Eduroamと日本への導入

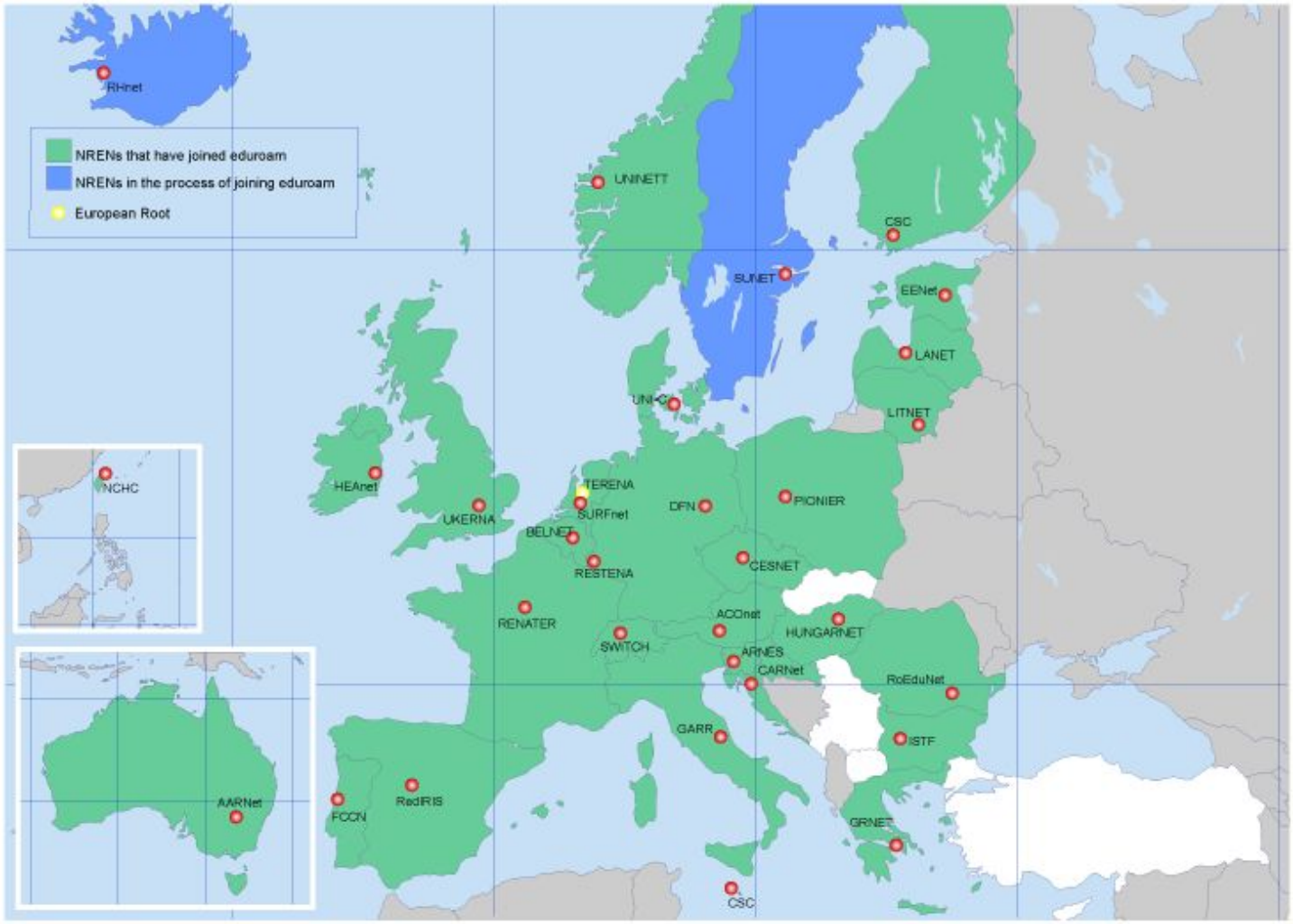
2006.10.5

東北大学 情報シナジーセンター
今井 哲郎

Eduroamとは

- TERENA Taskforce on Mobilityが規定した国際ローミング基盤
- ヨーロッパ全域･豪州，台湾などに広く普及しているデファクトスタンダード
- 基本はIEEE802.1X＋RADIUSプロキシツリー

Eduroamの普及



www.eduroam.orgより引用

Eduroam策定の経緯

TERENAではEduroamのための技術的候補として以下の3つの手法をピックアップした.

