

グリッド・UPKI活用のためのCSI講演会 (古牧温泉)  
2007年10月12日



# eduroamの構築と参加方法

後藤英昭 東北大学情報シナジー機構

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

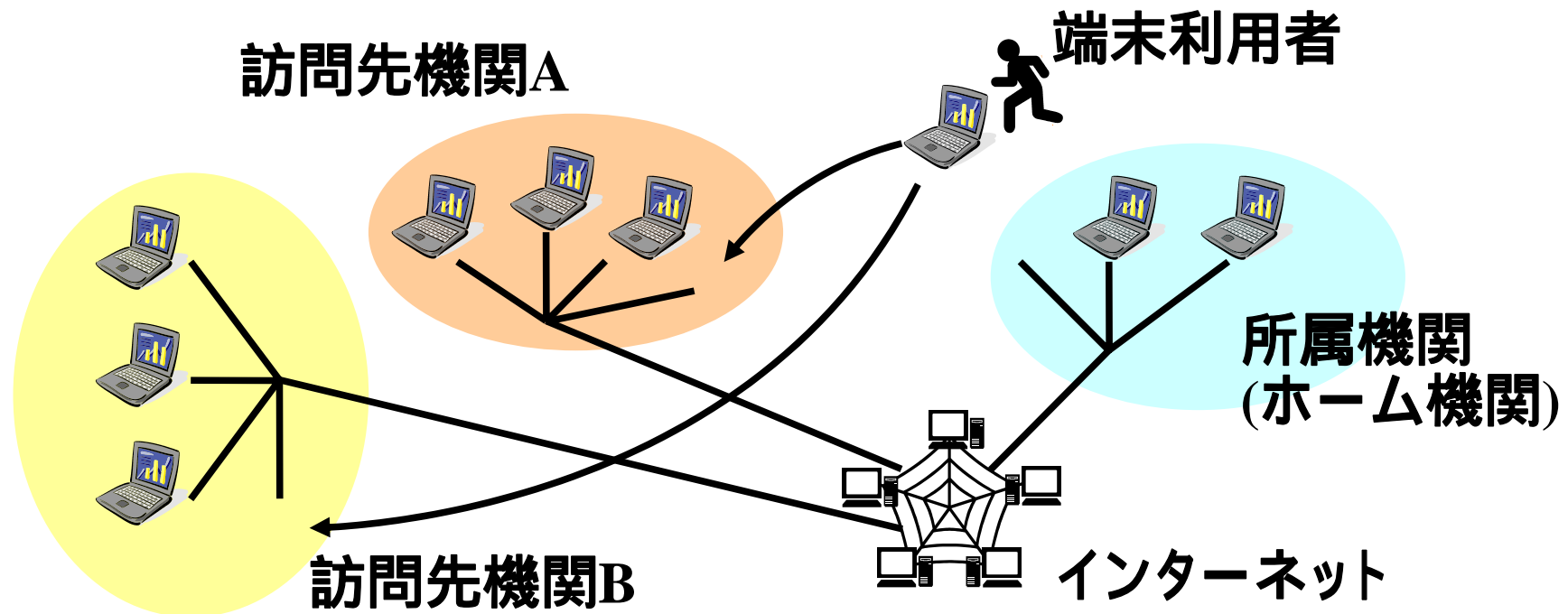


# 発表内容

- 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の問題と解決策
- 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を使って他機関の無線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



