==========
第6回 Interdomain Routing Security Workshop (IRS6)
日 時: 2005/10/07(金) 15:00-18:00
場 所: Cisco赤坂 16F
参加者: 47名 (登録者人数)
==========

1. 議題

- DNS/BGP Anycast Unicast RPF
  コーディネーター: 吉田(NTT-C)
  プレゼンター: 石田(WIDE)、森下(JPRS)

- xSPのルータにおいて設定を推奨するフィルタの項目について(IPv6版)
  KDDI 石原 清輝
  POWEREDCOM 向井 将(プレゼンター)
  DTI 馬渡 将隆

2. 議事

2.1 xSP のルータにおいて設定を推奨するフィルタの項目について(IPv6版)

- 発表資料:
  http://www.bugest.net/irs/docs_20051007/IRS-20051007-mukai.pdf

- 概要: 馬渡さんの xSP におけるフィルタの IPv6 版
  - 最小限やるフィルタ
  - 運用で負荷がなければやるフィルタ

- 本質的には IPv4 と IPv6 で変化はない。IETF のドラフト、RIR で進行中のものは今日は除外したい。

- フィルタリングする箇所
  - ピア接続
  - トランジット接続
  - 顧客接続
  - ルーター自身へのアクセス
  →それぞれに「パケットフィルタリング」と「経路フィルタリング」がある

Q: ルータ自身に ping される場合、traceroute する場合、
Path MTU Discovery の場合には対応できるか?
A: type などでフィルタリングするなどの対応が必要

コメント: IPv6 では 途中のルータが fragment しないので Path MTU Discovery が動かないと悲惨なことになる。全ての ICMP Type を空ける必要はないが、IPv4 みたいに全部落としておくと困る。

コメント: 落とすものだけではなく、通すものも書くべき

Q: OSPF とかは大丈夫か。
A: マルチキャストも通すべき

コメント: 具体的にこれはダメと書いた方がいいと思う

Q: 設定テンプレートのようなものはあるか?
A: 経路フィルタはあるが、パケットフィルタはないようだ。

コメント: 最低限通しましょうというものと、これは reject しましょうというものの両方が必要。ICMP は必要。通常は全て reject し、必要なものだけ通すのが通常ではないか。

コメント: 逆に絶対に reject しなければならないパケットは存在しないと思う。通さなければいけないものを考えるべき。

A: 基本的には Neighbor Discovery は通すか。Neighbor Discovery は disable にしてもいいが、今後必要とする機器が出る可能性はある。

Q: 逆にNeighbor Discoveryを通すべきと書くのはどうか。見識がある人のコメントが欲しい。

Q: IANA から RIR に割り振られた prefix のみ acceptするのはどうか。

コメント: RIR 間では一時的にポリシが違う場合があるが、RIR 間でポリシをあわせる方向にある。フィルタをまったくかかないか、やるなら最後までしっかりやってほしい。IPv4では中途半端なフィルタが問題になった。

Q: NRO はどういう経緯でできたのか
A: "ICANNに対抗するのではない"ということになっている。RIRのすりあわせをやってほしい.

コメント: オペレータとして、どのようなポリシがやりやすいかといったものをあげていければと思う

コメント: レジストリが経路フィルタリングのリストを管理すべきと主張していくべき。

コメント: アドレスのリストがあれば、マクロで展開するルータがあってもよい。RIR の数は 5、ルータベンダの数は実際にはそれほど多くない。

コメント: マクロがあって、プリセットされていて、展開されるのはどうか。

Q: APNIC においては、 IRR がやっていくと考えているが現状はどうか
A: IPv6 の IRR は、APNIC の承認が通り、準備をやっている段階。

Q: IRR と連携していければよいと思う
A: IPv6 の IRR の使われ方は決まっていない、IPv4 のように Aut-num Object等が登録されるだろうが、RIR に正しい情報として承認されたものが登録される仕組みを持つかは決まっていない。こういう情報が登録されるべきだ、という声を上げていく必要がある。
JPNIC の方は、v6 をやることは決まっているが、どういうことをやるのかどうかは決まっていない。実装はこれから。JPNIC で決まったものを APNIC に持って行くことは可能。ただし、APNIC の IRR にRIPE で登録したアドレスを登録できるかは不透明。将来的には CRISP で相互参照できるようになる可能性もある。

