NTMobileにおけるグループ認証方式の提案と実装

村 橋 孝 謙[†1] 鈴 木 秀 和[†1] 旭 健 作[†1]
内 藤 克 浩[†2] 渡 邊 晃[†1]

ユビキタスネットワークの発展に伴い，ネットワーク環境に依存しない通信接続性や通信中の移動を可能とする移動透過性が重要となっている．これらの条件が満たされた上で，さらにエンドエンドの認証と暗号化が実現できるとより有用である．

我々はトンネル技術と仮想アドレスを用いることにより通信接続性と移動透過性を同時に実現する NTMobile（Network Traversal with Mobility）と呼ばれるシステムを提案している．しかし現状の NTMobile はエンドエンドのセキュリティが考慮されていない．本稿では NTMobile に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機能を追加し，認証結果に応じて通信可否を決定する方法を提案する．提案方式の実装を完了した結果，必要十分なセキュリティを備えており，比較的広範囲での運用が可能であることを確認した．

Proposal of a Group Authentication Method in NTMobile and Its Implementation.

Takanori Murahashi ,[†1] Hidekazu Suzuki ,[†1]
Kensaku Asahi ,[†1] Katsuhiro Naito [†2]
and Akira Watanabe[†1]

With the spread of ubiquitous network, communication transparency, mobility, and end to end security become quite important matters. We have been proposing NTMobile (Network Traversal with Mobility), that can achieve communication transparency and mobility at the same time, however, it does not have the function to guarantee end to end security yet. In this paper, ACL(Access Check List) is added to NTMobile to achieve end to end authentication. We have implemented the proposed method and confirmed its high performance.

1. はじめに

ネットワーク技術の発展に伴い，IPv4 におけるグローバル IP アドレスの枯渇が問題になっている．その解決策として IPv6 への移行が必須とされているが，IPv4 との互換性がないために遅々として移行が進んでいない状況である．そのため，今後は IPv4 および IPv6 の混在したネットワーク環境が続くことが想定される．このようなネットワーク環境においても自由に通信を行うことができるネットワークの通信接続性が重要となる．

また，無線の有効利用の観点から，無線のリソースに応じてネットワークを切り替えて使用することが必須になると言われている．通信中に端末が移動すると，接続先ネットワークが切り替わる可能性がある．ネットワークの切り替えが発生すると IP アドレスが変化し，通信を継続することができない．そのため今後は IP アドレスの変化に関わらず通信を継続する移動透過性が重要となる．さらにネットワークが誰もが使用できるものになると，悪意を持つユーザによる犯罪が懸念されるため，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．

我々は，これまで通信接続性と移動透過性を同時に実現する NTMobile[1)–3)] を提案してきた．NTMobile では，上位ソフトウェアは DC（Direction Coordinator）から配布された仮想 IP アドレスを用いてセッションを確立する．通信パケットは，DC から指示されたトンネル経路を介して実 IP アドレスでカプセル化することにより相手ノードに送り届けられる．エンドノード間でトンネル経路を構築できない場合は，RS（Relay Server）を経由することによりトンネルを確立する．この方法により，通信経路上でアドレス体型が変化したり通信中に実 IP アドレスが変化しても，仮想 IP アドレスのセッションには影響を与えないようにすることができる．MTMobile はこのように通信の制約を完全に除去することができるが，エンドエンドの相手認証については今後の課題であった．

エンドエンドのセキュリティを実現する代表的技術として，IPsec[4)] が挙げられる．しかし IPsec は強固なセキュリティを確保できる反面，NAT との相性が悪いことや移動透過性に対応することが難しいといった問題がある．また IPsec では汎用性を重視したため設定項目が多く，特に大規模なネットワークにおいて設定にかかる負荷が大きい．さらに項目の選

†1 名城大学大学院理工学研究科
Graduate School of Science and Technology, Meijo University
†2 三重大学大学院工学研究科
Graduate School of Engineering, Mie University

択に専門的な知識を必要とするなどの課題がある．

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）[5] 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エンド端末間のセキュリティを確保し，かつ IP アドレスや物理的な配置に依存しない通信グループを構築することができる．このため大規模なシステムにおいても管理が容易であるという利点がある．しかし GSCIP においても NAT との相性問題があり，これを解決するためには NAT を改造する必要があった．[6]

そこで NTMobile においては，新たにエンドエンド認証の実現方法として，DC にアクセス制御リスト ACL（Access Control List）を保持させることによりグループ単位での認証を行う方法を提案する．通信開始時に両エンド端末のノード ID をもとに ACL から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コネクション処理を完了させる．

ACL によるアクセス制御方式を実装し，動作検証と性能測定を行ったので報告する．以下 2 章で既存方式の概要および課題を説明し，3 章で NTMobile の解説を行う．4 章で ACL を適用した NTMobile の概要および動作を説明し，5 章で評価を行い，最後に 6 章でまとめる．

2. 既存方式とその課題

NTMobile にエンドエンドのセキュリティ機能を追加しようとした場合，既存の技術をそのまま適用する方法が考えられる．そこで既存技術として IPsec と GSCIP をとりあげ，その課題を整理した．

2.1 IPsec

IPsec は IP 層で暗号化と認証を実現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．ESP（Encapsulating Security Payload）[7] では IP パケットの暗号化と改ざん検出が可能であり，IKE（Internet Key Exchange）[8] により，認証と共通鍵の共有が可能である．

パケットの処理方法は SA（Security Association）によって決定されるが，SA の管理を手動で行うことは管理負荷やセキュリティの問題上好ましくないため，多くの場合は IKE が使用される．IKE は SA の自動的な生成，管理を行う．ESP と IKE を組み合わせることで IP ヘッダを含めたパケットの改ざん検知も可能である．

ESP によりパケットの暗号化を行う場合，基本的に NAT を跨る通信を行うことができない．そのため，NAT を通過させる場合は UDP によるカプセル化を行う必要があるが[9]，IPsec の特徴である強固なセキュリティは確保できない．

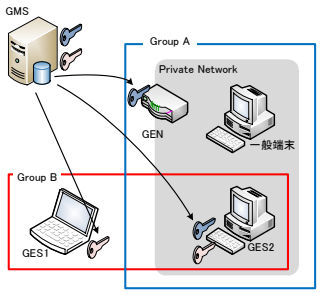


図 1 GSCIP 基本構成
Fig. 1 GSCIP Basic composition

IPsec は汎用性のため暗号化アルゴリズム・認証アルゴリズム・パケット処理方法など設定項目が多く，専門的な知識を要する．また，通信ペア毎の設定が必要なためネットワークの規模が大きくなると管理負荷が指数関数的に増大する．トンネルモードとトランスポートモードを併用するためにはそれぞれのモードに設定が必要となり，さらに管理負荷が高くなる．

2.2 GSCIP

GSCIP では，グループ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が 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．また，IPsec では難しかった端末単位およびドメイン単位の混在した通信グループの構築が容易に可能となる．

GSCIP を用いた通信グループの構成を図 1 に示す．GSCIP では同一の暗号鍵 GK（Group Key）を所有する構成要素 GE（GSCIP Element）を同一のグループに属するメンバとして考える．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，各 GE と管理サーバ GMS（Group Management Server）[10] 間に信頼関係のあることが前提である．GMS は各 GE の動作モードやグループ鍵の配送，グループ鍵の管理や GE と通信グループ番号の関連付けなどを行う．グループ鍵 GK は通信グループに応じて生成

され，定期的に更新を行う．

GMS は通信に必要な端末とは別に設置する必要がある．GSCIP では 1 つ GMS が管理グループ全体の管理を行う．そのため NTMobile に GSCIP を適用すると，NTMobile で想定している信頼関係とは別の信頼関係が必要となり，管理が複雑になる．また，GSCIP の相手認証には DPRP（Dynamic Process Resolution Protocol）[11] を使用するが，これは NAT を通過することができない．NAT を通過させるには NAT の改造が必要となる[12]．また GSCIP の移動透過プロトコル MobilePPC[13] においても通信に NAT の制約を受ける．

3. NTMobile

3.1 NTMobile とは

NTMobile はトンネル技術と仮想 IP アドレスを用いることで通信接続性と移動透過性を同時に可能とする．図 2 に NTMobile の概要を示す．NTMobile で使用する機器は，NTMobile の機能を実装した NTM 端末，NTM 端末を管理する DC（Direction Coordinator），NTM 端末間の通信を中継する RS（Relay Server）である．DC および RS はネットワークの規模により増設することができる．DC と NTM 端末，DC 同士および DC と RS の間には信頼関係のあることが前提である．

