IPv6 におけるネットワーク内部の隠蔽方式の提案

久保敷　透

IPv4 ではアドレスの枯渇に対して，根本的な解決策として IPv6 への移行が必須とされている．IPv4 では，これまでプライベートアドレスを定義し，NAT を設置することによりアドレスを延命させてきた．また，NAT を使用することでネットワークが隠蔽されるという利点があった．IPv6 へ移行した場合においても同様にしてネットワークを隠蔽したいという強い要望がある．これを実現するための一方式としてルータに任意に設定したアドレスをホストルートとして設定する方法がある．しかしこの方法では，ルータの設定に手間が掛かることや，IPv6 アドレス生成時の重複アドレスの検出がルータを越えて実現できないなどの問題がある．そこで本発表では，ルータに対してホストルートを自動的に設定し，かつアドレスの重複を確実に防止できる方式を提案する．

Researches on a conceal method of network in the IPv6

Toru Kuboshiki

With the exhaustion of the IPv4 address, it is assumed that a shift to the IPv6 is required as an ultimate solution. It was advantageous in that a network was concealed by using NAT in IPv4 as an anti-exhaustion measure. There is a strong demand I do it equally when I shifted to IPv6, and to want to conceal a network. The method of setting the address arbitrarily set to the router as one method to achieve this as a host route is proposed. However, there is the problem that the setting of the router requiring trouble and The IPv6 address duplication detection when generated it is not possible ahead of a router by this method. Therefore, in this announcement, I set a host route for a router automatically and suggest the method that can prevent the duplication of the address surely.

1. はじめに

インターネットを利用する機器の増加により IPv4 アドレスの不足が問題となっており，IPv4（Internet Protocol version 4）は数年で枯渇すると予測されている[1)]．IPv4 では枯渇問題の短期的な解決策として，プライベートアドレスを定義し，組織内でこのアドレスを使いまわす方法をとってきた．組織内の端末がインターネットへ接続する場合には NAT（Network Address Translation）を必要とする．NAT はプライベートアドレスをグローバルアドレスへ変換する機能を持ち，一つのグローバルアドレスを複数の端末で共有することによりアドレスを節約できる．この結果，組織内のインターネット側から組織内の端末やネットワーク構成などが隠蔽されるという副次的な利点があった．その反面，インターネット側から組織内へ向けて通信を開始することができない，いわゆる NAT 越え問題も発生している．

そして，枯渇問題を根本的に解決する方法として考えられたアドレスが IPv6（Internet Protocol version 6）である．IPv6 は IPv4 よりも広いアドレス空間を持ち，アドレスが不足する問題を解決している．これにより IPv6 へ移行した場合には，NAT が必要なくなる．しかし，NAT がなくなることにより，ナットワーク内部を隠蔽できるという利点がなくなる．また，IPv6 では端末自身がアドレスを生成することができる特徴がある．インタフェース ID を MAC アドレスから生成することで，アドレスの割り当てが容易になるという利点がある．しかし，MAC アドレスが不変であることから，生成されるインタフェース ID も不変になってしまい，端末を特定することができてしまう．

そこで，IPv6 においても端末やネットワーク構成を隠したいという要望からさまざまな研究が行われている[2)–6)]．まず端末のプライバシー保護の問題を解決するアドレスとして，一時アドレス（以下 TA：Temporary Address）[4)] がある．TA は IPv6 アドレスの下位 64 ビットのインタフェース ID をランダムに生成することで端末の特定を防ぐことができる．しかし，このアドレスでは，サブネット ID が見えているため，ネットワーク構成が予測できてしまう．ネットワーク

