IPA Technical Watch

IPA Better Life with IT

公衆無線 LAN 利用に係る脅威と対策

～公衆無線 LAN を安全に利用するために～

IPA 独立行政法人情報処理推進機構
技術本部 セキュリティセンター

目次

はじめに

2020 年の東京オリンピック・パラリンピックの開催を見据えて、観光立国を推進する観点からも、国を挙げて公衆無線 LAN の促進に取り組んでいる[1]。各企業や自治体において、訪日外国人旅行者向けの無料で利用できる公衆無線 LAN 環境の更なる整備・拡大が進められている。

IPA が昨年実施した「2015 年度情報セキュリティの脅威に対する意識調査」[2]では、公衆無線 LAN などのフリーWi-Fi の利用割合が前年の 3 倍以上という結果であった。また、総務省がスマートフォン（以下、スマホ）やタブレット端末で無線 LAN を利用している日本人、訪日外国人を対象に実施した「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」[3]では、訪日外国人のみならず、日本人の約 8 割も観光地でのインターネット接続に無料で利用できる公衆無線 LAN を利用しているという結果が出ている。一方で、同調査において公衆無線 LAN 利用時の基本的なセキュリティ対策を実施している日本人の割合が 2～3 割程度と著しく低いという結果もある。公衆無線 LAN は外出先で高速な回線を利用できたり、携帯電話回線のパケット通信量を削減できたりというメリットがある一方で、第三者に通信内容を盗み見られる（盗聴）などのセキュリティ上の懸念もある。

さらに、公衆無線 LAN の整備・拡大を進める自治体間で、接続環境の安全性に格差が生じているという問題もある。一部の自治体の公衆無線 LAN では、利便性を優先させたために犯罪に悪用される危険性があると指摘されている。

本書では、スマホやタブレット端末で公衆無線 LAN を利用する際の一般的な脅威と対策をまとめている。公衆無線 LAN の安全な利用のために、必要となるセキュリティ対策の手引きとして参照して欲しい。

本書の対象読者

本書の主な対象読書は、以下の方々を想定している。

・外出先で公衆無線 LAN に接続してスマホやタブレット端末を利用する方
・公衆無線 LAN を提供している、もしくは提供を検討している自治体や企業などの方

[1] 総務省：公衆無線 LAN の整備の促進
http://www.soumu.go.jp/menu_seisaku/ictseisaku/public_wi-fi/index.html
[2] 2015 年 12 月 24 日公開「2015 年度情報セキュリティに対する意識調査」報告書について
https://www.ipa.go.jp/security/fy27/reports/ishiki/index.html
[3] 2015 年 3 月 16 日公開「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」
http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000091.html

1. 公衆無線 LAN 利用者の現状

IPA が実施した「2015 年度情報セキュリティの脅威に対する意識調査（以下、IPA の意識調査）」および総務省が実施した「公衆無線 LAN 利用に関する情報セキュリティ意識調査（以下、総務省の意識調査）」の結果を基に、公衆無線 LAN 利用者の現状を推察する。

