

RPKIに関する最新動向

IETF117報告会

2023年8月28日(月)
木村泰司



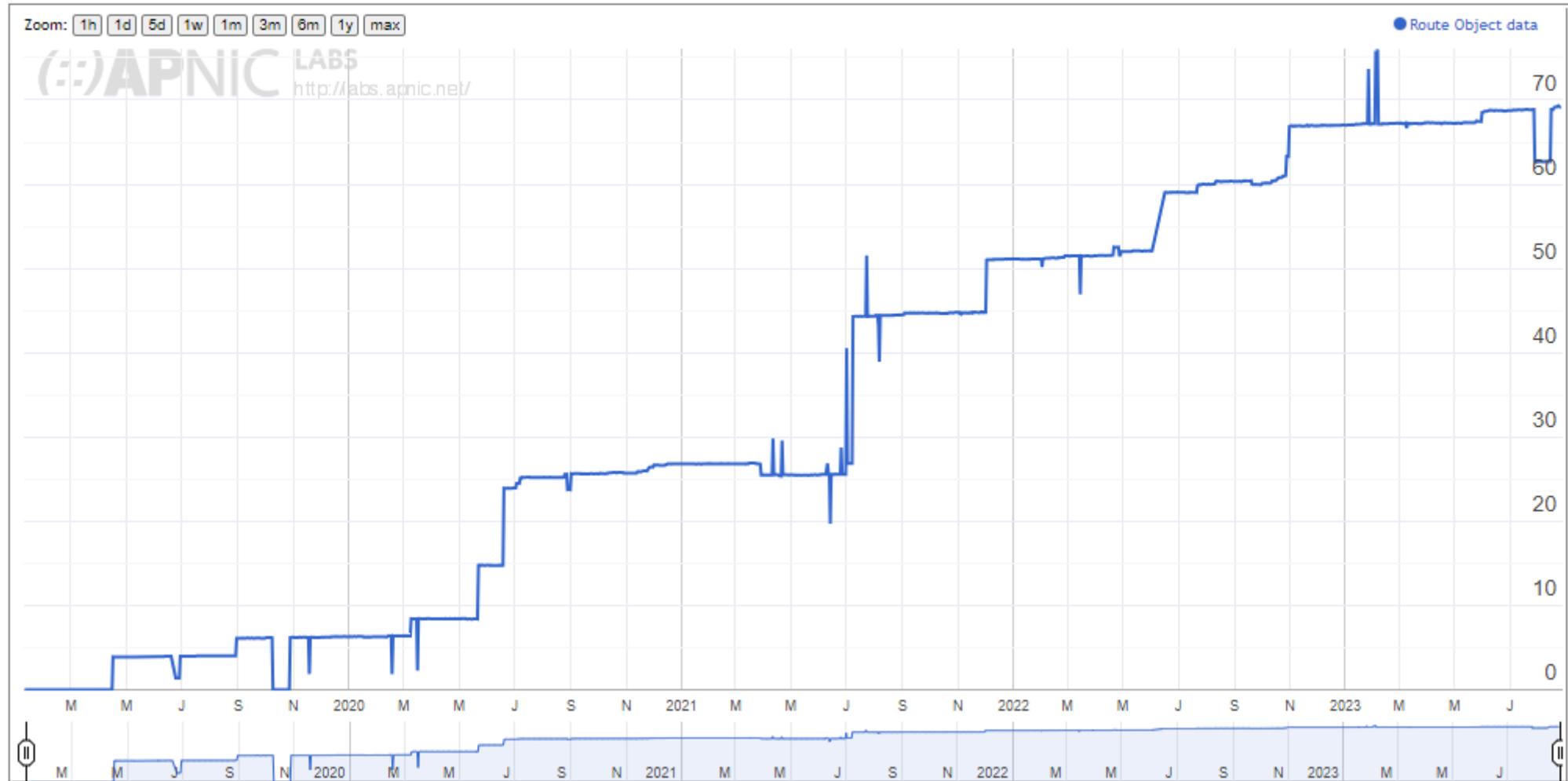
一般社団法人 日本ネットワークインフォメーションセンター

Copyright © 2023 Japan Network Information Center



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”, 2023/8/270時点



IETF SIDR Operations (sidrops) WG (1)

