

# どうする? 庁内・地域の 無線LAN

「無線LANは有線LANよりも危険である」  
これについては本特集で何度も触れるが  
この結論を覆すことはしない。  
もちろん、これはセキュリティ面での話であり  
無線LANが有効なケースは多々ある。  
重要なのは、無線LANを活用するときに  
十分なセキュリティ対策を施すことである。

## Part 1 u-Japanを担う無線LAN

「無線LANのセキュリティ技術を把握し  
安全な状態で活用すべき」

Part 2 総務省総合通信基盤局 藤本昌彦氏

Part 3 無線LANで地域情報化促進「みあこネット」

# u-Japanを担う無線LAN

無線LANは最先端の情報インフラとしてその将来像が見え始めてきた。  
セキュリティの問題は常に付きまとうが便利なものは使わずにはいられない。  
あえて例えるなら、交通事故による死者が1万人でも  
自動車社会を否定できないのと似ている。  
これは暴論だろうか。

編集部 = 文

麻生太郎総務大臣は平成16年5月11日、経済財政諮問会議で「u-Japan」構想を提案した。2010年を目標に、いつでも、どこでも、何でも、だれでもネットを利用できる社会を目指し、最終的には「世界の先進国の中で最も活力ある高齢化社会」の実現につなげたいとのこと。「u」は「ユビキタス」だが、麻生大臣の「ユニバーサルでもいい」という発言は、そこに起因している。

つまり、u-Japanはパソコンや情報家電、携帯電話といった情報機器をすべての国民で利用できる社会を目指すとも解釈できる。これまでのところ、u-Japan構想では無線LANについては触れられていないが、「いつでも」「どこでも」を実現するには無線LANの活用を避けては通れない。むしろ、安全な無線LAN環境の提供がキーポイントになると言っても過言ではない。

やや飛躍した話になるが、u-Japanの究極は無線LANスポットの無料化と、携帯電話のIP化(IP携帯電話)による利用料無料化に行き着くとも予想できる。いつでも、どこでも、だれもが無料でインターネットを利用できれば、「世界の先進国の中で最も活力ある高齢化社会」の実現も夢ではない。それゆえ、行政のサポートも重要になる。道路を歩くのが無料であるのと同様に、インターネットも本格的に社会イン

フラ化する可能性が十分にある。

## 庁内での無線LAN使用には運用規定をしっかりと決める

話を無線LANに戻そう。自治体における無線LANの活用には二つのシーンがある。一つは庁内LAN。もう一つは、地域情報化での情報インフラとしてである。

庁内LANについては、セキュリティが気になるところだ。無線LANは電波を飛ばすことから、庁外で電波が傍受される可能性は否定できない。つまり、データが無線LAN経由で漏洩する可能性があるということである。

ただし、現在の無線LAN技術では、かなり高いレベルのセキュリティ対策を実現しているため、設定さえしっかりしておけば、さほど心配する必要はないのかもしれない。その証拠に民間企業では無線LANの採用実績が増え続けている。調査会社IDCジャパンは、平成14年から平成19年までの無線LANの年間平均成長率が出荷ユニット数ベースで31.7%の伸びをみせるとの予測を平成15年9月に発表している。ただし、維持すべきセキュリティレベルに対応したポリシーと運用規定を設定し、監視する仕組みも必要である。

言うまでもなく、無線LANは配線の

必要がないのが最大メリットである。そのため、古い庁舎などで床下配線ができない建物では、無線LANが非常に有効であるし、市町村合併などによる大幅な組織変更でも、無線LANであればオフィスレイアウト変更時にかかるコストを削減することができる。

## 何が危険かの説明は必要だがセキュリティ管理は自己責任

無線LANは地域情報化対策の一環として利用できる。例えば、商店街の活性化のために、あるポイントに基地局を置くことで、利用客にインターネットを開放できる。

こうした、いわゆる“公衆無線LAN”は、都市部を中心に広がり始めている。ただし、公衆無線LANは手軽に利用できる反面、セキュリティ対策が脆弱な場合もある。基本的に前述の庁内LANと同じ問題を抱えているうえ、不特定多数が利用するという危険性がある。そのため、公衆無線LANの利用者には、そういった問題点をあらかじめ理解してもらわなければならない。

