次世代ネットワーク技術の
小規模ネットワークへの導入技法

末永洋樹[†]

[†] 日本大学理工学部電気工学科

平成13 年4 月10 日

目 次

第1章　はじめに

現在の社会は大量の情報の流通なしにはなりたたない情報社会である．その情報社会の基盤としてインターネットが特に重要な役割を担っている．インターネットは基幹ネットワークと末端ネットワークに分けられるが，最近では後者の中には家庭やサテライトオフィスのような小規模な組織も数多く存在する．これらの組織も小規模ではあるが独自のネットワークを構築していることが多い．このようなネットワークを本論文では小規模ネットワークと位置づける．このような小規模ネットワークではIPv4(IPバージョン4)[1]が広く用いられている．IPv4は現在最も広く用いられているインターネット技術であり，この上で多様なサービスが提供されいる．

インターネットは急速に発展しつつあり，IPv4の設計当初に比べるとはるかに大きな規模になっている．このため，IPv4の持つアドレス空間では十分なアドレスを確保できなくなってきている．とくに，小規模ネットワークでは必要なだけのアドレスは一般に確保できない．

アドレス空間の不足に対する対策としてはNAT(Natwork Address Translation)[2]と呼ばれる技術が広く用いられている．これは限られたグローバルアドレスを複数のホストで共有する技術である．NATを用いることで1つのアドレスを多くのホストで共有できる。しかしNATを用いたネットワークの通信形態はインターネット本来の通信形態とは本質的に異なる．このため，表面的にも潜在的にも多くの問題を問題を抱えているのがIPv4インターネットの現状である．

IPv4にはアドレス空間の枯渇に加えて経路表の増大という問題もある．このまま経路表が増大していくと，基幹ネットワークで動作しているルータの管理限界を越えてしまう．そうなるとインターネット全体が機能しなくなってしまう．

これらの問題を解決するために，IETF(Internet Engineering Task Force)では次世代のインターネットプロトコルとしてIPv6(IPバージョン6)[3]を策定し，研究・実験を行っている．その結果IPv6は既に十分安定して運用できる状態になっており，今後 基幹ネットワークは急速にIPv6に移行していくと予想する．

これらの研究・実験は基幹ネットワークでの運用を対象としたもので，主に経路表の増大への早急な対応が目的である．

一方，小規模ネットワークではアドレス空間の不足が深刻な問題になっている．しかし，小規模ネットワークを対象としたIPv6の導入に関する研究は現在は少ない．

そこで，著者は小規模ネットワークの諸問題の解決にIPv6の利用が有効であるという見地から，小規模組織でのIPv6ネットワーク構築についての研究を行った．著者の研究では小規模ネットワークにIPv6を導入するためにINSルータを用ている．これはINSルータ

を用ることで低コストでIPv6を導入できるためである．本論文では小規模組織へのIPv6の導入にINSルータが有効であることを示し，INSルータへIPv6のプロトコルスタックを実装するための指標を示す．次に小規模組織でのIPv6ネットワークの運用技法について述べる．

第2章　現在のインターネット技術 (IPv4)

2.1　IPv4インターネット技術の歴史と現状

現在のインターネットはもともと米国防総庁 (DARPA) が提案し構築したネットワーク技術に基づいている．

インターネットが存在する以前のネットワークといえば中央の処理能力の高い計算機の資源を，多数の処理能力の低い端末を使って利用するシステムを指していた．しかし，このシステムには中央のホストが停止するとシステム全体が停止するという問題があった。

この問題を解決するために，インターネットは一台のホストが停止しても，その他のホスト間の通信には支障がでない障害に強いネットワークを構築するという目的を持っていた．この仕組みを実現するためにインターネット上ではホスト間の格差をなくし，すべてのホストを同等に扱うようになっている．このとき，各ホストを識別するために用いられる識別子をIPアドレスとよぶ．現在利用されているIPv4(IPバージョン4)では識別子の長さは32bit固定長となっている．また，インターネット上では情報はホストからホストへバケツリレー式に転送される．そのため，あるホストから別のホストへ情報を伝えるためには転送の順番を示す経路情報が必要である．インターネット上のすべてのホストは近隣のホストに対する経路情報を保持している．

初期のインターネットでは管理者が手動でホストに経路情報を登録していた．しかし，この方式ではホストが増加すると経路情報の管理コストが指数関数的に増大してしまう．このため現在のインターネットでは経路情報はある程度自動で交換されるようになっている [4, 5, 6, 7, 8]．しかしインターネットの規模が大きくなり，様々な問題が発生している．

IPv4ではホストごとに固有のIPアドレスを使うことで，1対1の通信を提供している．IPv4の設計当時はコンピュータの数はそれほど多く無かったため，32bitのアドレス空間は十分なものとして設計された．しかし，インターネットの急速な進歩にともないホスト数はIPv4の設計当初とは比較にならないほど多くなっている．現在の予測 [9] では、21世紀前半にはIPv4のアドレス空間は枯渇してしまうとされる。アドレスを割り当てられないとインターネットを利用した通信は行えないため，アドレスの枯渇はインターネットの進歩の停止そのものを意味している．

また，IPv4には経路表の増大という問題もある。IPv4では各ホストは他のホストへの通信路を経路表として保持している。インターネット全体が大きくなるとホストの数も増加するので、経路表も必然的に大きくなる。基幹ネットワーク上のルータの保持できる経路表の大きさには限度があるため，過度に大きい経路表は保持することができず経路が失

われる．経路表を縮小するため、IPv4 にはいくつかのホストをひとまとまりにしたサブネットワークという考え方や、サブネットワークを集めた自律システム (AS)[10, 4] という考え方が導入されている。このような管理を経路の集約と呼ぶ。これにより、経路表は全てのホストの情報を持つ必要はなくなり、サブネットワークや AS の情報のみを持てばよくなる。

しかし現在は、このモデルを持ってしても扱いきれないほど多くの組織がインターネットに接続している。

2.2 アドレス空間の効率的な割り当て

IPv4 のアドレス空間にはホスト用のアドレスの他に、ホストの集合を示すネットワークアドレスが存在する。IPv4 に接続されるホストは一般にネットワークに属している。

これらのネットワークは運用する組織ごとに割り振られていることが多い。組織の規模により接続されるホストの数が異なるため、初期のインターネットではネットワークの規模をクラス分けして管理していた。クラス A のネットワークには約 16 万台のホストが接続可能であり，クラス B のネットワークには 65,534 台，クラス C のネットワークには 254 台のホストが接続可能である．現在はクラス B のネットワークが最も利用率が高く、すでにクラス B のアドレスは配布を中止している。

あるネットワークに実際に接続されるホストの数はネットワークに接続できるホストの上限にはならないことがほとんどである。このため、IPv4 ではアドレス空間を効率的に利用することができない。一般にアドレス空間の利用率は 7 割程度に留まるといわれている。

このように，クラスによるアドレス空間の管理はアドレスの利用効率が悪いことから IETF では CIDR[11, 12] と呼ばれるクラスによらないアドレス空間の利用法を策定し、効率のよいアドレス空間の利用を推し進めている。CIDR は Classless Inter-Domain Routing の略で従来のクラスの概念によらないアドレスの割り当ての手法である。CIDR では従来のクラス C にあたるアドレスを一つの組織に連続して割り当てる。例えば、クラス C 一つ分にあたる 254 個のアドレスでは足らないが、300 個程度のアドレスがあれば十分という規模のネットワークに対しては 2 つの連続したクラス C アドレスを割り当てることで効率よくアドレスを割り当てる。この連続したアドレス空間を CIDR ブロックと呼ぶ。従来のクラスによるアドレス割り当てでは、この場合でもクラス B のアドレスを割り当てるしかなく、多くのアドレスが無駄になっていた。

CIDR の利用によってアドレス空間の利用効率は若干向上するがアドレス空間そのものが広がることはないため、当面の対策という側面の強い技術である。したがって、CIDR を導入してもアドレスの枯渇は根本的に解決できない。

2.3 NATによるアドレス空間の拡張

IPv4にはプライベートアドレスと呼ばれる組織内部のみで利用できるアドレスが定義されている[13]。NAT(Network Address Translation)[2]と呼ばれる技術は、このプライベートアドレス空間を利用することでアドレス空間の拡張を行う。

NATではネットワークの入口に1個から数個のグローバルアドレスを用意し、ネットワーク内部ではプライベートアドレスを用いる。ネットワーク内部のホストが外部へ通信を行う場合には、内外のネットワークの中継箇所に用意してあるグローバルアドレスを一時的に利用する。この技術を用いると、一つのネットワークに必要なグローバルアドレスは高々数個となり、インターネットに接続できるホストの数は大幅に増える。

NATは大きく分けて2種類ある[14]。一つのグローバルアドレスに対して一つのプライベートアドレスを割り当てる方法と、一つのグローバルアドレスに対して複数のプライベートアドレスを割り当てる方法である。前者をNAT, 後者をNAPT(Network Address Port Translation)またはIP Masqueradingと呼び区別することもある。一つのグローバルアドレスに対して一つのプライベートアドレスを割り当てた場合、NATが機能している間はネットワーク内部のホストに外部からアクセスできる。逆に一つのグローバルアドレスに複数のプライベートアドレスを割り当てた場合、NATが機能していてもネットワーク内部のホストに外部からはアクセスできない。対応するプライベートアドレスが特定できないためである。アドレスの変換を行う場合に前者はソースアドレスにもとづくのにたいし、後者はポート番号にもとづくためにこのような違いが生じている。一般に前者のほうが運用の自由度は高いが、後者のほうがセキュリティは強固である。

しかし、インターネットは本来通信の両端に一意なアドレスがついていることを前提としたネットワークである。NATを利用したネットワークはこの仕組みと本質的に異なるため一部のサービスが利用できない。また、NATを提供するホストに障害が発生した場合にはネットワーク内部の全てホストが通信不可能な状態に陥る。そのためインターネットが本来持っている障害に強いネットワークという特性をなくしてしまう。

