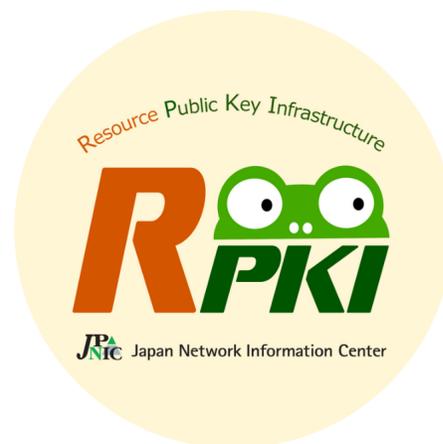


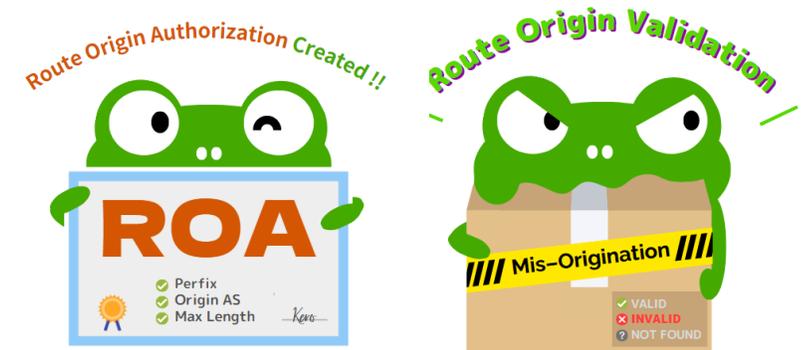
ROAキャン▲地域事業者がRPKIはじめてみて ～みんなの半歩が大きな一歩に～ @JANOG51

JPNIC 塩沢 啓



自己紹介

- 名前：塩沢 啓
- 所属：JPNIC
- 普段の業務：技術部・インターネット推進部
 - BGP、DNS運用
 - セミナー/イベントの企画運営
 - 最近はオンライン開催の配信もやったり
- JANOG歴
 - J39@金沢で初参加、J45@札幌で初スタッフ/初登壇、今回は2回目の登壇
- ROAキャン▲でもっとRPKIを広めたい
 - 今回はケーロちゃん（JPNICのRPKIキャラクター）もROAとROVに対応しました ☺ →



第一部 RPKI動き出す、一歩 「動き出すまでの、歩み」

ROA発行の流れ



ROA発行の流れ

準備

- 資源管理者証明書を準備（資源管理カード／ブラウザ内）
- 資源申請者証明書を担当者に発行（ブラウザ内）

発行

- JPNICのRPKIシステムでROAを発行 <https://rpki.nic.ad.jp/>
※ 自社でCA(Certificate Authority)を運用することも可能(BPKI: Business PKI)

確認

- 登録前後でROA発行状況を確認
 - RIPE <https://rpki-validator.ripe.net/ui/> , APNIC <https://netox.apnic.net/> , JPNIC <http://roa2.nic.ad.jp:8080/roas>
Cloudflare <https://rpki.cloudflare.com/?view=validator> , NLNOG <https://irrexplorer.nlnog.net/>
<https://console.rpki-client.org/> などなど
- 登録前後のトラフィックの確認
- 発行後は ROAと経路情報が乖離しないように！

参考 JPNIC ROAの作成と管理の方法 <https://nic.ad.jp/ja/rpki/howto-create-roa.html>
IRS33 ROA登録チートシート（長県大 岡田さん） <http://irs.ietf.to/wiki.cgi?page=IRS33>

JPNIC ROA Web

rpki.nic.ad.jp/xir/roa_list

JPNIC 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

日本語

最新の情報に更新 (メイン画面) ログアウト

ROAWeb (ipv4exh-lab)

作成されたROAはすぐに公開され、国際的に参照可能な状態になります。ご注意ください。

ROAの管理

Prefix (- 最大prefix長)	AS番号	状態(*1)	操作	観測されているBGP経路 (Prefixと経路広告元のAS)	
202.1.208.0/21-24	131971	発行済	<input type="button" value="削除"/> <input type="button" value="編集"/>		
211.120.240.0/21-24	2515	発行済	<input type="button" value="削除"/> <input type="button" value="編集"/>	211.120.240.0/21	2515

