

経路ハイジャックについて考える

～prologue of 経路奉行～



Telecom-ISAC Japan
BGP WorkingGroup
渡辺 英一郎

• Telecom-ISAC Japan

ISPの業界団体のひとつです。

主にISP間の情報共有の場。

<http://www.telecom-isac.jp>

• BGP Working-Group

BGP関連の情報共有を目的として活動

現在のテーマは “経路ハイジャック”

現在、約10ASが参加

発生頻度 まれ？でも某ISPでは年に1.2度発生。

対応策 **理想論**：全てのASが厳格にprefix filter！（無理っ！）

将来：so-BGP,S-BGP...実装にはまだかなあ。

現状（予防策）：

できるだけprefix-filter,as-path filter,prefix-limit....

やっているASもあるが、やっていないASもある。

現状（回復策）：

相手にコンタクトしてやめてー！と言う。

さらにlongerなprefixをadvertiseしてとりかえす。

Hijack発生時、

ある程度、自AS内の通信は確保できる。
でも、他ASとの通信は気づきにくい。

どうやって気づくの？

- お客様お問合せ⇒もうちょっと能動的に監視したいよね。
- 外部ツール(lookingglass,MyASn,IAR,etc)を利用して監視。
⇒あまり国内にはない。局地的なHijackは検知しにくい？
即時性を求める場合、外部サイトに繰返し確認するにも限界が。
- 他のASからtransitを買って監視。⇒維持費…。

みんな、やりたいことはいっしょ

日本のISP間で情報共有したほうがいいんじゃない？

お互い”give & take”で監視しあうのがいいんじゃない？

ひとまず、みんなの
経路集めてみない？

いいねえ！

いいねえ！

あ、オシ、経路ハイ
ジャック検知するプログ
ラム作ってみただけど

どうせ、検知するなら
日本の経路をcheckして
知らせようよ！

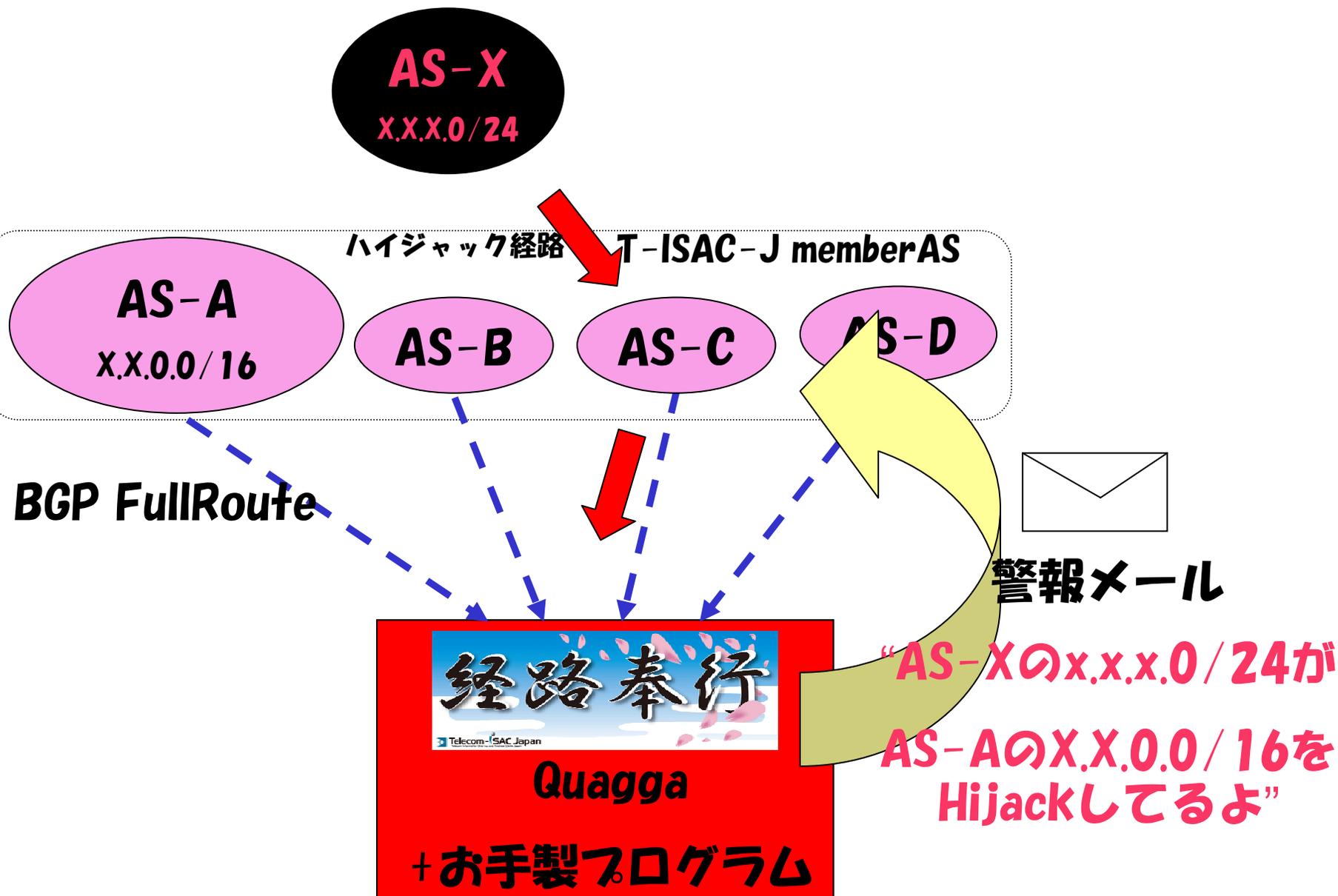
いいねえ！

そしてこんな感じになりました

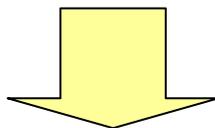
その名も

経路奉行

そしてこんな感じになりました(Cont.)



- 現在はT-ISAC-J BGP-WGに閉じた活動をしています。
- 経路奉行に興味があり、Give&takeなAS運用者の方々
T-ISAC-Jでいっしょに議論しませんか！
- 自ASのハイジャック警報だけでいいから知りたいの方々
例えばJPIRRのMaintenerに通知とか考えたい



興味のある人、ぜひご連絡ください。

bugyo@telecom-isac.jp



ご清聴ありがとうございました。