情報処理学会論文誌 Vol. 52 No. 12 3745–3754 (Dec. 2011)

推薦論文

インバウンド接続に適用可能なNAT によるマルチホーム化手法

金 勇[†1] 山口拓哉[†1] 山井成良[†2]
岡山聖彦[†2] 中村素典[†3]

近年のインターネットの普及と利用者の増加にともない，よりいっそう特定のサーバにアクセスの集中や増加が懸念され，それらを安定かつ効率良く処理していく方法としてマルチホームネットワーク化が注目されている．本論文では，管理が容易である NAT ルータを利用したマルチホームネットワーク化について考える．NAT ルータを利用したマルチホーム化には，NAT ルータの用途によっては，通信経路制御を行う際に特定の経路に負荷がかかるという問題点や通信そのものが行えないという問題点が生じる．また，特定の経路に負荷がかからないようにし，通信を行えるように設定を行った場合でも，サーバ側に本来期待しているアクセス元のログが残らないという問題が生じる．そこで本論文では，ソースルーティングオプションを利用した解決手法を提案する．本提案手法では，ソースルーティングオプションを利用して，送信元アドレスを変更することなく，往路と復路の通信経路が同一のものとなるようにする．本研究ではこのような機能を持つ NAT ルータを設計および実装し，提案手法の動作を確認するため，実験ネットワークを構築し実験を行い，通信経路制御ができていること，期待しているアクセス元のログが残っていることを確認した．

NAT-based Multihoming Method Applicable to Inbound Connection

Yong Jin,[†1] Takuya Yamaguchi,[†1] Nariyoshi Yamai,[†2]
Kiyohiko Okayama[†2] and Motonori Nakamura[†3]

With wide spread of the Internet and increasement of the Internet users, the concentrated accesses to a specific server becomes a critical problem. Multihoming network is attracted attention to provide stable and efficient Internet services. In this paper, we focus on the multihoming technology using NAT router which is easy to administrate. However, when control route selection using NAT router, problems occur in terms of load balancing and communication failure. Also, the problem that the log of the original access does not remain in the server causes. Thus, in this paper, we propose a new method to solve the problems by using loose source and record route option that can control the communication route without changing the source IP address. It is expected to make the bound and return communication route identical without changing the source IP address by using loose source and record route option. We also designed and implemented a NAT router with loose source and record route function. According to the result of experiments, we can confirm that the proposal system can control the communication route with remaining the access log as expected.

1. はじめに

近年，インターネットは社会的な情報基盤として広く利用され，WWW，電子メールのようなサービスを単に提供するだけでなく，これらを高速かつ安定的に提供することが重要視されるようになってきている．このような要求に対処する 1 つの方法として，自組織ネットワークを複数のバックボーンネットワーク（以下，単にバックボーンと呼ぶ）と接続し，通信先や途中のネットワークの状態に応じて利用するバックボーンを使い分けることにより通信速度や耐障害性の向上を図るマルチホームネットワークが注目されている．

マルチホームネットワークの構成方法として，AS（Autonomous System）番号取得による方法[1]，アプリケーションゲートウェイ（Application Level Gateway，以下 ALG）による方法[2),3)]，ネットワークアドレス変換（Network Address Translation，以下 NAT[4)]）による方法[5)–7)] などがあげられる．このうち，NAT を利用する方法は他の方法と比較して，導入コストや運用コストが比較的小さい，利用可能な通信プロトコルの制約が少ない，などの利点がある点で優れている．

ところが，この方法では組織外から接続される通信（以下，インバウンド接続）におい

†1 岡山大学大学院自然科学研究科
Graduate School of Natural Science and Technology, Okayama University
†2 岡山大学情報統括センター
Center of Information Technology and Management, Okayama University
†3 国立情報学研究所
National Institute of Informatics
本論文の内容は 2011 年 9 月の FIT2011 第 10 回情報科学技術フォーラムにて報告され，同プログラム委員長により情報処理学会論文誌ジャーナルへの掲載が推薦された論文である．

て，復路すなわち組織内から組織外への経路が往路と一致せずに通信不能になるなどの問題があるため，インバウンド接続への適用が困難であった．

そこで本研究では NAT を利用しながらインバウンド接続についても適用可能なマルチホーム化手法を提案する．この手法では NAT ルータにおいてソースルーティング用 IP オプションの 1 つである LSRR（Loose Source and Record Route）オプション[8] を追加することにより往復の経路の一致を可能にする．これにより NAT を用いたマルチホーム化方法の利点を活かしながら，インバウンド接続についてもマルチホームネットワークの利点を享受することが可能になる．

以下では，まず 2 章では従来のマルチホーム化方法とその問題点について述べる．次に 3 章では NAT を利用したマルチホーム化手法の問題点を詳述し，またその解決手法を提案する．4 章では提案手法の評価および考察を行う．最後に，5 章では結論と今後の課題について述べる．

2. 従来のマルチホーム化方法とその問題点

マルチホームネットワークの構成方法としては，1 章で述べたように，AS 番号取得による方法（方法 1），ALG による方法（方法 2），NAT による方法（方法 3）があげられる．以下ではこれらの方法とその問題点について述べる．

2.1 AS 番号取得によるマルチホーム化

現在，インターネットではネットワーク全体を AS と呼ばれる部分ネットワークの集合として扱い，AS 間で BGP4（Border Gateway Protocol version 4）[9] を用いて経路情報の交換を行う方法が一般的に用いられている．方法 1 は自組織のネットワークを AS として扱って AS の識別番号（AS 番号）を取得し，各バックボーンとの間で経路情報を交換して経路制御を行う方法である．この方法は組織内ネットワークとインターネットとの通信はネットワーク層レベルで冗長化でき，組織内外のホストにはいっさい変更を加える必要がないという利点を持つ．しかし，現状では BGP4 の運用が必須であり，これに関して次のような問題がある．

