2007－MBL－42 (3)
2007／9／27

プライベートネットワークに配置されたホームエージェントを用いたMobile IPv4手順の設計

野地川 栄光[†‡] 加藤 聰彦[‡] 伊藤 秀一[‡]

IETFにおいてMobile IPが標準化されており、インターネット環境や携帯ネットワークなどにおいて用いられている。現状のMobile IPはグローバルIPアドレスを持つネットワークでの利用を想定している。その一方でIPv4アドレス空間の枯渇のため、プライベートIPアドレスの使用とインターネットアクセス時のNATやNAPTの導入が広く行われている。それゆえ、端末がプライベートIPアドレスを使用したネットワークに移動した際にもIPの可動性を提供するNAT Traversal Mobile for IPの検討がIETFにて行われている。しかしこの手順にも、Home Agent (HA)がプライベートネットワークに存在し、端末のホームアドレス(HoA)がプライベートIPアドレスである場合や、移動先のネットワークがプライベートネットワークでかつForeign Agent (FA)は存在しない場合などを考慮していない。このため、筆者らは、これらの条件下において、移動端末の可動性を提供するMobile IPv4手順について検討している。本稿ではその詳細について報告する。

Design of Mobile IPv4 Procedure Using Home Agent Deployed in Private Network

Eimitsu Nojikawa[†‡] Toshihiko Kato[‡] Shuichi Itoh[‡]

The Mobile IP has been a standard track protocol at IETF, and it has used in the internet environment and mobile networks. The current Mobile IP assumes the use of the global IP addresses. On the other hand, in the real world, the NAT or NAPT devices are widely used due to the wide use of the private IP addresses because the number of internet systems increases and the IPv4 address's space is limited. Based on these situations, IETF is standardizing the NAT Traversal for Mobile IP in order to support IP mobility when a mobile node moved to a network using private IP address. However, it still has some problems in the situation where a Home Agent is located in a private network and the mobile node's home address is a private address, and where a foreign network is a private network, and a foreign agent does not exist in the network. In this paper, we propose a new Mobile IP protocol which takes account of those situations. This paper describes the details of our protocol.

1. はじめに

近年、IPモビリティを提供するために、IETFにおいてMobile IP[1]が標準化されており、インターネット環境や、携帯ネットワークで利用されている。Mobile IPとはこれらのネットワーク上でノードが移動しても、通信中のIPアドレスを変更せずに、またその通信を途切れることなしに維持することを実現するプロトコルである。すなわち、通常のIPネットワークでは、他の端末と通信をしている移動体端末が、そのまま、別のネットワークに移動すると、IPアドレスの再設定などが生じる。また仮にDHCPなどでIPアドレスを自動取得したとしても、IPルーティングの変更などが伴い、再度、通信をやり直さないとならない。Mobile IPはこれらの問題に柔軟性を持たせた移動体通信におけるIP通信拡張プロトコルである。

しかしながら、[1]では、インターネット内での通信や、LAN内での移動体通信を想定しており、現実的なインターネット環境を考慮すると不足があると考えられる。例えば、NATで分割されたグローバルネットワークとプライベートネットワーク間での端末の移動については、課題が残されている。そのためIETFで

† 株式会社 数理計画
† SUURI-KEIKAKU CO., LTD
‡ 電気通信大学 大学院 情報システム学研究科
‡ University of Electro-Communications

はNAT Traversal for Mobile IP[2]にて公開標準化し提案している。しかしながら、[2]では、HAもプライベートネットワークにいるケースについては、具体的には示していない。筆者らは、そこに着目し、その通信手順について設計を検討している[3]。本稿ではその詳細について述べる。

2. NAT Traversal for Mobile IP の概要と問題点

[2]では、以下のような3つのシナリオに対する提案を行っている。

- FAが不在、MNはNATのプライベートネットワークに位置し、co-located Addressを利用するケース
- MNとFAが同じNATのプライベートネットワークに位置し、FAを経由してMNの登録が行われるケース
- MNとFAが同じNATのプライベートネットワークに位置し、FAをパススルーしてMNを登録作業を行うが、MN自身のアドレスをco-located Addressとして登録するケース

