

キャッシングサーバにおける クエリトラフィック増加

佐藤正春 (*), 濱口一真(NTTコミュニケーションズ株式会社)

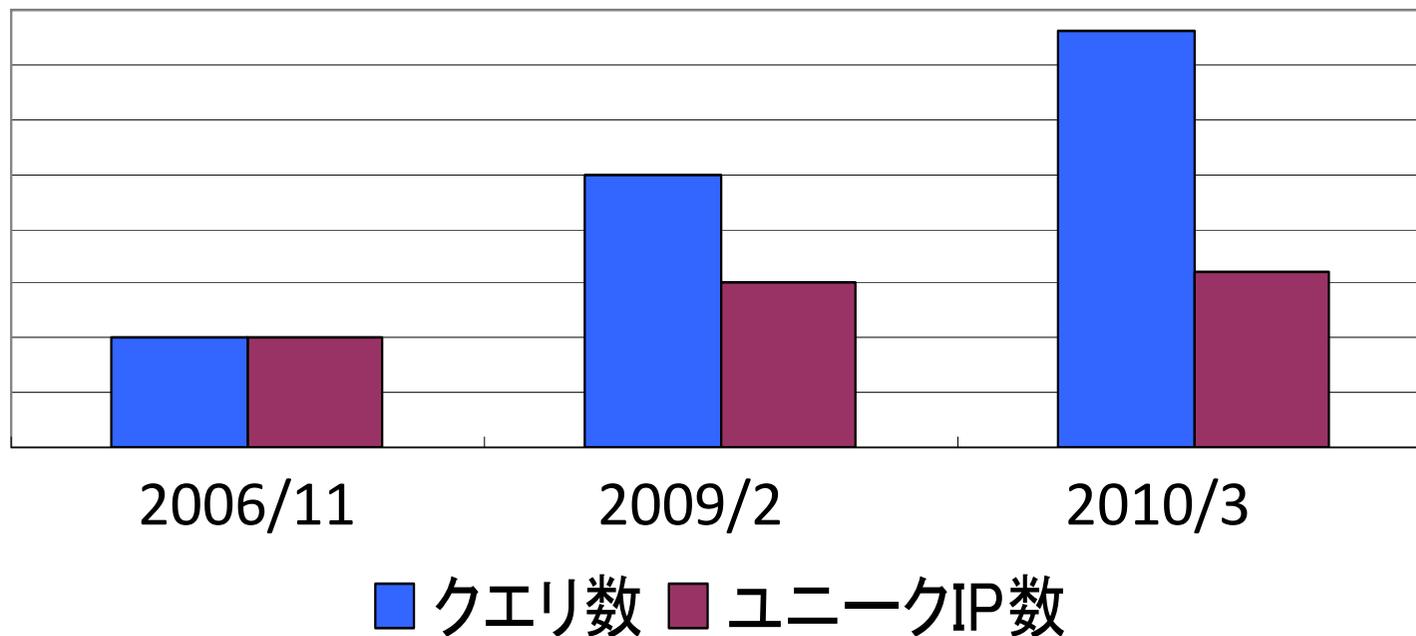
佐藤一道(*), 石橋圭介(NTT情報流通プラットフォーム研究所)

