

AS (autonomous system) についての考察

Consideration of autonomous system

柏木 肇*

Hajime KASHIWAGI

あらまし：つい最近、5～6年前までは、インターネット接続環境を整備するには、常時接続環境を設置するため電話系キャリアと専用線契約を行い、今となつては、とても使い物になりそうにない64Kbpsや128Kbpsであっても、キャリア系の電話会社にメタル専用線の引き込み契約を結び、工事を行った上に、さらに専用線接続サービスのある近隣のプロバイダに接続させて貰う為にISPとの契約を行い、固定アドレスを振り分けてもらう。と言った面倒な手続きと莫大なコストが必要であった。

しかし、近年のブロードバンドの急激な普及の波に乗り、個人でも手軽に100Mbps光ケーブルを使用した高速な常時接続環境が実現可能となり、中小企業やSOHO環境において、もはや高帯域常時接続環境は常識となった。これは社会の情報基盤の質が向上した事から来る、ネットワークに対する依存性の増大と言う現象に連携し、結果、将来的に切断の無いインフラのニーズの高まりが想定され、ネットワークの冗長構成の実現というキーワードにて、マルチルーティング環境を想定したネットワーク機器の必要性が高まってくるのではないかと考えられる。

筆者の研究する自律稼働を想定したネットワーク型セキュアアプライアンス機器においても、将来的な対応力の強化を目的とした冗長構成に対応したスペック構造が必要であると考えた結果、従来の単一のデフォルトルート構造のネットワークだけではなく、マルチルーティング環境にも対応したネットワーク機器のスタイルが望ましいと考え、調査した結果、ASの2bitから4bit化への進化が近々実施され、その事によってもたらされる利点と、実際に動き出さないと見えてこないであろう弊害が存在する事に気付かされた。

本発表は、前述の利点や隠された弊害等にスポットをあて、最終的に筆者の研究課題にフィードバックさせる目的にて、まとめたものである。

キーワード：自律システム、ネットワーク

1 枯渇する2bytesAS (autonomous system) を救済する次世代AS 4bytesAS

1.1 AS番号とは？ 大きなネットワークに割り振られるAS番号

番号体系と聞いて思いつくのは、身近なところだと電話番号であろう。市外局番や局番号などに分かれており、体系だって管理されている番号である。一方、インターネットの番号体系で最初に思いあたるのは当然IPアドレスである。この番号は、地域毎に管理する組織である「地域レジストリ」を設けて、IANA (internet assigned numbers authority) が地域レジストリ毎にIPアドレス

を割り振っている。この事から両者とも地域毎に分けた番号管理をしている事がわかる。

ただし、インターネットは、非常に複雑にネットワークが絡み合っているという特徴があり、電話番号のように国単位や地域単位で大雑把に分割管理する形態は取れない。このため、地域レジストリはワールドワイドで共通な概念に基づいて、ユニークなIPアドレスの割り振りルールに沿って活動している。更に、あまり表に出てこないものにインターネット向けの番号資源として、もう一つワールドワイドで使われているものが存在する。それがAS番号である。ASとは、autonomous systemの略で、直訳すると「自律システム」と訳される。

* セキュリティ大学院大学 〒221-0835,
横浜市神奈川区鶴屋町 2-14-1, Tsuruya-cho, 2-14-1, Kanagawa-ku,
Yokohama-city, Kanagawa-pref. dgs063108@iisec.ac.jp

AS は、多くの場合、ISP などの“比較的大きなネットワークを単位として表現”し、“ネットワークの単位”毎に番号を割り当てている。この番号を AS 番号と言い IP アドレスと比べて一般には馴染みが薄い。これはネットワークを相互接続する場合に使われる BGP (border gateway protocol) でネットワークを認識する為に使用される。インターネットにて使用される「IP アドレスがあと数年で枯渇する」と叫ばれるようになって随分経つので、もはや常識となりつつある IP アドレス枯渇問題であるが、同時に AS 番号にも枯渇の危機が迫っている。

1.2 AS 番号にも枯渇の危機が

AS 番号は、IP アドレスが 32 ビットの有限個の番号体系であるのと同じく、16 ビット (2bytes) で表現される有限個の番号体系である。IP アドレスの枯渇に関する問題は広く認識され、議論も多くされているが、一方、AS 番号の枯渇に関連する問題はあまり議論されていないのが現状である。

