RPKIのROVを試してみた件

JANOG52@長崎

2023年7月5日(水)

木村泰司

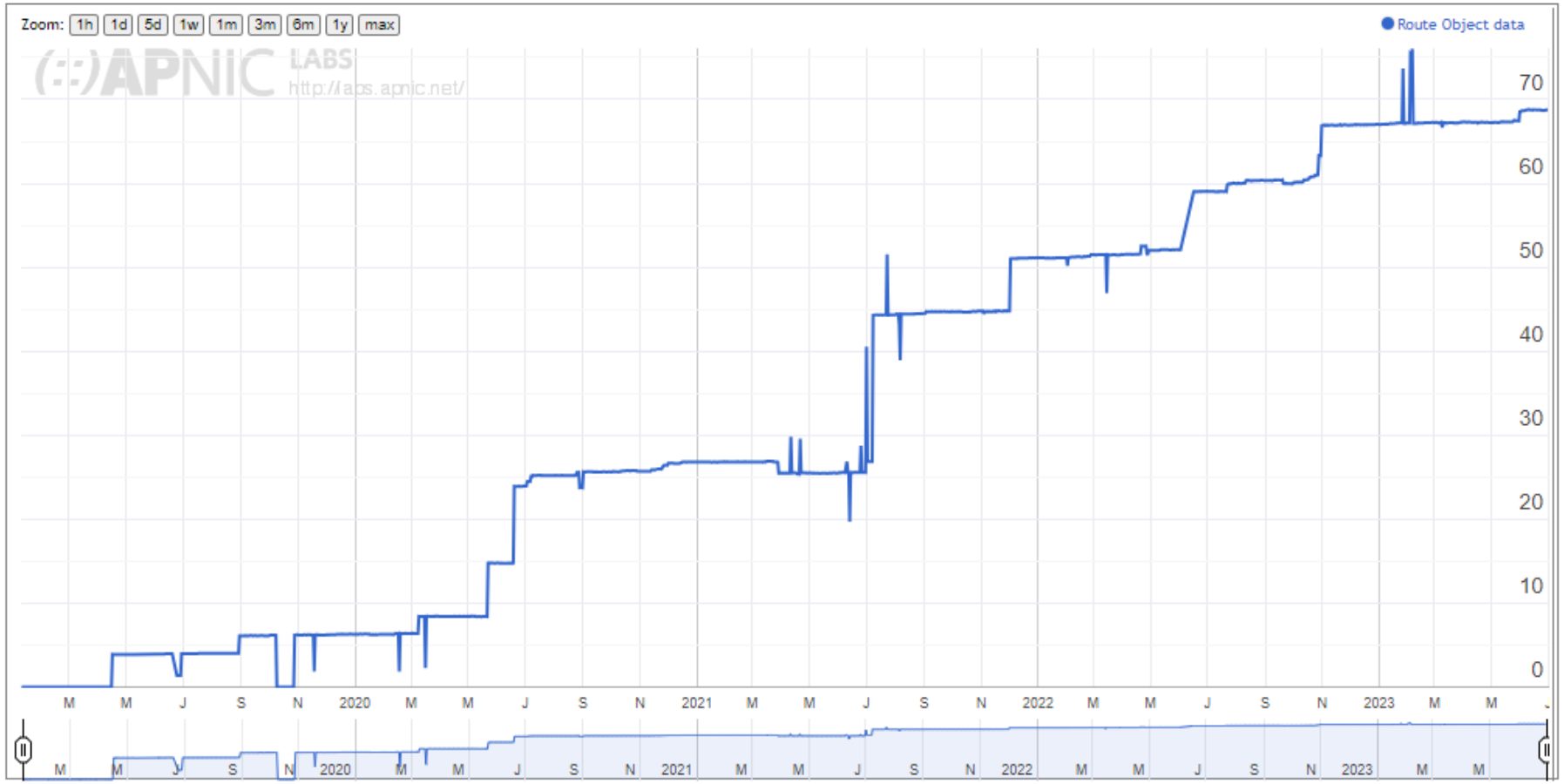
一般社団法人 日本ネットワークインフォメーションセンター

IPv4　71.8%
IPv6　71.3%

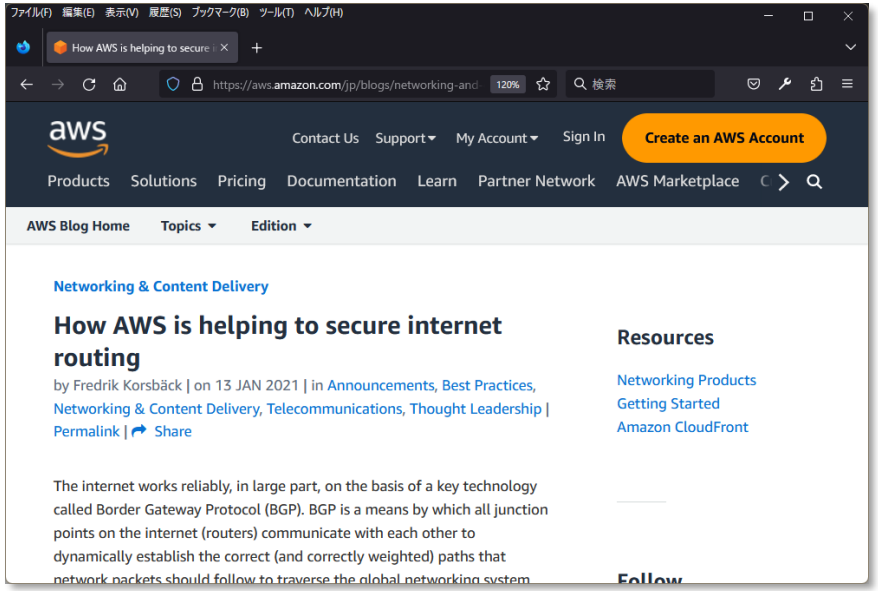
JPNIC管理のIPアドレスに対するROAによるカバー率