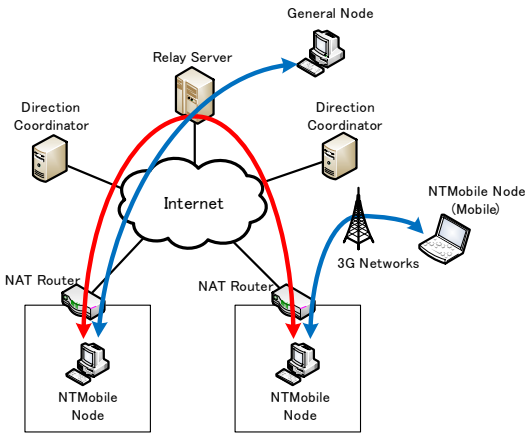


図 2 NTMobile の概要
Fig. 2 Overview of NTMobile network

NTMobile では DC が NTMobile 端末に対し仮想 IP アドレスを配布し，さらにトンネルの経路指示を行う．NTM 端末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い，実際の通信は実 IP アドレスでカプセル化を行う．実 IP アドレスが変化した場合においても同一の仮想 IP アドレスを使用し続けることができるので，アプリケーションは IP アドレスの変化を意識する必要がない．NTM 端末は起動時に DC に実 IP アドレスを登録するとともに，DC から仮想 IP アドレスを受け取る．

通信を行う NTM 端末が共に異なる NAT 配下にあるなど直接通信ができない場合は，RS（Relay Server）を介した通信を行う．また NTM 端末と RS 間にトンネルを構築し，RS に NAT 機能を持たせることにより，NTM 非対応の一般端末との通信を可能としている．NTMobile は DC から NTM 端末と RS に対して適切な指示を出すことにより，アドレス体系の異なる IPv4 プライベートアドレス，IPv4 グローバルアドレス，IPv6 アドレスを跨る通信接続性と移動透過性が実現可能である．

3.2 NTMobile の動作

NTMobile では通信時には両エンド端末間において UDP トンネルを生成し，これを用いて通信を行う．基本的な動作例として，NAT 配下にある NTM 端末 A から，グローバル IP アドレス環境に存在する NTM 端末 B へ通信を開始する場合の例を図 3 に示す．

通信開始時に，まず NTM 端末 A は DNS Request により通信相手端末ホスト名に対応した実 IP アドレスおよび仮想 IP アドレスを含む NTM レコードを取得する．DNS 問合せが完了すると，NTM 端末 A は取得した情報を用いて，自身が所属する DC（DC-A）にあらためてに Direction Request を送信し，トンネル構築の指示を依頼する．DC-A は両エンド端末の位置に応じて経路指示を送信する．両エンド端末はこの指示に従ってエンドエンドの UDP トンネル経路を生成する．

NTM 端末 A は指示に従い NTM 端末 B へトンネル構築要求 Tunnel Request を送信する．NTM 端末 B がトンネル構築応答 Tunnel Response を返答すると通信トンネルが構築され，以後の NTM 端末間の通信にはこの経路を使用する．このように NTMobile では DC が適切に経路指示を行うことにより NAT の制約を受けない通信が可能となる．

4. ACL を適用した NTMobile

4.1 ACL 適用方式の概要

NTMobile のセキュリティを高めるため，グループ単位でのアクセス制御方式を提案する．

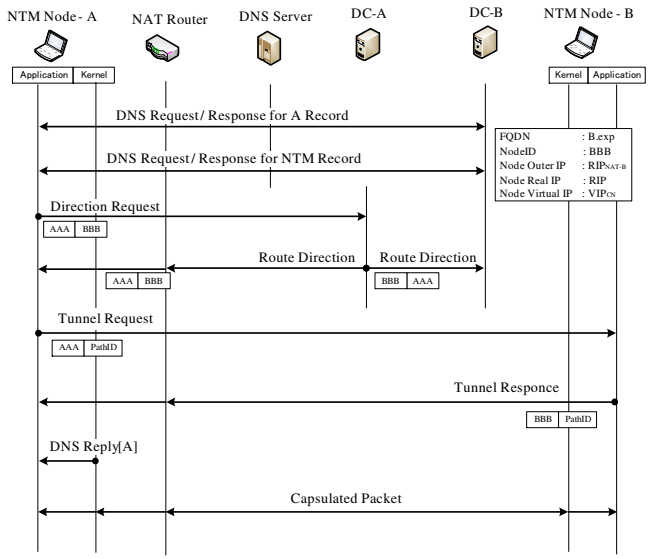


図 3 NTM 基本動作例
Fig. 3 NTMobile basic composition

提案方式では各 NTM 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プに所属している場合のみ以後の NTMobile ネゴシエーション処理を継続する．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ち，通信開始時には通信相手側の DC に対し所属グループの問い合わせと照合（アクセスチェック）を行う．例外として，通信相手側端末の情報が ACL に登録されていない場合はコネクション処理の破棄は行わない．これは DC が ACL を参照した際，ACL に未登録の端末にはアクセス制御を行う必要がないとみなすためである．

アクセスチェックは常に通信相手側 DC において行われる．これにより，通信相手側 DC は通信開始側のアクセスポリシに依らず，配下の NTM 端末を保護するためアクセスポリシを設定することができる．ACL への設定は，DC 配下のサーバを管理するネットワーク管理者が自らの端末から行う．DC と配下端末間には既に信頼関係があるため，エンドエンドの認証を実現するために新たな信頼関係を定義する必要はない．

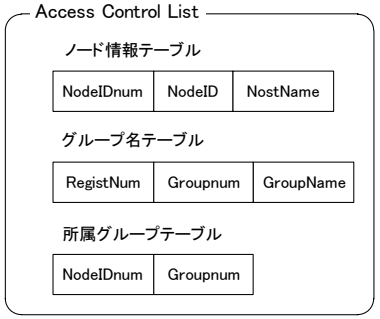


図 4 Access Control List
Fig. 4 Access Control List

4.2 ACL 構成

ACL はノード ID と所属グループの関係などを示すテーブルである．ACL の内容は図 4 に示すように，ノード情報テーブル，所属グループテーブル，グループ名テーブルからなる．

- ノード情報テーブル
  各 NTM ノードのノード ID とホスト名およびノード ID に対応する登録番号が含まれる．アクセスチェックの際はノード ID からノード ID 番号を探し当てる．
- グループ名テーブル
  定義されたグループ名一覧と，グループ名に対して付けられる登録番号からなる．
- 所属グループテーブル
  各ノード ID 番号と，そのノードが所属するグループ番号からなる．テーブル内の組み合わせで各ノードの所属グループが決定され，あるノードが所属するグループ毎に記述される．アクセスチェックの際はノード情報テーブルで検索されたノード ID 番号をもとに，所属グループ番号を検索する．

4.3 シーケンス

ACL を適用した通信の例を図 5 に示す．コネクション開始時の基本的なシーケンスは ACL を使用しない場合と同じであるが，新たに Access Check Request，Access Check，

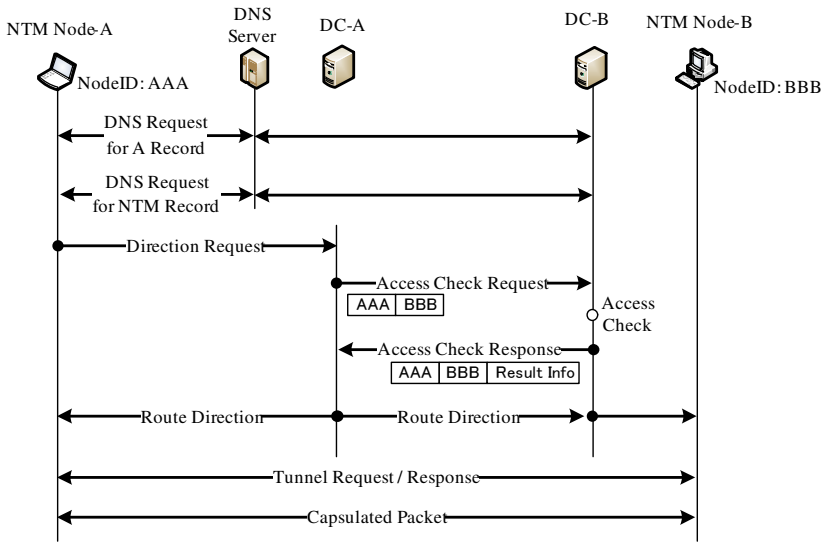


図 5 Access Check 動作シーケンス
Fig. 5 Sequence of Access Check

Access Check Response，の動作が追加され，Route Direction の内容を一部変更する．

ネゴシエーション開始から通信開始側 DC の Direction Request 受信以前，および通信開始側エンド端末の Tunnel Request 送信時以降は従来の動作と同様であるため，説明を省略する．

(1) 通信開始側 DC は Direction Request を受信すると，両エンド端末のノード ID をもとにアクセスチェック要求パケット Access Check Request を作成し，通信相手側 DC へ送信する．

(2) 通信相手側 DC は Access Check Request を受信すると，パケットに含まれるノード ID をもとに自身の持つ ACL からノード ID 番号を検索し，さらにノード ID 番号をもとに所属グループ番号一覧を取り出す．両エンド端末の所属グループ番号に一致するものがあるかを確認する．

