モバイルインターネット
（プロトコル概要と動向）

井上 淳（(株）東芝）

村田 嘉利（NTT 東海移動通信網（株））

1999 年 12 月 14 日

Internet Week 99 パシフィコ横浜

（社）日本ネットワークインフォメーションセンター編

目次

1 概要

ITEF の Mobile IP Working Group で Mobile IP プロトコルの標準化が検討されています。すでに RFC 化されている RFC2002 から RFC2004 の標準の内容を説明します。また、Mobile IP Working Group で何が最近話題になっているか、とくに次世代の移動通信 IMT-2000 に向けて Mobile IP の世界がどういった活動をしているか、さらにはプロトコルの拡張の方向、また、実装、製品、関連のリファレンスについて解説します。

2 IETF Mobile IP Working Group について

2.1 Mobile IP とはなにか

Mobile IP は、もともとは 1994 年頃から IETF Mobile IP Working Group で議論が開始されました。IETF Mobile IP Working Group で規定されている Mobile IP は、Internet 上でホスト移動性(Mobility)を透過的にサポートするプロトコルのことです。

当初の目標はサブネット間の Roaming をサポートすることでした。

一般に Internet において IP アドレスというのは、ホスト識別子であると同時に位置の識別子でもあります。IP アドレスによって、ホストが現在接続されているネットワークにパケットが配送されます。この Mobile IP を使用することで、移動しても同一の IP アドレス(ネットワーク識別子=Mobile IP 用語では Home Address と呼ぶ)を使用して移動するホストを識別できます。

もう 1 つの効用として、移動してもセッションを維持しながら通信を継続できる Mobility があります。

ノートパソコンの電源を一度切って、移動してから再び電源を入れて使用するような移動性は可搬性(Nomadicity)と呼ばれており、ここでいう Mobility とは異なります。

Mobile IP Working Group では、これに付随して、Mobile ノードの認証、経路をどのように最適化するか、異なる管理ドメイン間を移動する際のセキュリティ、最近登場してきた話題としては課金管理およびそれにまつわるいろいろなトピックを扱っています。

2.2 主な Mobile IP 関連 RFC

Mobile IP Working Group で規定されている Mobile IP 関連 RFC の一覧を示すと、1999 年 10 月現在、RFC1853、RFC2002、RFC2003、RFC2004、RFC2005、RFC2006、RFC2290、RFC2344、RFC2356 の計 9 種あり、その後も増えていません。

- IP in IP Tunneling (RFC1853)
- IP Mobility Support (RFC2002)
- IP Encapsulation within IP (RFC2003)
- Minimal Encapsulation within IP (RFC2004)
- Applicability Statement for IP Mobility Support(RFC2005)
- The Definitions of Managed Objects for IP Mobility Support using SMIv2 (RFC2006)
- Mobile IPv4 configuration option for PPP IPCP(RFC2290)
- Reverse Tunneling for Mobile IP (RFC 2344)
- Sun's SKIP Firewall Traversal for Mobile IP (RFC 2356)

図 1：Mobile IP 関連 RFC

とりあえず Mobile IP をやろうとすると、図 1 で示した RFC2002、RFC2003、RFC2004 を見る必要があります。

RFC2002 は、いわゆるベースプロトコルと言われるものです。どこの場所にいるかを認識したり、経路制御をどういう形で行うかなど、枠組みのところを記述した RFC です。

RFC2003 および RFC2004 は、経路制御にともなって一旦 Home Address に向かって送信されたパケットを、現在位置にカプセル化して配送する際のカプセル化に関する細かい規定です。したがって短い内容になっています。

その他の RFC は、それぞれの興味で見て下さい。

詳細は IETF のホームページを参照して下さい。

http://www.ietf.org/html.charters/mobileip-charter.html

2.3 Mobile IP 関連 Draft について

Mobile IP 関連の Draft は、発表されては消えるものもあり、玉石混淆でいろいろあります。図 2 の一覧には、1999 年 10 月現在の Draft を掲載しています。

- **Route Optimization in Mobile IP**
- **Mobility Support in IPv6**
- **Mobile IP Regionalized Tunnel Management**
- **Mobile IP Challenge/Response Extensions**
- **Mobile IP Network Access Identifier Extension**
- **Requirements on Mobile IP from a Cellular Perspective**
- **IP micro-mobility support using HAWAII**
- **Paging support for IP mobility using HAWAII**
- **Mobile IP Vendor/Organization-Specific Extensions**
- **IP Mobility Support for IPv4, revised**
- **Mobile IP Authentication, Authorization, and Accounting Requirements**

（その他もろもろ）

- **DIAMETER Mobile IP Extension**

図 2：Mobile IP 関連 Draft（99 年 10 月現在）

ここで触れるのは、Route Optimization in Mobile IP、Mobility Support in IPv6、DIAMETER Mobile IP Extension です。

一覧の最後尾に掲載した DIAMETER Mobile IP Extension は、Mobile IP の Working Group だけではなく、認証･課金系の AAA(トリプル A)Working Group の中のサブ Working Group の Draft を挙げたもので、同サブ Working Group では、Mobile IP 関連の認証･課金を扱っています。

DIAMETER は、最近、米国の次世代の携帯の規定に採用される可能性が出てきたことで注目されています。

2.4 Mobile IP ドキュメントをどう読むか

RFC に関しては、RFC2002、RFC2003 は必須です。RFC2004 は多くの人にとって必須です。RFC2005 は相互接続の基準を記述しています。また、RFC2006 は MIB 拡張のみを記述しています。

一方、Draft に関しては、息の長いものは目を通しておくことが必要です。特に現在は、Mobile IPv6 および DIAMETER 関連はフォローすべきで、あとは各人の興味に従って読めばよいです。MobileIPv4 プロトコルに関しては、最近は適用事例ばかりで、新しいパラダイムは見られ

ません。トピックはむしろ、関連 Working Group に話題が移っている観があります。たとえば IPNG、IPsec、PPPEXT、SVRLOC、AAA あたりで、特に IPNG、AAA などはフォローしておくほうがよいです。

また、メーリングリストはノーテルネットワークスのインターネットサービスで提供している mobile-ip@standards.notelnetworks.com に登録すると、活発な議論をウォッチできます。

3 Mobile IP プロトコルの概観

RFC2002 プロトコルに沿って詳しく述べます。

まず、構成要素と動作を図 3 に示しました。

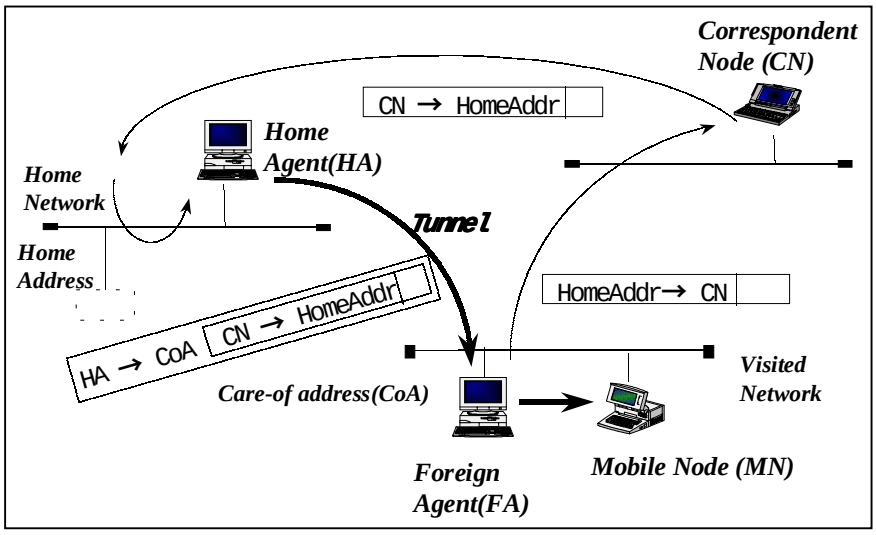

図 3：Mobile IP プロトコルの概観

ここで考える移動ノードが Mobile Node です。Mobile Node は、もともと接続されていたネットワークが本籍=Home Network で、Home Address を割り当てられていました。

それが訪問先のネットワークに移動した状況を想定しています。

Mobile IP の中のその他の構成要素としては 2 つあり、Home Agent は Home Network 上の 1 つのルータです。また、もう 1 つは Foreign Agent で、移動先のネットワークで、そこに移動してきた Mobile Node の世話をするエージェントです。これもルータの一種です。

一方、Mobile Node が話をする相手を Correspondent Node と呼び、CN と略します。

Correspondent Node は、常に Home Address に対してパケットを送信するイメージになります。それに対して、現在位置を示す仮のアドレスを Care-of address と呼びます。気付けアドレスと日本語で訳していま す。

Foreign Agent がいるモードでは、Foreign Agent の IP アドレスが Care-of address になります。Foreign Agent は、このサブネットワークに移動してきた Mobile Node 宛のパケットを一旦収集して、同じリンクにいる Mobile Node に配送する動作をします。

Mobile Node は、移動したら、現在位置を登録するメッセージを Home Agent に送信します。

仮に、Mobile Node が Care-of address のある Home Network に移動して位置情報を Home Agent に告げたとします。

Home Agent は、Correspondent Node から Home Address 宛に送信したパケットを、あるメカニズムを利用して横取りし、これを、Home Agent から Care-of address 宛すなわち Foreign Agent 宛のパケットにカプセル化して、Foreign Agent に送信します。

Foreign Agent は、カプセル化されたパケットの中を見ると、あたかも Correspondent Node が Home Agent 宛に送信したパケットのように見えるので、これをリンクレイヤーのメカニズムで、この Mobile Node に渡します。

Mobile Node の TCP/IP のスタックは、自分が Home Agent を持っているスタックであると思ってそれを処理します。

逆に Mobile Node が Correspondent Node に対してパケットを送信するときには、Care-of address を気にしないで、自分が Home Network にいる場合と同様に、Home Address をソースアドレスに付けて Correspondent Node に対してパケットを送信します。

