平成23年度　修士論文

邦文題目

NTMobileにおけるグループ認証方式の提案と実装

英文題目

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

情報工学専攻

(学籍番号: 103430037)

村橋　孝謙

名城大学大学院理工学研究科

内容要旨

ユビキタスネットワークの進展に伴い，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．

NTMobile（Network Traversal with Mobility）と呼ばれるシステムを提案している．これ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技術である．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．そこで本論文では 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その有用性を確認した結果，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．

目 次

第1章　序論

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．IPv6 は必要に迫られ徐々に導入されるものの，既存の IPv4 ネットワークはそのまま残ると考えられる．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．通信中に移動することにより，ネットワークが切り替わる可能性がある．このように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である．

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．

これまで通信の接続性と移動透過性を同時に実現する NTMobile（Network Traversal with Mobility）[1–3] を提案してきた．NTMobile では通信パケットを仮想 IP アドレスでカプセル化し，さらに DC（Direction Coordinator）による経路指示と RS（Relay Server）による NTMobile 端末間の中継により接続性と移動透過性を実現する．NTMobile の目的はこのように通信の制約を除去することであり，エンドエンドのセキュリティ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 越え技術 NAT-f [6] を使用するため

に NAT を改造する必要があった.

そこで NTMobile においては，新たにエンドエンドのセキュリティの実現方法として，アクセス制御リスト ACL（Access Control List）を用いてグループ単位での認証を行う方法を提案する．この方式では DC に新たに ACL と呼ぶデータベースを導入し，エンド端末のノード ID と所属グループ名を格納する．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．その成果をもとに IPsec，GSCIP，既存の NTMobile システムおよび提案方式の機能を比較し，有効性を確認する．

以降，2 章で IPsec および GSCIP の課題を述べ，3 章で NTMobile の概要について説明する．4 章では提案方式の詳細を述べ，5 章で実装と評価を行い，最後に 6 章でまとめる．

第2章　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/NAPT を跨る通信を行うことができない．IP アドレスの変換をともなう NAT を通過すると偽造パケットとみなされパケットが破棄されるためである．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．

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なっており，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不可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の混在した通信グループの構築が容易に可能となる．

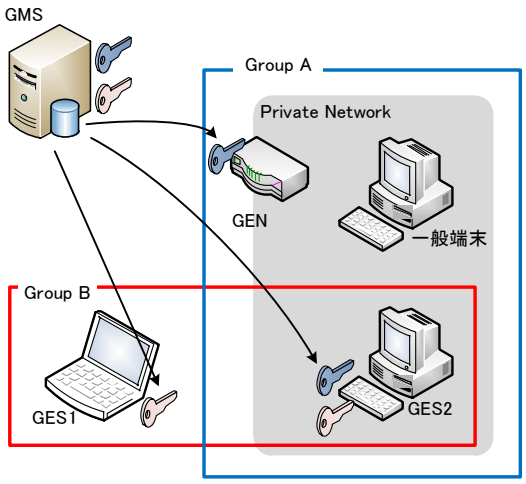

図 2.1　GSCIP 基本構成

GSCIP を用いた通信グループの構成を図 2.1 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 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] によって実現される．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り，基本的に GSCIP ネットワーク全体に対し 1 つの GMS を用意する．そのため複数の組織または互いに無関係なユーザが GMS を共用する場合，セキュリティを維持するため信頼のおける者に GMS の管理を依頼する必要がある．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.

第3章　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 3.1 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．

