Vol.2011-DPS-146 No.5
Vol.2011-CSEC-52 No.5
2011/3/10

IPv6 環境下におけるルータへのなりすましによる通信傍受の実験と対策の提案

坂本知弥[†]　佐々木良一[†]　甲斐俊文[††]

近年，インターネットの普及により，IPv4 アドレスの枯渇が懸念されている．その為，IPv6 の導入が進められており，IPv6 が導入された場合，IP アドレス数の大幅な増加だけでなく，様々な利点が期待されている．しかし，その利点を逆手に取った攻撃手法も同時に発見されており，迅速な対応が求められている．そのような攻撃手法の 1 つがアドレス自動割り当て時における，ルータへのなりすましによる不正 RA(Router Advertisement)攻撃である．既存対策としてはネットワーク機器やルータへの機能実装による対策が提案されているが，実現性や有効性の問題により，現実的ではない．そこで，本研究では実験を通じて不正 RA 攻撃がどの程度容易に実現出来るかを示すとともに，PC 側でフィルタリングを行う簡易で効率的な手法の提案と評価を行う．

Experiment of the network wiretapping by spoofing to the router in the IPv6 environment and proposal of its countermeasure

Tomoya Sakamoto[†]　Ryoichi Sasaki[†]　Toshifumi Kai[††]

In recent years, exhaustion of IPv4 address becomes a big issue caused by the spread of Internet. This tendency leads the introduction of IPv6 address which has the various advantages such as large increase of the number of the IP addresses. However, the attack technique that took the advantage underhand is discovered at the same time, and quick countermeasure is required. One of such attack techniques is unjust RA (Router Advertisement) attack by spoofing to the router in the address automatic allotment. Although the conventional measures to the network equipment or router have been proposed, these measures are not realistic from the view point of usefulness and effectiveness. Therefore we show how easily we can realize unjust RA attack through an experiment, and we propose and evaluate a filtering technique which is simple and effective in the PC side in this study.

1. はじめに

近年，インターネットの普及により，IPv4 アドレスの枯渇が懸念されている．その為，現在では世界各国で IPv6 の導入が進められている．IPv6 が導入された場合，現在問題となっている IPv4 アドレスの枯渇に対する根本的な解決はもちろん，その他様々な利点が期待されている．しかし，利点を逆手に取った攻撃や，セキュリティ上の欠点なども同時に発見されている為，IPv6 が本格的に普及するまでに迅速な対応を行う必要が出ている．

その例として，IPv6 導入時の利点の 1 つであるルータによるアドレス自動割り当て時における，ルータへのなりすましによる通信傍受が挙げられる．ルータによるアドレス自動割り当て機能は IPv6 から導入された新機構であり，ルータが RA(Router Advertisement)というメッセージパケットを送信することでホスト PC に IPv6 アドレスを自動生成するとともに，アドレス生成に用いたルータをデフォルトゲートウェイに設定するという機能である．しかし，この RA メッセージはホスト PC から送信することも可能である為，ホスト PC によるルータへのなりすましが可能であるとされている．

これを確認する為，著者らは実験を行い，IPv6 環境下におけるホスト PC によるルータへのなりすましは，IPv4 環境下における DHCP Spoofing によるなりすましよりも大幅に容易であることを確認するとともに，中間者攻撃が実現することも明らかにした．

既存の対策としては，ネットワーク機器やルータへの機能の実装によるものが挙げられている[1]．しかし，いずれも実現性や有効性の面で問題が生じており，効果的な解決策は未だに提案されていない．

そこで，本稿では実現性や有効性が高い方式として，ホスト PC 側で RA のパケットフォーマットに基づいたフィルタリングプログラムを行う手法を提案する．

本稿の 2 章に IPv4 アドレス枯渇の背景やルータへのなりすましによる通信傍受の概要を示す．3 章では通信傍受の実験を行い，その危険性を示すとともに結果から得られた考察を述べる．4 章では得られた考察に基づいた提案手法や手法の実装，性能評価について述べる．そして，5 章で既存対策との比較，及び評価を述べる．

[†] 東京電機大学
Tokyo Denki University
[††] パナソニック電工株式会社
Panasonic Electric Works Co. Ltd.

