# 第２部

# 特集2 IPv6 only Network構築と検証実験

櫨山 寛章, 上野 幸杜, 佐藤 弘崇, 石橋 尚武, 横石 雄大, 山岸 祐大, 石原 知洋

## 第１章　概要

2011年9月WIDE合宿の実験のメインテーマとして、参加者にDHCP6とDNS64/NAT64のアドレス変換によるIPv6 onlyアクセス環境のみを基本的に提供し、ユーザが普段利用しているOSやアプリケーションのIPv6対応状況の確認や、IPv6のみを有効にする設定やIPv6 onlyアクセス環境で快適に生活するための知見、NAT64/DNS64を実際に利用した際の問題点の洗い出しを行った。また、IPv4コネクティビティの提供方法としてSA46Tによる464トンネルを用いてWIDEバックボーンのIPv4グローバルアドレスをMACアドレス登録制のDHCP4で提供し、あわせて、IIJで開発しているSEIL 4RDルータとvyattaの4RD拡張を用いて4RDによるIPv4プライベートアドレスの提供実験を行った。2つのIPv4提供実験はともにアドレス変換、トンネリング技術である。また、対外線をIPoE方式で提供されるIPv6インターネット接続サービスのみを利用し、慶應義塾大学上野によって作成されたIPv6用LT2Pを用いてWIDEバックボーンへのL2トンネルを作成しWIDEバックボーンからのルーティングを行うため、多重カプセリングの影響を把握する検証も参加者を交えて実施した。

## 第２章　はじめに

ここでは、2011年9月6日から9月9日の4日間に開催されたWIDEプロジェクト2011年9月合宿で実施されたIPv6 onlyアクセスネットワーク利用実験に関する報告を行う。WIDEプロジェクトでは、WIDE合宿の実験ネットワークやWIDEバックボーンにてIPv4/IPv6のデュアルスタック環境の運用を長年行ってきた。また、2011年6月に実施されたWorld IPv6dayの前後で多くの商用ISPがIPv6接続サービスを提供開始した。一方で、実際にIPv6だけ提供されるアクセスネットワークとアドレス変換サービスを利用した場合、現在提供されているIPv4もしくはデュアルスタックによる接続サービスと比較して、どの程度利用できるのかに関しての知見は、世界的に見てあまり蓄積されていない。そこで、IPv6のみを利用してどこまでサービスネットワークとして構築し、提供できるかという点と、IPv6しかない環境ではユーザの利用においてどのような問題が生じるのかを洗い出すために、WIDE合宿ネットワーク全体のテーマとしてIPv6 only networkに着目して合宿ネットワークを設計し、構築、運用した。

## 第３章　The Camp 1109ネットワークの設計

合宿ネットワーク全体のテーマとして、IPv6 only networkを構築し、参加者全員がIPv6 only networkで生活するという方針は、2011年5月に北陸先端科学技術大学院大学で実施されたWIDE研究会の研究発表にて議論され、決定した。しかしながら、WIDE合宿参加者の多くは、特に企業からの参加者は、社内ネットワークサービスがIPv6に対応していないことが多く、IPv6接続性のみを提供しても日常の業務（メールの閲覧など）を実施することができない。そこで、合宿ネットワーク準備委員会（以降NetPC）では、WIDE合宿の実験ネットワーク（camp-net）にて、参加者がEMOBILEなどの商用モバイルインターネットサービスに退避せずに4日間生活できる、現実的なサービスとしてIPv6 only network環境の提供方法の模索を始めた。本章では、合宿ネットワークNOCチームで検討し、いくつかの事前検証を通して設計したcamp-netの概要、実験趣旨および技術解説を行う。

### 3.1 実験概要

まず、NOCチームにより、

1） DHCP6の利用実験、
2） NAT64/DNS64によるIPv6/IPv4アドレス変換の利用実験、
3） SA46TによるIPv6バックボーンを介したIPv4ネットワーク接続性提供実験、
4） WPA2 EAP-TLSによる無線LANアクセス認証、

の4つの実験を実施した。これに合わせて、慶應義塾大学、IIJ、NTT東日本、インターネットマルチフィードによって構成された実験チームによる4RDによるIPv6およびIPv4ネットワーク接続性提供実験が実施された。

### 3.2 対外接続

図3.1に示すように、今回のcamp-netではIPv6による2つの対外線を用意した。ひとつは松代ロイヤルホテルと慶応大学湘南藤沢キャンパス(SFC)を結ぶ衛星回線であり、もうひとつはNTT東日本により提供されたFTTH回線である。

まず衛星回線に関して説明する。衛星回線は1.5GHz帯を用いた回線で下り1.5Mbps,上り512Kbpsの回線利用申請を行った。衛星回線は合宿会期中通して安定していた。衛星回線を挟みSFC側のルータとcamp-netのコアルータとの間でVLANを構築した。

次にFTTH回線について説明する。FTTH回線ではNTT東日本をアクセスキャリア、インターネットマルチフィードをVNE (Virtual Network Enabler)、IIJをIPv6 ISPとして構成された2種類の商用IPv6アクセスサービスを検証した。設営に当たる2011年9月5日から9月6日午後8時まではフレッツ光ネクストのIPv6オプション付きの契約を行い利用した。9月6日午後8時からは、4RDの検証を実施するために、さらに光電話オプションをつけて再契約およびオプション変更に伴う工事を実施し利用した。光電話オプションのあり・なしの差異は、光電話オプションなしではIPv6はRAにて/64のIPv6アドレスが割り当てられ、一方、光電話オプションありの場合はDHCP6により/48のIPv6が割り当てられる。FTTH回線の変更を図示すると図3.1(b)のようになる。

IPv6インターネットへの接続性はIIJ mio FiberAc-cess/NF for IPv6ネイティブサービスを契約し利用した。9月6日午後8時までは、図3.1(a)に示すように、camp-netで用意したL2TPゲートウェイにFTTH回線上のRAで割り当てられる/64プレフィックス長のIPv6アドレスを設定した。

一方、9月6日午後8時以降は、図3.1(b)に示すように、IIJが研究開発しているSEILホームルータのWAN側インターフェースにFTTH回線上のDHCP6で割り当てられる/48プレフィックス長のIPv6アドレスを割り当てて、4RDのためのprefix delegationを実施できる構成に設定した。

