IXP’s challenges to RPKI: the JPNAP approach

Yohei Nishimura
Katsuyasu Toyama,
JPNAP

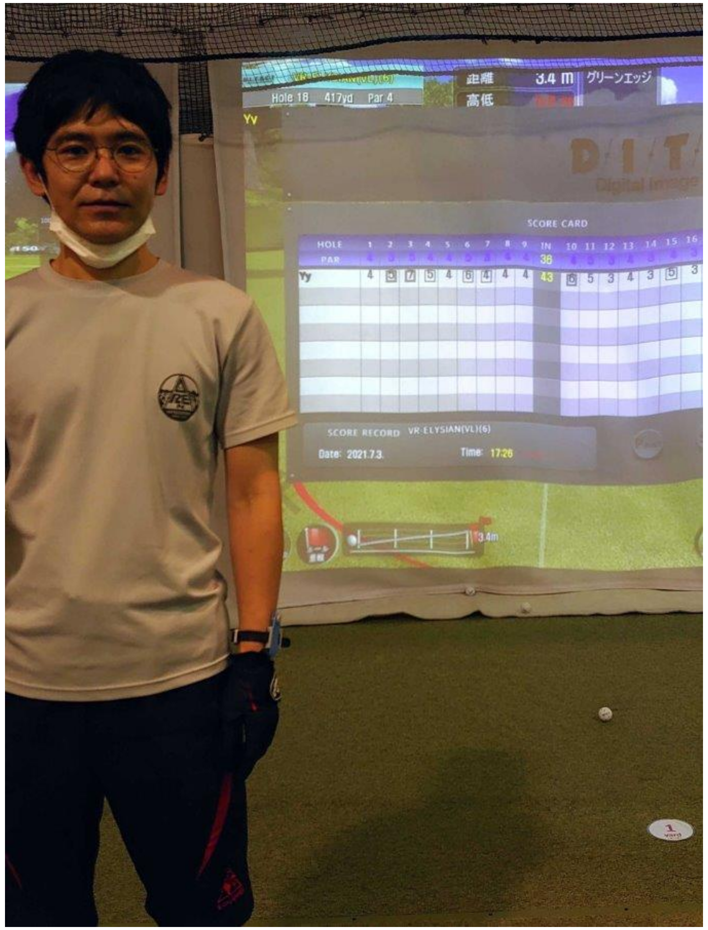
About your Speaker

Yohei Nishimura

- Senior Network Engineer
- JPNAP employee since 2022
- 15+ years in ISP/IXP industry

How I spend my free time:

- Traveling
- Riding a bicycle
- Playing Golf



About your Speaker

Katsuyasu Toyama

- **JPNAP** (2001, 2007-2012, 2015-)
  - COO, Representative Director, and EVP
- Asia Pacific Internet Exchange (**APIX**) association
  - Chairperson (2010-2017, 2019-)
- **Peering Asia**
  - Peering Asia WG member (2017-)
- NTT Communications
  - SVP of Internet and Mobile Services (2012-2015)
  - AS2914(GIN), AS4713(OCN)

from JANOG52 official photos

About JPNAP

- Providing nationwide Internet Exchange services in Japan (2001-)

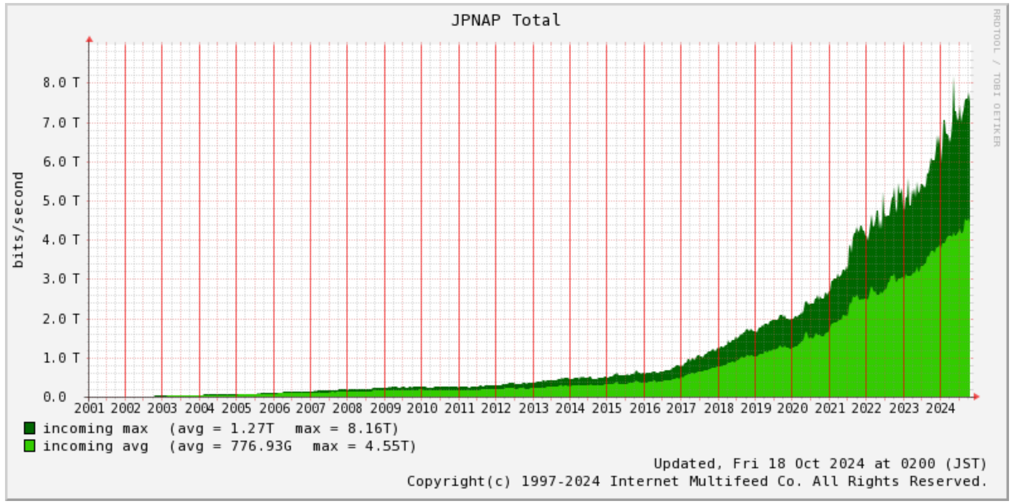
- 275 ASes (2024 Oct)

- Available in 5 cities:

  - Tokyo, Osaka, Fukuoka, Sendai and Sapporo

- Voluntary Services:

  - Public NTP Service (2005-)
  - Support F/I/K/M-ROOT DNS
  - Public RPKI Validators (2014-)



```
🟩 incoming max   (avg = 1.27T    max = 8.16T)
🟩 incoming avg   (avg = 776.93G   max = 4.55T)
                                    Updated, Fri 18 Oct 2024 at 0200 (JST)
                 Copyright(c) 1997-2024 Internet Multifeed Co. All Rights Reserved.
```

Introduction

- IXPs have many connections with internet operators across regions, regardless of their industry, size and nature.
- Then IXPs are expected to be key pillars in Internet infrastructure, especially in routing security.
- JPNAP would like to share the experiences, challenges and struggles on routing security, as one of the many IXPs working on it.

Routing Security as IXPs Key Responsibility

“IXPs Action” by MANRS:

1. **Filtering**. Implement filtering of route announcements at the Route Server based on routing information data (IRR and/or RPKI).
2. **Promotion**. Provide encouragement or assistance for IXP members to implement MANRS actions.
3. **Protect the peering platform**. Have a published policy of traffic not allowed on the peering fabric and perform filtering of such traffic.
4. **Coordination**. Facilitate communication among members by providing necessary mailing lists and member directories.
5. **Tools**. Provide monitoring and debugging tools to IXP members

https://manrs.org/ixps/

Secure yourself, and secure them as well

IRR as the basic security

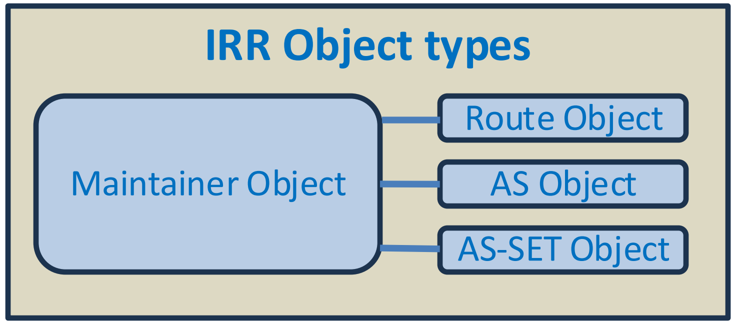
IRR as the basic security (early 2000s-)

