

公衆無線 LAN セキュリティ分科会 報告書(案)

2018年3月

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

目次

はじめに	1
第1章 公衆無線 LAN の現状	2
1. 1 公衆無線 LAN の概要	2
1. 2 公衆無線 LAN のセキュリティ上の脅威	8
1. 3 公衆無線 LAN のセキュリティ対策の現状	10
第2章 公衆無線 LAN のセキュリティ対策のあり方	15
2. 1 基本的考え方	15
2. 2 認証方式のあり方	18
2. 3 暗号化方式のあり方	20
第3章 セキュリティに配慮した公衆無線 LAN サービスの普及策	22
3. 1 公衆無線 LAN のセキュリティに対する利用者・提供者の意識向上	22
3. 2 データ利活用と連携したセキュアな公衆無線 LAN サービスの普及	26
3. 3 優良事例となるセキュアな公衆無線 LAN 環境の普及	28
第4章 今後の取組	30

はじめに

公衆無線 LAN については、2020 年に開催される東京オリンピック・パラリンピック競技大会に向けて、観光や防災の観点から、その普及が進んでいるが、公衆無線 LAN サービスの中には、セキュリティ対策が十分でないものも多く、公衆無線 LAN サービスを踏み台にした攻撃や情報漏洩等のインシデントが発生することが考えられる。

こうした状況を踏まえ、公衆無線 LAN セキュリティ分科会は、公衆無線 LAN におけるセキュリティ上の課題を整理し、必要な対策について検討を行うことを目的として、サイバーセキュリティタスクフォースの下に開催される会合として、2017 年 11 月に設置された。

本分科会においては、利便性と安全性のバランスに配慮しつつ、公衆無線 LAN のセキュリティ対策のあり方とセキュリティに配慮した公衆無線 LAN サービスの普及策について検討を行った。

検討の結果、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・啓発を図ることが必要であるとされた。

また、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、提供者は多様な方式を提供するなどサービスの選択肢を増やし、利用者がそれらのサービスを適切に選択できる環境を整備することが必要であるとされた。

さらに、自治体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必要なガイドラインの策定や、優良事例となる公衆無線 LAN サービスの環境整備の実証等を推進することが必要であるとされた。

本報告書を踏まえ、公衆無線 LAN サービスに関する利用者・提供者の意識向上、データ利活用施策との連携、優良事例の普及を推進するため、今後の取組として、「セキュアな公衆無線 LAN 環境の実現に向けた行動計画」を策定することとし、これにより公衆無線 LAN サービスの利便性と安全性の向上が図られるとともに、新たなサービスの創出や地域活性化が進むなど、公衆無線 LAN サービスの健全な発展が期待される。

第1章 公衆無線 LAN の現状

1.1 公衆無線 LAN の概要

(1) 公衆無線 LAN の概要

公衆無線 LAN¹は、電気通信事業者や自治体等のサービス提供者が無線 LAN のアクセスポイントを設置して、飲食店や宿泊施設、交通機関、競技場等においてインターネット接続サービスを提供するものとして、その普及が進んでいる。(図1-1)

一般に、無線 LAN を指す用語として、Wi-Fi²を用いることも多い。



図1-1 公衆無線LANの利用イメージ³

公衆無線 LAN の特徴として、

- ①誰でも使えるアンライセンスバンドであること(2.4GHz 帯又は 5GHz 帯)、
- ②利用者が使っている端末が世界中の Wi-Fi スポットで利用できるデファクトスタンダード

¹ LAN:Local Area Network の略。

² Wi-Fi(Wireless Fidelity)とは、無線 LAN 技術の推進団体である Wi-Fi Alliance による相互接続性の認定テストによって、一定レベルの相互運用性が保証されているもの。Wi-Fi Alliance は、1999 年に WECA(Wireless Ethernet Compatibility Alliance)の名称で設立され、2000 年3月から様々な機器の相互認証の認定業務を開始し、2002 年 10 月に現在の Wi-Fi Alliance に改名された(小林忠男監修・無線LANビジネス推進連絡会編『Wi-Fi のすべて』リックテレコム、6ページ参照)。

³ 図の出典は、公衆無線 LAN セキュリティ分科会(第1回)資料1-2。アクセスポイントの写真は「カシマスタジアムに高密度 Wi-Fi を導入・・・22 日のセビージャ戦から各種サービスを開始へ」
<https://www.soccer-king.jp/news/japan/jl/20170721/615811.html>

- ドであること、
- ③一つのアクセスポイント当たりのサービスエリアは数十メートルと狭いが、高速・大容量の通信が可能であること、
- といった点が挙げられる。【資料1】

こうした特徴から、誰もが自らのスマートフォンやパソコン等の端末を公衆無線 LAN のアクセスポイントに接続することにより、インターネット環境を利用することができる。

(2) 無線 LAN の普及の経緯

ア) 無線 LAN の普及の三段階

無線 LAN の普及は、大きく三つの段階に分けることができる。(図1-2)

第1段階においては、1999 年の IEEE802.11b の標準化により、家庭内・企業内において無線 LAN が普及した。

第2段階においては、ノートパソコンやゲーム機等に Wi-Fi チップが搭載され、Wi-Fi のモバイル利用が可能となり、公共インフラ化するようになった。また、2002 年頃から、通信事業者が公衆無線 LAN サービスを開始し、駅・空港・宿泊施設・飲食店等において、公衆無線 LAN サービスが普及した。

第3段階においては、スマートフォンの普及を契機として、無線通信トラヒックのオフロード対策の進展等により、公衆無線 LAN が急速に拡大した。

そして、公衆無線 LAN は、観光・防災等、街づくりに不可欠な社会基盤へと進化し、その利用者数は引き続き増加傾向にあり、国内における 2020 年度末時点の利用者数は、約 6,400 万人(2016 年度末時点で約 4,300 万人)と予測されている。【資料 2】



図1-2 無線LANの普及の三段階

近年、駅・空港・宿泊施設・飲食店等に導入する事例が多く見られ、自治体においても、地域活性化のツールとして公衆無線 LAN の整備が進んでいる。また、訪日外国人旅行者にとっても、利用できる場所が十分あることが重要である。

イ) 無線 LAN のさらなる普及の兆し

今後、訪日外国人旅行者の通信手段の確保を目的とした公衆無線 LAN の拡充が求められ、国を挙げて取り組む地方創生・観光立国化、2020 年に開催される東京オリンピック・パラリンピック競技大会の成功に向け、公衆無線 LAN は大きな役割を果たすことが期待されている。

こうした取組の一環として、例えば、訪日外国人旅行者が無料公衆無線 LAN の利用場所がわかりにくいという課題を解決するため、2015 年度より共通シンボルマークである「Japan.Free Wi-Fi」の掲出や、訪日外国人旅行者向けの無料公衆無線 LAN 環境に係る情報(アクセスポイントの場所や SSID⁴等)のウェブサイトへの登録を促進する事業を観光庁が推進している。【資料 3】

また、IoT⁵の普及により、スマートフォンやタブレット端末をワイヤレスでつなぐとともに、家庭内・企業内等に設置されるカメラやセンサー等をワイヤレスでつなぐ手段として無線 LAN の利用は今後ますます広がるものと期待されている。

ウ) 無線 LAN の規格の動向

無線 LAN の規格としては、IEEE802.11b、IEEE802.11a、IEEE802.11g、IEEE802.11n といった規格が策定され、高速・大容量の通信が実現するようになったが、今後、IEEE802.11ac、IEEE802.11ad、IEEE802.11ah、IEEE802.11ax といった規格が普及するものと見込まれている。【資料 4】

また、無線 LAN への接続・認証に要するパケット交換回数を効率化し、接続に要する時間を大幅に短縮させる技術として IEEE802.11ai といった規格が策定されている。これにより、駅や観光施設等の人々が密集する場所や、高速移動時の車内等における無線 LAN の利便性の向上が期待される。【資料 5】

⁴ SSID:Service Set Identifier の略。

⁵ IoT:Internet of Things の略。

(3) 公衆無線 LAN の利用形態・提供形態

ア) 多様な提供主体による公衆無線 LAN サービスの提供

公衆無線 LAN サービスには、電気通信事業者が提供するもの、自治体が提供するもの、空港・鉄道・宿泊施設・飲食店等が主体となって提供するものがある。

公衆無線 LAN のアクセスポイントの整備は、電気通信事業者等によって行われており、例えば、NTT グループは約 16 万のアクセスポイント、KDDI(ワイヤ・アンド・ワイヤレスを含む。)は約 20 万のアクセスポイント、ソフトバンクは約 40 万のアクセスポイントをそれぞれ整備している。【資料 6】

また、アクセスポイント共用化技術を活用することで、電気通信事業者等が整備した一つの公衆無線 LAN のアクセスポイントを複数の公衆無線 LAN サービス提供者で共用することができる。

これにより、エリアオーナーによる積極的な公衆無線 LAN サービスの提供が行われている。一つのアクセスポイントから店舗固有の SSID に加えて電気通信事業者の SSID を用いることにより、電気通信事業者がコストの一部を負担することが可能で、店舗側の負担が軽減されるというメリットがある⁶。

イ) スタジアムにおける公衆無線 LAN 環境

米国のスタジアムでは、公衆無線 LAN 環境の整備が進んでいる。例えば、2014 年に開業した Levi's Stadium(リーバイススタジアム)には 1,200 基のアクセスポイントが設置されており、スマートスタジアムとも言われている。第 50 回スーパーボウル開催時(2016 年 2 月)には、7万人の来場者にインターネットアクセスが提供された。また、2016 年に開業した U.S Bank Stadium には、1,300 基のアクセスポイントが設置されており、6万 6,000 人の来場者が公衆無線 LAN 環境を利用することができる。【資料 7】

国内においても、スタジアムにおける公衆無線 LAN 環境の整備が進んでいる。例えば、西武ドーム球場(現メットライフドーム)では、公衆無線 LAN 環境の整備が 2013 年に行われ、インターネットアクセスを提供するとともに、選手情報やピッチャーとバッターの対戦成績の配信、リプレイ動画の配信等の試合をより楽しくするための試みがなされている。また、2016 年には、NACK5 スタジアム大宮において、高密度公衆無線 LAN サービスの提供が開始されている。今後、2019 年に開催されるラグビーワールドカップや 2020 年に開催される

⁶ 前掲書(脚注2)、48 ページ参照。

東京パラリンピック・オリンピック競技大会に向けたスタジアムの整備において、高密度の公衆無線 LAN サービスが広がっていくものと考えられる⁷。

ウ) 災害時における公衆無線 LAN の利用

公衆無線 LAN は、平時の利用だけでなく、災害発生時には被災者支援に用いることができる。

例えば、2016 年4月に発生した熊本地震の際には、無料の公衆無線 LAN として、携帯電話事業者等による「00000JAPAN」(ファイブゼロ・ジャパン)⁸の提供やエリアオーナーWi-Fi の利用開放、避難所への特設 Wi-Fi の設置などを通じて、被災者の通信環境を確保する取組が実施された。

こうした取組について被災者へのアンケート調査によると、災害時の情報収集や通信手段として「役立った」との回答が9割を超えている一方、「00000JAPAN」の認知と利用状況については、「知っていたし利用した」との回答が 22.5%、「知っていたが利用していない」との回答が 37.1%、「知らなかった」との回答が 40.4%であった。携帯電話等他の通信代替手段が問題なく利用できたことが大きく寄与したと考えられるが、より大きな通信障害が発生した際の公衆無線 LAN の実用性を高めるためには、設置・利用場所の増加と認知度の向上を図る必要がある。【資料 8、資料 9】

⁷ 前掲書(脚注2)、49-50 ページ参照。

⁸ 「00000JAPAN」とは、各事業者が提供する公衆無線 LAN サービスを、大規模災害発生時に被災者の通信接続手段の一つとして利用してもらうことを目的に、災害用の統一 SSID「00000JAPAN」として公衆無線 LAN サービスを提供するものである。本取組は東日本大震災を教訓として始められており、2013 年9月に同災害において被災地となった岩手県釜石市で実証実験が行われた。その後、2014 年5月に正式運用が開始され、熊本地震で初めて実運用に至った。利用者からは電気通信事業者の区別なく簡易に接続できる「00000JAPAN」等の公衆無線 LAN の有用性が挙げられている。

1.2 公衆無線 LAN のセキュリティ上の脅威

(1) 脅威の分類

一般に、公衆無線 LAN におけるセキュリティ上の脅威としては、① 無線区間における通信傍受、② 他の端末からの不正アクセス、③ なりすまし、④ 不正なアクセスポイントの設置等が知られている⁹。(図1-3)

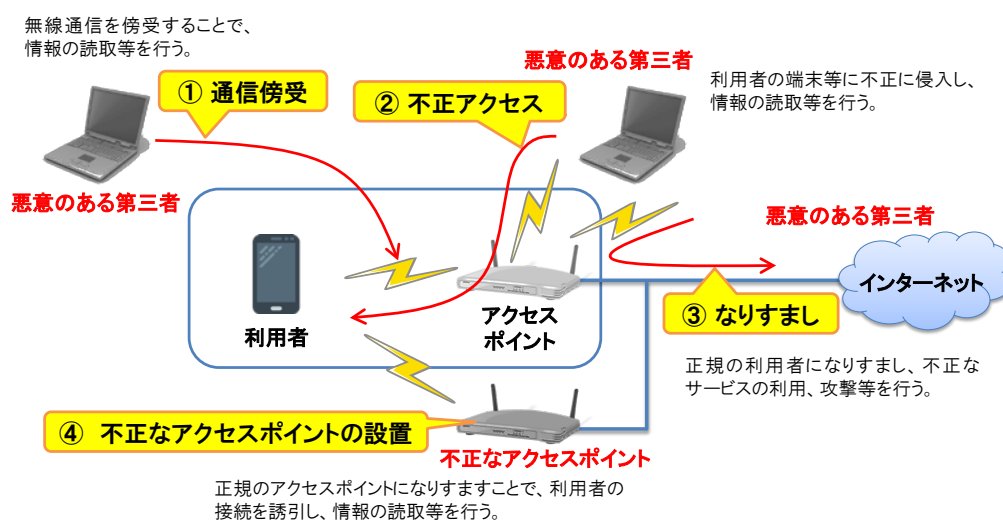


図1-3 公衆無線 LAN におけるセキュリティ上の脅威

① 無線区間における通信傍受

悪意のある第三者が利用者とアクセスポイントとの間の通信内容を傍受することであり、利用者とアクセスポイントの無線区間の通信が暗号化されていない場合、悪意のある第三者によって、その通信内容が窃用されるおそれがある。

⁹ ここでは、無線 LAN ビジネス研究会報告書(2012年7月20日公表)において示されている無線 LAN の情報セキュリティ上の脅威を挙げているが、他にも脅威の分類方法が知られている。例えば、IPA(情報処理推進機構)「公衆無線 LAN 利用に係る脅威と対策」(2016年3月30日公表)においては、公衆無線 LAN における一般的な脅威として、(1)「盗聴」(無線通信を傍受し、窃用すること)、(2)「なりすまし」(第三者が正規の利用者や機器になりすまして不正にサービスを利用すること)、(3)「悪意の AP」(第三者が通信内容を窃取するなど悪意のある目的で設置したアクセスポイント)、(4)「不正目的でのインフラ利用」(掲示板への犯罪予告の書き込みや違法ダウンロードなど、公衆無線 LAN が犯罪のためのインフラとして不正利用されること)が示されている。

<https://www.ipa.go.jp/files/000051453.pdf>

また、公衆無線 LAN セキュリティ分科会(第1回)においては、無線 LAN における主な脅威の分類がより詳細に示されており、(1)経路上の通信傍受、(2)ネットワークへの侵入、(3)DoS/Jamming による通信妨害、(4)アクセスポイント乗っ取り、(5)偽のアクセスポイント設置が挙げられており、あわせて、公衆無線 LAN における主な攻撃の分類とその対策が示されている。【資料 10、資料 11】

② 他の端末からの不正アクセス

悪意のある第三者が利用者の端末などネットワークに不正に侵入し、情報の窃取等が行われるおそれがある¹⁰。

③ なりすまし

第三者が不正に情報入手し、正規の利用者や機器になりすまして、不正なサービスの利用、あるいは攻撃が行われるおそれがある。

④ 不正なアクセスポイントの設置

悪意のある第三者が不正なアクセスポイントを設置し、正規のアクセスポイントになりすますことで、利用者の接続を誘引し、通信内容の傍受等が行われるおそれがある。また、ID やパスワードを窃取する目的で不正なアクセスポイントが設置されることもある。

このように、公衆無線 LAN は誰でも接続できるという利便性を有する一方、様々なセキュリティリスクが存在しており、例えば、利用者の通信内容が傍受され、ID やパスワードが盗まれるおそれがある。また、提供者側のリスクとして、例えば、提供者の設置したアクセスポイントが、迷惑メールの送信や掲示板への悪意ある書き込みに悪用されるおそれがある。【資料 13】

(2) 公衆無線 LAN における認証と暗号化

公衆無線 LAN におけるセキュリティ対策として、認証と暗号化が重要である。

このうち、認証とは、端末やアクセスポイントが接続相手の正当性を確認する仕組みであり、正当性が確認できない相手とは通信できない。認証を行うことにより、接続に係る情報が記録され、不正な端末による接続試行の検知や不正利用発覚後の特定の一助となる。【資料 14】

また、暗号化とは、通信の内容を容易に推定できないようにする仕組みであり、通信の内容を秘匿化するものである。無線区間におけるネットワーク層の様々な暗号化方式や、HTTPS や VPN¹¹といった、より上位層における暗号化方式を用いて、通信の内容を秘匿することができる。【資料 15】

¹⁰ 2016 年1月に発生した佐賀県公立学校の校内ネットワークにおける情報漏洩被害では、無線 LAN のアクセスポイントを介して不正に侵入され、管理者アカウントで管理されていたサーバから情報が盗み出された。【資料 12】

¹¹ HTTPS:Hyper Text Transfer Protocol Secure の略。VPN:Virtual Private Network の略。

1.3 公衆無線 LAN のセキュリティ対策の現状

(1) 提供者における公衆無線 LAN のセキュリティ対策の現状

公衆無線 LAN の利用者が利用しているサービスには、ネットショッピングやネットオークションでの買い物、インターネットバンキングやオンライントレード等の金融関連サービスといった金銭に関するものもある。他方、公衆無線 LAN サービスには、無線区間の通信が暗号化されていないアクセスポイントが存在しており、無線区間におけるネットワーク層の様々な暗号化方式には、既に脆弱性が発見されているものもあることから、利用にあわせて適切な強度の暗号化方式を設定することが望ましい。【資料 16】

ア) 無線区間の暗号化の実施状況等

自治体、空港、宿泊施設における公衆無線 LAN サービスの提供状況に関する調査結果¹²によれば、無線区間の暗号化の実施状況について、自治体は、暗号化している割合(42.0%)と暗号化していない割合(44.9%)は、ほぼ同数である。空港は、暗号化している割合(15.4%)を暗号化していない割合(69.2%)が大幅に上回っている。他方、宿泊施設は、暗号化している割合(57.5%)が暗号化していない割合(28.8%)を上回っている。(図1-4)

無線区間の暗号化がなされていないことにより、公衆無線 LAN で接続している機器同士で、他の通信を盗み見することができる懸念がある。しかし、自治体、空港、宿泊施設において、公衆無線 LAN サービスで接続している端末同士の通信はできないようになっている割合は、それぞれ、79.2%、76.9%、74.3%であり、ネットワーク分離機能やプライバシーセパレータ機能により、一定の対策が行われている。(図1-5)