# 無線LANローミングがもたらすもの

## ■ その他

- 海外出張中など、商用ブロードバンドサービスが利用しにくい地域におけるネットワーク利用手段の確保

# エデュローム eduroamとは

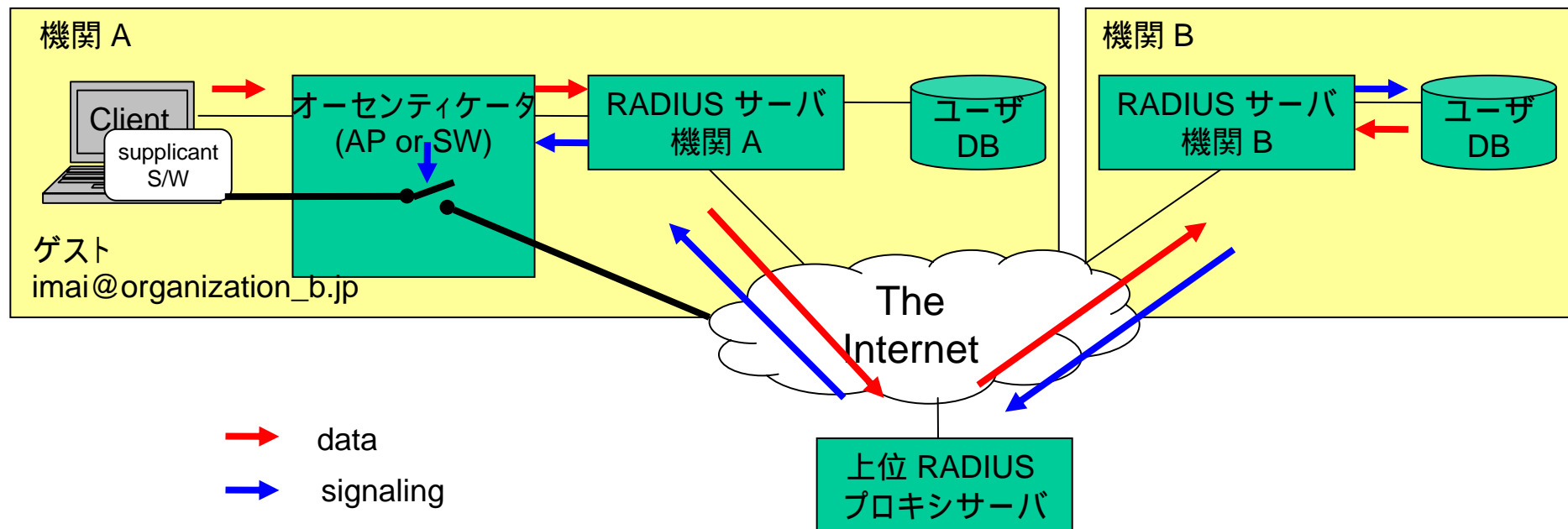



- ヨーロッパのTERENAで開発された、無線LANローミング基盤  
<http://www.eduroam.org/>
- ヨーロッパ29ヶ国の他、アジア太平洋地域ではオーストラリア、中国、台湾、香港、日本が参加  
(世界的なデファクトスタンダードに)
- RADIUSサーバの世界規模のツリーとIEEE802.1Xがベース



# 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

- 2006.8.31 : 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
- 2006.9.28 : eduroam JP ウェブサイト開設
- 2006.12 : APセカンダリサーバ(香港)と接続
- 2006.12 : 国情研, 北大, 京大, 高エネ研が接続
- 2007.6 : 九大が接続