このような 3 角形の経路となるのが Mobile IP プロトコル全体の動作です。

問題としては、経路が冗長になることや、パケットのソースアドレスと実際の発信元が異なっているため、セキュリティ的な問題が発生することなどが挙げられています。

3.1 2 つの動作モード

Mobile IP プロトコルの動作モードには、Foreign Agent モードのほかにもう 1 つ Co-located Care-of address モードがあります。

Co-located Care-of address モードは、訪問先のネットワークに Foreign Agent が存在せず、Mobile Node がデカプセリング機能を兼ねるモード

です。

Foreign Agent モードと Co-located Care-of address モードの違いは、Foreign Agent モードでは、Foreign Agent が定期的にビーコン的に流す Agent Advertisement と呼ばれるメッセージ、あるいは Mobile Node が問い合わせる Agent Solicitation で訪問先のネットワークの現在位置がどこかを検出･確認できるメカニズムになっています。

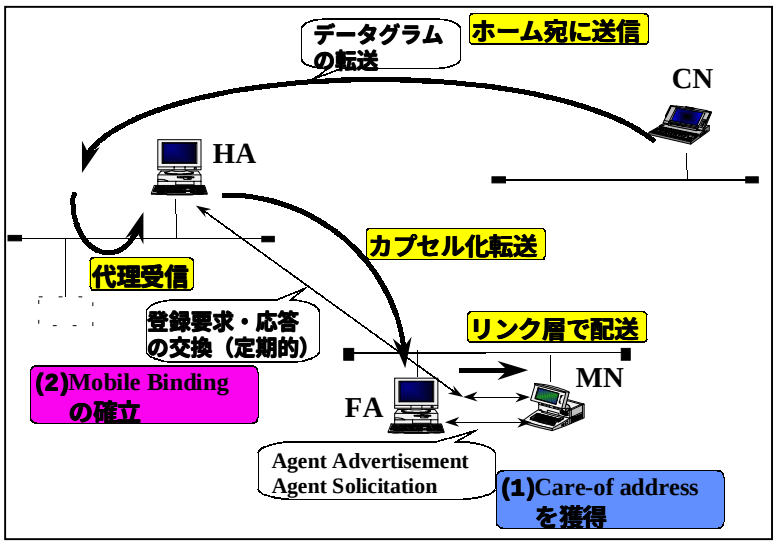

図 4：Foreign Agent モードの動作

これに対して、Co-located Care-of address モードでは、訪問先のネットワークに助けをしてくれるものがいないので現在位置の検出が曖昧になってしまいます。

Co-located Care-of address モードでは、Mobile Node が自分で DHCP などを使って Care-of address を獲得するため、訪問先に Foreign Agent がなくてもネットワークを移動できる利点があります。

半面、Co-located Care-of address モードでは、訪問するネットワークごとに 1 つずつ DHCP で、受けるためだけのアドレスを割り当てなければならないため、アドレス資源の浪費となります。これに比べ、Foreign Agent モードでは、複数の Mobile Node が Foreign Agent の同一アドレスを共用できるため、アドレス資源は浪費されずにすむのが利点です。

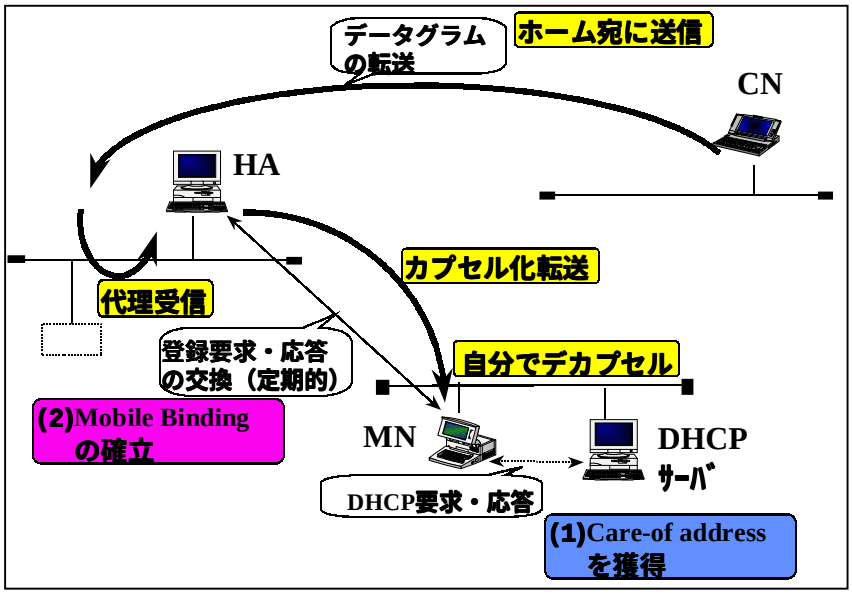

図 5：Co-located Care-of address モードの動作

3.2 RFC2002 の構成

RFC2002 の構成に沿ってもう少しプロトコルの内容の詳細を説明します。

RFC2002 は、第 1 章 Introduction、第 2 章 Agent Discovery、第 3 章 Registration、第 4 章 Routing Considerations、第 5 章 Security Consideration、第 6 章 Acknowledgements で構成されています。

第 1 章の Introduction に続き第 2 章に Agent Discovery が記述されています。

第 2 章には Mobile Node が移動先のネットワークに接続したときに、そのサブネットの何を頼って Mobile IP 動作をするかを知るためのメッセージのやりとりが記述されています。

頼る先が確認できたら、Mobile Node は、自分の Home Agent に現在位置の登録作業をしなければなりません。それを記述したのが第 3 章 Registration です。

登録が完了し、Home Address と Foreign Agent あるいは Co-located Care-of address との関連づけができたところで、はじめて Mobile Node へのデータの転送が行われます。

その際のカプセル化の形式、ブロードキャスト、マルチキャストの扱いなどを示したのが第 4 章です。先ほど述べた、Home Agent のパケット横取り機構である、ARP、Proxy ARP、Gratutious ARP に関しては第 4 章 6 節で説明されています。

したがって、第 4 章は、Mobile IP の 3 角形の経路でデータをどう配送していくかの規約が記述されています。

1. Introduction
2. Agent Discovery →MNの現在位置の検出
   2.1. Agent Advertisement , 2.2. Agent Solicitation
3. Registration →MNの現在位置の安全な登録
   3.1. Registration Overview ,3.2. Authentication, 3.3. Registration Request,
   3.4. Registration Reply, 3.5. Registration Extensions
4. Routing Considerations →MNへのデータ転送
   4.1. Encapsulation Types , 4.2. Unicast Datagram Routing,
   4.3. Broadcast Datagrams , 4.4. Multicast Datagram Routing,
   4.5. Mobile Routers, 4.6. ARP, Proxy ARP, and Gratuitous ARP
5. Security Considerations
6. Acknowledgments

図 6：RFC2002 の構成

3.3 Agent Advertisement/Solicitation

Foreign Agent モードで訪問先のネットワークで Care-of address を獲得するために、Agent Advertisement といって、Foreign Agent が一定時間ごとにサブネット上にブロードキャストするメッセージがあります。

それを待てない Mobile Node は、Agent Solicitation というメッセージを出して、頼れることになる Foreign Agent を探すための呼びかけを行います。いずれも ICMP Router Advertisement の拡張もしくは、Router Solicitation の拡張となっています。

Agent Advertisement のデータ形式は図 7 のようになっています。

Sequence Number、メッセージがあり、たとえば RFC2004 で規定されている Minimal Encapsulation ができるか、GRE Encapsulation ができるかといった、どのようなカプセル化をサポートするかなどに関してのフラッグが付いています。

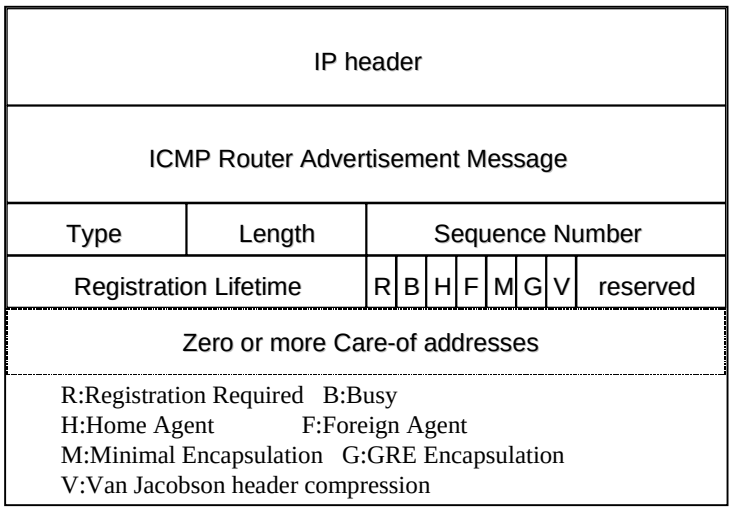

図 7：Agent Advertisement **のパケット形式**

3.4 Registration

Foreign Agent のアドレスがわかったら次に RFC2002 第 3 章の Registration に移ります。

Registration の内容は、Mobile Node から Foreign Agent を経由して Home Agent にパケットを送る際の規定です。基本的には Registration Request もしくは Registration Reply というメッセージを UDP で送ります。

