RPKI トピック

2020年11月27日(金)

木村泰司

発表者

名前	木村泰司
所属	日本ネットワークインフォメーションセンター(JPNIC)
担当	RPKI/認証局/セキュリティ/国際動向 IETF APNIC
業務	企画/開発/運用/ユーザサポート/調査/普及啓発
関係組織/団体	• WIDEプロジェクト • 慶応義塾大学 • JNSA PKI相互運用技術WG • フィッシング対策協議会 技術・制度検討WG • セキュリティ・キャンプ講師

内容

- トピック
- ROAの動向と効果について
- 新しいROAWeb

ROV = Route Origin Validation / ROAを使ったBGP経路の検証のこと

トピック

ROVへ

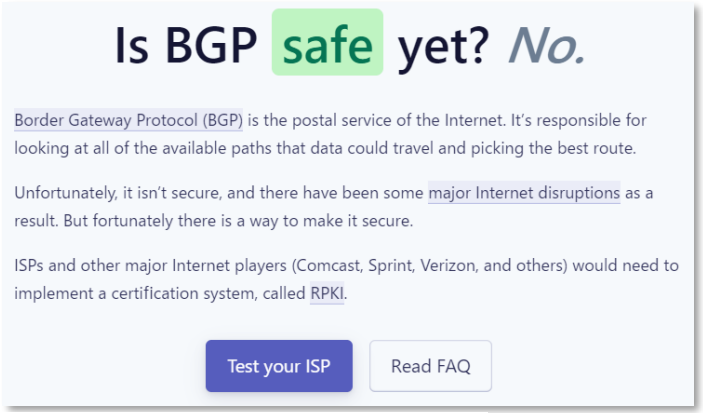
チェックツール

- **RPKI TEST**

ROVを導入しさえすれば
いいわけではないが…

RPKI TEST - RIPE Labs
https://labs.ripe.net/Members/nathalie_nathalie/rpki-webtest

- **Is BGP safe yet? No.**



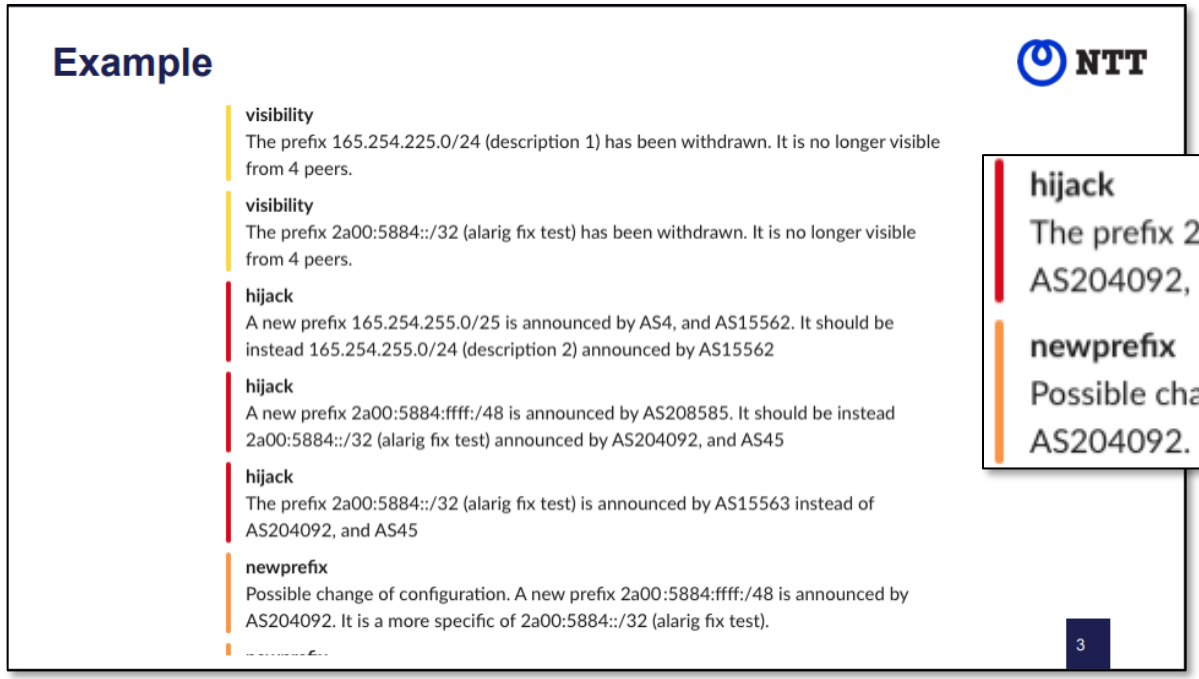
Is BGP safe yet? · Cloudflare
https://isbgpsafeyet.com/