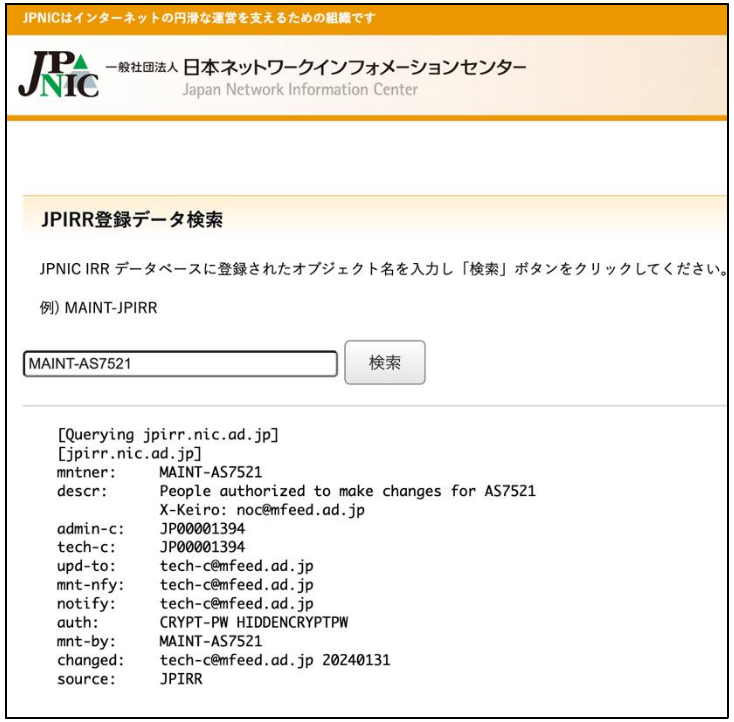
- **IRR (Internet Routing Registry) is a database that stores routing information as well as information about route priorities.**

- Gained attention in protecting routing security in early 2000s.

- In Japan, **JPIRR was launched in 2002** as an alternative to RADb by JPNIC, collaborating with JPNAP.

- **JPNAP starts IRR mirroring service(2003).**


IRR Object types


JPNICはインターネットの円滑な運営を支えるための組織です

一般社団法人 日本ネットワークインフォメーションセンター
Japan Network Information Center

JPIRR登録データ検索

JPNIC IRR データベースに登録されたオブジェクト名を入力し「検索」ボタンをクリックしてください。

例) MAINT-JPIRR

MAINT-AS7521

```
[Querying jpirr.nic.ad.jp]
[jpirr.nic.ad.jp]
mntner:     MAINT-AS7521
descr:      People authorized to make changes for AS7521
            X-Keiro: noc@mfeed.ad.jp
admin-c:    JP00001394
tech-c:     JP00001394
upd-to:     tech-c@mfeed.ad.jp
mnt-nfy:    tech-c@mfeed.ad.jp
notify:     tech-c@mfeed.ad.jp
auth:       CRYPT-PW HIDDENCRYPTPW
mnt-by:     MAINT-AS7521
changed:    tech-c@mfeed.ad.jp 20240131
source:     JPIRR
```

IRR as the basic security (early 2000s-)

Keiro-Bugyo (2008-)

- means “Route-Inspector”.
  (“Bugyo” comes from the officer name in the samurai era.)

- Validate of BGP routes from JPIRR member according to the JPIRR Route Objects.

- If it finds a BGP route that does not match the IRR route object, notifies the object owners.

- **JPNAP has supported in its building phase and is providing “Keiro-Bugyo” servers.**

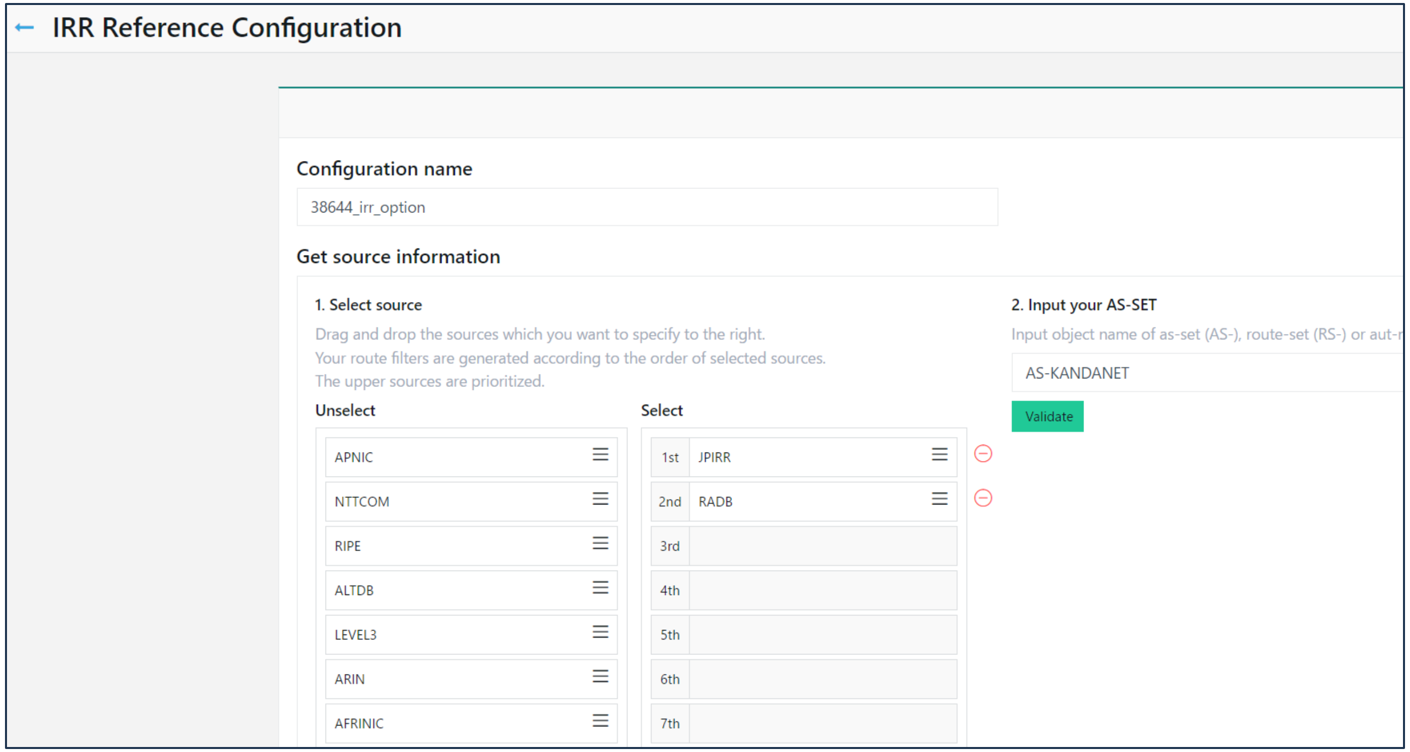
JPIRR Route Object example:

```
|route:     192.0.2.0/24
|descr:     EXAMPLENET
|           Example network
|           Example address
|           JAPAN
|           X-Keiro: example@nic.example   <--
Email address to be notified when a violation
occurs
|origin:    AS64496
|admin-c:   Example admin person
|tech-c:    Example tech person
|notify:    example@nic.example
|mnt-by:    MAINT-AS64496
|changed:   example@nic.example 20180215
|source:    JPIRR
```

IRR as the basic security (early 2000s-)

JPNAP Route servers have deployed the IRR Filter from the beginning (2011-)

- Automatically generate filters from pre-selected IRR sources.
- Use RADb as query source and bgpq4 as query engine.