この事については、APNIC (アジア太平洋地域の地域レジストリ) の Geoff Huston 氏が 2005 年 8 月に発表した“ Exploring Autonomous System Numbers ” (<http://www.potaroo.net/ispcol/2005-08/as.html>) で詳しく解説されているが、ここでは、「今のまま AS 番号の割り当てを続けると、早ければ 2010 年頃に AS 番号の割り当てが全部終わってしまう」と言われている。この手の予測の場合、その割り当て終了年が正確かどうかという議論よりも、「もうそろそろ次を考える必要があるのでは?」と認識する事が何より重要であると考えられる。

では、AS 番号が新しく割り当てられなくなると何が不便か? を考えてみたい。AS 番号は IP アドレスのように直接 IP 通信に影響を与えるわけではない。このため、既存の ISP に接続して、その ISP にデフォルト・ルートに向けているような場合は、全く関係ない。一方、^{※1} インターネット・エクスチェンジ (IX) に接続する等、他の複数の ISP と相互接続しているようなネットワークの場合、BGP を使って複数のネットワークとマルチホーム接続をしている。このようなネットワークを構築しようとする場合、ワールドワイドでユニークな AS 番号を使う必要がある。こうなると、「複数のネットワークにマルチホーム接続しようとする、新しいネットワーク」のユーザーにとっては、AS 番号が新たに割り当てられないために影響が出てくるわけである。

例えば、一般的な中小企業を想定してみよう、AS 番号を持たない小さな会社の人間が新たに企業ネットワーク資源を使用して ISP をはじめようと思ったとする。でも、AS 番号が無いのでマルチホームをして大きな ISP に対抗するようなネットワークを作れなくなってしまう。

1.3 近々 RFC になる “4bytesAS 番号”

IETF (internet engineering task force) では、早くから AS 番号の枯渇の問題に取り組み、AS 番号の番号空間を拡大する “4bytesAS 番号” の規格を定めている。現在のところ、Internet-Draft (RFC になる前の提案文書段階) であるが、近々正式に RFC (IETF の正式文書) として文書化されるとみられている。

この 4bytesAS 番号はどのように実装されるのか? IP アドレスの Verion4 から Version6 のように、BGP を Version4 から Version5 などの新しいバージョンに変更するような、インターネット全体を左右する大きな変更になるのか? 答えは NO である。

この 4bytesAS 番号は、既存の BGP-4 を拡張する形で、現在の 2bytes の AS 番号と互換性を保ちながら拡張される。さらに番号系も 2bytesAS の部分は 4bytesAS の番号系と共有される。したがって、現在既に取得している 2bytesAS は、インターネットに接続されている全てのルータが 4bytesAS 対応となっても、同じ番号を利用できる仕組みになっている。このあたりは IP アドレスの Version4 から Version6 への移行と比べて緩やかに行われる。

2 4bytesAS とは?

4bytesAS 番号とは、インターネットを構成する IP ネットワークを識別する番号である「AS (autonomous system) 番号」を、従来の 2bytes から 4bytes に拡張したものである。企業向け ISP 等の大規模ネットワークは AS 番号の割り当てを受けており、各 ISP の基幹ルータ間で、BGP-4 と呼ばれるルーティング・プロトコルを用いて経路情報を通知する際に使われている。

現在使われている AS 番号は、0~65535 という 2bytes の値である。2006 年 11 月時点で、約 4 万 1000 個が割り振られており、すでに全体の 6 割以上が消費された状態だ。このペースで消費が続くと、2010~2012 年には AS 番号が枯渇すると考えられている。これが、4bytesAS 番号の仕様開発を進める主な理由である。IETF では 4bytesAS 番号の仕様策定を進めており、2007 年前半には RFC 標準となる見込みである。新たに導入される 4bytesAS 番号の表現方法は、2bytes ずつをピリオドで区切ってそれぞれを 10 進数で表す。つまり、「0.0」から「65535.65535」という値で表現される。ISP などの基幹ルータが 4bytesAS 番号を処理するには、ルータの機能を拡張する必要がある。

ただし、4bytesAS 番号が標準化されても、すべてのISPの基幹ルータが、その時点ですぐに4bytesAS番号に対応するとは限らない。そこで問題になるのが、4bytesAS番号に対応済みのルータと未対応ルータが通信するケースである。この場合、対応ルータは、4bytesAS番号の通知用に予約されたAS番号であるAS23456番を処理し未対応ルータに通知する。その際加えて、4bytesAS番号情報を「NEW_AS_PATH」という新たに定義された属性情報に格納して送る。未対応ルータでは4bytesASをすべてAS23456として扱うことになるが、これまでと同様に2bytesでの処理が可能になるわけだ。



