# IPv6/IPsec と 6bone の動向

山本和彦
奈良先端科学技術大学院大学
Kazu@Mew.org

加藤 朗
東京大学
kato@wide.ad.jp

## 1 はじめに

2 年をひと昔と考えるインターネットでは、1 年間は状況が変動するのに十分な時間である。今年 1 年の間に、IPv6、IPsec、および、6bone にも大きな変化が起こった。本稿では、昨年 12 月からの更新された主な機能について述べる。

## 2 IPv6

この節では IPv6 に関する基本仕様とアドレス・アーキテクチャの変更について説明する。

### 2.1 基本仕様の変更

IPv6 ルータやホストが数多くのベンダで開発中であり、そのうちの一部はすでに製品化されている。University of New Hampshire の InterOperability Lab. での相互接続試験でも、多くの実装間で基本機能の相互接続性が検証されている。日本でも、IPv6 の開発が盛んであり、たとえば日立製作所からルータ NR60 がすでに出荷されている。このように IPv6 の基本部分の仕様はほぼ確定し、実装の方もおおむね対応していると言える。

これに伴って IPv6 の基本仕様 [1] を、Proposed Standard から Draft Standard へ “出世” させる作業が進められている。Proposed Standard にするためには、複数の独立した実装による相互接続性の検証のみならず、不要なオプションなどの排除が必要である。

このため、IPv6 のヘッダ形式に若干の変更が加えられた [2]。これまであまり利用されなかった、4 ビットのプライオリティ・フィールドはクラスという名前に変更され 8 ビットが予約された。不足分の 4 ビットは、まだあまり利用されていないフロー・ラベルから借用されたので、フロー・ラベルは 24 ビットから 20 ビットへ短縮された。

クラスとフロー・ラベルの利用方法はまだ研究段階である。クラスの 8 ビットはそれぞれのビットに意味を持たせて利用される予定である。たとえば、ルータが輻輳時に反転させる輻輳ビットが今後規定されるかもしれない。フロー・ラベルは、ラベル・スイッチなどの技術に応用される可能性がある。

その他の変更点を以下に示す。

- Source Routing — Strict Source Routing と Loose Source Routing の区別が無くなった。
- マルチキャスト・アドレス — 近隣探索の近隣要請や近隣通知で用いるマルチキャスト・アドレスを `ff02::1:xxxx:xxxx` から `ff02::1:ffxx:xxxx` に変更し、通常のマルチキャスト・アドレスでは 13 バイト目に `0xff` を使用しないことにした。
- プレフィックス表現 — `3ffe:500::/24` のようなプレフィックス表現をすることになった。ただし名前との混同を避ける為、少くとも 1 つは “:” を含む必要がある。
- MTU の最小値 — IPv6 では、AppleTalk との兼ね合いから MTU の最小値に 576 を選んでいた。しかし、たとえば 1500 のように大きな値に今後変更される予定である。

これらの変更はそれほど影響がないと考えられる。一方、後述の 経路集約型アドレスの導入はアドレス割当や経路制御など根本に係わる変更である。

### 2.2 経路集約型アドレス

IPv6 のアドレス・アーキテクチャでは、上 3 ビットのプレフィックスによってアドレス空間を 8 分割

している。000 で始まる空間は、ループバック・アドレスなど特殊なアドレスとして利用される。また、111 で始まる空間は、リンクローカル・アドレス、サイトローカル・アドレス、および、マルチキャスト・アドレスに割り当てられている。

当初のアドレス・アーキテクチャでは、グローバルなスコープを持つアドレスとして、プロバイダ型アドレスにプレフィックス 010 を割り当て、今後の実験のためにプレフィックス 100 を地域型アドレスに予約していた [3]。これに対し、最新のアドレス・アーキテクチャでは、プロバイダ型アドレスと地域型アドレスを破棄し、プレフィックス 001 に対して経路集約型アドレス (Aggregatable Address) を割り当てた [4]。

プロバイダ型アドレスでは、プレフィックス長に正式な合意はなかった。たとえば、48 ビットの Ethernet アドレスを下位の識別子として利用する場合は、プレフィックス長を 80 とすることが多かった。IPv4 と同様、ネットワーク部はサブネットを識別し、ホスト部はそのサブネット内で一意であった。

