

NTMobileにおける名前解決方式の提案と評価

083430033 細尾 幸宏
渡邊研究室

1. はじめに

スマートフォンなどの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。互換性がない IPv4 と IPv6 の混在環境における通信接続性や、接続するネットワークの切り替えによって IP アドレスが変化しても通信が継続できる移動透過性の実現が今後のネットワークにおける重要な課題である。

著者らは IPv4/IPv6 混在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 [1]。NTMobile では通信開始時に必要な NTM 端末情報を DNS レコード形式にしており、DNS の仕組みを利用して共有している。しかし、DNS キャッシュの影響により通信接続性が確保できない場合や、DNS レコードとして NTMobile 特有の端末情報が誰でも取得可能であるという管理上の課題があった。

本稿では NTM 端末情報の収集を DNS キャッシュの影響を受けないデータベース方式に変更し、端末情報をデータベースへ格納することで情報の秘匿性と、端末情報管理の柔軟性や拡張性を確保する方式について提案する。また、提案方式を実装し、評価を行った。

2. NTMobile

2.1 NTMobile の概要

図 1 に NTMobile の概要を示す。NTMobile は仮想 IP アドレスとトンネル通信を用いた技術であり、NAT 配下の NTMobile 対応端末 (NTM 端末) に対する接続性を確保できる。また、IPv4 と IPv6 ネットワーク間の接続性を確保することができ、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。

アプリケーションは仮想 IP アドレスを認識して通信を行い、実 IP アドレスの変化に影響されることなく通信を継続することができる。中継装置 RS(Relay Server) を用いることで異なる NAT 配下同士の通信や、IPv4 と IPv6 に接続する端末同士の通信を行うことが可能である。また、経路最適化により、異なる NAT 配下同士でも NAT の種類によっては直接通信に切り替えることができる。

2.2 NTMobile における DNS の利用状況

NTMobile は NTM 端末への接続性および移動透過性に必要な端末情報を DNS の仕組みを利用して取得する。管理装置 DC(Direction Coordinator) は DDNS(Dynamic DNS) 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 レコードが登録されている。NTM 端末には自身のホスト名と DC のドメイン名から FQDN(Fully Qualified Domain Name) が割り当てられる。これにより、FQDN を問い合わせることで既存の DNS の仕組みで NTM 端末情報が取得可能である。NTM 端末は自身の IP アドレスが変化した場合などに動的に DC が保持する端末情報を更新し、NTM レコードによる通信接続性を維持する。NTM 端末は通信開始時に接続しているネットワークのプライマリ DNS を介して NTM 端末情報を取得する。

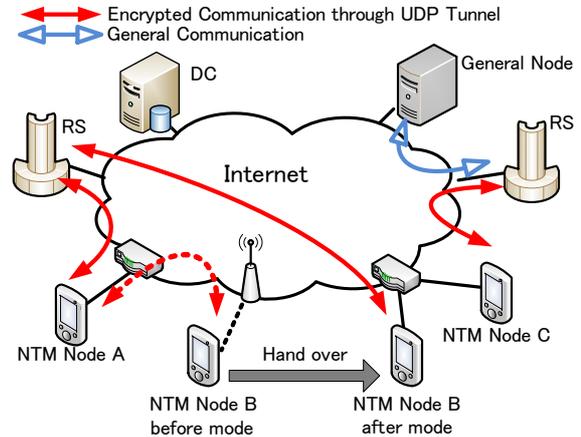


図 1: NTMobile の概要

2.3 NTMobile の課題

現状の NTMobile の名前解決は既存の DNS を利用する方式であるため、以下のような課題がある。

- DNS におけるレコード情報管理はテキスト形式によるものであり、携帯端末のように急激に進化しているネットワーク利用形態に対して NTM 端末情報の構成を柔軟に変更したり、新たなサービスに対応する拡張性に乏しい。
- NTM レコードとして追加で取り扱っている端末情報は、誰でも FQDN から NTM 端末情報を取得可能となっている。
- DNS サーバに DNS 問い合わせのキャッシュが残っている場合、NTM 端末が移動しても移動前の情報しか取得できず、通信を開始できない場合がある。
- 通信開始時に A, AAAA, NTM4, NTM6 の各レコードを取得する 4 回の DNS 問い合わせを行う必要があり、通信遅延の大きい 3G 回線等を使用している場合に接続時間が大きくなる可能性がある。

3. 提案方式

3.1 提案方式の方針

通信開始時に NTM 端末が行う DNS 問い合わせを DC_{MN} に依頼する方法に変更する。 DC_{MN} は NS レコードを用いて DC_{CN} を発見し、 DC_{MN} と DC_{CN} 間は新たに定義する独自のメッセージを用いて直接情報を収集する。これにより、通信開始時の DNS キャッシュの影響による接続性の課題と、オーバーヘッドの削減を行う。新たに追加される NS レコードの探索については、DC はグローバルネットワーク上に設置するため、NTM 端末から行う DNS 問い合わせに比べて高速に行うことができる。また、この方法により NTM 端末情報は 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 レコード形式ではなくデータベースへ格納し、NTMobile のモジュールが扱うこととする。

3.2 データベースによる情報管理

DC のデータベースでは Node Information テーブルと DC キャッシュの 2 つ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 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、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。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、情報があれば通信開始に関わる処理を省略可能である。

3.3 提案シーケンス

提案シーケンスを図 2 に示す。図 2 では MN, CN の DC をそれぞれ DC_{MN} , DC_{CN} とし、 DC_{CN} の上位 DNS サーバを DNS_{DC-CN} とする。また、CN は NAT_{CN} 配下に接続している場合について説明する。事前に、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。

MN はアプリケーションからの DNS Query を検出すると、 $FQDN_{CN}$ を抽出して独自のネゴシエーションを開始する。従来方式のように自分で CN の NTM 端末情報を収集せず、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。TXT レコードは、探索した DNS サーバが DC であるか一般の DNS サーバであるかを確認するために問い合わせを行う。 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ーによるトンネル再構築時に利用できるため、 DC_{MN} 内の DC キャッシュに保持する。

特定した DNS サーバが DC であった場合、 DC_{MN} は NTM Information Request/Response により DC_{CN} から CN の端末情報を取得する。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。

DC は従来の NTMobile と同様に収集した MN と CN の

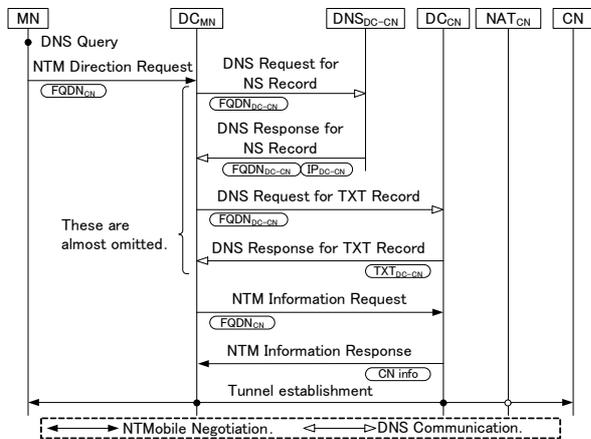


図 2: 提案シーケンス

表 1: 従来方式と提案方式の比較

	従来方式	提案方式
NTM 端末情報管理の柔軟性	×	○
NTM 端末情報の秘匿性	×	○
通信開始の確実性	△	○
通信開始のオーバーヘッド	△	○

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。

4. 評価

4.1 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 1 に示す。

NTM 端末情報管理の柔軟性

端末情報をデータベースによる管理に移行することで NTM 端末情報管理の柔軟性と拡張性を確保した。

NTM 端末情報の秘匿性

NTMobile の問い合わせに対してのみ端末情報を提供することが可能となった。

通信開始の確実性

NTM 端末が行っていた名前解決を DC の独自メッセージで行うことで、DNS 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可能になり、通信開始の確実性を確保した。

通信開始のオーバーヘッド

NTM 端末からの DNS 問い合わせを廃止することで通信開始時のオーバーヘッドが安定して小さくなる。

4.2 性能測定

提案方式を仮想マシンに実装し、性能測定を行った。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。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、実測値によるとそれにかかる時間は合計 450 から 490ms 程度であり、3G と Wi-Fi ネットワーク間における通信開始には約 950ms を要した。

これに対し、提案方式では DNS 問い合わせを行わないため通信開始時のオーバーヘッドは大幅に減少し、約 490ms と推測できる。提案方式は従来方式と比べて大幅に通信開始時のオーバーヘッドを削減する効果があるといえる。

5. まとめ

本稿では、NTMobile における名前解決時および端末情報管理に関する課題の解決手法について提案を行った。提案方式では 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柔軟性と拡張性を確保した。さらに、通信開始におけるオーバー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。また、提案方式を実装し、動作検証を行った。

参考文献

- [1] 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).

NTMobileにおける名前解決方式の 提案と実装

名城大学大学院 理工学研究科 情報工学専攻
渡邊研究室 083430033 細尾幸宏

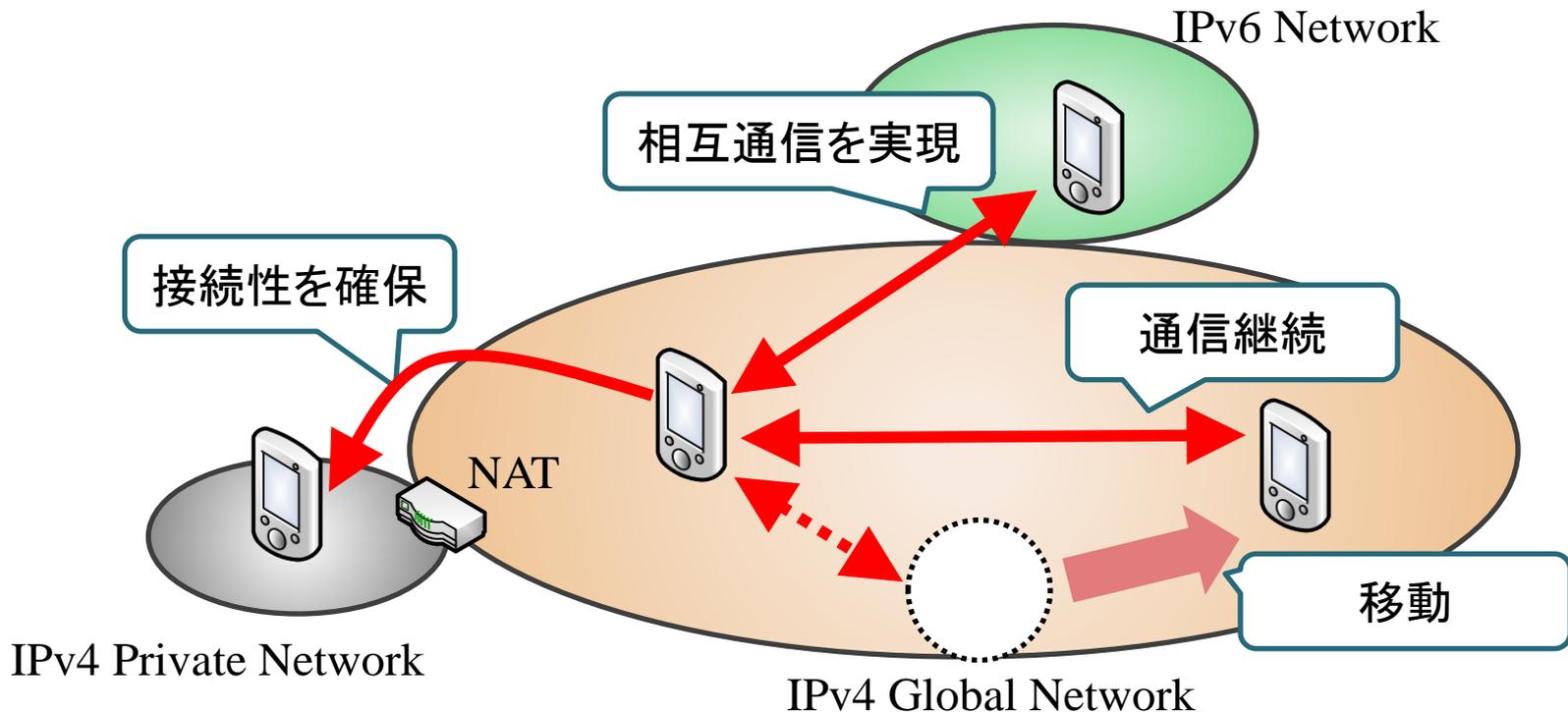
はじめに

- IPv4グローバルアドレスの枯渇問題
 - NAT設置で延命
 - NAT越え問題が発生
- IPv6へ移行することは必須
 - IPアドレスがほぼ無限
- しかしIPv4と互換性が無いため・・・
 - IPv4と通信できない
 - 急速な普及は望めない
- 混在環境への長期的な対策が必要

