経路ハイジャック ～経路奉行 meets JPIRR～

Telecom-ISAC Japan
BGP working group

Yoshida ‘tomo’ Tomoya
<yoshida@ocn.ad.jp>
Matsuzaki ‘maz’ Yoshinobu
<maz@iij.ad.jp>

1. 導入編

- ハイジャック？
- こんな検出システム

経路ハイジャック？

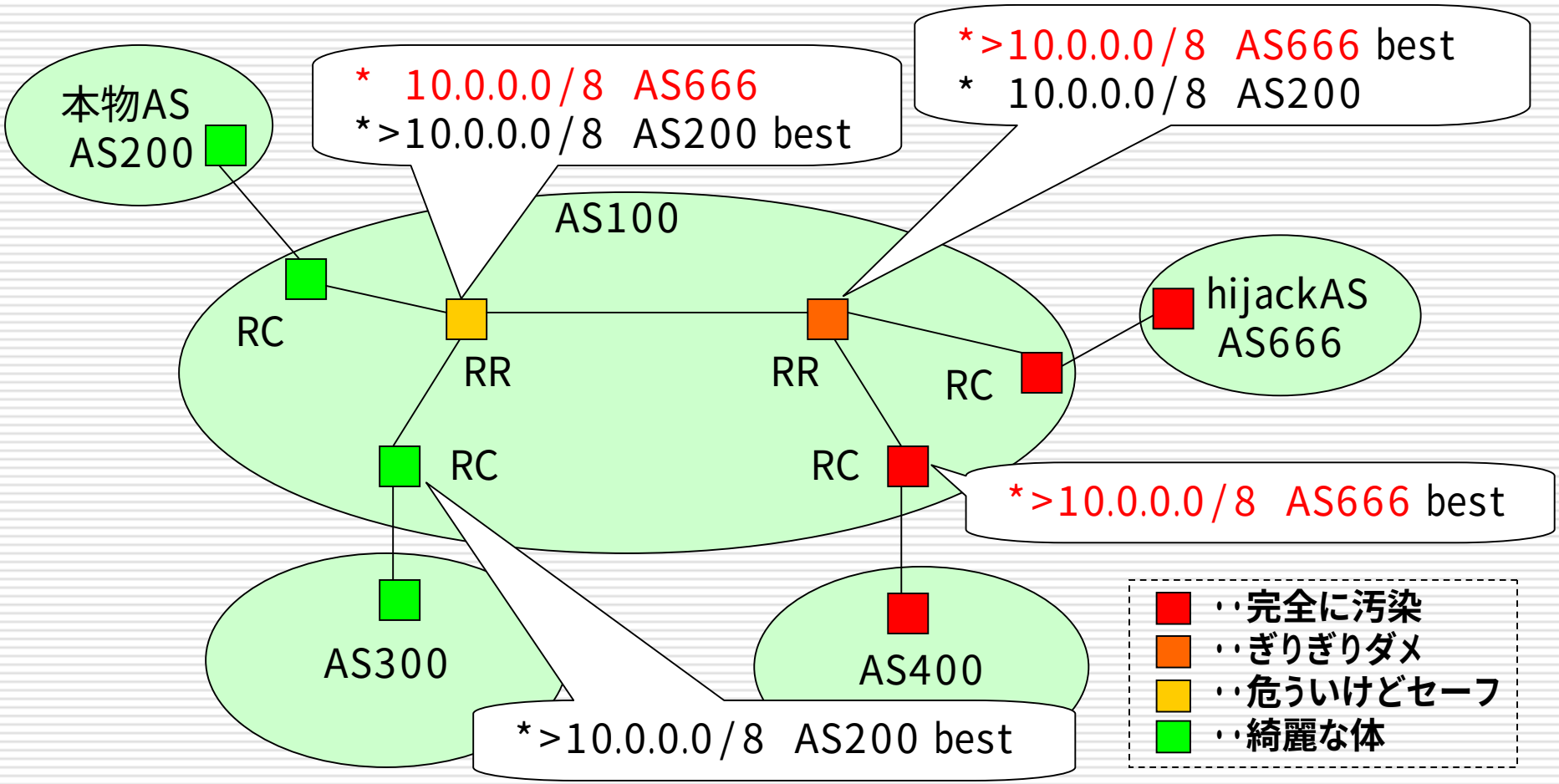
- **不正経路によるネットワークの乗っ取り**
  - **事故や設定ミス**
  - **不正利用**
  - **まあ、ハイジャックってちょっと名前が悪いかも**

