Mobile PPC における認証方式の提案

瀬下　正樹

モバイル端末の普及と，無線ネットワーク環境の広がりにより，端末が自由に移動しながらインターネットに接続するという利用形態が増えつつある．そのような状況下では，端末が移動しても通信を継続することが要求されるが，移動に伴い IP アドレスが変化するため，この要求を満たすことが難しい．そこで，端末の移動による IP アドレスの変化を隠蔽し，通信を継続できるようにする移動透過性の研究が盛んに行われている．我々は，移動透過性の一方式として，特別な位置管理エージェントを不要とし，P2P で移動透過性を実現する Mobile PPC の研究を行っている．しかし，これまでの Mobile PPC には移動ノードが移動した際に通信相手ノードとの間で成りすましを防止するための認証機構が定義されていなかった．そこで，本研究では Mobile PPC における認証方式についての提案を行う．

Proposal of Authentication Mechanisms in Mobile PPC

Masaki Sejimo

The demand for ubiquitous networking is increasing. Under such a situation, it is demanded to keep communicating even if the mobile node change their location. However, it is difficult to meet this demand because IP addresses change by the mobile node move. That's why mobility that can continue communications by concealing the change in IP addresses is actively studied. We are studying Mobile PPC that achieves mobility by P2P. However, the authentication mechanisms when moving between the mobile node and the correspondent node was not defined in current Mobile PPC. I propose the authentication mechanisms in Mobile PPC for that reason.

1　研究背景

ノートパソコンや PDA(Personal Digital Assistant)などのモバイル端末の普及と，無線ネットワーク環境の広がりにより，端末が自由に移動しながらインターネットに接続するという利用形態が増えつつある．そのような状況下では，端末が移動しても通信を継続することが要求されるが，既存のインターネットアーキテクチャでは移動に伴い IP アドレスが変化するため，この要求を満たすことが難しい．そこで，端末の移動による IP アドレスの変化を隠蔽し，通信を継続できるようにする移動透過性[1]の研究が行われている．

ネットワーク層における移動透過性保証プロトコルとして Mobile IP[2],[3]，LIN6(Location Independent Networking for IPv6)[4],[5]などが提案されているが，Mobile IP では Home Agent(以下 HA)，LIN6 では Mapping Agent(以下 MA)と呼ばれる特殊なネットワーク機器を用意する必要があり，導入するための敷居が高い．我々は，これらの特殊なネットワーク機器を必要とすることなく，P2P で移動透過性を実現する Mobile PPC(Mobile Peer to Peer Communication)[6]の研究を行っている．

Mobile PPC では，通信中に移動ノード（以下 MN）の IP アドレスが変化すると，その直後に MN から通信相手ノード（以下 CN）に対して，移動後の IP アドレスを Binding UPDATE(以下 BU)により通知する．BU により，エンド端末間では新旧 IP アドレスの対応関係を示すテーブルが作成され，以後の通信ではパケット送受信時に IP 層でこのテーブルを参照してアドレス変換を行う．これにより，TCP/IP プロトコルスイートを含む上位ソフトウェアに対し IP アドレスの変化を隠蔽し，通信を継続させることができる．BU 受信の際にはセキュリティの観点から MN を確実に認証する必要があるが，これまでの Mobile PPC には認証機構が定義されていなかった．

インターネットにおいて，端末間で認証を行う方法として，共有鍵暗号を利用する方式と公開鍵暗号を利用する方式がある．共有鍵暗号を利用する方式は，認証したい相手端末と共有鍵を事前に設定しておく必要がある．しかし，CN と通信する MN は任意であるため，一般的にこのような設定をしておくことは難しい．公開鍵暗号を利用した認証は，PKI のしくみを適用することで認証が可能であるが，現在の PKI が未整備である状況を考慮すると現実的でない．このため，端末間の認証では，CN と MN 間において認証に使用する鍵を，いつ，どのようにして安全に交換するかが

解決すべき課題となる．この課題の解決を行うための認証機構として IPv6 の Return Routability と，それと同様の手法を LIN6 に適用した方式[7]が提案されている．しかし Return Routability では HA，LIN6 では MA のような第三の機器を利用するため，特殊なネットワーク機器を使用しない Mobile PPC において，これらの認証機構は適していない．

