

報告

JANOG41.5 Interim Meeting (東京), 2018年4月20日  
JANOG41 BoFダイジェスト

# セキュア公衆無線LANローミング研究会 (NGHSIG) ～Passpoint/NGHにつないでみよう～

後藤英昭

東北大学・サイバーサイエンスセンター



1月  
26日 第8回セキュア公衆無線LANローミング研究会(BoF)・広島  
公開・主催者: 後藤 英昭

2018年1月26日(金) 14:10 - 14:45  
約2ヶ月前

広島国際会議場  
〒730-0811 広島市中区中島町1-5

地図を表示

- Passpoint/NGHの国内テストベッドの紹介と、会場でのトライアル利用を通じて、コミュニティのメンバーを集めたい。
- 主会場の裏番組、30分、空き部屋を ~~ジャック~~ 拝借
- 出席者4名 (私, 後輩, IIJ, 基地局メーカー)  
十数名期待したものの.....  
「JANOGで無線はあまり響かない」との噂？
- Merakiを持ち込み、会場の回線 (PoE)を借りてPasspointのデモ.



JANOG会場の

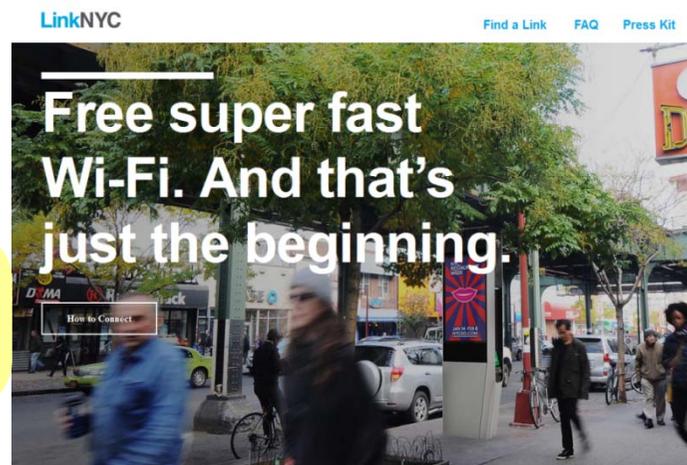


NGHSIGが認証連携基盤を  
提供しました (・▽・)ノ

# 次世代ホットスポット (Next Generation Hotspot, NGH)

- Wi-Fi AllianceとWireless Broadband Alliance (WBA)が共同推進する規格.
- PasspointによるSSID自動選択、自動接続.
  - **携帯電話並みの利便性**. 認証以降は1X認証と同等.  
(偽基地局への誘導を回避可能)
  - **北米のキャリアは既に運用中**.  
公衆無線LANでは、Boingo、LinkNYC、SF & San Jose Wi-Fiなどで導入済. **フリーWi-Fiもセキュアに**.
- 国際ローミングの規格化 (WRIX standard)
- 国内のキャリア、基地局ベンダは、**非対応**