(*1) 発行処理には2分程度かかることがあります。「発行済」の状態はそのROAがRPKIのリポジトリで公開されていることを示しています。
(*2) Routing Information Service (RIS) のBGPデータを元に、本サイトにおけるオリジン検証(ROV)の結果を表示しています。一部のBGP経路が表示されないことがあります。

ROA発行のできるリソース一覧

prefix表記のための正規化が行われているため、WHOISデータとは表記が異なる場合があります。

IPv4

Prefix	操作	観測されているBGP経路 (Prefixと経路広告元のAS)	
61.122.16.0/22	<input type="button" value="ROAを作成"/>	61.122.16.0/22	2522
103.210.108.0/22	<input type="button" value="ROAを作成"/>	103.210.108.0/22	2522
133.112.0.0/16	<input type="button" value="ROAを作成"/>	133.112.0.0/16	2522
150.41.0.0/16	<input type="button" value="ROAを作成"/>	150.41.0.0/16	2522
158.200.0.0/16	<input type="button" value="ROAを作成"/>	158.200.0.0/16	2522
192.47.97.0/24	<input type="button" value="ROAを作成"/>	192.47.97.0/24	2522
192.50.235.0/24	<input type="button" value="ROAを作成"/>	192.50.235.0/24	2522

Web操作でROAの発行が可能

<https://rpki.nic.ad.jp/>

RPKI

お知らせ

- 作成したROAがすぐに公開されるようになりました。(2020年10月30日)

RPKIシステム

通常ご利用いただくためのRPKIシステム (一つ目のボタン) と、国内でテストするためのRPKIシステム (二つ目のボタン) を提供しています。

[> RPKIシステムにアクセス <](#)

「RPKIシステム」では、WebインターフェースでROAを管理する「ROAWeb」とRPKIシステムを接続する「RPKI接続設定」がご利用いただけます。ROAの作成が完了するとすぐに公開され、APNICのTAL (トラストアンカーローグーター) を使って出る事ができるようになります。国際的に参照可能な状態になりますのでご注意ください。アクセスには異議申請者証明書が必要です。

[国内テスト用のRPKIシステムにアクセス \(*1\)](#)

「国内テスト用のRPKIシステム」は、ROAWebやRPKI接続設定を行ってROAを発行しても、APNIC TALを使っても出る事ができない状態で発行されます。(*2) JPNICのTALを利用することができます。ROAの動作を確認するためにご利用いただけます。アクセスには異議申請者証明書が必要です。

(*1) 証明書の番号が表示されます。改修を予定しております。
(*2) ファイルは公開リポジトリに置かれるため、URLを指定すればダウンロードは可能です。

株式会社

通常利用のRPKIシステムに加えて、
国内テスト用のRPKIシステムもあり

JPNIC ROA Web

作成されたROAはすぐに公開され、国際的に参照可能な状態になります。ご注意ください。

ROAの管理

ROAを新規作成 インポート エクスポート

Prefix (- 最大prefix長)	AS番号	状態(*1)	操作	観測されているBGP経路 (Prefixと経路広告元のAS)	
202.1.208.0/21-24	131971	発行済	🗑️ 🔄		
211.120.240.0/21-24	2515	発行済	🗑️ 🔄	211.120.240.0/21	2515

(*1) 発行処理には2分程度かかることがあります。「発行済」の状態はそのROAがRPKIのリポジトリで公開されていることを示しています。
(*2) Routing Information Service (RIS) のBGPデータを元に、本サイトにおけるオリジン検証(ROV)の結果を表示しています。一部のBGP経路が表示されないことがあります。