- **ここでは不正なBGP経路に注目**

ハイジャックされた時の困り具合

- PAアドレス、PIアドレス
  - 通信自体
- bgp nexthopになっているアドレス
  - IXセグメントやPNIのpoint-to-pointのアドレス
  - 適切に経路フィルタすることで対応可能
- 重要サイト
  - DNSやIRR
  - 著名なwwwとかも困るよね、たぶん

経路ハイジャックとAS



なぜ経路ハイジャックが起こるのか

- **どこかで誰かが不正経路の広報を許してる**
- **将来的には、不正経路が広報できない手段を**
  - soBGP, sBGP, pgBGP?
  - **ただし実装を変えるのには時間がかかる**

目の前にある問題

- **とりあえず現状を見てみないといけない**
  - **不正経路ってどのぐらい流れてるのか**
  - **考えられる実装はいろいろ**
  - **有志であつまって、いろいろ試してます**
    - Telecom-ISAC Japan BGP working group

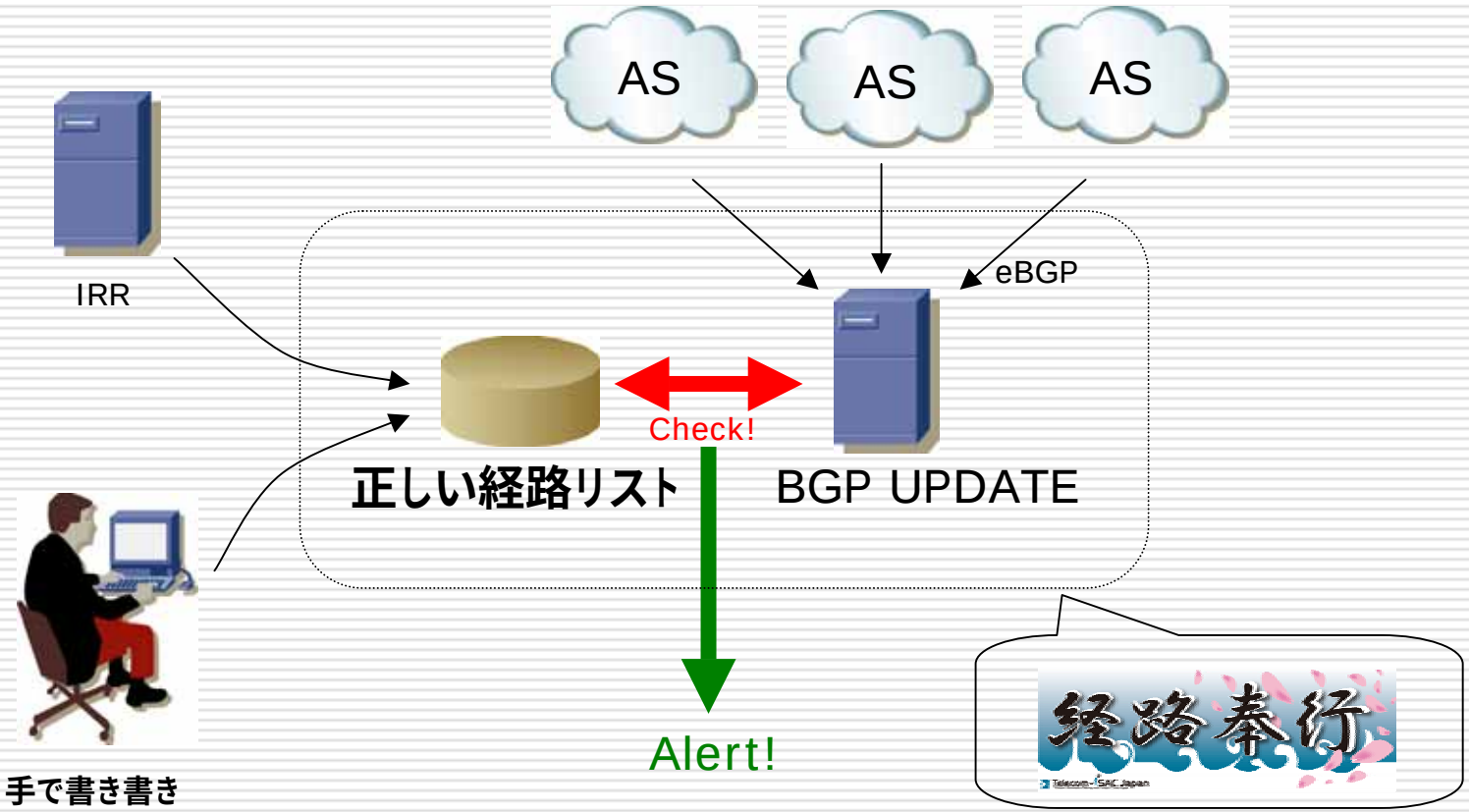
Telecom-ISAC Japan

- https://www.telecom-isac.jp/
- テレコム･アイザック推進会議
  - 情報システムは業界ごとに傾向がある
  - だったら、業界で集まってインシデント情報の共有や分析を行って、情報セキュリティ対策の充実をがんばりましょうという団体
- ここのbgpwgというワーキンググループ
  - がんばれ渡辺主査

検知システム

- **経路奉行**
  - BGP UPDATEと手元の設定リストを比較
  - 異常を検知するとアラートをメールで投げる
- irrzebra
  - zebraが経路受信時にirrを引いて検証
  - 結果によって独自のパス属性を付加して通知

経路奉行


AS
AS
AS
IRR
eBGP
Check!
正しい経路リスト
BGP UPDATE
手で書き書き
Alert!
経路奉行

正しい経路と経路奉行？

- **正しい経路をパス属性+NLRIで定義**
- **経路奉行では**
  - **広報元ASとprefixで設定**
    - 2497 { 210.130.0.0/16 ... } **みたいな書式**
    - IRR**も使ってる。**!gasXXXX**。一日一回設定更新。**
  - **広報元ASが異なる経路が見えるとアラート！**
    - **設定**prefix**と同じ若しくは細かい経路が見えた場合**
    - **現在はメールで送信中**