(3) アクセスチェック処理が完了するとその結果を Result Info に格納し，両エンド端末のノード ID と共に Access Check Response として通信開始側 DC へ送信する．

(4) 通信開始側 DC は Access Check Response を受信すると，Result Info が [OK] の値であった場合は通信開始端末および通信相手側 DC への Route Direction を送信する．Result Info が [NG] の値の場合は通信開始端末のみへ Route Direction を送信する．また RS に向けての Relay Direction 送信も行わない．

(5) 通信開始端末が Route Direction[OK] を受信した場合，Tunnel Request を通信相手端末に向け送信する．通信開始端末が Route Direction[NG] を受信した場合は Tunnel Request を送信せずネゴシエーションを中断する．

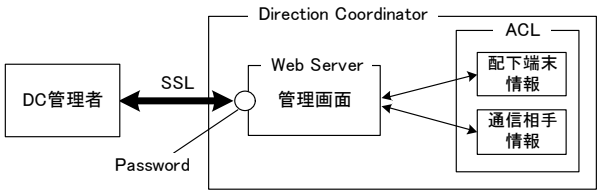


図 6 管理者とインタフェースの関係
Fig. 6 Administrator and interface

4.4 ACL の管理

ACL の管理は，Web ブラウザから操作を行うことで簡単かつ安全に各端末の所属グループを設定することができる．図 6 に管理者および管理インタフェースの関係を示す． DC は Web サーバとしての機能を持ち，Web サーバ上で ACL 管理システムを実行させる．DC 配下のネットワーク管理者は管理システムにログインし，ACL を設定することができる．管理者および管理画面間は SSL を用いてセキュリティが確保される．管理システムを使用することで，DC 管理者のみが通信グループを定義することができる．

5. 評　　価

5.1 機 能 比 較

IPsec，GSCIP，NTMobile および ACL を適用した NTMobile において各方式の有効性の確認のため機能比較を行った．比較結果を表 5.1 に示す．

- パケットの機密性

通信パケットの暗号化による機密性の比較を行う．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．それに対し，GSCIP においては TCP/UDP ヘッダを含まないペイロード部分のみとなる．これはファイアウォールの通過を目的としているためである．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．UDP カプセリング技術を使用しているため UDP ヘッダの暗号化を行うことができないが，その内容は保証される．

- グループ認証
  IPsec では各通信ペアに応じて SA の設定を行う必要があるため，大規模なネットワークでの使用は困難である．GSCIP においてはグループ鍵と通信グループの一対一の対応から容易なグループの定義と認証が可能である．これまでの NTMobile では，アクセス制御が定義されていなかったが，ACL を用いることでグループ単位のアクセス制御が可能となる．特定のサーバへのアクセス制御やクライアント/サーバ型のシステムでの柔軟なグループ定義を行うことができる．
- NAT への対応
  IPsec では，UDP でカプセル化することで NAT を通過することができるが，セキュリティの強度は低下する．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 に係る制約は一切存在しない．
- 移動透過性
  IPsec では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の継続が難しい．MOBIKE[14] では端末の移動時においてもセッションを維持することが検討されているが，トランスポートモードでの使用や両エンド端末の同時移動はできない．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ても通信を継続することができる．ただし GSCIP 単体では NAT 越え問題を解決できないため，NAT を経由する移動には対応できない．NTMobile では IP アドレスの変化に一切影響しない通信を行うことができる．

5.2 実　　装

図 7 に DC のモジュール構成図を示す．DC の主な機能は仮想 IP アドレスの管理・配布とトンネル構築指示である．本提案により，これらの機能に加えアクセス制御処理が追加される．DC の NTMobile デーモン内にアクセスチェック機能を実装する．また端末内に SQL Server を稼働させ，データベース内に ACL を構築する．DC はアクセスチェックの要求に応じてデータベースを参照する．

表 1　機能比較結果
Table 1　Functional comparison result

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

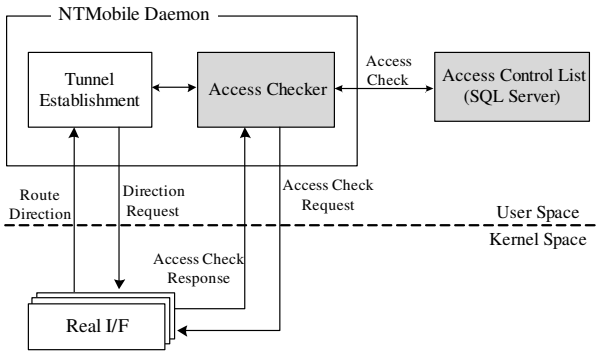


図 7　DC のモジュール構成
Fig. 7　Module configuration of direction coordinator

Access Checker は Direction Request を受信すると Access Check Request を送信する．また Access Check Request を受信すると Access Check を行い，その結果を Access Check Response に載せて返送する．

5.3 性 能 評 価

提案方式におけるアクセスチェック処理の追加によるオーバヘッドを調査するため，トンネル構築に要する時間を測定した．図 8 に試作ネットワーク構成を示す．NAT 配下に存在する NTMobile 端末 EN-B がグローバル IP アドレス空間に存在する EN-A に対しトンネルの構築を行う．各装置の仕様を表 2 に示す．なお，ACL には MySQL Server 5.1.41 を使用した．今回は中規模な組織での使用を想定し，EN-B 側，EN-A 側において各 100 台の端末を登録した．EN-B および EN-A はそれぞれ 10 のグループに所属しているものとする．

表 2 実験機器諸元
Table 2 Performance evaluation parameters

Name	OS / Product	CPU	Memory	NIC
EN-A	Ubuntu 10.04	Core 2 Duo U9400 1.4GHz	2048MB	1000Base-T
EN-B	Ubuntu 10.04	Core 2 Duo U9400 1.4GHz	2048MB	1000Base-T
DC-A	Ubuntu 10.04	Core 2 Duo P9400 2.4GHz	2048MB	1000Base-T
DC-B	Ubuntu 10.04	Core 2 Duo P9400 2.4GHz	2048MB	1000Base-T
Switch	Buffalo LSW10/100	—	—	100Base-TX
NAT	Buffalo BBR-4MG	—	—	100Base-TX

通信時，パケットの到達から次のパケットが送信されるまでの時間を EN-B および DC-B において Wireshark を用いて計測した．また DC-A においてアクセスチェック前後の時刻を取得することで，アクセスチェックのみに要する時間を計測した．制御メッセージの暗号化アルゴリズムは AES-CFB，認証アルゴリズムには HMAC-MD5 を使用する．

図 9 にトンネル構築時のシーケンスと，各処理に要した時間を示す．最初に DNS クエリ応答を受信してから Tunnel Request を受信するまで，24.52ms を要した．これが NTMobile コネクション処理に要した時間の全体となる．

DC-B が Direction Request を受信するとアクセスチェック関係処理が開始される．アクセスチェック関係処理として，まず Direction Request 復号・検証および Access Check Request パケット生成，暗号および MAC 生成処理が含まれ，これには 1.73ms を要している．Access Check Request 送信から Access Check Response 受信にかかる時間が 10.64ms である．Access Check Request パケットの復号・検証およびアクセスチェック，Access Check Response パケット生成，暗号および MAC 生成処理が含まれる．アクセスチェックには SQL 問合せとグループ番号照合処理が含まれ，平均で約 8.64ms を要している．アクセスチェック関係処理に要する時間を合計すると，12.37ms である．これが ACL 適用方式において既存の NTMobile から追加される処理にかかる時間である．以上がアクセスチェック関係処理である．

Access Check Response 受信から EN-B へ Route Direction を送信する際に要する時間は 5.47ms である．これには Access Check Response 復号，MAC 値の検証，さらに DC-A へ送信する Route Direction の生成，暗号，MAC 生成処理および送信処理，EN-A へ送信する Route Direction の生成，暗号，MAC 生成処理が含まれる．MN が Route Direction を受信してから Tunnel Request 送信に要する時間が 0.54ms である．Route Direction の復号・MAC 値の検証と Tunnel Request パケットの生成，暗号，MAC 生成処理が含まれる．

