《論　文》

公衆無線LANサービスと利用環境整備の動向

増　田　悦　夫

あらまし

東京五輪・パラリンピックの開催などに伴い訪日外国人（インバウンド）を増加させようとする政府方針が打ち出されている。一方，日本滞在時にインターネットを利用しようとした場合，接続手段である『公衆無線LANサービス』が経済的かつ容易に利用できず困ったという訪日外国人のアンケート結果が出ている。訪日外国人を増やすに当たり情報利用環境として公衆無線LANサービスの整備が喫緊の課題となっている。観光庁や総務省が連携して協議会を設置するなど，国を始めとして民間や地方自治体等で関連する取り組みが積極的に展開されつつある。

本稿では，公衆無線LANサービスのベースとなる無線LAN技術とその進展を概観するとともに，環境整備の急がれている公衆無線LANサービスについて，その仕組みやセキュリティ対策，利用環境整備の最近の取り組み状況，当面の課題などを示した。

キーワード：無線LAN，公衆無線LAN，環境整備，セキュリティ対策，IEEE802.11

1．まえがき

東京五輪・パラリンピックの開催などに伴い訪日外国人（インバウンド）を増加させようとする取り組みが行われている。年間の旅行客は2013年が1000万人強，2016年は2400万人前後になると想定されており，2020年には4000万人に拡大しようという目標が立てられている[1]。一方，日本滞在時にインターネットを利用しようとした場合，接続手段である『公衆無線LANサービス』が経済的かつ容易に利用できず困ったというアンケート結果[2][3]が出ている。そこでは，訪日外国人が滞在中困ったことのトップが公衆無線LANサービスの利用環境なっている。この結果を受け，観光庁と総務省が連携して協議会を設置する[4]など，環境整備を促進するための取り組みが，国，民間や地

方自治体等で活発に展開されつつある。

本稿では，公衆無線LANサービスのベースとなる無線LAN技術とその進展を概観するとともに，利用環境の整備が急がれている公衆無線LANサービスについて，その仕組みやセキュリティ対策，利用環境整備に向けた最近の取り組み状況，当面の課題について示す。

第２章では，無線LANの仕組みや技術の進展，特に高速化の進展について示す。続く第３章では，公衆無線LANサービスの提供主体，セキュリティ上の脅威や対策について示す。さらに第４章では，利用環境整備の必要性，民間（施設管理者や通信事業者など）や地方自治体等での取り組み状況，当面の課題を示す。第５章で全体をまとめる。

２．無線LAN技術とその進展

２.１　無線LANの仕組み

無線LAN（図１）は，企業やその施設，大学，官庁などの拠点内に構築された構内通信網（LAN：Local Area Network）において，端末との接続部分に無線を利用したものである。これは，基地局（AP：アクセスポイント）を介して各端末を接続する動作モードにあたり「インフラストラクチャモード」と呼ばれている[1)]。収容される端末（主に携帯されるモバイル端末）はAPと接続し，それを収容するスイッチを介して拠点内の他の端末，あるいはルータを介して，他の拠点内の端末とのデータ送受信を行う。

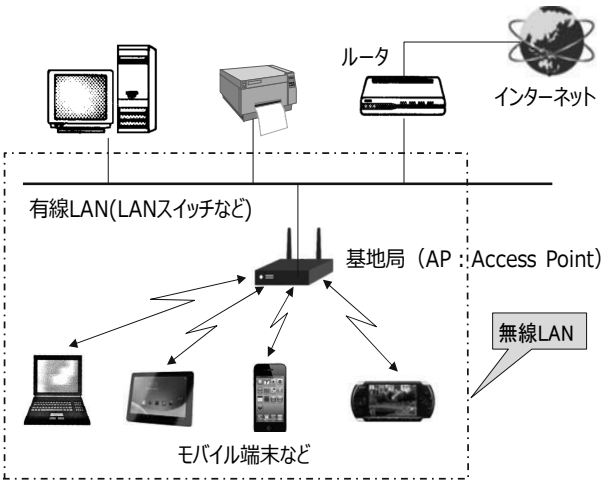


図１　無線LANの構成例（インフラストラクチャーモード）

1）他に，各端末が直接接続して相互にデータ送受信を行う「アドホックモード」がある

デスクトップPCなどをスイッチなどへケーブルで接続して通信する「有線LAN」とは異なり，接続ケーブルが不要な点が特徴であり，モバイル系の端末を接続する場合に都合がよい。有線LANに比較して通信速度や安定性などで劣ることが多いがその利便性などから普及が進んでいる。

2.2　無線LANの規格

無線LANの規格には様々なものがあるが，IEEEのLAN/MAN標準化委員会が策定したIEEE 802.11シリーズが標準として普及している。LANの規格を定めているのはIEEE802委員会であるが，特に無線LANの規格はIEEE802.11委員会が定めている。802.11シリーズの標準規格は1997年の初期規格策定後，通信速度の高速化（802.11a/b/g/n/ac），トラフィック種別ごとの優先制御（802.11e/aa/ae），セキュリティの強化（802.11i/w），無線LANネットワーク機能の拡充（802.11F/h/k/r/s/u/v/z），各国周波数への対応（11d/j/y）といった多くの追加規格により，高速化・高機能化が実現されてきている[5]。

特に通信速度の高速化に関連する規格とそれに関連する周波数や通信速度，技術，セキュリティの推移を表１に示す[6]。現在利用されている無線LANの規格のうち，1999年に策定されたのが802.11bと802.11aであり，802.11bと互換性があり，通信速度が802.11aなみに速いIEEE802.11gが普及している。また，2009年にはMIMO（Multiple Input Multiple Output）と呼ばれる技術を用いた802.11nが提供され，さらに2014年には，その後継の802.11acも規格化されている。