構成を隠蔽する技術として，NAT66（IPv6-to-IPv6 Network Address Translation）[5] や Mobile IPv6[6] を用いた方式がある．NAT66 では，IPv4 で利用してきた NAT と同様に，IPv6 においても NAT を利用するものである．しかし，IPv6 においても NAT を利用することに関して，必要ないという意見もある[7]．Mobile IPv6 を用いた方式では，ネットワークのゲートウェイがホームエージェントの役割を果たし，ホームアドレスにネットワーク内部を隠蔽できるアドレスを用いることで，ネットワーク構成を隠蔽する方式である．しかしこの方式は，Mobile IPv6 を基に考えられているため，そのまま Mobile IPv6 の課題が残されたままになってしまう．

本稿では，ネットワーク内部を隠蔽する方式として，端末に外部通信用アドレスと内部通信用アドレスを持たせ，通信端末によりアドレスを使い分ける．また，外部通信用アドレスにはネットワーク内部を隠蔽できるアドレスを用い，このアドレスのルーティングを可能とするための設定を行う．そして，外部通信用アドレスを生成し管理できるサーバを設置する．

以下，2 章で NAT66 と Mobile IPv6 の詳細を説明し，3 章でホストルートを用いた提案方式について述べる．そして 4 章で考察，5 章でまとめを行う．

2. 既存技術

2.1 NAT66

IPv6 では NAT を使用せずに自由に通信が行えることを目的として考えられている．しかし，NAT を利用することで企業などはネットワーク内の管理が容易になることや，セキュリティを高めることができるという考えから，IPv6 においても NAT が必要であるとし，NAT66 が考えられた．NAT66 においても，ネットワーク内部には，内部でのみ有効なアドレスを用いる．そして，インターネットへ接続する際にグローバルアドレスへ変換する．また，IPv4 における NAT のような内部からの通信を開始することにより，マッピングテーブルが生成されるため，外部から通信を開始できないという NAT 越え問題が起こらないように，双方向マッピングが可能となっている．アドレスを変換する部分はプレフィックスとサブネット ID であり，インタフェース ID は変換しない．また，IP ヘッダのチェックサムを変更しないようにアドレスを変換することで，トランスポート層に影響を与えないようにしている．**図 1** に NAT66 の動作を示す．NAT66 機器の内側のプレフィックスには ULA（Unique Local Unicast IPv6 ）[8]，外側にはグローバルなプレフィックスが割り当てられている．NAT66 は前半の 64 ビットのみを変換していることから，この 64 ビットの中でチェックサムの値を調整する．内側と外側のプレフィックスは決められた値に変換されるため，この変換で生じるチェックサムの差異をサブネット ID により調整し，結果的にアドレス全体のチェックサムが変わらないようにする．これによりチェックサムの再計算をする必要がない．しかし，IP アドレスを書き換えているため，ペイロード内に IP アドレスを含む SIP や FTP などのプロトコルではアプリケーションごとに対応が必要になってくる．

