

## Mobile IP の現状と問題点に関する一考察

石山 政浩<sup>†</sup> 井上 淳<sup>†</sup>  
岡本 利夫<sup>†</sup> 寺岡 文男<sup>††</sup>

本論では Mobile IP が普及しない原因について考察し、その問題点を指摘するとともにこれに代わるプロトコルの必要性について論ずる。Mobile IP は移動ノードとの透過的な通信機能を提供するが、現在のインターネット環境を分析すると、1) 通信基盤が移動透過環境を提供するに至っていない、2) アプリケーションが移動透過性を必要としていない、などが導き出される。また Mobile IP のアーキテクチャを分析すると、1) ホームアドレスおよびホームエージェントの準備が困難、2) Firewall 等のセキュリティ機構との不整合、が見出される。次に将来を展望すると、通信基盤やアプリケーションには移動透過性が必要とされるであろう。しかし Mobile IP の持つ問題は依然として残るため、将来においても Mobile IP は普及しないであろう。

### A study of the current Mobile IP status, the obstacles of its wide usage, and the future direction of mobility support

MASAHIRO ISHIYAMA,<sup>†</sup> ATSUSHI INOUE,<sup>†</sup> TOSHIO OKAMOTO<sup>†</sup>  
and FUMIO TERAOKA<sup>††</sup>

In this paper we discuss the reasons why Mobile IP has not been successfully deployed, the problems that Mobile IP has, and necessity of a new protocol that supports mobility. Although Mobile IP is a protocol for supporting transparent IP mobility, analysis of current internet environment shows that: 1) Mobility is not important because of a lack of network infrastructure, 2) There are few applications that make effective use of mobility. Also analysis of Mobile IP architecture shows that: 1) Providing Home Agent and Home Address face some difficulties, 2) It conflicts with the current internet security mechanisms such as firewalls. It is probable that mobile users will come to need mobility in the near future by the evolution of network environment. Still the problems that Mobile IP has will leave. Thus the deployment of Mobile IP will not happen without changing its architecture.

#### 1. はじめに

携帯端末の性能の向上と、移動通信機器の普及に伴い、移動先から携帯端末を利用したインターネットへのアクセス、いわゆるモバイルコンピューティングが活発に行われるようになってきた。一方、IETF では移動ノードの透過的なインターネットアクセスを提供するためのプロトコルである Mobile IP が提案されている。しかし、携帯端末によるインターネットの利用の普及度と比較すると、この Mobile IP プロトコルは全く普及していないといっても過言ではない。本論文では Mobile IP が普及しない原因について、インターネットの現状

および Mobile IP アーキテクチャの観点から考察し、また将来への展望を示す。

まず 2 章で Mobile IP プロトコルの概要を示す。3 章では、移動ノードの移動モデルを分類した上で、Mobile IP が提供する移動透過性が有効に利用できない理由について考察する。4 章では、現在のインターネットの利用形態と Mobile IP の乖離点について指摘するとともに、Mobile IP 自身のアーキテクチャの問題点について議論し、Mobile IP が普及しない原因を明らかにする。5 章では、移動透過性の必要性が増加する将来のインターネットの利用像を提示し、それでも現状の Mobile IP のアーキテクチャの問題点が依然として残ることを示す。これらをふまえて新しい移動透過性のプロトコルの必要性とその条件について論ずる。

#### 2. Mobile IP の理念とプロトコル概要

本章では、まず Mobile IP の理念と利点について述

<sup>†</sup> (株) 東芝 研究開発センター 情報・通信システム研究所  
Communication and Information Systems Research  
Laboratories, R&D Center, Toshiba Corporation.

<sup>††</sup> (株) ソニーコンピュータサイエンス研究所  
Sony Computer Science Laboratories Inc.

