2004－MBL－30　(3)
2004／9／17

モバイル端末の移動透過性を実現する Mobile PPC の提案

竹内　元規†　　渡邊　晃†

インターネットの普及により自由に移動しながらネットワークに接続したいというニーズが広まっている．しかし，インターネットに接続中の端末が移動するとIPアドレスが変化し，通信が切断されてしまう．この問題を解決する技術として移動透過性を実現する Mobile IP があるが，通信経路の冗長やホームエージェントによる一点障害が指摘されている．このような課題は，今後の P2P 通信への普及に対する大きな阻害要因となってしまう．そこで本研究では，モバイル端末がネットワークを移動しIPアドレスが変化した場合でも，両端末においてアドレス変換処理を行うことによって通信を継続させる方式 Mobile PPC(Mobile Peer to Peer Communication)を提案する．

The proposal of Mobile PPC realizing the mobility of mobile terminals

Motoki Takeuchi,†　Akira Watanabe †

The demand for ubiquitous networking is increasing, however, in normal cases, the communication between mobile nodes will break their connections when they change their locations. To solve the problem, Mobile IP has been studied for years, however, it needs an extra device called home agent. We propose Mobile peer to peer Communication protocol (Mobile PPC),that can keep their connections during their communications even though they change their locations, without using any extra devices.

1　研究背景

インターネットの普及により，モバイル端末もインターネットに接続するという利用形態が広まっている．今後，無線ネットワーク環境の広がりが予想され，自由に移動しながらネットワークに接続し，移動を行っても，通信を継続できることが要求されている．しかし，インターネットでは，電話網で当たり前のように実現している移動しながらの通信を簡単に実現することができない．これは，ノードを識別する IP アドレス自体に位置の情報を含んでいるため，ネットワークの移動前後で移動ノードに異なる IP アドレスが設定されることに起因している[1].

TCP/UDP 通信では，両端末の IP アドレスとポート番号の組によって通信が識別されているため，IP アドレスが変化すると移動前後で別の通信として扱われ，移動前に確立していた通信コネクション(セッション)が切断されてしまう．そこで，移動ノードがネットワークの移動により IP アドレスが変化した場合でも通信を開始･継続できるようにする移動透過性が必要となる．

移動透過性を実現するための研究は，これまでにいくつか行われている．これらの手法は，主にプロキシ方式，エンドツーエンド方式に分類することができる．プロキシ方式は，通信相手からのパケットをプロキシが中継し，移動ノード宛に転送を行う手法で，Mobile IP[2-6]，MSOCKS[8]がある．エンドツーエンド方式はプロキシを用いずエンド端末間による移動透過性を行う方式で，SIP Mobility Support[10]，An End-to-End Approach to Host Mobility[11]，LIN6[12]，MAT[13]がある．

プロキシ方式からエンドツーエンド方式へ移行する方式として，Mobile IPv6[7]がある．

Mobile IP は，移動ノードの位置を管理するホームエージェント(以下 HA)が導入され，移動ノード宛のパケットを HA が受信し，移動ノードの移動先に届くように，IP ヘッダを追加するトンネリング転送を行う．移動ノードから

†名城大学大学院理工学研究科
†Graduate School of Science and Technology, Meijo University

通信相手ノードへの通信は直接届けられる．しかし，通信経路の冗長やヘッダの追加によるオーバヘッド，HA による一点障害などの問題点が指摘されている．MSOCKS では，移動ノードのホスト名を識別子として用い，ネームサーバに移動ノードのホスト名に対してプロキシの IP アドレスを設定しておくことで，通信相手からのパケットをプロキシ経由で移動ノードへ転送をする．この方式では，ヘッダオーバヘッドは発生しないが，冗長なルーティングになることには変わりない．