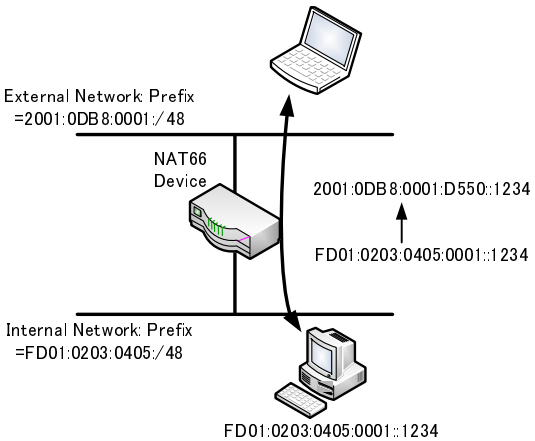

図 1 NAT66 の動作
Fig. 1 Movemet of NAT66

2.2 Mobile IPv6 を用いた方式

図 2 に Mobile IPv6 を用いたネットワーク構成の隠蔽方式を示す．この方式ではゲートウェイが Mobile IPv6 におけるホームエージェントの役割を果たしている．内部端末 IN（Internal Node）にはホームアドレス（HoA：Home Address）としてサブネット ID が任意に設定されたアドレスが割り当てられる．この任意のサブネット ID が割り当てられている領域を論理サブネットと呼ぶ．この論理サブネットは実際のトポロジーに関係なく存在する．そして，それとは別に実際のネットワーク構成に応じた気付けアドレス（CoA：Care-of Address）が割り当てられる．IN はホームエージェントに HoA と CoA の関係を登録しておく．外部端末 EN（External Node）にはグローバルアドレス G1 が割り当てられている．外部端末 EN が IN と通信を行う場合，送信元アドレスを G1 とし，宛先アドレスを HoA としてゲートウェイへ送信する．HoA のプレフィックスはインターネット上でルーティングが可能であるので，ゲートウェイまでパケットは

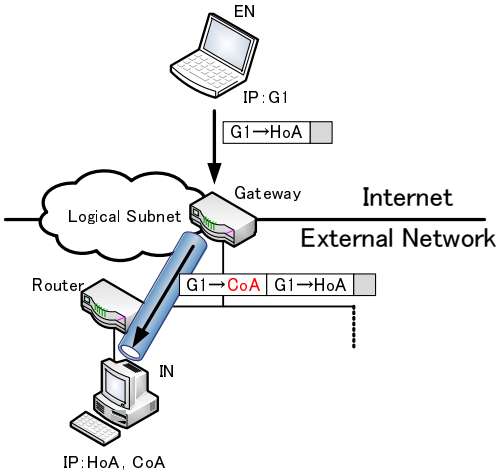

図 2 Mobile IPv6 によるネットワーク構成の隠蔽方式
Fig. 2 network topology concealment by Mobile IPv6

届けられる．このパケットの宛先アドレス HoA ではネットワーク内部をルーティングすることができない．そのため，内部でルーティングが可能であるアドレス CoA を宛先アドレスとした IP ヘッダでカプセル化し IN へ送信する．外部端末は論理サブネット宛てにパケットを送信しており，実際のサブネット ID を見ることができず，論理サブネットと実際のサブネットの関係はゲートウェイのみが把握しているため，ネットワーク構造を隠蔽することができる．しかしこの方式では，バインディングアップデートにより外部端末に気付けアドレスを通知しないように経路最適化を行わない．そのため，内部端末同士の通信を行う場合にも，ホームエージェントを経由して通信を行わなければならないため，冗長経路になる．

3. 提 案 方 式

本稿では，端末に 2 つのアドレスを保持させ，アドレスを使い分けることでネットワーク内部を隠蔽する．外部の端末と通信を行う場合には，ランダムに生成したアドレスを用いて通信を行い，内部端末同士の通信では，内部でのみ有効なアドレスを用いて通信を行う．外部との通信で用いるアドレスにはホストルートを設定する．以下に提案方式で用いる 2 つのアドレスやホストルート，新しく導入するサーバについて説明し，動作について述べる．

3.1 アドレス定義

提案方式で用いる 2 つのアドレスについて説明する．内部端末との通信には ULA を用いる．これは IPv4 におけるプライベートアドレスと同様のアドレスとしてサイトローカルアドレスというものがあったが，このアドレスはアドレスの重複の可能性などの問題により廃止された[9]．その代わりとして ULA が考えられた．ULA は高い一意性を持っているため，アドレスが重複する可能性が低くなっている．また，ULA はネットワーク内でのみ使用することを目的として考えられており，インターネットでの使用は推奨されていない．

一方，外部端末と通信を行う場合は，ネットワーク内部を隠蔽できるアドレスとして，サブネット ID を含めた下位 80 ビットをランダムに生成する CA を導入する．アドレスには期限を設け，定期的に CA を更新することで更にネットワーク内部が読み取られるのを防ぐ．CA はサブネット ID もランダムに生成されているため，パケットをルーティングすることができない．そこでホストルートを利用する．

