

DNS prefetchの影響

(JANOG24 lightning talk)

NTT Communications, OCN

吉村 知夏

chika.yoshimura@ntt.com

yosimura@ocn.ad.jp

DNS prefetchとは

- もともとはgoogle chromeの実装
 - リンク先のFQDNの名前解決を、あらかじめ行っておく
 - 名前解決の時間を短縮することで、WEBブラウジングの体感速度を高める
- DNSのquery数が増えることが予想される

www.ocn.ne.jpを見た場合

- google chrome 2.0.172.28
 - DNS prefetchなし

The image shows a Wireshark capture of a network packet. The filter is set to 'dns.flags.response != 1'. The packet list shows four DNS standard query A requests from 10.0.1.3 to 10.0.1.1. The first query is for www.ocn.ne.jp, followed by ad.nttnavi.co.jp, jxm.n.nttnavi.co.jp, and nttcommunications.122.2o7.net. A red oval highlights these four queries, and a bracket on the right indicates they are grouped together. Below the packet list, the details of the first frame are shown, including the protocol stack (eth:ip:udp:dns) and the raw packet bytes.

No.	Time	Source	Destination	Protocol	Info
1	0.000000	10.0.1.3	10.0.1.1	DNS	Standard query A www.ocn.ne.jp
3	0.332371	10.0.1.3	10.0.1.1	DNS	Standard query A ad.nttnavi.co.jp
5	2.046247	10.0.1.3	10.0.1.1	DNS	Standard query A jxm.n.nttnavi.co.jp
7	2.264435	10.0.1.3	10.0.1.1	DNS	Standard query A nttcommunications.122.2o7.net

www.ocn.ne.jpのクエリ
flushコンテンツのリンク先のクエリ など

4クエリ

www.ocn.ne.jpを見た場合

- google chrome 2.0.172.28
 - DNS prefetchあり

chrome_prefetch.pcap - Wireshark

Filter: dns.flags.response != 1

No.	Time	Source	Destination	Protocol	Info
1	0.000000	10.0.1.3	10.0.1.1	DNS	standard query A cdn.nttnavi.co.jp
2	0.002014	10.0.1.3	10.0.1.1	DNS	standard query A jxmn.nttnavi.co.jp
5	0.628030	10.0.1.3	10.0.1.1	DNS	standard query A 506506.ntt.com
7	0.630051	10.0.1.3	10.0.1.1	DNS	standard query A briller.ocn.ne.jp
9	0.635404	10.0.1.3	10.0.1.1	DNS	standard query A books.rakuten.co.jp
11	0.637735	10.0.1.3	10.0.1.1	DNS	standard query A blog.ocn.ne.jp
12	0.637831	10.0.1.3	10.0.1.1	DNS	standard query A broadband.ocn.ne.jp
13	0.640156	10.0.1.3	10.0.1.1	DNS	standard query A cafe.ocn.ne.jp
14	0.640158	10.0.1.3	10.0.1.1	DNS	standard query A cliplife.goo.ne.jp
17	0.652678	10.0.1.3	10.0.1.1	DNS	standard query A cocoa.ntt.com
19	0.660689	10.0.1.3	10.0.1.1	DNS	standard query A fun.ocn.ne.jp
21	0.665364	10.0.1.3	10.0.1.1	DNS	standard query A gravure.ocn.ne.jp
22	0.665365	10.0.1.3	10.0.1.1	DNS	standard query A kabegami.ocn.ne.jp
24	0.672395	10.0.1.3	10.0.1.1	DNS	standard query A map.ocn.ne.jp
27	0.677330	10.0.1.3	10.0.1.1	DNS	standard query A money.ocn.ne.jp
28	0.677337	10.0.1.3	10.0.1.1	DNS	standard query A movie.goo.ne.jp
31	0.688035	10.0.1.3	10.0.1.1	DNS	standard query A music.goo.ne.jp
33	0.692484	10.0.1.3	10.0.1.1	DNS	standard query A musico.jp
35	0.703563	10.0.1.3	10.0.1.1	DNS	standard query A ocn.dir.goo.ne.jp
36	0.707195	10.0.1.3	10.0.1.1	DNS	standard query A ocn.bsearch.goo.ne.jp
37	0.706781	10.0.1.3	10.0.1.1	DNS	standard query A news.goo.ne.jp
38	0.708297	10.0.1.3	10.0.1.1	DNS	standard query A ocn.dictionary.goo.ne.jp
39	0.708796	10.0.1.3	10.0.1.1	DNS	standard query A ocn.postcode.goo.ne.jp
42	0.714256	10.0.1.3	10.0.1.1	DNS	standard query A ocnsearch.goo.ne.jp
48	0.726779	10.0.1.3	10.0.1.1	DNS	standard query A ocntoday.blogzine.jp
50	0.739167	10.0.1.3	10.0.1.1	DNS	standard query A ocnhomepage.goo.ne.jp
52	0.742952	10.0.1.3	10.0.1.1	DNS	standard query A ocntransit.goo.ne.jp
53	0.743000	10.0.1.3	10.0.1.1	DNS	standard query A photofind.jp