なお、50ページで紹介する「みあこネット」は、公衆無線LANでありながら最先端のセキュリティを装備している。ぜひ、地域情報化の参考にさせていただきたい。

# 「無線LANのセキュリティ技術を把握し 安全な状態で活用するべき」

総務省は平成16年4月26日

無線LANのセキュリティに関するガイドライン

「安心して無線LANを利用するために」を公表した。

これは京都大学教授 吉田 進氏が座長を務める

「無線LANセキュリティ調査研究会」の検討を受けて

総務省 総合通信基盤局 電波部 移動通信課で作成したものである。

同ガイドラインの内容、そして無線LANのセキュリティについて

移動通信課 企画官の藤本昌彦氏に聞いた。

編集部 = 取材 / 文

まずは、「安心して無線LANを利用するために」として公開されたガイドラインの概要と目的について教えてください。

藤本 このガイドラインを作るに至ったのは、無線LANにはセキュリティ機能が用意されているにもかかわらず、使われていないことが多いという実態

があるからです。しかも、そういう機能があることを知っている人は、実は多い。設定が面倒というのもあるでしょうし、危ない目に遭うまで、なかなかその危険性に気づかないものです。そのため、ガイドラインではセキュリティの設定を促したいというのが一つ。それ

と、これまでの無線LANのセキュリティ技術には脆弱性がありました。最近では、安全を確保できる技術が出てきましたので、そちらを使ってもらうための啓蒙が必要と考えたのです。

## アクセスポイントの 成り済ましに要注意

ガイドラインの前半ではイラストなどを使って、無線LANの危険性をわかりやすく伝えています。ただ、予備知識のない人には、非常にセンセーショナルな内容だと思ってしまうのですが、「本当？」と疑う人もいませんか。

藤本 ガイドライン策定の基となった「無線LANセキュリティ調査研究会」では実際に飛んでいる電波を調べました。その結果、非常に無防備な無線LANが多いことがわかったのです。

メールの内容のほかにIDやパスワードも実際に見えたのですか？

藤本 何も設定しなかったら、簡単に見られます。通信内容を傍受できてしまうわけですから。もちろん、他人に成り済

無線LAN製品のセキュリティ機能(総務省が公表した無線LANのセキュリティガイドラインより)

セキュリティ機能	説明	
WEP	きちんと暗号化されているか	無線LAN通信を暗号化するための規格。ただし、現在のWEPには脆弱性が指摘されている
MACアドレス フィルタリング	アクセスポイントに端末のMACアドレスを登録した人は通信できて、登録していない人は通信できない	通信機器固有の識別子であるMACアドレスを用いてアクセスポイントに接続可能な無線LAN端末を制限する方式。ただし、MACアドレスは、容易に割り出し、詐称することができる
SSID	アクセスポイントのSSIDを知っている人だけが通信でき、知らない人は通信できない	無線LANのネットワークの識別子として利用されており、アクセスポイントと同一のSSIDを設定した無線LAN端末が通信可能となる。ただし、現在では、Windows XPや一部の無線LANカードのユーティリティソフトを使うとSSIDは容易に見ることができ、セキュリティ機能として用いるには問題がある。このため、一部のアクセスポイントにはSSIDを隠蔽する機能(ステルス機能)が用意されており、これを用いることでSSIDを容易に見ることができなくなる
IEEE802.1x 認証	暗号化されたものを信頼する人たちが一人ひとりに届けてくれれば、安心して通信を行うことができる	IEEE802.1xに対応した無線LAN端末(ノートパソコン等)とアクセスポイント、認証サーバーを用いた、ユーザー認証と個別暗号の鍵配布を行う方式
WPA		WEPの脆弱性を補強するためにWi-Fi Allianceによって策定されたセキュリティ規格。WPAは一つの技術によるセキュリティ機能ではなく、ユーザー認証を行う「IEEE802.1x」、新しい暗号化方式である「TKIP」などを組み合わせて高セキュリティを実現。WPAにはアクセスポイントと無線LAN端末にPre-Shared キーを設定するWPA-PSK方式とIEEE802.1x 認証と組み合わせて動作するWPA-EAP方式がある

