経路奉行・RPKIの最新動向

木村泰司

2015年11月18日(水)

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)
    - CA / 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)

経路奉行・RPKIの最新動向

- JPIRRと経路奉行　最新動向
- RPKI 最新動向
- RPKIとJPIRRの違い

JPIRRと経路奉行　最新動向

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の登録と経路奉行のはじめ方

AS番号の割り当てを受ける

AS番号の割り当て申請
https://www.nic.ad.jp/ja/ip/as-assign.html

JPIRRにMaintainerオブジェクトを登録する

JPIRRでのオブジェクト登録について
https://www.nic.ad.jp/doc/jpnic-01077.html

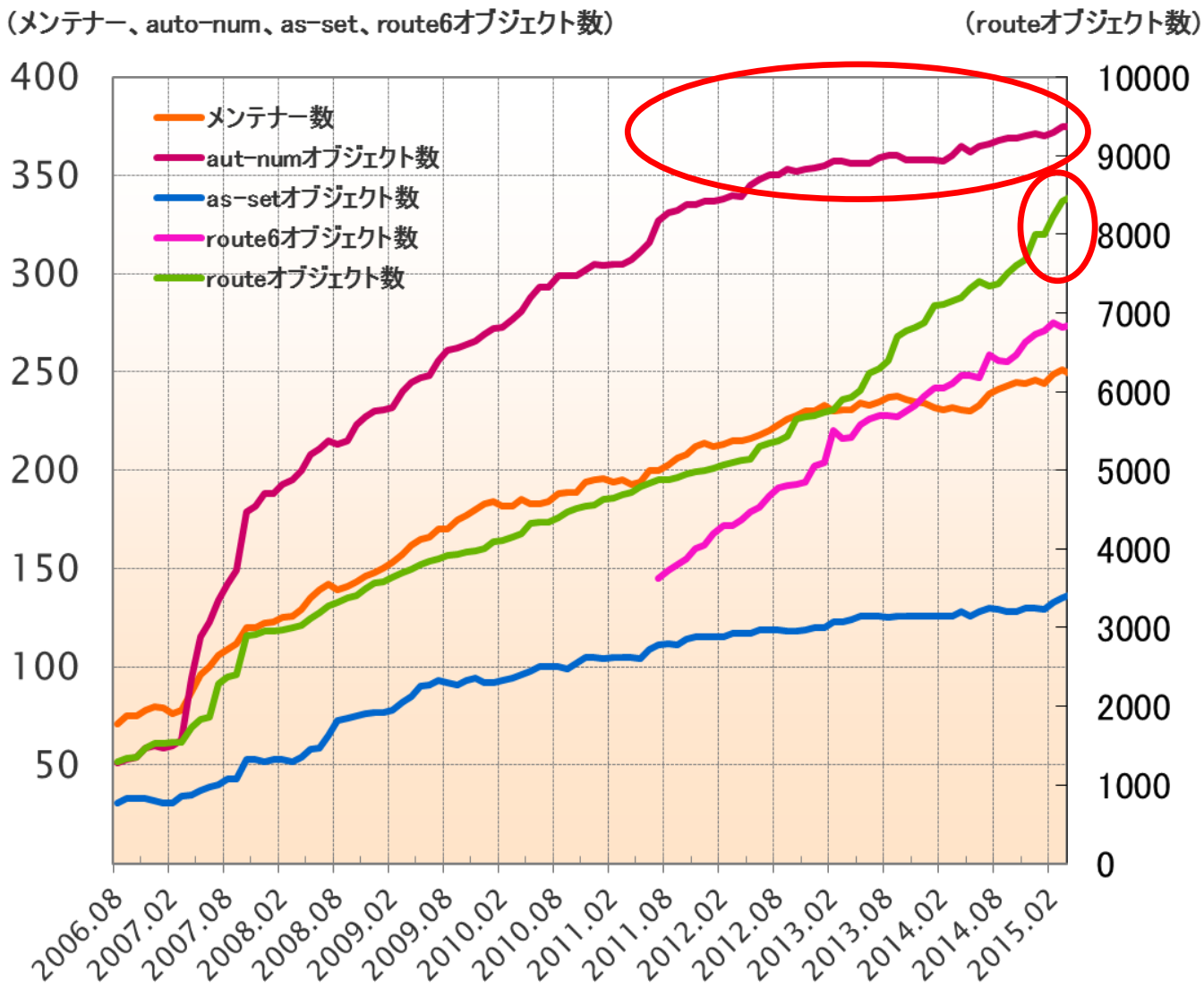
routeオブジェクトのdescr:にX-Keiro:を記述する

（同上）

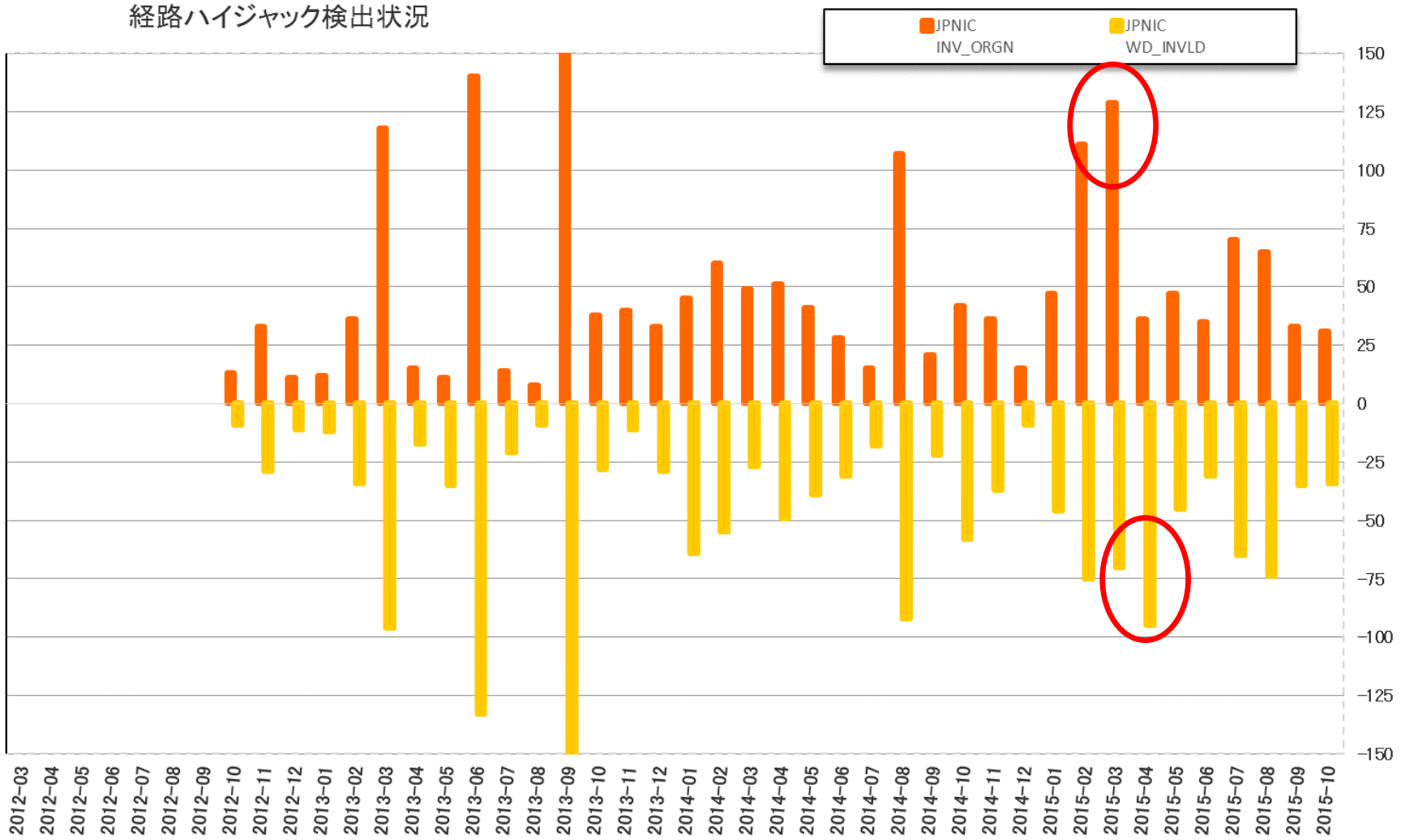
登録完了！

お問合せ窓口： irr-query@nic.ad.jp

JPIRRのオブジェクト登録数

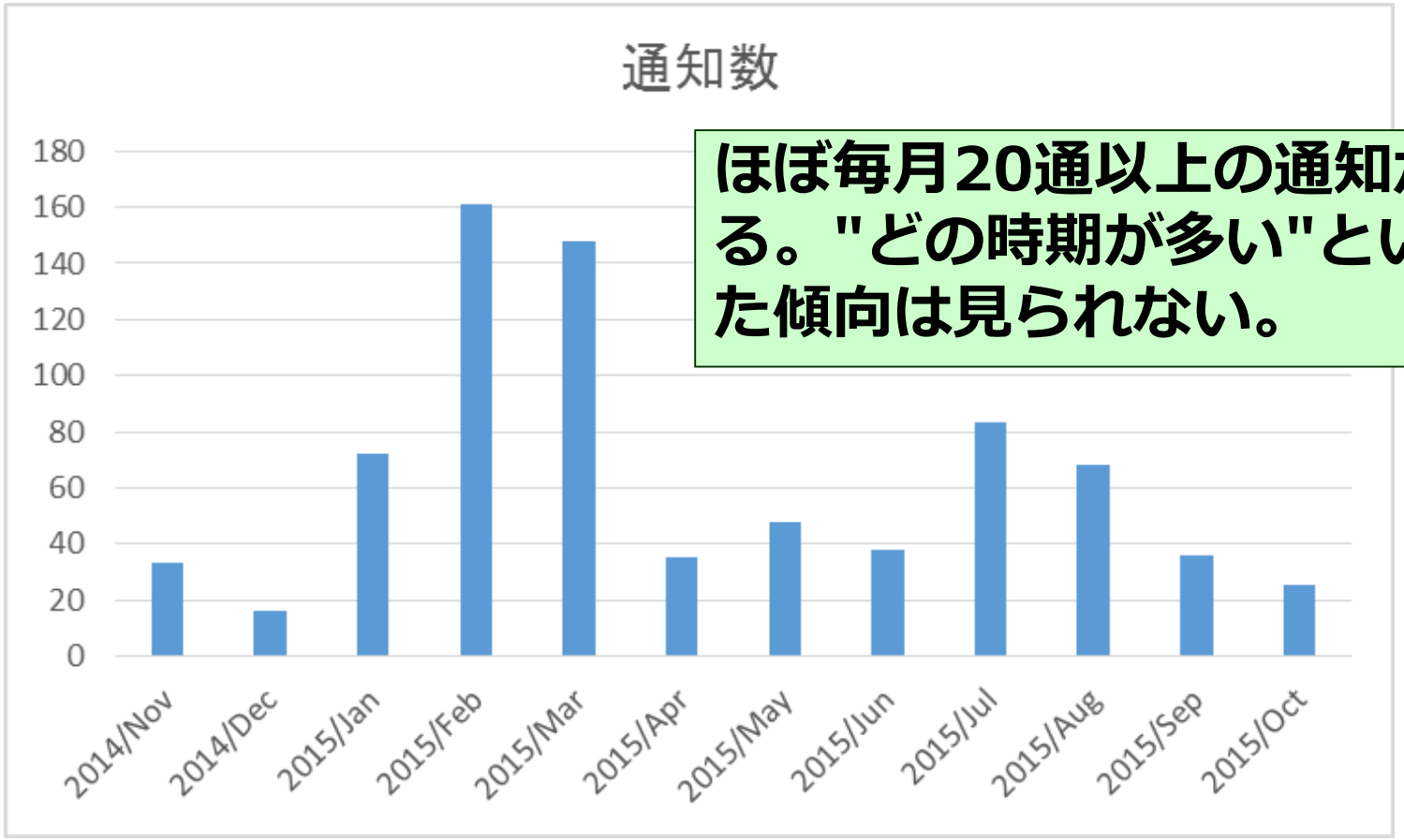


経路奉行 – 検出の推移



経路奉行 – メールによる通知数

- 一年間の通知数の変化



ほぼ毎月20通以上の通知がある。"どの時期が多い"といった傾向は見られない。

観測されていること

a. 何度も通知される prefix がある。（多いものは一年間で20回～110回）

⇒ そのprefixは要注意。JPIRR/WHOIS/RIPEstat/Looking Glass等で要調査。 **参考：https://www.nic.ad.jp/ja/ip/irr/counter-hi-jack.html**

b. 経路情報としてグローバルから見えていない prefix が、他のASで使われていることがある。

⇒ 特に「移転を受けたので経路広告しよう」「いままで内部で使っていたけど、これから経路広告しよう」という場合には要注意。将来的にはAS0のROAで正当性を示すことも(RFC7607)

c. 当時JPIRRに登録されていたが、実は割り当てられたアドレスではなかった…？

⇒ JPIRRはWHOIS DBと連動していないので登録できてしまいます。

(参考) BGPMONのTweetからは...

