

2024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

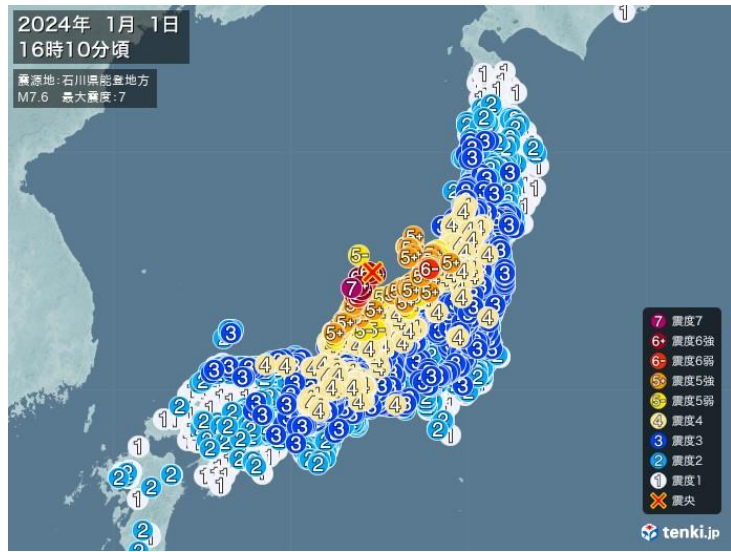
<tomoya.yoshida@ntt.com>



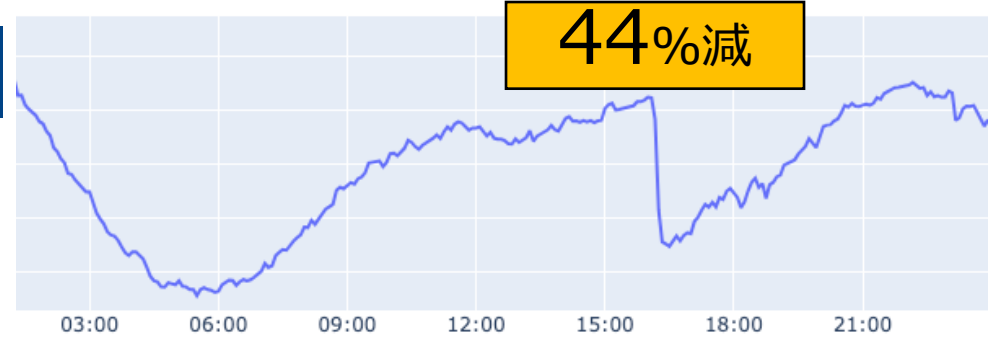
震災とインターネットトラフィック (1/1能登半島地震)



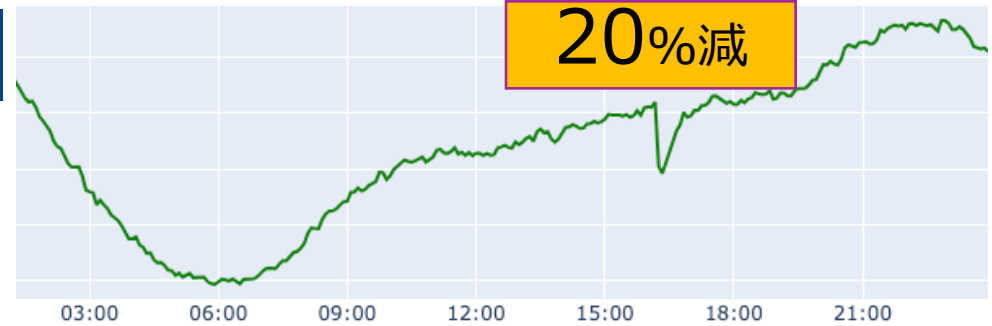
<海底ケーブル敷設船「きずな」>



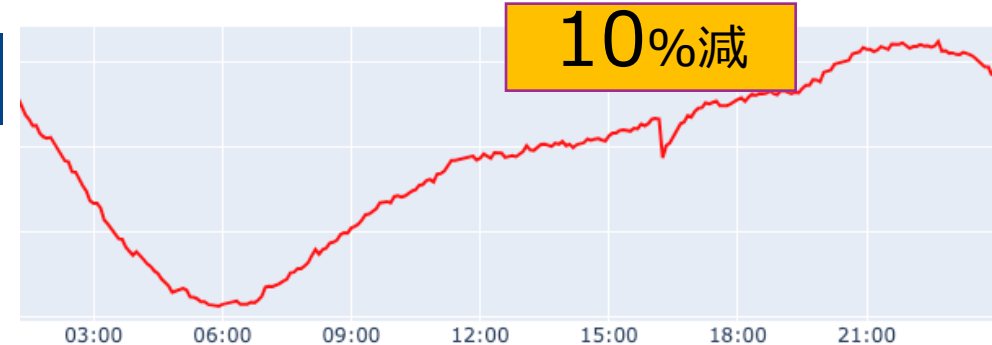
北陸



大阪



東京



画像出典:

<https://earthquake.tenki.jp/bousai/earthquake/detail/2024/01/01/2024-01-01-16-10-10.html>

https://www.docomo.ne.jp/info/news_release/detail/20240106_00_m.html

日本のインターネットの脆弱性分析に関する調査研究（信頼性をどう高めるべきか）

- ネットワークのトポロジはマップできた？が、コンテンツレイヤーやとの関係性が不明瞭
- 具体的なリスクや被害想定を仮置きし、マルチレイヤーでの課題抽出をしたい
- 具体的には、以下2つ

1. 首都圏直下地震 (関東圏の主要インフラに被害影響)

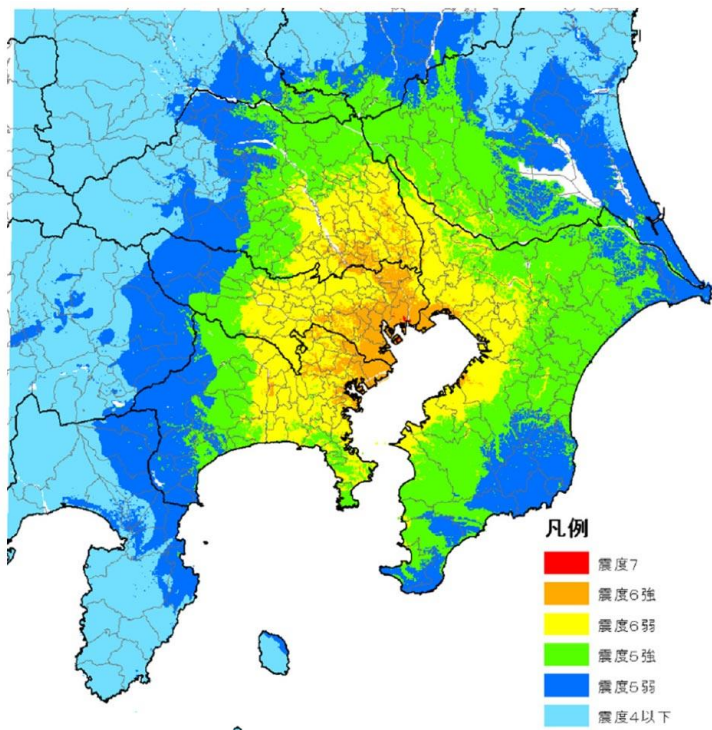
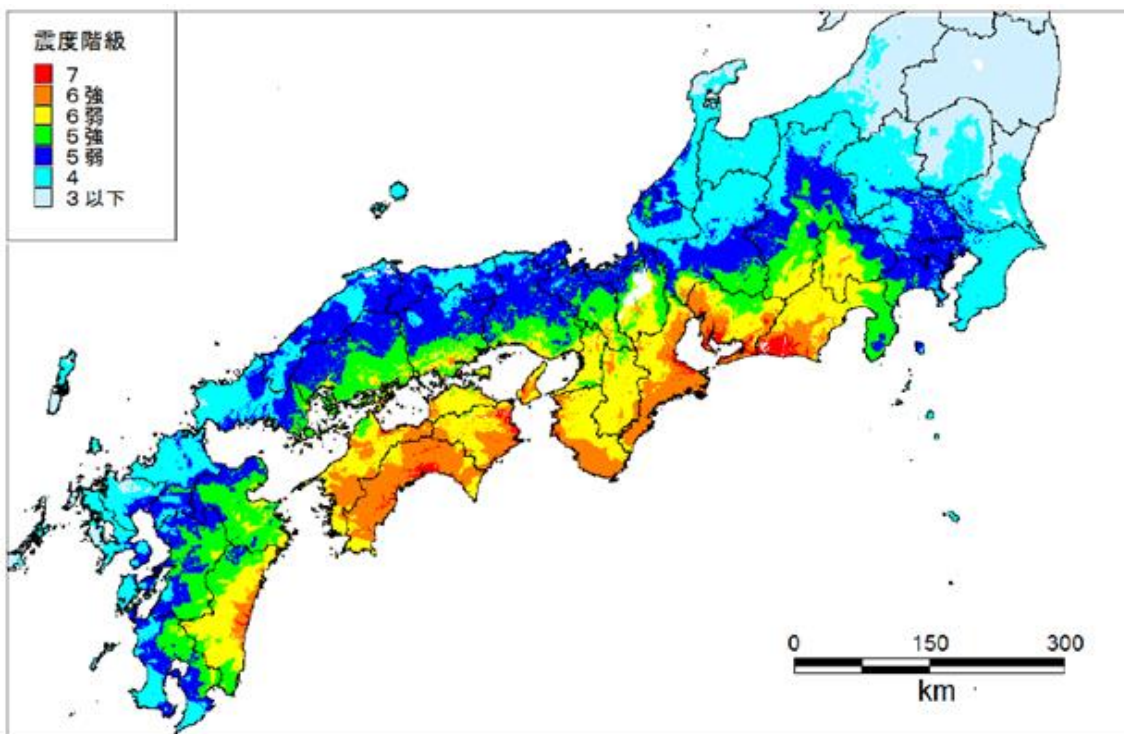


図 震度分布（都心南部直下地震）

2. 南海トラフ地震 (東海地域で名古屋に被害影響あり)



あくまで事例紹介であり、当該企業を非難するものではありません



【NEWS RELEASE】

2024年7月3日

株式会社KADOKAWA

ランサムウェア攻撃による情報漏洩に関するお知らせとお詫び

株式会社KADOKAWA（本社：東京都千代田区、取締役 代表執行役社長 CEO：夏野剛）は、現在発生している当社グループのシステム障害により、読者やユーザー、作家・クリエイター、取引先、株主・投資家をはじめ、関係するすべての皆様に、多大なるご心配とご迷惑をおかけしておりますことを深くお詫び申し上げます。

当社グループでは、「ニコニコ」を中心としたサービス群を標的として、ランサムウェアを含む大規模なサイバー攻撃を受けた事案が発覚した後、直に対策本部を立ち上げ、外部専門機関などの支援を受けながら、情報漏洩について鋭意調査を続けております。その最中、この攻撃を行ったとされる組織が、当社が保有する情報の一部を漏洩させたとする旨の主張があり、当該組織が公開した情報の検証を鋭意進めております。このたび自社内での調査により、下記情報については漏洩した可能性が高いと認識しましたのでご報告いたします。

<https://group.kadokawa.co.jp/information/media-download/1347/f4a4b93c03cb933c/>

デバイスに問題が発生したため、再起動する必要があります。
エラー情報を収集しています。再起動できます。

100% 完了



この問題と可能な解決方法の詳細については、以下を参照してください。

<https://www.windows.com/stopcode>

ネットに接続する場合は、この情報を伝えてください。

エラーコード: SYSTEM_THREAD_EXCEPTION_NOT_HANDLED

詳細は内部: 0x00000000

2024/7/19の出来事

7/19(金) 13:30頃 CrowdStrike Falcon(EDRソフトウェア) が導入されていたWindowsシステム(端末及びサーバ)にてシステムが再起動し“ブルースクリーン”へと陥る事象が世界中で発生

原因

CrowdStrikeが使用している設定ファイル(チャンネルファイル)の不具合

本設定ファイル(チャンネルファイル)は、CrowdStrike社のCloud環境内で管理されている

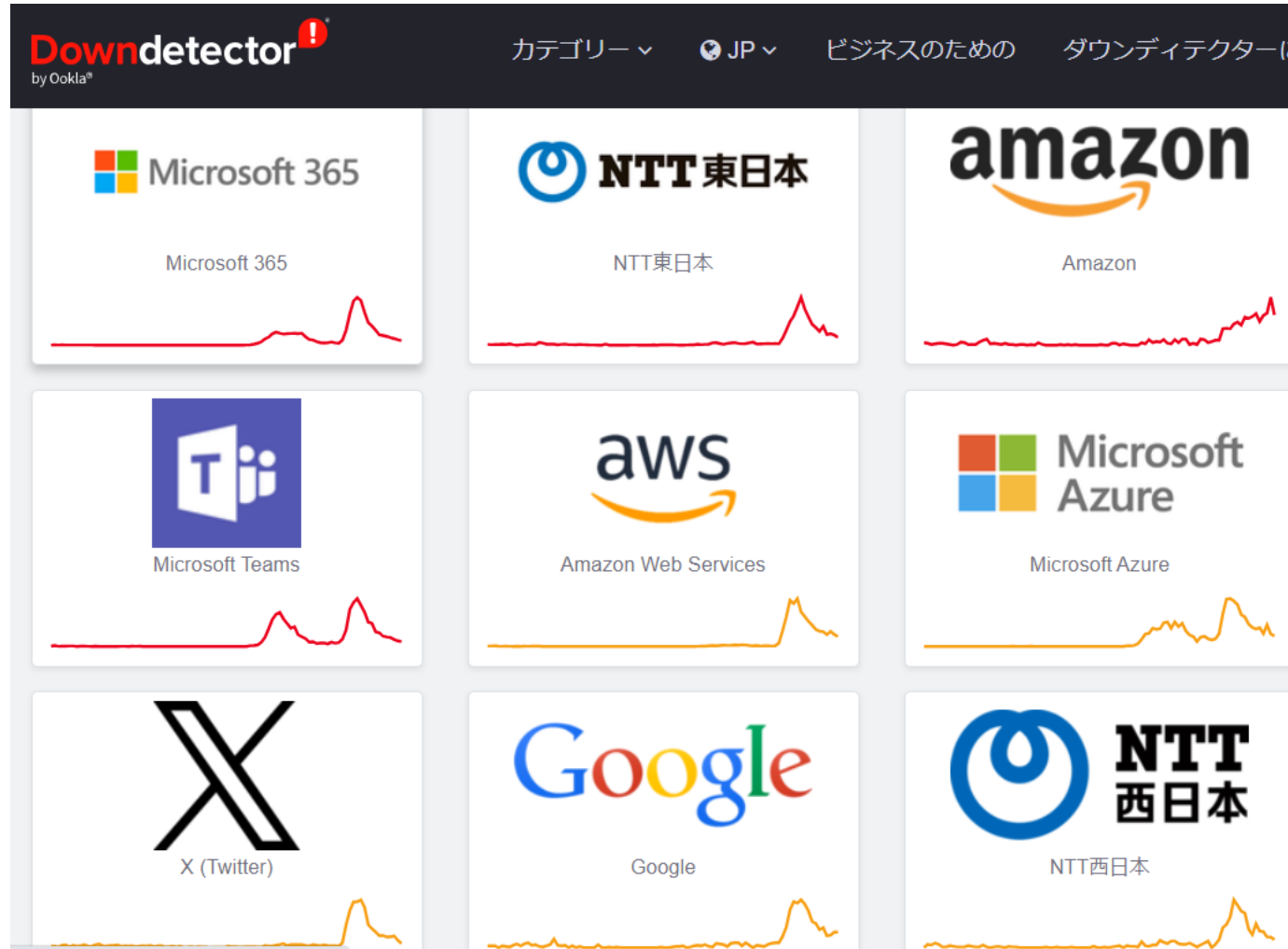
CrowdStrike社にて内容更新が行われ、更新されたチャンネルファイルがCrowdStrike Falcon導入端末にプッシュ送信されたことを契機に、不具合が発生

対処方法

当該チャンネルファイルの更新(切戻し)による復旧

CrowdStrike社がCloud環境内のチャンネルファイルを正常ファイルに置き換え(7/19金 14:27)

当日は、障害の共通項を見つけるのに苦労したが、いち早くNTTコムが総務省に報告し情報共有



石原総理大臣補佐官の航空自衛隊三沢基地及び米空軍三沢飛行場の視察

6月12日、石原宏高内閣総理大臣補佐官（国家安全保障に関する重要政策及び核軍縮・不拡散問題担当）は、航空自衛隊三沢基地及び米空軍三沢飛行場を視察しました。

1 石原補佐官は、航空自衛隊三沢基地において、亀岡北部航空方面隊司令官及び藤田第3航空団司令兼三沢基地司令との間で、三沢基地に所属する部隊や北部防衛のあり方、地元自治体との関係等について意見交換を行うとともに、F-35A戦闘機、E-2C/D早期警戒機、RQ-4Bグローバルホーク等を視察しました。

2 また、米空軍三沢飛行場では、ケンケル同飛行場副司令官との間で、三沢飛行場に所属する部隊の活動や在日米空軍の任務等について意見交換を行うとともに、同飛行場に所属するF16戦闘機や医療施設等を視察しました。



NoName057(16)
@Noname05716

We continue sending DDoS "gifts" to Japanese websites 🐱

t.me/noname05716eng...

✗ Liberal Democratic Party of Japan (closed by geo)
check-host.net/check-report/1...

✗ Mizuho Financial Group Financial Terms Glossary (closed by geo)
check-host.net/check-report/1...

✗ JR East Group Support - Transportation Company
check-host.net/check-report/1...

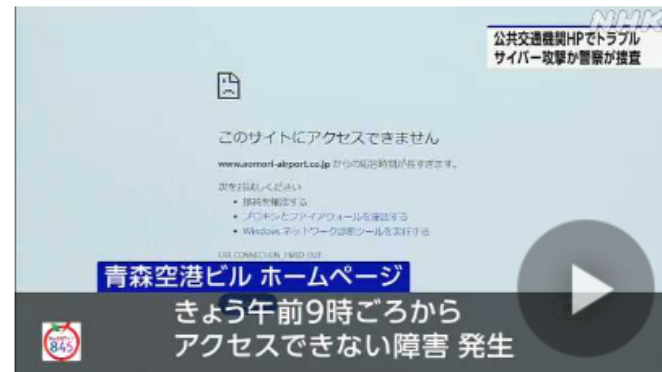
✗ JR East Group User Feedback Service
check-host.net/check-report/1...

✗ Aomori Railway Company
check-host.net/check-report/1...

<https://x.com/Noname05716/status/1813146578393190700>

青森県内の公共交通機関に 海外ハッカー集団がサイバー攻撃か

07月19日 20時28分



青森県内の公共交通機関のホームページにアクセスできないトラブルが相次いでいて、警察がサイバー攻撃を受けた可能性があるとして捜査しています。

県などによりますと、18日、海外のハッカー集団が県内の公共交通機関を名指ししたうえで、サイ

バー攻撃をしたという投稿をSNS上で確認したということです。

そして19日、県内の公共交通機関のホームページにアクセスできないトラブルが相次いでいることが確認されたということです。

このうち、青森空港ビルのホームページでは、19日午前9時ごろからサイトにアクセスできない障害が発生しているということです。

青森空港を発着する便に影響はないとしていますが、午後7時時点で青森空港ビルのホームページは復旧していません。

また、むつ市の下北交通によりますと、警察から会社のホームページがサイバー攻撃を受けていると連絡があり、アクセスできない状態が続いているということです。

<https://www3.nhk.or.jp/lnews/aomori/20240719/6080023161.html>



日米共同統合演習めぐり ロシア外務省が抗議 日本は反論

2024年10月12日 7時16分

ロシア外務省は、自衛隊とアメリカ軍が今月下旬から行う予定の大規模な実動演習をめぐって、在ロシア日本大使館に抗議したのに対し、日本側は受け入れられないとして反論した上で、日本周辺でロシア軍の活動が活発になっていることへの懸念などを伝えました。

自衛隊とアメリカ軍は、今月23日から来月1日まで、日米共同統合演習「キーン・ソード」を全国各地で行います。

[日米共同統合演習「キーン・ソード」めぐりロシア外務省が抗議 日本は反論 | NHK | ロシア](#)

← **ポストする**



NoName057(16) ✓

@Noname05716

Russia has sent a strong protest to Japan over joint exercises with the United States planned for late October–early November on Japanese territory, including in Hokkaido, close to the Russian borders. The Russian Foreign Ministry reported a warning to the Japanese embassy that such actions would entail “adequate countermeasures” aimed at protecting Russia’s sovereignty and strengthening its defense capabilities. Particular discontent was caused by the participation of non-regional NATO member states in the maneuvers, which, according to Russia, increases the threat and is unacceptable 🇷🇺

We punish russophobic Japan and remind that any measures directed against Russia can end badly 🐱

t.me/noname05716eng...

✗ International Economic Exchange Fund
check-host.net/check-report/1...

✗ International Development Center (IDCJ)
check-host.net/check-report/1...

<https://x.com/Noname05716/status/1845724395223781708>

キルネットによるへのDDoS攻撃 (2022)

DDoS攻撃 猛威



キルネットが投稿した動画(テレグラムから)

■サイト接続出来ず
「DDoS攻撃だ」と可能性を含め、詳細を確認している。監視体制を強化したい」。河野デジタル相は9日の記者会見でそう語った。

e-Govは、行政文書の開示請求や法令の検索ができるシステム。1日のアクセス件数は約780万件

親露ハッカー集団関与か

政府のオンラインシステム「e-Gov」や企業のホームページで、大量のデータを送りつけられてシステムがまひする「DDoS攻撃」が原因とみられる障害が相次ぎ、親ロシアのハッカー集団が関与を主張している。ロシアがウクライナ侵略を始めた時期から、同様の攻撃は全世界で5倍に増えたとの調査もあり、専門家は警戒を呼びかけている。(藤野平)

「世界で5倍」官民標的

標的にされた可能性がある省庁や企業

デジタル庁	行政情報・手続きサイト「e-Gov」
総務省	政治資金の届け出システム
文部科学省	非公表
宮内庁	ホームページが閲覧しづらくなる
地方税共同機構	地方税ポータルシステム「eLTAX」
名古屋港管理組合	ホームページが接続できなくなる
ミクシィ	会員制交流サイトmixi
ジェーシービー	JCBカードのブランドサイト
東京メトロ、大阪メトロ	運行情報などを紹介するホームページが接続しづらくなる
エヌ・ティ・ティ・イレゾナント	大手プロバイダーOCNのネットワーク
ドワンゴ	ニコニコ動画

6日午後10時過ぎから約40分にわたって、ホームページが閲覧できなくなった。民間企業にも被害が出た。信販大手「ジェーシービー」の一部のサイトが利用できなくなったほか、会員制交流サイト「mixi」も閲覧しづらいう状況になった。

■「官職妨害」
ハロシマはウクライナで犯罪を犯していない18日、本国政府全体に「官職妨害」のロシアを支持するハッカー集団「キルネット」が、通信アプリ「テレグラム」にマスク姿の人物と音声を投稿し、一連のシステム障害について、自分たちが「名古屋港管理組合」で

6日9日は、同庁を含め、総務省や文部科学省、宮内庁の4省庁の計23サイトが一時的に利用できなくなった。国内最大級の貿易港・名古屋港を運営する「名古屋港管理組合」では

サイバー攻撃の動向を分析しているNTTのサイバー専門家・松原実穂子さんによると、キルネットは、サイバー攻撃によって自分たちの政治的主張をアピールする集団「ハクティビスト」の一派とみられる。DDoS攻撃は、サイトが利用不能になるなど被害が見えやすく、ハクティビストに選ばれやすい手段とされている。

キルネットの活動は今年に入ってから確認されるようになった。5月には米英やドイツ、イタリアなどが10か国に「サイバー戦争」を宣言。翌月にはロシアのアナログ以上の政府機関や空港などの電子サービスに標的にしたと主張している。松原さんは「キルネットが日本を初めて標的にしたと見ている。ロシアを支持

出展：2022年9月13日 読売新聞夕刊記事より

被害あり

デジタル庁	行政情報・手続きサイト「e-Gov」
総務省	政治資金の届け出システム
文部科学省	非公表
宮内庁	ホームページが閲覧しづらくなる
地方税共同機構	地方税ポータルシステム「eLTAX」
名古屋港管理組合	ホームページが接続できなくなる
ミクシィ	会員制交流サイトmixi
ジェーシービー	JCBカードのブランドサイト
東京メトロ、大阪メトロ	運行情報などを紹介するホームページが接続しづらくなる
エヌ・ティ・ティ・イレゾナント	大手プロバイダーOCNのネットワーク
ドワンゴ	ニコニコ動画

被害なし

OCNバックボーンでの防御施策により被害影響なし

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

2024年トラフィック動向

- ブロードバンドトラフィックは、再度復調傾向に（増加→鈍化→増加）
 - ここ1年でダウンロードは**18.1%増（2023年 17.4%）**
 - ここ1年でアップロードは**15.9%増（2023年 11.0%）**
 - 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
- OCNも2024年に前年よりも増加傾向に
- モバイルトラフィックも以前同様に回復基調、ここ最近では**15%**程度の伸び
- 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）
- **ゲームのダウンロード**による通信量影響が年々顕著になっている
- 1日の最大瞬間風速は、全体的には収まってきている傾向（**平準化**）
- IPv6トラフィックは増加傾向だが、世の中のIPv6対応の鈍化もあり依然IPv4が多い
- **イベント時の急激なトラフィック増加変動**は定常化しつつある（2022年Wcupが最高）
- **HTTPからHTTPSへ**の動きは着実に進んでいる（TCP80は**6%**に）

OCNトラフィック推移(2020/2/25~)