コメント: IANA や NRO にリストを出してもらう方が現実的だと思う。

Q: IXとかに割り当てられているアドレスはブロックが決まっている。各RIRの持っている /32 から割り当てられるようになっており、各RIR が /32 など一定の単位で割り当てる方針を継続すれば、フィルタに活用できるのではないか。
A: レジストリとしては、IX 等には特殊アドレスというものを割り当てている。APNIC としては、それ専用のレンジを割り当てている。IX や DNS が一緒になっている。問題なのは IX はルーティングしないが、DNS はルーティングする点が異なる。RIPE はどうなのか不明。

Q: マイクロアロケーション用のブロックは各RIRで公表していた。APNICのIX用の 2001:07fa というのは、元をたどるとRIPEのようだ。DNSでは/32を流すが、IXは流さないなどをリストした方がいい。

コメント: 本当はRIRに出して欲しい

コメント: RIRのFTPサイトにdelegated-latestというファイルがあり、AS番号とプレフィックスが公開されている。ただし、どれぐらいの精度かはわからない。

コメント: だれかIPv6のレンジを分類する人が欲しい。JANOG でお知らせする

- IPv6 で考慮されるもの
  6to4
  RFC3068で定義
  グローバルなrelay routerの経路を広報
  日本では KDDI Labs さんが広報
  2002::/16,192.88.99.0/24をアナウンス
  anycast で回っている
  192.88.99.1
  2002:c058:6301::
  exact matchでのみ通るべき prefix

Q: 6to4 をサービスでやっている人はいる?

コメント: 自分の顧客に対して、KDDI にまでいくのは遠いので、顧客だけに提供するものはあるか

コメント: feel6 はそれに似たアプローチだが、6to4のアドレスではない

Q: 6to4の公共性はあるのか
A: 公共性はある。6to4自体はpeerからもacceptした経路を顧客に流してもいいが、トラフィックが大量に発生した場合も考えられるため、一般論としては定義できないのではないか。

コメント: KDDI では広報するから使ってね、というわけではなく、peerを通じて流している状態。ただし、研究所の話では 6to4 をやめるかもしれないとの事。

コメント: anycast って動くと考えられるが、よく考えると難しい。特に state があると、anycast がやられていること動かない可能性がある。逆に下手に流し続けると、下手に v6 流すとつかえない。tunnel 撲滅運動をしている人もいる。このページは pending にして、識者に聞いた方がいいと思う。
anycast で流しまくってそんなに簡単なものではない。

コメント: たまに abilene のをつかんで不便なこともある

コメント: あまり公共的なモノではなく、一般的なものではないと思う

コメント: WIDE がやっている v6fix に近いと思う。v6 に詳しい人は多いがほとんどは native につかっている人が多い。

Q: yosiki さんの感覚としては 6to4 みたいなものは残るか?
A: 残るとは思うが、6to4 として動かすのではなく、自分のところへの tunnel と言う形でサービスをする方が、ギャランティしやすいのではいかと思う。
「みれない」というクレームの原因が 6to4 にあれば、自分たちとtunnelする方向に向かうのではないか。

- ::/8
  - 感覚的には 0.0.0.0/8 に似ている

- IPv4 互換アドレス(RFC2893)
  - global には流れない

- IPv4 投射アドレス
  - IPv6 node 内部で使うだけなので global には流れない

- unspecified address
  - ND の Source Address に利用される
  - ルータは転送すべきではないと書かれている
  - IPv4 の special use と同様、フィルタして構わないと思う

Q: 一括で ingress filtering しても問題ないか - 特に異議なし

コメント: 未指定アドレスは外部のインタフェースでフィルタしても問題ないと思う

- /48 or longer の prefix
  - /48 より長い prefix は site に割り当てはされない accept するか, reject するか, 運用ポリシ次第か
  - 実際の IPv6 full route を見ると飛び交っている root server