- **日本に限らずあるPrefixが、アジアの別の国にあるASから経路広告されていることがある。**
  - 割り当てを確認できない顧客の prefix を経路広告せざるを得ない状況がある？
  - NIRにはIRRやRPKIシステムはなく、RADbなどを利用していると考えられる。とすると、prefix が間違っていても信じて経路広告せざるを得ない。
    ⇒ 本当は違う地域の割り当てであることも。

    アジア地域におけるルーティングセキュリティは重要！

RPKI 最新動向

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）

国際的な普及の状況

RPKI Dashboard, SURFnet, 2015/11/12
http://rpki.surfnet.nl/

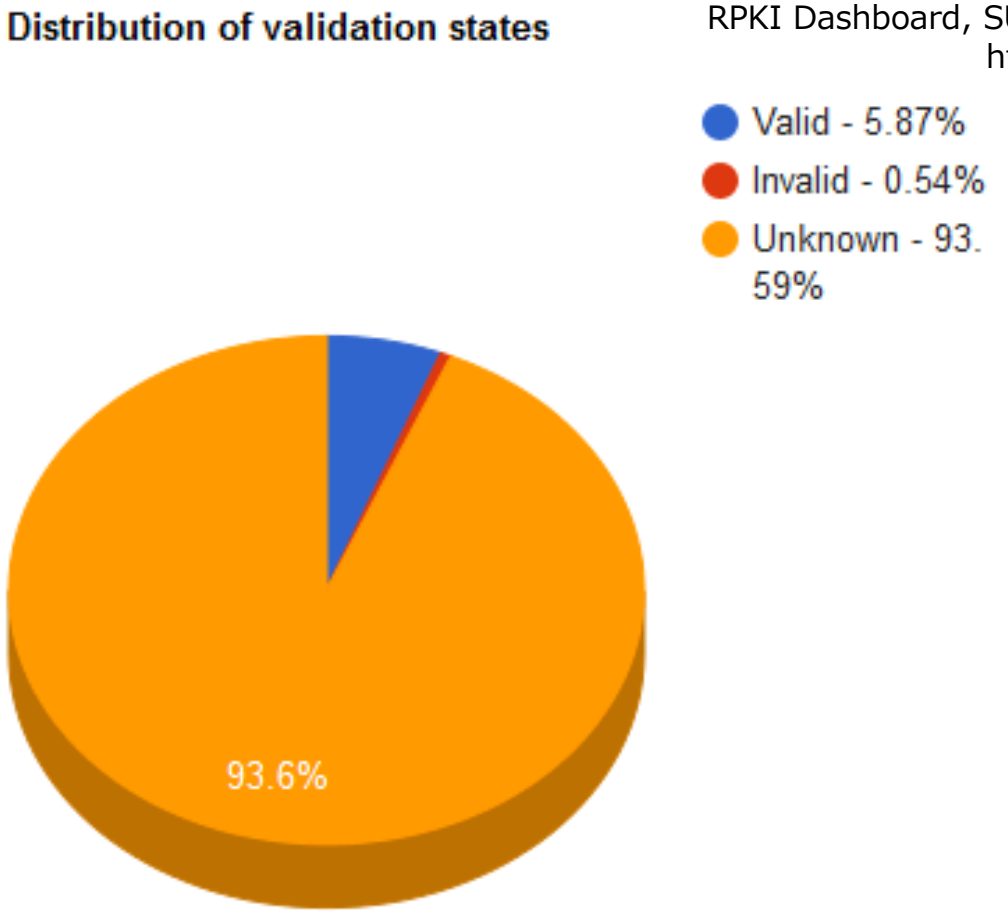
10 records per page　　Search:

RIR	Total	Valid	Invalid	Unknown	Accuracy	RPKI Adoption Rate
AFRINIC	13723 (100%)	238 (1.73%)	14 (0.1%)	13471 (98.16%)	94.44%	1.84%
APNIC	153546 (100%)	3037 (1.98%)	1105 (0.72%)	149404 (97.3%)	73.32%	2.7%
ARIN	216045 (100%)	1696 (0.79%)	333 (0.15%)	214016 (99.06%)	83.59%	0.94%
LACNIC	77088 (100%)	14994 (19.45%)	686 (0.89%)	61408 (79.66%)	95.63%	20.34%
RIPE NCC	155437 (100%)	16216 (10.43%)	1178 (0.76%)	138043 (88.81%)	93.23%	11.19%

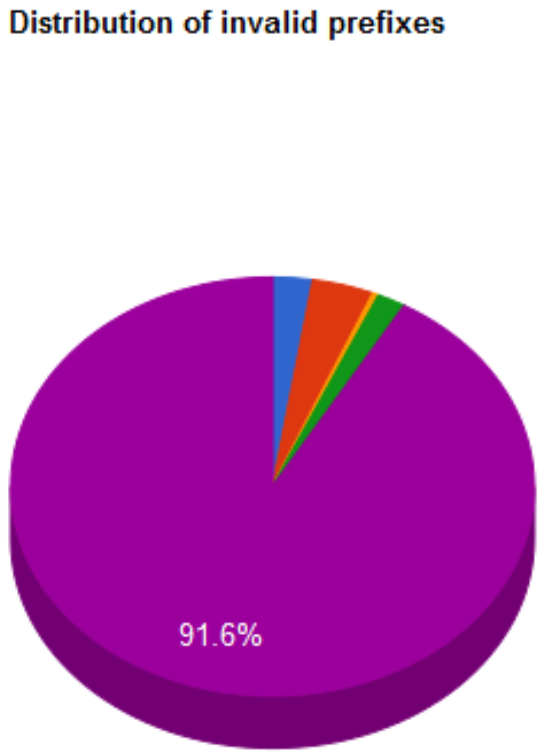
ROAによってカバーされるIPアドレスの割合はまだ低い。ただし単純増加の傾向ではある。

