

RPKIの最新動向のお話 ～トピック～

Internet Routing Security 25, 2016/9/20
木村泰司

覚えていりますか……

```
# 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 history, i injected, > best, i - internal,  
r RIB-failure, S Stale, R Removed
```

```
Validation: v - valid, n - notfound, - invalid, ? - undefined
```

```
SRx Status: I - route ignored, - SRx evaluation deactivated
```

```
SRxVal Format: validation result (origin validation, path validation)
```

```
Origin codes: i - IGP, e - EGP, ? - 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!?

Quagga SRx configuration
SRx Configuration settings
Configure BGPsec path validation.....
SRx Policy Configuration
Display commands
SRx Configuration Display
SRx Related BGP Display
Support.....

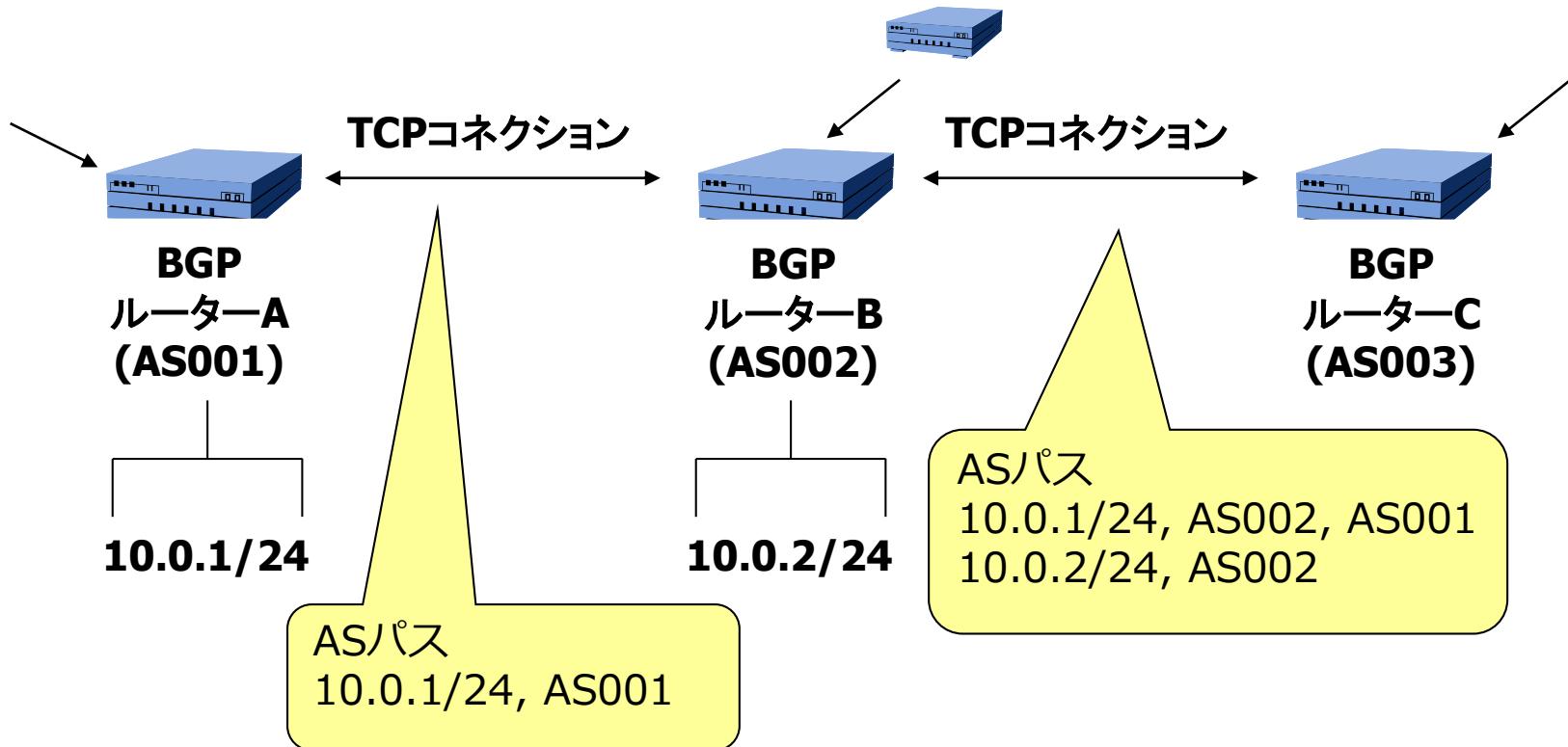
QuaggaSRx Users Manual

<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

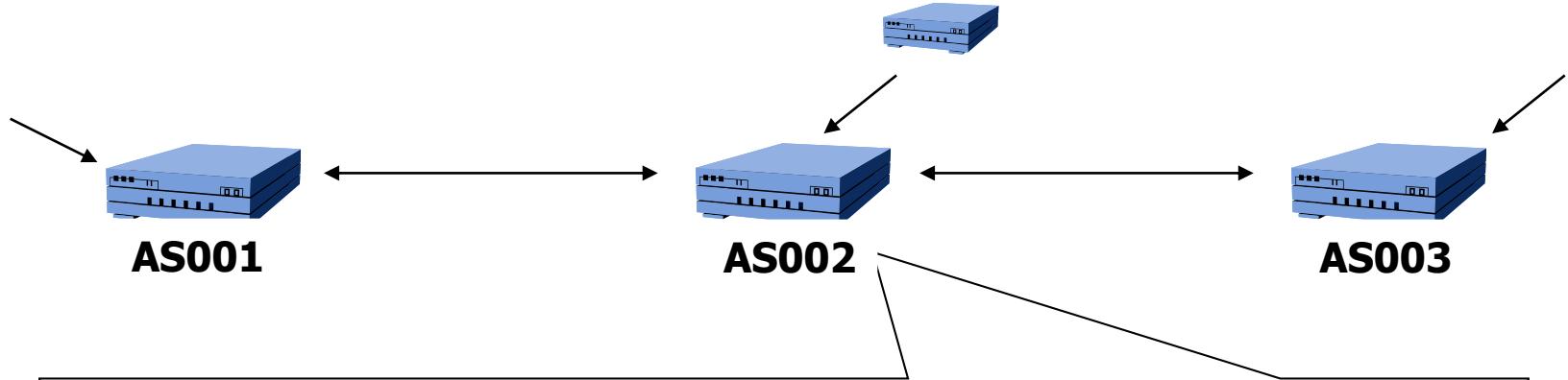
BGPとは（背景）



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。

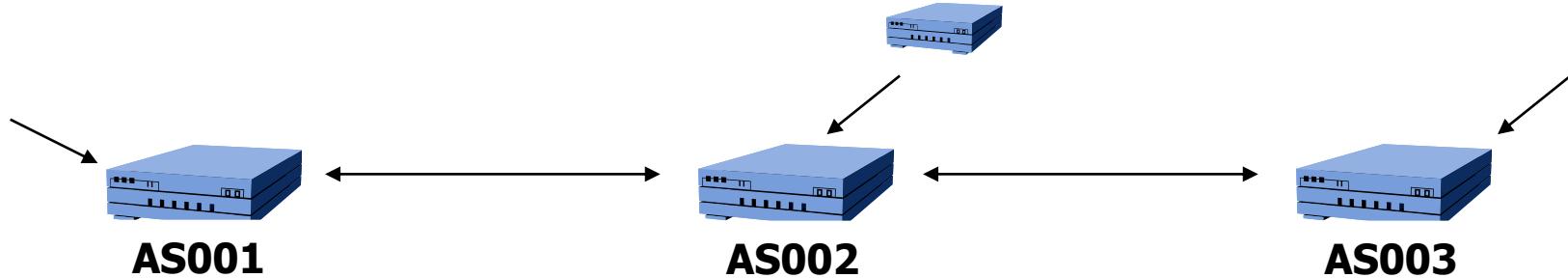
BGPSEC Path Signature