表１　無線LANに関する規格等の推移

	1997年	1999年	2003年	2009年	2014年
1)規格	IEEE802.11	IEEE802.11b IEEE802.11a	IEEE802.11g	IEEE802.11n	IEEE802.11ac
2)周波数	ISM2.4G	J52	W52,53 W56		
3)最大通信速度	2Mbps	11Mbps（11b） 54Mbps（11a）	54Mbps	65~600Mbps	293M~6.9Gbps
4)技術	DSSS	OFDM CCK		MIMO	MU-MIMO
5)セキュリティ	WEP	TKIP（WPA）	CCMP（WPA2）		

・DSSS：Direct Sequence Spread Spectrum（デジタル信号を広い帯域に分散して同時送信する方式）
・OFDM：Orthogonal Frequency Division Multiplexing（直交性を利用した周波数分割多重化方式）
・CCK：Complementary Code Keying（拡散符号に相補型符号を用いるDSSS方式）
・MIMO：Multiple Input Multiple Output（複数アンテナを同時に利用し異なるデータを送受信する技術）
・MU-MIMO：Multu User MIMO（電波に指向性を持たせ複数端末との同時通信が可能）
・WEP：Wired Equivalent Privacy（RC4アルゴリズムによる共通鍵暗号方式）
・TKIP（WPA）：Temporal Key Integrity Protocol（Wireless Application Protocol）（WEPの改良版。認証機能追加、鍵の定期的自動更新など）
・CCMP（WPA2）：Counter-mode CBC-MAC Protocol（Wireless Application Protocol 2）（WEPの改良版。認証機能追加、AESと呼ばれる強力な暗号アルゴリズを使用）

表２は，初期規格であるIEEE802.11を含め，これまでに策定された通信速度の高速化に関連する規格をまとめたものである。無線LANの規格で，最初の頃のIEEE802.11a/b/gなどはAPと端末とが１本のアンテナで通信をしていた。このタイプは，SISO（Single Input Single Output）と呼ばれる。その後，802.11nの規格で新たに複数のアンテナを使って通信を行う方式が導入された。この場合，APと通信する端末が複数存在する場合，時分割的に端末を切り替えてAPと通信するようになっている。このタイプは，単にMIMO（Multiple Input Multiple Output）あるいはSU-MIMO（Single User-Multiple Input Multiple Output）とも呼ばれる。これに対し，802.11acのMU-MIMOと呼ばれるタイプは，互いに干渉しない（高度な指向性を備えた）複数の信号波を用いることにより，複数の端末と同時に通信を行えるようにしている。但し，AP側のアンテナ数を複数の端末に分けて同時通信を行うため，端末側の通信速度はAP側の合計速度よりも低くなる。

表２　無線LANの規格（注：通信速度に着目した規格）

名称	策定時期	周波数帯[GHz]	最大通信速度[bps]	変調方式	特徴
IEEE802.11	1997年6月	2.4	2M	DSSS	IEEEが最初に策定した規格
IEEE802.11b	1999年9月	2.4	11M/22M	DSSS	2.5GHz帯を使う電子レンジや医療用機器、Bluetooth対応製品などとの電波干渉で速度低下が起こり得る。
IEEE802.11a	1999年9月	5	54M	OFDM	電波法により屋外での利用が不可で屋内のみ。
IEEE802.11g	2003年6月	2.4	54M	OFDM/DSSS（11bとの互換性考慮）	OFDMの採用で、11aなみの速度を実現。2.4GHz帯使用のため、電子レンジや医療用機器、Bluetooth対応製品などとの電波干渉あり得る。11bとの相互接続可能。
IEEE802.11n	2009年9月	2.4/5	65M~600M	OFDM	一次変調に64QAM（6ビット/波）、MIMO技術（アンテナ数は最大4）を採用。SU-MIMOとも呼ばれる。11a/b/gとの相互接続も可能。
IEEE802.11ac	2014年1月	5	293M~6.9G	OFDM	802.11ｎ規格の後継。一次変調に256QAM（8ビット/波）、MIMO技術（アンテナ数は最大8）を採用。MU-MIMOに対応。2.4GHzを使用する11b/g/nとの相互接続は不可。

・DSSS：Direct Sequence Spread Spectrum（デジタル信号を広い帯域に分散して同時送信する方式）
・OFDM：Orthogonal Frequency Division Multiplexing（直交性を利用した周波数分割多重化方式）
・MIMO：Multiple Input Multiple Output（複数アンテナを同時に利用し異なるデータを送受信する技術）
・SU-MIMO、MU-MIMO：Single-User MIMO、Multu User MIMO（電波に指向性を持たせ複数端末との同時通信が可能）
・QAM：Quadrature Amplitude Modulation（位相と振幅を組み合わせた波を利用する変調方式）

２.３　無線LANのセキュリティ対策

無線LANはケーブルを使わず電波で通信を行うため，電波を傍受されてデータを盗み見される危険性がある。そのため，セキュリティ対策が必要となる。無線LANでは，「機密性」（資格のある人以外はその情報へアクセスできないようにすること），「完全性」（情報は改ざんなどがなく正確で完全なこと），「可用性」（必要時はその情報をいつでも利用可能なこと）といった情報セキュリティの３つの基本的要件のうち，特に「機密性」，「完全性」が求められる。その対策として，認証，暗号化，侵入検知･防御の３つが考えられている。

①認証：資格のある正規の端末（クライアント）やユーザが信頼できる基地局（AP）を通じてネットワークへアクセスすることを保証するための対策。
②暗号化：送受信データを盗み見されても理解されないようにするための対策。
③侵入検知・防御：ネットワークへの不正侵入や不正トラフィックを検出したり防御したりする対策。

