

プライベートアドレスを3階層利用(3LPA)による大規模アドレス空間と移動

e:mail: ogawa.kiyoshi@nmiri.city.nagoya.jp, cs7039@cs.inf.shizuoka.ac.jp,
iida@hamamatsu-u.ac.jp, watanabe@cs.inf.shizuoka.ac.jp

プライベートアドレスを3階層(3LPA)用い、IP アドレスのスケーラビリティを確保するとともに、Mobile IP を利用した移動への対応について提案する。

キーワード: プライベートアドレス、3階層、MobileIP、移動対応

Mobility support and scalable address using 3 layered private address.

OGAWA Kiyoshi(*), SAWAI Arata(**), IIDA Noboru(***), WATANABE Takashi(**)

Nagoya Municipal Industrial Research Institute(*),
Faculty of Information Shizuoka University(**), University of Hamamatsu (***)

This paper proposes a scalable addressing method using 3 layered private address(3LPA) and its mobility support. The fixed 3 layered private address manage a gateway down on private address is proposed.

Keyword private address, 3 layerd, Mobile IP , mobility support

本提案では、プライベートアドレスを用い、大規模なネットワークを構築し、移動に対応することを考えた。具体的には、プライベートアドレスを三階層(3LPA)用いることによりMACアドレスよりも大きな空間を確保できる。このネットワークを Mobile IP[3]を利用して、移動に対応する方式を検討した。

1 用語

本研究では、RFC で提案されている用語を用いるほか、下記の用語を用いる。

- (1) グローバルアドレス : IPv4の32ビットのアドレスで、プライベートアドレス以外のもの。
- (2) プライベートアドレス : [2]で規定した、外部ネットワークにアドレスを送出しないで、内部ネットワークのみで利用するIPアドレス。
- (3) ゲートウェイ (GW) 異なるネットワークを接続するルータ。Mobile IPに対応していることを想定している。

2 識別子

識別子には、機器を識別するもの、利用者を識別するもの、サービスを識別するものがある。

表1 識別子の分類

	種類	分類
機器	MACアドレス	データリンク層

	IPアドレス	ルータ
	ホスト名+サブネット+ドメイン名	DNS
	電話番号	公衆網
利用者	ID	NIS
サービス	ポート番号	TCP, UDP
	メールアドレス	SMTP
	URL	HTTP

2. 1 識別子の管理

一つの識別子は、ある時間、ある時点で、一つのものを指し示していることが必要となる。これを厳しい識別子管理と表現する。厳しい識別子管理の場合でも、一つのものが、複数の識別子を持つことを許す場合と、許さない場合とがある。複数台の内線で共有している電話番号のように、識別子が一つのものを指していないか、集合を指している場合がある。これをゆるい識別子管理と呼ぶ。集合の管理が、識別子の管理と一体となっている場合と、識別子の管理と集合の管理とが切り離されている場合がある。

表2 識別子の管理

	特徴	分類	事例
厳しい識別	識別子は、一つの対象を		MACアドレス

別子管理	識別可能	一つの対象が複数の識別子を持つ場合。	IPアドレス (固定アドレス)
ゆるい識別子管理	識別子は、一つの集合を識別可能	識別子の管理と、集合の管理が別の場合。	DHCP ID

表3 識別子の管理主体

	管理区分	管理主体	管理方法
MACアドレス	上位24ビット	IEEE	OUIを厳密に管理
	下位24ビット	各組織	ユニークに
IPアドレス	プライベートアドレスの範囲	IETF	固定[2]
	グローバルアドレス	NIC	各組織に割当
	割当られたIP	各組織	各機器に割当
ドメイン名+ホスト名+ID	ドメイン名	NIC	登録名
	ホスト名、サブネット名	ネット管理者	付加可能
	ID	ホスト管理者	個別またはNIS管理