- Webベース＋RADIUS認証
- VPNベースの認証
- IEEE802.1Xベースの＋RADIUS認証

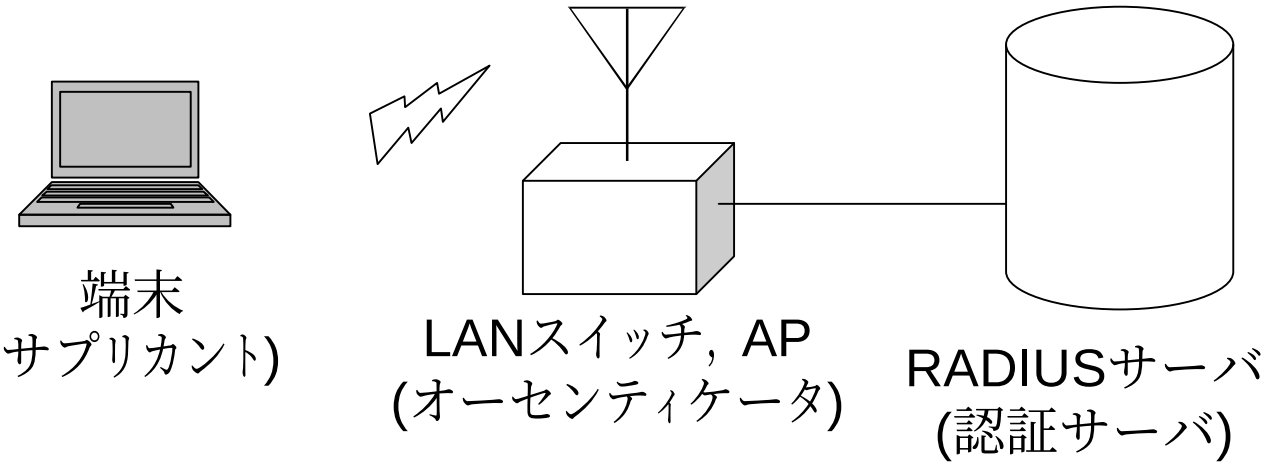
これらは以下の特徴を持つ.

- Web: scalable, not secure, already deployed
- VPN: not scalable, secure, already deployed
- IEEE802.1X: scalable, secure, new

以上のことから, TERENAではIEEE802.1Xベースの認証方式をとることになった.