www.ocn.ne.jpのクエリ
flushコンテンツのLink先のクエリ
プラス
LinkしているFQDNのクエリ

47クエリ
(約12倍)

www.ocn.ne.jpを見た場合

- Firefox 3.5

- DNS prefetchなし (network.dns.disablePrefetch:true)

The image shows a Wireshark capture of network traffic from Firefox 3.5. The filter is set to 'dns.flags.response != 1', which displays only DNS queries. Five queries are listed in the packet list pane, all from source IP 10.0.1.2 to destination IP 10.0.1.1. The queries are for www.ocn.ne.jp, ad.nttnavi.co.jp, cdn.nttnavi.co.jp, jxmn.nttnavi.co.jp, and nttcommunications.122.2o7.net. A red oval highlights these five rows. The packet details pane shows the first query (Frame 1) with a length of 73 bytes. The packet bytes pane shows the raw data of the first query, which is a standard query for www.ocn.ne.jp.

time	src addr	dst addr	protocol	information	length
0.882500	10.0.1.2	10.0.1.1	DNS	Standard query A www.ocn.ne.jp	73
0.506545	10.0.1.2	10.0.1.1	DNS	Standard query A ad.nttnavi.co.jp	76
0.887929	10.0.1.2	10.0.1.1	DNS	Standard query A cdn.nttnavi.co.jp	77
1.153843	10.0.1.2	10.0.1.1	DNS	Standard query A jxmn.nttnavi.co.jp	88
1.129055	10.0.1.2	10.0.1.1	DNS	Standard query A nttcommunications.122.2o7.net	89

Frame 1 (73 bytes on wire, 73 bytes captured)
Arrival Time: Jul 9, 2009 00:19:43.824838000
[Time delta from previous captured frame: 0.000000000 seconds]
[Time delta from previous displayed frame: 0.000000000 seconds]
[Time since reference or first frame: 0.000000000 seconds]
Frame Number: 1
Frame Length: 73 bytes
Capture Length: 73 bytes
[Frame is marked: False]
[Protocols in frame: eth:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]

Ethernet II, Src: Intel c3:02:0a (00:16:ea:c3:02:0a), Dst: AppleCom ea:82:71 (00:11:24:ea:82:71)

```
0000 00 11 24 ea 82 71 00 16 ea c3 02 0a 08 00 45 00  ..$.q.. .....
```

5クエリ

www.ocn.ne.jpを見た場合

- Firefox 3.5
 - DNS prefetchあり(default設定)

The image shows a Wireshark capture of network traffic from Firefox 3.5. The filter is set to 'dns.flags.response != 1', showing a list of DNS queries. A red circle highlights the first 59 queries, which are all standard queries for various domains. A callout bubble on the right contains the text '59クエリ (約12倍)'. Below the list, the details of the first frame (73 bytes) are shown, including the arrival time and protocols in the frame.

