

RPKIやってみませんか？

インフラストラクチャ本部 データセンターチーム マネージャー 黒河内 倫



自己紹介



氏名

黒河内 倫（くろこうち おさむ）

所属

グリー株式会社 インフラストラクチャ本部
データセンターチーム マネージャー

プロフィール

2002年 イッツ・コミュニケーションズ株式会社
2006年 楽天株式会社 ネットワーク構築・運用チーム
2011年 グリー株式会社 データセンターチーム

従業員数

1,867人（グループ全体・2014年09月末時点）

事業内容

ソーシャルゲーム事業

ソーシャルメディア事業

プラットフォーム事業

広告・アドネットワーク事業

ライセンス&マーチャンダイジング事業

ベンチャーキャピタル事業

1. グリーとしてのRPKIへのモチベーション

2. モックアップ環境での検証

3. Production環境適用にむけて

4. 課題と感じたところ

5. まとめ

1. グリーのRPKIへの モチベーション

Securityというよりは障害検知が目的

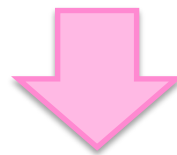


弊社は事業上、日本の携帯キャリアへの通信が多い

携帯キャリアだけのPrefix/IPアドレス数だけであれば少ないものの、
NATを利用しているため、1Prefixあたりのユーザ数が多い

そのため1Prefixでも障害が発生した場合、その影響範囲は大きい

もし、Mis-Originationされた経路がBGPで広報されても
何かしらの形で対応できる手段が欲しい



RPKIに期待



守れるもの

他ASのPrefixがMis-Originationされた際の対応が可能

具体的にはROAサーバの情報とBGPで受診した経路を比較し
その結果を用いて、attributeを書き換えることができる

守れないもの

自ASのPrefixがMis-Originationされた際

→ BGPMON/経路奉行などで対応可能

ASごとMis-Originationされた際

→ 後ほど岡田さんより詳細な説明あり



2. モックアップ環境での検証

まずはモックアップ検証



ROAサーバ

JPNIC様のROAキャッシュサーバを利用
更に弊社(AS55394)のPrefixをROAサーバに登録

ネットワーク検証環境

以下のソフトウェアを用意して検証を行った

VMware ESXi5.1

CISCO CSR1000v

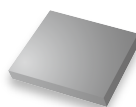
Juniper FireFly

※いずれもMakerのSiteからDownload可能



検証構成

192.41.192.218
(JPNIC様 ROAキャッシュサーバ)



インターネット

グローバルIPにNAT



```
route-map origin-validation permit 10  
match rpki invalid  
set local-preference 90
```

```
route-map origin-validation permit 20  
match rpki not-found  
set local-preference 100
```

```
route-map origin-validation permit 30  
match rpki valid  
set local-preference 110
```

検証環境Gateway

192.168.1.0/24

RPKIプロトコル

ESXiサーバ

Origin
Validation

ダミー経路送信

10.0.0.0/8

116.93.144.0/20

CSR1000v

OS : IOS-XE 3.10.03.S
IPアドレス : 192.168.1.48/24
AS番号 : 65000

↔
BGP Peer

Firefly

OS : JUNOS 12.1X46-D10
IPアドレス : 192.168.1.49/24
AS番号 : 65001

イレギュラーパターンで問題は発生したものの ROAサーバへの接続、OriginValidation自体は問題なく動作した

```
csr1000v#show ip bgp rpki table | inc 116.93.144.0  
116.93.144.0/20    24    55394    0    192.41.192.218/323
```

JPNIC様のROAサーバから受信されている

```
csr1000v#show ip bgp  
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,  
               r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,  
               x best-external, a additional-path, c RIB-compressed,  
Origin codes: i - IGP, e - EGP, ? - incomplete  
RPKI validation codes: V valid, I invalid, N Not found
```

	Network	Next Hop	Metric	LocPrf	Weight	Path
I*>	116.93.144.0/20	192.168.1.49	90	0	65001	i
N*>	10.0.0.0/8	192.168.1.49	100	0	65001	i

116.93.144.0

ROAサーバ上はAS55394-Originだが受信経路は65001-Originのため**"Invalid"** → LP90

10.0.0.0

ROAサーバに登録がないため**"Not Found"** → LP100



3. Production環境適用に向けて

構成概要

ASR9000を利用する予定

Route ReflectorでOriginValidationを行う

※全BGP-RouterがRPKI対応していないため

設計ポリシー

Local Preferenceで制御予定

invalidの場合 : Local Preference"-50"

