修 士 論 文

移動透過性とNAT越えを同時に実現する
アドレス管理手法の提案

平成24年度修了

三重大学大学院工学研究科

博士前期課程 電気電子工学専攻

通信工学研究室

西尾 拓也

目 次

図 目 次

表 目 次

第1章

序論

1.1 背景

近年，無線通信網の発展や携帯端末の高性能化により，携帯端末などの無線通信インターフェースを搭載した機器から高速無線通信技術を用いてインターネットへ接続する需要が増加している．インターネットにおいては，Internet Protocol（IP）を基盤技術として利用しており，一般的に IPv4 アドレスと呼ばれるネットワーク上における機器の識別番号を用いて通信を行なっている．

また，近年では第三世代移動通信システムを代表するセルラシステムや IEEE 802.11 などの複数の無線通信インターフェースを実装した携帯端末が普及してきており，異なるネットワークを切り替えて通信を継続することが可能である [1], [2]．一般に異なるネットワークでは異なるネットワークアドレスを利用しており，ネットワークを切り替えた場合，端末に割り当てられた IP アドレスも変化する．しかし TCP などの上位プロトコルでは IP アドレスをコネクション情報として利用しており，ネットワークを切り替えて移動する場合に生じる IP アドレスの変化はコネクションの切断につながり，通信中にコネクションが切断されると通信が継続できなくなるという課題がある．これは IP アドレスが端末の位置識別子としての役割と，端末識別子としての役割の 2 つの役割を担っているために生じる．このようなコネクション切断により通信が継続できなくなる課題を解決する技術を移動透過性技術と呼び近年多くの研究が行われている [3–8]．Mobile IP は IPv4 ネットワーク用と IPv6 ネットワーク用があり，それぞれを Mobile IPv4（MIPv4）[4], [9], [10],

Mobile IPv6（MIPv6）[11], [12], [13] として検討されている．また近年では IPv4/IPv6 ネットワークを同時に利用可能な Dual Stack Mobile IPv6（DSMIPv6）[14], [15] が提案されている．MIPv4 では，移動端末の位置管理及び移動端末宛のパケットの中継を行うホームエージェントと呼ばれる機器を経由した通信を行うことで移動透過性を実現している，このとき移動端末宛の通信は必ずホームエージェントを経由しなければならないため，通信経路が冗長となる．また，通信経路を最適化した場合，IP データグラム内の送信元アドレスと実アドレスが異なるため，ルータが IP データグラムを破棄する可能性がある [5], [6], [16], [17]．一方，MIPv6 では経路最適化を行うことが検討されており [18]，冗長な経路を避ける事が可能である．しかし，MIPv6 と MIPv4 には互換性がないため，この経路最適化機能は IPv4 ネットワークで利用することができず，MIPv4 に適用することはできない．また，DSMIPv6 では MIPv6 を拡張し IPv4 ネットワークでも利用可能としているため，MIPv4 において課題となっている経路最適化などの問題点は同様に残っている．Host Identity Protocol（HIP）[19], [20] では，IPv4/IPv6 ネットワークを同時に利用可能な手法であるが，Interactive Connectivity Establishment（ICE）[21] を用いたシグナリングコストが高いことが知られている [22].

近年ネットワークにおいて，IPv4 グローバルアドレスの枯渇のため IPv4 アドレス消費を抑制する目的とセキュリティの観点から，外部ネットワークと組織内ネットワーク間に Network Address Translation（NAT）と呼ばれるアドレス変換を行う機器を設置することが一般的である．組織内ネットワークにおいて外部ネットワークでは利用することができないプライベートアドレスを利用し，NAT の変換機能を用いて外部ネットワークで利用可能なグローバルアドレスとの変換を行うことが可能である．NAT を利用する場合では，NAT の性質により外部ネットワークから NAT 配下の組織内ネットワークが隠蔽されることから，外部ネットワークから NAT 配下のネットワークに向けて通信を開始する事ができない NAT 越えの問題がある [23]．NAT 越えを実現する技術は二種類に大別することができる．一つは NAT の機能を持った機器そのものに対して変更を加えるもの [24–31]，一つは NAT の機器自体には変更を加えず両エンドノード，または NAT や端末以外の第三の機器を導入することにより実現するものである [32–36]．NAT 自体に変更を加え NAT 越えを実現する技術では，パケットに対しカプセル化を行う必要や第三の機

器を利用することによる中継処理の必要が無いためスループットが高いという利点がある．一方，NAT 自体に変更を加える必要があるため，変更を加えた NAT 配下のネットワーク間でないと実現することができないという課題がある．

NAT に変更を加えず NAT 越えを実現する技術では，NAT 自体に変更を加えた技術のような接続するネットワークの制限がないため，既存のネットワークを用いて NAT 越えを実現することが可能である．しかし，NAT に変更を加えずに NAT 越えを実現する UDP ホールパンチング [32] ではセッションという概念がある TCP においてパケットが破棄されてしまうため，セッションの概念がない UDP を用いた実装を行う必要がある．また，第三の機器を導入する場合，パケットの中継処理が必要となるため，スループットが低下するという課題がある．

NAT 越えの問題はインターネットを利用するうえでエンドツーエンドの接続性という本来の理念を損なう要因となっているため，IPv4 アドレスの枯渇を根本から解決するためには IPv6 への移行は必須である．現在，IPv4 アドレスは広く普及したためアドレスの枯渇を迎えており，IPv6 アドレスへの移行が行われているが，IPv4 アドレスと IPv6 アドレスとの間には互換性がないため，IPv4 ネットワークを即座に IPv6 ネットワークへの移行することは困難であると考えられる．したがって，今後も当分の間は IPv4/IPv6 アドレスが混在した環境が想定される．今後のネットワークを考慮した上で現在のネットワークにおいてもシームレスな通信を実現するためには，NAT の存在する環境や IPv4 ネットワークと IPv6 ネットワークの混在環境における相互接続性や移動透過性を実現する必要がある．

そこで本稿では，IPv4/IPv6 アドレスが混在する環境において移動透過性や NAT 越えを同時に実現するために様々なアドレスを必要とすることから，移動透過性と NAT 越えを同時に実現するためのアドレス管理手法について検討を進める．

1.2　本研究の目的

本研究では移動透過性及び NAT 越えを実現するために利用するアドレス管理手法の検討を目的としている．本研究では，大きな目標として IPv4/IPv6 アドレスの混在ネットワークを考慮してプライベートネットワークとグローバルネットワークにかかわらず移動透過性と NAT 越えを同時に実現する Network Traversal with Mobility（NTMobile）を提案しており，移動透過性や NAT 越えを実現するための様々な機能を分担して実装を進めている [37], [38], [39], [40]．これを実現するために，提案法を実装した機器として端末（NTM 端末）と中継装置 Relay Server（RS），アドレス管理を行うサーバ Direction Coordinator（DC）の導入を行う．また，NAT に変更を加えないことにより移動透過性と NAT 越えを実現可能とするユーザを限定することはなく，提案法が実装された機器の導入を行うことのみで既存のネットワークに影響を与えることなく実現可能としている．実際の動作おいては，端末の情報を事前に DC に対して行い，DC の Domain Name System（DNS）機能を用いて通信相手端末の情報を取得後，DC からの指示のもと端末間でトンネルを構築することにより通信を行う．また，相手を一意に識別する仮想アドレスを用いることで，トンネル構築後は仮想アドレスを実アドレスでカプセル化することによりネットワーク間の移動による IP アドレスの変化を隠蔽する．仮想 IP アドレスの導入により，IP アドレスの位置識別子と端末識別子としての役割を完全に分離することが可能となり移動透過性を実現可能としている．実際の通信においては，パケットを UDP でカプセル化を行い通信を行なっている．また，両端末がプライベートネットワークである NAT 配下同士の場合，RS を用いてパケットの中継を行うことで NAT 越えを実現している．

この手法を実現するために，端末間の通信経路の構築方法を指示する必要がある．したがって，本提案における大きな目標である移動透過と NAT 越えを実現する手段の一部として，自身と通信相手の端末情報を管理・取得する手段が必要となるため，本研究ではアドレス管理の枠組みとして DNS サーバを拡張して利用することで，端末情報の管理と取得手段の確保を実現する．実際には DNS サーバである Berkeley Internet Name Domain（BIND）を拡張し，独自のレコードを登録可能とすることで提案法で必要となる様々な情報の管理を実現する．また，本アド

レス管理手法を Linux に実装し動作確認を行うことで，実現可能なアドレス管理手法であることを示す.

1.3　本論文の構成

第 2 章において移動透過性と NAT 越えに関する研究の概要について説明する.. 第 3 章では, 提案法における概要と本論文で目的となるアドレス管理手法について説明する. 第 4 章において提案法の実装及び実験結果をもとに有効性を検証する. 最後に第 5 章で本論文のまとめと今後の課題について述べる.

第2章

移動透過性とNAT越えを実現する関連研究

2.1 移動透過性とNAT越え

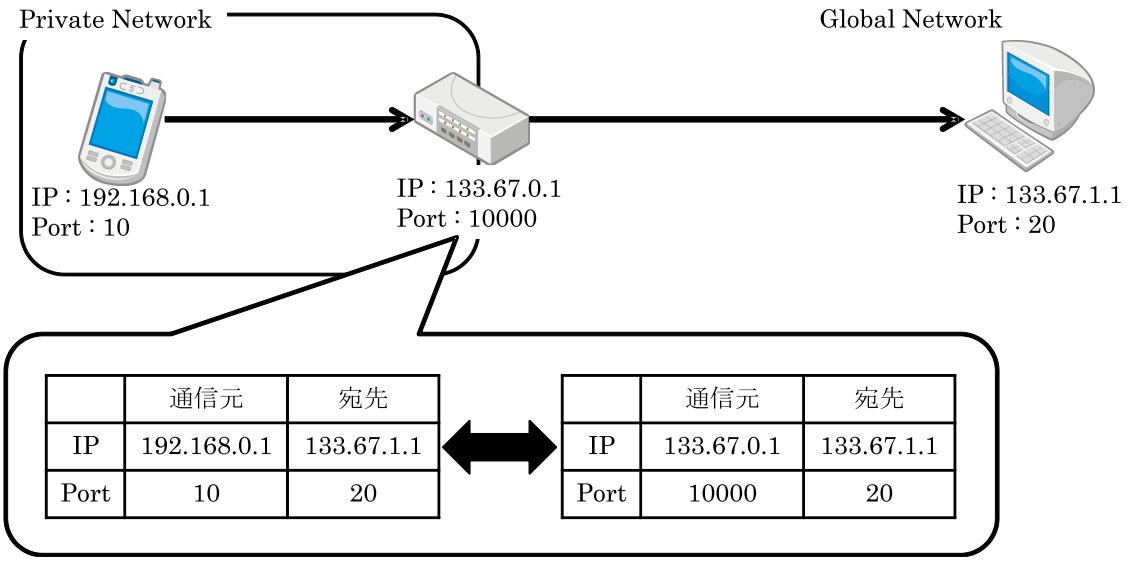
移動透過性とNAT越えの課題について記載する.

2.1.1 移動透過性

現在ではアクセススポットのような公衆無線LANのサービスが増加している. 持ち運びに便利で高性能な携帯端末が増加してきている現在, 移動しながら無線LANネットワークを切り替えて通信を継続できることのメリットは大きい. これらのネットワークではIPを基盤技術として利用しており, 一般的にIPv4アドレスと呼ばれるネットワーク上における機器の識別番号を用いて通信を行なっている. TCP/IPではIPアドレスを通信端末間でのコネクション情報としてりようしており, IPアドレスには端末が利用しているネットワークを識別するための位置識別子としての役割と, 端末がその端末であることを認識するための端末識別子としての役割がある. したがって, ネットワークを切り替えることにより利用するIPアドレスが変化した場合, 通信相手端末からは新たな端末として認識されるためコネクションが切断され通信を継続することができなくなる問題がある. この問題を解決する技術を移動透過性技術と呼び, 多くの実現手法が提案されている.

2.1.2　NAT 越え

現在のネットワークにおいてインターネットに接続するためには IP アドレスを用いて通信相手を識別する必要がある．つまり，通信相手を一意に識別可能なアドレスを用いることで自身と相手端末と通信を行うことができる．しかし，現在一般的に用いられているアドレス体系は IPv4 アドレスであり，インターネット空間における通信において端末を識別するために利用される一意に識別可能なグローバル IPv4 アドレスは枯渇の問題に直面している．近年ではグローバル IPv4 アドレスの有効利用のために，組織内のネットワークと外部ネットワークの間に NAT を設置し，図 2.1 に示すように，組織内でプライベート IP アドレスを用いて端末の識別を行い，外部ネットワークとの通信には NAT を用いてプライベート IP アドレスと一つのグローバル IPv4 アドレスとの変換を行うことでインターネットへの接続を可能としている．なお本論文において記述する NAT については，IP アドレスとポート番号を変換する Network Address Port Translation（NAPT）のことであり，一つのグローバル IP アドレスを用いて複数のプライベート IP アドレスを管理することが可能である．



	通信元	宛先
IP	192.168.0.1	133.67.1.1
Port	10	20

	通信元	宛先
IP	133.67.0.1	133.67.1.1
Port	10000	20

図 2.1 NAT によるアドレス変換動作例

インターネット通信において用いられる IP アドレスヘッダには通信元と通信先の一つずつの IP アドレスのみしか記載されないため，内部ネットワークから外部ネットワークに向けた通信を行う場合，内部ネットワークで用いられているプライベート IP アドレスは NAT の変換処理によってグローバル IP アドレスに書き換えられる．つまり，通信相手端末からは NAT のグローバル IP アドレスが送信元となる端末から通信が行わていると判断される．このとき NAT では通信先 IP アドレスと送信元プライベート IP アドレス，そしてその通信に用いられているポート番号をテーブル情報として保持する．その後の通信相手端末から返ってくる通信では，NAT によって通信元端末へ転送される．具体的には，通信相手端末の IP アドレスとポート番号を元に NAT において保持されたテーブル情報から内部ネットワークおいて通信を行なっている端末を識別しパケットの転送を行う．以上の処理によりプライベート IP アドレスを用いた通信を可能としているが，内部ネットワークから通信を行うことでテーブルが作成されること，そして内部ネットワークで利用しているプライベート IP アドレスが外部ネットワークでそのまま利用することができないことから，外部ネットワークから内部ネットワークに対して通信を開始することができない．これを NAT 越え問題と呼び様々な研究が行われている．

2.2　関連研究

動透過性と NAT 越えを解決する関連研究について説明する．なお，本論文において使用するグローバル IP アドレスを GIP，プライベート IP アドレスを PIP として記述する．

2.2.1　Mobile IP

NAT 越えと移動透過性を同時に実現できる既存技術として Mobile IP（MIP）がある．MIP では通信を行うエンド端末の他に，第三の機器として Home Agent（HA）を導入する．HA は移動端末である Mobile Node（MN）のホームネットワークに置かれ，MN の位置情報の把握や通信相手端末である Correspondent Node（CN）から MN へ送られてくるパケットの転送を行う．また MN はホームネットワークで取得する Home Address（HoA）と移動先のネットワークで取得する Care-of Address（CoA）の二つの IP アドレスを持つ．HoA は移動しても変化しない一意の IP アドレスであり，両エンド端末が常に HoA を MN として認識して通信を行うことで，MN の移動後の通信を継続する．