IPv4/IPv6混在環境における接続性と移動透過性
NTMobile (Network Traversal with Mobility)

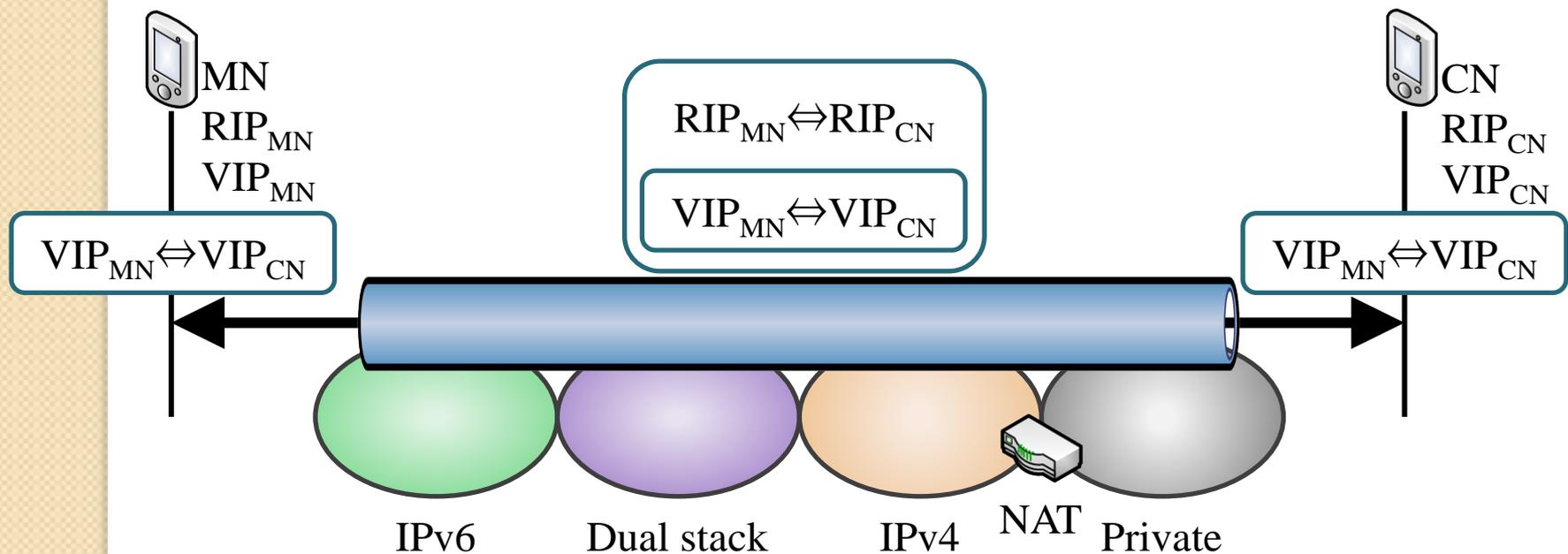
NTMobileの概要

- IPv4/IPv6間の相互通信
- NAT配下のNTM端末に対する接続性
- 移動しても通信が継続できる移動透過性



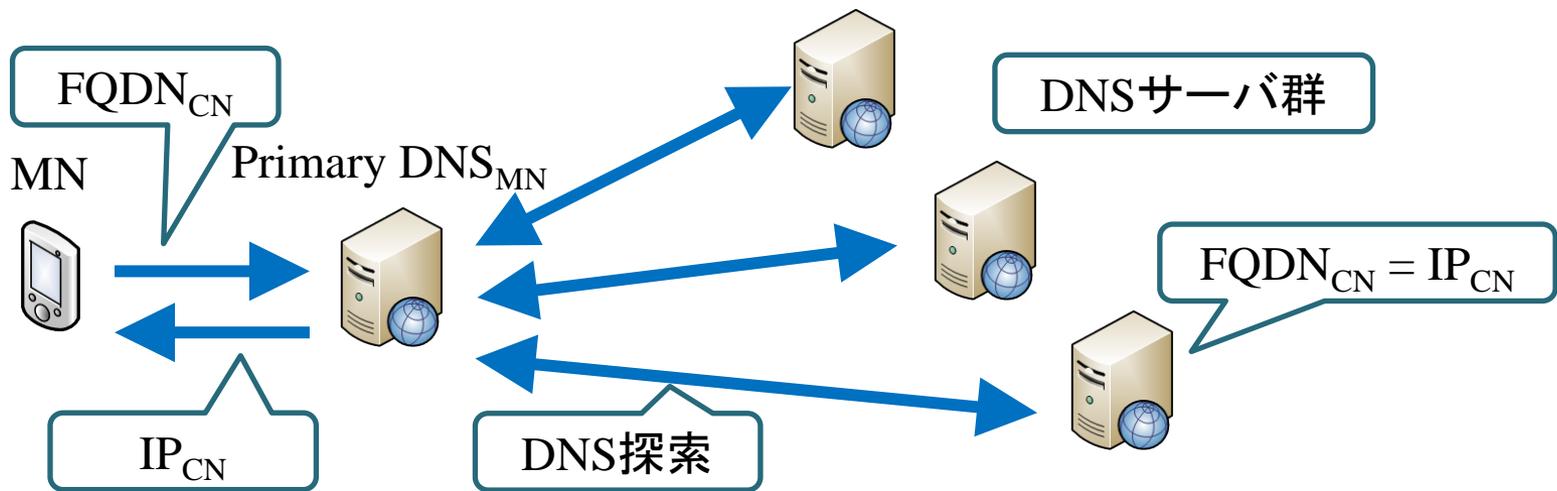
NTMobileの概要

- NTM端末は実IPアドレスと仮想IPアドレスを持つ
- アプリケーションは仮想IPアドレスを認識
- UDPトンネルが実ネットワークの制約を隠蔽



DNS (Domain Name System)

- ホスト名 (FQDN) とIPアドレスの関係を管理
- インターネットユーザに変換機能を提供



- NTMobileは情報管理, 共有にこの仕組みを利用
- 管理装置DCがDDNS機能をもつ

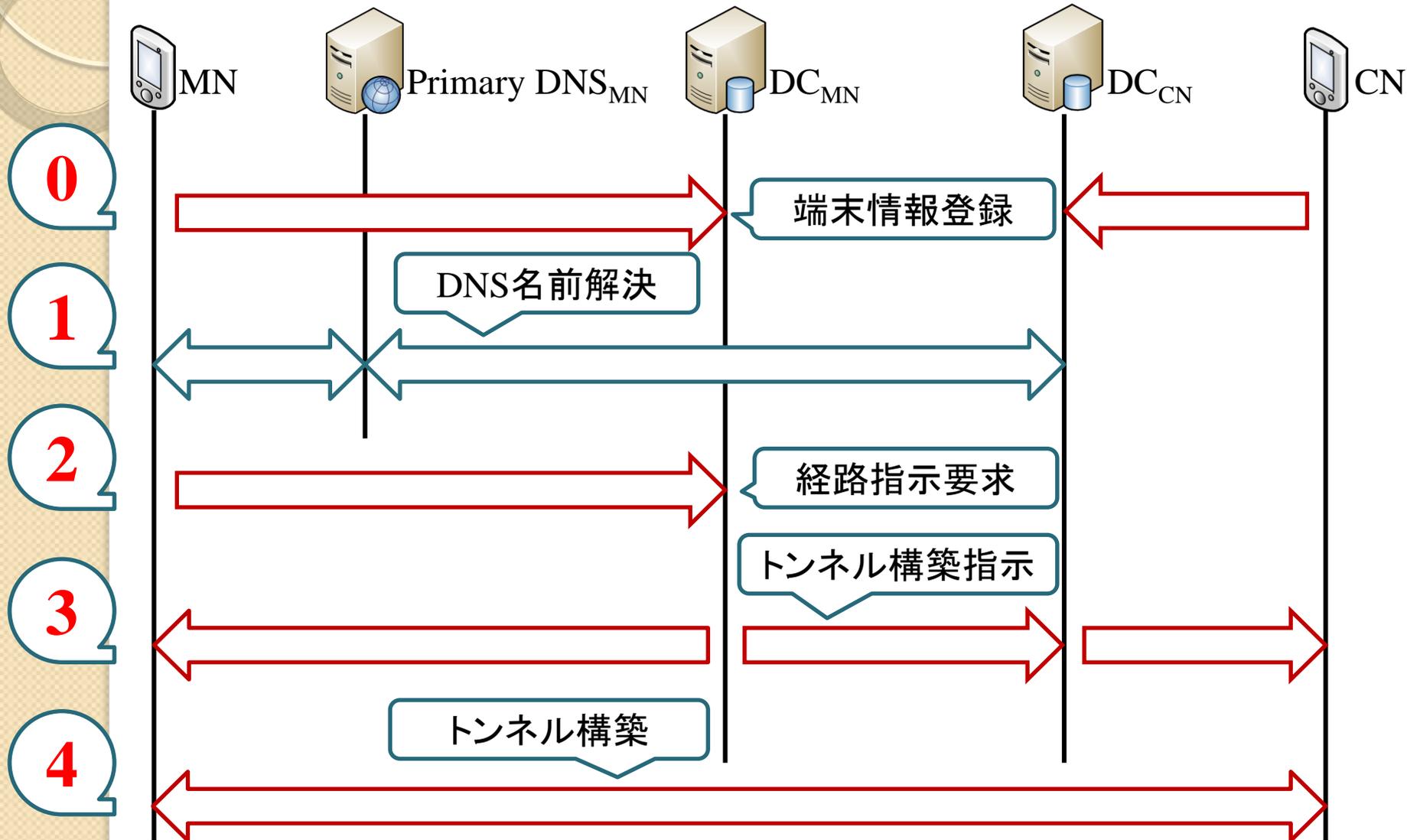
DC; Direction Coordinator

DDNS; Dynamic DNS アドレス情報を動的に更新するDNS

DNSの仕組みを利用する利点

- 独自の情報管理，共有システムが不要
 - DNSの形式に従えば，容易に情報共有システムとして運用可能
- インターネットが使える環境ならどこでも利用可能
- システムの規模に応じた分散管理に対応
- 世界中で運用されている実績