(1) BGP4 の運用には高い技術レベルと管理コストが必要になるため，BGP4 による経路制御機能を提供していない ISP（Internet Service Provider）が多数存在する．また，同機能を提供している ISP を利用したとしても金銭的なコストが大きい．

(2) 経路制御が宛先アドレスにのみ依存して行われ，現在の通信量などバックボーンの利用状況が反映されないため，通信先に偏りがあった場合に特定のバックボーンにトラフィックが集中する可能性がある．

(3) 経路制御が往路と復路で独立して行われるため，往復の経路が同一とは限らない．このため，たとえ往路（復路）で適切なトラフィック分散が行われていた場合でも復路（往路）のトラフィックが同一の経路に集中する可能性がある．

2.2 ALG によるマルチホーム化

方法 2 は，電子メールや WWW などの一部のアプリケーションにおいて，各バックボーンに属するアドレスを持つ ALG を導入し，これらの ALG を経由して組織内と組織外との間で通信することによりマルチホームネットワークを実現する方法である．この方法では，組織内から組織外へ接続される通信（アウトバウンド接続）については ALG が経路選択機能[⋆1] を持つことにより適切なバックボーンを選択することが可能になる．また，インバウンド接続については，たとえば組織内サーバに関する DNS 問合せに対して適切な ALG の IP アドレスを応答する手法[10)–13)] などにより適切なバックボーンを選択させることが可能である．したがって，方法 1 の欠点である，管理・運用コストの問題は比較的低減され，また経路選択機能の工夫により効果的なトラフィック分散を行うことも可能である．

一方，この方法では次のような問題がある．

(1) 適用可能なプロトコルが HTTP，SMTP など ALG に対応した一部のものに限られる．一般に 1 台の ALG を経由して複数の相手と通信を行う場合があるため，たとえば SMTP における宛先メールアドレスと MTA のように，最終的な通信先と経由する ALG とを個別に指定できるプロトコルしか利用できない．

(2) 特にインバウンド接続に適用する場合，組織内のサーバでは ALG がクライアントであると見なされ，実際のクライアントの情報の一部（IP アドレスなど）が失われる．その結果，たとえば IP アドレスに基づくアクセス制御に影響を及ぼす，あるいはサーバではクライアントの正しいアクセスログを記録できないなどの制約が生じる．

2.3 NAT によるマルチホーム化

方法 3 は，各バックボーンから個別の IP アドレスの割当てを受け，組織外と組織内との通信の際に NAT を用いて組織内の IP アドレスとバックボーンから割り当てられたアドレスとを相互変換することによりマルチホームネットワークを構成する方法である[5)–7)]．この方法では方法 2 と同様に管理・運用コストを方法 1 と比べて軽減することが可能になるだ

⋆1 通常の hop-by-hop の経路ではなく，end-to-end の経路を選択する機能であるため，本論文では経路選択と呼ぶことにする．

けでなく，適用可能なプロトコルの制約も方法 2 と比べて少ないため，広範囲に適用可能である．その意味で，この方法は他の方法より優れているといえる．

しかし，特にインバウンド接続に対しては，以下のような問題がある．

(1) 組織外から組織内への往路のパケットに対して宛先 IP アドレスだけが変換される場合には，変換後のパケットにはどちらのバックボーンを経由したかを示す情報が含まれていないため，組織内から組織外への復路のパケットをどちらのバックボーンに中継すればよいか判断が困難である．

(2) 組織外から組織内への往路のパケットに対して宛先 IP アドレスに加えて送信元 IP アドレスも変換される場合には，組織外のクライアントの IP アドレスが失われる．その結果，たとえば IP アドレスに基づくアクセス制御に影響を及ぼす，あるいはサーバではクライアントの正しいアクセスログを記録できないなどの制約が生じる．

この問題の詳細については次章で述べる．

3. インバウンド接続に適用可能な NAT によるマルチホーム化

前章で述べたように，既存のマルチホーム化方法にはいずれも問題がある．そこで，本章ではこれらのうち最も適用範囲が広い方法 3 に基づき，これをインバウンド接続にも適用できるように拡張する手法を提案する．

3.1 対象となるシステム構成

対象とするマルチホームネットワークの典型的な構成例を**図 1** に示す．この図では，組織内ネットワークは ISP A とは普通のルータ（図中の R）を介してインターネットに接続され，組織内ネットワークでは ISP A から割り当てられたグローバル IP アドレスが使用

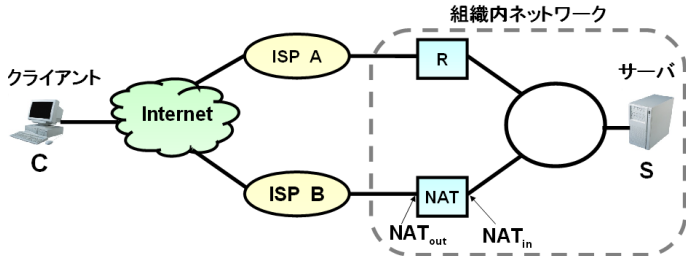

図 1　マルチホームネットワーク構成例
Fig. 1　Multihomed network configuration.