図 2.2 に Mobile IP の動作概要を示す．MN は移動先で GIP$_{\mathrm{CoA}}$ を取得すると，MN の HoA である ”GIP$_{\mathrm{HoA}}$ ”と移動先の CoA である ”GIP$_{\mathrm{CoA}}$ ”を記載した Binding Update を HA に送信する．HA はこれを受信すると GIP$_{\mathrm{HoA}}$ と GIP$_{\mathrm{CoA}}$ の対応関係を示すエントリを生成した後，GIP$_{\mathrm{HoA}}$ 宛のパケットを受信するようにホームネットワーク内に Address Resolution Protocol（ARP）パケットを送信する．これにより以後の通信では，CN が GIP$_{\mathrm{HoA}}$ 宛にパケットを送信すると，このパケットは HA に送り届けられる．

HA は GIP$_{\mathrm{HoA}}$ 宛のパケットを受信すると，アドレスの対応関係からこのパケットに対して GIP$_{\mathrm{CoA}}$ 宛の IP-in-IP カプセルを形成し，移動先の MN に転送する．MN はこのパケットを受け取るとでカプセル化し，GIP$_{\mathrm{HoA}}$ 宛のパケットを取り出す．また MN がパケットを送信する場合は，送信元のアドレスを GIP$_{\mathrm{HoA}}$ にして直接 CN に送信する．このように HoA を端末識別子として用い，CoA を位置識別子として用いることで，CN と MN は，MN の移動に関わらず常に MN を GIP$_{\mathrm{HoA}}$ として認識したまま通信を行うことが可能となる．

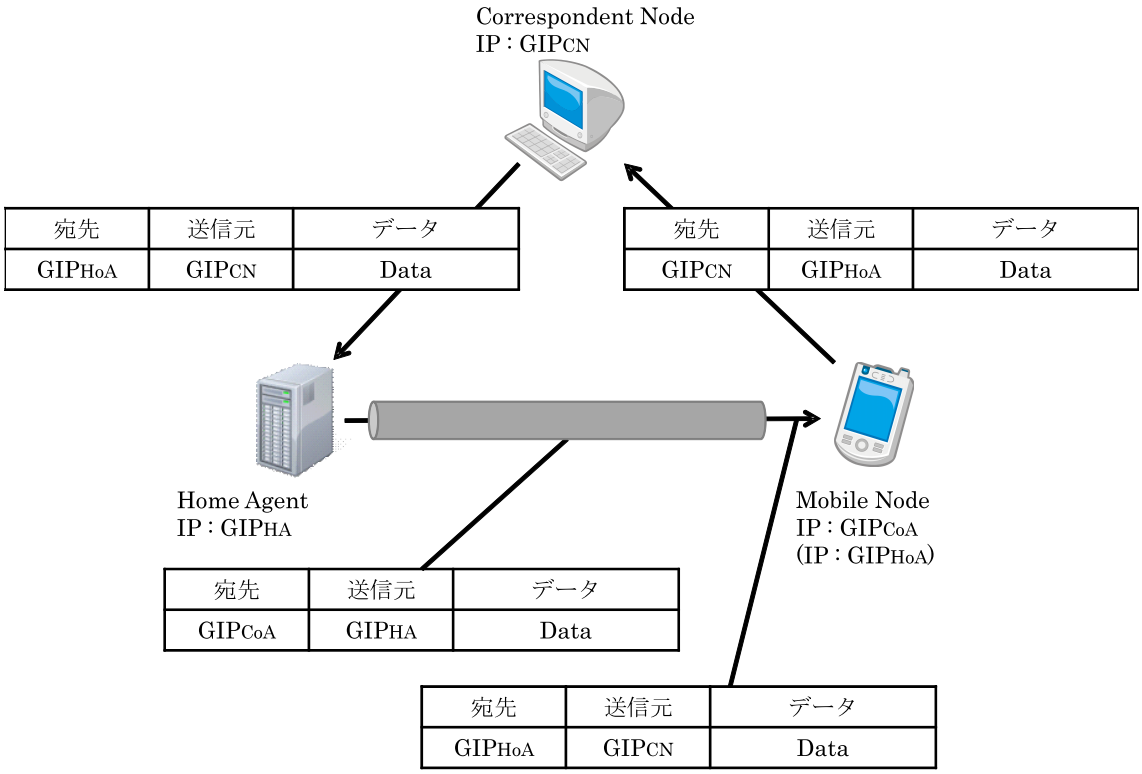


図 2.2 Mobile IP における動作概要

また MIP では NAT 越え問題に対応するため，UDP トンネルを利用する方式や特殊な NAT を導入する方式が提案されている．UDP トンネルを利用した MIP を図 2.3 に示す．図には CN から MN に対して送信する場合のパケットを記載する．この方式では MN が NAT 配下に移動して PIPCoA を取得すると，MN は HoA である ”GIPHoA ”を記載した UDP ベースの Binding Update を HA に送信する．この時 NAT のマッピングテーブルには，HA である GIPHA のポート番号 d からのパケットを MN である PIPCoA のポート番号 s に変換するマッピングエントリが生成される．

ここで s ′は，NAT が GIPHA のポート番号 d と PIPCoA のポート番号 s の通信に対して割り当てたポート番号である．HA は MN から Binding Update を受信すると，MN の CoA として GIPNAT，また UDP トンネルのポート番号 s ′をエントリに登録する．その後，GIPHoA 宛のパケットを受信すると，GIPNAT のポート番号

s ′宛の UDP トンネルを使用して転送する．このパケットは NAT により GIP_{NAT} のポート番号 s ′から PIP_{CoA} のポート番号 s に変換され MN まで転送される．また MN が CN にパケットを送信する場合も同じ UDP トンネルを使用して HA へ送信し，HA は UDP カプセルをでカプセル化して転送する．これによりパケットは NAT に影響されなくなるため，MN は NAT 配下に移動できるようになる．また，CN がプライベートネットワーク内の MN に対して通信を開始することができる．しかし，パケットが全て HA を経由して UDP カプセル処理が行われるため，スループットの更なる低下が課題となる．

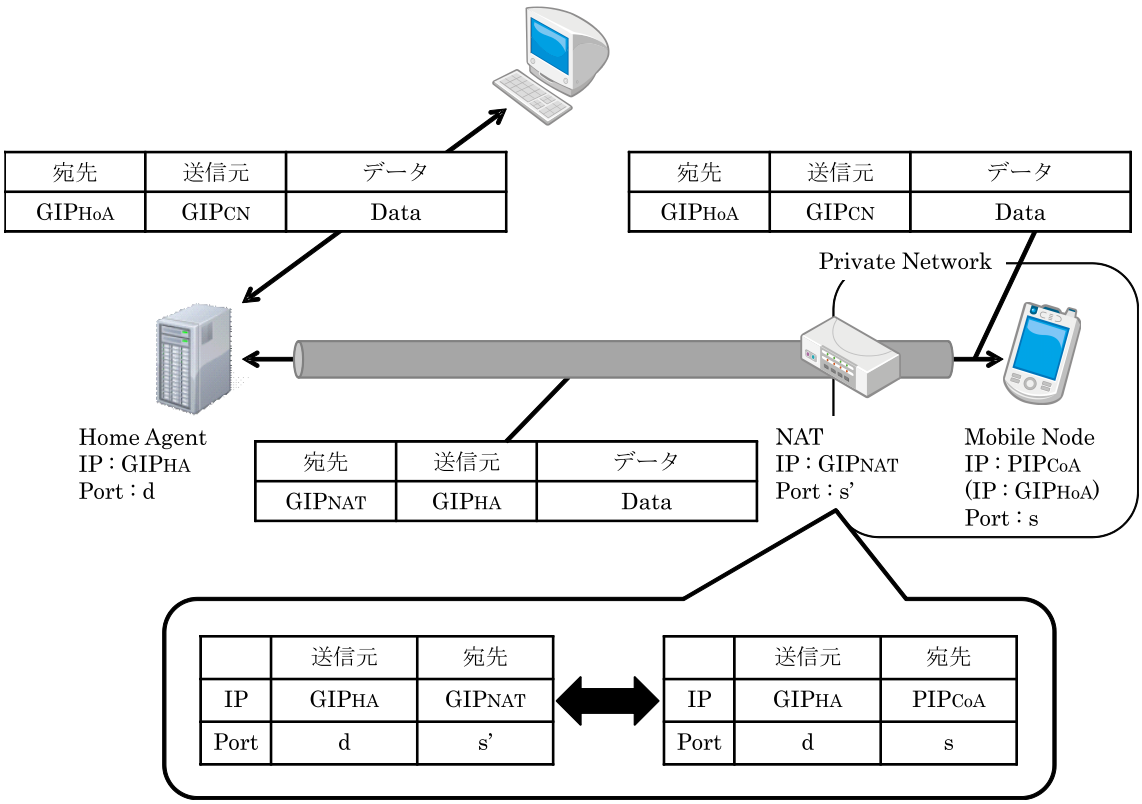


図 2.3 UDP トンネルを用いた Mobile IP における動作概要

2.2.2　SIP Mobility

移動透過性を実現する手法として Session Initiation Protocol（SIP）Mobility がある [41]. SIP Mobility は SIP を拡張することにより移動透過性を実現している．SIP Mobility の動作概要を図 2.4 に示す．また，端末構成を図 2.5 に示す．SIP を用いる端末は，Uniform Resource Identifier（URI）と呼ばれる不変で一意のアドレスを持ち，端末は事前に SIP サーバに対して，その URI と IP アドレス，ポート番号等の登録処理を行う．ユーザ端末は通信する相手端末の URI を SIP サーバに問い合せるか通知を受け，その IP アドレス（IPMN1）を得て直接相手と通信セッションを張ることができる．このため MIP の HA のような特定の機器を経由することなく通信を行うことが可能である．またユーザ端末が移動した場合，ユーザ端末は IP アドレス等の端末情報の更新処理を SIP サーバに対して行う．その後，SIP サーバから通信相手端末に向けて通知を行い，新たな IP アドレス（IPMN2）を取得することで再度，直接相手と通信セッションを行うことができる．また SIP サーバはセッション情報を管理しており，IP アドレス等の変更に伴い管理するセッション情報を変更することで，コネクションレスなセッションであればユーザ端末が通信中に移動しても通信セッションを継続することができる．すなわち，UDP を用いたリアルタイムセッションは SIP を用いることによりモビリティ制御とセッション制御を同時に実現することが可能となる．しかし，ユーザ端末が通信中に異なるネットワークに移動した場合，TCP のようなコネクション型の通信セッションでは IP アドレス等が変更され，そのセッションを継続することができず通信が切断される．また，IPv6 ネットワークでの利用は十分に議論されていない．

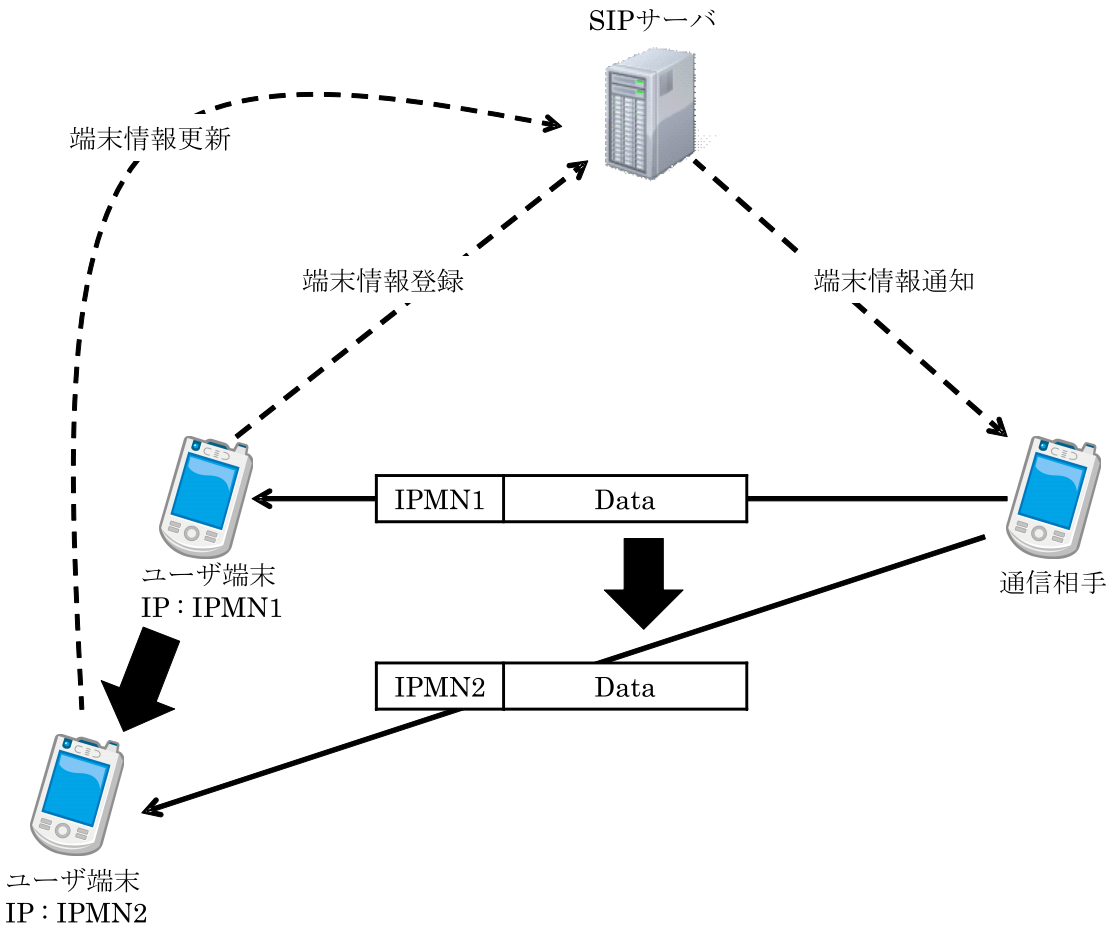


図 2.4 SIP Mobility における動作概要

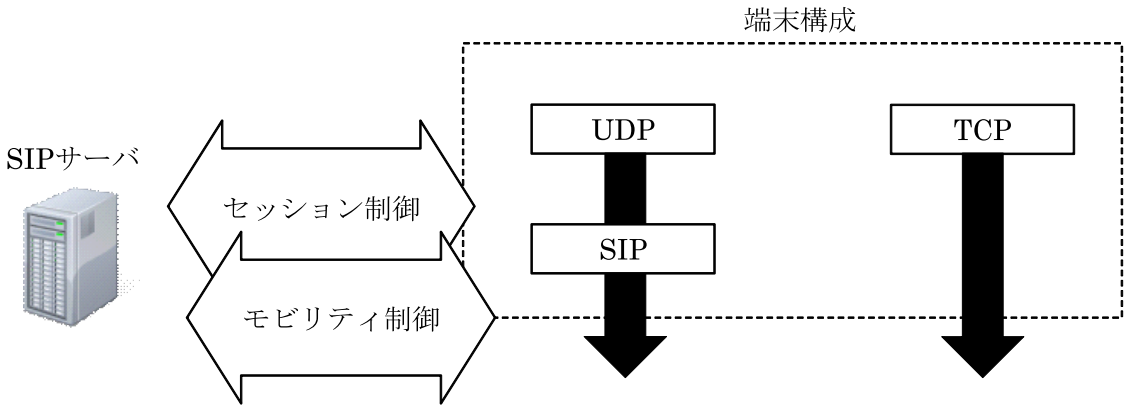


図 2.5 SIP Mobility における端末構成

2.2.3　All-SIP モビリティ

SIP は UDP のようなコネクションレス型の通信セッションであれば通信中に IP アドレスが変わっても通信セッションを維持できる．All-SIP モビリティはこの特徴を利用し，あらゆる通信セッションを UDP でカプセリングして，SIP だけでモビリティ制御とセッション制御を同時に実現可能としている [42], [43], [44]．All-SIP モビリティの基本概念を図 2.6 に示す．All-SIP モビリティでは通信中の TCP データもカプセリングして UDP データとして扱うため，ユーザ端末がネットワークを移動しても TCP セッションをそのまま継続することが可能である．すなわち，カプセリングされた TCP データは，でカプセリングして元の形式のまま取り出せるため TCP プロトコルをそのまま維持することが可能となる．