Vol.2011-DPS-146 No.5
Vol.2011-CSEC-52 No.5
2011/3/10

2. 背景

2.1 IPv4 アドレス枯渇の懸念

近年，インターネットの普及により，IPv4 アドレスの枯渇が懸念されている．図 1 は APNIC(Asia Pacific Network Information Center)のチーフサイエンティストである Geoff Huston 氏が予測する IPv4 アドレスの在庫枯渇の予想グラフである．図 1 の①は IANA(Internet Assigned Number Authority)が管理しているアドレスの在庫数を，図 1 の②は RIR(Regional Internet Registry)が管理している分配可能なアドレスの在庫数を示している．Geoff Huston 氏によると，遅くとも 2011 年中には管理されている全てのアドレスの在庫数が底を尽きてしまうと言われている[2]. また, 2011 年 2 月 3 日に IANA が管理しているアドレス在庫が枯渇したことも発表されている為，現在対応が求められている[3].

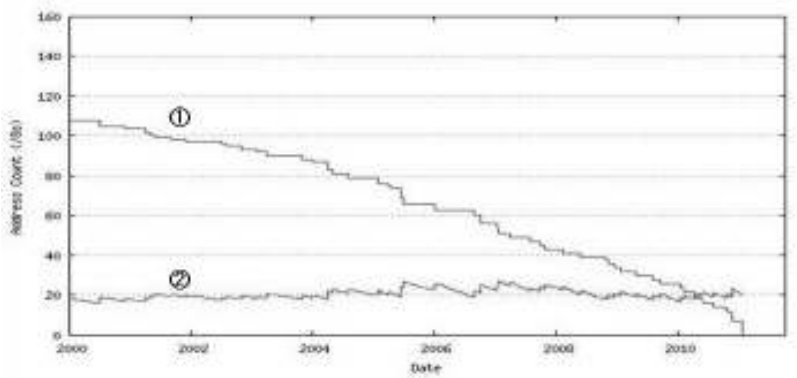

図 1　IPv4 アドレス枯渇予想図
Fig. 1　A forecast map of exhaustion of the IPv4 address

その為，世界各国で IPv6 の導入が検討されている．IPv6 が導入された場合，IP アドレス在庫数の増加はもちろん，ルータによるアドレス自動割り当て機能やマルチキャストの導入などの利点が期待されている. しかし, その利点を逆手に取った攻撃や，セキュリティ上の欠点なども同時に発見されている為，IPv6 が本格的に普及するまでに迅速な対応を行う必要が出てきた[4].

2.2 ルータへのなりすましによる通信傍受

本節では，IPv6 導入時の利点の 1 つであるルータによるアドレス自動割り当て時における，ルータへのなりすましによる通信傍受の概要について説明する．

通常，IPv6 では図 2 のように，DHCP の代わりにルータ（以下，正規ルータと呼ぶ）がアドレスの生成を行うが，その方法は 2 通りある．

（1）1 つ目は, ルータが RA メッセージをホスト PC に対して定期的に送信し, IPv6 アドレスを自動生成する方法である．RA にはアドレスを生成する為のプレフィックスと呼ばれる値（IPv4 アドレスでのネットワーク部に相当する）やアドレスの有効期限，ルータの優先度などが保持されている．

（2）2 つ目は，ホスト PC がルータに対して RS(Router Solicitation)と呼ばれる RA の要求メッセージを送信し，RA の受信を行う，ステートレスアドレス自動設定と呼ばれる方法である．

いずれかの方法により RA を受け取ったホスト PC は，RA に保持されたプレフィックスと自身の MAC アドレスを用いて IPv6 アドレスを自動生成する．そして，そのアドレスがネットワーク内で利用出来るのかどうかを確認する為, DAD と呼ばれる重複アドレス検出の為の近隣探索を行う．DAD によって，自動生成されたアドレスが利用可能だと判明した場合，自動生成された IPv6 アドレスを自身に設定するとともに，RA を送信したルータをデフォルトゲートウェイとして設定する．

