

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	<ul style="list-style-type: none">• 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

トピック

ROVへ

チェックツール

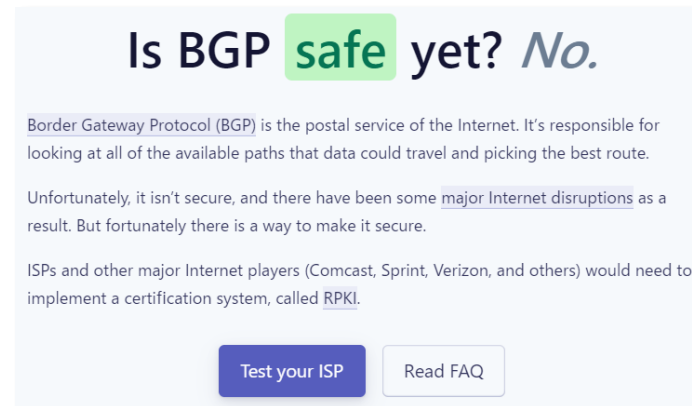
- RPKI TEST



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

Example

visibility
The prefix 165.254.225.0/24 (description 1) has been withdrawn. It is no longer visible from 4 peers.


visibility
The prefix 2a00:5884::/32 (alarig fix test) has been withdrawn. It is no longer visible from 4 peers.


hijack
A new prefix 165.254.255.0/25 is announced by AS4, and AS15562. It should be instead 165.254.255.0/24 (description 2) announced by AS15562

hijack
A new prefix 2a00:5884:ffff:/48 is announced by AS208585. It should be instead 2a00:5884::/32 (alarig fix test) announced by AS204092, and AS45

hijack
The prefix 2a00:5884::/32 (alarig fix test) is announced by AS15563 instead of AS204092, and AS45

newprefix
Possible change of configuration. A new prefix 2a00:5884:ffff:/48 is announced by AS204092. It is a more specific of 2a00:5884::/32 (alarig fix test).





hijack
The prefix 2a00:5884::/32 (alarig fix test) is announced by AS15563 instead of AS204092, and AS45

newprefix
Possible change of configuration. A new prefix 2a00:5884:ffff:/48 is announced by AS204092. It is a more specific of 2a00:5884::/32 (alarig fix test).

roamon (後述)と同じ通知のコンセプト!

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

可視化ツール

検索よりブラウザ向き？

- console.rpki-client.org



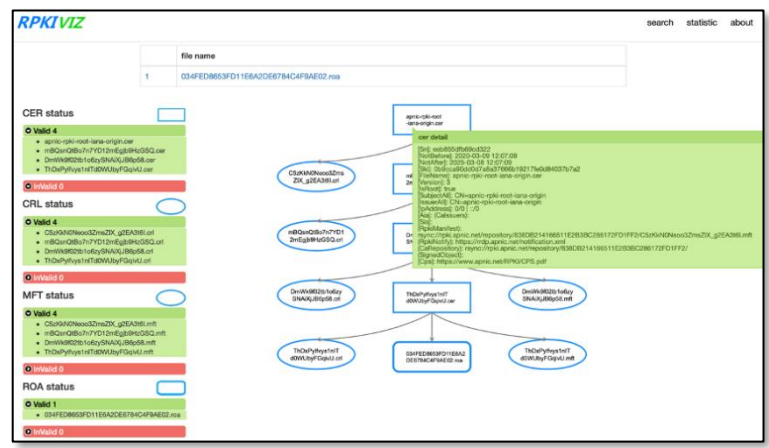
console.rpki-client.org
http://console.rpki-client.org/

Generated at Thu Nov 26 08:45:29 2020 by raki-client.

