ネットワークアドレス変換を用いたIP移動透過性の検討

岡崎 直宣[1)]・板山 俊一[2)]

A study of a method to support the mobility of IP addresses using IP address translations

Naonobu OKAZAKI, Shun-ich ITAYAMA

Abstract

Recently, various mobile networks have been provided for mobile Internet services. Mobile IP has a key protocol for location management for mobile nodes and is basically intended to support the mobility of global IP addresses. However, it requires each mobile node to extend the functions of its protocol stack and this lead us hard to introduce it.

In this paper, we will propose a new method to realize the mobility of IP addresses using a technique of IP address translations.

Key Words:

mobile networks, mobility of IP addresses, network address translator

1. はじめに

近年，第 3 世代携帯電話に代表される広域セルラー網やホットスポット型の無線 LAN など，さまざまなモバイルネットワークが構築され，IP 通信サービスが提供されつつある。これらのモバイルネットワークにおいて，移動ノード（MN：Mobile Node）の位置管理と移動時のシームレスな通信をサポートするプロトコルとして Mobile IP の研究が進められている。

MN の移動透過性には，（1）MN が移動しても MN が確立しているコネクションを維持できること，（2）MN の位置によらず MN との通信を開始できること，の二つの要素がある。携帯電話に当てはめると，（1）は移動して基地局が変わっても会話が続けられること，（2）はどこの基地局を使っていても着信できることに相当する。これは，携帯電話が移動しても変化しない電話番号を用いるからである。一般に MN が移動すると，インターネット上の識別子である IP アドレスが変わる。このため MN は通信相手ノード（CN：Correspondent Node）から移動前後で別の MN と判断される。Mobile IP では常に同じ IP アドレス（ホームアドレス）を使うことにより移動透過性を実現できる。Mobile IP は IP 層で実現するため，IP を利用する全てのアプリケーションが移動透過性を持つことができる。しかしながら，Mobile IP を利用する全ての端末に拡張が必要となる。そのため現状では導入が難しい。

ホームアドレスの代わりに DNS[1]の Dynamic Update（いわゆる DDNS[2]）を用いて移動透過性を簡便に実現する手法が提案されている[1]が，MN のローミング時にコネクションの維持ができないなどの課題がある。

1) 情報システム工学科助教授
2) 情報システム工学科学部生

[1] DNS（Domain Name System）：TCP/IP ネットワーク環境において，ドメイン名から対応する IP アドレスを取得できるシステム。
[2] DDNS（Dynamic DNS）：DNS データベースの内容に変更があったときにその変更を即座に通知したり，変更部分のデータだけを転送するなどの機能を持った DNS。

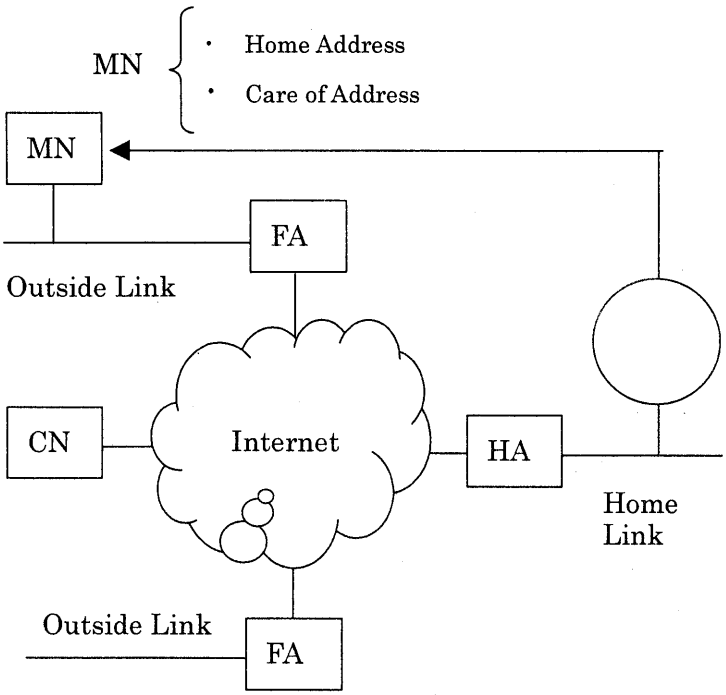


図1 Mobile IP のネットワーク構成

本論文では，Mobile IP のホームアドレスの替わりにドメインネームを用い，MN のローミング時にネットワークアドレス変換（NAT[3]）を用いてコネクションが維持できる移動透過性の実現方式を提案する。

