平成24年度　修士論文

邦文題目

NTMobileにおける名前解決方式の提案と評価

英文題目

Proposal of Name Resolution Method in NTMobile and its Evaluation

情報工学専攻

(学籍番号: 083430033)

細尾　幸宏

提出日: 平成25年1月31日

名城大学大学院理工学研究科

内容要旨

端末が接続するネットワーク環境にかかわらず通信開始を保証する通信接続性や，移動してネットワークが切り替わっても通信が継続できる移動透過性への需要が高まっている．我々は，IPv4/IPv6 ネットワークが混在する環境においてアドレス空間やアドレス体系に依存しない通信接続性と移動透過性を実現する NTMobile(Network Traversal with Mobility）を提案している．現状の NTMobile では端末情報の収集と管理を既存の DNS に依存する方法をとっており，通信開始時の情報収集における確実性や情報管理の柔軟性に欠けるという課題があった．そこで本論文では，情報管理を DNS の仕組みに依存する方法からデータベースを利用する方法へ移行し，DNS 依存によって発生する通信接続性における課題を解決する名前解決手法を提案する．また，提案手法の実装を行い，動作検証および評価を行った．この結果，提案方式ではデータベースによる端末情報管理により端末情報の秘匿性と拡張性および端末情報管理の柔軟性を確保した．また，通信開始において通信接続性を確保できない課題を解決し，実ネットワーク環境における従来方式の実測値を元にした提案方式の性能予測によって通信開始時のオーバヘッドを削減可能であることを確認した．

目 次

第1章　はじめに

スマートフォンなどの高性能な携帯端末の普及に伴い，ユーザがインターネットを利用する形態が大きく変化している．現在の状況は通信インフラとして広く普及している TCP/IP の当初の想定を超えており，様々な課題が明確になっている．最大の課題は IPv4 グローバルアドレスの枯渇である．IPv4 グローバルアドレス枯渇問題に対する短期的な対策として，NAT を設置する方法が一般的に行われているが，この対策によってグローバルアドレス側からプライベートアドレス側に対して通信を開始できない NAT 越え問題が発生しおり，IPv4 ネットワークの大きな課題となっている．

この課題に対する長期的な対策として，IPv6 [1] が定義されているが，現在利用されている IPv4 との間には互換性が無く，直接通信ができないため IPv6 の普及は進んでいない．このため，長期間 IPv4 と IPv6 が混在する環境になることが想定され，この環境における通信接続性を保証することは極めて重要である．

また，IP ネットワークには，通信端末が通信中に移動等によって端末が接続するネットワークや使用するインタフェースの切り替えを行うと IP アドレスが変化し，通信を継続できないという課題がある．このような問題を解決する技術は移動透過性技術と呼ばれ，現在までに様々な移動透過性技術が提案されてきた [2]．しかし，これらの多くは IPv6 が今後の主流になることを想定した IPv6 のみに対応した方式であり，NAT 越え問題が存在する IPv4 における移動透過性技術は少ない．

これらの課題を解決するため，IPv4/IPv6 ネットワークが混在する環境において通信接続性の確保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 [3–6]．NTMobile はトンネル通信と仮想 IP アドレスを用いた技術である．トンネル通信とアドレス変換により NAT 配下の NTMobile 対応端末（NTM 端末）に対する接続性を確保でき，IPv4 と IPv6 ネットワーク間の接続性を確保することができる．また，アプリケーションが仮想 IP アドレスを認識することで通信中にどのようなネットワークへ接続を切り替えても通信を継続できる．これらの手法により，実ネットワークの違いや実 IP アドレスの変化のような IP ネットワーク特有の制約を隠蔽し，NTMobile が提供する制約のない仮想的なネットワークに全てのアプリケーションを接続する技術である．

NTMobile では，通信トンネルの構築に必要な通信相手の NTM 端末情報を，通信開始側の NTM 端末が収集する必要がある．NTMobile はインターネットで世界的に分散管理されている既存の DNS（Domain Name System）[7, 8] の仕組みを利用することで NTM 端末情報を収集する手法をとっている．管理装置 DC（Direction Coordinator）が DDNS（Dynamic

DNS）[9] の機能を包含し，DNS レコードの形式の NTMobile 専用レコード（NTM レコード）として NTM 端末情報を DDNS に登録している．DNS レコード形式で扱うことにより，各 NTM 端末に割り当てる FQDN（Fully Qualified Domain Name）を問い合わせることで NTM 端末が接続しているネットワークのプライマリ DNS サーバを経由して NTM レコードを取得することができる．通信開始側の NTM 端末は通信相手の FQDN から端末情報を収集し，トンネル構築を行う．

しかし，既存の DNS の仕組みを利用することで，いくつかの課題が発生している．すなわち，DNS はインターネットにおける情報共有のためのシステムであり，DNS レコードと同様の形式で扱っている NTM レコードも通常の DNS レコードと同じく公開された情報として扱わざるを得ず，FQDN から誰でも NTM 端末情報を取得することが可能である．また，近年の携帯端末のように急激に進化するネットワークの利用形態に対して柔軟に対応するネットワークアーキテクチャとして，DNS レコード形式に従った現在の NTM 端末情報管理は拡張性に乏しいという課題がある．さらに，通信接続性を確保するためには NTM レコードを動的に更新し，全てのノードが最新の NTM レコードを取得可能状態を維持する必要がある．このため，DNS によるネットワークトラフィック削減などのために導入されている DNS キャッシュは利用できず，NTM 端末が通信を開始する際には毎回 DNS 探索をルートサーバから行う必要がある．これに関連した課題として，DNS サーバの設定やバージョン等により DNS キャッシュが NTM レコードの TTL 設定通りに適用されず，DNS サーバにキャッシュが残ってしまう場合がある．この場合，この DNS サーバを経由して DNS 探索を行う NTM 端末は，移動を行った NTM 端末に対してキャッシュが残っている期間は通信を開始することができないという課題が発生する．さらに，NTMobile が IPv4 と IPv6 の両ネットワークをサポートする上で必要な通信開始時の DNS 問い合わせは A, AAAA, NTM4, NTM6 レコード[1]の計 4 回であり，通信遅延が大きいネットワークに接続している場合に通信開始時のオーバヘッドが大きくなるという課題がある．

本論文では，NTMobile が DNS の仕組みに依存することで抱えている通信接続性の確保と通信開始時のオーバヘッドを低減する手法および NTM 端末情報の管理における秘匿性と柔軟性を確保する手法を提案する．具体的には，通信開始側の NTM 端末が行っていた合計 4 回の DNS 問い合わせを廃止し，管理装置 DC が NTM 端末情報の収集を行う．また，DNS キャッシュの影響を回避するため NTM 端末情報は DC 同士が新たに定義する独自の制御メッセージを用いて共有する．NTM 端末情報は DNS レコード形式からデータベースで管理する手法に変更する．これにより，NTMobile の問い合わせにのみ情報を提供する秘匿性と，今後の拡張等の柔軟性を確保する．また，提案方式を Linux に実装し，動作確認を行った．この結果，提案方式ではデータベースによる端末情報管理により端末情報の秘匿性と拡張性および端末情報管理の柔軟性を確保した．また，通信開始において通信接続性を確保できない課題を解決し，実ネットワーク環境における従来方式の実測値を元にした提案方式の

[1]NTM4 は IPv4 用の NTM レコード，NTM6 は IPv6 用の NTM レコードである．

性能予測によって通信開始時のオーバヘッドを大幅に削減可能であることを確認した．

以下，2 章で NTMobile について説明し，3 章で NTMobile における名前解決手法の課題について述べる．4 章で提案方式について説明し，5 章で提案方式の評価を行い，6 章で提案方式の今後の展開について述べ，7 章でまとめる．

第2章　NTMobile

2.1　NTMobile の概要

NTMobile の概要を図 2.1 に示す．NTMobile は NTM 端末，管理装置 DC（Direction Co-ordinator），中継装置 RS（Relay Server）によって構成される．DC や RS はグローバルネットワークに設置し，ネットワークの規模に応じて複数台設置による負荷分散を行うことができる．

NTM 端末と DC および RS，DC 同士，DC と RS 間にはそれぞれ事前に信頼関係があることが前提である．信頼関係を確認後，DC は NTM 端末に対して FQDN，Node ID，仮想 IP アドレスを配布する．NTMobile で使用される制御メッセージは各端末間で共有している暗号鍵を用いて暗号化される．

DC は DDNS（Dynamic DNS）[9] の機能を包含しており，NTM 端末の A レコードと AAAA レコードに加え NTM レコードを登録している．これらのレコード情報は通信接続性の確保