NTMobile通信シーケンス

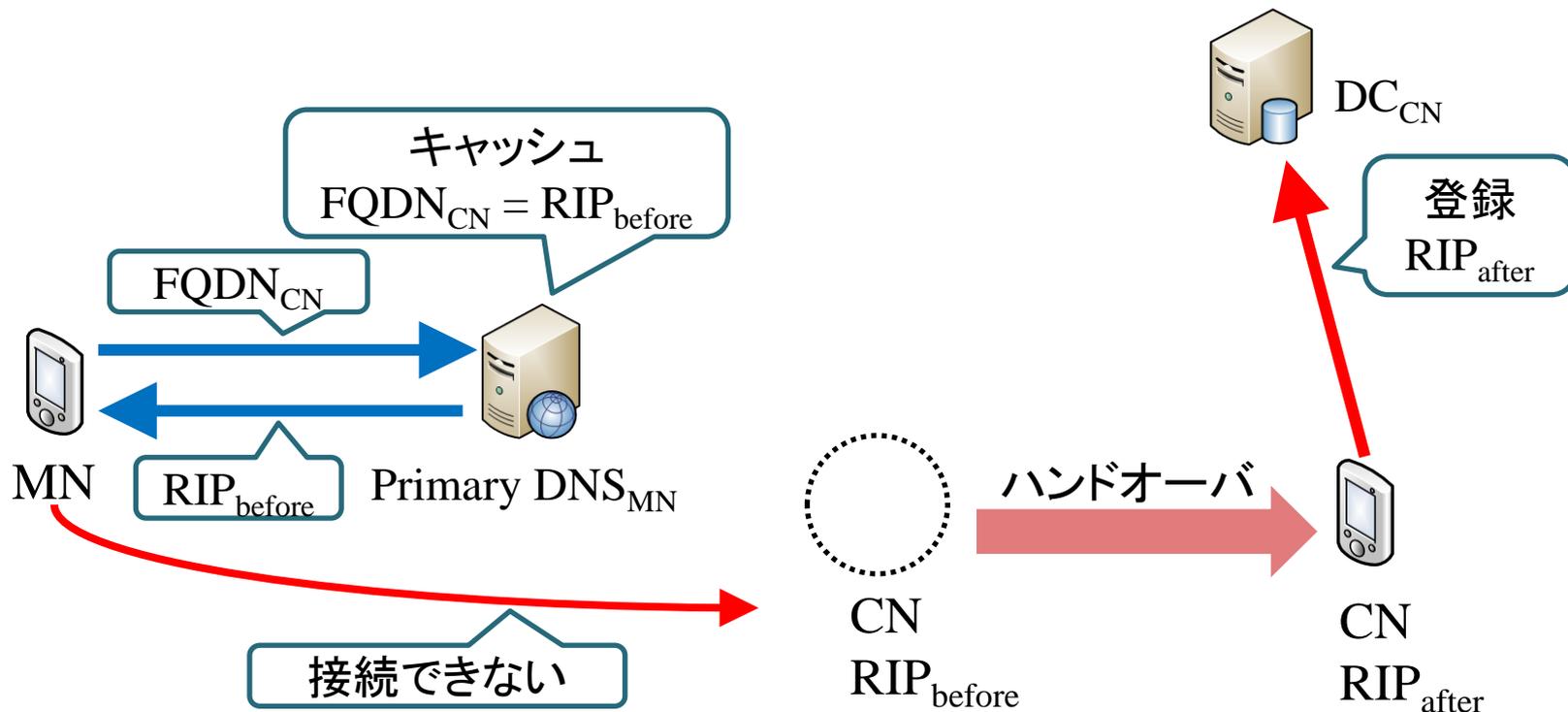




- **DNSを利用することによる
NTMobileの課題**

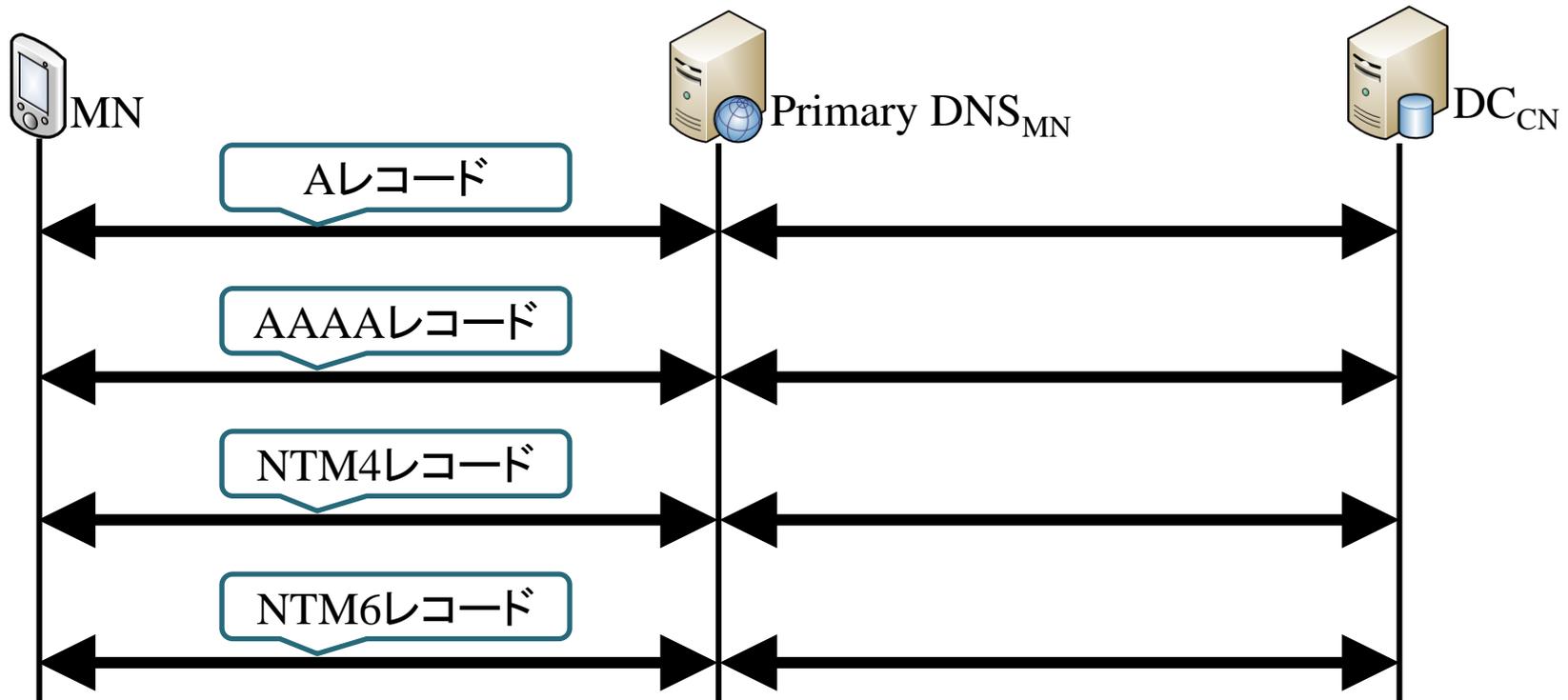
情報共有手法と管理の課題 1

- DNSキャッシュが有効だと最新アドレスが取得できない
 - DNSキャッシュを無効と毎回DNSによる探索が発生



情報共有手法と管理の課題 2

- 通信開始時のオーバーヘッド
 - 4回のDNS問い合わせが必要
 - 3G回線など遅延が大きい場合の問題



NTMレコード: NTMobile専用のDNSレコード

情報共有手法と管理の課題 3

- NTM端末情報をDNSレコード形式で管理
 - DNSレコードは固定的な形式のテキスト情報
 - 端末情報のリレーショナルな管理など複雑な処理ができない
- FQDNから誰でもNTMLレコードを取得できる

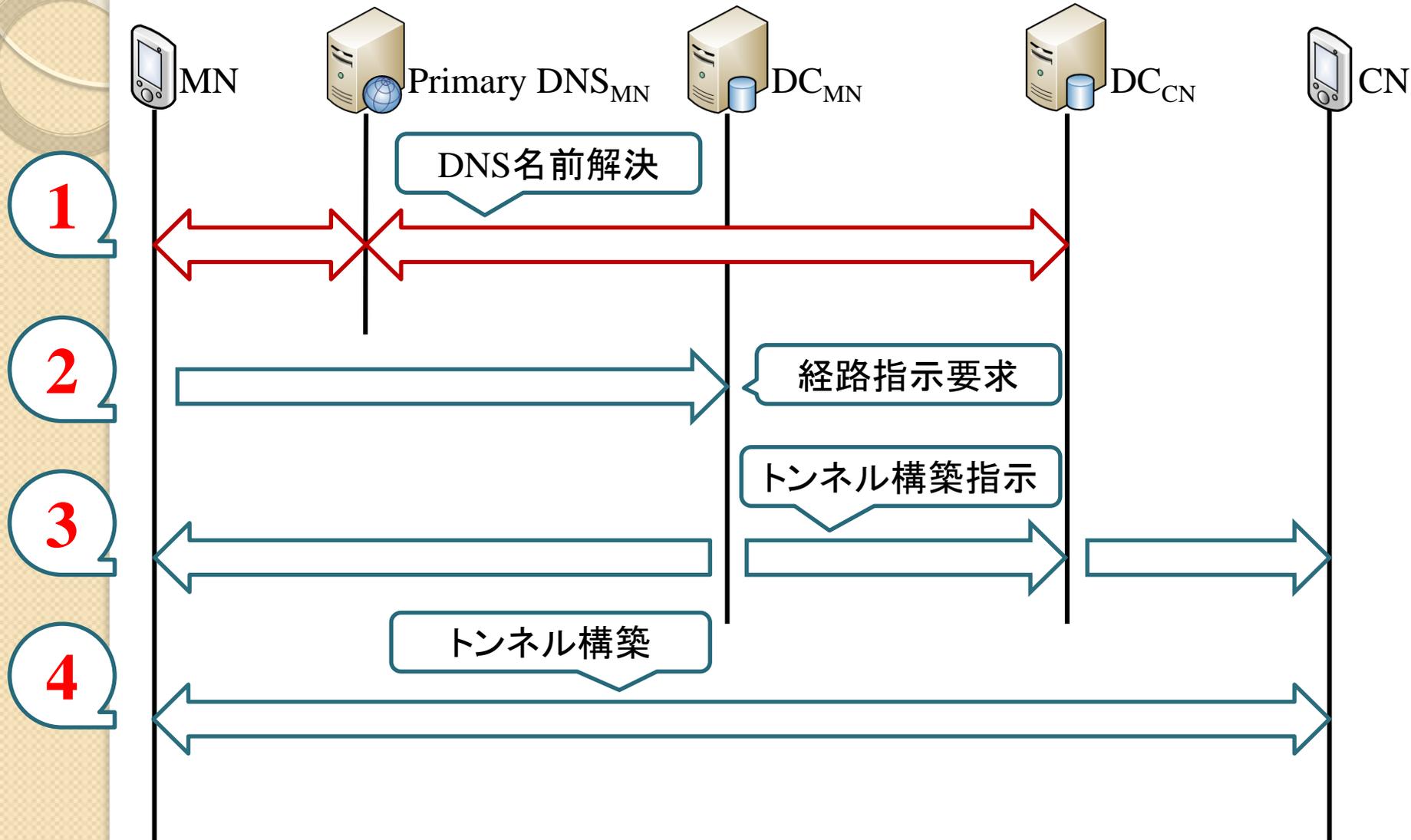


提案方式

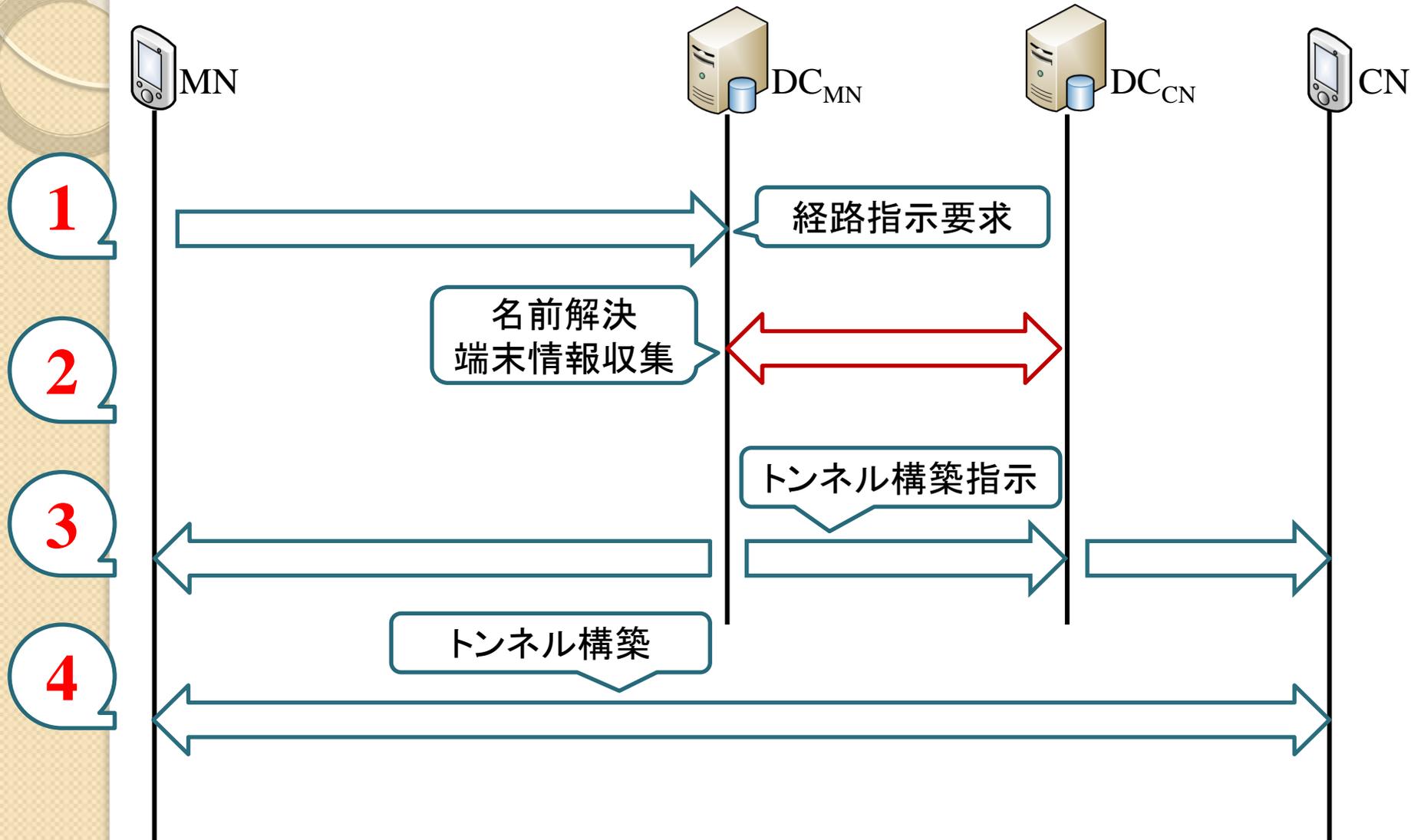
課題解決の方針

1. 通信相手の情報収集をDCに任せる
 - 通信開始時の遅延減少
 - DNSキャッシュの影響がない情報収集
 - DCの探索には引き続きDNSを利用
2. データベースによる端末情報管理
 - 端末情報を柔軟に構成
 - セキュリティの確保

