キャッシュ DNS Update
～今年のトレンド～

2015/11/19
Internet Week 2015 DNS DAY

NTTコム エンジニアリング株式会社
サービスネットワーク部 サービスネットワーク部門
西岡 孟朗
takeaki.nishioka@ntt.com

Index

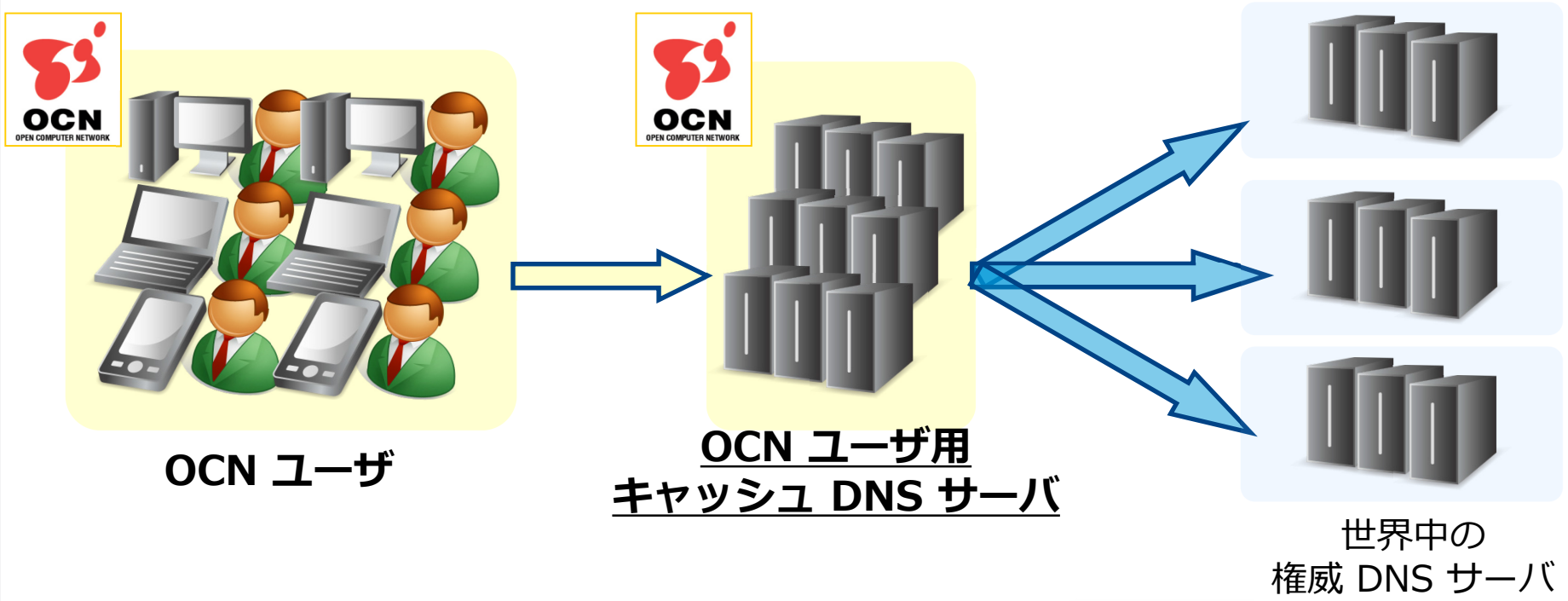
■ 長期的傾向
- ユーザクエリの変動

■ 最近のトピック
- DNS ランダムサブドメイン攻撃 (水責め攻撃)
- TLD 関連
- モバイルユーザからのクエリ

長期的傾向

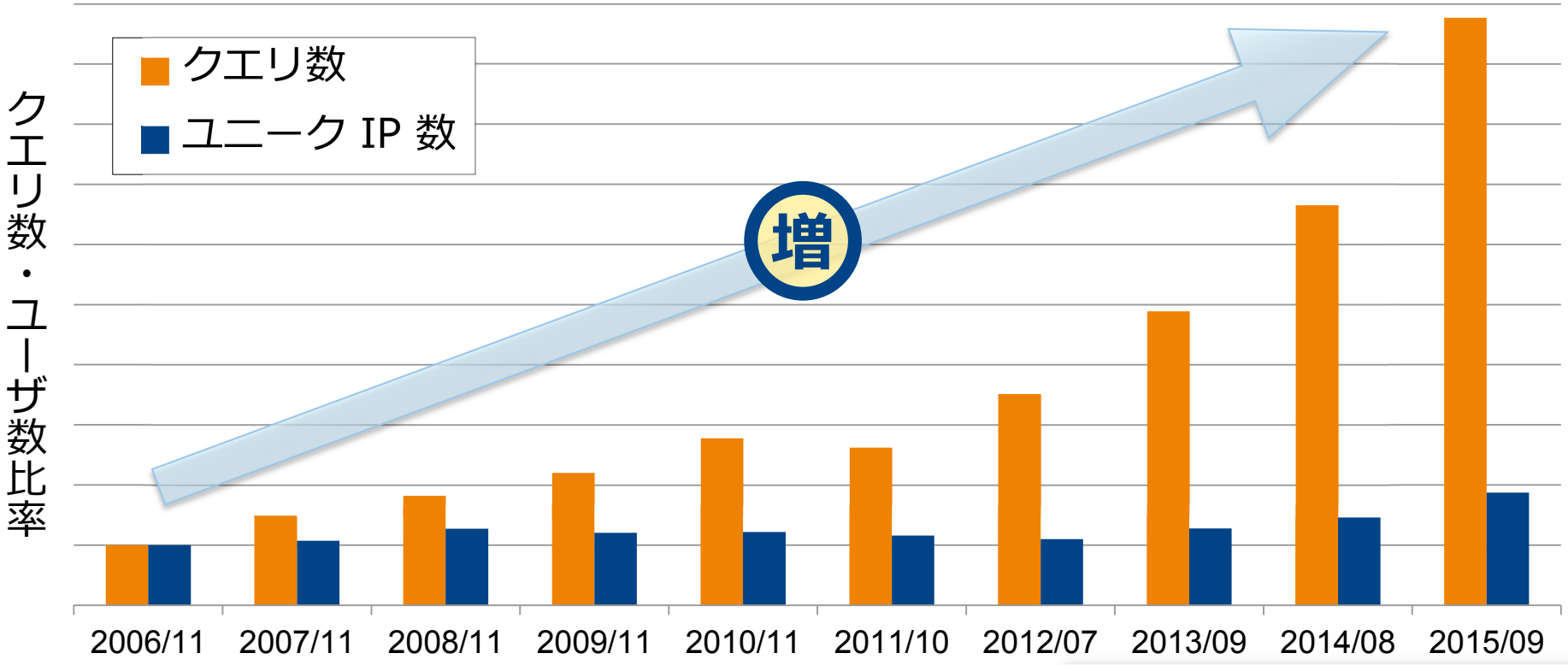
OCN の キャッシュ DNS

