資料３－１

「公衆無線LANセキュリティ分科会」論点整理

平成29年12月

論点整理における基本的考え方

基本的考え方

【検討の前提】

○　公衆無線LANのセキュリティ対策の検討においては、利便性と安全性のバランスに配慮した検討が必要。

○　セキュリティとコストはトレードオフの関係にあることも踏まえつつ、対象（ステークホルダ）や場面を整理した上で、誰が誰にどのような場面において何を守るかを特定し、求められるセキュリティ対策について、プライオリティを付けた重点的な検討が必要。

○　その際、利便性とプライバシーのバランスに配慮しつつ、認証方式の検討を行うこととし、セキュリティ対策については、市場実態や海外の事例、標準化の動向を踏まえた検討が必要。

【検討の方向性】

○　一律に、特定の認証方式や暗号化方式を推奨するのではなく、提供形態や利用シーンに応じて、提供者は多様な認証方式や暗号化方式による公衆無線LANサービスを提供するなど、利用者に与える選択肢を増やし、利用者がそれらのサービスを適切に選択することが可能な環境を整備してはどうか。

○　具体的にどのようなセキュリティ対策を行えばよいか分からない利用者や提供者も多いことから、利用者や提供者が、どのような利用シーンにおいてどのようなセキュリティ対策を講ずればよいか、適正な対策方法について、周知・啓発を図ってはどうか。

○　分科会の検討結果をもとに、2020年東京オリンピック・パラリンピック競技大会に向けて、自治体や民間企業等におけるセキュアな公衆無線LANサービスの環境整備の取組に繋げてはどうか。その取組に必要なガイドラインの策定や、ガイドラインに基づくリファレンスデザイン（模範事例）となる公衆無線LANサービスの環境整備の実証を図ってはどうか。

公衆無線LANセキュリティ分科会における検討事項

出典：公衆無線LANセキュリティ分科会（第1回）（平成29年11月24日）資料１－３

【検討事項１】公衆無線LANのセキュリティ対策について

- ①　認証方式について
- ②　暗号化について

【検討事項２】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

- ①　利用者・利用シーンに応じた公衆無線LANサービスの提供について
- ②　公衆無線LANサービスの環境整備について

検討事項1①　認証方式について

検討事項

○　公衆無線LANサービスを踏み台にした攻撃やなりすましによる不正アクセス等、不適切に公衆無線LANサービスが利用されるおそれがある。利用者を認証する方式として、例えば、Web認証、SIM認証、SNS認証等が挙げられるが、利便性と安全性のバランスに配慮しつつ、利用者が安心して公衆無線LANサービスを利用するためには、どのような認証方式が望ましいか。また、不正アクセス等を防ぐためには、どのような対策が求められるか。

現状・課題

【トレーサビリティ関連】

○　キャリアWi-Fi（通信キャリアが提供する公衆無線LANサービスをいう。以下同じ。）は、ある程度トレーサビリティが確保されているが、自治体Wi-Fi（自治体が提供する公衆無線LANサービスをいう。以下同じ。）やフリーWi-Fi(ここではキャリアWi-Fiや自治体Wi-Fi以外の公衆無線LANサービスをいう。以下同じ。）の中には、認証の仕組みを設けていないものもある。ログを一切残しておらず、不正利用が起きたときに対処できないものもある。

○　トレーサビリティの確保は、無線LANの技術以外で補完するという方法もある。認証や利用登録は、公衆無線LANサービスを利用するまでのハードルを高くしている。

○　Web認証等の簡素な認証しか実施していない事業者と、より厳格な認証を実施している事業者との認証連携では、全体としてのトレーサビリティは弱まることが考えられ、Level of Assuranceの評価も難しい。

【認証方式関連】

○　IEEE802.1xによる認証は、サーバーを維持・管理するコストが発生するため、このコストを誰が支払う仕組みにするか、ビジネスモデルをどうするかという課題がある。