コメント: いまの割り当てポリシならフィルタしたい。

コメント: /56 という話もあるので、それまでは /48 ぐらいまでは受け入れてもいいと思う

コメント: 怖さは /48 or longer でフィルタするというと、流していいと思う人がいっぱいいる。割って広報するのも容認するのか。

コメント：ドキュメントにおいてはニュートラルにしておいた方がいい。/48 以上は割り当てられることはないので、事故あるいは第三者的な妨害行為が考えられるとし、書かない方法もある

コメント：/32 をもっていれば、/33 * 2 を流すことを容認することを書こうとしている

コメント: その点には触れない

コメント：/32～/48の間でフィルタすればいいのではないかと書くと抑止効果になるのではいか。最低限/48で落とすべきと書く。書き方の問題であって、論点はシェアできている。

- 6bone
  2006/6/6 で終了予定
  originate は止まる? そうであれば落としても問題ない

コメント: 本当に落とすのであっても、これ以降のタイミングで落とせばいいやぐらいのところだと思う。落として弊害があるかどうか。

コメント: 影響度が分からないため pending。その日が来るまでわからない。

参考資料:
- xSPのルータにおいて設定を推奨するフィルタの項目について, http://www.bugest.net/irs/
- IPv6 BGP filter recommendations, http://www.space.net/~gert/RIPE/ipv6-filters.html

Q: 最終的にはどのようなアウトプットか。IPv4 と同様に文章にしていくということでいいか。
A: JANOG で発表し、6ヶ月ぐらいかかることになると思う。

2.2 DNS AnycastとRoutingに関する考察

- 背景
  DNS Anycast に関するID
  Operation of Anycast Services
  http://www.ietf.org/internet-drafts/draft-ietf-grow-anycast-01.txt
  BGP Anycast Node for Authoritative Name Server Requirements
  http://tools.ietf.org/wg/dnsop/draft-morishita-dnsop-anycast-node-requirements-01.txt

- uRPFとは(復習)

利点:
経路情報が変わった際にも動的に追従
欠点:
経路が変更された際に問題が起こる場合がある

RFC 3704 (BCP 84)
Ingress Filtering for Multihomed Networks

- RPF (Reverse Path Forwarding)

- Loose Reverse Path Forwarding w/o
  - いわゆる bogon フィルタ
  - パケットのソースアドレスがルーティングテーブルにあるかどうかを確認
  - 厳密にはリバースパスを確認するわけではない
  - Default free の世界でやるのが普通

- Strict Reverse Path Forwarding
  - パケットのソースアドレスは FIB を参照
  - SRPF ではパスの対称性があることを前提としている
  - 対称性がない場合には問題
    - RFC には運用で対応可能と書かれている
    - Edge ルータの edge 側 IF に適用することを想定している

- Feasible Reverse Path Forwarding
  - パケットのソースアドレスがRIBにあることを確認
    - パケットを受け取った interface が best でなくても良い
    - Source address に対してルーティングテーブルを引き、代替的に利用されうるインターフェースでもパケットは通過可能

- Feasible case Example 2
  - transit の関係で、このようなことが起こりうる
    →実例に近い

Q: ネットワーク D の経路が来ない理由がわからない
A: 前提条件: 左の方と右の方は、BGP の best の持ち方が違う
ネットワーク D の経路は ISP-Z には切っている
ISP-Aにとっては peer の経路が best になっており、ISP-Z には行かない

- Feasible case Example 3
  - ISP-Z と ISP-A の間には2回線があるが、複数回線ある場合、ある回線には特定の prefix を分けるといった mapping をしていると、それぞれの回線から聞こえているものしか受け取らないことになる。一部の経路だけがいかなかった, 経路交換の再、ISP-A からの経路が左から行かなかった場合、drop してしまう

Q: hot potatoは?
A: hot potatoの場合にも発生すると思う

Q: トラフィックエンジニアリングによって経路がなかったりすると通らないという理解で正しいか?
A: 正しい、通らない。

- Feasibleの考察
  - 動くことはうごく
  - ISP によってトポロジや適用の仕方を考えないと、パケットを落とすことにつながってしまう

コメント: customer AS が stub の AS なら、strict mode でも動くのではないか。

Q: 動かしている人は? - (特に反応なし)