従来方式の通信シーケンス (再掲)

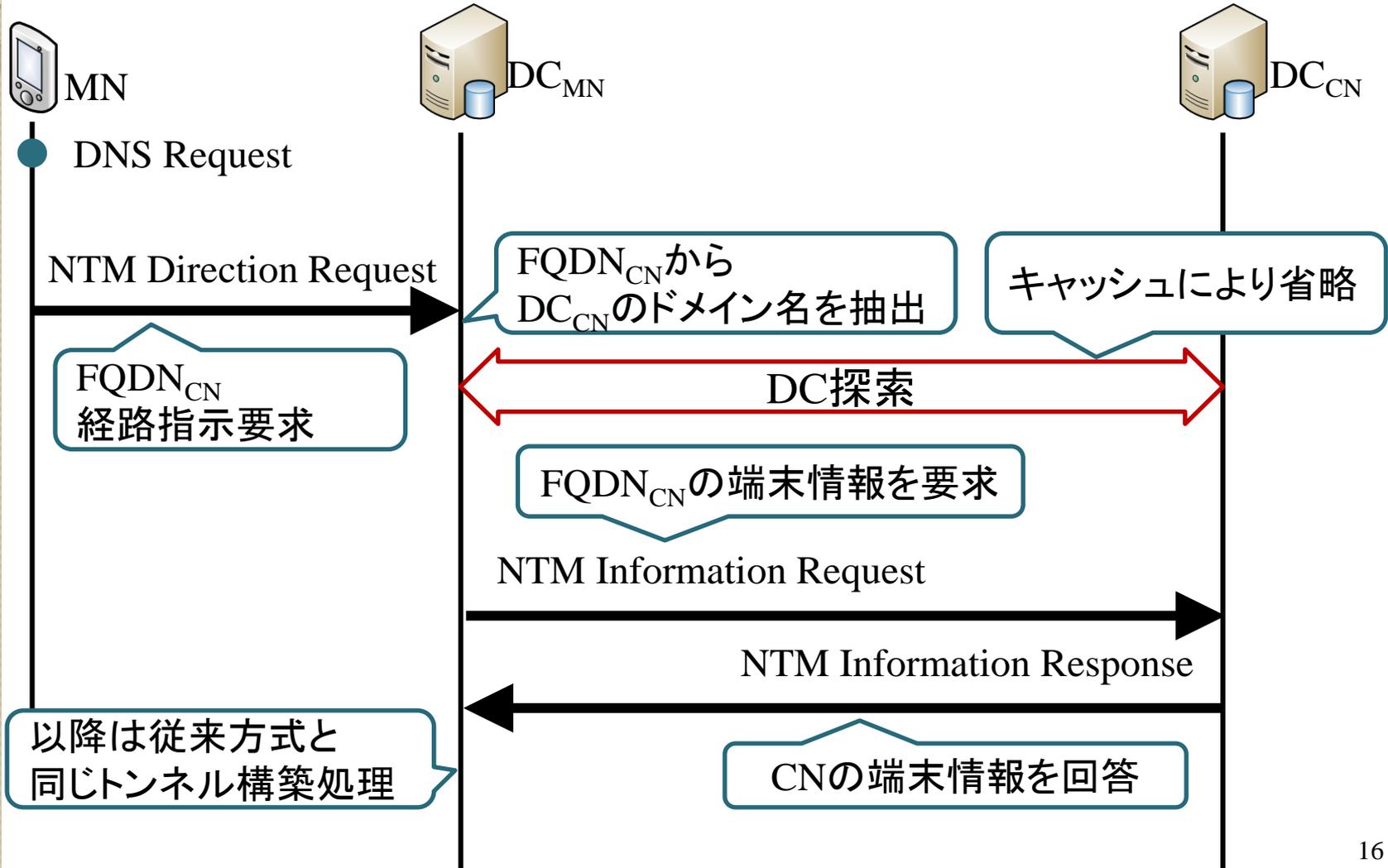


提案方式の通信シーケンス



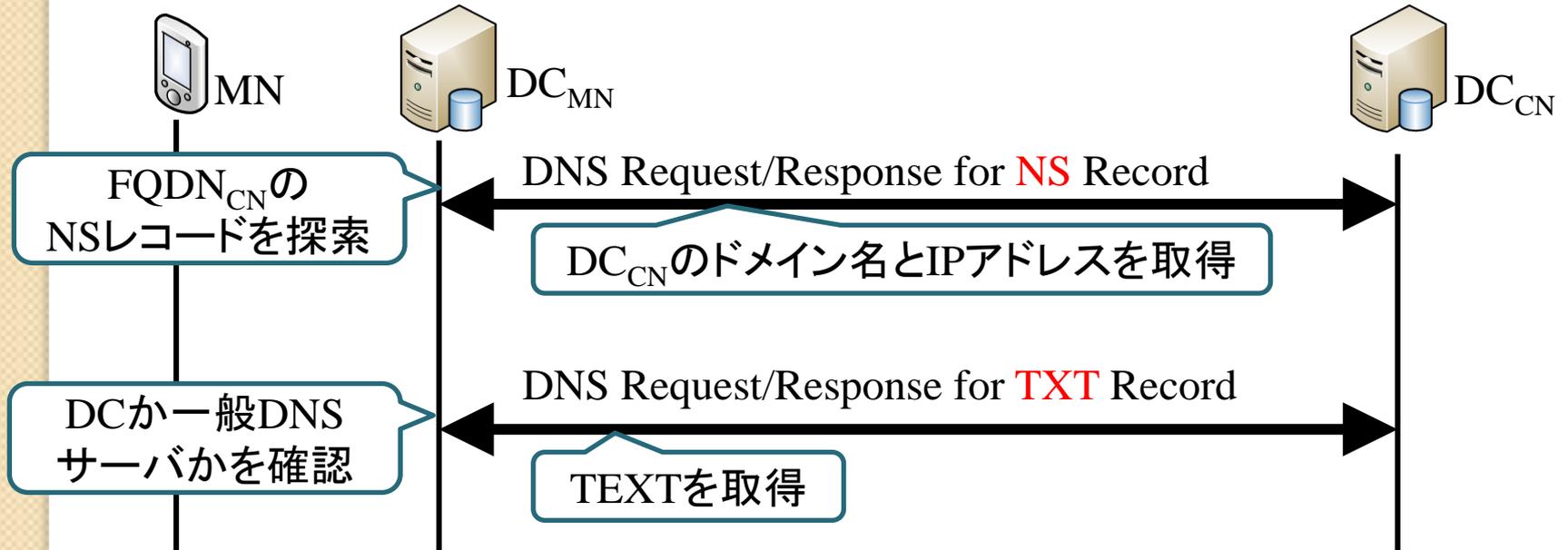
提案シーケンス

- $FQDN_{CN}$ を載せてトンネル構築指示を依頼
- DCのIPアドレスはキャッシュに残しておく



DCの探索方法

- NSレコードを利用してDC_{CN}を探索
- TXTレコードを利用してDCと一般DNSを判断
 - 情報収集方法を切り替え



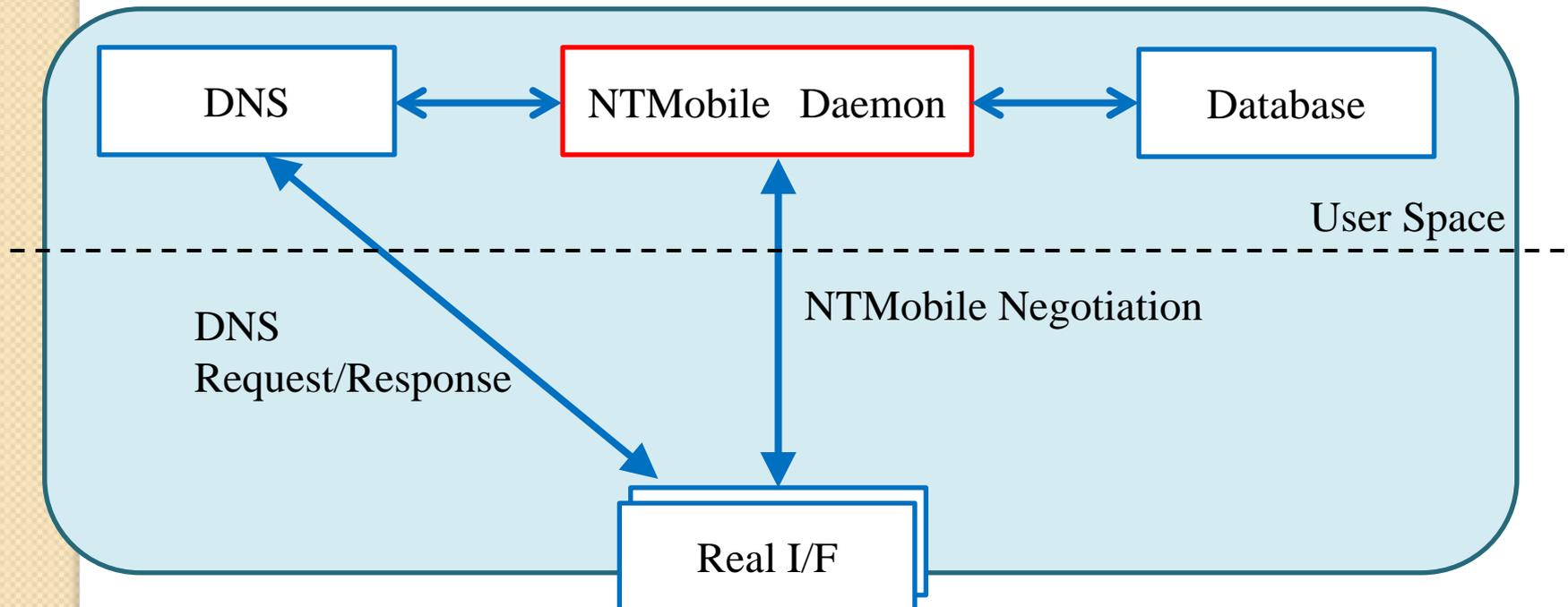
- NSレコード:ドメインを管理するDNSサーバの情報
- TXTレコード:任意の文字列を設定可能



○ **提案方式の実装と評価**

実装

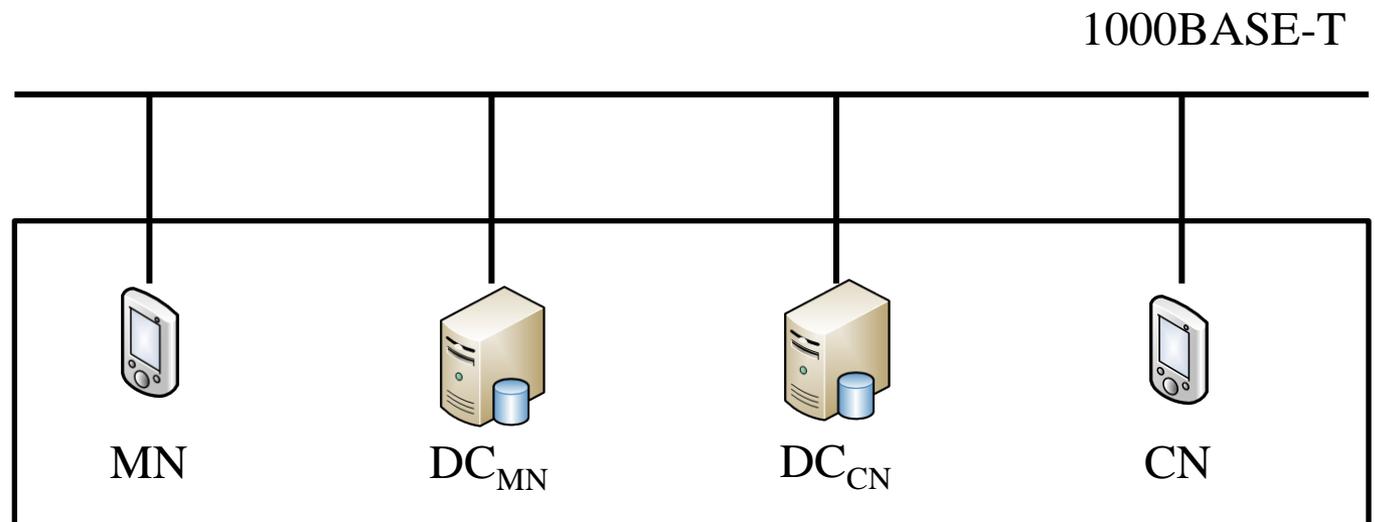
- DCのモジュール構成
 - デーモンプログラム
 - NTMobileのネゴシエーション処理を行う
 - データベース (Mysql 5.1)
 - DNS (Bind 9)