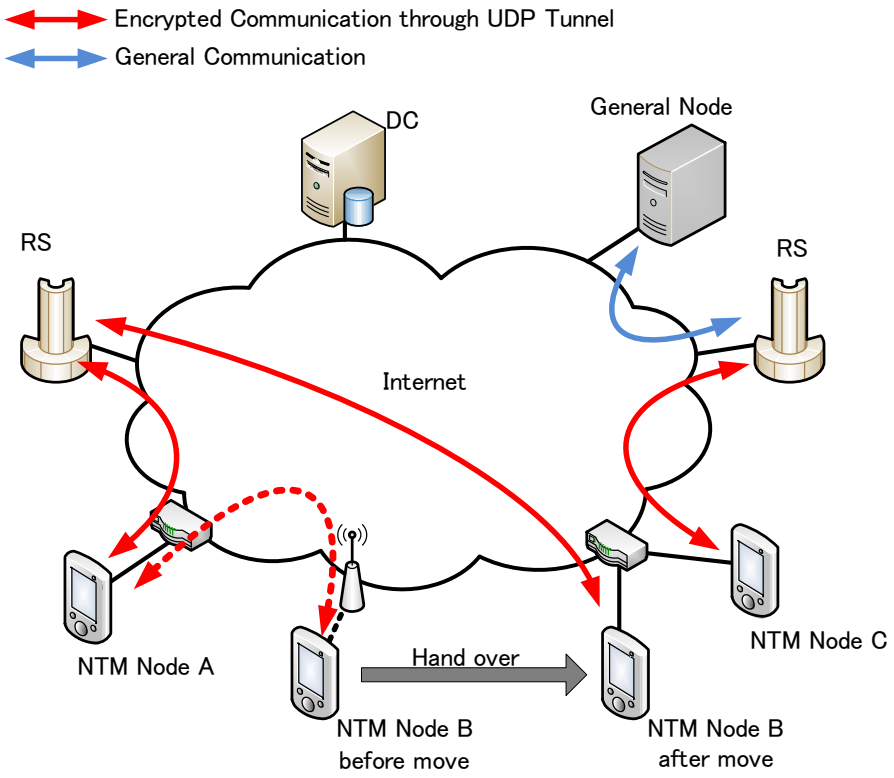

図 2.1　NTMobile の概要

のために最新の状態を保つよう動的に更新を行う．DC は DNS サーバとして管理するドメインを元に NTM 端末に一意な FQDN を割り当てる．この FQDN と各レコード情報を関連付けて管理することにより，FQDN から DNS 問い合わせを利用して NTM 端末情報への到達性を確保している．これにより，分散管理された異なる DC に所属する NTM 端末同士は FQDN を元に互いの NTM 端末情報を共有でき，通信接続性の確保に利用している．NTM レコードには NTM 端末を一意に識別する Node ID，実 IP アドレス，仮想 IP アドレス，NAT の外側の実 IP アドレス，アドレス情報を管理している DC の実 IP アドレスが記載されている．また，NTM 端末の通信開始要求を受けて通信トンネル構築時に適切なトンネル経路を判断し，指示を行う役割を担っている．DC が各 NTM 端末に割り当てる仮想 IP アドレスは一意なアドレスであり，各 DC は自身に割り当てられたアドレス空間から重複が起きないように割り当てを行う [10].

NTM 端末は実ネットワークから割り当てられる実 IP アドレスと，DC から割り当てられる仮想 IP アドレスの 2 種類の IP アドレスを保持する．NTM 端末上で動作するアプリケーションは仮想 IP アドレスに基づいた通信を行う．仮想 IP アドレスに基づくパケットは，NTM 端末間に構築される UDP トンネルによって転送される．トンネルの経路は通信を行う NTM 端末のどちらか一方がグローバルネットワークに接続している場合には必ずエンドツーエンドのトンネル通信を行うことができる [11].

RS は通信を行う NTM 端末が互いに異なる NAT 配下に接続している場合や NTMobile 未実装の一般端末と通信を行う場合，さらには一方のノードが IPv4，もう一方のノードが IPv6 ネットワークに接続している場合，通信の中継を行う装置である．ただし，NTM 端末同士が互いに異なる NAT 配下に接続していても NAT の種類によっては経路最適化によりエンドツーエンドのトンネル通信に切り替えることが可能である．

2.2 通信シーケンス

以後の説明では，通信開始側の NTM 端末を MN（Mobile Node），通信相手側の NTM 端末を CN（Correspondent Node）として説明する．また，端末 N の FQDN を $FQDN_N$，Node ID を NID_N，実 IPv4 アドレスを $RIP4_N$，仮想 IPv4 アドレスを $VIP4_N$，端末 N が NAT 配下に接続している場合の NAT の実 IPv4 アドレスを $RIP4_{NAT_N}$ とし，アドレス情報を管理している DC を DC_N，その実 IPv4 アドレスを $RIP4_{DC_N}$ とする．NTM レコードは IPv4 用の NTM4 レコードと IPv6 用の NTM6 レコードの 2 つが定義されている．端末 N の NTM4 レコードには，NID_N，$RIP4_N$，$VIP4_N$，$RIP4_{NAT_N}$，$RIP4_{DC_N}$ が含まれ，NTM6 レコードにはそれぞれの IPv6 アドレスが含まれる．N1 と N2 がトンネル通信時に用いる Path ID を PID_{N1-N2} と表す．Path ID は NTM 端末間の通信を一意に識別するための識別子である．

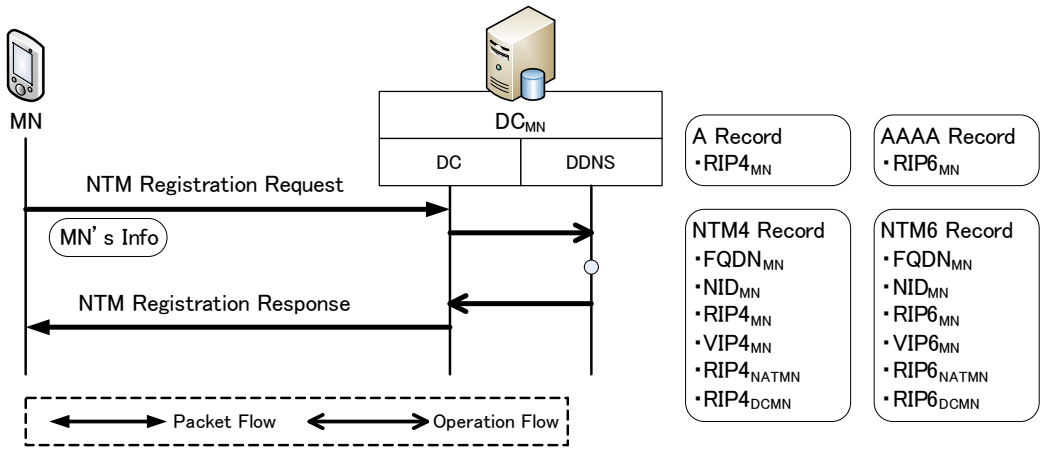

図 2.2　NTMobile 登録処理

2.2.1　登録処理

図 2.2 に NTMobile の端末情報登録処理を示す．NTM 端末は通信接続性の確保のために, 端末起動時に DC に対して実 IP アドレスなどの端末情報を登録する．MN は $FQDN_{MN}$, NID_{MN}, $RIP4_{MN}$，$RIP6_{MN}$ などを記載した NTM Registration Request を DC_{MN} に送信する．DC_{MN} は NTM Registration Request を受信すると，DNS サーバに登録されている NTM4, NTM6 レコードを更新する．このとき，NTM Registration Request の IP ヘッダに格納されている送信元 IP アドレスが，メッセージ内の RIP と異なる場合，MN がプライベートアドレス空間にいると判断し，IP ヘッダの送信元 IP アドレスを NAT の外側の IP アドレスとして NTM レコードを更新する．その後，MN へ応答として NTM Registration Response を返す．

登録完了後は MN と DC_{MN} は定期的にメッセージの交換をすることで制御メッセージ用の通信経路を確保する（Keep Alive）．これにより，DC_{MN} は NAT 配下にいる MN との制御メッセージ用経路を維持する．

2.2.2　名前解決処理

NTMobile は，DNS による名前解決をトリガとして NTMobile 特有のネゴシエーションを実行する．MN は DNS による名前解決処理を検出すると，そこに含まれる $FQDN_{CN}$ を元に A, AAAA, NTM4, NTM6 レコードの問い合わせを行う．A, AAAA レコードにより CN の実 IP アドレスを取得する．NTM4 レコードは IPv4 で，NTM6 レコードは IPv6 で NTMobile の通信トンネル構築を行うために収集する必要がある．これらの問い合わせは接続しているネットワークのプライマリ DNS サーバを経由して DC に到達し，各レコードを取得することができる．DNS サーバからの応答は一時的に待避し，取得した情報を元に 2.2.3 項で説明するトンネル構築処理を行う．

