

JPNIC総会 会員フォーラム

RPKIのこれまでとこれから



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

Copyright © Japan Network Information Center 

▶▶▶ ご案内

RPKI – リソースPKIは、JPNICのデータベースが活用される技術的な仕組みであると同時に、ルーティングにおける“経路情報の正しさ”に踏み込む技術です。2000年代にRFC化と実装が活発に行われ、2017年頃から日本において普及が始まり、2023年頃には“実証実験”としてROV導入の議論と検討と、時々動きを経て今日に至っています。

そして、RPKIは、様々な立場、IPアドレスの分配を受けた方・ASを運用をされている方、大学や学術組織で研究をされている方・そして通信事業に関係されている方、と、何かしらの関わりを持つものでもありました。

この時間は、国内におけるRPKIに関わる出来事や活動を振り返ると共に、インターネットのルーティングやレジストリの役割に関わる話題をみていきながら議論を深めていきます。JPNICという場においてインターネットの今後をどう捉えていくのか、識者の視座を交えながら、会場のみなさまと考えていきます。

RPKIのこれまで



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

Copyright © Japan Network Information Center ▶▶ 3

▶▶▶ RPKIの起こり

(移転の時期との関係)

	2005th	2006th	2007th	2008th
IETF	★2004 th Jun RFC3779	★Mar 1 st SIDR BoF ★Apr SIDR WG結成	★Mar I-D “ROA” ★Apr I-D “profile”	
APNIC	リソースPKI開発の 中心的存在	リソース証明書 エンジン部分の開発	I/F等の開発	Sep/Oct ★ MyAPNICへの 組み込み
ARIN		★システム設計開始	開発への参加	レジストリ連携の開発
RIPE NCC	リソース証明書の 実現性と効果の評価に着目	★Oct CATF結成 ★CertPROTO	開発への参加	★ Oct ベータテスト ★ Oct 開発
JPNIC	経路情報の登録機構	★ RIR検討への参加 リソースセキュリティの調査	設計	★ Oct ポリシー提案 2008-08 開発 利用実験

