経路ハイジャックされた話

公開版

Matsuzaki ‘maz’ Yoshinobu
<maz@iij.ad.jp>

IPアドレスと経路制御

- インターネットでは通信先のコンピュータを識別するためにIPアドレスを利用
  - IPアドレスの世界での一意性を担保するために、インターネットレジストリ(APNICやJPNICなど)がIPアドレスの割り振りと登記情報の管理を担う
- 割り振られたIPアドレスがインターネット経由で到達できるためには、BGPによる経路広報が必要
  - BGPは、ISP等のネットワークがIPアドレスの到達可能性情報を交換するための通信規約

不正経路広報

- BGPはその仕様上、どんなIPアドレスの情報でも経路広報できる
  - このため相互接続したネットワークを通じて、設定ミス等による不正な経路情報が流通する事故がたびたび発生している
- ISPはBGPで経路広報する前に、インターネットレジストリ(APNICやJPNICなど)の登記情報(WHOIS)を照会して、正しい利用者からの広報依頼であることを確認(しているはず)
  - 手動による確認であり、登記されている情報も限られているため、間違いも発生する

不正経路広報の検出と対応

- 不正と思しき経路を検出するプロジェクト
  - 世界にいくつか存在し、日本ではT-ISAC-JとJPNICが運用する経路奉行システムが稼働中
  - 経路の変動やIRRに登録された情報との差分を検出するなどの手法が採用されている
    - IRRは、ISP等が経路広報に関するポリシを登録、公開できるデータベース
    - 経路奉行ではIRRの情報を基に不正経路の検出を実装
- 検出後は、関連ネットワーク管理者に連絡する等して、不正経路の広報停止を実施
- 不正な経路広報を防ぐため、電子証明書を利用したRPKIによる経路広報元認証の仕組みが導入されつつあるが、まだ普及には時間がかかる見込み

IIJが遭遇した事例

- 160.13.0.0/16
  - 2014/10/21にIIJへ移転
  - https://www.nic.ad.jp/ja/ip/ipv4transfer-log.html
- IIJでは将来の利用に向けて在庫として保持
  - 経路広報せず、IRRにも未登録だったため、経路奉行の監視対象になっていなかった
- 実は他ネットワークから経路広報されてた
  - 2015/01/05 15:40JST 頃から広報
  - 160.13.0.0/17, 160.13.128.0/17

認知

- 2015/02/04、JANOG MLにて該当ネットワークが不正に経路広告されていると指摘
  - [janog:12845] IIJ to the white courtesy phone.
  - ピーターさんありがとう！

対応

- 不正経路広報の停止
  - 経路広報元の米国ISPに連絡
  - 2015/02/04からメール、電話にて連絡開始、IRR登録およびIIJからの経路広報開始
  - 2015/02/07、不正経路広報が停止
- ブラックリストからの削除
  - 2015/02/12、SpamHausにメールにて削除依頼
  - 2015/02/13、SpamHausのブラックリストから削除

広報元ISPとの連絡

- 2015/02/04
  - noc@にメール&電話して、よろしくとお願い
  - 口頭で分かったよーと言われるものの進展無し
- 2015/02/06
  - 再度NOCに電話して、チケット番号をもらう
  - ようやく進展