(図1) 4bytesAS番号を使った経路情報の通知の例

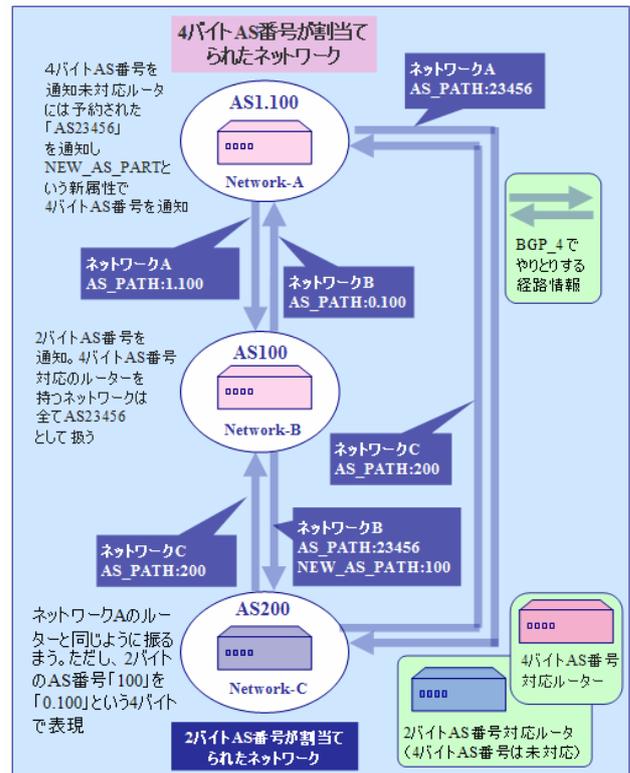
従来の2bytesのAS番号(0~65535)を4bytesに拡張して「0.0~65535.65535」と表現する。4bytesAS対応ルータが未対応ルータに経路情報を送るときは、予約されたAS番号であるAS23456を通知。加えて、新たに定義されたNEW_AS_PATH属性で4bytesAS番号を通知する。

3 問題は2bytesAS番号と4bytesAS番号の相互接続

3.1 問題点(怪しいと思われる点)

全く問題がないかと言うと、疑問は多くはない。ここで、AS番号の用途を押さえておく。AS番号に紐付けされたIPアドレスは、AS番号を識別する事で経路がインターネット全体としてループしないようになっている。このほか、何個のASを経由して流れてきた経路かを判定するために利用されている。もちろん、この辺りについては、BGPやインターネット経路制御の著名人達が何度も議論して、予測を繰り返し、概ね問題ナシという結論に達しているのも事実だが、全く影響がないか?と言うと、実際に実験をしたわけではなく、少し“怪しい”ところがある。

この“怪しい”と言っている部分は、2bytesASで運用されている空間と4bytesASで運用される空間の相互接続に関する部分である。これを単純化すると図2のようになる。



(図2) 4bytesAS番号と2bytesAS番号の変換

4bytesASの空間から2bytesASの空間にAS番号が入ったときに、2bytesASの空間では、4bytesASの情報を持つAS番号がAS_TRANSというAS23456に変換される。

4bytesASは、上位2bytesと下位2bytesを“:”で区切って10進数で表現する決まりとなっているので、上図のように4bytesASの空間から2bytesASの空間にAS番号が入った際に、2bytesASの空間では、4bytesASの情報を持つAS番号がAS_TRANSというAS23456に変換される。4bytesASの情報そのものは、拡張属性の中に封じ込められる。

通常この拡張属性はTRANSITIVE属性という「ASを通過して転送すべき情報」として扱われるわけだが、2bytesASの空間がTRANSITIVE属性を認識しなくても、そのまま転送される「はず」である。このときに以下の2点が問題になりそうなのである。

- ① 2bytesASの空間から4bytesASの空間を見ると、すべてがAS23456 (AS_TRANS) に見えてしまい、その経路に対するASを用いた経路制御が不能になる危険性。
- ② 2bytesASの空間を通過する4bytesASの隠ぺいされた拡張属性はTRANSITIVE属性だが、この2bytesAS空間で認識不能な拡張属性が正しく次の4bytes、又は2bytesASの空間に転送されるかは、実装依存となるため他の機器との整合性が図れるのか?