IPv4アドレスの在庫枯渇の時期が見えてきた頃、利用側の実装がない中での開発と議論が行われていた。

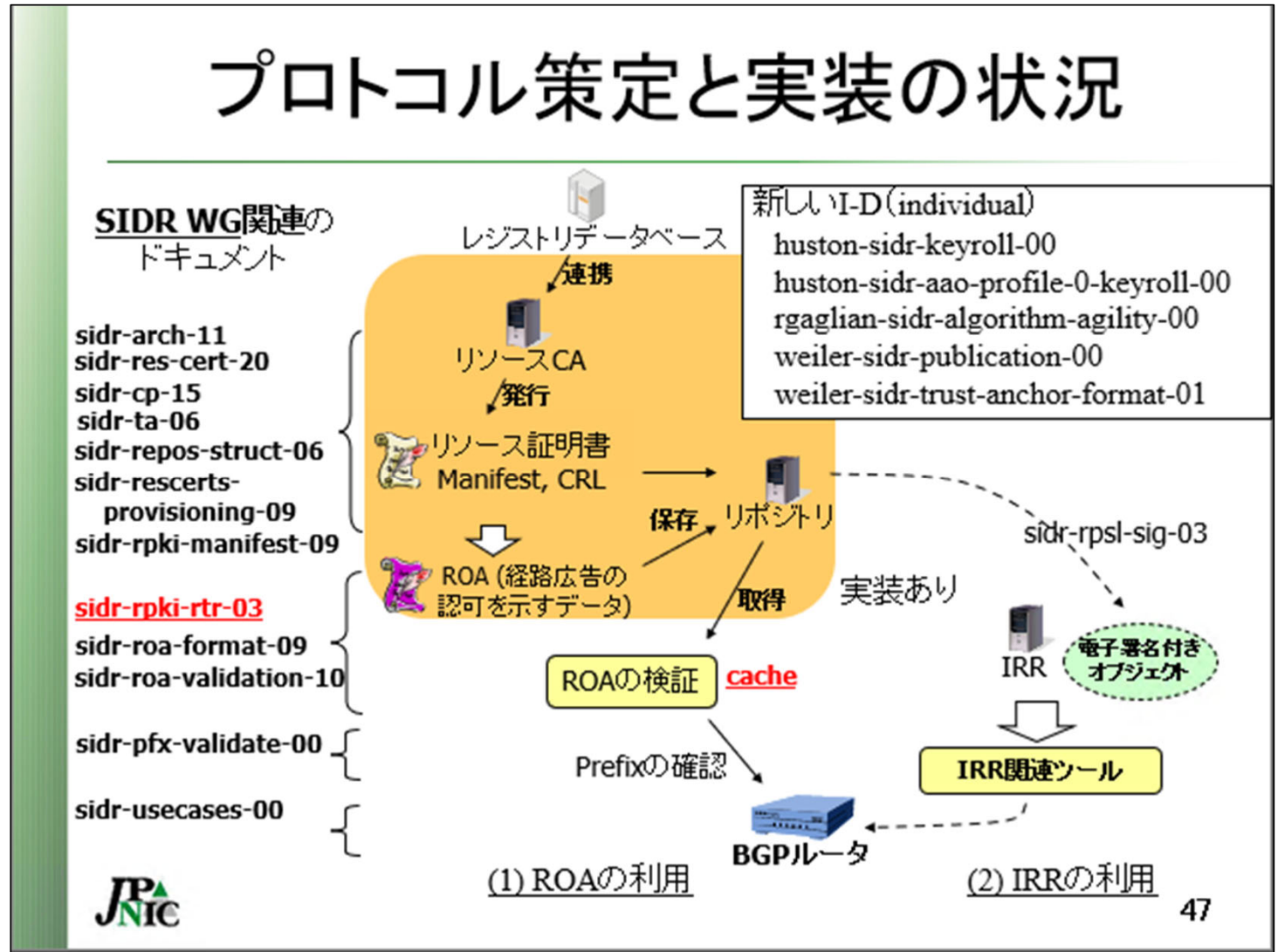
2009年資料より

▶▶▶ 2010年

“ROAキャッシュサーバ”に関する実装は限定的

IETF79参加報告より

プロトコル策定と実装の状況



▶▶▶ 2010年

2010年1月12日 ハンズオン@IIJ メモより

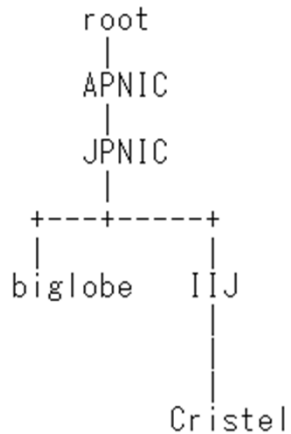
2010年11 IETF79@北京

#####1/12 10:00-20:00(17:30-20:00), IIJ, (Rob, Randy, Maz, Cristel, Taiji)

We've done today:

1. Both IIJ and NEC biglobe setup their rpki
2. They exchanged keys between IIJ and Cristel

assumed structure:



bpki.myrpki/ca.cer for resources (- used in XML transactions
 bpki.myirbe/ca.cer for servers (fo

RPKI testbed

賛沢！！

(RPKI tool 開発責任者) Rob Austin氏

(国内ISP) 松崎吉伸氏

(RPKI tool GUI 開発者) Michael Elkins氏

(Stephen Kent氏の同僚) Andrew Chi氏

木村の座席

Rob氏談 前はこうやって集まるのは普通だったし、IETFってそういう場所だったよね。

年表 - 2006年から2018年

2006 2008 2009 2012 2013 2015 2016 2017 2018

sidr WG started

RFC 6482
ROA profile
RFC 6486
Resource cert. profile
RFC 6490
RFC 6810
RTR
RFC 6811
Origin Validation
TAL

