NTMobileにおけるグループ認証方式の提案と実装

103430037 村橋 孝謙
渡邊研究室

1. はじめに

近年のユビキタスネットワークの進展に伴い，IPv4/IPv6などのネットワーク環境に影響されない通信接続性や端末の通信中の移動を可能とする移動透過性が重要となる．さらにエンド端末間の認証と暗号化はセキュリティ確保の上で重要である．

このような状況を考え，我々は通信の接続性や移動透過性を満たすNTMobile（Network Traversal with Mobility）[1]を提案している．NTMobileはトンネル技術と仮想アドレスを用いることでネットワークの移動透過性と接続性を同時に実現可能とする技術である．しかし，NTMobileは通信の制約を除去するのが目的であり，エンド端末間のセキュリティは別途考える必要がある．

エンド端末間のセキュリティを確保する技術として，IPsecがある．強固なセキュリティを確保することができる反面，NATとの相性が悪い，移動透過性への対応が難しいなどの課題がある．IPsecの課題を解決するための技術として，我々はGSCIP（Grouping for Secure Communication for IP）を提案してきた．GSCIPは通信グループと通信に必要な暗号鍵を一対一に対応付けることによりセキュリティの確保と柔軟な通信グループ構築を可能とするがNATが介在すると実現が困難という課題がある．

そこでNTMobileにおいてアクセス制御リストACL（Access Control List）を用いたグループ単位の認証を行い，認証結果に応じて通信可否を決定する方法を提案する．通信開始時にACLから両エンド端末の所属グループを検索し，同一のグループに所属していることが判明すればNTMobileの処理を続行する．提案方式を実装し，その有効性を確認した．

2. 既存技術と課題

2.1 IPsec

IPsecは暗号化と認証によりIPパケットを安全に運ぶための技術である．IPsecはIP層で動作するプロトコルのため，アプリケーションは特にセキュリティを意識することなく安全な通信を行うことが可能である．IPsecで使用されるセキュリティプロトコルESP（Encapsulating Security Payload）ではIPパケットの暗号化が可能であり，IKE（Internet Key Exchange）と組み合わせて使用することでパケットの改ざんに対する検知も可能である．

しかしESPによりパケットの暗号化を行う場合，NAPTを通過することができない．またIPsecトランスポートモードを使用する際は全ての通信ペアについて設定を行う必要があるため，IPsec適用端末の増加に伴い管理負荷が指数関数的に増大する問題がある．グループ単位に管理する場合トンネルモードを使用することができるが，ゲートウェイ単位に設定を行うためユーザ毎に異なる設定を行うなど柔軟な設定ができない．

2.2 GSCIP

GSCIPは，グループ名と暗号鍵を一対一に対応付けることにより管理者が容易に通信グループの定義を行うことができる技術である．GSCIPでは通信グループの定義はIPアドレスに依存しないため，端末が移動してシステム構成が変化した場合でも，グループ構成の再定義が不要である．IPsecでは難しかった端末単位およびドメイン単位の混在の混在した通信グループの構築が容易に実現できる．GSCIPでは，同一グループ間の通信はグループ鍵GKを用いた認証と暗号化が行われる．

GSCIPは容易な通信グループの定義を可能とするが，NAT超え問題と移動透過性問題を同時に解決することは難しい．独自のNAT超え技術NAT-fを利用することによりNAT超え問題を解決する方式があるが，既存のNATを改造する必要がある．また移動透過性についてはMobilePPCと呼ぶ独自の技術を用いることで解決することができるが，NAT超え問題を解決することができない．

3. NTMobile

NTMobileはトンネル技術と仮想IPアドレスを用いることでNATの使用やIPアドレスの変化に影響しない通信を可能とする技術である．図1にNTMobileの概要を示す．アプリケーションが通信を行う際には仮想IPアドレスを用い，実際の通信は実IPアドレスによるカプセル化を行う．実アドレスが変化してもアプリケーションはIPアドレスの変化を意識することなく通信を行うことができる．両エンド端末がNAT配下に存在する場合はRS（Relay Server）を中継することによりグローバル空間・プライベート空間を意識することなく移動することができる．またNTMobileはIPv6にも対応可能であり，IPv4プライベートアドレス，IPv4グローバルアドレス，IPv6アドレスを跨るような移動も可能である．

NTMobileでは端末間の通信接続性および移動透過性を確保することができるが，端末間のアクセス制御の方法までは定義していない．グループ単位のアクセス制御を実現することで，よりセキュリティの強度を高めることができる．

4. グループ制御方式の実現

NTMobileにてエンド端末間のセキュリティを実現するため，グループ単位でのアクセス制御を行う方式を提案する．提案方式では各NTMobile端末はそれぞれ定義された通信グループに所属し，両エンド端末が同一の通信グルー

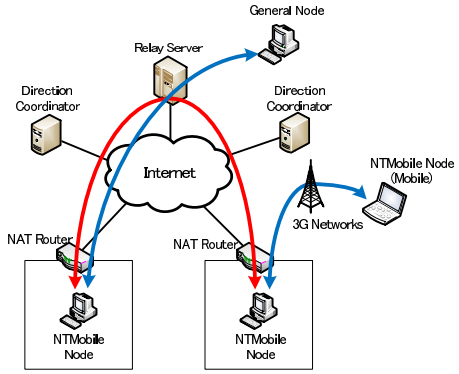


図 1: NTMobileの概要

プに所属している場合のみコネクションを確立させることができる．

図 2ACL を用いた通信シーケンスを示す．各 DC は，NTMobile 端末のノード ID，所属グループ番号などから成る ACL(Access Control List) と呼ばれるデータベースを持つ．通信開始側 DC が Direction Request を受信すると，通信相手側 DC へ両端末のノード ID からなるアクセスチェック要求 Access Check Request を送信する．通信相手側 DC はこれを受信すると ACL から両端末の所属グループを検索し，所属グループの一致確認（Access Check）を行う．Access Check が終了すると，その結果を Access Check Response として通信開始側 DC へ返す．

