セキュアな公衆Wi-Fiを構成する認証連携基盤とPasspoint/NGHの動向

セキュア公衆無線LANローミング研究会（NGHSIG）

http://nghsig.jp/
http://ngh.communities.jp/

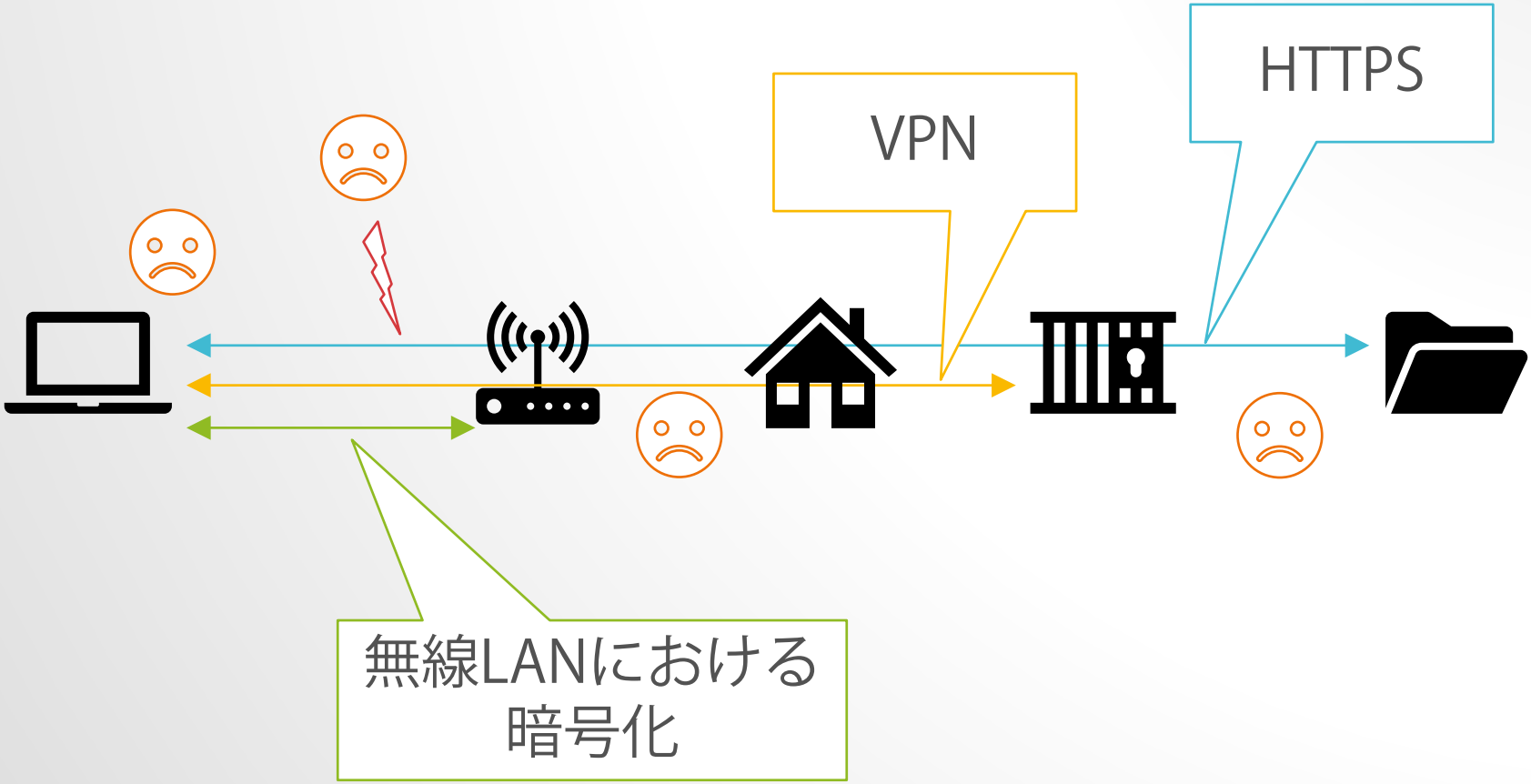
山口 潤 (E-mail: yamaguchi@communities.ne.jp / Twitter: @jyamag)

公衆無線LANの現状

- 2012年 携帯キャリアの無線LANオフロードで乱立する市街地無線LANの調整のために総務省で無線LANビジネス研究会が開かれる
  → 共用化などの方針が出されたが進展せず

- LTE環境が整ったため、オフロードは重視されず
- 市街地については大手２社主導
- ホテル、イベント会場においては出入りのSIerなどが構築
- SIerのリテラシーは千差万別