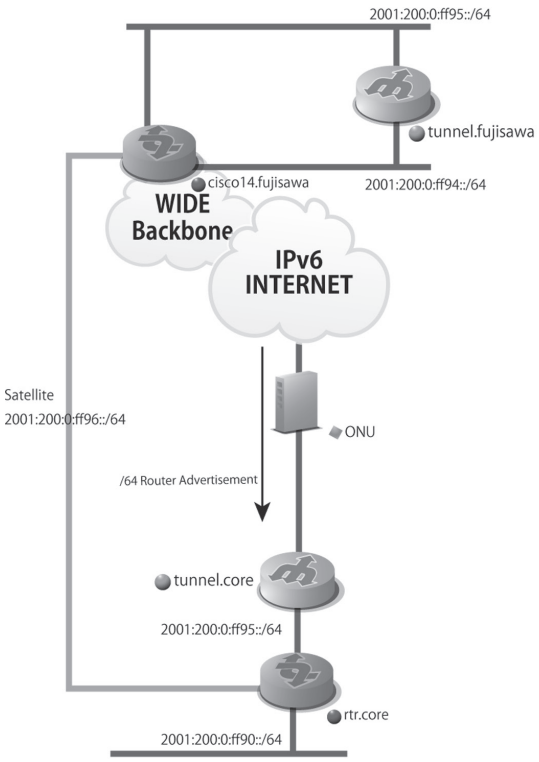
また、WIDEプロジェクトで運用管理するIPv6アドレスブロックを合宿ネットワークで利用するために、松代ロイヤルホテルと慶応SFCの間を結ぶL2TPトンネルをFTTH回線上に構築した。L2TPゲートウェイはLinux Debian squeeze (kernel 2.6.32) で構築したサーバ上にNOCの一人である上野が作成したIPv6用L2TP実装(v6tun [14])を用いた。筑波大学で開発されているオープンソースVPNソフトウェアであるut-vpn [15]と比較した事前検証では、v6tunはTCPで719Mbps、UDPで738Mbpsのスループットを記録し、他方、ut-vpn [15]はTCPで428Mbps、UDPで410Mbpsのスループットであったため、L2TPとしてv6tunを採用した。

### 3.3 NAT64/DNS64

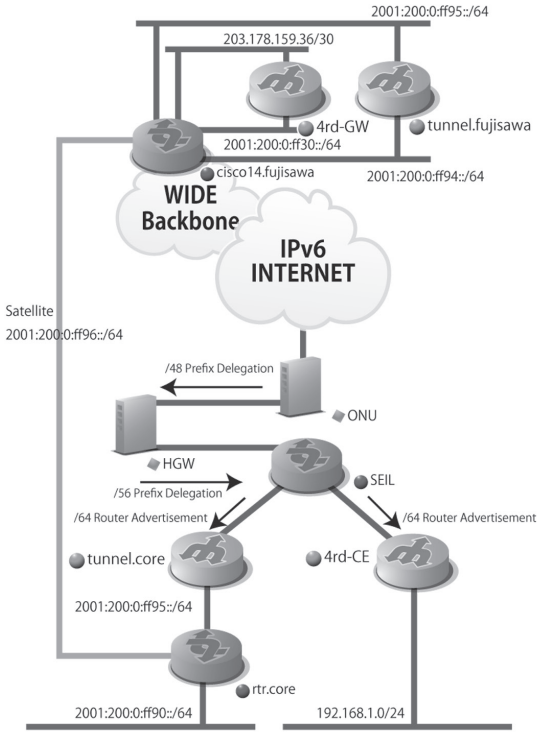
今回のcamp-netではユーザへのIPv6アドレス割り当てをISC DHCP6実装[16]を用いて提供した。一方、多くのネットワークがWorld IPv6 dayを経験した後でもIPv6に未対応であるため、6to4アドレス変換技術をcamp-netのIPv6 only接続性実験に組み入れることとした。そこで、camp-netの要求を満たす、2011年9月現在で構築可能な最良のNAT64 [17,18]とDNS64 [19]を用いた6to40アドレス変換の実装を検証した。

NOCチームのNAT64およびDNS64への技術要求事項は次のとおりである。

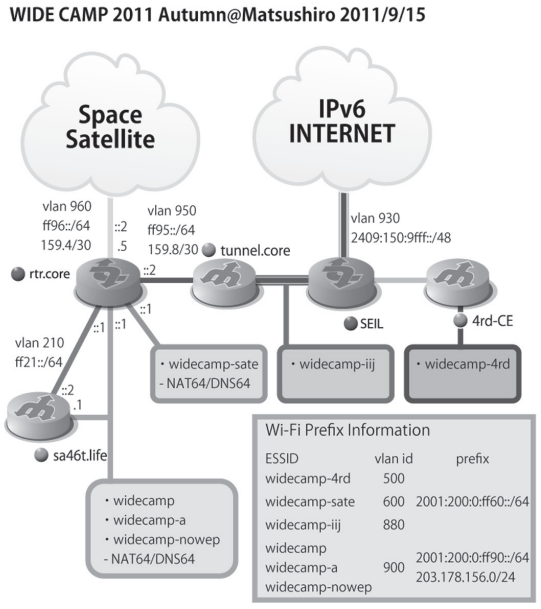
- 実装はオープンソースソフトウェアであること
  理由は、何らかのトラブルが発生した場合にデバッグがNOCチームによって行えるようにするためである。




(a) 合宿ネットワークバックボーン構成（9月6日午後8時まで）




(b) 合宿ネットワークバックボーン構成（9月6日午後8時以降）




(c) 合宿ネットワークアクセス周りの構成

図3.1　合宿ネットワークの構成

- 正常に動作するDNS64実装であること
  理由は、正常に動作しない実装をサービスに用いることはできないためである。
- 正常に動作するNAT64実装であること
  DNS64と同様に正常に動作しないNAT64実装をサービスに用いることはできないためである。特に変換によってペイロードを破壊しない事が必須である。
- 他のNAT44とのカスケード接続を利用しないこと
  理由としては、NAT64のみの不具合を正しく把握し、カスケード接続によって生じる可能性のあるトラブルを回避するためである。

DNS64とNAT64の実装の評価はプレホットステージ期間である7月1日から開始した。まず、DNS64の実装に関する評価について説明する。評価対象としたDNS64の実装はISC bind 9.8 p4 [20]、NLnet labs unbound [21]およびViagénie ecdysis [22]の3種類を検証した。このうち、2011年7月の段階で正常に動作したのはbindのみであったため、camp-netで用いる実装としてbindを採用した。