べ、プロトコルの概略を示す。

## 2.1 Mobile IP の理念

Mobile IP は、ネットワークの物理的な接続点が変わっても、同じ IP アドレスを使用し続けることにより IP 層による移動透過性 (mobility)<sup>8)</sup> を提供することを目的としている。この移動透過性は、単にノードがあるネットワークから他のネットワークへと移動できる可搬性 (nomadicity)<sup>9)</sup> と呼ばれる能力に比べ、以下の 2 点で優れている。

### 2.1.1 移動によるセッションの喪失の回避

可搬性のみを持つ移動ノードがあるネットワークから異なるネットワークに移動した場合、その IP アドレスが変化するため、それまでに使用していたセッション (たとえば telnet 等) が切断されてしまう。また、NFS のようなセッションの概念のない通信の場合も、通常は互いの IP アドレスを記憶しているため、IP アドレスの変化のためサービスの継続が不可能になる。

一方、Mobile IP では通信相手に通知する IP アドレスは一定のまま変化しないので、ユーザの移動によらず既存のセッション、サービスをそのまま継続して使用することができる。

### 2.1.2 ノード識別子として IP アドレスを使用可能

可搬性のみでの移動ノードがネットワーク上を移動する場合、何らかの方法でその移動先アドレスを知る機構が必要となる。

一方、Mobile IP では単に Home Address を知っているだけでよい。すなわち、一定の Home Address を使用し続けられるので、移動ホストに対して発呼するような応用でも、現在位置を意識せず常に Home Address を宛先 (ノード識別子) として使用できる。例えば、Voice over IP のようなアプリケーションで移動ホストに対して発呼する場合に、常に Home Address を識別子として使用できることの効用は容易に理解できるだろう。

また、サービスに対してノード単位のアクセス制御を行う場合、現在は IP アドレスを元に制御を行うことが多い。このような場合、一定のホームアドレスでノードを識別することで、移動先でも Home Network で受けていたサービスに透過的にアクセスすることが可能である。

## 2.2 プロトコルの概要

Mobile IP のプロトコルは現在、IPv4<sup>1)</sup> のための仕様と、IPv6<sup>3)</sup> のための仕様の 2 つが提案されている。本節では各々の概略と要求仕様を示す。

### 2.2.1 Mobile IPv4

Mobile IPv4 の概略構成を図 1 に示す。

- 移動ノードは 1 つの Home Address をもつ。これは永続的なノード識別子であり、ネットワーク上で移動しても通信相手は Home Address 宛にパケットを送信する。
- Care-of-Address (CoA) は、移動ノードが移動先ネットワークで割り当てられるアドレスで、Foreign Agent (後述) のアドレスか、もしくは DHCP など直接移動ノードに割り当てられる。後者を co-located care-of-address と呼ぶ。
- Home Address が属する IP サブネット (Home Network) には Home Agent と呼ばれるルータがある。これは移動ノードから現在位置の登録を受け取って管理し、移動先のノードにパケットをカプセル化転送する役割を果たす。
- Foreign Agent は各移動先ネットワークに配置されるルータで、移動してきた移動ノードに対して CoA を指示し、また Home Agent からカプセル化転送されたパケットを受け取ってデカプセル化し、移動ノードへリンク層のアドレスを利用して配送する。移動ノードが co-located CoA を使用する場合には Foreign Agent は必要ない。
- 移動ノードは、移動するとまず CoA を取得し、Home Agent (Foreign Agent がある場合にはそれを経由して) に対して登録を行う。登録が成功すると、Home Agent は移動ノード宛 (すなわち宛先が移動ノードの Home address) パケットを代理受信し、CoA を最終宛先として IPinIP でカプセル化<sup>2)</sup> し転送する。
- 移動ノードが co-located CoA を使用する場合は、Home Agent 発のカプセル化転送パケットは、直接移動ノードに到着するので、ノード自身がデカプセル化を行う。Foreign Agent が存在する場合、Home Agent からのカプセル化転送パケットは、Foreign Agent に到着するので、Foreign Agent はこれをデカプセル化し、得られた Home Address 宛のパケットを移動ノードに転送する。
- 移動ノードは、通信相手にパケットを送信する場合、自分の Home Address を source address として使用する。

### 2.2.2 Mobile IPv6

Mobile IPv6 の動作概略を以下に述べる (図 2)。Mobile IPv4 との主な相違点、個々の構成要素の動作を以下に示す。

- Foreign Agent という概念がなくなり訪問先ネットワークで必ず co-located CoA を取得する。す

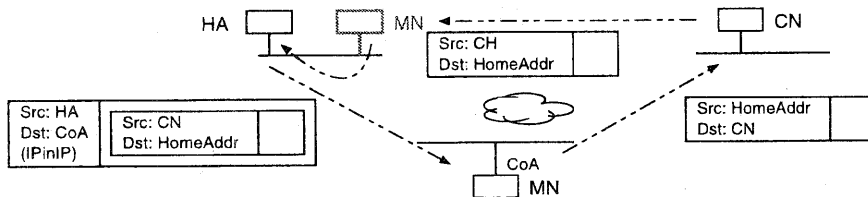


図1 Mobile IPv4の動作: 移動ノード(MN)は移動先から直接通信相手(CN)へ向けてパケットを送信し、CNはHome Address(HA)へ向けてパケットを返す。Home Agentはこれを代理受信してMNへと転送する