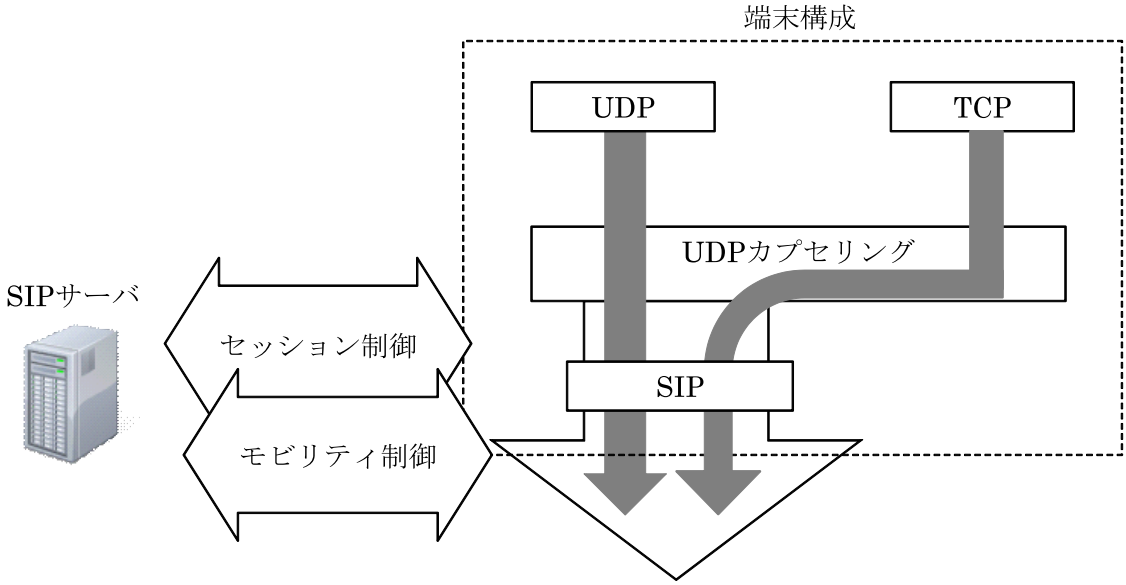


図 2.6 All-SIP モビリティにおける基本概念

図 2.7 に All-SIP モビリティのシステム構成を示す．All-SIP モビリティを実現する構成要素は All-SIP クライアントと SIP サーバである．All-SIP クライアントは，アプリケーションデータの通信セッションを全て UDP カプセリング/デカプセリングして送受信する機能を持つ．また，UDP カプセリングによって構成された UDP トンネル内の通信セッションを終端してアプリケーションとデータを授受するための仮想インターフェース（Virrual Interface : VIF）機能を持つ．UDP カプセリング機能は Session and Mobility Controller（SMC）モジュールに含まれ，SMC モジュールは SIP の制御管理機能も併せ持つため，All-SIP クライアントの端末登録やセッション制御，モビリティ制御を行う．また，SIP サーバに VIF 情報を配布する機能のみ追加する．これら機能を実装することにより SIP だけですべての通信セッションにおいて移動透過性を実現することが可能となる．

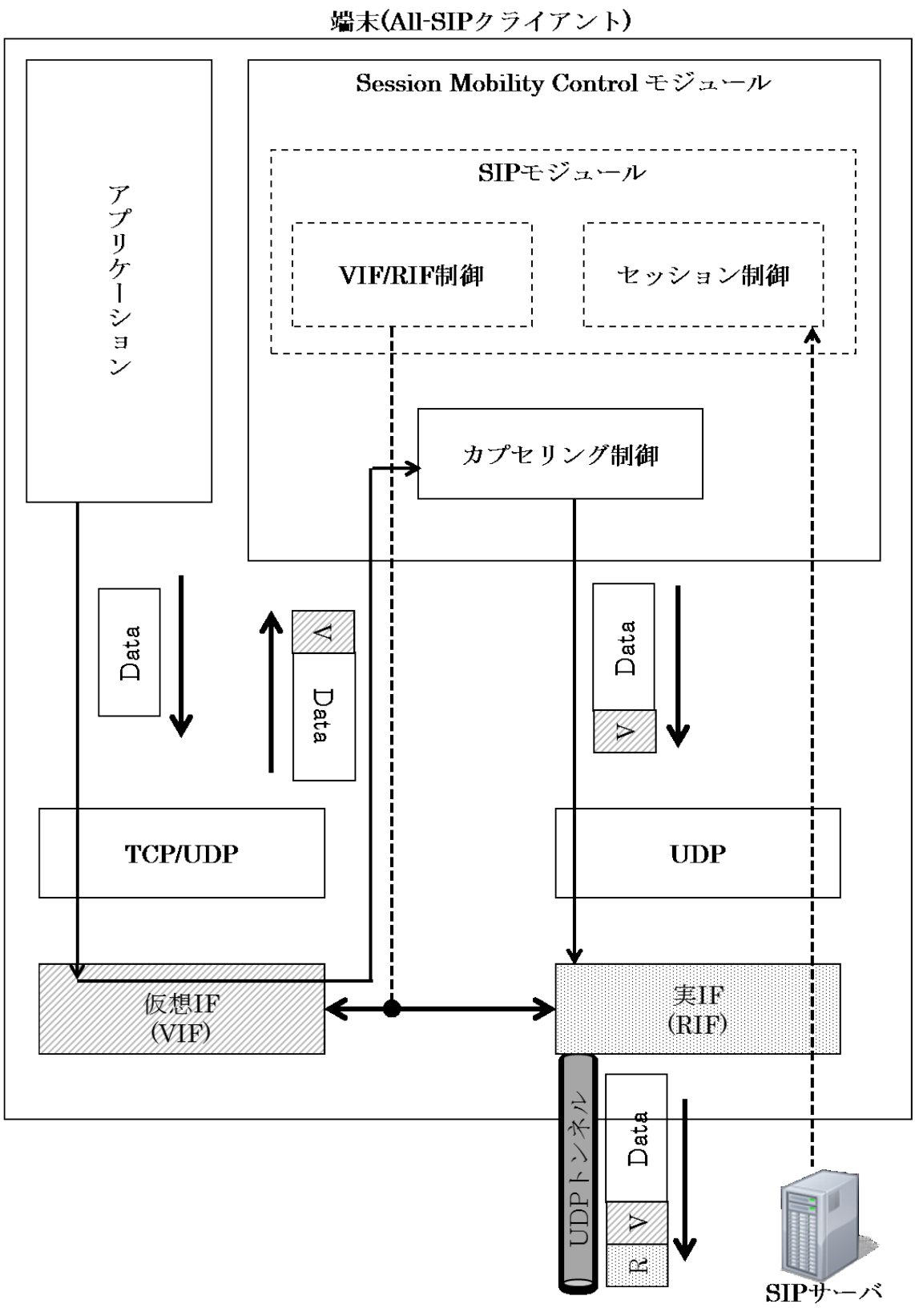


図 2.7 All-SIP モビリティにおけるシステム構成

2.2.4　UDP ホールパンチング

NAT 越え技術に UDP ホールパンチングがある．UDP ホールパンチングにおける動作概要を 2.8 図に示す．通信を行う両端末が NAT 配下のプライベートネットワークにある場合，外部ネットワークから通信を行うことができない課題を解決することが可能である．UDP ホールパンチングでは，NAT 配下の端末が外部に通信した際に作成される変換テーブルを互いに利用することで双方向からの UDP パケットを通過させることで実現している．

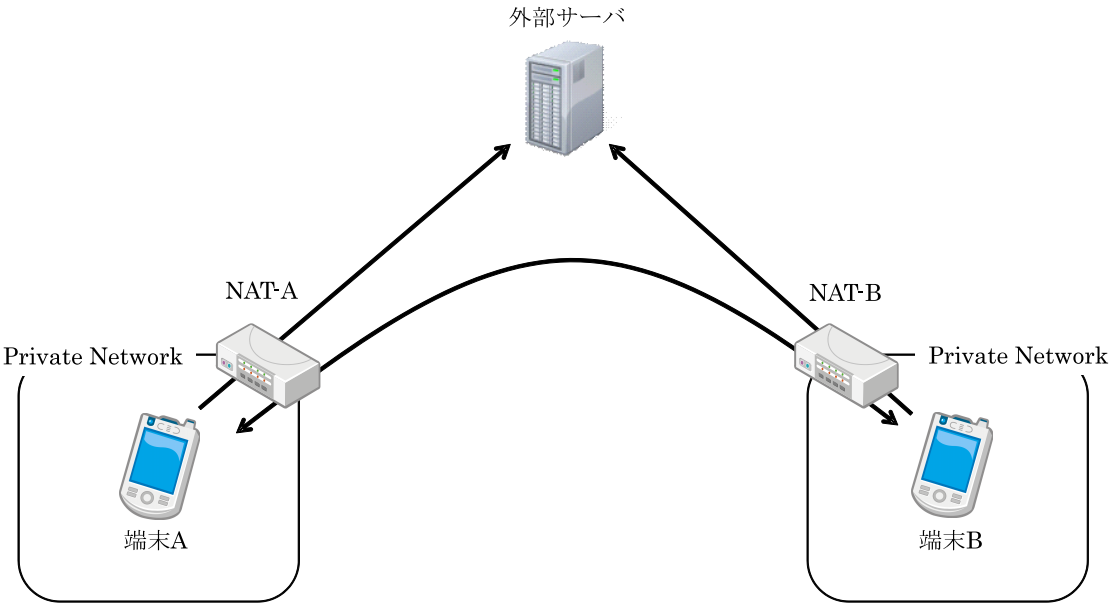


図 2.8 UDP ホールパンチングにおける動作概要

具体的な動作について説明する．まず端末 A と端末 B が外部サーバに向けて UDP 通信を行うことで，NAT-A と NAT-B では変換テーブルが作成され，この通信におけるポート番号を割り当てる．外部サーバでは端末 A と端末 B から送信されたパケットから IP アドレスとポート番号を取得し，両端末に対して通知を行う．

次に端末 A から通信を開始する場合について説明する．NAT の種類が Full Cone NAT と呼ばれる，端末と NAT が一対一で変換を行う NAT である場合，NAT 配下の端末が外部に向けて通信を行うと変換テーブルが作成される．変換テーブルが作成されると，外部から NAT に向けた通信は全て NAT 配下にある端末に送信されることから，端末 A からの通信は NAT-B を通過して端末 B に届き NAT 越えを実現することが可能である．

また NAT の種類が Restricted Cone NAT と Port-Restricted Cone NAT の場合，外部の通信先 IP アドレス，または外部の通信先 IP アドレス及びポート番号が一致している必要があるため，端末 A からの通信だけでは NAT を越えることができない．この場合における動作例を図 2.9 に示す．

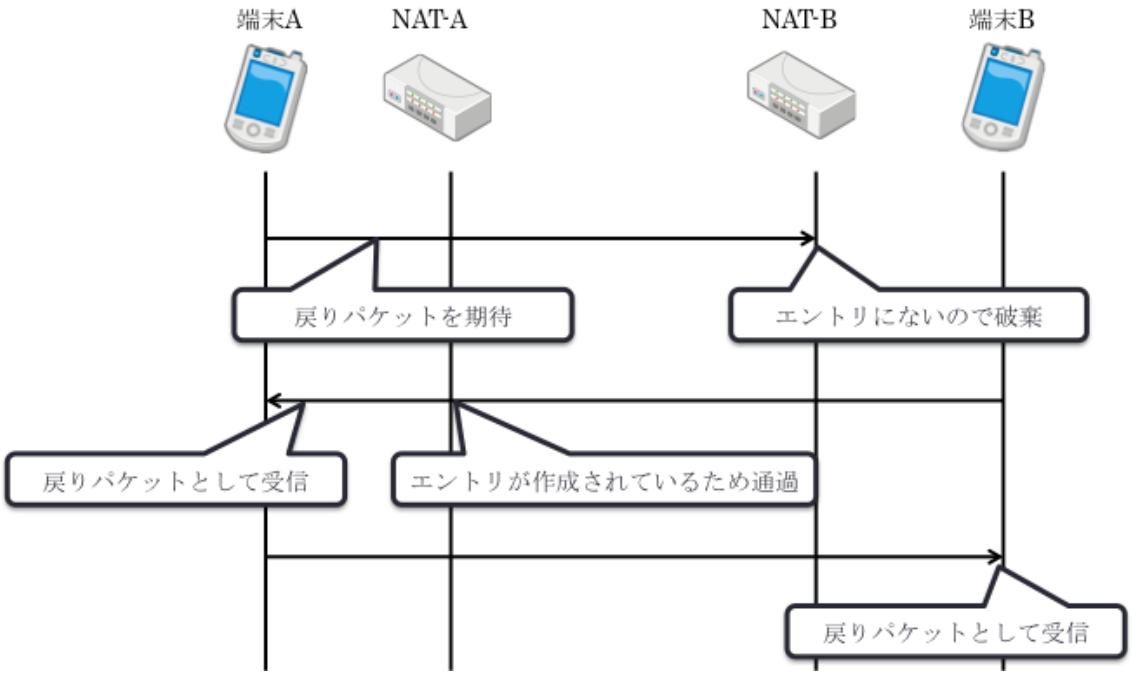


図 2.9 UDP ホールパンチングにおける動作例

Full Cone NAT と同様に，両端末が外部に向けて通信を行い NAT では変換テーブルを作成する．その後，端末 A から端末 B に向け通信を行う．しかし，NAT-B では端末 A と端末 B 間のテーブルがないためパケットが破棄される．ここで端末 A から端末 B に向けて通信を行った際に NAT-A では端末 B に向けた変換テーブルが作成されているため，端末 B から再度端末 A に向けて通信を行うことで NAT-A を通過して端末 A に通信を行うことができ NAT 越えを実現することが可能となる．また宛先が変わるとポート番号が変化する Symmetric NAT では，ポート番号の割り当ての規則性を元に何度もパケットを送ることで NAT 越えを実現している．しかしセッションの概念がある TCP での実現は難しく，多くが UDP に限られているという課題がある．

2.2.5　Mobile PPC

Mobile PPC は，IPv4 において第三の装置の補助を必要とせず，エンドエンドで移動透過性を実現するプロトコルである [45]．Mobile PPC では各エンド端末がカーネルの IP 層に CIT（Connection ID Table）と呼ぶアドレス変換テーブルを持ち，両エンド端末がこれを参照して全てのアプリケーションパケットの IP アドレスを変換することにより，上位アプリケーションに対してアドレスの変化を隠蔽し，かつパケットを正しくルーティングして通信を継続することができる方式である．ここで説明する記号について以下に示す．

- A : a　　：IP アドレス A，ポート番号 a
- A : a → B : b　：送信元 A : a から宛先 B : b へのパケット
- A : a ↔ B : b　：A : a と B : b との通信
- A : a ⇔ B : b　：A : a と B : b のアドレス変換