SIA	asID	Prefixes
rpki.rpki-net/repository/DEFAULT/3b/2434f8-0508-45fc-b714-31a3ecf1bd86/1/W00KvaEksa[540fRGA_eLPjY8nk-rea	AS8283	1: 91.208.34.0/24 (max: 24)
rpki.rpki-net/repository/DEFAULT/54/42b179-4790-4520-b174-50505392f472/1/AY7ne8K_0Ge70e1299j7W58Res-rea	AS8283	1: 94.142.242.0/24 (max: 24)
		2: 94.142.240.0/21 (max: 21)
		3: 94.142.241.0/24 (max: 24)
		4: 94.142.245.0/24 (max: 24)
		5: 94.142.246.0/24 (max: 24)
		6: 94.142.244.0/24 (max: 24)
		7: 94.142.247.0/24 (max: 24)
		8: 185.52.225.0/24 (max: 24)
		9: 185.52.226.0/24 (max: 24)
		10: 185.52.224.0/24 (max: 24)
		11: 185.52.227.0/24 (max: 24)
		12: 185.52.227.0/24 (max: 24)
		13: 94.142.248.0/24 (max: 24)
		14: 2a02:888::/32 (max: 32)
rpki.rpki-net/repository/DEFAULT/3b/31ad-f4a3-4ad5-909a-a853977b6457/1/Bz8eZ8dLl_49Rc8NPdruh0YAXX9-rea	AS8283	1: 185.114.12.0/24 (max: 24)
rpki.rpki-net/repository/DEFAULT/ca/1d2fd-4dbd-4362-ac7b-7a3ff1b00b716/1/9_-LdixteccendZn-yW5ex3TMM-rea	AS8283	1: 2001:678:688::/48 (max: 48)
rpki.rpki-net/repository/DEFAULT/48/1a1786-f497-44b0-aa98-c582350a73f1/1/30Ez5SahnN94980P1Ca1TP1Yaik-rea	AS8283	1: 45.154.24.0/24 (max: 24)
		2: 45.154.24.0/22 (max: 22)
		3: 45.154.25.0/24 (max: 24)
		4: 45.154.26.0/24 (max: 24)
		5: 45.154.27.0/24 (max: 24)
		6: 2w0f:ca100::/32 (max: 32)
rpki.rpki-net/repository/DEFAULT/eb/f413c2-c2ec-41f1-9d85-5d8634eb7d91/1/Be0w5SOMP9eCrGakrILKSz1ZbF-rea	AS8283	1: 45.141.28.0/22 (max: 22)
		2: 2a02:c801::/29 (max: 29)

例示されている /AS8283.html

- RPKIVIZ



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

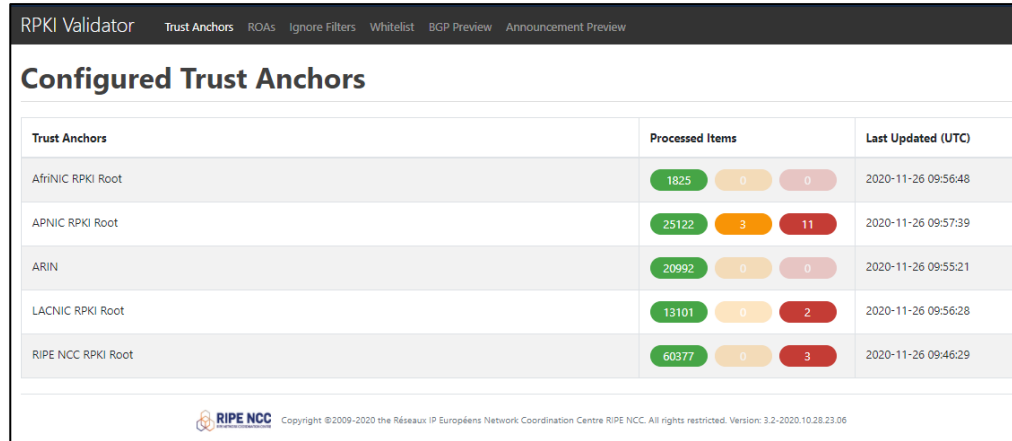
RPKIVIZ | RPSTIR2
http://rpkiviz.zdns.cn/

障害の調査にも

RPKI Validatorは…

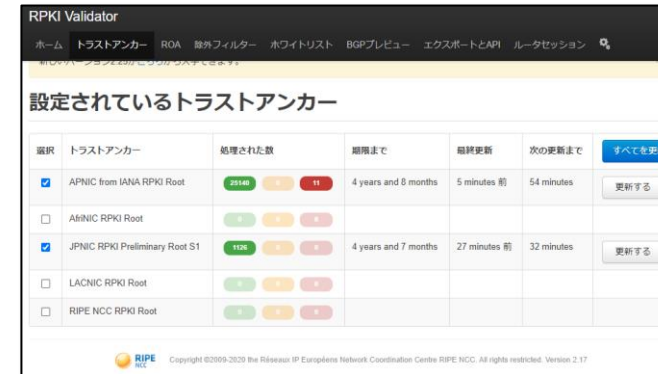
Webインターフェースを持つキャッシュサーバの
今後は！？

- 2021年に開発終了へ



Trust Anchors	Processed Items	Last Updated (UTC)
AfriNIC RPKI Root	1825 0 0	2020-11-26 09:56:48
APNIC RPKI Root	25122 3 11	2020-11-26 09:57:39
ARIN	20992 0 0	2020-11-26 09:55:21
LACNIC RPKI Root	13101 0 2	2020-11-26 09:56:28
RIPE NCC RPKI Root	60377 0 3	2020-11-26 09:46:29

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



選択	トラストアンカー	処理された数	期限まで	最終更新	次の更新まで	すべてを更新
<input checked="" type="checkbox"/>	APNIC from IANA RPKI Root	25140 3 11	4 years and 8 months	5 minutes 前	54 minutes	更新する
<input type="checkbox"/>	AfriNIC RPKI Root	1825 0 0				
<input checked="" type="checkbox"/>	JPNIC RPKI Preliminary Root S1	1126 0 0	4 years and 7 months	27 minutes 前	32 minutes	更新する
<input type="checkbox"/>	LACNIC RPKI Root	13101 0 2				
<input type="checkbox"/>	RIPE NCC RPKI Root	60377 0 3				