トンネル構築後, MN は待避していた DNS サーバからの応答に含まれる $RIP4_{CN}$ を $VIP4_{CN}$

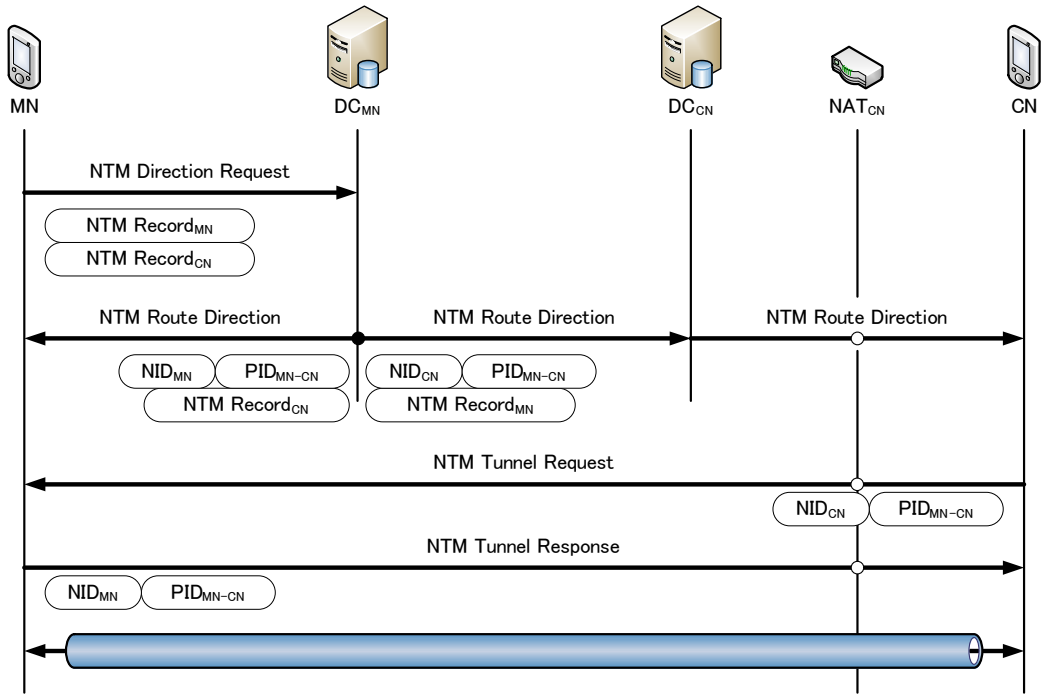

図 2.3　NTM 端末間のトンネル構築手順

に書き換えて DNS リゾルバへ渡す．これにより，MN のアプリケーションは通信相手の IP アドレスとして $VIP4_{CN}$ を認識することになる．

2.2.3　トンネル構築

図 2.3 にトンネル構築シーケンスを示す．NTM 端末は名前解決による情報収集完了後，DC にトンネル構築の指示を要求する．MN は 2.2.2 項で収集した CN の端末情報と自身の端末情報を DC_{MN} へ NTM Direction Request として送信する．DC_{MN} はメッセージ内の両端末の情報から最適なトンネル経路を判断する．DC_{MN} は経路判断を元にトンネル構築に必要な情報を載せた NTM Route Direction を MN と CN へ送信する．NTM 端末が NAT 配下にいる場合，NTM Tunnel Request を NAT 配下の NTM 端末が送信することによってトンネル通信の経路を確保する．

2.2.4　トンネル通信

アプリケーションは通信相手として仮想 IP アドレスを認識しているため，アプリケーションが生成したパケットは仮想 IP アドレスが記載される．これをカプセル化し，CN へ転送する．CN はカプセル化されたパケットをデカプセル化し，抽出したアプリケーションパケットを上位アプリケーションへ渡す．

2.2.5　ハンドオーバ時の動作

NTMobile では，通信中に NTM 端末がネットワークを切り替えた場合，通信開始時と同じトンネル構築処理を行うことによりトンネルの再構築を行う．このとき，MN は通信開始時に CN のレコード情報は取得済みであるため，2.2.2 項の名前解決処理は省略される．MN はこれと並行して 2.2.1 項で説明した登録処理を行い，DC に登録されている NTM レコードを最新の情報に更新する．

第3章　NTMobileにおける名前解決手法の課題

本章では，DNS の仕組みについて概説し，NTMobile における DNS 利用の状況についてまとめ，その課題について述べる．

3.1　DNS（Domain Name System）

DNS とはインターネット上のホスト名と対応する IP アドレスを管理し，相互に変換するシステムである．ドメイン名による階層構造を用いて世界中に分散管理された世界最大規模の分散型データベースであり，その管理情報は全世界に等しく提供するオープンなシステムである．

ホスト名”cn.example.ne.jp” を解決する DNS の動作シーケンス例を図 3.1 に示す．名前解決時にルートサーバから順に問い合わせをしてホストの管理サーバを特定して IP アドレスを取得する．

図 3.1 のように名前解決をする度にルートネームサーバから問い合わせを行うとサーバリソースやネットワークトラフィックに負荷がかかるため，探索結果を一定時間保持するキャッシュおよびネガティブキャッシュ [12] が定義されている．これにより，プライマリ DNS サーバはキャッシュを保持している名前解決については探索を行わず，直ちに MN へ回答を行う動作が一般的である．

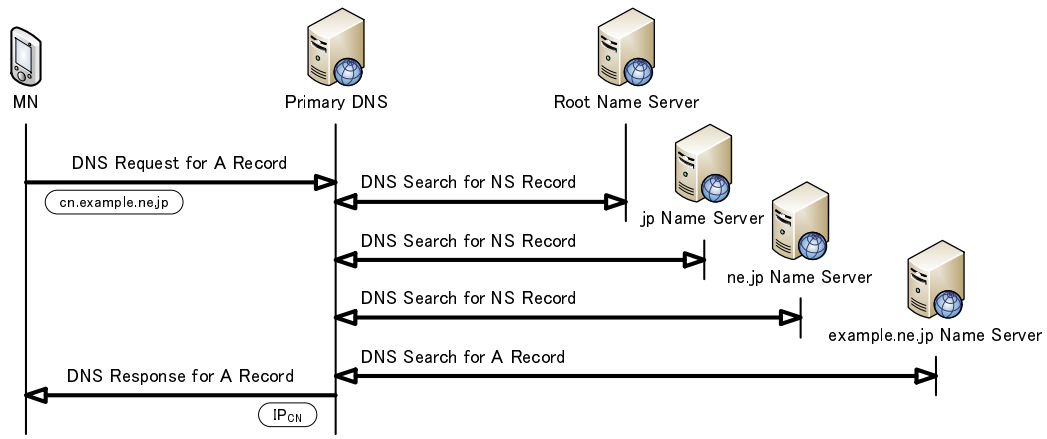

図 3.1　DNS の動作シーケンス

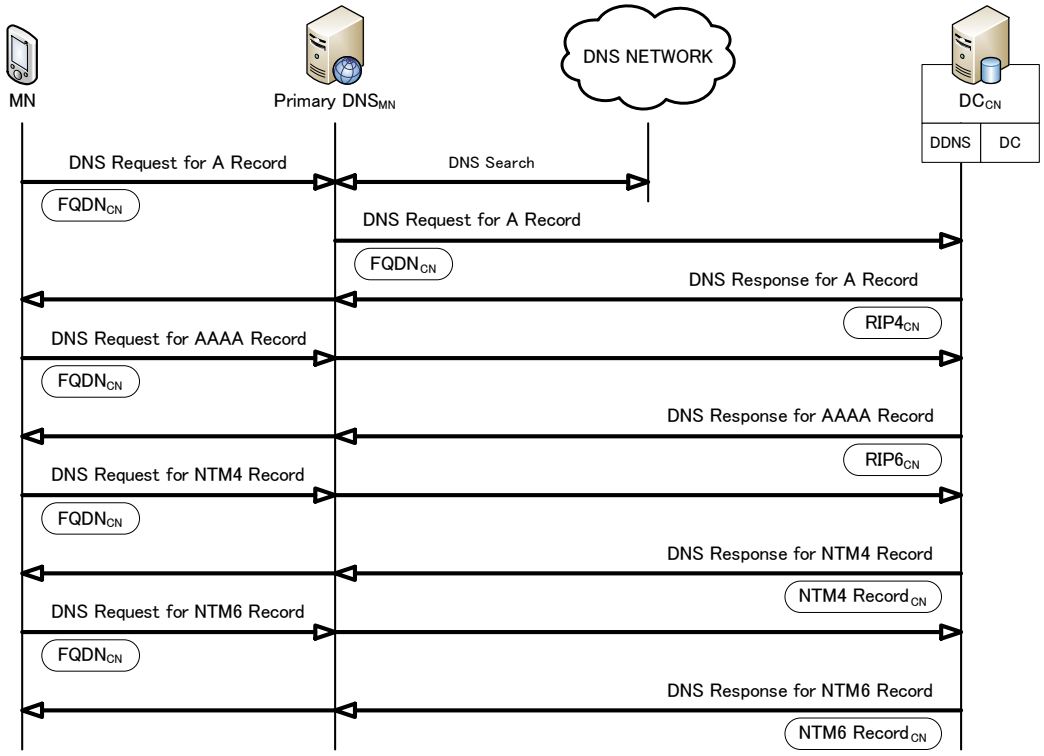

図 3.2　DNS による名前解決処理

3.2　DNS を用いた NTMobile の名前解決処理

NTMobile において通信トンネル構築に必要な NTM 端末情報の収集は DNS の名前解決処理そのものである．DC は自身に包含する DDNS に NTM レコードとして NTM 端末情報を登録している．これにより，DDNS の動作に従って FQDN を元に行われる DNS 問い合わせに対して NTM レコードを応答する．DNS の仕組みを利用している限り，NTM レコードの応答を特定の相手に限定することはできない．また，DNS における DNS レコードの管理はテキストファイルにレコードごとに列挙する方法が基本であり，データをリレーショナルに扱うなどの複雑な処理はできない．また，DC が管理する NTM レコードは DNS キャッシュの対象にならないよう，TTL（Time To Live）を小さく設定する．

通信開始時の NTMobile における名前解決処理を図 3.2 に示す．MN はアプリケーションが行う DNS 問い合わせを検出すると，そこに含まれる $FQDN_{CN}$ を元に A, AAAA, NTM4, NTM6 レコードの 4 種類の DNS レコードすべてを問い合わせる必要がある．DC_{MN} が最適なトンネル経路を判断するために，MN は CN に関する全てのレコードを問い合わせる．また，NTM レコードが取得できない場合は CN が一般端末であると判断する．この名前解決処理は MN が接続しているネットワークのプライマリ DNS を利用して行う．この DNS 問い合わせがグローバルネットワークの DNS サーバに対して名前解決が可能であれば，NTMobile による接続性が確保されていると言える．

3.3 DNS を用いた情報管理および情報収集の課題

DNS の仕組みに依存した NTMobile の名前解決処理は，DNS の特性により以下のような課題が発生している．これらの課題を DNS の仕組みを利用することによるスケーラビリティのような利点を残しながら解決する手法が必要である．