「無線LAN区間だけのセキュリティ対策のほか  
VPNを活用したり、SSLで暗号化するなど  
無線LAN区間だけでなく、全体で考えてほしい」

総務省 総合通信基盤局 電波部 移動通信課  
企画官

## 藤本昌彦氏



ましてメールを送ったりもできます。

**データの改竄や消去など、要は何でもできてしまう。**

藤本 はい、まったく無防備の状態ですから。これまでの説明は容易に想像できますが、意外と知られていないのがアクセスポイントに成り済ます方法です。いつものアクセスポイントに接続したつもりが、別のところにアクセスしているというわけです。

**確かに、それは意外と盲点かもしれません。**

藤本 だから、無線LANのセキュリティはしっかり設定しましょうということになるわけです。これまで無線LANで使われてきたセキュリティ機能は「WEP」「MACアドレスフィルタリング」「SSID」です。しかし、これらはいずれも脆弱性があり、無線LANをセキュアな環境にするには、「IEEE802.1x認証」「WPA」などを利用する必要があります(左表)。ただ、こうした無線LAN区間だけのセキュリティ対策のほかにも、VPN(Virtual Private Network: 仮想専用線)を活用したり、SSL(Secure Socket Layer)で暗号化してデータをやり取りしたりすることも重要です。無線LAN区間だけでなく、全体で考える必要があります。

### 有線LANでもVPNによって 外部のパソコンは接続不可に

最新の技術を導入すると、無線LAN

はすごいセキュアになると感じる人がいると思います。例えば、ネットワークに接続するのにも、しっかり認証するから、有線よりも安全な気すらしても無理はないのかと。なぜなら、一般的に自治体ではネットワークケーブルにパソコンを接続しただけで、ネットワークに参加できますから。

藤本 それは過信しすぎです。もし、無線LANのほうが安全だとしたら、だれも有線を使いませんよ。有線は配線の手間がありますが、無線ならアクセスポイントを置くだけでいい。手軽に使えてセキュアなら、だれもが無線LANを使用します。

**とはいえ、外から持ち込んだパソコンで、庁内にウイルスが蔓延するといったことが、無線LANのセキュアな環境によって防げるとも、考えられます。**

藤本 ウイルスはネットワークのセキュリティとは別に考えるべきで、無線だろうが有線だろうがウイルス対策は必要です。また、有線でもネットワークケーブルにパソコンを接続しただけでネットワークに参加できるのも、本来は問題なのでしょうね。各自治体でセキュリティポリシーを設定していますが、そういったところで根本から検討する必要があります。

### セキュリティ技術は日々進歩 無線LANの設定も簡単になる

実は最近、自治体で無線LANを使っているという話を聞かなくなったのです。

過去に使っていても、今は外してあるとか、ちなみに中央官庁でも使っていないですよ。

藤本 使ってはダメというわけではないのです。総務省ではセキュリティ責任者が差し支えないと判断した場合は、無線LANを使ってもいいのです。ただし、端末機器の認証に十分な暗号化をしなければならなかったり、セキュリティ要件が厳しいので、そうまでして使う必要はないだろうと。

**自治体も同じような状況ですか。**

藤本 意外と使われていると聞いています。ただ、役所は個人情報を扱うので、漏れたらとか、盗聴されたらとか、そういったことには非常に神経を尖らせていないといけません。要は、無線は有線よりも余計な心配が必要だから、面倒なので有線にしようという話になる。

**ところで、ここまでお伺いした感じだと、ガイドラインを出したとはいえ、無理に無線LANを薦めるのではないのですか。**

藤本 もちろん、使うのは自由です。無線LANのセキュリティ技術は日々進歩しているので、セキュリティの設定も簡単になります。あまり面倒なことを気にする必要がなくなれば、無線LANは一気に普及すると思います。