- チケットシステムで回しているNOCでは、まずチケット番号をもらって握っておくのが必須

原因調査

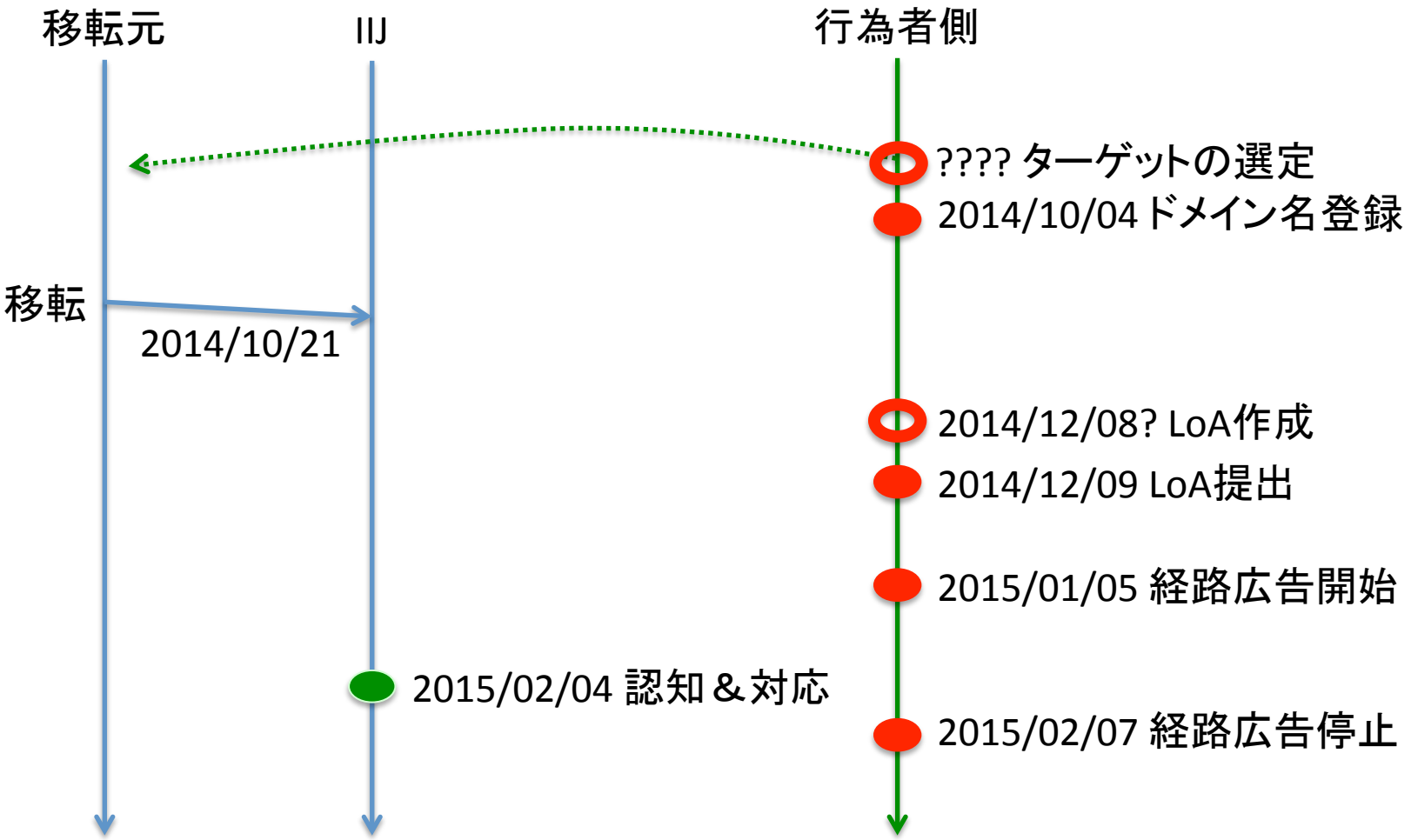
- 行為者がISPにLoAを提出して、広報依頼していた事が判明
- LoA (Letter of Authority)は、持ち込みIPアドレス等を利用する場合に、IPアドレスの保持者がISPに経路広報を許諾する書面
  - 広報を許諾する旨の内容
  - 該当するIPアドレスブロック
  - 責任者の署名、連絡先
- でも、IIJはそんなの提出してないよ？

移転前の組織情報を
参照したと思われる

偽装したLoA

が提出されてた

時系列まとめ


移転元
IIJ
行為者側
???? ターゲットの選定
2014/10/04 ドメイン名登録
移転
2014/10/21
2014/12/08? LoA作成
2014/12/09 LoA提出
2015/01/05 経路広告開始
2015/02/04 認知＆対応
2015/02/07 経路広告停止

法執行機関に相談してみた

- 事象の説明
  - インターネットの経路制御の仕組み
  - 行為者が行ったこと
  - 行為者の得られる利益や想定される背景
- いかんせん、今までに事例のない事案
  - どの部署に相談するかも結構問題

さて立件するとなると

- 何の罪に問えるか
  - 犯罪に該当するかどうか
- 被害判定
  - 被害って何？被害額っていくら？
  - どのぐらいの事業者が影響を受けるの？
- 行為者の居住地
  - どこに居るの？

他の疑わしい事例

- なぜ“疑わしい”かというと、普通ならそんなところから広報されないとは思うけど、被害者の事業上の判断は外から分からないから
- 例えば 160.14.0.0/17, 160.14.128.0/17
  - 同じ米国ISPから広報
  - 2015/02/10 広報開始
    - 160.13.0.0/16広報停止の３日後
  - 2015/05/16 広報停止

他の事例

- SANOGで報告された事例
  - 2014/08/29 インドの事業者が、利用していないネットワークを経路ハイジャックされた。SPAMの苦情が急増して事態に気がつく
- RIRから聞いた事例
  - パスポートやドメイン名を偽装してIPアドレス保持者に成り済まし、IPアドレス移転を試みる
- JANOGで報告されている事例

