2005－DSM－39（10）
2005／10／14

# 移動透過アーキテクチャに対応した情報コンセントシステムによるサイト内モビリティ管理手法

西村浩二 †　前田香織 ‡　相原玲二 ‡
† 広島大学情報メディア教育研究センター
‡ 広島市立大学情報処理センター

MIP や LINA、MAT などの移動透過性を実現するプロトコルやアーキテクチャは、高い汎用性やスケーラビリティを実現するため、移動しようとする端末に大幅な変更を要求する。その一方、比較的狭い範囲 (例えばサイト内) での移動透過性を目的とする場合、プロトコルのオーバヘッドや移動端末の改変の必要性が実現の妨げとなる可能性がある。本稿では、対象を単一のポリシで管理可能な中小規模のネットワークに限定し、移動透過性実現のための機能をネットワーク側に持たせることで、既存の端末を用いながら移動透過性を実現する方法について検討を行い、その実現可能性について述べる。

# An Approach to Localized Mobility Management by Information Outlet System with Mobility Support Architecture

Kouji NISHIMURA †,
Kaori MAEDA ‡ and Reiji AIBARA †
† Information Media Center, Hiroshima University
‡ Information Processing Center, Hiroshima City University

The protocols or architectures like MIP, LINA and MAT which provide mobility support in the Internet request the mobile node significant modification to realize its generality and scalability. On the other hand, considering localized mobility, protocol overhead and the necessity of significant modification to mobile node may become an obstacle to deploy. In this paper, we propose an information outlet system which provides mobility support. No modification to mobile node is required by limiting the scalability to local network and shifting the mobility function from mobile node to network.

## 1　はじめに

いつでもどこでもネットワークを利用できる環境を構築するため、無線アクセスポイントを設置し、その周辺で無線端末を利用したネットワークの接続性を提供するサービスが広く行われるようになってきた。

公衆の無線スポットは人が多く集まる場所にスポット的にアクセスポイントが設置され、別の無線スポットと通信エリアが重なることがほとんどないため、それぞれで異なったネットワークアドレスを利用しても不都合が生じることはない。しかし今後さらに整備が進み、アクセスポイントの設置密度が高くなった場合は、隣接する無線スポットの通信エリアが重なり、電波状況によっては隣の無線スポットのアクセスポイントの方が電波強度が強くなる状況が発生することが考えられる。

最近の無線機器には、現在接続中のアクセスポイントよりも電波強度が強いアクセスポイントを発見した場合に自動的に無線レベルでの接続を切り替えるローミング機能があるが、隣接する無線スポットが異なるネットワークアドレスを利用している場合には、再認証やネットワークアドレスが変わることによる通信断を防ぐため、識別子である ESSID(Extended Service Set IDendifier) を異なる値に設定して、ローミングが発生しないようにする。しかし複数の ESSID の利用は、ネットワークの管理が複雑になるだけでなく、移動のたびに利用者に WEP キーなどの設定の追加・変更あるいは確認を強いることになるため、利用者のサポート業務も膨大なものとなる。

一方、異なるネットワークアドレスを持つ無線スポットが隙間なく設置された環境で、無線端末が通信相手との接続を維持したまま移動できる機能を提供する移動透過プロトコル/アーキテクチャの研究や実装が行われている。その代表的なものとして MIPv4 (Mobile IPv4)[1] / MIPv6[2] や、LINA (Location Independent Network Architecture)[3] のほか、筆者らが提案してい

る MAT (Mobile IP with Address Translation)[4] などがあるが、これらはいずれも広域ネットワークにおける利用を想定した汎用性の高いプロトコル/アーキテクチャを目指しているため、移動端末のプロトコルスタックの改変を前提としている。そのため、移動端末の改変の必要性がこれらの方式の普及の妨げとなる可能性がある。

そこで本稿では、移動端末への改変を不要としたまま移動透過性を実現するため、適用対象を大学等のキャンパスネットワークのように単一のポリシの元で管理される範囲 (サイト内) に限定することで、移動透過性を実現するための機能 (モビリティ) をネットワーク側に持たせて管理することを考える。