ROA発行のできるリソース一覧

prefix表記のための正規化が行われているため、WHOISデータとは表記が異なる場合があります。

IPv4

Prefix	操作	観測されているBGP経路 (Prefixと経路広告元のAS)	
61.122.16.0/22	ROAを作成	61.122.16.0/22	2522
103.210.108.0/22	ROAを作成	103.210.108.0/22	2522
133.112.0.0/16	ROAを作成	133.112.0.0/16	2522
150.41.0.0/16	ROAを作成	150.41.0.0/16	2522
158.200.0.0/16	ROAを作成	158.200.0.0/16	2522
192.47.97.0/24	ROAを作成	192.47.97.0/24	2522
192.50.235.0/24	ROAを作成	192.50.235.0/24	2522

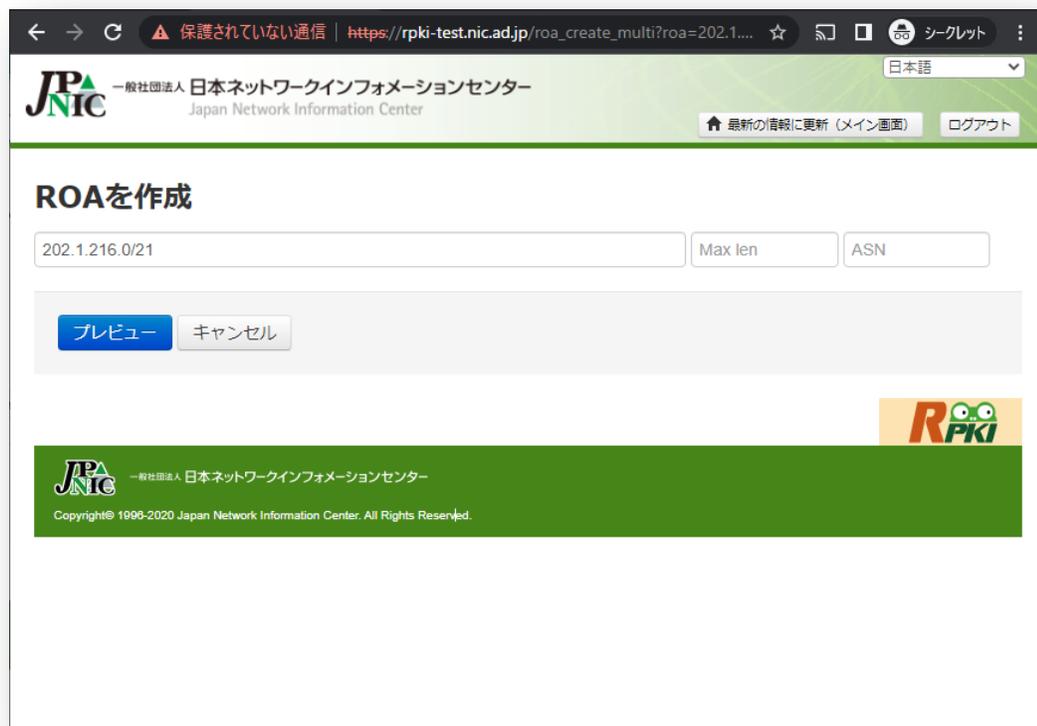
- ROAの管理

- 発行済みのROAが表示

- ROA発行のできるリソース一覧

- 「ROAを作成」をクリック

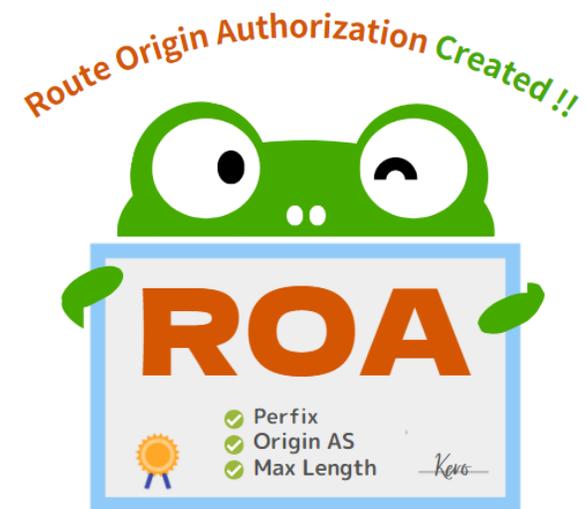
JPNIC ROA Web



The screenshot shows a web browser window with the URL https://rpk-test.nic.ad.jp/roa_create_multi?roa=202.1.... The page title is "ROAを作成" (Create ROA). The form contains a text input field with the value "202.1.216.0/21", a "Max len" field, and an "ASN" field. Below the input fields are two buttons: "プレビュー" (Preview) and "キャンセル" (Cancel). The page footer includes the JPNIC logo and the text "Copyright© 1999-2020 Japan Network Information Center. All Rights Reserved."

