

# IPv6脆弱性 VU#472363対応

2008/11/27

Hitachi Incident Response Team  
寺田真敏

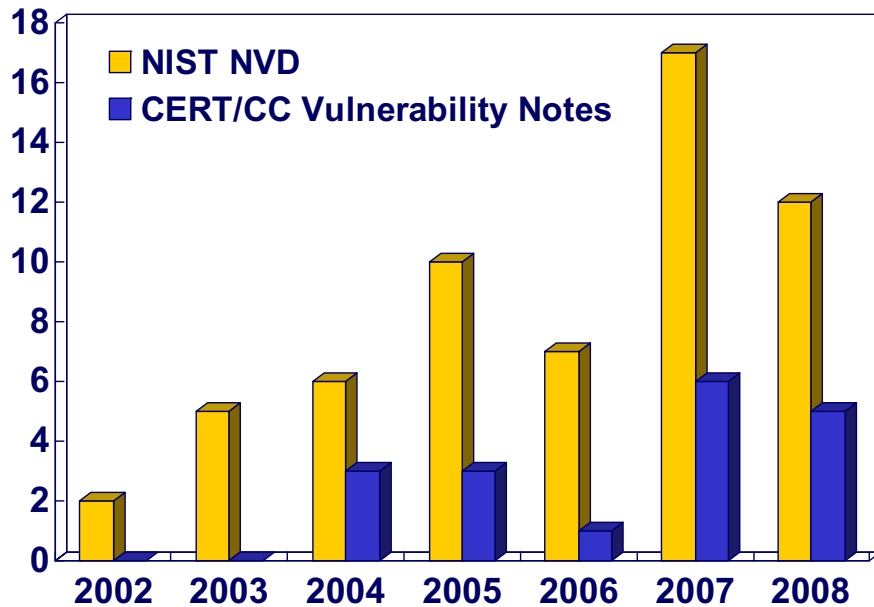
Copyright © Hitachi Incident Response Team. 2008. All rights reserved.

## Contents

1. IPv6に関する脆弱性報告
2. VU#472363の概要
3. VU#472363の対応経緯
4. 2008/9/11 VU#472363意見交換会
5. 脆弱性対応の課題

Copyright © Hitachi Incident Response Team. 2008. All rights reserved.

- IPv6に関する脆弱性報告件数は、少しずつではあるが、増えている。



IPv6に関する脆弱性報告の検索結果(2008年11月7日時点)

© Hitachi Incident Response Team. 2008.

- **CVE-2008-2085: SIPp Multiple Remote Buffer Overflow Vulnerabilities**  
Published: 05/12/2008、CVSS Severity: 7.5 (HIGH)
- **CVE-2008-1153: Cisco IOS Dual-stack Router IPv6 Denial Of Service Vulnerability**  
Published: 03/27/2008、CVSS Severity: 7.1 (HIGH)
- **CVE-2008-1057: OpenBSD ip6\_check\_rh0hdr () denial of service**  
Published: 02/28/2008、CVSS Severity: 7.8 (HIGH)
- **CVE-2008-0177: KAME Project IPv6 IPComp Header Denial Of Service Vulnerability**  
Published: 02/07/2008、CVSS Severity: 7.8 (HIGH)
- **CVE-2008-0630: MPlayer 'url.c' Remote Heap Based Buffer Overflow Vulnerability**  
Published: 02/06/2008、CVSS Severity: 6.8 (MEDIUM)
- **CVE-2008-0352: Linux kernel IPv6 jumbogram denial of service**  
Published: 01/18/2008、CVSS Severity: 7.8 (HIGH)

© Hitachi Incident Response Team. 2008.

- ❑ CVE-2008-3816: Cisco PIX and ASA Appliance IPv6 Denial of Service Vulnerability  
Published: 10/23/2008、CVSS Severity: 7.8 (HIGH)
- ❑ **CVE-2008-4404: Multiple Vendors IPv6 Neighbor Discovery Protocol Implementation Address Spoofing Vulnerability**  
Published: 10/03/2008、CVSS Severity: 10.0 (HIGH)
- ❑ **CVE-2008-2476: Multiple Vendors IPv6 Neighbor Discovery Protocol Implementation Address Spoofing Vulnerability**  
Published: 10/03/2008、CVSS Severity: 9.3 (HIGH)
- ❑ CVE-2008-3686: Linux Kernel "rt6\_fill\_node ()" Local Denial of Service Vulnerability  
Published: 08/14/2008、CVSS Severity: 4.9 (MEDIUM)
- ❑ CVE-2008-1576: Apple Mac OS X Mail Memory Corruption Vulnerability  
Published: 06/02/2008、CVSS Severity: 6.8 (MEDIUM)
- ❑ CVE-2008-2136: Linux Kernel 'ipip6\_rcv ()' Remote Denial of Service Vulnerability  
Published: 05/16/2008、CVSS Severity: 7.8 (HIGH)