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

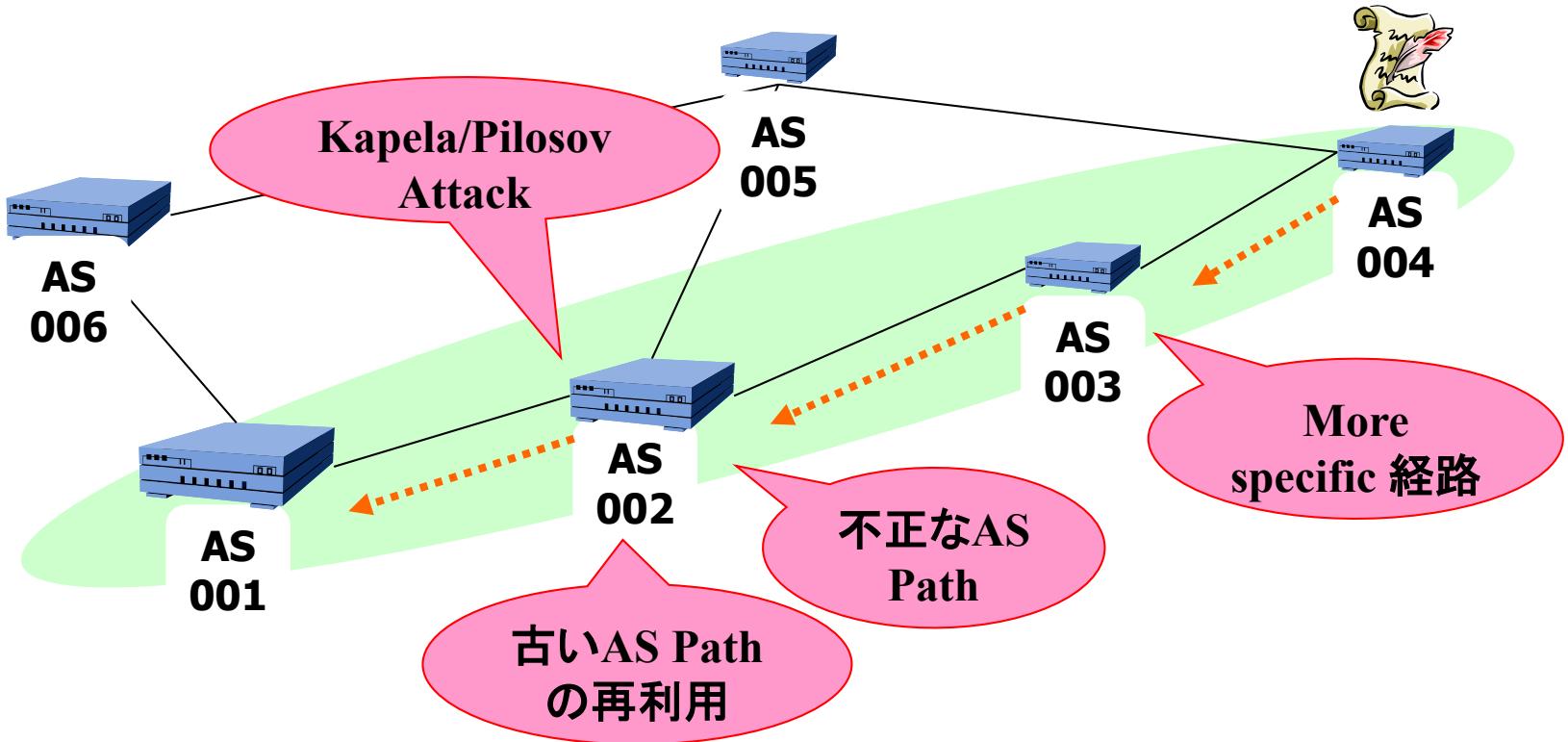
BGPSEC_Path_Signatures

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

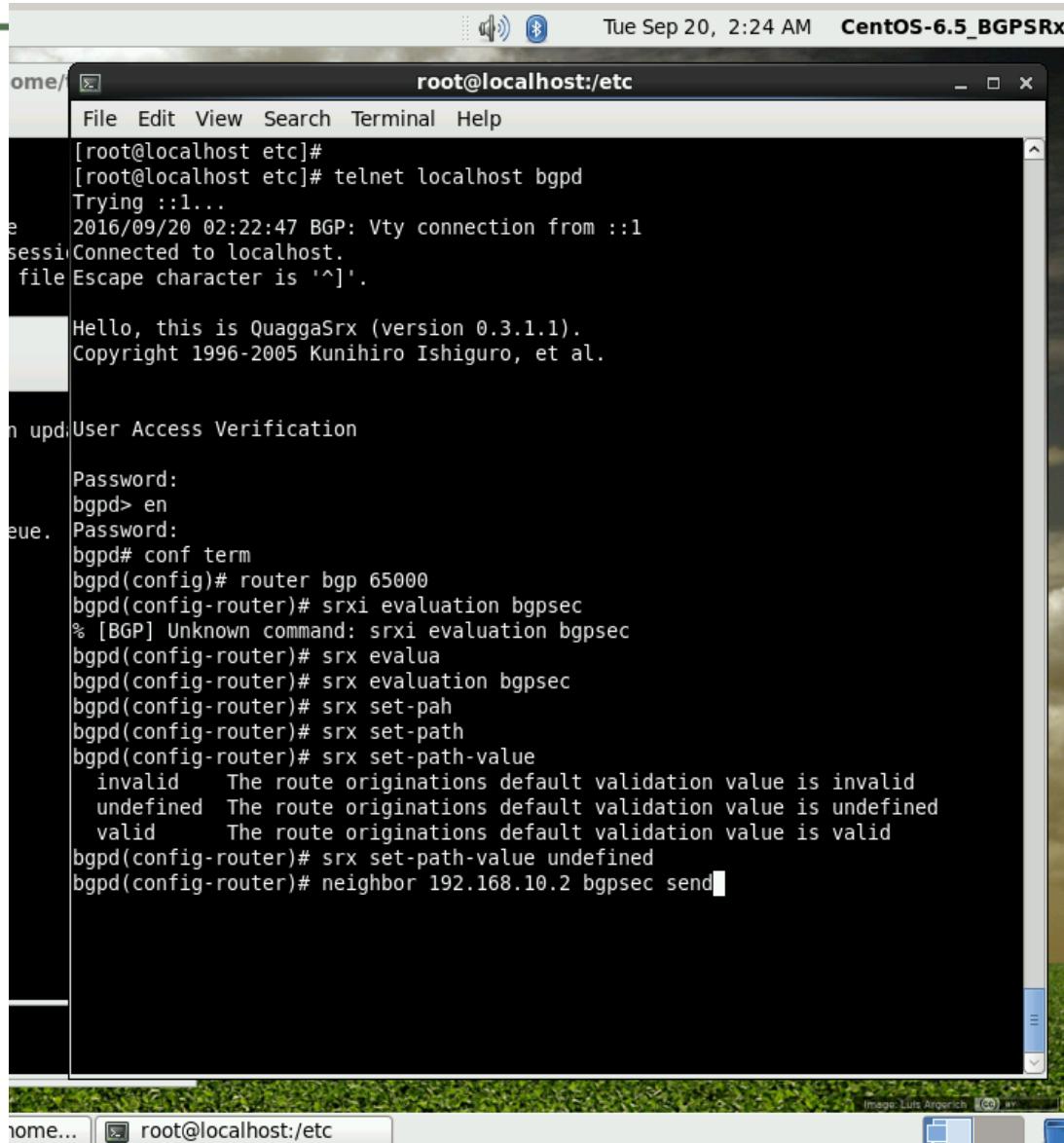


BGPSECは、電子署名のついたBGP Updateのメッセージを用いて、BGPルーターにおいて脅威となる事象を検出できるようにする仕組みである。

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...! ?