ROAの発行に必要な情報を入力

- Prefix
- Origin AS
- 最大prefix長 (max prefix length)



JPNIC ROA Web

- Prefix
- Origin AS
 - 異なるOrigin ASのROAを複数発行することも可能
 - 自社の複数のASから経路広告する場合
 - クラウドサービスなど他ASから経路広告する可能性がある場合 など
- **最大prefix長 (max prefix length/max length)**
 - ROAで許容される最大のプレフィックス長
 - Max-Length を不必要に長くする事は推奨されない (ref RFC9319)
 - 原則、経路情報と一致させるような設定が推奨
 - Origin詐称による経路ハイジャックのリスクを低減

(ex) 192.168.0.0/21のROA

✓ Prefix	192.168.0.0/21
✓ Origin AS	64500
✓ Max Length	/22

192.168.0.0/21 - 22 (Max-Length)



これより細かい
経路は許容されない

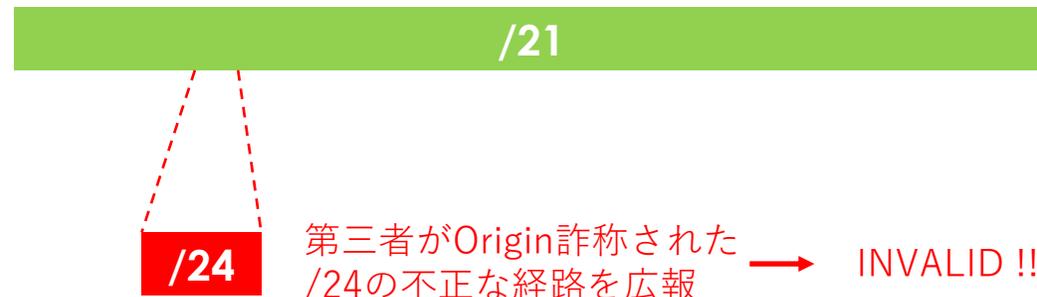
JPNIC ROA Web

- Prefix
- Origin AS
 - 異なるOrigin ASのROAを複数発行することも可能
 - 自社の複数のASから経路広告する場合
 - クラウドサービスなど他ASから経路広告する可能性がある場合 など
- **最大prefix長 (max prefix length/max length)**
 - ROAで許容される最大のプレフィックス長
 - Max-Length を不必要に長くする事は推奨されない (ref RFC9319)
 - 原則、経路情報と一致させるような設定が推奨
 - Origin詐称による経路ハイジャックのリスクを低減

(ex) 192.168.0.0/21のROA

✓ Prefix	192.168.0.0/21
✓ Origin AS	64500
✓ Max Length	/22

192.168.0.0/21 - 22 (Max-Length)



JPNIC ROA Web

作成されるROAの内容

ご注意： AS番号と最大prefix長が異同通りであることをご確認ください。作成されたROAはすぐに公開され、国際的に参照可能な状態になります。

プレビュー

Prefix	最大prefix長	AS番号
202.12.30.0/24	32	2515

RouteViewで観測されている経路情報

Prefix	観測元AS	観測される経路の状況
202.12.30.0/24	2515	valid

作成 キャンセル

ROAのプレビュー画面

- 観測されている経路情報とROVの状況が表示
- Invalidの場合は注意！

JPNIC ROA Web



- ROAが発行済になりました

作成されたROAはすぐに公開され、国際的に参照可能な状態になります。ご注意ください。

ROAの管理

Prefix (- 最大prefix長)	AS番号	状態 (1)	操作	観測されているBGP経路 (Prefixと経路広告元のAS)
202.1.208.0/21-24	131971	発行済	🗑️ 🔄	
211.120.240.0/21-24	2515	発行済	🗑️ 🔄	211.120.240.0/21 2515