sidrops WG started

sidr WG concluded

RFC8182
RRDP

ROAとROVに関するRFCが現れる

★IETF79

★JPNIC ROAWeb
試験提供開始

★JPNICのRPKシステムが
APNICと接続

★RPKIハッカソン@IIJ

★JANOG RPKIルーティングを試す会

★RPKIハッカソン@電力系勉強会

★RPKIハッカソン@ENOG20

★RPKIハッカソン@インターネット・マルチフィード

★ルーティングを守る@JPIXユーザ会

★電力系NCC情報交換会@広島

RPKI.NET

RPKI in
MyAPNIC

RIPE NCC's
beta testing

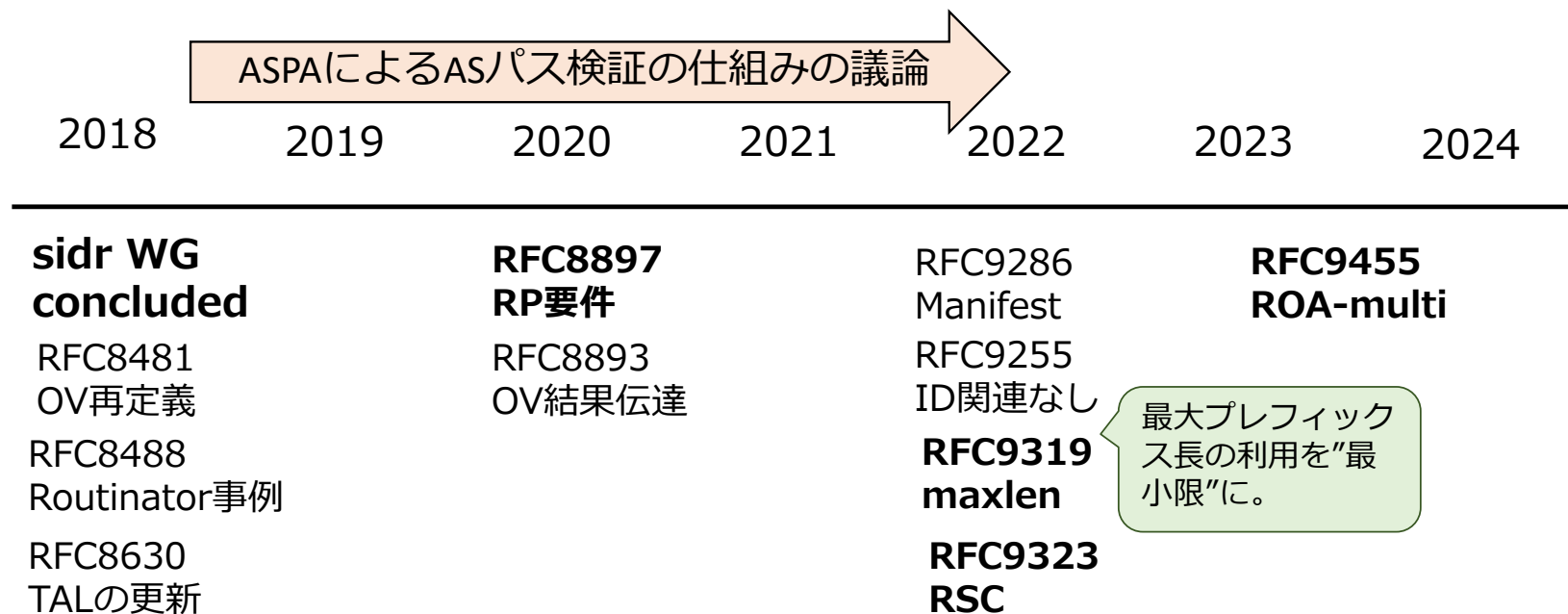
多くの方々に支えられてきました。



RIRにおけるRPKI/ROA実装



▶▶▶ 年表 - 2018年から2024年



最大プレフィックス長の利用を“最小限”に。

★IRS ドロップの話題

ROA作成に関わる数々のお問合せ

歴史的なIPアドレスに関する対応

総務省 ISP におけるネットワークセキュリティ技術の導入に関する調査 (NTTコミュニケーションズ, 三菱総合研究所)

経路セキュリティに関する取り組み

国内情報交換（意見醸成）の場

- Inter-Domain Routing Security (IRS) ワークショップ <http://irs.ietf.to/>
- InternetWeek ルーティングセキュリティ・セッション（毎年）
- JANOG, ENOG, QUNOG, TDNOG, TOPIC勉強会等
- ICT-ISAC BGP WG

米国

- NANOG（情報交換/意見醸成）
- IETF ルーティングエリア, SIDROPS, IEPGミーティング
- DHS（国土安全保障省）RPKI tools開発
- 米国国立標準技術研究所（NIST）
 - 標準化活動(IETF参加)
 - プロトタイプ実装(BGP-SRx)・シミュレーション環境（BRITE）
- BBN（RPKI提唱者は引退か/かつてはCNNIC技術者を受け入れ）
- Oracle社（旧Renesys社）経路情報の分析/コンサルテーション

- NIST, DHSはいち早く実装/実験/シミュレーション/モニタリング
- NANOGにて意見醸成

アジア

- APNIC
 - 標準化
 - APNIC Lab分析
- CNNIC, TWNIC, IDNIC（開始）