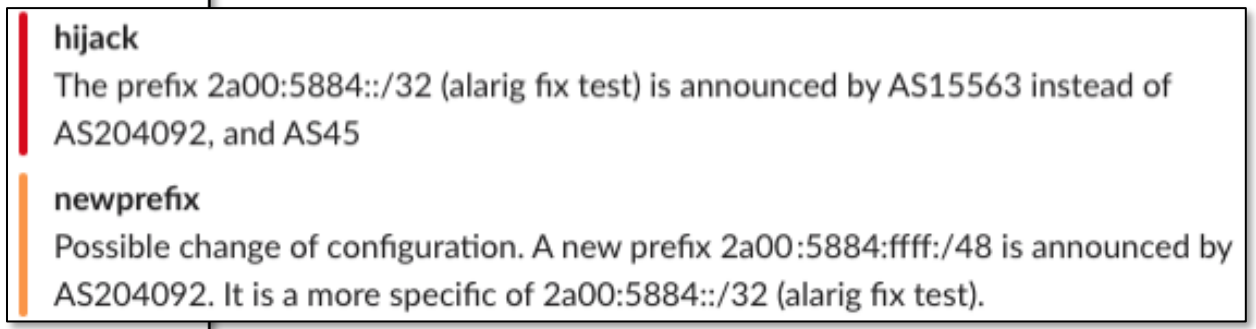
URLのQRコード(お試し用)

https://isbgpsafeyet.com/

通知ツール

- **BGPalerter**





BGPalerter, Real-time BGP monitoring, Massimo Candela
https://ripe79.ripe.net/presentations/111-BGPalerter_ripe79.pdf

roamon (後述)と同じ通知のコンセプト！

可視化ツール

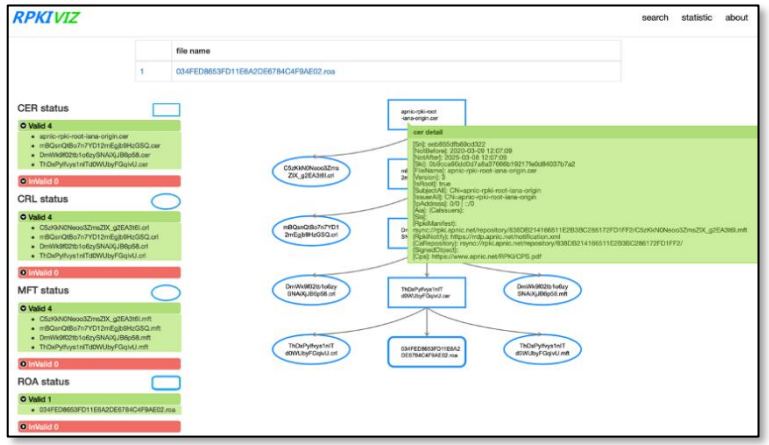
検索よりブラウズ向き？

- **console.rpki-client.org**

console.rpki-client.org
http://console.rpki-client.org/

例示されている /AS8283.html

- **RPKIVIZ**



RPKIVIZ | RPSTIR2
http://rpkiviz.zdns.cn/

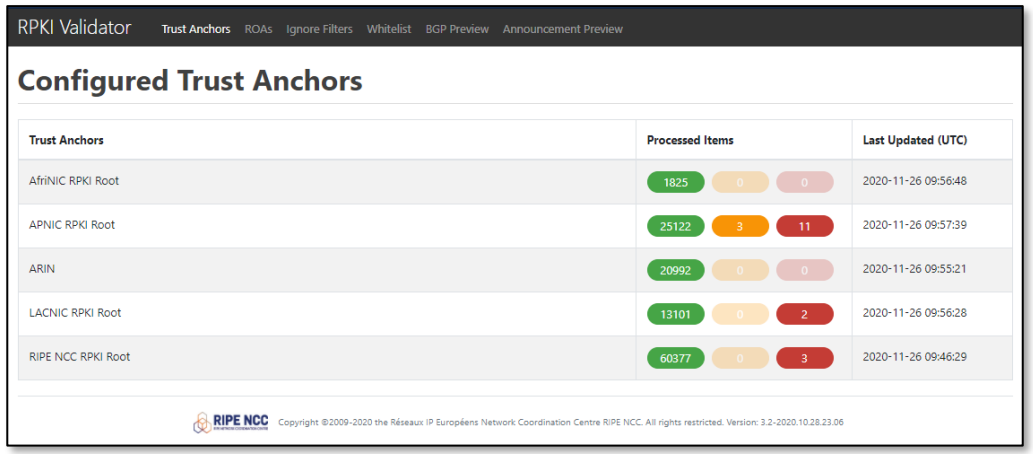
RPKIVIZ: Visualizing the RPKI | APNIC Blog
https://blog.apnic.net/2020/04/23/rpkiviz-visualizing-the-rpki/

障害の調査にも

RPKI Validatorは…

Webインターフェースを持つキャッシュサーバの今後は！？

- **2021年に開発終了へ**



RPKI Validator - Quick Overview of BGP Origin Validation
https://rpki-validator.ripe.net/trust-anchors

RPKI Validator 日本語版 (RIPE NCCスタッフと相談し日本語化)
http://roa2.nic.ad.jp:8080

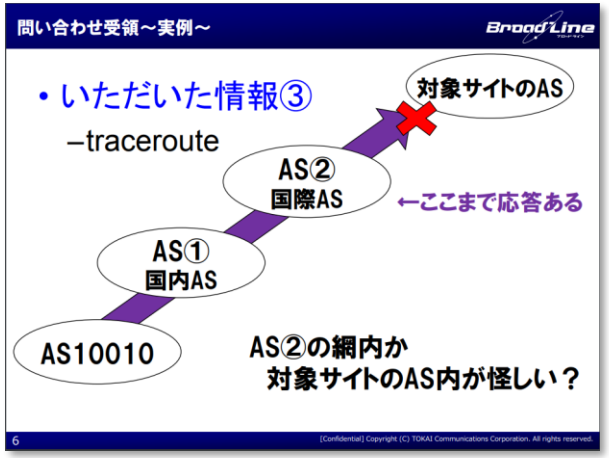
2021年1月1日　新しい機能の受け入れと開発を終了
2021年3月1日　新しいRFCとRIRのポリシー実装を終了
2021年7月1日　全体のメンテナンスを終了しアーカイブ