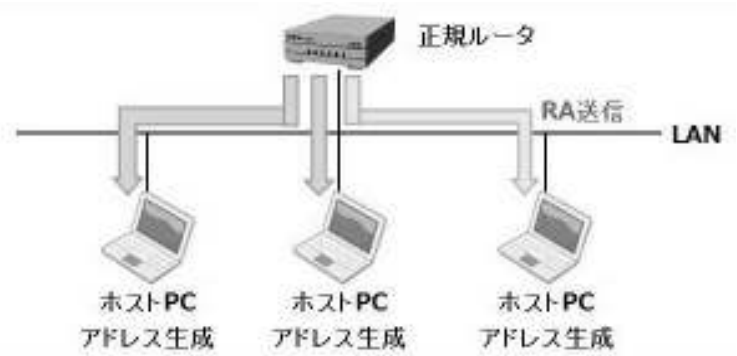

図 2　正規ルータによる RA 送信の流れ
Fig. 2　The flow of sending Router Advertisement by the true router

しかし, ホスト PC も RA（以下, 不正 RA と呼ぶ）を送信することが可能である為，LAN に接続したホスト PC（以下，攻撃者 PC と呼ぶ）が不正に RA を送信してルータへのなりすましを行うことが出来る．ここで，RA に設定されるルータの優先度には low，medium，high の 3 種類が定義されている．この時，正規ルータが送信する RA よりも攻撃者 PC が送信する RA の優先度が高い場合，ネットワーク内のホスト PC は

Vol.2011-DPS-146 No.5
Vol.2011-CSEC-52 No.5
2011/3/10

図 3 の①のように，パケットを全て攻撃者 PC へ送信してしまう．そして，攻撃者 PC にパケットを中継する設定が行われていた場合，図 3 の②のように攻撃者 PC が通信の中継を行うことで，通信傍受が行われることとなる．

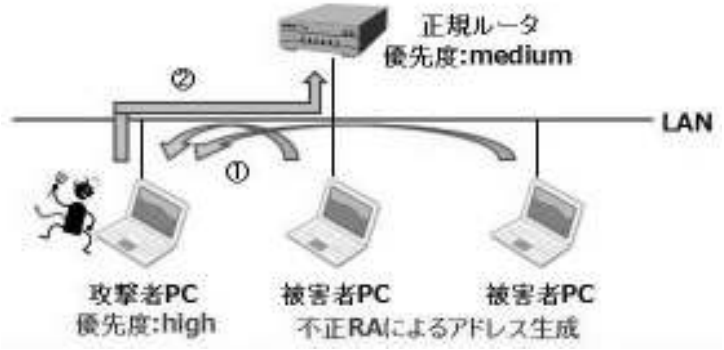

図 3　通信傍受の流れ
Fig. 3　The flow of network wiretapping

ここで，市販ルータにおける，ルータの優先度について調査を行った．まず，市販ルータの優先度の初期設定であるが，RFC4191 により medium に規定されていることが判明した[5]．その為，著者は市販ルータの優先度変更の可否について調査した．対象とした企業は，通信事業者向けルータ市場と企業向けルータ市場でトップシェアを誇る Cisco Systems，同じく通信事業者向けルータ市場で上位シェアである Juniper Networks，Alaxala Networks，また，企業向けルータの上位シェアであり，SOHO 市場でトップシェアである YAMAHA の 4 社について調査を行った．尚，2009 年度におけるルータ市場のデータは得られず，2005，2007，2008 年のルータ市場のデータを比較したところ，大きな変動は見られなかった為，以上の 4 社を対象とした[6][7][8].