2. 2 機器の識別

機器の識別には、データリンク層ではMACアドレス、ネットワーク層においてはIPアドレス、それより上位ではドメイン名を含むURL、メールアドレスを利用することがある。MACアドレス以外に、機器固有の番号を利用することも可能である。例えば、電話番号は、世界中で唯一の番号付けをしている。

2. 3 利用者の識別

利用者の識別は、携帯電話のように個人が利用することが前提となっている機器の場合には、機器の識別子と同一であってもよい。メールサーバのように、複数人で利用することがある場合には、IDという形で、その機器名に付加した形で利用する。IDは、特定のホストだけで有効な場合と、ネットワークで有効となるIDとがある。IPSに取得したIDは、ネットワークに接続する機器が利用できることが前提となっており、そこ

からIPSに接続し、IDとパスワードにより、電子メール、特定のサービスが利用可能となる。

表4 IDとネットワーク

	範囲	特徴
ID	その機器のみ	複数人利用
NIS、NIS+	ネットワーク内の対象機器	管理の簡便化
IPSのID	接続後に利用可能	接続する機器のIDが利用可能である

2. 4 サービスの識別

ポート番号をアービス識別子として用いる場合がある。メールアドレス、URLのように、規定のサービス名固有の形式であるため、ポート番号を省略することがある。電話番号、IDを複数保持する場合には、それぞれの番号に応じたサービスを利用する場合があり、これらは、サービスの識別に用いる場合である。

表5 複数主体の利用と複数個利用

	複数主体による利用	複数個の保持	主体名
MACアドレス	GWの間接利用	あり	PC、PDA
IPアドレス	GWの間接利用、DHCPによる再利用	あり	PC、PDA
ホスト名	GW、サーバの間接利用	あり	PC、PDA
電話番号	内線電話による共有	あり	電話機
ID	ありえる	あり	人

2. 5 識別子の登録場所

表6 主な登録場所

	主たる登録場所	その他の登録場所	関連情報
MACアドレス	その機器	ブリッジ (ルータ)	IEEEによるOUIの登録
IPアドレス	端末	ルータ	NIC
ドメイン名	DNSサーバ	端末	NIC
利用者ID	ホスト、NISサーバ	端末、本人	NISサーバ DNSサーバ
サービス	サーバ	端末	サービス毎

機器の場合に、MACアドレスのように、その機器自体が登録番号を持っているものがある。しかし、MACアドレスは、IEEEによるOUIの管理がしっかりしていることを前提としている。IEEEのOUIの登録ののち、個別の機器

上の登録が可能であるため、登録の仕組みとしては、2階層と考えることができる。また、現在のネットワークに、どのようなMACアドレスの機器がつながっているかを知り、テーブルを持つ場合がある。

2. 6 MACアドレス

Macアドレスは、2の48乗、すなわち、281474976710656、つまり2.8*10¹⁴、10の14乗の個数の機器を識別できる。上位24ビットは、会社名の登録であり、すべてのビットを使用しきっていない。各会社では、2の24乗、すなわち16777216、10の7乗の機器を識別できる。1677万台以上出荷している企業では、2つ以上の会社の識別番号を取得している。

2. 7 IPアドレス

ネットワークアドレス、ブロードキャストアドレスを含めた場合である。利用可能は、クラスA、クラスB、クラスCごとにネットワークが存在し、階層的に管理している場合である。

2. 7. 1 グローバルアドレス

IPv4のグローバルアドレスは、2の32乗よりも小さな数しか対応できない。すべての機器を、ユニークになおかつシームレスに識別するには、IPアドレスの枯渇が課題になる。

2. 7. 2 プライベートアドレス

表7 プライベートアドレスの種類

クラス	開始アドレス	終了アドレス	Prefix	
A	10.0.0.0	10.255.255.255	10/8	クラスA 1個分
B	172.16.0.0	172.31.255.255	172.16/12	クラスB 16個分
C	192.168.0.0	192.168.255.255	192.168/16	クラスC 256個分

