

## IPv6 環境下における IP アドレス付加時の 通信傍受対策技術の提案と開発

坂本 知弥†                      佐々木 良一†

†東京電機大学

〒101-8457 東京都千代田区神田錦町 2-2

sakamoto@isl.im.dendai.ac.jp, sasaki@isl.im.dendai.ac.jp

**あらまし** 近年のインターネットの普及により、日本に割り振られていたIPv4アドレスは2011年4月に枯渇した。その為、IPv6への早期移行が検討されており、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。先行研究ではRAの優先度を利用したなりすましに対し、クライアントPC側による簡易フィルタリング手法の提案及び実装を行った。本稿では、攻撃者による更なる攻撃方法の示唆と攻撃への対策手法の提案及び評価を行う。

### Proposal and development of the anti-wiretapping techniques at additional IP addresses in the IPv6 environment

Tomoya Sakamoto†                      Ryoichi Sasaki†

†Tokyo Denki University

2-2 Kandanshiki, Chiyoda, Tokyo 101-8457, JAPAN

sakamoto@isl.im.dendai.ac.jp, sasaki@isl.im.dendai.ac.jp

**Abstract** Caused by recent spread of the Internet, IPv4 addresses which have been allocated to Japan was depleted in April 2011. Therefore, it is considered quick transition to IPv6 which has various advantages such as large increase of the number of IP addresses. However, the attack technique 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. In previous studies, we proposed and implemented simple filtering program in the client PC side against spoofing using the priority of RA. In this paper, we suggest further attack possibility, propose and evaluate the countermeasures to the attack.

# 1 はじめに

近年のインターネットの普及により、日本に割り振られていた IPv4 アドレスは 2011 年の 4 月に枯渇した[1]。その為、現在では日本はもちろん、世界各国で IPv6 の導入が始められている。IPv6 が導入された場合、現在最も問題となっている IPv4 アドレスの枯渇問題を解決できるだけでなく、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 へ本格的に移行する前に迅速な対応を行う必要が出ている。

そのような問題の例として、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 からの新機構であり、ルータが RA(Router Advertisement)というメッセージパケットを送信し、クライアント PC がそれを受信することで IPv6 アドレスを自動生成し、送信元の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[2]。すなわち、同一ネットワーク内に RA メッセージを送信するルータが複数存在していた場合、クライアント PC に設定されるデフォルトゲートウェイも複数存在することとなる。また、この RA メッセージには送信元ルータの優先度が予め保持されており、RA メッセージを受信したクライアント PC はその優先度に従い、より優先度の高いルータを優先的に通信に用いることとなっている。しかし、この RA メッセージはクライアント PC が意図的に送信することも可能であり、優先度の設定を変更することも可能である為、クライアント 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。

先行研究では、攻撃者が RA メッセージの優先度を予め高く設定していると想定し、ルータの優先度が高く設定されている RA メッセージのみをフィルタリングするという対策手法の開発及び評価を行った[3]。

本稿ではより深い問題として、ルータと攻撃者が同程度の優先度であった場合に攻撃者が通

信傍受を行う攻撃方法を示唆し、その問題に対する対策の開発及び評価を行う。

本稿の 2 章にて、ルータへのなりすましによる通信傍受の概要や先行研究での対策手法について述べ、3 章にて攻撃者による更なる攻撃方法を示唆し、実験によって得られた考察を述べる。そして、4 章では得られた考察に基づいた 2 種類の提案手法について述べ、5 章にて提案手法の比較、及び評価を述べる。

## 2 不正 RA と対策の概要

本章では、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と先行研究での対策手法について述べる。

### 2.1 ルータへのなりすましについて

通常、IPv6 環境では図 1 のように、DHCP の代わりにルータ(以下、正規ルータ)が 2 種類の方法を用いてアドレス生成を行う。

いずれかの方法によって RA メッセージを受信したクライアント PC は、メッセージ内に保持されたプレフィックスという値(IPv4 でのネットワークアドレスに相当)と自身の MAC アドレスによって IPv6 アドレスを生成する。また、RA メッセージ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。

