

CKP夏の研究会 2023 (青森市男女共同参画プラザ)  
2023年7月10日

# セキュア公衆無線LANローミング基盤 Cityroam/OpenRoamingの技術と導入について

後藤英昭 東北大学・サイバーサイエンスセンター



本活動の一部は国立研究開発法人情報通信研究機構  
(NICT)の委託研究プログラムの支援を受けています。

セキュア無線LANローミング  
eduroamからCityroam, OpenRoamingへ

OpenRoamingの技術

公衆無線LANのセキュリティとプライバシー保護

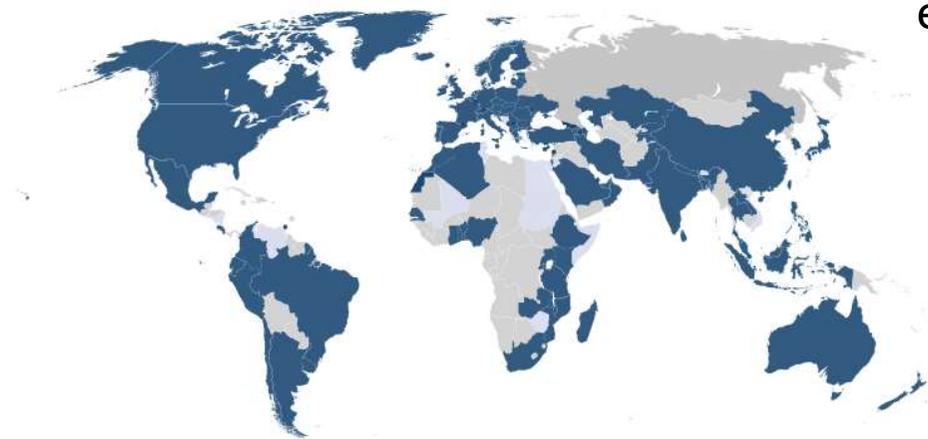
変化する公衆無線LANと、Cityroamの展開

# 国際学術無線LANローミング基盤「eduroam」 (RFC 7593)

## ■ 教育・研究用の学術無線LAN (Wi-Fi)ローミング基盤

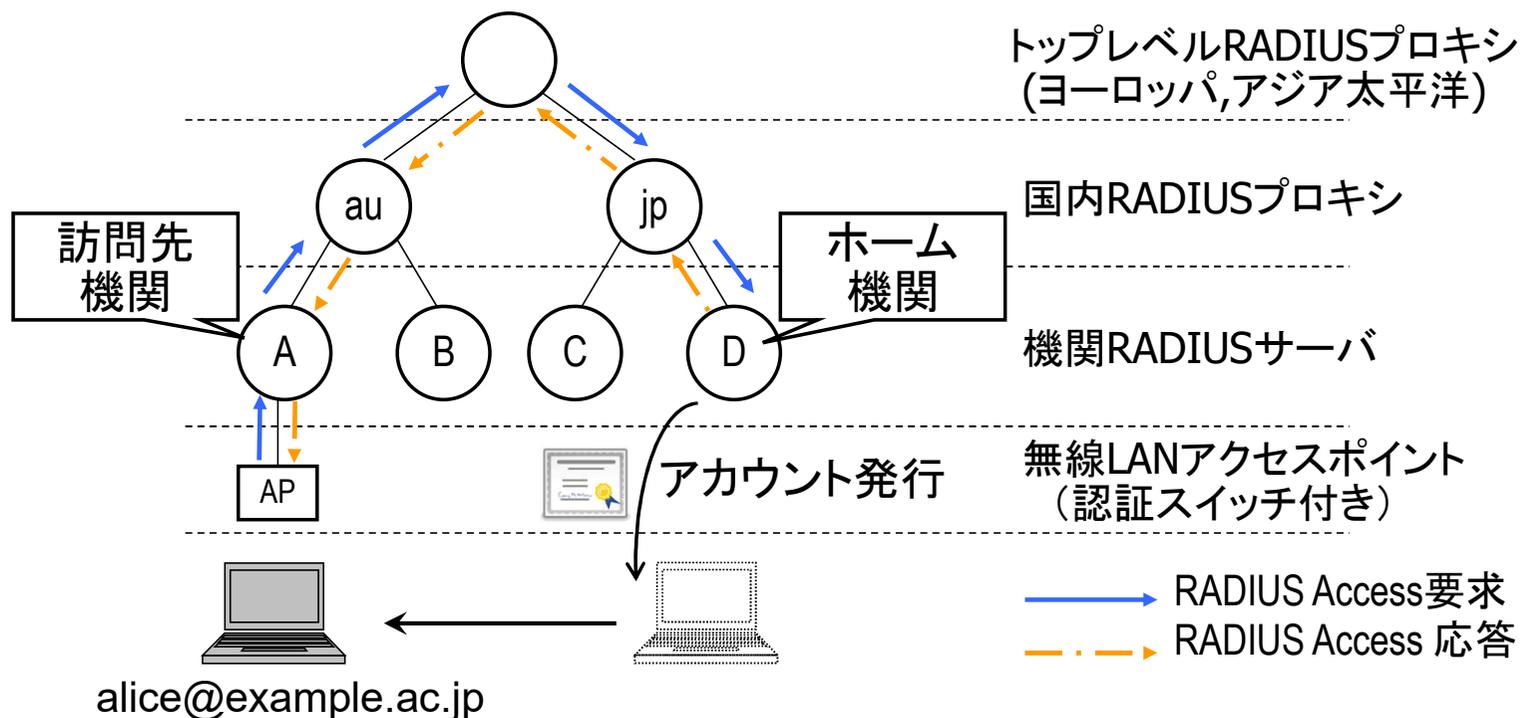
- 欧州TERENA (現GÉANT) で開発 (2003～)
- キャンパス無線のデファクト・スタンダード
- 世界中の参加機関で、無線LANが無料、安全、自動接続で利用可能
  - 互恵の精神に基づくサービス
- 802.1X方式による安全なユーザ認証
- 認証VLANによるアクセス制御&ポリシー適用も可能

eduroam Companion (Android, iOS)