無線ＬＡＮに関わるセキュリティ

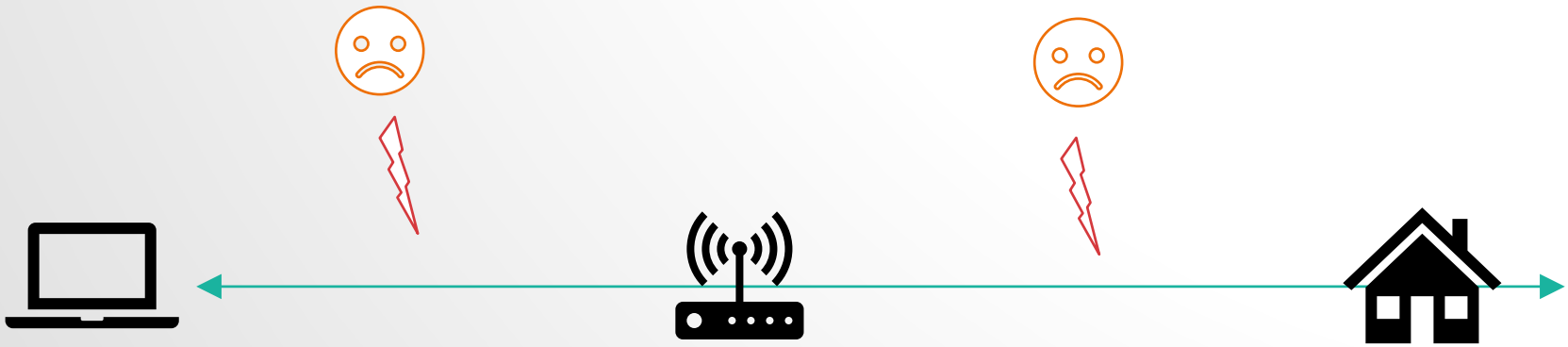


無線LAN使用時におけるセキュリティはVPNやHTTPSがあれば足りるということはありません。

公衆無線LANにおける攻撃の例 ＜盗聴＞

暗号化されていない区間から通信内容を盗聴する

- そもそもの暗号化を行っていなければ盗聴は容易
- 無線LAN区間で暗号化を行っていても有線区間での盗聴もある



用いられる攻撃手法：Eavesdropping など

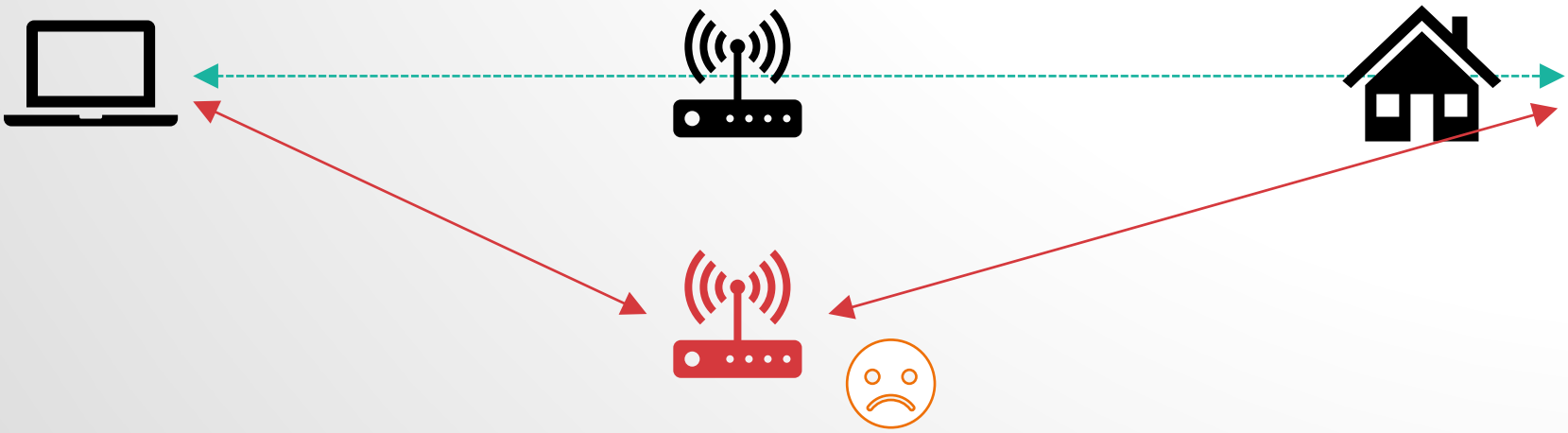
公衆無線LANにおける攻撃の例 ＜盗聴＞

宿泊施設での事例：有線区間で簡単に盗聴可能

公衆無線LANにおける攻撃の例 <APなりすまし>

偽APを設置し盗聴もしくは別サイトに誘導する

- 同じSSIDでAPを設置
- 共有鍵が漏れていればWPA2 Personalでも可能
- オフィスでも悪用の可能性は多分にある（退職者等）

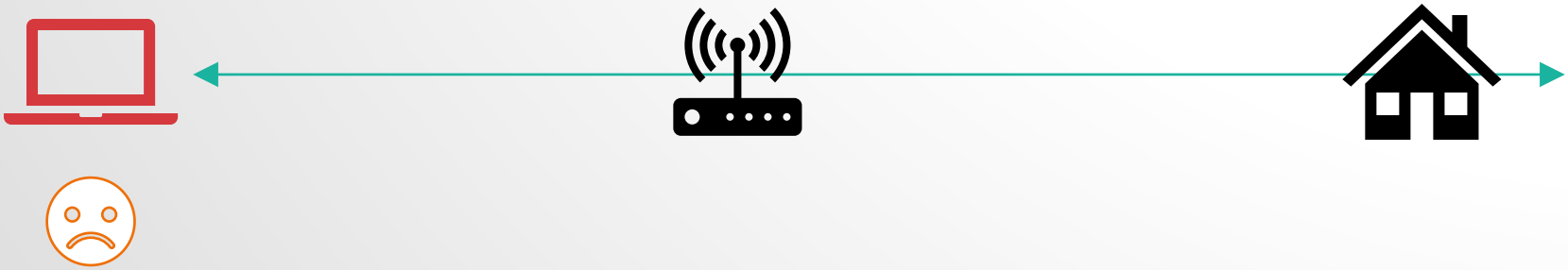


用いられる攻撃手法：Evil Twin など

公衆無線LANにおける攻撃の例 ＜端末なりすまし＞

第三者が正規ユーザーに偽装し犯罪等に利用する

- MACアドレスは偽装が容易
- MACアドレスのアクセスログを残すことで証拠としているサービスがあるが、偽装によって攻撃の発信源となった端末を追跡できなくなる