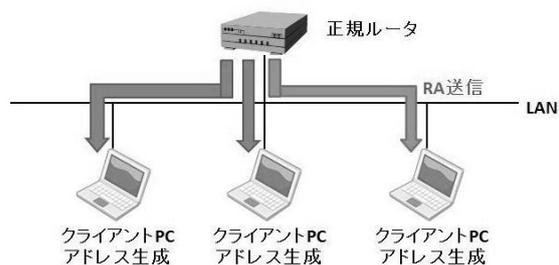


図 1 正規ルータによる RA 送信の流れ

一方、クライアント PC も RA メッセージを送信することが可能であり、LAN に接続したクライアント PC が不正に RA メッセージ(以下、不正 RA)を送信することでルータへのなりすまし(以下、

攻撃者 PC)を行うことが可能である。ここで、RA メッセージにはルータの優先度を設定することが可能であり、low, medium, high の 3 種類が定義されている[4]。この時、正規ルータが送信する RA メッセージよりも不正 RA の優先度の方が高く設定されていた場合、ネットワーク内の全てのクライアント PC(以下、被害者 PC)は図 2 の①のように一度通信を攻撃者 PC へ送信し、攻撃者 PC は図 2 の②のように正規ルータへ通信を転送することで、通信傍受が行われることが先行研究から判明している。

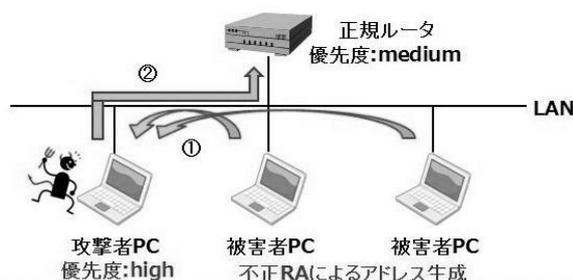


図 2 攻撃者 PC による通信傍受

また、正規ルータのルータ優先度の初期設定は medium に設定されており、設定が変更できるルータは非常に高価、且つ手間がかかるとされている。一方、攻撃者が通信傍受に利用すると推測されるツールは変更が自由である為、攻撃者は不正 RA のルータ優先度を予め high に変更し、通信傍受を行うことが予想された。

## 2.2 先行研究の提案手法

この問題に対し、著者らは被害者 PC 側における RA メッセージのメッセージフォーマットに基づいたフィルタリング手法を提案した。メッセージフォーマットは RFC4191 に規定されており、その中でルータ優先度を決定しているフィールドの値を参照し、RA メッセージのルータ優先度が high に設定された RA メッセージのみをフィルタリングするというものである[4]。先行研究にて機能、及び性能共に実装しても問題無いことを確認した。

## 3 更なる通信傍受方法の示唆

本章では、攻撃者が更なる攻撃を行う上で利用すると推測される、RA メッセージのルータ優先度が等しく設定されている場合の被害者 PC 側の OS の動作についての調査及び実験結果について述べ、考察を行う。

### 3.1 同優先度におけるクライアント PC の動作

本来、IPv6 環境下において複数のルータが同一ネットワーク内に存在する場合、クライアント PC は RA メッセージに設定されている優先度によって通信に使用するルータの優先度を決定する。しかし、そのルータ同士の優先度が同程度であった場合、優先されるルータは OS によって異なるということが、IPv6 普及・高度化推進協議会が 2009 年に作成したガイドラインで述べられており、表 1 の通りとなっている[5]。

表 1 OS 別におけるルータの優先順位

OS	同優先度での動作
Windows XP	後の RA を優先
Windows Vista	先の RA を優先
Windows 7 RC	先の RA を優先
Linux(2.6.17 以降)	先の RA を優先
FreeBSD(6.1R 以降)	先の RA を優先