# 2 サイト内モビリティ管理

## 2.1 現状の問題点

大学等のキャンパス内全体を複数のアクセスポイントでカバーしたい場合、ひとつの L2(Layer 2) ネットワーク上にひとつの L3 ネットワークを構築する方法が考えられる。しかしブロードキャストドメインを広くすると、ブロードキャストパケットやマルチキャストパケットによる輻輳が発生する恐れがある。そのため、適当な範囲でブロードキャストドメインを分割するのが一般的である。

広島大学においても、平成 16 年度末から CUP (Campus Ubiquitous Project) と呼ばれる全学的なプロジェクトが始動した。キャンパス内を広くカバーするようにアクセスポイントを設置し、LAN アクセス管理システム FEREC[5] を併用して利用者認証を行うシステムの構築を全学規模で行うプロジェクトである。前述のような考察から、設計時にはヒアリングを行い、FEREC の性能とエリアごとに予想される利用者数を勘案して、1 台あたりクラス C ひとつを管理するようにし、収容される FEREC ごと (実際には部局ごと) に ESSID も異なるものとした。そのため利用者の密度が高いエリアでは、ひとつのサービスにも関わらず複数の ESSID が同時に見える状態となり、どの ESSID を選択するべきか利用者が迷う場面が見られた。またセキュリティ向上の観点から、 CUP の開始に伴って全学的に設置するアクセスポイントには WEP キーの利用を義務付けることになった。結果、異なる ESSID に接続する際には WEP キーの入力が必要となったことも利用者を混乱させる原因となっている。

これらのことから、ひとつの L2 ネットワーク (ESSID) 上に複数の L3 ネットワークを構築するが、移動端末のアプリケーションからはひとつの L3 ネットワークのように扱えること、つまり利用者に L2,L3 の境界を意識させないことが望ましい。それを実現するには IP レベルでの移動透過性が必要となるが、既存の提案方式を利用するには移動端末のプロトコルスタックの改変が必須であることから、普及やサポートの面で困難が伴うことが予想される。

一方、近年普及しつつある無線 LAN スイッチでは、このような複数の L3 ネットワークの間で、移動端末への改変を強いることなく移動透過性を提供することが可能と謳われている。ただし、その多くが独自の機器やプロトコルに依存しており、マルチベンダ環境での相互運用性がないため、単一ベンダによるネットワーク構築が必須となる制限がある [6]。しかし無線 LAN スイッチが採用される背景には、利用者の端末に変更を加えることなく移動透過性を実現できることへの要求があることは明らかである。

そこで本稿では、移動端末の改変を必要とせず、複数の無線スポット間で共通の ESSID を利用し、無線スポット間でローミングが発生しても接続が維持されるシステムの構築について検討を行う。

## 2.2 関連技術

本稿ではシステムを構築する上での基本技術として、筆者らが以前から研究を行っている 2 つの技術を利用する。

1 つは利用者認証機能付き情報コンセントシステム PortGuard[7] である。PortGuard はネットワークの利用に際して利用者に認証を要求するシステムで、認証の結果によりシステムが稼動するゲートウェイ上のフィルタを操作して、外部ネットワークへの到達性を制御する。ゲートウェイは利用者認証のほか、DHCP(Dynamic Host Configuration Protocol)[8] による携帯端末への自動アドレス設定、1 対 1NAT(Network Address Translator)[9] の機能を持ち、配下の携帯端末に付与したプライベートアドレスとグローバルアドレスとの対応関係の管理と外部ネットワークから配下の携帯端末への到達性を提供する。

もう 1 つはアドレス変換方式による移動透過インターネットアーキテクチャMAT である。MAT 機能を持つ (MAT 対応の) 移動端末 (MN:Mobile Node) は、移動先で付与される一時的なアドレス (MA:Mobile Address)