なわち、Foreign Agentという特殊ルータの普及を期待する必要がなくなった。co-located CoAの取得方法はaddress auto-configuration<sup>14)</sup>や、DHCPv6<sup>15)</sup>など任意の方法でよい。

- Mobile IPv4のHome Agent経由の冗長な三角経路を回避するための経路最適化(Route Optimization)を条件つきで基本仕様に取り入れている。
- 移動ノード発IPパケットのSource Addressが、Home AddressからCoAに変更された。これにより、経路途中のIngress filtering<sup>7)</sup>によりMobile IPが使用できない状況を回避できるようになった。
- Mobile IPv6では、独自のUDPメッセージで移動情報を交換するのではなく、IPv6のDestination Optionを使って、通常の通信に織り混ぜて移動情報を交換する。以下の4つのDestination Optionが定義されている。

#### (1) Home Address Option (HAO)

送信者が通信相手に自分のHome Addressを通知するために使用する。これを含むパケットを受信した場合、あたかもHAO内に記述されたHome Addressから到着したものととして扱わなければならない。

#### (2) Binding Update Option (BUO)

送信者が通信相手にCoAとHome Addressの“binding”を要求するために使用する。Home Agentへの登録もこれを使用する。これを受信したホストは、Home Addressを持つホストがCoAに移動したことを認識する。

#### (3) Binding Acknowledgement Option (BAO)

BUOに対する了承応答として使用する。この応答を要求するかどうかはBUO内のフラグで指示される。通常BAOはHome Agentに対して要求され、通常の通信相手には要求されない。

#### (4) Binding Request Option (BRO)

移動ノードに対してBUOを要求するために使用する。Binding CacheにはLifetimeがあるので、それが切れる前にBROを使用してBinding Cacheを更新する。

- 移動ノードは、移動してCoAを取得すると、Home Agentに対してHAO, BUOを含むパケットを送信する。Home Agentはこれを了承すると、その移動ノードの現CoAとそれに纏わる情報群(binding)を生成し、BAOを返信する。bindingが生成されると、Mobile IPv4同様移動ノードのHome Address宛のパケットを代理受信しCoA宛にIPv6 in IPv6 tunneling等を用いて転送する。
  - 移動ノードが通信する場合、送信パケットに必ずHAOを含める。また、BUOを含めることもでき、その場合、受信した通信相手は、可能であればbinding cacheを生成してもよい。binding cacheが生成されると、通信相手が移動ホスト宛パケットを送信する際、Routing Header(RH)を使用してCoA経由でHome Address宛にパケットを送信する。従ってRHにより、パケットまずCoA宛にルーティングされ、結果的にHome Agentを経由しない経路最適化されたパケット交換が可能となる。
- 但し、BUOに対して受信側がbinding cacheを生成できない場合は、RHは使用できず、Mobile IPv4と同様にパケットはHome Agent経由で三角ルーティングされる。

### 3. 現状のインターネットの分析

現在、ノートPC等の携帯端末は数多く普及しており、インターネットの利用者も非常に多い。そして実際に携帯端末を利用して移動先からインターネットへアクセスする姿を見ることも珍しくない。このような環境は、Mobile IPの利用を促すように考えられるが、実際にはMobile IPの利用者はほぼゼロと言っても過言



移動ノードでこのようなアプリケーションを利用する場合、移動という行為自体の頻度が非常に少ないため、セッション自体が移動によって失われることが少ない。また、たとえ端末の移動によってセッションが途中で切断されてしまったとしても、もともとが接続/切断を頻繁に繰り返すアプリケーションなので、セッション切断による被害が比較的小さい。

さらに、たとえトランスポート層のセッションが切断されても、アプリケーション側で再接続を可能にするものも多くなってきている。たとえば The Olivetti and Oracle Research Lab(ORL)のVNC<sup>5)</sup>や、Unixのscreenコマンドを利用している場合のtelnetなどがこれに相当する。