1.1. 無線 LAN（Wi-Fi）接続時の環境

IPA の意識調査では無線 LAN 接続時の環境（スマートデバイスをインターネットに接続する方法）の割合は、以下の通りであった。

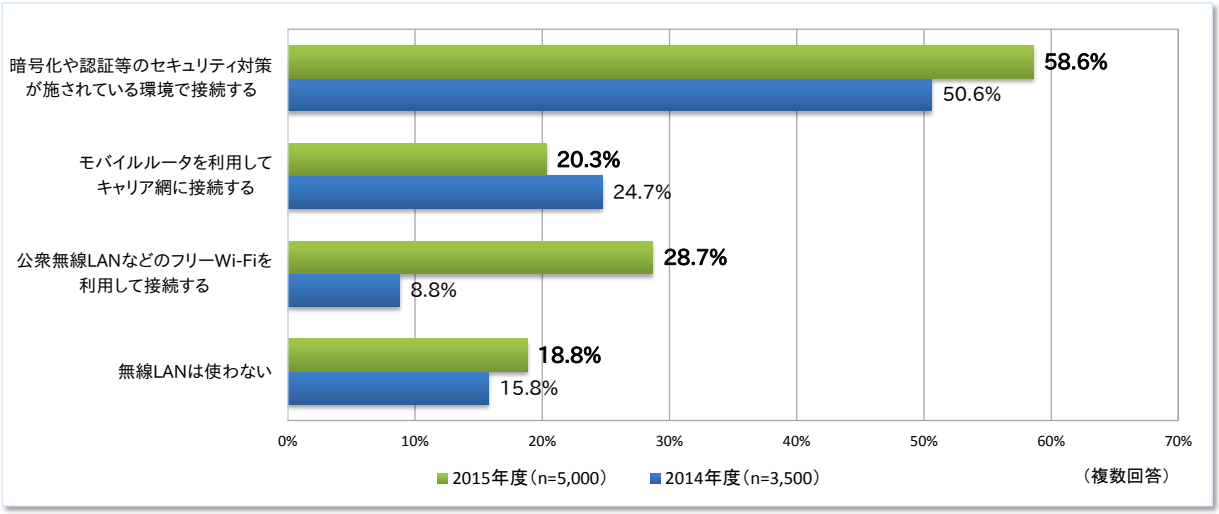

図 1-1-1：無線 LAN(Wi-Fi)を使ってスマートデバイスをインターネットに接続する方法
（「2015 年度情報セキュリティの脅威に対する意識調査」5-2-3）

公衆無線 LAN などのフリーWi-Fi を利用する割合が、昨年度の 8.8%から 28.7%と大きく増加している。公衆無線 LAN 環境の更なる整備・拡大が進み、利用者が増えていることが伺える。

1.2. 公衆無線 LAN（Wi-Fi）接続時に利用しているサービス

IPA の意識調査では公衆無線 LAN 接続時に利用しているサービスの割合は、以下の通りであった。

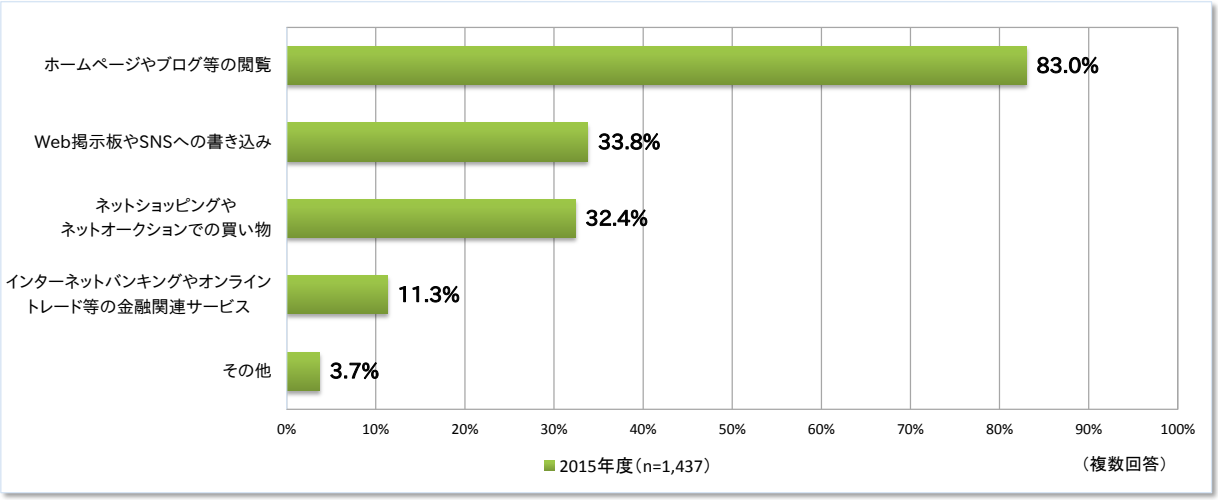

図 1-2-1：公衆無線 LAN などのフリーWi-Fi 接続時に利用しているサービス

（「2015 年度情報セキュリティの脅威に対する意識調査」5-2-4）

ホームページやブログなどの閲覧が 83.0%と最も多いが、ネットショッピングなどの利用が 32.4%、インターネットバンキングなどの利用が 11.3%と金銭の処理が発生するサービスを利用している割合も少なくない。