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，

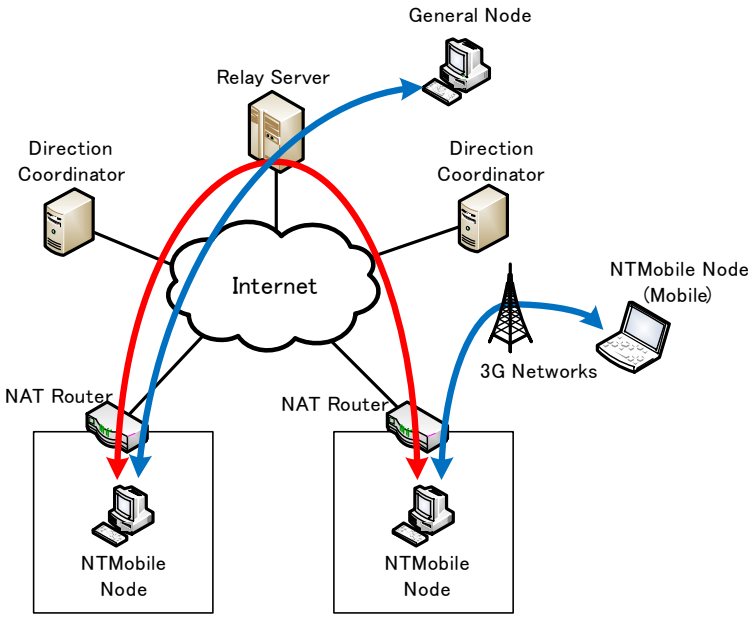

図 3.1　NTMobile の概要

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 を配下にある 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 3.2 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 アドレスを要求する．DNS Response により A レコードの返答を受けると，NTM レコードの問い合わせを行う．

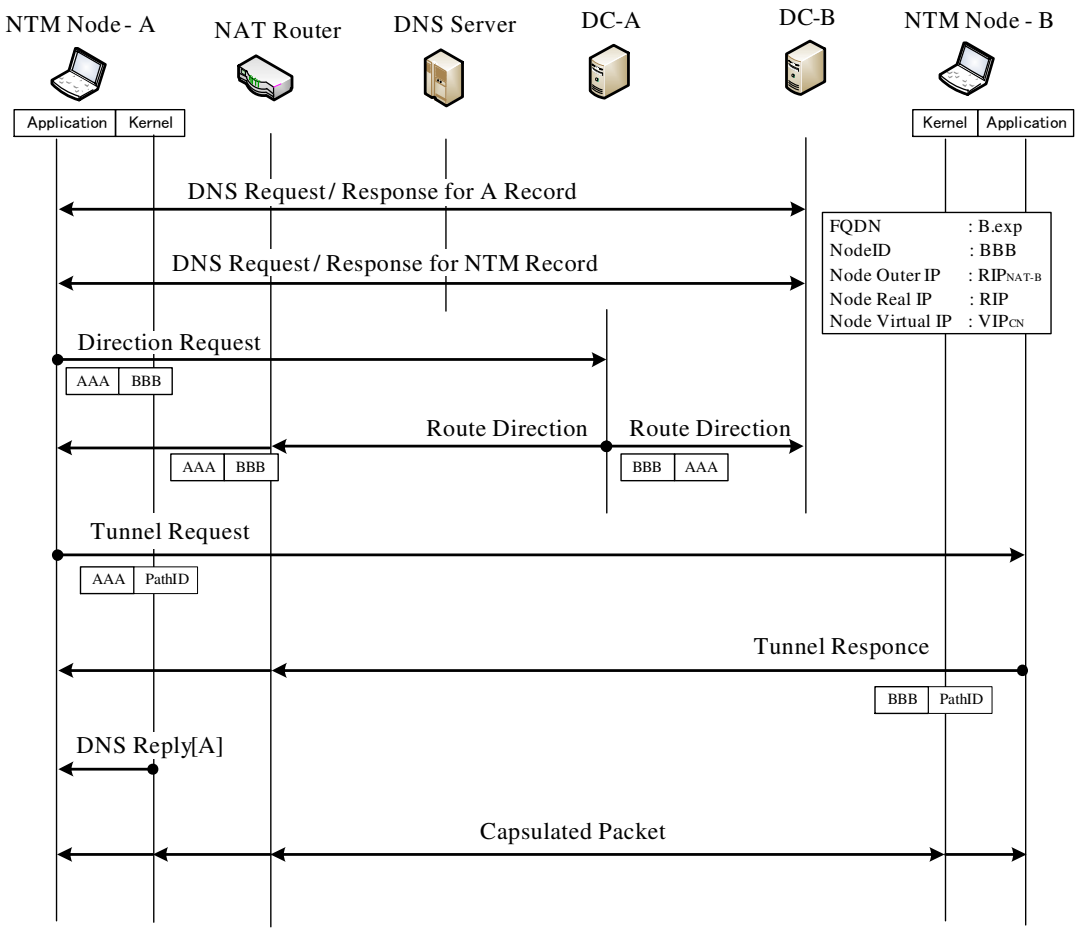

図 3.2　NTM 基本動作例

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 にあらためてに Direction Request を送信し，トンネル構築の指示を待つ．DC-A は Direction Request を受信すると両エンド端末の位置に応じて経路指示応答を送信する．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 IP パケットがカプセル化される．

