# RPKI状況

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

# サマリ

- みんな、RPKI ROA発行しよう
  - 導入コスト低い割にメリットがあるよ
- RPKI ROVの導入もよろしく
  - ただし、RPソフトウェアの更新を忘れずに

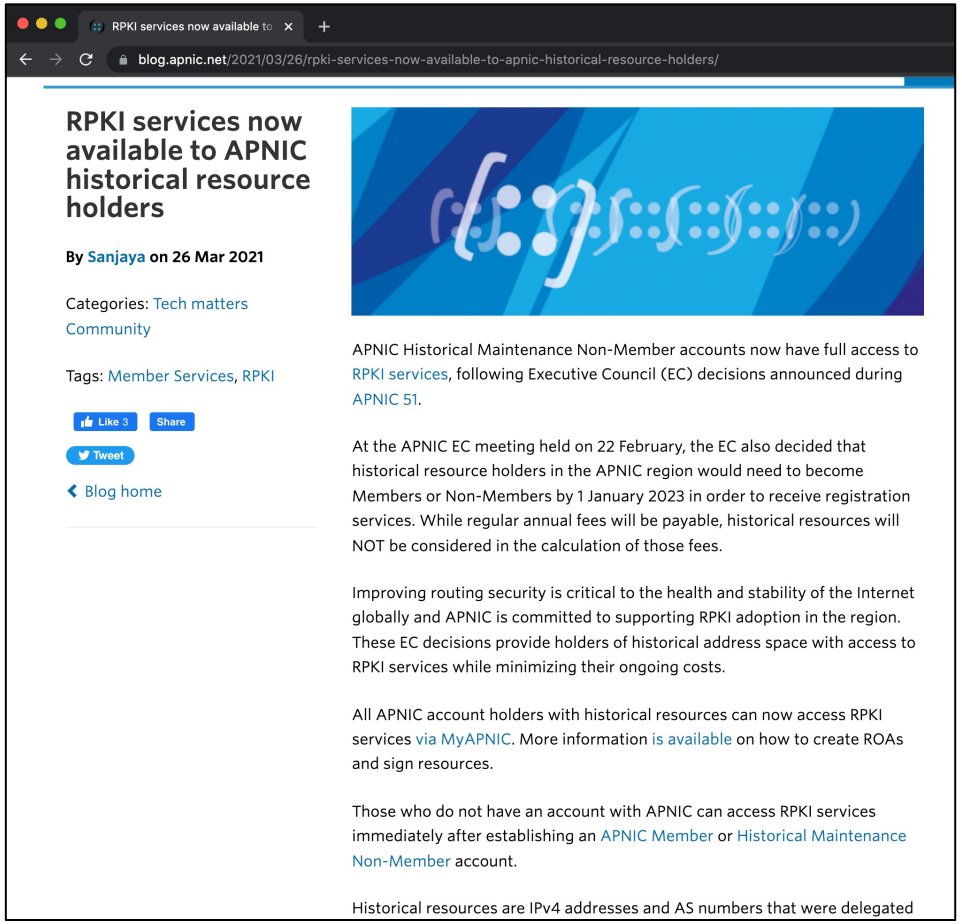
# Twitter事件 (2021/2/5)

- Twitter社の経路を他ASが広報
  - IPv4 /24の1経路を3時間程度
  - ミャンマーのCampana MYTHIC/AS136168が経路生成
    - 一部AS136168のピアがこれを受信
  - ミャンマー軍事政権からTwitterなどへの遮断命令が発出されてた

- 事件発生時にはROAは発行されておらず、IRR登録のみ
  - 今はTwitter関連のROAが発行されたみたい、よかったね

# APNICのRPKIサービスが対象拡大

- 歴史的番号資源保持者も利用可能に
- 歴史的番号資源とは:
  1. 現行の管理体制以前に委譲されたIPアドレスやAS番号で、
  2. “歴史的”状態を維持している番号資源


RPKI services now available to

blog.apnic.net/2021/03/26/rpki-services-now-available-to-apnic-historical-resource-holders/

RPKI services now available to APNIC historical resource holders

By Sanjaya on 26 Mar 2021

Categories: Tech matters
Community

Tags: Member Services, RPKI

Like 3 Share

Tweet

Blog home

APNIC Historical Maintenance Non-Member accounts now have full access to RPKI services, following Executive Council (EC) decisions announced during APNIC 51.

