プライベートネットワーク内のノードを通信相手とした移動透過性の実現方式

鈴木　秀和[†a)]　　渡邊　晃[†]

A Realization Method of Mobility in Case that a Correspondent Node is in a Private Network

Hidekazu SUZUKI[†a)] and Akira WATANABE[†]

あらまし　外出先ノードからホームネットワーク内の情報家電機器などと自由に通信を行いたいという要求が高まっている．このような新たな通信スタイルにおいて，移動ノードが通信中に移動しても通信を継続できる移動透過性が実現できると有用性が更に高まると考えられる．従来の移動透過性プロトコルは，移動ノードが通信相手ノードと通信を開始できることを前提としている．しかし，IPv4 ネットワークにおいては通信相手ノードがプライベートネットワークに存在するとグローバルネットワーク側から NAT を越えて通信を開始することができない．本論文ではこの問題を解決するために，NAT 越え技術として提案済みの NAT-f（NAT-free protocol）を既存の移動透過性プロトコルと融合する方式を提案する．移動ノードは通信開始時に NAT-f によりプライベートネットワーク内の通信相手ノードと通信を開始し，移動時は既存の移動透過性プロトコルを用いて通信を継続する．NAT-f と移動透過性プロトコルは異なるタイミングで処理を行うため，互いに独立性を保持しつつ，かつ容易に組み合わせることができる．NAT-f と Mobile PPC を実装したシステムを評価した結果，所定の機能を実行できること，かつ通信開始時のオーバヘッド及びスループットの低下は十分に小さいことを確認した．

キーワード　移動透過性プロトコル，NAT 越え，プライベートネットワーク，NAT-f，Mobile PPC

1. まえがき

無線ネットワーク環境の普及により，通信ノードはあらゆる場所からネットワークに接続できるようになりつつある．しかし，IP ネットワークでは通信中にノードが移動すると IP アドレスが変化するため，通信が切断されてしまう．この課題を解決するために，通信中に移動しても通信に影響を与えない移動透過性が盛んに研究されている [1]．これまでの移動透過性の研究は将来のネットワークを見越して，IPv6 を前提としたものが多かった [2]〜[4]．しかし，IPv6 は当初予想していたような普及をしていない．また，IPv6 が普及を始めたとしても当分の間は IPv4 と IPv6 が混在することが想定されている．したがって IPv4 においても移動透過性プロトコルを実現することは，移動体通信の利便性向上の観点から大きな意義がある．

IPv4 ネットワークではアドレス枯渇問題のため，すべての移動ノード（以下 MN：Mobile Node）にグローバル IP アドレスを割り当てることは困難であり，プライベート IP アドレスを積極的に利用する必要がある．Mobile IP [5] においては，プライベート IP アドレスの利用を想定した方式がいくつか提案されている [6]〜[8]．また筆者らが提案している Mobile PPC（Mobile Peer-to-Peer Communication）[9] においても，MN にプライベート IP アドレスが割り当てられた場合の移動透過性が検討されている [10]．これらの提案は MN の通信相手ノード（以下 CN：Correspondent Node）がグローバルネットワーク上のサーバであることを想定しており，MN から CN に対して通信を開始後，MN がプライベートネットワークとグローバルネットワークの間を移動するケースを実現している．しかし，近年 DLNA（Digital Living Network Alliance）[11] に対応した情報家電機器が充実しつつあり，ユーザは

† 名城大学大学院理工学研究科，名古屋市
Graduate School of Science and Technology, Meijo University, 1–501 Shiogamaguchi, Tempaku-ku, Nagoya-shi, 468–8502 Japan
a) E-mail: h.suzuki@wata-lab.meijo-u.ac.jp

外出先からこれらのコンテンツを利用したいという要求が高まっている．この場合，従来の考え方とは逆に，CN がプライベートネットワークに存在し，MN がグローバルネットワークに存在することになる．このようなケースでは，CN の直前に NAT（Network Address Translator）が存在するため，一般には MN から CN へ通信を開始することができない．これは NAT 越え問題と呼ばれており，IPv4 における大きな課題となっている．したがって，従来の移動透過性技術だけでは上記のようなニーズに対応することができない．

本論文では筆者らが既に提案済みの NAT 越え技術 NAT-f（NAT-free protocol）[12] を既存の移動透過性プロトコルと組み合わせることにより，新たな通信ケースを実現する．NAT-f は，グローバルネットワーク上のノードと NAT が通信に先立ちネゴシエーションを行い，NAT マッピングを動的に生成する．その後の通信は NAT に割り当てられたマッピングアドレス(注1)を介してエンドエンド通信を確立する．グローバルネットワーク上の MN が通信中に移動すると，MN と所定の機器が移動透過性プロトコルを実行することにより通信を継続する．NAT-f と移動透過性プロトコルは処理タイミングが異なるため，独立性が高く，容易に組み合わせることができる．

以下，**2.** では既存技術の概要と IPv4 ネットワークにおける通信ケースを整理する．**3.** において NAT-f を Mobile PPC と Mobile IP に組み合わせた場合の通信手順を示し，提案手法の応用例について述べる．**4.** において NAT-f と Mobile PPC を組み合わせたシステムの実装概要を示す．**5.** において実装したシステムの評価及びセキュリティや対応可能な通信ケースに関する考察を行い，最後に **6.** でまとめる．

2. 既存技術の現状

2.1 IPv4 ネットワークにおける移動パターン

図 1 に MN の移動パターンの例を示す．従来の研究では，CN はグローバルネットワークに存在することが前提である．MN の移動前，移動後のネットワークの組合せにより以下の四つのパターンが検討されている．

［Pattern 1］ グローバルネットワークからグローバルネットワークへの移動

［Pattern 2］ グローバルネットワークからプライベートネットワークへの移動

［Pattern 3］ プライベートネットワークからグローバルネットワークへの移動

［Pattern 4］ プライベートネットワークから異なるプライベートネットワークへの移動

Pattern 1 は最も基本的な移動パターンである．Pattern 2，Pattern 3 は移動前若しくは移動後の通信経路上に NAT が介在することになる．Pattern 4 はプライベートネットワークが階層的に構築された環境での移動が想定される．

以下に，Mobile IP と Mobile PPC による上記四つの移動パターンの実現方法を示す．

2.2 Mobile IP による実現

図 2 に Mobile IP のシーケンスを示す．MN は移動しても変化しないホームアドレス（以後 HoA）を送信元として，CN と直接通信を行う．MN が通信中に移動して DHCP などにより新しい IP アドレス（共存気付アドレス CCoA）が割り当てられると，HA（Home Agent）に対して BU（Binding Update）を送信する．HA は MN の HoA と CCoA の対応関係を Mobility Binding Table に保存する．以後，MN から CN への通信パケットは CN へ直接送信される．CN からの返信は HA が代理受信し，CCoA を用いた IP-in-IP カプセル化により MN へ転送される．

Pattern 2 を想定した技術として，Mobile IP Traversal of NAT [6] がある．MN はプライベートネットワークに移動してグローバルネットワーク上の HA に BU を送信する際，オプションとして UDP トンネルを要求する．BU 処理を終えた後，MN は CN あてのパケットを UDP-in-IP による逆方向トンネルを形成して，HA へ送信する．HA はデカプセル化後，CN へ転送する．CN から MN への通信は上記と逆の手順により，HA を経由して送信される．