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

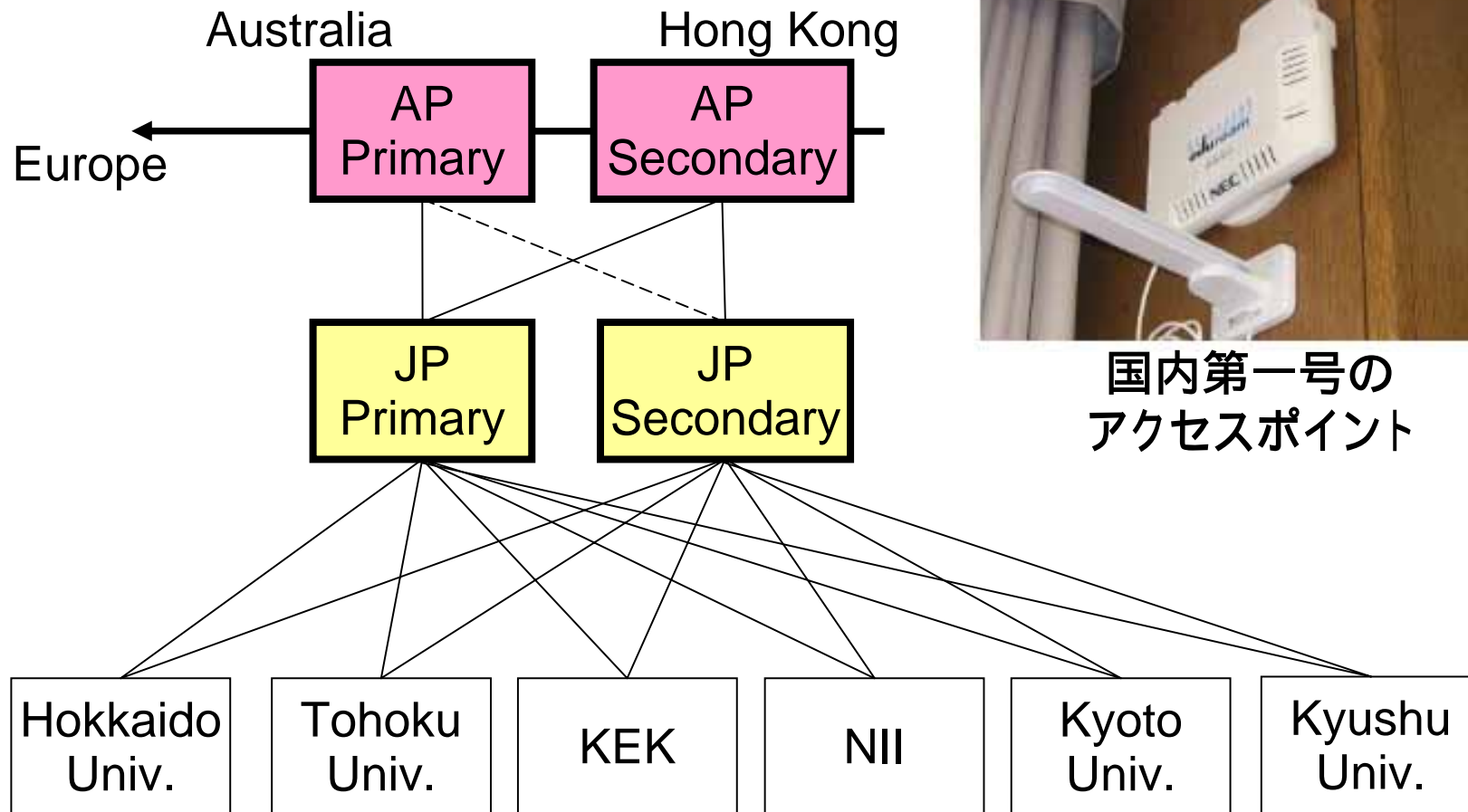


## eduroam JP参加機関 (2007年10月現在)

- 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

他機関も随時募集中

# eduroam JPのネットワーク構成



国内第一号の  
アクセスポイント


# eduroam JPポータルサイト

## 参加機関向けの情報提供

<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



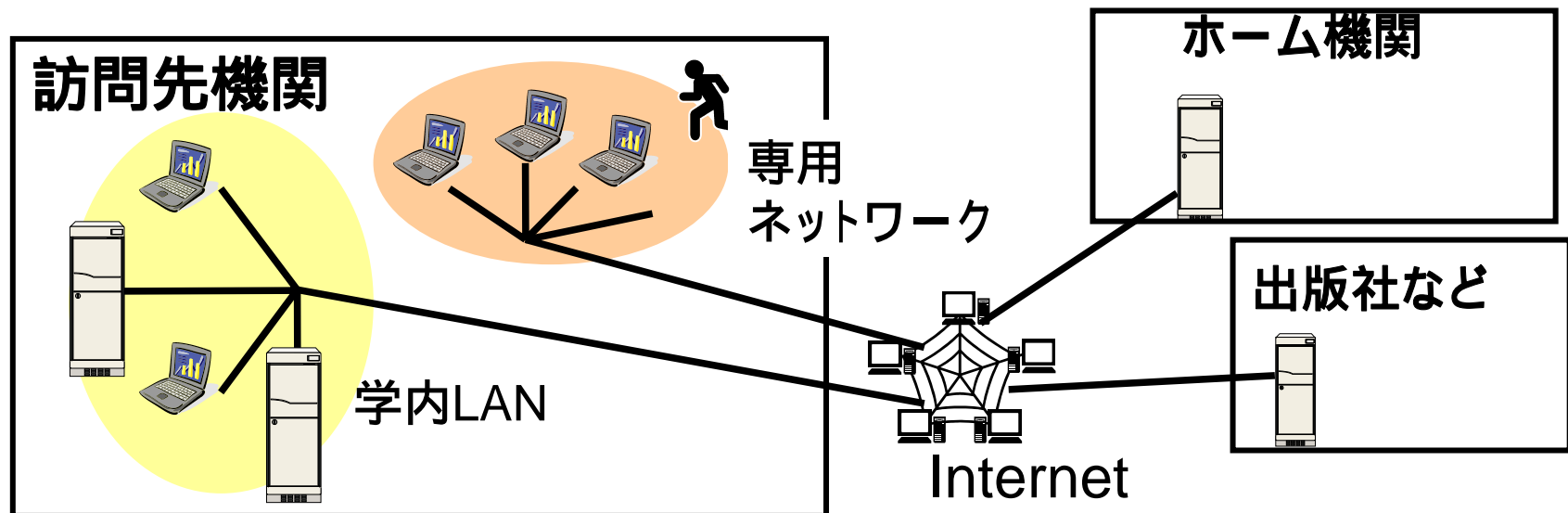
# 現行のEduroamの問題点

- 訪問先機関のアドレスをゲストに自由に利用させる形態(オープンアクセス)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
  - 通信制限/監視 (HTTP,SMTP) は運用が困難



