ルーティングセキュリティ最新動向

インターネットが社会的なインフラとしての重要性を増す中、ルーティング（経路制御）が適切に行われることへの期待も強まっています。今回は、ルーティングに問題があった場合にそれを検知する、または問題を予防するための取り組みである「ルーティングセキュリティ」を取り上げ、最新動向をお伝えします。

1. ルーティングセキュリティとは

「ルーティングセキュリティ」という言葉は、あまり聞きなれない言葉かもしれません。しかし、インターネットには欠かせないものの一つといえるでしょう。

インターネットは多くのネットワークによって成り立っています。それらは相互に接続し、結果として世界中のネットワークに接続することができます。それを実現するのがルーティング（経路制御）で、経路制御を行うために使われるものが経路情報です。

この二つは、どちらもインターネットには欠かせません。

目的のネットワークに到達するためには、そのネットワークがどこにあるのかを知るための経路情報が必要になります。一般的には経路情報が複数あり、その中から最適な経路を選択するために経路制御を行います。これらのどちらかに問題が起きた場合、目的のネットワークへの接続性が失われる可能性があります。

大きなネットワーク（ISP・企業等）を相互接続する際には、お互いが持つ経路情報を交換し、受け取った情報に基づき経路制御を行います。（経路情報にはIPアドレスの情報を含めたさまざま情報がありますが、今回は省略します）

それらを実現しているのはBGP（Border Gateway Protocol）というプロトコルです。大きなネットワークには、IPアドレスと同時にAS番号というユニークな数字が割り当てられます（ASとはAutonomous Systemの略で、日本語に訳すと自律システムとなります）。BGPでは、AS番号を用いて経路情報の交換を行います。それにより目的のネットワークがどこにあるのかを知ることができ、併せて自らのASがどこにあるかを知らせることができます。

この「経路情報の交換」によって経路制御にもたらされる問題がいくつかあります。それらの問題に対応するためには「知ること」「防ぐこと」が重要です。ここではこれらを総称して「ルーティングセキュリティ」と呼びます。

参考
「インターネット10分講座：BGP」
http://www.nic.ad.jp/ja/newsletter/No35/0800.html

2. 過去に発生した事例

BGPにより交換される経路情報には、自ASが直接接続していないASからのものも多く含まれます。その情報に誤った（または不正な）情報が混入してしまい、トラフィックに影響するトラブルが発生することは過去にもあり、問題視されていました。

具体的には、

1. 経路情報のアップデートに不正な（または通常使われない）属性（アトリビュート）がついて、解釈できないルータがBGPのセッションを切断してしまう

2. 正しくない経路情報を受信（交換）してしまい、他ASに流すべきトラフィックを別のASに転送したり、自分のASに吸い込んでしまう

等があげられます。

1については、ルータ仕様により発生することがありますが、ルータの設定で回避できる場合や、OSのバージョンアップ等で対処可能な場合があります。

2については、オペレーションミスやネットワーク構成の誤りによって発生します。

悪意を持って行う例はほとんどありませんが、被害を受けた側からするとインターネットへの接続性が失われるため大きな問題となります。この問題は「経路ハイジャック」や「権威のない経路広告」等と呼ばれています。

2008年にパキスタンテレコムが誤った経路を広告し、YouTubeへの接続性が失われた事例は長時間YouTubeに接続が不可能となったことから、当時大きく取り上げられました。

原因としては、パキスタンテレコムが何らかの目的でYouTubeへの接続を遮断しようとした際に起こったミスと考えられています。

参考
「Long BGP AS paths causing commotion」
http://bgpmon.net/blog/?p=125

「Saudi Telecom sending route with invalid attributes」
http://mailman.nanog.org/pipermail/nanog/2011-September/040300.html

BGPにおける経路制御では、細かい経路情報（サブネットマスクが長い情報）が優先されます。パキスタンテレコムはこのルールを利用して、YouTubeが広告している経路情報よりもさらに細かい経路情報をパキスタンテレコム内にのみ広告するつもりだったようですが、何らかのミスでこの経路情報を世界中に広告してしまい、結果としてYouTubeのトラフィックをパキスタンテレコム内に吸い寄せてしまいました。

