■4 群（モバイル・無線）-5 編（モバイル IP，アドホックネットワーク）

1 章 Mobile IP

（執筆者：阪田史郎）［2010 年 5 月 受領］

■概要■

ユビキタスサービスの一環として，いつでも，どこでも，誰とでも同じ環境で通信可能なサービスの実現を目指して，携帯電話のブロードバンド化（第 3 世代携帯電話）や，無線 LAN 技術を用いたサービスが展開されている．現状，第 3 世代携帯電話については，全国展開されており，また，広帯域なデータ通信が可能な無線 LAN についても，家庭やオフィス・店舗などへの普及に加えて IEEE 802.11 b/a/g を用いた駅や喫茶店などで利用できるようになっている．

また，高速有線アクセス手段としては，現在 ADSL に加え光によるサービスが本格化し始めており，今後これら無線・有線の高速アクセス手段を場所や環境に応じ自由に使い分けることが可能なサービスの登場が望まれている．

一方，これら複数のアクセス網を利用しつつ，IP サービスの継続性を保障可能な IP モビリティ技術が注目を浴びている．多メディアのアクセス網間のシームレスな移動を実現することで，適材適所なアクセス手段を利用することが可能となり，ユーザの利便性が格段に向上するからである．本モビリティ提供には，アクセス手段によらず，ユーザアプリケーションに影響を与えずに実現可能である，IP レベルにおけるモビリティによる実現が有効と考えられ，実現プロトコルとして現在 IETF（Internet Engineering Task Force）にて Mobile IP が検討されている．

一般に，インターネットにおいては，IP を用いてパケットのやり取りが行われている．この際，端末にはそれぞれ IP アドレスが振られており，IP アドレスによって，端末の属するネットワークにパケットが配送される．

IP アドレスは，端末が属するサブネットによって変更されるものである．そのため，端末はあるサブネットから，別のサブネットに移ると IP アドレスを変更しなければならず，以前の IP アドレス宛てに送られてきたパケットは，端末には届かないことになる．

Mobile IP は，同じ IP アドレス宛てで，移動した端末へパケットを配送する技術であり，TCP セッションなどを維持することを可能とする技術である．

【本章の構成】

本章では，Mobile IP の概要（動作概要と用語）（1-1 節），Mobile IP の標準化（1-2 節），Mobile IPv4 の基本動作ならびに拡張機能（1-3 節），Mobile IPv6 の基本動作ならびに拡張機能（1-4 節）について述べる．

■4 群 － 5 編 － 1 章

1-1 Mobile IP とは

（執筆者：大西浩行）［2009 年 5 月 受領］

詳細については，以降の節で述べるが，Mobile IP は，移動端末（Mobile Node：MN）がホーム網（MN が本来，属するネットワーク）で用いる IP アドレス（ホームアドレス）と，在圏網（MN の移動先ネットワーク）で用いる IP アドレス（気付けアドレス）を，専用エージェント（Home Agent：HA）に通知することで，在圏先の端末へのパケット着信を可能とする技術である．

図 1･1 に Mobile IPv4 の動作概要を示す．

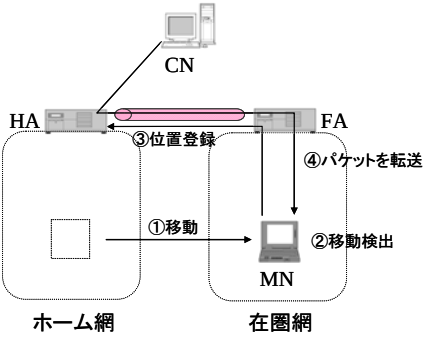

図 1・1 Mobile IPv4 の動作概要

●Mobile IP で用いられる用語

Mobile IP で用いられる代表的な用語を下記に示す．

- **Mobile Node（MN）**：あるネットワーク，あるいはサブネットワークからもう一方のネットワークへ接続点を変えるホスト，あるいはルータ．MN は IP アドレスを変えないでその位置を変更することが可能である．
- **Home Agent（HA）**：MN のホーム網上のルータで，MN がホーム網から離れたとき，MN へ配送するデータグラムのトンネル転送を行う．また，MN の現在の位置情報を保存する．
- **Foreign Agent（FA）**：登録されている MN へ，ルーチングサービスを提供する MN の訪問先ネットワーク上のルータ．FA は MN 宛ての HA からのトンネルをデカプセル化し，MN へデータを転送する．MN から送られたデータグラムについては，登録された MN のデフォルトルータとして動作する．Mobile IPv6 の場合は不要．
- **ホーム網**（Home Network）：実際に，MN のホームアドレスと同じネットワークプレフィックスを有するネットワーク（仮想的なネットワークも可能）．
- **在圏網**（Foreign Network）：MN のホームネットワークとは別のネットワーク．
- **ホームアドレス**（Home Address）：MN に，長期にわたり割り当てられる IP アドレス．端末がインターネットに接続されている場所にかかわらず不変．

・**気付けアドレス**（Care-of Address）：ホームから離れている間，MN へ向かうデータグラム転送のための，トンネルの終端．FA 気付けアドレスと，共存気付けアドレスがある．
・**Correspondent Node（CN）**：MN が通信する相手．通信端末は移動であっても固定であってもよい．

■4 群 － 5 編 － 1 章

1-2 Mobile IP の標準化

（執筆者：大西浩行）［2009 年 5 月 受領］

IP モビリティ技術である，Mobile IPv4，Mobile IPv6，Network Mobility（NEMO）は，Internet Engineering Task Force（IETF）にて検討が行われている．IETF は，TCP/IP などのインターネットで利用される技術を標準化する組織であり，検討対象技術ごとに七つの Area に分かれており，各エリア内に更に検討対象を絞り込んだ Working Group（WG）が複数ずつ存在する．一般的に IETF における仕様は，各 WG において，仕様の草稿の段階のもの（Internet-Draft（I-D）と呼ばれる），をベースに議論が行われ（I-D のバージョンは更新されるたびに，数字が増えていく），WG の承認が得られたあと，IESG（Internet Engineering Steering Group：WG から提出された仕様を審査する機関）のレビューを得るなどを経て，仕様として Fix されたもの（RFC：Request For Comments）が制定される．

Mobile IP は，1992 年に，IP Routing for Wireless/Mobile Hosts（mobileip）WG において議論が開始された．以来，2003 年までの間，本 WG にて Mobile IPv4，Mobile IPv6，及びハンドオーバ機能の検討が行われてきたが，2003 年 7 月のウィーン会合にて，Mobility for IPv4（mip4）WG，Mobility for IPv6（mip6）WG 及び MIPv6 Signaling and Handoff Optimization（mipshop）WG の三つの WG に分割され，それぞれテーマに関連した課題を取り扱うこととなった．一方，Network Mobility（NEMO）については，2002 年から IETF の Network Mobility（nemo）WG において議論が開始された．本 WG は WG が立ち上がる時期に，既に Cisco 社から IPv4 をベースとした NEMO 機能を具備した製品が市場に出ていたため，IPv4 は既に技術が確立しているとし，IPv6 向けの検討が行われていた．

その後，mip6 WG と nemo WG は，Mobility EXTensions for IPv6（mext）に統合され今にいたる．**表 1･1** に，Mobile IPv4，Mobile IPv6 において RFC 化されているドキュメントのうち代表的なものを列挙する．

Proxy Mobile IPv6 は，2006 年 1 月に設立された Network-based Localized Mobility Management（NETLMM）WG にて検討が行われている．設立の背景は，端末主導型のモビリティ制御技術である Mobile IPv6 に対して，ネットワークインテリジェンスに基づく，IP ベース・ネットワーク型移動制御技術への要求の高まりである．設立当初，NETLMM WG は要求条件を満足する，シンプルで柔軟性の高いプロトコルの策定を目指した．検討開始当初，WG より委任されたプロトコルデザインチームが基礎検討を行い，NETLMM プロトコルの仕様化を進めた．この検討と平行して，NETLMM WG では Mobile IPv6 との親和性の向上に関する議論が高まった．この流れを受け，2006 年 11 月のサンディエゴ会合において，NETLMM プロトコルのコンセプト・機能を継承しつつ，土台となるプロトコルを Mobile IPv6 へと変更する，Proxy Mobile IPv6 の検討が開始された．

2009 年 1 月現在，Proxy Mobile IPv6 のプロトコルは IETF で承認され，IPv4 への対応をはじめとする，各種拡張の議論が継続して検討されている．また，移動通信ネットワークの国際標準化団体である，3GPP，3GPP2，及び WiMAX Forum において Proxy Mobile IPv6 の採用が決定しており，今後は商用ネットワークにおいて普及することが期待される．

表 1・1　Mobile IPv4，Mobile IPv6 の主な RFC

	Mobile IPv4	Mobile IPv6
基本動作	IP Mobility Support for IPv4(RFC3344)	Mobility Support in IPv6 (RFC 3775)
リバーストンネリング	Reverse Tunneling for Mobile IP, revised（RFC3024)	RFC3775でサポート
ハンドオーバ	Low-Latency Handoffs in Mobile IPv4 (RFC 4881)	Fast Handovers for Mobile IPv6 (RFC 4068)
階層化Mobile IP	Mobile IPv4 Regional Registration (RFC 4857)	Hierarchical Mobile IPv6 mobility management (HMIPv6) (RFC 4140)
NAT対応	Mobile IP Traversal of Network Address Translation (NAT) Devices(RFC3519)	ー
動的HA選択	Mobile IPv4 Dynamic Home Agent Assignment (RFC 4433)	RFC3775でサポート
セキュリティに関する拡張	・Authentication, Authorization, and Accounting (AAA) Registration Keys for Mobile IPv4 (RFC 3957) ・Mobile IPv4 Challenge/Response Extensions (Revised) (RFC 4721)	・Authentication Protocol for Mobile IPv6 (RFC 4285) ・Mobile Node Identifier Option for Mobile IPv6 (MIPv6) (RFC 4283)
経路最適化に関する拡張	ー	Enhanced Route Optimization for Mobile IPv6 (RFC 4866)
ネットワークモビリティ	ー	Network Mobility (NEMO) Basic Support Protocol (RFC 3963)