課題 1 DC 管理の柔軟性と拡張性

NTMobile ではあらゆるネットワーク環境において通信の接続性を確保するために NTM 端末情報を管理する必要がある．また，携帯端末は急激な進化を遂げており，その進化に対して柔軟に対応可能なシステムである必要がある．しかし，現時点では NTM 端末情報は DNS レコードとしてテキストファイル形式による画一的なデータ形式となっている．IP レベルのネットワークアーキテクチャとして近年のスマートフォンによる急激なネットワーク利用形態の変化や新たなサービスなどに柔軟に対応し，NTM 端末情報を拡張できるシステムであることが望ましい．

課題 2 NTM 端末情報の秘匿性

DNS レコードを用いた情報管理では DNS 問い合わせによって NTM 端末情報が公開されている状態となっている．すなわち，誰でも FQDN を用いて NTMobile のために追加で DDNS へ登録している NTM レコードを取得することが可能である．これにより，NTM レコードに含まれる情報に対してセキュリティを確保することができず，NTMobile のシステム拡張性が制限される．

課題 3 通信開始時の確実性

NTM 端末が DNS による問い合わせを受けると，DNS サーバにキャッシュが残る場合がある．この場合，キャッシュが残っている期間は NTM 端末が移動していても移動する前の情報しか得ることができず，通信の接続性を確保することができない．このため，DNS レコードの TTL を短く設定する必要があるが，キャッシュを利用できず毎回 DNS 問い合わせによる探索を必要とする．DNS を利用した NTMobile の名前解決処理には必ず一般の DNS サーバが介在することになる．NTM レコードは DNS キャッシュの対象にならないよう設定していても，一部の DNS サーバのバージョンや設定によっては強制的に NTM レコードがキャッシュされるなどの問題が発生する場合がある．このため，確実な通信接続性を確保するにはこのような課題に対応する必要がある．

課題 4 通信開始のオーバヘッド

NTMobile は通信開始時に NTM 端末が通信相手の FQDN から通信相手の A, AAAA, NTM4, NTM6 レコードを合計 4 回の DNS 問い合わせで収集する必要がある．NTM 端末が携帯端末等であることを想定すると，通信遅延の大きい 3G 回線を使用している可能性が高く，接続開始時のオーバヘッドが大きくなる．

第4章　提案方式

4.1　提案方式の方針

3.3 項で示した課題を回避するため，NTM 端末から行っていた複数の DNS 問い合わせを DC_{MN} に依頼する方法に変更する．DNS レコードの 1 つである NS レコードを問い合わせることで，指定したドメインの情報を管理する DNS サーバのホスト名や IP アドレスを取得することができる．これを利用し，DC_{MN} は NS レコードを用いて DC_{CN} を発見する．そして，CN の端末情報は DC_{CN} から DNS の仕組みを使わず収集する．このために DC_{MN} と DC_{CN} 間で独自の制御メッセージを定義し，直接端末情報を取得する．DC はグローバルネットワーク上に有線接続で設置するため，NS レコードの問い合わせは比較的高速に行うことができる．また，DNS レコードの 1 つである TXT レコードには任意の文字列を指定可能であり，NTMobile の DC であることを示す文字列を DC の TXT レコードに登録することで DC と一般 DNS サーバの判別に利用する．この方法により，NTM 端末情報を DNS 問い合わせによって取得する必要がなくなるため，NTM 端末情報を DNS レコードではなくデータベースとして DC に保持させる．

4.2　データベースによる情報管理

図 4.1 にデータベースの構成を示す．DC のデータベースでは 2 種類のテーブルで情報を管理する．Node Information テーブルには DC に登録を行っている NTM 端末の端末情報を記録し，NTMobile における経路判断およびトンネル構築に利用する．DC キャッシュは DC

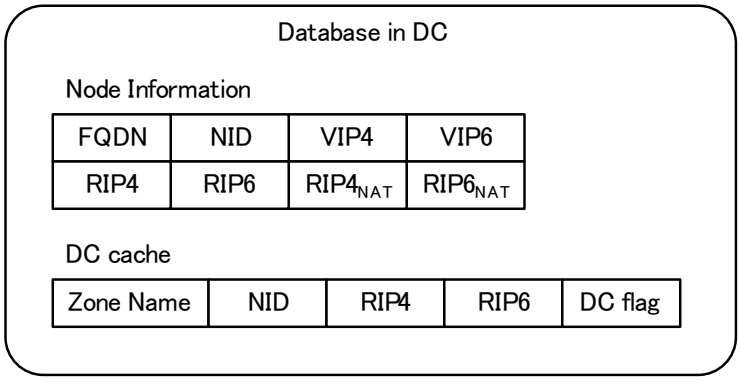

図 4.1　データベースの構成

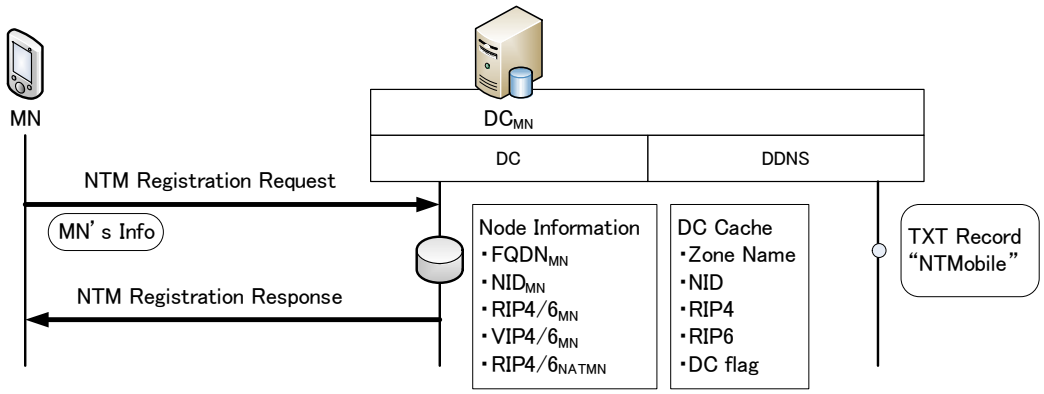

図 4.2　提案方式の端末情報登録

および DNS サーバの情報を一時的に保持するテーブルであり，DC が新たに管理する情報である．DC キャッシュは NS レコードと TXT レコードの問い合わせ結果から判断して登録し，今後同一ドメインの FQDN に対して通信を開始する際に参照する．Zone Name は DC および DNS サーバのドメイン名であり，管理しているゾーン名を指す．DC flag は DNS サーバが NTMobile の DC として対応しているかどうかを示す情報である．DC キャッシュの情報はキャッシュのように扱う．この情報を管理することにより，NTM 端末が通信を開始する際，通信相手の FQDN のドメインが DC キャッシュに存在するかを確認し，情報があれば NS レコードや TXT レコードを問い合わせる必要がなくなる．

また，DC は DNS レコードの 1 つである TXT レコードに NTMobile の DC であることを示す文字列を含んで登録しておく．これは，4.3.1 節においてこの DNS サーバが DC であるか一般の DNS サーバであるかを判断するために使用する．

DC における端末情報の登録，管理を図 4.2 に示す．従来方式で DDNS に登録されていた NTM レコードの情報は DC が管理するデータベースへ移行し，DDNS では NTM 端末情報を管理する必要はない．代わりに，DDNS には TXT レコードを新たに登録する．また，NS レコードは DNS サーバとして運用する上で必須の DNS レコードであり，その登録は従来と同様である．

4.3　提案シーケンス

提案シーケンスを図 4.3 に示す．MN, CN の DC に対する登録処理および Keep Alive による制御メッセージの経路確保は従来と同様である．登録処理を受け取った DC はその情報を Node Information テーブルに登録しておく．DC は NTM Registration Request によって受け取った端末情報を Node Information テーブルに登録しておく．

