

無線アクセスに関する調査研究報告書

青木栄二

1. 無線アクセスシステムの現状

1.1 国内の状況

1.1.1 無線アクセスシステムの分類

現在、日本で制度化されている無線アクセスシステムは、固定系として FWA と無線 LAN があり、移動系として携帯電話と PHS がある。表 1 - 1 にそれらの特徴を示す。

ここ数年のインターネットの急激な普及に伴い、有線無線に関らずアクセスシステムの技術革新とサービス展開はめざましいものがある。その中でも特に際立っているのが、ADSL と無線 LAN である。本調査研究では、インターネット常時接続環境を必要とされる場所において、柔軟、迅速、経済的に構築可能なものとして無線 LAN を中心に報告する。

表 1 - 1 無線アクセスシステムの特徴

システム名	周波数帯	最大伝送速度	伝送距離	制度化
FWA	22/26/38GHz	156Mbps	3km 程度	1998 年 12 月
	60GHz	1Gbps	数 100m 程度	2000 年 8 月
無線 LAN	2.4GHz	11Mbps	5km 程度	1999 年 10 月
	5.2GHz	54Mbps	3km 程度	2000 年 3 月
携帯電話	800MHz	9.8kbps	-----	-----
	2GHz	384kbps	-----	-----
PHS	1.9GHz	128kbps	3km 程度	1998 年 9 月

1.1.2 無線 LAN システム

無線 LAN とは、2.4GHz 帯周波数を使用する小電力データ通信システムで、ISM(Industrial, Scientific, Medical) バンドと呼ばれ、産業、科学、医療分野での各種応用機器との周波数共用を前提としている。この周波数帯を使用した無線通信は、ISM 機器から発生する雑音などを容認または回避する必要がある。以前使用できる周波数帯域は、2,471~2,497MHz だったのが、1999 年 10 月から新たに追加割り当てされて 2,400~2,483.5MHz となった。また無線 LAN としては、2,4GHz 帯と別に 5GHz 帯でも割り当てが行われているが、こちらは衛星系と同じ周波数帯のため屋内での使用に限定されている。

5.15-5.25GHz 電気通信業務用および公共業務用固定衛星
特定小電力データ通信(屋内のみ)