# ローミングの基本: eduroamのしくみ

- IEEE 802.1x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)

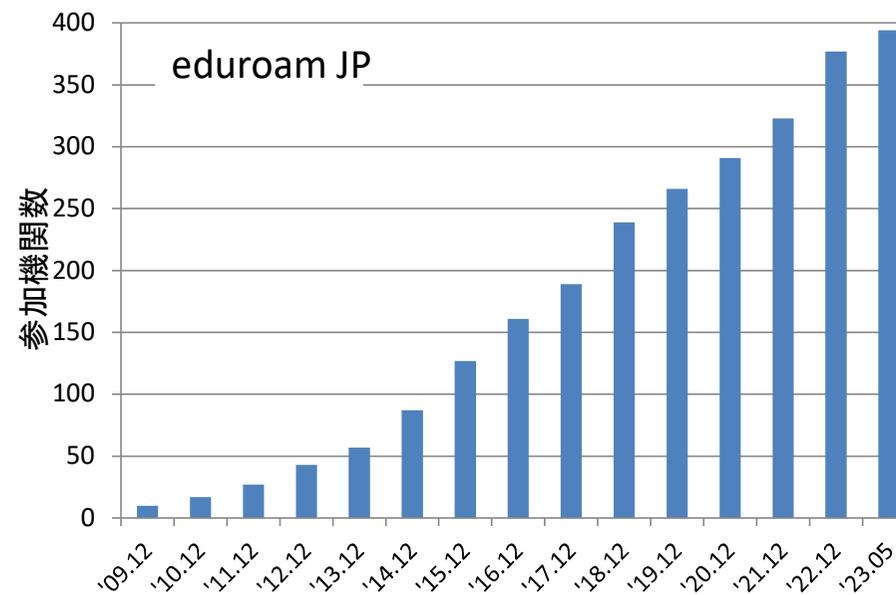


# eduroam JP

- 2006年8月 日本導入 (国立情報学研究所(NII)が運用)
- 2023年7月現在 国内396機関 (国立大学は92%)

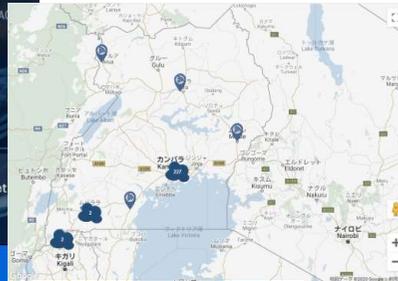


初等・中等教育機関にも導入開始  
(2016～)



# 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.



“Extended virtual campuses”  
in Ireland (Jan. 2021)

<http://www.universitytimes.ie/2021/01/heanet-to-extend-wifi-initiative-for-students-to-90-new-locations/>

教育における  
IT環境整備の重要性

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/connection](https://heanet.ie/services/connection)...  
#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)

# Off-campus eduroam as digital infrastructure

Jisc News > Call for local authorities to support students with free wifi in public ...

News

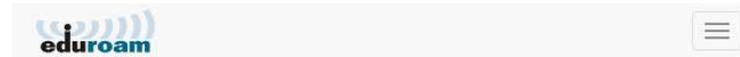
## Call for local authorities to support students with free wifi in public spaces

19 May 2021

Building on efforts to tackle digital poverty, Jisc has written to the Local Government Association, urging authorities to provide free internet access to students in public spaces via our eduroam connectivity service.



Jisc, UK (May, 2021)



## eduroam in Libraries, transport hubs, hospitals, and beyond.

The original eduroam use case was for a researcher at one institution to easily be able to collaborate with researchers at another institution without having to jump through bureaucratic hoops to get Internet access. This is relevant in South Africa too, because we have a great deal of inter-institution collaboration, but a more important use-case, when you bring eduroam to Africa, is the potential it has to play in bridging the digital divide.



TENET, South Africa (July, 2021)

## 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)

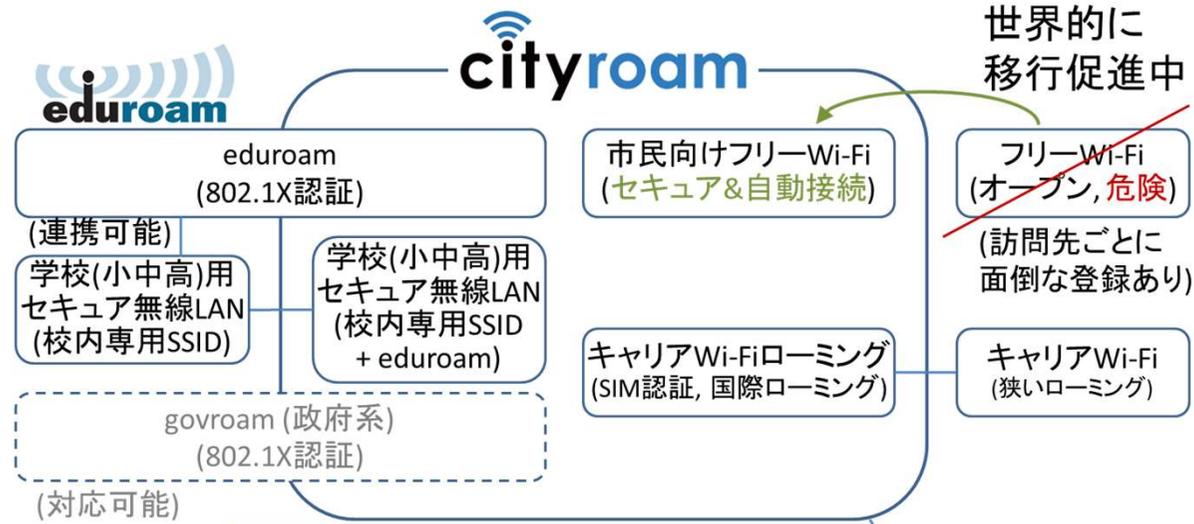
*“Everyone benefiting from connectivity means that it should not matter where you live or how much you earn. So we propose today to equip every European village and every city with free wireless internet access around the main centres of public life by 2020.*