○　eduroamという大学等において相互利用可能なローミングサービスは、認証サーバ間で認証情報が交換されており、一度登録すれば、eduroamのある場所では、どこでもすぐに公衆無線LANサービスを利用することができる。

○　Web認証では、偽の認証画面によってIDやパスワードが窃用される可能性がある。

検討事項1①　認証方式について

現状・課題

【接続アプリ関連】

○　公衆無線LANサービスが普及する過程では、キャプティブポータルから接続するものが多かったが、最近はアプリを入れて接続するものが多い。しかし、訪日外国人にとって、日本に来る前に事前にアプリを入れる人は少なく、また、日本に来てからどのようにアプリを入れるかといった課題がある。

○　偽アプリの懸念があり、利用者にとって、見知らぬアプリを入れる抵抗感はある。

○　他方、アプリが普及すれば安心な利用環境ができ、アプリは便利かつ安全という評判が広まるので、インパクトがある。

考え方

○　**キャリアWi-Fiでは、**SIM認証、携帯電話をIDとしたWeb認証、アプリによる認証等によるサービスが提供されており、これらの認証方式により、**一定のトレーサビリティが確保できているという認識**。

○　一方、**自治体Wi-FiやフリーWi-Fiでは、**Web認証やSNS認証等によるサービス、あるいは、認証のないサービスが提供されており、**公衆無線LANの技術によりトレーサビリティが十分に確保できない場合もある。**この場合においても、利便性を考慮し、公衆無線LANを誰が利用していたかを**何らかの手段**（例えば、周囲の人の目や監視カメラ）**で補完できれば、公衆無線LANサービスにおけるトレーサビリティを確保できる**のではないか。あるいは、**二要素認証も選択肢の一つ**となるのではないか。

○　利用者がアプリを入れるという手間がかかる一方、アプリを入れることにより無線区間の暗号化も実現できるといった長所もあり、公衆無線LANに接続する主な端末は、ノートPCからスマートフォンになっていることを踏まえると、**アプリによる接続は選択肢の一つ**となるのではないか。その際、**接続アプリの信頼性を担保する仕組みが必要**ではないか。

検討事項1②　暗号化について

検討事項

○　公衆無線LANサービスにおいて、暗号化が行われていない通信では、通信内容が盗み見されるおそれがある。情報漏洩のインシデント等の対策として、クライアント（端末）とアクセスポイント間のネットワーク層（無線区間）における暗号化（WPA2等）やサービス層における暗号化（HTTPS等）が挙げられる。技術の動向を踏まえつつ、公衆無線LANサービスの利用者にとって、セキュアな通信を実現するためには、どのような対策が求められるか。

現状・課題

○　公衆無線LANサービスの利用者や提供者において、暗号化されていない公衆無線LANサービスのリスクが十分に知られておらず、実際にはどのように対策すればいいか分からないという意見が多い。

○　適切なセキュリティ対策を実施している利用者は少なく、利用者への啓発活動や安全な利用形態の情報提供が必要。

○　VPNは安全と言われているが、提供元が不明なVPNサービスもある。VPNサービスの提供元が信頼できるかどうかを慎重に判断することができるよう、利用者に注意喚起をしていく必要がある。

考え方

○　利用者や提供者が、暗号化されていない公衆無線LANサービスのリスクについて判断できるよう、**信頼できる機関からセキュリティ対策に関する情報を発信してはどうか**。

○　よりセキュアな通信を行う場合、その通信が**HTTPS（SSL/TLS）によるものであるか、利用者においてURLを確認**するよう、**利用者への周知・啓発を図ってはどうか**。

○　特にセキュアな通信を行う場合、無線区間における暗号化のほか、VPNによる方法も選択肢の一つとなる。その際、VPNサービス提供者が提供する**VPNアプリの信頼性を担保する仕組みが必要**ではないか。