Lifecycle of the RIPE NCC RPKI Validator, Nathalie Trenaman — 20 Oct 2020　より
https://labs.ripe.net/Members/nathalie_nathalie/life-cycle-of-the-ripe-ncc-rpki-validator-1

IETF sidropsで様々な標準化が進み、セキュアな実装やメンテナンスが負担に。今後はCAに注力。

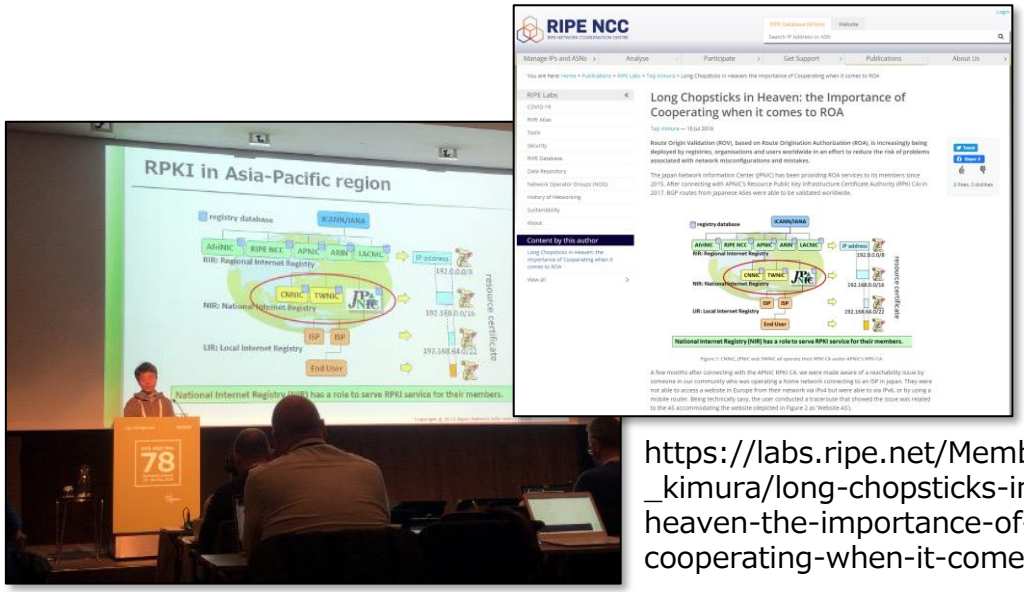
これまでのお話

IW2018: “ほんとにあったRPKIの話”, 杉山 亮太, TOKAI コミュニケーションズ



ほんとにあったRPKIの話, IWショーケース仙台
https://www.nic.ad.jp/sc-sendai/program/iwsc-sendai-d1-7.pdf

RIPE78: “Long chopsticks in heaven - When packets dropped using ROA -”, RIPE78, May 2019, Taiji Kimura

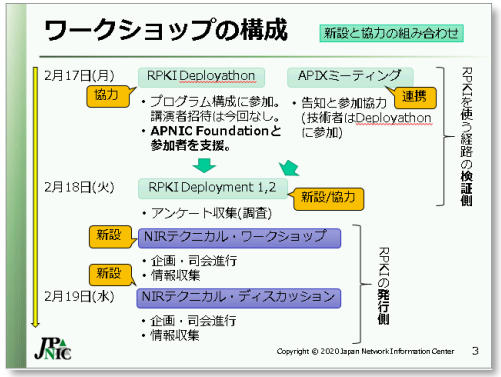


https://labs.ripe.net/Members/taiji_kimura/long-chopsticks-in-heaven-the-importance-of-cooperating-when-it-comes-to-roa