■4 群 － 5 編 － 1 章

1-3 Mobile IPv4

（執筆者：大西浩行）［2009 年 5 月 受領］

1-3-1 Mobile IPv4 の基本動作

Mobile IPv4 は RFC 3344 IP Mobility Support for IPv4 において規定され，大きく，Agent Discovery 機能（移動検出機能），位置登録機能，パケット転送機能の三つを提供する．

以下，Mobile IPv4 の動作について，MN がホーム網にいる場合，在圏先に移動した場合について説明する．

●ホーム網に MN がいる場合

MN がホーム網（MN が本来所属するネットワーク）にいる際の動作は，通常の IP 通信の動作と一緒である．以下動作について概要を示す．

（Agent Discovery）

① モビリティーエージェント（FA もしくは HA）は Agent Advertisement（エリア情報を広告するメッセージ）を通知する．

② MN は Agent Advertisement を受け取り，それがホーム網（MN が本来存在するネットワーク）上であるか，在圏網（MN の移動先ネットワーク）上であるかを検出する．検出は，自身のもつホームアドレスと，Agent Advertisement に含まれるネットワーク情報が同一の場合はホーム網，異なる場合は在圏網と判断する．なおこの際，MN は，定期的な Agent Advertisement 受信を待たずに，Agent Solicitation メッセージを用い Agent Advertisement を要請することも可能である．

（位置登録）

③ 他網からホーム網へ戻ってきた場合には，MN は Registration Request メッセージと Registration Reply メッセージのやり取りを行い，HA へ登録されている MN の位置登録情報を削除する．

（パケット送受信）

・通常の IP ルーチングを行う．

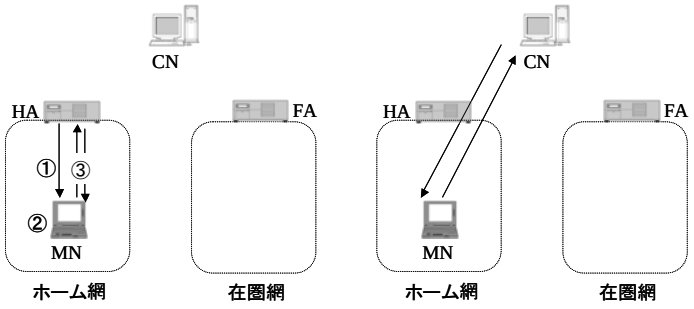

図 1・2　ホーム網における動作概要

●在圏網へ MN が移動した場合

MN が移動した場合，MN は位置検出後，HA に対して位置登録を実施する．以下動作について概要を示す．

（移動検出）

① モビリティーエージェント（FA もしくは HA）は Agent Advertisement を広告する．

② MN は Agent Advertisement を受け取り，それがホーム網上であるか，在圏網上であるかを検出する（この際，MN は，定期的な Agent Advertisement 受信を待たずに，Agent Solicitation メッセージを用い Agent Advertisement を要請することも可能である）．

（位置登録）

③ MN は在圏網へ移動したことを検知した後，在圏網上で気付けアドレス（Care-of Address）を生成．気付けアドレスは FA の Advertisement から取得（Foreign Agent Care-of Address：FA 気付けアドレス），もしくは DHCP のような割当メカニズムによって取得する（Co-located Care-of Address：共存気付けアドレス）方法がある．

④ MN は，Registration Request メッセージ，Registration Reply メッセージを HA とやり取りし，新しい気付けアドレスを HA に登録を行う．この際，HA には，ホームアドレスと気付けアドレスの対応付けが，生成／更新される．

（パケット送受信）

⑤ MN のホームアドレスへ送られたパケットは HA によってインターセプト（後述）され，HA によって MN の Care-of Address へトンネリング転送される．

⑥ MN によって送られるパケットは HA を通過する必要がなければ（1-3-2 項，リバーストンネル参照），直接 CN に対してパケットが送信される．

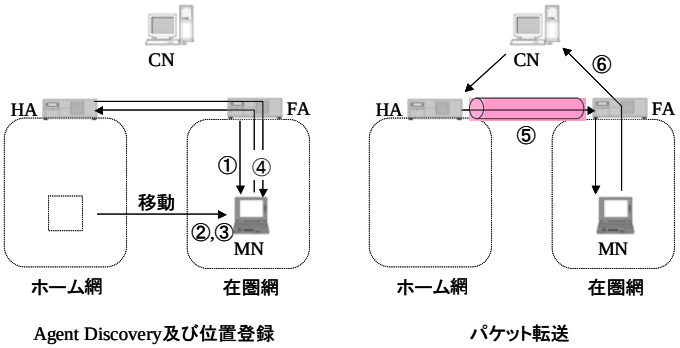

図 1・3　在圏網における動作概要

以下，Agent Discovery 機能，位置登録機能，パケット転送機能のそれぞれについて説明する．

(1)　Agent Discovery 機能（移動検出機能）

Agent Discovery は MN が現在つながっているネットワークがホーム網か在圏網か判断するための手段である．エリア情報は，Agent Advertisement によって定期的に広告されるが，任意のタイミングで Agent Advertisement 受信を促すための方法として Agent Solicitation があ

る（HA/FA は，Agent Solicitation を受信すると，Agent Advertisement を送信する）．

移動検出後，MN は気付けアドレス生成を実施するが，Mobile IPv4 では気付けアドレスの取得方法として，二つのモードがある．

(a) FA 気付けアドレス

Agent Advertisement メッセージによって，FA により提供される，気付けアドレス．この場合，気付けアドレスは FA の IP アドレスになる．このモードでは，FA がトンネルの終端であり，トンネルされたパケットを受信，デカプセル化後，MN へ配送する．このモードの利点は，多くの MN で，同じ気付けアドレスが共用可能であり，限りある IPv4 アドレスを有効利用可能な点である．

(b) 共存気付けアドレス

MN 自身のネットワークインタフェースの一つに，何らかの外的手段によって振られる，在圏網におけるアドレスである．共存気付けアドレスを用いる場合，MN がトンネルの終端点になり，MN 自らデカプセル化処理を行う．

共存気付けアドレスを用いた場合，FA を用いる必要がないという利点がある（例えば，FA をまだ展開していないネットワーク上でも，移動のサポートが可能である）．

しかしながら，MN が移動する可能性のあるすべての網において，アドレスをプールする必要があり，アドレスの有効利用は難しい．

(2) 位置登録機能

Mobile IP には 2 種類に登録方法がある．FA を経由で HA へ位置登録を行う方法と，直接 HA へ位置登録を行う方法である．いずれかの方法をとるか，下記に条件を示す．なお，これら位置登録メッセージは，予め MN，FA，HA が有しているセキュリティ情報に基づき認証される（セキュリティ情報の配布方法については本 RFC のスコープ外）．

- HA へ FA 経由で位置登録
  - MN が FA 気付けアドレスを用いている場合
- HA へ直接位置登録
  - MN が共存気付けアドレスを用いている場合
  - MN がホーム網に戻ってきた場合

下記に FA 経由で HA に位置登録を行う方法と直接 HA に位置登録を行う方法について示す．

(a) HA へ FA 経由で位置登録（図 1･4）

a) MN は FA へ Registration Request を送信．

b) FA は Registration Request を処理し，その後，HA へ中継する．

c) HA は登録成功，もしくは登録拒否の旨を示した，Registration Reply を FA へ送信．

d) FA は Registration Reply を処理し，MN に Registration Reply を中継する．

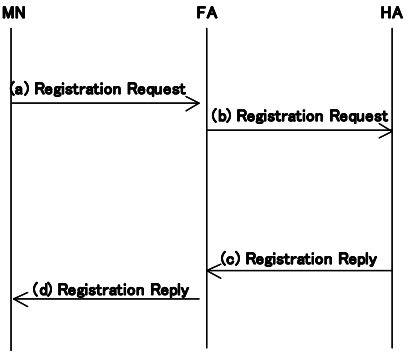

図 1・4　FA 経由での位置登録概要

(b)　HA へ直接位置登録（**図 1･5**）

a) MN は HA へ Registration Request を送信.

b) HA は登録成功，もしくは登録拒否の旨を示した，Registration Reply を MN へ送信.

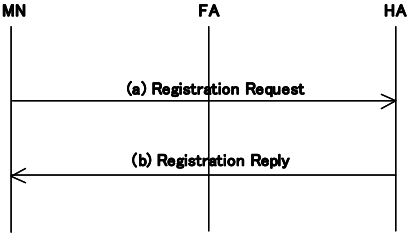

図 1・5　HA への直接位置登録概要

(3)　パケット転送機能

(a)　HA における MN 向けパケットのインターセプト方法

HA は，proxy ARP，gratuitous ARP を用い，位置登録のあった MN 宛てのパケットのインターセプトを行う.

