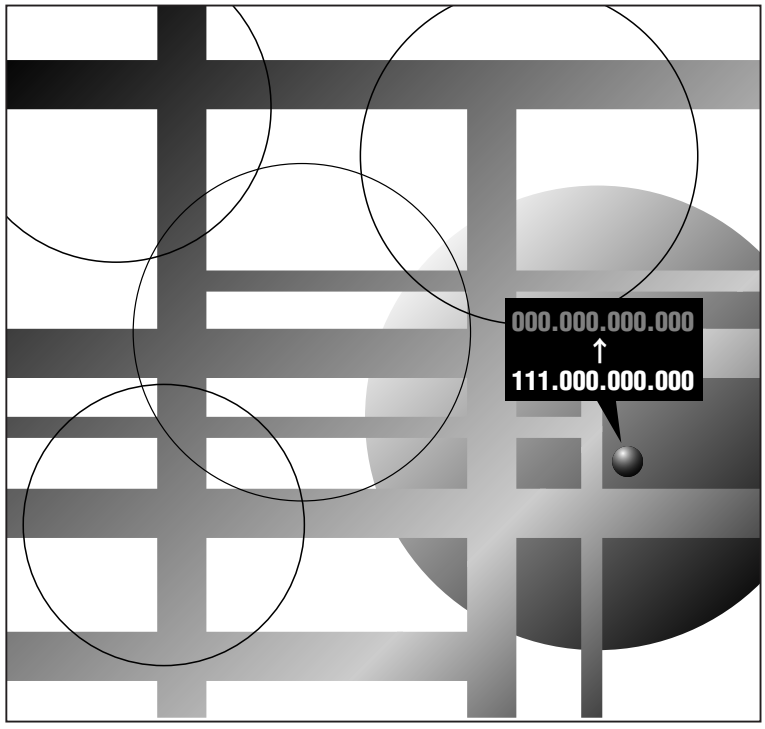
インターネット最新テクノロジー：第47回

携帯インターネット接続環境を提供する

モバイルIP（Mobile IP）

2001年8月から東京都世田谷区の三軒茶屋駅周辺エリアにおいて、モバイルインターネットサービス（以下、MIS Jump）による「モバイルIP」技術を使った無線インターネット接続の実証実験が始まった。この技術を使えばIPアドレスが変化しても途切れずに通信し続けられるため、今後の携帯インターネット接続サービスでの利用が期待されている。 Jump www.miserv.net

太田昌孝　東京工業大学



無線LANを使った携帯インターネット環境を構築

最近筆者は研究成果の実用化のため、MISという会社の設立にかかわった。MISによるサービスの目標は、無線LANにモバイルIPという技術を組み合わせることにより、いつでもどこでも、そして移動しながらでもインターネットに接続された「携帯インターネット環境」を社会の情報通信インフラとして提供することだ。

低速、高額、従量制の電話網と高速、低額、定額制のインターネット

携帯インターネット環境というと、携帯電話やPHSからウェブや電子メールを利用するサービスと混同されがちだが、これらのサービスはあくまで携帯電話網やPHS電話網という電話のための情報通信インフラを経由し、インターネットへ接続するものである（図1）。固定接続環境でのアナログモデムやISDNを経由してのインターネット接続と同じ原理だ。

しかし、電話網は音声伝送のために設計された網であり、これを網としての素性が大いに異なるインターネットへの接続に利用すると、さまざまな不都合が生じる。電話網はインターネットに比べて速度が遅く、料金が高額で、しかも課金は従量制である。そこで、今後のインターネット時代にはインターネット専用の情報通信インフラを整備する必要がある。たとえば固定のインターネット接続環境で言うと、電話網からのダイアルアップではないADSLやケーブルモデム、あるいは光イーサネットによって高速なブロードバンド環境が実現されている。確かにISDNでは電話交換機部分だけをルーターに置き換えた定額制サービスも不可能ではないが、最初からインターネットのための環境を整備するのと比べると低速で高額となってしまう。これと同じことがPHSなどの携帯環境でも言えるのだ。