上記①，②の２つが基本的対策であるが，企業の無線LANの場合には上記①～③の３つの対策によりセキュリティの強化を図っている場合が通例である。

表３に無線LANのセキュリティ規格を示す。「WEP」は無線LANの最初のセキュリティ規格で，送信側と受信側に同一の情報（キー）を設定し，このキーにより暗号化／復号化を行うようにしている。鍵が固定（64ビットまたは128ビット）なため脆弱性が指摘されている。WEPの脆弱性を改善し，より強固なセキュリティを可能としている規格が「WPA」である。WPAでは，TKIP（Temporal Key Integrity Protocol）と呼ばれる暗号化，即ち，暗号キーをユーザーごとにダイナミックに生成し，定期的にキーを変更して暗号化する方式を提供している。また，IEEE802.1xによるユーザー認証を提供している。即ち，RADIUS（Remote Authentication Dial-In User Service）サーバを利用し一元的なユーザー認証を可能としている。ユーザー ID，パスワードによる認証の他，デジタル署名による認証もオプションとしてサポートしている。この認証では端末－AP/スイッチ－RADIUSサーバ間でEAP（Extensible Authentication Protocol）と呼ばれるプロトコルを利用している。「WPA2」あるいはIEEE802.11iは，AES（Advanced Encryption Standard）と呼ばれるより強力な暗号化手法を利用している点でWPAよりも強力なセキュリティ規格となっている。

表３　無線LANのセキュリティ規格

名称	策定時期	策定主体	内容
(1)WEP (Wired Equivalent Privacy)	1997年	IEEE	・強力な認証なし ・基本的な暗号方式（注：秘密鍵暗号方式の一種。RC４をベース。脆弱性があり、信頼性にやや欠ける。）
(2)WPA (Wi-Fi Protected Access)	2002年	Wi-Fi アライアンス	・ユーザー認証：企業用はIEEE802.1x（EAP：Extensible Authentication Protocol）、個人用はPSK（Pre-Shared Key）方式 ・TKIP（注：Temporal Key Integrity Protocol。WEPの弱点を補強。暗号鍵RC4を周期的に更新する機能を追加）による暗号化
(3)WPA2 (Wi-Fi Protected Access 2)/IEEE802.11i	2004年	Wi-Fi アライアンス /IEEE	・ユーザー認証：同上 ・TKIPやAES（Advanced Encryption Standard、米国NISTが制定）による強力な暗号化

２.４　AP－端末間の接続動作概要

無線LANにおいて端末がデータ通信を開始する際，有線LANの場合はPCのLAN接続口とスイッチとをケーブルで接続することになるが，無線LANでは「アソシエーション」と呼ばれる一連の処理シーケンスにより端末とAPとを接続することになる。

アソシエーションには，APの識別子であるSSID（Service Set IDentifier）を用いる。無線LANは電波を使った通信のため，複数のAPと交信可能な「混信」状態が生じ得る。このため，通常は無線LANのAPと各端末とに共通のSSIDを設定し，APはSSIDが一致する端末としか通信しないようにする。

アソシエーションの手順は以下のようになっている。

(i) APは（SSIDや伝送速度，暗号プロトコルなどの含まれた）ビーコン信号を周期的（例えば100ms毎）にブロードキャストで送信している。

(ii) 無線LANに収容された端末（クライアント）はビーコン信号から利用可能な周波数を探しSSIDを指定する。その後，APにアソシエーション（接続）要求を出す。

(iii) APはアソシエーション（接続）の応答で接続の可否を通知する。

無線LANにおける基地局（AP）－端末間の接続動作概要を図2に示す。即ち，①端末のAPの検出，②認証，③アソシエーション，④暗号化されたデータフレームの送受信の順に行われる。

2.5 AP-端末間接続設定のための規格，システム

無線LANでは有線LANに比べ設定が複雑なため，設定を容易に行える以下のような規格や，システムが利用されている。

(1) WPS（Wi-Fi Protected Setup）

無線LAN機器の接続やセキュリティに関する設定を容易に行うことができる機能である。2007年1月，Wi-Fiアライアンス[2)]によって策定され，メーカーを問わず利用できる。WPSに対応した機器同士は，多岐に渡る画面入力などを行うことなく簡単な操作で設定を行うことができる。WPSでは，無線LANアクセスポイント（Wi-Fi アクセスポイント）や無線 LANルータ（Wi-Fi ルータ）が親機となり，パソコンやゲーム機など接続したい子機に SSIDやWPA の設定などの情報を送る。

(2) AOSS（Air Station One-Touch Secure System）

バッファローの無線LANルータ（Wi-Fiルータ）などが備える簡易設定機能である。対応機器同士では専用のボタンを押すだけで設定が完了する。AOSSに対応した機器同士では，接続したい機器のAOSSボタンを押し，次に無線ルータなどのAOSSボタンを押すだけで，最適な設定を自動的に選択・設定して接続できるようにしてくれる。

(3) らくらく無線スタート

NECアクセステクニカ株式会社（現・NECプラットフォームズ）が開発した無線LAN自動設定システムである。先発であるバッファローのAOSSと共に二大無線設定システムとして知られ，AOSSとともにWi-FiアライアンスにWPSを策定させる要因となった。