- **Proxy ARP**：ARP Request に答えることが不可能，もしくは，答えようとしないかのどちらかであるノードに代わって，別のノードが送信する ARP Reply.
- **Gratuitous ARP**：他のノードの保持している ARP キャッシュ中のあるエントリを，同時に更新させるため，あるノードによって送信される ARP パケット.

以下に動作概要を示す.

MN が在圏網に移動した場合：

1) MN が，在圏網に移動したことを検知.

2) Registration Request を送信.

3) HA は，Registration Request 受信後，Registration Request が正しい場合，MN に代わって gratuitous ARP を実行し，また MN 宛ての ARP Request に対しては proxy ARP の送信を行う．ただし，HA において Registration Request が拒否された場合，HA では ARP の処理（gratuitous ARP 及び proxy ARP）は実行されない．

MN がホーム網に戻ってきた場合：

1) MN は，ホーム網に戻ってきたことを検知．
2) MN 自身が gratuitous ARP を送信．
3) MN の HA が Registration Request 受信後，Registration Request が正しい場合，MN 宛ての ARP Request に対する proxy ARP 送信処理を無効にする．ただし HA において Registration Request が拒否された場合，HA では ARP の処理（gratuitous ARP 及び proxy ARP）は実行されない．

(b) 転送方法

本節では，HA から気付けアドレスまでの転送時に用いられる，カプセル化方式について示す．

●IP in IP カプセル化

IP in IP カプセルの方法について**図 1･6** に概略図を示す．

外側の IP ヘッダの，送信元アドレスには HA のアドレスが，受信先アドレスには，気付けアドレスが設定される．外側の IP ヘッダに付ける IP オプションがない場合，20 バイトの増加になる．

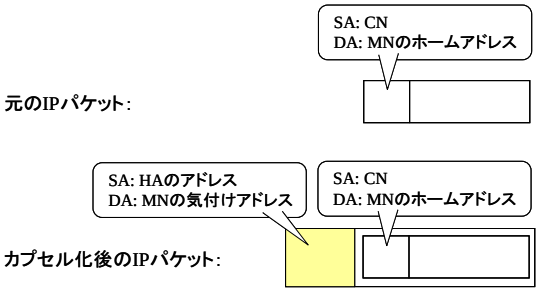

図 1・6 IP in IP カプセル化概要

1-3-2 リバーストンネリング

リバーストンネリング機能は，RFC 3024 で規定される機能である．Mobile IPv4 では，前節で示した様に，MN からのパケットは，ホームアドレスを送信元アドレスに設定し，通信相手端末に転送される．この送信元アドレスは，本来本ネットワーク発のアドレスには付与されるものではないため，ルータなどがフィルタリングを実施している場合，該当パケットを誤ったパケットであると判断し廃棄される恐れがある（**図 1･7** 参照）．

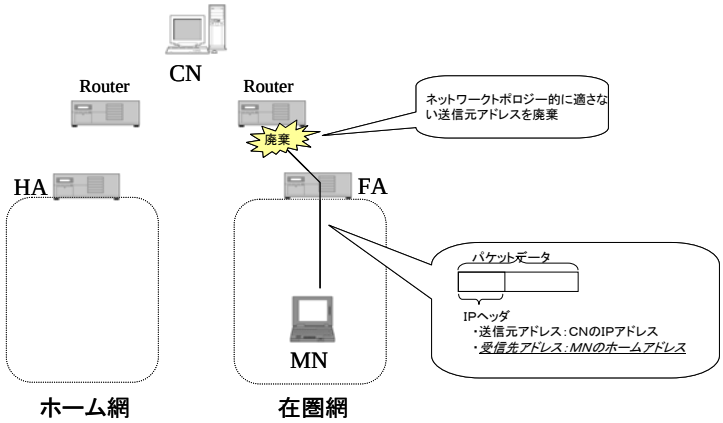

図 1・7　リバーストンネリングを用いない場合の問題点

リバーストンネリング機能は，これを回避するために，MN からのパケットに対して図 1・8 のように MN と HA の間でカプセリングする機能である．カプセリングすることにより，送信元アドレスは，MN の気付けアドレスになり，またホームアドレスを送信元アドレスとしてパケットが HA から送信されるが，トポロジー的に適正であるため，フィルタリングを実施しているルータが存在した場合にも問題なくパケットの送信が可能となる（**図 1・8**）

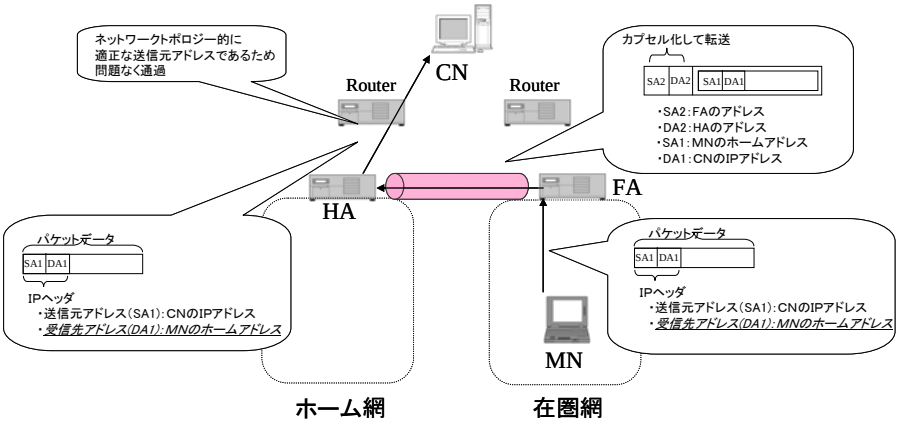

図 1・8　リバーストンネリングによる転送

リバーストンネリングの方法は，前述のように，MN から FA までカプセリング化せずに転送する Direct Delivery Style と，MN から FA までカプセリング化する Encapsulating Delivery Style の二つがある．**図 1・9** に両方の形態を示す．

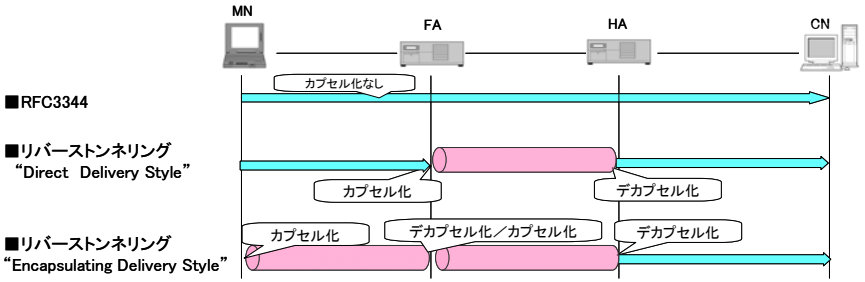

図 1・9　Mobile IPv4 の基本動作（RFC 3344）並びにリバーストンネリング機能の比較

1-3-3 ハンドオーバ

Mobile IP の基本機能（RFC 3344）により MN の移動は可能であるが，更にハンドオーバ（通信中の移動）中におけるパケットの送受信の途切れる時間を軽減する方法として，RFC 4881（Low-Latency Handoffs in Mobile IPv4）が規定されている．本 RFC では，従来 RFC 3344 では，Agent Advertisement によって移動検知を実施していたが，これらは IP レイヤ（Layer 3）におけるメッセージのため，移動検知が遅れるとし，Layer 2 における移動検知をトリガとして動作することを特徴としている．本 RFC 4881 には，大きく以下の二つの方法が規定されている．MN が位置登録を実施するタイミングとして，移動前か移動後かで，二つの方法が規定されている．

・PRE-REGISTRATION Handoff Method
・POST-REGISTRATION Handoff Method

それぞれについて以降に説明する．

(1) PRE-REGISTRATION Handoff Method

本方式は，MN が移動する前に，新しい FA 経由で HA に対して位置登録を実施する方法である．具体的な動作について，**図 1・10** を用いて示す．

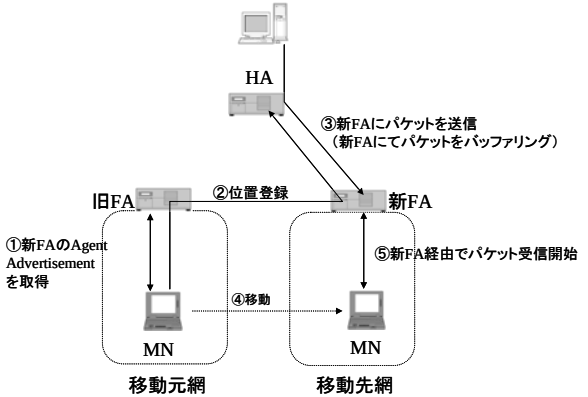

図 1・10　PRE-REGISTRATION Handoff Method の動作概要

① 端末は移動を layer 2 レベルで移動を検知すると，移動先である新 FA の Agent Advertisement を要求/受信.
② 新 FA 経由で，HA に対して位置登録を行う.
③ HA からのパケットは新 FA にフォワードされ，新 FA にてパケットがバッファリングされる.
④ 移動（③と同等のタイミングに発生することも考えられる）.
⑤ 端末は新 FA 配下に移動後，Agent Solicitation を送信．その後，新 FA にてバッファリングされたパケットが端末に送信される.

(2) POST-REGISTRATION Handoff Method

本方式は，MN が移動した後に，HA に対して位置登録を実施する方法である．具体的な動作については，**図 1･11** を用いて説明する.