動作検証

- 仮想マシンによる測定環境
 - ネゴシエーションによるオーバヘッドの測定
- ネゴシエーションの時間は
50.6ms (10回の平均値)

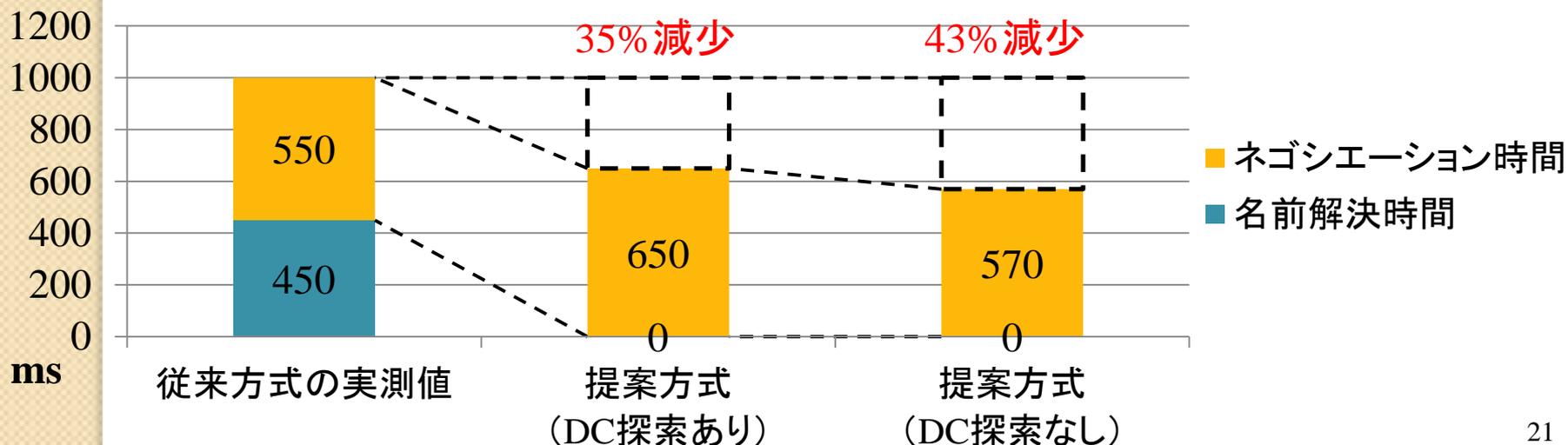
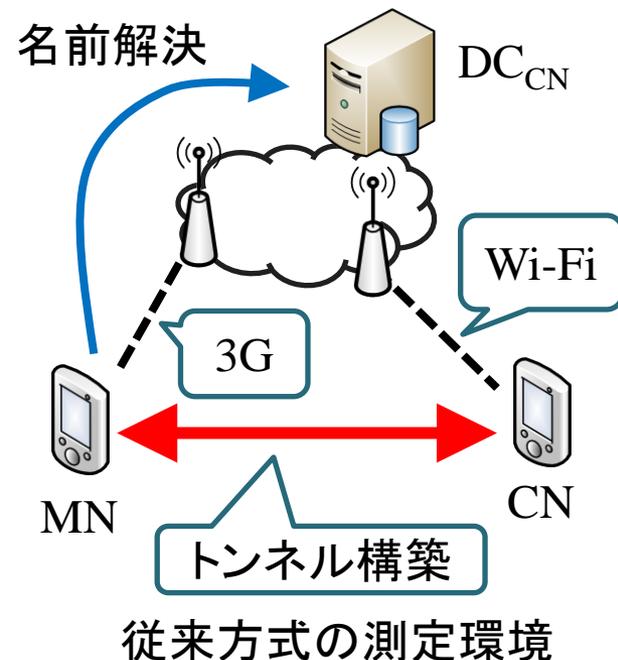
平均RTT:
MN-MN : 0.36ms
DC_{MN}-DC_{CN} : 0.36ms
MN-DC_{MN} : 0.35ms
CN-DC_{CN} : 0.39ms



実環境における予測

- 従来方式の実測値は合計1秒
 - 名前解決時間: 450ms (3G環境)
- 提案方式における予測値
 - 名前解決時間は0
 - 端末情報取得に20ms増加
 - DCの探索に最大80ms増加

※国内の一般的なRTT: 20ms



比較

	DNSレコードを用いる方式	提案方式
通信開始の確実性	✕ DNSキャッシュの影響を受ける	○ DNSキャッシュの影響を受けない
通信開始のオーバーヘッド	△ 通信遅延の影響が大きい	○ 通信遅延の影響が小さい
端末情報管理の柔軟性	△ テキストによる画一的な端末情報管理	○ データベースにより柔軟性と拡張性を確保
NTM端末情報の秘匿性	△ 誰でもNTMレコードを取得可能	○ NTMobileネゴシエーションに対してのみ提供

まとめ

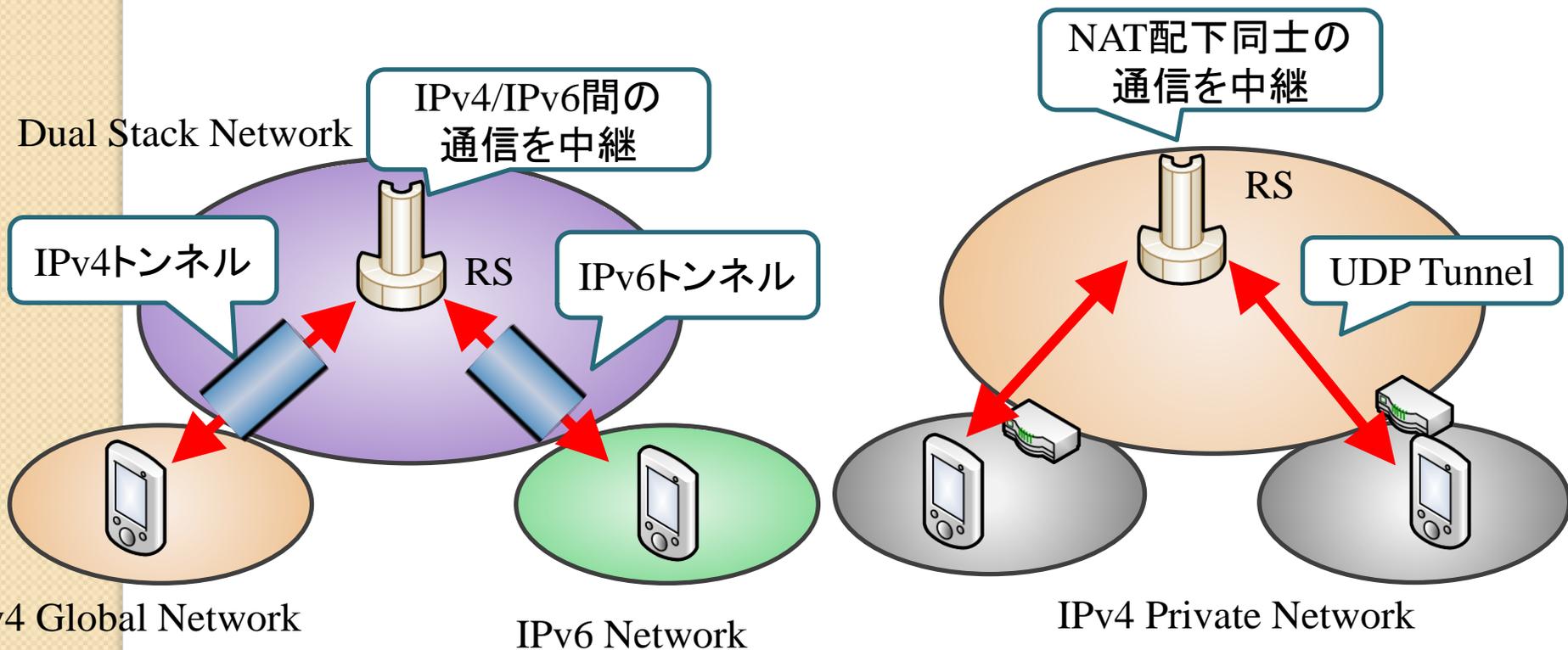
- NTMobile
 - IPv4/IPv6混在環境で通信接続性と移動透過性を実現
- 提案方式
 - DNS依存による制約を排除
 - 情報管理をデータベースへ移行
 - 端末情報管理の柔軟性と拡張性を確保
 - 端末情報の秘匿性確保
 - 通信開始時のオーバヘッドを削減
- 今後の予定
 - 提案方式の実環境における有用性の検証

