RPKIのROVをいじって考える
野良BoF

2022年7月15日(金) 11:00-12:05

JANOG50

アブストラクト

- JPNICより分配されたIPアドレスに対するRPKIのROAカバー率は、**IPv4 47.1%、IPv6 62%(2022年6月現在)**。BGPルータにおいてROAを使ったBGP経路の検証（Route Origin Validation - ROV）は、AWS、Google、CloudFlare他、国際的な通信事業者で導入されていますが、国内ではあまり進んでいません。
- ROVを導入すれば自社のBGPルータで不正な経路が検知できるようになるはずです。**しかし実際はどのような設定によって、どのように判定し、ルータではどのように扱うことができるのでしょうか。**このBoFでは実際に不正な経路を流してみてROVを行い、そのBGPルータの挙動をみていきます。設定を色々といじってどうなるかをみながら考えます。**あなたと共に。**

野良BoFの内容

1. **ROVで経路をCHANGE －10分くらいで魅せるROVの効果, hiromu shiozawa**

   ⇒　ROVをご覧いただきます。

2. **1にまつわるエトセトラ, Taiji Kimura**

   ⇒　ハンズオン そのー。ssh クライアントを使ってJPNICのハンズオン環境にログインし、ROVの設定とROVの結果となる経路表を見てみましょう。ROVにまつわる「かんがえる」テーマの下地となるお話です。

3. **経路探訪 －珠玉のROV－, Hiroyuki Ashida**

   ⇒　逸般の誤家庭にあるルータを使ってROAキャッシュサーバに接続してみましょう。インターネットにはどのような経路が流れているのか探訪していきます。

4. **いじるじかん　かんがえるじかん**

   ⇒　いくつかのテーマで。

ROVを体験!?

ハンズオン - ルータでroute-mapを確認

■設定を確認します。
vyos@router$ show conf com

■設定モードに変更します。
vyos@router$ conf
[edit]
vyos@router#

(以下は設定のコマンド)
vyos@router# set protocols bgp 65▼ neighbor 172.16.100.100 address-family ipv4-unicast route-map import ROUTES-IN
vyos@router# set protocols bgp 65▼ neighbor 172.16.100.200 address-family ipv4-unicast route-map import ROUTES-IN

※▼はrouterの番号です (ex) vyos@router101 → 65101

ハンズオン - ルータでRTRを設定

```
vyos@router# set protocols rpki cache k1-host3 address 192.168.10.3
vyos@router# set protocols rpki cache k1-host3 port 323
vyos@router# commit
vyos@router# save
```

ハンズオン - 偽の経路はどうなるのか

- **ルータでInvalidの経路が見えなくなる事を確認します。**

■routerで実行
router# run show rpki cache-connection
(RPKIキャッシュサーバに接続していれば情報が表示されます)
router# run show rpki prefix-table
(ROAを使って有効なprefixの一覧が表示されます)
router# run show ip bgp
(LocPrfの値を確認します)