Eduroamの仕組み

- IEEE802.1X
  - LANスイッチや無線アクセスポイント(AP)でユーザを認証するための仕組み

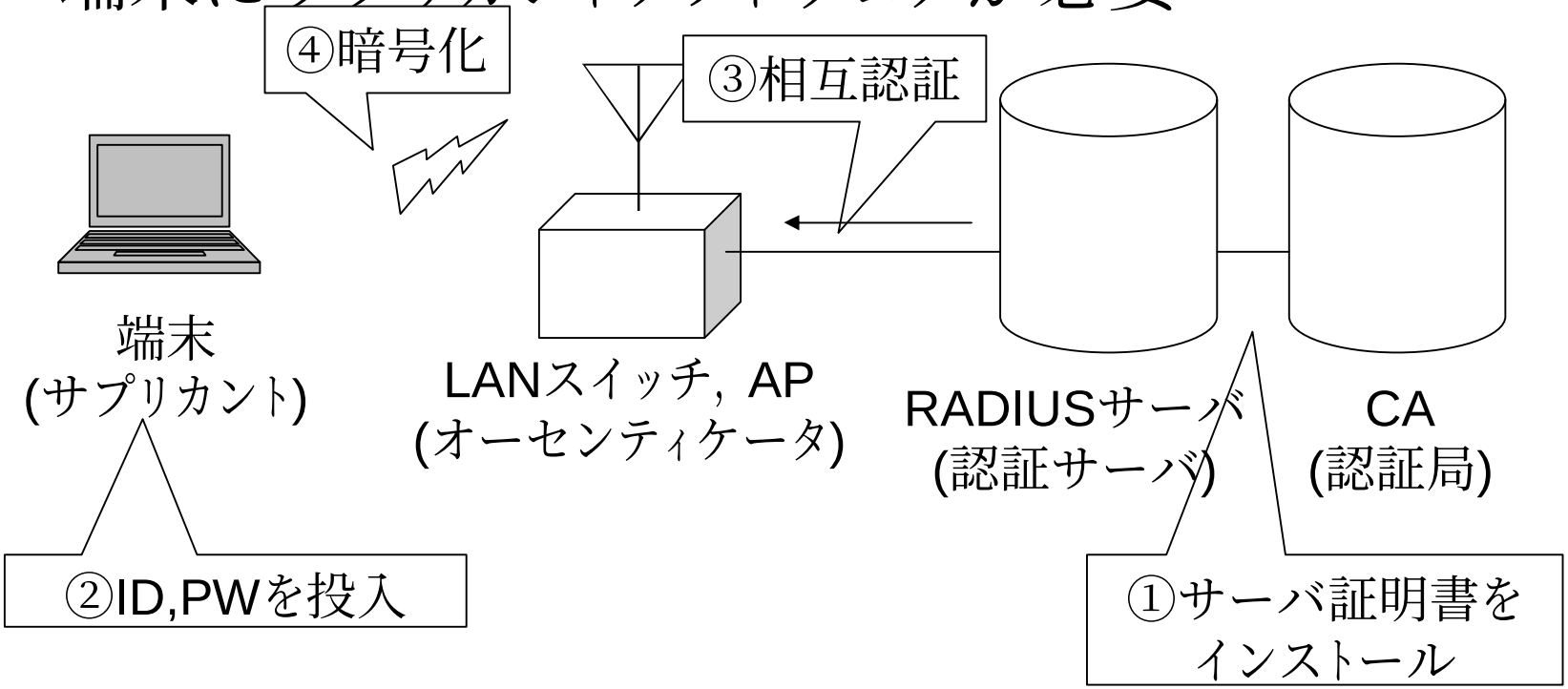


Eduroamの仕組み

- IEEE802.1X
  - 認証の方式は5種類
    - EAP-MD5
    - LEAP
    - EAP-TLS
    - EAP-TTLS
    - PEAP
  - EduroamではEAP-TTLSが推奨