また、以下の4つの条件を前提としている。

① MN-HA間でUDP（HAを宛先にし、ポート番号は434）を利用することが可能
② NATによりプライベートとパブリックネットワークに分割されルーティングが可能、且つIPトンネリングに関しては[1]に従う
③ ②によって、各トンネリング手法は[4]にも従う
④ 逆方向トンネルと、順方向トンネルはここでは同じように利用される。つまり順方向と逆方向トンネルはお互いに対称であるため双方向トンネリングが結果的に形成される。

以上の前提条件をもとに提案されており、その基本メッセージシーケンスを図1に示す。

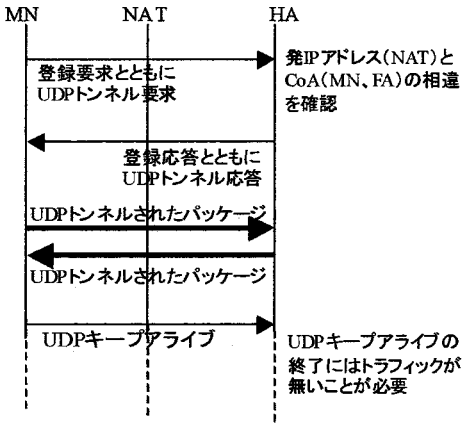

図1 基本メッセージシーケンス

3. 通信手順の設計

3.1 アプローチ

筆者らは、図2に示すようなネットワークを想定し以下のアプローチを提案している。

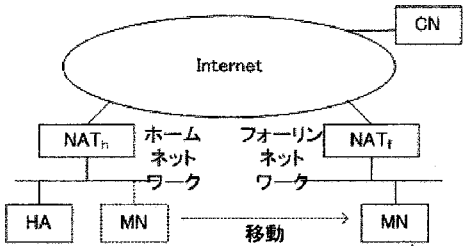

図2 想定するネットワーク構成

まず筆者らは次の2つの条件を仮定する。第一に、ホームネットワークのNATにおいてMobile IPが登録手順で使用するポート番号434あてのUDPデータグラムに対しては、HAにフォワーディングするよう設定する。第二に、ホームネットワークに割り当てられるグローバルIPアドレス(NAT$_h$のインターネット側のアドレス)については何らかの手順で知りえているものとする。

次に、プライベートネットワークへの移動時のIPモビリティ実現手順を以下に示す。

(1) 移動の検出

他の網への移動は、インタフェースのアクティベーションとその後のDHCPなどによるIP

アドレスの取得により検出する。取得した IP アドレスが気付アドレス(CoA)となる。なお CoA はプライベート IP アドレスである。

(2) CoA の登録

移動を検出すると MN は HA に対して Registration Request を送出する。MN は HA に対応するグローバル IP アドレスを何らかの方法で、入手できるため、Registration Request メッセージの IP ヘッダ中のあて先 IP アドレスはそのグローバルアドレスに設定する。IP ヘッダのソースアドレスは動的に取得したプライベート IP アドレスであるが、このアドレスはフォーリンネットワークの NAT によりグローバル IP アドレスに変換される。またメッセージ中の CoA、HoA、HA アドレスはプライベートアドレスである。

このメッセージを受信した HA は MN の HoA と CoA の対応(モビリティバインディング)を管理する。ただし CoA としてはメッセージ中の CoA ではなく、そのメッセージの IP ヘッダのソースアドレスとして格納されているグローバル IP アドレスを記録する。HA はこれに対して Registration Reply メッセージを返信する。メッセージ中に含まれるアドレスはすべてプライベート IP アドレスであるが、IP ヘッダのアドレスについては NAT_h と NAT_f で適切な変換が行われる。