At the APNIC EC meeting held on 22 February, the EC also decided that historical resource holders in the APNIC region would need to become Members or Non-Members by 1 January 2023 in order to receive registration services. While regular annual fees will be payable, historical resources will NOT be considered in the calculation of those fees.

Improving routing security is critical to the health and stability of the Internet globally and APNIC is committed to supporting RPKI adoption in the region. These EC decisions provide holders of historical address space with access to RPKI services while minimizing their ongoing costs.

All APNIC account holders with historical resources can now access RPKI services via MyAPNIC. More information is available on how to create ROAs and sign resources.

Those who do not have an account with APNIC can access RPKI services immediately after establishing an APNIC Member or Historical Maintenance Non-Member account.

Historical resources are IPv4 addresses and AS numbers that were delegated

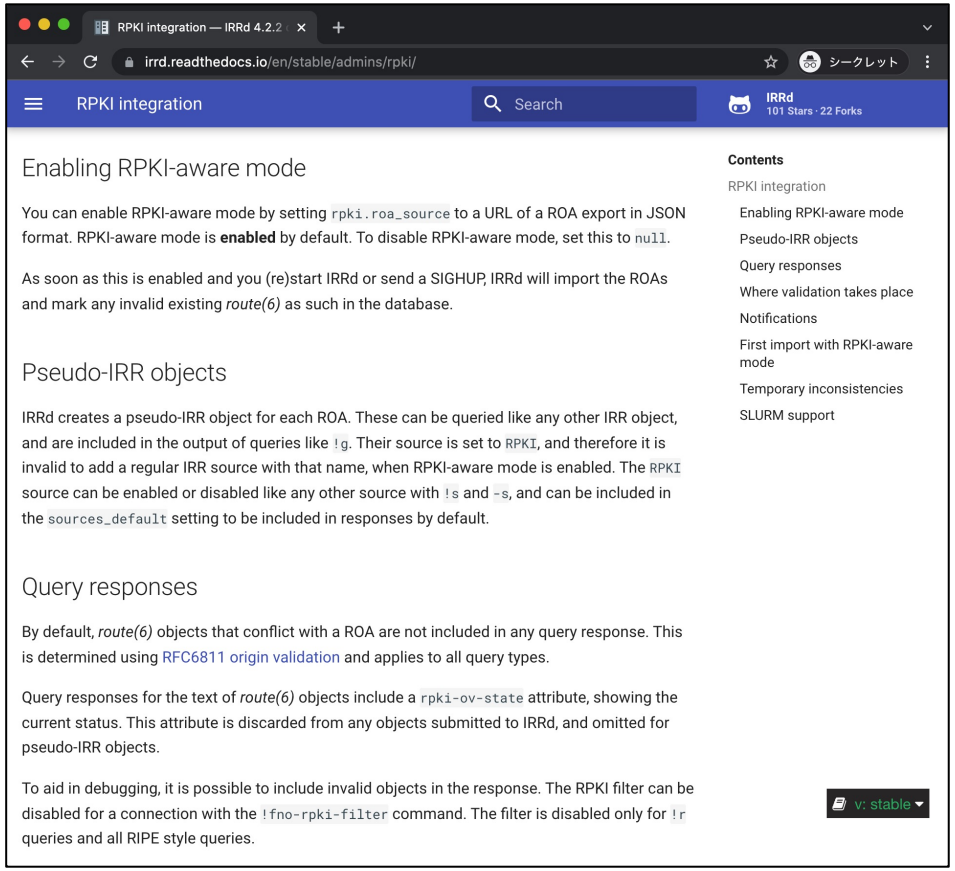
# APNICに登記情報が残っている歴史的番号資源保持者の方に

- 2023年1月1日までにアカウントの開設が必要です
  - 歴史的番号資源は費用計算には計上されません
  - 普通のAPNICメンバーになることも可能

- 手続きがあるので、早めの着手を
  - 正当性を示す各種文章の提出が求められるかも
  - 英語でやりとり

# RPKI ROAを作ると嬉しい

- ROAと矛盾するIRR登録が自動削除
  - IRRがRPKI-aware modeを有効にしている場合
  - 第三者がRADBとかに勝手にobjectを登録できなくなる
- ROAと矛盾する経路が伝搬しない
  - ROA Invalid経路を破棄している場合