¹² 総務省「無線 LAN の能率的かつ安全な利用のための情報セキュリティ対策の周知啓発事業」(2017年度)において行った「地方公共団体が提供する「公衆無線 LAN サービス」の概要に関する調査結果」及び「企業・団体等がお客様向けに提供する「公衆無線 LAN サービス」の概要に関する調査結果」によるもの(調査期間:2017年10月30日～同年11月17日)。地方公共団体については、1,741市区町村に調査票を発送した結果、513市区町村(572サービス)から回答があった。空港については、28箇所の空港に調査票を発送した結果、13箇所の空港(13サービス)から回答があった。宿泊施設については、412箇所の宿泊施設に調査票を発送した結果、66箇所の宿泊施設(66サービス)から回答があった。

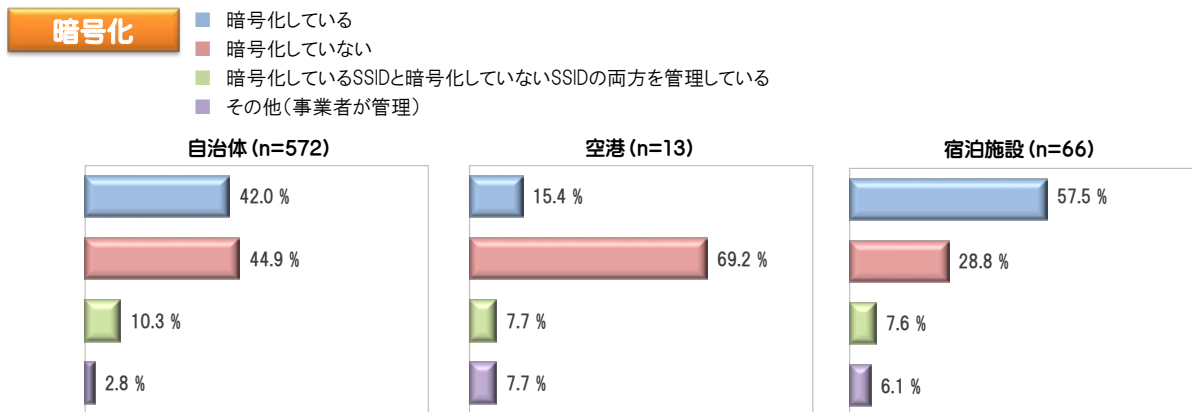


図1-4 暗号化の状況

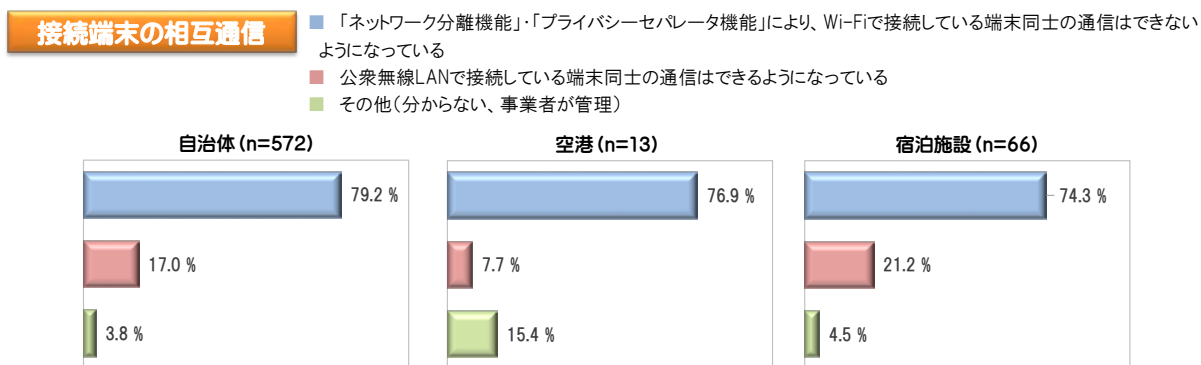


図1-5 接続端末の相互通信の状況

イ) 公衆無線 LAN 機器の設定状況等

公衆無線 LAN 機器(ルータ等)の ID やパスワードを初期設定から変更している割合は、自治体では 72.4%、宿泊施設では 89.4%である。他方、初期設定のまま利用している割合は、自治体では 20.1%、宿泊施設では 9.1%と一定程度ある。(図1-6)

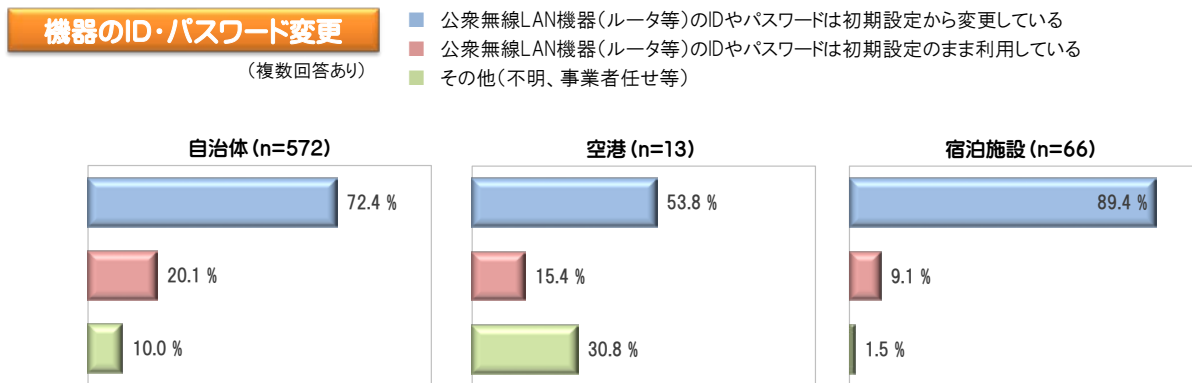


図1-6 機器の ID・パスワード変更の状況

他方、機器ファームウェアの更新は、十分に行われているとは言えない。機器ファームウェアの更新を都度実施している割合は、自治体では 44.4%、宿泊施設では 25.8%であり、比較的、自治体では都度実施している状況にある。1年に1回程度実施している割合は、自治体では 10.0%、宿泊施設では 18.2%であり、一方、実施していない割合は、自治体では 31.3%、宿泊施設では 51.5%である。(図1-7)

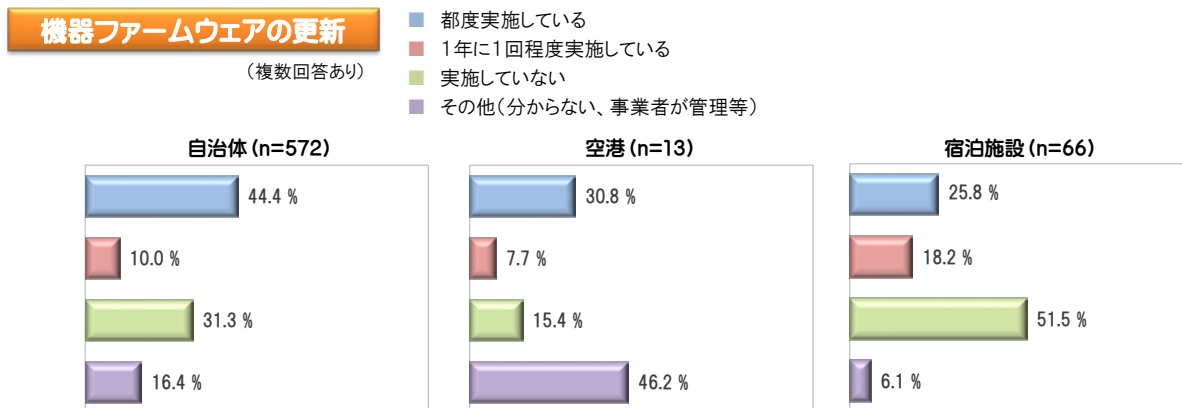


図1-7 機器ファームウェアの更新の状況

ウ) 認証(利用者確認)方法の状況等

公衆無線 LAN サービスの認証方式として、利用登録方式、SMS 連携方式、SNS アカウ
ントを使用した認証方式、メール認証方式等が挙げられる。自治体では、メール認証方式
の割合が最も多く 42.3%である。空港や宿泊施設では利用者の確認はしていない割合が最
も多く、それぞれ 61.5%、90.9%である。(図1-8)

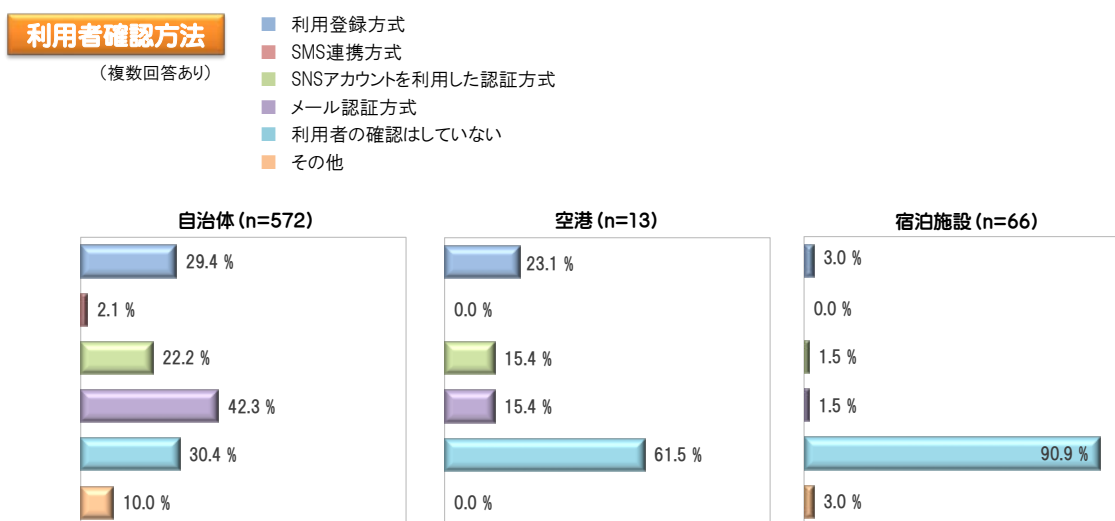


図1-8 利用者確認方法の状況

先の回答で利用者の確認はしていない割合が多かった空港や宿泊施設では、目視や監視カメラにより利用者の出入りを十分把握できる環境で提供している割合が、それぞれ100%、84.8%と非常に多い。他方、自治体では、不特定多数が利用するが、目視や監視カメラにより利用者の出入りを十分把握できる環境で提供している割合は 57.7%にとどまっている。(図1-9)

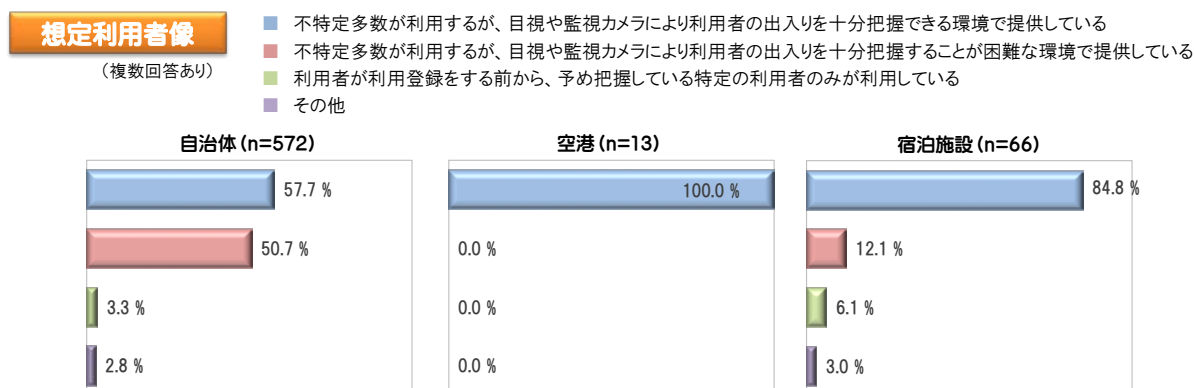


図1-9 想定利用者像の状況

(2) 利用者における公衆無線 LAN のセキュリティに対する意識

公衆無線 LAN の更なる普及が期待される中、公衆無線 LAN の利用において利用者が求める改善点として、「情報セキュリティへの対策の強化」が 65%を占め、最も多い。【資料 17】

公衆無線 LAN 利用時の脅威について、一定の認知はされているものの、セキュリティ対策の実施については低い傾向にあり、特に、日本人についてその傾向が強い。また、「AP (アクセスポイント) の暗号化の種類の確認と適切な対応」や「SSL サイト (HTTPS) の確認と重要な情報入力に係る適切な対応」といった暗号化に関するセキュリティ対策は、十分に実施されているとは言い難い状況にある。【資料 18】

また、約7割の利用者が公衆無線 LAN のセキュリティに「不安を感じている」と回答しており、約5割の利用者は、「不安を感じているが、利用する」と回答している。(図1-10)

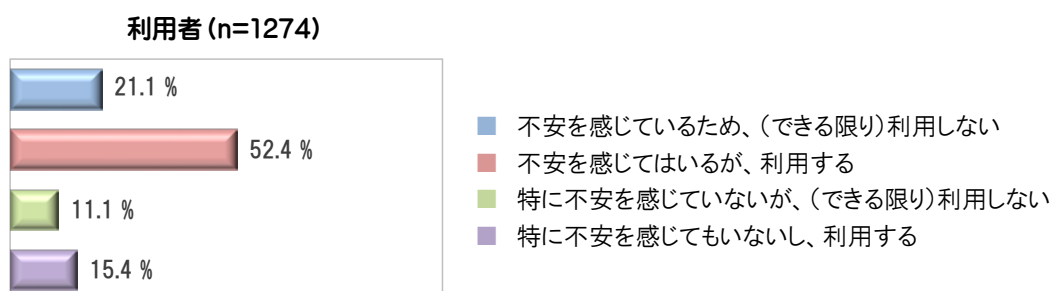


図1-10 利用者における公衆無線 LAN のセキュリティに関する意識

公衆無線 LAN サービスの利用に当たって、セキュリティを高めるための工夫は誰がすべきか(利用者が工夫すべきか、提供者が工夫すべきか)という点については、無料公衆無線 LAN か有料公衆無線 LAN かで分かれている。具体的には、無料公衆無線 LAN の場合、「利用者が工夫すべき」又は「どちらかといえば利用者が工夫すべき」と回答した割合が 62.3%であるのに対し、有料公衆無線 LAN の場合、「公衆無線 LAN サービスの提供者が工夫すべき」又は「どちらかといえば公衆無線 LAN サービスの提供者が工夫すべき」と回答した割合が 68.1%となっている。したがって、公衆無線 LAN 利用者は、総じて無料公衆無線 LAN では利用者が工夫すべきであるが、有料公衆無線 LAN では提供者が工夫すべきという認識が強い傾向にある。(図1-11)

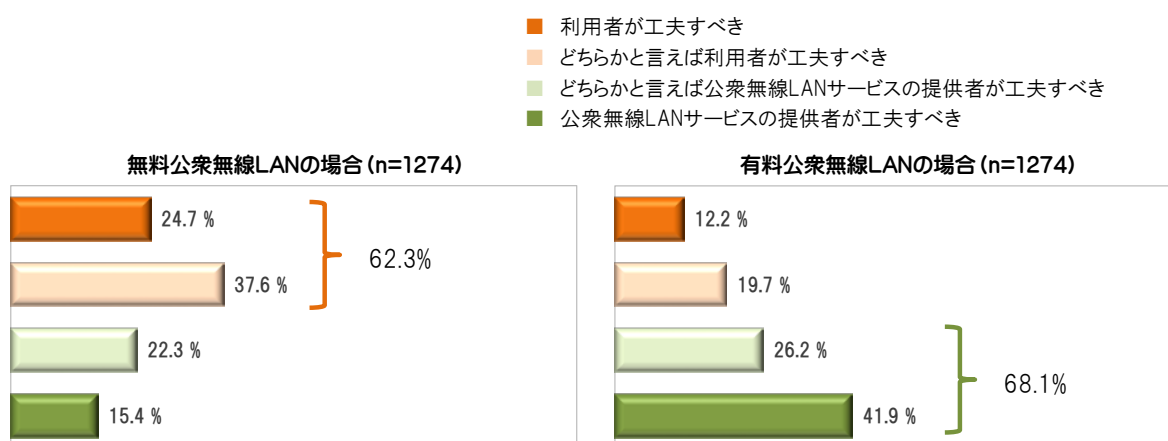


図1-11 公衆無線 LAN のセキュリティを高める主体

(3) 公衆無線 LAN のセキュリティ対策の必要性

これまで見てきたように、公衆無線 LAN の普及の阻害要因の一つに、利用者が抱えるセキュリティに対する不安がある。他方、公衆無線 LAN には、テレワーク環境の提供、リッチコンテンツの配信、観光客向けの観光情報案内、災害等の緊急時における情報提供といった様々なサービスの利用が期待されていることから、利便性と安全性のバランスに配慮し、様々な利用者・利用シーンに応じたセキュリティ対策が必要である。【資料 19】

また、サービスの範囲や課金の有無等、様々な公衆無線 LAN の提供形態が存在することから、提供者のビジネス環境等を配慮し、提供形態や目的に応じたセキュリティ対策が必要である。【資料 20】

第2章 公衆無線 LAN のセキュリティ対策のあり方

2.1 基本的考え方

(1) 検討の前提

公衆無線 LAN のセキュリティ対策のあり方を検討するに当たっては、以下の三点を前提とすることが適当である。

- ① 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を行う。
- ② 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(利用シーン)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を行う。
- ③ 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¹³、標準化の動向を踏まえた検討を行う。

(2) 基本的考え方

公衆無線 LAN のセキュリティ対策の基本的な考え方として、以下の三点が挙げられる。

- ① 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・啓発を図ることが求められる。
- ② 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、利用者を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することが必要である。

¹³ 諸外国の公衆無線 LAN の整備状況については、【資料 21】を参照。

- ③ 2020 年に開催される東京オリンピック・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ることが必要である。また、こうした取組を 2020 年以降のレガシーとして確立していくことも重要であり、こうした取組に必要なガイドラインの策定や、優良事例となる公衆無線 LAN サービスの環境整備の実証等を推進することが考えられる。

(3) 公衆無線 LAN サービスの全体像

公衆無線 LAN のセキュリティを考える際には、公衆無線 LAN を取り巻く環境全体を俯瞰して、その対象者に応じた対策を検討することが必要である。例えば、スマートフォン等の端末を利用する「公衆無線 LAN 利用者」、アクセスポイントや VPN・認証サーバを設置する「公衆無線 LAN 提供者」、さらに、サイバー空間において様々なデータ利活用を行う「各種サービス提供者」という三つの類型に整理することができる¹⁴。(図2-1)

