T6
RPKI/ROAの国際動向
～ どんなときに使える!? ～

木村泰司

2016年11月29日(火)

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)
  - 国際動向(IETF)

RPKI/ROAの国際動向

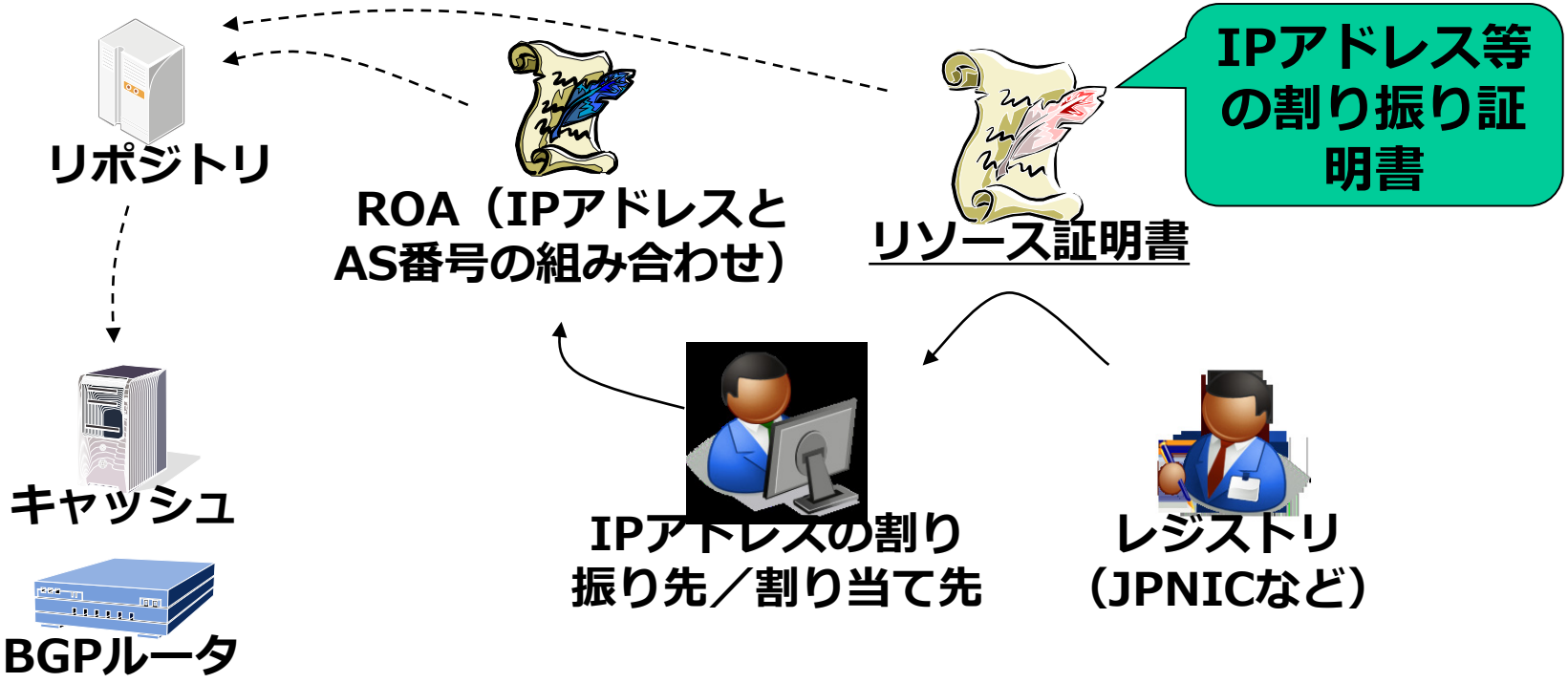
- RPKI/ROA 最新動向
- AS Path Validation
- BGP communityと共に

