

## IPv4-IPv6 ゲートウェイの改良

緒方 健一† 長田智和† 谷口 祐治‡ 河野 真治† 玉城 史朗†

† 琉球大学 理工学研究科 ‡ 琉球大学 総合情報処理センター

〒 903 - 0213 沖縄県 中頭郡 西原町 千原 1 番地

E-mail: kenchi@ads.ie.u-ryukyu.ac.jp

あらまし 近年、インターネットの普及により、各地に分散していたコンピュータ資源が、ネットワークを介して結ばれるようになった。それに伴って、ネットワークの多様化・大規模化が進み、IPv4 では、アドレスの不足などの問題が起こると考えられている。そこで、次世代インターネットプロトコルとして IPv6 が策定され、各地で移行に向けた取り組みが行われている。しかし、現在のネットワーク環境を考えると、IPv4 のネットワークを即座に IPv6 に移行するのは困難であり、既存のネットワークを残したまま移行が行われる可能性もある。このように IPv6 への移行期には、不安定なネットワーク運用を余儀なくされる。また、移行後も安定してネットワークを利用するためには、異なるネットワーク間の通信を確保する機構が必要である。本研究は、そのシステムの一つとして IPv4-IPv6 ゲートウェイを提案し、相互通信を保証しようとするものである。

キーワード： ネットワーク, IPv6, ゲートウェイ

### Improvement of IPv4-IPv6 Gateway

Kenichi OGATA† Tomokazu NAGATA†  
Yuji TANIGUCHI‡ Shiro TAMAKI† Shinji KONO†

† Graduate School of Science and Engineering, University of the Ryukyus.

‡ Center for Integrated information processing, University of the Ryukyus.

1, Senbaru, Nishihara, Nakagami, Okinawa, 903 - 0213 JAPAN

E-mail: kenchi@ads.ie.u-ryukyu.ac.jp

**Abstract** In recent years, Distributed computer resources are connected by the Internetworking. Now, network have many variation and grew large-scale one. One of the internet protocol of IPv6 is designed and experimented in various locations because IPv4 is not suitable for guaranting enough address space. But it is difficult to change IPv6 from IPv4 at once because of it's high replacing cost. Transitional period of IPv6, we must do unstable network operations. After the transitional period of IPv6, we needs a system which connect with IPv4 and IPv6 network. In this paper, to solve such problems, we propose an IPv4-IPv6 Gateway.

**Key Words** : Network, IPv6, Gateway

## 1 はじめに

近年、インターネットの普及により、各地に分散していたコンピュータ資源が、ネットワークを介して結ばれるようになった。それに伴い、ネットワークの多様化が進み、結果として、既存のIPv4ではアドレスが足りなくなると考えられてきた。そこで、次世代インターネットプロトコルとしてIPv6が策定され、各地で実験が行われている。

本研究では、IPv6のネットワークを、既存のIPv4ネットワーク上に構築し、運用することで、現状における問題点などの検証を行ってきた。また、それにより導出される問題の解決手段として、IPv6に関するDNSの設定などの対処を行ってきた。しかし、実際のネットワーク環境を考えた場合に、IPv4のネットワークが即座にIPv6のネットワークに移行するのは困難である。また、管理コストや人的コストの面から、既存のネットワークがそのまま残ることも考えられることから、お互いの通信を確保するためには、IPv4とIPv6のネットワークを接続する機構が必要となる。

## 2 IPv4の限界とIPv6

ネットワーク環境は、利用者層の変化により、その利用形態や利用目的が多様化し、大きく変化した。ネットワークの変化に対しては、IPv4の柔軟な拡張性により対応してきたが、それも限界を迎えている。現在、IPv4が抱えている問題点としては次のようなものがある。

### (1) スケーラビリティに関する問題

IPアドレスにあるクラス概念は、大きな組織には大きなアドレス空間、小さな組織には小さなアドレス空間を割り当てるという意味では合理的なものであったが、限られた空間で全世界をカバーするためには、大雑把で非効率過ぎた。そこで、NAT<sup>1</sup>が導入されるようになった。NATによって、少数のグローバルアドレスでも、大規模なネットワーク運用が可能である。また、NATにはセキュリティとしての一面も存在することから、現在ではネットワーク接続の一形態となっている。これらのことから、必ずしもすぐにIPv6へと移行する必要はなくなっているが、IPv6には、アド