そこで本稿ではエンド端末間のみで実現可能な Mobile PPC に適した認証方式の提案を行う．

以下，第 2 章では移動透過性保証プロトコルの既存技術の代表として Mobile IP の通信方式とその課題を説明し，第 3 章で Mobile IPv6 の認証機構として導入されている Return Routabiliy とその課題を説明する．そして，第 4 章で我々が研究を行っている Mobile PPC の利点と課題，第 5 章で Mobile PPC における認証方式として提案方式の説明を行い，第 6 章で実装， 7 章で評価，8 章でむすびについて述べる．

2 Mobile IP

2. 1 Mobile IPv4

2. 1. 1 Mobile IPv4 の概要

Mobile IPv4 は IPv4(IP version 4)において移動透過性を保証する．Mobile IPv4 では，MN はノード固有の IP アドレスであるホームアドレスと移動先で割り当てられる気付けアドレスの二つの IP アドレスを持つ． MN は気付けアドレスが変わるとホームアドレスの属するネットワークに接続された HA へホームアドレスと気付けアドレスの対応関係を登録する．

登録の際，セキュリティの観点から HA は MN を認証する必要があるが，静的な関係である HA と MN の間に事前に共有鍵を保持させておき，この共有鍵を使った認証を行う．

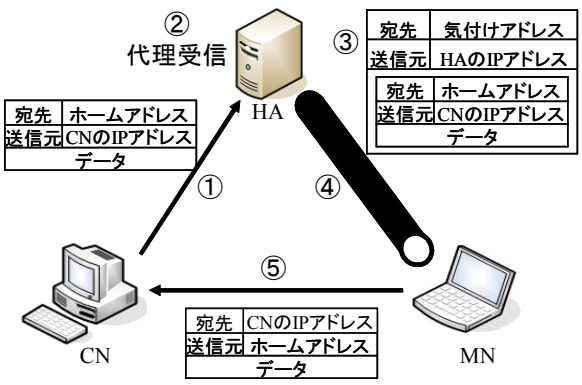

図 1．Mobile IP の通信

Mobile IP によるデータ通信を図 1 に示す．CN は MN へパケットを送信する場合は，宛先を MN のホームアドレスとして送信する（①）．ホームアドレス宛のパケットは HA が受信する（②）．HA は MN から常に最新の気付けアドレスの通知を受けているため，ホームアドレス宛のパケットの宛先を知ることが可能となる（③）．この際，HA は MN にパケットが CN から送信されているように見せかけるためにトンネリング処理を行う（④）．MN から CN へのパケットは送信元をホームアドレスとして CN に直接送信する（⑤）．しかし，送信元アドレスとして使われるホームアドレスがインターネット内での位置を正しく表していないため，途中のルータで不正パケットと見なされ破棄されてしまう可能性があり，このような場合は HA を経由するトンネリング処理を行う必要がある．

2. 1. 2 Mobile IPv4 の問題点

Mobile IP の問題点は，HA という特殊な装置が必要であり導入するための敷居が高いということと，HA を経由した冗長な通信経路になることが挙げられる．また HA は複数設置することができないため，HA による一点障害の危険がある．

2. 2 Mobile IPv6

2. 2. 1 Mobile IPv6 の概要

Mobile IPv6 は IPv6(IP version 6)において移動透過性を保証する．Mobile IPv6 は Mobile IPv4 の考え方に基づいて設計されており，基本的な動作は同じだが， Mobile IPv4 での課題の一つである通信経路の冗長を解決するために CN と MN が直接通信する経路最適化機能が追加された．経路最適化機能は CN にもホームアドレスと気付けアドレスの対応関係を保持させ，IP 層において対応表と拡張ヘッダを利用したアドレス変換を行うことによって移動性を可能にしている．