さらにNATの管理は一般に繁雑であり、運用コストが上昇するという欠点も持つ。NATの利用そのものは低いコストで行えるようになりつつあるが、障害が発生した場合は原因の究明が困難になることが多いため安定した運用には高度の技術が要求される。NATが普及した場合、これらの欠点はインターネット全体の進歩を妨げる要因になると考える。

第3章　次世代インターネット技術 (IPv6)

3.1　IPv6の概要

ここまで見てきたようにIPv4には多くの欠点が明らかになってきおり、IPv4は既に技術としての寿命を迎えていると考える。

現在IPv4を根本的に置き換える新しいプロトコルとして、IETFでは次世代ネットワーク技術としてIPv6(Internet Protocol Version6)が策定されている。IPv6はIPv4の抱える問題点を根本から解決することを目的として設計されている．設計はIETFのIPngワーキンググループで行われた．IPv6はIPv4の問題点の解決に加えて新しく追加された機能や，性能の向上した機能も持っている．

IETFでIPv4の問題点が詳しく調査されたのは1991年7月である．調査の結果は1999年11月にRFC1380[9]としてまとめられ，その結果をもとに対策を講じた．対策は大きく分けて二つの方針となった．一つは前章で述べたようなIPv4の改善措置であり，もう一つはIPv4を完全に置き換える新しいプロトコルの策定である．この方針に従い，IETFではIPv4の限界を引き伸ばしつつ次世代のインターネットプロトコルを設計した．

IETFではまず次世代インターネットプロトコルの評価基準[15]を定め，候補を募集した．次にいくつかの候補のなかから基準を満たすものを集め，IPng(IP Next Generation)[16]として比較検討を行った．この時点で候補として上がったプロトコルは3つあり，それぞれCATNIP案，SIPP案，TUBA案と呼ばれた．これらの候補にはいずれも欠陥があり，そのままでは次世代インターネットプロトコルとして標準化できなかった．検討を重ねた結果SIPP案が欠点を解消し他の案の利点を取り入れる形で発展した．1994年7月にはこのSIPP案がIPv6と名前を変え次世代インターネットプロトコルとして採用された．

その後IETFはIPv6の設計と実験に積極的に取り組み，現在ではIPv6の基本設計は完了している．現在もいくつか未解決の問題はあるが，いずれも致命的なものではなくIPv6は十分安定して運用できるようになっている．今後は急速にIPv6が普及すると予想できる．

3.2　IPv6の優位点

IPv6はIPv4に比べ以下のような利点をもつ．

128bitの広大なアドレス空間 IPv6のアドレス空間は128bitである．このためIPv4のア

ドレス空間の枯渇を根本的に解決できる．

IPv4 のアドレス空間は 32bit 固定長であるのに対し，IPv6 のアドレス空間は 128bit 固定長である．仮に IPv6 のアドレスを地球上の陸地全てに均等に割り当てたとすると，1 平方インチあたり 3 個の割り当てが可能になる．この数は現在存在するすべてのコンピュータの数を大きく上回るものであり，枯渇するとは考えにくい．

むしろ，コンピュータ以外の機器に対しても積極的にアドレスを割り当てるような使い方が考えられる．

アドレス構造の多層化 IPv4 ではアドレス空間はネットワーク部とホスト部の二つに分かれているのみで，組織内でサブネットマスクを利用することでアドレスの管理を階層化している．

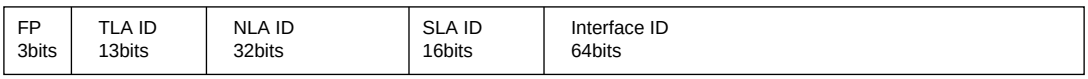
このため，バックボーンのルータは多数のネットワーク番号を管理しなければならず経路表が増大している．ルータの管理できる経路表の大きさには限界があり，このままでは経路表を管理しきれなくなることが分かっている．

IPv6 ではアドレス構造が多層化されているため，バックボーンのルータは必要最低限な経路のみを管理するだけでよい．

このため，IPv4 よりも大きなネットワークを容易に管理できる．

現在の IPv6 アドレスの割り当てを 3.1 に示す．

図 3.1: IPv6 のアドレス構造



- FP は format prefix と呼ばれる．アドレスの種類を表している．これによりアドレスの有効範囲や構造が決まる．
- TLA ID は Top-Level Aggregation Identifier と呼ばれる．TLA ID は大規模なネットワーク管理組織に割り当てられる．現在は地球をアメリカ，ヨーロッパ，アジアに分けそれぞれの地域を担当する管理組織が存在する．
- NLA ID は Next-Level Aggregation Identifier と呼ばれる．NLA ID は中規模のネットワーク管理組織に割り当てられる．
- SLA ID は Site-Level Aggregation Identifier と呼ばれる．これは組織内部で自由に使うことができる．

IPv6 のルーティングでは，まず TLA-ID を調べることで大まかな地域を決定し，NLA-ID, SLA-ID と順に調べていくことでネットワークを限定していく．

設定の一部自動化 IPv4 ではアドレスの設定法にはユーザが手動で行うか，DHCP サーバを用いて行うかの 2 通りしかない．DHCP サーバはアドレスの割り当てや DNS サーバのアドレスの通知などを行うサーバである．

IPv6 ではネットワークにホストをつなぐと自動的にアドレスが生成される．このため，ユーザが手動で設定を行う必要はない．DNS サーバのアドレスの通知や，管理者が指定したアドレスの割り当てを行うためには DHCP サーバが必要になるが，これらが不要な場合には DHCP サーバは不要である．

したがって，ネットワークの管理コストが IPv4 に比べて低くなる．

セキュリティを考慮した設計 IPv4 上で安全な通信を実現するためには，IPsec を別途導入するかアプリケーションで対応する必要がある．

IPv6 では IPsec が標準で利用できる．このため，IPv4 に比べ容易に安全な通信を実現できる．

マルチキャスト通信の積極的な利用 IPv4 でマルチキャスト通信を実現するためには，マルチキャストパケットを特別に扱う必要がある．

IPv6 ではマルチキャストは必須機能の一つである．近隣のホストの探索やルータの探索などにもマルチキャストが利用される．

マルチキャストを積極的に利用することで，通信の効率化が可能になる．

エニーキャスト通信の採用 エニーキャストは IPv6 で導入された新しい通信形態である．

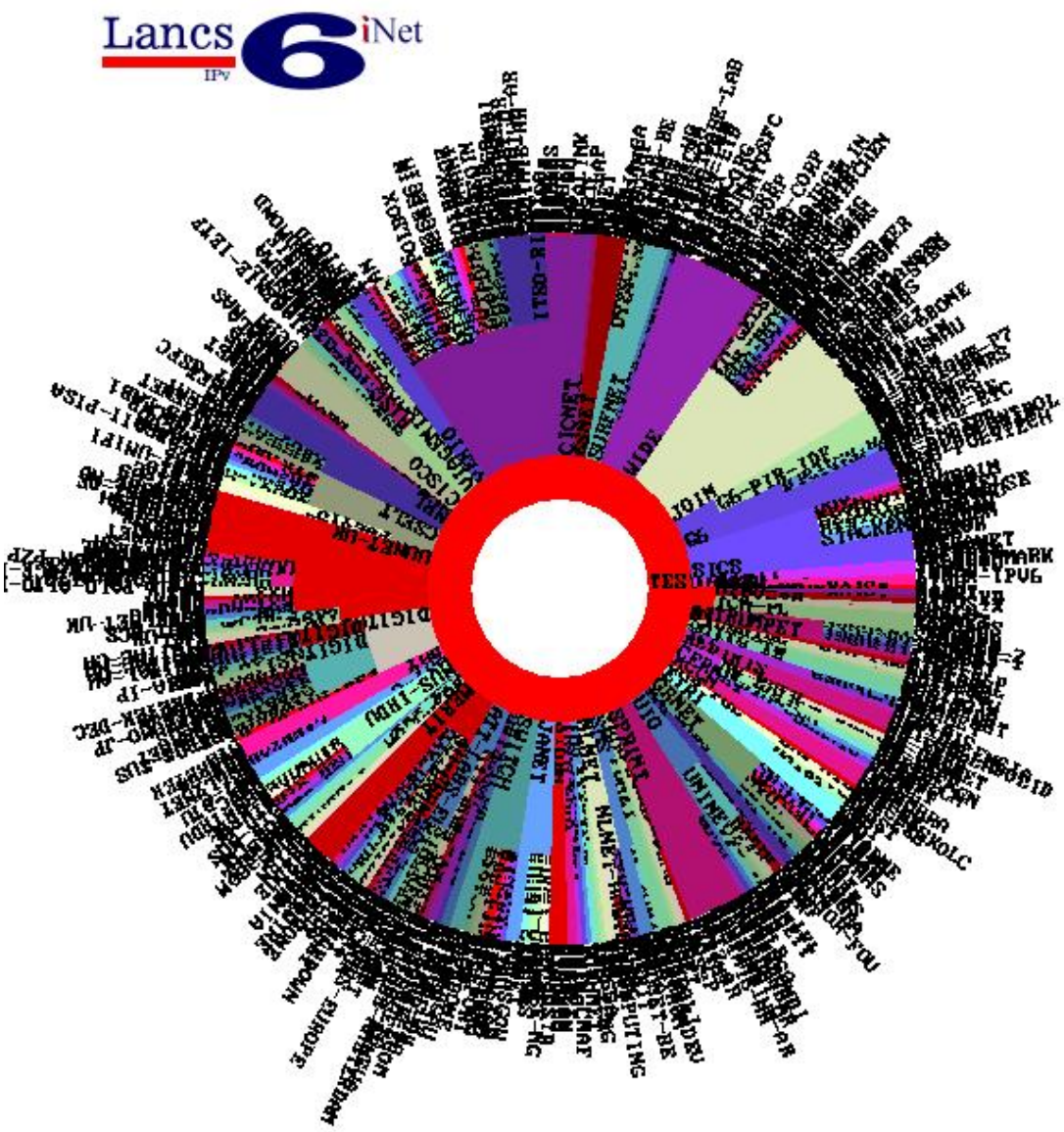
エニーキャストアドレスは複数のインターフェースの集合である．エニーキャストアドレスへの通信を行うと，最も近いインターフェースが自動的に選択される．

