ITRC meet50 INI分科会セッション (VisLab OSAKA & Virtual)
2021年11月24日

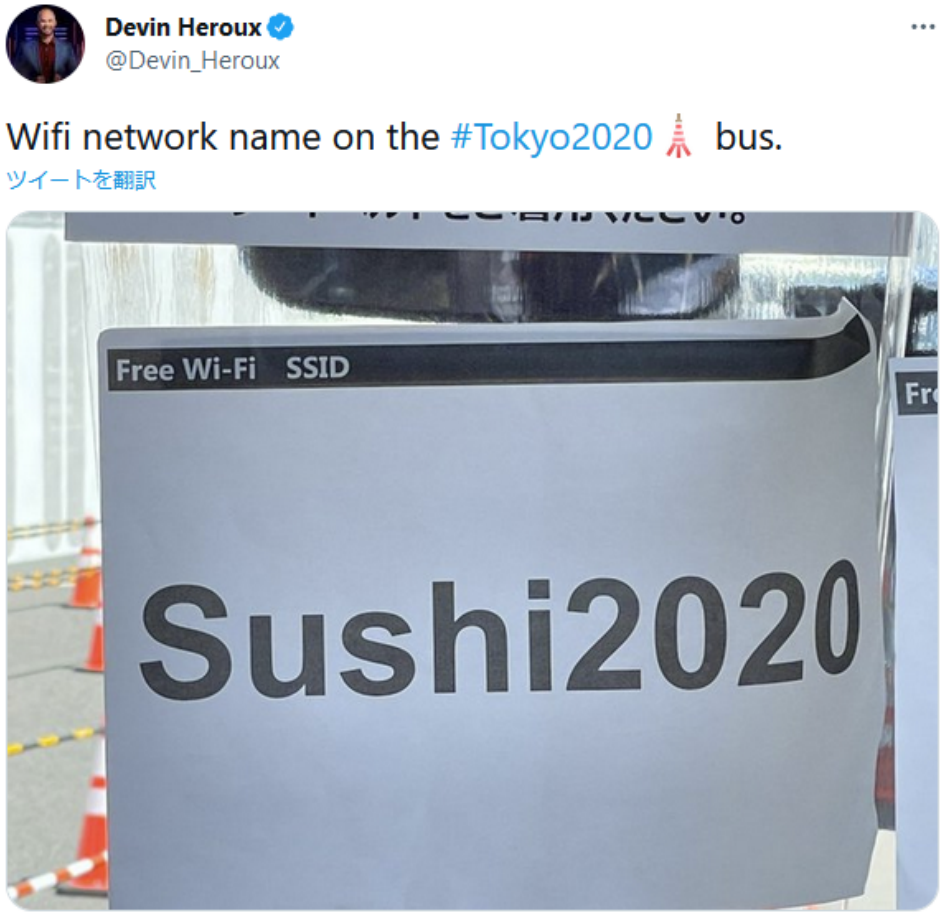
セキュア無線LANローミング基盤 eduroam, Cityroam, OpenRoamingの 技術と開発動向

後藤英昭　　東北大学・サイバーサイエンスセンター

今日の話

- 公衆無線LANのセキュリティとローミング
- 次世代ホットスポット(NGH)　と呼ばれていた何か
- 国際学術無線LANローミング基盤 eduroam
- WBA OpenRoaming
- セキュア公衆無線ローミング基盤 Cityroam

公衆無線LANのセキュリティ? 🤔



https://twitter.com/Devin_Heroux/status/1419092561570893825

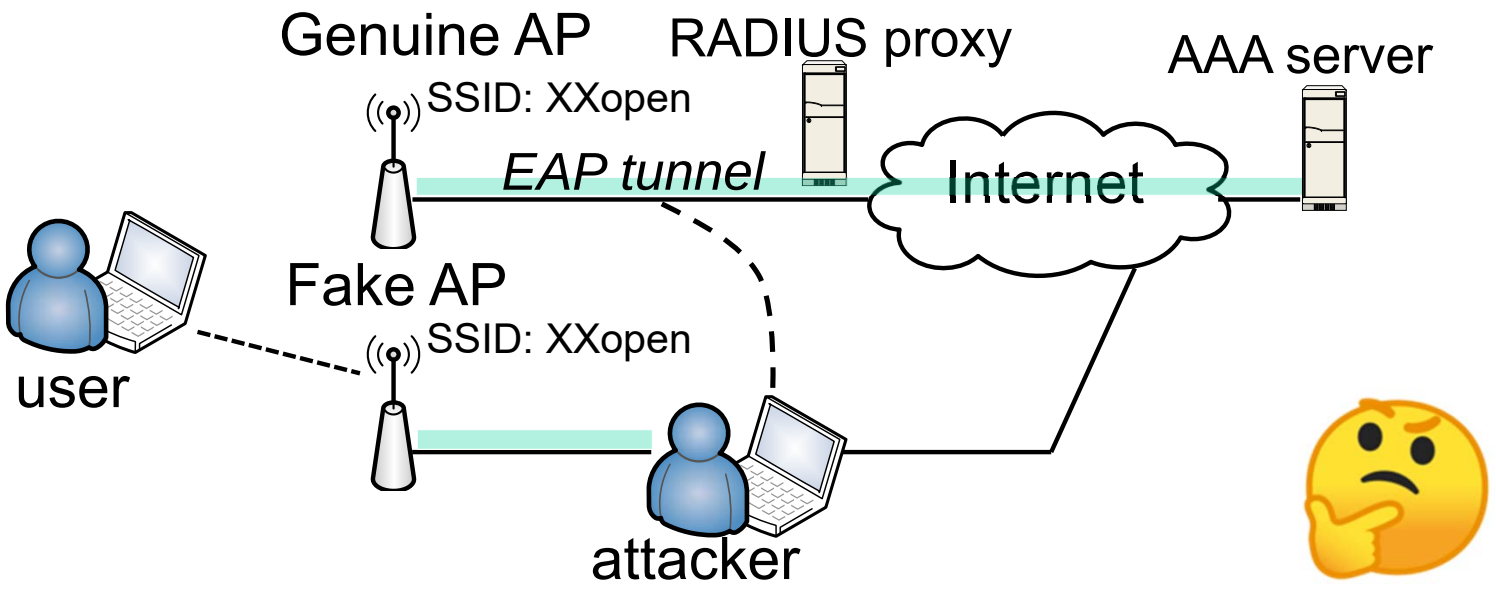
https://twitter.com/PabloRochat/status/1400475642211180547

公衆無線LAN / キャンパス無線LANのセキュリティ

- 無線区間の盗聴
  - 鍵を大勢で共用するWPA2 Personal (PSK)では対策不可
  - WPA2 Enterprise (802.1X)で端末ごとの暗号化で対策
- 有線区間の盗聴
  - 店舗や個人宅設置の基地局では、利用者やロケーションオーナーによる有線の盗聴が問題になりうる.
  - 上流(有線)部分で盗聴可能なため，暗号化して無線LANコントローラ(WLC)に収容するなどの対策が必要
  - 偽基地局対策 (次項参照)
- 不十分なプライバシ保護
  - 利用者に不透明な行動分析，追跡
  - 最近は、MACアドレスランダム化など，端末側で対策

公衆無線LAN / キャンパス無線LANのセキュリティ

- 偽基地局問題
  - オープンやWPA2-PSKでは，SSIDと鍵さえ合っていれば、偽の基地局でも自動で繋がり大変危険！
    (MITM攻撃, 盗聴, マルウェア挿入, 基地局からの能動攻撃など)
  - 正しい事業者の基地局であることを確認する必要性
    1X認証なら「サーバ証明書の検証」で対策可



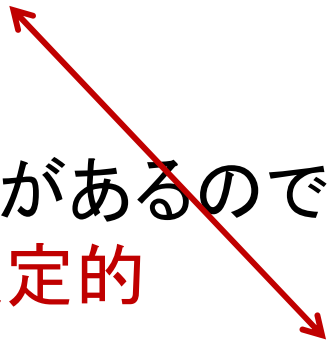
EAP: Extensible Authentication Protocol

公衆無線LAN / キャンパス無線LANのセキュリティ

- キャプティブポータルの問題
  - 偽基地局による誤操作誘導
  - ID/PWの窃取
  - HTTPSのリダイレクトによる証明書エラーに，利用者が惑わされる (無視するクセがつくのは大問題)
  - 最近の端末はmini browserによる部分的な対策あり.