遠距離のコンピュータ同士を公衆回線など

を利用して接続するネットワークとしてはこれまでもWAN（Wide Area Network）があった。しかしこの世界は電話網会社の独占が長らく認められてきたため、電話網技術しか育っていない。そこで、今現在は規制のないLANの世界で育ったインターネットに適した技術がWANの世界でも利用される傾向にある。

携帯インターネット環境の実現のためには無線の利用が必須だが、ここで注目されるのが、最近急速に普及してきた無線LAN技術だ。現在もっとも一般的な無線LANの規格はIEEE802.11bだ。この技術は無線局免許が不要な2.4GHzの周波数帯域を利用し、100m程度の距離で11Mbpsの通信を可能にしている。

無線を利用した各種のインターネット接続サービス

無線インターネットとしてもっとも古くからあるのはFWA（Fixed Wireless Access）という技術であり、専用の周波数を利用して固定した相手に専用線程度の接続を提供する。しかしFWAはあくまでWANの技術であり、電話網会社の提供する旧来の専用線の代替物にすぎず、サービスの値段や通信速度も多少は専用線よりましといった程度のものだ。

これに対して無線LANは、FWAに比べて到達距離は短いがはるかに安価であり、要所要所に無線基地局を配置すれば、一般家庭でも利用可能な無線インターネット環境を構築できる。しかし、それだけでは無線基地局内での利用しかできないし、これだけならば、ADSLでも同程度のサービスが提供できて無線の価値を十二分に発揮しているとは言いがたい。

そこで、もう少し進んだ無線の利用がファーストフードチェーンの店舗や空港などの多くの人が集まる場所に無線LANの基地局を何台か設置する「ホットスポット」サービスである（図2）。無線LAN端末機能を持つノートパソコンやPDAを持った人間がホットス