2）無線LAN製品の普及促進を目的とした業界団体で製品の認証などを行っている。

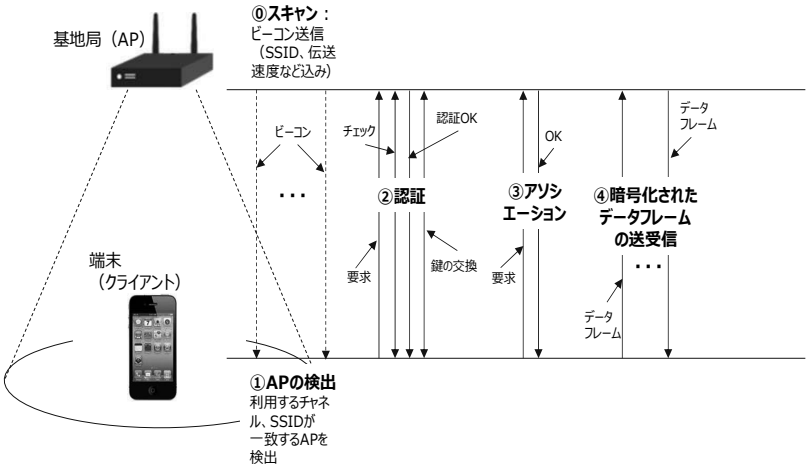


図２　基地局（AP）－端末間の接続動作概要

３．公衆無線LANサービスとセキュリティ対策

公衆無線LANサービスは，人の多く集まる商業施設，公共交通機関，宿泊施設，学校などで提供される，無線LAN経由のインターネット接続サービスである。街中や旅先においてノートパソコンやスマートフォン，携帯ゲーム機などの端末を用いて高速なネット接続を利用できるようにしたものである。

３.１　公衆無線LANサービスの提供主体による分類

APを設置する主体の観点から，以下の２形態に分けられる。

⑴　通信事業者が提供するもの

通信事業者が自らAPを設置し提供するもので，利用できるのはその事業者と契約する人に限られる（注：訪日外国人が日本国内の公衆無線LANを利用できない原因となっている）。ほとんどが月額課金制（有料）となっている。また，スマートフォン等モバイル端末の普及に伴う携帯電話網への通信圧迫を軽減する目的で公衆無線LANへの迂回（トラフィック・オフロード，図３）を考慮したAPの設置も行われている。

⑵　施設管理者が提供するもの

駅や空港，飲食店，宿泊施設など公衆を対象とする施設で提供される。その施設の利用者や顧客なら誰でも無料で自由に利用できるようになっている場合が多い。APの設置は施設への集客支援，住民へのサービス向上（公共施設の場合）などを目的としている。無料の公衆無線LANサービスの拡大・普及を推進する団体としてFREESPOT協議会が知られており，2016年12月18日時点で１万3355拠点でFREESPOTサービスが提供されている[7]。

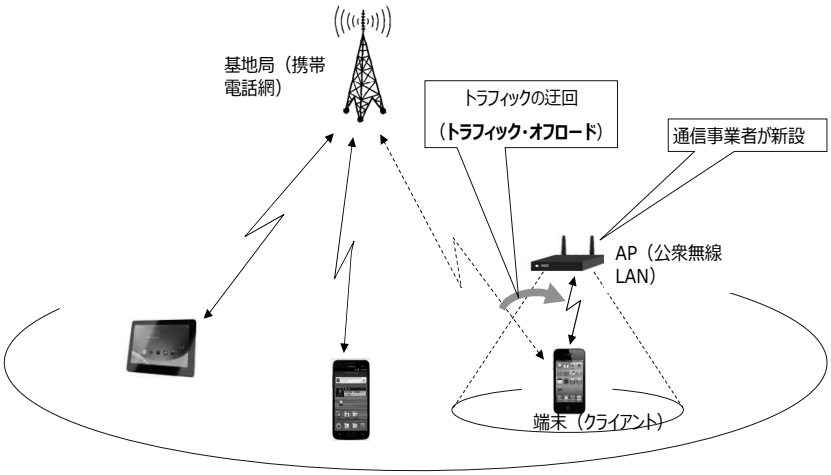


図3　トラフィック・オフロードのイメージ

3.2　公衆無線LANサービスに対する脅威[8]

公衆無線LANサービスに対する脅威として，以下に示すような4種が知られている。

①盗聴

公衆無線LANでは無線の出力範囲（スポット）にいるすべてのユーザが電波を受信可能である。APと利用者端末間の通信が暗号化されていない場合，第三者に通信内容を窃用（盗聴）される恐れがある。また，暗号化されている場合でも，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ような利用形態では，第三者が暗号化された通信の解読に必要な情報を得ることができるため盗聴される危険性がある。

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で，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が不正に接続されてしまうなどの被害が考えられる。

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，実在する正規のAPと同一のSSID，暗号化キーを設定したAPを設置する場合がある。正規の利用者が誤って悪意のAPに接続してしまうと，通信内容を知られてしまい悪用される恐れがある。

④インフラの不正利用

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サービスが犯罪のためのインフラとして不正利用されることである。主に，公衆無線LANサービ

スを提供する側への脅威となる。事前登録や認証手続きなどによる利用者確認なしに公衆無線LANへの接続を許容しているような場合，利便性は大きく向上するものの，不正利用の実行者（犯人）を特定することが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。

3.3　公衆無線LANのセキュリティ対策[8]

前述したような脅威に対し採られている対策を脅威と対応づけて図 4 に示す。即ち，暗号化，認証機能の導入，AP接続アプリの利用，VPN通信の利用などが挙げられる。

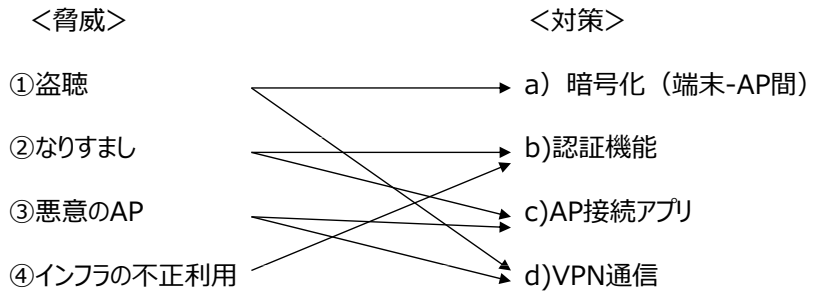


図 4　公衆無線LANサービスに対する脅威とセキュリティ対策[8]