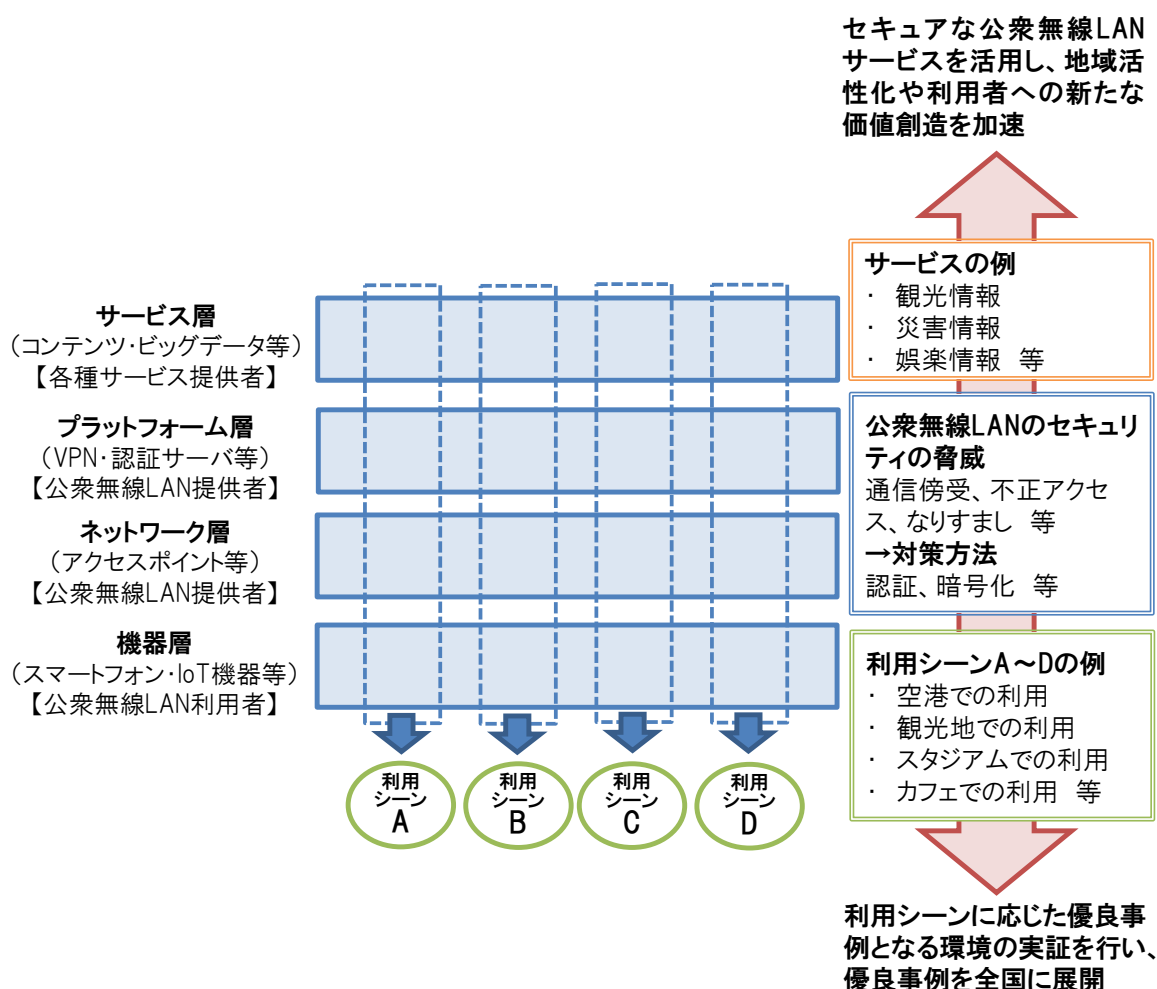


図2-1 利用者・利用シーンに応じたセキュリティ対策の必要性

¹⁴ 公衆無線 LAN セキュリティ分科会では、例えば、ステークホルダごとに、どのような利用動機があり、求められる対策は何かといった事例が提示された。【資料 22】

このような「公衆無線 LAN 利用者」、「公衆無線 LAN 提供者」、「各種サービス提供者」に対する脅威として、例えば、以下の脅威が考えられる。

① 「公衆無線 LAN 利用者」に対する脅威

通信の盗聴や攻撃を受けることが考えられる。また、公衆無線 LAN 利用者のレイヤには、近年急増している IoT 機器も含めることができる。公衆無線 LAN 提供者のアクセスポイントの末端にある IoT 機器が公衆無線 LAN を介して DDoS 攻撃等の踏み台となるおそれもある。

② 「公衆無線 LAN 提供者」に対する脅威

提供しているサービスの品質が落とされることが考えられる。また、偽アクセスポイントの設置のおそれや、アクセスポイントの脆弱性をついたサイバー攻撃が行われるおそれがある。さらに、公衆無線 LAN の提供事業者がアクセスポイント等の機器を提供ベンダーが提供する際、機器そのものに脅威が内包されているおそれがある¹⁵。

③ 「各種サービス提供者」に対する脅威

公衆無線 LAN の接続端末やアクセスポイントからの不正な通信や DDoS 攻撃を受けることが考えられる。公衆無線 LAN サービスがサイバー空間に対して安易な攻撃の可能性を提供するものにならないよう、対策を講ずる必要がある。

このように、さまざまな対象者(ステークホルダ)に対する脅威が存在することを踏まえ、公衆無線 LAN の利用形態や提供形態に応じたセキュリティ対策のあり方を検討する必要がある。

¹⁵ 公衆無線 LAN セキュリティ分科会(第2回)資料2-2スライド8を参照。

2.2 認証方式のあり方

脆弱な認証方式が採用されている場合、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の不正なサービス利用のおそれがある。利用者を認証する方式としては、例えば、Web 認証、SIM 認証、SNS 認証等が挙げられるが、本節においては、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、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について整理を行う。【資料 23】

(1) 課題

① 認証によるトレーサビリティの課題

公衆無線 LAN におけるトレーサビリティの課題として、キャリア Wi-Fi(電気通信事業者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。

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が行われる場合、全体としてのトレーサビリティは弱まることとなり、Level of Assurance (LoA) の確保も難しい。

② 認証方式の課題

IEEE802.1X による認証は、サーバを維持・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¹⁶。

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

③ 接続アプリの課題

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、最近では接続アプリを介して接続するものが多い。しかし、訪日外国人旅行者

¹⁶ IEEE802.1X による認証方式の一つとして、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。

にとって、日本に来る前に事前に国内用の接続アプリを導入する人は少なく、日本に来てからどのように接続アプリを入れるかといった課題がある。また、偽アプリに対する懸念があり、利用者にとって、見知らぬアプリを入れることに抵抗感があるのが一般的である。

他方、信頼に足る接続アプリが普及すれば、セキュアな公衆無線 LAN サービスの利用環境が大きく改善することが期待される。

(2) 考え方

- ① キャリア Wi-Fi では、SIM 認証、携帯電話を ID とした Web 認証、接続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、接続相手の正当性を確認することができ、一定のトレーサビリティも確保できていると考えられる。
- ② 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のほか、認証のないサービスも提供されており、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、利用環境によっては、公衆無線 LAN を誰が利用していたかを何らかの手段(防犯カメラ等)で補完することにより、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一助となる。あるいは、本人確認性を高めたい場合は、二要素認証¹⁷も選択肢の一つとなると考えられる。
- ③ 利用者が接続アプリを入れるという手間がかかる一方、接続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、接続アプリによる接続は選択肢の一つとなると考えられる。その際、接続アプリの信頼性を担保する仕組みが必要である。

¹⁷ 二要素認証は、種類の異なる二つの情報を用いて認証を行う方式。一般に、要素(認証に用いる情報)は三つに分類される。三つとは、記憶情報(ユーザが知っていることに基づく情報: Something You Know)、所持情報(ユーザが持っているものに基づく情報: Something You Have)、生体情報(ユーザの身体的特性に基づく情報: Something You Are)である。一例として、記憶情報としてパスワード、所持情報としてスマートフォン等の端末情報、生体情報として指紋が挙げられる。公衆無線 LAN における二要素認証の方法として、例えば、記憶情報(パスワード)と所持情報(携帯電話番号等)を組み合わせることができる。

2.3 暗号化方式のあり方

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。このため、情報漏洩等のインシデント対策として、クライアント(端末)とアクセスポイントとの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。【資料 24、資料 25】

しかしながら、無線区間におけるネットワーク層の暗号化方式の中には、既に脆弱性が発見されているものもある。また、上位層で暗号化を行う SSL/TLS 通信においても、様々な脆弱性が発見されている。

例えば、2014 年 10 月、米 Google 社は、HTTPS 通信等に用いられる SSL3.0 に「POODLE」という脆弱性があることを発表した。また、2017 年には、無線区間の通信の暗号化に用いられる WPA2 に「KRACKs」¹⁸という脆弱性が発見されたと報道された。Wi-Fi Alliance は、異なる鍵交換の仕組みを採用するなど、より改良された WPA3 を発表し、その詳細は 2018 年中に公表予定としている。【資料 26、資料 27】

本節においては、こうした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について整理を行う。

(1) 課題

- ① 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わからないという意見が多い。
- ② 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、さらなる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である。
- ③ 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。

¹⁸ WPA2 に 10 個の脆弱性が発見され、それぞれが KRACK (Key Reinstallation Attack: 鍵再インストール攻撃)によるものであるため、KRACK の複数形として KRACK s と呼ばれている。

(2) 考え方

- ① 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適時適切に発信することが求められる¹⁹。
- ② よりセキュアな通信を行う場合、その通信が HTTPS(TLS²⁰)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・啓発を図ることが適当である。
- ③ 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（VPN サービスの形態として、端末からインターネットのクラウド上までの通信を暗号化するコンシューマ向けのサービスがある。）。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ある。例えば、VPN サービス提供者は、VPN アプリに関する要件や仕様を明示して、利用者が判断できる状態にする方法が考えられる。

¹⁹ 例えば、2017 年 10 月 16 日(米国時間)に無線 LAN(Wi-Fi)の暗号化規格である WPA2 における脆弱性が公開されたことを受けて、様々な機関から注意喚起等がなされた。

IPA(情報処理推進機構)は、「WPA2 における複数の脆弱性について」という注意喚起を行った(2017 年 10 月 17 日公表、同年 10 月 18 日更新、同年 11 月 10 日最終更新)。

https://www.ipa.go.jp/security/ciadr/vul/20171017_WPA2.html

国内で使用されているソフトウェアなどの脆弱性関連情報とその対策情報を提供し、情報セキュリティ対策に資することを目的とする脆弱性対策情報ポータルサイトである JVN(Japan Vulnerability Notes)は、「Wi-Fi Protected Access II (WPA2) ハンドシェイクにおいて Nonce およびセッション鍵が再利用される問題」について、情報を発信した(2017 年 10 月 17 日公表、同年 12 月 11 日最終更新)。

<https://jvn.jp/vu/JVNVU90609033/index.html>

総務省は、「無線 LAN(Wi-Fi)暗号化における脆弱性について」という注意喚起を行った(2017 年 10 月 18 日公表)。

http://www.soumu.go.jp/menu_kyotsuu/important/kinkyu02_000274.html

²⁰ HTTPS に用いられるプロトコルには SSL(Secure Sockets Layer)と TLS(Transport Layer Security)があるが、SSL には脆弱性があることが発表されており、TLS であることが適当である(2018 年3月時点において、TLS1.2 が最新バージョンである。)。

第3章 セキュリティに配慮した公衆無線 LAN サービスの普及策

本章では、訪日外国人旅行者、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について整理を行う。

また、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について整理を行う。

3.1 公衆無線 LAN のセキュリティに対する利用者・提供者の意識向上

(1) 公衆無線 LAN のセキュリティに関する周知・啓発

総務省は、Wi-Fi(無線 LAN)の安全な利用について「Wi-Fi 利用者向け簡易マニュアル」(2014年4月策定、2015年3月改定)や「Wi-Fi 提供者向けセキュリティ対策の手引き」(2014年4月策定、2016年8月改定)等を作成し、周知・啓発を実施している。また、これらのマニュアル等は、「国民のための情報セキュリティサイト」にも掲載されている。(図3-1)



図3-1 総務省における周知・啓発の取組

これらのマニュアル等は Wi-Fi の安全な利用を進めるための簡易でわかりやすいツールであるが、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ものの、提供者においてどこまで実施すべきかが読み取れないといった課題も指摘された。

このため、本報告書の内容を踏まえ、総務省において、「Wi-Fi 利用者向け簡易マニュアル」や「Wi-Fi 提供者向けセキュリティ対策の手引き」を改定し、具体的なセキュリティ対策の事例を紹介する等、公衆無線 LAN サービスのセキュリティに関するさらなる周知・啓発を図ることが適当である。また、公衆無線 LAN サービスを利用する青少年を対象としたセキュリティ対策の利用マニュアルを新たに策定し、周知・啓発を図ることが適当である。あわせて、「国民のための情報セキュリティサイト」のコンテンツの充実を図ることが適当である²¹。

さらに、オンライン教育等(例えば、放送大学や「gacco」²²)の教育コンテンツを活用した公衆無線 LAN の利活用やセキュリティに関する周知・教育、e-ネットキャラバン²³等の活動を通じた青少年・高齢者向けの公衆無線 LAN の利用に関する周知・啓発等を行うことも考えられる。

こうした取組について、例えば、関係事業者団体等を通じて、公衆無線 LAN の提供者等に情報発信することも有効であると考えられる。また、関係府省や国民生活センター等との情報共有を図ることも有効であると考えられる。

²¹ その他、総務省では、テレワークセキュリティガイドラインを公表しており、2017 年度中に当該ガイドラインを改訂し、公衆無線 LAN をテレワークで使用する際の対策等について記載することとしている。【資料 28】

²² 我が国における大規模公開オンライン講座(JMOOC)プラットフォームの一つである「gacco」では、ビデオ講義とレポート(課題提出)等を組み合わせた本格的でインタラクティブな講座が提供されており、不特定多数を受講対象とした一般公開講座と、受講対象者を特定した利用者限定講座が開講されている。

例えば、総務省に関係する一般公開講座として、「社会人のためのデータサイエンス演習」(2017 年 11 月 28 日開講)、「総務省 ICT スキル総合習得プログラム(e ラーニング編)」(2018 年 1 月 16 日開講)が開講されている(2018 年 1 月現在)。

https://lms.gacco.org/courses/course-v1:gacco+ga063+2017_11/about

https://lms.gacco.org/courses/course-v1:gacco+ga098+2018_01/about

また、セキュリティに関する一般公開講座として、過去に「情報セキュリティ『超』入門」(2015 年 5 月 13 日開講)、「情報セキュリティ「初級」」(2015 年 10 月 8 日開講)が開講された。

https://lms.gacco.org/courses/gacco/ga024/2015_05/about

https://lms.gacco.org/courses/course-v1:gacco+ga045+2015_10/about

なお、「情報セキュリティ「初級」」講座は、2016 年度及び 2017 年度には、政府機関に勤務する職員を対象とした情報セキュリティ研修の教材(利用者限定講座)として、採用されている。

http://gacco.co.jp/news/release/news_20160908.html

²³ e-ネットキャラバンとは、インターネットの安心・安全な利用のために、保護者・教職員等向け及び小学生～高校生向けに実施する啓発・ガイダンスをいう。

(2) 民間主体によるセキュアな公衆無線 LAN の取組

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。

ア) 「公衆無線 LAN 版安全・安心マーク」制度の活用

民間主体の取組の一例として、インターネット接続サービス安全・安心マーク推進協議会²⁴による「公衆無線 LAN 版安全・安心マーク」制度を活用することが考えられる。

これは、インターネット接続サービス安全・安心マーク推進協議会が、従来の「インターネット接続サービス安全・安心マーク」に加え、公衆無線 LAN サービスを提供している事業者や自治体等を対象に、セキュリティ対策や個人情報保護への取組等が一定基準に達している目安である「公衆無線 LAN 版安全・安心マーク」を付与するものである²⁵。【資料 29】

こうした民間主体の取組により、利用者や提供者が、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確認することが可能となるが、現時点においては認知度が高いとは言えない状況にある。このため、総務省においても関係事業者団体の協力等を得ながら、「公衆無線 LAN 版安全・安心マーク」に関する周知・普及を図ることが求められる。

イ) 選択式のセキュリティ機能の提供

また、提供者が無線区間の暗号化を行っていない従来の無料の公衆無線 LAN サービスに加え、新たに無線区間の暗号化に対応した公衆無線 LAN サービスを提供することで、利用者は暗号化あり／無しのサービスを選択することが可能となる。具体的には、次のような選択式のセキュリティ機能の提供が考えられる。

²⁴ インターネット接続サービス安全・安心マーク推進協議会は、一般社団法人日本インターネットプロバイダー協会、一般社団法人テレコムサービス協会、一般社団法人電気通信事業者協会、一般社団法人日本ケーブルテレビ連盟から構成されている。

²⁵ 2018 年1月時点における「公衆無線版 LAN 安全・安心マーク」取得者は、4社(株式会社テルベル(Wi-Fi Air)、株式会社朝日ネット(ASAHI ネットおまかせ Wi-Fi)、株式会社ケーブルテレビ富山(安心・安全ケーブル Wi-Fi)、株式会社エコネット(エコネット Wi-Fi))にとどまっている(括弧内はサービス名を示す)。マークの有効期限は、発行日から起算して1年であり、有効期限満了前に更新審査を受け、合格しない場合には、マークを使用し続けることはできないこととされている。

<https://www.isp-ss.jp/about/>

① 公衆無線 LAN サービスの利用登録時等におけるサービスの選択

利用者は、公衆無線 LAN サービスの利用登録時等に暗号化あり／無しのサービスを選択できるようにすることが考えられる。(図3-2)

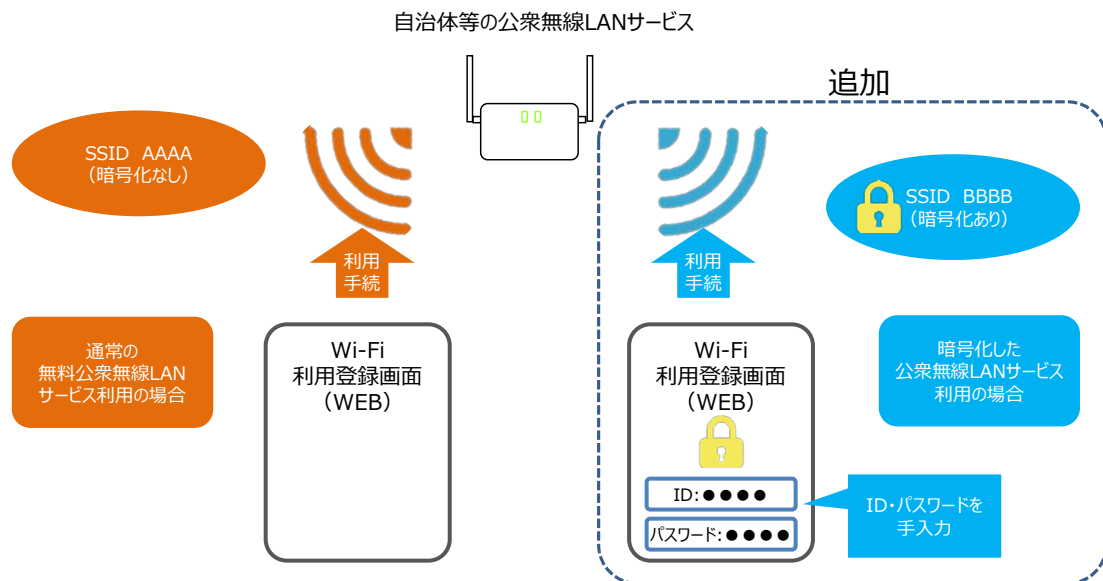


図3-2 選択式のセキュリティ機能の提供(利用登録時等におけるサービスの選択)

② 接続アプリ上でのサービスの選択

サービスの選択をより簡易に実現するために、公衆無線 LAN サービスの接続アプリ上においても暗号化あり／無しのサービスを選択できるようにすることも考えられる。(図3-3)

