2 アドホック・ネットワーク構築技術
—外部との接続—

大江将史* 藤澤慎一** 染川隆司***
藤枝俊輔**** 三屋光史朗*****

ここ数年の情報化の流れは，インターネットの発展に支えられているといっても過言ではない．そしてインターネットは，社会基盤の1つとして認知されるようになり，見本市，国際会議といったイベント会場において，各種相互実験や検証を行うために，インターネットへ接続するといった形態のアドホックなネットワーク構築を行う場合がある．

このようなアドホック・ネットワークを運用する場合には，通常のインターネット運用とは異なり，その規模や，実験の内容に依存したノウハウを必要とする．

WIDEプロジェクトが年2回行っている研究会合宿では，その会場を「あるインターネットへ接続した組織」とし，その参加者を「利用者」と仮定し，アドホック・ネットワークを構築し，そのネットワーク上で，IPv6やマルチキャスト，QoSといった次のインターネットに求められている技術の相互運用や検証を行っている．

本稿では，この合宿における運用経験の中から，次世代のインターネットプロトコルとしてのIPv6と現在のインターネットプロトコルであるIPv4の相互運用を目的としたアドホック・ネットワークを運用において，衛星回線を利用したインターネットへの接続，IPv4/IPv6のDNS，IPv4 NAT，およびIPv6/IPv4の相互接続性を実現するトランスレータといった，「外部との接続に必要な技術」について，その技術の役割とネットワークでのデザイン，効果・影響，運用について述べる．

アドホックネットワークにおける外部との接続

ここ数年の情報化の流れは，インターネットの発展を支えてきたといっても過言ではない．そして，見本市，国際会議といったイベントにおいては，すでにインターネットへの接続が不可欠といってもよい状況になっている．また，災害時に，被災地をインターネットと接続し，被災者との通信媒体として，インターネットを利用する試みも研究が進められている．このような一時的にインターネットに接続されたネットワークを「アドホック・ネットワーク」と呼ぶ．アドホック・ネットワークは，国際会議のような場でのインターネットへの接続点の提供や，見本市会場でのネットワーク機器間での相互運用性の検証といった目的に応じて，設計・構築・運用がされる．

* 奈良先端科学技術大学院大学情報科学研究科 masa@fumi.org
** 横河電機（株）ITシス技術開発部 Shin-ichi_Fujisawa@yokogawa.co.jp
*** 奈良先端科学技術大学院大学情報科学研究科 ryuji-so@is.aist-nara.ac.jp
**** 慶應義塾大学環境情報学部 sirokuma@sfc.wide.ad.jp
***** 慶應義塾大学環境情報学部 mitsuya@sfc.wide.ad.jp

WIDEプロジェクトでは，春・秋の年2回の合宿において，IPv6やマルチキャスト，QoSといった次のインターネットに求められている技術の相互運用を目的とした，アドホック・ネットワークを構築し，このネットワーク上で，さまざまな実験を行い，成果を挙げている．

今回は，WIDE合宿のアドホック・ネットワークを例にして，「外部との接続に必要な技術」を中心に述べていきたいと思う．

■外部への接続の重要性

WIDE合宿では，会場内にネットワークを敷設し，かつ，インターネットへの常時接続を行っている．単に電子メールの受送信や，WWWブラウジングを行う場合であれば，参加者が，電話回線やPHS，携帯電話などを利用し，インターネットに接続すればよいし，そのために，主催者は，会場内に電話回線を設置すればよいだろう．

しかし，我々WIDEプロジェクトは，インターネットの研究者のコミュニティであり，研究者たちが，一堂に会する年2回の合宿では，200名以上の参加者が利用するネットワークを運用する機会がある．そこでは，合宿

ネットワークを「インターネットに接続されたある組織」と仮定し，このネットワーク上で，IPv6やマルチキャスト，QoSといった，次のインターネットに求められている技術の検証を，合宿参加者自らが利用することにより，実践的実験・検証を行う．そのためには，合宿ネットワークをインターネットへ接続し，「活きた」ネットワークにすることが，必要不可欠である．

