経路制御の現状と異常経路検出時の対処

インターネットでは、ネットワーク間で経路情報が適正に受け渡されることによって、常に正しい宛先にパケットが送られます。ここでは、経路制御のプロトコルを紹介した後、誤った経路情報の広報による問題点を取り上げます。

2.1 経路制御プロトコルの種類と用途

インターネットは、数多くのネットワークの相互接続によって形成され、その状態は常に変化しています。新たなネットワークが接続されるかもしれませんし、何らかの理由で既存の接続が切断されるかもしれません。また、接続されているネットワーク自体も変化します。1つのネットワークが国や地域を越えて広がっていくこともあるでしょうし、事業撤退などでネットワークが縮退することもあります。このような変化の中でも目標とする相手と通信できるのは、きちんとパケットが宛先まで届くように経路制御されているからです。

インターネットでの多くの変化に手作業で対応することは不可能です。このため、自動的に最適な経路を見つけて制御してくれる動的な経路制御プロトコルが必須となります。動的な経路制御によって、需要に応じて分配したIPアドレスを簡単に使えるという利点もあります。組織内などの比較的小さなネットワークでは、RIP（Routing Information Protocol）やOSPF（OpenShortest Path First）といった経路制御プロトコルが採用されることが多いようです。一方、ISP間や大規模ネットワーク間といったインターネットでの経路制御には、BGP（Border Gateway Protocol）が標準的な経路制御プロトコルとして利用されています。

BGPの設計当初は、組織内のネットワークでOSPFやIS-IS（Intermediate System to Intermediate System）等を組織内経路制御プロトコル、IGP（Interior Gateway Protocol）として利用し、ネットワーク間でBGPを組織間制御プロトコル、EGP（Exterior Gateway Protocol）として利用して、IGPとEGP間で経路情報を同期しながら運用するネットワーク構成が想定されていました。しかし、OSPFやIS-ISなどのIGPでは、BGPが扱うような大量の経路情報を処理することが想定されていないため、その構成を変更する必要がありました。このため、BGPの経路情報をIGPに渡すのではなく、BGPとIGPをそれぞれ独立したものとして非同期で運用する構成が標準的な設計として広まりました。

また、最近の大規模なネットワークでは、網内の経路数増加に対応したりIGPの収束速度を早めたりするために、ネットワークのトポロジー（構成）と必要最小限の経路情報のみをIGPで運用し、その他すべての経路情報をBGPで運用するといった構成に変化しています。このためBGPを正しく運用することは、ネットワーク間のみならず、ネットワーク内の経路制御を適切に行う上でも重要なものになっています。

2.2 ネットワークポリシ

各ネットワークは、経路制御のポリシを個別に持っています。すべてを経路制御プロトコルに任せておき一切気にしないというポリシもあるでしょうし、より明確な意思を持って経路を選択しているネットワークもあるでしょう。BGPでは、経路情報を交換する際に、それぞれのネットワークのポリシを設定できます。ただし、設定できることはそれほど多くありません。経路のフィルタと優先度の設定、後処理のために目印を付けるくらいです。BGPで経路制御する際には、これらを組み合わせて上手にネットワークのポリシを実装し、意図したとおりの状態になるように設計する必要があります。

ほとんどのネットワークが標準的に持っているポリシがあります。これは、相互接続する相手の種別に応じたポリシで、カスタマ、ピア、アップストリームの3つです。カスタマは、ピアやアップストリーム等、他のネットワークへの中継（トランジット）を行います。経路制御では、ネットワーク自体が保持する全経路をカスタマに送信することに加えて、カスタマから広報された経路を他のネットワークにも送信します。ピアは、カスタマを含め互いのトラヒックを交換する関係にあり、ネットワーク自体とカスタマの経路のみを互いに交換します。アップストリームは、カスタマとは逆の動きで、他のネットワークへの中継を行ってもらっているネットワークです。アップストリーム向けにはネットワーク自体とカスタマの経路を広報するとともに、アップストリームからは全経路を広報してもらいます（図-1）。

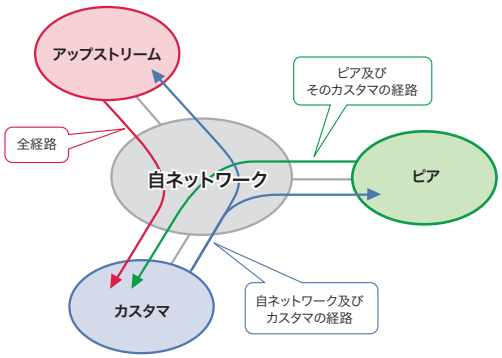

図-1　ピア、カスタマ、アップストリーム

2.3 経路数の現状

BGPで広報した経路情報は、相互接続されたネットワークを通じて世界に伝わっていきます。同様に、世界中のネットワークがそれぞれ経路情報を広報しているため、BGPを運用しているとインターネットに接続しているさまざまなネットワークからの広報を受信することになります。