その後には Mobile-Home Authentication Extension を付けることが必須になっています。

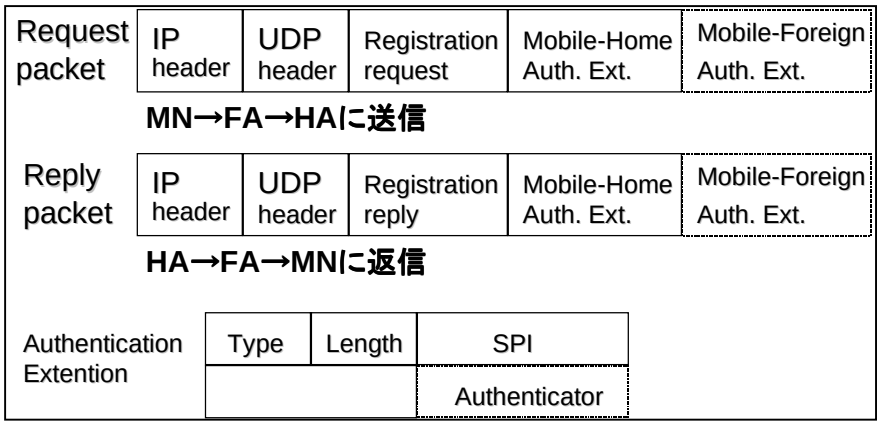

図 8：Registration

この Extension を付ける理由ですが、誰からか明確に認証されていない Mobile Node からメッセージが送られてきた場合に、その Mobile Node にむやみにパケットを送信してしまうのでは、セキュリティ的にも問題が生じます。そこで、この部分では、あらかじめ共有鍵で交換された認証子、keyed MD5 の認証子を付けて、認証された Mobile Node から登録メッセージが来ていることを確認するために認証の Extension を付けています。

この認証 Extension の付加に関しては、Mobile Node と Home Agent 間では必須、一方、Mobile Node と Foreign Agent 間、Foreign Agent と Home Agent 間の認証はオプショナルで付加しても、しなくてもよいことになっています。

認証の Authentication Extension は、TYPE の部分で Mobile Node と Home Agent 間か、Foreign Agent と Home Agent 間か、Mobile Node と Foreign Agent 間かを識別します。

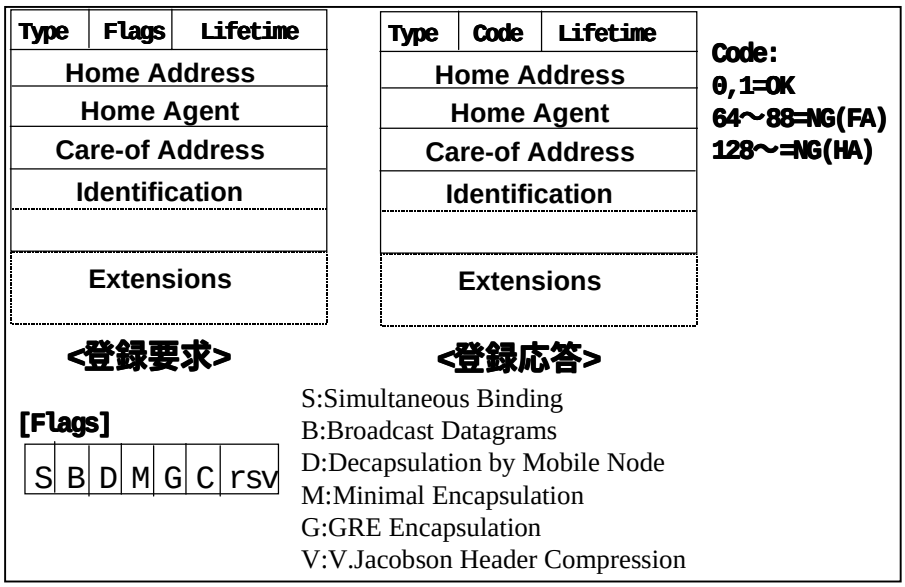

図 9：Registration のパケット形式

Registration のパケット形式を見ると、Registration の Request Packet、Reply Packet のメッセージの形式には、各々、もともといたところの Home Address と、Home Agent、Care-of address、Identification、および Extension が内容に含まれます。

このパケットをやりとりすることによって、Care-of address と Home Address とのバインディングが行われます。

このバインディングにはライフタイムがあり、一定時間経過するごとに、この Request Packet を再送して、ライフタイムを延長してやる必要があります。

また、フラッグも示されており、ベースプロトコルのフラッグですが、

カプセル化の形式、ヘッダコンプレッションするか、Broadcast Datagrams を Home Agent から Foreign Agent に送るか、Simultaneous Binding で一度に複数の Foreign Agent を経由してバインドし、複数の Foreign Agent からパケットが流れてくるのを受けるかといった属性値を、フラッグの部分で規定しています。

Registration のパケット形式の中で、コードの部分があります。コード 0 または 1 は登録成功、またエラーコード 64 から 88 は Foreign Agent の都合で登録失敗、128 以上は Home Agent の都合で登録失敗を表します。

Registration の Extension は、MD5 で正しいホストから登録依頼メッセージが来ているかを、Type の部分で識別します。Type32 が Mobile-Home、Type33 が Mobile- Foreign、Type34 が Foreign- Home を表します。

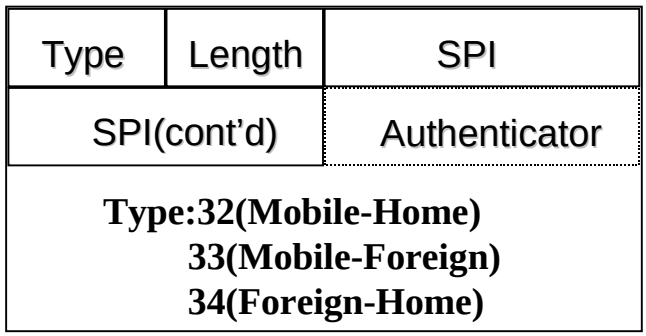

図 10：Registration **の** Extension

これ以外にも最近、いくつかの Extension が提案されています。たとえば、Network Access Identifier (NAI)です。その Mobile Node を使用しているユーザ情報(xxx@yyy のような)を載せて、ユーザごとにアクセス制限を行うものも提案されています。

また、Challenge-response も提案されています。これは、リプレイアタックを防ぐための拡張で、一部実装されて、接続試験も行われています。

これで、Home Agent と Care-of address のバインディング、モビリティバインディングが確立したことになります。

3.5 Proxy ARP/Gratuitous ARP **について**

Correspondent Node が Home Address 宛にパケットを送信してきた際に、Home Agent は登録されている Home Address に宛てたものなら、それを横取りしなくてはなりません。そのときの機構が RFC2002 の第

4 章 6 節に記述されている Proxy ARP、Gratuitous ARP です。

Home Agent が、留守になっている Mobile Node の代理受信を行うことを制御します。

Proxy ARP は、あるノードが、他のノードの代理で ARP に対して応答することです。たとえば Mobile Node が留守中に、Home Agent が Mobile Node 宛てに送られるべきパケットを代理受信するために使用します。

もう 1 つの Gratuitous ARP は、代理受信しているものをリセットする場合や、Mobile Node が離れたときに、Mobile Node 以外の IP ノードがもっている ARP キャッシュのエントリーをクリアするために使用する ARP のメッセージです。

Gratuitous ARP のメッセージを使用することで、Mobile Node が離れるときには、同じサブネット上の他の IP ノードの ARP キャッシュのエントリーを全部クリアします。それと同時に、Home Agent が Proxy ARP を行って、Mobile Node 宛のパケットは、Home Agent が一旦獲得して、それをカプセル化して、Mobile Node の現在位置に送信できるようにします。

Mobile Node が戻った場合には、代理受信状態だったものを、Gratuitous ARP を使用して、代理受信状態を解除して元に戻すことになります。

3.6 カプセル化の方式

最後に Datagram を Mobile Node 宛てに転送することになります。そのためのカプセル化方式は 3 方式があります。その 3 方式は、IP in IP(RFC2003)、Minimal Encapsulation (RFC2004)、GRE Encapsulation (RFC1701)です。実際には、主に RFC2003、たまに RFC2004 が使用されています。

Foreign Agent モードでは、Foreign Agent が、送られてきたカプセル化されたパケットを解いて、その中身の Home Address 宛てパケットをリンク層メカニズムを通して Mobile Node に転送します。Co-located Care-of address モードでは、Mobile Node 自身がカプセル化を解いて、Home Address 宛てパケットを抽出し、TCP/IP スタックに収容します。

3.6.1 IP in IP カプセル化

IP in IP カプセル化では、送られてきたパケットにさらにヘッダ部分として、ソース:Home Agent、デスティネーション: Mobile Node の Care-of address という情報が付加される形式となります。付加のヘッダ部分で 20 バイト増えることになります。

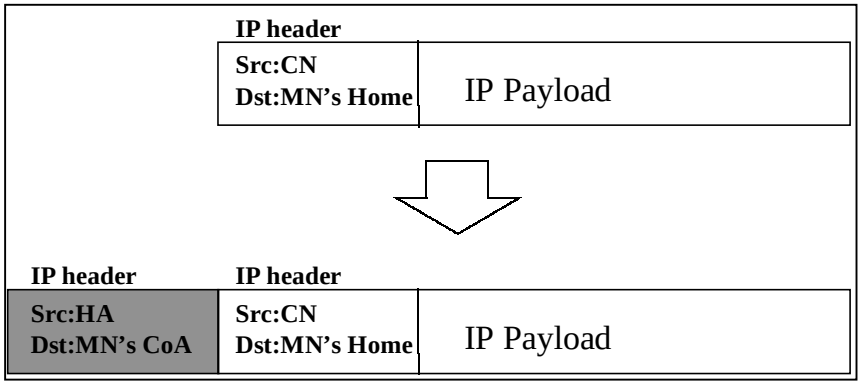

図 11：IP in IP カプセル化

3.6.2 Minimal Encapsulation

Minimal Encapsulation では、新規付加ヘッダ部分は IP in IP と同じです。送られてきたパケットにあったヘッダに替わって、Mobile Node の Home Address 情報が挿入されます。この場合、最短で 12 バイト増加することになります。

