IPv4/IPv6 混在ネットワークにおいて通信接続性と移動透過性を実現する NTMobile の研究

鈴木秀和[†1]　上醉尾一真[†1]　納堂博史[†2]
西尾拓也[†3]　内藤克浩[†3]　渡邊晃[†1]

モバイルインターネット環境の普及に伴い，ユーザが通信中に様々なネットワークへ移動することが考えられる．本稿では，IPv4/IPv6 ネットワークが混在した環境において，ネットワークのアドレス空間やアドレス体系に依存することなく，ノードの通信接続性の確立と移動透過性を同時に実現する NTMobile（Network Traversal with Mobility）を紹介する．NTMobile ではノード間にトンネルを構築した上で仮想 IP アドレスを用いたコネクションを確立する．NTMobile を Android スマートフォンおよび Linux PC に実装することにより，IPv4/IPv6 混在環境において通信接続性と移動透過性を確保できることを確認した．

A Study on NTMobile that Achieves Both Connectivity and Mobility in IPv4 and IPv6 Networks

Hidekazu SUZUKI,[†1] Kazuma KAMIENOO,[†1]
Hiroshi Nodo,[†2] Takuya NISHIO,[†3]
Katsuhiro NAITO[†3] and Akira WATANABE[†1]

With the spread of mobile Internet environment, it is thought that users are going to move to various networks during communication. In this paper, we introduce a network architecture called “Network Traversal with Mobility” (NTMobile) that can achieve both connectivity and mobility of nodes in IPv4 and IPv6 networks. An NTMobile node creates a tunnel with a correspondent node, and establishes a connection with their virtual IP addresses through the tunnel. We have implemented the proposed method on Android smartphone and Linux PC, and confirmed that connectivity and mobility are achieved in IPv4 and IPv6 networks.

1. はじめに

近年，スマートフォンやタブレット端末などの高性能な携帯端末と無線通信環境の普及に伴い，ユーザはいつでもどこからでもインターネットに接続することが可能になった．このような携帯端末は，ユーザの位置やネットワークの帯域に応じて，Wi-Fi や 3G などの複数の無線通信メディアを切り替えて通信を行うことができる．このように通信中に通信インタフェースを切り替えたり，異なる無線通信基地局に切り替えると同時に，端末が接続するネットワークも変化するため，端末の IP アドレスが変化してしまう．これにより確立したコネクションが切断されてしまい，通信を継続することができない．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[1)]．

現在のネットワークやネットワークサービスの多くが採用している IPv4 ネットワーク環境では，NAT（Network Address Translation）を導入してプライベート IPv4 ネットワークを利用することが一般的である．また，少しずつではあるが IPv6 ネットワークへの移行も進んでいる．IPv4 と IPv6 は互換性がないため，当分の間は IPv4 と IPv6 が共存するネットワーク環境になることが想定されている．このような異なるアドレス空間/アドレス体系が混在する環境において移動透過性を実現するためには，通信開始時や移動時における端末間の通信接続性を確実に確保する必要がある．

そこで筆者らは，IPv4/IPv6 混在環境において通信接続性と移動透過性を同時に実現する NTMobile（Network Traversal with Mobility）を提案している[2),3)]．本稿では，NTMobile アーキテクチャの全貌と IPv4/IPv6 混在環境で想定しうる状況下において，どのように通信接続性と移動透過性を実現するのかについて述べる．また，NTMobile を市販の Android スマートフォンへ実装し，実環境において動作検証を行った．その結果，プライベート IPv4 ネットワーク，グローバル IPv4 ネットワーク，IPv6 ネットワーク間で確実に通信を開始することができ，かつ通信中に様々なネットワークへ移動しても通信を継続できることを確認した．

†1 名城大学大学院理工学研究科
Graduate School of Science and Technology, Meijo University
†2 名城大学理工学部
Faculty of Science and Technology, Meijo University
†3 三重大学大学院光学研究科
Graduate School of Engineering, Mie University

2. 関 連 研 究

本章ではアドレス空間やアドレス体系が異なるネットワークにおいて，移動透過性を実現する既存技術について述べる．

2.1 DSMIP

DSMIPv6 は，IPv6 ネットワークにおいて移動透過性を実現する Mobile IPv6 を IPv4/IPv6 混在環境へ適用した技術である[4]．DSMIPv6 では移動端末に対して，ホーム ネットワークで取得する HoA（Home Address）と訪問先ネットワークから取得する CoA（Care of Address）の 2 種類のアドレスを割り当て，アプリケーションが HoA を用いた通信を行うことにより，端末の移動に伴う CoA の変化を隠蔽する．

Mobile IPv6 では経路最適化を行うことにより，MN（Mobile Node）と CN（Correspondent Node）間にてエンドツーエンドの通信を行うことができる．しかし，IPv6 特有のヘッダオプションを使用するなど，IPv4 パケットへの適用を想定していない．そのため，MN が IPv4 ネットワークに位置する場合や IPv4 アプリケーションを使用している場合には，経路最適化を行うことができない．また，MN が NAT 配下に接続している際には，常に HA（Home Agent）を介した冗長な経路で通信を行うか，特殊な NAT が必要となる[5]．

2.2 HIP

HIP（Host Identity Protocol）は IETF にて標準化された次世代モバイルプロトコルである[6]．HIP では，IP 層の上位に新たに HIP 層を定義し，固定のノード識別子 HI（Host Identifier）とネットワーク から取得した IP アドレスの変換を行う．上位層においては HI を用いたコネクションを確立することにより，端末の移動に伴って IP アドレスが変化しても，その影響を受けることなく通信を継続することができる．また，HIP では IPv4 ネットワークにおいて NAT 越えを実現するために，ICE（Interactive Connectivity Establishment）[7] を用いた手法が提案されている[8]．ICE を用いることにより，通信経路上に存在する NAT の種類に応じて最適な経路で通信を行う事ができる．しかし，ICE には通信開始時に行うシグナリングにより 2〜10 秒程度のオーバヘッドが発生するという課題がある[9]．

2.3 UPMT

提案技術と類似したアプローチにより NAT をまたがった移動透過性を実現する技術として，UPMT（Universal Per-Application Mobility management using Tunnels）が提案されている[10),11]．UPMT はアプリケーション層の移動透過技術で，NAT 配下に存在するノードはインターネット上に設置した AN（Anchor Node）に対してトンネルを構築し，AN は受信パケットをデカプセル化した後，NAT によるアドレス変換を行って通信相手ノードへ転送する．

