資料 30－3

情報通信ネットワークの将来像とセキュリティ技術に関する標準化を巡る議論の動向について

～ “インターネットの基本的なサービスをより安全にする仕組み”と合わせて ～

2021年4月7日

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

ご意見を伺いたい二つの話題

1. **インターネットの基本的なサービスをより安全にする仕組みについて**
   - RPKI
   - DNSSEC

⇒中期的な話題

2. **国際的な標準化活動と情報通信アーキテクチャに関する技術動向の把握について**

⇒長期的な話題

インターネットの基本的なサービスを
より安全にする仕組みについて

1. インターネットの基本的なサービスをより安全にする仕組み

- **ルーティング(経路制御)**
  - IRR (Internet Routing Registry)
  - RPKI (Resource Public-Key Infrastructure)
- **DNS**
  - DNSSEC (Domain Name System Security Extensions)

RPKIについて ーRPKIとはー

- **Resource Public-Key Infrastructure**
  - IPアドレスやAS番号といった番号資源（Number Resource）の割り振り／割り当てをリソース証明書で証明する

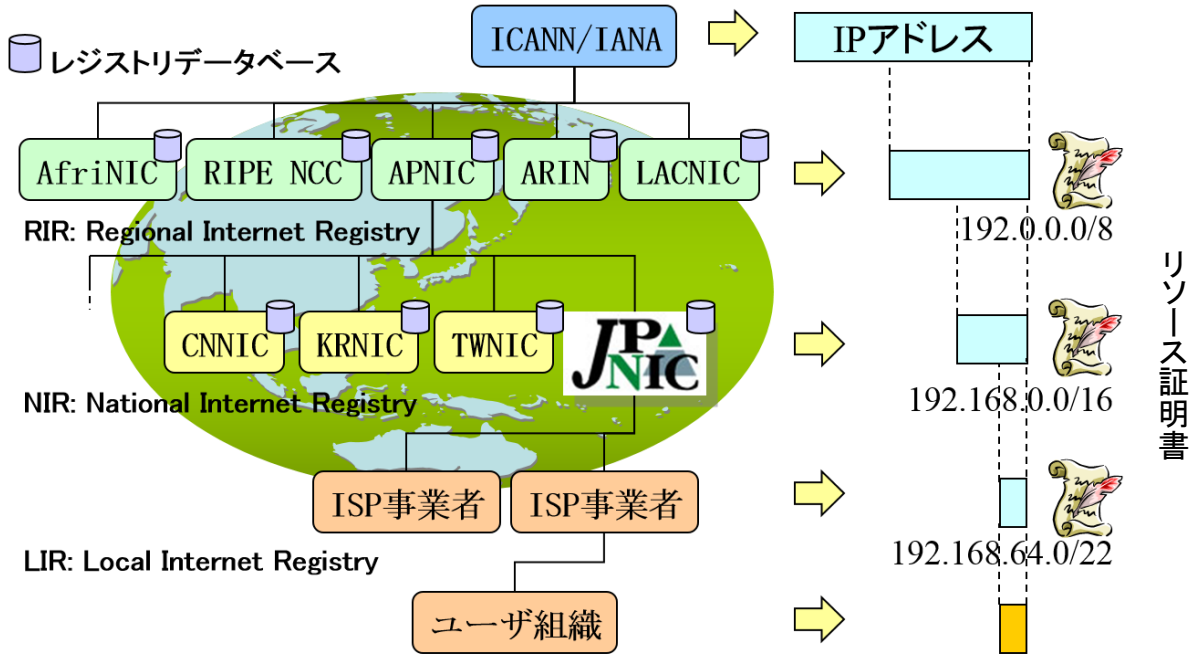
IPアドレスが正しいものかを確認できる

↓

BGPの経路情報が正しいかどうかを確認できる

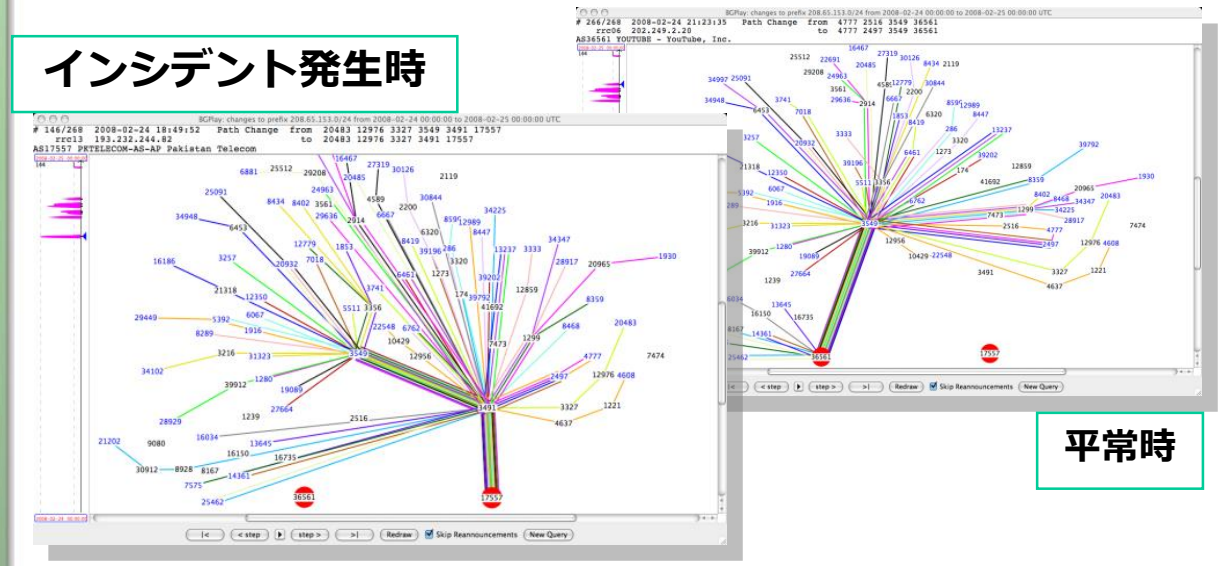
↓

IPアドレスの不適切な利用を検知するために利用できる



ルーティングに関わる代表的な事例

□ YouTube(2008年)



YouTube Hijacking: A RIPE NCC RIS case study, 17 Mar 2008, RIPE NCC, http://www.ripe.net/internet-coordination/news/industry-developments/youtube-hijacking-a-ripe-ncc-ris-case-study

YouTubeの経路情報が別のASによって広告され、約2時間半の間、アクセスできなくなった。

□ MyEtherWallet.com(2018年)

手法

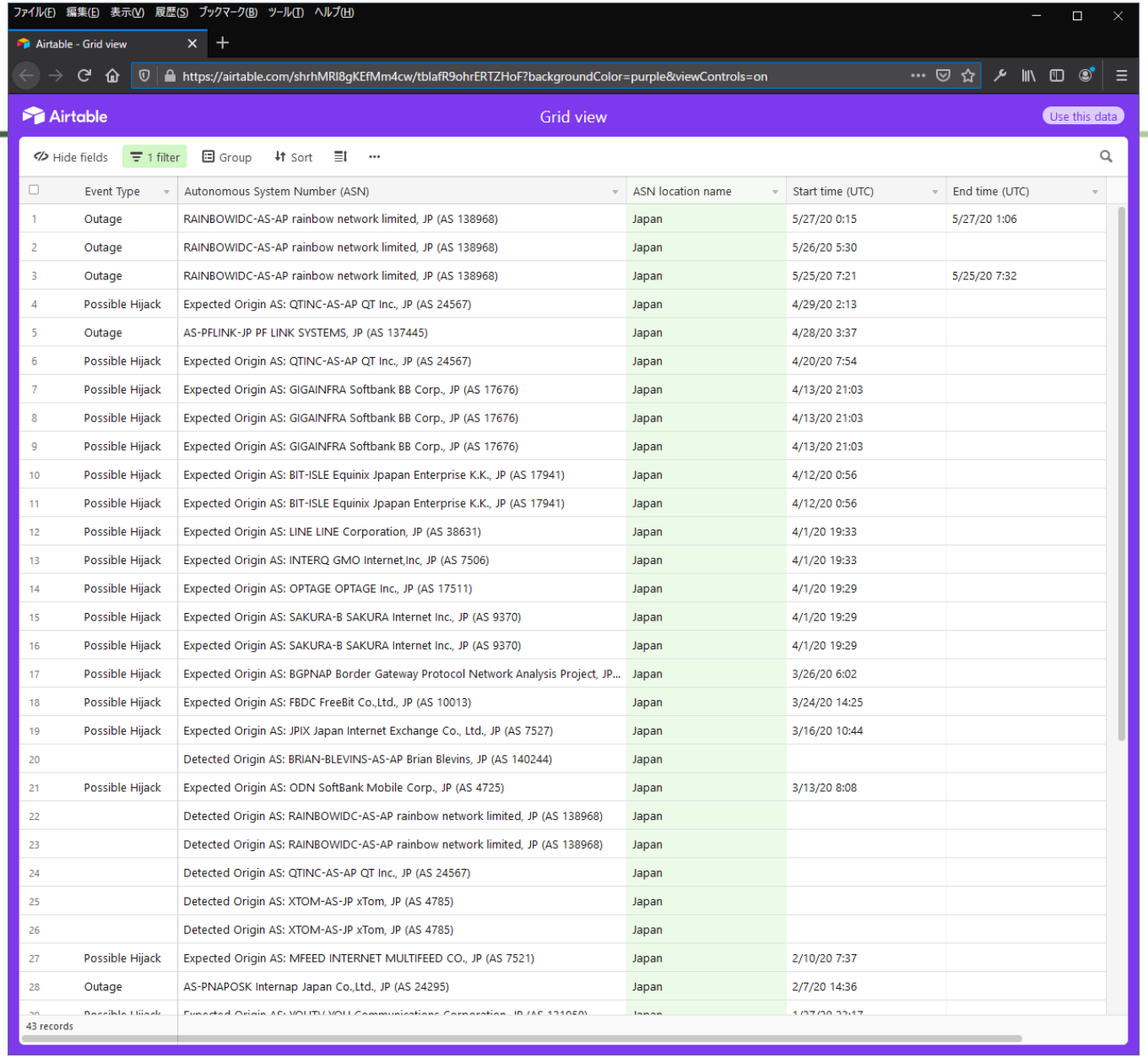
- AWS Route 53の経路(/23など)を/24で経路広告
- MyEtherWallet.comの問い合わせに対して偽のAレコードを応答
- サーバ証明書は自己署名証明書だった模様（本来EV SSL証明書"MyEtherWallet Inc"）