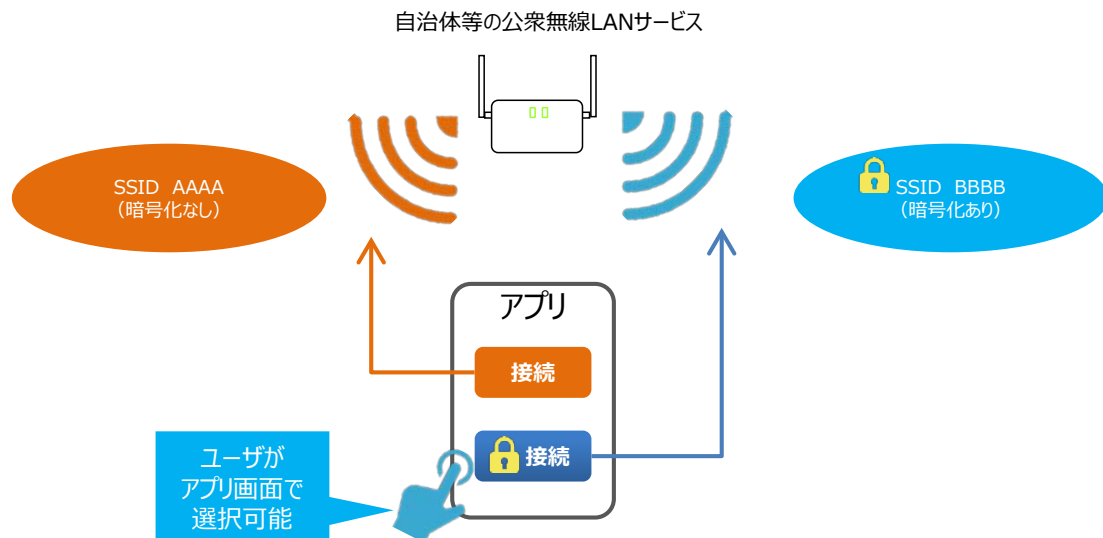


図3-3 選択式のセキュリティ機能の提供(接続アプリによるサービスの選択)

3.2 データ利活用と連携したセキュアな公衆無線 LAN サービスの普及

公衆無線 LAN サービスの普及においては、データ利活用の様々な取組と連携した公衆無線 LAN サービスの提供が考えられる。セキュアな公衆無線 LAN サービスと他の取組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ることが求められる。

(1) 利用者にとって利用しやすいアプリの促進

例えば、利用者にとって利用しやすいアプリの提供を促進することにより、セキュアな公衆無線 LAN サービスの普及を図ることが考えられる。

その際、公衆無線 LAN に接続することだけを目的としたアプリではなく、さまざまなコンテンツサービスのアプリの機能と連携を図ることも利便性の観点から考えられる。

(2) 多様なサービスを提供する情報基盤との連携

公衆無線 LAN サービスのさらなる普及のため、公衆無線 LAN 向けだけに整備した基盤に加え、サービス提供等のために利用者の属性情報の登録された他の情報基盤と連携し、この情報を公衆無線 LAN の認証に活用することも考えられる。

例えば、総務省では、訪日外国人旅行者等のスムーズな移動、観光、買い物等の実現に向け、スマートフォン、交通系ICカードやデジタルサイネージ等と、共通クラウド基盤を活用した多様なサービス連携(個人属性・言語等に応じた情報提供や手続の簡略化等)を実現する、IoT おもてなしクラウドの実用化に向けた取組を行っている。【資料 30～資料 32】

公衆無線 LAN サービスとIoT おもてなしクラウドを連携することにより、例えば、IoT おもてなしクラウドに登録された利用者の属性情報を当該利用者の許諾を前提として、公衆無線 LAN の認証に用いることが考えられる²⁶。(図3-4)

²⁶ 具体的には、IoT おもてなしクラウド事業でも検討されている IoT おもてなしクラウドへの個人の属性情報の登録を行った訪日外国人旅行者等が公衆無線 LAN を使用する際に、公衆無線 LAN サービスがIoT おもてなしクラウドの ID と連携することで、その情報を用いて、認証や暗号化を行う連携が考えられる。

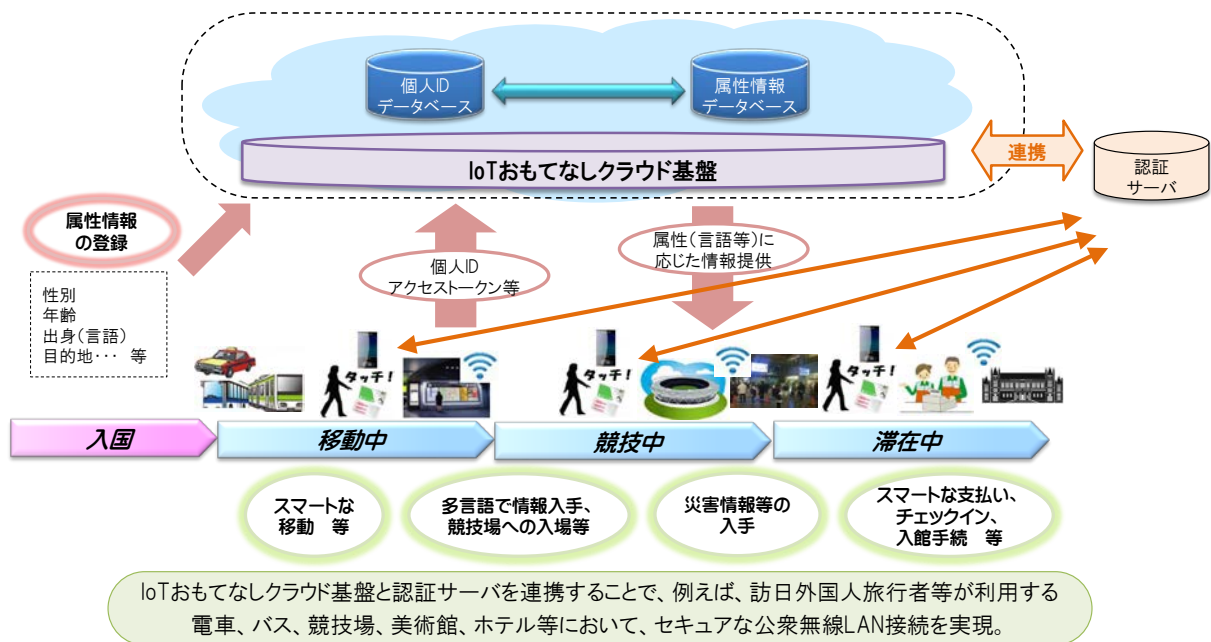


図3-4 公衆無線 LAN サービスとIoT おもてなしクラウドの連携のイメージ

3.3 優良事例となるセキュアな公衆無線 LAN 環境の普及

セキュリティとコストのバランスを考慮しつつ、公共施設等においてセキュアな公衆無線 LAN 環境を整備し、これを優良事例として全国に横展開で広める取組も有効であると考えられる。

(1) 自治体におけるセキュアな公衆無線 LAN の環境整備

総務省では、これまで、自治体における Wi-Fi 環境整備事業を推進しており、2016 年度からは、公衆無線 LAN 環境整備支援事業を行っている。

本事業は、防災の観点から、防災拠点(避難所・避難場所、官公署)等における Wi-Fi 環境の整備を行う地方公共団体等に対し、その費用の一部を補助するものであり、2016 年度は 13 団体に支援を行い、2017 年度は 82 団体(同年6月交付決定分)及び 11 団体(同年 11 月交付決定分)に支援を行っている。【資料 33、資料 34】

本事業では、Wi-Fi 環境を整備する際には、SMS 連携方式による認証方式、SNS アカウントを利用した認証方式及び利用していることの確認を含めたメール認証方式併用のいずれかを原則必要としている²⁷。【資料 35】

引き続き、こうした事業等を通じて優良事例を創出し、自治体におけるセキュアな公衆無線 LAN 環境の整備を進めていくことが必要である。その際には、例えば、各地の優良事例を調査・公表するほか、これを踏まえ、所要の政策支援を行うなど、セキュアな公衆無線 LAN 環境の普及を促進する取組を行うことも考えられる。

(2) 東京オリンピック・パラリンピック競技大会に向けた環境整備

オリンピック・パラリンピック競技大会等の大規模イベントの開催時、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。例えば、リオ大会では、“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²⁸。そこで、2020 年に開催される東京オリンピック・パラリンピック競技大会に向けて、開催地(東京等)となる自治体等において、セキュリティに配慮した公衆無線 LAN 環境を構築することが求められる。

²⁷ ただし、災害時における公衆無線 LAN の開放時や、屋内外問わず、利用者の容姿又は氏名の確認を取ることが可能な場所での使用時(例:学校への来訪者を目視、記録簿、防犯カメラ等により適切に把握できる場合)には、当該認証基準を適用しなくてもよいケースとしている。

²⁸ <https://www.skycure.com/pr/skycure-issues-mobile-travel-advisory-rio-olympic-games-details-riskiest-wifi-hotspots-rio/> (Skycure)

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 環境の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ことが求められる。

利用者側で公衆無線 LAN の接続先が安全なものであるかを確認することができるサービスとして、既に、いくつかのサービスが提供されている。例えば、NTT ドコモは、危険な Wi-Fi スポットに接続した際に情報漏えいを防止する機能のサービスを提供している²⁹。また、国内のセキュリティベンダである FFRI は、接続先の Wi-Fi スポットが安全かどうかをチェックする機能のサービスを提供している³⁰。

また、総務省では、「競技会場における ICT 利活用促進事業」(2017 年度補正予算)を実施することとしている。本事業は、競技会場において無線 LAN やデジタルサイネージ等の ICT を利活用することで、訪日外国人旅行者や障害者等が緊急時の避難情報等に容易にアクセスできるモデルの実証等を通じ、競技会場における ICT 利活用の促進を図るものである。【資料 36】

こうした事業等を通じて、デジタルスタジアムの実現に向けたセキュアな公衆無線 LAN 環境の整備が進むことも期待される。民間事業者等における取組として、優良事例となるセキュアな公衆無線 LAN 環境を実現するデジタルスタジアムを整備し、これを優良事例として全国に横展開する取組も期待される。

その際、例えば、公益財団法人東京オリンピック・パラリンピック競技大会組織委員会と連携し、競技会場等で提供される公衆無線 LAN サービスの SSID 等の情報や接続アプリを、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おいて提供する仕組みを作ることも考えられる。

²⁹ NTT ドコモは、2017 年 12 月 5 日から、Android 向けに、危険な Wi-Fi スポットに接続した際に情報漏えいを防止する機能を有する「セーフ Wi-Fi」を「安心ネットセキュリティ」サービスに追加し、利用者に提供している。

https://www.nttdocomo.co.jp/info/news_release/2017/12/04_00.html

³⁰ 国内のセキュリティベンダである FFRI は、Android 向けに、高度な暗号化方式が採用されている認証方式の Wi-Fi スポットを「安全な Wi-Fi スポット」、そうでないものを「危険な Wi-Fi スポット」としてアプリの画面上部にチェック結果を通知するサービスを提供している。

<http://www.ffri.jp/blog/2016/06/2016-06-15.htm>

第4章 今後の取組

本報告書を踏まえ、今後の取組として、国(総務省)、民間事業者等によるセキュアな公衆無線 LAN 環境の実現に向けた行動計画(別添)を推進していくことが適当である。

セキュアな公衆無線 LAN 環境の実現に向けた行動計画

セキュアな公衆無線 LAN 環境を実現する観点から、産官学の連携により、以下の取組を進めることとし、その進捗状況については本分科会において定期的に検証し、追加的な課題の洗い出しとともに、サイバーセキュリティタスクフォースにおける「IoT セキュリティ総合対策」のプログレスレポートに含めて公表する。

1. 利用者・提供者の意識向上

(国における取組)

- Wi-Fi利用者・提供者向けマニュアル(手引き)の改定(2018年夏頃を目途)【3. 1節】
- オンライン教育等の教育コンテンツを活用した周知・啓発(2018年秋頃を目途に開始)【3. 1節】
- e-ネットキャラバン等の活動を通じた青少年・高齢者向けの公衆無線 LAN の利用に関する周知・啓発(2018年度以降に実施)【3. 1節】
- 「公衆無線 LAN 版安全・安心マーク」に関する周知活動の実施(今後も継続的に実施)【3. 1節】

(民間事業者における取組)

- 暗号化の有無を識別可能な公衆無線 LAN サービスの提供(接続アプリの提供等)(民間事業者の取組に期待)【3. 1節】

2. データ利活用施策との連携

(国・民間事業者における取組)

- 公衆無線 LAN サービスと IoT おもてなしクラウドとの連携推進(2019年中を目途に実用化)【3. 2節】

3. 優良事例の普及

(国・民間事業者等における取組)

- 自治体に対する公衆無線 LAN 環境整備支援事業の継続的推進(2019年度まで継続)及び 優良事例の普及促進(優良事例の調査・公表及びこれを踏まえた所要の政策支援については、2018年夏以降に実施)【3. 3節】
- デジタルスタジアムの実現に向けたセキュアな公衆無線 LAN 環境の整備及び 公衆

無線 LAN サービスの SSID 等の情報や接続アプリを、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おいて提供する仕組みの構築（2018 年度以降に実
施）【3. 3 節】

参考資料

公衆無線LAN (Wi-Fi) の特徴

【資料1】

○ 公衆無線LAN (Wi-Fi)は、誰でも使えるアンライセンスバンド、世界共通どこでも使えるデファクトスタンダード、サービスエリアはスポットで高速通信といった特徴がある。

① 誰でも使えるアンライセンスバンド

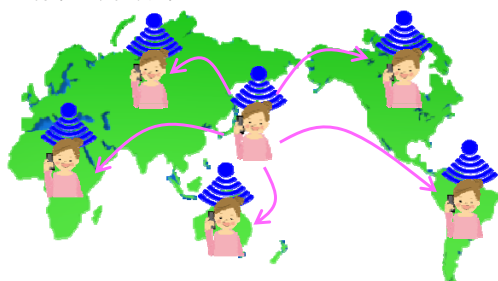
法律上の免許(ライセンス)が不要であることから誰でも手軽に利用できる通信インフラ

オーナーが自由にネットワーク構築



② 世界共通どこでも使えるデファクトスタンダード

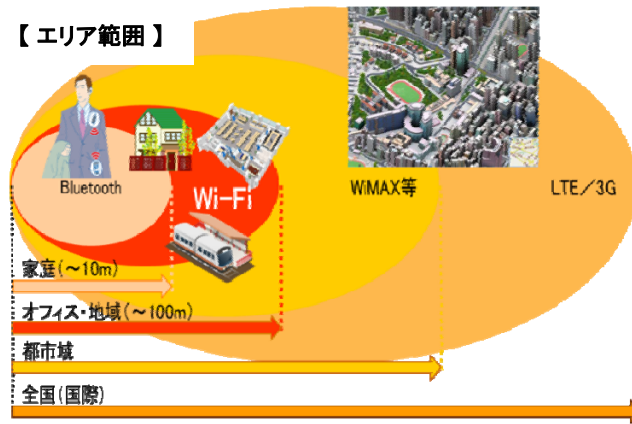
普段使っている端末が、世界中のWi-Fiスポットで利用できる



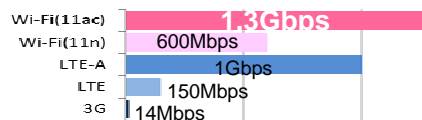
③ サービスエリアはスポットで高速通信

エリア範囲は狭いが、高速・大容量の通信ができる

【エリア範囲】

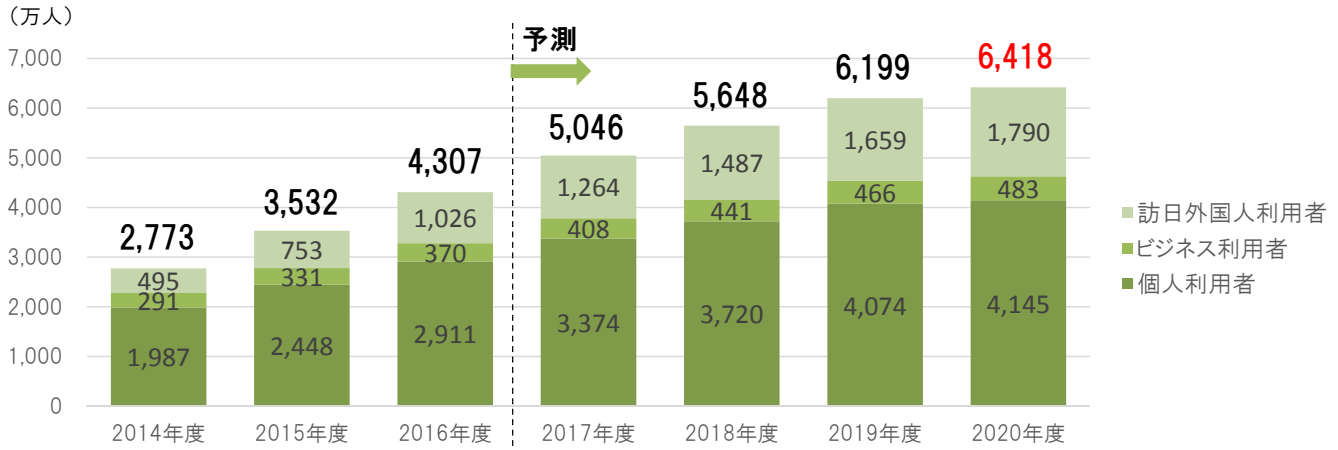


【通信速度】



○ 公衆無線LANは、観光・防災等、街づくりに不可欠な社会基盤へと進化し、その利用者数は引き続き増加傾向にあり、国内における2020年度末時点の利用者数は、約6,400万人(2016年度末時点で約4,300万人)と予測されている。

公衆無線LANサービスの利用者数の予測



(注1) 日本在住の個人・ビジネス利用者は、各年度末の利用者数。2017年度以降は予測値。
 (注2) 日本在住の個人・ビジネス利用者の定義は、1か月に1回以上利用するアクティブユーザー。
 (注3) 訪日外国人利用者の定義は、訪日時に1回以上利用したユーザーの年間合計数。

「2017年公衆無線LAN利用者動向調査」(ICT総研)
<http://ictr.co.jp/report/20170921.html> を基に作成。

出典：公衆無線LANセキュリティ分科会(第1回)資料1-2

無料公衆無線LANに関する周知・広報の取組

○ 訪日外国人旅行者が無料公衆無線LANの利用場所がわかりにくいという課題を解決するため、2015年度より共通シンボルマークである「Japan.Free Wi-Fi」の掲出や、無料公衆無線LAN環境に係る情報のウェブサイトへの登録を促進する事業を観光庁が推進。

シンボルマーク

(1)シンボルマークの普及促進

訪日外国人旅行者が無料で公衆無線LAN環境を利用できるスポットに対して、視認性を高めるための共通シンボルマークの普及を促進する。

○共通シンボルマークデザイン



< 共通シンボルマークの掲出基準 >

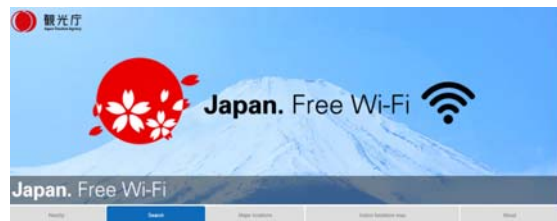
- ①利用者の費用
無料であること(利用手続きの費用も含む)。なお、接続時は無料で、一定期間を過ぎると有料の契約を促すものについては対象とする。
- ②利用手続き
訪日外国人旅行者が容易に利用できること。なお、初期画面や同意画面がある場合は、多言語による案内情報が含まれること。