コネクションに要した時間のうち，アクセスチェック関係処理の追加によるオーバヘッド

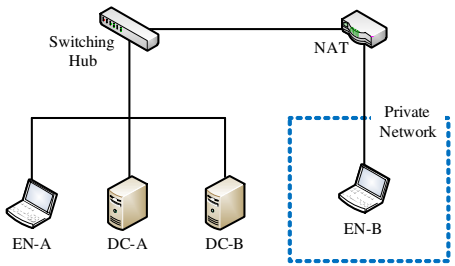


図 8 試作ネットワーク構成
Fig. 8 Trial Network

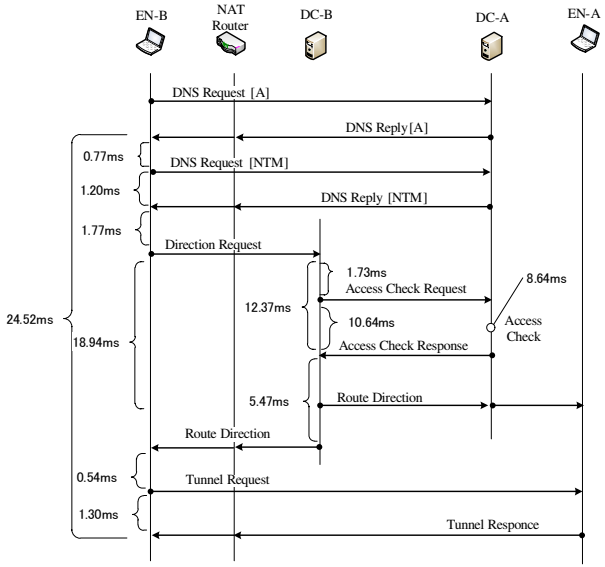


図 9 ネゴシエーション時間
Fig. 9 Negotiation time

の割合は大きいが，この処理を含めてもトンネル構築に要する時間は 25ms 以下である．グループ単位のアクセス制御を可能とすることに対する利便性を考えると，処理時間の増加は実用上問題ないといえる．

6. む す び

本論文では移動透過性と接続性を実現する NTMobile にグループ制御機能を加えた方式を提案し，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．ACL により同一グループに所属する端末同士のアクセスを許可することで，特定の端末の保護や通信グループの保護など，幅広いセキュリティの確保が可能である．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ヘッドは僅かであり実用上問題のない程度であることを確認した．

参 考 文 献

1) 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率手法と実装，DICOMO2011 論文集，pp. 1339–1348 (2011).
2) 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).
3) 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，DICOMO2011 論文集，pp. 1139–1145 (2011).
4) S.Kent and K.Seo: Security Architecture for the Internet Protocol, RFC 4301, IETF(2005).
5) 鈴木秀和，竹内元規，加藤尚樹，増田真也，渡邊　晃 : フレキシブルプライベートネットワークを実現するセキュア通信アーキテクチャGSCIP の提案，DICOMO2005 論文集，Vol. 2005, No. 6, pp. 441–444 (2005).
6) 鈴木秀和，宇佐見庄五，渡邊　晃 : 外部動的マッピングにより NAT 越え通信を実現する NAT-f の提案と実装，情報処理学会論文誌，Vol. 48, No. 12, pp. 3949–3961 (2007).
7) S.Kent: IP Encapsulating Security Payload (ESP), RFC 4303, IETF (2005).
8) C.Kaufman, P.Hoffman, Y.Nir and P.Eronen: Internet Key Exchange Protocol Version 2(IKEv2), RFC 5996, IETF (2010).
9) Levkowetz, H. and Vaarala, S.: Mobile IP Traversal of Network Address Translation(NAT) Devices, RFC 3519, IETF (2003).
10) 今村圭佑，鈴木秀和，後藤裕司，渡邊　晃:セキュア通信アーキテクチャGSCIP を実現するグループ管理サーバの実装と運用評価，DICOMO2008 論文集，pp. 1516–1522(2008).
11) 鈴木秀和，渡邊　晃 : フレキシブルプライベートネットワークにおける動的処理解決プロトコル DPRP の実装と評価，情報処理学会論文誌，Vol. 47, No. 11, pp. 2976–2991(2006).
12) 後藤裕司，鈴木秀和，渡邊　晃 : NAT を跨る閉域通信グループの提案と評価，情報処理学会論文誌，Vol. 52, No. 9, pp. 1234?1243 (2011).
13) 竹内元規，鈴木秀和，渡邊　晃 : エンドエンドで移動透過性を実現する Mobile PPC の提案と実装，情報処理学会論文誌， Vol. 47, No. 12, pp. 3244–3257 (2006).
14) Eronen, P.: IKEv2 Mobility and Multihoming Protocol (MOBIKE), RFC4555, IETF(2006).

NTMobileにおけるグループ認証方式の提案と実装

村橋孝謙 †　鈴木秀和 †　内藤克浩 ‡　渡邊晃 †
† 名城大学大学院 理工学研究科　‡ 三重大学大学院 工学研究科

研究背景

- 通信接続性の需要
  - IPv4プライベート/グローバル共存環境の自由な通信
  - IPv4/IPv6の自由な通信

通信接続性

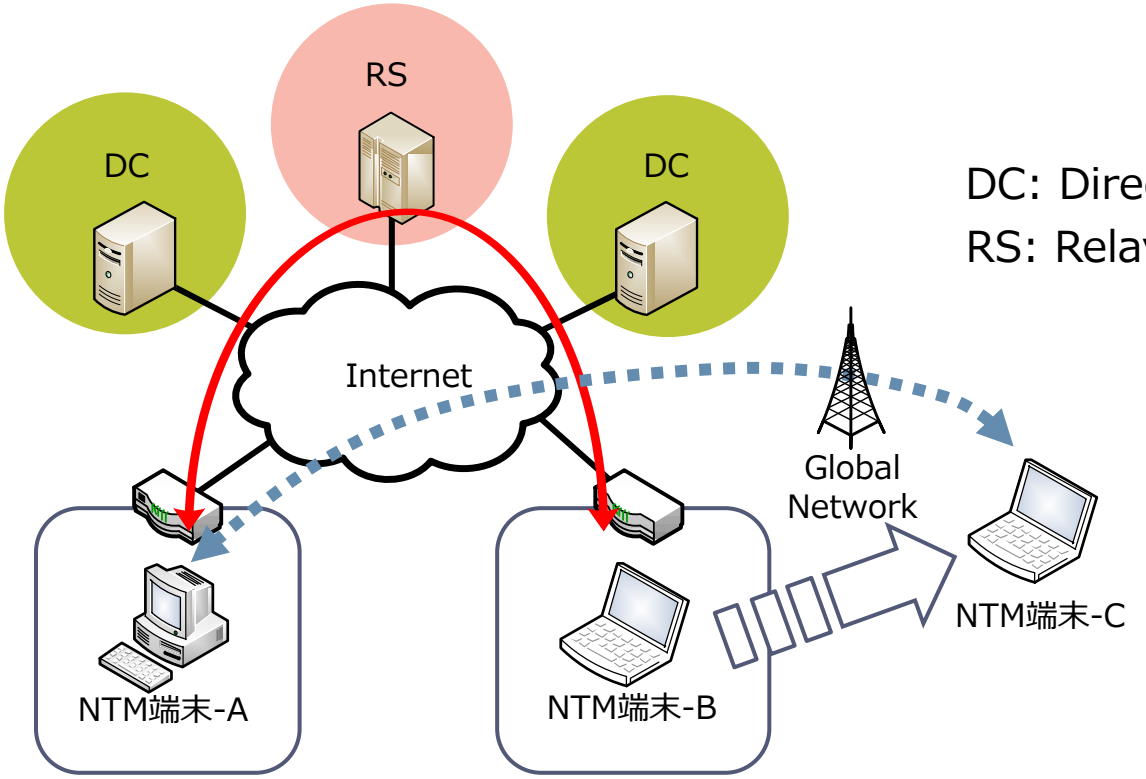
- 移動通信の需要
  - 複数無線I/F搭載
  - 通信中のネットワーク切り替え時にも通信を継続したい

移動透過性

通信接続性と移動透過性を同時に実現する
NTMobile (Network Traversal with Mobility)

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
  - パスワードに頼らない認証

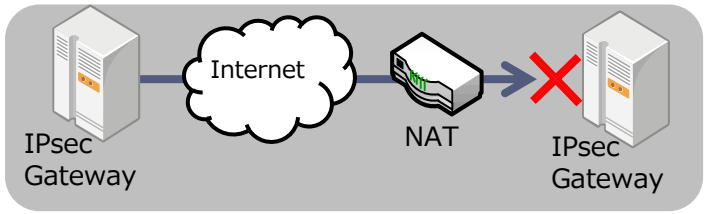
- 認証によりアクセス制御を可能とする技術

IPsec　　特徴：強固なセキュリティ

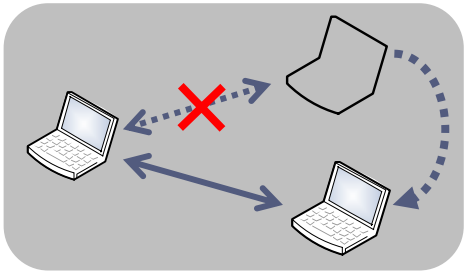
GSCIP　　特徴：柔軟なグルーピング

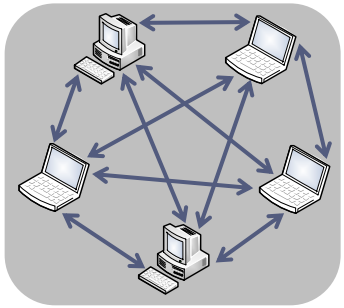
IPsecの課題

- 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　　NATとの相性が悪い
    （偽装パケットと判断されるなど）
  - 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