しかし，通信相手ノードがグローバルネットワークに存在していても常に AN を中継したデータ転送となるため，提案方式と比較すると経路が冗長であること，また AN に負荷が集中するなどの課題がある．なお，UPMT においても ICE を用いてエンドツーエンド通信を行う拡張仕様があるが，前述の通りシグナリングのオーバヘッドが高いと考えられる．また，IPv4 と IPv6 をまたがった通信や移動については考慮されていない．

3. NTMobile アーキテクチャ

3.1 要 求 仕 様

NTMobile では，以下に示す 6 つの要求を実現するアーキテクチャである．

(1) どのようなネットワーク環境であっても通信接続性を確保したい．
(2) 通信中にネットワークを自由に切り替えたい．
(3) 既存のアプリケーションをそのまま利用したい．
(4) 既存のルータや NAT などの通信設備を変更したくない．
(5) 通信経路はできるだけ最適化したい（エンドツーエンド通信）．
(6) 既存端末との接続性が確保できる．

3.2 概　　要

NTMobile では仮想 IP アドレスを導入することにより，ノード識別子と位置識別子を完全に分離する．仮想 IP アドレスはノード識別子であり，既存のアプリケーションがコネクション/セッションを確立する際に使用する．端末が実ネットワークから割り当てられる実 IP アドレスは位置識別子であり，アプリケーションが確立したコネクションをカプセル化することにより，既設のルータの経路制御により仮想 IP アドレスに基づくパケットを転送する．

3.2.1 システム構成

図 1 に NTMobile アーキテクチャの概要を示す．NTMobile システムは，NTMobile を実装した端末（NTM 端末），NTM 端末のアドレス情報や NTM 端末にトンネル構築を指示する DC（Direction Coordinator），特定の状況下において NTM 端末間または NTM 端末と一般端末間の通信を中継する RS（Relay Server）から構成される．

NTM 端末はデュアルスタックをサポートし，IPv4 ネットワーク，IPv6 ネットワーク，およびデュアルスタックネットワークに接続することができる．ここで，IPv4 プライベート

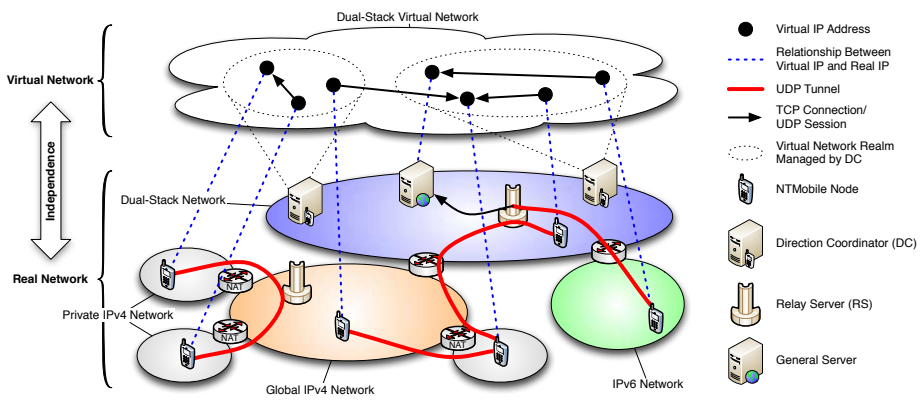


図 1　NTMobile アーキテクチャの概要
Fig. 1　Overview of NTMobile architcture.

ネットワークを構成する NAT ルータは，SPI（Stateful Packet Inspaction）などのフィルタリング機能を実装している一般的な NAT ルータであり，NTMobile に関わる特別な機能は一切持つ必要はない．NTM 端末は上記すべてのネットワークへの移動を想定しており，無線 LAN や 3G，WiMAX などの無線通信インタフェースを実装しているスマートフォンのような携帯端末を想定している．

DC は Dynamic DNS 機能を有しており，NTM 端末の FQDN と実 IPv4/IPv6 アドレスの対応関係に加えて，3.2.2 項で述べる仮想 IP アドレスを管理する．DC はそれぞれ重複のない仮想アドレスプールを保有しており，NTM 端末が起動時に行うアドレス登録処理の際に仮想 IP アドレスを割り当てる．また，NTMobile 専用の DNS レコード（NTMv4/v6 レコード）を定義し，DC は NTM 端末の実 IP アドレスと仮想 IP アドレスの対応関係も管理する．NTM 端末のアドレス管理の他，3.5 節で述べるトンネル構築の指示，および NTM 端末間の暗号化通信や認証に用いる暗号鍵の生成，配布も行う．

RS は下記のケースに該当する場合に，端末間の通信を中継する役割を担う．

- NTM 端末が NTMobile を実装しない一般端末と通信する場合
- 2 台の NTM 端末が異なるプライベート IPv4 ネットワークに存在する場合
- 2 台の NTM 端末が IPv4 ネットワークと IPv6 ネットワークに分かれて存在する場合

通信を中継する RS は，トンネル構築時に DC によって決定される．

DC と RS は全ての端末からアクセスを受けられるよう，デュアルスタックネットワーク上に設置される．また，ネットワークの規模に応じて複数台設置することにより，DC や RS に発生する処理負荷を分散することが可能で，スケーラビリティを確保できる．

3.2.2　仮想 IP アドレス

NTM 端末には，接続先ネットワークから割り当てられる実 IPv4/IPv6 アドレスの他に，各 DC で管理されている仮想 IPv4/IPv6 アドレスが起動時に割り当てられる．NTMobile における仮想 IP アドレスは次のような特徴を持つ．

- 実ネットワークから独立した一意なアドレスであり，一度設定されたら端末が再起動するまで同じアドレスが使われ続ける．
- 仮想 IP アドレスは実ネットワークのアドレスと衝突しないよう定義され，unreachable なアドレスでもよい．

NTM 端末は接続先ネットワークのアドレス体系に関わらず，常に仮想 IPv4/IPv6 アドレスの両方を保持している．すなわち，NTMobile では実 IP ネットワーク上に仮想デュアルスタックネットワークが構築されており，NTM 端末は仮想ネットワーク上で通信相手端末と通信を行うことになる．NTMobile では IP 層より上位層の通信を仮想 IP アドレスを用いて確立することにより，NTM 端末は接続しているネットワークのアドレス空間やアドレス体系の違いを考慮しなくてよい．従って，NTM 端末がネットワークを移動して実 IP アドレスが変化しても，アプリケーションからその変化は隠蔽され，常に一意なアドレス情報をアプリケーションへ提供することができる．