エンドツーエンド方式の中で，SIP[9]を用いているのが SIP Mobility Support である．この方式では，SIP URI をノード識別子とし，SIP によって移動ノードの IP アドレスを通信相手に通知する手法をとっているが，SIP による基盤が必要になるほか，この手法のみでは TCP コネクションを維持させることができず，Mobile IP などの手法と組み合わせる必要がある．

エンドツーエンド方式をトランスポート層におけるアプローチで解決しているのが An End-to-End Approach to Host Mobility である．これは，TCP にオプションを導入し，移動ノードの IP アドレスが変化した際には，TCP オプションによって通知を行う．この方式では，TCP の拡張が必要であり，移動透過な通信をサポートするのは TCP に限られるので UDP 通信では適用することができない．

エンドツーエンド方式をネットワーク層におけるアプローチで解決しているものに LIN6, MAT がある．これらの方式では，ノード識別子と IP アドレスの対応を保持する位置管理サーバを設け，ノード識別子と位置指示子の機能を分離させることで，IP アドレス変化時の問題を解決している．しかし，LIN6 では，IPv6 のアドレス構造を利用した縮退アドレスモデルを適用しているため，アドレスの利用効率が低下する．独自のアドレス体系を持つため，ノード識別子のグローバルユニークな割り当てが必要となる．また，IPv6 を前提としており，IPv4 には適用できない．MAT では，2 つの IP アドレスを保持させ，1 つをノード識別子，もう一方を位置指示子として両者を対応付ける方式で，通常の IP アドレスを使用することができる．LIN6，MAT とも，IP アドレスの対応を保持するための位置管理サーバが必要である．

Mobile IPv6 は，Mobile IP の考え方に基づいて設計されているが，移動ノードが新しく取得した IP アドレスを直接通信相手へ通知することができるため，エンド端末間の通信が可能となっている．しかし，通信開始時には HA を経由するルーティングを行うため，HA が必須となっている．

その他に，IPsec[14]を用いて移動透過性をサポートする方式[15]が提案されている．これは，エンド端末が IPsec のトンネルモードを使用し，移動時に IKE プロトコルを拡張した IP アドレスの通知機能を付加することで実現している．ただし，IKE の鍵更新が必要なため，処理のオーバヘッドが大きいという課題がある．

今後はネットワークの特徴を最大限に活かせる P2P(Peer-to-Peer)通信の要求がますます増加すると考えられるが，プロキシ方式における課題は，P2P 通信普及の大きな阻害要因となる可能性がある．また，新たなネットワーク機器による基盤が必要となると十分な普及に至るまでその機能が発揮できない．P2P 通信が個人間の通信が主体となることを踏まえると，特殊な位置管理サーバを必要とせず，手軽に移動透過な通信を提供できることが望まれる．

本稿では，エンド端末の IP 層にアドレス変換処理を挿入し，移動ノードの IP アドレスが変化しても，上位ソフトには影響を与えないまま，パケットが正しくルーティングされるように IP アドレスの変換を行うことで IP アドレスの変化を隠蔽する通信方式 Mobile PPC（Mobile Peer to Peer Communication）を提案する．Mobile PPC は，現時点においては FPN(Flexible Private Network)[16]の環境下を想定し移動透過性を実現している．

以下，2 章で既存技術の代表として Mobile IP, LIN6 の通信方式とその課題，３章で提案方式の通信方式を説明し，4 章で提案方式の実装，5 章で評価，6 章にむすびについて述べる．

2 既存技術

2.1 Mobile IP

Mobile IP は，IP 層で移動透過性を保証するプロトコルである．

移動ノードはホームアドレスと気付アドレスの二つの IP アドレスを持ち，ホームアドレスは移動によって変化することなく，同じアドレスを使い続ける．通信相手ノードは，移動ノードのホームアドレスを知っているだけでよく，移動ノードと通信する場合には，ホームアドレス宛にパケットを送信する．