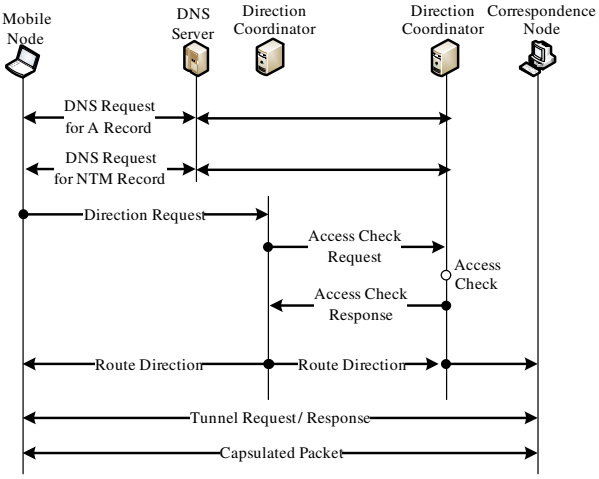


図 2: ACL を用いた通信シーケンス

5. 評価

5.1 既存技術との比較

IPsec/ESP を使用した場合，GSCIP を使用した場合および ACL を適用した NTMobile について機能比較を行った．比較結果を表 1 に示す．

- パケットの機密性
  IPsec において ESP を使用し暗号化を行った場合，暗号化範囲は TCP/UDP ヘッダを含むペイロード部分となる．また GSCIP では TCP/UDP ヘッダを含まないペイロード部分，NTMobile では NTM ヘッダと MAC 値を除くペイロード部分が暗号化される．GSCIP および NTMobile では，TCP/UDP ヘッダの暗号化が不可能なためトラフィック解析の危険性がある．
- 多対多通信の管理負荷
  IPsec トンネルモードでは管理が比較的容易であるが，個人単位に細かな設定を行うことができない．IPsec トランスポートモードではきめ細かい設定ができるが，管理が煩雑である．GSCIP および NTMobile では個人単位またはグループ単位の通信制御を柔軟に行うことができる．
- NAT への対応
  NAT の存在する環境では，IPsec の使用が困難である．GSCIP において NAT 越えを行うためには NAT を改造する必要がある．それに対し NTMobile では NAT に係わる制約が一切無存在しない．
- 移動透過性
  IPsec では通信端末を識別するために IP アドレスを使用しているため，端末がネットワークを移動して IP アドレスが変化した場合には通信を継続することができない．GSCIP ではグループ鍵で通信グループを管理しているため，端末がネットワークを移動したでも通信を行うことができる．ただし GSCIP 単体では NAT を経由する移動には対応しない．NTMobile ではどのようなネットワーク環境であっても移動透過性を実現できる．

表 1: 機能比較結果

	IPsec	GSCIP	NTMobile(ACL)
機密性	◎	○	○
多対多通信の管理負荷	△	◎	◎
NAT への対応	△	△	◎
移動透過性	×	○	◎

NTMobile では IPsec ほど強固なセキュリティを得ることはできないが，NAT や通信環境に依存しない通信が可能なため広範囲での運用が可能である．

5.2 性能評価

一方のエンド端末が NAT 配下，他方のエンド端末がグローバルアドレス空間に存在する場合の端末間のネゴシエーションによるオーバヘッドを測定した．その結果，全体で 24.521ms を要し，そのうち本提案により実装を行ったアクセスチェック関係処理には 12.368ms を要した．アクセスチェック関係処理にて増加するオーバヘッドはわずかな値であり，実用上の影響はないと考えられる．

6. まとめ

本稿では移動透過性と接続性を実現する NTMobile にグループ制御方式を加えた方式の概要を説明し，その評価を行った．アクセス制御リストを用いることでグループ単位のアクセス制御を行うことができる．これにより NTMobile をより安全なシステムとすることができた．また特定のネットワークにおいて動作検証と性能測定を行った結果，追加される機能に対しオーバーヘッドは実用上問題のない程度となることを確認した．

参考文献

[1] 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，pp. 1349–1359 (2011).

NTMobileにおけるグループ認証方式の提案と実装

名城大学大学院　理工学研究科　情報工学専攻
渡邊研究室　103430037　村橋　孝謙

研究背景

- 通信接続性の需要
  - IPv6移行の停滞から，今後はIPv4/IPv6は共存
  - IPv4プライベート/グローバル共存環境でも
    自由に通信を行いたい

通信接続性

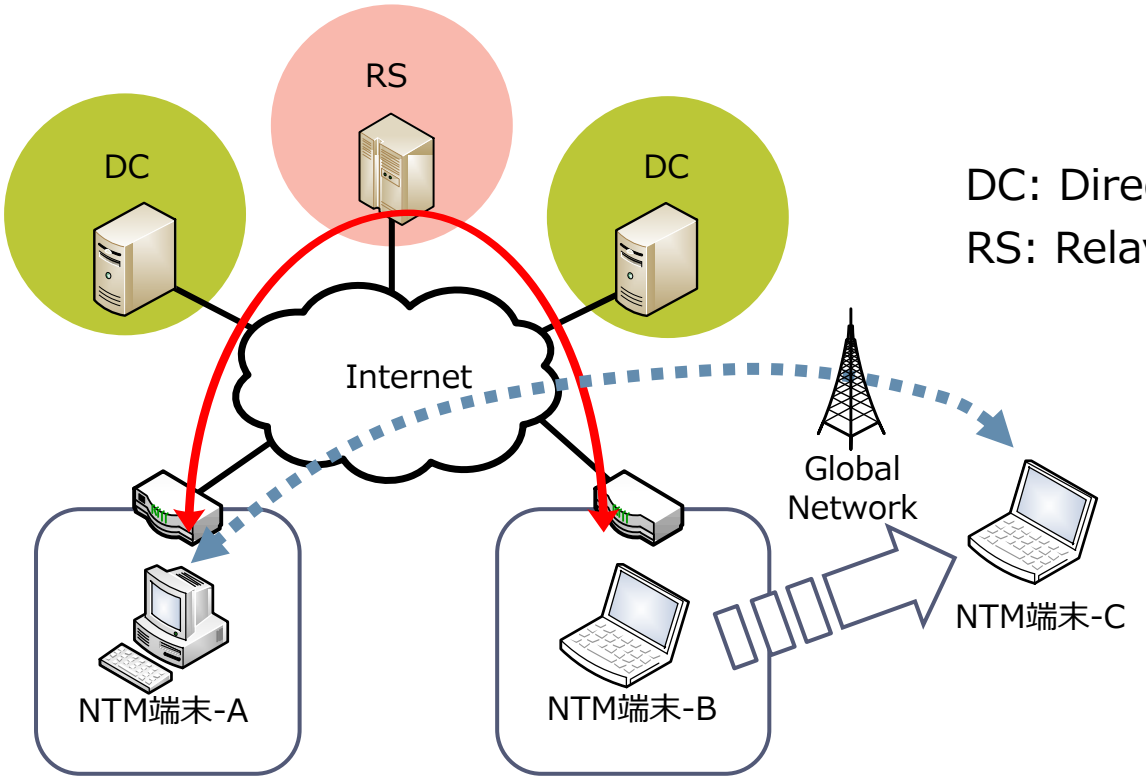
- 移動通信の需要
  - 複数無線I/F搭載
  - 通信中のネットワーク切り替え時にも通信を継続したい