Pattern 3 の移動パターンを実現する方法として，Reverse Tunneling for Mobile IP [7] を利用する方法がある．これはネットワークトポロジーの整合性を図り，Ingress Filtering 問題を解決するための手法である．HA の機能を NAT に搭載し，かつこの技術を応用することにより，MN の HoA にプライベート IP アドレスを割り当てることができる．MN は HoA を送信元として CN と通信を開始するが，NAT により HoA から HA のグローバル IP アドレスに変換される．MN が移動して BU 処理を終えた後，MN から CN への通

(注1)：NAT でマッピングされた IP アドレスとポート番号の組．

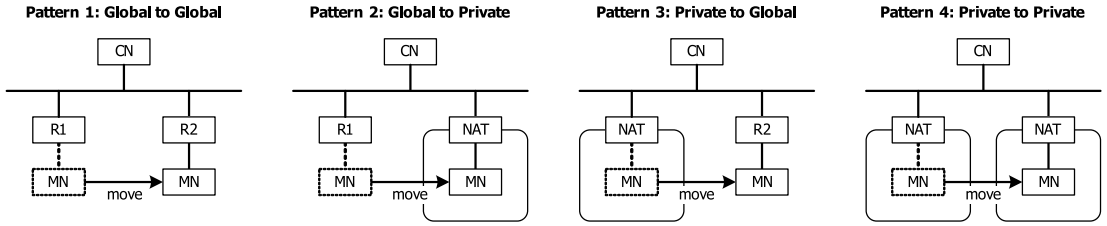

図 1　既存技術による移動パターン
Fig. 1　Mobility patterns based on existing technologies.

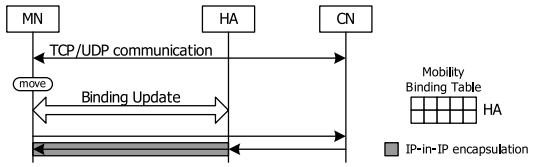

図 2　Mobile IP シーケンス
Fig. 2　Mobile IP sequence.

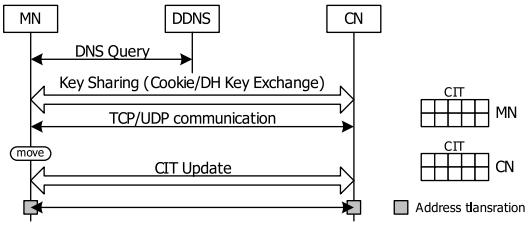

図 3　Mobile PPC シーケンス
Fig. 3　Mobile PPC sequence.

信パケットは逆方向トンネリングにより HA を経由して送信される．

文献 [8] では Pattern 4 の移動パターンを想定した方式が提案されている．NAT に独自機能を実装した GRA（Global Roaming Agent）と呼ぶ装置を導入し，配下にプライベートネットワークの Mobile IP 網を構築する．Mobile IP 網内に設置された HA や FA（Foreign Agent）と連携することにより，GRA は MN がどの Mobile IP 網に接続しているかを管理したり，Mobile IP 網間のパケット転送を行う．

2.3　Mobile PPC による実現

図 3 に Mobile PPC の基本シーケンスを示す．Mobile PPC は HA のようなプロキシ装置を必要としないエンドエンドの移動透過性プロトコルである．Mobile PPC では，通信の開始時は DDNS（Dynamic DNS）[13] により CN の IP アドレスを取得する．MN と CN は通信開始に先立ち，Cookie 交換及び Diffie-Hellman（以下 DH）鍵交換による 2 往復のネゴシエーションにより認証鍵を共有する [14](注2)．更に通信パケットのコネクション識別子 CID（Connection ID）(注3)を用いて，CIT（Connection ID Table）と呼ぶアドレス変換テーブルを IP 層に生成しておく．MN が通信中に移動して IP アドレスが変化した際，CN に対して移動前後の IP アドレスの関係を CIT Update（以下 CU）処理により直接通知し合い，CIT を更新する．CU 処理では通信開始時に共有しておいた認証鍵による相手認証を行う．その後両ノードは更新した CIT に基づいて，すべての通信パケットにアドレス変換処理を行う．これにより，IP 層より上位では移動前の IP アドレスとして処理される．その結果，上位層から IP アドレスの変化を隠ぺいすることができる．

Mobile PPC では Pattern 2 から Pattern 4 に対応するため，NAT 越え技術として知られている hole punching [15] の原理を導入する方法を提案している [10]．通信開始時の認証鍵共有処理または移動後の CU 処理において通信経路上に NAT の存在を確認すると，MN から CN に対して hole punching を実行し，NAT にマッピング情報を生成する．MN は CN からの応答により NAT の外側に割り当てられた IP アドレスとポート番号を取得する．これにより，CN は NAT のアドレス変換に対応した CIT を生成することができる．

2.4　新たなニーズへの対応と通信ケースの定義

近年，外出先からホームネットワーク内の情報家電機器と通信するための研究が盛んに行われている [16], [17]．このような場合，既存技術の前提とは異なり，CN はプライベートネットワーク内に存在することになる．

そこで本論文では MN の移動パターンに CN の位置

(注2)：認証鍵共有処理の詳細は付録を参照．
(注3)：TCP コネクション，または UDP ストリームを識別するための情報であり，送信元/あて先 IP アドレス，ポート番号とプロトコルタイプの五つの値の組からなる．

表 1　IPv4 ネットワークにおける通信ケースの定義
Table 1　Definition of communication case in IPv4 network.

MN の	CN の位置	
移動パターン	Global Network	Private Network
Pattern 1	Case 1	Case 5
Pattern 2	Case 2	Case 6
Pattern 3	Case 3	Case 7
Pattern 4	Case 4	Case 8

を組み合わせた通信ケースを定義する．表 1 に IPv4 ネットワークにおける通信ケースを示す．既存技術は CN がグローバルネットワークに存在することを前提としているため，Case 1 から Case 4 に対応している．Case 5 から Case 8 のような新たな通信ケースを実現するためには，MN から CN に対する NAT 越えを実現する必要がある．

3. NAT-f と移動透過性プロトコルの融合

本論文では CN 側の NAT 越え問題を解決するために，筆者らが既に提案済みの NAT-f を移動透過性プロトコルと融合することにより，新たな通信ケースを実現する．NAT-f は，通信開始ノードと NAT が連携することにより NAT 配下のノードに対して通信を開始できる技術である．プライベートネットワークに存在する既存のノードをそのまま利用できるという利点があり，本論文が対象とするホームネットワークへの導入に適している．NAT-f は Mobile IP，Mobile PPC のどちらとも共存することが可能であるが，ここでは Mobile PPC を中心にその方法を述べる．NAT-f は通信開始時，Mobile PPC は移動時にアドレス変換テーブルを生成する．そのため，両者の技術には独立性があり，大きな修正を加えることなく組み合わせることができる．

以下に，本論文で用いる記号を定義する．

- Gi; グローバル IP アドレス
- Pi; プライベート IP アドレス
- $FQDN_n$; ノード n の FQDN
- N_n; ノード n のホスト名
- $A : p$; IP アドレス A，ポート番号 p
- $proto$; プロトコルタイプ（TCP/UDP の区別）
- $S \rightarrow D$，$D \leftarrow S$; S から D への通信
- $S \leftrightarrow D$; S と D 間の通信
- $S \overset{T}{\Leftrightarrow} D$; 変換テーブル T に基づく S から D，または D から S へのアドレス変換

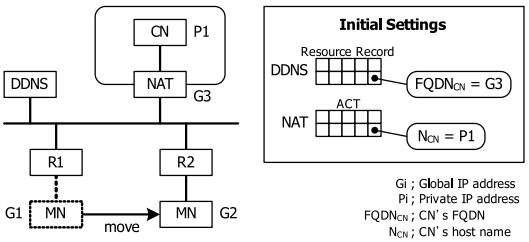

図 4　システム構成と事前設定
Fig. 4　System configuration and initial settings.

