平成26年度　卒 業 論 文

和文題目

NTMobileにおけるNTM端末とDC間の認証強化に係わる検討

英文題目

Researches on strengthening of authentication between NTM terminal and DC in NTMobile

情報工学科　渡邊研究室

(学籍番号: 110425300)

三輪　卓也

提出日: 平成27年2月12日

名城大学理工学部

概要

スマートフォンやタブレットの普及，ネットワークの発展に伴い，相手のネットワーク環境に影響されず通信を開始できる通信接続性と，移動しながら通信ができる移動透過性の要求が高まっている．我々はあらゆるネットワーク環境において移動しながら通信ができる技術として，NTMobile(Network Traversal with Mobility) を提案している．NTMobile ではモバイル端末の認証として，現状ではパスワードを利用しているが，この方法ではパスワードの漏洩などに対処できず，セキュリティ上万全とは言えない．本稿では，その対策として公開鍵証明書をモバイル端末に保持させる方式について提案する．モバイル端末として利用を想定しているスマートフォンは耐タンパ性が保障されていないため，秘密鍵が漏洩する懸念があるが，秘密鍵をパスワードで暗号化することにより，これを防止する．

目 次

第 1 章　はじめに **1**

第 2 章　NTMobile **3**

2.1　NTMobile の構成 3

2.2　NTM 端末の登録方法 4

2.3　NTM 端末の認証方法 5

2.4　利点と課題 5

第 3 章　提案方式 **7**

3.1　登録方法 7

3.2　公開鍵証明書に含まれる情報 8

3.3　認証方法 9

第 4 章　評価 **10**

第 5 章　まとめ **11**

謝辞 **12**

参考文献 **13**

研究業績 **14**

第1章　はじめに

スマートフォンやタブレット等の高性能な携帯端末の普及，Wi-Fi ネットワークやモバイルネットワーク等の様々なネットワークの発展に伴い，相手のネットワーク環境に影響されず通信を開始できることを保証する通信接続性は，ネットワーク技術において極めて重要な要素となっている．通信の最中においても，端末の移動や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，通信を継続することができない．このような問題を解決するため，移動しながら通信ができる移動透過性の技術の要求も高まっている．

また，現在も今後も主要なインターネットプロトコルとして存在し続けるであろう IPv4 は，グローバルアドレスの枯渇問題が最大の課題として挙げられる．そこで，NAT(Network Address Translation) を経由し，家庭内や企業内でプライベートアドレスのネットワークを構築し，この課題の解決が図られてきた．しかし，グローバルネットワーク側からプライベートネットワーク側に対して通信を開始できないという NAT 越え問題が新たに生じ，通信接続性が確保できない課題へと直結している．NAT 越え問題を解決する技術としては，[1]，[2]，[3] 等が提案されてきたが，いずれも端末の移動を考慮しておらず，移動透過性の要求を満たすことはできていない．

一方で，移動透過性の技術を実現するためにも様々な研究が行われてきたが，IPv6 対応の方式 [4]，[5]，[6] 等が主流であった．今後も IPv4 が主流となることを考慮すると，IPv4 ネットワーク上で移動透過性を実現する技術が要求される．そのため，[7]，[8]，[9]，[10] 等の IPv4 対応の研究も行われてきたが，NAT が存在するためにそれぞれ課題を抱えており，どれも現実的な技術を実現するには至っていない．

我々は，あらゆるネットワーク環境において移動しながら通信ができる技術として，NTMobile(Network Traversal with Mobility)[11]，[12]，[13]，[14] を提案している．NTMobile では，仮想 IP アドレスの導入とトンネル技術を用いることにより，移動透過性を実現する．各通信端末に一意な仮想 IP アドレスが割り当てられ，アプリケーションはこのアドレスに基づいて通信を行う．実際には仮想 IP アドレスに基づくパケットを実 IP アドレスによりカプセル化し，実 IP アドレスの変化をアプリケーションに対して隠蔽することによってこれを実現している．また，NTMobile は，DC(Direction Coordinator) と RS(Relay server) と呼ぶ装置をグローバルネットワーク上に設置するのみで IPv4 における NAT の制約を受けず，通信接続性と移動透過性を同時に実現することが可能である．

NTMobile を普及させるにあたり，万全なセキュリティを確保することは必要不可欠なことである．インターネットの普及に伴いサイバー犯罪が問題となっていることは事実であり，各種対策が求められる．中でも不正アクセスによる犯罪は増加傾向にある．そこで，本稿では NTMobile における各通信機器間の認証方法に着目し，安全性が低い箇所により確実な方法を提案することに