次にNAT64の実装に対する評価について説明する。評価したNAT64の実装はlinuxnat64 [23]、tayga [24]およびecdysis [22]の3種類である。

linuxnat64とecdysisはステートフルNAT64 [18]の実装であり、一方、taygaはステートレスNAT64 [17]の実装である。評価の結果、camp-netではlinuxnat64を採用した。採用した理由は、まず、taygaのステートレスNAT64は収容するユーザ数だけIPv4アドレスを必要とするが、NAT44のカスケードを利用しないという要求事項と、camp-netで参加者全員を収容できるほど十分なグローバルIPv4アドレスを保持していないことから、検討段階でtaygaステートレスNAT64は要求事項を満たせなかった。次に、linuxnat64とecdysisを実際に動作させて評価したところ、2011年7月の段階では、ecdysisの実装ではTCPペイロードを破壊する挙動が確認されたため、特に不具合もなく正常に動作したlinuxnat64をcamp-netでは採用した。bindとlinuxnat64の設定例は8章に付録として記載しておく。

### 3.4 IPv4 over IPv6カプセル化技術

6to4アドレス変換とは別に、camp-netではIPv6未対応のOSやアプリケーションを利用する参加者のために、464カプセル化技術の検討も行った。camp-net NOCが公式サービスとして用意する464カプセル化技術としてはSA46T [25 ～ 28]のソフトウェア実装を採用した。このSA46Tソフトウェア実装は慶應義塾大学と富士通との共同研究で研究開発され、過去のWIDE合宿での実験や

表3.1　無線LAN 設定と接続性、アドレス変換技術の一覧

| ESSID | Accounting | Channel | Address version | Address scope | DNS | Address allocation | Trans. / Encap. |
|---|---|---|---|---|---|---|---|
| widecamp | WPA2 EAP-TLS | 11b/g/n | v6 | global | DNS64 | DHCP6 (automatic) | NAT64 |
| | | | v4 | global | DNS64 | DHCP4 (registration) | SA46T |
| widecamp-a | WPA2 EAP-TLS | 11a | v6 | global | DNS64 | DHCP6 (automatic) | NAT64 |
| | | | v4 | global | DNS64 | DHCP4 (registration) | SA46T |
| widecamp-sat | WPA2 EAP-TLS | 11b/g/n | v6 | global | DNS64 | DHCP6 (automatic) | NAT64 |
| | | | v4 | N/A | N/A | N/A | N/A |
| widecamp-nowep (hidden) | MAC addr. Auth. | 11b/g/n | v6 | global | DNS64 | DHCP6 (automatic) | NAT64 |
| | | | v4 | global | DNS64 | DHCP4 (registration) | SA46T |
| widecamp-iij | WPA2 EAP-TLS | 11b/g/n | v6 | global | N/A | RA from SEIL (automatic) | N/A |
| | | | v4 | N/A | N/A | N/A | 4RD |
| widecamp-4rd | WPA2 EAP-TLS | 11b/g/n | v6 | global | N/A | RA from SEIL (automatic) | N/A |
| | | | v4 | private | Proxy resolver | DHCP4 from SEIL (automatic) | 4RD |

JGN-XとThaiSARNとの間でのビデオストリームを用いた検証[29]などによって実績があるため採用した。

また、追加実験として4RD [30]の検証も実施した。4RD検証実験は慶應義塾大学、NTT東日本、インターネットマルチフィードおよびIIJによって構成された4RD検証チームから9月1日に急遽提案され、camp-netでこの実験を受け入れたことによって実施が決まった。4RD検証実験ではIIJが開発しているSEILホームルータ上での4RD実装を4RD-CE（4RD Customer Edge Router）として合宿地に設置し、vyattaの4RD実装[31]を4RD-BR（4RD Boarder Router）としてWIDEバックボーン藤沢NOC内に設置した。4RD-CEでIPv6パケットにカプセリングされたIPv4パケットはNTT東日本のフレッツ網からインターネットマルチフィードのバックボーンを経由してIIJのIPv6網に入り、そこからWIDEバックボーンにルーティングされ4RD-BRでIPv4パケットに戻されることになる。

### 3.5 WiFiアクセスとアドレス割り当て

ユーザアクセス周りのトポロジーは図3.1（c）に示すような構成とした。また、表3.1では図3.1（c）に対応した無線LANのチャネル、認証方式、VLAN、利用IPアドレスタイプ、IPアドレスの割り当て方、アドレス変換方式の一覧である。基本的に、無線LANアクセスはWIDE個人証明書を用いたWPA2 EAP-TLSにより提供した。WIDE個人証明書を用いたWPA2 EAP-TLSによる無線LANアクセス認証は2008年3月合宿からcamp-net NOCにより継続して行われている実験である。また、ESSID widecamp-nowepを、WPA2 EAP-TLSが行えないデバイスや個人証明書をインストールし忘れたユーザのためのバックアップとして隠しESSIDに設定して用意した。ESSID widecamp-nowepでの認証は文献[32]で説明されているradiusを用いたMACアドレスと接続APの対応によるレイヤ2レベルの認証（アカウンティング）により行った。IPアドレス自動割り当てと名前解決用のリゾルバの自動設定はISC DHCP実装[16]を用いてDHCP4とDHCP6を提供した。ただし、ESSID widecamp-4rdでは4RD-CEとして動作しているSEILホームルータがRA、NAT44、DHCP4およびname proxyとして動作しているため、SEILホームルータによってIPアドレスと名前解決用のリゾルバの自動設定を行った。

### 3.6 物理機材およびクラウド資源の活用

松代ロイヤルホテルでの設営作業を省力化するために、2011年9月合宿ではほとんどのサーバをクラウド環境に構築した。利用したクラウド環境は、StarBED [33]上のCISCO UCSサーバを6台とWIDE藤沢NOCに設置したWIDE Cloud Controller（WCC）[34]のクローンサーバを用いて構築した。藤沢のWCCサーバはクラウド環境のコントローラおよびNFSサーバとして利用し、StarBED上のサーバは仮想マシンを配置するスレイブノードとして利用した。仮想マシンとしてはqemu-kvm 0.14.1、Linux Kernel 3.0.4を用い、libvirt 0.9.4を用いて仮想マシンの操作を行った。また、StarBEDと藤沢のWCCサーバ間はWIDEバックボーン上に広域VLANを設定して同一L2セグメントに収容できるようにした。詳細は、第4部「クラウドコンピューティング基盤の構築と運用」や第28部「大規模な仮設ネットワークテストベッドの設計・構築とその運用」を参照してほしい。

## 第４章　実験

本章では、実験結果について報告する。前節までで述べたようにcamp-netでは「WPA2 EAP-TLSによるアクセス認証の検証」、「NAT64/DNS64によるIPv6 onlyアクセス環境の検証」、「SA46Tによる464カプセル化の検証」、「4RDによる464カプセル化の検証」の4つの実験が行われた。