無線LANの有効なセキュリティ対策

- Captive Portal API (Capport), RFC 8908
  - 安全性向上. 最近の端末で実装が進んでいる.
- IEEE 802.1X (1X認証)
  - 現在普及している実用的なセキュリティ
    (WPA2-AESを使用すること. TKIPは脆弱性あり)
  - サーバ証明書の検証が必要
    (PEAP方式のMS-CHAPv2には脆弱性あり)
  - 有線部分の盗聴対策は別途必要.
- VPN方式
  - オープンWi-Fiには偽基地局問題があるので、
    VPN方式のセキュリティ対策は限定的
  - 有線区間も含めて暗号化による通信内容の保護が可能
    (VPNサービスの提供者を信じるしかない)



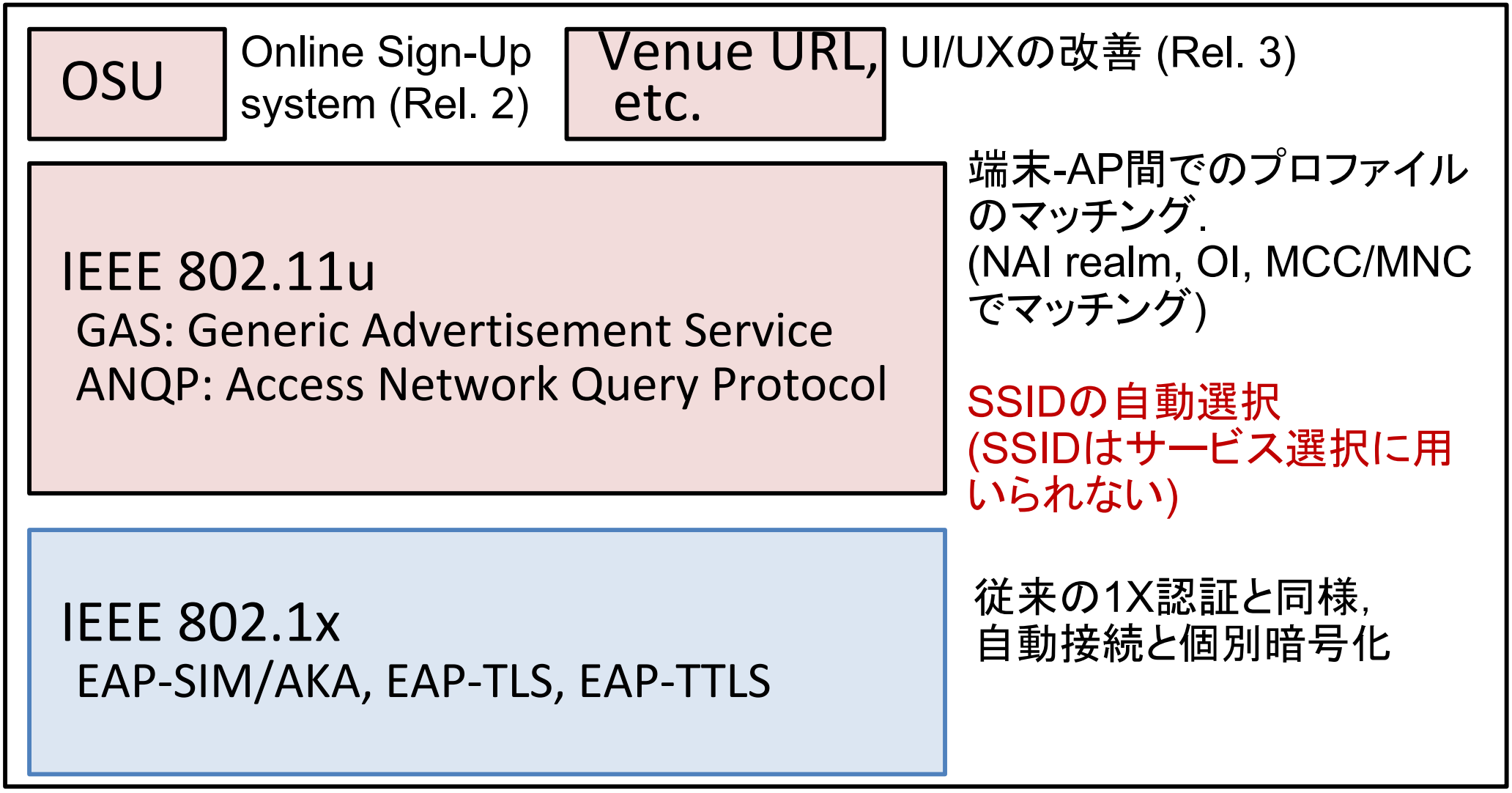
次世代ホットスポット (Next Generation Hotspot, NGH) と呼ばれていたもの

- Wi-Fi AllianceとWireless Broadband Alliance (WBA)が共同推進するコンセプト規格.
  - 現在、NGHの名称は使われない.
- PasspointによるSSID自動選択、自動接続.
  - 携帯電話並みの利便性を提供
  - 自分のサービス契約に合致する基地局に自動接続
  - SSID選択後は1X認証と同等で、安全な接続 (偽基地局への誘導を回避可能)
- 国際ローミングの標準化
  - WBA WRIX (Wireless Roaming Intermediary eXchange) standard

Passpoint or Hotspot 2.0?

- 技術仕様としてPasspointとHotspot 2.0は同じもの
  - Passpoint technical specification
  - 基地局メーカーでは “Hotspot 2.0”表記が好まれる.
  - 通信事業者では “Passpoint”表記がよく見られる.
- Release 2, 3で機能追加
  - OSU: Online Sign-Up (R2)
  - Policy provisioning (R2)
  - Venue URL (R3)
  - Operator Icon Metadata (R3)
- Wi-Fi Allianceの認証を受けたものがPasspointと呼ばれる (が，少し緩和された)
  - Wi-Fi CERTIFIED Passpoint™
  - iOSでもまだRel.1の段階

Passpointの仕組み



Next Generation Hotspot (NGH):

Passpoint + Roaming (+ something sophisticated)

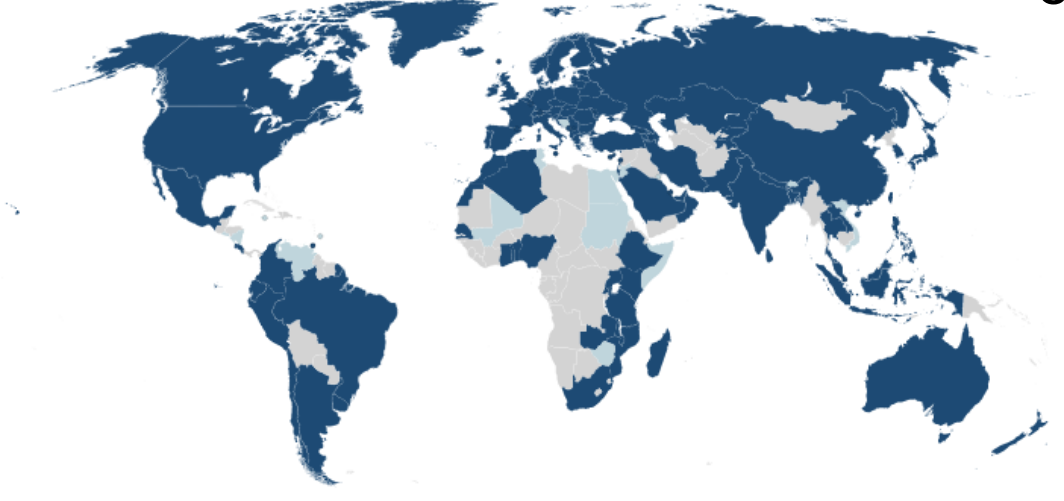
WBA WRIX standard
(Wireless Roaming Intermediary eXchange)

ローミング認証連携のための仕様

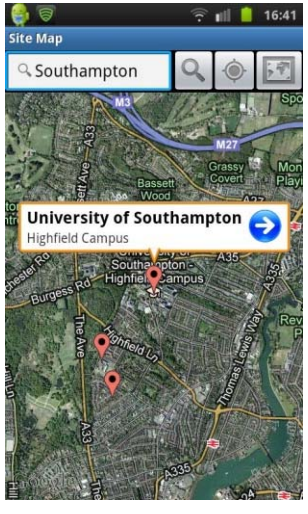
- WRIX-i (Interconnect)
- WRIX-n (Network)
  - 実体はRADIUS. 属性値などを取り決め.
  - この2つだけでもローミング接続は可能.
- WRIX-L (Location)
  - OpenRoamingでは必須.
- WRIX-d (Data clearing)
- WRIX-f (Financial settlement)

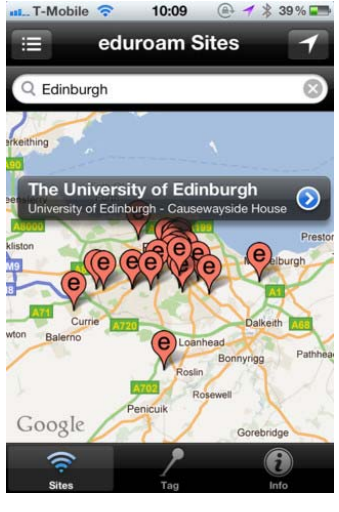
国際学術無線LANローミング基盤「eduroam」

- 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
  - キャンパス無線のデファクト・スタンダード
  - 世界中の参加機関で、無線LANが無料、安全、自動接続で利用可能
    - 互恵の精神に基づくサービス
  - 802.1X方式による安全なユーザ認証
  - 認証VLANによるアクセス制御&ポリシー適用も可能



eduroam Companion (Android, iOS)