上記“①”に関する問題は、新しくつながる 4bytesAS のネットワークがひとつの大きな AS23456 というネットワークに見えてしまうため、AS 番号でフィルターするなどの BGP 特有の機能が有効に機能しなくなる危険性があるのではないかと？

このため、経路制御オペレーションに、それなりの悪影響を及ぼしそうな事が想像できる。

“②”に関する問題は、多くの実装が出現し、混在状態となる。それを相互接続する等して実際に実験するしかなく、現時点での検証は難しいと考えざるを得ない。いずれの場合も、このような新しい技術や資源が出現する度に、この手の不安は付き物となり、その時々で適切に対処する必要がある。しかし、事前に影響を考察し、対策可能な部分を検討しておくという事に大きな意味があると考えられる。

現時点で、4 bytes AS に対応したルータやネットワーク言機器が殆ど存在しない状態であり、実際のネットワーク機器を用いた実証も十分に出来ていない。そのため今後必ず実証実験が必要となる。

4 まとめ

つい最近、5~6年前までは、インターネット接続環境を整備するには、常時接続環境を設置するため電話系キャリアと専用線契約を行い、今となっては、とても使い物になりそうにない 64Kbps や 128Kbps であっても、キャリア系の電話会社にメタル専用線の引き込み契約を結び、工事を行った上に、さらに専用線接続サービスのある近隣のプロバイダに接続させて貰う為に ISP との契約を行い、固定アドレスを振り分けてもらう。と言った面倒な手続きと莫大なコストが必要であった。

しかし、近年のブロードバンドの急激な普及の波に乗り、個人でも手軽に 100Mbps 光ケーブルを使用した高速な常時接続環境が実現可能となり、中小企業や SOHO 環境において、もはや高帯域常時接続環境は常識となった。これは社会の情報基盤の質が向上した事から来る、ネットワークに対する依存性の増大と言う現象に連携し、結果、将来的に切断の無いインフラのニーズの高まりが想定され、ネットワークの冗長構成の実現というキーワードにて、マルチルーティング環境を想定したネットワーク機器の必要性が高まっていくのではないかと考えられる。

筆者の研究する自律稼働を想定したネットワーク型セキュア アプライアンス機器においても、将来的な対応力の強化を目的とした冗長構成に対応したスペック構造が必要であると考えた結果、従来の単一のデフォルト ルート構造のネットワークだけではなく、導入使用に想定された環境にてマルチルーティング環境を使用しないと

でも、これに対応したネットワーク機器のスタイルが望ましいと考え、調査した結果、AS の 2 bytes から 4 bytes 化への進化が近々実施され、その事によってもたらされる利点と、実際に動き出さないと見えてこないであろう弊害が存在する事に気付かされた。

筆者の研究するネットワーク型 セキュリティア プライアンス機器においても、ネットワークに対する依存度が高まるであろう将来の汎用性や安定性などを考えると、前述の 4 bytes AS に対応した機能が必須条件の一つとなるのではないかと考えられる。

本発表では、技術的な掘り下げを含めた、前述の利点や隠された弊害等にスポットをあて、最終的に筆者の研究課題にフィードバックさせる目的にて、調査研究内容をまとめたものである。

- ※ Internet eXchange : インターネットは全てのネットワークを(直接/間接的に)相互接続する必要があるが、多数の ISP, IDC を直接互いに相互接続するのは大変である(仮に 100 社なら約 5 万本必要)。そこで ISP, IDC の相互接続を IX で行う事により、接続距離の短縮化が実現で出来、運用も簡単になる。具体的には、LAN 接続と同様にスイッチングハブを用いて各 ISP のボーダールータを相互に接続してトラフィック交換を行う形態が一般的である。レイヤ 3 スイッチやルータを用いて構築されたレイヤ 3 IX (L3IX) という呼ばれるネットワークも存在するが、こちらは IX というより実態はパーシャル (部分) トランジットであり、一般には IX には分類されない。“L3IX ではない”, と言う事を強調するために、一般の IX を L2IX と呼ぶ事もある。ISP によっては、コスト節約のために相互接続を IX (つまり他社経由) に任せられる場合がある。

参考文献

- [1] 総務省総合通信基盤局データ通信課が中心となって立ち上げている次世代 IX 研究会 関連資料より
- [2] Geoff Huston, “Exploring Autonomous System Numbers”, <http://www.potaroo.net/ispcol/2005-08/as.html>, APNIC (アジア太平洋地域の地域レジストリ)
- [3] Scott M. Ballew, 日本シスコシステムズ監訳, 田和 勝 訳, CISCO ルータによる IP ネットワーク管理, オライリー・ジャパン, 1998 年 04 月 発行