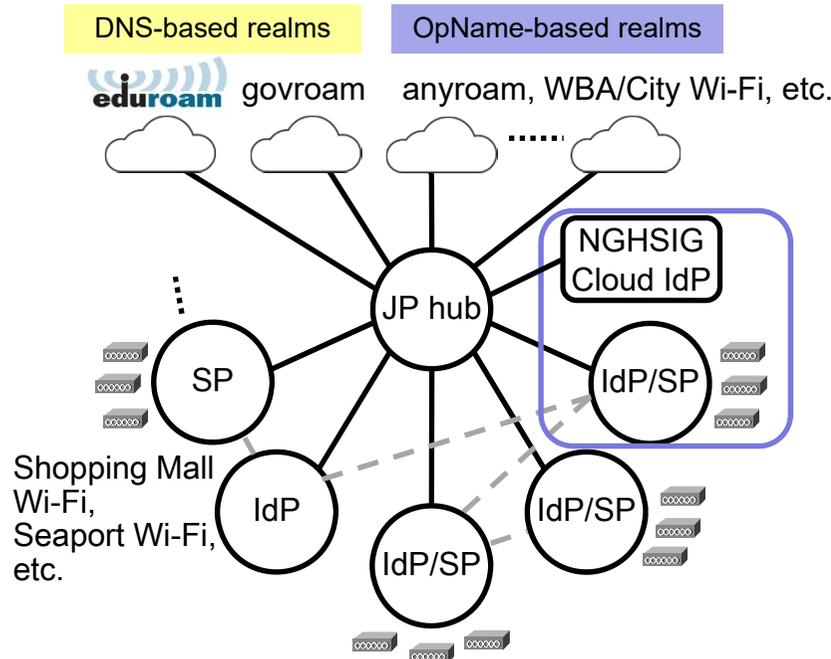
無線LAN認証連携基盤  
&国内NGH基盤を作ろう！



# City Wi-Fi Roaming 2017に乗ってみた

2018も準備中

- WBA主導の、NGH実証実験トライアル
  - World Wi-Fi Day (6/20)から8/20まで開催.
  - 40程度の携帯電話会社と無線LANオペレータ、約20都市が参加. 東北大学が学術機関として世界初参加 (NGHSIG代表)
  - フリーWi-FiでEAP-SIM/AKA認証
  - eduroamをNGHに乗せる  
認証連携アーキテクチャを開発



国内5地点でサービス提供

JANOG41 Bar BoF (広島)  
2018年1月26日

# 次世代ホットスポット(NGH) と セキュア公衆無線LANローミング研究会(NGHSIG)

後藤英昭 東北大学・サイバーサイエンスセンター

JANOG会場の  eduroam

NGHSIGが認証連携基盤を  
提供しています (・▽・)ノ

## 次世代ホットスポット (Next Generation Hotspot, NGH)

- Wi-Fi AllianceとWireless Broadband Alliance (WBA)が共同推進する規格.
- Hotspot 2.0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
  - 認証以降は従来の1X認証と同等なので、安全な接続 (偽基地局への誘導を回避可能)
- 国際ローミングの規格化
  - WBA WRIX (Wireless Roaming Intermediary eXchange) standard

# Hotspot 2.0 or Passpoint?

- 技術仕様としてHotspot 2.0とPasspointは同じもの
  - Hotspot 2.0 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で機能追加
  - OSU: Online Sign-Up
  - Policy provisioning
- OSU等を含めてWi-Fi Allianceの認証を受けたものがPasspointと呼ばれる
  - Wi-Fi CERTIFIED Passpoint™
  - iOSでもまだRel.1の段階

# Hotspot 2.0の仕組み

OSU

IEEE 802.11u

GAS: Generic Advertisement Service

ANQP: Access Network Query Protocol

NAI realm,  
OI, または,  
MCC/MNCによる  
プロファイルのマッチング

SSID自動選択、自動接続

IEEE 802.1x

EAP-SIM/AKA, EAP-TLS, EAP-TTLS

いわゆる従来の  
dot1X認証、  
自動接続

**Hotspot 2.0**

# WBA WRIX standard

(Wireless Roaming Intermediary eXchange)