# 現行のeduroamの問題点 解決策1

- ゲスト専用ネットワークの利用
  - 責任問題は部分的に解決可能.
  - 不正利用者の追跡はあいかわらず難しい.
  - ホーム機関のローカルリソースが利用できない.

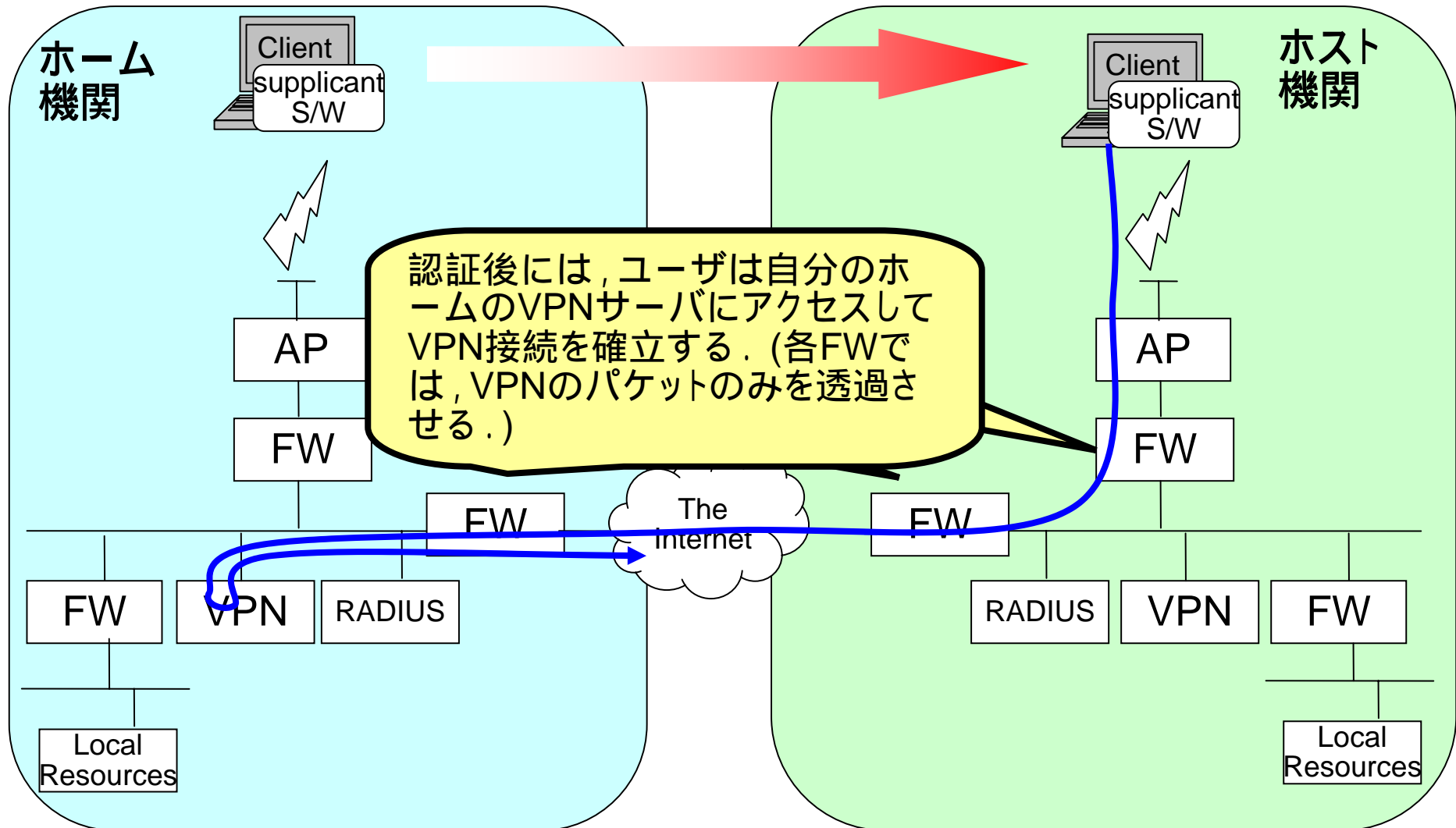




## 現行のeduroamの問題点 解決策2

- VPN接続のみを許す運用
  - = VPN-only ポリシーの適用
  - 国内外多くの機関で採用。
    - オーストラリア, 英国, 日本, スイスなど
  - 不正利用者の所属機関がわかりやすい。
  - ホーム機関のローカルリソースが利用可能。