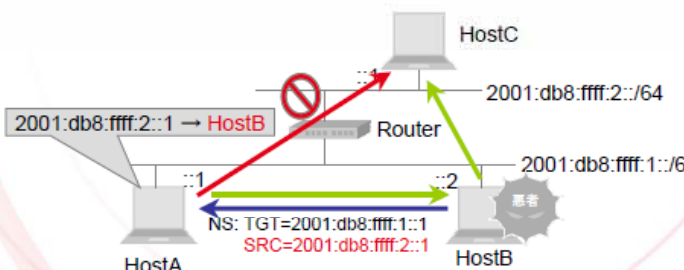


© Hitachi Incident Response Team. 2008.

Internet Initiative Japan Inc.

## 脆弱性の概要

- NSパケットのソースアドレスを偽装することで、任意のホスト宛の通信を攻撃ホストに向けることができる (NS:Neighbor Solicitation)
- 少なくともKAMEにおいて問題が発生する



2008年9月11日(木)に実施した「VU#472363 意見交換会」に末永洋樹さん@IIJから提出された資料です。

© 2008 Internet Initiative Japan Inc.

© Hitachi Incident Response Team. 2008.

## VU#472363が割り当てられるまでの対応

- 2008/ 7/17 (木) FW: IPv6 Neighbour Discovery – Vulnerability Responsible Disclosure
- オーストラリアのAlcatel-Lucentの発見者からIPv6 NDPの脆弱性について、2008年8月16日に開示するとの記載があるメールを受信する
- 社内関係者に脆弱性影響有無の確認を展開する
- 2008/ 7/18 (金) 社内関係者から社外の製品開発者にも展開したいとの連絡を受ける
- 2008/ 7/20 (日) 発見者に社外関係者への展開可否の確認をとる
- 発見者からの回答で、脆弱性情報の取り扱い状況を把握する
- 国内のIPv6製品開発者に情報展開する必要があるが、どうやって展開するのか？
  - 情報セキュリティ早期警戒パートナーシップを利用できるが、そもそも、この脆弱性は報告に値する脆弱性なのか(情報展開の緊急度は)？
- 2008/ 7/21 (月) 社外IPv6製品開発者の知り合いに、影響度について相談する
- 2008/ 7/22 (火) IPAに報告する(【IPA#87434\*\*\*】届出情報として受信される)
- 発見者からVU#472363が割り当てられたとの連絡が入る
- 2008/ 7/23 (水) IPAにVU#472363が割り当てられたとの連絡を入れる
- 2008/ 7/31 (木) CERT/CCからVU#472363に関する脆弱性情報を受信する

© Hitachi Incident Response Team. 2008.

## VU#472363が割り当てられた後の対応

- 2008/ 8/ 7 (木) 社内関係者から相互接続に影響がでることも考えられるとの連絡を受ける
- 2008/ 8/11 (月) 社外IPv6製品開発者の知り合いに、対応のエスカレーションについて相談する
- 2008/ 8/21 (木) CERT/CCがIPv6用の情報交換MLを開設する
- 2008/ 9/ 1 (月) 社外IPv6製品開発者の知り合いと、対応のエスカレーションについて相談する
- RFCにプレフィックスチェック(NetBSDでの対策)に関する記載はない。では、RFCに明記されていない脆弱性対応策をどう扱うべきなのか？
  - 現状のNDPの仕様に依存したプロトコルが存在するかもしれない。
  - IPv6 Ready Logoへの影響があるかもしれない。
- JPCERT/CCにIPv6製品開発者が意見交換するための場(対策ならびに、対策に伴う影響について)の設定を依頼する
- 2008/ 9/11 (木) VU#472363意見交換会(場所:JPCERT/CC)
- 2008/ 9/25 (金) IPv6用の情報交換MLに海外製品開発者主催の会議案内が流れる
- 2008/ 9/28 (日) CERT/CCにVU#472363意見交換会の検討結果を報告する
- 2008/10/ 1 (水) JPCERT/CCにVU#472363意見交換会議事録の配布を依頼する
- 2008/10/ 3 (金) VU#472363の公開

© Hitachi Incident Response Team. 2008.