レス空間の単なる拡張という意味だけでなく、ルーティングやネットワークポロジに関する対処を正しく行えるプロトコルとして、導入の必要性がある。

### (2) 管理問題

IPv4では、基本的にネットワークに接続するコンピュータの設定は手動で行われることを前提にしていた。しかし、ネットワークが大規模化し、その管理に多くのコストがかかるようになった。DHCPなどの技術でエンドユーザ側の管理の手間は省略できるが、ルータなどのネットワーク機器の設定にはある程度の知識を必要とするため、その手間を省くことができない状況が生まれている。さらにCIDR<sup>2</sup>が導入されたことでネットワークポロジの変更に対するコストがさらに大きくなった。ネットワークの規模が拡大するにも関わらず、ネットワークを管理する手法や、ノウハウを持った人材の育成は遅れている。

### (3) セキュリティ

インターネット上で展開されるサービスも多様化し、電子商取引なども行われている。これらのサービスが安全に行われるためには、メッセージの暗号化や認証などのセキュリティ対策が万全でなければならない。しかし、IPv4には、パケットレベルでの暗号化や認証技術などが無いため、対策は個々のアプリケーションに委ねられている。

### (4) 実時間データ送受信に関する遅延問題

低価格化と高機能化により、個人へのコンピュータ普及が拡大したことから、情報発信型アプリケーションが利用され始めた。しかし、音声や動画を配信する場合に遅延が発生すると、内容が飛んでしまうなど、データの価値が少なくなる。従来のIPv4において、ストリームデータの配信に遅延が起きるのは、IPv4の通信がどのデータに対しても平等に提供されていたからである。よって実時間でのデータ送信を優先するなどの機構を設ける必要が出てきた。

これらの問題を解決することを目的とし、IPv4に変わるプロトコルとして、IPv6が策定された。その特徴としては、次のものが挙げられる。

<sup>1</sup> Network Address Translation

<sup>2</sup> Classless Inter Domain Routing

(1) アドレス空間の拡張

IPv6は、128ビットのアドレス空間を持つ。このアドレスが将来的に十分であるかどうかを現段階で判断することはできないが、32ビットのアドレス空間をもつIPv4よりも長い期間利用可能であると考えられる。

(2) ヘッダ構造の変化

IPv6は、図2に示すようなヘッダ構造を持つ。これは図1に示したIPv4のヘッダ構造よりもシンプルである。

0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1															
バージョン		IHL		サービスタイプ				全長							
識別子				フラグ				オフセット							
TTL (寿命)				プロトコル				ヘッダチェックサム							
始点アドレス															
終点アドレス															
オプションおよびパディング															

図 1: IPv4 のヘッダ構造

0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1															
バージョン		トラフィッククラス				フローラベル									
ペイロード長				次ヘッダ				中継順序数							
始点アドレス															
終点アドレス															

図 2: IPv6 のヘッダ構造

このようなIPv6のヘッダフォーマットの単純化は、パケットを中継するルータの負荷を軽減するための改善、およびIPv4であまり利用されなかったヘッダの廃止、という2つのことが行われた結果である。

(3) Plug&Play

IPv6では、容易なホストの自動設定の実現も行われている。自動設定がもつべき機能としては次のものがある。

- ネットワーク設定の自動設定
- ローカルリンクによるホスト間接続
- 大規模ネットワークに接続する場合に、サイト内での通信やグローバル通信まで自動設定する。
- リナンバリングを容易に行えること
- 移行期に、IPv4及びIPv6が利用可能なように、アドレス2重化へ対応する

このように、ホストの設定のしやすさから、規模の大小に関係なくネットワーク構成に柔軟に対応できること、それがIPv6で取り組まれている。

(4) セキュリティ

IPv6では、ネットワークレイヤレベルでセキュリティ機能を実装することで、従来よりもユーザの利便性は向上する。また、従来通りアプリケーションに特化した形で新たなセキュリティ機能を持つことも可能である。現在では、FireWallなどのようにネットワーク全体を遮断・隠蔽する形でセキュリティ対策が取られているが、ソフトウェアレベルでIPv6のセキュリティ機能を有効に活用できれば、恒常的にセキュリティを確保できる。