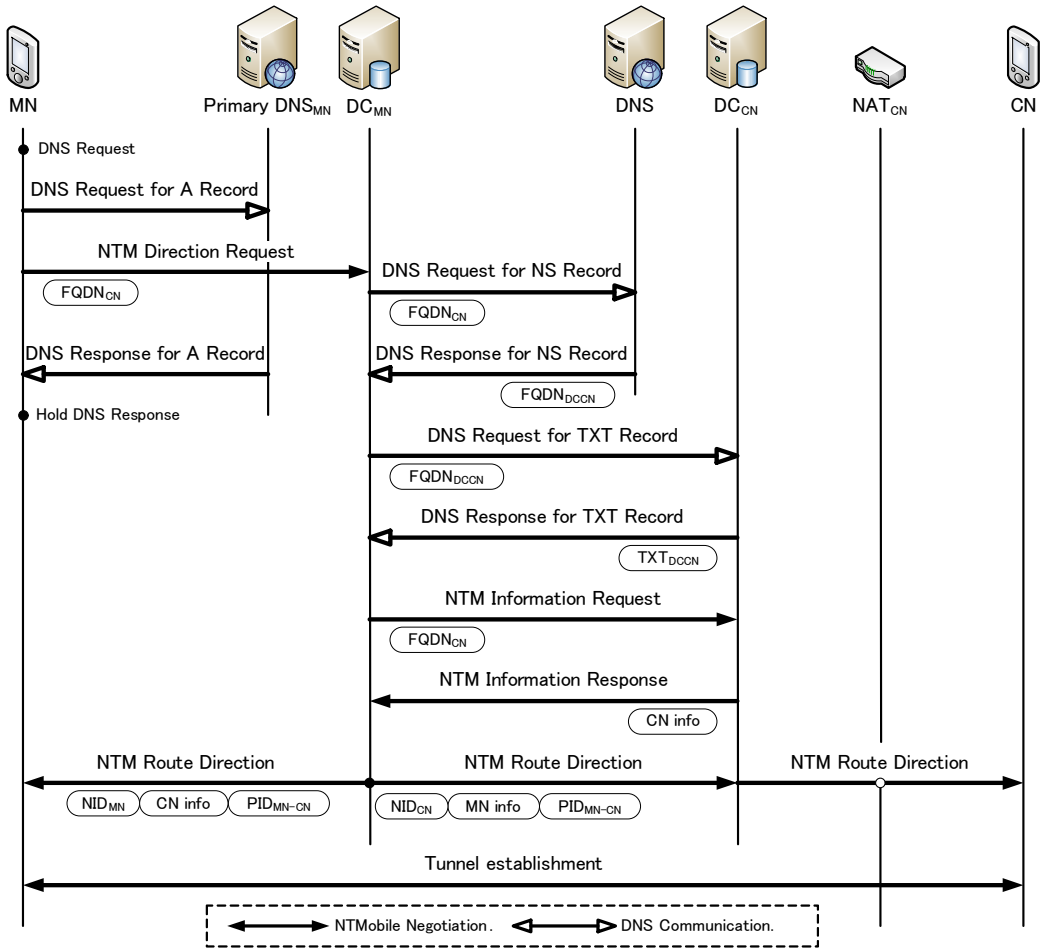

図 4.3　提案シーケンス

4.3.1　名前解決処理

MN はアプリケーションからの DNS 問い合わせを検出すると，そのパケットから $FQDN_{CN}$ を抽出して独自のネゴシエーションを開始する．ここで，トリガとなった DNS 問い合わせのパケットはそのまま DNS サーバに向けて送出させ，その応答パケットは待避しておく．この理由については 4.4 節で詳細に説明する．

MN は NTM Direction Request に $FQDN_{MN}$ と $FQDN_{CN}$ を記載して DC_{MN} へ送り，名前解決およびトンネル構築指示を依頼する．DC_{MN} は NTM Direction Request に記載されている $FQDN_{MN}$ で Node Information テーブルを検索することにより MN の端末情報を取得し，$FQDN_{CN}$ のドメインで DC キャッシュを検索する．DC キャッシュに情報が無い場合，$FQDN_{CN}$ の NS レコードを DNS クエリにより問い合わせる．DNS からの NS レコードの応答には DNS サーバの名前だけが含まれ，IP アドレスが含まれていない場合がある．その場合には DNS サーバの名前から DNS クエリにより再度 IP アドレスを問い合わせる．

ここで，CN が一般端末であった場合，DNS サーバが一般のものである場合があるため，NS レコードによる DNS サーバの名前解決後，その DNS サーバが DC であるかどうかの判

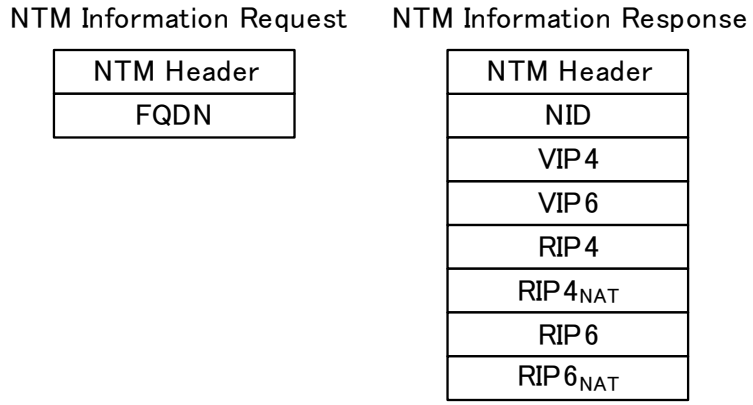

図 4.4　メッセージフォーマット

断を行う必要がある．よって，再度 DNS クエリによって DC_{CN} の TXT レコードの問い合わせを行う．

これにより，DC_{MN} は NS レコードによって特定した DNS サーバが DC であるか一般の DNS であるかを判断できる．DC_{MN} が収集した DC_{CN} の情報は，今後の通信確立時およびハンドオーバによるトンネル再構築時に利用できるため，DC_{MN} 内に DC キャッシュとして保持しておく．

特定した DNS サーバが DC であった場合，DC_{MN} は提案方式で新たに定義する独自の制御メッセージである NTM Information Request/Response により NTM 端末情報を収集を行う．NTM Information Request に $FQDN_{CN}$ を載せ，DC_{CN} に CN の端末情報を要求する．DC_{CN} は，$FQDN_{CN}$ が示す CN の端末情報を Node Information テーブルから検索し，NTM Information Response に載せて DC_{MN} へ送り返す．これにより DC_{MN} は CN の端末情報の取得を完了する．NTM Information Request/Response のメッセージフォーマットは図 4.4 に示す通りである．NTM Information Request には通信相手の FQDN を含み，NTM Information Response にはその FQDN に対応した NTM 端末情報を含む．これにより，NTM 端末の端末情報収集が DNS のキャッシュの影響をうけることを防ぐことができる．

特定した DNS サーバが一般の DNS サーバであった場合，DC_{MN} は DNS サーバに直接 $FQDN_{CN}$ の A レコードと AAAA レコードのみを問い合わせる．

4.3.2　トンネル構築

DC は従来の NTMobile と同様に収集した MN と CN の端末情報を元に経路を判断し，NTM Route Direction によって MN と CN が通信可能なトンネル構築を指示する．

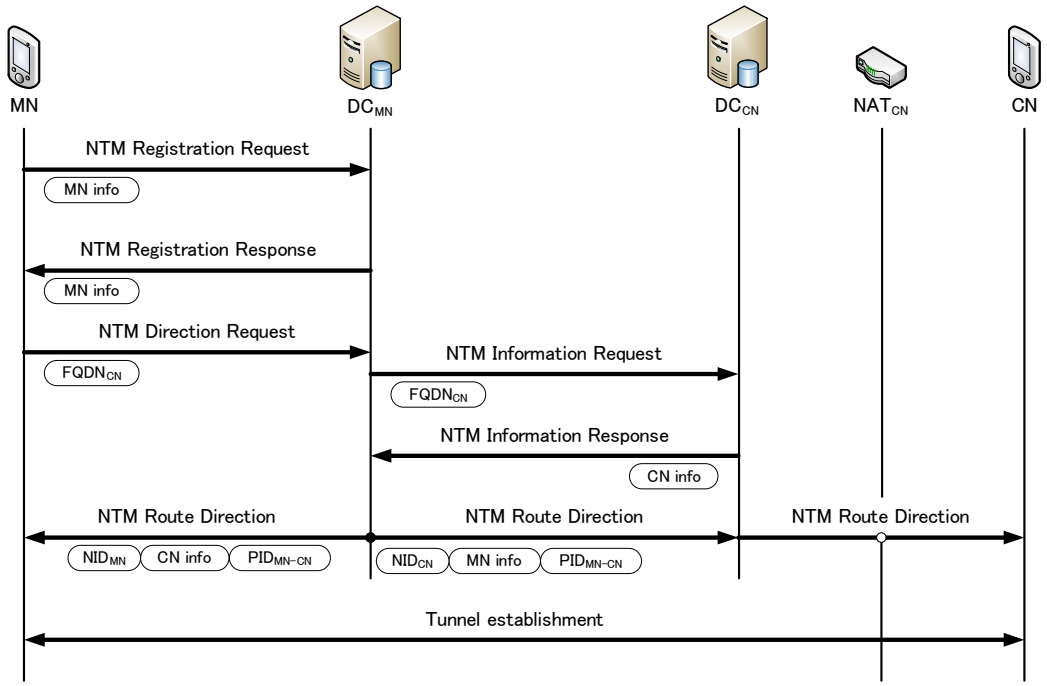

図 4.5　ハンドオーバ時の動作

4.3.3　ハンドオーバ時の動作

ハンドオーバ時の動作を図 4.5 に示す．MN がネットワークを切り替えた場合，変化したアドレス情報などを載せた NTM Registration Request を DC_{MN} に送り，Node Information テーブルを最新の情報に更新する．次に，MN は 4.3.1 項の名前解決処理と同様に $FQDN_{CN}$ を NTM Direction Request に載せて DC_{MN} に送信する．DC_{MN} は $FQDN_{CN}$ が示す CN の端末情報を再度収集する必要があるが，DC キャッシュに DC の管理ゾーンに関する情報を保持しているため，ただちに NTM Information Request/Response により CN の端末情報を受け取ることができる．更新された MN の端末情報と最新の CN の端末情報からトンネル経路を判断し，NTM Route Direction によって新たなトンネル構築を指示する．NTM 端末は，指示に従ってトンネルを再構築する．

4.4　内部ネットワークに対する名前解決

提案の通信シーケンスでは，トンネル構築に係わる A レコードなどの名前解決を NTM Direction Request によってグローバルネットワークに配置されている DC に全て任せる形になっている．このため，MN が接続しているネットワーク内に CN の情報を管理する DNS サーバがあり，かつその DNS サーバが外部からの DNS 問い合わせに対して応答しないような場合には，MN が CN の情報を取得できず通信ができないという課題が発生する．このような場合に対応するため，図 4.6 に示すように NTMobile の名前解決処理と並行してプライ

