

APNIC 58

TE WHANGANUI A TARA
WELLINGTON,
AOTEAROA NEW ZEALAND
30 August - 6 September 2024

#apnic58



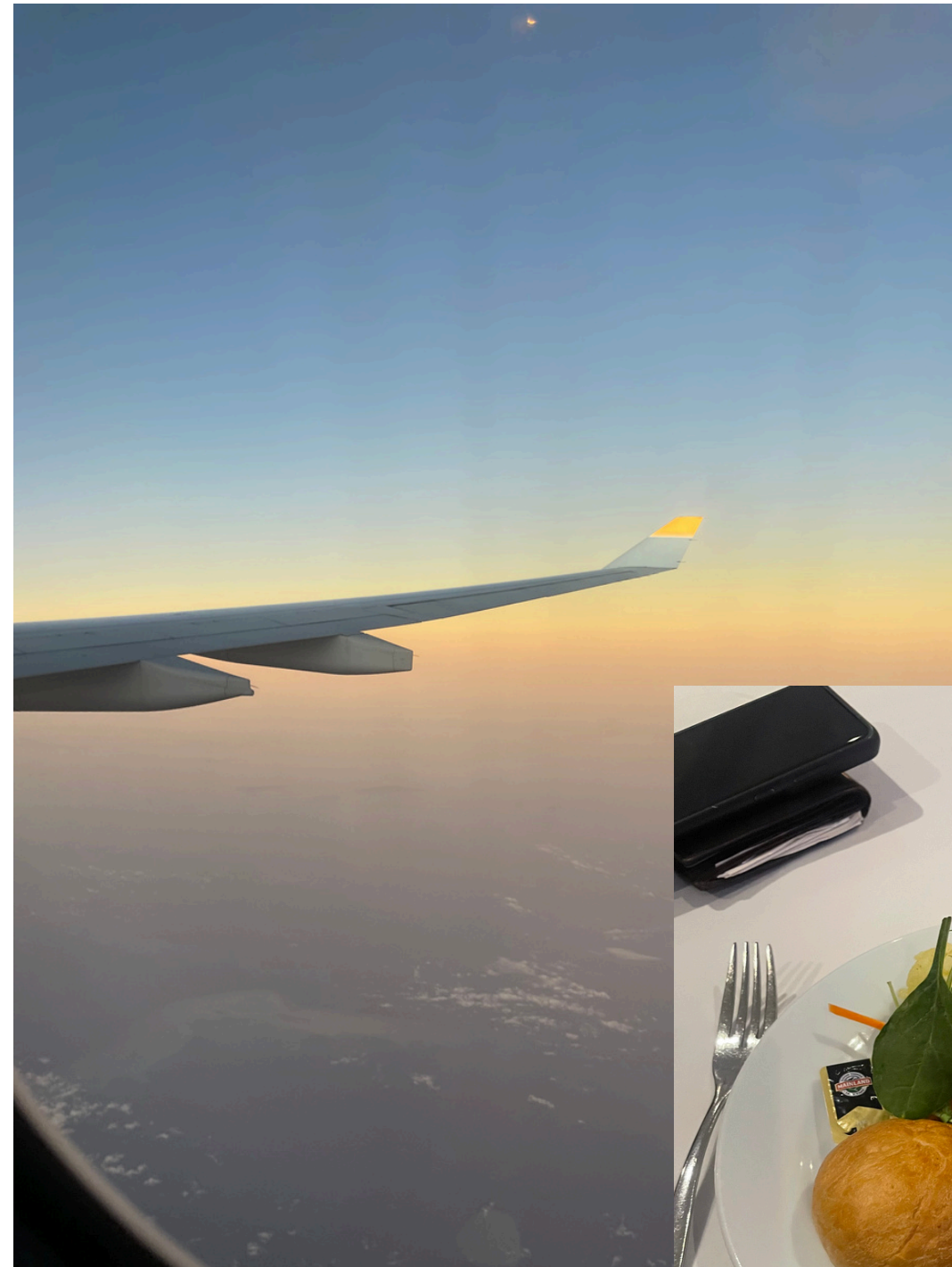
APNIC58参加報告

慶應義塾大学 2年 島田 怜奈



Agenda

- 自己紹介
- 本カンファレンスの概要
- 参加したセッション
- 特に印象に残ったセッションの紹介
 - Technical Session 1
 - Routing Security SIG
 - Open Policy Meeting
- 他参加者との交流
- カンファレンス全体の感想
- 参加プログラムに対する所感