(*1) 発行処理には2分程度かかることがあります。「発行済」の状態はそのROAがRPKIのリポジトリで公開されていることを示しています。
(*2) Routing Information Service (RIS) のBGPデータを元に、本サイトにおけるオリジン検証(ROV)の結果を表示しています。一部のBGP経路が表示されないことがあります。

ROA発行のできるリソース一覧

prefix表記のための正規化が行われているため、WHOISデータとは表記が異なる場合があります。

IPv4

Prefix	操作	観測されているBGP経路 (Prefixと経路広告元のAS)
61.122.16.0/22	🗑️ 🔄	61.122.16.0/22 2522

Routing

Showing 1 to 3 of 3 entries

AS番号	プリフィックス	状態
131971	202.1.208.0/21	VALID
131971	202.1.208.0/22	VALID

Showing results for 202.1.208.0/21

JPNIC <http://roa2.nic.ad.jp:8080/roas>

Showing 1 to 2 of 2 entries (filtered from 1,174,504 total entries)

source data embed code in

Prefix Routing Consistency (202.1.208.0/21)

APNIC <https://netox.apnic.net/>

Showing 1 to 10 of 10 entries

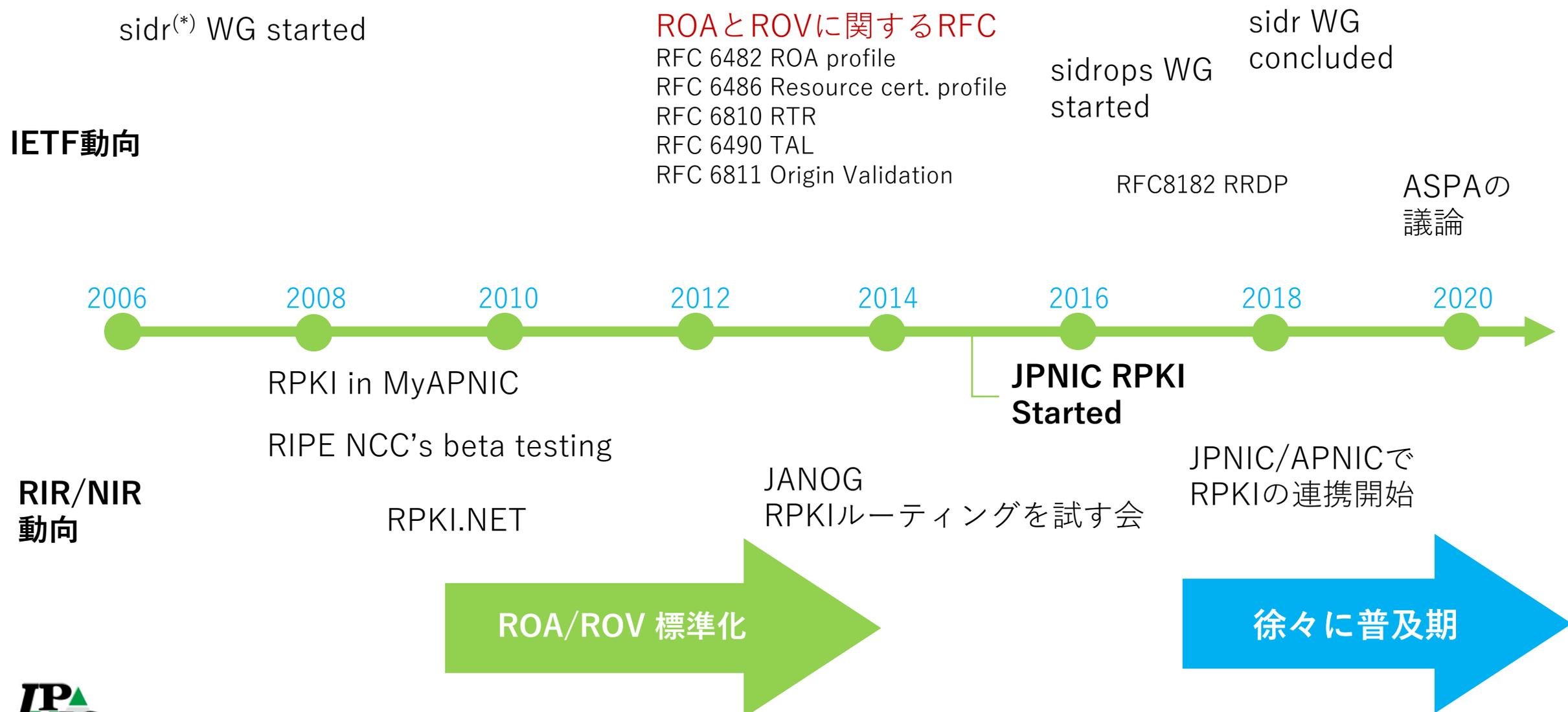
prefix	Origin	ASN Name	In	RPKI
202.1.208.0/21	AS131971	NW-SEC-EXP-J Network Inform	VALID - valid announcement	😊