経路広告に対するROAの発行割合

RPKI Dashboard, SURFnet, 2015/11/12
http://rpki.surfnet.nl/



ROAを使ったOrivin Validation結果の内訳



経路情報とROAのAS番号が違う

AS番号が合っていてPrefix長が合っていないROA（未広告？）

ROAの最大Prefix長よりも細かい経路が流れている

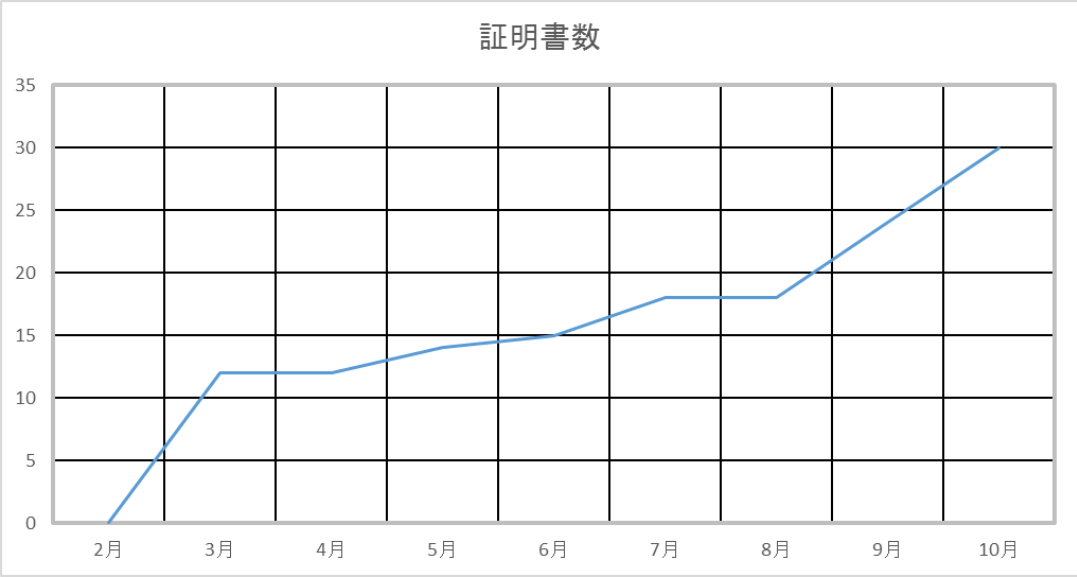
AS番号もPrefixも合っていないROA

RPKI Dashboard, SURFnet, 2015/11/12
http://rpki.surfnet.nl/

実際の経路情報とは異なるROAが約8.4%発行されている。去年は10%くらい。（全ROA数も増加）

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
  - 29
- 発行されているROA
  - 100
- 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
  - 1.76% IPv4
  - 0.86% IPv6 (/48の個数)



RPKI実装の最新動向

- **RPKI Tools　http://rpki.net/**
  - RPKI CA、GUI、RPKIキャッシュ
  - routeオブジェクト生成機能
  - BGPSEC向けルータ証明書発行機能

  （実装中情報：開発者より）
  - PostgreSQLへの移行コードの実装中
  - Up-Downで鍵を安全に交換しBPKI接続するためのOOB（Out of Band）プロトコルの実装中
  - Rsyncに変わる差分転送プロトコルの RRDP（RPKI Repository Delta Protocol）を実験的に実装中

RPKIに関わる標準化動向

- **IETF Secure Inter-Domain Routing WG (SIDR)**
  - BGPSEC – ASパス検証
    - ほぼ固まってきた。
      6つのInternet-Draftのうち3つがWGコメント終了
  - RRDP - rsyncに代わる配布プロトコル
    - WGで議論中。試験的な実装が出てきた。
  - RPSL署名 – IRRオブジェクトへの署名
    - 議論復活。

BGPSECについてはASの証明書管理を議論中。Path Validationを試せる時期はまだ先。
Rsyncは変わっていく可能性大。

RPKIのJPIRRの違い
5W1H

What

- **RPKI**
  - レジストリから分配されたIPアドレスやAS番号を証明書を通じて確認できるPKI
    ↓
    ちゃんと分配されたアドレスであることと、そのOrigin ASが確認できる(ROA)。

- **JPIRR**
  - ルーティングポリシーを登録/WHOISで参照できるデータベース
    ↓
    AS毎のルーティングに関わる情報を共有できる。

Who

- **RPKI**
  - RIR, NIR, ISPが運用
    - RPKIシステム
    - レジストリデータベース
  - IPアドレスホルダが登録／BGPオペレーターが利用
  - 仕様はIETF (SIDR WG, IDR WG)
    - 仕様検討
    - 実装者も参加

- **JPIRR**
  - IRRオペレータが運用
    - JPIRR
      :
  - BGPオペレーターが登録・利用
  - 仕様はIETF / RIPE
    - RPSL

When

- **RPKI**
  - IPアドレスが分配されてから
  - Origin ASが決まったらROAを発行する
  - 経路表の自動的な検査のために定期的に使われる
- **JPIRR**
  - AS番号が割り当てられたときから
  - Mntnerオブジェクトの登録内容、連絡先の情報などが決まったときに登録する
  - 経路フィルターを作るときや人が経路情報をチェックするときに使われる

Where

- **RPKI**
  - 証明書やROAはレジストリにあるサーバに。配布は分散可能。
  - 運用はNIR / RIR / ISP
  - RPKIキャッシュサーバでROA検証される
- **JPIRR**
  - 登録されたデータがあるのはIRRのデータベース
  - 運用はJPNIC
  - ユーザの端末を使って登録情報が閲覧される

Why

- **RPKI**
  - 経路情報などに現れるIPアドレスが正しい事を確認するため
  - 正しい分配先によってによって、経路広告などの情報を示すするため
  - IPアドレスの正しさを確認するため
- **JPIRR**
  - ルーティングのオペレーションに必要な連絡先やASのつながりやポリシーを共有するため
  - ルーティングに関わるトラブルシュートのため

How

- **RPKI**
  - レジストリツリーに合わせて電子証明書を発行
  - リポジトリを使って情報を配布／クライアントが辿る
  - ROAを使ってOriginを確認
- **JPIRR**
  - ルーティングレジストリがDBとして機能
  - ミラーリングによって他のIRRと情報を共有
  - routeオブジェクトを使ってOriginを確認

おわり