IPv6 通信の学習に基づく NDP 悪用攻撃対策手法の提案

衛藤将史† 鈴木 未央† 小林 悟史‡ 井上大介† 中尾康二†

† 独立行政法人 情報通信研究機構
東京都小金井市貫井北町 4-2-1

‡ 株式会社ディアイティ
東京都江東区東陽三丁目 23 番 21 号プレミア東陽町ビル

あらまし IPv6 環境における脅威の大半は，IPv6 アドレスの詐称による Neighbor Discovery Protocol (NDP : 近隣探索プロトコル) の悪用に起因することが明らかとなっている．本研究では，L2 スイッチ上において NDP の悪用を防止するシステム NDP Guard を提案する．NDP Guard はネットワークに接続された端末の物理ポート，MAC アドレスおよび IP アドレスの組を記憶することで，条件に合致しないノードの通信を不正通信として破棄する．これにより IPv6 環境における攻撃の多くを防ぐことが可能となる．本稿では NDP Guard の Open vSwitch をベースとしたプロトタイプ実装をもちいて，24 件の攻撃シナリオをもちいて検証し，NDP を悪用した攻撃に対する提案手法の有効性の評価を行う．

A Method for Prevention of Attacks Abusing NDP based on Learning IPv6 Communications

Masashi Eto† Daisuke Inoue† Mio Suzuki† Koji Nakao†

†National Institute of Information and Communications Technology (NICT)
4-2-1, Nukui-Kitamachi, Koganei, Tokyo, 184-8795, Japan

Abstract Through our experiments and analysis of security threats on IPv6 environment, we have recognized that abuse of Neighbor Discovery Protocol (NDP) is the primary cause of the most of the threats. This paper proposes “NDP Guard”, a method to prevent abuses of NDP, which runs on a layer 2 (L2) switch. NDP Guard learns a combination of physical port, MAC address and IPv6 address of hosts connected to the L2 switch, and discards packets that are unmatched to predefined policies as abused access. This paper introduces the mechanism of NDP Guard and implementation of a prototype system based on Open vSwitch. Some evaluations of effectiveness of the proposed system are also presented by applying practical twenty four attack scenarios of abusing NDP.

1 はじめに

世界的に IPv6 への対応が進む一方で，IPv6 のセキュリティ上の脅威が数多く指摘されており，それが IPv6 のより一層の普及促進を阻む一つの要因となっている．これに対し，IETF，ITU-T，NIST (アメリカ国立標準技術研究所) をはじめとする国内外の標準化団体や研究機関，さらに各 IPv6 関連製品ベンダなどによって，IPv6 ネットワーク上の脅威とと対策の検討が進められているが，[1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 17, 18] 根本的な対策は十分に進んでいないのが現状である．

また，著者らは，IPv6 セキュリティについての検討を行う国内組織である IPv6 技術検証協議会おいて，参加企業が提供する IPv6 対応製品・サービスをもちいて，既知・未知の脅威の検証作業を行い，これらの脅威への対策の検討および検証作業を行ってきた [17]．その結果，IPv6 における脅威の多くは IPv6 において導入された近隣探索プロトコル (Neighbor Discovery Protocol: NDP) が原因となっていることが明らかとなった．

NDP は IPv4 における ARP に相当する機能として IPv6 に導入された近隣探索のためのプロトコルである．ここでは ルータ発見 (RD) やアドレス解決といった近隣探索機能のほか，IPv6 アドレスの自動設定や重複アドレス検出，リダイレクトなど，さまざまな機能が提供されている．

しかし，NDP に含まれるさまざまな機能には全般的に，その設計段階からセキュリティに関する検討が不足しており，それがさまざまな脅威の原因と

なっている．例えば，ルータ発見 (RD) はルータがデフォルト経路を配信するための機能であるが，ルータ広告 (RA) メッセージを受信したノードが，メッセージの送信元であるルータを認証する機能は元来提供されていない．したがって，ローカルネットワーク内において攻撃ノードがルータになりすまして RA メッセージを送信した場合，受信ノードは攻撃ノードをデフォルト経路として通信を行い，結果として，すべての通信を盗聴されることとなる．

このほかにも IPv6 における NDP を悪用した攻撃手法は数多く知られており，このような攻撃を防御するための根本的な対策が必要とされている．したがって本研究はレイヤー 2 (L2) スイッチ上で IPv6 通信を学習し，あらかじめ設定されたポリシーにもとづいて前述の NDP 悪用攻撃を対策するための手法を提案する．