影響

- 総額15万ドル（約1630万円）相当が不正送金される
- サーバ証明書のエラーを無視して接続したユーザは他のウォレットに送金させられた

不正な経路広告によって偽のDNS応答を返し、偽のサーバにアクセスさせ不正送金したという報告

MyEtherWallet、DNSサーバーにハッキング、15万ドル分のETH盗難か
https://jp.cointelegraph.com/news/myetherwallet-warns-that-a-couple-of-its-dns-servers-have-been-hacked
AWS DNS network hijack turns MyEtherWallet into ThievesEtherWallet - The Register, 2018/4/24
https://www.theregister.co.uk/2018/04/24/myetherwallet_dns_hijack/

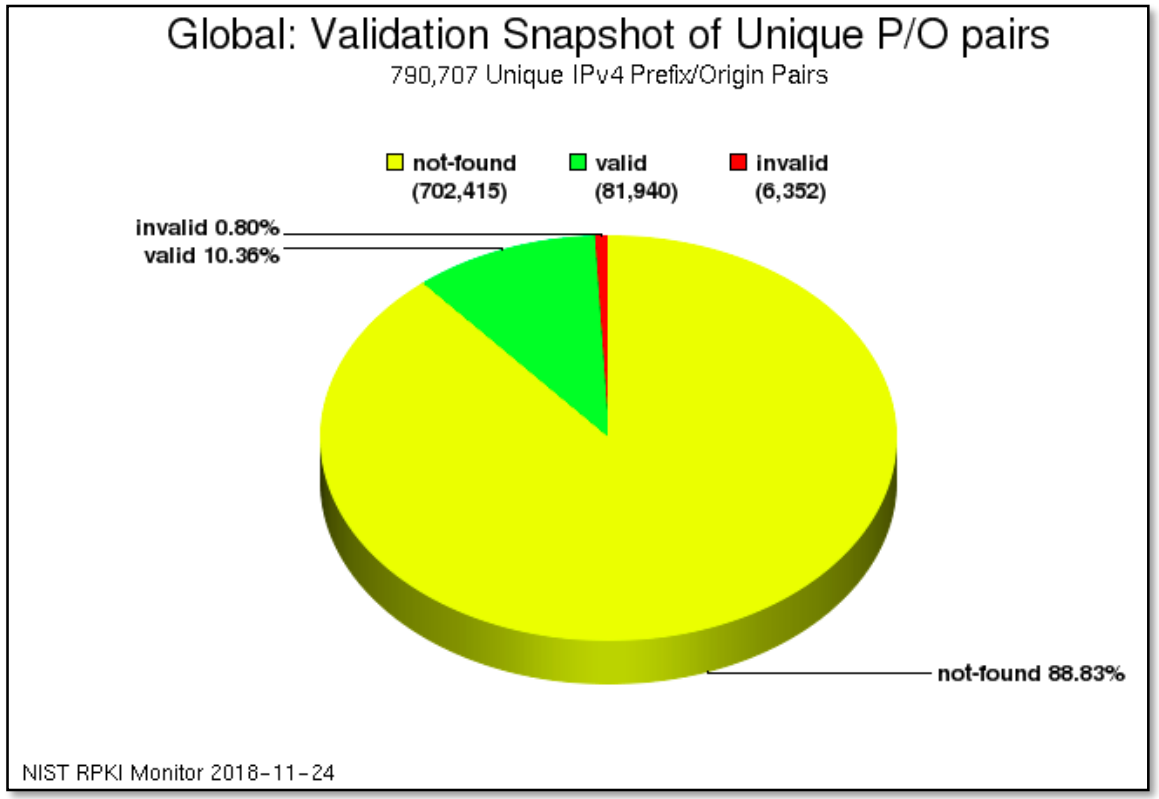


	Event Type	Autonomous System Number (ASN)	ASN location name	Start time (UTC)	End time (UTC)
1	Outage	RAINBOWIDC-AS-AP rainbow network limited, JP (AS 138968)	Japan	5/27/20 0:15	5/27/20 1:06
2	Outage	RAINBOWIDC-AS-AP rainbow network limited, JP (AS 138968)	Japan	5/26/20 5:30	
3	Outage	RAINBOWIDC-AS-AP rainbow network limited, JP (AS 138968)	Japan	5/25/20 7:21	5/25/20 7:32
4	Possible Hijack	Expected Origin AS: QTINC-AS-AP QT Inc., JP (AS 24567)	Japan	4/29/20 2:13	
5	Outage	AS-PFLINK-JP PF LINK SYSTEMS, JP (AS 137445)	Japan	4/28/20 3:37	
6	Possible Hijack	Expected Origin AS: QTINC-AS-AP QT Inc., JP (AS 24567)	Japan	4/20/20 7:54	
7	Possible Hijack	Expected Origin AS: GIGAINFRA Softbank BB Corp., JP (AS 17676)	Japan	4/13/20 21:03	
8	Possible Hijack	Expected Origin AS: GIGAINFRA Softbank BB Corp., JP (AS 17676)	Japan	4/13/20 21:03	
9	Possible Hijack	Expected Origin AS: GIGAINFRA Softbank BB Corp., JP (AS 17676)	Japan	4/13/20 21:03	
10	Possible Hijack	Expected Origin AS: BIT-ISLE Equinix Jpapan Enterprise K.K., JP (AS 17941)	Japan	4/12/20 0:56	
11	Possible Hijack	Expected Origin AS: BIT-ISLE Equinix Jpapan Enterprise K.K., JP (AS 17941)	Japan	4/12/20 0:56	
12	Possible Hijack	Expected Origin AS: LINE LINE Corporation, JP (AS 38631)	Japan	4/1/20 19:33	
13	Possible Hijack	Expected Origin AS: INTERQ GMO Internet,Inc, JP (AS 7506)	Japan	4/1/20 19:33	
14	Possible Hijack	Expected Origin AS: OPTAGE OPTAGE Inc., JP (AS 17511)	Japan	4/1/20 19:29	
15	Possible Hijack	Expected Origin AS: SAKURA-B SAKURA Internet Inc., JP (AS 9370)	Japan	4/1/20 19:29	
16	Possible Hijack	Expected Origin AS: SAKURA-B SAKURA Internet Inc., JP (AS 9370)	Japan	4/1/20 19:29	
17	Possible Hijack	Expected Origin AS: BGPNAP Border Gateway Protocol Network Analysis Project, JP...	Japan	3/26/20 6:02	
18	Possible Hijack	Expected Origin AS: FBDC FreeBit Co.,Ltd., JP (AS 10013)	Japan	3/24/20 14:25	
19	Possible Hijack	Expected Origin AS: JPIX Japan Internet Exchange Co., Ltd., JP (AS 7527)	Japan	3/16/20 10:44	
20		Detected Origin AS: BRIAN-BLEVINS-AS-AP Brian Blevins, JP (AS 140244)	Japan		
21	Possible Hijack	Expected Origin AS: ODN SoftBank Mobile Corp., JP (AS 4725)	Japan	3/13/20 8:08	
22		Detected Origin AS: RAINBOWIDC-AS-AP rainbow network limited, JP (AS 138968)	Japan		
23		Detected Origin AS: RAINBOWIDC-AS-AP rainbow network limited, JP (AS 138968)	Japan		
24		Detected Origin AS: QTINC-AS-AP QT Inc., JP (AS 24567)	Japan		
25		Detected Origin AS: XTOM-AS-JP xTom, JP (AS 4785)	Japan		
26		Detected Origin AS: XTOM-AS-JP xTom, JP (AS 4785)	Japan		
27	Possible Hijack	Expected Origin AS: MFEED INTERNET MULTIFEED CO., JP (AS 7521)	Japan	2/10/20 7:37	
28	Outage	AS-PNAPOSK Internap Japan Co.,Ltd., JP (AS 24295)	Japan	2/7/20 14:36	

