キャッシュ DNS Update ～今年のトレンド～

NTTコム ソリューション＆エンジニアリング株式会社
エンジニアリング事業部
オペレーション部門
図師 稔
minoru.zushi@ntt.com

Index

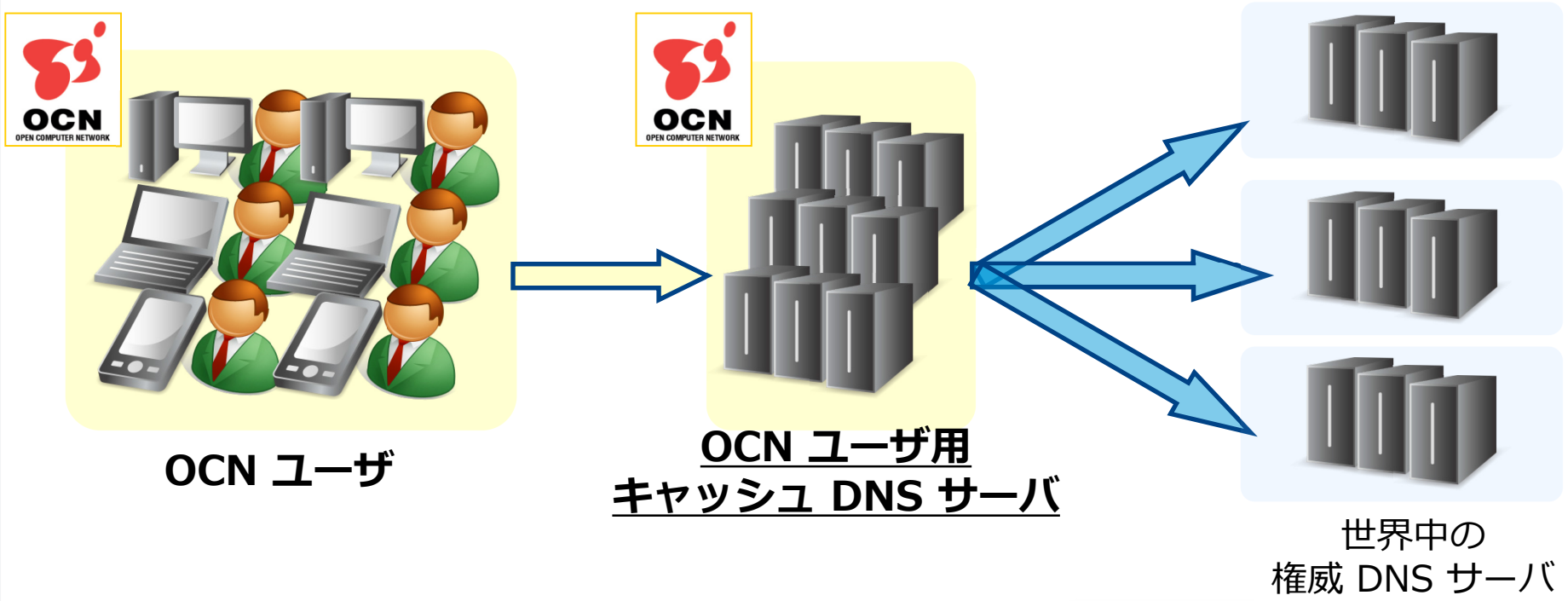
■ 長期的傾向
- ユーザクエリの変動

■ 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)
- 新 gTLD 関連
- MVNO ユーザからのクエリ