a）暗号化

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（第 2 章の表 3 を参照）。公衆無線LANサービスを利用する際，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おく必要がある。一方，サービス提供者には，誰でも見ることができる場所に暗号化キーを掲示するような方法ではなく，SMS（Short Message Service）など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必要となる。

b）認証機能

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。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，管理することにより，なりすまし対策が可能となる。また，「EAP（Extensible Authentication Protocol）－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く面倒な手続きもなく利用できるため利用者の利便性が高い。サービス提供者側にとってはSIMカードにより契約者の特定が可能となるため不正目的でのインフラ利用が抑止できる効果が期待できる。ただ，EAP－SIM認証では認証サーバの構築，管理が必要となりサービス提供者側の負担が大きくなり得る。

c）AP接続アプリ

事前にアプリをインストールしておくと利用可能なAPの探索や接続のための設定が不要となり，手続きの簡素化，誤接続の防止などが実現できる。ただ，アプリの利用にあたっては機能等を事前に十分に確認しておく必要がある。

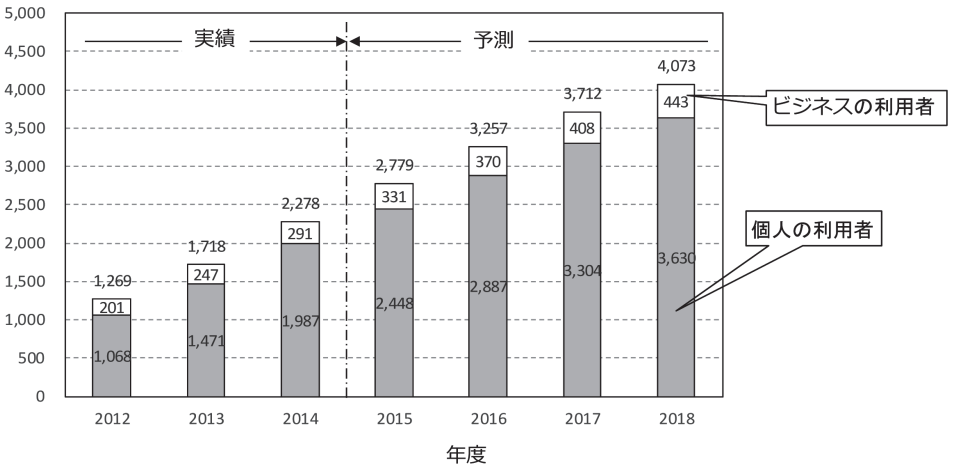
d）VPN通信

VPN（Virtual Private Network）はインターネットなど不特定多数で共用される回線を使った通信において，暗号化やトンネリング[3)]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技術である。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となるため，公衆無線LAN経由でのWebサイトアクセスにおいて，APや接続先サイトのセキュリティ対策の方式や対応状況を意識しなくて済むため利用者にとってメリットが大きい。ただし，VPNサーバの設置や事前のVPNサービス契約が必要となる。

4．利用環境整備の取り組み状況

4.1　公衆無線LANサービスの利用者数

図5[9]は，2015年4月時点にまとめた公衆無線LANサービスの利用者数の推移と今後の予測である。2014年度末で利用者数は2,278万人で，個人利用者が1,987万人，ビジネス利用者が291万人である。この予測によると，今後，利用者数は毎年400～500万人程度のペースで伸び続け，2018年度には4,000万人を超えるとのことである。



（注）利用者数は，1か月に1回利用がある人を重複なしに数えた場合の数

図5　公衆無線LANサービスの利用者数［万人］[9]

3）通信ネットワーク上の2点間を結ぶ仮想的な直結回線を設定すること。

4.2　利用環境整備の必要性

東京五輪・パラリンピックの開催などに伴い訪日外国人（インバウンド）を増加させようとする取り組みが行われており，年間の訪日旅行客を，2013年の1000万人強，2016年の2400万人前後の実績に対し，2020年には4000万人に拡大しようという政府目標が立てられている。その反面，訪日外国人向けのアンケート結果では，滞在中に最も困ったことのトップが，日本滞在時にインターネットを経済的かつ容易に利用するための手段である公衆無線LANサービスの環境整備の遅れとなっている（図 6 [3]）。このため，利用環境整備の取り組みが急務とされている。

4.3　政府の取り組み状況

「明日の日本を支える観光ビジョン構想会議」では，2016年 3 月，明日の日本を支える観光ビジョンの柱となる 3 つの視点のうち，視点 3 として「すべての旅行者がストレスなく快適に観光を満喫できる環境に」を掲げ，通信環境の飛躍的向上のための取り組みとして，以下の 5 点を挙げている[10]。即ち，