← IRR Reference Configuration

Configuration name

38644_irr_option

Get source information

1. Select source

Drag and drop the sources which you want to specify to the right.
Your route filters are generated according to the order of selected sources.
The upper sources are prioritized.

Unselect	Select	
APNIC	1st	JPIRR
NTTCOM	2nd	RADB
RIPE	3rd	
ALTDB	4th	
LEVEL3	5th	
ARIN	6th	
AFRINIC	7th	

2. Input your AS-SET

Input object name of as-set (AS-), route-set (RS-) or aut-r

AS-KANDANET

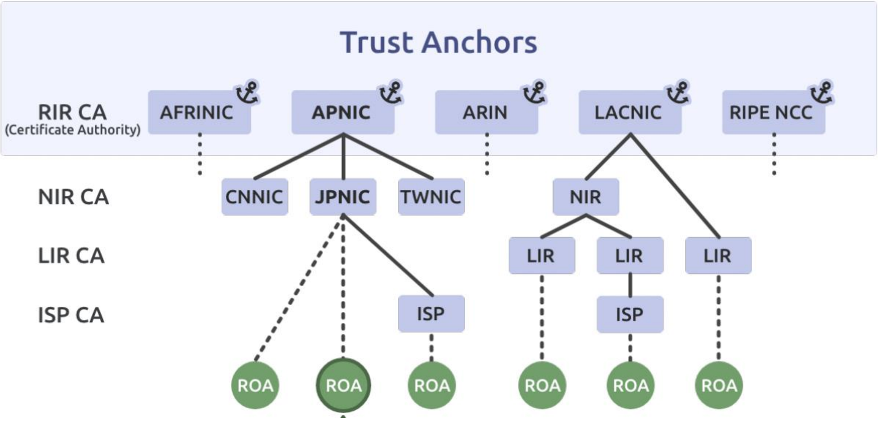
Deploy RPKI into IXP

RPKI Recap.

- **RPKI (Resource Public Key Infrastructure)** is a public key infrastructure that uses digital signatures to prove the assignment of Internet address resources (IP addresses and AS numbers).

- RPKI forms a tree structure with RIR as the top Trust Anchor and TA provides their Trust Anchor Locator (TAL) that contains URL of the RIR Repository and Public Key of the Root Certificate.

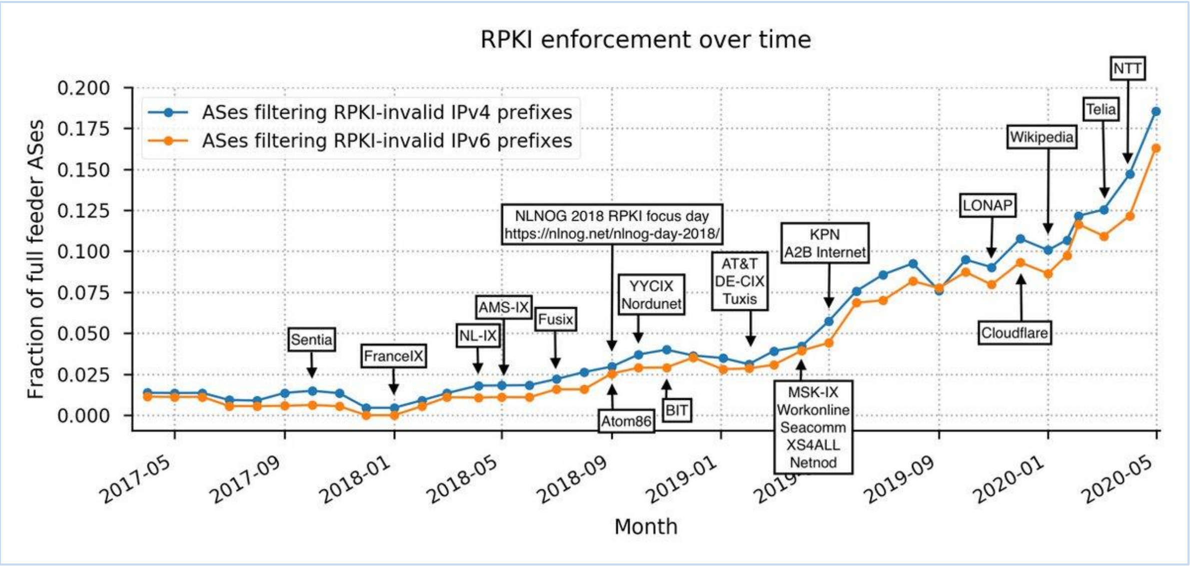
- ROA（Route Origin Authorization） is positioned at the bottom of the tree and used for ROV (Route Origin Validation)



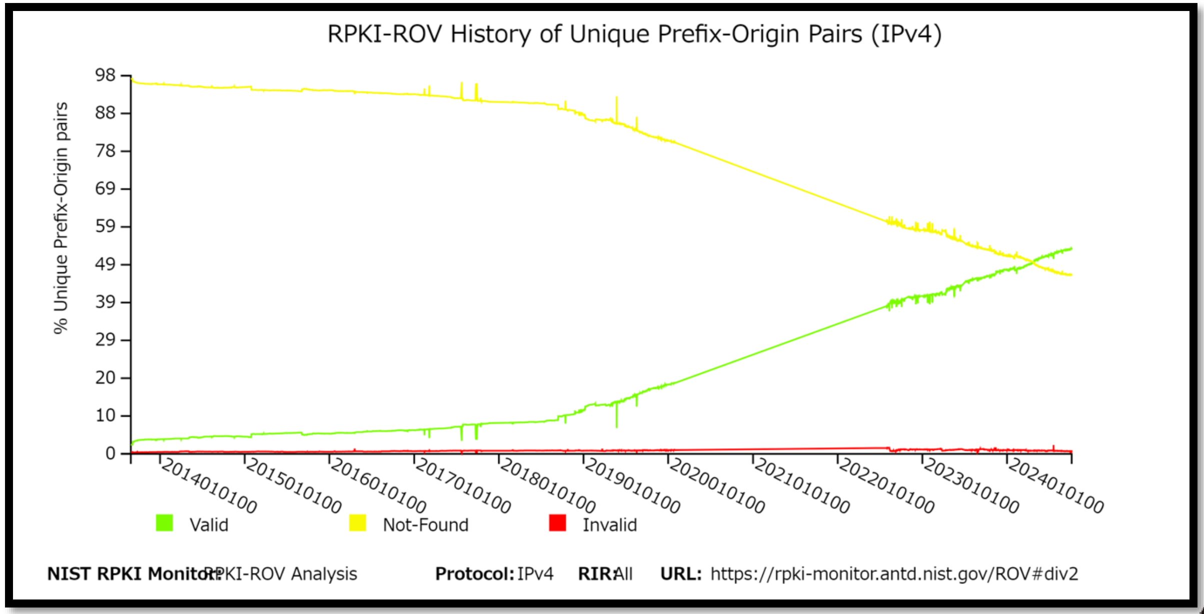
The rise of ROV (Late 2010s)

