10'00"00 インターネット10分講座

MIN SEC 1/100S INTERNET

IPv6セキュリティ ～問題点と対策～

今回のインターネット10分講座では、IPv6環境におけるセキュリティ問題について、代表的な問題点を挙げ、その対策や緩和策を解説します。

1. はじめに

現在、IPv6に対応したネットワーク機器やサービスの普及が進みつつありますが、このIPv6環境におけるセキュリティ問題およびその対策・緩和策については広く理解されているとは言えません。本稿では、その理解の一助となるよう、IPv6環境のセキュリティについての誤解を取り上げた後、IPv6環境における代表的なセキュリティ問題であるFirst Hop SecurityおよびIPv6移行・共存技術に関わるトンネルの問題について、その対策や緩和策を解説します。

2. IPv6セキュリティについての誤解

まず、IPv6に関するセキュリティ上の誤解について、取り上げておきます。

2.1 IPv6環境でのIPsecについての誤解

よくある誤解として「IPv6環境ではIPsec（Security Architecture for Internet Protocol）が使われるためIPv4環境よりも安全である」という声をよく聞きます。これはある意味では正しいのですが、ある意味では間違っていると思われます。確かに、IPsecによる暗号化により通信路は安全になります。しかし、既に現在でもSSL/TLSによる暗号化はある程度は普及しており、通信の暗号化は可能です。また、IPsec、SSL/TLS両方の技術に共通する注意点として、通信相手を正しく確認（オンラインの認証）せずに暗号化を行っても、通信を中継し、平文に戻してしまうような中間者攻撃（man-in-the-middle）ができてしまうという意味で、効果は低いと言えます。つまりIPsecに暗号機能があること自体によって一概に安全になったとは言えないと考えられます。

また、IPsecはIPv4においても実装されていますが、暗号化および認証に用いる鍵の管理が難しいため、組織内でのVPN（Virtual Private Network）など限られた目的での利用が主で、ノード間の通信暗号化のためにはほとんど利用されていない現状があります。このため、IPv6 環境になったからといって、急にIPsecが利用されるというのは考えにくいでしょう。

2.2 IPv6環境の安全性についての誤解

また別の誤解として、後述する不正RA（Router Advertisement）の問題がクローズアップされているせいか、先ほどの誤解とは矛盾するようですが「IPv6環境はIPv4環境よりも危険である」との意見もあります。

例えば「IPv4環境ではNAT内のノードに対しては外部からアクセスできなかったのに、IPv6環境においては外部からアクセスできるようになるので危険なのではないか」と言われています。確かに、IPv6環境ではend-to-endの到達性を重視していますが、必要の無い通信に関してはノードまたは経路途中のファイアウォール等で適切なフィルタリングを行えば、IPv4と同等のセキュリティレベルを確保できます（RFC4942 2.3※1）。

このようなIPv6環境とIPv4環境の安全性に関する筆者の見解は、IPv4環境よりも安全になっている部分もあれば、IPv4環境で起こり得る問題を引き継いでいる部分もあり、IPv6環境で新たに問題になっている部分もある、というものです。

ここで、OSI※2の7階層モデルを考えてみます。

IPv4とIPv6はネットワーク層に相当し、ネットワークにIPv6を導入することは、ネットワーク層におけるプロトコルの変更となるため、セキュリティ対策にも違いが出てきます。

一方、TCP/UDPなどのトランスポート層やアプリケーションに対しては、IPv6の導入によって、プロトコル自体が変わるわけではないため、ネットワーク層ほどの変化ではないと言えます。このため、従来のIPv4環境で用いられてきたセキュリティ対策の大半をIPv6環境で引き続き行いつつ、追加でIPv6環境に合わせた対策が必要になります。

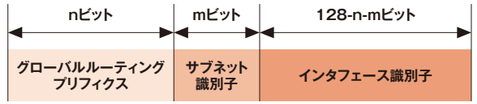
3. First Hop Securityについての問題

First Hop Securityとは、エンドノードと隣接ノードの間のセキュリティという意味であり、主にエンドノードとその同一リンク内のセキュリティをどのように確保するかというコンテキストで用いられます。ここではそのFirst Hop Securityについての代表的な問題として、不正RAによる盗聴とICMPv6エラーメッセージによるDoS攻撃（サービス妨害攻撃）の問題を取り上げます。