- 5.25-5.35GHz 地球探査衛星
気象レーダー
- 5.80GHz 高速道路の ETC

国内の ISMバンド内周波数の分配を、図 1 - 1 に示す。

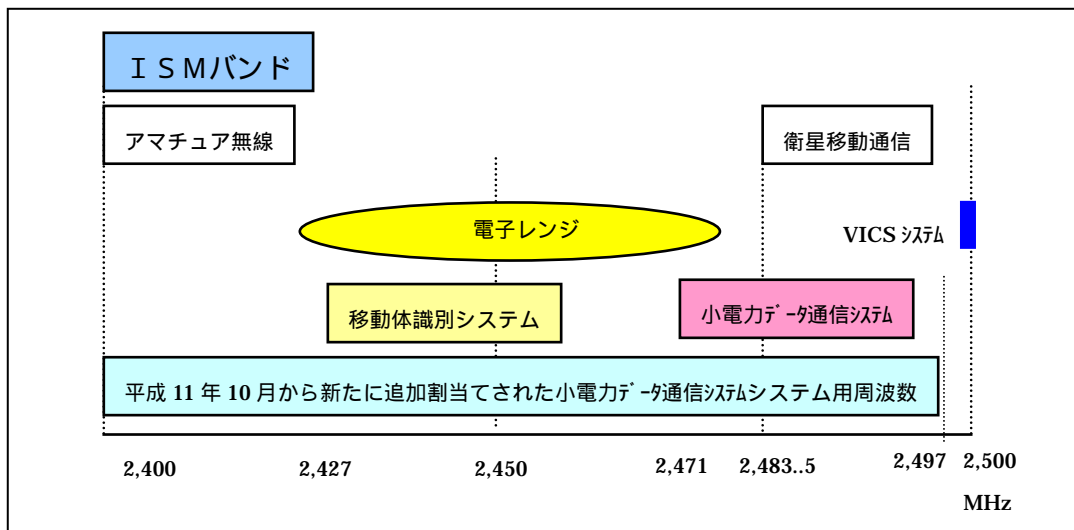


図 1 - 1 周波数分布図

小電力データ通信システムは、共用の周波数帯である ISM バンドの使用を前提としているため、他のシステムからの干渉をある程度許容し、かつ、他のシステムに干渉を与えにくい伝送方式である「スペクトル拡散方式」を採用している。電波の送信出力は 1MHz 幅当たり 10mW 以下である。(平成 11 年 10 月から追加された新たな周波数帯では、スペクトル拡散方式以外の伝送方式の採用も可能となっている。)

また、他の無線システムからの干渉を許容することを条件に、平成 4 年に電波法第 38 条二の 1 及び電波法施行規則第 6 条第 4 項第 4 号の規定に基づく技術基準適合証明制度により無線局の免許を要しないシステムとなっている。なお、小電力データ通信システムの主な技術条件については、表 1 - 2 に示す。

表 1 - 2 技術条件

送信周波数	2,400MHz 以上、2,497MHz 以下
変調方式	FH、DS、又はこれらの複合方式
送信出力	10mW / MHz
空中線利得	絶対利得 2.14dB 以下
占有周波数帯幅	26MHz 以下 (拡散帯域 = 500kHz 以上)
その他	識別符号等の混信防止機能が必要

2.4GHz 帯の周波数の電波を使用する小電力データ通信システムの特長をまとめると以下の点が挙げられる。

- ・ 無線局免許が不要 免許申請手続、手数料、電波利用料等が不要
- ・ 広帯域伝送が可能 約 1Mbps ~ 10Mbps 程度の伝送速度により画像伝送も可能
- ・ スペクトル拡散方式の採用により混信を与えにくく受け難い。秘匿性が高い
- ・ 安 価
- ・ 設置が簡単