検討事項2①　利用者・利用シーンに応じた公衆無線LANサービスの提供について

検討事項

○　訪日外国人や観光客、テレワークを行う勤労者等、どのような利用者・利用シーンに対して、どのような公衆無線LANサービスを提供すれば、セキュリティに配慮した公衆無線LANサービスのさらなる普及が図られるか。

現状・課題

○　事業者側のセキュリティ対策について、無料で提供されることも多い公衆無線LANサービスにおいて、どこまで対応できるか、また、対応する必要があるかは大きな課題。

○　既存の「Wi-Fi提供者向けセキュリティ対策の手引き」に実施すべきセキュリティ対策例の記載はあるが、提供者においてどこまで実施すべきか読み取れない。

○　データ利活用のための公衆無線LANサービスのあり方に関するプラスの議論が必要。

考え方

○　セキュアな公衆無線LANサービスは有料、そうではないサービスは利用者自身でセキュリティ対策をする必要があるが無料、という棲み分けも考えられるのではないか。

○　民間主体の取組により、公衆無線LANサービスがセキュアな水準を満たしていることを示すことで、セキュアな公衆無線LANサービスの展開にインセンティブを与える仕組みも考えられるのではないか。

○　セキュアな公衆無線LANサービスと他の施策を連携することにより、地域活性化や利用者への新たな価値創造を加速し、安心・安全な公衆無線LANサービスのさらなる普及を図ってはどうか。

検討事項2② 公衆無線LANサービスの環境整備について

検討事項

○ 公共施設やスタジアム等におけるアクセスポイントの設置について、標準規格の策定動向を踏まえつつ、提供者において、どのようなアクセスポイントの設置形態がセキュリティの観点から望ましいか。

現状・課題

○ 駅などにおける公衆無線LANの4分の1から3分の1程度のトラヒックは、接続手順に係るもの。より効率化することが可能な標準規格が策定されており、標準化の普及が進められている。

○ 米国には約1,800のアクセスポイントを設置したスタジアムがあるが、日本ではこうした環境はまだ整っていない。

○ オリンピック・パラリンピック競技大会等のイベント開催時、公共施設やスタジアム等においては、悪意のある者に偽アクセスポイントを設置されるおそれがある。過去に、リオでは数多くの盗聴目的のフリーWi-Fiの取締りが行われた。

考え方

○ 公衆無線LANサービスの利用が多く見込まれる公共施設やスタジアム等では、セキュリティに配慮した公衆無線LANサービスの環境整備が求められることから、**提供者は、公共施設やスタジアム等に設置されているアクセスポイントを適切に管理することが必要**であり、**利用者には、アクセスポイントが正規のものであるかを確認する方法が求められる**のではないか。一方、悪意のある者が設置した偽アクセスポイント等、いわゆる野良Wi-Fiのセキュリティ対策が必要ではないか。

○ セキュリティとコストのバランスを考慮しつつ、**セキュリティに配慮した公衆無線LAN環境を公共施設やスタジアム等でいくつか整備し、これを模範事例として、全国に広めてはどうか**。また、2020年東京オリンピック・パラリンピック競技大会に向けて、**開催地（東京等）となる自治体において、推奨されるセキュアな公衆無線LAN環境を構築**してはどうか。その際、例えば、組織委員会と連携し、公衆無線LANサービスのESSIDやアプリの情報を、オリンピック・パラリンピック公式サイトといった信頼できるサイトに掲載する仕組みを作ってはどうか。