- ROV gained widespread attention and adoption by IXPs and network operators.
  e.g. Google and AWS announced 99% of its owned IP space in ROA and plans to implement ROV.

- APIX members deployment:
  - BKNIX(2019 Mar)
  - HKIX(2020 Aug)
  - IX Australia(2020 Sep)
  - JPNAP(2020 Nov)

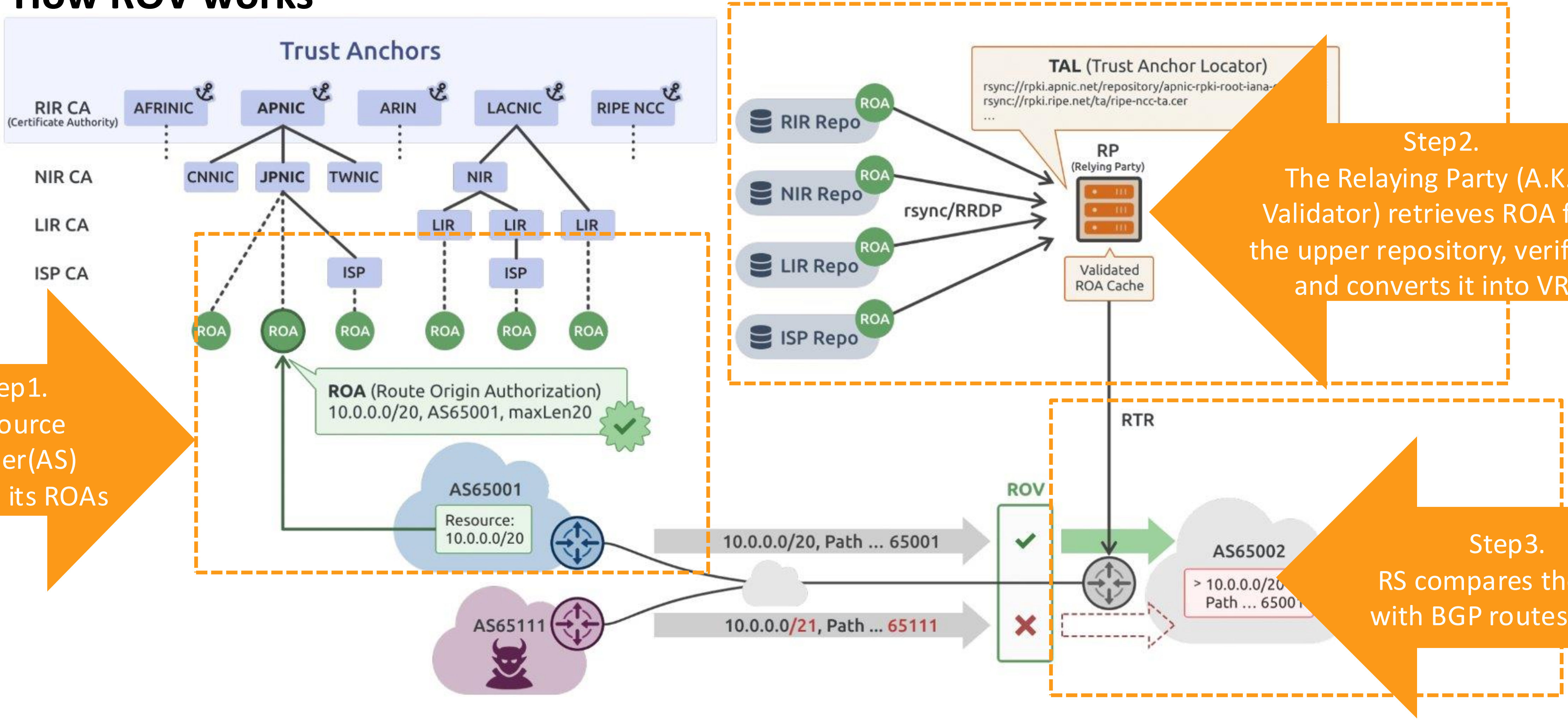


https://x.com/JobSnijders/status/1256326712347881473



JPNAP Route servers have deployed the ROV (2020 Nov-)

How ROV works



Step1.
Resource Holder(AS) creates its ROAs

Step2.
The Relaying Party (A.K.A. Validator) retrieves ROA from the upper repository, verifies it, and converts it into VRP.

Step3.
RS compares the VRP with BGP routes (ROV)

Design Considerations : ROV policy on route servers

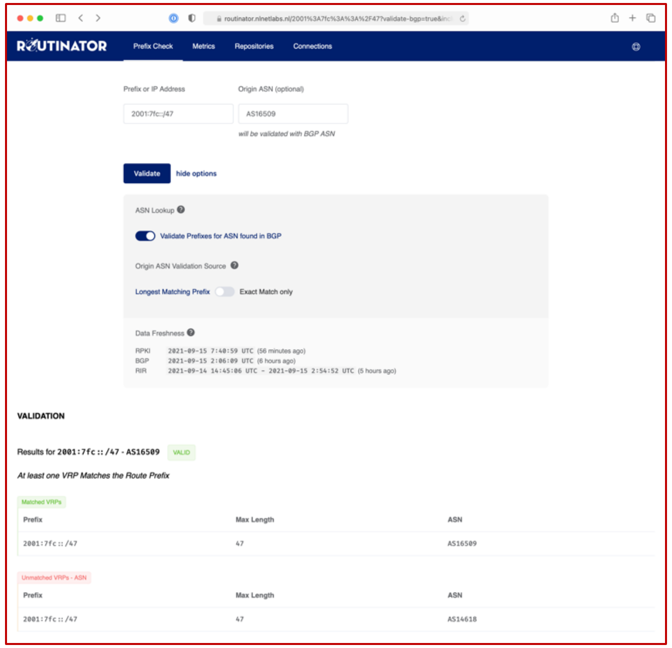
- ROV was not matured : ROA registration rate was below 20% (Late 2010s)
- A Question: **Should dropping invalid routes be mandatory or optional?**
- We asked for comments from the APNIC community.
  Strategy for deploying RPKI ROV to Route Server on IX(APNIC48)
  Got positive feedback on **rejecting invalid routes**:
  - "avoid complex policies for customers."
  - "acceptable to reject invalid routes."