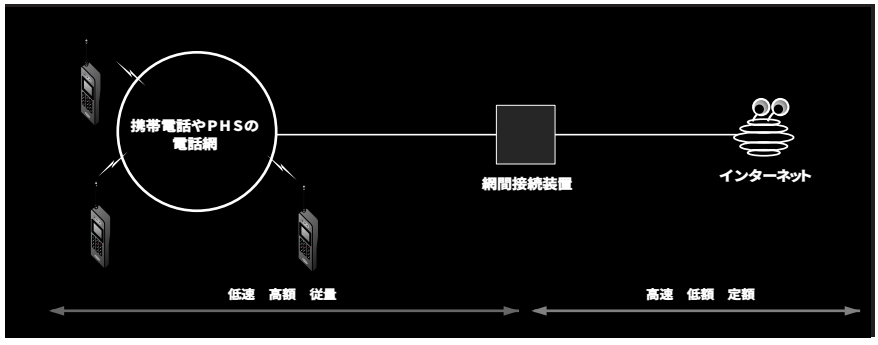


図1　携帯電話やPHSによるインターネット接続

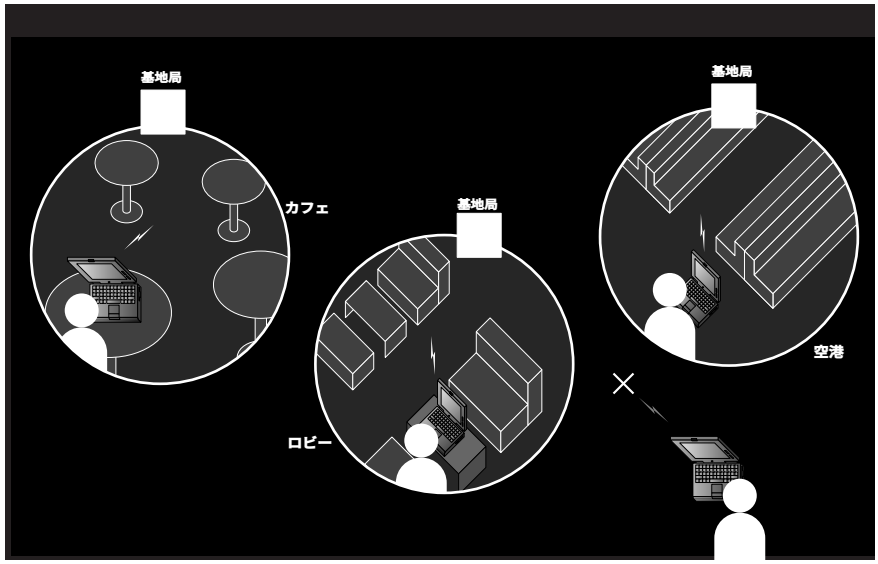
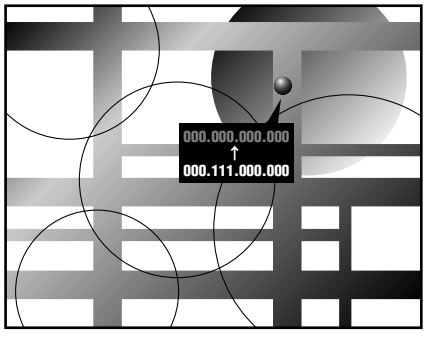
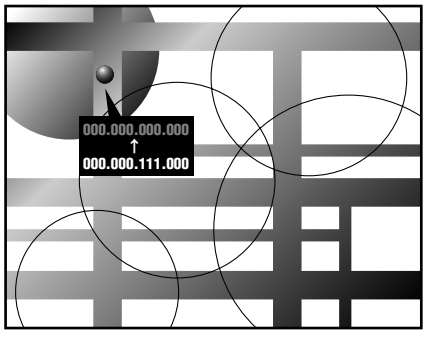


図2　ホットスポットによるサービス

LAN（ラン／Local Area Network）：コンピュータ同士を直接接続した小さなネットワークのこと。「社内LAN」などと表現する。電話回線や専用線などで接続するネットワークはWAN（ワン／Wide Area Network）という。





ポットに行くと、基地局周辺でインターネットを利用できるわけだ。

しかし、これも移動という観点からは中途半端なサービスである。ホットスポット周辺という限定された場所でノートパソコンを使うとなれば、イスや電源もあったほうが便利だということになり、そしてそこまでインフラを提供するなら、さらに有線でイーサネットの口を設けてしまえばよいということになる。またPDAを使うとなると、そのデバイス自身が持つ携帯性に比べて、アクセスできる範囲としての携帯性が基地局に依存するためにかなり小さくなってしまい、十分な活用がなされているとは言い難くなってしまう。

せっかく無線を使うなら無線基地局をホットスポットに限定することなく密に配置して、端末は基地局間を渡り歩いていつでもどこでもインターネットが利用できる環境を構築することが重要になる。

2つのIPアドレスを使い分けることで実現するIPの機動性

インターネットで通信する機器はすべてIPアドレスを持つ必要がある。このIPアドレスは電話番号のようなものでパケットの行き先を決定するものだ。ルーターはこのIPアドレスで経路表を引くのだが、このときに電話番号での市外局番や国番号を利用するのと同じように、ある地域の端末には上位ビットの同じIPアドレスがふられる。このようにすれば経路表は地域ごとに持てばよく、インターネット全体でもそれほど大きくならない。

このIPアドレスは自分が接続したプロバイダー（ISP）の持つ範囲から動的もしくは静的に割り当ててもらうが、これは携帯インターネット端末でも同じで、無線基地局から割り当ててもらうことになる。

しかしここで、携帯インターネット端末ならではの問題が発生する。それは、ホットスポットのような狭い範囲でならそれぞれの基地局の属するアドレスの範囲を共通にできるが、広域の携帯環境では基地局間の移動に伴ってIPアドレスは変化せざるをえないということだ。たとえるならば、基地局が変わるごとに電話番号が変わる携帯電話といった状況になってしまう。インターネットのアプリケーションは通信中に相手のIPアドレスが変化すると通信が途絶してしまうのだ。断続的に移動して移動中は端末を使わないのなら、それでもあまり困らないが、インターネット電話を受信する場合など、移動しながら継続的にインターネットを使うためには、固定したアドレスが必要になる。

そこで登場するのが、モバイルIPという技術だ。モバイルIPでは、携帯端末は固定したホームアドレスと、移動することで絶えず変化する出先アドレスの、2種類のIPアドレスを持たせ、この2つをつなげて各携帯端末の面倒をみるホームエージェントというものを置く。