*発表者

クエリトラフィック増加推移

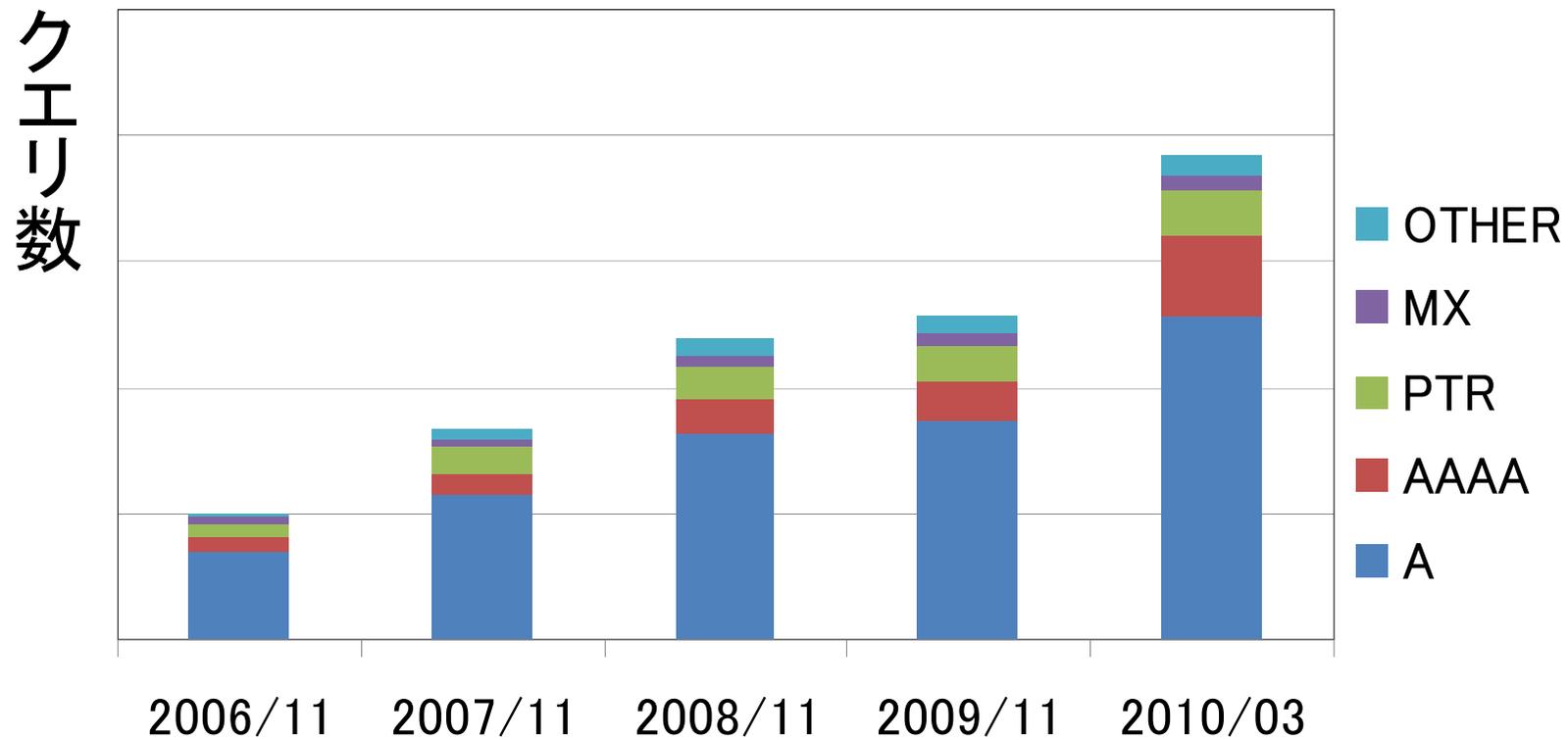
ユーザ数・クエリトラフィック数推移

- 2006年11月, 2009年2月, 2010年3月のそれぞれ1日分のクエリに対し、クエリ数、ユニークIP数を算出
- クエリ数、ユニークIP数とも増加。ただし、ユニークIP数の伸びに対してクエリ数の増大が著しい⇒ユーザ当たりのクエリ数増加



クエリタイプ別推移

- 特にA/AAAAの増加(2009年比約1.5倍)が顕著



クエリトラフィック増加内容分析

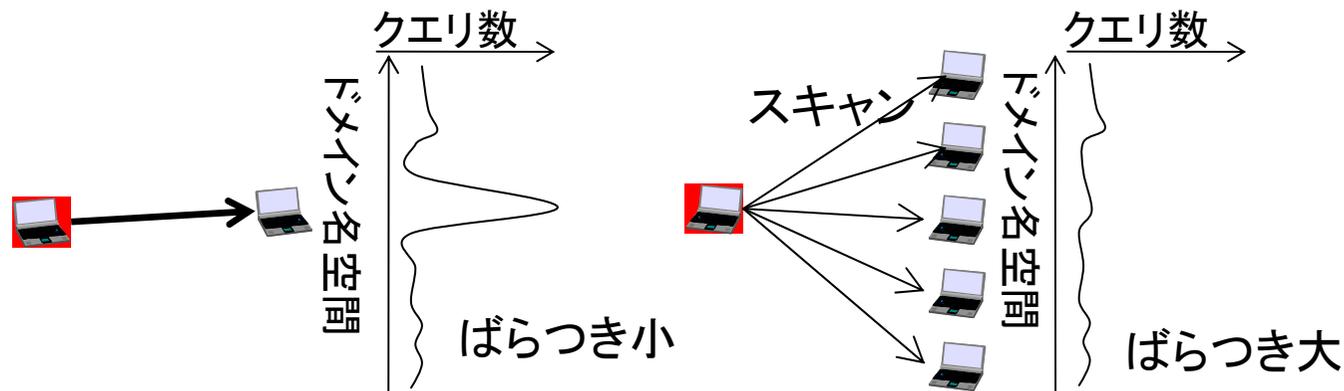
クエリ数増加分析

- 2010年に増加した大量クエリ送信ユーザはどのようなユーザか？
- これまで:大量クエリ送信ユーザ≒不要クエリ送信ユーザ(*)
 - 不要クエリ:アプリ/HGW実装ミスによる存在しないドメインへの繰り返しクエリなど。ユーザにとって不要。
- ブラウザプリフェッチによるクエリは必ずしも不要クエリではない。正常クエリによる大量クエリ送信ユーザが増加しているのか？
- Firefox3.5のリリース2009年6月をまたいだ、2009年2月と2010年3月のデータを比較

*:豊野剛他, “DNSキャッシングサーバにおける異常クエリ分析,” 情処学会 DSM研究会, 2008年3月.

大量クエリ送信ユーザの特性分析法

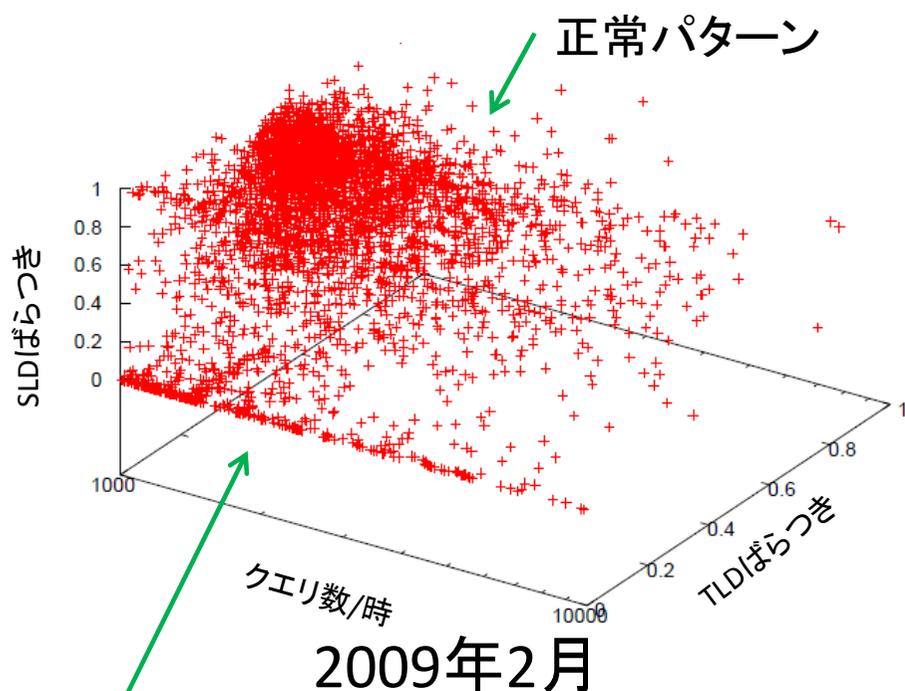
- クエリ先ドメインのばらつきにより、ユーザの特性を分析(*)
 - 同ドメインへの繰り返しクエリ: ばらつき小
 - 多数ドメインへのスキヤンのクエリ: ばらつき大
 - 正常ユーザはばらつきが中間となる(.com, .jp等にほどよくばらつく)
 - TLD, SLDのばらつきを評価
- 同手法で2009年2月、2010年3月のデータを比較