IPv4はアドレス数、IPv6は/48の数で算出

Use of Route Object Validation for Japan (JP)

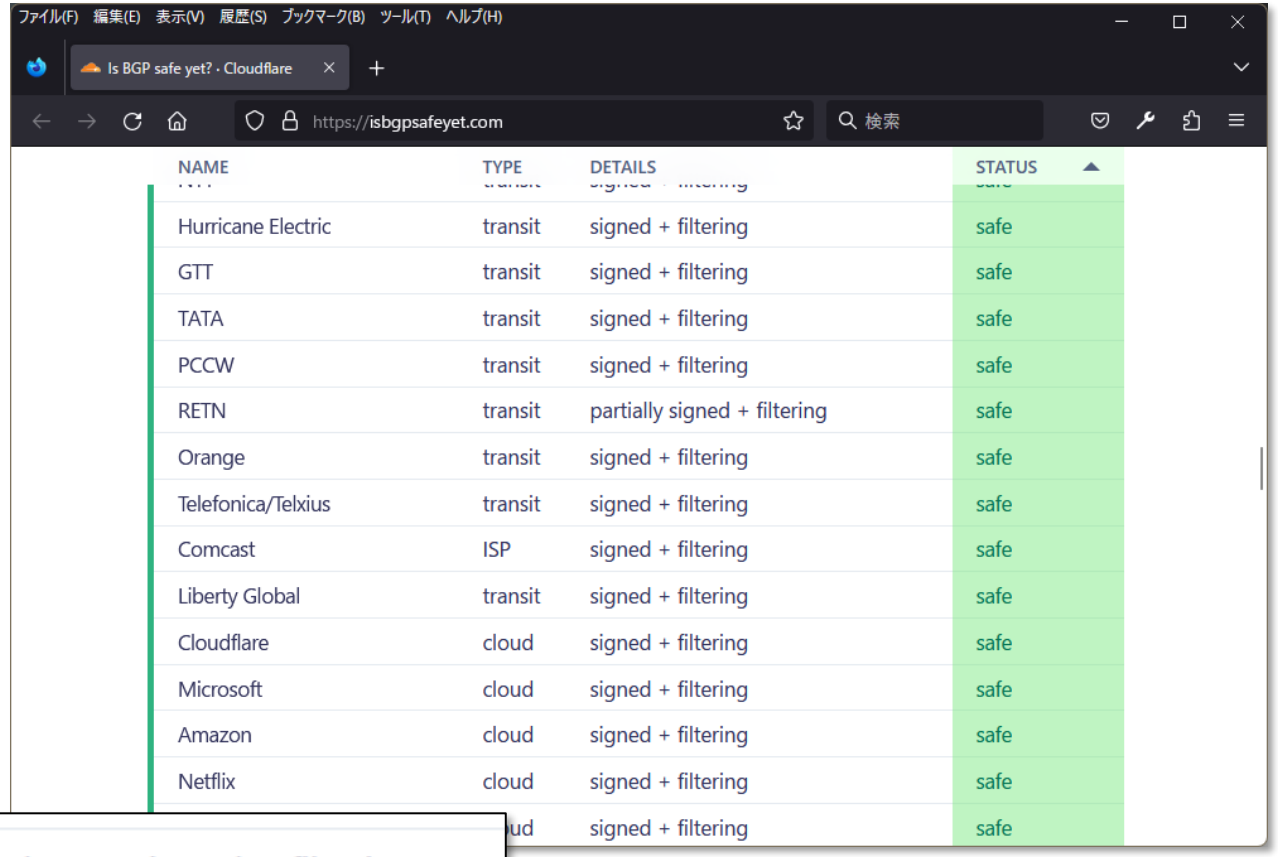
Display: **Addresses** (Advertised ROA-Valid Advertised Addresses), **IPv4**, **Percent** (of Total)