される．また，ISP B とは NAT 機能を持つルータ（図中の NAT．以下，NAT ルータ）を介して接続され，ISP B から割り当てられたアドレスと組織内ネットワークで用いられるアドレスを相互変換する役割を果たす．ルータと NAT ルータは物理的に離れた場所に設置されていてもかまわない．

この構成において，組織内ネットワークではプライベート IP アドレスを用いてもよい．その場合，ISP A との接続にも NAT ルータが用いられ，また組織内ネットワークにおける組織外へのデフォルト経路は ISP A 経由になっているものとする．また，組織内ネットワークに設置されているホスト（図中のサーバなど）の管理者は組織内ネットワークの管理者とは必ずしも一致するとは限らないものとする．

このようなネットワーク構成は中小規模の組織では比較的よく見られるか，あるいは容易に採用できると思われる．

3.2 インバウンド接続における問題点

本論文ではこれ以降図 1 において，インターネットに接続されているクライアントから組織内ネットワークに接続されているサーバへの TCP インバウンド接続に対する経路選択について議論する．なお，UDP インバウンド接続については 4.3 節において考察する．

同図における経路選択機能は，方法 2 の場合には比較的容易に実現できる．すなわち，図 1 の NAT ルータの代わりに ALG を設置し，クライアントからサーバへのアクセスに先だって行われる DNS による名前解決において，サーバあるいは ALG のグローバル IP アドレスのうち適切なほうを応答する方法[10)–13)] を適用すればよい．

方法 3 の場合においても，基本的には方法 2 と同様の手法を適用することが考えられる．この手法では，NAT ルータに対して ISP B から割り当てられているグローバル IP アドレスのうちの 1 つ（以下，$\mathrm{NAT_{out}}$）をサーバ用として選び，$\mathrm{NAT_{out}}$ とサーバのグローバル IP アドレス（以下，S）とを 1 対 1 で相互変換するようにあらかじめ NAT ルータを設定する．これにより，事前の名前解決において S あるいは $\mathrm{NAT_{out}}$ のうちの適切なほうを組織内ネットワーク側の DNS サーバが応答すれば，往路については応答に応じて ISP A あるいは ISP B を経由させることができる．

しかし，この手法では復路についてはうまく経路選択を行うことができない．その場合の往復のパケットの流れを**図 2** に示す．

同図において往路の経路として ISP B が選択された場合，クライアントの IP アドレスを C とすると，クライアントからサーバへのパケットは送信元アドレスが C，宛先アドレスが $\mathrm{NAT_{out}}$ として NAT ルータに送られる（同図 (1)）．NAT ルータでは $\mathrm{NAT_{out}}$ と S との

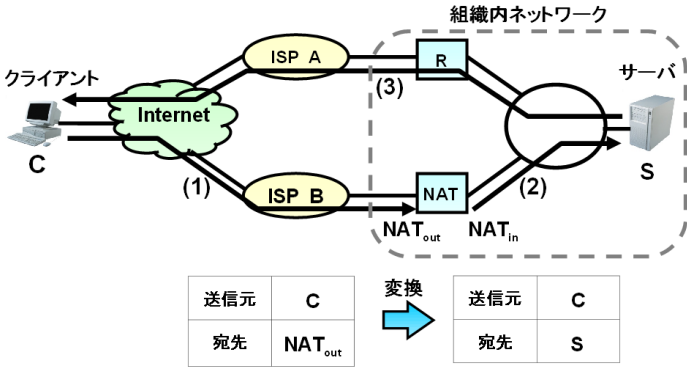

図 2　NAT 利用時のパケットの流れ（往復経路不一致例）
Fig. 2　Packet flow of NAT (Inconsistency of bound and return routes).

間で相互変換が行われるため，クライアントから受信したパケットは宛先アドレスが S に変換され，サーバに中継される（同図 (2)）．このとき，送信元アドレスは C のままであることに注意する．サーバでは応答として送信元アドレスが S，宛先アドレスが C であるパケットをクライアントに送信する．ところが，組織内ネットワークではインターネットへのデフォルト経路は ISP A 経由であるため，このパケットは NAT ルータを経由せずにクライアントに配送される（同図 (3)）．その結果，クライアントでは送信したパケットの宛先 $\mathrm{NAT_{out}}$ とは異なる送信元 S からパケットを受信することになり，クライアント・サーバ間で正しく通信が行われない．

一方，この問題に対して NAT ルータでクライアントのアドレスも変換する手法が考えられる．この手法では $\mathrm{NAT_{out}}$ と S との相互変換だけでなく，C と NAT ルータの組織内ネットワーク側アドレス（以下，$\mathrm{NAT_{in}}$）との相互変換も行うようにする．その場合の往復のパケットの流れを**図 3** に示す．

同図において往路の経路として ISP B が選択された場合，クライアントからサーバへのパケットは同様に送信元アドレスが C，宛先アドレスが $\mathrm{NAT_{out}}$ として NAT ルータに送られる（同図 (1)）．NAT ルータでは $\mathrm{NAT_{out}}$ と S との間および C と $\mathrm{NAT_{in}}$ との間で相互変換が行われるため，クライアントから受信したパケットは送信元アドレスが $\mathrm{NAT_{in}}$，宛先アドレスが S に変換され，サーバに中継される（同図 (2)）．サーバでは応答として送信元アドレスが S，宛先アドレスが $\mathrm{NAT_{in}}$ であるパケットを送信する（同図 (3)）．このパケットは宛先である NAT ルータが受け取り，送信元アドレスが $\mathrm{NAT_{out}}$，宛先アドレスが C に変換した後にクライアントに配送される（同図 (4)）．その結果，前例とは異なり，クライアント・サーバ間の通信自体は正しく行われる．

