モバイルは今

MobileIP version 6

楯岡 孝道
電気通信大学 tate@cs.uec.ac.jp

いうまでもないことだが，インターネットでは世界中で唯一のIPアドレスを用いたend-to-end通信を行うことが基礎となっている．さまざまな中継機構や代理機構を用いることで，end-to-endの通信をせずにインターネットへ参加することも可能だが，どうしてもある種の歪みができてしまう．インターネット通信の移動透過性を得る場合においても，IPレベルで移動透過性を付加することが，最も直感的な移動サポートの導入となるだろう．

IETFにおける長い議論の末に，次世代IPのIPv6（IP version 6）に対する拡張であるMIPv6（MobileIP version 6）がRFC標準となる運びとなった．そこで，今回はMIPv6について紹介する．

●

MIPv6はIPv6ネットワークにおいてIPレベルの移動透過性を実現するプロトコルである．すなわち，移動ノードがネットワーク上を移動し，IPv6アドレスが変化した場合でも，それまでの通信を継続でき，かつ，常に同じIPv6アドレスを用いてこの移動ノードを呼び出すことができる．

MIPv6はIP version 4向けのMobile IP（MIPv4）の動作を元にしている．どちらの場合でも共通の構成要素は移動ノード（MN: Mobile Node）と相手ノード（CN：Corresponding Node），そしてホームエージェント（HA：Home Agent）である．移動ノードはノード個有のIPアドレスとしてホームアドレスを持つ．ホームアドレスの属するネットワークをホームネットワークと呼び，ホームエージェントはホームネットワークに接続している．このホームネットワークはインターネット上のホストから到達可能であれば，実際に存在していても，ホームエージェント内の仮想的なものでもよい．また，移動ノードは移動先で移動先ネットワークに属するIPアドレスの割り当てを受ける．このIPアドレスを気付アドレス（CoA：Care-of-Address）と呼び，通常DHCPやIPv6アドレス自動設定によって設定される．

移動ノードは移動先で気付アドレスの割り当てを受けると，自らのホームアドレスと気付アドレスの対応をホームエージェントに登録し，移動ノードとホームエージェントとの間でIPトンネリングを行う．そして，後述する経路最適化（Route Optimization）を行わない場合，移動ノードと相手ノードとの通信はすべてホームエージェントを経由して行われる．これにより，移動ノードは常にホームアドレスを用いて連続した通信を行うことができる．

MIPv6はMIPv4と比較すると，経路最適化に関して大幅に改良された．MIPv4の弱点の1つは，基本的にすべての通信がホームエージェントを通過することであった．このため，移動先においてはたとえ隣のノードとの通信ですら一度ホームエージェントを経由して通信することになり，通信効率が悪化する．これを避けるための拡張仕様として移動ノードと相手ノードとの間で直接通信する経路最適化が提案されていたが，経路最適化を行う際には移動ノードと相手ノードとの間に認証が可能な信頼関係が必要なうえ，組織のファイアウォールで一般的なingress filterで通信が阻害されるという問題点があった．そのため，実際にはごく限られた状況でしか利用できなかった．

経路最適化を行う際には，相手ノードから移動ノードへ直接パケットを送るために，移動ノードのホームアドレスと気付アドレスの対応表（Binding Cache）を各相手ノードが持たなくてはならない．一方で，この対応表を不正に書き換えれば，インターネット上のどこにでも移動ノード宛パケットを転送させることができる．これを