Conclusion:
Valid, NotFound → accept, Invalid → drop

Design Considerations : Relaying Party (A.K.A RPKI Validator)

Routinator3000

- Single binary with built-in RTR server
- Provides Web API/GUI
- Built-in exporter compatible with Grafana integration
- **Active ongoing development**
  - Follows the latest RFCs
  - Quick response to issues



Prefix or IP Address: 2001:7fc::/47

Origin ASN (optional): AS16509

will be validated with BGP ASN

ASN Lookup

Validate Prefixes for ASN found in BGP

Origin ASN Validation Source

Longest Matching Prefix / Exact Match only

Data Freshness

```
RPKI   2021-09-15 7:40:59 UTC (56 minutes ago)
BGP    2021-09-15 2:06:09 UTC (6 hours ago)
RIR    2021-09-14 14:45:06 UTC - 2021-09-15 2:54:52 UTC (5 hours ago)
```

VALIDATION

Results for 2001:7fc::/47 - AS16509 VALID

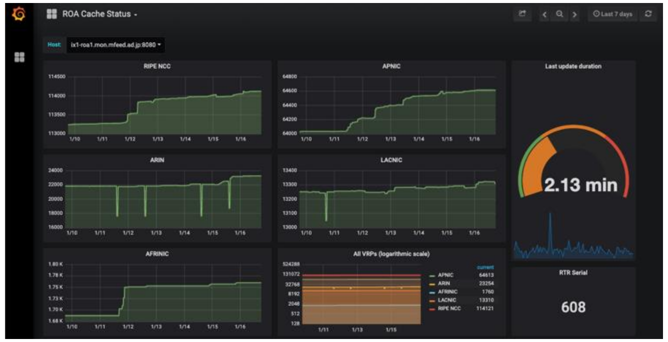
At least one VRP Matches the Route Prefix