移動透過性

NTMobile

研究背景（NTMobile）

- 仮想IPアドレス，トンネル技術を使用
  - アプリケーションは仮想IPアドレスを使用した通信
  - 実際の通信は実IPアドレスでトンネル通信



DC: Direction Coordinator
RS: Relay Server

NTMobileへの要求

- エンドエンドの確実な認証
  - 情報漏洩の危険
  - 社内サーバの保護など
- セキュリティとアクセス制御を可能とする技術

IPsec　　特徴：強固なセキュリティ

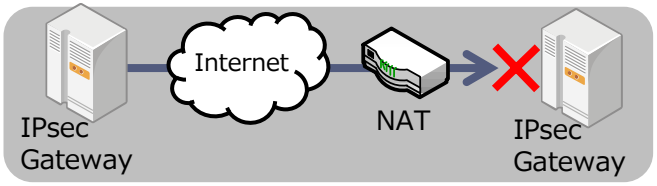
GSCIP　　特徴：柔軟なグルーピング

GSCIP: Grouping for Secure Communication for IP

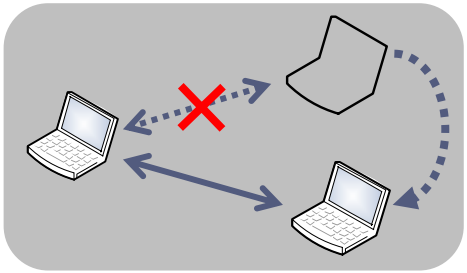
IPsecの課題

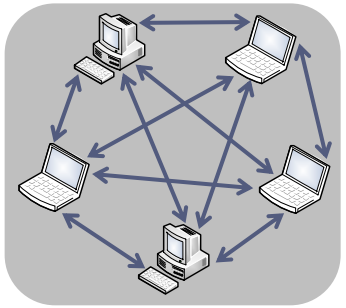
- 暗号化，相手認証など強固なセキュリティ
- NATへの対応　移動透過性　管理負荷 の課題あり

  - NATへの対応　　暗号化のためNATを通過できない
  - 移動透過性　　IPアドレスの変化への対応が難しい
  - 管理負荷　　大規模ネットワークでの管理負荷は巨大