3.2.3　トンネル通信による仮想コネクションの確立

仮想 IP アドレスは unreachable な値であるため，そのままでは実ネットワーク上で正しくルーティングすることができない．そのため，仮想 IP アドレスで確立された通信の IP パケットを実ネットワークで転送するために，NTM 端末間で UDP トンネルを構築する．**表 1** に構築されるトンネル経路の一覧を示す．NTMobile では，できる限りエンドツーエンド通信が行えるように，通信ペアとなる NTM 端末が存在するネットワークに応じて，DC から NTM 端末に対して最適なトンネル構築が指示される．

通信ペアが共に IPv4 ネットワークに接続している場合，どちらか一方の NTM 端末がグローバル IPv4 ネットワークに存在すれば，他方は NAT 配下のプライベート IPv4 ネットワークにいても，エンドエンドの最適経路によるトンネル通信を実現できる．このとき，UDP トンネルを用いて実ネットワーク上で通信を行うため，NTM 端末間の通信経路上に SPI に対応した NAT ルータが存在しても，アドレス変換されるのはカプセル化ヘッダであ

表 1　IPv4/IPv6 ネットワーク間の通信可否とトンネル経路
Table 1　Availability of communication and its tunnel route between IPv4/IPv6 networks.

通信開始側 NTM 端末の接続先ネットワーク	通信相手端末の接続先ネットワーク（NTM 端末／一般端末）							
	Global IPv4		Private IPv4 (A)		Private IPv4 (B)		IPv6	
Global IPv4	○	△[*1]	○	×	○	×	△	△
Private IPv4 (A)	○	△[*1]	○[*2]	⊗	○[*2]	×	△	△
Private IPv4 (B)	○	△[*1]	○[*2]	×	○[*2]	⊗	△	△
IPv6	△	△	△	×	△	×	○	△[*1]

○：End-to-End，△：RS 経由，⊗：End-to-End（トンネルなし）だが移動不可，×：通信不可
[*1]：NTM 端末が移動時に通信を継続したい場合．
[*2]：経路最適化を適用した場合．経路最適化を行わない場合は △．

り，確実に仮想 IP アドレスによるコネクションを確立することができる．

通信ペアが共に同一の NAT 配下，または異なる NAT 配下のプライベート IPv4 アドレスに存在する場合は，RS に対してトンネルを構築する．RS は双方のトンネル経路上で確立される仮想コネクションを中継する．なお，NTMobile では経路最適化を定義しており，この処理が可能な場合はトンネル通信を RS 経由からエンドエンドの最適パスに切り替えることができる[12]．RS 経由の通信中に両 NTM 端末が直接通信相手にトンネル構築用の制御メッセージを投げ合ってみる．NAT の種類によってはメッセージの交換ができる場合があり，その場合は両 NTM 端末間で直接トンネルを構築することができる．

RS に対してトンネルを構築する別のケースとして，通信相手が一般端末の場合がある．この場合，RS は NTM 端末からのパケットをデカプセル化した後，送信元/宛先仮想 IP アドレスをそれぞれ RS および一般端末の実 IP アドレスへ変換する．これにより，RS が NTM 端末の代理で一般端末と通信を行うことになる．そのため，一般端末に対して NTM 端末のアドレスは隠蔽されるため，NTM 端末は移動しても通信を継続することができる．

一方，IPv6 ネットワークに着目すると．通信ペアは常にエンドエンドで通信が可能である．従って，仮想 IP アドレスによるコネクションを実ネットワーク上で確立するために，NTM 端末間で UDP トンネルが構築される．通信ペアが IPv4 ネットワークと IPv6 ネットワークに別れている場合は，両 NTM 端末はデュアルスタックネットワークに設置されている RS へトンネルを構築する．この場合，UDP/IPv4 トンネルと UDP/IPv6 トンネルが構築されるが，その上で確立される仮想コネクションは IPv4/IPv6 どちらでも構わない．

このように UDP トンネルを NTM 端末間，または RS と構築することにより，仮想デュアルネットワーク上で確立される通信を実ネットワーク上でルーティングすることができる．さらに UDP でカプセル化される仮想 IP アドレスに基づく IP パケットは，DC から配布される暗号鍵で暗号化され，盗聴の防止や改ざんの検出が可能である．

3.3　アドレス登録処理

NTM 端末 N は起動時に接続先ネットワークから取得した実 IPv4 アドレス $4RIP4_N$ または実 IPv6 アドレス $RIP6_N$ を DC_N へ登録する．DC_N はこれらの実 IP アドレスと NTM 端末の FQDN の対応関係を，A/AAAA レコードとして登録する．また，DC_N は NTM 端末 N へ仮想 IPv4 アドレス $VIP4_N$ と仮想 IPv6 アドレス $VIP6_N$ を配布し，NTMv4/v6 レコードに実 IPv4/IPv6 アドレスとの対応関係を登録する．NTMv4/v6 レコードには，上記の他に DC_N の IP アドレスや，NTM 端末 N がプライベートネットワークに存在する場合は，NAT ルータのグローバル IP アドレスなどが併せて登録される．

なお，NTM 端末 N と DC_N 間，各 DC 間および DCRS 間には信頼関係があるものと仮定する．また，NTM 端末 N がプライベートネットワークに存在する場合は，DC_N に対して定期的に Keep-Alive を実行し，NTMobile 制御チャネルを維持する[⋆1]．

3.4　名前解決処理

NTMobile は，NTM 端末が通信開始時に行う名前解決処理をトリガとして動作する．図 **2** に NTMobile のシーケンス概要を示す．以降，通信開始側 NTM 端末を MN，通信相手側 NTM 端末を CN と表記し，MN から CN に対して通信を開始する場合について述べる．

MN のアプリケーションは CN の FQDN から IP アドレスを解決するために，DNS 問い合わせを行う．MN の DNS リゾルバはプライマリ DNS サーバに対して A レコードを問い合わせるクエリを送信する．CN の IP アドレスを管理している DC_{CN} は CN の実 IPv4 アドレス $RIP4_{CN}$ を応答する．この応答を受信した MN は，DNS リゾルバへ渡す前にこれを一時待避させておき，CN の仮想 IP アドレスなどの情報を取得するために NTMv4/NTMv6 レコードの問合せを行う，これにより，MN は DC_{CN} から CN の仮想 IPv4/IPv6 アドレスの他，CN がプライベート IPv4 ネットワークに存在する場合は NAT ルータのグローバル IPv4 アドレスなどを取得する．