プライベートアドレスは、1つのグローバルアドレスでインターネットに接続されているネットワークの内部を管理するのに道いることができる。プライベートアドレスには、クラスA、クラスB、クラスCの3種類のアドレスがある。下記アドレスは、RFCで宣言されており、戸別のネットワーク内部で、長期的に安定的に利用可能である。各クラスのアドレスは、グローバルアドレスを割り当てないアドレスとして、あらかじめ予約さ

れており、外部ネットワークに、このアドレスでデータを転送しないことになっている。

表8 グローバルとプライベート

	グローバルアドレス	プライベートアドレス
IPの付与	付与されているアドレス数内	機器の増加を想定したアドレス付与方式を設定可能
サブネット	与えられた数の範囲内でのみサブネット作成可能	機器の増加を想定したサブネット設定可能
ネットワークの変更	外部への影響あり	ゲートウェイを変更しなければ変更なし

グローバルアドレスに対して、プライベートアドレスでは、内部ネットワークの設計に柔軟に対応できる。

2. 8 ドメイン名

WEBのURL、電子メールアドレスは、ドメイン名上で定義されている。ピリオドで分割したネットワークにおいて、アルファベットのみを用いた場合でも、4文字で、4区分でも、10の22乗を識別できる。たとえば、著者の一人が管理しているドメイン名は、"Nmiri.city.Nagoya.jp"である。この4文字、4文字、6文字、2文字は、表1の4文字、4区分と同一のドメインを表現できる。

表9 文字で表現できる規模

	例	数	文字数
1	A	26	1
2	Ab.cd	456976	5
3	Abc.def.ghi	5*10 ¹²	11
4	Abcd.efgh.ijkl.mnop	4*10 ²²	19
5	Abcde.fghij.klmno.pqrst.uvwxy	2*10 ³⁵	29
6	-(too long)	8*10 ⁵⁰	41

表10 サービスにおける名前とポート番号

	ドメイン名のみ	ドメイン名+ポート番号
FTP	ftp.domain.jp	Domain.jp:25
HTTP	www.domain.jp	Domain.jp:23
mail	Mail.domain.jp	Domain.jp:25
pop	Pop.domain.jp	Domain.jp:100

URLのポート番号、プロトコル名ごとにホスト名を変えることによる識別は、現状では、名前の識別数を1桁増える程度である。

3 識別子の時間的変化と移動

識別子の時間的な変化には、登録、取消し、移動の3種類が考えられる。移動は、登録と取消しの組み合わせであると考えられる。移動前と移動後のサービスの整合性を考慮すると、移動として一括で理解するとよい。時間的な変化の最も特徴的な事例として、移動を検討する。各識別子には、事実上変更されない部分、管理組織がしっかりしている部分、長期的に変更しない部分がある。3つの識別子のうち、プライベートアドレスの取り決めは、長期的に安定している。この仕組みを、利用することにより、移動における識別子を検討する。

表11 時間的な変化の長い識別子

	変更期間	管理組織
プライベートアドレス	長期(RFCの改訂による)	IETF
MACアドレス上位24ビット	新規追加は随時	IEEE
ドメイン名	随時変更	NIC

機器の移動には、閉じたサービスの範囲内では、閉じたサービスに対応した識別子を持っていればよい。インターネット接続、異なる管理主体下にあるネットワークの移動を考慮する場合には、世界的な管理の仕組みのある識別子での移動対応するとよい。

表12 移動と課題

移動の種類	対応方法	課題
携帯電話	電話番号	ローミング
データリンク	MACアドレス	利用許可
ネット内移動	IPアドレス	
ネット外移動	Mobile IP	HA, FAの実装
IP非依存移動	DHCP	貸与IP数