自己紹介

島田怜奈

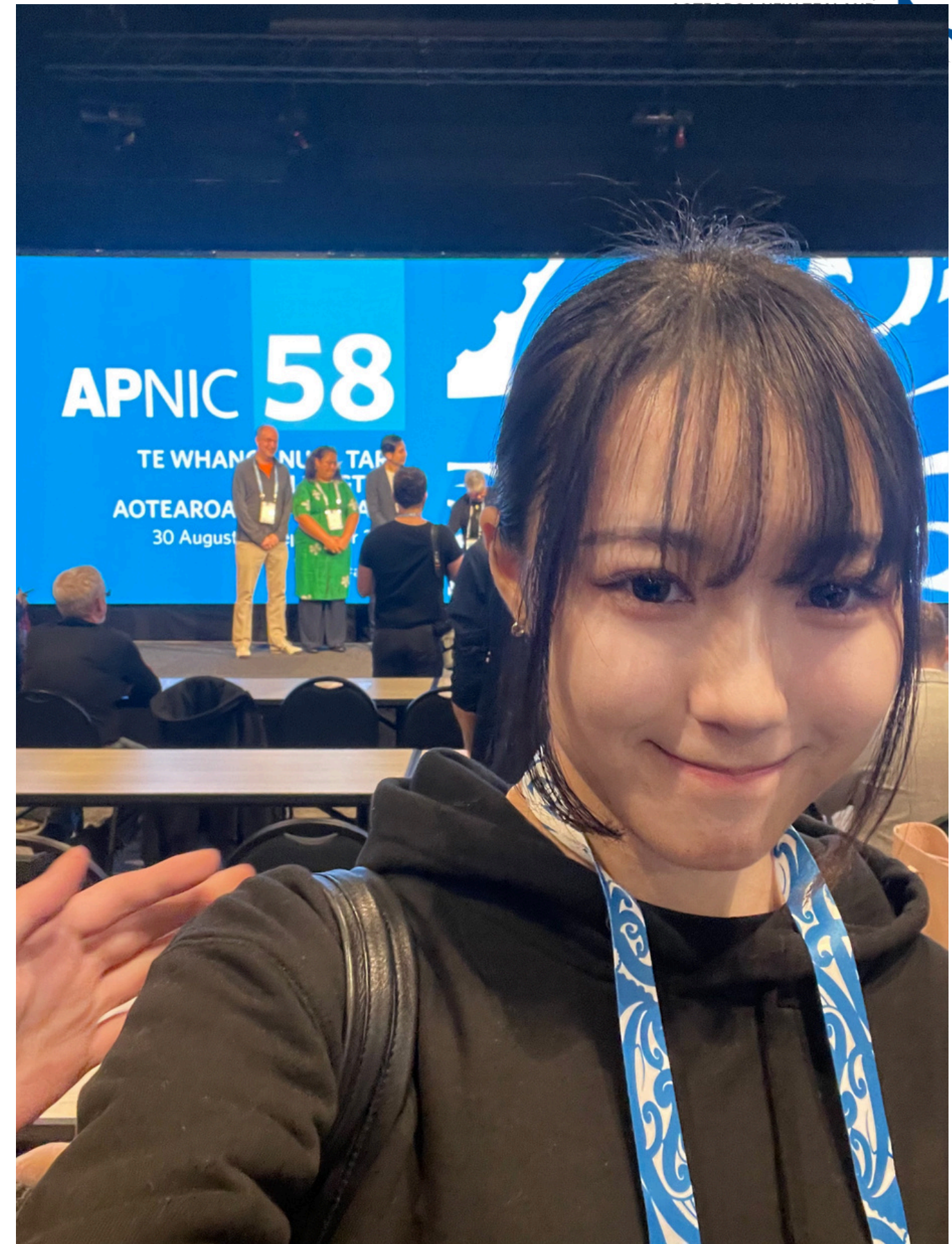
- ・ 慶應義塾大学 学部2年
- ・ 村井合同研所属

興味

- ・ BGP
- ・ RPKI (ASPA)
- ・ セキュリティ技術全般

参加動機

- ・ 国外の技術者との交流
- ・ 諸技術についての知見を深める
- ・ 英語ONLYで技術について議論
- ・ RPKIについて話す人を探す



本カンファレンスの概要

APNIC58

場所：ニュージーランド・ウェリントン

開催期間：8/30~9/6

フェローとしては9/3~9/6にかけて参加。

インターネットに関する様々な技術や
ポリシーについての議論に参加した。





参加したセッション

- AP Star Meeting
- Newcomers Session
- APNIC Opening Ceremony and Keynotes
- Technical Session 1
- Technical Session 2
- NextGen and Leadership BoF
- Welcome Social
- Ipv6 Deployment
- Routing Security SIG
- APNIC/FIRST Security Track 1
- Technical Session 3
- Lightning Talks
- Open Policy Meeting - Policy SIG 1
- Open Policy Meeting - Policy SIG 2
- APNIC Member Meeting 1
- Closing Social