以下本論文では，2 章で既存の IP 移動透過性の実現方式について紹介し，その現状と課題について明らかにする。3 章では本論文で提案する方式について述べ，その詳細な通信プロトコルを示す。最後に 4 章でまとめと今後の課題を示す。

2. 既存の IP 移動透過性の実現方式

本章では既存の IP 移動透過性の実現方式について紹介し，その現状と課題について明らかにする。

既存の IP 移動透過性の実現方式には，以下の Mobile IP と DDNS を用いた方式がある。

2.1 Mobile IP

Mobile IP ネットワークは以下の端末により図1のように構成される。

・移動ノード MN（Mobile Node）
・ホームエージェント HA（Home Agent）
・フォーリンエージェント FA（Foreign Agent）
・通信相手ノード CN（Correspondent Node）

Mobile IP では MN は 2 つのアドレスを持つ。1 つは「ホームアドレス（Home Address）」であり，これは MN のインターネット接続位置にかかわらず一定の値をとる。すなわち，MN の永続的な識別子の働きをするものである。もう 1 つは「気付けアドレス（Care of Address）」であり，これは MN のインターネットへの接続位置，つまり FA のアドレスである。従って MN が別のサブネットに移動すると気付けアドレスは変化する。ホームアドレスと気付けアドレスの対応付けを「バインディング」と呼ぶ。Mobile IP の機能は，移動ノードのホームアドレスを指定することで MN との通信を可能にする。

Mobile IP では MN が接続しているリンクを 2 種類に分けて考える。MN のホームアドレスが示すリンクを「ホームリンク（Home Link）」と呼ぶ。ホームリンクは MN が通常接続しているリンクということができる。ホームリンク以外を「外部リンク（Outside Link）」と呼ぶ。外部リンクは移動先で接続するリンクである。Mobile IP の機能を別の表現で定義すると，実際のインターネットへの接続位置にかかわらず，MN は仮想的には常にホームリンクに接続しているように見せる機能である，ということができる。

Mobile IP では MN のホームリンク上に「ホームエージェント（HA：Home Agent）」を設置する。HA は MN のバインディングを管理する。また HA はホームリンクの経路情報をインターネット内に広告する。さらに Mobile IPv4 では外部リンクに「外部エージェント（FA）」を設置する。FA は MN に気付けアドレスを割り当てる。

[3] NAT（Network Address Translator）：プライベート IP アドレスと，グローバル IP アドレスを相互に変換し，プライベートネットワークからグローバルネットワークにアクセスできるようにするアドレス変換装置。

Mobile IP の動作は，（1）ホームリンク/外部リンクの認識，（2）バインディングの更新，（3）データ通信に分けられる。ホームリンク/外部リンクの認識は，MN が別のサブネットに移動したことを検知し，そのサブネットがホームリンクか外部リンクかを認識し，外部リンクの場合は新しい気付けアドレスを得るという動作である。MN が外部リンクに接続して新しい気付けアドレスを得ると，この気付けアドレスを HA に通知し，バインディングを更新する。このとき，別のノードによる偽りのバインディング更新を防止するため，バインディング更新のパケットには MN を認証するためのデータが付加される。HA はバインディング更新パケットの認証に成功すると MN のバインディングを更新し，応答パケットを MN に返信する。

Mobile IP は IP 層で実現されるため，Mobile IP を利用する全ての端末の IP プロトコルスタックの変更が必要である。そのため，現状では導入が難しい。また現在のインターネットモデルでは，ホームアドレスの定義が難しい。特にこれから大量のユーザの増加が見込まれる家庭ユーザなどでは，そのアドレスをどのネットワークに置くのかが疑問である。ほかにも HA が一点障害になってしまう問題点もある。HA がクラッシュしたり HA への通信路に障害が発生したりすると，MN と CN 間の通信路が正常であっても MN との通信はできなくなる。HA は MN のホームリンク上に設置しなければならず，地理的に分散にして複製をおくことができない。