3.2 ホストルート

ホストルートとは端末までのルートをルーティングテーブルに一意に設定するものである．通常のプレフィックスによるルーティングをプレフィックスとインタフェース ID の組み合わせによりルーティング先を決定する方法である．これによりサブネット ID がランダムである CA においてもルーティングが可能となる．しかし，全ルータに端末のホストルートを設定することは，ルーティングテーブルを膨大させてしまう．また，IPv6 では端末にアドレスが割り当てられたときに，アドレス重複検出を行う．この範囲は同一サブネット内のみでルータを越えて検出することはできない．この方式で用いるアドレスは，実際のサブネットに関係なくサブネット ID がランダムであるため，アドレス重複検出が行えない．

3.3 CAS

隠蔽アドレス管理サーバ（CAS:Concealed Address Management Server）では，ホストルートでの課題の解決や CA の管理などに用いる．以下に機能を述べる．

(1) CA の管理

端末からアドレスの要求があった場合に，外部通信用アドレス CA を生成し，端末に割り当てる．すべての CA は CANS で管理し，どの端末にどの CA が割り当てられているのかを把握しているためアドレスは重複しない．また，CA の有効期限も管理し，有効期限が過ぎた CA のホストルートを削除する．

(2) ホストルートの自動設定

端末に CA を割り当てたのち，CAS は端末までパケットをルーティングできるようにホストルートを設定する．ホストルートの設定は，端末が所属しているサブ

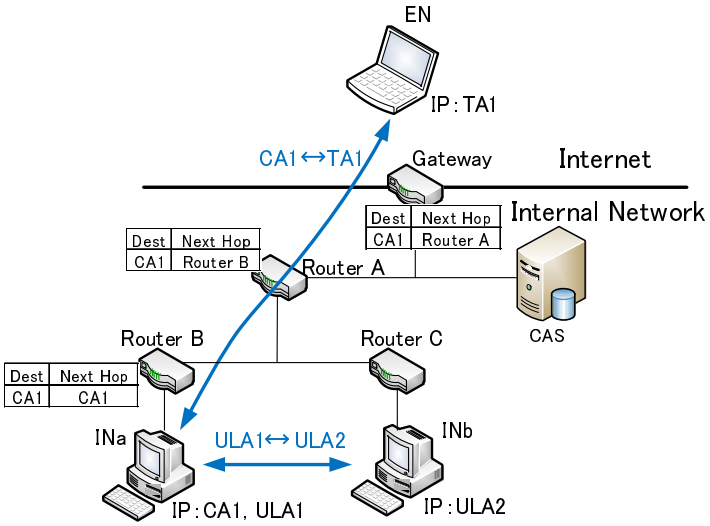

図 3 提案方式の概要
Fig. 3 A proposal method

ネットのルータからゲートウェイまでのルータに対して行う．これにより，ルーティングテーブルのエントリー数の増大を抑える．

(3) ネットワーク構成の把握

CAS はホストルートの設定のために，端末が所属しているサブネットを把握し，必要なルータにのみホストルートを設定する．そのため，ネットワーク構成を把握しておかなければならない．その方法としてネットワークを監視するために用いられるプロトコルである SNMP（Simple Network Management Protocol）を利用する方法がある[10]．提案方式では，マネージャである CAS が監視対象であるルータの MIB（Management Information Base）を参照することでネットワーク構成を把握する．

3.4 提案方式の概要

図 3 に提案方式の概要を示す．内部端末の INa は ULA1 と，CA の 2 つのアドレスが割り当てる，INb は INa とは異なるサブネットに所属しており，ULA2 のみ割り当てられている．外部との通信を必要としない端末では，CA は割り当てない．外部端末である EN には，一般に生成される TA 割り当てられている．そして，ネットワーク内に CAS が設置されており，CAS はネットワーク構成を把握しており，INa に割り当てられている CA1 のホストルートがゲートウェイ，ルータ A，ルータ B に設定されているとする．INa が INb と通信を行う場合は，通信相手が内部端末と判断すると ULA1 を用いて通信を行う．ULA1 は通常のプレフィックスによるルーティングにより通信が行える．一方，EN と通信を行う場合は CA1 を用いて通信を行う．外部からパケットがゲートウェイに到達したとき，それぞれのルータはルーティングテーブルに記載されているホストルートを参照することで INa までパケットを届けることができる．