この 4 社に対して直接の問い合わせによる調査を行った結果，優先度を変更出来るルータを製造している企業は Alaxala Networks のみであり，その機種は 2 台のみ，コストも最も低い価格で数百万円以上するものであった．また，Cisco Systems では製造はされていないが，ソフトウェアを導入することで優先度の変更は可能であることが判明した．しかし，ソフトウェアを実装出来るルータは限られており，導入する際の設定に手間がかかる為，あまり実用的ではないということが言える．

一方，攻撃者 PC で使用されると推測される RA 作成ツールは導入が容易であり，優先度を自由に変更することが可能である．その為，RA の優先度が high に変更されることで容易に通信傍受が行われるという危険性が存在する．

2.3 問題点

RA の優先度を利用した攻撃手法の問題点は，ルータへのなりすましが容易である点にあり，その要因は 2 つ挙げられる．

（1）1 点目はルータへのなりすましが IPv4 時よりも容易な点にある．IPv4 にも DHCP Spoofing という同様の攻撃手法が存在する．DHCP Spoofing は，DHCP になりすまし，ホスト PC が IP アドレスを割り当てられる際に自身をデフォルトゲートウェイとして設定させる手法である．この手法は一度成功してしまうと，永続的に通信を傍受することが可能となるが，ホスト PC が IP アドレスを取得していない時か，IP リース時間が迫っている時にしか行えない手法であり，タイミングを図る手間が存在する．一方，本研究対象である RA の優先度を利用した攻撃手法は正規ルータよりも優先度が高い RA を送信するだけでルータになりすますことが可能である為，非常に容易であると考えられている．

（2）2 点目は無線 LAN 環境下においても同様の手法が行える点にある．無線 LAN 環境下においても RA の送信は可能である為，公共の無線 LAN や WEP などの脆弱な暗号方式を用いた無線 LAN が利用されている場合，暗号を解くことで通信傍受を行われる危険性が存在する．

また，攻撃者がルータになりすますことにより，通信傍受だけでなく，以下の問題も考えられる為，被害者にとってリスクが大きいと考えられている．

（1）1 点目は通信傍受の認知が困難な点にある．一般に，IPv6 では複数のアドレスを所持することができ，RA を送信するルータの数だけ IPv6 アドレスが自動生成されることとなっている．それは RA のプレフィックスの値がそれぞれのルータによって異なっている為である．その為，通常は正規ルータと攻撃者 PC による 2 種類のアドレスが生成されることとなる．しかし，IPv6 アドレスの生成方法は単一である為，RA のプレフィックスを同値にした場合，ホスト PC に生成されるアドレスは 1 種類のみとなる．その為，RA のプレフィックスを同値にした場合は通信傍受されているかどうかの認知が一見しただけでは困難になる問題が存在する．また，生成されるアドレスからプレフィックスを判別することが可能である為，正規ルータの RA のプレフィックスと同値にすることが容易な点も問題であるとされている．

（2）2 点目は中間者攻撃への移行が容易な点にある．2.2 節で述べたように，攻撃者 PC が正規ルータよりも優先度を高くした RA を送信するだけでホスト PC が送信する全てのパケットを引き寄せることが可能である.その為，攻撃者 PC の設定によってはパケットの改ざんやフィッシングサイトへの誘導などの攻撃が容易に行える可能性があると考えられている．

Vol.2011-DPS-146 No.5
Vol.2011-CSEC-52 No.5
2011/3/10

3. 通信傍受の実験

3.1 実験目的

本実験は，主にルータへのなりすましが容易であるかを調査し，本研究対象である RA の優先度を利用した攻撃手法がどの程度危険なのかを実証する為に行った．この実験を通じてその危険性を示すとともに，結果から得られた考察を述べる．

3.2 実験環境

実験環境は表 1 の通りである．

RADVD は RA を作成・送信するツールであり，Wireshark は特定の通信セッションを抽出して表示するネットワーク・アナライザツールである．また，パケットの改ざんには netfilter というパケットフィルタリング技術を利用しており，その為のモジュールとして ip6tables，及び ip6_queue を使用した．