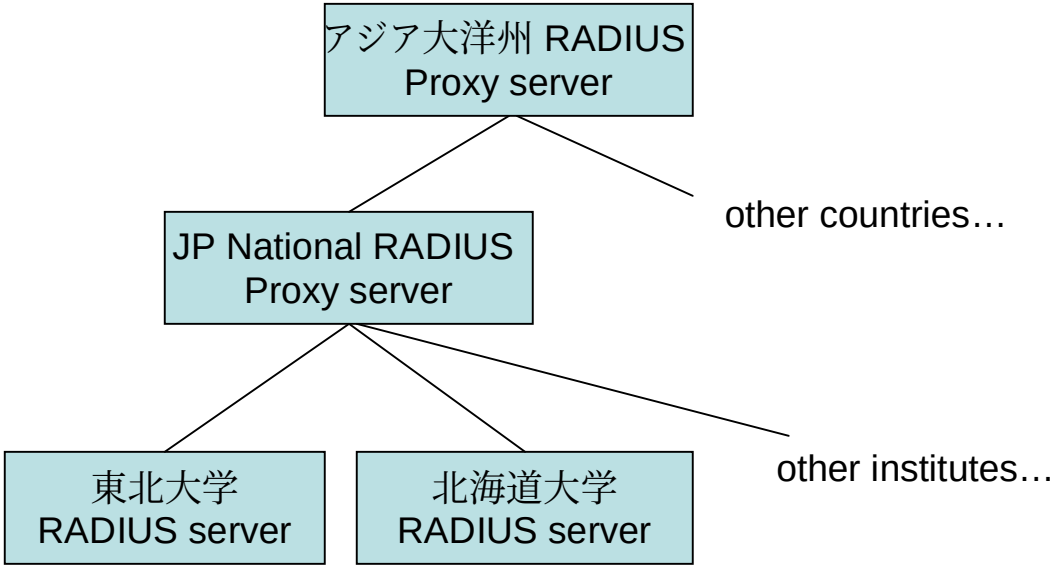
Eduroamの仕組み

- EAP-TTLS
  - 端末側はID･パスワード認証
  - 認証サーバはサーバ証明書をインストール
  - 端末にサプリカントソフトウェアが必要



Eduroamの仕組み

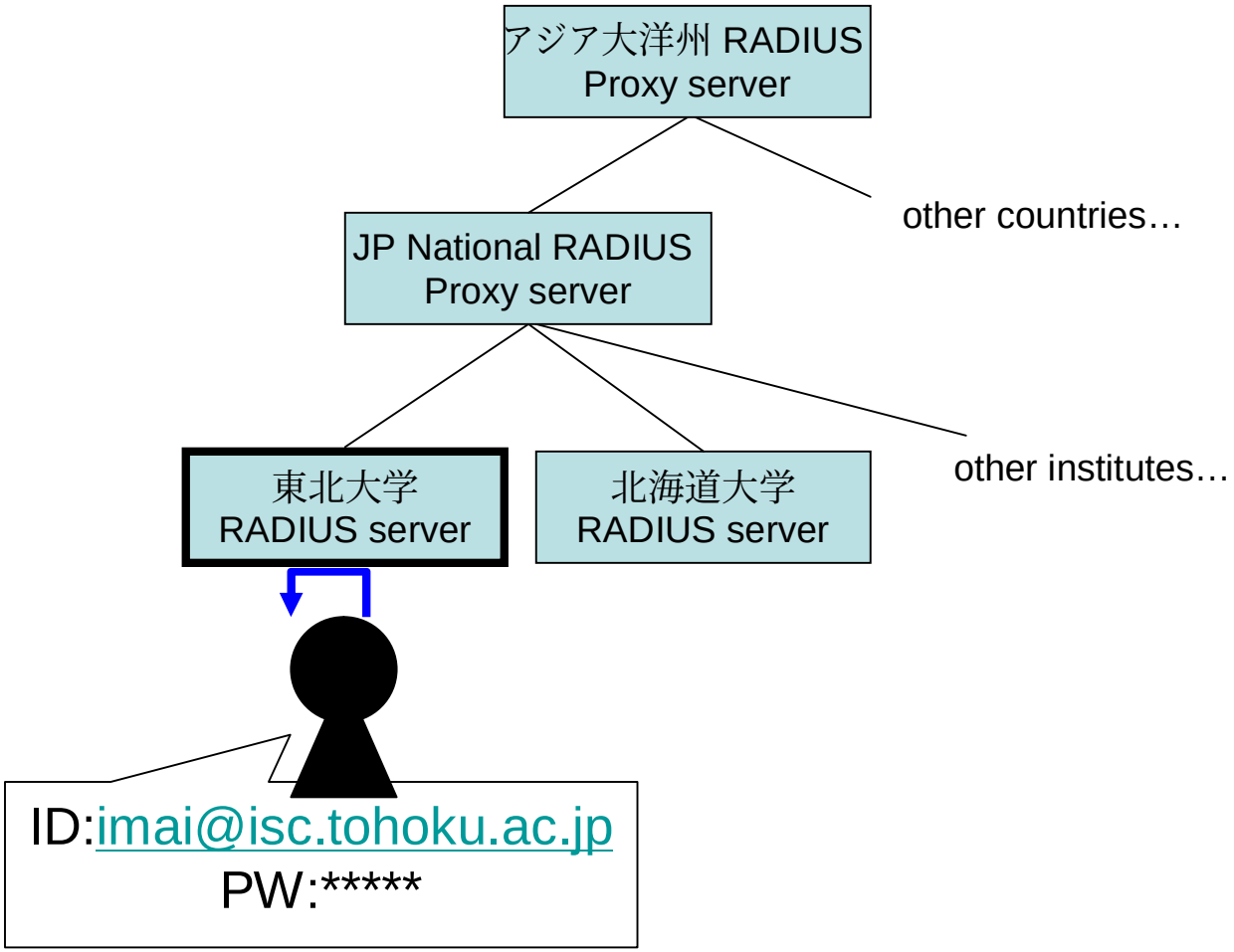
- RADIUSプロキシツリー



ユーザIDにレルム情報を付与する.
各プロキシはそのレルム情報を見て当該のサーバに転送する.