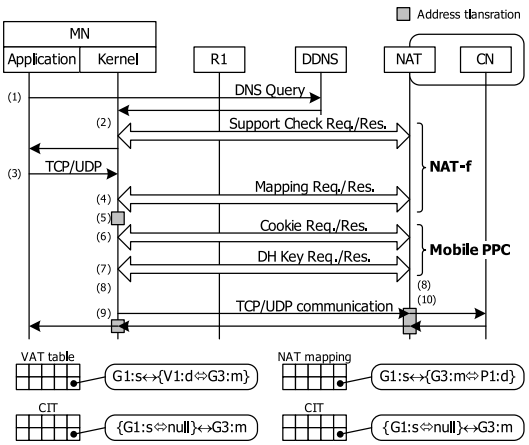

図 5　MN が通信を開始するときの NAT-f シーケンス
Fig. 5　NAT-f sequence when MN starts communication.

3.1 システム構成

図 4 に本論文が想定するシステム構成を示す．グローバル IP アドレス $G1$ をもつ MN が，特定のホームネットワーク内部に存在する CN へ通信を開始する．その後，MN は CN と通信中にルータ R1 配下のネットワークから R2 の配下ネットワークに移動して，新しいグローバル IP アドレス $G2$ を取得したことを想定する．MN と NAT はそれぞれ NAT-f と Mobile PPC を実装しており，CN はこれら機能を有さない一般ノードでよい．NAT-f を利用するための必要な事前設定として，DDNS サーバには $FQDN_{CN}$ と NAT のグローバル IP アドレス $G3$ の対応関係が，NAT には N_{CN} と CN のプライベート IP アドレス $P1$ の対応関係が既に登録されているものとする．

3.2 NAT-f による通信開始手順

図 5 に通信開始時における NAT-f シーケンスを示す．以下に，MN が NAT-f により CN と通信を確立するまでの手順について述べる．

（1） MN は DDNS サーバに対して CN の

$FQDN_{CN}$ に対応する IP アドレスを要求する．DDNS サーバは DNS リソースレコードを検索し，$FQDN_{CN}$ に対応する IP アドレス $G3$ を応答する．

（2） MN は受信した DNS 応答を IP 層に一時待避させてから，DNS 応答に記載されている IP アドレス $G3$ あてに Support Check Request を送信する．あて先ノードまたはあて先 NAT が NAT-f に対応していれば Support Check Response が応答される．MN は Support Check Response を確認し，あて先が NAT-f 対応 NAT であれば待避させた DNS 応答に記載された IP アドレスを仮想 IP アドレス $V1$ に書き換え，アプリケーションには CN の IP アドレスを $V1$ として通知する．ここで仮想 IP アドレスとは外部ノード（MN）が NAT 配下の内部ノード（CN）を一意に特定するために割り当てるアドレスであり，$FQDN_{CN}$ から生成する．これにより MN の IP 層では，送信パケットのあて先仮想 IP アドレスから NAT 配下のどのノードと通信したいのかを判断することが可能になり，CN との通信に必要な NAT マッピング情報を NAT に生成させることができる．仮想 IP アドレスを導入することにより，NAT 配下の複数のノードと同時に通信することが可能となる．

なお，あて先が NAT-f 対応 NAT ではない場合(注4)，待避させた DNS 応答をそのまま上位層へ渡し，取得した IP アドレスをそのままアプリケーションへ通知する．この場合，CN がグローバルネットワークに存在する場合が想定される．

（3） MN のアプリケーションは仮想 IP アドレスをあて先として送信処理を行い，下記パケットが IP 層に渡される．

$$G1 : s \rightarrow V1 : d \quad [proto]$$

MN は IP 層において，送信パケットのあて先が仮想 IP アドレスの場合，パケットの CID（$G1$，s，$V1$，d，$proto$）を用いて VAT（Virtual Address Translation）テーブルと呼ぶアドレス変換テーブルを参照する．VAT テーブルとは，仮想 IP アドレスと NAT のマッピングアドレスとの変換関係を示すテーブルで，以後の NAT-f マッピング処理完了時に生成される．MN が CN に初めて通信する場合は VAT テーブルに該当するエントリがないため，マッピング処理を開始する．

ここで，送信パケットのあて先が仮想 IP アドレスでない場合は，VAT テーブルの参照や以下のマッピング処理など NAT-f 一連の処理を行わない．Support Check Response により CN が Mobile PPC に対応していることが分かったら（6）の Mobile PPC 認証鍵共有処理へ移行し，対応していない場合は（9）の処理へ移行して通信を開始する(注5)．

（4） MN は送信しようとしていた TCP/UDP パケットをカーネル内に一時待避し，Mapping Request を NAT へ送信する．Mapping Request には待避したパケットの CID と，仮想 IP アドレスに対応する CN のホスト名 N_{CN} が記載される．NAT は Mapping Request を受信すると，通知された CID と N_{CN} に対応する IP アドレスから

$$G1 : s \leftrightarrow \{G3 : m \overset{NAT}{\Longleftrightarrow} P1 : d\} \quad [proto]$$

のように NAT マッピング情報を生成する．これは CN のポート番号 d と NAT のポート番号 m がマッピングされたことを示しており，CN から MN へ通信を開始した場合に NAT で生成されるマッピング情報と同様のものである．NAT は $G3 : m$ をマッピングアドレスとして Mapping Response に記載して MN へ応答する．

MN は Mapping Response を受信すると，仮想 IP アドレスとマッピングアドレスの変換関係を示すエントリ

$$G1 : s \leftrightarrow \{V1 : d \overset{VAT}{\Longleftrightarrow} G3 : m\} \quad [proto]$$

を生成し，VAT テーブルに格納する．その後，先ほど待避した TCP/UDP パケットを復帰させ，マッピング処理を完了する．

（5） 復帰した TCP/UDP パケットは VAT テーブルに基づいて，あて先 IP アドレス・ポート番号が $V1 : d$ から $G3 : m$ に変換される．ここで，提案方式では Mobile PPC と組み合わせるため，Mobile PPC の通信開始時の処理，すなわち認証鍵共有処理を行う．認証鍵共有処理は通常の Mobile PPC と同じだが，VAT テーブルに基づいて変換された通信パケットをトリガとして実行する点が異なる．

(注4)：Support Check Request は ICMP Echo Request の上で定義されているため，あて先ノードまたはあて先 NAT が NAT-f に対応していない場合は Support Check Request とメッセージデータが同じ ICMP Echo Reply が応答される．MN は Support Check Request の応答の違いにより，あて先が NAT-f 対応 NAT か否かを判断する．
(注5)：Mobile PPC の対応確認方法は **4.1** を参照．

（6） MN はアドレス変換された TCP/UDP パケットを再度カーネル内に待避してから，NAT へ Cookie Request を送信して Cookie 交換を行う．MN は NAT からの Cookie Response を受信後，待避していたパケットを復帰させる．以上の処理を終えると，MN は TCP/UDP 通信を開始し，（9）の処理へ移行すると同時に，そのバックエンドで（7）の DH 鍵交換処理を実行する．

（7） MN は DH 秘密鍵及び DH 公開鍵を生成し，DH Key Request により DH 公開鍵を NAT へ送信する．NAT も同様に DH 秘密鍵及び DH 公開鍵を生成後，DH Key Response により DH 公開鍵を応答する．