2.2 DDNS を用いた移動透過性

Mobile IP では常に同じ IP アドレス（ホームアドレス）を使うことで移動透過性の実現を目指している。そこでホームアドレスの変わりにドメインネームを用いて移動透過性を実現する方式が提案されている[1]。

DNS はインターネット上のノードに対する人間が扱いやすい名前（FQDN : Full Qualified Domain Name）と IP アドレスとの相互変換を行う分散データベースである。ただし，このデータベースはネットワーク上で共有されており，階層的に管理されている。DDNS はこのデータベースを動的に更新するための機構である。IP

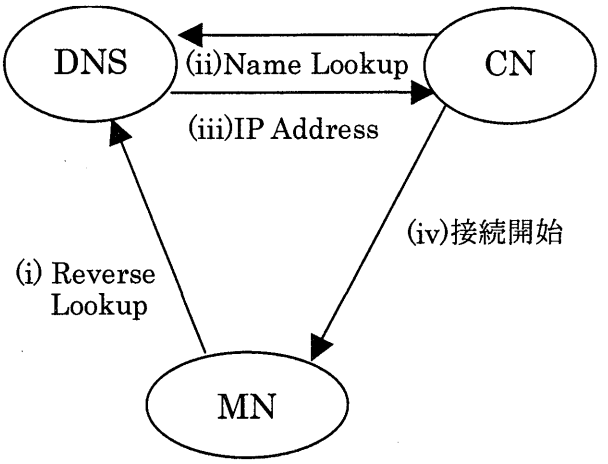


図 2　DDNS を用いた実現方式

アドレス変化時には MN が DDNS を用いてノードの名前に対応する IP アドレスを更新すれば，そのノードには常に同じ名前で通信可能になる。MN と通信するノードは，従来通りにノード名に対応する IP アドレスを DNS から得て通信を行えばよい。この方式を図 2 に示す。

DDNS は移動透過性を実現できる簡便な方法であるが，以下のような課題がある。

・ノード移動時のコネクション維持

CN が DDNS を用いて MN と通信を行っている際，MN が通信中に移動した場合には通信を継続きない。これは，インターネットプロトコル（IP）では，ノードのネットワークインターフェースに IP アドレスが割り当てられる。IP アドレスはノードのインターネット内での位置を表し，経路制御に利用される。一方，ユーザは文字列によるホスト名でノード識別するが，ノード名は DNS によって IP アドレスと対応付けられている。すなわち，IP アドレスはノード識別子としての意味ももつ。移動ノードがあるサブネットから別のサブネットに移動すると，その移動ノードが持つ IP アドレスは変化する。IP アドレスが変わってしまい，MN はほかのノードから認識できなくなり，移動前に確立していた TCP コネクションも移動後は切断されてしまう。TCP コネクションは両端のノードの IP アドレスとポート番号の 4 つ組で管理されているからである。したがって，通信を行いながら移動する用途には適さない。

