IETF報告会（88th バンクーバー）

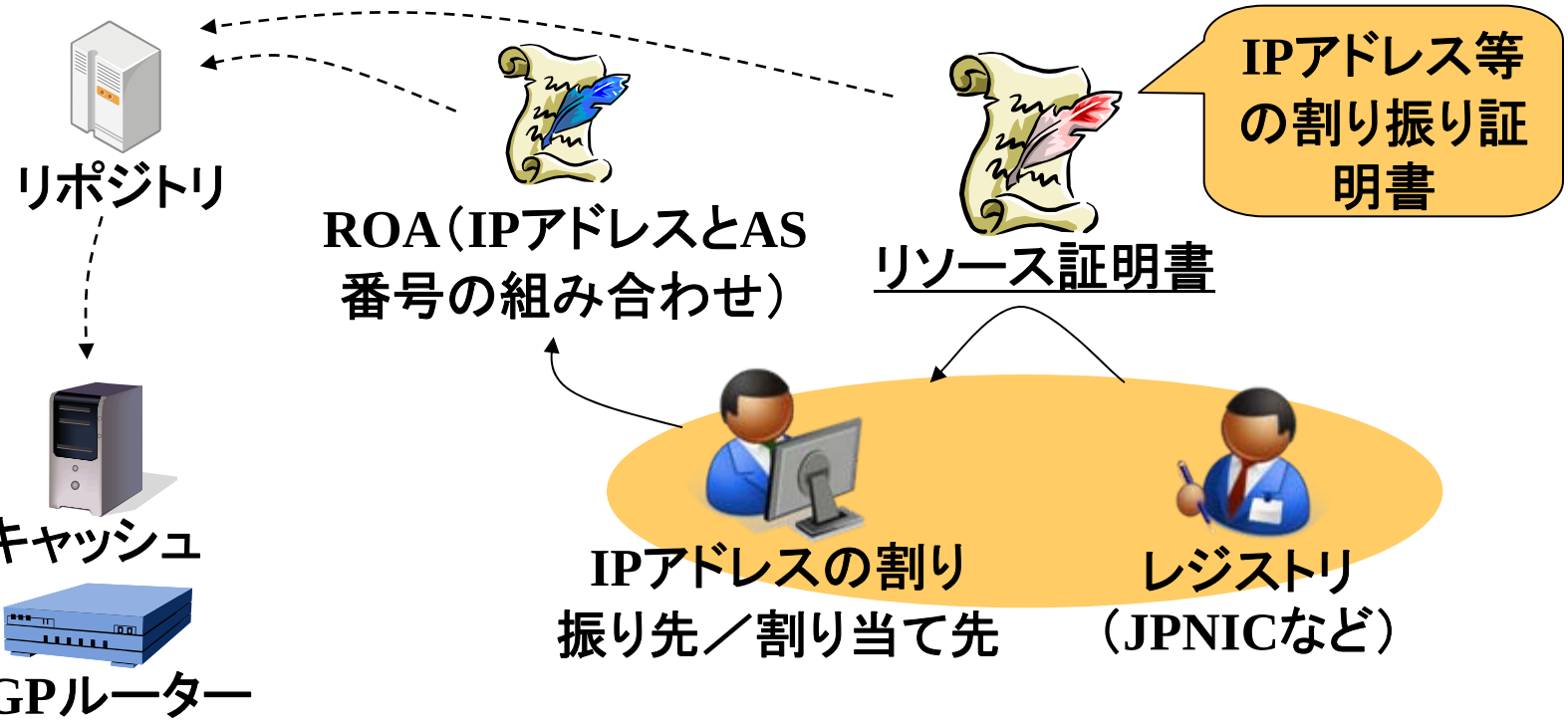
RPKI関連

木村泰司
taiji-k at nic.ad.jp

RPKIとは

RPKI （リソースPKI）

⇒ Resource Public-Key Infrastructure



内容

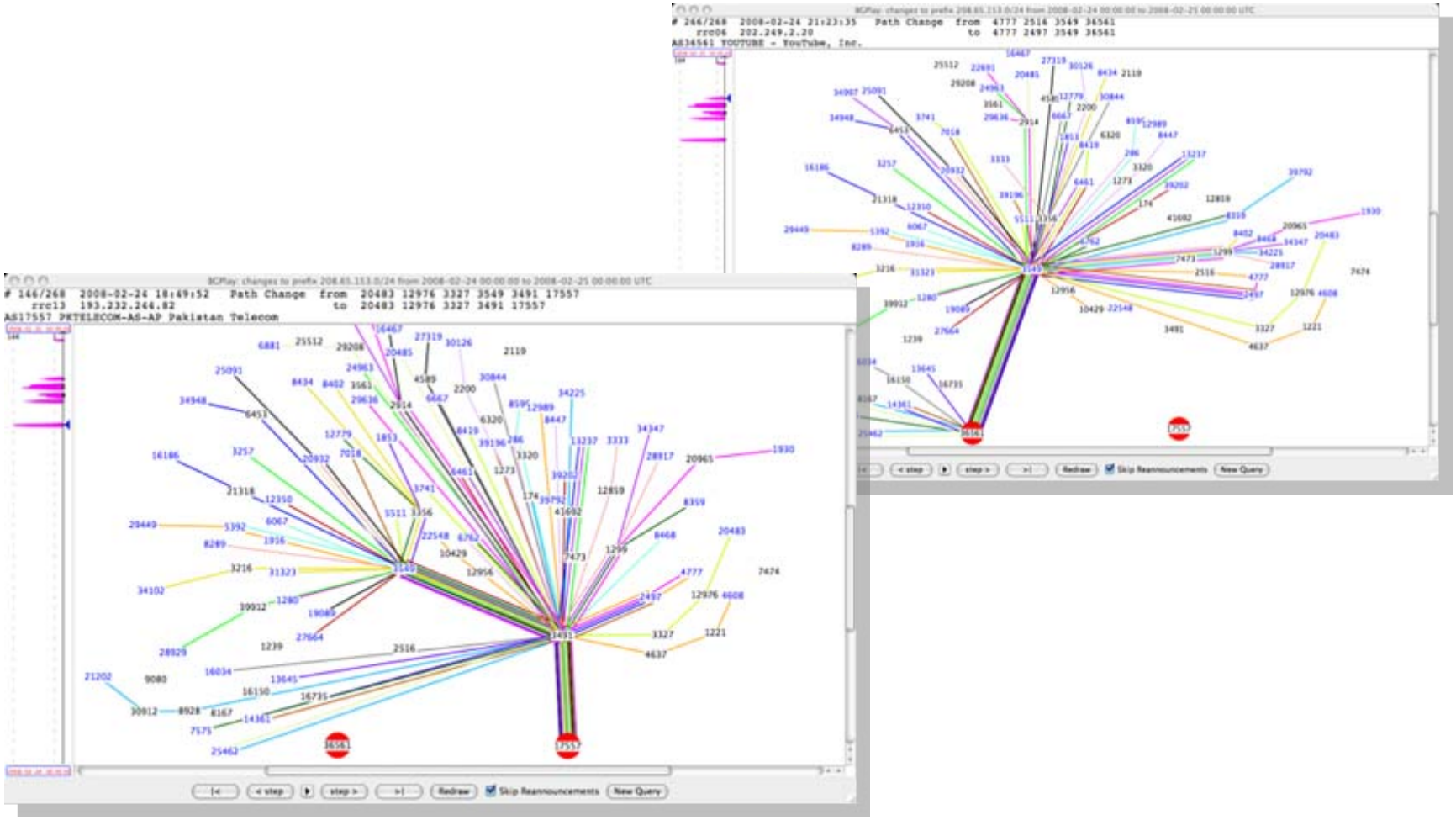
- RPKIのこれまで
- プロトコル策定の概況
- デプロイメントの状況
  ～Topic エクアドルのIXP～
- 論点と今後