RPKI 最新動向

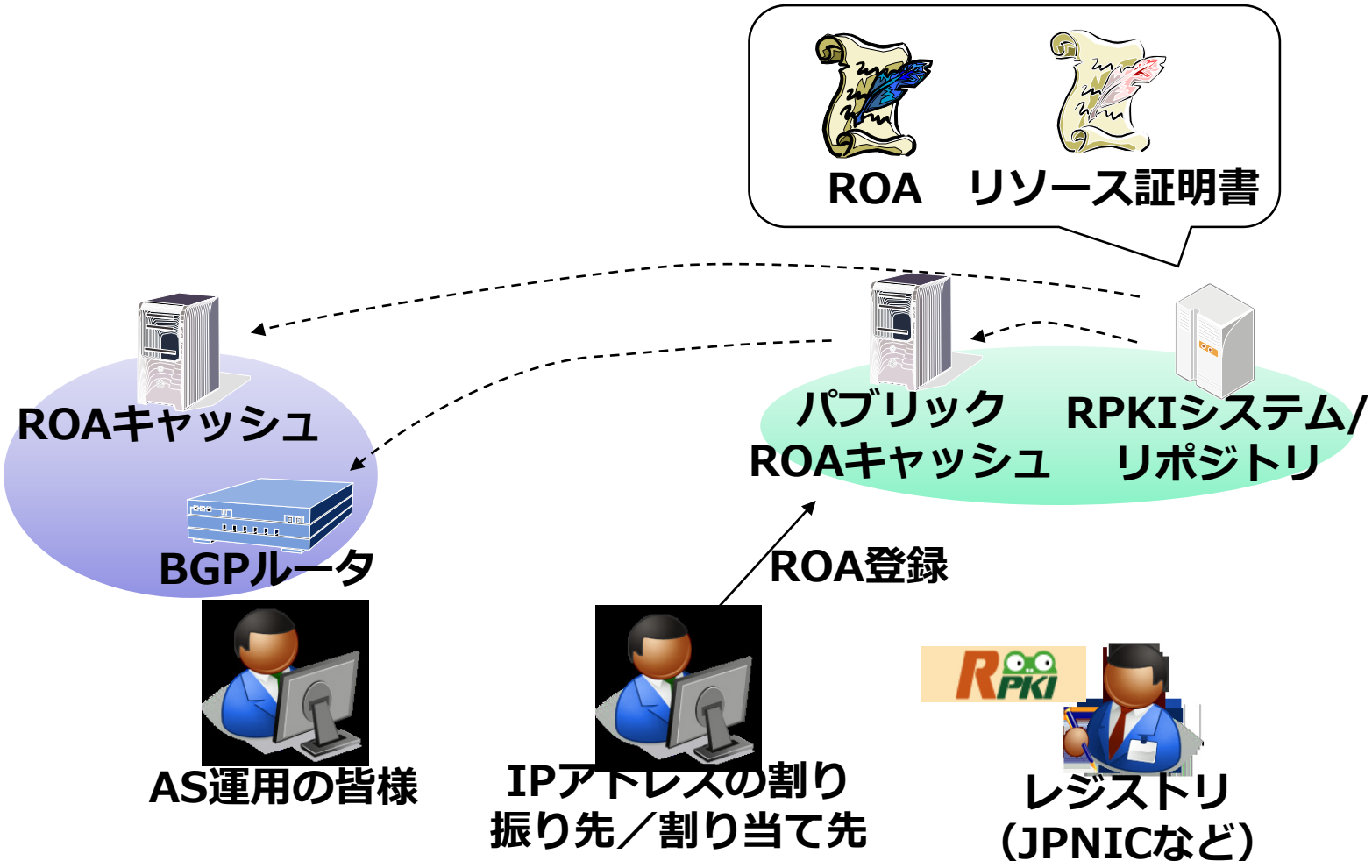
RPKIとは(1/2) - モデル

RPKI （リソースPKI）

⇒ Resource Public-Key Infrastructure



RPKIとは(2/2) - 実際のご利用の形



国際的な普及の状況(1/3)