この後，DC_{MN} および DC_{CN} と共に通信ペアとなる端末間でトンネル構築処理を実行する．トンネル構築が完了したら，待避していた A レコードの応答に記載されている CN の実 IP アドレス RIP_{CN} を仮想 IP アドレス VIP_{CN} に書き換えて，DNS リゾルバへ渡す．以上の処理により，MN のアプリケーションは CN の IP アドレスを VIP_{CN} と認識する．

⋆1 アドレス登録時に NAT ルータにマッピングされたポート番号を維持するため．

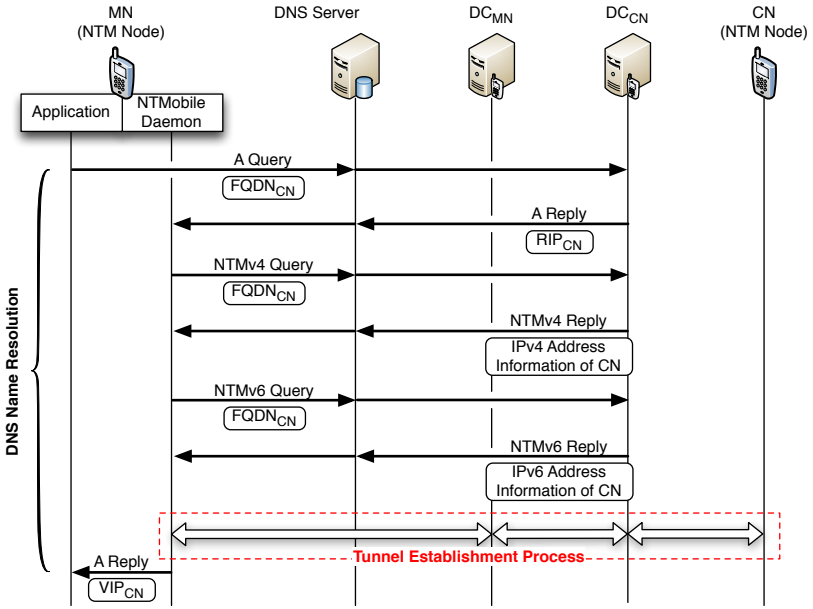
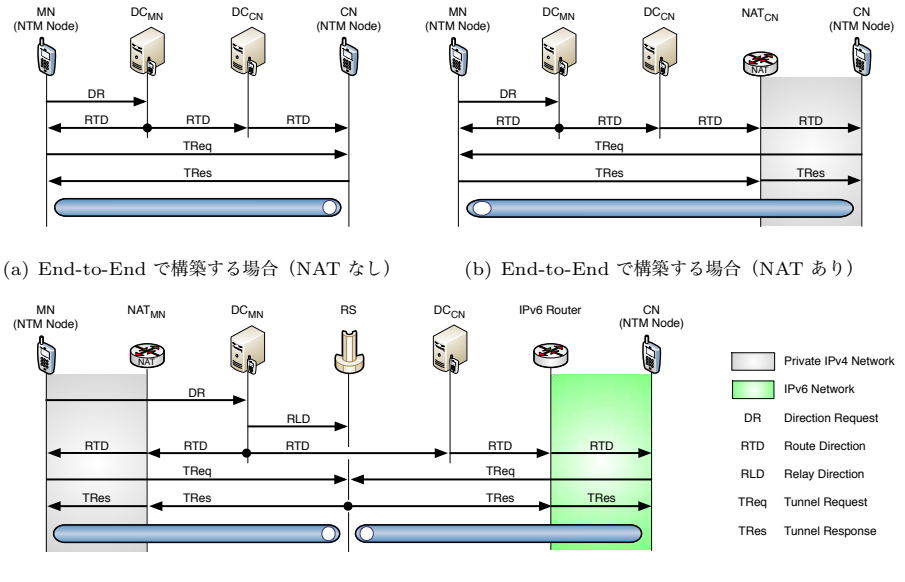


図 **2**　NTMobile シーケンス
Fig. 2　NTMobile sequence.



(a) End-to-End で構築する場合（NAT なし）　(b) End-to-End で構築する場合（NAT あり）

(c) RS を経由する場合（IPv4-IPv6 間の例）

図 **3**　トンネル構築処理
Fig. 3　Tunnel Establishment Process.

3.5　トンネル構築処理

図 **3** にトンネル構築シーケンスの例を示す．トンネル構築処理は，MN と CN の接続先ネットワークの組み合わせにより，複数パターンのトンネル構築シーケンスが存在するが，処理手順はすべて次の 3 ステップで構成されている．

(1)　NTM 端末は DC にトンネル構築の指示を要求する．
(2)　DC は通信ペアとなる端末のアドレス情報から，最適なトンネル経路を求め，NTM 端末にトンネル構築の指示を出す．
(3)　NTM 端末は DC からの指示に従ってトンネルを構築する．

本稿では以下の 3 つの基本パターンについて説明する．

3.5.1　End-to-End でトンネルを構築する場合（NAT ルータなし）

MN と CN 間の通信経路上に NAT ルータが存在しない場合は，図 **3(a)** に示すように MN から CN に対して直接トンネル経路を構築する．このトンネル構築シーケンスとなるのは，

- MN と CN が共にグローバル IPv4 ネットワークに存在する．
- MN と CN が共に IPv6 ネットワークに存在する．

場合であり，最も基本的なパターンである．

MN は DS_{MN} へ Direction Request メッセージを送信する．このメッセージには MN 自身のアドレス情報と NTMv4/v6 レコードにより入手した CN のアドレス情報，および CN との間に構築するトンネルの識別子 PID_{MN-CN} が記載されている．

MN は DS_{MN} へ Direction Request メッセージを送信する．このメッセージには MN 自身のアドレス情報[⋆1]と名前解決処理で入手した CN のアドレス情報，および CN との間に

⋆1 アドレス登録時に DS_{MN} から NTMv4/NTMv6 レコードを問い合わせた結果．

構築するトンネルの識別子 PID_{MN-CN} が記載されている．

DS_{MN} は Route Direction メッセージにより，MN に対しては CN へ向けて直接トンネルを構築するよう指示する．一方，CN に対しては MN からのメッセージを待つよう指示する．なお，Route Direction は DS_{MN} が生成した共通鍵 K_{MN-CN} を MN と CN に配布する役割も担う．