RPKIのこれまで

RPKIのこれまで

- BBN Report 8217, “An Architecture for BGP Countermeasures,” November, 1997
  - IPアドレスの割り振り構造に沿って認証局を置き、インターネット経路制御のセキュリティ向上のためにIPアドレスとAS番号を確認できるような電子署名のアーキテクチャを提唱
- Secure Inter-Domain Routing WG発足, 2006年4月
- 2008年2月YouTube経路ハイジャック事件
- 2011年4月のIPv4アドレス在庫枯渇に先立ち地域インターネットレジストリが「アドレスの割り振り証明」として導入を急ぐ

YouTube経路ハイジャック事件



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

プロトコル策定の概況

Secure Inter-Domain Routing (SIDR) WG

RPKIとSIDR WG

SIDR WG関連の
ドキュメント

⇒ Origin Validation はほぼRFC化

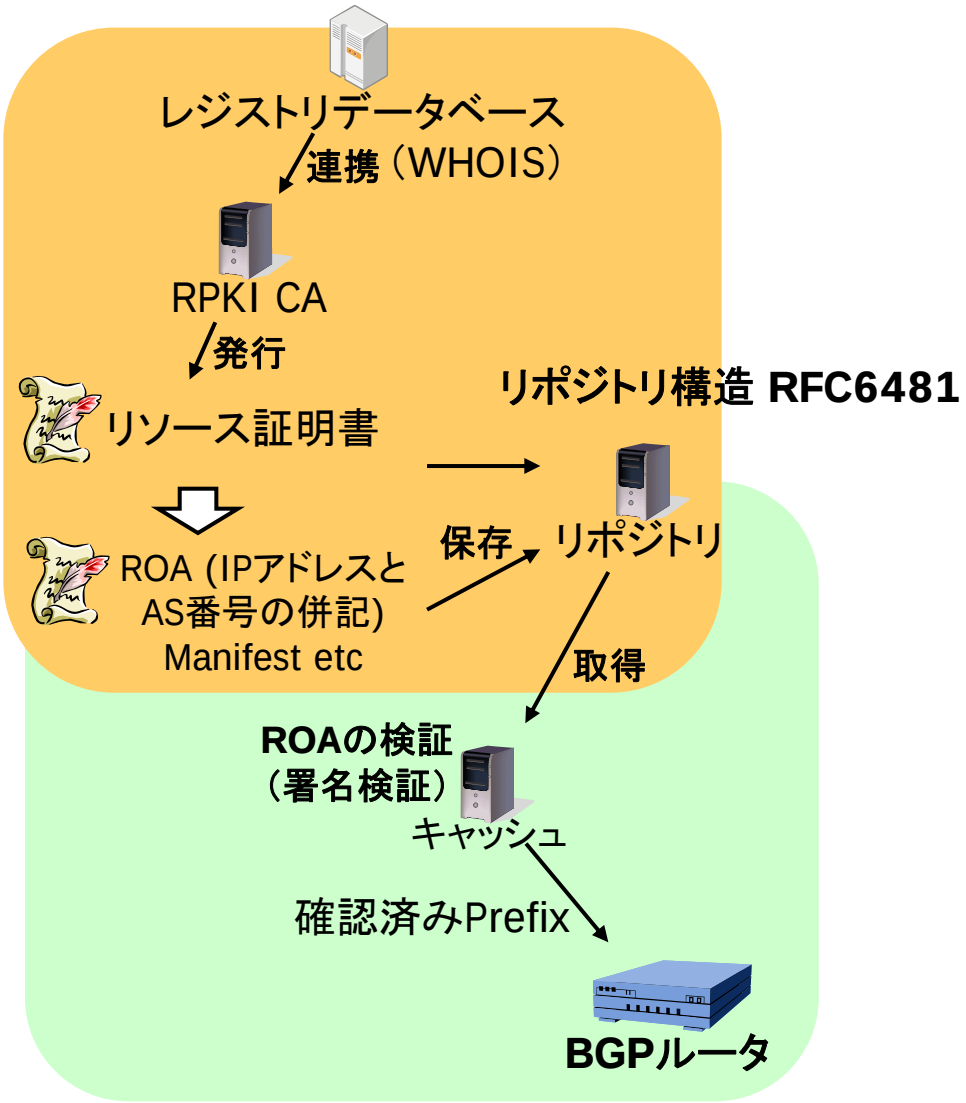
アーキテクチャ RFC6480

証明書プロファイル RFC6487
証明書ポリシー RFC6484
アルゴリズム RFC6485
発行処理 RFC6492

Manifest RFC6486
Ghostbusters RFC6493
ROA書式 RFC6482

トラストアンカー RFC6490
ROA検証 RFC6483
prefix検証 RFC6811

RPKI-to-Router RFC6810



RPKIとSecure BGPの目指すもの

- IPアドレスの設定ミスや不正な設定を、BGPルーターで検知できる仕組み
  - Origin Validation
    - 他のネットワークが自ASのIPアドレスを使い始めたことが検知できる
  - Path Validation
    - ASパスが途中で変えられてしまったことが検知できる

BGPSEC
＝ Origin Validation ＋ Path Validation

SIDR WG – ドキュメント状況

- BGPSEC関連

draft-ietf-sidr を省略

An Overview of BGPSEC （BGPSECの概要）	bgpsec-overview-03 2013-07-15（**大きな変更なし**）
A Profile for BGPSEC Router Certificates, Certificate Revocation Lists, and Certification Requests （ルーター証明書、CRL、発行要求のデータ書式）	bgpsec-pki-profiles-06 2013-09-17（**大きな変更なし**）
BGPSEC Protocol Specification （BCPSECのプロトコル仕様）	bgpsec-protocol-08 2013-11-05（**大きな変更なし**）
Threat Model for BGP Path Security （BGPパスのセキュリティにおける脅威モデル）	bgpsec-threats-08 2013-11-22（IESGレビュ中）
Security Requirements for BGP Path Validation （BGPパス検証のためのセキュリティ要求）	bgpsec-reqs-08 2013-10-09（**大きな変更なし**）
BGP Algorithms, Key Formats, & Signature Formats （鍵のアルゴリズム、書式、署名形式）	bgpsec-algs-05 2013-09-17（**大きな変更なし**）
BGPSEC router key rollover as an alternative to beaconing （BGPルータにおけるキーロールオーバー）	bgpsec-rollover-02 2013-04-15（Expired）