not-foundの場合 : Pass

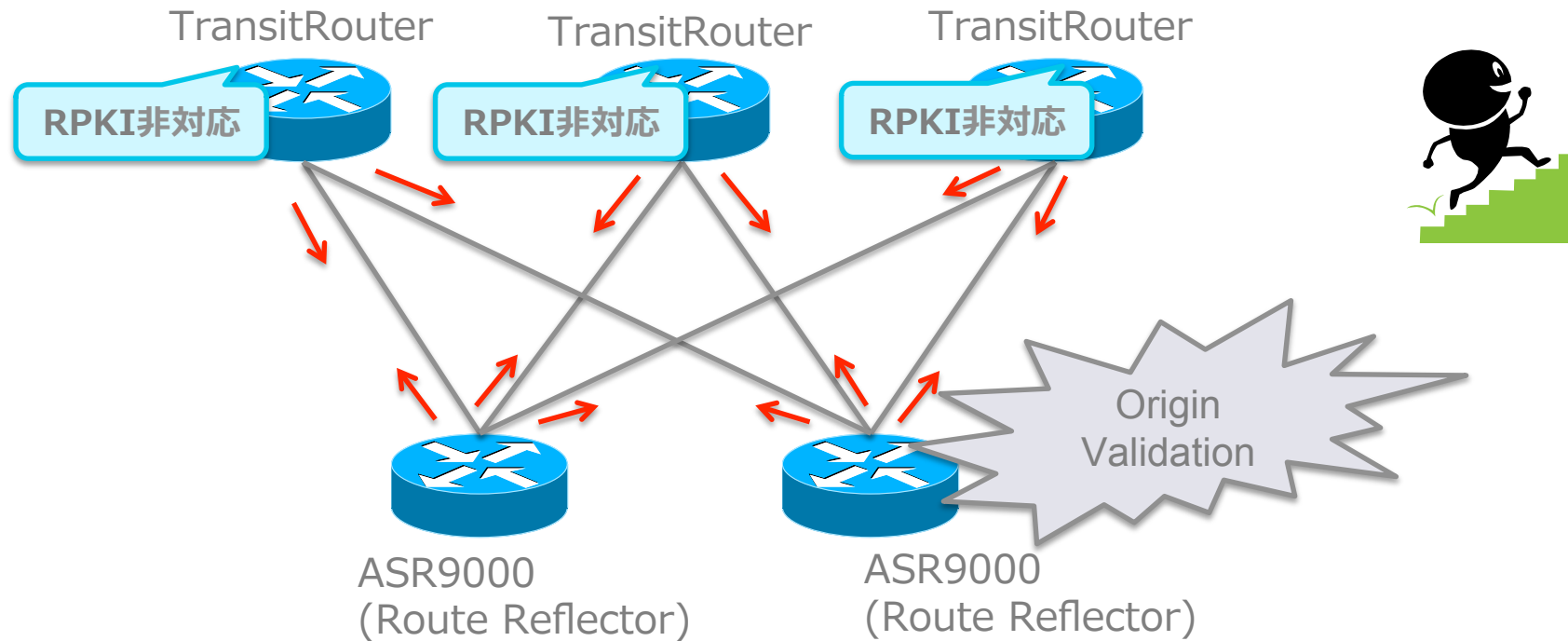
validの場合 : Local Preferenceを"+50"

ROAサーバ

未定(考え中)



ASR9000でのRoute Reflector構成を検討



Route ReflectorでValidationを行い、それをClientに返せるか！？



そもそもValidationできませんでした

RPKIはiBGPには対応をしていない

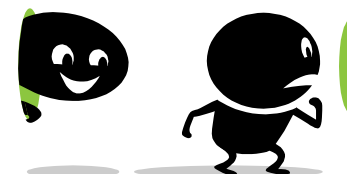


RFCも(明言はされていないが)、
基本的にはExternalの接続を想定されている

そのためeBGPのみに適用される

外部接続部分のRouterでValidationを行う前提に
標準化もRouterOSも実装もされている

**この様にAS内の一箇所で集中的に
Validationする設計はできない**



4.課題と感じたところ

環境の都合上、Cisco様の機器をベースに情報を記載をさせていただきます

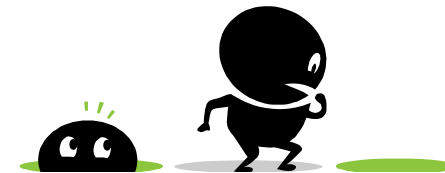
ROAサーバ側の課題(その1)



IPv4/IPv6の指定が出来ない

IPv4とIPv6の指定ができない(不具合がある訳ではない)

IPv4だけのネットワークでも、ROAサーバにIPv6の情報があれば、
IPv4/IPv6すべての情報がSyncされてしまう



ROAサーバ側の課題(その2)



Maxlenが活かされていない

RPKIにはMaxlenという(MaxPrefixLength)という項目があるが、
このようなテーブルを発見した

Network	Maxlen	Origin-AS	Source	Neighbor
2.0.0.0/16	16	3215	0	210.173.170.254/323
2.0.0.0/12	16	3215	0	210.173.170.254/323
2.1.0.0/16	16	3215	0	210.173.170.254/323
2.2.0.0/16	16	3215	0	210.173.170.254/323
2.3.0.0/16	16	3215	0	210.173.170.254/323
2.4.0.0/16	16	3215	0	210.173.170.254/323
2.5.0.0/16	16	3215	0	210.173.170.254/323
2.6.0.0/16	16	3215	0	210.173.170.254/323
2.8.0.0/16	16	3215	0	210.173.170.254/323
2.9.0.0/16	16	3215	0	210.173.170.254/323
2.10.0.0/16	16	3215	0	210.173.170.254/323
2.11.0.0/16	16	3215	0	210.173.170.254/323
2.12.0.0/16	16	3215	0	210.173.170.254/323
2.13.0.0/16	16	3215	0	210.173.170.254/323
2.14.0.0/16	16	3215	0	210.173.170.254/323