3.1 不正RAによる盗聴

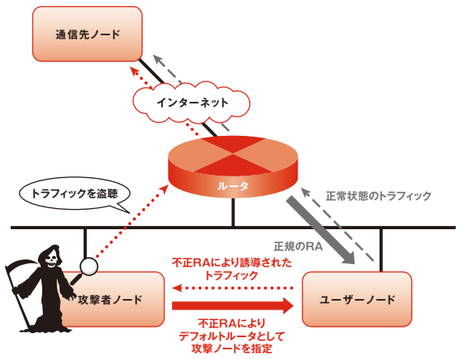
おそらく、IPv6のセキュリティに関わる問題のうち一番よく知られているものが、この不正RAによる盗聴の問題です。この問題は、IPv6で導入されたRAによるステートレスアドレスの設定に起因しています。IPv6ではノードの設定を簡略化するために、ルータが送信するRAに含まれるネットワークのプリフィクスやデフォルトルータの情報に基づき、ノードが自動的にアドレスを設定する仕組みが備わっています。一般的には、**図1**に示されるアドレス全体のうち、グローバルルーティングプリフィクスおよびサブネット識別子はRAによって提供され、インタフェース識別子についてはノードが生成してアドレス全体を構成します。

図1：グローバルユニキャストアドレスのフォーマット



しかし、このアドレス設定プロセスには認証や署名などのセキュリティ的な機能は特に備わっていないため、悪意ある者が組織内のネットワークに不正なRAを送信し、デフォルトルータになりすまして、通信の内容を盗聴できてしまいます（**図2**）。また、悪意が無くとも、ネットワーク機器の設定を誤ったり、OSの設定でネットワーク共有を有効にしたノードを繋いだりすると、意図せずに、上記のデフォルトルータになってしまうような不正なRAを送出してしまうことになります。

図2：不正RAを送信してユーザートラフィックを攻撃ノードに誘導し盗聴



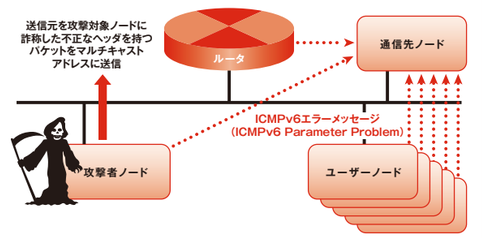
同様の問題はIPv4環境におけるDHCPによるアドレス設定でも起こり得るのですが、IPv4環境での不正DHCP問題に対しては、DHCP snoopingなどの対策がスイッチに実装され普及しています。それに対し、IPv6環境における不正RAの対策としては、RA Guard（RFC6105※3）やSEND（SEcure Neighbor Discovery, RFC3971※4）などが存在しますが、現時点では広く実装され普及しているとは言えません。このような機能が無いスイッチでネットワークを運用している場合、NDPMon※5やrafixd※6などのモニタリングツールにより不正RAの検出を行う、という対策も存在します。また、ネットワークの運用形態にもよりますが、悪意のあるユーザーによるネットワーク接続を防ぐために、IPの通信が起こる前の段階で、データリンク層で認証/アクセス制御のできるIEEE802.1x等を使ってユーザー認証を行うという対策も考えられます。

なお、この問題の詳細と緩和策については、RFC6104※7において解説されています。

3.2 ICMPv6エラーメッセージによるDoS攻撃

RFC4443※8などに記述されているICMPv6の仕様において、各ノードは問題のあるパケットを受信した際に、Parameter Problemというエラーメッセージを送信元アドレスに返します。ここで、問題のあるパケットの送信先アドレスがマルチキャストアドレスの場合、通常はエラーメッセージを返しませんが、特定のエラーの場合は例外的に返すべきであるという仕様になっています。この仕様を悪用することで、悪意ある者が送信元アドレスを攻撃対象ノードのアドレスに詐称し、問題のあるパケットをマルチキャストアドレスに送信することで、同一リンク上の各ノードが一斉にエラーメッセージを返すことになります。このため、1個の問題のあるパケットが、エラーメッセージを返すノードの個数分のパケットに増幅されて、詐称された攻撃対象ノードに届くことになり、攻撃対象ノードのCPU資源およびネットワーク帯域に対するDoS攻撃を行える可能性があります（**図3**）。

図3：ICMPv6エラーメッセージを発生させるパケットをマルチキャストアドレスに送信することによる反射型増幅攻撃



この問題の緩和策として、各ノードにおいてParameter Problemのエラーメッセージを返さない設定にすること、もしくはフィルタ設定を行うこと、送信ICMPメッセージのレートリミットを行うこと、等が考えられています。また2013年5月現在、IETFにおいてもこの問題は認識されており、関連する仕様を変更すべきかどうかの検討が行われています。

4. IPv6移行・共存技術に関わるセキュリティ問題

2007年11月に発行したニュースレター37号のインターネット10分講座「IPv4/IPv6共存技術」※9でも解説されていますが、IPv4からIPv6へのスムーズな移行・共存のために、デュアルスタック、トンネルなどのさまざまな技術が開発されてきました。これらの技術は実際に移行のために用いられており、IPv6環境への移行に貢献しているのですが、反面、これらの移行・共存技術に起因するセキュリティ問題があることが分かってきています。IPv4だけのネットワークと違い、IPv6が導入されることでIPv4とIPv6の共存環境になります。共存環境ではトンネルが使われることがありますが、このためにUDPやHTTPのペイロードへのカプセル化が行われることがあります。つまりIPv4環境では必要のなかったことが、IPv6の導入によって新たに必要になってきます。ここでは、その中の代表的な問題である自動トンネルによる問題について取り上げます。