トンネル構築要求に応じてトンネル構築応答 Tunnel Response を返答されると通信トンネルが構築され，以後の NTMobile 端末の通信時に IP パケットがカプセル化されて送信される．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．

第4章　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．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（必須ではない），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．

GSCIPではシステム全体の管理を行うGMS管理者が必要であるが，ACLはDC内に実装することでシステム全体の管理者が不要となる．ただしDCの管理者は必要である．

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の内容を図4.1に示す．データベースはDCの配下領域内の端末（通信相手側），DCの領域外の端末（通信開始側）それぞれの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の計6つからなる．

- ノード情報テーブル
  各NTMノードのノードIDとホスト名が格納されており，新たにノードIDに対応するインデックス番号（ノードID番号）が付けられる．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，対応するインデックス番号（グループ番号）からなる．

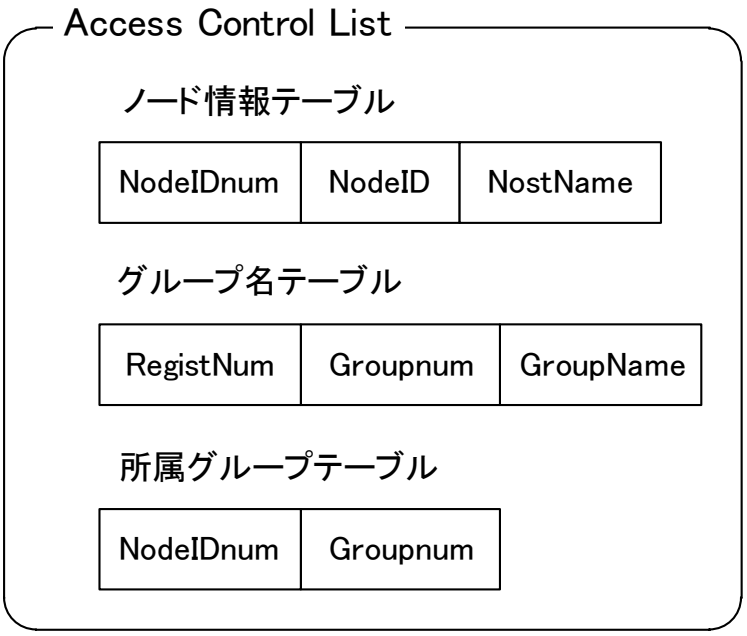

図 4.1　Access Control List

- 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 1 つ毎に 1 行ずつ記述される．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 4.2 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，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