長期的傾向

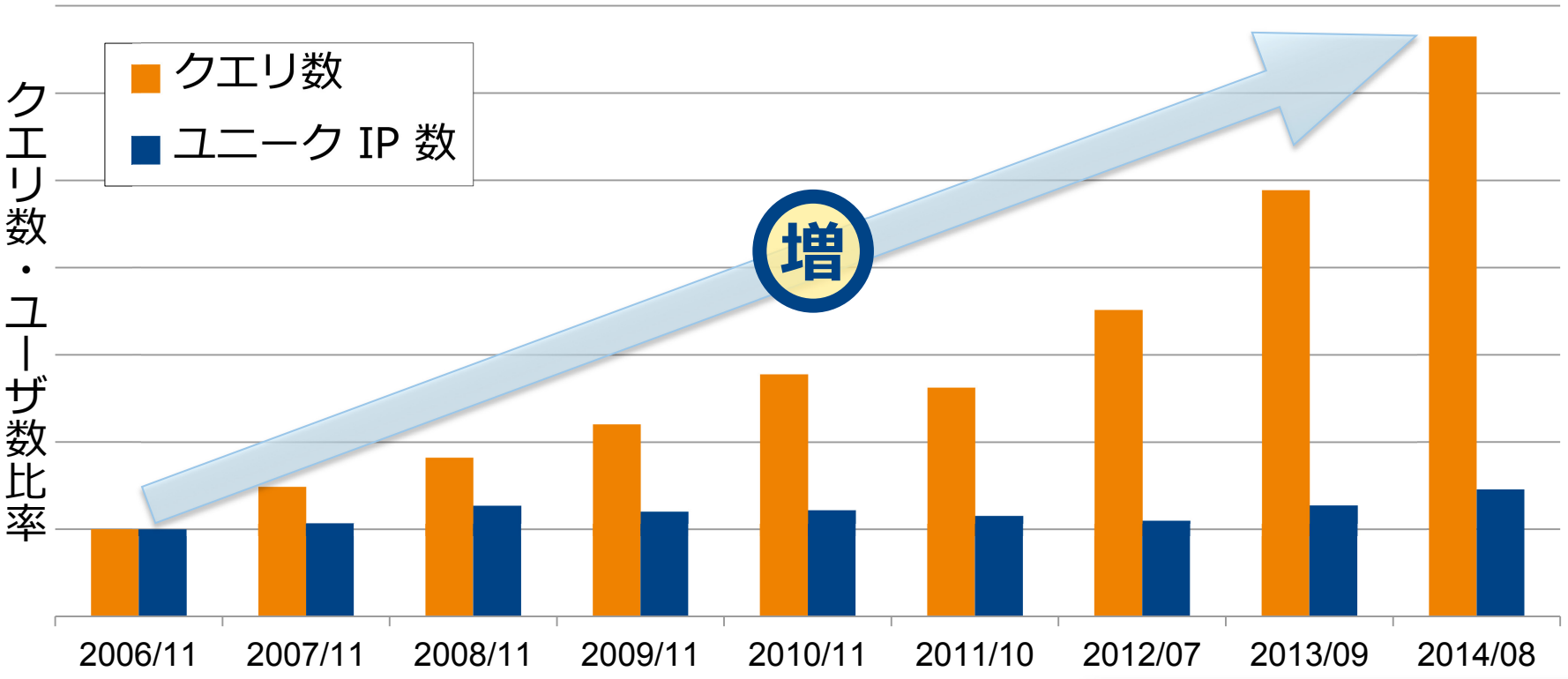
OCN の DNS

- OCN ユーザ数　　：**約800万**
- ユーザからのクエリ数：**約270億 / 日**
- DNS サーバ数　　：**約100台**



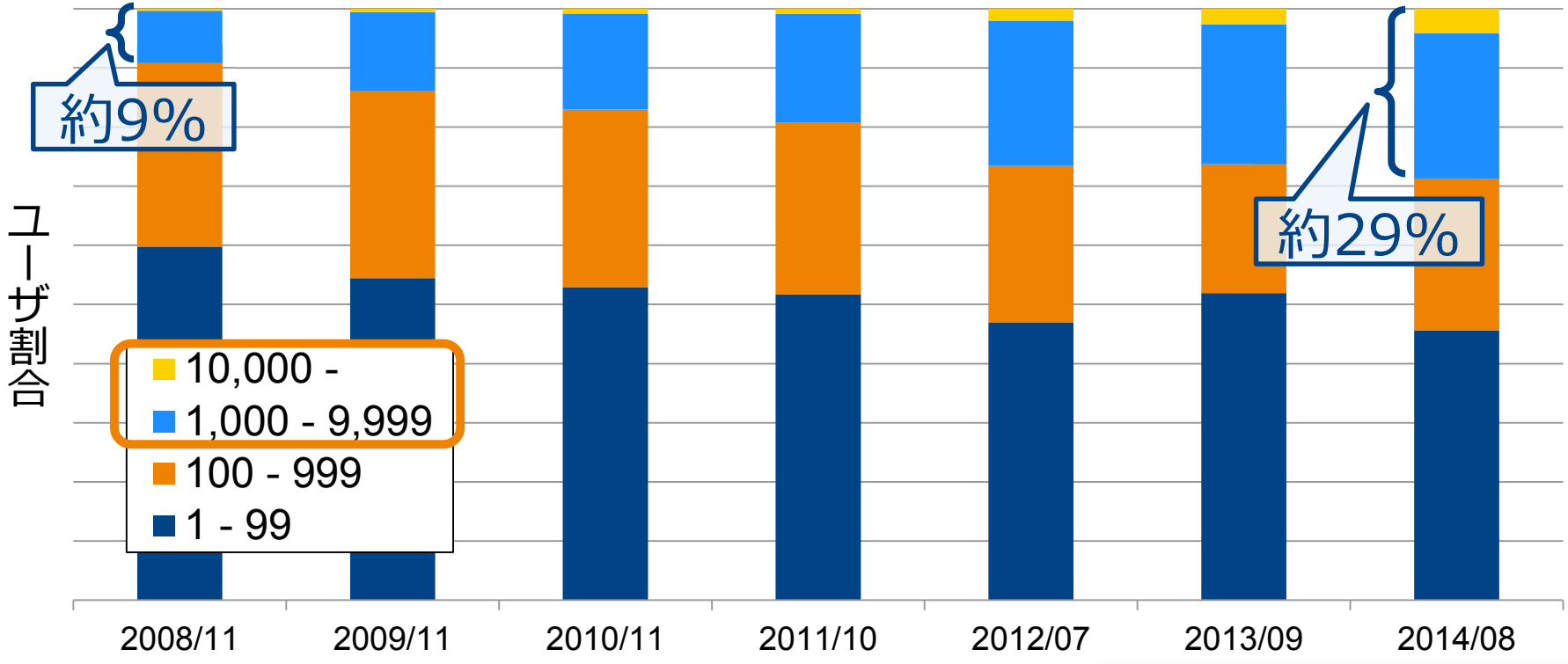
ユーザからのクエリ数・ユーザ数

- 2006 年と比べてクエリ数は 6 倍以上
- ユーザあたりのクエリ数が大きく増加している



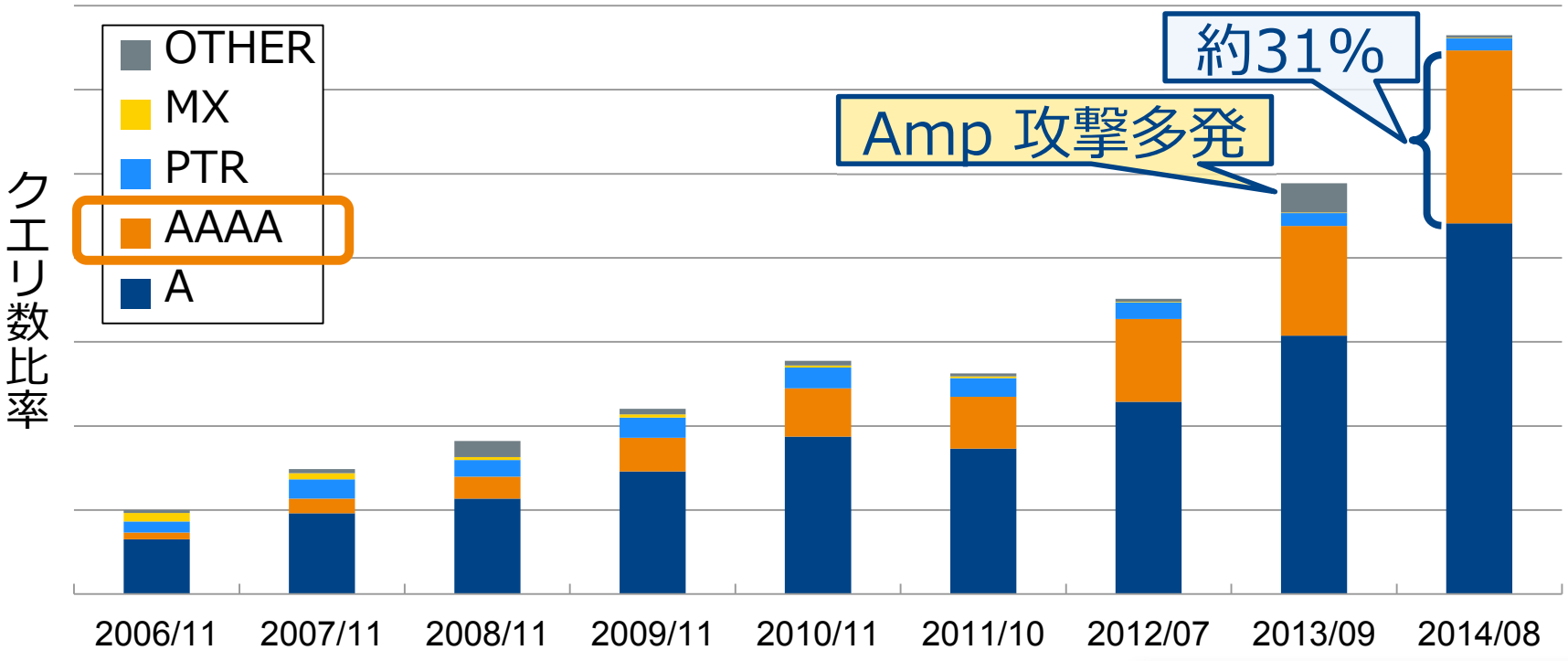