本稿ではまず第 2 章において，関連研究に触れた上で，第 3 章で提案手法である NDP Guard について述べる．第 4 章で実験環境による評価と考察を行い，最後に第 5 章でまとめを述べる．

2 関連研究

IPv6 の NDP 機能は RFC 4861 [19] において規定されている．NDP は IPv4 の ARP の機能を代替するだけにとどまらず，プラグアンドプレイと呼ばれる自動設定機能をはじめ，ルータ，プレフィックス，パラメタの探索，アドレス自動設定，アドレス解決，重複アドレス検出，リダイレクトなど数多くの機能が提供されている．

また，IPv4 では近隣探索プロトコルとして Address Resolution Protocol (ARP) [20] が用いられてきたが，IPv6 NDP では以下の 5 種類の ICMPv6 [21] が用いられる: ルータ要請 (Router Solicitation: RS)，ルータ広告 (Router Advertisement: RA)，近隣者要請 (Neighbor Solicvitation: NS)，近隣者広告 (Neighbor Advertisement: NA)，リダイレクト (Redirect)．これらの機能により，IPv4 と比較して IPv6 の利便性は大きく高まり，同時に運用面での負担を削減することとなった．

このようにさまざまな機能を追加した一方で，NDP はその仕組みの複雑さと設計時のセキュリティへの考慮不足により，さまざまなセキュリティ上の脅威の原因となっている．根本的な対策としては，NDP にノードの認証機構を導入するなどの工夫が考えられるが，IPv6 はすでに普及し，さまざまな機器において広く使用されているため，現時点で NDP に仕様変更を加える事は影響範囲が大きく好ましくない．したがって，既存の NDP の仕様はそのままに運用面においてそのセキュリティ上の脅威を防ぐ手法を確立する必要がある．

3 提案手法

本研究では，L2 スイッチ上において NDP の悪用を防止するシステム NDP Guard を提案する．NDP Guard はネットワークに接続された端末の物理ポート，MAC アドレスおよび IP アドレスの組を記憶することで，あらかじめ設定されたポリシーに合致しないノードの通信を不正通信として破棄する．これにより IPv6 環境における攻撃の多くを防ぐことが可能となる．

3.1 概要

NDP Guard の概要を図 1 に示す．

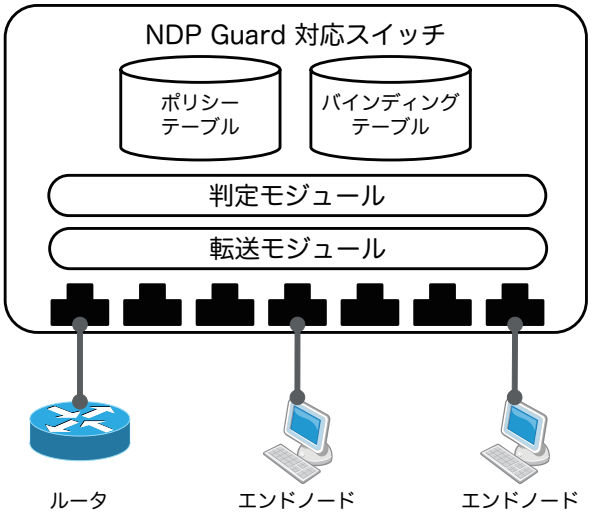

図 1: NDP Guard の概要図

NDP Guard は L2 スイッチにおいて，Ethernet フレームの L2 アドレス (MAC アドレス) と L3 アドレス (IPv6 アドレス) とその入力元物理ポートの組をテーブル上で管理する．このテーブルをバインディングテーブル (第 3.3 節) と呼び，NDP Guard はすべての入力パケットに対してこのテーブルとの照合を行い，IPv6 アドレスの詐称が行われたパケットを不正と判断し破棄する．さらに，IPv6 アドレスの詐称ではなく，あたかもルータのように虚偽の RA や ICMPv6 リダイレクトを送信する攻撃を防ぐため，ポリシーテーブル (第 3.2 節) において各物理ポートの信頼情報を管理しておく．信頼できる物理ポートにルータなどのネットワーク機器のみを接続しておくことで，それ以外の物理ポートから流入した NDP パケットを不正と判断し破棄する．