外部からもVALIDになっているか確認！

第一部 RPKI動き出す、一歩 「動き出すまでの、歩み」

RPKIの動向と、普及に向けたこれまでの活動実績や課題感

RPKIとROAのこれまで



ROAのこれから

OBSERVATORY | ROUTING SECURITY

Will 2023 be the Year Half of the Internet is RPKI-Enabled?

By Aftab Siddiqui • 16 Jan 2023

Valid ROA %

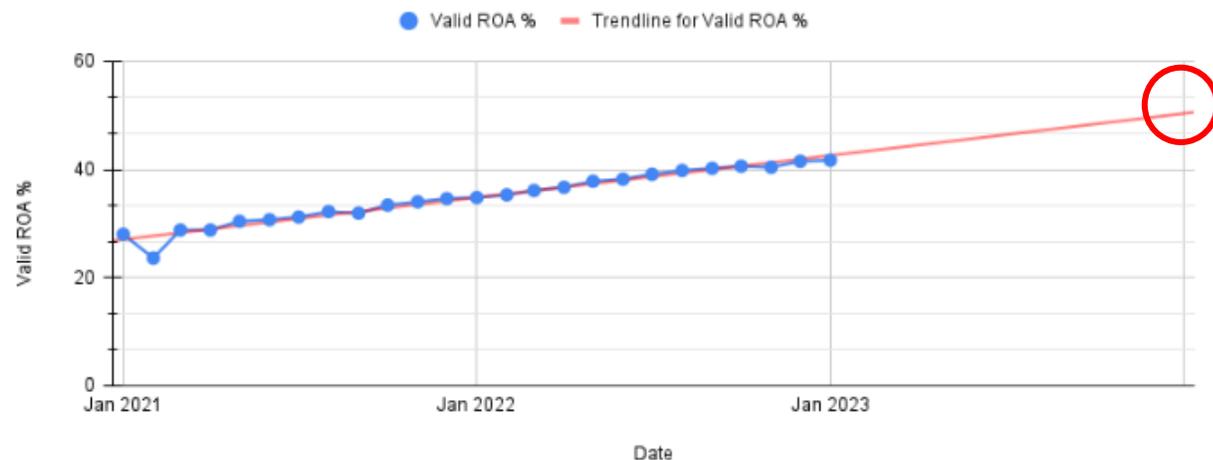


Figure 11 – Percentage of valid RPKI-enabled resources (IPv4 and IPv6) based on RIPE Stat and NIST RPKI monitor.