それでは図3を軸にして解説しよう。携帯端末は、無線基地局から割り当てられた出先アドレス(1)を、絶えずホームエージェントに登録する(2)。通信相手がホームアドレスにパケットを投げると(3)、ホームエージェントが仮に受け取り、出先アドレス向きのIPパケットのなかに収めて携帯端末に転送する(4)。

逆に携帯端末から通信相手へパケットを送出するときは、ホームアドレスを送信者アドレスとして行う。ただ、一部のISPでは偽の送信者アドレスを名乗って自分の正体をふせたまま他者に多数のパケットを送ることで相手の機能を麻痺させるDoS攻撃を防ぐために、パケットのソースアドレスをチェックして、そのISPに属するIPアドレスを送信者アドレスとしないようなパケットはフィルタリングして通さないことがある。このようなフィルターは踏み台を利用した分散DoS攻撃に対しては無力で実効性がなく、またソースアドレスのチェックをしているとサーバーの性能が落ちるため、あまり推奨できる方法ではないのだが、あくまでフィルターにこだわるISPもある。このようなときには携帯端末からのパ

▼

DoS攻撃（ディー・オー・エス攻撃）：DoSとは「Denial of Service」の略で、悪意を持つ何者かが第三者のコンピュータを利用して、標的にしたコンピュータに対して大量のパケットデータを一斉に送るもの。処理能力を上回る量のデータを受信したサーバーは、通常のサービスを行うことができなくなる。

ケットもホームエージェント経由にすることで、フィルターを通過させられる。

無線での接続環境の提供に求められる高度なセキュリティー

実は、モバイルIPは10年ほど前から存在した技術だが、これまで商用サービスは行われてこなかった。その理由は、無線環境でのセキュリティーの欠如にある。

有線環境と異なり、無線環境では誰もが他人宛てのパケットを受信し、また他人になりすましてパケットを送信できる。そこで、商用サービスのためには、お金を支払っていない不正な利用者からのパケットを受け取らないという認証システムが必須である。また、パケットの中身を他人に見られないための暗号化も必要だ。これらは現在の暗号技術を使えば難しいことではないが、そのためには無線基地局と携帯端末がセッション鍵という秘密情報（パスワードのようなもの）を共有する必要がある。しかし携帯環境では、どの携帯端末がどの無線基地局を利用するかはあらかじめわからないし、端末も基地局も増えていくものであり、すべての携帯端末と無線基地局があらかじめセッション鍵を共有するのは無理だ。

そこで、MISでは、独自の技術を開発してセキュリティーを確保している（図4）。個々の利用者にIDとパスワードを与え、認証サーバーのデータベースにも入れておく。携帯端末は必要に応じてセッション鍵を生成し、パスワードで暗号化してIDとともに無線基地局に送る（1）。無線基地局は認証サーバーにセッション鍵を解読してもらい（2と3）、セッション鍵に基づいたパケット単位の認証と暗号化が可能となる（4）。これだと、パスワードを知らない不正な利用者がでたらめなデータを送っても、無線基地局とセッション鍵を共有できない。またIDとパスワードによる携帯端末の利用者の特定は、インターネットを利用した犯罪者を追及するためにも有用だ。

