RL-001

IPv6 サイトマルチホーミングにおけるルーティングヘッダを用いたサイト出口ルータ選択手法

A Site Exit Router Selection Method with Routing Header in IPv6 Site Multihoming

山口 拓哉 † Takuya Yamaguchi
金　勇 ‡ Yong Jin
山井 成良 § Nariyoshi Yamai
岡山 聖彦 § Kiyohiko Okayama
中村 素典 ¶ Motonori Nakamura

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（World Wide Web），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一つの方法として，自組織ネットワーク（サイト）を複数の ISP(Internet Service Provider) 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ミング技術（サイトマルチホーミング）が注目されている．

IPv6 でのサイトマルチホーミングに関しては，IPv4 の場合とは異なり，サイト内のノードには各 ISP から委譲されたプレフィックスの範囲内のアドレスが 1 つずつ付与され，パケット送出時にはノードはそのうちの 1 つを選択して送信元アドレスとして用いる．ただし，多くの ISP ではセキュリティ上の理由から流入フィルタリング (ingress filtering)[1, 2] を実施しているため，これを回避するには送出されたパケットの送信元アドレスに対応した ISP を経由するように経路制御を行う必要がある．ところが，通常のサイトでは宛先アドレスにもとづく経路制御を行っているため，宛先アドレスが同じパケットは送信元アドレスに依らずに同一の ISP を経由し，結果として流入フィルタリングによりパケットが破棄される場合がある．これに対して，送信元アドレスに基いた経路制御（送信元アドレス依存経路制御．以下 SAD(source address dependent) ルーティング）[3] を用いる方式（たとえば [4]）が提案されている．この方式ではサイト内の広範囲で SAD ルーティングに対応したルータが必要となり，実環境への導入に問題が生じる．

そこで，本論文では IPv6 サイトマルチホーミングにおいてルーティングヘッダにより ISP との接続点となるルータ（サイト出口ルータ）を指定する方式を提案する．本方式ではサイト内のノードがサイト外に送信する場合に，送信元 IP アドレスに対応したサイト出口ルータの IP アドレスをルーティングヘッダにより指定する．これにより，サイト内のネットワークでは宛先アドレスに基づく通常の経路制御方式をそのまま用いながら，ISP による流入フィルタリングを回避することが可能になる．

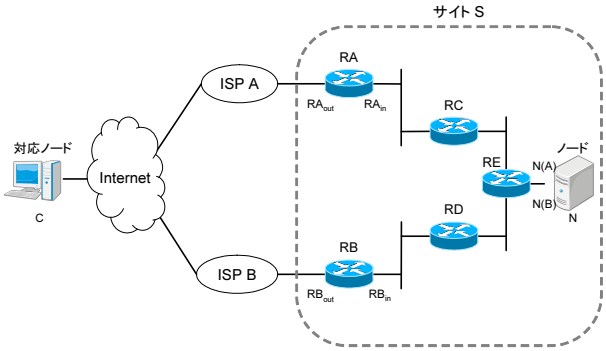

図 1: 典型的な IPv6 サイトマルチホーミングの構成

以下，まず 2 章では従来の IPv6 サイトマルチホーミング手法とその問題点について述べる．次に 3 章ではルーティングヘッダを用いた IPv6 サイトマルチホーミング手法を提案する．4 章では提案手法の評価及び考察を行う．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 IPv6 サイトマルチホーミングとその問題点

2.1 対象とするネットワーク構成

まず，本論文で対象とするネットワーク構成を図 1 に示す．サイト S は複数の ISP（図中では ISP A，B）に接続されてそれぞれからプレフィックスが委譲され，サイト内の各ノードはこれらのプレフィックスの範囲内のアドレスを 1 つずつ付与されている．サイト S と ISP A，B との接続点にはそれぞれサイト出口ルータ RA，RB が存在する．これらのルータは一般的には物理的に離れた場所に設置されており，異なったセグメントに属している．

以下の議論では，この図においてサイト S 内のノード N 宛にサイト外の対応ノード（corresponding node）C から発信する場合*を考える．この場合，ノード N には ISP A，B から委譲されたプレフィックスに属す

*たとえば C がクライアント，N がサーバの場合．

†岡山大学大学院自然科学研究科, Graduate School of Natural Science and Technology, Okayama University
‡情報通信研究機構, National Institute of Information and Communications Technology
§岡山大学情報統括センター, Center for Information Technology and Management, Okayama University
¶国立情報学研究所, National Institute of Informatics