ご清聴ありがとうございました

補足資料

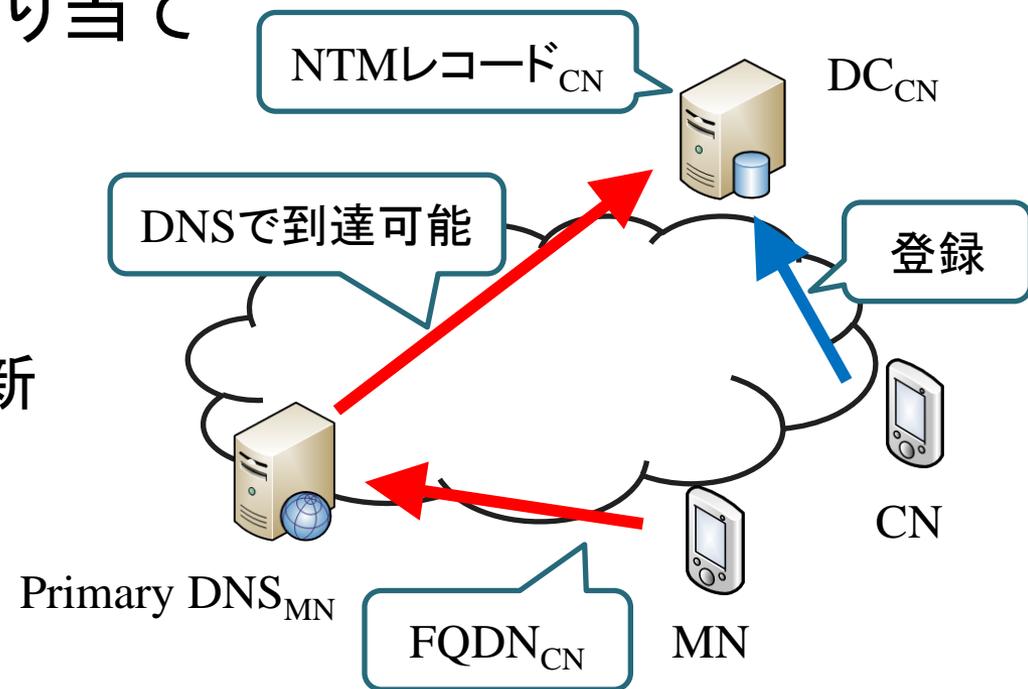
NTMobileの概要

- IPv4とIPv6をまたがる通信
- NAT配下同士の通信
 - NATの種類によっては直接通信に切り替え



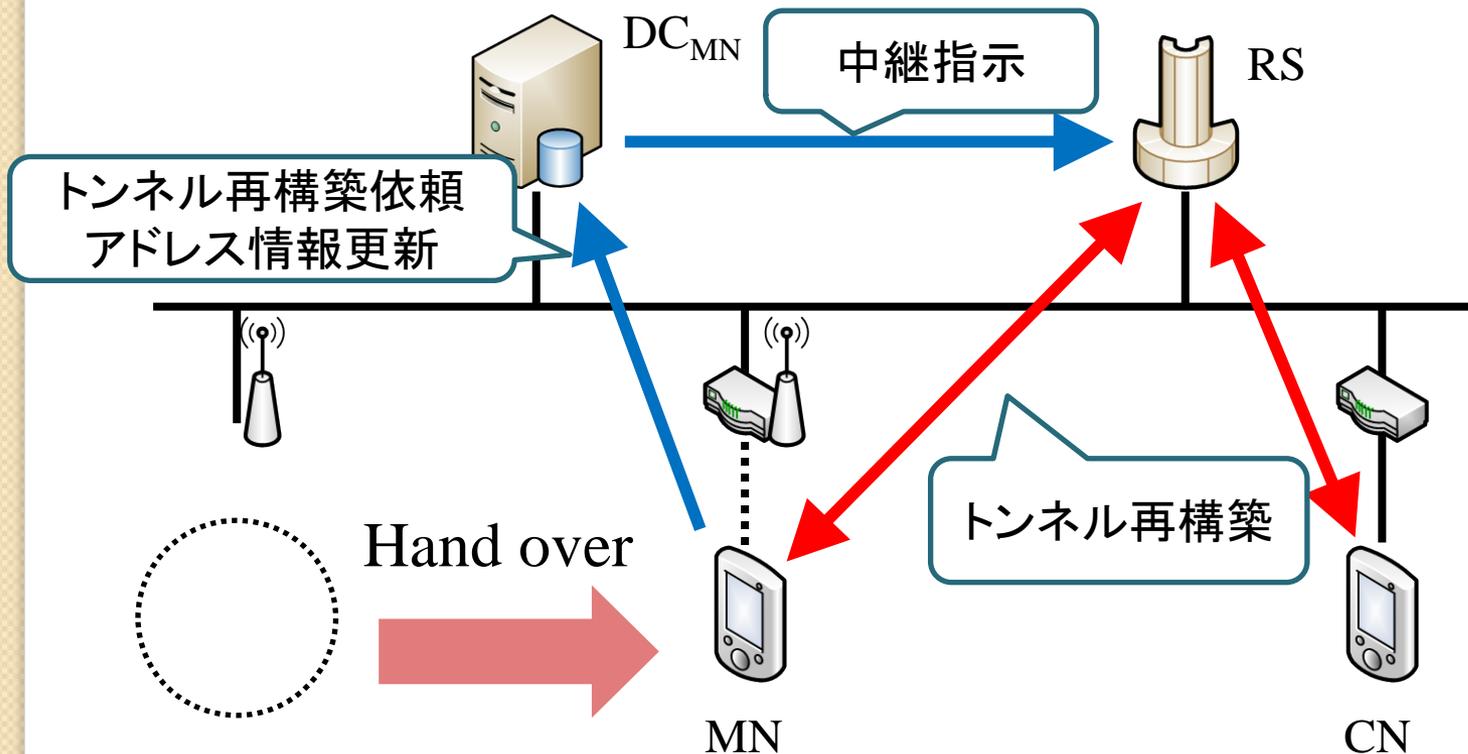
DCの役割

- DDNS (Dynamic DNS)
 - DNSの仕組みで到達可能
- FQDN登録
- 仮想IPアドレス割り当て
- 端末情報管理
 - NTLMレコード
 - DNSレコード形式
 - 実IPアドレスを更新
- 経路判断・指示