CN が対応表を保持していない保持していないときは図 1 と同様の手順で通信が行われる．

2. 2. 2 Mobile IPv6 におけるセキュリティ

MN から HA および CN へホームアドレスと気付けアドレスの対応関係を登録する際，セキュリティの観点から HA および CN は MN を認証する必要がある．HA が MN を認証する場合は，静的な関係である両端末間で事前に共有鍵を保持させておくことにより IPsec[8]を用いた認証を行う．CN が MN を認証する場合は，後述する Return Routability を用いて認証を行う．

2. 2. 3 Mobile IPv6 の問題点

Mobile IPv6 は通信経路の冗長の問題は解決されているが，通信初期の数パケットや登録の際の認証において HA を使用するため，導入するための敷居が高いということと， HA による一点障害の問題がある．また，拡張ヘッダの追加によりヘッダオーバヘッドが発生する．

3 Return Routability

3. 1 Return Routability の概要

Return Routability は Mobile IPv6 で導入されている認証機構である．Return Routability は MN と HA 間の信頼関係を利用することと，共有鍵となる情報を二つに分解しそれぞれ異なる経路から配送することにより MN と CN 間で共有鍵を登録直前に保持させ，登録時にこの共有鍵を使用した認証を行う．Mobile IPv6 では通信開始時において CN を送信元としたパケットが HA を経由して MN へ送られた場合と，MN が移動し IP アドレスが変化した場合に MN から CN へ登録パケットが送信され，そのたびに Return Routability が実行される．

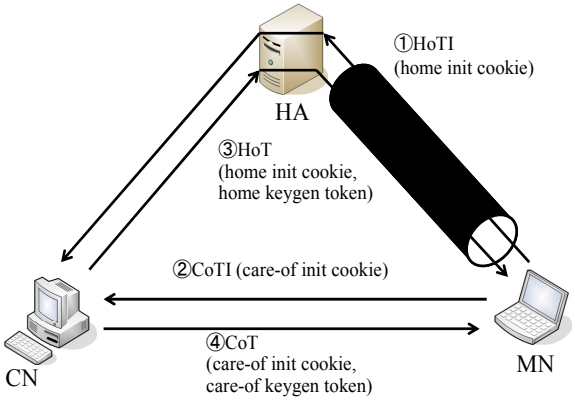

図 2. Return Routability の動作

Return Routability の動作を図 2 示す．ここで，MN と HA 間は IPsec を使用し安全な通信路で通信をする．MN は CN へ Home Test Init (以下 HoTI)（①）と Care-of Test Init (以下 CoTI)（②）を同時に送信する．これらのパケットには HoTI と CoTI に対する CN からの応答を認証するために HoTI には home init cookie，CoTI には care-of init cookie と呼ばれる乱数が含まれる．HoTI は HA を経由し，MN と HA 間は IPsec で保護され HA へ送られる．CoTI は平文のまま CN へ送信される．

CN は HoTI と CoTI の二つの Test Init を受信したら，組み合わせると CN と MN の共有鍵になる home keygen token と care of keygen token を生成し，MN へ HoT(③)と CoT(④)を同時に送信する．HoT には MN から受け取った home init cookie と自身が生成した home keygen token，CoT には MN から受け取った care -of init cookie と自身が生成した care of keygen token が含まれ，HoT は HA を経由し HA と MN 間は IPsec で保護され MN へ送信される．CoT は平文のまま MN へ送信される．

MN は CN から HoT と CoT を受信すると，そこに含まれる Home Init Cookie と Care of Init Cookie を検証し CN の認証を行う．CN を認証した MN は CN から受信した home keygen token と care of keygen token から共有鍵を作成し，この共有鍵によって認証データを生成する．MN は登録パケットに，この認証データを付加し CN へ送信する．

登録パケットを受信した CN は認証データの検証を行い登録パケットの認証を行う．

3. 2 Return Routability の課題

Init cookie の組で MN は CN の認証を行い，kegen token の組で CN は MN の認証を行っているため，Init Cookie の組 や kegen token の組 を攻撃者が得ることができれば CN や MN へのなりすましが可能となる．