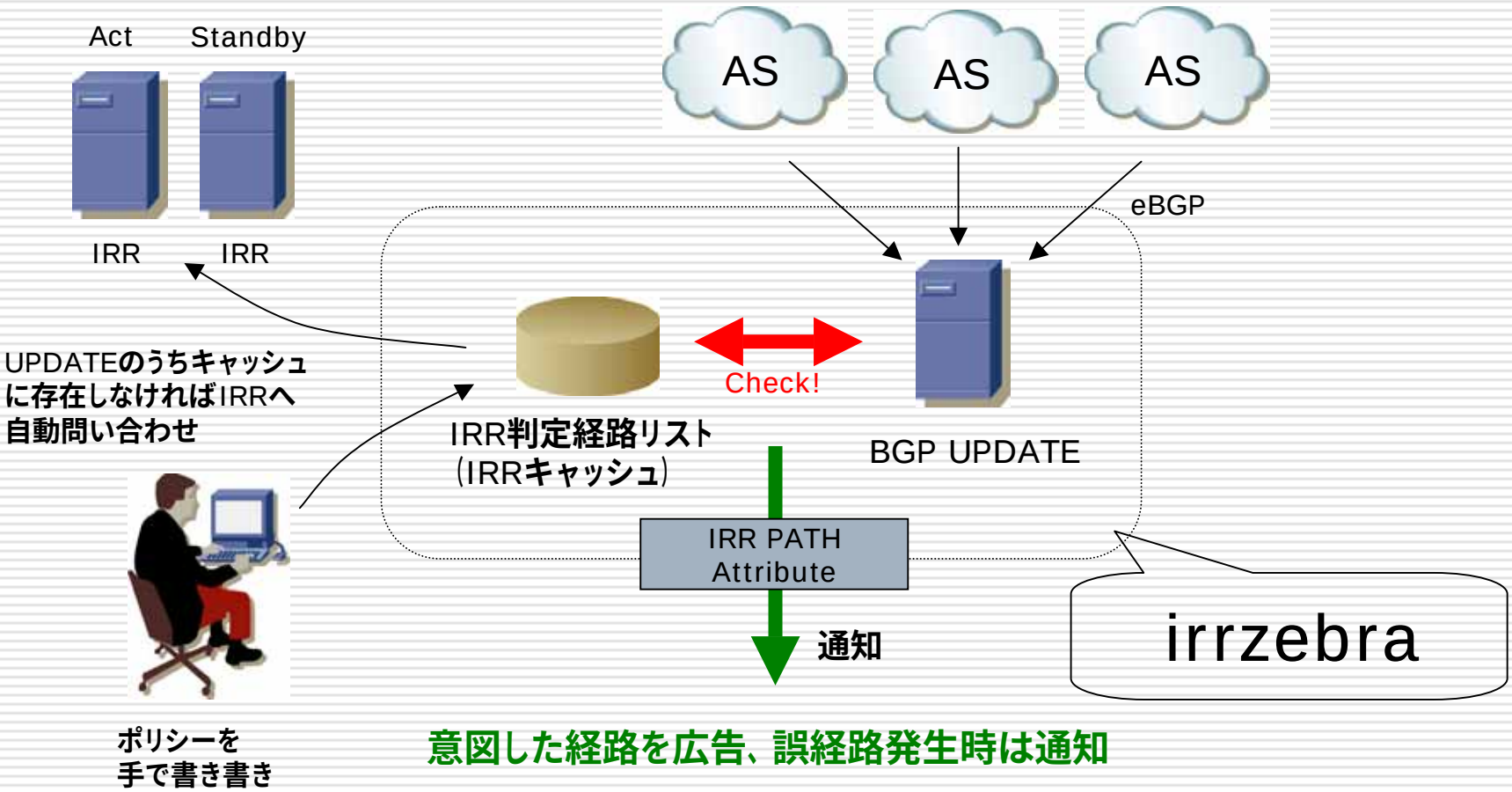
経路奉行と設定ファイル

- 設定が正しくないと誤検知だらけ
- IRR (RADB) を利用した設定情報
  - IRRのゴミobjectがいっぱい
  - 1日に400アラートとか泣きそう
- 手書きによる設定
  - イレギュラ対応
    - パンチングホールやマルチプルオリジン
  - Martianアドレスなどbogon経路の監視設定

JPIRRと経路奉行

- IRRを利用した設定を改善したい！
  - JPIRRが頑張ってるらしい
  - ・・・使えるかも
- JPIRRを使いたいとお願い
  - 2006年10月6日 (金) 10:00 ミラー開始
  - http://www.nic.ad.jp/ja/topics/2006/20061006-01.html
- だいぶよくなった ☺
  - それでも手書き設定はなくせないけど

irrzebra


Act
Standby
IRR
IRR
AS
AS
AS
eBGP
UPDATEのうちキャッシュ
に存在しなければIRRへ
自動問い合わせ
Check!
IRR判定経路リスト
(IRRキャッシュ)
BGP UPDATE
IRR PATH
Attribute
通知
irrzebra
ポリシーを
手で書き書き
意図した経路を広告、誤経路発生時は通知

irrzebraの判定・通知・制御機能

- **判定**
  - Origin**属性と**NLRI**の異なり具合で7段階に分類**
  - **異なり具合を独自の**IRR PATH**属性で表現**
- **通知**
  - IRR PATH**属性値に基づき経路異常通知**
- **制御**
  - IRR PATH**属性値に基づき経路制御**
  - route-map**で操作可。普通のルータと同じイメージ**
  - **暫定対応用**more-specific**経路生成も可能**
    - **でもこの機能はちょっと注意が必要**