気付アドレスは，移動ノードが移動先のネットワークで割り当てられるアドレスである．移動ノードのネットワーク間移動をサポート

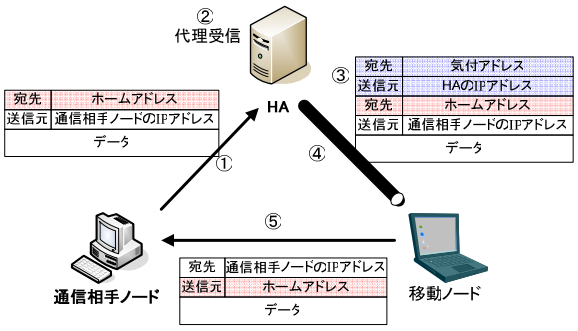

図 1　Mobile IP の通信
Fig.1 communication of Mobile IP.

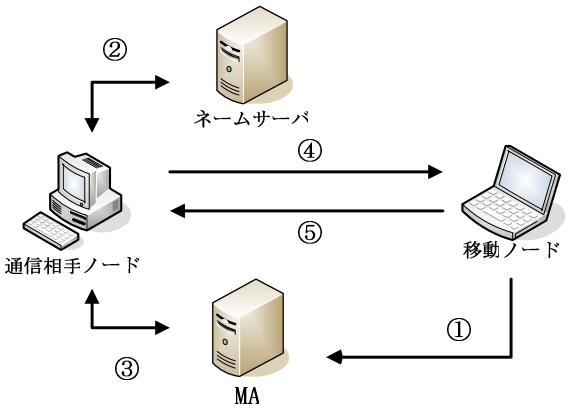

図 2　LIN6 の通信
Fig.2 communication of LIN6.

するために, ホームアドレスの属するネットワーク内に HA を設置する．HA は，移動ノードのホームアドレスと気付アドレスの対応付けを行い, ホームアドレス宛のパケットを受信し，移動ノードへ転送する役割を持つ.

Mobile IP の動作は，HA への登録，データ通信に分けることができる.

移動ノードが別のネットワークへ移動した場合, 移動先のネットワークで新しく取得した気付アドレスを HA へ登録し, 移動ノードのホームアドレスと気付アドレスの対応付けを更新する.

Mobile IP によるデータ通信を図 1 に示す．通信相手ノードから移動ノードへパケットを送信する場合は, 宛先を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 により受信される(②)．HA は，このパケットに対し更に IP ヘッダでカプセル化することによって移動ノードへパケットを転送する(③)(④).

移動ノードから通信相手へのパケットは直接送られる(⑤)．また，このとき送信元アドレスは，ホームアドレスとなっている．これは，コネクションが両端末の IP アドレスとポート番号の組によって管理されているため, 気付アドレスを送信元とすると別の通信として認識されてしまうためである.

通信相手からのパケットは HA を経由させ，移動ノードに転送することで移動ノードが移動しても通信を継続させることが可能となる.

Mobile IP の問題点はまず，図 1 に示すように, 移動ノード宛のパケットは必ず HA を経由するルーティングとなるため, 通信が冗長な三角経路を通ることになる．また，HA という特殊な装置の導入が必要であり，HA を複数設置することができないため，HA による一点障害などの課題がある．さらに，移動ノードから通信相手ノードへパケットを送信する場合に, 送信元アドレスとして使われる気付アドレスは移動ノードのインターネット内での位置を正しく表していないため, 途中のルータでは送信元アドレスを偽っている不正パケットと見なされ，破棄されてしまう可能性がある.

2.2　LIN6

LIN6(Location Independent Networking for IPv6)は，IP アドレスに含まれているノード識別子と位置指示子の機能を分離させるために，IPv6 アドレスに対して縮退アドレスを適用したアドレスモデルを用いている．LIN6 のアドレスモデルでは，移動ノードの IPv6 アドレスの上位 64 ビットを位置指示子, 下位 64 ビットをノード識別子として扱う．また，上位 64 ビットに対し LIN6 プレフィックスと呼ばれる固定値を定義しておき，IP 層よりも上位層ではノード識別子と LIN6 プレフィックスを合わせた固定アドレス, 下位層ではノード識別子と位置指示子を合わせた通常のアドレスとなるように変換を行う．これにより，上位層ではノードの位置や移動にかかわらず一定のアドレスとなるため，移動透過的な通信が可能となる.