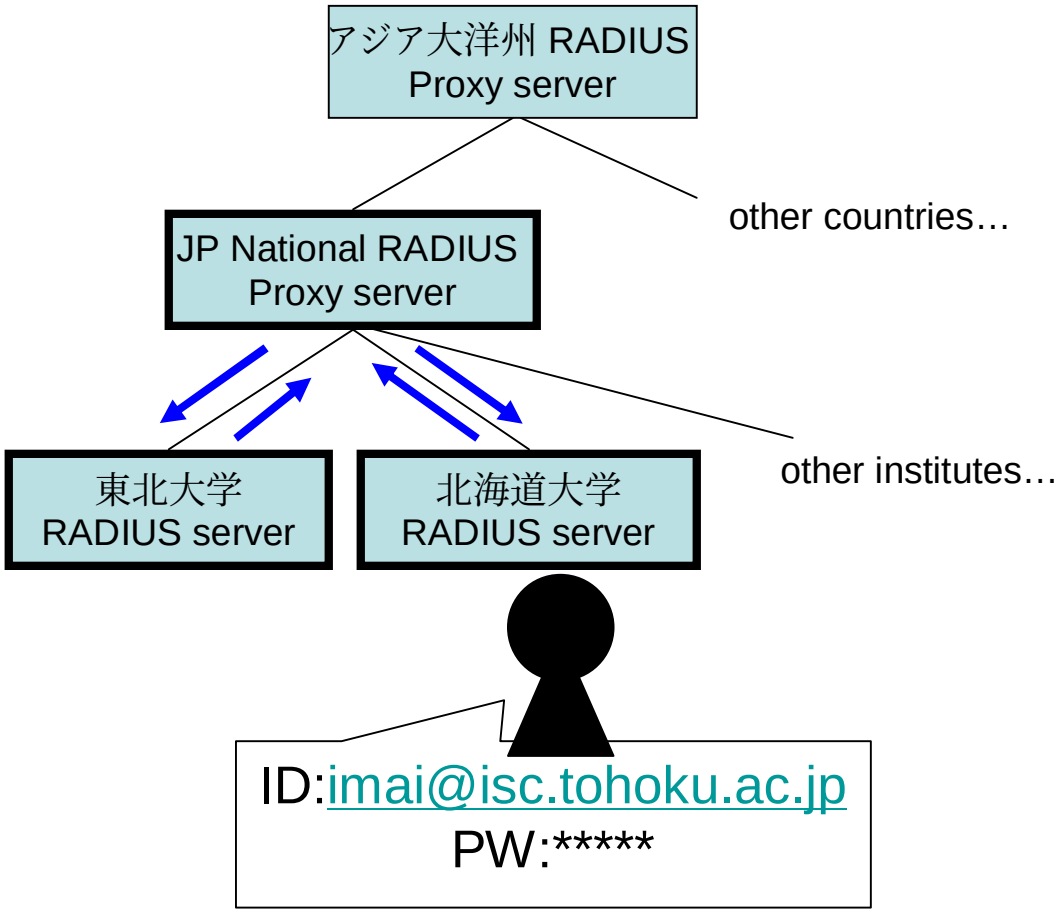
Eduroamの仕組み

- ユーザが自分のホームにいるとき



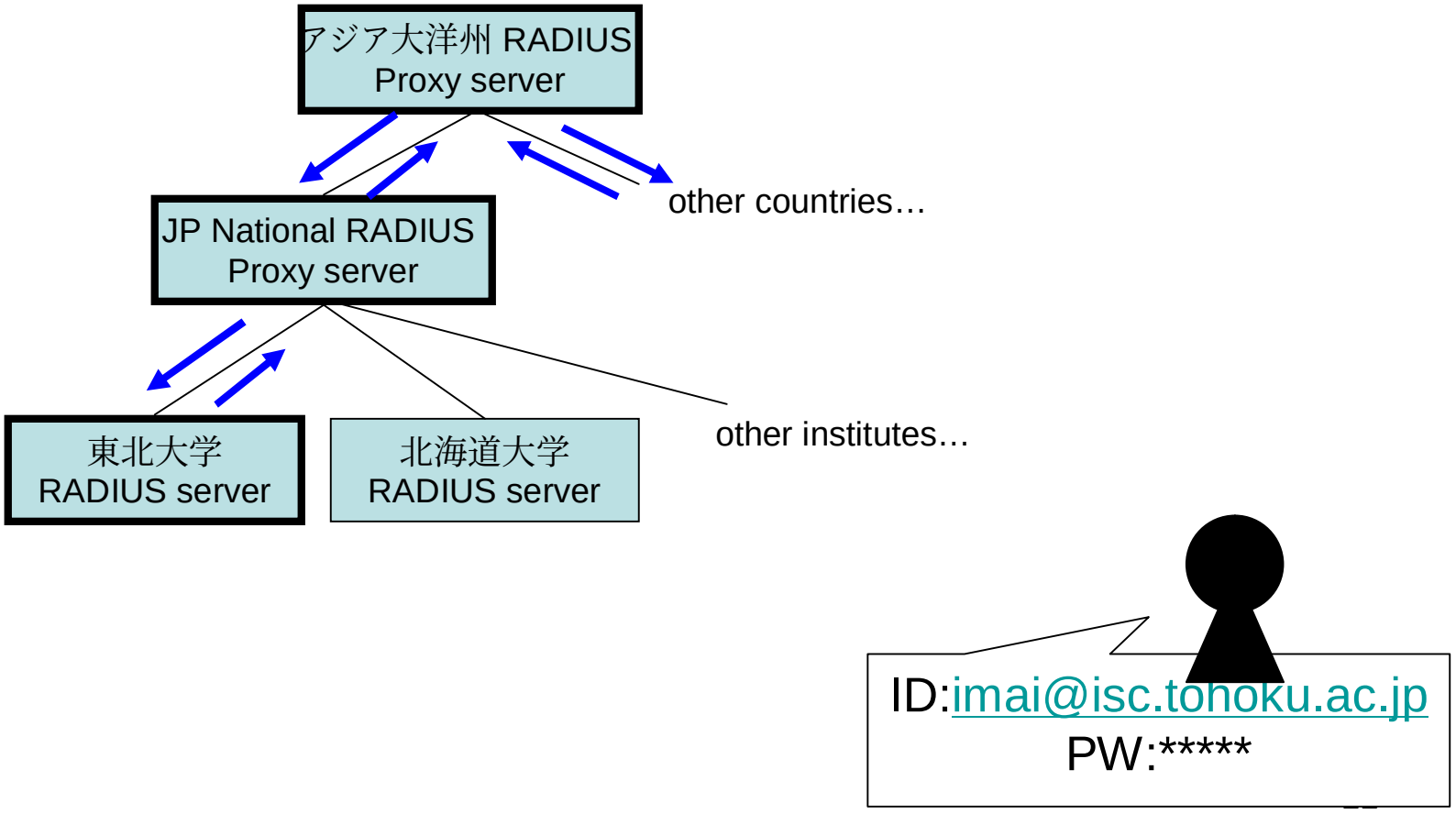
Eduroamの仕組み

- ユーザがほかの大学にいるとき

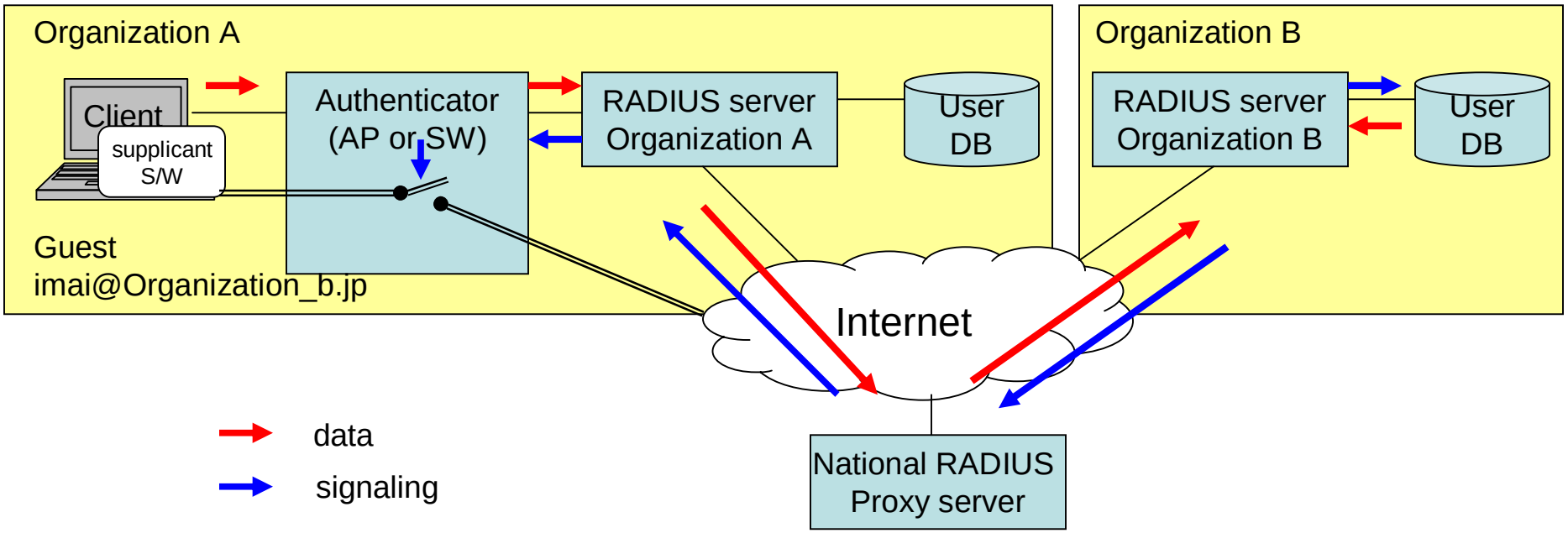


Eduroamの仕組み