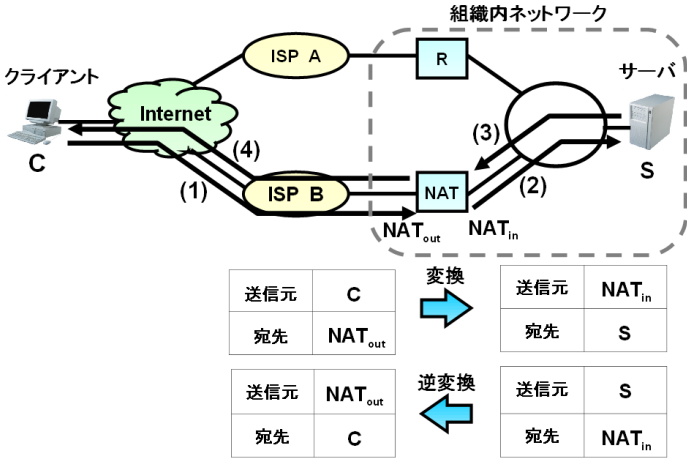

図 3　NAT 利用時のパケットの流れ（クライアント情報損失例）
Fig. 3　Packet flow of NAT (Loss of client information).

しかし，この手法では方法 2 と同様の問題が新たに生じる．すなわち，サーバではクライアントの IP アドレス情報が失われるため，アクセスログの記録やアクセス制御などに制約が生じる．

3.3　インバウンド接続における復路の経路選択

前節で述べた問題点の本質的な原因は，復路の経路選択がフロー単位で行えない点にある．組織内ネットワークの機器のうち，NAT ルータだけがフローを識別する機能を有するため，図 1 において NAT ルータが ISP A，B の両方に接続されている場合には NAT ルータが復路の経路選択を行うことが可能であるが，そうでない場合にはクライアントの IP アドレスを維持したままフロー単位で復路の経路を指定できる機能が必要になる．

そこで，本論文では前節で述べた問題点を解決する手法として，IP オプションの 1 つである LSRR（Loose Source and Record Route）オプションを用いる手法を提案する．提案手法を用いた場合の動作を，**図 4** を用いて説明する．

同図において往路の経路として ISP B が選択された場合，クライアントからサーバへの

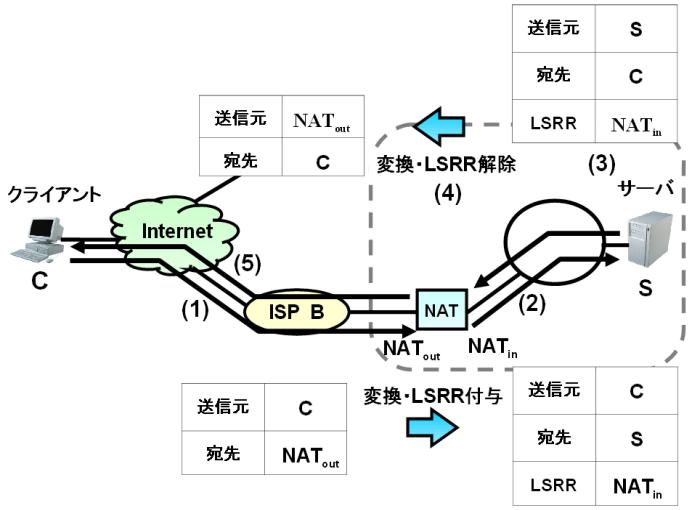

図 4　LSRR オプションによる復路の経路選択
Fig. 4　Return route selection using LSRR option.

パケットは送信元アドレスが C，宛先アドレスが NAT_{out} として NAT ルータに送られる（同図 (1)）．ここで，従来と同様に NAT ルータでは NAT_{out} と S との間で相互変換が行われるため，クライアントから受信したパケットは宛先アドレスが S に変換される．さらに NAT ルータはこのパケットに対して NAT_{in} を経由してきた直後に見えるように LSRR オプションを追加した後，サーバに中継する（同図 (2)）．我々の調査の範囲では，Windows 系を除く多くのオペレーティングシステムでこのオプションはフロー単位で有効であり，サーバがクライアントに対して応答パケットを送出する際にはちょうど逆の経路をたどるように LSRR オプションを付加する．したがって，サーバが送出するパケットは送信元アドレスが S，（最終の）宛先アドレスが C となり，さらに LSRR オプションとして NAT_{in} を経由するように指定されることになる（同図 (3)）．NAT ルータはこのパケットを受け取ると，まず LSRR オプションを削除し（同図 (4)），さらに送信元アドレスを S から NAT_{out} に変更してクライアントに配送する（同図 (5)）．

これにより，クライアント・サーバ間の通信はフロー単位で LSRR オプション中に経由した経路（LSRR オプションが存在しない場合にはデフォルト経路）が記録され，これに従って復路の経路選択に利用されるだけなく，クライアントの IP アドレスはパケット中にそのまま残されるため，これを用いてアクセス制御を行ったりアクセスログを残したりすることが可能となる．

3.4　Path MTU の減少への対処

提案手法では NAT ルータで 8 バイトの LSRR オプションを追加するため，クライアントからサーバへのパケットを NAT ルータが中継する際，受信したパケットの大きさによっては送出するパケットの大きさが MTU を超過する場合がある．このとき，DF（Do not Fragment）フラグが設定されていると，パケットの細分化（fragmentation）を行えないためサーバへの送出に失敗することになる．また，DF フラグが設定されていない場合には細分化が行われるためサーバへの送出には成功するが，細分化のためのオーバヘッドが余分にかかることになり，好ましくない．この問題はクライアントから見ると，Path MTU の減少と等価である．

そこで，本節ではこの問題への対処法を検討する．

なお，サーバからクライアントへのパケットについてはサーバ自身が LSRR オプションを付加し，ペイロードサイズの減少をサーバ自身が検知できるため，上記の問題は生じない．