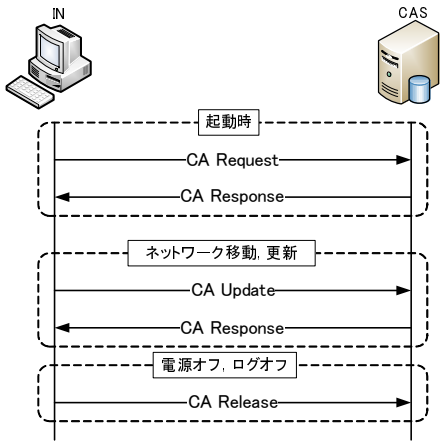

図 4 CA の取得，解放
Fig. 4 terminal and the server

3.5 CA の取得と開放

図 4 に CA の取得と開放について示す．端末は CAS に対しアドレスの取得要求やアドレス解放などの要求を出す．端末の起動時に CA を要求する CA Request を CAS に送信する．それに対し CA を生成し，CA Response により CA を通知する．また，端末がネットワークを移動した場合に ULA が変更されるため，

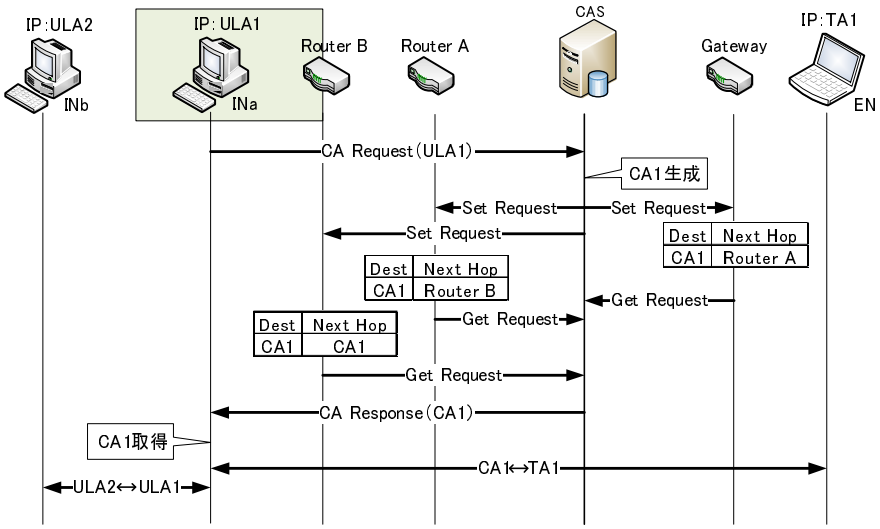

図 5 CA の取得動作
Fig. 5 An assignment process of CA

新たな CA とホストルートの再設定を要求するため CU Update を送信したり，電源を切ったりログオフした時のアドレスを解放するための CA Release を送信する．それぞれの動作について説明していく．

