新しいインターネットプロトコルIPv6への移行

新しいインターネットプロトコルであるIPv6の開発・実装が盛んになっている。本稿ではIPv6の具体的な技術や仕組みよりも、これが必要になった背景や移行のために必要な作業、移行後のインターネットの状況について概説する。

1. IPv6開発の背景

IPv6[1]の開発は、近年のインターネットで目立ってきたさまざまな問題を解決するための仕切り直しと言えるであろう。IPv4[2]の問題点としてアドレスの枯渇や経路表の爆発的増大がよく知られている。これらはIPアドレスにA～Cのクラスを導入したアドレスアーキテクチャとアドレスの割り当て方が原因といえる。現在のアドレス空間の使用率は多くても数パーセントといわれており、現実にはアドレス空間にはまだまだ余裕がある。しかしIPv4の32ビットというアドレス空間が狭すぎることも事実である。たとえば32ビットでは地球上のすべての人間が1人1個のIPアドレスを使うことはできない。また経路表の爆発的増加に関しては、理論的には全世界中のIPアドレスをすべて割り当て直せば解決できる。しかしこの作業は途方もない労力、費用、時間がかかるので現実的でない。そこでIPv6の普及と同時にアドレス割り当ての仕切り直しをしようというわけである。

IPv4はセキュリティを考慮していない。インターネットが本当の意味での実用的なネットワークになるためには、セキュリティのサポートが必須である。IPのセキュリティ機能（IPsec）[3]はIPv4/v6双方に適用できるが、現在IPv4でIPsecを実装している製品はほとんどないであろう。この問題に関してもIPv6の普及と同時にIPsecをサポートする製品を普及させることができる。

新しいサービスへの要求も高まっている。実時間通信機能、移動通信機能、大規模なマルチキャストなどである。IPv4における移動通信についてはMobile IP[4]の標準化作業が進んでいるが、セキュリティ関連の問題が未解決である。IPv4もマルチキャストを実現しているが、配送範囲がホップカウントでしか制御できないなどの問題がある。実時間通信を実現するには、通信開始に先立って通信経路に沿って資源予約をする必要がある。IPv4/v6双方に適用可能な資源予約プロトコルとしてRSVP[5]が提案されているが、標準化作業はまるでIPv6の普及を待つかのように滞っている。

インターネットサービスプロバイダー（ISP）が多数登場するにつれ、1つの組織が複数のISPに接続するという形態も出てきた。これをマルチホーミングという。経路情報集約という観点から、マルチホーミングの組織はそれぞれのISPが割り当てた複数のアドレスを持つことになる。このためホストの1つのインターフェイスが複数のIPアドレスを持てるような仕組みが必要となる。また、ISPがサービス内容を競うようになると、接続するISPを変更する組織も出てくる。これをリホーミングという。やはり経路情報集約という観点から、リホーミングを行うと新しいISPから新しいIPアドレスの割り当てを受けることになる。すなわち組織内すべての機器のアドレス付け替えが生じる。このためアドレス付け替えを容易に行うための仕組みが必要となる。

参考文献

[1] S. Deering and R.Hinden,"Internet Protocol,Version6(IPv6) Specification", RFC 1883, January 1996.

[2] J. Postel, "Internet Protocol", RFC 791, September 1981.

[3] R. Atkinson, "Security Architecture for the Internet Protocol", RFC1825, August 1995.

[4] C. Perkins,"IP Mobility Support", RFC 2002, October 1996.

[5] R. Braden, L. Zhang, S. Berson, S. Herzog, and S.Jamin,"Resource ReSerVation Protocol (RSVP) – Version 1 Functional Specification", work in progress.

2. IPv6でなにが変わるか？

2.1. 大規模ネットワークへの適応

IPv6のIPアドレス長は128ビットである。単純に計算すると、地球の表面に対して1平方センチメートルあたり 1000京個以上のアドレスを割り当てることができる。また地球の人口を100億人とすると1人当たり100兆の100兆倍以上のアドレスを持てることになる。IPv6のアドレス割り当てはISPごとに経路情報が集約可能な方式(Provider Based Unicast Address)[6]が基本となっている。Provider Based Unicast AddressはIPアドレス全体の1/8を占めており、事実上これが枯渇することはないであろう。

アドレス割り当ても最初から計画的に行うことができる。Provider Based Unicast Address の割り当ては各地域の登録機関（Regional Registry）が行うことになっている。現在INTERNIC、RIPE NCC、Apniの3つのRegional Registryが存在する。実際には Regional Registryの下部組織として各国を管轄するNIC（日本の場合はJPNIC）がIPアドレスの割り当てを行うことになるだろう。するとIPアドレスの値はトップレベルではRegional Registry単位で集約可能となり、地域内では国単位で集約可能となり、国の中ではISPごとに集約可能となるであろう。このようにきれいな階層構造を持たせることで経路表の増加を抑え、より大規模なインターネットを構築できるようになる。