また OSI での無線 LAN モデルを図 1 - 2 に示す。

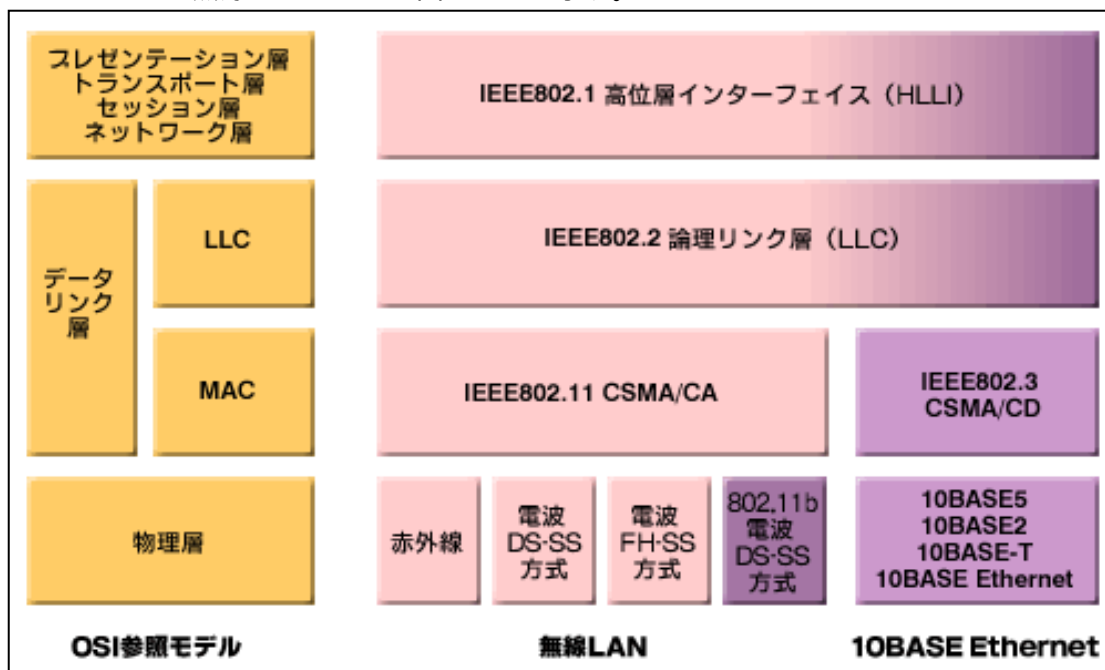


図 1 - 2 OSI での無線 LAN の位置づけ

1.1.3 市場の動向

FWA と比較して、無線 LAN は無線局の免許が不要であり、伝送距離や伝送速度などの面で技術的に安定してきた。そのため電波干渉の心配が少ない地方において、自治体などの自営インフラとしての導入事例も増えてきた。ただし、屋外用無線 LAN ネットワークの構築をできるメーカーは少なく、低価格化だけでは FWA に取って代わることはできない。

一方屋内用については、パソコンの普及により一家に 2 台 3 台となると家庭内に有線ケーブルで配線するより、無線 LAN のアクセスポイントを設置した方が簡単とあって、急激に販売が伸びている。ADSL や CATV などブロードバンドの常時接続回線を導入した家庭では、必需品となりつつある。さらに家電量販店における低価格化が売り上げに拍車をかけている状況である。

その普及の大きな要因として、米国の電気電子技術者協会 (IEEE: Institute of Electrical and Electronics Engineer) が 1990 年に無線 LAN を扱う 802.11 ワーキンググ

ループを設立し、IEEE802.11b という規格が標準化され、メーカーがこぞって新製品に取り組んだこと、それにより互換性ができたことである。以前伝送速度は 1Mbps 程度だったものが、現在では 11Mbps が主流となっている。これだと有線における 10Mbps と何ら遜色なく、むしろ PC カードによっては実効速度において無線の方が速いケースもある。配線だらけの PC 利用者にとっては、非常に利便性の高いものとなっている。

市場は無線 LAN のさらなる高速化を要求しており、2.4GHz 帯では IEEE802.11b の後継版ともいえる IEEE802.11g や 5GHz 帯の IEEE802.11aなどを視野に入れて展開している。

1.2 欧米の状況

1.2.1 周波数の割り当て

(1) 米国

2GHz 帯の動向としては、1998 年 FCC(Federal Communication Commission)により、加入者向けデータおよびインターネットサービスを可能とする MMDS(Multi channel Multi point Distribution Service)が開放された。それ以外では、表 1 - 3 に示すように各種無線アクセスシステムに分配されている。

表 1 - 3 2GHz 帯の各種無線アクセスシステム

周波数レンジ(GHz)	サービス形態	チャンネル数	チャンネル帯域
2.150-2.162	MDS	2	6MHz
2.305-2.320	WCS	2	5MHz, 10MHz
2.345-2.360	WCS	2	5MHz, 10MHz
2.500-2.596	ITFS	16	6MHz
2.596-2.644	MMDS	8	6MHz
2.644-2.686	ITFS	4	6MHz
2.686-2.689	MMDS	31	125KHz

MDS Multi point Distribution Service

ITFS Instructional Television Fixed Service

WCS Wireless Communications Service

5GHz 帯の動向としては、1997 年 1 月に屋内外において免許不要で利用できる無線アクセス用周波数として、5.150-5.350GHz と 5.725-5.825GHz の合計 300MHz が割り当てられた。これらの周波数については、帯域がデータ通信を実現するのに十分であることと、すでに割り当てられている軍事レーダーや航空無線航行などに干渉を与えないことが考慮されている。その結果、表 1 - 4 に示すとおり 3 つの周波数帯において異なる送信電力制限値が設けられた。また 1998 年 6 月に規定が改正されて、5.725-5.825GHz は 23dBi の指向性アンテナを用いた 1 対 1 固定通信にも割り当てられた。

表 1 - 4 5GHz 帯の周波数割り当てと送信電力制限

周波数レンジ(GHz)	送信電力	最大アンテナ利得	出力電力	利用制限
5.150-5.250	50mW	6dBi	200mW	屋内のみ
5.250-5.350	250mW	6dBi	1W	屋内・屋外
5.725-5.825	1W	6dBi	4W	屋内・屋外
		23dBi	200W	屋内・屋外