(掲載) RIPE 79でのIPアドレス・AS番号分配ポリシーに関する提案ご紹介 https://blog.nic.ad.jp/2019/3348/

roamonを開発。

APRICOT 2020/APNIC 49カンファレンスで発表。
RPKI slack の開始。



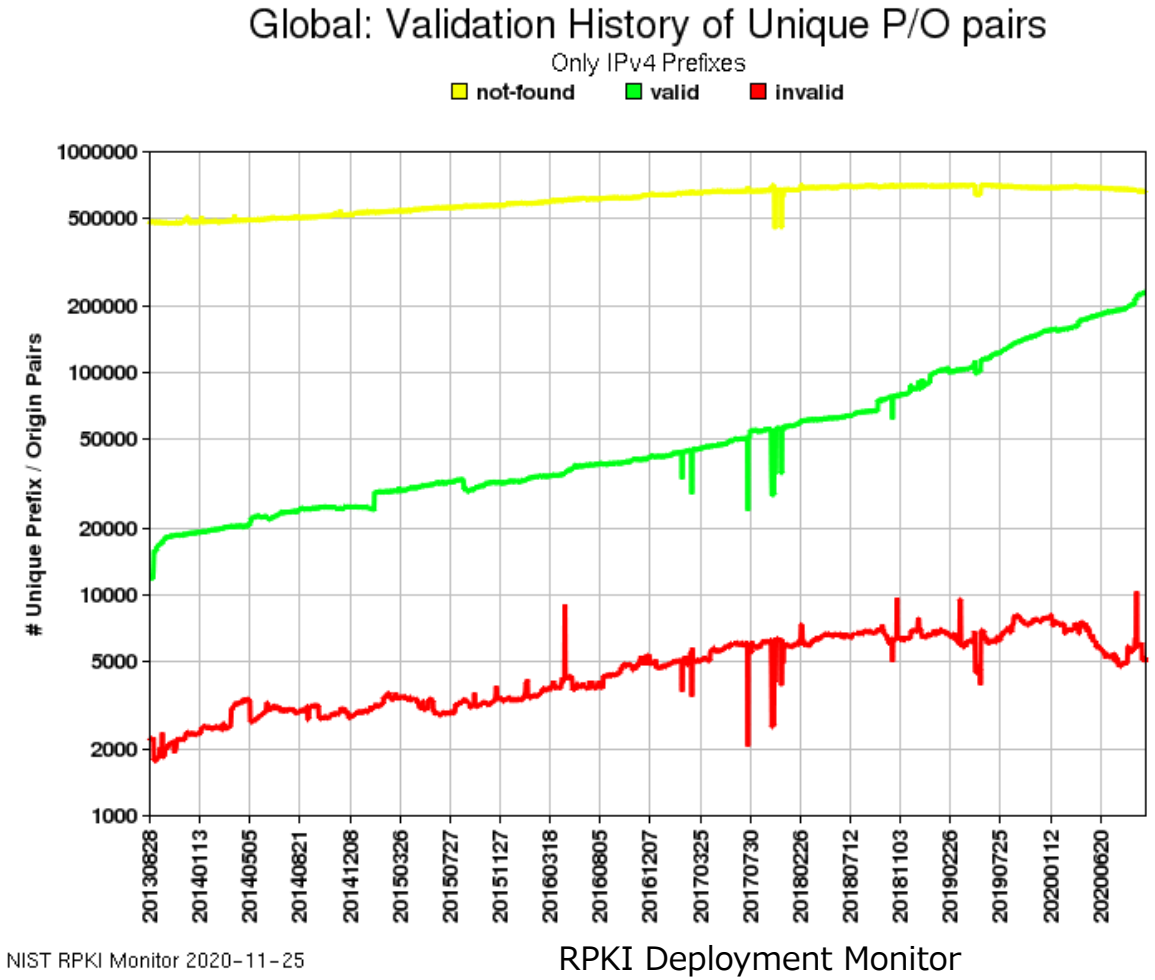
roamon

- JPNICで大学生と共同で開発したコンセプト実装
  roamon-verify, roamon-alert, roamon-web
- できること
  - **$ python3 roamon_verify_controller.py get --all**
    BGP経路(RouteViews)とRoutinator生成のVRPをダウンロード。
  - **$ python3 roamon_verify_controller.py rov --ip <prefix...>**
    指定されたIPアドレス・プレフィックスに対するROV結果を表示。
  - **$ python3 roamon_verify_controller.py rov --asn <AS番号...>**
    コマンドで指定されたASをオリジンASとするすべての経路についてROV結果を表示。
- 入手方法（詳細は下記）

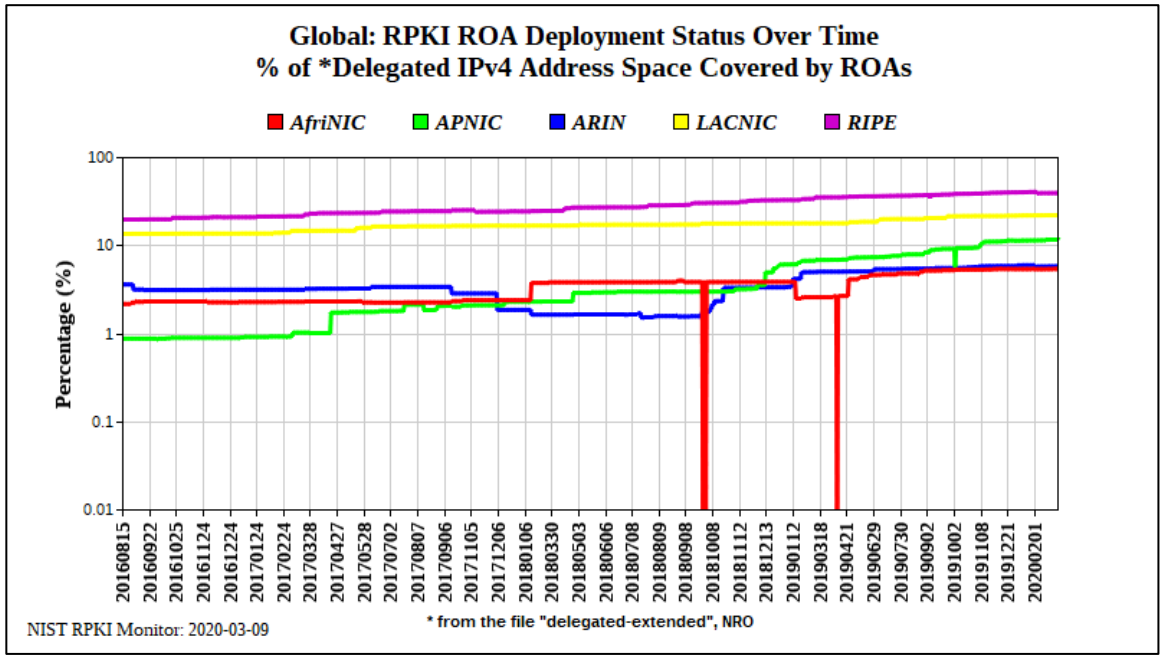
  $ git clone https://github.com/taiji-k/roamon-verify.git