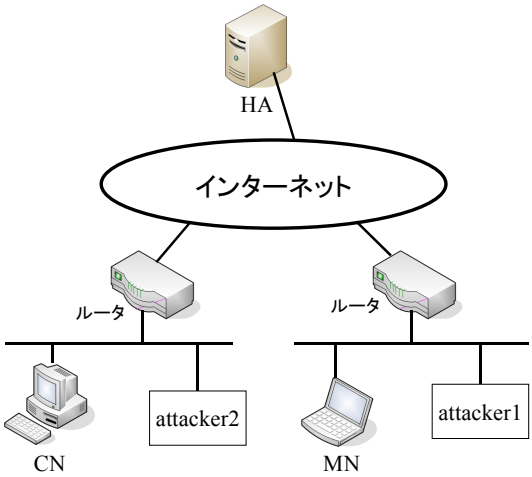

図 3. MN や CN の近傍に攻撃者が接続

広域インターネット内では二つの Init Cookie や二つの keygen token はそれぞれ異なる経路を通るため，バックボーン内に存在する攻撃者が Init Cookie の組や kegen token の組を盗聴することは現実的に難しい．また図 3 の attacker1 のように MN と同一リンク上に attacker1 が存在する場合は，care-of init cookie や care-of keygen token を得ることが可能だが HA と MN 間が IPsec によって保護されているため home init cookie や home kegen

token を得ることはできない．しかし図 3 の attacker2 のように攻撃者が CN と同一リンク上に接続した場合, init cookie の組や kegen token の組を盗聴することが可能である．このため Return Routability は CN 近傍の攻撃者に対して脆弱性があるという課題がある．

また, この脆弱性により攻撃者が共有鍵を手に入れた場合, 攻撃者は CN 近傍から離れた後も継続して通信を乗っ取ることができる．そのため Mobile IPv6 では共有鍵の有効期限を短く設定し, Return Routablity を定期的に実行することでこの問題を解決する．このため定期的に実行される Return Routablity によりネットワークのトラヒックが増加するという課題と, 移動時毎に実行される Return Routability がハンドオーバに影響を与えるという課題がある．

また，通信開始時の CN から HA 間においては認証機構が定義されていない通常の TCP/IP 通信が行われるため，通信の乗っ取りの危険があり，これは Return Routability によって防ぐことができない．

上記以外の課題として，HA を導入する必要があるため，設置コストが高いということと， HA による一点障害の危険がある．また，HA のような特殊なネットワーク機器に依存した認証機構であるためエンドエンドで移動透過性を保証するプロトコルには適していない．

4 Mobile PPC とその課題

4. 1 Mobile PPC の概要

Mobile PPC はエンド端末以外の特殊なネットワーク機器を不要とし，P2P で移動透過性を実現するプロトコルである．Mobile PPC では通信開始時において相手の IP アドレスを知る方法(初期 IP アドレスの解決)と通信中に IP アドレスが変化しても通信を継続できる方法(継続 IP アドレスの解決)を異なるアプローチによって解決しており, 後者が Mobile PPC 特有の機能である．初期 IP アドレスの解決には，ホスト名と IP アドレスの関係を動的に管理する Dynamic DNS(DDNS)[9],[10]を利用する．これにより，ホスト名を識別子として通信開始時における端末の IP アドレスを知ることが可能となる．一方，継続 IP アドレスの解決には，IP アドレスが変化すると，その直後に MN から CN に対して，移動後の IP アドレスと継続させる通信の識別情報を Binding UPDATE(以下 BU)により通知する．BU により，エンド端末間では新旧 IP アドレスの対応関係を示すテーブルが作成され, 以後の通信では図 4 のようにパケット送受信時にネットワーク層でこのテーブルを参照してアドレス変換を行う．これにより，TCP/IP プロトコルスイートを含む上位ソフトウェアに対し IP アドレスの変化を隠蔽し，通信を継続させることができる. Mobile PPC では拡張ヘッダや HA を使用しないため, ヘッダオーバヘッドや HA を経由することによる通信経路の冗長および一点障害などの問題がない．また IPv4 と IPv6 のどちらにも実装可能である．