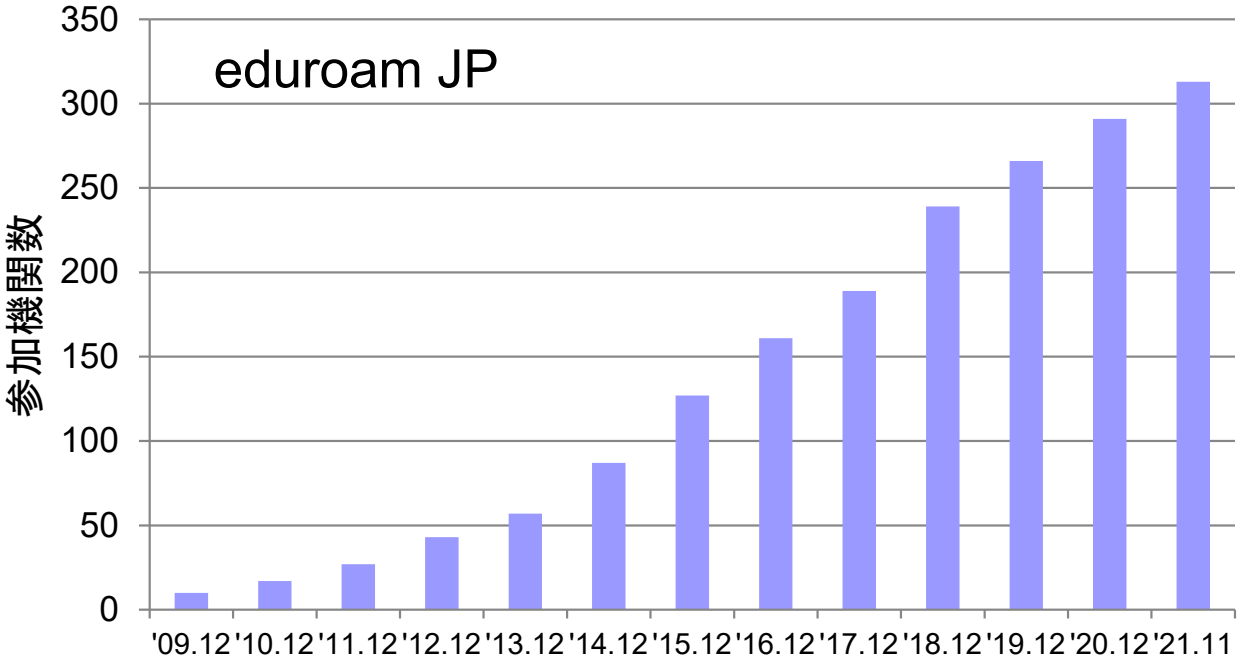




eduroam JP

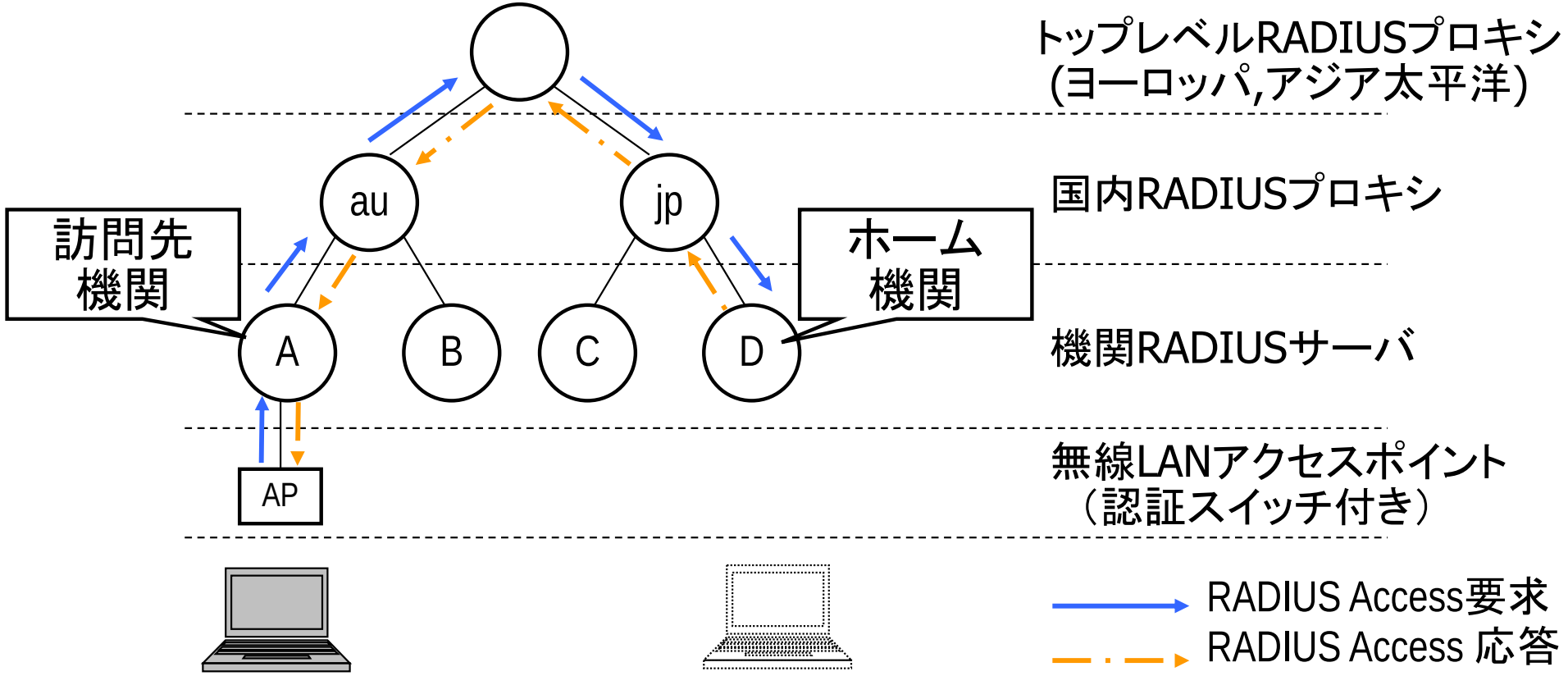
- 2006年8月 日本導入 (国立情報学研究所(NII)が運用)
- 2021年11月現在 国内313機関 (国立大学は90%)

初等・中等教育機関にも導入開始 (2016～)



eduroamのしくみ

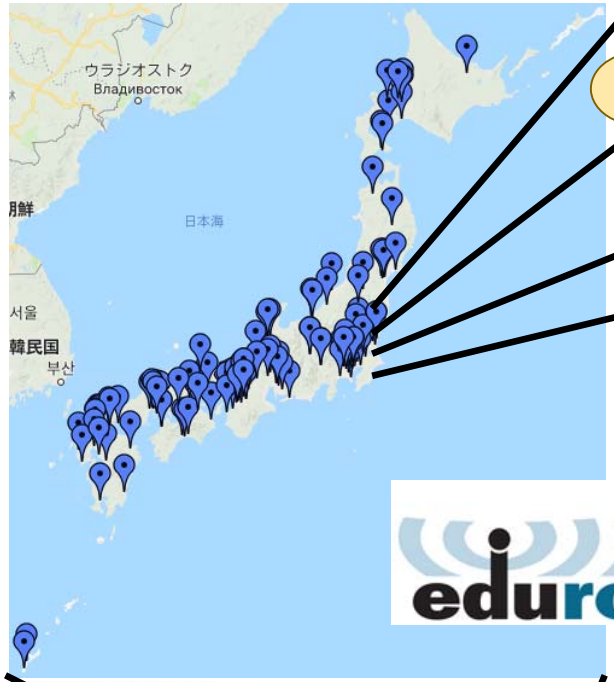
- IEEE802.1x認証に基づいた，**安全なユーザ認証・認可**
- 利用者が所属機関のアカウントを使って訪問先で利用
  - レルム付きのIDを使用.　　例: alice@example.ac.jp
- RADIUSツリーを介して認証情報を相互利用（認証連携）
- 標準の構成では、機関ごとにRADIUSサーバが必要



eduroam市街地サービス　継続中！

- 仮想的なキャンパスネットワークの拡大 !!

国内313機関 (2021/11現在)



世界の106か国が加盟

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
(2010～2020年)

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！

Cityroam

eduroam

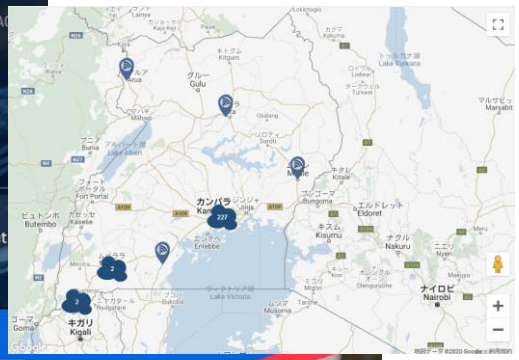
認証連携

学校のアカウントによる
NWアクセスを実現

※ キャンパス無線LANのアウトソーシング
　オプションの創成も

Off-campus eduroam as digital infrastructure

South Africa:
eduroam at most universities, addressing digital divides and COVID-19 (July, 2020)



Today a University of Cape Town student living in Khayelitsha can access eduroam, the high-speed internet offered by nearly all South African universities and an additional 105 countries around the world, at their local library. A University of Witwatersrand (Wits) student living in Sebokeng needs only to travel 30 minutes to North-West University's Vaal Triangle Campus to download their course content and videos quickly and for free on the eduroam network, while a University of South Africa (UNISA) student anywhere can check the eduroam interactive map to see where their closest internet access point is.

ut NEWS IN FOCUS OPINION SPORT MAGAZINE RADIUS SECTIONS Search

NEWS JAN 5, 2021

Government to Extend WiFi Initiative for Students to 90 New Locations

Difficulty accessing the internet in rural communities has become a major talking point in higher education circles since the outbreak of the pandemic.