NATへの対応


移動透過性

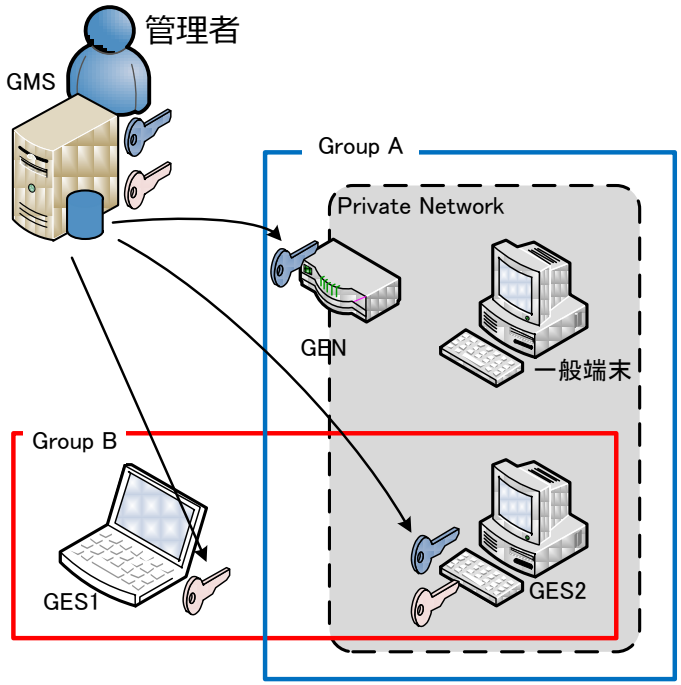

管理負荷

GSCIP

- 通信グループと暗号鍵を１対１に対応
  - 柔軟な通信グループ構築が可能

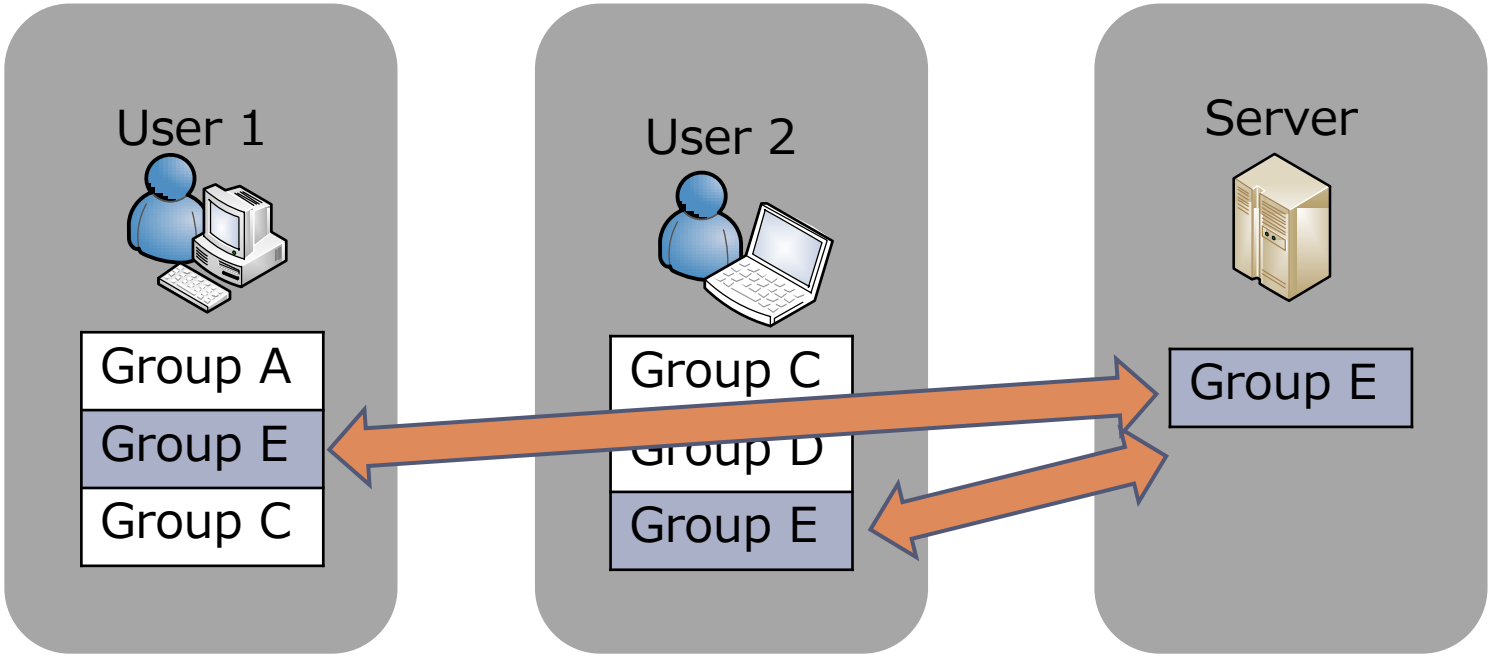
- 新たな管理装置(GMS)が必要
- 管理装置との信頼関係が必要

解決 → NTMobileへ



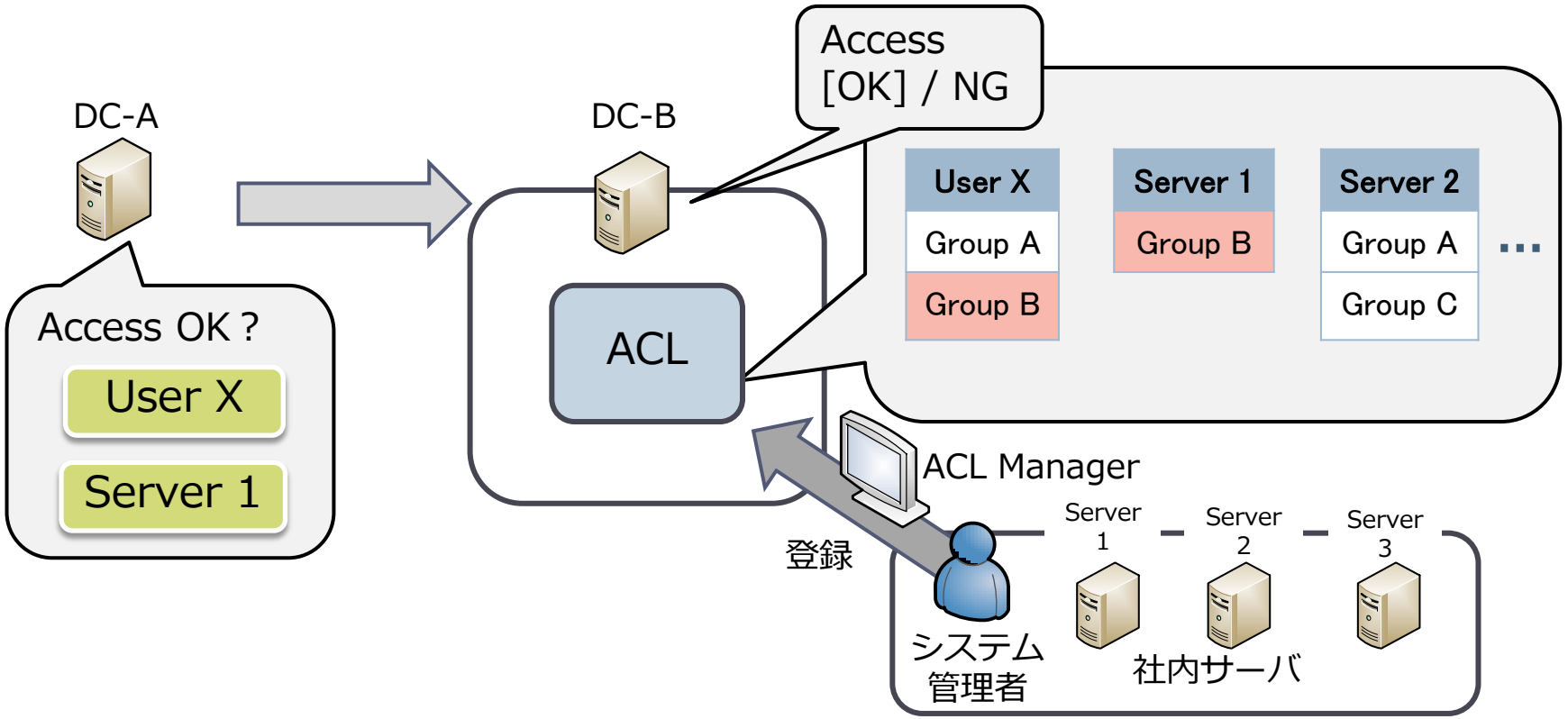
提案方式 (1/2)

- NTMobileにアクセス制御機能を追加
  - 各端末はいずれかのグループに所属
  - 通信時に両エンド端末の所属グループを確認
  - 同一グループ所属のときネゴシエーション処理を継続