3.3 IPv6 インターネットの運用状況

現在 IPv6 は実験運用の段階である．世界各国で IPv6 の実験用のネットワークが構築され，その上で実験が続けられている．この実験用のネットワークは 6bone と呼ばれる．6bone には既に多くの組織が接続されており，相互に通信を行っている．6bone のトポロジを図 3.2 に示す．

最新の状況は http://www.6bone.net/6bone-backbone.html で参照できる．

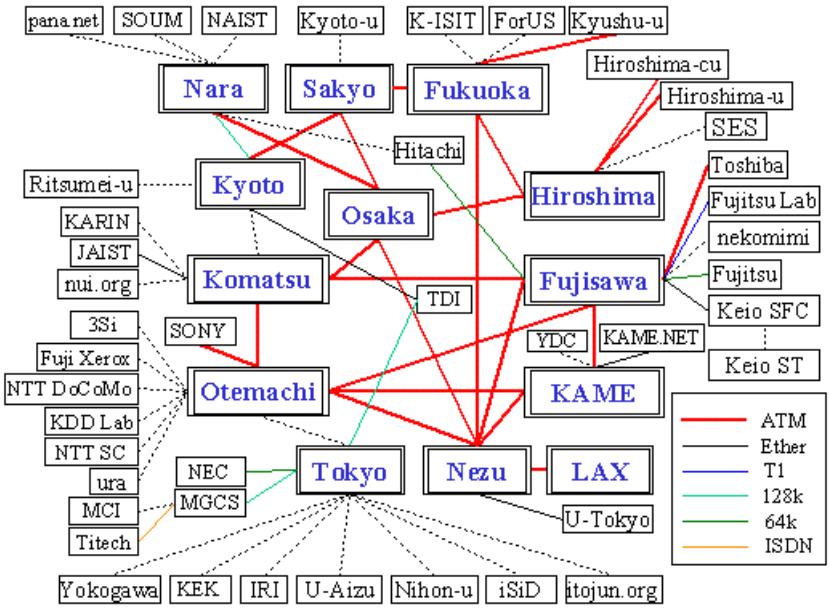
図 3.2: 6Bone のトポロジ



日本国内にも 6bone-jp と呼ばれる IPv6 ネットワークが存在しており，実験が行われている．6bone-jp のトポロジを図 3.3 に示す．

最新の情報は http://6bone.v6.wide.ad.jp/topology.html で参照できる．

図 3.3: 6Bone-jp のトポロジ



これらの実験ネットワークは主に IPv6 によるバックボーンの運用を目的としているものである．BGP, OSPF, RIPng などのルーティングプロトコルの実験やマルチキャスト通信の実験などが主な目的である．

6bone への接続を受け付けているプロバイダもいくつか存在する．表 3.1 にあげるプロバイダは実験目的での接続を受け付けているプロバイダである．

これらの組織の利用している 3ffe::で始まるアドレスは実験用に予約されているアドレスである．実験以外の一般的な目的での接続は 2001::で始まるアドレスを用いることが決まっている．

2001::で始まるアドレスは 1999 年 7 月に APNIC より配布が開始されている．このアドレスは IPv4 とほぼ同様の手続きによって取得できる．APNIC はアジア地域全体のネットワークを管理する組織である．今後は国ごとの管理組織がアドレスの管理を行っていくことになると予想できる．日本においては，WIDE プロジェクトが APNIC から pTLA の割り当てを受けており，商用まで含めた一般的な接続の実験が近く開始される予定である．

6bone は当初 IPv4 インターネットの上に構築されていた．これは IPv6 が単独で運用できるほど完成されていなかったためである．現在も IPv4 を経由して 6bone へ接続されている組織は多いが，IPv6 のみで接続されている組織が増えてきている．IPv6 はすでに単独で運用できるようになっていると考えられる．逆に IPv6 インターネットの上で IPv4 を用いる組織も今後現れると予想できる．

アドレス	組織名
3ffe:501::/32	WIDE Project
3ffe:502::/32	APAN
3ffe:503::/32	NTT Software Lab.
3ffe:504::/32	IRI
3ffe:505::/32	IMASY
3ffe:506::/32	DML
3ffe:507::/32	IIJ
3ffe:508::/32	INTEC
3ffe:509::/32	6bone event team
3ffe:50a::/32	DTI
3ffe:50b::/32	AI3
3ffe:50c::/32	TTNet

表 3.1: IPv6 での接続を受け付けているプロバイダ

IPv6 設計当初に比べると 6bone 接続組織は飛躍的に増加している．今後実験運用が終わり正式な運用がはじまると商用組織も含めより多くの組織が接続すると予想される．現在は IPv6 インターネットに接続する方法は限られているが IPv6 接続を受け付けるプロバイダも増えてくると考えられ，IPv4 インターネットから IPv6 インターネットへの移行はほぼ確実である．

第4章　小規模ネットワークへのIPv6の導入

4.1　小規模ネットワークの定義

本論文では小規模ネットワークとして，外部への接続点が1つないしは2つ程度であり，外部への経路の帯域もそれほど大きくないネットワークを想定している．接続されているホストの数は数十程度であり，経路の制御に比較的簡単な経路制御プロトコルか，もしくは静的な制御を用いているものとする．また，ネットワークの管理を専門に行う人員はおらず，利用者が自分で管理しているとする．例としては，サテライトオフィスや大学の研究室，家庭内ネットワークなどがこれにあたる．

このようなネットワークは接続されているホストの数は少ないが，数多く存在するため，インターネットに占める割合は大きい．

4.2　小規模ネットワークの現状と問題点

小規模ネットワークの大部分ではIPv4を用いた運用が行われている．外部との接続はINS回線を用いたダイアルアップ接続であるか，比較的低速な専用線を用ている場合がほとんどである．IPv4のアドレスがすでに不足していることから，接続されているホストの数に比べ十分な数のアドレスは確保できないのが普通である．

そのため，小規模ネットワークではアドレスの不足が恒常的な問題となっている．現在はNATによりアドレスの不足を補っているが，NATはアドレスの不足を根本的に解決する技術ではなく，あくまで一時的な対策にすぎないと著者は考える．

アドレス空間の不足はIPv6の導入により解決可能であるが，基幹ネットワークを対象としたIPv6の導入実験は数多く行われているのに対し，小規模ネットワークを対象とした導入実験の例はほとんどない．小規模ネットワークは大規模ネットワークに比べ機材や予算の面で大きく劣っていることが多く，大規模ネットワークでの研究結果はそのままでは小規模ネットワークには持ち込めない．また，小規模ネットワークにおいては一般にネットワーク管理を専門とする人員は確保できない．大規模ネットワークの運用は常に管理者の存在を前提にしており，このモデルは小規模ネットワークには適用できない．従って，小規模ネットワークのアドレスの不足の解消の見通しは全く立っていないと考える．

4.3 INSルータを用いたIPv6の導入

小規模ネットワークのアドレス空間の不足を解決する最良の方法はIPv6の導入であると著者は考える．しかし，基幹ネットワークを対象とした既存の研究はそのままでは小規模ネットワークに持ち込めないため，著者は小規模ネットワークに適したIPv6の導入手法をいくつか考案した．それらを導入コストが低いと予想する順に示す．

- INSブリッジと呼ばれる機材を利用する手法．この手法は参考文献[17]にすでに報告がある．INSブリッジはINS回線を利用して全てのネットワークトラフィックを交換する機器である．
- 二つめはパーソナルコンピュータやワークステーションを利用してIPv6パケットを交換する手法である．パーソナルコンピュータやワークステーションを利用したIPv6プロトコルスタックは十分に開発が進んでいるため，容易に利用できる．
- 三つめはINSルータと呼ばれる機器を利用する手法である．INSルータはINS回線を利用してネットワークトラフィックのルーティングをする機器である．INS Bridgeとの違いは全てのパケットは交換せずに，通信先のネットワークに応じてルーティングを行う点である．

この中で小規模ネットワークに最適な導入手法として著者はINSルータを用いた手法を選択し，実装を行った．ただし，小規模ネットワークといっても実際には様々な運用形態が考えられる．したがって運用形態に応じてコストも変化すると考える．いくつかの視点から著者の試算したコストの比較を以下に示す．ここではそれぞれの環境での運用形態として図4.1-4.3のようなネットワークを仮定する．

