資料2－6

公衆無線LANにおけるセキュリティ対策

2017年12月1日

（株）KDDI　技術開発戦略部
三宅　優

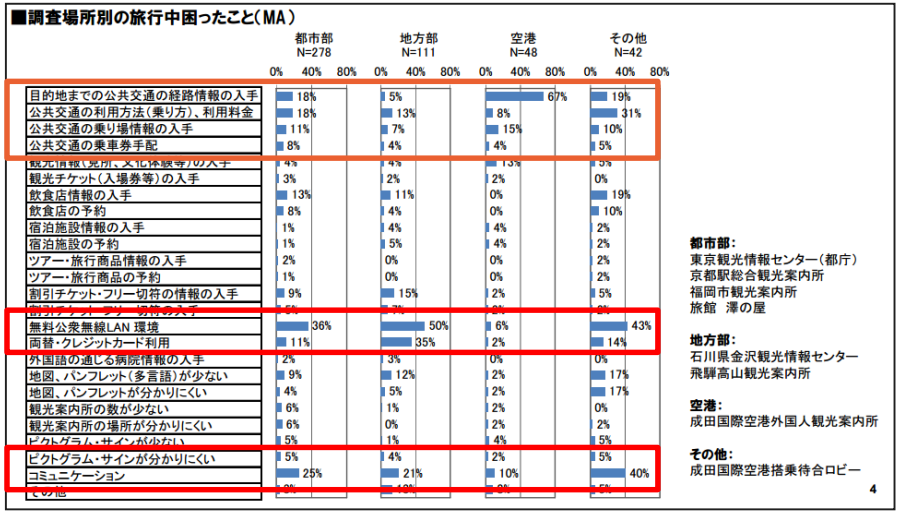
目次

公衆無線LANのセキュリティの状況

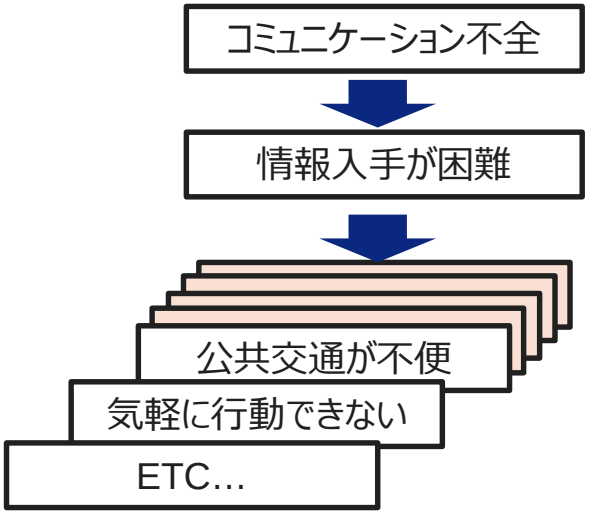
課題認識

【訪日外国人が抱える課題】

- 訪日外国人が来日した際に最も困る事は、公衆無線LANの少なさ、コミュニケーションが突出。次に公共交通の利用方法や情報の入手が来る。
- 検索エンジンが使えない、会話で情報が手に入らない等の問題に波及している。



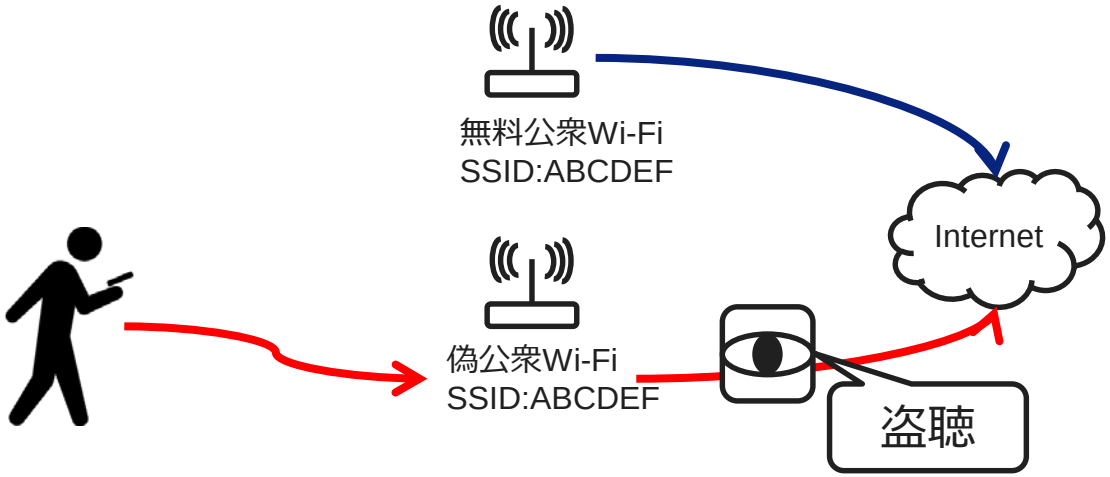
観光庁調査 https://www.mlit.go.jp/common/000190659.pdf



