分散システム／インターネット運用技術 16−13
（1999. 11. 26）

# 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

梶田将司　　結縁祥治

名古屋大学情報メディア教育センター

〒464-8603 名古屋市千種区不老町1
{kajita, yuen}@media.nagoya-u.ac.jp

あらまし 本稿では，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実現を示す．

キーワード NAT，マルチホーム，プライベートアドレス，経路制御

# A Semi-Multihoming Technique Using Network Address Translator

Shoji Kajita　Shoji Yuen

Center for Information Media Studies, Nagoya University

Furo-cho 1, Chikusa-ku, Nagoya 464-8603 JAPAN
{kajita, yuen}@media.nagoya-u.ac.jp

**Abstract** 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 of our technique at CIMS, Nagoya University.

**Key words** NAT, Multihome, Private address, Routing Policy

# 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及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毎にAS(Autonomous System) 番号を取得し，経路制御を行う必要がある [1]．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，ある程度の規模をもったネットワークに1つのAS番号を割り当てざるを得ない．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) 既に対外接続があり，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．

本稿では，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．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[1]，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の運用に用いている機器構成及び設定を示す．

[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 NATによる準マルチホーム化

## 2.1 基本概念

本稿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．従って，$N_{in}$ 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．

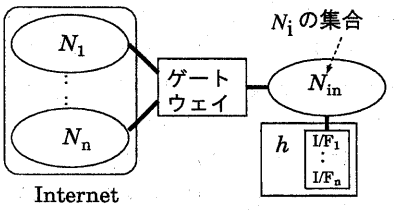


図 1: NATなしの準マルチホーム化

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，あまり一般的とは言えないので，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[2])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個所，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

[2]2個所以上の接続についても同様の方法で拡張できる．

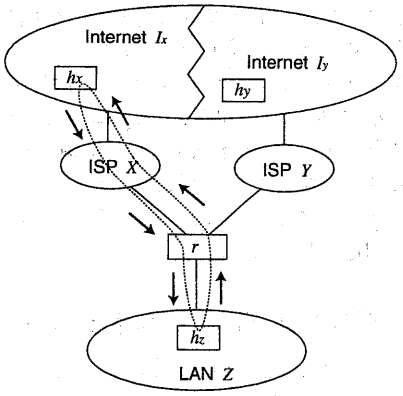


図 2: 内部ホストを起点とする場合のパケットの流れ

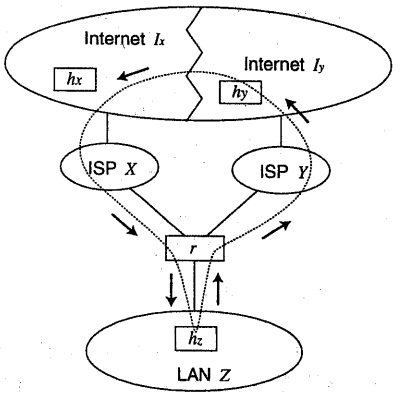


図 3: ISP $X$ を経由した場合の外部ホストを起点とする場合のパケットの流れ

$X$ 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 $T_x : N_z \to N_x$，$T_y : N_z \to N_y$, $T_z : (N_x \cup N_y) \to N_z$ 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．

$$\mathsf{nat}(P(s,d)) = \begin{cases} P(T_x(s),d) & \text{if } s \in N_z \\ & \text{and } d \in I_x \\ P(T_y(s),d) & \text{if } s \in N_z \\ & \text{d } d \in I_y \\ P(s,T_z(d)) & \text{otherwise} \end{cases}$$

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 [3]．

この場合，内部ホストと外部ホスト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，パケット $P(h_z, e)$ をルータ $r$ に送信する．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 $T_x : h_z \to T_x(h_z)$ を登録する．そして，$e \in I_x$ ならば ISP $X$ へ，$e \in I_y$ ならば ISP $Y$ へ転送される．復路では，$P(T_x(h_z), e)$ 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 $T_x^{-1}$ により $P(e, h_z)$ に変換される (図2参照)．□

(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 $T_x(h_z)$ 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 $P(e, T_z(T_x(h_z))) = P(e, h_z)$ に変換され，アドレス変換 $T_z : T_x(h_z) \to h_z$ が NAT に登録される．これに対する応答は，$T_z^{-1}$ により，$P(T_z^{-1}(h_z), s) = P(T_x(h_z), s)$ としてルータ $r$ から発信される．$T_y(h_z)$ 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

[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] $T_x$, $T_y$, $T_z$ は 1 対 1 変換である．