図 4.1: INS ブリッジによる接続

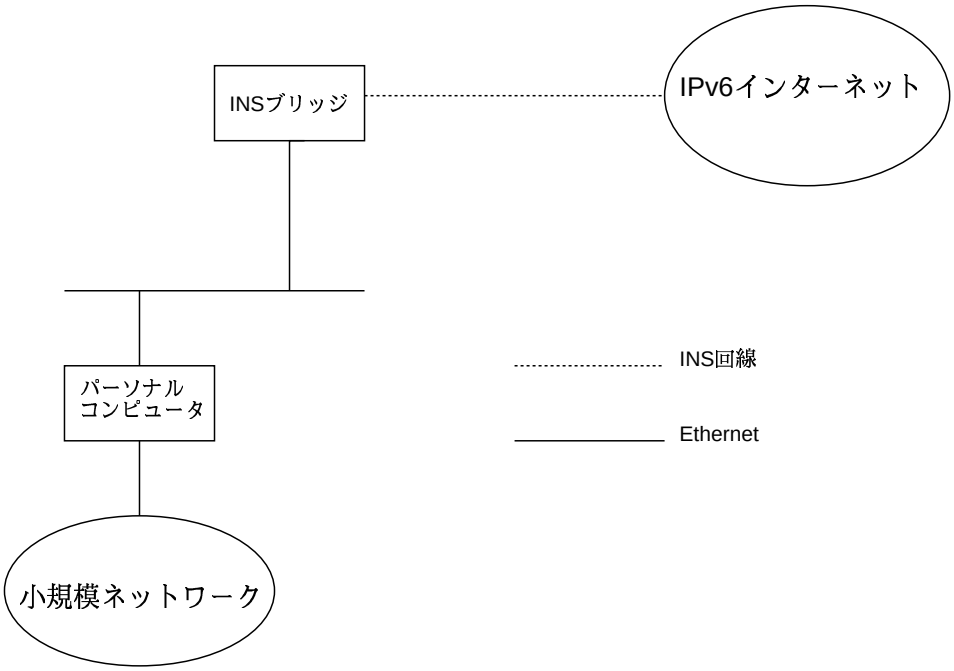


図 4.2: パーソナルコンピュータを利用した接続

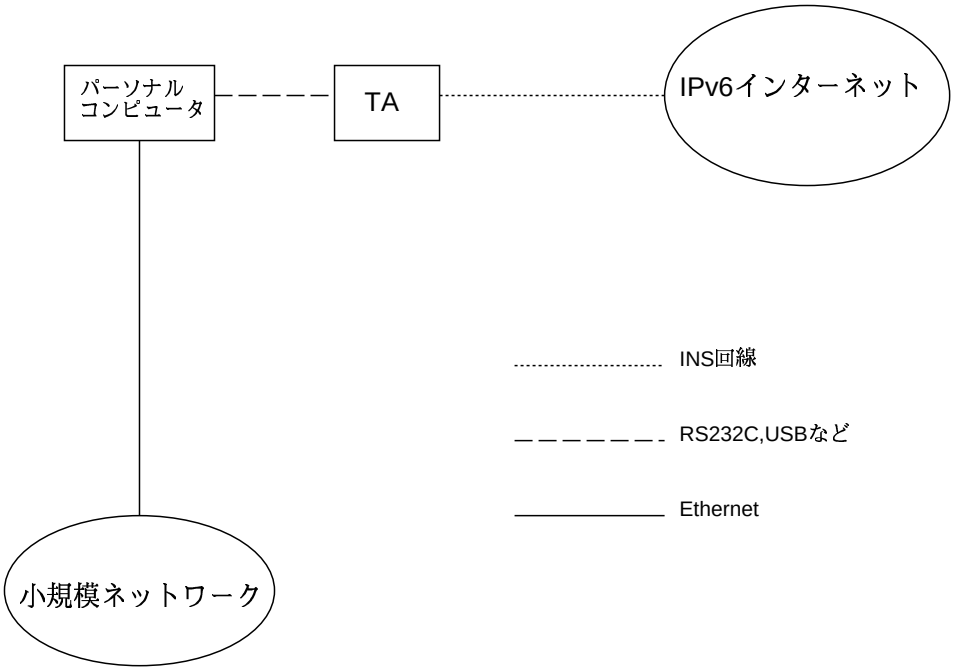
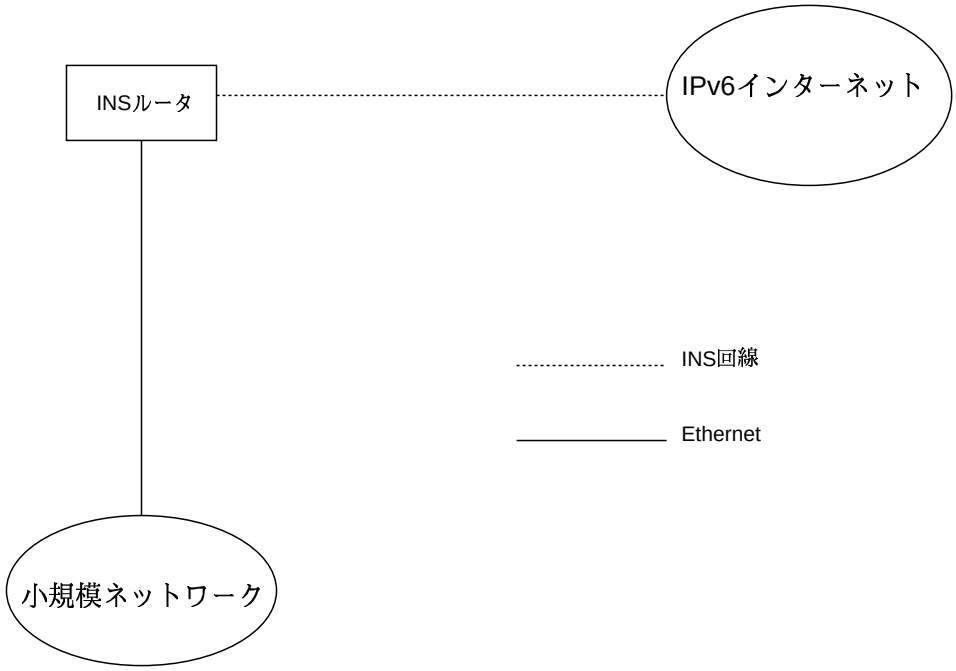


図 4.3: INS ルータによる接続



INS ブリッジを利用した場合，INS 回線への接続に INS ブリッジが用いられる他に小規模ネットワーク用のセグメントを構築するルータが必要になる．ここではパーソナルコンピュータを利用したルータを想定している．

パーソナルコンピュータを利用した場合，INS 回線への接続にはターミナルアダプタ (TA) が必要になる．パーソナルコンピュータは小規模ネットワーク用のセグメントを構築し，TA を利用して小規模ネットワークと IPv6 ネットワーク間を接続する．

INS ルータを利用した場合，INS 回線への接続と小規模ネットワーク用のセグメントの構築の両方を INS ルータで行える．

導入コストの比較 それぞれの手法について導入コストの比較を行った結果を表 4.1 に示す．

手法	想定した機材	コスト
INS ブリッジ	PlatHome 製 EntrySystem/PICKLES	19,9500 円
	ヤマハ製 リモートルータ RT103i	15,8000 円
	合計	35,7500 円
PC ルータ	PlatHome 製 EntrySystem/PICKLES	19,9500 円
	ヤマハ製 TA/リモートルータ RTA50i	49,800 円
	合計	24,9300 円
INS ルータ	ヤマハ製 TA/リモートルータ RT50i	49,800 円
	合計	49,800 円

表 4.1: INS ルータと PC ルータの比較

この結果から，導入コストについては INS ルータを用いた場合が最も低く，INS ブリッジを利用した場合が最も高いことが分かる．INS ブリッジは INS ルータに比べ単純な処理のみを行うため実装が容易だが，目的が限られていることから安価には入手できない場合が多い．それに対して INS ルータはすでに広く普及しているため入手は容易である．

INS 回線と専用線の比較 最後に INS 回線を利用してネットワークを構築した場合と専用線をもちいてネットワークを構築した場合のコストの違いを示す．INS 回線と専用線では課金の体系が異なる．INS 回線は接続時間により課金されるのに対し，専用線は常時接続されているため，月単位で課金される場合が多い．ここでは両者を比較するため，1999 年 9 月 6 日から 1999 年 9 月 8 日に行った WIDE ワークショップでの実験をもとに INS 回線の接続時間を決定した．WIDE ワークショップでの INS 回線の接続時間を表 4.2 に示す．

このうち，終日実験を行ったのは 1999 年 9 月 7 日のみである．サテライトオフィスでの利用に最も近いの同日のデータであると考え，以下の試算では接続時間として 13 時間 41 分 12 秒を採用している．利用する機材として 64[kbps] から 128[kbps] までの帯域にはヤマハ製のリモートルータ RTA50i を利用し，192[kbps] 以上はヤマハ製のリモートルータ RT104p を利用するものとして計算している．

日付	接続時間
1999 年 9 月 6 日	6 時間 4 分 35 秒
1999 年 9 月 7 日	13 時間 41 分 12 秒
1999 年 9 月 8 日	6 時間 59 分 36 秒

表 4.2: WIDE ワークショップでの接続時

また，接続料金としては 1999 年 12 月現在の NTT のサービスの中から広く用いられているサービスとして INS64,DA64,DA128,DA1500,HSD64,HSD128,HSD1500 をについて計算した．INS64 は一般の家庭やサテライトオフィスなどで音声通話とデータ通信を兼ねて提供されているサービスである．DA64,DA128,DA1500 は高速専用線サービスの一つで，保守契約が簡略化されているが利用料金がやすい．HSD64,HSD128,HSD1500 も高速専用線サービスの一つであるが，保守契約が充実しているため大規模な企業のオフィスなどに利用される．

それぞれのサービスの帯域と利用料金を表 4.3 に示す．

回線種別	帯域	料金
INS64	64[kbps]	10 円/20 秒
INS64	128[kbps]	20 円/20 秒
DA64	64[kbps]	69,000 円/月
DA128	128[kbps]	112,000 円/月
DA1500	1.5[Mbps]	650,000 円/月
HSD64	64[kbps]	148,000 円/月
HSD128	128[kbps]	185,700 円/月
HSD1500	1.5[Mbps]	1103,000 円/月

表 4.3: INS 回線と専用線の回線費用の比較

以上をもとに回線の種類とコストの関係を試算したのが図 4.4 である．

また，回線の導入コストまで含めて試算した場合を図 4.5 に示す．導入コストとしては，INS ルータの購入費用，施設設置負担金，配線工事費，基本工事費を想定している．