- 前年よりもルーティングインシデントの発生件数は多かったが、**RPKIの利用が普及**したため**深刻な被害には至らなかった**
- 2023年末には、**ValidなROAの割合が50%以上**になると予測

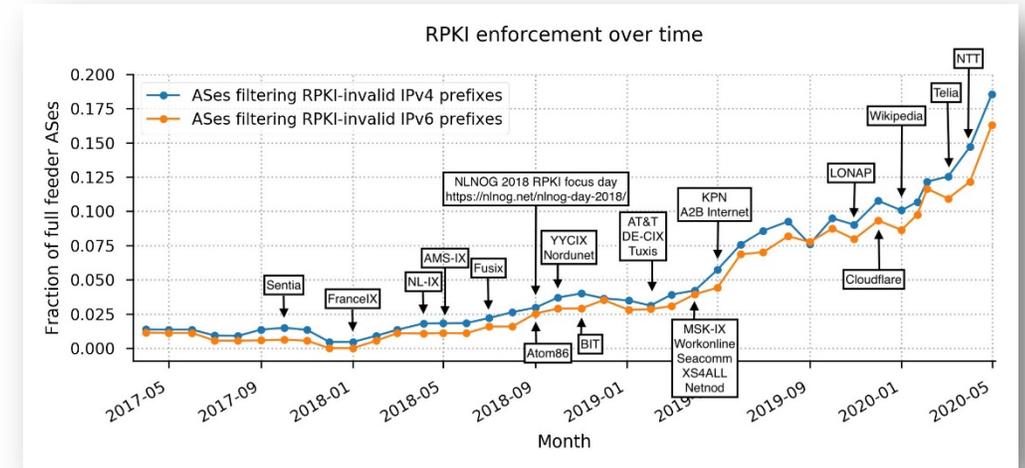
ROVの実装

RoVista
Overview of ROV Filtering Ratio

Show: 10 Search:

Rank ▲	ASN	Country	Organization	ROV-Ratio
1	3356	United States	Level 3 Parent, LLC	1
2	1299	Sweden	Telia Company AB	1
3	174	United States	Cogent Communications	1
4	3257	United States	GTT Communications Inc.	1
6	2914	United States	NTT America, Inc.	1
7	6939	United States	Hurricane Electric LLC	1
8	6461	United States	Zayo Bandwidth	0
9	6453	United States	TATA COMMUNICATIONS (AMERICA) INC	1
10	3491	United States	PCCW Global, Inc.	1
11	1273	European Union	Vodafone Group PLC	0

<https://rovista.netsecurelab.org/>



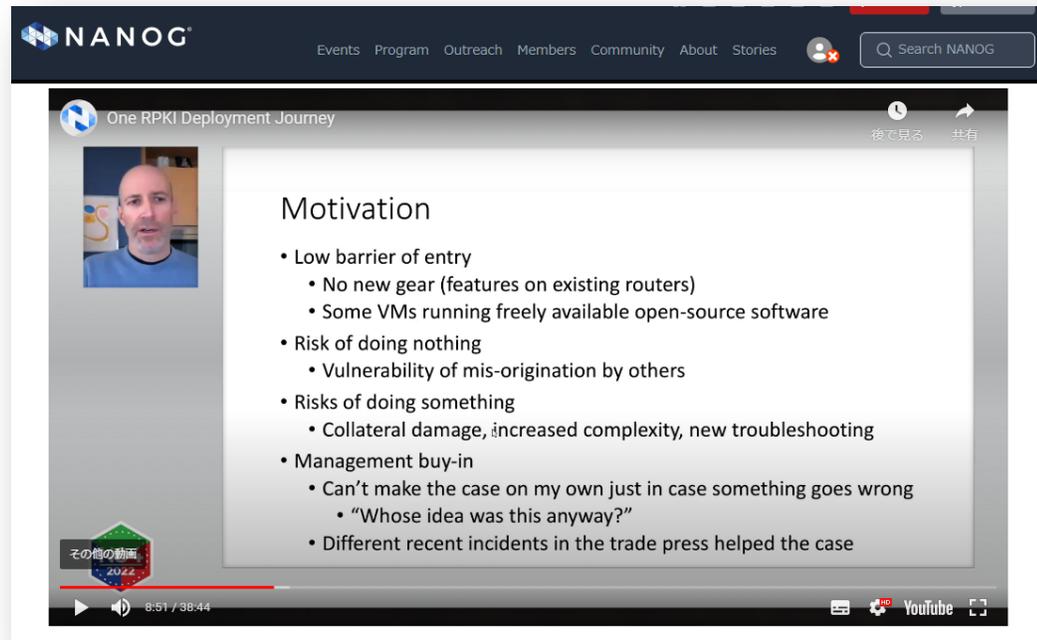
<https://twitter.com/JobSnijders/status/1256326712347881473>