- OCN ユーザ数　　：**約800万**
- ユーザからのクエリ数　　：**約360億 / 日**
- キャッシュ DNS サーバ数：**数十台**



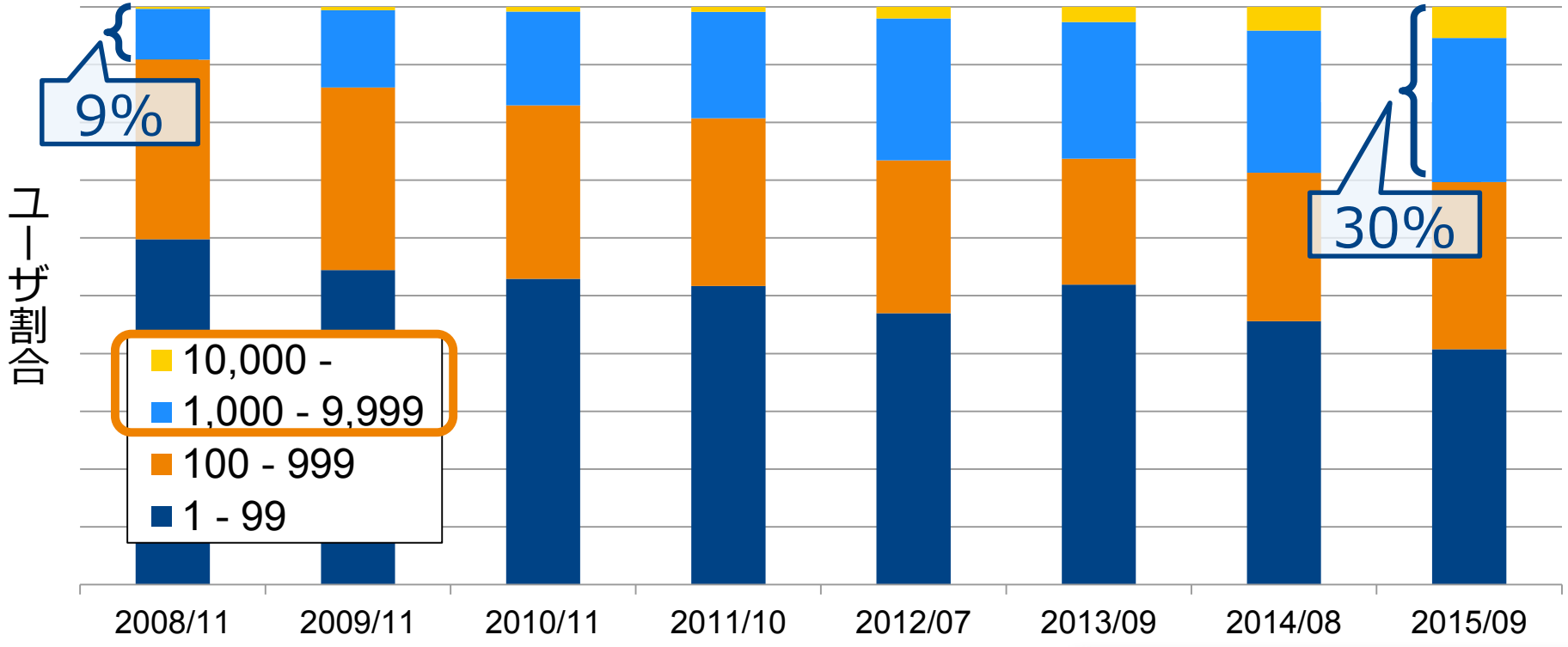
ユーザからのクエリ数・ユーザ数

- 2006 年と比べてクエリ数は 10 倍弱
- ユーザあたりのクエリ数が大きく増加している



一日のクエリ数別ユーザ割合

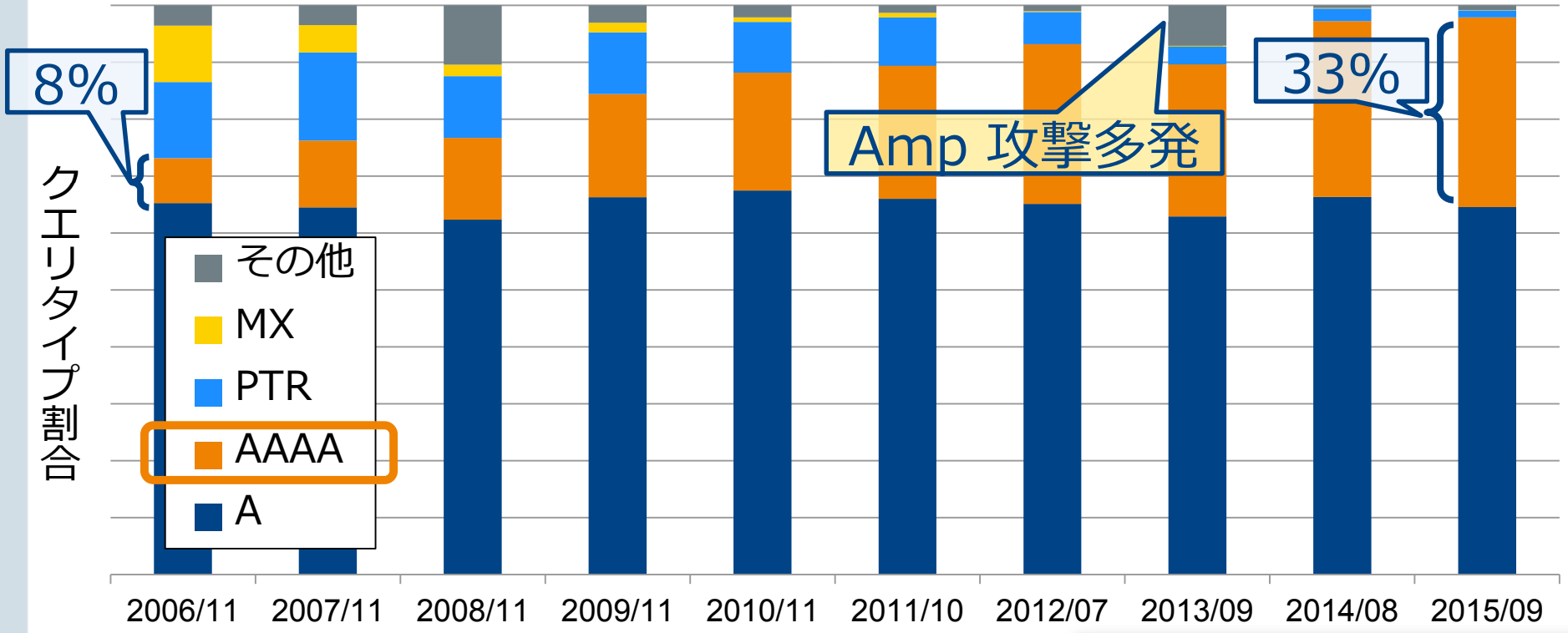
- 1,000 クエリ / 日以上のユーザ割合が増加傾向
  - Web ページの複雑化、ブラウザのプリフェッチ
  - スマホの Wi-Fi オフロード普及も一因か*