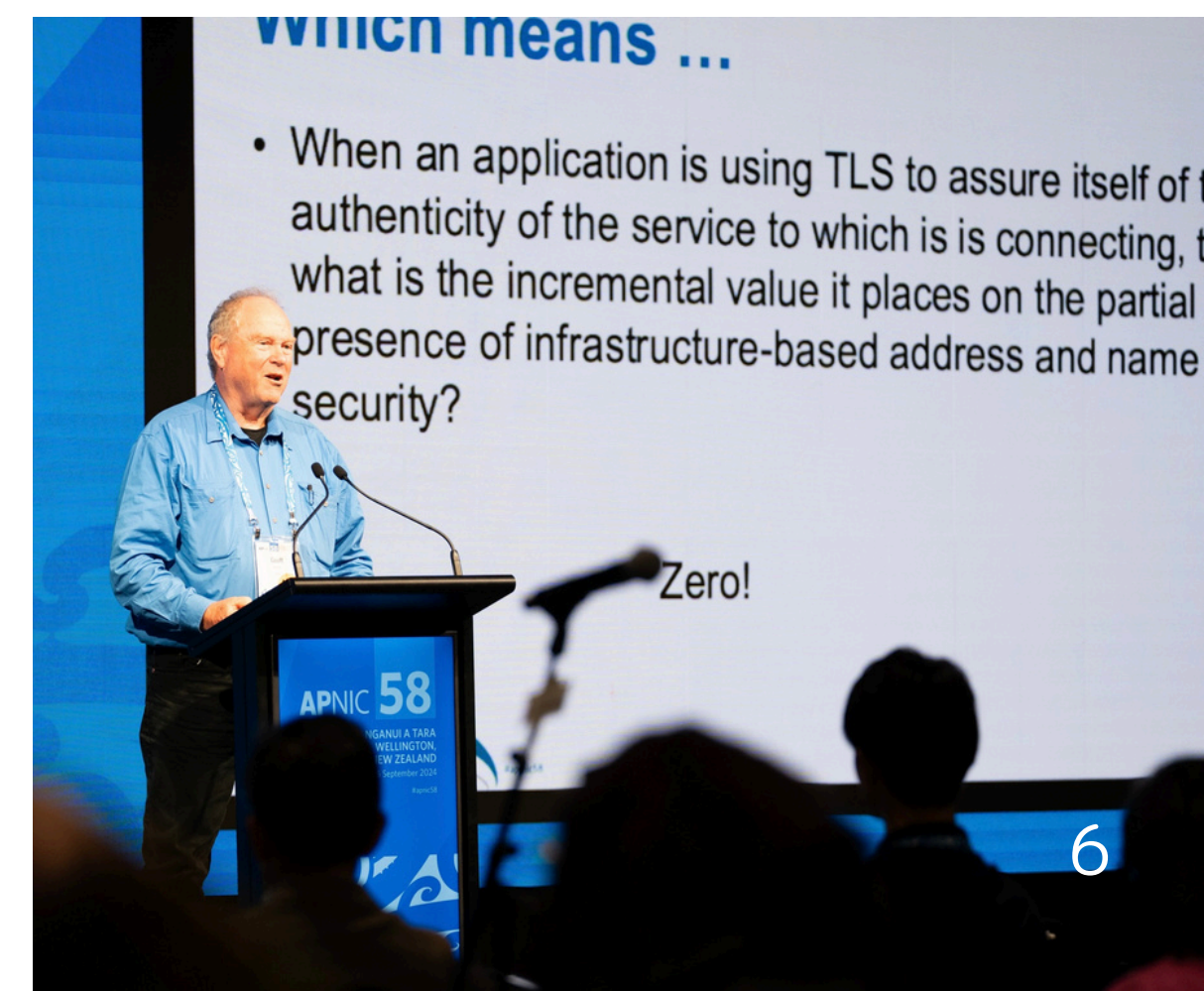
Technical Session 1

～インフラセキュリティ、クラウド、Starlinkと 最近のHOTなトピックに関する講演～

普及率が停滞しているDNSSEC/RPKI...これは「市場における失敗」なのか？

- インターネットは規制が少ない環境で運用
- セキュリティ技術の導入は「任意」
- 「導入価値 < コスト」の場合には導入されないことがある

→技術の普及率をどのように高めていくべきか再考する必要性





Routing Security SIG

□ルーティングセキュリティに関するトピックのみを扱った議論の場□

<4つのRPKIに関する講演>

- ① ROAおよびVRPの機能的な弱点