一日のクエリ数別ユーザ割合

- 1,000 クエリ / 日以上のユーザ割合が増加傾向
  - Web サイトの複雑化、ブラウザのプリフェッチ?
  - 大量クエリ送出ユーザの一部は攻撃の踏み台か



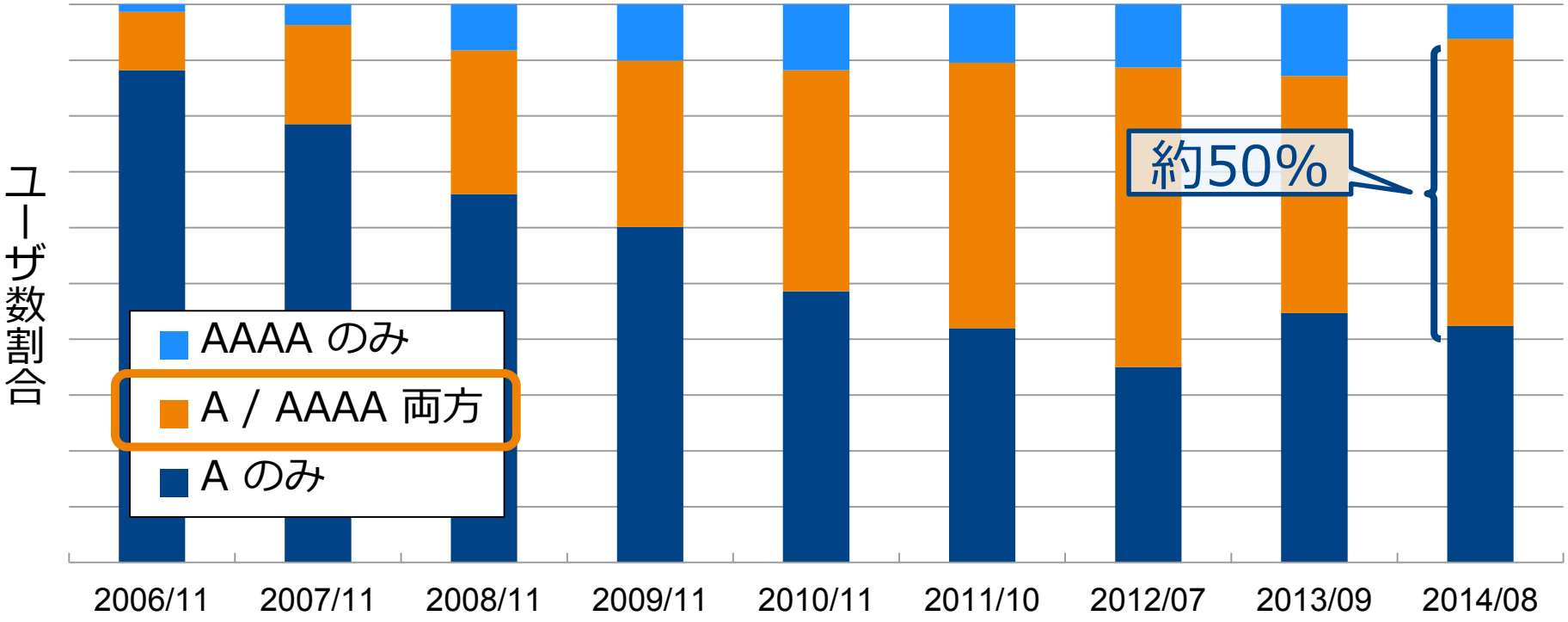
ユーザからのクエリのクエリタイプ

- A, AAAA が増加、クエリのほとんどを占める
  - 2006 年と比べて AAAA クエリ数は 25 倍以上
  - 2013 年の OTHER は Amp 攻撃の ANY クエリ