* 2014/11 の調査によれば、自宅に固定回線を持つスマホ利用者の約7割が自宅ではWi-Fiを利用
“http://www.soumu.go.jp/menu_news/s-news/01iicp01_02000028.html”

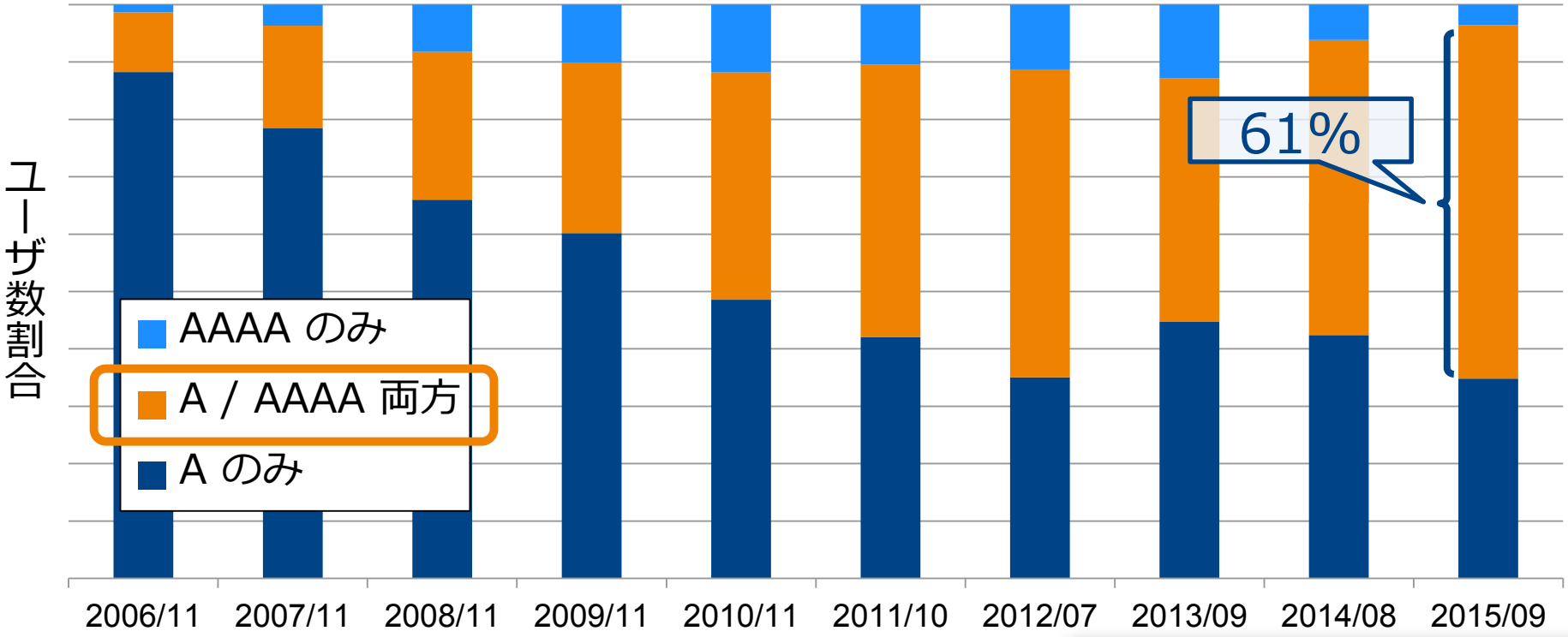
ユーザからのクエリのクエリタイプ

- AAAA が増加、A と AAAA だけで 98% を占める
  - AAAA の割合は 2006 年の 4 倍以上に増加
  - 2013 年の「その他」は Amp 攻撃の ANY クエリ



AAAA クエリ送出ユーザの割合

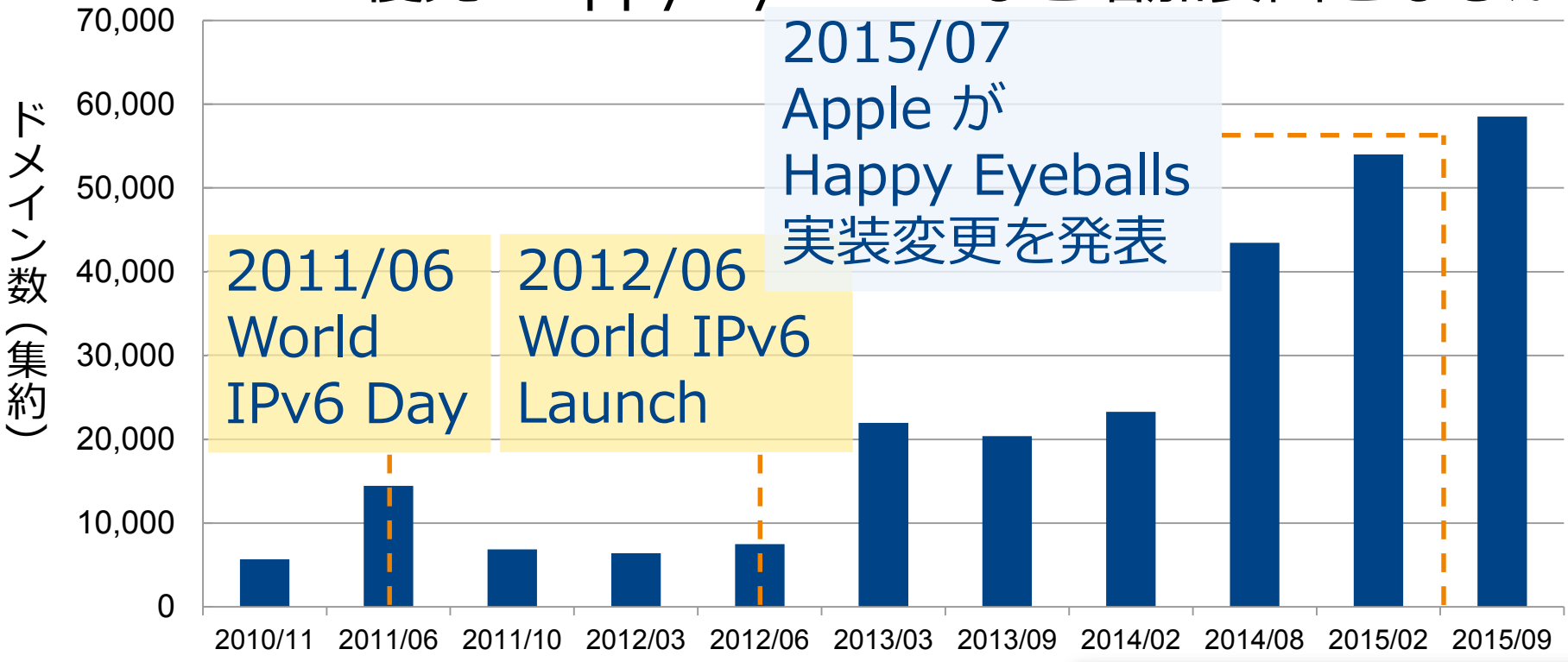
- 「A/AAAA 両方」ユーザ割合は引き続き増加傾向
- IPv6 対応 OS の普及が進んでいる
  - WinXP シェアは 12% に低下* (昨年のほぼ半分)