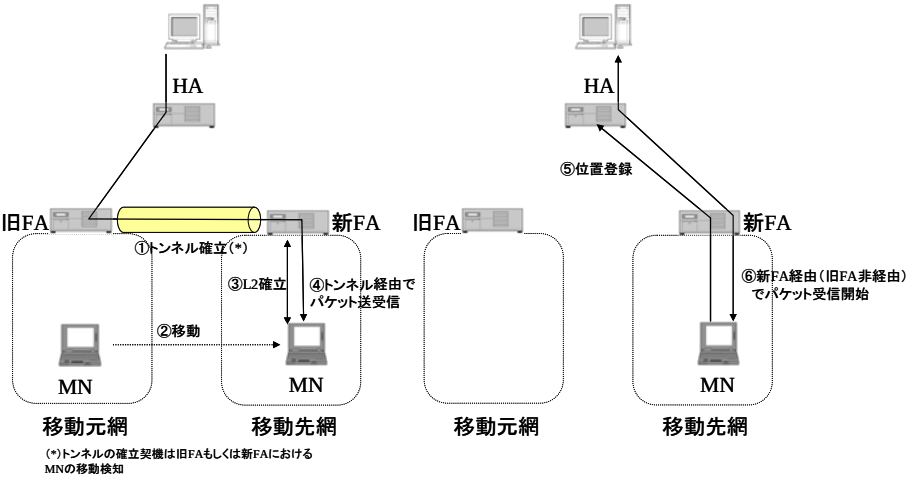

図 1・11 POST-REGISTRATION Handoff Method **の動作概要**

① 旧 FA，もしくは新 FA にて，Layer 2 レベルで MN の移動検知を実施後，旧 FA-新 FA 間でトンネルを確立.
② 移 動.
③ MN が新 FA 配下で Layer 2 のリンクを確立.
④ 旧 FA-新 FA 間のトンネル経由で，パケットを受信開始.
⑤ 新 FA を HA に位置登録.
⑥ 新 FA 経由（旧 FA 非経由）でパケット受信を開始.

1-3-4 階層化 Mobile IPv4

RFC 3344 では，MN が移動した際に，HA に位置登録を実施するが，HA の位置が遠い場合, 位置登録に要する時間が長くなることを問題点として, 階層構造をもつ Mobile IP が RFC 4857

Mobile IPv4 Regional Registration において規定されている．本 RFC において，Gateway Foreign Agent（GFA）と呼ばれる装置が新たに規定されており，HA-GFA-FA の階層構造をとり，FA 間の移動の際には GFA に位置登録を実施，GFA 間の移動の際には HA に位置登録を実施している（**図 1･12**）．

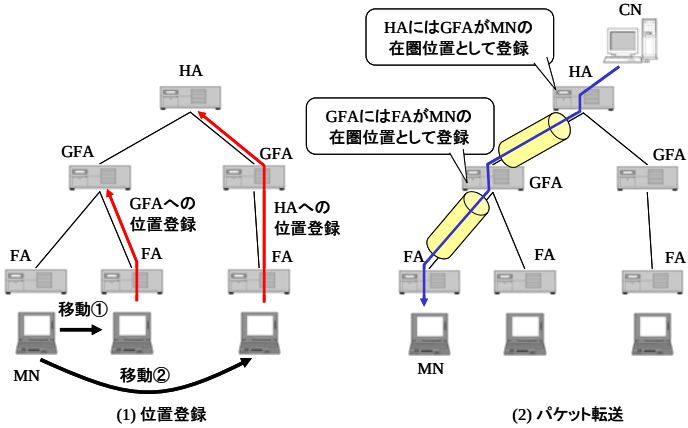

図 1・12　階層化 Mobile IPv4 の動作概要

1-3-5 Mobile IPv4 における NAT 越え

Mobile IPv4 において MN が企業網や，家のネットワークなど，NAT の内側に移動する場合がある．この際，MN には，プライベートアドレスが割り振られるため，その IP アドレスを HA へ登録した場合，MN へパケットを転送することは不可能である（プライベートアドレスに対してルーチングを実施することができないため）．RFC 3519 Mobile IP Traversal of Network Address Translation（NAT）Devices では，このような NAT 配下の MN の動作を実現する方法について規定している．

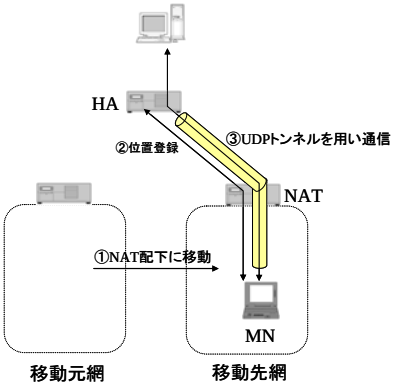

図 1・13　Mobile IPv4 における NAT 越えの動作概要

なお，本 RFC では，NAT が Mobile IP プロトコルが用いる UDP ポート番号（434）の通過を許容すること，MN が共存気付けアドレスで動作することを前提としている．

具体的な動作については，**図 1･13** を用いて説明する．

① MN が NAT 配下に移動.

② HA に位置登録．この際，HA は，位置登録メッセージ中に含まれるアドレス（プライベートアドレス）と，位置登録メッセージの送信元アドレス（グローバルアドレス）が異なることから，MN が NAT の配下にいることを検知.

③ MN と HA は，UDP トンネリングにより，パケットの送受信を実施（パケット転送においても，Mobile IP の位置登録メッセージと同じ UDP ポート番号（434）を用いることで，新たに NAT において穴あけをすることを不要としている）．また，NAT におけるマッピング（グローバルアドレス⇔プライベートアドレス）が消失しないよう，MN-HA 間で定期的にキープアライブのパケットを以降送信する．

1-3-6 動的 HA 選択

Mobile IP において HA は，位置登録情報を扱う重要なノードであると同時に，転送時に必ず通るノードである．そこで，負荷分散並びに，MN に近い位置の HA を割り当てるという観点から，動的に HA を割り当てる仕様が，RFC 4433 Mobile IPv4 Dynamic Home Agent Assignment において規定されている．具体的な動作について，**図 1･14** を用いて説明する．

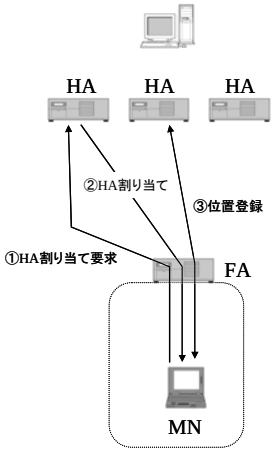

図 1・14　動的 HA 選択の動作概要

① MN が Requested HA（HA の割当を実施する HA）に対して割当要求を送信（本メッセージは基本的には，通常の位置登録と同一であるが，HA のアドレスが，ALL-ZERO-ONE-ADDR（255.255.255.255，もしくは，0.0.0.0）になっている）.

② Requested HA が Assigned HA（割り当てた HA）のアドレスを返信.

③ MN は，Assigned HA に対して位置登録を実施.

1-3-7 セキュリティに関する拡張

Mobile IPv4 における位置登録方法において，認証の方法の拡張方法が規定されている．リプレイアタックなどの攻撃に対する強化のために MN-FA 間のメッセージのやり取りに乱数値を用いる認証方法として，RFC 4721 Mobile IPv4 Challenge/Response Extensions（Revised）が規定されている．また，AAA を用いた認証を可能とする方法について，RFC 3957 Authentication, Authorization, and Accounting（AAA）Registration Keys for Mobile IPv4 で規定されている．以下，RFC 4721 の概要について，**図 1･15** を用い動作概要について説明する．

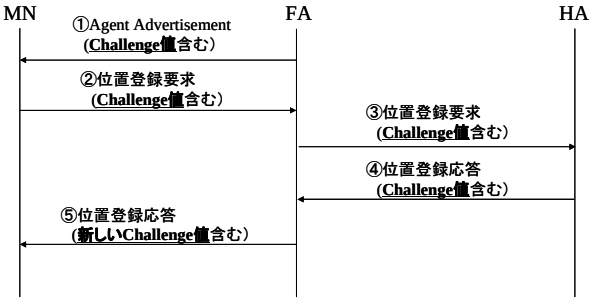

図 1・15　RFC 4721 の動作概要

① FA から Agent Advertisement の中に乱数値（Challenge 値）を入れて広告する．
② MN は位置登録時，上記 Challenge 値をメッセージ中に含め送信する．この際，FA は①で広告したものと同一の Challenge 値であるかのチェックを実施する．
③ FA は，HA に位置登録をフォワード．その後，HA にて位置登録．
④ HA は，位置登録応答を FA に送信．
⑤ FA は，位置登録応答を，新しい Challenge 値と共に MN に送信．

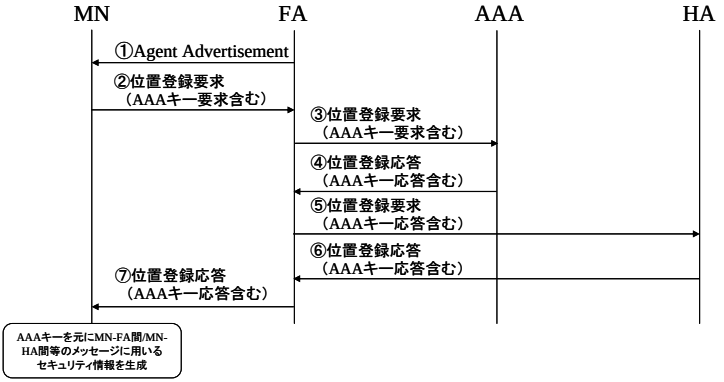

図 1・16　RFC 3957 の動作概要

以下，RFC 3957 の概要について，**図 1･16** を用い動作概要について説明する．AAA を用いた認証では，本来 MN が，FA や HA とメッセージの交換をする際に必要なセキュリティ情