よってセキュリティ強化を図る．

以降，2 章で NTMobile の構成と各通信機器間のセキュリティについて触れ，モバイル端末の認証方法の課題について述べる．3 章で提案方式について，モバイル端末の登録方法から認証方法まで詳細に述べる．4 章で提案方式の評価をし，5 章でまとめる．

第2章　NTMobile

2.1　NTMobile の構成

図 1 に NTMobile の構成を示す．NTMobile は，NTMobile の機能を実装した端末 (NTM 端末) と NTM 端末の管理や通信経路の指示を行う Direction Coordinator(DC)，必要に応じて通信を中継する Relay Server(RS) から構成される．DC と RS は最上位 DC である rootDC から公開鍵証明書が発行されており，DC 同士及び DC と RS 間で行われる通信は，あらかじめ共有した共通鍵を用いて暗号化される．NTM 端末はアカウント取得時にパスワードを DC に登録することで DC との信頼関係を構築する．

NTM 端末は接続先の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 種類のアドレスを保持している．仮想 IP アドレスは NTM 端末が接続先のネットワークを切り替えても変化しない一意なアドレスであり，各 DC が管理下の NTM 端末に重複しないよう割り当てを行う．仮想 IP アドレスに基づくパケットを実 IP アドレスによりカプセル化し，実 IP アドレスの変化をアプリケーションに対して隠蔽することによって移動透過性を実現している．DC が NTM 端末の移動パターンに応じた通信経路やトンネル構築の指示を行うことで，様々な状況における移動透過性を実現可能である [2]．RS は，異なる NAT 配下に存在する NTM 端末同士の通信の場合と，通信相手が NTMobile に対応していない一般端末である場合に通信を中継し，IPv4 と IPv6 間の通信時にも使用される．

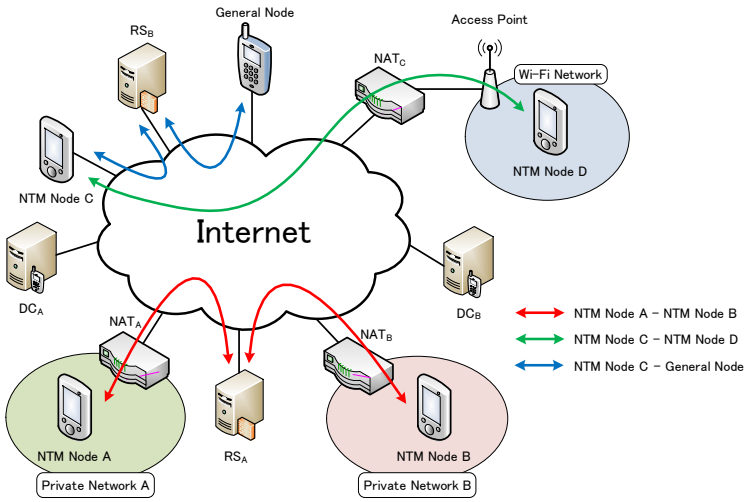

図 1　NTMobile の構成

2.2　NTM 端末の登録方法

図 2 に現状の NTM 端末の登録シーケンスを示す．NTM 端末には予め使用する DC の FQDN が登録されていることを前提とする．ユーザは NTMobile のアカウント作成用アプリケーションを起動し，アカウントサーバ (AS) に接続する．初めにメールアドレス (Login ID) とパスワードの入力が要求される．これらの情報の入力が完了すると，NTM 端末は SSL 通信により AS を認証するとともに共通鍵を共有し暗号化通信を開始する．Create User Request のメッセージとともに Login ID とパスワードを AS に送信する．AS はこれらを受け取ると，ユーザのメールアドレス宛てにタイムスタンプとパスワードのハッシュを送信し，ユーザがメール内に記載されている URL をクリックすることにより本人確認を行う．本人確認が完了すると，AS は NTM 端末の FQDN を生成し，登録要求を行った NTM 端末の Login ID とパスワードと共に自身のテーブルに保存する．AS が Login User Response のメッセージとともに NTM 端末の FQDN を送信し，NTM 端末がこれを保存することで登録は完了となる．