time	src addr	dst addr	protocol	information	length
0.000000	10.0.1.2	10.0.1.1	DNS	Standard query A www.ocn.ne.jp	73
3.408871	10.0.1.2	10.0.1.1	DNS	Standard query A ad.nttnavi.co.jp	76
3.993068	10.0.1.2	10.0.1.1	DNS	Standard query A cdn.nttnavi.co.jp	77
4.320592	10.0.1.2	10.0.1.1	DNS	Standard query A jxmn.nttnavi.co.jp	78
7.658198	10.0.1.2	10.0.1.1	DNS	Standard query A nttcommunications.122.2o7.net	89
8.170527	10.0.1.2	10.0.1.1	DNS	Standard query A ocntoday.bloggine.jp	80
8.270175	10.0.1.2	10.0.1.1	DNS	Standard query A ocn.bsearch.goo.ne.jp	81
8.285732	10.0.1.2	10.0.1.1	DNS	Standard query A blog.ocn.ne.jp	74
8.292856	10.0.1.2	10.0.1.1	DNS	Standard query A ocn.dir.goo.ne.jp	77
8.298330	10.0.1.2	10.0.1.1	DNS	Standard query A ocn.dictionary.goo.ne.jp	83
8.309306	10.0.1.2	10.0.1.1	DNS	Standard query A ocntownpage.goo.ne.jp	81
8.324372	10.0.1.2	10.0.1.1	DNS	Standard query A map.ocn.ne.jp	73
8.329962	10.0.1.2	10.0.1.1	DNS	Standard query A ocntransit.goo.ne.jp	80
8.338844	10.0.1.2	10.0.1.1	DNS	Standard query A www.goo.ne.jp	73
8.356467	10.0.1.2	10.0.1.1	DNS	Standard query A ocnsearch.goo.ne.jp	79
8.361855	10.0.1.2	10.0.1.1	DNS	Standard query A 506506.ntt.com	74
8.365108	10.0.1.2	10.0.1.1	DNS	Standard query A broadband.ocn.ne.jp	79
8.390519	10.0.1.2	10.0.1.1	DNS	Standard query A juicystyle.ocn.ne.jp	80
8.395425	10.0.1.2	10.0.1.1	DNS	Standard query A cocoa.ntt.com	73
8.398959	10.0.1.2	10.0.1.1	DNS	Standard query A fun.ocn.ne.jp	77
8.400380	10.0.1.2	10.0.1.1	DNS	Standard query A kidscare.ocn.ne.jp	78
8.423653	10.0.1.2	10.0.1.1	DNS	Standard query A www.my-affiliate.com	80
8.426676	10.0.1.2	10.0.1.1	DNS	Standard query A tr.my-affiliate.com	79
8.450507	10.0.1.2	10.0.1.1	DNS	Standard query A cafe.ocn.ne.jp	74
8.453856	10.0.1.2	10.0.1.1	DNS	Standard query A name-ocn.ne.jp	77

Frame 1 (73 bytes on wire (73 bytes captured))
Arrival Time: Jul 9, 2009 00:04:53.940000000
[Time delta from previous captured frame: 0.000000000 seconds]
[Time delta from previous displayed frame: 0.000000000 seconds]
[Time since reference or first frame: 0.000000000 seconds]
Frame Number: 1
Frame Length: 73 bytes
Capture Length: 73 bytes
[Frame is marked: False]
[Protocols in frame: eth:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]

```
0000 00 11 24 ea 82 71 00 16 ea c3 02 0a 08 00 45 00  ..$.q... ..E.  
0010 00 3b 39 b5 00 00 80 11 ea fa 0a 00 01 02 0a 00  ;9.....  
0020 01 01 fb bb 00 35 00 27 e5 db 51 23 01 00 00 01  ....5...Q#...  
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....
```

