NATによる準マルチホーム化技法

梶田将司[†] 結縁祥治[††]

本論文では，ネットワークの基幹に属さない任意の規模のネットワークが局所的なポリシーに基づいて複数のインターネット接続を行う方法を提案する．本手法では，NAT（ネットワークアドレス変換）を用いて複数の外部ネットワークをプライベートネットワークにマッピングすることによる複数接続を実現する．本技法によるマルチホーム化は，ネットワークが異なる複数のグローバルアドレスを用い，接続する側の利用者が通信先に応じて経路を選択することで一方的に信頼性，効率の向上を目的とするため，通常のマルチホーム化と区別し，**準マルチホーム化**と呼ぶ．準マルチホーム化によって，複数の対外接続を局所的なポリシーに基づいて制御することができるようになるため，実際の運営形態に応じた柔軟な負荷の分散と接続の確保が可能になる．最後に名古屋大学情報メディア教育センターにおける本技法の実現方法および評価結果を示す．

A Semi-multihoming Technique Using Network Address Translator

Shoji Kajita[†] and Shoji Yuen[††]

This paper presents a multihoming technique for a middle or small sized network using NAT (Network Address Translator). We call our technique *semi-multihoming* since we only consider the user-side multihoming, where the typical multihoming enables to bridge the connections while ours does not. The advantage of our technique is that the flexible load-balancing between the connections is possible based on the local routing policy independent of the global policy to which the network may belong. NAT is the key technology to enable our technique to implement on the existing network equipments. Finally, we show an implementation and the result of our technique at Center for Information Media Studies, Nagoya University.

1. はじめに

マルチホーム化とは，IP ネットワークを複数の接続点によってインターネット接続することであり，外部接続に対する信頼性の向上と負荷分散が可能になる．近年の IP ネットワークの一般化により，マルチホーム化を行って，IP ネットワークの信頼性を確保しながら効率的にネットワークを運用するニーズが高まっている．

通常のマルチホーム化では，大域的な経路情報をインターネットから取得するとともに，自ネットワークの経路情報をアナウンスする必要がある．現在では，BGP4 による経路情報の交換および経路制御が一般的に行われているため，ネットワークを構成する組織ごとに AS（Autonomous System）番号を取得し，経路制御を行う必要がある[3]．経路制御において，あまりに小規模なネットワークの経路を含めると，経路情報の増大と不安定化を招くため，ある程度の規模を持ったネットワークに 1 つの AS 番号を割り当てざるをえない．このため，中小規模のネットワークでは経路情報のアナウンスによるマルチホーム化は困難である．

また，比較的規模の大きなネットワークであっても，(1) すでに対外接続があり，ある程度の信頼性が保たれているとマルチホーム化が組織全体の要求として（特に予算面で）認識されにくい，(2) 大規模な組織ではインターネットの利用目的が多様になり，ネットワーク全体として負荷のバランスをとるのが非常に困難である，という問題が生じ，実際にはマルチホーム化できない場合も多い．

本論文では，このような問題に対して，インターネットの基幹部分には属さない中小規模のサブネットワークが自ら定める経路情報に基づいてマルチホーム化を行う技法について述べる[1]．本技法によるマルチホーム化は，ネットワークが異なる複数のグローバルアドレスを用い，接続する側の利用者が通信先に応じて経

† 名古屋大学情報メディア教育センター
Center for Information Media Studies, Nagoya University
†† 名古屋大学大学院工学研究科
Graduate School of Engineering, Nagoya University

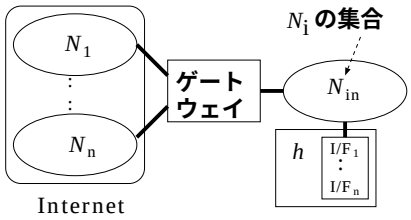

図 1 NAT なしの準マルチホーム化
Fig. 1 Semi-multihoming without NAT.

路を選択することで一方的に信頼性，効率の向上を目的とする☆1ため，通常のマルチホーム化と区別し，「準マルチホーム化」と呼ぶ．本技法により，複数の対外接続を局所的なポリシーに基づいて制御することができるようになる．このため，実際の運営形態に応じた柔軟な負荷の分散と接続の確保が可能になる．本技法の具体例として名古屋大学情報メディア教育センターにおいて実際に運用を行った結果を示す．

本論文の構成は以下のとおりである．まず，2 章で NAT を用いた準マルチホーム化技法の基本的なアイデアについて述べるとともに既存の技術を用いた場合の問題点を述べる．3 章では，本技法による解決方法を示す．4 章および 5 章では，本センターにおける実現方法および評価結果について述べる．最後に 6 章で本論文をまとめる．