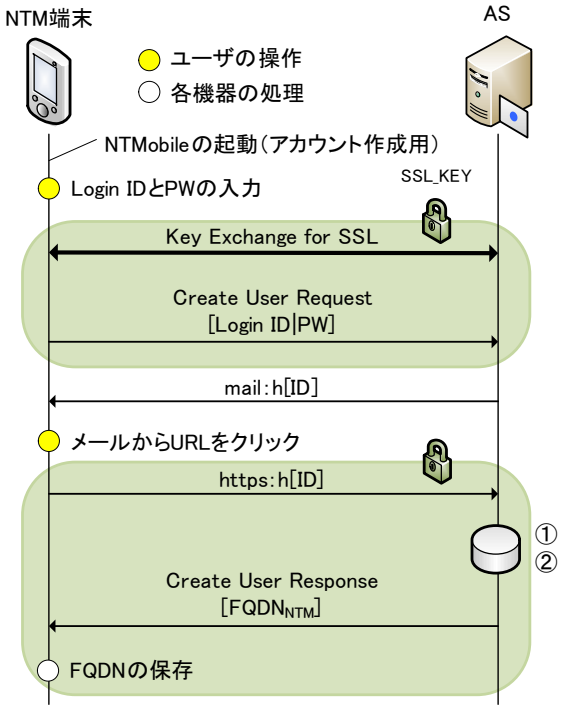

図 2　NTM 端末登録シーケンス

2.3　NTM 端末の認証方法

図 3 に現状の NTM 端末の認証シーケンスを示す．DC と AS は信頼関係が構築されていることを前提とする．ユーザがログイン画面より Login ID と PW を入力すると，NTM 端末は通常の SSL 通信により DC を認証するとともに共通鍵を共有する．その後，NTM 端末は入力された Login ID と PW 及び FQDN を DC に対して送信する (Login Request)．このメッセージを受け取った DC は AS に問い合わせ (Authentication Request) を行う．AS は DC から受け取ったログイン情報から NTM 端末を認証する．認証が完了すると，乱数 Authtoken を生成し，DC に対して応答 (Authentication Response) を返す．Authtoken は次回以降の認証で AS への問い合わせを省略するために利用される．DC は Authentication Response を受け取ると，NTM 端末との共通鍵 $CK_{NTM\text{-}DC}$ を生成し，NTM 端末の FQDN と共に Node Info Table に登録する．その後，DC は Login Response により $CK_{NTM\text{-}DC}$ と Authtoken を配布する．以後の NTM 端末と DC との間の全ての通信において，暗号鍵に $CK_{NTM\text{-}DC}$ を，認証鍵に Authtoken を利用する．

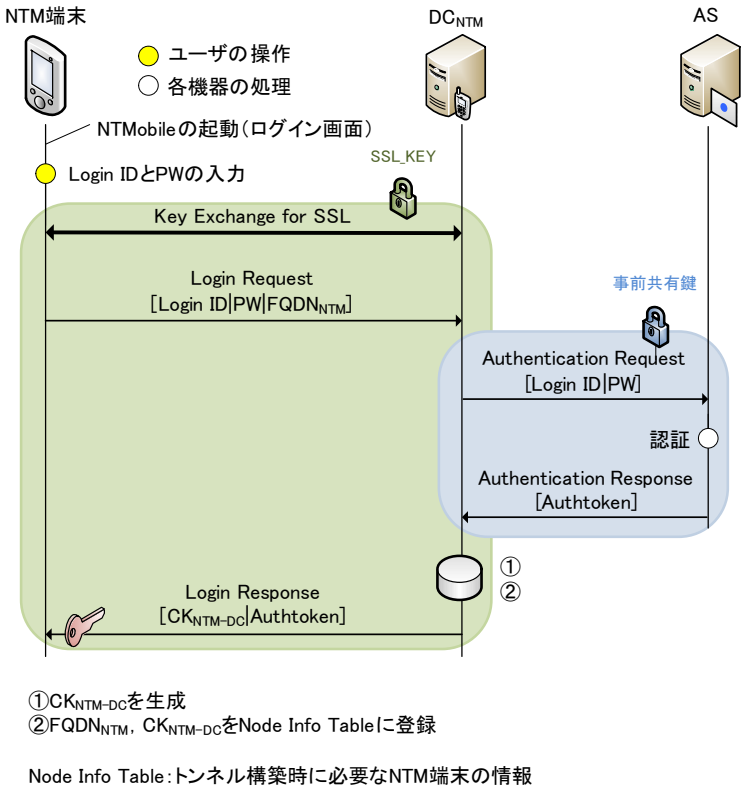

図 3　NTM 端末認証シーケンス

2.4　利点と課題

現状の方法における利点は，ユーザが ID とパスワードを設定する簡単な操作のみで，安全に DC との共通鍵及び認証鍵を共有し，信頼関係を構築できる点にある．しかし，課題として，パス