（8） MN と NAT は DH 鍵交換後，自身の DH 秘密鍵と相手の DH 公開鍵から認証鍵を生成する．

（9） MN は移動前の CID 情報として下記のような CIT を生成してから，復帰したパケットを NAT へ送信する．

$$\{G1 : s \overset{CIT}{\Longleftrightarrow} null\} \leftrightarrow G3 : m \quad [proto]$$

ここで，*null* はアドレス変換を行わないことを意味する．

（10） NAT は MN からのパケットを受信後，MN と同じ内容の CIT を生成する．その後，（4）で生成した NAT マッピング情報に基づいて，当該パケットのあて先 IP アドレス・ポート番号を $G3 : m$ から $P1 : d$ に変換し，CN へ転送する．

以上の処理により，MN から CN への通信開始が完了する．ここまでのアドレス変換処理による TCP/UDP パケットの IP アドレス及びポート番号の遷移を図 6 にまとめる．CN から MN への応答パケットは上記と逆の変換処理を行う．すなわち，CN から MN への応答パケット

$$P1 : d \longrightarrow G1 : s \quad [proto]$$

は NAT 内の NAT マッピングに基づいて，送信元が $G3 : m$ に変換される．その後，MN の IP 層で VAT テーブルに基づいて送信元が $V1 : d$ に変換される．MN が移動前であるため，CIT に基づくアドレス変換は行われない．以後，上記アドレス変換処理が TCP/UDP パケット送受信ごとに繰り返し実行される．

3.3 NAT-f と Mobile PPC の融合による通信継続手順

図 7 に MN が R2 配下へ移動した後の通信シーケンスを示す．MN は CN と通信中に移動した場合は，既存の Mobile PPC による CU 処理を実行した後，VAT テーブル，NAT マッピング及び CIT に基づく 3 種類のアドレス変換を同時に実行する．以下に，MN と CN が通信を継続するまでの手順について述べる．

（1） MN は別のネットワークに移動したことを検知すると，DHCP 処理を実行して新しい IP アドレス $G2$ を取得する．

（2） アドレス取得後，MN は NAT に対して CU 処理を行う．NAT に送信する CU Request には移動前 IP アドレス $G1$ と移動後 IP アドレス $G2$ が記載され，通信開始時に共有した認証鍵を用いて署名を付加する．CU Request を受信した NAT は認証処理を終えた後，CIT を

$$\{G1 : s \overset{CIT}{\Longleftrightarrow} G2 : s\} \leftrightarrow G3 : m \quad [proto]$$

のように更新してから，CU Response を応答する．

MN は CU Response を受信したら，NAT と同様に自身の CIT を更新する．以上により，CU 処理は完了する．

（3） 上位層から渡された TCP/UDP パケット

$$G1 : s \rightarrow V1 : d \quad [proto]$$

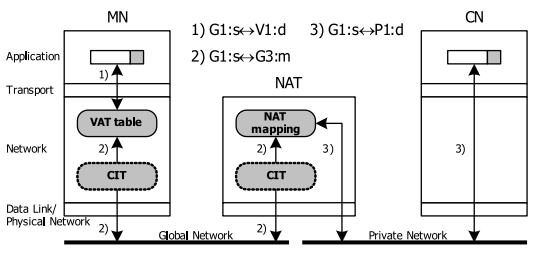

図 6 MN 移動前における IP アドレス/ポート番号の遷移
Fig. 6 IP address/port number transition before MN moves.

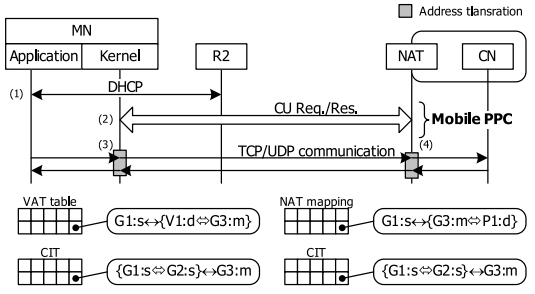

図 7 MN 移動後における Mobile PPC シーケンス
Fig. 7 Mobile PPC sequence after MN moves.

は，VAT テーブルに基づくアドレス変換，及び CIT に基づくアドレス変換が行われる．すなわち，上記パケットは送信元が移動前から移動後の IP アドレスへ，あて先が仮想 IP アドレスからマッピングアドレスへ変換され，最終的に

$$G2 : s \rightarrow G3 : m \quad [proto]$$

として NAT へ送信される．

（4） NAT は受信パケットに対して，CIT に基づくアドレス変換及び NAT に基づくアドレス変換が行われる．すなわち，上記パケットは送信元が MN の移動後から移動前の IP アドレスへ，あて先がマッピングアドレスから CN のプライベート IP アドレスへ変換され，最終的に

$$G1 : s \rightarrow P1 : d \quad [proto]$$

として CN へ転送される．

以上の処理により，MN の上位アプリケーション，NAT アドレス変換処理部及び CN は，移動が発生して MN の IP アドレスが変化したことに気づくことなく，通信を継続することができる．ここまでのアドレス変換処理による TCP/UDP パケットの IP アドレス及びポート番号の遷移を図 8 にまとめる．なお，CN から MN への通信は通信開始時と同様に上記と逆の手順でアドレス変換を行う．すなわち，NAT 内の NAT マッピング情報に基づいて送信元が $P1 : d$ から $G3 : m$ に，更に CIT に基づいてあて先が $G1$ から $G2$ に変換される．その後，MN の IP 層で CIT に基づいてあて先が $G2$ から $G1$ に，VAT テーブルに基づいて送信元が $G3 : m$ から $V1 : d$ に変換される．

3.4 Mobile IP への応用

図 9 に NAT-f と Mobile IP を組み合わせたシーケンスを示す．MN の HoA を $G1$，移動後の CCoA を $G2$ とし，MN と NAT に NAT-f 機能が実装されているものとする．MN は通常の NAT-f の手順により，下記の VAT テーブル及び NAT マッピングを生成後，VAT テーブルに基づくアドレス変換を行い CN への通信を開始する．

$$G1 : s \leftrightarrow \{V1 : d \overset{VAT}{\Longleftrightarrow} G3 : m\} \quad [proto]$$
$$G1 : s \leftrightarrow \{G3 : m \overset{NAT}{\Longleftrightarrow} P1 : d\} \quad [proto]$$

NAT は上記マッピング情報に従ってアドレス変換を実行し，MN からの通信パケットを CN へ転送する．

MN が CN と通信中に別のネットワークに移動すると，通常の Mobile IP の手順により HA と BU 処理を行い，Mobility Binding Table を登録する．MN から CN への通信パケットは，送信元 IP アドレスが常に HoA であるため，これを受信した NAT は MN 移動前に生成された NAT マッピングの情報に従って CN へ転送することができる．CN からの応答パケットはあて先 IP アドレスが HoA となるため，HA が代理受信する．その後，HA は Mobility Binding Table の情報に基づいて，受信パケットを IP-in-IP カプセル化してから MN の CCoA あてへ転送する．上記パケットを受信後，MN はデカプセル化してから VAT テーブルに基づいて送信元を NAT のマッピングアドレス $G3 : m$ から仮想 IP アドレス $V1 : d$ へアドレス変換して上位層へ渡す．

以上の手順により，Mobile IP においても NAT-f を組み合わせることにより CN がプライベートネットワークに存在しても通信の開始及び継続を実現できる．NAT 及び CN は通信相手となる MN のアドレスを HoA として認識しているため，MN 移動後のネットワークに FA が設置されている場合や，Reverse

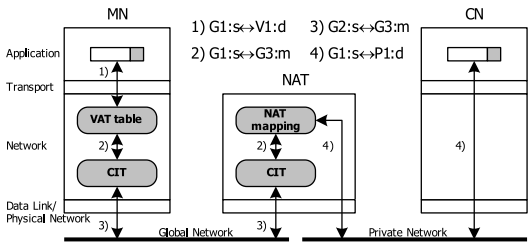

図 8 MN 移動後における IP アドレス/ポート番号の遷移
Fig. 8 IP address/port number transition after MN moves.