### 4.1 実験概要とタイムライン

表4.1は合宿期間中に発生したイベントのタイムラインを示す。「WPA2 EAP-TLSによるアクセス認証の検証」と「NAT64/DNS64によるIPv6 onlyアクセス環境の検証」は9月6日の午前10時から開始した。初日（9月6日）の段階では、widecamp-nowepおよびSA46Tを通したIPv4グローバルアドレスによるアクセスを行うためのMACアドレス登録ページは隠した状態で、IPv6のみのアクセス環境を参加者に強制的に利用させるようにした。WIDE個人証明書の入れ忘れなどでIPv4アドレスで構築された社内網にアクセスしなければならないと言ったIPv4アドレスが必要な参加者には、NOCにヘルプデスクを用意し個別対応を行った。

表4.1　Time line of experiments

| Date | Events |
|---|---|
| 2:00 PM, Sep. 5th | 設営開始 |
| 4:00 PM, Sep. 5th | FTTH 回線上への IPv6 L2TP トンネルの設定終了 |
| 4:50 PM, Sep. 5th | 衛星回線の設定終了 |
| 3:00 AM, Sep. 6th | DHCP ヘルパーの動作不良（チェックサムエラー）を特定、camp-net トポロジーから削除 |
| 9:00 AM, Sep. 6th | 衛星回線の動作検証終了 |
| 10:00 AM, Sep. 6th | started the WPA2 EAP-TLS の検証と DNS64/NAT64 による IPv6 only アクセス環境の検証を開始 |
| 8:00 PM, Sep. 6th | 4RD 検証実験のための FTTH 回線の設定変更を開始 |
| 9:00 PM, Sep. 6th | 4RD 検証実験のための FTTH 回線の設定変更が終了 |
| 10:00 PM, Sep. 6th | 4RD 検証実験のための設定終了と NOC チームでの事前検証開始 |
| 1:30 PM, Sep. 7th | SA46T による IPv4 アクセス環境用の MAC アドレス登録ページを開設し、SA46T による IPv4 アクセス環境を参加者に解放 |
| 3:15 PM, Sep. 7th | 合宿参加者を交えた 4RD 検証実験の開始 |
| 4:15 PM, Sep. 7th | fixed the mis-configuration of firewall on MAC アドレス登録ウェブサーバ上の firewall の設定ミスを特定し、修正 |
| 5:47 PM, Sep. 7th | radius サーバの設定ミスを特定し、修正 |
| 10:00 PM, Sep. 7th | ほぼすべての参加者が WPA2 EAP-TLS または widecamp-nowep で ESSID のいづれかに接続し、検証実験に参加できる状態になったことを確認 |
| 1:42 PM, Sep. 8th | DNS64 サーバ上で DNSSEC を有効にする |
| 4:30 PM, Sep. 8th | 有志による SA46T および 4RD のパフォーマンス測定開始 |
| 5:30 PM, Sep. 8th | ns.wide 上の設定ミス（lame delegation）を特定、修正 |
| 6:00 PM, Sep. 8th | 負荷向上により、DNS64 サーバを WIDE クラウド上から独立した物理サーバへ移行 |
| 8:00 PM, Sep. 8th | 有志による SA46T と 4RD の比較検証開始 |
| 10:00 PM Sep. 8th | FTTH 回線のパフォーマンスチューニングを開始 |
| 11:00 PM Sep. 8th | FTTH 回線のパフォーマンスチューニング終了 |
| 11:00 AM Sep. 9th | camp-net を停止、撤収開始 |
| 2:30 PM Sep. 9th | 撤収終了 |

また、EMOBILEなどの商用モバイルインターネットと個人用WiFiルータを持ちこむ参加者は昨今増えているため、初日はNOCチームでFox Huntingチームを結成し、個人用WiFiルータによるrouge APの取り締まりを実施した。rouge APを用いてIPv4ネットワークにアクセスしていた参加者に対しては、ホテルの宿泊部屋で松代ロイヤルホテルが用意しているIPv4ネットワークを使うか、rouge APとして実験に影響しない程度に会場から遠く離れて利用する、またはNOCのヘルプデスクにて有線で提供しているのSA46T経由のIPv4ネットワークを利用するように促し、できる限りIPv6 onlyアクセス環境の検証実験に参加するように取り組んだ。

表4.1に示すように、9月7日午後1時半にSA46Tによるグローバルipv4アクセスを利用するためのMACアドレス登録ウェブページを開設し、参加者にグローバルIPv4アクセスの利用を開放した。また、9月7日午後3時15分から4RDによるNAT44を介した IPv4アクセスの利用を参加者に開放した。上記のタイムラインから、ほとんどの参加者は少なくとも丸1日はIPv6のみのアクセス環境で会場では過ごしたことになる。

## 4.2　アンケート

ここでは実験に対して参加者に行ったアンケート結果を報告する。アンケート結果はWIDEプロジェクトのメンバーであれば[35]で閲覧することができる。2011年9月合宿参加者は総数153名でそのうち2011年9月17日の午後1時半までにアンケートに回答した参加者は110名、回答率71.9%であった。図4.1は参加者が利用したアクセスネットワークの組み合わせの割合、およびNOCが実施した実験（IPv6 onlyおよびSA46T）に対する回答の集計結果である。一方、図4.2は4RD検証実験に対するアンケートの集計結果である。

図4.1（a）は参加者が利用したアクセスネットワークの組み合わせの割合を集計した結果である。驚くことに30名（19.6%）の参加者が合宿期間中を通してNAT64/DNS64によるアドレス変換を伴うIPv6 onlyのアクセスネットワークだけで生活したと回答した。IPv6とSA46TによるIPv4アクセスネットワークを利用したと申告した参加者は7名いた。解析したところ、初日のWPA2 EAP-TLSの設定またはIPv6 only設定に失敗し、IPv4アドレス利用が開放された段階でSA46TによるIPv4アクセスネットワークに逃げ込んだ参加者が多かった。33名の参加者はIPv6と4RD環境を利用したと申告した。これらのユーザはMACアドレス登録をしてまでIPv4アクセスを利用しようとは思わなかったユーザではないかと推測できる。34名の参加者は全ての組み合わせを試し、その多くは4RDとSA46Tの比較実験に参加した参加者であった。図4.1（c）および図4.1（d）から90名の参加者（58.8%）は今回camp-netで提供したIPv6 onlyアクセスの品質やSA46Tで提供したIPv4ア

クセスの品質に満足したようであった。

SA46Tや4RDなどのIPv4アクセスを利用した主な理由を以下に列挙する。

理由1） 持ってきたPCにWIDE個人証明書を入れ忘れたが、メールサーバがIPv4のみでDNS登録もされていないため、sshでログインするためにIPv4アクセスを利用した。