・頻繁な移動への対応

ＭＮの頻繁に移動が起きると更新内容が相手

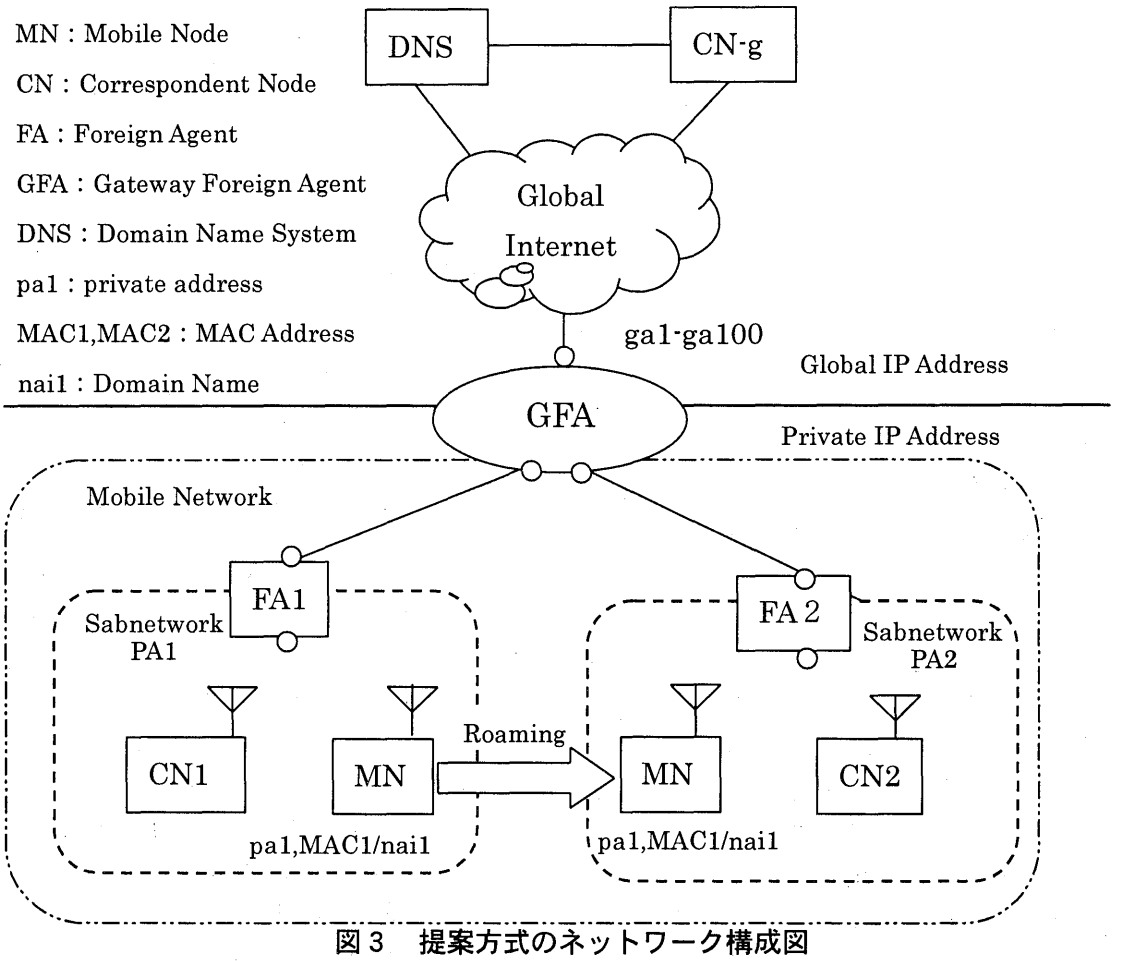


図3 提案方式のネットワーク構成図

に伝わらない可能性がある。DNS からの応答メッセージには秒単位での有効期限が付加されており，問い合わせ側は結果をその時間だけキャッシュしておくことができる。これは DNS 階層をたどる際に既に得た結果を効果的に再利用するための機能である。移動透過性を実現するような場合には有効期限を短く設定するが，それでもキャッシュの有効期限内に MN が移動すると，キャッシュ内の IP アドレスが利用されてしまい，通信に失敗する。

・誤接続の可能性

DDNS で登録されたレコードは明示的に消去するまでは DNS 上に残るため，MN がレコードの消去を怠ると古いレコードが残ったままになる。このように古いレコードが残った状態で IP アドレスが他ノードによって再利用されると，誤ったノードに接続されることになる。

3. 提案方式

本論文では，ホームアドレスの代わりにドメインネームを用い，MN のローミング時に NAT を用いてコネクションが維持できる移動透過性の実現方式を提案する。提案方式では，ネットワーク内部の装置の拡張により移動透過性が実現できるため，Mobile IP に比べより容易に実現可能である。以下，3.1 で提案方式のネットワーク構成，3.2 で新たに拡張する機能，3.3 で通信シーケンスを述べる。

3.1 ネットワーク構成

提案方式のネットワーク構成を図 3 に示す。モバイルネットワークに新たに GFA（Gateway Foreign Agent）を導入し，FA に NAT 機能などを拡張した。GFA と FA の詳細については 3.2 にて後述する。モバイルネットワークは 1 つの管理主体にて管理される。ここでは GFA が，モバイルネットワークの管理を行う。モバイルネットワーク内の各サブネットに存在するプライベート IP アドレスは重なっていないものとする。FA はこのサブネットを管理する。モバイルネットワーク内では，内部の FA により MN の位置管理が行われている。通信相手ノードはグローバルネットワーク上に存在する CN-g，同じサブ