**Jean-Claude Juncker - State of the Union speech, September 2016”**

# Cityroam : セキュア公衆無線LANローミング基盤 (2018~)

- 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
- ANP: フリーWi-Fi, 自治体Wi-Fi, 学校 等



市民も使える  
セキュアな  
公衆無線LAN

- 共通SSID “cityroam” および Passpointによるセキュア&自動接続
- ひとつの利用登録で、どこでも利用可

- 世界のWi-Fi/携帯電話とローミング (相互利用)
- 旅行者も訪問先ごとの登録が不要



City Wi-Fi  
Wi-Fi事業者  
携帯電話会社 等

<https://cityroam.jp/>

## Cityroamのサービスエリア

- 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, 2021, 2022,  
コミックマーケット95-97, 99-101

新しい方向性:  
学校・大学も  
公衆無線LAN提供

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。

可搬型 eduroam  
/Cityroam基地局



# 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)



旅館こうろ (京都)  
(2017/8 eduroam導入時より)



京都市10公園内自販機  
(2020/5)



温泉宿 うるおい館 (長野)  
(2021/5)

# WBA OpenRoaming

<https://wballiance.com/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.**



- Canary Wharf, London
- Lake Geneva
- Barcelona, Valencia, etc.
- **京都, 長野, ほかに国内各地 (Cityroam)**
- São Paulo Airport (GRU)
- Dublin
- Azores, ...

# 新 TOKYO FREE Wi-Fi

- 4か所からスタート (2023/4時点)
- 令和5年度中に600か所以上に拡大予定



<https://wi-fi.metro.tokyo.lg.jp/>



都庁第二本庁舎3階

Wi-Fi6 eduroam



東京観光情報センター (ハスタ新宿)

Wi-Fi6E eduroam



新宿都税事務所 (本館4F、本館6F)

Wi-Fi6 eduroam



東京都立大久保病院 (3F外来待合エリア) \*実証実験中

Wi-Fi6 eduroam

西新宿スマートポール 22基  
(2021-2022導入)



+

セキュア無線LANローミング

eduroamからCityroam, OpenRoamingへ

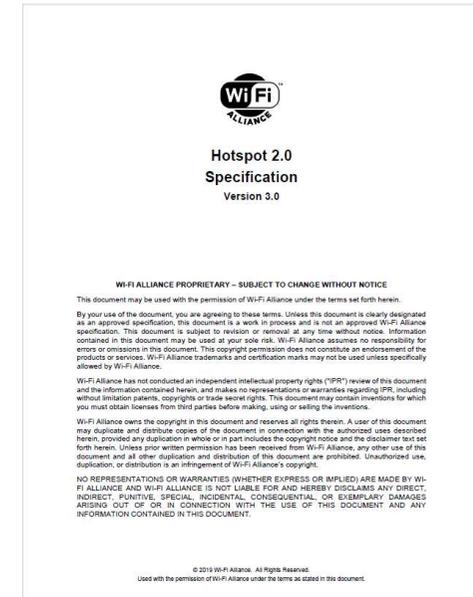
**OpenRoamingの技術**

公衆無線LANのセキュリティとプライバシー保護

変化する公衆無線LANと、Cityroamの展開

# OpenRoamingの基盤技術・仕様

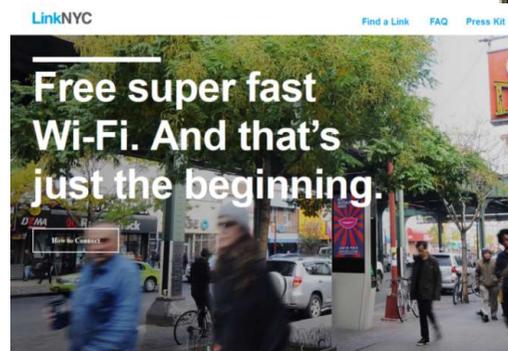
- WPA2/3 Enterprise (IEEE 802.1X)
- **Wi-Fi CERTIFIED Passpoint**
  - 携帯電話並みの利便性を提供
  - 自分のサービス契約に合致する基地局に自動接続
  - SSID自動選択後は1X認証と同等で、安全な接続 (偽基地局への誘導を回避可能)
- WBA WRIX (Wireless Roaming Intermediary eXchange) Standard
  - 次世代ホットスポット / Next Generation Hotspot (NGH) コンセプト
  - ローミング方式の国際標準
- WBA OpenRoaming Standard
  - RadSec + Dynamic Peer Discovery (DPD), PKI, 他



## Passpointの黎明期

- 幾つかの事業者がセキュアWi-Fiを提供開始:
  - San Francisco & San Jose Wi-Fi (2014)
  - Orange Romania (2014)
  - LinkNYC (2016), InLinkUK (2017)
  - Boingo Passpoint Secure at 40+ airports in US, Brazil, Portugal, UK, ...
  - 北米キャリア(複数)がPasspointによるオフローディング機能を端末にプリインストール