4.1 トンネルに関わる一般的な問題

この問題は、RFC6169※10に述べられているトンネルに関するセキュリティ問題に関連するため、まずはRFC6169に関連する部分を解説します。RFC6169では、IPv6に限定されないトンネルに関する複数の問題について解説されているのですが、冒頭の2章において、トンネルによるセキュリティ機器のバイパスについての問題が解説されています。まず、一般的なトンネルに用いられるパケットは、UDPやHTTPのパケットのペイロード内にカプセル化されるため、単純なアドレス・プロトコル・ポート等に基づいてフィルタを行うファイアウォール機器や、シグネチャに基づいて検知を行う侵入防御システム(Intrusion Prevention System)などの機器では、正しくフィルタが行えません。このため、DPI(Deep Packet Inspection)のような、より高度な機能を備えた機器でなければ、カプセル化されたパケットのペイロードを検査し、その結果に基づいてフィルタすることは困難です。また、DPI機能を持つ機器においても、そのようなフィルタを効率的に行う仕組みを実装するのは難しいと言えます。さらに、機器によっては、IPv6への対応が遅れており、IPv4環境と比較するとIPv6環境では利用できる機能が限られる場合もあります。

このことにより、例えば、通常はポリシーに基づいてファイアウォールによりアクセス制御が行われている組織のネットワークにおいて、ネットワーク管理者の意図に反して、トンネルに関わるパケットがファイアウォールを通ってしまう場合があり得ます。そのような意図しない経路が存在する場合には、マルウェアや悪意ある者がその経路を悪用し、ネットワーク管理者に気付かれずに組織の内部情報を外部に送信したり、組織内部からSPAM送信やDoS攻撃を行ったりする可能性があります。

4.2 IPv6環境の自動トンネルに関わる問題

さて、先ほどは一般的なトンネルによるセキュリティ機器のバイパス問題について説明しましたが、IPv6移行・共存技術の一つに自動トンネルという仕組みがあり、ユーザーが意図せずにポリシーに違反した通信を行ってしまうおそれがあります。ここでも同様の問題が発生します。自動トンネルについての技術的な詳細は割愛しますが、その名の通りユーザーが明示的に設定しなくてもOSが自動的にトンネルを使った通信を行うような仕組みです。この仕組みにより、例えば、トンネルによりファイアウォールのアクセス制御を通ってしまい、結果的に組織内のユーザーが意図せずポリシーに違反した通信をできてしまう可能性があります。

また、自動トンネルに用いられるリレールータには、一般的には認証やロギングの仕組みが備わっていないため、悪意を持った者が自分の足跡をたどられないように、自動トンネルを用いる可能性が考えられます。

管理者がこのような自動トンネルによる通信を防ぐためには、自動トンネルの動作の仕組みを十分に理解し、ファイアウォールやエンドノードで適切な設定を行うことが重要です。例えば、自動トンネル技術の一つであるTeredoの場合は、一律に禁止するポリシーであれば、ファイアウォールでUDP3544番ポートのフィルタを行い、エンドノードでTeredoを無効化することで禁止することができます。

5. IPv6アドレスに関わるプライバシー上の問題

次に、IPv6アドレスに関わるプライバシーの問題について取り上げます。前述の不正RAによる盗聴の問題でも説明した通り、IPv6環境においてはRAによるステートレスアドレス設定が利用されています。その際、アドレスの一部となるインタフェース識別子については、ノードが備えているネットワークカードのMACアドレスを元に一意に生成しています。しかしこのインタフェース識別子は、基本的には同じノードを利用する際には変化することはありません。このためインタフェース識別子と個人情報の結びつけが行われた場合に、個人を追跡可能となり、プライバシー上の問題があると指摘されています。

例えば複数のWebサービスに広告を提供している会社が、アクセスログとして広告を表示したノードのアドレス情報とその広告を提供しているサービスを保存しているとします。その場合、アドレス情報にはノードを特定できるインタフェース識別子が含まれていますので、その識別子とアンケートサイト等の別経路で入手した個人情報との突き合わせを行った場合に、ある個人がいつどのようなサービスを利用したか特定できるという問題が指摘されています。この問題への対策として、RFC4941※11において一時アドレスという仕組みが提案されています。この仕組みでは、インタフェース識別子の生成の際にランダムな要素を加え、定期的にインタフェース識別子を変更することで、ノードの特定を防いでいます。古いOS等では、この一時アドレスの仕組みがデフォルトでは有効になっていない場合がありますので、プライバシーを気にされる方は確認をお勧めします。