2.2. セキュリティの向上

IPv6は最初から拡張ヘッダとして認証ヘッダ[7]とESP（Encapsulating Security Payload）ヘッダ[8]が組み込めるようになっている。認証ヘッダはIPパケットの送信ホストが本物であることおよび送信パケットの内容が途中で改竄されていないことを、送信ホストが受信ホストに対して証明するためのものである。ESPヘッダは送信ホストと受信ホストの間で送信データの秘密保持を行うものである。

IP層でのセキュリティ機能の応用はVPN（Virtual Private Network）であろう。VPNとは、離れた地点に存在するネットワーク同士をインターネットを専用線のように利用して接続する手法である。2地点のルーター間で認証ヘッダやESPヘッダを使用することにより、インターネット転送中のセキュリティが確保できるのである。またVPNは移動コンピュータにも適用できる。ある組織に属する移動コンピュータが組織外へ移動した際、移動コンピュータと所属組織をVPNで接続することにより、移動コンピュータと所属組織内のコンピュータがセキュリティを保って通信できる。

IP層でのセキュリティの対象はホストやルーターを単位としたものである。したがってユーザーの認証やユーザーごとの送信データの秘密保持は上位層の役割であることに変わりはない。

2.3. 実時間通信の実現

IPv6が稼働しているネットワークでは実時間通信が可能になるであろう。実時間通信を行うためには、各ルーターは通信に先立って資源を予約し、通信開始後はその資源を使うべきパケットを選別しながら中継しなければならない。細かい

参考文献

[6] R. Hinden and S. Deering, "IP Version 6 Addressing Architecture",RFC 1884, January 1996.

[7] R. Atkinson, "IP Authentication Header", RFC 1826, August 1995.

[8] R. Atkinson, "IP Encapsulating Security Payload (ESP)", RFC 1827,August 1995.

話になるが、IPv6ヘッダはフローラベルというフィールドをもち、ルーターはどのパケットが実時間通信に属するものであるかを容易に判断できるようになっている。IPv6を実装したルーターはおそらくRSVPも実装すると思われるので、IPv6が普及すると同時にRSVPを利用した実時間通信も可能になると思われる。

2.4. プラグ・アンド・プレイへの対応

IPv6ではホストのネットワークへのプラグ・アンド・プレイが容易になる。IPv6にはデータリンク内でのみ一意なリンクローカルアドレスという種別のアドレスがあり、ホストが持っている情報のみでIPアドレスを生成できる[9]。すなわちホストをあるサブネットに接続するだけで、他のコンピュータのサービスに頼ることなく、独自にリンクローカルアドレスを生成して同一リンク内の他のホストと通信できるようになる。さらに接続したサブネットにルーターが存在すれば、ルーターからの情報（Router Advertisement）[10]を受信することによってインターネット全体で一意なIPアドレスを生成し、インターネット全体と通信することもできる。

2.5. 中継処理の高速化

IPv6の原案はSIP（Simple IP）という名称であったが、その名が示すようにIPv6はさまざまな簡略化を施してパケット中継処理の高速化を図っている。IPv6の基本ヘッダには最低限必要なフィールドしか存在しない。あまり使われない部分は拡張ヘッダとなる。拡張ヘッダに関しても、CPUが高速にアクセスできるようにフィールド長によって各フィールドの配置場所を制限している。

また最近、MPLS（Multiprotocol Label Switching）という技術が提案されている。従来のIPパケットの中継は受信先アドレスをもとに経路表を調べて中継先を決定するが、この処理に時間がかかる。MPLSは特別な"ラベル"からすぐに中継先を決定できるようにする技術である。ラベルはIPヘッダにあるものを使用してもいいし、データリンク層のもの（たとえばATMのVPI/VCI）を使用してもよい。IPヘッダのラベルとして、実時間通信の項で触れたフローラベルを利用しようという提案もある。

2.6. 未解決の課題

マルチホーミングやリホーミングのために、IPv6は1つのインターフェイスが複数のIPアドレスを持てるように規定している。しかしこれは仕組みがあるというだけであり、運用上の手間はさほど軽減されない。移動通信にしても現在はIPv4におけるMobile IPを拡張した提案があるだけで、セキュリティの問題はそのまま残っている。マルチキャストについては経路制御方式の標準化がまだ済んでいない。また、IPv6のマルチキャストアドレスは配送の範囲を示すスコープ（たとえば組織内のみ）を定義しているが、これをどのように実現するかは未解決である。

3. 移行の手順

IPv4とIPv6は互換性がないので、そのままでは双方の機器を混在させることは

参考文献

[9] S. Thompson and T. Narten, "IPv6 Stateless Address Autoconfiguration", RFC 1971, August 1996.