用いられる攻撃手法：MAC Spoofing など

公衆無線LANにおける攻撃の例 ＜個人なりすまし＞

LoA(Level of Assurance) 本人確認性が低いサービス

- 規約とボタンのみの承認制

  → 規約を読ませることが主

  MACアドレスの記録だけでは利用者には紐づかない

- メールアドレス認証

  → メール通達性確認すらしていない事業者も多い

  メールアドレス発行時に本人確認していない

- ＳＮＳ認証

  → SNS事業者との捜査協力連携はしていない

  アカウント発行時に本人確認していないSNSも多い

LoAの低いサービス


●●●●● au 4G
11:56
44%
192.168.2.1
ログイン
キャンセル
誰でも無料で「WiFi」を利用できます。
下記の利用規約をお読み下さい。
利用規約
第１章　総則
第１条（規約の適用）
同意します
規約の承認のみ


●●●●○ au
17:57
59%
正常に表示されない方はこちら
| English | 한국어 | 中文(简体字) | 中文(繁体字) |
ภาษาไทย
無料インターネット
無料インターネットのご利用にはメールによる認証が必要です。メールアドレスを入力後、「接続」ボタンを押して下さい。
メールの折り返しなどで
本人性確認をしていない
メールアドレス
hoge@moge.com
接続

参考：攻撃手法についての資料

- 11/24より総務省にてサイバーセキュリティタスクフォース 公衆無線LANセキュリティ分科会が開催（年度内４回程度の実施）

  http://www.soumu.go.jp/main_sosiki/kenkyu/cybersecurity_taskforce/index.html

- 第１回目の構成員説明資料にてわかりやすくまとまっているので必見です

認証方式別問題点＜オープン認証＞

- 暗号化されていない無線区間
- WebサイトがHTTPSを使用していても端末は無防備
- １度利用したSSIDを端末が覚えてしまう

  OSによっては容易に削除できない

  → 偽装APによる格好のターゲット

認証方式別問題点＜WEP/WPA Personal＞

- 共有されたパスワード
- 利用者の多さから共有鍵の変更がなかなか為されない
- 共有鍵が漏れていれば盗聴は容易
- オフィスにおいては情報漏洩リスクも

認証方式別問題点＜アプリ認証＞

- 対応外端末での利用不可

  → 欧米系利用者はPCを併用することが多い（市街地実測：5%）

- アプリを入れることへの拒否反応

  → 訪日客のアプリ利用比率は高くない（市街地実測：1%）

- アプリによって行っていることは異なる

  ・単なる初回登録の回避を行っているもの

  ・規約同意の回避を行っているもの

  ・プロファイルの入れ込みを行っているもの

  ・オープンなのかWEP/WPAなのか明示されていない

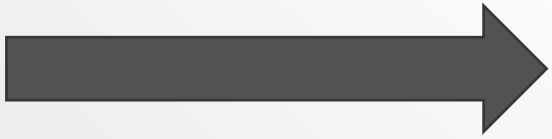
- 高いレイヤでの認証

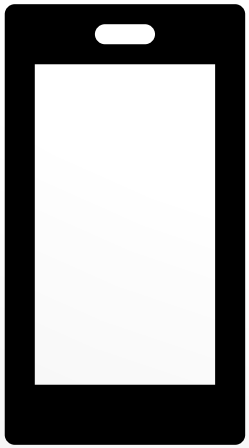
  → 認証回避型アプリは第７層での認証

事例：アプリと偽装APでの通信

- スマートフォンにプロファイルをインストール

0000hogehoge





事例：アプリと偽装APでの通信

- OSによってはプロファイルは容易に削除できない
- 利用者は危険性を熟知していないので一度接続した接続履歴を削除しない

事例：アプリと偽装APでの通信

- 知らない間につながり勝手に通信が行われる
- アプリを使っていなくてもプロファイルや接続履歴がそのままであれば同じことが起きる
- 共有鍵が漏れていればPSKでも同様

SSID: 0000hogehoge
（偽装）

0000hogehoge

対策：WPA2 Enterprise(IEEE 802.1Xを使った認証)

- IEEE 802.1X対応のサーバを用いて利用端末を認証
- ユーザーごとに異なるID/PASS or 証明書を用いる
- 利用者/AP/認証サーバ間で信頼確認を行う

- ID発行に手間がかかる

  → 利用者：SSIDが変わるごとにID/PASSを入れ込むのは面倒

  → オーナー：設備が過大になる（証明書の発行・本人確認）
- ３大キャリアでは徐々に増加

  （0001docomo / 0002softbank / au_Wi-Fi2）

  国内の公衆無線LANでサービス展開しているのは、ほぼ有償契約サービスのみ


eduroam

国際学術無線LANローミング基盤　eduroamとは

- 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
- IEEE 802.1Xを使った認証連携基盤として世界最大

  89か国・地域、週10億認証、1万ロケーション
- 訪問先の無線LANが随時・無料で利用可能

  ESSIDは世界共通の“eduroam”

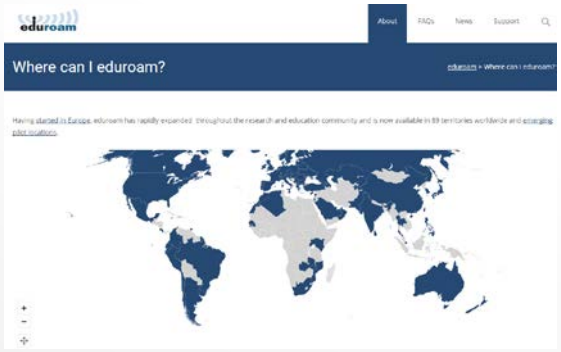
  一度設定を行えば、ロケーションごとに APを探す→ID/PASS打ち込み

  →認証 の手間は発生しない

  ex)