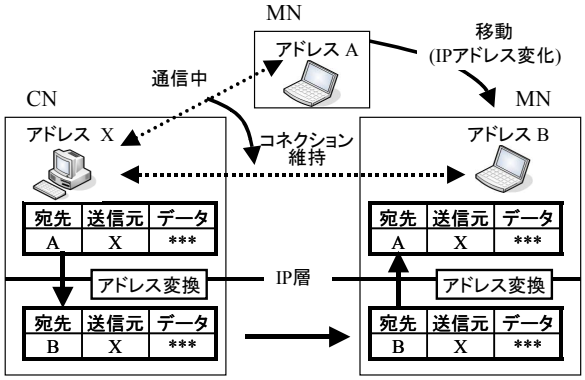

図 4. アドレス変換の例

4. 2 Mobile PPC の課題

現状の Mobile PPC は FPN (Flexible Private Network) [11],[12]という閉じた環境を前提に検討されているため FPN 以外の環境では移動時の成りすましに対する認証機能がなく汎用性に欠けている．FPN 以外の環境で使用する場合，セキュリティの観点から BU パケットの確実な認証が必要である．

インターネットにおいて, 端末間で認証を行う方法として, 共有鍵暗号を利用する方式と公開鍵暗号を利用する方式がある. 共有鍵暗号を利用する方式は, 認証したい相手端末と共有鍵を事前に設定しておく必要がある．しかし，CN と通信する MN は任意であるため, 一般的にこのような設定をしておくことは難しい. 公開鍵暗号を利用した認証は， PKI のしくみを適用することで認証が可能であるが, 現在の PKI が未整備である状況を考慮すると現実的でない．このため，端末間の認証では，CN と MN 間において認証に使用する鍵を，いつ，どのようにして安全に交換するかが解決すべき課題となる． この課題の解決を行うための認証機構として IPv6 の Return Routability と，それと同様の手法を LIN6 に適用した方式が提案されている．しかし Return Routability では HA, LIN6 では MA のような第三の機器を利用するため，特殊なネットワーク機器を使用しない Mobile PPC において, これらの認証機構は適していない．

5 提案方式

本論文では P2P で実現可能な Mobile PPC における認証方式の提案を行う.

本研究では MN が送信した BU パケットを CN が認証するための認証機構として Diffie-Hellman 鍵交換[14]を利用する. Diffie-Hellman 鍵交換とは, 両端末間において, 離散対数問題を利用したアルゴリズムにしたがって生成した乱数を交換することにより, その乱数を盗聴されたとしても盗聴者には知ることのできない共有鍵を生成する鍵交換方式である. 本提案方式では通信に先立って端末間でネゴシエーションを行う機構を Mobile PPC へ追加し, その機構を用いて Diffie-Hellman 鍵交換を行うことにより MN と CN に共有鍵を保持させておき, 移動時にこの共有鍵を用いて MN の認証を行う.

認証方式の流れを図 5 に示す. はじめに, CN は priv_key と呼ぶ乱数を生成し, その乱数から pub_key と呼ぶ値を算出する. ここで, CN が生成した priv_key を priv_key_cn, pub_key を pub_key_cn と呼ぶ. CN は TCP/IP 通信に先立ち MN へ pub_key_cn を送信する (①). CN から pub_key _cn を受信した MN は priv_key を生成し, priv_key から pub_key を算出する. ここで, MN が生成した priv_key を priv_key_mn, pub_key を pub_key_mn と呼ぶ. CN は MN へ pub_key_mn を返信する (②). 両端末間で pub_key の交換が完了すると, 端末自身が保持する priv_key と相手端末から受信した pub_key により共有鍵を生成する (③).

以上の Diffie Hellman 鍵交換の動作が完了した後, 通常の TCP/IP 通信が行われる.

MN が移動し, IP アドレスが変化したときは, BU に共有鍵で作成した MAC(Message Authentication Code)を付加し CN へ送信する (④). CN は BU を受信すると付加された MAC を検証し MN の認証を行う (⑤).

$$MAC = f(BU, 共有鍵) \quad (1)$$

ここで, f( ) は一方向ハッシュ関数を表す. 式(1)の BU は BU パケット全体を表す.