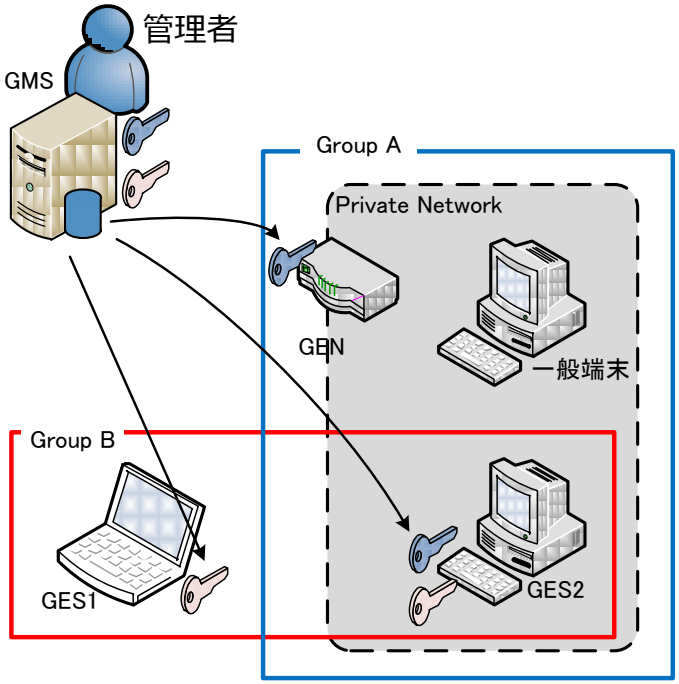

移動透過性


管理負荷

GSCIP
(Grouping for Secure Communication for IP)

- 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

- GMS(Group Management Server)
  - 対応端末へ暗号鍵を配布
  - 同一グループの端末は同一の鍵を配布される
  - グループ内は鍵を使用したセキュアな通信



- 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

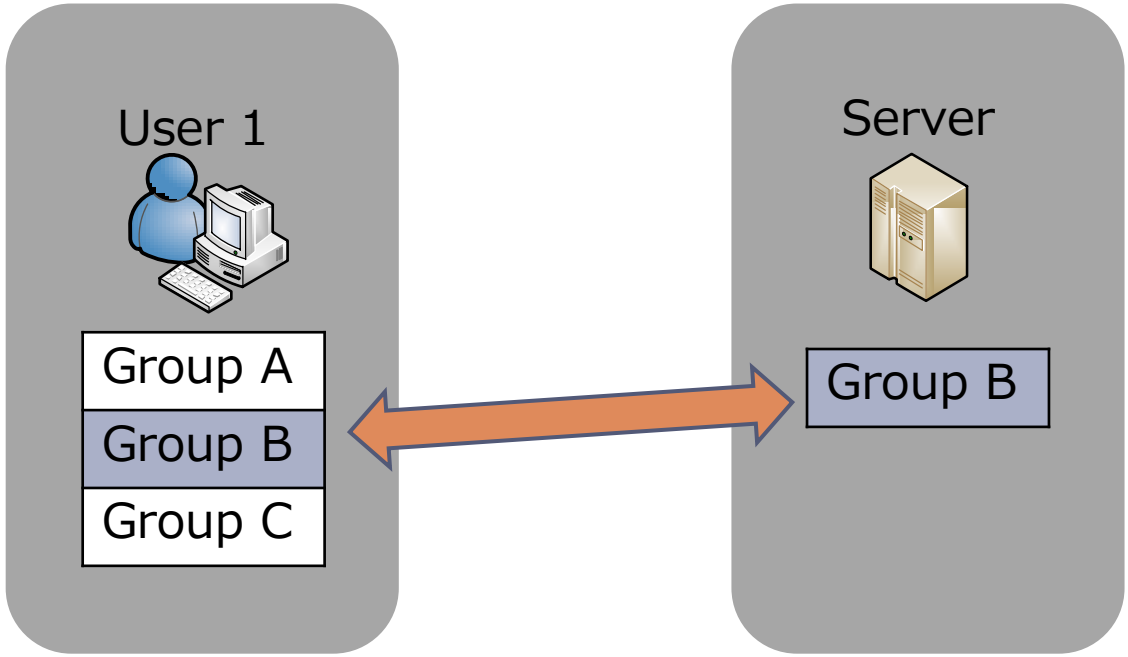
提案

- NTMobileにグループ単位のアクセス制御を追加
  - GSCIPを参考
- IPsecのような規模に応じた管理負荷の極端な肥大化を防ぐ
- 新たな装置を使用しない
  - 新たな信頼関係の必要性を無くす

- NTMobileを使用し接続性・移動透過性を維持する

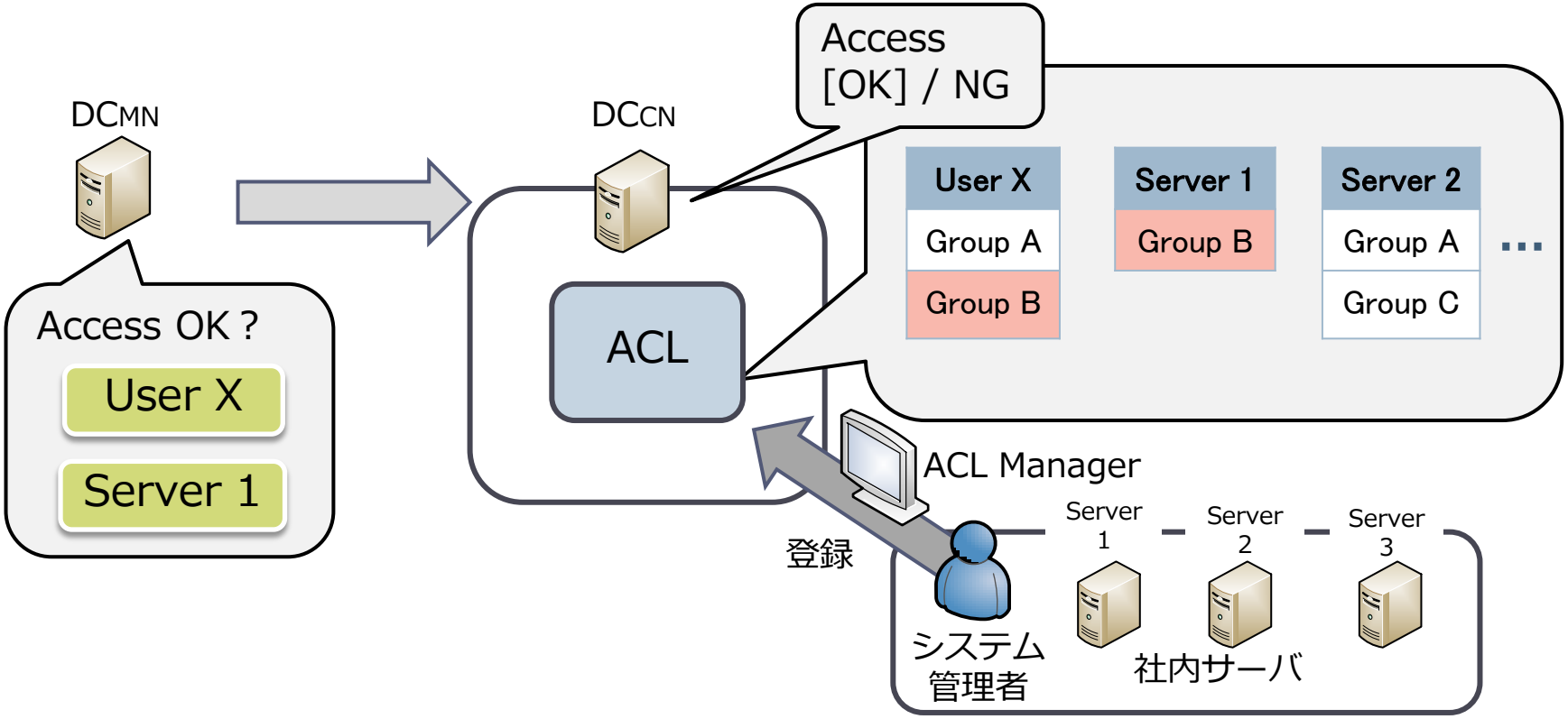
提案方式 (1/2)

- NTMobileにアクセス制御機能を追加
  - 各NTM端末はいずれかの通信グループに所属
  - 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