■対外線の種類とその確保

合宿会場内のネットワークをインターネットに接続するには，合宿地とインターネット間を通信インフラを介して接続しなければならない．我々は，この合宿外部へ接続するための通信メディアを「対外線」と定義している．WIDE合宿においては，合宿地とWNOC（WIDE Network Operation Center; WIDEが運用するインターネットの接続点）間をつなぐ対外線として，次に示す通信インフラを利用する．

- **衛星回線**

静止軌道上にある通信衛星（CS）を経由し，日本国内の任意の2点間を接続する．我々は，Kuバンドの可搬局（75cmのパラボラアンテナと衛星モデムで構成，**図-1**）を利用し，合宿地-WNOC間を（株）JSATのJCSAT経由で接続している．

このメディアは，衛星を捕らえることができれば，災害などで，通信インフラに大きな障害があっても利用することが可能である．しかし，静止衛星を利用するため一定の遅延があり，また，Kuバンドを利用しているため，強い降雨時には，減衰による通信障害が発生する．回線速度は，アンテナの大きさや，衛星モデムの性能に依存するが，両方向で2Mbps程度である．

- **専用線**

通信キャリアから提供される定額のディジタル専用線で，大学や企業間を接続する際に利用するものと同様のサービスを，臨時という形で契約し利用する．NTTの場合は，256Kbps～384Kbpsくらいまでは，メタルで接続され，それ以上の場合は，光ファイバになる．回線速度は64Kbpsから選択地域によっては，サービス内容が制約される場合がある．

- **無線**

無線や赤外線をメディアとして利用して，ネットワークをブリッジ接続する．目視距離程度（～6km）の建物間のネットワークを接続する際に利用する．

- ISDN

回線費は，利用時間と距離に応じた従量制であるので，ネットワークの規模や，実験内容に合わせて利用する．また，他の対外線で通信不能になった場合の対応策として準備する．

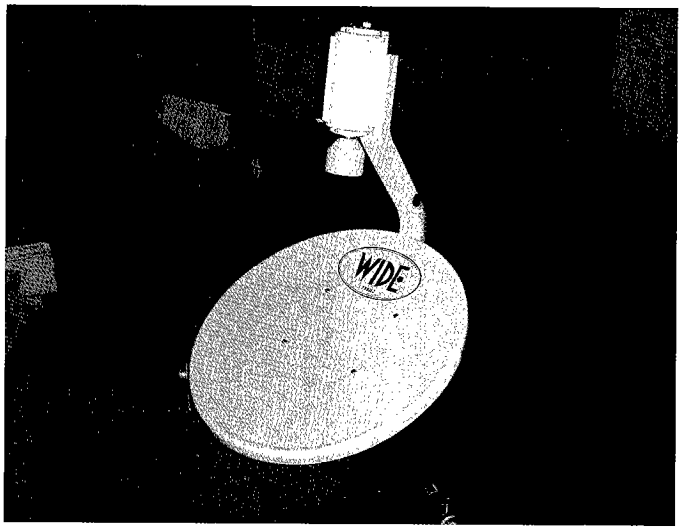

図-1　75cmのパラボラアンテナ

WIDE合宿では，これらのメディアを実験の内容に合わせて，利用する．たとえば，1999年秋の合宿では，実験の1つとして；複数の物理メディアを1つの論理的回線として扱う実験を行った．このために，合宿地とWNOC-SFC（WIDE SFC NOC; 慶應義塾大学湘南藤沢キャンパス）間に3本の128Kbpsのディジタル専用線と衛星回線を用意した．また，IPv6対応ISDNルータの検証を行うためのISDN回線も用意した．

2000年春合宿では，IPv6のルーティングプロトコルの検証のために2カ所のWNOCへの接続が必要となった．このため，JGN（Japan Gigabit Network）山梨NOCとの間にT1（1.5Mbps）ディジタル専用線を用意し，WNOC-SFC・WNOC-NARA（WIDE NARA NOC; 奈良先端科学技術大学院大学）と合宿地間でATMを利用した論理的な接続を行った．

以上に示すように，実験の内容や，利用できるメディアに合わせて，最適な対外線運用を計画し，準備を行う．

■IPv4/IPv6/NATを考慮したDNS

臨時にインターネットに接続したネットワークであっても，DNS（Domain Name System）サーバの運用は，必要である．その理由として次のことが挙げられる．