1.3. 観光先で利用するインターネット接続手段

総務省の意識調査では日本人観光客が観光先で利用したインターネットの接続手段の割合は、以下の通りであった。

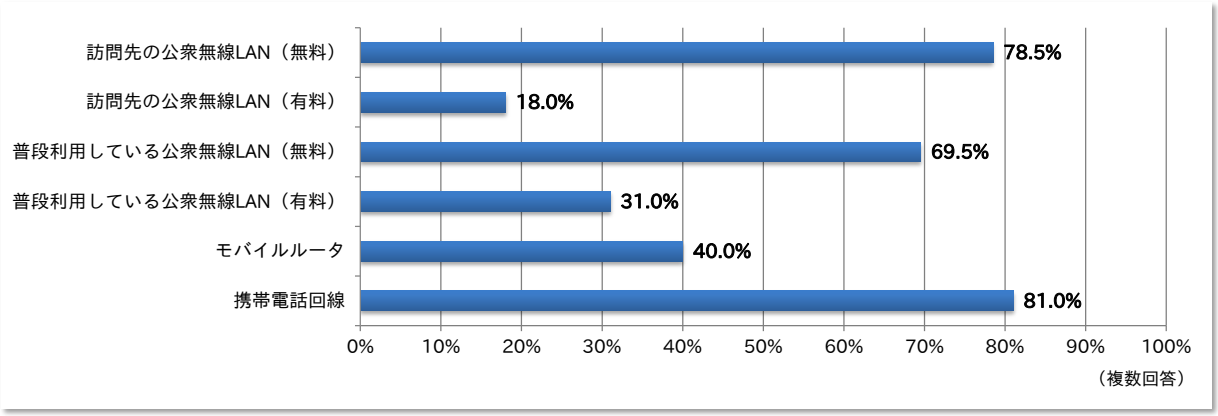

図 1-3-1：観光先で利用したインターネット接続手段（日本人）

（総務省「公衆無線 LAN 利用に係る調査結果（概略版）」より IPA にてグラフを作成）

携帯電話回線が 81.0%、次いで訪問先の公衆無線 LAN（無料）78.5%、普段利用している公衆無線 LAN[4]（無料）69.5%となっている。日本人観光客の 4 人のうち 3 人は、訪問先のフリーWi-Fi を利用していることになる。

[4] 公衆無線 LAN 事業者や携帯電話事業者が提供する Wi-Fi サービスなどのフリーWi-Fi

1.4. 公衆無線 LAN の脅威に対する認知度と対策実施率

総務省の意識調査では公衆無線 LAN 利用時の脅威（盗聴・なりすまし・悪意のアクセスポイント（以下、AP）やサイトへの接続）について、日本人観光客の認知度と対策実施率は以下の通りであった。