AAAA クエリ送出ユーザの割合

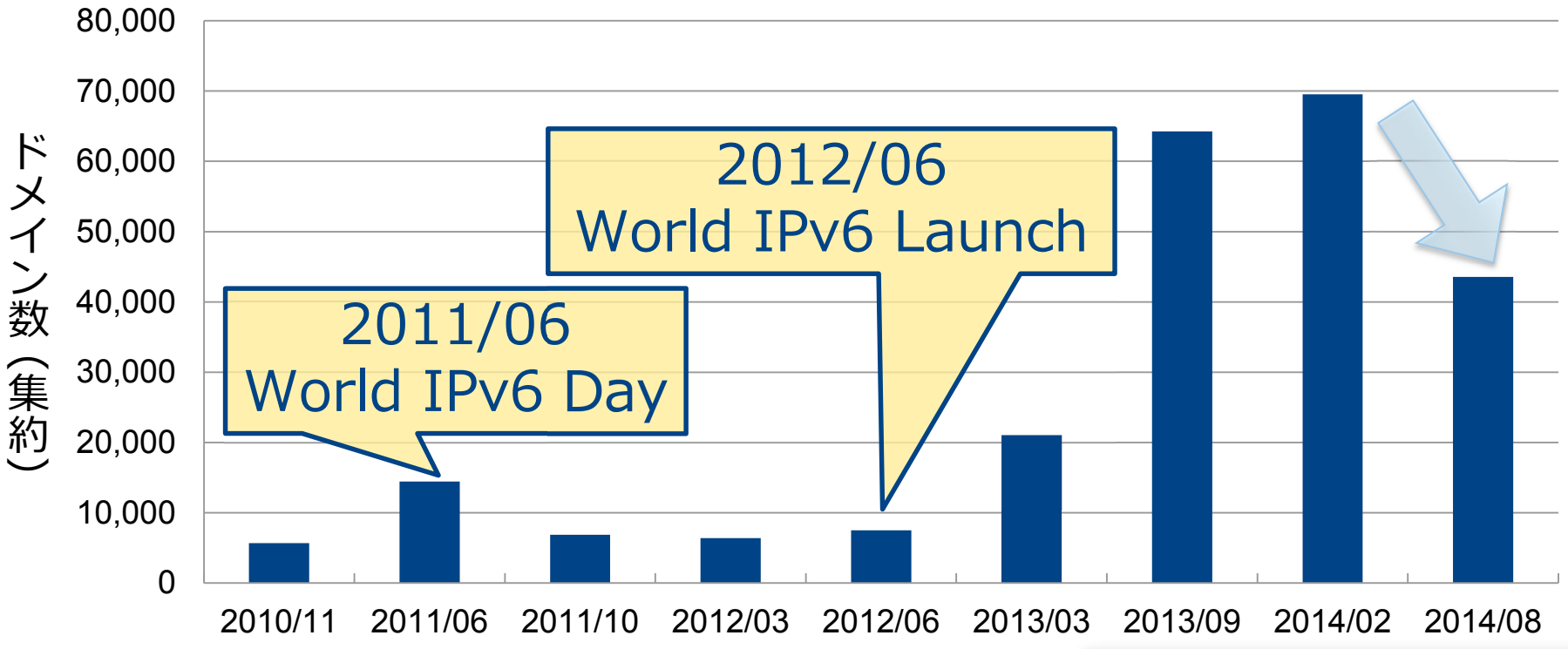
- 「A/AAAA 両方」ユーザ割合の増加は鈍化
- WinXP 端末の減少や IPv6 普及に伴い漸増するか
  - WinXP (標準で IPv6 非対応) のシェア 23.87%*



* 2014/09 時点 “http://www.netmarketshare.com/operating-system-market-share.aspx”

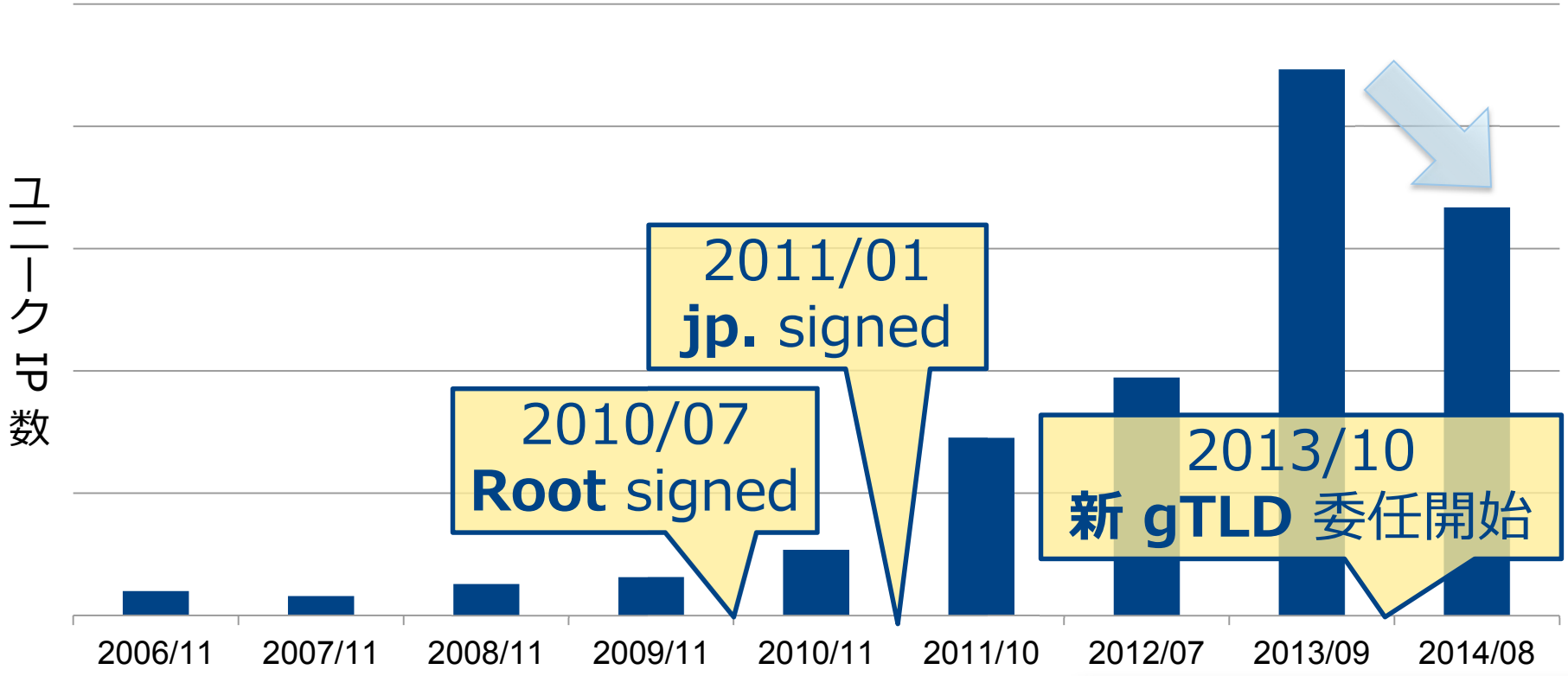
AAAA つきドメイン数 (組織別集約)