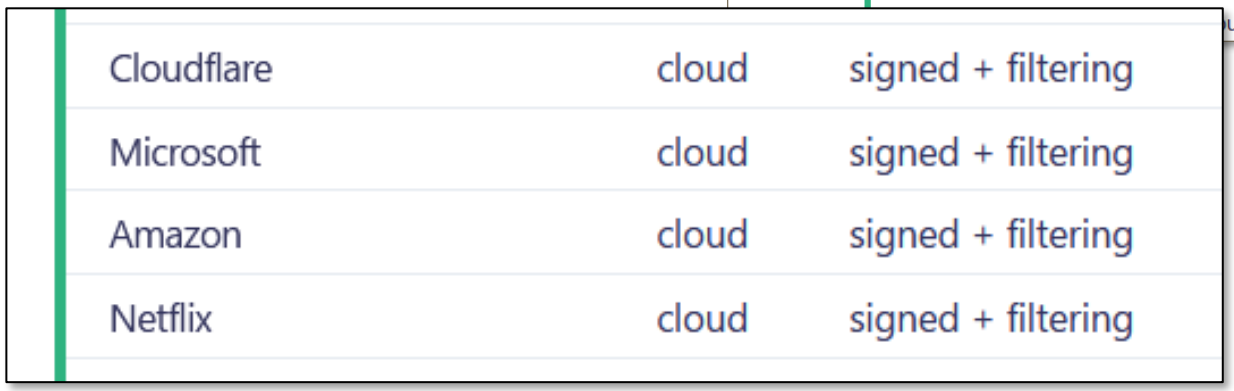
Use of Route Object Validation for Japan (JP), APNIC Labs, https://stats.labs.apnic.net/roa/JP
経路広告されているアドレスのうちROAによってカバーされているIPv4アドレス", 2023/6/30時点



How AWS is helping to secure internet routing
by Fredrik Korsbäck | on 13 JAN 2021
https://aws.amazon.com/jp/blogs/networking-and-content-delivery/how-aws-is-helping-to-secure-internet-routing/



Is BGP safe yet? · Cloudflare
https://isbgpsafeyet.com/



ロシアISPによる Twitter経路ハイジャックの影響調査, 當間 拓矢, JANOG 51 LT, NTT コミュニケーションズ
https://www.janog.gr.jp/meeting/janog51/wp-content/uploads/2023/01/janog51-lt-toma-1.pdf