# 京都発「みあこネット」 無線LANで地域情報化促進の実現へ

インターネットをいつでも、どこでも、だれにでも。  
それも無料で！  
京都を情報自由都市にすべく、「みあこネット」がスタートする。  
ここで使われているのは、もちろん無線LAN。  
それゆえ、「みあこネット」の取り組みには  
地域インフラの整備という視点でも、学ぶべきことが多い。

倉増 裕 = 取材 / 文

京都発の無線インターネットサービス「みあこネット」がスタートしたのは、2002年5月。市民みずからが自分の住んでいる地域を情報化するプロジェクトとして、NPO(特定非営利活動)法人である日本サスティナブル・コミュニティ・センター(SCCJ)によって「みあこネット」は立ち上げられた。

SCCJが「みあこネット」をスタートさせた目的は「だれもが、どこでも、安全にインターネットを利用できる環境を実現する」(SCCJ代表理事・高木治夫氏)ことにある。

## 無線インターネットの利用は 「自己責任で」では発展しない

「みあこネット」のほかにも無線LANを活用し、不特定多数を対象とした無線インターネットサービスが公共施設やファーストフード店、街角、さらには移動中の乗物へと広がっている。このようなユビキタス環境を実現するにあたって、無線LANが大きな戦力となることは言うまでもないが、問題はその

安全性だ。もちろんセキュリティは無線だけの問題ではないが、だれもがキャッチできるという無線ならではの固有の問題があることは事実だ。

そのため、無線インターネットサービスでは、自己責任において利便性と安全性を勘案して、問題ないと考えられるレベルでの情報活用を行うというのが常識である。

しかし運営主体として、この常識に甘んじることがあってはならないというのが「みあこネット」の基本姿勢だ。

つまり「無料サービスだからセキュリティは適当というのでは地域情報化を阻害する。無料といえども安全性を保証してこそ社会のインフラとなる」(高木氏、以下同じ)との考え方が基本にある。

セキュリティの重要性を指摘することはたやすい。しかし不特定多数に開かれた無線環境で、これをどのように実現するのか。「みあこネット」はこの実現に向けて、技術的課題の克服、市民参加をベースとしたビジネスモデルの構築、技術や環境の変化を見通したうえでのシステム展開を開始した。

この三つの側面におけるオリジナル路線に、今後の社会インフラとしての「みあこネット」普及の大きな可能性が隠されている。

## 電話は気軽に借りられるのに インターネットは借りれない

スタートしてから約2年、この間「みあこネット」は大きな変化を遂げた。そしてこの変化にこそ「みあこネット」の目指す方向性と主張の色濃い反映を見ることができる。

まずサービス開始当初の『みあこネット1』では、技術的には無線部分のセキュリティを確保するという大きな課題を克服している。詳細な解説は省くが、ここでは「動的に切り替わる個別のカギ」「2段階認証」などを活用してセキュアな環境を用意した。

また、SCCJにはもともと、障害者と健常者の壁を取り払うことによって、だれもが暮らしやすい世界を目指すという大きな目標があった。そこで、その壁を取り払う手法として、視覚障害



「無料サービスだからセキュリティは  
適当というのでは地域情報化を阻害する。  
無料といえども安全性を保証してこそ  
社会のインフラとなる」

NPO法人日本サステナブル・コミュニティ・センター  
代表理事

## 高木治夫氏

者向けのキー入力システム「打ち込み君」や新聞コンテンツ読み上げシステム「ユビキタス・ラジオ」などを相次いで実用化した。いつでもどこでもだれにでも安全に使える「みあこネット」の構想も、この延長線上にある。

「外出先で他社の電話は気軽に借りることができるのに、インターネットは違う。端末は持っているから接続口だけを貸してくださいと言っても、なかなか貸してもらえないものでもない。これはセキュリティの問題が絡むので当然だが、世界中に限なく張り巡らされているネットワークなのに、自社以外では使えないのは一般の常識から考えるといかにも不自然」という素朴な疑問があった。「みあこネット」には、それを実現しようという思いも込められている。