インターネットでのBGP経路数は、この原稿の執筆時点においてIPv4でおよそ32万経路、IPv6で2300経路程度です。ここ最近、経路数はIPv4とIPv6ともにほぼ線形で増加しています。そして、今後もこの増加傾向は続くと考えられます。経路数の増加要因としては、新たなネットワーク接続やサービス拡充のためのネットワーク追加、トラヒック制御のための経路広報が考えられます。

経路情報の増加は、そのままルータでのメモリ消費につながるため、ルータの増強時期を検討する上でも注意すべき項目です。今後の懸念として、IPv4アドレスの在庫枯渇があります。APNICのミーティングでIPアドレスの移転ポリシが合意に達したこともあり、枯渇前後からIPv4アドレスの利用効率を高めるために、より細かな単位で経路が広報されることが予想されます。これは、さらに経路数が増加することにつながると思われます。

2.4 権威なき広報

BGPでは、経路ハイジャックがたびたび問題になります。これは、主に他人の経路情報を勝手に生成して広報することによる問題で、そのネットワーク宛の通信が関係のないネットワークに送られてしまい通信できなくなるといったトラブルを引き起こしています。このような問題が攻撃手法として利用されたときには、さまざまな悪用方法が考えられます。単純な通信妨害にとどまらず、他者に成りすまして偽のサイトを立ち上げたり、通信内容を盗聴するといったことも考えられます。実際に、2008年に著名な動画投稿サイトがアクセス不能になったり、2010年4月にアジアのあるASが世界中のさまざまな経路情報を数万件も広報してしまうという問題が発生しています。

このような事例では、その発生原因までが明確に報告されることは稀ですが、状況等から考えて意図しないBGPの設定ミスによるものだと推測できます。また、これまで報告された他の事例でも、そのほとんどが設定ミスによるものだと推測でき、「経路ハイジャック」という呼び名がその実態に比べて不穏すぎると思えるため、個人的には「権威なき広報」と呼ぶほうが適当だと考えています。

BGP自体はどのような経路情報が交換されるかを認識していないため、このような権威なき広報が起こってしまいます。どの経路情報を受け取り、どの経路情報を受け取らないかは、すべてポリシ、つまり各ネットワークの経路情報制御の運用に依存します。このため、運用によっては、この権威なき広報を防いだり、その影響範囲を狭めたりできる可能性があります。

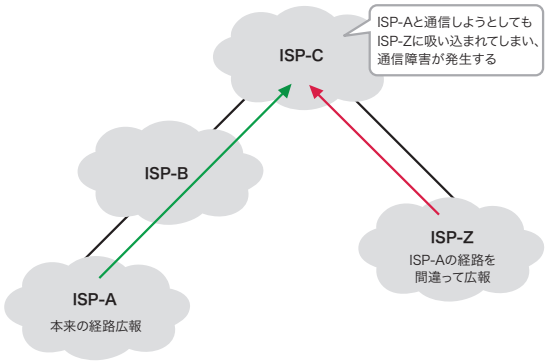

図-2　権威無き経路広報による、通信障害

たとえば、それぞれのネットワークにおいて、カスタマから広報される経路情報を厳密にフィルタリングすれば、権威なき広報で世界中のネットワークに迷惑をかけることはありません。過去には、カスタマ向けの受信経路フィルタを行っていないネットワークにも経路情報を中継した責任があると指摘する意見もありました。IIJは、BGP接続を利用されているお客様には経路情報を広報する前に連絡いただき、厳密な経路フィルタを設定しています。

一方で、権威無き広報を行ってしまったネットワークのアップストリーム内に、経路フィルタを実装していないネットワークが1つでもあったときには、そこから世界中に経路情報が広がってしまう可能性があります。現在でも断続的にこのような問題が発生していることから、いまだにカスタマ向けに厳密な受信経路フィルタを実装していないネットワークが多いと考えられます。より多くのネットワークが適切に経路フィルタを運用することで影響を軽減できる可能性が高まります。今後も、運用者コミュニティ等を通じて、よりよい運用を呼びかけていこうと考えています。

