

経路ハイジャックに一撃 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 A
- 10.666.40.0/21 origin B
- 10.666.48.0/21 origin B
- 10.666.64.0/21 origin B
- 10.666.72.0/22 origin B
- 10.666.76.0/22 origin C
- 10.666.96.0/23 origin D
- 10.666.98.0/23 origin D
- 10.666.100.0/23 origin D

全てRADBにrouteオブジェクトあり

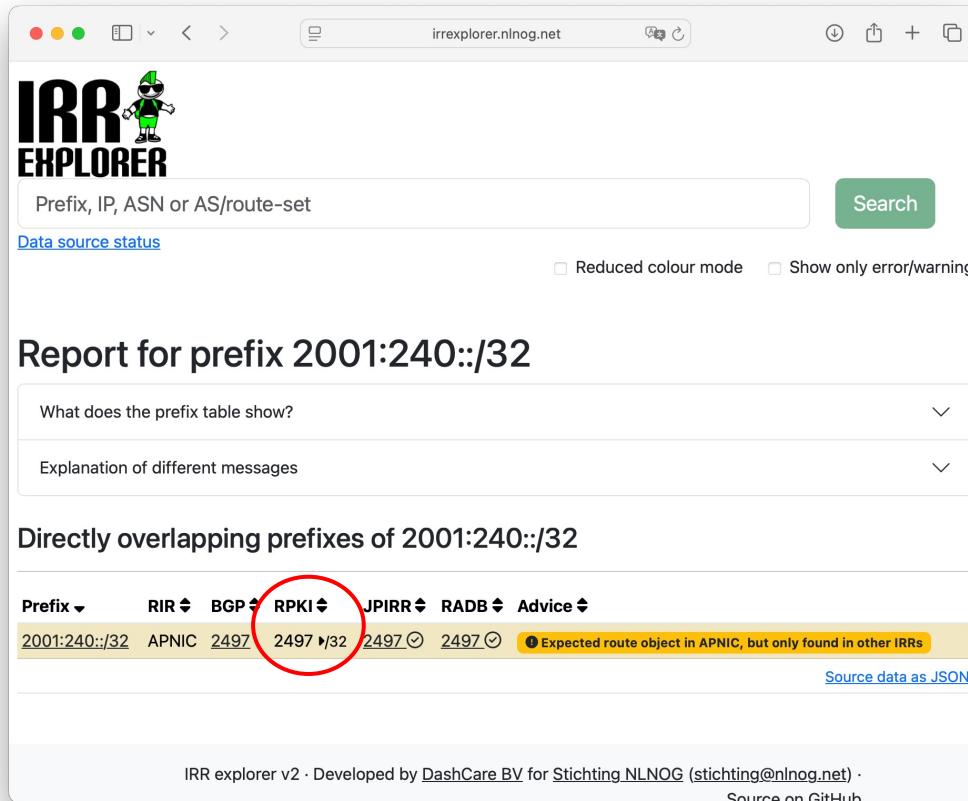
- ・「descr: Customer Prefix」と書いてあるもの多め
- ・メンテナのAS番号相当部分とorigin ASは異なる
- ・RADBは誰でもなんでも登録できる
 - ・一味が勝手に登録した可能性
 - ・上流ASがトランジットのために自動登録したかも

RPKI Origin Authorization (ROA)

- RPKIで、prefixの広報元ASとprefix長を示す電子証明書
 - 例: 2001:240::/32, AS2497, Max Length /32
- 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、受信した経路情報と比較して制御に使う
 - RPKI Origin Validation (ROV)
 - 広報元ASが違うとか、prefix長が違うとか