報をどのように MN 側に配布するかを規定している（FA や HA への配布方法は本 RFC 外）．大まかな動作としては，MN が AAA に FA や HA と共有するセキュリティ情報の元となる情報（AAA キー）の要求を行い，MN は AAA から受け取った AAA キー情報を元に，FA や HA と共有するセキュリティ情報を生成する仕組みとなっている．

① MN が FA より Agent Advertisement を受信．
② MN が AAA キー要求を含む位置登録を送信．
③ FA は，AAA に対して位置登録要求を送信．
④ AAA により AAA キーが割り振られ，位置登録応答に含まれる．
⑤ FA から HA に対して位置登録要求を送信．
⑥ HA が FA に対して位置登録応答を送信．
⑦ MN に対して位置登録応答を送信．MN を位置登録応答に含まれる AAA キーを元に，FA や HA との共有するセキュリティ情報を生成．

■4群 － 5編 － 1章

1-4 Mobile IPv6

1-4-1 Mobile IPv6の基本動作

（執筆者：大西浩行）［2009年5月 受領］

Mobile IPv6の基本的な動作は，Mobile IPv4に似ているが，1-4-2項で後述するようにいくつかの違いがある．Mobile IPv6はMobile IPv4と同じく，移動検出方法，位置登録機能，パケット転送機能を提供する．以下，Mobile IPv6の動作について，MNがホーム網にいる場合，在圏先に移動した場合について説明する．なお，Mobile IPv6は，RFC 3775 Mobility Support in IPv6にて規定されている．

＃Mobile IPv4における位置登録要求/応答は，Registration Request/Registration Replyであったが，Mobile IPv6では，ホームアドレスと気付けアドレスを括り付ける情報（Binding Cache）を更新する意として Binding Update/Binding Acknowledgement と名前が変わっている．

●ホーム網にMNがいる場合

MNがホーム網（MNが本来所属するネットワーク）にいる際の動作は，通常のIP通信の動作と一緒である．以下動作について概要を示す（**図1･17**）．

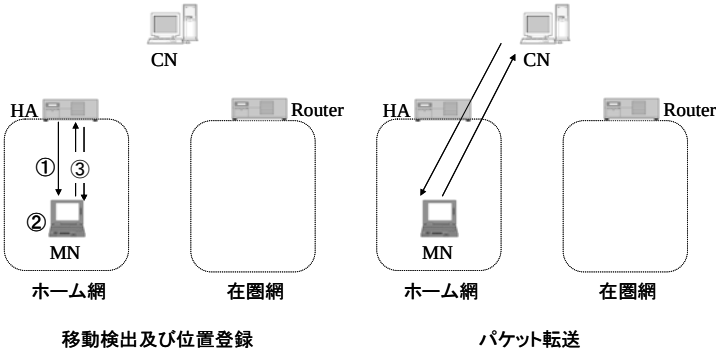

図1･17　ホーム網における動作概要

（移動検出）

① ルータは周期的にRouter Advertisement（ルータ広告）を送信．

② MNはRouter Advertisementを受け取り，ホーム網（MNが本来存在するネットワーク）上であるか，在圏網（MNの移動先ネットワーク）上であるかを検出する．検出は，自身のもつホームアドレスと，Router Advertisementに含まれるネットワーク情報が同一の場合，ホーム網，異なる場合在圏網と判断する．なお，この際，MNは，定期的なRouter Advertisement受信を待たずに，Router Solicitationメッセージを用いRouter Advertisementを要請することも可能である．

（位置登録）

③ 他網からホーム網へ戻ってきた場合には，MNはBinding Updateメッセージと Binding Acknowledgementメッセージのやり取りを行い，HAへ登録されているMNの位置登録情報を削除する．

（パケット送受信）

・通常の IP ルーチングを行う．

●在圏網へ MN が移動した場合

MN が移動した場合，MN は位置検出後，HA に対して位置登録を実施する．以下動作について概要を示す（**図 1･18**）．

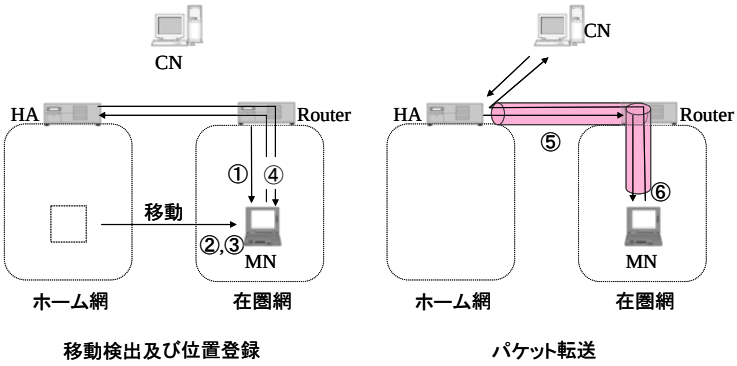

図 1・18　在圏網における動作概要

（移動検出）

① ルータは周期的に Router Advertisement（ルータ広告）を送信．

② MN は Router Advertisement を受け取り，ホーム網上であるか，在圏網上であるかを検出する（この際, MN は, 定期的な Router Advertisement 受信を待たずに, Router Solicitation メッセージを用い Router Advertisement を要請することも可能である）．

（位置登録）

③ MN は在圏網へ移動したことを検知した後，在圏網上で気付けアドレス（Care-of Address）を生成．Mobile IPv6 の場合，気付けアドレス生成は，IPv6 のアドレス生成方法（Router Advertisement のネットワークプレフィックスを用いてアドレスを生成する方法や，DHCP によりアドレスを取得する方法）を流用する．

④ MN は，Binding Update メッセージ，Binding Acknowledgement メッセージを HA とやり取りし，新しい気付けアドレスを HA に登録を行う．この際，HA には，ホームアドレスと気付けアドレスの対応付けが，生成もしくは更新される．

（パケット送受信）

⑤ MN のホームアドレスへ送られたパケットは HA によってインターセプト（後述）され，HA によって MN の care-of address へトンネリング転送される．

⑥ Mobile IPv6 の場合，後に説明する経路最適化が行われない限り，MN から CN 向きのパケットも HA へのトンネル経由で転送される．

Mobile IPv4 の場合，上記 HA 経由でパケット送受信を継続するが，Mobile IPv6 では HA 非経由のパケット送受信を実現するため，経路最適化の手順が規定されている．経路最適化においては，CN に対して MN の現在位置を通知する必要がある．MN が HA に対して位置登録を送信する場合，予め何らかの認証情報を共有しておくことは可能であるが，MN と CN

の場合，CN が不特定多数であるため，そのような事前の共有は難しく異なる手法が必要である．Mobile IPv6 では，MN からの位置登録メッセージを CN で確認するための手段として，Return Routability という方法を規定している．Return Routability は，PKI など，特定のインフラを想定することなく，CN，MN，HA のみで MN の位置登録情報の確認を実現することを目的としている．具体的には，CN が，MN のホームアドレスと気付けアドレスに対して，HA 経由，MN への直接ルートでトークンを払い出し，MN が両方のトークンを含む位置登録を送信してきた場合，そのホームアドレスをもつ MN が，その気付けアドレスに対して移動したと確認する仕組みをとっている．以下，**図 1･19** を用いて動作概要について説明する．

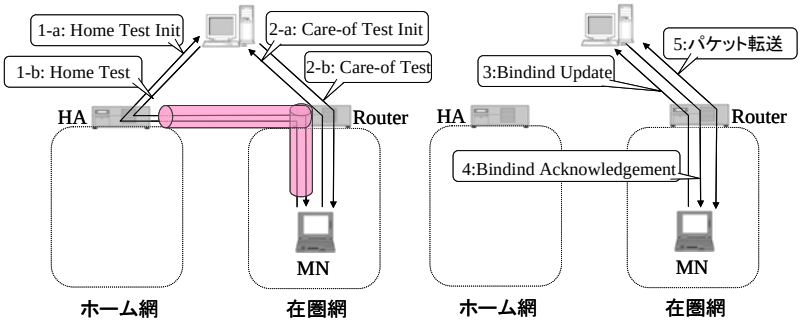

図 1・19　経路最適化の動作概要

①-a　MN は，トンネル経由で CN に対して Home Test Init（ホームアドレスに対してトークン発行を依頼するメッセージ）を送信．

①-b　CN は MN に Home Test を用いてトークンを発行．

②-a　MN は，直接ルートで CN に対して Care-of Test Init（気付けアドレスに対してトークン発行を依頼するメッセージ）を送信．

②-b　CN は，MN に対して Care-of Test を用いてトークンを発行（#Home Test Init と，Care-of Test Init の送出タイミング，Home Test/Care-of Test の受信タイミングは順不同）．

③　MN は，両方のトークンを含む Binding Update を CN に送信．

④　CN は，払い出したトークンと一致するかを確認後，Binding Acknowledgement を送信．

⑤　MN と CN 間で直接ルートによるパケット送受信．なお，本直接ルートによるパケット送受信は，通常の HA 経由での通信とは異なり，ルーチングヘッダを用い通信を行う（詳細については，後述する）．

以下，移動検出方法，位置登録機能，パケット転送機能それぞれについて説明する．

(1)　移動検出機能，位置登録機能

Mobile IPv6 では，通常の IPv6 ルータがサポートする，Router Advertisement/Router Solicitation を用いて移動検出を行う．