(3) CN との通信

双方向トンネリングを用いて行う。さらに[2]と同様に UDP カプセル化を用いる。MN(HoA)から CN への IP データグラムは、CoA(プライベートアドレス)から HA(グローバルアドレス)への IP ヘッダと、あて先ポートが 434 の UDP ヘッダにカプセル化されて送出される。このうち外側の IP ヘッダのソースアドレスは NAT_f によりグローバルアドレスに変換される。

NAT_h を経由して HA に配信された IP データグラムは、カプセル化がとかれ、CN に向けて送信される。このとき NAT_h でソースアドレス(MN の HoA)がグローバルアドレスに変換される。CN からの IP データグラムは NAT_h のグローバルアドレスあてに送られ、あて先アドレスが MN の HoA に戻される。このあて先のデータグラムは HA が取り込み、NAT_f のグローバルアドレスあての IP ヘッダと UDP ヘッダを付加して送出する。これは上記と逆の処理により最終的に MN に配信される。

3.2 通信手順方針の検討

(1) 二つの NAT はいずれも NAPT 機能で動作する。NAT_f は、市販のブロードバンドルータに実装されていると想定し、それを利用する。
(2) フォーリンネットワークに移動した MN は Co-located CoA を利用するものとする。そのネットワークプレフィックスはホームネットワークと同様でも良い。
(3) Mobile IPv4 の代表的実装例である Monarch プロジェクトにおける、MN のコンフィギュレーションファイルの中では、HA の実アドレスはスタティックに初期設定される。本稿でも同様であるとするが、NAT_h 上に NAPT された HA のグローバル IP アドレスについては、HA の実アドレスとは、独立したパラメータとして[2]では動作することを前提とする。
(4) MN はホームネットワークにいるとき、その通信は全て HA を経由せずに行う。この時、CN との通信において、NAPT でマッピングされた NAT_h のグローバル IP アドレスを利用して 1 対 N(複数の MN も可)で通信を行う。
(5) NAT_h では、HA に対して UDP ポート番号 434 を HA に NAT マッピングしたグローバル IP アドレスから、HA のプライベート IP アドレスに転送許可している。
(6) ホームネットワークには、管理外の MN が存在する可能性を許容する。また、フォーリンネットワークには、筆者らが想定する管理外の HA や FA が存在する可能性も許容する。
(7) HA と MN には共通鍵を持たせ、安全性を確保する。

3.3 通信手順

(1) 記号表記

本稿で利用する表記の一覧は以下である。

- NAT_h_HA : NAT_h 上の HA に NAPT されたグローバル IP アドレス

- NAT_h_MN:NAT_h上の MN に NAPT されたグローバル IP アドレス
- NAT_f_MN : NAT_f上の MN に NAPT されたグローバル IP アドレス
- src : 送信元 IP アドレス
- dst : 宛先 IP アドレス
- srcUDP/srcTCP : 送信元 UDP/TCP ポート番号
- dstUDP/dstTCP : 宛先 UDP/TCP ポート番号
- HA_addr: HA のプライベート IP アドレス
- MN_f : MN のフォーリンネットワーク上のプライベート IP アドレス
- CN_addr : CN のグローバル IP アドレス

その他の表記は[1][2]に準拠する。

(2) 移動の検出詳細

① MN は NAT_f の裏側のプライベートネットワークに移動し、ネットワークインターフェースのアクティベーションを行う。

② MN は自身の IP アドレスを DHCP によって取得する。

③ IP 取得直後に、他管理のモビリティエージェントから、Agent 広告メッセージを受け取る可能性がある。その場合、Registration Request を行うが、共通鍵が違うため、認証されない。この時点では、CoA も決定はされていない