- **対外線へのDNSトラフィックの抑制**

貴重な対外線帯域を会場内からの外部へのDNS問合せで消費するのは非効率

- **メンテナンス性**

合宿地内においても，WWWによる情報提供やメール

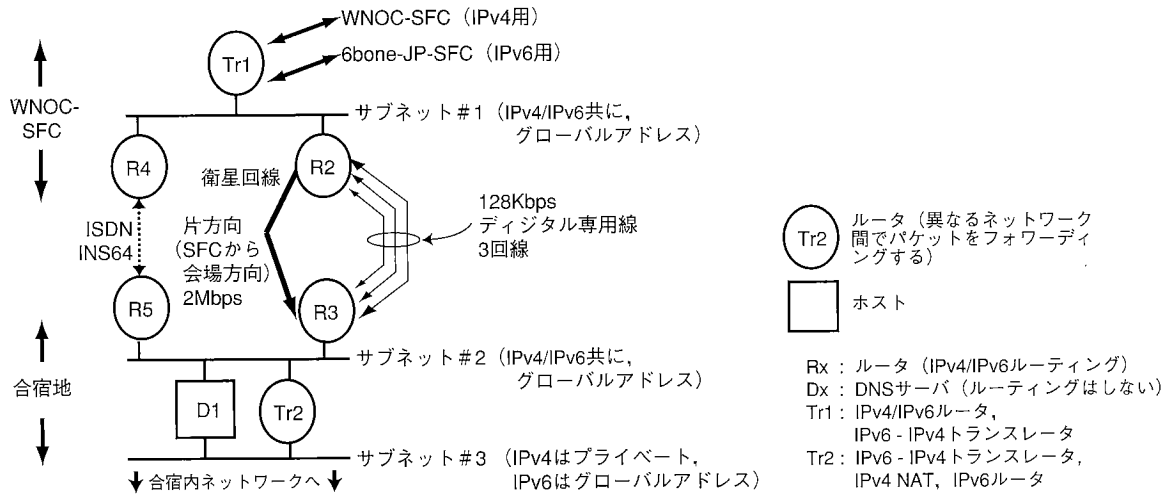

図-2　1999年秋 WIDE合宿ネットワーク構成図（対外線区）

サーバの運用，合宿地内のホスト管理，各種実験との連携のために，DNSを合宿地内で運用

- **逆引き対策**

IPアドレスに対するホスト名を調べること，つまり逆引きによって，ホストのIPアドレスが正当な場合であるどうかを確認する場合がある．このために，合宿地のすべてのホストのIPアドレスを管理することが必要

以上の理由に加えて，WIDE合宿におけるDNSは，IPv6-IPv4トランスレータとの連携や，IPv6アドレスの逆引きの管理といった各種実験と関連するために，合宿地内での運用が必須となっている．

そして，IPv4については，NAT内のプライベートIP用とNAT外のグローバルIP用DNSを個別のDNSエントリで運用した．これは，NAT内とNAT外で，同一のホスト名に対して異なるIPアドレスを応答するためである．これを利用して，WWWサーバやFTPサーバをNAT内とNAT外に同時に設置することにより，対外線帯域の資源を節約，NAT障害時においてもWWWやFTPのサービスを利用可能にした．

■NATの活用

WIDE合宿では，IPv4アドレスとして，グローバルな24bit（クラスC）のアドレスブロックと，プライベートアドレスを利用し，IPv6に関しては，グローバルな48bitのアドレスブロックを使用している．

IPv4に関しては，参加者が200名を超えることから，プライベートアドレスを利用し，グローバルアドレスを持つネットワークとは，NATを介して接続した．このNATは，単なるNATではなく，IPv4 NATとIPv6ヘッダ型トランスレータを実装したNAT-PT[1]であり，ヘッダ変更型IPv4-IPv6トランスレータとIPv4 NATを同時に運用することができた．IPv6に関しては，グローバルアドレス，IPv4に関しては，プライベートアドレスでの利用が可能である．