"!" may have unexpected results (see... Packets: 118 Displayed: 59 Marked: 0

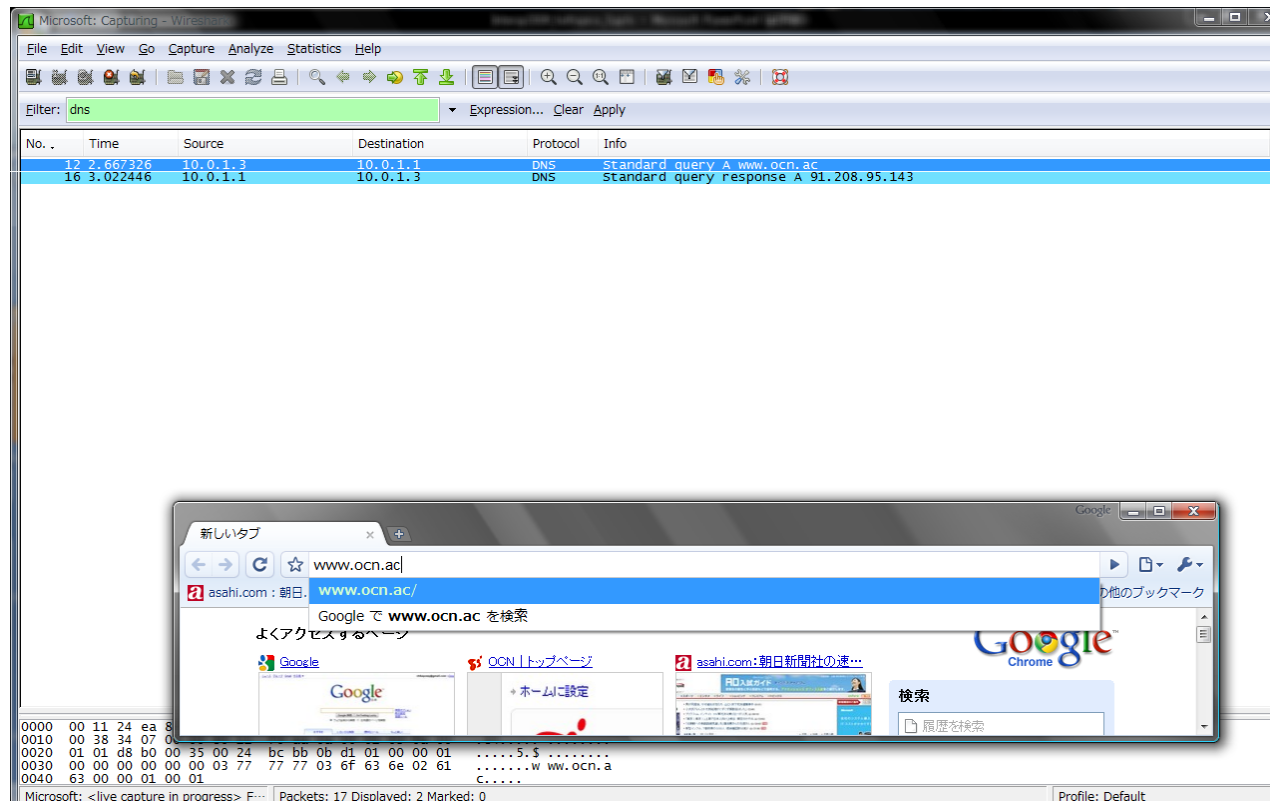
59クエリ
(約12倍)

DNS prefetchとは

- prefetchあり/なしで、query数に10倍以上の差が出る
 - どの程度増加するかは、WEBページのリンク数に依存する
- さらにchromeでちょっと実験