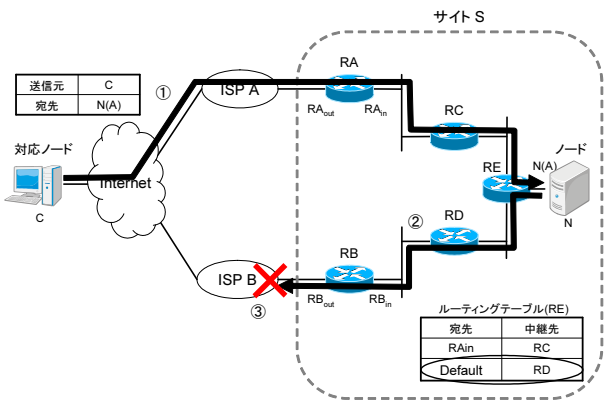

図 2: 通常の経路制御を用いた場合のパケットの流れ

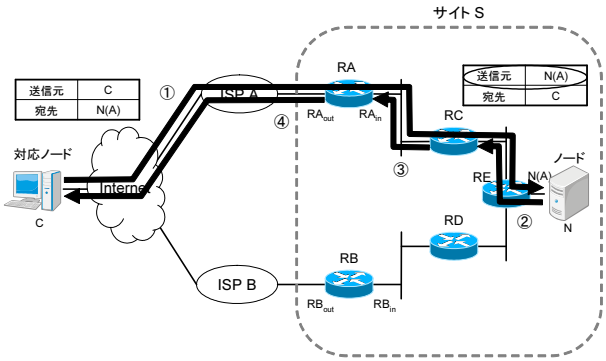

図 3: SAD ルーティングを用いた場合のパケットの流れ

るアドレス N(A)，N(B) が付与され，対応ノード C は N(A)，N(B) のいずれかを宛先アドレスに指定して通信が行われる．サイト内の各ルータの IP アドレスは原則として ISP A，B から委譲されたいずれのプレフィックスに属するものでも構わないが，サイト出口ルータ RA，RB の外側インタフェースの IP アドレス RA_{out}，RB_{out} はそれぞれ ISP A，ISP B から委譲されたプレフィックスに属するものとする．

なお，サイト内のノードからサイト外に発信を行う場合については 4.4 節で議論する．

2.2 IPv6 サイトマルチホーミングにおける課題

通常，インターネットでは宛先アドレスに基づいた経路制御が行われている．ところが IPv6 サイトマルチホーミングではこのような経路制御を用いると通信が行えない場合がある．その状況を図 2 を用いて詳述する．

図 1 の環境において対応ノード C がアドレス N(A) を宛先アドレスとして用いてノード N と通信する場合を考える．その際の往復のパケットの流れを図 2 に示す．なお，図中の番号は以下の説明における番号と対応している．また，サイト S における対応ノード C へのデフォルト経路は ISP B 経由のものとする．

1. 対応ノード C から送出された N(A) 宛のパケットはインターネット内の経路制御に従って ISP A 経由でノード N に配送される．
2. ノード N は対応ノード C への応答パケットを送出する．このパケットの送信元アドレスは N(A) となる．サイト S では対応ノード C 宛のデフォルト経路は ISP B 経由のものであるため，このパケットは ISP B 用のサイト出口ルータである RB まで中継される．
3. RB が ISP B にパケットを中継しようとすると，そのパケットの送信元アドレス N(A) は ISP B から委譲されたプリフィックスに属さないものであるため，ISP B の流入フィルタリングにより廃棄される．

このように，サイト外からサイト内への通信では，流入フィルタリングによりパケットが廃棄される可能性があるため，往復とも同じ ISP を経由するように経路制御を行う必要がある．

2.3 SAD ルーティング

このような問題を解決する方法として，SAD ルーティングが知られている．これはルータが送信元アドレスに基づいて中継先（next-hop）を決定する経路制御方式で，多くのルータではポリシルーティング（PBR: Polocy Based Routing）機能 [5] により実現可能である．

図 3 を用いて SAD ルーティング使用時のパケットの流れを詳述する．同図において全てのルータは SAD ルーティング機能を備えており，送信元 IP アドレスが ISP A のプレフィックス Prefix(A) に属する場合のデフォルト経路に対する中継先は ISP A に向かう上位のルータに設定されているものとする．なお，送信元アドレスが ISP B のプレフィックス Prefix(B) に属する場合には，通常の経路制御に従ってデフォルト経路である ISP B 経由の経路が選択される．

