S6
BGPにおけるセキュリティ技術の最新動向
～適用範囲を知り今後に備える～

木村泰司

2017年11月28日(火)

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

発表者

- **名前**
  - 木村泰司（きむらたいじ）
- **所属**
  - 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 (JPNIC)
    - PKI / RPKI / DNSSEC / セキュリティ情報：
      調査 (執筆)・セミナー・企画・開発・運用・ユーザサポート
- **業務分野**
  - 電子証明書 / RPKI / DNSSEC (DPS/鍵管理/HSM他)
  - 国際動向(IETF)

BGPにおけるセキュリティ技術の最新動向

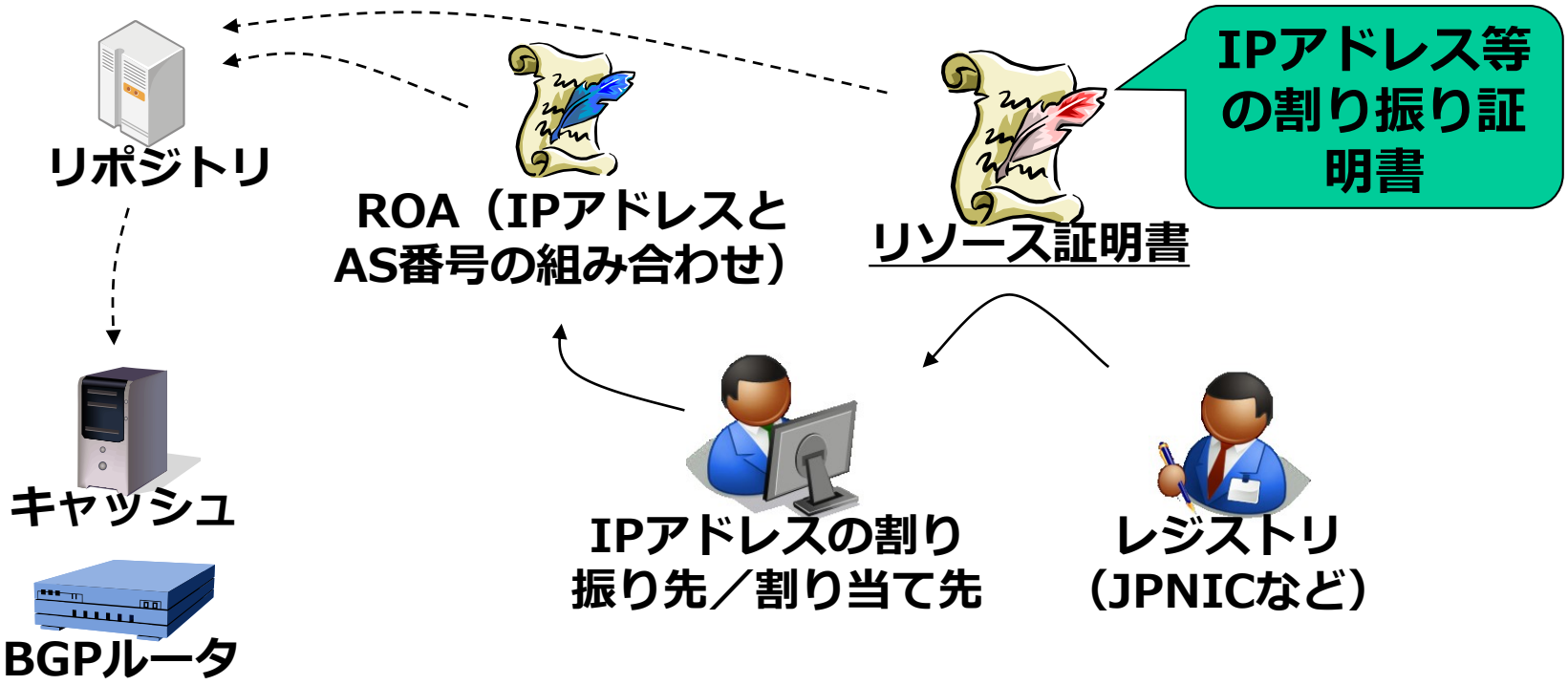
- BGPsec 最新動向
- JPIRRとJPNIC経路奉行 入門
- 技術と仕組みの適用範囲