Matched VRPs

Prefix	Max Length	ASN
2001:7fc::/47	47	AS16509

Unmatched VRPs - ASN

Prefix	Max Length	ASN
2001:7fc::/47	47	AS14618

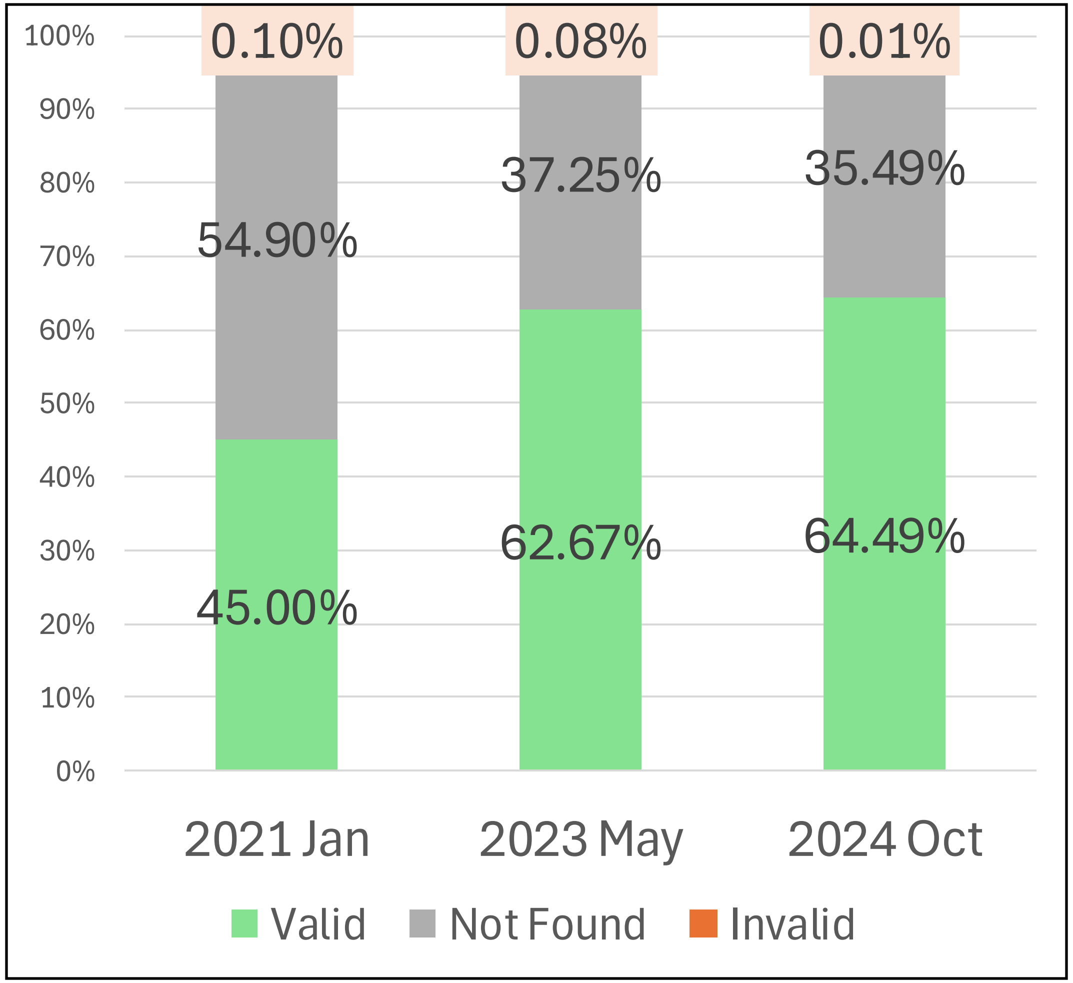


ROA Cache Status

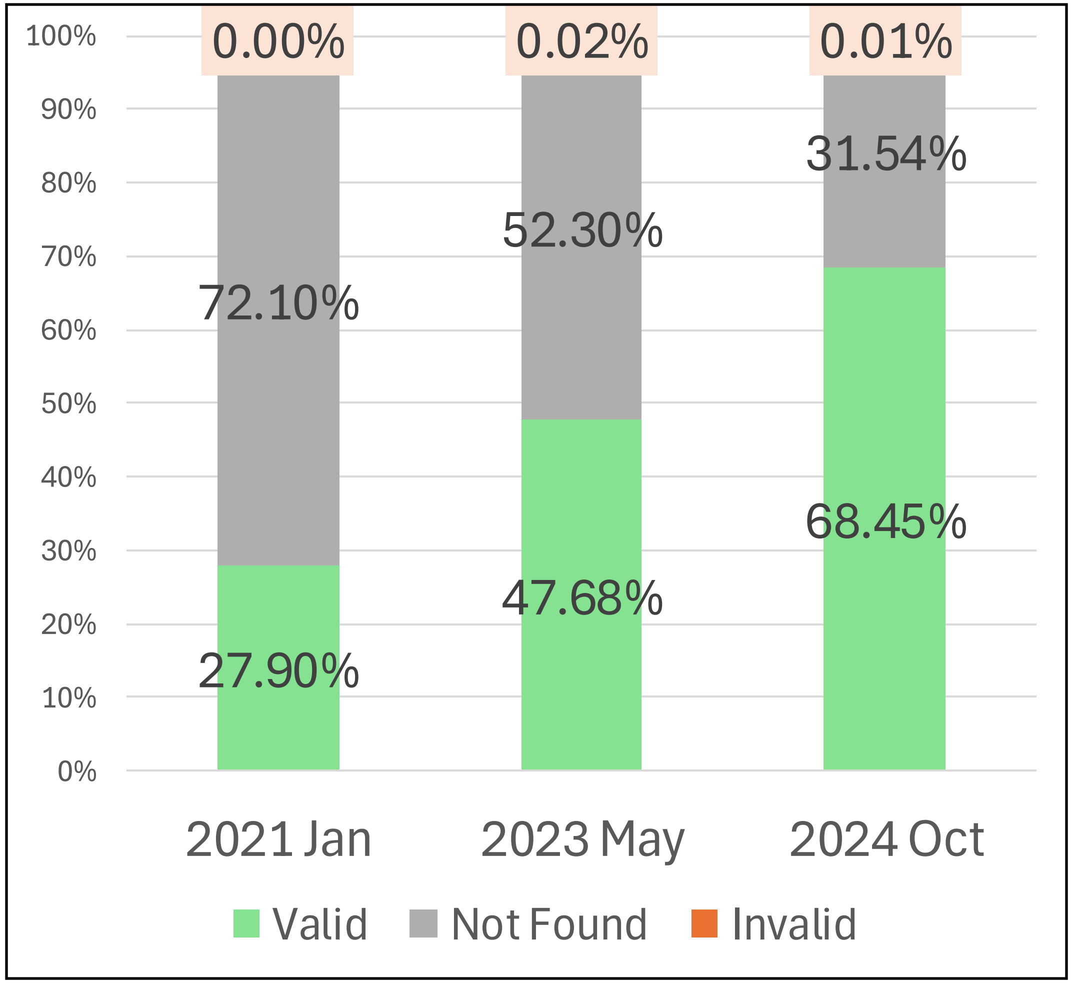
Host: ix1-roa1.mon.mfeed.ad.jp:8080

ROV Analysis on JPNAP Tokyo

IPv4



IPv6

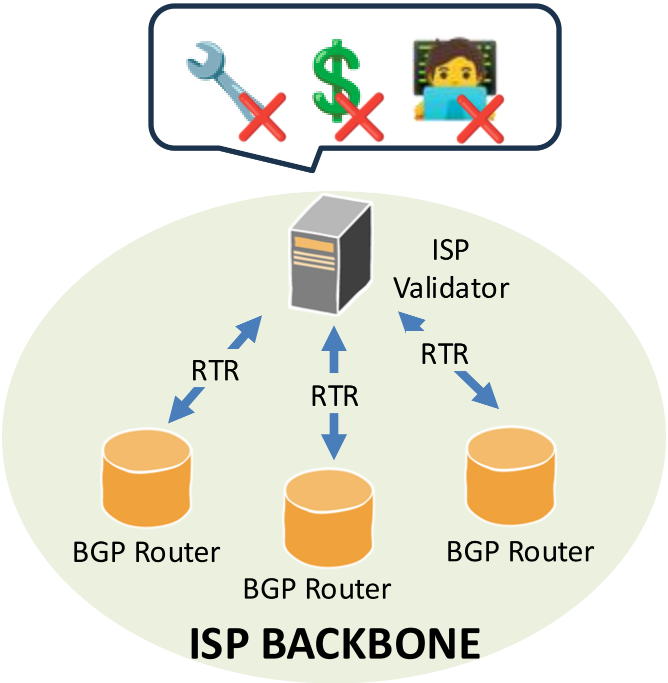


Support IXP members to deploy RPKI

Validator : the challenge in deploying ROV

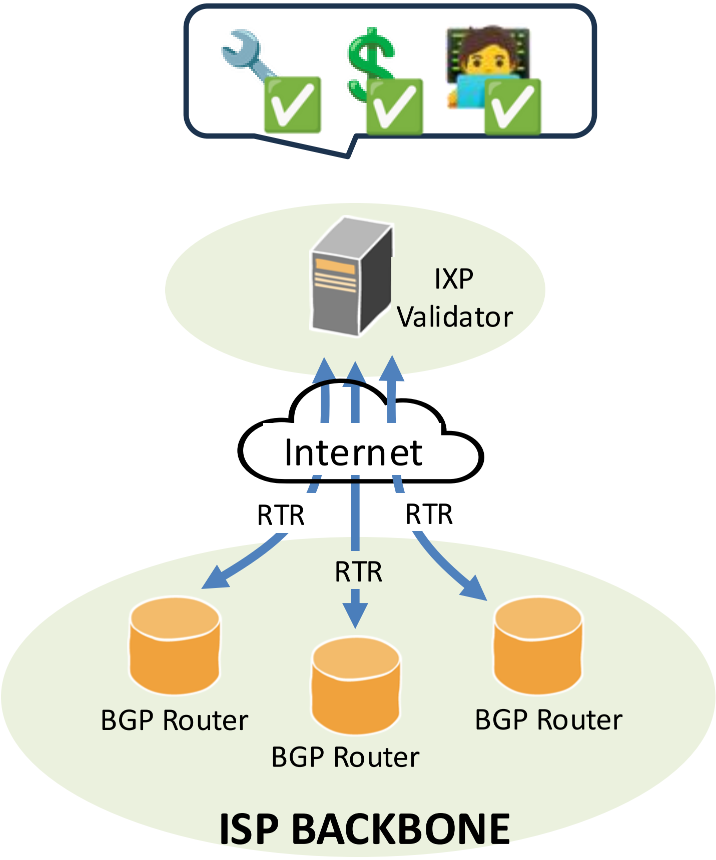
- RPKI ROV Standard assumes an internal validator within each AS.