ROAの動向と効果について

ROV valid (有効) 数の増加



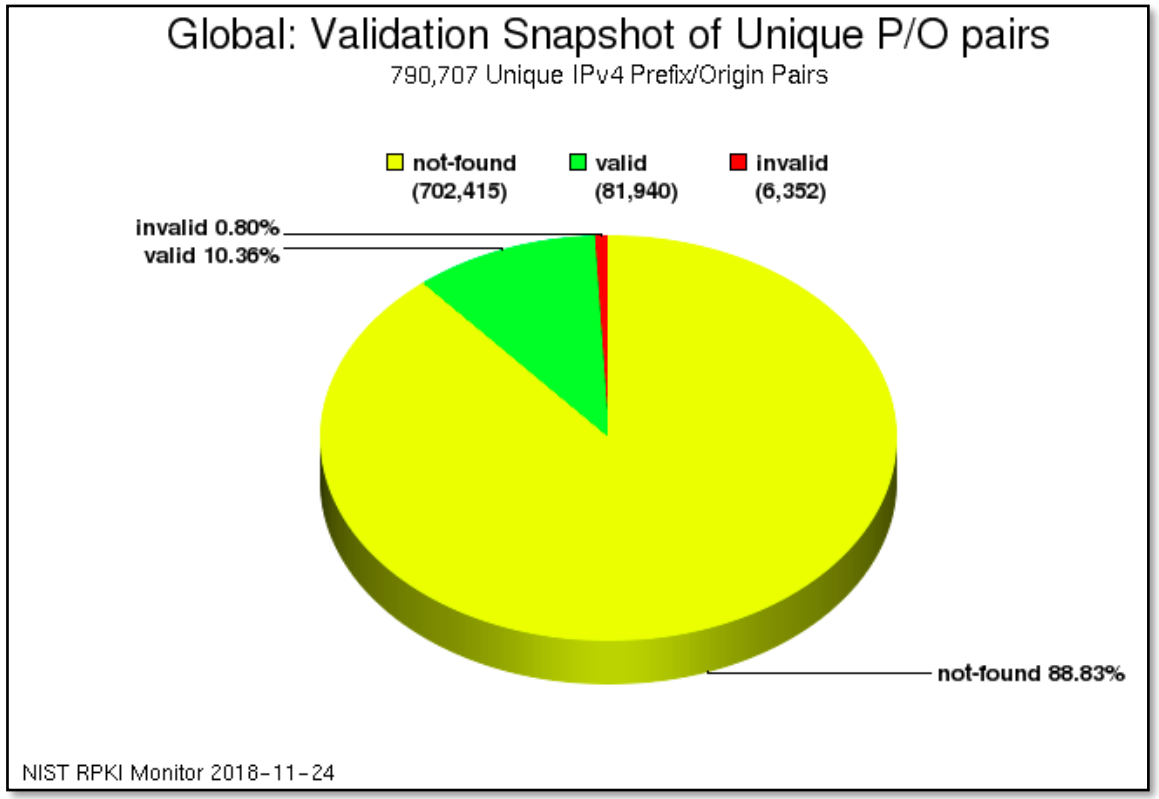
RPKI Deployment Monitor
https://rpki-monitor.antd.nist.gov/