ニュースと解説
RPKIのAPNICとの連携

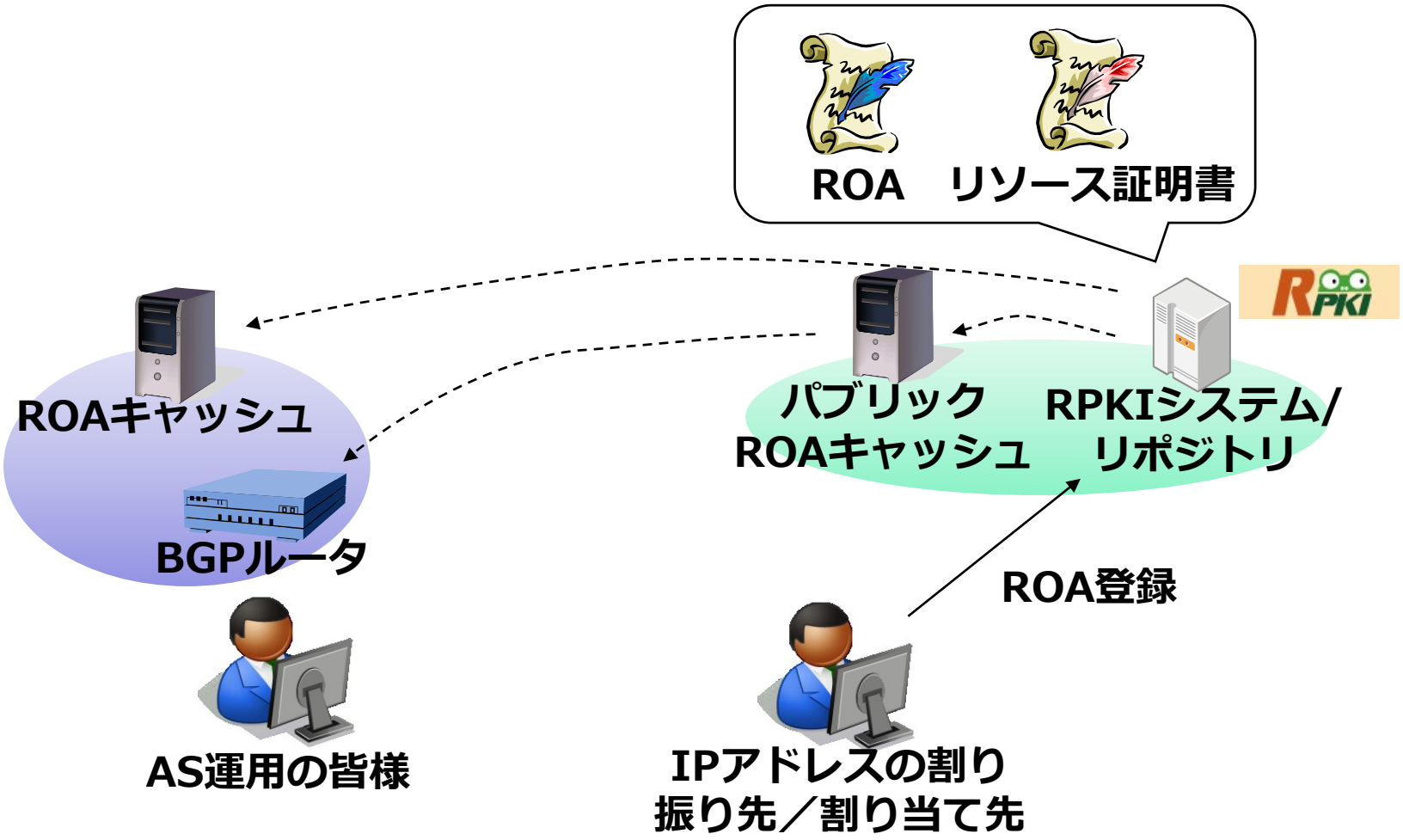
RPKI - モデル

RPKI （リソースPKI）

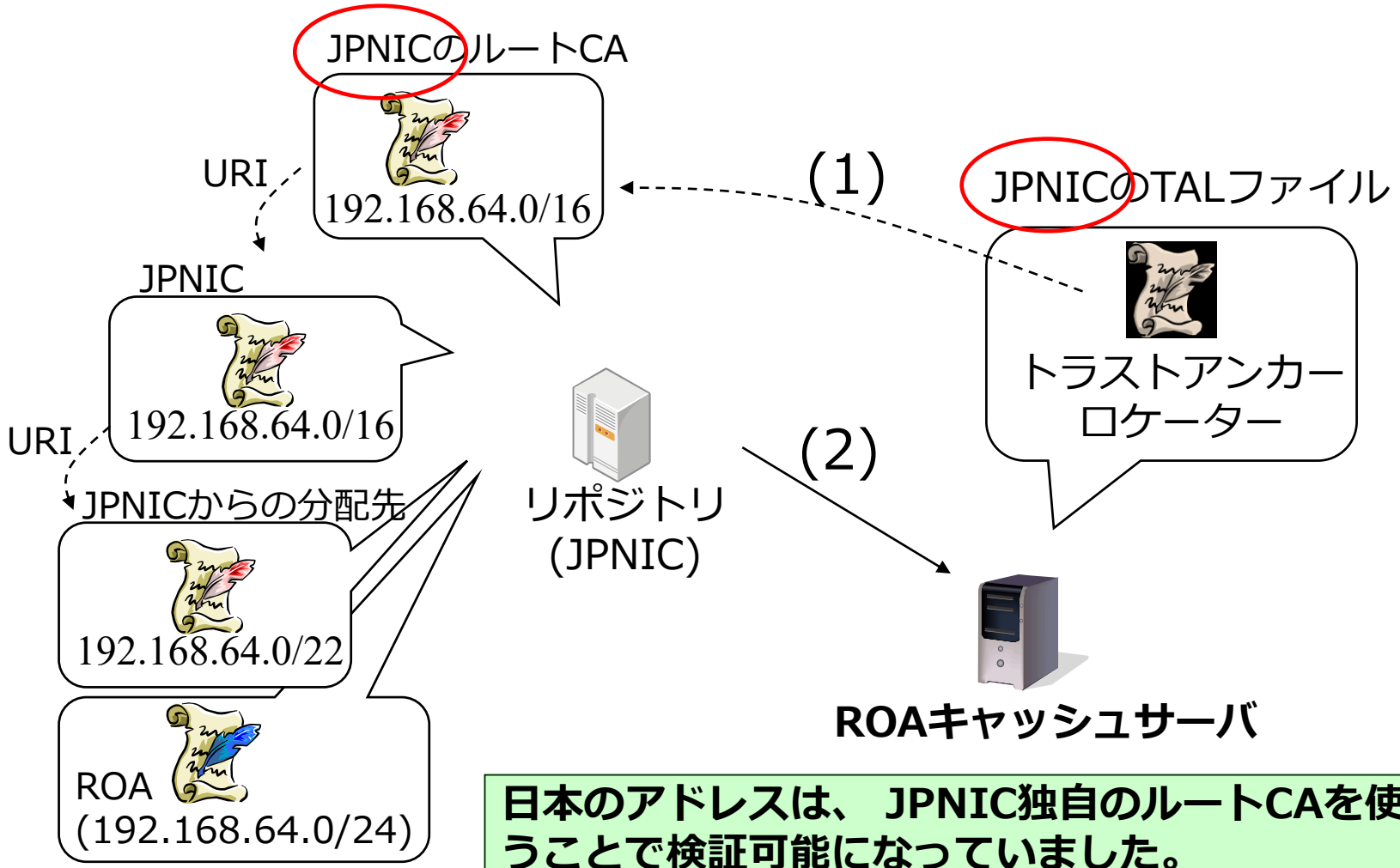
⇒ Resource Public-Key Infrastructure



RPKI - 実際の利用

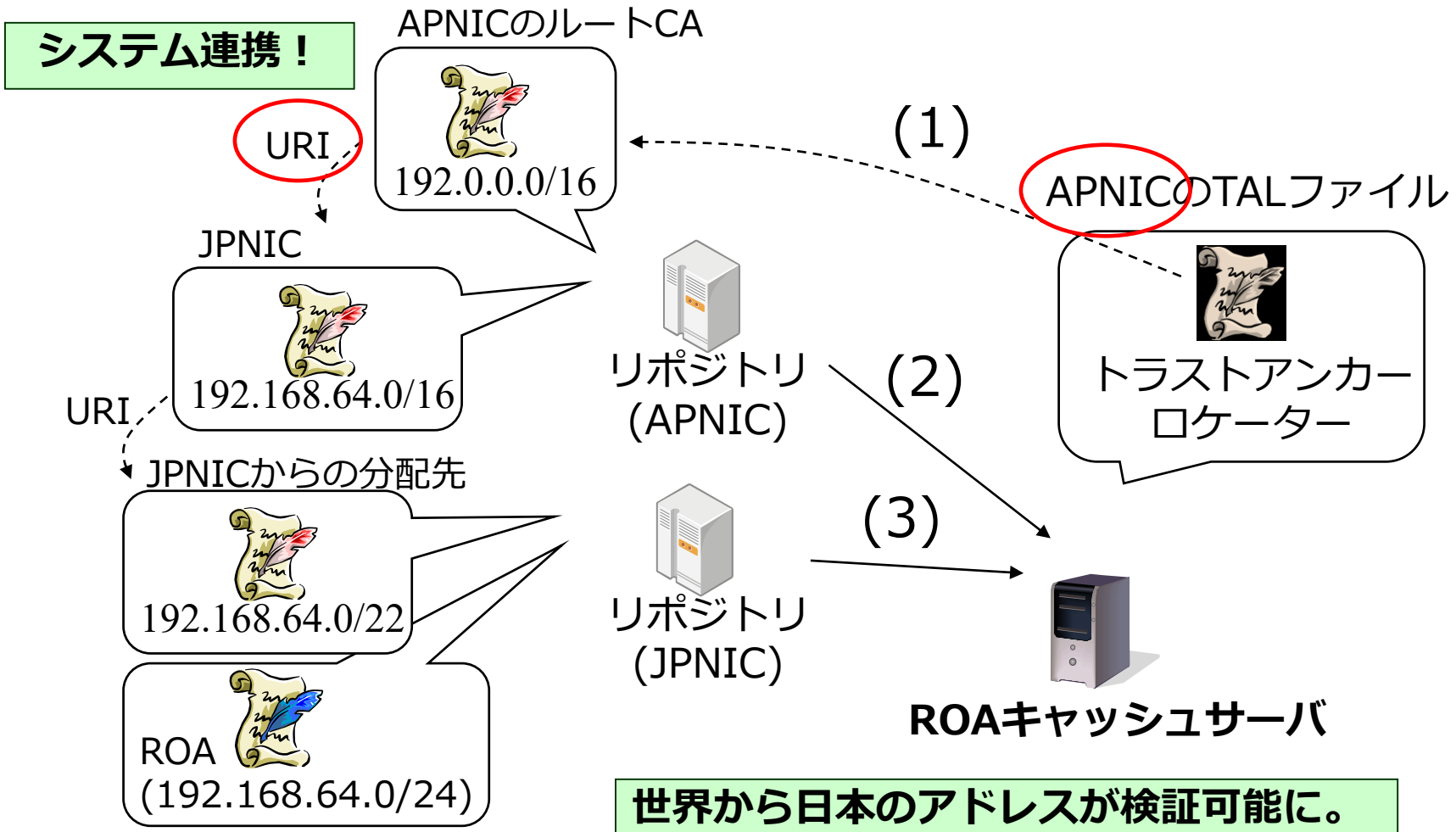


これまで(JPNIC)



日本のアドレスは、 JPNIC独自のルートCAを使うことで検証可能になっていました。

今回の連携により



BGPMOMでもみえます

- **連携の前(8/7)**

```
$ whois -h whois.bgpmon.net " --roa 2515 202.12.30.0/24"
[Querying whois.bgpmon.net]
[whois.bgpmon.net]
1 - Not Found
```

- **連携の後(8/18)**

```
$ whois -h whois.bgpmon.net " --roa 2515 202.12.30.0/24"