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



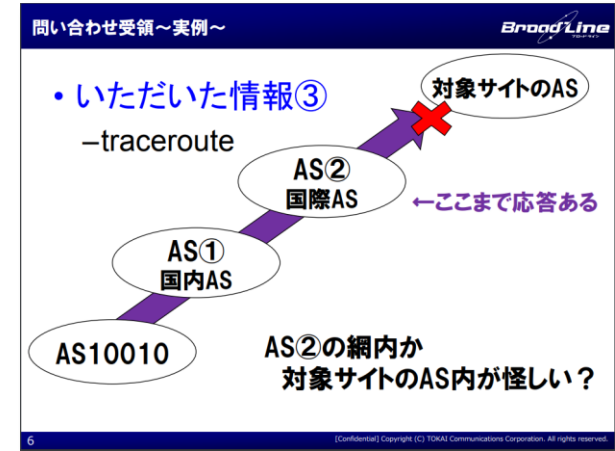
RIPE78: “Long chopsticks in heaven - When packets dropped using ROA -”, RIPE78, May 2019, Taiji
Kimura



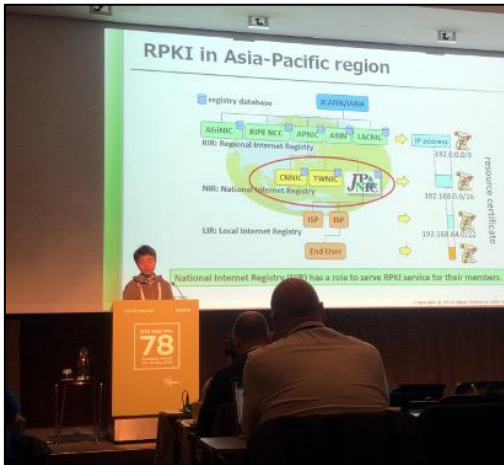
roamonを開発。



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

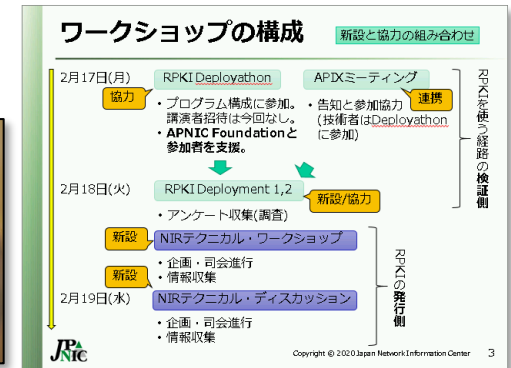


ほんとにあったRPKIの話, IWショーケース仙台
<https://www.nic.ad.jp/sc-sendai/program/iwsc-sendai-d1-7.pdf>