  T大学の学生が研究発表会で訪れたK大学を訪問

  K大学のSSID:eduroamに自動認証・接続



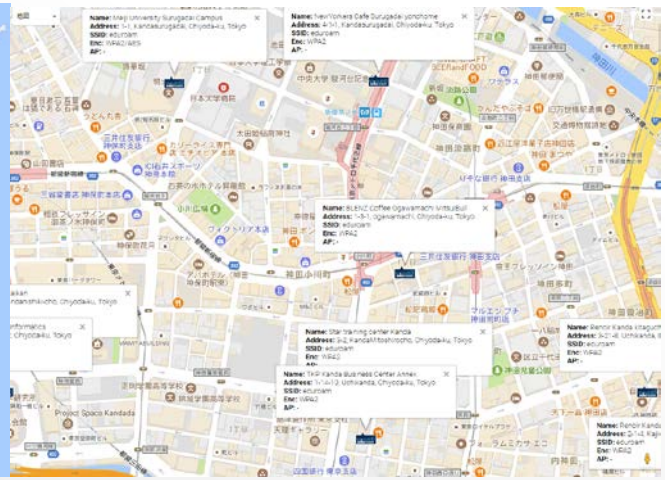
日本におけるeduroam

- 2006年導入
- 国立情報学研究所が運用
- 国内189機関にて導入

  2017年には大阪教育大学附属平野小学校において運用開始

  初等中等教育機関にも展開
- カフェ、会議室、旅館、コワーキングスペース等

  街中にも展開中



教育機関外におけるeduroam展開

- 空港での展開（スウェーデン・ノルウェーなど）
- 街中における展開（ドイツ、ポルトガルなど）
- 博物館、病院にて導入
- さらにはカフェ、バーなどでも

EDUROAM CONQUERS SWEDEN

Sweden is a worldwide leader when it comes to public ICT infrastructure, and so it's easy to understand why it's one of the leading countries in offering eduroam in public spaces.

eduroam was initially offered to Swedish universities and colleges, and almost all of them run eduroam today. More than 100,000 unique devices are authenticated per month, roughly 500,000 individuals are active within higher education in Sweden. The implementation and usage of eduroam in Sweden has indeed been a great success, but Sweden is aiming even higher.

The Swedish National Research and Education Network SUNET sought a partner to provide eduroam in places where students hang out outside normal campus areas. The solution that was chosen is to offer eduroam via SUNET's provider The Cloud through their existing access points, says Valter Nordh who is in charge of eduroam at SUNET, Sweden.

The first places targeted were travel hubs, such as airports and railway stations. Today, SUNET can provide eduroam in 934 locations through 16,146 access points all over

Pär Wellow is the Product Owner in charge of mobile solutions at Swedavia Airport Telecom AB. He notices a keen demand for the service. "In May 2012 we started offering free Wi-Fi connections to all visitors throughout all Swedavia airports. At that point, we had to restrict the usage, but that was not a popular move. Despite quite generous amounts of data we soon got feedback from many customers about the data limitations. But, when we launched eduroam the complaints almost disappeared. It turns out it was mostly students complaining about restricted usage of Wi-Fi. Overall, airport visitors are a crowd that expect excellence, and Wi-Fi is an extremely important part of the experience. So, today we are very happy to be able to offer eduroam together with SUNET and The Cloud."

Roald Sandén, General Manager of The Cloud Nordics adds: "The benefit from the eduroam service is apparent not only for the users, but also for our venue partners in all segments." He continues: "The transport segment where we cover the airports in cooperation with Airport Telecom, and the railway stations in cooperation with Jernhusen was the

SUNET

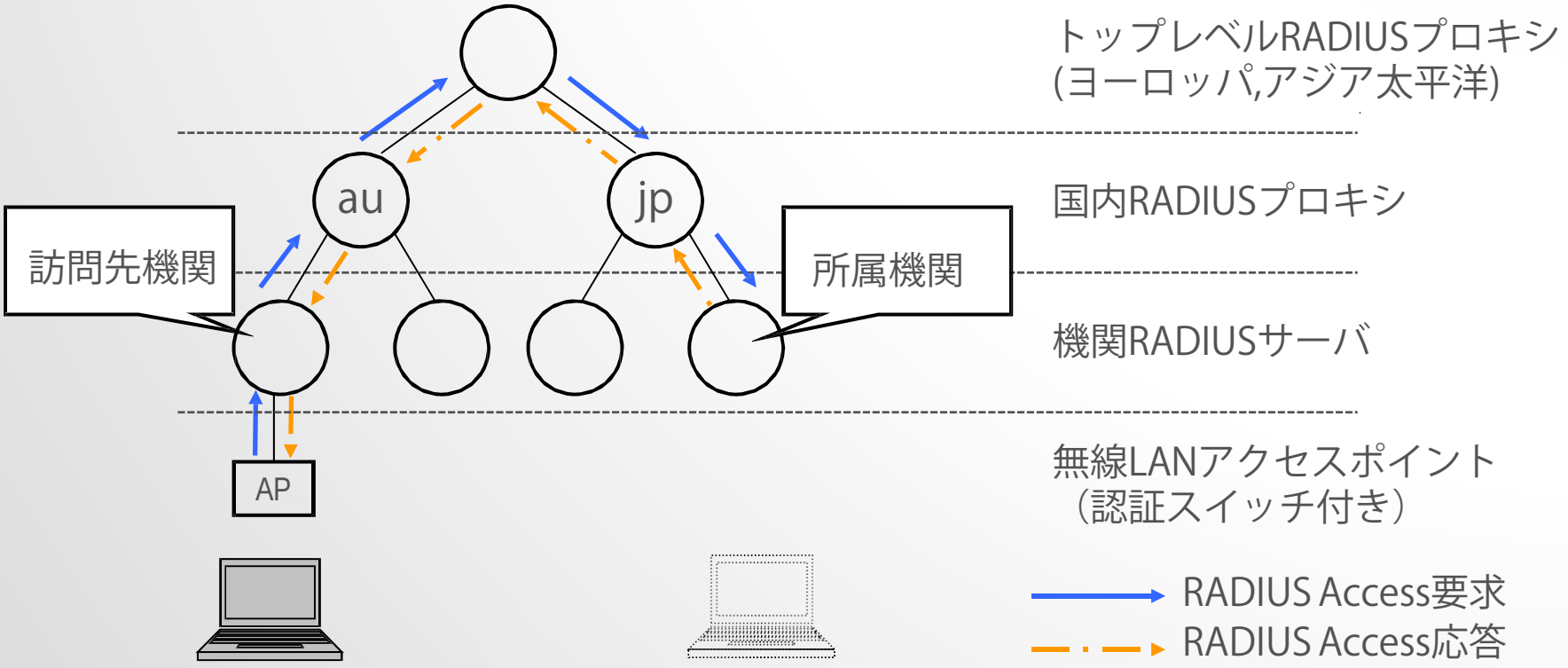
Some of the commercial venues providing eduroam in Sweden:

Hotels:
Best Western
Clarion
First Hotel
Park Inn
Radisson
Quality Hotel

Restaurants, cafés & bars:
Burger King
Starbucks
Barista
O'Learys
Stars and Stripes

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
- RADIUSツリーを介して認証情報を相互利用（認証連携）



Passpoint
NGH(Next Generation Hotspot)

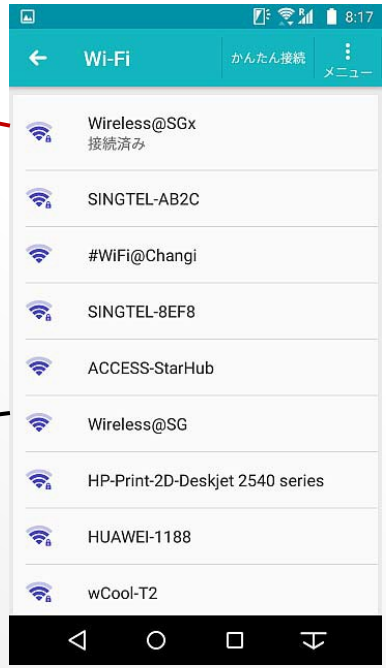
海外における公衆無線LANにおける近年の動き

- IEEE 802.1Xを使った認証を併設
  IdP（Identity Provider）による本人特定厳格化
  という動きが出てきた。

Hong Kong

Secure (802.1x)

Open +
Captive Portal



Singapore

公衆無線LANにおけるセキュア化を阻むもの

- オーナー or 事業者ごとに異なるSSID

  県と市が異なるサービスを展開し、同じロケーションで別SSID

  同じサービスでもサービス種別・オーナーへの料金体系ごとにSSIDを変えてしまう

  当社のサービスだと主張するSSID

- 非暗号化APの展開

  小エリアサービスにも関わらずPASS発行プロセスが煩雑なため、暗号化されていない形態での導入が多い

- 事業者・オーナー・行政の誤った認識

  「海外では認証が無いのにパスワードを設けるのは訪日客の理解が得られない」

  → セキュリティの面から本人確認が行えない・暗号化されないサービスは数年前から減少傾向

そこで…… NGH (Next Generation Hotspot)

- 北米を中心に展開が始まっていた
  IEEE802.11uを用いて接続可能なサービスを自動検出・選択
  ユーザ自らSSIDを探さなくても良い
- WPA2エンタープライズが必須
  IEEE 802.1X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
- SIMベースの認証（EAP-SIM、EAP-AKA）
  ※ ID / PASSWORDベースの認証・クライアント証明書(EAP-TLS)
  も使用可能