VNNIC, IRINN

欧州

- RIPE NCC → RIS、RPKI Validator 開発
- nINetLabs → RPKI Krill 開発
- EuroIXなどのIX（議論および導入）

国際

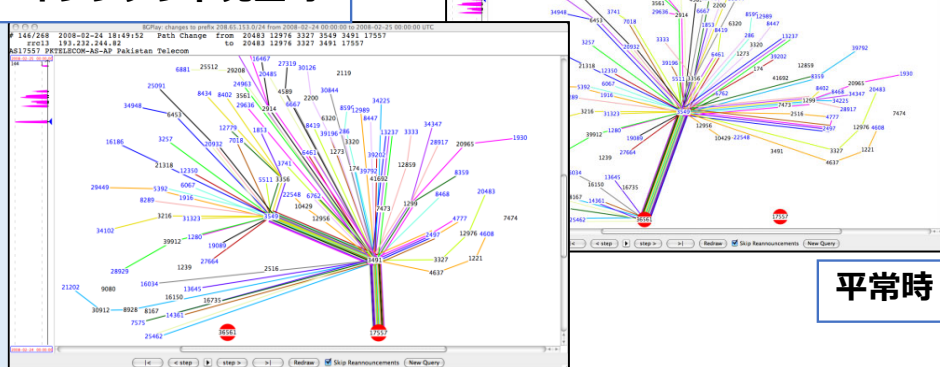
- ISOC → MANRS
- ICANN → SSAC

ルーターティングに関わるインシデントの歴史 - オリジン検証関連 -

代表的なインシデント事例

- 1997年 米国フロリダ接続事業者によるルートリーク発生。多数の不到達。
- 2008年 パキスタン・テレコムによりYouTubeへの到達性が一時的に失われる。
- 2013年 米国国内の経路が東欧経由に不正に変更される報告
- 2014年 ビットコイン・マイニングプールに対する不正経路/不正サーバ
- 2017年 Googleにおけるルートリーク発生の報告。国内で大規模な接続障害発生。
- 2018年 AWS Route53に対する不正経路発生。MyEtherWalletの偽サイトへ誘導される。[DNS]
- 2022年 ウクライナの”Internet Names Center”に対する不正経路が観測される(※1)。[DNS]
- 2023年 ロシアにあるISPによる不正経路の影響で、ミャンマーにおけるTwitterへのアクセスができなくなる。

インシデント発生時



平常時

YouTube Hijacking: A RIPE NCC RIS case study, 17 Mar 2008, RIPE NCC, <http://www.ripe.net/internet-coordination/news/industry-developments/youtube-hijacking-a-ripe-ncc-ris-case-study>

YouTubeの経路情報が別のASによって広告され、約2時間半の間、アクセスできなくなった。

[DNS]は不正な経路情報により偽のDNS応答が送られるようになり偽サイトに誘導される事例

(※1) Did Ukraine suffer a BGP hijack and how can networks protect themselves? - MANRS, <https://manrs.org/2022/03/did-ukraine-suffer-a-bgp-hijack-and-how-can-networks-protect-themselves/>