しかし、IPv6 普及・高度化推進協議会へ問い合わせを行ったところ、Windows7 に関しては動作確認を行っていないこと、またそれ以外の OS に関しては動作が変更されている可能性があることが判明した。そこで著者らは実際にガイドライン通りの動作を行うか実験を行った。

### 3.2 同優先度における OS の動作確認

本節では、3.1 節にて述べた動作の確認を行い、そこから行われ得る通信傍受の方法、及び実験から得られた考察を述べる。尚、今回動作の確認を行った OS は Windows Vista 及び 7 の 2 種類のみである。

本実験の実験環境は表 2、ネットワーク環境

は図3の通りである。

表2 実験環境

使用ルータ	RTX1200
攻撃者 PC	Vine Linux-2.6.12
使用ツール	RADVD-1.0 Wireshark-1.4.6

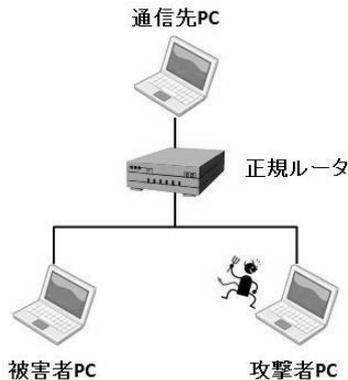


図3 ネットワーク環境

本実験では、RAメッセージに設定されているルータの優先度が同程度の場合における、OSによるルータ選択の動作を確認する。尚、正規ルータと攻撃者PCが送信するRAメッセージのプレフィックスなどの諸設定は等しく設定されている。手順は以下の通りである。

- (1). 正規ルータによる RA メッセージの送信
- (2). 攻撃者 PC による不正 RA の送信
- (3). 通信先 PC に対して被害者 PC が通信を行う
- (4). (1)と(2)を入れ替えて同様に通信

以上の手順を、被害者 PC の OS が Windows Vista, 及び 7 の 2 種類の場合に分けて行った。その結果は表 3 の通りである。

表3 OS 別におけるルータの優先順位結果

OS	正規ルータの RA 送信	攻撃者 PC の RA 送信	通信傍受
Vista	先	後	不可
	後	先	一部可
7	先	後	可
	後	先	可

尚、被害者 PC の OS が Windows Vista, 攻撃者 PC が先に RA メッセージを送信していた場合の通信傍受が一部可となっている理由は、初回の通信では攻撃者 PC を介して通信が行われるが、攻撃者 PC の ICMP Redirect によってその後の通信に攻撃者 PC が仲介しなくなる為である。

### 3.3 考察

本実験の結果から、被害者 PC の OS が Windows 7 であれば正規ルータと攻撃者 PC の優先度が同程度であっても通信傍受が行えることが判明した。また、OS が Windows Vista の場合はガイドライン通りの動作を行うが、正規ルータよりも攻撃者 PC が先に RA メッセージを送信すれば正規ルータよりも優先されることが判明した為、攻撃者 PC が ICMP Redirect を送信しなければ Windows 7 と同様に通信を傍受できると推測される。

## 4 対策の提案

本章では、3 章にて示唆した攻撃方法についての問題点をまとめ、それに対する対策手法を提案する。

### 4.1 問題点のまとめ

3 章にて示唆した攻撃方法は、RAメッセージに設定されたルータの優先度が同程度であった場合における OS のルータ選択の動作を利用したものであり、Windows Vista では特定の条件において、Windows 7 では無条件で通信を傍受することが可能であることが分かった。この攻撃の問題点は正規ルータと攻撃者 PC の見分けがつかない点にある。先行研究にて想定した攻撃方法の場合は、RA メッセージに設定されているルータ優先度の差を用いた方法であった為、正規ルータと攻撃者 PC を見分けることができた。しかし、本研究での攻撃方法の場合、