MN は CN に向けて Tunnel Request メッセージを送信する．CN は Tunnel Response メッセージを応答し，トンネルの構築を完了する．両 NTM 端末は，どの仮想アドレス宛のパケットをどの UDP トンネルに入れて転送するかを記録するトンネルテーブルを生成する．

3.5.2 End-to-End でトンネルを構築する場合（NAT ルータあり）

MN と CN 間の通信経路上に NAT ルータが存在する場合は，図 **3(b)** に示すように NAT ルータの配下に存在する NTM 端末から Tunnel Request を送信する．この場合，CN から MN に対して直接トンネル経路を構築することになる．このトンネル構築シーケンスとなるのは，

- MN と CN がグローバル IPv4 ネットワークとプライベート IPv4 ネットワークに分かれて存在する．

場合でのみである．

DS_{MN} は CN に対して MN に向けて Tunnel Request を送信するよう指示を出す．このとき，CN は NAT_{CN} の配下に存在するが，定期的に Keep-Alive により維持している制御チャネルを用いることにより，NAT の外側から内側へメッセージを届けることができる．

3.5.3 RS に対してトンネルを構築する場合

上記 2 パターン以外では直接トンネルを構築することが困難であるため，RS を経由したトンネル経路を構築することになる．このトンネル構築シーケンスとなるのは，次のケースである．

- MN と CN が異なるプライベート IPv4 ネットワークに存在する．
- MN と CN が異なるアドレス体系（IPv4 と IPv6）のネットワークに存在する．
- MN の通信相手が NTMobile を実装しない一般端末である．

IPv4/IPv6 混在環境では，図 **3(c)** に示すように必ずデュアルスタックネットワーク上に設置された RS を経由する必要がある．そこで，DC_{MN} は RS に対して MN と CN からの Tunnel Request メッセージを待ち受けるよう指示する．次に，MN と CN に対して RS に向けて Tunnel Request を送信するよう指示する．以上の処理により，MN と CN は同一の RS との間にトンネルを構築する．RS ではどの仮想アドレス宛のパケットをどの UDP トンネルに入れて中継転送するかを記録するリレーテーブルが生成される．

3.6 カプセル化転送処理

MN は名前解決処理により CN のアドレスを仮想 IP アドレス VIP_{CN} と認識しているため，このアドレスに向けてパケットデータの送信処理が行われる．IP 層において，MN はトンネルテーブルに基づいて送信元 VIP_{MN}・宛先 VIP_{CN} のパケットをカプセル化する．このとき，新しく追加されたカプセル化ヘッダに記載される IP アドレスは，MN 自身の実 IP アドレス RIP_{MN} とトンネル出口の CN または RS の実 IP アドレスとなる．その後，トンネル構築処理中に共有した共通暗号鍵 K_{MN-CN} を用いて暗号化および HMAC（Hash-based Message Authentication Code）の付与を行い，パケットを送信する．

従って，NTM 端末間の通信経路上に NAT ルータが存在する場合は，外側の IP ヘッダおよび UDP ヘッ ダが NAT によりアドレス変換され，カプセル化されたオリジナルの IP パケッ トは仮想 IP アドレスのまま維持される．RS を中継する場合はリレーテーブルに従って，外側の IP ヘッダと UDP ヘッダの IP アドレス・ポート番号を変換して転送する．トンネルの出口に当たる CN は，受信したパケットを復号・デカプセル化してから上位アプリケーションへ渡す．

以上の処理により，NTM 端末が存在するネットワークに応じた最適なトンネル経路が構築され，仮想 IP アドレスによる通信接続性を確立することができる．なお，同一 NTM 端末間であれば，構築された 1 つのトンネルで複数のコネクションをまとめて転送することができる．

3.7 ハンドオーバ時のトンネル再構築

NTM 端末が移動して実 IP アドレスが変化した場合，通信開始時とまったく同じトンネル構築処理を実行してトンネルの再構築を行う[3]．図 **4** に NTM 端末移動時におけるアドレスの変化の様子を示す．例えば，プライベートネットワークに接続した MN が IPv6 ネットワークに存在する CN と仮想 IPv4 アドレスによる通信を開始した場合，MN と CN はデュアルスタックネットワーク上の RS を中継してトンネル通信を行う．この状態で MN がグローバル IPv4 ネットワークへ移動すると実 IP アドレスが変化するため，MN はトンネルの再構築を行う．トンネルの再構築処理が完了しても，NTM 端末の上位アプリケーションは常に同一の仮想 IP アドレスに基づいたコネクションを確立しているため，実 IP アドレスの変化に影響されることはなく，通信継続性を満たすことができる．さらに MN がデュアルスタックネットワークへ移動すると，実 IPv4 アドレスが変化すると共に，IPv6 アドレスを取得する．このとき，MN は CN と IPv6 による直接通信が可能なため，CN に対し

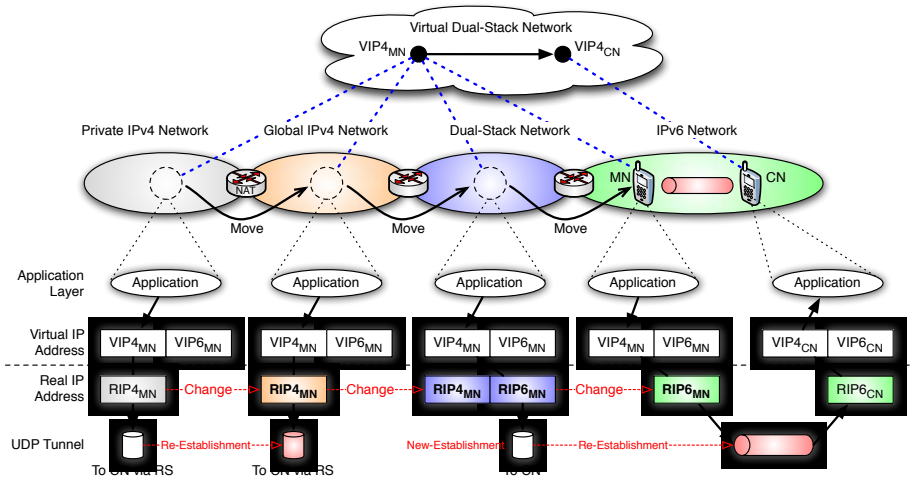


図 4　NTM 端末の移動に伴う IP アドレスの遷移
Fig. 4　IP address transition associated with move of NTM node.