2. 見えちゃうあれこれ編

- 勘弁してくれ〜〜
- ちゃんと情報登録してくれ〜〜

見えちゃうあれこれ

- **あれこれ1**
  - Bogon**経路**
  - **誤検知**
  - **その他** ☹
- **あれこれ2**
  - **経路ハイジャック**

でもって見えちゃう、あれこれ1

- bogon(**駄目**)**経路**
  - **プライベートブロックやその他**bogon**経路**
- **誤検知**
  - **特殊経路制御**
    - **マルチプルオリジン、パンチングホールなどなど**
  - new IANA allocation
  - bug
- **その他** ☹
  - **不正経路として検知して然るべき経路**

検知したアラート数の概要

2006年

	7月	8月	9月	10月	11月	12月
bogon	6	127	9	12	12	14
誤検出	18	38	10	65	7	6
その他 ☹	1		3		7	29

→ **JPIRRを参照開始**

- **参加AS、対象ASともに7つ**
- 1prefix**につき1アラート**

bogon経路

- プライベート空間は定期的に誰か広報する
  - bogon filterが流行ると見えなくなるはず
- 割り振られていないアドレス

- 考えられる原因
  - 実験環境からの漏洩
  - typo、設定ミス
  - 悪用のための一時的な広報？

bogon経路　事例

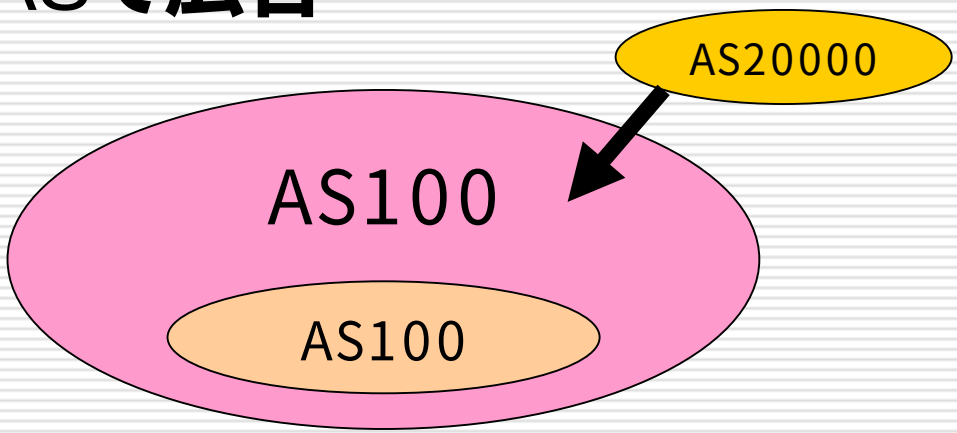
- 2006年8月　オーストリア方面から
- bogon経路そのものが山ほど
  - /8 x 65
- bogon route-serverから受信した経路をremove-private-asし、そのまま広告？
  - 5分後に一度消える
  - がまたその2分後に復活
  - 復活後18分で停止
    - 影響時間は30分ぐらい
    - uRPF-looseは当然効かなくなるよね

誤検知

- **特殊経路制御**
  - **マルチプルオリジン、パンチングホールなどなど**
  - **ほとんどこれ。確認後に設定追加**
- new IANA allocation
  - **最近/8が5つ割り振り**
- **設定を正しく維持すれば減らせる**
  - **きちんと減ってきている ☺**
  - **現在は手動で設定を変更している部分の影響**

誤検知　事例

- PIアドレスだと自分は思っている（自AS経路）
- その一部が突然別ASで広告
- ハイジャックか？
- ・・・
- 実は違う



- PIを持ち込んできた顧客が自分の知らぬ間にASを取得し、一部が広告される

- IRRや検知リストの設定維持を頑張る

その他 ☹

- **検知システムが検知して然るべき経路群**
  - **他のASが何か広報してる･･･**
- **今のところ、設定ミスか原因不明**
  - **直したと連絡がある** or **勝手に直ってる**
  - PNI**の**point-to-point**アドレスの漏洩？**
  - typo?
  - **設定ミス？**