Mobile PPC は，通信開始時のアドレス解決と通信中の移動に係わるアドレス解決を明確に分離し，前者を Dynamic Domain Name System（DDNS）[46] により実現し，後者を Mobile PPC が実現する．Mobile PPC の動作を図 2.10 に示す．Mobile PPC では両エンド端末が共に移動できるため CN，MN といった区別は存在しないが，便宜上，図 2.10 で移動するエンド端末を MN，その通信相手端末を CN とする．CN と MN は既に DDNS を用いて，GIP$_{CN}$: s ↔ GIP$_{MN}$: d の通信を開始しているものとする．通信中に MN が移動して新しく IP アドレス GIP$_{MN}$ 'を取得すると MN は CN との間で MN の移動前後の IP アドレス GIP$_{MN}$，GIP$_{MN}$ 'を記載した CU（CIT Update）Request/Response を交換し，両エンド端末は以下のような CIT エントリを生成する．

GIP$_{CN}$: d ↔ {GIP$_{MN}$: s ⇔ GIP$_{MN}$ ': s }

以後，MN が CN にアプリケーションパケットを送信する場合は IP 層で CIT を参照し，パケットの送信元アドレスを GIP$_{MN}$ から GIP$_{MN}$ 'に変換して送信し，CN はこれを受信すると，逆に GIP$_{MN}$ 'から GIP$_{MN}$ に変換して上位アプリケーションに渡す．CN が MN にパケットを送信する場合は逆の処理を行う．以上の処理によ

りパケットは正しくルーティングされ，かつ両エンド端末の上位アプリケーションでは MN の IP アドレスが変化したことに気付くことなく通信を継続できる．

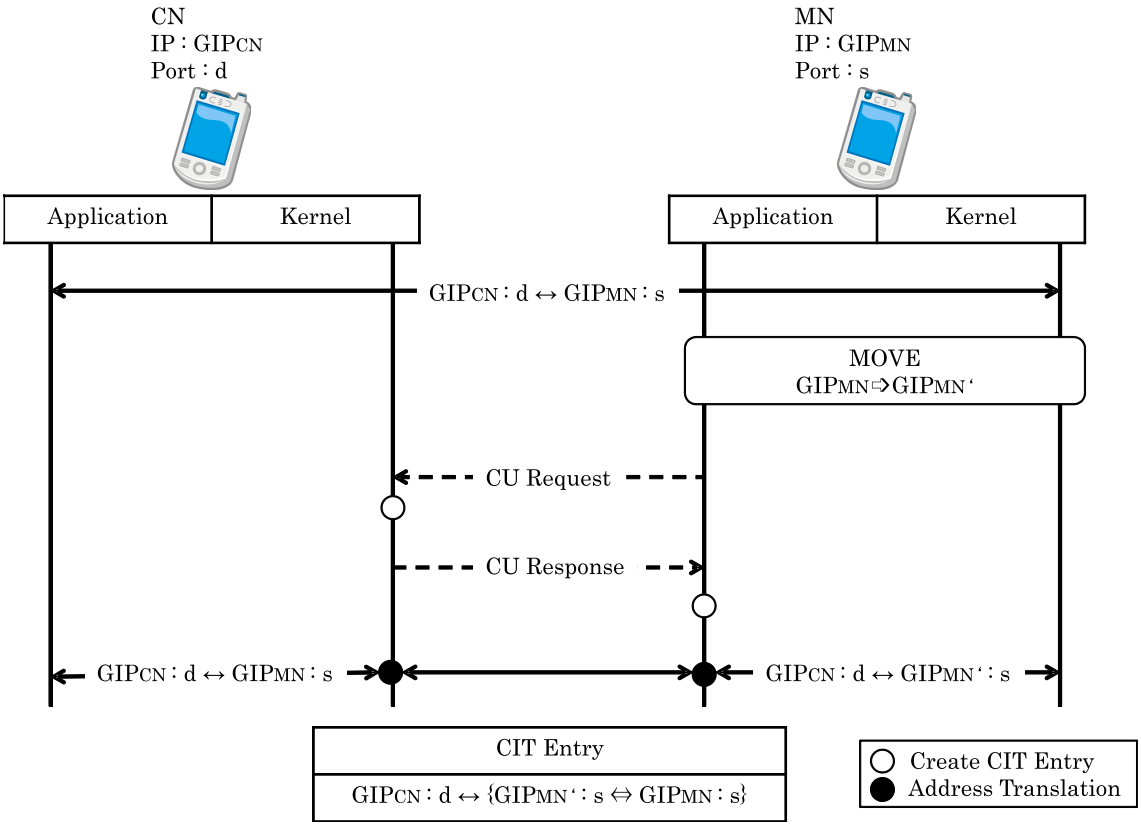


図 2.10 Mobile PPC における動作例

Mobile PPC では NAT 越え問題に対応するため，UDP ホールパンチングを組み合わせる方式がある．図 2.11 に UDP ホールパンチングを用いた Mobile PPC の動作概要を示す.

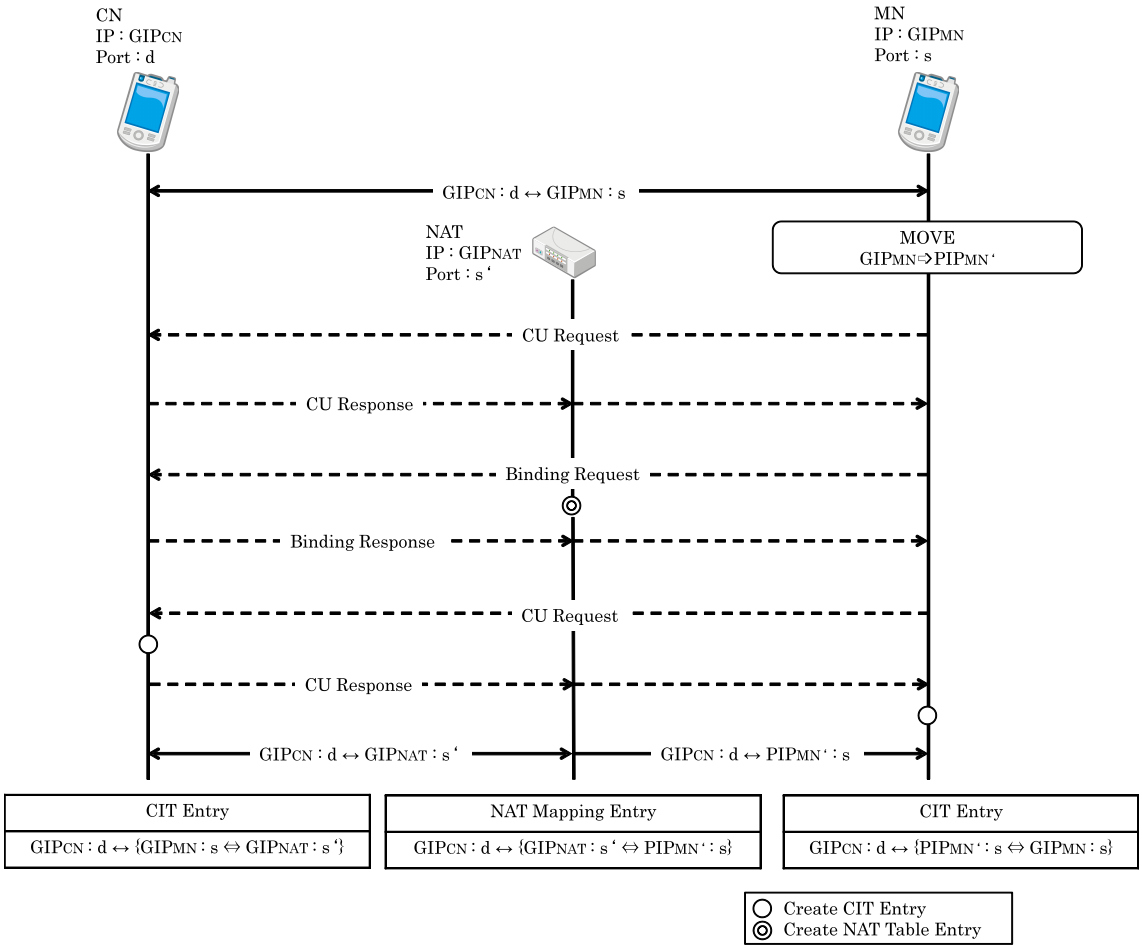


図 2.11 UDP ホールパンチングを用いた Mobile PPC における動作概要

MN は移動して新しく IP アドレスを取得すると CN との間で CU Request/Response を交換するが，この時 CN は CU Request に記載されている MN の移動後の IP アドレス PIPMN ′と IP ヘッダの IP アドレス GIPNAT が異なることを検出すると，MN が NAT 配下に移動したと判断する．その場合，CN は MN に UDP ホールパンチングに当たる Binding 処理を行うよう要求するフラグを付けた CU Response を返す．MN は要求に従い，CN との通信で使用しているプロトコルをベースにした

Binding Request/Response を CN との間で交換する．これにより NAT のマッピングテーブルには以下のマッピングエントリが生成される．

GIP$_{CN}$: d ↔ {GIP$_{NAT}$: s ′ ⇔ GIP$_{MN}$ ′: s }

その後，MN は CN との間で再度 CU Request/Response を交換し，CN，MN はそれぞれ以下のような CIT エントリを生成する．

CN:　GIPCN : d ↔ {GIP$_{MN}$: s ⇔ GIP$_{NAT}$: s ′ }

CN:　GIPCN : d ↔ {GIP$_{MN}$ ′: s ⇔ GIP$_{MN}$: s }

以上の動作により，マッピングエントリと CIT エントリが対応付けられる．以後は通常の Mobile PPC と同様に，CIT テーブルを参照したアドレス変換を行うことで通信を継続する．近年の NAT には，Stateful Packet Inspection（SPI）と呼ばれる TCP シーケンス番号等の通信の整合性をチェックするフィルタリング手法が搭載されていることが多い．このため，Binding Update によって作成した TCP セッションのシーケンス番号と移動前に行っていた通信の TCP セッションのシーケンス番号が異なると，通信経路上の NAT が SPI 機能を有する場合，TCP パケットが破棄される可能性がある．またこの方式では MN が移動する際に CN が NAT 配下に存在すると，MN からの CU Request が CN に到達せず，Binding 処理を開始できない．したがって MN の移動時，CN はグローバルネットワークに存在しなければならない．更に通信開始時の NAT 越えは想定しておらず，プライベートネットワーク内の CN に対して通信開始するには別の技術との組み合わせが必要であるという課題がある．

第3章

移動透過性とNAT越えを同時に実現するアドレス管理手法

本章では移動透過性とNAT越えを同時に実現するアドレス管理手法の提案を行う．移動透過性は端末がネットワークを越えて移動することによって，異なるIPアドレスの割り当てが行われ，通信の継続性が失われるため，移動によるIPアドレスの変化を隠蔽し，通信を行なう端末間で一意に端末を識別可能な仮想IPアドレスの導入により実現する．また，NAT越え問題を解決するため，端末間あるいは中継器に向けてトンネル通信を行うことで実現する．この手法には端末のアドレス管理が必要であり，アドレスの管理を行う枠組みとしてDNSを拡張することで移動透過性とNAT越えの実現を可能としている．

初めに移動透過性とNAT越えを実現するための枠組みについて説明し，その後，本稿で提案するアドレス管理手法についての説明を行う．

3.1　提案法における概要

提案方式の大きな目的は，IPv4 ネットワークと IPv6 ネットワークの混在環境においても移動透過性を少ないオーバーヘッドで実現することである．図 3.1 は提案法の概要図であり，システムは Direction Coordinator（DC），Relay Server（RS），提案法を実装した NTM 端末により構成される．また，提案法では，SPI などを実装する一般的な NAT を想定しており，NAT の実装変更などは必要としない．なお，DC 及び RS は必要に応じて増設することができ，規模拡張性も有した設計となっている．

提案法では，提案法に必要な端末の情報を DC に登録しておき，その後通信を行いたい端末の情報を取得することで移動透過性と NAT 越えを実現する準備を可能とする．また，自身の端末情報と通信相手の情報を DC に対して送信することで DC から経路構築方法を受け取り，DC の指示に従って互いに経路の構築を行うことで移動透過性と NAT 越えを実現している．提案法において利用するアドレスとしては，DC が NTM 端末に重複なく仮想 IP アドレスを割り振ることを想定しており，アプリケーションは仮想 IP アドレスを用いて通信を行うことにより，移動に伴う実 IP アドレスの変化を隠蔽している．また，NTM 端末間の通信にはトンネル技術を採用しており，通信開始時に送信される DNS の A レコード要求を検出することにより，トンネル構築を開始する．実際の通信では，アプリケーションは仮想 IP アドレスを用いて IP データグラムの生成を行うが，カプセル化により実 IP アドレスが割り当てられることによりトンネルを用いた通信を実現している．また，実 IP アドレスが変化した場合にも，カプセル化される IP データグラムは同一の仮想 IP アドレスを利用しつづけるため，移動透過性を実現可能である．

IPv4 ネットワークにおいて NTM 端末の双方又は片方がグローバル IP アドレスを利用可能な場合，グローバル IP アドレスを持つ端末に向けて通信を開始することにより，NTM 端末間で直接トンネルを構築可能である．一方，NTM 端末の双方が NAT 配下に存在し，プライベート IP アドレスを利用している場合，各エンド端末は同一 RS に向けてトンネルを構築することにより，RS を経由したトンネル構築を行う．また，IPv4/IPv6 の混在したネットワークにおいて，双方が IPv6

アドレスを利用可能な場合，NTM 端末間で直接トンネルを構築可能であり，片方が IPv6 アドレスのみ利用可能な場合，RS を経由したトンネル構築を行う．結果として，提案法では，IPv4 ネットワーク，IPv6 ネットワークに関わらず，両エンド端末の移動透過性を実現可能である．