* 2015/09 時点 “http://www.netmarketshare.com/operating-system-market-share.aspx”

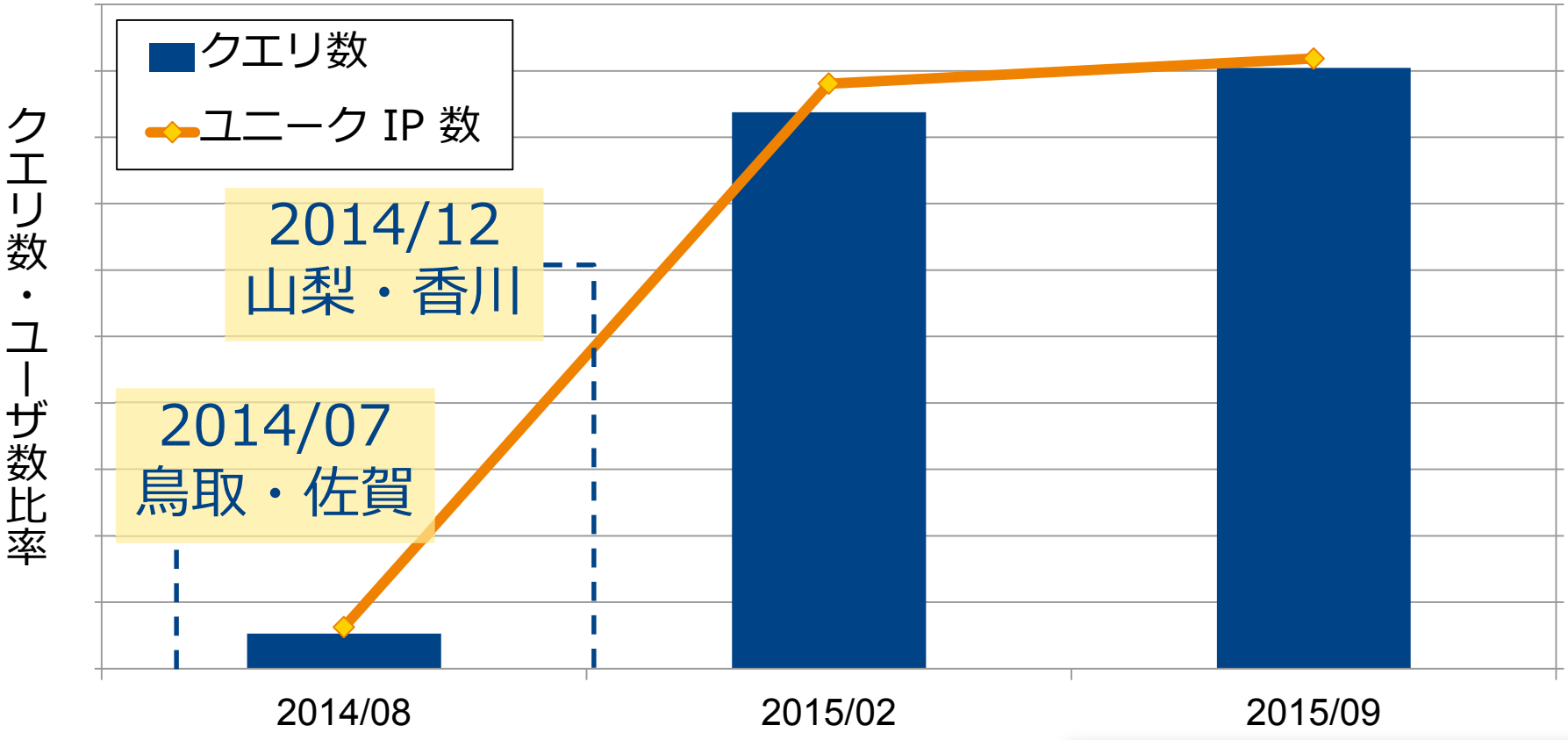
AAAA つきドメイン数 (組織別集約)

- example.com, example.co.jp などの単位で集約
- W6L 後増加傾向が続いている
  - IPv6 優先 Happy Eyeballs など増加要因となるか