- example.com, example.co.jp などの単位で集約
- W6L 後増加していたが減少に転じている



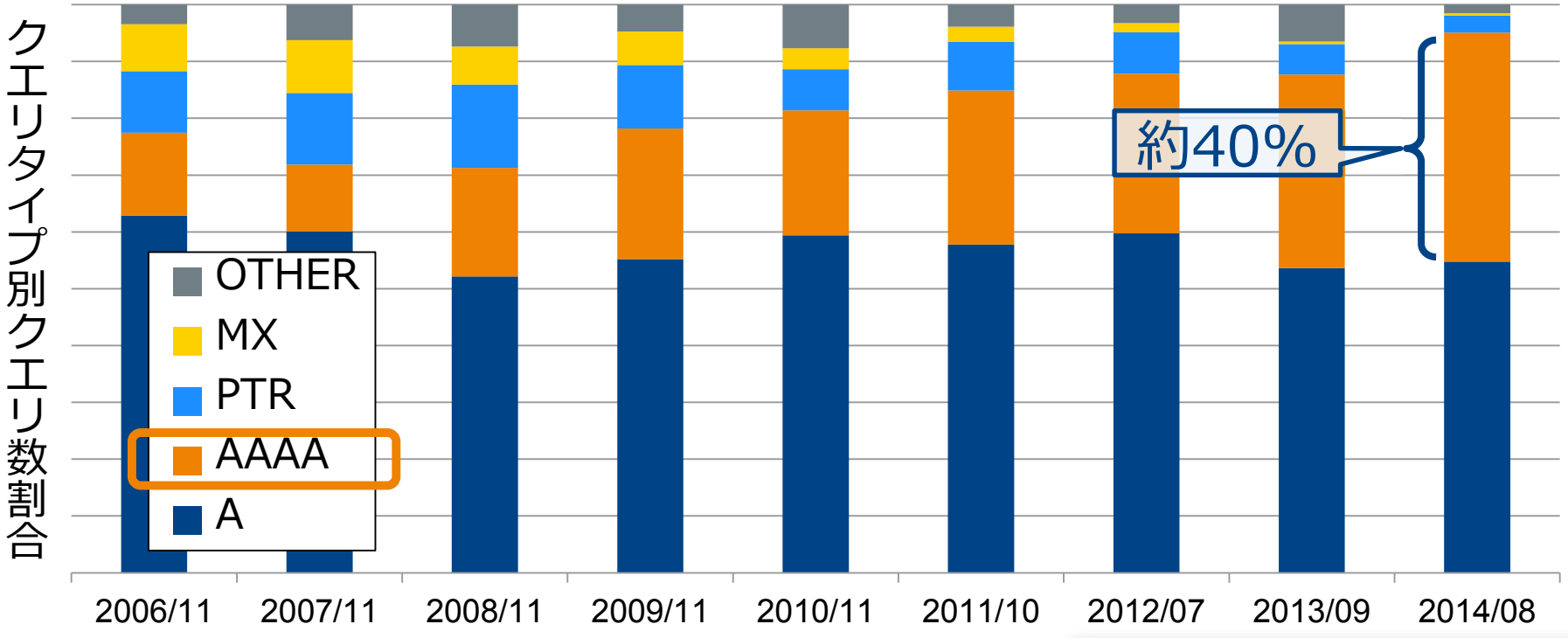
DNSSEC 対応クエリ送出ユーザ数

- DO bit つきクエリ送出ユーザは増加がストップ?
- 約 1 % のユーザから送出されている



キャッシュサーバが送出するクエリ

- AAAA の割合が増加傾向
  - 約 40 % が AAAA クエリ
- PTR, MX など A, AAAA 以外は減少傾向



DNS ランダムサブドメイン攻撃 (水責め攻撃)