## 1. 意見交換会開催の趣旨

IPv6の実利用が進んでいることもあり、IPv6に関する脆弱性が報告されはじめた。脆弱性によっては、実装依存／仕様依存かはっきりしないときもある。また、対処方法によっては、相互接続性を阻害する可能性もある。これらの状況を踏まえ、今後、IPv6に関する脆弱性が報告がされたときに、製品開発者間で意見交換できる場を作っていくこと、その具体的な事例積上げとして、VU#472363に関する意見交換会を開催した。

© Hitachi Incident Response Team. 2008.

## 2. 議事内容

### (1) NDPの脆弱性とその対策について

VU#472363の脆弱性の概要とその影響について解説した[1]。

### (2) 実装ベースでの対処と、仕様ベースでの対処の方向性

実装ベースでの対処として、破棄方式(NSメッセージを破棄し、応答もしない)と非キャッシュ方式(NSメッセージに対して応答はするが、キャッシュエントリを作成しない)がある。検討の結果、破棄方式は、実運用に影響する可能性があることから、非キャッシュ方式が良いという結論に至った(実装ベースでの対処可)。

### (3) IPv6 Ready Logoへの影響

破棄方式、非キャッシュ方式のいずれも、IPv6 Ready Logo取得に関して影響はないことを確認した。

### (4) 国内でのIPv6用の情報交換MLの立ち上げについて

情報の取り扱いなど運用上の課題は残るが、IPv6に関する脆弱性が報告された際の検討会開催通知や、意見交換の場として、国内用のIPv6用の情報交換MLは無いよりは、有る方が良いという結論に至った。

© Hitachi Incident Response Team. 2008.

- VU#472363が割り当てられるまでの対応における課題
  - 国内のIPv6製品開発者に情報展開する必要があるが、どうやって展開するのか？
  - 情報セキュリティ早期警戒パートナーシップを利用できるが、そもそも、この脆弱性は報告に値する脆弱性なのか(情報展開の緊急度は)？
- VU#472363が割り当てられた後の対応における課題
  - 実装ベースでの対処と、仕様ベースの対処の方向性を相談する場は必要ではあるが、どうやって意見交換の場を調整するのか？
  - 仕様ベースの対処が必要となった場合の進め方は？