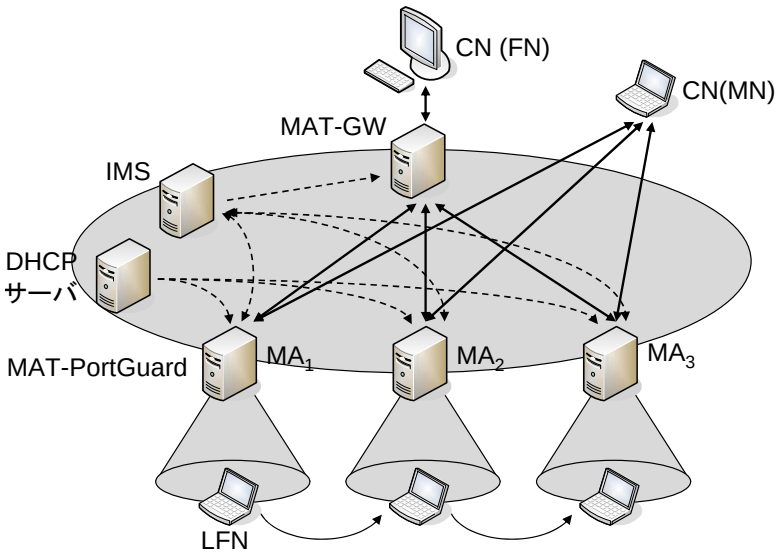


図 1: システム概要図.

と、アプリケーションが通信を行う際に使用する恒久的なアドレス (HA:Home Address) を持つ。MN は移動に伴って MA が変更となるたびに HA との対応表を更新し、移動端末内で HA と MA との間のアドレス変換を行うことで、アプリケーションに対して移動透過な環境を提供する。また、MAT 対応のルータは MR(Mobile Router) と呼ばれる。MN が HA に対応する MA との間の 1 対 1 のアドレス変換を提供していたのに対し、MR は配下のネットワークに対応して多対多のアドレス変換機能を提供する。そのため MAT 機能を持たない端末 (FN:Fixed Node) と一緒に移動することで配下の FN(LFN:Local FN) に対して移動透過性を提供することができる [10]。

本稿では PortGuard を MR として構成し、MR が保持する MA と HA の対応表を複数の PortGuard で共有することで、LFN に対して移動透過性を提供するシステムの構築を考える。つまり、通常 MR は対応表とアドレス変換機能の両方を持ち LFN と共に移動するが、本稿ではアドレス変換機能に相当する PortGuard 自身は移動せず、対応表と LFN のみが共に移動するシステムを構築する。

# 3 システム構成

## 3.1 システム概要

システムの概要を図 1 に示す。本システムでは主に MAT-PortGuard,IMS,MAT-GW の 3 つのサーバが協調して動作することで機能を提供する。以下、それぞれについて説明する。

### 3.1.1 MAT-PortGuard

図 1 において、円錐で示されている部分がひとつの無線スポットを表している。無線スポット内には複数のアクセスポイントがあり、それらの間では L2 レベルの通常のローミングが行われる。それぞれの円錐の頂点部分に位置するサーバが MAT-PortGuard である。MAT-PortGuard では通常の PortGuard としての NAT 機能の他に、MAT 技術に基づいたアドレス変換機能を持つ。

本システムでは、LFN が複数の無線スポット間を渡り歩くことを可能とするため、全無線スポットで同一のアドレス空間を使用する。すなわち、すべての MAT-PortGuard が DHCP で LFN に払い出す IP アドレスをシステム全体で共有し、各 MAT-PortGuard は DHCP リレーサーバのように振舞う。本システムでは LFN に払い出される IP アドレスをポータブルアドレス (PA) と呼び、LFN はどの無線スポットにいても同一の PA を使い続ける。

次に、LFN が無線スポットを移動してもゲートウェイが変わらないように見せかけるため、MAT-PortGuard のローカル側には共通の MAC アドレスと IP アドレスを用いる。MAC アドレスに関しては、複数ある MAT-PortGuard のいずれかの MAC アドレスに合わせるか、ベンダ識別子 (OUI:Organization Unique Identifier) 内

の U/L(Universal/Local) ビットを 1(ローカル管理) にした上で適当に決定する。

#### 3.1.2 IMS

MAT における IMS(IP Address Mapping Server) は、HA と MA の対応表の管理や配送を行うサーバである。MN からの HA をキーとした MA の問い合わせに対して、HA に対応する MA を応答する。MN は MA の存在の有無により CN が MN か FN かを判断して適切な処理を行う。本システムでは情報コンセントシステムとして必要な端末の識別情報、すなわち MAC アドレスと PA、さらに各種フラグ (認証済みフラグや HA 固定フラグなど) を加えた 5 項組

$$(MAC, PA, MA, HA, Flag)$$

で端末を管理する。そこで本システムでは、これらを統合した機能を持つサーバを IMS(Information Mapping Server) と呼び、以後断わりなく IMS と呼ぶ場合は Information Mapping Server を指すものとする。