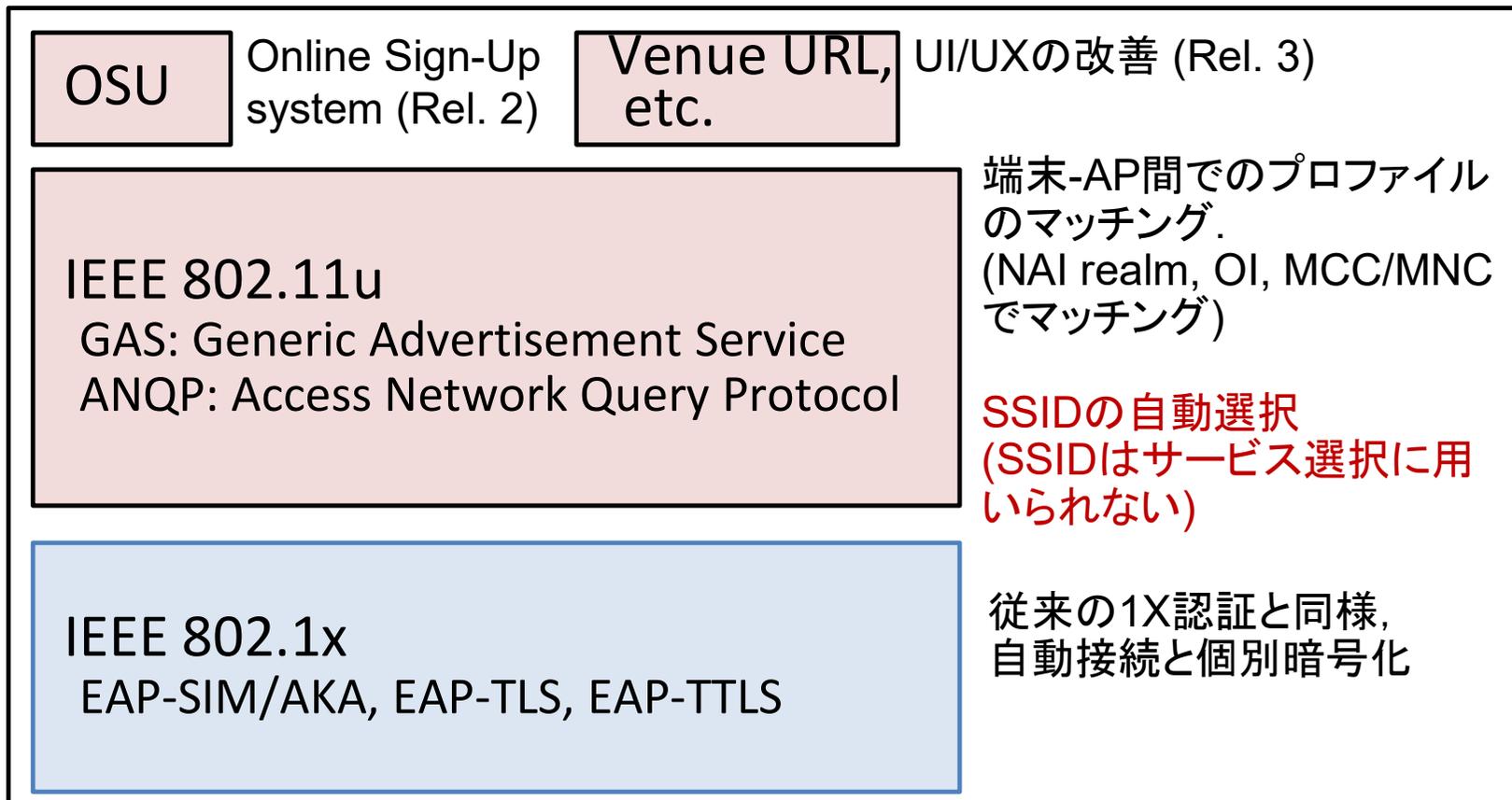
Wi-Fi Alliance と  
Wireless Broadband Alliance  
(WBA) が Passpoint/NGH を  
共同推進.



Look!



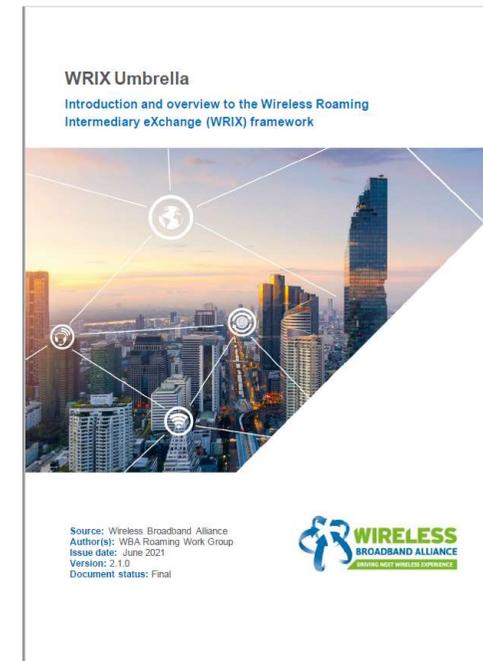
# Passpointの仕組み



# WBA WRIX Standard (Wireless Roaming Intermediary eXchange)

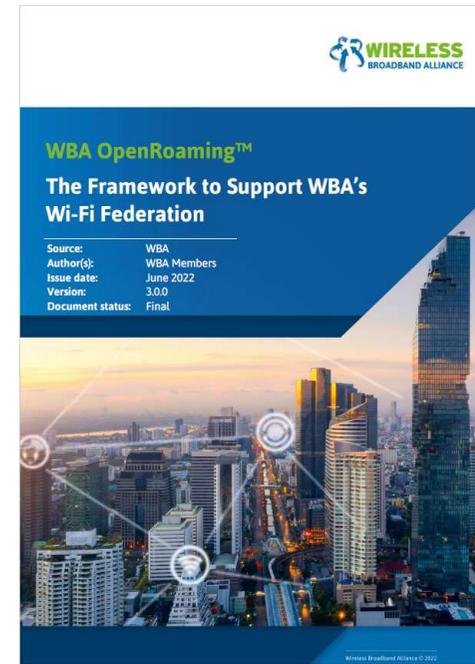
## ローミング認証連携のための仕様

- WRIX-i (Interconnect)
- WRIX-n (Network)
  - 実体はRADIUSの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)