- ② RTBHとRPKIの互換性問題
- ③ ルーティングセキュリティにおけるSMGの導入
- ④ アジア圏、諸地域におけるRPKI普及動向

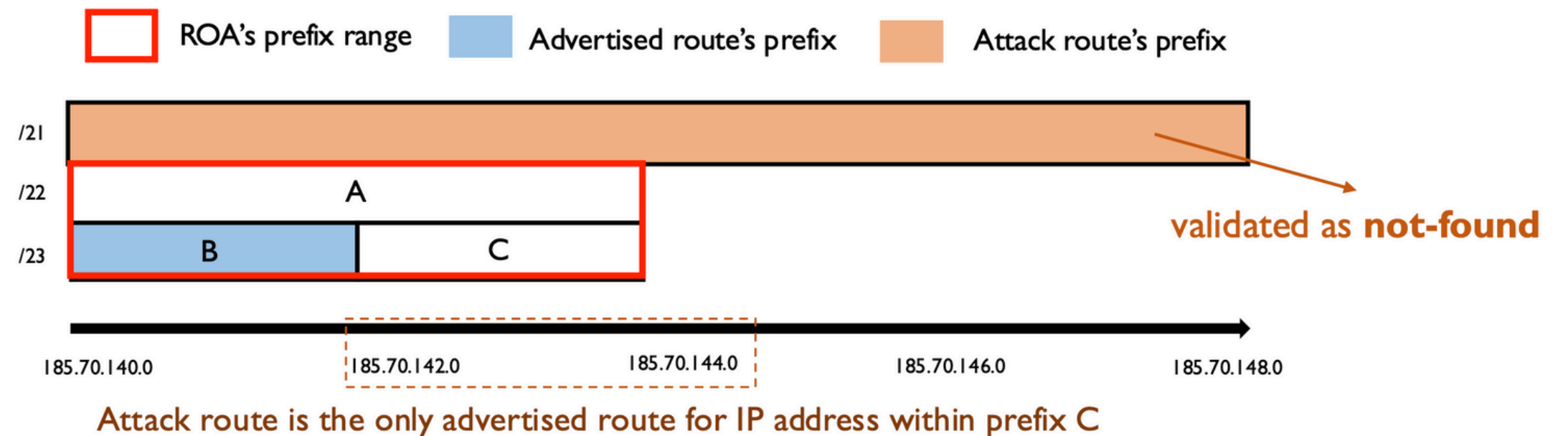


Problem statement of inconsistent securities of ROAs and VRPs

～ROAおよびVRPの機能的な弱点～

< BGPはRPKIによってセキュアになるはずだが、実はROA自体にも欠点がある >

- Super-prefix hijack
- Forged-origin hijack



→対策として諸技術の導入を検討すべき

Super-prefix hijack: DISCO(NDSS 2020) , SLURM(RFC 8416)