[Querying whois.bgpmon.net]
[whois.bgpmon.net]
0 - Valid
------------------------
ROA Details
------------------------
Origin ASN:       AS2515
Not valid Before: 2017-07-18 15:27:08
Not valid After:  2018-07-17 08:58:07  Expires in 333d1h16m31s
Trust Anchor:     rpki-repository.nic.ad.jp
Prefixes:         202.12.30.0/24 (max length /32)
```

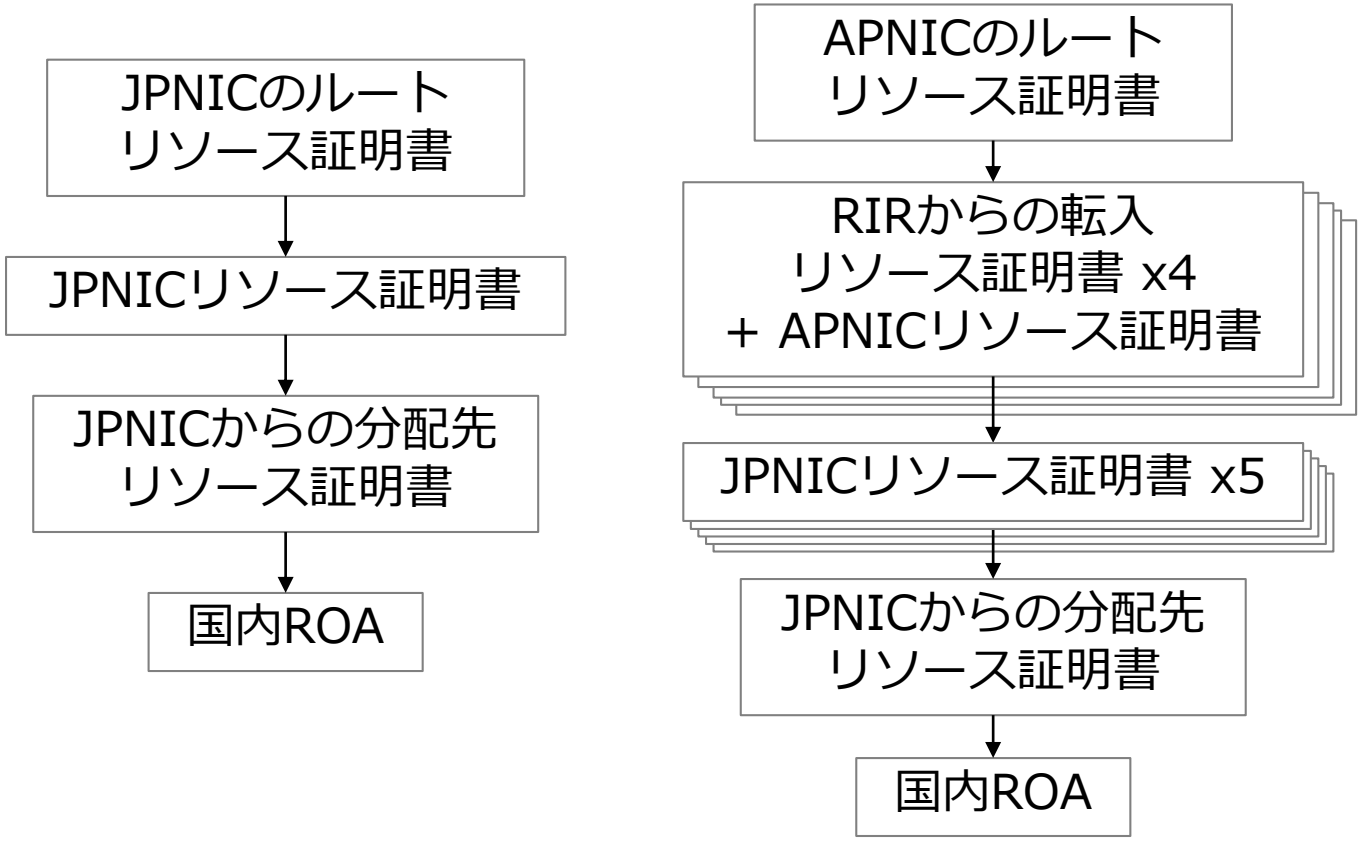
海外から日本の経路のオリジン検証が行われるようになりました

Tipsといいますかオススメ

- **JPNICのTALは消さないで。**
  - APNICから辿れなくなったときにもROAが検証できます
  - RPKIに起きている問題の原因究明に役立ちます