■IPv4とIPv6相互接続環境の実現

過去4回の合宿では，次のインターネットプロトコルであるIPv6と現在のIPv4を相互運用する際に必要な技術の検証を行っている．IPv6の運用においては，IPv6の実験ネットワークである6boneへ接続し，参加者が利用する末端部分まですべてをIPv6に対応させ，IPv6プロトコルスタック，IPv6とIPv4ネットワークの同時運用を行っている．そのため，IPv4とIPv6間の橋渡しトランスレータや，IPv6を考慮したDNSは，対外線の運用において必須である．WIDE合宿では，NAT-PTとは別に，TCPリレー型IPv6-IPv4トランスレータやトランスレータと連携するDNS，IPv6アドレスの逆引きを考慮したDNSの運用を行った．これらの研究技術すべての相互運用を行い，インターネットを利用する組織をIPv6化した場合の問題点や運用方法についての検証を行う．

WIDE合宿の構成－対外線区－

ここでは，衛星回線を用いた1999年秋合宿の対外線区構成を例に，各実験の構成を述べる．1999年秋合宿の対外線区は，ISDN回線を2本，128Kbpsの専用線を3本，2Mbpsの衛星回線を1本で構成した（**図-2**）．

専用線とISDN，および衛星回線の端点は，静岡県舘山寺の合宿会場と神奈川県藤沢市の慶應SFCに設置した．合宿ネットワークをインターネットに接続するために，IPv4/IPv6ルータTr1を設置した．Tr1は，合宿ネットとWNOC-SFC（IPv4用），WIDE-6bone（IPv6用）間を接続しており，BSD系OS用のIPv6プロトコルスタックであるKAME[2]が導入されたPCである．また，Tr1は，TCPリレー型IPv6-IPv4トランスレータを兼ねたルータである．

この対外線区上で，衛星回線と3つの専用線を1つの仮想データリンクとして扱う実験，IPv6対応ISDNルータの検証（R4,R5），TCPリレー型IPv6-IPv4トランスレータ（Tr1），ヘッダ型トランスレータとIPv4 NATを兼ねたTr2，IPv4/IPv6 DNS（D1）の実験を行った．

専用線と衛星回線を利用した対外接続

衛星回線は，ディジタル専用線（128Kbps～）に比べて，高帯域（2Mbps）であり，日本国内であれば，静止衛星方向（南南西）空間を確保できればどこでも利用することができる．たとえば，災害によって，通信インフラが壊滅した状況下でも利用できる．1999年秋合宿では，WNOC-SFCから合宿地への一方向2Mbpsで衛星回線を用意した．単方向の2Mbpsの回線を用意するのは，合宿におけるトラフィックの流れは，合宿地からのデータの流れより，外部からの合宿地へのデータの流れが大きい．これは，合宿地から外部へのHTTP（Web）やFTP（ファイル転送），POP/IMAP（メールの転送）といったサービスへの応答に対する転送データ量の方が大きいためである．

ルータR2は，トラフィックの種類に応じて衛星回線経由，地上線経由を切り替えるポリシールーティングを行っている．このポリシーは，HTTPや，FTP，POPといったバルク性のトラフィックに関しては，WNOC-SFCから合宿地へ衛星回線経由でルーティング，telnetや，sshといった反応速度を要求するトラフィックは，地上線経由でルーティングされるように設定している．これにより，高遅延だが帯域幅が広いメディアの利点を活かした利用を行っている．

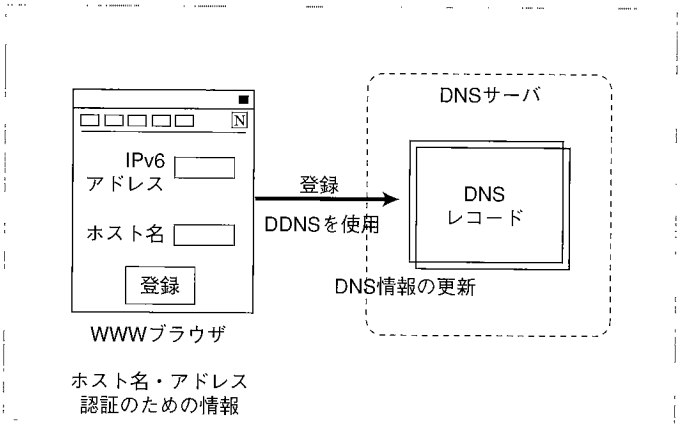

図-3　WebとDNSの連携

DNSの運用

DNSサーバは，KAMEスタックの利用によりIPv4/IPv6での応答処理が可能なBINDを利用して運用を行った．IPv4/IPv6の両方が利用可能であるため，ホスト名に対しては，IPv6アドレス（AAAAレコード）とIPv4（Aレコード）のエントリが登録される．