(5) 実時間データ送受信

IPv6では、フローラベルと優先度の2つの機能が実装されており、ヘッダにその領域が確保されている。フローラベルとは、複数の実時間通信が行われていた場合に、各パケットがどの実時間通信に属しているかを示すヘッダである。優先度とは、各パケットのデータがどの程度重要であるかを示すものである。実時間通信での問題は、ネットワーク回線の容量、確保された通信帯域に対して、実時間に通信すべきデータが巨大な場合などである。このような場合、実時間通信を実現するため、優先度が利用される。具体的には、各パケットに付けられている優先度のヘッダフィールドにより、全てのパケットを実時間で通信することが困難な場合には、優先度の低いパケットを送信しない、もしくは遅延して送信するように指定しておくことができ、実時間通信を実現できる。

### 3 実験ネットワーク

琉球大学総合情報処理センターでは、NTT 情報流通プラットフォーム研究所(NLA1)およびLinux IPv6 Users Group(NLA2)から、IPv6アドレスを取得し、運用および各種検証・実験を行っている。本研究では、当初、琉球大学総合情報処理センター内に、ネットワーク実証研究を目的として設置された“OSN<sup>3</sup>”および“SG<sup>4</sup>”の2つ実験ネットワー

<sup>3</sup> Open System Network  
<sup>4</sup> Server Group network

クによる接続を行っていたが、2000年1月にネットワークの拡張を行い、琉球大学工学部情報工学科の研究室内に、新たに“XRD<sup>5</sup>”実験ネットワークを構築した。これにより、“OSN”と“SG”による2つのネットワーク構成から、“OSN”と“SG”と“XRD”の3ネットワーク構成へと移行した。それに伴い、学内でもトンネリングによる接続を開始し、現在は、図3に示す構成で運用している。

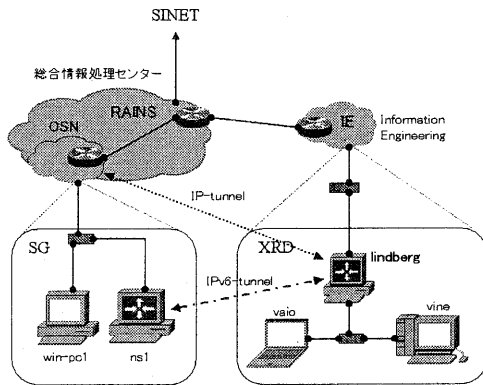


図3: 学内 IPv6 ネットワーク

## 4 ネットワークにおける問題点とその対応例

本研究で構築した実験ネットワークの運用において、以下に示すような問題点が導出された。

### (1) IPv6 アドレスの使用

IPv6 は、128 ビットのアドレス空間を持つことから、そのアドレスの表記が既存の IPv4 に比べると長くなる。そこで、IP アドレスをそのまま利用するよりも、DNS を用いて、アドレスとホスト/ドメイン名の解決を図ることが重要となってくる。これは特に、末端の組織になるほど重要性が増してくる。なぜなら、末端の組織ほど IPv6 のアドレスが長くなる性質があるためである。IP アドレスを隠蔽することで、利便性が増すと考えられることから、DNS によるアドレスとホスト/ドメイン名の相互変換は重要である。

### (2) トンネリングで構成されるネットワーク

トンネリングは、IPv6 パケットを IPv4 のパ

ケットに格納し、IPv4 ネットワーク上を送受信する手法である。IPv6 でのトンネリングでは、通信する IPv6 の機器の間に、その他の IPv6 機器を必要としない利点があるが、IPv4 のネットワークが途絶えると IPv6 の通信も途絶えてしまい、IPv4 に複数の経路があっても、通信できなくなる。これは、IPv6 のトンネリングは対象となる2つのホスト間での設定による接続となるため、動的にトンネリングのホストを切り換えることができないからである。

### (3) 煩雑な経路情報

静的に経路情報を設定する場合、管理者がネットワークの構成を把握しておくことが必要である。しかし、接続するホストやネットワークが増えた場合、必要な経路情報量も増加し、かつ、複雑になるため、管理が困難になる。

### (4) IPv4-IPv6 の相互通信

IPv4 のサーバに対して、IPv6 のクライアントが要求を出した場合には応答が返されない。移行コストなどの面から既存ネットワークが残る場合、既存の IPv4 サーバの資源をそのまま利用するには、新規に構築される IPv6 のホストに機能を移すか、もしくは IPv6 のクライアントが接続可能な方法を構築する必要がある。IPv6 の導入に関しては、既存ネットワークに設定を加えないことが望ましく、相互の通信を確立するために何らかの機構が必要となる。