JPNICのTALも併用しておくのがオススメ

解説 - ツリー構造の現状



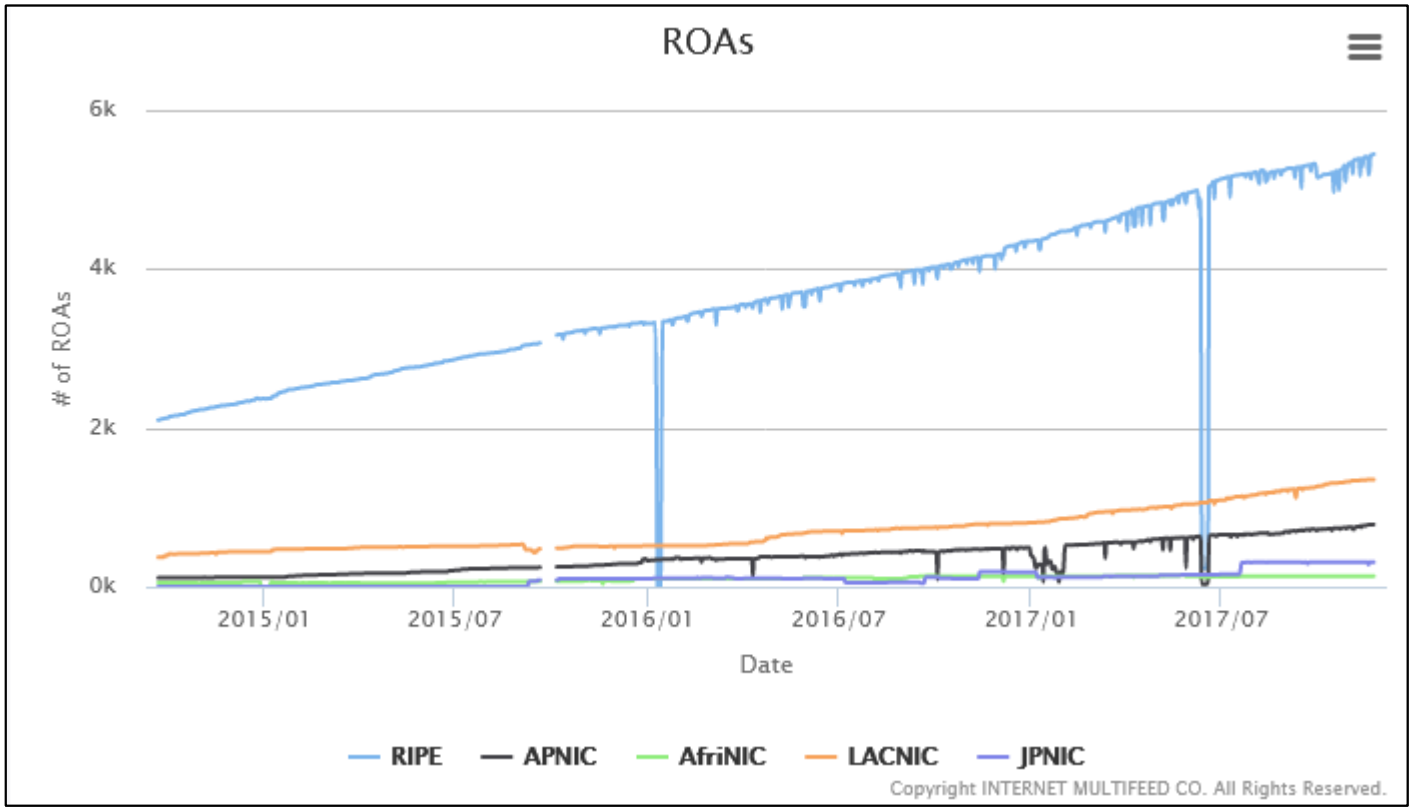
APNICのTALとJPNICのTALの両方を使うと、国内のprefixを持つROAが二つ見える。ツリーが異なるため、片方にエラーが起きてももう片方に影響はでにくい(署名の系として)。

BGPsecの最新動向

RPKIの普及に関わる状況

RIRごとのROAの数

ROA数, MF RPKI Project, 2017/11/23
http://www.mfeed.co.jp/rpki/roa_cache/statistics.html#roas



RIPE地域のROA数がダントツで引き続き純増中。
NIRのあるAP地域は厳しい状況…

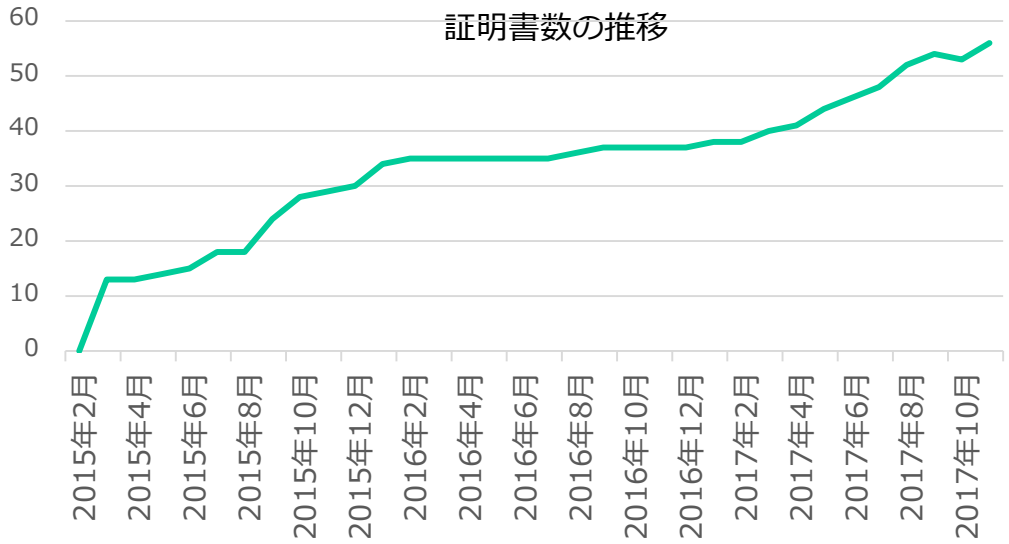
アジア太平洋地域の状況

- **APNIC**
  - 2015年からの「Ready to ROA」キャンペーンはひと段落
  - 五つのトラストアンカーを一つに移行中
- **CNNIC**
  - RPKIシステムを提供開始（6月頃）
    ただしAPNICとは連携していないので、APNICのTALを使って中国のROAは取得できない
  - 実験やInternet-Draft作成などが活発
- **VNNIC**
  - RPKIについて積極的にヒアリング

興味を持っているNIRは徐々に増えているが、依然として提供までのハードルは高いと感じられている模様

JPNICのRPKI試験提供（2015年3月～）

- アドレスホルダ毎に発行される証明書数
  - 56
- 発行されているROA
  - 159
- 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
  - 3.3% IPv4
  - 40%(!) IPv6

