続
- 12月：国情研, 北大, 京大, 高エネ研が接続

運用主体：

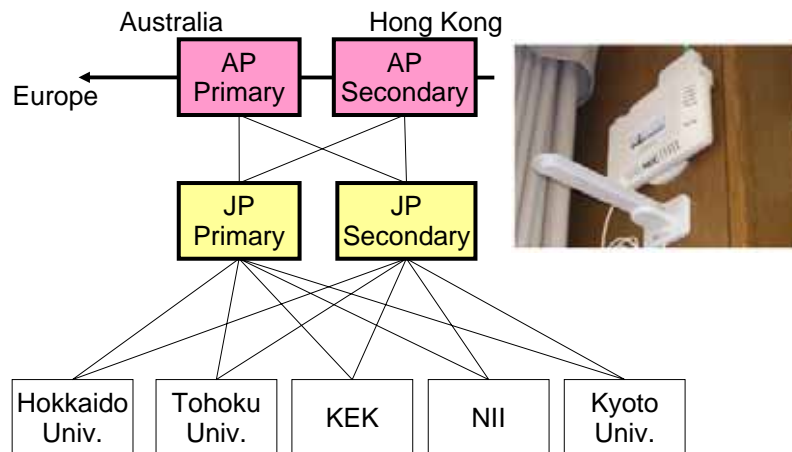
国立情報学研究所 ネットワーク運営・連携本部 認証作業部会  
eduroamグループ

## eduroam.jp参加機関 (2007年2月現在)

- 北海道大学
- 東北大学
- 国立情報学研究所
- 高エネルギー加速器研究機構
- 京都大学
- 九州大学 (準備中)

他機関も随時募集中

## eduroam.jpのネットワーク構成



## eduroam.jpポータルサイト

<http://www.eduroam.jp/>

- ニュース
- 参加機関リスト
- 参加サポート
- ソフトウェア提供



## eduroam.jpに参加するには

### ■必要な設備

- 機関トップレベルRADIUSサーバ (必須)
- 無線LANアクセスポイント (なるべく多く)
- ファイアウォール
- VPNサーバ

### ■運用体制

- 責任者, 最低二名の技術担当者

### ■申請方法

- 国立情報学研究所 ネットワーク運営・連携本部 認証作業部会 eduroamグループ に連絡 ([www.eduroam.jp](http://www.eduroam.jp)参照)

## eduroamを利用するには (エンドユーザ)

### ■所属機関のRADIUSサーバにアカウントが必要

- 所属機関・部局に申請

### ■端末にサブリカントソフトウェアを導入

- 所属機関で採用している方式(EAP-TTLS, PEAP など) のもの

- PEAPの場合、Windowsならサブリカント不要

### ■端末にVPNクライアントソフトウェアを導入

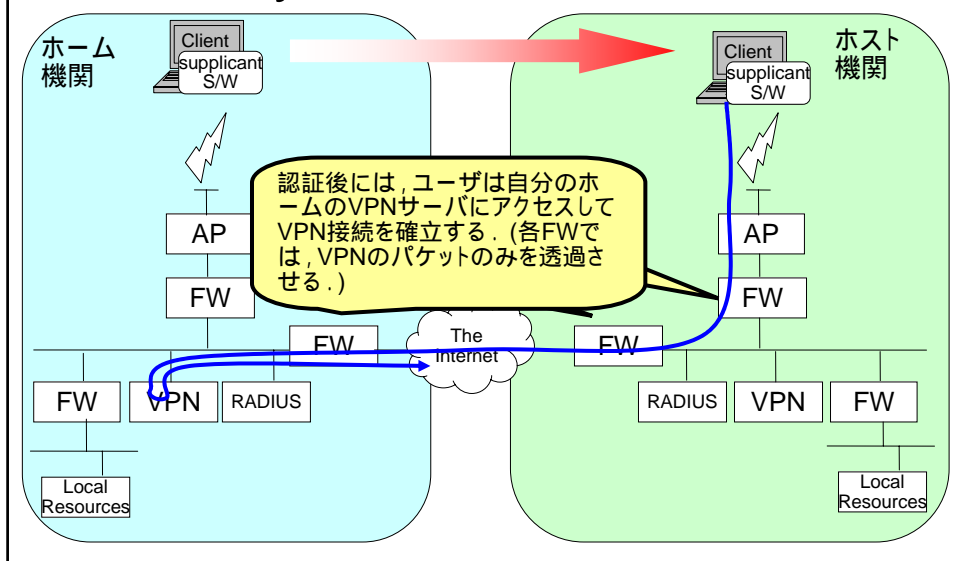
- PPTPはWindowsで標準対応

## 現行のeduroamの問題点

- 訪問先機関のアドレスをゲストに貸し出す形態が一般的
  - 故意または無意識のネットワーク不正利用における責任の所在が不明確
  - 不正利用者の追跡が困難
  - 電子ジャーナル等の利用規約違反の恐れも