DNSには，ホスト名に対するIPアドレスを解決する目的以外に，IPアドレスに対するホスト名を解決する役割も持っている．たとえば，UNIXのrコマンドや，一部のFTPサービスでは，IPアドレスに対するホスト名が正しく解決できるかどうかで認証を行う場合がある．このため，IPアドレスからのホスト名の対応も同様に登録を行う必要がある．IPv4の場合，登録が必要なアドレスは，あらかじめ割り当てられているアドレスと，DHCPで配布されているアドレスだけである．しかし，IPv6の場合には，IPアドレスがネットワークインタフェースのMACアドレスから生成されるEUI-64形式のアドレスに依存する．たとえば，MACアドレスが00:90:cc:07:09:5bのインタフェースのIPv6アドレスのホスト識別部は0290:ccff:fe07:095bとなり，これにネットワークアドレスが付加されたものがIPv6アドレスとなる．このため，IPアドレスからホスト名へのエントリを管理するためには，あらかじめ参加者が利用するネットワークインタフェースカードのMACアドレスを調べて登録する必要があるが，これは困難であり現実的ではない．

そこで，BINDに実装されているDynamic DNS（DDNS）[3]の機能を用いて，参加者が必要に応じてDNS情報を動的に更新する仕組みを提供することにした．実際には，BINDのDDNはアクセスコントロールがまだ十分ではなかったため，WWWを利用した登録用ページを提供し，IPv6アドレスとホストの対応情報を登録可

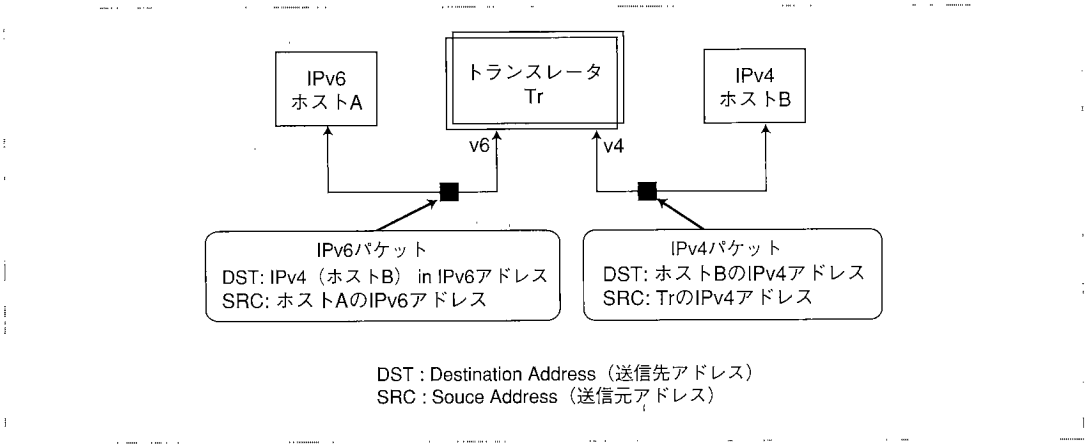

図-4　トランスレータ

能にした.

参加者は, IPv6が利用可能となった時点で, 利用するIPv6アドレスとホスト名, 参加者の番号, あらかじめ配布したパスワードを入力することでDNS情報を更新することが可能になる. 更新の際にはBINDのDDNSの機構が利用されている (**図-3**参照). ユーザが直接DDNSの機構を利用することは禁止し, Webサーバからの登録要求だけを受け付けるようにし, BINDに実装された単純なアクセスコントロールでアクセス制限をかけることができた. 登録の仕組みは提供できたが, サブネットを移動するたびにIPv6アドレスのネットワーク部は変更になり, IPv6アドレスが変わってしまう, そのため, サブネットごとにDNS情報の登録が必要になってしまう. その問題は, 合宿ネットワークにおけるすべてのサブネットで, IPアドレスからホスト名の対応をホスト部だけで解決できるようにネットワークアドレスを集約することで解決した.