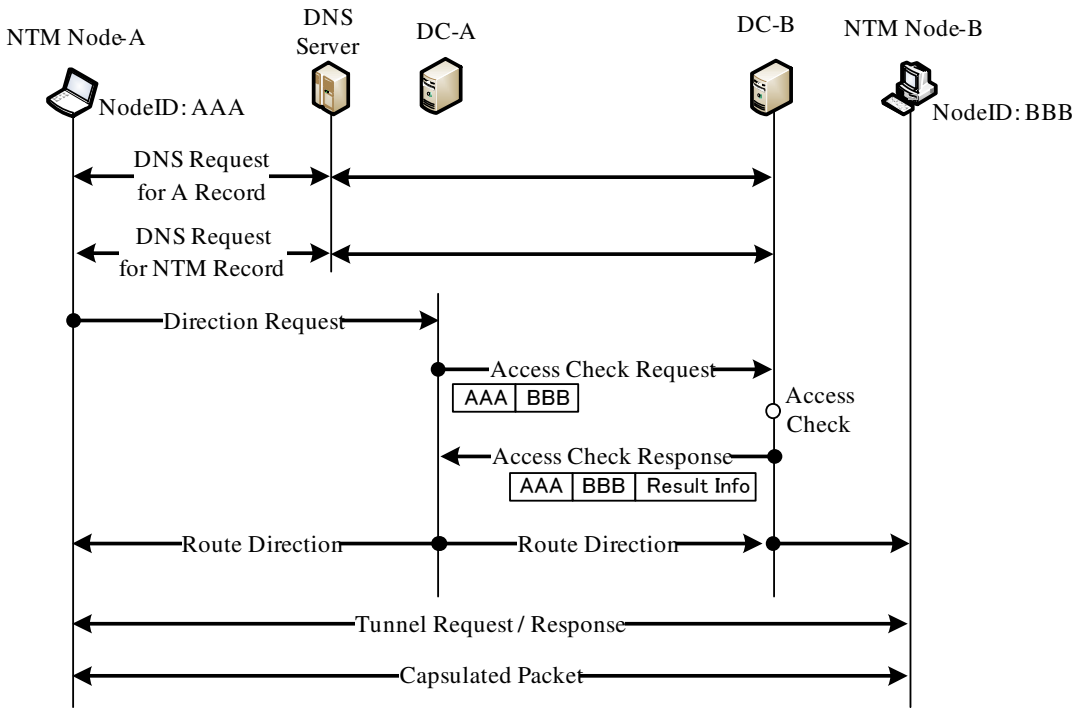

図 4.2　Access Check 動作シーケンス

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．

4.4　ACL の管理

ACL をデータベースの直接操作により管理を行うことは困難である．専用のインタフェースを作成し，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

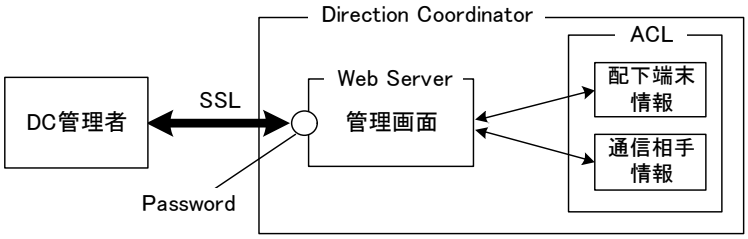

図 4.3　管理者とインタフェースの関係

ループを設定することができる．図 4.3 に管理者および管理インタフェースの関係を示す．ACL を導入した DC は各自の端末に 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．管理システムは DC の配下端末側および通信相手側における，それぞれ端末の情報と所属グループを指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．図 4.4 に管理画面の例を示す．管理画面では，ノード情報の登録時にはまずノード ID およびホスト名を入力する．必要であれば通信グループを新たに登録し，また各ノードの所属グループを指定する．

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容易に定義することができる．

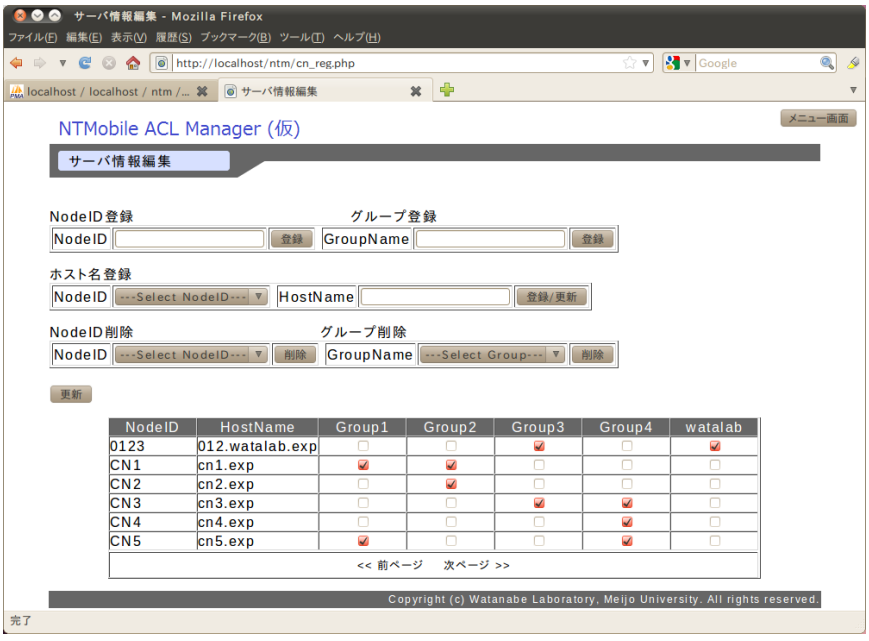

図 4.4　ACL 管理画面

第5章　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う．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．ACL を使用した場合も同様である．