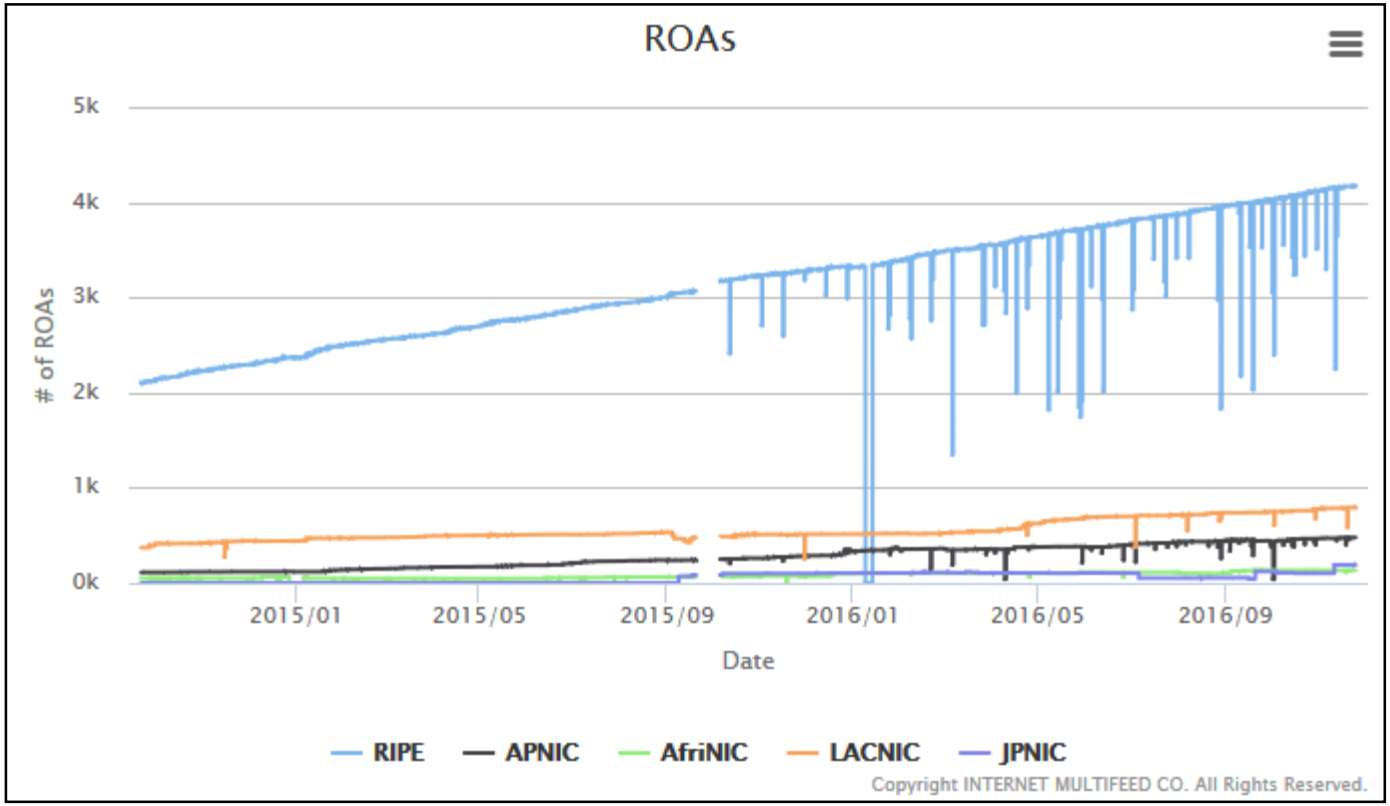
RPKI Dashboard, SURFnet, 2016/11/25
http://rpki.surfnet.nl/

RIR	Total	Valid	Invalid	Unknown	Accuracy	RPKI Adoption Rate
AFRINIC	15655 (100%)	304 (1.94%)	20 (0.13%)	15331 (97.93%)	93.83%	2.07%
APNIC	178144 (100%)	5465 (3.07%)	1201 (0.67%)	171478 (96.26%)	81.98%	3.74%
ARIN	242994 (100%)	2760 (1.14%)	621 (0.26%)	239613 (98.61%)	81.63%	1.39%
LACNIC	80763 (100%)	15001 (18.57%)	1283 (1.59%)	64479 (79.84%)	92.12%	20.16%
RIPE NCC	176105 (100%)	19560 (11.11%)	2263 (1.29%)	154282 (87.61%)	89.63%	12.39%