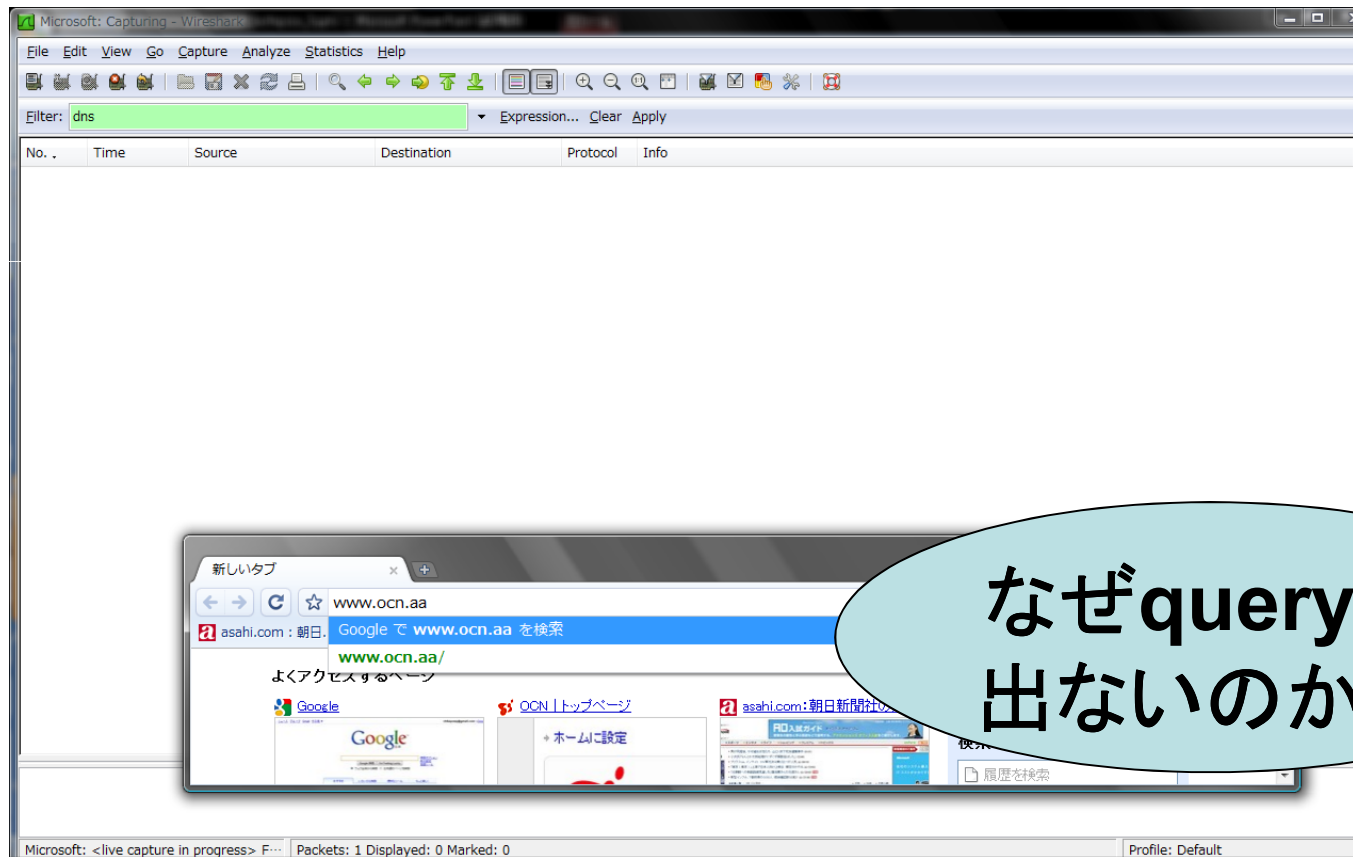
ちょっと実験

- google chrome 2.0.172.28 + prefetchあり
- www.ocn.ac
- Enterを打ってないがqueryは送信される



ちょっと実験

- **www.ocn.aa**
- **queryは送信されない**



ちょっと実験

- **www.ocn.a[a-z](26FQDN)を全部試してみた**

No.	Time	Source	Destination	Protocol	Info
163	36.324120	10.0.1.1	10.0.1.3	DNS	Standard query response, No such name
178	43.926874	10.0.1.3	10.0.1.1	DNS	Standard query A www.ocn.a1
182	44.308596	10.0.1.1	10.0.1.3	DNS	Standard query response, No such name
187	45.843568	10.0.1.3	10.0.1.1	DNS	Standard query A www.ocn.am
188	45.867035	10.0.1.1	10.0.1.3	DNS	Standard query response, No such name
196	48.211585	10.0.1.3	10.0.1.1	DNS	Standard query A www.ocn.an
197	48.214853	10.0.1.1	10.0.1.3	DNS	Standard query response, No such name
201	53.901217	10.0.1.3	10.0.1.1	DNS	Standard query A www.ocn.ao
202	54.056417	10.0.1.1	10.0.1.3	DNS	Standard query response, No such name
213	57.944364	10.0.1.3	10.0.1.1	DNS	Standard query A www.ocn.aq
216	58.251952	10.0.1.1	10.0.1.3	DNS	Standard query response, No such name
221	60.108655	10.0.1.3	10.0.1.1	DNS	Standard query A www.ocn.ar
222	60.282648	10.0.1.1	10.0.1.3	DNS	Standard query response, No such name
232	63.494726	10.0.1.3	10.0.1.1	DNS	Standard query A www.ocn.as
233	63.497985	10.0.1.1	10.0.1.3	DNS	Standard query response, No such name
241	65.121475	10.0.1.3	10.0.1.1	DNS	Standard query A www.ocn.at
245	65.425566	10.0.1.1	10.0.1.3	DNS	Standard query response A 80.92.66.6
247	67.085107	10.0.1.3	10.0.1.1	DNS	Standard query A www.ocn.au
248	67.245753	10.0.1.1	10.0.1.3	DNS	Standard query response, No such name
260	74.800235	10.0.1.3	10.0.1.1	DNS	Standard query A www.ocn.aw
263	75.049845	10.0.1.1	10.0.1.3	DNS	Standard query response, No such name
269	76.938419	10.0.1.3	10.0.1.1	DNS	Standard query A www.ocn.ax
274	77.479993	10.0.1.1	10.0.1.3	DNS	Standard query response, No such name
281	81.471559	10.0.1.3	10.0.1.1	DNS	Standard query A www.ocn.az
283	81.680669	10.0.1.1	10.0.1.3	DNS	Standard query response, No such name