表 1　実験環境
Table. 1　Environment of experiment

使用ルータ	RTX1200
攻撃者 PC	Vine Linux-2.6.12
使用ツール	RADVD-1.0 Wireshark-1.2.9
パケット改ざん時の 使用モジュール	ip6tables ip6_queue
パケット改ざん プログラムの使用言語	C 言語

3.3 実験の内容と結果

本実験では，正規ルータと攻撃者 PC が RA を送信する中で，通信傍受が行われるホスト PC（以下，被害者 PC と呼ぶ）が別ネットワークのホスト PC に対して Ping を送信した際の通信経路の測定を行い，通信傍受が行われた場合は中間者攻撃の事例としてパケットの改ざんを行う，というものを行った．

環境構築は図 4 のようになっている．まず，正規ルータの優先度を medium に設定した RA を被害者 PC に送信する．一方，攻撃者 PC の優先度は low，medium，high の 3 通りにそれぞれ変更し，被害者 PC が RA を受け取った際にそれぞれどのような通信経路をたどるかを測定した． 尚，通信の測定は攻撃者 PC 側で Wireshark を起動させて測定を行った．

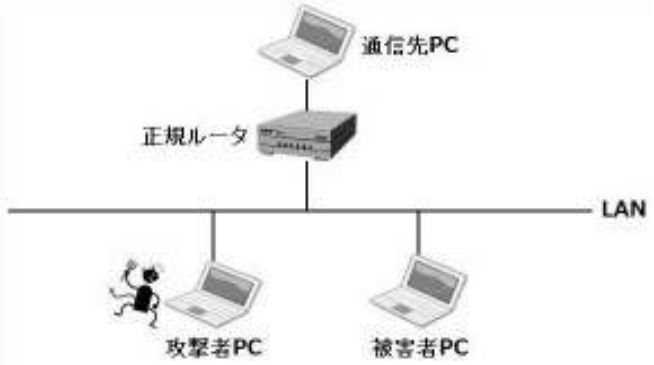

図 4　通信傍受の実験環境
Fig. 4　Environment of experiment of network wiretapping

その結果，攻撃者 PC の優先度が low，medium に設定されている場合は通信傍受が行われなかったが，優先度が high に設定されている場合は通信傍受が行われていることを確認した．

また，正規ルータでミラーポートを利用してネットワークの監視を行ったところ，被害者 PC から通信先 PC へ 1 回 Ping を送信するごとに ICMP Redirect が行われていることも確認出来た．

ここで，ICMP Redirect とは，図 5 のような流れとなっている．被害者 PC が図 5 の①のように攻撃者 PC(図 5 のルータ 1）にパケットを送信した際，攻撃者 PC は自分宛のパケットではない為，図 5 の②のように，ICMP Redirect を被害者 PC へ送信する．それと同時に，攻撃者 PC は図 5 の③のように，正規ルータ(図 5 のルータ 2)へパケットを転送する．そして，被害者 PC は図 5 の④のように今後の通信を行う．

本実験により，Ping を 1 回送信するごとに ICMP Redirect を行っていることが見受けられた為，通信傍受が行われていることが確認出来たと言える．

Vol.2011-DPS-146 No.5
Vol.2011-CSEC-52 No.5
2011/3/10

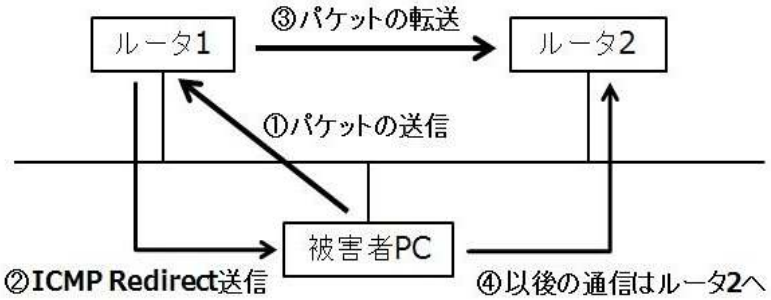

図 5　ICMP Redirect の流れ
Fig. 5　The flow of ICMP Redirect

通信傍受が行われていることを確認した為，次は netfilter を利用してパケット改ざんを行うことにした．しかし，通常，パケットはネットワークノイズによるエラーチェックや改ざんの有無を検査する為, Checksum というフィールドを用いて算出しており，パケットを単に書き換えても破棄されてしまう．従って，その値を正しく設定することでパケットの改ざんが可能になると考え，再計算を行った．