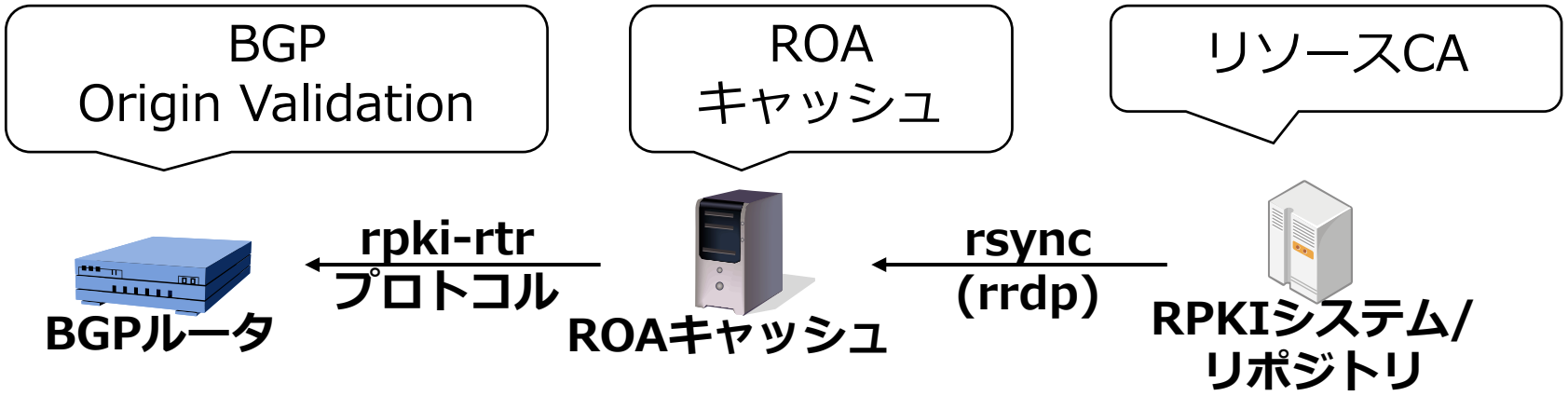


BGPsecの最新動向

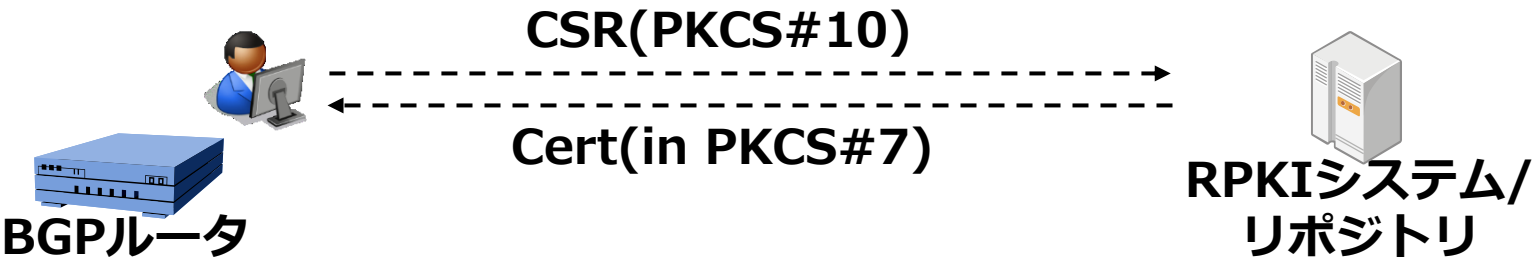
実装

全体の構成

オリジン検証

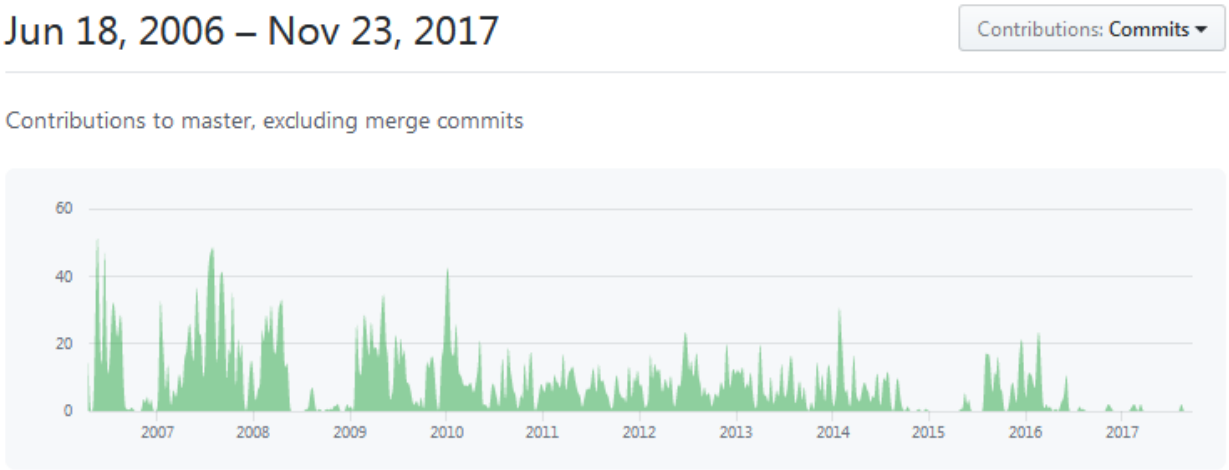


ASパス検証



リソースCA

- **RPKI Tools**
  - 情報と入手元
    https://github.com/dragonresearch/rpki.net
  - 動向
    - RRDPに対応
    - バグフィックスなど



https://github.com/dragonresearch/rpki.net/contributers
© 2017 GitHub, Inc.

ROAキャッシュ

- **RPKI Tools**
  - 情報と入手元　1つ前のスライドと同じ
  - 動向　ARIN TALが入る/TALのHTTPS対応
- **RPKI Validator**
  - 情報と入手元
    https://github.com/RIPE-NCC/rpki-validator
  - 動向　2017年には大きな動きがない
- **RPSTIR**
  - 情報と入手元
    https://github.com/bgpsecurity/rpstir
  - 動向　2017年には大きな動きがない

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

- **NIST BGP Secure Routing Extension (BGP-SRx / BGPSEC-IO)**

  https://www-x.antd.nist.gov/bgpsrx/
  - ASパス検証に対応(動作を確認！)
- **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

BGPsecの最新動向

標準化動向

標準化動向 - IETF SIDR WG
(Secure Inter-Domain Routing WG)

- **リソース証明書検証の見直し**
  - 検証されたリソースセット(Verified Resource Sets)を定義して、移転などで上位リソース証明書から一部のリソースが除かれた際にもROA等が有効とみなされる方式提案
  - IESGレビュー (Proposed Standard)
- **BGPルータ鍵**
  - BGPsecのためのAS証明書手順
  - WGチェアの判断待ち
- **slurm**
  - 検証結果を上書きする提案
  - IESGレビュー (Proposed Standard)

標準化動向 - IETF SIDROPS WG (SIDR Operations WG)

- **SIDR WGから移管**
  - BGPsecルータ証明書ロールオーバー
  - オリジン検証の結果をピアに伝える方式 (Extended Community)
  - RIPE RPKI Validatorのツリー検証方式
- **最近の話題**
  - TALファイルへの電子署名
  - RPの要件定義