- **快適な日本周遊の為にも、目先では「公衆無線LANの利用エリア」が広がることは重要**

課題認識

【利用者の不安】
- リオ・オリンピック／パラリンピックでは数多くの盗聴目的Free Wi-Fiが発見され、取り締まりが行われた。
- 訪日外国人や、パケット代を節約したい若者等に高い需要がある無料の公衆無線LANではあるが、現状では簡単に偽アクセスポイント（AP）を構築できる。その状況についてはあまり知られていない。
- またその存在を知っている人でも、街中に溢れる数多くのSSIDから、安全なWi-Fiを判別するのは困難な状況にある。



【利用者からみたあるべき姿（要件）】
①最小限の手間で
②安全に送受信できる通信環境を
③なるべく多くの場所で利用できる。

ユーザ視点と提供者視点の分類

ユーザー視点

提供者視点

視点A
- 信頼できるサービスを利用したい
- 通信内容は見られたくない
- 他人に自分の権利を使われたくない

視点B
- 使えれば何でも良い
- セキュリティよりもネットにつながることが重要

視点C
- 決めた人以外は使わせたくない
- 未払いの人には使わせたくない
  →キャリアのWi-Fi等

視点D
- 誰でもどんどん使って欲しい
- 利用者は多い程よい
- 利用者に対して手間をかけたくない
  →客寄せ用、マーケティング用のWi-Fi

暗号、認証の強さは、ユーザー視点、提供者視点で決まる

提供者が構築する認証の強さは、提供者の視点次第

視点C

【対面認証】
市場でもっとも厳しい認証方法。例えば銀行の住所変更。
電話、生年月日、通帳残高、その他で本人確認をする。
とても面倒臭いがめったに無い事なので許されている。

【生体認証】
個人を特定しやすい。
生体認証情報を鍵とすることは論理的には可能。企業では多数使われている。
但し倫理的な壁がある為、端末内部で閉じられていることが多い。（iPhone、FIDO等）

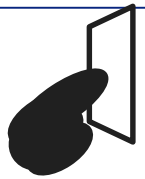
Wi-Fiでは一般的に使われていない

【SIM認証】
キャリアだけがSIM内部の鍵を知っている。
また個人を特定しており、詳細な個人情報も持っている。
ここまでが、個人を特定可能な認証と呼べる。（盗まれたらサービス停止）

視点D

【メール認証】ここから個人特定は事実上できないといえるが、訪日外国人はこれが多い。
メールアドレスはネット上のもので、次々作れる。
キャリアメール限定のメール認証はSIM認証に近いが、フリーメールが使えることもある。

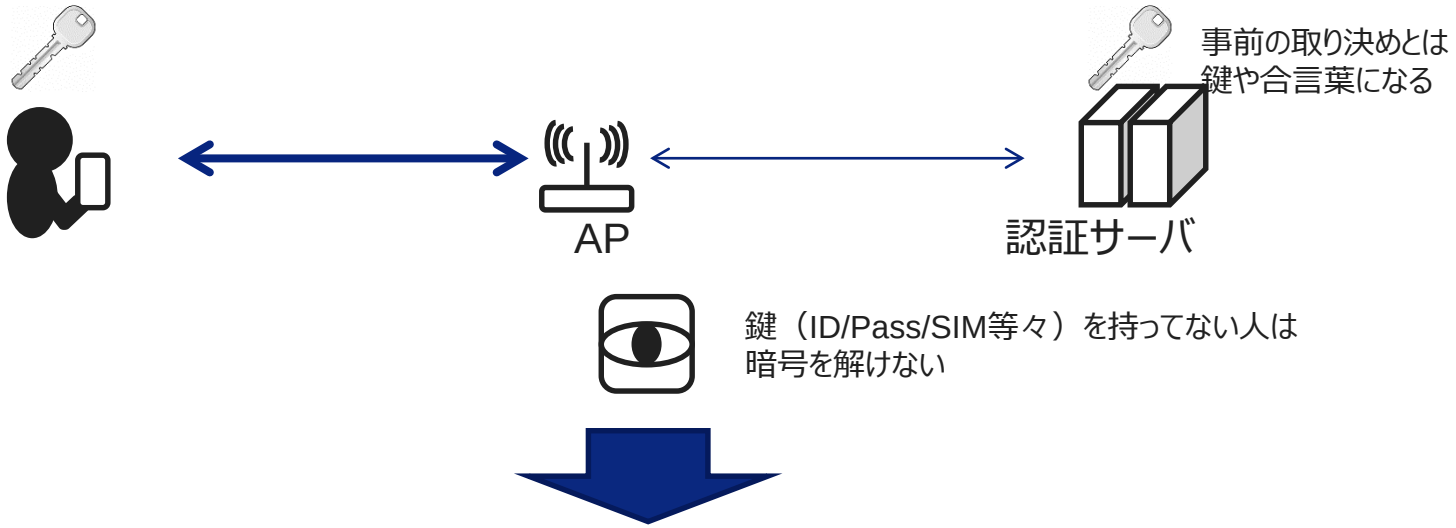
【SNS認証】
大手SNSの認証機構を使うが、架空のアカウントを作れるので、個人特定は不可といえる。