解決案：VPN接続のみを許す運用  
(多くの機関で運用実績あり)

## VPN-only ポリシー

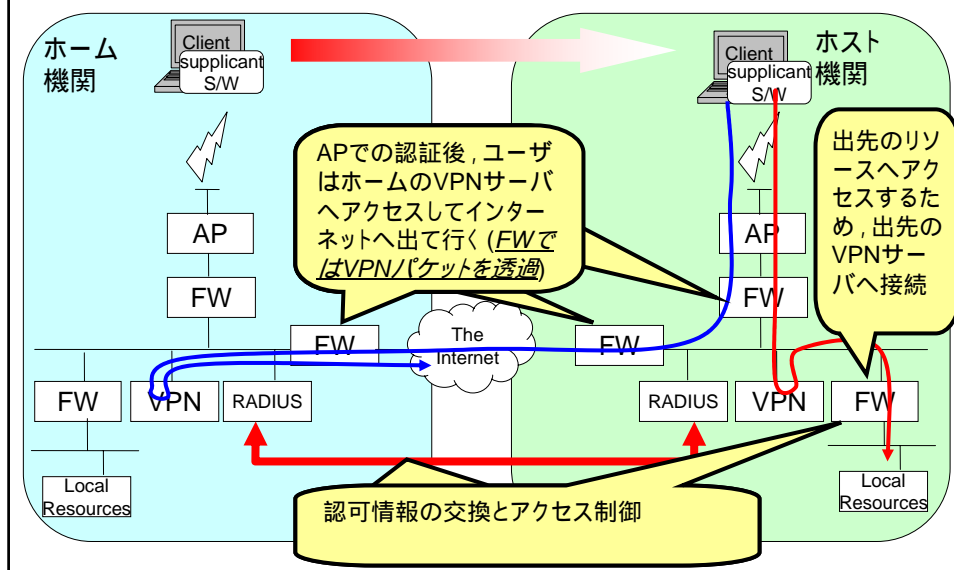




## 通過推奨プロトコル

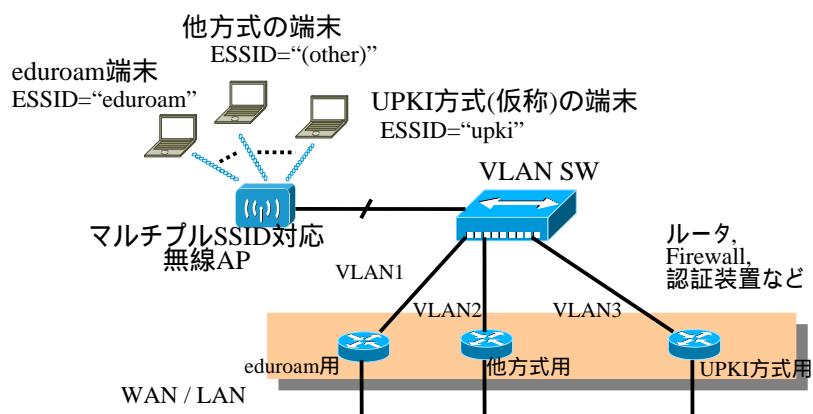
- RADIUS(UDP/1812 , UDP/1813) ,
- Standard IPsec(ESP(50) , AH(51) , IKE(UDP/500)) ,
- Cisco IPsec(TCP/10000)
- OpenVPN(UDP/1194) ,
- PPTP(GRE(47) , (TCP/1723)) ,
- pop3(TCP/110) ,
- pop3s(TCP/995) ,
- imap4(TCP/143) ,
- imaps(TCP/993) ,
- smtp(TCP/465) ,
- msa(TCP/587) ,
- SSH(tcp/22)

## キャンパスユビキタスネットワークの開発



## 複数方式の同時サービス

### ■マルチプルSSID対応の無線LAN機器を利用



## まとめ

### ■eduroamを日本に導入

- UPKI構築事業で試験運用中
- 参加機関を募集中
- VPN-onlyポリシーを推奨

### ■キャンパスユビキタスネットワークの研究開発が進行中

- 次世代eduroamとの連携も視野に