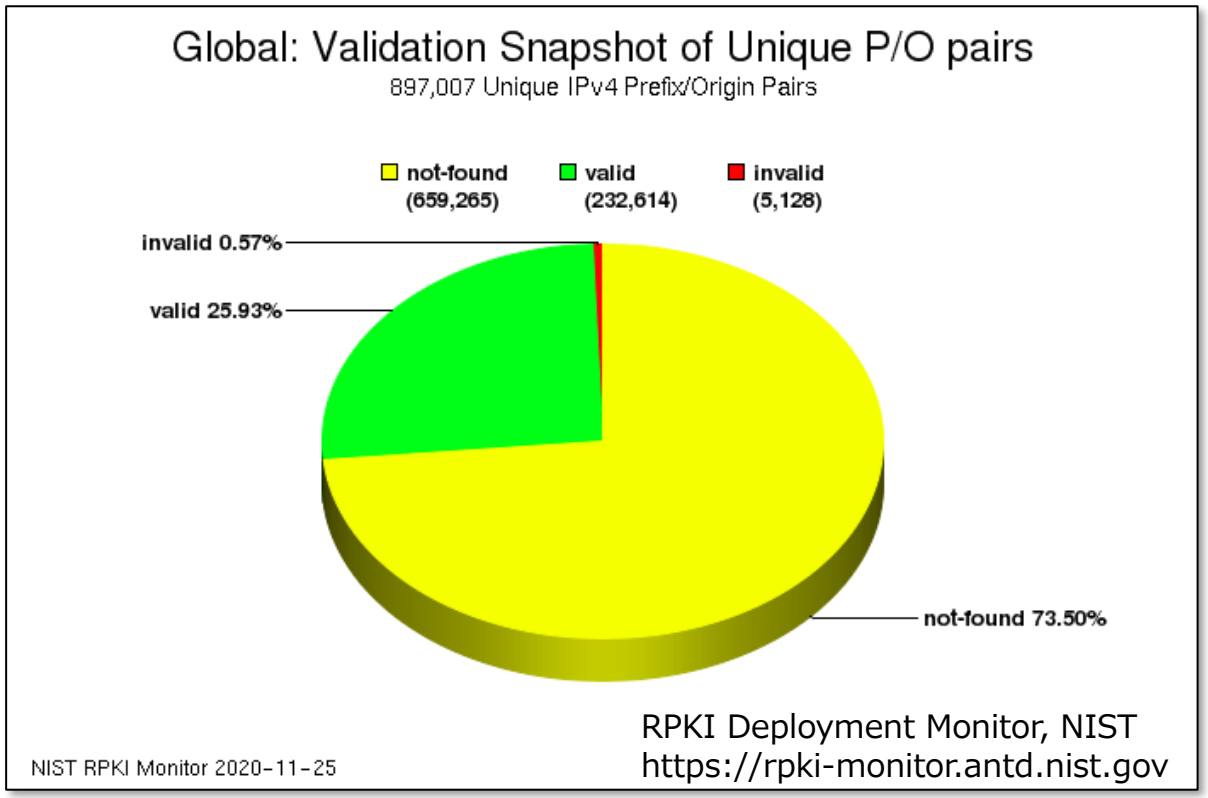
依然、RIPE地域のROA数が多い。
APNIC地域も増加中。

NIST RPKI Monitorより

2018年



2020年



RPKI Deployment Monitor, NIST
https://rpki-monitor.antd.nist.gov

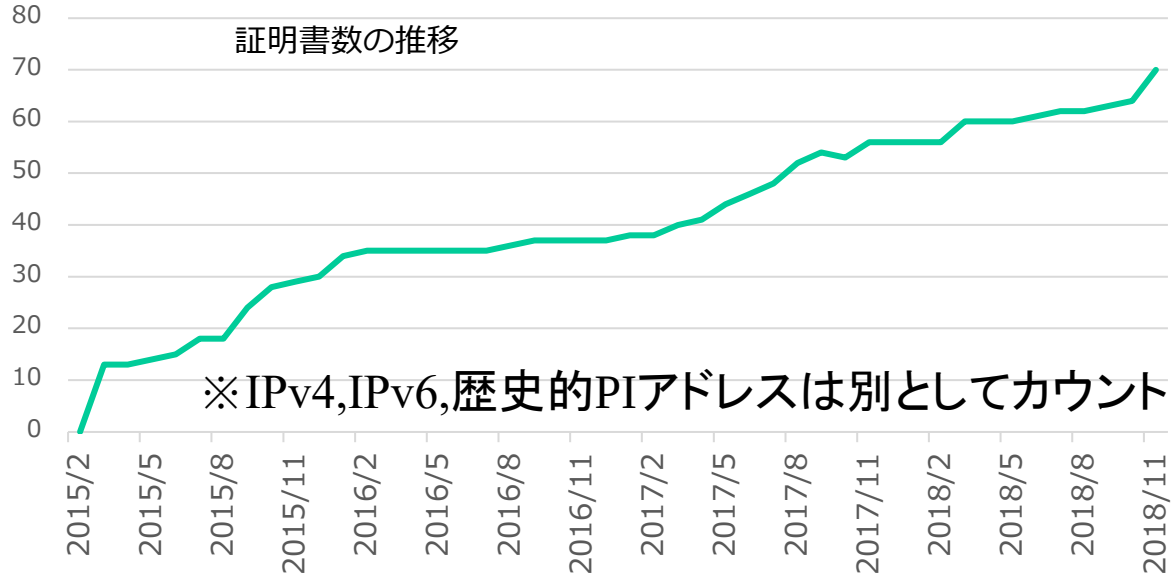
- **Invalid:AS** Covering ROA Prefix, maxLength Satisfied, and AS Mismatch.
- **Invalid:ML** Covering ROA Prefix, maxLength Exceeded, and AS Match.
- **Invalid:ML-AS** Covering ROA Prefix, maxLength Exceeded, and AS Mismatch.
- **Invalid:AS-SET** The origin AS could not be determined from the BGP update used to announce the prefix (i.e., because it contains an AS-SET), and a ROA covering the prefix exists.

二年前に比べて明らかにカバー率が増加。大手事業者のROV導入も鍵か。

JPNICのRPKI試験提供

2018年11月

- アドレスホルダ毎に発行される証明書数
  - 70
- 発行されているROA
  - 256
- 割り振られているIPアドレスに対してROAがカバーする割合
  - 3.5% IPv4
  - 38.1% IPv6