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/>



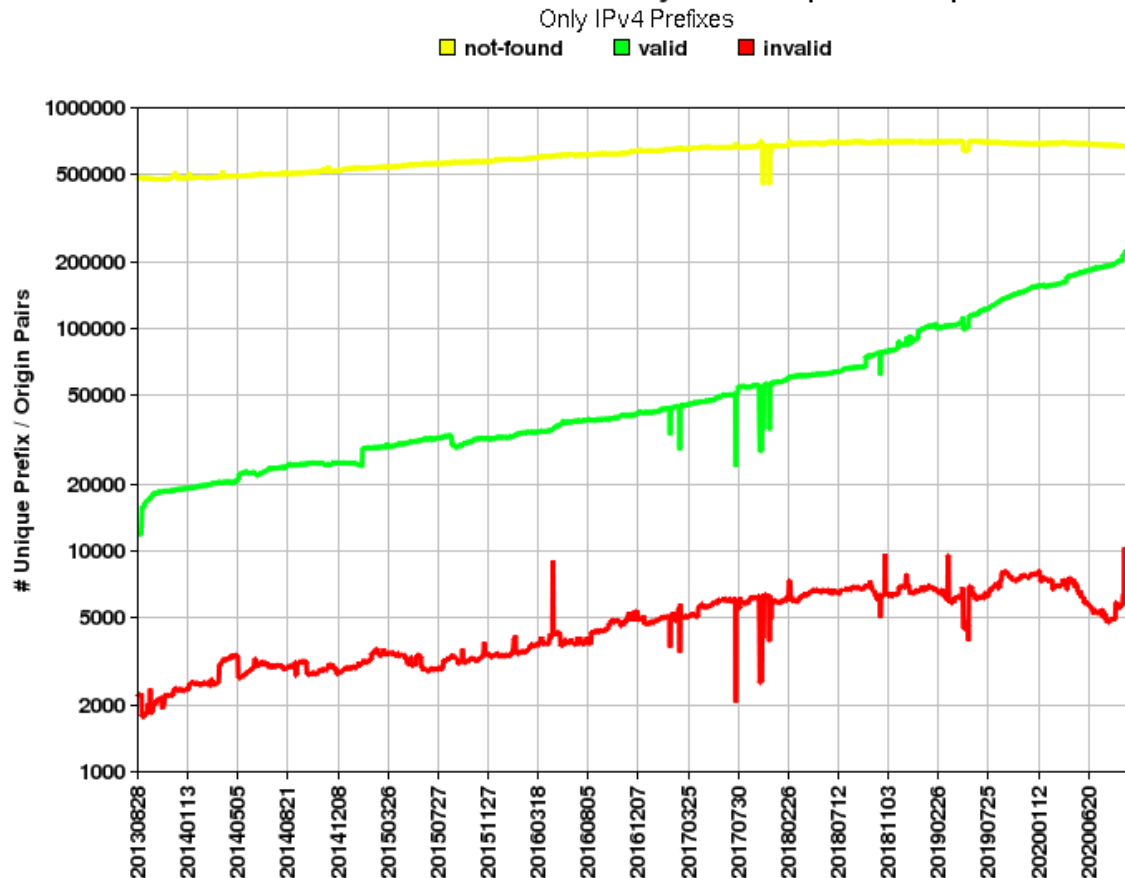
roamon

- 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

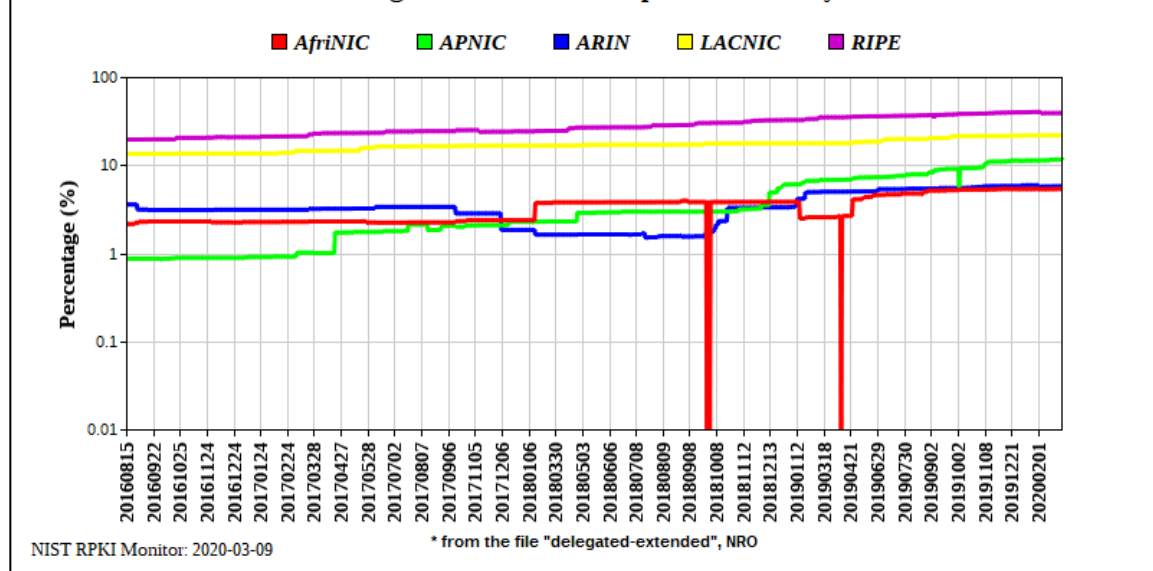
Global: Validation History of Unique P/O pairs