3.1 電話番号を持った移動

電話番号を持った移動は、携帯電話である。異なる管理主体間のサービスの移動対応は、ローミングと呼ばれ、あらかじめ管理主体間の契約と変換方式が設定されている。

3.2 MACアドレスを持った移動

MACアドレスを持った移動は、MACアドレス対応するネットワークサービスでは、該当MACアドレスの利用の許可、不許可が設定可能である。移動への対応は、ネットワーク間での設定による。

3.3 IPアドレスを持った、ネットワーク内の移動

ネットワーク内の移動では、IPは移動に対応できる。例えば、同じネットワークの接続口が2箇所に設置してある場合に、あるIPアドレスを持った機器を一方から他方に移動しても、移動後に同じIPアドレスを利用

しつづけることができる。この際に、同じネットワーク(サブネット)内であれば設定の変更の必要はない。

3.4 IPアドレスを持った、ネットワーク外への移動

IPアドレスを持った、ネットワーク外への移動対応が、Mobile IPである。Mobile IPは、グローバルアドレスを前提にしていたが、3LPAでは、プライベートアドレス3階層において利用する拡張を提案する。

4 プライベートアドレス

プライベートアドレスは、その利用する組織で、内部の構造を設計し、ユニークな識別子として利用することができる。プライベートアドレスでは、そのネットワーク内での通信ができればよく、それ以外は、GWにおける機能だけを利用する場合がある。この場合には、各ネットワークのユニーク性は必要とならない。ネットワーク全体を管理することを検討する場合には、ユニークな番号付けの規則を定めることは有用であり、推奨できる方式が確立するとよい。

4.1 フラットなプライベートアドレス

プライベートアドレスを、1階層だけで用いる場合には、ユニークな識別子として、IPアドレスを利用することができる。

クラスA、クラスB、クラスCで割り当てられたものを、平行して利用した場合に、17891328個のアドレス空間が表現できる。

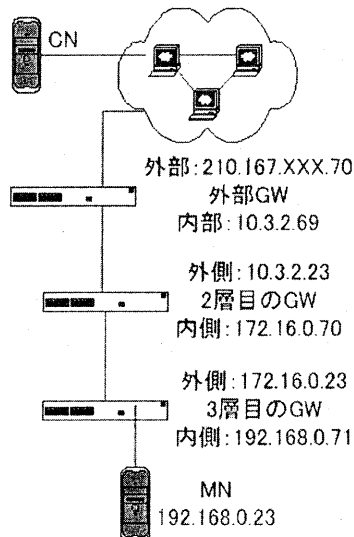


図1 3階層プライベートネットワーク

4.2 2階層用いた、プライベートアドレス

1層目と2層目を同じクラスを利用しないのは、ネットワークの設定変更の際に、GWの上と下で同じアドレスが登場する可能性をなくすためである。IPアド

レス、ネットワーク構造を変化させないという前提にたてば、もっと大きなアドレスを割り当てることが可能である。この方法では、MACアドレスで表現できるアドレス数よりも少ない。全機器をプライベートアドレスで振り分けることができない。

4. 3 3階層用いたプライベートアドレス

3層用いる場合、1層目と2層目を同じプライベートアドレスの異なる値をとることは可能である。また、1層目と、3層目とを、同一のアドレスで設定することも可能である。例えば、1層目は、ルータ、スイッチングハブのネットワーク機器のみに設定し、3層目は、端末機器のみに設定する規則にしていれば、複雑な設定状態をまぬかれることはできる。

表13 三階層プライベートアドレスの諸元

項目	内容
管理主体	ネットワーク管理者
識別子	IPアドレス+各GWのIPアドレス
登録場所	GW(HA), 端末(MN)
移動対応	IP, Mobile IP, DHCP
対応IP数	10の18乗

4. 4 固定的3層プライベートアドレス(3LPA)

クラスA、クラスB、クラスCの3階層を、それぞれ異なる層に固定して用いたネットワークで、10の18乗のアドレス空間が確保できる。これは、MACアドレスよりも十分大きい。そのため、これ以上の階層付けを行うのではなく、3階層に固定した管理方法を検討する。