2015年に比べるとすべての地域で1～2%ほど上昇

国際的な普及の状況(2/3)

ROA数, MF RPKI Project, 2016/11/25
http://www.mfeed.co.jp/rpki/roa_cache/statistics.html#roas



ROA数はRIPE地域がダントツ。APNICの地域は直接MyAPNICを使用するLIRは開始するも…

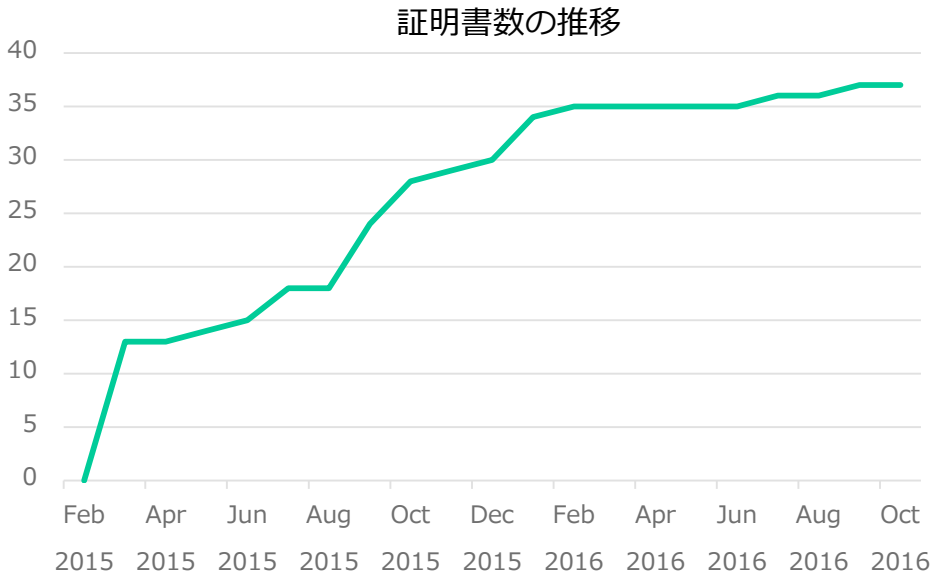
国際的な普及の状況(3/3)

- **CNNIC**
  - RPKIのテスト環境を希望者向けに提供中
  - RPKIシステムを開発中（～12月予定）
  - IPアドレスの移転や運用ミスの影響に配慮するための実験やInternet-Draft作成などが活発
- **KRNIC**
  - RPKIの試験的な提供に向けた準備活動中
- **IRINN（インドのNIR）**
  - 調査中
- **JPNIC**
  - RPKIシステムは試験提供されているが、APNICとの接続は作業中（接続したが技術課題あり)

NIRにおける準備と提供が普及の鍵と考えられる。ただしルーティングセキュリティの注目度は高くない。

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
  - 37
- 発行されているROA
  - 103
- 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
  - 2.00% IPv4
    - 1.76% (2015)
  - 0.93% IPv6 (/48の個数)
    - 0.86% (2015)



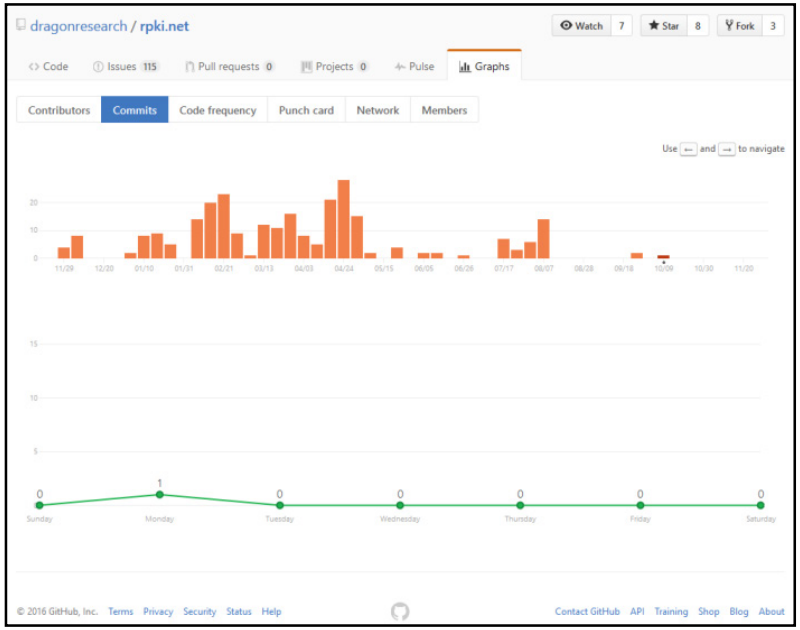
実装の最新動向(1/3)