INS ルータを用いる場合，上の図中の 128[kbps] 以下が最もコストが低くなるが，192[kbps] を越えると回線とのインターフェースが変わるため，急激にコストが悪化する．小規模ネットワークではこの程度の帯域で十分なことが多いため INS ルータの導入は小規模ネットワークに適していると言える．

接続形態はある程度の時間接続する場合には専用線接続が良い．とくに Degital Access サービスは現状では非常にコストの低い接続法である．INS ルータと組み合わせて用いると非常に低い運用コストを達成できる．

図 4.4: INS ルータと専用線の回線費用の比較 (接続時間のみ)

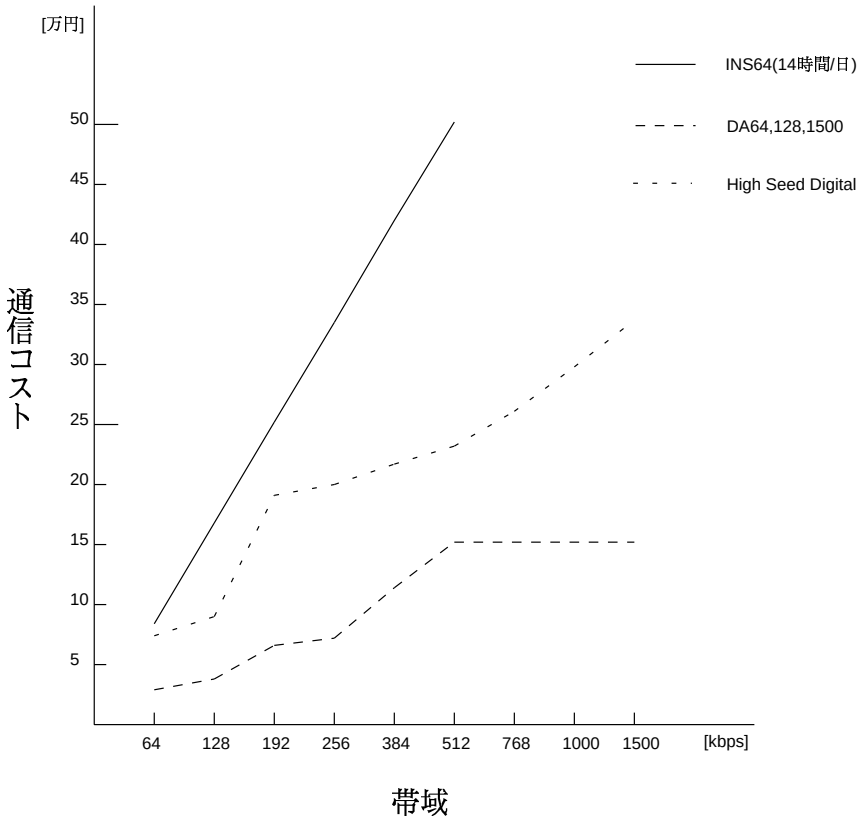
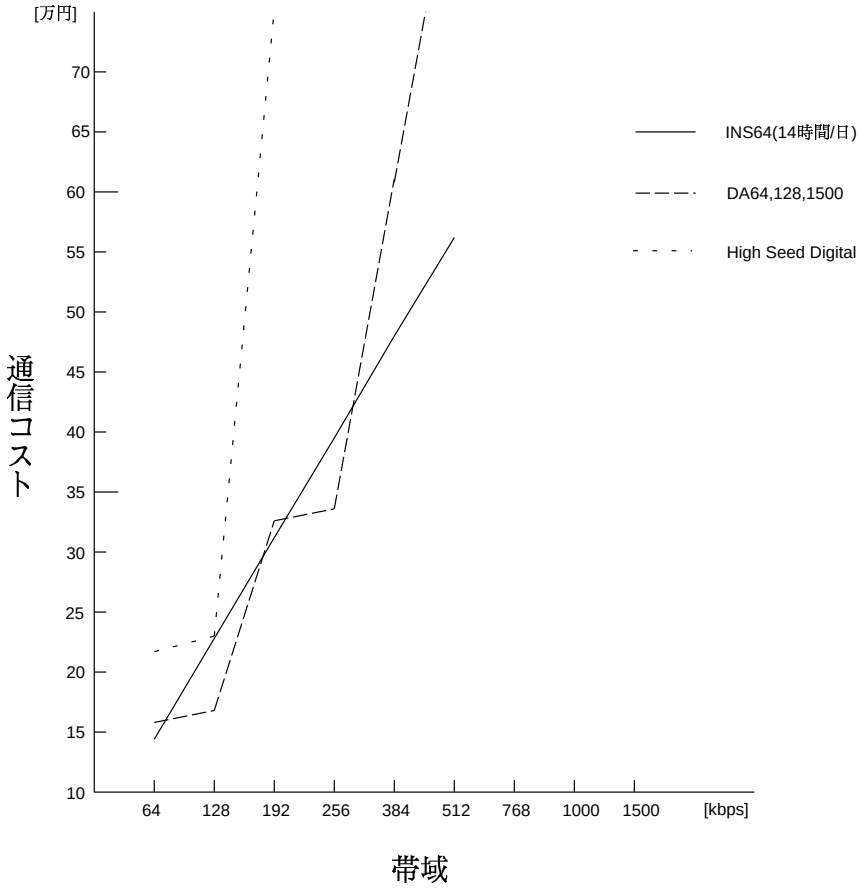


図 4.5: INS ルータと専用線の回線費用の比較 (導入コスト込み)



第5章　WS-One

5.1　WS-One の概要

WS-One は東京工業大学とヤマハ株式会社との共同研究として実装を進めてきた IPv6 プロトコルスタックである．現在の WS-One はヤマハ株式会社製の INS ルータ上で動作する．著者はこのルータにより研究室のネットワークに IPv6 の導入を行ってきた．以下に WS-One の特徴を示す．

- IPv4 と IPv6 を同時に扱えるデュアルスタック構成である．
- INS 回線と Ethernet の間で IPv6 のルーティングが行える．
- 特殊なハードウエアを必要とせず，既存の INS ルータのファームウエアの書き換えのみで利用できる．

これらの特徴により，既存の IPv4 ネットワークに WS-One を導入するだけで IPv6 ネットワークへの接続の大部分が完了する．デュアルスタック構成を取っているため，IPv4 の接続も同時に確保できるため IPv4 のサービスもこれまでと同様に利用可能である．

本実装はヤマハ株式会社との守秘協定の下での共同研究として行ってきたため，実装の詳細については記述できない．ここでは一般的なことについてのみ言及する．

5.2　WS-One の実装

著者は表 5.1 および表 5.2 で示した目標に基づき WS-One の実装を進めてきた．以下に現在の実装状況を示す．

表中の重要度は以下の意味である．

a IPv6 対応 Dial-up router としては必須．

b 将来的には必須になるが，現状ではなくてもよい．

c あったほうが用途は広がるが，なくてもよい．

それぞれの項目についての詳細は以下の通りである．

表 5.1: RFC で規定されている機能

機能	重要度	状況
NA send	a	不完全
NA receive	a	不完全
NS send	a	不完全
NS receive	a	不完全
RA send	a	実装済
RA receive	b	未実装
RS send	b	未実装
RS receive	a	実装済
MLD	b	未実装
IP Aliase	a	不完全
IPV6CP	a	実装中
Multicast	a	不十分
Anycat	b	未実装
RIPng	c	実装中
v4 over v6 Tunnel	c	未実装
v6 over v4 Tunnel	c	未実装
v6 over v6 Tunnel	c	未実装

NA send NA は Neibor Advertize の略で近隣広告と呼ばれる機能である．これにより IPv6 ネットワーク中で自分の存在を周囲に通知する．IPv4 では ARP に相当する機能である．

NA send はこの NA メッセージを近隣のホストに対して通知する機能であり，この機能がないと近隣のホストからの通信を受けとることができない．

NA receive これは近隣からの NA メッセージを受けとる機能である．受けとったメッセージは通常一定時間保存する．そのため，ホスト内部には常に近隣のホストの情報が存在することになる．

NS send NS は Neibor Solicitation の略で近隣探索と呼ばれる機能である．IPv6 アドレスに対応するホストが見つからない場合，近隣探索により目的のホストを探す．

NS send は NS メッセージを送信する機能である．

NS recieve 近隣からの NS メッセージを受け取り，必要であれば NA メッセージを送信する機能である．

RA send RA は Router Advertize の略でルータ広告と呼ばれる機能である．IPv6 のルータとして動作するホストは近隣のホストにたいして自分がルータであることを RA メッセージにより通知する．

表 5.2: Internet Draft で規定されている機能

機能	重要度	状況
ICMP Name Lookup	b	未実装
CSI[1]	b	未実装
Default Address Selection	b	未実装
IND[2]	c	未実装

この機能があることで，IPv4 のように手動での経路設定は必要なくなる．同じセグメント内部に複数のルータが存在する場合でも，RA を適切に処理することで効率よい経路の選択が可能となる．この仕組みは default address selection と呼ばれ，現在 IETF で仕様の策定が行われている．

RA send は RA メッセージを近隣にたいして送信する機能である．RA の送信を行わなくても手動で経路設定を行えるが，管理を簡単にするためにも RA メッセージの送信は行えることが望ましい．

RA receive 近隣のルータから RA メッセージを受けとる機能である．通常ルータとして動作するホストは RA による経路制御よりも高度な経路制御を必要とするため RA メッセージを受け取り，経路を設定することはない．

しかし，RFC ではその場合でも RA メッセージを受けとった場合にはそのメッセージが適切であるかどうかを調べた上でメッセージを破棄するのが望ましいとされているため，実装することが望ましい．

RS send RS は Router Solicitation の略でルータ探索と呼ばれる機能である．通信を行うために必要な経路が見つからなかった場合に RS メッセージを送信することでルータを探すことができる．

ルータ自身は通常隣接する経路を保持しているため RS を送信することはない．しかし，RS は RFC の中で必須の機能として定義されているため実装したほうがよいと言える．

RS receive 近隣からの RS メッセージを受信して必要に応じて RA メッセージを送信する機能である．ルータとして機能する場合には必須の機能である．

この機能がないと，近隣のホストにたいして手動で経路を設定しなくてはならなくなる．

MLD MLD は Multicast Listener Discovery の略でマルチキャスト通信を行う意思を近隣に対して通知する機能である．

IPv6 はマルチキャスト通信を積極的に利用する．現在はマルチキャストを前提とするサービスは少ないが，今後は増加すると予想できる．将来を考て実装しておくのが望ましい．

IP Alias IP Alias はインターフェースに対して自動で生成されたアドレス以外のアドレスを割り当てる機能である.

