RPKIの最新動向のお話 ～トピック～

Internet Routing Security 25, 2016/9/20

木村泰司

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 - notfou        - invalid, ? - undefined
SRx Status:    I - route ignored,          SRx evaluation deactivated
SRxVal Format: validation resu  (origin validation, path validation)
Origin codes: i - IGP, e - E , ? - 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

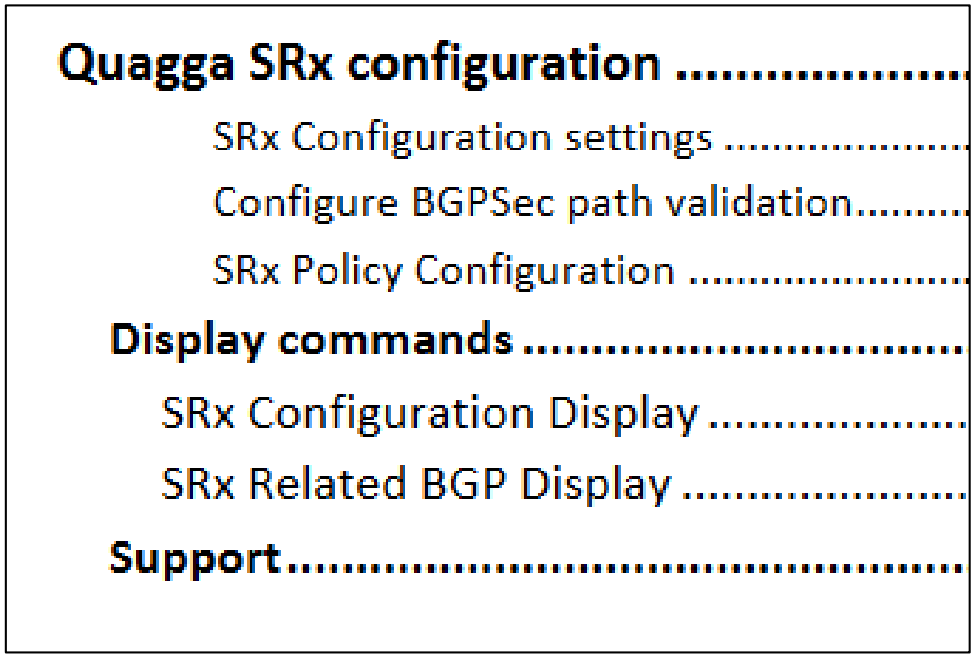
*> DE83681B v(v,-) + 200,

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

まさかの

BGPSEC実装

NIST BGP-SRx で!?