ネット内のCN1，別のサブネット内のCN2と表す。この図3でMNが初期接続時にFA1で割り当てられたプライベートIPアドレスをpa1とし，MNのMACアドレス[4]をMAC1，ドメインネームを"nai1"とする。またMNがグローバルネットワークと通信を行う際，GFAのNATにより割り当てられるグローバルIPアドレスをga1とする。

3.2 拡張機能

ここでは本提案方式にて新たに導入したGFAとFAに拡張した機能を述べる。

3.2.1 GFA

GFAは，モバイルネットワークとグローバルインターネットの接続地点にあるNAT機能を持ったルータである。提案方式では，MNのドメインネーム登録の際にMNのIPアドレスではなく，GFAのグローバルIPアドレスの1つであるgaを登録するメッセージ（RegReqメッセージ）を送信する。GFAは，NATによるグローバルIPアドレスとプライベートIPアドレスの対応をNATテーブルに記録する。このとき，MACアドレスをプライベートIPアドレスに付加する。NATテーブルに登録したMACアドレスと，同一のMACアドレスがNATテーブルに存在すると，GFAはNodeResメッセージにNATテーブルにあるMACアドレスとプライベートIPアドレスをパラメータ値として送信する。GFAは，ドメイン登録メッセージを送信すると，登録完了メッセージ（RegAckメッセージ）をFAに送信する。

3.2.2 FA

MNがFAの管理するサブネットに接続し，プライベートIPアドレスをMNに割り当てる。提案方式では，FAはMN接続時に得るMACアドレスをNodeReqメッセージとしてGFAに送り，GFAからのNodeResメッセージのパラメータ値でMNが初期接続かFA間ローミングかを判断する。このときのパラメータ値にnew_nodeが含まれていると，MNは初期接続と判断し，new_node以外のパラメータ値であるとローミング時の接続と判断する。MNが初期接続時はDHCP[5]によってIPアドレスを割り当てる。ローミング時はDHCPで割り当てるプライベートIPアドレスpa2とGFAに登録されているNATテーブルのプライベートIPアドレスpa1を対応付けし，NATテーブルを作成する。

3.3 通信シーケンス

提案方式を実現するためにはMNを行うための登録手順と通信を行うための手順（通信シーケンス）が必要である。提案方式の通信シーケンスは，（1）グローバルネットワークのCN-gとの通信，（2）同じサブネット内のCN1との通信，（3）別のサブネットのCN2との通信の3通りある。さらに，（a）MNからCNへの発信，（b）CNからMNへの着信，（c）MNのローミング時の通信，の3通りについて考える必要がある。以下では，GFAとFAの基本動作を示し，グローバルネットワークとの通信の場合を述べる

3.3.1 移動端末の管理

MNがFAに接続すると，FAはMNのMACアドレスを検出する（MAC1 detect）。FAはMACアドレスをGFAに送信する（NodeReq[MAC1]）。GFAはNATテーブルにMAC1と一致するエントリを検索する。GFAのNATテーブルにMAC1のエントリが存在するかどうかによって，以下の2つの場合に分けられる。

case1 初期登録

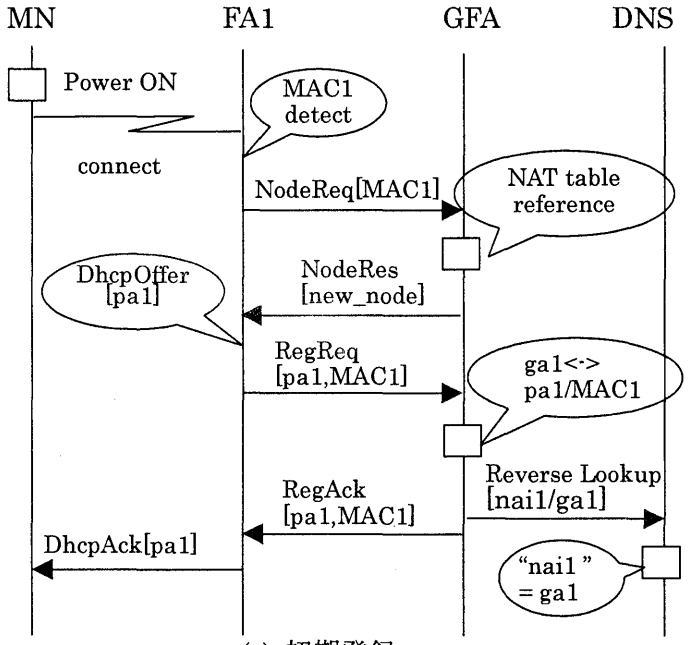
GFAのNATテーブルにMAC1のエントリが存在しない場合，MNの初期登録時とみなす。このとき以下のような動作を行う（図4(a)）。