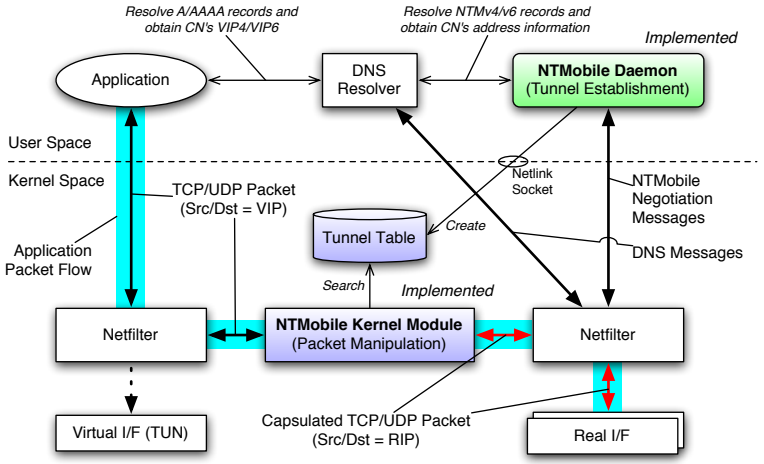


図 5　モジュール構成（NTM ノード側）
Fig. 5　Module configuration (NTM node).

て UDP/IPv6 トンネルを直接構築する．これまでの RS 経由の通信から CN への直接通信に自動的に切り替わるため，RS の負荷軽減や伝送遅延の減少，またスループットの向上などを図ることができる．その後も MN は移動を繰り返すたびにトンネルの再構築を行うが，上位層で確立した仮想コネクションは常に維持される．

また，トンネルの再構築と平行して，DC に登録されている NTM 端末のアドレス情報を更新することにより，移動後の NTM 端末に対する到達性を提供することができる．すなわち，NTMobile は通信接続性を確立するしくみをそのまま移動透過性の実現手法として応用しており，その結果，NTM 端末は通信中に様々なアドレス空間のネットワークへ移動しても通信を継続することができる．

4. 実　　装

NTMobile は Android OS を搭載した携帯端末での利用を想定しているため，Linux カーネルで実現できるように実装した．以下に，NTMobile システムを構築する各装置の実現方法について述べる．

4.1 NTM 端末

図 5 に NTM 端末のモジュール構成を示す．NTM 端末にはユーザ空間で動作する NTM デーモンと，カーネルでパケット処理を行うカーネルモジュール，および仮想インタフェースを実装する．

NTM デーモンは Netfilter[⋆1] を利用して，DNS クエリの応答をフックする．クエリ応答を解析して A/AAAA レコードの結果を取得していたら，そのレコードを保持している DC へ NTMv4/v6 レコードの問合せを行う．その後，トンネル構築処理の終了時に，Netlink ソケットを通じてカーネルに実装されているトンネルテーブルにエントリを登録する．また，NTMobile デーモンは netlink ソケットを通じてカーネル空間から送信されるリンク情報およびアドレス情報の変化通知を受信することにより，L2 ハンドオーバおよび IP アドレスの変化を検出する．

通常のアプリケーションが送信する IP パケットの宛先は仮想 IP アドレスとなっているため，仮想インタフェースに向けてカーネルへ渡される．仮想インタフェースに渡される

⋆1 http://www.netfilter.org/

IP パケットは Netfilter によりパケット操作モジュールに渡され，カプセル化，暗号化などの処理が行われ後，実インタフェースから送信される．受信時は逆の手順により復号，デカプセル化された後，アプリケーションへデータが渡される．

一般にカプセル化を行うための仮想インタフェースとして，TUN/TAP デバイス[*1]があり，NTMobile でも TUN デバイスを採用する．この仮想インタフェースは OpenVPN をはじめとする多くの VPN ソフトウェアで採用されており，一般的には TUN/TAP デバイスに渡されたパケットデータを一度ユーザ空間へ戻してからカプセル化および暗号化を行い，再度ソケットを通じて送信することによりトンネル通信を実現している[13]．この手法では，カーネル空間とユーザ空間の間でメモリコピーが 2 回発生するため，スループットが低下するという課題がある．そこで，NTMobile では TUN デバイスに向けて渡されるパケットを Netfilter でフックすることにより，カプセル化処理をすべてカーネルモジュール内で完結するように設計した．これにより，冗長のない処理フローを実現できるため，カプセル化処理に伴うスループットの低下を抑制している[3]．

上記の仕組みを Linux PC に加えて，市販の Android スマートフォンである Samsung 社製 Galaxy S2（SC-02C）にも実装を行った．Galaxy S2 はメーカからカーネルのソースコードが公開されており，任意にカーネルの機能を有効にすることが可能である．NTM デーモンを ARM アーキテクチャ向けにクロスコンパイルし，ネイティブプログラムとして実装した．NTMobile を実装する際にカーネルのソースコードを変更する必要は一切ないが，パケットのフックや NTM デーモンとカーネルモジュール間でデータのやりとりを行ったり，トンネル通信の暗号化や認証を行うために，以下の機能を有効にしてカーネルを再構築した．

- Network packet filtering framework
- Netfilter NFQUEUE over NFNETLINK interface
- “NFQUEUE” target Support
- AES cipher algorithms
- MD5 digest algorithm
- CBC support
- Universal TUN/TAP device driver support

4.2 Direction Coordinator および Relay Server

図 **6**，図 **7** に DC と RS のモジュール構成を示す．DC と RS には，上述した NTM 端末のモジュールの一部を実装する．DC は NTM 端末のアドレス情報を動的に登録するために，Dynamic DNS サーバを稼働させる．この DNS サーバには NTMv4/NTMv6 レコードを扱えるよう，`bind`[*2]に機能を追加して実現している．NTM 端末および RS との制御メッセージ交換は NTM デーモンが行う．

RS は DC および NTM 端末との制御メッセージ交換を行う NTM デーモンに加えて，パケット処理を行うカーネルモジュールを実装する．RS はカプセル化/デカプセル化に加えて，アドレス変換機能を実装する．これは RS が NTM 端末と一般端末間の通信を中継する場合に用いる．なお，RS は受信したカプセル化パケットの転送処理が主な役割であるため，仮想インタフェースは実装しなくてもよい．

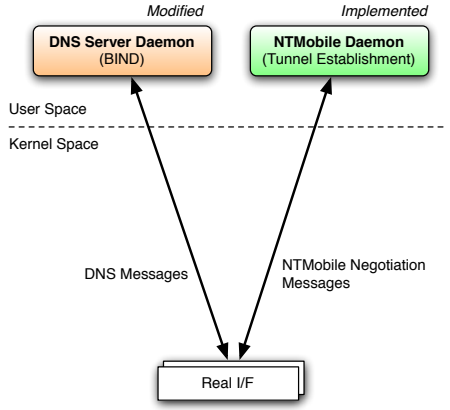


図 **6** モジュール構成（DC 側）
Fig. 6 Module configuration (DC).