全体の処理の流れを図 2 に示す．NDP Guard は IPv6 パケットを受信すると，はじめにポリシーテーブルおよびバインディングテーブルを参照してパケットの転送可否を決定する．ポリシーテーブルには，物理ポートごとにパケットの転送条件 (ポリシー) が記

述されており，バインディングテーブルは Ethernet フレームの L2 アドレス (MAC アドレス) と L3 アドレス (IPv6 アドレス) とその入力元となった物理ポートを一つのエントリとした情報が自動的に格納されている．ポリシーテーブルの転送条件判断のために，バインディングテーブルのエントリの情報が参照されることとなる．

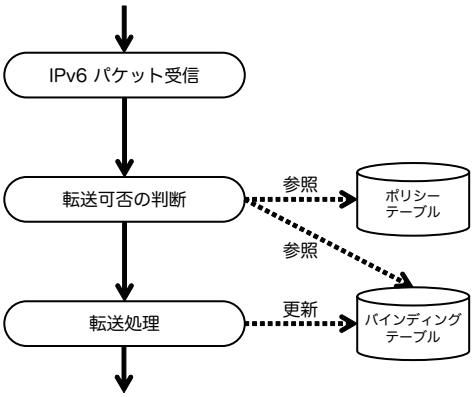

図 2: 処理の流れとテーブルの関係

3.2 ポリシーテーブル

ポリシーテーブルは，スイッチングを行う各物理ポートに対して適用されるポリシーを保持するテーブルであり，物理ポートの信頼情報を記録する「物理ポート定義テーブル」とポートごとにパケットの通信の可否を定義する「トラフィック制御テーブル」から構成される．物理ポート定義テーブルには，スイッチの物理ポートがそれぞれ信頼できるか否かが記述され，この信頼情報が後述するバインディングテーブルの学習の際に参照される (表 1)．ここで信頼できる物理ポートとは，正規のルータやサーバが接続され，詐称したノードからの不正パケットが流入しないことを意味する．したがって，ネットワーク管理者は当該物理ポートには正規のルータやサーバ以外のノードを接続しないよう厳密に運用する必要がある．

表 1: 物理ポート定義テーブルのエントリの例

ポート	属性
eth0	信頼できるポート
eth1	信頼できるポート
eth2	信頼できないポート
eth3	信頼できないポート

また，トラフィック制御テーブルには，パケットに適用するポリシーを記述する (表 2)．ここでは物理ポートごとに，プロトコルおよび IPv6 アドレスで指定されたパケットと，そのパケットに対するアクションが規定される．

3.3 バインディングテーブル

バインディングテーブルは Ethernet フレームの L2 アドレス (MAC アドレス) と L3 アドレス (IPv6 アドレス) とその入力元となった物理ポートを一つのエントリとした情報を格納しており，IPv6 アドレスの詐称による NDP を悪用した不正パケットの検知に用いられる．バインディングテーブルのエントリの例を表 3 に示す．バインディングテーブルのエントリは，パケットの監視により動的に生成される．新しいパケットを検知した際に必要となるパラメータ (送信元 MAC アドレス，送信元 IPv6 アドレス，入力元インターフェイス) をパケットから抽出してバインディングテーブル上に新しいエントリを作成する．タイマにはエントリが作成された時点，またパケットが再観測された時点で規定の値を設定し，一定間隔で減少させる．エントリの新しさを保つため，バインディングテーブルのエントリ上のタイマ値が 0 になった時点で当該エントリを破棄する．なお，観測されたパケットが NA や重複検知メッセージ (Duplicate Address Detection: DAD) の場合には，送信元 IPv6 アドレスではなく，NA および DAD メッセージにおいて指定されたターゲットアドレスをエントリに追加する．

3.4 ポリシーの検討

NDP Guard では，図 2 に示すように，判定モジュールがこれまでに述べたポリシーテーブル，バインディングテーブルを参照しながら，設定されたポリシーにしたがってパケットの転送可否を決定する．一方 IPv6 環境における NDP を悪用した脅威は，ルータを詐称することによる攻撃，ノードを詐称することによる攻撃，サーバを詐称することによる攻撃，そして DoS 攻撃の 4 つに類型化することができる．したがって，それぞれに対して適切なポリシーを検討する必要がある．