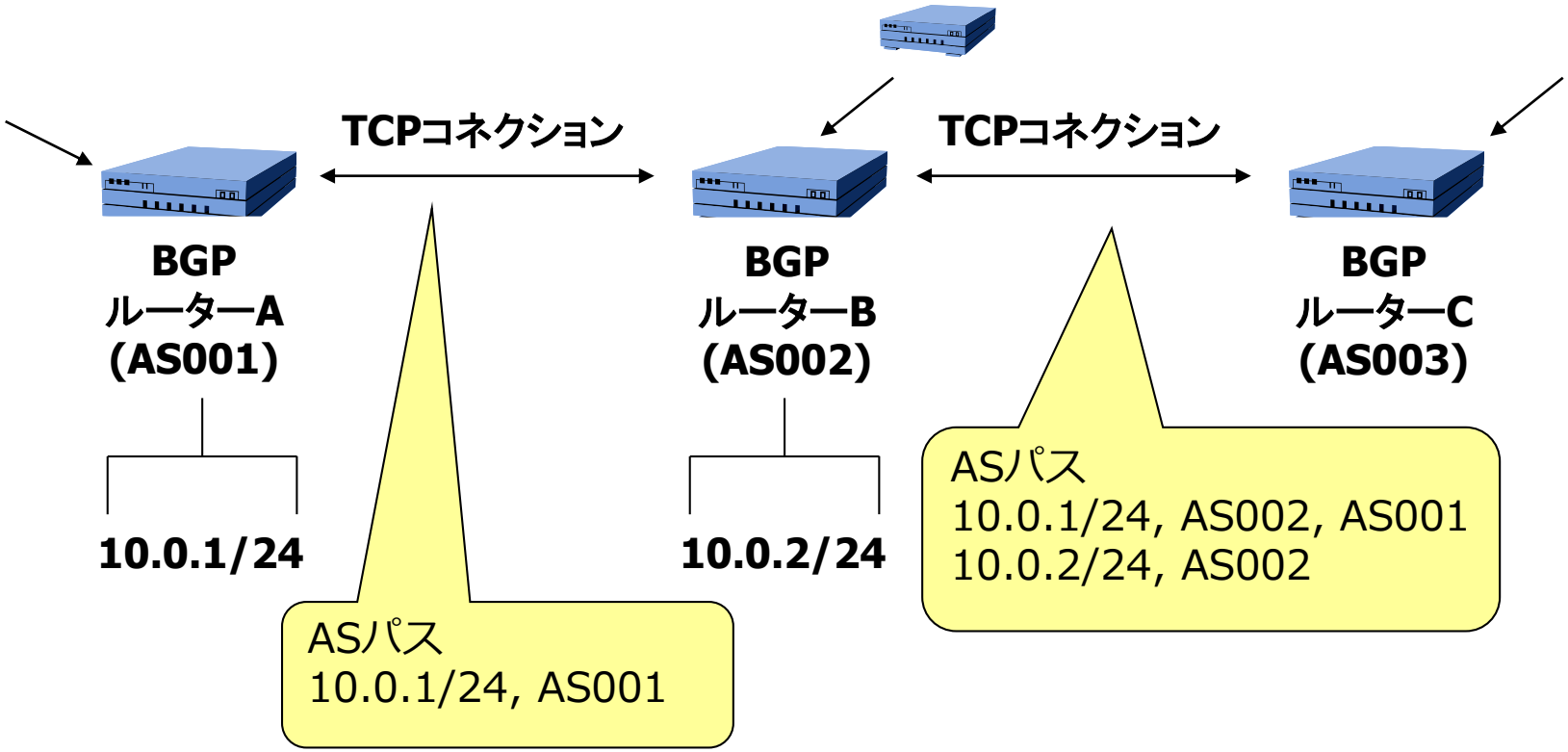


QuaggaSRx Users Manual
https://www-x.antd.nist.gov/bgpsrx/documents/QuaggaSRxUsersManual-4-1-a.pdf