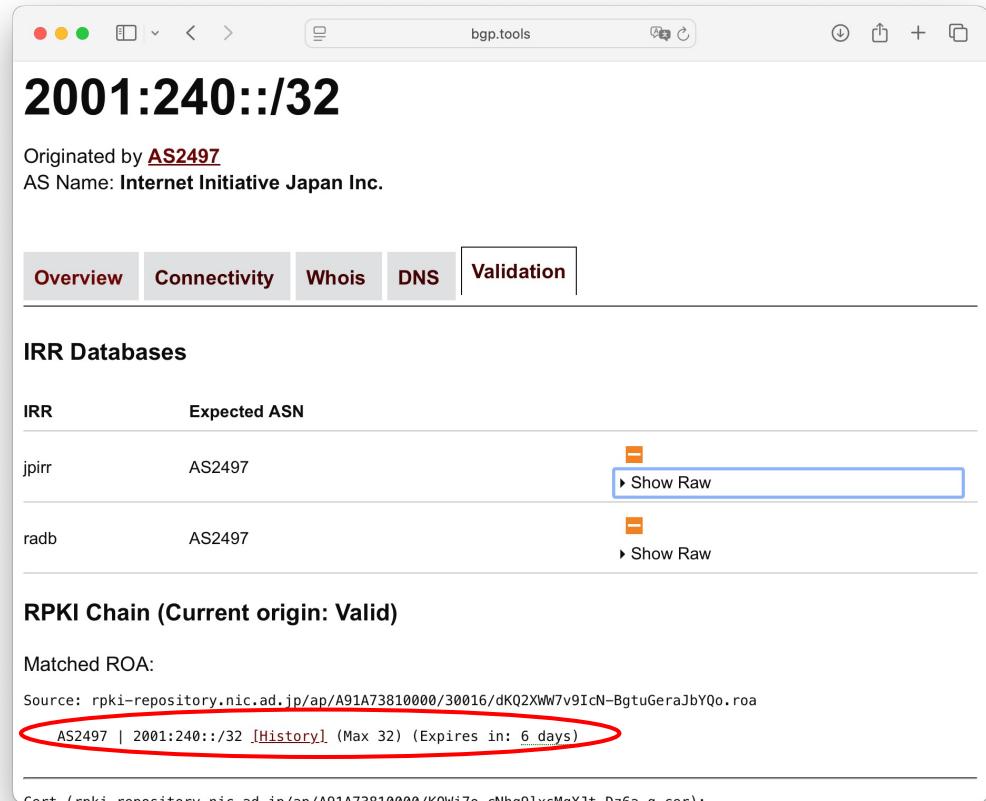
ROAやIRRの登録状況を見るツール

<https://irrexplorer.nlno.g.net/>



The screenshot shows the 'IRR EXPLORER' interface. At the top, there's a search bar with placeholder text 'Prefix, IP, ASN or AS/route-set' and a green 'Search' button. Below the search bar are two checkboxes: 'Reduced colour mode' and 'Show only error/warning'. The main section is titled 'Report for prefix 2001:240::/32'. It includes sections for 'What does the prefix table show?' and 'Explanation of different messages'. Under 'Directly overlapping prefixes of 2001:240::/32', there's a table with columns: Prefix, RIR, BGP, RPKI, JPIRR, RADB, and Advice. A row for '2001:240::/32' lists APNIC, 2497, 2497, 2497, 2497, and 2497. A note indicates 'Expected route object in APNIC, but only found in other IRRs'. At the bottom, it says 'IRR explorer v2 · Developed by DashCare BV for Stichting NLNOG (stichting@nlno.g.net) · Source on GitHub'.

<https://bgp.tools/>



The screenshot shows the 'bgp.tools' interface. The main title is '2001:240::/32'. It states 'Originated by AS2497' and 'AS Name: Internet Initiative Japan Inc.'. Below this are tabs for Overview, Connectivity, Whois, DNS, and Validation (which is selected). The 'IRR Databases' section shows entries for jpirr (AS2497) and radb (AS2497), each with a 'Show Raw' link. The 'RPKI Chain (Current origin: Valid)' section shows a table with columns: IRR, Expected ASN, and RPKI Chain. It lists 'jpirr' with 'AS2497' and a 'Show Raw' link. The 'Matched ROA' section shows a table with columns: Source, ROA, and History. It lists 'Source: rpkirepository.nic.ad.jp/ap/A91A73810000/30016/dKQ2XW7v9IcN-BgtuGeraJbYQo.roa' and 'AS2497 | 2001:240::/32 [History] (Max 32) (Expires in: 6 days)'. A note at the bottom says 'Cert (rpkirepository.nic.ad.jp/ap/A91A73810000/K0Wli7o-cNba01ycMaY1t-D762.a.cert)'.