参考
「YouTubeがダウン－原因はパキスタンでのアクセス遮断か」
http://japan.cnet.com/news/media/20368032/

「YouTube Hijacking: A RIPE NCC RIS case study」
http://www.ripe.net/internet-coordination/news/industry-developments/youtube-hijacking-a-ripe-ncc-ris-case-study

経路情報をねじ曲げたと思われる事例も発生しています。経路情報をねじ曲げて、トラフィックを自らのネットワーク経由とする例です。

先にあげたパキスタンテレコムの例では、トラフィックを吸い込んでしまうだけで終わりました（これはこれで問題ですが）。しかしこの場合、トラフィックが自ネットワーク経由になるだけで、最後には正しい宛先に送っています。

一見何の問題もないように見えますが、なぜこのようなことをするのでしょうか。これも、二つの理由が考えられます。

1. 設定ミスにより、上位ISPから受信した経路情報を、別の上位ISPに広告してしまった
→経由するネットワークが増えるため、通信速度や品質が劣化する **（図1参照）**

2. 何らかの悪意があり、意図的に自ネットワークを経由するよう経路情報を操作した
→経由したネットワーク内で中間者攻撃（Man-in-the-Middle）等の不正な情報取得が行われている可能性を否定できない **（図2参照）**

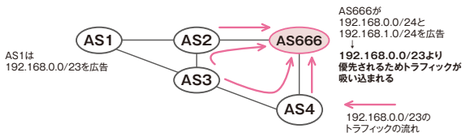
1に関しては実際に顕著な通信品質劣化が発生したことで事象が判明した事例があります。また、2については中間者攻撃の可能性を指摘した事例がいくつか報告されています。

図2：経路ハイジャックと中間者攻撃（Man-in-the-Middle）の例

（正常な例）

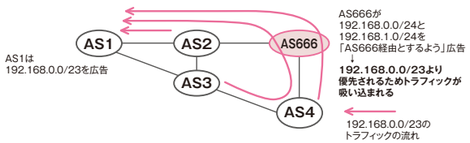
AS1が「192.168.0.0/23」を所有し、広告した場合
トラフィックの流れは上記のようになる
（ただし、トラフィックコントロール等をしない場合）

（経路ハイジャックの例）



AS666が「192.168.0.0/24と192.168.1.0/24」を
不正に広告した場合、トラフィックの流れは上記のようになり
本来の所有者であるAS1にトラフィックが流れなくなる

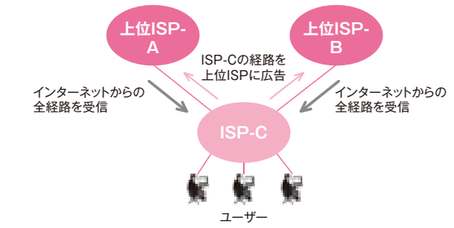
（中間者攻撃の例）



AS666が「192.168.0.0/24と192.168.1.0/24」を
ねじ曲げて広告した場合、トラフィックの流れは上記のようになる
※上記の例はAS666_AS2_AS1という経路パスを広告した場合

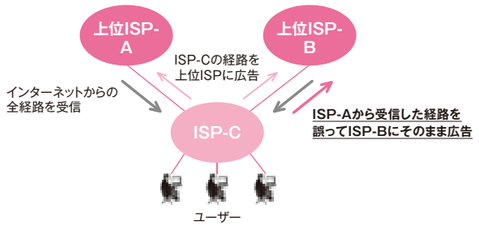
図1：設定ミスによる通信品質劣化の例

（正常な例）



上位ISP2社に経路を広告することで
上位ISPのどちらかに問題が起きてもユーザーの接続性は保たれる

（問題のある例）



ISP-Cが上記のような間違った広告をすることで、ISP-B→C→Aという
通信が発生する可能性 → ホップ数の増加や通信品質の劣化につながる

最近はIPv6でも権威のない経路広告と思われる事象が発生しており、Internet Week 2011のルーティングセキュリティセッションでも報告されました。IPv6の場合、アドレス表記が長いためIPv4よりも設定ミスが発生する可能性が高くなると思われます。