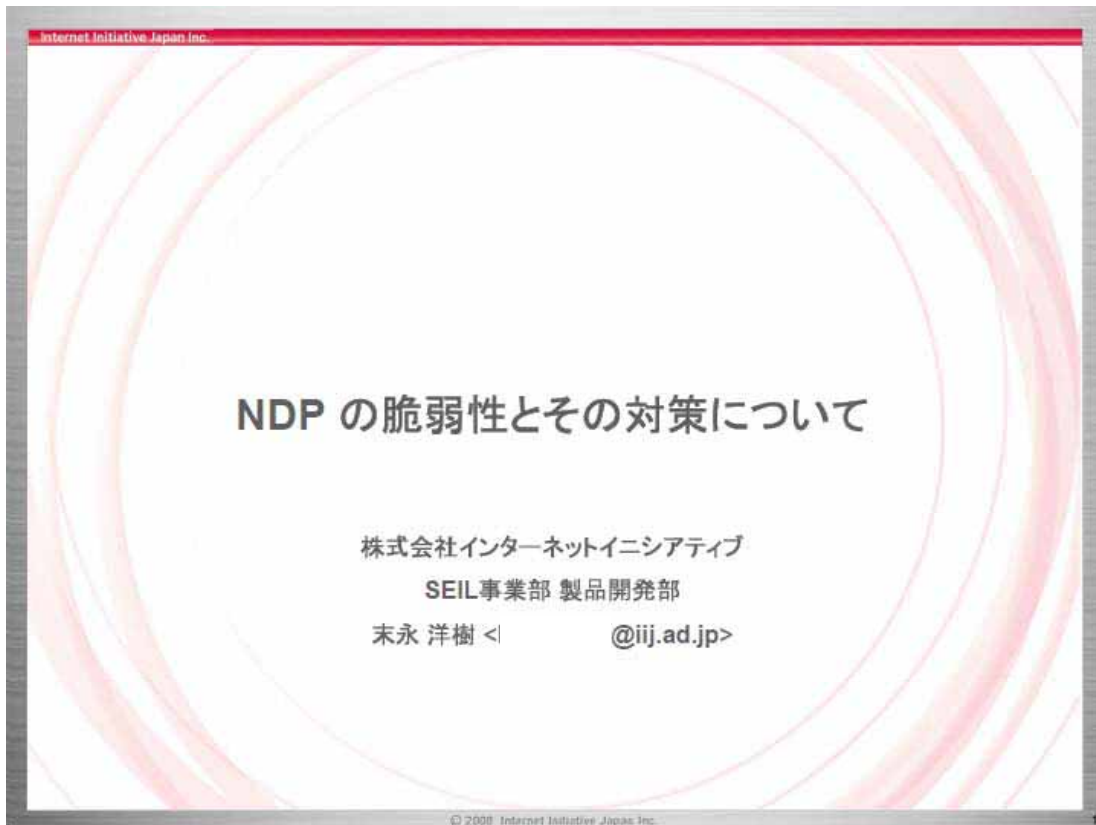
**⇒脆弱性対策のための国内製品開発者間の横連携は発展途上にある。**

© Hitachi Incident Response Team. 2008.

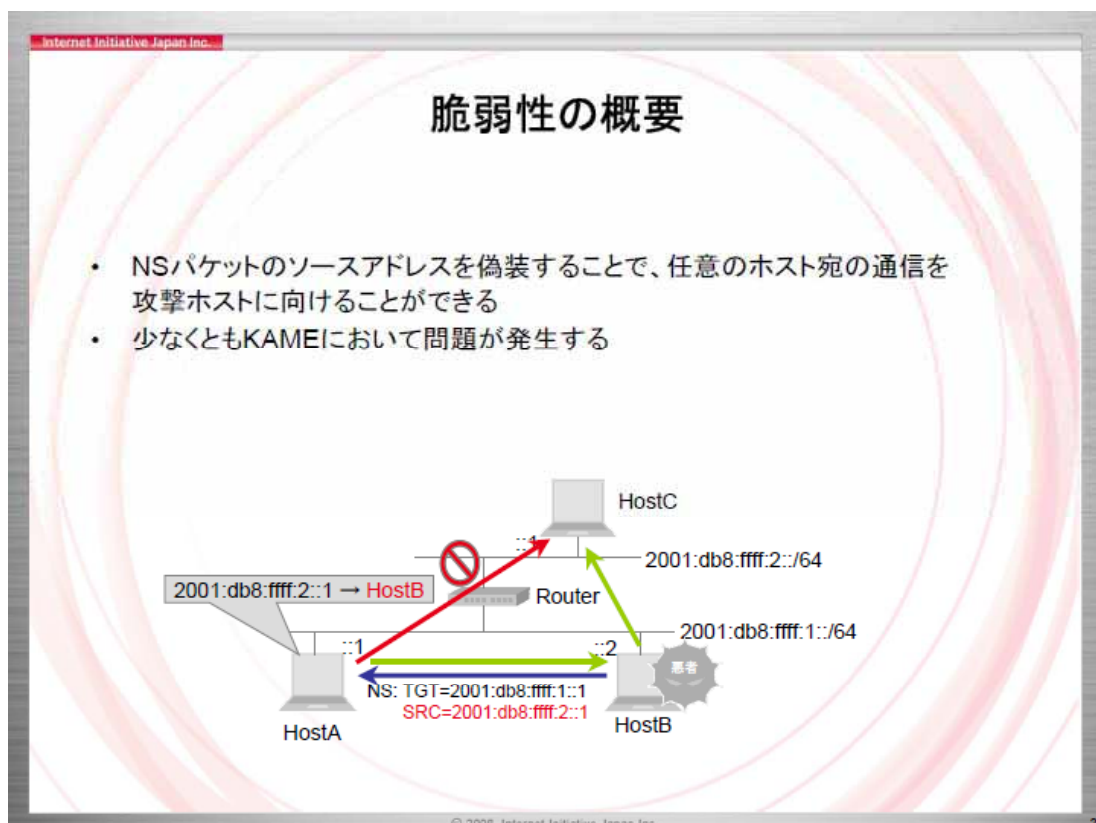
1. NDPの脆弱性とその対策について  
意見交換会開催にあたり、末永さん@IIJ、佐原さん@IIJにVU#472363の脆弱性についての解説資料を準備して頂きました。
2. VU#472363  
IPv6 実装における Forward Information Base のアップデートに関する問題  
<http://www.kb.cert.org/vuls/id/472363>  
<http://jvn.jp/cert/JVNVU472363/index.html>
3. IPv6 Ready Logo Program  
<http://cf.v6pc.jp/>
4. NetBSDでの対策  
[http://cvsweb.netbsd.org/bsdweb.cgi/src/sys/netinet6/nd6\\_nbr.c.diff?r1=1.88&r2=1.90](http://cvsweb.netbsd.org/bsdweb.cgi/src/sys/netinet6/nd6_nbr.c.diff?r1=1.88&r2=1.90)