SIDR WG – ドキュメント状況

- BGPSEC関連（新しいI-D）

draft-ietf-sidr を省略

BGPSec Considerations for AS Migration （AS番号の変更）	as-migration-00 2013-07-10
Template for a Certification Practice Statement (CPS) for the Resource PKI (RPKI) （RPKIのためのCPSテンプレート）	cps-isp-03 2013-10-08
Policy Qualifiers in RPKI Certificates （policyQualifierを入れるためのRFC6487の変更）	policy-qualifiers-01 2013-10-02
A Publication Protocol for the Resource Public Key Infrastructure (RPKI) （XMLを使ったRPKIの情報公開プロトコル）	publication-04 2013-10-20
Router Keying for BGPsec （RTRのための鍵生成）	rtr-keying-03 2013-09-17
BGP Prefix Origin Validation State Extended Community （BGPルータにおける状態のエンコード方式）	origin-validation-signaling-03 2013-08-29
Responsible Grandparenting in the RPKI （IPアドレスの割り振り元の登録がない場合などの対応）	個人ドラフトgrandparenting-03 2013-08-03

SIDR WG – ドキュメント状況

- わけありExpired

draft-ietf-sidr を省略

Local Trust Anchor Management for the Resource Public Key Infrastructure （ローカルトラストアンカー）	ltamgmt-08 2013-04-05（新しい方向へ）
Multiple Repository Publication Points support in the Resource Public Key Infrastructure (RPKI) （複数の配布ポイントを作るためのURL表記）	multiple-publication-points-00 2013-05-22（
Securing RPSL Objects with RPKI Signatures （WHOISやIRRで使われている記述言語RPSLにおけるRPKI署名）	rpsl-sig-05.txt 2012-05-10（新しい著者？）

ミーティング

- Secure Inter-Domain Routing WG
  - 2013年11月5日 9:00-11:30 (40名ほど)

アジェンダと議論　－　WG documents

- An Out-Of-Band Setup Protocol For RPKI Production Services, Rob Austein
  - draft-austein-sidr-rpki-oob-setup-00
  - RPKI CA間のRPKI用「Business PKI」の相互認証プロトコル。MLで議論開始。
- A Publication Protocol for the Resource Public Key Infrastructure (RPKI), Rob Austein
  - draft-ietf-sidr-publication-04
  - XMLを使ったRPKIの情報公開プロトコル。実装がまだ一つのみ。Standard(ST)を目指す。

アジェンダと議論 － Deployment

- Report on RPKI Interoperability testing, David Mandelberg
  - 相互運用実験。テストデータの署名検証。CRLに不明な番号が入っている場合の対応方法をディスカッション。結論：acceptすべき。

アジェンダと議論　－　継続案件

- Suspenders: A Fail-safe Mechanism for the RPKI
  - draft-kent-sidr-suspenders-00
  - LTAMに代わるLOCKの提案
    - リソース証明書の検証をせずに、ROAを検証する方式。RPKI CAが公開鍵とURLを持つ「LOCK」を発行しておくと、URL先のデータ「INRD」で指定されているROAを区別できる。
  - 議論
    - どのLOCKを信用すればいいのか。
    - 外部データを加えることと時間の要素を加えることに懸念がある。
    - 不必要なチェックが増えてしまうのでは。
      ほか

アジェンダと議論　－　継続案件

- Validation changes
  - draft-huston-rpki-validation-00
  - IPアドレスが移転されるときのリソース証明書の有効性についてのI-D。どういう手順になるのか。
  - 議論
    - 直接関係のないEEと別のRIRなどが手順を踏む必要があり、有効性を保つためには複雑過ぎる。
    - 結論
      - 移転のセマンティクスをWGで議論できるようにすべき。

デプロイメントの状況

～ Topic エクアドルのIXP ～

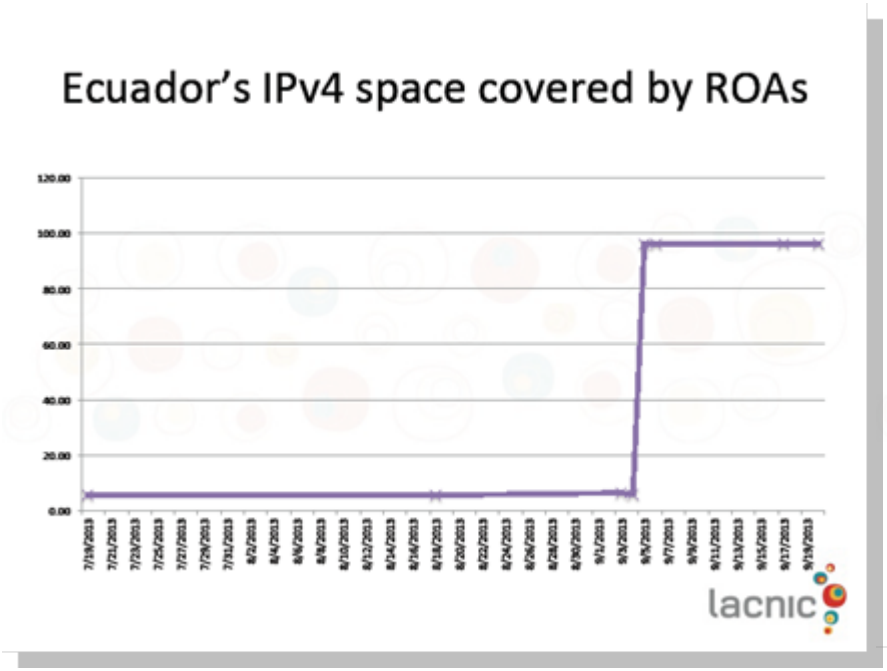
Topic　エクアドル（1/2）

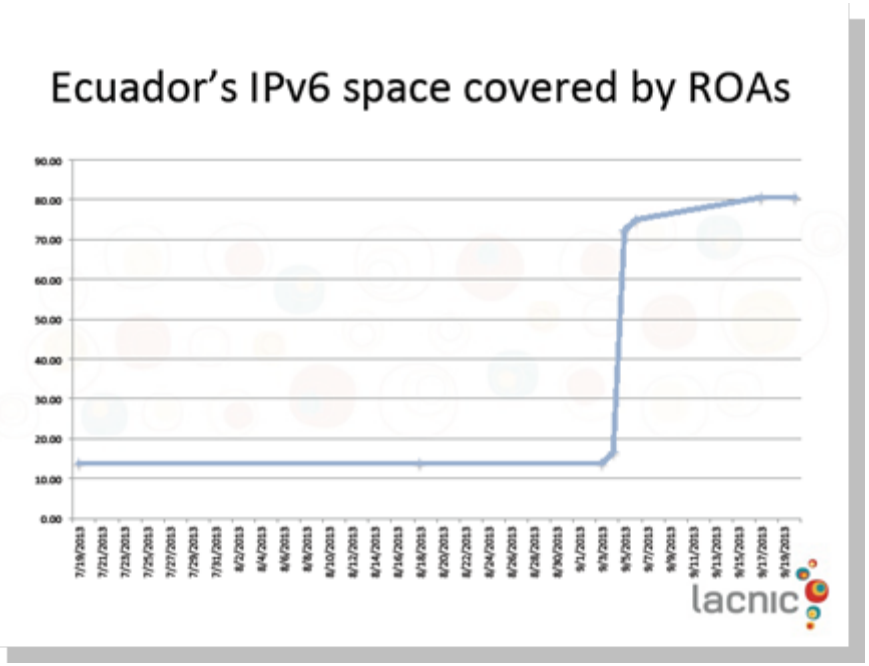
- エクアドル国内のIXPであるNAP.ECでRPKIを導入するイベントが開催される（2013年7月、9月）
- IPアドレスの割り振り先組織の担当者が集まってリソース証明書とROAを発行
- ルートサーバにおけるOrigin Validationが実装されるなどツールを用意

