IPv6 導入に伴うセキュリティリスクに関する分析

武田圭史 †　　水谷正慶 ‡　　中井研 †

† 慶應義塾大学 環境情報学部
†† 慶應義塾大学大学院 政策・メディア研究科
252-8520 神奈川県藤沢市遠藤 5322

keiji, mizutani, nakai@sfc.wide.ad.jp

あらまし　IP バージョン 4(IPv4) アドレスの枯渇に伴い今後 IP バージョン 6(IPv6) の導入が進むと予想されるが，大規模かつオープンなネットワークにおいて異なるネットワークプロトコルが導入にされることにより新たなセキュリティリスクが顕在化することが考えられる．本分析では IPv6 を広く組織等において導入する際に予想されるセキュリティ環境の変化及び従来のセキュリティ機能の実装に関する課題について調査しそのリスクについて整理した．IPv4/v6 のデュアルスタック化による脆弱性暴露機会の増大や，ファイアウォールやウイルス対策ソフトウェア等における IPv6 に関する運用機能の提供が十分とは言えないなどの課題について述べる．

An Analysis of Security Risk on Introduction of IPv6

Keiji Takeda†　　Masayoshi Mizutani‡　　Ken Nakai†

†Keio University Faculty of Environment and Information Studies
‡Keio University Graduate School of Media and Governance
5322 Endoh Fujisawa Kanagawa 252-8520 Japan

keiji, mizutani, nakai@sfc.wide.ad.jp

Abstract　While it is expected to increase introduction of IP version 6 (IPv6) due to exhaustion of IP version 4 (IPv4) address new types of security risks by the introduction of the new protocol to large scale open network can emerge. In this analysis changes in security environment and issues around existing security functions on IPv6 are analyzed. Increasing exposure of vulnerabilities on IPv4/v6 dual stack system and inadequate implementation of security operation function of security software such as firewall and anti-virus software are also mentioned.

1　はじめに

これまでにインターネットで広く利用されてきた Internet Protocol version 4(以下 IPv4) アドレスの割り当てが限界に近づきアドレス枯渇が問題視されるようになるとともに Internet Protocol version 6[1](以下 IPv6) の利用が注目されてきている．2011 年にも IPv4 アドレスの在庫が枯渇するとの予測が行われていることなどから，今後企業や公共機関など組織で新規に公開するサーバ等での利用を中心に IPv6 の導入が進むと考えられる．機器や OS における IPv6 プロトコルスタック実装の提供はこれまでも先行的に行われており，ハードウェアやソフトウェア等の実行環境の面からは IPv6 利用に向けた前提が整いつつあると言える．しかしながら IPv6 の実環境での運用を前提としたセキュリティ面での検証はこれまで十分に行われているとは言

い難い．本研究では今後，企業等の組織においてIPv6の利用が進むことを想定し，どのような潜在的なセキュリティリスクが存在するのか，また従来使用されてきた各種セキュリティ機能の実装への影響とそれらの課題について調査分析した．

2　関連研究

IPv6の実運用環境への導入を前提としたセキュリティリスクに関しては以下のような分析が行われRequest For Comment(RFC)などの形で公開されている．Daviesらは RFC4942[2]においてIPv4環境からIPv6環境へ移行する際，両プロトコルが混在するネットワーク環境となることで，従来とは異なる様々なリスクが発生することを指摘している．Hoaglandら[3]はIPv4からIPv6対応への移行期において活用されるIP Tunnelingの技術がセキュリティ対策をbypassする手段となりセキュリティ上のリスクとなるとしている．IPv6のプロトコルの仕様の一部に関してセキュリティに関するの懸念[4][5][7][8]やプライバシーに関する懸念[11]が指摘されており，これらに対する解決策の提案[6][9][10][11]が行われている．日本国内においてもIPv6の導入に関するガイドライン[12][13]においてセキュリティについて配慮すべき事項が述べられているほか，セキュリティの観点からのプロトコルの分析結果など[14][15][16]が発表されている．以下の章ではこれらの内容を参考としつつ，IPv6の導入に際して想定されるセキュリティリスクの全体像について分類・整理を行い，導入に際して考慮すべき事項及び研究開発の課題について検討する．

3　IPv6導入におけるセキュリティリスクの分類

本項では前項に挙げた分析などを参考としながら，今後組織等においてIPv6を導入するにあたり想定されるリスクについて以下に分類し列挙する．

3.1　プロトコルの仕様に起因するリスク

IPv6プロトコルの仕様は長く利用されているが実際の運用環境において十分な実績を有するとは言い難く，特に攻撃への利用可能性といった視点からの検証があまり行われていないこともあり，今後様々な問題が露呈する可能性がある．ここではプロトコルの仕様によってもたらされるリスクについて想定されるものを列挙する．

