

RPKI状況

Matsuzaki 'maz' Yoshinobu

<maz@ij.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

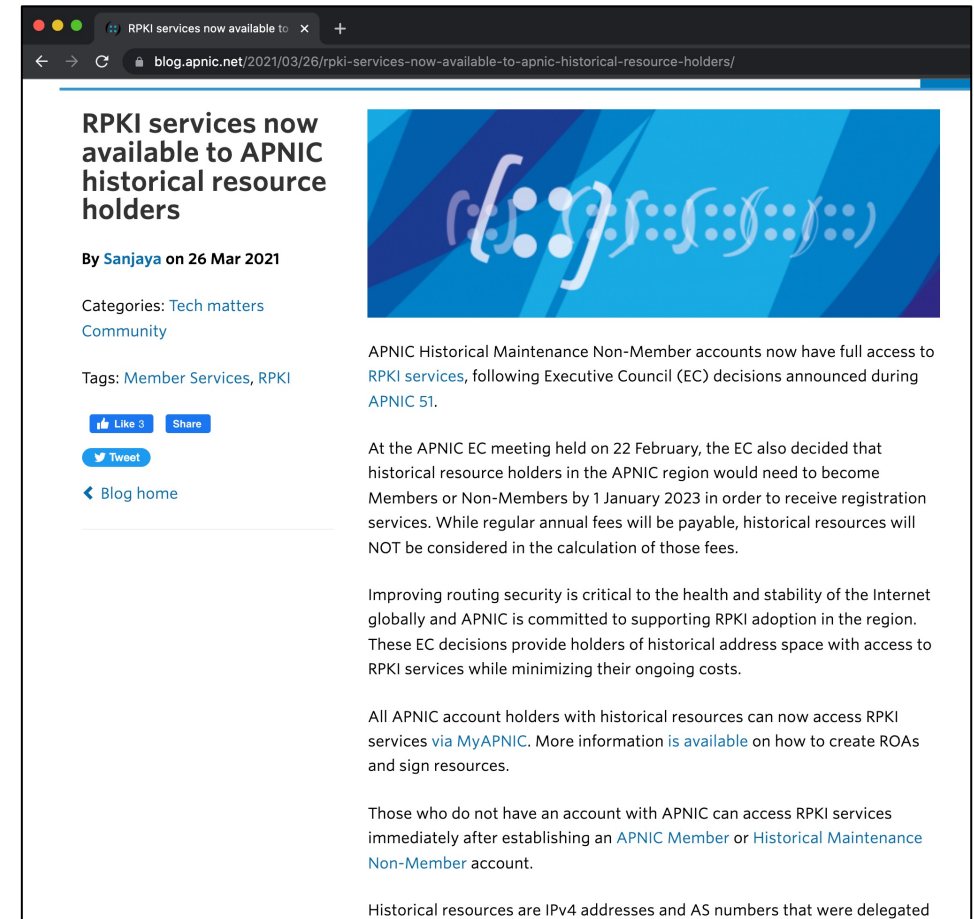
- ただし、RPソフトウェアの更新を忘れずに

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

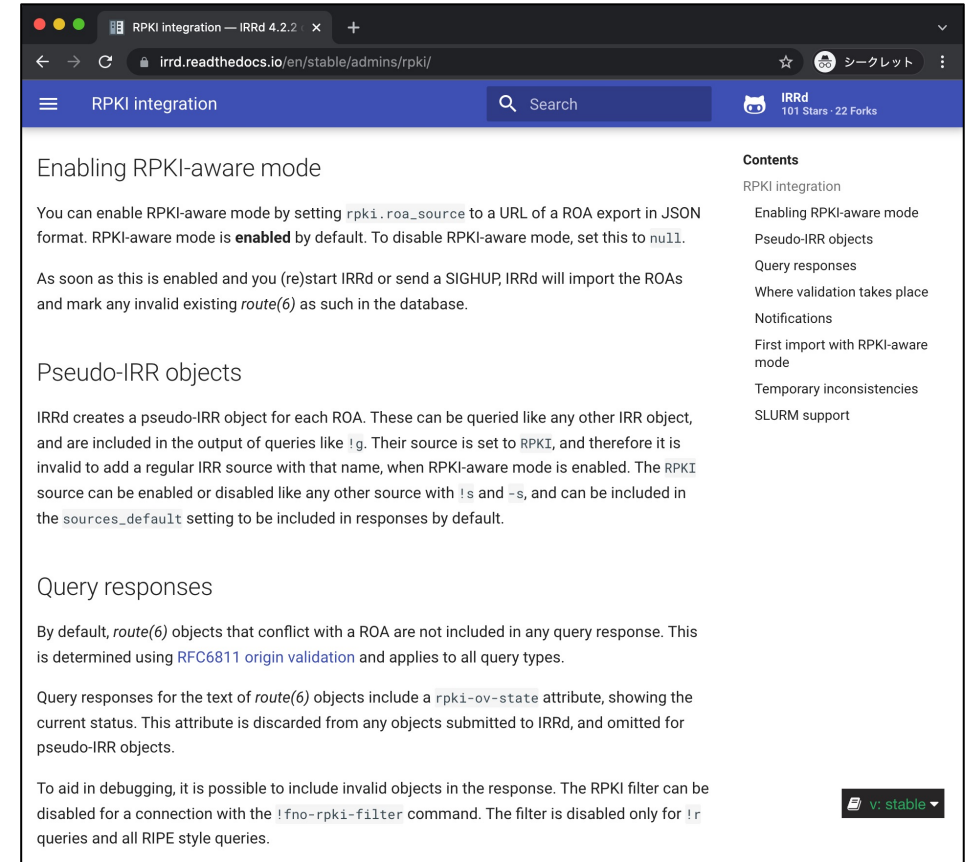


APNICに登記情報が残っている 歴史的番号資源保持者の方に

- 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一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

```
maz — vi MIIEpTCCA42gAwIBAgIUJ605QIPX8rW5m4Zwx3WyuW7hZu...
# RPKI Signature: 192.0.2.0 - 192.0.2.255
# MIIGjwYKoZiHvcNAQcCoIIGgDCCBnwCAQMxDLbG1ghkgBZQMEAgEwDQYLKoZ
# IhveNAQKQAS+gggSpMIIEpTCCA42gAwIBAgIUJ605QIPX8rW5m4Zwx3WyuW7hZu
# QwDQYJKoZiHvcNAQELBQAwMzExMC8GA1UEAxM0FDRTJDRUY0RkIyMUI3RDExR
# TNFMTg0RUZDMUyOTdCMzc3ODY0MjAeFw0yMTA1MjAxNjA1NDVaFw0yMjAzMTYx
# NjA1NDVaMDMxMTAvBgNVBAMTKDkxNDY1MkEzQkQ1MUMxNDQyNjAxOTg0ODIUNUM
# 0NUFQRjA1M0ExODcwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIABAQCycT
# Qr0b/qB2W3i3Ki8PhA/DEWyii2TgGo9pgCw091sIRI6Zb/k+aSiwWP9kScz1cQg
# tPCVwr62hTQZCIowBN0BL0cK0/5k1imJdi5qdM3nvKswM8CnoR11vB8pFwruZm
# r5xphXRvE+mzuJVLgu2V1upmBXuWloeymudh6WwJ+6DjwPX03RiXBejBr0FNXha
# Fle08y4DPfr/S/tXJ0Bm7QzQptmbPLYtGfprYu451iFFqP94UeLpISfXdd36AKG
# zqTFcc3EW915UFE1MFLInoEogqtoLoKABt0IKOFgKeC/EgeaBdWLe469ddC9rQ
# ft5w6g6cmxG+aYDdIEB34zrAgMBAAQjggGvMIIBqzAdBgNVHQ4EFgQUKUZSo71R
# wUQmZiIn1xFq/BToYcwHwDVR0jBBgwFoAU0s4s70+yG30R4+GE78Hi17N3hKI
# wDAYDVR0TAQH/BAIwADA0BgNVHQ8BAf8EBAMCB4AwGAYDVR0gAQH/BA4wDDAKBg