IPv6 トランスポートのクエリ数

- ひかり電話ルータの自動接続対応エリアが拡大中*
- これに伴い IPv6 クエリはさらに増加する見込み

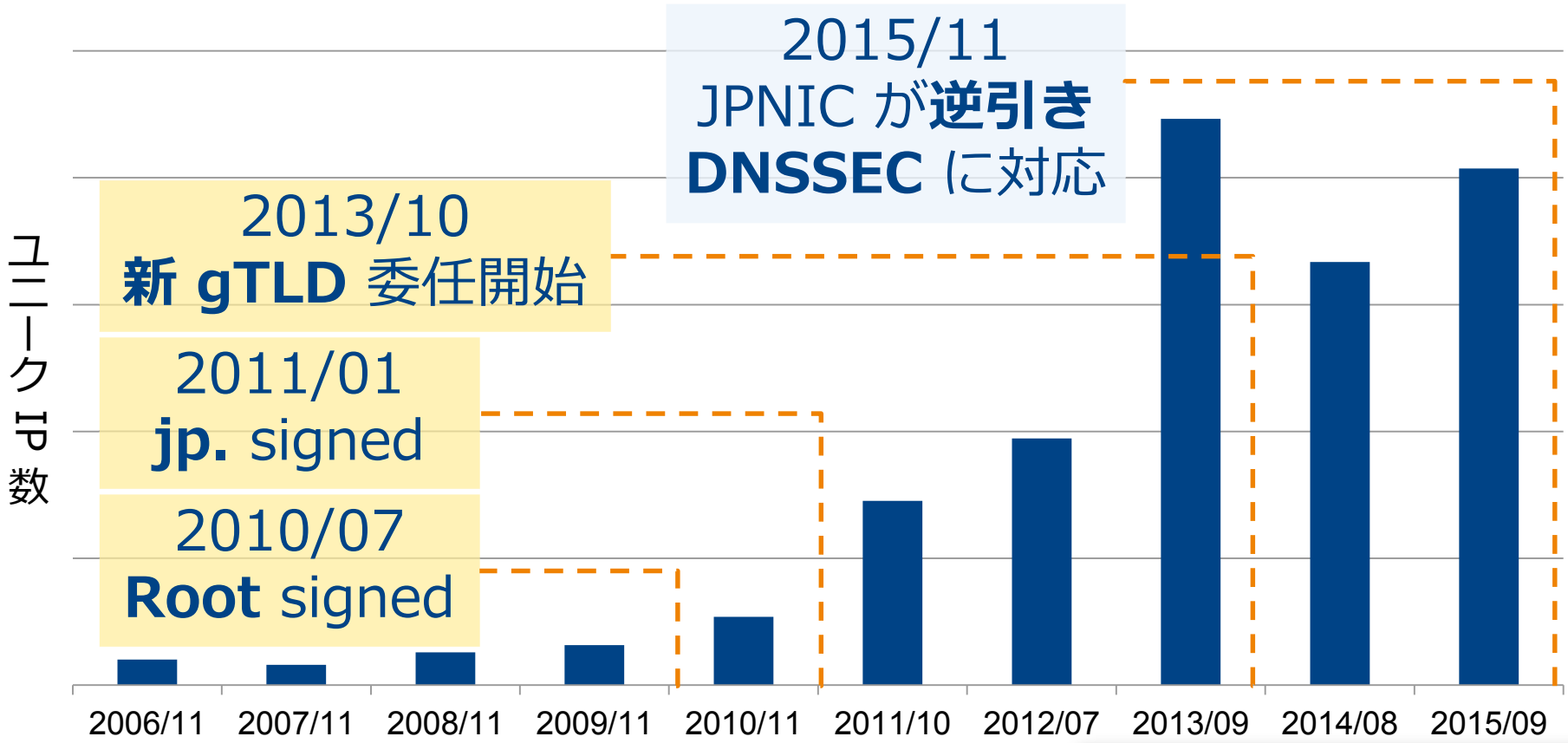


* “http://service.ocn.ne.jp/ipv6/access/”

NTT Communications Global ICT Partner Innovative. Reliable. Seamless.