ウェブサイト

(2)国内外への情報発信

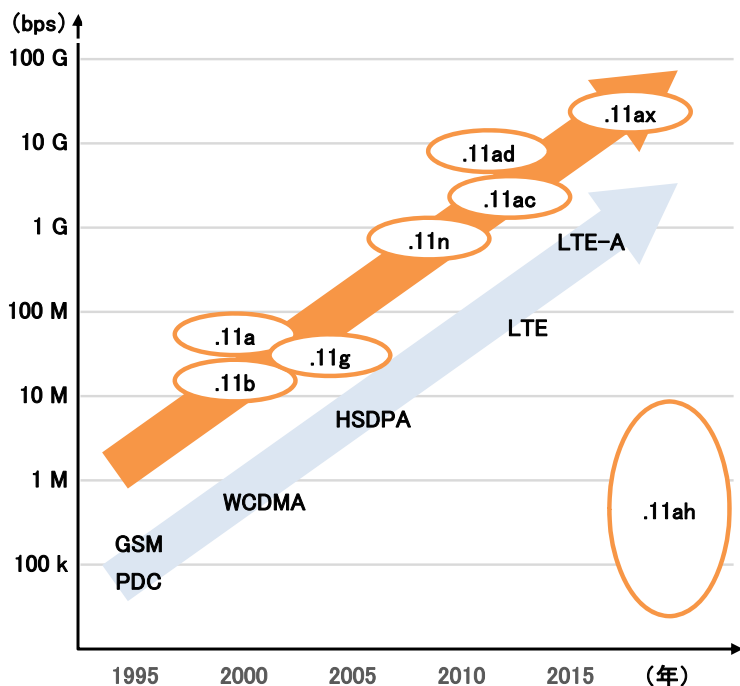
訪日外国人旅行者に対して、無料公衆無線LAN環境に係る情報を幅広く周知・広報するため、ウェブサイトを作成。官民連携による情報発信を進める。

<http://japanfreewifi.jnto.go.jp/eng/wifi-spot-list.php?location=curp>



- ・登録アクセスポイント数は14万超、事業者数は1500超(2018年1月時点)
- ・場所やSSIDに加え、利用方法やサポートする言語も掲載
- ・掲載情報はオープンデータとして提供

○ 無線LANの規格としては、IEEE802.11b、IEEE802.11a、IEEE802.11g、IEEE802.11nといった規格が策定され、高速・大容量の通信が実現するようになったが、今後、IEEE802.11ac、IEEE802.11ad、IEEE802.11ah、IEEE802.11axといった規格が普及するものと見込まれている。



規格名	最大通信速度	使用周波数帯
IEEE802.11b	11 Mbps	2.4 GHz
IEEE802.11a	54 Mbps	5 GHz
IEEE802.11g	54 Mbps	2.4 GHz
IEEE802.11n	600 Mbps	2.4 / 5 GHz
IEEE802.11ac	6,900 Mbps	5 GHz
IEEE802.11ad	6,800 Mbps	60 GHz
IEEE802.11ah	150 kbps~2.7 Mbps	920 MHz
IEEE802.11ax	10,000 Mbps	5 GHz

- .11ac: .11nを拡張し、MU-MIMO機能の搭載により、通信速度の向上・大容量化を実現
- .11ad: 60GHz帯を利用することで、.11acよりも高速化
- .11ah: 920MHz帯(日本)を利用することで、低速であるが到達距離の向上・省電力化を実現
- .11ax: OFDMA(直交周波数分割多元接続)技術等の適用により、スループットを4倍以上に向上(策定中)

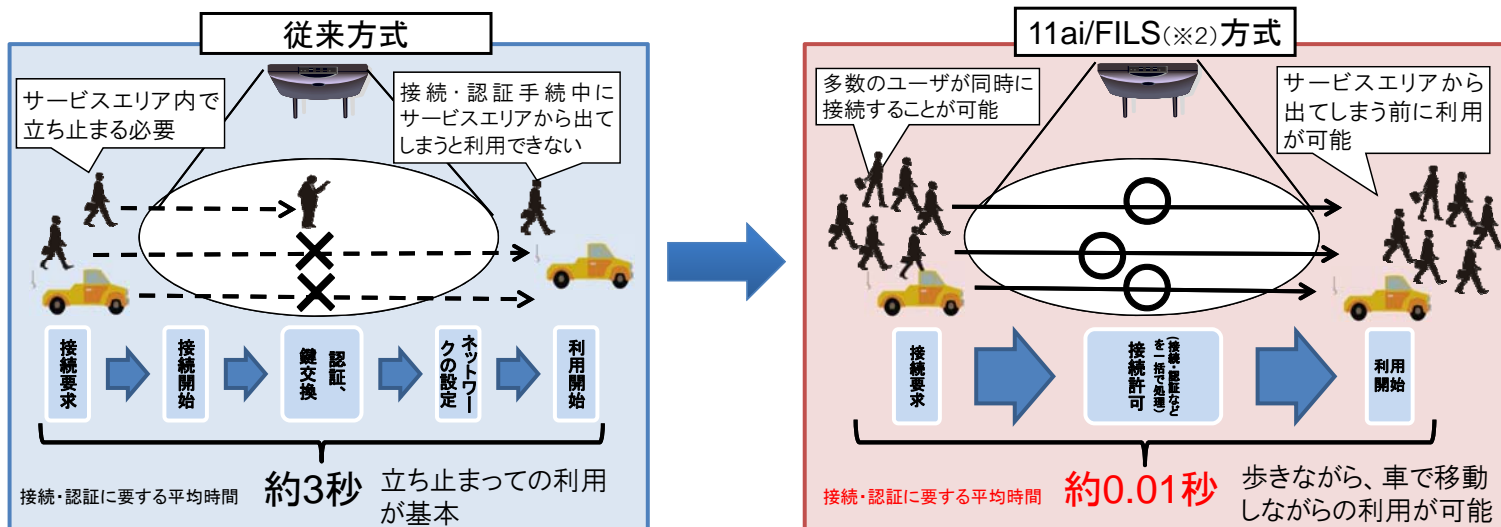
小林忠男監修・無線LANビジネス推進連絡会編『Wi-Fiのすべて』(リクテレコム)を基に作成。

IEEE802.11aiの概要

【資料5】







- 無線LANへの接続・認証に要するパケット交換回数を効率化し、接続に要する時間を大幅に短縮させる技術としてIEEE802.11aiといった規格が策定されている。これにより、駅や観光施設等の人々が密集する場所や、高速移動時の車内等における無線LANの利便性の向上が期待される。
- セキュリティの堅牢さを損なわず、混雑した環境での不要な電波の利用を削減するなどの特長を有する。
- 我が国の発案で、2016年12月にIEEE802.11にて、標準化完了。Wi-Fi Allianceで最優先機能として標準化プログラム(OCE※1)が2018年にリリースされる予定。

(※1) OCE : Optimized Connectivity Experience



(※2) FILS : Fast Initial Link Setup

○ NTTグループは約16万のアクセスポイント、KDDI(ワイヤ・アンド・ワイヤレスを含む。)は約20万のアクセスポイント、ソフトバンクは約40万のアクセスポイントをそれぞれ整備している。

	NTTグループ	KDDI (ワイヤ・アンド・ワイヤレス)	ソフトバンク
スポット数	16万 ※提供エリアの詳細公開中 東急電鉄、阪急電鉄、阪神電気 鉄道等で事業者連携を実施	20万 ※提供エリアの詳細公開中 JR西日本、スターバックス、ビック カメラ等で事業者連携を実施	40万 ※提供エリアの詳細公開中 東京ガーデンテラース、日産スタジアム、 京セラドーム等と事業者連携を実施
利用可能場所 の例	 ※ 自治体、鉄道・空港、 商業施設等エリア	 ※ 自治体、鉄道、商業施設エリア + KDDI グループのエリア	 ※ 自治体、SA/PA、商業施設エリア + ソフトバンクのエリア
利用手続	<ul style="list-style-type: none"> 利用していることの確認を含めたメール認証方式等 接続アプリのダウンロード 	<ul style="list-style-type: none"> 利用していることの確認を含めたメール認証方式等 接続アプリのダウンロード 	無料電話の発信 (必要なパスワードを入手)
開始時期	平成25年11月	平成26年12月	平成27年7月
利用時間	個別 (エリアオーナーによる)	無制限 ※ID有効期間 2週間 (更新可)	無制限 ※ID有効期間 2週間
サービスロゴ	 ※Wi-Fi接続アプリ	 ※Wi-Fi接続アプリ	

無料公衆無線LAN整備促進協議会第4回幹事会資料を基に作成。

スタジアムにおける公衆無線LAN環境

○ 近年、競技場では、カバーする範囲を縮小したアクセスポイントを多数設置することで利用者あたりの通信容量を向上し、多数の来場者による利用に係る通信容量の不足や無線通信の混雑といった問題に対応している。

米国の事例

- **Levi's Stadium**(2014年7月オープン) : 1,200基のアクセスポイントを設置することで、第50回スーパーボウル開催時(2016年2月)には、7万人の来場者にインターネットアクセスを提供。
- **U.S. Bank Stadium** (2016年7月オープン) : 理論上は1,300基のアクセスポイントにより全6万6,000人の来場者が無線LANを利用可能。
- **SunTrust Park** (2017年2月オープン) : 設置するアクセスポイント数は700基程度の規模であるが、Levi's Stadiumの40Gbpsを大きく上回る100Gbpsの回線設備を2式導入することで、20Mbps~200Mbpsの実効速度を実現。

日本の事例

- 日本では、西武ドーム球場やNACK5スタジアム大宮等において、インターネットアクセスを提供。
- さらに、アプリを用いて、競技と連動したエンターテインメントサービスや位置案内サービス等も提供。

競技と連動したエンターテインメントサービスの例



「スーパーボウルで実証、世界最強「ITスタジアム」」(日経産業新聞)(2016年8月9日)
 「ITスタジアム頂点競う、米、スマホで楽しみやすく、USバンク・スタジアム、Wi-Fi接続1300基」(日経産業新聞)(2016年12月7日)
 「エヌ・ティ・ティ・ブロードバンドプラットフォーム株式会社、西武ドームにおける「スタジアム Wi-Fi ソリューション」導入」(Cisco)
https://www.cisco.com/c/ja_jp/solutions/service-provider/mobility/case-studies/0907-wifi-nttbp-cs.html
 「NACK5スタジアム大宮 高密度Wi-Fiサービス「ARDIJA FREE Wi-Fi」開始のお知らせ」
<https://www.ardija.co.jp/news/detail/10856.html>
 「西武ドームにおけるスタジアムエンターテインメントサービスの拡充について ~日本初、スマートフォン向け実況解説付きマルチビュー映像配信~」
<http://www.ntt-bp.net/articles/news/?p=1546> を基に作成。

- 2016年4月に発生した熊本地震の際には、無料の公衆無線LANとして、携帯電話事業者等による「00000JAPAN」の提供やエリアオーナーWi-Fiの利用開放、避難所への特設Wi-Fiの設置などを通じて、被災者の通信環境を確保する取組が実施された。
- 災害時における「00000JAPAN」の認知と利用状況の調査した結果、「知っていたし利用した」と回答したのは22.5%、「知っていたが利用していない」と回答したのは37.1%、「知らなかった」と回答したのは40.4%であった。
- 携帯電話等の他の代替手段が問題なく利用できたことが大きく寄与したと考えられるが、より大きな通信障害が発生した際のWi-Fiの実用性を高めるためにも、設置・利用場所の増加と認知度向上を進める必要がある。

利用された公衆無線LAN	数	備考
「00000JAPAN」 (ファイブゼロ・ジャパン)	九州全域で最大約55,000のアクセスポイントを利用開放	通常、有料で提供している公衆無線LANサービスを災害用統一SSID「00000JAPAN」の名称で無料開放する取組を実施
エリアオーナーWi-Fiの利用開放	15,000以上のアクセスポイントにおいて実施	九州全域でエリアオーナー(自治体、コンビニエンスストア)が設置したアクセスポイントを登録手続なしで利用できる取組を実施
避難所への特設Wi-Fiの設置	最大602箇所、752のアクセスポイントを設置	避難所に臨時の公衆無線LANを設置
くまもとフリーWi-Fi	170箇所にアクセスポイントを設置	通常、メールアドレスの登録が必要になるが、一部のアクセスポイントで登録手続なしで利用できる取組を実施

総務省「熊本地震におけるICT活用状況に関する調査」(平成28年)
「情報通信白書」(平成29年度)225-226ページを基に作成。

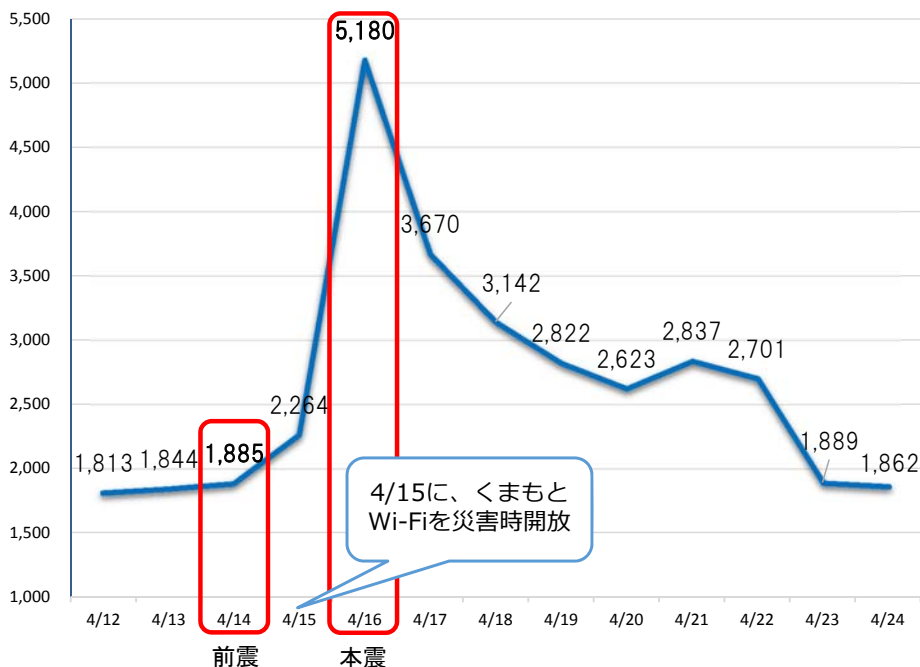
熊本地震における公衆無線LANの利用②

【資料9】

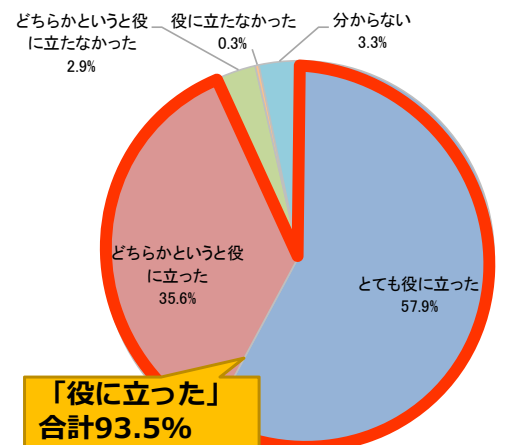
- くまもとフリーWi-Fiへのアクセスは、熊本地震発生後、急増。2016年4月16日は、5000回を超えており、災害時に公衆無線LANが積極的に活用されている。
- 災害時の情報収集や通信手段として「役に立った」との回答が約9割を超えている。

(縦軸:
無料インターネット
利用回数)

くまもとフリーWi-Fiの利用状況の推移



Wi-Fiは、災害時の情報収集や通信手段として役に立ったか？
(n=306)



2017年3月「熊本地震における被災地のWi-Fi利用状況等に係る調査研究」を基に作成。

○ 無線LANにおける主な脅威として、経路上の通信傍受、ネットワークへの侵入、DoS/Jammingによる通信妨害、アクセスポイント乗っ取り、偽のアクセスポイント設置が挙げられる。

DoS : Denial of Service

種別	要因	イメージ図
脅威1 経路上の通信傍受	通信暗号強度	
脅威2 ネットワークへの侵入	アクセスポイントの認証強度	
脅威3 DoS/Jammingによる通信妨害	脆弱な規格の使用	
脅威4 アクセスポイント乗っ取り	アクセスポイントの脆弱性・設定	
脅威5 偽のアクセスポイント設置	アクセスポイントの設定・管理	

公衆無線LANセキュリティ分科会(第1回)資料1-4を基に作成。

公衆無線LANにおける主な攻撃の分類とその対策

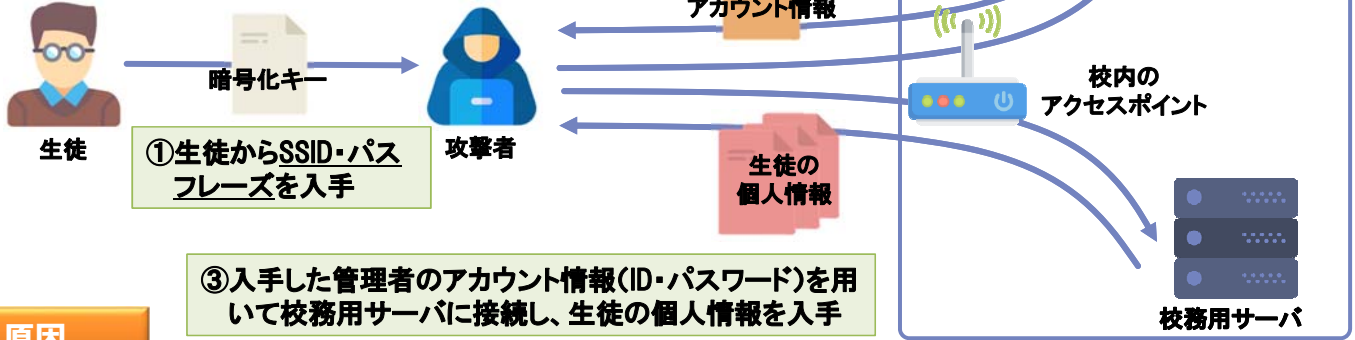
攻撃の種類	攻撃の目的	攻撃の手法	脆弱性	対策
1 MAC Spoofing	DoS なりすまし	① 攻撃者はトラフィックを監視し、接続端末のMACアドレスとアクセスポイントのMACアドレス・SSIDを入手。 ② 正規の接続端末のMACアドレスを詐称し、アクセスポイントに接続。	IEEE802.11規格においてMACアドレスに関するコントロールフレームが保護されていない仕様	IEEE802.11wを利用する / IPSを利用する
2 Evil Twin	盗聴	① 攻撃者は正規のアクセスポイントと同じSSIDの偽アクセスポイントを設置し、正規のアクセスポイントよりも強い電波でビーコンを送信。又は、類似のSSIDの偽アクセスポイントを設置 ② 接続端末のユーザは誤って偽アクセスポイントを選択して接続。	クライアント機器の仕様や利用者の不用意なアクセスポイントへの接続	不用意に不特定多数が利用する環境のアクセスポイントに接続しない
3 Jamming / deauthentication attack	DoS	① 攻撃者はトラフィックを監視し、接続端末のMACアドレスとアクセスポイントのMACアドレス・SSIDを入手。 ② 攻撃者はDisassociationパケットと呼ばれるマネジメントデータフレームを偽装し、アクセスポイントと接続端末に送信。 ③ 接続端末の認証が解除され、接続断。	IEEE802.11規格においてマネジメントデータフレームが認証なしで送信される仕様	IEEE802.11wを利用する
4 Eavesdropping Plain Text (open network)	盗聴	① 攻撃者はトラフィックを監視し、パケットを収集。必要な情報を収集する。	オープンネットワークでは通信が暗号化されていない点	アクセスポイントに暗号化と認証を設定
5 WEP Key Cracking (arp replay)	盗聴	① 攻撃者はトラフィックを監視し、接続端末のMACアドレスとアクセスポイントのMACアドレス・SSIDを入手。 ② 攻撃者はやりとりされるARPパケットを収集し、アクセスポイントに接続端末のARPリクエストを偽造し送信。 ③ 攻撃者は、ARP応答から接続端末への十分な量のIVを収集し、収集したIVを基にWEPの鍵を特定し、トラフィックを復号し、盗聴。	WEPの鍵管理における暗号理論的な脆弱性	WPA2を利用する
6 WPA/WPA2(WPS enabled AP)	盗聴	① 攻撃者はトラフィックを監視し、接続端末のMACアドレスとアクセスポイントのMACアドレス・SSIDを入手。 ② 攻撃者はデータフレームからWPSが有効になっていることを確認。PIN方式の認証における脆弱性を悪用し、認証キーを特定	WPSのPIN方式では容易にブルートフォース攻撃が実行できる	WPS機能を無効にする
7 WPA/WPA2(key bruteforcing)	盗聴	① 攻撃者はトラフィックを監視し、接続端末のMACアドレスとアクセスポイントのMACアドレス・SSIDを入手。 ② 攻撃者はデータフレームからPSKモードであることを確認。 ③ 攻撃者はDisassociationパケットと呼ばれるマネジメントデータフレームを偽装し、アクセスポイントと接続端末に送信。 ④ 攻撃者は認証時のパケットを取得し、オフラインでブルートフォース攻撃を実行して、鍵を特定。	PSK方式において、8~63文字のASCIIコードのパスフレーズを使用	強固なパスフレーズを設定する