RPKI and Origin Validation Deployment in Ecuador, Nov 3 2013, Sofa Silva Berenguer, http://www.iepg.org/2013-11-ietf88/RPKI-Ecuador-Experience-v2b-1.pdf より

Topic　エクアドル(2/2)

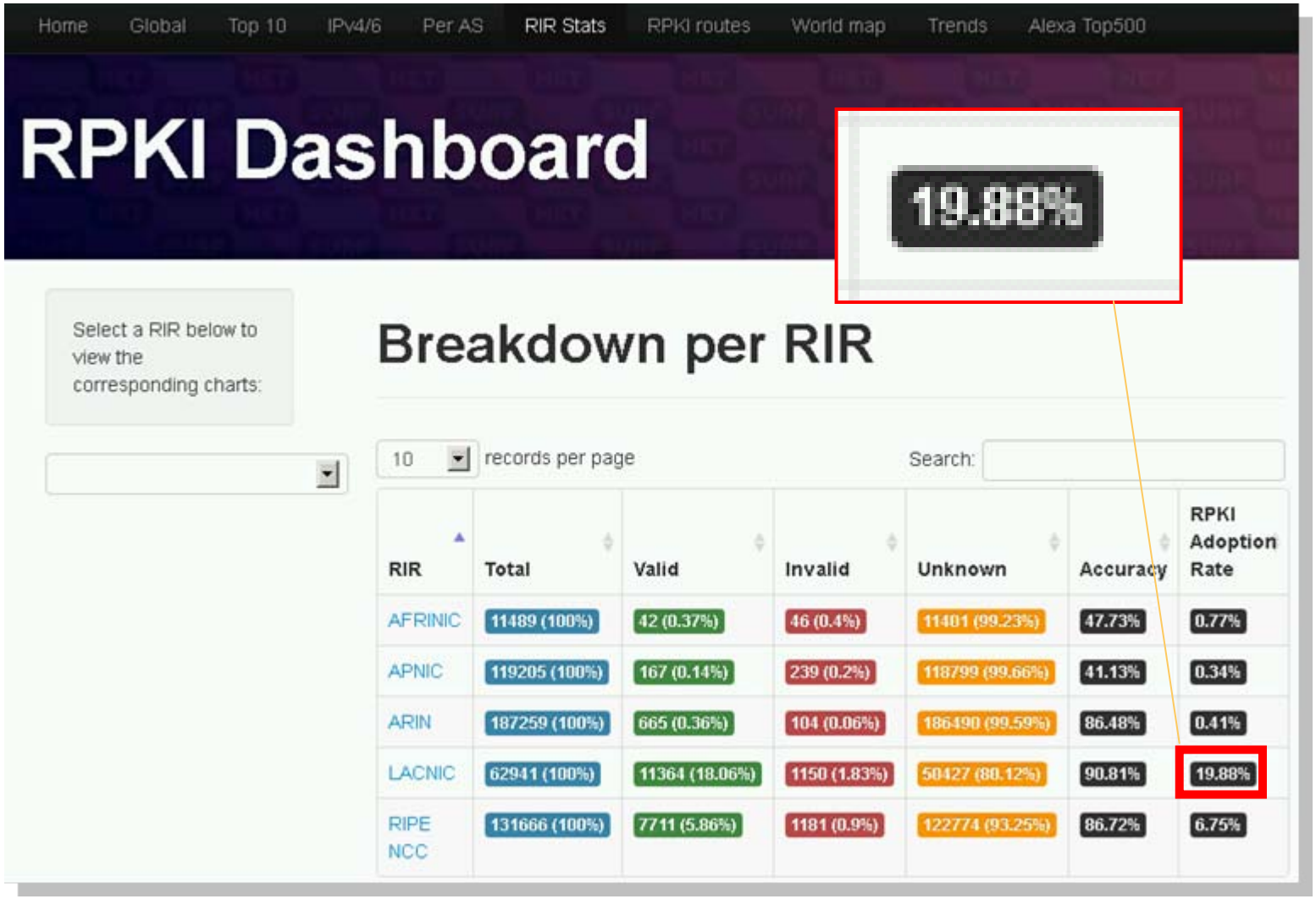
- 2013年9月4日～5日にROAの発行数が激増
- IPv4、IPv6共にカバー率が90%ほどに上昇





RPKI and Origin Validation Deployment in Ecuador, Nov 3 2013, Sofa Silva Berenguer, http://www.iepg.org/2013-11-ietf88/RPKI-Ecuador-Experience-v2b-1.pdf

RPKI Dashboardでみても



RPKI Dashboard, http://rpki.surfnet.nl/

論点と今後

（1）RPKIの普及

- 利用環境
  - BGPルーター
  - RPKI cache サーバ

- 尺度

  A)どれくらいの著名なWebサイトのIPアドレスが有効なROA範囲内にあるか

  B)経路広告されている経路情報のうち、ROAがカバーしているprefixの数

BGPルーター

- Cisco
  – ASR1000, 7200, 7600 in releases 15.2(1)S or XE 3.5
  – IOS-XR 4.2.1以降

（設定例　RPKI cacheサーバの指定）

```
cisco-rpki-rtr#show running-config | begin bgp

router bgp 64500
 bgp log-neighbor-changes
 bgp rpki server tcp 10.1.1.6 port 8282 refresh 600
```

(参考)
http://www.ripe.net/lir-services/resource-management/certification/router-configuration
http://www.cisco.com/en/US/partner/docs/routers/asr9000/software/asr9k_r4.2/general/release/notes/reln_a9k_421.html

BGPルーター

- JunOS
  - Release 12.2以降

（設定例　RPKI cacheサーバの指定）

```
routing-options {
    autonomous-system 64511;
    validation {

        group rpki-validator {
            session 10.1.1.6 {
                refresh-time 120;
                hold-time 180;
                port 8282;
                local-address 10.1.1.5;
            }
        }
    }
}
```