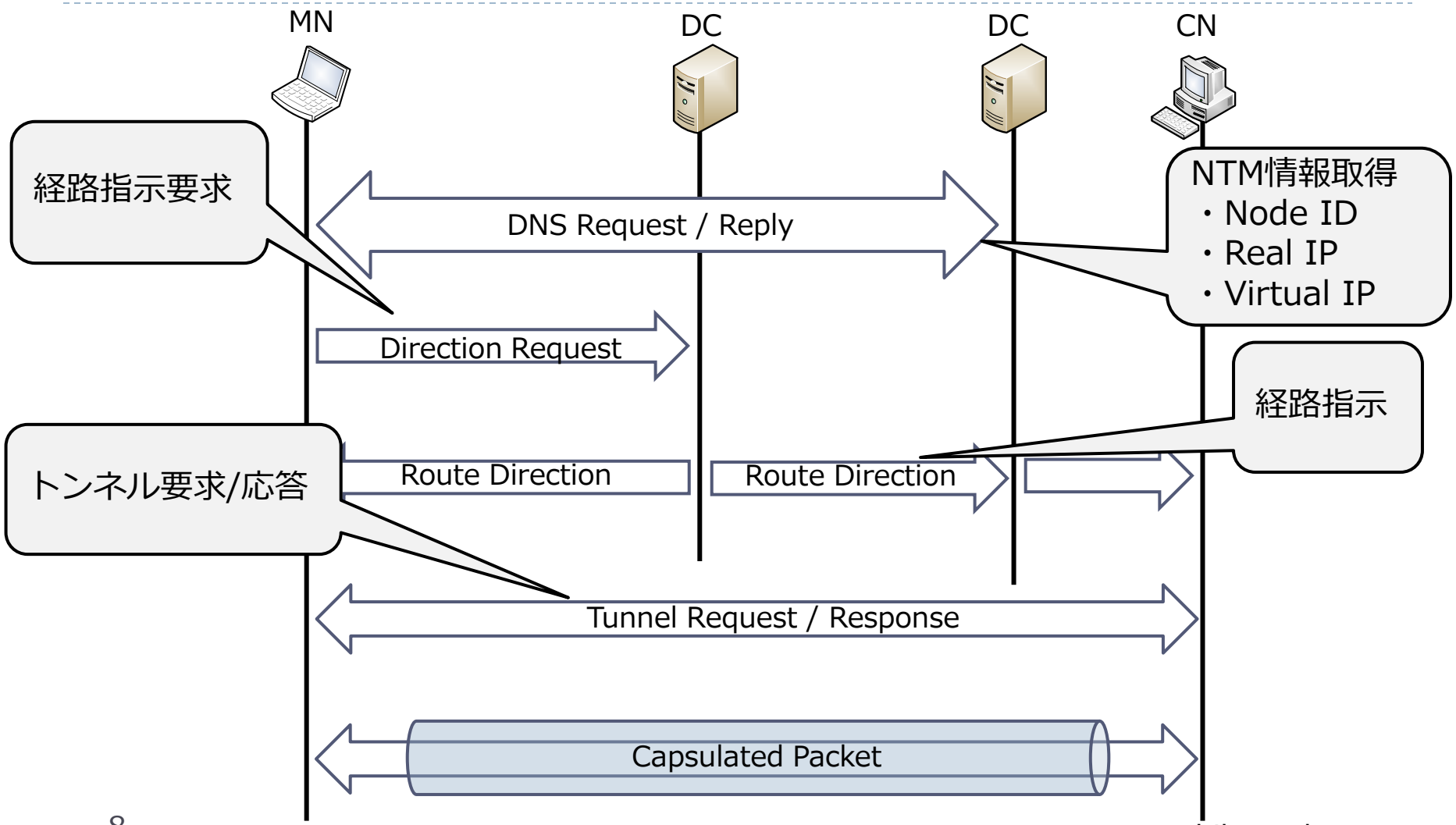


提案方式 (2/2)

- DCにACL(Access Control List)を追加
  - ACL：各ノードのNode ID，所属グループを格納
  - 所属グループの確認・アクセス制御



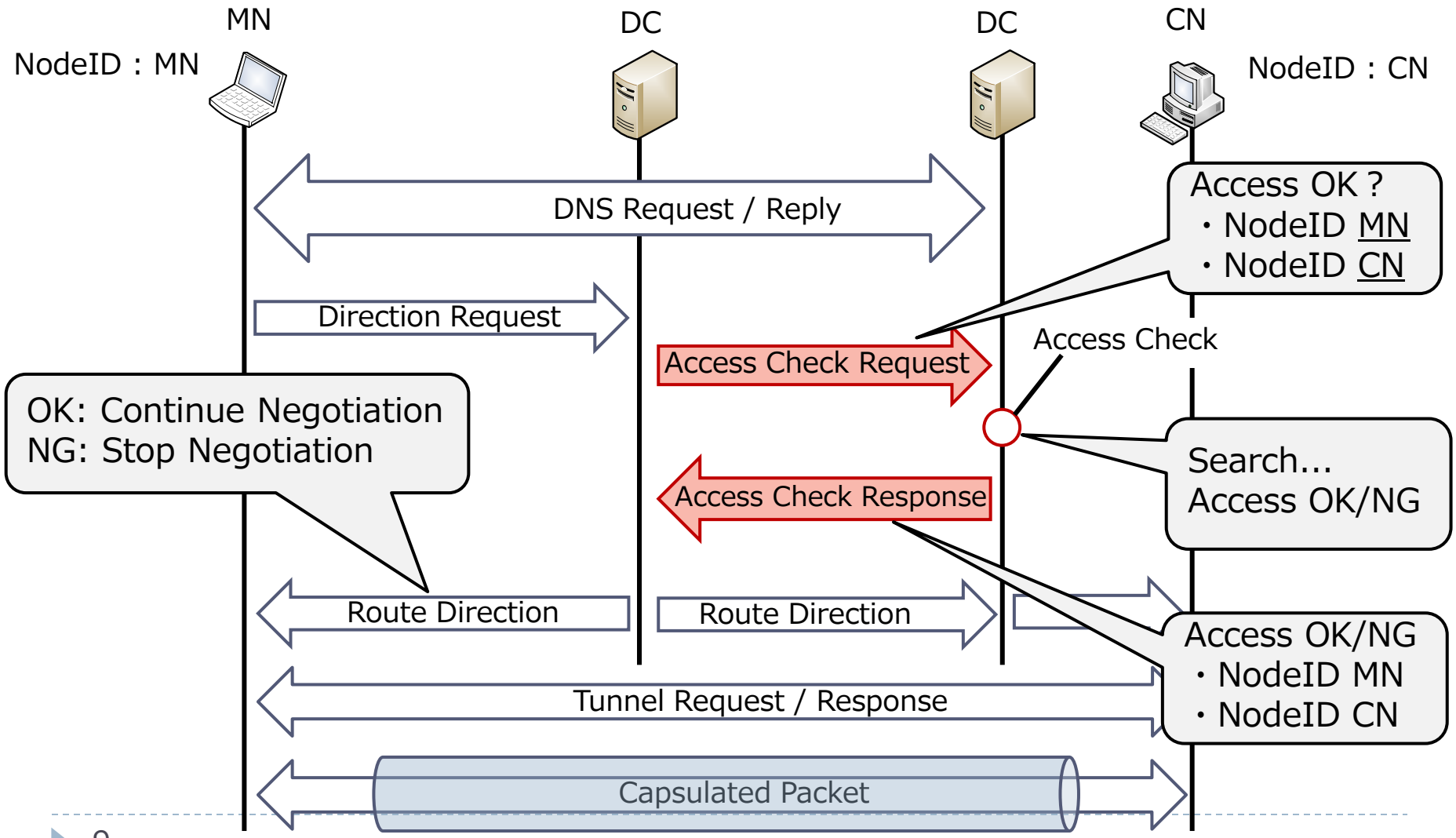
NTMobile (基本動作)