▶▶▶ ホワイトハウスにおけるRPKIのROA/ROV普及に関する文書

- 2024年9月に政府機関に関わるサービス事業者を含むISP等におけるRPKI/ROAの普及に関する文書を公開 ⇒ **現在は非公開(HTTP 404)**
 - Roadmap to Enhancing Internet Routing Security, Office of The National Cyber Director, September 2024,
<https://www.whitehouse.gov/wp-content/uploads/2024/09/Roadmap-to-Enhancing-Internet-Routing-Security.pdf>

要点

- 2023年の**国家サイバーセキュリティ戦略実施計画**に沿う位置づけ。
- BGP経路制御における異常状態を「**プレフィックス・ハイジャック**」「**パス・ハイジャック**」「**ルート・リーク**」の三つと位置づけ。
- 北米地域におけるROV結果Validとなるカバー率は39%**とヨーロッパ地域の70%よりも低い。
- ARIN(北米地域のレジストリ)の事業者との**契約条項(RSA)の政府機関用テンプレート**を作成。
- ISPおよび政府の関わるサービス提供者に**IPアドレス・AS番号に関する確認とROA作成の推進・効果報告**等を奨励。政府によける**予算ガイドライン**等を提供。

“異常状態”	対策技術
プレフィックス・ハイジャック	ROA + ROV (および経路フィルター)
パス・ハイジャック	ASPAおよび経路フィルター等
ルート・リーク	ASPAおよび経路フィルター等

木村整理



2022年度から2025年度にかけて

総務省 ISP におけるネットワークセキュリティ技術の導入及び普及促進に関する調査

MRI

①RPKI ②DNSSEC ③DMARC

参考1. 実証実験参加者一覧

【①RPKI】実証実験参加者一覧	【②DNSSEC】実証実験参加者一覧	【③DMARC】実証実験参加者一覧

Copyright © Mitsubishi Research Institute

22

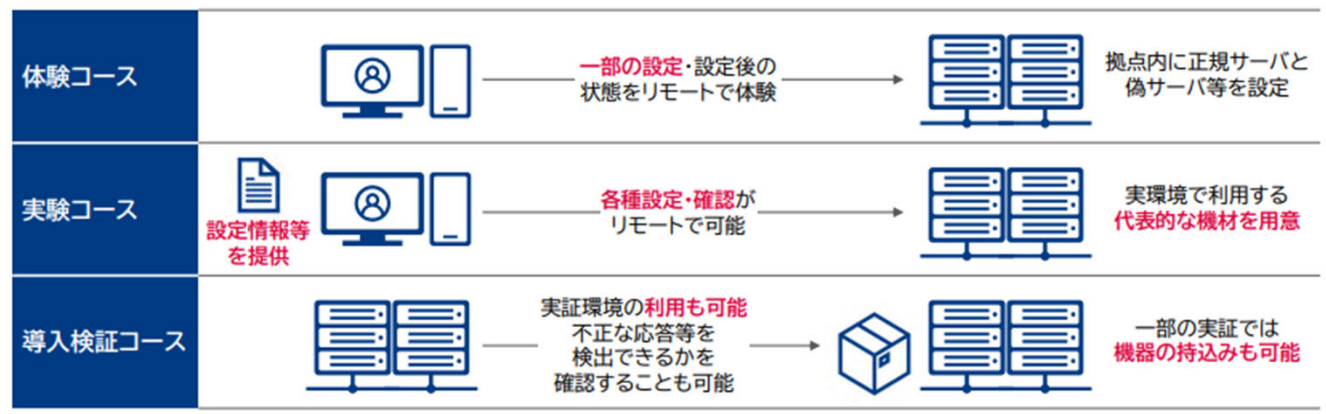
ISPにおけるネットワークセキュリティ技術の導入に関する調査, MRI, 総務省サイバーセキュリティタスクフォース (第43回) 資料43-1-1, https://www.soumu.go.jp/main_content/000878673.pdf





4.1.1. 技術的課題の調査（実証環境の整備）

- 各実証コースの利用を想定し、実証環境を整備した。
- RPKIの仮想環境では、ネットワーク通信機材の持込みによる検証を想定し、3大学の協力の基、**慶応大学（SFC:神奈川）、大阪大学、長崎県立大学**に設置。また、検証用及び実態を体験するためフルフロー環境を用意。
- DNSSECの仮想環境では、正しく検証できていることを確認するために、実際に**不正なDNS応答を流せる環境**を用意。
- DMARCの仮想環境では、送信したメールのレポートの確認、受信したメールの**レポート結果等が確認できる環境**を用意。



ISPにおけるネットワークセキュリティ技術の導入に関する調査, MRI, 総務省サイバーセキュリティタスクフォース（第43回）資料43-1-1, https://www.soumu.go.jp/main_content/000878673.pdf

▶▶▶ JPNICにてRPKIガイドラインを公開

- RPKIのROAを使ったインターネットにおける不正経路への対策ガイドライン

<https://www.nic.ad.jp/ja/rpki/guideline/>



(総務省サイバーセキュリティ統括官室 参事官補佐 梅城崇師氏(右)からガイドライン・フレームを受け取る
JPNIC佐藤晋事務局長(左))

RPKIを活用してインターネットルーティングの信頼性を向上させませんか？ — 「RPKIのガイドライン」を公開しました, JPNICブログ, <https://blog.nic.ad.jp/2025/10557/>