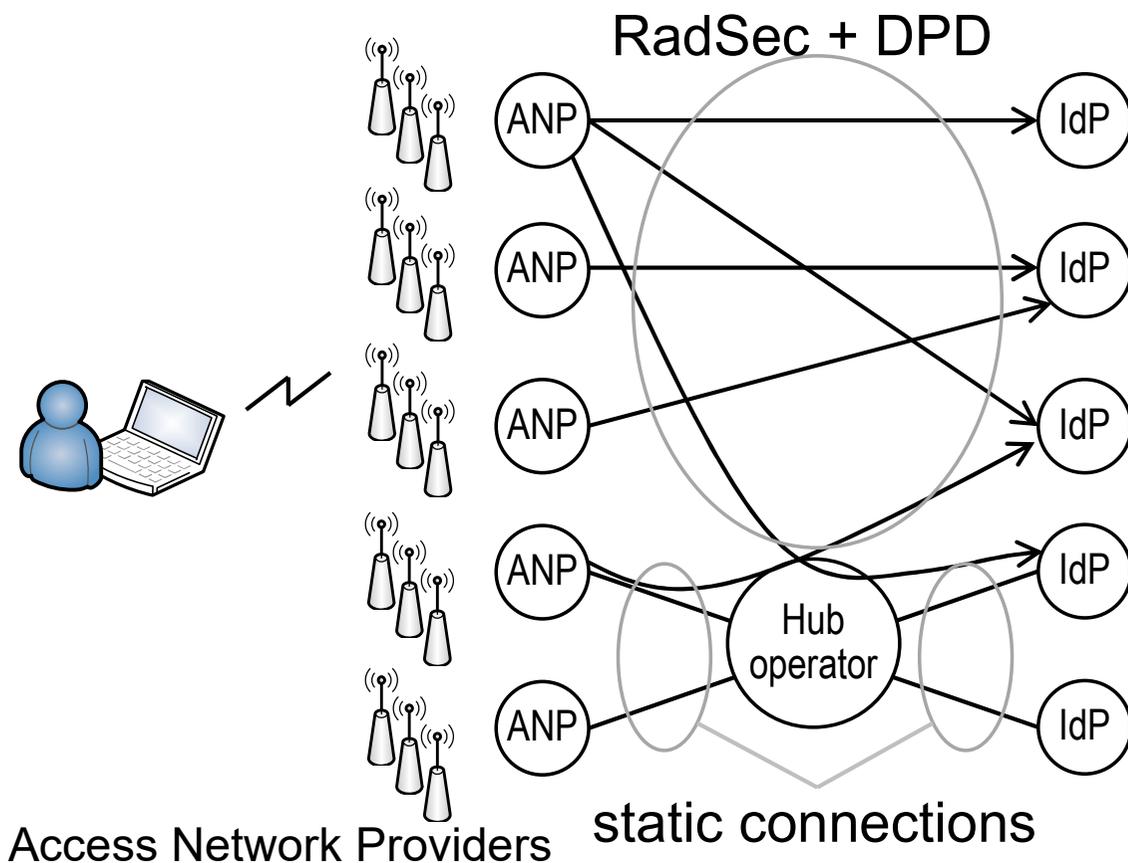
# OpenRoaming Standard

- OpenRoaming Version 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 Version 2 (2021):
  - 課金システムとQoSに関連する仕様を定義
- OpenRoaming Version 3 (2022):
  - 課金システムの強化や信頼性向上など