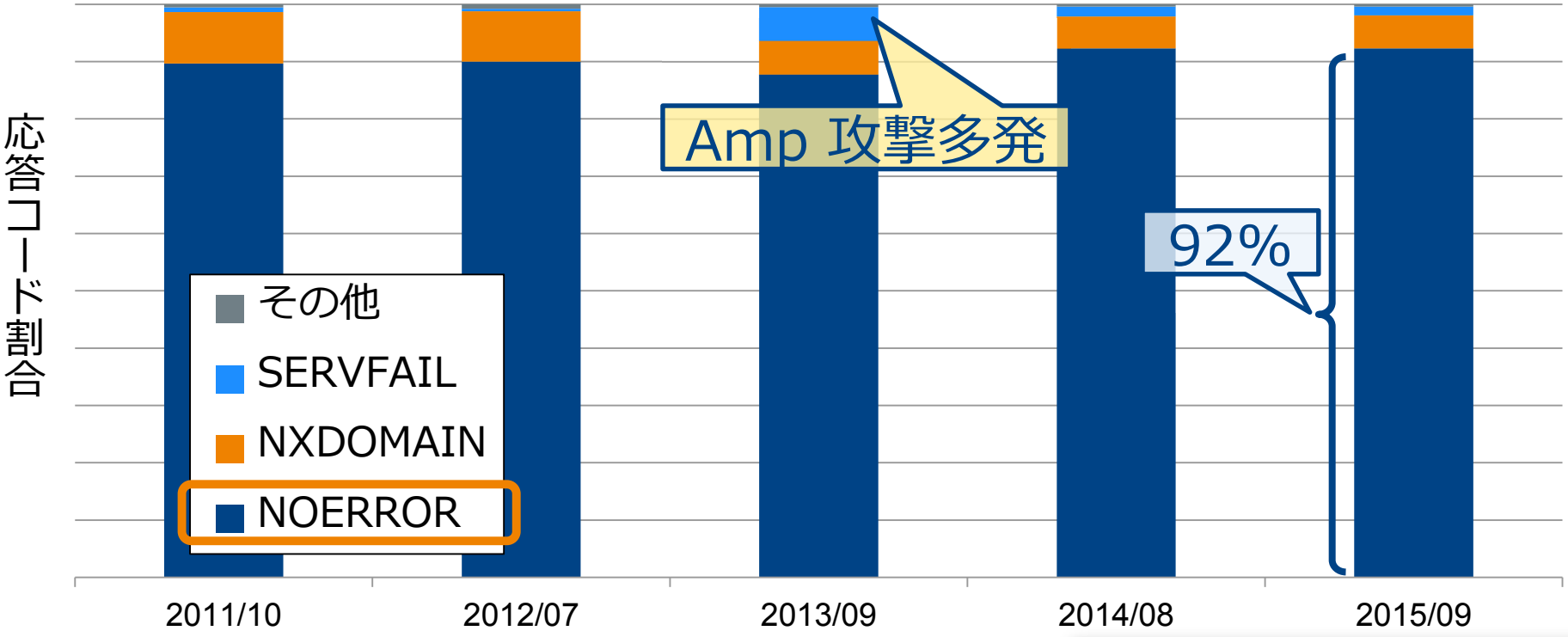
DNSSEC 対応クエリ送出ユーザ数

- DO bit つきクエリ送出ユーザは増加傾向
- 送出ユーザは総ユーザの 0.8% 程度



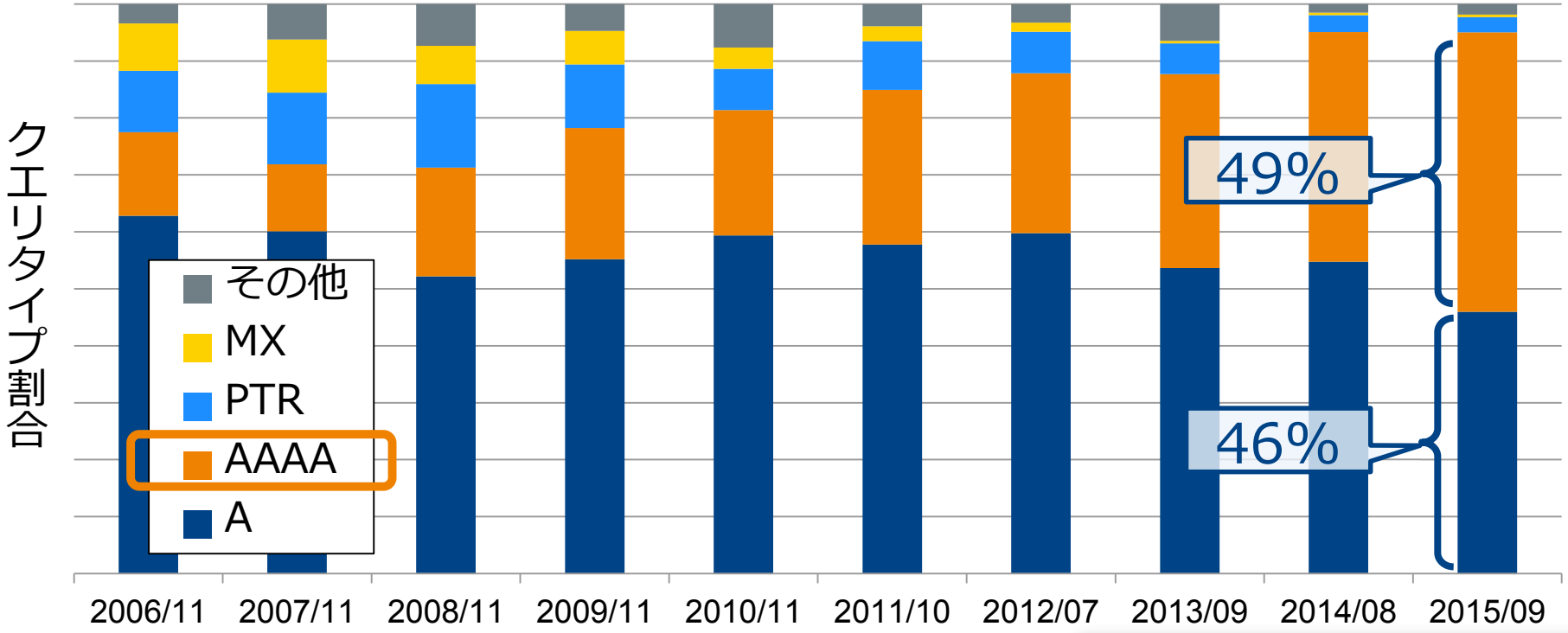
ユーザへの応答のレスポンスコード

- NOERROR が約 90% を占める傾向に変化なし
  - NOERROR / NXDOMAIN / SERVFAIL が 99%
  - 2013 年の SERVFAIL は Amp 攻撃への応答



キャッシュサーバが送出するクエリ

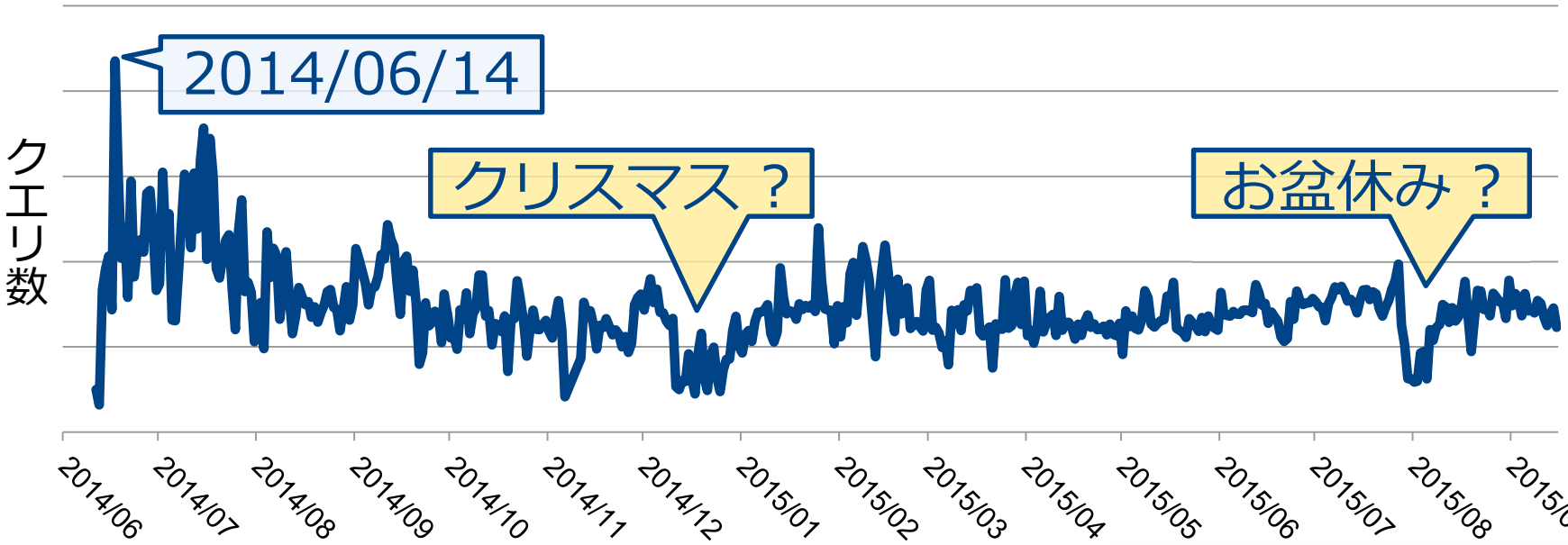
- AAAA の割合が増加し A の割合を超えた
  - A のみ存在する FQDN でのキャッシュ時間の差
- PTR, MX など A, AAAA 以外の割合は減少傾向



DNS ランダムサブドメイン攻撃 (水責め攻撃)

ランダムサブドメインクエリ

- 一時期に比べると落ち着いたが継続して観測
- 現在は総クエリの約 2 % 程度
  - 2014/06/14 が最大：総クエリの約 6.5 %
    - ✓ *.google.com クエリは総クエリの約 6.3 %



* 2015/08 上旬は、その前後の期間のランダムクエリと同程度の非ランダムクエリを観測
“http://www.npa.go.jp/cyberpolice/detect/pdf/20150925.pdf”

TLD 関連

ユーザクエリの TLD ランキング

- 上位 4 TLD が総クエリの約 95 % を占める
  - 新 gTLD は昨年に続き TOP 20 ランクインなし
- local. など内部向けと思われるクエリも上位に

順位	TLD	クエリ割合	昨年
1	com.	51.771%	1
2	jp.	24.190%	2
3	net.	18.220%	3
4	org.	1.026%	5
5	arpa.	0.870%	4
6	tv.	0.282%	6
7	gov.	0.256%	59
8	cn.	0.220%	8
9	co.	0.199%	13
10	me.	0.167%	12