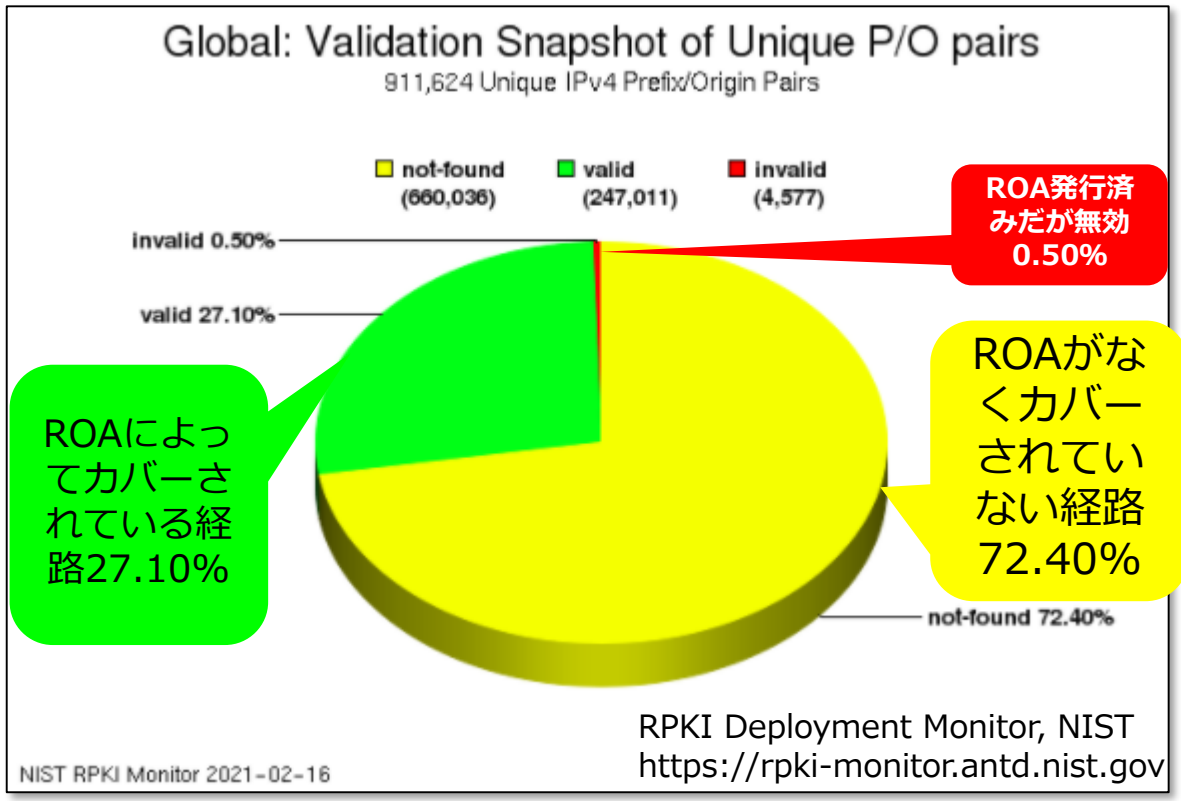
Airtable
https://airtable.com/shrhMRl8gKEfMm4cw/tblafR9ohrERTZHoF?backgroundColor=purple&viewControls=on

グローバルな普及の状況 - NIST(アメリカ国立標準技術研究所)が観測するカバー率

2018年



2021年



RPKI Deployment Monitor, NIST
https://rpki-monitor.antd.nist.gov

- **Invalid:AS** Covering ROA Prefix, maxLength Satisfied, and AS Mismatch.
- **Invalid:ML** Covering ROA Prefix, maxLength Exceeded, and AS Match.
- **Invalid:ML-AS** Covering ROA Prefix, maxLength Exceeded, and AS Mismatch.
- **Invalid:AS-SET** The origin AS could not be determined from the BGP update used to announce the prefix (i.e., because it contains an AS-SET), and a ROA covering the prefix exists.