# OpenRoamingのアーキテクチャ

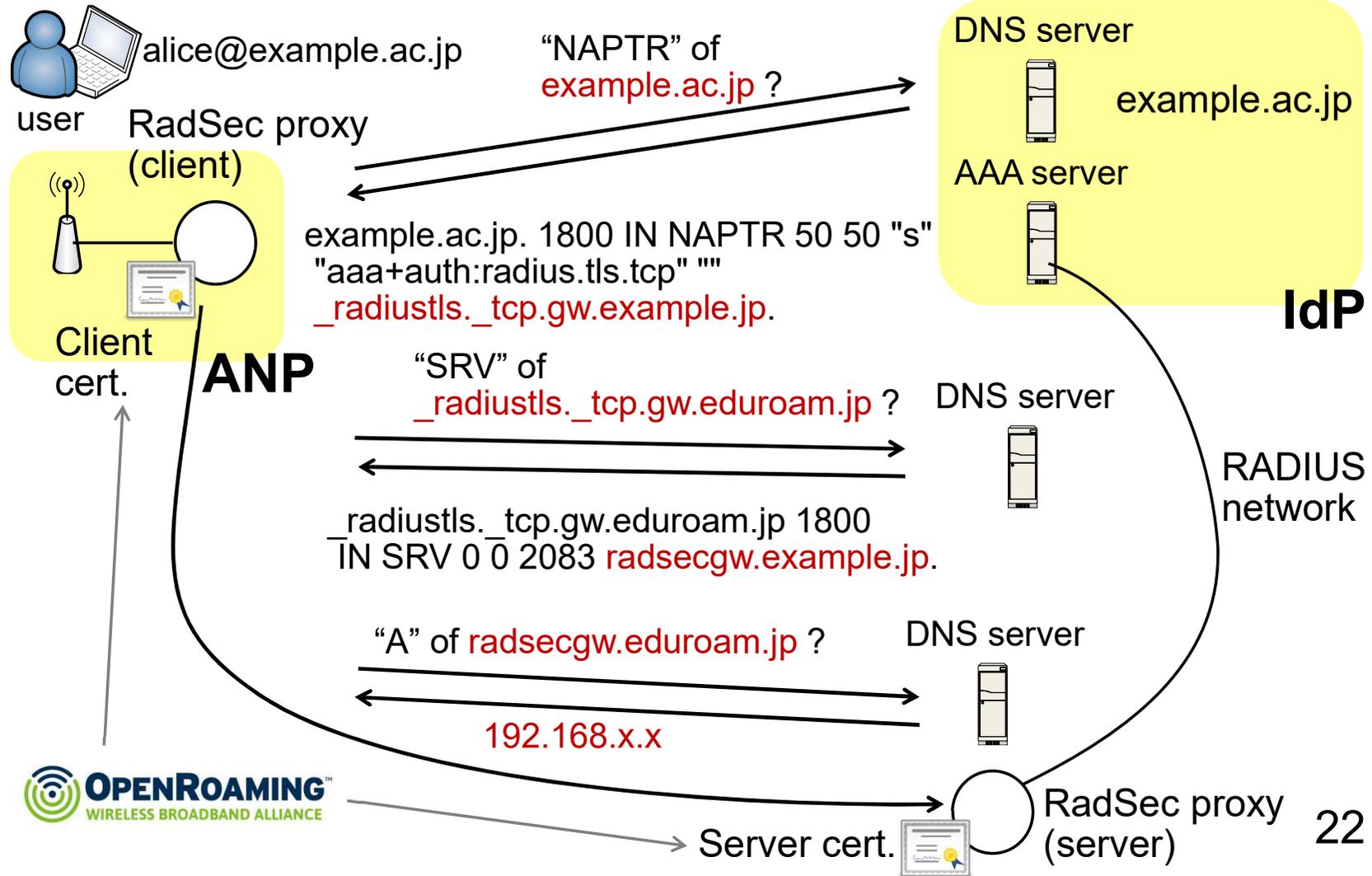
- RadSec + Dynamic Peer Discovery (DPD)を用いたP2P接続が基本
- RadSec end-pointには、WBAIDと、TLS用電子証明書が必要.
- 課金が絡む場合などは、ハブ事業者が仲介.



# OpenRoamingの認証連携

(RadSec + Dynamic Peer Discovery)

RFC 6614, RFC 7585



構築は面倒くさいですか？



Cityroam経由なら、簡単です！

- ✓ WBAとのやり取りはおまかせ
- ✓ RADIUS接続 (従来の802.1X)
- ✓ Passpoint設定の追加 (基地局)
- ✓ マップデータなどの提出