このように、経路情報は常に危険な状態にさらされているのです。

参考
「AS33259 leaking」
http://mailman.nanog.org/pipermail/nanog/2010-February/018521.html
「Facebook's detour through China and Korea」
http://bgpmon.net/blog/?p=499
「Defending Against BGP Man-In-The-Middle Attacks」
http://www.renesys.com/tech/presentations/pdf/blackhat-09.pdf

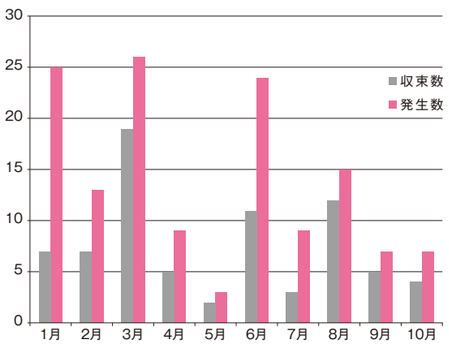
3. 最近の「経路ハイジャック」発生数

この事象がどの程度発生しているかは、毎年Internet Weekでも報告されています。

2011年のInternet Weekで報告された件数(2011年1月～10月)は138件でした。月に平均するとおよそ14件となります。最大で月に26件という月もありましたが、最小でも3件あり、0件という月はありませんでした。**(図3参照)**

JPIRRへの登録更新漏れやASの運用都合によるアラートも含まれてしまうため、すべてが「経路ハイジャックが疑われる状態である」というわけではありませんが、全く発生しない月はないということが見て分かります。

図3:「経路ハイジャック通知実験」での通知数(2011年)



4. 日本における取り組みの紹介

日本においても、対策については検討されています。ルーティングを脅かす事象そのものを防ぐことは困難ですが、事象が発生した際に「気づく・知らせる」ことができるような実験をしています。

・気づく:財団法人日本データ通信協会　テレコム・アイザック推進会議(Telecom-ISAC Japan) BGP-WGによる「経路奉行」
・知らせる:経路奉行と連携したJPNICによる「経路ハイジャック通知実験」**(図4参照)**

「経路奉行」はTelecom-ISAC Japan BGP-WGのメンバー(14社:2011年11月現在)より受信しているBGPの経路情報(フルルート:インターネット上の全経路情報)とJPIRRに登録されているRouteオブジェクトの情報を比較し、差異がある場合にアラートを発します。発せられたアラートはJPNICの「経路ハイジャック通知実験」サーバにも転送され、JPIRRのRouteオブジェクトまたはRouteオブジェクトに紐づいているメンテナーオブジェクトの「X-Keiro」に記載されたメールアドレスに「経路ハイジャックの疑いがある」ことを通知します。**(図5参照)**

海外にも同様の取り組みはありますが、日本国内に特化しているシステムは「経路奉行」以外には存在しません。現時点では国内の経路変動をいち早く知ることができる唯一のシステムです。

先の項目で紹介した経路ハイジャック発生数も、この「経路奉行」により検知した数です。

図4:JPNICと経路奉行の連携

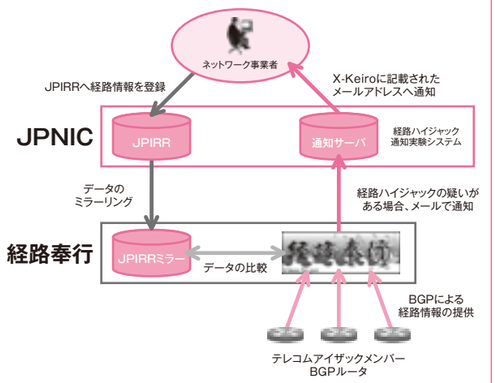


図5:X-keiroの記載例

```
(AS2515の登録例)
mntner:    MAINT-AS2515
descr:     Japan Network Information Center
           People authorized to make changes for AS2515
           X-Keiro: okadams@nic.ad.jp
           X-Keiro: kawabata@nic.ad.jp
           (以下略)
```