Cormac Watson
EDITOR

The government will extend internet access for students to 90 new locations across the country in order to create "extended virtual campuses", Higher Education Minister Simon Harris announced today.

HEAnet will lead the initiative, rolling out eduroam – a WiFi connection that students can automatically connect to – to locations accessible to students, such as libraries, museums, public offices, coffee shops and shopping centres.

Eduroam is already available to students in a number of locations, including libraries in Longford and Galway, the Convention Centre and Custom House Quay in Dublin

"Extended virtual campuses" in Ireland (Jan. 2021)
http://www.universitytimes.ie/2021/01/heanet-to-extend-wifi-initiative-for-students-to-90-new-locations/

RENU in Uganda:
Town-wide eduroam to help students learning under COVID-19 (Oct. 2020)

Off-campus eduroam as digital infrastructure

HEAnet
@HEAnet

Did you know that there are more than 160 eduroam Wi-Fi hotspots across Ireland? Click here to view a map of all live eduroam locations: heanet.ie/services/conne... #eduroam #eduroameverywhere
ツイートを翻訳

LIR HEAnet
@LIRHEAnet

"On the buses" from today a very visual message about @eduroam on Dublin Bus. Looks great! @HEAnet
ツイートを翻訳

HEAnet, Ireland: 160 locations + “eduroam on Dublin Buses” (Mar. 2021)

eduroamは……

ちょっと贅沢なキャンパス無線LANじゃないの？

いえいえ、もはや、

デジタル時代の教育・研究を支える社会のインフラ

です.

一般の公衆無線LANより安全で利便性が高い ☺

ところで、市民一般向けは？ 

公衆無線LANの動向: WiFi4EU

- EU全域に市民が利用できるフリーWi-Fiを整備
  - 公衆無線LANは、電気や水道のように、行政が提供すべきインフラ.
  - 自宅にネットワークを引けない層にも、ネットワークアクセス手段を提供.
  - 電子化された公共サービスへのアクセス手段.
    (デジタル時代の社会福祉)

> *"Everyone benefiting from connectivity means that it should not matter where you live or how much you earn. So we propose today to equip every European village and every city with free wireless internet access around the main centres of public life by 2020.*
> ***Jean-Claude Juncker - State of the Union speech, September 2016"***

OPENROAMING™
WIRELESS BROADBAND ALLIANCE

One Global Wi-Fi Network

VISION: Provide Automatic & Secure Wi-Fi Everywhere to Everyone

MISSION: Create an open framework for all types of players to develop their Wi-Fi services and business

OVERVIEW

WBA OpenRoaming™ creates the framework to connect billions of users and things to millions of Wi-Fi networks globally

WBA OpenRoaming™ is a roaming federation service enabling an automatic and secure Wi-Fi experience globally. With WBA OpenRoaming™, we are creating an open connectivity framework for all organizations in the wireless ecosystem to power new opportunities in the 5G era.

It encompasses three key elements:

https://wballiance.com/openroaming/

WBA OpenRoaming

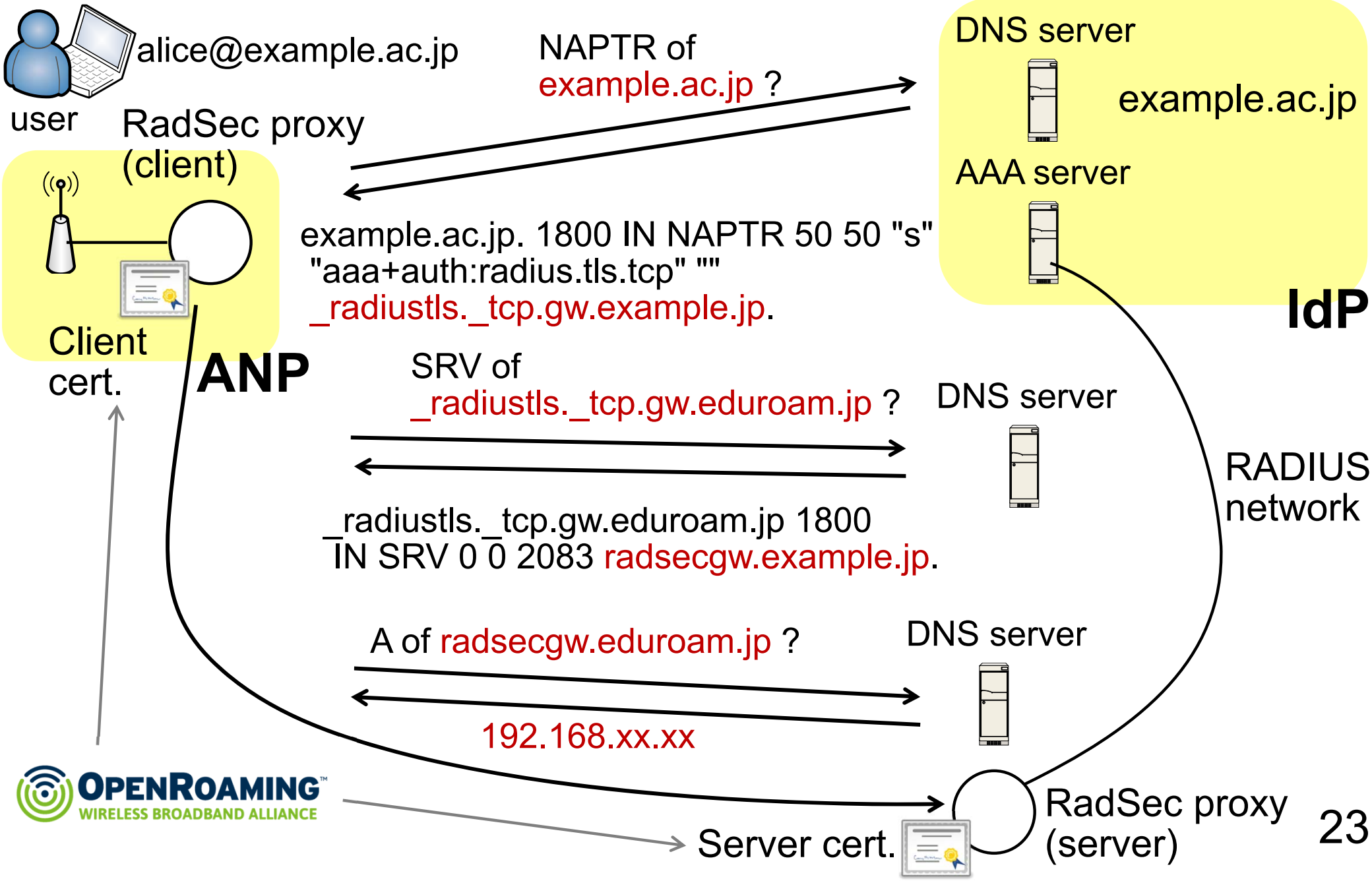
- 多数の携帯電話会社，ISP，ローミングフェデレーションなどを相互接続する，世界初のオープンなローミング基盤.
- 元は Cisco OpenRoaming (2019)
  WBAに移管済み (2020.3～)
- 2種類に大別されたモデルと、ポリシー別RCOI
  - Settled: 個別のローミングアグリーメントと仲介業者が必要
  - Settlement-free: 簡素なローミング契約. Free Wi-Fi向け.