資源ホルダに確認の上、ROA発行

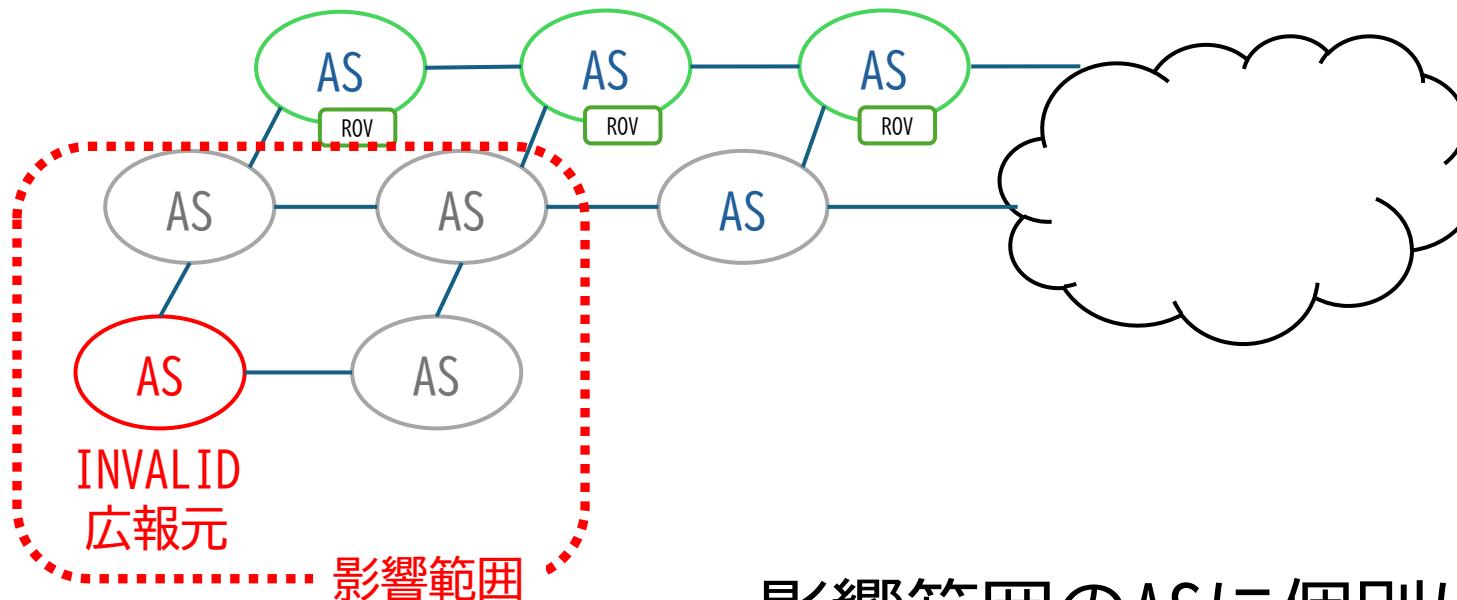
- 10.666.0.0/16、AS0、Max Length 16
 - インターネット上で広報されないとする、いわゆるAS0 ROA発行
- ほぼ瞬時に効果が出た！
 - RADBのrouteオブジェクト消失
 - RADBはROA INVALIDになるオブジェクトを応答しない（2023年実装）
 - インターネット上からほぼ全ての経路情報が消失
 - ROVで実質的なインターネット到達性が失われる

ハイジャック経路が残るところ

- ROVされてない広告Path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していない)
 - あるいはその上流と直接ピア (しかもROVしていない)
- 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
- ROVされてないところに要注意
 - ピアやカスタマーからの経路広報
 - INVALIDな経路がすり抜ける事がある