【ワンタップ認証】
利用規約を読んでOKを押せば利用できる。多くのフリー公衆無線LANがこの方式を採用。

通信の暗号化が進まないのはフリーな公衆無線LANに対するユーザーの想い

【暗号化の為に必要なもの】
暗号化を利用するには、基本として、端末、サーバー間で「事前の取り決め」が必要。
この事前の取り決めによって、無線通信の暗号化方式が決まる。



通信の暗号化を行うには、事前に端末側とサーバー側で鍵が必要となる。
キャリアWi-Fiは、SIMを払い出すときに一緒に鍵を入れている（EAP-SIM/EAP-AKA）
→お客様は意識すること無く利用できる

フリーな公衆無線LANで暗号化が進まないのは、**この鍵を入れる作業が面倒、若しくは周知が不十分だから**。
→最近はアプリをダウンロードして鍵をインストールする方法が主流（EAP-TTLS等）
　但しフリーな公衆無線LAN提供者毎に違う鍵が必要なので、一般のお客様はダウンロードの手間を嫌う傾向

利用者のニーズと普及

- 普及期に入り、単につながるだけでは無く様々な要素が公衆無線LANに求められている。
- 今後の公衆無線LAN普及の鍵は、多様化するユーザーニーズへの対応
  選択肢をしっかり提示できることが重要

これまで

公衆無線LANを使いたい

これから

	もっと簡単に 公衆無線LANを使いたい	地図しか見ないから簡単なのがよい 危険性をよく知っているから手軽なのがよい
更に	安全に 公衆無線LANを使いたい	面倒でも暗号化はして欲しい カード決済をしたいから有料でも安全が良い
	付加価値のある 公衆無線LANを使いたい	近くのTAX FREEのショップを知りたい クーポンが付いているWi-Fiアプリが欲しい

KDDI Wi-Fiサービスにおけるセキュリティ対策

SSID	暗号化	備考
au_Wi-Fi	WPA2	スマートフォンに鍵をインストール
au_Wi-Fi2	WPA2 Enterprise	スマートフォン内の鍵を利用
Wi2	暗号化なし	
Wi2premium	暗号化なし	
Wi2_club	WPA2	スマートフォンに鍵をインストール
Wi2premium_club	WPA2	スマートフォンに鍵をインストール
UQ_Wi-Fi	WEP	スマートフォンに鍵をインストール
Wifi_square	暗号化なし	

基本方針　：　KDDIのスマートフォンにはユーザにパスワードを入力させずに暗号化アクセス

鍵の配布　：　モバイル通信に利用する鍵の利用、または、アプリ経由でインストール
セキュリティ　：　アプリでユーザが設定可能（セキュリティ強　⇒　接続先を限定、
サービスエリア拡大⇒暗号化されていないアクセスポイントにも接続可能）