ベンダや他事業者のソリューションに乗ってもOK！

- ✓ 教育研究サポートのために、ぜひeduroamの併設を！

セキュア無線LANローミング

eduroamからCityroam, OpenRoamingへ

OpenRoamingの技術

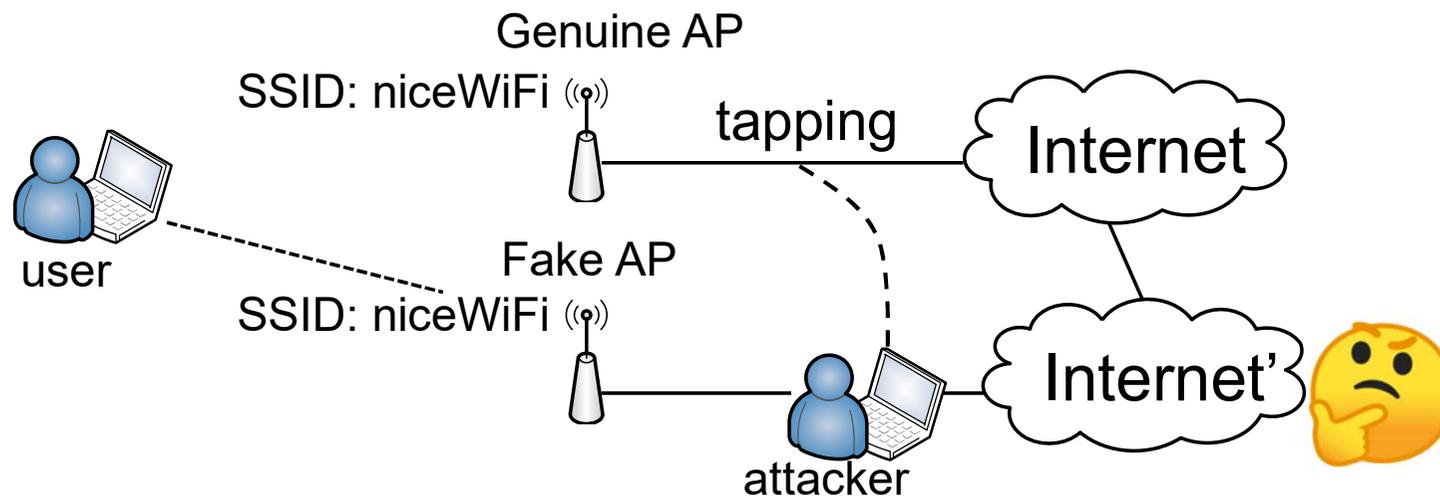
**公衆無線LANのセキュリティとプライバシー保護**

変化する公衆無線LANと、Cityroamの展開

# 公衆無線LANのセキュリティ

## ■ 中間者攻撃(MITM)と偽基地局の問題

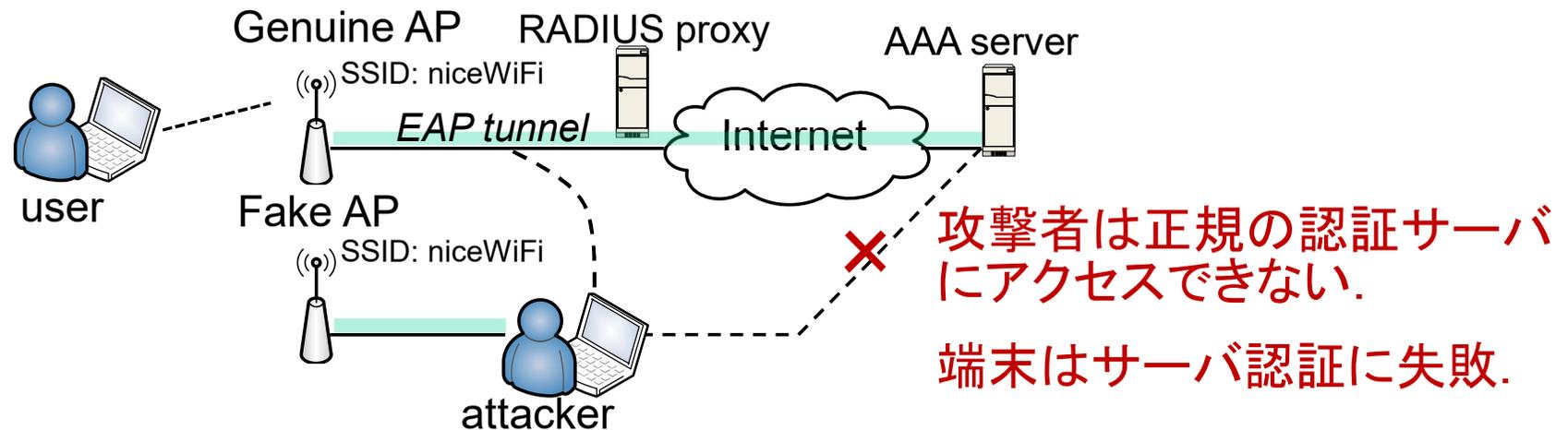
- オープンやWPA2-PSKでは, SSIDと鍵さえ合っていれば、  
偽の基地局でも自動で繋がり、危険！  
(MITM攻撃, 盗聴, マルウェア挿入, 基地局からの能動攻撃など)
- 正しい基地局でも、  
マルウェア埋め込みや、ケーブルにいたずら などがある。



偽基地局の向こうは  
偽サーバだらけの  
偽物のインターネット

## WPA2/3 Enterpriseで安全な公衆無線LANに

- 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 (Enterprise) なら「サーバ証明書の検証」で対策可
- EAP (Extensible Authentication Protocol)の仕組みによって、パスワードの保護が可能.

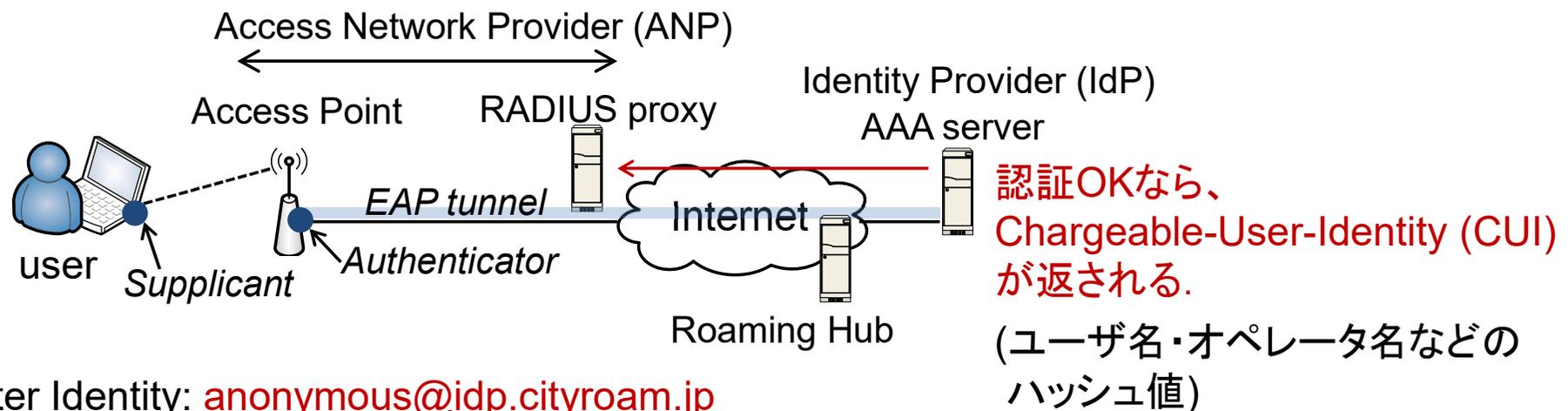


## もう一つのセキュリティ面

- 公衆無線LAN事業者にとってのセキュリティ
  - 利用者による不正利用の際、事業者が責任を問われないことが重要.
  - 利用者の身元の紐づけと、追跡手段の確保.
  
- 社会にとってのセキュリティ
  - 詐欺等の犯罪の抑制.
  - 反社・テロ活動の抑制.
  - 市民の行動解析による防災、減災.
  - 大規模災害時におけるコミュニケーション手段の確保.

# OpenRoamingにおけるプライバシー保護

- IdP側での、利用者による明示的な同意を基本とする。
  - ANPや中間proxyに見えるのは、仮名ID (Pseudonymous ID) まで.
  - 同意なしの行動解析や利用者追跡を不可能にする.
  - 行動解析・利用者追跡は, ANPとIdPのログを突き合わせる.  
(ユーザ名、タイムスタンプ、MACアドレス、CUIなど)



Outer Identity: **anonymous@idp.cityroam.jp**  
(トンネルの外側 – ANPにも見える)

Inner Identity : **alice@idp.cityroam.jp**  
(トンネルの内側 – 端末とIdPにしか見えない)

## OpenRoamingにおけるプライバシー保護

- 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. 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ー問題があり, 保護のための技術仕様が策定された.