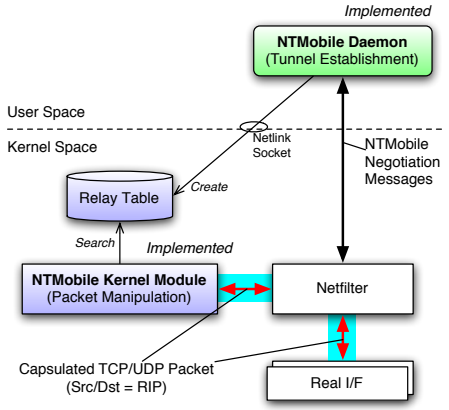


図 **7** モジュール構成（RS 側）
Fig. 7 Module configuration (RS).

*1 http://vtun.sourceforge.net/tun/
*2 http://www.isc.org/software/bind

5. 評　　価

5.1 通信接続性および移動透過性の検証

本稿では，NTMobile で実現する通信接続性と移動透過性の検証を行う．図 **8** に構築したシステム構成と動作検証の概要を示す．ネットワークの種類として，プライベート IPv4 ネットワーク，グローバル IPv4 ネットワーク，デュアルスタックネットワークおよび IPv6 ネットワークを構築した．各ネットワーク内に NTM 端末が Wi-Fi で接続できるよう，アクセスポイント（以後 AP）を設置した．AP は市販されている無線ブロードバンドルータで，ネットワークの構成に合わせてルータ機能や NAT 機能を設定した．RS および DC はデュアルスタックネットワーク上に設置し，仮想マシンとして動作させた．

今回は下記 4 つのケースを想定した通信および移動を行い，その動作確認を行った．MN と CN 間の通信に使用したアプリケーションは，`iperf` と `ping` で IPv4 アドレスで通信を行った．MN は各ネットワークの AP に手動で接続を切り替えることにより，異なるネットワークへの移動をエミュレートした．

Case 1：**IPv4** 環境における通信接続性の確認

グローバル IPv4 ネットワークに接続した MN から，プライベート IPv4 ネットワークに存在する CN へ通信を開始した．この場合，MN と CN 間は直接 UDP/IPv4 トンネルが構築され，NAT 越え通信ができることを確認した．

Case 2：**IPv4** 環境における移動透過性の確認

Case 1 の通信中に MN を CN とは異なるプライベート IPv4 ネットワークへ移動させた．移動を検知した MN は DHCP により新たなプライベート IPv4 アドレスを取得し，NTMobile によりトンネルの再構築を開始した．このケースでは異なるプライベート IPv4 ネットワーク間の通信となるため，RS を経由したトンネル経路となった．トンネル構築完了後，MN の通信は切断されずに継続できた，

また，RS 経由で通信を継続中に，経路最適化処理を行ったところ，今回用いた NAT は Cone 型 NAT であったため MN と CN 間で直接制御メッセージを交換でき，トンネル経路が RS からエンドエンドに切り替わった．その際にも，通信の切断は発生せず，移動透過性を実現できることを確認した．

Case 3：**IPv4/IPv6** 混在環境における移動透過性の確認

Case 2 で通信を継続中に，MN をデュアルスタックネットワークへ移動させた．ここでは MN は DHCP により新たなグローバル IPv4 アドレスを取得すると共に，IPv6 ルータから Router Advertisement を受信して IPv6 アドレスを自動生成する．CN とは IPv4 で通信していたため，アドレスの取得が完了すると UDP/IPv4 トンネルを再構築する．MN はグローバル IPv4 アドレスを取得したため，MN と CN 間は再び直接トンネルが構築され，通信も継続して行われることを確認した．

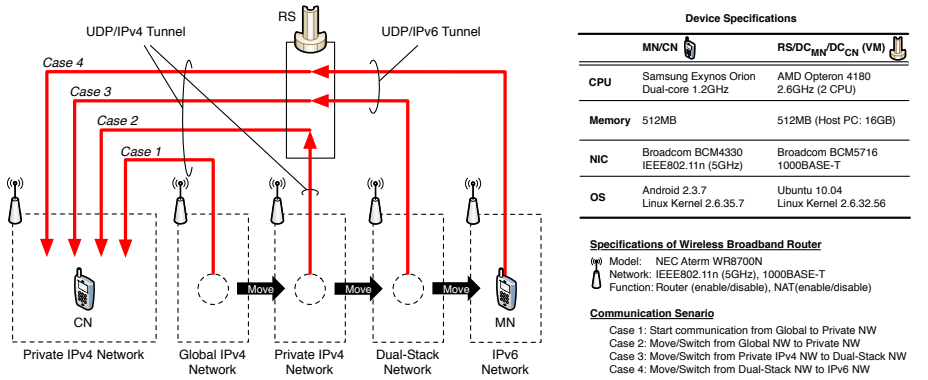


図 **8**　システム構成と動作検証の概要

Fig. 8　System configuration and overview of operation verification.

Case 4：**IPv4/IPv6** 環境をまたがった通信接続性と移動透過性の確認

Case 3 で UDP/IPv4 トンネルによる通信を継続中に，MN を IPv6 ネットワークへ移動させた．この場合，MN と CN は異なるプロトコル体系のネットワークに存在するため，MN から RS に対しては UDP/IPv6 トンネルが，CN から RS に対しては UDP/IPv4 トンネルが再構築された．トンネル再構築後，MN は IPv6 ネットワーク上で IPv4 アプリケーションによる通信の継続が可能であることを確認した．

上記の通り，様々なアドレス空間・アドレス体系が混在した複雑なネットワークであっても，ユーザはネットワークの違いを意識することなく通信を開始することができ，かつ通信中に移動しても継続できることを，市販の実機で実証した．なお，今回の動作検証ではアプリケーションが IPv4 通信を行った場合であったが，NTMobile の原理上，IPv6 アプリケーションでも同様に動作する．また，NTMobile の性能評価については，文献 14)，15) にて行っており，実用上問題ないことが示されている．以上の結果より，NTMobile は高い有用性と実用性を兼ね備えていることを確認できた．