NATおよび, トランスレータ

■2種類のトランスレータ

1999年秋合宿では, 異なる2種類のトランスレータTr1とTr2を運用した. Tr1は, IPv6ホストがIPv4ホストへ通信できるトランスレータであるfaithd[4] (KAMEのリリースパッケージに含まれている) を利用した. faithdは, telnetや, ftpといったTCPアプリケーション用のトランスレータであり, 本実験では, telnet, ftp, ssh, pop3, smtpのトランスレーションを行った. Tr2は, NAT-PTとTCP/UDP port番号変換機能を有したIPv4 NATを実装したものを用いた. このNATおよびトランスレータは, IPv6ホストからIPv4ホストへのICMPやTCP/UDPを用いた通信が利用でき, かつ, IPv4アドレスに関しては, プライベートアドレス, IPv6アドレスに関しては, グローバルアドレスを持ったホストが混在する環境において, 大きな効果を持つ. また, 両トランスレータは, IPv6ホストやIPv4ホストに手を加えることなく, 通信が可能であり, この意味で, 透過的なトランスレータ機能を提供できる.

■DNSとトランスレータの連携

トランスレータTr1とTr2を透過的に運用するためには, DNSとの連携が必須である. 両トランスレータは, IPv4アドレスをIPv6アドレス中にマップしたIPv6アドレスによる通信をIPv6からIPv4へトランスレートする. この機構を**図-4**を用いて説明する. IPv6アドレスを持ったホストAとIPv6とIPv4アドレスを持ったトランスレータホストTr, そして, IPv4アドレスを持ったホストBがあるとする.

IPv6ホストAがIPv4ホストBへのトランスレータを介した通信を行う場合, ホストAは, 送信先アドレス (Distnation Address) として, IPv6アドレスにホストBのIPv4アドレスを組み込んだアドレスを指定した, IPv6パケットを送信する. トランスレータTrは, 受け取ったIPv6アドレスから組み込まれたIPv4アドレスを取り出し, 送信先アドレスとし, ホストTrのIPv4アドレスを送信元アドレスとしたIPv4パケットに変換 (トランスレート) し送信する.

このようにして, IPv6ホストからIPv4ホストへの通信を実現する. つまり, IPv6ホストが, IPv4ホストをトランスレータを介して通信するには, 明示的に, IPv4アドレスをIPv6アドレスに組み込んだアドレスを利用しなければならない. そこで, 透過的なトランスレータ利用を実現するために, DNSにIPv4アドレスをIPv6アドレスに組み込む機能を実装したtotdやnatptdとBIND DNSを併用運用した.