3.6 CA の取得動作

図 5 に INa における CA の取得動作を示す．ネットワーク構成については図 3 と同様であり，INa はルータ B の配下に存在する．まず始めに，INa は ULA を生成するために必要なプレフィックス情報を，ルータ広告により取得し ULA1 を生成する．外部の端末との通信が必要な場合には，あらかじめ CAS のアドレスを登録しておき，CA を取得するために CAS へ向かって CA を要求する CA Request を送信する．CA Request の送信元アドレスは ULA1 である．これを受け取った CAS はアドレスが重複していない CA1 を生成する．次に ULA1 が割り当てられているサブネットと，あらかじめ SNMP により取得しているネットワーク構成から，外部までの通信ルートに対応するルータにホストルートを設定する．図 5 の場合はルータ A とルータ B，ゲートウェイにホストルートを設定する．ホストルートの設定方法にも SNMP を利用する．SNMP は管理対象の MIB を参照するだけでなく，MIB の情報を変更することができる．これによりルータのルーティングテーブルにホストルートを設定する．CAS は対応するルータに対し Set Request パケットを送信し，MIB 情報を変更するよう要求する．それに対しルータは Get Response パケットを応答する．ルータすべてから Get Response が返ってきたら，INa へ CA Response を送信し CA1 を通知し，INa は CA1 を割り当てる．CA1 を割り当てられた INa は外部端末には CA1，内部端末には ULA1 とアドレスを使い分けて通信を行う．

3.7 ネットワーク移動時と更新の動作

図 6 にネットワークを移動したときの動作を示す．内部端末 IN がルータ B の配下からルータ C の配下へ移動しネットワークが変わった場合，新たにルータ C からルータ広告を受け ULA3 を生成する．そして，今まで利用してきた CA1 に対するホストルートを変更しなければならない．そのため，新しく生成した ULA3 を用いて CAS にネットワークを移動したことを知らせる CA Update を送信する．CA Update のパケットにはネットワークを移動する前に使われていた CA1 の情報が記載されている．もし，更新の動作であればすでにホストルートは削除されているため，以前使っていた CA の情報か記載されない．この情報を基に CAS は各ルータ，ゲートウェイにホストルートの再設定を行う．ルータ A，ルータ C，ゲートウェイにはホストルートの変更，追加を行い．ルータ B にはホストルートを削除する．

3.8 CA の解放

端末が電源を切ったり，ログオフした場合には，CA を解放する CA Release を CAS に送信する．これを受け取った CAS は CA のホストルートの設定をすべて削除する．また，期限が切れた CA も同様にホストルートを削除する．

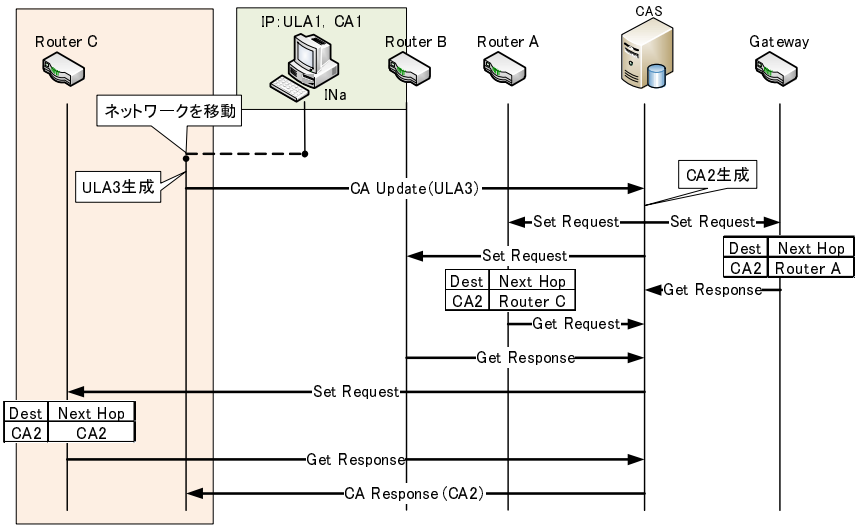

図 6 移動時の動作
Fig. 6 An assignment process of CA

4. 考　　察

本稿では，ホストルートをネットワーク内部を隠蔽する方式として利用し，2 つのアドレスを使い分け，ホストルートで挙げられる問題を解決した．既存技術である NAT66 はゲートウェイを改造するのみだが，IP アドレスを書き換えているため，データ内にアドレス情報を必要とするアプリケーションなど，通信が制限されてしまう．Mobile IPv6 を利用したネットワーク内部の隠蔽方式では，ネットワーク内部のすべての端末に Mobile IPv6，ゲートウェイにホームエージェントの機能を実装しなければならず，導入コストが高いと考えられる．また，経路最適化を行わないため，ゲートウェイにトラフィックが集中してしまうことや，カプセル化によるオーバヘッドなどによる遅延が起こってしまうと考えられる. 提案方式では，導入コストも Mobile IPv6 を用いた方式よりも低く抑えることができ，NAT66 のような通信に制限が発生してしまうことはない．