K. Ishibashi, et.al, "Characterizing DNS Client Behavior Using Hierarchical Aggregate Entropy", 2nd DNS SSR, Feb. 2010.

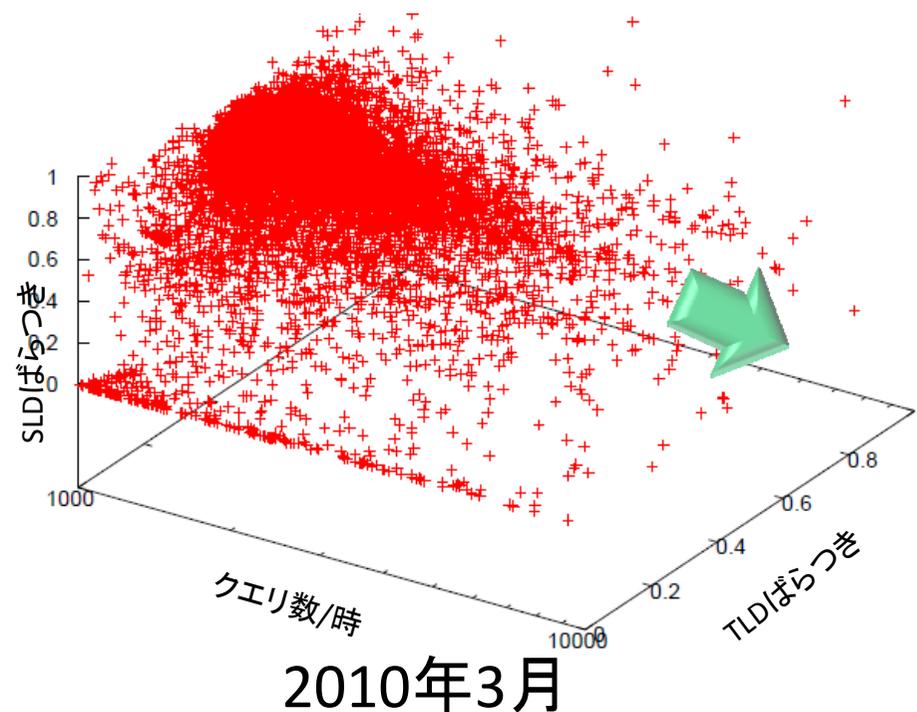
大量クエリ送信ユーザのクエリばらつき

- 1000クエリ/時以上送信する大量クエリ送信ユーザのTLD/SLDばらつきをプロット
- 2010年3月データでは正常パターンを示すユーザ数増加



2009年2月

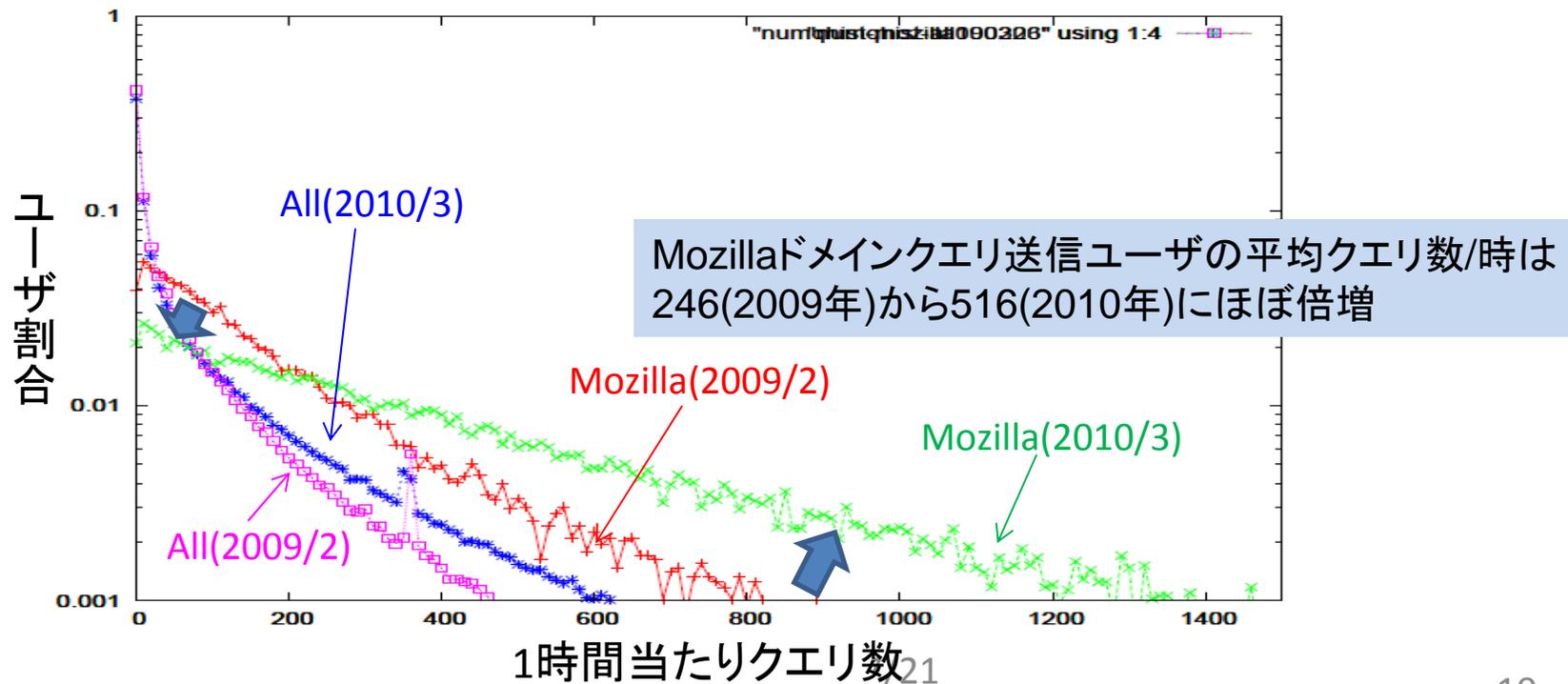
ばらつき小⇒リポートクエリ送信者



2010年3月

プリフェッチの影響調査

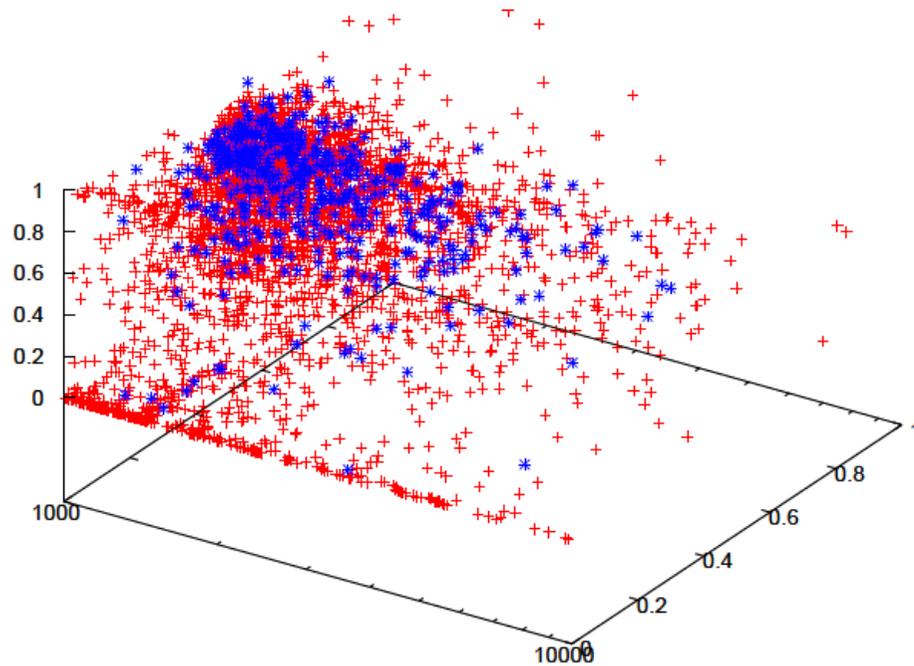
- 大量クエリ送信ユーザ数増加に対するプリフェッチの影響を調査するため、mozillaドメイン(addon.update.mozilla.org)クエリ送信IPのクエリパターンを調査
 - Firefoxは(アップデート確認等で)Mozillaドメインの名前解決を行うと仮定
 - 注意: 同送信IPは全体の2%(Firefoxシェアの12分の1であり、Firefoxユーザの網羅性はない)
- 1時間当たりクエリ数のユーザ分布を比較
- 2009/2⇒2010/3でmozillaドメインクエリ送信ユーザについて、少量クエリ送信ユーザ割合が減少し、大量クエリ送信ユーザ割合が増加