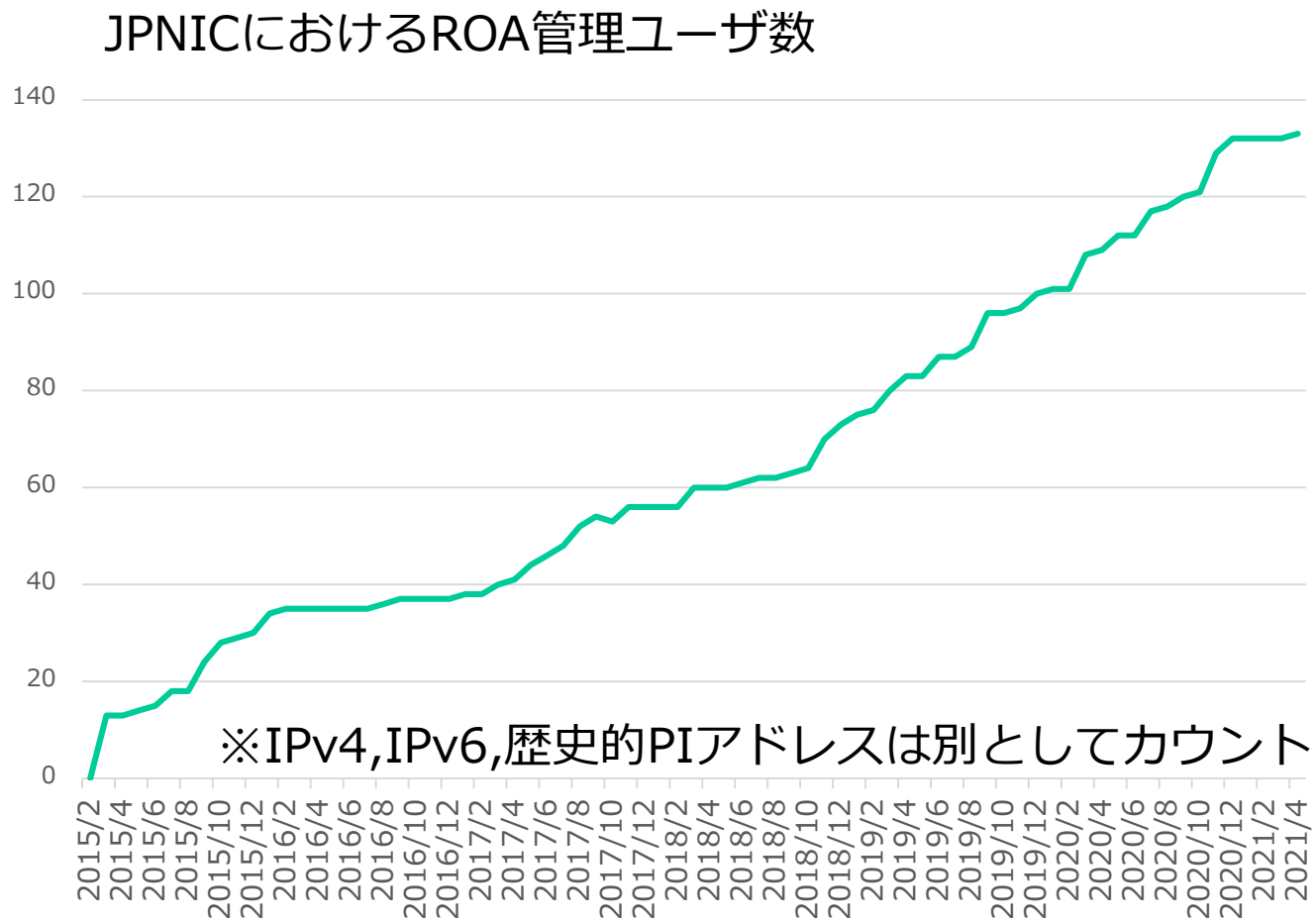
二年前に比べて明らかにカバー率が増加。大手事業者のROV導入も鍵か。

JPNICのRPKI試験提供

2021年4月

- **割り振られているIPアドレスに対してROAがカバーする割合**
  - 44.6% IPv4
  - 57.2% IPv6

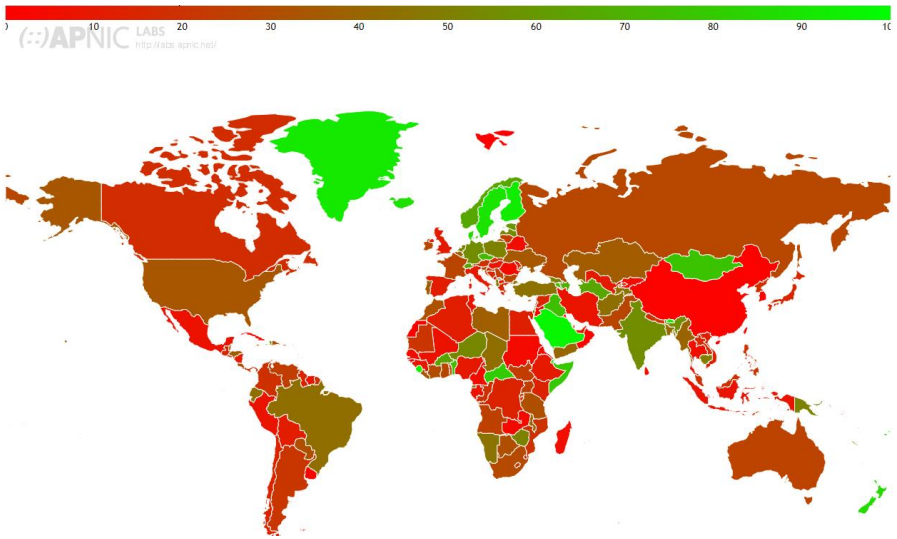
IPアドレスの分配を多く受けている**20社**のうち、**7社**が利用を開始。(テストを含む)



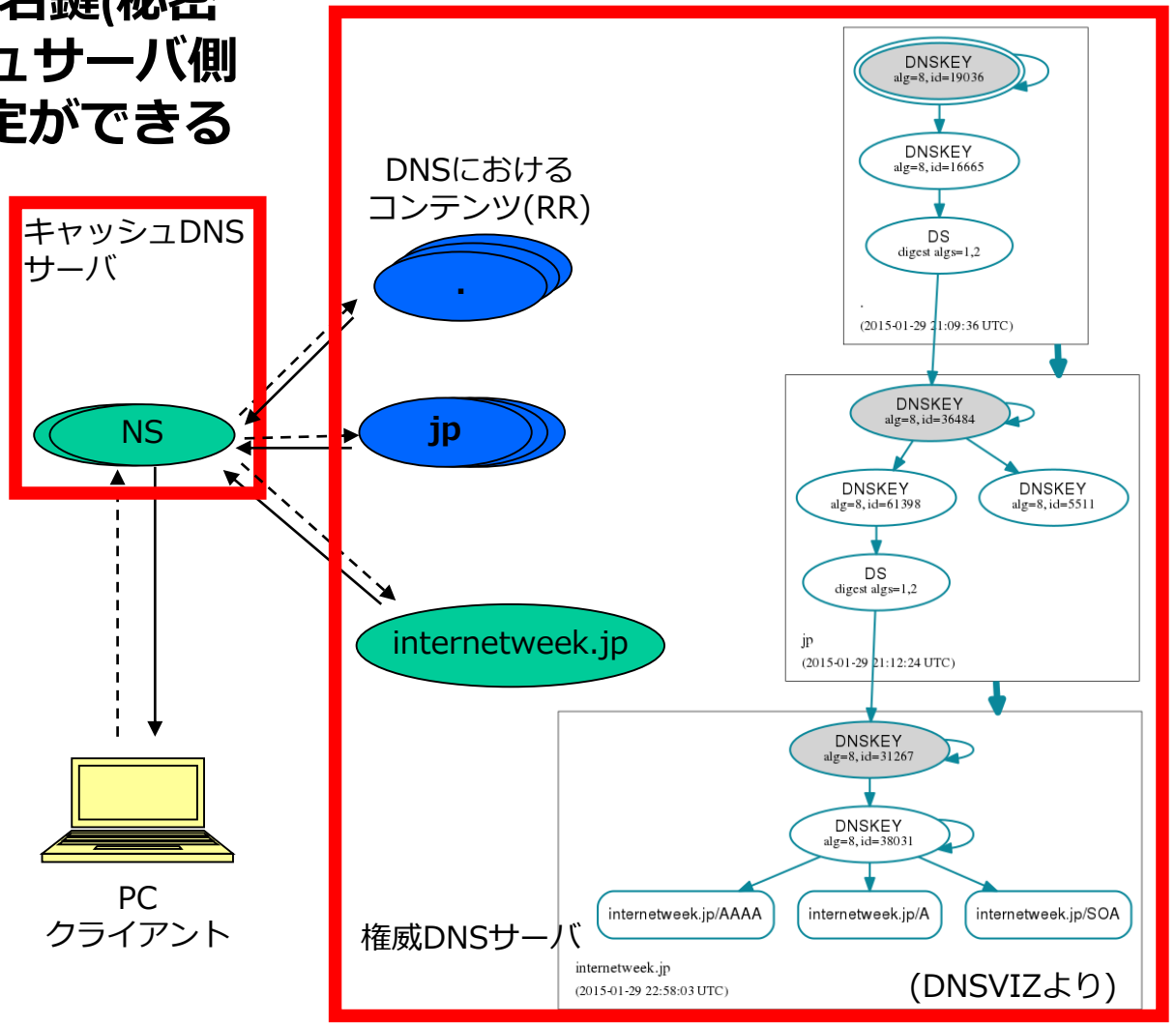
日本としてのルーティングセキュリティに関する状態把握が重要になっている

DNSSECについてーDNSSECとはー

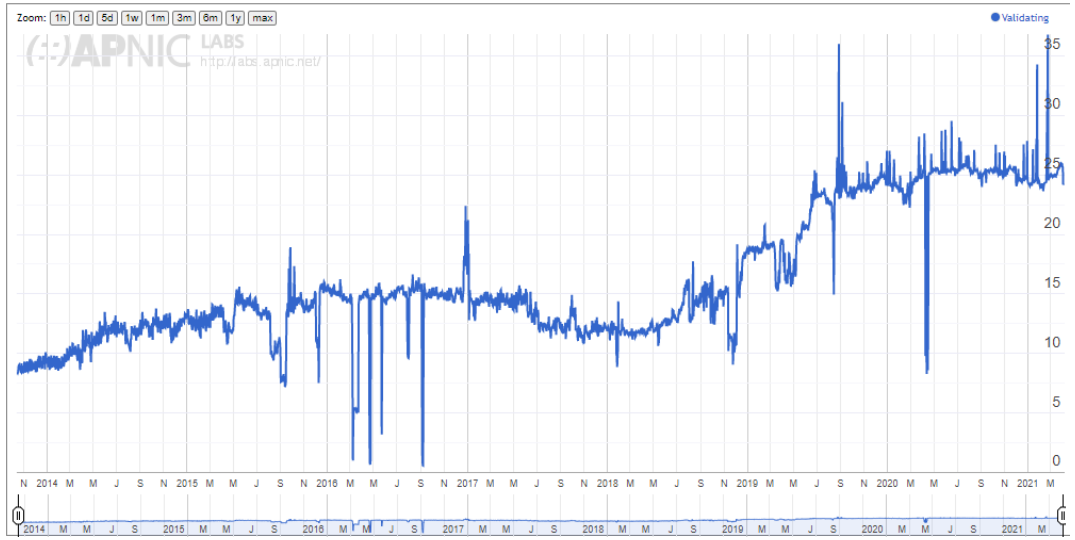
- 権威DNSサーバのコンテンツ(内容)を署名鍵(秘密鍵)で署名することによりDNSキャッシュサーバ側でそのコンテンツが正当であるかの判定ができる
- DNSのツリー構造の中に署名鍵情報(公開鍵)を登録することによりDNSの中に閉じて解決が可能
- 但しルートの署名鍵情報についてだけは別途正当性の確認が必要



世界のValidation状況 (APNIC Labsによる計測結果より)

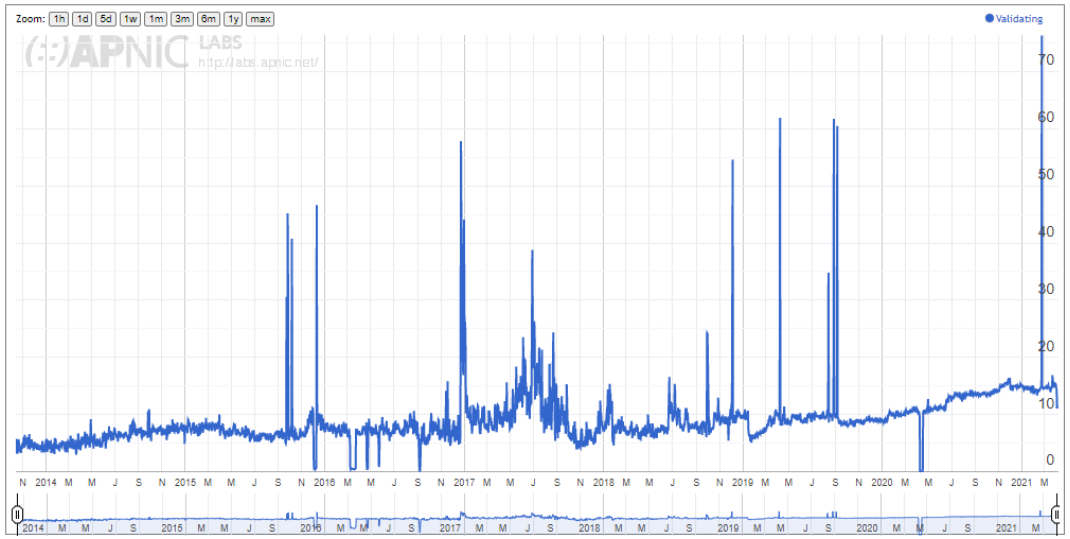


DNSSEC―日本の普及状況―



Use of DNSSEC Validation for World (XA)