# grBgEFBQc0AjbHhBGNVHR8EwJBYMFagYKBSh1Byc3luYzovL3Jwa2kuZXhhbXBsZ
# S5uzXzc4NjQyLmNybDBsBgggrBgEFBQcBAQRGMF4wXAYIKwYBBQUHMAKGUHUJzeW5
# j0i8vcbBraS51eGFtcGx1Lm51dC9yZXBvc210b3J5LzNBQ0UyQ0VGNzCMjFCN0
# QxMUUzRTE4NEVGGzFFmjk3QjM3Nzg2NDIuY2VyYmBkGCSsGAQUFBwEHAQH/BAowC
# DAGBAIAAQUAMEUGCCsGAQUFBwELBDkwNzA1BgggrBgEFBQcwDYpaHR0cHM6Ly9y
# cmRwLmV4YW1wbGUubmV0L25vdG1maWNhdG1vb154bWwDQYJKoZiHvcNAQELBQAw
# DggEBAEjC98gVp0Mb7uiKaHyLp0453mtJ+AKN07fsK/qGw/e90DJv7cp1hvjj4u
# y3sgf7PQ7cKNGrGybyq/1E0jce+ARGVjbi2BzrZSwANB846Snwsktw6cenaif6A
# ww6q00NspAepMBd2Vg/9sKFvOwJFV0gNcqiQIXP5rGJPWbc0Mv52a/7adjfXwpn
# OijjIT0gMl0QGmC2TPZpydZKjlxEATdFEQssa33x3Dn1pp+/r9xuNVYTRcC36owR
# aVA3jzN6F6rDE8r8xs3y1ISVz6JeCQ4YRYwbMsjjc/tiJLM7ZYxTe5IrYz1ZtN6
# n/SEssJASwRIgps2EhCt/HS2xAmGCOhgUxggGqMIIBppIBA4AUkUZSo71RwUQmA
# ZiIn1xFq/BToYcwCwYJZiIAWUBAIBoGswGgYJKoZiHvcNAQKDMQ0GcyqGSIB3
# DQEIEAevMBwGCSqGSIb3DQEJBTFFw0yMTA1MjAxNjA1NDVaFw0yMjAzMTYx
# jBDEiBCAr4vKeUvHJINsE0YQwUmoo48qrOU+iPuFbQRqX3BFjANBgkqhkiG9w
# 0BAQEFAASCAQB85HsCBru3EcVocf4nC6Z3jz0Jt+fVlyTDAObF6GTNwgxe7jSA
# Inyf51UzIGahVY3sQiiXbdWcVYtPb4118KvyeXh8A/HLp4eeAJnt19D3igt38M
# o84q5pf9pTQXx3hbsm511lp0ip/TKVMqzE42s60Pox3M0+6eKH3/vBKnw1s1ayM
# 0MunPDTBFZL3JJEGPWFIZHEcrypevbqR7Jjsz5vp0qyF2D9v+w+nyh20PmuePm7
# YqL0w/E99PVBs9uI+hmbiCz/BK2Z3VRjrr1rUU+49e1dSTKZ2sJyhCbbV2Ufgi
# S2F0qAgJzjilyN3BDQLV8Rp9cGh0PpV1KH2na
# End Signature: 192.0.2.0 - 192.0.2.255
```