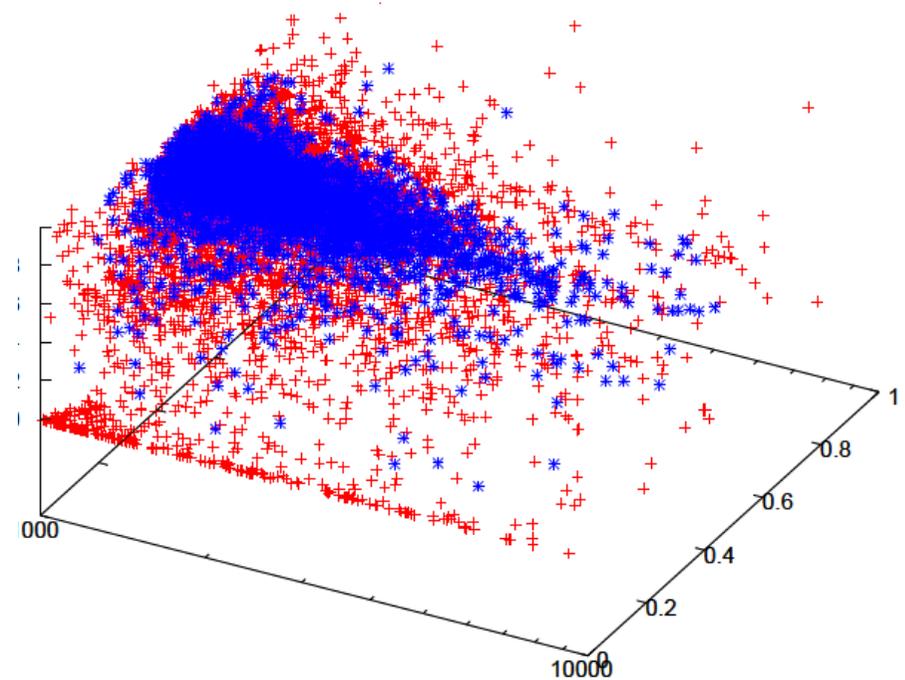
Mozillaドメインクエリ送信者のばらつき

- Mozillaドメインクエリ送信ユーザが1000qph以上送信ユーザに占める割合が増加。正常クエリ送信パターンを示す。

● :mozillaドメインクエリ送信ユーザ



2009年2月



2010年3月

まとめ

- 2009年から2010年にかけてのクエリ数増加を調査。
 - ユーザ当たりのクエリ数増加。
 - 大量クエリ送信ユーザが増加。
 - 同ユーザ群は正常クエリ送信パターンを示す
 - Mozillaドメインクエリユーザは同パターンと合致。
 - ただし、プリフェッチがクエリ数増加の主要因かどうかは要追加検証
- 考察
 - 従来、ヘビーユーザ対策は「帯域制御の運用基準に関するガイドライン」などによる利用制限が一般的
 - クエリ増大がプリフェッチの影響とすると、従来の極一部のユーザによる大量不要クエリ送信と異なり、対処が困難

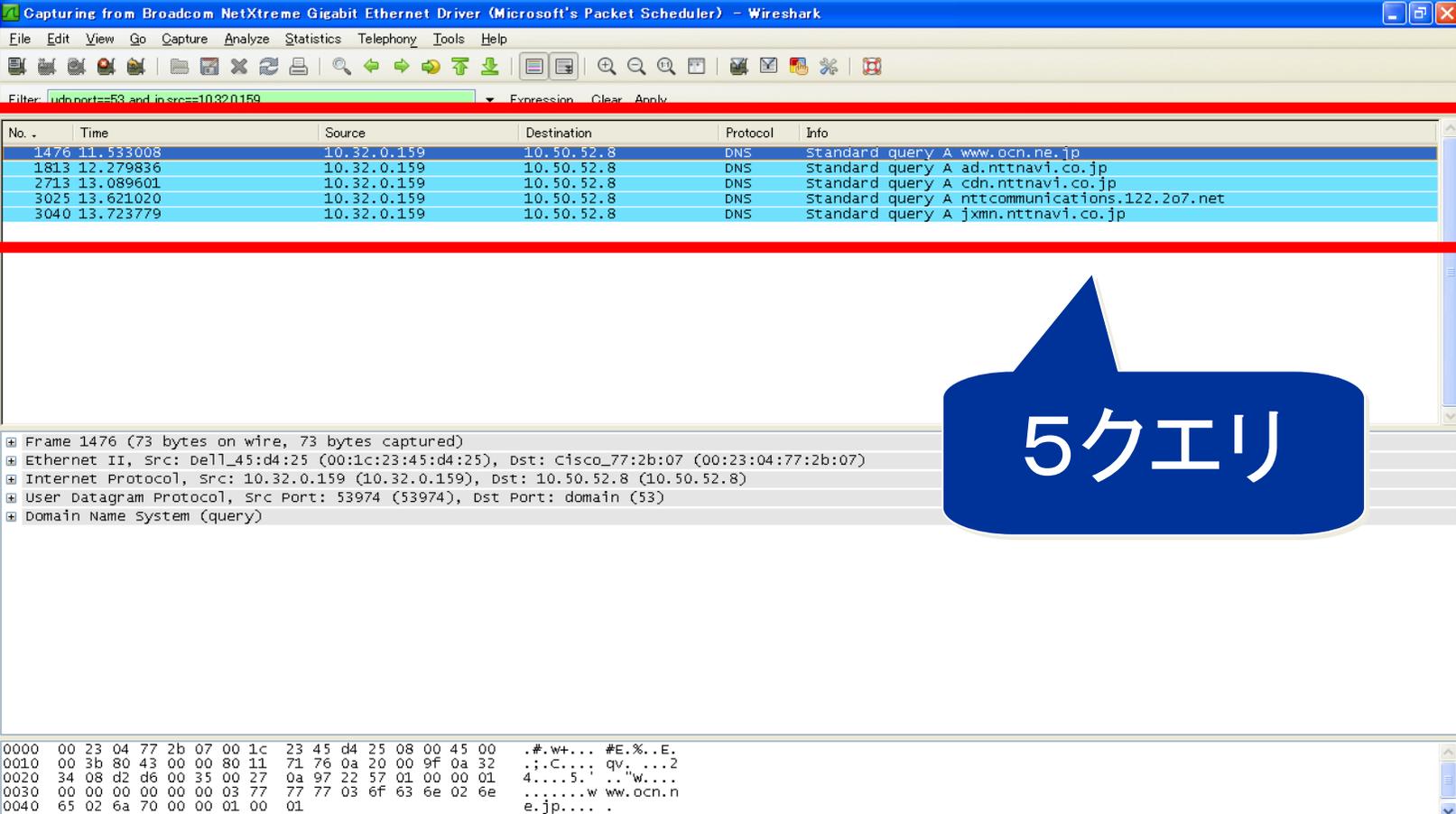
参考

ブラウザプリフェッチ

- もともとはgoogle chromeの実装
 - Firefoxもver3.5から実装実装済み
- ページ内のリンクしているFQDNの名前解決を、あらかじめ行っておく
- 名前解決の時間短縮をすることで、WEBブラウジングの体感速度を高める
- キャッシュDNSへのクエリ数が増える

Prefetchの実験結果 (www.ocn.ne.jp)

- ・Internet Expolrer 8 - DNS prefetchなし



The image shows a Wireshark network traffic capture window. The main pane displays a list of captured packets, with five DNS queries highlighted in blue and enclosed in a red rectangular box. The queries are:

No.	Time	Source	Destination	Protocol	Info
1476	11.533008	10.32.0.159	10.50.52.8	DNS	Standard query A www.ocn.ne.jp
1813	12.279836	10.32.0.159	10.50.52.8	DNS	Standard query A ad.nttnavi.co.jp
2713	13.089601	10.32.0.159	10.50.52.8	DNS	Standard query A cdn.nttnavi.co.jp
3025	13.621020	10.32.0.159	10.50.52.8	DNS	Standard query A nttcommunications.122.2o7.net
3040	13.723779	10.32.0.159	10.50.52.8	DNS	Standard query A jxmn.nttnavi.co.jp

A blue callout bubble with the text "5クエリ" (5 queries) is positioned over the bottom right of the packet list. Below the packet list, the details pane shows the structure of the selected packet (Frame 1476):

- Frame 1476 (73 bytes on wire, 73 bytes captured)
- Ethernet II, Src: Dell_45:d4:25 (00:1c:23:45:d4:25), Dst: Cisco_77:2b:07 (00:23:04:77:2b:07)
- Internet Protocol, Src: 10.32.0.159 (10.32.0.159), Dst: 10.50.52.8 (10.50.52.8)
- User Datagram Protocol, Src Port: 53974 (53974), Dst Port: domain (53)
- Domain Name System (query)

The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII:

```
0000 00 23 04 77 2b 07 00 1c 23 45 d4 25 08 00 45 00  .#.w+... #E.%..E.  
0010 00 3b 80 43 00 00 80 11 71 76 0a 20 00 9f 0a 32  .;.C...: qv. ...2  
0020 34 08 d2 d6 00 35 00 27 0a 97 22 57 01 00 00 01  4....5.  .."w...  
0030 00 00 00 00 00 00 03 77 77 77 03 6f 63 6e 02 6e  .....w ww.ocn.n  
0040 65 02 6a 70 00 00 01 00 01  .....e.jp.... .
```

Prefetchの実験結果 (www.ocn.ne.jp)

- Fire Fox 3.6.2 - DNS prefetchあり

Capturing from Broadcom NetXtreme Gigabit Ethernet Driver (Microsoft's Packet Scheduler) - Wireshark