Frame 14 (70 bytes on wire, 70 bytes captured)
Arrival Time: May 24, 2009 07:11:47.291779000
[Time delta from previous captured frame: 0.000000000]
[Time delta from previous displayed frame: 0.000000000]
[Time since reference or first frame: 0.000000000]
Frame Number: 14
Frame Length: 70 bytes
Capture Length: 70 bytes
[Frame is marked: False]
[Protocols in frame: eth:ip:udp:dns]
Ethernet II, Src: Intel_c3:02:0a (00:16:8c:00:02:0a), Dst: Intel_c3:02:0a (00:16:8c:00:02:0a), Protocol: IP, Length: 60, Metric: 0
0000 00 11 24 ea 82 71 00 16 ea c3 02 0a
0010 00 38 3f da 00 00 80 11 e4 d7 0a 00
0020 01 01 f5 42 00 35 00 24 8e f5 1d 05
0030 00 00 00 00 00 00 03 77 77 77 03 6f
0040 63 00 00 01 00 01

Microsoft: <live capture in progress> F... Packets: 318 Displayed: 46 Marked: 0

新しいタブ
www.ocn.az/

Google で www.ocn.az を検索

よくアクセスするページ
Google

asahi.com: 朝日新聞

ccTLDが存在しない場合は、
queryを送らない

ちょっと実験

- **www.ocn.o[a-z](26FQDN)を全部試してみた**

The screenshot shows a Wireshark capture of a DNS query and response. The packet list pane shows two packets: a standard query A for www.ocn.om (No. 49) and a standard query response, No such name (No. 50). The packet details pane shows the query structure: Ethernet II, Internet Protocol (10.0.1.3 to 10.0.1.1), and Internet Protocol (10.0.1.3 to 10.0.1.1). The raw data pane shows the hex and ASCII representation of the query.

Overlaid on the Wireshark window is a Chrome browser window showing the address bar with `www.ocn.om` and a search bar with the text "Googleで www.ocn.om を検索". The browser page displays search results for "よくアクセスするページ" (Pages accessed frequently).

www.ocn.om(オマーンのccTLD)だけquery送信

ちょっと実験

- **www.ntt.co.jp** と打つ
- **www.ntt.co** の時点でquery送信

The image shows a Wireshark capture of a DNS query and response. The packet list pane shows four packets:

No.	Time	Source	Destination	Protocol	Info
1	0.000000	10.0.1.3	10.0.1.1	DNS	Standard query A www.ntt.co
2	0.167297	10.0.1.1	10.0.1.3	DNS	Standard query response, No such name
3	8.190710	10.0.1.3	10.0.1.1	DNS	Standard query A www.ntt.co.jp
4	8.258283	10.0.1.1	10.0.1.3	DNS	Standard query response A 163.137.191.238

The packet details pane for the third packet (No. 3) shows:

- Header checksum: 0x1d77 [correct]
- User Datagram Protocol, Src Port: 50919, Destination port: domain (53)
- Domain Name System (query)
- Transaction ID: 0x1c7e
- Flags: 0x0100 (standard query)

The packet bytes pane shows the raw data of the query, including the domain name 'www.ntt.co.jp'.

Overlaid on the Wireshark window is a Google Chrome browser window showing a search for 'www.ntt.co.jp'. The address bar contains 'www.ntt.co.jp' and a search box below it contains 'Google で www.ntt.co.jp を検索'. A light blue oval callout points to the 'co' part of the domain in the address bar.

coはコスタリカのccTLD

DNS prefetch まとめ

- **chrome**では、アドレスバーに入力した時点で**query**を送る
 - Firefoxでは送らない
- **chrome**では、存在するTLDかどうか判断して**query**を送る
- しかし、弊害あり。**ntt.co**の時点で**query**を送る
 - 無駄クエリとなる

DNSサーバへの影響

1. 端末が出すquery数は飛躍的に増える
 - 大規模キャッシュサーバにとって打撃あり
 - Firefox3.5では、DNS Prefetchはdefault ON
2. 1source IP addressごとのquery数を制限している場合は、注意が必要
 - バースト的にqueryが送信される

DNSサーバの管理者は、クエリ増加に備えて設定を見直しましょう