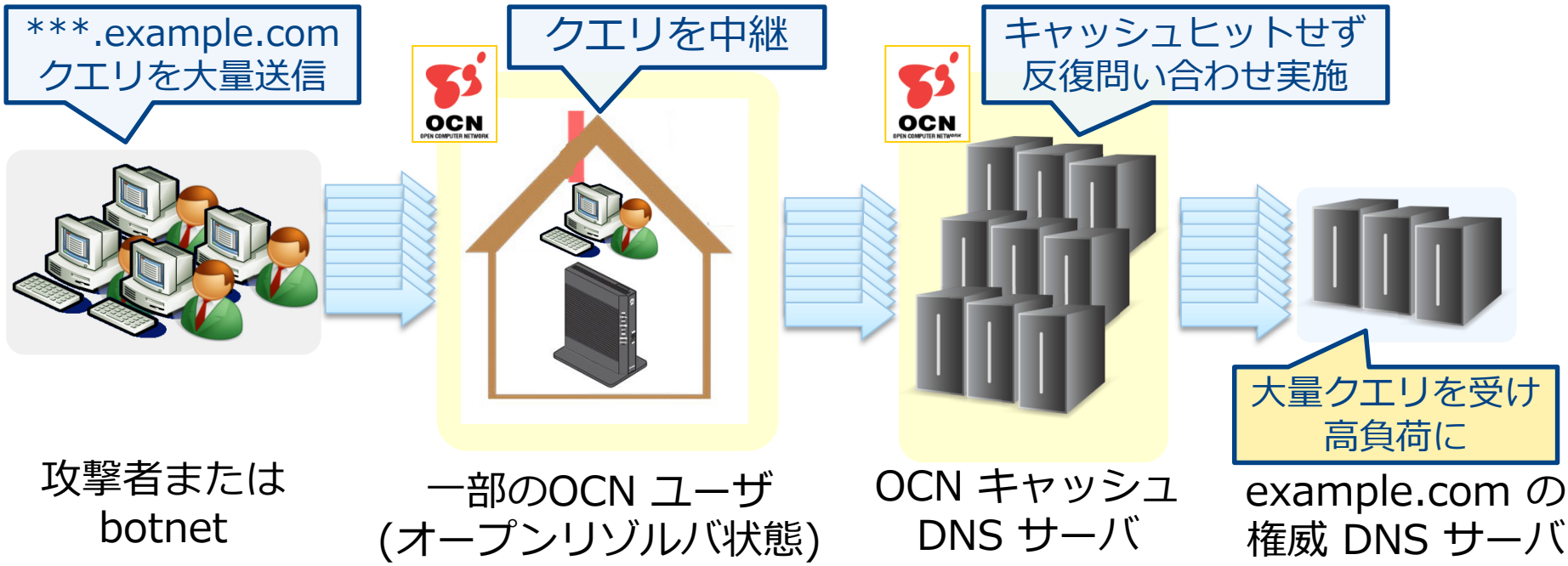
DNS ランダムサブドメイン攻撃とは

- 2014年初頭から世界的に観測される DDoS 攻撃
- オープンリゾルバ・オープンフォワーダを悪用
- 攻撃対象のランダムなサブドメインの大量クエリ
  - 例：wtqningt.www.example.com の A レコード

    ランダムなサブドメイン　攻撃対象ドメイン名
  - キャッシュ DNS サーバでキャッシュが効かない
    → 権威 DNS サーバへ大量のクエリが発生
    → 権威 DNS サーバが高負荷になり応答が悪化
    → キャッシュ DNS サーバも高負荷に
- 攻撃対象ドメイン名の権威 DNS サーバが標的か
  - 攻撃対象ドメイン名は中国語圏サイトのものが多い

DNS ランダムサブドメイン攻撃

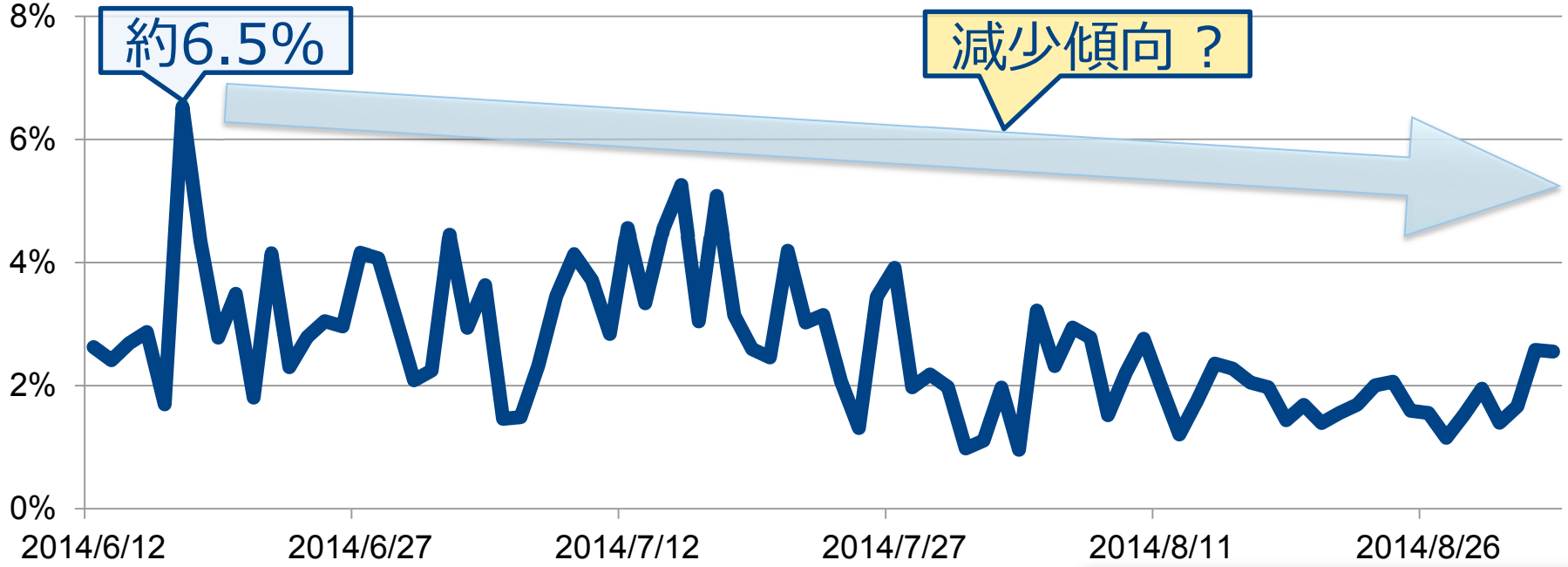
■ 一部の OCN ユーザが該当クエリを送出
- オープンリゾルバ状態の端末が踏み台に？



■ 攻撃対象のドメインを検知する仕組みを導入

総クエリ中の検知ドメインクエリ割合

- ゆるやかだが減少傾向か
- 06/17 検知ドメインクエリは総クエリの約 6.5 %
  - cf. *.google.com クエリは総クエリの約 3 %
- 現在も香港関連ドメインなどで時々ピークが発生



新 gTLD 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 TOP 20 ランク外
- local., wpad. など内部向けと思われるクエリも

順位	TLD	クエリ割合
1	com.	53.211%
2	jp.	24.667%
3	net.	16.674%
4	arpa.	1.290%
5	org.	0.611%
6	tv.	0.311%
7	local.	0.297%
8	cn.	0.263%
9	info.	0.217%
10	biz.	0.170%

順位	TLD	クエリ割合
11	li.	0.170%
12	me.	0.152%
13	co.	0.128%
14	cc.	0.121%
15	asia.	0.091%
16	kr.	0.074%
17	localdomain.	0.071%
18	io.	0.057%
19	us.	0.055%
20	wpad.	0.054%

* 赤地はルートゾーンに登録のないドメイン名

TLD ランキング (新 gTLD のみ抜粋)

- 新 gTLD クエリ全体で総クエリの約 0.02 %
- ルートゾーンにないドメイン名のクエリも一定数
  - Name Collision の可能性がある

順位	TLD	クエリ割合	状態
60	home.	0.008959%	保留中
115	xyz.	0.001962%	委任済
138	global.	0.001085%	委任済
150	tokyo.	0.000994%	委任済
189	group.	0.000581%	委任待
212	data.	0.000498%	競争中
215	mail.	0.000478%	保留中
216	corp.	0.000478%	保留中
221	club.	0.000459%	委任済
229	today.	0.000412%	委任済