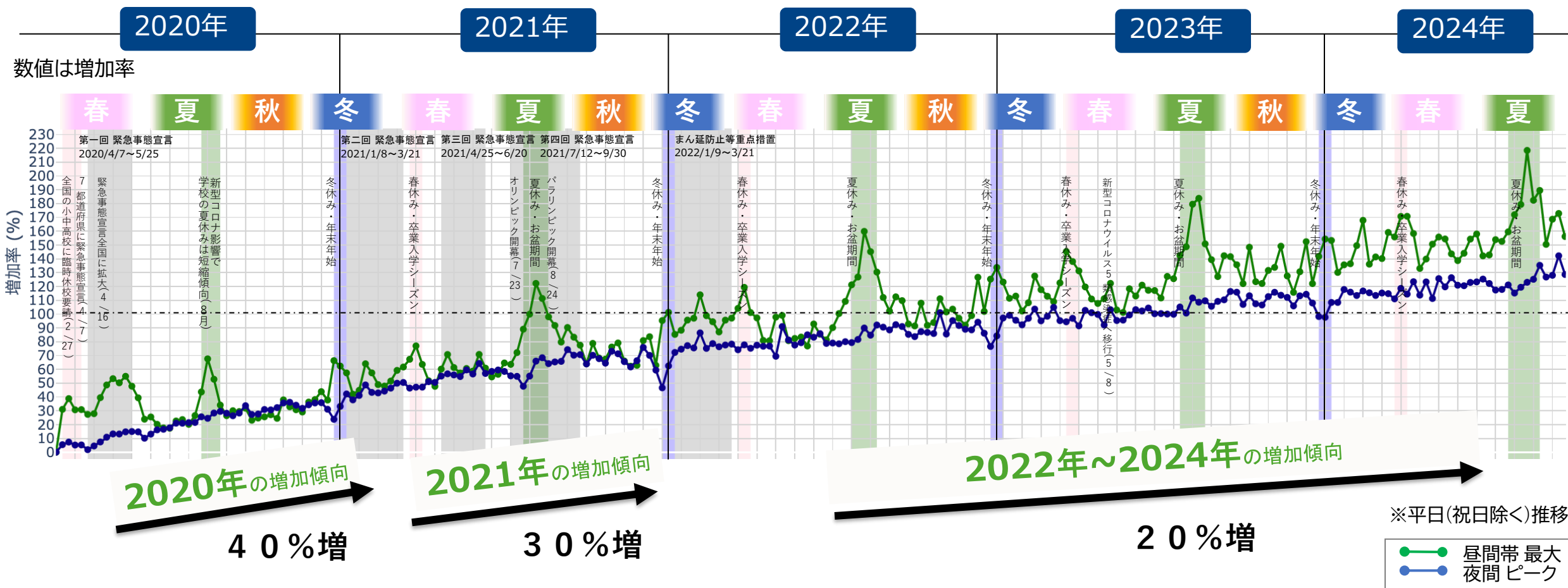
昼間帯ピーク
夜間ピーク

の増加率
の増加率

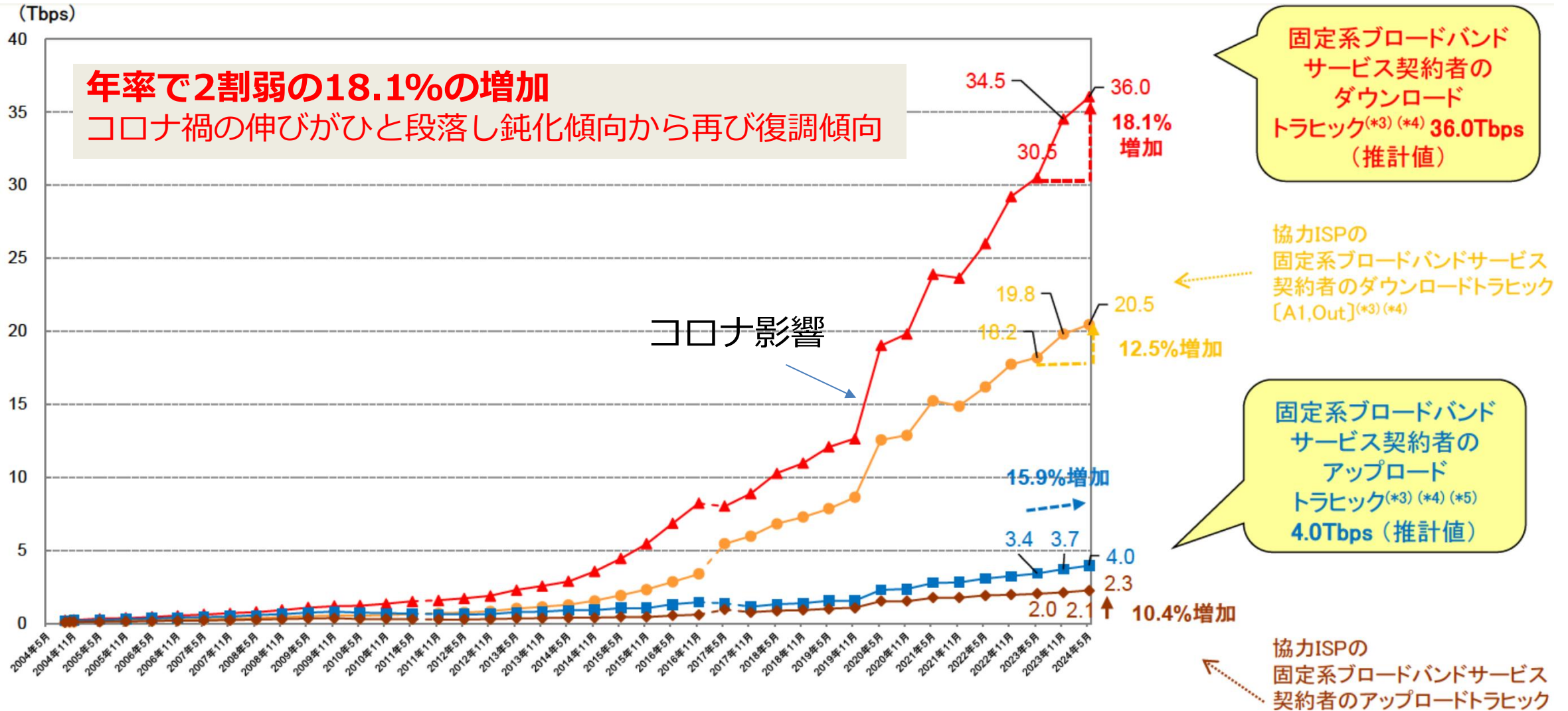
通常4年で倍→3年

最大瞬間風速はLIVE中継とゲームDL

リモワ回帰

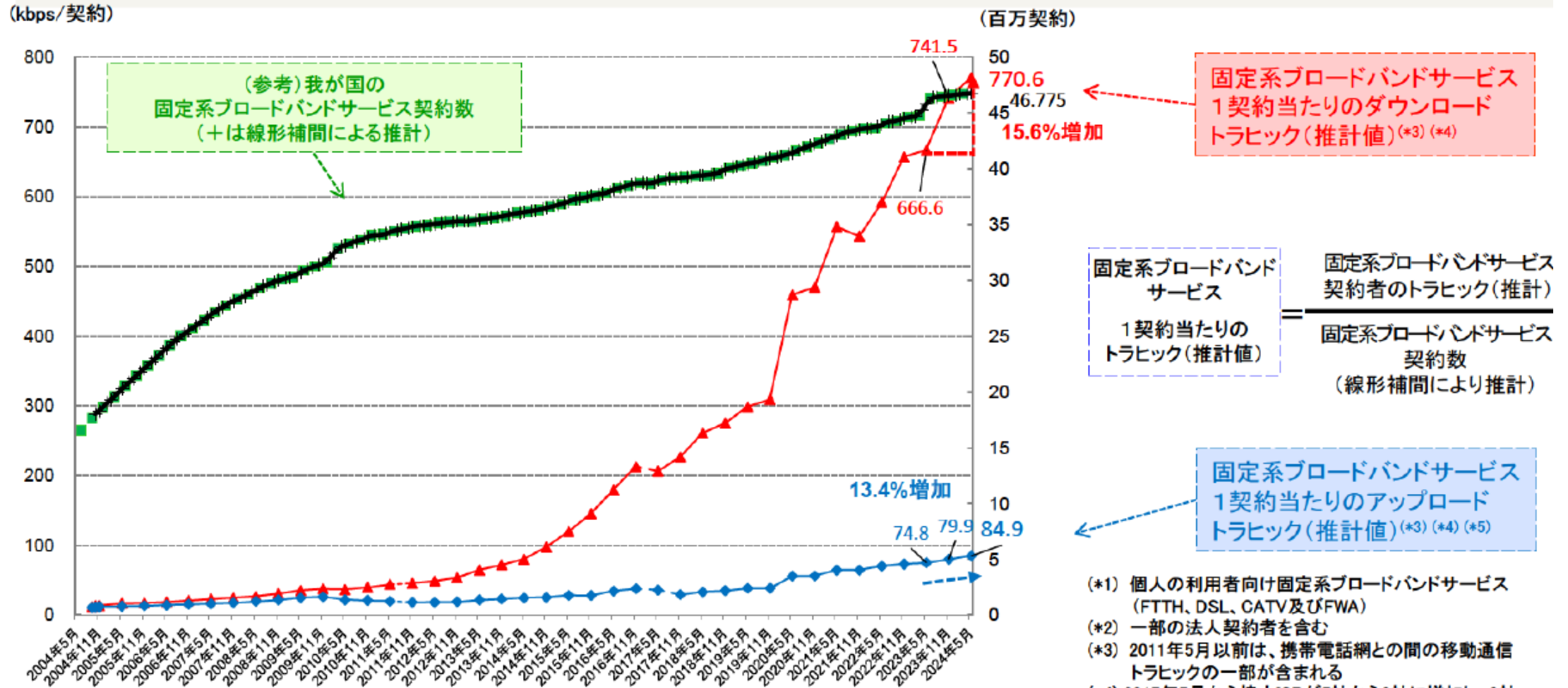


日本国内のトラフィック推移



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」 2024年8月9日

日本国内のトラフィック推移



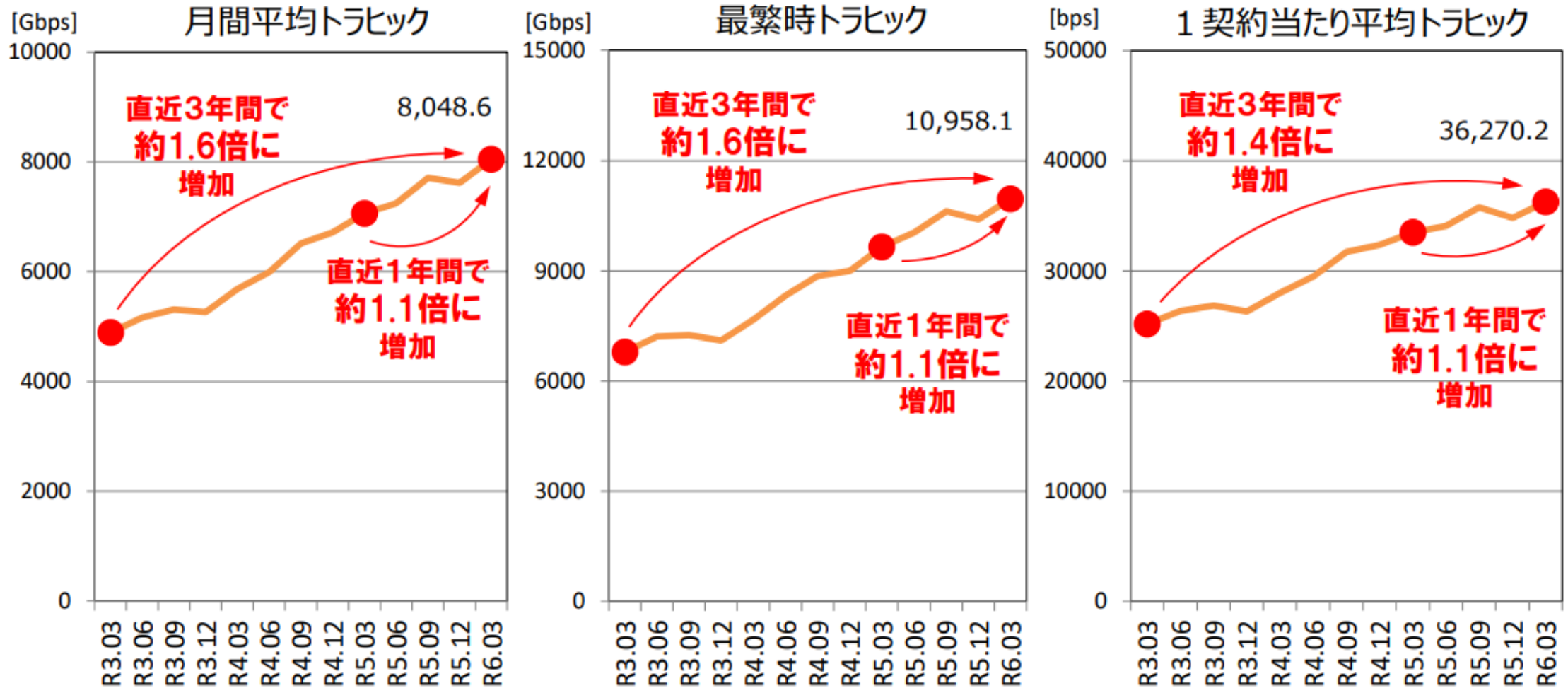
「電気通信サービスの契約数及びシェアに関する四半期データの公表(令和5年度第4四半期(3月末))(令和6年6月28日総務省報道資料)」より計算 (https://www.soumu.go.jp/menu_news/s-news/01kiban04_02000243.html)

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」 2024年8月9日

- (*1) 個人の利用者向け固定系ブロードバンドサービス (FTTH、DSL、CATV及びFWA)
- (*2) 一部の法人契約者を含む
- (*3) 2011年5月以前は、携帯電話網との間の移動通信トラフィックの一部が含まれる
- (*4) 2017年5月から協力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計値としたため、不連続が生じている。
- (*5) 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

移動通信トラヒックの推移

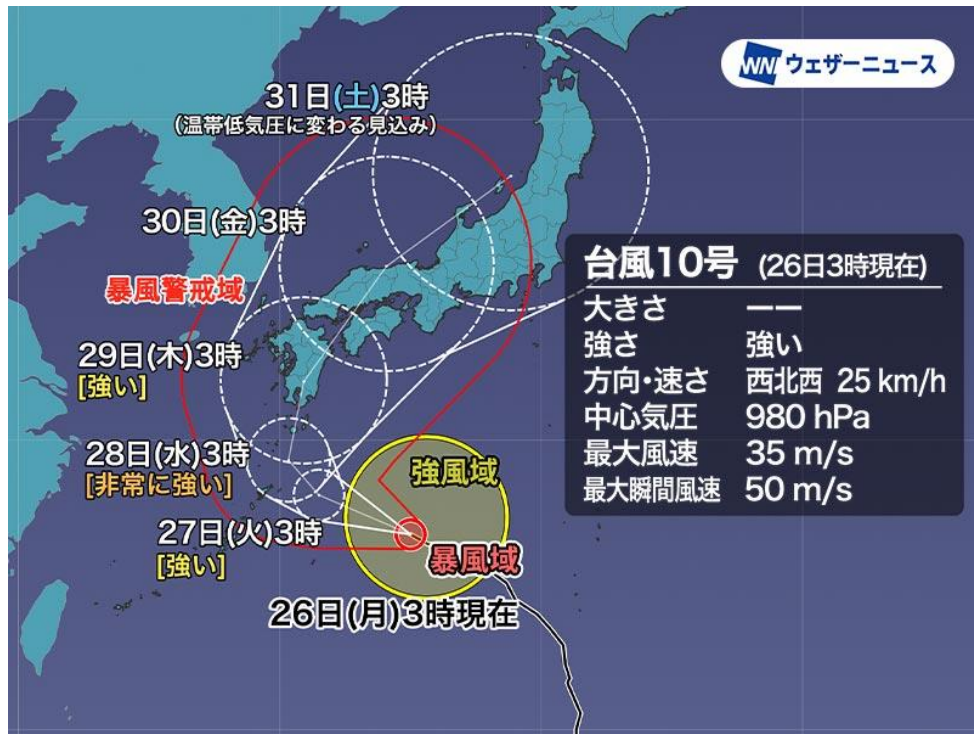
固定通信トラヒックの傾向と類似 年約**1.1倍**の伸び



出典：総務省「我が国の移動通信トラヒックの現状（令和6年3月）」

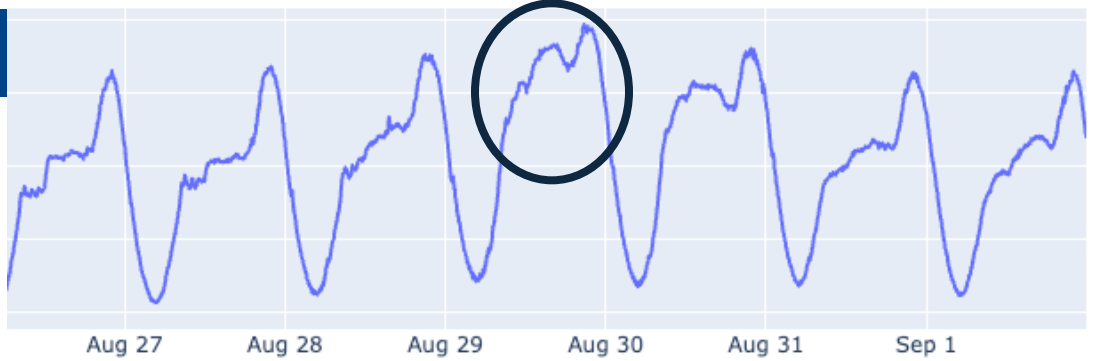
気象影響とインターネットトラフィック

2024年8月29日に九州に台風10号上陸、OCNの**九州エリア**の通信量が急増
鉄道運休もあり在宅者多数で通信帯域ひっ迫するも、臨時の即時対応等で回避

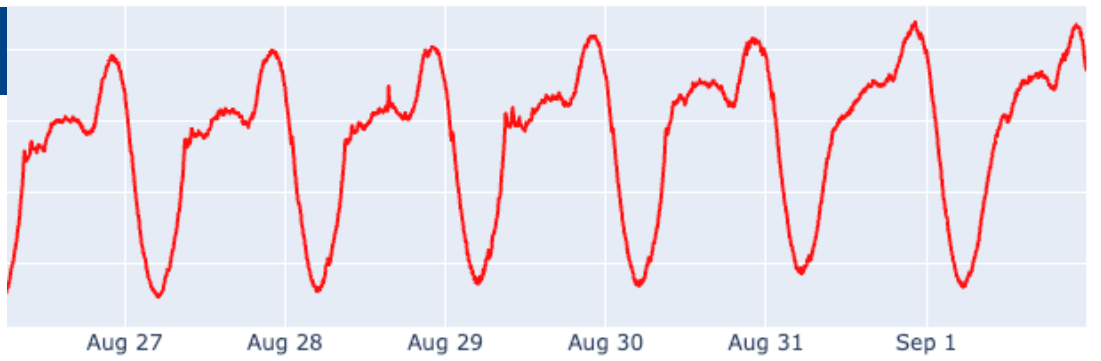


台風10号上陸
8/29 8時頃

九州



東京



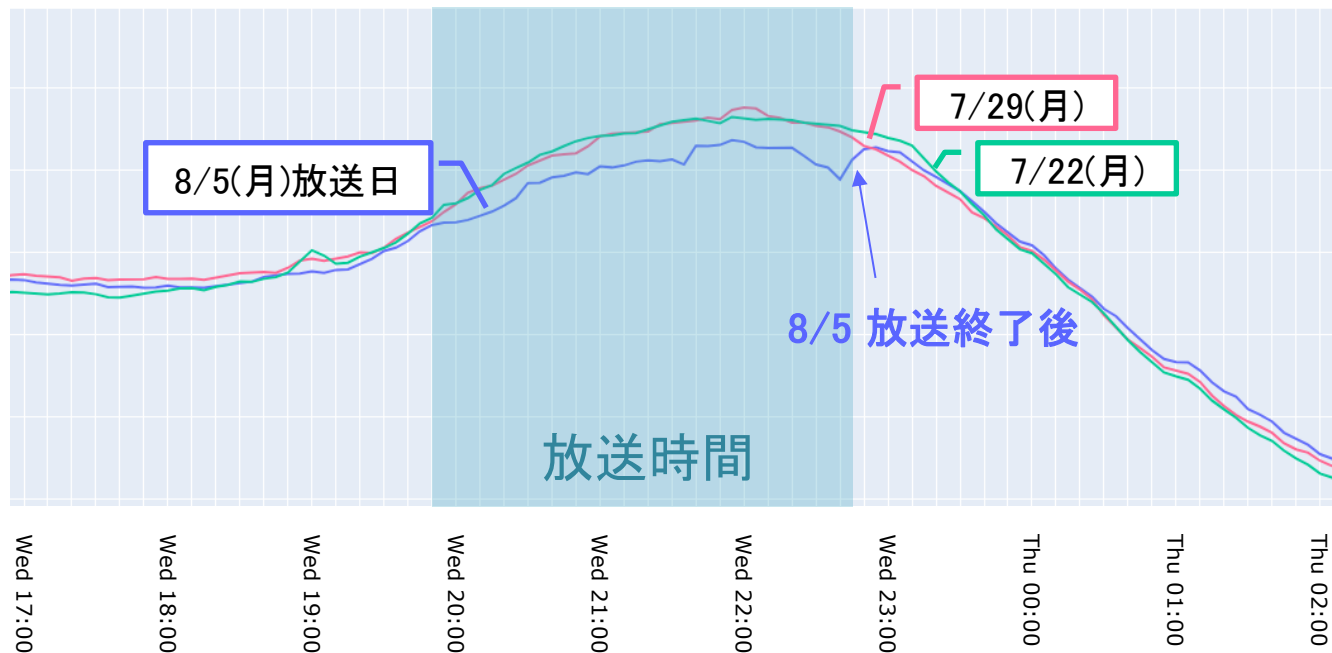
画像出典: ウェザーニュース
台風10号(サンサン) 進路が西寄りに変化 上陸後は西日本各地を通過のおそれ
<https://weathernews.jp/s/topics/202408/260025/>

パリ五輪：テレビ放送とインターネットトラフィック

視聴率の最高：8月5日NHK(総合)

「バレーボール男子準々決勝・日本×イタリア戦」

20時の放送開始～放送終了の間ネット通信量が減少
多くの人々がテレビ放送を通して試合を観戦していた



■バレーボール男子準々決勝・日本×イタリア
NHK(総合) 8月5日 19:50-20:55分の平均世帯視聴: 17.0%
NHK(総合) 8月5日 22:00-22:45分の平均世帯視聴: 23.1%

(引用元: ビデオリサーチ(関東地区、平均世帯視聴率)https://www.videoor.co.jp/tvrating/past_tvrating/sport/olympic-summer/paris2024/01.html)



画像出典: NHK NEWS WEB
<https://www3.nhk.or.jp/news/html/20240805/k10014537901000.html>

ネット通信量の最大値

パリ五輪 > 東京五輪

※予選ラウンド「日本×ドイツ戦」
日テレ放送があったが、夕方の時間帯
ということもあり通信量が増加した

2020年 TBS日曜劇場 と インターネットトラフィック (過去の再掲)

7/19~



21:00~

https://www.tbs.co.jp/hanzawa_naoki/

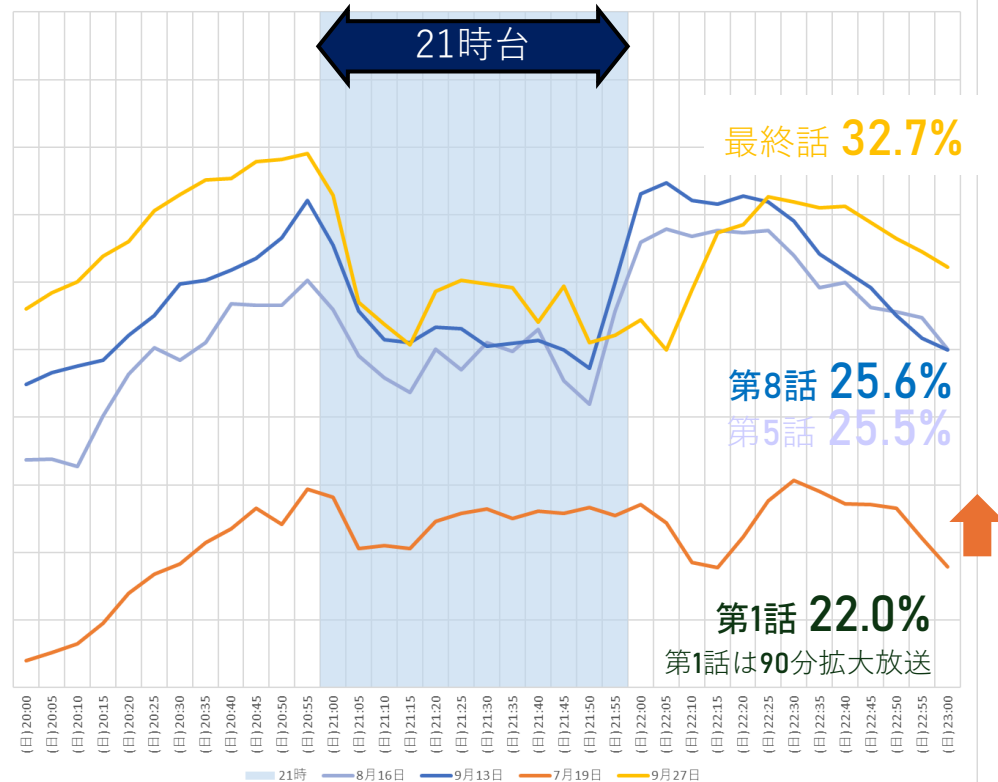
10/11~



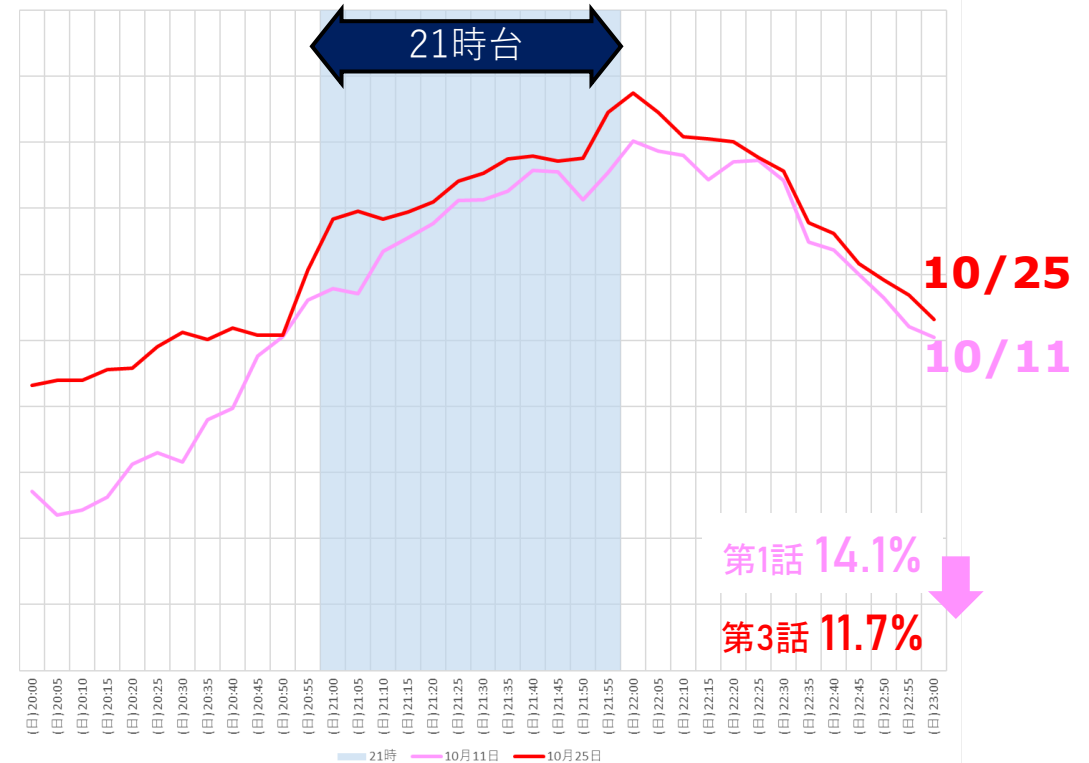
20:00~23:00

https://www.tbs.co.jp/kikenna_venus/

日曜劇場[半沢直樹]とインターネット



日曜劇場[危険なビーナス]とインターネット

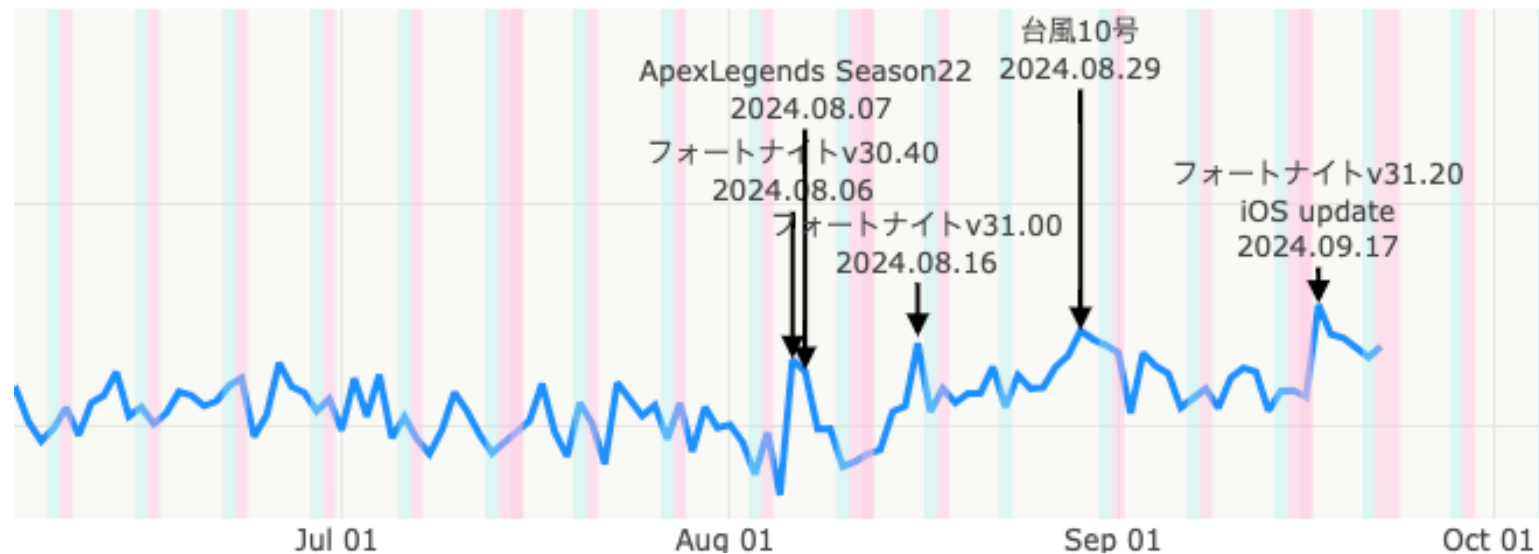
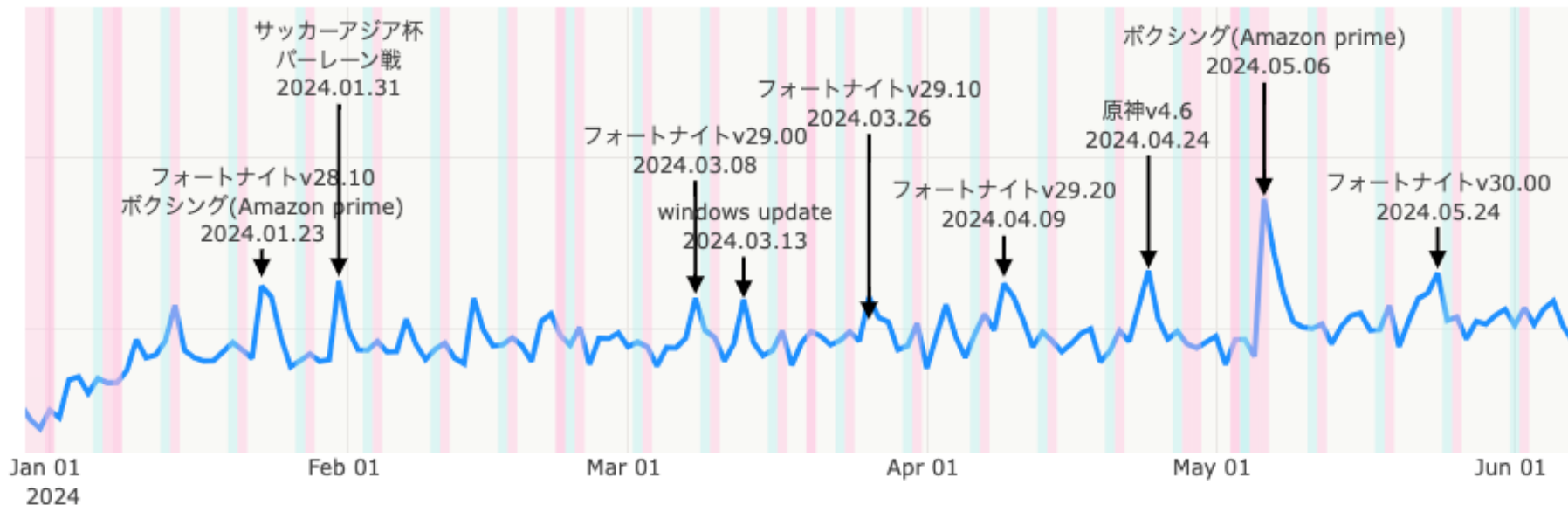


企業規模別 テレワーク実施率の推移 [正社員ベース]