NIST RPKI Monitor 2020-11-25

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

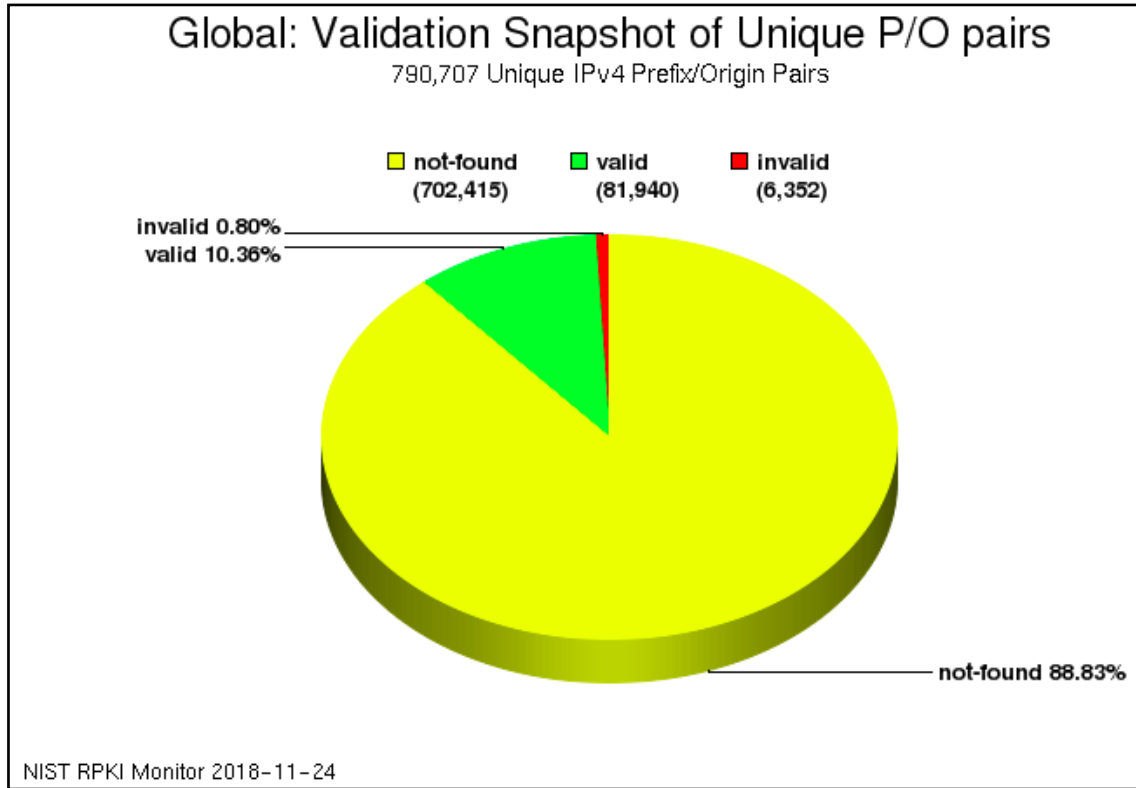
Global: RPKI ROA Deployment Status Over Time
 % of *Delegated IPv4 Address Space Covered by ROAs