このため、たとえIPアドレスが変わって使用中のセッションが失われたとしても、ユーザが被る被害は再接続に伴うオーバーヘッドだけである。オフライン移動ではIPアドレスの変化の間隔が長いので、再接続に伴うオーバーヘッドの負担もユーザには苦痛が小さい。

対して、移動ノードに対して発呼する必要があるアプリケーションでは、移動透過性が有効に働くのは2.1.2節で述べた。しかし現在はそのようなアプリケーションはまだ少ない。

よって、現在のモバイルユーザが使用するアプリケーションは移動透過性を使用しない。このためやはりMobile IPは現在のユーザに必要ながなく、可搬性だけで十分となる。

### 3.4 現在のインターネット環境における Mobile IP の普及の阻害理由

以上の議論をまとめると、次の2つの理由によりユーザは移動透過性を必要とせず、結果としてMobile IPの普及を阻害している。

- インフラストラクチャの未整備  
移動透過性はオンライン移動の際に有効に働くが、残念ながら現段階では十分なネットワークインフラストラクチャが存在せず、ユーザはオンライン移動を行う事ができない。
- 移動透過性を必要とするアプリケーションの不在  
移動ノードは固定ノードと同じアプリケーションを同じように利用している。このため、移動ノードは移動透過性を有効に活用できない。

## 4. Mobile IP アーキテクチャの問題点

Mobile IPのアーキテクチャそのものが、現在のインターネットの利用モデルと大きく乖離しており、問題を多く抱えている。以下、Mobile IPのアーキテクチャ自身が持つ問題について述べる。

### 4.1 Home Address の問題

Mobile IPでは、Home Addressが不可欠な要素であるが、現在のIPv4ではこのHome Addressの扱いが難しい。IPv4のIPアドレスは枯渇の方向に向かっており、数多くのIPアドレスを取得するのは難しい状況にある。

このため、企業ユーザについて考えてみると、現在多くの企業では、Firewallを設置してprivate address<sup>6)</sup>を使用しているケースが数多く見られる。この場合、Home Addressとして使用できるのはprivate addressであり、この結果必然的にMobile IPを利用して接続できるホストは、自分のサイト内だけに限られることになる。

また、一般ユーザの大多数はダイヤルアップサービスを利用している。これはISPが、ISPが持つアドレス集合から現在空いているアドレスを、端末に対して動的に割り当てる形式である。このため、Home Addressといった固定的なアドレスを割り当ててもらうことは困難といえる。

よって、現在のMobile IPのアーキテクチャでは、Mobile IPの使用範囲が厳しく制限される。

### 4.2 Home Agent の問題

Mobile IPは、Home Agent無くして使用することはできない。これは、Mobile IPを使用した場合、移動ノードと通信相手とが正常であっても、Home Agentに障害が発生した場合には、通信が全くできなくなることを意味している。

また、Home Agentの設置場所も問題である。企業や大学など、固定的で常時接続のネットワークを持っている場合には問題ないが、ダイヤルアップサービスを利用している、常時接続のネットワークを持たないユーザの場合は、どこかにHome Agentを設置してもらう必要があり、これはユーザにとってみるとMobile IPを使用することに対する大きな障壁となりうる。

そして、Mobile IPを使用すると、Home Agentを経由する三角経路を使用することになる。通常はノード-ノード間のネットワークが正常であればその2つのノード間で通信が可能である。しかしMobile IPを使用すると、移動ノードと通信相手間だけではなく、通信相手とHome Agent間、そして移動ノードとHome Agent間という3つのネットワーク経路が正常であることが要求される。これはネットワークの障害に対してより脆弱となることを意味している。同時に、移動ノードと通信相手間のネットワーク的な距離が近くても、Home Agentとの距離が遠ければ移動ノードと通信相手間のネットワーク距離は結果として遠くなってしまふ。

#### 4.3 セキュリティに関する問題

現在のインターネットでは、ほぼすべての組織が何らかのセキュリティに対するポリシーを明確に持っている。このポリシーを具現化する1つの方法として、Firewallがある。ほとんどの組織は、機能差はあるものの何らかのFirewallを介してインターネットへと接続しているのが現状である。このような環境下ではMobile IPの利用は困難となる。