1. 対応ノード C から送出された N(A) 宛のパケットはインターネット内の経路制御に従って ISP A 経由でノード N に配送される．
2. ノード N は対応ノード C へ送信元アドレス N(A) の応答パケットを送出する．このパケットはまずルータ RE に送られ，送信元 IP アドレスがプレフィックス Prefix(A) に属するため，RE は SAD ルーティングにより ISP A に向かう方向の上位ルータである RC に中継する．
3. 同様に RC は SAD ルーティングによりこのパケットを上位ルータである RA に中継する．
4. 同様にサイト出口ルータ RA では SAD ルーティングによりこのパケットを ISP A に中継する．

このように，SAD ルーティングを用いると往復の経路が一致するため，流入フィルタリングを回避することが可能になる．

2.4 SAD ルーティングの問題点

SAD ルーティングは流入フィルタリングの回避には効果的であるが，一方で大規模なネットワークでは導

入が困難である，管理コストが大きくなる，あるいは耐障害性の面で劣るなどの問題点がある．本節では，この問題について詳述する．

SAD ルーティングの比較的容易な実現方法として，前節で述べたように PBR 機能を利用する方法がある．ところが，この方法ではサイト内の多くのルータに管理者が PBR 機能の設定を正しく行う必要があり，管理コストが増大するという問題点が生じる．PBR 機能が正しく動作しないと通信に支障を来たす危険性があるため，管理者の負担は大きい．たとえば図 3 においてルータ RC で PBR 機能が正しく動作しない場合，前節のパケットの流れのステップ 3 において RC はデフォルト経路情報に従って受信したパケットを RE に中継し，RC と RE との間でパケットの循環が発生する結果を招く．また，現在普及しているルータでは，PBR 機能は送信元アドレスに基づいて静的に中継先を指定できる機能しかないため，たとえば図 3 の例において RC が故障した場合，たとえ RE から RA への迂回経路が存在していたとしてもその経路を利用することができないなど，耐障害性の面でも問題が残されている．

これに対して，動的な SAD ルーティングを行えるようにルータを機能拡張する方法（たとえば文献 [4]）が提案されている．この方法では障害発生箇所を迂回して SAD ルーティングを行えるため，耐障害性の面では上記の方法より優れている．ところが，この方法では SAD ルーティングを行う全てのルータに機能拡張が必要であるため，実環境への導入が困難である．

さらに別の方法として，サイト出口ルータ同士を仮想リンクで接続し，たとえば図 3 において送信元アドレスが Prefix(A) に属するパケットが正しくないサイト出口ルータ RB に届くと，RB が仮想リンクを通じてこれを正しいサイト出口ルータ RA に転送するような方法 [6] が知られている．ところが，この方法では図 3 において送信元アドレスが N(A) であるパケットをノード N が送出すると，このパケットは RB に届いた後，RA に転送されるため配送経路が（N-RE-RD-RB-RD-RE-RC-RA）となるのに対し，SAD ルーティングの場合の配送経路は（N-RE-RC-RA）であるため，無駄な迂回を行う点が問題となる．また，RB が故障すると RA 経由での通信も行えなくなる可能性があるため，耐障害性の面でも問題がある．

3. ルーティングヘッダを用いたサイト出口ルータ選択

前章で述べたように，従来の方法ではサイト出口ルータ選択に SAD ルーティングを用いたため，いずれも導入・運用面や耐障害性の面で問題があった．そこで本章ではこれらの問題点を軽減するため SAD ルーティングに基づかないサイト出口ルータ選択方法を提案する．

3.1 提案手法の概要

SAD ルーティングは往復の経路を一致させる方法として十分ではあるが，復路で通過するルートを何らかの方法で指定することができれば他の方法でも構わない．そこで，本章では，途中で経由するルータの指定ができる，IPv6 におけるソースルーティング用の拡張ヘッダであるルーティングヘッダ (Routing Header)[7] を用いる手法を提案する．

我々の研究グループではこれまでに IPv4 の LSRR（Loose Source and Record Route）オプション [8] を用いたマルチホーミング手法を提案した [9]．この手法では TCP 通信のみを対象とし，対応ノードからのサイト内ノード宛の SYN パケットがサイト出口ルータを通過する際に LSRR オプションを付加し，あたかもサイト出口ルータを通過した直後のように装ったパケットをサイト内ノードに送出した．UNIX/Linux 系の多くの OS では LSRR オプション付き SYN パケットを受信すると，以降に出力される同一コネクションのパケットには同じサイト出口ルータを経由するように LSRR オプションが自動的に付加されるため，往復の経路が一致するようになった．