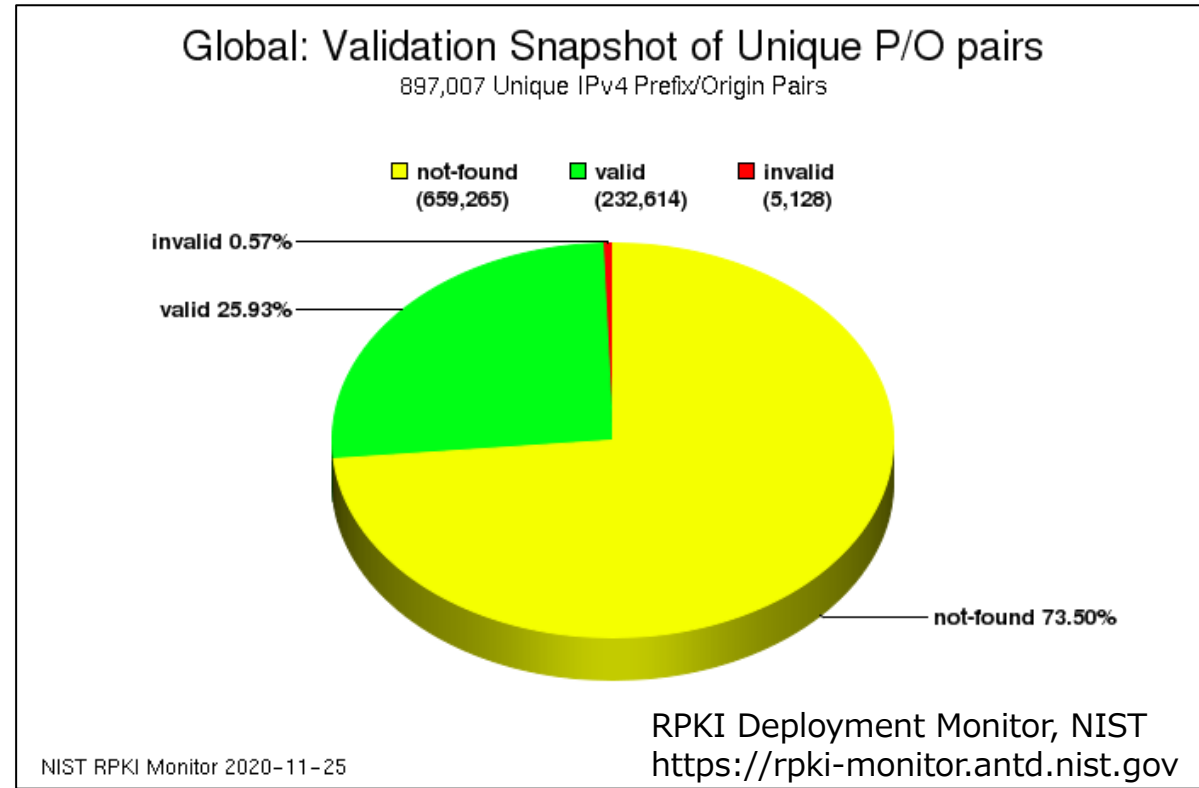
**依然、RIPE地域のROA数が多い。
 APNIC地域も増加中。**

NIST RPKI Monitorより

2018年



2020年

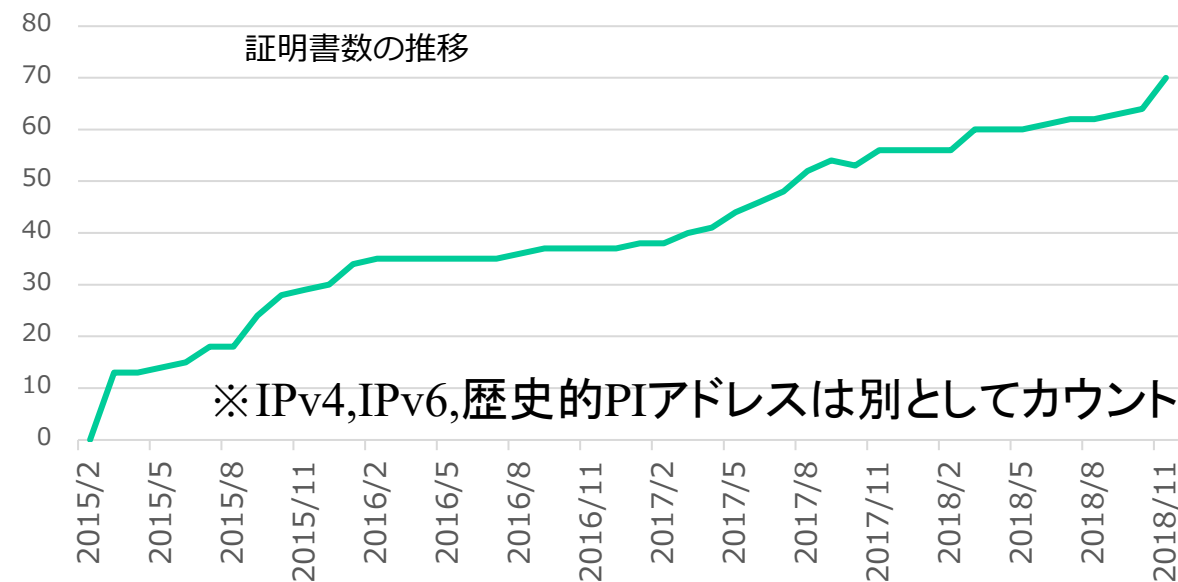


- **Invalid:AS** Covering ROA Prefix, maxLength Satisfied, and AS Mismatch.
- **Invalid:ML** Covering ROA Prefix, maxLength Exceeded, and AS Match.
- **Invalid:ML-AS** Covering ROA Prefix, maxLength Exceeded, and AS Mismatch.
- **Invalid:AS-SET** The origin AS could not be determined from the BGP update 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。