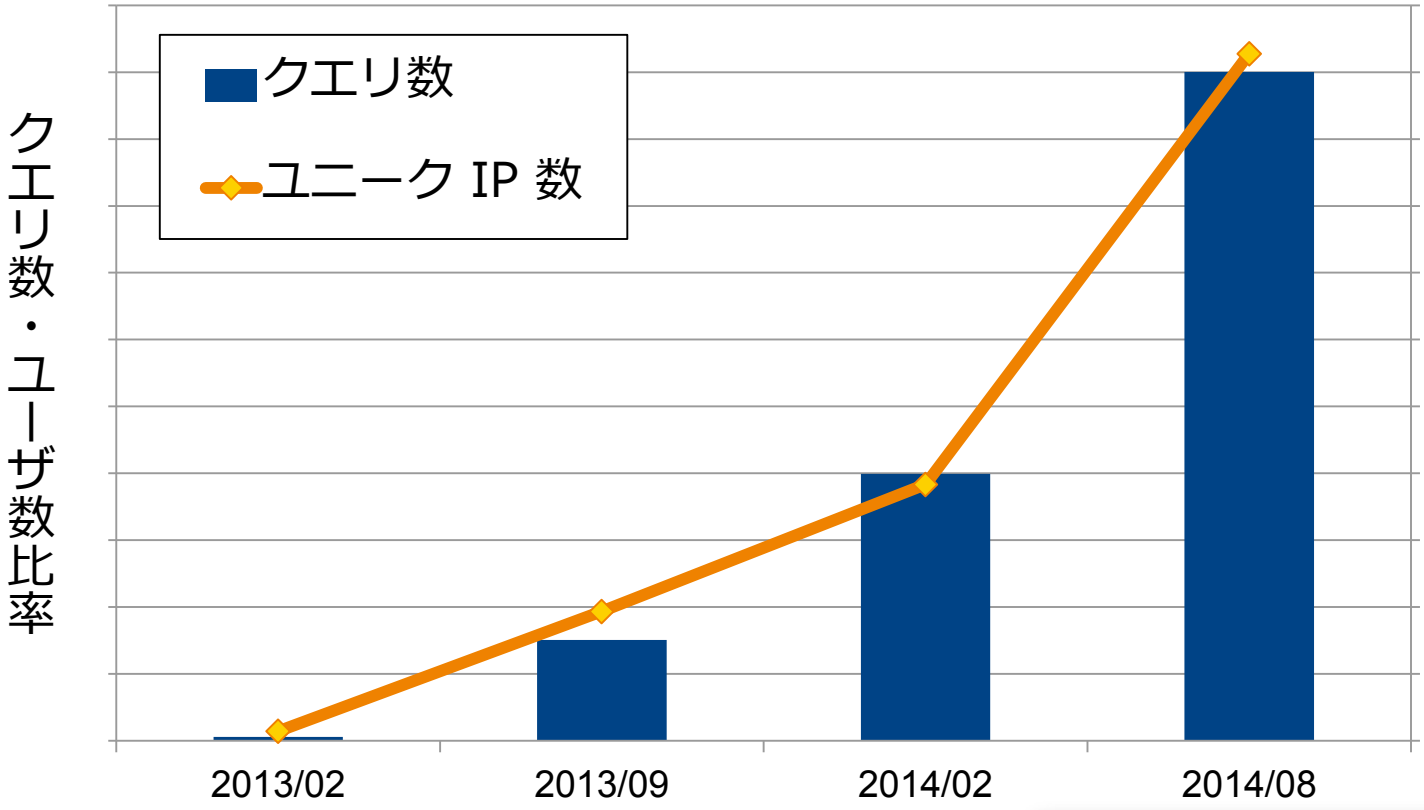
順位	TLD	クエリ割合	状態
280	solutions.	0.000244%	委任済
302	sapphire.	0.000205%	取下げ
359	ltd.	0.000156%	委任待
372	link.	0.000142%	委任済
379	marketing.	0.000138%	委任済
402	wiki.	0.000120%	委任済
421	storage.	0.000107%	契約中
472	sap.	0.000089%	委任待
514	tips.	0.000074%	委任済
523	world.	0.000071%	委任済