その他 ☹ 事例1

- 2006年11月　韓国方面から　6ASで検出
- 細かい経路でorigin ASが異なる経路
  - /27 x 1
- 生成元に連絡がとれず経由ASの協力を得て解決
  - 経由ASでの経路フィルタ
  - 生成元に連絡して経路広報の停止
  - 影響時間は16時間ぐらい

その他 ☹ 事例2

- 2006年11月 インドネシア方面から　1ASで検出
- prefix長は同じでorigin ASが異なる経路
  - /17 x 2, /14 x 1
- 該当経路は直ぐに削除された
  - 影響時間は5分ぐらい
- その後の調査で他にもこのASから不正経路の広報があったことが判明
  - 検知システムにはそれらの経路が届かなかった

その他 ☹ 事例3

- 2006年12月　日本方面から　1ASで検出
- 細かい経路でorigin ASが異なる経路
  - /32 x 15, /30 x 14
- 広報元に連絡、対応してもらった
  - 影響時間は23分ぐらい

3．さあこれから益々頑張るぞ編

・システムのさらなる改善
・頑張れ、頑張る、JPIRR

検知システムが見るもの

- **検知の前提条件**
  - **不正経路が検知システムに届く**
  - **正常な経路と見分けがつく**

- **実はここに検知システムの限界がある**

検知システムが見ないもの

- **検知システムに届かない不正経路**
  - **局所的なハイジャック**
  - **検知システムに届く前にフィルタされている場合**
- **正常な経路と見分けがつかない不正経路**
  - **正常経路の定義**
    - origin AS**が同じとか**
  - whois**など、登録情報の乗っ取り**

検知システムは使える？使えない？

- すべてを解決するわけじゃない
- でも、不正経路の状況を「お手軽」に知れる
  - 問題の認知
- しかもIRRへの登録も進む ☺
  - IRRへの正確な登録は将来のために必要
- というわけで、頑張っておくとよい感じ

システムの改善

- 今のところ、大きく2つ
  - 経路の収集
    - 検知システムにできる限り経路を届ける
  - 経路の判別
    - 届いた経路から不正経路の判別をする

- 実は他にもいろいろ
  - 通知方法とかいっぱい
  - 頑張ります

検知システムに経路を届ける

- **収集する経路を増やす**
  - **多くのASから**
    - **AS毎に持っている経路は異なるかもしれない**
    - **大きなネットワークの場合には多くの拠点からも経路をもらったほうがよい**
- **検知システムの到達性をよくする**
  - **到達性がないと、そもそも経路も届かない**
  - eBGP multihop**はお手軽でいいんだけどね**