The screenshot shows a terminal window titled "root@localhost:/etc" running on a CentOS 6.5 system. The window displays a series of BGP configuration commands and their errors. The session starts with a telnet connection from the local host, followed by the QuaggaSrx version information. It then attempts to enable BGP (bgpd) and set up a configuration router. The configuration process involves several command-line errors related to route originations and path validation, which are highlighted in red in the original image.

```
[root@localhost etc]# telnet localhost bgpd
Trying ::1...
Tue Sep 20 02:22:47 BGP: Vty connection from ::1
Connected to localhost.
Escape character is '^]'.

Hello, this is QuaggaSrx (version 0.3.1.1).
Copyright 1996-2005 Kunihiro Ishiguro, et al.

User Access Verification

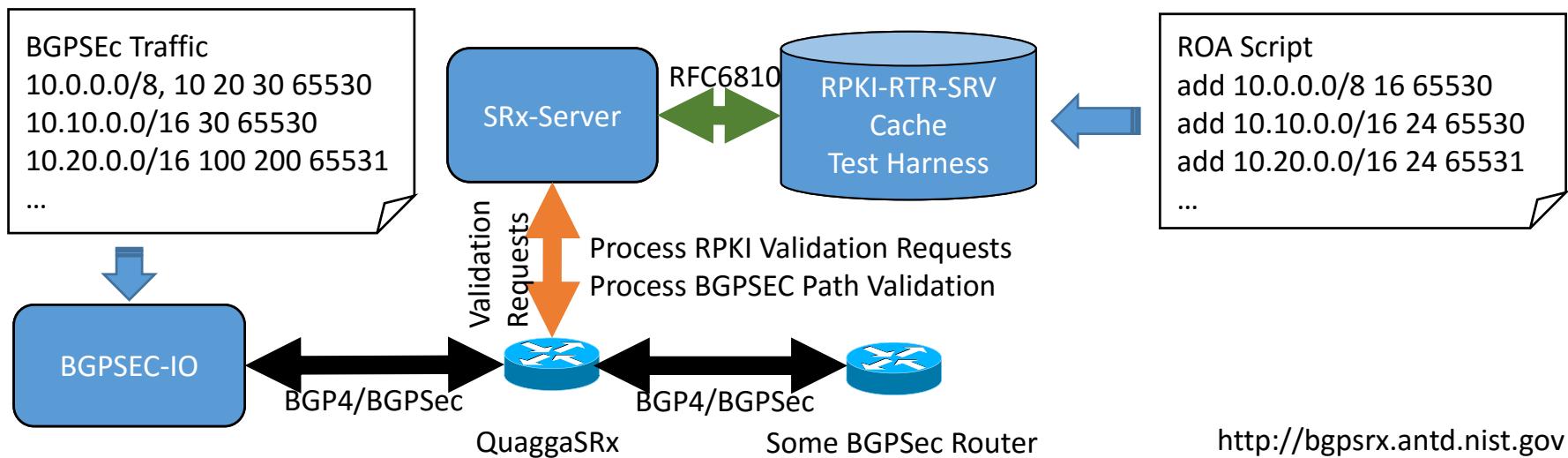
Password:
bgpd> en
Password:
bgpd# conf term
bgpd(config)# router bgp 65000
bgpd(config-router)# srx1 evaluation bgpsec
% [BGP] Unknown command: srx1 evaluation bgpsec
bgpd(config-router)# srx evalua
bgpd(config-router)# srx evaluation bgpsec
bgpd(config-router)# srx set-pah
bgpd(config-router)# srx set-path
bgpd(config-router)# srx set-path-value
    invalid  The route originations default validation value is invalid
    undefined The route originations default validation value is undefined
    valid    The route originations default validation value is valid
bgpd(config-router)# srx set-path-value undefined
bgpd(config-router)# neighbor 192.168.10.2 bgpsec send
```

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