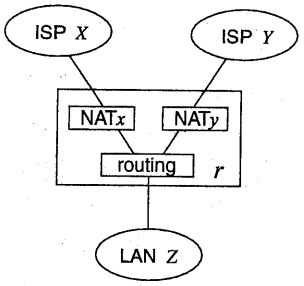

図 4: 分割NATテーブル

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，例えば，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言えず，保守や維持管理の点から望ましいとは言えない．さらに，ISP毎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[3]．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$\mathsf{nat}_x$, $\mathsf{nat}_y$は以下のように与えられる．

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

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

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$\mathsf{NAT}_x$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$\mathsf{nat}_y$によって$P(h_x,h_z)$と変換され，その変換$T_z : T_y(h_z) \to h_z$が$\mathsf{NAT}_y$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，$\mathsf{nat}_x^{-1}$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$\mathsf{NAT}_x$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割り当てによる解決

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$T_x(h_z)$及び$T_y(h_z)$がNATによりどちらも$h_z$に変換される[5]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[6]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ルーティングにより決定する．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[7]．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$h_x \in I_x$であれば，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$\mathsf{NAT}_x$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

[5] $T_z(T_x(h_z))) = T_z(T_y(h_z)) = h_z$
[6] エイリアス IP アドレスとも呼ばれる．
[7] $dom(T)$は変換$T$の定義域を表す．

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$T_z : T_x(X(h_z)) \rightarrow X(h_z)$が$\mathrm{NAT}_x$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 $X$経由であることがわかり，$\mathrm{NAT}_x$の$T_z^{-1}$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$T_z : T_y(Y(h_z)) \rightarrow Y(h_z)$が$\mathrm{NAT}_y$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 $Y$経由であることがわかるので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割り当て及びソースルーティングを行うことにより，準マルチホーム化が可能となる．

この構成自体は，2.1章におけるNATを用いない場合に近い．しかし，NATを用いることによって異なったネットワークアドレスを単一のネットワークアドレスに変換できるため，2.1章のようなネットワーク機器に対する特別な機能の要求はなく，一般的なネットワーク機器を用いることができる．

さらに，NATテーブルは外部接続ごとに独立しているため，一般的なNAT機能をもつゲートウェイ装置を接続先毎に個別に設置することができる．これにより，複数の独立した接続を確保することができ，個別のゲートウェイ機器に障害が発生してもソースルーティングを変更するだけで済む．

# 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[4]．

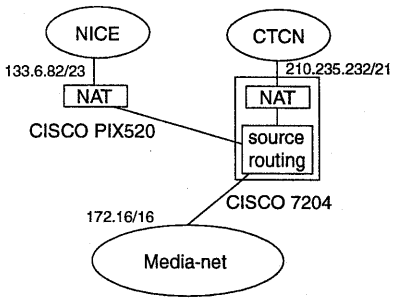


図 5: 本センターでの準マルチホームの運用構成

## 4.1 機器及びネットワーク構成

本センターのネットワーク機器及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全て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，現在のところ，CTCN側より国内向け非学術サイトの情報の供給を受けている．それ以外の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．

## 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．

(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

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 まとめ

本稿では，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について述べ，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について紹介した．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[3]．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．

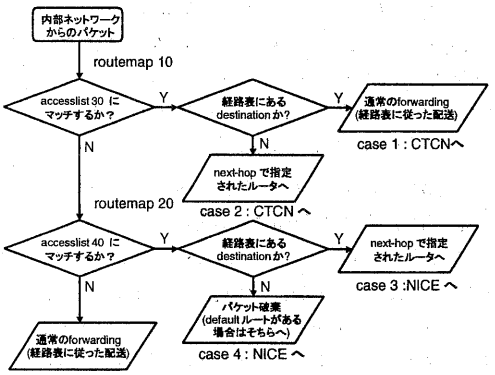


図 7: CISCO 7204の動作フロー

## 謝辞

CISCO ルータに関する技術情報及び的確な助言を頂きましたネットワンシステムズ(株)田木孝司氏に感謝致します．

## 参考文献

[1] J. Hawkinson and T. Bates: "Guidelines for creation, selection, and registration of an Autonomous System (AS)", RFC1930, March 1996

[2] K. Egevang and P. Francis: "The IP Network Address Translator (NAT)", RFC1631, May 1994

[3] P. Srisuresh and M. Holdrege: "IP Network Address Translator (NAT) Terminology and Considerations", RFC2663, August 1999

[4] 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，1999年11月(発表予定)