○ セキュアな公衆無線LAN環境を構築するに当たって、**技術開発要素はあるか**。

関連資料

諸外国の公衆無線LANの整備状況

国・地域	整備の特徴	整備状況（時期）
米国	2000年代半ばから自治体独自の整備。持続可能なサービスモデル模索が続き、最近はサービスのリニューアル事例も見られる。	「コミュニティWi-Fi（各住宅・企業内で運用されている公衆無線LANのホットスポット）」のホットスポット数：3,107万8,609か所、「商用Wi-Fi」のホットスポット数：104万9,151か所（2015年2月）
英国	2012年ロンドン五輪開催でロンドン市での整備が進む。	大手通信事業者のホットスポット数：4万1,798か所（2014年6月）、都市部の公共施設無料ホットスポット数：1,000か所（2015年3月）
フランス	2006年からパリ市等で自治体主導の無料公衆無線LAN整備が進展。	大手通信事業者2社のアクセスポイント数：約800万か所（2014年末）
ロシア	大都市自治体と大手通信事業者が整備。2018年サッカーW杯に備え、モスクワ市が整備中。	国内の公衆無線LANのアクセスポイント数：20万か所（2013年末）
ブラジル	「ユニバーサル・サービス化目標（PGMU）」で、ブロードバンド・サービス品質確保に関する規則があり、通信事業者にアクセスポイントの詳細情報の報告を義務付け。	国内アクセスポイント数：58万6,098か所 うち有料734か所、無料3,903か所、有料無料混合型58万1,461か所（2015年1月）
韓国	2013年から政府の無料「公共Wi-Fi」拡大事業で全国的に整備中。	国内の無料「公共Wi-Fi」拠点数：7,000か所（2014年末）
中国	都市部のオフロードを主目的とする通信事業者による整備が近年活発化。	通信事業3社の加入者向けアクセスポイント数：600万か所
台湾	2011年以降、行政院主導の無料サービス「iTaiwan」と自治体の独自サービスが連携。	国内のiTaiwan拠点数：4,600か所（2014年6月末）
香港	政府がアクセスポイントを設置する一方、民間企業に対してアクセスポイントの開放を求める、官民連携によるサービスの提供。	各種アクセスポイント数の合計：2万8,850か所 うち政府と通信事業者連携の無料アクセスポイント数：5,000か所以上（2014年11月末）

出典：「諸外国の公衆無線LANサービス 整備動向」（平成27年マルチメディア振興センター）http://www.soumu.go.jp/main_content/000351040.pdfを基に作成。

過去のオリンピック・パラリンピック競技大会における公衆無線LANの状況

2012年　ロンドン大会

○　ロンドンの首都圏内に50万ヶ所以上、オリンピック・パーク内に1,500基以上のアクセスポイントを整備(※1)。

○　オリンピック施設と選手村では、選手と家族用にWPA2-PSKの暗号化方式のWi-Fiを整備(※1)。

○　2014年時点で、ロンドン市内のWi-Fiのうち、23%が暗号化なし、6%がWEP、54%がWPA、17%がWPA2(※2)。

2014年　ソチ大会

○　オリンピック施設周辺で約2,500基のアクセスポイントを整備(※3)。

○　US-CERTは、ロシアへ渡航する人に向けて、オリンピックに便乗したサイバー犯罪のおそれがあると注意喚起(※4) 。

2016年　リオ大会

○　“Sheraton-GuestRoom”といった、ホテルの名前を利用した偽アクセスポイントが設置された(※5)。

○　オリンピック施設周辺のWi-Fiのうち、18%が暗号化なし、7%がWPA、75%がWPA2 (※6) 。

出典

(※1)　https://www.globalservices.bt.com/jp/ja/casestudy/london_2012_wi_fi_access　(BT)

(※2)　https://news.sophos.com/en-us/2014/04/30/how-safe-are-londons-wi-fi-hotspots-see-the-results-of-our-warbiking-ride-video/(Sophos)

(※3)　https://www.avaya.com/blogs/archives/2016/07/avaya-delivers-on-olympic-sized-network.html (Avaya Connected Blog)

(※4)　https://www.us-cert.gov/ncas/tips/ST14-001(US-CERT)

(※5)　https://www.skycure.com/pr/skycure-issues-mobile-travel-advisory-rio-olympic-games-details-riskiest-wifi-hotspots-rio/ (Skycure)

(※6)　https://securelist.com/it-threats-during-the-2016-olympic-games-in-brazil/75045/(Kaspersky Lab)