- 完全性保障性
  パケットの改ざんに対する耐性を比較する．IPsec ESP では完全性保証を実現するために IKE と併用する必要がある．また GSCIP では IP ヘッダを含むパケット全体の認証を行うことができる．NTMobile では MAC 値を除くパケットの NTMobile 部分の認証を行うことができる．IP ヘッダおよび UDP ヘッダの認証は行われないが，NTM ヘッダに含まれる送信元ノード ID/パス ID を用いることで送信者を保証することは可能である．

- 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．NTMobile では，通常はアクセス制御自体が不可能である．ACL を用いることでグループ単位のアクセス制御が可能であり，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容易に行うことができる．

- NAT への対応
  IPsec では，NAT-T [9] により IPsec パケットを 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

表 5.1　機能比較結果

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

越えを行うためには NAT-f 技術を用い，NAT を改造する必要がある．それに対し NTMobile では NAT の内側からの通信開始および RS を用いることで NAT の制限を回避することができる．

- 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を継続することができない．MOBIKE [14] を適用することで端末の移動時においてもセッションを維持することができるが，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不可能である．また Mobile IP [15] を使用して移動透過性を解決する場合は特殊な機器を設置する必要がある．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 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しない．NTMobile では仮想 IP アドレスを用いることで IP アドレスの変化に影響しない通信を行うことができる．

NTMobile では IPsec ほどの強固なセキュリティを得ることはできないが，必要十分なだけのセキュリティは備えており，NAT や通信環境に依存しない通信が可能なため比較的広範囲での運用が可能である．

5.2　実装

図 5.1 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 Daemon 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．

ACL 適用方式は現行の NTMobile の追加・修正により実現している．DC において，Direction Request の受信に応じて Access Check Request が出されるよう追加される．さらに Access Check Request の受信に応じて Access Check が行われ，この完了により送信