Router Advertisement は，一定周期間隔で広告されるが，Router Solicitation により Router Advertisement の送信を MN から促すことも可能である．なお，Mobile IPv6 では，FA が存在しないため，気付けアドレスの生成は，共存気付けアドレスのみになる．また，位置登録方

法についても，HA への直接登録のみとなる．

(2) パケット転送機能

(a) HA における MN 向けパケットのインターセプト方法

HA は，Neighbor Advertisement を用い，周辺ノードに対して MN 宛 IP パケットの送信先を自身（HA）のリンクアドレスに書き換えることで，MN 宛てのパケットのインターセプトを行う．以下に動作概要を示す．

●MN が在圏網に移動した場合

1) MN が，在圏網に移動したことを検知．
2) Binding Update を送信．
3) MN の HA は，Binding Update 受信後，Binding Update が正しい場合，MN に代わって Neighbor Advertisement を実行する．Neighbor Advertisement を受信したノードは，MN のホームアドレス宛のパケットを，HA に対して送信開始．

●MN がホーム網に戻ってきた場合

1) MN は，ホーム網に戻ってきたことを検知．
2) MN は HA に対して Binding Update を実施．
3) MN は Binding Acknowledgement を受信後，Neighbor Advertisement 送信を実施．

(b) 転送方法

Mobile IPv6 では，HA 経由での転送時と，Return Routability 後，直接ルートで通信する際で方式が異なる．以下，それぞれについて示す．

(1) HA 経由での転送

HA⇔MN 区間で IP カプセリングが行われる．**図 1･20** に，CN→HA 区間と，HA→MN 区間におけるパケットの概要を示す．

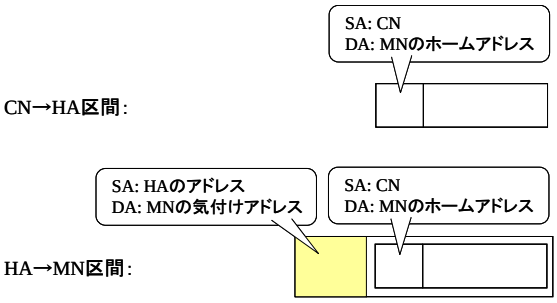

図 1・20 IP カプセリングパケットの概要

(2) 直接ルートでの通信

MN⇔CN 間直接通信を実施する際の方法を以下に示す（**図 1･21**）．MN→CN 方向，CN→MN 方向ともに，ホームアドレスは，オプションヘッダ内に格納し，IP ヘッダ内では MN の気付けアドレスを用いて通信することで，直接ルートでの通信かつ CN/MN 双方で MN の

ホームアドレスを認識可能としている．

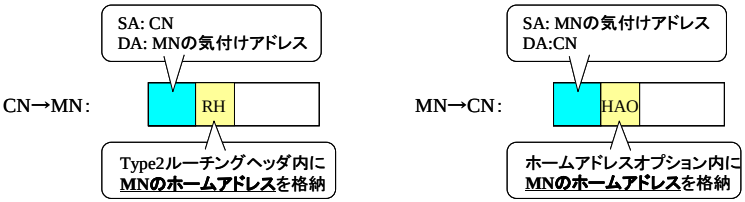

図 1・21　MN⇔CN 間直接通信の概要

●動的 HA 選択について

Mobile IPv6 では，Dynamic Home Agent Address Discovery という HA を動的に発見する手段が用意されている．具体的には，特定のアドレス（Home-Agents anycast address）に Discovery メッセージを送信すると，HA のアドレスが返信される仕組みとなっている．

1-4-2 Mobile IPv4 と Mobile IPv6 の違い

（執筆者：大西浩行）［2009 年 5 月 受領］

前節の説明で既に述べられたところもあるが，以下に，Mobile IPv4 と Mobile IPv6 の主な違いについて示す．

- Mobile IPv4 における FA 相当が不要．
- Mobile IPv6 ではパケット転送の経路最適化機能がサポートされている．
- Mobile IPv6 では，転送の多くのパケットが IPv6 ルーチングヘッダにより転送されるため，すべてのパケットが IP カプセリングを用いる Mobile IPv4 に比べオーバヘッドが少ない．

1-4-3 ハンドオーバ

（執筆者：大西浩行）［2009 年 5 月 受領］

Mobile IPv6 のハンドオーバを実現する技術として，RFC 4068 Fast Handovers for Mobile IPv6 が規定されている．本 RFC では，HA に登録することなしに，旧 AR（移動前のネットワークの Access Router）と，新 AR（移動後のネットワークの Access Router）間で，パケットをフォワードすることにより，ハンドオーバの高速化を実現している．なお，本方式の動作パターンには大きく，移動前に旧 AR-新 AR 間のトンネルを設定する“Predictive”モードと，移動後に旧 AR-新 AR 間のトンネルを設定する“Reactive”モードがある．

図 1・22 を用い“Predictive”モードの動作について説明する．なお，以下シーケンスでは省略しているが，MN から HA への位置登録は独立に実施される．

① 新 AR のプレフィックスを取得．
② 旧 AR に対して，新 AR への転送開始（トンネル設定）を要求．
③ 旧 AR から新 AR に対してトンネルが確立されるとともに，パケットが転送開始．
④ MN が移動．
⑤ 新 AR に対してパケット転送を要求．
⑥ 新 AR にてバッファリングされていたパケットが MN に転送．

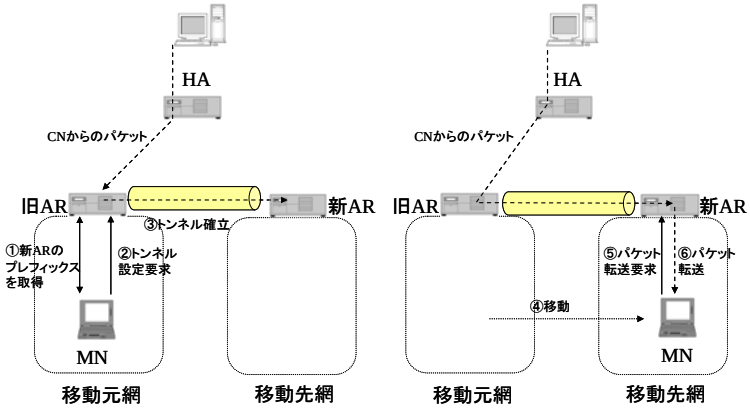

図 1・22　Fast Handovers for Mobile IPv6“Predictive”モード

図 1･23 を用い“Reactive”モードの動作について説明する．なお，以下，シーケンスでは省略しているが，MN から HA への位置登録は独立に実施される．

① 新 AR のプレフィックスを取得.
② MN が移動.
③ 新 AR 経由で，旧 AR に転送開始（トンネル設定）を要求.
④ トンネル設定後，転送開始.

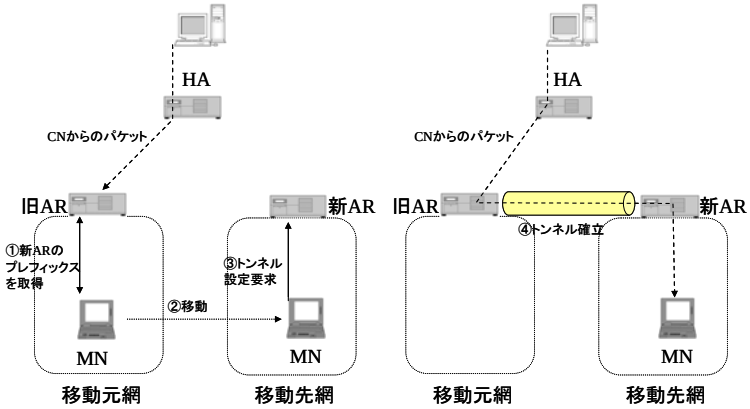

図 1・23　Fast Handovers for Mobile IPv6“Reactive”モード

1-4-4 階層化 Mobile IPv6

（執筆者：大西浩行）［2009 年 5 月 受領］

Mobile IPv6 において，位置登録時間削減，信号数削減（HA への信号）を目的として，RFC 4140 Hierarchical Mobile IPv6 mobility management（HMIPv6）が規定されている．本 RFC において，Mobility Anchor Point（MAP）と呼ばれる装置が新たに規定されており，HA-MAP

の階層構造をとり，MAP 内の移動には MAP に位置登録を実施，MAP 間の移動の際には HA に位置登録を実施している（**図 1･24**）．なお，MN は，気付けアドレスとして，AR 配下の On-link Care-of Address（LCoA）と，MAP 配下の Regional Care-of Address（RCoA）を保持し，HA には，RCoA を MAP には LCoA を現在位置として位置登録を行う．