本研究では、実験ネットワークによって導出された問題点に対して、以下の手法で解決を図っている。

### (1) IPv6 に対応した DNS 設定

IPv6 のアドレスとドメイン名とを関連付けるため、DNS に対して IPv6 に対する設定を行った。これにより、ドメイン名による各種管理コマンドの利用が可能になった。例えば、正引きファイルには AAAA レコード、逆引きファイルには IP6.INT などの設定を行う。

### (2) 経路情報の制御

経路情報の取得のため、トラフィックの中継を行うルータホストに、GNU Zebra を導入した。研究初期のネットワークが2ネットワーク構成であったのに対し、ネットワーク拡張後は、IP トンネリングによる接続も開始され、3ネットワーク構成となった。拡張後、手動による経路設定だけではトラフィック交換ができないな

<sup>5</sup> X(cross)RoAD network

どの不具合があったが、GNU Zebraを用いることで、必要な経路情報を自動的に取得できるため、経路問題が解決され、管理者の負担も減った。

IP トンネリングなどの手法は、IPv4 に依存した IPv6 ネットワークの利用形態である。また、現状では、IPv6 サーバと IPv4 クライアントによる相互通信は可能だが、IPv4 サーバと IPv6 クライアントでは、応答が見られないなどの状況が確認できた。そこで次に示す、IPv4-IPv6 ゲートウェイを提案し、構築を行った。

## 5 IPv4-IPv6 ゲートウェイ機構

このゲートウェイ機構の主な処理としては、

- (1) IPv4/IPv6 デュアルスタック
- (2) IPv4 および IPv6 アドレスの相互変換

などがある。現在構築しているネットワーク上の IPv6 サーバは、IPv4 への応答が可能だが、IPv4 のサーバは IPv6 クライアントからの要求に対して応答できない。ここで提案する、IPv4-IPv6 ゲートウェイ機構は、デュアルスタックホストとして IPv4 および IPv6 の両方のプロトコルを処理し、通信の中継点となることで、IPv4 と IPv6 の境界を無くすものである。これは、移行戦略を進めるための有効な手法である。このゲートウェイは IPv4 お

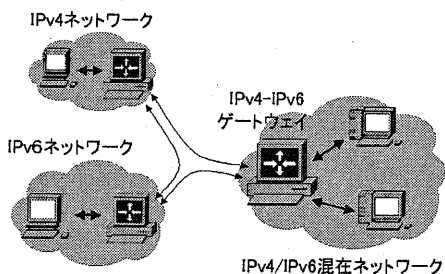


図 4: IPv4-IPv6 ゲートウェイ機構

よび IPv6 の両方のプロトコルをサポートする。このゲートウェイを経由することにより、通信を行うホスト間の IP が異なっても、IP アドレスを相互に変換することが可能で、異なる IP のネットワーク間での通信が可能となる。また、今回構築する改良型のゲートウェイでは、ホスト/ドメイン

名による通信を可能とするため、各アドレスとホスト/ドメイン名との変換情報を持つようにする。ゲートウェイは、各クライアントからの要求の受け口となる。ゲートウェイ内部では、アドレスやドメイン名の変換テーブルを利用して相互変換を行い、通信を行う。例えば、IPv6 クライアントからの要求を IPv4 クライアントからの要求のように変えることで、IPv4 の通信としてデータの取得が可能となる。また、このゲートウェイを応用し、IPv4 および IPv6 のバックボーンを必要に応じて使い分けことが可能である。

### 5.1 IPv4-IPv6 ゲートウェイと問題点

現在、提案した IPv4-IPv6 ゲートウェイの構築を行っているが、その構築しているゲートウェイは、次のような処理を行っている。ここでは、IPv6 クライアントと IPv4 サーバとの通信を例にとって説明する。

- (1) IPv6 クライアントはゲートウェイに対して要求を送信する。
- (2) ゲートウェイは、IPv6 によって、クライアントからの要求を受け付ける。
- (3) ゲートウェイは、自分自身の IPv4 アドレスを使って IPv4 のサーバと通信を行う。
- (4) ゲートウェイは、サーバから返されるデータを IPv6 による通信で、要求元に返す