BGPSECとは

- 電子署名の技術を使って不正なBGPメッセージから経路を守る技術

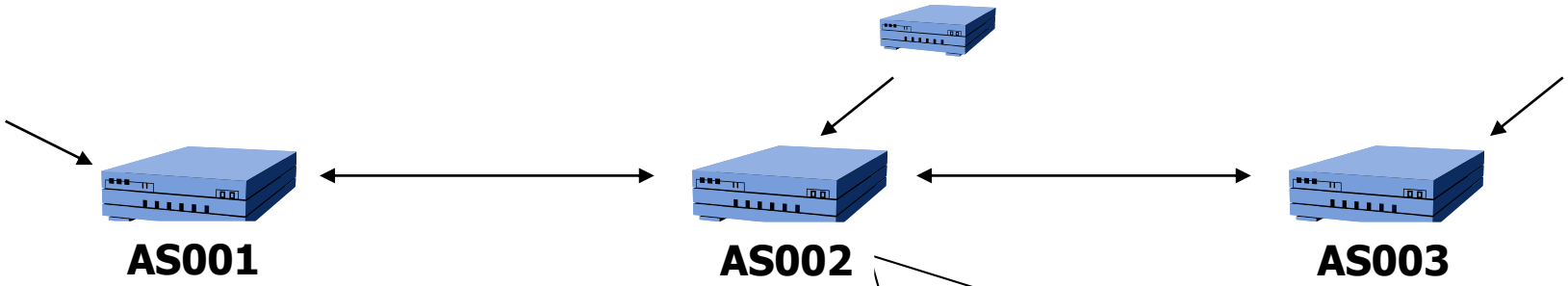
BGPとは（背景）



BGPとは（背景）

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。

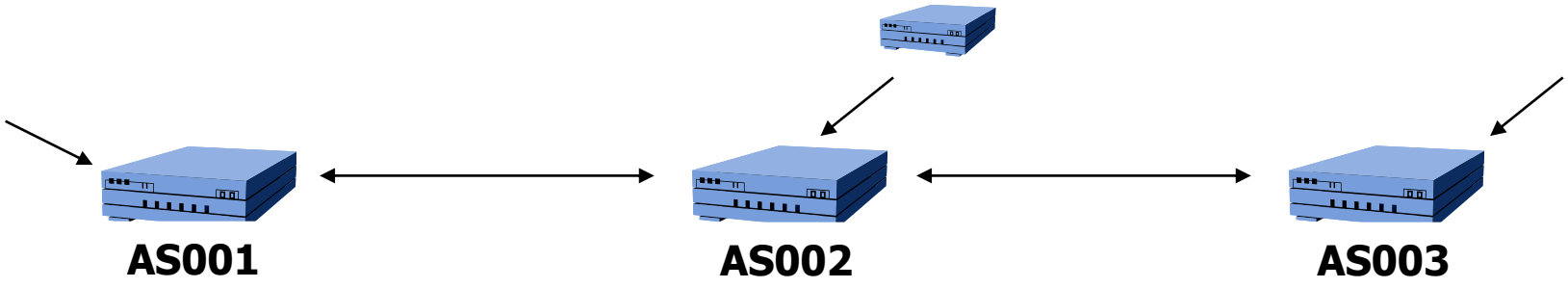
BGPSEC Path Signature



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}

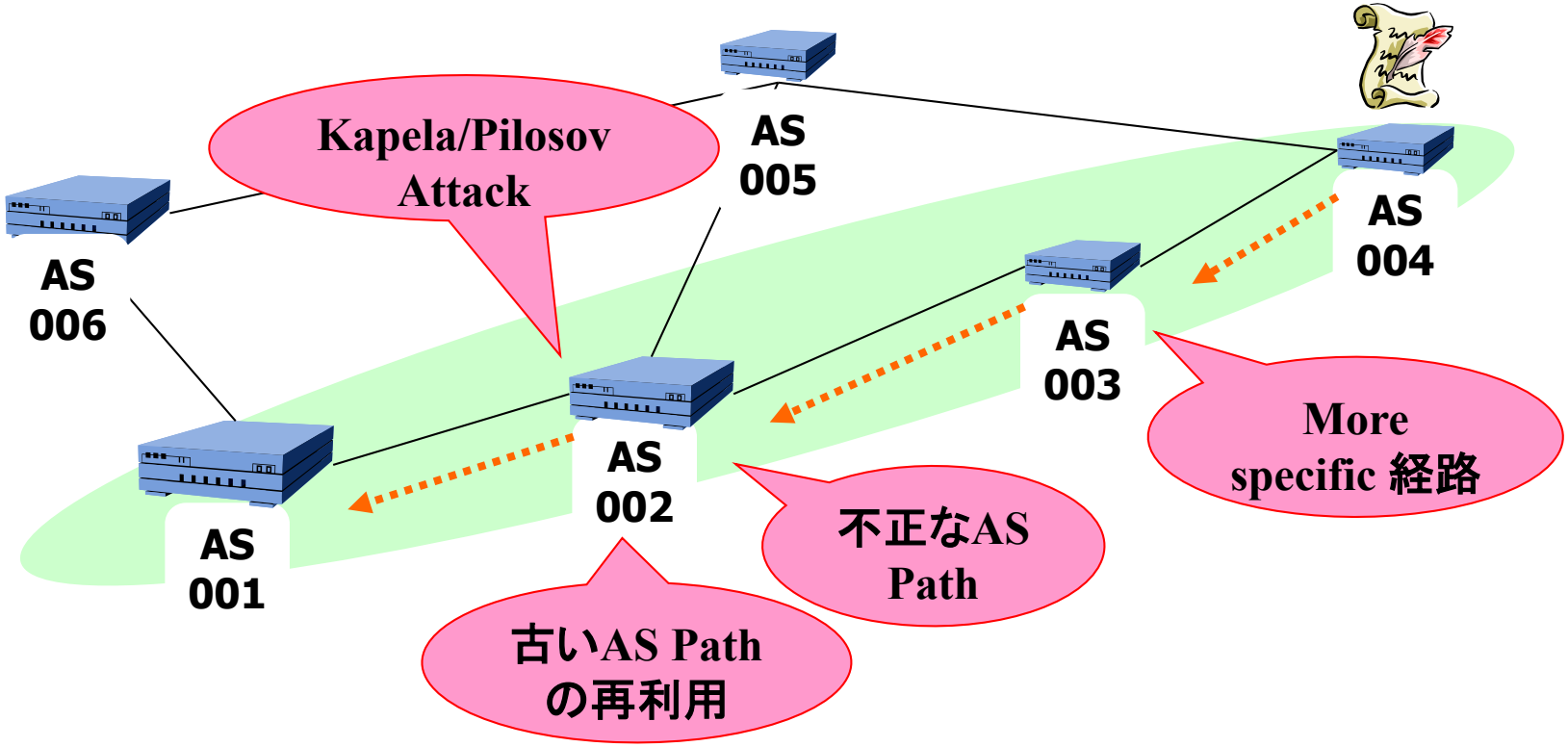
NLRI: Network Layer Reachability Information（ネットワーク層到達性情報）