ところが，IPv6 環境で同様の方法を試したところ，UNIX/Linux 系 OS であっても自動的にはルーティングヘッダを付与しないことが判明した．そこで，提案手法ではサイト内のノードが送信元アドレスに応じて適切なサイト出口ルータを経由するようにルーティングヘッダを付加する方法を採用する．一方，サイト出口ルータではサイト内ノードで付加されたルーティングヘッダは不要であり，逆にルーティングヘッダ付きのパケットをサイト外に送出すると経路途上のルータや対応ノードで破棄される可能性があるため，付加されたルーティングヘッダを削除するようにする．このような動作により，サイト内のルータはサイト出口ルータを除いて通常の経路制御を行えばよく，比較的容易に導入することができる．また，耐障害性についても，サイト内ノードからサイト出口ルータへは通常の経路制御により障害発生箇所を迂回できるため，問題は発生しない．このように，ルーティングヘッダは従来の SAD ルーティングが持つ問題点をいずれも軽減できる点で優れている．

3.2 ルーティングヘッダの付加

提案手法ではサイト内ノードに新たにミドルウェアを導入することでルーティングヘッダの追加を行う．このミドルウェアは OS から出力されるパケットのうち，送信元 IP アドレスが Prefix(A) に属し，かつ宛先 IP アドレスがサイト外であるものを受信し，経由ノードとしてサイト出口ルータのサイト側アドレス RA_{in} を指定したルーティングヘッダ†を付加した後，これをネットワークに送出する．ルーティングヘッダの種類（type）はサイト内ノードとサイト出口ルータの間で合意があれば任意のものが利用可能である．

一方，送信元アドレスが Prefix(B) に属するパケットについては，デフォルト経路を含む，サイト外宛の全ての経路が ISP B を経由するものであれば，特にルーティングヘッダの付加は必要ない．ただし，このようなパケットが ISP A を経由して送出される可能性がある場合には上記の同様の方法でルーティングヘッダを追加する必要がある．

なお，送信元アドレスにかかわらず，宛先がサイト

†実際には，宛先アドレスに RA_{in} を設定し，本来の宛先アドレスはルーティングヘッダ内に退避する．

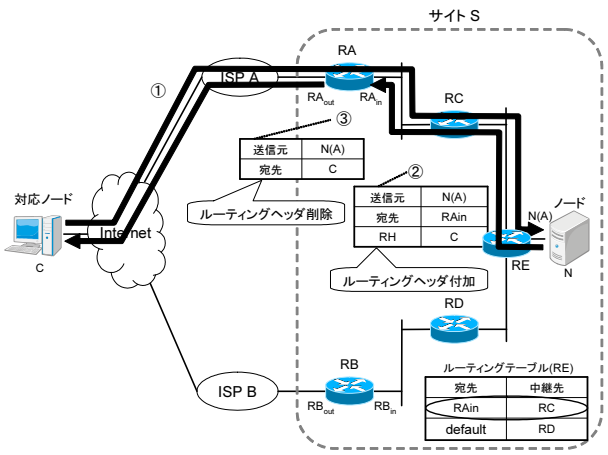

図 4: ルーティングヘッダを利用する経路制御の例

内の別のノードであるパケットはいずれのサイト出口ルータも経由する必要がないため，ルーティングヘッダは付加するべきではない．

3.3 ルーティングヘッダの削除

サイト出口ルータでは，サイト内ノードで付与されたルーティングヘッダから本来の宛先アドレスを取り出して現在の宛先アドレスをこれに書き換え，ルーティングヘッダを削除した後に ISP 側に中継する．このような機能は通常のルータには備わっていないため，どのようにしてサイト出口ルータでルーティングヘッダの削除を行うかが問題となる．

最も単純な方法は，いわゆる PC ルータを用いる方法である．その場合，OS の持つ機能（たとえば OpenBSD における PF(packet filter)[10] や divert[11]）によりルーティングヘッダ付きパケットを取り出し，上記の処理を行うことは比較的容易である．一方，性能，機能面で PC ルータを用いることが困難である場合も考えられる．そのような場合には，サイト出口ルータで PBR を用いてルーティングヘッダ付きパケットだけを外付けの PC ルータに中継して上記の処理を行わせる方法が有効と思われる．