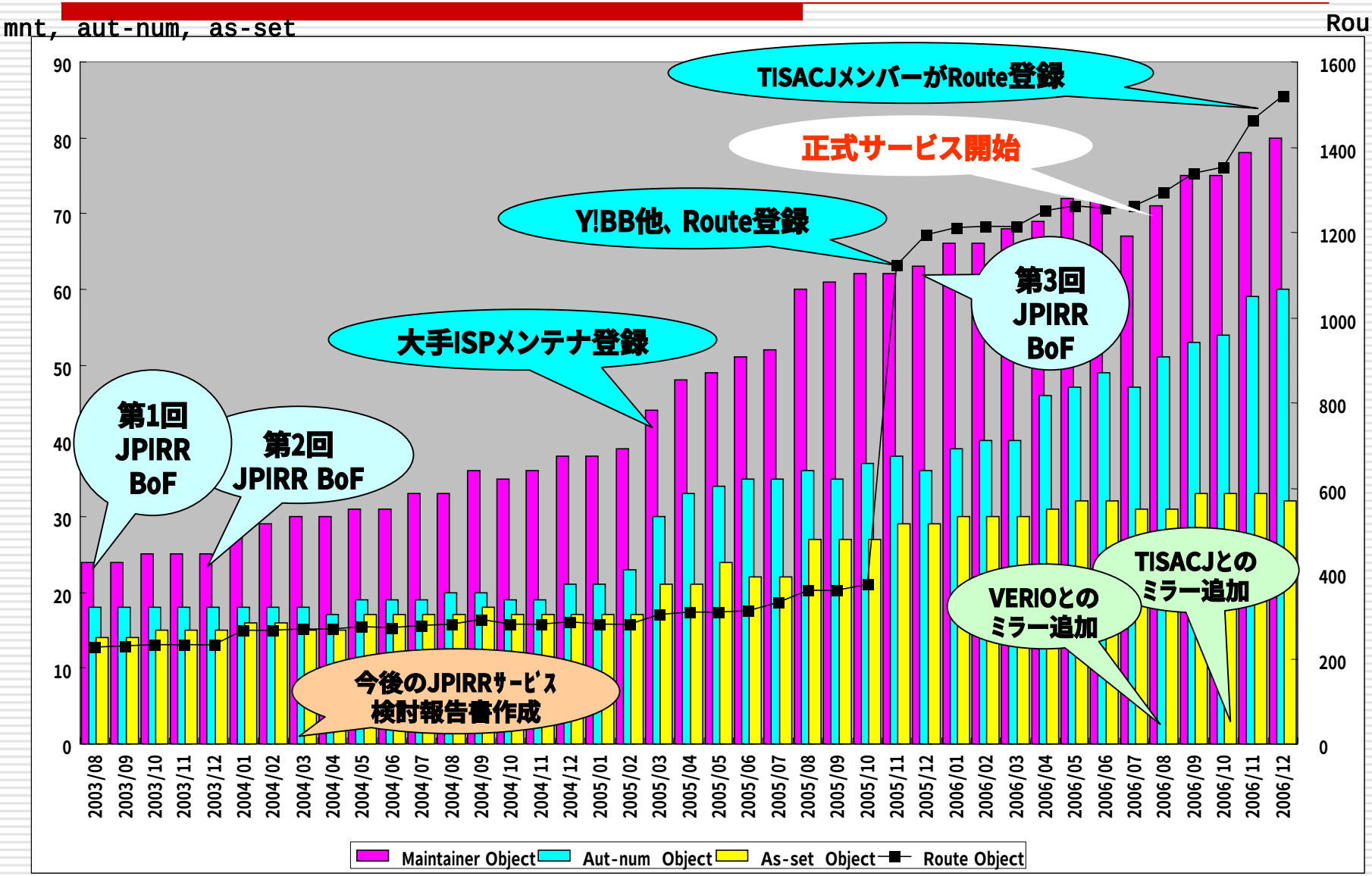
不正経路を判別する

- **設定情報を綺麗に維持する**
  - IRRの登録情報を綺麗に維持
  - 頑張れJPIRR
  - IRRに正しい情報を登録し、維持しましょう！
- **判別方法を頑張る**
  - もっといろいろ見る
    - パス属性、状態変化
  - ぐっと来るアイディア募集中

IRR情報の正しさの重要性

- Routeオブジェクトを登録
- BGPで経路広告
- これで安心しちゃダメです
- 両方間違ってたら検知できない
- どうすればよい？
- 適切なIRR情報のみが適切に登録されるIRRの必要性
- 頑張れ、頑張る、JPIRR

JPIRR、頑張ってます



レジストリ情報と連携します

- **4月から実験開始**
- **メンテナー登録頂き、実験に是非とも参加してください！**

ちょろちょろ見えてるJPIRRユーザ

- 6AS **以外の** JPIRR Maintainer
  - **ここ2ヶ月で3件ぐらい何らか検知**
  - **ハイジャックなのか誤検知なのか不明**

- **皆で頑張りましょう**

経路奉行のオープン化考えてます(案)
～co-operated with JPIRR～

プレイヤー 今のところJPIRR登録ASに限る	経路 情報 提供	経路 検索 web	経路 検索 vty	アラート 通知
BGP-WGメンバ (Telecom-ISAC Japan会員)	○	○	○	○
経路奉行限定メンバ (Telecom-ISAC Japan非会員)	○ よろしく		○	○
アラートを受け取りたいだけのAS ・・・というのを考え中				○(*1)