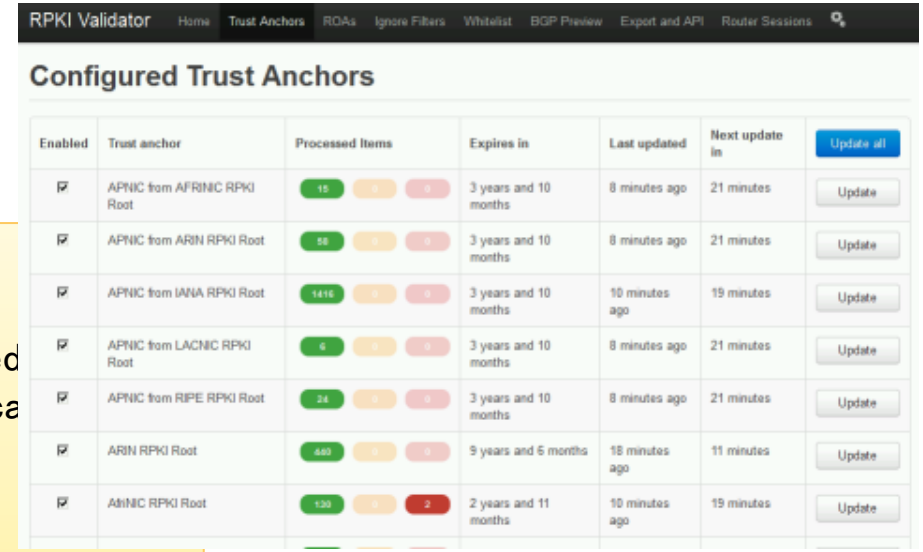
(参考)
http://www.ripe.net/lir-services/resource-management/certification/router-configuration

RPKI cache サーバ

- RPKI Tools
  https://rpki.net/

  # apt-get install rpki-rp

- RIPE NCC RPKI Validator

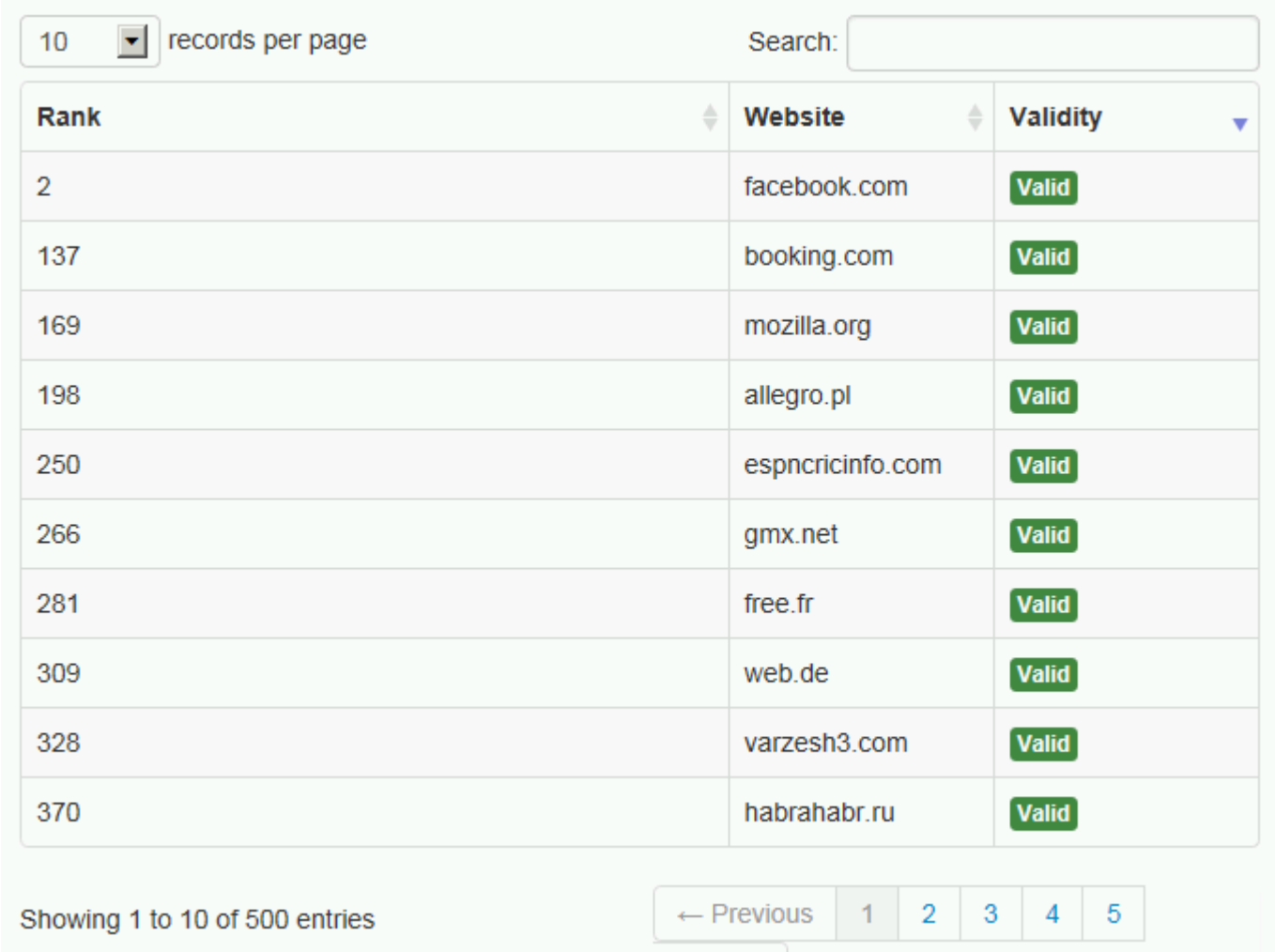


http://localcert.ripe.net:8088/trust-anchors

```
[rcynic]
rsync-program = /usr/bin/rsync
authenticated   = /var/rcynic/data/authenticated
unauthenticated = /var/rcynic/data/unauthentica
lockfile = /var/rcynic/data/lock
xml-summary = /var/rcynic/data/rcynic.xml
jitter = 600
use-syslog = true
log-level = log_usage_err

trust-anchor-locator.1 = /var/rcynic/etc/apnic-testbed.tal
```

Top sites



10 records per page Search:

Rank	Website	Validity
2	facebook.com	Valid
137	booking.com	Valid
169	mozilla.org	Valid
198	allegro.pl	Valid
250	espncricinfo.com	Valid
266	gmx.net	Valid
281	free.fr	Valid
309	web.de	Valid
328	varzesh3.com	Valid
370	habrahabr.ru	Valid