Filter: udp.port==53 and ip.src==10.32.0.159

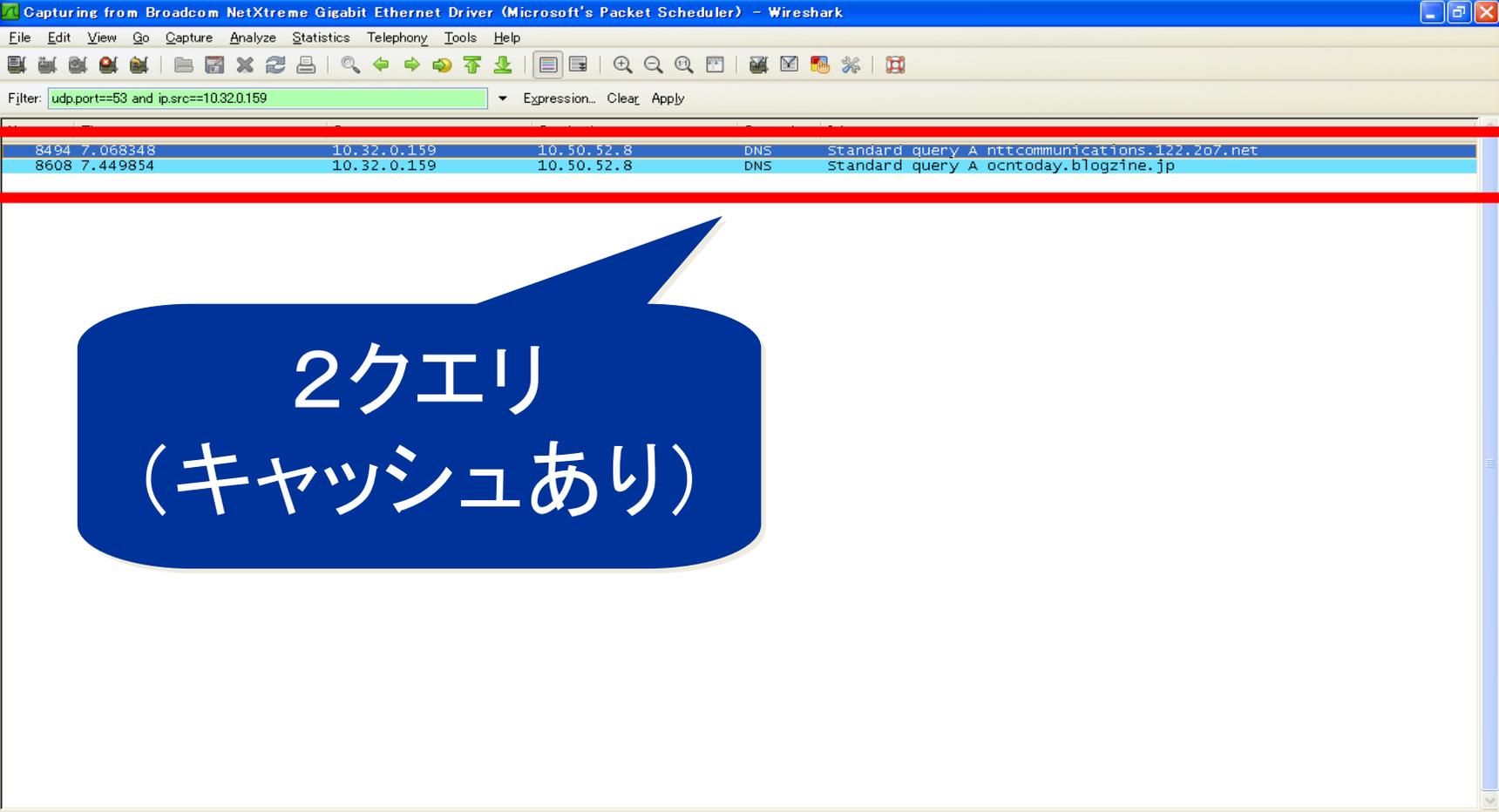
No.	Time	Source	Destination	Protocol	Info
3998	14.264827	10.32.0.159	10.50.52.8	DNS	Standard query A www.ocn.ne.jp
4387	14.604575	10.32.0.159	10.50.52.8	DNS	Standard query A ads1.msn.com
4426	14.639722	10.32.0.159	10.50.52.8	DNS	Standard query A ad.nttnavi.co.jp
4977	15.115633	10.32.0.159	10.50.52.8	DNS	Standard query A cdn.nttnavi.co.jp
5095	15.312254	10.32.0.159	10.50.52.8	DNS	Standard query A rad.msn.com
5127	15.404218	10.32.0.159	10.50.52.8	DNS	Standard query A nttcommunications.122.207.net
5252	15.864906	10.32.0.159	10.50.52.8	DNS	Standard query A jxmn.nttnavi.co.jp
5380	16.058302	10.32.0.159	10.50.52.8	DNS	Standard query A ocntoday.blogzine.jp
5385	16.074245	10.32.0.159	10.50.52.8	DNS	Standard query A blog.ocn.ne.jp
5387	16.076445	10.32.0.159	10.50.52.8	DNS	Standard query A ocn.dir.goo.ne.jp
5388	16.077208	10.32.0.159	10.50.52.8	DNS	Standard query A ocn.bsearch.goo.ne.jp
5393	16.084922	10.32.0.159	10.50.52.8	DNS	Standard query A ocndictionary.goo.ne.jp
5395	16.087139	10.32.0.159	10.50.52.8	DNS	Standard query A ocntownpage.goo.ne.jp
5396	16.088195	10.32.0.159	10.50.52.8	DNS	Standard query A map.ocn.ne.jp
5401	16.091325	10.32.0.159	10.50.52.8	DNS	Standard query A ocncntransit.goo.ne.jp
5405	16.093867	10.32.0.159	10.50.52.8	DNS	Standard query A www.ocn.rakuten.co.jp
5407	16.098219	10.32.0.159	10.50.52.8	DNS	Standard query A ocnpostcode.goo.ne.jp
5409	16.100396	10.32.0.159	10.50.52.8	DNS	Standard query A www.goo.ne.jp
5411	16.103327	10.32.0.159	10.50.52.8	DNS	Standard query A ocncnsearch.goo.ne.jp
5413	16.105540	10.32.0.159	10.50.52.8	DNS	Standard query A mypage.ocn.ne.jp
5416	16.111667	10.32.0.159	10.50.52.8	DNS	Standard query A mail.ocn.ne.jp
5417	16.111726	10.32.0.159	10.50.52.8	DNS	Standard query A cocoa.ntt.com
5421	16.121027	10.32.0.159	10.50.52.8	DNS	Standard query A urana1.ocn.ne.jp