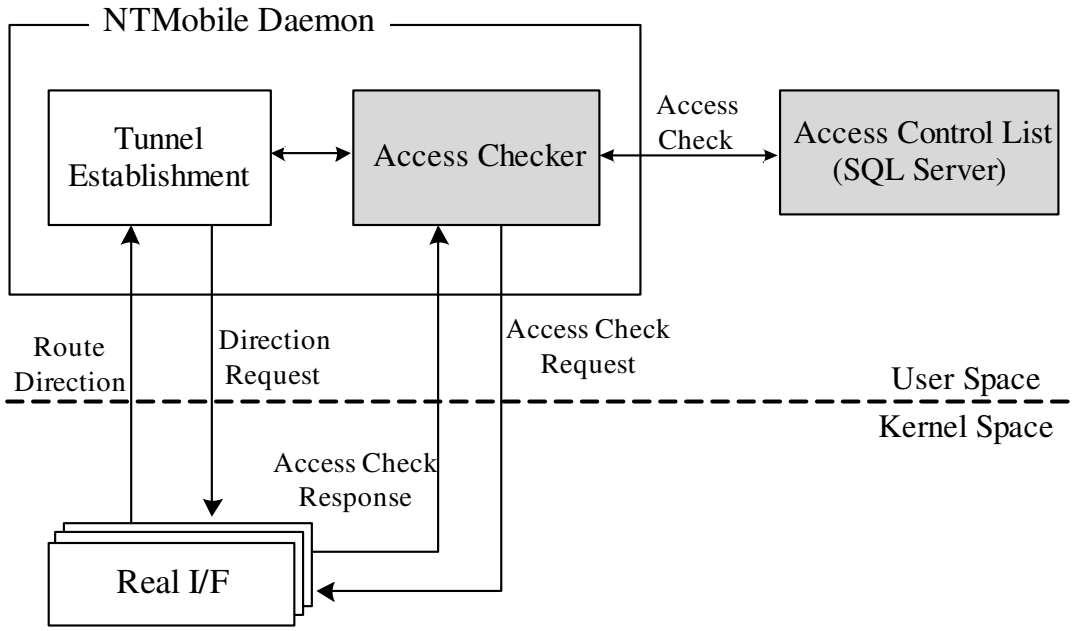

図 5.1　DC のモジュール構成

元 DC へ Access Check Response が返される．また Route Direction のパケット内に Access Check の結果格納，さらに Access Check 結果によって Route Direction が通信開始側のみに返されるよう変更されている．

5.3　性能評価

提案方式においてアクセスチェック処理の追加によるオーバーヘッドを得るため，ACL を適用した NTMobile システムを用いトンネル構築に要する時間を測定した．図 5.2 に試験時のネットワーク構成を示す．NAT 配下に存在する NTMobile 端末 MN がグローバル IP アドレス空間に存在する CN に対しコネクションの確立を行う．各装置の仕様を表 5.2 に示す．また各装置間の RTT を表**??**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，MN 側，CN 側において各 100 台の端末を登録する．MN および CN はそれぞれ 10 のグループに所属しているとする．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 MN および DC_{MN} において Wireshark を用いて計測した．また DC_{CN} 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 5.3 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

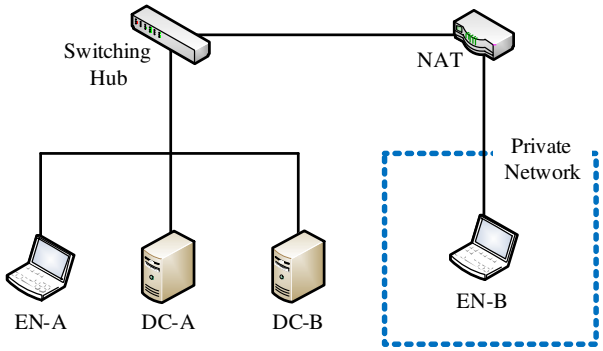

図 5.2　試験時のネットワーク構成

ン処理に要した時間の全体となる．

DC_{MN} 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 MN 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_{CN} へ送信する Route Direction の生成，暗号，MAC 生成処理および送信処理，MN 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．

処理時間全体のうち，約半分をアクセスチェック関係処理が占めている．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ーヘッドの割合は大きいが，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．

[h]

表 5.2　実験機器諸元

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 LSW10/100-16N	—	—	100Base-TX
NAT	Buffalo BBR-4MG	—	—	100Base-TX