NGHを使えば異なるSSIDを跨いでも自動的にセキュア接続できる

＝無料公衆無線LANにとっても有用

NGH (Next Generation Hotspot)とは

- NGH …WBA・WFA共同で推進する次世代公衆無線LANの 「規格」
  - Hotspot 2.0

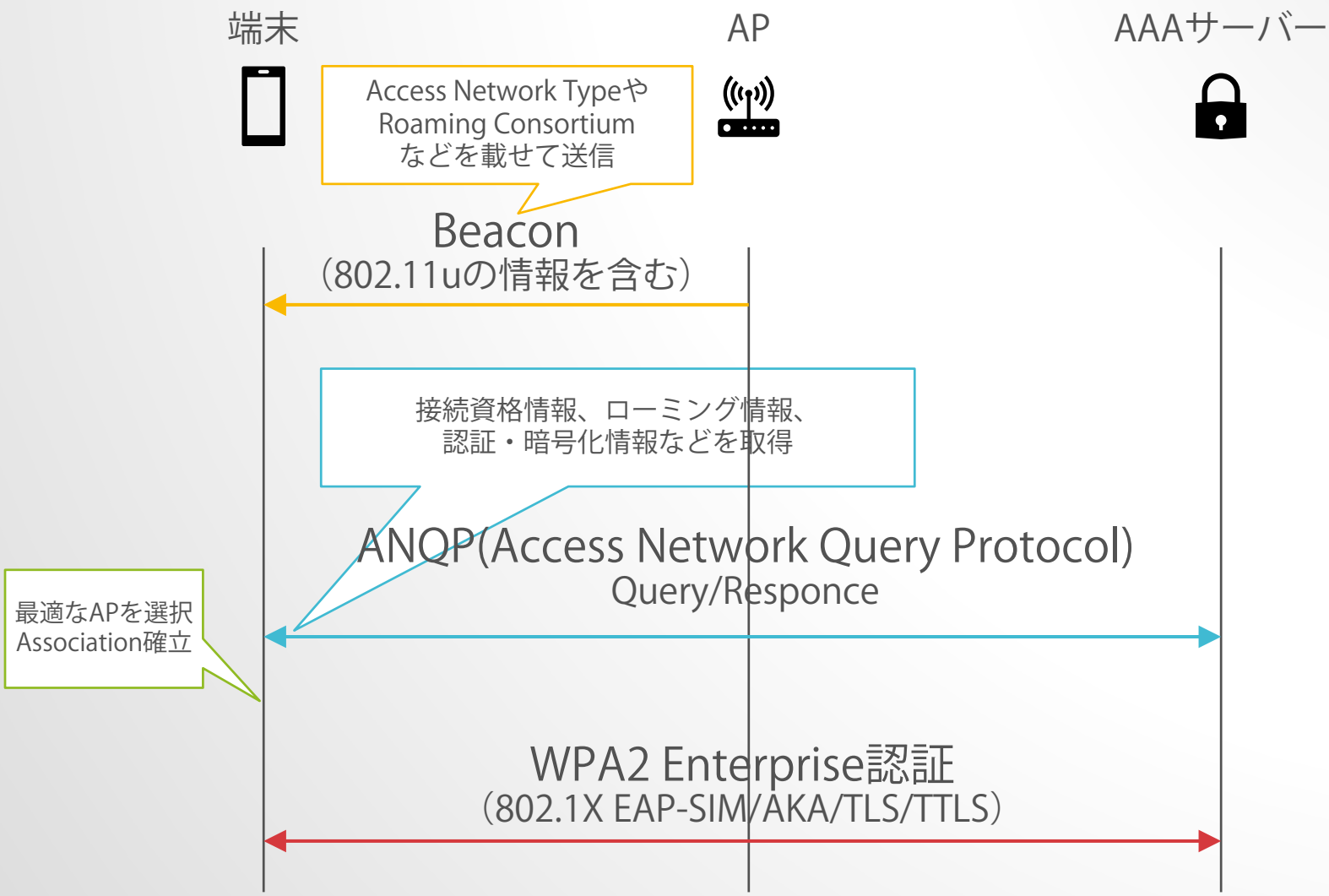
    Passpoint認定デバイスをサポートするネットワークを実装するための技術仕様（システム）
    - Wi-Fi CERTIFIED Passpoint ™