2. NAT による準マルチホーム化

2.1 基本概念

本論文で提案する準マルチホーム化の基本的なアイデアは，「ホスト h が**内部のネットワーク N_{in} において**接続先ごとの n 個のアドレス $N_1(h), \ldots, N_n(h)$ を見掛け上持つようにする」ことである．したがって，N_{in} の各ホストはそれぞれ n 個のインタフェースを持ち，**図 1** のように N_{in} に接続される．

通常，ISP（Internet Service Provider）から割り当てられるネットワークアドレスは ISP ごとに異なっているため，各 N_i $(i = 1, 2, \ldots, n)$ は異なったネットワークアドレスが割り当てられる．しかし，図 1 のような構成では，N_{in} に n 個の異なるネットワークが混在するため，ルータ，ハブなどのすべてのネットワーク機器で複数のネットワークに対応したインタフェースを持つ必要がある．また，適当な単一のネットマスクで扱えない複数のネットワークを，1 つのネットワークで運用すること自体，あまり一般的とはいえないので，保守性やトラフィック効率の低下を招くことが予想される．

2.2 NAT による実現

そこで，外部ネットワーク N_i をネットワークアドレス変換（NAT[4]）を用いて内部ネットワークと同じネットワークに変換し，単一のネットワークを構成する．

以下，簡単のため，対外接続先として ISP X と ISP Y の 2 カ所，内部ネットワークとして LAN Z を仮定する．これら 3 つのネットワークはルータ r で相互に接続されているとする☆2．ルータ r は，ISP X と ISP Y に対するルーティング情報 (I_x, I_y) を保持する．ここで，I_x，I_y はインターネットアドレス空間全体 I の分割で，(I_x, I_y) は LAN Z から外部に対する任意のパケットに対して，宛先が I_x に属する場合は ISP X 側に，I_y に属する場合は ISP Y 側に発信することを意味する．ISP X，ISP Y，および LAN Z から割り当てられているネットワークを N_x，N_y および N_z とする☆3．

NAT については，ISP X，ISP Y，LAN Z に対するアドレス変換をそれぞれ $T_x : N_z \rightarrow N_x$，$T_y : N_z \rightarrow N_y$ とする☆4．このアドレス変換に従って，ソースアドレス s，宛先アドレス d のパケット $P(s, d)$ のアドレス変換 nat は以下のように定義される．

$$\mathsf{nat}(P(s,d)) = \begin{cases} P(T_x(s), d) & \text{if } s \in N_z \\ & \text{and } d \in I_x \\ P(T_y(s), d) & \text{if } s \in N_z \\ & \text{and } d \in I_y \\ P(s, T_x^{-1}(d)) & \text{if } d \in N_x \\ & \text{and } s \in I_x \\ P(s, T_y^{-1}(d)) & \text{if } d \in N_y \\ & \text{and } s \in I_y \end{cases}$$

nat はセッション開始時にアドレス変換をアドレス束縛として NAT テーブル NAT に追加する．それ以後の，ソースアドレスもしくは宛先アドレスが同じホストからのすべてのセッションに対して同じアドレス変換（逆変換を含む）を行うものとする[5]．

この場合，内部ホスト h_z と外部ホスト e 間の通信は次のように行われる．

(1) 内部ホストを起点とする通信

往路では，ホスト $h_z \in N_z$ は経路表に従い，パ

☆1 このような視点は大域的な信頼性向上というインターネットの原則からは外れることになるが，現在のバックボーンを中心とした構成と課金システムにおいては一般的な要求である．

☆2 2 カ所以上の接続についても同様の方法で拡張できる．

☆3 N_x，N_y はグローバルアドレス，N_z はプライベートアドレスと仮定する．

☆4 T_x，T_y は 1 対 1 変換である．

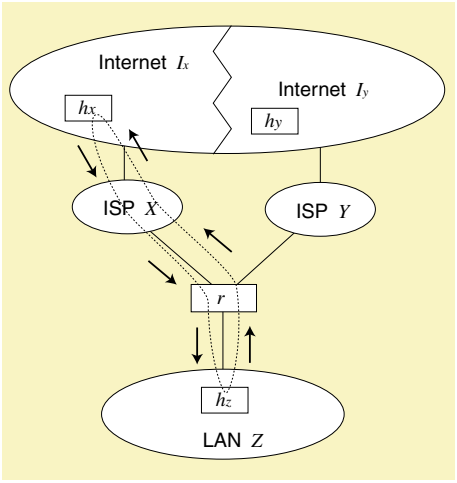

図 2 内部ホストを起点とする場合のパケットの流れ
Fig. 2 Packet flows from an internal host.