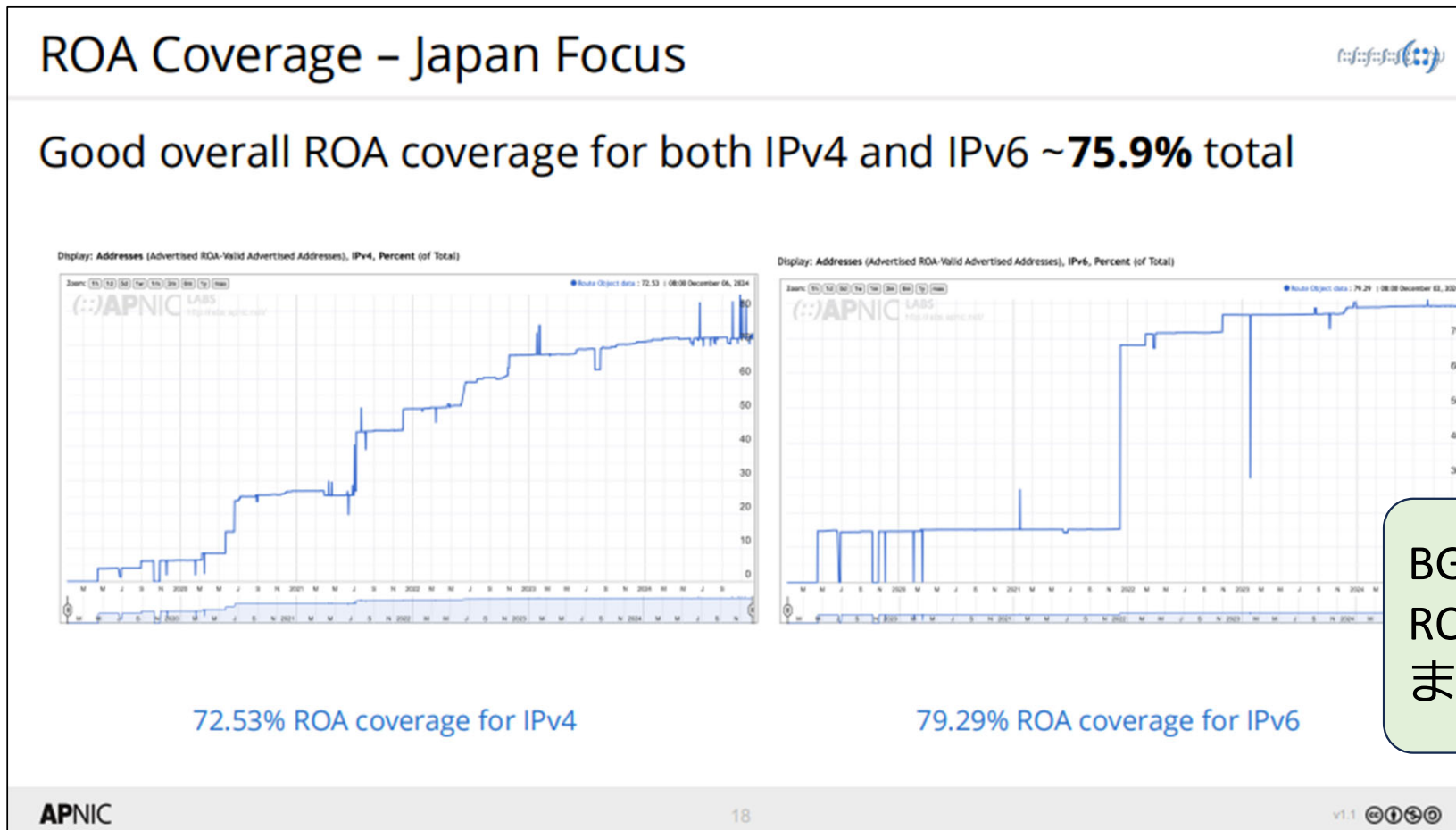
RPKIのこれから



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

Copyright © Japan Network Information Center ▶15

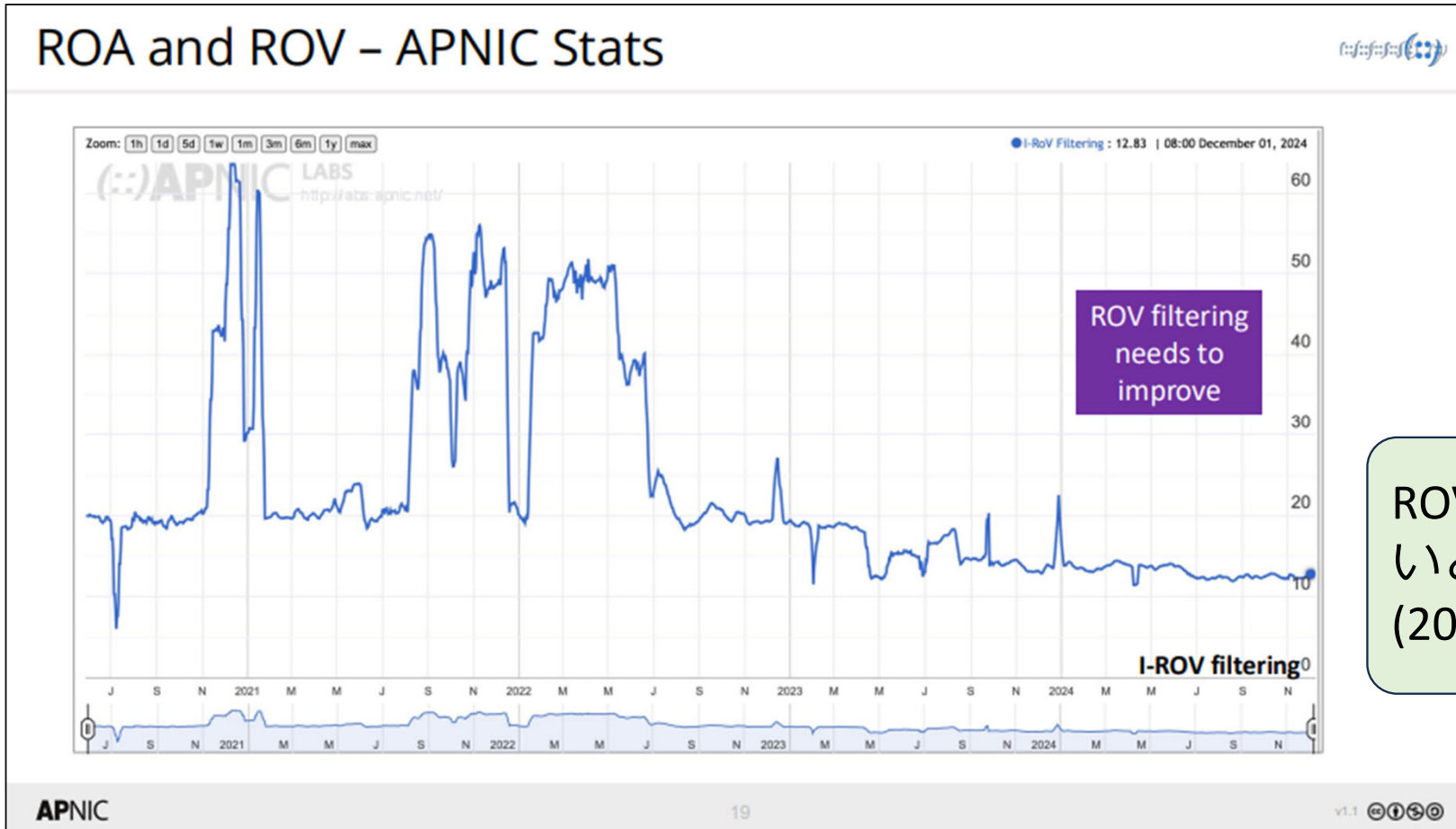
▶▶▶ ROAによるカバー率



BGP経路における
ROAカバー率は高
まりつつある。

Why ROV?, RPKI Deployment Status in Japan, JANOG 55, Sheryl(Shane) HERMOSO,
<https://www.janog.gr.jp/meeting/janog55/wp-content/uploads/2024/12/janog55-lt-Shery-00.pdf>

▶▶▶ ROVの適用について(1/2)