ASパス検証の実装は進みつつも、まだ試されていないためか、オリジン検証の仕様を改善(複雑化)する議論が進む。

JPIRRとJPNIC経路奉行入門

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

JPIRRのサービス

- **オブジェクト検索**
  - JPIRR、APNICとRADBの登録オブジェクト
  - 検索するツールを使ってフィルタリングルールの生成が可能
- **オブジェクト登録**
  - ガーベージコレクター★
- **オペレーションに利用できるツール類の提供**
  - Policy Check Service
- **他IRRとのミラーリング**
  - APNIC、RADBおよびRIPEとミラーリング

よく使う検索コマンド

ASのルーティングポリシーを見る

```
$ whois -h jpirr.nic.ad.jp AS2515
```

AS-SETを見る

```
$ whois -h jpirr.nic.ad.jp AS-???
```

routeオブジェクトを見る

```
$ whois -h jpirr.nic.ad.jp 202.12.30.0/24
```

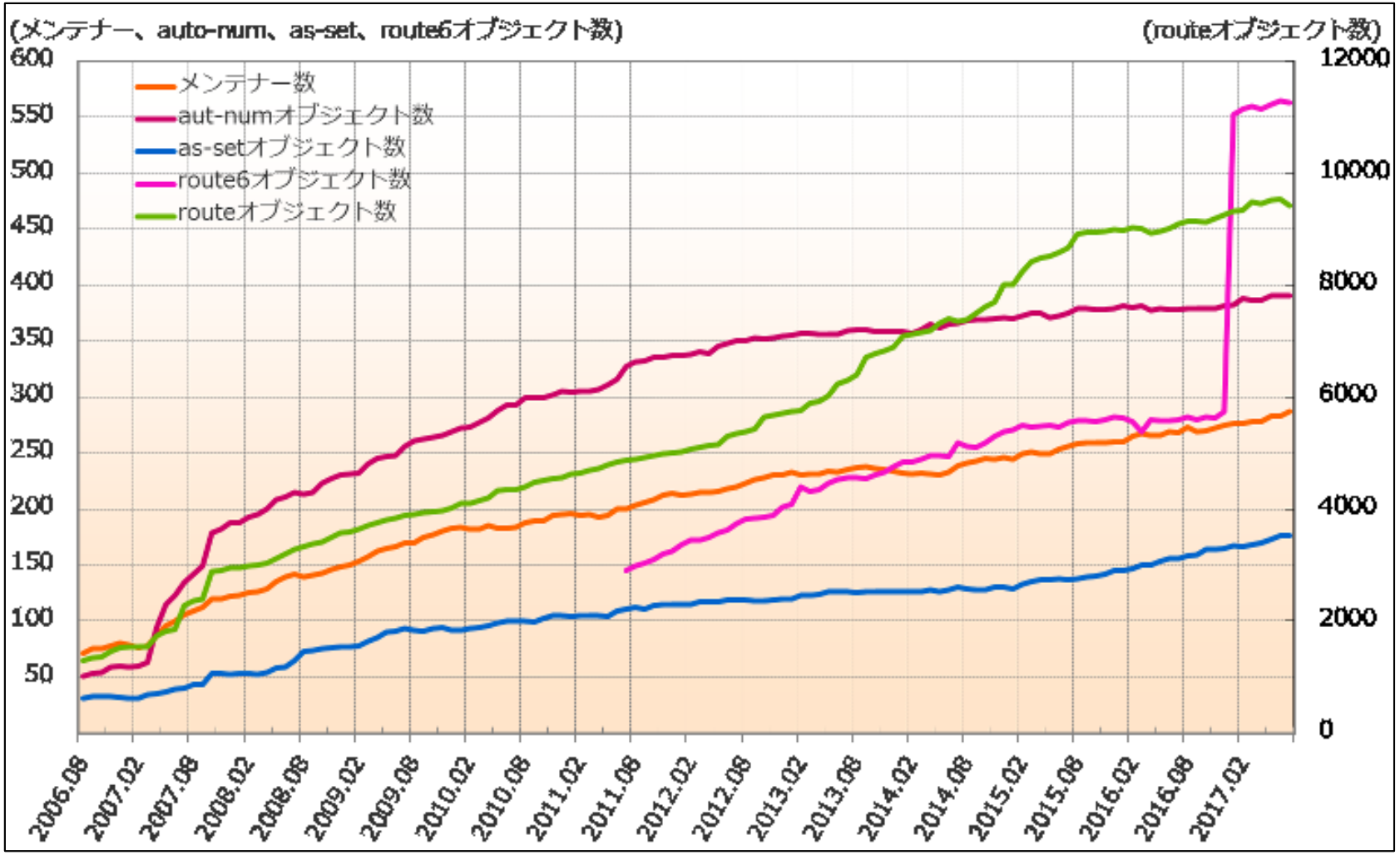
ASの広告するprefixを見る(IPv4)

```
$ whois -h jpirr.nic.ad.jp ¥!gAS2515
```

ASの広告するprefixを見る(IPv6)

```
$ whois -h jpirr.nic.ad.jp ¥!6AS2515
```

JPIRRに登録されているオブジェクト数



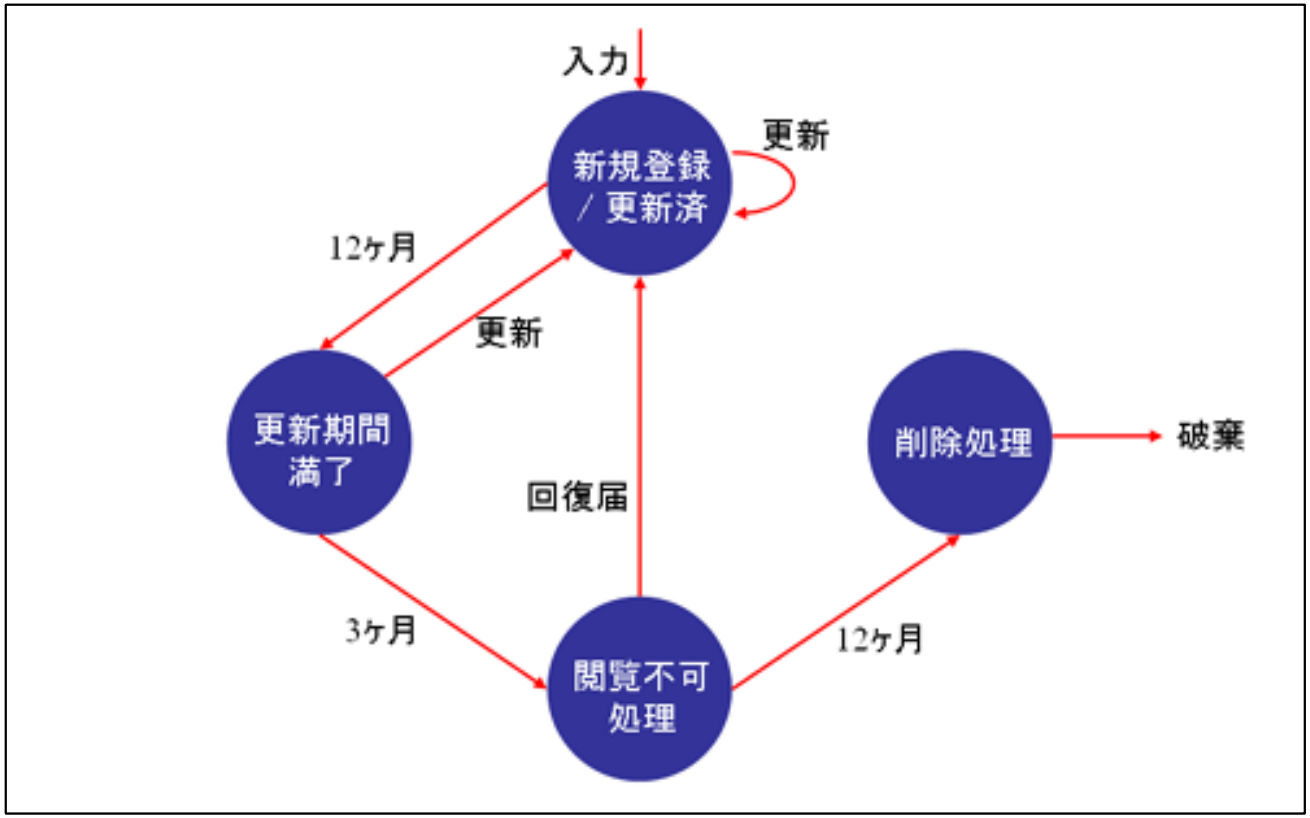
JPIRRに登録されているオブジェクト数の推移(最終更新日2017年8月10日)
https://www.nic.ad.jp/ja/stat/ip/index.html#jpirr-stat