# RPKIアプリケーション

- RPKIのリソース証明書で、他のファイルに電子署名
  - Resource Tagged Attestation (RPKI-RTA)
  - RPKI Signed Checklist (RPKI-RSC)
- RPKI-RTA
  - 一つのファイルに複数の署名が追加できる
- RPKI-RSC
  - 複数のチェックサムのリストに一つの署名が追加できる

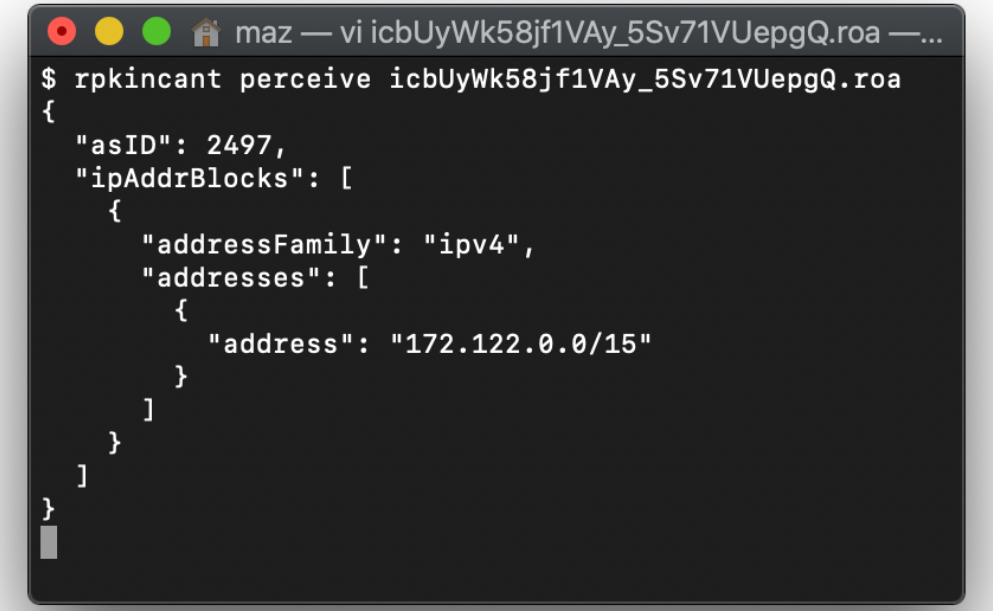
- 議論継続中
  - See also: The I in RPKI does not stand for Identity

# RFC9092
# Finding and Using Geofeed Data


192.0.2.0/24,US,WA,Seattle,

- Geofeed(RFC8805)
  - ip_prefix,alpha2code,region,city,postal_code
- 例えばGoogleのGeofeed事例
  - https://www.gstatic.com/geofeed/corp_external
- これにRPKIの電子証明書で署名して正当性を担保