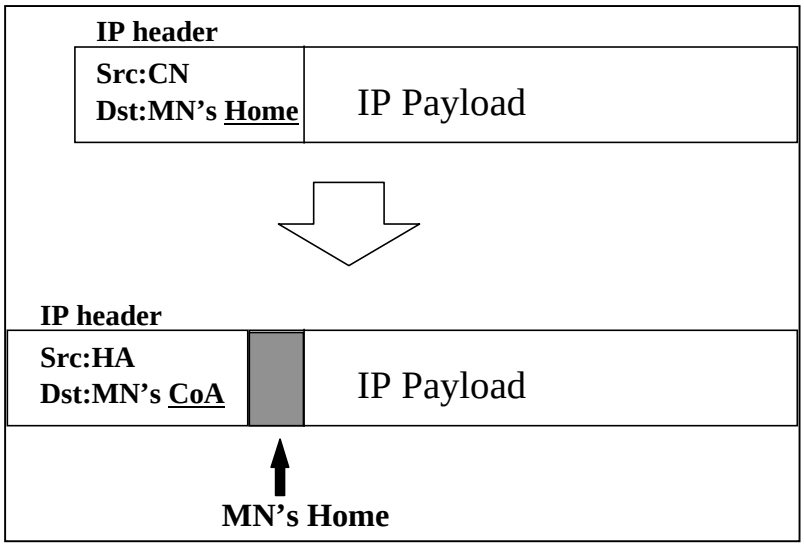

図 12：ミニマルエンカプスレーション

3.7 マクロモビリティをサポート

ところで、Mobile IP は、電波の強度が変わった場合など、基地局を移

動するといった機能、いわゆるマイクロモビリティに関してはサポートしていません。

これは、RFC2002 の第 1 章の Introduction で明確に宣言しています。Mobile IP でサポートするのはマクロモビリティとよばれる移動性で、1 秒間に 1 回程度のサブネット間移動をサポートしています。

4 課題への挑戦

Mobile IP に関する課題への挑戦はこのほかにも、いろいろと行われています。ここでは、経路の冗長性を解消する Route Optimization、End-to-End の完結型の Mobility Support、セキュリティに関する Reverse Tunneling、ファイアウォールの透過のモデル、Mobile IPv6 と Mobile IPv4 の違いなどについて簡単に説明します。

4.1 Route Optimization

Mobile IP では、経路が 3 角形となるため、冗長性が指摘されてきました。この冗長性を解消する Route Optimization が提案されています。現在はまだドラフト段階にあります。

この提案によると、経路を最適化するための新しい概念として、Binding Cache を各々の構成要素に持たせます。これによって、Mobile Node の現在の Care-of address 情報を各々がキャッシュします。Mobile Node が移動したら Binding Cache のアップデートメッセージを UDP で送信して、現在位置情報を更新します。

ところで、事実上の当事者となる Home Agent、Foreign Agent に Binding Cache を持たせることはさほど問題ではありません。しかし、すべての Correspondent Node にも Binding Cache をもたせるとなると、既存環境へのインパクト的にも問題となります。

もともと、Route Optimization は、Mobile IPv4 用に作られていました。

これに対して Mobile IPv6 では、デフォルトで Route Optimization 的な機能を盛り込んでいます。最近では Mobile IPv4 での議論は下火になってきており、この問題に関しては、Mobile IPv6 で一気に打開する空気が支配的になってきました。

4.2 セキュリティの問題

先に述べたように、Mobile Node の現在位置と、送られてくるパケットのソースアドレスとがトポロジー的に一致せず、パケットフィルタやファイアウォールのセキュリティでアクセスを拒否される事態が生じます。そうした問題を解決する方法として、Reverse Tunneling が有効とされ

ています。また、IPsec との協調で IPsec の認証機構を使用してファイアウォールとの折り合いをつけるといった方法も検討されています。

4.2.1 Reverse Tunneling

Mobile Node がインターネット上にあり、Home Agent、Correspondent Node が組織内のあるサーバだとします。その際、ベースプロトコルを使用するとなると、Mobile Node から Correspondent Node へのパケットは直接送られることになります。その際、組織の内外の境界に設置されたファイアウォール、もしくはパケットフィルタから見ると、Mobile Node の現在位置とパケットのソースアドレスとの整合が確認できないため、外部から内側アドレスを騙った攻撃と判断してそのパケットをフィルタリングしてしまいます。

したがって、Mobile Node は、Correspondent Node にアクセスできないことになります。

その対策として、すべてのパケットを一旦 Home Agent に集めてしまうのが Reverse Tunneling です。

つまり、Care-of address 発 Home Agent 宛というパケットの中に、もともとは Home Address 発 Correspondent Node 宛だったパケットもカプセル化して送ってしまいます。

これによって、Mobile Node の物理的な現在位置と付加カプセルのトポロジー的な位置とが見かけ上一致することになり、パケットフィルタを通過できることになります。

経路は、さらに冗長になります。インターネット環境では、現状止むを得ないとの声が多いです。

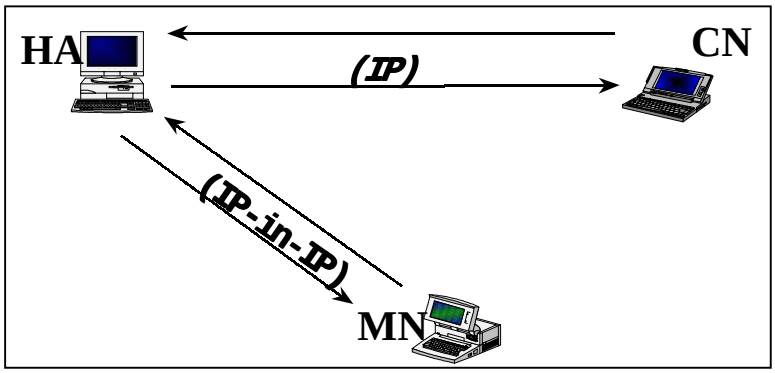

図 13：Reverse Tunneling

4.2.2 IPsec **との協調**

IPsec は、IP レベルのセキュリティメカニズムで、ノード間のセキュリ

ティアソシエーション(SA)、認証ヘッダ(AH)、暗号化ペイロード(ESP)などが規定されています。

もともとは、サン･マイクロシステムズの鍵管理プロトコル SKIP を使った、SKIP Firewall Traversal for Mobile IP がベースになったRFC2356 に記述されています。

サン･マイクロシステムズ自身も、IPsec で認証を行ってファイアウォール透過を行うモデルを規定し、提案しています。

内向き、外向きを規定しており、多重ファイアウォールの場合のモデルも想定しています。

また東芝も早くからサン･マイクロシステムズと共同研究してきており、この共同研究の応用成果として、ISS'97 で、End-to-End のセキュリティアソシエーションで内容の保証、たとえば暗号化をしてやって、Link-by-Link、たとえばファイアウォール 1、ファイアウォール 2、ファイアウォール 3 と通過していく時には、Link-by-Link のセキュリティで透過の際のホストの認証をしていく方式を提案しています。

サン･マイクロシステムズの方式も東芝の方式もよく似通っています。ESP セキュリティで中身を保護して、Mobile Node とファイアウォールごとの間で認証を繰り返し、認証が正しければ透過させてCorrespondent Node に辿り着く仕組みとなっています。

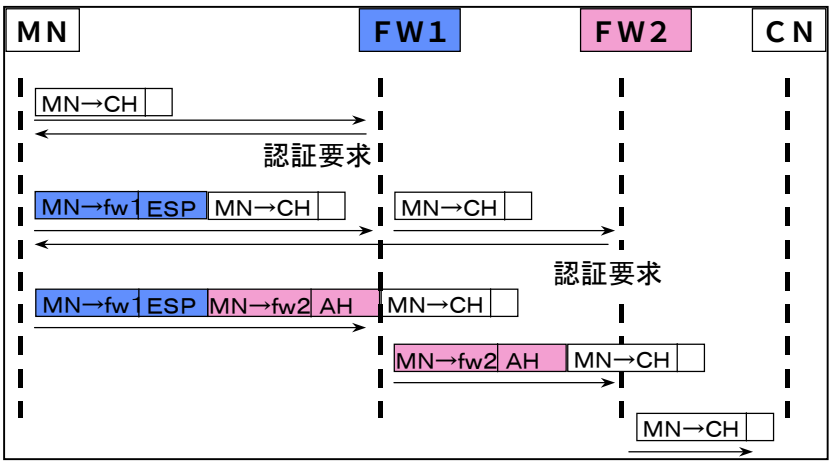

図 14：IPsec によるファイアウォール透過

4.3 Mobile IPv6 について

そろそろ最終案と言われながら、なかなか最終案が固まらないのがMobile IPv6 です。

Mobile IPv4 との違いは、Foreign Agent モードがなくなることで、

Mobile IPv6 では Co-located Care-of address モードだけとなります。

Care-of address は、何らかのアドレス自動構成で獲得することになります。また、経路制御は、Mobile IPv6 のデスティネーションオプションと呼ばれるもので行います。

Care-of address 経由で Home Address 宛てに転送するという経路制御をルーティングヘッダで行います。このため、場合によっては、Mobile Node までの配送経路の冗長さを回避できます。

移動ノードが移動した場合、Binding Cache で Binding のアップデートも行って、経路最適化を行います。

現状、最終案にならないのは、実装が少ないことも大きな理由です。

海外では、米国のカーネギーメロン大学のデーブ･ジョンソン氏のグループの Monarch プロジェクトが、熱心に実装･接続試験を行っています。

わが国でのプロジェクトでは KAME があり、これにも Mobile IPv6 が採用されると言われており、それに期待しています。また、Mobile IPv6 の通信経路は当初は、Mobile IPv4 と同様の 3 角形経路となります。現在位置情報を Binding して、Binding Cache を更新し、Home Address と Care-of address を Binding したあとからは、Care-of address に直接パケットを送信することになります。