(i) FAはMACアドレスをGFAに送信する（NodeReq[MAC1]）。

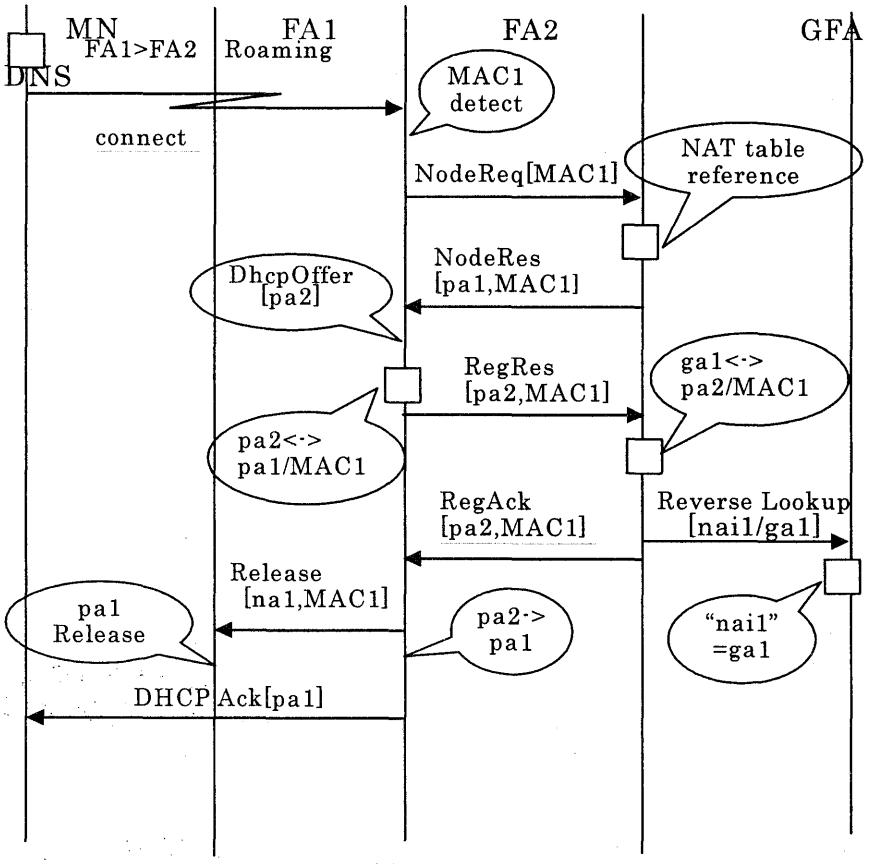
(ii) GFAはNATテーブルにMAC1と一致す

[4] MACアドレス（Media Access Control Address）：MACアドレスとはすべてのNIC（Network Interface Card）に固有の番号のこと。Ethernetの場合MACアドレスは48bitで，前半24bitはIEEEが管理する各ベンダー固有のアドレス，後半24bitがNICごとの固有の番号となっている。世界中で同じMACアドレスを持つNICは存在しない。

[5] DHCP（Dynamic Host Configuration Protocol）：ノードの起動時に動的にIPアドレスを割り当て，終了時にIPアドレスを回収するプロトコル