経路集約型アドレスでは、ネットワーク部を上位 64 ビット、ホスト部を下位 64 ビットと明確に定義している。これまでと同様ネットワーク部はサブネットを識別するが、ホスト部 (正確にはインターフェイス識別子) はそれだけでグローバル・ユニークである[1]。ホスト部はグローバル・ユニークなトークンから、EUI 64 形式[2]に従った 64 ビットの識別子を生成することが推奨されている。たとえば、48 ビットの Ethernet アドレスから生成する場合、文献 [4] で示された方法に従って 64 ビットに変換する。

ネットワーク部はバイト境界を意識して、図 1のように TLA(Top Level Aggregator)、NLA(Next Level Aggregator)、および、SLA(Site Level Aggregator) に分割されている [5]。ここで注目すべき点は、サイト内外の境界を明確に定義していることであり、SLA 以下を Site Local Address に利用することも可能である。

TLA は全体で 8,192 しかないため、大規模なバックボーンプロバイダなどに割り当てられることが想定されており、そのための割り当て基準案も作成されている [16]。プロバイダ型アドレスに比べて、経路の集約に重点が置かれており、TLA をバックボーンプロバイダだけではなく、Internet Exchange に割り当てることも可能である。TLA が割り当てられた IX に接続している ISP は、適当な量の NLA の割り当てを受ける。ISP が利用するバックボーンプロバイダを変更した場合の ISP およびその顧客のアドレス付け替えが不要になる。

経路集約型アドレスには、ホスト部のみでグローバル・ユニークであること、サイトの内外が明確に定義されていることを利用して、モバイルやマルチホーム技術に有効利用される可能性がある。また、サブネットのプレフィックス長が 64 と固定であることから、組織内ネットワークの管理が楽になる利点もある。

# 3 IPsec

この節では、IPsec に関する基本仕様の変更と暗号アルゴリズムの策定状況について述べる。

## 3.1 基本仕様の変更

IPsec の基盤をなす認証ヘッダ [6] と暗号ペイロード [7] では、セキュア・ハッシュ関数や暗号アルゴリズムから独立した枠組を与えている。このため、認証方式や暗号方式は、個々の “変換” を定義することで実現する。

これまでさまざまな変換が規定されたが、多くの変換にリプレイ攻撃を防止するための通し番号フィールドがあった。このため、通し番号を共通部として取り出し、認証ヘッダと暗号ペイロードのフィールドとして定義した [8][9]。

この書式の変更によりこれまでの認証ヘッダと暗号ペイロードは、最新のそれらと互換性がない。新しい認証ヘッダと暗号ペイロードには、新たにヘッダ番号が割り当てられた訳ではないので、一見新旧の区別が付かない。この問題は、通信当事者間があらかじめ合意をとることによって実現する。

理屈上は区別が付くが、古い仕様を基にした製品はすでに出荷されており、新 IPsec 対応の製品今後出てくることを考えると、混乱は避けられないと予想される。

[1] 正確にはグローバル・ビットが立っている必要がある
[2] http://standards.ieee.org/db/oui/tutorials/EUI64.html

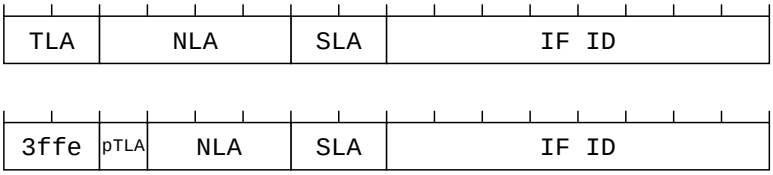


図 1: 上は経路集約型アドレス。下は経路集約型アドレスに従ったテスト・アドレス。

### 3.2 暗号アルゴリズム

IPsec を普及させるためには、政府の輸出規制や企業の特許に煩わされない暗号アルゴリズムを標準で選択する必要がある。IETF の IPsec 分科会は暗号アルゴリズム策定のための準備を進めている。

公開鍵暗号では RSA が一般的であるが RSADSI 社の特許に制約されているので、今後特許の切れた Diffie–Hellman が標準に選ばれるだろう。共有鍵暗号にはいくつもの選択肢があるが、強度と特許問題ともに申し分のない CAST[10] が選択させる可能性が高いと思われる。

日本で開発された優れた暗号は、アルゴリズムを RFC にする努力さえ払われなかった。この意味では、日本の暗号界から世界への貢献は低く、まことに残念である。

## 4 6bone

この節では、6bone の世界規模でのリナンバリングとその他関連情報について説明する。

### 4.1 リナンバリング

これまで 6bone は、プロバイダ型アドレスに基づいたテスト・アドレスを使用してきた [11]。また、経路制御には RIPng[12] を利用してきた。

簡単に予想できたことであるが、6bone に接続するネットワークの増加により、RIPng による経路制御は破綻した。また、プロバイダ型アドレスから経路集約型アドレスに移行する必要も発生した。