5425	16.127064	10.32.0.159	10.50.52.8	DNS	Standard query A juicystyle.ocn.ne.jp
5427	16.132720	10.32.0.159	10.50.52.8	DNS	Standard query A cg101.ocn.ne.jp
5429	16.139546	10.32.0.159	10.50.52.8	DNS	Standard query A news.goo.ne.jp
5434	16.141000	10.32.0.159	10.50.52.8	DNS	Standard query A ocntv.goo.ne.jp
5437	16.142500	10.32.0.159	10.50.52.8	DNS	Standard query A money.ocn.ne.jp
61				DNS	Standard query A broadband.ocn.ne.jp
61				DNS	Standard query A movie.goo.ne.jp
61				DNS	Standard query A music.goo.ne.jp
61				DNS	Standard query A musico.jp
61				DNS	Standard query A gravure.ocn.ne.jp
61				DNS	Standard query A cafe.ocn.ne.jp
61				DNS	Standard query A www.bidders.co.jp
61				DNS	Standard query A obento.ocn.ne.jp
61				DNS	Standard query A ocn.study.goo.ne.jp
61				DNS	Standard query A ocn.job.goo.ne.jp
61				DNS	Standard query A ocn.autos.goo.ne.jp
61				DNS	Standard query A koibito.ocn.ne.jp
61				DNS	Standard query A rd.rakuten.co.jp
63				DNS	Standard query A journal.ocn.ne.jp
6331				DNS	Standard query A fun.ocn.ne.jp
6332	18.4...			DNS	Standard query A htm.ocn.ne.jp

62クエリ
(キャッシュ無し)

Broadcom NetXtreme Gigabit Ethernet Drive... Packets: 7851 Displayed: 63 Marked: 0 Profile: Default

Prefetchの実験結果 (www.ocn.ne.jp)

・Fire Fox 3.6.2 - DNS prefetchあり



The image shows a Wireshark packet capture window with a filter set to 'udp.port==53 and ip.src==10.32.0.159'. Two DNS query packets are highlighted with a red box:

No.	Time	Source	Destination	Protocol	Details
8494	7.068348	10.32.0.159	10.50.52.8	DNS	Standard query A nttcommunications.122.207.net
8608	7.449854	10.32.0.159	10.50.52.8	DNS	Standard query A ocntoday.blogzine.jp

A blue callout bubble with white text is overlaid on the lower part of the image, stating:

2クエリ
(キャッシュあり)

The status bar at the bottom of the Wireshark window shows 'Broadcom NetXtreme Gigabit Ethernet Driver', 'Packets: 11740 Displayed: 2 Marked: 0', and 'Profile: Default'.