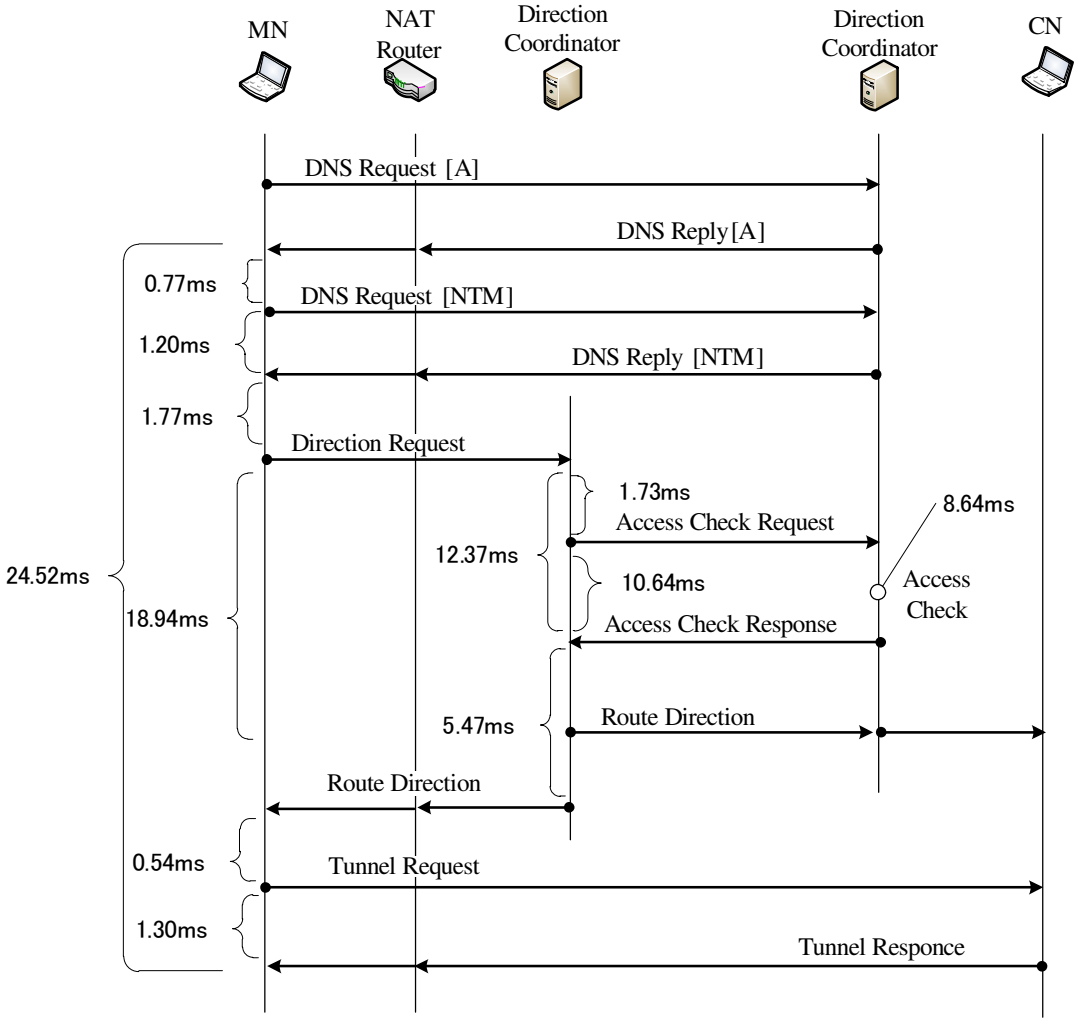

図 5.3　ネゴシエーション時間

第6章　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，これにより NTMobile をより安全なシステムとすることができる．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．

謝辞

本研究を遂行するにあたり，多大なる御指導そして御協力を頂きました，名城大学大学院理工学研究科　渡邊晃教授に心より厚く御礼申し上げます．本研究を遂行するにあたり，多大なる御指導そして御協力を頂きました，名城大学大学院理工学研究科　柳田康幸教授，旭健作助教，鈴木秀和助教，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．本研究を遂行するにあたり，有益なご助言，適切なご検討をいただいた，名城大学理工学部情報工学科渡邊研究室の納堂博史氏，名城大学理工学部情報工学科鈴木研究室の上醉尾一真氏に心より感謝いたします．また本研究を遂行するにあたり，有益なご助言，適切なご検討をいただいた，名城大学理工学研究科情報工学科渡邊研究室の皆様に心より感謝いたします．

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：NTMobilebile 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), RFC 4555, IETF (2006).

[15] C. Perkins, E.: IP Mobility Support for IPv4, RFC 3220, IETF (2002).

研究業績

学術論文

なし

国内会議（査読あり）

1. 村橋孝謙, 鈴木秀和, 渡邊晃 “通信アーキテクチャ CGSCIP の管理運用評価”, マルチメディア, 分散, 協調とモバイル（DICOMO2010）シンポジウム論文集, Vol.2010, No.1，pp.938-943，Jul.2010.

研究会・大会等

1. 村橋孝謙，鈴木秀和，渡邊晃 “通信アーキテクチャ CGSCIP の管理運用評価”，情報処理学会第 72 回全国大会講演論文集，Mar.2010.
2. 村橋孝謙, 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，MBL[モバイルコンピューティングとユビキタス通信研究会研究報告]，Vol.2012-MBL-61, No.34, pp. 1–8 Mar. 2012.