3.4.1　MTU の通知

通常の場合，ルータは MTU 超過のためにパケットの送出に失敗した場合，送信元に対して宛先到達不可（Destination Unreachable Message – Fragmentation needed and DF set）を意味する ICMP（Internet Control Message Protocol）メッセージを送付する．このメッセージにはルータの正しい MTU が含まれているため，送信元はその値に Path MTU を更新し，これを超えないように調整してパケットの再送信を行うことができる．

提案する NAT ルータにおいても，これと同様の方法で新しい MTU を送信元に通知することが可能である．ただし，通知する MTU は LSRR オプションの追加分 8 バイトを見込んで実際のインタフェースの MTU より 8 バイトを減じた値[⋆1]とする．

なお，一部の環境あるいはソフトウェアでは Path MTU の減少を認識できず，通信に支障をきたす可能性がある[14]．しかし，Path MTU の減少はたとえば L2TP[15] などの IP トンネリング技術を用いる場合にも生じる問題で，提案手法特有の問題ではない．

3.4.2　SYN パケットのみへの LSRR オプションの付加

提案方法はフロー単位で有効であることから，OS 内部では付加された LSRR オプションをコネクション確立時にフロー単位で記録していると推察できる．その場合，NAT ルータ

⋆1 たとえば MTU が 1,500 バイトのイーサネットの場合，1,492 バイトとなる．

はクライアントから最初に送られる SYN フラグ付きパケット（以下，SYN パケット）のみに LSRR オプションを付加すれば，それ以外のパケットについては LSRR オプションの付加が不要になり，その結果クライアントから見た見かけ上の Path MTU は変わらないことになる．また，これにより LSRR オプション付加によるオーバヘッドの軽減も図ることができる．

なお，この方法が有効に機能するのであれば原則的にパケットの細分化が発生しないため，ICMP による MTU の通知は不要になり，また何らかの理由で通知を行う場合でも実際のインタフェースの MTU より 8 を減じる必要がなくなる．

3.5　NAT ルータの実装

これまでに述べた手法に基づき，我々は LSRR オプションの追加・削除機能を持つ NAT ルータの試作を行った．本節ではその実装方法を述べる．なお，前節で述べた Path MTU の減少については，試作 NAT ルータにおいてすべてのパケットの LSRR オプションを付加し，これにより MTU を超える場合には ICMP メッセージを返すもの（以下，試作 NAT ルータ 1）および SYN パケットだけに LSRR オプションを付加するもの（以下，試作 NAT ルータ 2）のそれぞれを実装した．

試作 NAT ルータは FreeBSD 7.2 上で自作プログラムとして実装した．試作 NAT ルータの構成を**図 5** に示す．同図に示すように，内部には 2 つのプログラムがあり，プログラム 1 は宛先アドレスの変換と LSRR オプションの付加，プログラム 2 は送信元アドレスの変換と LSRR オプションの削除を行う．これらのプログラムへのパケットの受け渡しは，FreeBSD の IPFW（IP FireWall）機能[16] により divert ソケット[17] を介して行われる．試作 NAT ルータ 1 において MTU を超える場合の ICMP メッセージの送信はプログラム 1 が行う．

なお，試作 NAT ルータが有効に機能するためには，OS のカーネルパラメータ net.inet.ip.sourceroute を 1 に設定する必要があることに注意する．この設定を怠ると，サーバから受信した LSRR オプション付きパケットがプログラム 2 に渡される前にカーネルにより廃棄されるため，動作しない．

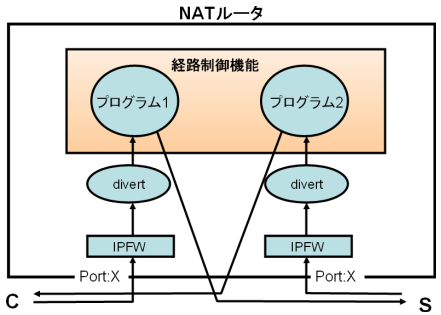

図 5　試作 NAT ルータの構成
Fig. 5　Configuration of prototype NAT router.

4.　試作 NAT ルータの評価と考察

本章では試作した NAT ルータの機能や性能を評価するために行った実験について述べる．また，提案手法の適用範囲について考察する．なお，以下のすべての実験では試作 NAT ルータ 1，2 の両方を用いた．

4.1　動作確認実験

まず，試作した NAT ルータを用いてクライアント・サーバ間で正しく通信が行えるかどうかを確認するため，動作確認実験を行った．実験環境を**図 6** に示す．また，各 PC の諸元を**表 1** に示す．この環境においてクライアント PC1，サーバ PC2 ともデフォルト経路はルータの役割を果たす PC4 を経由するように設定した．また，サーバ PC2 では OS を FreeBSD 7.1，CentOS 5.4，Windows 2003 Server，Windows 7 の 4 通りに変え，FTP サーバを動作させたうえでクライアント PC1 からアクセスさせた．

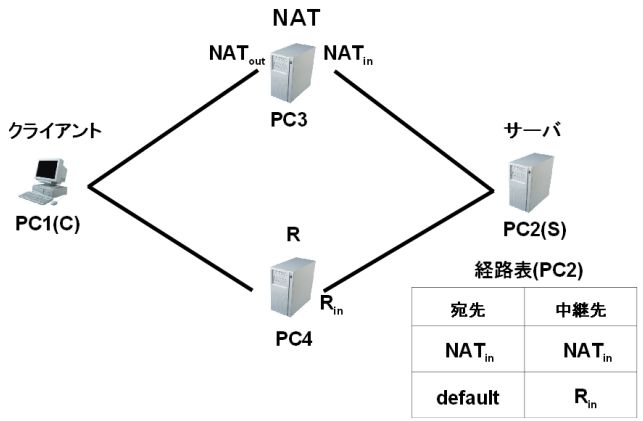

図 6　実験環境
Fig. 6　Evaluation environment.