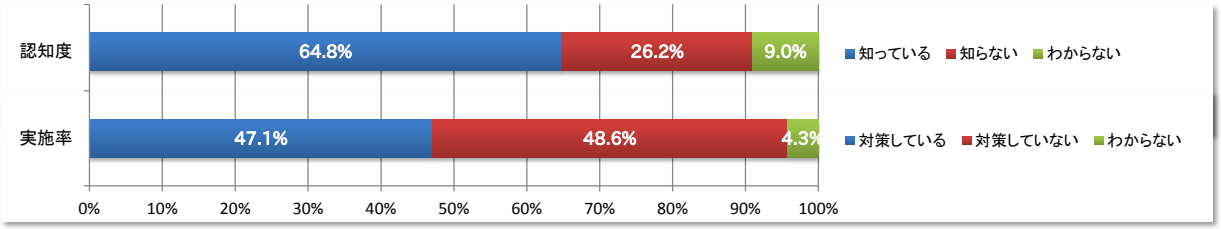

図 1-4-1：公衆無線 LAN 利用時の脅威認知度および対策実施率（日本人）

（総務省「公衆無線 LAN 利用に係る調査結果（概略版）」より IPA にてグラフを作成）

脅威の認知度は全体の半数を上回る 64.8%である一方で、対策の実施率は 47.1%と半数に満たず、十分な対策がなされていないと言える。

なお、訪日外国人の場合は脅威の認知度 85.3%、対策の実施率 72.0%であり、実施率の方が低くなるという同様の傾向が見られるものの、日本人に比べて全体的に認知度、実施率が高い結果となっている。日本人の 35.2%が公衆無線 LAN 利用時の脅威を認知していないことは大きな課題と言える。

1.5. 公衆無線 LAN のセキュリティ対策を行うべき主体

総務省の意識調査では公衆無線 LAN のセキュリティ対策を行うべき主体について、利用者が工夫すべきという日本人観光客の意見は 65.0%であり、利用者がセキュリティ対策を実施すべきという意見が半数を超える。一方で、事業者が工夫すべきとする意見が 35.0%であり事業者に安全への取り組みを期待する日本人観光客も少なくない。

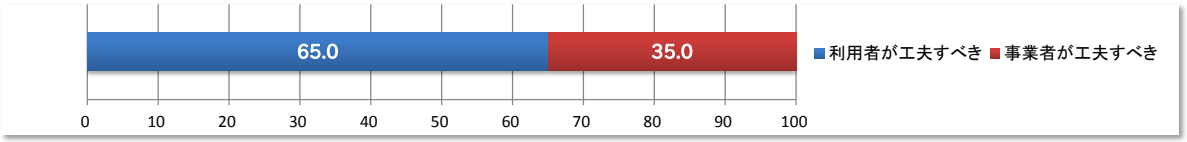

図 1-5-1：公衆無線 LAN（無料）のセキュリティ対策の工夫をすべき主体の割合（日本人）

（総務省「公衆無線 LAN 利用に係る調査結果（概略版）」より IPA にてグラフを作成）

なお、訪日外国人の場合、利用者が工夫すべきが 59.4%、事業者が工夫すべきが 40.6%と日本人観光客の意見とほぼ変わらない傾向にある。

2. 公衆無線 LAN に係る脅威

公衆無線 LAN の利用または提供において、想定される脅威は多岐に渡る。ここでは、公衆無線 LAN 環境における一般的な脅威について紹介する。

2.1. 盗聴

自己に宛てられていない無線通信を傍受[5]し、窃用することを意味する。公衆無線 LAN を利用した通信は受信可能な端末（アンテナ）があれば無線の出力範囲にいるすべてのユーザが受信可能であるため、基本的には誰もが傍受することができると言える。

公衆無線 LAN（AP）と利用者の端末間の通信が暗号化されていない場合、第三者に当該通信のデータを傍受されると通信内容を知られてしまい、その情報を窃用（盗聴）される恐れがある。

なお、AP と利用者の端末間の通信が暗号化されている場合でも、AP 接続に必要となる SSID[6]と暗号化キーを不特定多数の利用者で共有するようなフリーWi-Fi の利用においては、第三者が暗号化された通信の復号に必要な情報を得ることができるため、盗聴される可能性はある。

2.2. なりすまし

第三者が盗聴などの手口によって不正に情報を入手し、正規の利用者のアカウント情報を悪用したり、機器情報を偽装したりすることで、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を意味する。

例えば、AP との接続へのアクセス制限として MAC アドレスフィルタリング[7]を設定している場合、MAC アドレスを偽装することによって本来接続できないはずの端末を、不正に接続されてしまうなどの被害が考えられる。