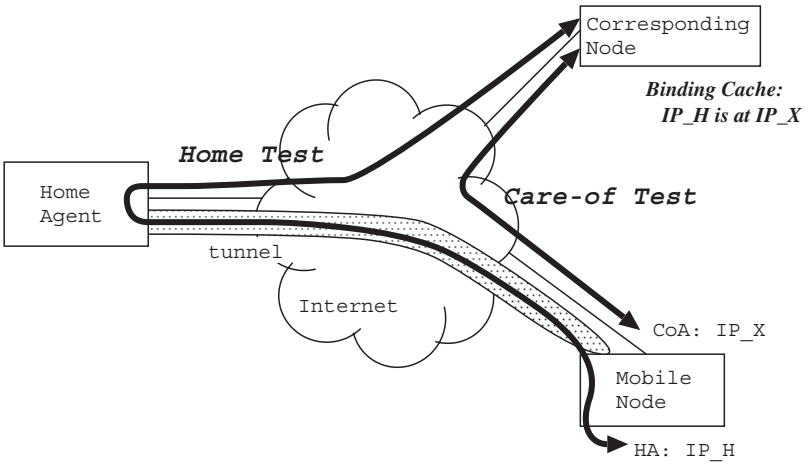

図-1　Return Routability の動作

避けるため，この対応表の更新には何らかの認証機構が必要となる．しかし一般にすべての相手ノードとIPsecのような確実な認証を行うのは難しい．MIPv6 ではこれをReturn Routabilityという方法で解決している．

Return Routabilityでは，**図-1** のように，相手ノードと移動ノードとの間でホームアドレスと気付アドレスのそれぞれを用いて確認用パケットを交換する．確認用パケットの交換は移動ノードから開始される．まず，移動ノードはホームアドレスを送信元としたHome Test Initパケットと，気付アドレスを送信元としたCare-of Test Initパケットを，それぞれ相手ノードに送信する．前者は経路最適化をせずにホームエージェントを経由して，後者は気付アドレスからのIPパケットとして，相手ノードに到着する．相手ノードではそれぞれに対し，別々の乱数（home keygen tokenとcare-of keygen token）を含む返答をHome TestパケットおよびCare-of Testパケットとして送信する．返答に関しても前者はホームエージェントを経由して，後者は気付アドレスに直接，送られる．返答を受けとった移動ノードは，ホームアドレスと気付アドレスの対応を更新するパケットに，両方の乱数を結合した値を用いて電子署名を行う．相手ノードは自らが送信した乱数によって署名された更新パケットのみを受けつける．

このようにして確認した更新パケットは，ホームアドレスから届いたパケットと同程度には信頼できる．もちろん，両方のアドレス宛のパケットが通過するネットワーク上のホストならば，各乱数を盗聴し，更新パケットを偽造することが可能だが，そのようなホストはそもそもMobile IPを利用していなくても通信の妨害や盗聴が可能なため，通常のIPによる通信と同程度の信頼性といえる．

相手ノードでReturn Routabilityが利用可能な場合には，経路最適化が行われ，移動ノードと相手ノードの間で直接通信が行われる．この際，相手ノードと移動ノードとの間に特別な信頼関係が不要なため，一般的なノードでのReturn Routabilityの使用も現実的である．もし，相手ノードがReturn Routabilityに対応していない場合には，通信効率は落ちるものの，従来のMIPv4 同様にホームエージェントを経由した通信が可能となる．

また，MIPv6 ではIPv6 のIPオプションヘッダを活用し，ホームアドレスをIPオプションとしてパケットに含めることで，ファイアウォールを通過することが可能になっている．

●

遅延の影響の少ない単純なデータ転送や，移動時に再接続しても影響が少ないメッセージ送信など，応用分野によっては，VPNやDynamic DNS等で得る移動透過性で十分であろう．また，もちろんMIPv6 では対応しきれない問題も多い．しかし，MIPv6 は他の手法と比較して通信効率を向上させやすく，かつ移動前後でも通信を継続できるなどアプリケーション側の対応も容易である．

IPv4 におけるMIPv4 は，すでにIPv4 が普及した後に制定されたこともあり，普及しなかったが，MIPv6 はまだ十分普及可能なタイミングで制定された．また，MIPv6 はMIPv4 の反省を元に，既存ネットワークに容易に導入可能なように設計されている．RFC 標準となることにより，各ノードへのMIPv6 の導入，特に移動しないノードへの経路最適化サポートの導入が進めば，MIPv6 の弱点である通信の非効率さも解消される．実用段階に入ったMIPv6 をどう使うか，考えてみるのはいかがだろうか．

（平成 16 年 1 月 5 日受付）