### 「みあこネット」は グリーンレンタル感覚

ではインターネット環境における「みあこネット」の存在価値とは何か。高木氏はこれを飲み水との比較で説明する。

つまり無線インターネットサービスのない時代は、水を飲む場所は自宅が勤務先に限られており、水が飲みたければ自宅や勤務先に戻らねばならなかった。

次に人の集まる地域での無線インターネットサービスが実用化されるに及んで、人は外出先でも水が飲めるようになった。しかし外出先で飲む水とはあくまで一般的な意味での水という液体のことであり、この水が飲み水として安全であるかどうかはわからない。この水に毒が入っていないという保証はなく、あくまでも自己責任においてこれを飲む覚悟が必要だ。その覚悟がない場合は、少なくとも飲み水としては利用しないに限る。そこで水の安全性を保障、外出先で安心して水が飲める環境として提供したのが『みあこネット1』だ。

水飲み場所はまず10か所からスタートしたが、「だれもが参加できる情報自由都市の建設を目指す」という殺し文句が、伝統を誇りつつ新しいモノ好きという京都の市民感覚を刺激し、3

か月後には100か所を超えた。100か所を超えたころから「みあこネット」は全国にその名が知られるようになり、昨年末には北海道から沖縄まで23都道府県で基地局は300か所超に。

基地局が燎原(りょうげん)の火のように拡大している裏には、「みあこネット」特有の同志的なコミュニケーションの広がりに加えて、基地局オーナーとなったことを後悔させないさまざまなくふうがある。

まず、「みあこネット」の基地局オーナーには希望すればだれでもなることができるが、オーナー負担は月額4,700円であり、「基地局オーナーになっても経済的メリットはまずない」と夢は語らない。では基地局オーナーとなるメリットは何かというと、「感覚としては観葉植物などのグリーンレンタルに近い。客間の亭主として、来客のもてなしには極めて有効で今後の必需品となる」と、おもてなしツールとしてのアピールだ。

この説明に納得すれば晴れて基地局オーナーになることができる。基地局



「みあこネット」を運営する  
日本サステイナブル・コミュニティ・センターの  
オフィス。なんとも家庭的である

の設置作業は無線ルーターにケーブルを接続するだけで完了するという簡単なもので、企業内LANや学内LAN、家庭内LANにそのまま接続できる。基地局を追加しても従来システムの安全性が損なわれる心配がないなど、基地局オーナーとなるにあたっての煩わしさを解消するくふうも、「みあこネット」普及の大きなポイントであるようだ。

## VPNでよりセキュアになった 『みあこネット2』

無線部分のセキュリティの確保に重点を置いた『みあこネット1』を経て、次に『みあこネット2』が登場する。『みあこネット1』から『みあこネット2』への進化の最大のポイントは、「安全な水が飲めるだけでなく、どこからでも自分の好きな水を選んで飲める」ということだ。

具体的にはVPN( Virtual Private Network: 仮想専用線 )に対応することで、インターネットに接続された場所なら世界中どこでも無線ルーターを

接続して基地局を設置することが可能となった。VPNによって、インターネットを経由しながら、プライベートな同一ネットワーク上にいるかのような利便性と安全性が確保できる。どこにいても、「みあこネット」という京都の水を飲めるようになったのである。

もう少し詳細について解説しよう。

オーナーは基地局を設置して無線ルーターをLANに接続する。このとき無線ルーターは自動的に「みあこネット」のサーバーとVPNでつながるため、LANへ影響を及ぼすことはない。

次に、「みあこネット」の利用者が無線ルーターに接続すると、「みあこネット」の認証サーバー( PPTPサーバー )に128ビットで暗号化された通信による認証を受け、正当な利用者であれば接続を許可する。「みあこネット」の利用者は、「無線ルーター」「仮想専用線」「みあこネットのサーバー」「インターネット網」の経路で通信を行う。この途中ではLANへ直に接続できないことから、「みあこネット」の無線ルーターがセキュリティの穴になることはない。

VPN対応によって大きな進化を遂げた『みあこネット2』だが、SCCJの目標とするハードルはさらに高い。当面の大きな問題となるのが、飲み水として安全に浄化するための浄水場の存在だ。