- **RPKI Tools**

  http://rpki.net/

  https://github.com/dragonresearch/rpki.net

  - GitHubへ移行
  - 内部コードをかなり刷新(RRDPには未対応)



実装の最新動向(2/3)

- **RPKI Validator**

  https://github.com/RIPE-NCC/rpki-validator
  - 2017年度には多国語言語対応などを予定
- **RPKI Validator --- JPNICで日本語化**

  http://roa2.nic.ad.jp:8080/

実装の最新動向(3/3)

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

  https://www-x.antd.nist.gov/bgpsrx/

  - AS Path Validation に対応！

- **BIRD BGPsec**

  http://www.securerouting.net/tools/bird/

BGP-SRxの経路をBIRD BGPsecで検証に成功！
(IETF97 SIDR WGにて発表)

標準化動向

- **IETF Secure Inter-Domain Routing WG (SIDR)**
  - Slurm – 検証結果を上書きする提案
    - 継続議論中
  - CA同士の相互運用性テストの必要性
- **IETF SIDR Operations(sidrops) WG設立**
  - ルーティングオペレーターだけでなくCA運用やROAの導入されていないASオペレーターを含めた運用の議論の場

    https://datatracker.ietf.org/wg/sidrops/charter/

SIDR WGはcloseの方向。今後、IPアドレス移転やASの引っ越しなど、sidropsで議論される。

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/

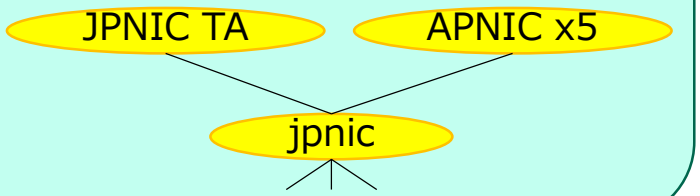
  - IPアドレスの割り振りを受けている方がROAを登録したりRPKIのCAを立ち上げてつなげたりできる。
- **ROAキャッシュサーバ**

  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

"jpnic"がAPNICとつながりましたがROAはまだ発行できていないです…



AS Path Validation

覚えていますか....