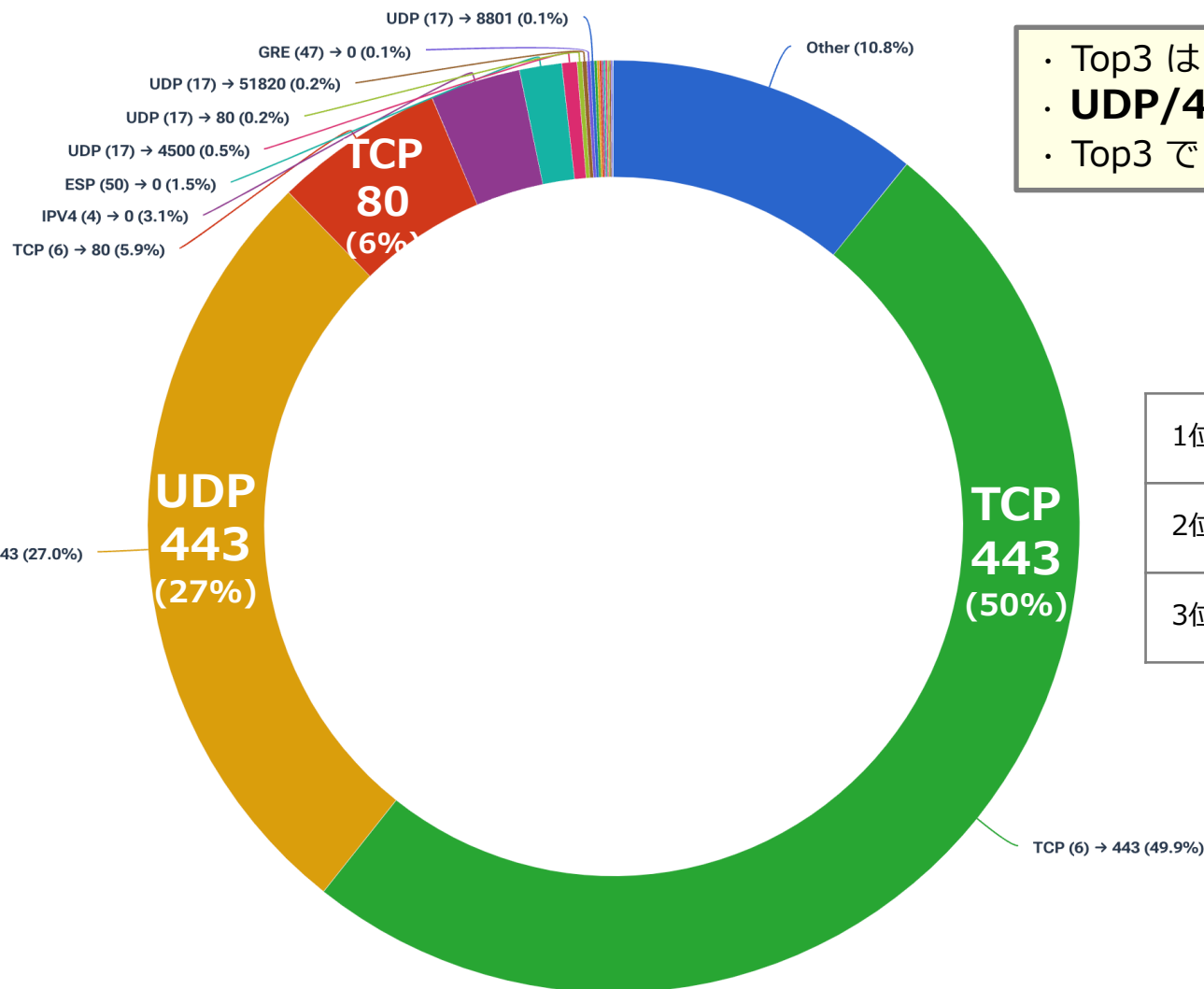


パーソル総合研究所による、第九回・テレワークに関する定量調査より
公開日：2024年8月30日（金）

特徴的な日ごとのOCNトラフィック変動（2024）



プロトコル分析 (2024年8月)



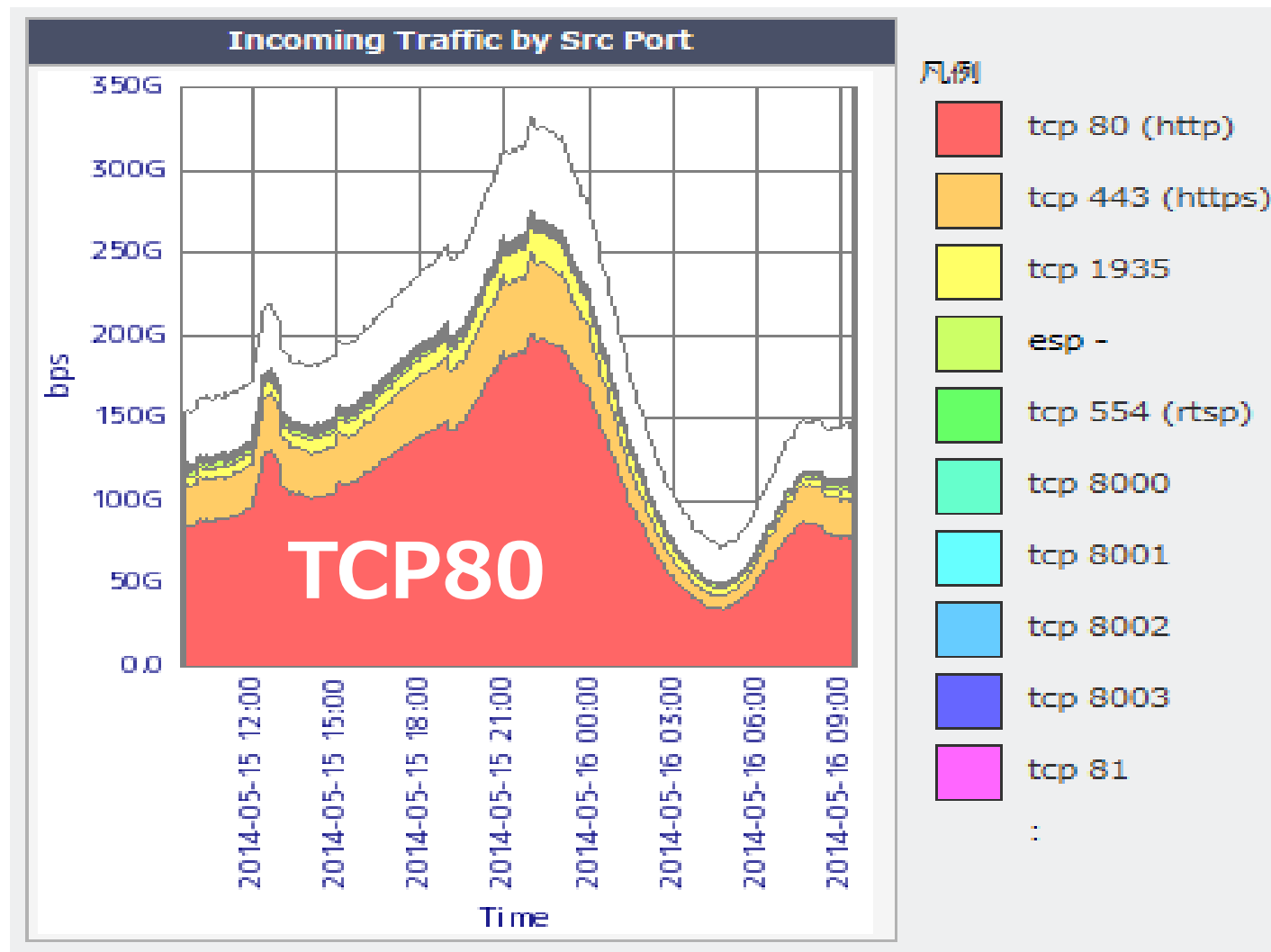
- Top3 は **TCP/443, UDP/443, TCP/80** ⇒ 直近5年傾向変わらず
- **UDP/443** は増加傾向 ⇒ **QUIC (HTTP/3)** の普及
- Top3 で **トラフィック全体の8割以上を占める**

	2019年度	2020年度	2021年度	2022年度	2023年度	2024年度
1位	TCP/443	TCP/443	TCP/443 (60%)	TCP/443 (55.5%) ↓	TCP/443 (48.2%) ↓	TCP/443 (49.9%) ↑増
2位	UDP/443	UDP/443	UDP/443 (27%)	UDP/443 (21.1%) ↓	UDP/443 (26.4%) ↑	UDP/443 (27.0%) ↑増
3位	TCP/80	TCP/80	TCP/80 (10%)	TCP/80 (9.7%) ↓	TCP/80 (7.6%) ↓	TCP/80 (5.9%) ↓減

10年前の2014年

約8割はTCP80

2014年～2016年、80->443へのTransitionが顕著に



プロトコル分析 (2023年度 vs 2024年度)

- 多少の順位の入れ替えはあるが、**Top20まで大きな変化はなし**
- Top20圏外からの唯一のランクインは、7位の「UDP/80」

Protocol	Source Port Number	Average Gbits/s	95th Percentile Gbits/s	Max Gbits/s
Total				
TCP (6)	443	HTTPs		
UDP (17)	443	HTTPs		
TCP (6)	80	HTTP		
IPv4 (4)		主にIPIP (MAP-E)		
ESP (50)		IPsec		
UDP (17)	4500	IPsec		
UDP (17)	8801	Zoom?		
GRE (47)		IPsec		
UDP (17)	3480	O365系?		
UDP (17)	51820	WireGuard		
TCP (6)	183	OCBInder?		
TCP (6)	8080	HTTPs		
TCP (6)	110	POP3		
TCP (6)	995	POP3S		
UDP (17)	3478	STUN		
TCP (6)	993	IMAPS		
UDP (17)	3481	通話系?		
UDP (17)	4501	IPsec		
UDP (17)	12346	(不明)		
UDP (17)	53	DNS		
TCP (6)	7000			
UDP (17)	16393			
UDP (17)	2426			

2023年10月

Protocol	Source Port Number	Average Gbits/s	95th Percentile Gbits/s	Max Gbits/s
Total				
TCP (6)	443	HTTPs		
UDP (17)	443	HTTPs		
TCP (6)	80	HTTP		
IPv4 (4)		主にIPIP (MAP-E)		
ESP (50)		IPsec		
UDP (17)	4500	IPsec		
UDP (17)	80			
UDP (17)	51820	WireGuard		
GRE (47)		IPsec		
UDP (17)	8801	Zoom?		
TCP (6)	183	OCBInder?		
TCP (6)	8080	HTTPs		
UDP (17)	3478	STUN		
UDP (17)	3480	O365系?		
UDP (17)	4501	IPsec		
TCP (6)	995	POP3S		
TCP (6)	110	POP3		
TCP (6)	993	IMAPS		
UDP (17)	3481	通話系?		
UDP (17)	12346	(不明)		
UDP (17)	53	DNS		
TCP (6)	7000			
UDP (17)	16393			
UDP (17)	2426			

2024年8月

UDP/80
Top20圏外から
唯一ランクイン

Top10

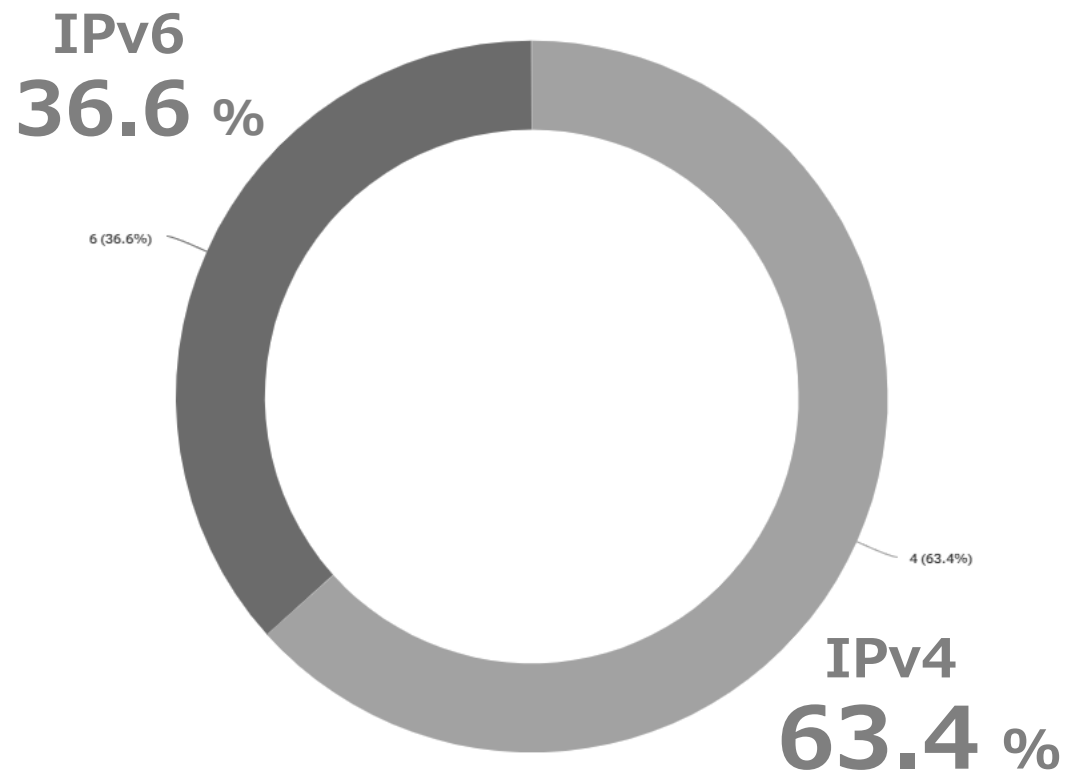
Top20

IPv4/IPv6比率 (2023年度 vs 2024年度)

- IPv4 : IPv6 = **6 : 4** ※ 「IPv4が6割」… 字面的にややこしい
- 1年前と比較すると、**IPv6比率は2%上昇** 微妙?!

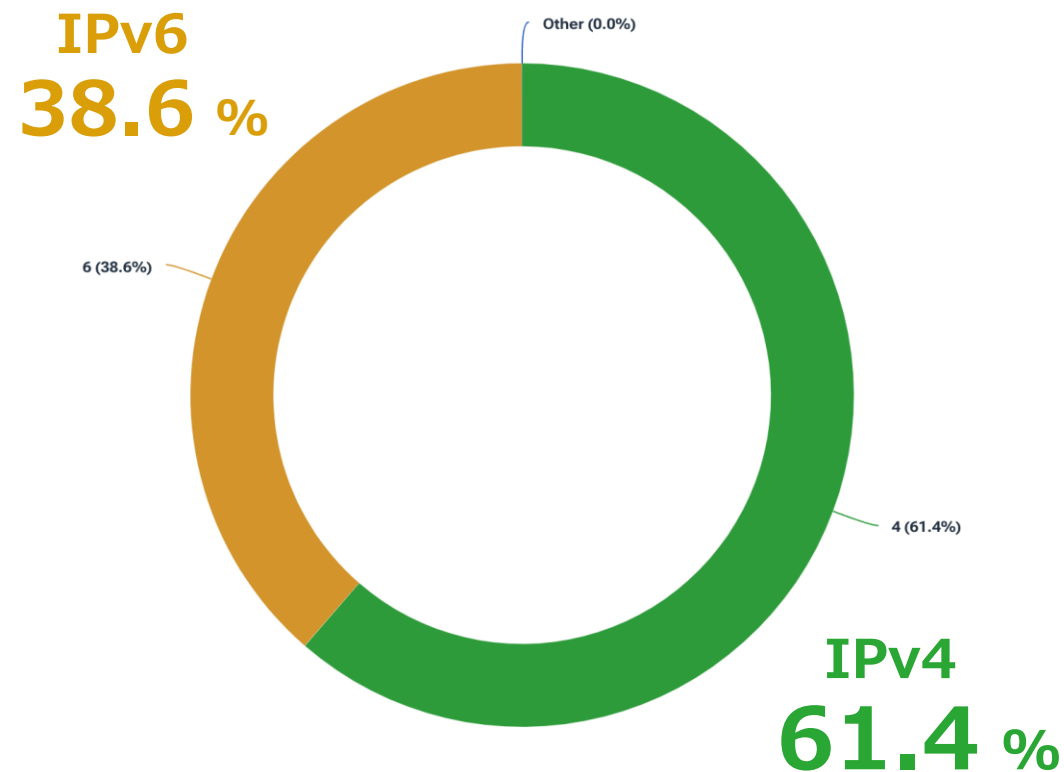
2023年度

(10月~11月)



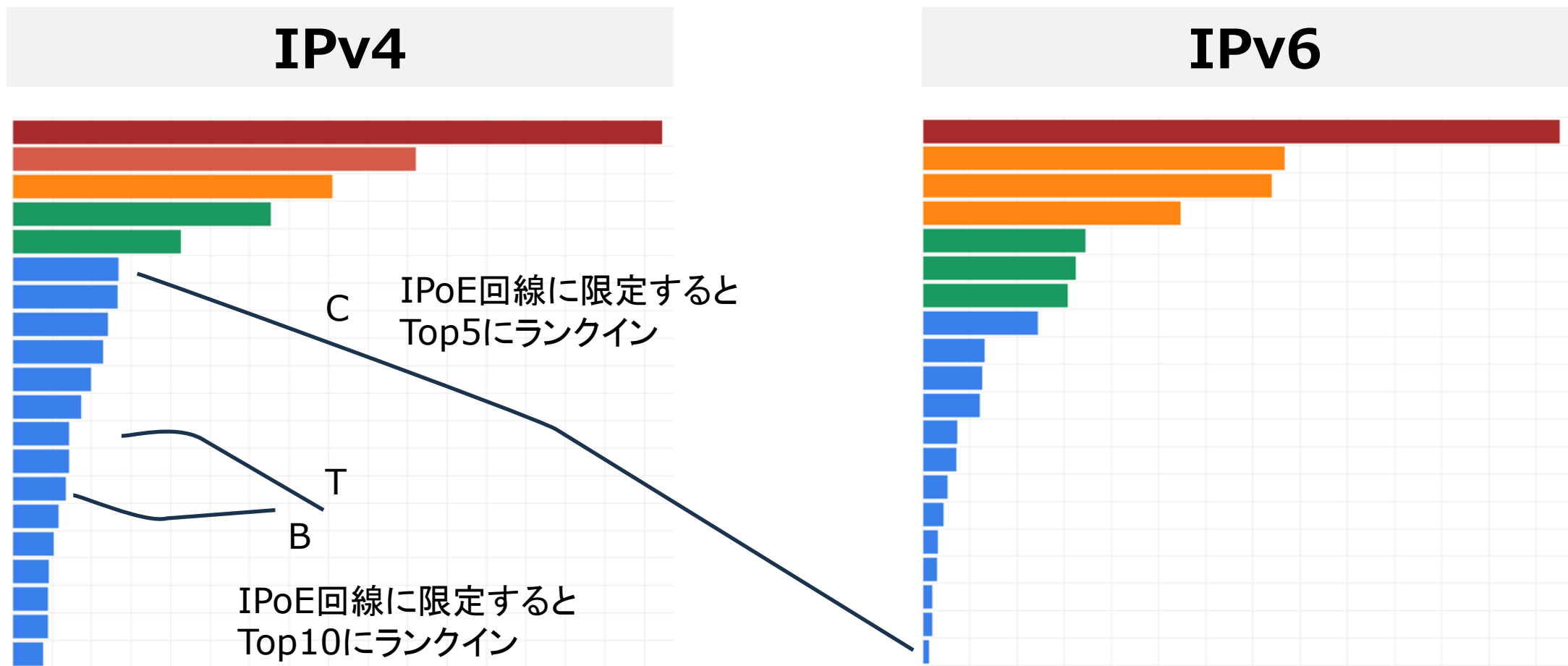
2024年度

(8月~9月)

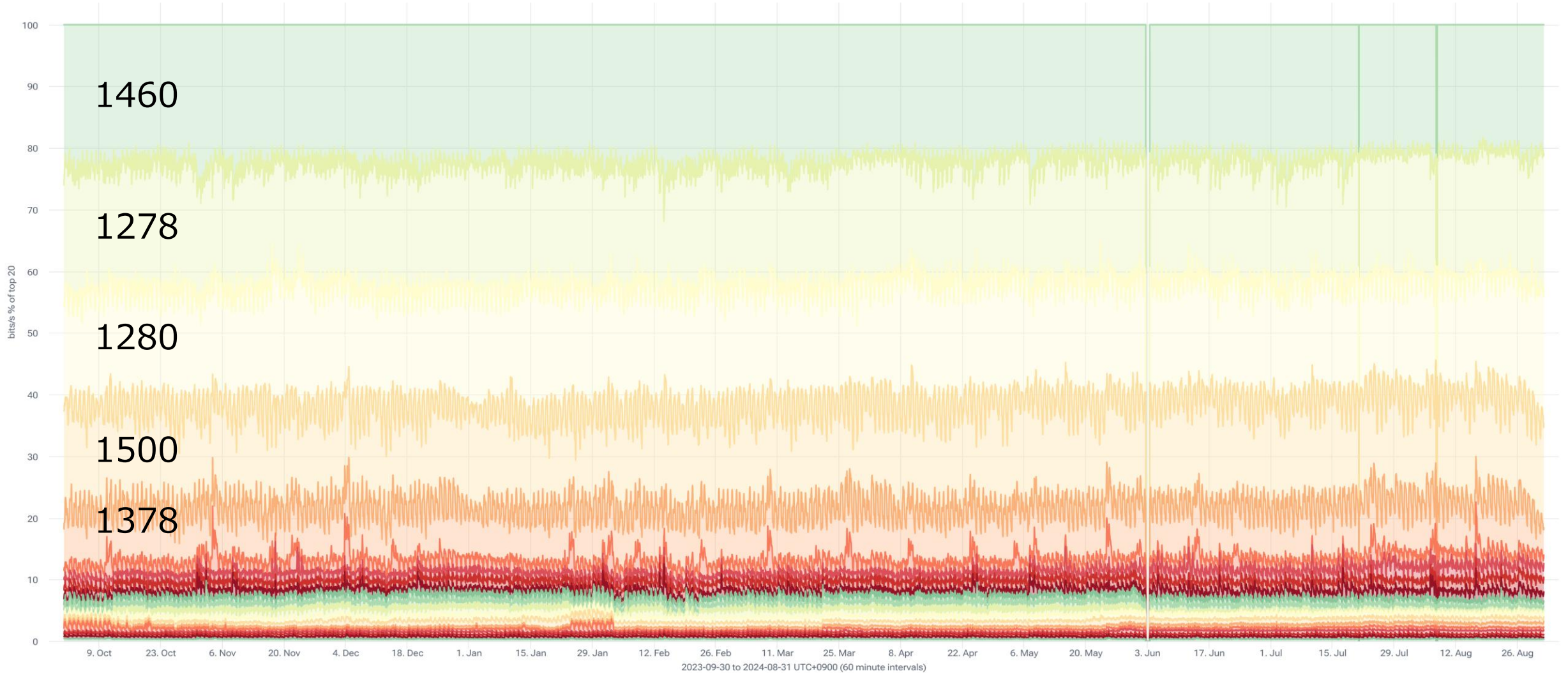


IPv4/IPv6トラフィック（2024/8） - AS別トップ20 -

- 主要なコンテンツはIPv6対応済みなので、IPv6比率をより高めるためにはユーザ側のIPv6対応が必要
- 一方、トラフィック上位にくるASの中には IPv4 only のASも存在 (Twitch, ByteDance, …etc)

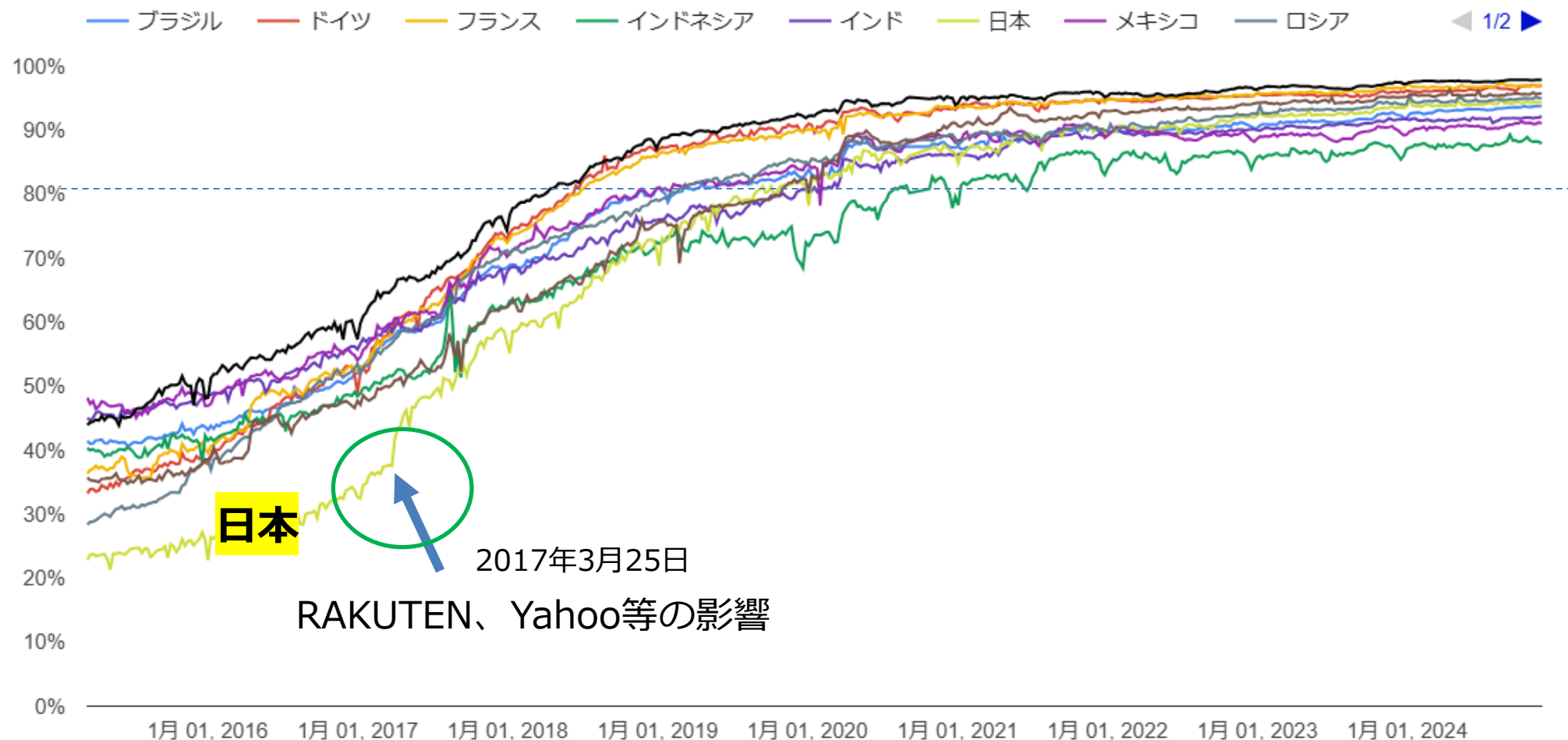


下り Traffic の Packet size 分布 (2023-2024)



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

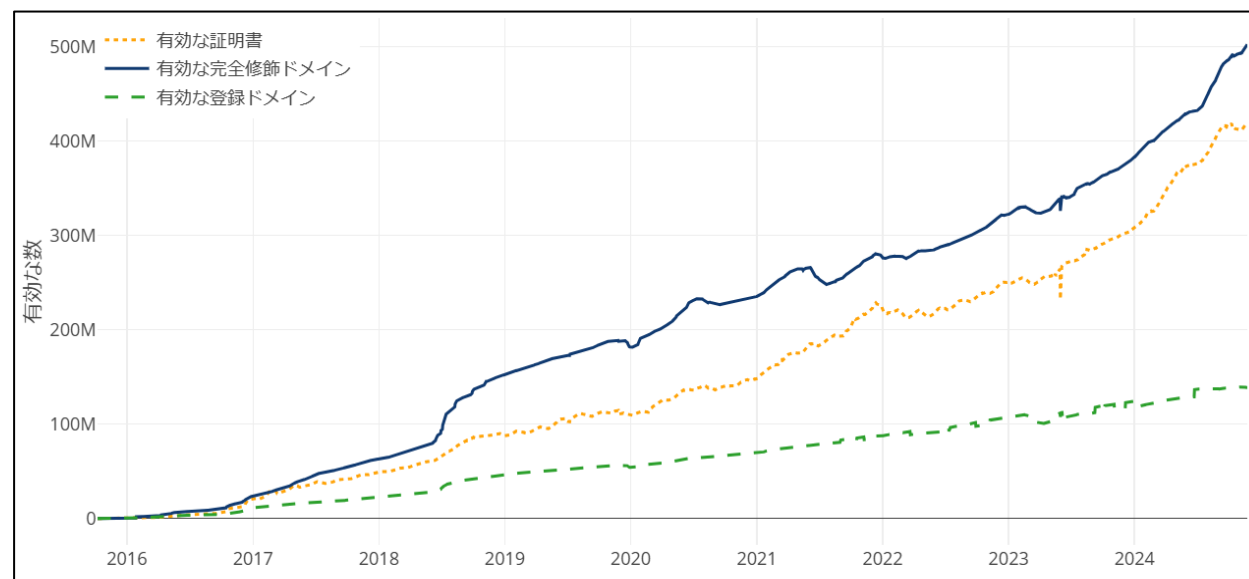
現在**94%** 微量ながら右上がりに 5,6年前は最下位 → 上位に



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

HTTPS化の加速

- Let's Encryptの普及（無料で**4億**以上の有効なSSL証明書発行）
- 通信は秘匿化
- Google
 - HTTPS 優先でランキング シグナルに反映
 - 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SSL化
 - SSL対応済み -> SSL対応済み ◎
 - SSL対応済み -> SSL非対応 ×