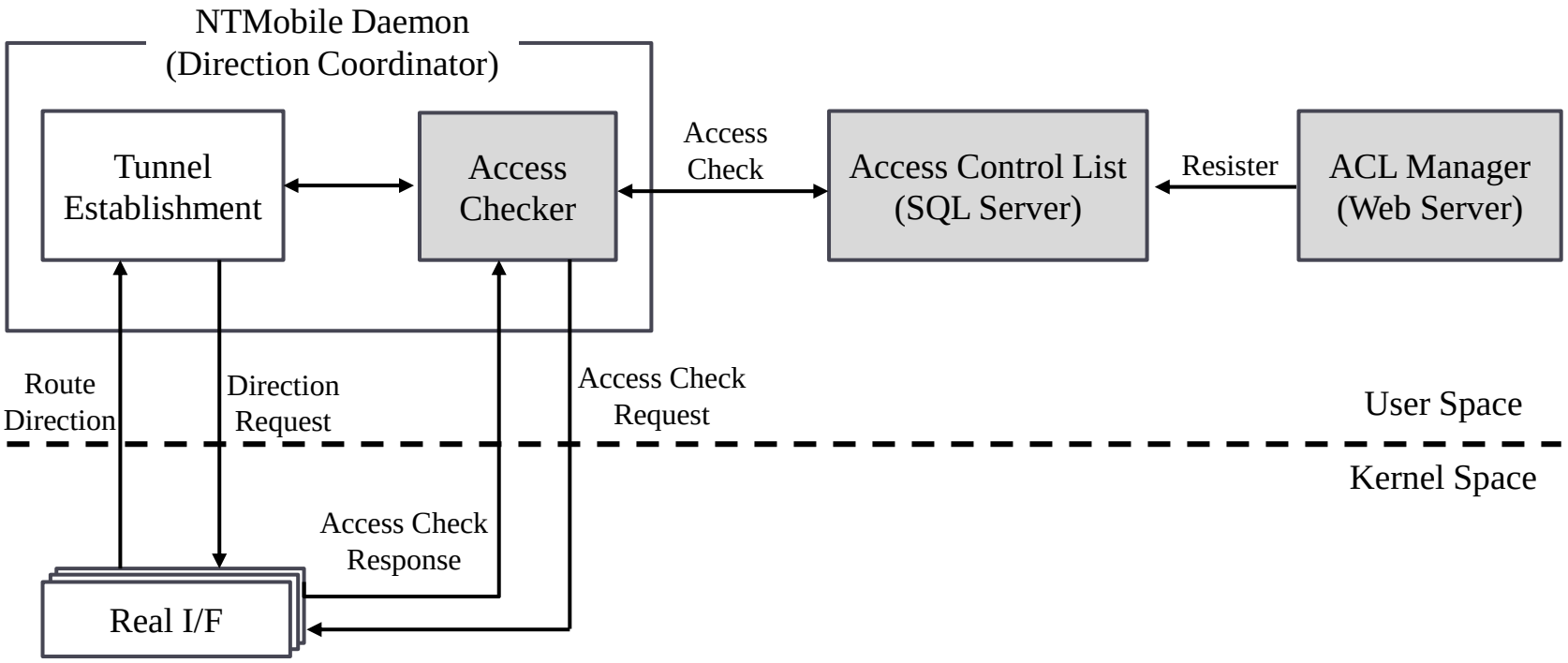
MN: Mobile Node

CN: Correspondence Node

NTMobile (Access Checkによる拡張)



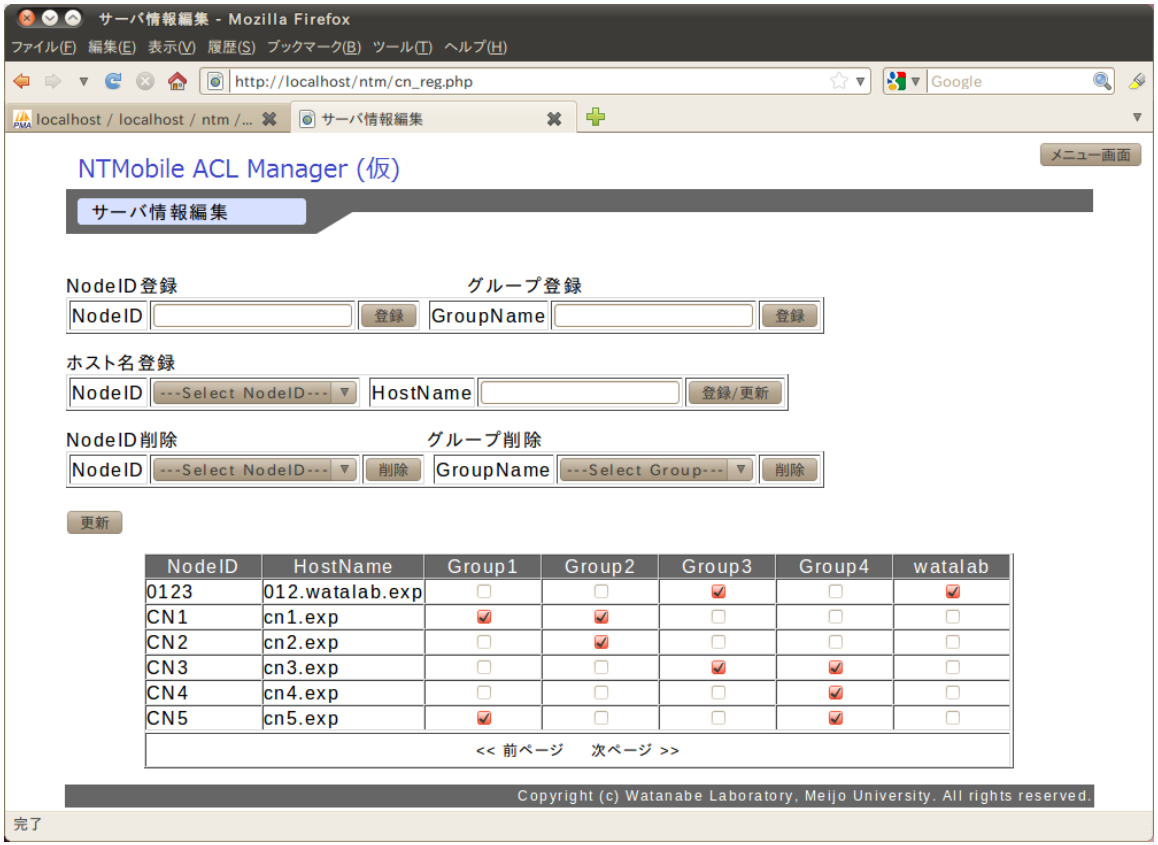
実装概要 (Direction Coordinator)



- DCにAccess Check関係処理を実装
  - NTMobile Daemon内に問合せ要求/応答処理
  - 端末内SQL ServerからAccess Check問合せ
  - ACL Manager(管理画面)から端末情報の登録が可能

