# eduroamの紹介

後藤英昭（東北大学/国立情報学研究所）

2017年6月5日　NII学術情報基盤オープンフォーラム

# USBメモリ　拾う？拾わない？


- 拾わない
- 拾う

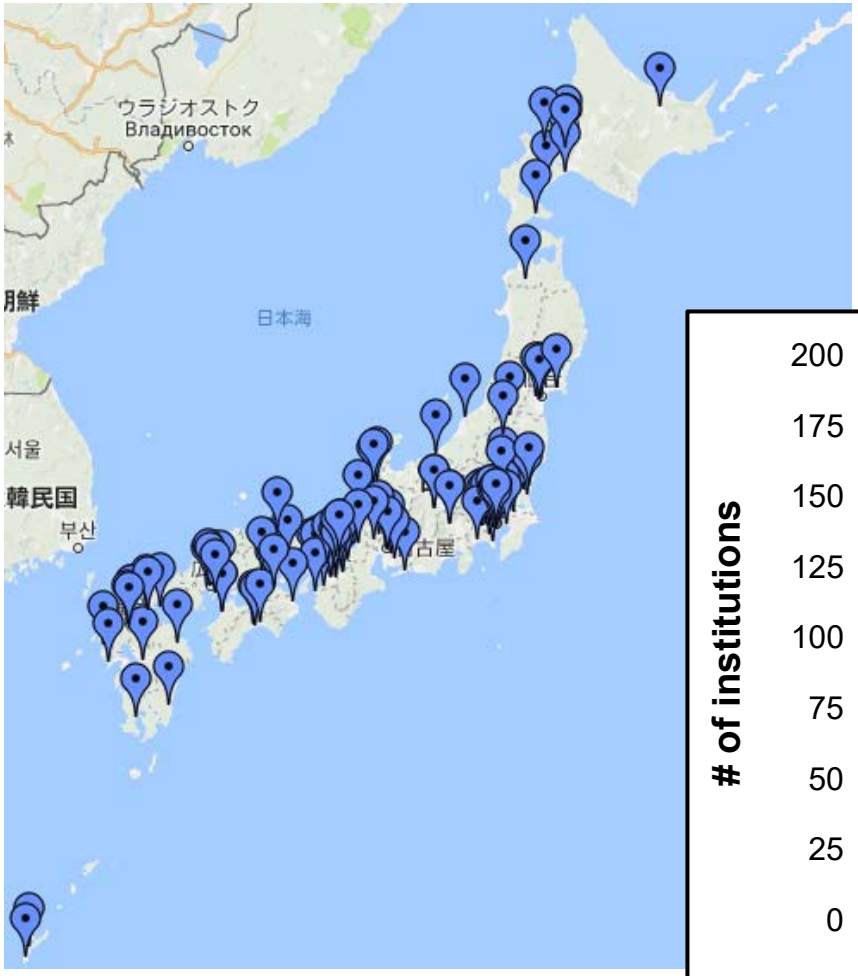
無線LANと、どう関係があるの？

# 国際学術無線LANローミング基盤「eduroam」

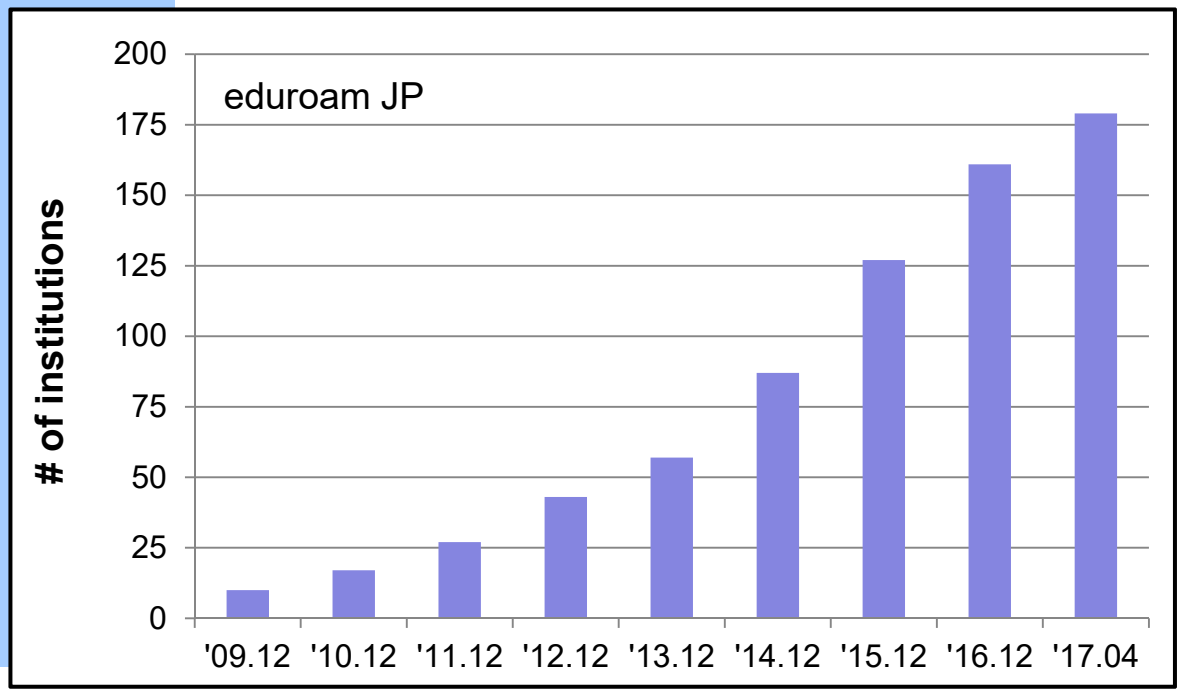
- 教育・研究用の学術無線LAN (Wi-Fi)ローミング基盤
  - 欧州TERENA (現GÉANT) で開発 (2003年)
  - キャンパス無線のデファクト・スタンダード
- 日本では「eduroam JP」の名称で運用中
  - “user@学校名.ac.jp” など、どの参加機関でも使える共通アカウント
  - 互恵の精神に基づくサービス
- メリット
  - 訪問先の無線LANが随時、シームレスに利用可能
  - 802.1X方式による安全なユーザ認証
  - 幅広い端末に対応 (Windows/Mac/スマートフォン等)
  - 来訪者に容易にネットワーク利用環境を提供