CN と MN の通信中において, 攻撃者が MN に成りすまして BU を CN へ送信するには, CN と MN が保持している共有鍵を取得する必要がある. 移動時において MN から CN へ送信される MAC の付加された BU から共有鍵を推測することは事実上不可能である. また通信開始に先立つネゴシエーションを盗聴し共有鍵を生成するには Diffie Hellman 鍵交換の性質上 priv_key_mn と pub_key_cn , または pub_key_mn と priv_key_cn を取得する必要がある. pub_key_cn や pub_key_mn は平文で通信路を流れているため盗聴することが可能だが, priv_key_mn や priv_key_cn は通信路を流れないため盗聴することができない. このため CN と MN の通信中において, 攻撃者が MN に成りすまして BU を CN へ送信することは不可能である. しかし, 通信に先立って行われるネゴシエーションには認証機構がないため, この際に通信が乗っ取られる危険があるが, これは Mobile PPC を導入する以前の通常の TCP/IP 通信においても発生する問題である.

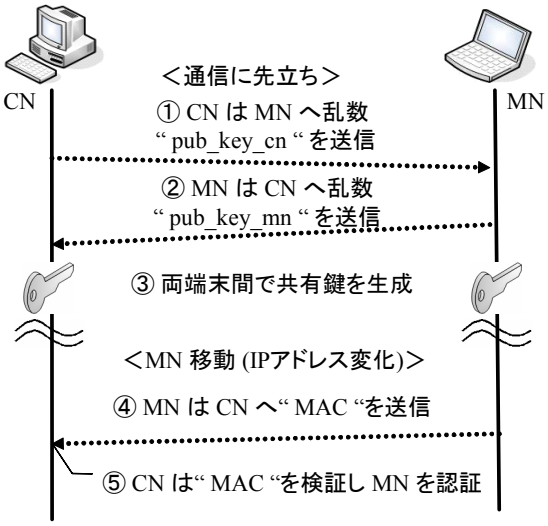

図 5. Diffie-Hellman 鍵交換を利用した認証

6 実装

5 章で説明した提案方式は FreeBSD への実装を検討しており, すべての処理をネットワーク層で実現させる。TCP/IP 通信に先立つネゴシエーションには従来から我々が研究を続けてきた動的処理解決プロトコル DPRP(Dynamic Process Resolution Protocol)[12],[13]を拡張したものを使用し, Diffie Hellman 鍵交換にはオープンソースライブラリである OpenSSL を採用する。

Diffie Hellman 鍵交換には事前に共有されているべき p および g という値があり, すべての Mobile PPC 実装端末に, p に 512 ビットの素数, g に 2 を設定する.

認証に使用する MAC の計算には HMAC_SHA1 を使用する. MAC は次式に従って生成される.

$$MAC=HMAC\_SHA1(msg , 共有鍵) \quad (2)$$

msg は BU パケットの認証を必要とするデータを

示す．共有鍵は Diffie Hellman 鍵交換によって共有された鍵を示す．

7 評価

7.1 Return Routability との比較

7.1.1 セキュリティの比較

Return Routability と提案方式を 2 つの項目で比較した結果を表 1 に示す．

まず，通信開始時における乗っ取りについての比較を行う．通信開始時における乗っ取りとは CN が意図した MN とは異なる端末と通信を開始することを意味する．Return Routability では IPv6 の通信開始時における通信の乗っ取りを防ぐことはできない．提案方式においても通信に先立って行うネゴシエーションには認証機能がないため通信の乗っ取りを防ぐことはできない．しかし，これは Mobile IPv6 や Mobile PPC を導入する以前から，TCP/IP 通信に存在する問題といえる．

次に移動時における乗っ取りについての比較を行う．移動時における乗っ取りとは，登録パケットを受信する以前に通信していた端末と受信後に通信する端末が異なることを意味する．Return Routability では登録パケット送信時に鍵交換を行うが，この鍵交換には脆弱性があるため移動時における乗っ取りの危険がある．本提案方式では登録パケット送信時において，通信に先立って実行された Diffie-Hellman 鍵交換により生成した共有鍵を使用して認証を行うため移動時における乗っ取りの危険はない．