これまでインタフェース識別子による特定の問題について説明してきましたが、ネットワークプリフィクスについても同様の問題が指摘されています。現在IPv6の家庭向け接続サービスを行っているISPの中には、運用負荷の軽減もしくはトラブルを防ぐ目的で、ユーザーに対して固定もしくは半固定のネットワークプリフィクスを割り当てている場合があります。このような場合には、一度割り当てられたネットワークプリフィクスは基本的には変更されないため、ネットワークプリフィクスから一意にユーザー（もしくは家族）を特定できてしまいます。この場合は、もしユーザーが一時アドレスを利用しても、ネットワークプリフィクスは変化しないため同様に特定が可能です。

ISPのIPv6サービスを契約する際には、プライバシーの点からは、このような固定ネットワークプリフィクスについても考慮したほうがよいでしょう。

6. まとめ

本稿では、IPv6環境のセキュリティに関する誤解について取り上げた後、IPv6環境における代表的なセキュリティ問題と、その対策・緩和策について解説してきました。IPv6環境をIPv4環境と比較すると、IP層については大きく変更され、その変更に伴ってデュアルスタックやトンネルなどの移行・共存技術が導入されていますが、IP層以外の大半の部分については互換性が保たれています。このため、IPv4環境で用いられたセキュリティ対策の大半はIPv6環境でも引き続き有効となりますので、そのまま使用しつつ、追加でIPv6環境に合わせた対策を行っていく必要があります。

また現在、IPv6セキュリティ問題についての議論を行っている場として、IPv6技術検証協議会のセキュリティ評価・対策検証部会、IPv6普及・高度化推進協議会のセキュリティWG、日本セキュリティオペレーション事業者協議会のセキュリティオペレーションWG、日本ネットワークセキュリティ協会のIPv6セキュリティ検証WGなどが存在します。本稿で解説した問題の詳細や他の問題について興味を持たれた方は、それぞれが発行している報告書やドキュメント※12 ※13 ※14を参照されるとよろしいかと思います。また、米国NIST（National Institute of Standards and Technology）が、“Guidelines for the Secure Deployment of IPv6”※15というよくまとまったドキュメントを発行しており、こちらも参考になります。

“Enjoy Happy IPv6ing!!”

（独立行政法人情報通信研究機構 鈴木未央／衛藤将史）

※1 RFC4942：IPv6 Transition ／ Coexistence Security Considerations
http://tools.ietf.org/html/rfc4942

※2 インターネット用語1分解説：OSI参照モデルとは
http://www.nic.ad.jp/ja/basics/terms/osi.html

※3 RFC6105：IPv6 Router Advertisement Guard
http://tools.ietf.org/html/rfc6105

※4 RFC3971：SEcure Neighbor Discovery（SEND）
http://tools.ietf.org/html/rfc3971

※5 NDPMon
LORIA/INRIA, "NDPMon - IPv6 Neighbor Discovery Protocol Monitor", November 2007,
http://ndpmon.sourceforge.net/

※6 rafixd
KAME Project, "rafixd - developed at KAME - An active rogue RA nullifier", November 2007,
http://www.kame.net/

※7 RFC6104：Rogue IPv6 Router Advertisement Problem Statement
http://tools.ietf.org/html/rfc6104

※8 RFC4443:Internet Control Message Protocol（ICMPv6）for the Internet Protocol Version 6（IPv6）Specification
http://tools.ietf.org/html/rfc4443

※9 JPNIC Newsletter No.37 インターネット10分講座：IPv4/IPv6共存技術
https://www.nic.ad.jp/ja/newsletter/No37/0800.html

※10 RFC6169：Security Concerns with IP Tunneling
http://tools.ietf.org/html/rfc6169

※11 RFC4941：Privacy Extensions for Stateless Address Autoconfiguration in IPv6
http://tools.ietf.org/html/rfc4941

※12 IPv6技術兼用協議会，“セキュリティ評価・対策検証部会 最終報告書 概要編”，2012,
http://ipv6tvc.org/download.html

※13 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”，2012,
http://www.v6pc.jp/jp/wg/securityWG/index.phtml

※14 日本セキュリティオペレーション事業者協議会 セキュリティオペレーションWG, 日本ネットワークセキュリティ協会IPv6セキュリティ検証WG, 2011,
http://isog-j.org/activities/result.html

※15 Frankel, S., Graveman, R., Pearce, J., and M. Rooks, "Guidelines for the Secure Deployment of IPv6", National Institute of Standards and Technology Special Publication 800-119, 2010,
http://csrc.nist.gov/publications/nistpubs/800-119/sp800-119.pdf