移動ノードが組織外に移動して、組織外のホストとMobile IPを使用して通信する場合を考える(図3(a))。2章で述べたように、Mobile IPを使用すると、移動ノード(MN)と、通信相手(CN)、そしてHome Agent(HA)での三角形の経路でパケットが交換される(Mobile IPv6であっても、binding cacheが生成されなかったケースではこうなる)。この場合、組織外ホストからHAへの到達性が必要となるが、組織外ホストとHAとの間にFirewall F1が存在するため、この通信は通常困難なものとなる。なぜなら、通常の通信モデルでは、Firewallの内側と外側の通信には必ずFirewallが介在するため、Firewallはホスト間の通信をすべて把握することができる。その結果Firewallが通信の可否を判断することができる。しかし、移動ノードが組織外のネットワークに移動している場合には、移動ノードから通信相手に対して、F1を介さずに直接パケットが送られるため、F1はどのような通信が移動ノードと通信相手で始まったのかを知ることができない。結果、突然外部ホストからの移動ノード宛てのパケットがF1に届くこととなり、F1によって通信を遮断されてしまう。

次に移動ノードが組織外に移動して、Firewallによって守られている他の組織内のホストとMobile IPを使用して通信する場合を考える(図3(b))。この場合、前述の問題に加えて、移動ノードは、Home Agentの属するFirewall F1と、通信相手が属するFirewall F2の2つのFirewallと何らかのネゴシエーションを行わなければならないとなり、事態はより複雑になる。

これらの問題を解決するために幾つかの方法が提案されている<sup>10)11)12)</sup>が、通信オーバーヘッドの増加の問題や、多種多様化するFirewallメカニズムへの対応などがあり、一般には認められていないのが現状である。

よって、現在のMobile IPのアーキテクチャでは、Firewallが存在する通信モデルでの利用には大きな障壁があるといわざるを得ない。

#### 4.4 Mobile IP アーキテクチャの問題点について のまとめ

以上の議論をまとめると、現在のインターネット利用モデルにおいて、Mobile IPのアーキテクチャは次の3

つの問題があるといえる。

- Home Addressの問題

現在のインターネットのモデルでは、Home Addressの定義が難しい。特にこれから大量のユーザの増加が見込まれる家庭ユーザ等では、そのアドレスをどのネットワークのに置くのか疑問となる。

- Home Agentの問題

Home Agentは、常時接続のネットワークに接続しておかなければならず、Home Agentは機能しなければ移動ノードは全く通信することができない。これは通信の健全性を脆弱にし、同時にインターネットのEnd-Endの通信モデルに全く反している。

- Mobile IPのセキュリティの問題

現在のインターネット環境においてFirewallは必須ともいえるメカニズムであるが、Firewallのある環境でのMobile IPの利用は、プロトコルが複雑化し、オーバーヘッドも大きい。加えて、この問題に対する議論もまだ十分ではない。

### 5. 将来の展望

以上、現在のインターネット利用形態とMobile IPのもつ問題点について議論し、Mobile IPの普及を阻害する要因について考えてきた。では、将来的な問題はどうか。以下、今までの議論をふまえてMobile IPの今後について考察する。

#### 5.1 インフラストラクチャに関する展望

現在のユーザが行う移動モデルはインフラストラクチャに起因する問題からオフライン移動であり、これは可搬性のみで十分に移動透過性はあまり求められていないということ述べた。

しかし、将来的には、IP層による移動透過性が十分必要になるシナリオが考えられる。

まず、インターネットの成長に伴い、今後もネットワークへの物理的な接続点が増加していくと考えられる。学校や会社等の建物内への遍在的普及は想像に堅くなく、ネットワークへの接続点を持つ部屋が当然ようになっていくだろう。そして、ネットワークへの接続点が増加すればするほど、移動ノードのIPアドレスの変更の機会は増加する。すなわちオンライン移動を行う機会が増加する。

また、現在でこそ携帯端末が使用できるデータリンクは多くないが、将来的には多種多様なデータリンクが利用できる可能性がある。たとえばIrBusのような赤外線インターフェイスや、IEEE802.11のような無線LANの普及、またIEEE1394やUSBのような新しい有線イ