公衆無線LANセキュリティ分科会(第1回)資料1-4を基に作成。

- 攻撃者は、入手したSSID・パスワードを用いて、校外からも接続可能な状態にあった校内のアクセスポイントから、校内ネットワークに侵入。窃取した管理者のアカウント情報を用いて校務用サーバにログインし、個人情報にアクセス。生徒の個人情報等が漏洩(学生の個人情報1万4355人分及び成績808人分の流出が確認された。)

事例概要

②入手したSSID・パスワードを用いて校外まで届く無線LANに接続し、管理者のアカウント情報を入手



原因

- 無線LANアクセスポイントから、個人情報を保管した校務用サーバにアクセス可能であった点
- 校務用サーバのアクセス認証が、ID・パスワードのみの管理者のアカウント情報であった点

佐賀県プレスリリース「学校教育ネットワークの不正アクセス事案に係る個人情報関連ファイルの調査結果についてお知らせします」(最終更新日:2016年8月9日)
<http://www.pref.saga.lg.jp/kiji00349832/>
 佐賀県教育委員会事務局「佐賀県学校教育ネットワークセキュリティ対策検討委員会から提言がなされました」(最終更新日:2016年10月28日)
<http://www.pref.saga.lg.jp/kyouiku/kiji00351508/index.html>
 及び「日経NETWORK」(2016年9月号)(日経BP社)を基に作成。

公衆無線LANにおけるセキュリティリスクへの対応

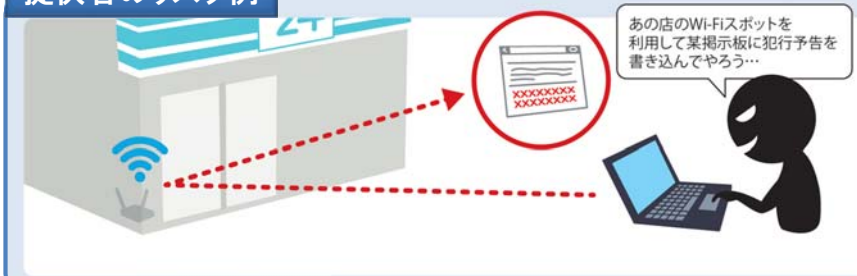
- 公衆無線LANは誰でも接続できるという利便性を有する一方、様々なセキュリティリスクが存在。
- 端末やアクセスポイントの正当性を検証する認証や通信内容の暗号化等を適切に行うことにより、公衆無線LANにおけるリスクを軽減することができる。

利用者のリスク例



- 利用者の通信内容が盗聴され、ID・パスワードが盗まれるおそれ 等

提供者のリスク例



- 迷惑メールの送信や掲示板への悪意ある書き込みに悪用されるおそれ 等

- 認証とは、端末やアクセスポイントが、接続相手の正当性を確認する仕組みであり、正当性が確認できない相手とは通信できない。
- 認証を行うことにより、接続に係る情報が記録され、不正な端末による接続試行の検知や不正利用発覚後の特定の一助となる。

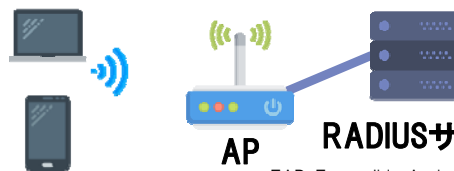
PSK方式(パーソナル)



APに設定されているパスフレーズと、利用者が入力したパスフレーズが一致することで認証。

PSK:Pre-Shared Key
AP:Access Point

EAP方式(エンタープライズ)



RADIUSサーバが、各端末に保存された情報等を基に認証。

EAP:Extensible Authentication Protocol
RADIUS:Remote Authentication Dial-in User Service

	認証方式	認証サーバの要否	端末側の認証	アクセスポイント側の認証	特徴
パーソナル	PSK	不要	SSID・パスフレーズ	-	利用者がパスフレーズを入力する。
エンタープライズ	EAP-TLS	必要	電子証明書	電子証明書	セキュリティ強度は高いが、各端末で電子証明書を管理する必要がある。
	EAP-TTLS	必要	ID・パスワード	電子証明書	端末側の認証をID・パスワードとすることで、EAP-TLSの煩雑さに対処したものの。
	EAP-SIM/AKA	必要	SIM/USIM	乱数	SIM/USIMカードが挿入されている端末は、自動で認証される。

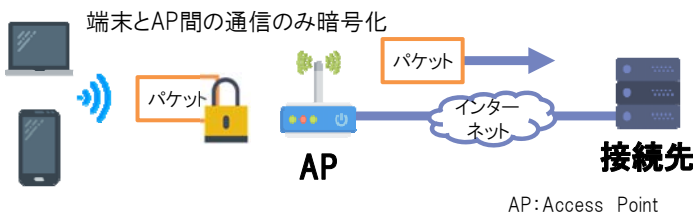
EAP-TLS: Extensible Authentication Protocol Transport Layer Security EAP-TTLS: Extensible Authentication Protocol Tunneled Transport Layer Security
EAP-SIM:Extensible Authentication Protocol Method for Global System for Mobile Communications(GSM) Subscriber Identity Modules
EAP-AKA:Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement
SIM: Subscriber Identity Module USIM:Universal Subscriber Identity Module

出典：公衆無線LANセキュリティ分科会(第1回)資料1-2

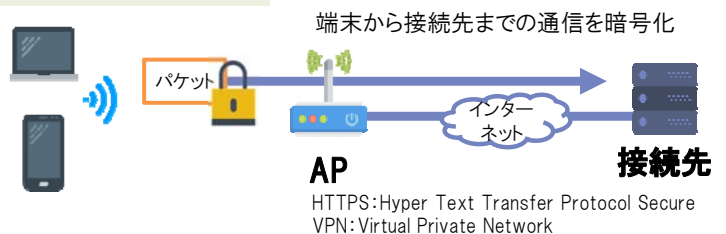
無線LANのセキュリティ対策：暗号化

- 暗号化とは、通信の内容を容易に推定できないようにする仕組みであり、通信の内容を秘匿化するもの。
- 無線区間におけるネットワーク層の様々な暗号化方式には、既に脆弱性が発見されているものもあり、利用にあわせて適切な強度の暗号化方式を設定することが望ましい。
- HTTPSやVPNといった、より上位層における暗号化方式を用いて、通信の内容を秘匿することもできる。

ネットワーク層における暗号化



HTTPS及びVPN



暗号化方式	特徴
WEP	<ul style="list-style-type: none"> ○ 無線LANにおける最初の情報セキュリティ対策方式。 ○ 暗号化鍵が自動で更新されず、これを悪用した短時間で解読する方法が存在。
WPA	<ul style="list-style-type: none"> ○ 鍵管理の方法をTKIPに変更し、WEPを拡張して策定。 ○ WEPとの互換性を有し、WEP対応の多くの端末で利用可能。
WPA2	<ul style="list-style-type: none"> ○ 暗号化アルゴリズムや改ざん検知の方式に、より強固なもの(CCMP)を用いて策定。 ○ 現時点では無線LANにおける最も強固な暗号化方式。
HTTPS(SSL/TLS)	<ul style="list-style-type: none"> ○ パケットのペイロード部分のみ暗号化して通信する。
VPN	<ul style="list-style-type: none"> ○ 全体を暗号化したパケットを、暗号化された擬似的なトンネルを用いて通信する。

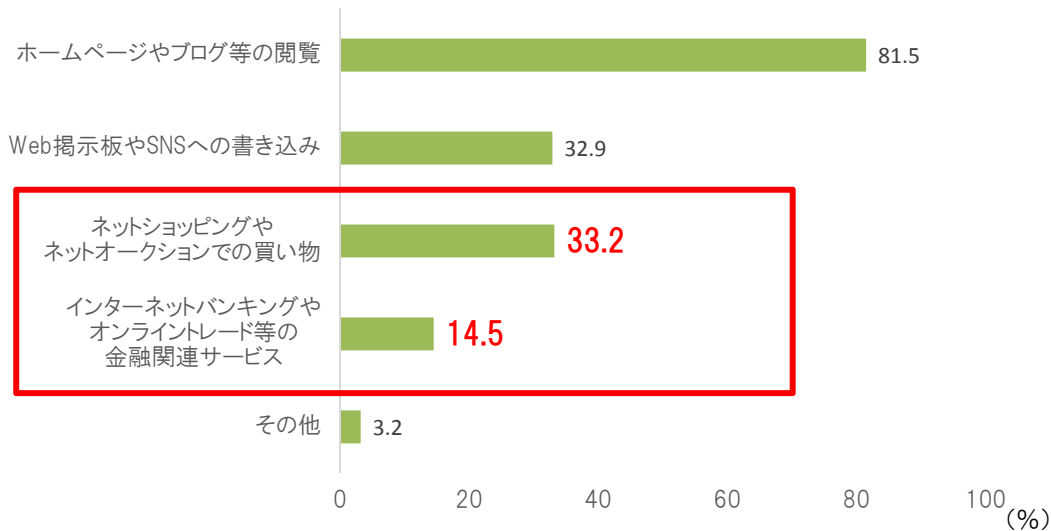
WEP:Wired Equivalent Privacy WPA:Wi-Fi Protected Access WPA2:Wi-Fi Protected Access 2
SSL:Secure Sockets Layer TLS:Transport Layer Security TKIP:Temporal Key Integrity Protocol CCMP:Counter mode with CBC-MAC Protocol

出典：公衆無線LANセキュリティ分科会(第1回)資料1-2

- 公衆無線LANの利用者が利用しているサービスには、ネットショッピングやネットオークションでの買い物、インターネットバンキングやオンライントレード等の金融関連サービスといった金銭に関するものもある。
- 他方、公衆無線LANサービスには、無線区間の通信が暗号化されていないアクセスポイントが存在。
- 上位レイヤで暗号化を行うSSL/TLS通信においても、様々な脆弱性が発見されている。

【最近の脆弱性の例(括弧内は発見年)】 BEAST & CRIME(2011年)、Lucky 13(2013年)、POODLE(2014年)、Heartbleed(2014年)

公衆無線LANの利用者が利用しているサービス(2016年)(複数回答可)



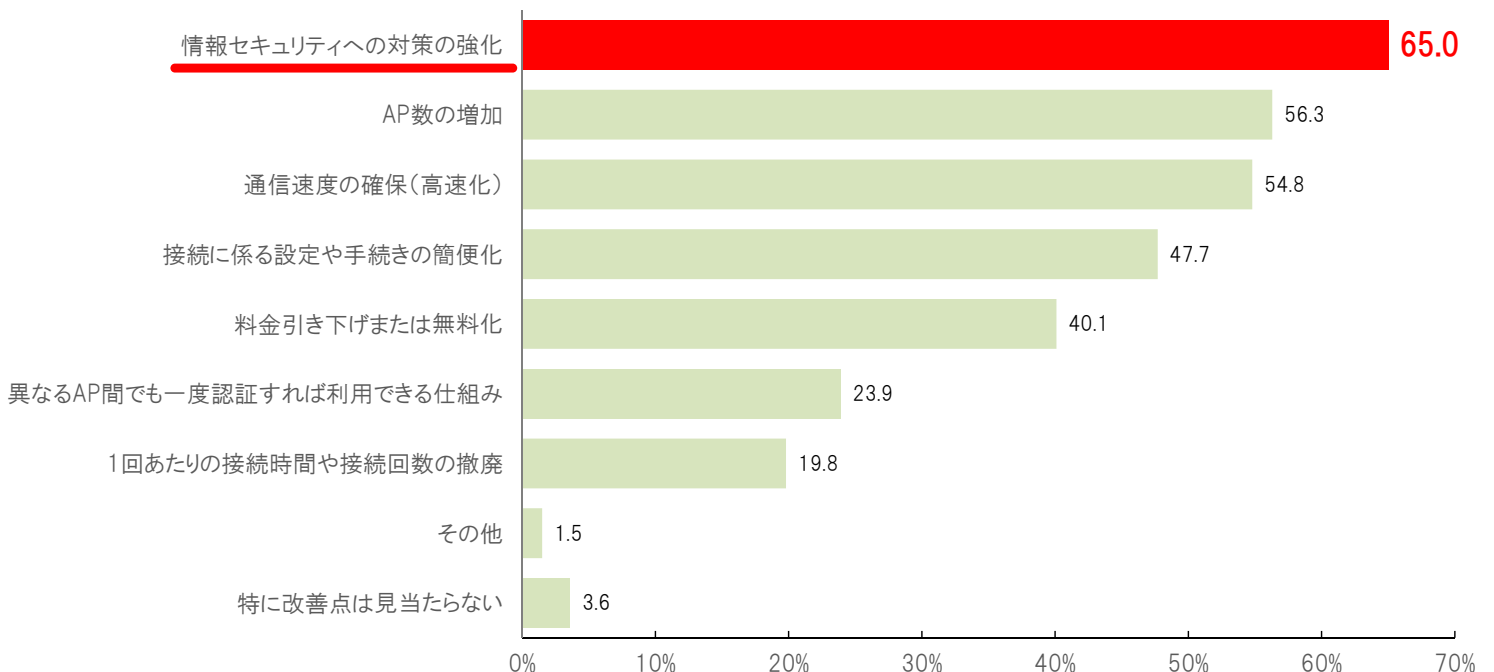
「2016年度情報セキュリティの脅威に対する意識調査」(情報処理推進機構) <https://www.ipa.go.jp/security/fy28/reports/ishiki/index.html> を基に作成。

出典: 公衆無線LANセキュリティ分科会(第1回)資料1-2

利用者における公衆無線LANのセキュリティに対する意識① 【資料17】

- 公衆無線LANの更なる普及が期待される中、公衆無線LANの利用において利用者が求める改善点として、「情報セキュリティへの対策の強化」が65%を占め、最も多い。

普段利用している公衆無線LAN利用に係る改善点について(複数回答可)

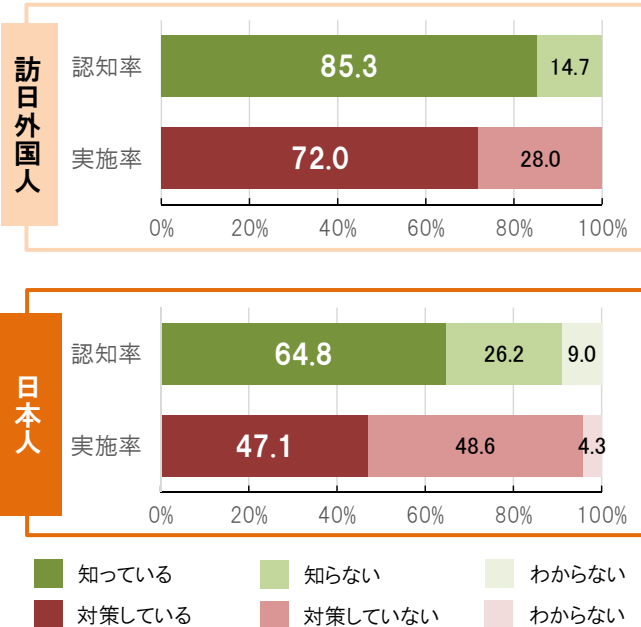


「公衆無線LAN利用に関する情報セキュリティ意識調査結果」(総務省) http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000091.html を基に作成。

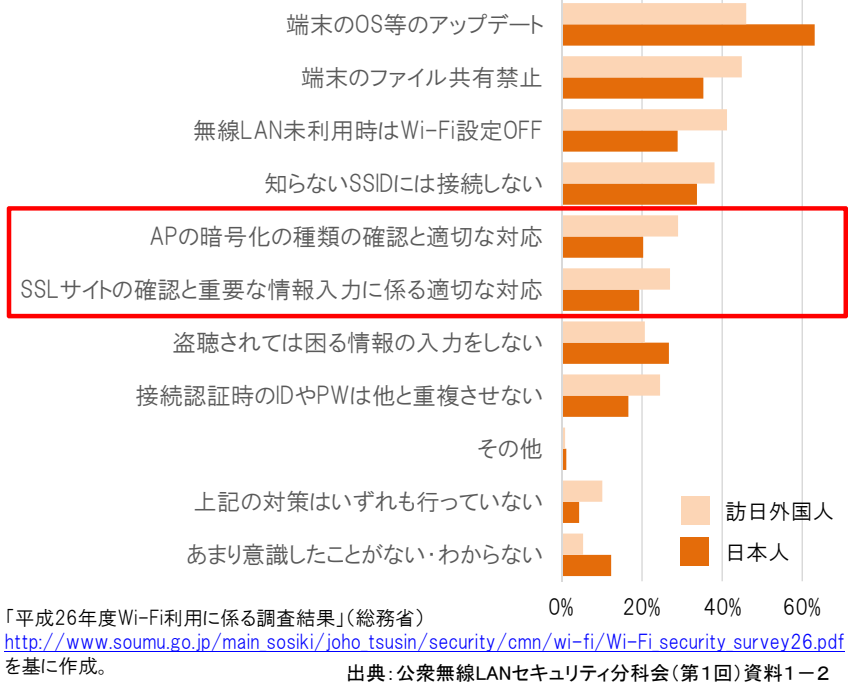
出典: 公衆無線LANセキュリティ分科会(第1回)資料1-2

- 公衆無線LAN利用時の脅威について、一定の認知はされているものの、セキュリティ対策の実施については低い傾向。特に、日本人についてその傾向が強い。
- また、「AP(アクセスポイント)の暗号化の種類の確認と適切な対応」や「SSLサイト(HTTPS)の確認と重要な情報入力に係る適切な対応」といった暗号化に関するセキュリティ対策は、十分に実施されているとは言い難い。