→ traceroute をかけると、AS 内にはいった time-exceeded packet が uRPF にひっかかって落とされる. 帰りのパケットが落とされてしまう 例えば、ローカルアドレスでインフラを作っている会社もあるが、loose でも strict でもいれてしまえば、経路がわからない。しかも、それが 自分のエッジルータで落とされている。あとは、インフラのアドレスが グローバルだが、アナウンスしていない場合にも落とされる

→ Ultima Online のソフトが、traceroute してきて、経路上のルータに ping をして RTT が高くなっているポイントに文句を言えということが あったが、そういう人にとっては敵かもしれない

→ インフラアドレス自体は広告しておく、しかしルータの足に対するパ ケットを止めるという方法はある。直接ルータがアタックされないよう にし、経路を広報する。

→ OSPF の場合にはneighborの関係でinternal routeに載るので到達性が あるが、IS-IS では /32 はアナウンスされて到達性があるが、 connected の部分には readability をなくすことはある。

- 関係ないですが、Bogon route server の話
  Bogon route server がもう少しでできる
  tokyo でそろそろ上げる
  興味があれば peer をあげてください

- no-export を使う DNS の経路の配信
  route 情報は際限なくでていくのを防ぐために no-export
  トラブルが発生した際の範囲を限定化している
  root DNS server によってポリシが違う
  例: f.root:no-export 属性を付加

- DNS anycast とは
  RFC 3258
  Distributing Authoritative Name Servers via Shared Unicast Addresses

  UDP で 1 packet
    ほぼ保証されているといっても過言ではない
    返答が 512 byte 以下
    EDNS か TCP に fall back

  どれかを識別するために、サーバの tag ID をつける

- 最近の Internet Draft

  - draft-ietf-grow-anycast
    ルーティング: 5ページぐらい書かれている

  - draft-morishita-dnsop-anycast-node-requirements
    ルーティングへのRequirementsに対する記述はいまのところない

- DNS Anycast と uRPF

  - 現在の root サーバにおける DNS Anycast 実装
    local node が多数
    global node が少数

    f.root-server はローカルノードでやりなさいということを restrict
      root server から遠いところを救済
      本物以外は local node
    i.root-server:
      そうではない運用
      global node. local node 特に制限なし
      受けた方が決める,

local node の方が問題

- 何が問題か
  no-export community の活用

  正常時には問題ないが、障害発生時に大問題
  関係者が複数存在
    DNS Anycast のグローバル管理者、
    ローカルサイトオペレータ
    ピアしているオペレータ
    異常を受けた当事者
  -> プレイヤーがたくさんいて問題が複雑化

- 問題(その1)

  Q: どのモードでuRPFを動かしているのか? strictか?
  A: 特に考えていない

  Q: root server のオペレータは uRPF をしているか?
  A: そういうことも考えられるという話。ただし、そういうことをしている
     オペレータもいる

  Q: local から announce される経路は no-export がついているという前
     提か?
  A: はい

  Q: 本質的には multihome でも起こりうる話ではないか
  A: multihome の場合には判断する人は同じだが、今回の例では違う。
     multihome でも起こりうるが、もっと起こりやすくなる。

  Q: uRPF の責任にもみえなくない
  A: uRPF が悪いともいえなくもない、こういう問題が起きる可能性がある
     という点を広めたい

  Q: 本質とはずれるかもしれないが、AS aのLocalとGlobalから出るものは、
     prefix lengthが同じか?
  A: 同じ。no-export で出て行かないので、best にならない

- DNS Anycast を騙る
  - DNS Anycast の AS番号/IPアドレスを騙られた時に、それをいち早く検
    出できるか
  - DNS Anycast の経路がとこから聞こえてくるのが正しいか確認できるか
    ファーミングやフィッシングのために、特定のサイトに誘導できる懸念
    がある

  Q: 悪意をもったアナウンスに対してIRRは有効か?
  A: RADB にはいっているのは本当かうそかわからない, JPIRR はたぶん大
     丈夫

  Q: 攻撃対象は route server に限らない。経路騙り、routing どろぼうは
     ある組織に対しても起こりうるし、root server にも起こりうる。
  A: Anycast の deploy だけに向かっており、リスクが増大しているという
     懸念

3. 今後のIRSの予定

- 次回は　 2006年 1月12日(木)
- 次々回は 2006年 4月 7日(金)

以上。