表 1　各 PC の諸元
Table 1　Specification of each PC.

PC	CPU	メモリ	OS
PC1	i7 2.9 GHz	256 MB	FreeBSD 7.0
PC2	Pentium4 2 GHz	512 MB	FreeBSD 7.1 他
PC3	Pentium4 2 GHz	512 MB	FreeBSD 7.2
PC4	Celeron 564 MHz	128 MB	FreeBSD 7.0

まず，クライアントからサーバを直接指定してアクセスさせたところ，正常にアクセスできた．また PC3，PC4 において tcpdump [18] を用いて各リンクのパケットを観測したところ，クライアント・サーバ間の通信は往路，復路とも PC4 を経由していることを確認した．

次に，クライアントから NAT ルータ PC3 の組織外側アドレス NAT_{out} を指定してアクセスさせたところ，PC2 の OS が FreeBSD 7.1，CentOS 5.4 の場合には試作 NAT ルータ 1，2 のいずれにおいても正常にアクセスできることを確認した．ただし，いずれの OS においてもソースルーティング用オプション付きパケットの受信を有効にするカーネルパラメータ net.inet.ip.accept_sourceroute を 1 に設定する必要があった．また PC3，PC4 において各リンクのパケットを観測したところ，クライアント・サーバ間の通信は往路，復路とも PC3 を経由し，また PC3 で LSRR オプションの付加および削除が正しく行われていることを確認した．また，いずれの実験においても PC2 において FTP のアクセスログに PC1 の IP アドレスが記録されていることを確認した．

しかし，PC2 の OS が Windows 2003 Server および Windows 7 の場合には，ソースルーティング用オプション付きパケットの受信を有効にする方法が不明であったため，正常にアクセスできなかった．

これらの結果により，サーバ上でソースルーティング用オプション付きパケットの受信を有効にできる場合には，試作 NAT ルータ 1，2 のいずれにおいても LSRR オプション付加による復路の経路選択機能は有効に動作し，またサーバではいずれの経路を経由した場合でもクライアントの IP アドレスが保存されることが確認された．

4.2　性能評価実験

提案手法では NAT ルータにおいて 8 バイトの LSRR オプションの付加・削除がともなうため，通常の NAT ルータよりもオーバヘッドが大きいと予想される．そこで，試作 NAT ルータ 1，2 が通常のルータ，通常の NAT ルータと比較してどの程度のオーバヘッドを持つか調べるため，図 6 と同様の環境において性能評価実験を行った．サーバ PC2 の OS は FreeBSD 7.1 とした．

表 2　性能評価実験結果—インバウンド方向
Table 2　Result of performance evaluation–Inbound direction.

PC3 種別	スループット（Mbps）	通常ルータとの差（%）
通常ルータ	88.5	—
通常 NAT ルータ	88.3	0.2
試作 NAT ルータ 1	87.9	0.7
試作 NAT ルータ 2	88.2	0.3

表 3　性能評価実験結果—アウトバウンド方向
Table 3　Result of performance evaluation–Outbound direction.

PC3 種別	スループット（Mbps）	通常ルータとの差（%）
通常ルータ	89.6	—
通常 NAT ルータ	89.4	0.2
試作 NAT ルータ 1	89.0	0.7
試作 NAT ルータ 2	89.0	0.7

この実験では，図 6 における PC4 は用いず，PC3 を通常のルータ，通常の NAT ルータ，および試作 NAT ルータ 1，2 の 4 通りに切り替え，それぞれの場合において FTP を用いて 200 MB をデータをインバウンド方向（put コマンドを使用）とアウトバウンド方向（get コマンドを使用）に伝送した合計 8 通りについて TCP スループットの測定を行った．用いたネットワークの種類はすべて 100 BaseT である．

インバウンド方向のスループットの測定結果を**表 2**，アウトバウンド方向のスループットの測定結果を**表 3** に示す．これらの表から，いずれの場合でも提案手法ではオーバヘッドは十分小さく，実用上問題ない範囲といえる．また，オーバヘッドの違いは以下のように説明できる．

インバウンド方向のスループットについては，試作 NAT ルータ 1 では通常のルータと比べて 0.7%程度のスループットの低下が見られることが分かる．これはアドレス変換に要するオーバヘッドが 0.2%程度，見かけ上の Path MTU が 8 バイト減少した影響が 0.5%程度であることを考慮すると妥当な値といえる．また，試作 NAT ルータ 2 では見かけ上の Path MTU が減少しないため，通常の NAT ルータと同程度のスループットが得られていることが分かる．

一方，アウトバウンド方向のスループットについては，試作 NAT ルータ 1 でも試作 NAT

ルータ 2 でも，通常のルータと比べて 0.7%程度のスループットの低下が見られることが分かる．これはいずれの場合でもアウトバウンド方向にはすべてのパケットに LSRR オプションがサーバにより付加されるため，ペイロードサイズが 8 バイト減少した影響を受けたものと考えられる．

4.3　適用範囲に関する考察

提案手法の適用には様々な前提条件が必要となるため，対象や環境によっては提案手法が適用できない場合がある．そこで本節では提案手法の適用範囲について考察する．

4.3.1　LSRR オプションの無効化

現在，多くのネットワーク機器やホストでは，セキュリティ上の理由により LSRR オプションが標準的に無効化されている．したがって，提案手法はそのままでは多くの環境で利用することができず，ルータやホストで LSRR オプションを有効化するように設定変更を行う必要がある．しかし，その必要が生じるのは組織内ネットワークのルータおよびマルチホーム化のサービス対象となるホスト（サーバ）だけであり，組織外のネットワーク機器やクライアントでは設定変更の必要はない．