ルータを詐称する攻撃に対する防御　ルータを詐称して虚偽の RA や他のパケット (ICMPv6 リダイレクトや too big メッセージ) を送信することにより通信を妨害する攻撃に対しては，表 4 のようなポリシーを設定する．この設定により，信頼できないポートからの RA の送信をすべて破棄し，ルータの詐称による攻撃からノードを防御することが可能となる．また，ICMPv6 リダイレクトや too big メッセージなど，本来ルータからしか送信され得ないパケットによる攻撃からノードを防御することも可能となる．

表 2: トラフィック制御テーブルのエントリの例

ポート	プロトコル	優先度	アドレス	アクション
eth0	any	1	any	フォワード
eth1	any	1	any	フォワード
eth2	NDP	1	他物理ポートにバインドされたアドレス	ドロップ
eth2	UDP	10	ソースポート 53	ドロップ
eth3	TCP	10	宛先ポート 80	ドロップ

表 3: バインディングテーブルのエントリの例

送信元 MAC アドレス	送信元 IPv6 アドレス	入力ポート	タイマ
00:10:bc:de:93:12	2001:db8:cafe::1	eth0	3549
00:10:bc:de:93:20	2001:db8:cafe::53	eth1	1825
a0:eb:90:3e:01:09	2001:db8:cafe:1:98b3:b2b0:8721:0b9f	eth2	92
52:54:00:57:c7:2d	2001:db8:cafe:1:5054:ff:fe57:c72d	eth3	319
:	:	:	:

ノードを詐称する攻撃に対する防御　他のノードを詐称して NA を広告する (あるいは DAD に対して NA や DAD を返す) ことにより通信を妨害する攻撃に対しては，表 5 のようなポリシーを設定する．この設定により，すでに他の物理ポートのバインディングテーブルに記載されている IPv6 アドレスを使用してパケットを送信した場合に，そのパケットは破棄される．また，他の物理ポートのバインディングテーブルに記載されているアドレスを使用して DAD を行う (悪意の) ノードが会った場合は，当該パケットを破棄することにより，アドレスの詐称 (乗っ取り) を抑制することが可能となる．

サーバを詐称する攻撃に対する防御　DHCPv6 サーバや DNS サーバを詐称して虚偽の情報を送信する攻撃に対しては，表 6 のようなポリシーを設定し，DNS や DHCPv6 サーバを信頼できるポートに接続する．この設定により，サーバを詐称して他のノードに虚偽の情報を送信しようとした場合，それらのパケットは破棄される．

DoS 攻撃に対する防御　大量のセッションを作成する，あるいは大量のノードを詐称してサービスを妨害する DoS 攻撃に対しては，各ポートのバインディングテーブルのエントリ数の上限値を適切に設定し，かつ表 7 のポリシーを使用する．この設定により，多数のアドレスを詐称して大量のセッションを作成しようとした場合，バインディングテーブルのエントリ数が上限に達する．そのため，新たなアドレスを使用して詐称パケットを送信しようとした場合，新しいレコードをバインディングテーブルに加えることができず，当該パケットは破棄される．

4　評価

これまでに述べた提案手法の仕様にしたがい，本稿ではオープンソースの仮想 L2 スイッチソフトウェアである Open vSwitch を基礎に，提案手法のプロトタイプ実装を行った．本稿では，このプロトタイプ実装を含む検証環境を構築し，IPv6 環境において NDP を悪用する模擬攻撃シナリオを用いた実験を行うことで，提案手法の有効性を評価する．模擬攻撃シナリオとして，IPv6 技術検証協議会において実施された 40 の攻撃シナリオ [17] のうち，NDP を悪用した攻撃である 24 シナリオ (表 10) を抽出して評価を実施する．また，攻撃検知の偽陽性に関する評価として，一般的な通信において誤検知が無いことを確認する．

4.1　評価環境

評価のため図 3 に示す環境を構築した．本環境には中央の境界ルータをはさんで 2 つの L3 セグメント (実験ネットワーク 1，2) が用意され，それぞれのセグメントに攻撃ノードおよびユーザノードが配置されている．NDP Guard 対応 L2 スイッチは実験ネットワーク内のアクセス用スイッチとして実験ネットワーク 2 に設置され，境界ルータ，攻撃ノード Y，ユーザノード B および E が接続されている．実験作業の管理のため，すべてのマシンは管理ネットワークに接続されているが，予期せぬ実験トラフィックの流入を避けるため，管理ネットワークにおいては IPv4 アドレスのみを使用している．攻撃シナリオでは，攻撃ノード X，Y から NDP Guard 配下の他のノード (ユーザノード B，E) や，境界ルータの対向側の各ノード (ユーザノード A，C，D)，さらに境界ルータ自体に対して，不正な NDP パケット等を送信することで攻撃を行い，ユーザノードの