3階層用いる場合には、ネットワークの管理上、どのクラスを1層目で用い、どのクラスを2層目で用い、どのクラスを3層目で用いるかを決めてみると、ルーティングが簡単である。

この場合に、どの層を1層目にし、どの層を2層目にとするとよいかは、ネットワークの設計上の課題となる。また、各層をサブネットとして管理するかどうかにもよる。この6種類の層別に限定すれば、その方式の識別子を表のように定め、ネットワークが管理に利用することができる。端末が第3層のみを利用することを限定してあれば、移動前と移動後で、ネットワークの設定について、大きな変更をせずに利用できる可能性がある。

現時点では、原則として厳しい識別子管理を行えば、移動に伴うIPアドレスの転送が可能であり、DHCPによる管理と連動可能であるが、推奨方式は、その他の条件が特定できないため評価できていない。固定的3階層構造をとっていると次の利点雅考えられる。

- ・アドレスで、どの層かがわかる。(アドレスの理解

性)

- ・アドレスで、どの順番でルーティングすればよいか

がわかる。(ルーティングの理解性)

- ・アドレスの不適切な設定がわかる場合がある

- ・移動後のクラス、サブネットを変えなくてもよい場合がある。

- ・網の接続方法を変更した場合の、対処方法が限定できる。

- ・ネットワーク、機器の識別のための登録情報を、GW、HA、端末に登録できるためいずれをも利用可能である。

表14 三階層プライベートアドレス拡張

暗号化	登録内容
平文	外部ゲートウェイの外部アドレス
拡張	暗号化識別子拡張
暗号化	外部ゲートウェイの内部アドレス
暗号化	2層目のゲートウェイの外側アドレス
暗号化	3層目のゲートウェイの外側アドレス
暗号化	MNプライベートアドレス

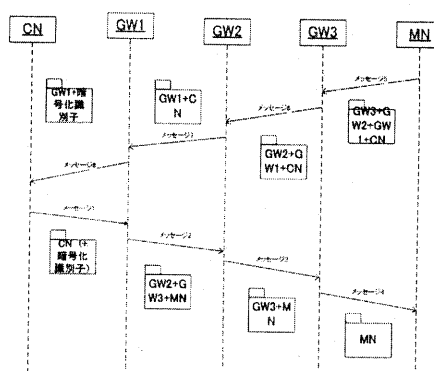


図2 パケットの流れ

プライベートアドレスは、組織内で管理するため、各GWに、整合性をとるための設定を行うことを前提にできる。HAが3層目のネットワークに存在する場合でも、HAが1層目に存在する場合でも、各ゲートウェイのアドレスを識別子として付加して用いることにより、ユニークなアドレス空間が確保できる。外部ゲートウェイの内部アドレス、2層目のゲートウェイの外側アドレス、3層目のゲートウェイの外側アドレス、MNプライベートアドレスの4つのアドレスを暗号化したものを識別子として用いる。実際には、MNから

GW1 までは、MN, GW3, GW2, GW1 の情報を持ち、GW1 で暗号化識別子にする。CN から来た暗号化識別子は、GW1 で解読し、GW2, GW3, MN の経路に翻訳する。

4. 5 プライベートアドレス3層管理の課題

3LPA の課題は、GW のアドレスを前提としているため、GW がダウンした場合の、ネットワークの回復方法、接続方法である。プライベートアドレスの付与方法を、固定的に決定していれば、GW がダウンした場合の接続の回復については定型的な処理が可能である。そうでないと、どのネットワークが、どの時点でダウンし、どこどこが接続されているかを、ネットワーク全体で調整する必要がある。

3階層を固定的に指定し、各 GW と端末で各 GW のアドレスを管理していれば、特定の GW がダウンした場合には、他の GW 機能をもった機器に代替機能を働かせることにより、網をすみやかに回復させることができる。主な回復手順は、下表の通りである。

