
第7回 Interdomain Routing Security Workshop (IRS7)

日 時: 2006/01/12(木) 15:00-18:00

場 所: Cisco新宿

参加者: 23名 (登録者ベース)

1. Agenda

- IPv6経路とIRR
- xSP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

2. 議事

2.1. IPv6経路情報とIRRの状況について

Speaker: NTT小林さん、外山さん

- ・ 目的
経路のあり方を議論したい
- ・ 調査
IPv6経路情報と比較
 <=> WHOIS
 <=> IPv6 IRR (route6オブジェクトが登録できる)
- ・ 経路の状況
増加 sTLA 87% (6BONE以外の)
RIR毎に比率が違う
AFRINICは抜けている
6BONEは減少
- ・ Origin AS別
微増
- ・ Prefix Length別経路数
/32が多いが/48も増えている
- ・ Prefix Lengthによる分類
/35 more longer = 14.6%
/48は増加
- ・ IPv6経路の状況
経路数は増加
/32以上のprefixが増加
/48が流れると増殖するのでは？
- ・ 経路集約の考え方
LIR、ISPへの割り振りアドレス:
 /48での割り当て予定がある
 1つの集約したアドレスで方法すること
 NWの構成に沿って階層化、集約できることが必要
- ・ 経路情報とIRRの突合
inet6numと
route6と
- ・ 方法
prefix -> IRI -> whois

inet6num
 ARIN -> NetRange
 LACNIC -> inetnum
 statusにより、広報すべきか確認できる

- ・ inet6num
Best Match(分割された)が増えている
 - Exact Match
 - No Match
- ・ 整合度
/32に拡張後も、/35がそのまま広報されているものがある
NoMatch: 6to4とAFRINIC
- ・ statusによる状況の確認
集約すべきかなどがわかる
NON-PORTABLEやLIRによる集約が可能な経路がある
フラグメント数: 2が多い
今後/48が増加する可能性がある
- ・ route6の登録状況
Best Match、Exact Match、No Matchに分類
No Matchが多い(半数以上)
- ・ サーバ別/source別 登録状況
RIPEでの登録活動が大きく寄与。
- ・ route6との整合度合
BestMatchの中には・ route6のoriginを確認 -> originが違うものがある
- ・ Origin不整合のパターン(Exact Match)
実際のOriginがroute6のorigin ASの配下から広報されているケース
- ・ Origin不整合のパターン(Best Match)
Exact Matchと同様のものが・ ・
ミスオペ?パンチングホール
パンチングホールいいのか? -> 近藤さん: 「したい」
マルチホームしているかは、わからない。
route-viewでも、マルチホームはしてなさそう。

IXのアドレス空間が流れている
Peering Addressが流れている (登録されている/32に含まれる/128と/64が)
- ・ Summary
/48であるべきもの、あってはならないもの、区別できるような仕組みがあるといいかも。

inet6numでみると Registryに登録されたものだけが広報されている
ただ、100経路前後は広報しなくてもいい経路

route6でみると、RIPE、RADBの活動により登録は増えているが、登録率は悪い。
- ・ Discussion
IPv6の経路フィルタ・ ・ exactで

whoisのstatusは有益か
RIPEのALLOCATED-BY-LIRにはいろいろなものが含まれ過ぎている

Repositoryが乱立するとこまる
/48の区別はwhois+IRRで
- ・ 議論内容
 - 不要というのは?
必要性がないもの。
Aggregateの観点で集約できてないもの。
 - PAでながす
IPv4は違反ばかり なぜか? 使い勝手が悪いから

IPv6になったときに悪いというのはどうか？
eBGPは/48とかをうけないルータ？箱でがんばるか？

- データベースは？
意図しているか、してないか？(IRRに登録すれば意図している)
意図しているものを不要とするかしないか？
不要とすれば、IRRには/48が登録できないようにするとか