ガーベージコレクター(1/3)

- **オブジェクトに更新が無かった場合に閲覧不可にする機能**
  - 初期状態から 12 ヶ月の間オブジェクトに更新が無かった場合 「更新期間満了」状態へ
  - さらに 3 ヶ月の間更新が無かった場合 「閲覧不可処理」(回復したい場合は、再度ご登録)
  - 12 ヶ月が経過すると該オブジェクトに対して 「削除処理」

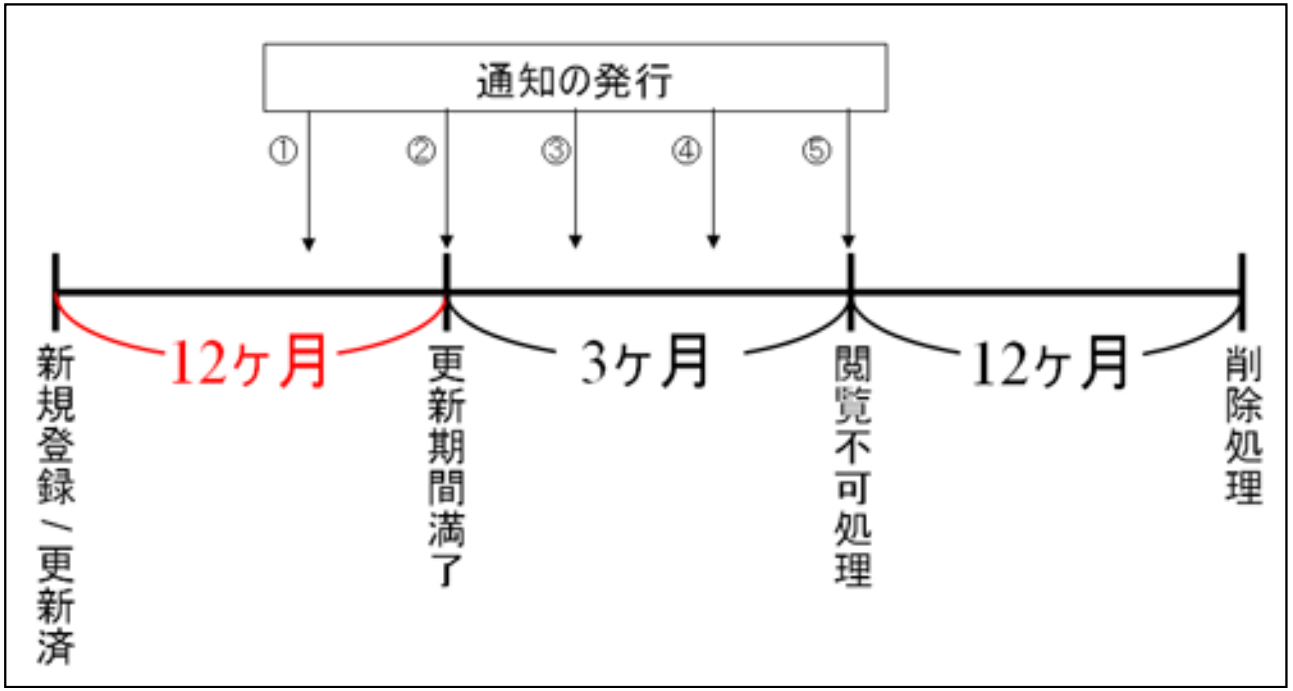
(参照) IRR オブジェクト ガーベージ コレクター の運用について
https://jpirr.nic.ad.jp/gc/doc/

ガーベージコレクター(2/3)



IRR オブジェクト ガーベージ コレクター の運用について
https://jpirr.nic.ad.jp/gc/doc/

ガーベージコレクター(2/3)