④ 第一の検知方法として、MN はホームネットワークで Agent 広告メッセージを受け取っていたとした場合、その Lifetime 内に再度メッセージを受信することを仮定する。[1]の推奨通り、Lifetime フィールドの 1/3 程度の短い時間間隔で HA は送信することとして、3 秒とした場合、1 秒間隔で Agent 広告メッセージが流れている前提となる。しかし、Agent 広告メッセージが無い場合、MN は自ら Agent 要請メッセージをリンク上に送信する。仮に他管理のモビリティエージェントからの応答があっても、その結果は③と同様であるため、結果として MN は移動を検知する。

⑤ 第二の方法として、Agent 広告メッセージのネットワークプレフィックス長拡張で判断する方法であるが、フォーリンネットワークにモビリティエージェントがいることが前提となる。もし居る場合は、受け取った広告メッセージと従来のメッセージのネットワークプレフィックス長を比較して、違えば、移動を検知する。同じである場合、移動していないことも検討できるため、④の方法で移動を検知する。

⑥ 以上より、移動が検知され、MN としては、DHCP で取得した IP アドレス、つまり MN_f を CoA として利用する（co-located CoA）。

(3)Registration Request と UDP トンネル要求拡張

① MN は Registration Request メッセージに MN_f を CoA フィールドにセットし、コンフィギュレーションファイルより HA に HA_addr をセットし、同ファイルの設定から、NAT_h_HA に対して IP パケットを送信する。

[IP ヘッダ：src＝MN_f ,dst＝NAT_h_HA]
[UDP ヘッダ：srcUDP=ephemeral,dstUDP=434]
[Registration Request :
Type=1,D=1,HoA,HA=HA_addr,CoA=MN_f,T=1]
[UDP トンネル要求拡張 :
Type=144,F=1,Encapsulation =4(default)]
[MN-HA 認証拡張：Keyed HMAC-MD5]

② この Registration Request は、インターネットに送信される際に、NAT_fの NAPT 機能により以下に変換される。

[IP ヘッダ：src＝NAT_f_MN ,dst＝NAT_h_HA]
[UDP ヘッダ：srcUDP=ephemeral,dstUDP=434]
[Registration Request :
Type=1,D=1,HoA,HA=HA_addr,CoA=MN_f,T=1]
[UDP トンネル要求拡張 :
Type=144,F=1,Encapsulation =4(default)]
[MN-HA 認証拡張：Keyed HMAC-MD5]

(4)HA 上での登録診断と UDP トンネル許可

① NAT_h で受け取られたパケットは、そのまま HA_addr に変換され転送される。

[IP ヘッダ：src＝NAT_f_MN,dst＝HA_addr]
[UDP ヘッダ：srcUDP=ephemeral,dstUDP=434]
[Registration Request :
Type=1,D=1,HoA,HA=HA_addr,CoA=MN_f,T=1]
[UDP トンネル要求拡張 :
Type=144,F=1,Encapsulation =4(default)]
[MN-HA 認証拡張：Keyed HMAC-MD5]

② HA に転送された Registration Request は、共通鍵の照合および、MN-HA 認証拡張にて HMAC-MD5 を用いた一貫性認証を行い、登録の受諾確認を行う。ここで MN から送られた要求の CoA と送信元 IP アドレスは相違があるが、[2]では、送信元 IP アドレスを信頼する。以上問題がなければ、MN に対する HA 上の Mobility Binding は以下の情報に更新される。
[HoA , CoA : NAT_f_MN , Identification ,Lifetime]
③ 次に UDP トンネル要求拡張の F=1 にて強制的トンネリング要求し、Registration Request メッセージの T=1 にて、逆方向トンネルを必須とする。また、IP-in-UDP カプセル化を用いるとする。
④ HA は問題が無ければホームネットワーク上に不要な ARP 要求を行い、HoA に対する代理 ARP を行う。よって、HoA の MAC アドレスは HA と対応付けられ、各ノードに認識される。