LIN6 では，Mapping Agent(以下 MA)と呼ばれる位置管理エージェントが必要となる．MA はノード識別子と移動ノードの現在の位置情報との対応関係を保持し, 現在の位置情報を通知する役割を持つ.

LIN6 によるデータ通信を図 2 に示す. まず，移動ノードはノード識別子と現在の IPv6 アドレスを MA に登録しておく①．通信相手ノードはネームサーバに問合せ, 移動ノードのノード識別子と移動ノードを管理している MA の IPv6 アドレスを取得する②．通信相手ノード

は MA に移動ノードのノード識別子を示すことで移動ノードの IPv6 アドレスを取得する③. このように IPv6 アドレスを取得した通信相手ノードは移動ノードに対しパケットを送信することが可能となる④. 移動ノードがパケットを返信する際には, 通信相手ノードの場合と全く同様に相手ノードの MA に位置情報を要求し, その返答を受信することにより返信する⑤.

MA は複数設置することが可能なため, Mobile IP の HA のように, 一点障害点などの問題は起こらない.

LIN6 の縮退アドレス方式は, IPv6 のアドレス構造を利用していることもあり, IPv4 への適用は困難であり, アドレスの利用効率も低下する. さらに, 独自のアドレス体系を持つことになるため, ノード識別子のグローバルユニークな割り当てとその管理機構が必要になるなどの課題がある. また, MA のような特殊な装置が必要になる.

3 提案方式

3.1 アプローチ

IP アドレスの変化にかかわりなく, 通信を可能にするためには, 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 アドレスの解決と呼ぶ)と, 通信中に IP アドレスが変わった場合に通信を継続できる方法(継続 IP アドレスの解決と呼ぶ)の２つを解決する必要がある.

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ダイナミック DNS(以下 DDNS)[17-18]という技術が既に実用になっており, これを採用する. しかし, この方法だけでは継続 IP アドレスの解決にならない. これは, 実際の通信が始まってしまうと DNS は参照されず, 同じ IP アドレスを使い続けるためである.

そこで, 本方式では初期 IP アドレス解決には DDNS を採用し, 継続 IP アドレス解決として, エンド端末間で移動時の通知を行い, 移動後も通信を継続できる通信方式（Mobile Peer to Peer Communication;以下 Mobile PPC）を提案する. 本方式により, IP アドレスの変化に影響されることなく常時 P2P 通信が可能な環境を提供することが可能になる.

3.2 Mobile PPC による継続 IP アドレスの解決

Mobile PPC では, 通信を行っているエンド端末の IP 層に移動の通知処理, アドレス変換処理を挿入することで, 継続 IP アドレスを解決する.

Mobile PPC 対応ノードは, 移動前後のコネクション識別子の対応関係を記したテーブル（Connection ID Table ; 以下 CIT）を保持する. ここで, コネクション識別子とは通信を行っている両端末の IP アドレスとポート番号の組, プロトコル番号の５つの情報のことを示す.

移動ノードが他端末と通信中に別のネットワークへ移動した場合, 移動先で新しく取得した IP アドレスと継続させたい通信のコネクション識別子を Binding UPDATE(BU)パケットを用いて通知する. BU は ICMP Echo Request をベースに定義されているパケットで, メッセージフォーマットを図 3 に示す.