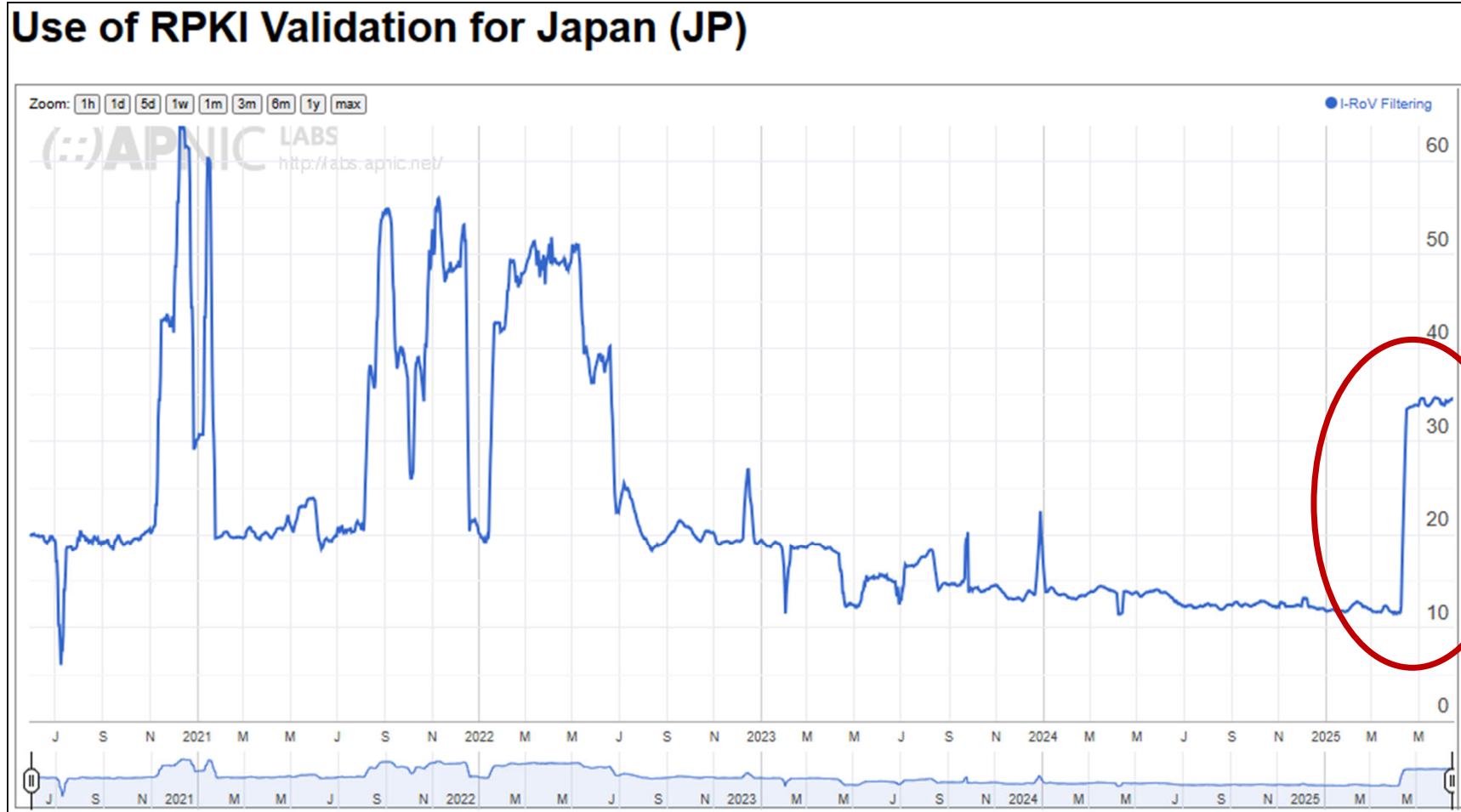


ROVの適用率は低いという指摘...
(2025年1月時点)

Why ROV?, RPKI Deployment Status in Japan, JANOG 55, Sheryl(Shane) HERMOSO,
<https://www.janog.gr.jp/meeting/janog55/wp-content/uploads/2024/12/janog55-lt-Shery-00.pdf>



ROVの適用について(2/2)



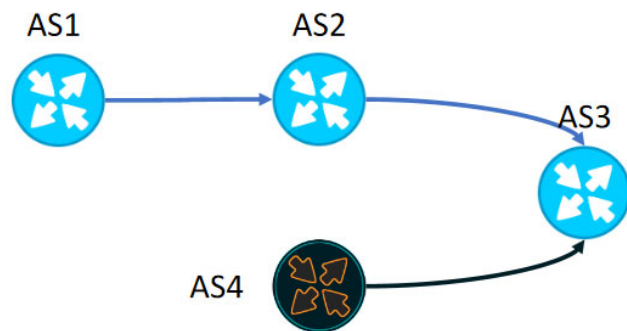
Use of RPKI Validation for Japan (JP) - RPKI I-ROV Filtering World Map, <https://stats.labs.apnic.net/rpki/JP>



▶▶▶ ASPA - Autonomous System Provider Authorization ASパスを検証する仕組み

AS_PATH Verification

1. If the closest AS in the AS_PATH is not the receiver's neighbor ASN then procedure halts with the outcome "invalid";
2. If in one of AS_SEQ segments there is a pair (AS(I-1), AS(I)) is "invalid" then the procedure also halts with the outcome "invalid";



ROA {x.x.x.x, AS1}
 ASPA {AS1, AS2}
 ASPA {AS2, AS3}
 ASPA {AS3, 0}

BGP Quadrant: Possible Future

	BGP Hijacks	BGP Route Leaks
Mistake	ROA	ASPA
Malicious	ROA + ASPA	ROA + ASPA

AS_PATH Verification Using ASPA

<https://datatracker.ietf.org/meeting/102/materials/slides-102-sidrops-as-path-verification-using-aspa-00.pdf>

▶▶▶ 技術課題

- **ASPA実装が現れつつある**
 - CAソフトウェア - Krill
 - RPソフトウェア - rpki-client, StayRTR, Routinator, RPSTIR2
- **JPNICのRPKIシステム(開発課題)**
 - ASPA未対応ほか
 - ROAWebのUI改善
 - リポジトリ/パブリケーションサーバの堅牢性

- 2024年4月16日 障害報告：RPKIリポジトリの障害について
<https://www.nic.ad.jp/ja/topics/2024/20240416-01.html>
- 2025年2月27日 RPKIシステムリポジトリの高負荷状態について
<https://www.nic.ad.jp/ja/topics/2025/20250227-04.html>
- 2025年3月27日 JPNICのRPKIリポジトリで最新のデータが取得できない状況について
<https://www.nic.ad.jp/ja/topics/2025/20250327-01.html>

メッセージ

頂いたメッセージは個人の見解によるものであり、ご所属組織等を代表するものではないものとさせていただきます。また、将来に渡って何かを保証するものでもない点、ご了承ください。

中村修氏

インターネットは、インターネットを構成するすべてのネットワークが、“IPパケットの配送にはベストを尽くす！”というシンプルな“合意”に基づいて稼働している自律分散協調システムのネットワークです。

協調しない、もしくは悪意を持ってこの協調システムへの攻撃に対して、現在RPKIのデプロイメントが進行中です。すべてのネットワークがROVをする必要はありませんが、ROAの登録などすべてのネットワーク運用者が、RPKIを理解し、経路交換という最も重要な協調作業を成し遂げる必要があります。日本では、JPNICが音頭をとり、この活動を推進しています。

すべての人間にとってのライフラインであるインターネットを、安心して利用可能な情報インフラとして運用する責任は、お集まりいただいた皆様の協調作業が必要不可欠です。皆さんと共に頑張っていきましょう。