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

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

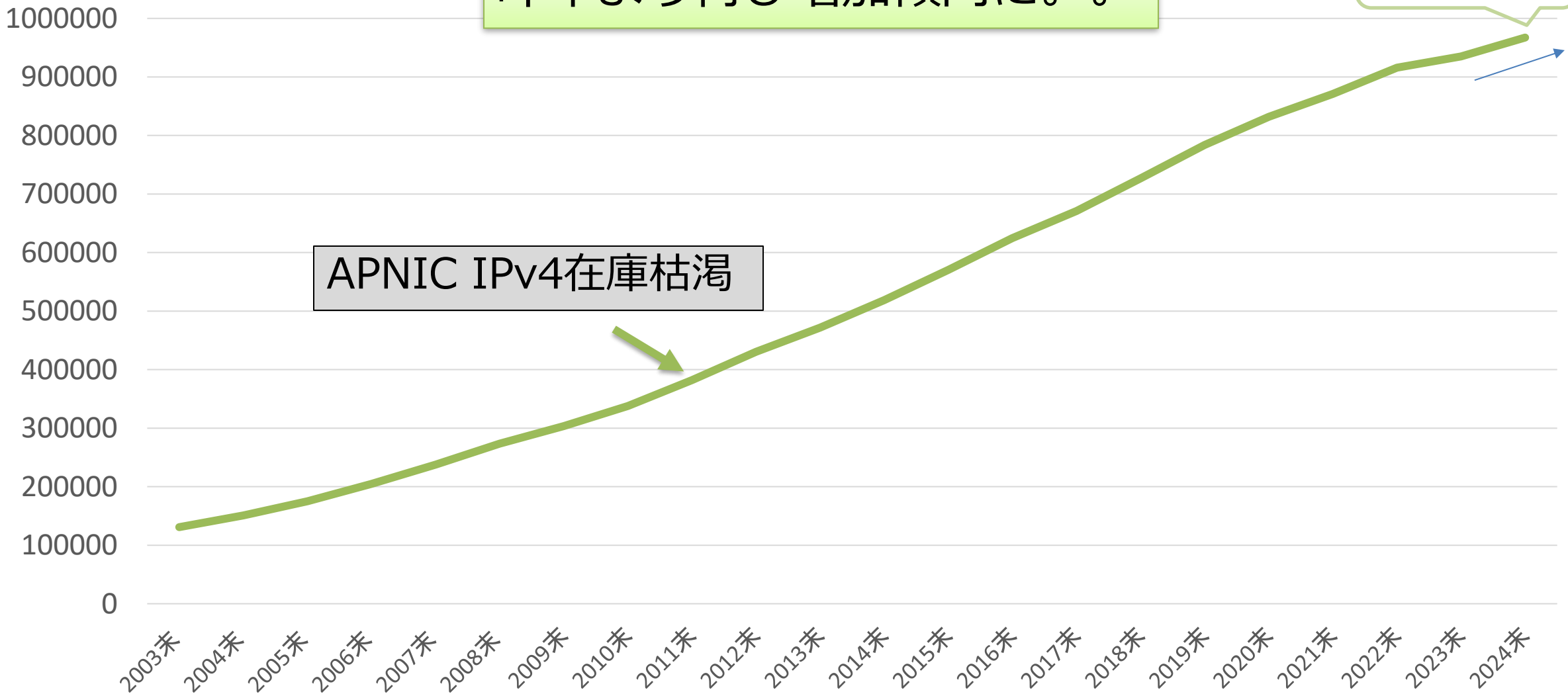
ルーティング動向

- IPv4経路が約**96.7万**に到達（**昨年から+3.2万、一昨年は+2.0万**）
 - 年増加率は**約1.05倍**で伸び率は昨年とほぼ同等（**一昨年1.05倍**）
 - **/24は全体の約6割強**、経路増大の主要因、移転影響もあり
- IPv6経路は**21.5万経路**に到達
 - ここ1年間で**+約2.5万経路（昨年+2.8万）**
- IPv4経路：IPv6経路 = **82% : 18%**
- 観測されるAS番号は約7.5万AS
 - 2020年以降、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だが、更なる普及が必要

IPv4経路数の推移

昨年より再び増加傾向に。。

967244経路
(2023/11)



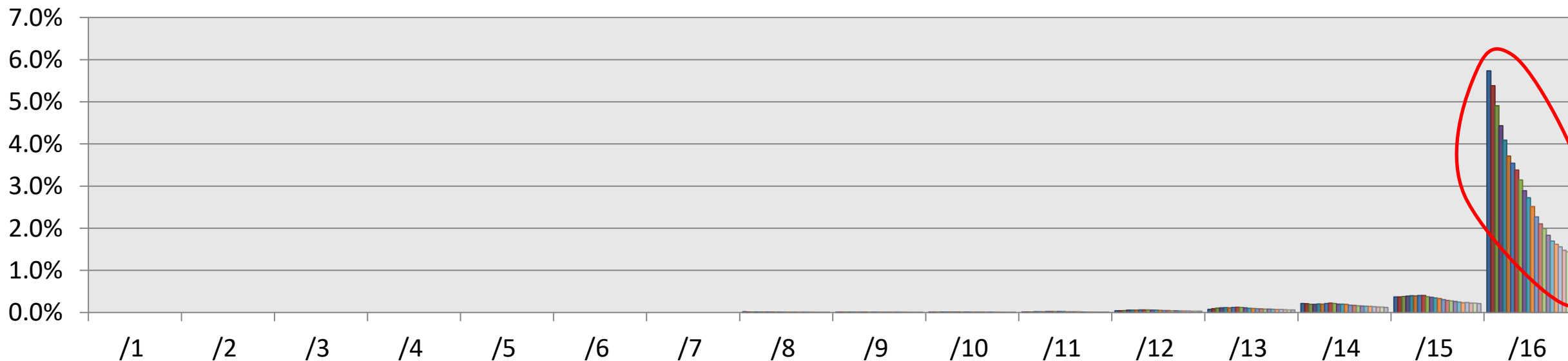
APNIC IPv4在庫枯渇

IPv4経路数の推移（2003年～2024年）

経路数

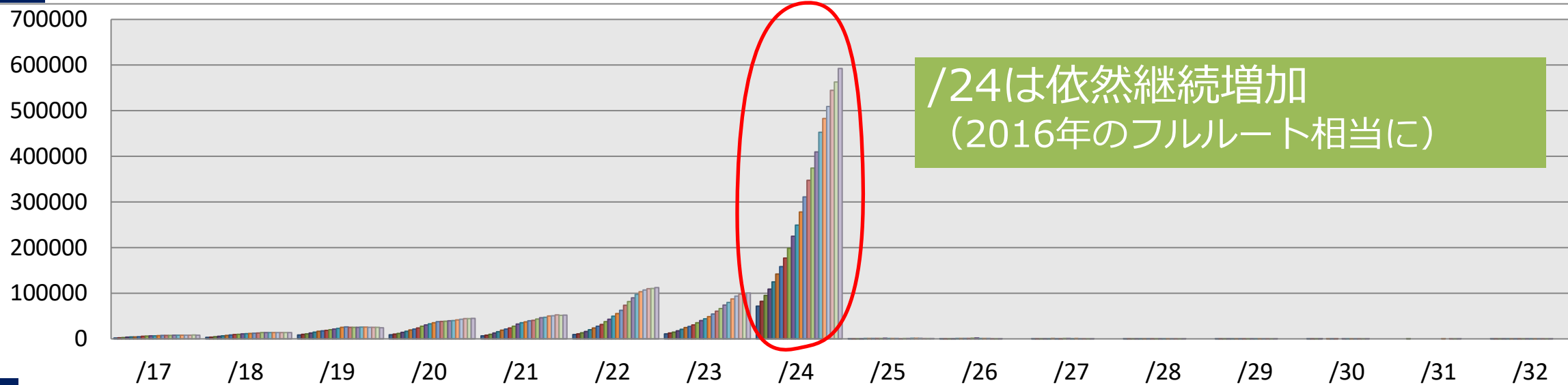


割合

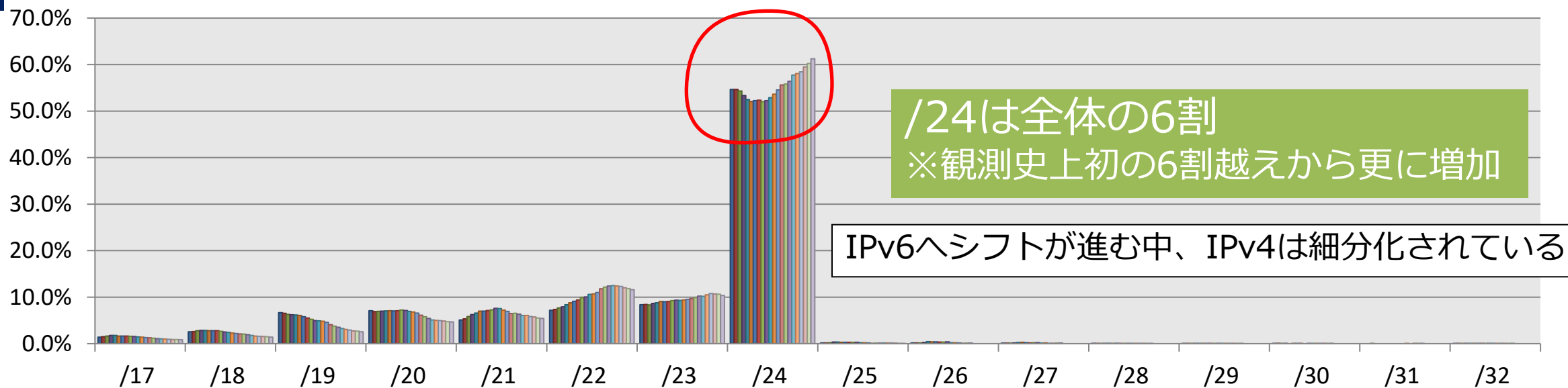


IPv4経路数の推移 (2003年~2024年)

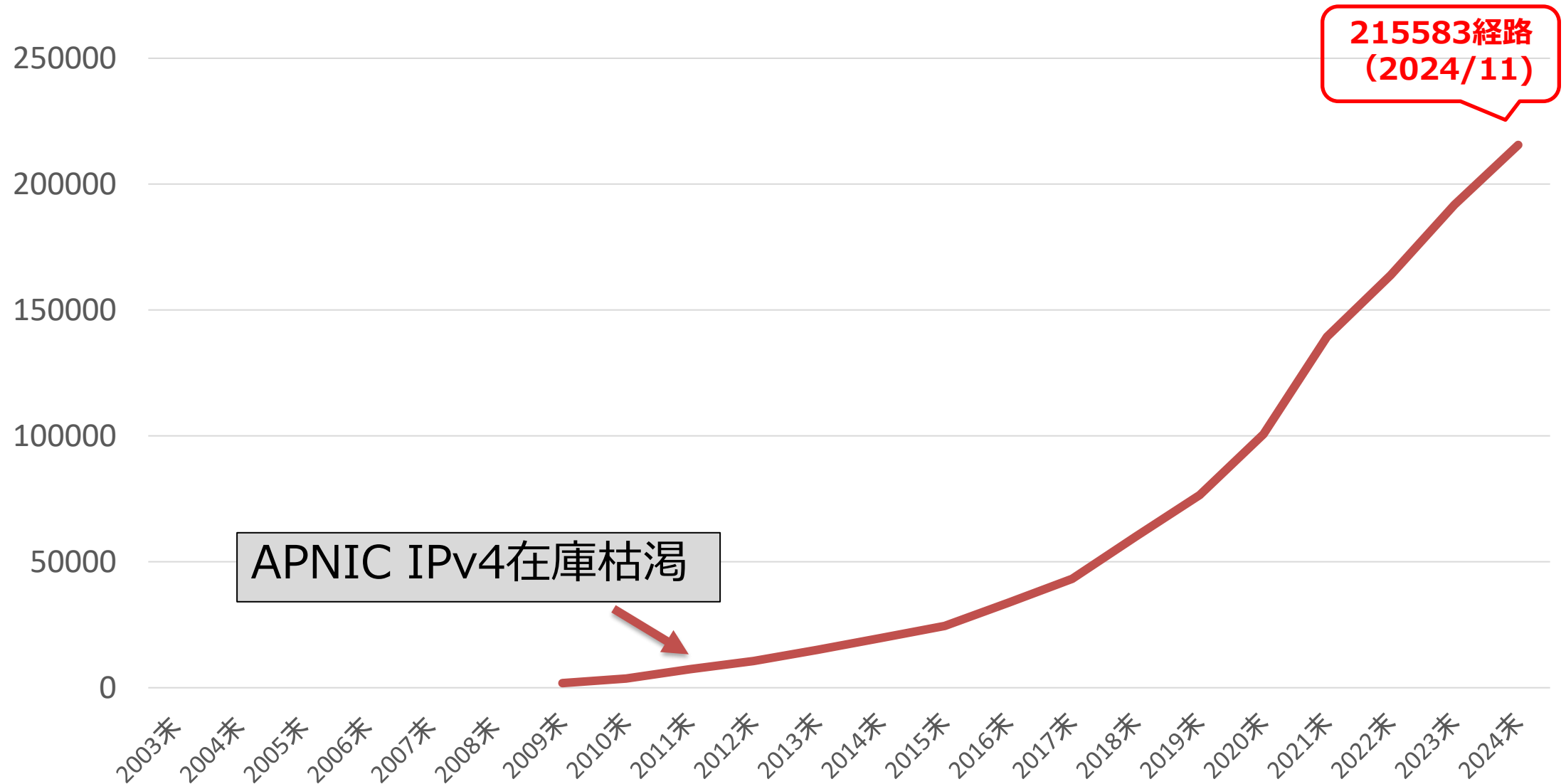
経路数



割合

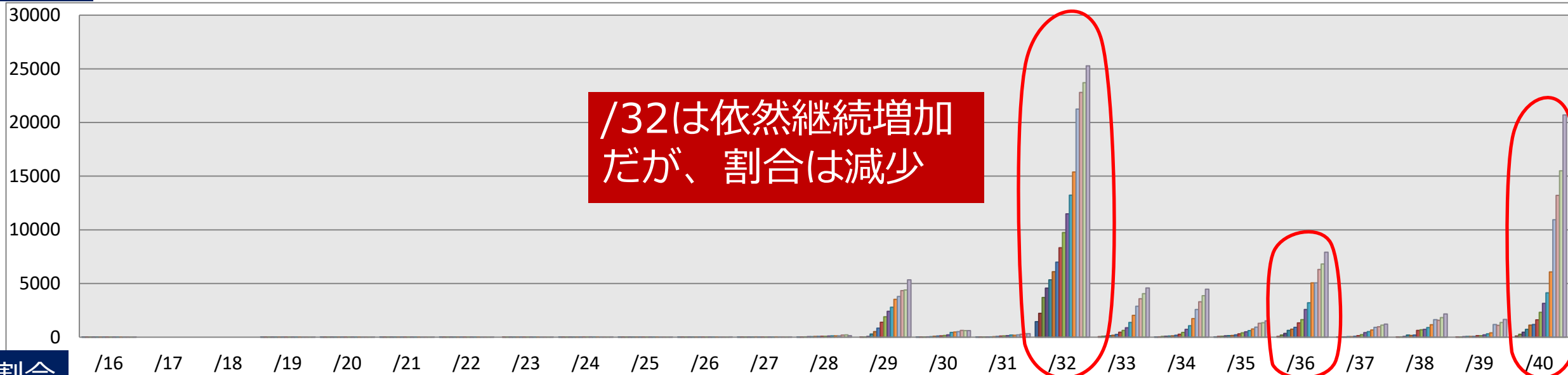


IPv6経路数の推移

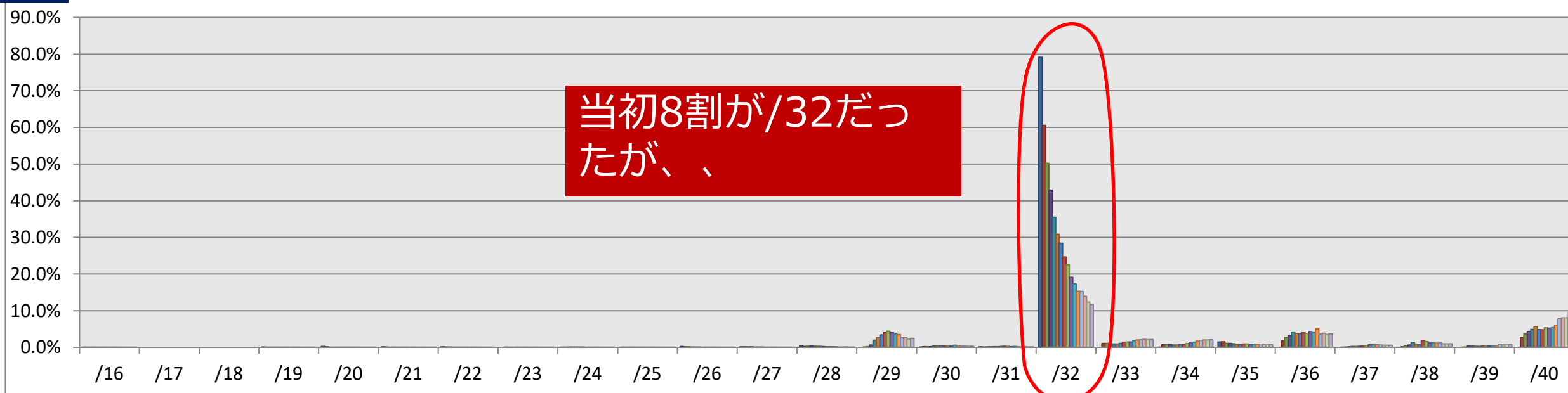


IPv6経路数の推移 (2009年~2024年)

経路数

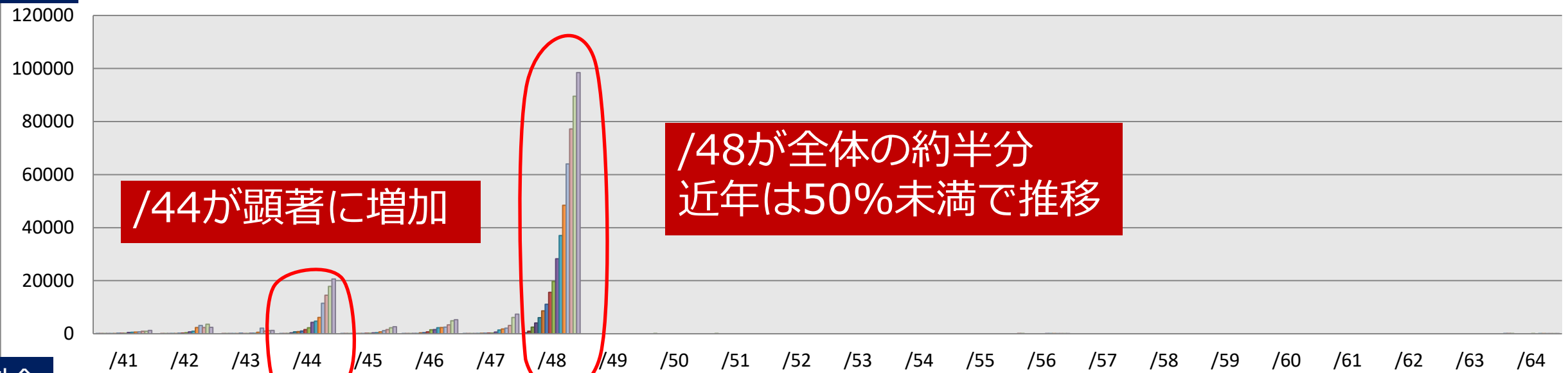


割合

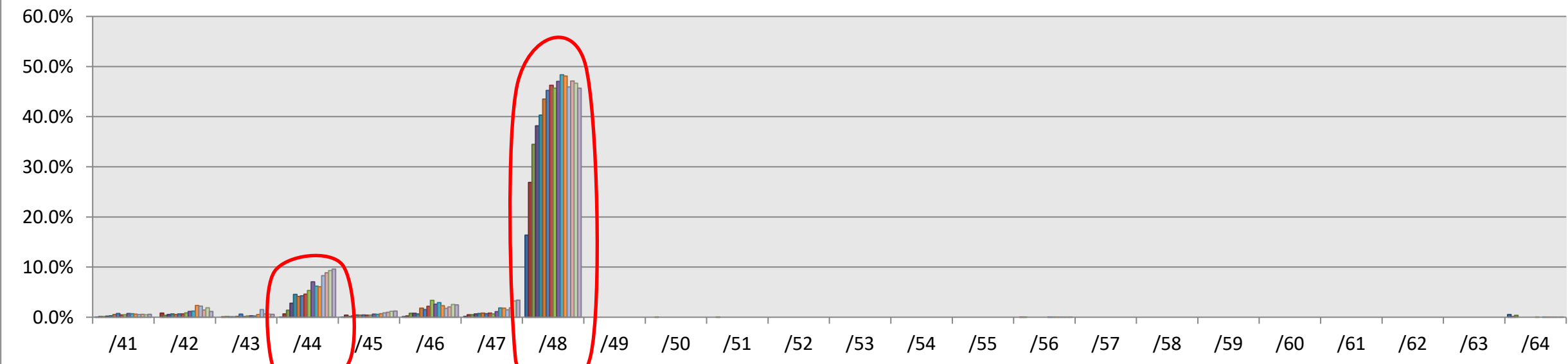


IPv6経路数の推移 (2009年~2024年)

経路数



割合



IPv4/IPv6 経路数の推移

経路数

1000000

900000

800000

700000

600000

500000

400000

300000

200000

100000

0

IPv4(967244)

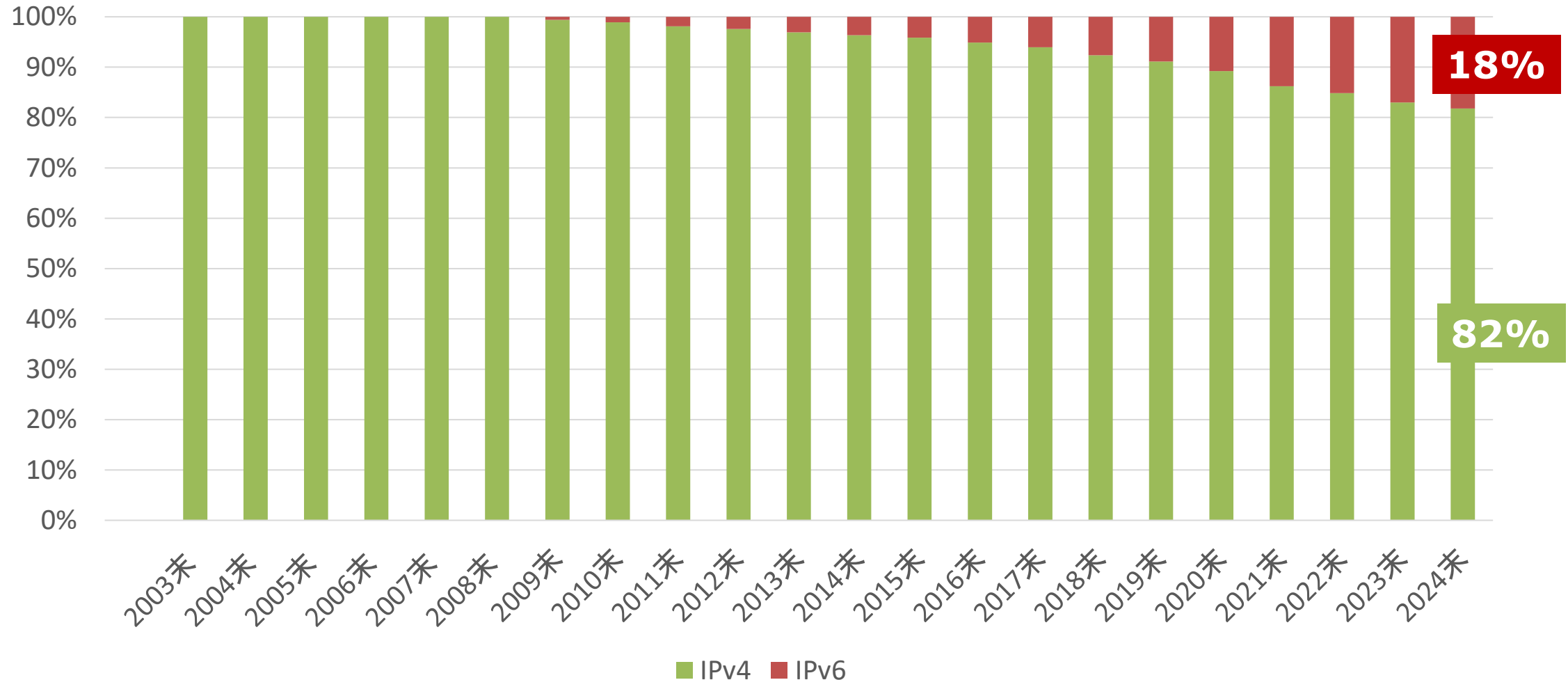
IPv6(215583)

2003末 2004末 2005末 2006末 2007末 2008末 2009末 2010末 2011末 2012末 2013末 2014末 2015末 2016末 2017末 2018末 2019末 2020末 2021末 2022末 2023末 2024末