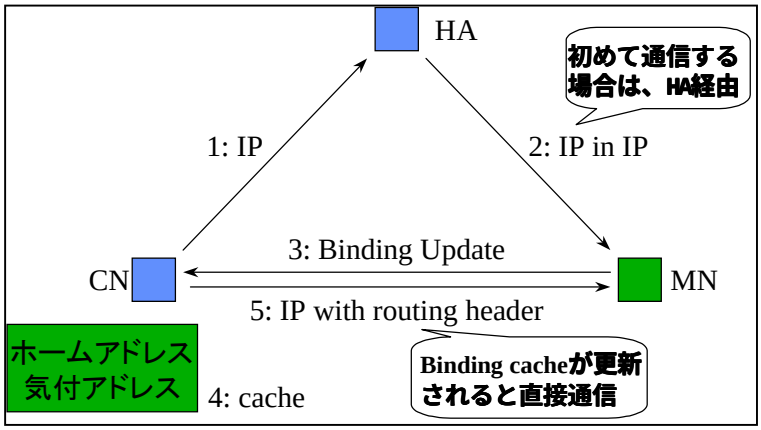

図 15：Mobile IPv6 の通信経路

4.4 最近の話題

Mobile IP Working Group では、ホストの移動性をサポートしようということで議論して、プロトコルを確立してきました。最近は、IETF の Web サイトを見ても、内容が変化してきています。

しかし、最近では実際に ISP に、こういった Mobile IP の枠組みを使わせようということで、たとえば IMT-2000 次世代セルラに適用していこ

うという狙いでコロンビア大学の研究グループがセルラ IP を提案しています。

また、スウェーデンのエリクソンが IMT-2000 のための Mobile IP への要求事項を提案しています。

一方、ISP への採用拡大への環境づくりとしては、AAA サーバと連携して、認証に対するスケール性を改善しようという試みや、モバイルサービスで料金を徴収したいと考える ISP の要望に歩調を合わせ、課金の枠組みと連携しようという動きがあります。

AAA サーバとの連携に関しては、IETF のチャーターにも明確に謳われており、最近のチャーターの半分ぐらいが認証系・課金系で占められるようになっています。

さらに、IETF だけでは十分ではないとして、3GPP2 という米国の第 3 世代の携帯情報通信システムの技術・業界団体との交流、接続試験なども行われています。

4.4.1 AAA Working Group

IETF の Working Group として AAA Working Group 関連の話題が最近中心になっています。AAA Working Group は、1997 年の IETF 会議からできた Working Group で、認証・課金・オーソライゼーション系の Working Group です。5 つの Sub Working Group が組織されています。Sub Working Group には

①Authentication
②Authorization
③Accounting
④Mobile IP
⑤E-Commerce

があります。

Mobile IP Sub Working Group が設けられたのは、米国版の次世代携帯情報システム IMT-2000 by ANSI(TIA:Telecommunication Industry Association aka 3GPP2)で AAA サーバを使用した課金・認証を検討しているという背景があります。

IMT-2000 には、RADIUS、その次世代版に相当する DIAMETER という認証プロトコルを使用することを検討しています。

ANSI Mobile IP model for IMT-2000 のネットワークシステムイメージは、Home Network と Foreign Network と呼ぶ 2 つの別々に管理される管理ドメインがあって、Home-Foreign 間での移動を明確に認証された形で枠組みを作ろうというものです。

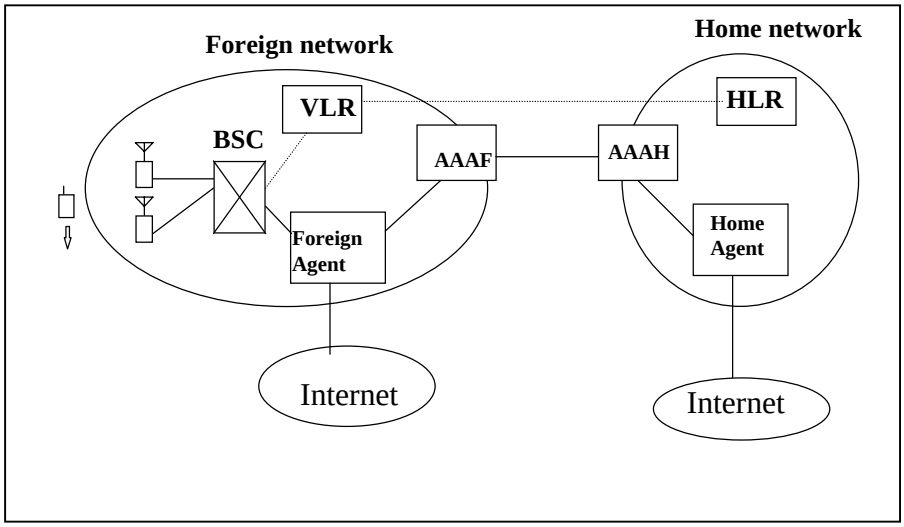

図 16：ANSI Mobile IP model for IMT-2000

構成要素には、Foreign Agent、Home Agent のほかに、AAA サーバ(AAA-H、AAA-F)があり、ドメインごとに、認証･課金を AAA サーバで管理しています。

この認証プロトコルの初版には、DIAMETER が当初間に合わず、RADIUS を使用しました。第 2 版では DIAMETER の Mobile IP の Extension を使用することになりそうです。

DIAMETER に関しては、サン･マイクロシステムズのサンラボラトリーのパット･カルホーン氏が薦しています。

4.4.2 DIAMETER

Mobile IP ではエージェント間で Keyed MD5 で認証する方法がありますす。しかし、鍵の配布のスケーラビリティに問題があります。また、課金が欠けているので ISP には魅力に乏しいです。

そこで DIAMETER では、大規模な ISP でもスケールする SA のカギ配布機構を実現している AAA サーバがこの機能を集中して管理します。課金情報も Accounting Extension で規定します。Mobile Node を IP アドレスだけでなく、NAI(Network Access Identifier)で識別できるようになります。

このほか、Cross-domain authentication と Authentication が可能になります。また、移動ノードへの Home Address の動的割り当て、Home Agent の動的割り当ても可能になります。

DIAMETER では AAA サーバなど各要素間のプロトコルをそれぞれ規

定しています。このそれぞれのプロトコル交換で認証を行うことで、AAA サーバが認証キーを配布します。それによって、管理された形での交信ができるようになります。

4.4.3 Mobile IP の効用

米国、欧州では、無線業者の相互乗り入れを考えています。このため、互いがローミングするケースが多く、認証の枠組みが、Mobile IP の問題点の現状を打開するものになります。

4.4.4 End-to-End の新規 Mobility プロトコル

東芝が DiCoMo99 で論文発表した End-to-End で完結した IP 層による移動透過性保証の一方式を紹介します。

特徴としては、既存ノードとの通信も可能にしていることです。基本的には、IPsec のトンネルモードを使用し、トンネルエンドポイントを動的に変更するプロトコルとなっています。

Mobile Node との通信には、IPsec Tunnel モードを使用します。その際にノード間は End-to-End 通信になります。アプリケーションには不変の Haddr、IPsec Endpoint には移動先アドレス Care-of address を使います。

Mobile Node の移動によるセッション喪失を回避するため、Tunnel Endpoint を動的に変更するプロトコルとして SA Gateway Update と SA Local Update をサポートします。

Mobile Node は移動すると Dynamic DNS Update で自分のアドレスレコードを Care-of address に変更します。

また、SA Local Update では、dest フィールドが以前の Care-of address を現在の Care-of address にし、自分の SA を変更します。

さらに、SA Gateway Update で、dest フィールドが自分でない通信相手に対し、通信相手の以前の Care-of address を新規 Care-of address に変更する旨、要求します。

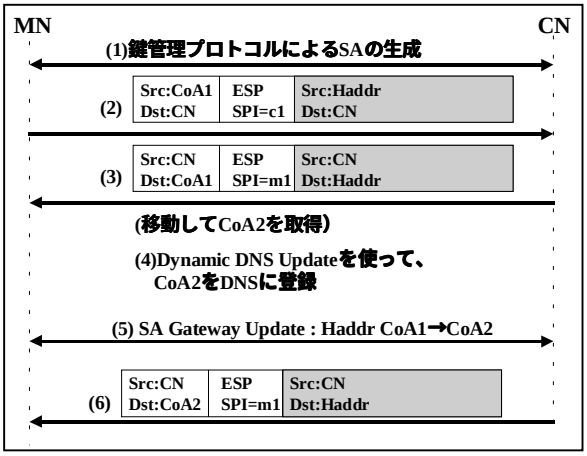

図 17：新規 Mobility プロトコルの通信方法

また、新たに DNS に Haddr を示す Resource Record を定義しました。これによって、移動ノード宛の発呼をサポートしました。

Mobile Node への発呼は、①DNS を使って、Mobile Node の AAAA(CoA1)と HAAAA(Haddr)を取得、②AAAA を使って SA を生成するよう鍵管理プロトコルに通知し、アプリケーションには HAAAA を通知、これによって鍵管理プロトコルが生成されることになります。

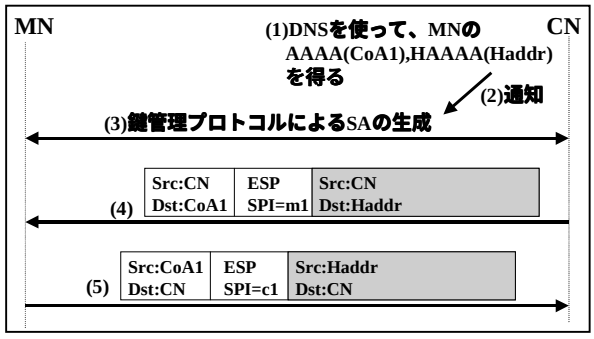

図 18：新規 Mobility プロトコルの Mobile Node への発呼

一方、既存ノードとの通信では、既存ノードが①IPsec を利用できない、②SA Gateway Update を利用できない、③HAAAA を利用できない、という問題点があります。このため、既存ノードと通信するために、①IPsec の代わりに Care-of address、②SA Gateway Update の代わりに IPsec Tunnel による通信、③HAAAA の代わりに Care-of address が移動先ノードの宛先、となってパケットが届くようにしました。これによって既存ノードとの互換性を確保しましたが、移動透過性は保証できていません。