IRR オブジェクト ガーベージ コレクター の運用について
https://jpirr.nic.ad.jp/gc/doc/

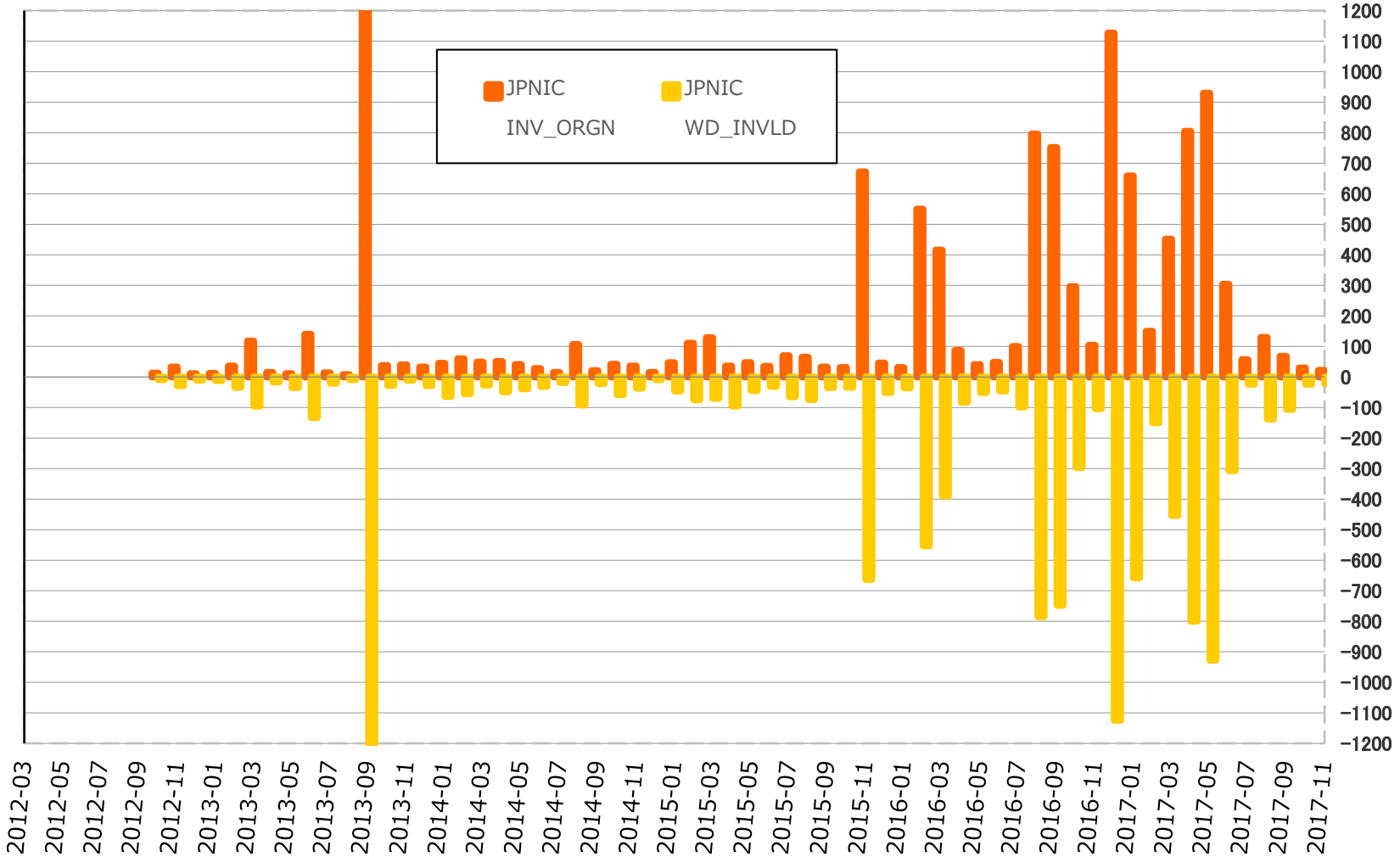
JPNIC経路奉行

- JPIRRへ登録されたRouteオブジェクトと異なるOrigin ASを持つ経路情報を検知し通知

Routeオブジェクトの例

```
|route:      202.12.30.0/24
|descr:      JPNICNET
|            Japan Network Information Center
|            Kokusai Kogyo Kanda Bldg. 6F
|            2-3-4 Uchi-Kanda
|            Chiyoda-ku, Tokyo 101-0047
|            JAPAN
|            X-Keiro: okadams@nic.ad.jp                <--追加記述
|            X-Keiro: okadams-noc@nic.ad.jp              <--複数あて先に通知する場合
記述
|origin:     AS2515
|admin-c:     SN3603JP
|tech-c:      YK11438JP
|tech-c:      MO5920JP
|notify:      system@nic.ad.jp
|mnt-by:       MAINT-AS2515
|changed:     apnic-ftp@nic.ad.jp 20080116
|source:      JPIRR
```

JPNIC経路奉行 検知の状況



JPNICが運営する経路奉行への経路提供組織

- 株式会社インターネットイニシアティブ
- インターネットマルチフィード株式会社
- エヌ・ティ・ティ・コミュニケーションズ株式会社
- エヌ・ティ・ティ・スマートコネクト株式会社
- KDDI株式会社
- 株式会社KDDI研究所
- さくらインターネット株式会社
- ソネットエンタテインメント株式会社

経路提供組織の皆様の御協力に感謝いたします。
JPNICが自身で収集した経路情報も検出対象としています。

IRRを活用するツール

- **irrtoolset/irrtoolset**
  - https://github.com/irrtoolset/irrtoolset
  - Rtconfig ルータのBGP設定生成ツール。IRRのデータを使った継続的なフィルター更新業務に。
- **IRR Power Tools**
  - https://github.com/6connect/irrpt
  - 自動bogonフィルタ生成。経路変更など更新通知メール。ルータ BGP設定生成。など。

情報源とお問い合わせ先

- **JPIRR**
  - JPIRR
    https://www.nic.ad.jp/ja/irr/
- **オブジェクトの登録方法**
  - JPIRRでのオブジェクト登録について
    https://www.nic.ad.jp/doc/jpnic-01077.html
- **お問い合わせ先**
  - IRR担当
    irr-query@nic.ad.jp

技術と仕組みの適用範囲

適用範囲

仕組み / 技術	JPNIC経路奉行	BGPsec オリジン検証	BGPsec ASパス検証
機能	ミスオリジンの検知	ミスオリジンの検知/対策	パス違いの検知/対策
できること	メール通知	経路表表示 優先度付け メール通知 (BGPMON等)	経路表表示 優先度付け 通知(?)
適用可能な範囲	JPIRRに登録されたprefix(国内)	ROAが作られたprefix(国際)	AS証明書を導入したルータ

国内のprefixの検知をするのか、一歩進めて対策を講じるのか、もしくは国際的なprefixを対象とするのか。ASパス検証は更にその先の技術という位置づけになる。

ケースごとに利用できる仕組み

- **国内のIPアドレスに対するミスオリジンを検知したい**

  ⇒ JPIRRで「X-Keiro:」を登録してメールで通知を受ける。

  ⇒ JPNICのRPKIシステムでROAを発行してパブリックキャッシュサーバをBGPルータで利用する。

  ⇒ JPNICのRPKIシステムでROAを発行してキャッシュサーバを立て、それをBGPルータで利用する。

  - RPKIの場合
    - JPNICのTALを使うと国内のIPアドレスが対象になる
    - RIRのTALを使うと国際のIPアドレスが対象になる

ケースごとに利用できる仕組み

- **特定のASとIPネットワークのミスオリジンやASパスの変化を検知したい**

  ⇒ BGPMONなどの経路監視サービスを利用する。

ケースごとに利用できる仕組み

- **オリジン検証を試したい**

  (BGPルータで試す場合)
  ⇒ パブリックキャッシュサーバを指定する。

  (キャッシュサーバとBGPルータで試す場合)
  ⇒ UbuntuやCentOSで”rpki-rp”パッケージもしくはrpki-validatorを使う。

  (リソースCAを含めて一式を試す場合)
  ⇒ RPKI ToolsもしくはBGP-SRxをセットアップする。

(情報) dockerを使ってRPKI Validationを試してみる
http://goto-infamous.hatenablog.com/entry/2017/10/16/014648

ケースごとに利用できる仕組み

- **ASパス検証を試したい**

  ⇒ BGP-SRxをセットアップする。

  ※JPNICで試していますのでご相談いただければ幸いです。

おわり

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