本実験では，改ざんの例として宛先アドレスの改ざん・送信を行い，その通信を測定した．その結果，測定画面で実際にパケットが改ざんされていることを確認することが出来た．

3.4 考察

本実験から，通信傍受が行えることが実際に確認出来た．また，通信傍受の実験が約 1 週間, パケット改ざん, すなわち中間者攻撃の実施が約 1 ヵ月で出来たことから，大学生でも比較的容易に通信傍受を行うことができ，多少時間をかければ中間者攻撃まで至ることも判明した．さらに，実験結果からフィッシングサイトへの誘導といった攻撃も可能であると考えられる為，実際にネットワークで攻撃が行われた場合，多大な被害が予想される．

4. 通信傍受の対策

4.1 既存の対策

本章では，既存対策と提案手法の概要，及び比較を述べる．

まず，既存対策についてであるが，公表されている既存対策は主に以下の 2 種類が挙げられる[1].

- スイッチのフィルタリング機能の実装による RA の正否判別
- ルータの SEND(Secure Neighbor Discovery)機能の実装による不正 RA の無効化

ここで SEND とは，信頼された機関に裏付けられた認証パスによって，セキュアな近隣者の探索を行う機能のことである[9].

しかし，前者はコストの問題により，後者は設定の手間や特許の問題により現実的ではないとされている．また，後者に関しては，ユニキャスト通信という特定のホスト PC への通信手法が存在する為，ルータへ機能を実装すること自体が効果的ではないとされている．

4.2 対策の提案

4.1 節において，スイッチなどのネットワーク機器への機能の実装や，ルータへの機能の実装は現実的ではないと述べた．そこで，被害者 PC 側における RA のメッセージフォーマットに基づいたフィルタリングを行う手法を提案する．

RA のメッセージフォーマットは図 6 のようになっている．そのフォーマットによると，ルータの優先度を決定するフィールドは Prf というフィールド名であり，2bit で表現されている[5].

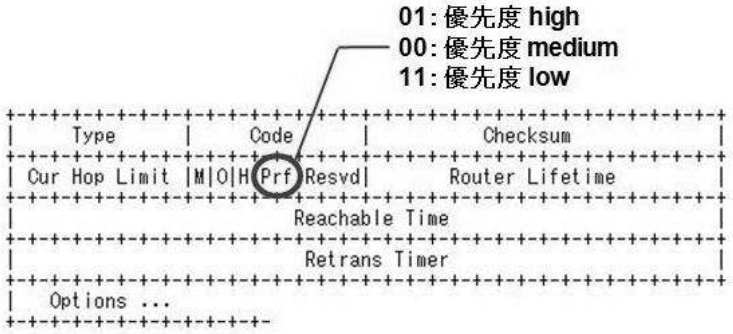

図 6　RA のメッセージフォーマット
Fig. 6　A message format of Router Advertisement

また, 2.2 節で述べたように, 大半の正規ルータの RA の優先度は medium である為，攻撃者 PC の RA の優先度は予め high に設定されることが予想される．そこで，これを逆手に取って，本研究の提案手法では，被害者 PC が RA を受け取る際にパケットの Prf フィールドを調べ，設定されている優先度が high であった場合はパケットを受