(5) Registration Reply と UDP トンネル応答拡張

① MN に返信する Registration Reply は以下となる。ただし、CoA フィールドは、Registration Request メッセージの CoA の値をコピーする。
[IP ヘッダ：src＝HA_addr,dst＝NAT_f_MN]
[UDP ヘッダ：srcUDP=434,dstUDP = ephemeral]
[Registration Reply：
Type=3,code=0,HoA,HA=HA_addr,CoA=MN_f]
[UDP トンネル応答拡張：
Type=44,F=1,Keepalive Interval=0(default)]
[MN-HA 認証拡張：Keyed HMAC-MD5]
②NAPT 機能により変換され、以下となる。
[IP ヘッダ：src＝NAT_h_HA,dst＝NAT_f_MN]
[UDP ヘッダ：srcUDP=434,dstUDP=ephemeral
[Registration Reply：
Type=3,code=0,HoA,HA= HA_addr,CoA= MN_f]
[UDP トンネル応答拡張：
Type=44,F=1,Keepalive Interval=0(default)]
[MN-HA 認証拡張：Keyed HMAC-MD5]

(6)MN での Registration Reply とトンネリングの確認

① Registration Reply が NAT_f_MN 宛に届き、MN_fに転送される。
[IP ヘッダ：src＝NAT_h_HA,dst＝MN_f
[UDP ヘッダ：srcUDP=434,dstUDP=ephemeral
[Registration Reply：
Type=3,code=0,HoA,HA=HA_addr,CoA= MN_f]
[UDP トンネル応答拡張：
Type=44,F=1,Keepalive Interval=0(default)]
[MN-HA 認証拡張：Keyed HMAC-MD5]
②MN では、共通鍵の確認、そして MN-HA 認証拡張により、その一貫性認証を確認を行い、code=0 により登録受諾を確認。また UDP トンネル応答拡張で KeepAlive Interval=0 のため MN 側の設定に委ねられたことを確認。また、IP-in-UDP カプセル化での双方向トンネリングが完成したことを確認する。

(7)CN との UDP トンネル経由の通信

①MN は CN との通信で、例えば HTTP 通信を仮定する。
[IP ヘッダ：src=HoA,dst=CN_addr]
[TCP ヘッダ：srcTCP=ephemeral,dstTCP=80]
[TCP データ部：HTTP_REQUEST]
②既に確立されている UDP トンネリングを利用するため、[2]によりカプセル化データを生成し、IP パケットを再構築する。
[外部 IP ヘッダ：src=MN_f,dst=NAT_h_HA]
[UDP ヘッダ：srcUDP=ephemeral,dstUDP = 434]
[UDP データ部：
[MIP Tunnel data message header：
type=4,Next header=44]
[IP ヘッダ：src=HoA,dst=CN_addr]
[TCP ヘッダ：srcTCP=ephemeral,dstTCP = 80]
[TCP データ部：HTTP_REQUEST]]
③次に NAT_fによって NAPT 変換されるため以下のようになる。
[外部 IP ヘッダ：src= NAT_f_MN,dst=NAT_h_HA]
[UDP ヘッダ：srcUDP=ephemeral,dstUDP=434]
[UDP データ部：
[MIP Tunnel data message header：
type=4,Next header=44]
[IP ヘッダ：src=HoA,dst=CN_addr]
[TCP ヘッダ：srcTCP=ephemeral,dstTCP=80]
[TCP データ部：HTTP_REQUEST]]