管理画面（ACL Manager）

- DC配下端末のグループ登録/編集
- DC配下端末へアクセス可能な端末の情報登録/編集



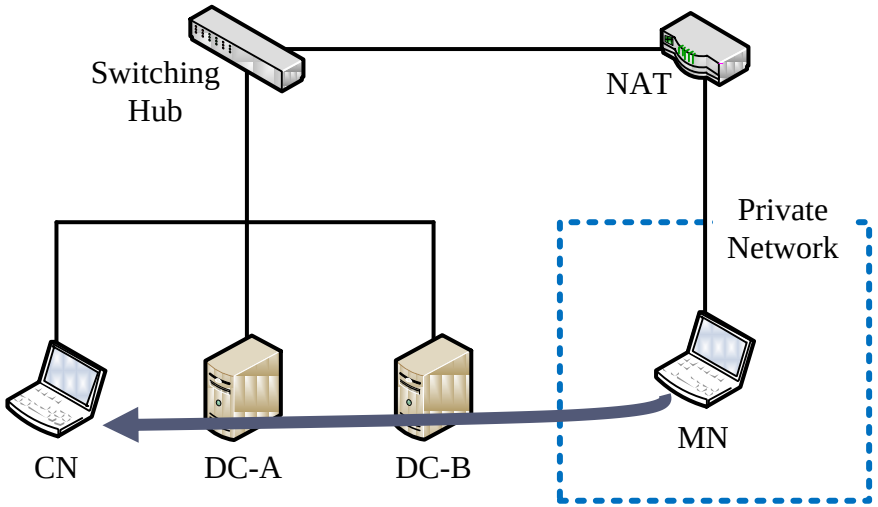
性能測定 （測定方法）

- NTMobileネゴシエーション時間
  - アクセスチェック関係処理に要する時間の測定
  - Wiresharkを利用
  - Access Check自体は処理前後の時刻差分から計算
- プライベート環境下 MN から外部の端末 CN へトンネル構築

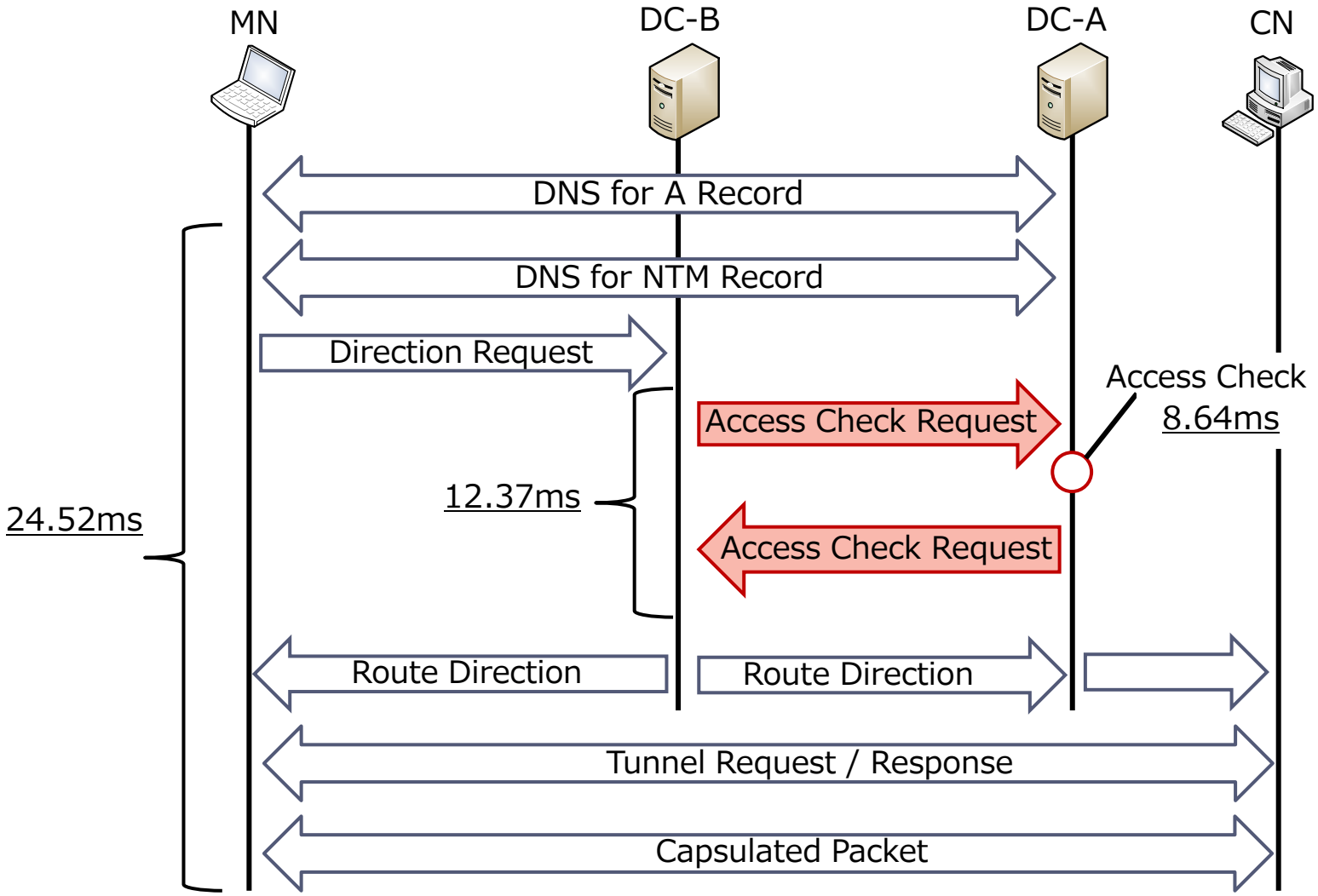
NTM Node (MN, CN)
OS : Ubuntu 10.04
CPU : Core 2 Duo U9400 1.4GHz
Memory : 2048MB
Ethernet : 1000Base-T

Direction Coordinator (DC-A, DC-B)
OS : Ubuntu 10.04
CPU : Core 2 Duo P9400 2.4GHz
Memory : 2048MB
Ethernet : 1000Base-T

Switching Hub, NAT
Ethernet : 100Base-TX



測定結果


MN
DC-B
DC-A
CN
DNS for A Record
DNS for NTM Record
Direction Request
Access Check Request
Access Check
8.64ms
12.37ms
24.52ms
Access Check Request
Route Direction
Route Direction
Tunnel Request / Response
Capsulated Packet

まとめ

- アクセス制御を追加したNTMobileの概要

- アクセス制御方法
  - DC内にACLを構築
  - 同一グループ所属のときネゴシエーション完了へ

- 実装・測定
  - グルーピングによるアクセス制御の実現
  - 追加機能に対し僅かなオーバヘッド

機能比較

	IPsec(ESP)	GSCIP	NTMobile	NTMobile(ACL)
機密性	◎	○	○	○
グループ認証	○	◎	×	◎
NAT	△	△	◎	◎
移動透過性	△	○	◎	◎