- 25.32%



Use of DNSSEC Validation for Japan (JA)

- 14.83%

(APNIC Labsによる計測結果より)

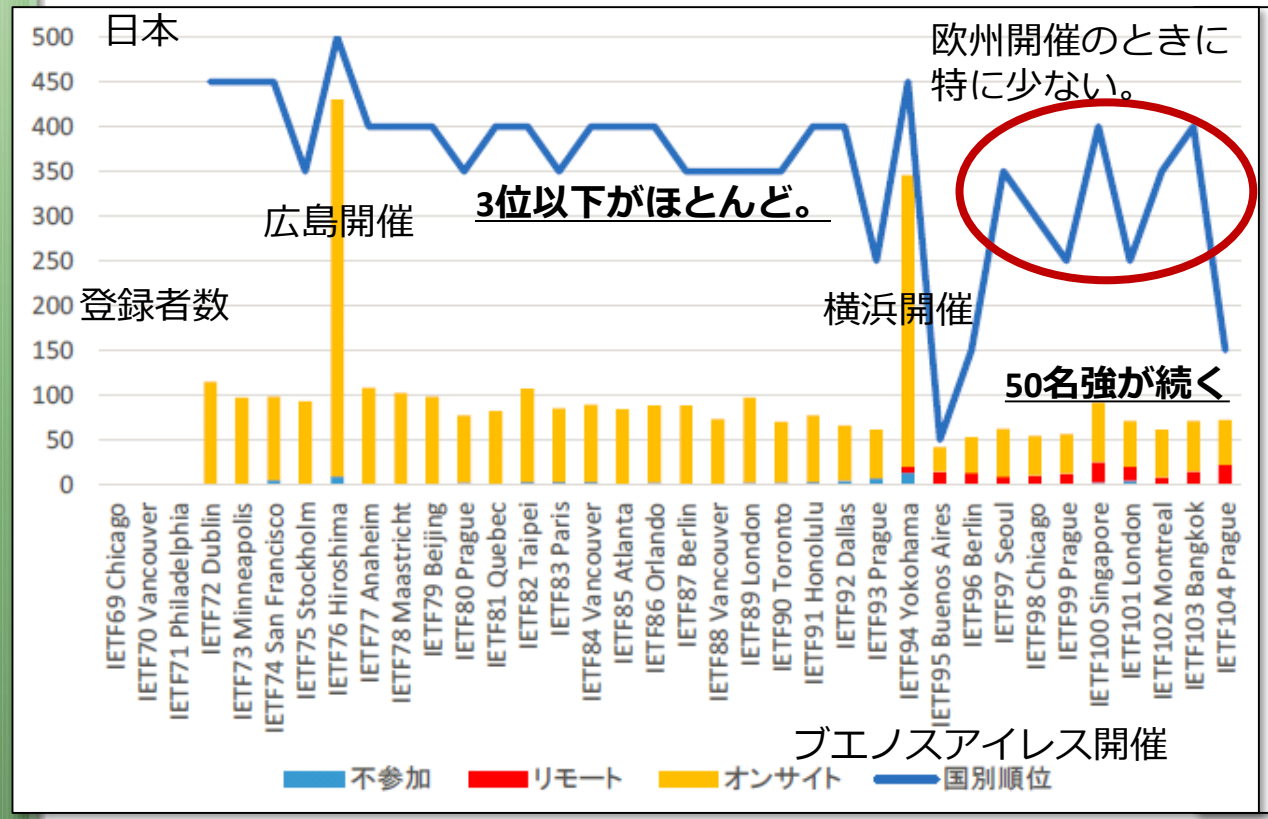
日本における普及率は著しく低い(Validationの普及)。

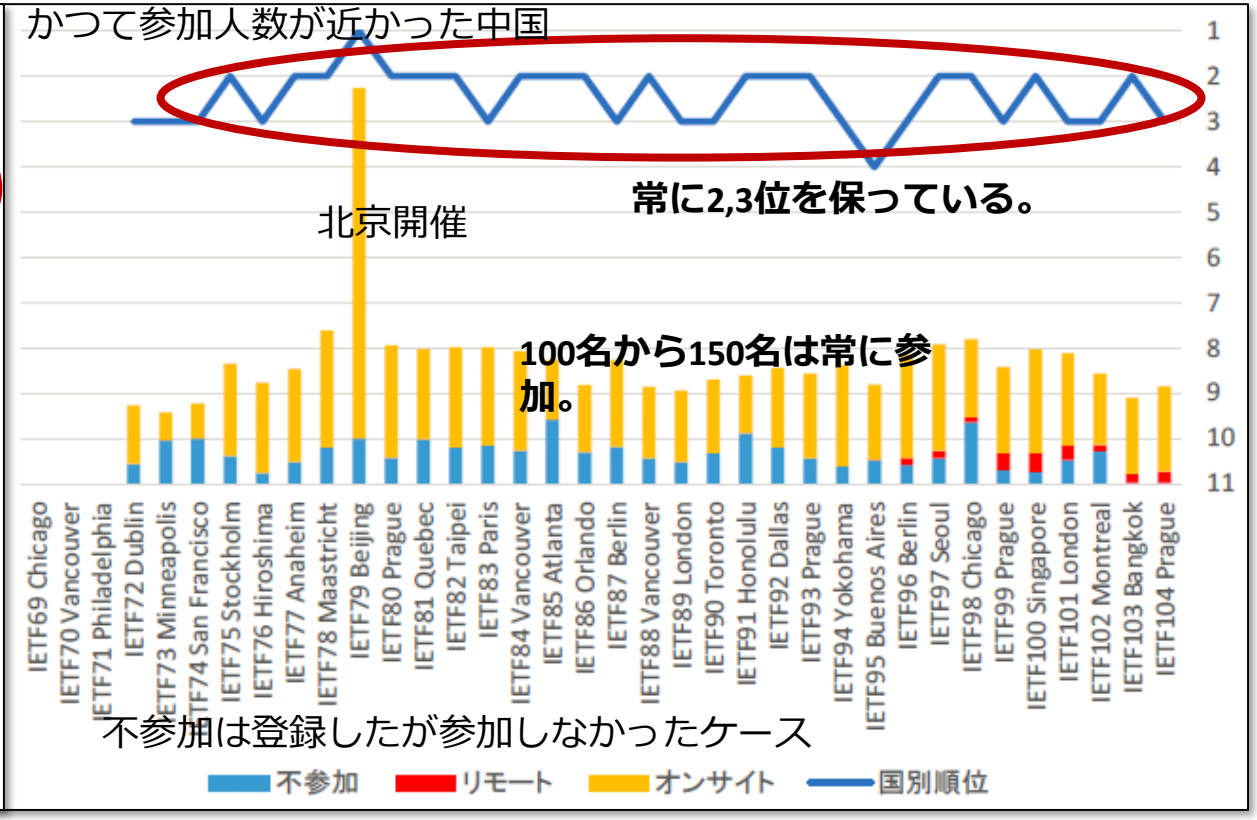
2. 国際的な標準化活動と情報通信アーキテクチャに関する技術動向の把握について

IETF 参加者数

- **日本は6年前から100名以下**

参加国の順位↓





IETF104全体報告,米谷嘉朗, IETF104報告会 より
https://www.isoc.jp/wiki.cgi?page=IETF104Update&action=ATTACH&file=IETF104%2Dyoneya%2Epdf

New IPの提案内容とIETF,IABの反応

- 2030年代のインターネットに向けて新たな要件を上げアドレスや追加ヘッダー、ネットワークの新たな仕組みをITU-T TSAG(Telecommunication Standardization Advisory Group)にてプレゼンテーション(2019年9月)
- IETFはITU-T TSAGからの「リエゾンステートメント」に回答。一つ一つの必要性を論理的に否定(2020年3月)。
- IRTF(IETFと関わるリサーチグループ)では2030年代のアーキテクチャに興味を持っているグループはある。