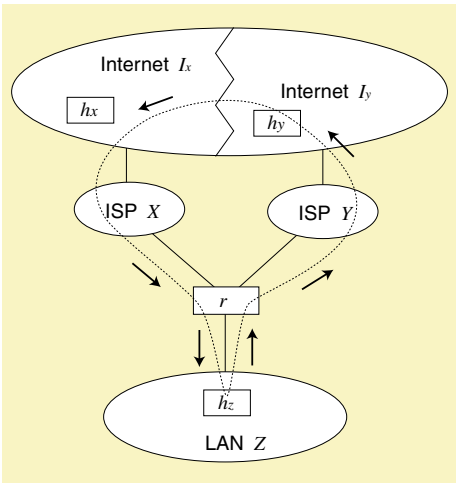

図 3 ISP X を経由した場合の外部ホストを起点とする場合のパケットの流れ
Fig. 3 Packet flows from an external host in ISP X.

ケット $P(h_z, e)$ をルータ r に送信する．$e \in I_x$ ならば，ルータ r は nat により $P(T_x(h_z), e)$ に変換し，NAT にアドレス変換 $T_x : h_z \rightarrow T_x(h_z)$ を登録した後，ISP X へ転送する．同様に，$e \in I_y$ ならば，$P(T_y(h_z), e)$ に変換し，NAT にアドレス変換 $T_y : h_z \rightarrow T_y(h_z)$ を登録した後，ISP Y へ転送する．

復路では，$e \in I_x$ の場合，$P(T_x(h_z), e)$ に対する応答パケット $P(e, T_x(h_z))$ は，NAT に登録されている T_x の逆変換 $T_x^{-1} : T_x(h_z) \rightarrow h_z$ により $P(e, h_z)$ に変換される（**図 2** 参照）．$e \in I_y$ の場合も同様． □

(2) 外部ホストを起点とする通信

外部ホスト e が内部のホスト h_z を $T_x(h_z) \in N_x$ として参照した場合，パケット $P(e, T_x(h_z))$ が ISP X 側のインタフェースに受信されるので，nat により $P(e, T_x^{-1}(T_x(h_z))) = P(e, h_z)$ に変換され，アドレス変換 $T_x^{-1} : T_x(h_z) \rightarrow h_z$ が NAT に登録される．これに対する応答は，NAT に登録されている T_x^{-1} の逆変換 $T_x : h_z \rightarrow T_x(h_z)$ により，$P(h_z, s) = P(T_x(h_z), s)$ としてルータ r から発信される．$T_y(h_z) \in N_y$ として参照を受けた場合も同様． □

2.3 問 題 点

内部のホスト h_z は見かけ上 2 つのアドレス $T_x(h_z)$ と $T_y(h_z)$ を持つ．外部のホスト $h_y \in I_y$ から内部ホスト h_z が $T_y(h_z)$ として参照されると，往路のパケット $P(h_y, T_y(h_z))$ は ISP Y 経由となり，復路のパケット $P(T_y(h_z), h_y)$ も ISP Y にルーティングされる．ところが，$T_x(h_z)$ として参照されると，往路のパケット $P(h_y, T_x(h_z))$ は ISP X 経由であるのに対して，復路のパケット $P(T_x(h_z), h_y)$ は経路表により ISP Y 経由となってしまう（**図 3**）．これは，外部からの参照とルータ r の持つ経路情報が独立であることが原因であり，宛先アドレスによる経路制御を行う限り解決できない．このため，経路制御は宛先アドレスではなく，NAT におけるアドレス束縛に基づく必要がある．このような状況は，たとえば，内部ネットワークにメールホストを配置し，そのホストを ISP X と ISP Y の両方のホスト名で MX レコードに登録して，メール配送の信頼性を向上させようとすると必ず発生する問題点である．

非対称的なルーティングは，運用としては一般的とはいえず，保守や維持管理の点から望ましいとはいえない．さらに，ISP ごとにルータを用意するとアドレス変換が複数の NAT テーブルにわたってしまうことになる[5]．このような経路制御を含めた NAT テーブル情報の交換は自明でなく，現在のところ直接的な実装は我々の知る限りでは存在しない．

3. 分割 NAT テーブルによる実現

本章では以上の問題点を解決し，NAT テーブルを接続先ごとに分割する技法を示す．

3.1 NAT テーブルの分割の問題点

ルータ r の機能を**図 4** のように分ける．ここで，ISP X と ISP Y に対する変換規則 nat_x，nat_y は以下のように与えられる．

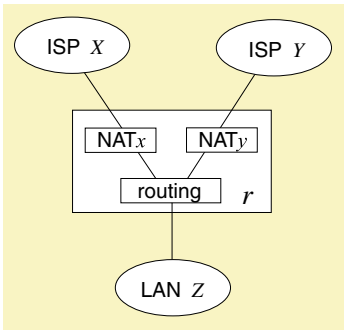

図 4 分割 NAT テーブル
Fig. 4 Partitioned NAT tables.