④NAT_hに到達したパケットはHA_addrに転送され以下のようになる。
[外部IPヘッダ：src= NAT_f_MN,dst=HA_addr]
[MIP Tunnel data message header：
type=4,Next header=44]
[IPヘッダ：src=HoA,dst=CN_addr]
[TCPヘッダ：srcTCP=ephemeral,dstTCP=80]
[TCPデータ部：HTTP_REQUEST]]
⑤HAでは、その送信元アドレスが、Mobility Binding上のMNのCoAアドレスに相当することから、カプセル化の解除をMIP Tunnel data message headerを確認し行う。
[IPヘッダ：src=HoA,dst=CN_addr]
[TCPヘッダ：srcTCP=ephemeral,dstTCP=80]
[TCPデータ部：HTTP_REQUEST]
⑥HAはCNに転送する。
[IPヘッダ：src= NAT_h_MN,dst=CN_addr]
[TCPヘッダ：srcTCP=ephemeral,dstTCP=80]
[TCPデータ部：HTTP_REQUEST]
⑦ CNでは、HTTPサービスが提供中で、その応答としてNAT_h_MN宛に返す。
[IPヘッダ：src=CN_addr ,dst=NAT_h_MN]
[TCPヘッダ：srcTCP=80,dstTCP=ephemeral
[TCPデータ部：HTTP_REPLY]
⑧NAT_hでは、HoAに転送を行う。
[IPヘッダ：src=CN_addr ,dst=HoA]
[TCPヘッダ：srcTCP=80,dstTCP=ephemeral
[TCPデータ部：HTTP_REPLY]
⑨ホームネットワーク上に到達したIPパケットはHAに捕捉される。HAではMNに転送するために、Mobility Bindingを確認し、MNのHoAからCoAにパケットを転送するために、以下のIPパケットを再構築する。
[外部IPヘッダ：src=HA_addr,dst=NAT_f_MN
[UDPヘッダ：srcUDP=434,dstUDP = ephemeral]
[UDPデータ部：
[MIP Tunnel data message header：
type=4,Next header=44]
[IPヘッダ：src = CN_addr ,src = HoA]
[TCPヘッダ：srcTCP=80,dstTCP=ephemeral]
[TCPデータ部：HTTP_REPLY]]
⑩NAT_hにてNAT_f_MN宛に転送される。
[UDPヘッダ：srcUDP=ephemeral,dstUDP=434]
[UDPデータ部：

[外部IPヘッダ：src=HA_addr,dst=NAT_f_MN
[UDPヘッダ：srcUDP=434,dstUDP = ephemeral]
[UDPデータ部：
[MIP Tunnel data message header：
type=4,Next header=44]
[IPヘッダ：src = CN_addr ,src = HoA]
[TCPヘッダ：srcTCP=80,dstTCP=ephemeral]
[TCPデータ部：HTTP_REPLY]]

⑪NAT_fにてMNに転送される。
[外部IPヘッダ：src=HA_addr,dst=MN_f
[UDPヘッダ：srcUDP=434,dstUDP = ephemeral]
[UDPデータ部：
[MIP Tunnel data message header：
type=4,Next header=44]
[IPヘッダ：src = CN_addr ,src = HoA]
[TCPヘッダ：srcTCP=80,dstTCP=ephemeral]
[TCPデータ部：HTTP_REPLY]]
⑫MNに転送されたIPパケットは、UDPトンネリングのエンドポイントとして認識され、指定された形式でカプセル化解除される。
[IPヘッダ：src = CN_addr ,src = HoA]
[TCPヘッダ：srcTCP=80,dstTCP=ephemeral]
[TCPデータ部：HTTP_REPLY]
⑬MNでは、このIPパケットは自身のHoA宛のパケットであることを認識し、TCPデータ部の情報を、アプリケーションに受け渡して通信を完了する。

3.4 メッセージシーケンス例

図3では、筆者らの提案する通信手順によりMNとHAをトンネルのエンドポイントとしたNAT経由でのMobile IP通信を利用するための双方向トンネリング環境が整うことを確認している。この環境により、MNはデータ通信をプライベートネットワークにいるHA経由で行うことが可能となる。