5　今後の Mobile IP の動向

5.1　Mobile IP の接続試験

Mobile IP の接続試験は、過去 1995 年 11 月、1997 年 4 月、1999 年 7 月の 3 回開催されています。

1 回、2 回はベースプロトコルの確認、3 回目は、ベースプロトコルと DIAMITER･AAA の確認を目的に掲げていました。

実際には、参加者として 1 回目は大学、2 回目は大学とソフトウェアベンダーが中心で、研究レベルの段階にありました。3 回目ではキャリアや機器ベンダー中心に様変わりし、Windows 環境上で動作するなどといった製品レベルでの実装が急速に進んでいます。

接続試験は、接続マトリックスを作成し、結果を記入し、直後の IETF で匿名で報告することが RFC で決められています。

ベースプロトコルは、1 回目は Mobile IPv4、2 回目からは Mobile IPv4 と Mobile IPv6 を対象に参加を呼びかけました。しかし、実際には Mobile IPv4 がほとんどで、3 回目でも Mobile IPv6 実装は 2 例に留まっています。

5.2　Mobile IP の実装例と参考文献

Mobile IP に関する実装例の URL および参考文献、学会などを参考までに示しておきます。実装例は以下のとおりです。

- Stanford (Linux):
  http://gunpowder.stanford.edu/mip/
- CMU (FreeBSD):
  http://monarch.cs.cmu.edu/software.html
- National Univ. of Singapore (Linux, Windows?):
  http://mip.ee.nus.edu.sg
- Portland State univ. (FreeBSD):
  http://www.cs.pdx.edu/research/SMN/index.html
- Politehnica univ. of Bucharest (Windows NT):
  http://mip-nt.aii.pub.ro/
- Lancaster univ (Linux):
  http://www.cs-ipv6.lancs.ac.uk/MobileIP
- IKV++ GmbH (Windows NT):
  http://www.ikv.de/products/roamin
- Sun (Solaris, Linux):
  http://playground.sun.com/pub/mobile-ip
- Cisco (IOS):
  http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t1/mobileip.htm

●Ecutel (Windows):
http://www.ecutel.com/productstrial.htm
●Telxon (embeded):
http://www.telxon.com
●Toshiba (Solaris, Windows):
http://www.toshiba.co.jp/product/nc/ncg
●Helsinki univ. (Linux):
http://www.cs.hut.fi/Research/Dynamics
●Microsoft (Windows):
http://www.research.microsoft.com/msripv6
●Charles Perkins:
http://computer.org/internet/v2n1/perkins.htm

参考文献は以下のとおりです。

●「Jim Solomon:Mobile IP -- The Internet Unplugged」（詳説 Mobile IP 寺岡文男、井上淳監訳）Prentice Hall 社
MOBILEIP WG の元 Chair が動向をまとめたもの。よくまとまっている。
●「Charles E.Perkins: Mobile IP -- Design Principles and Practices, Addsison Wesley」
RFC2002 の編者による。Advanced topics なども広くカバー。

学会は以下のとおりです。

●情報処理学会：モバイルコンピューティング研究会
●ACM: MobiCom(MC2R)

6　モバイルインターネット

インターネットとモバイルの接点、移動通信システムから見たモバイルインターネットについて紹介します。

6.1　モバイルとインターネット

移動通信システムの多くは、ネットワーク自体は IP リーチャブルではありません。IMT-2000 の第 3 世代の当初は IP リーチャブルでなく回線交換でサービスを開始する予定です。

インターネットにとってモバイルは何か、ということですが、モバイルは、インターネット網に対するワイアレスのエンタランス回線です。わかりやすくいうとインターネットを通すための土管のようなもの(インフラ)と言えます。

モバイルにとってインターネットは何か、というと、それはキラーアプリケーションの１つと言えるでしょう。

7　ワイアレスシステムの最新動向

インターネットなどのネットワークや情報システムを活用したサービスを新たに提供しようとすると多くの場合、ワイアレスシステムも考慮する必要があると思います。まず最初に、現状のワイアレスシステムの最新動向を紹介します。具体的には、インターネットとモバイルとの関係をシステムごとに分けて述べていきたいと思います。

まずは PHS と、それを利用した位置情報サービスである「いまどこ」サービスを採り上げます。

PHS は、1999 年初めごろまでは、伝送速度は 32Kbps でした。その後 64Kbps 化が実現し、サービスエリアの拡大が図られています。

サービスとしては移動機のロケーションがいろいろな面で重要になっています。そこで DoCoMo の「いまどこ」というサービスに関して簡単に説明します。

次に、パケット通信ができ、IP パケットをトランスペアレントに通せるということで、インターネットと関連の深い移動通信パケットシステム「PDC-Packet」について説明します。

続いて、携帯電話でインターネットサーフィン(Web サーフィン)を行う「ｉモード」というサービスのシステム概要を説明します。

さらに、移動通信事業者は、モバイル向けに ISP サービスを行っています。その中で DoCoMo の「mopera」を紹介します。

最後に次世代移動通信システム IMT-2000 に関しては、無線システムの動向と、サービス開始当初のネットワークの構成がどうなっているかを述べます。

7.1　PHS の動向

まず PHS の動向については、64Kbps 化が実現し、そのエリア拡大が進められています。そこで DoCoMo の PIAFS64K サービスのしくみと端末の状況、さらには、PHS を活用して位置情報を知ることができる「いまどこ」サービスのシステム構成について触れてみます。

7.1.1　PIAFS64K サービス

DoCoMo では、データ通信に非常に特化している端末として「611S」、

「P-in」の 2 種類を提供しています。

611S は携帯電話にも使えるタイプの PHS で、64Kbps/32Kbps データ通信に対応できます。P-in はデータカード一体型モデルです。

インターネットへはダイアルアップによる RAS への LAN アクセスあるいは、IPS へ接続します。PHS 全体のマーケットの伸びは緩やかですが、64Kbps によるデータ通信マーケットは急成長しています。

7.1.2 PIAFS64K サービスの仕組み

もともと PHS は、上りと下りの伝送を 1 つの周波数チャンネルで行っています。全部で 8 チャンネル多重をかけて、上り 4 チャンネル、下り 4 チャンネルに分けています。

上り/下りそれぞれの先頭のチャンネルを制御用物理チャンネルに使用しています。したがって、通常の通話では、同時に 1 つの基地局で 3 チャンネルの上り/下り通話ができます。1 チャンネル(スロット)は 32Kbps の通信速度が得られます。

PIAFS64K サービスでは、64Kbps 化するため、1 人のユーザにこの 3 チャンネル中の 2 チャンネル分を割り当てる方式をとっています。

したがって、回線が占有されていない際には 2 チャンネルを確保した通話者は 64Kbps のサービスが受けられます。しかし、先行占有者がいる場合には 1 チャンネル分しか使用できないので 32Kbps のサービスを受けることになります。

１つの基地局に複数の無線機がある場合には、１つの無線機だけが制御に対応し、他はユーザのトラフィック利用のみで使用されます。チャネル割り当ては、無線機を渡り歩く場合は隣接スロットの割り当てはしていません。これはシンセサイザの切り替え時間によるものです。

DDI ポケットの H"サービスでは、1 つの移動機に 2 つの受信機が搭載されていて、2 つの基地局から受信できるようになっています。それを順次切り替えます。それゆえ、将来的には下り 128Kbps の通信の可能性もあると考えられます。

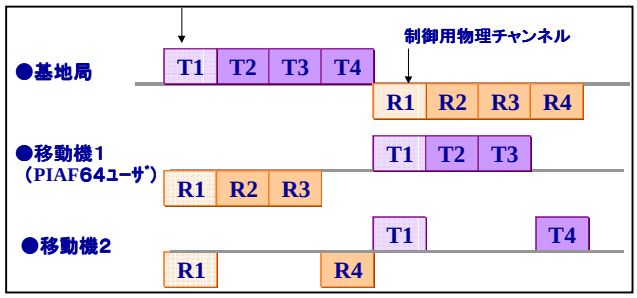

図 19:PIAFS64K サービスの仕組み

7.2 「いまどこ」サービス

通常、PHS の基地局(CS)は、数 100m 間隔で配置されています。移動機は、周囲の基地局から電波を受信して 2 つの基地局を選択します。位置情報センターでは、移動機と 2 つの基地局の交信が確認されると、位置情報サーバが両基地局の位置情報を元に、この移動機の現在位置を両基地局の中間点と確定します。

この移動機の位置情報を、「いまどこ」サービス加入者のパソコンへ緯度経度情報として提供します。

また、位置情報サーバは、位置情報センターのデータベースと照合し、地図情報として加入者のファクシミリに出力するサービスも提供しています。現状では、基地局の設置間隔が数 100m 単位のため、2 つの基地局の中間値を PHS の現在位置とするのでは精度が高いとは言えません。そのため、交信基地局を増やしたり、電波の強度の計算を加えることで、精度の向上を図ることも試みられています。いずれにしても、100m 程度の誤差が生じることは避けられないと想定されています。

ただし、移動機だけで位置情報が得られる便利さは評価されています。

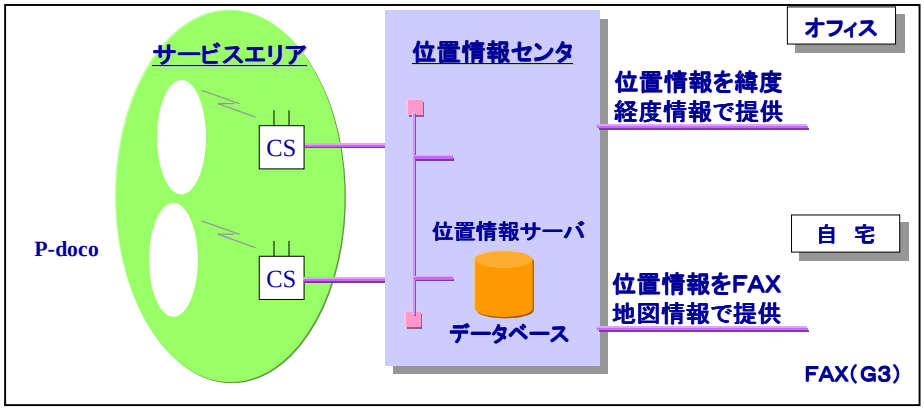

図 20：「いまどこ」サービスのシステム構成

サービスメニューは、法人向け、個人向けに分かれています。

具体的なアプリケーションとしては、当初ビジネス向けを想定していました。しかし、サービス契約者は 20 歳代が少なく、30 歳代後半から 40 歳代が多いことを考えると、親が契約して子供に持たせ、行き場所を監視するために利用するケースが多いようです。これも塾通いで帰宅が遅くなっている為では無いでしょうか？