- ユーザがほかの国にいるとき



Eduroam



※ユーザIDのレルム名にはDNSドメイン名と同じ文字列を使うことを推奨

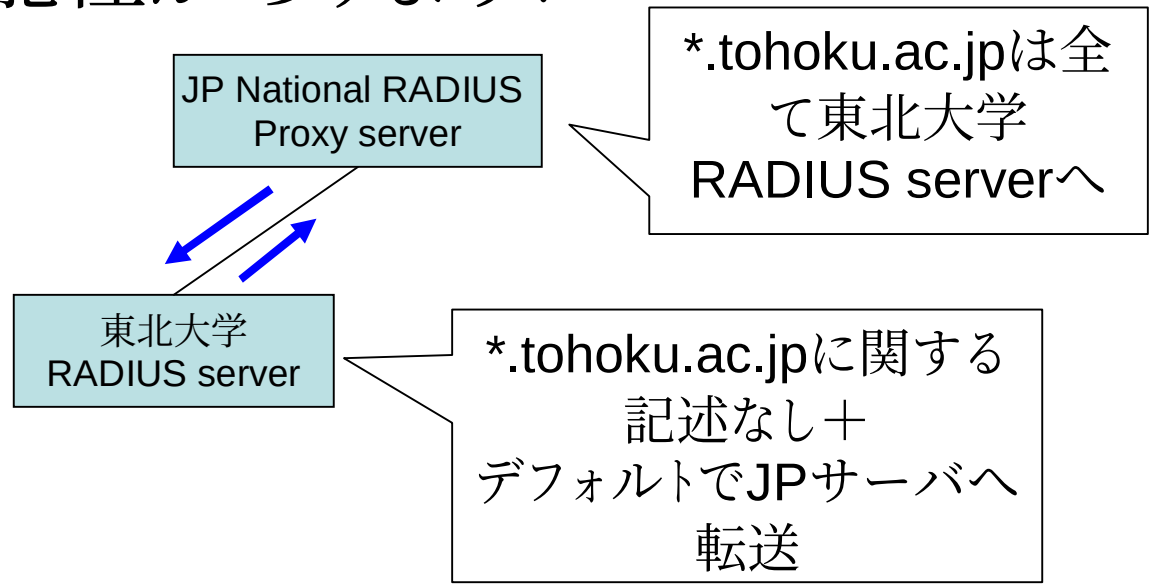
Eduroamの日本への導入

- 東北大情報シナジーセンターが先行導入
- 北大を始め九大，京大，NIIの5機関に先行して展開予定
- 参加に関しては，追って情報をeduroam.jpのWebsiteにUP