$$\mathsf{nat}_x(P(s,d)) = \begin{cases} P(T_x(s),d) & \text{if } s \in N_z \\ P(s,T_x^{-1}(d)) & \text{otherwise} \end{cases}$$

$$\mathsf{nat}_y(P(s,d)) = \begin{cases} P(T_y(s),d) & \text{if } s \in N_z \\ P(s,T_y^{-1}(d)) & \text{otherwise} \end{cases}$$

内部からの通信は，前章の場合と同様に以下のように行われる．$P(h_z,e)$ はルータ r において $e \in I_x$ ならば，ISP X 側に送られ，$P(T_x(h_z),e)$ に変換され，その変換 $T_x : h_z \to T_x(h_z)$ が NAT_x に登録される．これに対する応答パケット $P(e,T_x(h_z))$ は $P(e,h_z)$ に変換される．$e \in I_y$ も同様．

外部からの通信においては，外部ホスト $h_x \in I_x$ が内部ホスト h_z を $T_y(h_z)$ として参照した場合，往路のパケット $P(h_x,T_y(h_z))$ は nat_y によって $P(h_x,h_z)$ と変換され，その変換 $T_y^{-1} : T_y(h_z) \to h_z$ が NAT_y に登録される．このパケットに対する応答パケット $P(h_z,h_x)$ は $h_x \in I_x$ なので，nat_x^{-1} によって変換を受けようとするが，必要なアドレス変換が NAT_x に登録されていないので，変換できない．$h_y \in I_y$ が内部ホスト h_z を $T_x(h_z)$ によって参照しようとする場合も同様である．

3.2 複数の IP 割当てによる解決

このような問題が生じる原因は，変換されたアドレスがどの NAT テーブルによって変換されたかが記録されないためである．NAT テーブルの切替えは内部ネットワークの情報のみで行われなければならないので，内部ホスト h_z の外部からの参照アドレス $T_x(h_z)$ および $T_y(h_z)$ が NAT によりどちらも h_z に変換されることが問題である．そこで，ホスト h_z に対し，実 IP アドレス h_z 以外に ISP X 用の内部アドレス $X(h_z)$，ISP Y 用の内部アドレス $Y(h_z)$ を論理 IP アドレス☆として用意し，参照経路ごとに内部アドレスを区別することにする．このとき，応答パケットをどちらの NAT テーブルに適用するかは，応答パケットのソースアドレスにより経路を選択する（以下，これをソースルーティングと呼ぶ）．内部ホストにおいて外部から参照されるアドレスの集合を $N_z^{ex} \subseteq N_z$ とすると，ISP X と ISP Y に対するアドレス変換 T_x，T_y に対して，$dom(T_x) = X(N_z^{ex})$，$dom(T_y) = Y(N_z^{ex})$ となる☆☆．ここで，$X(N_z^{ex})$，$Y(N_z^{ex})$，N_z^{ex} は互いに素である．

内部ホストから外部への接続

発信の場合は，ソースルーティングの影響を受けない $h_z \in N_z^{ex}$ を発信アドレスとする．$h_x \in I_x$ に対するパケット $P(h_z,h_x)$ は，ISP X 側にルーティングされ，$P(T_x(h_z),h_x)$ と変換され，$T_x : h_z \to T_x(h_z)$ を NAT_x に登録する．応答パケットは $T_x(h_z) \in N_x$ であるので，ISP X 側に到着し，$P(h_x,h_z)$ と変換される．$h_y \in I_y$ の場合も同様． □

外部ホストから内部への接続

(1) 外部ホスト $h_x \in I_x$ が内部ネットワークのホスト h_z を ISP X 経由で参照する場合：
ISP X からの参照なので，h_z は $T_x(X(h_z))$ として参照される．$p(h_x,T_x(X(h_z)))$ は $P(h_x,X(h_z))$ に変換され，この変換 $T_x^{-1} : T_x(X(h_z)) \to X(h_z)$ が NAT_x に追加される．応答パケット $P(X(h_z),h_x)$ はソースアドレスが $X(h_z)$ であるので ISP X 経由であることが分かり，NAT_x の T_x によって $P(T_x(X(h_z)),h_x)$ に変換される．