© Hitachi Incident Response Team. 2008.





© Hitachi Incident Response Team. 2008.



© Hitachi Incident Response Team. 2008.

Internet Initiative Japan Inc.

## どのような環境で問題となるか

- 悪意をもったユーザがオンラインで接続可能なセグメントで問題が発生する
  - そこの無線LAN環境でDNSを乗っ取るのか？
  - 通信を傍受・改ざんするのか？
- ルータに対して攻撃可能な場合は、特に被害が大きい
  - アクセスルータに收容されている他の顧客の通信をまるごと吸い込む
- 参考: ND への攻撃については SEND 関連の人たちがまとめている
  - RFC 3756 IPv6 Neighbor Discovery (ND) Trust Models and Threats

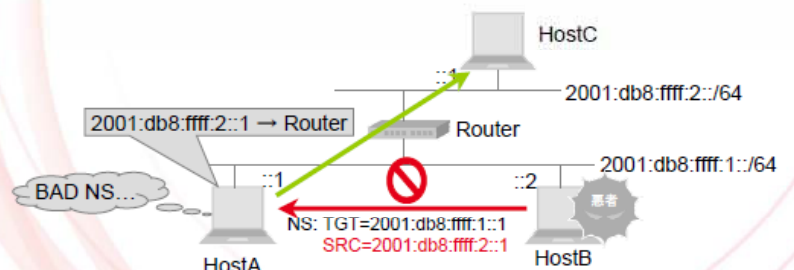
© 2008 Internet Initiative Japan Inc. 3

© Hitachi Incident Response Team. 2008.

Internet Initiative Japan Inc.

## NetBSDの対策方法

- NSパケットのソースアドレスが自分の所属するプリフィックスに含まれない場合は不正なパケットとする
  - が、RFC 的にはプリフィックスをチェックしろと明記されているわけではない



© 2008 Internet Initiative Japan Inc. 4

© Hitachi Incident Response Team. 2008.



Internet Initiative Japan Inc.

## NetBSD の対策例(src/sys/netinet6/nd6\_nbr.c)

```

void
nd6_ns_input(struct mbuf *m, int off, int icmp6len){
    ...
    if (IN6_IS_ADDR_UNSPECIFIED(&saddr6)) {
        ...
        /* ソースアドレスがUNSPECIFIEDの場合(DAD NS)の処理 */
        ...
    } else {
        /* ソースアドレスがUNSPECIFIEDではないが... */
        /*
         * Make sure the source address is from a neighbor's address.
         */
        if (in6ifa_ifplocaladdr(ifp, &saddr6) == NULL) {
            /* インターフェイスについているプリフィックスに含まれないならエラー */
            nd6log((LOG_INFO, "nd6_ns_input: " "NS packet from non-neighbor%n"));
            goto bad;
        }
    }
    ...
}

```

© 2008: Internet Initiative Japan Inc.

© Hitachi Incident Response Team. 2008.

Internet Initiative Japan Inc.

## この対策による弊害など

- 異なるプリフィックス同士で通信できていた環境で、通信ができなくなりますが...
  - ルータ屋としては、このようなネットワークは現状ではまず無いと思っています
- 現状のNDPの仕様に依存したプロトコルが存在するかも？
  - Mobile IP はひとまず問題なし
  - ほかには...？
- IPv6 Ready LOGO のテストに通らなくなる可能性
  - 現行のテストツールでは問題ありません
  - RFC に明記されていない脆弱性対応策をどう扱うべきなのかは問題

© 2008: Internet Initiative Japan Inc.

© Hitachi Incident Response Team. 2008.

---

**END**

**IPv6脆弱性  
VU#472363対応**

**2008/11/27**

**Hitachi Incident Response Team  
寺田真敏**