IPv6 ではアドレスは自動生成されるため，手動で割り当てる必要はないが DNS サーバなどの管理を行う場合には固定的なアドレスを割り当てたほうが便利なことも多い.

したがって，効率のよい管理を行うためには実装したほうがよい.

IPV6CP IPV6CP は PPP 接続の際にアドレスの設定を行う機能である.

Multicast Routing マルチキャスト通信を行う場合に必要になる機能である．ルータはマルチキャスト通信のパケットを重複がないようにすべてのホストに送信する必要があるため，特殊な経路制御を行う必要がある.

現在は PIM と呼ばれる経路制御アルゴリズムが広く利用されている.

Anycast エニーキャスト通信は IPv6 ではじめて採用された新しい通信形態である.

現在ではエニーキャストを利用したサービスは提供されていないが，将来的には各種サービスを提供するサーバを自動的に探索するなどの用途に利用されることが予想される.

RIPng IPv4 で用いられていた経路制御プロトコルである RIP を IPv6 で利用できるように拡張したプロトコルである．小規模なネットワーク内のルーティングには一般的に RIPng が利用されている.

v4 over v6 Tunnel IPv6 のパケットを IPv4 のネットワークを利用して送受信する機能である.

現在は IPv6 での PPP 接続を受け付けているサイトは少ないため，IPv6 ネットワークへの接続には事実上トンネルを用いる他にない．そのため，IPv6 導入の初期段階では事実上必須になる可能性がある.

v6 over v4 Tunnel IPv4 のパケットを IPv6 のネットワークを利用して送受信する機能である.

IPv6 へ移行したあとでも IPv4 ネットワークへの接続が全く必要ないとは限らないため，このような機能が必要になる.

v6 over v6 Tunnel IPv6 のパケットをカプセル化して IPv6 ネットワーク上に流す機能である．IPv6 には標準で暗号化機能が定義されているため，この機能があれば簡単に VPN を構築できるようになる.

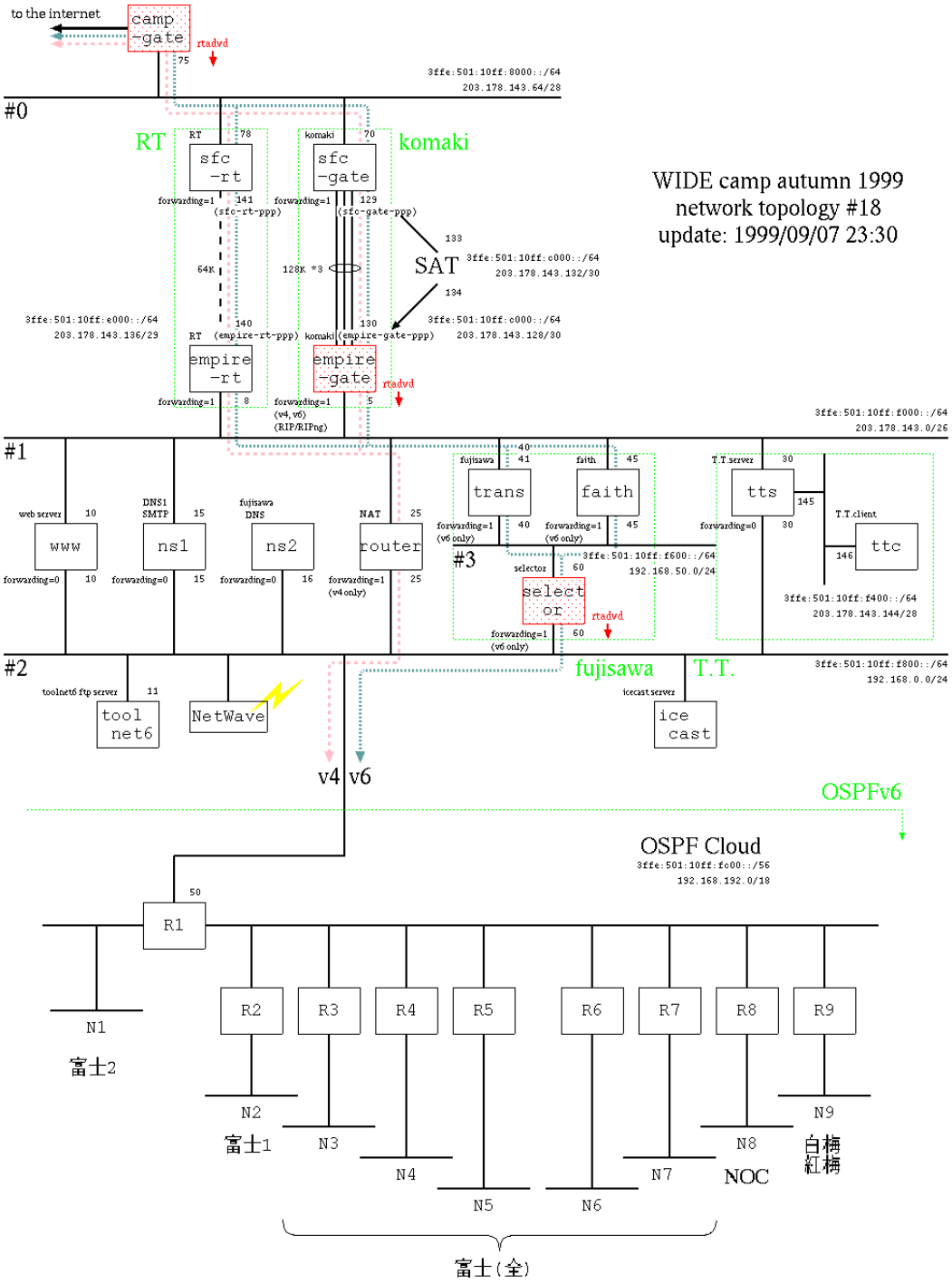
サテライトオフィスでは頻繁に使われることが予想される.

5.3 WS-One運用実験

著者はWS-Oneを用いて小規模ネットワークへのIPv6の導入実験を繰り返してきた．その実験結果を示す．

WIDEワークショップでの実験 1999年9月6日から1999年9月8日にかけてWIDEワークショップにおいてWS-One運用実験を行った．WIDEワークショップの開催地である浜松のホテルと藤沢の慶応大学の間をINS回線2本とWS-Oneを用て接続し，WS-Oneが実際の運用に耐え得るか検証した．この実験のネットワーク構成図を図5.1に示す．

図 5.1: WIDE ワークショップでの実験ネットワーク



実験中の回線の状況は図 5.2-5.6 のようになった.