	Return Routability	提案方式
通信開始時における乗っ取り	×	×
移動時における乗っ取り	△	○

表 1. Return Routabiliy **との比較**

また，Return Routability は移動時以外にも定期的に実行される必要があり，そのたびに鍵交換の脆弱性による通信の乗っ取りが発生する危険がある．

7.1.2 運用面の比較

Return Routability は HA のような特殊なネットワーク機器を使用するため，導入のコストがかかる．本提案方式は特殊なネットワーク機器を必要とせずエンド端末間で実現可能である．

また Return Routability は複雑な鍵交換が位置登録時毎に実行されるため，ハンドオーバに影響を与える．提案方式は登録時において，MAC を付加するだけなので，ハンドオーバに影響を与えない．

7.2 評価のまとめ

本提案方式を Mobile PPC へ実装することにより BU における通信の成りすましを防止することが可能となる．本提案方式は特殊なネットワーク機器を必要とせずエンド端末間のみで実現可能であるということと，ネットワーク層ですべての処理を行うため上位のソフトウェアに影響を与えないという利点がある．また，Return Routability やそれを応用した認証機構に比べて安全性が高い．

8 むすび

Mobile PPC における認証方式の提案を行った．今後は提案方式の実装と有効性の確認を行う．

謝辞

本研究は栢森財団の助成を受けて実施したものである．

参考文献

[1] 寺岡文男 ，“インターネットにおけるモバイル通信プロトコルの標準化動向,”, 電子情報通信学会論文誌,Vol.J84-B,No.10,pp.1746-1754,Nov.2000

[2] C. E. Perkins.”IP Mobility Support for IPv4,” RFC 3344. Aug.2002.

[3] D.Johnson, C. Perkins, J. Arkko, “Mobility Support in IPv6,” RFC3775. June 2004.

[4] M. Kunishi, M. Ishiyama, K. Uehara, H. Esaki, and F. Teraoka, “LIN6: A new approach to mobility support in IPv6,” Third International Symposium on Wireless Personal Multimedia Communications, pp.1079-1084, Nov.2000

[5] 國司光宣，石山政浩，植原啓介，寺岡文男，“移動体通信プロトコル LIN6 の性能評価,”情報処理学会論文誌， Vol.43, no.2, pp.398-407, Feb.2002

[6] 竹内元規，渡邊晃,“モバイル端末の移動透過性を実現する Mobile PPC の提案,” 情報処理学会研究報告，2004-MBL-30, pp.17-24, Sep. 2004.

[7] 田中康之，國司光宣，石山政浩，寺岡文男，“LIN6 および HLIN6 における認証機構,” 電気情

報通信学会論文誌，vol.J87-D-I No.5，pp.497-507, May.2004
[8] S. Kent and R. Atkinson, “Security Architecture for the Internet Protocol,” RFC 2401.1998.
[9] R. Droms ，“Dynamic Host Configuration Protocol”，RFC2131，March 1997.
[10] Vixie (Ed.), P., Thomson, S., Rekhter, Y. and J. Bound, “Dynamic Updates in the Domain Name System”, RFC 2136,April 1997.
[11] Flexible Private Network ,Watanabe lab.Division of Information Sciences ， MeijoUniversity ， http://www-is.meijo-u.ac.jp/%7Ewatanabe/research/fpn1.html
[12] 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 の仕組み,”情報処理学会研究報告，Vol.2004, No.75, 2004-CSEC-26, PP259-266, July.2004.
[13] 渡邊晃,井手口哲夫,笹瀬巌, “イントラネット閉域通信グループの物理的位置透過性を可能にする動的処理解決プロトコルの提案”，電子情報通信論文誌,Vol.J84-D1,No.3,pp.269-284 ,March.2001
[14] W.Diffie, M.E. Hellman “New Directions in Cryptography,” IEEE Transactions on Information Theory, Vol. IT-22, No.6 Nov.1976.

謝辞

本研究を進めるにあたり，多大なるご指導，ご鞭撻を賜りました渡邊晃教授に心より感謝いたします．また有益なご助言，ご検討を頂きました渡邊研究室の皆さんに深く感謝いたします．