また，NTM 端末間や NTM 端末と RS の間で行われるトンネル通信は，トンネル構築時に DC より配布される共通鍵を用いて暗号化される．

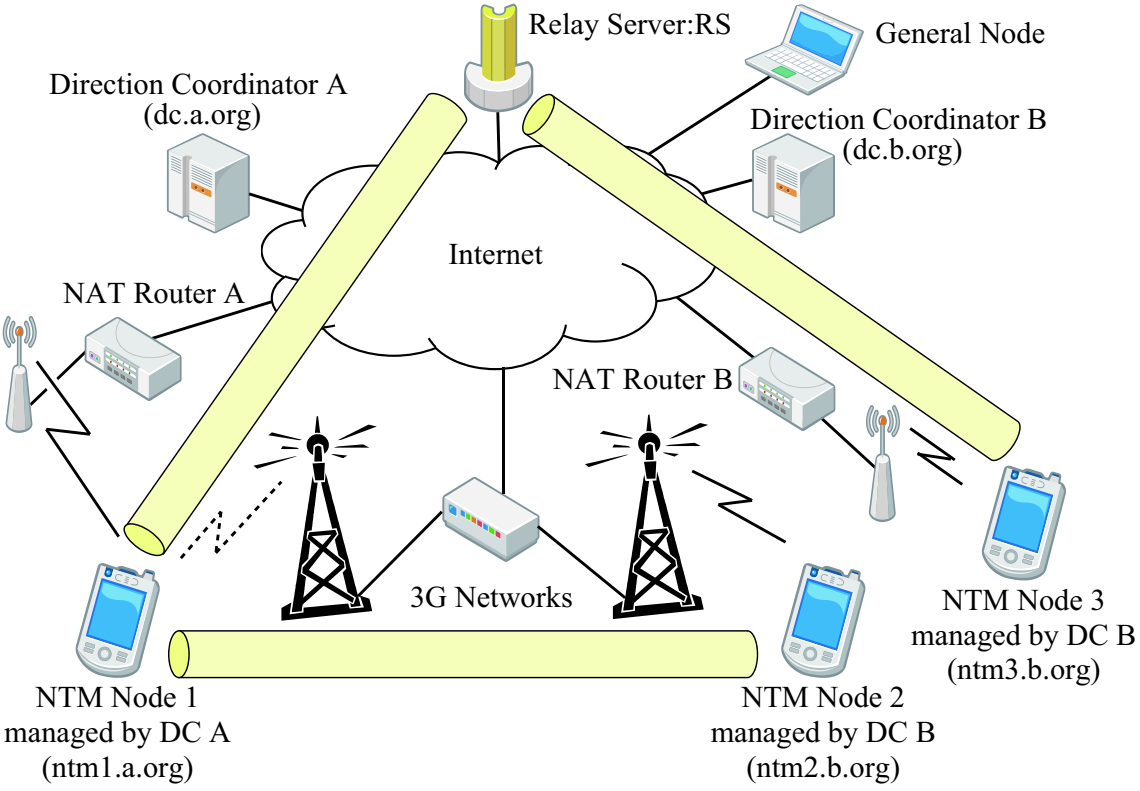


図 3.1 提案法におけるネットワーク概要

3.2　提案法におけるアドレス及び位置情報管理

3.2.1　アドレス管理

提案法では，移動透過性を実現するために，ノード間において一意となる仮想アドレスが割り当てられる必要がある．DC がノードに対して割り当てる仮想アドレスの管理手法について説明する．

提案法では，アプリケーションは仮想 IP アドレスを用いて通信を行う．仮想 IP アドレスは通信を行っている NTM 端末間で一意に端末を識別可能とする必要があるため，重複しないように割り当てを行う必要がある．そこで，管理者は仮想 IP アドレスのアドレス帯域を予め各 DC に割り当てを行うものとする．そして，各 DC は管理する NTM 端末に仮想 IP アドレスの重複が起きないようにアドレスの割り当てを行うものとする．仮想 IP アドレスは IPv6 アドレスの利用を想定している．IPv6 アドレスには大きく分けて 3 種類あり，各インターフェースに付与されるユニキャストアドレス，複数のノードに割り当て可能なマルチキャストアドレス，複数のインターフェースに割り当て可能で最も近いインターフェースに配信されるエニーキャストアドレスがある．また，これらアドレスのそれぞれに対して，あるリンクのみで一意であるリンクローカルなものと，全ての IPv6 アドレスにおいて一意であるグローバルなものがある．また，特殊なアドレスとして，アドレスがまだ割り当てられていないことを示す::で表される無指定アドレスや，ホストが自分自身にデータグラムを送るための::1 で表されるループバックアドレスがある．現在使用されているアドレスとして，ルータを越えてインターネット上で利用可能なグローバルユニキャストアドレスや，LAN の同一セグメント内でのみ利用可能な fe80::/64 で表されるリンクローカルユニキャストアドレス，IPv4 でのプライベートアドレスと同様な役割である fd00::/7 で表されるユニークローカルユニキャストアドレスがある．したがってこれらのアドレスを避けて仮想 IP アドレスの帯域を利用する必要がある．本論文では文書化のために利用される 2001:db8::/32 で表されるアドレスを用いて仮想アドレス割り当ての概要を説明する．なお，IPv6 のサブネットマスクは/48 のように表され，この場合先頭の 48 ビットがネットワークアドレス，それ以降をホストアドレスとして利用される．

図 3.2 は提案法における仮想ネットワーク例を示したものであり，提案法の仮想

ネットワークとして，2001:db8::/32 のアドレス帯域を用いる場合について示している．管理者は DC A に対して 2001:db8:1000::/48，DC B に対して 2001:db8:2000::/48，DC C に対して 2001:db8:3000::/48 のアドレス帯域を予め割り当てを行うことにより，各 DC が管理するアドレス帯域が他 DC と重複しないようにする．また，各 DC は各 DC に管理される NTM 端末に対して割り当てられているアドレス帯域から仮想 IP アドレスの割り当てを行うものとする．結果として，提案法におけるネットワークでは，DC へのアドレス帯域の割り当てのみで仮想 IP アドレスの重複を防ぐことができるため，簡易なアドレス管理を実現可能としている．

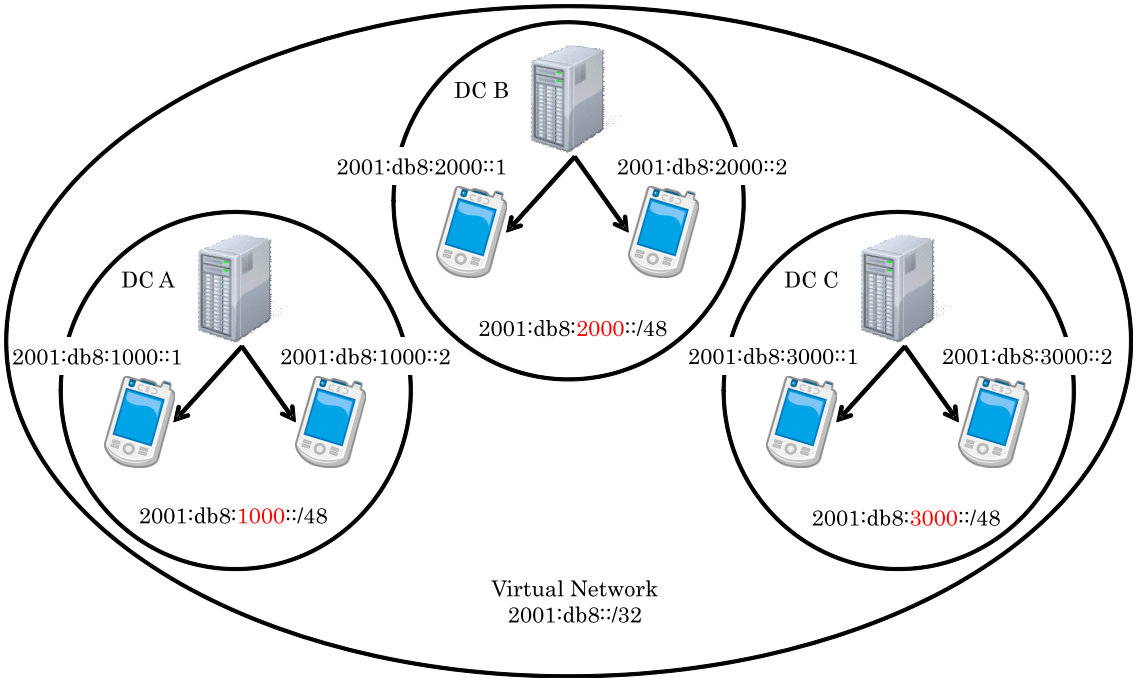


図 3.2 提案法における仮想ネットワーク例

3.2.2　位置管理

提案法では，各 DC が NTM 端末を管理することから，NTM 端末が自身を管理する DC に関する情報を入手する手段が必要となる．また，NTM 端末間の通信を行う際には，通信相手端末の位置情報に関する情報が必要となる．そこで本提案では，情報入手手段として DNS を拡張して利用する．DNS ではホスト名から IP アドレスを検索する際に A レコードの探索を行う．

提案法では，NTM 端末を管理する DC の IP アドレス及び，NTM 端末に関する情報を DNS の専用レコード（NTM レコード）として実装することにより，NTM 端末が移動先ネットワークのプライマリ DNS サーバーを経由して提案法の専用レコードの探索を行う．提案法の専用レコードは IPv4 ネットワークと IPv6 ネットワークに対応可能とするため，IPv4 ネットワーク用の情報と IPv6 ネットワーク用の情報を一つの DNS 専用レコードとして実装を行い，NTM 端末が移動先ネットワークのプライマリ DNS サーバーを経由して専用レコードの探索を行うことが可能となる．表 3.1 は IPv4 ネットワークと IPv6 ネットワークを想定した提案法専用レコードの要素であり，NTM 端末を識別するためのノード ID，物理インタフェースの IPv4/IPv6 アドレス，端末が NAT 配下に存在する場合の NAT ルータの IPv4/IPv6 アドレス，端末を管理する DC の IPv4/IPv6 アドレス，仮想インタフェースの IPv6 アドレス，端末のポート番号，NAT ルータのポート番号が含まれる．なお，物理インタフェースの IPv4/IPv6 アドレスは NTM 端末から通知されることにより登録される．また，NAT ルータの IPv4 アドレスは NTM 端末からのパケットのソースアドレスを確認することにより DC が登録を行う．NAT ルータの IPv6 アドレスはセキュリティの観点等から今後利用される可能性を考慮しレコードの要素として用意されているが，現状では使用しておらず常に::が記載される．ポート番号は Internet Service Provider（ISP）により提案法で利用するポート番号が遮断されてしまう可能性を考慮して，端末では固定のポート番号を利用しないことを想定しており，通信相手の待ち受けているポート番号を取得するために登録を行う．また，NAT のポート番号は NTM 端末からのパケットのソースアドレスを確認することにより DC が登録を行う．

表 3.1 提案法専用レコードフォーマット

Record Name	Record Size
Node ID	128 bit
Real IPv4 Address of NTM node	32 bit
Real IPv4 Address of NAT router	32 bit
Real IPv4 Address of Direction Coordinator	32 bit
Real IPv6 Address of NTM node	128 bit
Real IPv6 Address of NAT router	128 bit
Real IPv6 Address of Direction Coordinator	128 bit
Virtual IPv6 Address of NTM node	128 bit
Port Number of NTM node	16 bit
Port Number of NAT router	16 bit

3.2.3　起動時の位置登録処理

図 3.3, 3.4 は NTM 端末の起動時の位置登録処理である．NTM 端末は以下の手順に従い，DC に自身の位置情報の登録を行う．

DC や RS の台数が小規模で，これらサーバ群の管理者が同一であれば，事前共有鍵方式により信頼関係を構築することができるが，ネットワークの規模が拡大すると，任意の DC 間および DC と任意の RS 間で共通鍵を共有することが困難となる．そこで，DC と RS に公開鍵証明書を発行し，これを用いた相互認証方式を検討している．DC を管理する DC が証明書を発行する役割を担うことより任意の DC 間および DC と RS 間の信頼関係を構築することができる．

登録手順と，NTM レコードに登録する IP アドレスは，NTM 端末が接続しているネットワークごとに手順が異なるため，NTM 端末が IPv4 アドレスのみを取得している場合，NTM 端末が IPv6 アドレスのみを取得している場合，NTM 端末が IPv4/IPv6 アドレスの両アドレスを取得可能なデュアルスタックネットワークに接続している場合について説明する．なお，DC の物理インターフェースの IPv4/IPv6 アドレスや仮想 IPv6 アドレスは，NTM 端末の接続先のネットワークに関わらず，常にアドレスを記載している．NTM 端末をシャットダウンした場合，再度通信を開始するときに以前に接続した DC のアドレスに対して通信を行うため，常に DC の IPv4/IPv6 アドレスを両方記載しておくことで IPv4 ネットワーク，IPv6 ネットワークのどちらからでも通信を開始可能としている．また，常に仮想 IPv6 アドレスを記載することで NTM 端末が IPv4 ネットワークにいても仮想 IPv6 アドレスに基づいた通信を行う，または，IPv6 ネットワークにいても仮想 IPv6 アドレスに基づいた通信を行うことを可能としている．また，A/AAAA レコードには NTM 端末の実 IP アドレス，NTM レコードには，登録用メッセージに記載されている情報をそのまま登録している．

- NTM 端末が IPv4 アドレスのみを取得している場合

  図 3.3 に IPv4 ネットワークにおける起動時の位置登録処理を示す．提案方式では，各 NTM 端末はいずれかの DC により管理されることを想定しており，自身を管理する DC に対して IPv4 ネットワーク経由で自身の FQDN を用いて NTM レコードの検索を行う．検索結果から DC の IPv4 アドレスと IPv6 アドレス，端末の仮想 IP アドレスを取得する．これにより自身を管理する DC を判断することが可能となる．次に IPv4 ネットワーク経由で自身の情報を登録する Registration Request を送信することにより自身の位置情報を登録する．Registration Request には IPv4 ネットワークと IPv6 ネットワークの両情報が記載される．NTM 端末が IPv4 アドレスのみ取得している場合は，ノード ID AAA，端末の実 IPv4 アドレス RIP4MN，端末の仮想 IP アドレス VIPMN，DC の実 IPv4 アドレス RIP4DC，DC の実 IP アドレス RIP6DC，端末のポート番号 PortMN，FQDN A.exp の情報が含まれている．また，NTM 端末の実 IPv6 アドレスには::のみ記載している．なお，DC は Registration Request の送信元アドレスを確認することにより，NTM 端末が NAT 配下にいる場合には，NAT ルータの実 IP アドレスである RIP4NAT と NAT のポート番号 PortNAT も入手可能である．これらの情報は提案法専用の NTM レコードに登録される．登録処理後，DC は Registration Response を NTM 端末に返信を行う．

  また，NTM 端末が NAT ルータ配下に存在する場合，DC から NTM 端末に向けて通信を開始することができない．しかし，本提案方式では DC から NTM 端末に指示を出す必要があるため通信コネクションを維持する必要がある．そこで，NTM 端末は定期的に Update Request を DC に送信し，DC から Update Response を NTM 端末に返信を行うことにより，NAT テーブルを更新することでコネクションを維持する．