Showing 1 to 10 of 500 entries ← Previous 1 2 3 4 5

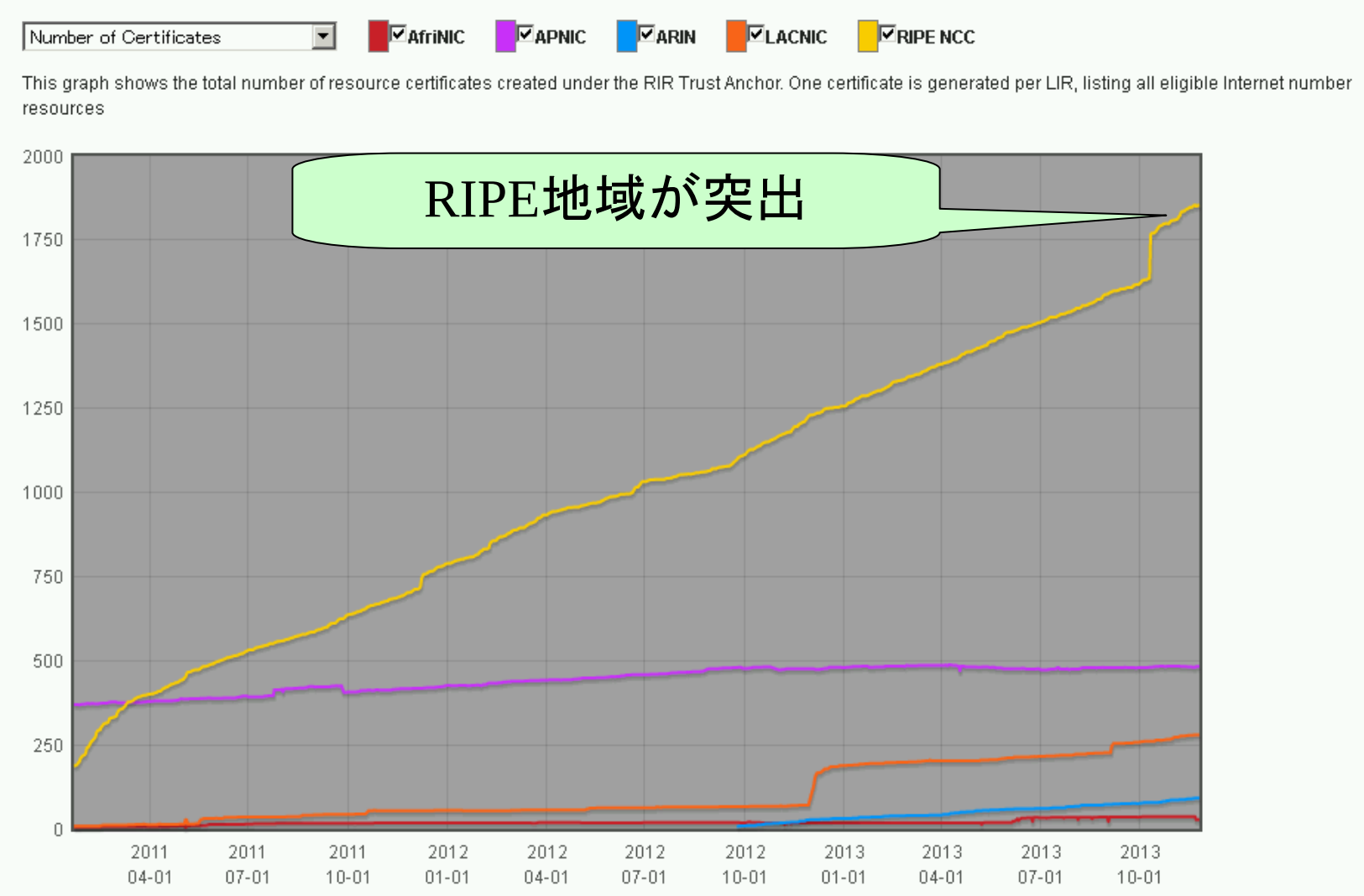
RPKI Dashboard, http://rpki.surfnet.nl/top500.php

RPKI Adoption Rate

RIR	Total	Valid	Invalid	Unknown	Accuracy	RPKI Adoption Rate
AFRINIC	11489 (100%)	42 (0.37%)	46 (0.4%)	11401 (99.23%)	47.73%	0.77%
APNIC	119205 (100%)	167 (0.14%)	239 (0.2%)	118799 (99.66%)	41.13%	0.34%
ARIN	187259 (100%)	665 (0.36%)	104 (0.06%)	186490 (99.59%)	86.48%	0.41%
LACNIC	62941 (100%)	11364 (18.06%)	1150 (1.83%)	50427 (80.12%)	90.81%	19.88%
RIPE NCC	131666 (100%)	7711 (5.86%)	1181 (0.9%)	122774 (93.25%)	86.72%	6.75%