表 4: ルータ詐称攻撃に対するポリシー

属性	対象パケット	アクション
信頼できるポート	ANY	フォワード
信頼できないポート	RA	ドロップ
信頼できないポート	ICMPv6 リダイレクト	ドロップ
信頼できないポート	ICMPv6 too big	ドロップ

表 5: ノード詐称攻撃に対するポリシー

属性	対象パケット	アクション
信頼できるポート	ANY	フォワード
信頼できないポート	他物理ポートのバインディングテーブルに存在するパケット	ドロップ
信頼できないポート	他物理ポートのバインディングテーブルに存在する DAD パケット	ドロップ

通常の通信を阻害する．したがって，本研究においては NDP Guard を介して通信することで，さまざまな攻撃シナリオが無効化されることを確認する．

なお，第 3.2 節で言及したポリシーテーブルにおける物理ポート定義テーブルには，表 8 に示す値を設定した．すなわち，図 3 内の NDP Guard 対応 L2 スイッチでは，境界ルータが接続された物理ポートのみを信頼できるポート，その他のポートを信頼できないポート (不正通信が行われる可能性のあるポート) として設定した．

表 8: NDP Guard 対応 L2 スイッチにおける各ノードの信頼設定

機器名	trusted
境界ルータ	true
攻撃ノード Y	false
ユーザノード B	false
ユーザノード E	flase

また，同じく第 3.2 節におけるトラフィック制御テーブルには各種攻撃を防ぐため，表 9 で示すポリシーを設定している．

4.2 異常通信 (各種攻撃シナリオ) の検知

評価には文献 [17] に記載されているうち，NDP が原因となって引き起こされている 24 の攻撃シナリオを用いた．

紙面においてすべてのシナリオの評価結果の詳細を記載することは困難であるため，本稿においては検証を実施したシナリオの一部の結果を掲載する．

4.2.1 シナリオ 1: 詐称した RA を送信してユーザトラフィックを盗聴する

本攻撃シナリオでは，攻撃ノード Y がユーザノード B に対して Y 自身をデフォルト経路と詐称する RA メッセージを継続的に送信し，ユーザノード B のデフォルト経路を攻撃ノード Y に仕向けることで，ユーザノード B の通信の盗聴を試みる．

このような本来の攻撃に対して，本検証環境において実行された結果を図 4 に示す．ここでは，実験開始 0 秒後から 1 分 10 秒後までの時系列 (X 軸) に沿うかたちで環境上の各ノードの活動を可視化している．ここでは，実験開始 10 秒後から開始された攻撃ノード Y からの RA が NDP Guard によって停止され，ユーザノード B に到達していないことがわかる．これは攻撃ノード Y が NDP Guard における信頼できない物理ポートに接続されていることから，表 9 の RA をドロップするポリシーに抵触し，パケットが破棄されたためである．

RA パケットが破棄されたことでユーザノード B における不要な経路変更が発生しなかったため，実験開始 40 秒後に開始されたユーザノード B からユーザノード A への HTTP 通信は，結果的に正常に行われたことが確認された．

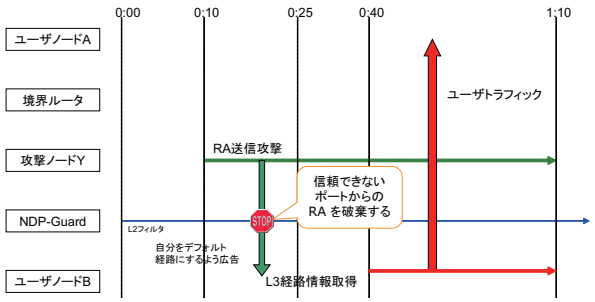

図 4: 攻撃シナリオ 1 におけるタイムライン

表 6: サーバ詐称攻撃に対するポリシー

属性	対象パケット	アクション
信頼できるポート	ANY	フォワード
信頼できないポート	DNS サーバ用ポートからのパケット	ドロップ
信頼できないポート	DHCPv6 サーバ用ポートからのパケット	ドロップ