移動の通知処理は, 図 4 のように移動ノードの IP アドレスが変化した直後に移動ノードより実行し, 通信相手の認証を行いながら, 移動情報を通知する. BU により両端末において,

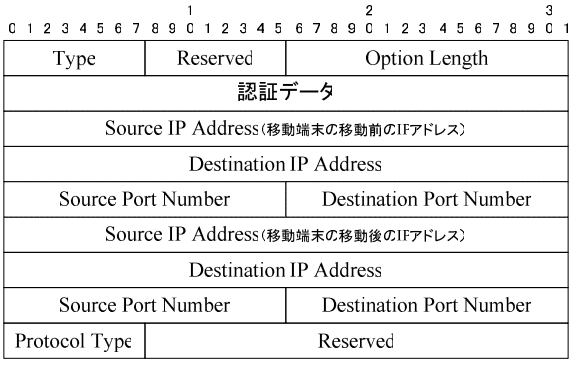

図 3 BU パケットフォーマット
Fig.3 BU packet format

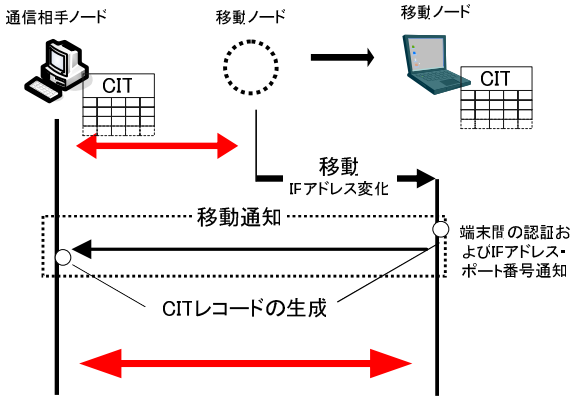

図 4 移動情報の通知
Fig.4 The notice of move information

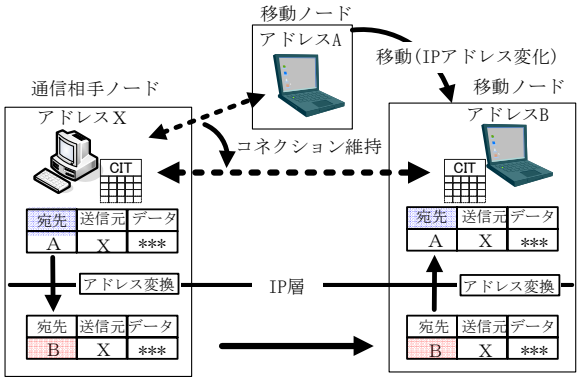

図 5　アドレス変換の例
Fig.5 The example of address translation

移動情報を元に CIT レコードが生成される.

Mobile PPC では，現時点では FPN 環境を想定しており, ノード間はあらかじめ共通鍵を保持している. 通信相手の認証はこの共通鍵を用いて認証を実現している.

移動情報を通知した後は，作成された CIT レコードに従い全送受信パケットに対し，IP 層にて IP アドレスの書き換え処理を行う.

アドレス変換は, 図 5 のように両端末で行う. パケット受信時には通信開始時のコネクション識別子となるようにアドレス変換を行い, 送信時には, 正しくルーティングされるようにアドレス変換を行う．これにより，移動による IP アドレスの変化を TCP/UDP や上位層プロトコルに対して感知させないため, 移動後もコネクションを維持させることが可能となる.

4　提案方式の実装

4.1　実装の概要

実装対象となる OS はオープンソースで，IP 層に関する情報や処理内容の資料が多い FreeBSD を採用した.

4.2　試作モジュールの説明

Mobile PPC の機能を実現するための試作モジュールとその機能を表 1 に示す.

移動の通知処理時に, 移動情報を持つ BU パケットを生成することになるが，本実装では, Mobile PPC が FPN 環境で実装されることを利用し, 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（Dynamic Process Resolution Protocol; 以下 DPRP と略す）[19-20]を拡張したものを使用する．ここで，DPRP とは柔軟なセキュア通信グループを実現する手段として考案されたプロトコルで, 通信に先立ちエンド端末と中継装置が情報交換し, 通信に必要となる動作テーブルを自動生成するプロトコルである.