順位	TLD	クエリ割合	昨年
11	biz.	0.140%	10
12	cc.	0.135%	14
13	in.	0.134%	27
14	info.	0.131%	9
15	li.	0.126%	11
16	local.	0.111%	7
17	io.	0.098%	18
18	asia.	0.098%	15
19	ru.	0.076%	28
20	to.	0.070%	20

* 赤地はルートゾーンに登録のないドメイン名

*昨年比 UP DOWN

TLD ランキング (新 gTLD のみ抜粋)

- 新 gTLD クエリは昨年の約 5 倍に増加
  - 新 gTLD クエリ全体で総クエリの約 0.03 %
- 人気サイトでの使用があれば更に増加の可能性も

順位	TLD	クエリ割合	昨年
62	xyz.	0.004962%	115
76	link.	0.003706%	372
85	tokyo.	0.003272%	150
97	pics.	0.002604%	-
104	chat.	0.002350%	-
124	global.	0.001541%	138
127	club.	0.001494%	221
128	red.	0.001491%	-
139	pink.	0.001181%	833
167	town.	0.000783%	-

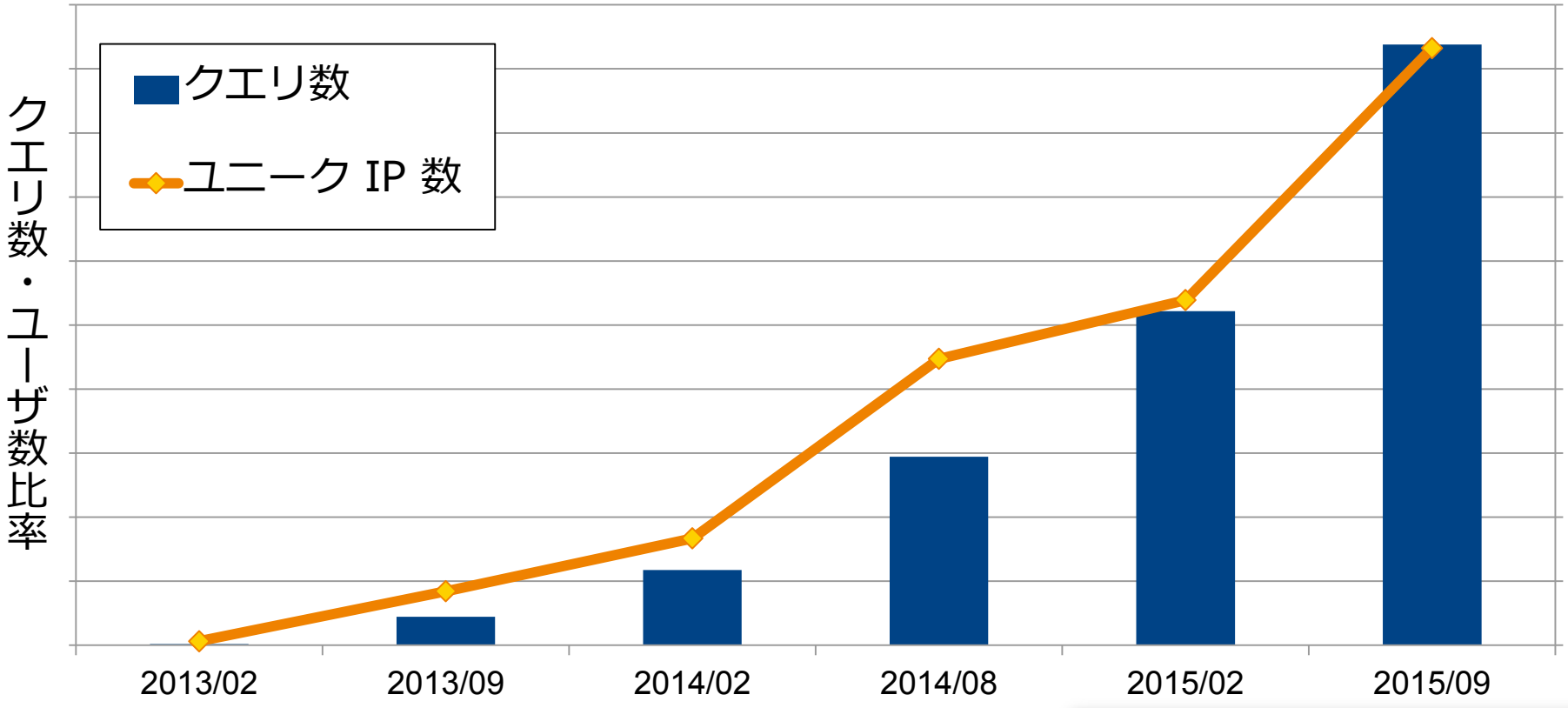
順位	TLD	クエリ割合	昨年
168	holiday.	0.000778%	-
176	click.	0.000702%	-
178	work.	0.000672%	-
192	solutions.	0.000565%	280
204	marketing.	0.000436%	379
212	top.	0.000405%	-
231	gift.	0.000263%	-
232	moe.	0.000257%	971
234	today.	0.000255%	229
236	tools.	0.000254%	-