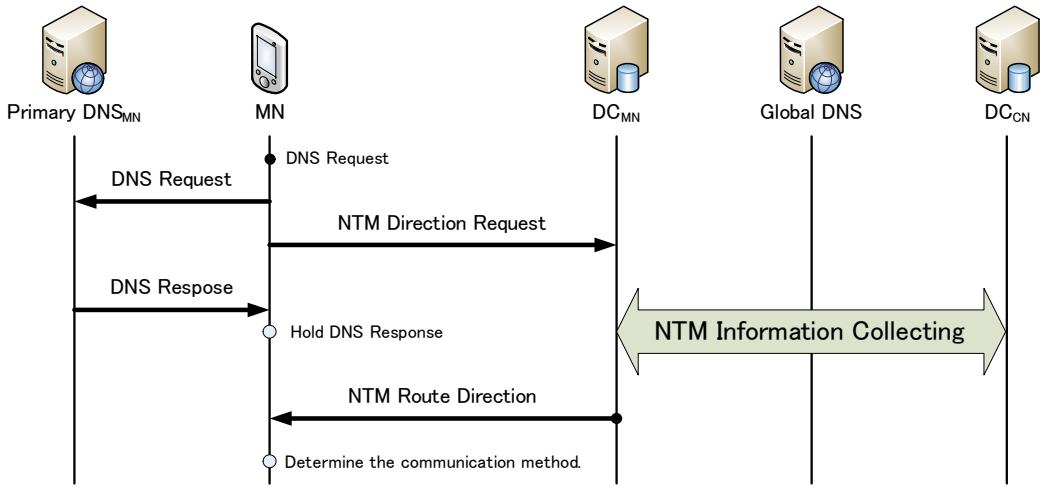

図 4.6　内部 DNS 専用の名前解決

マリ DNS サーバへの問い合わせもそのまま実行させる．プライマリ DNS サーバからの応答がある場合は，NTMobile の名前解決より先に終了する場合が多いため，一時的に待避しておく．

NTMobile の処理完了後，MN は DC_{MN} の名前解決の結果によって内部ネットワーク側との直接通信を行うか NTMobile のトンネル通信を行うかを選択する．DC_{MN} が CN の名前解決に成功すればトンネル構築を行う．DC_{MN} から名前解決ができない場合，待避していた DNS 応答の結果をアプリケーションに通知し，実アドレスによる通信を行う．

第5章　評価

5.1　提案方式の利点

従来の DNS レコードを用いた方式と提案方式の比較を表 5.1 に示す.

- DC 管理の柔軟性
  DNS レコードとして登録，管理されていた NTM 端末の端末情報をデータベースによる管理に移行することにより自由に端末情報を管理できるようになり，柔軟性が確保された.

- NTM 端末情報の秘匿性
  従来の DNS レコードを用いた管理方法では DNS 問い合わせによって NTM 端末の端末情報が公開されている状況にあった．提案方式では NTM 端末情報をデータベースに格納することで NTMobile の問い合わせに対してのみ NTM 端末情報を提供することができるようになった.

- 通信開始時の確実性
  DNS サーバに残るキャッシュの影響を受けることなく通信相手の端末情報を取得することができるようになったため，より確実な接続性を確保することができるようになった.

- 通信開始のオーバヘッド
  携帯端末のネットワークへの接続状況によっては通信遅延が大きい環境が想定されるため，通信開始に時間を要する可能性があった．提案方式で NTM 端末が複数の DNS 問い合わせによって NTM 端末情報を収集する必要がなくなった．DC はいずれもグローバルネットワークに優先接続により設置するため，遅延は安定して小さくなる.

表 5.1　DNS レコードを用いた方式と提案方式の比較

	DNS レコードを用いた方式	提案方式
DC 管理の柔軟性	△	○
NTM 端末情報の秘匿性	△	○
通信開始の確実性	×	○
通信開始のオーバヘッド	△	○

5.2 性能測定

5.2.1 実装

提案方式を Linux に実装し，動作確認を行った．図 5.1 に DC のモジュール構成図を示す．実装は Linux ディストリビューションの Ubuntu10.04，カーネルバージョン 2.6.32-44-generic を使用した．また，連携する DNS は Bind9.0 を使用し，提案方式のデータベースによる端末情報管理のため，新たにデータベースソフトの MySQL 5.1 を DC にインストールした．

DC にはトンネル構築などのネゴシエーションを行う NTM デーモンをデーモンプログラムとして実装している．また，DC は DNS 問い合わせを行うため，DNS サーバ機能を搭載している．NTM デーモンには新たに扱う NS レコード，TXT レコードおよびデータベースを扱うモジュール群を追加し，通信シーケンスの変更を行った．また，NTM 端末とのネゴシエーションを行う NTM デーモンに対しても通信シーケンスの変更に対応するよう実装を行った．動作確認を行い，正常に通信が行えることを確認した．

5.2.2 動作検証

動作検証として通信開始における動作を確認し，通信開始時のオーバヘッドを測定した．図 5.2 に試験ネットワーク構成を示す．1 台の実機 PC 上にインストールした VMware 5.0 を利用して NTM 端末 2 台および DC2 台を仮想マシンとして構築し，同一のプライベートネットワークへブリッジ接続した．また，ネゴシエーション時に使用する暗号化アルゴリズムと

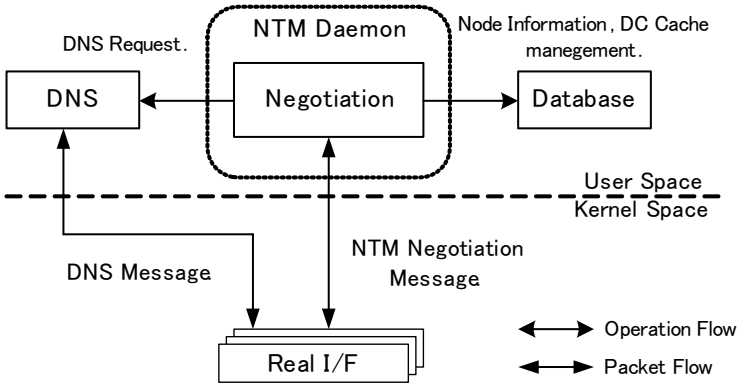

図 5.1　モジュール構成図

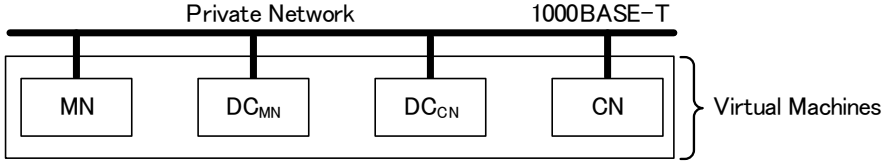

図 5.2　試験ネットワーク構成

して AES-CFB [13]，認証アルゴリズムは HMAC-MD5 [14]，鍵長 128bit とし，事前に設定した．

5.2.3 性能評価

表 5.2 に名前解決処理に要した時間の測定結果を示す．測定回数は 10 回の平均値を示している．ネゴシエーション時間合計とは NTM 端末が DNS 問い合わせを検出した時から DNS 応答に仮想 IP アドレスを書き込んでリゾルバに渡すまでの時間である．DC 処理時間とはネゴシエーション時間の一部で，DC が NTM Direction Request を受け取ってから NTM Route Direction の送信を完了するまでの処理時間である．DNS 解決時間は DC 処理時間の一部で，DC キャッシュが無い場合，DNS サーバの探索から NTM Information Request を送信するまでの処理時間を示す．

測定は仮想マシンによって行ったため通信遅延はほとんどないが，実ネットワークでは通信遅延が大きく影響を及ぼす．実ネットワークにおける提案方式のネゴシエーションにかかる時間の予測および従来方式との比較を図 5.3 従来の DNS レコードを用いる方式においては，3G ネットワークに接続した携帯端末から A, AAAA, NTM4, NTM6 の各レコードを取得するまでに 4 往復の問い合わせを必要とし，文献 [15] における実測値によると，それにかかる時間は合計 450ms 程度であった．さらに，NTM Direction Request の送信から NTM Route Direction の受信まで 200ms 程度であった．また，3G ネットワークと無線 LAN にそれぞれ接続した携帯端末同士の NTM Tunnel Request/Response の 1 往復に要する時間はおよそ 340ms であり，ネゴシエーション全体を合計するとほぼ 1 秒かかった．一方，提案方式では最初から DC にトンネル構築の指示を依頼するため，3G ネットワークでの 4 往復分の通信時間が発生しない．また，提案方式では CN の端末情報を取得するため DC 同士で 1 往復の通信を行う．グローバルネットワーク上における国内の一般的な RTT は 20ms 程度であるため，この時間が加算される．NTM 端末と DC の内部処理にかかる時間が従来方式と同じと仮定し，通信に係わる時間の違いに着目すると，実ネットワークにおけるネゴシエーション時間合計の推測値は従来方式が約 1s に対し，提案方式では約 570ms と推測できる．

提案方式においては DC_{MN} は 2 回目の問い合わせ以降は DC キャッシュに保持する情報を用いて CN の端末情報を取得することができる．しかし，DC キャッシュに該当する情報が無い場合は DNS の仕組みを用いて DC を発見する必要があり，NS，A，AAAA，TXT レコード問い合わせによる 4 往復の通信が追加される．この時間を推測すると，通信時間の増加は 80ms 程度である．この場合，表 5.2 の DNS 解決時間の部分が 80ms となり，提案方式のネゴシエーション時間合計は約 650ms になると推測できる．提案方式では DC キャッシュの時間を長めに設定できるため，通信開始時のオーバヘッドを大きく削減することができる．