①2020年までに，主要な観光・防災拠点における重点整備箇所（推計29000箇所）に，無料 Wi-Fi 環境の整備を推進

②災害用統一 SSID を利用した災害時におけるキャリア Wi-Fi を含む Wi-Fi の無料開放を促進

③2018年までに，20万箇所以上で，事業者の垣根を越えてシームレスに Wi-Fi 接続できる認証連携の仕組みを構築

④2020年までに，プリペイド SIM 販売拠点を倍増させ，無料 Wi-Fi 環境と相互補完的

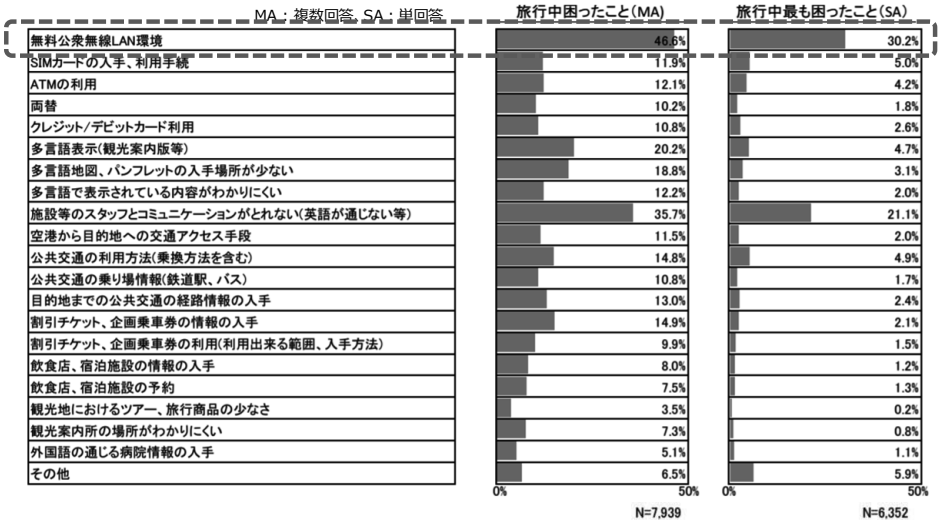


図 6　訪日外国人旅行者へのアンケート結果（一部）[3]

に通信環境全体を改善（複数国からの国際便が乗り入れる全ての空港（21箇所），訪日外国人が訪問する拠点の店舗数1500箇所）

⑤新幹線トンネルにおける携帯電話の通じない区間の解消を加速

また，総務省では，自治体及び第三セクターを対象に，2014年度から「観光・防災Wi-Fi ステーション整備事業」，2016年度から「公衆無線LAN環境整備支援事業」を実施しており，観光や防災等の観点から，地域活性化等に寄与する公衆無線LAN環境の整備を促進している。また，訪日外国人がより円滑に無料公衆無線LANサービスを利用できる環境の実現に向けて，2016年２月には，利用開始手続の簡素化・一元化の推進のために，⑴共通の技術仕様の策定，⑵実証実験の実施，⑶全国各地への普及を内容とする取組方針を策定している[11]。

また，2016年１月には，2014年から３回に亘る幹事会を経て，観光庁と総務省との連携により，訪日外国人旅行者向けの無料公衆無線LANの整備促進に取り組むための協議会『無料公衆無線LAN整備促進協議会』を設置した[4]。当該協議会では訪日外国人旅行者が利用できる無料公衆無線LANスポットの視認性を高めるため，共通シンボルマーク（Japan.Free Wi-Fi）（図７）を策定している。

４.４　民間や地方自治体の取り組み状況

観光庁や総務省など国による公衆無線LAN環境の整備に向けた取り組みの方針を受け，民間の施設管理者，同通信事業者，地方自治体などにおける利用可能拠点の拡大や利便性向上の取り組み，さらにはこれらを支援する製品の提供などが積極的に行われている。利便性の向上としては，以下のような取り組みが行われている。

①スマホアプリの導入：初回だけ登録すると次回からはタップのみでログイン可能（ファミマのアプリ）

②多言語への対応：日本語以外に英語，中国語，韓国語

③事前登録なしに利用可能（利用規約に同意するだけ）：タリーズ，富山県

④メールアドレスなどを初回だけ登録するだけで，その後は簡単に利用可能（中野区，徳島などの自治体）

⑤案内所などでパスポート提示でIDとPWDを入手可能

⑥利用できる場所の地図表示：和歌山県

図７　共通シンボルマークのデザイン[4]