環境に依存しない通信

グループ単位のアクセス制御

必要十分なセキュリティ

社内向けなど
情報漏洩の抑制などに適当

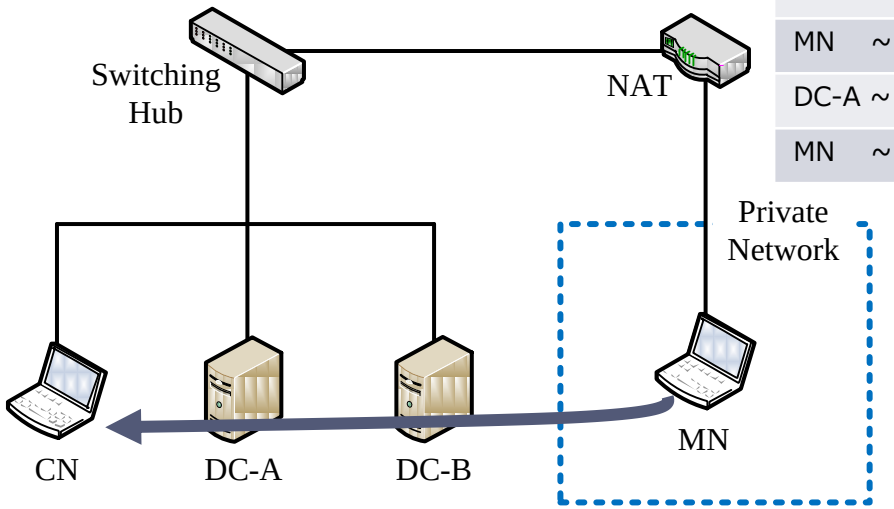
性能測定　（測定方法）

- NTMobileネゴシエーション時間
  - アクセスチェック関係処理に要する時間の測定
  - Wiresharkを利用
  - Access Check自体は処理前後の時刻差分から計算
- プライベート環境下 MN から外部の端末 CN へトンネル構築

NTM Node (MN, CN)
OS : Ubuntu 10.04
CPU : Core 2 Duo U9400 1.4GHz
Memory : 2048MB
Ethernet : 1000Base-T

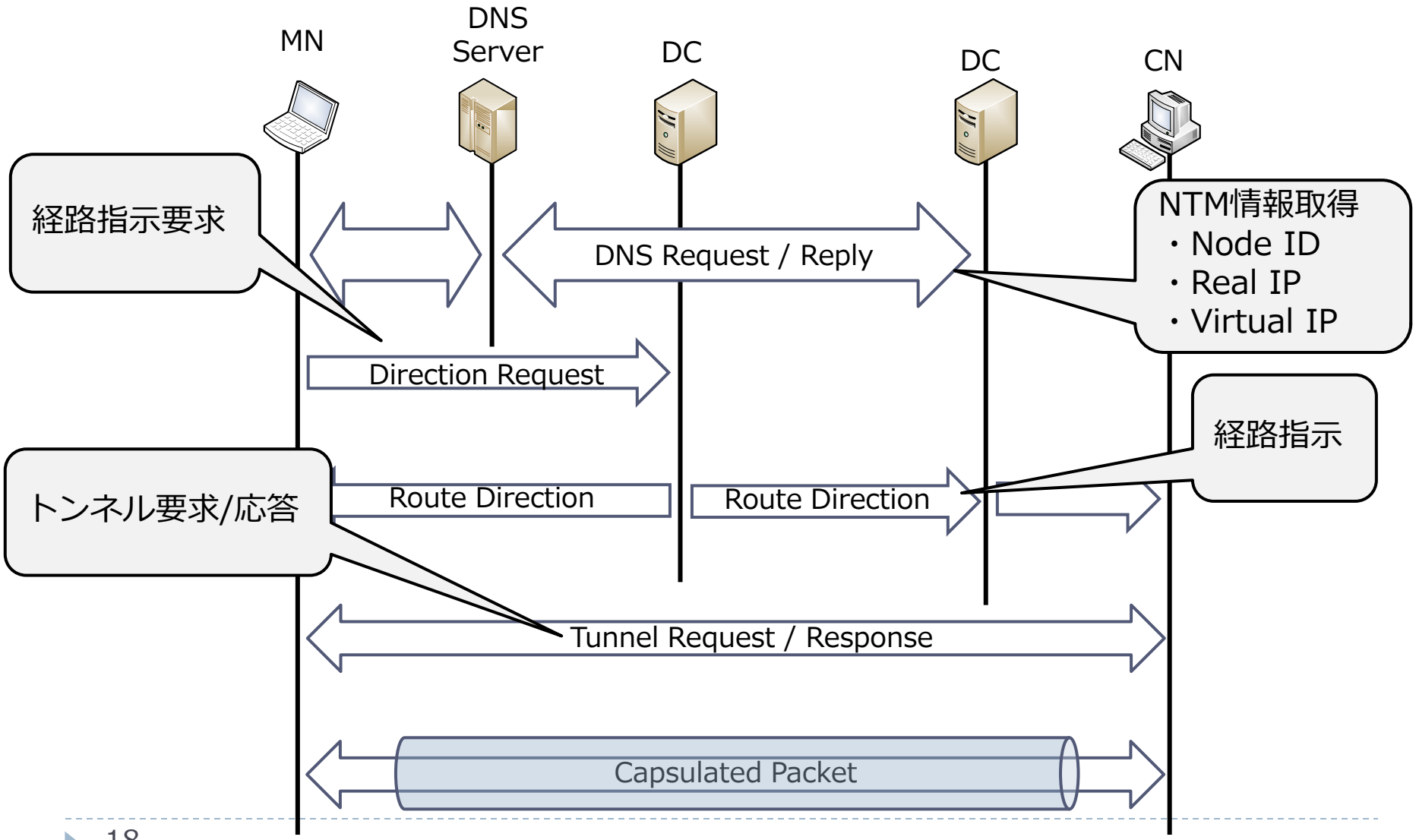
Direction Coordinator (DC-A, DC-B)
OS : Ubuntu 10.04
CPU : Core 2 Duo P9400 2.4GHz
Memory : 2048MB
Ethernet : 1000Base-T

Switching Hub, NAT
Ethernet : 100Base-TX



	RTT[ms]
CN ~ DS-A	0.797
CN ~ DS-B	0.747
MN ~ CN	1.306
DC-A ~ DC-B	0.705
MN ~ DC-B	1.229

NTMobile (基本動作)



NTMobile (Access Checkによる拡張)