理由2） 利用しているOS（Windows XPやMacOS X 10.5.8など）でIPv6設定が行えなかった、もしくは設定の仕方がわからずあきらめた。

理由3） Lenovo ThinkPad'の無線LAN設定ではIPv6 onlyの設定がうまく設定できなかったため、IPv4アクセスを利用した。

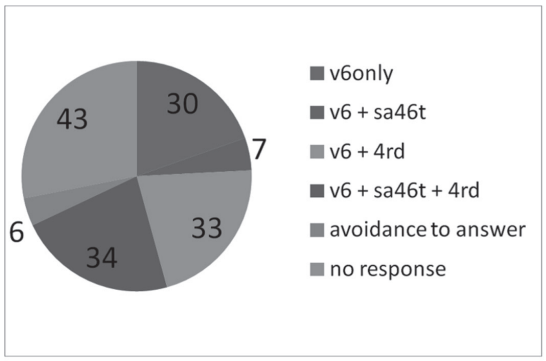
理由4） skypeやwindows live messangerなどのIPv6 only環境に未対応のアプリケーションを仕事で利用するために、IPv4アクセスを利用した。

理由5） IPv4アドレスしか設定されていない会社のVPNサーバ（IPsec VPNまたはPPTP）に接続するために、IPv4アクセスを利用した。

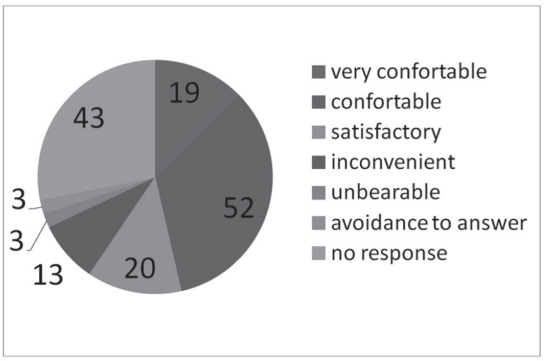
理由6） Andoroid OSでWPA2 EAP-TLSを設定しようとしたが、名前解決をIPv4で行っている挙動を示したのでIPv4アクセスを利用した。

理由7） あるウェブページがAAAAでの名前解決時にServFAILエラーを返し、閲覧できなかったため、IPv4アクセスを利用した。

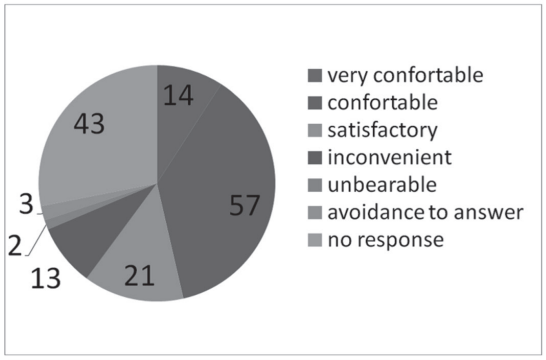
理由8） DNS64の応答速度が遅くなったため、IPv4アクセスを利用した。



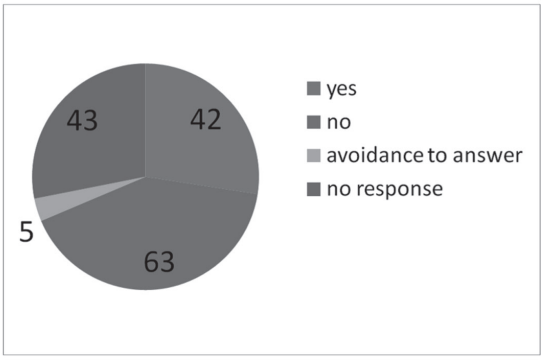

(a) 参加者が利用したと申告したユーザアクセスの割合




(b) Q1: 今回の合宿では主に IPv6 のみを提供しましたがいかがでしたか？




(c) Q2: 今回のネットワークの品質はいかがでしたか？




(d) Q3: SSID:widecamp において IPv4 の認証サービスを使いましたか?

図4.1　NOC による実験のアンケート結果

理由9） VMWareのNATから外部にアクセスできなくなったために、IPv4アクセスを利用した。
理由10）SA46Tと4RDの比較検証実験に参加するためにIPv4アクセスを利用した。

図4.2 (b)、図4.2 (c)、図4.2 (d)、図4.2 (e)および図4.2 (f)は4RD検証結果に対するアンケート結果をまとめたものである。ほとんどの参加者は提供された4RD環境に満足した。しかしながら、一部の参加者から4RD環境での不具合が報告された。報告された不具合に関しては次節4.3に記載する。

## 4.3 報告されたトラブル

本節ではNOCや合宿参加者メーリングリストに報告されたトラブルをまとめる。

### 4.3.1 WPA2 EAP-TLSに関するトラブル

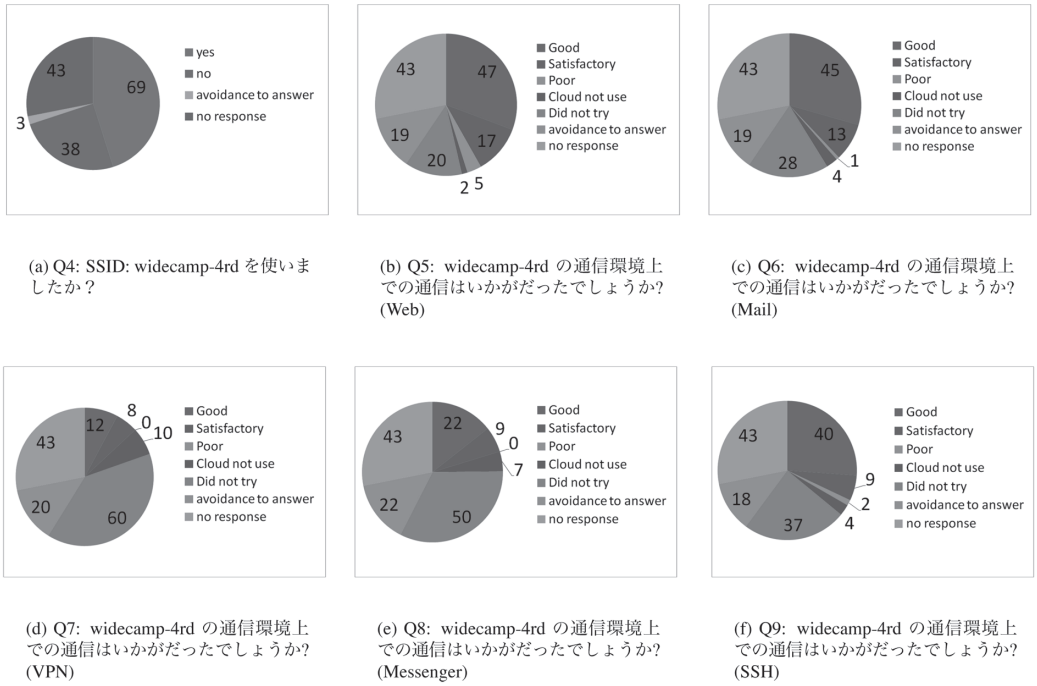
不幸なことに、9月6日から9月7日かけて最も多かったトラブルはWPA2 EAP-TLSに関するトラブルであった。