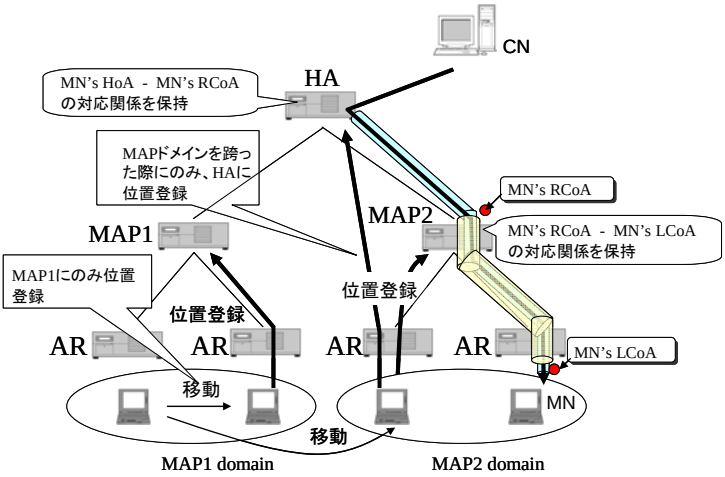

図 1･24　階層化 Mobile IPv6 の動作概要

1-4-5 Proxy Mobile IPv6

（執筆者：西田克利）［2009 年 5 月 受領］

Mobile IPv6 は，端末（Mobile Node，以下 MN）が Home Agent（以下，HA）に位置が変わったことを通知することで，移動制御を実現する技術であった．すなわち，Home Address（以下，HoA）と移動先ネットワークにて取得した Care-of Address（以下，CoA）の組合せを通知することで，移動後にも通信相手（Correspondent Node，以下 CN）とのパケット送受信が可能とする．

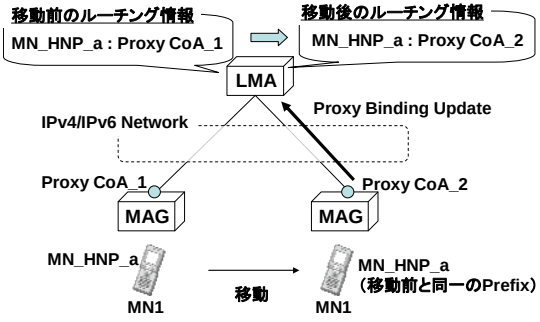

図 1･25　Proxy Mobile IPv6 概要

端末主導型のモビリティ制御技術であった Mobile IPv6 に対して，ネットワークのエッジノードが MN の移動検出し，MN による移動制御を必要としない，ネットワーク型移動制御技術が Proxy Mobile IPv6（以下，PMIPv6）である．

PMIPv6 が適用されるネットワーク（Proxy Mobile IPv6 Domain．以下 PMIPv6-Domain）では，ネットワークエッジノードである Mobile Access Gateway（MAG）が MN の接続を検出し，PMIPv6-Domain におけるモビリティアンカーとなる Local Mobility Anchor（LMA）に，MN が割り当てられたプレフィックス（MN Home Network Prefix）と，MAG の IP アドレス（Proxy Care of Address）の組合せを通知する．これにより，LMA まで転送された MN 宛パケットは，MN が接続する MAG までカプセル化転送され，端末へ届けることが可能となる（**図 1･25**）．

PMIPv6 では，端末はモビリティ制御に関与しない．そのため，PMIPv6 は，IPv4 のみ，IPv6 のみ，デュアルスタックの 3 種類の MN をサポートすることが可能である．

(1) Proxy Mobile IPv6 と Mobile IPv6 の類似点及び差異

メッセージフォーマット及び Mobility Option

PMIPv6 は，Mobile IPv6【RFC 3775】において規定される Binding Update，及び Binding Acknowledgement のメッセージを拡張し，Proxy Binding Update（PBU），Proxy Binding Acknowledgement（PBA）として規定している．

● **Proxy Binding Update（PBU）**

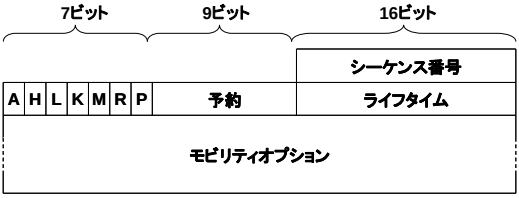

図 1・26 Proxy Binding Update メッセージの構造

PBU は，MAG から LMA に対して送付されるメッセージであり，P フラグが Binding Update メッセージに加えられている．P フラグは，PBU を Mobile IPv6 の BU と区別する識別情報として利用される．

なお，**図 1･26** 中の R フラグ及び M フラグは，NEMO【RFC 3963】及び階層化 Mobile IPv6【RFC 4140】にそれぞれ規定されている．

● **Proxy Binding Acknowledgement（PBA）**

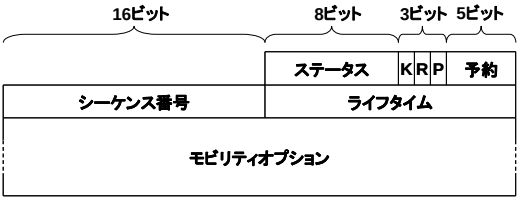

図 1・27 Proxy Binding Acknowledgement メッセージの構造

PBA は，LMA から MAG に対して送付されるメッセージであり，PBU と同様，P フラグが加えられている．なお，**図 1･27** 中の R フラグは NEMO【RFC 3963】において規定されている．

また，Mobility Option も Mobile IPv6 で規定されるものに加え，PMIPv6 では下記の Mobility Option を新たに定義している．

- **Home Network Prefix Option**

PBU 及び PBA に付与され，MN の IPv6 Home Network Prefix を通知するために使用する．

- **Handoff Indicator Option**

PBU 及び PBA に付与され，MN の接続種別を通知するために使用する．本オプションにより，初期接続，インタフェース切替，MAG 間ハンドオーバなどを通知することが可能である．

- **Access Technology Type Option**

PBU 及び PBA に付与され，MN が接続するアクセス種別を通知するために使用する．本オプションにより，仮想 IF，PPP，イーサネット，WLAN，WiMAX を通知することが可能である．

- **Mobile Node Link-layer Identifier Option**

PBU 及び PBA に付与され，MN のリンクレイヤ識別子を通知するために使用する．ただし，リンクレイヤ識別子（Link Layer Address など）が取得できないアクセスの場合，使用されない．

- **Link-local Address Option**

PBU 及び PBA に付与され，MN のリンクローカルアドレスを通知するために使用する．

- **Timestamp Option**

PBU 及び PBA に付与され，メッセージが作成された時刻を付与するために使用する．本オプションを利用することで，LMA 及び MAG はタイムスタンプをベースとしたメッセージ順序制御を行うことが可能となる．

このほか，一つ以上の Vendor-Specific Mobility option【RFC 5094】を付与することも可能である．

(2) 基本動作（初期接続及び MAG 間ハンドオーバ）

図 1･28 に，MN が PMIPv6-Domain に初期接続した際の情報フローを示す．

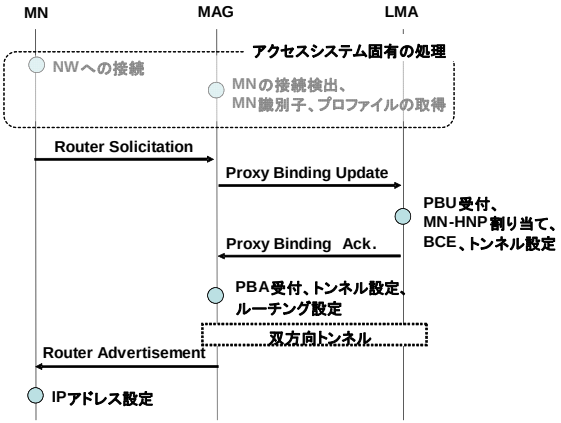

図 1・28　初期接続時の情報フロー

MAG は MN の接続を検出し, Proxy Binding Update を LMA に対して送信する. なお, Router Solicitation メッセージは MN 接続後の任意のタイミングで到着し，Proxy Binding Update の送信とは独立に制御される.

Proxy Binding Update メッセージ

IPv6 header (src=Proxy-CoA, dst=LMAA)
Mobility header
- BU /* P & A flags MUST be set to value 1 */

Mobility Options

- Mobile Node Identifier option	(mandatory)
- Home Network Prefix option(s)	(mandatory)
- Handoff Indicator option	(mandatory)
- Access Technology Type option	(mandatory)
- Timestamp option	(optional)
- Mobile Node Link-layer Identifier option	(optional)
- Link-local Address option	(optional)

LMA は Proxy Binding Update の正当性を確認すると，MN に対して Home Network Prefix を割り当て，MAG に対して Proxy Binding Acknowledgement を送信する．また，Binding Cache Entry（BCE）を作成し MAG-LMA 間の双方向トンネルを設定する.

Proxy Binding Acknowledgement メッセージ

IPv6 header (src=LMAA, dst=Proxy-CoA)
Mobility header
- BA /* P flag must be set to value of 1 */

Mobility Options

- Mobile Node Identifier Option	(mandatory)
- Home Network Prefix option(s)	(mandatory)
- Handoff Indicator option	(mandatory)
- Access Technology Type option	(mandatory)
- Timestamp Option	(optional)
- Mobile Node Link-layer Identifier option	(optional)
- Link-local Address option	(optional)

MAG は Proxy Binding Acknowledgement を受信すると, LMA との双方向トンネルを設定し, MN のデータトラヒックに対するパスを設定する．MAG は Router Advertisement を MN に対して送信し，LMA から受信した Home Network Prefix を通知する.

MN は Router Advertisement より取得した Home Network Prefix をベースに，Stateful あるいは Stateless Address Configuration を行い，アドレスの取得を完了する.

本処理により，MN では Home Network Prefix をベースとするアドレスが，MAG 及び LMA では Home Network Prefix に対するルーチング情報が，それぞれ設定される．なお，PMIPv6-Domain では，MAG が MN のデフォルトゲートウェイとして動作する.