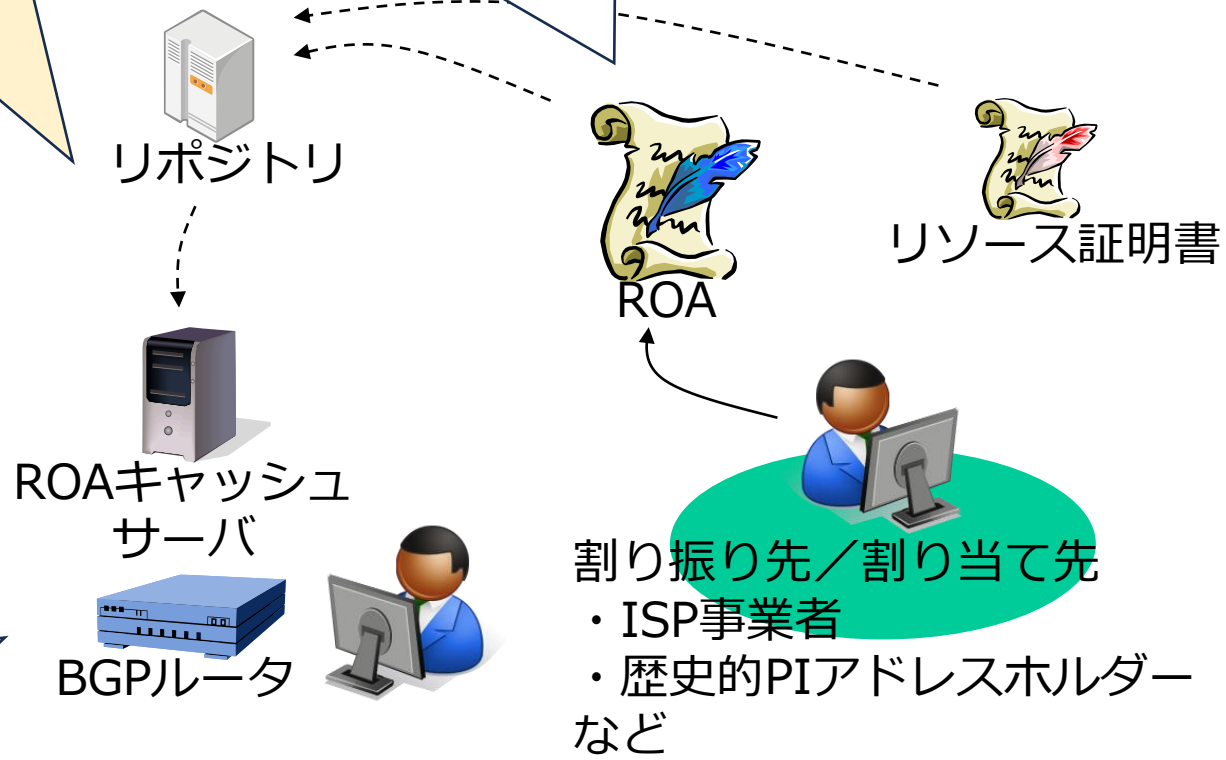
よさそう。
でも…。

ROVを導入しても
問題ない？

ROVを導入すれば
本当に不正な経路
から守られる？

導入後に問題が
あったときに対処
できる？

ROAはBGP経路と合わせておけば大丈夫そう。



総務省　ISP におけるネットワークセキュリティ技術の導入及び普及促進に関する調査

RPKIを応用したルーティングセキュリティ技術（ROVやASPA）は、技術的に導入によって効果が得られそうな技術である。しかし導入する事業者の観点では”敷居”に感じられることがある。