3.2 節にて述べたように RA メッセージの設定を全て等しく設定して攻撃を行っている為、被害者 PC から一見ただけでは見分けがつかないという問題がある。

## 4.2 提案手法

4.1 節で示したように、被害者 PC からは正規のルータと攻撃者 PC のどちらから RA メッセージを送信されたかを確認することができない為、著者らは RA メッセージの特性を利用した提案手法を提案する。

ここで、RA メッセージの特性について述べる。ルータには一定の間隔で RA メッセージを送信する値が定義されており、この値はネットワークごとに変更することが可能である。ネットワーク内に存在するクライアント PC は一定間隔で送信される RA メッセージを受信し、IPv6 アドレスを構成する動作を行っている。

そこで本稿では、直前に受信した RA メッセージとの時間差分を算出し、受信した間隔が一定でなければ特定の処理を行う手法を提案する。通常であれば図 4 の①のように正規ルータから一定の間隔で RA メッセージの送信が行われる。一方、攻撃者 PC がネットワーク内に存在している場合、正規ルータによる RA メッセージの送信と攻撃者 PC による不正 RA の送信が行われる為、図 4 の②のように RA メッセージが異なった間隔で被害者 PC に受信されると想定される。従って、RA メッセージを受信した間隔が異なる場合は正規ルータ以外のネットワーク機器、すなわち攻撃者 PC による不正 RA が送信されていると判断し、後述する 2 種類の処理のいずれかを行うという手法を著者らは提案する。尚、ネットワークに送信されている全ての RA メッセージに処理を行うのではなく、現在デフォルトゲートウェイとして利用している IPv6 アドレスのプレフィックスと同値である RA メッセージに対して処理を行うこととする。

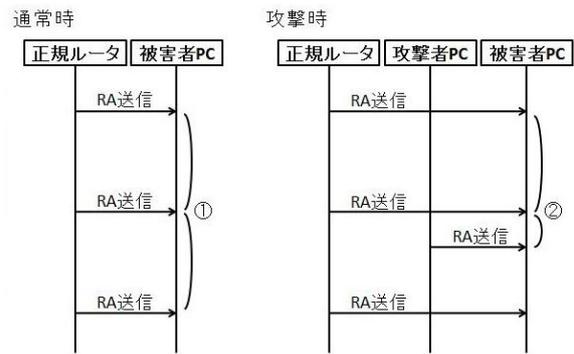


図 4 RA 送信の時間間隔

攻撃者 PC から RA メッセージが送信されていると判断した場合に行われる処理として提案する手法は以下の 2 種類である。

- (i). RA メッセージの送信者の IPv6 アドレスごとに RA メッセージの受信回数を保持しておき、最も受信回数が多い IPv6 アドレスをデフォルトゲートウェイとして利用
- (ii). 異なった間隔の RA メッセージの受信を拒否し、被害者に対して警告を表示

手法(i)は、被害者 PC がネットワークに接続した時から RA メッセージの送信者の IPv6 アドレスごとに RA メッセージの受信回数を保持しておき、異なる間隔で RA メッセージが送信された場合は最も受信回数が多い、すなわちネットワークに接続してから受信回数が最も多い RA メッセージの受信のみを許可する処理である。

一方、手法(ii)は、異なった間隔の RA メッセージが受信された際、その RA メッセージを破棄し、被害者 PC に対して警告を表示するという処理である。

## 5 提案手法の比較と評価

本章にて、4.2 節で述べた提案手法の比較、及び評価について述べる。

まず、手法(i)について述べる。メリットとして、攻撃者 PC よりも先にネットワークに接続していた場合、正規ルータとの通信を確立することが可能である。また、同一ネットワーク上に同値のプレフィックスを送信する正規ルータが複数存

在する場合でも対応することが可能である。しかし、攻撃者 PC が先に RA メッセージを送信した場合、攻撃者 PC との通信が確立してしまう恐れがある。また、RA メッセージの受信回数を制御する機能が別途必要となってしまう、被害者 PC 側に負担がかかってしまうことが考えられる。