『みあこネット2』はいつでもどこでも好きな水が飲める環境を実現したが、これらの水は浄水用のプールを経由して配られる。『みあこネット2』の運用を経て、「必要とされる大量の水に対して大きな浄水場を用意する従来の方式が必ずしもベストではない」ことがわかってきた。つまり「巨大なプールを用意してすべての水をここに集めて浄水するのではなく、各拠点が充実した浄水機能を持つことによってネットワークの効率と安全性がさらに高まる」との判断だ。

そして『みあこネット2』の次のサービスとして予定している『みあこネット3』では、浄水機能の分散化を実現することになった。より具体的には、各基地局に設置するルーターにVPNサーバー機能を持たせるということで、これに向けたルーターの開発がすでに進ん

でいる。今後のネットワークにおける世界の汎用品としての期待が持たれる製品だ。

## 災害発生時に有効な IPv6を活用した映像発信

VPNサーバー機能を組み込んだルーターによる『みあこネット3』のサービス開始は年内にも実現する見通しだが、その次のバージョンである『みあこネット4』では、IPv4環境からIPv6環境への移行を実現する。

『みあこネット3』から『みあこネット4』への変化を飲料水に例えると「飲みたい水を身近の強力な浄水機で浄化していつでも飲める」環境から、「いつでもどこでも飲めるというレベルを超えて、走りながらでも自由においしい水が無理なく飲める」環境への進化ということになる。

IPアドレス枯渇の抜本的解決として理解されるのが一般的なIPv6への見方だが、「みあこネット」の立場からは「走りながら水が飲めるし、移動中の水でも自宅にいながら飲める」、つまり中継が可能なことが最大のメリットとなると見られている。例えばタクシーの中でも、「みあこネット」を利用できるようになるのである。

また、IPv6のキャパシティを活用することによって、『みあこネット4』では映像の発信が可能になる。

応用例としては災害時の情報発信がある。例えば土砂崩れが発生した場合、下流の危険地域の住民が緊急に必要とする情報と、それ以外の地域が必要とする情報には当然のことながら違いがある。しかし、マスメディアでは地域

ごとに違う放送はできないため、『みあこネット4』を活用することになる。『みあこネット4』の基地局ごとに違う情報を流すことにより、「みあこネット」の利用者は自分に最適な情報を受け取ることができるというわけだ。

災害対策として自治体関連から強い関心を集める要因は、ここにあり、早くも自治体からの引き合いは強いという。

## 携帯電話の無線LAN対応により ネットがみんなのものになる

サービス開始当初の『みあこネット1』を経て現在の『みあこネット2』、まもなくサービス開始を予定している『みあこネット3』、さらには来年の『みあこネット4』と、技術と環境に対応したすばやい進化が「みあこネット」の大きな特徴だ。「みあこネット」を動かす原動力について、高木氏は次のように語る。

「インターネットの有用性は、実は一般に知られているよりもはるかに大きく深い。従来は大企業をはじめとする

一部の人々が享受できたこのメリットを、一般消費者すべてが享受できてこそ本来のコピキタ社会に一步近づくことができる」

高木氏によると、現在のインターネット活用環境は決して人に優しいものではない。「パソコンに慣れなければインターネットが使えないという環境を変えることによって、インターネットは人間に優しいツールとなる。インターネット端末がパソコンである必要は毛頭ない」との立場から、携帯電話が無線LANにも対応することによって、「みあこネット」の標準端末としてだれもが使える環境が実現すると予測する。

「インターネットの世界で安全な水を飲みたいという人は多いにもかかわらず、安全な水が飲めるような環境作りを目指して取り組んでいる人はいるのだろうか。わたしたちは、その実現を目指す。この活動が大きく花開いたとき、インターネットは本当の意味で文化となることができる」という高木氏のことばが、さらに現実味を帯びてきた。[e-Gov](#)

「みあこネット」の基地局。  
基地局の設置作業は無線ルーターに  
ケーブルを接続するだけで完了