(2) 欧州

1992年にETSI(European Telecommunications Standards Institute)が、HIPERLAN(High Performance LAN)の標準化に着手して、1993年にCEPT(European Conference of Postal and Telecommunications Administrations)が、5.150-5.250GHzを欧州各国共通の周波数として、5.250-5.300GHzを各国毎の拡張用としてHIPERLAN/1に割り当てた。また1999年11月に追加割り当てとして、5.300-5.350GHzおよび5.470-5.725GHzの周波数帯が決定された。これによって免許不要な無線アクセスシステムは、HIPERLAN Type2として合計455MHzの帯域が使用可能となった。表1-5に欧州の割り当て状況を示す。

表 1 - 5 HIPERLAN 対応の周波数帯

周波数レンジ(GHz)	出力電力	利用制限
5.150-5.250	200mW	屋内のみ
5.250-5.350	200mW	屋内のみ
5.470-5.725	1W	屋内・屋外

1.2.2 システム標準化

(1) 米国

IEEE802.11では、1997年3月から2.4GHz帯と5GHz帯のワーキンググループが中心に活動を行ってきた。これらのワーキンググループに関しては、1998年7月に基本変調方式が採択された後、詳細な議論が行われている。また5GHz帯の変調方式の議論については、その詳細が詰められる中で、並行してグローバルな標準化活動の視点から欧州のETSI BRAN(Broad band Radio Network)とMMAC推進協議会5GHz帯移動アクセス特別部会のイーサネットワーキンググループとの間で共存問題を検討して、互いに協調した規格化を目指してきた。下記にIEEE802.11のワーキンググループ一覧を示す。

802.11a 5GHz帯で動作する物理層の無線技術を作成することが目的。

802.11b 2.4GHz帯の高速無線技術を作成することが目的。

802.11c 802.1Dブリッジに追加する802.11MAC独自の仕様を作成。

有線LANと無線LANの橋渡しをするためのもの。

- 802.11d 802.11 規格が使用できない国や地域に向けた仕様を作成。
- 802.11e 無線上で QoS をサポートするための拡張 MAC 規格を作成。
- 802.11f IAPP(Inter Access Point Protocol)の作成。
IAPP はサブネットをまたいだローミングを可能にする字術。
- 802.11g 11b の高速版として上位互換性があり最大 54Mbps を実現する。
- 802.11h 802.11MAC と 802.11a の物理層無線技術に追加する DCS と TPC を規定。
DCS(Dynamic Channel Selection)
TPC(Transmit Power Control)
- 802.11i 802.11MAC のセキュリティを改善する仕様を作成。

(2) 欧州

ETSI のプロジェクトとして、BRAN が固定系や移動系の無線システムの標準化に取り組んでおり、HIPERLAN Type2 として 5GHz 帯の無線アクセスシステム、HIPERACCESS として準ミリ波やミリ波帯の FWA(Fixed Wireless Access)の標準化を進めている。なかでもニーズが増大しつつある HIPERLAN Type2 に関しては、日本および米国と同一の周波数を使用し免許の不要なサービスを目指して、互いに規格の統一を図るよう進められている。

2 . 地域情報化のための無線 LAN

2 . 1 無線 LAN のセキュリティ

全世界オープンなネットワークであるインターネットは、普及すればするほどセキュリティの問題が必ずついてまわる。ネットワークの構築者は、ファイアウォールや認証システム、暗号化などの技術を駆使して、セキュリティを高めようとしているものの、完璧なセキュリティもいつかは破られてしまうという、不正アクセス者とのいたちごっこである。これは有線でも無線でも同じことで、すべての不正アクセスを完全に防ぐことは、不可能だと考えられる。

無線における電波信号は、実際利用する範囲以外の屋内および屋外にも飛んでいくため、到達エリア内なら誰にでも受信することができる。しかし、無線 LAN は一般的なテレビやラジオの利用方法とは異なり、単純に電波を受信したからといって通信の内容がわかるというものではない。PHS の会話の内容がわからないのと同じである。