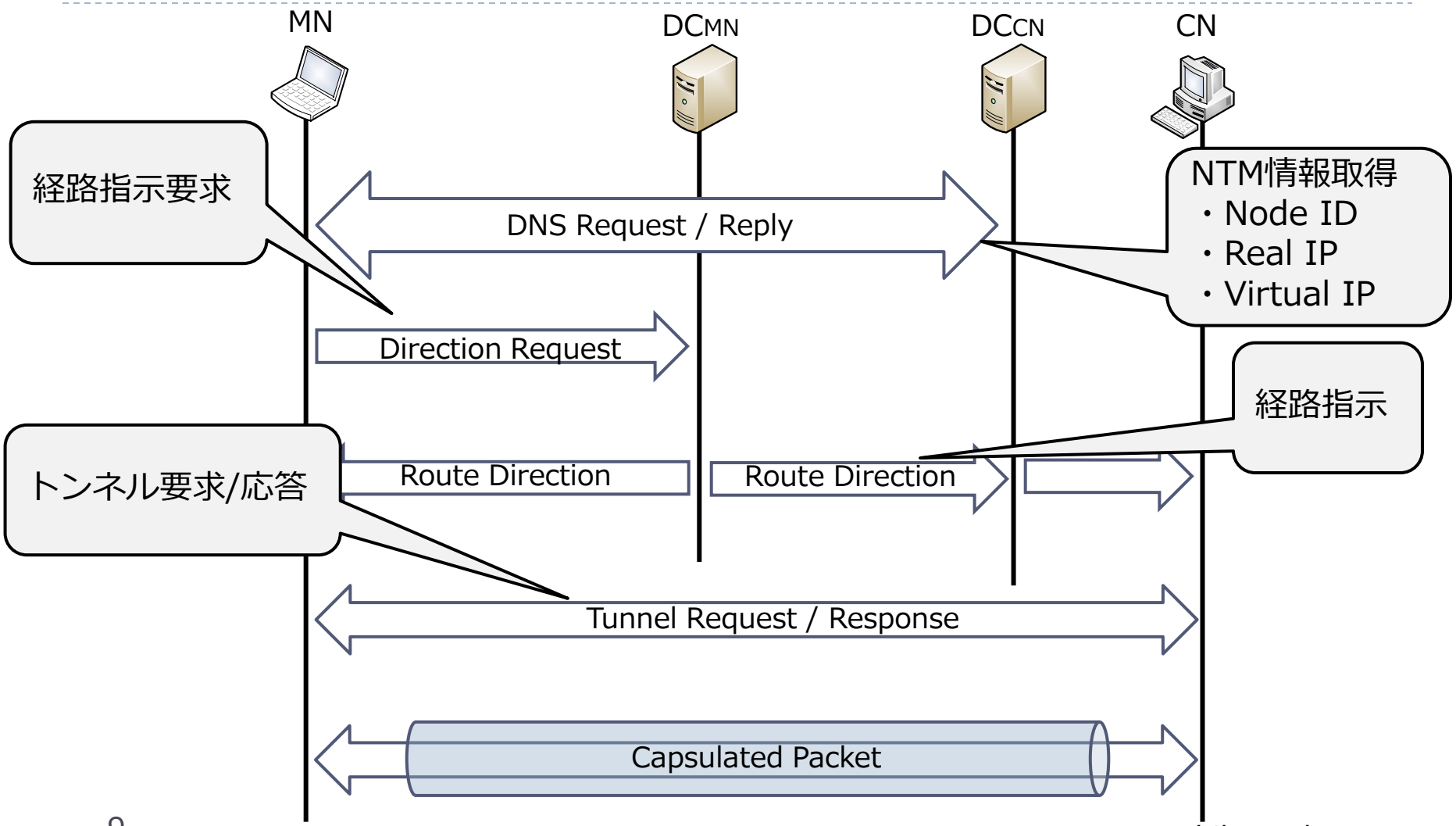


提案方式 (2/2)

- DCにACL(Access Control List)を追加
  - ACL：各NTM端末のNode ID，所属グループを格納
  - アクセスチェックにより，所属グループの確認・アクセス制御



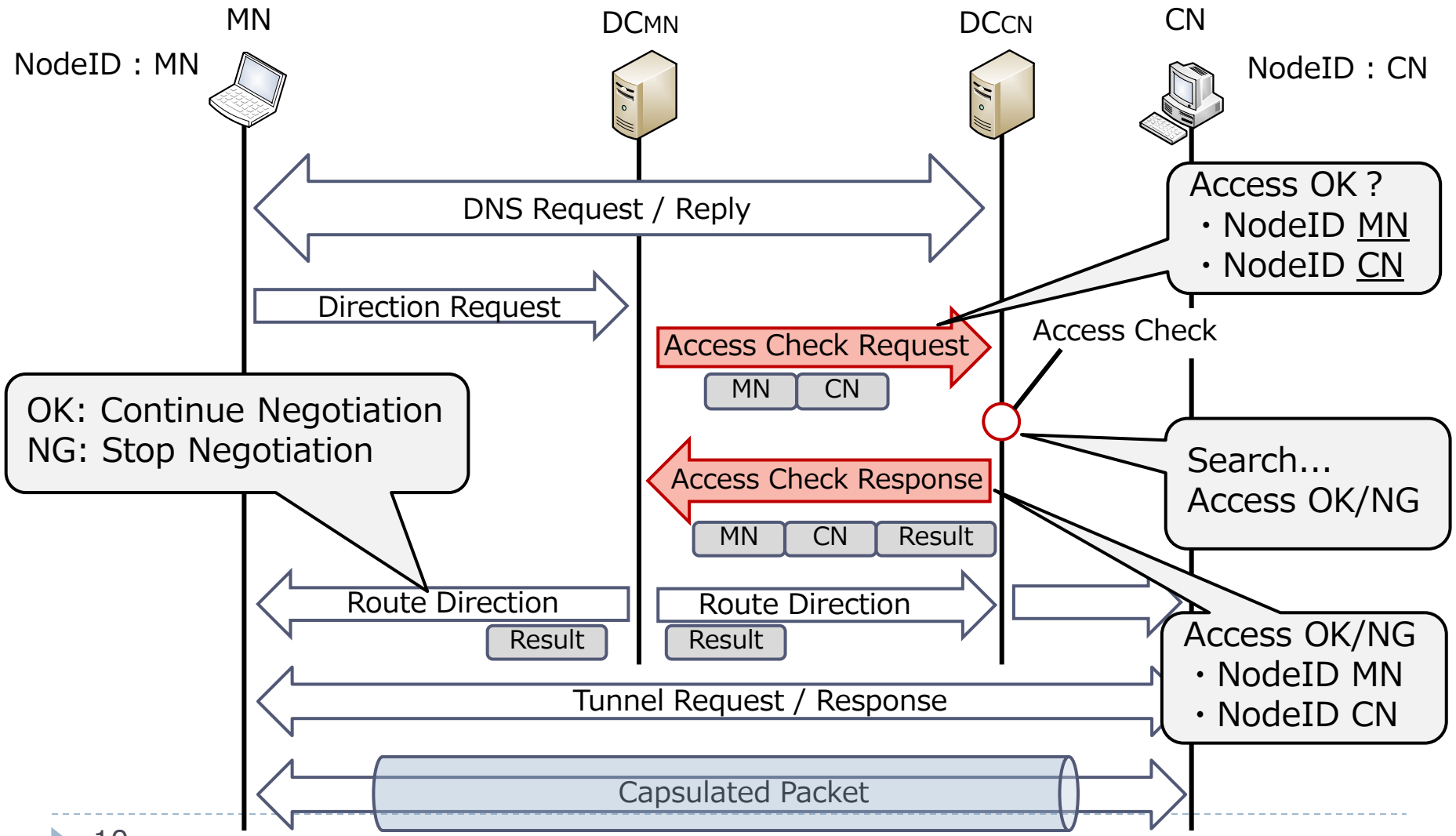
NTMobile (基本動作)