さらに，もし mobile IPv6 で用いられるタイプ 2 ルーティングヘッダ [12] の処理機能がサイト出口ルータ自身に備わっていれば，その機能を有効にする方法も考えられる．この場合，ルーティングヘッダが付いたまま ISP 側に中継されるが，これは通常の使用時と同じであり，特に問題ではない．ただし，タイプ 2 ルーティングヘッダのサイト出口ルータ選択への適用は厳密には文献 [12] の規定に違反しており，実際に動作するかどうかは実装依存である．

3.4 全体の動作

これまでに説明した提案手法の動作を図 4 に示す．この図では対応ノード C がアドレス N(A) を宛先アドレスとして用いてサイト内ノード N と通信する場合を想定している．なお，図中の数字は以下の動作の番号と一致している．

1. 対応ノード C から送出された N(A) 宛のパケットはインターネット内の経路制御に従って ISP A 経由でノード N に配送される．
2. ノード N は対応ノード C へ送信元アドレス N(A) の応答パケットを送出する際に，経由ノードとしてサイト出口ルータのサイト側アドレス RA_{in} を指定したルーティングヘッダを付加する．実際に送出されるパケットの宛先アドレスは RA_{in} であるため，通常の経路制御によってサイト出口ルータ RA まで配送される．
3. RA は宛先アドレスをルーティングヘッダに退避していた本来の宛先である対応ノード C に変更し，ルーティングヘッダを削除した上で ISP A に送出する．

3.5 Path MTU の減少への対処

提案手法において 24 バイトのルーティングヘッダを付加すると，その分だけパケットの大きさが増加し，その結果ノードの MTU（Maximum Transfer Unit）あるいはノードからサイト出口ルータまでの経路上の Path MTU を超過する可能性があるという新たな問題が生じる．これはノードから見ると Path MTU が 24 バイト分減少した場合と等価であり，ノードは見かけ上の Path MTU に合わせてペイロードを少なくする必要がある．

そこで，この問題への対処方法として，ノード内のミドルウェアでは次の 2 種類の処理を行うようにする．まず，ルーティングヘッダを付加したパケットを送出する際にその大きさがネットワークインタフェースの MTU を超える場合には，ミドルウェアが “Packet Too Big” を通知する ICMPv6 メッセージ（Type=2）を生成して OS に返す．この場合，通知する MTU には本来の MTU から 24 を減じた値‡を用いる．また，ネットワークから “Packet Too Big” を通知する ICMPv6 メッセージを受け取ると，以下のように動作する．

1. ミドルウェアは ICMPv6 メッセージ中に含まれている元のパケット（の一部）を調べ，この中にルーティングヘッダが含まれているかどうかを確認する．
2. もし元のパケットにルーティングヘッダが含まれていれば，通知された MTU から 24 バイトを減じた値を新しい MTU とした ICMPv6 メッセージを生成し，OS に中継する．
3. そうでなければ，元の ICMPv6 メッセージをそのまま OS に中継する．

これによりルーティングヘッダが付加された状態で発生した MTU 超過に対しても正しくペイロードサイズを調整することが可能になる．この場合，本来は往復で Path MTU の大きさが同じである環境でもこれらが異なることになる．しかし，一般の IPv6 環境でも往復の経路が異なるため Path MTU の大きさが異なる場合があるため，問題とはならない．

‡たとえば MTU が 1500 バイトのイーサネットの場合，1476 バイトとなる．

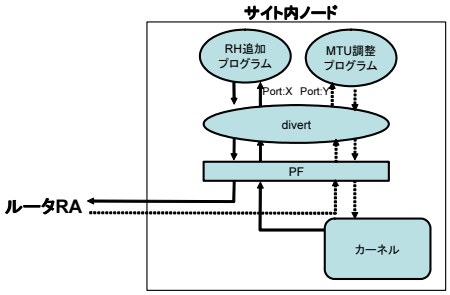

図 5: サイト内ノードの内部構成

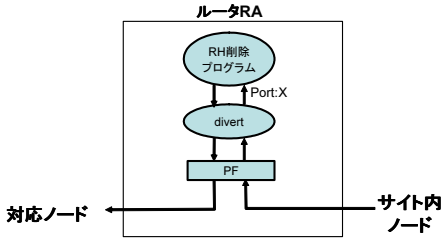

図 6: サイト出口ルータの内部構成

4. 試作システムの実装と評価

前章で述べた手法が実際に機能するかどうかを検証するため，ルーティングヘッダ追加機能を持つノードおよび同削除機能を持つサイト出口ルータから構成される試作システムの実装を行った．本章では試作システムの実装方法および動作検証実験，性能評価実験について述べる．また提案システムの適用範囲に関する考察も行う．