(2) 外部ホスト $h_x \in I_x$ が内部ネットワークのホスト h_z を ISP Y 経由で参照する場合：
ISP Y からの参照なので，h_z は $T_y(Y(h_z))$ によって参照される．$P(h_x,T_y(Y(h_z)))$ が $P(h_x,Y(h_z))$ に変換され，変換 $T_y^{-1} : T_y(Y(h_z)) \to Y(h_z)$ が NAT_y に追加される．応答パケット $P(Y(h_z),h_x)$ はソースアドレス $Y(h_z)$ によって ISP Y 経由であることが分かるので ISP Y 側にソースルーティングし，$P(T_y(Y(h_z)),h_x)$ と変換される．

(3) 外部ホスト $h_y \in I_y$ が内部ネットワークのホスト h_z を ISP Y 経由で参照する場合：
(1) と同様

(4) 外部ホスト $h_y \in I_y$ が内部ネットワークのホスト h_z を ISP X 経由で参照する場合：
(2) と同様 □

以上のように，NAT テーブルを分割し，論理 IP アドレスによる複数の IP 割当ておよびソースルーティン

☆ エイリアス IP アドレスとも呼ばれる．

☆☆ $dom(T)$ は変換 T の定義域を表す．

グを行うことにより，準マルチホーム化が可能となる．

3.3 NAT 技術利用に対する考察

本手法は本質的には，ネットワークアドレスを外部接続ごとにホストに複数割り当てる手法である．しかし，実際にネットワークを構成する場合，外部接続ごとに連続しないネットワークに属するパケットが流れると経路制御や保守が複雑になるため，運用コストが上昇する．NAT を用いることで内部ネットワークの構成に応じて自由にネットワーク設定をすることができ，一般的なネットワーク機器による低コストでの構成が可能になる．

本手法は新たな実装などを開発することなく，現有のネットワーク構成と機器で実用的なネットワーク構成手法を示すことを前提とした．さらに，本手法では NAT 機能を機器ごとに分散して配置することができる．このような点において負荷分散が本手法の第一目的である．第二の目的として接続の二重化がある．障害が発生した場合，発信経路情報を変更し，障害の発生したゲートウェイに発信しないようにする．この手法としては，デフォールトルータを用意して切り替える方法とホストで発信経路を個別に切り替える方法が考えられる．

4. 名古屋大学情報メディア教育センターにおける実現

名古屋大学情報メディア教育センター（以下，本センター）における準マルチホーム化を具体例として示す．本技法による準マルチホーム化は平成 11 年 4 月より運用を開始した[6]．

4.1 機器およびネットワーク構成

本センターのネットワーク機器およびネットワーク構成の概略は以下のとおりである．(1) 対外接続先は NICE（名古屋大学キャンパスネットワーク）と CTCN（中部テレコミュニケーション（株）），(2) NICE 側 NAT 機器は CISCO 社 PIX520，CTCN 側 NAT 機器は CISCO 社 7204 を使用，(3) ルーティングは 7204 が兼任（内部のネットワーク機器はすべて 7204 をデフォールトゲートウェイとして指定），(4) NICE 側のネットマスクは 23 ビット，CTCN 側のネットマスクは 21 ビット，内部ネットワーク（Media-net）はプライベートのクラス B（**図 5** 参照）．

また，7204 における経路情報は，国内向け非学術サイトについては CTCN 経由，海外および国内学術サイトについては NICE 経由となるように設定されている．

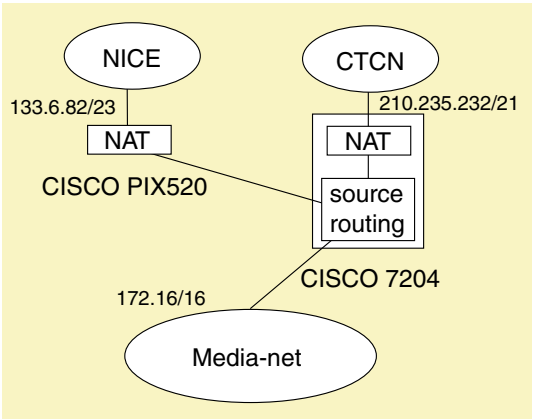

図 5 本センターでの準マルチホームの運用構成
Fig. 5 The semi-multihome configuration at CIMS.

(a) PIX520 の設定

```
#
# NAT の設定
#
static (inside,outside) 133.6.82.1 172.16.1.101 \
    netmask 255.255.255.255 0 0
static (inside,outside) 133.6.82.101 172.16.1.1 \
    netmask 255.255.255.255 0 0
```

(b) 7204 の設定

```
# NAT の設定
ip nat inside source static 172.16.1.111 \
    210.235.232.1
ip nat inside source static 172.16.1.1 \
    210.235.232.101
# source ルーティングの設定
access-list 30 permit host 172.16.1.111
access-list 40 permit host 172.16.1.101
interface FastEthernet0/0
  ip policy route-map semi-multihome
route-map semi-multihome permit 10
  match ip address 30
  set ip default next-hop 210.158.17.61
route-map semi-multihome permit 20
 match ip address 40
 set ip next-hop 172.16.252.2
```

図 6 各ルータでの設定
Fig. 6 Configuration settings of the routers.