- **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

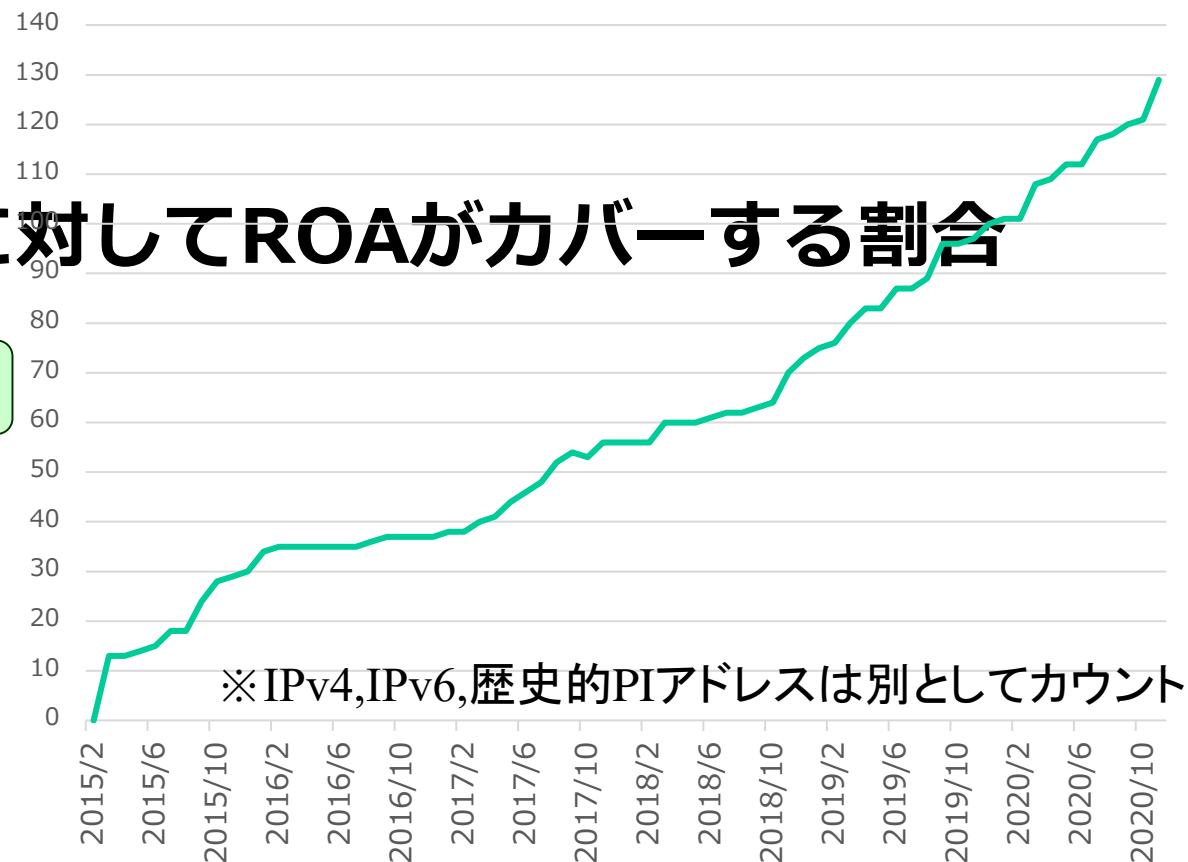




- **アドレスホルダ毎に発行される証明書数** *正確にはハンドル数
 - 129
- **発行されているROA**
 - 721 *新ROAWebでは更に多い。
- **割り振られているIPアドレスに対してROAがカバーする割合**
 - 43.6% IPv4
 - 57.4% IPv6

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)。



The screenshot shows a web browser window with the URL <https://rpkinic.ad.jp>. The page header includes the JPNIC logo and the text "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". The main content area features a green header with "RPKI" and a sub-header "お知らせ" (Notice) with a bullet point: "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)". Below this is a section titled "RPKIシステム" (RPKI System) with a sub-header "国内テスト用のRPKIシステムにアクセス (*1)" (Access to the RPKI system for domestic testing (*1)). The text explains that the system provides two RPKI systems: one for normal use and one for domestic testing. It also includes a note about the use of APNIC TAL and the requirement for a resource record certificate. At the bottom, there is a "情報" (Information) section with links to "ROAの作成と管理の方法" (Method of creating and managing ROA), "RPKI Validator 日本語版" (RPKI Validator Japanese version), and "リソースRPKI(RPKI) - JPNIC" (Resource RPKI - JPNIC).

画面と変更点(2/3) - 新しいROAWeb

ROAWeb (JPNICNET)

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)
192.41.192.0/24	2515	発行済		192.41.192.0/24 2515
202.12.30.0/24	2515	発行済		202.12.30.0/24 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) Route Views (<http://archive.routeviews.org/>) 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。

リソース証明書の一覧

リソース証明書が「発行済」になるとROAを作成できます。リソース証明書が「発行済」になるまでに2分程度かかることがあります。

ファイル名	6M28JKbDxTC5mBWue1wNo--KhNU.cer
状態	発行済
有効期限 - 自動更新	2021年11月15日10:30:02 (日本時間/UTC+9)
IPv4	192.41.192.0/24
ファイル名	is2rHh6mM7qK0Yogy3I2DpKAxLY.cer
状態	発行済
有効期限 - 自動更新	2021年11月15日10:30:02 (日本時間/UTC+9)
IPv4	202.12.30.0/24

ROAWebのアカウントの削除や、BPKI接続への変更をご希望される場合には、JPNIC RPKI担当 <rpki-query@nic.ad.jp> までご連絡ください。
 ※ROAWebアカウントを削除するとリソース証明書やROAは全て失効され、公開リポジトリから削除されます。

「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
is2rHh6mM7qK0Yogy3I2DpKAxLY.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ワード入力画面などが無い。)
- 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**

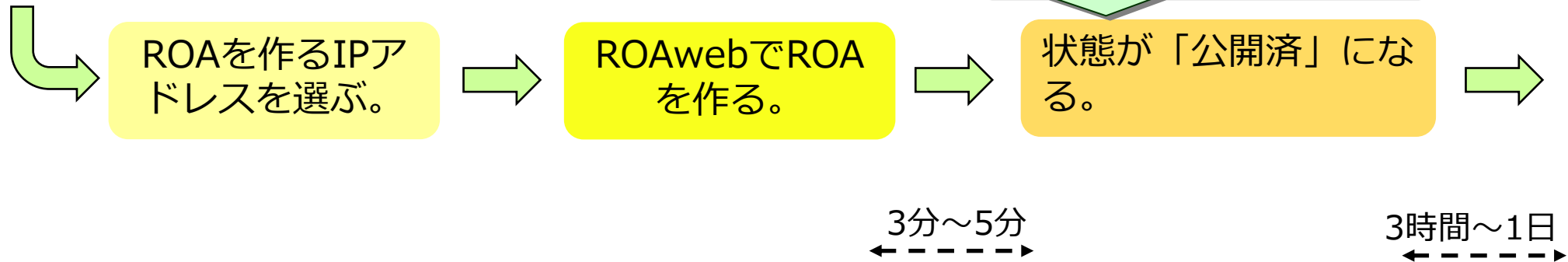
- 従来はご利用いただいているROAWebからの「同期」によってROAが国際的に参照可能になっていました。作成から数時間のタイムラグがありました。今後は数分間後には公開状態になります。