日本の事情

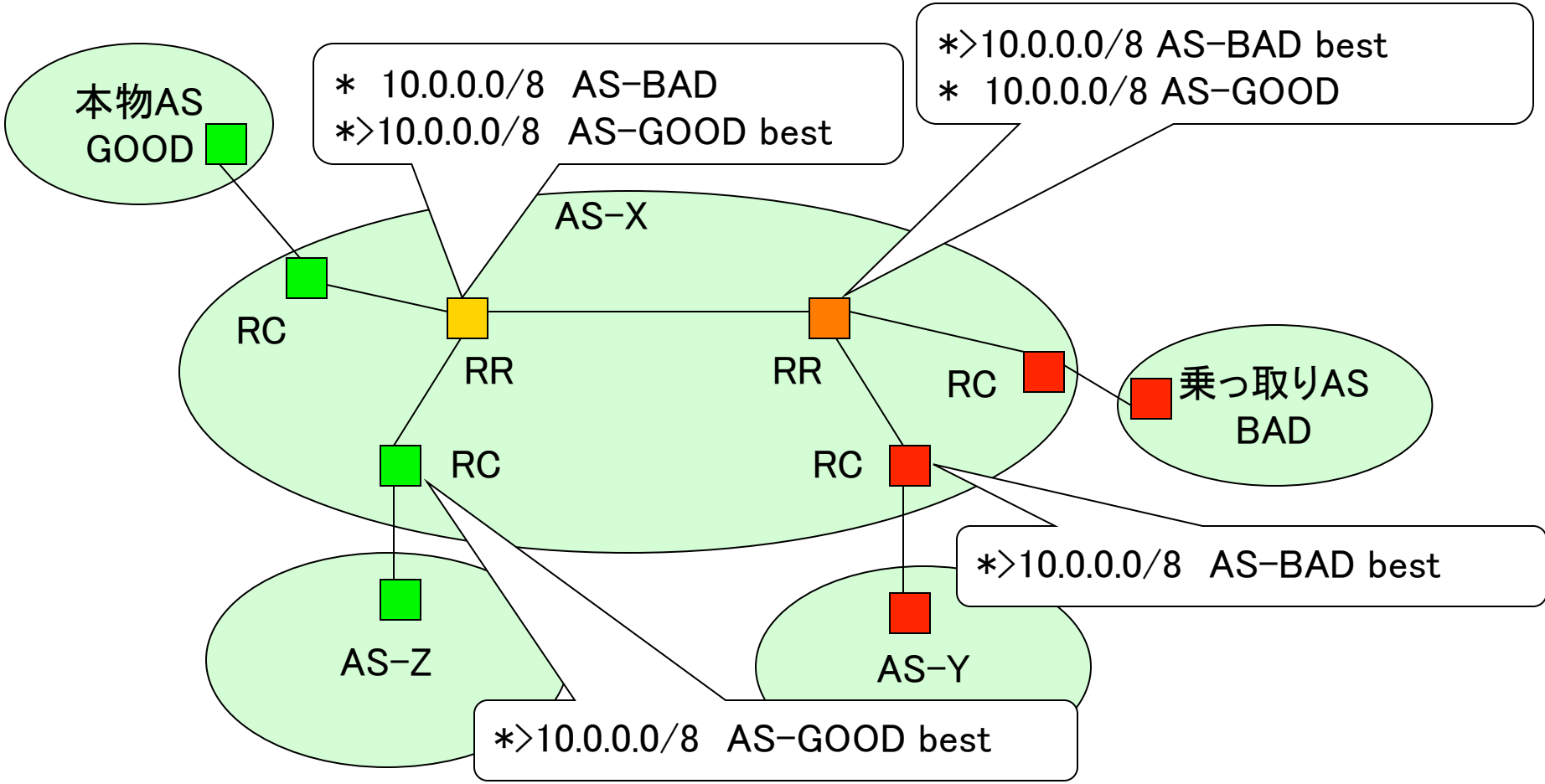
- 歴史的割り当てが多い
  - 連絡先が不明確なIPブロック
  - 比較的巨大なIPブロック
- 広報されないIPブロック
  - 一意性を担保するため、組織内で利用
  - でもって今更なかなか変更できない

→　狙われやすそう

運用での対応策

- whois登録情報の整備
- IRRへの登録および経路広報
- 経路奉行などでの経路監視
- spamの苦情傾向の把握
  - 経路モニタだけでは検出しきれない局所的なハイジャックでも検出可能かもしれない
- RPKIの実装とか

ASの中でさえ、汚染具合は違うかも



話してみよう

- 何らかの悪意をもって経路ハイジャックするケースが際立ってきている
  - どう思いますか？
- 事例の共有、対策の拡充が重要
  - JPNICの管理範囲は乗っ取りにくそうという状況を作れれば良いんじゃないかなあ
- この件に関しては、行為者に何らかのペナルティを課したいと考えているんだけど、どう思いますか？
  - 警察への要請とか