表 7: DoS 攻撃に対するポリシー

属性	対象パケット	アクション
信頼できるポート	ANY	フォワード
信頼できないポート	すべてのバインディングテーブルに存在しないパケット	フォワード

```
# 他ポートに登録されているアドレスを
# ターゲットとした DAD/NA をドロップ
eth1 1 drop nsna binding other

# 他ポートに登録されているアドレスを
# ソースアドレスとしたトラフィックをドロップ
eth1 2 drop any binding other

# RA をドロップ
eth1 3 drop icmp 134 any

# リダイレクトをドロップ
eth1 4 drop icmp 137 any

# TOO BIG をドロップ
eth1 5 drop icmp 2 any

# UDP 53（DNS サーバ）をソースとする
# パケットをドロップ
eth1 6 drop udp port 53 any

# UDP 547（DHCPv6 サーバ）をソースとする
# パケットをドロップ
eth1 7 drop udp port 547 any

# UDP 546（DHCPv6 クライアント）宛の
# パケットをドロップ
eth1 8 drop udp port any 546
```

表 9: 投入したポリシー

4.2.2 シナリオ 2: 大量の NS/NA を発生させてルータの L2 経路情報を溢れさせる

本攻撃シナリオは，攻撃ノード X および Y が結託して大量の NS/NA メッセージを発生させることにより，境界ルータの L2 経路テーブルを溢れさせるものである．ここで攻撃ノード X は，解決対象の IPv6 アドレスを順次変化させながら NS メッセージによる問い合わせを行い，攻撃ノード Y がそれらの問い合わせに自動的に応答する．攻撃ノード X は受信した応答メッセージの処理は特に行わないが，境界ルータはそれらのアドレス情報を記憶しておく必要があるため，結果的に境界ルータの L2 経路テーブルが溢れることになる．

このような本来の攻撃に対して，本検証環境において実行された結果を図 5 に示す．ここでは，実験開始 30 秒後から NS/NA の大量送信が開始されるが，じきに NDP Guard において適切に設定されたバインディングテーブルのエントリ数の上限値に達し，それ以降のパケットが破棄される．これにより，境界ルータに必要以上の NS/NA メッセージが到達しなかったため境界ルータのパフォーマンス低下が避けられ，結果的にユーザの通信も問題なく行われた．

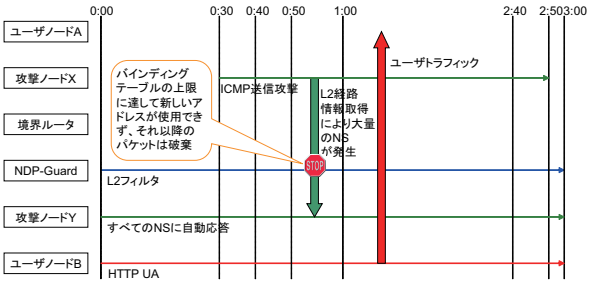

図 5: 攻撃シナリオ 2 におけるタイムライン

以上の攻撃をはじめとして，表 10 に示す全攻撃シナリオについて評価を行い，これらの攻撃がすべて無効となることを確認した．

4.3 通常の L7 通信への影響

NDP Guard が通常の通信に与える影響を評価する．具体的には，さまざまなアプリケーション (L7) プロトコルを用いた通常の通信が NDP Guard によって阻害されないことを確認する．本評価では，表 11 に示す各アプリケーションプロトコルについて，ユーザノード B および E の間で，双方向から