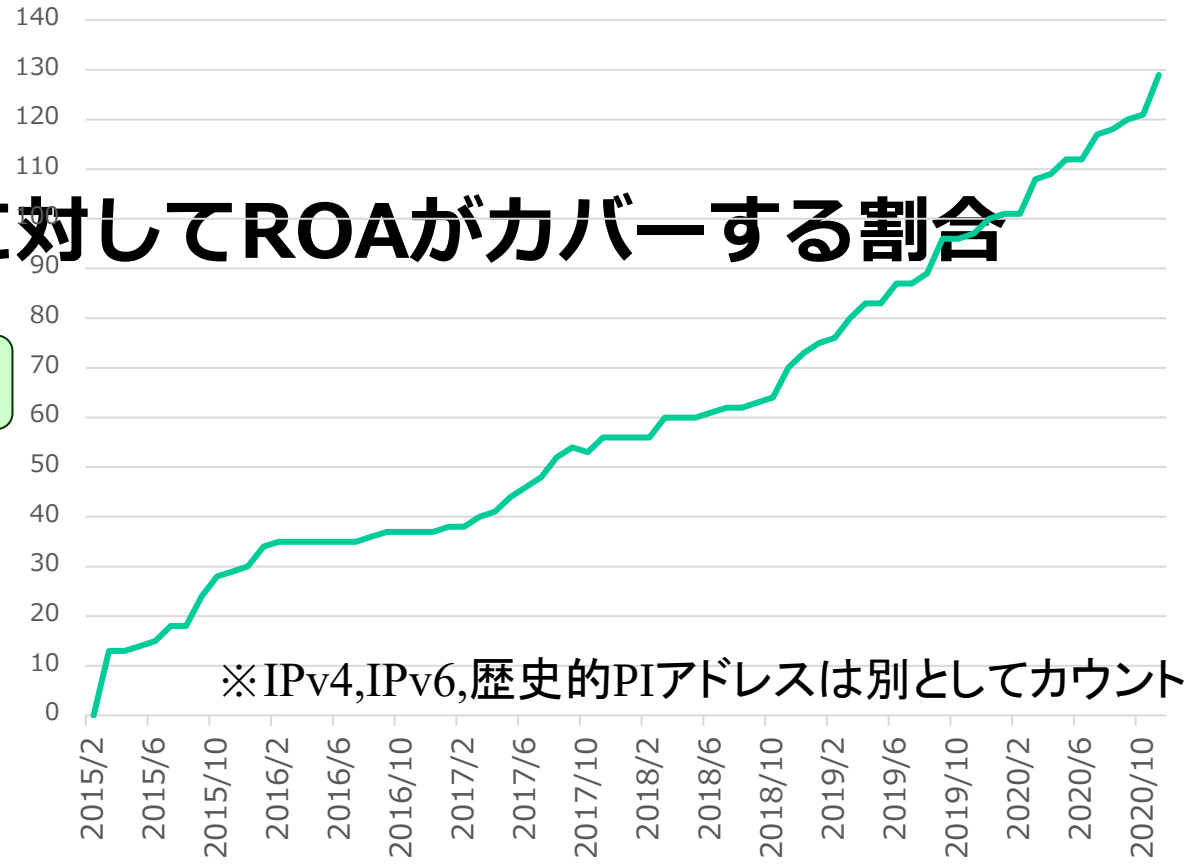
JPNICのRPKI試験提供

2020年11月

- **アドレスホルダ毎に発行される証明書数** *正確にはハンドル数
  - 129
- **発行されているROA**
  - 721 *新ROAWebでは更に多い。
- **割り振られているIPアドレスに対してROAがカバーする割合**
  - 43.6% IPv4
  - 57.4% IPv6

気が引き締まる数字に

IPアドレスの分配を多く受けている**20社**のうち、**7社**が利用を開始。(テストを含む)



新しいROAWeb

画面と変更点(1/3) - ログイン不要のトップ画面

＞　RPKIシステムにアクセス　＜

こちらをクリックすると新しいROAWebにアクセスします。

国内テスト用のRPKIシステムにアクセス（*1）

こちらをクリックするとJPNICのTALを使わないと辿れないROAを発行するROAWebにアクセスします(従来のROAWeb)。

画面と変更点(2/3) - 新しいROAWeb

「ROAの即時作成・即時削除」

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。

観測されているBGP経路（Prefixと経路広告元のAS）

一部、表示できないBGP経路も。

6M28JKbDxTC5mBWue1wNo--KhNU.cer
発行済
2021年11月15日10:30:02 (日本時間/UTC+9)
192.41.192.0/24
is2rHh6mM7qK0Yoqy3I2DpKAxLY.cer
発行済
2021年11月15日10:30:02 (日本時間/UTC+9)
202.12.30.0/24

「複数のリソース証明書表示」

画面と変更点(3/3) - まとめ

- **ログイン不要のトップ画面**
  - 従来は直接ログイン後の画面にアクセスする形になっていました。（証明書を使っているためパスアワード入力画面などがない。）
  - 新しい画面では、お知らせや国内テスト用のRPKIシステムにアクセスできます。
- **ROAの即時作成・即時削除**
  - 従来はご利用いただいているROAWebからの「同期」によってROAが国際的に参照可能になっていました。作成から数時間のタイムラグがありました。今後は数分間後には公開状態になります。
- **複数のリソース証明書表示に対応**
  - 一つのアカウントでもAPNICからは複数のリソース証明書が発行されています。トラブルシューティングのため個々に表示しています。

使い方の例

「ROAを新規作成したい。」

ROAを作るIPアドレスを選ぶ。 → ROAwebでROAを作る。 → 状態が「公開済」になる。 → 世界の色々なキャッシュサーバを使って状態を確認する。

何か異常があると「処理中」のままになる。

3分～5分

3時間～1日

「経路を変更したい。」

現在の経路と変更後の経路を確認する。 → ROAwebでROAを変更する。 → 状態が「公開済」になる。 → 世界の色々なキャッシュサーバを使って状態を確認する。