WPA2 EAP-TLSに関するトラブルで最も多かった項目は「WIDE個人証明書の入れ忘れて来てしまったが、メールサーバがIPv4のみなのでどうしたらよいのか？」という相談であった。NOCヘルプデスクに直接相談に来た参加者にはMACアドレスの登録を手動で行いwidecamp-nowepもしくは有線接続でSA46TによるIPv4アクセスを利用し、NOCのサポートでWPA2 EAP-TLSの設定を行った。しかしながら、NOCヘルプデスクに相談しにくる参加者は少なく、相談しに来なかった参加者は自分の部屋で松代ロイヤルホテルが提供するIPv4アクセスを利用するか、商用モバイルインターネットサービスを使い、rouge APを立ち上げていることをNOCから注意されるという参加者が多かった。

また、9月7日までradiusサーバの設定ミスがあり、認証が不安定であったこともトラブルとして上がった。設定ミスはWIDE mocaワーキンググループの木村泰司氏らの手助けにより、9月7日中に解決された。

### 4.3.2 IPv6対応に関するトラブル

参加者からは次のようなIPv6対応に関するトラブルが報告された。




(a) Q4: SSID: widecamp-4rd を使いましたか？

(b) Q5: widecamp-4rd の通信環境上での通信はいかがだったでしょうか? (Web)

(c) Q6: widecamp-4rd の通信環境上での通信はいかがだったでしょうか? (Mail)

(d) Q7: widecamp-4rd の通信環境上での通信はいかがだったでしょうか? (VPN)

(e) Q8: widecamp-4rd の通信環境上での通信はいかがだったでしょうか? (Messenger)

(f) Q9: widecamp-4rd の通信環境上での通信はいかがだったでしょうか? (SSH)

図4.2 4RD 検証実験のアンケート結果

- フォールバックルーチンが長すぎる
  IPv6 onlyアクセスに接続したほとんどの参加者がこのトラブルを報告した。このトラブルはWindowsユーザやMac OSユーザから多く報告された。このトラブルの原因は、Windows 7やMac OS XではIPv4プロパティが有効になっている場合、接続時にIPv4の対外接続性の確認も行っているためでIPv4接続確認のタイムアウトで1分から2分待たされるためである。NOCチームからの推奨設定として、IPv6 onlyアクセス環境でIPv4を使わない場合はIPv4プロパティを無効にすることをアナウンスした。実際に設定した参加者の多くは「IPv4の設定を無効にするのは衝撃的だが、実際、非常に快適になった。」と回答した。

- DHCP6未対応によるトラブル
  Windows XPやMac OSX 10.6（Snow Leopard）以前のOSではDHCP6に対応していないため、DNSリゾルバの設定の仕方がわからないという参加者が多く存在した。NOCチームでは、DHCP6未対応のOSと手動で設定するDNSサーバのアドレスをアナウンスし、設定方法がわからない参加者はNOCヘルプデスクにて対応した。

  一方で、Windows 7やMac OS 10.7（Lion）を利用していた参加者からはDHCP6やDNSリゾルバ設定に関するトラブル報告はほとんどなかった。例外として、Think Padなどの無線LANアクセス設定アプリケーションを利用していた参加者からは設定がうまく反映されないとの報告を受けた。

- OSでIPv6のみの設定ができないことによるトラブル
  Windows XPやAndroid OS（バージョン2.xのデバイス）ではIPv4プロパティを無効にできない。Windows XPの場合、DNS名前解決でローカルプロキシを127.0.0.1で立ち上げて利用しているためである。Android OSに関しては詳しい原因調査を行えなかったが、参加者からは「おそらく名前解決はIPv4パケットを使っているようだ」という報告が挙げられた。

- GUI、デバイスのIPv6未対応によるトラブル
  いくつかのGUIやハードウェアでIPv6未対応に関連するトラブルが報告された。初期型のMac Book AirでSnow Leopardを用いていた参加者から、GUIで設定したDNS64の設定がいつの間にか消えてしまうというトラブルが報告された。NOCで調査したところ、“sudo networksetup-setdnsservers” AirPort”2001:200:0:ff80::5”をコマンドラインから実行すると設定が消えない事が判明したため、これを回避方法として指定した。また、参加者が持ち込んだApple社のUSBイーサネットアダプタはIPv6に未対応であることや、古いデバイス・古いOSを利用している参加者からデバイスドライバの再インストールを頻繁に行ったという報告を受けた。

#### 4.3.3 アプリケーションに関するトラブル

ここでは、参加者から報告された、特定のアプリケーションに関するトラブルを記載する。

- アプリケーションのIPv6未対応に関するトラブル
  Arkkoがインターネットドラフト[36]で指摘しているように、インスタントメッセンジャーやVoIPアプリケーションの多くはやはりIPv6未対応のものが多く、利用できなかった。

  また、CVSNTやNOD32のウィルスデータベースアップデートなど、おそらくIPv4ソケットしか利用していないWindows上のアプリケーションがいくつか確認された。

  Mac OSXでは、Cocoaフレームワークで実装されたアプリケーションはIPv6 only環境で動作し、Cocoaフレームワークを利用していないアプリケーションの多くはIPv6 only環境で利用できないとの報告を参加者から受けた。

  また、HTTPベース、XMPPベースのアプリケーションの多くは利用できた。利用できないHTTPベース、XMPPベースのアプリケーションはサーバへのアクセスに対しIPv4アドレス表記をアプリケーション内で埋め込まれているようであった。

- MTUブラックホールによるトラブル
  Path MTUディスカバリが正常に動作しないことに起因するMTUサイズの不整合でパケットが破棄される問題をMTUブラックホールと一般的に呼称する。このMTUブラックホールに関するトラブルもいくつか発生した。

  まず、9月5日の設営時にWIDEクラウド上を経由するパケットが軒並み破棄されるというトラブルに遭遇した。これはWIDEクラウドのMTUサイズが9000に設定されていることによるもので、MTUサイズを1500に設定することで回避した。