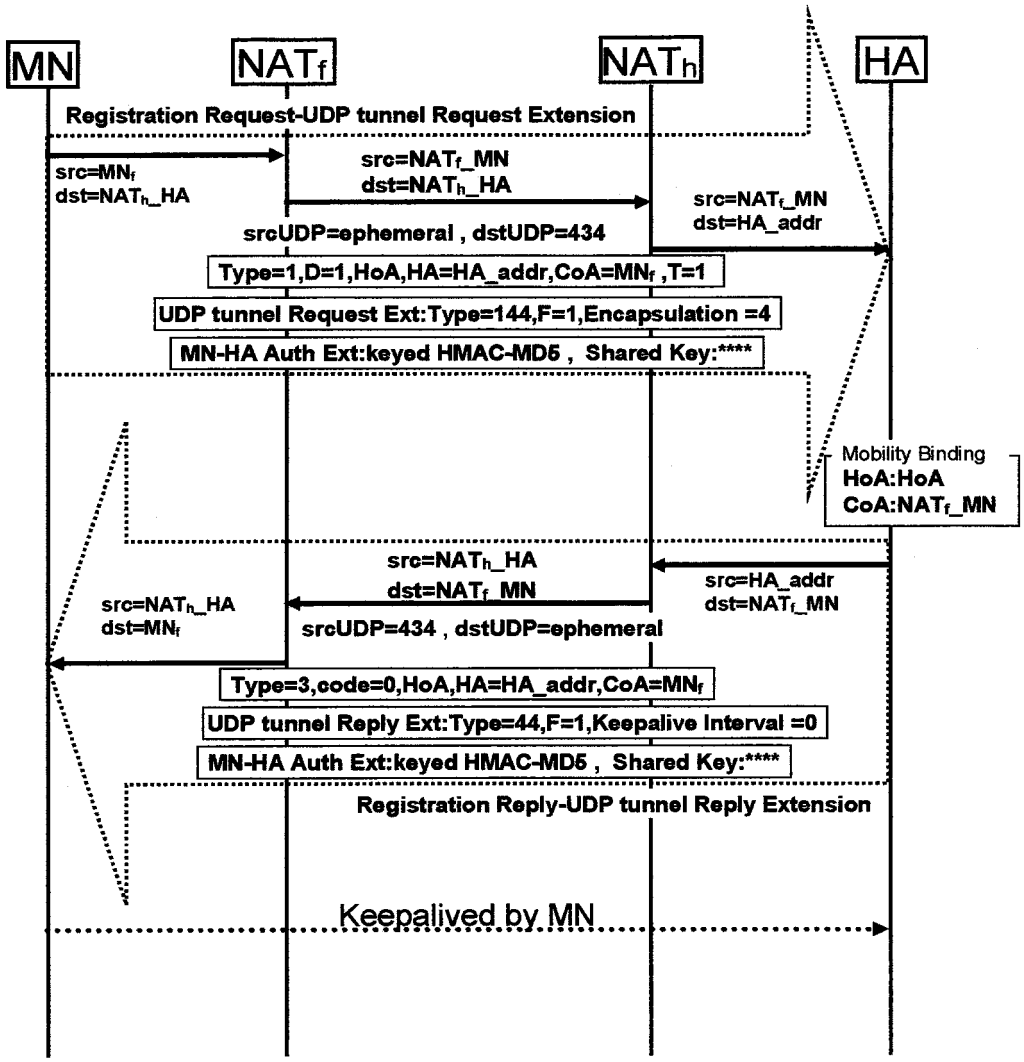

図3　Registration Request/Reply とトンネル要求(応答)拡張

また、図4では、MN と CN 間の通信において双方向トンネリングを用いてデータ通信を行う事例のメッセージシーケンスを示す。

HTTP 以外の通信プロトコルでも同様に Mobile IP での通信を行うことができる。

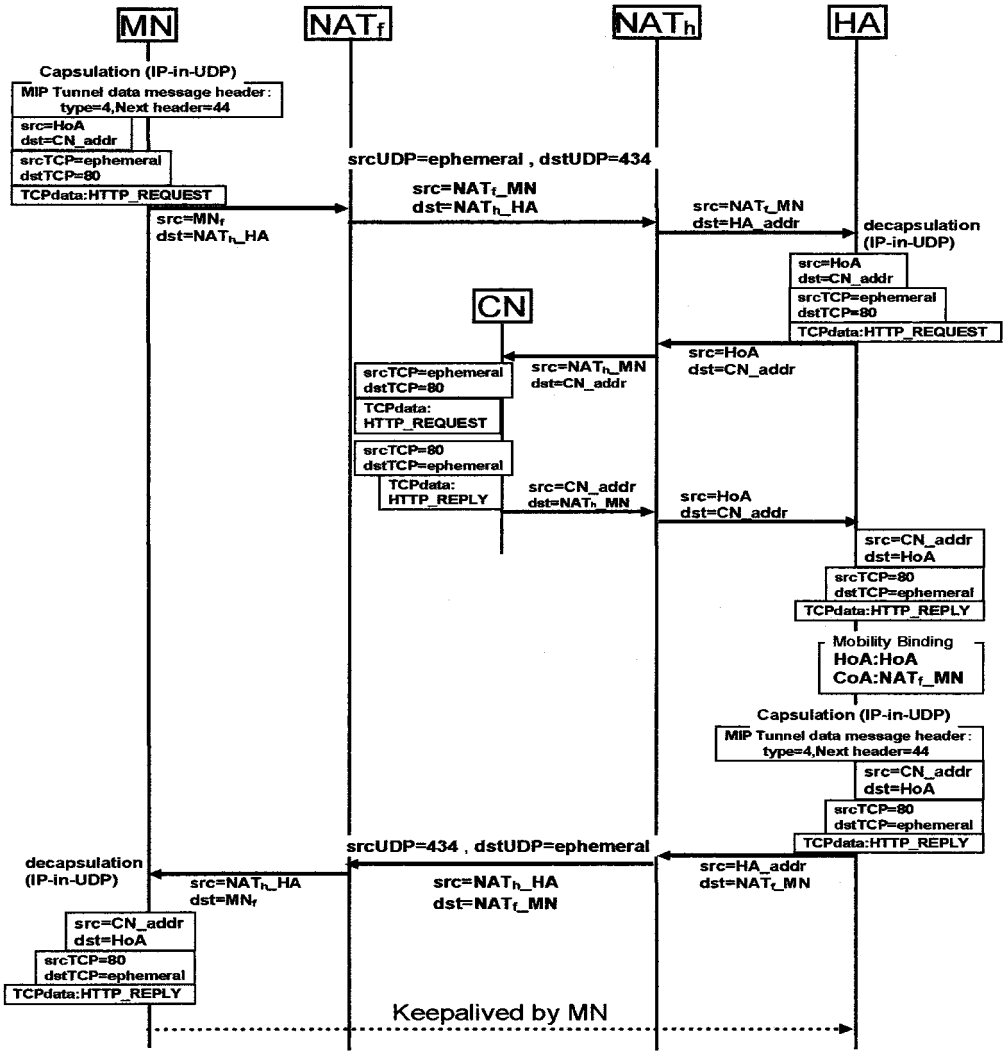

図 4　CN との双方向トンネリングによる HTTP 通信の例

4. おわりに

本稿で、筆者らは、プライベートネットワークに HA が配置されるような場合の Mobile IP の通信手順の設計検討を行った。今後は、この方式の評価を進める予定である。

参考文献

[1] C. Perkins, Ed., "IP Mobility Support for IPv4," RFC3344, Aug. 2002.

[2] H. Levkowetz and S. Vaarala, "Mobile IP Traversal of Network Address Translation (NAT) Devices," RFC 3519, Apr. 2003.

[3] 野地川 栄光、加藤 聰彦、伊藤 秀一, "プライベートネットワークに配置された Home Agent を用いる Mobile IPv4 手順の提案," 信学会, B-6-5 総合大会, Mar. 2007.

[4] G. Montenegro, Ed., "Reverse Tunneling for Mobile IP, revised," RFC 3024, Jan. 2001.