表 5.2　測定結果

	計測結果 [ms]
ネゴシエーション時間合計	50.6
DC 処理時間	32.0
DNS 解決時間	7.5

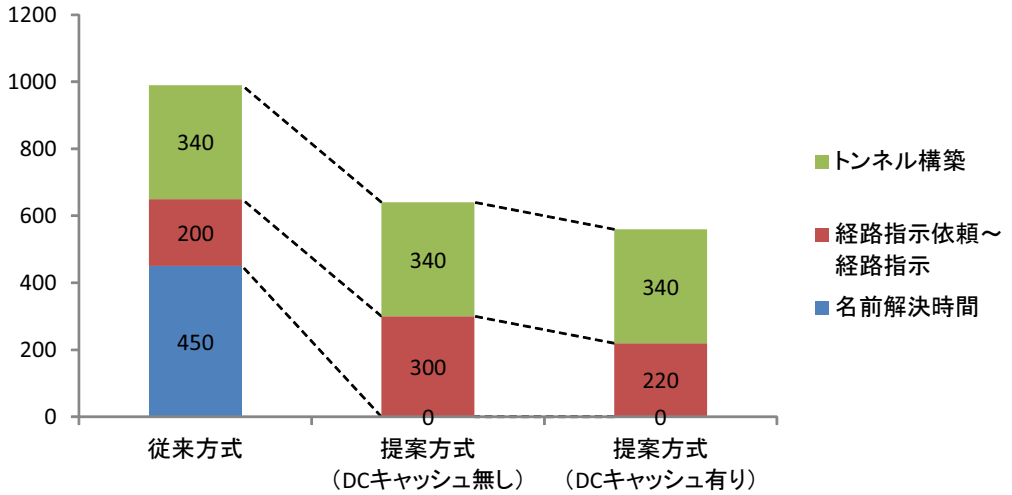

図 5.3　実ネットワークおける予測値と従来方式との比較

第6章　提案方式の今後の展開

提案方式は，別途検討を行っている NTMobile におけるグループ認証の適用および移動透過性技術におけるダブルジャンプ問題の解決に対して効果的だと考えられる点がある．詳細な検討は引き続き必要ではあるが，提案方式による NTMobile の今後の展開について述べる．

6.1　グループ認証の適用

NTMobile は実ネットワークにおける制約を排除したネットワーク本来のオープンな世界を実現している．しかし，実ネットワーク上において NAT がもたらした副次的な効果である外部ネットワークから内部ネットワークの構造が見えなくなる性質は，組織のセキュリティにおいて効果的であるという側面を持っている．NTMobile において全てのノードに対して接続性を確保する性質は，セキュリティの観点から保護したいノードに対して不正アクセスの脅威を助長しかねない性質であるとも言える．このため，NTMobile では文献 [16] においてグループ単位の認証機能を追加し，認証結果に応じた通信の可否を制御する方式について検討を行っている．従来方式にこのグループ認証を適用する場合，図 6.1 に示すように NTM 端末

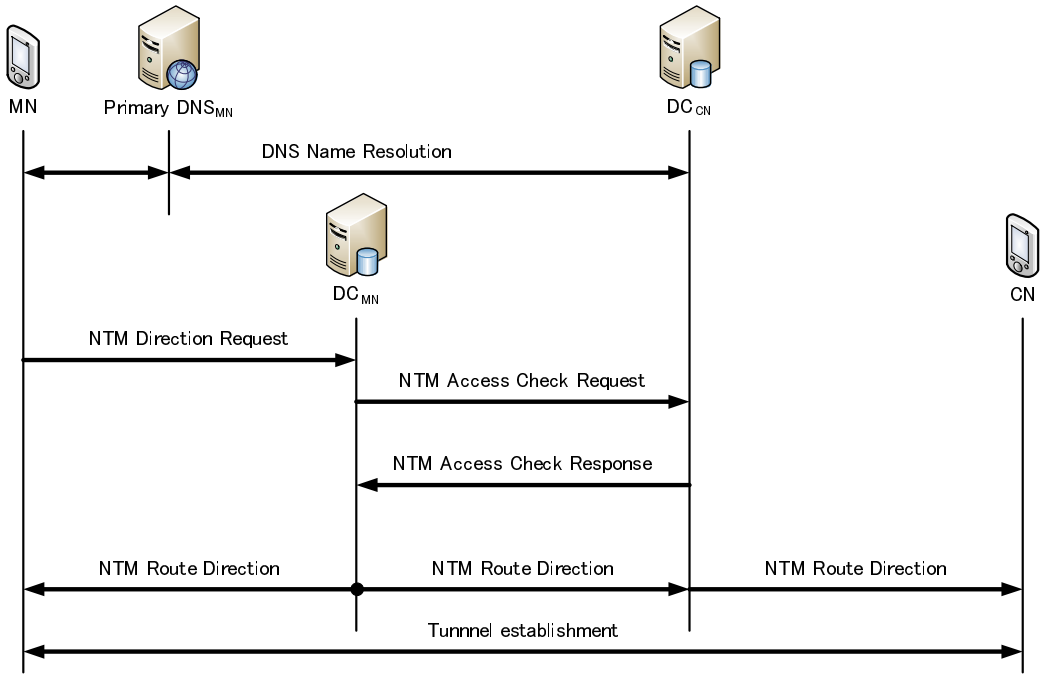

図 6.1　従来方式におけるグループ認証の通信シーケンス

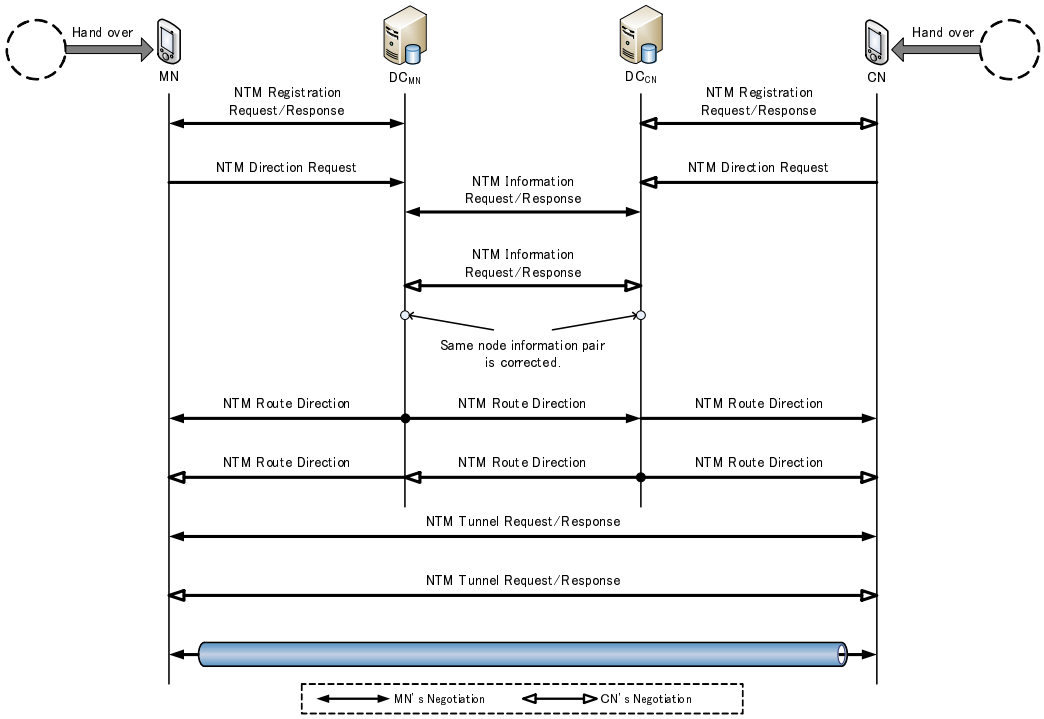

図 6.2　ダブルジャンプ時の通信シーケンス

が登録している DC 間に専用の制御メッセージ NTM Access Check Request/Response による情報交換が必要であった．しかし，提案方式において NTMobile が DC 間で NTM Information Request/Response による通信を行うため，従来冗長とみられていたグループ認証のための情報交換を NTMobile の基本シーケンスに取り込むことが可能となり，オーバヘッドが発生しない認証機能の追加が可能な見込みである．

6.2　ダブルジャンプ問題の解決に向けて

ダブルジャンプ問題とは移動透過性技術における課題であり，通信中の 2 台のエンドノードが同時にハンドオーバを行った場合，移動透過性が実現できなくなる問題である [17]．従来方式の NTMobile では，ハンドオーバ直後に自身の新たな IP アドレスと通信相手の今まで使用していた IP アドレスを含んだ NTM Direction Request を用いてトンネル構築を行うよう DC に依頼を行っていた．このため，ダブルジャンプが発生すると両エンドノードは通信相手の移動前の IP アドレスとのトンネル構築を行ってしまい，通信を継続することができない．

提案方式におけるダブルジャンプ時の通信シーケンスを図 6.2 に示す．提案方式では，エンドノードが同時にハンドオーバを行った場合，直ちに NTM Registration Request/Response によって自身の DC に最新の IP アドレスを登録する．そして，NTM Direction Request によって通信相手の FQDN を指定して DC にトンネルの再構築を依頼する．DC は FQDN を元に