- **RoVista** : 27,000以上のASのROV実装状況を測定
- **Tier 1を中心にROVを実装していることが判明**
 - Level 3 (AS 3356), Telia (AS 1299), GTT (AS 3257), NTT America (AS 2914), TATA Communications (AS 6453), PCCW Global (AS 3491), Orange (AS 5511), AT&T (AS 7018), Liberty Global (AS 6830), Sprint (AS 1239), and CenturyLink (AS 209)

国際的な通信事業者やIXを中心にROVの実装も進む

ROVの実装

Comcast のROVを導入したモチベーション



The screenshot shows a video player interface for a video titled "One RPKI Deployment Journey" on the NANOG website. The video content includes a speaker and a list of motivations for RPKI deployment:

- Motivation
 - Low barrier of entry
 - No new gear (features on existing routers)
 - Some VMs running freely available open-source software
 - Risk of doing nothing
 - Vulnerability of mis-origination by others
 - Risks of doing something
 - Collateral damage, increased complexity, new troubleshooting
 - Management buy-in
 - Can't make the case on my own just in case something goes wrong
 - "Whose idea was this anyway?"
 - Different recent incidents in the trade press helped the case

- **すでに一部の大手ISPではROVが行われている**
 - Invalidなプレフィックスはすでに落とされている
- **参入障壁が低い**
 - 新しい機材が不要（既存のルータに搭載可能）
 - 自由に利用できるオープンソースソフトウェアを実行するVMもある
- **何もしない場合のリスク**
 - 他者による誤った広報の可能性はある
- **何かした場合のリスク**
 - 巻き添え被害、複雑性の増大、新たなトラブルシューティングの発生

RPKI普及に向けた活動とこれまでの課題感

- **RPKI普及状況：海外、日本国内でも徐々に普及**
 - ROA：カバー率は年々上昇している
 - まずはROAの発行から！
 - 過去に発行したことがあったなという方は今一度確認を。現在の経路情報と乖離がないような運用も。
 - ROVは国際的な通信事業者やIXを中心に実装されては始めている
- **JPNICにおける普及活動**
 - コミュニティの場などで最新動向発表、ハンズオンセミナー開催
 - JANOG、地域NOG、Internet Week、IRS etc...
 - ROA Webの使い方や、ROVを体験するハンズオン
 - オンライン開催で場所を問わず今までより気軽に参加
- **日本国内の登録数も増えるが、一方で地域の事業者との取り組みが課題に…**
 - オンラインセミナーなど気軽に参加いただけるとは、密なコミュニケーションは取りづらい。
 - RPKI/ROAの普及に向けて、みんなが「一歩、動き出す」にはどうすればいいか？

第二部 新技術 普及する、一步

第二部 新技術 普及する、一歩

- RPKIに限らず、インターネットをより安全にするための技術
 - ルーティング
 - DNS
 - アプリケーション
 - メール、Web etc...



第71回JPNIC総会 座談会「インターネットを守るための技術普及を官民で考える」より
<https://youtu.be/ijP6QSQxfA0>

第二部 新技術 普及する、一步

「一步、動き出す」ためのオモテとウラの取り組み…

・ オモテ

- ・ 継続的な情報発信
- ・ 先駆者達のknow-howを共有
- ・ コミュニティのbest practiceを議論
- ・ 産学官の連携



・ ウラ

- ・ コミュニティの活用
 - ・ みんなでやっ払いこう
 - ・ 何かあったら助けられる環境
- ・ 一緒に悩める仲間作り！



新技術の普及について、うまくいった経験や取り組んでいる事例、
こうしたらもっとうまくいくという事があったら教えてください！