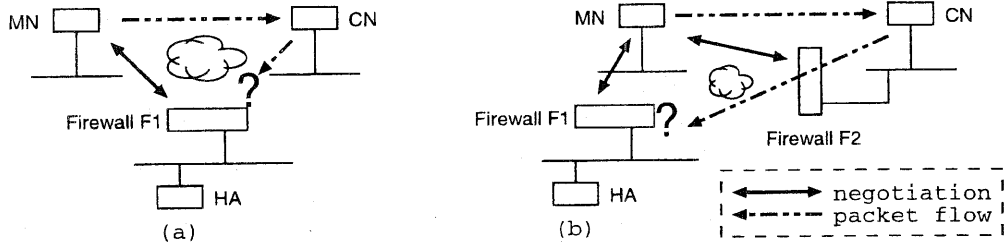


図3 Mobile IPとFirewall: MNからCNにパケットが向かうため、FirewallはMNとCN間の通信を把握することができない

インターフェイスなどである。現在でも北米では地域こそ限定されているものの、広域の無線インターネットアクセスサービス<sup>16)</sup>がすでに実現している。また、さらにインターネット/イントラネットの普及に従って、建物の内外にとらわれず、様々な場所に様々なデータリンクの接続点が遍在する可能性がある。これはすなわちネットワークの移動の機会がますます増加し、それにしたがってIPアドレスが変更される機会も増加するということを示している。ユーザは移動中あるいは移動先のネットワークインフラストラクチャから、速度やコストを意識して、最も適切なものを選ぶ自由を手に入れることになる。この結果、携帯端末は、ある無線から他の無線へ、あるいは、無線から有線へ、有線から無線へというようなデータリンクの変更を行うようになる。

このような状況下においては移動透過性の利点を活用できる。たとえユーザがネットワークを利用して、アクティブなセッションを持っていたとしても、ユーザは自由に最適なデータリンクを利用することができる。たとえば低速な無線LANを利用していましたが、移動先に高速な100Base-TXの接続点が存在した場合、可搬性のみではセッションを中断しなければ100Base-TXのネットワークに移動できないが、移動透過性があれば現在使用中のセッションを無駄にすることなく100Base-TXのネットワークに移動することができ、ユーザの移動の自由度が著しく向上することになる。

### 5.2 アプリケーションに関する展望

現在ユーザが利用できるアプリケーションは移動透過性を必要としないことを述べた。

しかし、現在の携帯端末の性能の向上は目を見張るものがあり、固定ホストに何らひけをとらない端末を持ち歩く人も多い。そして、5.1節で述べたように、今後移動透過性が有効となるインフラストラクチャが普及すると、端末が移動先/移動中にネットワークに接続する時間が長くなると考えられる。このような環境では、移動透過性を利用したアプリケーションの有効性が高まり、今後こういったアプリケーションが開発、使用されるこ

とも想像される。

また、インターネットの利用度が増えるに従い、現在インターネットに接続されていない機器もこれから逐次接続されていくことも考えられる。たとえば移動する車が持つ情報へのアクセスなどが始まると、移動透過性が有効に働くため、これを利用するアプリケーションも増えていくと思われる。

### 5.3 Mobile IPのアーキテクチャが抱える問題に対する展望

現在のMobile IPのアーキテクチャはインターネット利用のモデルと不整合を起こしていることについて述べた。この問題は将来も深刻な問題となると考えられる。Home Addressの問題は、IPv6になれば解決する問題であるが、IPv4では避けることができない問題である。

Home Agentの存在は、移動ノードが通信するために不可欠な存在であるが、インターネットの利用の重要性が高まれば高まるほど通信の堅牢性に対する要求も増大していくことから、通信の堅牢性を下げるHome Agentの存在と三角経路の発生は、将来も問題視されると考えられる。

そして、セキュリティに対する関心も高まっている中、Firewallの存在も将来より重要になっていくだろう。Mobile IPとFirewallの共存は、Home Agentを介する三角経路から複雑な問題となり、多くの議論を呼ぶことになるだろう。

### 5.4 将来の展望のまとめ

将来、移動ノードのオンライン移動の機会は現在よりもより多く起きると考えられる。また、より多くの移動ノードの普及とその性能向上から鑑みるに、移動ノードに対してのアクセス要求もより求められていくかもしれない。ゆえに、移動透過性の必要性はこれから高まる方向にある。

一方、現状のMobile IPは移動透過性を提供するが、Mobile IPが想定している移動モデルとの相違と、その実現メカニズムから、移動透過性を受けるためだけ

に Mobile IP を利用するには 4 節で述べたようなペナルティは大きすぎるものである。

特に Home Agent の存在は、(a) 設置のコストが高く、(b) End-End の通信モデルを破壊し、(c) 三角経路のオーバーヘッドを発生させ、(d) Firewall のある通信モデルと衝突する、という点から現状も将来的にも非常に大きな問題となり、普及を阻害する要因でありつづけ、結果的に Mobile IP は利用されないという将来像を容易に予想させる。