# eduroam JP と 国内動向

- 国内のeduroam参加機関 (2017.6現在 179機関)




高等教育機関と国の研究機関が対象
(2016年より初等・中等教育機関にも
展開開始)



# eduroamの国際動向

- 世界89か国(地域)に普及 （2017.6現在）
  - 欧州の全域
  - アジア16地域
  - カナダ，USA，ロシア，南アメリカ各国，南アフリカ共和国，カタール，UAE等
  - スバールバル諸島やニューカレドニアにも！

# 国際動向：キャンパス外におけるeduroam

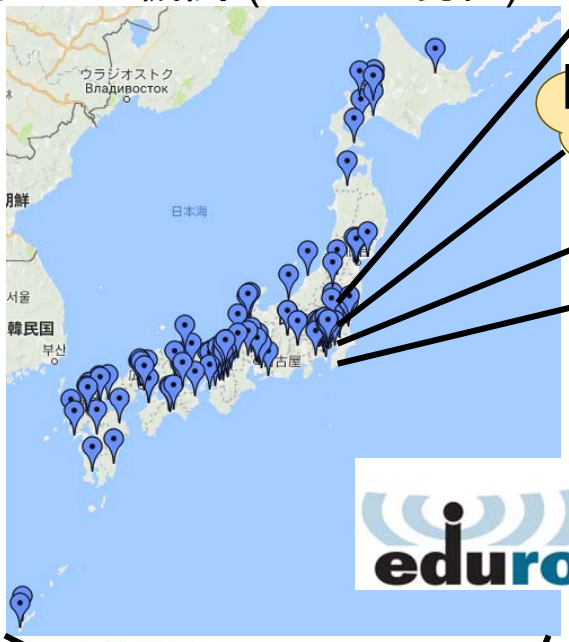
- スウェーデン（SUNET）
  - 空港や主要鉄道駅でeduroam提供
- ノルウェー（UNINETT）
  - 国内14の空港でeduroam提供
- ルクセンブルク市
  - 自治体が運営するHotCityの市街地基地局で利用可
- ミュンヘン，ヨーク，ポルト，他
  - 市街地で利用可
- ロンドン自然史博物館，他
- ……


最近は、病院iへの導入も進んでいる.
2017年現在、UKでは132の病院に導入済み.