Forged-origin hijack: DFOH(NDSS 2024)

A tale of two synergies: Uncovering RPKI practices for RTBH

□RTBHとRPKIの互換性問題□

< DDoSにはRTBH, BGP hijackにはRPKI...だがこの二つは併用不可能? >

- ・ RTBHを採用しているIXPの約91%がROAを作成をしている。
→うち85%がRPKI上ではinvalid とされる RTBHリクエストを送信している

<i>Operator Profile</i>	<i>IPv4</i>	<i>IPv6</i>
RPKI-strict	4	1
RPKI-loose	26	1
RTBH-agnostic	182	6

Number of IXP peers -involved in RTBH - grouped by RTBH+RPKI attitude

← 調査によりRTBH用の経路広告が RPKI invalidとなったケース数

具体的な一つの解決策はまだ無い。

→どちらか一方の効果を損なうことなく両者を併用できる運用方法を模索したい

A Signed Group of Multiple-Origin ASes for Use in the Resource Public Key Infrastructure (RPKI)

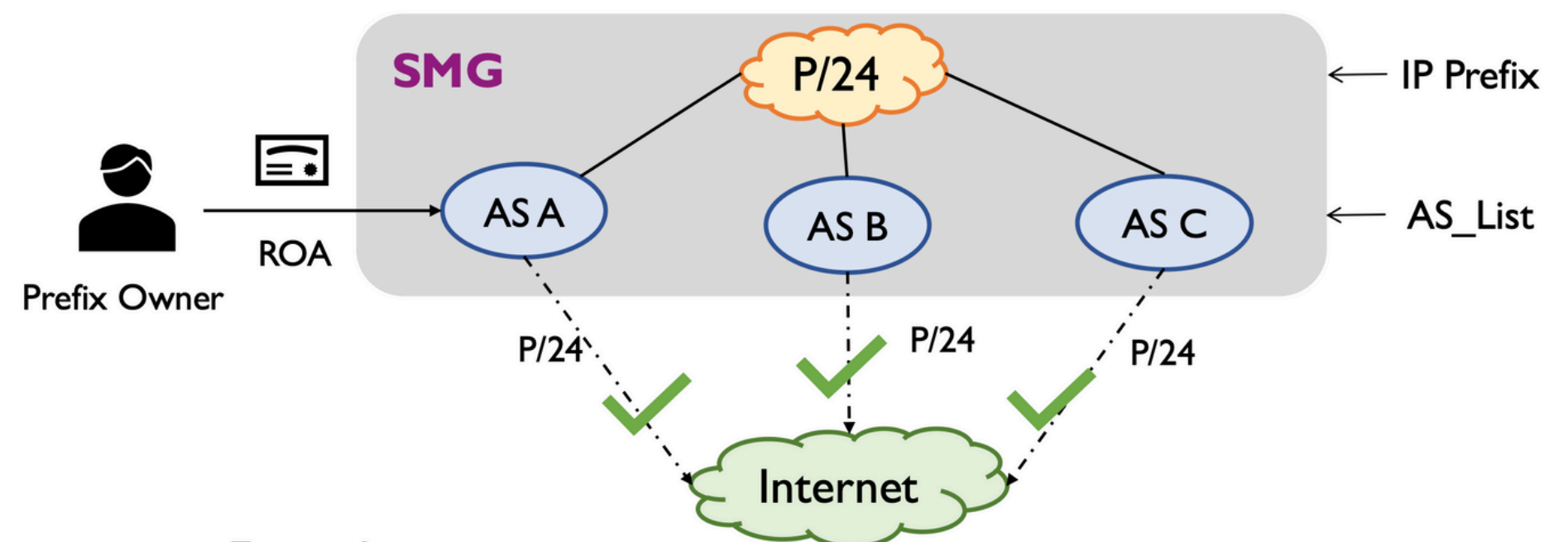
□ルーティングセキュリティにおけるSMGの導入□

ROAと違い、複数のASグループと一つのprefixの対応関係を証明

- ・ ROAとSPL方式で組み合わせてより正確なValidation結果を得る。

正直これは完全に理解しているとは言い難いので引き続き調査したい。

- ・ そもそもなぜSMGが必要なのか？
- ・ 実際のユースケースは？
- ・ 運用上の懸念点は？



Example:

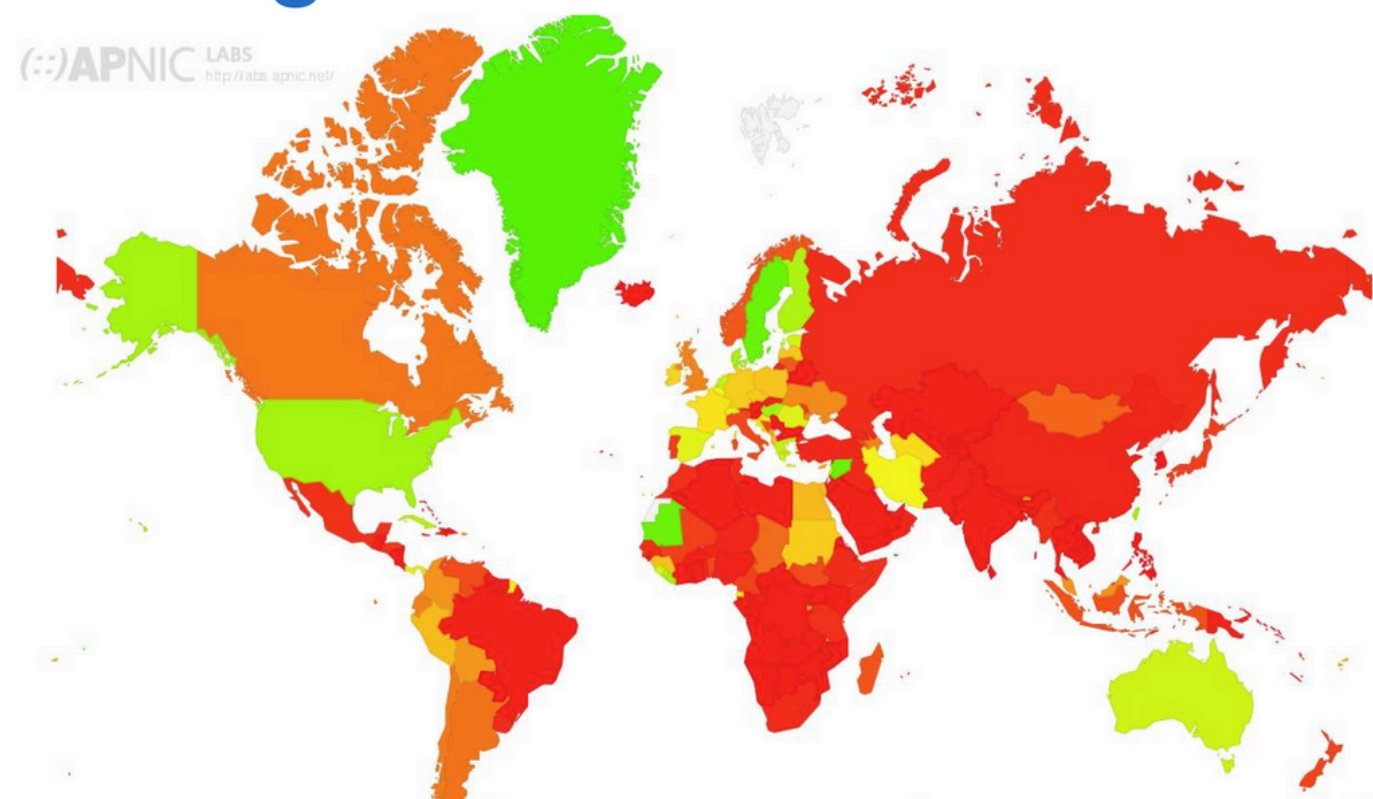
Signed MOAS Group Object: P/24 {AS A, AS B, AS C}