昨今、無線 LAN の急速な普及により、研究者レベルでは無線 LAN におけるセキュリティの脆弱性について、レポートが出されている。それに伴いメディアも、どれだけ多くのユーザーが無防備に電波を出しているのかを指摘している。それはあくまで受信レベルであって、解読レベルというものではない。確かに ESSID や WEP などのセキュリティをまったく設定せずに使用しているケースも見受けられるが、有線につながれたインターネットの世界でもまったく無防備状態のものが多々存在する。無線 LAN においても利用者側の意識によって、システム全体で高いセキュリティとすることが可能なのである。

2 . 1 . 1 傍受と盗聴

傍受とは、無線通信を交信相手でない者が故意または偶然に受信することであり、盗聴とは、他人の会話を（機器などを用いて）気づかれぬように聞くことである。

一般的には、音声通信の世界である。アマチュア無線機を使用して、コードレス電話機などを盗み聞きする方法で、受信したい周波数を機器の一部改造により、本来なら受信できない周波数帯を受信するものである。こんな傍受はアナログ通信だから比較的簡単に可能となるが、デジタル通信では、暗号化などにより解読できないようにしている。コードレス電話機も最近のものはデジタル化している。

無線 LAN ももちろんデジタル通信であり、さらにスペクトラム拡散という技術を使って、必要となる周波数帯域幅より広く電波を拡散し、空中では電波をゴミのように見せている。この技術は、もともと軍用として開発されたもので、現在でもさまざまな重要通信設備で利用されている。

無線 LAN の電波を受信するには、2.4GHz 対応のアンテナおよびスペクトラムアナライザがあれば可能である。この場合、スペクトラムアナライザで、どのような周波数帯にどれ

くらいの強さで電波が出ているかを表示することができる。しかし、その信号を解読しデータを解析することは、よほどの時間と労力、さらにはコストをかけないと不可能である。果たしてこの単なる電波の受信を傍受と呼べるのか、そのレベルで無線の信頼性が失われるのかは、非常に疑問である。

2.1.2 IEEE802.11b の問題点

通常市販されている IEEE802.11b 準拠の無線 LAN は、次のようなものでセキュリティを確保している。

- ・ スペクトラム拡散 直接拡散方法 (DS 方式) と呼ばれる拡散技術を採用し、拡散符号と呼ばれる符号により電波を拡散
- ・ ESSID 通信を行う各無線機に、すべて共通する文字列を設定することで、ID を知らないユーザーを拒否する。
- ・ MAC アドレス登録 無線機に MAC アドレスを登録して、その固有の機器のみ通信可否の設定を行う。
- ・ WEP データを 64bit あるいは 128bit など暗号化するもの。

このような複数のセキュリティ機能を持っているに、なぜ危ないと言われるのか？ それはひとえに仕様が公開されているからである。標準化を行うことで、各メーカー製品の互換性ができ、業界は発展し普遍性がユーザーメリットにもつながる。しかしその反面、誰でもその技術を手に入れることができるということでもある。

まずスペクトラム拡散の DS 方式で使用されている拡散符号もそのひとつで、符号は 1 種類で公開されている。そのため拡散符号が分かれば、拡散された電波も変調する前の、元の拡散していない電波に戻すことができる。

次に ESSID の場合、「ANY」という設定があり、空港などのホットスポットにおいてどのアクセスポイントにもアクセスできるようにしたものである。この設定をしておけば、仮に固有の ESSID を設定しておいてもアクセスできる可能性がある。本来なら ESSID の意味をなさないのだが、利用の性質上そういった製品もあるということである。また一部の製品の設定ユーティリティでは、ESSID をスキャンして探すことができるものもある。

MAC アドレス登録は、非常に有効であるものの、不正アクセス者は常に不正な方法を考えるもので、仮に何らかの方法でそのアドレスを入手されたら、正規のユーザーになりすまされてしまう。その際は防ぐことができない。

最後に WEP は、無線電波のデータ自体を暗号化するため有効な手段と考えられる。しかし、2001 年 2 月に米国カリフォルニア大学パークレイ校の研究者や、インスタット社のレポートによって、その脆弱性を指摘されている。この問題は、暗号プロトコル設計の見通しの未熟さにあったもので、その重要性を認識し改善することで回避することができると考えられる。既に多くのベンダーがセキュリティ強化に乗り出している。