ワードが漏れると他の端末からもログインできるため安全性が低いことが挙げられる．また，辞書攻撃 *1 への耐性がないため，予測されやすいパスワードを設定しているユーザはパスワードを解析される恐れがある．このため，DC 側が NTM 端末を認証する際の安全性に懸念がある．

*1辞書（ファイル）に載っている単語を片っ端から試行し，パスワードを解析する手法

第3章　提案方式

節 2.4 に挙げた課題を解決するために，公開鍵証明書を NTM 端末に保持させる方式について提案する．DC のみに発行していた公開鍵証明書を NTM 端末にも持たせることで双方向の確実な認証を行う．NTM 端末が保持する秘密鍵はユーザのパスワードで暗号化する．ユーザがログインするには所定の NTM 端末を保持し，かつパスワードを知っている必要があり，安全性が高まる．従来の方式との互換性維持も考慮しており，ユーザ目線からは認証方法に大きな変化がないという特徴がある．

3.1　登録方法

図 4 に提案方式の登録シーケンスを示す．NTM 端末には予め使用する DC の FQDN が登録されていることを前提とする．ユーザは NTMobile のアカウント作成用アプリケーションを起動し，アカウントサーバ (AS) に接続することで登録を行う．NTM 端末は SSL 通信により AS を認証するとともに共通鍵を共有し暗号化通信を開始する．ここで NTM 端末側で自身の秘密鍵/公開鍵ペアを生成する．メールアドレス (Login ID) とパスワード，及び個人情報の入力が要求される．個人情報は公開鍵証明書の発行審査に利用される．個人情報には氏名，団体名 (会社名)，住所，電話番号がある．これらの情報の入力が完了すると，生成された秘密鍵をパスワードで暗号化し，NTM 端末に保存する．NTM 端末の公開鍵と入力された情報のうちの Login ID と個人情報が AS に送信される (Create User Request)．AS はこれらを受け取ると，ユーザのメールアドレス宛てにタイムスタンプと Login ID のハッシュを送信する．ユーザはメール内に記載されている URL をクリックすることにより本人確認を行う．本人確認が完了すると，個人情報を基に公開鍵証明書の発行審査が行われる．審査の過程で，電話による直接確認も場合によっては行われる．審査が通ると，AS から公開鍵証明書と FQDN が発行され，Create User Response のメッセージとともに，NTM 端末の FQDN が送信される．公開鍵証明書はユーザのメールアドレス宛てに送信され，ユーザがこれを NTM 端末に保存することで登録手続きは完了となる．