2.3. 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、実在する正規の AP と同一の SSID、暗号化キーを設定した AP を意味する。過去に接続した正規の AP の情報が端末に保存されている場合、悪意の AP を認識すると自動的に接続してしまうことになる。利用者が誤って悪意の AP に接続してしまうと、通信内容を第三者に知られてしまい悪用される恐れがある。

---

[5] 電波法要説（情報通信振興会）によると、積極的意思をもって、自己に宛てられていない無線通信を受信することを傍受と呼び、無線通信の傍受自体では違法性は問われない。ただし、通信を傍受してその存在や内容を第三者に漏えいしたり、窃用したりすると電波法第 59 条に抵触し、罰せられる対象となる。

[6] SSID（Service Set IDentifier）：無線 LAN の通信規格で定められた AP の識別子。複数の AP が存在している空間において混線を避けるために利用される名前。

[7] MAC アドレスフィルタリング：特定の MAC アドレスを持つ端末以外は、接続できないようにするアクセス制限機能。

また、アカウント情報を不正に入手する目的で、悪意の AP が実在するウェブサービスを騙った偽の認証画面を表示させることもある。このような仕掛けがされていた場合、悪意の AP に接続した利用者が正規の認証画面と誤認して情報を入力してしまうと、当該ウェブサービスで不正利用の被害に遭う恐れがある。

例えば、ショッピングサイトの ID やパスワードの情報を知られてしまった場合、商品を不正に購入されてしまい、身に覚えのない商品の代金を請求されるなどの被害が考えられる。

2.4. 不正目的でのインフラの利用

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を意味する。主にサービス提供者側の脅威と言える。

事前登録や認証手続きなどによる利用者確認を行わずに公衆無線 LAN への接続が可能な場合、利便性は大きく向上する。しかし、このような確認を行わない場合、ある公衆無線 LAN から犯罪行為が実行されたことが確認できても、実行者（犯人）を特定することは困難となることから、犯罪のためのインフラとして不正利用される恐れがある。

3. 公衆無線 LAN のセキュリティ対策

公衆無線 LAN の主なセキュリティ対策について紹介する。なお、以下で紹介する対策は公衆無線 LAN の利用目的や利用時の脅威によって想定されるリスク、また実施するセキュリティ対策のメリット、デメリットなどを考慮し、適切な対策を選択、実施することが望まれる。

3.1. 公衆無線 LAN に係る主なセキュリティ対策

公衆無線 LAN に係る主なセキュリティ対策を、前述した脅威への対策と効果の有効性を以下の表に示す。また、それぞれの対策について必要となる作業や費用の面から見た利用、提供のしやすさの指標も参考として表に含めている。

表 3-1-1：公衆無線 LAN の主なセキュリティ対策

セキュリティ対策	脅威（脅威への対策効果）				利用しやすさ	提供しやすさ
	盗聴	悪意の AP	なりすまし	不正利用		
暗号化（AP と端末間）	○	―	―	―	○	◎
認証機能	―	―	◎	○	○	△
AP 接続アプリ	―	○	○	―	◎	○
VPN 通信	◎	○	―	―	○	△

凡例：◎ … 高い（容易）　○ … 条件次第　△ … 低い（困難）　― … 対象外

3.2. 暗号化

ここでは無線 LAN の通信において AP と端末間の通信内容を暗号化する WEP（Wired Equivalent Privacy）、TKIP（Temporal Key Integrity Protocol）、CCMP（Counter-mode CBC-MAC Protocol）[8]の 3 通りの暗号化方式について取り上げる。

いずれの方式も暗号化キーを利用し、AP と端末間の通信内容を暗号化する方式である。WEP については暗号化した通信内容でも解読されてしまう危険性が指摘されている[9]。そのため、特に家庭内無線 LAN では WEP の利用は避けるべきである。