MAT-PortGuard は配下に LFN が移動してきたことを検知すると、自らが取得した端末情報をキーとして IMS に問い合わせを行って利用の可否を確認し、MAT における移動手順にしたがって自らが管理する MA への更新などを行う。

#### 3.1.3 MAT-GW

前述のように MAT-GW は CN が FN の場合にのみ使用され、MAT-PortGuard から転送されたパケットの送信元アドレス MA を、さらに HA に変換して CN に送信する。一方、CN から見て HA を持つ通信相手のように振舞うことから、MIP におけるホームエージェントと同様の役割を担う。

LFN は複数の MAT-PortGuard 間を移動しても最初に払い出された PA を使い続けることができ、またこの機能により移動によって MA が変化しても HA は変化しないため、FN な CN との通信を継続することができる。

### 3.2 端末の接続と移動

端末はあらかじめ IMS に MAC アドレスと HA の組を登録することで、接続時に常に同じ HA を利用するようにできる。あらかじめ登録していない場合は、その都度空いている HA が割り当てられるため、同じ HA になる保証はない。

端末が MAT-PortGuard の配下に接続されると、新規端末の場合はまず DHCP により PA を取得し、以降アドレス更新時にも同一の PA が割り当てられる。次に利用者は通常の PortGuard の利用方法にしたがって利用者認証手続きを開始する。一方、他の MAT-PortGuard で認証済みの端末の場合は相手端末へのパケットを送信する。ここで MAT-PortGuard は端末の MAC アドレスと PA の組を取得できるので、これをトリガとして IMS に対してそれらをキーとした検索を行って、IMS エントリを取得する。

認証済みフラグが立っている場合は、他の MAT-PortGuard で認証済みであるため、新たに MA を割り当て、IMS エントリの更新を行った後、新しい MA を使って端末に関するパケットを処理する。新規端末の場合は IMS エントリがないか、認証済みフラグが立っていないため、利用者認証を要求し、認証が成功した場合にのみ認証済み端末と同様の処理を行う。

### 3.3 CN との通信

#### 3.3.1 LFN→CN

MAT-PortGuard は LFN から $(PA, CN)$[1]のパケットを受け取ると、通常の NAT 動作によりアプリケーション層を含めて送信元アドレスを HA に書き換える。その後、MAT 動作により送信元アドレスをさらに MA に書き換えて $(MA, CN)$ とする。次に MAT-PortGuard は CN の MA ($MA_{CN}$ と書く) を問い合わせる。$MA_{CN}$ の取得に成功した場合、CN は MN であることがわかるので、MAT-PortGuard はパケットを直接 CN に送信する。一方 $MA_{CN}$ の取得に失敗した場合、CN は FN である。MAT-PortGuard はパケットを LFN の HA を宛先とするパケットでカプセル化 [11] して、$(MA, HA(MA, CN))$ となったパケットを MAT-GW に送信する。MAT-GW では受信したパケットの宛先アドレスに対応する MA を調べ、それが送信元アドレスと一致した場合はカプセル化を解いてパケットを送信する。

[1]パケットの送信元、宛先アドレスを $(src, dst)$ と表記する。また IP-in-IP の場合は $(src, dst(src, dst))$ と表記する。

### 3.3.2 CN→LFN

CN が MN の場合、CN は $(MA_{CN}, MA)$ なるパケットを送信するため、MA を管理する MAT-PortGuard に到達する。CN が FN の場合、CN は $(CN, HA)$ なるパケットを送信するため、MAT-GW に到達する。MAT-GW では、受信パケットの宛先アドレスに対応する MA を調べる。得られる MA は LFN に対応するものなので、送信元アドレスとは一致しない。そこで MAT-GW は宛先アドレスを MA に書き換えて、$(CN, MA)$ となったパケットを MA を管理する MAT-PortGuard に送信する。MAT-PortGuard では、MAT 動作により送信元アドレスが CN に、宛先アドレスが HA に書き換えられる。その後 NAT 動作によりアプリケーション層を含めて宛先アドレスが PA に書き換えられて、LFN に送信される。