表 4 に公衆無線LANサービスの環境整備に関する取り組み状況を示す。

表 4　公衆無線LANサービスの環境整備に関する取り組み状況

分類	利用可能拠点の拡大や利便性向上			支援製品の提供
	施設管理者	通信事業者	地方自治体	
取組事例	【小売店舗内】 ①家電量販店：ﾋﾞｯｸｶﾒﾗ、ﾖﾄﾞﾊﾞｼ、ｺｼﾞﾏなど ②ｺﾝﾋﾞﾆ：7&I、ﾛｰｿﾝ、**ﾌｧﾐﾘｰﾏｰﾄ（接続ｱﾌﾟﾘ）** ③ｶﾌｪ、飲食店、ﾌｧｰｽﾄﾌｰﾄﾞ店：ｽﾀｰﾊﾞｯｸｽ、ﾄﾘｰｽﾞ/ﾀﾞｲﾔﾓﾝﾄﾞﾀﾞｲﾆﾝｸﾞ、ｴｰ･ﾋﾟｰｶﾊﾞﾆｰ（塚田農場等）/ﾌﾚｯｼｭﾈｽ（訪日客他すべて無料、制限なし）、ﾏｯｸ（拡大中）、ﾓｽﾌｰﾄﾞｻｰﾋﾞｽ（2016年内に1200店舗）、など ④その他：薬局（ツルハHD）、みやぎ生協（48店舗） 【交通関係】 ⑤駅やその周辺：東京ﾒﾄﾛ･東京都交通局（専用ｱﾌﾟﾘ使用）、JR東日本（山の手線、中央線、他拡大中）、京急（ｱﾌﾟﾘ）、東急（渋谷駅周辺・商業施設）、京成、東武、西武、秋葉原地域、北海道中央ﾊﾞｽ（宿泊施設のWi-Fi機能整備） ⑥車内（駅とは別に）：都営地下鉄・東京ﾒﾄﾛ（地下鉄車内）、高速ﾊﾞｽ（ﾊﾞｽ車内）、西部（特急車両内）、東京ﾓﾉﾚｰﾙ（車内）、横須賀線一部（車内）、ｴﾑｹｲや大和自動車交通のﾀｸｼｰ（車内）、など 【ｽﾀｼﾞｱﾑ関係】 ⑦ｽﾀｼﾞｱﾑ：東京ﾄﾞｰﾑ（ｿﾌﾄﾊﾞﾝｸ機能を利用）、ｼﾞﾘｰｸﾞ：**ｽﾏｰﾄｽﾀｼﾞｱﾑ**（NTT東）	①ｿﾌﾄﾊﾞﾝｸ：訪日外国人向けにスポットを無料開放、行動ﾃﾞｰﾀを収集,携帯番号+pwd入力で2W無料、FREE Wi-Fi PASSPORT ②NTT：駅構内などの公共施設や福岡市などで無料開放、ｼﾞﾘｰｸﾞｽﾏｰﾄｽﾀｼﾞｱﾑの実証実験など） ③KDDI：約24万拠点のうち6万拠点を無料開放、その他提携店舗で買い物や来店に対し無料開放 ④ﾋﾞｯｸﾞﾛｰﾌﾞ：8万AP（ｺﾝﾋﾞﾆ、主要駅、新幹線車内、ｶﾌｪなど）で利用可能。有料。	①長野県：旅館・ﾎﾃﾙに補助金,駅・ﾊﾞｽﾀｰﾐﾅﾙ ②徳島県：避難所、公園、防災拠点 ③富山県：駅周辺（案内所、商業施設） ④和歌山県：利用できる場所の地図表示（ｴﾇｼｽ+NTTｸﾞﾙｰﾌﾟ） ⑤沖縄県：提供エリアの拡大（ホテル、観光・商業施設、飲食店、空港など。沖縄セルラー電話など）、沖縄全島フリーWi-Fi共同実証実験推進協議会、スマホアプリの利用。 ⑥東京中野区：駅周辺から区全域へ拡大 ⑦東京渋谷区（NTT東日本と）：区内の店舗ﾔｵﾌｨｽ（平常時+災害時対応）	①**ASAHIネットおまかせWi-Fi**：ﾒｰﾙｱﾄﾞﾚｽなどの登録で端末や通信会社に関係なくﾈｯﾄ利用可能（ﾌﾚｯｼｭﾈｽﾙﾍﾟや坂善商事にて採用） ②NTTﾌﾞﾛｰﾄﾞﾊﾞﾝﾄﾞ・ﾌﾟﾗｯﾄﾌｫｰﾑ：ｼﾞｬﾊﾟﾝ・ｺﾈｸﾃｯﾄﾞ・ﾌﾘｰWi-Fi ③USEN：公衆無線LAN接続ｼｽﾃﾑ ④ﾍﾟﾈﾌｨｯﾄ・ﾜﾝ+ﾜｲﾔﾚｽｽﾎﾟｰﾄ：飲食店割引とWi-Fi利用を海外7拠点で（SIMカードとして）訪日客向けに販売 ⑤ﾌｫﾝｼﾞｬﾊﾟﾝ：ワイファイ共有サービス「FON」 ⑥**BEACONETS**：BLEを使って公衆無線LANへ自動接続できるﾋﾞｰｺﾝ（FNETS）

この表の中の取り組み事例として 4 例（注：表中で太字で示している）を紹介する。

【事例 1】ファミリーマート Wi-Fi 簡単ログインアプリ（ファミリーマート）[12]

ファミリーマートが2015年 2 月16日に配信を始めた，スマホ向けのアプリで，名前のとおり，店舗内での Wi-Fi 接続を簡単に行えるようにしたものである。ファミリーマートでは店舗内での Wi-Fi 接続サービスを2013年に開始しているが，接続の都度，メールアドレスとパスワードを打ち込むが必要があった。

このアプリを利用するにあたり，初回だけメールアドレスとパスワードを入力するだけで，２回目以降は画面上のログインボタンをタップするだけでインターネットへ接続できる。ファミリーマートとしては，このアプリの導入により，消費者に来店を促すことやこのアプリを経由してクーポンやキャンペーン情報を配信し販売促進を図ることなどを狙っている。

【事例 2】スマートスタジアム（Jリーグ＋NTT）[13]

「スマートスタジアム」とは，観客がスマートフォンやタブレットなどを利用しスポーツの観戦を複合的に楽しめる競技場のことである。2020年の東京五輪・パラリンピックに向けて，NTTがその仕組みなどを検討している。例えば，観戦中に選手の情報を検索したり，見逃したシーンを視聴できたり，飲食物を注文したりできる。NTTは，大宮アルジーヤの本拠地「NACKスタジアム大宮」に Wi-Fi のスポットを75か所設置し，無料で高速ネット通信が楽しめる環境を構築した。

【事例 3】ＡＳＡＨＩネット おまかせ Wi-Fi（朝日ネット）[14]

朝日ネットが，2014年 9 月に提供開始した『ＡＳＡＨＩネット おまかせルーター』と関連したサービスで，「ＡＳＡＨＩネット おまかせルーター」の全機能に加え，AP機能やAP利用者向けのコンテンツ配信機能まで利用できるようにしたサービスである。

フレッシュネスバーガーを運営するフレッシュネスでは，このサービスを利用し，2015年６月10日より，都内の６店舗で訪日外国人だけでなくすべての利用者が無料で Wi-Fi を利用できるようにし，その後も全国の店舗に提供範囲を広げつつある。同様に洋服のサカゼンでも，2015年10月１日より，このサービスを導入している。

【事例４】BEACONETS（富士通ネットワークソリューションズ）[15]

富士通ネットワークソリューションズ（FNETS）が2015年11月11日に販売開始した，Bluetoothを活用した情報配信型ビーコン である。Bluetooth通信を活用した一般的なビーコンと異なり，情報配信量を31バイトから240バイトに拡張している。このため，ビーコン発信機器からURLや無線LAN接続に必要な情報（SSID，セキュリティキー），短いメッセージ文などを管理サーバー経由なしに直接送信できる。制御するアプリを起動していると，無線LANのスポットへ近づくだけで，SSIDやセキュリティキーを自動で送信しその無線LANへ接続できる。