■時系列・出来事

2018年7月
- ITU IMT-2020/5G Workshopにて発表 (Richard Li氏, Huawei USA)

2019年9月
- ITU-T TSAGにて発表(Sheng Jiang氏, Huawei)
- Proposal
- IETFへのリエゾンステートメント

2020年2月
ITU-T SG13 Regional workshop for Africa にて発表(Macro Carugi氏, Huawei Research Contractor)

2020年3月
IETF, リエゾンステートメントに回答

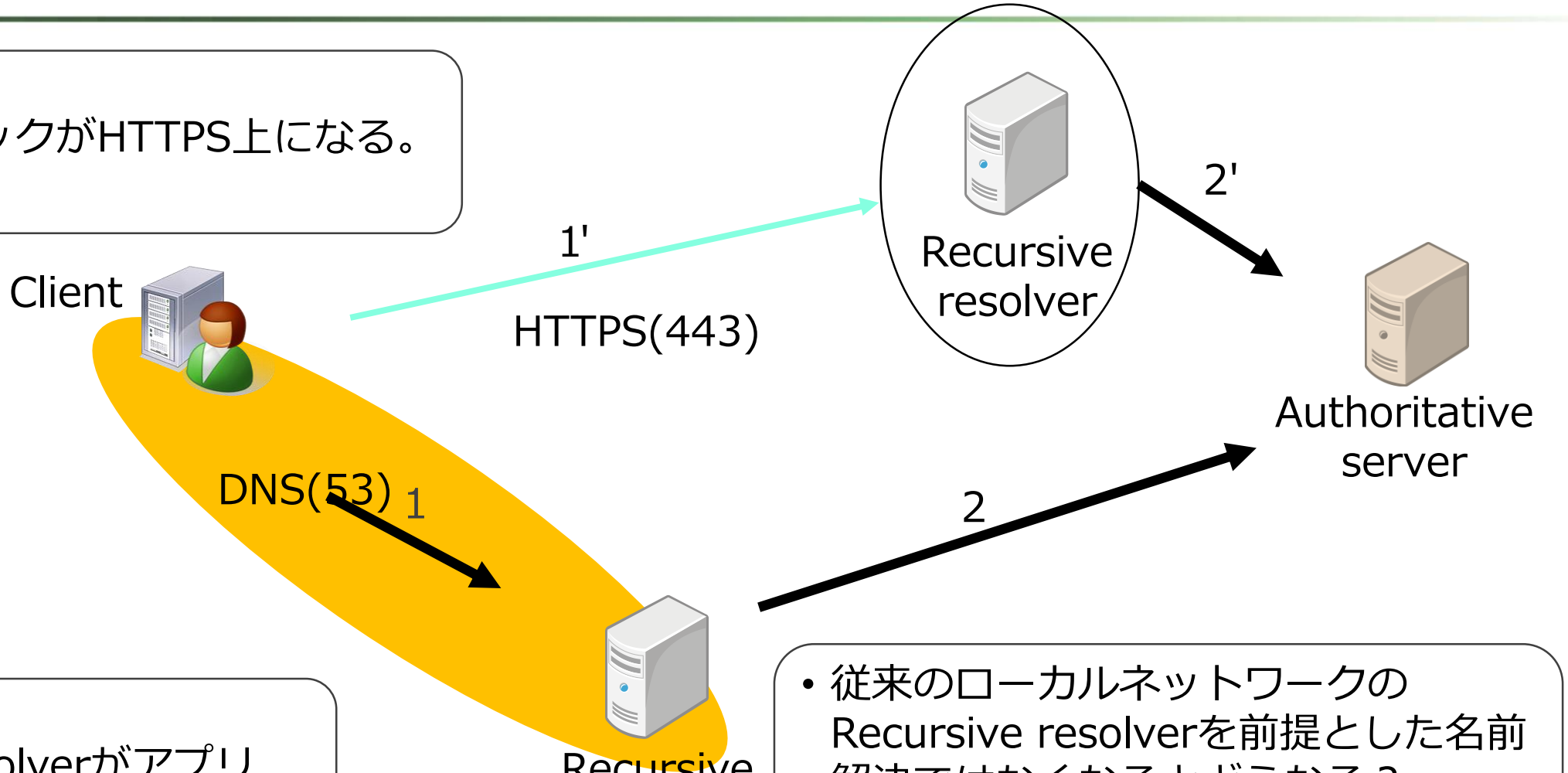
■New IPにおいて提案されている仕組み
- semantic address
- service oriented routing
- geographic address
- deterministic latency service
- user-defined request for network
- Inter-AS audit

■IETF,IABの反応(リエゾンステートメントへの回答)
- トップダウン型デザインである”New IP”の必要性を示すエビデンスはない。一つ一つの必要性を論理的に否定。
- 現在のデザインが「電話とコンピューター」のためというのは間違い。衛星についても昔から(RFC2488,1999)対応。
- ネットワークのリソース制御はRSVP,MPLS等すでにある。
- ITU-Tにはインターネットの仕様はIETFで提案するように要請。

■IETFにおける関連する動きと今後
- サイドミーティング network2030, 2019/11/20, IETF106, 88名参加
  IRTFで興味。会場では活動の継続に前向きの反応。

DoTとDoH - Encrypted DNS(Encrypted transport)

変わること１
DNSトラフィックがHTTPS上になる。
暗号化される。

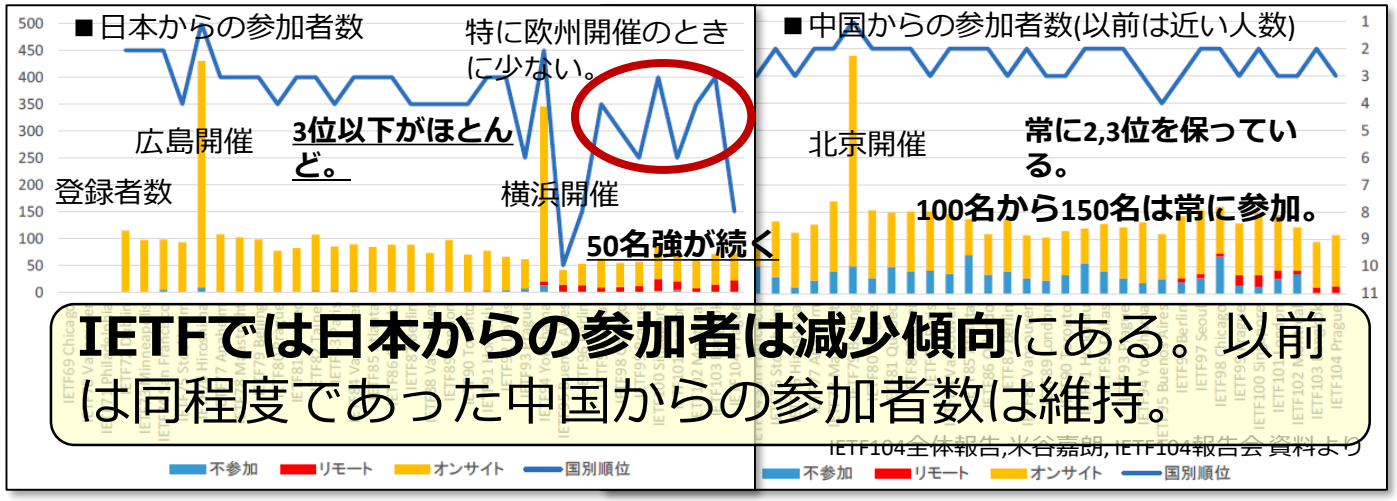


変わること２
Recursive resolverがアプリケーションによって選択される。

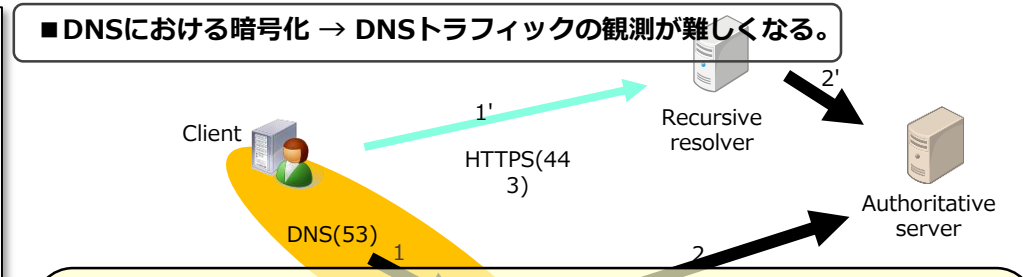
- 従来のローカルネットワークのRecursive resolverを前提とした名前解決ではなくなるとどうなる？
- アプリケーションはどういう仕様に？