5.2 NTMobile の応用例

NTMobil は様々なネットワークから NAT 配下の端末に対して通信を開始することができる．そのため，ホームネットワーク内の情報家電機器などに遠隔接続する利用方法が考えられる．文献 16) では NTMobile の一部機能を拡張することにより，外出先から家庭の DLNA（Digital Living Network Alliance）準拠の機器に蓄積されたコンテンツを再生するシステムを提案している．ホームネットワーク内に DA（DLNA Agent）と呼ぶ RS に DLNA 通信に必要な機能を実装した装置を設置する．外出先の NTM 端末は DA を中継することにより，NTMobile の機能を持たない一般の情報家電への遠隔接続が可能で，かつコンテンツ再生中に NTM 端末は移動しても通信を継続することを確認している．

近年は音楽・動画のストリーミング配信サービスやクラウドを利用したサービスが展開されている．以前は携帯端末にコンテンツを移動あるいはコピーして持ち運ぶスタイルが主流であったが，高速無線通信技術の発達により，コンテンツはネットワーク上のどこかにあり，それらにアクセスするスタイルに変化してきた．スマートフォンはクラウドサービスとの連携が非常に密接かつ簡単であり，多くのユーザは 3G などのキャリア回線を利用している．NTMobile を導入することにより，スマートフォンでコンテンツを再生中に移動したり，キャリア回線から Wi-Fi など異なる無線通信ネットワークへハンドオーバしても通信を継続することができる．また，キャリア回線で発生する膨大なマルチメディアトラフィックを，インターネットへオフロードすることにもつ繋がる．

NTMobile により，さらに柔軟なサービスの利用方法が期待できるが，NTMobile を実装しない一般端末でも同等の恩恵を受けられると非常に有用である．上記遠隔 DLNA 通信システムの DA に着目すると，NTMobile の機能を有する装置を中継することにより，一般端末に対しても通信接続性と移動透過性を提供している．これを DLNA 通信だけでなく，一般の通信にも拡大して適用することが考えられる，例えば，モバイルルータのような小型携帯通信機器に NTMobile を組み込み，無線 LAN のアクセスポイントとして動作させる．モバイルルータは接続した配下の機器の代理で NTMobile に関わる処理を行うことができれば，カーネルへの機能追加が困難な携帯機器（例えば iPhone やポータブルゲーム機など）に対して，間接的に NTMobile の機能を提供することができる．

6. ま と め

本稿では，今後のインターネットで想定される IPv4/IPv6 混在環境において，通信接続性と移動透過性を同時に実現する NTMobile アーキテクチャの全貌を述べた．NTMobile は実ネットワークとは独立した仮想 IP アドレスを用いてコネクションを確立し，このパケットを実 IP アドレスでカプセル化してトンネル通信を行う．これにより，様々なアドレス空間・アドレス体系が混在したネットワーク上で確実な通信接続性を実現することができる．また，仮想 IP アドレスにより実 IP アドレスの変化を隠蔽しているため，移動後にトンネルの再構築をおこなうことにより，IPv4 ネットワークにおける NAT や，IPv4/IPv6 ネットワーク間をまたがった移動透過性を実現できる．

NTMobile を Android スマートフォンへ実装し，実環境において動作検証を行った．その結果，プライベート IPv4 ネットワーク，グローバル IPv4 ネットワーク，IPv6 ネットワーク間で自由な双方向通信を実現できることを確認した．また，それらのネットワーク間でハンドオーバしても通信を継続できることを確認した．

参 考 文 献

1) Le, D., Fu, X. and Hogrefe, D.: A Review of Mobility Support Paradigms for the Internet, *IEEE Communications Surveys & Tutorials*, Vol.8, No.1, pp.38–51 (2006).
2) 鈴木秀和，水谷智大，西尾拓也，内藤克浩，渡邊　晃：NTMobile における移動透過性の実現と実装，DICOMO2011 論文集，Vol.2011, pp.1339–1348 (2011).
3) 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，DICOMO2011 論文集，Vol.2011, pp.1349–1359 (2011).
4) Soliman, H.: Mobile IPv6 Support for Dual Stack Hosts and Routers, RFC 5555, IETF (2009).
5) Levkowetz, H. and Vaarala, S.: Mobile IP Traversal of Network Address Translation (NAT) Devices, RFC 3519, IETF (2003).
6) Moskowitz, R. and Nikander, P.: Host Identity Protocol (HIP) Architecture, RFC 4423, IETF (2006).
7) Rosenberg, J.: Interactive Connectivity Establishment (ICE): A Protocol for Network Address Translator (NAT) Traversal for Offer/Answer Protocols, RFC 5245, IETF (2010).
8) Komu, M., Henderson, T., Tschofenig, H., Melen, J. and Keranen, A.: Basic Host Identity Protocol (HIP) Extensions for Traversal of Network Address Translators, RFC 5770, IETF (2010).
9) Maenpaa, J., Andersson, V., Camarillo, G. and Keranen, A.: Impact of Network Address Translator Traversal on Delays in Peer-to-Peer Session Initiation Protocol, *Proc. of IEEE GLOBECOM2010* (2010).
10) Bonola, M., Salsano, S. and Polidoro, A.: UPMT: Universal Per-Application Mo-

bility Management Using Tunnels, *Proc. of IEEE GLOBECOM2009* (2009).
11) Bonola, M. and Salsano, S.: S-UPMT: a secure Vertical Handover solution based on IP in UDP tunneling and IPsec, *GTTI Riunione Annuale 2010* (2010).
12) 納堂博史，鈴木秀和，内藤克浩，渡邊　晃：NTMobile の経路最適化の検討，研究報告モバイルコンピューティングとユビキタス通信，Vol.2012-MBL-61, No.33, 情報処理学会，pp.1–8 (2012).
13) Khanvilkar, S. and Khokhar, A.: Virtual Private Networks: An Overview with Performance Evaluation, *IEEE Communications Magazine*, Vol.42, No.10, pp.146–154 (2004).
14) 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，研究報告モバイルコンピューティングとユビキタス通信，Vol.2012-MBL-62, No.19, 情報処理学会，pp.1–8 (2012).
15) 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，DICOMO2011 論文集，情報処理学会，pp.1–11 (2012).
16) 清水皓平，鈴木秀和，内藤克浩，渡邊　晃：移動透過性に対応した遠隔 DLNA 通信システム，研究報告コンシューマ・デバイス＆システム，Vol.2012-CDS-4, No.12, 情報処理学会，pp.1–8 (2012).