なお、公衆無線 LAN の場合は家庭内無線 LAN とは異なり、不特定多数の利用者が接続する環境であるため、AP 接続に必要となる SSID と暗号化キーを不特定多数の利用者で共有するケースもある。その場合、自分以外の利用者も同一の暗号化キーの情報を知っていることになり、CCMP を採用した暗号化通信であっても解読することが可能である。

[8] 無線 LAN 機器の設定においては、CCMP ではなく AES（Advanced Encryption Standard）と表記されることが多い。

[9] 総務省：安心して無線 LAN を使用するために
http://www.soumu.go.jp/main_sosiki/joho_tsusin/lan/pdf/lan_2.pdf

公衆無線 LAN を利用する際、自分以外の利用者と同一の暗号化キーを共有する AP では、通信が暗号化されている場合でも盗聴される危険性があることを認識して欲しい。

また、サービス提供者は誰でも見ることができる場所に暗号化キーを掲示するといった方法ではなく、SMS（Short Message Service）で暗号化キーを個別に送信したり、暗号化キーを定期的に変更したりするなど、盗聴への抑止効果が期待できる提供方法の工夫が求められる。

3.3. 認証機能

ここでは WEB 認証と IEEE802.1X[10]における EAP-SIM 認証[11]を取り上げる。一般的な WEB 認証では AP へ接続後、ブラウザに ID とパスワードを入力する画面が表示され、正しい情報を入力することで公衆無線 LAN の利用が可能となる。WEB 認証に必要となる ID とパスワードを適切な方法で提供、管理することで、なりすましの対策となる。

EAP-SIM 認証は端末に挿入された SIM カードの情報を利用した認証となるため、ID、パスワードなどの入力は不要で、認証開始からネットワークが利用できるまでの時間が短いという特徴がある。面倒な手続きもなく利用できることから利用者の利便性は高い。

また、SIM カードを一意に特定できることで契約者の特定も可能となるため、不正目的でのインフラ利用の抑止への効果も期待できるというサービス提供者側のメリットもある。しかし、EAP-SIM 認証に限らず、IEEE802.1X による認証には認証サーバの構築、管理が必要となるため、サービス提供者側の負担が大きくなることが課題と言える。

3.4. AP 接続アプリ

事前にアプリをインストールしておけば利用可能な AP の探索や接続のための設定が不要になるといった、公衆無線 LAN の利用に必要な手続きの簡素化、誤接続の防止などが実現できる。

ただし、すべてのアプリが同等の機能や操作性を提供できるわけではないため、同じ公衆無線 LAN サービス利用目的のアプリであっても、利用者は実際に利用するにあたっては事前に十分な確認が必要となる。

また、アプリの利用により得られる効果や使い勝手などはアプリの実装に依存し、アプリの実装は開発コストに依存するため、セキュリティレベルの高い十分な機能を有したアプリの提供はサービス提供者側の負担となることが課題と言える。

[10] IEEE802.1X：LAN に接続する端末に対して使用される認証規格。
[11] EAP-SIM 認証：EAP（Extensible Authentication Protocol）による認証で SIM カードの情報を利用する方式。

3.5. VPN 通信

VPN（Virtual Private Network）はインターネットなど不特定多数で利用する回線を使った通信において、暗号化やトンネリングなどの処理によって安全性を高め、通信経路上の盗聴を防ぐことができる技術である。