http://www.eduroam.jp/

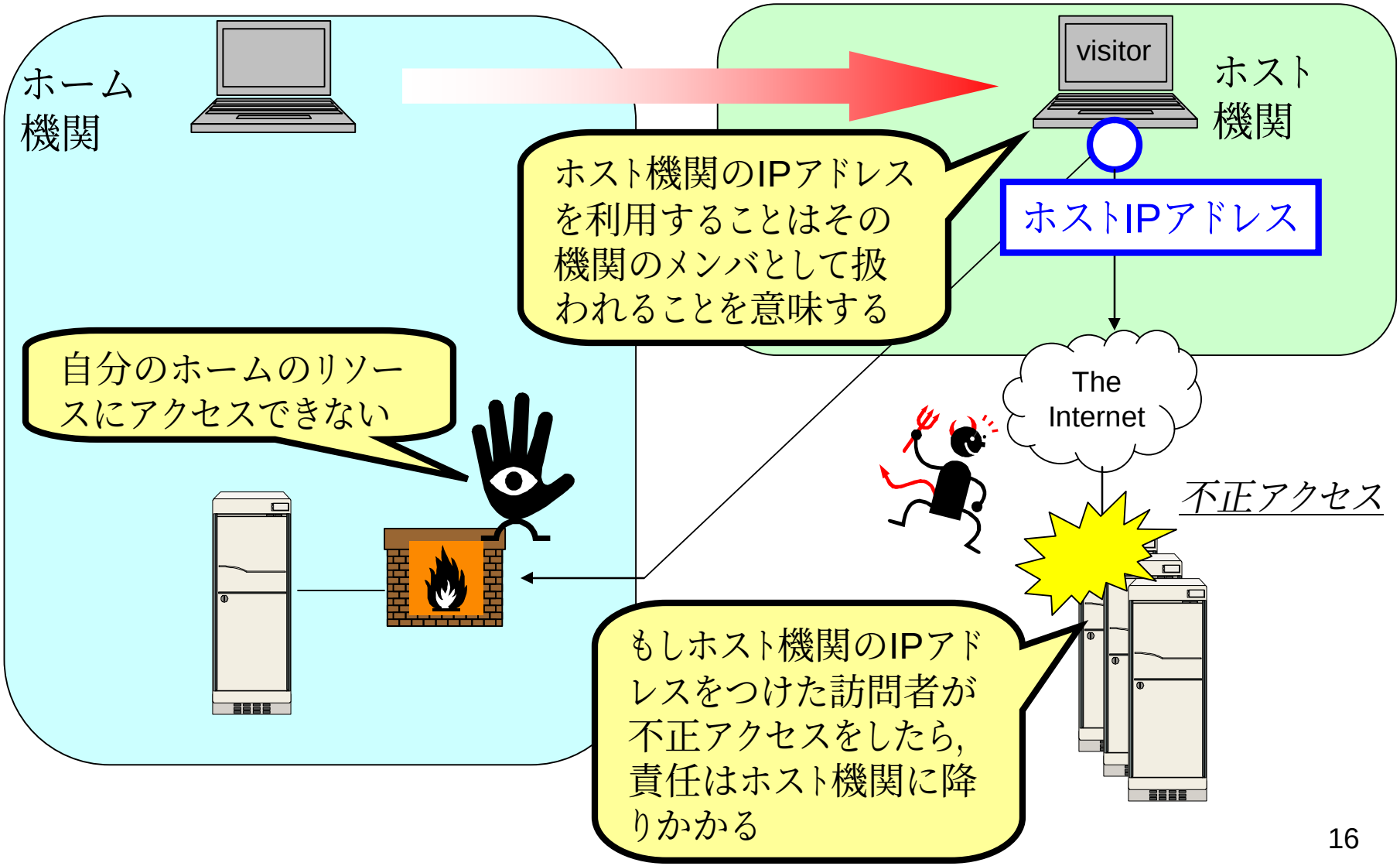
FreeRadiusの設定上の注意 (ループの回避)

- 各機関以下のRADIUSサーバの設定によっては，JPサーバとの間にループが発生する可能性があります.



※各機関は必ずproxy.confに自分のドメインは自分で処理する旨の記述を加えてください

トレーサビリティに関する問題



トレーサビリティ：ケーススタディ1

A大学では電子ジャーナルXを購読していないが，隣のB大学は購読している．そこでA大学の学生はB大学に行き，無線LANローミングを使って電子ジャーナルXをダウンロードした．ところが少し多目にダウンロードしたので，出版社はライセンス違反と判断してB大学に苦情を送った．