# 公衆無線LAN – eduroam連携　継続中！

## □ 仮想的なキャンパスネットワークの拡大 !!

国内179機関 (2017.6現在)




学術クラウド

図書館・学内LAN

Internet

電子ジャーナル等

NHNテコラス 提供


キャンパス外でも自由に
学術NW・コンテンツへ
アクセス可能に！

**認証連携**

学校のアカウントによる
NWアクセスを実現

世界の89か国が加盟

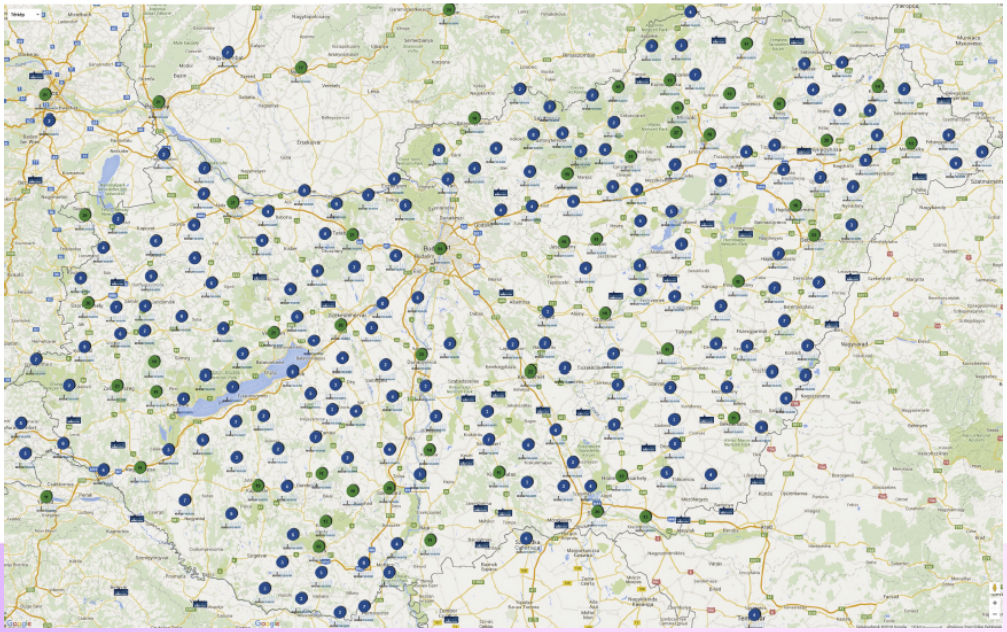
関東地域のカフェ、会議場、大型店舗等の
屋内130AP

※ キャンパス無線LANのアウトソーシング
オプションの創成

# 事例: ハンガリー

- NIIF/Hungarnetのプロジェクト (2014-2016, phase 1)
  - 1,700+の小中学校にeduroamを導入
    - eduroam IdP-as-a-Service, SP-as-a-Serviceを実現
  - 教職員に加え、生徒と親も対象
  - 生徒向けのコンテンツ・フィルタは、学校または親が与える端末側に実装 (法律上の責任は、家庭>学校>プロバイダ)

**Figure 2.** eduroam service locations in Hungary (mostly at schools)



# 事例: 大阪教育大学附属平野小学校

- 大容量の基地局を全教室に導入
  - クラス全員が「一斉に端末を使える」環境を実現
- 国内の小中高で初のeduroam導入
  - 現時点で、eduroamは教職員用

# これらはセキュリティ対策では ありません！

- SSIDステルス化
  - 正規利用者の通信を傍受すれば見えてしまう.
- MACアドレス認証（MACアドレス登録）
  - 電波を傍受すれば見えてしまう.
  - MACアドレスを変更できる端末は少なくない.
    偽装して突破可能.
  - 最近のOSには「MACアドレスランダム化」の機能があり,
    事前登録制は現場で混乱を招く.（実用的ではない）

残念ながら，大学でも，調達仕様書に書かれていることがあった.

# 無線LANのセキュリティ

- オープンWi-Fi +ウェブ認証（キャプティブ・ポータル）
  - 通信内容は筒抜け / 通信路のハイジャックも容易
  - ID・パスワードの漏洩リスクが非常に高い
  - 偽基地局対策が困難（中間者攻撃、マルウェア注入など）
- WPA2-PSK（WPA Personal）
  - 利用者認証がなく、大人数でもトラブルが少ない ☺
  - 鍵が秘密にできる少人数環境でしか、安全性が保てない
    - 鍵が漏れたら盗聴・不正侵入は容易（職員用にはダメ）
  - 偽基地局対策、不正利用監視が難しい
    - 盗聴、中間者攻撃、マルウェア注入のリスクあり

道端に落ちている怪しいUSBメモリを、常用のPCに挿すよりも、危険なケースがある.
同様のことが無線自動接続&ログインで行われる.