IPv4 サーバと IPv6 クライアントの通信を可能としている。しかし、この処理の過程でのホストの指

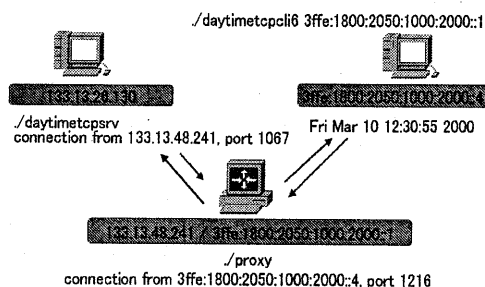


図 5: 現在の使用例

定方法には問題がある。現行のゲートウェイは、実際に IPv6 クライアントと IPv4 のサーバの通信が可能かどうかを、検証するために作成したもので

あるため、プログラムに不安定な部分がある。使用例を見て分かるように、データの要求先がゲートウェイとなるなど、一意でないため、ネットワークの構成を知っていなければ利用できないなどの問題がある。また、IPv6ではホスト/ドメイン名を利用した方が、IPアドレスを直接指定するよりも有効であるので、このゲートウェイの機能強化を図るためには、各IPアドレスとホスト/ドメイン名とを相互に参照するためのデータベースが必要になる。そこで現在作成しているゲートウェイにアドレスに関するデータベースを持たせることで、要求先の持つ各IPアドレスとホスト/ドメイン名の変換やそれによる対象ホストの指定が可能になる。

## 5.2 改良型 IPv4-IPv6 ゲートウェイ

改良型のゲートウェイとして提案する機構の重要な部分は、図6に示すような、アドレスとホスト/ドメイン名の変換テーブルである。この変換テーブルを利用して、ユーザ側でのホスト指定には、ホスト/ドメイン名を利用し、IPv6アドレスそのものは隠蔽する。そして、実際の通信には各アドレスを利用するなどの通信方法が考えられる。このようにIPv6の持つ複雑な部分を隠すことで、エンドユーザ側でのIPv6の利便性を向上させることができる。また、ゲートウェイが変換処理ばかりを行うだけでは、トラフィック交換の負荷となるので、このゲートウェイを利用する際にオプションを指定することで、IPv4の通信かIPv6の通信かを明示する必要がある。通信の際に適切なオプションを与えることで、不必要な変換処理を省くことが可能である。

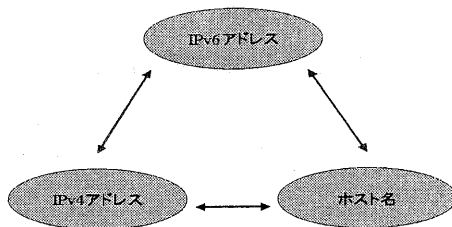


図6: アドレス変換テーブル

## 6 終わりに

本研究では、既存のIPv4ネットワーク上に、IPv6実験ネットワークを構築することで、運用における問題点を導出し、それについて解決を図っている。実際にIPv6の移行がどの時期に、どれくらいの期間をかけて行われるかは定かではないが、着々と移行に関する研究はなされている。本研究では、移行期間中、またそれ以後のネットワークの相互接続性を確保するため、IPv4-IPv6ゲートウェイを提案し、その有効性を実証した。現在、基本的なサーバ・クライアント通信である daytime サーバおよびクライアントを用い、その間にIPv4-IPv6ゲートウェイを構築することで、このゲートウェイに関する実験を行っている。これまでに構築した、IPv4クライアントおよびサーバ、IPv6クライアントおよびサーバにおいて、ホスト/ドメイン名による動作が確認できれば、その応用として、別のアプリケーションへの対応などが考えられる。今後の課題としては、まず、改良したゲートウェイを実ネットワークで動かすことが挙げられる。また、それにより導出される問題点を解決することで、構築しているネットワークの利便性の向上を図る。

## 参考文献

- [1] ネットテクノロジーラボ 著, “最新技術解説 入門 IPv6,” 1999.
- [2] Mark A. Miller 著, トップスタジオ 訳, 宇夫陽次朗 監修, “IPv6 入門”, 翔泳社, 1999
- [3] W.Richard Stevens 著, 篠田陽一 訳, “UNIX ネットワークプログラミング 第2版 Vol.1 ネットワーク API:ソケットとXTI”, ピアソン・エデュケーション | トッパン, 1999.
- [4] 緒方健一, 谷口祐治, 長田智和 “IPv6 移行期における IPv4/IPv6 ゲートウェイの実装” 情報処理学会第60回全国大会講演論文集(3), pp.453-454, 2000,