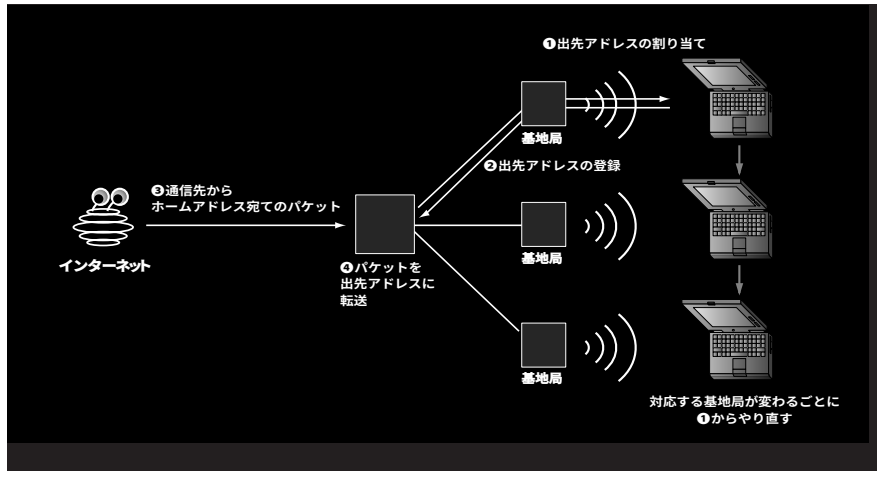


図3　モバイルIPにおけるパケットの転送

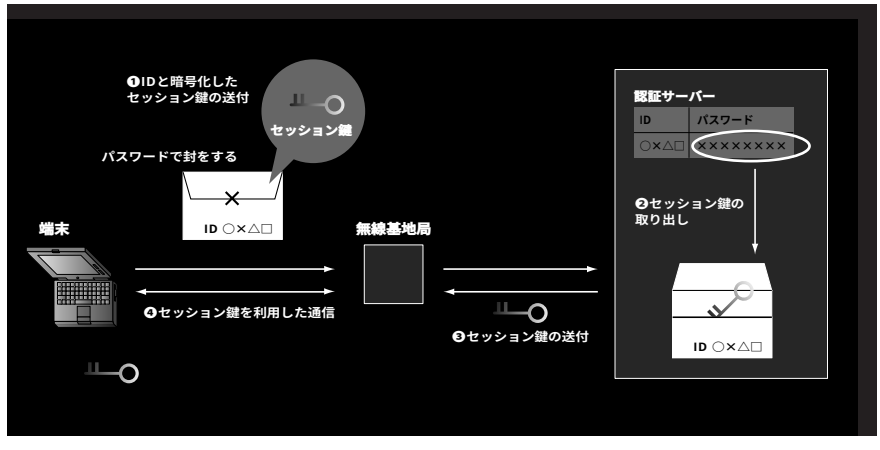


図4　セキュリティーの確保（セッション鍵を共有する）

パケット：通信における送受信の単位で、データ自体のほかにヘッダーやトレイラーと呼ばれる制御情報からなる。データの送信元や送信先などもこの制御情報に入れられる。大きなデータも小さなパケット単位で送受信することで、複数の通信が1つの回線を共有できる。

［インターネットマガジン　バックナンバーアーカイブ］ ご利用上の注意

このPDFファイルは、株式会社インプレスR&D（株式会社インプレスから分割）が1994年～2006年まで発行した月刊誌『インターネットマガジン』の誌面をPDF化し、「インターネットマガジン　バックナンバーアーカイブ」として以下のウェブサイト「All-in-One INTERNET magazine 2.0」で公開しているものです。

http://i.impressRD.jp/bn

このファイルをご利用いただくにあたり、下記の注意事項を必ずお読みください。

- 記載されている内容（技術解説、URL、団体・企業名、商品名、価格、プレゼント募集、アンケートなど）は発行当時のものです。
- 収録されている内容は著作権法上の保護を受けています。著作権はそれぞれの記事の著作者（執筆者、写真の撮影者、イラストの作成者、編集部など）が保持しています。
- 著作者から許諾が得られなかった著作物は収録されていない場合があります。
- このファイルやその内容を改変したり、商用を目的として再利用することはできません。あくまで個人や企業の非商用利用での閲覧、複製、送信に限られます。
- 収録されている内容を何らかの媒体に引用としてご利用する際は、出典として媒体名および月号、該当ページ番号、発行元（株式会社インプレスR&D）、コピーライトなどの情報をご明記ください。
- オリジナルの雑誌の発行時点では、株式会社インプレス R&D（当時は株式会社インプレス）と著作権者は内容が正確なものであるように最大限に努めましたが、すべての情報が完全に正確であることは保証できません。このファイルの内容に起因する直接的および間接的な損害に対して、一切の責任を負いません。お客様個人の責任においてご利用ください。

このファイルに関するお問い合わせ先
株式会社インプレスR&D
All-in-One INTERNET magazine 編集部
im-info@impress.co.jp