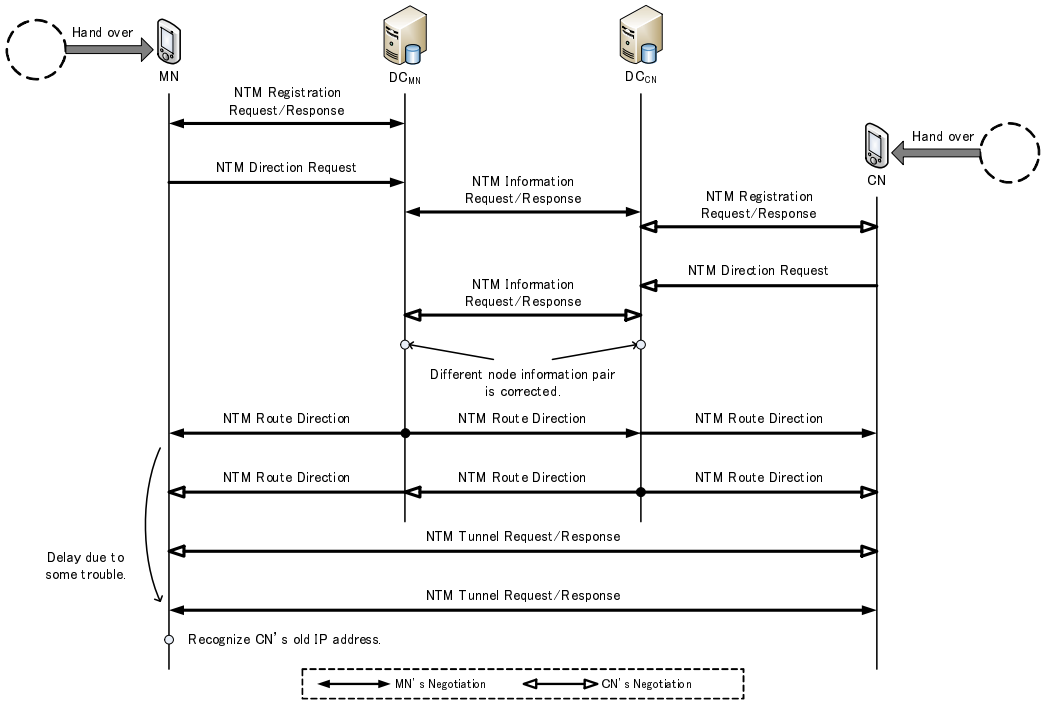

図 6.3　ダブルジャンプ問題が発生する場合

この時点での IP アドレスを通信相手の DC に NTM Information Request/Response によって問い合わせる．両 DC が NTM 端末が移動した後の IP アドレスを取得でき，これを元にトンネルを構築する指示を出す．よって，NTM Route Direction には両エンドノードの移動後の IP アドレスが記載され，ダブルジャンプ問題を解決することが可能である．

しかし，現在このダブルジャンプ問題の解決は図 6.3 に示すような条件下において課題を抱えている．それは，ダブルジャンプがわずかにズレたタイミングで発生し，先にハンドオーバした NTM 端末から開始されたトンネルの再構築処理が通信相手のハンドオーバ前の IP アドレスに対して行われ，かつ，直後に発生した通信相手のハンドオーバによって開始されたトンネルの再構築処理より何らかの理由でパケット到着が遅れてしまう場合である．この場合，大きく遅延した NTM Route Direction や NTM Tunnel Request の影響によりハンドオーバ前の古い情報のトンネルテーブルが生成されてしまい，通信継続ができなくなる．発生する可能性は高いとは言えないが，検討が必要である．また，NTMobile におけるシームレスハンドオーバの実現については文献 [18] において別途検討を行っている．

第7章　まとめ

本論文では，アドレス空間や体系に依存しない通信接続性の確立と移動透過性を同時に実現する NTMobile における通信端末情報の管理および収集方法が抱えていた課題の解決手法について提案を行った．提案方式では通信開始におけるオーバヘッドを大きく削減するとともに，DNS 問い合わせを使用することによるキャッシュの影響により通信接続性の確保ができない場合がある課題を解決する通信シーケンスの提案を行った．さらに，DNS レコードとして公開されていた端末情報をデータベースに格納し，秘匿性を確保するとともに運用管理の容易さと柔軟性を向上させた．また，提案方式を実装し，動作確認を行った．この結果，提案方式ではデータベースによる端末情報管理により端末情報の秘匿性と拡張性および端末情報管理の柔軟性を確保した．また，通信開始において通信接続性を確保できない課題を解決し，実ネットワーク環境における従来方式の実測値を元にした提案方式の性能予測によって通信開始時のオーバヘッドを大幅に削減可能であることを確認した．加えて，提案方式を用いることによる今後の NTMobile の機能拡張について展望を述べた．今後は実ネットワーク環境において実装したシステムの詳細な性能評価を行う．

謝辞

本研究に関して，研究の方向や進め方など終始御熱心な御指導とご教示を賜りました，名城大学理工学部情報工学科　渡邊晃教授に心より厚く御礼申し上げます.

本論文を作成するにあたり，快く査読を引き受けてくださり，熱心にご指導を頂きました，名城大学理工学部情報工学科　柳田康幸教授に心より厚く御礼申し上げます.

本研究を進めるにあたり，研究内容に関して終始御熱心な御指導とご教示を賜りました，名城大学理工学部情報工学科　旭健作助教に心より厚く御礼申し上げます.

本研究を進めるにあたり，研究内容に関して終始御熱心な御指導とご教示を賜りました，名城大学理工学部情報工学科　鈴木秀和助教に心より厚く御礼申し上げます.

本研究を進めるにあたり，研究内容に関して終始御熱心な御指導とご教示を賜りました，三重大学大学院工学研究科　内藤克浩助教に心より厚く御礼申し上げます.

最後に，本研究を行うにあたり，適切なご検討を頂いた，名城大学理工学部情報工学科渡邊研究室並びに鈴木研究室の皆様に心より感謝致します.

参考文献

[1] Deering, S. and Hinden, R.: Internet Protocol, Version 6 (IPv6) Specification, RFC2460, IETF (1998).

[2] Le, D., Fu, X. and Hogrefe, D.: A review of mobility support paradigms for the internet., *IEEE Communications Surveys and Tutorials*, Vol. 8, No. 1-4, pp. 38–51 (2006).

[3] 鈴木秀和，上醉尾一真，水谷智大，西尾拓也，内藤克浩，渡邊　晃：NTMobile における通信接続性の確立手法と実装，情報処理学会論文誌，Vol. 54, No. 1, pp. 367–379 (2013).

[4] 内藤克浩，上醉尾一真，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，情報処理学会論文誌，Vol. 54, No. 1, pp. 380–393 (2013).

[5] 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，DICOMO2012 論文集，Vol. 2012 (2012).

[6] 土井敏樹, 鈴木秀和, 内藤克浩, 渡邊　晃：NTMobile における RS の検討, DICOMO2012 論文集，Vol. 2012 (2012).

[7] Mockapetris, P.: DOMAIN NAMES - CONCEPTS AND FACILITIES, Rfc1034, IETF (1987).

[8] Mockapetris, P.: DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION, Rfc1035, IETF (1987).

[9] Vixie, P., Thomson, S., Rekhter, Y. and Bound, J.: Dynamic Updates in the Domain Name System(DNS UPDATE), RFC2136, IETF (1997).

[10] 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，DICOMO2012 論文集，Vol. 2012 (2012).

[11] 納堂博史，鈴木秀和，内藤克浩，渡邊　晃：NTMobile における自律的経路最適化の提案，情報処理学会論文誌，Vol. 54, No. 1, pp. 394–403 (2013).

[12] Andrews, M.: Negative Caching of DNS Queries (DNS NCACHE), Rfc2308, IETF (1998).

[13] of Standards, N. I. and Technology: Specification for the ADVANCED ENCRYPTION STANDARD(AES), Technical report, FIPS 197 (2001).

[14] Krawczyk, H., Bellare, M. and Canetti, R.: HMAC: Keyed-Hashing for Message Authentication, Rfc2003, IETF (1997).

[15] 上醉尾一真，鈴木秀和，内藤克浩，渡邊　晃：IPv4/IPv6 混在環境における NTMobile の検討，情報処理学会第 74 回全国大会論文集，pp. 3–221–3–222 (2011).

[16] 村橋考謙，鈴木秀和，旭　健作，内藤克浩，渡邊　晃：NTMobile におけるグループ認証方式の提案と実装，情報処理学会研究報告，Vol. 2011-MBL-59 (2011).

[17] Huitema, C.: Multi-homed TCP, Internet-draft, IETF (1995).

[18] 福山陽祐，鈴木秀和，渡邊　晃：IPv4 移動体通信において携帯電話網と無線 LAN 間をシームレスに移動する方式の提案，DICOMO2011 論文集 (2011).

研究業績

研究会・大会等

1. 細尾幸宏, 鈴木秀和，渡邊晃, “GSCIP の Windows への実装に関する検討”, 平成 19 年度電気関係学会東海支部連合大会論文集，Sep.2007.

2. 細尾幸宏, 鈴木秀和，渡邊晃, “GSCIP の Windows への実装に関する検討”, 情報処理学会第 70 回全国大会講演論文集，Mar.2008.

3. 細尾幸宏, 鈴木秀和，渡邊晃, “GSCIP の Windows への実装に関する検討”, マルチメディア, 分散, 協調とモバイル（DICOMO2008）シンポジウム論文集, Vol.2008, No.1, pp.616-621，Jul.2008.

4. 細尾幸宏, 鈴木秀和，内藤克浩，旭健作，渡邊晃, “NTMobile における DNS 実装の変更が不要な データベース型端末情報管理手法の検討”, 情報処理学会研究報告，2012-MBL-64，Nov.2012.

受賞歴

1. モバイルコンピューティングとユビキタス通信研究会・奨励発表（2012 年 11 月）
細尾幸宏，鈴木秀和，内藤克浩，旭健作，渡邊晃, “NTMobile における DNS 実装の変更が不要な データベース型端末情報管理手法の検討”, 情報処理学会研究報告, 2012-MBL-64，Nov.2012.

付 録A　記号の定義

- RIP_N ; ノード N の実 IP アドレス
- VIP_N ; ノード N の仮想 IP アドレス
- NID_N ; ノード N の識別子
- PID_{N1-N2} ; ノード N1 とノード N2 間で構築するトンネルの識別子