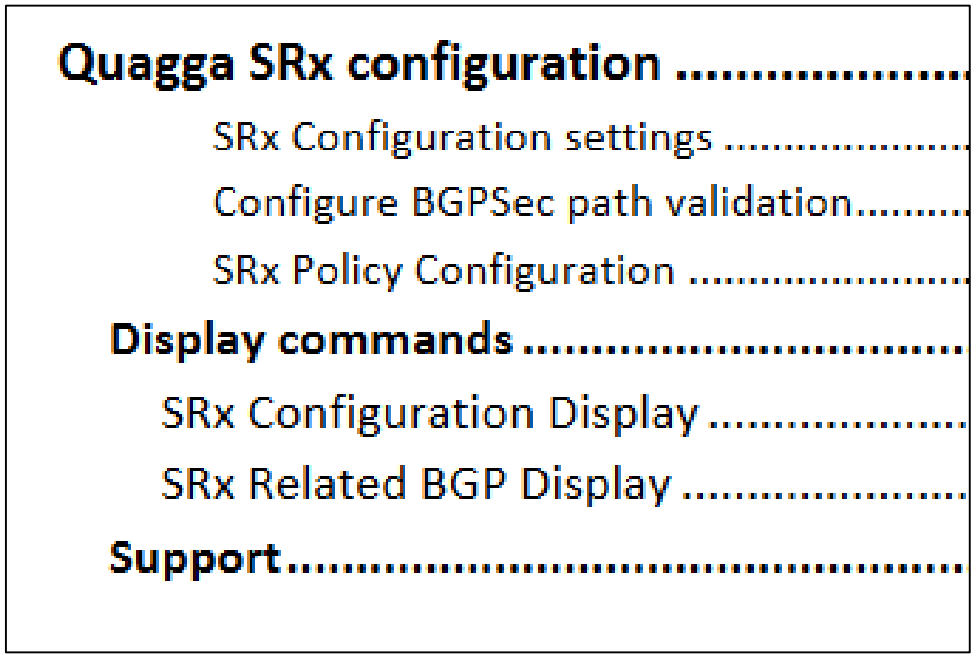
```
# telnet localhost bgpd
Escape character is '^]'.

Hello, this is QuaggaSrx (version 0.99.16-0.3.0.0
Copyright 1996-2005 Kunihiro Ishiguro, et al.

User Access Verification
Password:
bgpd> en
bgpd# sh ip bgp

BGP table version is 0, local router ID is 192.41
Status codes: s suppressed, d damped, h histor        d, > best, i - internal,
              r RIB-failure, S Stale, R Rem

Validation:    v - valid, n - notfoun       - invalid, ? - undefined
SRx Status:    I - route ignored,           SRx evaluation deactivated
SRxVal Format: validation resu             (origin validation, path validation)
Origin codes: i - IGP, e - E P, ? - incomplete

   Ident     SRxVal SRxLP Status Network          Next Hop            Metric  LocPrf Weight Path
*> DE83681B v(v,-) + 200,       202.12.30.0      192.41.192.226                200s      0 65001 2515 i
*> FBF4BE57 n(n,-) + 100,       202.12.31.0      192.41.192.226                100s      0 65001 2515

bgpd#
```

Ident SRxVal SRxLP Status

*> DE83681B v(v,-) + 200,

*> FBF4BE57 n(n,-) + 100,

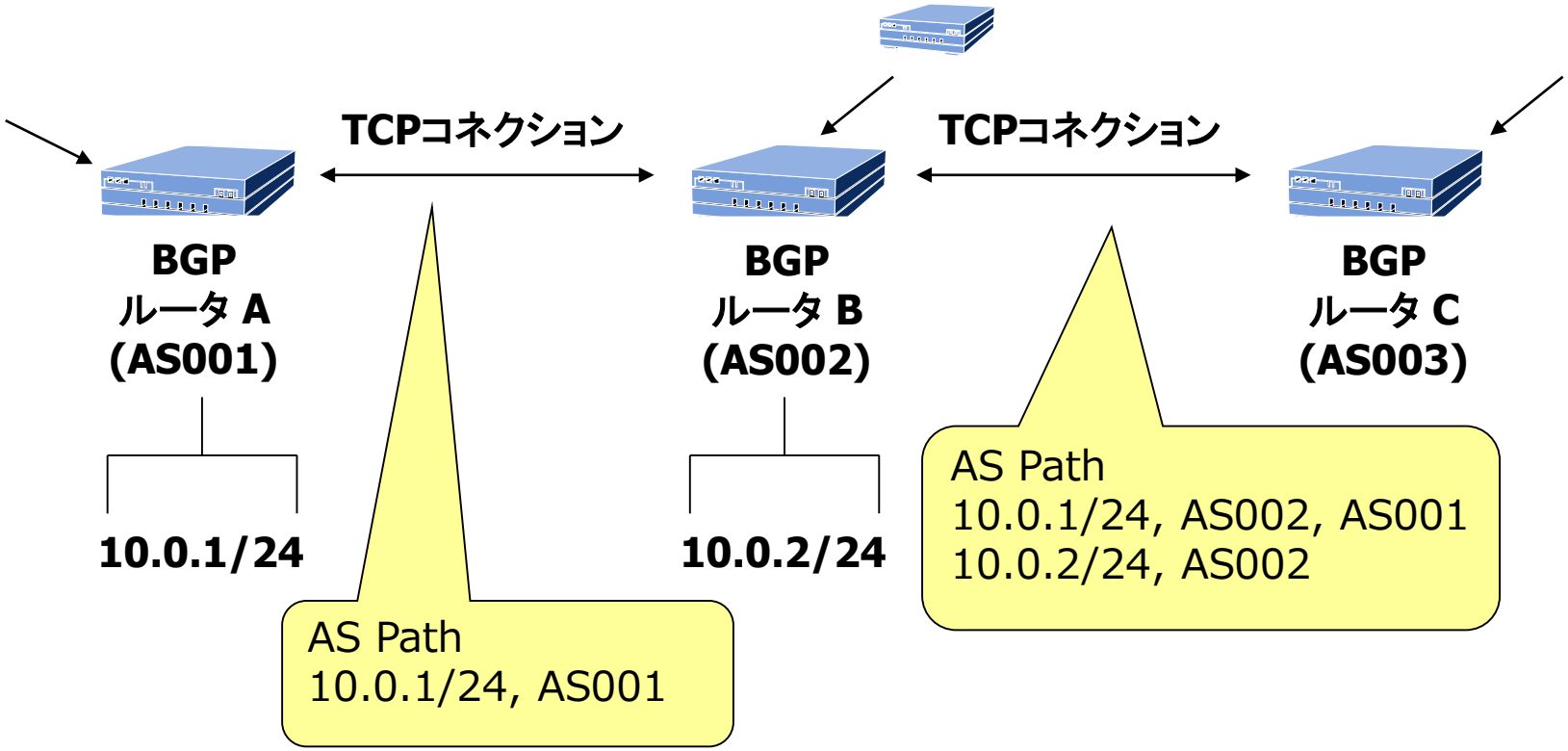
NIST BGP-SRx で実装!!