  次に、UDPを用いたアプリケーションでL2TP上を経由しているパケットでMTUブラックホールと思われるトラブルが参加者から報告された。残念ながらNOCチームではこのトラブルの原因を合宿中に解析できなかった。

- アドレス・プロトコル変換へプロトコル仕様上対応していないことによるトラブル
  Open VPNやApple Mobile Me IPSec/PKIベースの通信などIPSecを用いているアプリケーションはその仕様上NAT64/DNS64のアドレス変換には対応できない。そのため、多くの参加者からIPv6 onlyアクセス環境で会社へのVPNが利用できないというトラブルの報告を受けた。また、4RDの環境でも、ある参加者からApple Mobile Me IPSec/PKIベースの通信が行えないというトラブルの報告を受けた。こちらの原因特定は残念ながら期間中に実施できなかった。

#### 4.3.4 名前解決に関するトラブル

ここでは名前解決に関するトラブルを報告する。

- IPv4アドレス表記に関連するトラブル
  Arkkoのインターネットドラフト[36]でも指摘されているように、多くの参加者からIPv6 onlyアクセス環境からIPv4サーバに対しIPv4アドレス表記で通信できないというトラブルの報告が挙げられた。これは、IPv4アドレス表記を用いると、たとえgetaddrinfoのようなIPv6対応ソケットを用いたとしても、NAT64/DNS64の仕様上、DNS64により指定されたIPv6 mapped IPv4アドレスでユーザ側のソケットを作成しないためである。HTTP、SSH、IMAP、SMTP、POPFileなどのアプリケーションの設定で指定するサーバをIPv4表記で書いていたり、サーバのアドレスがIPv4表記で組み込まれていたりする場合に発生する。設定変更できるものに関しては、対象となるIPv4アドレスをDNSに登録したうえで、アプリケーション側の設定をFQDNで設定すれば動作するが、参加者の多くがDNS管理者ではないため、DNSに登録されていないIPv4アドレスに対応できないケースが散見された。

  また、VNC、PPTP、IPSecなどのアプリケーションはこのIPv4アドレス表記による問題とともに、プロトコル仕様上の問題やMTUブラックホールの問題も重なり、切り分けが非常に困難であった。

- AAAA逆引きが設定されていないことによるトラブル
  ホットステージ期間中の検証で、一部の商用ウェブサービスがAAAAの逆引きを要求してくることが明らかとなった。そのため、NOCチームではcamp.wide.ad.jpドメインで利用する全てのIPv6アドレスに対し逆引きを設定した。

- lame delegationによるトラブル
  合宿期間中に、ある参加者から一部の商用ウェブサービスがAAAAの逆引きを要求してきているが逆引きができていないという指摘を受けた。NOCチームで調査した結果、camp.wide.ad.jpドメインの上位ドメインであるwide.ad.jpドメインを管理するns.wide.ad.jp上の設定ミスでlame delegationが発生していることが明らかとなった。設定ミスを修正することでこの問題は解消された。

- DNS64の負荷による応答速度劣化によるトラブル
  DNSSECをDNS64サーバで有効にしたあと、DNSSECの検証や参加者のアクセス増加によりDNS64の負荷が向上し応答速度劣化によるトラブルが発生した。当初DNS64はWIDEクラウド上の仮想マシンとして動作させていたが、急遽独立した物理サーバとして再構

築し、負荷の解消を行った。物理サーバに移行した後は、特に負荷による応答速度の劣化は生じなかった。

- 不適切なAAAA応答を返す権威サーバに関連するトラブル
  合宿期間中、一部のウェブページでNAT64/DNS64で名前解決が失敗し閲覧できないというトラブルが多くの参加者から報告された。この現象は国内外問わず、航空券・ホテル検索ページで頻繁に発生していた。NOCチームと有志により解析したところ、この原因はRFC4074[37]で指摘されているIPv6移行期に発生する可能性のある不適切なAAAA応答を返す権威サーバによりDNS64がAAAAレコードの問い合わせからAレコードの問い合わせにフォールバックせずにエラーコードをクライアントに返してしまう現象により発生していることが明らかとなった。エラーとしてはRFC4074[37]の4.2節で述べられている“Return Name Error”、4.3節で述べられている“Return Other Erroneous Codes”、4.4節で述べられている“Return a Broken Response”を実際に観測した。これらのエラーは権威サーバの実装に起因するものなのでNOCチーム側では解決できないトラブルであった。

# 第5章　考察

## 5.1　IPv6環境への移行における提言

ここでは、合宿ネットワークでの実験で得た知見を通した、NOCチームからのIPv6環境への移行における提言を記載する。

- IPv6対応が可能であれば外部からアクセスのあるサーバはIPv6対応すべきである
  理由としては、今回の実験からNATやNAPTを挟んだ環境では容易にMTUブラックホール問題やスループット低下など、様々な問題が生じ、切り分けが難しいため、デュアルスタックなどでIPv6対応できるのであれば、今のうちに対応してしまうのが得策である。
- 最新バージョンのOSに移行すべきである
  理由としては、Window 7やMac OSX 10.7（Lion）からのトラブル報告はほとんどなく、一方で古いバージョンのOSを利用した参加者からは様々なトラブルの報告を受けたため、運用コスト上は最新バージョンのOSに移行したほうがよい。
- AAAAの逆引き設定をすべきである
  理由はAAAAの逆引きを認証に利用する商用ウェブサービスが存在するためである。
- DNSサーバやウェブアプライアンスのDNS応答がRFCに則っているか否かの検証をしたほうがよい
  理由としては、不適切なDNS応答はクライアント側では対応できないためである。RFCに則った応答を返せばウェブサービスがIPv6対応していなくてもDNS64/NAT64のアドレス変換によってIPv6 onlyネットワークからもウェブサービスを利用できる。
- MTUサイズに注意を払う
  理由はPath MTUディスカバリが動作しないことが多いためである。

## 5.2　研究課題

ここでは、今後の研究課題として広く議論しなければいけない項目を述べる。

### 5.2.1　PMTUD、MTUブラックホール問題

今回の実験ではMTUブラックホール問題はさまざま個所で発生した。主原因はPath MTUディスカバリが運用上の理由やアドレス変換・カプセリングが挟まった段階で正常に動作しないことに起因している。一方でVPNなどの多くのトンネル・カプセル化技術ではPMTUDが正常に動作していることを前提に実装されているものが多い。

可能性のある解決方法としては、RFC規約違反であるが、DF bitが設定されていてもルータやVPNゲートウェイでフラグメントを行うように実装することが考えられる。また、MTUブラックホールが発生している個所を効率よく特性する手法が現在確立していないこともあり、そのような検証ツールの研究開発も必要である。