- This could be an obstacle to proceed ROV, especially for small ISPs:
  - Covering equipment costs
  - Following security updates



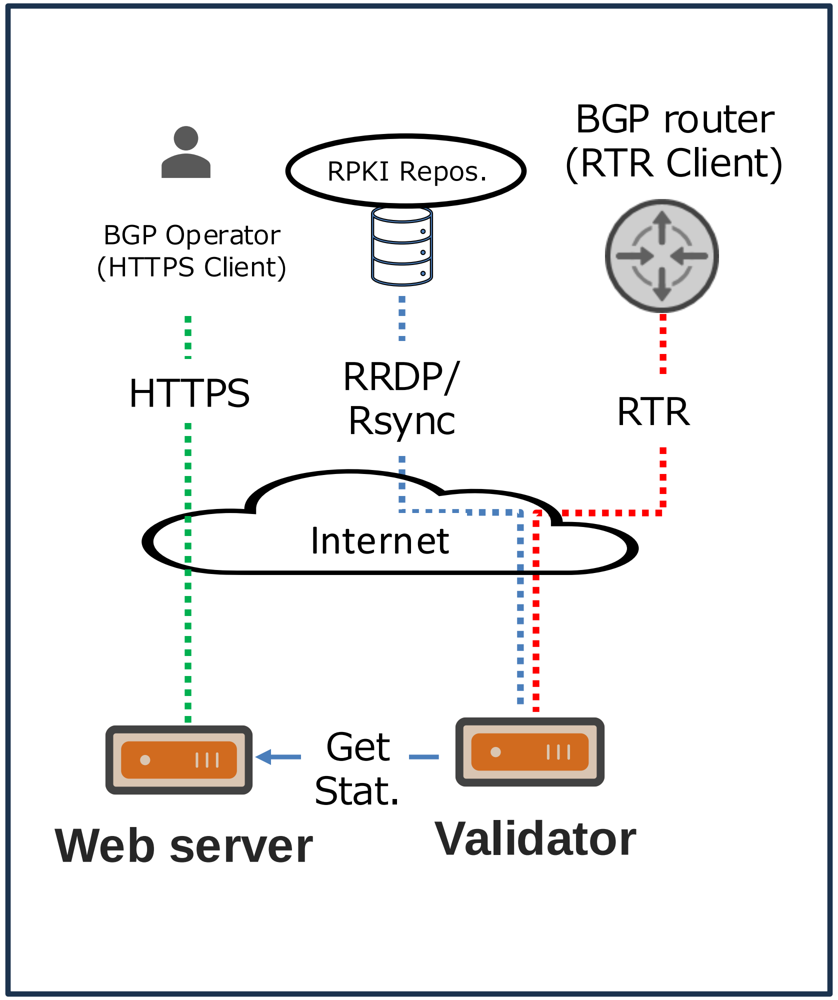
Validator : the challenge in deploying ROV (contd.)

- An idea: Public (shared) Validators by IXP
  - Reduces Operational Burden
  - Cost Savings
  - Not defined in ROV Standard



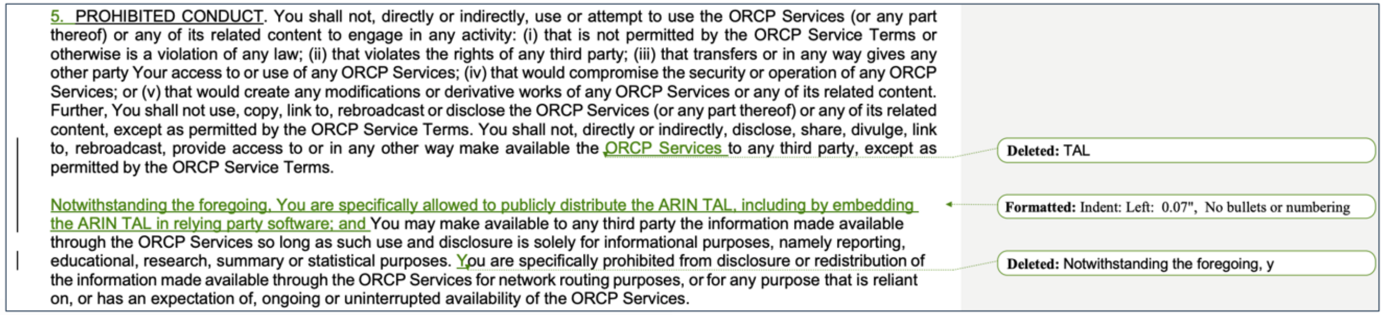
JPNAP made Public RPKI Validator (Gen1,2014-)

- Use RPKI toolkit
- ARIN TAL was not provided due to the “Relaying Party Agreement (RPA) ”
- No redundancy



JPNAP updated Public RPKI Validator (Gen2,2023-)

- ARIN TAL Redistribution Allowed (2022 Sep)
- Some ISPs have asked for commercial-level RPKI validators from IXPs (JPNAP, BBIX, JPIX).
- **JPNAP, BBIX and JPIX decided to provide validators in response to this request.**



5. PROHIBITED CONDUCT. You shall not, directly or indirectly, use or attempt to use the ORCP Services (or any part thereof) or any of its related content to engage in any activity: (i) that is not permitted by the ORCP Service Terms or otherwise is a violation of any law; (ii) that violates the rights of any third party; (iii) that transfers or in any way gives any other party Your access to or use of any ORCP Services; (iv) that would compromise the security or operation of any ORCP Services; or (v) that would create any modifications or derivative works of any ORCP Services or any of its related content. Further, You shall not use, copy, link to, rebroadcast or disclose the ORCP Services (or any part thereof) or any of its related content, except as permitted by the ORCP Service Terms. You shall not, directly or indirectly, disclose, share, divulge, link to, rebroadcast, provide access to or in any other way make available the ORCP Services to any third party, except as permitted by the ORCP Service Terms.

Notwithstanding the foregoing, You are specifically allowed to publicly distribute the ARIN TAL, including by embedding the ARIN TAL in relying party software; and You may make available to any third party the information made available through the ORCP Services so long as such use and disclosure is solely for informational purposes, namely reporting, educational, research, summary or statistical purposes. You are specifically prohibited from disclosure or redistribution of the information made available through the ORCP Services for network routing purposes, or for any purpose that is reliant on, or has an expectation of, ongoing or uninterrupted availability of the ORCP Services.