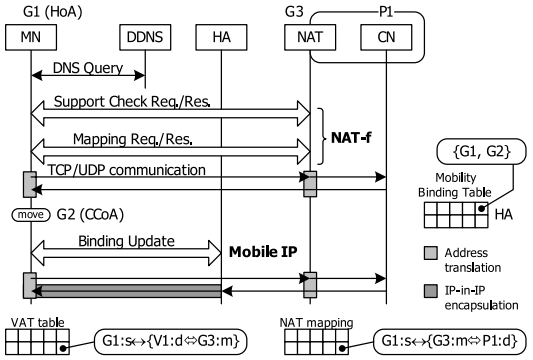

図 9 Mobile IP と NAT-f を組み合わせたシーケンス
Fig. 9 Sequence that combines Mobile IP and NAT-f.

Tunneling を行う場合においても，NAT-f を適用することが可能である．

3.5 提案手法の応用例

移動透過性プロトコルは，これまで述べてきたホスト単位の移動透過性を実現する技術のほかに，ネットワーク単位の移動透過性を実現する技術がある．ネットワーク単位の移動透過性技術として，Mobile IP をベースとした NEMO（Network Mobility）[18], [19] や，Mobile PPC をベースとした Mobile NPC [20] がある．これらは移動透過性プロトコルを実装したルータ MR（Mobile Router）の配下にモバイルネットワークを形成し，移動透過性プロトコルを実装しない一般のノード LFN（Local Fixed Node）を収容する．MR が移動して IP アドレスが変化しても，配下の LFN はグローバルネットワーク上の CN と確立していた通信を継続できる．NEMO は Mobile IP の拡張として定義されており，プロトコル上の違いは NEMO を運用することを示すフラグと，モバイルネットワークの情報をやり取りするためのオプションが制御情報に追加されたことである [21]．MR と HA が扱うアドレスに関する情報は，MR の HoA と気付アドレス（CoA），及びモバイルネットワークのプレフィックス情報である．これらは MR 側から見るとすべて送信元側の情報であり，あて先側の情報は含まれない．一方，提案方式特有のアドレスである仮想 IP アドレスは，MR 側から見るとあて先側の情報として用いられる．したがって，NAT-f は Mobile IP と同様に NEMO 固有の制御に影響を及ぼすことなく組み合わせて利用することができる．提案方式を NEMO に応用する場合は，MR に NAT-f を実装して仮想アドレス変換処理などを行う．これにより，LFN はプライベートネットワークに存在する CN との通信を開始，継続することができる．

IPv4 ネットワークは当分の間，IPv6 ネットワークと混在することが想定される．このような混在したネットワークにおいて移動透過性を実現する技術として DSMIP（Dual Stack Mobile IP）[22] がある．DSMIP は MN が IPv4/IPv6 の両者に対応することにより，IPv6 ネットワーク，IPv4 グローバルネットワーク，及び IPv4 プライベートネットワークの間を移動することを実現しており，IP Mobility の普及に適した解決策である．しかし DSMIP においても，CN は IPv6 ノードであること，または IPv4 グローバルアドレスが割り当てられていることを前提としており，IPv4 プライベートネットワーク内のノードと通信を開始することができないという課題が残されている．このようなシステムにおいても，提案方式を応用することにより上記課題を解決できると考えられる．

このように，提案方式は既存の多くの移動透過性に関するシステムに適用可能である．

4. 実　　装

NAT-f と Mobile PPC を組み合わせた方式を確認するために，FreeBSD 6.1-RELEASE を用いてプロトタイプシステムを実装した．以下に MN 側と NAT 側の実装概要をそれぞれ示す．

4.1 MN の実装概要と移動検知処理

図 10 に MN におけるカーネルモジュールの実装を示す．NAT-f モジュール及び Mobile PPC モジュールは IP 層に実装され，IP 入出力関数 `ip_input()`，`ip_output()` から呼び出される．特にパケット送信時は `ip_output()` においてルーチング処理が行われるが，両モジュールはそれ以前に呼び出されて所定の動作を行う．

3. に示した処理手順を可能とするため，NAT-f モジュールの呼出しインタフェースを Mobile PPC 呼出しインタフェースより上位になるように変更した．このような変更は両モジュールが `ip_input()`，`ip_output()` から独立した実装となっているため，容易に実現可能である．NAT-f と Mobile PPC の主処理は従来のまま利用するが，融合するにあたり以下の機能追加・修正を施した．NAT-f モジュールのネゴシエーション処理に Mobile PPC 対応フラグを設定する機能を追加した．本論文のように両モジュールが融合されている

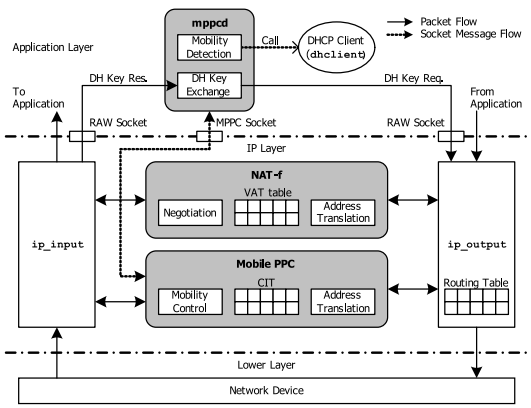

図 10　MN におけるカーネルモジュールの実装
Fig. 10　Implementation of kernel modules in MN.

場合は Support Check Response にフラグを設定し，NAT-f モジュールの処理を完了したら Mobile PPC モジュールが呼び出される．Mobile PPC モジュールが実装されていない場合はフラグが設定されていないため，NAT-f 単体の処理だけが実行される．なお，MN の IP レベルにおける通信相手が NAT-f に対応していない場合は **3.2**（2）の DNS 書き換え処理を行わないため，以後の NAT-f 処理は実行されない．このような工夫により，NAT-f と Mobile PPC を融合した場合だけでなく，NAT-f，Mobile PPC 単体の機能でも動作するようにした．

Mobile PPC の DH 鍵交換処理はユーザランドで動作するデーモン `mppcd` が行う．Cookie Response を受信した MN は，Mobile PPC カーネルモジュールから MPPC socket(注6) を通じて `mppcd` に DH 鍵交換処理を指示する．`mppcd` は RAW socket を用いて DH Key Request/Response を送受信する．認証鍵を生成後，MPPC socket を通じて Mobile PPC カーネルモジュールに登録する．なお，DH 鍵交換処理は OpenSSL [23] を利用し，RFC3526 [24] と RFC4306 [25] で定義されている DH グループ 1，2，5 及び 14 の素数と原始根がシステム共通のパラメータとして実装した(注7)．