Vol.2011-DPS-146 No.5
Vol.2011-CSEC-52 No.5
2011/3/10

け取らずに破棄することにした．そのフィルタリングの動作の詳細は図 7 の通りである．

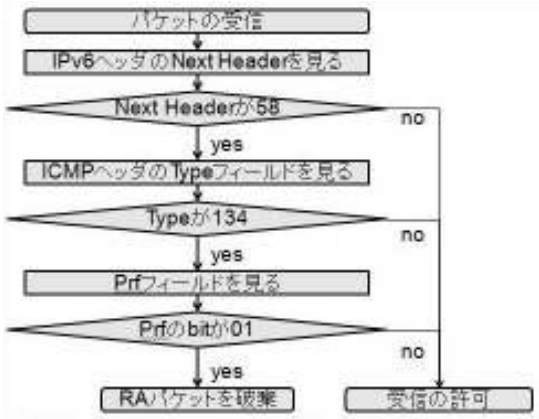

図 7　RA フィルタリングのフローチャート
Fig. 7　The flow chart of filtering Router Advertisement

まず，パケットを受信した時に IPv6 ヘッダの Next Header フィールドを見る．Next Header の値が 58 の場合，受信したパケットは ICMP パケットであることが RFC1883 で規定されている[10]．RA メッセージは ICMP パケットである為，パケットの IPv6 ヘッダから Next Header フィールドが 58，すなわち ICMP パケットであることが判明した場合，次に ICMP ヘッダの Type フィールドを見る．Type フィールドが 134 の場合，このパケットは RA パケットであることが判明する[11]．従って，RA パケットのメッセージフォーマットから Prf フィールドを参照し，ルータの優先度に応じてフィルタリングをかけることが可能となる．尚，IPv6 パケットのパケットフォーマットは図 8 を，ICMP パケットのパケットフォーマットは図 9 をそれぞれ参照してもらいたい．

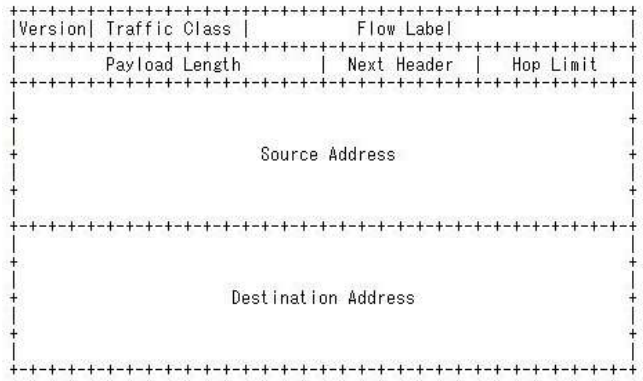

図 8　IPv6 パケットのパケットフォーマット
Fig. 8　Packet format of PIv6 packet

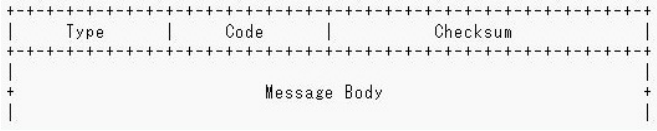

図 9　ICMP パケットのパケットフォーマット
Fig. 9　Packet format of ICMP packet

4.3 対策の実現

4.2 節で挙げた対策を表 2 に示すような環境で対策プログラムを開発することにより，Linux 上で実現した．

表 2　実現環境
Table. 2　Environment of realization

実現 PC	Ubuntu-9.1
実現時の使用モジュール	ip6tables, ip6_queue
対策プログラムの使用言語	C 言語
対策プログラムのステップ数	約 160 ステップ

対策プログラムは，パケット改ざんのプログラムを応用して作成し，そのステップ数は約 160 ステップであった．動作は，4.2 節で述べた通り，受信したパケットの IPv6

ヘッダ，及び ICMP ヘッダから RA パケットであることを確認した場合，Prf フィールドを参照する．そして，Prf フィールドが high であった場合は受信したパケットを破棄するというものである．パケット受信の検知からパケット破棄処理に要する時間は約　196 ミリ秒(10 回測定の平均値)であり，実装しても問題にならないことが明らかになった．

今回の実現環境は Linux であった為，今後は Windows 上でも実現出来るようにしていく予定である．

5. 既存対策との比較

本章では，既存対策と提案手法との比較を行う．その比較は表 3 の通りである．

表 3　既存対策と提案手法の比較
Table. 3　Comparison of Existing countermeasures and proposal of countermeasures