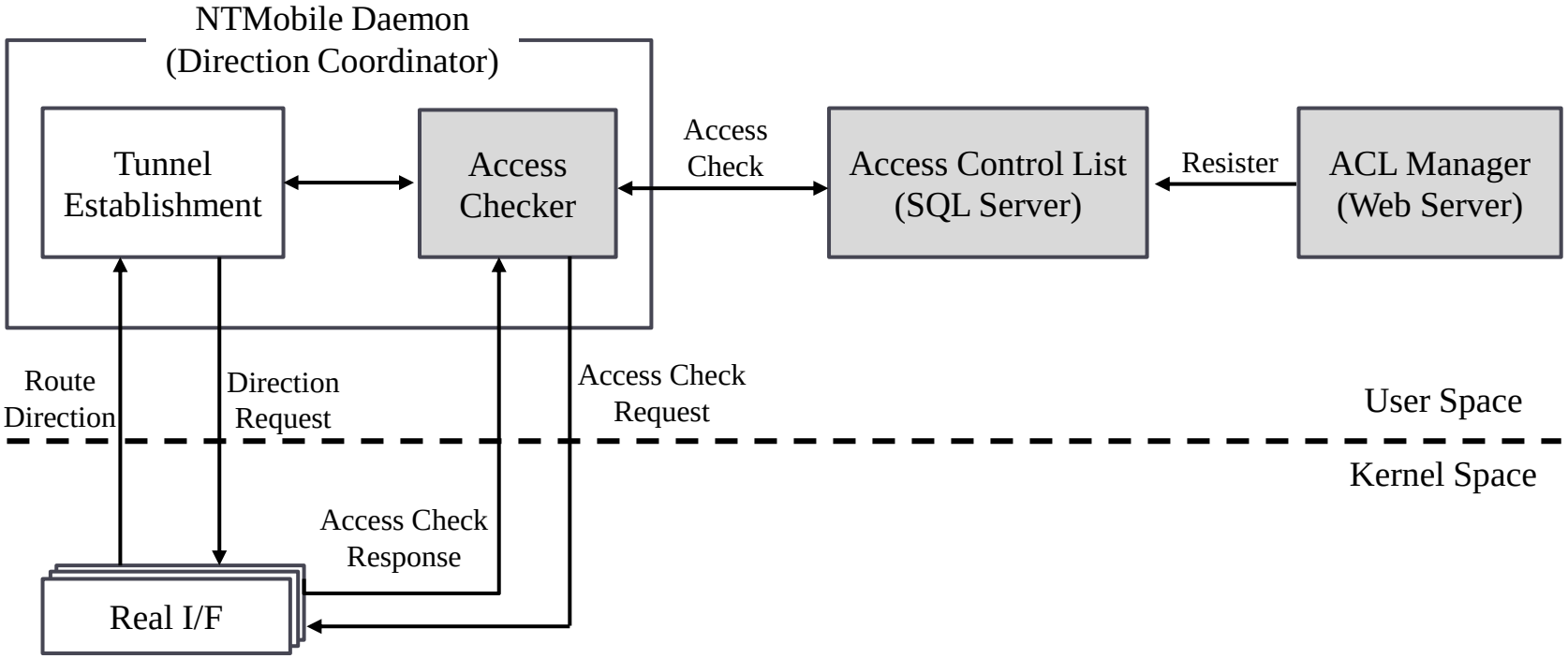
MN: Mobile Node

CN: Correspondent Node

NTMobile (Access Checkの拡張)



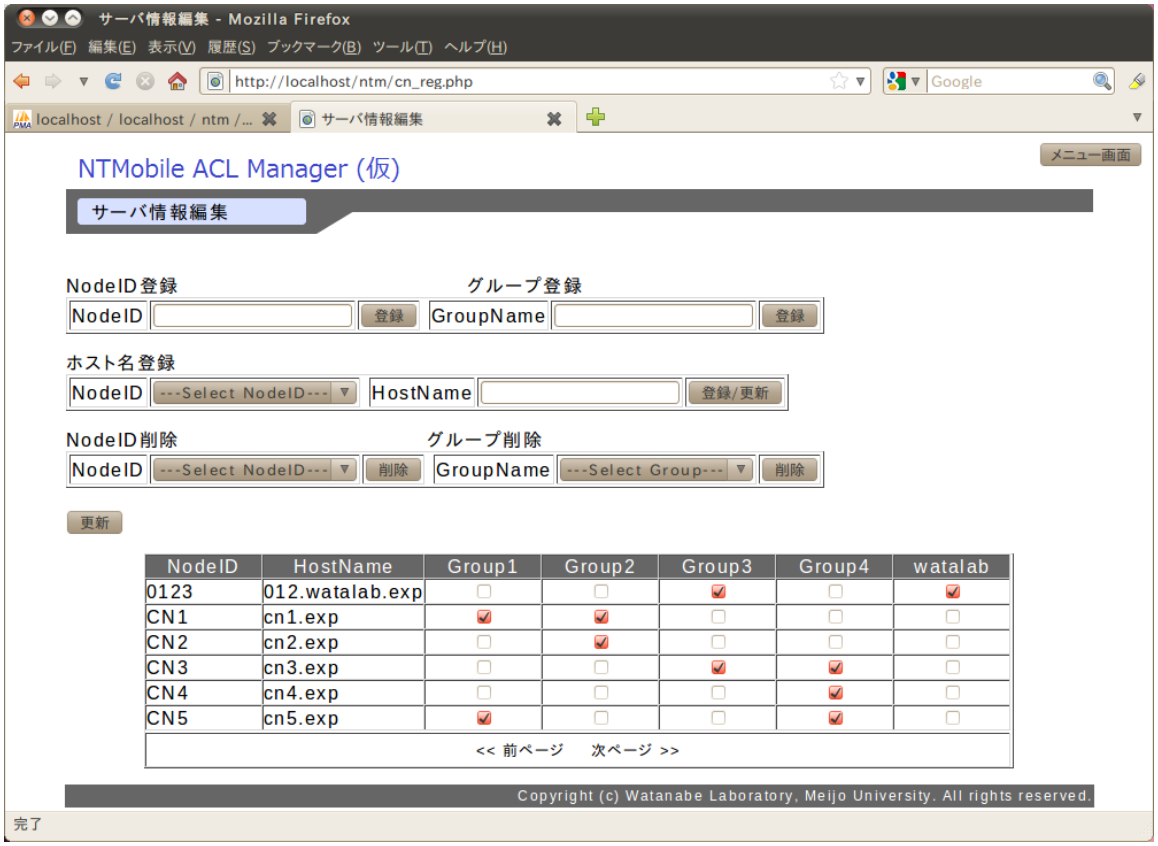
実装概要 (Direction Coordinator)



- 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



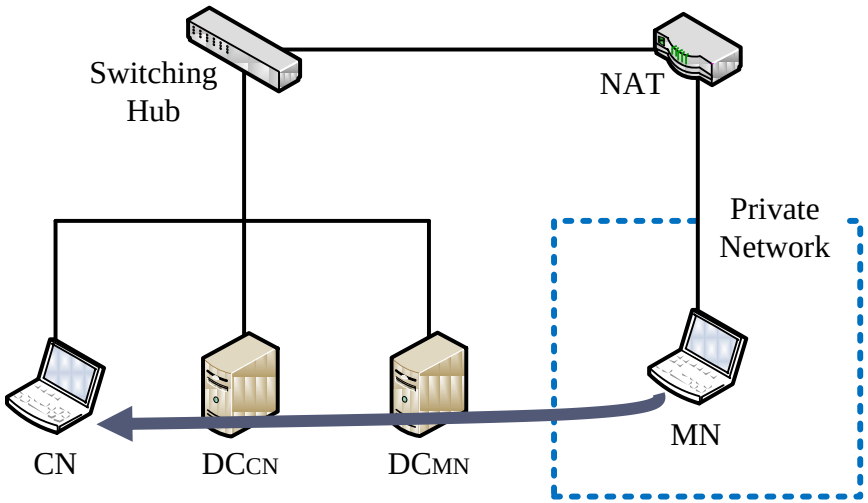
性能測定　（測定方法）

- 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

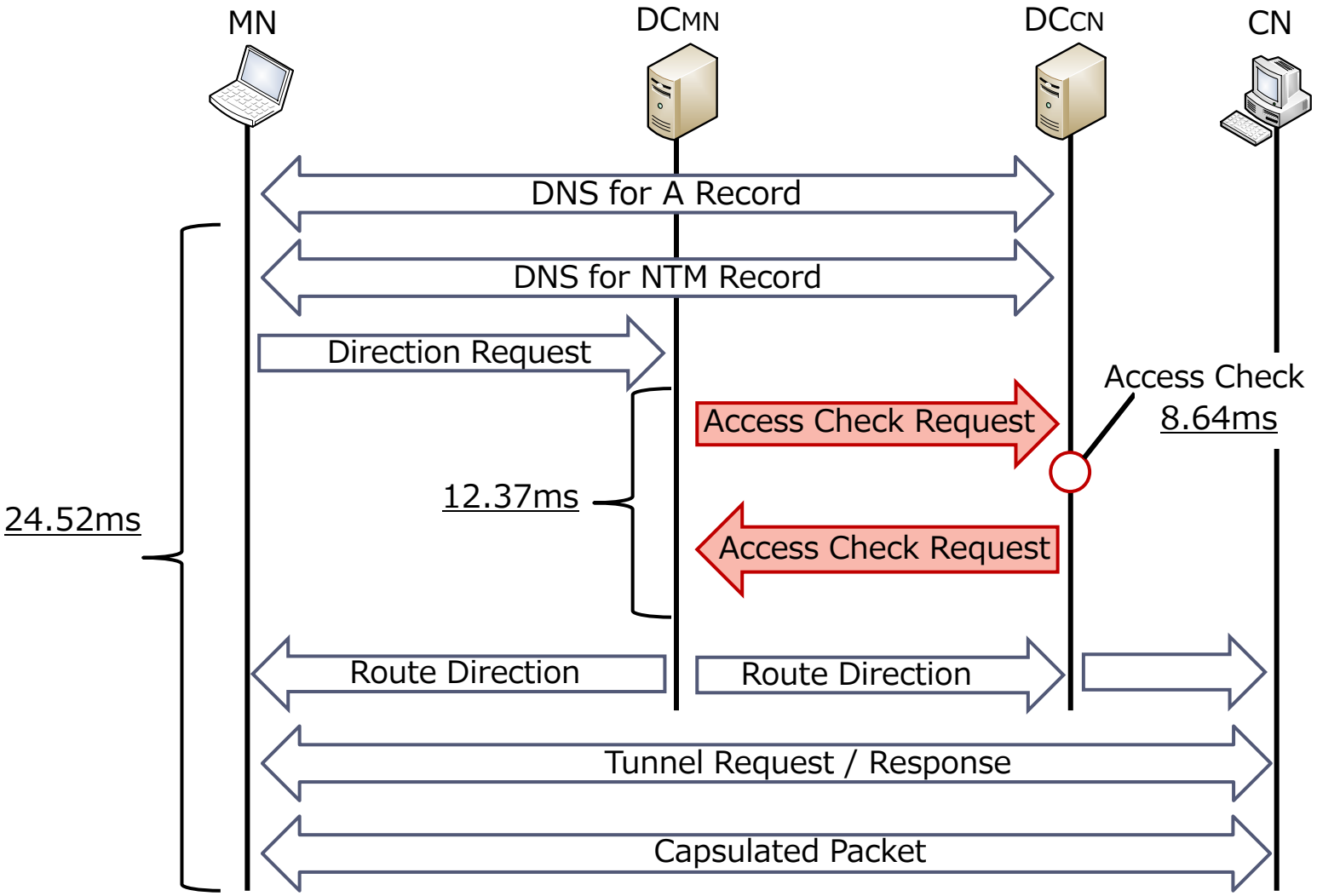
NTM Node (MN, CN)
OS : Ubuntu 10.04
CPU : Core 2 Duo U9400 1.4GHz
Memory : 2048MB
Ethernet : 1000Base-T