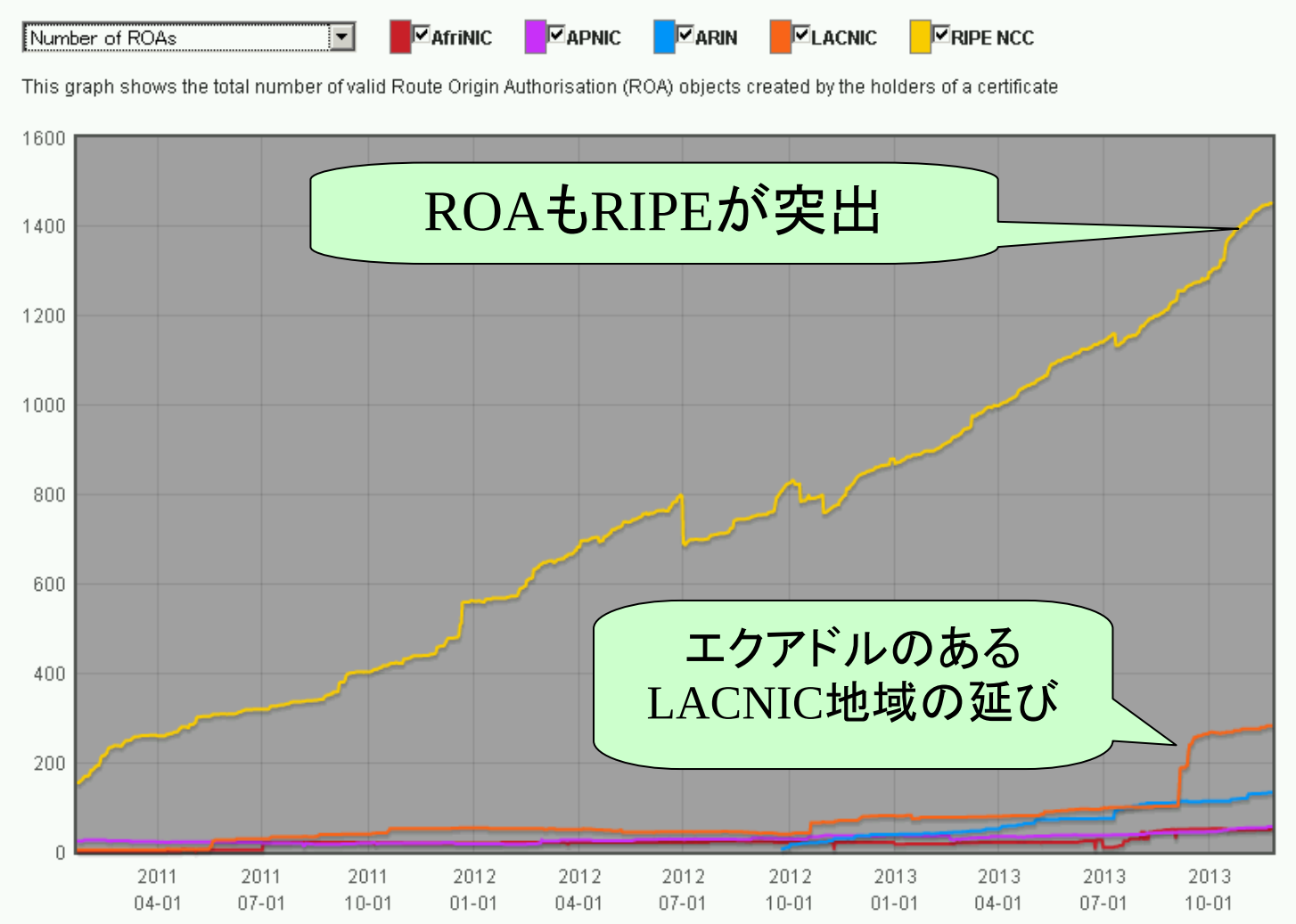
RPKI Dashboard, http://rpki.surfnet.nl/

内訳:リソース証明書の発行数



Statistics, RIPE NCC, http://certification-stats.ripe.net/

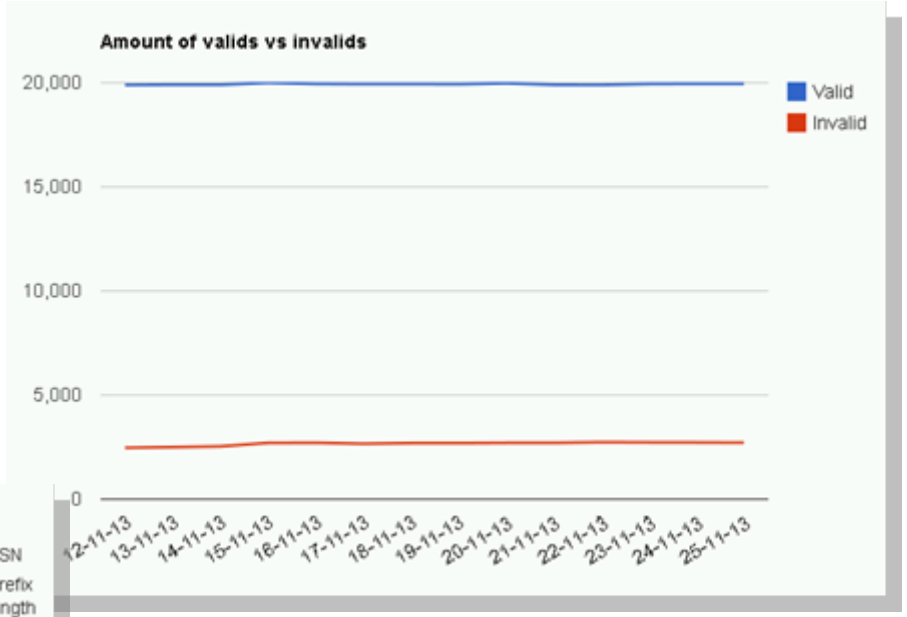
内訳:ROAの発行数

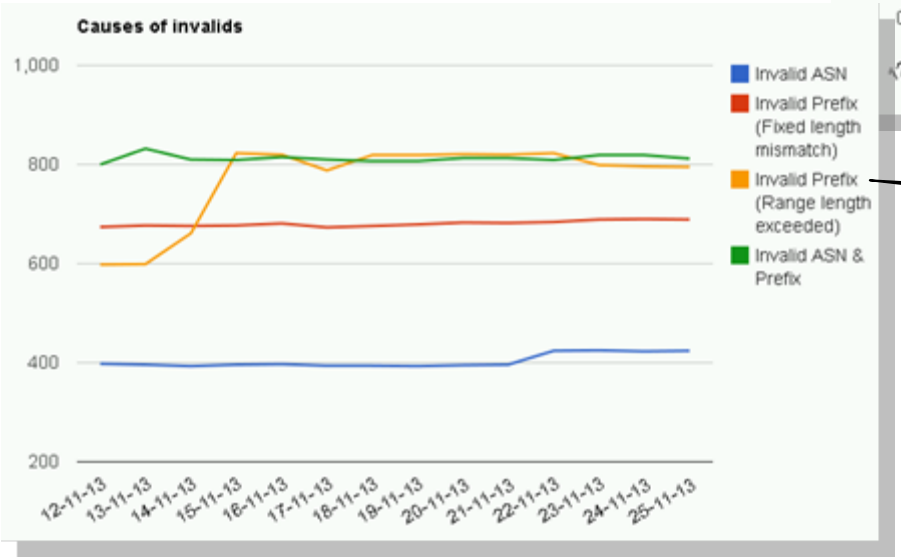


Statistics, RIPE NCC, http://certification-stats.ripe.net/

ROAと経路情報との違い

51万経路中ROAに照らし合わせてvalidだったprefix数約20,000





invalidだった2,720 prefixの内訳。AS番号が異なる「Invalid ASN」は1,200近くある。

RPKI Dashboard, http://rpki.surfnet.nl/ より

（2）BGPSECの仕組みと議論

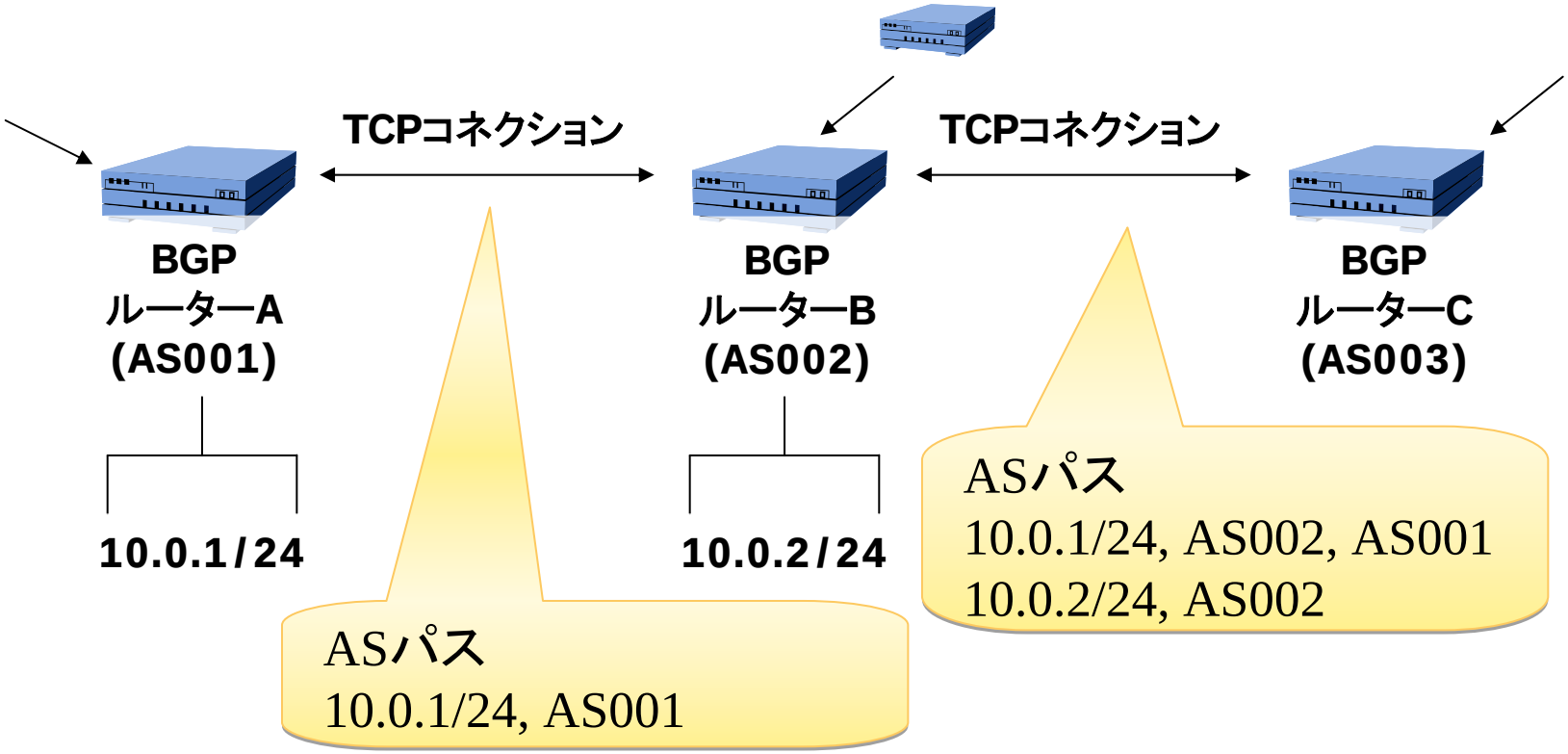
□BGPSECとは

- Origin ValidationとPath Validationが行われたBGPのセキュリティ技術
  - Path Validationとは電子署名の技術を使ってASパスを確認すること

□GROW(Global Routing Operations) WGにおける指摘

- draft-ietf-grow-simple-leak-attack-bgpsec-no-help

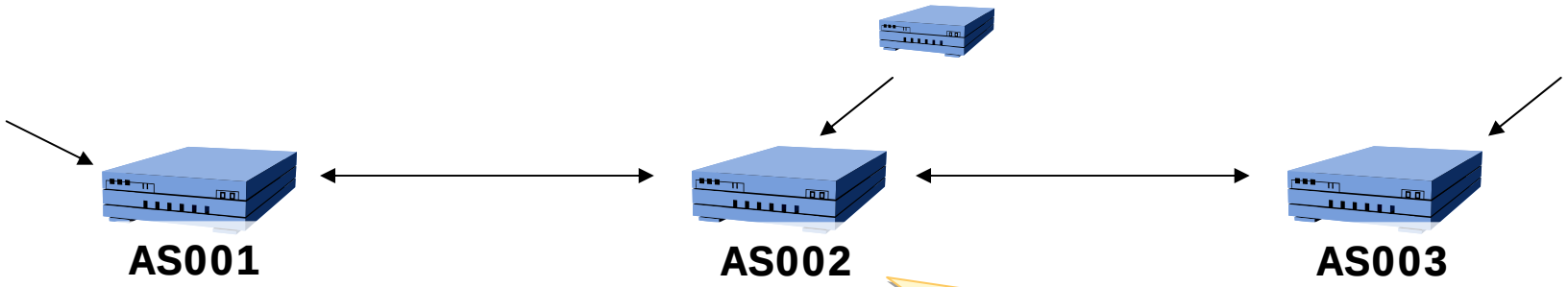
BGPとASパス