4.2 準マルチホームの設定

図 6 に NAT 機器および 7204 におけるソースルーティングの設定を示す．**図 7** に 7204 のソースルーティングの動作フローを示す．この設定において，`accesslist 30` と `accesslist 40` はそれぞれ CTCN 側，NICE 側からのセッションの応答パケットかどうかをチェックする．それ以外は発信パケットなので，経路情報に従ってルーティングする．

4.3 動 作 例

ここでは，実アドレスとして `172.16.1.1` を持つホ

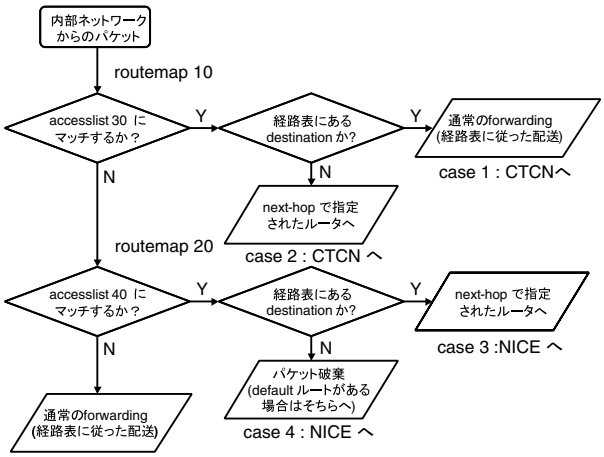

図 7 CISCO 7204 の動作フロー
Fig. 7 Operation flow of the CISCO 7204 router.

表 1 各サーバの用途と使用される IP アドレス
Table 1 IP addresses of the application servers.

ホスト名	用途	内部→外部	外部→内部	
			NICE 経由時	CTCN 経由時
sv001	DNS サーバ	172.16.1.1	172.16.1.101	172.16.1.111
sv003	ニュースサーバ	172.16.1.3	172.16.1.103	172.16.1.113
sv005	メールサーバ	172.16.1.5	172.16.1.105	172.16.1.115
sv006	telnet・ftp サーバ	172.16.1.6	172.16.1.106	172.16.1.116
sv007	telnet・ftp サーバ	172.16.1.7	172.16.1.107	172.16.1.117
sv009	WWW サーバ	172.16.1.9	172.16.1.109	172.16.1.119

スト h_z に論理アドレスとして `172.16.1.101`（NICE 側）と `172.16.1.111`（CTCN 側）を設定した場合の動作例を示す．なお，紙面の都合上，NICE 経由の外部ホストからの通信が正しく行われることのみを示す．

外部ホスト $h_{NICE}(\in I_{NICE})$ → $NICE$ → Media-net の場合

往路： $h_{NICE}[P(h_{NICE}, 133.6.82.1)]$ → NICE → PIX520[$P(h_{NICE}, 172.16.1.101)$ に NAT] → h_z

復路： h_z → 7204 [$P(172.16.1.101, h_{NICE})$ なので図 7 中の case 4] → PIX520[$P(133.6.82.1, h_{NICE})$ に NAT] → NICE → h_{NICE}

外部ホスト $h_{CTCN}(\in I_{CTCN})$ → $NICE$ → Media-net の場合

往路： $h_{CTCN}[P(h_{CTCN}, 133.6.82.1)]$ → NICE → PIX520[$P(h_{CTCN}, 172.16.1.101)$ に NAT] → h_z

復路： h_z → 7204[($P(172.16.1.101, h_{CTCN})$ なので図 7 中の case 3] → PIX520[$P(133.6.82.1, h_{CTCN})$ に NAT] → h_{CTCN}

5. 本技法による効果の評価

実際のネットワーク環境で本技法による効果を評価するため，外部ネットワークを起点としたセンター内部の各サーバへ通信について検証した．

5.1 実験条件

評価に用いたデータは，2000 年 1 月 9 日から 1 月 29 日までの 19 日間について，外部ネットワークを起点とするホストからの内部ホストへのアクセス状況を，CISCO 7204 でソースルーティング時に用いられる `access-list` に対するログ機能により採取するとともに，その時点の CISCO 7204 のルーティング状況を `traceroute` コマンドを用いて調べることにより収集した．各内部ホストは，**表 1** に示すように特定のサービスについてのみ，外部からのアクセスが許可されている．NICE 側ルータ（PIX）および CTCN 側ルータ（7204）での各ホストに対する設定は，表 1 に示す IP アドレスを用い，図 6 と同様に行った．また，外部を起点とする通信の負荷分散の方法は**表 2** のとおりに行った．

内部から外部への通信時のルーティングポリシー

表 2 外部を起点とする通信の負荷分散方法
Table 2 Load balancing from external sites.