[10] T. Narten, E. Nordmark, and W. Simpson, "Neighbor Discovery for IP Version 6 (IPv6)", RFC 1970, August 1996.

できない。かといって全世界の機器にいっせいにIPv6を実装するのは現実的でない。そのためIPv4の部分とIPv6へ移行した部分の相互運用性を保ちながら徐々にIPv6へ移行する仕組みが必要になる[11]。IPv4からIPv6への移行は次のように進む。

1. 初期状態はインターネット内のすべてのノードがIPv4である。
2. インターネット内にIPv6ノードやIPv6サブネットが点在するようになる。
3. インターネットの大部分がIPv6になり、局所的にIPv4が残るようになる。
4. 最終的にはすべてがIPv6ノードになる。

第2段階への移行はすでに実現されている。現在約20か国の組織が6boneというIPv6の実験バックボーンに参加している[12]。第2段階ではIPv4の海の中にIPv6の島が点在するので、IPv6-over-IPv4トンネリングという手法により、IPv6の島同士がIPv6で通信できるようにする。

第3段階への移行が、IPv6普及の鍵になる。なぜならこれはISPがIPv6へ移行することを意味しているからである。そのためにはIPv6の仕様を完全に決定し、ユーザーに見える形でIPv6の利点が明らかにならなければならない。外部と通信しないネットワークはIPv6に移行する必要はないので、将来ある程度の期間は局所的にIPv4が残るであろう。しかしやがてIPv4を実装した製品はなくなると思われるので、時間が経てば自動的に第4段階に達するであろう。

4. 実装状況

UNIX系やWindows系のオペレーティングシステムで稼働するIPv6の実装も多くなってきた。この中には製品もあればフリーで配布されているものもある。さらにIPv6をサポートするルーターも増えている。日本ではWIDEプロジェクトのv6ワーキンググループ[13]がRFCに完全に準拠したフリーなコードの開発を行っている。このコードはBSD/OSやFreeBSDで稼働する。年内にもリリースされるだろう。

5. おわりに

本稿ではIPv6に移行するとインターネットがどのように便利になるかについて述べた。しかしユーザーの観点では大規模ネットワークへの適応や中継処理の高速化のような利点ははっきりとはわからないだろう。プラグ・アンド・プレイやセキュリティの向上、実時間通信のような利点はユーザーが直接体感できるが、これらはIPv4でやってできないことではない。このように、ユーザーにとっては敢えてIPv6に移行すべき理由はないというのが実情である。したがってIPv6への移行はISP主導で行わなければならない。プラグ・アンド・プレイやセキュリティの向上、実時間通信などの利点をうたってIPv6サービスを提供するISPが一日も早く登場することを願うものである。

（寺岡文男・ソニーコンピュータサイエンス研究所）

参考文献

[11] R. Gilligan and E. Nordmark, "Transition Mechanisms for IPv6 Hosts and Routers", RFC 1933, April 1996.

[12] 6bone home page, http://www-cnr.lbl.gov/6bone/

[13] WIDE Project, v6 Working Group homepage,http://www.wide.ad.jp/wg/ipv6/index.html

［インターネット白書ARCHIVES］ご利用上の注意

このファイルは、株式会社インプレスR&Dが1996年～2012年までに発行したインターネットの年鑑『インターネット白書』の誌面をPDF化し、「インターネット白書ARCHIVES」として以下のウェブサイトで公開しているものです。

http://IWParchives.jp/

このファイルをご利用いただくにあたり、下記の注意事項を必ずお読みください。

- 記載されている内容（技術解説、データ、URL、名称など）は発行当時のものです。
- 収録されている内容は著作権法上の保護を受けています。著作権はそれぞれの記事の著作者（執筆者、写真・図の作成者、編集部など）が保持しています。
- 著作者から許諾が得られなかった著作物は掲載されていない場合があります。
- このファイルの内容を改変したり、商用目的として再利用したりすることはできません。あくまで個人や企業の非商用利用での閲覧、複製、送信に限られます。
- 収録されている内容を何らかの媒体に引用としてご利用される際は、出典として媒体名および年号、該当ページ番号、発行元（株式会社インプレスR&D）などの情報をご明記ください。
- オリジナルの発行時点では、株式会社インプレスR&D（初期は株式会社インプレス）と著作権者は内容が正確なものであるように最大限に努めましたが、すべての情報が完全に正確であることは保証できません。このファイルの内容に起因する直接的および間接的な損害に対して、一切の責任を負いません。お客様個人の責任においてご利用ください。

お問い合わせ先 | 株式会社インプレスR&D | ✉ iwp-info@impress.co.jp