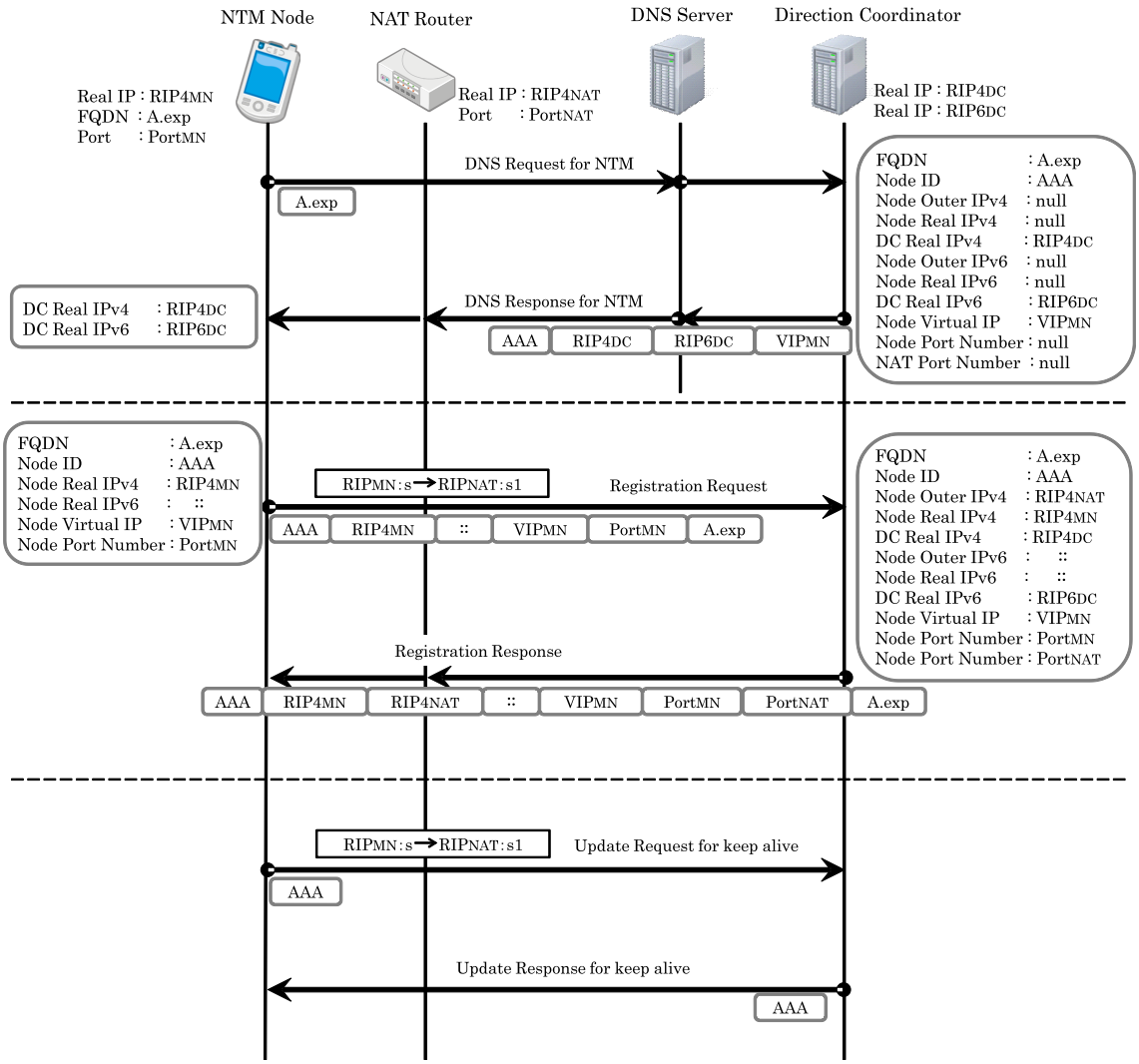


図 3.3 IPv4 ネットワークにおける起動時の位置登録処理

- NTM 端末が IPv6 アドレスのみを取得している場合

  図 3.4 に IPv6 ネットワークにおける起動時の位置登録処理を示す．NTM 端末が IPv6 アドレスのみ取得している場合，自身を管理する DC に対して IPv6 ネットワーク経由で自身の FQDN を用いて NTM レコードの検索を行う．IPv4 ネットワークの動作と同様に，検索結果から DC の IPv4 アドレスと IPv6 アドレス，端末の仮想 IP アドレスを取得する．これにより自身を管理する DC を判断することが可能となる．次に IPv6 ネットワーク経由で Registration Request を送信することにより自身の位置情報を登録する．IPv4 ネットワークの動作と同様に Registration Request には IPv4 ネットワークと IPv6 ネットワークの両情報が記載される．この場合，Registration Request にはノード ID BBB，端末の実 IPv6 アドレス $\mathrm{RIP6_{MN}}$，端末の仮想 IPv6 アドレス $\mathrm{VIP_{MN}}$，DC の実 IPv4 アドレス $\mathrm{RIP4_{DC}}$，DC の実 IP アドレス $\mathrm{RIP6_{DC}}$，FQDN B.exp の情報が含まれている．また，NTM 端末の実 IPv4 アドレスには 0.0.0.0 のみ記載している．

  なお，IPv4 ネットワークと同様に DC は Registration Request の送信元 IP アドレスを確認することにより，NTM 端末が NAT 配下にいる場合には，NAT ルータの実 IP アドレスも入手可能である．これらの情報は提案法専用の NTM レコードに登録される．登録処理後，DC は Registration Response を NTM 端末に返信を行う．

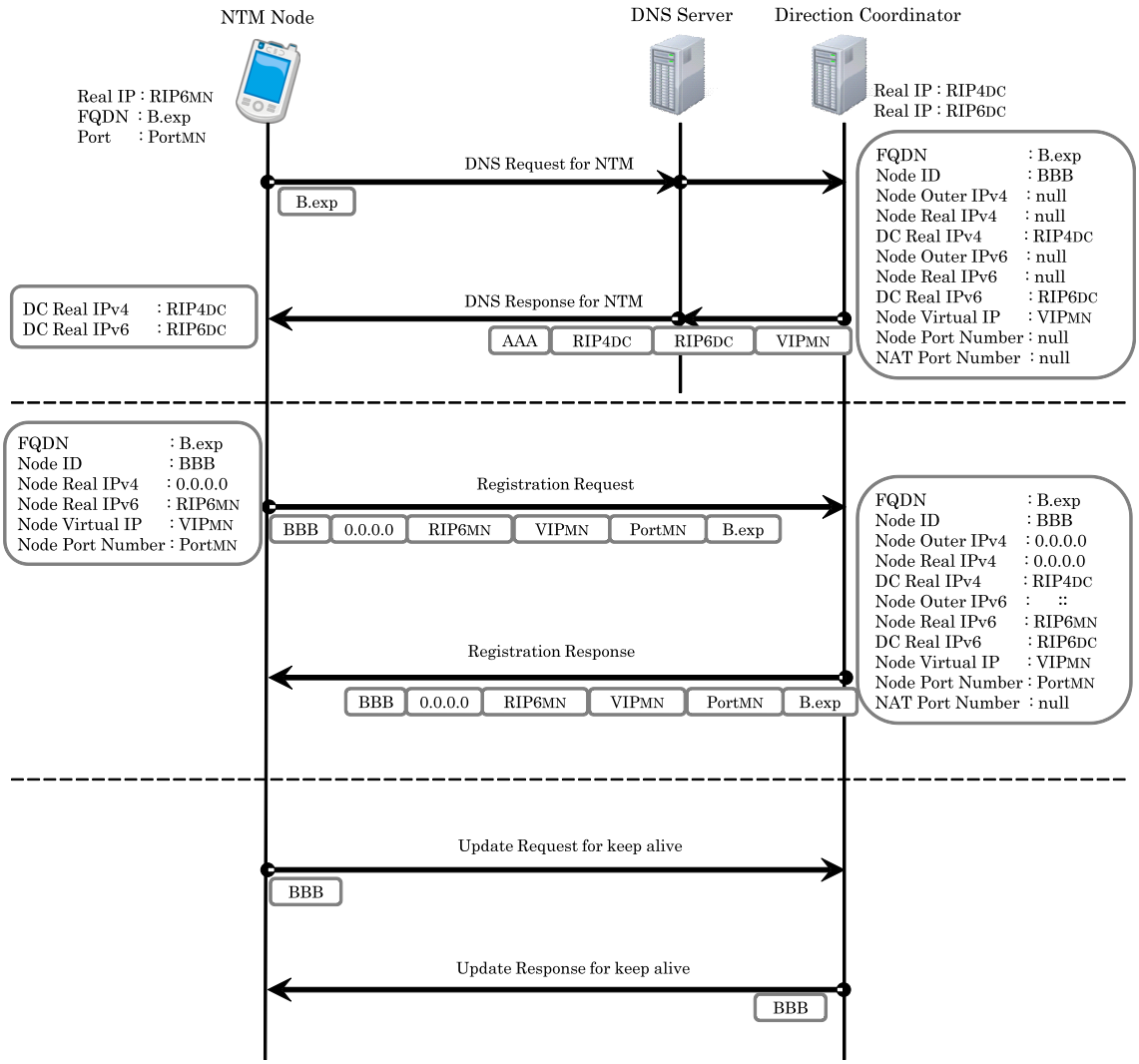


図 3.4 IPv6 ネットワークにおける起動時の位置登録処理

- NTM 端末がデュアルスタックネットワークに接続している場合

  NTM 端末がデュアルスタックネットワークに接続している場合，自身を管理する DC に対して IPv4 ネットワーク経由で Registration Request を送信することにより自身の位置情報を登録する．これは NAT の有無を調べるため IPv4 ネットワーク経由で送信を行い，また IPv6 アドレスではネットワーク内でのみ使用可能なリンクローカルアドレスなどが割り当てられている可能性を考慮しているためである．

3.2.4　移動時の位置更新処理

図 3.5, 3.6 に IPv4 ネットワークと IPv6 ネットワークにおける NTM 端末が移動後に行う処理を示す.

- 位置情報の更新

  NTM 端末が移動により変化した位置情報を DC に対して通知するために, Registration Request に新たな位置情報を記録し自身を管理する DC に向けて送信を行う. DC は位置情報の更新後, NTM 端末に向けて Refistration Response を返信する.

- DC とのコネクション維持

  IPv4 ネットワークを利用している場合, 起動時の位置登録処理と同様に, DC と NTM 端末間のコネクションを維持するために, NTM 端末は定期的に Update Request を DC に送信し, DC からは Update Response を NTM 端末に向けて返信する.

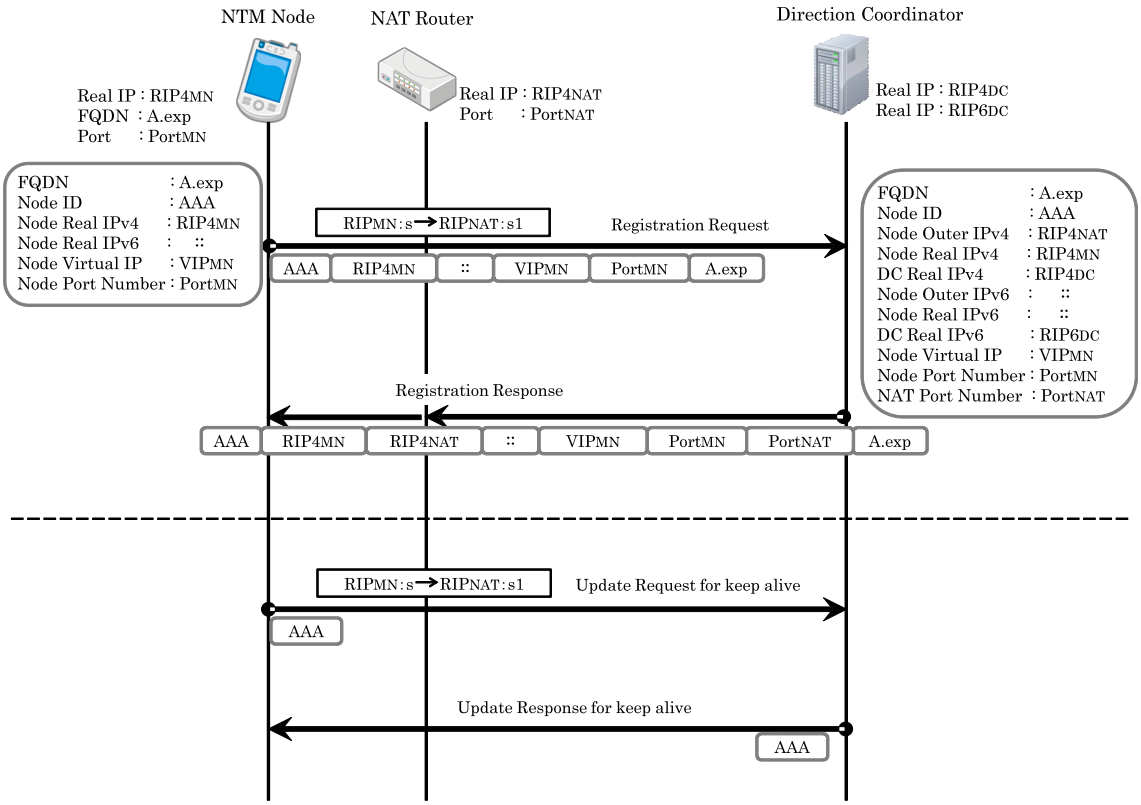


図 3.5 IPv4 ネットワークにおける移動後の位置更新処理

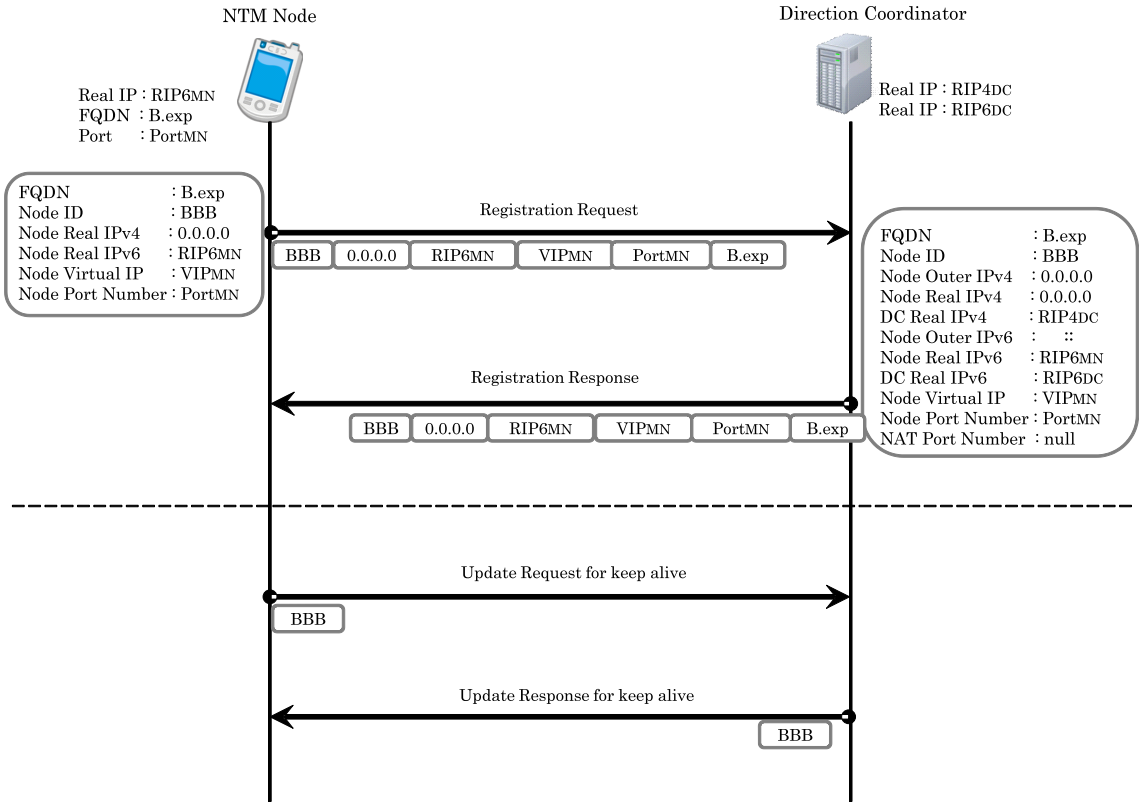


図 3.6 IPv6 ネットワークにおける移動後の位置更新処理

第4章

実装・実験結果

本章では本研究において用いた機器の実装環境および，動作確認，実験時に用いた諸元について記す.

4.1 実装

4.1.1 DC の実装

図 4.1 に提案法における DC のモジュール構成を示す. 提案法における DC 機能は全てユーザ空間に実装されており，アドレスの登録を行う DNS サーバとアドレス管理を行う DC デーモンに大別される. 実装実験では，提案法における専用レコードを実装するにあたり，DNS サーバである BIND の拡張を行った.