- 利用者特定の困難性
  ネットワークを複数の利用者が共用する環境下において広大なアドレス空間内で一時的に使用するアドレスを頻繁に変更することが可能となり利用者の特定が困難な状況が発生する．IPv6においてはDHCPを用いずにホストが自律的に制御する動的なアドレスを使用することが可能であるため，ネットワークノードへの適切な接続管理が行われていない環境などにおいて，特定のアドレスを特定の時刻に誰が使用していたかを管理することが難しい状況が発生する．このような特性を悪用することにより悪意を持ったユーザが不正行為を行った場合に追跡を逃れることが可能となる．

- 単一ホストの複数アドレスの使用
  IPv6では単一のホストが複数のアドレスを使用することが可能なためアクセス制御のための設定が煩雑となる．このため設定ミス等が生じやすくこれらを利用した不正行為が発生する可能性がある．また，単一ホストが複数のアドレスを使い分けることで不正行為の追跡を混乱させることが可能となる．ファイアウォール等においてアドレスを使用したアクセスコントロールのための手順が煩雑になり設定の抜けや漏れが発生しやすくなるリスクもある．

- トンネリングプロトコルによる単一ホストの複数アドレスの使用
  IPv6では柔軟なネットワーク構成が可能となりモバイルＩＰの利用や，IPv4との

混在環境などにおいてトンネリングプロトコルが活用されるものと考えられる．これらトンネリングプロトコルの使用を制限しないネットワークにおいて，トンネリングプロトコルがアクセス制御をバイパスする手段として利用される可能性がある．特に暗号化によってパケットの監視等が行えなくなる場合にこれらトラフィック上でのセキュリティ管理が困難となることが予想される．これらの事態を防止するにあたってはファイアウォールの設定等によりこういったトンネリングプロトコルの利用を制限するか適切に管理することが可能な一定範囲での利用とすることが考えられる．

- Router Advertisement におけるなり済まし
  ルータの設定を自動的に行うことを可能とする Router Advertisement（以下 RA）機構において，認証の仕組みがないために，悪意のあるホストがルータになりすますことができる．SEcuring Neighbor Discovery プロトコルを使用するなどネットワークセグメントにおける接続認証を強化するなどの対策が必要となる．

3.2 IPv4 から IPv6 への移行および混在に起因するリスク

- 端末のデュアルスタック
  Windows Vista や Mac OS X など現在市販されている多くのパソコン端末に搭載されているオペレーティングシステム (OS) が IPv4 と IPv6 のデュアルスタックの実装となっておりデフォルトで両プロトコルが動作，可能な限り IPv6 の利用を優先する動作を行う．このためユーザが意図せず IPv6 での通信が行われたり IPv6 パケットへの返答が行われる場合が発生する．悪意のあるユーザがこうした OS の挙動を悪用する可能性がある．
  このようなデュアルスタックのホストが IPv6 で DNS クエリを送信する場合において DNS サーバが IPv6 で適切に設定されていない場合において不正な DNS クエリ応答を送信することで対象ホストからのアクセスを不正なサイトへ誘導することが可能となる．

- ネットワーク機器のデュアルスタック
  ファイアウォールやルータにおいて管理者が意識せずに IPv4, IPv6 の両プロトコルが動作している場合において，IPv6 プロトコルにおけるアクセス制御等の設定が行われないまま利用されるリスクがある．セキュリティに関するネットワーク機器に関しては管理者が意識的に設定しない限り動作しないデフォルトクローズとなる設定が望ましいと考える．

- セキュリティプログラムの IPv6 対応現在市販されている多くのセキュリティ関連のソフトウェアが IPv6 への対応をうたっているが，一部のセキュリティ対策ソフトウェアは IPv6 に対応しておらずデュアルスタックで運用されている状態において IPv6 による脅威に対して十分な対応ができない可能性がある．市販または一般に公開され利用可能なホスト用セキュリティ対策ソフトウェア製品の IPv6 への対応状況を確認したところ１２社の製品のうち４社の製品が未対応であった．また IPv6 対応とされている製品であっても IPv6 に関する設定項目のインタフェースが存在せず IPv4 に比べ機能面や柔軟性の面において制限を受ける場合がある．

3.3 実装に起因するリスク

- プロトコルスタック実装の検証不足
  これまで多くのシステムにおいて実用環境での IPv6 での利用実績が少ないためにプロトコルスタックの実装自体の検証が不十分である可能性がある．特に RFC 等で明示的に規定されていない例外的なパケット等の処理に関しては実装毎に動作が異なり，脆弱性の原因となりうる．プロ