2020年度にJPNICで実施した調査の背景

- 情報通信アーキテクチャが議論される国際的な標準化の場では、サイバーセキュリティにも関わる新しい仕組みが議論され標準が策定されている。標準を使ったサービス化が行われ我が国でも利用される。
- 標準化の場で、**2030年を見据えた情報通信アーキテクチャの議論が現れている**。Huaweiの「New IP」，ITU-Tにおける「Network 2030」，IETFサイドミーティングでの議論がある。
- 情報が自由に流通し、マルチステークホルダーによって自律的に運営される開放的なサイバー空間を維持・発展させていくためには、**国際的な動向や標準化動向の把握は必須**であるが…



IETFでは日本からの参加者は減少傾向にある。以前は同程度であった中国からの参加者数は維持。



施策が根本的に効果を持たない状況を避けるためには**アーキテクチャの動向を認識する人を増やしていく必要。**

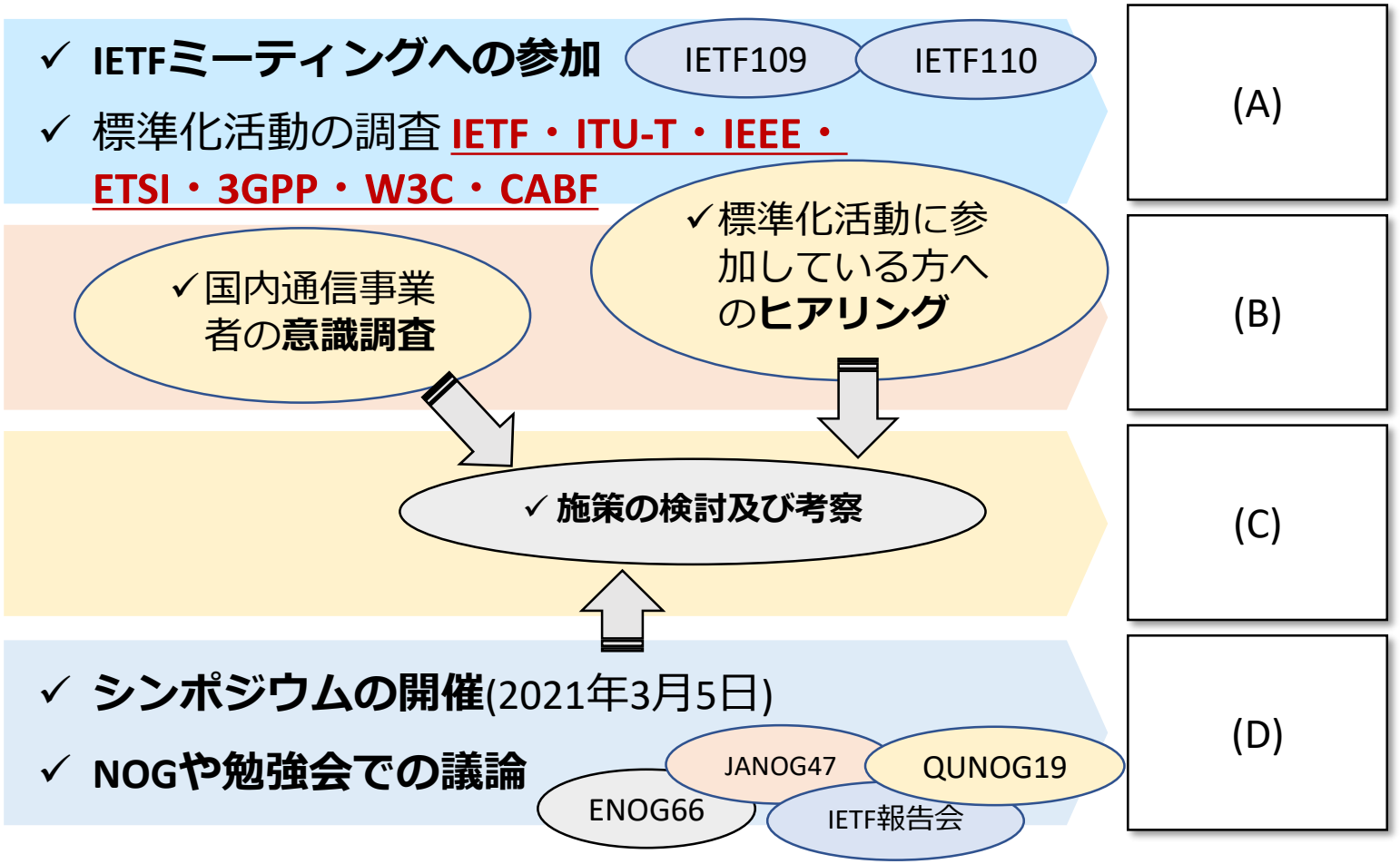
2030年を見据えた「Beyond5G推進戦略」の推進においては**情報通信アーキテクチャの視点で国際的な動向を主体的に把握し積極的に関与していくことが重要**であり、**国際動向を俯瞰した見方が必要**となる。そこで本調査では**基本的な調査として国際的な標準化団体を横断的に調査し、積極的な関与のための課題を洗い出す。**

当該調査の実施項目

本調査では、**実際に標準化会合に参加**すると共に標準化活動に参加している方への**ヒアリング**、**国内通信事業者への意識調査**、**周知広報**と議論のための**発表やシンポジウムの開催**を行った。

本調査の４つの実施項目

1. 情報通信ネットワークのアーキテクチャに関する国際的な議論状況
2. 日本からの参加の動向と国内議論活発化のための調査
3. 我が国からの参加者及び日本政府が取るべき施策に関する提言
4. 国内議論の活性化に資する周知広報の実施



(A) 調査内容と結果(概要)

標準化団体
- IETF
- ITU-T
- IEEE
- ETSI
- 3GPP
- W3C
- CABF

■調査内容(※)	①概要	○標準化団体の目的 ○議論の領域 ○対象とする技術 ○意思決定の方式 ○参加者の増減傾向等
	②動向	○コンセプトや方針 ○注目すべき技術 ○アーキテクチャの差異 ○サイバーセキュリティやプライバシーを確保する上で重要と考えられる技術
	③参加者の動向	○所属する国や組織の種別 ○最近の趨勢
■結果(概要)	○標準化団体の間で共通して見られた傾向 • **中国やインドが積極的に参加**してきている一方で**日本からの参加は全体的に減少** ○各標準化団体の違いや特徴 • **IETFが個人参加であることは他の団体と比べて特徴的** • 参加には組織会員である必要がある団体：ETSI・3GPP・W3C・CABF(パブリックフォーラムもある) • **将来の情報通信アーキテクチャについてはITU-T、ETSIにグループがあり**、IETFでは非公式もしくは研究の一環として議論される。 • **サイバーセキュリティに関する話題はすべての標準化団体で存在**している。**各々影響力の異なる分野**となっている。一部、複数の団体で扱われる技術がある。	

(※) 仕様書に基づく調査の内容

(A) 参加者数などの動向・趨勢や動き

団体	参加者数などの動向	趨勢や動き
IETF	• **IETFミーティングの全体的には1,000～1,200名前後**で推移	• 中国籍の企業からの参加者は**ルーティングエリアに多い**。
ITU-T	• **Study Group(SG)によって差がある**。だいたい一つのSGには300名から400名。	• SG13は全体で200名、日本は10名ほど。**SG17では日本10名のところ、韓国15名、中国30名。**
IEEE SA	• IEEE SAの参加資格となるIEEEは160ヵ国以上、40万人を超える会員がある。SA(標準化協会)の総数は不明。	• **日本は上位5ヵ国に入る**。しかしプレゼンスは落ちてきていてインドや中国がきている。
3GPP	• 参加者は**6,000名を超え中期的に増加傾向**にある。	• ここ10年ほどは**アジアが欧州、中東、アフリカを合わせた数に匹敵する程度に多い**。
W3C	• 2021年2月現在で**435会員**。オフィスは、オーストラリア、ベルギー、フランス、ブラジル、中国、韓国、日本にある。	• ブラウザベンダーなどの米国のIT企業が中心だが、**最近は中国の企業が積極的に参加している**。
ETSI	• 会員数は2020年12月時点で**755組織**。ドイツ、イギリス、フランスが多く、続いて米国他。	• **ETSI in China**に位置づけられる団体SESECが中国にある。また**ETSI in India**という位置づけられる団体SESEIがインドにある。
CABF	• 認証局メンバーは、米国(11)、中国(5)、スペイン(3)、オランダ(3)の順で多い。	• **Webブラウザの影響力が大きい**ため、認証局メンバーは**議論において不利な状況**にある。