IRRに登録されたものは宣言されたもの。
IXの/48は、Assigned + Portableで、特殊アドレス。
-> 宣言すれば良いはなし

素性を知るには・・WHOIS+IRR
RIPEは判断しにくい(ALLOCATED-BY-LIRだけでは・・)
APNICはAssigned + Portable
RIPEはportableかどうかわからない
IRRの登録率は悪いので、WHOISの情報も使わないと・・
最終的にはIRRをみないと意図したものかどうかはわからない
理想的には流す経路をIRR route6 objectの登録率を100%にする
どの段階で登録を促進するか？(ビジネスが軌道にのってから？)
オペレーションに使うデータベースはIRR

IRRの登録 インフラが整ってないと皆登録しないだろう
割り振り != 経路 -> IRR必要
もし割り振り = 経路 であれば、IRRはいらないだろう

でかいところ(Verioとか) 自分でもってる 満足している
ちょっとfilterしたいところ - IRRをみる

- 経路爆発は？
HW的に頑張ればよい？
どれくらい必要か？ by ciscoさん
IPv4は1M
IPv6は256K

FIBのテーブル
alternate経路もいれるか？
テーブルが大きくなると収束時間の問題

実運用にのると細かい経路が増えてくるだろう
その段階でHWが対応できればよいだろう
管理できるかが重要ではないか？

経路増加で死んでるleaf ispもあるよ

- PI用の割り当て
ポリシーを新規に定義しなきゃ
PAはPAで分割せずに流す。PIはPIで別のを。
- more specificは
現在filterしても、もともと遅いので許容範囲。
deployしてくると、/48も通さないとぐるっと回っちゃう -> 遅くなる。
- IRRに対して
まずはどうしたいか？
IRRに対する機能要望を挙げる。

2.2. 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) Speaker: 馬渡さん、向井さん

- ・ ICMPv6
全て通すか、必要なものだけ通すか？
全てrejectはNG
Path MTU Discovery 最低必要

- ・ NDP
acceptで統一でよいのでは？
- ・ 6to4
結構使ってる。今後どうか？
filterはexact matchでaccept
- ・ Long Prefix
/49 or longerをreject
/32 - /48 を通す (short prefix /20とかがある)
/56にしましょうという話もあるが、それは決まってから変更
global unicast 2000::/3 を通すか？
/64も実際たくさん流れている・・・
- ・ Bogon Prefix
RIRに割り振りされたもののみ
RIRのdelegated-latestを元に
-> 信頼性が不明、データがない、実際難しい
IPv6 IRRを用いるか？
Team Cymru あまりupdateがない

bogon registryを誰かが作る？
- ・ 6bone
2006/6/6 に停止予定(本当に?)
停止してからreject
3ffe::/16 81経路
止めて様子を見るか？
- ・ 箇所
ピア、トランジット、顧客、ルータ自身へ
- ・ 顧客向け egress prefix filter
filter必要無いのでは？ (full route)
ユニークローカルなど、内部で使っている場合は出してはダメ。
マルチキャスト mBGPでも sourceが流れてくるだけでff00はこない。
自ASのprefixはrejectしてはダメ。
- ・ ICMPv6の処理
非優先にできる？
ルートプロセッサに渡す時に
v4ではできる。v6は？
CSR-1ではプロセス優先度が
多少実装もあるのでは？
typeでも優先度が違うのでは
最低限ではなくなってる
現状、まだやらなくてもいいかも
- ・ AS-PATH
v6は長いのがある
- ・ 顧客からの ingress packet
全部受けないと
- ・ system protection acl
書いてもいいのでは？
- ・ NTP
普通に通ってます
NTPだけを落とすことはないだろう
ルータへのpacket filterで落とすのはあり
- ・ delegated latest

afrinicって大丈夫？
これからfilter generateできる？
適用して実際の経路と比較

- ・ bogon prefix
Team Cymruに聞いてみます 馬渡さん

- ・ 文書化
ファイルは1つで

3. 次回

- ・ 4/7(金) 15:00-18:00
- ・ 箱 30-50人
- ・ 芝がいいな
- ・ agenda
bogonの話
IPv6 filter文書化
吉田さん、にしかずさん

以上