- DNS サーバ機能

  本提案方式では，NTM 端末の位置情報を DNS の提案手法専用レコードとして管理を行なっている. 実装においては，DNS サーバである Bind-9.7.1 に IPv4 アドレスと IPv6 アドレス用の提案法専用レコードを定義することにより，NTM 専用の DNS レコードの実装を行った. これにより提案法専用レコードを DNS サーバの機能を用いて問い合わせすることが可能な状況とした. なお，一般の DNS サーバでは本提案法における専用レコードをサポートしていないが，RFC3597 [47] では未知のリソースレコードは圧縮せずに中継することが規定されているため，RFC3597 に準拠した DNS サーバが利用され

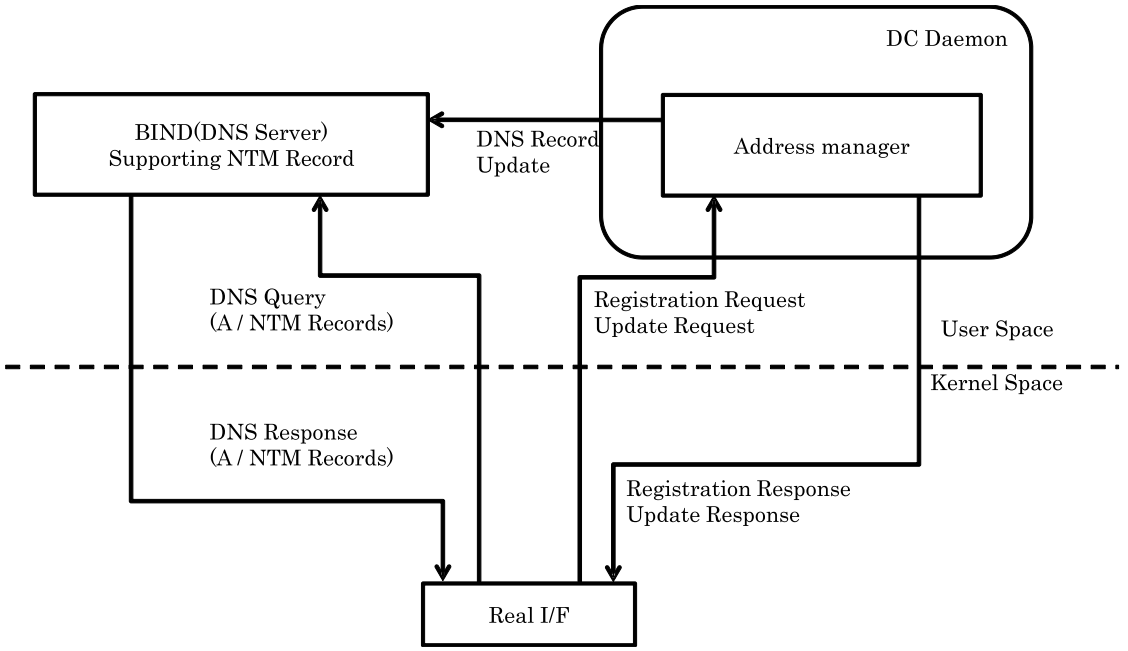


図 4.1 提案法における DC のモジュール構成

ている場合には，提案法にて用いる専用レコードの問い合わせで支障は発生しない．また，DNS サーバは Dynamic DNS に対応しており，DC に実装した機能である DC デーモンからの通知により情報の更新を行うものとする．

- DC の通知

  NTM 端末は最初の起動の時点では自身を管理する DC の情報をもたない．DC は各 NTM 端末の提案法専用レコード内に自身の IP アドレスの情報を含ませる．次に，NTM 端末は自身の FQDN を探索することにより，自身を管理する DC を発見可能としている．このとき一般の DNS サーバを経由する可能性があるが，RFC3597 に準拠した DNS サーバであれば未知のレコードを破棄することなく転送するため，自身の管理する DC に対して問い合わせを到達させることが可能である．

- NTM 端末の位置管理

  NTM 端末は起動後及び移動後は Registration Request を用いて自身の位置情

報を DC に送信するため，DC は受信した位置情報に応じて，Dynamic DNS の機能を用いて DNS の提案法専用レコードの情報を更新する．

4.1.2　NTM 端末の実装

図 4.2 に提案法における NTM 端末のモジュール構成を示す．NTM 端末では，アドレス管理に関する実装をユーザ空間で行っている．ユーザ空間では，IP アドレス変化の検知機能，DNS 情報の更新機能，DNS における提案法専用レコードの問い合わせ機能などを実装することにより，NTM 端末の移動管理とアドレス管理を実現している．本提案手法では，DNS 情報の登録，更新機能を実装した．以下に端末の動作概要を説明する．

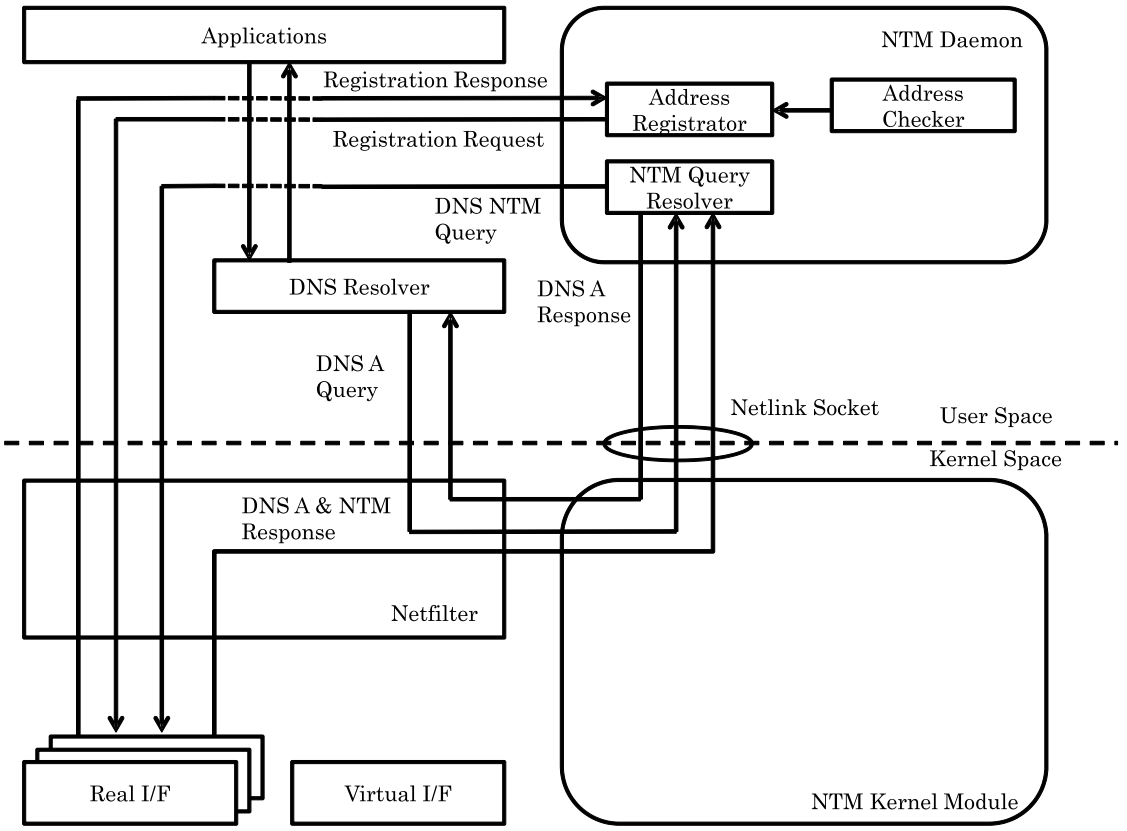


図 4.2 提案法における端末のモジュール構成

- IP アドレス変化の検知

  提案方式において NTM 端末では，ユーザデーモンがインタフェース状態を監視することにより，インタフェースの割り当て IP アドレスの変化を検出する．また，IP アドレスの変化を検出した場合には，IP アドレスの更新処理を行う．

- 提案法専用レコードの登録と仮想 IP アドレスの取得

  NTM 端末は自身の提案法専用レコードの問い合わせを行うことにより，仮想インタフェースで利用する仮想 IP アドレスを DC から取得する．また，NTM 端末は起動時にインタフェースの実 IP アドレスを確認し．自身の DC 対して Registration Request を用いて登録を行う．

- 位置情報の更新

  NTM 端末は IP アドレス変更時に Update Request を用いて自身の仮想 IP アドレス，実 IP アドレスなどを DC に通知することで，位置情報の更新を行う．

本提案手法では DC に対して Registration Request を送信する機能を実装することで動作確認を行なっている．

4.2　動作確認

実装実験では，提案法専用レコードを実装するにあたり，DNS サーバである BIND を拡張した．具体的には，IPv4 アドレスと IPv6 アドレスを管理可能とする提案法専用レコードを新たに定義することにより，IPv4/IPv6 アドレスの混在するネットワークにおいても DNS サーバ機能を利用して専用レコードを問い合わせ可能とした．実験諸元を表 4.1 に示す．

表 4.1 評価諸元

OS	Linux
Distribution	Ubuntu 10.04
Kernel version	linux-2.6.32-24-generic
CPU	Intel Core i7 2.93GHz （4 cores 4 threads）
Memory	2.0 Gbytes
BIND	bind-9.7.1

動作確認に関して，以下の手順の動作を確認した．

- 位置情報の通知

  NTM 端末から位置情報を DC に向けて送信した．

- 位置情報の受信

  DC 上の DC デーモンは NTM 端末からの位置情報を受信した．

- DNS への登録

  DC 上の DC デーモンは受信した位置情報に応じて，拡張した DNS サーバに提案法専用の NTM レコードの追加及び更新を行った．

- NTM レコードの探索

  DC 上の DNS サーバである BIND で管理されている提案法専用の NTM レコードを問い合わせ，提案法専用レコードの情報を取得した．

4.2.1　DC における専用レコード更新処理時間

DC 上のデーモンは多数の NTM 端末からの要求を処理する必要があるため，動作確認だけでなく処理性能も重要と考えられる．そこで，DC 上のデーモンが NTM 端末からの位置情報を受信した後，DNS への専用レコード更新処理が終了するまでの処理時間の測定を行った．測定は 10 回実施し，平均処理時間は約 5.59[msec] であった．また，同様に一般的に用いられる IPv4 アドレスを登録するための A レコードと IPv6 アドレスを登録するための AAAA レコードの更新処理時間の測定も行った．測定は 10 回実施し，平均処理時間は A レコードで 5.51[msec]，AAAA レコードで 5.55[msec] であった．

本結果より，DNS サーバで一般的に用いられる A レコードと，本提案手法で新たに定義した専用レコードとの平均処理時間の差は小さいことが分かった．したがって，DC 上のデーモンは既存の Dynamic DNS を利用しているが，大きなオーバーヘッドは発生しておらず，規模拡張性なども有するものと考えられる．

4.2.2　DC における端末管理可能台数

DC ではネットワークを越えた端末の移動が発生する度に，提案法における専用レコードの更新処理を行う必要がある．そこで，DC 内の拡張した DNS サーバにあらかじめ多くの提案法専用レコードを登録しておき，間隔をあけて端末から更新処理を行い，更新成功率の測定を行った．これにより端末の管理可能台数と，端末がある時間内に何回のネットワーク移動を行なっても正しく更新可能であるかを判断することが可能となる．実際にはあらかじめ DC の DNS サーバに対し 1 万個の専用レコードを登録した場合と，10 万個の専用レコードを登録した場合について行い，端末からの更新間隔を小さくすることで更新成功台数の測定を行なっている．更新要求数は，あらかじめ専用レコードを 1 万個登録した場合では 1 万回，あらかじめ専用レコードを 10 万個登録した場合では 10 万回行った．なお，一般的なレコードである A レコードについても同様の条件で更新成功率を測定した．図 4.3 に更新成功率を示す.

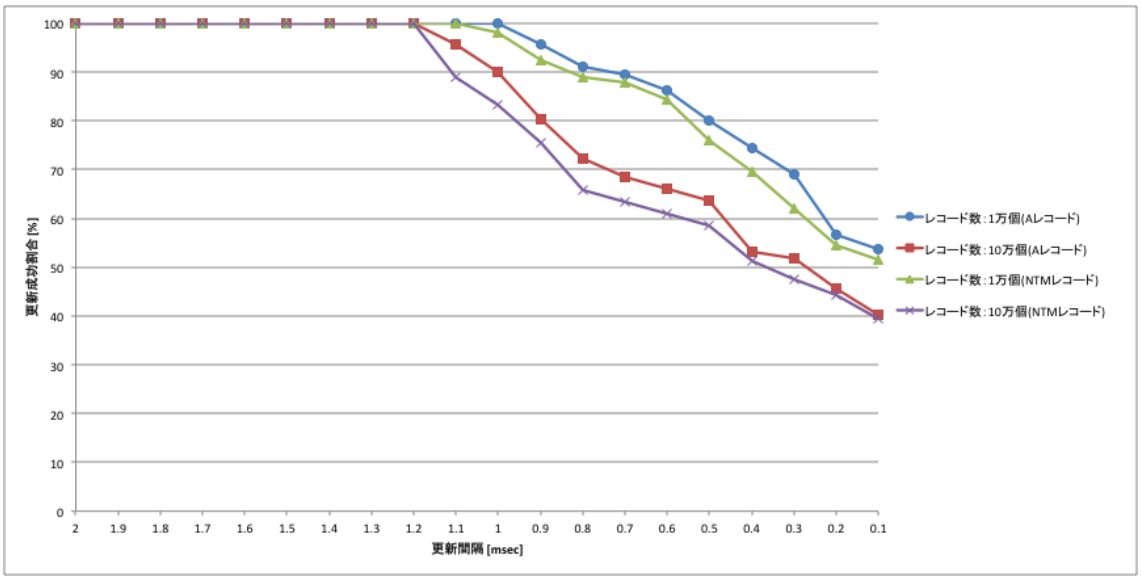


図 4.3 更新処理成功率

図 4.3 より，1 万個の専用レコードをあらかじめ登録した場合では，更新間隔が 1.1[msec] 以上の場合において全ての端末が更新成功となることが分かる．また，10 万個の専用レコードをあらかじめ登録した場合では，更新間隔が 1.2[msec] 以上の場合において全ての端末が更新成功となることが分かる．あらかじめ専用レコードを 1 万個登録したときの更新間隔が 1.0[msec] 以下の場合，またはあらかじめ専用レコードを 10 万個登録したときの更新間隔が 1.1[msec] 以下の場合において更新成功率が 100%でなくなる理由としてネットワークスループットによるパケットロスと CPU の処理限界が考えられるため検証を行った．ネットワークスループットについては iperf を用い，UDP パケットとしてデータ 500[Mbytes] を 5 回転送した結果，95.5[Mbps] であった．提案法で用いているメッセージのサイズは 2816[bits] であり，更新できなくなる間隔を 1.0[msec] とすると，更新できなくなる時点で 1.0[msec] あたり約 2.8[kbits] 送信していることになる．一方ネットワークスループットから考えると，1.0[msec] あたり 100[kbits] パケットを送信することができることがわかる．したがって，送信するメッセージサイズとネットワークスループットを比較して，ネットワークスループットの方が非常に高いため，ネットワークスループットによるパケットロスが更新成功率に大きな影響を与えているわけではないと考えられる．次に CPU に関して全て更新成功可能な更新間隔 1.3[msec]