⇒ 実証実験
- ○ 導入検証コース / 実験コース / 体験コース
- ○「三つの確証」

⇒ 技術面/運用面で解明していないことについて調査研究
- ○慶応義塾/WIDEプロジェクト
- ○大阪大学
- ○長崎県立大学

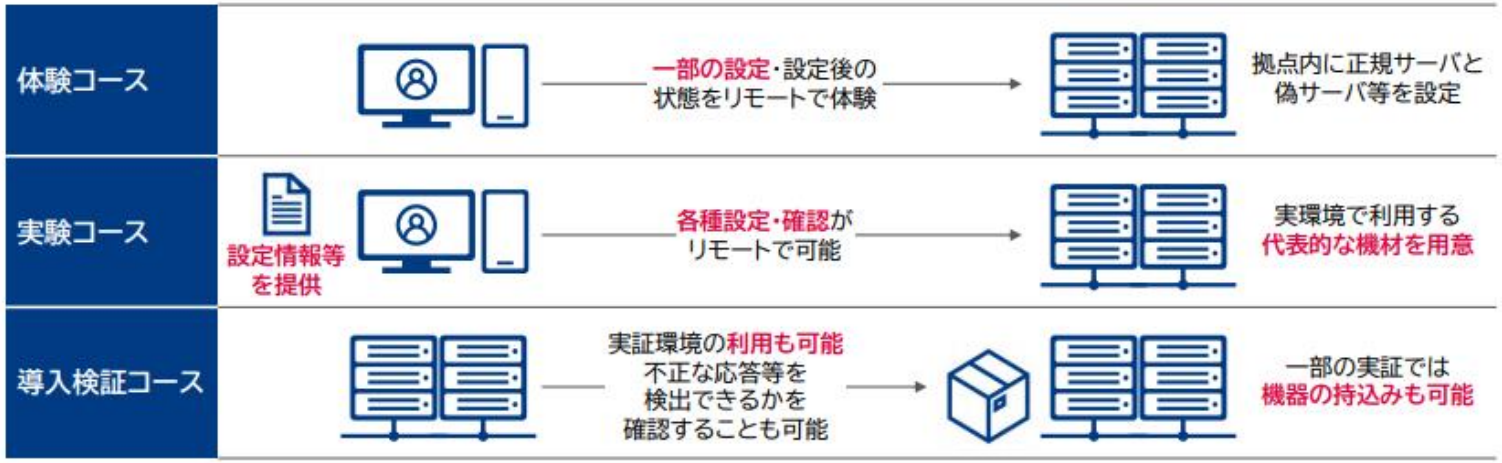
ISPにおけるネットワークセキュリティ技術の導入に関する調査, MRI, 総務省サイバーセキュリティタスクフォース（第43回）資料43－1－1,https://www.soumu.go.jp/main_content/000878673.pdf

MRI

①RPKI ②DNSSEC ③DMARC

4.1.1. 技術的課題の調査（実証環境の整備）

- 各実証コースの利用を想定し、実証環境を整備した。
- RPKIの仮想環境では、ネットワーク通信機材の持込みによる検証を想定し、3大学の協力の基、慶応大学（SFC：神奈川）、大阪大学、長崎県立大学に設置。また、検証用及び実態を体験するためフルルートを流す環境を用意。
- DNSSECの仮想環境では、正しく検証できていることを確認するために、実際に不正なDNS応答を流せる環境を用意。
- DMARCの仮想環境では、送信したメールのレポートの確認、受信したメールのレポート結果等が確認できる環境を用意。