そこで、IETF の ngtrans 分科会[3]では、期間を 1997 年 10 月 1 日〜11 月 1 日と定めて、以下のように移行することを決定した。

- テスト・アドレスとして TLA を 1 つ取得する
- NLA の上位 1 バイトを pTLA (pseudo TLA) と定義し (図 1)、6bone の TLA を構成する組織に割り当てる。従って、実質的な NLA は 3 バイトになる。
- pTLA 組織間では、RIPng による経路交換を止めて、BGP4+[13] に移行する。

なお、テスト・アドレス用の TLA としては `0x3ffe` が割り当てられている [15]。WIDE Project は、pTLA として `0x05` の割り当てを受た。従って、WIDE 6bone は外部に対して `3ffe:500::/24` という経路をアナウンスすることになる。

本原稿の執筆時点では、WIDE 6bone は経路集約型アドレスへの移行は完了し、外部との経路制御プロトコルの BGP4+ 化を進めている。また、割り当てや登録を行なうレジストリも準備している。

### 4.2 関連情報

6bone のために正式に `6bone.net` といドメインが取得された。これに伴って 6bone の正式なホームページが、`http://www.6bone.net/` に変更された。なお、日本の 6bone に関する情報は、`http://www.v6.wide.ad.jp/` から得られる。

6bone のレジストリはこれまで RIPE が担当していたが、このほど ISI へ移行した。URL は `http://www.ISI.EDU/~davidk/6bone/` である。

## 5 おわりに

来年は IPv6 と IPsec の製品がさらに増えてこの分野は活発化するだろう。とくにプロバイダはこれらの技術に真剣に取り組む時期にさしかかっている。

[3] 6bone 分科会は 1997 年 8 月の Munich IETF から ngtrans 分科会に合併した

今後大きな変更はないだろうが、これらの開発中の製品や 6bone の運用からのフィードバックによって、これからも数多くの改良が提案され採用されると考えられる。そのため、関係者は常に最新の文書を参照するようにお願いしたい。

## 参考文献


[1] S. Deering and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 1883, December 1995.

[2] S. Deering and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", Internet-Draft, draft-ietf-ipngwg-ipv6-spec-v2-00.txt, July 1997.

[3] R. Hinden and S. Deering, "IP Version 6 Addressing Architecture", RFC 1884, December 1995.

[4] R. Hinden and S. Deering, "IP Version 6 Addressing Architecture", Internet-Draft, draft-ietf-ipngwg-ipv6-addr-arch-v2-04.txt, November 1997.

[5] R. Hinden, M. O'Dell, and S. Deering, "An IPv6 Aggregatable Global Unicast Address Format", Internet-Draft, draft-ietf-ipngwg-unicast-aggr-01.txt, July 1997.

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

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

[8] S. Kent and R. Atkinson, "IP Authentication Header", Internet-Draft, draft-ietf-ipsec-auth-header-02.txt, October 1997.

[9] S. Kent and R. Atkinson, "IP Encapsulating Security Payload (ESP)", Internet-Draft, draft-ietf-ipsec-esp-v2-01.txt, October 1997.

[10] R. Pereira and G. Carter, "The ESP CAST128-CBC Algorithm", Internet-Draft, draft-ietf-ipsec-ciph-cast128-cbc-00.txt, July 1997.

[11] R. Hinden and J. Postel, "IPv6 Testing Address Allocation", RFC 1897, January 1996.

[12] G. Malkin and R Millear, "RIPng for IPv6", RFC 2080, January 1997.

[13] Tony Bates, Ravi Chandra, Dave Katz, and Yakov Rekhter, "Multiprotocol Extensions for BGP-4", Internet-Draft, draft-ietf-idr-bgp4-multiprotocol-01.txt, September 1997.

[14] Pedro Marques and Francis Dupont, "Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing", Internet-Draft, draft-ietf-idr-bgp4-ipv6-00.txt, November 1997.

[15] R. Hinden, R. Fink, and J. Postel, "IPv6 Testing Address Allocation" Internet-Draft, draft-ietf-ipngwg-testv2-addralloc-00.txt, July 1997.

[16] R. Hinden and M. O'Dell, "TLA and NLA assignment Rules" Internet-Draft, draft-ietf-ipngwg-tla-assignment-00.txt, July 1997.