RPKI Asia-Pacific Update

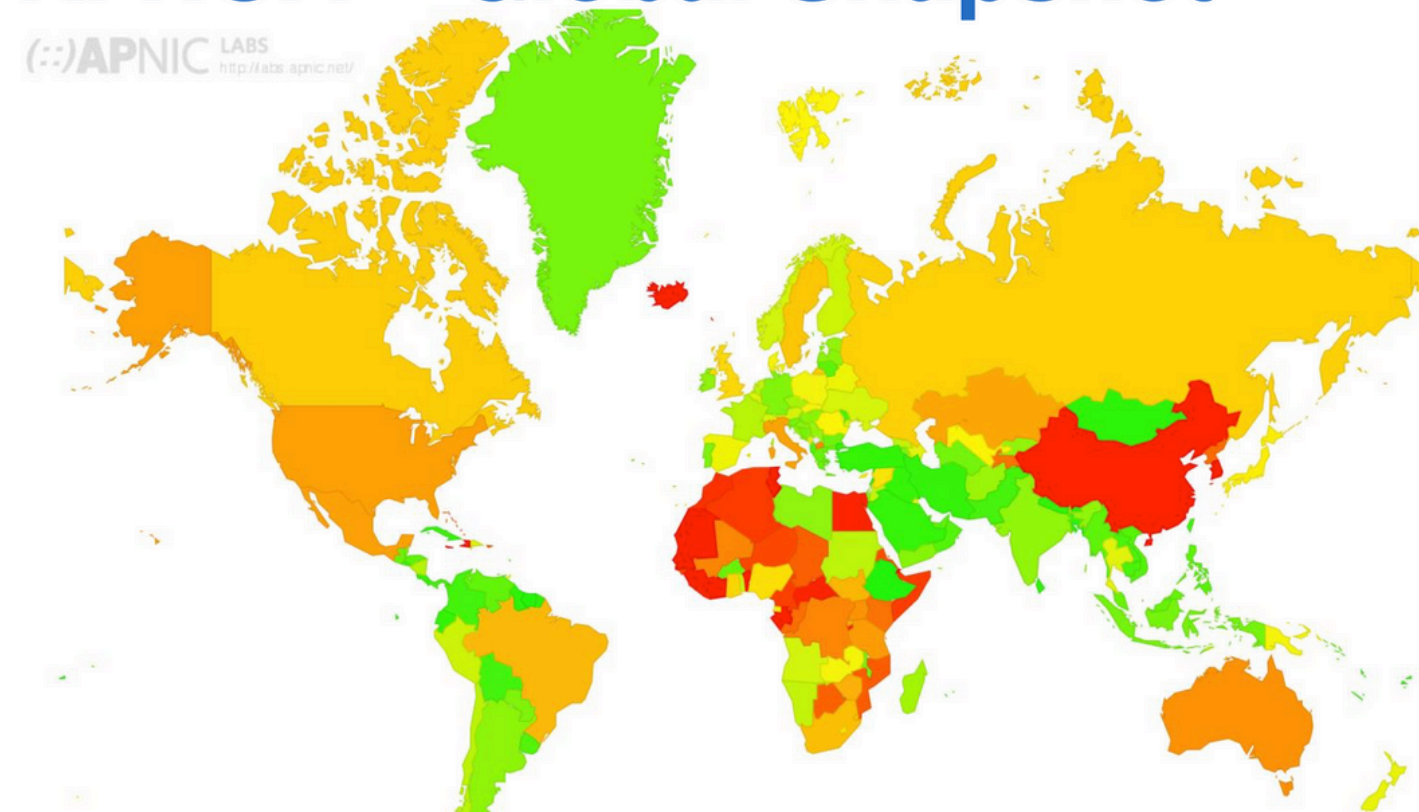
□アジア圏、諸地域におけるRPKI普及動向□

日本のROA普及率は悪くはない。ROV実施状況はまだまだ。

Route Origin Validation



RPKI ROA – Global Snapshot



・ Validationを実施しなければRPKIの本来の意義は失われる

→自分が関与しているコミュニティのネットワークに率先してROVを導入する



Open Policy Meeting

□IPアドレスやAPNICの運営方針などを決める□

IPv6の割り当てサイズの最小値を/32から/36に変更するという提案や、IPv6アドレスをIoT機器に導入するという提案など斬新なものが多く見えた

結果的にコンセンサスとなったものは無かったが、投票に参加させてもらった

→これからも多くの面白いプロポーザルが生まれそうなのでメーリスを積極的にチェックしていきたい

ipv6の例え方やRPKIのipv6応用についての話がとても興味深かった

IPv6 for Sand

“If the earth were made entirely out of 1 cubic millimetre grains of sand, then you could give a unique address to each grain in 300 million planets the size of the earth”
---- Wikipedia