4.1 試作システムの実装

試作システムでは提案手法が正しく動作するかどうかの検証を主目的としたため，サイト出口ルータとして 3.3 節で述べた 3 種類の方法のうち，最も単純な PC ルータを用いる方法を採用した．また，サイト内ノード，サイト出口ルータの両方とも OS として OpenBSD を採用した．これは OpenBSD では IPv6 に対応した divert 機能が利用できたためである．また，ルーティングヘッダの種類としてはタイプ 0 を用いた．タイプ 0 ルーティングヘッダはセキュリティ上の理由により既に廃止になっている [13] が，3.2 節で述べたようにサイト内ノードとサイト出口ルータの間で合意があれば任意のものが利用可能であり，また OpenBSD では比較的簡単な作業でタイプ 0 ルーティングヘッダの処理を有効化できたため，敢えてこれを採用した．

サイト内ノードの内部構成を図 5 に示す．PF はカーネルから出力されたパケットのうち，3.2 節で述べたルーティングヘッダ付加の対象となるパケットのみを divert ソケット経由でルーティングヘッダ（RH）追加プログラムに渡すように動作する．ルーティングヘッダ追加プログラムはルーティングヘッダを付加した後，divert ソケット経由でパケットを送出する．また，PF は “Packet Too Big” を通知する ICMPv6 メッセージを divert ソケット経由で MTU 調整プログラムに渡し，MTU 調整プログラムは必要であれば MTU の値を書き換えた上でカーネルにこの ICMPv6 メッセージを渡すように動作する．

同様に，サイト出口ルータにおいても，図 6 に示すように PF と divert ソケットを利用してルーティングヘッダ付きのパケットをルーティングヘッダ（RH）削除プログラムに渡すように動作する．ルーティングヘッダ削除プログラムはルーティングヘッダを削除した後，divert ソケット経由でパケットを送出する．

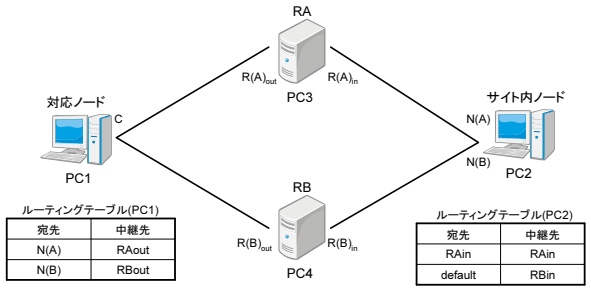

図 7: 実験環境

4.2 動作確認実験

まず，試作したサイト内ノードおよびサイト出口ルータを用いて対応ノードとの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 7 に示す．また，実験で用いた各 PC の諸元を表 1 に示す．なお，図中のネットワークではいずれのリンクも 100BaseTX を用いた．

この環境において，サイト内ノード（PC2）ではデフォルトゲートウェイを通常のルータである RB（PC4）に設定した．また，対応ノード（PC1）では，サイト内ノードの 2 つのアドレスのうち，N(A) は RA 経由で，N(B) は RB 経由でそれぞれアクセスできるように経路設定を行った．

動作確認実験では，サイト内ノード上では HTTP サーバを動作させ，これを対応ノードから N(A) あるいは N(B) を直接指定してアクセスするようにした．また，tcpdump[14] を用いて，パケットの配送経路，ルーティングヘッダの有無およびパケット長を観測した．その結果，往路，復路とも N(A) を指定した場合には RA

表 1: 各 PC の諸元

PC	CPU, メモリ	OS
PC1	Core2 Duo 2.93GHz, 2GB	FreeBSD 8.2
PC2	Core2 Duo 2.93GHz, 2GB	OpenBSD 5.0
PC3	Core2 Duo 2.93GHz, 2GB	OpenBSD 5.0
PC4	Core2 Duo 2.93GHz, 2GB	FreeBSD 8.2