ハンズオン - 正しいDNS応答

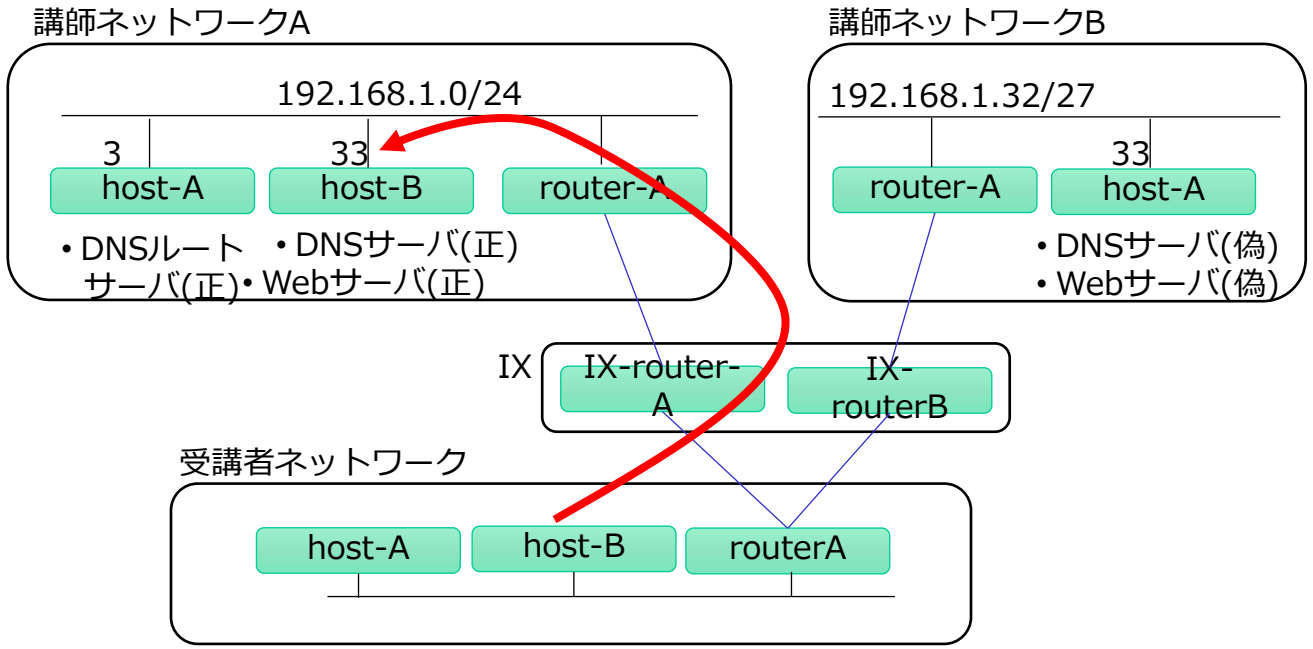
◇正しいサイト？　答え→ ✓

(curlでアクセスしてみます)

```
host$ curl https://www.handson.test/
:
```

★アドバンス★　(怪しい経路は？)

```
router$ show ip bgp neighbors 172.16.100.200 received-routes
```



エトセトラ

ROVについて考えるための話題1/4 – リスタート

リスタートするとルーティングできるようになるまで、やっぱり時間かかります？
→ **お試しをば。。**

↓

(野良BoF当日の様子)

今回の環境（ただし80万に近い経路数）では通常のBGP機能のリスタートと大きく変わらなかった。

ROVについて考えるための話題2/4 - トポロジー

ROVやっても意味がないことがある。
→ **どこでROVするといいのか**

↓

(野良BoF当日の様子)

まずは自ASでの観測は必要そう。その上でCDNやDNSなど利用されるサービスを踏まえてトポロジーをみていく必要も。ROVが行われるといい場所は必ずしも自ASではない可能性あり。

ROVについて考えるための話題3/4 - キャッシュサーバの場所

キャッシュサーバへの経路が不正経路の影響を受けてしまうことがあります(笑)
→ **やっぱり手元が安心？**

↓

(野良BoF当日の様子)

セットアップ自体は Docker 利用など簡単化が可能。(冗長構成や監視を踏まえると実験運用が必要か。)

ROVについて考えるための話題4/4 - Invalid経路の考え方

drop するとご覧の通りきれいに動きます。
→ **中身を見ないで drop してOK？**

↓

(野良BoF当日の様子)

段階的な対応が可能。
(a) Invalid経路をみるだけ
(b) Loc-Pref を下げる(ベストパスになる可能性を残す) (c) community の値をセット(周辺情報などからdrop) (d) Invalid経路をすべてdrop
これらをサービスに応じて。

議論メモ

- **Validation (会場より)**
  - やっている方（自前で用意）
    - Upsteam, peer の inbound に。transitはまだ。
  - 導入判断
    - Best pathの優先度を下げるなどからか。
    - Invalid な経路がどれくらいあるのかを観測したい。
  - ためす
    - まずはラボなどで試すのがいいのではないか。
    - コンテナなど実際に動かすのは大事。

おわり