Prefetchの実験結果 (www.ocn.ne.jp)

- google chrom 5.0.375.55 - DNS prefetchあり

The image shows a Wireshark packet capture window with a filter set to 'udp.port==53 and ip.src==10.32.0.159'. The packet list pane shows a series of DNS standard query requests. Two packets at the top are highlighted with a red box: packet 3268 (12.908245) and packet 4635 (25.187502), both showing a query for 'www.ocn.ne'. A white speech bubble points to these packets with the text 'www.ocn.ne の時点でクエリ送信'. A blue speech bubble at the bottom contains the text '63クエリ (キャッシュ無し)'. The background shows a list of other DNS queries for various domains like ad.nttnavi.co.jp, blog.ocn.ne.jp, etc.

No.	Time	Source	Destination	Protocol	Length	Info
3268	12.908245	10.32.0.159	10.50.52.8	DNS	Standard query A	www.ocn.ne
4635	25.187502	10.32.0.159	10.50.52.8	DNS	Standard query A	www.ocn.ne.jp
10503	70.775671	10.32.0.159	10.50.52.8	DNS	Standard query A	ad.nttnavi.co.jp
10889	71.171597	10.32.0.159	10.50.52.8	DNS	Standard query A	blog.ocn.ne.jp
10890	71.173029	10.32.0.159	10.50.52.8	DNS	Standard query A	cafe.ocn.ne.jp
10891	71.176694	10.32.0.159	10.50.52.8	DNS	Standard query A	cg101.ocn.ne.jp
10893	71.178452	10.32.0.159	10.50.52.8	DNS	Standard query A	broadband.ocn.ne.jp
10895	71.180537	10.32.0.159	10.50.52.8	DNS	Standard query A	cocoa.ntt.com
10896	71.181384	10.32.0.159	10.50.52.8	DNS	Standard query A	gravure.ocn.ne.jp
10897	71.182231	10.32.0.159	10.50.52.8	DNS	Standard query A	juicystyle.ocn.ne.jp
10898	71.183078	10.32.0.159	10.50.52.8	DNS	Standard query A	mail.ocn.ne.jp
10899	71.183925	10.32.0.159	10.50.52.8	DNS	Standard query A	map.ocn.ne.jp
10900	71.184772	10.32.0.159	10.50.52.8	DNS	Standard query A	money.ocn.ne.jp
10901	71.185619	10.32.0.159	10.50.52.8	DNS	Standard query A	movie.goo.ne.jp
10902	71.186466	10.32.0.159	10.50.52.8	DNS	Standard query A	music.goo.ne.jp
10903	71.187313	10.32.0.159	10.50.52.8	DNS	Standard query A	mypage.ocn.ne.jp
10904	71.188160	10.32.0.159	10.50.52.8	DNS	Standard query A	musico.jp
10905	71.189007	10.32.0.159	10.50.52.8	DNS	Standard query A	news.goo.ne.jp
10906	71.189854	10.32.0.159	10.50.52.8	DNS	Standard query A	ocn.bsearch.goo.ne.jp
10907	71.190701	10.32.0.159	10.50.52.8	DNS	Standard query A	obento.ocn.ne.jp
10908	71.191548	10.32.0.159	10.50.52.8	DNS	Standard query A	ocn.job.goo.ne.jp
10909	71.192395	10.32.0.159	10.50.52.8	DNS	Standard query A	ocndictionary.goo.ne.jp
10910	71.193242	10.32.0.159	10.50.52.8	DNS	Standard query A	ocn.dir.goo.ne.jp
10911	71.194089	10.32.0.159	10.50.52.8	DNS	Standard query A	ocnpostcode.goo.ne.jp
10912	71.194936	10.32.0.159	10.50.52.8	DNS	Standard query A	ocnsearch.goo.ne.jp
10913	71.195783	10.32.0.159	10.50.52.8	DNS	Standard query A	ocntownpage.goo.ne.jp
10914	71.196630	10.32.0.159	10.50.52.8	DNS	Standard query A	ocntransit.goo.ne.jp
10915	71.197477	10.32.0.159	10.50.52.8	DNS	Standard query A	ocntoday.blogzine.jp
10916	71.198324	10.32.0.159	10.50.52.8	DNS	Standard query A	ocntv.goo.ne.jp
10917	71.199171	10.32.0.159	10.50.52.8	DNS	Standard query A	urana1.ocn.ne.jp
10918	71.200018	10.32.0.159	10.50.52.8	DNS	Standard query A	www.goo.ne.jp
10919	71.200865	10.32.0.159	10.50.52.8	DNS	Standard query A	www.bidders.co.jp
10920	71.201712	10.32.0.159	10.50.52.8	DNS	Standard query A	cdn.nttnavi.co.jp
10921	71.202559	10.32.0.159	10.50.52.8	DNS	Standard query A	www.ocn.rakuten.co.jp
10922	71.203406	10.32.0.159	10.50.52.8	DNS	Standard query A	bbm.ocn.ne.jp
10923	71.204253	10.32.0.159	10.50.52.8	DNS	Standard query A	brillier.ocn.ne.jp
10924	71.205100	10.32.0.159	10.50.52.8	DNS	Standard query A	journal.ocn.ne.jp
10925	71.205947	10.32.0.159	10.50.52.8	DNS	Standard query A	rad.msn.com
10926	71.206794	10.32.0.159	10.50.52.8	DNS	Standard query A	nttcommunications.122.2o7.net
10927	71.207641	10.32.0.159	10.50.52.8	DNS	Standard query A	digimaga.ocn.ne.jp
10928	71.208488	10.32.0.159	10.50.52.8	DNS	Standard query A	ecoblog.ocn.ne.jp
10929	71.209335	10.32.0.159	10.50.52.8	DNS	Standard query A	506506.ntt.com
10930	71.210182	10.32.0.159	10.50.52.8	DNS	Standard query A	faminavi.in