よって、Home Agent のような移動ノードと Fatal share するものを必要としない、End-End で終端可能な IP 層による移動透過性を提供するプロトコルを考案する必要があると考えられる。

また、現在のようなネットワークからの長期の接続断が起きる移動モデルも、将来あり続けると考えられる。たとえネットワークへの接続点が遍在していても、接続 / 通信コストの問題や、携帯端末のバッテリー容量等の問題から、携帯端末が常時接続状態にあるという仮定は難しい。

これは 3.1 節で述べたように、IP 層での移動透過性では問題を解決できない。この問題を解決するにはより上位層での解決が必要である。すなわち、コネクションの切断を意識したアプリケーションや、あるいはそのようなアプリケーションを支援するセッション層の定義である。上位層による移動透過性は、長期の接続断が起きる移動モデルだけでなく、短期の接続断を伴う移動モデルにも適応可能である。しかし、再接続に伴うオーバーヘッドと、既存のアプリケーションの支援という意味からは、IP 層による移動透過性の方がより有効に働く。

最終的には、オンライン移動における移動透過性は IP 層で提供し、オフライン移動での移動透過性はアプリケーション層あるいはセッション層で提供するようにするのが望ましいと考えられる。

## 6. おわりに

本稿では、現状の移動端末の移動モデルとインターネットの利用形態について分析し、Mobile IP が普及しない原因について考察した。

Mobile IP が普及しない原因は、インフラストラクチャの欠如による移動透過性の不必要性と、現在のインターネットの利用形態と Mobile IP のアーキテクチャの不整合にある。インフラストラクチャの欠如は将来的に改善されることが期待されるが、Mobile IP のアーキテクチャに起因する問題点は依然として残る。

よって、我々は移動透過性が必要とされる将来のインターネット利用に向けて、Mobile IP に代わる新たな移

動透過性を提供するプロトコルが必要となると考える。

## 参 考 文 献

- 1) Perkins, C.: IP Mobility Support, RFC 2002 (1996).
- 2) Perkins, C.: IP Encapsulation within IP, RFC 2003 (1996).
- 3) Johnson, D. B. and Perkins, C.: Mobility Support in IPv6, draft-ietf-mobileip-ipv6-06.txt (1998) (Work in progress).
- 4) Teraoka, F., Uehara, K., Sunahara H. and Murai, J.: VIP: a protocol providing host mobility. CACM, Vol. 37, No.8, pp. 67 - 75 (1994).
- 5) Richardson, T., Stafford-Fraser, Q., Wood, K.R. and Hopper, A.: Virtual Network Computing. IEEE Internet Computing, Vol.2 No.1 pp. 33 - 38 (1998).
- 6) Rekhter, Y., Moskowitz, B., Karrenberg, D., Groot G.J., and Lear, E.: Address Allocation for Private Internets, RFC1918 (1996).
- 7) Ferguson, P. and Senie, D.: Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing, RFC2267 (1998).
- 8) Solomon, J.D.: Mobile IP, Prentice Hall, Reading, New Jersey (1998).
- 9) Stevens, W.R.: TCP/IP Illustrated, Volume 1, Addison Wesley, Reading, Massachusetts (1994).
- 10) Montenegro, G. and Gupta, V.: Sun's SKIP Firewall Traversal for Mobile IP, RFC 2356 (1998).
- 11) Montenegro, G.: Reverse Tunneling for Mobile IP, RFC2344 (1998).
- 12) Ishiyama, M., Inoue, A., Fukumoto, A and Okamoto, T.: Design and Implementation of Mobile IP System with Security Consideration, LNCS 1368, pp. 238 - 253 (1998).
- 13) Perkins, C. and Johnson, D.B.: Route Optimization in Mobile IP, draft-ietf-mobileip-optim-07.txt (1997) (Work in progress).
- 14) Thomson, S. and Narten, T.: IPv6 Stateless Address Autoconfiguration RFC1971 (1996).
- 15) Bound J. and Perkins, C.: Dynamic Host Configuration Protocol for IPv6 (DHCPv6), draft-ietf-dhc-dhcpv6-13.txt (1998) (Work in progress).
- 16) Metricom. The Ricochet Wireless Network Overview. <http://www.ricochet.net/ricochet/> (1997).