例: 1440109999999999@wlan.mnc<MNC>.mcc<MCC>.3gppnetwork.org

セキュア無線LANローミング

eduroamからCityroam, OpenRoamingへ

OpenRoamingの技術

公衆無線LANのセキュリティとプライバシー保護

変化する公衆無線LANと、Cityroamの展開

# 変化する公衆無線LAN

## COVID-19前

- 観光&インバウンド目当てが主流
- 補助金プログラム多数
- どこにでもフリーWi-Fi設置
- あちこちにキャリアWi-Fi
- 自治体Wi-Fiの導入が盛ん
- ~ Wi-Fi 5 (11ac)
- 使いにくい
- セキュリティがヤバい！
- 学術系は eduroam で解決  
(でも一般向けが無いじゃない！)



## COVID-19禍中

- 観光&インバウンド需要の急減
- 補助金の大幅縮小
- 更新できない or 低利用率で撤去
- 5Gで頑張るから終息 🙄
- 継続性に課題
- Wi-Fi 6 / 6E (でもモノが来ない.....)
- 使いにくい
- セキュリティがヤバい！
- やっと、やっと、国際ローミング開始  
(まだ始まったばかり)



# 公衆無線LANの将来像は？

## COVID-19禍中

- 観光&インバウンド需要の急減
- 補助金の大幅縮小
- 更新できない or 低利用率で撤去
- 5Gで頑張るから終息 🤖
- 継続性に課題
- Wi-Fi 6 / 6E (でもモノが来ない.....)
- 使いにくい
- セキュリティがヤバい！
- やっと、やっと、国際ローミング開始 (まだ始まったばかり)



## 現在～近い将来

- デジタルサービス&住民利用が主軸
- 補助金への依存軽減
- 設置場所の適性を重視
- 5G/6G + Wi-Fi コンバージェンス
- 自治体Wi-Fiも継続性重視
- Wi-Fi 6 / 6E / 7による効率化
- ローミングで利便性向上
- 気軽に得られるセキュリティ
- 国際ローミングによる新サービス、新ビジネス開拓

# ローミング基盤で対応できること

- デジタルサービス&住民利用が主軸
- 補助金への依存軽減
- 設置場所の適性を重視
- 5G/6G + Wi-Fi コンバージェンス
- 自治体Wi-Fiも継続性重視
- Wi-Fi 6 / 6E / 7による効率化
- ローミングで利便性向上
- 気軽に得られるセキュリティ
- 国際ローミングによる新サービス、新ビジネス開拓

別途→

別途→

開発中

開発中

cityroam

eduroam

OPENROAMING™  
WIRELESS BROADBAND ALLIANCE

実装上の留意点

## Cityroam導入のポイント

- 技術的にはeduroamと大差ない.
  - RADIUS周りは共用できる.
  - 基地局にPasspoint設定を追加する程度.
  - その他の面倒な部分は、Cityroam基盤におまかせ.
  - 自前でアカウントを発行しないなら、むしろeduroamより簡単.
- 通信事業者に相当する 設置・運用 が必要.  
(OpenRoamingは世界の通信事業者を含むローミング基盤)
  - SIで基地局を設置するだけでは不十分.  
SIのオマケではない運用体制が必要ということ.
  - 店舗などの設置には「マネージドWi-Fi」が必要.  
オーナーは、基地局ではなくサービスを買う.

## 導入提案: 通信事業者, ベンダ

- Wi-Fi事業者, ISP, CATV会社, 他
  - 認証連携基盤の運用
  - マネージドWi-Fiへの転換
  - マネージドIdPの提供 (必要に応じて)
  - 自治体向けや、学校向け、店舗向けなど、パッケージ化されたソリューションを提案.
  - 防災・減災のために、地域での **ローカルブレイクアウト (LBO)** と **ローカル認証** を考える.
- 機器ベンダ, システムインテグレータ
  - 通信事業者と協同でソリューション開拓

## 導入提案: 自治体, 施設オーナー

### ■ 自治体Wi-Fi, フリーWi-Fi

- 観光ばかりではなく、市民サービス指向に転換 (デジタルサービス対応)
- 市民センターや図書館、博物館など、公共施設に重点的に導入
- 市民向けのOpenRoamingだけでは足りない.  
教育・研究向けのeduroamの併設が強く望まれる.  
(eduroam無しでは、大半の利用者を失う → 価値の喪失)
- 運用を任せられるマネージドWi-Fiの導入
- 防災・減災や、交通を含む、都市デザインを考える (Smart City)

### ■ 教育委員会

- 小中高にもeduroamの早期導入を推進.  
GIGAスクールの持ち帰り端末を、図書館や勉強カフェ、コワーキングスペースなどで、安全に利用可能に. (デジタル時代の学習環境整備)

# 導入提案: 学校

## ■ 小中高校、他

- 早期のeduroam導入。(生徒の デジタルID の整備が本題)
- 高大連携では既にeduroamの活用事例があることに留意.
- 避難所になる場所に、市民も使えるOpenRoamingを導入する.  
(避難所でも安全な無線LAN利用環境が必要)

## ■ 高等教育機関・研究所等

- 従来のeduroamに加えて、OpenRoamingを導入.
- 訪問者用のゲストアカウントの手間を減らせる.
- 生涯学習や地域連携におけるネット活用を推進.

## まとめ

- OpenRoamingで、セキュリティと利便性を両立
- 観光も市民サービスも、セキュア公衆無線LANで支援
- Cityroamなら、eduroamもOpenRoamingも一括整備、デジタル時代の教育・研究を支援
- GIGAスクールの持ち帰り端末を市街地でも活用可能に
- マネージドWi-Fi を開拓する必要あり

## 課題

- 早期普及 & 応用開拓
- LBOとローカル認証の開発、実装