(a) 初期登録



(b) 移動登録

図4　移動端末の管理

るエントリを検索する（NAT table reference）。

（iii）GFA は FA に new_node パラメータ値を含んだ NodeRes メッセージを送信する（NodeRes[new_node]）。

（iv）FA は MN へ DHCP にてプライベート IP アドレス pa1 を割り当てる（DhcpOffer[pa1]）。

（v）FA は MN の IP アドレスと MAC アドレスを GFA に送信する（RegReq[pa1,MAC1]）。

（vi）GFA は NAT テーブルに新たな条件を登録する（ga1<->pa1/MAC1）。

(vii) GFA は ReverseLookup メッセージを送信し，DNS は MN のドメインネームに新たな IP アドレスを登録する（“nai1”=ga1）。
(viii) GFA はドメイン登録要求を行うと，FA1 に NAT テーブル作成完了メッセージを送信する（RegAck[pa1,MAC1]）。
(ix) FA1 は MN に pa1 を割り当てる（DhcpAck[pa1]）。

case2　移動登録

GFA の NAT テーブルに MAC1 のエントリが存在する場合，MN はローミングによる FA2 への接続と判断する。このとき以下のような動作を行う（図4(b)）。
(i) FA は MAC アドレスを GFA に送信する（NodeReq[MAC1]）。
(ii) GFA は NAT テーブルに MAC1 と一致するエントリを検索する（NAT table reference）。
(iii) GFA は FA に[pa1,MAC1]パラメータ値を含んだ NodeRes メッセージを送信する（NodeRes[pa1,MAC1]）。
(iv) FA2 は MN へ DHCP にてプライベート IP アドレス pa2 を割り当てる（DhcpOffer[pa2]）。
(v) FA2 は MN の移動前の IP アドレス pa1 と移動後の IP アドレス pa2 の NAT テーブルを作成する（pa2<->pa1/MAC1）。
(vi) FA2 は GFA に na2 を送信する（RegRes[pa2,MAC1]）。
(vii) GFA は RegRes メッセージにより新たに NAT テーブルを作成する（ga1<->pa2/MAC1）。このとき MAC アドレスが同一であるエントリが NAT テーブルに存在すると，新たに作成したものを使用する。
(viii) GFA は ReverseLookup メッセージを送信し，DNS は MN のドメインネームに新たな IP アドレスを登録する（“nai1”=ga1）。
(xi) GFA はドメイン登録要求を行うと，FA2 に NAT テーブル作成完了メッセージを送信する（RegAck[pa1,MAC1]）。
(x) FA2 は MN の移動前に割り当てた pa1 の解放メッセージを FA1 に送信する（Release [na1,MAC1]）。
(xi) FA2 は GFA からのパケットをアドレス変換（pa2 -> pa1）。
(xii) FA2 は MN に pa2 を割り当てる（DhcpAck[pa1]）。

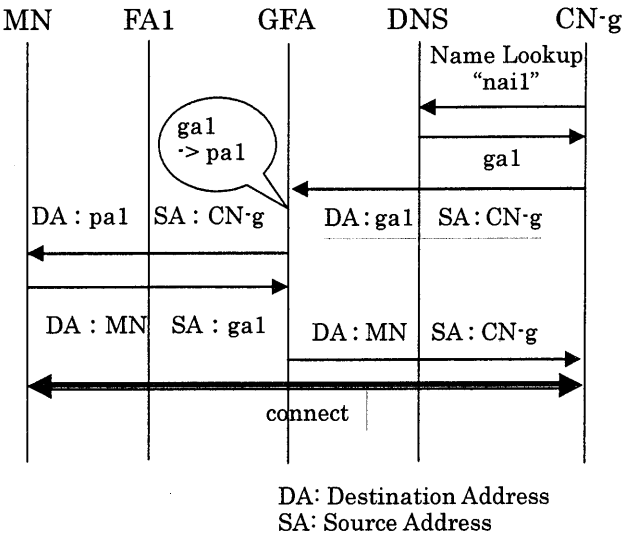


図5　CN-g から MN への通信開始時の動作

3.3.2　通信シーケンス

ここでは，グローバルネットワークへの発信，グローバルネットワークへの着信，MN のローミング時について述べる。

(a) グローバルネットワークへの発信

MN から CN-g へ通信を行う場合，GFA で NAT を用い，プライベート IP アドレスからグローバル IP アドレスに変換して通信を行う。この通信形態はプライベートネットワークからグローバルネットワークに NAT を介して通信を行う方法と同じである。