表 2: 性能評価実験結果（内向きスループット）

PC2，PC3 の種別	スループット	通常との差
通常	88.56Mbps	-
試作システム	88.48Mbps	0.1%

表 3: 性能評価実験結果（外向きスループット）

PC2，PC3 の種別	スループット	通常との差
通常	88.48Mbps	-
試作システム	87.04Mbps	1.6%

を，また N(B) を指定した場合には RB を経由し，ルーティングヘッダによるサイト出口ルータ選択が正しく動作していることを確認した．また，RA を経由する場合のルーティングヘッダの付加・削除が適切に行われていることを確認し，さらにパケット長は対応ノードと RA との間で 1476 バイトとなっており，MTU の調整が正しく行われていることも確認した．

4.3 性能評価実験

提案手法では 24 バイトのルーティングヘッダの付加・削除を伴い，また見かけ上の Path MTU も減少するため，通常の経路制御よりもオーバヘッドが大きいと予想される．そこで，試作システムを用いた場合と通常のルータを用いたと比較してどの程度のスループットの低下が生じるかを調べるため，図 7 と同様の環境において性能評価実験を行った．

この実験では，図 7 における PC4 は用いず，PC2，PC3 を両方とも通常のもの，両方とも試作システムのものの 2 種類に切り替え，それぞれの場合において iperf[15] を用いて TCP スループットの測定を行った．

表 2，表 3 にそれぞれサイト外からサイト内（内向き）方向，サイト内からサイト外（外向き）方向のスループットの測定結果を示す．これらの結果から，以下のようなことがわかる．まず，内向きのスループットの低下は 0.1%であり，十分小さいといえる．オーバヘッドが生じている理由は，測定用プロトコルとして TCP を用いたため，外向きの ACK パケットについては 24 バイトのルーティングヘッダの付加・削除が必要となり，そのオーバヘッドによるものであると推察できる．一方，外向きのスループットの低下が 1.6%と比較的大きくなっている．この理由は，ルーティングヘッダの付加による 24 バイト分のペイロードの減少によるものであると推察できる．なお，MTU である 1500 バイトに対して 24 バイトは 1.6%に相当する．

4.4 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．

4.4.1 ルーティングヘッダ無効化による影響

4.1 節で述べたように，試作システムで用いたタイプ 0 ルーティングヘッダは現在廃止されている．タイプ 0 ルーティングヘッダでは経由するノードを複数指定できるため，1 つのパケットで同一のノードを何回も経由することが可能になり，その結果特定のノードに対してサービス不能攻撃を行いやすくなることが廃止の理由である．しかし，試作システムではタイプ 0 ルーティングヘッダを処理するノードはサイト出口ルータのみであり，またサイト出口ルータではタイプ 0 ルーティングヘッダを削除する処理を行うため，サービス不能攻撃は成功せず，問題とはならない．また，IPv6 のタイプ 0 ルーティングヘッダは IPv4 の LSRR オプションとは異なり，経由ノードとして指定されていない単に通過するだけのルータではルーティングヘッダの参照は原則として行われない．したがって，タイプ 0 ルーティングヘッダを用いた実装であっても，サイト内で特にルーティングヘッダの有無を確認してタイプ 0 ルーティングヘッダ付きパケットを廃棄する設定が行われているルータが存在しない限り，有効に動作すると思われる．

なお，サイト内ノードで付加したルーティングヘッダが含まれるパケットはサイト外にはそのままでは中継されないため，サイト外ではこの問題は発生しない．また，サイト外からのタイプ 0 ルーティングヘッダ付きパケットによる攻撃に対しては，サイト出口ルータでフィルタリング可能であるため問題ない．

4.4.2 サイト内ノードからの発信

提案手法は送信元 IP アドレスに応じたサイト出口ルータを経由するようにルーティングヘッダを付与するため，サイト外からサイト内への発信に対する応答だけでなく，サイト内ノードからサイト外ノードへの発信に対しても適用可能である．ただし，この場合，サイト内ノードによる送信元アドレスの選択が課題として残されている．この課題に対して文献 [16] では標準的な規則が示されている．しかし，提案手法では，これに限らずノードは任意の方法で送信元アドレスを選択しても，選択された送信元アドレスに基づいて適切なサイト出口ルータを経由するように経路制御できる．

4.4.3 サイト出口ルータの多重化

サイト内のネットワーク構成によっては，1 つの ISP に対して複数のサイト出口ルータを設置する場合が考えられる．たとえば遠隔キャンパスを持つ大学では各キャンパスで複数の ISP と接続する構成がありうる．