提案方式では，下位 80 ビットをランダムに生成した CA を用いるため，ホストルートを利用している．ホストルートの設定は CAS が自動的に行うため，手間がかからない．また，ネットワーク内で障害が発生し，どこかのルータが機能しなくなったとしても，CAS では SNMP が機能しているため，障害を検知しホストルートの再設定も可能であると考えられる．

またホストルートでは，エントリー数が膨大になってしまう問題があるが，提案方式では，ネットワーク内のルータは自身の配下に属している端末のホストルートのみで良いためエントリー数の増大を抑えることができる．しかし，ネットワーク構造をツリー構造に例えるとすると，葉の近いルータほど効果があるが，根に近いルータほどやはりエントリー数は増大してしまう．このときゲートウェイに関しては，すべての端末のホストルートを所持することになる．提案方式で適用できるネットワークの規模に関しては，各ルータのメモリ容量に影響されると考えられ，一番ルーティングテーブルのエントリー数が多くなるゲートウェイが収容できるエントリー以下の端末が存在するネットワークに限られてくる．さらに収容できる端末数を増やしたいと考えるならば，CAS を複数設置し，それぞれの CAS で範囲指定された中で CA の生成をすることでルーティングテーブルの増大を更に抑える方法が考えられる．

表 1 評価
Table 1 Evaluation

	導入コスト	アプリケーション	負荷
NAT66	○	×	○
Mobile IPv6	×	○	△
提案方式	△	○	△

5. ま と め

本稿では，ネットワーク内部の隠蔽方式の提案として，通信相手により 2 つのアドレスを使い分け,，外部端末との通信に用いる CA のルーティングを可能とするため，ホストルートを設定し，ホストルートで問

題となるエントリー数の増大を抑え，アドレスの重複を防ぐ方式を提案した．今後は実装と評価を行う．

参 考 文 献

1) *http://www.kokatsu.jp/blog/ipv4/*.
2) 北村阿多信吾，村田正幸：IP 通信のセッション多重化を刷新する Unified Multiplex 通信アーキテクチャ，信学技報 (2006).
3) 榊間慧一，阿多信吾，北村　浩：匿名性を有しつつ識別管理可能な IP アドレスを用いた通信システムの構築，信学技報 (2009).
4) Narten, T., Draves, R. and Krishnan, S.: Privacy Extensions for Stateless Address Autoconfiguration in IPv6, *RFC4941* (2007).
5) Wasserman, M. and Baker, F.: IPv6-to-IPv6 Network Address Translation (NAT66), *draft-mrw-behave-nat66-02.txt* (2008).
6) de Velde, G.V., Hain, T., Droms, R., Carpenter, B. and Klein, E.: Local Network Protection for IPv6RFC4864 (2007), *RFC4864* (2007).
7) Thaler, D., Zhang, L. and Lebovitz, G.: IAB Thoughts on IPv6 Network Address Translation, *draft-iab-ipv6-nat-02.txt* (2009).
8) Hinden, R. and Haberman, B.: Unique Local IPv6 Unicast Addresses, *RFC4193* (2005).
9) Huitema, C. and Carpenter, B.: Deprecating Site Local Addresses, *RFC3879* (2004).
10) 加来　徹，有田敏充，兒玉清幸，吉田和幸：IPv6 ネットワークトポロジ表示システムについて，マルチメディア分散，協調とモバイル (DICOMO2007) シンポジウム論文集，Vol.2007, No.1, pp.1748–1753 (2007).