図 5.2: 1999 年 9 月 6 日午後の回線の接続状態

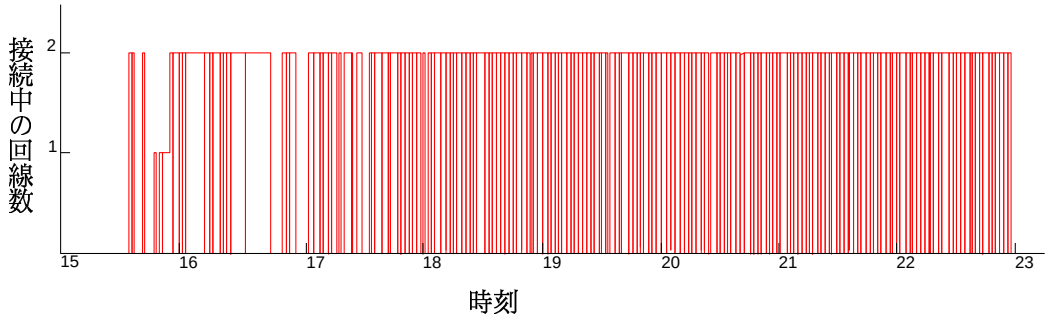


図 5.3: 1999 年 9 月 7 日午前の回線の接続状態

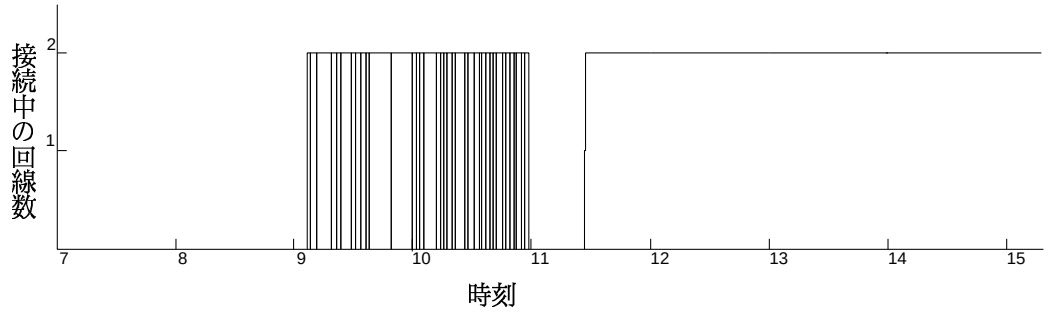


図 5.4: 1999 年 9 月 7 日午後の回線の接続状態

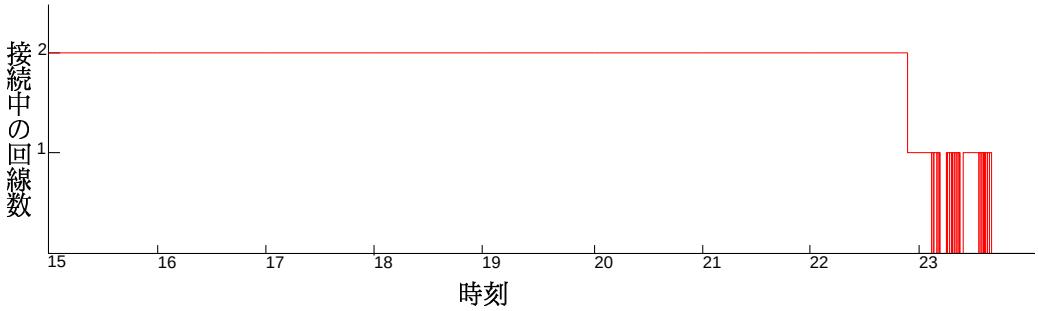


図 5.5: 1999 年 9 月 8 日午前の回線の接続状態

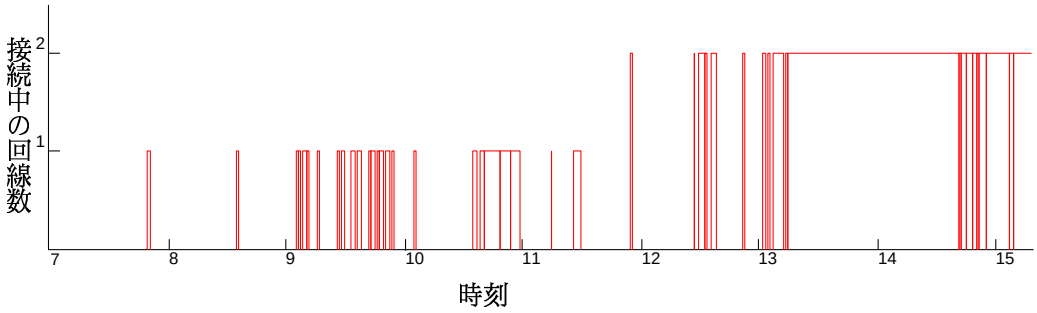
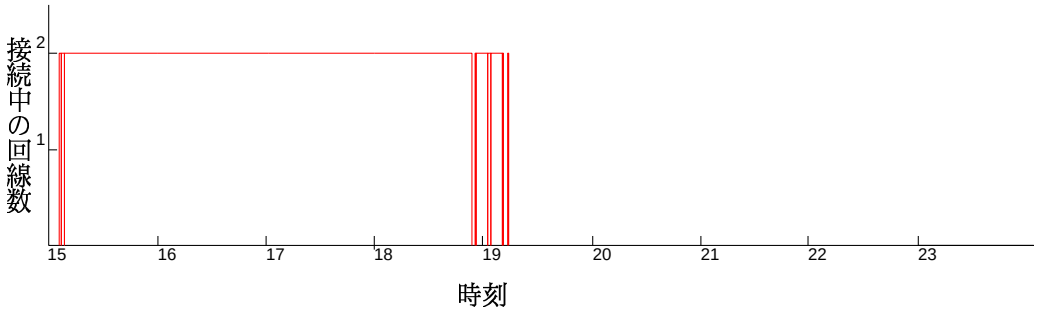


図 5.6: 1999 年 9 月 8 日午後の回線の接続状態



実験前半では接続と切断が頻繁に行われている．これは設定のミスによりIPv6のパケットが流れているにも関わらず自動切断が働いていたためである．9月7日の実験ではこの点を修正し，正常に接続を維持できるようになった．9月7日の午後に利用するINS回線を1回線に限定したところ，再び接続が行えない状態になった．9月8日になっても状況は改善せず，やむおえずINSルータを再起動したところ正常に接続が行えるようになった．正常に接続が行えるようになったあとでも接続と切断を繰り返すことがあったが，INSルータの再起動により正常な接続が行えることが分かった．

以上の結果から，WS-OneはIPv6パケットの送受信に関してはほぼ完成していると言える．ただし，接続と切断を頻繁に繰り返すと接続不能な状態に陥ることから，INS回線の接続を行っている部分に問題があることが明らかになった．

YAMAHA-東工大 接続実験 1999年10月14日と1999年10月15日に東京工業大学とヤマハ株式会社の間をWS-Oneで接続し、IPv6を利用した通信が正常に行えるかどうかを確認した。WIDEワークショップでの実験で見付かった不具合を修正し、新しい機能をいくつか追加したので、それらの確認も合わせて行った。

あらしく追加した機能はIPv6の自動設定機能である。この機能があるとWS-Oneを設置したネットワーク内のホストはとくに設定をしないでもIPv6による通信が行える。実際に東京工業大学側とヤマハ株式会社側にホストを用意して通信を行ったが、とくに設定をしなくても問題なく通信できることを確認した。

ただし、通信を行う場合には通信相手となるホストのIPv6アドレスを口頭で伝える必要があった。DNSサーバに登録することでこの問題は解決できる。しかし、現在のところWS-OneにIPv6対応のDNSサーバ機能を追加する予定はないのでDNSサーバは別途必要である。

IPv6に対応したDNSサーバについてはすでに研究が行われている[18]。DNSサーバのデータベースを動的に更新する手法に関しても研究がすすんでる[19]ため、改善を期待できる。

これらのWS-Oneによる実験によりいくつかの事実が明らかになった．

IPv6を用いた場合はNATを用いることなく全てのホストにIPアドレスを振ることができる．さらにIPv6はアドレスの設定が自動化されているため，DHCPによるアドレス管理は必ずしも必要ない．高度な設定を行う場合はDHCPによる管理が必要になるが，著者の実験環境ではDHCPを用いなくてもネットワークは問題なく機能する．逆に実際にあるホストのアドレスはホストの起動時に自動的に生成されるため，実際にそのホスト起動しないと生成されるアドレスを知ることができない．

IPv6はアドレス空間が広いため，ユーザがアドレスを覚えることは現実的ではない．そのため，IPv4以上にDNSが重要な意味を持つと考える．しかし，現状ではIPv6アドレスをDNSに登録するためには管理者が手でアドレスを登録する必要がある．IPv4の場合は初めにアドレスの割り当てを決定し，あらかじめDNSサーバに登録できる．しかし，

IPv6の場合にはアドレスは自動で生成されるため，あらかじめDNSサーバにアドレスを登録するわけにはいかない．

IPv6であっても手動でアドレスを設定することは可能である．IPv4と違い一つのインターフェースに複数のアドレスを割り当てることも可能である．この機能を利用することでIPv4と同様のDNS管理を行うことも可能である．ホストが小数の場合はこの方法で管理を行うのがもっともコストが低いと考える．

ただし，この方法が有効なのはネットワーク上に常に存在するホストのみである．ノートブックコンピュータのように移動を前提としたホストの場合，アドレスの登録は不可能である．IPv4の場合，DHCPサーバでこのようなホストに割り当てるアドレスを管理しており，そのアドレスをDNSに登録しておくことができる．しかし，DHCPサーバを用いずにIPv6を運用した場合この方法は使えない．

IPv6用のDHCPサーバについてはIETFで議論されている．また，最新のBINDではDNSサーバのレコードを動的に更新できる．これらの環境が整えばIPv6であってもIPv4同様に移動するホストを管理できると考えるが，現状では管理は困難であると考える．

IPv6特有の問題もいくつか存在している．一つはサブネットの管理である．IPv4ではサブネットマスクを自由に設定できることから，組織内で仮想的なアドレス管理を行うことができる．しかし，IPv6ではプリフィックスは64bitまでという制限があり，小規模な組織に対しては56bit程度のプリフィックスが割り当てられることが多い．このため，組織内で階層的なアドレスの管理を行う場合最大でも8階層が限度である．

著者の運用するネットワークでは問題は生じなかったが，小規模なネットワークであってもアドレスを階層管理する必要が生じる可能性がある．この場合，IPv4に比べ自由度の低いネットワークしか構築できない．

IPv6が普及するまでの移行期間はIPv4とIPv6が共存しているネットワークが多く存在するはずである．さらに小規模ネットワークにおいてはIPv4はプライベートアドレス空間でIPv6がグローバルアドレス空間というネットワークになる可能性が高い．

この場合，IPv4は外部から参照される可能性はない．しかし，IPv6は外部から参照される可能性がある．IPv4，IPv6ともに内部からは参照される可能性がある．このとき，DNSの名前空間の管理に問題が発生する．外部からの問い合わせに対してはIPv6アドレスのみを返し，内部からの問い合わせに対してはIPv4,IPv6両方のアドレスを返すように設定する必要がある．

この問題の解法としていくつかのモデルが考えられる．

一台のDNSサーバが問い合わせごとに異なる返事を返すことができればこの問題は解決できる．しかし，現在インターネットで広く用いられているBINDでこのようなサーバを構築した場合，ドメインを分割して管理する必要がある．この場合，おなじアドレス空間に対して複数のドメインが存在することになり，ユーザに不自由を強いることになる．

問い合わせが外からきたのか内から来たのかを区別し，必要な情報のみを返す機能をもったDNSサーバが存在すればこの問題は根本的に解決できるが，現状では解決不可能である．