また，この手法を用いた場合でも組織外ネットワークから送信された LSRR オプション付きパケットは外部ネットワークとの接続部分で廃棄することが可能であるため，少なくとも組織外からの攻撃に対するセキュリティは低下しない．ただし，組織内ネットワークにおいては LSRR オプションの有効化により，たとえばアドレス広告のないネットワークにもゲートウェイの指定によりアクセスが可能になるなどの危険性が生じるため，ネットワークの構成や設定によっては注意が必要である．

4.3.2　UDP 通信への適用

UDP については TCP とは異なりコネクションの概念がないため，サーバからクライアントへ送信されるパケットが同一フローに属するかどうか判別することが通常は困難である．したがって，一般には UDP 通信については提案手法は適用できないと思われる．しかし，現在ではネットワーク上の多くのサービスがトランスポート層プロトコルとして TCP を用いており，この制約による影響は事実上それほど大きくないと思われる．

ただし，UDP を用いた重要なアプリケーションとして DNS がある．NAT を用いたマルチホーム化手法では，インバウンド接続の経路選択に DNS を利用すると想定しているため，DNS プロトコルについては往復とも同一の経路を経由するように対応する必要がある．この問題に対しては，たとえば NAT ルータが DNS サーバを兼ねる，あるいは NAT ルータ経由での問合せのみを受信し，応答を必ず NAT ルータ経由で送信するような DNS サーバを用意する，などの方法で対応可能である．

4.3.3　複数のサーバへの適用

組織内ネットワークに複数のサーバが存在する場合，クライアントが NAT ルータ経由でこれらにアクセスするには 1 台のサーバにつき 1 つの IP アドレスが必要である．現在，IPv4 のアドレスは枯渇しつつあるため，組織内に多数のサーバが存在する場合には IP アドレスの割当てが困難になることが今後予想される．

この問題については，ALG を用いたマルチホーム化でも同様であり，たとえば 1 つのアドレスに対してサービスの異なる複数のサーバを対応させ，宛先ポート番号に応じて変換後の宛先 IP アドレスを決定するような仕組みの導入などが対策方法として考えられる．

4.3.4　IPv6 環境への応用

IPv6 の場合には一般に各サーバは複数のアドレスを持つことができる．したがって，各 ISP から割り振られたアドレスを 1 つのサーバに割り当て，NAT 機能を導入することなくマルチホーム化を実現することが可能である．しかし，この場合にも各バックボーンの流入フィルタリング（ingress filetering）を回避するために往復の経路を一致させる必要があり，たとえば組織内ネットワークにおいて送信元アドレスに基づく経路制御機能の導入が新たに必要になる[19]．

この問題の 1 つの解決策として，提案手法の IPv6 環境への応用が考えられる．IPv6 においても routing header と呼ばれる拡張ヘッダ[20] を用いることにより，LSRR の指定と同様の効果を得ることが可能である．したがって，提案手法を IPv6 環境へ応用すれば，組織内ネットワークの広範囲に新たな経路制御機能を導入する必要がなく，提案手法に基づいて既存のネットワーク機器および対象ホストでの routing header の有効化を行うだけで往復の経路を一致させることができると思われる．

5. ま と め

本論文では，NAT ルータへ LSRR オプションを付加・削除する機能を導入することにより，インバウンド接続についても復路の経路選択を可能にするマルチホーム化手法を提案した．またこのような機能を持つ NAT ルータを試作し，実際に通信が行えること，オーバヘッドはたかだか 0.7%程度であることを確認した．これにより，導入コストや管理コストが比較的小さく利用可能な通信プロトコルの制約が少ないという NAT によるマルチホーム化方法の利点を活かしながらインバウンド接続についてもマルチホームネットワークの利点を享受することが可能になった．

今後の課題としては DNS を用いた動的トラフィック分散機能[10)–13)] と組み合わせ，実環境において動作検証および性能評価を行うことがあげられる．また，IPv6 環境においても提案手法を導入し，有効性を検証することもあげられる．