中国・インドを含むアジアからの参加が目立ってきている団体が多い。ただし、標準化団体やその中のグループによって状況は様々であり国別の趨勢はその一端に過ぎない。

(A) 将来のアーキテクチャに関する議論

団体	将来のアーキテクチャの検討	現在のアーキテクチャとの差異
IETF	• **2019年9月頃にnetwork2030やNew IPの議論** • **FIPE(Future Internet Protocol Evolution)というサイドミーティング(非公式)も開催**された。	• **Semantic Addressingや衛星網との統合**など(New IPの要素技術に位置づけられる) • **ルーティングの新しい方式提案**など
ITU-T	• SG(Study Group)13で組成されたFG(Focus Group)で「2030年以降に向けた将来のネットワークに関するコンセプト」 • **ホログラフィック通信、Tactile Internet、デジタルツインズ、IIIoT（Industrial Internet of Things）などのユースケース。New IPはこれらの実現という位置づけにあった。**	• **Multi-Semantic Addressing**：複数のアドレス体系(IPv4, IPv6だけではなく、Service IDやContent IDなど他の識別子も含む)をサポート • **Deterministic Networking**：従来のパケットベースの通信につきものの遅延揺らぎを抑制できる技術 (**IETF、IEEEなどでも同様の検討はある**) • **Intrinsic Security for Privacy**：ユーザ情報とIPアドレスの情報を結びつけ、AS間での監視機能を強化するアイディアなど
IEEE SA	• IEEE SAでは**2030年といった検討は見当たらない。**標準化ではなく**学術的なグループとしてIEEEにおいてFuture Directions CommitteeにおけるFuture networksがある。**	—
ETSI	• **Non-IP Networkingグループ**によって行われている。	• IPヘッダーの処理をソフトウェアではなくハードウェアで行いやすくする。パケットをMACアドレス、**IPアドレス、ポート番号で扱うのではなくフロー表で扱う提案**も。
3GPP	• 2030年という将来の仕様を定める動きは見当たらない。**現行のRel-15に対して次世代Rel-16、次々世代Rel-17がある。**	• Rel-17では**衛星5G、ドローン運航管理、5Gマルチキャスト/ブロードキャスト等**の新たな無線アクセス網
W3C	• **2030年という将来の仕様を定める動きは見当たらない。**ウェブペイメント、デジタル出版、Web of Thingsといった検討がある。	
CABF	• **2030年という将来の仕様を定める動きは見当たらない。**	

いずれの団体においても新たな技術の取り組みはある。2030年という将来を視野に入れた動きはIETF、ITU-T、ETSIに見られる。

(A) 注目すべき技術とサイバーセキュリティに関連する話題

団体	注目すべき技術	サイバーセキュリティに関連する話題
IETF	• **IoT機器の安全なファームウェア更新技術やIoT機器の正当性検証技術等**の標準化(SUIT, RATS, TEE) • HTTP/3 (HTTP over QUIC) • **DNSプライバシーとDNSリゾルバ探索・選択**	• **DoTやDoH**、DNS通信の暗号化技術でユーザの意図しない形でローカルネットワークの管理外にあるDNSサーバに集中する構造 • **QUIC利用**のネットワークの監視への影響 • IoT機器の正当性検証の仕組みが議論
ITU-T	• New IPにも含まれる**遅延揺らぎを抑制する伝送技術**。モバイル網、固定網に加え、衛星網を取り込める**インテグレーション技術に位置づけられるMany Nets**。**3GPPでも検討。**	• 2018年頃技術的な議論であった**New IPは2019年に政治的な問題になり反対多数(SG13)**。 • **セキュリティに関する議論はSG17等でも**行われている。
IEEE SA	(IEEEは国際的に支部を持ち大規模な学会でもあるため、多くの研究活動が行われているが今回はそれらの調査は行っていない。)	• **802WGでは無線LANのWPA3**が2018年に策定され既に採用する製品がある。2019年に脆弱性が指摘されたが改修。
ETSI	• **IoTやM2M(oneM2Mと連携)**が挙げられる。IoTセマンティック相互運用(IoT Semantic Interoperability)	• **適格証明書**（Qualified Certificate）や**トラストサービス** • **TC CYBERにおけるサイバーセキュリティに関する標準化の系統だてたマップ**
3GPP	• ネットワークスライシング と3GPP標準のネットワークの組み合わせ • **衛星や成層圏における無人飛行体を利用した5Gネットワーク**	(5G以降のネットワークとサイバーセキュリティについては既に総務省 標準化戦略WGで検討が行われている。)
W3C	• ウェブペイメント、デジタル出版、ウェブと音声通信（API標準化）、メディアとエンターテイメント、Web of Things	• 多要素認証やセキュリティトークンなどのWebAuthn • セキュリティAPIや動作環境の整備を検討するWebAppSec • **Web上での決済方式に関するWeb Payments**
CABF	• ETSIにおけるトラストサービスと合わせて、CABFのガイドラインに基づく**Webのトラストについて継続的に注目すべき状況**	• S/MIME証明書ワーキンググループ • EVコードサイニング

すべての標準化団体において注目すべき技術とサイバーセキュリティに関連する話題がある。我が国における技術施策や制度に関係するものもあるが、調査を進めると中にはボランタリーな活動に支えられているものがある。

(B) 調査内容と結果(概要)

標準化団体
- IETF
- ITU-T
- IEEE
- ETSI
- 3GPP
- W3C
- CABF

■調査内容(※)	**①我が国からの参加者の動向**	○所属する組織の種別等の属性 ○参加の目的 ○最近の趨勢 ○実際の会合等への参加による知見
	②我が国からの参加にあたっての課題	○積極的かつ継続的により多く参加するために想定される課題を検討し整理
■結果(概要)	○標準化団体の間で共通して見られた傾向 • **参加者の減少、固定化や高齢化傾向**。新たな参加者の活性化に課題。 • 参加目的は、**動向把握、必要な標準の作成**、また**不必要な標準を作らせない活動** • **課題：戦略的な活動のためのノウハウ継承**、国内体制の整備、チームでの参加などの**体制、意識改革** ○各標準化団体の違いや特徴 • **個人での参加の場合、ボランタリーベース**になることが多く、**継続にはサポートを要する**。 • 課題：企業の国際標準を利用する意識作り、**活動成果のアピール、継続的なサポートを得る仕組みづくり**	

(※) 仕様書に基づく調査の内容

(B) 日本からの関与活性化に向けた課題

標準化団体	日本からの関与活性化に向けた課題
IETF	• 参加者の固定、高齢化。教育や、**若手向けの所属組織内部での活動も重要** • **設計工程での議論への参加**、政治力や提案力といった**標準化を進める上での突破力不足。** • **勉強会などボランティアベースで不十分な領域も**あり。**単なる勉強会や報告会だけではなく、議論や、実装を試すことができるような場づくり。**
ITU	• **標準化スキルの継承が課題。**複雑なルールがあり、外部から突然トップ（議長）にすえるというやり方は出来ない。経験が必要。若い人にはやりにくい場。 • **会社での成果の見せ方や本人のモチベーション維持の支援。**作った標準のアピールの補助、**日本や世界の産業にどのように役立ったかなどを解説するなどの支援**
IEEE	• **経験者によるOJTが必要。国内でシャドウコミッティを組織し、**議事的な国際会議を日本で行うなどして、**外交交渉能力の高い共有的な人材を育成。**寡占の構築でなく市場を作る視点の醸成。 • 学者の標準化活動のあり方にも対応が考えられる。ビジネスをしたい人と組み、技術的な美しさだけでなく、寛容さを持つこと、学術研究の要件に不必要な標準化を求めないなど
ETSI	• **ノウハウや動向調査などを共有する場の整備** • 国としての重点目標になりえる活動について、**ボランタリーベースの体制ではなく、支援を元に組織、体制の強化を図るべき。**
3GPP	• 通信事業者以外の企業の参加が増えており、ユースケース議論が進んでいる。日本における新たな層の巻き込み、やり方の模索 • **自分のドメインに閉じない検討ができる環境の醸成、協調の必要性。アプリケーションとネットワークの開発の協調。**
W3C	• 積極的に標準化活動に参加する人が減少傾向。**業務の範囲に限定した活動、予算の削減。** • グローバル市場に関れるような大企業であっても標準化には消極的。
CABF	• **若い参加者への会社の全権委任**の必要性 • 標準化結果の責任の所在の問題。民間企業としての厳しさ。業界団体が旗を振って議論を見ながら連れて行くことが望ましい。

参加者の高齢化や固定化が課題として挙げられ、ITUやIEEEにおいては標準化団体における経験を要することから、その支援が課題となっている。**各分野に閉じずに横断的な検討が必要という声も複数あった。**

ご意見を頂きたいこと

- **インターネットの基本的なサービスをより安全にする仕組みについて**
  - RPKI
  - DNSSEC

自律的に運営されるインターネットの基盤的なサービス（ルーティングとDNS）をどう守っていくか。

日本としてのルーティングセキュリティに関する状態把握は？

政府による普及促進(ガイドラインや調達基準・事業者への働きかけ・消費者への啓発活動)

- **国際的な標準化活動と情報通信アーキテクチャに関する技術動向の把握について**

オープンで自由に情報が流通しマルチステークホルダーによるインターネットの将来への関与の考え方、特にこれからの人にどうアプローチすべきか。

国際動向を把握して国内施策に役立ててていくための国内での活動は？

2030年のような将来のアーキテクチャに積極的に関与することについて