トコルスタックに存在する脆弱性を検証するための環境，ツール等 [16] を利用した確認検証などが進むことが期待される．

3.4 処理負荷の増大によるリスク

- オプションヘッダによるサービス妨害 (DoS)
  IPv6 では任意の数のオプションを設定することができる拡張ヘッダの機能を有している．不正なプログラムが大量のオプションヘッダを持つ IP パケットを送信することで，受信側の処理に負荷をかけサービス妨害 (Denial of Service) の原因とすることが可能となる場合がある．RFC2675 に規定されるホップバイホップ・オプションは，ルータを通るごとに処理が行われ，Payload Length のフィールド値の上限である 65536 オクテットを超えるパケットを送信することを可能とする．また Type0 のルーティングヘッダに関しては 2 つのホスト間を往復するような経路を指定することによるサービス妨害攻撃の可能性が指摘されたが，この問題への Type0 のルーティングヘッダのオプションが廃止され [9] 現在の実装ではこのオプションは使用されていない．

- IP アドレス長が増加することによる負荷の増大
  IP アドレスの表現自体の長さが 32bit から 128bit となることにより IPv4 に比べ IP アドレスを含む各種ネットワークトラフィック，ログエントリ等の処理負荷及び容量が増加することが見込まれる．これらにより過負荷の状態が発生し計算機資源の容量が適切でない場合にサービス妨害がもたらされる可能性がある．

3.5 設定・運用に起因するリスク

- ホストへの到達性
  IPv6 を利用する各ホストがグローバルに到達可能なアドレスを持つことによって，適切なアクセスコントロールが行われていない状況下において外部のネットワークから直接アクセスすることが可能となる．従来の IPv4 環境においては NAT(Network Adress Translation) が利用されることが多く，内部ホストはプライベートアドレスを使用していたためにアクセス制御の設定に関わらず外部から内部に対して直接送信されるパケットを受信することができなかった．IPv6 では各ホストが有効なグローバルアドレスを利用するケースが増加すると考えられることから，NAT によるセキュリティ上の恩恵を受けることができず，当該ホスト上で脆弱性を有するサービス等が稼働している場合に不正なパケットの受信による被害に遭遇する可能性が高まると考えられる．ただしこれらはファイアウォールにおいて TCP 接続を行うプロセス等を動的に管理し内部ネットワークからの要求に基づく外部トラフィックの受信のみを許可するなど適切なアクセス制御を行うことにより防御が可能である．

- 固定アドレスによるプライバシの懸念
  Mac OS X などににおいてデフォルトでプライバシ拡張機能が OFF とされているため，利用者が意識しない限りホストのネットワークインタフェースが持つ MAC アドレスから生成したリンクローカルアドレスが使用される．このため通信先からは同一ホストからのアクセスをアドレスを用いて特定することができてしまう．こういった機能をサービス提供側で使用する環境が増えるとネットワーク上での利用者の動向等を容易に追跡することが可能となりプライバシ上のリスクとなる可能性がある．デフォルトでの IPv6 のプライバシ拡張機能の利用が推奨される．

- DNS の逆引きの設定および運用
  IPv4 では DNS を用いて IP アドレスから DNS を用いて対応する FQDN を検索しアクセス制御に用いたりログに記録したりということが行われているが，IPv6 ではアドレス空間が膨大なものとなるため

全てのアドレスに対してエントリーを登録するのは現実的ではなく逆引きの機能を利用しない場合もでてくると考えられる．このような場合において，ログやセキュリティ上の機能において逆引きを利用することができず従来のセキュリティ対策の継続するにあたって制限となる場合がある．

4　IPv6 導入に向けた課題

前項で分類整理したように今後 IPv4 と IPv6 を混在環境で利用していくにあたって現時点においても様々なリスクが想定されている．また，これまでに明らかになっていない新たなリスクが発見されてくるとも考えら得れる．IPv6 がプロトコルとして持つ様々な機能はネットワークの柔軟な運用を可能とするが同時に管理の複雑さを増大させる原因ともなりうる．従来の IPv4 ネットワークにおいては NAT によるグローバルアドレスとプライベートアドレスの変換によってネットワーク外部から内部に対する一方的なアクセスは自然と制限されてきた．各ホストがグローバルに意味を持つアドレスを持つようになることによって，各ホストでのセキュリティ対策の必要性が高まるとともに，これまで以上にファイアウォールによるアクセス制限が重要な意味を持つことになる．またトンネリングや ICMP の制御等ファイアウォールにより制御すべき対象が増加することからファイアウォールの設定を正確かつ効果的に行うためのインタフェース等の仕組みが重要な要素となると考えられる．現在入手可能なセキュリティ対策機器の多くは IPv6 へ対応とされているものの，十分な運用実績があるとは言い難く，また利用者にとってもこれら機器の設定に不慣れなことが想定されることから，今後セキュリティの観点からこれらシステムの対応状況の確認，適切なデフォルト設定値の検証や管理・運用を支援するための技術について本格的な研究の取り組みが期待される．