# 無線LANのセキュリティ（続）

- WPA2-AES (WPA Enterprise) / eduroam
  - 1X認証による安全な利用者認証 ☺
  - 利用者個別の暗号化による安全な通信 ☺
  - 偽基地局対策が可能 ☺
  - 認証システムが必要
  - 利用者サポートが若干多い？（認証トラブルなど）

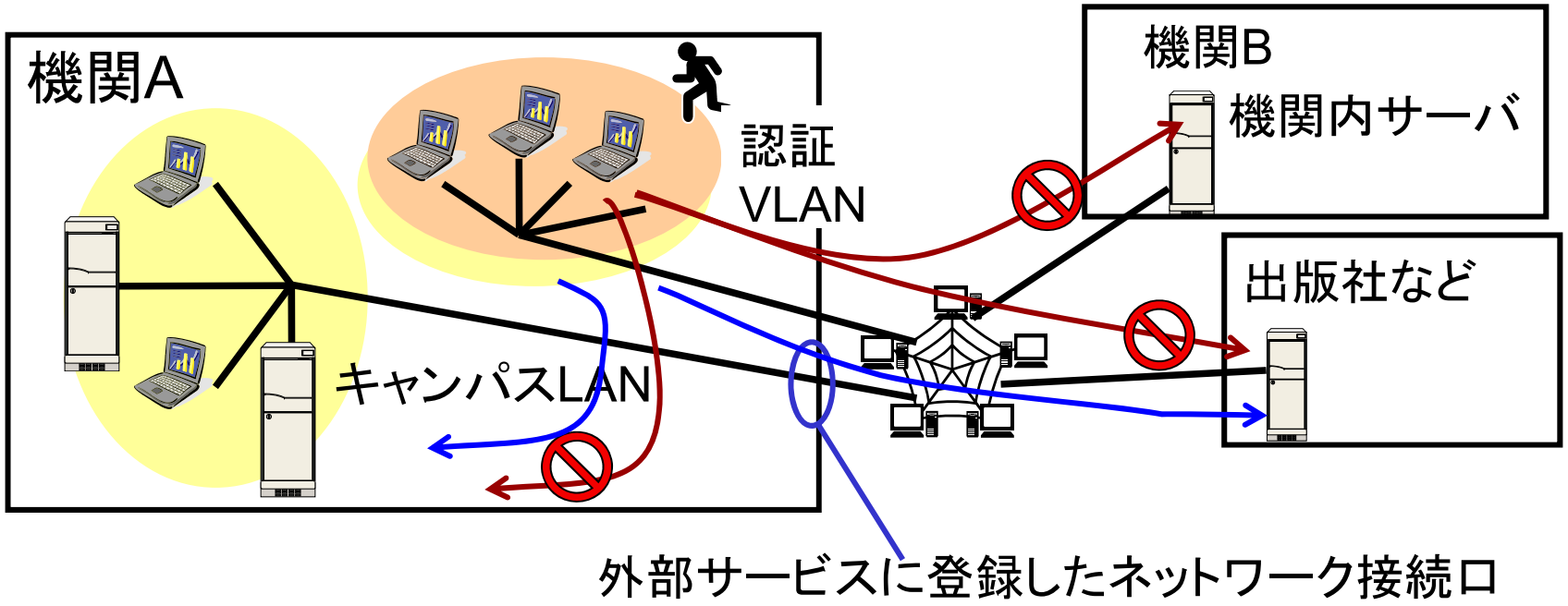
基地局システムと、認証システムの、正しい設計が重要.

良く設計されたシステムなら、サポートも減らせる.

# キャンパス無線LANを一本化

- 「認証VLAN」を導入すれば、自機関の利用者として認証された者の端末をLANに直接収容することができ、利便性が大幅に向上.

訪問者はゲストネットワークに収容し、学内LANにアクセス禁止.



# まとめ

- 安全のためWPA Enterprise (1X認証)の導入を！
  - キャプティブポータル/ウェブ認証は、セキュリティ面で問題が多い.
  - セキュリティ対策では、現在、1X認証が唯一の選択肢.

- eduroamを導入して、
  グローバルスタンダードなキャンパス無線LANに.
  - 他機関との相互利用、市街地での利用も可能.
  - ネット時代の新しい教育・研究環境の実現.

- キャンパス無線LANはeduroamに一本化可能
  - 認証VLANで、訪問者をゲストネットワークに振り分け.
  - eduroamは、訪問者向けというより、
    主に機関の構成員に大きな利便性をもたらすもの.