      WFAによる機器認定プログラム（ハード / ソフト）

  - WRIX（Wireless Roaming Intermediary Exchange）

    事業者間相互接続・精算規格

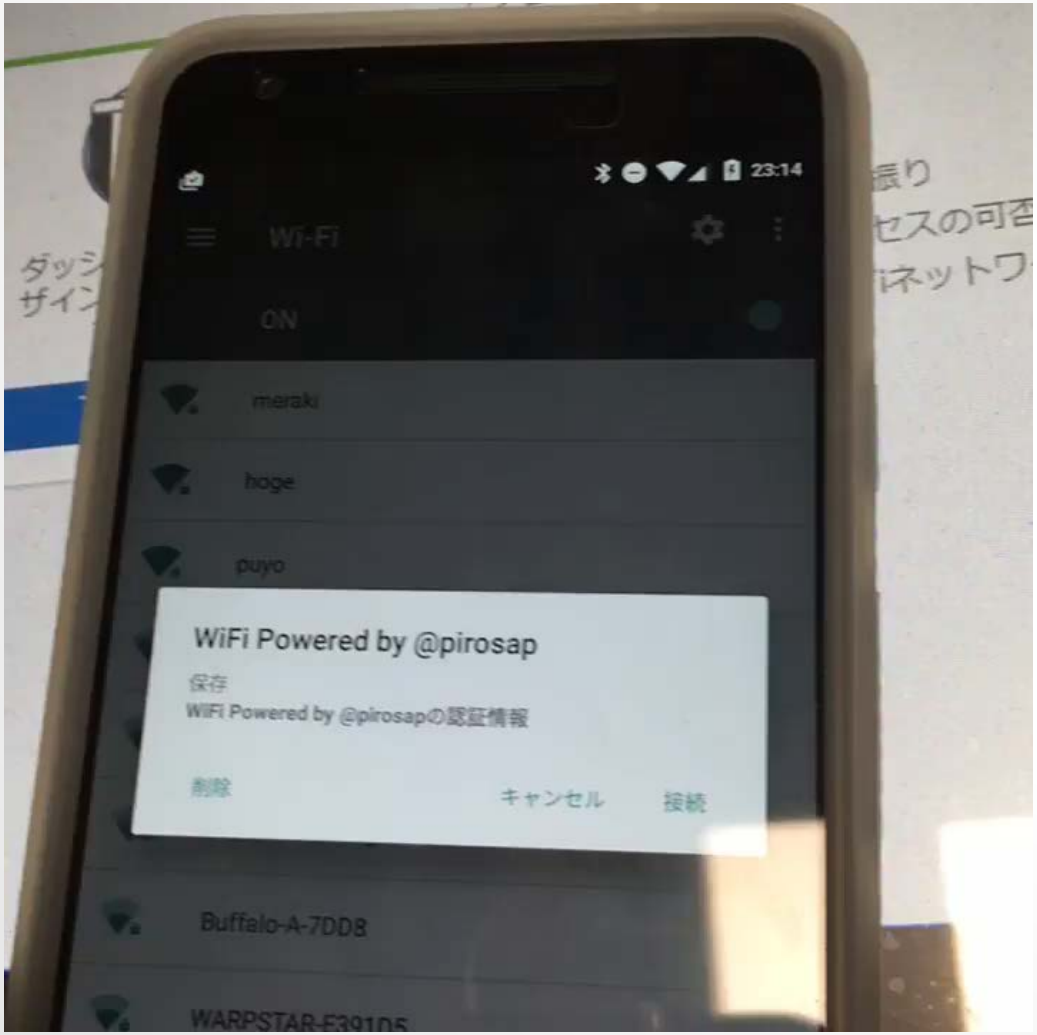
端末と認証サーバ間の動き



※ 端末・AP・AAAサーバ間のやりとりを簡略した図です
実際の接続手順とは異なります

端末と認証サーバ間の動き

AP側のSSIDをAからBに変更 → 端末が新たに見つけたSSID:Bに自動接続します



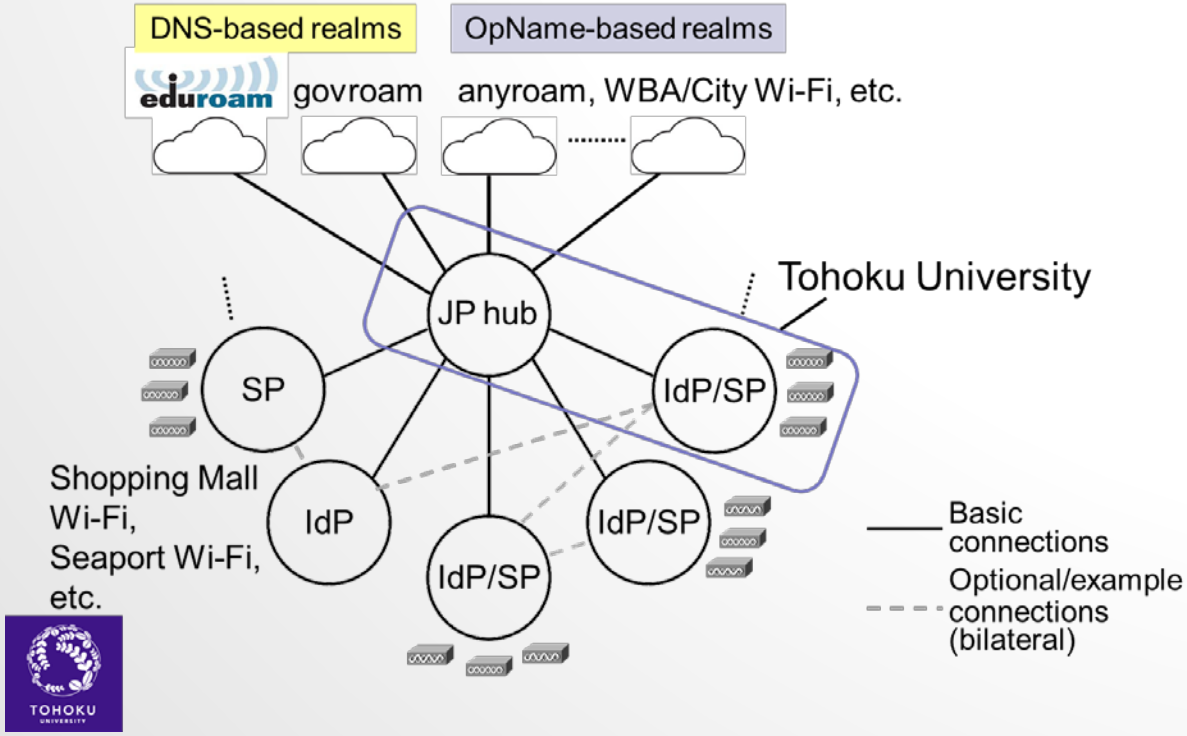
City Wi-Fi Roaming

セキュア公衆無線LAN研究会(NGHSIG)の立ち上げ

- 各公衆無線LANとの認証連携を実現し、
  会議場・宿泊施設や市街地でのサービス提供の下地となる基盤を開発
- セキュアなコミュニティWi-Fiローミング基盤の構築
- 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
- 小規模・地域事業者間の連携を図るとともに、大手の事業者への波及方法を探る
- 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テストベッド

- IEEE 802.1Xでの認証連携を行うためのテストベッド
- eduroam、anyroamと接続
- 国内外の公衆無線LAN事業者、IdPと接続



東北大学 後藤英昭准教授 作成資料より引用

City Wi-Fi Roaming Trial (2017/6/20 – 8/20)

- 2016年のWORLD Wi-Fi Dayから始まった公衆無線LANを繋ぐプロジェクト
- NGH基盤で各オペレーターを結び、ひとつのアカウントでローミング利用
- 2017年は17都市、日本からは東北大学が参加
  （学術機関としては世界初）

Passpoint対応無線LANアクセスポイントを探す

- Passpoint対応したアクセスポイントは？？

日本のメーカーに問い合わせ

・開発したいけど需要がはっきりしないと社内の稟議が……

・Passpointってなんですか？ 802.11u？？

残念ながらPasspointに対応したAPはありませんでした。

海外メーカーに問い合わせ

・日本仕様では削ったものを持ってきています！

・日本には扱ったことのある者がいないので……

・日本には営業しか置いてません！

メーカーにも知見がない。

NGHSIG自らAPの対応状況をチェックすることに

Passpoint対応無線LANアクセスポイントの選定

- とりあえず使える技適取得済みアクセスポイント

MikroTik hAP ac

ラトビアのメーカー

技適番号取得済み。大容量での実用性は未検証。

Aruba

以前よりPasspointに対応、動けば安定（Passpoint設定以外で躓くことはあります）

CISCO Meraki

長いことベータ版……（色々と課題あり。NGHSIGからの報告を受け、改善へ。）

Ubiquiti (UAP-AC-PRO)