5　今後の課題

本分析では IPv6 のプロトコルの仕様および実験環境における試験的な IPv6 プロトコルの設定および利用から IPv6 の導入において発生が予想されるセキュリティ上のリスクについて分析した．今後実際に利用可能なツール等を用いて想定される脅威環境を再現し，実装および運用上の問題点を個別に検証したいと考えている．

6　まとめ

本発表では IPv6 を広く組織間等において導入する場合のセキュリティ環境の変化及び従来のセキュリティ機能の実装に関する課題について分析した．IPv6 の導入や IPv4 からの移行に際してのセキュリティリスクについて様々な指摘が行われておりそのいくつかについては対策方法が提案されているものの，その実装状況はベンダーによって異なり，実用にあたっては十分な検証が必要と考えられる．また，様々なセキュリティ対策機器，ソフトウェアのの IPv6 の対応が十分完了しているとはいえず，現時点での利用実績も多くないことから，テストベッド等を通じた実用性の検証，また各種攻撃への耐性等について検証することが必要と考えられる．本分析を通じて整理した IPv6 導入に際してのリスクの理解と認識は広く共有し，当初よりセキュリティを考慮したネットワークの設計と IPv6 導入施策が必要であろう．現行のネットワーク利用環境において IPv4/v6 のデュアルスタックが動作している場合が多く，今後これらを悪用した攻撃が行われる危険性も高い．こういった脅威の動向を監視しリスクの定量的な評価，評価結果に基づく具体的な対策の実施を可能とすることが必要である．

参考文献

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

[2] E. Davies, S. Krishnan, and P. Savola. IPv6 Transition/Coexistence Security Considerations. RFC 4942. 2007.

[3] J. Hoagland, S. Krishnan, and D. Thaler. Security Concerns With IP Tunneling. Internet-Draft draft-ietf-v6ops-tunnel-security-concerns-01. 2008.

[4] P. Nikander, Ed., J. Kempf, and E. Nordmar. IPv6 Neighbor Discovery (ND) Trust Models and Threats. RFC3756. 2004.

[5] P. Savola, and C. Patel. Security Considerations for 6to4. RFC3964. 2004. http://www.ietf.org/rfc/rfc3964.txt

[6] G. Van de Velde, T. Hain, R. Droms, B. Carpenter, and E. Klein. Local Network Protection for IPv6. RFC4864. 2007.

[7] E. Davies and J. Mohacsi. Recommendations for Filtering ICMPv6 Messages in Firewalls. RFC 4890. 2007.

[8] S. Roy, A. Durand, and J. Paugh. IPv6 Neighbor Discovery On-Link Assumption Considered Harmful. RFC4943. 2007.

[9] J. Abley, P. Savola, and G. Neville-Neil, Deprecation of Type 0 Routing Headers in IPv6. RFC5095. 2007.

[10] D. Thaler, S. Krishnan, and J. Hoagland. Teredo Security Updates, Internet-Draft draft-krishnan-v6ops-teredo-update-05. 2009.

[11] T. Narten, R. Draves, and S. Krishnan. Privacy Extensions for Stateless Address Autoconfiguration in IPv6. RFC4941(3041). 2007.

[12] IPv6 普及・高度化推進協議会. IPv6 移行ガイドライン　セキュリティ編. 2005.

[13] 総務省. 電子政府システムの IPv6 対応に向けたガイドライン. 2007.

[14] 力武健次. IPv6 化に伴うセキュリティ環境変化とその影響について. 総務省「次世代の情報セキュリティ政策に関する研究会」. 2008.

[15] 小柏伸夫, 衛藤将史, 中尾康二. IPv6 環境における攻撃検出回避とその対策. SCIS2008. 2008.

[16] 力武健次, 衛藤将史, 鈴木未央, 井上大介, 中尾康二, 小林悟史, 秋葉澄伸. NGN/IPv6 セキュリティ試験システムの設計と評価. 信学技報, vol. 109, no. 86, ICSS2009-26, pp. 97-102, 2009.