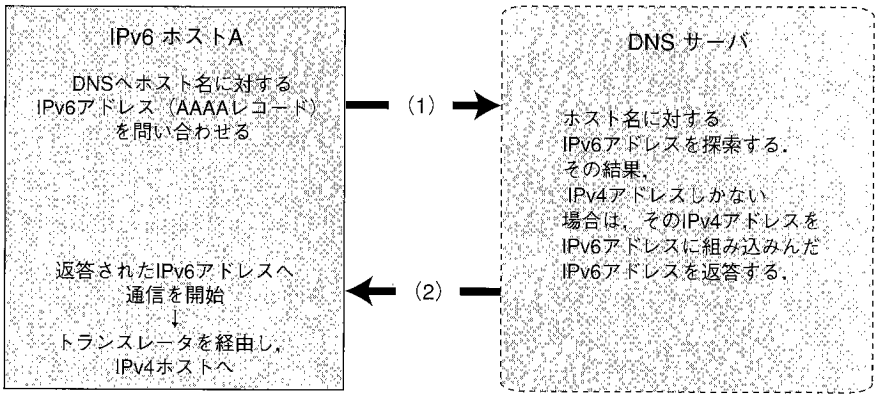

図-5　DNSとトランスレータの連携

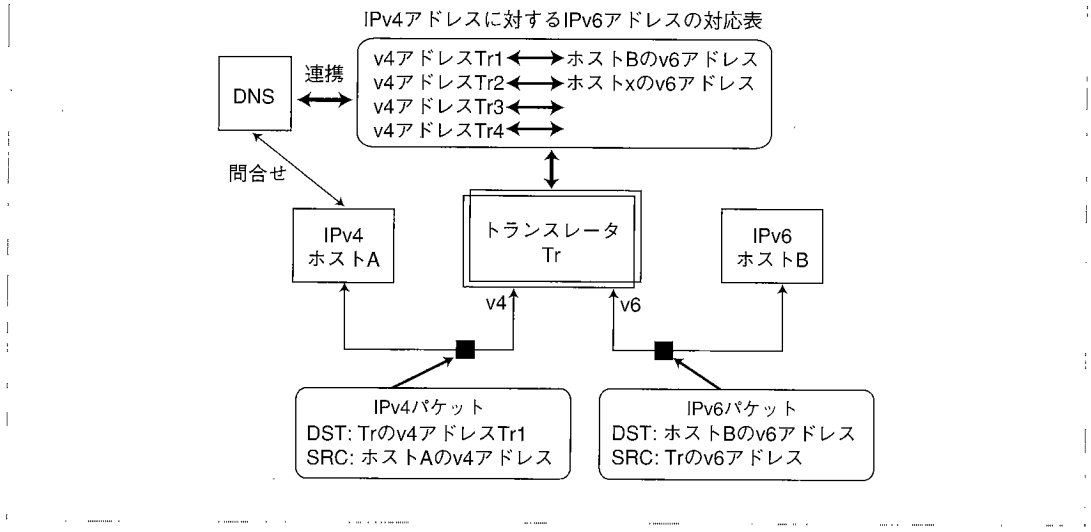

図-6　IPv4からIPv6ホストへの通信

この機能は，DNSへのホスト名に対するIPv6アドレス問合せ（**図-5 (1)**）に対して，ホスト名に対するアドレスがIPv4のみの場合は，IPv6アドレスにIPv4アドレス組み込み変換したIPv6アドレスを，そのホストのIPv6アドレスとして，応答する（**図-5 (2)**）ものである．

これにより，IPv6ホストは，IPv4ホストに対し，トランスレータを介して，透過的な接続が可能となる．

今回の合宿では，実験を行えなかったが，2000年秋合宿では，IPv4ホストからIPv6ホストに対してトランスレーションをNAT-PTで行う実験を予定している．この場合は，IPv6からIPv4のときと異なり，IPv6アドレス（128bit）のすべてをIPv4（32bit）へ写像することはできないため，IPv4ホストは，任意のIPv6ホストと通信することはできない．そこで，いくつかのIPv6ホストを選択的にIPv4ホストに見せ，IPv4対IPv6アドレスの対応管理を行う（**図-6**）．この部分の実装には，DNSといったホスト名を解決をする機構とNAT-PTとの密接な連携によるアドレス対応表の更新が必要である．

最後に

今回は，WIDE合宿を例にして，IPv6/IPv4混在環境における対外線およびIPv6-IPv4トランスレータの運用について述べた．今回用いたOSやアプリケーションは，KAMEを通して配布されており，誰もが利用できる状態となっている．特に，トランスレータに関しては，来るべきIPv6時代において，IPv4からIPv6への移行方法として運用が必須であり，また，WIDE合宿の運用結果から，これらの技術は，実用段階に入ったといっても過言ではない．これらの技術が，各種イベントにおける運用に参考になれば幸いである．

参考文献

1) Tsirtsis, G. and Srisuresh, P.: Network Address Translation - Protocol Translation (NAT-PT), RFC2766 (2000).
2) KAME Project: http://www.kame.net
3) Vixie, P. (Ed.), Thomson, S., Rekhter, Y. and Bound, J.: Dynamic Updates in the Domain Name System (DNS UPDATE), RFC2136 (1997).
4) Hagino, J. and Yamamoto, K.: An IPv6-to-IPv4 Transport Relay Translator, Internet-Draft (2000).

（平成12年7月10日受付）