QuaggaSRx Users Manual
https://www-x.antd.nist.gov/bgpsrx/documents/QuaggaSRxUsersManual-4-1-a.pdf

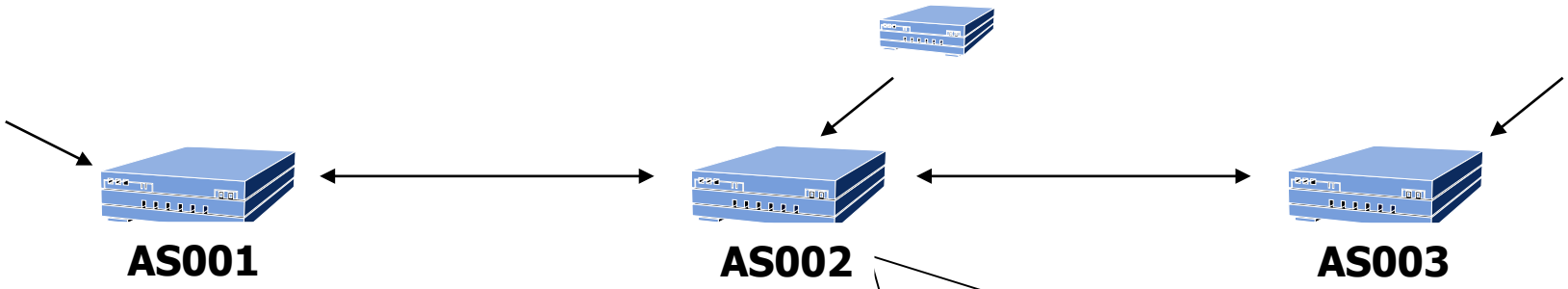
AS Path Validatioとは(1/3)

- AS Pathに…



AS Path Validationとは(2/3)