表 15 GW (HA) ダウン時の回復手順

順番	事象
1	GW 2 (HA) ダウンの MN による検出
2	MN による GW2' による経路の起動
3	GW2' による仮想ネットワークの起動
4	MN と GW2' による通信の開始
5	CN と GW2' の通信の回復

4. 6 スケーラビリティ

移動対応では、ドメイン名ではホスト名重複を解決する必要がある。プライベートアドレスでは、Mobile IP を利用することが可能である。

表 16 ドメイン名とプライベートアドレス

	ドメイン名	プライベート
拡張	文字数、階層	階層の段数
制約	文字数	転送方式
規模	10の20乗以上	10の18乗程度
変化	既得権	固定
移動	ホスト名重複	Mobile IP 利用
統合	サブネット名	1層目のアドレス

組織が統合した場合に、ドメイン名は変更する可能性がある。サブネット名に同一の名称がなければ、ドメイン名の変更だけで統合可能な場合がある。プライベートアドレスでは、組織の統合に際して、1層目のアドレスに重複がなく、階層構造が同じであれば変更なく対応可能な場合がある。

5 まとめと今後の課題

プライベートアドレスを3階層で利用することにより、MAC アドレス以上の空間を確保する方式を提案

した。3層のプライベートアドレスでは、アドレスの変換ではなく、経路上のアドレスを付加し、ゲートウェイで暗号化識別子とする方式を提案した。内部のプライベートネットワーク上の GW がダウンした場合の対応方法についても提案した。ゲートウェイまでの経路情報の暗号化は、内部のネットワーク構造を外部に伝達することになるため、暗号化しよりの具体化においてセキュリティの考慮が課題である。

参考文献

- [1] Internet Protocol, IETF, RFC791, 1981
- [2] Y. Rekhter, Address Allocation for Private Internets, RFC1918, February 1996
- [3] Charles Perkins, IP Mobility Support, RFC3220, IETF, 2001
- [4] Farid Adrangi, Prakash Iyer, Mobile IPv4 Traversal Across VPN or NAT and VPN Gateways, draft-adrangi-mobileip-natvpn-traversal-01.txt, February 23 2002
- [5] 小川清, 渡辺尚, 移動体通信におけるサービス品質の体系化, 62回情報処理学会全国大会 6T-6
- [6] 西村泰行, 阪智貴, 小川清, 渡辺尚, 移動体通信規約のための通信シミュレーションの設計, 62回情報処理学会全国大会 6T-7
- [7] 小川清, 澤井新, 飯田昇, 渡辺尚, 場合分けによる Mobile IP 経路最適化における 1 方式, MBL18-2-5
- [8] 小川清, 澤井新, 渡辺尚, 飯田登場合分けによる Mobile IP 経路制御最適化における登録方式について, 63回情報処理学会全国大会, 4E-5
- [9] 横口健介, 小竹一也, 小川清, 斉藤直希, インタネット経由する無線端末間経路最適化通信規約の実験装置の設計, 63回情報処理学会全国大会 IF-3
- [9] 澤井新, 小川清, 飯田登, 渡辺尚, Mobile IP における経路最適化選択指標の検討, MBL19-11
- [10] 澤井新, 小川清, 飯田登, 渡辺尚, 場合分けによる Mobile IP 経路最適化における事前, 事後登録方式の検討, 信学会 2001 年 ソサエティ大会 B-6-85
- [10] 横口健介, 小竹一也, 小川清, 澤井新, 飯田登, 渡辺尚, Mobile IP のプライベートアドレス拡張について, 信学会全国大会 2002-B-6-113
- [11] 井戸上 彰・横田英俊・長谷川 亨・加藤聰彦, 独立したプライベートアドレスを使用するモバイル IP ネットワーク間のローミング手順, 信学会全国大会 2002-B-6-111