OpenRoaming Standard

- OpenRoaming Release 1 (2020):
  - 基本的なアーキテクチャと運用方式，PKIなどを定義
  - Settlement-freeモデルが主
- OpenRoaming Release 2 (2021):
  - 課金システムとQoSに関連する仕様を定義
- OpenRoaming Release 3 (2022?):
  - 現在策定中
  - 課金システムの強化や信頼性向上などが含まれる見込み

OpenRoamingの認証連携
(RadSec + Dynamic Peer Discovery)

RFC 6614, RFC 7585



OPENROAMING™
WIRELESS BROADBAND ALLIANCE

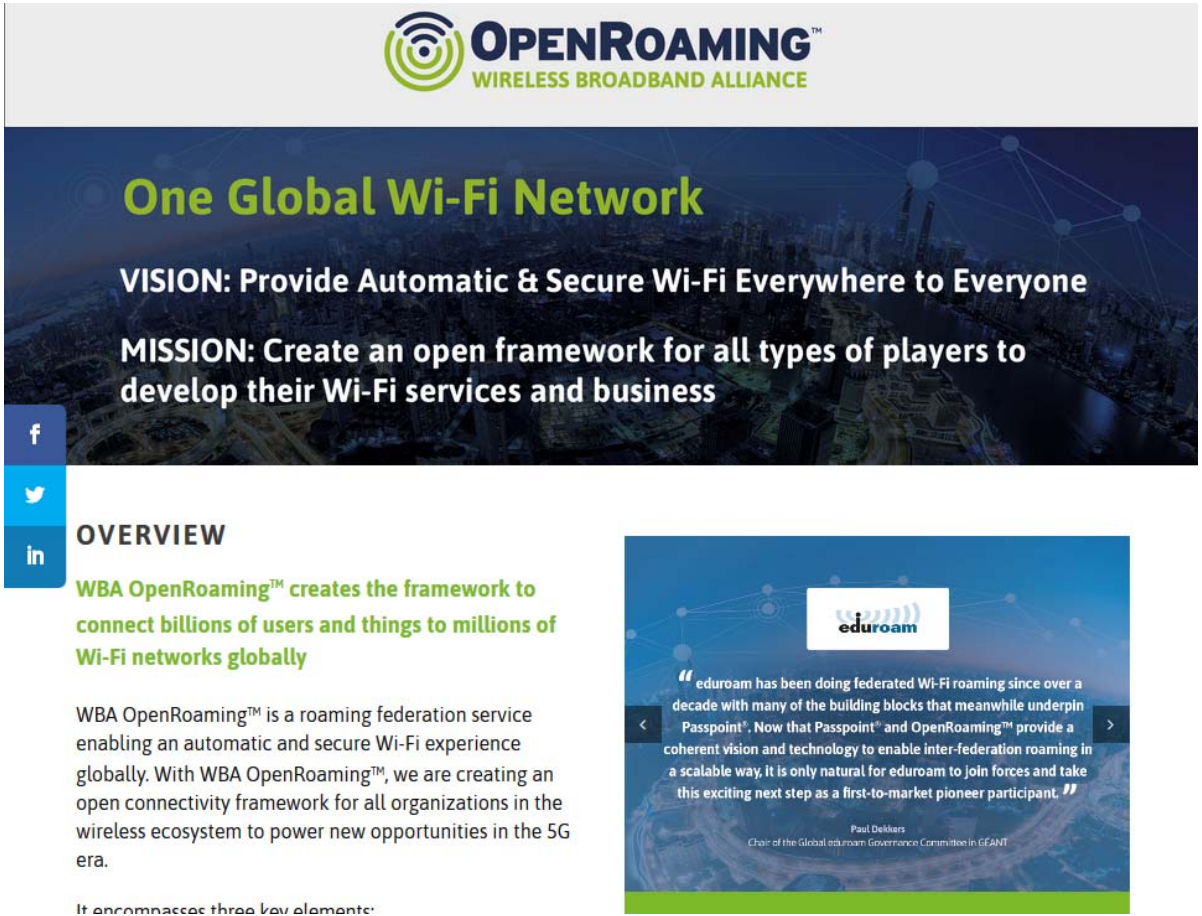
OpenRoamingのセキュリティとプライバシー保護

- IdP側での、利用者による明示的な同意を基本とする.
  - 基本的に，仕組み上，ANP側では個人識別できない.
  - 同意なしの行動解析や利用者追跡を不可能にする.
  - 不正利用時の利用者追跡は，ANPとIdPのログを突き合わせることにより実現.
- Baseline Policyにより，サイトごとの差異を減らす工夫
  - 行く先々でいちいち利用規約に同意させるのでは，ローミングのメリットが薄れるので，この負担を軽減.
  - ANP側に厳しい利用制限(AUP)などがあれば，明確に利用者に伝える必要がある (仕組みは開発中)
- IMSI Privacy Protection
  - SIM認証では，認証情報に加入者識別番号が平文で含まれるプライバシ問題があり，保護技術を並行して議論.

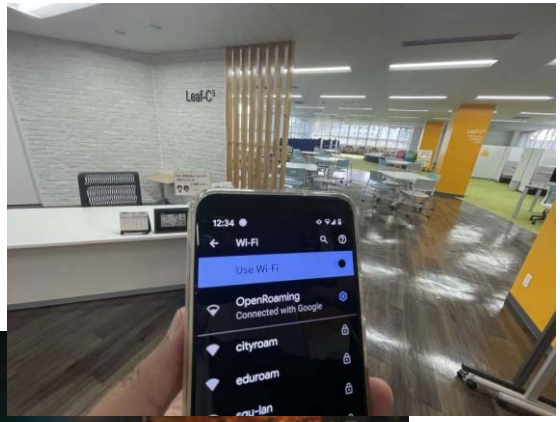
IMSI: International Mobile Subscription Identity

WBA OpenRoamingへの参加

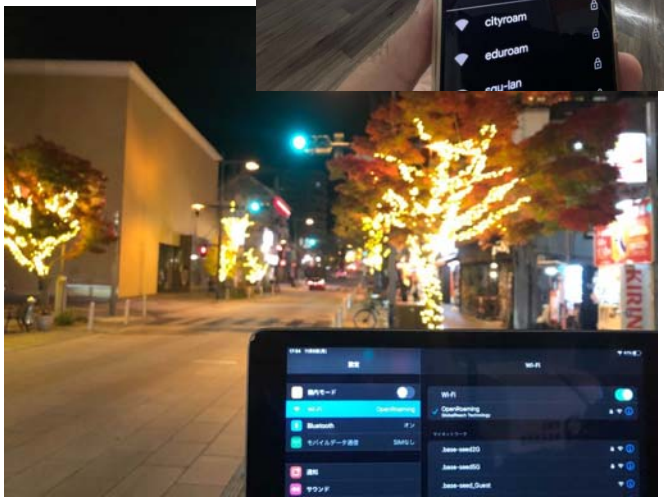
- eduroam (GÉANT)とCityroamが、OpenRoamingに初期メンバーとして参加.
  - eduroamとOpenRoamingの間でローミングを実現 (WBAと共同開発中)
  - OpenRoaming対応エリアでeduroamアカウントを利用可能に (Passpoint用プロファイルが必要、eduroam CATで対応済み)