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

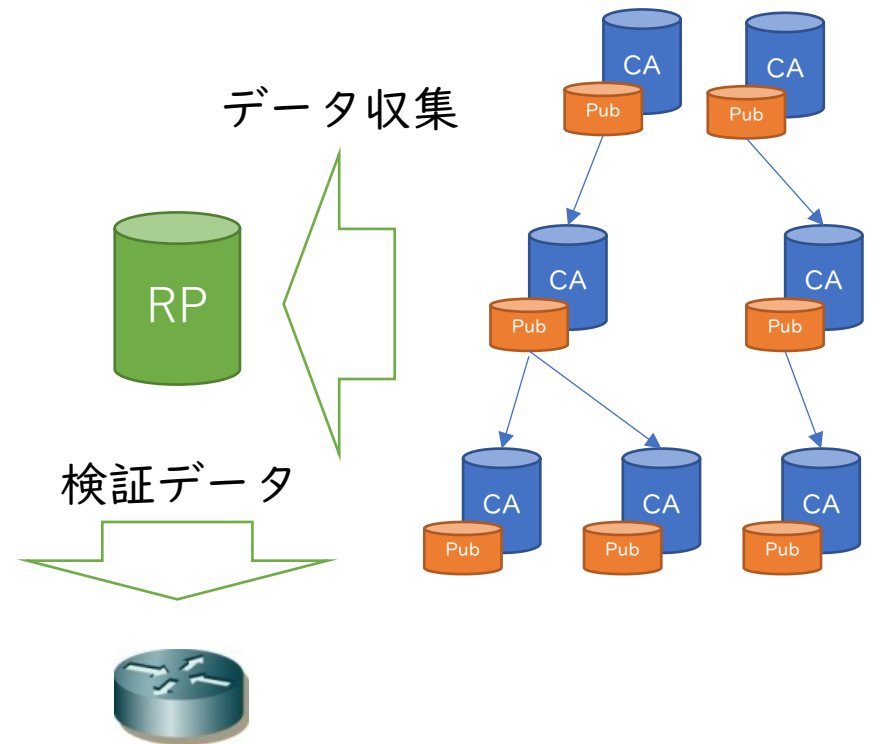
```
maz — vi icbUyWk58jf1VAy_5Sv71VUepgQ.roa —...
$ rpkincant perceive icbUyWk58jf1VAy_5Sv71VUepgQ.roa
{
  "asID": 2497,
  "ipAddrBlocks": [
    {
      "addressFamily": "ipv4",
      "addresses": [
        {
          "address": "172.122.0.0/15"
        }
      ]
    }
  ]
}
```

- 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
- \$ rpkincant 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