と，全ては更新成功しない更新間隔 0.5[msec] の時の CPU 使用率をシステムモニターにて確認したところ，1.3[msec] では CPU 使用率が約 60%であり，0.5[msec] では CPU 使用率が 100%になることがあることが分かった．また，一般的なレコードである A レコードと，本提案手法で新たに定義した専用レコードとの比較では，事前に 1 万個と 10 万個のレコードを登録したそれぞれの場合について差が小さいことが分かる．したがって，CPU による処理の限界が更新成功率に影響を与えていると考えられる．

本結果より，あらかじめ専用レコードを 1 万個登録した場合では，1 万の端末全てが 11 秒の間に 1 回ネットワークを移動して更新要求を行なっても，DC において専用レコードを更新可能であることが分かった．また，あらかじめ専用レコードを 10 万個登録した場合では，10 万の端末全てが 120 秒の間に 1 回ネットワークを移動して更新要求を行なっても，DC において専用レコードを更新可能であることが分かった．なお，ネットワークの移動による端末からの更新要求が成功する割合は，DC における CPU の処理性能によって変化するものと考えられる．また，登録台数の妥当性に関して，三重大学の学生数と三重大学に割り当てられた IP アドレスのクラスを用いて考察する．2012 年 5 月 1 日現在，三重大学の学生数は 8824 人であるため，全学生が提案法実装端末を利用した場合において，三重大学に DC を 1 台設置するのみで提案法を実現可能であることがわかる．また，三重大学に割り当てられた IP アドレスはクラス B であり，ホストアドレスの 16bit 分を全て割り当てた場合において，サブネットマスクを考えないとすると 65534 台に割り当てることが可能となるため，同様に三重大学に DC を 1 台設置するのみで提案法を実現可能であることがわかる．したがって三重大学であれば DC を 1 台設置するのみでアドレス管理を実現可能である．

第 5 章

結論

5.1 本論文のまとめ

本研究では，グローバル IP アドレス空間及びプライベート IP アドレス空間によらず，また IPv4 アドレスと IPv6 アドレスの混在ネットワーク環境において移動透過性と NAT 越えを同時に実現可能なアドレス管理手法の提案を行った．既存のネットワークに対して影響を与えることなく，提案法に用いる機器のみ導入することで移動透過性と NAT 越えを同時に実現可能である．本提案手法の管理方式では端末と DC 間の信頼関係が結ばれていれば，あらかじめ DC の情報を端末が知る必要はないため柔軟な運用が可能となる．さらに，アドレス管理を行う DC は複数設置することができるため，ネットワーク規模拡大に対しても柔軟に機器の追加で対応可能である．規模拡大の場合における DC の追加では，仮想 IP アドレスの割り当て方法を工夫したことで容易に重複を防ぐことができるため，新たな DC 導入のハードルも低いと考えられる．また，提案方式は DNS 用の専用レコードを新たに定義するものであり，DNS と同様の規模拡張性を有する方式である．

実装においては，DNS サーバである BIND を拡張することにより提案法専用レコードの実装を行い動作確認を行った結果，提案アドレス管理手法が実現可能であることを確認した．本研究において，DC の導入コストや管理コストを抑えるためにはより多くの端末管理が可能であることが望ましいため，一般的な DNS サーバにおける処理時間と新たなレコードの定義により生じる処理時間を，一般的に用いられる A レコードと AAAA レコード，提案法における専用レコードと

の比較により検証した結果，処理時間の差はほとんどなく新たなレコードの導入に影響がないことを確認した．また，具体的に管理可能な端末の台数を調べるため，DC に対して登録を行う端末数を 1 万台の場合と 10 万台の場合において検証した．この結果から，登録端末数が 1 万台の場合では，登録している 1 万台の全端末が 11 秒の間に一回接続先ネットワークの切り換えを行っても失敗することなく端末情報を更新することが可能であることが分かった．また，同様に登録端末数が 10 万台の場合では，登録している 10 万台の全端末が 120 秒の間に一回接続先ネットワークの切り換えを行っても失敗することなく端末情報を更新することが可能であることが分かった．

これらの結果から提案法は，既存のネットワークに影響を与えることなく新たに機器を導入することのみで移動透過性と NAT 越えを実現し，また移動透過性と NAT 越えに必要なアドレス管理において，実装実験から新たな機器の導入に影響はなく規模拡張性を有する方式であることが確認できた．

参 考 文 献

[1] Buddhikot, M., Chandranmenon, G., Han, S., Lee, Y.W., Miller, S. and Salgarelli, L., “Integration of 802.11 and third-generation wireless data networks, ” Proc. IEEE INFOCOM 2003, Vol.1, pp.503-512, 2003.

[2] Zhang, Q., Guo, C., Guo, Z. and Zhu, W., “Efficient mobility management for vertical handoff between WWAN and WLAN, IEEE Communications Magazine, ” Vol.41, No.11, pp.102-108, 2003.

[3] Le, D., Fu, X. and Hogrere, D., “A Review of Mobility Support Paradigms for the Internet, ” IEEE Communications Surveys, 1st Quarter 2006, Vol.8, No.1, 2006.

[4] Perkins, C., “IP Mobility Support for IPv4, Revised, RFC 5944, IETF, 2010.

[5] Bonola, M., Salsano, S. and Polidoro, A., “UPMT: Universal per-application mobility management using tunnels, ” Proc. 28th IEEE Conference on Global Telecommunications (GLOBECOM ’09), 2009.

[6] Bonola, M. and Salsano, S., “S-UPMT: A secure Vertical Handover solution based on IP in UDP tunneling and IPsec, ” GTTI Riunione Annuale 2010 (online), available from (http://www.gtti.it/GTTI10/papers/gtti10 submission 29.pdf), 2010.

[7] L. A. Magagula and H. A. Chan, “IEEE802.21-Assisted Cross-Layer Design and PMIPv6 Mobility Management Framework for Next Generation Wireless Networks, ” Proc. IEEE WIMOB ’08, pp.159-164, Oct.2008.

[8] Le, D., Fu, X. and Hogrefe, D. “A Review of Mobility Support Paradigms for the Internet, IEEE Communications Surveys, ” Vol.8, No.1, pp.38-51, 2006.

[9] available from (http://www.mip4.org), retrieved, 2012.

[10] C. Perkins, “IP Mobility Support for IPv4, Revised, ” RFC 5944, IETF, 2010.

[11] Johnson, D., Perkins, C. and Arkko, J., “Mobility Support in IPv6, ” RFC 3775,IETF, 2004.

[12] Ishiyama, M., Kunishi, M., Uehara, K., Esaki, H. and Teraoka, F., “LINA: A New Approach to Mobility Support in Wide Area Networks, ” IEICE Trans. Comm., Vol.E84-B, No.8, pp.2076-2086, 2001.

[13] Perkins, C., Johnson, D. and Arkko, J., “Mobility Support in IPv6, Revised, ” RFC 6275, IETF, 2011.

[14] Oliman, H., “Mobile IPv6 Support for Dual Stack Hosts and Routers, Revised, ” RFC 5555, IETF, 2009.

[15] Kuntz, R. and Lorchat, J. “Versatile IPv6 Mobility Deployment with Dual Stack Mobile IPv6, ” pp. 49-54, 2008.

[16] Montenegro, G., “Reverse Tunneling for Mobile IP, revised, ” RFC 3024 ,2001.

[17] Ferguson, P. and Senie, D., “Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing, ” RFC 2827, IETF, 2000.

[18] Perkins, C. and Johnson, D., “Route Optimization in Mobile IP, ” draft-ietf-mobileip-optim-11.txt, 2001, Work in progress.

[19] Moskowitz, R. and Nikander, P., “Host Identity Protocol (HIP) Architecture, ” RFC 4423, IETF ,2006.

[20] Heer, T. and Varjonen, S., “Host Identity Protocol Certificates, ” Revised, RFC 6253, IETF, 2011.

[21] Westerlund, M. and Perkins, C., “IANA Registry for Interactive Connectivity Establishment (ICE) Options, ” RFC 6336, IETF, 2011.

[22] Nikander, P., Gurtov, A. and Henderson, T.R., “Host Identity Protocol (HIP): Connectivity, Mobility, Multihoming, Security, and Privacy over IPv4 and IPv6 Networks, ” IEEE Communications Surveys & Tutorials, Vol.12, No.2, pp.186-204, 2010.

[23] Levkowetz, H. and Vaarala, S., “Mobile IP Traversal of Network Address Translation (NAT) Devices, ” RFC 3519, 2003.

[24] Turanyi, Z., Valko, A. and Campbell, A. T., “4+4: an architecture for evolving the Internet address space back toward transparency, ” SIGCOMM Comput. Commun. Rev., Vol.33, pp.43-54, 2003.

[25] Ng, T. S. E., Stoica, I. and Zhang, H., “A Waypoint Service Approach to Connect Heterogeneous Internet Address Spaces, ” Technical report, USENIX Annual Technical Conference 2001, 2001.

[26] UPnP Forum, “Internet Gateway Device(IGD) Standardized Device Control Protocol V 1.0,” http://www.upnp.org/, 2001.

[27] Cheshire, S., Krochmal, M. and Sekar, K., “NAT Port Mapping Protocol (NAT-PMP), ” Internet Draft draft-cheshire-nat-pmp-03, 2008.

[28] Borella, M., Lo, J., Grabelsky, D. and Montenegro, G., “Realm Specific IP: Framework, ” RFC 3102, IETF, 2001.

[29] Borella, M., Grabelsky, D., Lo, J. and Taniguchi, K., “Realm Specific IP: Protocol Specification, ” RFC 3103, IETF, 2001.

[30] Kondo, K., “Capsulated Network Address Translation with Sub-Address (C-NATS), ” Internet Draft draft-kuniaki-capsulated-nats-05, IETF, 2003.

[31] Francis, P. and Gummadi, R., “IPNL: A NAT-extended internet architecture, ” SIGCOMM Comput. Commun. Rev., Vol.31, pp.69-80, 2001.

[32] Ford, B., Srisuresh, P. and Kegel, D., “Peer-to-Peer Communication Across Network Address Translators, Technical report, ” Proc. USENIX Annual Technical Conference 2005, pp.179-192, 2005.

[33] Huitema, C., “Teredo: Tunneling IPv6 over UDP through Network Address Translations (NATs), ” RFC 4380, IETF, 2006.

[34] Mahy, R., Matthews, P. and Rosenberg, J., “Traversal Using Relays around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN), ” RFC 5766, IETF, 2010.

[35] Wakikawa, R. , Kuntz, R. , Zhu, Z. and Zhang, L. “Global HA to HA Protocol Specification, ” draft-wakikawa-mext-global-haha-spec-02, IETF, 2011.

[36] Rosenberg, J., “Interactive Connectivity Establishment (ICE): A Protocol for Network Address Translator (NAT) Traversal for Offer/Answer Protocols, ” RFC 5245, IETF, 2010.

[37] 鈴木 秀和, 水谷 智大, 西尾 拓也, 内藤 克浩, 渡邊 晃, “NTMobile における相互接続性の確立手法と実装, ” マルチメディア, 分散, 協調とモバイル (DICOMO 2011) シンポジウム論文集, Vol.2011, No.1, pp.1339-1348, 2011.

[38] 内藤克浩, 西尾拓也, 水谷智大, 鈴木 秀和, 渡邊 晃, 森 香津夫, 小林 英雄, “NTMobile における移動透過性の実現と実装, ” マルチメディア, 分散, 協調とモバイル (DICOMO 2011) シンポジウム論文集, Vol.2011, No.1, pp.1349-1359, 2011.

[39] 上醉尾 一真, 鈴木 秀和, 内藤 克浩, 渡邊 晃, “IPv4/IPv6 混在環境で移動透過性を実現する NTMobile の実装と評価, ” マルチメディア, 分散, 協調とモバイル (DICOMO 2012) シンポジウム論文集, Vol.2012, No.1, pp.1169-1179, 2012.

[40] 上醉尾 一真, 鈴木 秀和, 内藤 克浩, 渡邊 晃, “NTMobile の Android 端末への実装と評価, ” 情報処理学会研究報告, Vol.2012-MBL-62, No.19, pp.1-8, 2012.

[41] Salsano, S., Mingardi, C., Niccolini, S., Polidoro, A. and Veltri, L., “SIP-based Mobility Management in Next Generation Networks, ” IEEE Wireless Communication, Vol.15, No.2, 2008.

[42] H. Miyajima, L. Zhang, H. Hayashi and T. Fujii, “An Implementation of Enhanced All-SIP Mobility, ” in Proc. of IEEE PIMRC2008, 2008.

[43] Seta, N., Miyajima, H., Zhang, L., Hayashi, H. and Fujii, T., “All-SIP Mobility: Session Continuity on Handover in Heterogeneous Access Environment, ” Proc. of IEEE VTC2007-Spring, pp.1121-1126, 2007.

[44] 宮島 春弥, 張 亮, 林 秀樹, 藤井 輝也, “移動通信における All-SIP モビリティ, ” 電子情報通信学会誌, Vol.94, No.1, pp.47-51, 2011.

[45] Suzuki, H., Terazawa, K. and Watanabe, A., “Implementation of NAT Traversal for Mobile PPC with the Principle of Hole Punching, ” Proc. IEEE International Region 10 Conference 2009 (TENCON2009), 2009.

[46] Vixie, P., Thomson, S., Rekhter, Y. and Bound, J., “Dynamic Updates in the Domain Name System (DNS UPDATE), ” RFC 2136, IETF, 1997.

[47] Gustafsson, A., “Handling of Unknown DNS Resource Record (RR) Types, ” RFC 3597 (2003).

謝 辞

本研究を遂行するにあたり、多忙な時間を割いてご指導ならびに御助言を下さった小林英雄教授、森香津夫教授、内藤克浩助教に深く感謝いたします. また、研究室の設備などでご協力くださった山本好弘技術職員、ならびに通信工学講座学生諸氏に深く感謝いたします.

研究業績

- 西尾 拓也, 内藤 克浩, 水谷 智大, 鈴木 秀和, 渡邊 晃, 森 香津夫, 小林 英雄, “NTMobile における端末アドレスの移動管理と実装”, マルチメディア, 分散, 協調とモバイル (DICOMO2011) シンポジウム論文集, Vol.2011, No.1, pp.1139-1145, 2011 年 7 月.
- 西尾 拓也, 内藤 克浩, 鈴木 秀和, 渡邊 晃, 森 香津夫, 小林 英雄, “NTMobile 用の IPv6 位置管理方式の提案と実装”, 2011 年電気系学会東海支部連合大会講演論文集, F2-5, 2011 年 9 月.
- 西尾 拓也, 内藤 克浩, 鈴木 秀和, 渡邊 晃, 森 香津夫, 小林 英雄, “NTMobile におけるシームレスな IPv4/IPv6 アドレスの管理手法と実装”, マルチメディア, 分散, 協調とモバイル (DICOMO2012) シンポジウム論文集, Vol.2012, No.1, pp.1180-1186, 2012 年 7 月.
- Takuya Nishio, Katsuhiro Naito, Hidekazu Suzuki, Akira Watanabe, Kazuo Mori, Hideo Kobayashi, “Mobility Management and Implementation of Node Addresses in NTMobile”, in Proc. of the 9th IEEE VTS Asia Pacific Wireless Communications Symposium (APWCS2012), D3-5, CD Proceedings, Kyoto, August 2012.
- Takuya Nishio, Katsuhiro Naito, Hidekazu Suzuki, Akira Watanabe, Kazuo Mori, Hideo Kobayashi, “Implementation of Node Management Scheme in IPv4/IPv6 Networks for NTMobile”, in Proc. of The 2nd International Symposium for Sustainability by Engineering at MIU (IS2EMU 2012), CO-6, November 2012.