札幌学院大

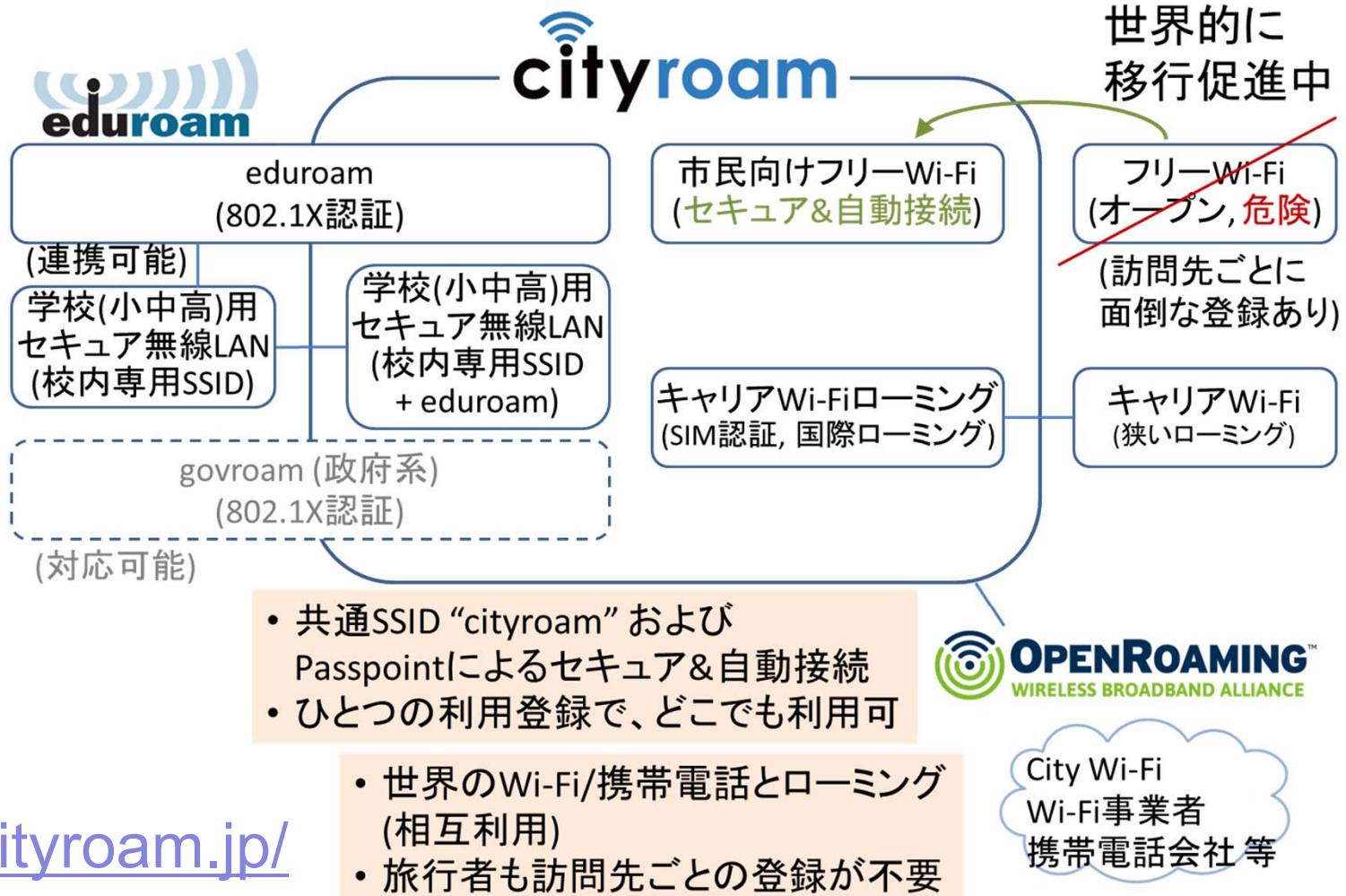


長野市



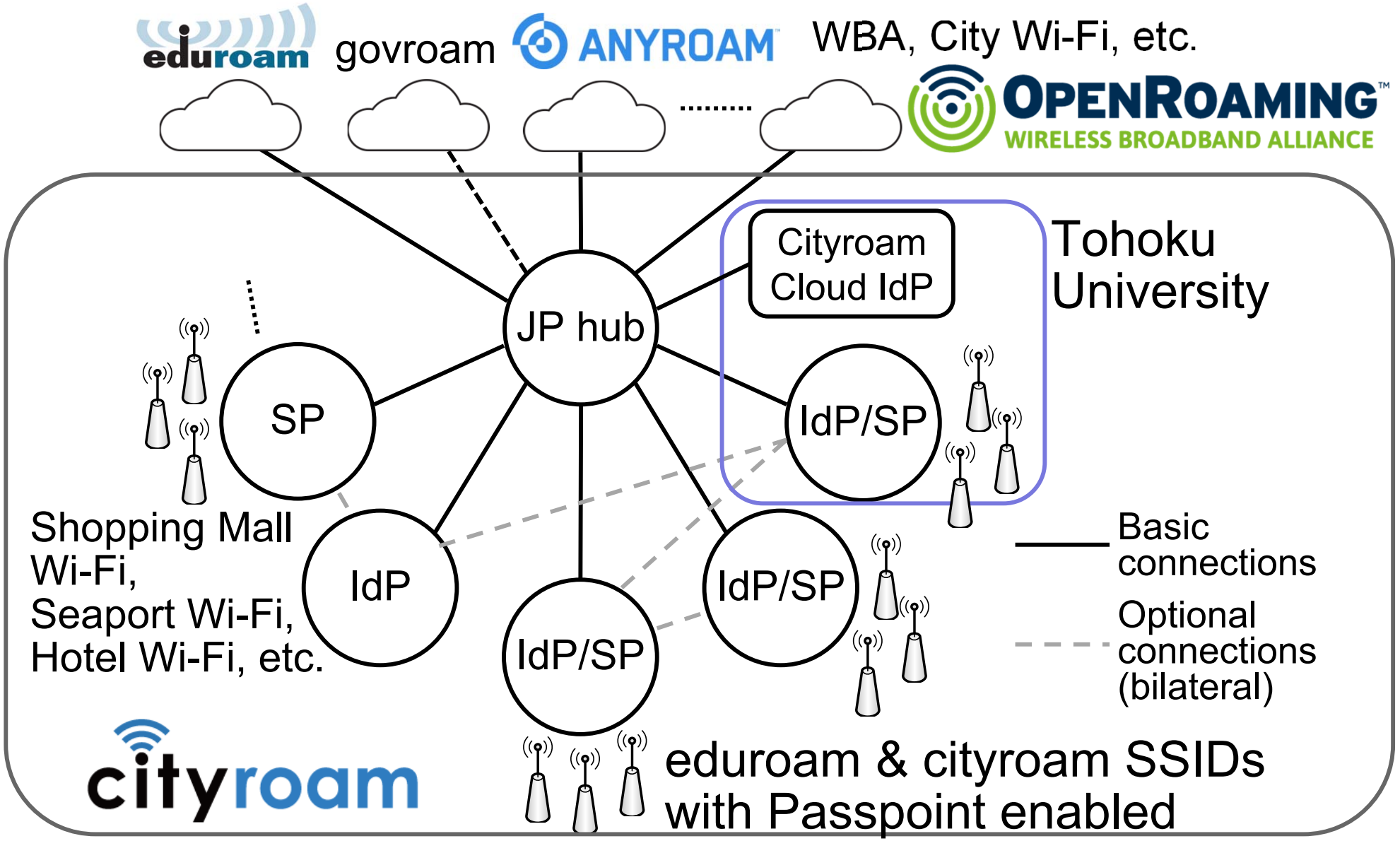
Cityroam：セキュア公衆無線LANローミング基盤

- 様々なローミングシステムを相互接続し、小さな自治体や通信事業者でも容易に参加できる、セキュア公衆無線LANシステム.
  - IdP: eduroam, ANYROAM, 携帯電話会社(SIM認証), プロバイダ 等
  - SP: フリーWi-Fi, 自治体Wi-Fi, 学校 等



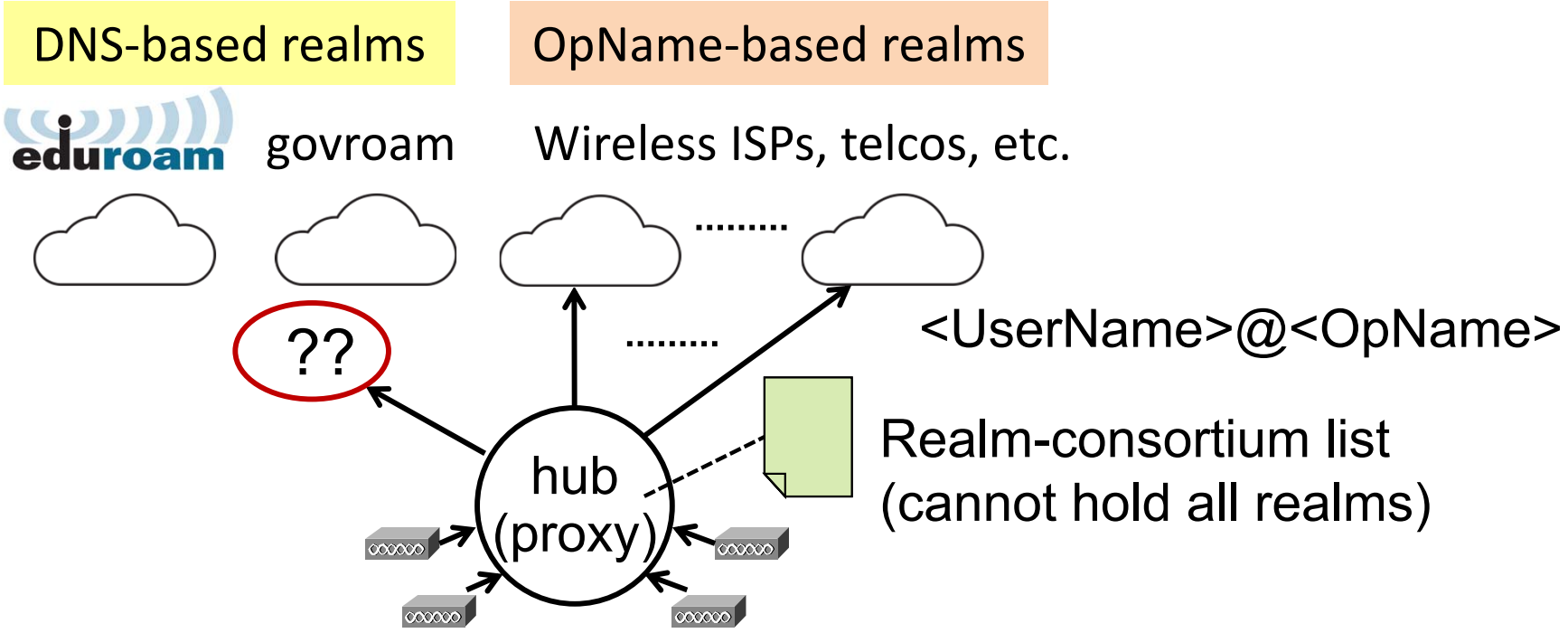
https://cityroam.jp/

セキュア公衆無線LANローミングテストベッド (2017.4-)