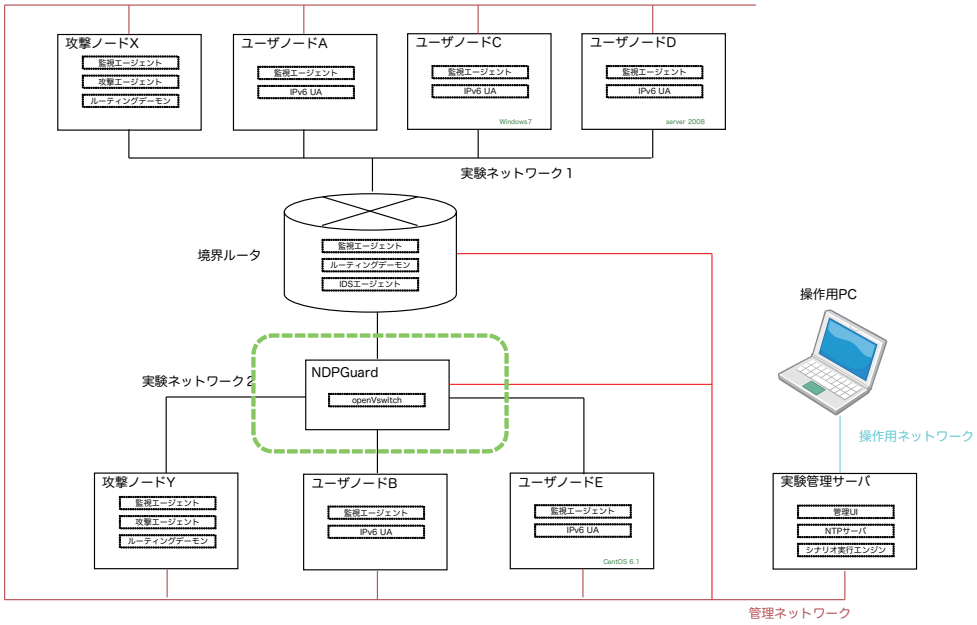

図 3: NDP Guard の評価環境

の接続要求に対して各アプリケーション (L7) のコネクションが確立されることを確認した．このことから，通常の通信において提案手法が既存の通信プロトコルに悪影響をおよぼさないことがわかった．

5 おわりに

本稿では，IPv6 環境における脅威の多くが NDP の悪用に起因していることから，NDP を悪用した攻撃を防ぐ機構 NDP Guard を提案した．NDP Guard は L2 スイッチとして機能しながら，入力トラフィックの物理ポート，MAC アドレス，IPv6 アドレスを記憶し，あらかじめ設定されたポリシーにしたがってパケットの転送可否を決定する．これにより，適切にポリシーを設定することでホストの詐称や DoS 攻撃といった NDP の悪用による攻撃を防ぐことが可能となる．また，本稿では Open vSwitch を基礎とした NDP Guard の実装を行った．そして評価環境において，24 の NDP 悪用攻撃シナリオに沿った実証実験を行い提案手法の有効性を評価した．実験の結果，NDP を悪用するすべての攻撃を防ぐことができることを確認した．攻撃シナリオによっては，複数の手順を踏んで攻撃を実施するが，いずれの攻撃も IPv6 アドレスの詐称といった攻撃のごく初期の段階で一連の攻撃を防ぐことが確認できた．また，さまざまプロトコルを用いた通信についても検証を行い，NDP Guard によって通常の通信が阻害されることがないことを確認した．今後はパフォーマンスに関する評価を行い，提案手法のスケーラビリティを検証する予定である．

参考文献

[1] J. Arkko, J. Kempf, B. Zill, and P. Nikander. SEcure Neighbor Discovery (SEND). RFC 3971 (Proposed Standard), March 2005. Updated by RFCs 6494, 6495.

[2] S. Kent and K. Seo. Security Architecture for the Internet Protocol. RFC 4301 (Proposed Standard), December 2005. Updated by RFC 6040.

[3] E. Davies, S. Krishnan, and P. Savola. IPv6 Transition/Co-existence Security Considerations. RFC 4942 (Informational), September 2007.

[4] P. Savola and C. Patel. Security Considerations for 6to4. RFC 3964 (Informational), December 2004.

[5] G. Nakibly and F. Templin. Routing Loop Attack Using IPv6 Automatic Tunnels: Problem Statement and Proposed Mitigations. RFC 6324 (Informational), August 2011.

[6] G. Van de Velde, T. Hain, R. Droms, B. Carpenter, and E. Klein. Local Network Protection for IPv6. RFC 4864 (Informational), May 2007.

[7] E. Davies and J. Mohacsi. Recommendations for Filtering ICMPv6 Messages in Firewalls. RFC 4890 (Informational), May 2007.