技適番号取得済み。なかなか手に入らない。

CISCO

BoingoのPasspointサービスなどで利用実績あり

Ruckus

コントローラ無いとPasspoint非対応

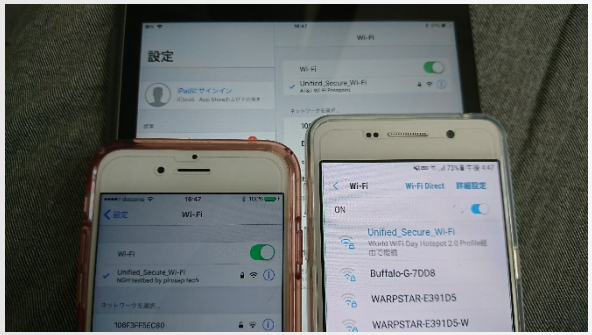
LinkNYCなどで利用実績あり

クライアント側のPasspoint対応状況

- Passpoint対応した端末は？？

  Windows10 / MacOS 10.9以降 / Android 6.0以降 / iOS 7以降

- プロファイルがインストールできれば



SSIDを指定しなくても端末が勝手につなぎます

IEEE 802.1Xを使ったセキュアな認証です

- プロファイルがインストールできない端末もあり…

Android 6の端末を中心に多数存在

証明書のインストールでこける端末も

国際版はOKでも国内キャリア版はNGの場合も

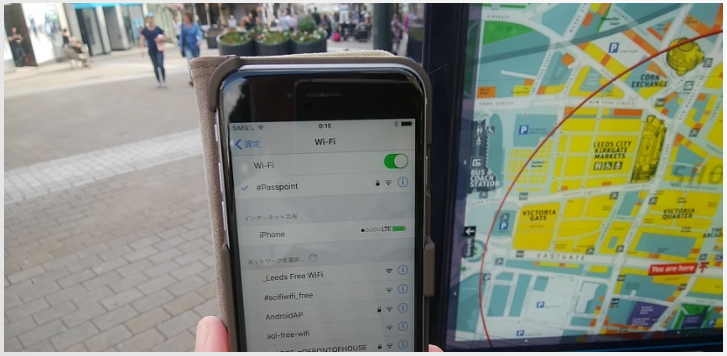
NGHSIG自ら端末の対応状況をチェックしました

City Wi-Fi Roaming 接続実証実験

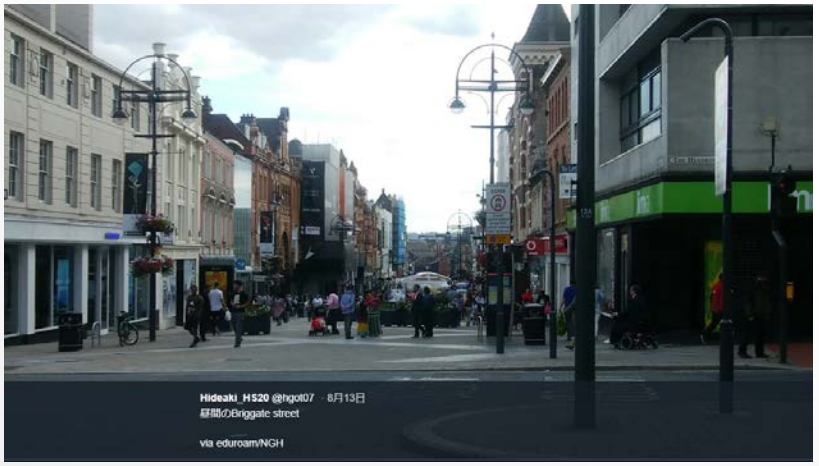
- 海外キャリア・IdPのアカウントで繋げる＠日本

京都 旅館こうろ様

- 日本のアカウントで海外で繋げる＠イギリス



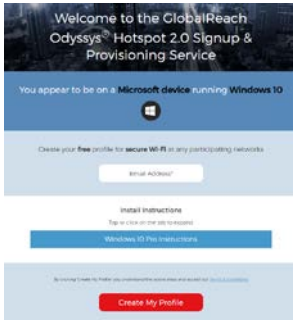
Leeds市街地

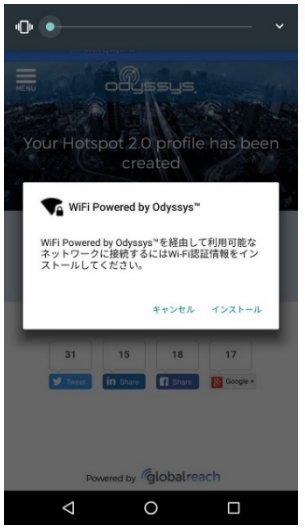


その他NGH事例：イベントにおける運用

WIRELESS GLOBAL CONGRESS (NYC 13-16 November 2017)

- オンラインサインアップ
- プロファイル生成
- イベント会場で接続





その他、市政府・ケーブル通信事業者・ホテルチェーン・空港など
市街地におけるNGH事例が広がっています

今後の課題

- セキュアな公衆無線LANとして本人紐づけが大事となる

  特に海外キャリアは本人確認性を重要視する

  → IdP（Identity Provider / ID発行機関）とどう連携するか

- 国際間を跨いだ法的問題

  →問題発生時の連絡手順の確立

  →約款表記・接続先機関明示など

- どうNGHを普及させるか

  →補助金要件から微妙にズレる

- 知見の集積

  →端末側の問題、AP側の問題はまだまだある

セキュア公衆無線LAN研究会(NGHSIG) のご案内

ネットワークオペレーター、IdP、端末メーカー、APメーカー、オーナー……
NGHについて知見の蓄積・情報交換を行っているグループです。

SIGを月 1 回程度開催のほか、ML・Wikiなどでの情報交換を行っています。
興味ある方は以下のURLからご連絡ください。

http://nghsig.jp/

ご清聴ありがとうございました