2.1.3 IEEE802.11b のデータ解析方法

無線 LAN の電波の中身は、無線通信で必要な情報、ネットワーク通信で必要な情報、それにデータ本体である。仮に電波を受信したとしてもデータそのものを見ることは難しい。その電波を解析するものとして、以下のものが必要となる。

- ・ IEEE802.11b 準拠の無線 LAN カード（広範囲の場合はアンテナ）
- ・ 電波スキャンのためのソフトウェア（使用チャンネルのサーチ）
- ・ ESSID 解析のためのソフトウェア
- ・ WEP 暗号解析アルゴリズム搭載のソフトウェア
- ・ ネットワークパケットモニター

暗号アルゴリズム解析のためのソフトウェア以外なら市販されているため、誰でも簡単に手に入れることが可能である。最近では、「無線 LAN 解析ソフトウェア」なるものも登場してきている。しかし、データ内容をすべて傍受盗聴できるという製品ははまだ発売されていない。

そこで実際に電波を総合的に解析するには、多大な費用と有能な労力の投資によるリバースエンジニアリングが必要とされる。興味本位の個人レベルではとても難しく、研究者が学術的な見地から研究するのであれば意味があると思われる。他に考えられるとすれば、スパイ活動や地下組織の企業戦略ぐらいであろう。

2.1.4 IEEE802.11b 準拠製品以外のセキュリティ

IEEE802.11b でも必要な設定を施せばそれなりのセキュリティが確保される。ただし、技術仕様の公開と重ねて、ユーザー側の利用方法によっては必ずしも安全とは言い切れない。

そこで屋外用の無線 LAN については、セキュリティ面を重視するのであれば、IEEE802.11b 準拠以外の製品を導入するのほひとつの選択ではないかと考えられる。大手キャリア業者や自治体の自営設備であるマイクロ無線やアクセス回線としての FWA が、なぜセキュリティ上、取りざたされないのか？ それは電波法で守られた使用周波数帯の免許と、技術的な仕様等が公開されることのない、メーカーの独自仕様となっているからである。2.4GHz 帯を使用する無線 LAN 製品でも、IEEE802.11b に準拠しない独自方式の製品は、セキュリティに関わる技術的な使用を一切公開していないので、FWA と同等に近い信頼性が得られるのではないだろうか。

2.2 ファーストマイルエリアでの活用

2.2.1 離島や山間部での無線 LAN

姫島での調査のように、僻地とまでいなくてもネットワークをつなげるのに難しいところはたくさん存在する。とても民間による設備投資では追いつかないのが現状であり、インフラを維持していく保守費用だけでもかなりのコスト負担を強いられる。特に離島に

においては、海底ケーブルを敷設する以外、無線もしくは衛星での接続となってしまう。予算が潤沢にあれば問題ないが、限られた中では無線 LAN の活用がもっとも現実的な方法だと言える。

また山間部においても集落同士を結んでいくためには、光ケーブルの総延長距離がかなり伸びてしまう。その割に対象世帯や人口は少なくなっていく。ここでも無線 LAN の活用は有効な手段だと言える。

地方における自治体では、自営ネットワークとして早期に無線 LAN を導入したところもあり、事例をあげればきりが無い。

2.2.2 面的展開の無線 LAN

市町村が全世帯向けに構築するネットワークとしては、CATV がもっともポピュラーである。HFC と呼ばれるもので、幹線に光ケーブルを敷設し各家庭には同軸ケーブルで接続する。これが仮にケーブルテレビ放送を考慮せず、IP ネットワークだけでよければ、無線 LAN による構築は、もっと経済的となるような地理上適した自治体もある。各家庭の屋根にテレビアンテナがあるように、無線 LAN のアンテナがあっても不思議ではない。また無線アンテナの種類によってはもっと小型なので、屋内の窓枠に取り付けるか、もしくは机の上に置くことも可能だ。