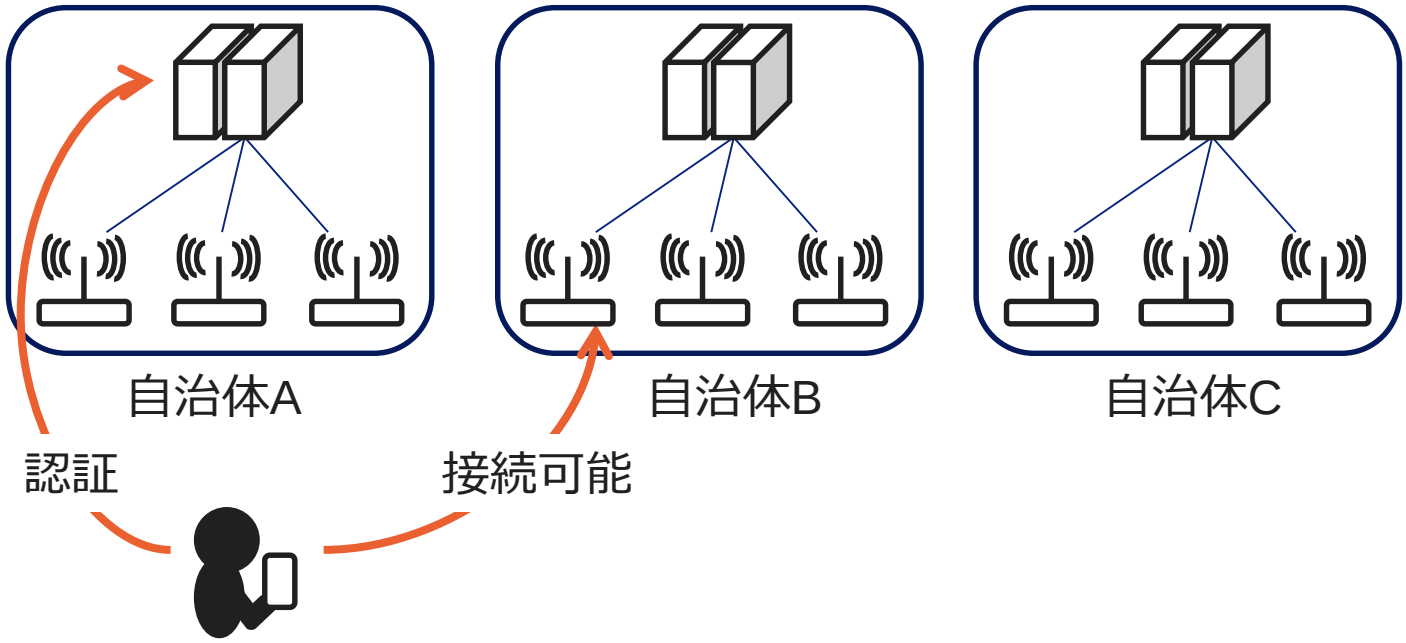
au Wi-Fi接続ツール

■ au Wi-Fi接続ツール

- スマートフォン向けのアプリで、au Wi-Fi接続の設定が可能

共通認証基盤

【現状の共通認証の課題】
訪日外国人の利便性向上目的で共通の認証基盤が整備されれば、ユーザの認証の仕組みが進み、公衆無線LAN利用に対する安全性が高まる。認証情報を使えば、暗号化の利用も促進できる。
しかし、利用者の特定を可能となる認証情報に何を利用するかが課題。



共通認証基盤の例：　公衆無線LANサービス間で認証情報を共有。ある公衆無線LANで登録を行うと、　他の公衆無線LANサービスでもその認証情報が利用できるようになる。

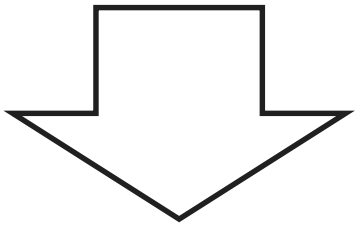
認証の強度について

■ 認証の強度

- インターネットでは様々な認証サービスが行われているが、認証の強度レベルはまちまち
  - パスポート等の個人のIDと紐付いて発行されたID ⇒ 信頼度は高い
  - SNS、Webサービス等のID ⇒ 誰でも取得可能なIDのため、架空アカウントの作成も可能

■ LoA: Level of Assurance

- ID情報の信頼度を表すもので、LoA1～LoA4の4段階で分類
- NIST SP800-63、 ISO/IEC 29115、ITU-T X.1254



- 認証の強度を扱える共通認証基盤を構築可能か？
- 認証の強度に応じたサービス提供が可能か？
  （例えば、レベルが低い認証情報の場合はサービスを限定する、等）

公衆無線LANのセキュリティ対策について

必要とされる対策（案）

■ セキュリティ対策のために必要とされる機能

- **暗号化**
- **認証強化**
- **偽アクセスポイント対策**

■ 公衆無線LAN接続用セキュリティアプリの配布・展開

- **具備する機能（例）**
  - 共通認証基盤を利用した利用者認証機能
  - 偽アクセスポイント対策
  - 安全性に考慮したAPの判定・接続
  - 無線区間の自動暗号化対策
  - VPN機能の提供
- **課題**
  - 不正アプリ対策

セキュリティが高い公衆無線LANサービスも選択できる環境整備が必要

セキュリティに配慮した
公衆無線LANサービスの普及について

公衆無線LANの安全性対策

■ 安全性基準の策定

- ガイドライン等でセキュリティ対策のレベルを規定
- 公衆無線LAN提供者がどのセキュリティレベルでサービスを行っているかを提示

■ 不正なアクセスポイントの探索、通知

- 問題があるアクセスポイントを探し出す仕組み
- 問題があるアクセスポイント、不正なアクセスポイント発見時の対策手順の確立（設置者への注意喚起、利用者への注意喚起、等）


Designing The Future
KDDI