IPv4 ネットワークでは，IPv6 ルータが定期的に送信する RA（Router Advertisement）のような仕組みがないため，MN は移動を検知する手段がない．Mobile IPv4 では FA からのエージェント広告により移動の検知は可能であるが，Mobile PPC では FA のような装置を想定していないため，MN が自律的に解決する手段が必要となる．また，従来の Mobile PPC は IP アドレス取得後に行うアドレス重複確認の終了と同時に，カーネルの ARP 関数から CU 処理を開始する仕組みであった．そこで IP 入出力関数以外のカーネル関数を変更することなく，かつ移動を自律的に検知して CU 処理をカーネルモジュールに指示する移動検知モジュールを `mppcd` に実装した．

図 11 に移動検知処理の仕組みを示す．`mppcd` は定期的にネットワークデバイスのリンク状態を監視し，ネットワークに接続したと判断したらルーチングテーブルから取得したゲートウェイの IP アドレスを用いて ping を実行する．一定時間内に応答を受信できなかった場合，異なるネットワークに接続したと判断し，`dhclient`(注8) を実行する．以上の処理が完了したら，Mobile PPC カーネルモジュールに対して CU 処理を指示する．Mobile PPC カーネルモジュールは `mppcd`

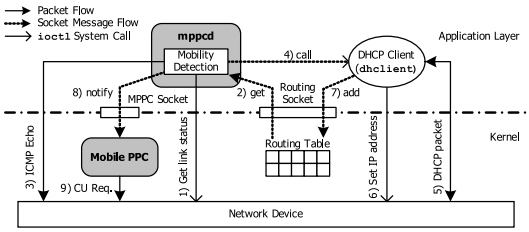

図 11　移動検知処理の仕組み
Fig. 11　Mechanism of mobility detection operation.

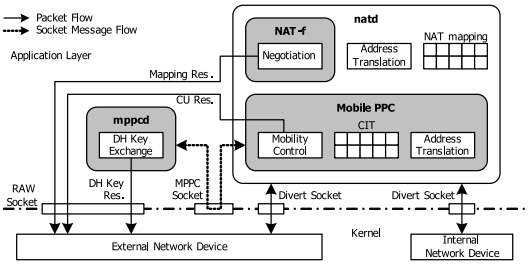

図 12　natd の拡張によるモジュールの実装
Fig. 12　Implementation of modules by extended of natd.

からの指示を受けると，CU Request を生成して該当する CN へ送信する．これにより，Mobile PPC モジュールのカーネル依存度を少なくし，かつ自律的に移動検知から CU 処理を実行することを可能とした．

4.2　natd の拡張

図 12 に NAT-f と Mobile PPC に対応した NAT のモジュール実装の概要を示す．これまで NAT-f 及び Mobile PPC の機能はカーネルに実装していたが，今回，アプリケーションレベルで動作する `natd`(注9) を拡張することにより実現した．

`natd` は Divert socket を経由して送受信パケットのアドレス変換を行う．受信パケットが NAT-f または Mobile PPC に関するメッセージであれば，各モジュールに処理を移す．Mapping Request の場合，`natd` のマッピングを行う処理を呼び出し，マッピング情報を生成後，MN あての Mapping Response を Raw socket 経由で送信する．Mobile PPC に関するメッセージの場合は，Mobile PPC モジュールを呼び出して処

(注6)：ユーザランドと Mobile PPC カーネルモジュール間のデータ受渡しを実現するために実装されたソケットインタフェース．
(注7)：素数のサイズは順に 768，1024，1536，2048 bit であり，原始根は 2 である．
(注8)：FreeBSD に搭載されている DHCP クライアント．IP アドレス，ゲートウェイ情報の設定からアドレス重複確認を行う．
(注9)：FreeBSD に搭載されている NAT アプリケーション．

理を行い，NAT-f と同様に各 Response メッセージを RAW socket 経由で送信する．

なお，NAT のマッピング情報と CIT を統合することも可能だが，今後の各プロトコルの拡張を考慮し，あえて各モジュールの独立性を確保した．この方法では NAT は MN 移動後の通信パケットに対して，CIT と NAT によるアドレス変換を 2 回行うことになる．

4.3 アドレス変換に伴うチェックサム

VAT テーブル及び CIT に基づくアドレス変換処理は，IP アドレスとポート番号のみを変換する．IP ヘッダ及び TCP/UDP ヘッダのチェックサムは差分計算により修正する．これは NAT のアドレス変換と原理は同様であり，RFC3022 [26] に準じた演算を行う．

5. 評価と考察

MN と NAT で行われるアドレス変換処理が，MN と CN のエンドツーエンドのスループットに与える影響を明らかにするために，iperf [27] を用いて TCP/UDP スループットを測定した．また，通信開始時に発生するオーバヘッド及び `mppcd` による移動検知から通信継続までに要する時間，すなわち通信断絶時間を測定した．

測定環境は図 4 に示す構成とし，NAT，DDNS サーバ及び R1/R2 をスイッチで接続した．表 2 に各装置の仕様を示す．MN の移動は UTP ケーブルを R1 から R2 につなぎ直すことでエミュレートした．Cookie と認証鍵の生成に用いるハッシュ関数には MD5 を使用し，DH 鍵交換における DH グループは Group 1 とした．

5.1 スループット性能

iperf により MN から CN に対して TCP トラヒックを 60 秒間送信した．NAT-f と Mobile PPC を実装したシステムにおいて，移動前と移動後のスループットを測定した．また比較のため，同一装置により NAT-f と Mobile PPC を実装していない通常のシステムにおいても測定した．この場合は NAT にあらかじめ静的マッピングを設定し，MN が CN へ通信を開始できるようにした．

表 3 に TCP スループット測定結果を示す．未実装時のスループットが 69.3 Mbit/s であったのに対して，実装時の移動前は 69.1 Mbit/s，移動後は 67.9 Mbit/s であった．実装時の移動前は MN において VAT テーブルに基づくアドレス変換処理が加わるが，スループットに対する影響はほとんどないといえる．実装時の移動後は，更に MN と NAT において CIT に基づくアドレス変換が加わるため，未実装時のスループットから約 2%低下していた．低下の要因は NAT 装置における CIT のアドレス変換処理にあることが分かった．今回使用した NAT 装置のプラットホームは FreeBSD ではサポートされておらず，本来の性能を発揮していないことが原因であった．

以上の結果より，NAT-f と Mobile PPC を組み合わせても，スループットの低下は十分に小さく，実用上問題ないといえる．

5.2 通信開始時のオーバヘッド

表 4 に通信開始時に発生するオーバヘッドとその内訳を示す(注10)．MN が最初の TCP/UDP パケットを送信する際，カーネルに一時待避させてから実際に送信されるまでに行われる処理は，表 4 のうち NAT-f による DNS 応答書換え，マッピング処理，及び Mobile

表 2 装置仕様
Table 2 Device specifications.

	MN	CN	NAT
CPU	Pentium M 1.73 GHz	Core2 U7600 1.20 GHz	Geode LX800 500 MHz
Memory	512 MByte	2037 MByte	256 MByte
NIC	100Base-TX	100Base-TX	100Base-TX
OS	FreeBSD 6.1	Windows Vista	FreeBSD 6.1

表 3 Iperf による TCP スループット測定値
Table 3 TCP throughput on the proposal method using iperf.

	スループット
NAT-f/Mobile PPC 未実装時	69.3 [Mbit/s]
NAT-f/Mobile PPC 実装時（移動前）	69.1 [Mbit/s]
NAT-f/Mobile PPC 実装時（移動後）	67.9 [Mbit/s]

表 4 MN の通信開始時に発生する処理時間の内訳
Table 4 Details of overhead when MN starts communication.