- 2016年11月設立

2012 2013 2015 2016 2017 2018 2019 2020 2021 2022 2023

sidrops WG started

sidr WG concluded

RFC8897
RP要件

RFC9286
Manifest

RFC9455
ROA-multi

RFC6482 RFC6810
ROA profile RTR

RFC8182
RRDP

RFC8481
OV再定義

RFC8893
OV結果伝達

RFC9255
ID関連なし

RFC6486 RFC6811
Resource Origin Validation
cert. profile

RFC8488
Routinator事例

RFC9319
maxlen

最大プレフィックス長の利用を“最小限”に。

RFC6490
TAL

RFC8630
TALの更新

RFC9323
RSC

RFC9324
経路リフレッシュ

ROAとROVに関するRFC

RFC8608
rtr-keying
RFC8634
bgpsec-rollover

BGPSECに関するRFC

RFC8608
bgpsec-algs-rfc8208-bis

▶▶▶ IETF SIDR Operations (sidrops) WG (2)

- セキュアドメイン間ルーティング(SIDR)の運用に関する経験と、開発やリサーチ/計測のコミュニティ（発表者要約）
- ゴール
 1. SIDRが意識されているインターネットにおける運用上の問題を特定し、その問題に対する解決策や回避策を決定するために、さまざまな運用者から意見を求める。
 2. SIDRが意識されていないインターネットとの相互作用に関する問題を特定し、それらの問題に対する解決策や回避策を決定するために、すべてのオペレーターから意見を求める。
 3. 特定された問題に対する運用上の解決策を策定し、情報文書またはBCP文書に文書化する。

(出典 : <https://datatracker.ietf.org/wg/sidrops/about/> *DeepL翻訳を使用)

▶▶▶ IETF SIDR Operations (sidrops) WG (3)

- **IETF117におけるsidrops WG会合**

- 2023年7月25日(月) 17:30-18:35

- 35~40名

- Minutes

- <https://datatracker.ietf.org/doc/minutes-117-sidrops-202307250030/>

- SIDR Operations (sidrops) - Datatracker

- <https://datatracker.ietf.org/wg/sidrops/about/>

▶▶▶ IETF117 sidrops WG会合アジェンダ (1/3)

- プレフィックス・リストへのRPKI署名 /
A profile for RPKI Signed Lists of Prefixes, Geoff Huston,
draft-spaghetti-sidrops-rpki-prefixlist
 - ASが経路広告するプレフィックスの一覧に対して署名したオブジェクトの提案。IRRにおけるroute-set:オブジェクトにあたる。
- ASPAオブジェクトを使ったASパス検証 /
BGP AS_PATH Verification Based on ASPA Objects, Sriram Kotikalapudi,
draft-ietf-sidrops-aspa-verification
 - 順調に進行中。WG Last Call。

▶▶▶ IETF117 sidrops WG会合アジェンダ (2/3)

- 人が読み取りやすいVRP記法 /
Human Readable Validate ROA Payload Notation,
draft-timbru-sidrops-vrp-notation
人が読み取りやすいASPA記法
Human Readable ASPA Notation, Oliver Borchert
draft-timbru-sidrops-aspa-notation
 - RPソフトウェアごとに共通の記法にするなどの提案。
ASPAの方はValidated ASPA Payloads (VAPs)と呼ばれる。
- RPKI公開サーバのベスト・カレント・プラクティス /
RPKI Publication Server Best Current Practices, Ties de Kock
draft-timbru-sidrops-publication-server-bcp
 - ドラフトの中身が示されていない。ドラフトは単にRRDPとRsyncのオンラインサービスを維持するためにCDNを使っていいとか、その程度。オブジェクトのセキュリティの話はない。

▶▶▶ IETF117 sidrops WG会合アジェンダ (2/2)

- RPKI署名オブジェクトにおけるCMS署名時刻属性の利用 /
On the use of the CMS signing-time attribute in RPKI Signed Objects, Job Snijders
draft-spaghetti-sidrops-cms-signing-time
 - RRDPからrsyncにfail overするときに起きる問題の提起。RPがファイルを書き込むときにタイムスタンプを現在時刻にしてしまう。CMS署名時刻を必須にする提案。
- RPKIとIPsecに基づくAS間のソースアドレス検証 /
An RPKI and IPsec-based AS-to-AS Approach for Source Address Validation,
Yangfei Guo
draft-xu-ipsecme-risav-02.txt
 - RPKIを使ったIPsec SAの保護とソースアドレス検証(SAV)。IPSECMEへ。

おわり