# rpkimancer / rpkincant



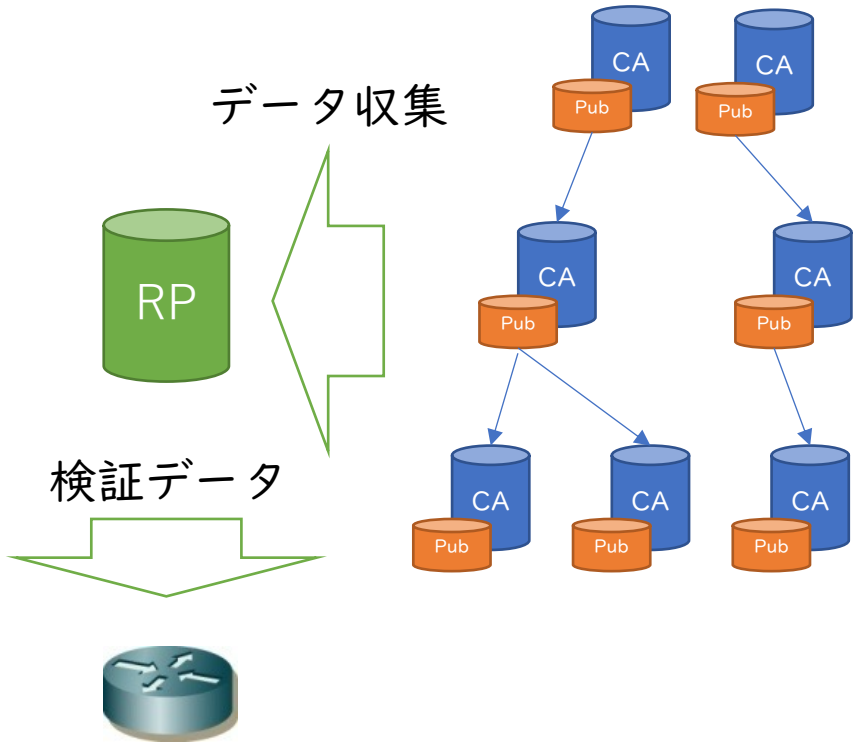

- RPKI署名オブジェクトの作成、閲覧ツール
  - https://github.com/benmaddison/rpkimancer
  - Python3.8 or later
- $ rpkicant perceive <file>
  - Manifests (RFC6486)
  - ROAs (RFC6482)
  - Ghostbuster Records (RFC6493)

print_roa以外でもROAを表示するツールが出てきた

# RPKIキャッシュ(RP)運用の注意点

- RPはRPKIオブジェクトを定期的に収集
  - TALを起点にPubサーバを辿る
- RPは検証後のROAをルータに送信
  - ルータが受信経路との比較に用いる

- 疑問
  - 公開データの一貫性？
  - 悪意のあるCAがいたら？



# 公開(Publication)サーバの運用

- 版がある
  - CAが公開する一式の電子証明書や署名済みデータのファイル群
  - RPKI manifestにファイルのリストが掲載
- 署名済みデータは個別のファイル
  - 例えば、ROAはそれぞれ一つのファイルになってる

  → ファイルがいっぱいある

- 公開サーバでのデータ更新には注意が必要

# 公開(Publication)サーバの注意点

- データに一貫性を持たせる
- rsyncサーバ側はatomicな切り替え大事
  - module pathをsymbolic linkを用いて切り替えるなど
- RRDPサーバ側でも一貫性大事
  - 負荷分散装置を使って複数サーバで運用している場合など
  - RRDPでは複数のHTTPセッションを通じてデータを取得
    - その結果が一貫性あるデータでないと困る
- RP側はなるべくRRDP使う

https://www.ripe.net/ripe/mail/archives/routing-wg/2021-April/004297.html
https://datatracker.ietf.org/doc/draft-ietf-sidrops-prefer-rrdp/

# 悪意のあるCA問題

- 番号資源保持者であれば、認証局(CA)になれる
  - TLSサーバ証明書と異なり、範囲は委譲された番号資源に限る
- 悪意あるデータがあるかもしれない
  - 無駄に大量のデータ
  - 無駄に膨大な信頼の連鎖
  - 無駄に長いファイル名
  - 異常なデータ
- いくつかのシナリオは調査済み
  - RPRPなどの活動
  - 調査結果を元に、各RP実装は修正版を公開

https://labs.ripe.net/author/koen-van-hove/improving-the-resiliency-of-rpki-relying-party-software/

# サマリ

- みんな、RPKI ROA発行しよう
  - 導入コスト低い割にメリットがあるよ
- RPKI ROVの導入もよろしく
  - ただし、RPソフトウェアの更新を忘れずに