用途	ホスト名	負荷分散方法
DNS サーバ	sv001	NICE 側からの経路と CTCN 側からの経路双方を NS レコードに登録.
メールサーバ	sv005	NICE 側からの経路を優先度 10 で，CTCN 側からの経路を優先度 20 で MX レコードに登録.
telnet・ftp サーバ	sv006, sv007	NICE 側からの経路のみ．sv006, sv007 を DNS ラウンドロビンにより選択.
WWW サーバ	sv009	NICE 側からの経路のみ.

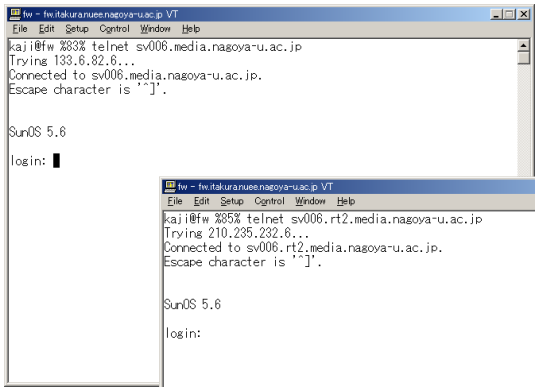

図 8 外部ホストから NICE および CTCN 経由で sv006.media.nagoya-u.ac.jp にアクセスした場合.
Fig. 8 Accesses to sv006.media.nagoya-u.ac.jp from an external host via NICE and via CTCN.

は，NICE，国内学術系および海外は NICE（および SINET）経由，国内非学術系は CTCN 経由となるように設定した．これは，CTCN から BGP4 により国内フルルートを受け取り，その中の学術系だけを `as-path` フィルタにより除去した．

5.2 実験結果

まず，センターの内部ホスト sv006.media.nagoya-u.ac.jp に対して，外部ホストから NICE および CTCN 経由でアクセスした場合のスクリーンショットを**図 8** に示す．アクセスには `telnet` を使用した．ここで使用した外部ホスト（`fw.itakura.nuee.nagoya-u.ac.jp`）に内部からアクセスする場合は NICE 経由となるため，本技法により非対称経路問題が解決されない場合，外部ホストからの CTCN 経由の `telnet` 接続が行えない．しかし，図 8 に示されているように，sv006 への接続が NICE 経由（参照アドレスは sv006.media.nagoya-u.ac.jp）であっても CTCN 経由（参照アドレスは sv006.rt2.media.nagoya-u.ac.jp）であっても `telnet` セッションが正常に開始されていることが分かる．

次に，19 日間の内部ホストへのアクセス状況を**表 3** および**表 4** に示す．表 3 は，内部から外部へのアクセス時の経路が NICE 経由に設定されているネットワークからのアクセス状況を，表 4 は，内部から外部へのアクセス時の経路が CTCN 経由に設定されているネットワークからのアクセス状況を示している．表は，外部から内部へのアクセス時の経路（NICE 経由また CTCN 経由）ごとにまとめてある．

内部から外部へのアクセスが NICE 経由となるホストからのアクセスについては，非対称経路問題が発生しうる通信は 5.44%であることが分かる（表 3 参照）．もちろん，その通信は本技法により正しく通信がなされている☆．一方，内部から外部へのアクセスが CTCN 経由となるホストからのアクセスについては，27.62%が本技法により正しく通信がなされている．後者の方が改善率が高い理由は，メールサーバや WWW サーバへのアクセスは主に NICE 経由になるように設定されているためである（表 2）．

以上の結果から，実際に運用されているネットワーク環境での本技法の有効性が確認された．

6. まとめ

本論文では，NAT を用いて，局所的な経路情報に基づいてマルチホーム化を実現する方法および，その具体例として名古屋大学情報メディア教育センターにおける実装例と運用の評価結果について述べた．

本技法は RFC2663 に示されている Multihomed NAT の 1 つの実現方法である[5]．RFC2663 では，複数の NAT ルータによる Multihomed NAT として，NAT テーブルの情報交換による方法が述べられている．しかし，本技法ではどの NAT テーブルによって変換されたかの情報を失わないように 1 つのホストに複数の IP アドレスを割り当てることで複数の NAT 機器による Multihomed NAT を実現している．これにより，従来の NAT ルータをそのまま用いることができる．また，本手法では，必ずしもプライベートアドレスを使用する必要はないが，内部ネットワーク機器

☆ 往路（外部から内部へ）が CTCN 経由の場合，復路（内部から外部へ）も CTCN 経由になっている．

表 3 内部から外部へのアクセスが NICE 経由となるホストからのアクセス
Table 3 Access statistics from interal hosts via NICE.