Deleted: TAL

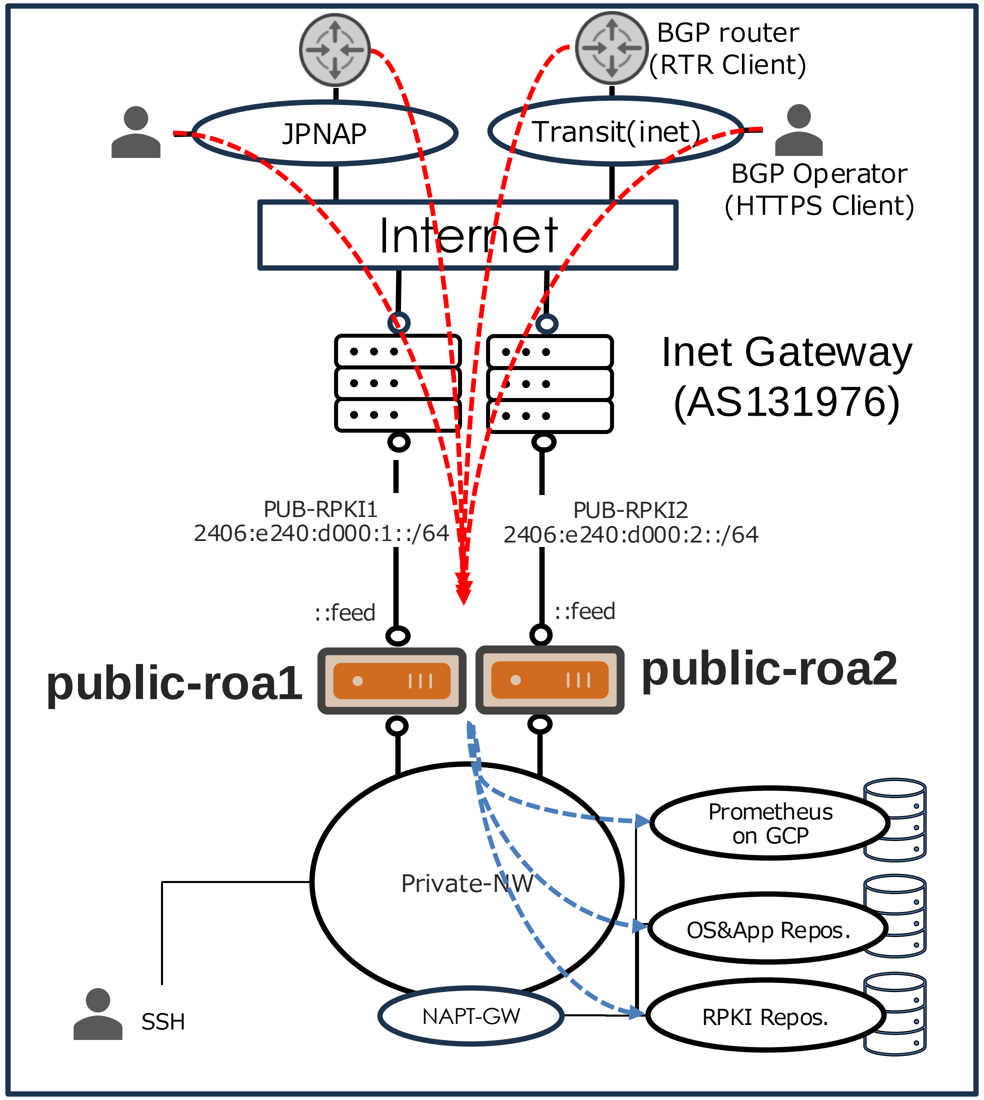
Formatted: Indent: Left: 0.07", No bullets or numbering

Deleted: Notwithstanding the foregoing, y

https://www.arin.net/announcements/2022/documents/rpa_092922_redline.pdf

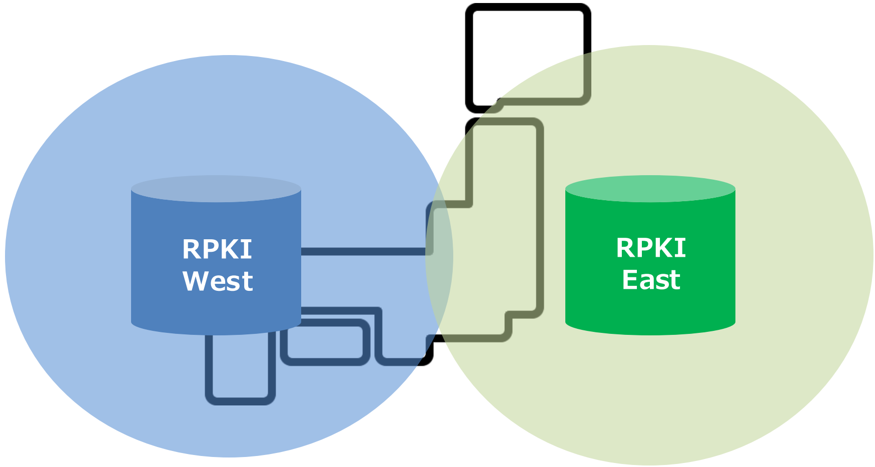
JPNAP Public RPKI Validator (Gen2)

- With redundancy and location diversity
- Dedicated backend interfaces against DDoS attacks
- ROV results visible on the Looking Glass
- Located on Global AS, not on IX LAN
- Interop tested with 3 types of routers (Cisco, Juniper, Arista)
- Only IPv6 transport



Ref: JPNAP Public RPKI Validator Details

Hosts	West JAPAN	public-roa1.mfeed.ad.jp (2406:e240:d000:1::feed) public-roa2.mfeed.ad.jp (2406:e240:d000:2::feed)
	East JAPAN	public-roa3.mfeed.ad.jp (2400:b420:d000:1::feed) public-roa4.mfeed.ad.jp (2400:b420:d000:2::feed)
Protocols/ Ports	RPKI Service	RTR （TCP323）
	WebGUI	HTTPS（TCP443）
	Transport Encryption	None



Experiences from 1 year operation

- A lower number of connections than expected (discuss next).
- Need to monitor software vulnerabilities.
- Contributed to increase ISPs’ interest on RPKI through promotions.

Current & Next Challenges

About the Public RPKI Validator

To increase user... 📈 🤔

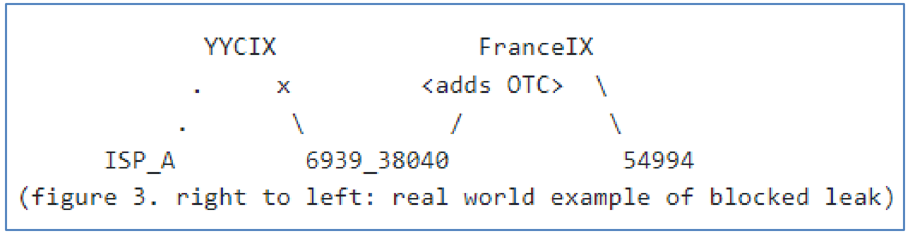
- Is transport security a key factor?
  - Encryption like TLS
  - RTR Proxy (like RTRTR from NLnet Labs)
- Still need IPv4 transport?
- Need more promotions?

Beyond the Public RPKI Validator

What can we do next to enhance routing security?

- ASPA
  - A rising star, but still under changing drafts.
  - ASRA!? A Profile for Autonomous System Relationship Authorization (ASRA)

- BGP Role(RFC9234)
  - Propose new Role capability and attribute “Only To Customer”
  - Designed against route leak
  - Architecture not related to RPKI
  - In field testing between YYCIX and FranceIX



```
            YYCIX                  FranceIX
        .          x          <adds OTC>   \
       .            \            /           \
   ISP_A          6939_38040                54994
(figure 3. right to left: real world example of blocked leak)
```

https://mailarchive.ietf.org/arch/browse/idr/?q=rfc9234%20OR%20%22draft-ietf-idr-bgp-open-policy%22

Thank You!