公衆無線LAN利用時の脅威の認知率とセキュリティ対策の実施率

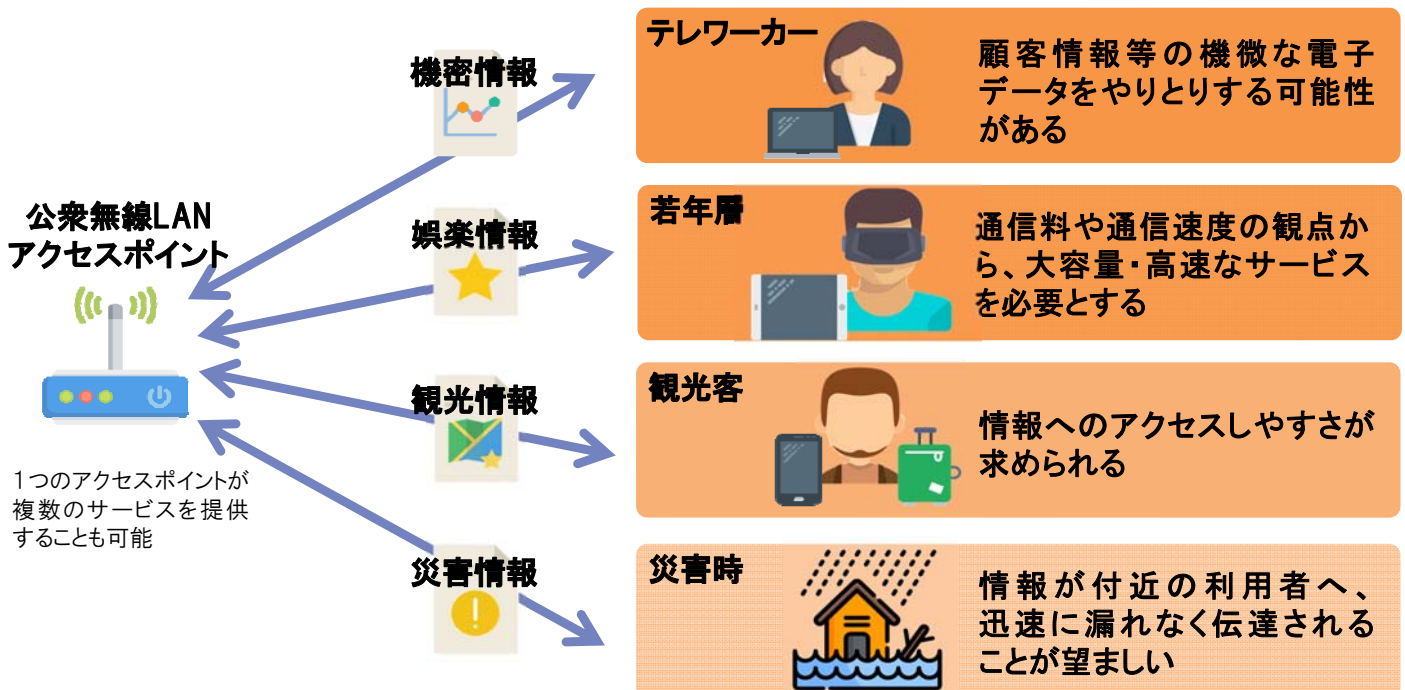


公衆無線LAN利用時に実施しているセキュリティ対策

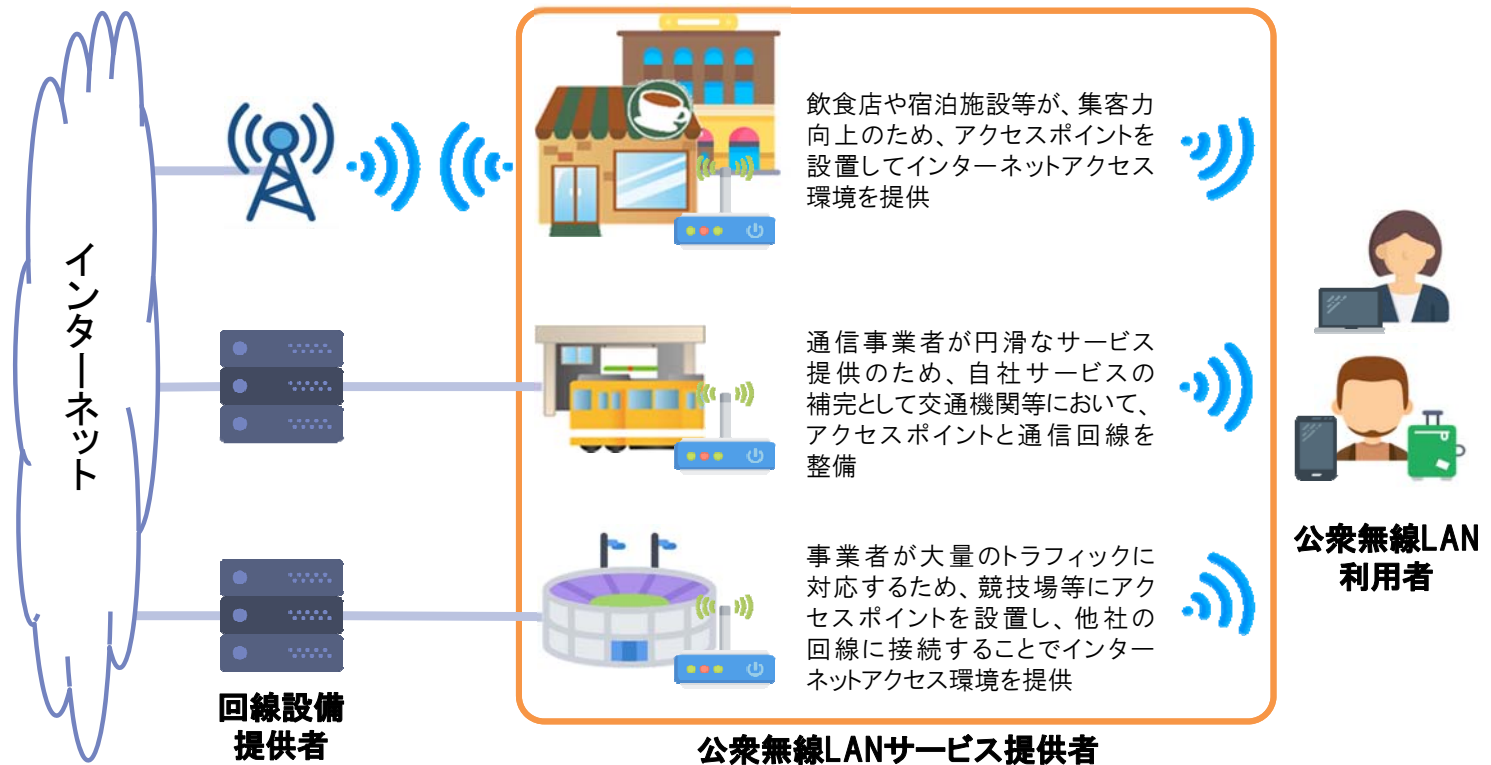


公衆無線LANの利用形態を踏まえたセキュリティ対策の必要性 【資料19】

- 公衆無線LANの普及の阻害要因の一つに、利用者が抱えるセキュリティに対する不安があると考えられる。
- 他方、公衆無線LANには、テレワーク環境の提供、リッチコンテンツの配信、観光客向けの観光情報案内、災害等の緊急時における情報提供といった様々なサービスの利用が期待されている。
- 利便性と安全性のバランスに配慮し、様々な利用者・利用シーンに応じたセキュリティ対策が必要。



- サービスの範囲や課金の有無等、様々な公衆無線LANの提供形態が存在。
- 提供者のビジネス環境等を配慮し、提供形態や目的に応じたセキュリティ対策が必要。



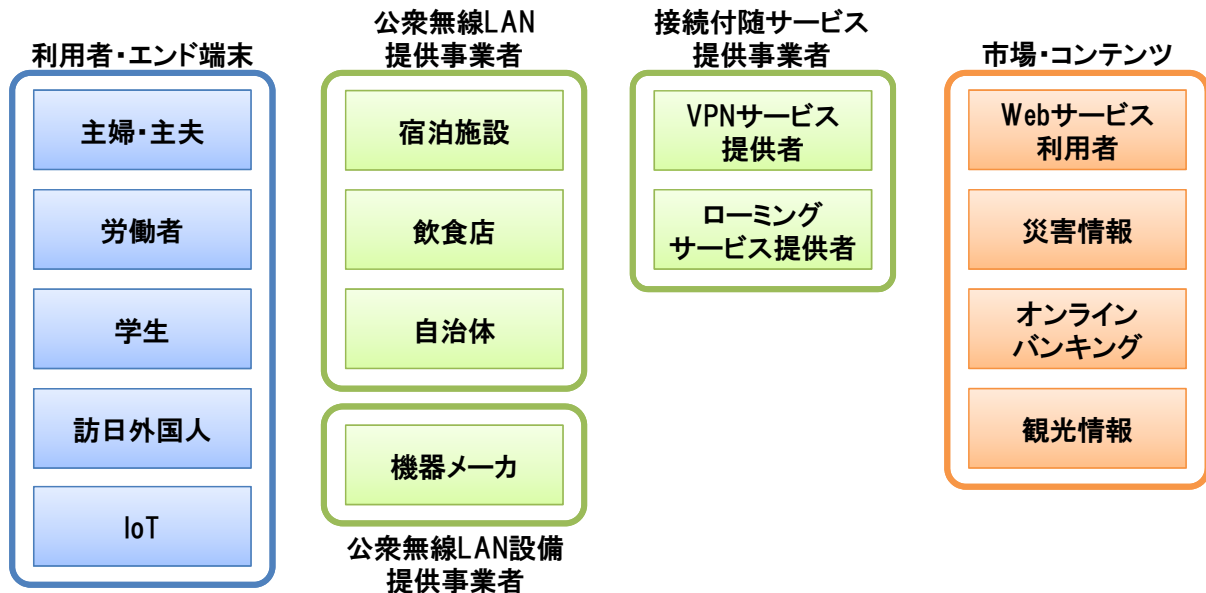
出典：公衆無線LANセキュリティ分科会（第1回）資料1-2

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、最近で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：3107万8609か所、「商用Wi-Fi」のホットスポット数：104万9151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：4万1798か所(2014年6月)、都市部の公共施設無料ホットスポット数：1000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：58万6098か所 うち有料734か所、無料3903か所、有料無料混合型58万1461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：7000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：4600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：2万8850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：5000か所以上(2014年11月末)

「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。

出典：公衆無線LANセキュリティ分科会（第3回）資料3-1



	利用者・エンド端末	公衆無線LAN提供事業者	公衆無線LAN設備提供事業者	接続付随サービス提供事業者	市場・コンテンツ
モチベーション	快適なネット環境で情報入手	利用客・訪問者の誘致	需要の獲得	新たなサービスの開拓	憂いなくデータ利活用や本業を推進
対策	脅威を把握し安全な利用を促進	脅威を把握し安全な利用形態を仕様化	トレーサビリティに必要な機能の提供	本人確認やローミングサービス等を提供	レスポンス体制の整備
考えられる課題	促進方法、リテラシ教育	指導方法、体制支援と優遇制度	トレーサビリティ等の必要な機能と、その設計手法の提示	国や業界団体による認定制度	事態対処訓練

公衆無線LANセキュリティ分科会(第2回)資料2-2を基に作成。

認証方式に応じた本人の推定と課題

認証方式	確度	利用者の利便性	本人の推定	課題
登録無し	×	◎	推定不可	
メールアドレス	登録のみ	×	偽のメールアドレスを入力された場合、推定不可	本人証明にならない場合がある
	メール送信確認	○	メールアドレス取得時の本人証明の確度に依存	本人証明されていないアドレスもあり
他のアカウントの利用 (Facebook等)	○	△	利用したアカウントの本人証明の確度に依存	必ずしも本人確認されていない
個人情報登録・提示 (パスポート・免許証等)	○	×	公的に利用されている	
SIM情報	○	◎	SIMを発行したキャリアアカウントに依存	モバイルキャリアに限定される

公衆無線LANセキュリティ分科会(第2回)資料2-4を基に作成。

	利便性	セキュリティ強度
(1) 暗号化なし	◎	×
(2) 暗号化あり:WPA2-PSK(Pre Shared Key) <ul style="list-style-type: none"> ■ 暗号鍵:全ユーザ共通(※) ■ 「暗号化なし」よりはセキュリティを確保 ■ ただし、全ユーザが共通の暗号鍵を利用するため、高いセキュリティを確保するためには定期的な暗号鍵の変更が必要(実際は、企業において頻繁な暗号鍵の変更は実施されておらず、PSK利用における課題。) 	○ (暗号鍵の定期的な変更をしない場合は△)	
(3) 暗号化あり:WPA2(IEEE802.1X/EAP:証明書ベース) <ul style="list-style-type: none"> ■ 暗号鍵:ユーザ個別 ■ 認証サーバと連携し、ユーザごとに異なる暗号鍵を生成可能なため、高いセキュリティを確保可能 ■ ただし、IEEE802.1Xは証明書ベースのため、公衆無線LANにおいては証明書の運用が課題 	△ ◎	

(※) 同じSSID配下でユーザごとに異なる個別の暗号鍵を利用可能な機能(個別PSK)を実装した製品がリリースされている。ただし、既存製品の仕組みでは、ユーザ登録との連携はうまく実現できていない。

公衆無線LANセキュリティ分科会(第2回)資料2-3を基に作成。

サービス層における暗号化

【資料25】

○ 公衆無線LANにおける盗聴等の脅威に対するサービス層における暗号化として、HTTPS(TLS)通信を利用することや、VPNサービスを利用することが考えられる。

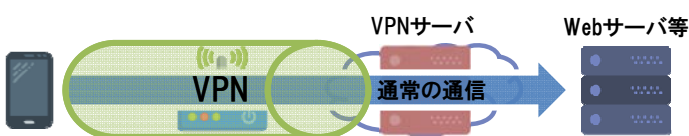
1. HTTPS(TLS)通信を利用



○ 端末・Webサーバ区間の通信が全て暗号化されているため、暗号化されていないアクセスポイントを利用した場合でも、安全な通信が可能

- × 保護対象がWeb通信に限定される
- × 全てのWebサーバでTLS/SSLプロトコルが使われていない

2. VPNサービス(※)を利用



○ 無線区間を含む端末・VPNサーバ区間の通信は全て暗号化されているため、暗号化されていないアクセスポイントを利用した場合でも安全な通信が可能

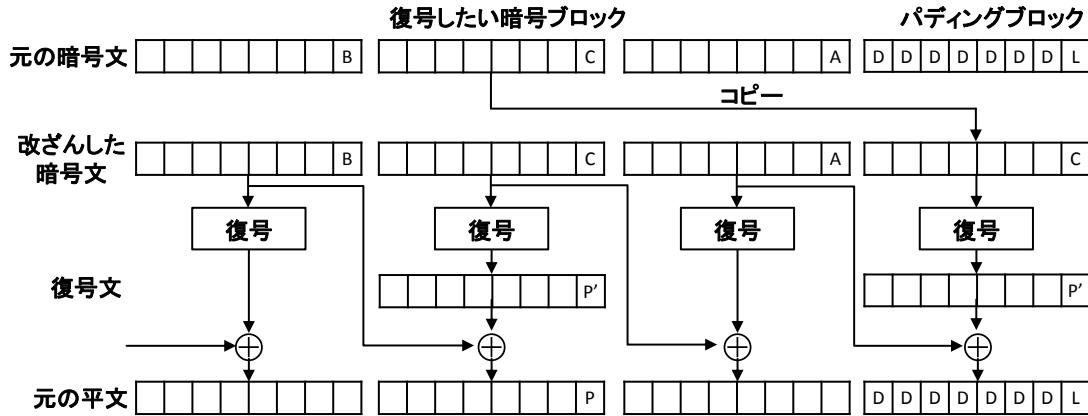
○ 通信プロトコルによらず、安全な通信が可能

- × VPNサーバに全てのトラフィックが集まるため、情報が健全に取り扱われない場合、重大なセキュリティリスクになる

(※) 2017年、米国大手企業との提携を謳うVPN業者が存在していることが判明。有名企業の知名度を利用して、利用者の個人情報盗もうとしていた。

公衆無線LANセキュリティ分科会(第2回)資料2-1を基に作成。

- 2014年10月、米Google社は、HTTPS通信等に用いられるSSL3.0に脆弱性を発見したと発表。
- 本脆弱性はSSL3.0の仕様起因のもので、ブロック暗号がCBCモードで使用されている環境では、総当たりで攻撃する場合よりもはるかに少ない回数で暗号文の解読が可能。
- 本脆弱性はSSL3.0に固有のものであるが、TLSでの通信を意図的に失敗させることでSSL3.0を利用させることが可能。



【解読のメカニズム】

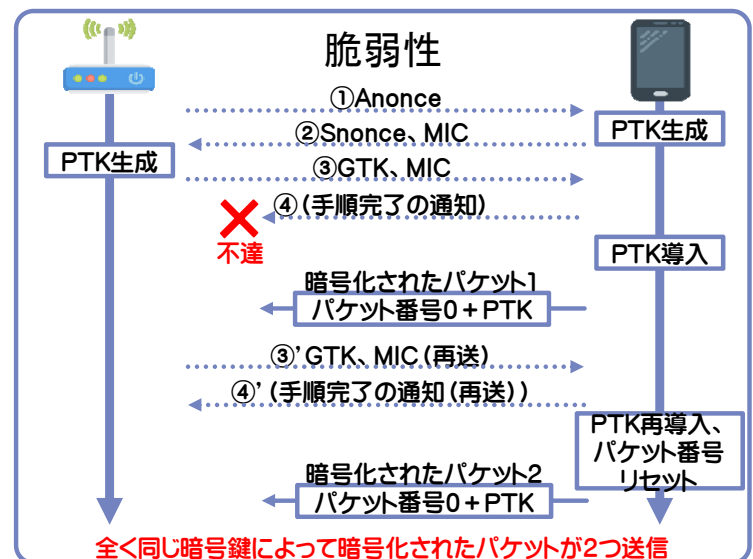
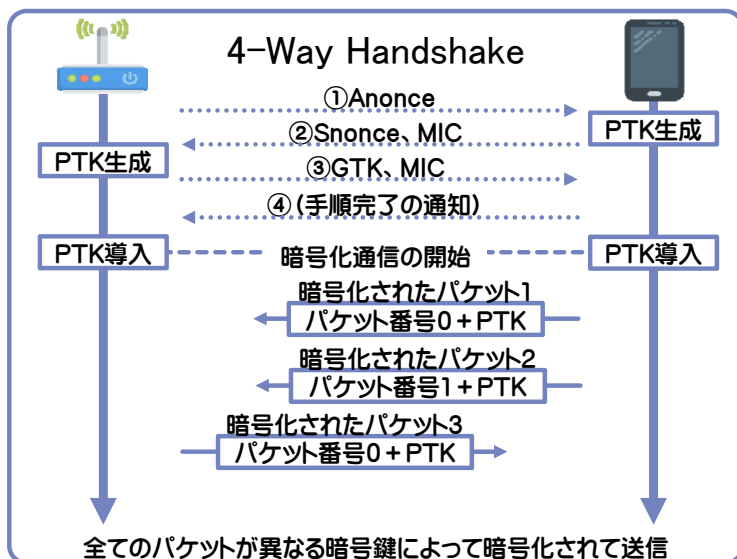
- (1) 中間者攻撃によりSSL3.0通信を有効化
- (2) 改ざんした暗号文をサーバに送信し、復号結果を観測(パディングオラクル攻撃)
- (3) C=Lとなった場合、AとLの排他的論理和からP'を導出
- (4) P'とBの排他的論理和からPを導出
- (5) 解読を試行する箇所を1バイト左にシフトし、(2)~(4)の手順を繰り返し実行

- 平文を一定長のブロックに分割して暗号化するブロック暗号の持つ、「同一の平文は同一の暗号文になる」という特徴に対処する暗号利用モードの一つであるCBCモードでは、初期化ベクトルと復号文の排他的論理和をとることで元の平文を導出。
- 直前の暗号ブロックをIVに利用すること、パディングブロックの末尾の値以外の値の検証を省略していることという、SSL3.0の二つの実装方法が原因であり、SSL3.0の無効化以外の対策はなし。