処理内容	該当箇所	処理時間
a) DNS 応答書換え	**3.2** (1)〜(2)	0.45 [ms]*1
b) マッピング処理	**3.2** (3)〜(5)	0.61 [ms]*2
c) Cookie 交換	**3.2** (6)	0.73 [ms]*2
d) DH 鍵交換	**3.2** (7)	54.51 [ms]*2
e) 認証鍵生成（MN）	**3.2** (8)	5.40 [ms]
f) 認証鍵生成（CN）	**3.2** (8)	38.92 [ms]
通信開始までの総オーバヘッド（a+b+c）		1.79 [ms]

*1 処理時間 + 1RTT（RTT は MN〜DDNS 間の RRT）
*2 処理時間 + 1RTT（RTT は MN〜NAT 間の RRT）

(注10)：表 4 及び表 5 における数値は実験環境における小さな RTT (Round Trip Time) 値によるものである．実環境における RTT の値については例えば文献 [28] を参照のこと．

PPC の Cookie 交換の合計処理である．したがって，通信開始までのオーバヘッドは上記処理時間の合計，すなわち 1.79 ミリ秒となる．認証鍵共有処理の後半部分（DH 鍵交換と認証鍵生成）は TCP/UDP 通信のバックエンドで行われるため，通信開始時のオーバヘッドには含まれない．

上記結果から分かるように，**3.4** に示した NAT-f と Mobile IP を組み合わせたシステムにおいても，通信開始時に発生するオーバヘッドは十分許容できる範囲であるといえる．

5.3 通信断絶時間

表 5 に移動時の通信断絶時間とその内訳を示す(注10)．表中の処理内容はそれぞれ下記の間の処理である．

- ネットワーク移動：UTP ケーブル抜線〜挿線
- 移動検知：リンク確立判断〜ping タイムアウト
- IP アドレス取得：DHCP Discover 送信〜IP アドレス設定
- アドレス重複確認：Gratuitous ARP 送信〜タイムアウト
- CU 処理：CU Request 送信〜CIT 更新

通信断絶時間の合計は 4.51 秒であった．このうち，ネットワークの移動に 1.64 秒を要しているが，実際は無線 LAN における L2 ハンドオーバに該当するため，50〜400 ミリ秒になると推測される [29]．上記時間を除いた通信断絶時間に着目すると，DHCP によるアドレス取得と Gratuitous ARP によるアドレス重複確認の合計が 97.6%を占める結果となった．一方，`mppcd` やカーネルモジュールによる CU 処理，すなわち提案方式特有の処理時間は十分に短いことが分かる．

上記の結果より，移動に伴うパケットロスを減らすためには，アドレス取得に関する処理時間を抑えることが課題となる．この課題については文献 [30] において別途検討済みである．

表 5　通信断絶時間の内訳
Table 5　Details of communication break time.

処理内容	該当箇所	処理時間	
ネットワーク移動	**3.3** (1) 手動	1.64	[s]
移動検知	**3.3** (1) `mppcd`	28.70	[ms]
アドレス取得	**3.3** (1) `dhclient`	2.11	[s]*1
アドレス重複確認	**3.3** (1) Kernel	0.69	[s]
CU 処理	**3.3** (2) Mobile PPC	41.26	[ms]*2
総通信断絶時間		4.51	[s]

*1 処理時間 + 2RTT（RTT は MN〜R2 間の RRT）
*2 処理時間 + 1RTT（RTT は MN〜NAT 間の RRT）

5.4 セキュリティに関する考察

攻撃者は Mapping Request や CU Request に記載されている MN の送信元 IP アドレスを改ざんすることにより，セッションのハイジャックを試みることが考えられる．Mobile PPC では MN と NAT は通信開始時に認証鍵を共有しているため，CU Request/Response に署名を付加することにより，メッセージ完全性を保証できる．Mobile PPC の安全性は上記認証鍵の共有方法に依存する．本論文では自宅や友人などある特定のネットワークに対してアクセスすることを想定としているため，MN と NAT との間で事前に秘密鍵を共有することが可能である．したがって，MN と NAT は認証を伴った認証鍵共有を実行することが可能であり，中間者攻撃を防止できる．NAT-f の Mapping 処理においても MN と NAT が事前共有鍵を保持することにより，Mapping Request/Response の暗号化や認証を行うことが可能である．

事前共有鍵に基づくシステムは導入が比較的容易であるが，鍵の管理が煩雑になったり，不特定の相手と鍵を共有することが困難であるなどの課題がある．提案方式の適用対象を不特定なネットワークにまで拡張するには，PKI（Public Key Infrastructure）によるディジタル署名認証や公開鍵認証などの手法を利用する必要がある．

5.5 各通信パターンへの対応

移動透過アーキテクチャの実用性を評価する上で，対応可能な通信ケースの広さは重要な指標と考えられる．本論文では **2.4** に示した Case 5 の実現方法を取り上げたことになる．提案方式が他の通信ケースを実現する可能性について考察した．

Mobile PPC では **2.3** で述べたように，hole punching 処理を導入することにより Case 2 から Case 4 を実現できる手法を提案済みである．提案方式は移動透過性プロトコルの機能をそのまま利用しているため，そのまま Case 2 から 4 に対応することができる．Case 6 はグローバルネットワークからプライベートネットワークへの移動のため，Case 5 とは移動後の処理だけが異なる．移動後の処理に着目すると，Mobile PPC に関する処理しか行わない．したがって，Case 2 と同様の処理を行うことにより Case 6 は実現可能である．Case 7 については，文献 [10] の hole punching の手法を NAT-f のマッピング処理に対して導入することにより，実現可能であると考えられる．Case 8 は Case 4 の実現方法と同じ考え方で対応することが可

能である．すなわち，Case 7 の通信開始時の処理と Case 6 の移動後の処理を組み合わせることで実現できる．

6. むすび

本論文では，これまで検討の対象となっていなかった移動透過性の通信ケース，すなわち MN が宅外からホームネットワーク内の CN に通信を開始し，MN が移動した場合においても通信を継続できる方式を提案した．NAT-f を適用することにより，NAT-f と移動透過性プロトコルが互いに独立性を保持しつつ，容易に組み合わせることができることを示した．NAT-f と Mobile PPC を組み合わせたシステムを実装して性能評価を行った結果，スループットの低下は十分に小さく，実用上問題ないことを確認した．