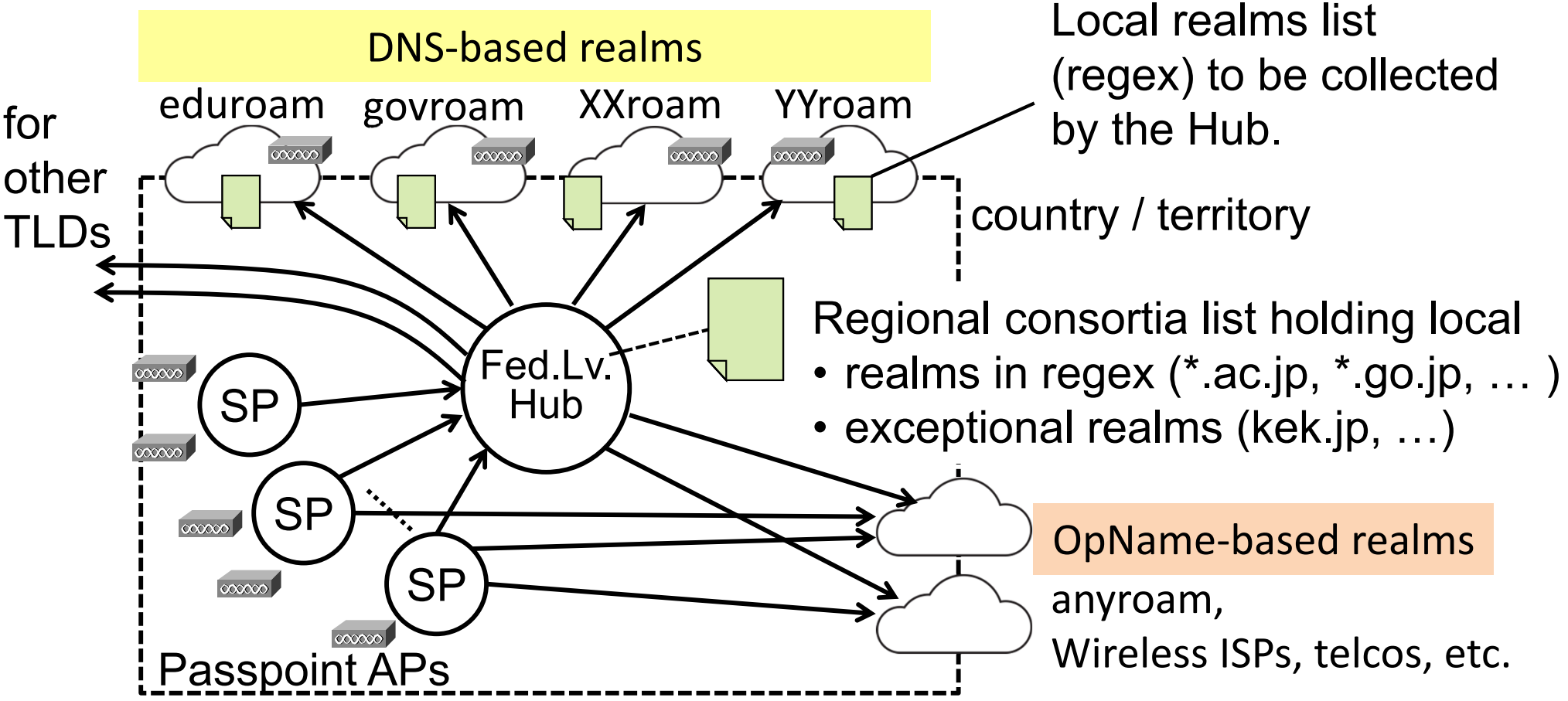
認証ルーティングのスケーラビリティ問題

- サービスプロバイダ(SP)が認証要求のレルムを見ただけでは、どの*Roaming Consortium*のアカウントか判別できない.
  - eduroam/govroam のレルム例:
    <UserName>@<InstName>.ac.ccTLD
    <UserName>@<InstName>.ccTLD
    <UserName>@<InstName>.gTLD



Inter-Federation スケーラブル認証ルーティング （2020）

- 各国・地域がHubを運用し，
  そのccTLDのレルムについて面倒を見る方式.



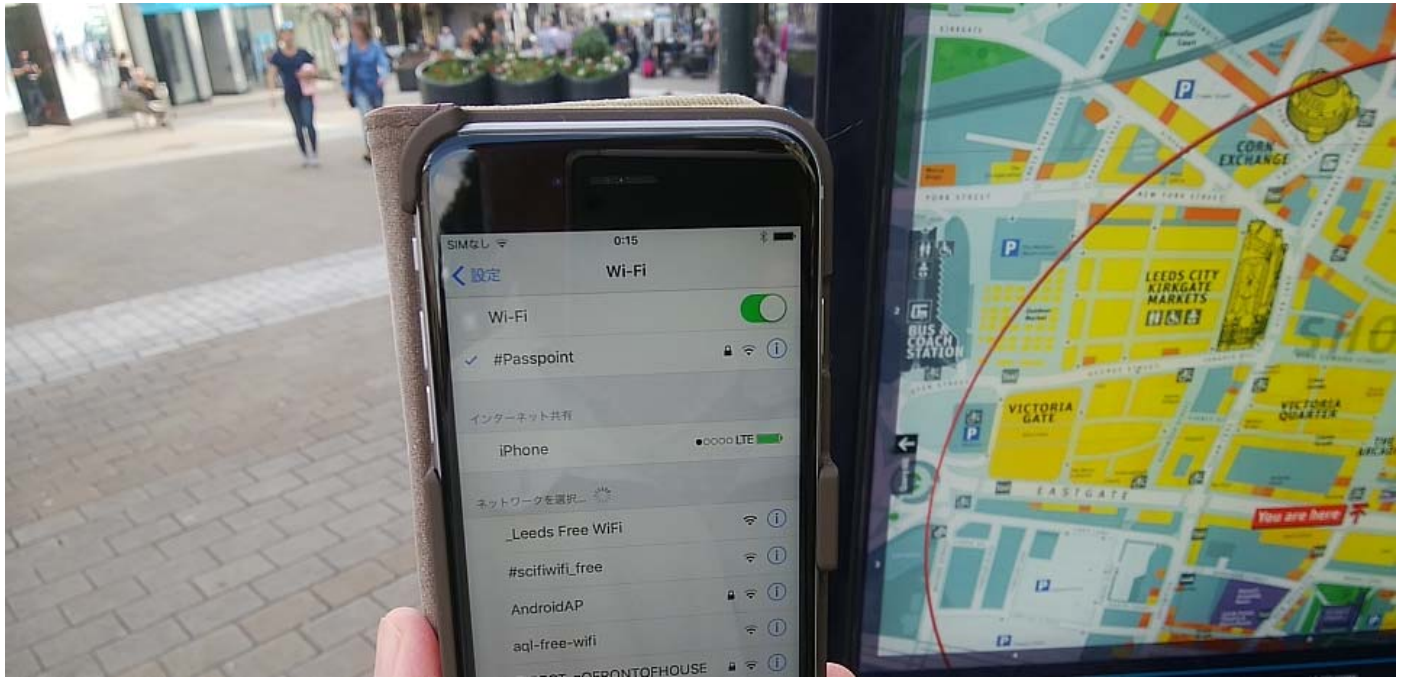
H. Goto, “Inter-federation Roaming Architecture for Large-scale Wireless LAN Roaming Systems,” JIP Vol.29, 2021.

eduroam on NGHの実証実験

- City Wi-FI Roamingトライアル 2017にて、
  市街地のNGHサービスにeduroamを乗せる実証実験
  - インターローミングの仕組みを開発し、NGH基盤に接続
  - ロシア ER Telecom からRADIUS認証テスト
  - UKのバーミンガム, リーズにて接続テスト

It works!

☺☺☺



Briggate Street, Leedsにおいて、
eduroamアカウントによる接続

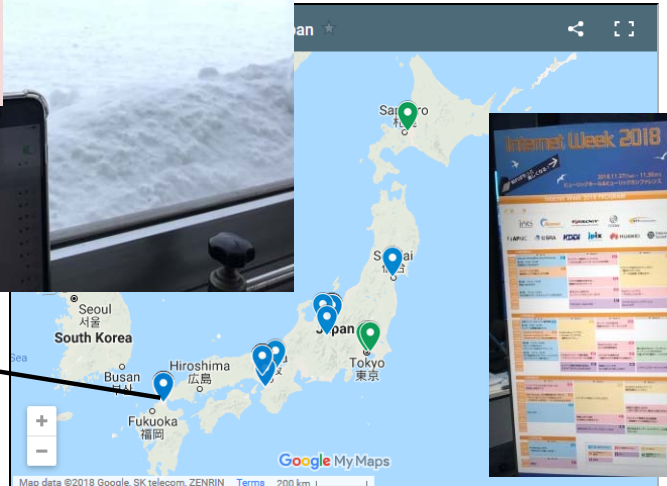
Cityroamのサービスエリア

- 現在、12市町村でCityroam APを提供中
  - カフェ, ホテル, ショッピングモール 等
  - 札幌学院大学 (市民サービスの充実, 地域連携)
  - スキーリゾート (Hakuba47)
  - 北九州モノレール全駅
  - 会議場における一時的なサービス提供
    Internet Week 2018, 2019, AXIES 2018,
    コミックマーケット95-97

新しい方向性:
学校・大学も
公衆無線LAN提供

可搬型 eduroam
/Cityroam基地局

Cityroamを利用すると、eduroamと
公衆無線LANを融合したサービスを、
迅速に提供できる.