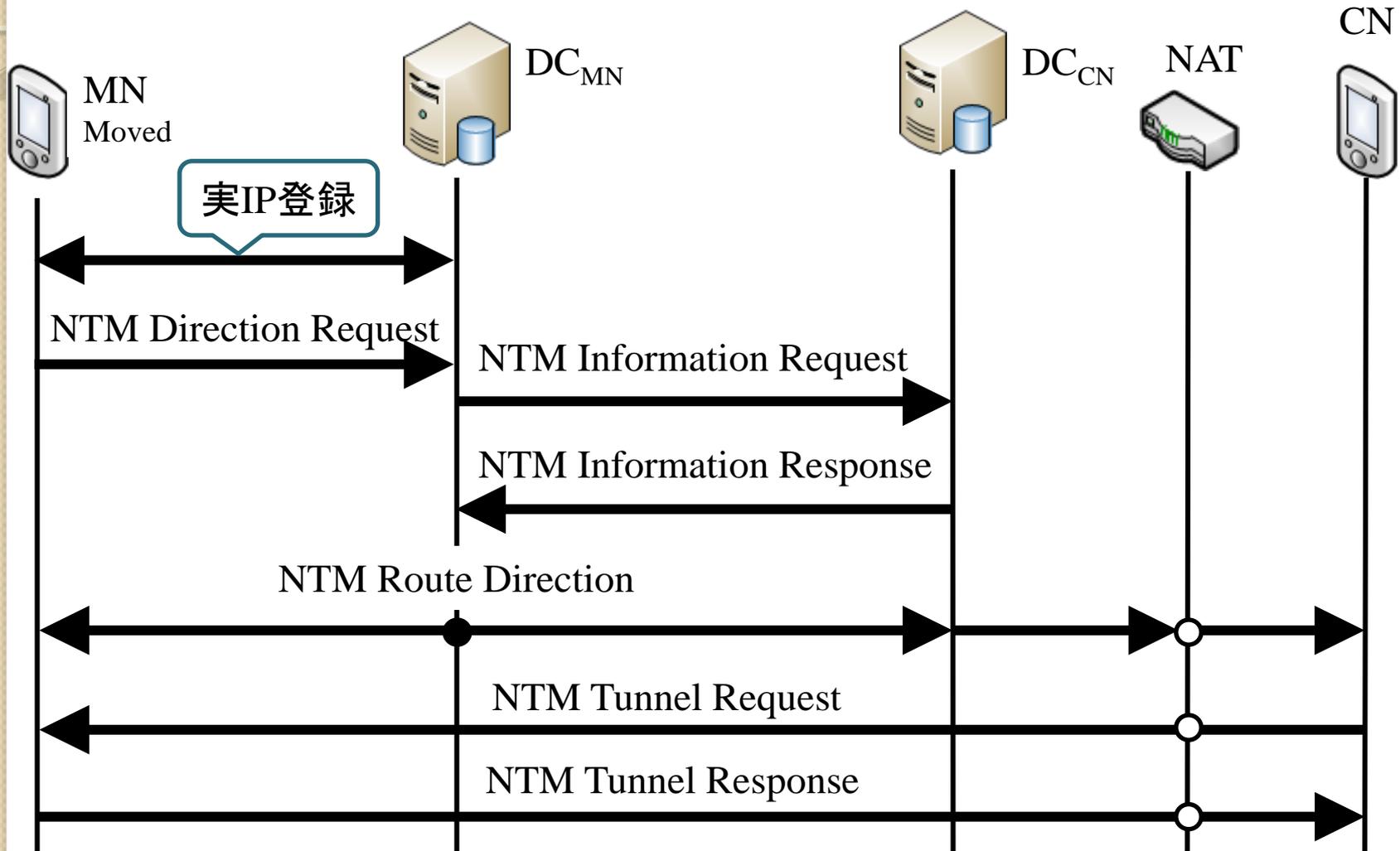
ハンドオーバー時

- MN-CN通信中にMNがNAT配下へ移動
- RS経由のトンネルを再構築



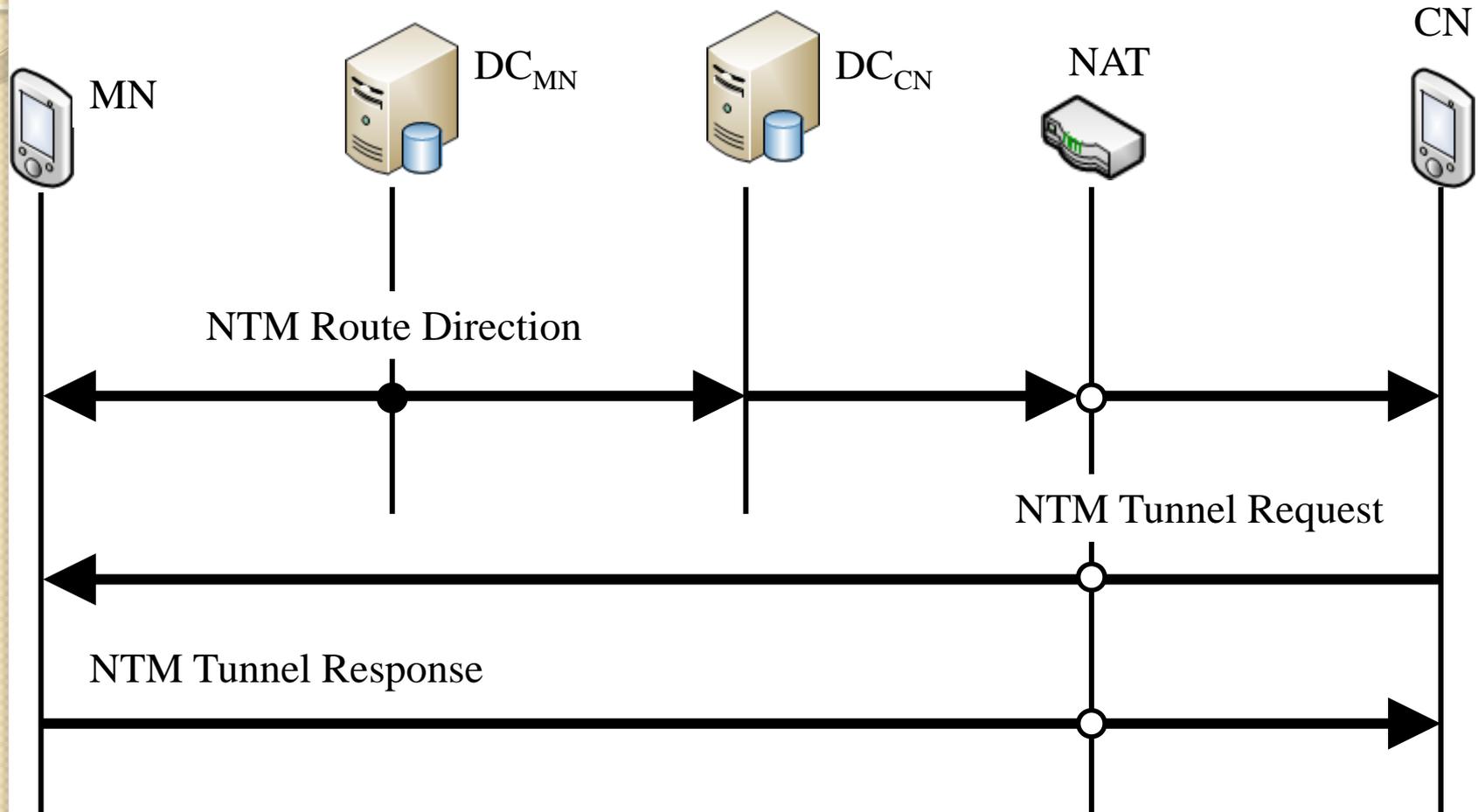
ハンドオーバー時

- 移動後の実IPアドレスを更新してトンネル再構築



通信シーケンス

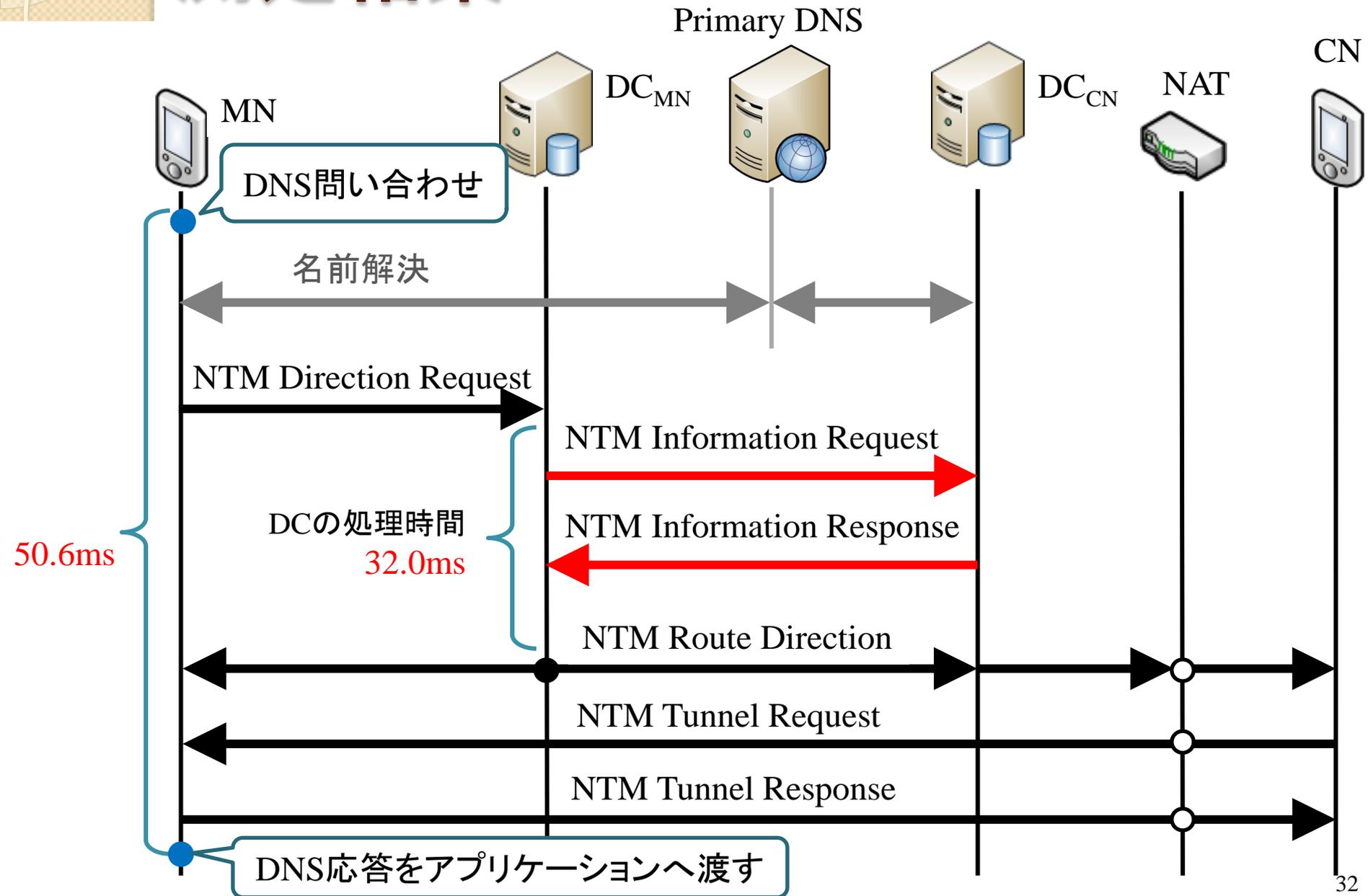
- トンネルの指示・構築は従来と同様



データベース

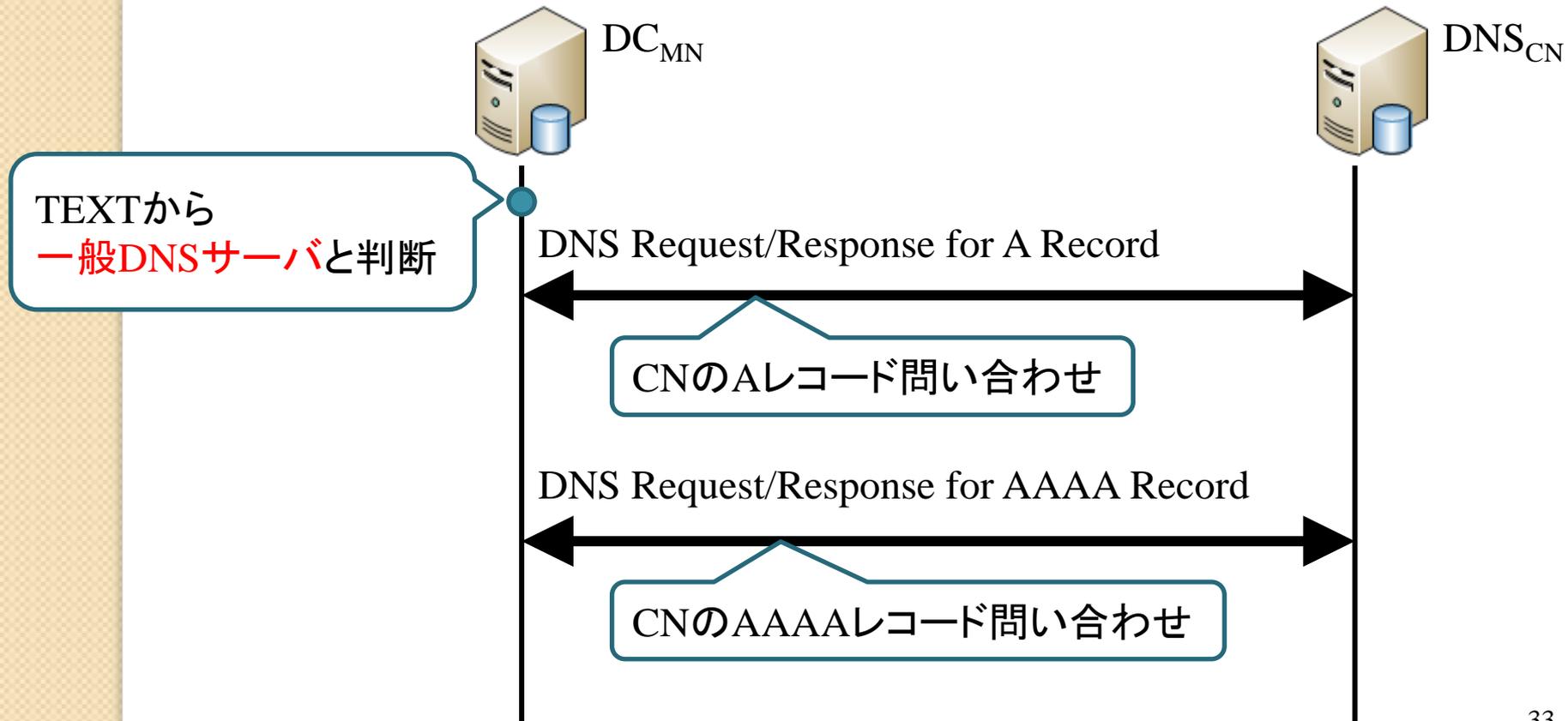
- NTMLレコード情報をデータベースに格納
- Node Informationテーブル
 - NTM端末情報を管理
- DCキャッシュ
 - ドメインごとのDNSに関する情報を管理
 - CNのFQDNから管理しているDNSを特定
 - DNSのNTM Mobile対応状況を管理
 - 直ちに端末情報を取得可能