参 考 文 献

1) Hawkinson, J. and Bates, T.: Guidelines for creation, selection, and registration of an Autonomous System (AS), RFC 1930, IETF (1996).
2) 中川郁夫，上谷　一，鍋島公章，樋地正浩，今野幸典：マルチホーム環境におけるアプリケーションルーティング技術の提案，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研究報告，No.98-DSM-12-7, pp.37–42 (1998).
3) 山井成良，土居正行，岡山聖彦，中村素典：マルチホームネットワークにおける電子メールシステムの高信頼化運用手法，情報科学技術フォーラム情報技術レターズ，Vol.6, pp.373–376 (2007).
4) Srisuresh, P. and Egevang, K.: Traditional IP Network Address Translator (Traditional NAT), RFC 3022, IETF (2001).
5) 岡山聖彦，山井成良，島本裕志，宮下卓也，岡本卓爾：マルチホームネットワークにおける透過的な動的トラヒック分散，情報処理学会論文誌，Vol.41, No.12, pp.3255–3264 (2000).
6) 梶田将司，結縁祥治：NAT による準マルチホーム化技法，情報処理学会論文誌，Vol.42, No.12, pp.2818–2826 (2001).
7) 岡山聖彦，山井成良，久保武志，宮下卓也：マルチホームネットワークにおけるアプリケーションプロトコルの性質を考慮した動的トラフィック分散，情報処理学会論文誌，Vol.46, No.4, pp.1007–1016 (2005).
8) Postel, J. (Ed.): Internet Protocol, RFC 791, IETF (1981).
9) Rekhter, Y., Li, T. and Hares, S. (Eds.): A Border Gateway Protocol 4 (BGP-4), RFC 4271, IETF (2006).
10) Delgadillo, K.: Cisco DistributedDirector, Cisco Systems, Inc. (online), available from ⟨http://www.cisco.com/warp/public/cc/pd/cxsr/dd/tech/dd_wp.pdf⟩ (accessed 2011-06-23).
11) 下川俊彦，木場雄一，中川郁夫，山本文治，吉田紀彦：広域分散環境における DNS と経路情報を利用したサーバ選択機構，電子情報通信学会論文誌 B，Vol.J86-B, No.8, pp.1454–1462 (2003).
12) 金　勇，山井成良，岡山聖彦，清家　巧，中村素典：マルチホーム環境における DNS 応答の多重化による自組織宛メール配送の動的経路選択手法，情報処理学会論文誌，Vol.51, No.3, pp.998–1007 (2010).
13) Jin, Y., Yamai, N., Okayama, K. and Nakamura, M.: An Adaptive Route Selection Mechanism Per Connection Based on Multipath DNS Round Trip Time on Multihomed Networks, *Proc. 2010 10th Annual International Symposium on Applications and the Internet* (*SAINT 2010*), Seoul, Korea, IEEE-CS/IPSJ, pp.52–58 (online), DOI:10.1109/SAINT.2010.21 (2010).
14) Lahey, K.: TCP Problems with Path MTU Discovery, RFC 2923, IETF (2000).
15) Lau, J., Townsley, M. and Goyret, I. (Eds.): Layer Two Tunneling Protocol – Version 3 (L2TPv3), RFC 3931, IETF (2005).
16) Antsilevich, U.J.S., Kamp, P.-H., Nash, A., Cobbs, A. and Rizzo, L.: ipfw – IP firewall and traffic shaper control program, FreeBSD System Manager's Manual (online), available from ⟨http://www.freebsd.org/cgi/man.cgi?query=ipfw⟩ (accessed 2011-06-23).
17) Cobbs, A.: divert – kernel packet diversion mechanism, FreeBSD Kernel Interface Manual (online), available from ⟨http://www.freebsd.org/cgi/man.cgi?query=divert⟩ (accessed 2011-06-23).
18) Tcpdump/Libpcap: TCPDUMP/LIBPCAP public repository, Tcpdump/Libpcap (online), available from ⟨http://www.tcpdump.org/⟩ (accessed 2011-06-23).
19) Ohira, K. and Okabe, Y.: Host-Centric Site-Exit Router Selection in IPv6 Site Multihoming Environment, *Proc. 1st International Workshop on Protocols and Applications with Multi-Homing Support* (*PAMS 2011*), Biopolis, Singapore, IEEE-CS, pp.696–703 (online), DOI:10.1109/WAINA.2011.114 (2011).
20) Deering, S. and Hinden, R.: Internet Protocol, Version 6 (IPv6) Specification, RFC 2460, IETF (1998).

(平成 23 年 7 月 12 日受付)
(平成 23 年 9 月 12 日採録)

推 薦 文

問題点の指摘と解決方法の提示が明解に行われており，実装を用いた評価も行われており説得力に富む．よって推薦論文として十分な資質を兼ね備えていると考えられる．

（FIT2011 第 10 回情報科学技術フォーラムプログラム委員長　井宮　淳）

金　　勇（学生会員）

平成 21 年岡山大学大学院自然科学研究科電子情報システム工学専攻博士前期課程修了．現在，同大学院自然科学研究科産業創成工学専攻博士後期課程に在学中．主に管理の容易なマルチホームネットワーク構築技術に関する研究に従事．分散システム，ネットワークアーキテクチャ等に興味を持つ．

山口　拓哉（学生会員）

平成 23 年岡山大学工学部通信ネットワーク工学科卒業．現在，同大学大学院自然科学研究科（電子情報システム工学専攻）博士前期課程在学中．分散システム，ネットワークアーキテクチャ等に興味を持つ．

山井　成良（正会員）

昭和 59 年大阪大学工学部電子工学科卒業．昭和 61 年同大学大学院博士前期課程修了．昭和 63 年同大学院基礎工学研究科（物理系専攻情報工学分野）博士後期課程退学．同年奈良工業高等専門学校情報工学科助手．同講師，大阪大学情報処理教育センター助手，同大学大型計算機センター講師，岡山大学総合情報処理センター（現，情報統括センター）助教授を経て，平成 18 年より同教授．分散システム，ネットワーク運用管理，ネットワークセキュリティの研究に従事．IEEE，電子情報通信学会各会員．博士（工学）．

岡山　聖彦（正会員）

平成 2 年大阪大学基礎工学部情報工学科卒業．平成 4 年同大学大学院基礎工学研究科博士前期課程修了．同年同大学院基礎工学研究科博士後期課程を退学し，同大学工学部助手．奈良先端科学技術大学院大学情報科学研究科助手，岡山大学工学部助手，同大学総合情報基盤センター助教を経て，平成 22 年同大学情報統括センター助教．平成 23 年同准教授．博士（工学）．インタネットアーキテクチャ，ネットワーク管理，ネットワークセキュリティの研究に従事．電子情報通信学会会員．

中村　素典（正会員）

1994 年京都大学大学院工学研究科博士後期課程単位取得退学．立命館大学理工学部助手，京都大学経済学部助教授，京都大学学術情報メディアセンター助教授を経て，2007 年より国立情報学研究所教授，2008 年より総合研究大学院大学教授（併任），現在に至る．博士（工学）．IEEE，日本ソフトウェア科学会，電子情報通信学会各会員．コンピュータネットワーク，ネットワークコミュニケーション，認証連携等の研究に従事．