IPv4/IPv6 経路数の割合推移

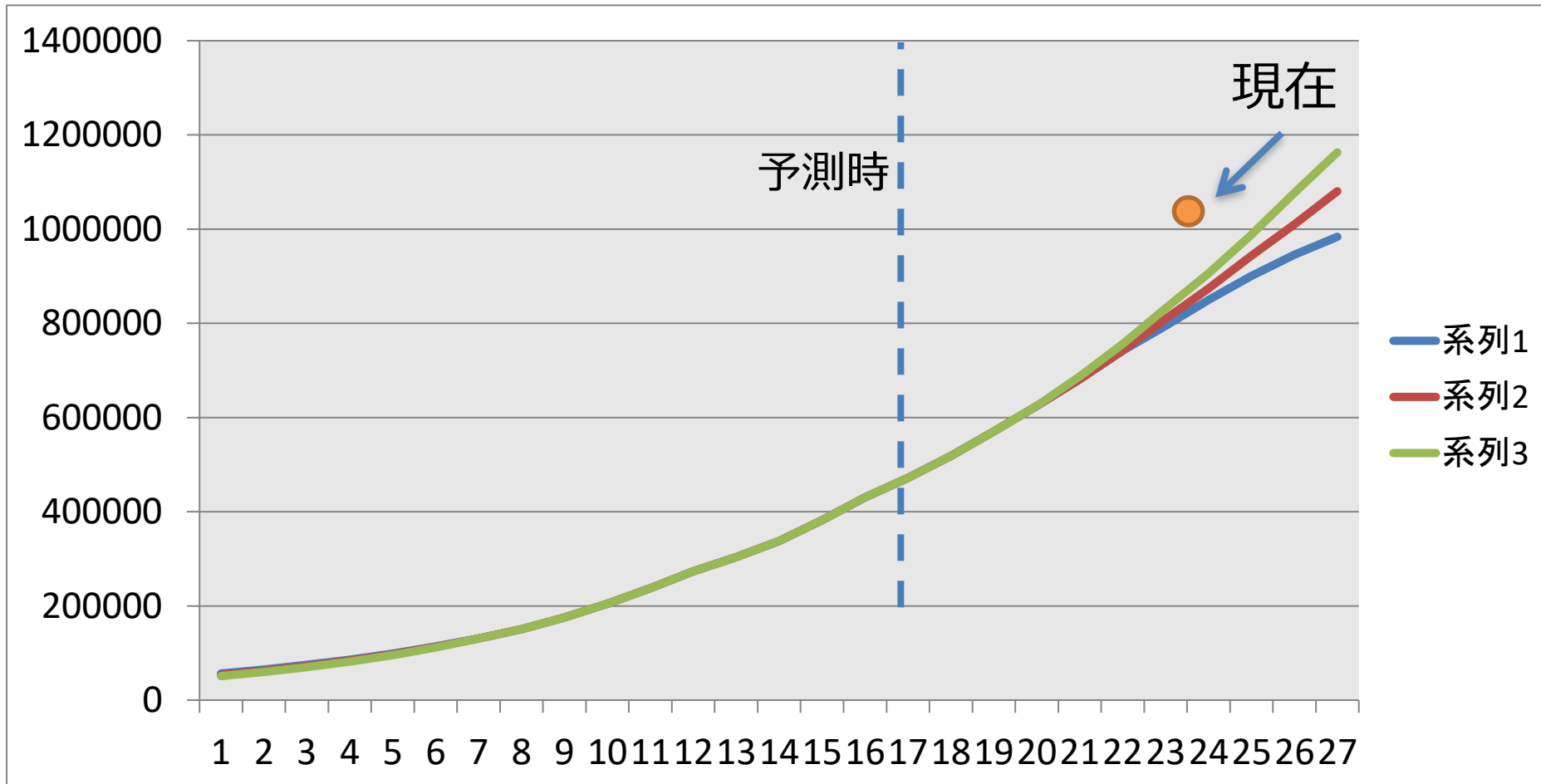
着実にIPv6化が進んでいる

どこかでTEのためのv4経路分割は減らしたい



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。



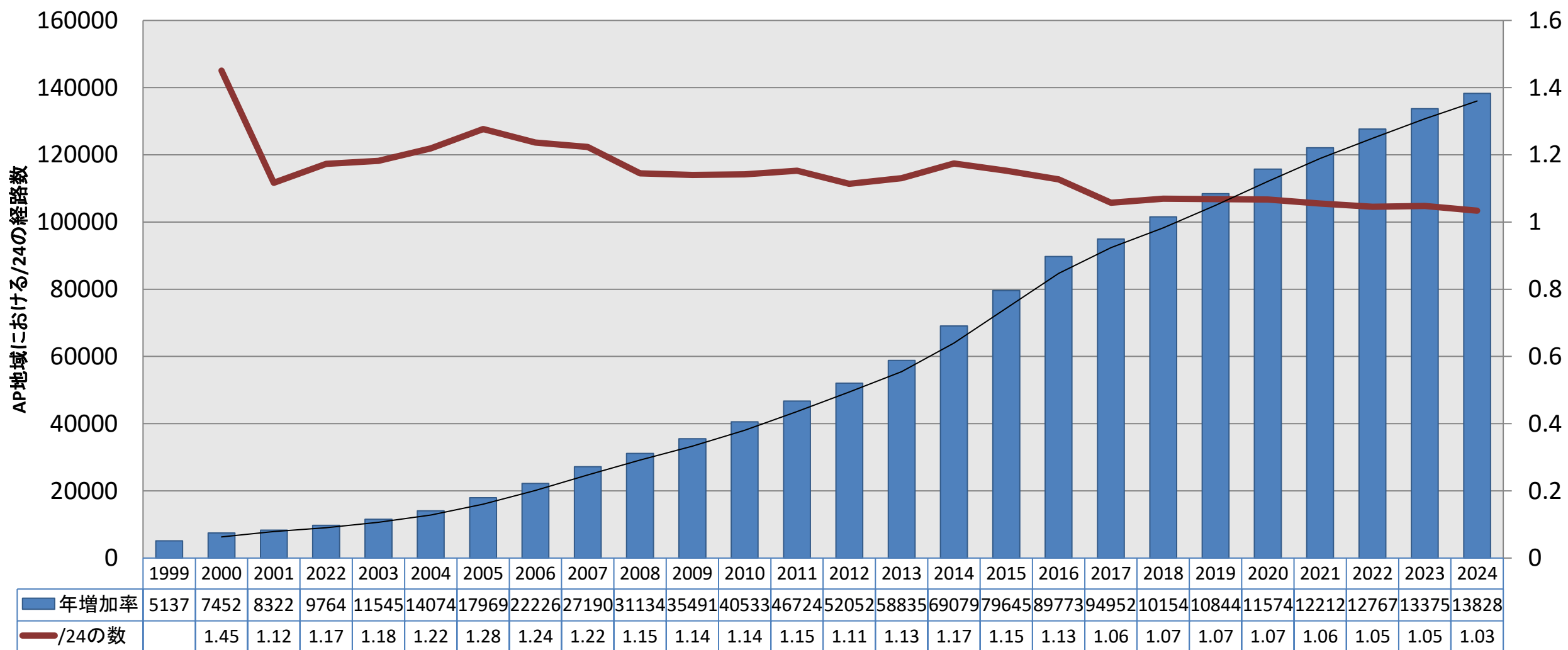
AP地域の/24の推移

AP地域の/24のみで**13.8万経路超**、増加率は**過去最少の3%増**に（年々減少）

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）

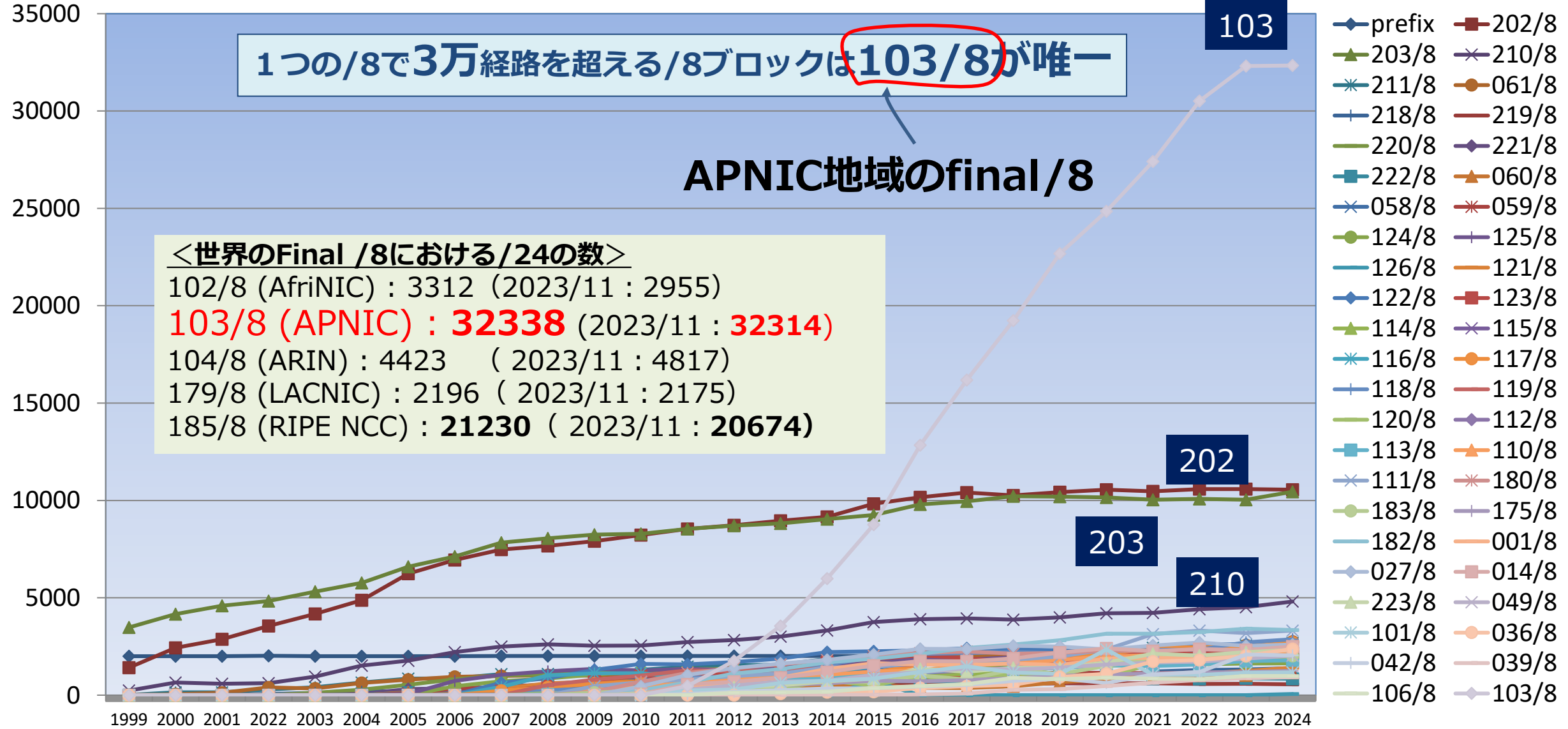
経路数

増加率



AP地域の/24の推移

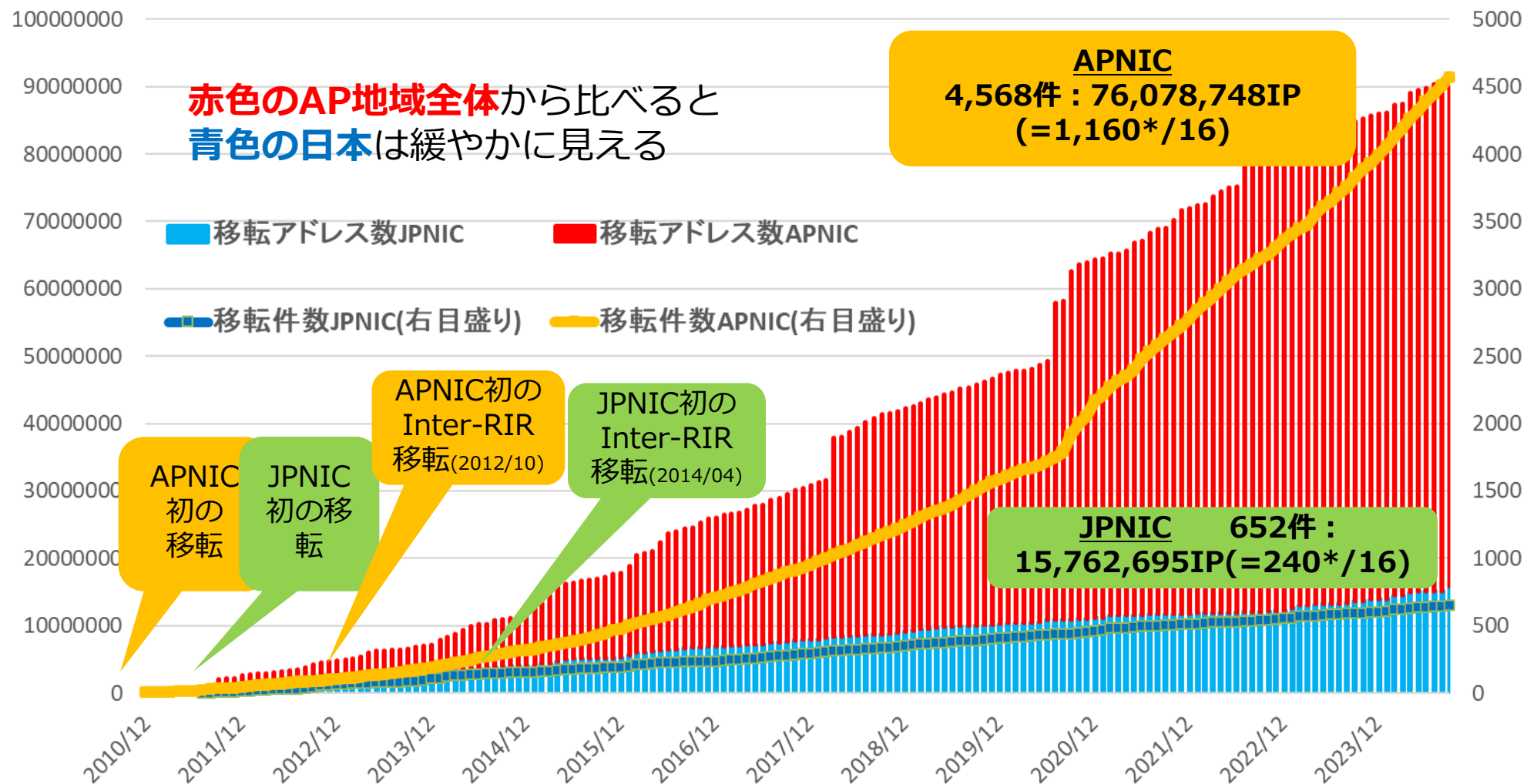
伸びが鈍化



日本のIPv4アドレス移転状況

- 2024年11月現在**668**件(昨年+**63**, 1年前+56, 2年前+46)
 - **申請件数は近年増加、大きなサイズは国際移転が中心**
- 国際移転も**145**件 (昨年+**19**, 1年前+**4**, 2年前+**4**)
 - 他レジストリ→JPNIC : **109**件 (昨年+**2**, 1年前+**4**, 2年前+**4**)
 - JPNIC→他レジストリ : **36**件 (昨年+**17**, 1年前**0**, 2年前**0**件)
 - **国際移転による他レジストリへの流出が急増**
- 移転の理由
 - **純粋にIPv4アドレス不足のケースが多い**
- 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**, 1年前**0**, 2年前**0**)
 - <https://www.nic.ad.jp/ja/ip/transfer/wishlist.html>
- AS番号の移転**17**件 (昨年+**2**, 1年前+**3**, 2年前+**3**)

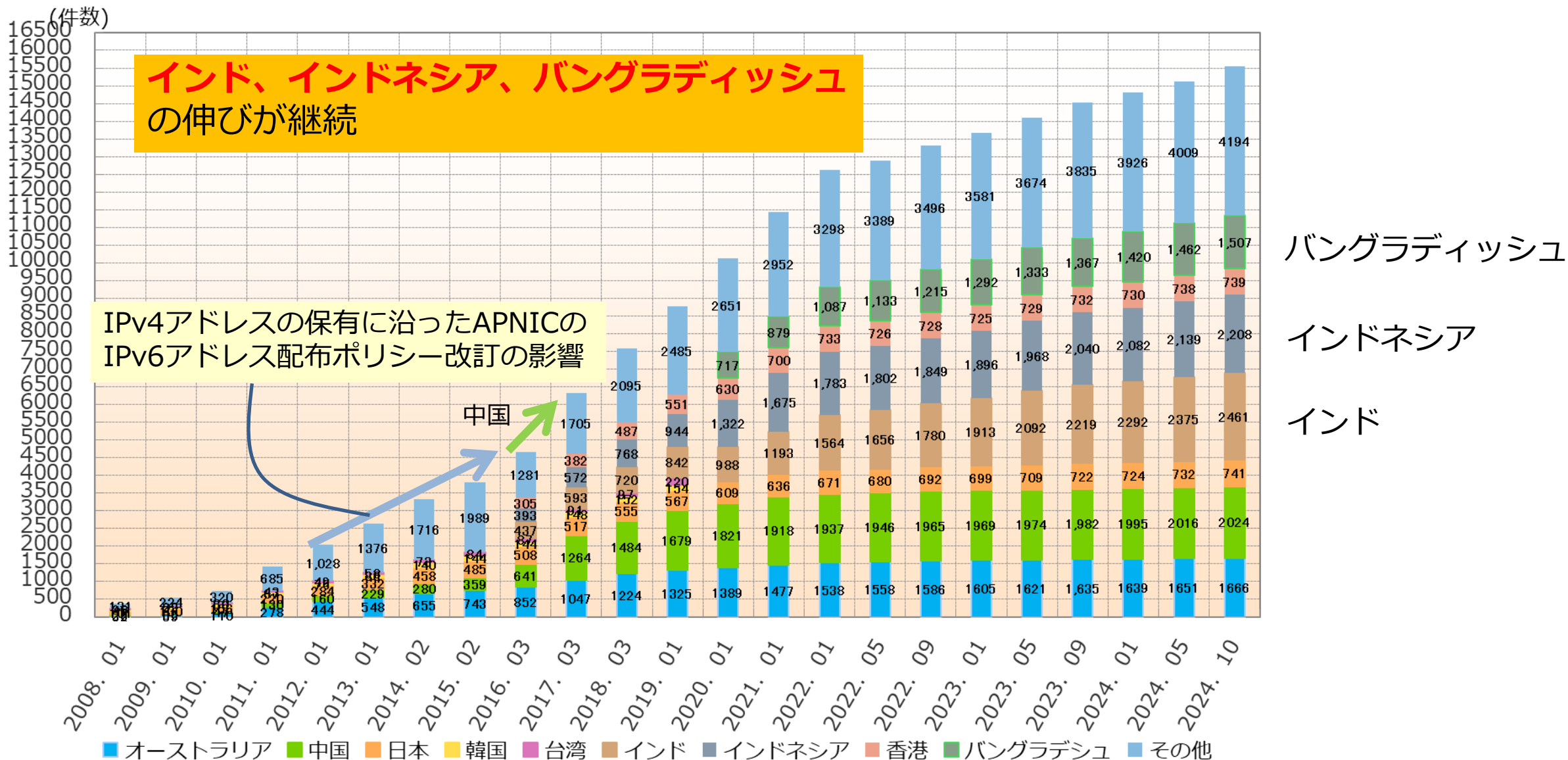
APNIC地域と日本の移転状況比較



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

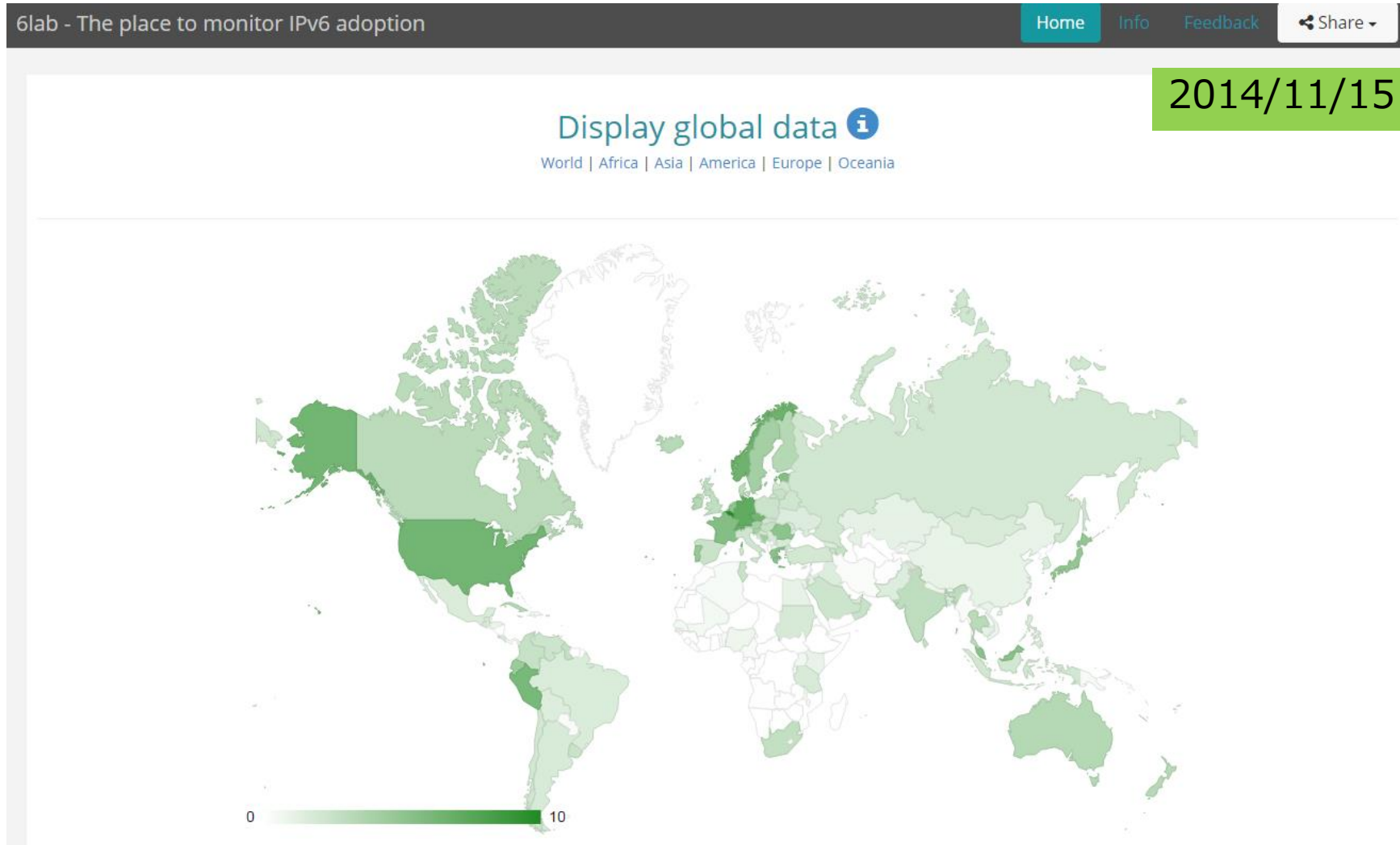
出典：JPNIC統計情報

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

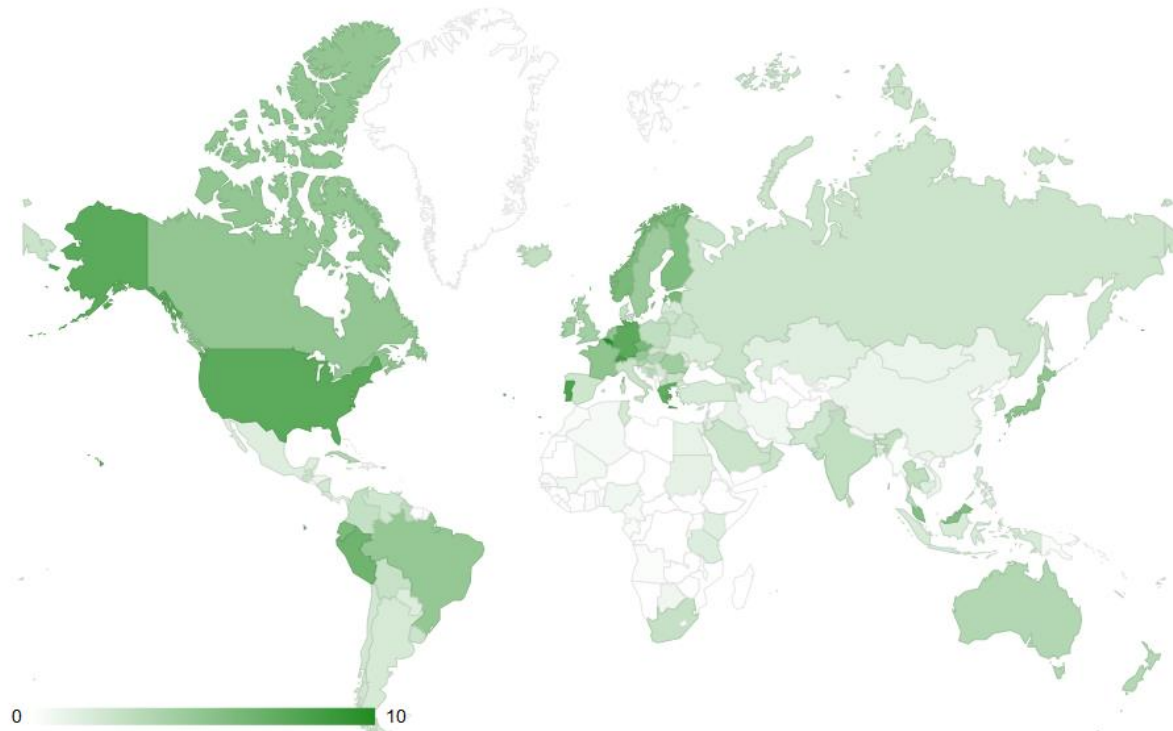
Feedback

Share

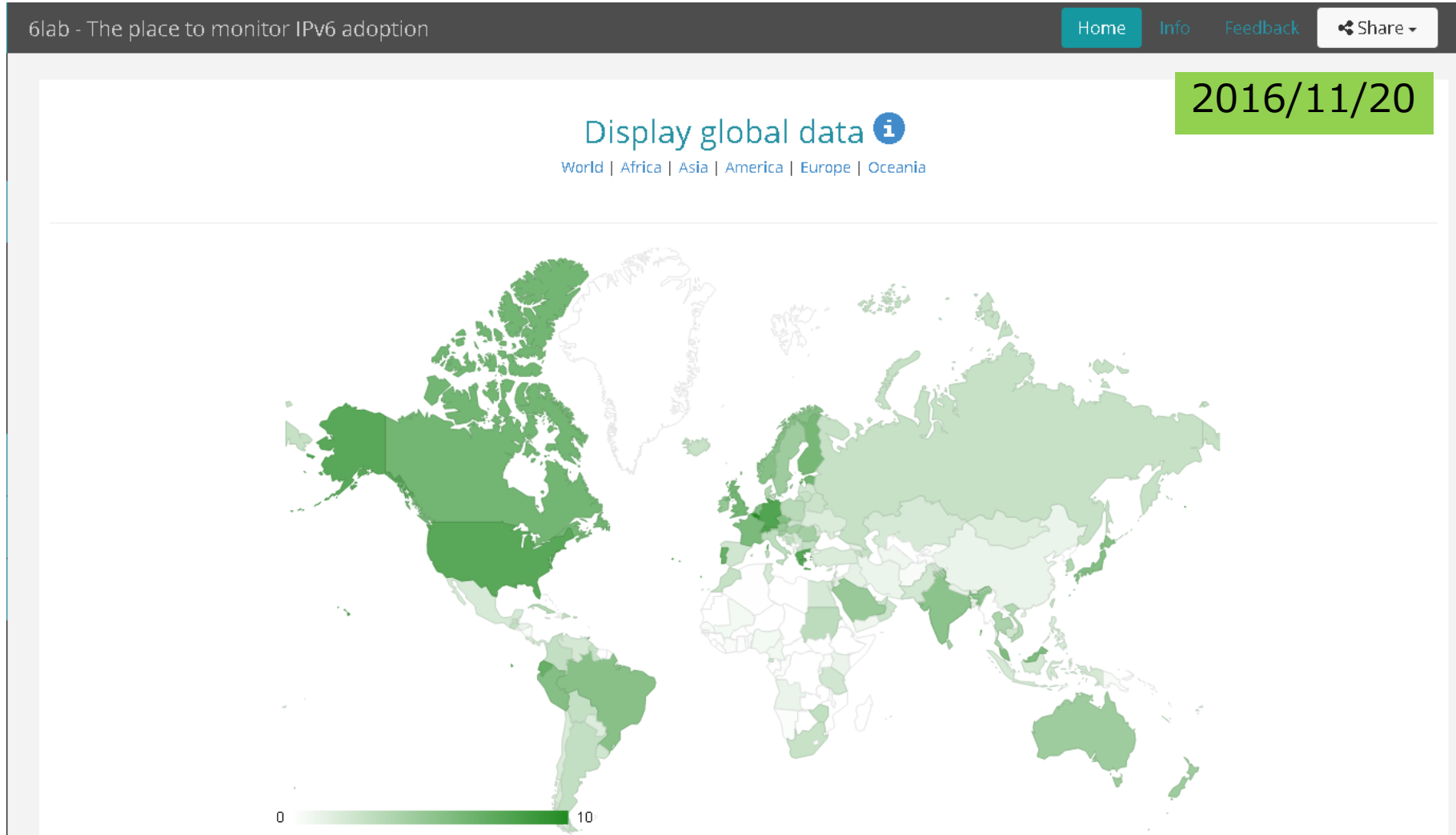
2015/11/19

Display global data 

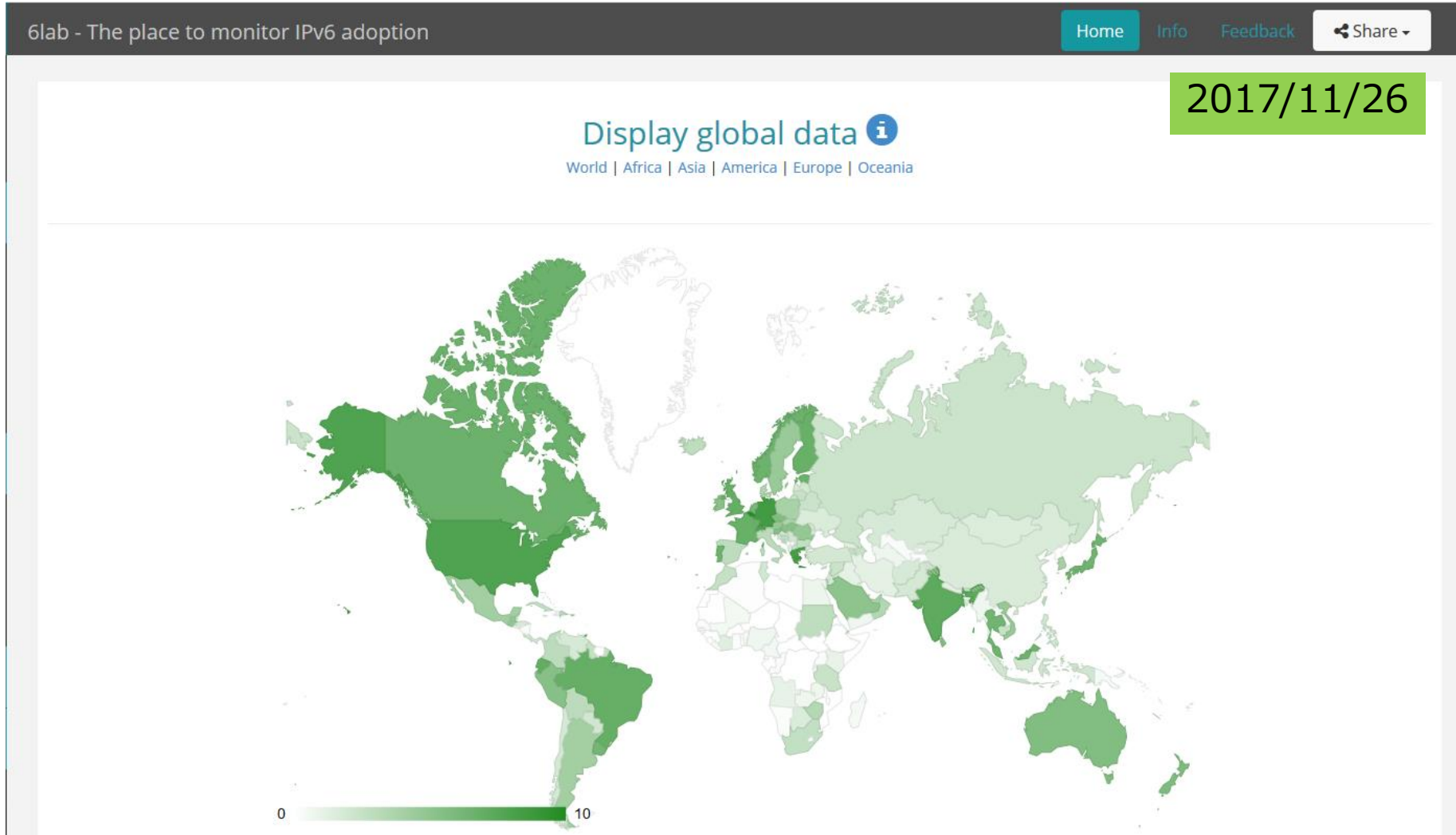
World | Africa | Asia | America | Europe | Oceania