DoCoMo では、位置情報サービス専用の簡易端末 P-doco も商品化しています。これを携行していると移動しても現在位置が常時確認できます。

猫の首に付けるという利用形態もありますが、車両の盗難防止用としての利用などが現実的と言えます。

7.3 DoPa の最新動向

7.3.1 DoPa の概要

PHS は回線交換型システムで、64Kbps 回線を時間課金で提供しているサービスです。もう 1 つの無線伝送サービスとして、DoCoMo では、パケット交換タイプのサービス「DoPa」を提供しています。

DoPa は、インターネットサービスプロバイダあるいは企業等の LAN に対するパケット交換タイプの無線伝送路を提供するサービスです。システムとしては PDC-Packet と呼んでいます。システム構成は DoPa とはやや異なりますが、DDI の PacketOne もこれに類するサービスです。

また、DoPa では、ネットワークのベースには携帯電話網 PDC を利用しています。情報端末から PGW(パケットゲートウェイ)に対して PPP で論理セッションを確立します。

PDC-Packet 網の中のルーティングは、IP ルーティングではなくて、電話番号をベースとする独自のルーティングを行い、IP をカプセリングする方法を採用しました。

米国には CDPD という同じようなパケットサービスがあり、IP ルーティングを採用しています。ただ、IP ルーティングにした結果、接続先は 1 つの ISP のみとなり、企業等の LAN へはインターネット経由となっています。

わが国の場合、セキュリティの関係で、インターネット経由でイントラネットに乗り入れることを嫌がるユーザが多いことも事実です。そこで、ネットワークそのものは多目的で利用できるようにするため、電話番号に IP を完全にカプセリングして閉じこめて、専用線、ISDN 回線で、企業の LAN や ISP に渡す方式を採用しました。そのために PGW に IP と電話番号の関係を記憶しておくテーブルを持たせています。

セキュリティ面では、接続先を特定の電話番号に制限することで、強制的に接続先が他にならないようにすることも可能です。

最大伝送速度は、DoCoMo の場合は上り 28.8Kbps、下りも 28.8Kbps です。PocketOne では下りが 64Kbps、上りが 14.4Kbps と上りも下りも 14.4Kbps の 2 サービスがあります。下りを高速にするのは、サーバ側からの情報量が、移動機側からの上りの情報量に比べて圧倒的に多いという状況を勘案して効率的な回線利用を意図したものと言えます。

なお、１つのチャネルを複数のユーザが同時に利用した場合、DoCoMo は速度保障をしていませんが、PocketOne では、64 Kbps サービスに対して 13 Kbps を保障しています。

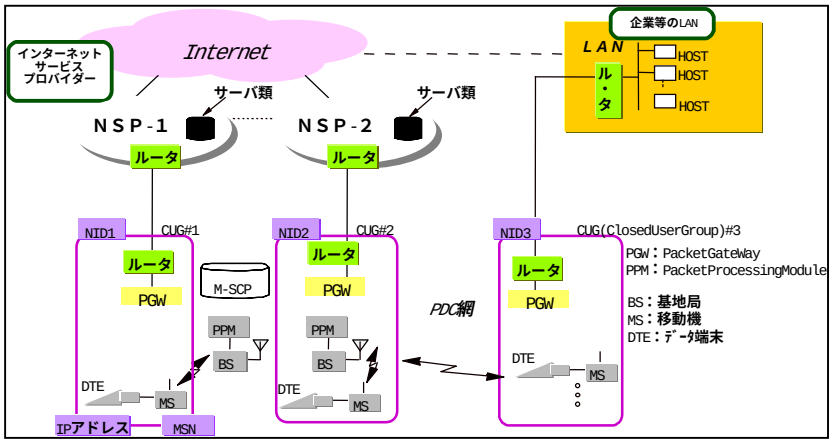

図 21：DoPa システムの構成

7.3.2 Dopa と回線交換データ通信の違い

続いて、パケット交換と回線交換データ通信の違いについてです。回線交換では、モデムネゴシエーションがまず最初に行われ、次いで PPP の起動、アプリケーションの起動、そしてデータの送受信が行われます。一方、 Dopa では、モデムネゴシエーションの部分は不要で、PPP からスタートします。１度、PPP により論理セッションが確立されれば、要求があった時だけデータの送受信ができます。

回線交換では時間課金のためモデムネゴシエーションを含め接続中の時間すべてが課金対象になります。

これに対してパケット交換データ通信では、情報量に応じて課金される従量課金を採用しています。このため、実際に送信したかあるいは受信したパケットに対して課金されます。

また、Dopa では、移動機と基地局間の物理的な通信が何らかの環境の悪化で途切れた場合でも、論理セッションは回線交換に比べて長時間接続状態のまま継続されます。このため、基地局との間の通信状態が回復すればそのまま再接続され、データが送られてきます。利用者側からは、見かけ上通信が切れていないように見えます。

このため、高速道路での自動車や新幹線の中からの通信といった高速移動のモバイル通信に適しています。

最近は、パケット通信機能を内蔵した PDA 端末や、無線パケットモデムが登場してきており、それらを使用した新しいアプリケーション分野も開拓されています。

たとえば、自販機などに無線パケットモデムを組み込むことによって、自販機の広域管理システムが構築できるようになっています。

また、運送会社が自社管轄の車両に無線パケットデータ通信端末を搭載し、運行管理する会社も出てきました。同様にバスロケーションシステムに利用する動きもあります。

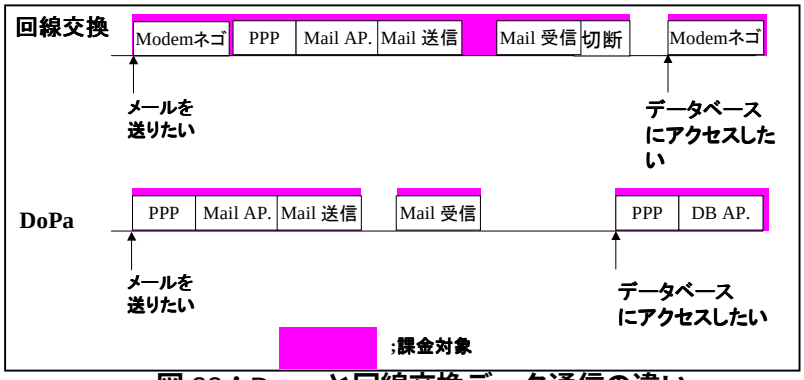

図 22：Dopa と回線交換データ通信の違い

7.4 i モードサービス

ｉモードサービスは、1999 年 2 月 22 日に DoCoMo がサービスを開始しました。携帯電話で Web サーフィンができるサービスです。1999 年 8 月には 100 万加入を突破、10 月初めには 200 万加入を突破し、成功を収めています。携帯端末にブラウザを搭載した先例では、米国に PocketNet と言う CDPD を使用したサービスがあり、日本にもアステルの mozio サービスがあります。しかし、ｉモードサービスほどには成功したとは言えないでしょう。

ｉモードのサービスとしては、インターネットメールをサポートしています。しかも自動メール受信を行っているのが通常のメールサービスとは異なっています。情報アクセスとしては、通常タイプのプル型情報サービスのほか、プッシュ型情報サービスもあります。プッシュ型の場合、システムのキャパシティなどの制約条件があり、実際には天気情報だけが提供されています。また、URL を入力すれば、ホームページにアクセスできます。しかし、ディスプレイサイズや、Java をサポートしていないなどの問題から、実用的な閲覧にはかなり無理な状況というのが現実です。

具体的なシステム構成としては、パケット網を使用しており、PDC-Packet 網上にｉモードサーバを配置し、課金系と認証系のデータベースシステムを運用しています。インターネット経由でコンテンツプロバイダに接続する方式を採っています。

ｉモードの場合、コンパクト HTML という HTML のサブセットを使用しており、HTML を知っていれば、一部制限事項を覚えるだけでコンテンツを書けます。一方、Phone to という電話番号を入れると自動的に発信をかけられるタグが追加されており、携帯インターネットならではの利用が可能です。

これに対して、DDI の EZWeb および IDO の EZ アクセスでは WAP を

使用しています。IP の記述言語は、UP 社が提供している HDML を採用しています。これは XML をベースにしており、HTML ではありません。そのため、コンテンツ作成者は、改めて習得する必要があります。この不便さを緩和するため、変換用プロキシを提供しています。

ところで、ｉモードの成功の理由の１つはパケットにあると言えます。携帯情報端末で情報にアクセスしているときに、必要な情報すべてをダウンロードしてセーブしてから見るというのでは、効率や使い勝手が悪くなります。

これに対してパケットの場合、見ながらアクセスを行っても、パケットを実際にダウンロードしなければ課金されず、しかも切り忘れが生じません。回線交換網では、切り忘れはそのままコストに影響します。パケットは、一度接続作業を行えば、論理的には接続状態を保てるので、立ち上げ時間も少なくて済みます。また、テキスト中心のコンテンツであれば料金も少なくて済むことになります。