４.５　今後の課題

公衆無線LANにおける今後の課題として，無料サービスにおける不正利用対策，利用者数の増加に伴う性能低下対策が考えられる。

⑴　無料の公衆無線LANサービスにおける不正利用への対応

自治体などでは「無料」で提供している公衆無線LANサービスが多い。電話会社やネット接続事業者と契約せずに誰もが利用できる点で便利である。反面，この場合は利用者を特定することが難しい。この点を悪用した犯罪も増加している。例えば，他人のIDやパスワードを入手し，それを使って（公衆無線LAN経由で）通販サイトにアクセスし不正注文したり，あるいは（公衆無線LAN経由で）他人のブログにアクセスし脅迫する内容を書き込んだりする，などが知られている。このような場合，実際にアクセスした人が誰なのかを特定できない点が問題となる。発信元を隠してサイバーテロや犯罪を引き起こす可能性も想定される。このようなことから，総務省では，2016年度より自治体の整備する公衆無線LANの一部（即ち，整備費の補助を行った自治体の無線LAN）で利用者のメールアドレス等を事前登録する制度を義務化した。しかしながら，事前登録は使い勝手の面では逆効果となり利用者数の減少にもつながる恐れがある。利便性を担保した上で不正利用の防止をどのように実現させるかの検討が必要である。

⑵　利用者数の増加や同時利用に伴う性能低下への対応

公衆無線LANサービスのAPは商業施設や公共施設など人が多く集まるところへ設置される。スマートフォンの普及によりLTEなどの携帯電話回線を利用する端末が増加すると速度制限がかかり，トラフィック・オフロードとして携帯電話回線から公衆無線LANのAPへ自動的に切り替わるようなケースが今後増加する可能性が考えられる。APに対する端末の接続数が許容量を超えてしまうと使用できなくなる。使用できても通信

速度が低下する事態も起こり得る。設置主体である施設管理者や通信事業者は，APのトラフィックデータを収集・監視し，同時接続数の変動を吸収し得るようなAP数の設備を適正化するよう管理していく必要がある。

5．まとめ

以上，本論文では，インターネットを利用する際の接続手段として今後益々利用環境の整備が求められる公衆無線LANサービスについて，技術面，サービス面，利用環境整備の取り組み面に着目して，これまでの経緯や現状，今後についてまとめた。

まず，公衆無線LANサービスのベースとなる無線LAN技術とその進展を概観し，その後，利用環境整備が急がれている公衆無線LANサービスについて，その仕組みや利用環境整備の取り組み状況，当面の課題などについて示した。

無線LANの技術面では，通信速度の高速化が進行し，数100M ～数Gbpsクラスで，ひとつのAPを複数の端末で同時使用できるものが登場している。今後の通信需要の拡大に対応して製品の開発が加速され普及していくものと考えられる。

利用環境整備の取り組みについては，東京五輪・パラリンピックの開催等に伴う政府の訪日外国人拡大政策に後押しされて，利用可能な拠点の拡大や利便性の向上，関連製品やスマートフォンアプリの開発などが民間や地方自治体において積極的に推進されていくものと予想される。その裏で，特に無料の公衆無線LANサービスについては，不正利用に対するセキュリティの確保という面と接続の利便性を高めるという面とのトレードオフをどのようにとればよいか，その落とし所の検討が求められる。

参考文献・サイト

［1］外国人旅行客 2000万人突破，読売新聞，2016.11.30

［2］外国人旅行者に対するアンケート調査結果について，観光庁，http://www.mlit.go.jp/common/000190659.pdf

［3］「訪日外国人旅行者の国内における受入環境整備に関する現状調査」結果，無料公衆無線LAN整備促進協議会，第 3 回幹事会資料，資料 2 別添，H28.1.12，http://www.mlit.go.jp/common/001115689.pdf

［4］無料公衆無線LAN整備促進協議会，http://www.mlit.go.jp/kankocho/Wi-Fi-kyougikai.html

［5］浅井裕介，井上保彦，鷹取泰司：IEEE 802.11における無線LAN標準化動向，NTT技術ジャーナル，2013年 8 月

［6］無線LANの基礎と最新技術動向 – JPNIC，https://www.nic.ad.jp/ja/newsletter/No61/0800.html

［7］FREESPOT，http://www.freespot.com/index.php
［8］野澤裕一，小川貴之：「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 テクニカルウォッチ，2016年 3月30日発行，https://www.ipa.go.jp/files/000051453.pdf
［9］ICT総研｜市場調査・マーケティングカンパニー，http://ictr.co.jp/report/20150416000081.html
［10］明日の日本を支える観光ビジョン―世界が訪れたくなる日本へ―，明日の日本を支える観光ビジョン構想会議，平成28年３月30日，http://www.mlit.go.jp/common/001126598.pdf
［11］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，報道資料，H28.2.19，http://www.soumu.go.jp/menu_news/s-news/01kiban04_02000102.html
［12］ファミリーマートWi-Fi簡単ログインアプリ　使い方，http://www.family.co.jp/services/famimawi-fi/howto.html
［13］NTTグループによる「スマートスタジアム」サービス　第一弾（報道発表資料），http://www.ntt.co.jp/news2016/1606/160624a.html
［14］『ＡＳＡＨＩネット おまかせルーター』を提供開始（プレスリリース），http://asahi-net.jp/companyinfo/news/20140908release.pdf
［15］情報量が８倍！「情報配信型ビーコン BEACONETS」を販売開始（プレスリリース），http://www.fujitsu.com/jp/group/fnets/resources/news/press-releases/2015/1111.html