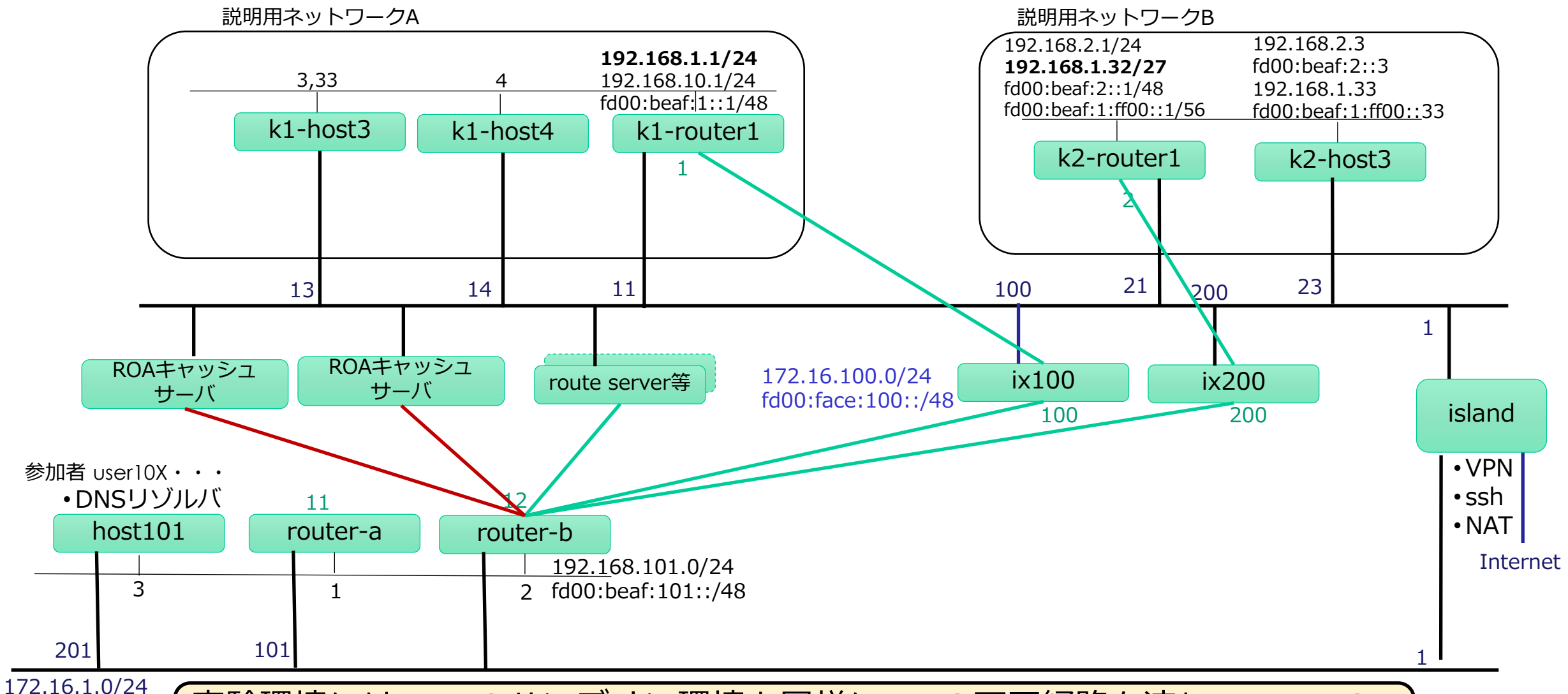
慶応大学

大阪大学

長崎県立大学

ISPにおけるネットワークセキュリティ技術の導入に関する調査, MRI, 総務省サイバーセキュリティタスクフォース（第43回）資料43－1－1,https://www.soumu.go.jp/main_content/000878673.pdf

実験環境



実験環境にはJPNICのハンズオン環境と同様にBGPの不正経路を流して、ROVの基本動作を確認する仕組みを用意。

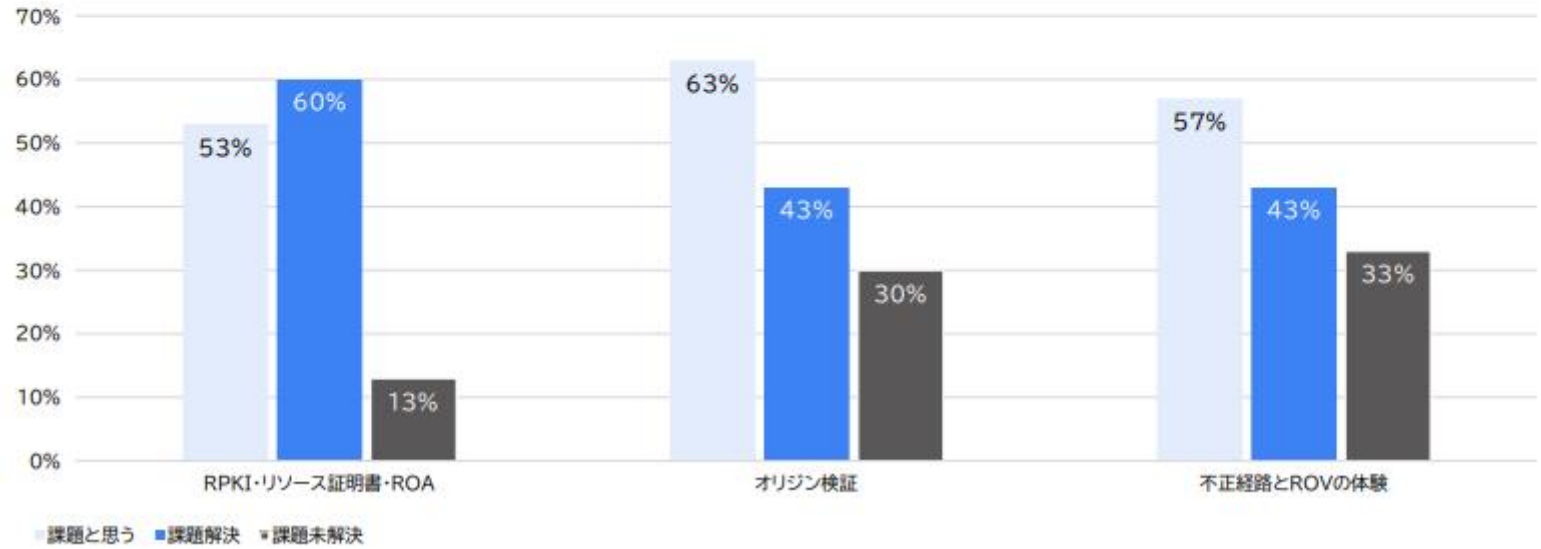
結果...