B大学はローミングのログを解析し，A大学に連絡の上，共同で当事者を捜索．

膨大な人的コストを費やされる．
学内の部局間でさえこのようなユーザ追跡は困難．
ましてや大学間では無理．(外国ならなおさら)．

トレーサビリティ：ケーススタディ2

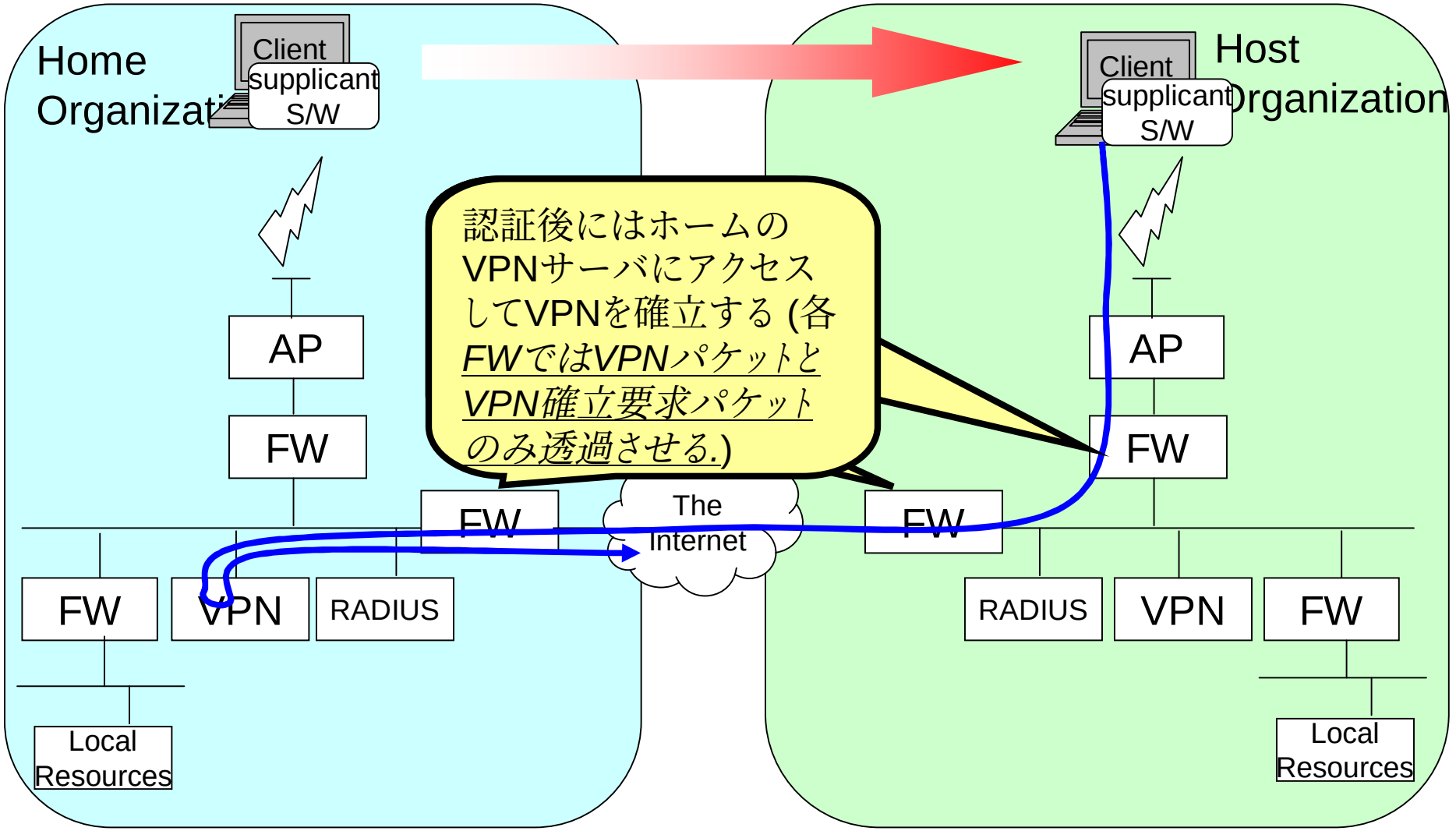
大学には多くの内部向けウェブサイトなどのリソースがあり，これらは一般に外部から閲覧されないようにアクセス制限がかけられている．A大学の職員がB大学でローミング機能を利用すると，B大学の内部情報を見ることができた．

ウェブサーバの管理者がログを見ても，学内のIPアドレスを利用しているので，部外者のアクセスにはなかなか気づかない．

ホームのIPアドレスを利用させるべき

(ただし，ローカルのリソースへアクセスする方法として出先のIPアドレスを使う方式も検討中)

日本向けのEduroam運用(提案)



議論

- Eduroamのコミュニティでは, VPNを利用した認証方式はスケーラブルでないとしている.
- 同様のことがVPN限定の方式にも言えるのではないか？

議論

- VPN方式がスケーラブルでないとしたのは，FWで透過させる全てのIPアドレスを設定する必要があり，VPN方式ではこのリストが全ヨーロッパで数千にもおよぶからであるとされる．

FWにはポート番号(プロトコル番号)のみを記述することで，この問題をクリア

※世界中のVPNサーバにパケットが送れてしまうが，
セキュリティ的には問題なし

まとめ

- Eduroamの紹介
- 日本への導入
- トレーサビリティの問題などを指摘
- 日本向けのEduroam運用の紹介