無線を面的に展開していく上で、もっとも気をつけなければならないのが、チャンネルを考えたセル設計である。電波空間を効率よく利用しないと、電波干渉によって品質の悪いネットワークとなってしまう。そういった問題を回避する手段として、一般的な DS 方式ではなく、FH 方式の無線 LAN を使用することも考えられる。

FH 方式とは、周波数ホッピング方式のことで、Bluetooth と同様に、ある一定間隔ごとに次から次へとチャンネルを変えていくものである。最大の利点として、干渉に強いことである。DS 方式であればチャンネル固定のため、同一周波数帯に干渉が起きた場合、その

障害がなくなる限り通信は切断されたままとなる。図 3 - 1 に DS 方式との比較を示す。この方式の弱点として、伝送速度が 1.6Mbps と低速だったものの、現在では最大 10Mbps となった。また利用周波数が特定しにくいいため、セキュリティ面でも有効なシステムである。

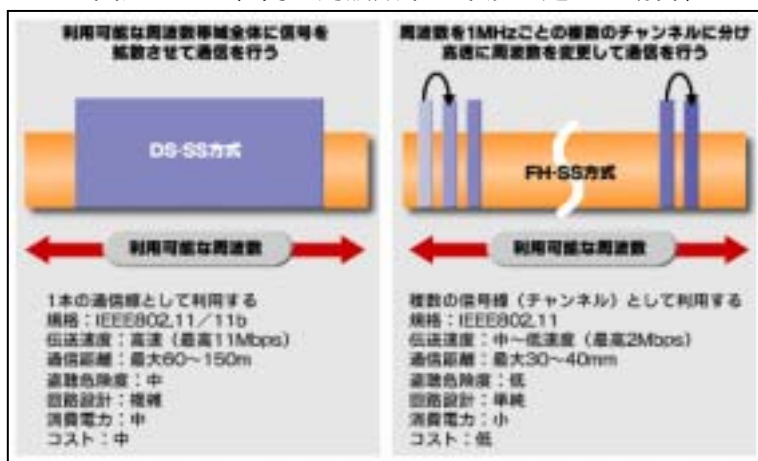


図 2 - 1 FH と DS の比較

2.2.3 無線ホットスポット

最近もっともニュース記事で出てくるのが、無線ホットスポットである。これはもともと米国にて始まったサービスであり、空港や駅などの公共的なそれもよく立ち寄る場所において、インターネットに接続できるというサービスである。それが公共的なエリア以外にもホテルやカフェなど、利用可能な場所が増えつつある。米国では、商用サービスとして早くから立ち上がっているものの、数百ものエリアを持っていたリーディングカンパニーの突然の倒産、事業者間のローミングがなくて使える場所が限られているなど、まだ過渡期にあるサービスだと思われる。しかし、ユーザーサイドの利便性を高めるために、iPassのようなローミングサービスや ISP 間の連携、さらにはホットスポットを統合したサービスの開発など、いつでもどこでも利用できるインターネット時代には、不可欠のサービスとなりつつある。

日本においては、商用第 1 号としてモバイルインターネットサービスが、「Genuine」というサービス名で今年 4 月から東京において開始した。他にもキャリア系がメーカーなどとタイアップしながら実験サービスを行っている。将来的には携帯電話との競合も予想されるため、NTT ドコモもさっそく実験を開始した。NTT ドコモの場合、FOMA とのハイブリッドを予定している。自治体においても、役所のロビーや公共施設のロビーなどで、ホットスポットサービスを開始したところもある。

今後ホットスポットは、IEEE802.11a と IEEE802.11b の競合も交えながら、いたるところで展開されると思われる。果たしてユーザーサイドに立った利便性のある協調したサービスとして発展するのだろうか？ それともそれぞれのサービス事業者が利益の囲い込みに奔るのか？ 無線 LAN の技術革新とともにこれからも変化の激しい市場となるだろう。ラジオやテレビのように普遍的なものとなるまでには、解決しなければいけない多くの課題、たとえば制度面での整備、突破口となるビジネスモデルの創出、双方向という性質上のセキュリティ確保など、が残されている。