# 4 考察

## 4.1 機能に関する考察

以下では、本システムが想定する LFN が MAT 非対応の CN と通信する場合について、文献 [12] に述べられているサイト内モビリティ管理手法が満たすべき要件それぞれについて考察を行う。

**ハンドオーバ時の通信不能時間を短縮すること** 移動透過プロトコル/アーキテクチャの研究では、複数インタフェースを使ったバイキャスティングなどにより通信不能時間をなくすことが検討されているが、実現のためのコストは膨大となる。一方本システムでは移動端末への改変を許していないため、通信不能時間は移動端末が新しいアクセスポイントを発見して切り替えるのに必要な時間と、その後端末がパケットを送信するまでの時間の和となる。端末に keep-alive を行うクライアントプログラムを導入すれば後者の通信不能時間の短縮は図れるが、本システムは移動しながら IP 電話などのリアルタイム通信を利用する用途には適していない。

**ハンドオーバ時のシグナリング (通信) 量が削減できること** 本システムでは、LFN からのパケット送出をトリガにして LFN の移動を検出するため、ハンドオーバに関する特別なプロトコルは不要である。ただし、移動検出を高速化するために前述のクライアントプログラムを導入する場合は、一定間隔で生存確認のパケットが送出されることになる。

**移動端末の位置が隠蔽されていること** 本システムで、LFN は CN との通信に HA あるいは MA を使用する。そのため、CN またはその通信を傍受した第三者は、MAT-GW あるいは MAT-PortGuard の位置は特定することができるが、LFN の位置は特定できない。また、スパイウェアなどにより LFN 内の情報が開示されたとしても、LFN は PA しか持たないため、さらなる位置の特定は困難である。

**無線帯域の効率的な利用ができること** 本システムでの無線区間は LFN と MAT-PortGuard の間を想定しており、その区間においてカプセル化などは行われない。

**シグナリングの範囲が極小化されていること** 本システムでは、移動透過を実現させるためのシグナリングはサイト内、しかも帯域等の通信資源が十分に確保可能な有線区間に閉じている。

**移動端末とネットワークとの間で事前のセキュリティに関する信頼関係の構築を必要としないこと** 本システムでは LFN の識別情報として MAC アドレスを利用しており、事前に MAC アドレスを登録することで、HA を固定的に割り当てることも可能である。したがって事前に特別な信頼関係を構築する必要はないが、MAC アドレスをはじめとする端末の識別情報が完全に詐称された場合には対応できない。これは実現コストと運用コストとのバランスを考慮するという PortGuard の開発コンセプトに基づくものであるが、必要に応じて文献 [13] などの手法を併用することもできる。

**多様な無線技術に対応可能であること** 本システムでは、現在のところ端末の識別情報に MAC アドレスを使用している。MAC アドレスが変わると異なる端末と認識されるため、現在は無線 LAN とその他の無線技術との間で移動することはできない。また有線 LAN との間の移動も同様である。前項に示した手法などを併用し、端末認証を行うことで、 MAC アドレスに依存しないシステムを構築することも可能である。

**移動端末の改変を必要としないこと** 本システムでは移動端末に一切の改変およびクライアントソフトウェアの導入を要求しない。

**IPv4,IPv6 両方に対応可能であること** 本システムは DHCP を RA(Router Advertizement) に置き換えることで、IPv6 にも対応可能である。

### 4.2 セキュリティに関する考察

ここでは、LFN と MAT-PortGuard 間の盗聴および LFN 間の通信の問題と、MAT-PortGuard と IMS 間の認証問題について考察する。

本システムでは PortGuard と同様に、仕様に LFN と MAT-PortGuard 間の通信の暗号化を含めていない。したがって、技術的には LFN と MAT-PortGuard 間の通信は近隣の LFN から盗聴される可能性がある。これは暗号化を必須とすることによる端末の複雑化や運用の煩雑さを防ぐことのほか、通信路の一部をシステム側で暗号化することで利用者が LFN と CN 間で暗号化されていると誤解することを防ぐ狙いがある。盗聴を防止するには LFN と CN 間での暗号化が不可欠であり、ネットワークの機能としてではなく、利用者教育によって解決する必要があると考えている。なお、異なる MAT-PortGuard 配下の LFN は同一のサブネット上にあるが、宛先アドレスに PA を指定して通信することはできない。