下記に公衆無線 LAN を利用したスマホからのウェブサイトへのアクセスを例に、VPN などの暗号化される通信の対象と範囲の比較について、イメージ図を示す。

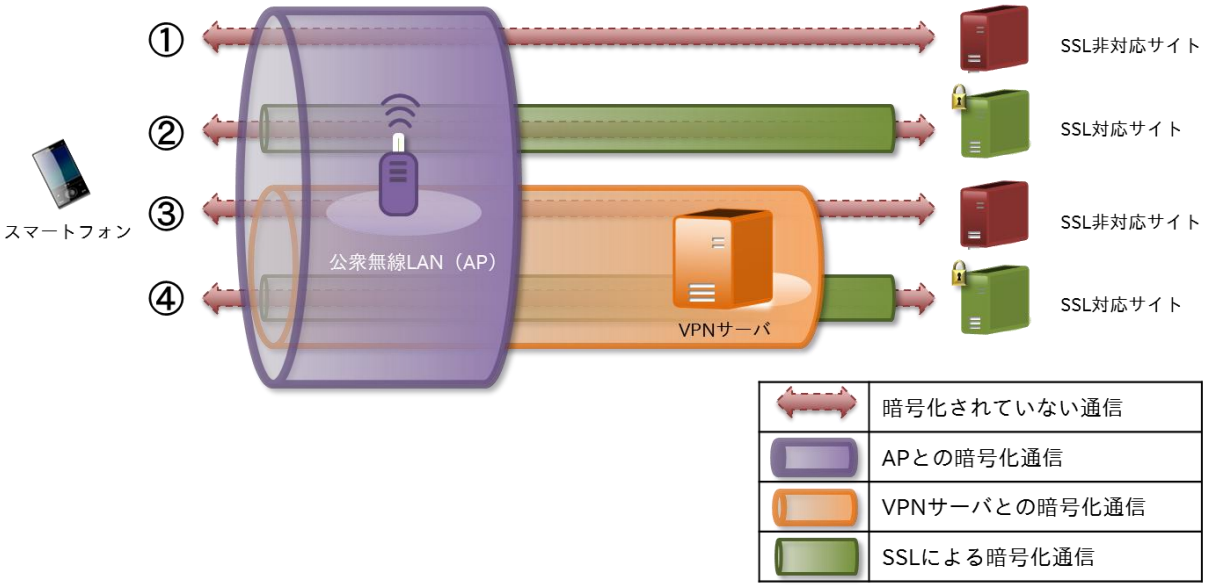

図 3-5-1：暗号化される通信の（盗聴の対策ができる）対象と範囲の比較イメージ

図のように VPN 通信を利用すると、VPN を経由して接続したサイトの情報（URL など）や入力内容すべてが暗号化の対象（図中の③および④）となる。公衆無線 LAN を利用したウェブサイトのアクセスにおいて、AP の暗号化方式や接続先サイトの SSL 対応有無を特に意識しなくても盗聴の対策ができるため、利用者にとってのメリットは大きい。

ただし、VPN 通信の利用には VPN サーバの設置や事前の VPN サービス契約が必要であるなど、利用者、サービス提供者共に作業面あるいは費用面でのコストに対する懸念はある。

4. まとめ

公衆無線 LAN を利用することで、携帯電話回線を利用するより快適な通信が行えたり、訪日外国人が普段使用している自国のスマホで通信が行えたりするなど、様々な利便性がある。ただし、これまで述べてきたように同時に様々な脅威も存在するため、家庭内無線 LAN とは区別をして適切に利用する必要がある。

公衆無線 LAN を安全に利用するためのポイントとして、下記の 2 点が挙げられる。

1. VPN 通信を利用する
2. 第三者に知られては困る情報は入力および表示をしない

詳細について以下に述べる。なお、あわせて総務省が提供している「Wi-Fi 利用者向け 簡易マニュアル[12]」や「一般利用者が安心して無線 LAN を利用するために[13]」も参照されたい。

4.1. VPN 通信を利用する

公衆無線 LAN などのフリーWi-Fi を利用する際、暗号化設定がされていない場合や不特定多数の利用者と同一の暗号化キーを共有する場合には、AP との通信内容が盗聴されるというリスクは避けられない。

そのため、ID、パスワードといったログイン情報やクレジットカード番号、個人情報など、重要な情報を入力が必要となる場合はもちろん、第三者に知られては困る情報をやりとりする場合は SSL 対応サイトのみに限定することが重要である。

ただし、すべてのサイトが SSL に対応しているとは限らず、また SSL 対応有無を判断しながらの利用は利便性を大きく損ねるため、VPN 通信を利用することを推奨する。なお、VPN 通信を利用すると、万が一、悪意の AP に接続してしまった場合の盗聴にも有効となる。