ホスト名	NICE 経由		CTCN 経由	
	セッション数	割合	セッション数	割合
sv001	17248	5.34%	15878	4.92%
sv003	26489	8.20%	3	0.00%
sv005	210988	65.32%	1532	0.47%
sv006	11865	3.67%	57	0.02%
sv007	14105	4.37%	88	0.03%
sv009	24723	7.65%	19	0.01%
小計	305418	94.56%	17577	5.44 %

表 4 内部から外部へのアクセスが CTCN 経由となるホストからのアクセス
Table 4 Access statistics from interal hosts via CTCN.

ホスト名	NICE 経由		CTCN 経由	
	セッション数	割合	セッション数	割合
sv001	41610	7.43%	388938	69.42%
sv003	266	0.05%	14987	2.68%
sv005	66464	11.86%	1562	0.28%
sv006	1809	0.32%	0	0.00%
sv007	865	0.15%	0	0.00%
sv009	43734	7.81%	0	0.00%
小計	154748	27.62%	405486	72.38%

に余分なアドレスを必要とする点でプライベートネットワークに適している．

本手法を応用して接続の二重化を行うことで信頼性を向上させるためには，障害発生の検知とルーティングの切替え機構を実現する必要がある．通常のマルチホームの場合は，外部からの経路情報によって経路の切替えが行われる．しかし，本手法では内部のポリシーのみで経路選択を行うため，別に経路選択のための機構を用意する必要がある．4 章における実現例では，経路選択のために CISCO 7204 の経路選択を用いている．この構成で CISCO 7204 が外部からルーティング情報を受け取り，自分に有利な経路選択を行って動的に経路を選択することは可能である．しかし，現在の運用においては，経路情報に対する費用負担の問題から，静的な経路選択を行っている．動的な経路選択について，具体的にどのような基準で経路選択を行えばよいか，経路の障害をどのように検出するか，などの問題について検討する必要がある．同様に，負荷分散の観点から，外部からの参照も含めて回線負荷を動的にバランスさせる機構の実現も求められる．

謝辞 CISCO ルータに関する技術情報および的確な助言をいただきましたネットワンシステムズ（株）田木孝司氏に感謝いたします．

参 考 文 献

1) 梶田，結縁：NAT によるプライベートネットワークの準マルチホーム化技法，情報処理学会研究報告，Vol.99, No.98, pp.73–78 (1999).
2) Berkowitz, H.: To be multihomed: Requirements & Definitions, Internet-Draft. http://www.ietf.org/internet-drafts/draft-berkowitz-multirqmt-02.txt (1999).
3) Hawkinson, J. and Bates, T.: Guidelines for creation, selection, and registration of an Autonomous System (AS), RFC1930 (Mar. 1996).
4) Egevang, K. and Francis, P.: The IP Network Address Translator (NAT), RFC1631 (May 1994).
5) Srisuresh, P. and Holdrege, M.: IP Network Address Translator (NAT) Terminology and Considerations, RFC2663 (Aug. 1999).
6) 山里，梶田，濱口，結縁：名古屋大学情報メディア教育システムの現状と課題，情報処理学会分散システム/インターネット運用技術研究会，情報処理学会分散システム/インターネット運用研究会報告，Vol.99, No.98, pp.55–60 (1999).

(平成 13 年 5 月 8 日受付)
(平成 13 年 10 月 16 日採録)

梶田　将司（正会員）

平成 2 年名古屋大学工学部情報工学科卒業．平成 7 年同大学院工学研究科情報工学専攻博士課程満了．名古屋大学工学部助手．平成 10 年同情報メディア教育センター助手．工学博士．専門は音声情報処理，e-Learning 全般．日本音響学会第 15 回粟屋潔学術奨励賞，電子情報通信学会第 56 回論文賞受賞，電子情報通信学会，日本音響学会，日本教育工学会，IEEE 各会員．

結縁　祥治

平成 2 年名古屋大学大学院博士後期課程満了．現在，名古屋大学大学院工学研究科助教授．並行計算モデルの応用面から，プロセス代数の確率モデルへの拡張および実時間性への拡張に関する研究に従事．形式的な手法による実際的なソフトウェアのモデル化に興味を持っている．