外部からの問い合わせを処理するサーバと内部からの問い合わせを処理するサーバを個別に構築することでも問題を解決できる．しかし，この場合同じアドレス空間に対して複

数の DNS サーバが存在することになる．ユーザは内部用のサーバを参照することで期待通りの結果を得ることができるが，管理者は 2 台のサーバの持つデータベースを同期させつつ管理する必要がある．データベースの同期には一般的な方法は現状では存在しないため，管理者が個別に対応しなくてはならない．

第6章　考察と課題

6.1　IPv6導入の利点と欠点

IPv6 導入の利点を以下に挙げる．

1. アドレスの不足を根本的に解決できる
2. 設定が自動化されているため管理コストを下げられる

また，IPv6 導入の欠点としては以下が考えられる．

1. 管理するに当たって IPv6 特有の問題を理解しなくてはいけない
2. 諸設定に関する知識が要求される
3. IPv4 のプライベートネットワークとの共存が難しい

これらの欠点は IPv6 そのものの欠点ではないが，IPv6 導入の大きな障害であると考える．とくに IPv4 のプライベートネットワークとの共存はほぼすべての小規模ネットワークで必要だと考えられることから早急に運用技法を確立する必要がある．

IPv6 導入の欠点全体に，原因が IPv6 にあるのではなく新技術を導入するという行為にあるという特徴がある．したがって，導入を終えてしまえばこれらの欠点はやがて解消すると考える．

6.2　IPv6INS ルータについての考察

本研究により，小規模ネットワークへの IPv6 導入にはダイアルアップルータが有効であることが明らかになった．これは従来の PC ルータを利用したネットワーク構築に比べて導入コストが低くすむことが大きな要因である．小規模ネットワークでは一般にネットワーク構築に十分な予算が確保できないことが多い．そのため，現在の小規模ネットワークではダイアルアップルータが多く用いられている．したがって，既存の設備をほぼそのまま利用できる本研究のフレームワークは有効に機能することが期待できる．現在の機材を IPv6 に移行した場合，性能の低下が懸念されるが，この点についても実験結果から問題は発生しないことが明らかになった．したがって，著者の小規模ネットワークへの IPv6 にはダイアルアップルータが有効であるという主張は正しいと結論できる．

今後 WSONE は小規模ネットワークに IPv6 を導入するために必要十分な機能を実装し，安定動作させることが課題である．また，IPv6 の導入を進めるにあたって IPv4 との混在環境をどうするかという問題が必然的に発生する．この問題は導入初期にのみ発生するが，現状では大きな障害であると考える．この点に関して WSONE を用いてコストの削減を計ることができれば IPv6 導入の大きな助けになると考える．

著者の構築したネットワークは IPv4 で提供されるサービスに対し，IPv6 で提供されるサービスが不足している．今後，IPv4 と同様のサービスを行えるように研究を進めていく必要がある．IPv6 が普及するためには IPv4 と同等以上のサービスが低コストで提供できることが必須である。この点を解決できない限り、IPv6 の普及は難しいといわざるを得ない。

WSONE の実装は今後小規模ネットワーク用の INS ルータとして必要十分な機能を持つように進める．表で a となっている項目は著者が小規模ネットワーク用の INS ルータとして必須であると考える項目であり，この項目の実装を完全にすることが目標である．小規模ネットワークへの IPv6 導入そのものについても，IPv4 の抱える問題点の解消に有効であることが明らかになった．従来の NAT を用いた運用に比べ管理コストを下げられるためである．現在の NAT はインターネット技術の本筋から外れたものであり，管理には多大なコストがかかる．NAT に基づくネットワーク構築はネットワークにインターネット技術に対する深い理解と同様に NAT に対する理解を求めるものである．これに対し，IPv6 を利用したネットワーク構築は本来のインターネット技術のみの理解で行える．管理者はインターネット技術そのものに対する理解に全力をあげることができるため，その分サービスの向上を期待することも可能である．これは IPv6 導入の大きなメリットであると考える．

6.3 今後の課題

1. INS ルータの実装についても不十分な点がいくつか存在している．これらの点の解消が必須である．INS ルータの実装が完全になれば IPv6 導入はきわめて容易になると予想できる．

2. 本研究により INS ルータを用いることで IPv6 の導入コストを大きく下げられることが明かになったが，導入後にも様々な問題が発生することも同時に明らかになった．導入コストだけではなく運用コストまで含めて IPv6 の導入を促せるような研究が必要だと著者は考える．

第7章　おわりに

本研究により以下が明らかになった。

1. INS ルータを利用すると小規模ネットワークに低コストで IPv6 を導入できる。
2. IPv6 は小規模ネットワークでの運用に対して十分な性能を持っている。
3. 既存の IPv4 ネットワークに IPv6 を導入することで既存のサービスを利用しつつ段階的ににアドレスの不足を解決できる。

これらの事実について次のように考える。

IPv6 はまだ新しい技術である。新しい技術の導入においては常にコストの問題が発生する．しかし本研究により小規模ネットワークへの IPv6 の導入手法として INS ルータの利用が非常に適していることが明かになった．INS ルータを用いることで最低限のコストで小規模ネットワークに IPv6 を導入できると考える．

IPv4 インターネットのアドレスは必ず不足する。IPv4 インターネット上で大きな位置を占める小規模ネットワークのアドレス空間の不足は最優先で解決しなければいけない問題である．アドレス空間の不足に根本から対応できる技術は現状では IPv6 以外の選択はない．本研究により IPv6 は小規模ネットワークにおいて十分な性能を持つことが明らかになった。従って，小規模ネットワークには積極的に IPv6 を導入すべきであると考える．

現在は IPv6 を前提としたサービスはまだ少ないが，基幹ネットワークでは IPv6 への移行が急速に進んでおり，現在の IPv4 インターネットが IPv6 インターネットにおきかわるのは時間の問題であると考える．IPv6 インターネットに対する IPv4 インターネットの優位点は存在しない．IPv4 を前提としたサービスが必要な場合であっても，IPv4 と IPv6 の混在環境として運用が可能であることが本研究により明かになった．したがって，小規模ネットワークが IPv4 に固執する理由はなく，IPv6 の導入は早いほうがよいと考える．

以上から，今後の小規模ネットワークでは INS ルータを用いた IPv6 導入を積極的に進めるべきであると結論する．

参考文献

[1] Jon Postel. INTERNET PROTOCOL. *RFC791, IETF*, 1981.

[2] K. Egevang and P.Francis. The IP Network Address Translator (NAT). *RFC1631, IETF Network Working Group*, 1994.

[3] S. Deering and R. Hinden. Internet Protocl, Version 6 (IPv6) Specification. *RFC2460, IETF Network Working Group*, 1998.

[4] Y. Rekhter and T. Li. A Border Gateway Protocol 4(BGP-4). 1995.

[5] G. Malkin and R. Minnear. RIPng for IPv6. *RFC2080, IETF Network Working Group*, 1997.

[6] J. Moy. OSPF Version 2. *RFC2328, IETF Network Working Group*, 1998.

[7] G. Malkin. RIP Version 2. *RFC2453, IETF Network Working Group*, 1998.

[8] R. Coltun, D. Ferguson, and J. Moy. OSPF for IPv6. *RFC2740, IETF Network Working Group*, 1999.

[9] P. Gross and P.Almquist. IESG Deliberations on Routing and Addressing. *RFC1380, IETF Network Working Group*, 1992.

[10] D. Mills. Exterior Gateway Protocol Formal Specification. *RFC904, IETF Network Working Group*, 1984.

[11] V. Fuller, T. Li, J. Yu, and K. Varadhan. Classless Inter-Domain Routing (CIDR): an Address Assignment and Aggregation Strategy. *RFC1519, IETF Network Working Group*, 1993.

[12] Y. Rekhter and T. Li. An Architecture for IP Address Allocation with CIDR. *RFC1519, IETF Network Working Group*, 1993.

[13] Y. Rekhter, B. Moskowitz, D. karrenberg, and G. de Groot. Address Allocation for Private Internets. *RFC1597, IETF Network Working Group*, 1994.

[14] P. Srisuresh and M. Holdrege. IP Network Address Translator (NAT) Terminology and Considerations. *RFC2663, IETF Network Working Group*, 1999.

[15] C. Partridge and F. Kastenholz. Technical Criteria for Choosing IP The Next Generation (IPng). *RFC1726, IETF Network Working Group*, 1994.

[16] S. Bardner and A. Mankin. The Recommendation for the IP next Generation Protocol. *RFC1752, IETF Network Working Group*, 1995.

[17] 白砂哲. 小規模ネットワークに適した次世代インターネット技術の導入手法. 1998.

[18] S. Thomson and C. Huitema. DNS Extentions to support IP version 6. *RFC1886, IETF Network Working Group.*

[19] P. Vixie, S. Thomson, Y. Rekhter, and J. Bound. Dynamic updates in the Domain Name System (DNS UPDATE). *RFC2136, IETF Network Working Group*, 1997.

[20] Mark A. Miller, 宇夫陽次朗. IPv6 入門. 1999.

謝辞

本研究の指導を精力的に行ってくださった郵政省通信総合研究所非常時通信研究室の大野浩之室長に感謝する．同時に，著者が本研究を郵政省通信総合研究所にて行うことを快諾してくださった日本大学理工学部電気工学科の日向隆教授に感謝する．

本研究はヤマハ株式会社と共同で行った．INS ルータのファームウエア開発について多くの助言をくださった同社の高山明氏，小池田恒之氏，広瀬良太氏，木村俊洋氏に感謝する．

WIDE ワークショップにおいて INS ルータを利用した実験に対し多大な支援を行ってくださった WIDE プロジェクトに感謝する．

著者の実装した INS ルータを利用して貴重な助言をくださった KAME プロジェクトの萩野純一郎氏，および東京大学情報基盤センターの加藤朗助手に感謝する．

最後に著者の研究生活を支え，貴重な意見を聞かせてくれた東京工業大学大野研究室のメンバに感謝する．