BGPは、BGPルーターが、IPアドレスやASパスについてPeer（またはNeighbor）と交換するためのプロトコル。BGPでは、基本的にセッションを張ったままにし、ネットワークトポロジーに変更があるとUpdateメッセージと呼ばれるメッセージを送りあう。

7. インターネット経路制御のセキュリティに関する動向 – BGPSEC, IPA, 2011年12月, http://www.ipa.go.jp/security/fy23/reports/tech1-tg/b_07.html

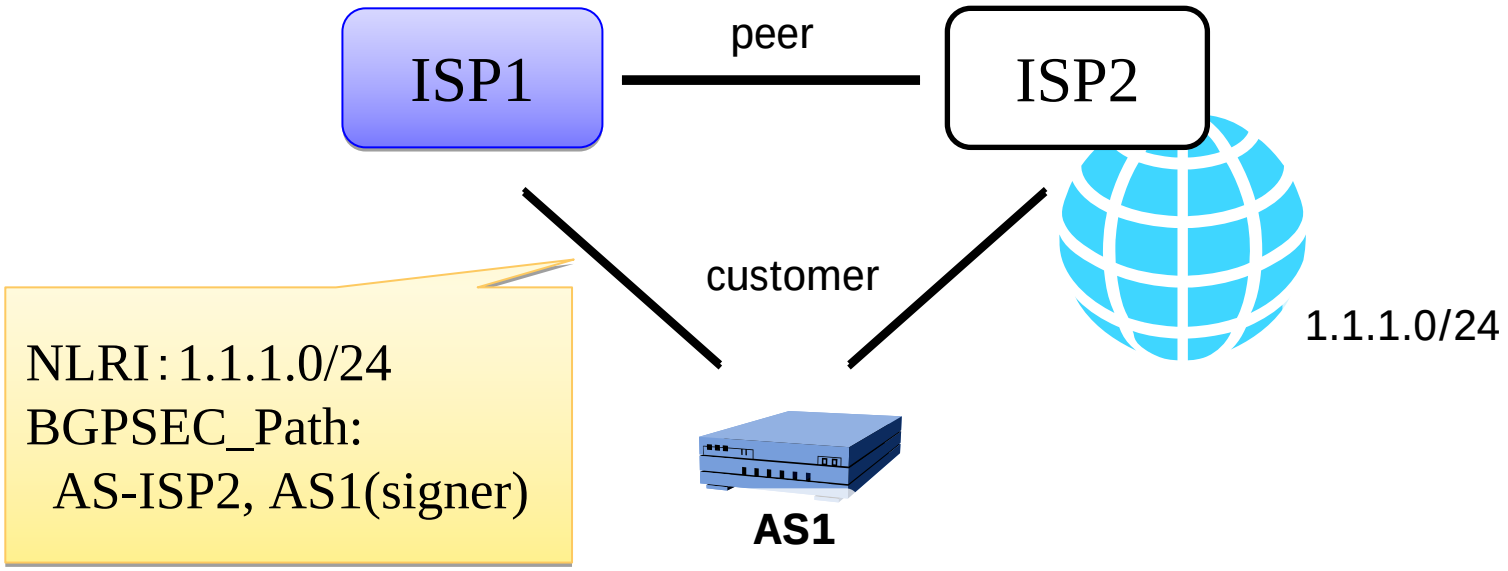
BGPSEC Path Signature



NLRI：10.0.1/24
BGPSEC_Path:
  Secure_Path:
    AS001(target),AS002(signer), pCount, Sig(AS001, AS002, pCount)

NLRI: Network Layer Reachability Information（ネットワーク層到達性情報）

Route-Leaks & MITM Attacks Against BGPSEC draft-ietf-grow-simple-leak-attack-bgpsec-no-help



AS1が、ISP2から受けた経路情報をISP1に流し、ISP1が受け入れるポリシーである場合（customer経路をpeerからの経路よりも優先する場合）ISP1から1.1.1.0/24に向けた経路はAS1を通ることになってしまう。BGPSEC_Pathに含めるAS番号を制限できないために起こることが指摘されている。

Route-Leaks & MITM Attacks Against BGPSEC,
draft-ietf-grow-simple-leak-attack-bgpsec-no-help-03 より

写真

Bits-N-Bites

バンクーバー市内の様子

おわり