「日経NETWORK」(2018年1月号)(日経BP社)を基に作成。

WPA2の脆弱性(KRACKs)について

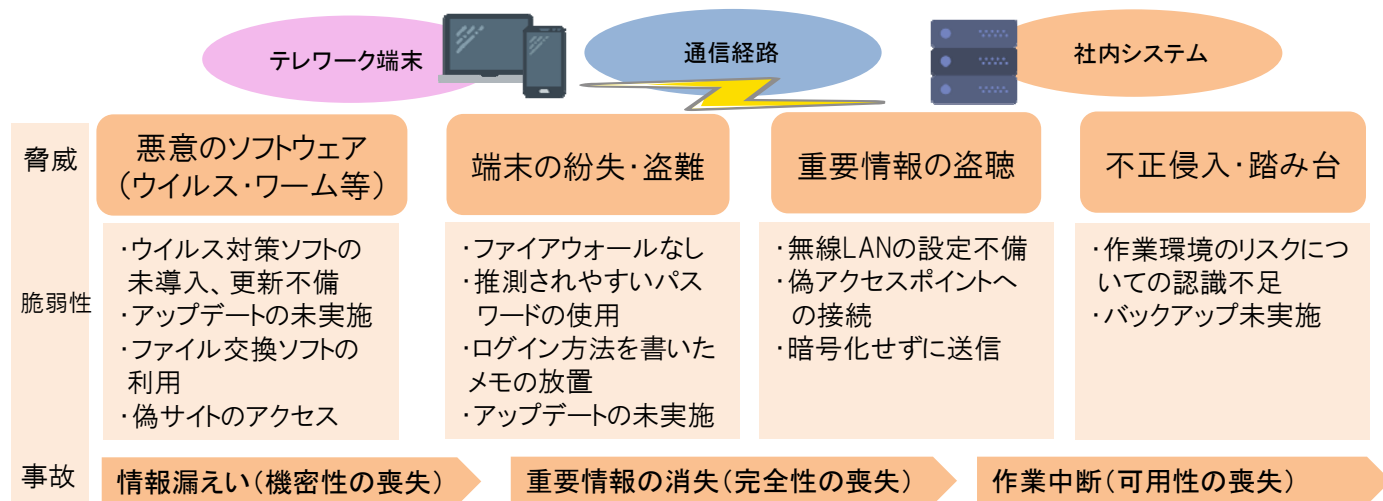
- 2017年、無線区間の通信の暗号化に用いられるWPA2に「KRACKs」という脆弱性が発見されたとの報道。
- 本脆弱性は、WPA2の暗号化に用いる鍵を交換する仕組みである、4-Way Handshakeに起因するものであり、無線LAN接続にこの仕組みを利用する全ての機器に影響。本脆弱性を悪用することで、通信の盗聴が可能であるが、現在のところ、被害事例の報告は無し。



Wi-Fi Allianceは、異なる鍵交換の仕組みを採用する等、より改良されたWPA3を発表、詳細は平成30年中に公表予定

- テレワークセキュリティガイドラインは、情報セキュリティ対策の初心者でもわかりやすく活用しやすい構成とすることにより、民間のテレワーク導入を支援し、普及促進を図ることを目的としている。
- 具体的には、テレワークを実施する上で必要となる情報セキュリティ対策を「ルール」「人」「技術」の三つの要素に分類し、具体的対策を紹介。テレワーク時に注意すべきセキュリティ対策のポイントをガイドラインとして、ウェブページで公開・周知。

テレワークにおける脅威と脆弱性



2017年度中に当該ガイドラインを改訂し、公衆無線LANをテレワークで使用する際の対策等について記載する予定。

公衆無線LAN版安全・安心マーク制度の概要

- インターネット接続サービス安全・安心マーク推進協議会が、従来の「インターネット接続サービス安全・安心マーク」に加え、公衆無線LANサービスを提供している事業者や自治体等を対象に、セキュリティ対策や個人情報保護への取組等が一定基準に達している目安である「公衆無線LAN版安全・安心マーク」を付与するもの。



インターネット接続サービス安全・安心マーク

【対象】
ISP(インターネット接続サービス提供事業者)



公衆無線LAN版安全・安心マーク

【対象】
無線LANサービスの提供者

一次審査(随時受付)

一般社団法人日本インターネットプロバイダー協会、
一般社団法人テレコムサービス協会、
一般社団法人電気通信事業者協会が審査項目に基づき実施。

二次審査(年3回実施)

安全・安心マーク審査委員会にて実施。

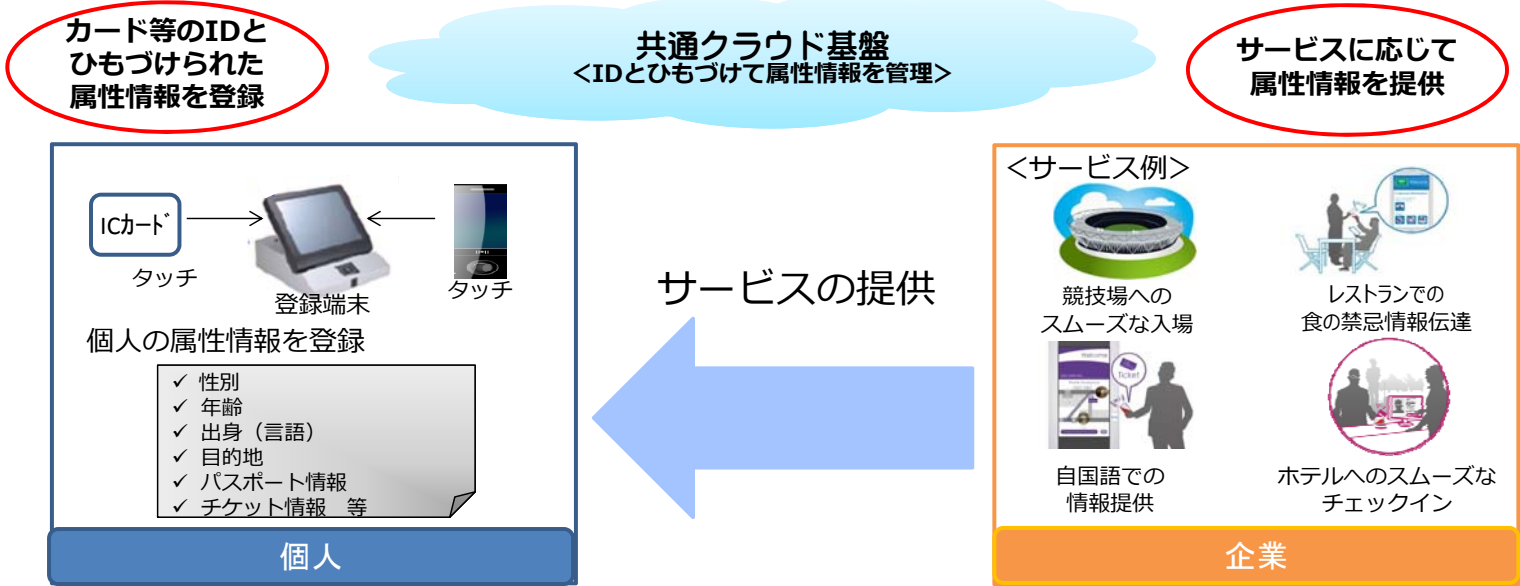
認定(有効期限は1年間)

期限満了前に更新審査を実施し、合格した場合継続使用可能。

審査項目

1 無線区間の暗号化またはその手法の案内	6 ユーザーに対して基礎的なセキュリティの啓発を行っているか
2 ユーザー利用規約または契約約款等の整備と公表	7 セキュリティに関する取組
3 ログ情報・利用者情報等の取扱いについて	8 災害時等の公衆無線LAN活用について
4 本人確認をしていることの確認	9 個人情報保護に関する取組
5 ネットワークの制御について	

○ 訪日外国人等のスムーズな移動、観光、買い物等の実現に向け、スマートフォン、交通系ICカードやデジタルサイネージ等と、共通クラウド基盤を活用した多様なサービス連携(個人の属性・言語等に応じた情報提供や支払手続の簡略化等)をめざす。

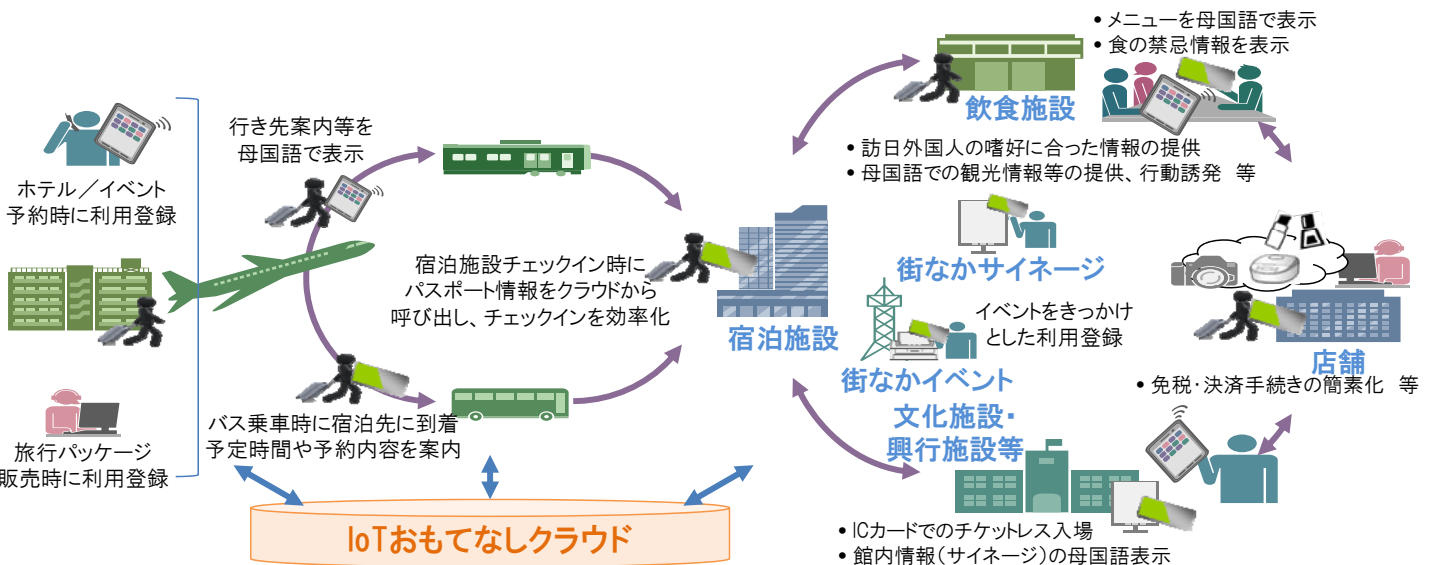


IoTおもてなしクラウドに係る検討の経緯

- 2015年5月～ 都市サービス高度化WGIにおいて、都市機能高度化に向けた議論開始
- 2015年7月 2020年に向けた社会全体のICT化推進に関する懇談会において、「アクションプラン(第一版)」とりまとめ
- 2016年1月 サービス検討SWGにおいて、「おもてなしインフラ報告書」をとりまとめ
- 2016年12月～ 2016年度IoTおもてなしクラウド事業として、クラウドを構築し、3地区で実証を実施

2016年度 IoTおもてなしクラウド事業の実証概要 【資料31】

○ IoTおもてなしクラウドを試験的に構築。訪日外国人の訪日前から滞在中、帰国時までには体験する各種サービスについて、IoTおもてなしクラウドとICカードを活用した実証を実施。



千葉・幕張・成田地区(モニター:1,800名) 於:千葉市美術館、イオン幕張 等	スムーズなホテルのチェックイン、美術館へのチケットレス入場、デジタルサイネージによる自国語での観光情報・経路案内等の提供、レストランでのスムーズなサービスの提供、多言語翻訳
港区 六本木・虎ノ門エリア(モニター:249名) 於:羽田空港国際線ターミナル、ホテルオークラ東京 等	空港からリムジンバスを利用しホテルに宿泊する訪日外国人に対するスムーズな情報伝達・チェックイン、スムーズな免税手続き、レストランでのスムーズな情報提供
港区 乃木坂エリア(モニター:96名) 於:国立新美術館	美術館へのチケットレス入場、デジタルサイネージによる自国語での文化情報の配信
港区 竹芝エリア(モニター:94名) 於:竹芝客船ターミナル、汐留ビルディング 等	デジタルサイネージによる自国語での観光情報・経路案内、災害情報の提供
渋谷地区(モニター:134名) 於:渋谷谷かみち総合インフォメーション、eplus LIVING ROOM CAFE&DINING 等	音楽イベントへのチケットレス入場や、デジタルサイネージによる自国語での観光情報の提供

- 【おもてなしクラウドの機能の高度化・ルール検討】 実運用に向け、クラウド機能の高度化、関係者間のルールの整備を行うとともに、異なるクラウド間の連携について検証。
- 【各場面を想定した実証の実施】 地方の観光地での観光を含め、各場面を想定したサービスについて実証するとともに、関係者間のルールを検証。



「第11回2020年に向けた社会全体のICT化推進に関する懇談会幹事会」(2017年12月12日)資料を基に作成。

公衆無線LAN環境整備支援事業の概要

- 防災の観点から、防災拠点(避難所・避難場所、官公署)及び被災場所として想定され災害対応の強化が望まれる公的拠点(博物館、文化財、自然公園等)における公衆無線LAN環境の整備を行う地方公共団体等に対し、その費用の一部を補助。

ア 事業主体: 財政力指数が0.8以下(3か年の平均値)又は条件不利地域(※)の普通地方公共団体・第三セクター

※ 過疎地域、辺地、離島、半島、山村、特定農山村、豪雪地帯

イ 対象拠点: 最大収容者数や利用者数が一定以下の

- ① 防災拠点: 避難所・避難場所(学校、市民センター、公民館等)、官公署
- ② 被災場所と想定され災害対応の強化が望まれる公的拠点: 博物館、文化財、自然公園等

ウ 補助対象: 無線アクセス装置、制御装置、電源設備、伝送路設備等を整備する場合に必要な費用等

エ 補助率: 1/2(財政力指数が0.4以下かつ条件不利地域の市町村については2/3)

イメージ図



公衆無線LAN環境整備支援事業における交付決定団体一覧 【資料34】

2016年度当初予算 (13団体)		2017年度当初予算 (2017年6月交付決定分：82団体)						2017年度当初予算 (2017年11月交付決定分： 11団体)	
総合通信局	団体名	総合通信局	団体名	総合通信局	団体名	総合通信局	団体名	総合通信局	団体名
北海道	北海道和寒町	北海道	北海道赤平市	関東	茨城県茨城町	近畿	滋賀県甲賀市	北海道	北海道更別村
	北海道寿都町		北海道興部町		群馬県下仁田町		京都府南山城村	東北	秋田県五城目町
	北海道喜茂別町		北海道神恵内村		埼玉県嵐山町		大阪府枚方市	関東	栃木県那須町
東北	山形県酒田市		北海道士幌町		千葉県東金市		奈良県		千葉県長生村
	信越		長野県白馬村		北海道洞爺湖町		千葉県鴨川市	奈良県橿原市	東海
長野県中川村			北海道美瑛町		東京都新島村		奈良県田原本町	近畿	
北陸	石川県穴水町		北海道鹿追町		山梨県甲府市	奈良県吉野町	中国		兵庫県神戸市
	福井県あわら市		北海道留萌市		山梨県北杜市	広島県安芸高田市		中国	鳥取県津和野町
中国	鳥取県琴浦町		北海道釧路町		新潟県阿賀野市	鳥取県八頭町	四国		岡山県井原市
	鳥取県湯梨浜町		北海道中川町		新潟県佐渡市	島根県西ノ島町		九州	広島県大崎上島町
四国	愛媛県大洲市		北海道七飯町	新潟県魚沼市	香川県小豆島町	九州	福岡県久留米市		
	九州		宮崎県小林市	北海道比布町	長野県飯田市		香川県三豊市		
鹿児島県天城町			北海道上川町	長野県中野市	長野県佐久市	徳島県			
			東北	青森県平川市	長野県川上村	徳島県阿波市			
		青森県今別町		長野県川上村	愛媛県大洲市	高知県黒潮町			
		青森県鶴田町		長野県南牧村	福岡県宗像市	福岡県志免町			
		岩手県遠野市		長野県小布施町	熊本県美里町	熊本県甲佐町			
		秋田県仙北市		富山県朝日町	宮崎県小林市	宮崎県高鍋町			
		秋田県三種町		石川県能登町	宮崎県高鍋町	宮崎県木城町			
		宮城県七ヶ浜町		福井県福井市	宮崎県都農町	宮崎県椎葉村			
		山形県遊佐町		福井県坂井市	鹿児島県鹿屋市	鹿児島県湧水町			
		福島県郡山市		福井県池田町	鹿児島県湧水町	鹿児島県和泊町			
		福島県南相馬市		福井県南越前町	静岡県西伊豆町				
		福島県平田村		福井県越前町	静岡県松崎町				
		福島県楢葉町		福井県高浜町	三重県玉城町				
				静岡県西伊豆町					
				静岡県松崎町					
			三重県玉城町						
				沖縄	沖縄県伊江村				

公衆無線LAN環境整備支援事業における認証基準に係る要件 【資料35】

○ 総務省が公表している「Wi-Fi提供者向けセキュリティ対策の手引き」(2016年8月)等も参照しつつ、「公衆無線LAN環境整備支援事業」を活用して、不特定かつ多数の者の利用を目的としてWi-Fi環境を整備する場合、不正利用防止及び利用者の利便性の観点から、①「SMS連携方式」による認証方式、②「SNSアカウントを利用した認証方式」及び③「利用していることの確認を含めたメール認証方式」の併用のいずれかが原則必要(※)。

① SMS連携方式

- 利用開始時に電話番号を入力
- システムからSMSで発行された利用コードを入力することで利用可能



② SNSアカウントを利用した認証方式

- 利用開始時に自身が利用しているSNSサービスにログインすることで利用可能



③ 利用していることの確認を含めたメール認証方式

- 利用開始時にメールアドレスを登録し、登録したアドレスに返信される利用コードの入力や認証URL等で利用可能



(※) 上記認証基準を適用しなくてもよいケース

- ・災害時における公衆無線LANの開放時
- ・屋内外問わず、利用者の容姿又は氏名の確認を取ることが可能な場所での使用時(例:学校への来訪者を目視、記録簿、防犯カメラ等により適切に把握できる場合)

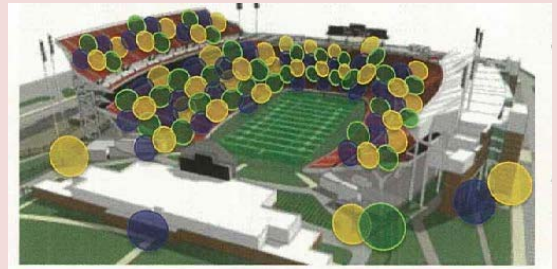
- 多くの訪日外国人観光客の来場が予想されるラグビーワールドカップ、2020年に開催される東京オリンピック・パラリンピック競技大会の競技会場については、災害発生時の情報提供・避難誘導手段の確保が必要。
- 高速無線LANやデジタルサイネージ等のICTを利活用したモデル事業を実施。特に、競技場で無線LAN経由によって提供するモバイル向けサービスを活用し、車椅子の方（観客、大会関係者いずれも）向けのガイド機能について実証を行う（避難誘導におけるアクセシビリティ確保のモデルを構築）。

デジタルサイネージ活用イメージ



サイネージにより、多言語による災害情報、避難経路情報の提供が可能

無線LANカバーエリアイメージ



- <無線LAN経由の配信コンテンツ例>
- ・災害発生時の情報提供、避難経路
 - ・車椅子の方向けアクセシビリティマップ
 - ・駐車場情報
 - ・売店情報、キャッシュレス購入