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



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



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

6lab - The place to monitor IPv6 adoption

Home

Info

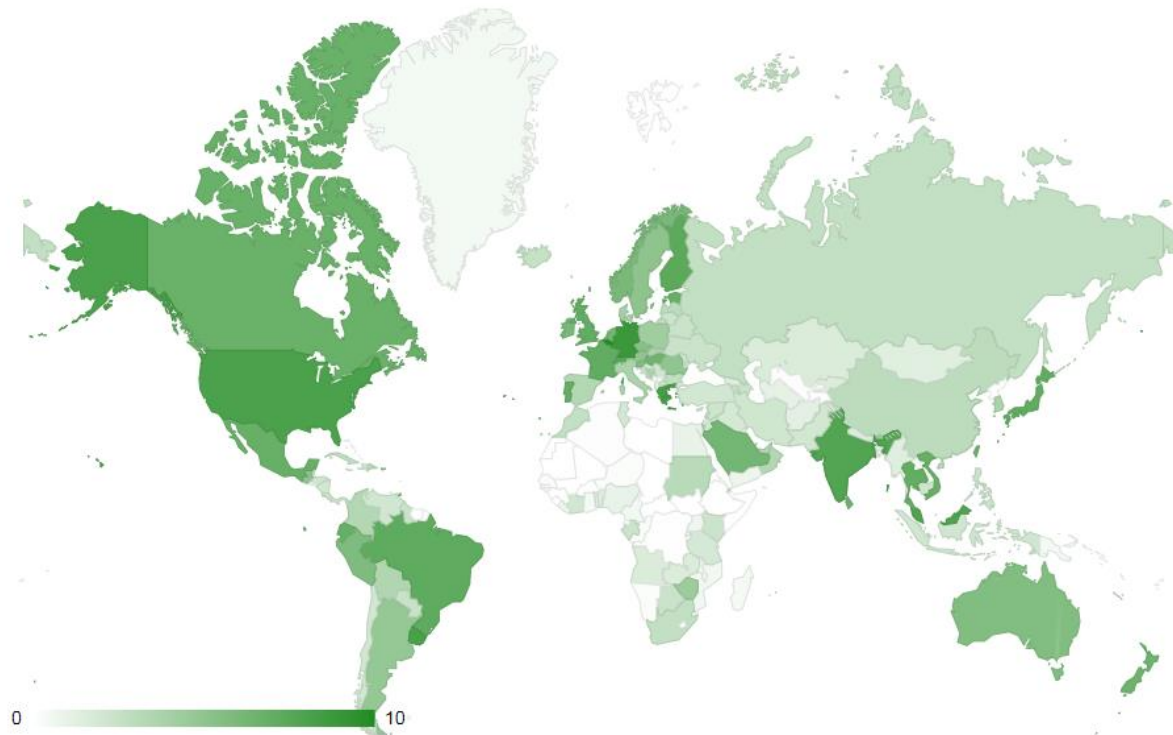
Feedback

Share

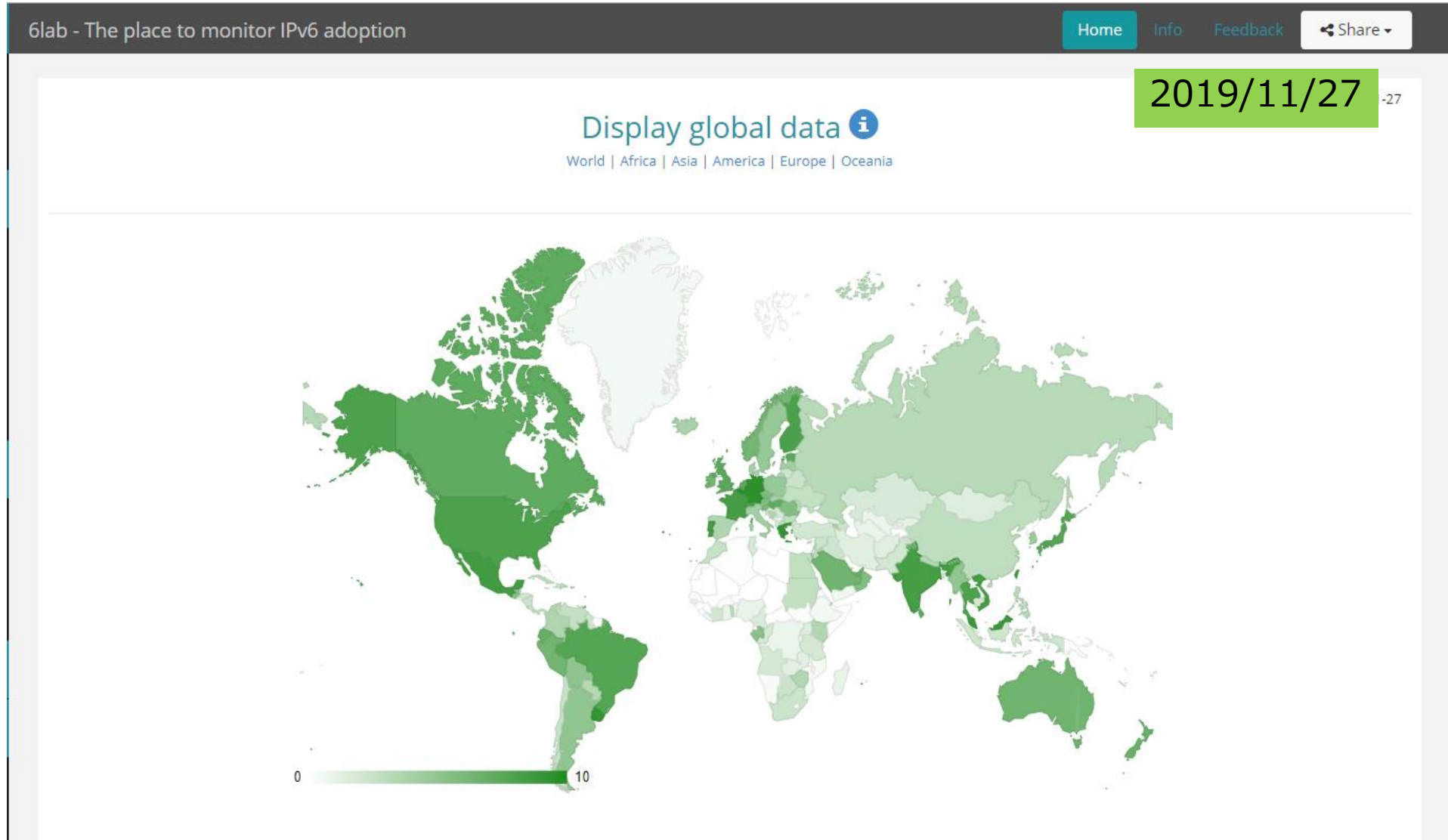
2018/11/25

Display global data 

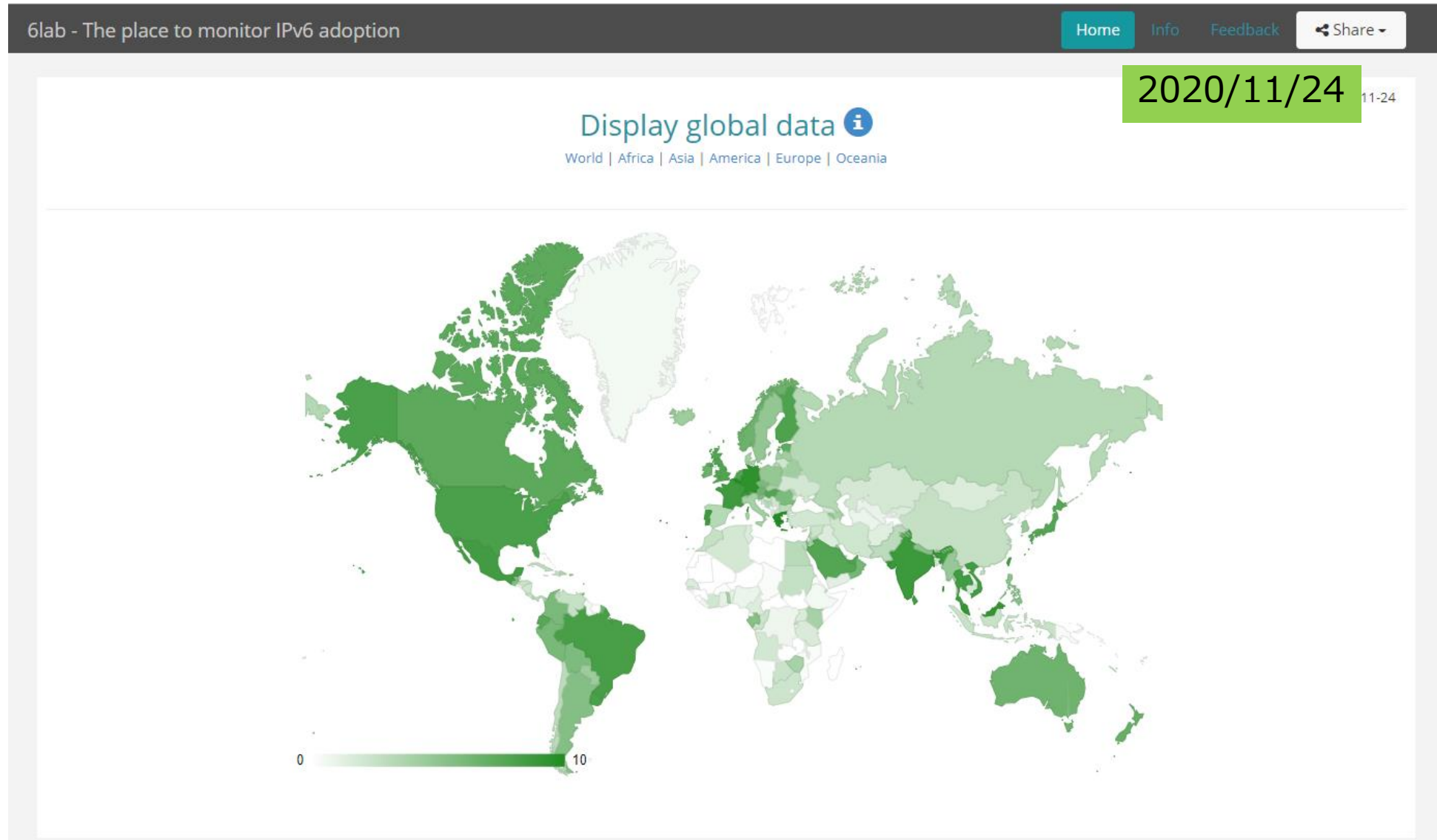
World | Africa | Asia | America | Europe | Oceania



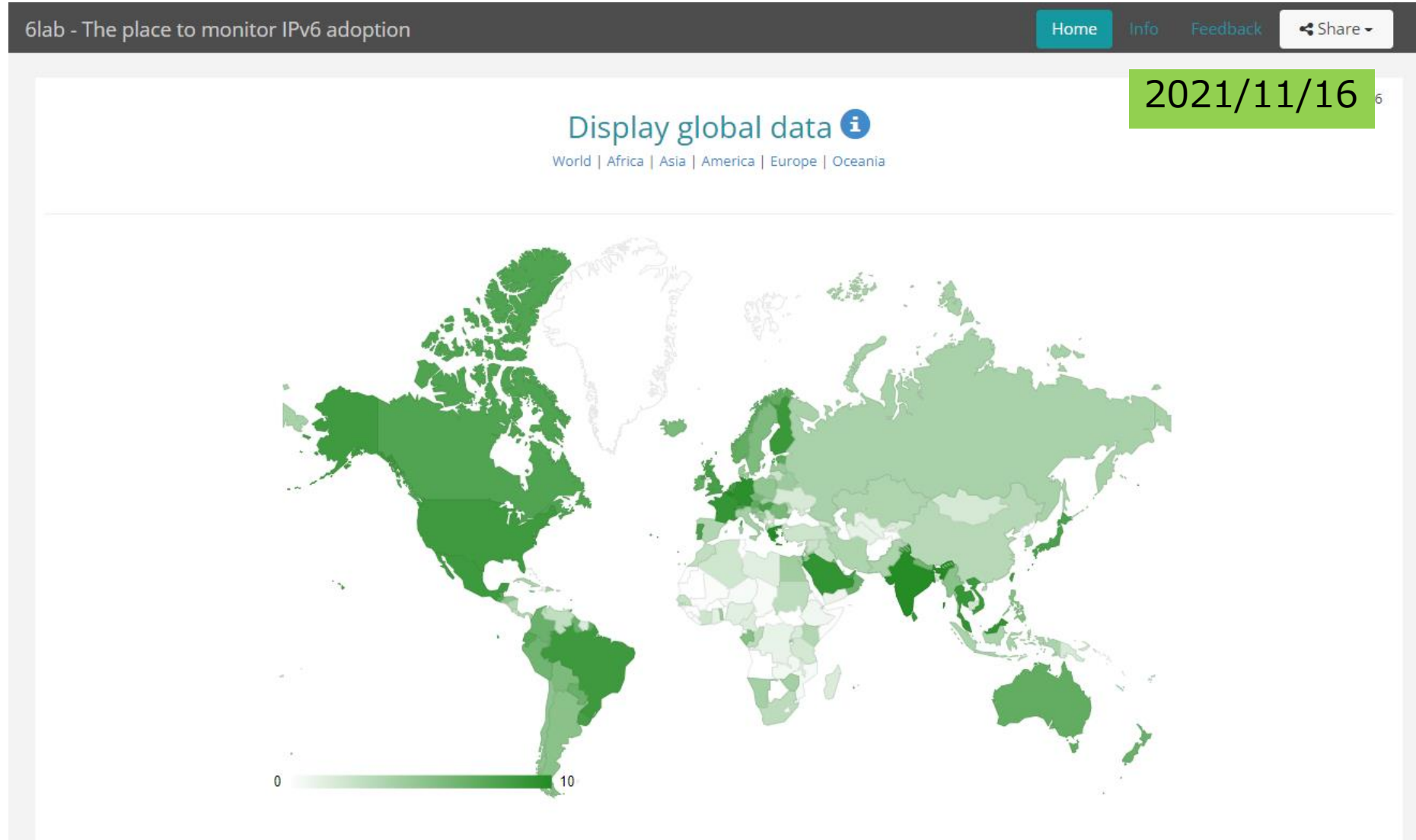
http://6lab.cisco.com/stats/



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



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



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

6lab - The place to monitor IPv6 adoption

Home

Info

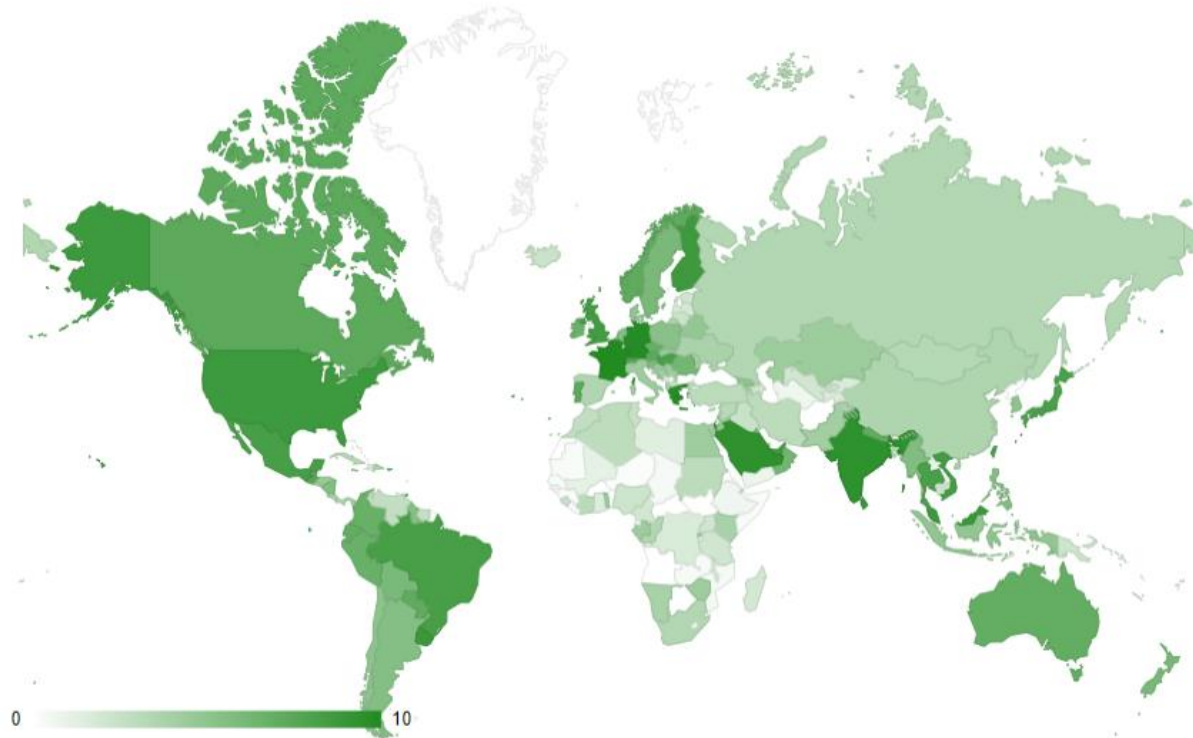
Feedback

Share

2022/11/16

Display global data 

World | Africa | Asia | America | Europe | Oceania



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

6lab - The place to monitor IPv6 adoption

Home

Info

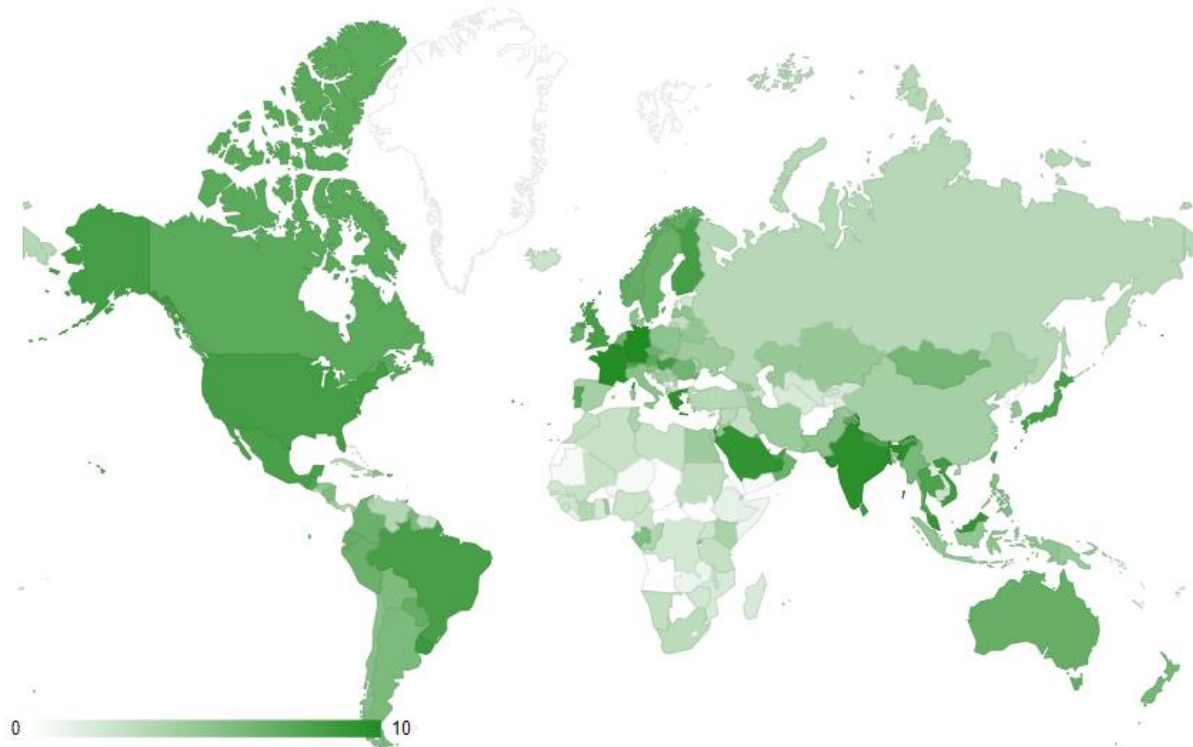
Contact

Share

2023/11/14

Display global data 

World | Africa | Asia | America | Europe | Oceania

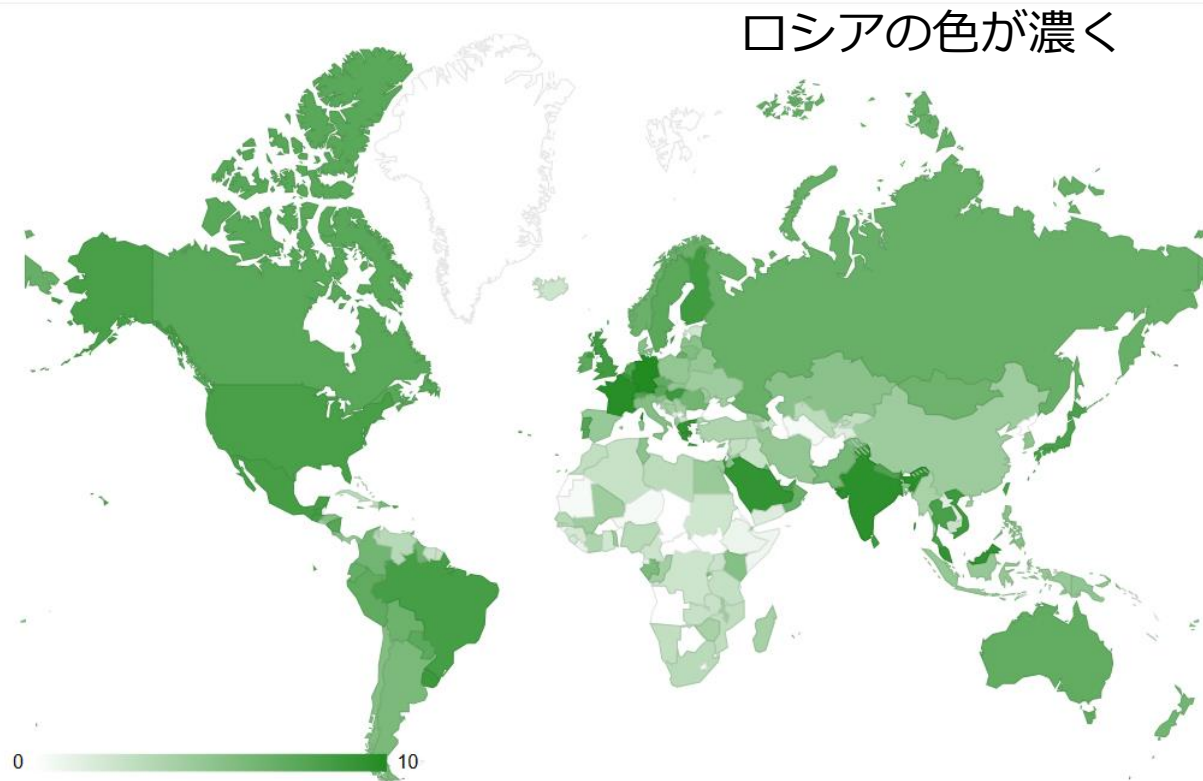


<http://6lab.cisco.com/stats/>

着実にIPv6化は進展中

Display global data ⓘ
World | Africa | Asia | America | Europe | Oceania

2024/11/13



■ 参照データ
Prefix
Transit
Contents
User

AS番号 (2byte/4byte)

- 2byteAS

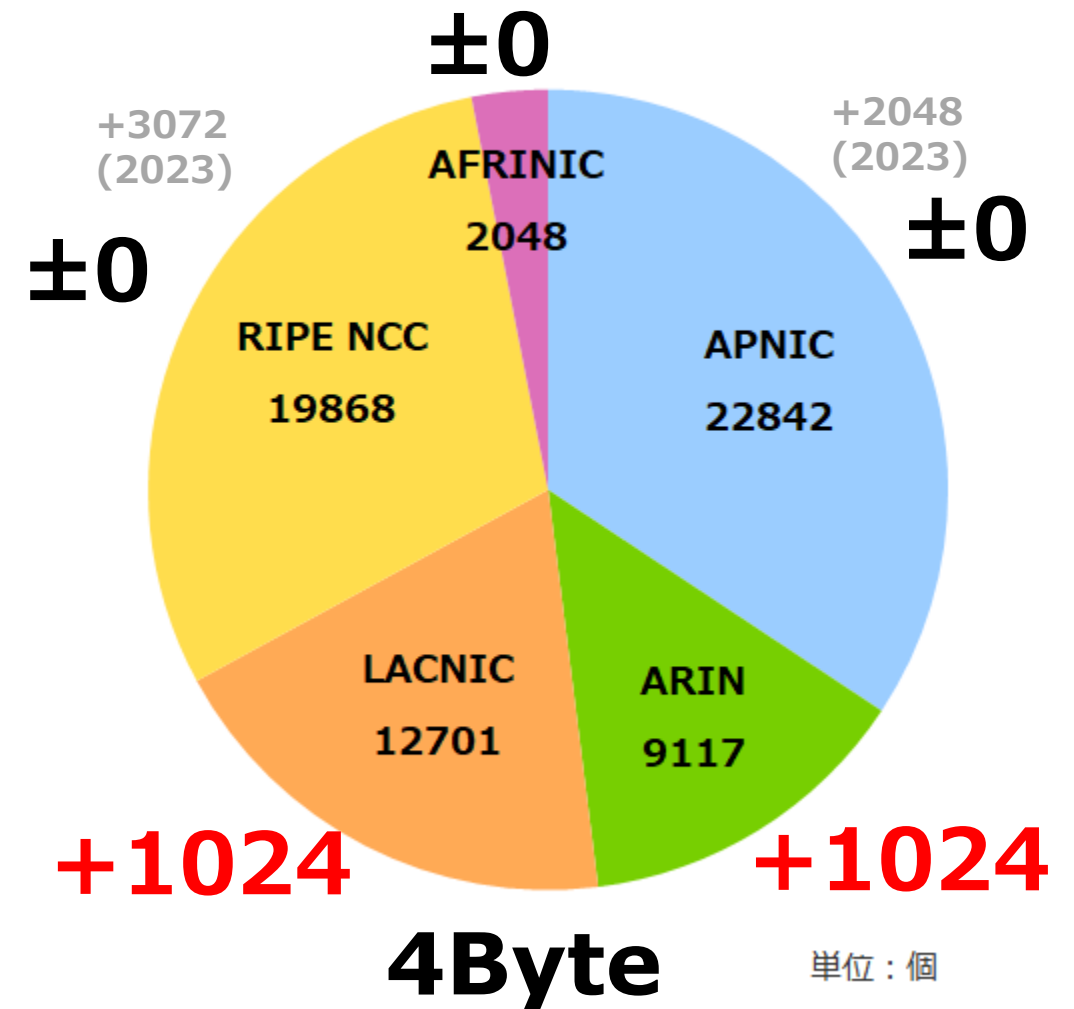
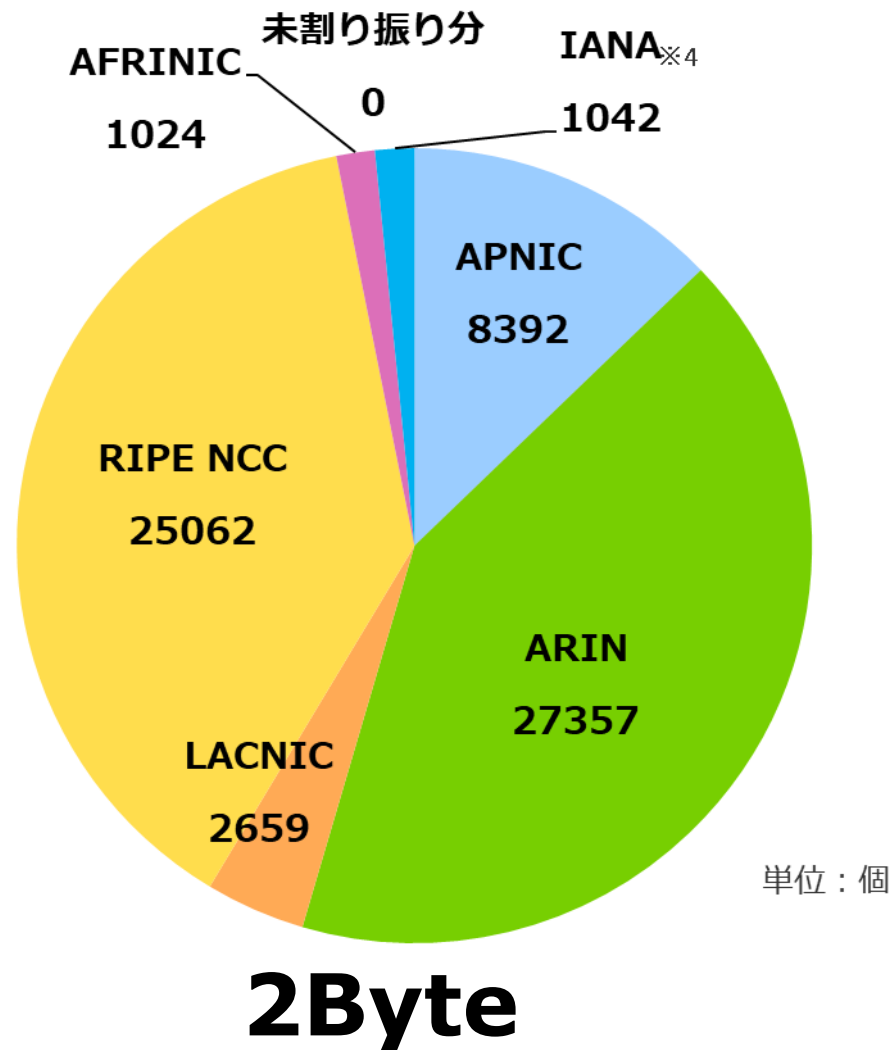
- IANA在庫は**8年前枯渇** (2016-07-29 RIPEが最後)
- RIRに若干の在庫があり4byte対応が困難な事業者向けには2byte配布中
- **JPNIC : 割り当て履歴のない在庫が枯渇、返却されたAS番号を再利用中**
2024年2月より、2ByteASの再割り当てを開始