岡田雅之氏

長崎県立大学の岡田です。みなさんこんにちは。長崎に教員として赴任してから6年目になりました。学生と一から研究用ネットワークを構築してゆくことから初めて、人のネットワークも一緒に紡ぐことができてきたのかなとおもっています。皆様には釈迦に説法ですが、インターネットの根幹をなすBGPによる経路制御とそのセキュリティであるRPKIに関する技術に取り組むことは学習・研究だけでなく人のつながりを得ることにもつながり学生にも大変有意義です。このような取り組みに国内でイニシアティブをとるJPNICや関連組織の皆様と頑張っけてゆきたいです。

シェリル・ハリソン (Sheryl Harsono) 氏

ジョブ・スナイダース(Job Snijders)氏

ジョブ・スナイダースによる声明 — 国際的RPKI専門家より
=====

RPKIは日本のインターネット分野にとって極めて重要なシステムであり、国内外のルーティングインフラの安全性を高めています。JPNICが認証局およびRPKIデータ公開ポイント運用者として行ってきた取り組みに、感謝と敬意を表します。JPNICの努力によって、日本のISPやネットワークオペレーターの間でRPKIの普及が進みました。

近年、JPNICは日本のRPKI公開ポイントのレジリエンス（耐障害性）とパフォーマンスを大幅に向上させました。私が確認した改善点には、エンドポイント冗長性の強化、より高速なデータ配信を実現するHTTP構成の改善、RsyncとRRDPのアクセス方式を統一する最新のIETF標準の導入などがあります。

これらの改善が実現できたのは、JPNICの高度な専門知識と経験を持つスタッフのおかげだと認識しています。日本のRPKI公開ポイントの安定性は、グローバルなルーティング運用にも良い影響を与えています。JPNICのRPKI活動への投資を、引き続き日本のコミュニティの皆様にお願ひしたいと思います。

お疲れ様です！（日本語で）

菊池直輝氏

サイバー攻撃が多様化している昨今、グローバルアドレスを安全に運用する上でROV導入は不可欠です。
事業者間でROV導入が一層進むことで、安全で信頼性の高いネットワークの実現が期待されますし、期待しています。

グローバルアドレスを多数保有する我々ソフトバンクが積極的に取り組むことで、それらに大いに貢献できると考えています。
当社は2025年4月にROV導入が完了しました。引き続きRPKI/ROV等の普及促進に協力してまいります。

ディスカッション

ご発言は個人の見解によるものであり、ご所属組織等を代表するものではないものとさせていただきます。また、将来に渡って何かを保証するものでもない点、ご了承ください。

テーマ

- A) ROAの普及やROV導入
- B) JPNICやレジストリのRPKIシステム
- C) ルーティングセキュリティに関わる人材

よろしければ事前に頂いたコメントをご紹介します。

金子康行氏

2023年度に総務省のRPKI実証実験に参加し、自社のRPKI導入に向けた動きをスタートしましたが、その後諸事情あり、2025年4月ようやくROAを作成しました。ROA作成自体はそう難しい作業ではありませんが、万が一誤った形で作成してしまうと当社サービスに甚大な影響を与えてしまうため、非常に緊張しました。作業後の確認や切り戻しが容易でなかったり、実はJPNICさんのツールにバグがあってヒヤヒヤしたり、といったあたりの話は、8月22日のENOG87で詳しく発表する予定なので、ご興味のある方はぜひENOGにご参加ください！今後はROVの実装についても、検討を進めていきたいと思っています。

山口勝司氏

インターネットは生活にとって無くてはならない社会インフラとなりました。経路情報はインターネットを支える重要な要素であり、不正な経路情報による通信障害や犯罪によるセキュリティリスクを低減する必要性が世界的に高まっています。

日本国内ではROAの作成は進んでいるものの、ROVについては低調な状況が長らく続いてきました。しかし、2022～23年度にかけて総務省が行ったルーティングセキュリティに関する実証実験の事業の結果を反映した、ISPにおける不正経路対策ガイドラインが昨年度JPNICにより公開されました。これによりROV実施の機運が高まると共に、多くの事業者がROVに取り組みやすい状況になりつつあります。

BIGLOBEでは不正な経路情報への対策を行うことは、インターネット接続サービスを提供する事業者として今後必須となる重要な事項であると考え、取り組みを進めています。

具体的には、2022年度には自社が広報するIPアドレスのROA作成を完了し、2024年度～2025年度にかけてROVの実施に取り組んでいます。RPKIの技術には運用上の課題と考えられる点も幾つかあり、2023年度からISPにおけるROV実施のベストプラクティス、RPKIの信頼性向上をテーマとした研究を大学と共に継続して行っています。将来的には研究の成果をインターネット運用コミュニティに何らかの形で公開し、日本でのROVの推進にわずかながら寄与できればと考えております。

RPKIの技術はより多くのASが導入することにより、インターネット全体で大きな効果を発揮します。日本国内でも今後多くの事業者でROVが行われるようになり、より安全なインターネットが実現することを期待しております。

3つの中から選んでお話ください。

A) ROAの普及やROV導入

B) JPNICやレジストリのRPKIシステム

C) ルーティングセキュリティに関わる人材

おわり



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

Copyright © Japan Network Information Center ▶ 32

お持ち帰り情報

- RPKIパブリケーションサーバの増強設備が稼働中(5/28～)
- RPKIの”効果検証”が始まります。
- 技術検証環境GKKは次回のJANOG56@島根にて詳細の発表を予定しています。

ご連絡先： RPKI担当 rpki-query@nic.ad.jp