- **複数のリソース証明書表示に対応**

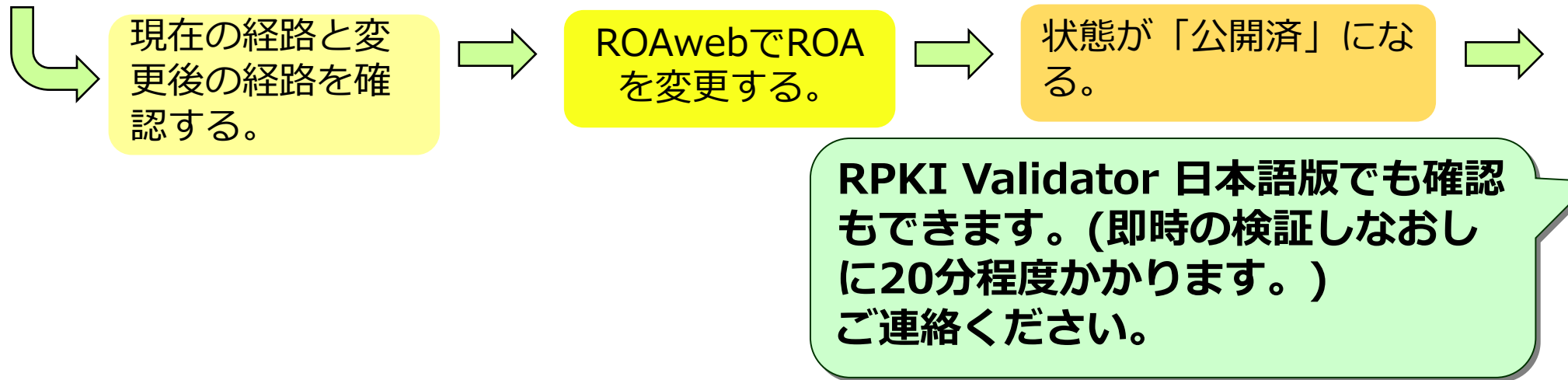
- 一つのアカウントでもAPNICからは複数のリソース証明書が発行されています。トラブルシューティングのため個々に表示しています。

使い方の例

「ROAを新規作成したい。」



「経路を変更したい。」



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！

お問い合わせ窓口： 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

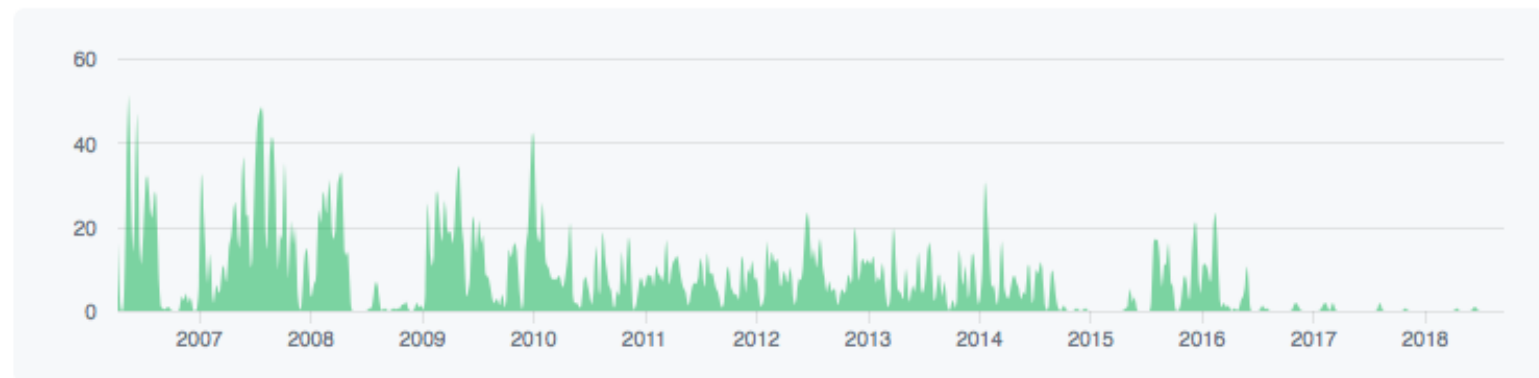
- **RPKI Tools**

- <https://github.com/dragonresearch/rpki.net>

Jun 18, 2006 – Nov 26, 2018

Contributions: **Commits** ▾

Contributions to master, excluding merge commits



<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>