表 10: 検証された攻撃シナリオ

シナリオ
アドレスを詐称した NA をルータに送付してトラフィックを妨害する
詐称した RA をルータに送付してトラフィックを妨害する
詐称した ICMPv6 リダイレクトを送信してユーザトラフィックを盗聴する
詐称した ICMPv6 リダイレクトを送信してユーザトラフィックを妨害する
詐称した RA を送信してユーザトラフィックを盗聴する
詐称した RA を送信してユーザトラフィックを妨害する
DAD に対して NA を返し続けることによりユーザノードの IPv6 アドレス取得を妨害する
DAD に対して DAD を返し続けることによりユーザノードの IPv6 アドレス取得を妨害する
送信元を詐称したマルチキャストパケットを送信してパケットの増幅攻撃を行う
多量の NS/NA を発生させてルータの Neighbor Cache を溢れさせる
DHCPv6 サーバから虚偽の情報を送付することによる中間者攻撃
大量の DHCPv6 Solicite メッセージを送信し，DHCPv6 サービスを停止させる
大量の DHCPv6 によるアドレス取得を実施し，DHCPv6 サービスのアドレスプールを枯渇させる
thc-ipv6 を使った攻撃（MTU 縮小）を実施する
詐称した MLD listener done を使用してマルチキャストストリームを強制的に切断する
大量のセッションを作成して NAT64（NAT66）の状態テーブルを枯渇させる
大量の prefix を広告して端末のプレフィックステーブルを枯渇させる
大量のセッションを作成してファイアウォールのテーブルを枯渇させる
MAC アドレスの異なる大量のパケットを送信して FDB を枯渇させる
虚偽の DNS サーバの情報を RA で広告する
Anycast DNS を使用して虚偽の情報を送信する
RA で大量の more specific route を広告して端末のルーティングテーブルを枯渇させる
ソースアドレスを詐称して lifetime を 0 にした RA を広告し，端末に付与するプレフィクスを無効化する
虚偽の DHCPv6 サーバで広告した虚偽の DNS サーバから大量の AAAA レコードを送信して，アプリケーショントラフィックを妨害する

表 11: 正常通信の評価結果

プロトコル	結果
NS/NA (NDP)	✓
RS/RA (NDP)	✓
DHCPv6	✓
HTTP	✓
SSH	✓
FTP	✓
SMTP	✓
telnet	✓

[8] J. Abley, P. Savola, and G. Neville-Neil. Deprecation of Type 0 Routing Headers in IPv6. RFC 5095 (Proposed Standard), December 2007.

[9] T. Chown. IPv6 Implications for Network Scanning. RFC 5157 (Informational), March 2008.

[10] T. Chown and S. Venaas. Rogue IPv6 Router Advertisement Problem Statement. RFC 6104 (Informational), February 2011.

[11] E. Levy-Abegnoli, G. Van de Velde, C. Popoviciu, and J. Mohacsi. IPv6 Router Advertisement Guard. RFC 6105 (Informational), February 2011.

[12] M. Kohno, B. Nitzan, R. Bush, Y. Matsuzaki, L. Colitti, and T. Narten. Using 127-Bit IPv6 Prefixes on Inter-Router Links. RFC 6164 (Proposed Standard), April 2011. Updated by RFC 6547.

[13] D. Dugal, C. Pignataro, and R. Dunn. Protecting the Router Control Plane. RFC 6192 (Informational), March 2011.

[14] National Institute of Standards and Technology. IPv6 Guide Provides Path to Secure Deployment of Next-Generation Internet Protocol. http://www.nist.gov/itl/csd/ipv6_010511.cfm.

[15] IPv6 普及･高度化推進協議会 セキュリティWG. IPv6 対応セキュリティガイドライン（第 1.0 版）. http://www.v6pc.jp/jp/upload/pdf/swg-IPv6SecurityGuideline_v1.0.pdf.

[16] IPv6 普及・高度化推進協議会 IPv4/IPv6 共存 WG. IPv6 家庭用ルータガイドライン（2.0 版）. http://www.v6pc.jp/jp/upload/pdf/v6hgw_Guideline_2.0.pdf.

[17] IPv6 技術検証協議会. IPv6 技術検証協議会 セキュリティ評価・対策検証部会 最終報告書概要編. http://ipv6tvc.jp/documents/20121023Report.pdf, 2012.

[18] ITU-T. Recommendation itu-t x.1037 : Ipv6 technical security guidelines. *SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY*, 2013.

[19] Thomas Narten, Erik Nordmark, W Simpson, and H Soliman. Rfc4861: Neighbor discovery for ip version 6 (ipv6). *Standards Track, http://www. ietf. org/rfc/rfc4861. txt*, 2007.

[20] David C Plummer. Rfc 826: An ethernet address resolution protocol. *InterNet Network Working Group*, 1982.

[21] Alex Conta and Mukesh Gupta. Internet control message protocol (icmpv6) for the internet protocol version 6 (ipv6) specification. 2006.