## ローミング認証連携のための仕様

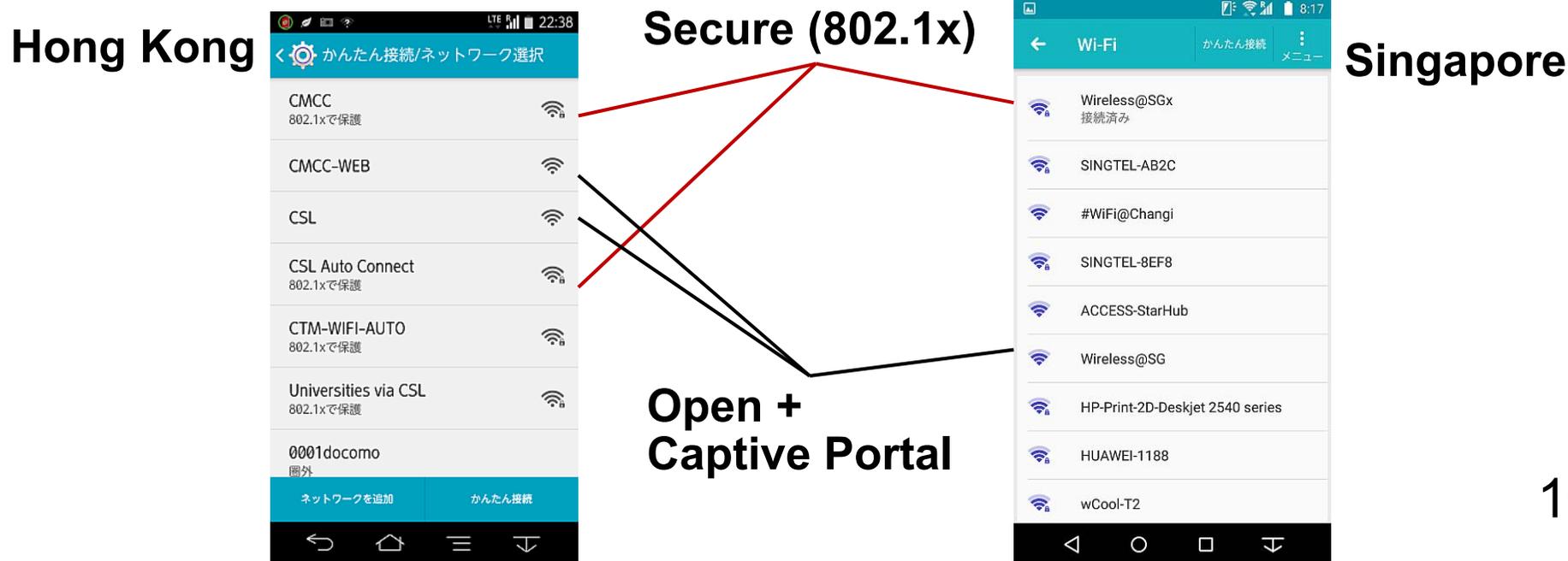
- WRIX-i (Interconnect)
  - 実体はRADIUS. 属性値などを取り決め.
  - とりあえずこれだけでもNGH基盤への接続は可能.
  
- WRIX-L (Location)
- WRIX-d (Data clearing)
- WRIX-f (Financial settlement)
- WRIX-n (Network)

# Passpoint / Hotspot 2.0 普及状況

- 幾つかの事業者がセキュア接続用に提供開始:
  - San Francisco & San Jose Wi-Fi (2014)
  - Orange Romania (2014)
  - LinkNYC (2016), InLinkUK (2017)
  - Boingo Passpoint Secure (25+ airports in US, Brazil, Portugal)
- Passpointはベストなソリューションに見えるが、  
いったいいつ来るの?
  - iOS 7, Android 6.x, Windows 10で対応  
(ただし、相性や機能不全が残っている)
  - 海外大手ベンダのエンタープライズ向け基地局は対応
  - 多くの公衆無線LAN事業者はまだ興味がない?
  - 対応機種への更新には時間がかかる

# 公衆無線LANの最近の動向

- 公衆無線LANのセキュリティ対策が大きな課題
  - 海外ではフリーWi-Fiでも1X認証の併設が見られる。
  - フリーWi-Fiのサインアップに、最低でもSMSによる紐付けが要求される国が少なくない。(欧州, 東南アジア)
  - 北米を中心にPasspointサービスが出始めてきた。
- 日本のフリーWi-Fiは対策が進んでいない 😞





# 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”**

# 「セキュア公衆無線LANローミング研究会 (NGHSIG)」 (2017.1～)

- eduroam, anyroam, govroamと認証連携を実現し、~~会議場や市街地でのサービス提供の下地となる基盤を開発する。~~

接続済み

- 商店街Wi-Fiや、イベント用Wi-Fiを接続して、セキュアなフリーWi-Fiを実現。(早期実用化を指向)
- 大手の事業者への波及方法を探る。
- セキュアなコミュニティWi-Fiローミング基盤の構築。
- (危険な)キャプティブポータルに代わるビジネスモデルの発掘、創成、及び、関連技術の開発。
- 運用における問題の洗い出し・解決 (法的問題)