メンテナーオブジェクトやRouteオブジェクトのdescr項に「X-Keiro」という行を作成し、メールアドレスを登録します

もう一つの取り組みはリソースPKI - Resource Public-Key Infrastructure(RPKI)に関するものです。RPKIは、IPアドレスやAS番号が記載されたリソース証明書を発行するための認証基盤で、国際的にIPアドレスの割り振りを行っている五つの地域インターネットレジストリ(RIR)によって実験的に提供されています。日本の国別インターネットレジストリ(NIR)であるJPNICでは、日本におけるリソース証明書の提供や実用性について調査しており、そのために、技術動向とRIRの動向を継続的に調査しています。

リソース証明書は、記載されたIPアドレスやAS番号が正しく割り振られていることを示しています。

そしてリソース証明書は、ルータが、受け取った経路情報を確認するために使うことが想定されています。経路情報に記載されたIPアドレスが、設定ミス等によって本来の割り当て先ではないときには、ルータがそれを検知できます。検知した経路情報を無視し、自らの経路表に加えないようになれば、経路ハイジャックを自動的に避けられるようになるかもしれません。なお、この仕組みでは、受信した経路情報が別のISPに広報されてしまうような問題には対応できません。

これに対応するために、2011年の前半、BGPSECと呼ばれる仕組みの標準化がIETFで始まりました。BGPSECは、IPアドレスの正しさに加えて、ASパスの正しさを検証できる仕組みです。2節で述べた中間者攻撃を検知できる仕組みであるとされています。

参考
「An Overview of BGPSEC, M. Lepinski, S. Turner, Oct 31, 2011」
http://tools.ietf.org/html/draft-ietf-sidr-bgpsec-overview-01
「A Threat Model for BGPSEC, Stephen Kent, March 31, 2011」
https://tools.ietf.org/agenda/80/slides/sidr-5.pdf

BGPSECにおいては、各ASに対して発行されたルータ証明書を用いて、ASが発行する経路情報に含まれる「ASパス属性」と呼ばれる情報に、電子署名が施されます。すると、経由するネットワークの本来の順列を、ルータが電子署名付きで受信できるようになります。もしどこかのASが、意図的に本来と異なるネットワークを経由するようなASの順列を作り出し、経路情報として流していても、ルータが不適切な順列であることを検知できます。リソース証明書と同様に、YouTube事件のような、経路ハイジャックをルーターが自動的に避けられるようになるかもしれません。

リソース証明書とBGPSECは、いずれもRPKIがあって、はじめて実現できるものです。しかし実用性は未知数であり、ヨーロッパ地域のRIRであるRIPE NCCにおける総会では、RPKIの取り組みを継続すべきかどうかというところまで議論されました。結果、継続することになりましたが、ルータベンダーやIETFなどにおいて、実用性に関する議論が継続的に行われています。JPNICでもRPKIの実験提供について検討しています。

参考
「Agenda RIPE NCC General Meeting November 2011」
http://www.ripe.net/lir-services/ncc/gm/november-2011/agenda

5. 今後について

先に紹介しました「経路奉行」と「経路ハイジャック通知実験」は、通知のためにJPIRRの情報を利用します。そのJPIRRに不正確な情報や登録漏れがあると、正しい通知ができないだけでなく、正しくない通知を行ってしまう恐れがあります。

そのためにも、JPNICやTelecom-ISAC Japan BGP-WGはInternet Week等のイベントで現状の報告やルーティングセキュリティの重要性を解説し、運用者の皆様への啓発活動を行っております。また、JPNICにおいてはJPIRRへの登録を促進するためにも「経路ハイジャック通知実験」の通知範囲拡大を検討中です。

現状は「経路ハイジャックの疑いがある」という通知と、被害を受けている恐れのあるプリフィクス(IPアドレス空間)のみを通知していましたが、それに加え「どのASから誤った広告がされているか」を通知するよう、システムの改善を検討しています。

(KDDI株式会社 中野達也／
JPNIC 技術部 木村泰司／岡田雅之)