	スイッチへの実装	SEND	提案手法
対策箇所	スイッチ	ルータ	ホスト PC
コスト	かかる	かかる	かからない
実装の手間	かかる	かかる	かかる
ユニキャスト通信での判定	可能	不可	可能
medium 同士の対策	不可	可能	不可

本研究の提案手法と既存対策を比較すると，各ホストへの実装の手間は依然として存在するが，被害者 PC 側での対策である為，ユニキャスト通信であっても RA 判別を行うことが可能であり，コストがかからないという利点がある．

尚，提案手法において，攻撃者 PC が送信する RA の優先度が low である場合は，正規ルータに設定されている medium が優先される為，問題が無い．しかし，お互いの RA の優先度が medium の場合は OS によって使用するアドレスの優先度が存在し，通信傍受が成功してしまう場合があると考えられる．従って，今後はその問題を解決していく予定である．

6. おわりに

本稿では，IPv6 環境下のアドレス自動割り当て時におけるルータへのなりすましによる調査を行い，実際に実験を行うことで危険性を示した．また，既存の対策における問題点を洗い出し，その問題点を解消する対策案として，被害者 PC 側で動作する RA のパケットフォーマットに基づいたパケットフィルタリング手法の提案を行い，Linux 上に対策プログラムを開発し，機能・性能とも問題無いことを確認した．

今後は Windows 上に同様な機能を実装し，対策手法の実現・性能評価を行うとともに，ルータの優先度が medium 同士の場合におけるルータへのなりすまし，及び通信傍受についての調査や対策の検討を行う予定である．

謝辞　IPv6 に関する種々の知識をご教授いただき，研究の方向付けに関しご議論いただいた株式会社インターネットイニシアティブ(Internet Initiative Japan Inc.)の歌代和正氏，島慶一氏，山本和彦氏に感謝申し上げる．

参考文献

[1]　北口善明 “IPv6 のセキュリティ”, http://www.jnsa.org/seminar/2009/0127nsf2009/data/A4_3Kitaguchi.pdf (2011 年 1 月 25 日)
[2]　IPv4 Address Report , http://www.potaroo.net/tools/ipv4 (2011 年 2 月 3 日)
[3]　社団法人日本ネットワークインフォメーションセンター IANA における IPv4 アドレス在庫枯渇、および JPNIC の今後のアドレス分配について, http://www.nic.ad.jp/ja/pressrelease/2011/20110204-01.html (2011 年 2 月 3 日)
[4]　独立行政法人 情報処理推進機構セキュリティセンター, 情報セキュリティ技術動向調査タスクグループ報告書 - 2009 年下期, http://www.ipa.go.jp/security/fy21/reports/tech1-tg/documents/tech-1-2009b-001.pdf (2011 年 1 月 25 日)
[5]　RFC4191 Default Router Preferences and More-Specific Routes, http://www.ietf.org/rfc/rfc4191.txt (2011 年 1 月 25 日)
[6]　2005 年 国内ルータ市場, http://cloud.watch.impress.co.jp/epw/cda/topic/2006/05/11/7781.html (2011 年 2 月 3 日)
[7]　2007 年 国内ルータ市場, http://www.itmedia.co.jp/enterprise/articles/0804/16/news009.html (2011 年 2 月 3 日)
[8]　2008 年 国内ルータ市場, http://journal.mycom.co.jp/news/2009/04/17/039/index.html (2011 年 2 月 3 日)
[9]　RFC3971 SEcure Nighbor Discovery , http://www.ietf.org/rfc/rfc3971.txt (2011 年 1 月 25 日)
[10]　RFC1883 Internet Protocol, Version 6(IPv6) Specification, http://www.ietf.org/rfc/rfc1883.txt (2011 年 1 月 25 日)
[11]　IPv6 Neighbor Discovery, http://www.infraexpert.com/study/ipv6-5.htm (2011 年 1 月 25 日)