MN から MAG へ転送されたパケットは, モビリティアンカーである LMA までトンネル転送される．LMA は，受信したパケットのカプセル化ヘッダを外した後，LMA が保持する

ルーチング情報に従って，外部ネットワークあるいは PMIPv6-Domain 内へ転送される．

図 1･29 に，MN が MAG 間ハンドオーバを行った際の情報フローを示す．

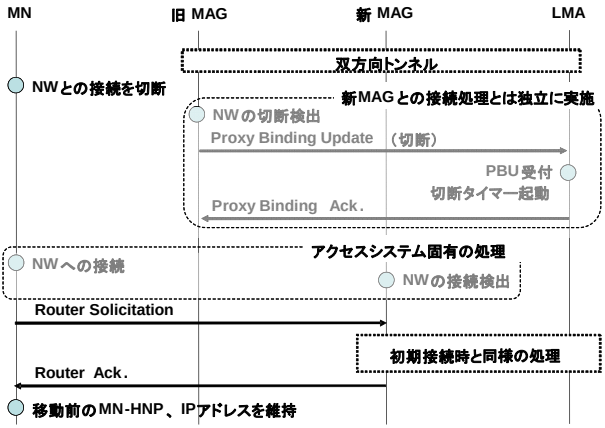

図 1・29　ハンドオーバ時の情報フロー

MN が異なる MAG（新 MAG）配下へ移動すると，新 MAG は MN の接続を検出し，図 1･29 に記載される手順を実施する．これにより，新 MAG と LMA 間に双方向トンネルが設定される．新 MAG は端末から受信した Router Solicitation に対して，Router Advertisement を送信し，LMA から通知された Home Network Prefix を MN に対して通知する．MN は現在保持する Home Network Prefix と同一の情報を取得することで，同一の IP アドレスをそのまま使用して通信を継続する．

なお，移動前に接続していた MAG（旧 MAG）は MN との接続が切断されたことを検出し，LMA に対して Proxy Binding Update（Lifetime = 0）を送信し，Binding Cache Entry の削除を依頼する．LMA は一定時間を待って Binding Cache Entry を削除し，MN に対して，Proxy Binding Acknowledgement を送信する．本処理は，上記手順とは独立に実施することが可能である．

(3)　セキュリティ

MAG-LMA 間で交換されるメッセージは，IPSec などによる改ざん防止やメッセージ認証機能を提供するエンド-to-エンドセキュリティによって保護されていなければいけない．

なお，Mobile IPv6 と違い，Proxy Binding Update に Home Address destination option や Type 2 Routing header が存在しないため，IPSec におけるポリシー情報／セキュリティアソシエーション選択で特別な考慮は必要ない．

(4)　IPv4 サポート

PMIPv6 は IPv4 端末をサポートすることが可能である．また，IPv4 アドレスをもつ LMA 及び MAG で構成される PMIPv6-Domain に提供することも可能である．

IPv4 アドレスサポートの拡張

【draft-ietf-netlmm-pmip6-ipv4-support-18.txt】が提供された PMIPv6 では，MN の IPv4 ホーム

アドレスを MAG-LMA 間で送受信するために，IPv4 Home Address Request Option，及び IPv4 Home Address Reply Option が使用される．また，LMA が MAG に対して IPv4 デフォルトルータ情報を通知するために, IPv4 Default-Router Address Option が規定されている. さらに，LMA が MAG に対して DHCP サーバとして動作するべきかを指定する IPv4 DHCP Support Mode も新たに規定されている．

また, PMIPv6 を MAG 及び LMA が IPv4 アドレスをもつ PMIPv6-Domain で適用する場合，Proxy Binding Update 及び Proxy Binding Update Acknowledgement メッセージは UDP をトランスポート層とする信号となる．すなわち，これらのメッセージを送信する際，MAG および LMA は，従来の Proxy Binding Update 及び Proxy Binding Update Acknowledgement に設定される Mobility Header 情報を，IPv4 ヘッダをもつ UDP 上に設定する（IPv6 ヘッダ情報は設定しない）.

1-4-6 経路最適化に関する拡張

（執筆者：西田克利）［2009 年 5 月 受領］

1-4-1 項でも述べたように，Mobile IPv6 では，Return Routability 処理を行うことで，MN と CN 間で直接パケットを送受信する, パケット転送経路の最適化が可能である. しかし, Return Routability は，Home Address Test と Care-of Address Test を MN と CN 間で交換しなければならないため，MN が移動した際のハンドオーバ遅延が大きくなる．特に，Home Address Test は HA を経由するため，その遅延は大きくなることが想定される.

また，Home Address Test あるいは Care-of Address Test を行う際に，悪意のある第三者がこれらのメッセージを傍受できる場合, Redirection-based Flooding などのセキュリティ上脅威がある．この脅威による影響を少なくするためには，Return Routability 処理頻度を高めることが考えられるが，これはシグナリング量の増加という副作用が伴う.

上記のような課題を解決するために, Enhanced Route Optimization for Mobile IPv6（RFC 4866）において，Mobile IPv6 の経路最適化の拡張方式が規定されている．RFC 4866 では，上記セキュリティ脅威の解決に必要な，MN が保持する HoA の正当性確認を，Cryptographically Generated Address（CGA，RFC 3972）を採用することで実現する．また，Care-of Address Test を Binding Update と重畳する機能，及び HA への Binding Update と同時に CN への Binding Update を送信する機能などを提供する．これにより，ハンドオーバ時の最適経路更新に掛かる時間の短縮を可能としている.

1-4-7 セキュリティに関する拡張

（執筆者：西田克利）［2009 年 5 月 受領］

(1) IKEv2 及び Revised IPSec へのセキュリティアーキテクチャ拡張

IPSec 仕様を規定する RFC 2401 が改訂（RFC 4301）されたことに伴い，RFC 4301 と IKEv2 に準拠する Mobile IPv6 のセキュリティ方式拡張が，Mobile IPv6 Operation with IKEv2 and the Revised IPsec Architecture（RFC 4877）に規定されている.

変更点としては，Mobility Header の Type Value 及び，ICMP message type 及び code を IPSec Selector として利用することが可能となったことなどがある.

(2) 認証方式の拡張

Mobile IPv6 では，端末の識別に IPv6 アドレス（Home Address）を利用する．Mobile Node

Identifier Option for Mobile IPv6（MIPv6）（RFC 4283）では，IPv6 アドレス以外の識別子を利用して，端末の認証などを可能とするオプションが規定されている．このオプションは，Mobile Node Identifier Option と呼ばれ，Fully Qualified Domain Name（FQDN）や International Mobile Station Identifier（IMSI）などを，Binding Update により HA へ通知することが可能となる．HA はこの情報を利用することで，AAA などの認証装置に接続可否を問い合わせる，といったことが可能となる．

また，本オプションは，Mobile IPv6 における認証方式である IKE/IPSec の代替手段としても利用される．

1-4-8 Network Mobility (NEMO)

（執筆者：鈴木俊博）［2009 年 5 月 受領］

MN 機能を有しない端末群に対するネットワーク単位での移動の提供や，MN 機能を拡張しネットワーク単位での移動を可能とする技術が Network Mobility（以下，NEMO）である．

NEMO でサポートする移動するネットワーク（以下，Mobile Network）は，少なくとも一つのモバイルルータ（Mobile Router，以下 MR）に複数の MN（MN 機能を有しない端末を特に Local Fixed Node（LFN）と呼ぶ）が接続された構成となっている（**図 1･30**①）．

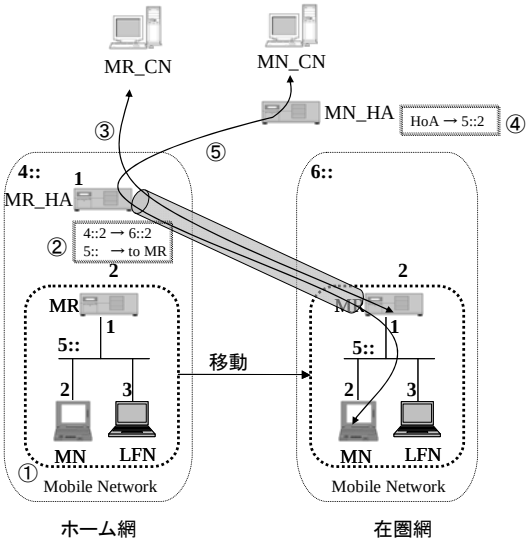

図 1・30　NEMO の動作概要

NEMO では，1-4-5 項にて説明した拡張以外に Binding Update メッセージ上に新たに Mobile Network Prefix Option を規定している．Mobile Network Prefix Option は，MR からの Binding Update（以下，BU）に付与され，MR が管理する Prefix 情報を Home Agent（以下，HA）に通知する．本オプションを通知された HA は，MR のホームアドレスと気付けアドレスの対応関係とともに，Prefix 情報と気付けアドレスの対応関係を，生成もしくは更新する（図 1･30②）．

MR のホームアドレス宛に送られたデータグラムは HA によってインターセプトされ，MR の気付けアドレスへトンネリングされる（図 1･30③）．同様に，Mobile Network の配下に在

圏する LMN へのデータグラムもトンネリングされることにより, LMN に伝達される. Mobile Network に接続する MN の気付けアドレスは，通常の Mobile IPv6 の動作と同様に Mobile Network Prefix により生成され, ホームアドレスとの対応関係が MN の HA にて管理される（図 1･30④）．したがって，MN 宛のデータグラムは，MN の HA にて MN の気付けアドレス宛に転送されると MR の HA によってインターセプトされ，MR 宛に再送信される．本データグラムはトンネリングの終端である MR によって，MN 宛に送信される（図 1･30⑤）．Mobile Network から外部への通信についても，MR と HA 間のトンネルを経由して行われる．