(*1) **通知/拒否の方法案**:「mntner: “remarks: hj_alert=no”」

奉行･irrzebra 接続AS募集中

- Telecom-ISAC Japanメンバの人
  - そのままBGPWGにご参加ください ☺
- Telecom-ISAC Japanメンバじゃない人
  - 会費など無しで参加できるようになりました ☺
  - 既存接続ASから推薦人を探してね
  - 審査やNDAなどの諸手続きを経て参加できます
- 詳しくはBGPWGメンバまで
  - AS17676, AS4713, AS2510, AS2518, AS4688, AS4725, AS2497 等など
  - AS名はJPIRRで引いてね ☺
    - whois –h jpirr.nic.ad.jp asXXXX

４．ハイジャック、実対応編

・当日会場からの予想外の報告
～今ハイジャックを受けているんです～
その後・・・

2Prefixが今ハイジャックされている

- STNETさんから報告
  - 今ハイジャックを受けているんです・・・
  - 1/26AM 本会議の質疑応答にて報告があった
    - 未使用のプリフィックスのため実害は無し

- とりあえず発表終了後、紙にハイジャックをうけているプリフィックスと連絡先をメモしてもらった・・・

さあ、調査開始

- 経路奉行、irrzebra
  - AS7018から同一プリフィックスが11月末広告
  - 両方ともに1ASのみで観測
    - 他のASではベストパスになっていなかった
- IRRへの登録状況
  - AS7018は情報なし（経路広告のみ）
  - STNETさんは、JPIRR and RADBに登録あり
- JPNIC方面
  - 年末このブロックを払い出す前の確認では、経路は広告されていなかった
  - 恐らくこのあとにAS7018から広告されたかんじ

IRRへの登録状況

- **route: 122.＊＊＊.64.0/19**
- **descr: STCN**
- **origin: AS7522**
- **notify: stcn-adm@stnet.ad.jp**
- **mnt-by: MAINT-AS7522**
- **changed: stcn-adm@stnet.ad.jp 20070117**
- **source: JPIRR**

- route: 122.＊＊＊.64.0/19
- descr: STCN
- origin: AS7522
- notify: stcn-adm@stnet.ad.jp
- mnt-by: MAINT-AS7522
- changed: stcn-adm@stnet.ad.jp 20061120 #10:04:36(UTC)
- changed: stcn-adm@stnet.ad.jp 20061120 #10:10:29(UTC)
- source: RADB

ハイジャックが消える

- IIJから早速AS7018へコンタクト
  - 早速週明けの1/29に経路広告停止が確認
    - I have removed the statics and asked our customer care center to check how they even came into the network. I'm terribly sorry for the problem this might have caused to you and/or your customer
  - 依然原因は不明・・・
- とりあえず一件落着

今回の一件について

- **観測AS**
  - **1ASのみで観測**
  - **観測ASを増やすことは重要**

- **JPIRRとの連動**
  - **検出できていた**
  - **正確に情報が登録されていれば検出可**
    - **通知方式などを検討する必要あり**

ということで・・・

1. 経路奉行への接続方法

- Telecom-ISAC Japanに既に加盟されている方、これから加盟される方
  - そのままBGPWGにご参加下さい。

- Telecom-ISAC Japanメンバ以外の方で、検知システムのみの利用
  - 検知システムにfull-routeを提供頂きます、会費等はありません
  - 既存のBGPWG参加メンバから推薦人を探して下さい
    - AS2497, AS2510, AS2518, AS4713, AS4688, AS4725, AS17676
  - 審査やNDA等の諸手続きを経て参加できます

2．JPIRRへの登録方法

- **PA/PIアドレス、ASをJPNICより取得されている方、JPIRRへご登録ください**
  - **費用はかかりません**

- **JPIRR参考情報**
  - **新規ユーザ登録**
    - http://www.nic.ad.jp/doc/jpnic-01048.html
  - **登録者、利用者向け、全般の情報**
    - http://www.nic.ad.jp/ja/ip/irr/