* 赤地はルートゾーンに登録のないドメイン名

MVNO ユーザからのクエリ

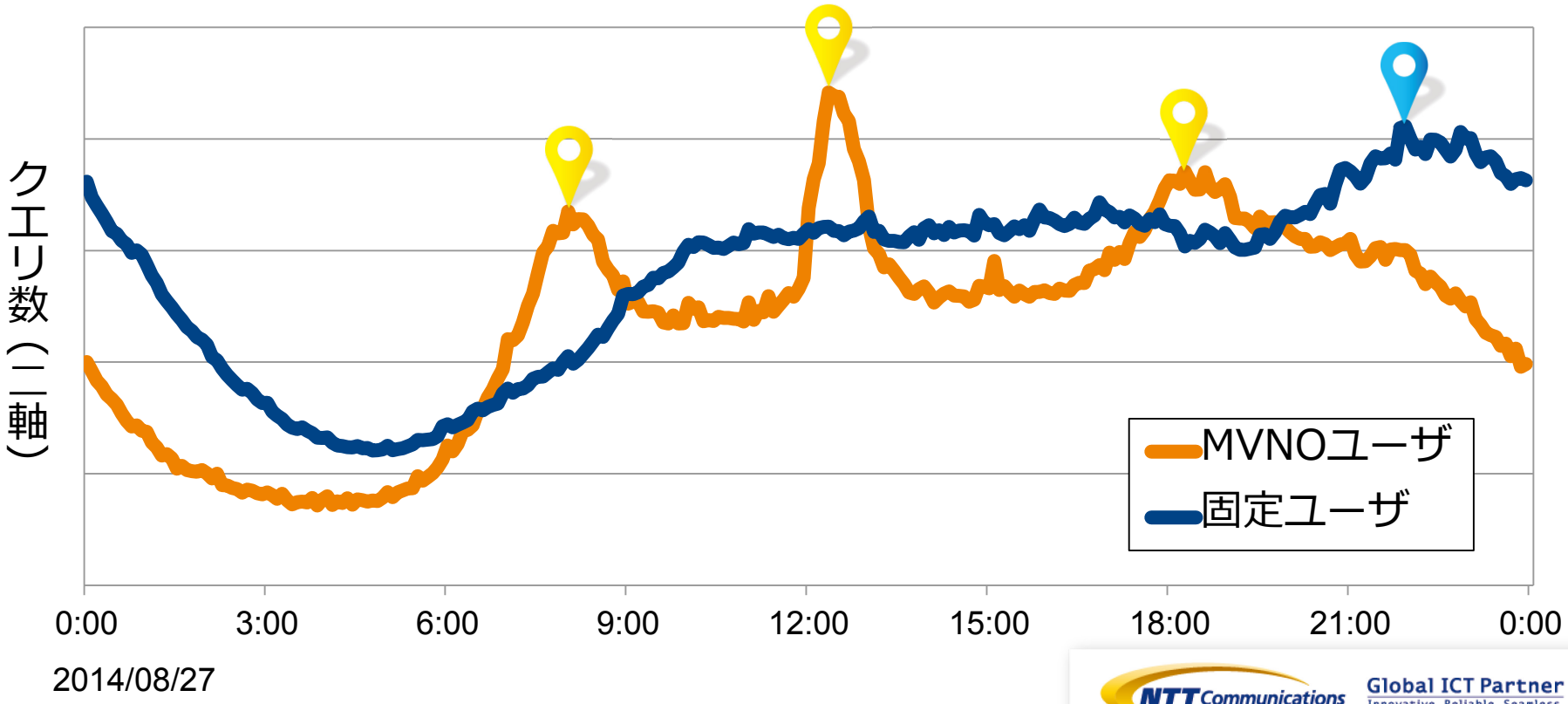
MVNOユーザからのクエリ数・ユーザ数

- 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大きな変化はない



MVNO クエリ数の時間変動

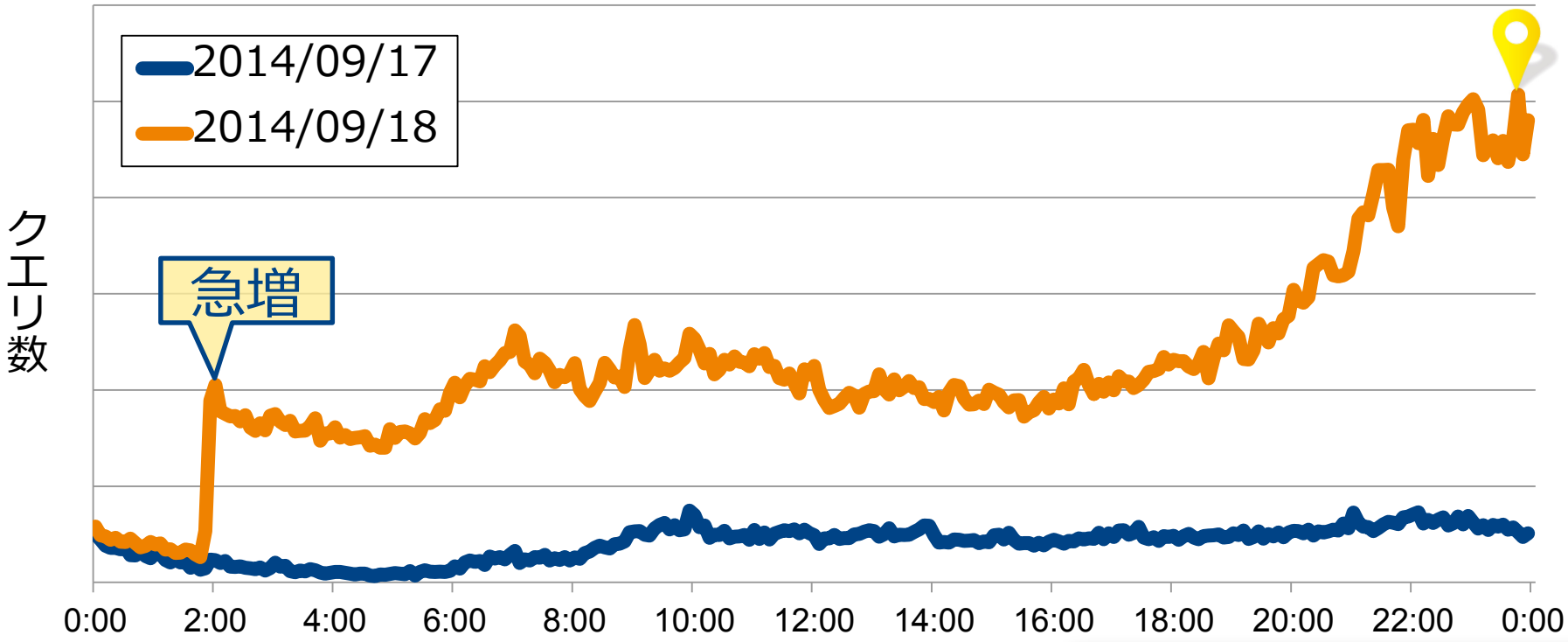
- MVNO ユーザは通勤時間帯と昼休みに突出
  - 15 時にも小休憩 ？
- 固定ユーザは夜間帯にゆるやかなピーク



その他トピック

iOS アップデート関連クエリ

- 2014/09/18 2時 iOS 8 配信開始
  - 2 時からクエリが急増 (夜ふかし組?)
  - ピークは同日 24 時ごろ (帰宅後組?)



* swcdn.apple.com / appldnld.apple.com およびその CNAME のクエリ数

まとめ

■ 長期的傾向

- A / AAAA クエリが引き続き増加傾向
- ユーザあたりのクエリ数も引き続き増加傾向

■ 最近のトピック

- DNS ランダムサブドメイン攻撃が継続中
- 新 gTLD の Name Collision と思われるクエリも
- MVNO は通勤、昼休み時間帯にクエリが増加
- キャッシュ DNS でも iOS 8 トラフィックを観測

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