Cityroamのサービスエリア

- ホテル，ホール，コワーキングスペースなど，多様なサイトに展開中

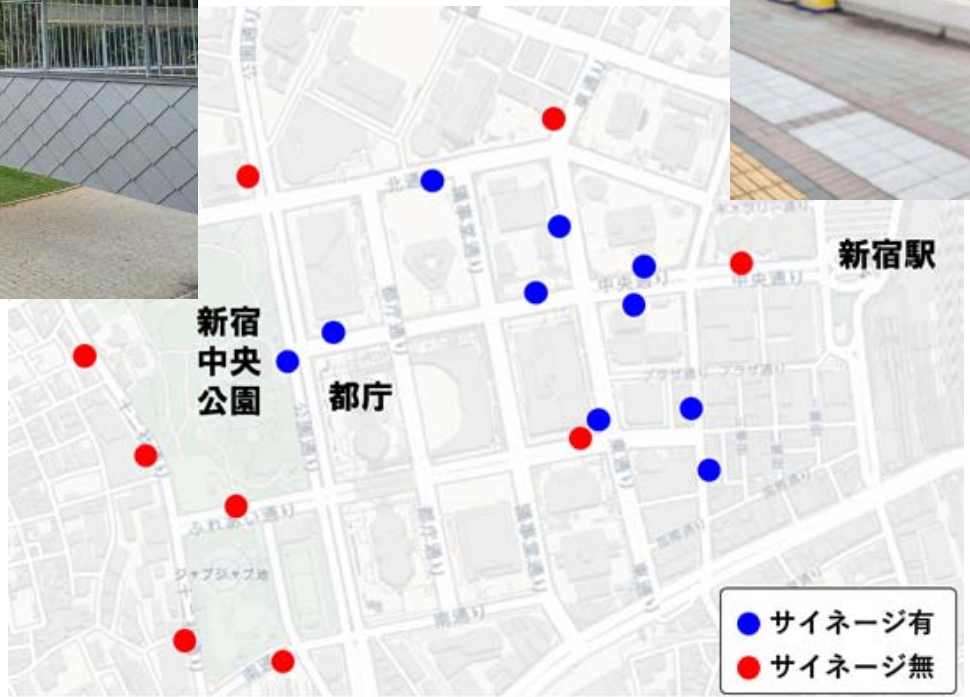
コワーキングスペースもりおか
(2020年 OpenRoaming追加)

勤労者女性会館しなのき (長野)
(2021/5)

温泉宿　うるおい館 (長野)
(2021/5)

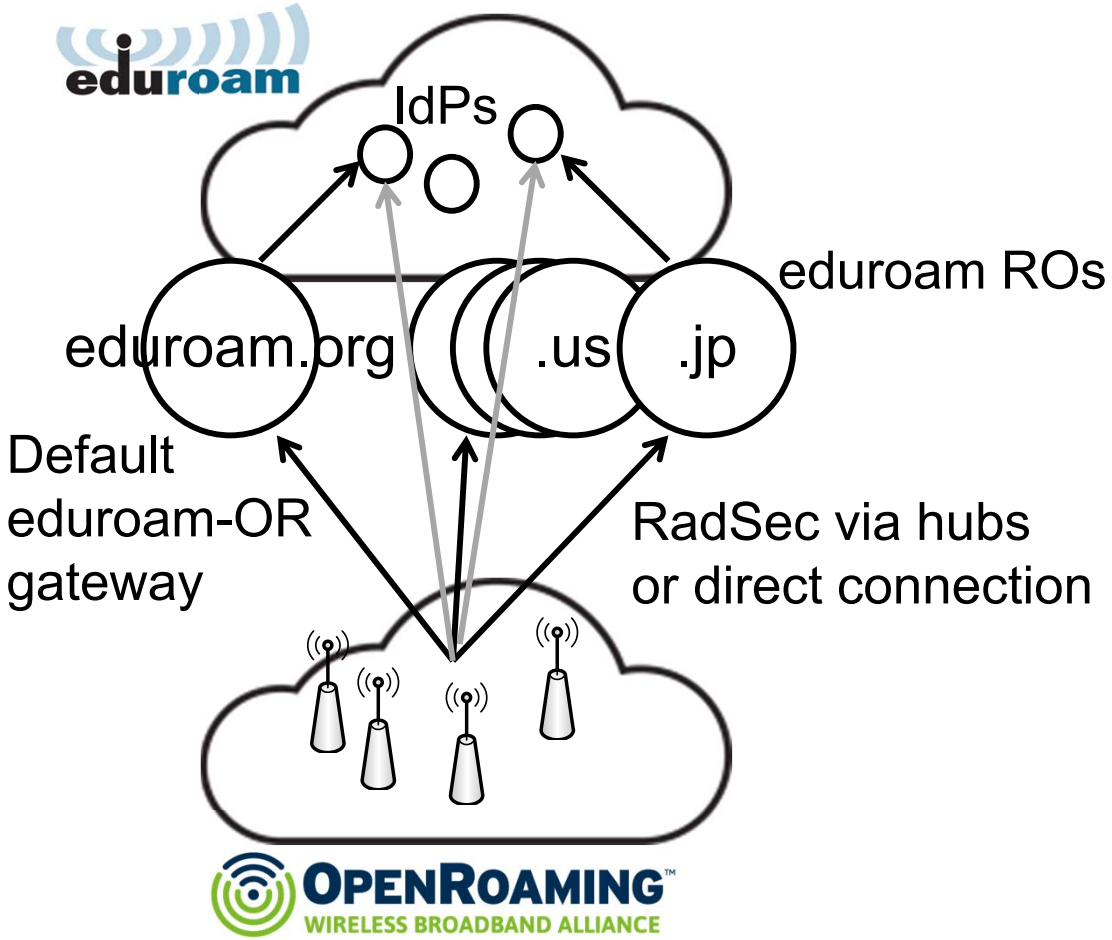
Cityroamのサービスエリア

- 東京都による西新宿スマートポール 令和3年度事業
  - PoC, Smart City
  - eduroam, Cityroam, OpenRoaming が利用可能に.
    (2か所で先行導入済み)

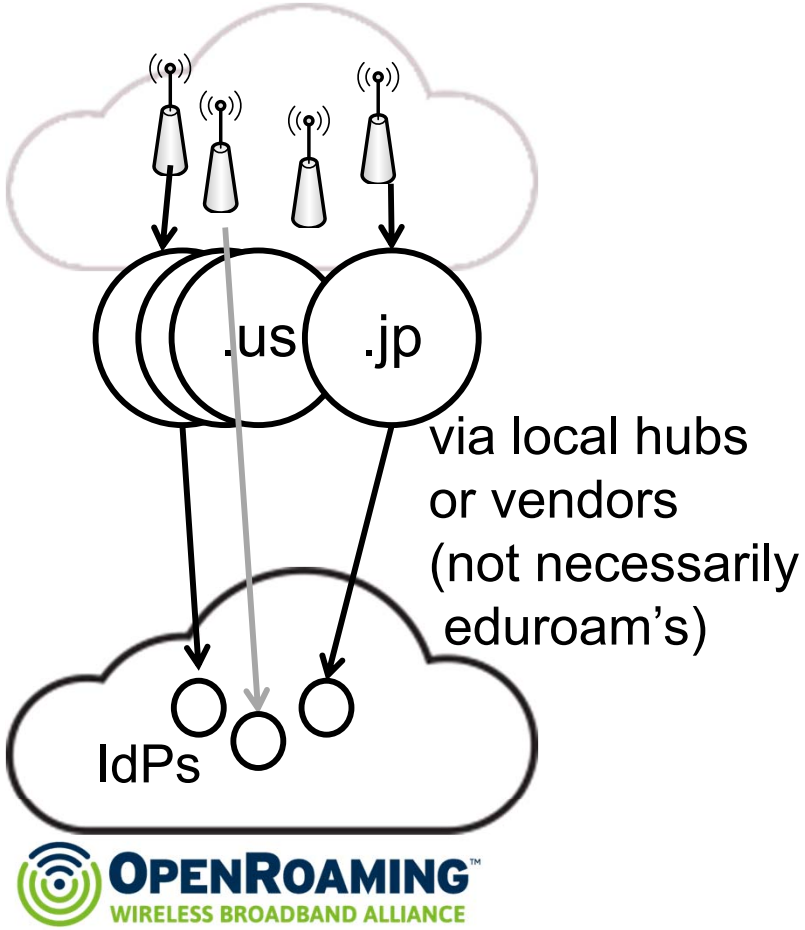


eduroam – OpenRoaming 連携技術・運用方式の開発

eduroam via OpenRoaming ANPs



Universities providing OpenRoaming service for visitors and residents.)



問題点: NAPTRを追加した機関しか利用できない
(既存eduroamのような一枚岩ではない)

ANP: Access Network Provider

まとめ

- 公衆無線LANのセキュリティ対策と利便性向上が急務.
- 学術系のeduroamは，off-campus eduroamが普及
  - デジタル時代の教育・研究を支えるインフラ
- OpenRoaming
  - 安全で利便性の高い公衆無線LANを実現
  - 不正利用時の責任所在を明確化
  - 利用者中心のプライバシ保護・制御
- セキュア公衆無線LANローミング基盤 Cityroam
  - フリーWi-Fiの容易なセキュア化とローミング対応を実現
  - 国内でOpenRoamingに乗るなら簡便・最速

課題

- SIM認証の普及と、認証ルーティングの改善
- Cityroam / OpenRoamingの普及