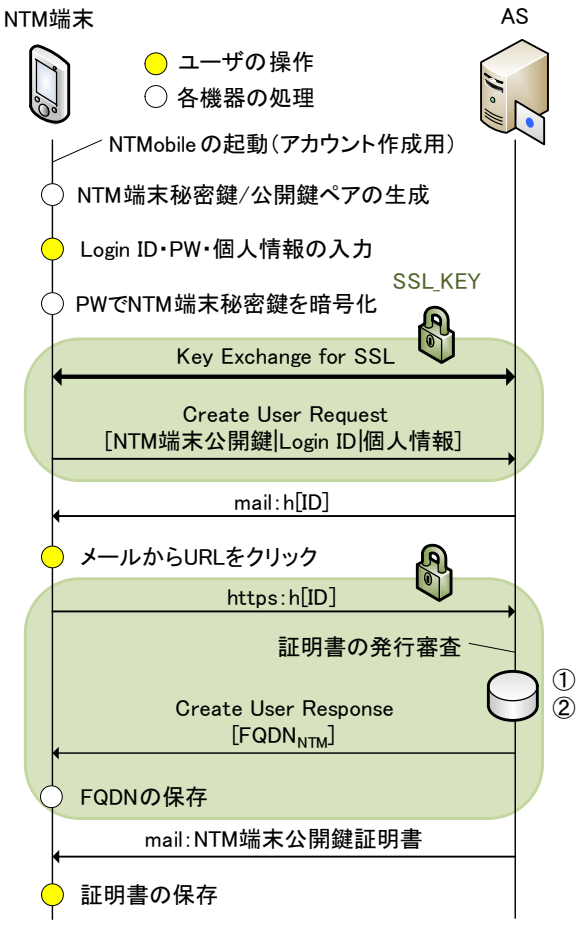

図 4　提案方式の登録シーケンス

3.2　公開鍵証明書に含まれる情報

表 1 に公開鍵証明書に含まれる情報を示す．AS の公開鍵を用いて，証明書に含まれる AS の署名を検証することによって，偽装及び改ざん検知を行う．

表 1　公開鍵証明書に含まれる情報

情報	説明
ユーザの識別情報	ユーザの Login ID，FQDN，個人情報
AS の識別情報	NTM 端末の認証局にあたる AS の IP アドレス，FQDN
NTM 端末公開鍵	それ自体
有効期限	証明書の有効期限を示す情報
AS の署名	証明書の内容のハッシュを AS の秘密鍵で暗号化したもの

3.3　認証方法

図 5 に提案方式の認証シーケンスを示す．DC は予め AS の公開鍵証明書を保持しているものとする．ユーザはログイン画面より Login ID とパスワードを入力する．NTM 端末はまず秘密鍵をパスワードで復号する．次に SSL 通信により DC を認証するとともに共通鍵を共有し，暗号化通信を開始する．NTM 端末は秘密鍵を用いて Login ID と FQDN，自身の公開鍵証明書と共に電子署名 ($PriKey_{NTM}[h[ID]]$) を生成して DC に Login Request を送信する．これを受け取った DC は AS の公開鍵を用いて，NTM 端末の公開鍵証明書の検証を行う．AS によって発行された正規なものであることが確認されると，証明書に含まれる NTM 端末の公開鍵を用いて，電子署名 ($PriKey_{NTM}[h[ID]]$) を検証することにより NTM 端末を認証する．電子署名 ($PriKey_{NTM}[h[ID]]$) の検証は，それ自身を公開鍵によって復号した NTM 端末側のものと，DC 側が NTM 端末から送信された情報を基に生成した 2 つのダイジェストを比較することにより行う．NTM 端末の認証が完了すると，DC は共通鍵 $CK_{NTM\text{-}DC}$ と Authtoken を生成し，Login Response のメッセージとともに NTM 端末に配布する．$CK_{NTM\text{-}DC}$ 及び Authtoken とはこれまでと同じように，以後の NTM 端末と DC との間の全ての通信における暗号鍵と認証鍵にそれぞれ利用する．

このように，最後まで正常にシーケンスが流れ NTM 端末が Login Response を受け取ることで認証が完了する．ログイン情報を入力した時点では認証は行われず，電子署名 ($PriKey_{NTM}[h[ID]]$) の検証までシーケンスは必ず流れるという特徴がある．これにより，総当たり的にパスワードを試行する種の攻撃によるパスワード解析を防ぐことができる．

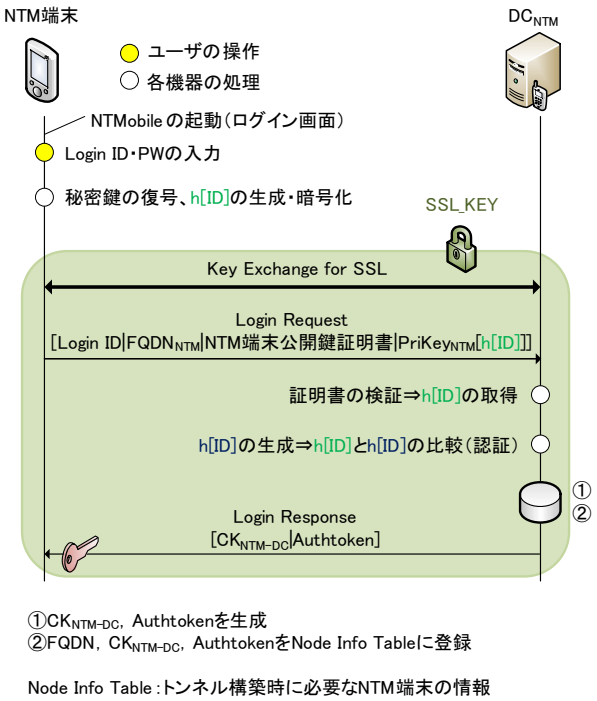

図 5　提案方式の認証シーケンス

第4章　評価

表 2 に NTMobile における現状の認証方式と提案する認証方式のセキュリティ脅威への耐性を示す.

不正ログインについて，現状の方式ではパスワードが漏れた場合，任意の端末からログインすることが可能なので，△とした．これに対して提案方式では，公開鍵証明書による端末認証を行っているので，所定の端末以外ではログインすることは不可能であり，○とした.