次に MAT-PortGuard と IMS 間の認証問題は、事前に共通鍵を生成して互いに登録しておき、通信時にはその鍵で暗号化を行う。MAT-PortGuard も IMS もネットワーク管理者がネットワークサービスとして設置するものなので、登録に関するコストはあらかじめ算定することができる。

## 5 おわりに

本稿では、適用対象を単一のポリシの元で管理されるサイト内に限定することで、移動透過性を実現するための機能をネットワーク側に持たせて管理するシステムを提案し、その機能についての考察を行った。その際、筆者らが研究・開発を行っている MAT 技術と、PortGuard による利用者および携帯端末の管理技術を基本技術として利用し、移動端末に改変を加えることなく移動透過性を実現している。現在、各機能の実装を行っているところである。

本システムでは移動端末への改変を一切行わないことを必須条件としたため、ハンドオーバ時の通信不能時間は無線インタフェースや OS のローミング機能の速度に依存する。しかし、サイト内での移動は距離も限られていることから利用形態が異なっている可能性があり、問題とはならないことも予想される。また移動端末に簡単なクライアントを導入することで、より高速かつ安定した移動が可能であると考えている。今後これらについて調査・検討を行う予定である。


### 謝辞

日頃から PortGuard、MAT に関する議論にご参加いただいている広島大学相原研究室、広島市立大学前田研究室の各位に感謝します。特に広島大学藤田貴大君、梶原大輔君、広島市立大学上浦大智君には MAT や MR の実装者の立場から有益なご意見等をいただきました。本研究の一部は、日本学術振興会科学研究費補助金 (17300019, 17500037) の支援を受けて実施しています。ここに記して謝意を表します。


## 参考文献


[1] C. Perkins: “IP Mobility Support for IPv4”, RFC 3344 (2002).

[2] D. B. Johnson, C. Perkins, J. Arkko: “IP Mobility Support for IPv6”, RFC 3775 (2004).

[3] M. Ishiyama, M. Kunishi, K. Uehara, *et al.*: “LINA: A New Approach to Mobility Support in Wide Area Networks”, IEICE Transaction on Communication, Vol.E84-B, No.8, pp.2076–2086 (2001).

[4] 相原 玲二, 藤田 貴大, 前田 香織, 野村 嘉洋: “アドレス変換方式による移動透過インターネットアーキテクチャ”, 情報処理学会論文誌, Vol.43, No.12, pp.3889–3897 (2002).

[5] FEREC: *http://www.ferec.jp*

[6] J. Kempf, K. Leung, P. Roberts, *et al.*: “Problem Statement for IP Local Mobility”, Internet Draft, IETF, draft-kempf-netlmm-nohost-ps-00.txt (2005). (work in progress)

[7] 西村 浩ニ, 前田 香織, 相原 玲二: “遠隔機器制御プロトコルを用いた有線/無線 LAN 用情報コンセントシステム”, 情報処理学会論文誌, Vol.43, No.2, pp.662–670 (2002).

[8] R. Droms: “Dynamic Host Configuration Protocol”, RFC 2131 (1997).

[9] K. Egevang, P. Francis: “The IP Network Address Translator (NAT)”, RFC 1631 (1994).

[10] 藤田 貴大, 西村 浩二, 相原 玲二: “アドレス変換によるモバイルネットワークとその評価”, インターネットコンファレンス 2004 論文集, pp.29–38 (2004).

[11] W. Simpson: “IP in IP Tunneling”, RFC 1853 (1995).

[12] J. Kempf, K. Leung, P. Roberts, *et al.*: “Requirements and Gap Analysis for IP Local Mobility”, Internet Draft, IETF, draft-kempf-netlmm-nohost-req-00.txt (2005). (work in progress)

[13] 朴 美娘, 馬場 義昌, 岡崎 直宣: “無線 LAN システムにおけるシームレスユーザ認証方式に関する考察”, マルチメディア，分散，協調とモバイル (DICOMO 2005) シンポジウム論文集, pp.97–100 (2005).