BGPSEC Path Signature



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}

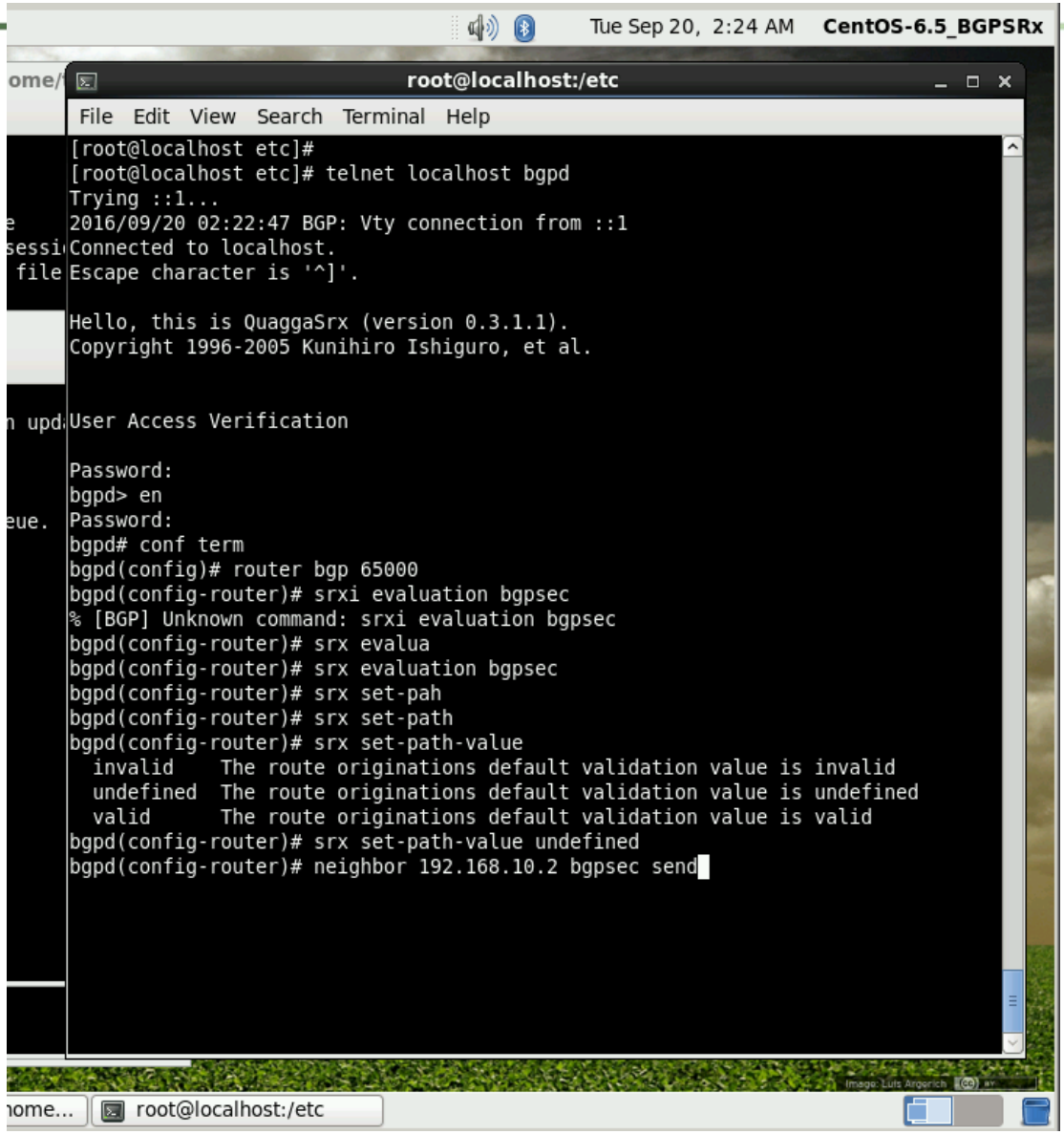
BGPSECの脅威モデル



BGPSECは、電子署名のついたBGP Updateのメッセージを用いて、BGPルーターにおいて脅威とある事象を検出できるようにする仕組みである。
脅威となる事象：(1)不正なAS Path (2)More specific経路 (3)古いAS Pathの再利用
(4)Kapela/Pilosov Attack(故意のUpdateメッセージ操作)

https://www.internetsociety.org/publications/isp-column-june-2011-securing-bgp-bgpsec ほか

動くのか…！？

