あなたのIPv4アドレス 狙われていませんか？

～経路ハイジャックとRPKI ROA～

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

/16がこんな感じの広報されてた

- 10.666.32.0/21　　origin AS-A
- 10.666.40.0/21　　origin AS-B
- 10.666.48.0/21　　origin AS-B
- 10.666.64.0/21　　origin AS-B
- 10.666.72.0/22　　origin AS-B
- 10.666.76.0/22　　origin AS-C
- 10.666.96.0/23　　origin AS-D
- 10.666.98.0/23　　origin AS-D
- 10.666.100.0/23　　origin AS-D

全てRADBにrouteオブジェクトあり

- 「descr: Customer Prefix」と書いてあるもの多め
- メンテナのAS番号相当部分とorigin ASは異なる

- RADBは誰でもなんでも登録できる
  - 一味が勝手に登録した可能性
  - 上流ASがトランジットのために自動登録したかも

RPKI Origin Authorization (ROA)

- RPKIで、prefixの広報元ASとprefix長を示す

- ROAの内容は資源ホルダが意図したと推定できる
  - RPKI的なデジタル署名
  - RPKI CA (RIRやNIR)での認証システム

- 世界からROAを集めて、受信した経路情報と比較
  - RPKI Origin Validation (ROV)
  - 広報元ASが違うとか、prefix長が違うとか

資源ホルダに確認の上、ROA発行

- 10.666.0.0/16、AS0
  - インターネット上で広報されないとする、いわゆるAS0 ROA発行

- ほぼ瞬時に効果が出た！

→ RADBのrouteオブジェクト消失
  - RADBはROA INVALIDになるオブジェクトを応答しない（2023年実装）

→ インターネット上からほぼ全ての経路情報が消失
  - ROVで実質的なインターネット到達性が失われる

ハイジャック経路が残るところ

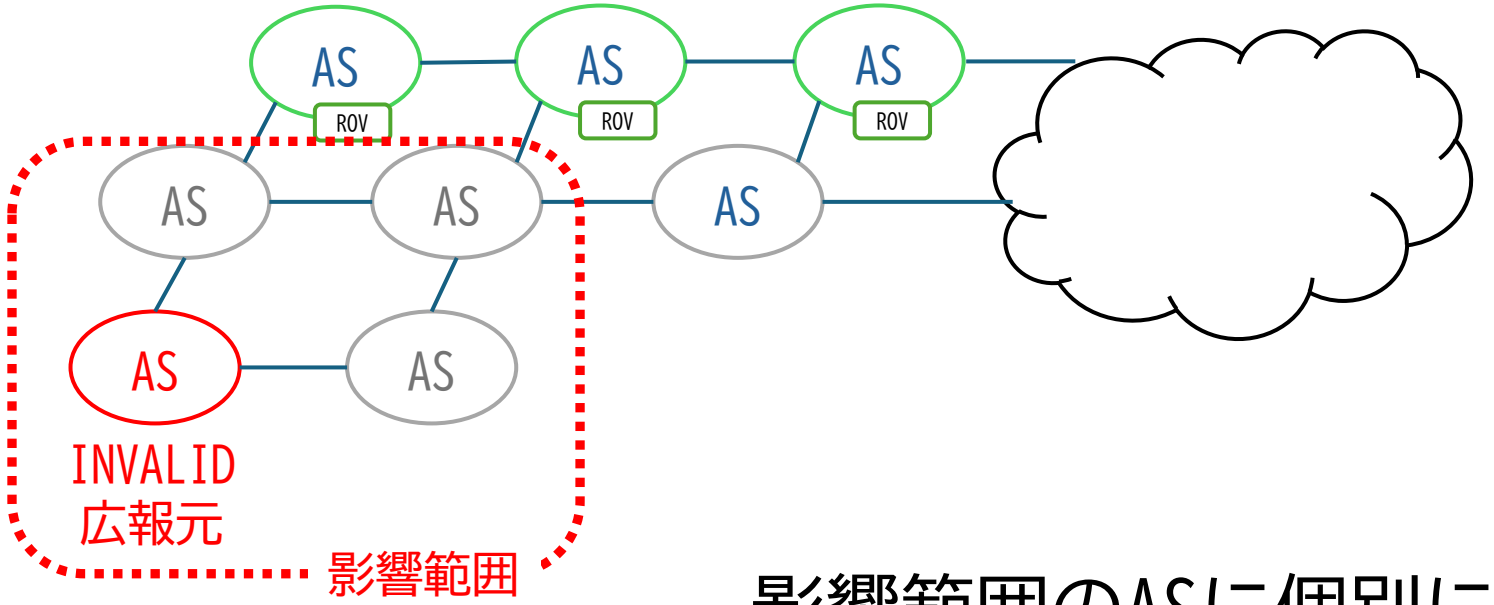
- ROVされてないASを抜けていく

- 顧客(INVALID広報元)から受信しちゃってる上流
  - 経路の確認が不十分
- INVALID広報元と直接ピア（しかもROVしてない）
  - あるいはその上流と直接ピア（しかもROVしてない）

- すごく限られたネットワークで経路が見える
  - グローバルな到達性はほぼなくなる

ROV導入状況とINVALID経路の影響

- 大手のISPが概ね導入している模様
  - 既に不正(INVALID)経路の影響が局所化できる状態



影響範囲のASに個別に連絡して対応

まとめ

- ROAは非常に強力な手段になっている
  - 即時にハイジャック経路を実質的に止められる

- RPKIに関連する運用の重要性が高まる
  - CA、Publication、Cache、Router
- RPKIに偽情報が無いのが大事
  - 人的ミス
  - 認証