2.5 異常経路の検出

ここまでに示したとおり、他人が自分自身の経路情報を勝手にBGPで広報することは、現状では完全に予防することはできません。このため、権威なき広報が発生したときには、何よりも素早くそれを検知する必要があります。異常経路の検出に関しては、世界中でさまざまな取り組みが行われています。どの検知システムも、正常と見なす経路と実際のBGPでの経路の変動を逐次比較して、違いがあれば異常経路と判断しています。このような仕組みであるため、検知システムには次の2つの課題があります。

- 何をもって正常と見なすかという判断部分
- 比較対象となるBGPの経路情報をどこから得るかという経路収集部分

1番目の「判断部分」に関しては、いくつかの手法が試されています。たとえば、長期間安定して広報されている経路を正しいと見なし、その状態から広報元に変動があったときに異常と見なすシステムがあります。また、手作業で正しい経路の状態を登録しておき、それとの差異が生じたときに異常と見なすシステムもあります。

2番目の「経路収集」に関する課題は、難しい課題です。ネットワークは、それぞれ経路制御のポリシを持っているため、当然保持している経路情報もそれぞれ異なります。また、ネットワークの内部にはBGPが動作しているルータがあります。これらもそれぞれ異なる経路情報を保持している可能性があります。局所的な影響も検知しようとすると、より多くのネットワークやルータから経路情報を得る必要があります。

2.6 日本国内での取り組み

日本国内での異常経路の検知に関する取り組みとして、Telecom-ISAC Japanが運営している経路ハイジャック検知システム「経路奉行」があります。経路奉行は、JPNICが運用するIRR (Internet Routing Registry)、JPIRRに登録されているrouteオブジェクトを正常な経路状態として判断基準に採用し、これと日本国内のISPからシステムに提供されているBGP経路情報とを逐次比較して異常経路を検出するシステムです。routeオブジェクトに登録されている広報元と異なる広報元から経路情報が広報されたときに異常と判定しているため、設定ミスによる異常経路を検出するには有用なシステムです。また、日本国内のISPから経路情報を得ているため、国内での影響をある程度推測することもできます。IIJも当初からこのシステムの運用に参加し、よりよい検出に向けて活動を続けています。また、IIJ自身の経路を監視するという目的のため、利用者としてもシステムを活用しています。これまでには、IIJが広報している経路情報が他ネットワークから広報された際に、経路奉行からの警報を受信したこともあります。

2.7 異常経路検出時の対処方法

警報を受信したときには、まず現在の状態を外部のLooking Glassサイトなどで確認します。これまでのほとんどの事例では、数分間程度で問題の経路情報が消えて復旧しているため、検知システムからの警報を受信したときにはすでに回復している可能性もあります。

しかし、残念ながら、まだ問題の経路広報が継続しているときには、該当経路の広報元への連絡を試みます。その際、こちら側に経路広報の正当性があることを伝えるために、常日頃からIR (Internet Registry) やIRRの登録情報をきちんと更新しておくことが大切です。

問題の広報元への連絡がうまくいかないときには、そのアップストリームと思われるネットワークに連絡して、対応への援助を求めることも有用です。それでも解決できないときには、周辺のネットワークや運用者コミュニティに適切な連絡先を問い合わせてみたり、助力を求めたりするなどして、解決に向けてできるかぎり対応する必要があります。

短中期的にはこのような運用での対処を行いつつ、長期的にはより簡単に正しい経路であることを判別する方法を検討します。その１つが電子署名を利用して認証を行うRPKI (Resource Public Key Infrastructure) です。RPKIを利用すると、IRからIPアドレスが割り振られる際にリソース証明書と呼ばれる電子署名が発行され、IPアドレスの利用権利を明確にできます。この仕組みを利用してルータで経路情報を認証し、正しい広報元から広報されている経路情報であることを自動的に判別します。すでに、いくつかのルータベンダによる実装が進んでおり、実際に電子署名で経路情報の認証が可能なファームウェアの検証試験も行われています。ただし、証明書の発行や電子署名の運用に関する課題もあり、RPKIの導入までにはいましばらくの時間がかかるとも思えますが、IIJは信頼できる経路制御のために継続的な活動を行くつもりです。

執筆者:
松崎 吉伸（まつざき よしのぶ）
IIJ ネットワークサービス本部 ネットワークサービス部 技術推進課 シニアエンジニア。あれこれ面白しろそうな事を見つけては頑張っている。
IIJ-SECTメンバ、The Asia Pacific OperatorS Forum co-chair、APNIC IPv6 SIG chair、JPCERT/CC専門委員。