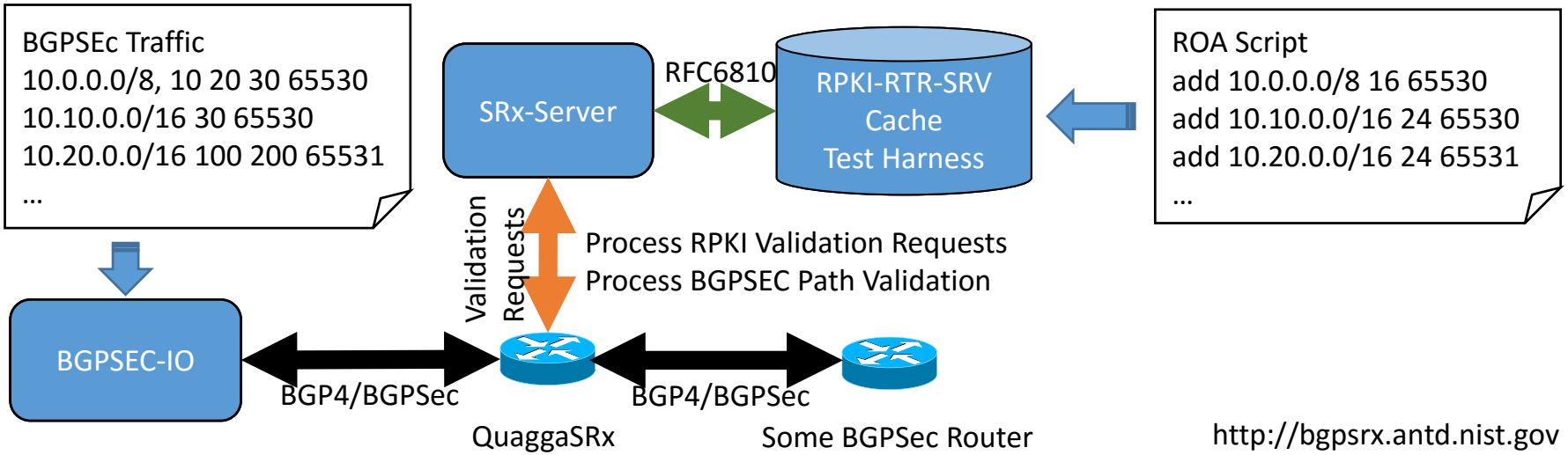


つづく

NISTからのニュース

BGP-SRx 0.4.2 Software Suite

- QuaggaSRx:
  - RPKI / BGPSec Router
- SRx Server:
  - RPKI / BGPSec Validation Server
- BGPSEC-IO:
  - BGPSEC Traffic Generator
- RPKI-RTR-SVR:
  - RPKI Validation Cache Simulator



交流スペース

交流スペース

- BGPの経路フィルター使っている方？
- Prefixフィルター？ / AS Pathフィルター？
- 国内だと Origin Validation より Path Validation の方が業務上は合う？！ (yes/no)

おわり