RPKI Validator 日本語版でも確認もできます。(即時の検証しなおしに20分程度かかります。)
ご連絡ください。

おわり

JPNIC RPKI担当
rpki-query at nic.ad.jp

RPKIのはじめ方

資源管理者証明書を準備（資源管理カード／ブラウザ内）

申請における認証について
https://www.nic.ad.jp/ja/ip/id-procedure.html

↓

資源申請者証明書を担当者に発行（ブラウザ内）

資源申請者証明書発行マニュアル
https://www.nic.ad.jp/doc/issue-manual-02.pdf

↓

リソース証明書とROAの発行開始

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

↓

発行完了！

お問合せ窓口： ip-service@nir.nic.ad.jp
（または rpki-query@nic.ad.jp）

JPNICのRPKIまとめ

- **試験提供サービス**

  https://www.nic.ad.jp/ja/rpki/

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

  - IPアドレスの割り振りを受けている方がROAを登録したりRPKIのCAを立ち上げてつなげたりできる。
- **ROAキャッシュサーバ**

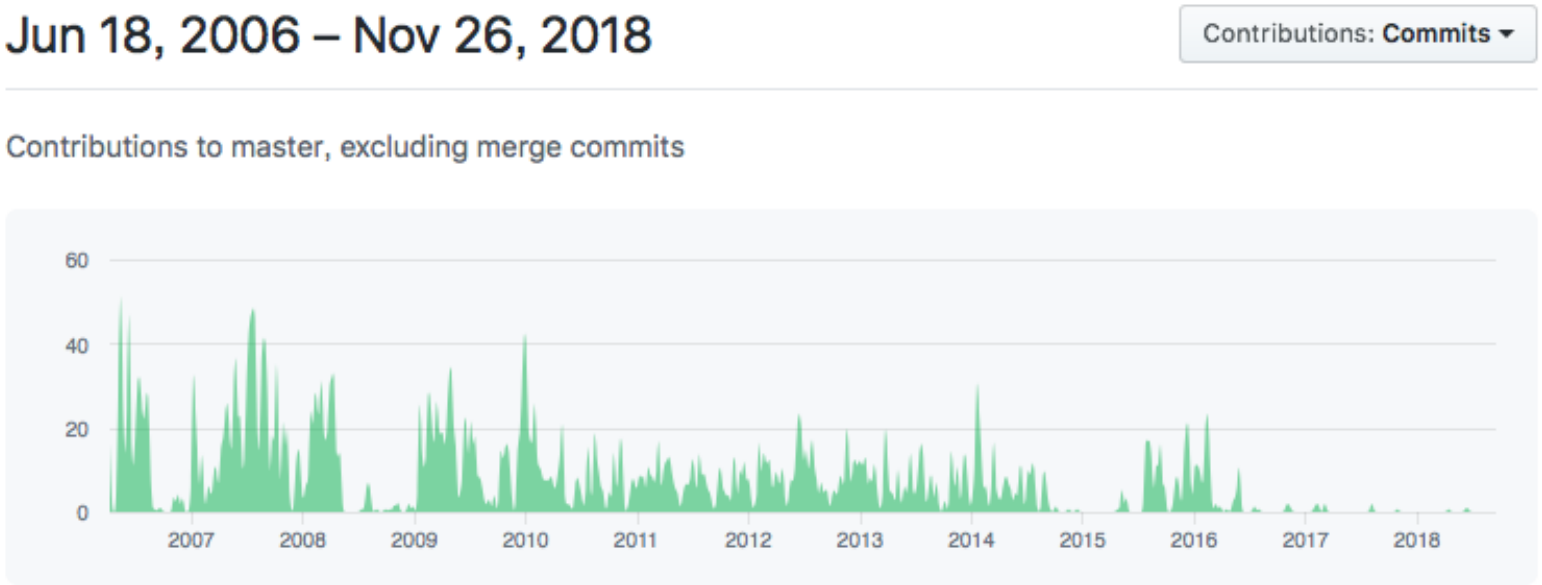
  192.41.192.218　port　323
- **日本語版RPKI Validator**

  http://roa2.nic.ad.jp:8080/
- **JPNICのTrust Anchor**

  https://serv.nic.ad.jp/rpki/jpnic-preliminary-ca-s1.tal

リソースCAの実装

- **RPKI Tools**
  - https://github.com/dragonresearch/rpki.net



https://github.com/dragonresearch/rpki.net/graphs/contributors
© 2018 GitHub, Inc.

ROAキャッシュの実装

- **RPKI Tools**
  - 情報と入手元　1つ前のスライドと同じ
- **RPKI Validator**
  - https://github.com/RIPE-NCC/rpki-validator
- **RPSTIR**
  - https://github.com/bgpsecurity/rpstir
- **ROUTINATOR**
  - NLnetLabs/routinator
    https://github.com/NLnetLabs/routinator

BGPルータ

- **Cisco “BGP - Origin AS validation”**
  - Cisco Feature Navigatorより
    IOS XE - ISR 4451-X, ASR1002-Xほか
    IOX - ME3800, 7201ほか
- **Juniper “Origin Validation for BGP”**
  - Juniper Feature Explorerより
    EX9200 - Junos OS 12.3R2, M7i - Junos OS 13.2R2, vMX - Junos OS 14.1R5ほか
- **Nokia(旧Alcatel-Lucent)**
  - SR OS 12.0.4R以降

BGPルータ

- **VyOS**
  https://www.vyos.io/
  - ROVの考え方の理解に最適
- **NIST BGP Secure Routing Extension (BGP-SRx / BGPSEC-IO)**
  https://www-x.antd.nist.gov/bgpsrx/
  - ASパス検証に対応
- **BIRD BGPsec**
  http://bird.network.cz/
  http://www.securerouting.net/tools/bird/
  - ASパス検証に対応
- **FRRouting**
  https://github.com/FRRouting/frr
  - オリジン検証に対応

BGPルータ

- **GoBGP**

  https://osrg.github.io/gobgp/

  https://github.com/osrg/gobgp/

  - オリジン検証に対応

その他 - Webブラウザ

- **機能**
  - WebサーバのIPアドレスがROAに入っているかどうかを確認し、オリジン検証の結果を表示する。

- **Firefox addon**
  - rtrlib/firefox-addon
    https://github.com/rtrlib/firefox-addon
- **Chrome 拡張**
  - rtrlib/chrome-extension
    https://github.com/rtrlib/chrome-extension