こちらの詳細は、後ほど岡田さんより別途ご説明



ネットワーク機器の課題(その1)

OriginValidation時の挙動

OriginValidationはRoute[map/Policy]で定義を行う

そのため動作としては、基本的に
Ext]

communityの添付

Local Preferenceの添付

など**attribute**を変更することしか出来ない

Invalid = “Mis-Origination”されているという状況であるため、
ここはalert(snmp/syslog)をあげる仕組みが欲しい



ネットワーク機器の課題(その2)



Reboot時の挙動



機器にRebootなどが発生すると、
起動後のRoute(map/Policy)がすべてNotFoundの扱いとなってしまう
原因は起動時の動作が以下の通りとなるからである

1. RouterのOS起動
- ↓
2. BGP-Neighborが張られる
- ↓
3. ただしこの時点ではROAサーバとのPeerが貼れていない
そのためROA情報がないため、Route[map/Policy]が
全部Not-found扱いでFIBが作成される
- ↓
4. その後RPKIサーバに問い合わせる、
しかしFIBは完成しているため、FIB情報は上書きされない

エビデンス : `clear ip bgp (soft)`でFIBに書きかわる

対処方法 : 設定で回避可能であるか確認中(eemであれば対応可能)

ネットワーク機器の課題(その3)



情報が少ない

弊社の環境上、Cisco機器(ASR9000/CSR1000v)での実装だった

特にASR9000(IOS-XR)については非常に苦労した

今回、Production環境の実装に向けては、
Cisco様に多大なご協力を頂いたが、Cisco様の中でも情報が少なかった

**RPKIは2年以上前に実装されているにも関わらず、
現状利用Userが殆どいないことがわかった**



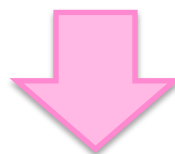
ROAキャッシュサーバの課題



配置方法PublicなROAサーバはインターネットのどこに配置すべきか？

EndUser

Validationされた経路がほしいユーザもいれば
自社でValidationしたいユーザもいる



Transit

ValidationしたPrefixを提供するサービス
ROAサーバを提供して、提供ユーザ側でValidationしてもらうサービス

IX(Internet Exchange)

Route ServerでValidationを行い、Prefixを提供するサービス
ROAサーバを提供して、提供ユーザ側でValidationしてもらうサービス



ユーザとしては2つの提供パターンが欲しいがTransit/IXには負担がかかる

5.まとめ

現状のRPKIを取り巻く状況



ROAキャッシュサーバ

RIRの足並みが揃っていないと感じる

+ 国際移転アドレスがAPNICのROAサーバに登録できなかった

+ 登録方法がRIRごとによってまちまちに見えた

ここはうまく連携をしてほしい

RPKI自体の信頼性が無くなるようなことには、なって欲しくない



Routerの実装

RPKIに対応しているMakerも少ない

またMakerでも情報や導入実績が少ない

実装面でも強化が必要



まだまだこれからのプロトコル

今後のRPKI



本当の最終ゴールは**"BGPSEC"**としたい

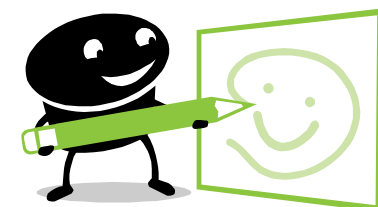
BGPSEC="Origin Validation"+"Path Validation"

ただ**"Origin Validation"**できなければ、
"BGPSEC"は実現できないと考える

幸い、RPKIは検証は簡単にできる



まずは一緒にRPKIを使い倒してみませんか？



あるべき姿

1. インターネット上でのマスク長勝負がなくなる
※吸い込まれたら吸い込み返す世界はNo!!!
2. Secureでないネットワークが
インターネットに繋がっても、他の事業者に影響しない
3. 間違ったPrefixが広報されても、Routingされない

まだこの辺り

まず最初の一歩を踏み出そう！



参考資料



RPKI

<https://www.nic.ad.jp/ja/rpki/>

BGPSEC

https://www.ipa.go.jp/security/fy23/reports/tech1-tg/b_07.html

JANOG

<http://www.janog.gr.jp/meeting/janog30/program/rpk.html>

<http://www.janog.gr.jp/meeting/janog31/program/rpki.html>

<http://www.janog.gr.jp/meeting/janog32/program/rpki.html>

Nanog

<https://www.nanog.org/meetings/nanog52/presentations/Sunday/110612.nanog-origin-validation.pdf>

<https://www.nanog.org/meetings/nanog49/presentations/Tuesday/bgp-origin-validation-FINAL.pdf>