# セキュア公衆無線LANローミングテストベッド (2017.4-)

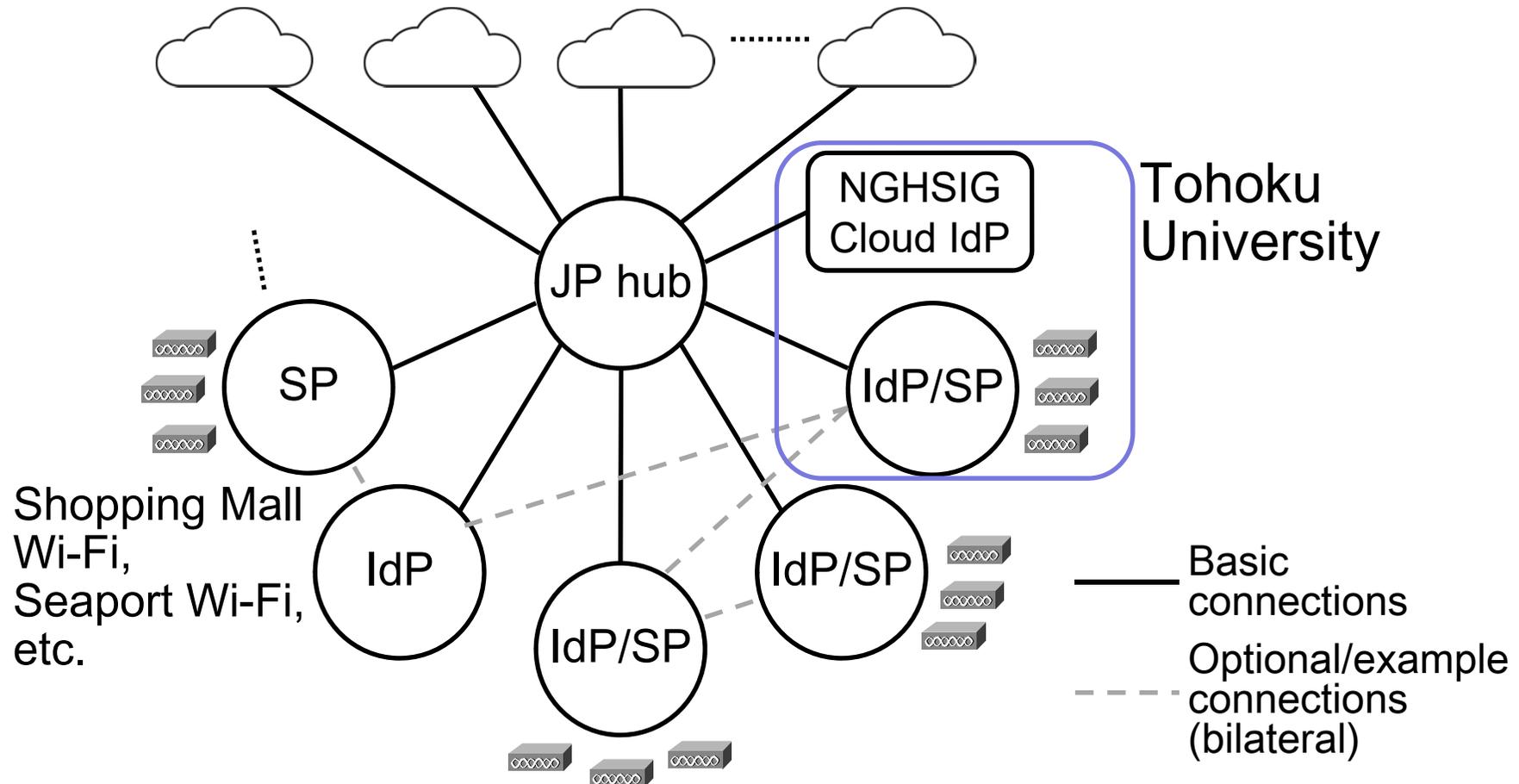
DNS-based realms

OpName-based realms



govroam

anyroam, WBA/City Wi-Fi, etc.