移動の通知には，拡張 DPRP パケットに BU メッセージ（図 3）を付加したものを利用し，通信相手の認証と移動通知処理を行う.

表 1　試作モジュールの構成と機能
table.1 Function table of the trial system

モジュール	機能
アドレス変換	送信／受信パケット毎に呼び出されるモジュール. CIT レコードの内容にしたがって, アドレス変換処理やそれにともなうチェックサムの再計算を行う.
移動管理	移動の通知処理を行うモジュール. 自端末の IP アドレス変更時に, BU パケットを生成し通信相手に移動情報を通知する.
CIT 操作	CIT を管理するモジュール. CIT レコードの検索・生成・更新を行う

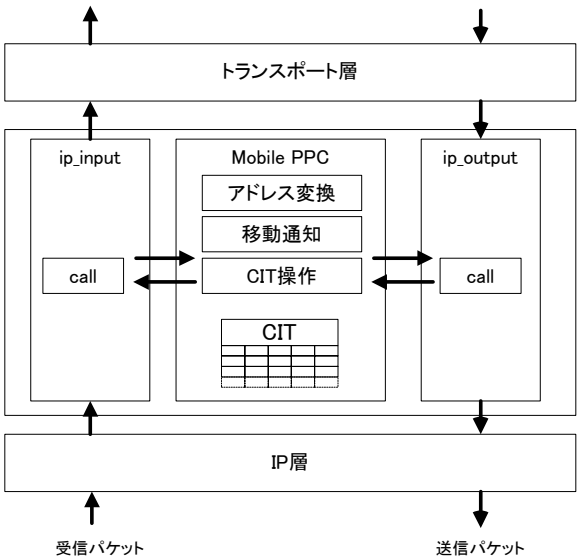

図 6　IP 層での処理
Fig.6 Processing in IP layer

4.3 実装方式

Mobile PPC における試作モジュールは, 図 6 に示すように，IP 層で行われる既存の処理に変更を加えないよう，IP 層の入出力の最適な場所で呼び出し, 処理を終えたら差し戻す形を採用している.

5 評価

5.1 既存技術との比較

Mobile IP(MIP), Mobile IPv6(MIPv6), LIN6, 提案方式(提案)を 7 つの項目で比較した結果を表 2 に示す.

プロキシ方式である Mobile IP は，通信が冗長な三角経路になってしまい，Mobile IPv6 でも通信開始時に HA を経由した冗長な経路になる．また，HA による一点障害も発生する．エンドツーエンド方式の LIN6，提案方式では冗長経路や一点障害の問題はない.

通信時にヘッダの追加を行う Mobile IP, Mobile IPv6 は，ヘッダ長が長くなったとこによるオーバヘッドが発生する.

Mobile IP は，通信相手ノードに変更を加えない設計となっており, 送信元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, 途中のルータにより不正パケットとみなされる問題がある. エンド端末で処理を行う設計である Mobile IPv6，LIN6，提案方式では，この問題にも対応できる.

LIN6 では, 独自のアドレス形態であるため, IPv6 が前提でアドレスの利用効率が悪いなどの制約が生まれてしまう.

表 2　既存技術との比較
table.2 Comparison with existing technologies

	MIP	MIPv6	LIN6	提案
通信経路	×	△	○	○
耐障害性	×	×	○	○
ヘッダオーバヘッド	×	×	○	○
送信元アドレス	×	○	○	○
アドレス制約	○	○	×	○
普及の容易さ	×	△	△	○
認証	○	○	○	△

普及の容易さを比較すると，Mobile IP における HA，LIN6 における MA が必須となっているので, 新たなネットワーク機器による基盤が必要となり, 十分な普及に至るまでその機能が発揮できない. 提案方式では，DDNS を必要とするが, DDNS はすでに実用となっている技術であり，既存環境への適用も容易である.

ノードが移動した際のノード認証として，Mobile IP，Mobile IPv6，LIN6 では移動ノードと HA，MA の関係を利用した認証が行われているが，提案方式は現時点では FPN という閉じた環境での認証機構のみとなっている.