測定結果



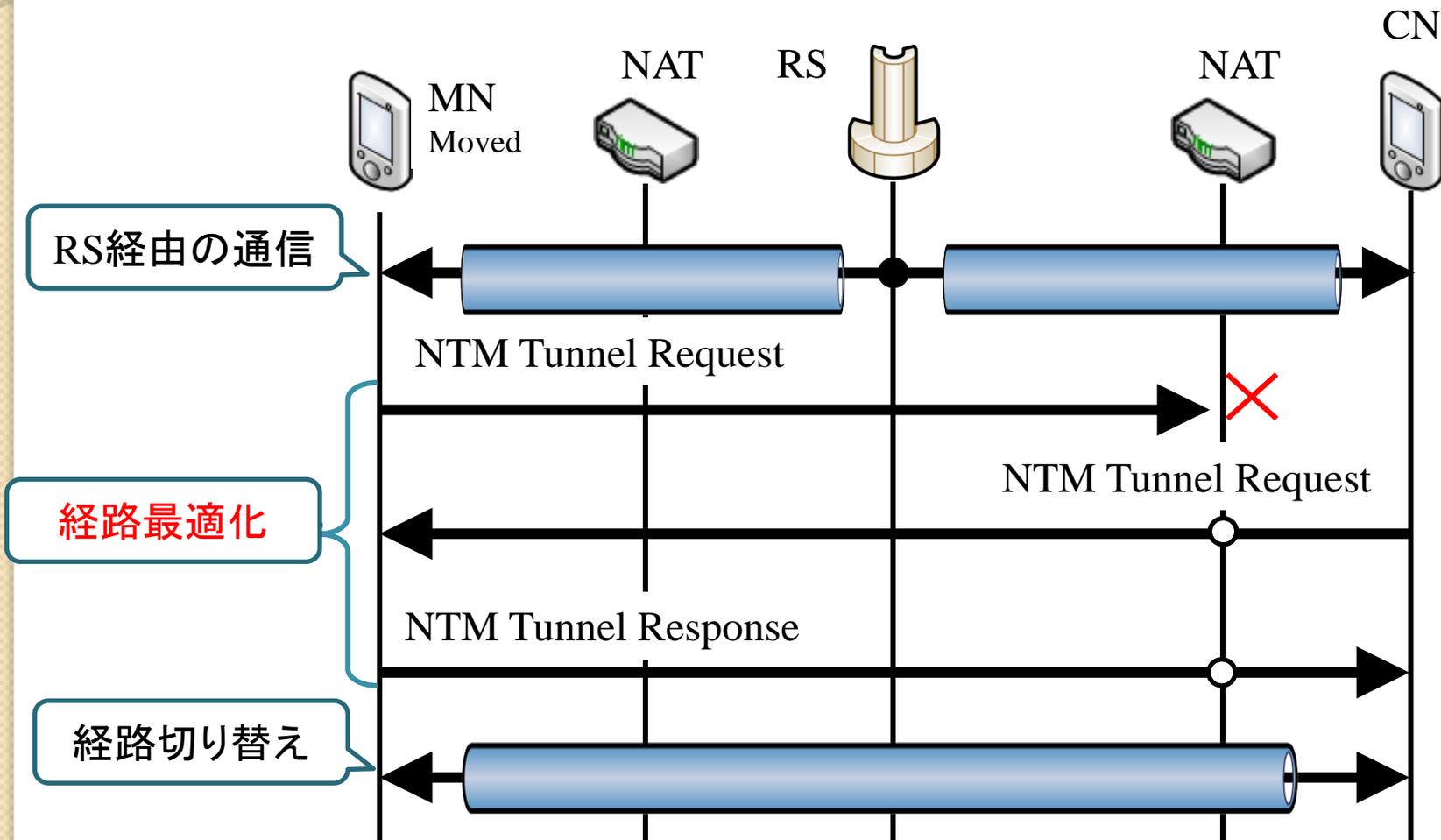
一般のDNSサーバへの対応

- 通信相手のDNSが一般DNSサーバの場合
- 直接A, AAAAレコードを問い合わせる



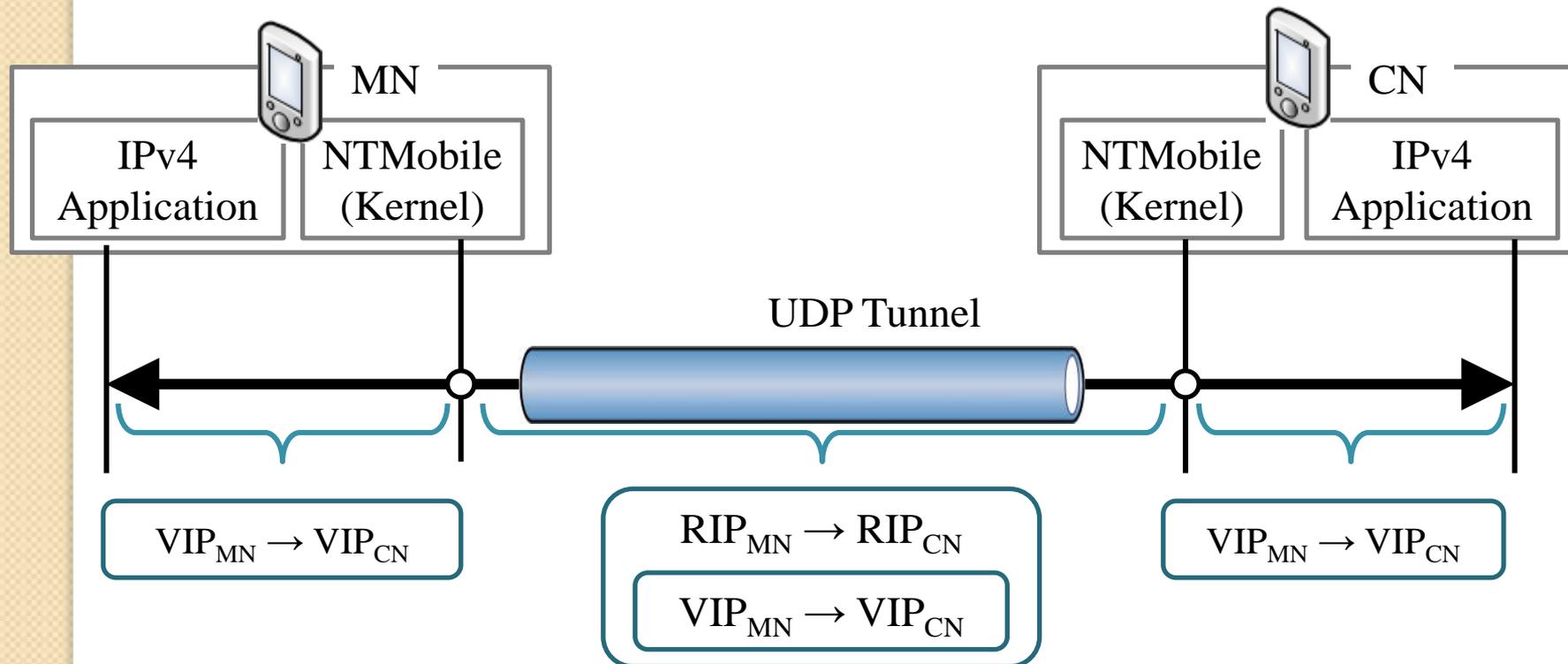
経路最適化

- RS経由の通信と並行して実行
- NATの種類に依存
- 異なるNAT配下端末同士でE2E通信



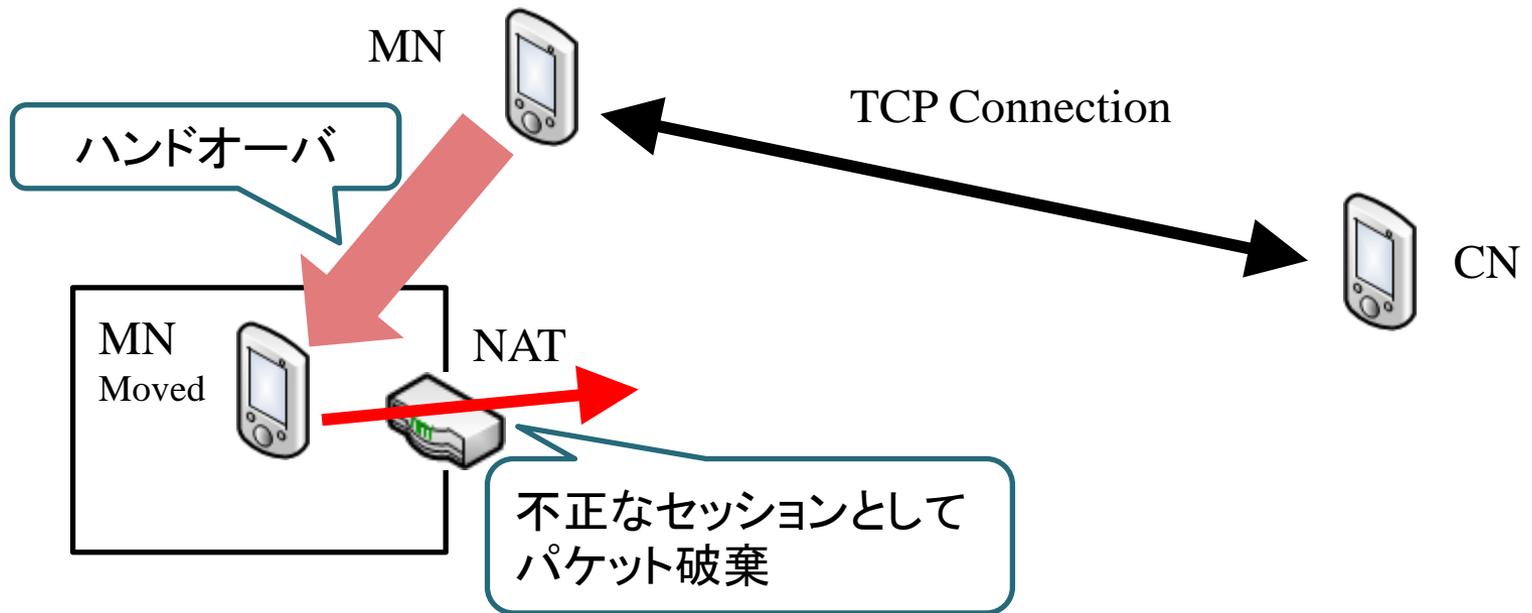
トンネル通信詳細

- アプリケーションは仮想IPアドレスを使用
- アプリケーションパケットの暗号化



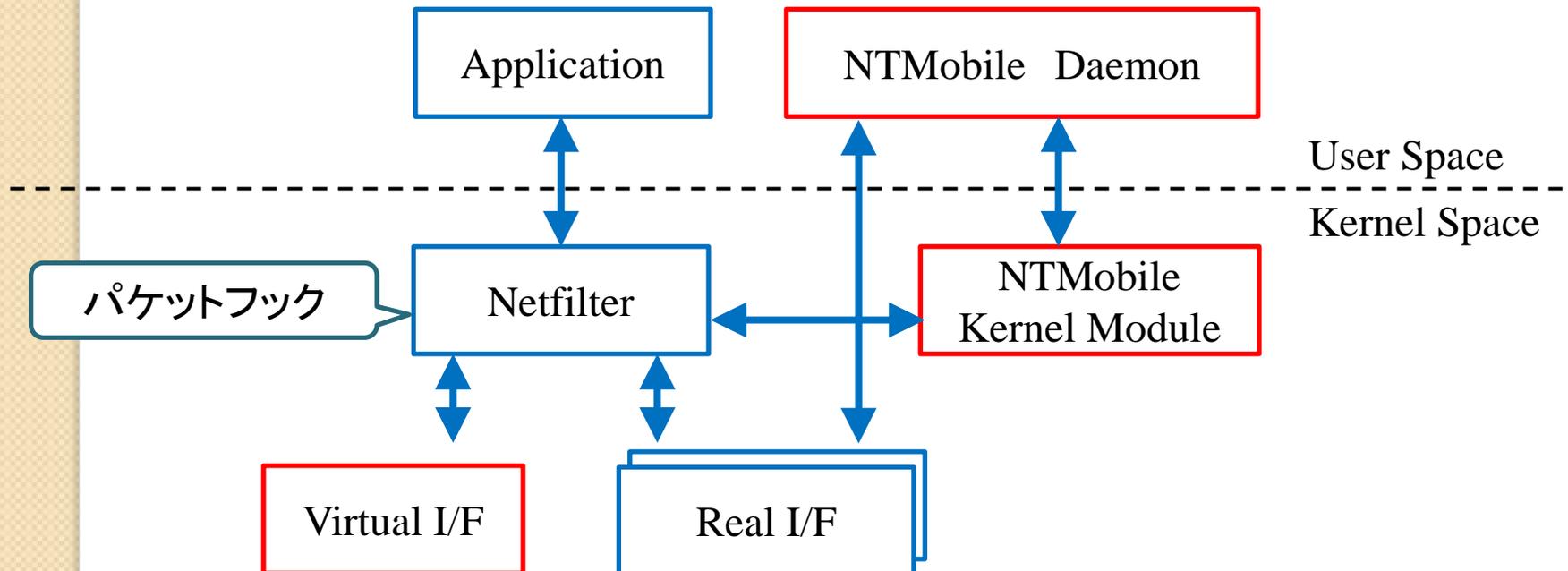
SPI (Stateful Packet Inspection)

- TCPのセッションを監視するフィルタ
- 多くのNATに搭載
- NATを跨った移動時にパケット破棄の問題
 - NTMobileではUDPトンネルを用いて解決



NTM端末のモジュール構成

- デーモンプログラム
 - トンネル構築などのネゴシエーション
 - NetlinkによりL2ハンドオーバ, IPアドレス変化を検知
- カーネルモジュール
 - カプセル化・暗号化



NTMレコード

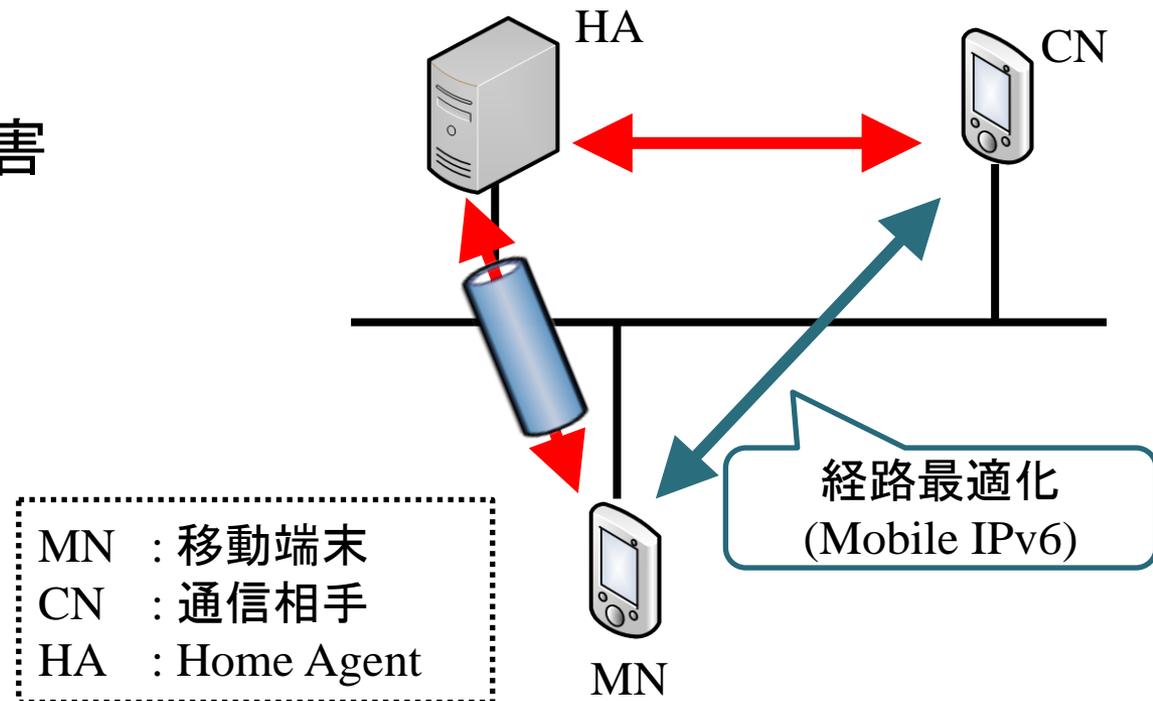
- IPv4用のNTM4レコードとIPv6用のNTM6レコード
- Node ID
 - NTM端末を一意に識別するID
- 仮想IPアドレス (IPv4/IPv6)
 - DCが重複なくNTM端末に割り当てる
- 実IPアドレス (IPv4/IPv6)
 - NTM端末が接続ネットワークから取得
 - NTM端末のIPアドレス変化に伴い動的に更新
- NATの外側の実IPアドレス (IPv4/IPv6)
 - プライベートアドレス空間への接続を識別
- DCのIPアドレス (IPv4/IPv6)
 - NTM Route Directionの転送に使用

NTMobileとDSMIPの機能比較

- IPv6ネットワークにおいて同様の機能
 - 移動透過性
 - 経路最適化
- IPv4ネットワークにおけるNTMobileの優位性
 - 経路最適化に対応
 - 管理, 中継装置の多重化に対応
- NATが混在する環境におけるNTMobile
 - グローバルIPv4アドレスは必ずしも必要ではない
 - NATの改造は不要
 - DSMIPではどちらかに対応が必要

類似研究

- DSMIP(Dual Stack Mobile IPv6)
 - IPv4/IPv6混在環境において移動透過性を実現
 - HA経由によりCNに対してMNの移動を隠蔽
 - IPv4における課題
 - 経路最適化
 - HAの一点障害



NTMobileの想定アプリケーション

- NTMobileはエンドツーエンド通信を実現
 - サーバ転送を必要としないリアルタイム性
 - 通話, 動画, チャット, ゲーム
 - ホームネットワークへの接続が容易
 - ファイル管理系コンテンツ
 - コンテンツ提供者のサーバ管理不要なサービス
 - ネットワークサービスへの参入が容易に

ハンドオーバー処理の最適化

- 最新実IPアドレスの更新処理を省略