このような構成に対して，提案手法では 1 つのプレフィックスに対してルーティングヘッダで指定できるアドレスは 1 つに限られるため，そのままでは同一の ISP に対する複数のサイト出口ルータのうち適切なものを選択することはできない．しかし，これらのサイト出口ルータに共通の仮想 IP アドレスを割り当て，各サイト出口ルータから仮想 IP アドレスに対する経路情報を適切なコストで広告すれば，サイト内ノードはそのうち最もコストの小さいサイト出口ルータを選択することができる．

5. まとめ

本論文では，IPv6 サイトマルチホーミング環境において，ルーティングヘッダを付加・削除する機能を導入することにより，送信元アドレスに応じて経由するサイト出口ルータを選択する手法を提案した．また，この手法に基づいて試作したシステムを試験運用した結果，正しい経路が選択され，またオーバヘッドも実用上問題ないことが確認された．これにより，従来の SAD ルーティングよるサイト出口ルータ選択の問題を軽減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 [17][18] 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挙げられる．また，試作システムではプレフィックスとサイト出口ルータの対応付けやサイト内ネットワークの範囲を手動で行っているため，たとえば DHCPv6[19] を用いた設定の自動化についても今後行っていきたい．

参考文献

[1] Ferguson, P. and Senie, D.: “Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing,” RFC2827, IETF, May 2000.

[2] Baker, F. and Savola, P.: “Ingress Filtering for Multihomed Networks,” RFC3704, IETF, March 2004.

[3] Bagnulo, M., Garcia-Martinez, A., Rodriguez, J. and Azcorra, A.: “End-site routing support for IPv6 multihoming,” Computer Communications, September 2005.

[4] Ohira, K. and Okabe, Y.: Host-Centric Site-Exit Router Selection in IPv6 Site Multihoming Environment, *Proceedings of 1st International Workshop on Protocols and Applications with Multi-Homing Support* (*PAMS 2011*), pp.696–703, 2011.

[5] Cisco Systems Inc.: Policy-Based Routing (Online), available from ⟨http://www.cisco.com/warp/public/cc/pd/iosw/tech/plicy_wp.pdf⟩ (accessed 2012-04-18).

[6] Huitema, C., Draves, R. and Bagnulo, M.: Ingress filtering compatibility for IPv6 multihomed sites (Online), available from ⟨http://ops.ietf.org/multi6/ietf61/IETF61_ingress_filter.pdf⟩ (accessed 2012-04-18).

[7] Deering, S. and Hinden, R.: Internet Protocol, Version 6 (IPv6) Specification, RFC2460, IETF (1998).

[8] Postel, J. (Ed.): Internet Protocol, RFC 791, IETF (1981).

[9] 金勇，山口拓哉，山井成良，岡山聖彦，中村素典：“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（推薦論文）”，情報処理学会論文誌，Vol.52，No.12，pp.3745–3754，2011.

[10] PF: The OpenBSD Packet Filter (Online), available from ⟨http://www.openbsd.org/faq/pf/⟩ (accessed 2012-04-18).

[11] divert - kernel packet diversion mechanism, OpenBSD Programmer’s Manual (Online), available from ⟨http://www.openbsd.org/cgi-bin/man.cgi?query=divert⟩ (accessed 2012-04-18).

[12] Johnson, D., Perkins, C. and Arkko, J.: “Mobility Support in IPv6,” RFC3775, IETF, June 2004.

[13] Abley, J., Savola, P. and Neville-Neil, G.: “Deprecation of Type 0 Routing Headers in IPv6,” RFC5095, IETF, December 2007.

[14] TCPDUMP/LIBPCAP public repository (online), avaiable from ⟨http://www.tcpdump.org/⟩ (accessed 2012-04-18).

[15] Iperf Project (Online), available from ⟨http://iperf.sourceforge.net/⟩ (accessed 2012-04-18).

[16] Draves, R.: “Default Address Selection for Internet Protocol version 6 (IPv6),” RFC3484, IETF, February 2003.

[17] 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).

[18] Yong Jin, Nariyoshi Yamai, Kiyohiko Okayama, Motonori Nakamura: “An Adaptive Route Selection Mechanism Per Connection Based on Multipath DNS Round Trip Time on Multihomed Networks”, *Journal of Information Processing*, Col.20, No.2, to appear, 2012.

[19] Droms, R. (Ed.), Bound, J., Volz, B., Lemon, T., Perkins, C. and Carney, M.: “Dynamic Host Configuration Protocol for IPv6 (DHCPv6),” RFC3315, IETF, July 2003.