2015 年 11 月より、愛媛県公衆無線 LAN 推進協議会が提供する「えひめ Free Wi-Fi」で実証実験[14]を行っている。アプリによる AP 接続と VPN 通信および不正サイトへのブロックといったセキュリティ機能が提供される内容となっており、公衆無線 LAN の利用において、利用者の利便性とセキュリティを確保できる優良なモデルと考える。

ただし、上記のようなセキュリティ機能を有する公衆無線 LAN の場合、アプリの開発やサービス提供などにかかる費用が発生するため、利用者への無償提供にあたってはサービス提供者側がいかに費用を捻出するかが課題と言える。

---

[12] Wi-Fi 利用者向け 簡易マニュアル
http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/cmn/wi-fi/Wi-Fi_manual_for_Users.pdf
[13] 一般利用者が安心して無線 LAN を利用するために
http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/cmn/wi-fi/Wi-Fi_manual_for_ippan_riyousha.pdf
[14] トレンドマイクロ株式会社：フリーWi-Fi 向けセキュリティサービス「あんしんフリーWi-Fi™」を提供開始
http://www.trendmicro.co.jp/jp/about-us/press-releases/articles/20151112005507.html

4.2. 公衆無線 LAN を利用する場合はやりとりする情報を限定する

何らかの理由により VPN 通信ができない場合、公衆無線 LAN を安全に利用するためのポイントは、「第三者に知られては困る情報は入力および表示をしない」ことである。

例えば、ID やパスワード情報を入力しなければいけないサイトへのアクセスは控えるなど、万が一、盗聴されてしまった場合でも、当該サイトへの不正ログインといった被害に発展しないよう、外部に漏れても影響のない情報のやりとりに限定することが推奨される。

もし外出先において重要な情報の入力が必要となってしまう場合は、携帯電話回線を利用するなど、必要となる通信の内容に応じて公衆無線 LAN の利用可否を判断することが重要となる。

おわりに

総務省や各自治体が公衆無線 LAN の環境を整備していくことは、旅先での情報収集に活用できるなど、訪日外国人のみならず日本人観光客にとってもメリットのある取り組みと考える。しかし、それは公衆無線 LAN が安全に利用できることが前提である。

また、外出先によって公衆無線 LAN の利用に必要な条件が異なる場合、赴く先々で公衆無線 LAN 環境の確認および設定が必要となり、利用者の負荷が高くなる。そのため、公衆無線 LAN の環境や条件などが標準化され、国内の公衆無線 LAN がシームレスで利用できるような利便性向上の取り組み[15]も期待される。

本書では公衆無線 LAN を安全に利用するための主な脅威と対策、利用時のポイントについて述べてきた。自宅や学校、会社のみならず、外出先や移動中においても端末で AP の一覧表示を確認すると複数の SSID が表示されることが多く、国内の無線 LAN 利用者の多さや公衆無線 LAN の環境が整備されていることが実感できる。

今後も公衆無線 LAN を取り巻く環境の大きな変化などに応じて、公衆無線 LAN の安全な利用に関する情報を提供していきたい。まずは本書が現在の公衆無線 LAN に係る脅威や対策を正しく理解し、公衆無線 LAN を大いに、かつ安全に活用するための一助となることを願う。

[15] 総務省：「利用しやすく安全な公衆無線 LAN 環境の実現に向けて ～訪日外国人に対する無料公衆無線 LAN サービスの利用開始手続の 簡素化・一元化の実現等に向けた取組方針～」の公表
http://www.soumu.go.jp/menu_news/s-news/01kiban04_02000102.html

IPA テクニカルウォッチ

「公衆無線 LAN 利用に係る脅威と対策」

～公衆無線 LAN を安全に利用するために～

[発　　行]　2016 年 3 月 30 日
[著作・制作]　独立行政法人情報処理推進機構 技術本部 セキュリティセンター
[執　筆　者]　野澤 裕一　小川 貴之