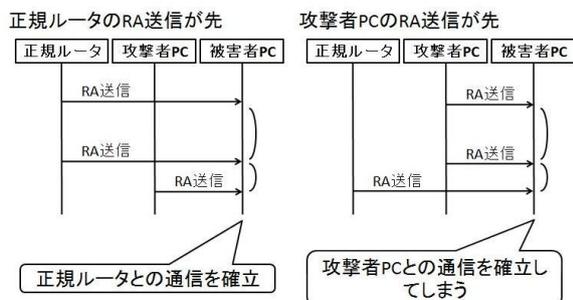


図 5 手法(i)における RA メッセージの処理

次に、手法(ii)について述べる。この手法は手法(i)のような別途の機能は必要なく、非常に容易な処理のみで対策を行うことが可能である。また、被害者自身に警告を促すことで余計な通信を抑制する効果があると考えられる。さらに、この手法の場合、図 6 のように攻撃者 PC が先に RA メッセージを送信した場合であっても、その後の正規ルータの RA メッセージによって被害者 PC へ警告が表示される為、被害拡大の抑制を期待することができる。

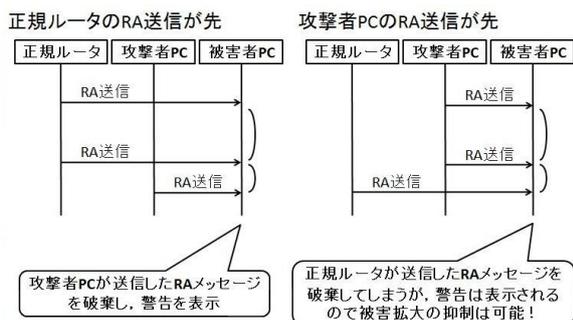


図 6 手法(ii)における RA メッセージの処理

両者の手法を比較すると、被害拡大の抑制という点において手法(ii)の方がより実用的であり、効果的であると著者は考える。

最後に提案手法の評価についてであるが、時間差分による手法は、RA メッセージが一定間隔で送信されるという特性に基づいて提案し

ており、この手法を用いることで攻撃者 PC による通信傍受の成功率を低減することが可能であり、さらなる攻撃に対する攻撃コストの増加を期待することができる。しかし、通信の状態によっては時間間隔が変動してしまい、それによって通信が行えなくなってしまうことも考えられる為、受信の際の時間間隔の閾値の最適化を図る必要があると考えられる。

## 6 終わりに

本稿では、IPv6 アドレス自動生成時におけるルータへのなりすましによる通信傍受のさらなる攻撃として、ルータの優先度が同程度の場合における OS の挙動を利用した攻撃手法を推測し、実験によりその危険性を示した。また、その対策として 2 種類の手法を提案・比較し、後者の手法の実用性を示した。

今後は時間差分の算出値の最適化を図ると共に、提案手法の開発、及び実装を行い、性能評価を行う予定である。

## 参考文献

- [1]. JINIC(Japan Network Information Center) 「IPv4 アドレスの枯渇に関して」 2011 年 4 月 15 日, <http://www.nic.ad.jp/ja/ip/ipv4pool/>
- [2]. RFC4862 IPv6 Stateless Address Autoconfiguration, September 2007, <http://tools.ietf.org/html/rfc4862>
- [3]. 坂本知弥, 甲斐俊文, 佐々木良一 “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”, 情報処理学会研究報告 Vol.2011-CSEC-52, No.5, pp.1-7, 2011 年 3 月
- [4]. RFC4191 Default Router Preferences and More-Specific Routes, November 2005, <http://tools.ietf.org/html/rfc4191>
- [5]. IPv6 普及・高度化推進協議会「IP4 サーバ環境への IPv6 導入ガイドライン」 2009 年 11 月, p129, [http://www.v6pc.jp/jp/upload/pdf/IPv6ServiceDeployment\\_Guideline.pdf](http://www.v6pc.jp/jp/upload/pdf/IPv6ServiceDeployment_Guideline.pdf)