5.1 提案方式の課題

Mobile PPC の課題としては次の３点が挙げられる
(1) 移動時の認証機能
(2) 移動時のパケットロス
(3) 移動ノードの同時移動

(1)では，現在 FPN 環境を想定し，共通鍵を利用した端末間の認証を行っているが, グローバルな環境時での認証機能が定義されていないため, 一般環境に本方式を適用すると通信の乗っ取りなどの懸念がある.

(2)は，移動透過性を実現する上でハンドオーバ時にパケットロスが起こらないことが望ましいが，現時点では，ロスが発生する可能性がある．これは，エンドツーエンド方式共通の課題であり, 無線レイヤに係わる検討が必要である.

(3)では，移動ノード同士が全く同時に移動した場合は通信が継続できなくなる可能性がある. この課題は未解決であり今後整理していく必要がある.

6 むすび

本稿では, 移動端末がネットワークを移動し IP アドレスが変化した場合でも，通信中のコネクションを維持させるための手法を提案した. 今後は, 課題の解決方法を検討してしていくとともに, 提案システムの実装を通して有効性を確認する．また，IPv6 についてもこの手法の適用を検討する.

謝辞

本研究は柏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ノード移動透過性プロトコル，電子情報通信学会論文誌, Vol.J87-D-I, No.3, pp.308-328(2004)

[2] Perkins,C. : IP Mobility Support for IPv4, RFC3344,IETF,Aug.2002

[3] Perkins,C.：IP Encapsulation within IP", RFC 2003, October 1996

[4] Calhoun,P. and Perkins,C：Mobile IP Network AddressIdentifier Extension, RFC 2794, March 2000.

[5] C. Perkins, P. Calhoun : Mobile IP Challenge/Response Extensions. RFC 3012.November 2000.

[6] G. Montenegro : Reverse Tunneling for Mobile IP, revised RFC3024, Jan. 2001.

[7] Johson,D.B. and Perkins,C. : IP Mobility Support in IPv6 , Internet-draft , TETF , Nov.2002

[8] D.Maltz and P. Bhagwat，“Msocks : An architecture for transport layer mobility.”Proc. IEEE IN-FOCOM’98，pp.1037-1045，March 1998.

[9] J. Rosenberg, H. Schulzrinne, G. Gamarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, and E. Schooler, “SIP : Session initiation protocol.”,june.2002.RFC3261

[10] E. Wedlund and H. Schulzrinne, “Mobility support using sip.” Proc. Second ACM International Workshop on Wireless Mobile Multimedia, pp.76-82, Sept.1999

[11] Alex C. snoeren and Hari Balakrishnan , “An End –to-End Approach to Host Mobility” MIT Laboratory for Computer Science Cambridge MA 02139 , 6th ACM/IEEE International Conference on Mobile Computing and Networking , August 2000

[12] 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 , No.8 , PP.2076-2086 (2001)

[13] 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, no.12, pp.3889-3897, Dec.2002.

[14] S. Kent，R. Atkinson，“Security Architecture for the Internet Protocol”，November 1998, RFC2401

[15] 竹仲雅彦, 藤本信吾, 藤野信次, ”IPsec/IKEによるセキュアなシームレスローミング方式の試作.” 情報処理学会研究報告, 2004-CSEC-26, July 2004.

[16] Flexible Private Network，Watanabe lab. Division of Information Sciences，Meijo University，http://www-is.meijo-u.ac.jp/~watanabe/research/fpn.html.

[17] R. Droms，“Dynamic Host Configuration Protocol”，RFC2131，March 1997.

[18] Vixie (Ed.), P., Thomson, S., Rekhter, Y. and J. Bound, : "Dynamic Updates in the Domain Name System", RFC 2136,April 1997.

[19] 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, 2004-CSEC-26, July 2004.

[20] 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