- 4byteAS

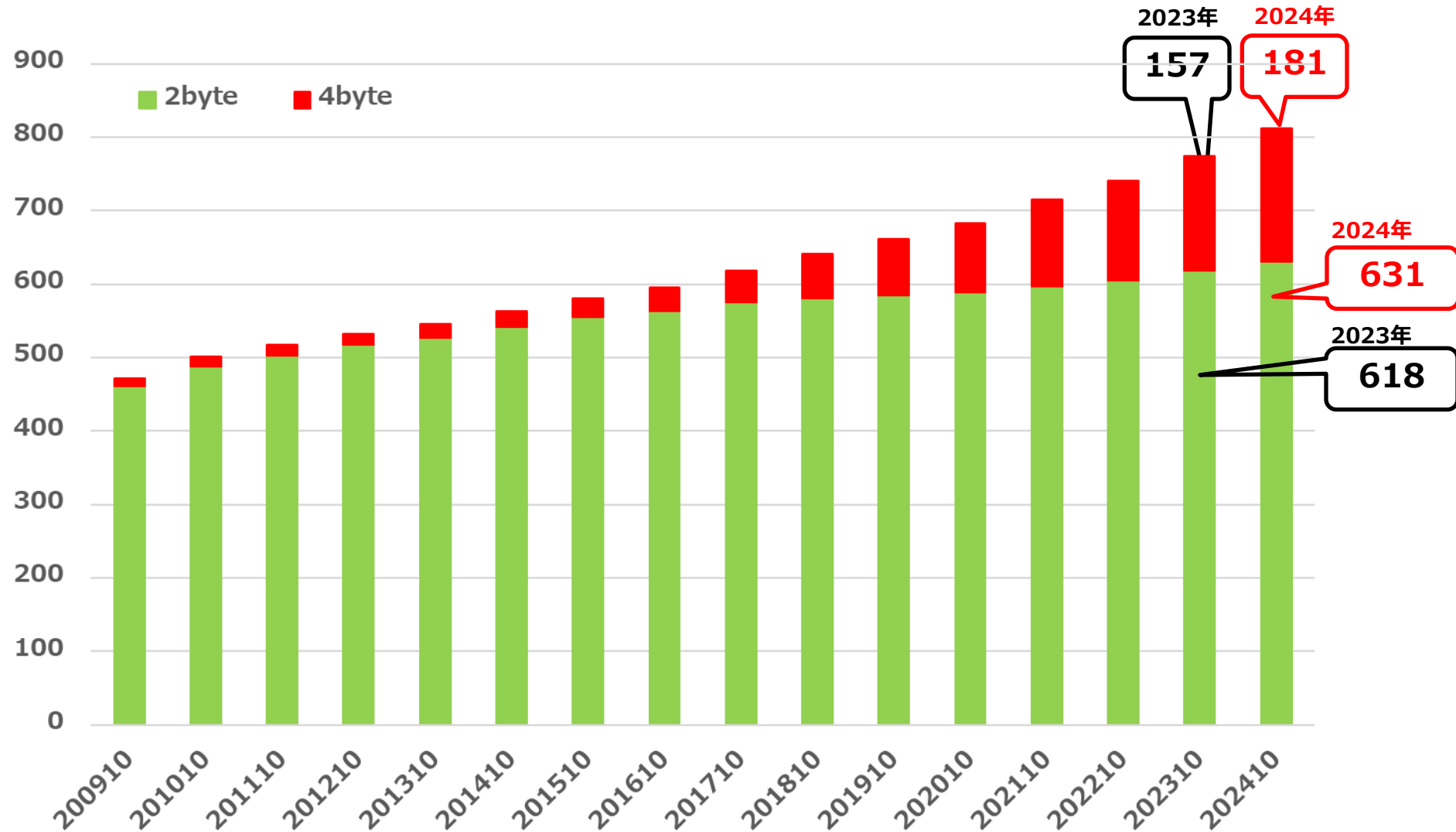
- 全世界的には4byteがほぼ主流、APNICもほぼ4byte
- 日本は大分浸透してきた
 - **上流ISPや自ASが4byteAS非対応のケースが若干あるが微量に**
 - 2020年 : 2byte : 4byte = 2:9 (4件 : 18件)
 - 2021年 : 2byte : 4byte = 3:8 (2020/11-2021/10 : 33件)
 - 2022年 : 2byte : 4byte = 5:9 (2021/11-2022/10 : 28件)
 - 2023年 : 2byte : 4byte = 1:2 (2022/11-2023/10 : 32件)
 - **2024年 : 2byte : 4byte = 1:2 (2023/11-2024/10 : 37件)**

AS番号の割り振り状況

4 Byte AS番号の旺盛な需要に応じてRIRへの割り振りも増加



JPNICのAS番号払い出し状況



JPNIC 統計情報データより

インターネットレジストリ関連トピック

ICP-2 新RIR設立要件の改定作業：「原則案」に対する意見募集が始まりました。(和訳付き)

<https://blog.nic.ad.jp/2024/10159/>

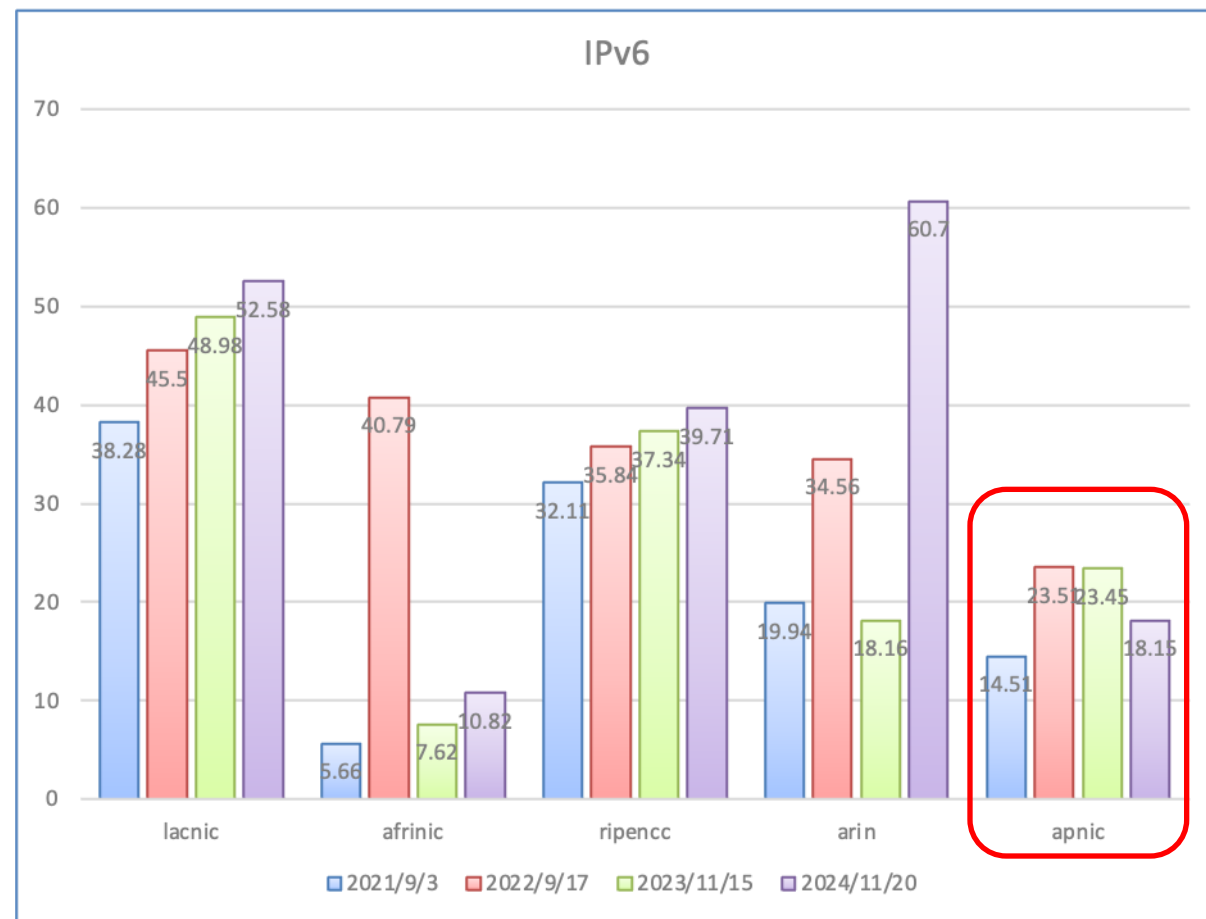
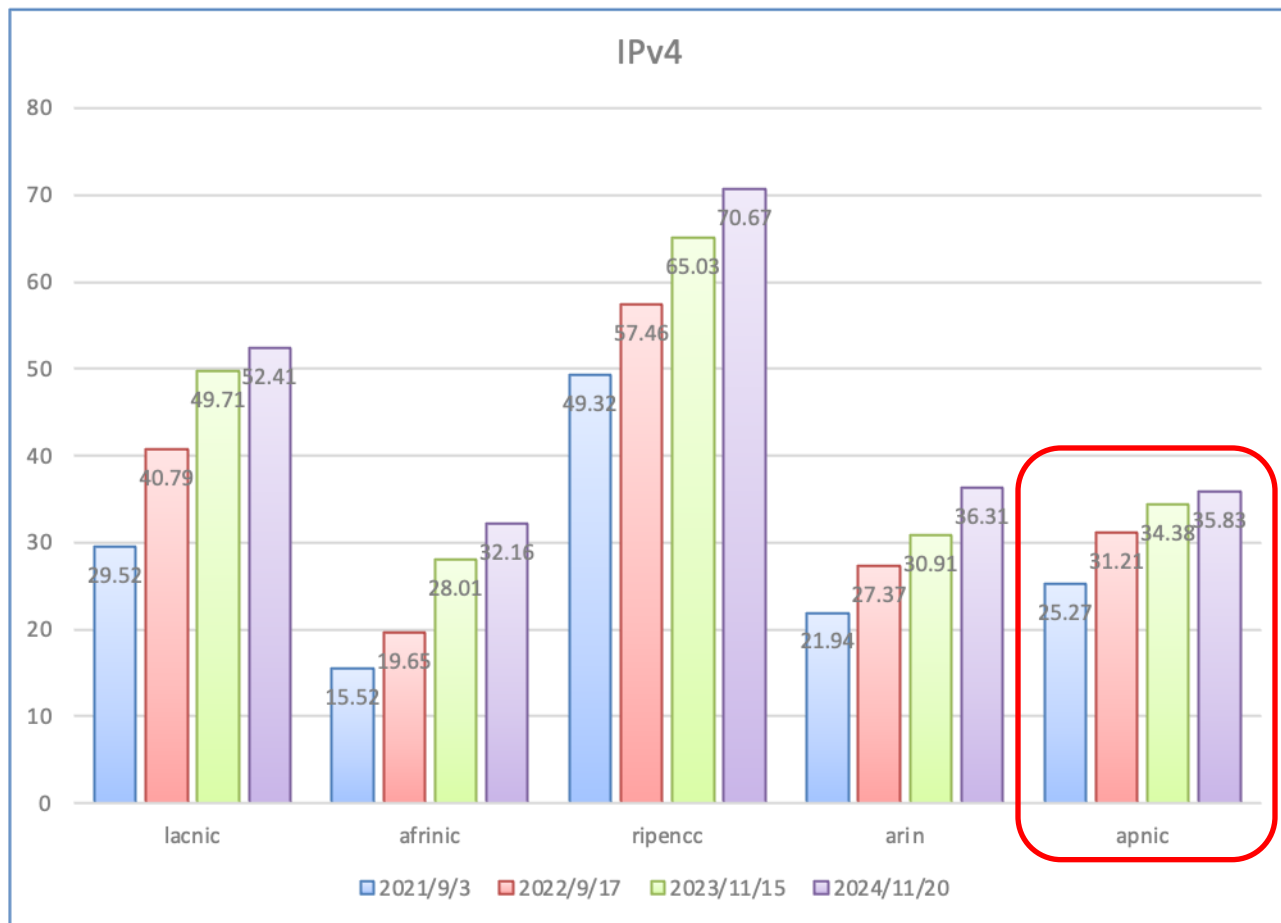
JANOG53:The Internetの運営機構を堅牢にするために

<https://www.janog.gr.jp/meeting/janog53/robust/>

地域インターネットレジストリの統治機構に関する2023年のまとめと2024年の展望

<https://blog.nic.ad.jp/2024/9469/>

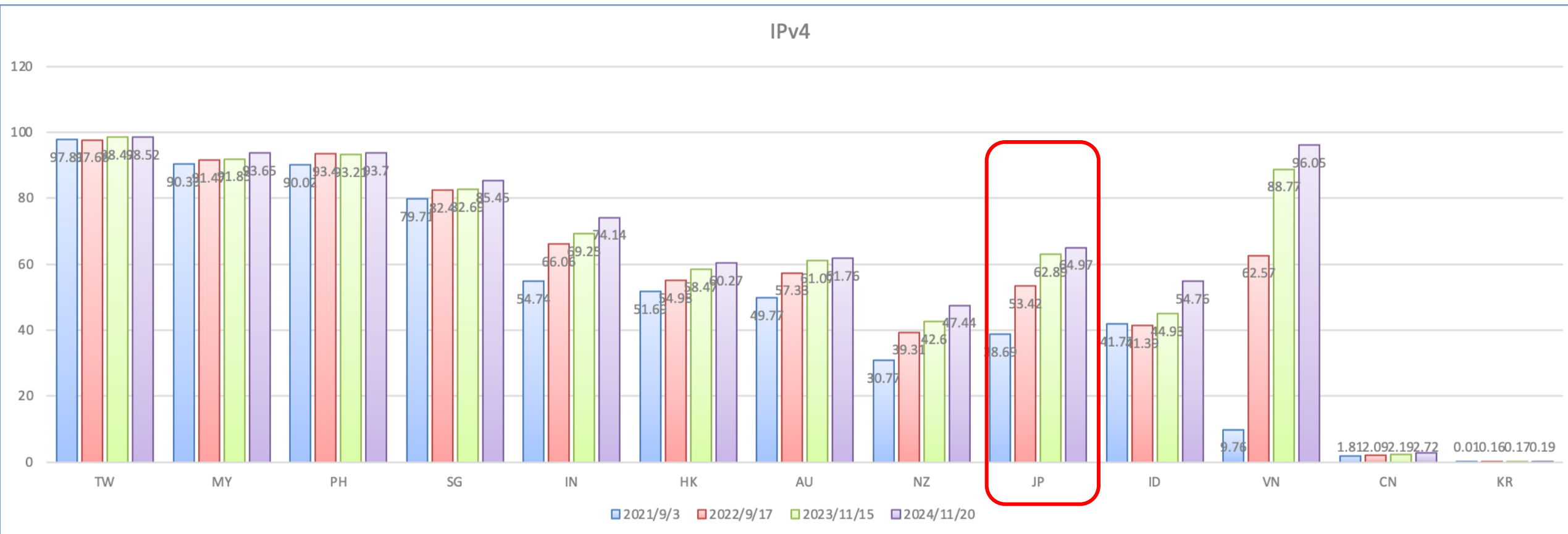
RPKI ROA登録状況 (RIR毎のROA登録率)



APNICのROA登録率は昨年と比べ、横ばい傾向?(IPv4:+1.25%/IPv6:-5.3%)

<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64.97%(前年比+2.08%)、歴史的にも埋蔵IPが多くある？

APNICリージョン諸国も概ね増加傾向だが、中国(CN)/韓国(KR)は国としての取り組みは見られず
韓国(KR)はOECD38か国中最下位 100億ウォン規模の予算申請をしたが2025予算案に反映されず。。

APNICリージョン主要国のROA登録率 (IPv6)

IPv6



日本(JP)は82.72%(前年比+1.73%)

APNICリージョン諸国は横ばい傾向。SGがなぜか2024/11/10から激減。(NROの集計間違い?)

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

国内Top10 ASのROAカバー率（2024年）

IPv4

IPv6

※ROA adoption rate for advertised routes:
2024/11/20時点の広報経路に対するROAカバー率

Rank	ASN	# of adv routes (/24units)	ROA adoption rate for advertised routes(*)	2023/11/15との増減
1	AS17676	158,449	95.03%	
2	AS4713	112,079	98.20%	+0.18%
3	AS2516	70,711	91.34%	-4.38%
4	AS2907	34,720	6.17%	+5.41%
5	AS17506	21,024	0.00%	0.00%
6	AS2527	15,044	100.00%	
7	AS2497	14,830	61.71%	+2.12%
8	AS2518	14,336	100.00%	
9	AS17511	11,952	0.00%	
10	AS9605	9,972	99.93%	+0.49

Rank	ASN	# of adv routes (/64units)	ROA adoption rate for advertised routes(*)	2023/11/15との増減
1	AS17676	18,695,992,639,488	100.00%	
2	AS9595	4,410,931,412,992	0.00%	
3	AS4713	4,406,636,511,233	99.90%	
4	AS2516	2,757,369,069,568	99.84%	+20.09%
5	AS2527	141,733,920,768	100.00%	
6	AS2519	103,079,215,104	0.00%	
7	AS55391	73,014,444,032	100.00%	
7	AS55392	73,014,444,032	100.00%	
9	AS9370	68,719,476,736	100.00%	
9	AS63784	68,719,476,736	100.00%	

昨年と比べ、IPv4/IPv6ともに広報経路数のランキングに大きな変動なし。
(昨年、IPv4広報数が11位だったAS9605が10位へ上昇)

AS2516(KDDI)のIPv6登録率が上昇。

RPKIトピック

RPKIに関するガイドライン案について



総務省「サイバーセキュリティタスクフォース政策分科会」
「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」
事業の中で「RPKIに関するガイドライン案」が公開されました。

総務省 | サイバーセキュリティタスクフォース | ICTサイバーセキュリティ政策分科会 (第5回) (soumu.go.jp)
https://www.soumu.go.jp/main_sosiki/kenkyu/cybersecurity_taskforce/02cyber01_04000001_00286.html
参考資料2・RPKIのROAを使ったインターネットにおける不正経路への対策ガイドライン案
https://www.soumu.go.jp/main_content/000941397.pdf

RPKI(ROA/ROV)導入に関するさまざまな点を考慮に入れて策定いたしました。
ぜひ、ご一読を。

2024/5/31 janog53.5 RPKIホットトピック 渡辺英一郎氏の資料より



2024/11/13にJPNIC HPで公開

<https://www.nic.ad.jp/doc/jpnic-01324.html>

RPKIトピック

- ❑ RIPEアカウントを乗っ取られ、不正なROAが登録され経路ハイジャックされる（2024/01）
安易なID/PW利用、2FA無、端末のマルウェア感染で情報流出
- ❑ JPNIC CA障害（2024/04）
CA(rpki-repository.nic.ad.jp）がダウンしROAキャッシュサーバからアクセス不可に
証明書/ROAのDLがNGになった。。
- ❑ LACNIC CAリプレース（2024/04）
古いversionのROAキャッシュサーバだと、LACNICからのROA検証ができない事案あり
新しいversionに更新することをおすすめ
- ❑ 米国でのBGPセキュリティ規制化？（2024/05）
米国での経路ハイジャックによるセキュリティインシデント事例に対してFCCがすべてのBIAS（
Broadband Internet Access Service）事業者にはRPKI導入計画や進捗を記述したプラン作成の義務化
上位9社のサービスプロバイダに対し、四半期ごとに公開データを提出すること

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

2024年 DNSトピック

- ドロップキャッチ案件
 - .mobiのレジストリサービス用旧ドメイン名 (dotmobiregistry.net) がドロップキャッチ (2024年9月)
 - watchTowrの調査チームが2023年12月に期限切れになっていたことを発見し取得
 - whoisサーバーを設置すると大量のクエリーを受信。政府機関・サービスサイト・認証局などが送信元に含まれており、不正な応答による攻撃や、.mobiドメイン名のサーバー証明書の発行が可能な状態になっていた
 - 鹿児島県で利用していた複数のドメイン、コロナ関連の支援金サイトなど公共性の高い多数のドメインが対象に
- 「.io」ドメインが消失？
 - 「.io」：イギリス領インド洋地域(チャゴス諸島の周辺地域)に割り当てられたccTLD
 - イギリスがチャゴス諸島の返還を決定したため、「.io」ドメインの存続が不安視される事態に
 - ICANNの声明によると、現時点では単なる憶測、しかるべき対応はきちんと適切な時間をかけて実施
- KeyTrap (2024年2月)
 - フルリゾルバーに負荷の高いDNSSEC検証処理を強いるDoS攻撃手法、bind影響大
- gTLDにおけるDNS Abuse対応義務の明文化 (2024年4月)
 - マルウェア、ボットネット、フィッシング、ファームウェア、spamの5つを悪用項目に定義し対応義務化
 - .topレジストリがDNS Abuse違反についてICANNから全体通知された (2024年7月)
- 次回のルートゾーンKSKロールオーバーの日付発表
 - 2025年1月11日：次のKSK「KSK-2024」がルートゾーンに出現
 - 2026年10月11日：KSK-2024で署名開始 (ロールオーバー)
 - 2027年1月11日：現在のKSK-2017を失効

【注意喚起】鹿児島県が使用していたドメインが第三者に再取得され、別のホームページで使用されていることを確認しました

鹿児島県が過去に使用していたドメイン（ホームページアドレス）について、事業終了等に伴う運用停止後に、第三者に再取得されていることが判明しました。

下記ドメインを使用したホームページは、本県とは全く無関係ですので、ご注意ください。

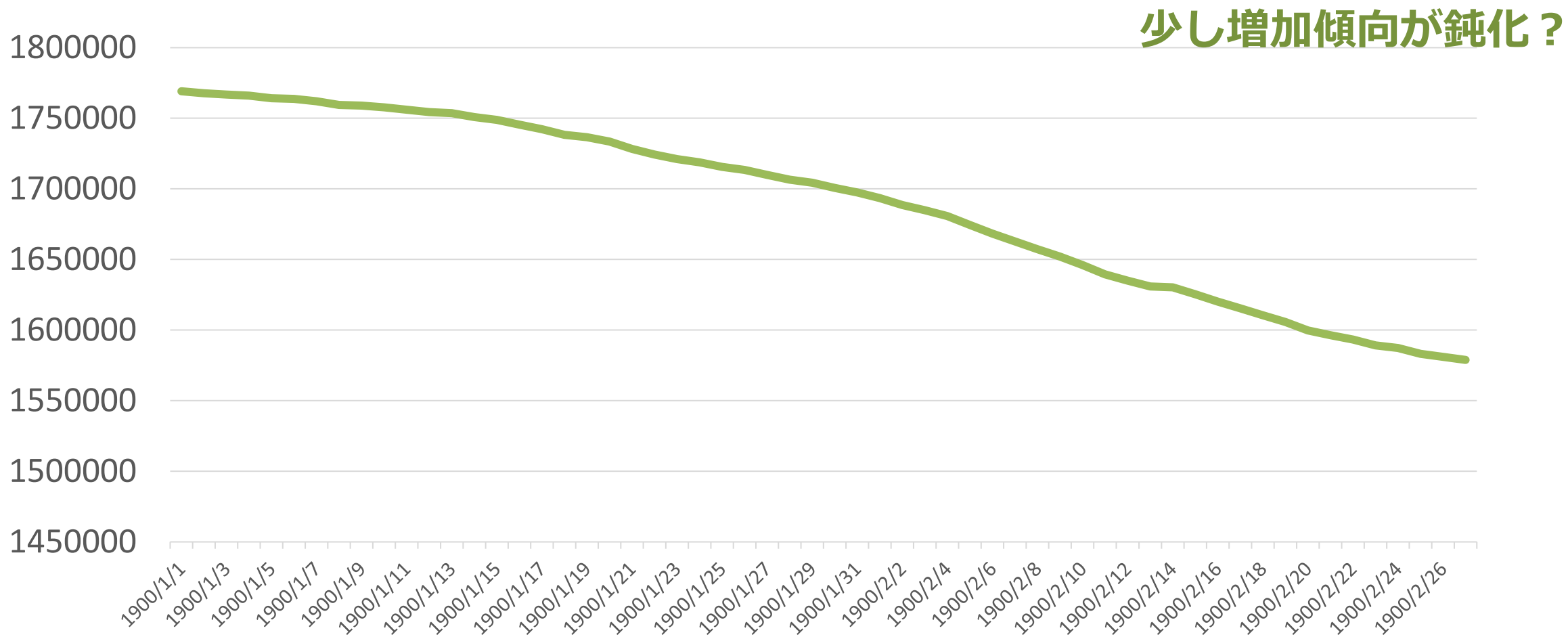
1 第三者に再取得されたドメイン

- kagoshima-wellness.net（かごしまのウェルネス）【総合政策課計画管理室、産業人材確保・移住促進課】
- kg-rakumegu.com（らくらく鹿児島巡り事業（R3年度））【PR観光課】
- kagoshima-rakumeguri.com（らくらく鹿児島巡り事業（R4年度））【PR観光課】
- greboo-coupon.jp（ぐりぶクーポンに関する広報）【商工政策課】
- kagoshima-online.com（令和2年度合同企業説明会特設サイト”鹿児島で働かんげー？”）【産業人材確保・移住促進課】
- kagojobfair.net（令和3年度合同企業説明会特設サイト”かごしまJobフェア”）【産業人材確保・移住促進課】
- amamiryukyu.ip（時を紡ぐ彩りの島 奄美・琉球）【PR観光課】



出典：鹿児島県HPより

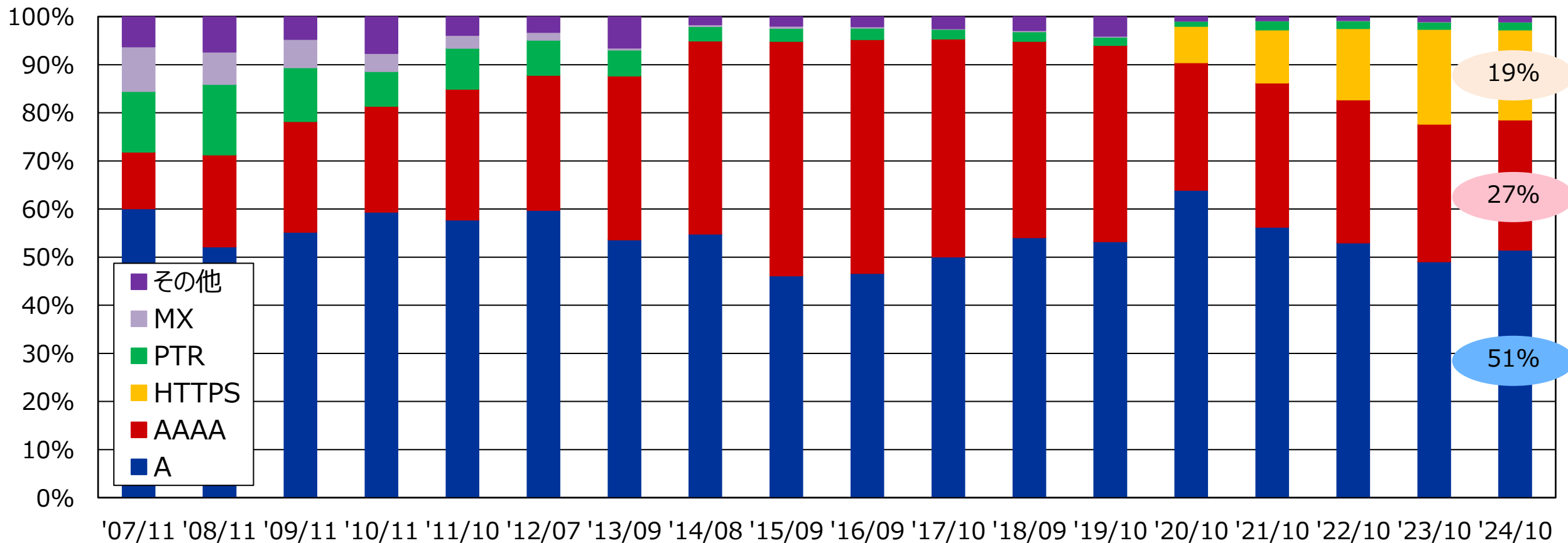
JPドメイン数の推移



JPRSの公開データより作成

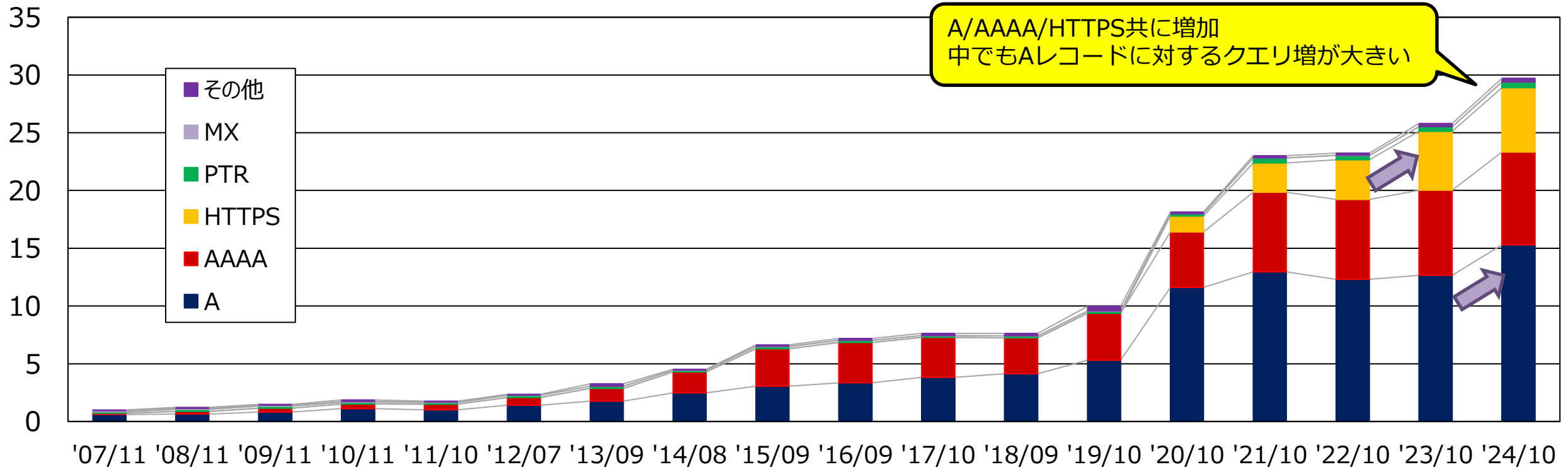
OCNユーザのクエリタイプ毎の割合推移

- A + AAAA + HTTPSの3レコードで約**97%**
- HTTPSレコードへのクエリは去年まで増加傾向だったが今年には割合に変化なし
 - クライアント(ブラウザ)のHTTPSレコード対応が十分に普及した？