Whois, RPKI and RTA provide authenticity for IPv6

Resource Tagged Attestations, or RTAs, are a new type of RPKI object, allowing any arbitrary file to be signed 'with resources' by one or more parties. The RTA object is a separate file that cryptographically connects the document with a set of resources. The receiver of the object can use an RPKI validator to show these resources, and verify that it was created by the rightful holder(s) of those resources.

registry database

- whois
- RDAP
- RPKI

IOT IPv6 prefix Meta Data

- IOT usage description
- IOT item lifecycle
- CGA public key
- Necessary graph
- ...

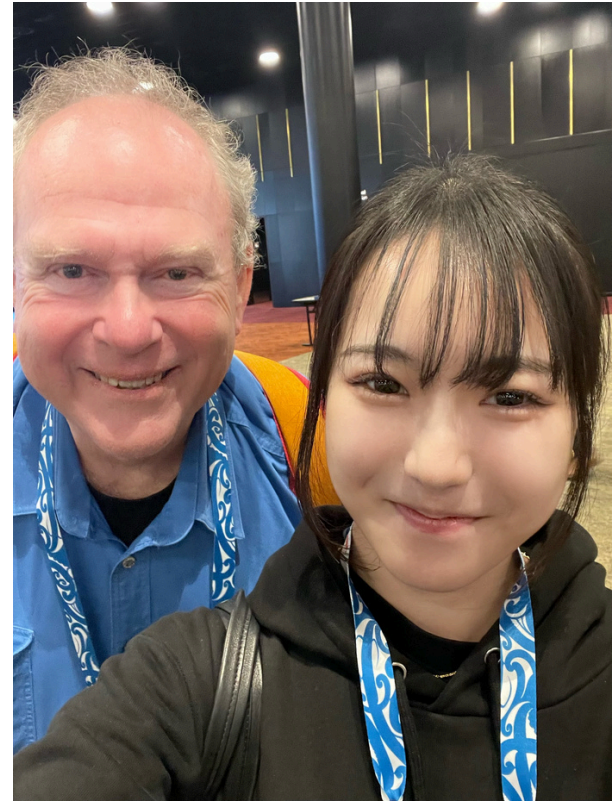
12



他参加者との交流

様々な場を通して多くの技術者の皆様と議論を交わしたり、
談笑する機会があった。

特にRPKIに関するドラフトの著者の方やGeoff Huston氏と議論を
交わせたのは貴重な経験で今後の活動において有益となると思う



カンファレンス全体の感想

想像以上にオープンな議論の場で驚いた。

IXPのオペレータなど日常的にネットワークの運用を行っている方が多いのか、議論が全て現実的なファクトに基づいており諸課題の本質が追求されていた。とても見習いたいと感じた。



まとめと今後の展望

- ・ オープンな場に参加することの重要性を感じた
→ 未参加の会議が沢山あるのでいつか参加したい
- ・ 何事も主権を握るのは人なので技術は適切に使用する必要がある
 - ・ セキュリティを勉強するにあたって倫理的な観点も身につけたい
- ・ 今後のインターネットの利便性の向上に貢献できる人材でありたい
(背伸びはせず出来ることから頑張ろうと思う)





参加プログラムに対する所感

金銭面のみならず精神面においても出国前から手厚いサポートをいただき、そのおかげで安心して過ごすことができ、本当に感謝しています。

学生という立場でこのような国際的な場に参加する機会が滅多にないためその機会を与えてくださった本プログラムには深い感謝をすると共にこの経験を無駄にせず、将来的に業界に還元していきたいです。

同様のプログラムがまたあるならば知り合いに積極的に進めたいと思います。

本当にありがとうございました。