(b) グローバルネットワークからの着信

CN-g が MN に通信を始めようとするとき，MN のドメインネーム”nai1”を DNS に問い合わせる。DNS は”nai1”に登録してある IP アドレス ga1 を返信する。CN-g は ga1 をもつ GFA に接続する。GFA は，NAT テーブルにあるエントリを用いて，アドレス変換を行う（ga1 -> pa1）。宛先 IP アドレスが pa1 となり，MN へと転送される（図5）。

(c) MN のローミング時

MN のローミング時は，3.3.1 の case2 の登録動作を行う。CN-g からのパケットは GFA が FA2 宛のパケットにアドレス変換を行い（ga1 -> pa2），FA2 は自らが管理するプライベート IP アドレスから MN のプライベートアドレスに

アドレス変換を行う（pa2 -> pa1）。MN と FA は MAC アドレスを用いてデータリンクレイヤで通信を行う。このことより，新たなサブネットに移動した場合にも，MN は移動前 IP アドレス（pa1）を変えずに，通信が途切れることなく通信の継続ができる。

3.4 考察

Mobile IP はホームアドレスを持つことにより IP アドレスが変わらずに FA 間の移動ができる。また IP 層で実現するため，全てのアプリケーションが移動透過性を持つことができる。しかし，Mobile IP で移動透過性を実現するためには，Mobile IP を利用する全ての端末の IP プロトコルスタックの変更が必要になるので実現は難しい。DDNS を用いた方式では，既存の装置を拡張することなく移動透過性を実現できるが，MN のローミング時に通信が途切れるといった課題があった。

提案方式では，DNS と NAT を用いてモバイルネットワーク内に拡張した GFA と FA を設置することにより移動透過性を実現した。ホームアドレスの代わりにドメインネームを用いた。また，DNS に登録する IP アドレスを MN のプライベート IP アドレスを GFA にてアドレス変換を行ったグローバル IP アドレスにした。このことにより，CN-g からの通信の場合，MN の宛先が GFA のグローバル IP アドレスとなるため，MN がサブネットを移動しても宛先 IP アドレスは変わらない。CN-g からのパケットは，NAT テーブルにあるエントリにてアドレス変換を行い，移動先 FA のプライベート IP アドレスとなる。GFA からのパケットは，NAT テーブルのエントリにてアドレス変換を行い，またこのときの MN と FA の通信は，データリンクレイヤにて行う。これにより，MN の移動前プライベート IP アドレスを変えることなく通信の継続を行える。

また，モバイルネットワーク内の GFA と FA の拡張で実現可能なことにより Mobile IP に比べより実現を容易にした。

4. まとめ

本論文では，IP 移動透過性を実現する方式としてホームアドレスの代わりにドメインネームを用い，MN のローミング時にコネクションが維持できる方式を提案した。提案方式は，ネットワーク内部に提案する GFA と拡張した FA だけで移動透過性を実現できる。Mobile IP は IP 層で実現されるため，Mobile IP を利用する全ての端末に拡張が必要である。提案方式は，Mobile IP に比べより導入が容易である。

今後の課題として，MN のローミング時における通信の中断時間が TCP のコネクションや上位アプリケーションに与える影響を詳細に調べる必要がある。また，異なる管理主体のモバイルネットワーク間における MN のローミングの実装方式について詳細な検討を行う必要がある。

参考文献

[1] 楯岡 孝道, "DNS による IP 移動透過性の実現", IPSJ Magazine, Vol.44, No.6, pp.656-657, 2003.

[2] 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, Num.10, pp.1746-1754, 2001.

[3] 井戸上 影, 久保 健, 横田 英俊, "プライベートアドレスを使用するモバイルネットワーク間のローミング手順とその実装," 情報処理学会論文誌, Vol.42, No.12, pp.2958-2967, 2003.

[4] 石山 政浩, 井上 淳, 岡本 利夫, 寺岡 文男, "Mobile IP の現状と問題点に関する一考察," 情報処理学会研究報告, Vol.98-MBL-110, pp.71-78, 1998.

[5] A. Idoue, H. Yokota and T. Kato, "Proposal of Hierarchical Mobile IP Supporting Private Address Utilizing NAT Function and Its Implementation on UNIX Operationg System," IEICE Trans. Comnn., Vol.E84-B, No.12, pp.3155-3165, 2001.