OCNユーザからのクエリ数の推移

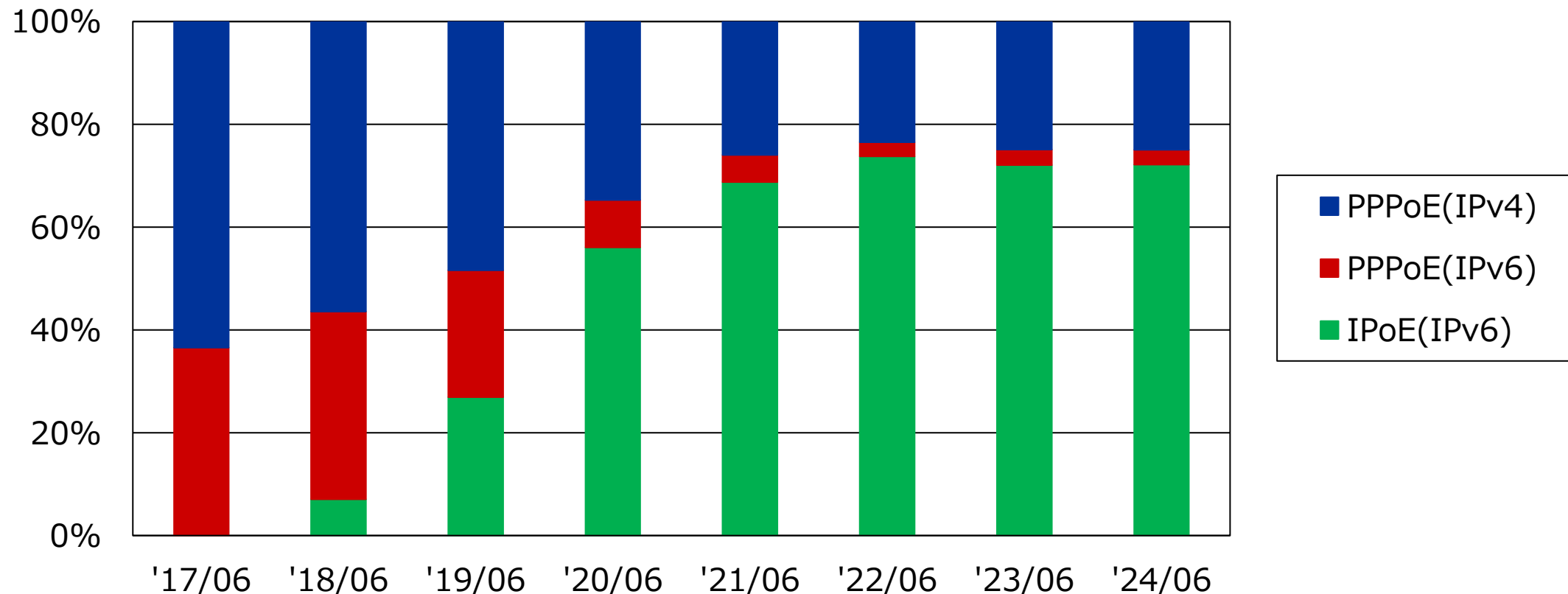
- 割合的には微増だがAレコードは数としては増加傾向に
 - Aレコード：21%増、AAAAレコード/HTTPSレコード：共に9%増
- クライアント(やブラウザ)の挙動変化が原因か、それともWEBページに含まれるドメイン数が増えたのか、詳細は不明



※縦軸は'07/11の値を1とする

OCN DNSのIPv4/IPv6のトラフィック割合

- DNSトラフィックのクエリ数をカウント(平日のピーク時間帯)
- IPoE(IPv6)のDNSクエリは70%超



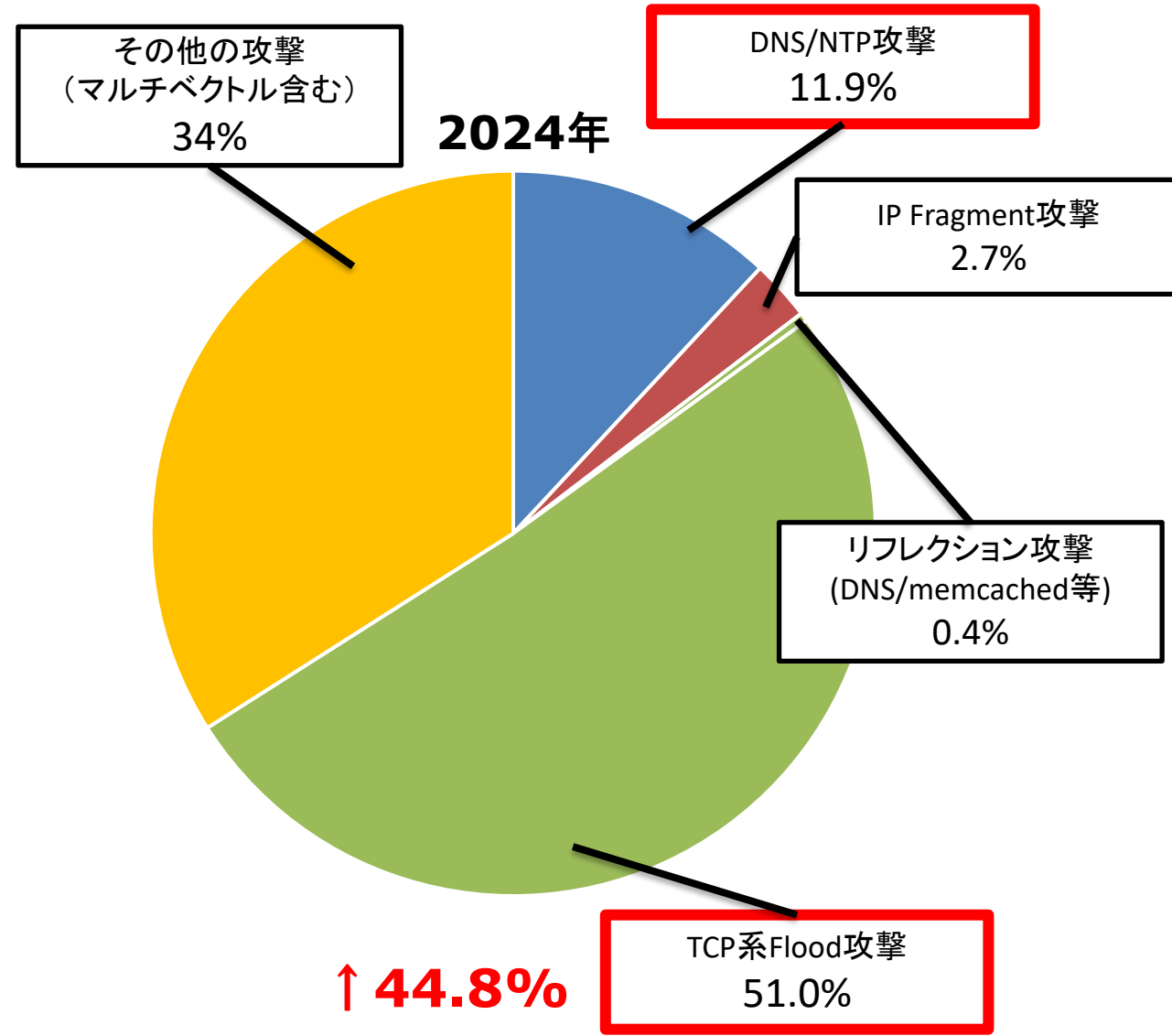
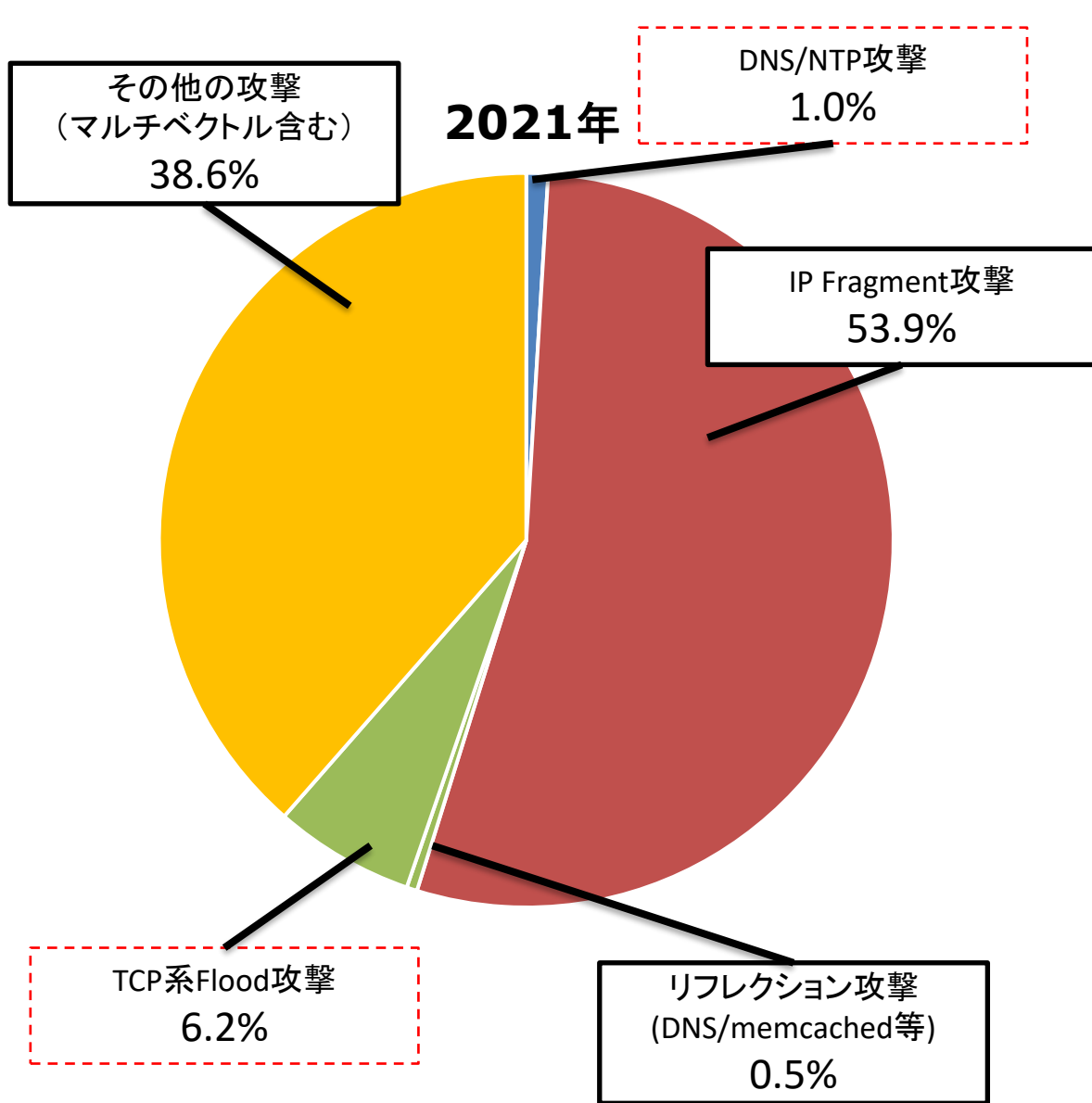
内容

- 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

2024年セキュリティ動向

- ランサムウェアによる被害／実害報告が多数発生（明日は我が身）
 - 標的型攻撃、サプライチェーンを狙った攻撃、業務停止に至るまで多数
 - 個人情報、顧客情報の搾取
 - DDoS攻撃との組み合わせにより攻撃検知の複雑化
- DDoS攻撃のトレンド
 - 完全にビジネス化されておりターゲットの弱点をついた攻撃が誰でもお安く簡単に、、
 - 攻撃コードをAIで作成する事例も出てきた
 - 親ロシア派のハクティビストによる攻撃で日本が複数回主要ターゲットに
 - 1Tbpsを超える大量の攻撃から、少量で観測や対処が困難な攻撃までバリエーションも多数
 - 古典的な増幅型（反射）攻撃、脆弱なbotを活用した大規模攻撃まで
- 政治要因による攻撃の増加
 - ロシアウクライナ侵攻 反ロシアに対する攻撃
 - イスラエル・ガザ戦争 イスラエル支援国に対する攻撃
 - 中国 vs アメリカ（台湾／日本）

OCNでの攻撃種別 (2021/2024年の比較)



Noname057(16)によるDDoS攻撃 (宣言)

主要要因

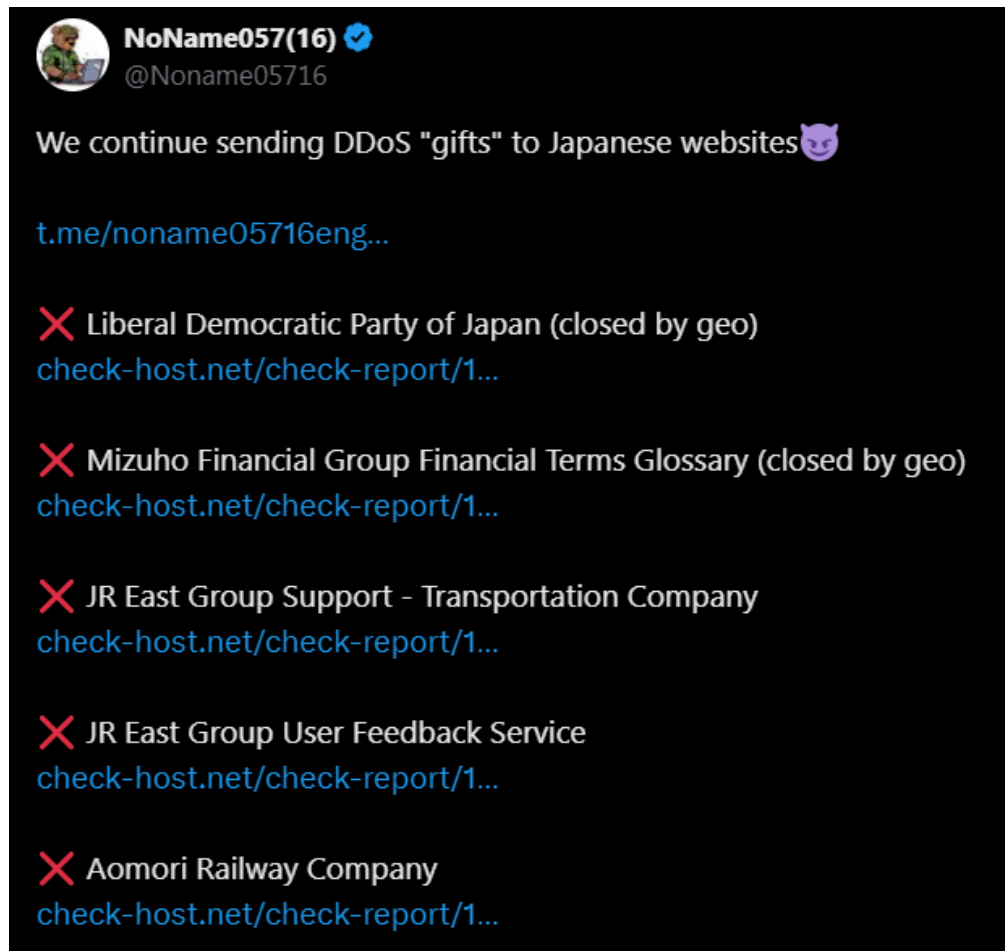
政治的背景

ターゲット

主要インフラ

公共機関

大企業など



(事例)

弊社のお客様へ
攻撃予告通り
攻撃開始

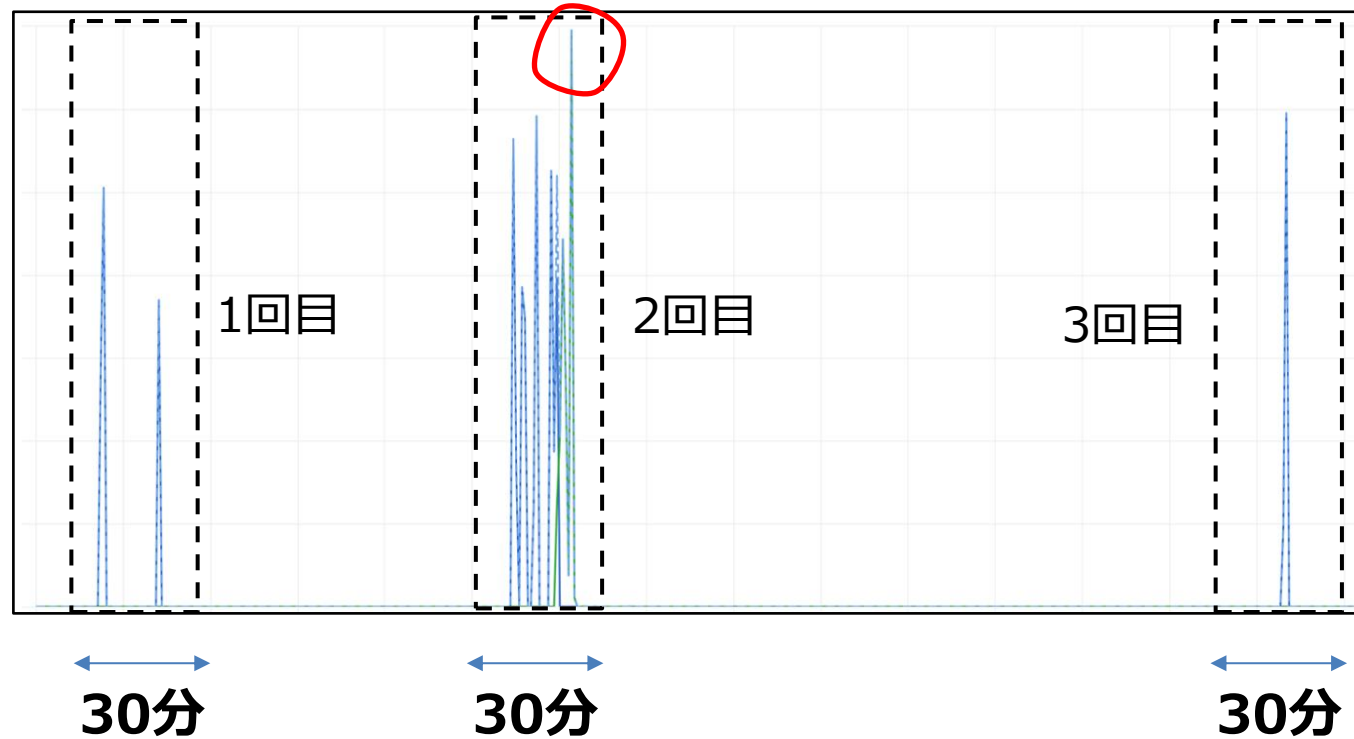
少量DOSにより
検知防御が困難

予告情報を元に
社内連携し通信確
認や防御策を講じ
先手で対処

<https://x.com/Noname05716/status/1813146578393190700>

超絶驚きの攻撃がやってきた事例

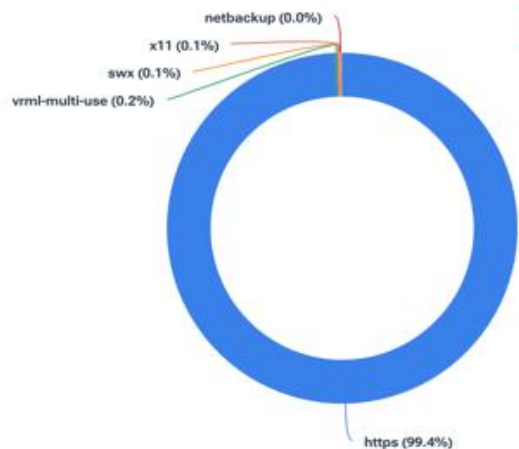
最大1.4Tbps



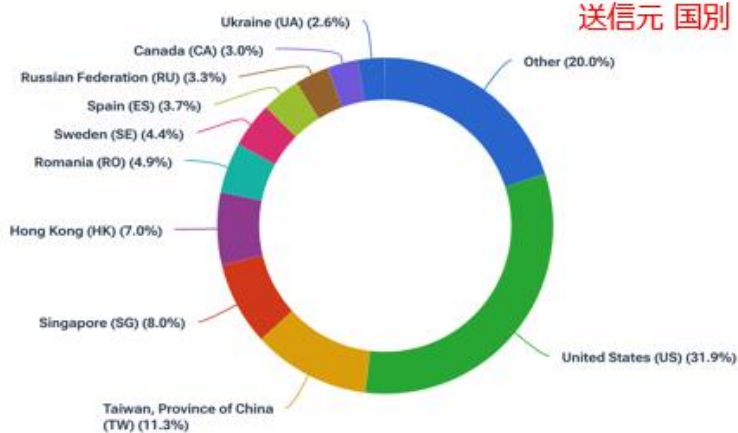
超絶驚きの攻撃がやってきた事例

全てIPv4、99% HTTPS/TCP443

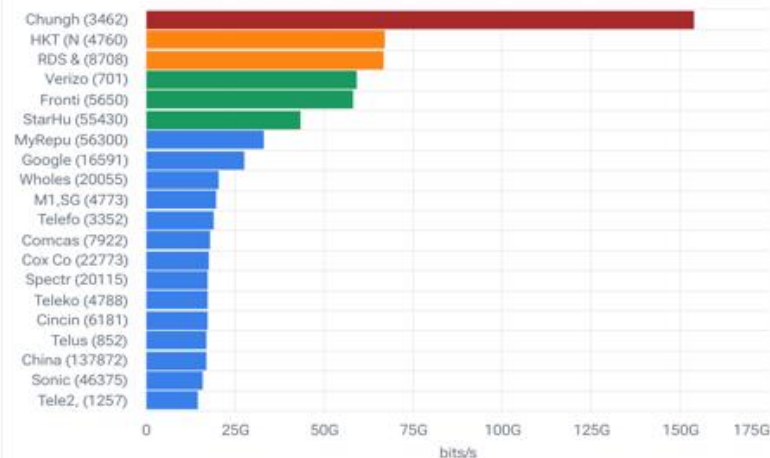
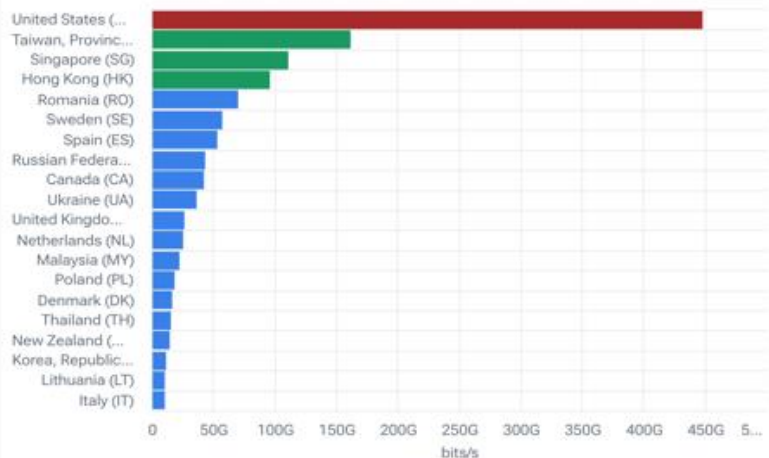
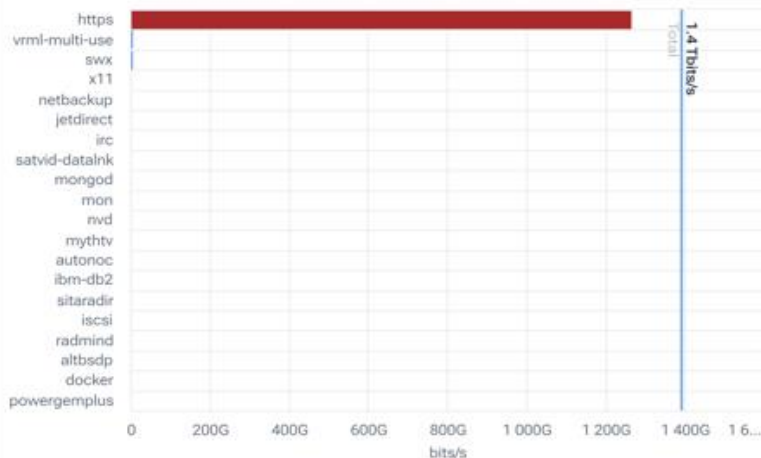
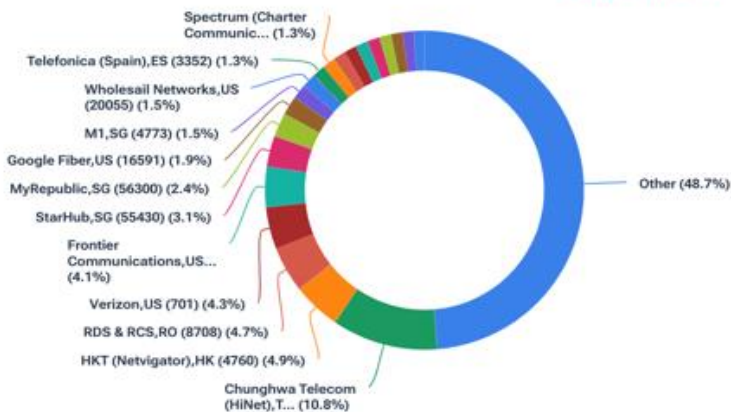
プロトコル別



送信元 国別



送信元 AS別



その他攻撃の傾向

■ DDoS攻撃トレンド

- DNSサーバへの攻撃増加
→DNS水攻め攻撃の流行
(DNSランダムサブドメイン攻撃)
- TCP系Flood攻撃の増加・大容量化
→TCP Floodで1Tbps超えの攻撃を観測
- ボリューム攻撃orターゲティングした攻撃
→対策がしづらい攻撃が多い

G7サミットでのDNS水責め攻撃例(マイナビ社 記事)

TECH+ > 企業IT > セキュリティ > サイバー攻撃「水責め」の恐怖、G7も襲ったDDoS攻撃を解説【前編】
レポート

サイバー攻撃「水責め」の恐怖、G7も襲ったDDoS攻撃を解説【前編】

掲載日 2024/05/21 07:00 著者：金子春信

f x  

サイバー攻撃 標的型攻撃 サーバ

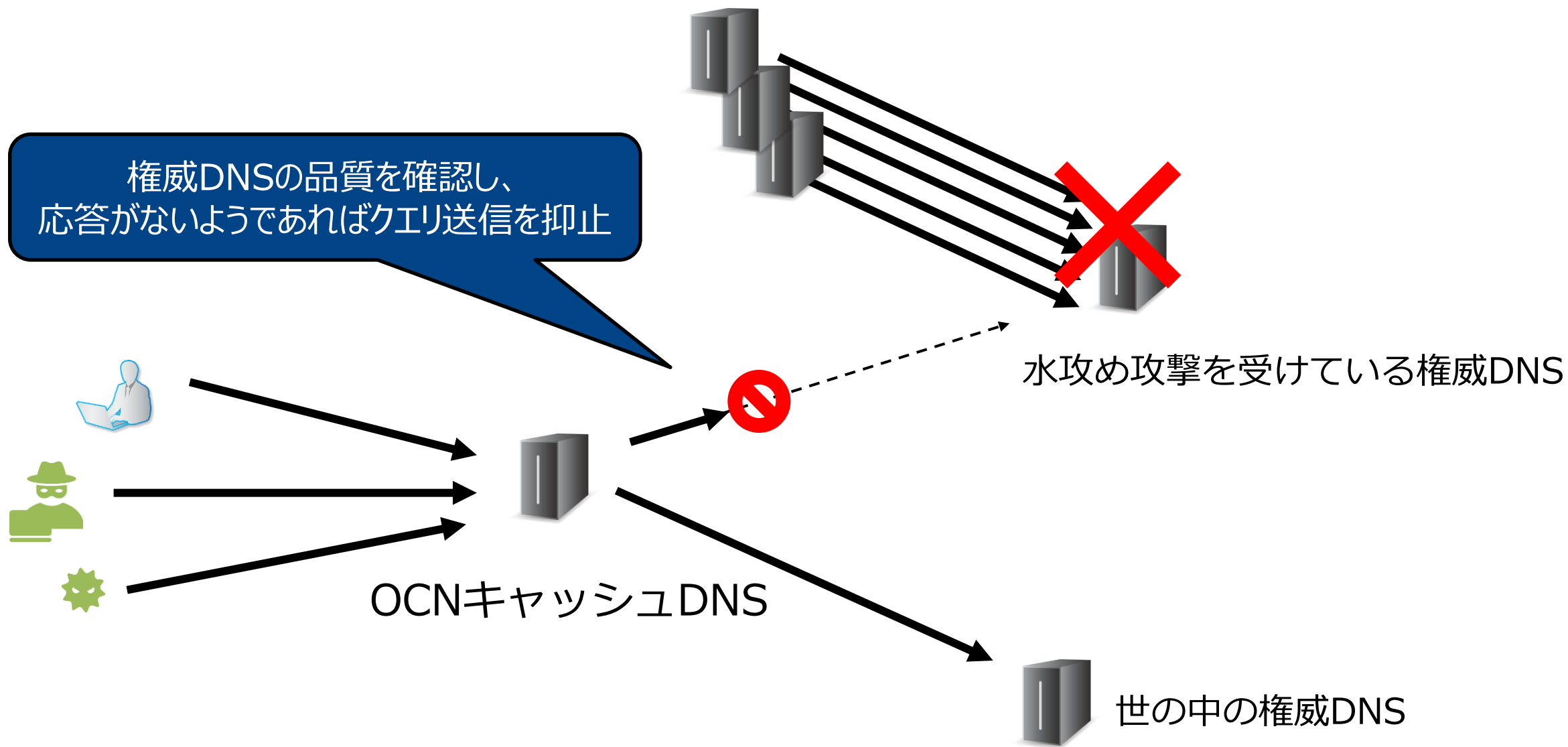
三 目次

- ・日本と世界での被害動向
- ・水責めの標的「DNS」とは?
- ・なぜ被害が続くのか?

「水責め」という恐ろしい名前のサイバー攻撃があるのをご存知でしょうか。これは元々アメリカで「DNS Water Torture Attack」と名付けられ、それが和訳された呼び名です。水を顔に浴びせたり大量に飲ませたりする拷問を語源として命名されたというなんとも恐ろしげな攻撃です。

出典) <https://news.mynavi.jp/techplus/article/20240521-2946840/>

OCNキャッシュDNSが攻撃に加担しないための対応



DDoS防御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

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

2024年のまとめ

- **トラフィック動向**
 - コロナの5類移行も落ち着き、2024年はコロナ以前の傾向に戻ってきた印象
 - ゲームDLやイベント時の通信量増加（ボクシング、WBC等）は以前継続も業界連携し対応
 - IPv6へのトラフィック移行は緩やかで、現傾向が継続する場合はIPv4/v6が長期共存
- **ルーティング動向**
 - IPv4は多少鈍化傾向だが96.7万経路に到達、2026年上期に100万経路が見えてきた
 - IPv6は経路は緩やかに順調増加、IPv6が全体の18%へ
 - 日本におけるRPKIによる経路情報の信頼向上施策も徐々に浸透、ROVは課題
- **DNS動向**
 - ドメインのドロップキャッチは要注意（ドメインの計画的ご利用を）
 - HTTPSレコードはA/AAAAに続き3番目に多く全体の2割に定着
 - 全体のクエリ数は依然として増加傾向、クエリ増加に伴う設備増強は継続的に必要
- **セキュリティ動向**
 - ランサムウェアによる被害が顕著、各企業で各々対策が必要
 - DDoS攻撃も政治的要因や標的型攻撃で多数発生、被害の抑止と共に加害者にならないように
 - 明日は我が身なので、普段から検知防御の対策や仕組みを導入ししっかり備えることが寛容