- "BGPSEC Path Signature"をつけて…

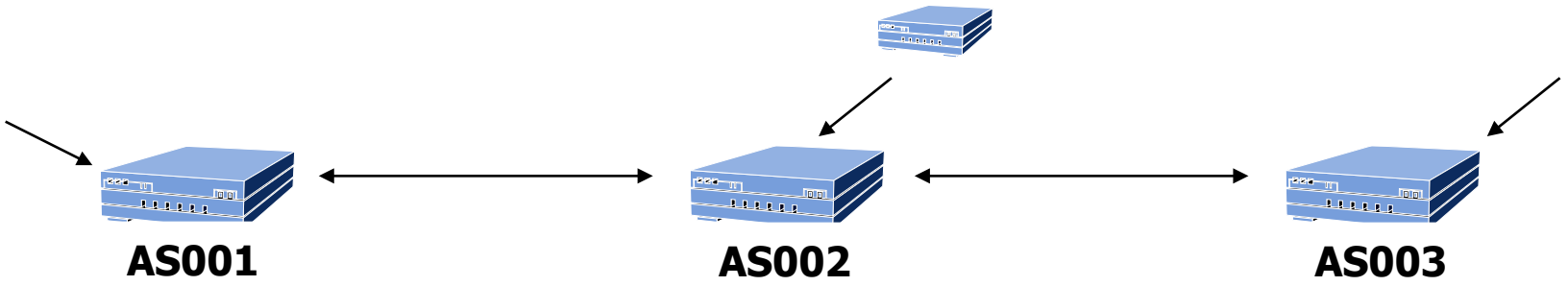


NLRI : 10.0.1/24
AS_Path: AS002 AS001
BGPSEC_Path_Signatures
　AS001 sig　{10.0.1/24, AS001, AS002}
　AS002 sig　{ {10.0.1/24, AS001, AS002} , AS003}

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

AS Path Validationとは(3/3)

- 渡してゆくことで、ASの意図通りのPathになっているかどうかを確認する機能です。



NLRI : 10.0.1/24
AS_Path: AS003 AS002 AS001
BGPSEC_Path_Signatures
AS001 sig {10.0.1/24, AS001, AS002}
AS002 sig { {10.0.1/24, AS001, AS002} , AS003}
AS003 sig { {10.0.1/24, AS001, AS002, AS003} , AS004}

動いたようです

- **AS Path Validationによる不正なAS Pathを検知する動作例**
  - BGPSec Interoperability Test , QuaggaSRx and BIRD BGPsec, IETF 97 , Seoul, South Korea Nov. 17, 2016

  https://www.ietf.org/proceedings/97/slides/slides-97-sidr-bgpsec-interoperability-quaggabird-01.pdf

  - Origin Validationの結果「i (i, v) 」と AS Path Validationの結果「i (v, i) 」が確認されてました。

    ⇒ 「BGPSEC」完成の日が近づきつつある…

BGP communityと共に

Origin validation status (おさらい)

状態	説明
Valid	Origin ASとprefixがROAと一致しており、最大プレフィックス長(max prefix length)の範囲内
Not found	Origin ASとprefixが一致するROAがない
Invalid	prefixが一致し、最大プレフィックス長(max prefix length)の範囲内にあるがOrigin ASが異なる

Validation結果を伝える仕様

- **"BGP Prefix Origin Validation State Extended Community"**

  [draft-ietf-sidr-origin-validation-signaling]

  - :0 "Valid"　:1 "Not found"　:2 "Invalid"
  - IBGP用
  - デフォルトではEBGPでは送れないが設定したら処理できる(SHOULD)

Validation結果を伝える例

- **ルートサーバからピアにOrigin Validationの結果を伝える "Signaling Prefix Origin Validation Results from a Route-Server to Peers"**

  [draft-ietf-sidr-route-server-rpki-light]

  - ルートサーバから受け取ったValidationの結果を経路制御のために使うことができる

BGP Communityと共に(1/2)

- **Origin Validationの結果を伝える**
  - どこまで動く？RPKI/Router, 2012/7/12, Tomoya Yoshida

    https://www.janog.gr.jp/meeting/janog30/doc/janog30-rpk-after-yoshida-01.pdf
- **AS Path Validationの結果を伝える**
  - RFC/ドラフトなし

もし、Origin ValidationとAS Path Validationの結果を伝えることができたら...

BGP Communityと共に(2/2)

- **アイディア（ディスカッション）**
  - 顧客のprefixがおかしい時、上流に...
  - 顧客側のAS Pathがおかしい時、上流に...
  - 上流から顧客のmis-origin経路がきた時
    （新たな検知/通知サービスとなるか!?）
  - ピア先からのAS Pathがおかしい時、IBGPで...

おわり