*昨年比 UP DOWN

モバイルユーザからのクエリ

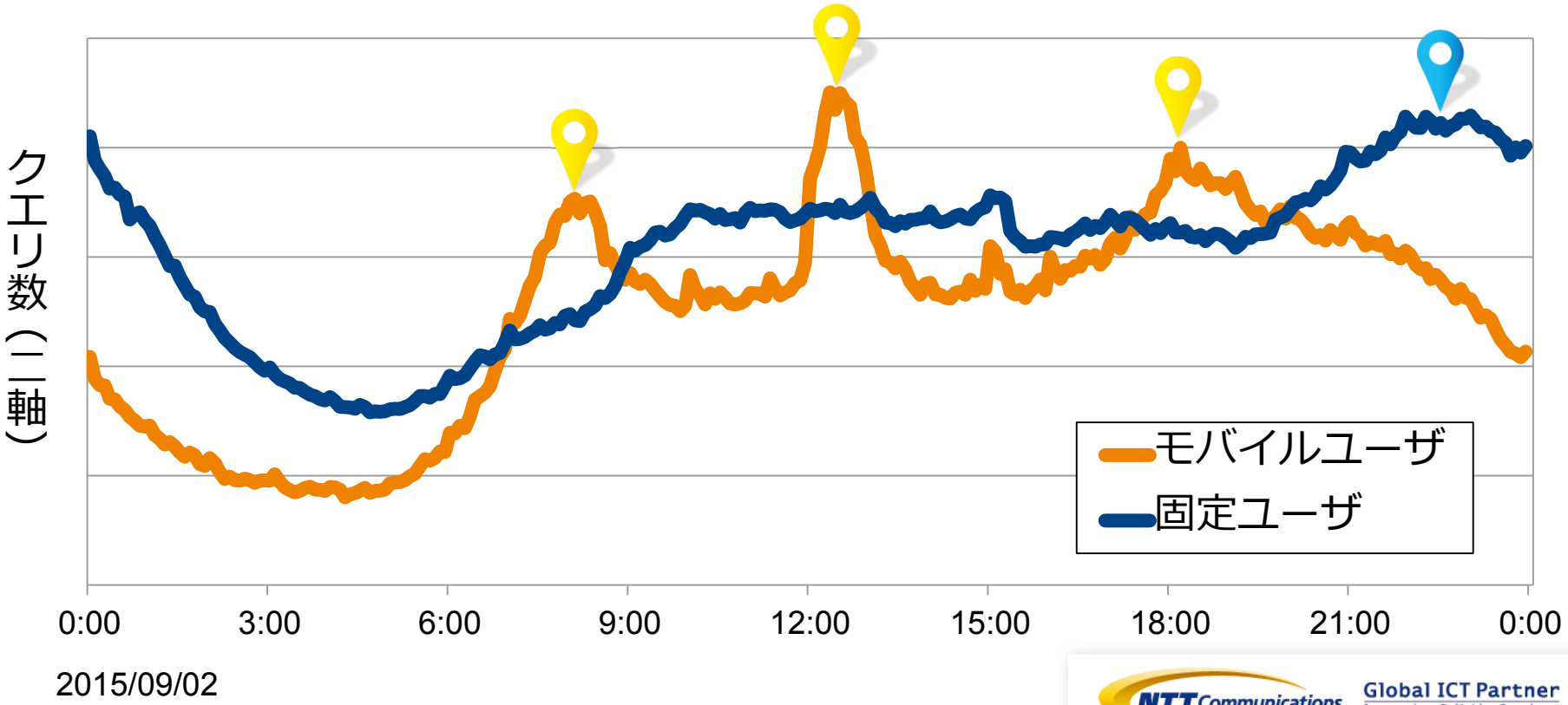
モバイルユーザからのクエリ数・ユーザ数

- ユーザ数の増加にほぼ比例してクエリ数も増加
- ユーザあたりのクエリ数には大きな変化なし



モバイルユーザからのクエリ数の時間変動

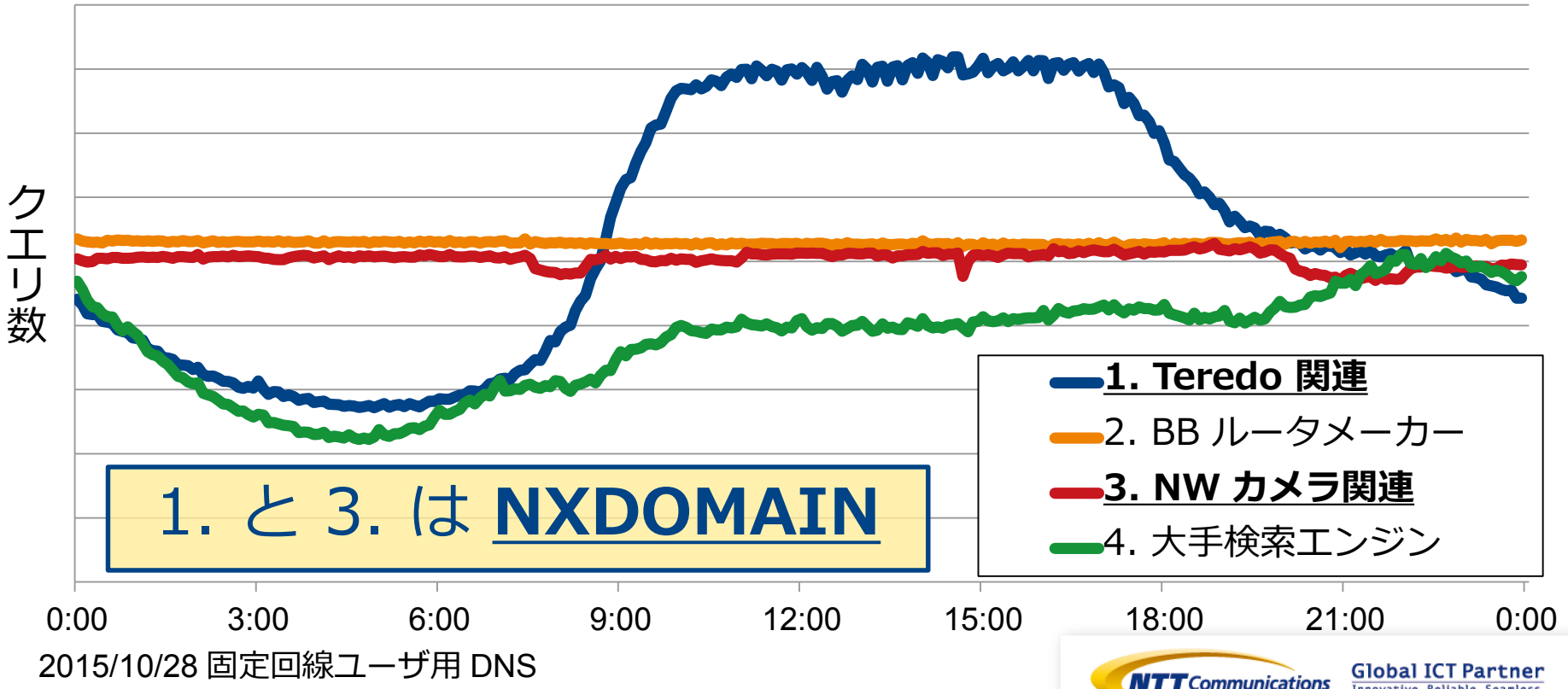
- モバイルユーザは通勤時間帯と昼休みに突出
- クエリ数は増加したが時間変動は昨年とほぼ同じ
  - 昨年に続き 15 時には小休憩？



その他トピック

FQDN TOP 4 のクエリ数の時間変動

- Teredo：ビジネスタイムに OS が自動送信？
- BB ルータ / NW カメラ：組み込み機器が送信か
- IoT 普及に伴いモノからのクエリが増加しそう



まとめ

■ 長期的傾向
- ユーザあたりのクエリ数が増加傾向
- 特に AAAA クエリが増加傾向

■ 最近のトピック
- DNS ランダムサブドメイン攻撃は継続している
- 新 gTLD クエリはまだまだ少ないが徐々に増加
- モバイルは通勤通学、昼休み時間帯がピーク
- 存在しないドメインがクエリ数ランキング上位に

ご清聴
ありがとうございました

Special Thanks To
NTT ネットワーク基盤技術研究所のみなさま