総当たり攻撃について，現状の方式ではパスワードの一致・不一致によるワンステップの認証を行っているので，攻撃を仕掛けることが容易であり，単純なパスワードを設定している場合に解析される恐れがあるので，△とした．これに対して提案方式では，最後までシーケンスが正常に流れることで認証を行っているため，この攻撃による解析は現実的ではなく，○とした.

辞書攻撃について，現状の方式ではパスワードはハッシュ関数によって圧縮され，端末内に保持される．この情報が漏洩すると，辞書攻撃を仕掛けることが可能であり，推測されやすいパスワードを設定している場合に解析される恐れがあるので，△とした．これに対して提案方式では，パスワードは端末内に保持されることはないため，攻撃を仕掛けることが不可能であり，○とした.

このように提案方式は，各種セキュリティ脅威への耐性は優れていると言えるが，クライアントごとに公開鍵証明書を発行する必要があるので，管理が面倒になるという欠点がある．また，証明書の発行審査等の影響で，従来の NTM 端末のアカウント登録処理に比べ時間を要する．このため，企業等 DC を独自に導入し管理するようなシステムでは，提案方式が有用であると言える.

表 2　NTMobile における各認証方式の各種脅威への耐性

各種脅威	現状の方式	提案方式
不正ログイン	△	○
総当たり攻撃	△	○
辞書攻撃	△	○

第5章　まとめ

本稿では，NTMobile における NTM 端末と DC 間のセキュリティをより強化した認証方法について提案した．提案方式では，NTM 端末の保有者でかつパスワードを知っているユーザのみが DC との信頼関係を構築できることを示した．パスワードは秘密鍵を復号するためだけに使用されるので，どこにも保管されず送信もされない．ユーザの頭の中に留まるのみという点でセキュリティ性がより向上していると言える．従来の方式との親和性も保たれており，ユーザ目線からは認証の流れに大きな変化がないことも特徴であり，提案方式を従来の方式に追加することでユーザがどちらの方式を使用するか選択できる方法を採ることが可能である．

今後は提案方式の実装を行い，性能評価を行う予定である．

謝辞

本研究を遂行するにあたり，多大なる御指導と御教授を賜りました，名城大学理工学研究科渡邊晃教授には心から感謝致します．また，本研究を進めるにあたり，数々の有益な御意見ならびに御助言を賜りました，渡邊研究室および鈴木研究室の諸氏に感謝します.

参考文献

[1] 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).

[2] Rosenberg, J.: Interactive Connectivity Establishment (ICE): A Protocol for Network Address Translator (NAT) Traversal for Offer/Answer Protocols, RFC 5245, IETF (2010).

[3] Westerlund, M. and Perkins, C.: IANA Registry for Interactive Connectivity Establishment (ICE) Options, RFC 6336, IETF (2011).

[4] 相原玲二，藤田貫大，前田香織，野村嘉洋 : アドレス変換方式による移動透過インターネットアーキテクチャ，情報処理学会論文誌，Vol.43，pp.3889.3897 (2002).

[5] Perkins, C., Johnson, D. and Arkko, J.: Mobility Support in IPv6, RFC 6275, IETF (2011).

[6] Ishiyama, M., Kunishi, M., Uehara, K., Esaki, H., and Teraoka, F.:LINA : A New Approach to Mobiity Support in Wide Area Networks, IEICE Trans. Commun. Vol.E84-B, pp.2076-2086 (2001).

[7] 関　顕生，岩田裕貴，森廣勇人，前田香織，近堂徹，岸場清悟，西村浩二，相原玲二 : IPv4 拡張した移動透過通信アーキテクチャMAT の設計と性能評価，情報処理学会論文誌，Vol.52，No.3，pp.1323.1333 (2011).

[8] 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).

[9] Montenegro, G.,Reverse Tunneling for Mobile IP, revised, RFC3024, IETF (2001).

[10] Levkowetz, H., and Vaarala, S.,:Mobile IP Traversal of Network Address Translation (NAT) Devices, RFC3519, IETF (2003).

[11] 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).

[12] 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).

[13] 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).

[14] 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，情報処理学会論文誌，Vol.54，No.10，pp.2288-2299 (2013).

研究業績

研究会・大会等（査読なし）

（1）三輪卓也，鈴木秀和，内藤克浩，渡邊晃：NTMobile における NTM 端末の認証方法の強化，平成 26 年度電気・電子・情報関係学会東海支部連合大会論文集，Sep. 2014.