Direction Coordinator (DCMN, DCCN)
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
DCMN
DCCN
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

補足資料

機能比較

IPsec ESP

- ✓ 強固なセキュリティ
- ✓ NAT/NAPTとの共存が困難
- ✓ 移動透過性の確保に課題
- ✓ 大規模ネットワークでの管理が困難

GSCIP

- ✓ IPアドレス・物理的配置に依存しない通信
- ✓ 容易・柔軟なグルーピング

NTMobile (ACL)

- ✓ NATの影響を受けない
- ✓ 移動透過性の実現
- ✓ 容易・柔軟なグルーピング，セキュリティ

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

Access Check Response (Result)

- Result Info
  - Access [OK] の場合
    - No Access Control
      (通信相手側端末がACLへ未登録の際はアクセス制御を行わない)
    - Access Control Allowed
      (同一グループ所属を確認)
  - Access [NG] の場合
    - Not Fount Client ID
      (アクセス制御が有効なとき，通信開始側端末がACL未登録の場合)
    - Different Group
      (両エンド端末が異なる通信グループに所属)

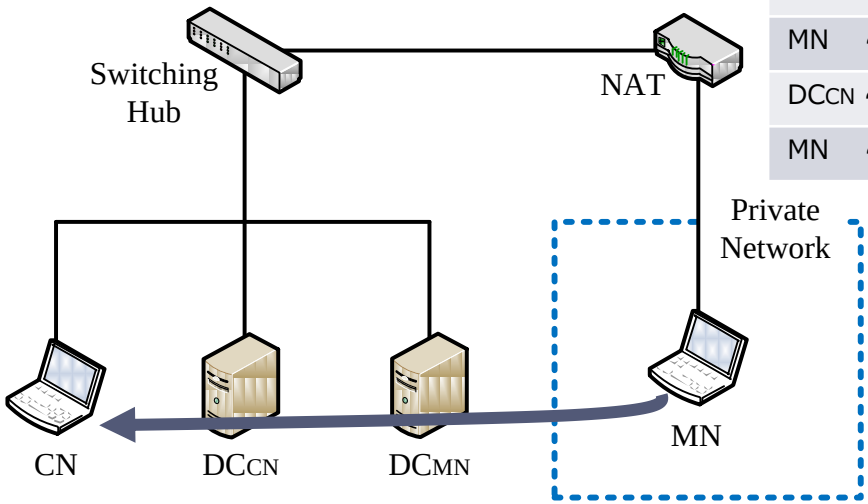
性能測定　（測定方法）

- 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

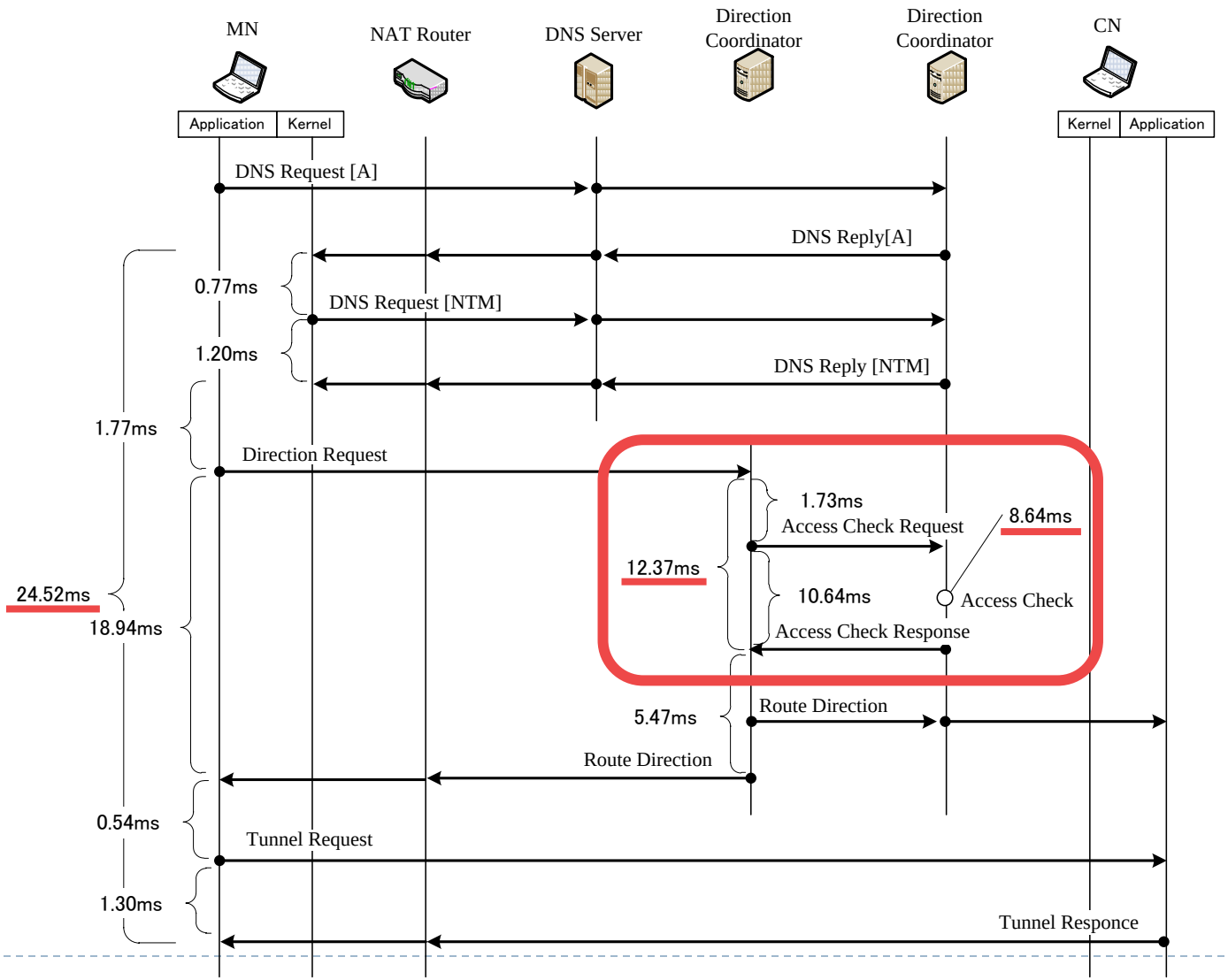
Direction Coordinator (DCMN, DCCN)
OS : Ubuntu 10.04
CPU : Core 2 Duo P9400 2.4GHz
Memory : 2048MB
Ethernet : 1000Base-T

Switching Hub, NAT
Ethernet : 100Base-TX



	RTT[ms]
CN ~ DCCN	0.797
CN ~ DSMN	0.747
MN ~ CN	1.306
DCCN ~ DCMN	0.705
MN ~ DCMN	1.229

性能測定　（測定結果）


MN
NAT Router
DNS Server
Direction Coordinator
Direction Coordinator
CN
Application
Kernel
Kernel
Application
DNS Request [A]
DNS Reply[A]
0.77ms
DNS Request [NTM]
1.20ms
DNS Reply [NTM]
1.77ms
Direction Request
1.73ms
Access Check Request
8.64ms
12.37ms
10.64ms
Access Check
24.52ms
18.94ms
Access Check Response
5.47ms
Route Direction
Route Direction
0.54ms
Tunnel Request
1.30ms
Tunnel Responce