## テストベッドでできること

### ■ IDプロバイダ側:

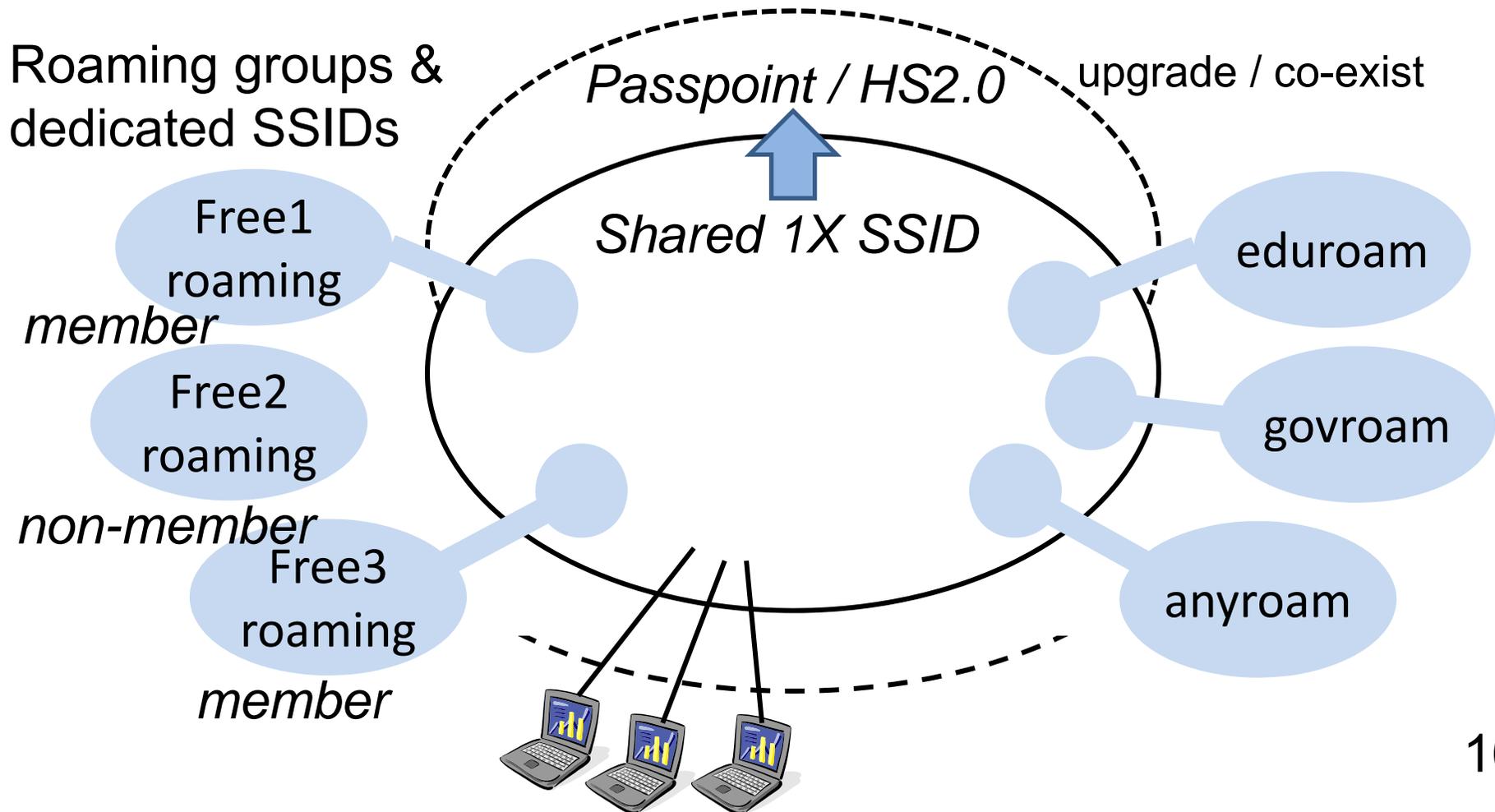
- RADIUS IdPを接続することで、EAPによる安全な認証連携で、利用者がフリーWi-Fiに乗れるようになる。  
(不正利用対策として、利用者の紐付けが必要。クレジットカード紐付けや、身分証明書による本人確認を推奨。最低限SMS方式。)

### ■ サービスプロバイダ側:

- 802.1x、または、Passpoint対応の基地局を接続することで、紐付けのある(信頼できる)利用者にフリーWi-Fiを提供できる。
- SP側には匿名でも、IdP側で紐付けが行われており、追跡手段が得られるので、無用な責任を問われにくい。
- イベント等の一時的な基地局設置でも、セキュアな環境を容易に構築できる。

# 基本的なアイデア

- 多数のローミングコンソーシアムを結ぶ認証連携
- Passpoint非対応の基地局のために、共通SSIDを使用



# City Wi-Fi Roaming 2017

## ■ WBA主導の、NGH実証実験トライアル

- World Wi-Fi Day (6/20)から8/20まで開催.
- 40程度の携帯電話会社と無線LANオペレータ、約20都市が参加. 東北大学が学術機関として世界初参加 (NGHSIG代表)