### 5.2.2 RFC4074で指摘されている不適切なDNS応答

4.3.4節で説明したように、RFC4074[37]で指摘されている不適切なDNS応答にどのように対応するかも研究課題の一つである。理想的には全てのDNSリゾルバ実装がRFCに則った実装に改修されることであるが、非常にコストが高い。

可能性のある解決方法としては、DNS64のフォールバックの仕様を次のように変更することである。

- NXDOMAINやServFailがAAAA応答で返されてもA要求を出すようにDNS64の仕様を変更する。
- DNS64側でアクセスされる可能性のあるAレコードをあらかじめ探索しキャッシュしておく。DNS応答がNOERRORの場合、DNS64リゾルバはAAAA要求を発行する。仮にAAAAレコードが存在すればDNS64リゾルバはクライアントに対しAAAAレコードを返し、そうでなければキャッシュされているAレコードを返す。

### 5.2.3 プロトコル仕様上変換できないプロトコルに対するアドレス変換

IPSecやFTPなど、いくつかのプロトコルは、その仕様上IPv4/IPv6変換が行えない。しかしながら、これらの問題はサーバ側がIPv6対応すれば簡単に解決する問題なので、無理に変換する仕様を研究したりRFCで標準化する必要はない。

## 第6章 おわりに

ここでは、2011年9月WIDE合宿にて実施したIPv6 onlyアクセス環境の検証実験に関して報告した。検証結果はAWFIT2011[38]での発表論文ややIETF 82 TAIPEI[39]でのインターネットドラフトで文書としてまとめ発表し、Global IPv6 summit TAIPEIやInter-net WeekのBoFで口頭発表を行った。発表した結果、WIDEプロジェクト内外から追検証を行ってほしいという要望が多く上がったため、2012年3月WIDE合宿で“Life with IPv6ワークショップ”としてワークショップを開催し、より工学的な観点から2011年9月WIDE合宿で実施した実験の追検証を実施する運びとなった。2012年3月WIDE合宿での“Life with IPv6ワークショップ”における検証結果は来年度のWIDE報告書や国内外の会議、標準化会議などで発表したい。

## 第7章 謝辞

WIDEプロジェクト2011年9月合宿に参加し実験にご協力頂いた全ての参加者、および実験環境の一部としてStarBED3・JGN-Xの環境から資源提供していただいた情報通信研究機構テストベッド研究開発推進センターおよび北陸StarBED技術センターに感謝の意をここに示す。

## 第8章 付録：ISC bind 9.8とlinuxnat64を用いたDNS64/NAT64の設定例

ここでは、付録として、camp-netにおけるISC bind 9.8とlinuxnat64を用いたDNS64/NAT64の設定例を記載する。英語による設定例は文献[40]を参照していただきたい。

camp-netではLinux Debian squeeze（kernel 2.6.32）64bitを用いて構築した。以下、Linux Debian squeeze（kernel 2.6.32）64bitでの設定である。

### 8.1 NAT64 implementation（linuxnat64）の入手

http://sourceforge.jp/projects/sfnet_linuxnat64/から図8.1に示すコマンドで入手できる。

### 8.2 linuxnat64のコンパイル

図8.2に示すように、linux kernel sourceをapt-getコマンドで入手し、次にlinuxnat64の作業ディレクトリに移りmakeコマンドでコンパイルを実行する。

### 8.3 linuxnat46の設定

まずIPv6およびIPv4 prefixを単一の物理インターフェース（例えばeth0）に設定する。camp-netではロードバラン

スを行うためnat64を3台用意した。ここでは、3台のうちの一つを例として記載する。NAT64の物理インターフェース(eth0)には以下のアドレスを割り当てた。

```
2001:200:0:ff81::37/64
203.178.158.37/26
```

次にDNS64がA応答で入手したIPv4アドレスをIPv6アドレスに格納してユーザに通知するために使われるアドレス変換用のプレフィックスを用意する。camp-netでは次のプレフィックスををアドレス変換用プレフィックスとして用いた。

```
2001:200:0:ff99::/96
203.178.159.24/30
```

そして、図8.3に示すようにlinuxnat64のカーネルモジュールを起動し、仮想インターフェース(nat64)にnext hopの設定を設定する。

```
#git clone git://linuxnat64.git.sourceforge.net/gitroot/linuxnat64/linuxnat64
```

図8.1　gitによるlinuxnat64の入手

```
#apt-get install linux-headers-'uname -r'

#cd <your_working_dir>/linuxnat64/modules/

#make
```

図8.2　linuxnat64のコンパイル

```
# insmod /path/to/nat64.ko ipv4_address=203.178.159.25 \
  prefix_address=2001:200:0:ff99::
# ip link set nat64 up
# ip -6 route add 2001:200:0:ff99::/96 dev nat64
# ip route add 203.178.159.24/30 dev nat64
```

図8.3　linuxnat64の起動と設定

```
ipv6 route 2001:200:0:FF99::/96 2001:200:0:FF81::37
ip route 203.178.159.24 255.255.255.252 203.178.158.37
```

図8.4　ciscoルータでのNAT64へのスタティック経路の設定

最後に、バックボーンルータ（ここではciscoルータ）に図8.4に示すような形式でアドレス変換プレフィックスをNAT64へ向けるスタティックルートの設定を投入する。この設定はrc.local等に記載して再起動時に自動的に設定されるようにしておく。

### 8.4 ISC bind の入手とコンパイル

bind 9.8以降のソースコードを入手し、bindのマニュアルに沿ってコンパイルする。aptから入手できるbindのバージョンが9.8以降であればaptでバイナリを入手しても構わない。

### 8.5 bindの設定

まず、bindのマニュアルに沿って設定ファイルを作成する。次に、named.confに次の設定を追加する。dns64の次に記入しているIPv6アドレスプレフィックスはアドレス変換用アドレスプレフィックスである。設定するネットワーク環境に合わせて変更して欲しい。

```
dns64 2001:200:0:ff99::/96 {

clients { any; };
mapped { any; };
suffix ::;
recursive-only yes;

};
```

そして、named-checkconfコマンドでnamed.confのsyntax errorを確認する。syntax errorがないことが確認できたらrndcによってbindの再起動を行う。再起動後、動作確認を行う。DNS64をリゾルバとして設定し、適当なIPv4アドレスのみ設定されたサーバのURLを名前解決した結果がアドレス変換プレフィックスのIPv6アドレスで返されると成功である。上記の設定の場合、2001:200:0:ff99::xxxx:yyyyが返されることになる。名前解決によって返されたアドレスに対しping6で応答が返ってきた場合、NAT64も動作している事が確認できる。