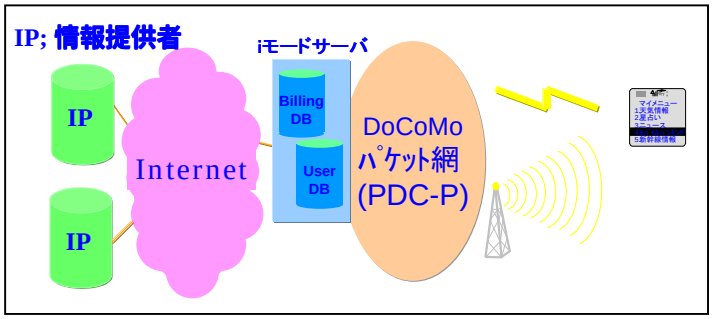

図 23：ｉモードのシステム構成

7.5　ｉモードの主要なコンテンツ

ｉモードの主要なコンテンツを表 1 に示します。これらのなかでは、エンターテイメント系が最も多くアクセスがあり、サービスをよく利用しています。また、新聞(ニュース)関係も利用が多い状況です。モバイルバンキングは、当初注目度が高かった割には利用されていないのが現実です。

表 1：主要コンテンツ

取引系	・モバイルバンキング ・格安旅行情報 ・ホテル予約 ・書籍販売 ・航空券予約 ・賃貸不動産情報 ・コンサートチケット予約
データベース系	・レストランガイド ・字引サービス ・電話番号案内 ・乗り換え案内
生活情報系	・天気予報 ・ニュース速報 ・株価情報 ・競馬情報 ・原宿街情報 ・映画情報
エンターテイメント	・音楽系情報 ・占い ・ネットワークゲーム ・カラオケ

ところで、ｉモード端末を応用して CGI も利用することができます。ｉモード端末を利用した受発注システムなども開発されています。面白いところでは、鍵の開け閉めなどリモートコントロール的なサービス端末としてｉモード端末を利用する動きもあります。現在カラー端末が登場しています。これは第 2 世代に当たります。今後第 3 世代の Java(jini) 搭載へと進むことになりそうです。

7.6　mopera サービス

mopera サービスは、モバイルユーザ向けにチューニングしたインターネット接続サービスです。位置情報、ハウジングサービスのほか、携帯電話、PHS 電話料金に付加してして徴収する料金回収代行サービスを行っています。E ビジネスなどインターネットを活用したサービス事業を展開する企業にとって、代金回収の機構作りは大きな課題となっています。その意味では、そうした周辺の機構までを提供することは新たなビジネスモデルになりますので、注目されています。

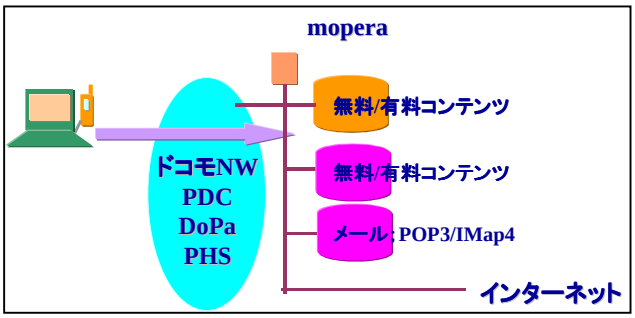

図 24：mopera のシステム構成

7.7　GPS サービス

DoCoMo は、位置情報管理では、スナップトラック社の GPS 技術を採用した位置情報サービスを開始しました。

サービスメニューは、自分の位置を表示する、目的地の地図を表示する、経路サービスなどを用意しています。

現在提供している端末の大きさはシャープのザウルス程度で、携帯電話を接続して利用します。センターとのやりとりが必要で、交信から 30 秒以内に地図情報を受信完了します。

サービスエリアは全国です。携帯電話が利用できる所であればどこでも利用できます。

最大の特徴は、精度と感度の良さです。一般の GPS の場合、少なくとも 3 個から 4 個の衛星が直接見えていなければならず、D-GPS でなければ精度は 100m 程度です。一方、この端末では、窓の側にいれば衛星が直接見えていなくても測位可能です。精度は 50m 以下です。利用した感じは 10m 程度の誤差に納まっています。サービスイメージは図 25 のとおりです。

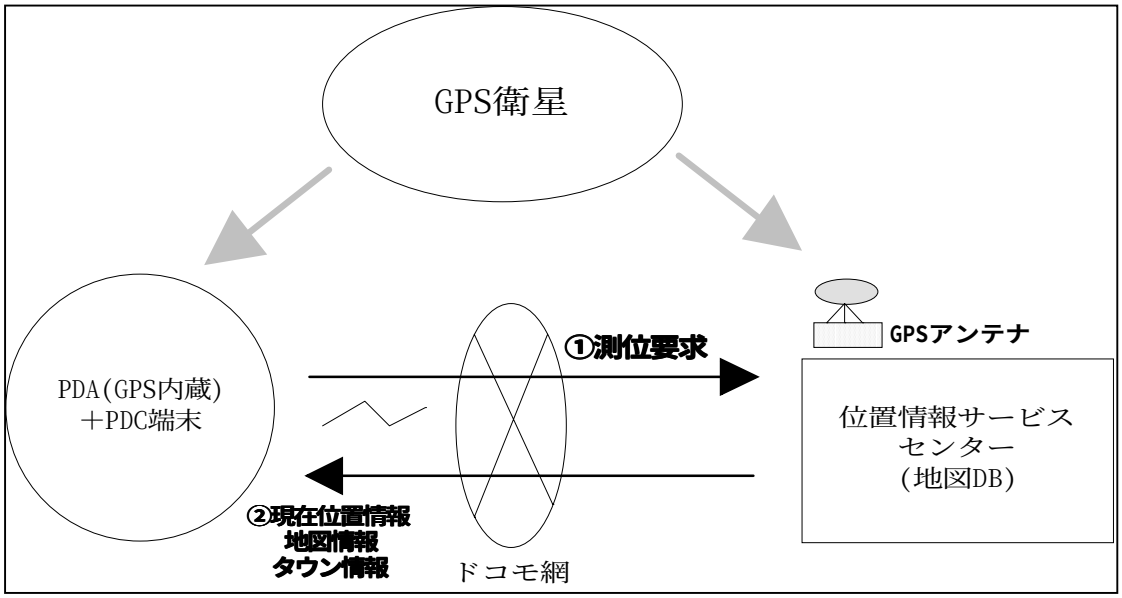

図 25：GPS 技術による位置情報サービス

GPS 内蔵の PDA＋PDC 端末は、位置情報サービスセンターに測位要求を出します（矢印①）。そうすると、現在位置情報、地図情報、タウン情報が同センターから送られてくるという仕組みです（矢印②）。

8　IMT-2000 への展開

IMT-2000 はいわゆる第 3 世代の携帯情報通信サービスで、そのサービス面と無線サービスから見た展開、第 3 世代の要求条件、端末イメージ、ネットワーク構成などを説明します。

IMT-2000 の当初のサービスの狙いは、ユニバーサルサービス、パーソナルサービス、マルチメディアサービスを実現することを目的にしてきました。

しかし、ユニバーサルサービスについては、当初構想とは異なる状況になってきています。

ユニバーサルサービスの実現には通信方式の標準化が大きなカギとなります。実際にはいくつもの方式が併記される状態になっています。 わが国と欧州は W-CDMA、米国は CDM2000 を支持しており、ネットワークアーキテクチャも、GSM という欧州規格のネットワークと、ANSI41 という米国規格とが併走しています。

また、さらなる高速伝送を目指して、第 4 世代の研究も始まっています。

一方、ソフトウェア無線という考え方も登場しており、無線機の特性を

ソフトウェアで変更する研究が行われています。これが実現できれば、無線方式の不統一の問題をも容易にクリア可能と考えられます。

第 3 世代の要求条件では、伝送速度は 2Mbps までの多元レートを目指しており、サービスエリアもアウトドアからインドアまでを対象にしています。屋内では 2Mbps、低速移動 384Kbps、高速移動 128Kbps、パケットと非対称を標榜しています。

ネットワーク構成としては、回線交換網だけでなく、IP 網の検討も行われているようです。

DoCoMo では 2001 年春の実用化に向けて実用化実験を行ってきています。東京／横須賀において、64Kbps から 384Kbps の伝送速度が混在できる形で、インターネット上の各種のサービスを実験しました。また、ビデオフォン、28.8Kbps モデム、64Kbps の PC カードモデムなどの動作確認も行っています。

また、中国、韓国、タイ、シンガポールなどとの共同実験も進行中です。

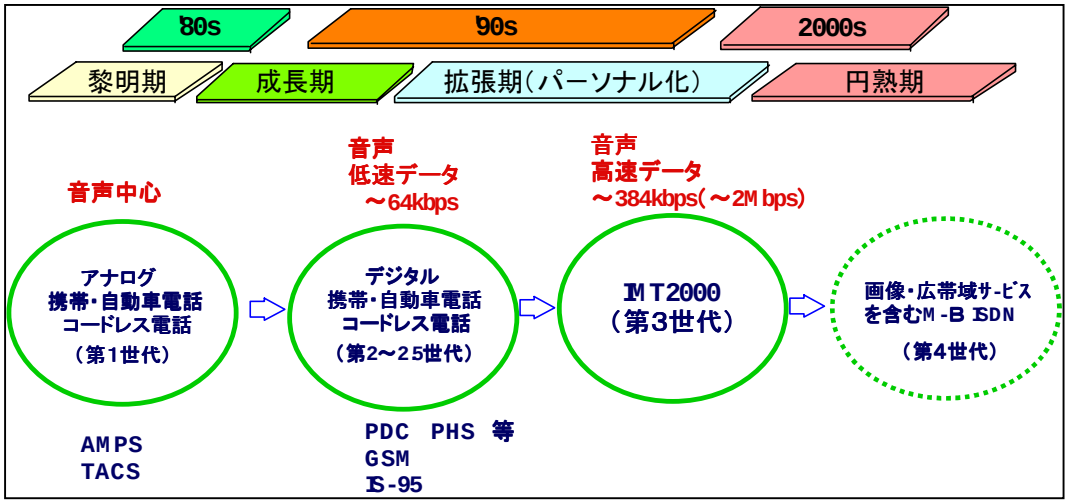

図 26：移動通信システムの IMT-2000 への展開