# VPN-only ポリシー

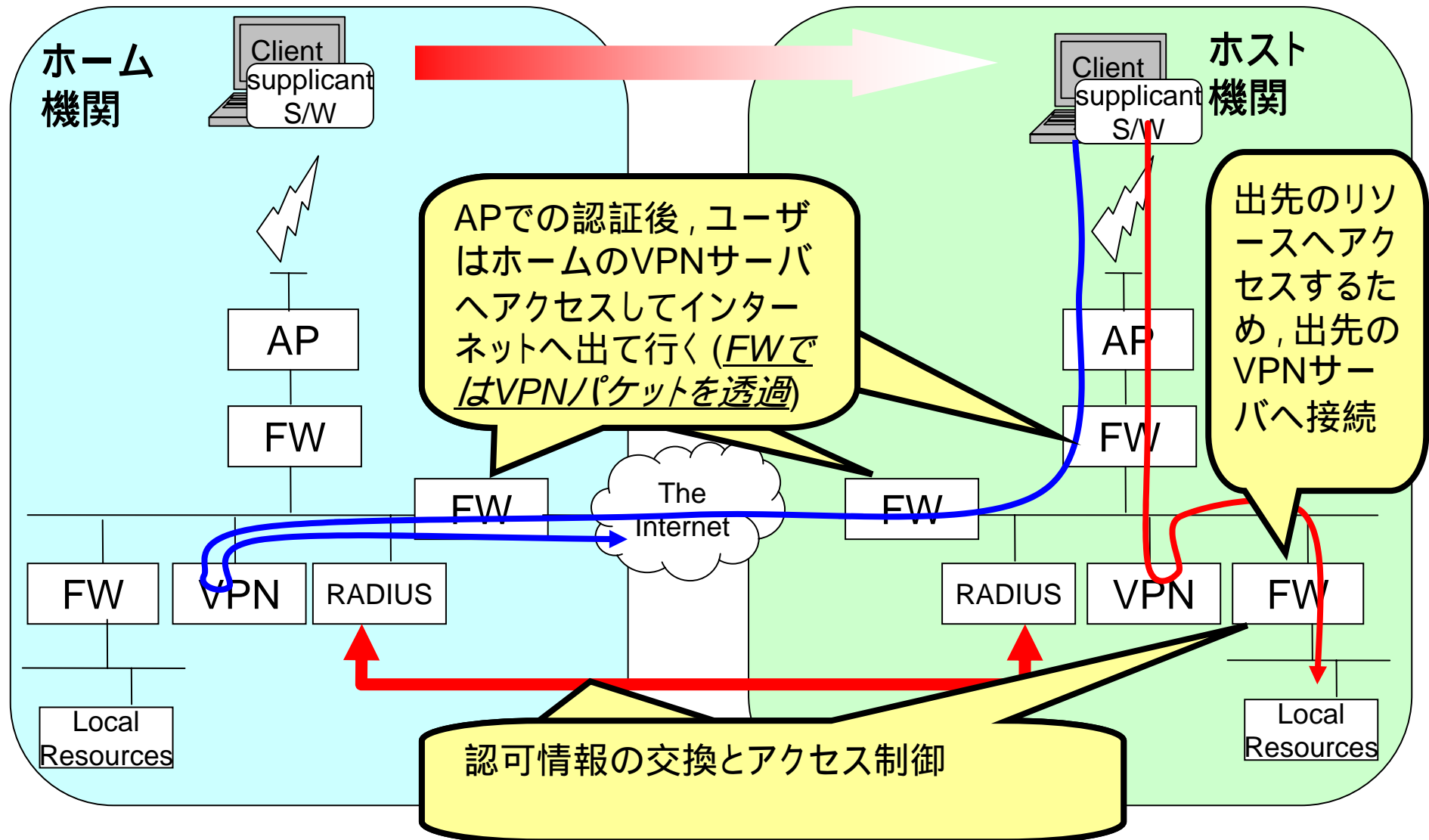




# 通過推奨プロトコル

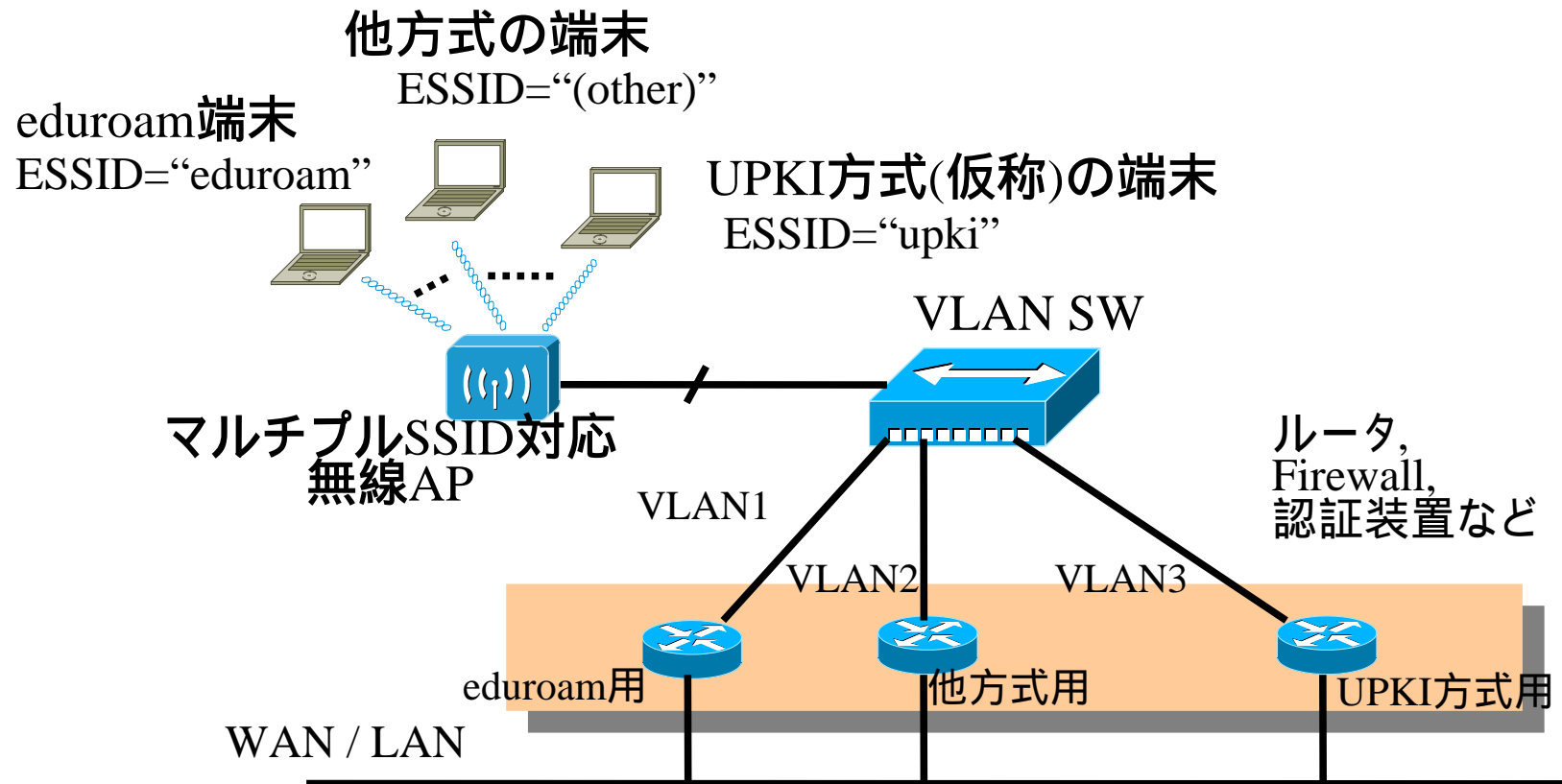
- PPTP (GRE protocol(47) , 1723/tcp)
- OpenVPN (1194/udp, 1194/tcp)
- SSH (22/tcp)
- IPsec NAT-traversal (4500/udp, 4500/tcp, 500/udp)
- L2TP (1701/udp, 1701/tcp)
  
- pop3 (110/tcp)
- pop3s (995/tcp)
- imap4 (143/tcp)
- imaps (993/tcp)
- smtp (465/tcp)
- msa (587/tcp)

# 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