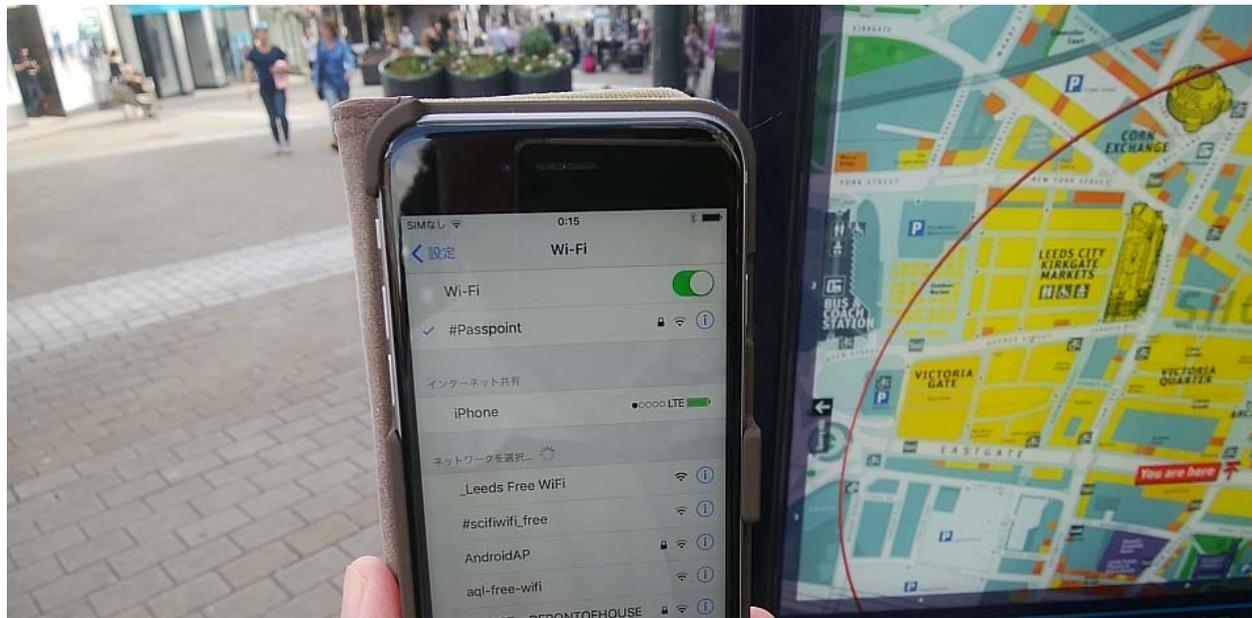
国内5地点でサービス提供  
(京都のホテルを含む)

OPERATORS AROUND THE WORLD INCLUDE:

AT&T, 2 Degrees NZ, Airtel, AIS TH, Bell Mobility, Boingo Wireless, BT, Celcom Axiata Berhad, China Mobile, Dialog Axiata,	Du, Etisalat Nigeria, Fon, Hong Kong Telecom, Idea Cellular, iPass, Korea Telecom, MegaFon RU, Mobilinek, Mobily, Mobitel,	MTN Nigeria, NTT DOCOMO, Omantel, Orange, Portugal Telecom, PT Telkom Indonesia, Robi Axiata,	Shaw Communications, SK Telecom, Smartone, Sudatel, Swisscom, Tata Telecom, Telstra, TELUS, T-Mobile USA, TRUE, Videotron, ER Telecom
--	--	---	---

## eduroam on NGHの実証実験

- City Wi-Fi Roamingトライアルにて、  
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



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

- セキュア公衆無線LANローミング研究会(NGHSIG)  
へようこそ (・▽・)ノ
  - <http://nghsig.jp/>
  - Wikiとメーリングリストあり☑ (希望者のみ)
  
- Passpointや認証連携は必須ですか？  
いいえ、1Xだけ、PasspointだけでもOK！
  
- 会費は？  
運営体制の整備も含めて検討中。  
海外ローミングの調整やWBA, WFAとの連携に経費(旅費,  
会費等)が必要なので、企業からの補助が欲しいです (正直)