MRI

①RPKI ②DNSSEC ③DMARC

参考3. RPKI体験コースの結果

- 体験コースの主な内容である「RPKI・リソース証明書・ROA」、「オリジン検証」、「不正経路とROVの体験」は**各々53%～63%とそれぞれ課題認識が高い。**
- 体験コースの受講によって課題解消できた内容は、「RPKI・リソース証明書・ROA」は60%であり、**基礎的な内容については課題解消**できている。
- 一方、体験コースの情報だけでは課題解消できていないという回答は、「不正経路とROVの体験」が33%と高く、**他の実験コースなどの参加を推奨する必要**がある。



ISPにおけるネットワークセキュリティ技術の導入に関する調査, MRI, 総務省サイバーセキュリティタスクフォース（第43回）資料43－1－1,https://www.soumu.go.jp/main_content/000878673.pdf

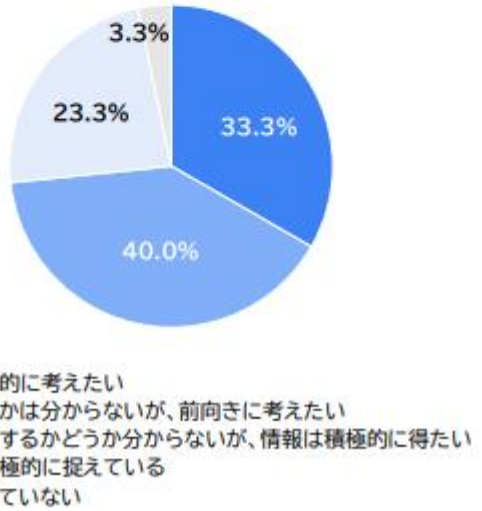
MRI

①RPKI　②DNSSEC　③DMARC

参考3. RPKI体験コースの結果

- 体験コースの受講の感想では、「RPKIに技術について**基礎的な知識が身につけられた」が73.3%**であり、基礎的な知識を習得するために有効である。
- また、「RPKI技術導入の検討に大いに役立った」が16.7%であり、上記とあわせて90%である。

- 今後のRPKIの導入については、「導入を積極的に考えたい」33.3%、「導入に至るかわからないが前向きに考えたい」40%であった。
- 「導入を検討するかどうか分からないが情報は積極的に得たい」が23.3%であり、「導入を積極的に考えたい」、「導入に至るかわからないが、**前向きに考えたい」とあわせると90%以上**と高く、**実体験はRPKI普及の効果が見込める。**



ISPにおけるネットワークセキュリティ技術の導入に関する調査, MRI, 総務省サイバーセキュリティタスクフォース（第43回）資料43－1－1,https://www.soumu.go.jp/main_content/000878673.pdf

技術的にわかってきたこと/論点と動き

BGPルータは安定して動作

複数のROAキャッシュサーバを指定して一つがダウンしても大丈夫

ROAが違っているようなケースでは、ROAキャッシュサーバで”例外”を設けられる。BGPルータでも対処できる。
(運用が簡単かは別として)

ROAキャッシュサーバの運用場所は…?安定性は…?

2023年度は…

実証実験、
開始しました。

＋

ガイドライン
＝指針

ガイドラインについて

(一口にガイドラインと言っても…)
内容により、関係者が順守すべき項目を示すものであったり、取り組むことが望ましいとされる基準の目安を示すものであったりしうる(*1)。

⇒ **実証実験が行われたあとに作られるガイドライン**

(*1) 国の行政機関が公表したガイドライン等の実態把握のための調査研究 報告書, 平成28年3月 株式会社 NTT データ経営研究所, 平成 27 年度 総務省 行政評価局請負調査
https://www.soumu.go.jp/main_content/000424429.pdf

今日のお話

■前半 ※敬称略

山口勝司 (ビッグローブ株式会社)

中村修 (慶応義塾大学 / WIDEプロジェクト)

■後半

ディスカッション