今後はあらゆる通信ケースにおいて，アドレス空間の違いに影響されない柔軟な移動透過アーキテクチャの実現を目指す．

謝辞 本研究の一部は，日本学術振興会科学研究費補助金（特別研究員奨励費 20・1069）の助成を受けたものである．

文　献

[1] 寺岡文男，“インターネットにおけるノード移動透過性プロトコル，” 信学論（D-I），vol.J87-D-I, no.3, pp.308–328, March 2004.
[2] D. Johnson, C. Perkins, and J. Arkko, “Mobility support in IPv6,” RFC 3775, IETF, June 2004.
[3] M. Ishiyama, M. Kunishi, K. Uehara, H. Esaki, and F. Teraoka, “LINA: A new approach to mobility support in wide area networks,” IEICE Trans. Commun., vol.E84-B, no.8, pp.2076–2086, Aug. 2001.
[4] 相原玲二，藤田貫大，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，” 情処学論，vol.43, no.12, pp.3889–3897, Dec. 2002.
[5] C. Perkins, “IP mobility support for IPv4,” RFC 3344, IETF, Aug. 2002.
[6] H. Levkowetz and S. Vaarala, “Mobile IP traversal of network address translation (NAT) devices,” RFC 3519, IETF, April 2003.
[7] G. Montenegro, “Reverse tunneling for Mobile IP, revised,” RFC 3024, IETF, Jan. 2001.
[8] 井戸上彰，久保　健，横田英俊，“プライベートアドレスを使用するモバイルネットワーク間のローミング手順とその実装，” 情処学論，vol.44, no.12, pp.2958–2967, Dec. 2003.
[9] 竹内元規，鈴木秀和，渡邊　晃，“エンドエンドで移動透過性を実現する Mobile PPC の提案と実装，” 情処学論，vol.47, no.12, pp.3244–3257, Dec. 2006.
[10] 鈴木秀和，渡邊　晃，“Hole punching を用いた NAT 越え Mobile PPC の設計，” 情処学 MBL 研報，vol.2008, no.44, pp.69–74, May 2008.
[11] Digital Living Network Alliance, DLNA Networked Device Interoperability Guidelines Expanded, Oct. 2006, http://www.dlna.org/
[12] 鈴木秀和，宇佐見庄五，渡邊　晃，“外部動的マッピングにより NAT 越え通信を実現する NAT-f の提案と実装，” 情処学論，vol.48, no.12, pp.3949–3961, Dec. 2007.
[13] P. Vixie, S. Thomson, Y. Rekhter, and J. Bound, “Dynamic updates in the domain name system (DNS update),” RFC 2136, IETF, April 1997.
[14] 瀬下正樹，渡邊　晃，“Mobile PPC における認証方式の実装，” DICOMO2006, vol.2006, no.6, pp.809–812, July 2006.
[15] B. Ford, P. Srisuresh, and D. Kegel, “Peer-to-peer communication across network address translators,” Proc. USENIX Annual Tech. Conf., pp.179–192, Anaheim, CA, April 2005.
[16] Y.J. Oh, H.K. Lee, J.T. Kim, E.H. Paik, and K.R. Park, “Design of an extended architecture for sharing dlna compliant home media from outside the home,” IEEE Trans. Consum. Electron., vol.53, no.2, pp.542–547, May 2007.
[17] 茂木信二，田坂和之，テープウィロージャナポンニワット，堀内浩規，“情報家電の広域 DLNA 通信方式の提案，” 信学技報，NS2007-10, April 2007.
[18] V. Devarapalli, R. Wakikawa, A. Petrescu, and P. Thubert, “Network mobility (NEMO) basic support protocol,” RFC 3963, IETF, Jan. 2005.
[19] K. Leung, G. Dommety, V. Narayanan, and A. Petrescu, “Network mobility (NEMO) extensions for Mobile IPv4,” RFC 5177, IETF, April 2008.
[20] 坂本順一，鈴木秀和，渡邊　晃，“ネットワーク単位の移動透過性を実現する Mobile NPC の実装と評価，” DICOMO2006, vol.2006, no.6, pp.821–824, July 2006.
[21] 島　慶一，湧川隆次，“WIDE プロジェクトと最新インターネット技術研究動向: 3.WIDE プロジェクトにおける IPv6 モビリティ技術の研究開発，” 情報処理，vol.46, no.8, pp.879–886, Aug. 2005.
[22] H. Soliman, “Mobile IPv6 support for dual stack hosts and routers (DSMIPv6),” Internet Draft, IETF, Nov. 2007, draft-ietf-mip6-nemo-v4traversal-06.txt
[23] OpenSSL, “The open source toolkit for SSL/TLS,” http://www.openssl.org/
[24] T. Kivinen and M. Kojo, “More modular exponential (modp) diffie-hellman groups for internet key exchange (IKE),” RFC 3526, IETF, May 2003.
[25] C. Kaufman, “Internet key exchange (IKEv2) protocol,” RFC 4306, IETF, Dec. 2005.
[26] P. Srisuresh and K. Egevang, “Traditional IP network address translator (traditional NAT),” RFC 3022, IETF, Jan. 2001.
[27] NLANR/DAST, “Iperf,” http://dast.nlanr.net/

projects/Iperf/
[28] 菊池　豊，藤井資子，山本正晃，永見健一，中川郁夫，“遅延計測による日本のインターネットトポロジーの推定,” 信学技報，IA2007-27, July 2007.
[29] A. Mishra, M. Shin, and W. Arbaugh, “An empirical analysis of the IEEE802.11 MAC layer handoff process,” ACM SIGCOMM Comput. Commun. Rev., vol.33, no.2, pp.93–102, April 2003.
[30] 金本綾子，鈴木秀和，伊藤将志，渡邊　晃，“IPv4 移動体通信システムにおけるパケットロスハンドオーバの提案,” 情処学論，vol.50, no.1, Jan. 2009.（掲載予定）

付　　録

Mobile PPC の認証鍵共有処理

MN は CN との通信に先立ち，Cookie C_{MN} を生成して CN へ Cookie Request を送信する．Cookie は MN と CN の IP アドレス，乱数，及び生成時刻のデータを結合し，ハッシュ関数により出力される値として生成される．

$$C_{MN} = h(IP_{MN} \mid IP_{CN} \mid N_{MN} \mid T_{MN})$$

Cookie Request を受信した CN は Cookie C_{CN} を生成し，受信した C_{MN} とともに Cookie Response を MN へ応答する．

$$C_{CN} = h(IP_{CN} \mid IP_{MN} \mid N_{CN} \mid T_{CN})$$

MN は受信した C_{MN} を検証後，TCP/UDP 通信を開始してから DH 鍵交換をバックエンドで行う．MN は DH 秘密鍵 $Priv_{MN}$ をランダムに生成し，それに対応する DH 公開鍵 Pub_{MN} をシステム共通の素数 p 及び始根 $g < p$ により計算する．

$$Pub_{MN} = g^{Priv_{MN}} \bmod p$$

その後，DH Key Request により CN へ DH 公開鍵と Cookie を送信する．DH Key Request を受信後，CN は C_{CN} を検証してから，MN と同様に DH 秘密鍵と DH 公開鍵を生成する．

$$Pub_{CN} = g^{Priv_{CN}} \bmod p$$

上記 DH 公開鍵と Cookie を DH Key Response に記載して MN へ応答する．

DH 鍵交換終了後，MN と CN は自身の DH 秘密鍵と受信した相手の DH 公開鍵により共通鍵 CK を生成する．

$$CK = \begin{cases} {Pub_{CN}}^{Priv_{MN}} \bmod p & \text{（MN 側）} \\ {Pub_{MN}}^{Priv_{CN}} \bmod p & \text{（CN 側）} \end{cases}$$

更に生成した共通鍵と交換した Cookie のハッシュ値を求め，最終的な認証鍵 AK を生成する．

$$AK = h(CK \mid C_{MN} \mid C_{CN})$$

上記認証鍵は移動後の CU Request/Response の署名生成，及び検証のために用いられる．

（平成 20 年 5 月 8 日受付，8 月 22 日再受付）

鈴木　秀和　（学生員）

平 16 名城大・理工・情報科学卒．平 18 同大大学院理工学研究科修士課程了．現在，同大学院理工学研究科博士後期課程に在学中．平 20 日本学術振興会特別研究員．主として，ネットワークセキュリティ，モバイルネットワーク，ホームネットワークに関する研究に従事．IEEE，情報処理学会各学生員．

渡邊　　晃　（正員）

昭 49 慶大・工・電気工卒．昭 51 同大大学院工学研究科修士課程了．同年，三菱電機（株）入社．平 3 同社情報技術総合研究所移籍．平 14 名城大・理工教授，現在に至る．主としてルータ，ネットワークセキュリティに関する研究に従事．博士（工学）．IEEE，情報処理学会各会員．