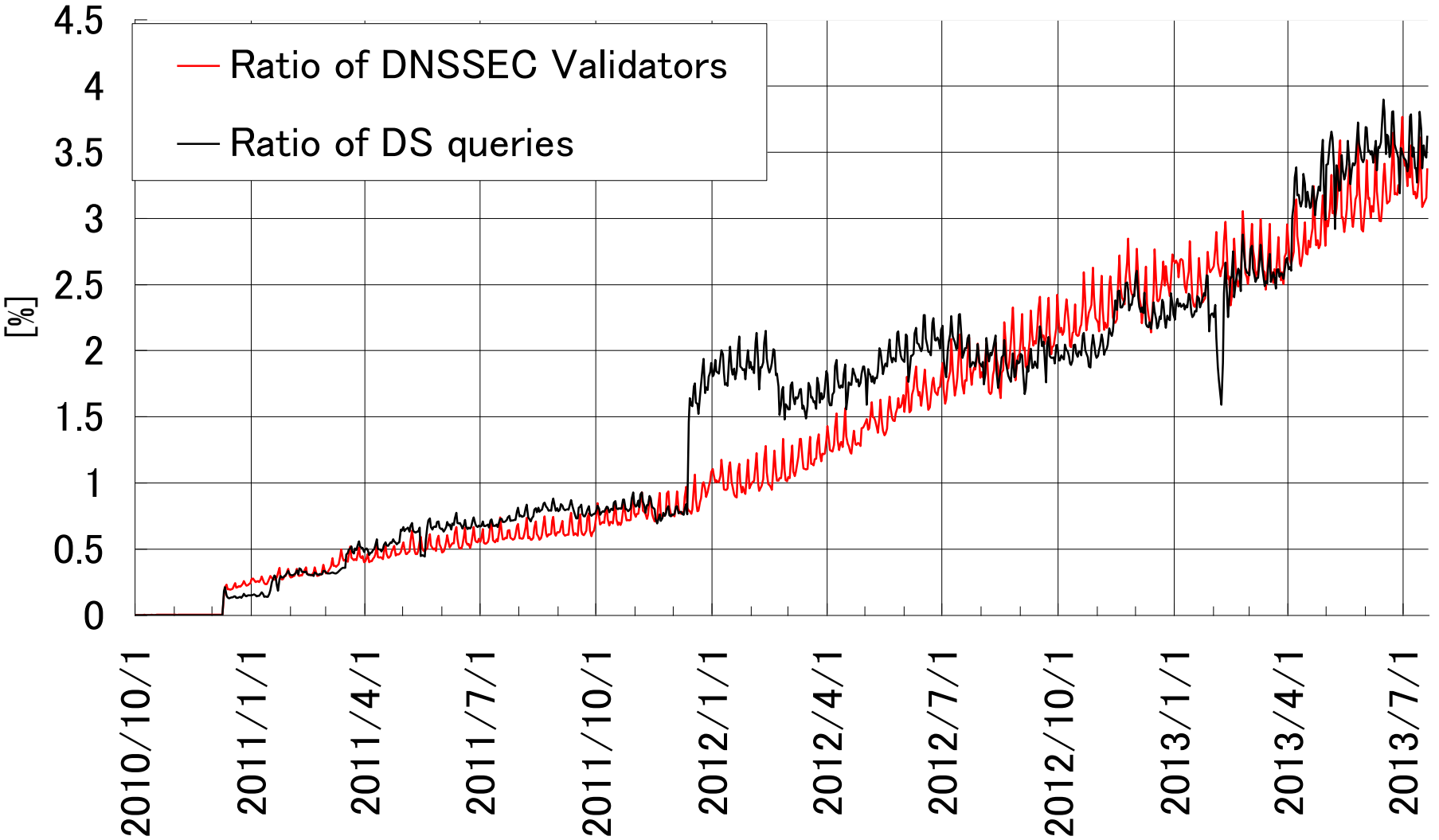
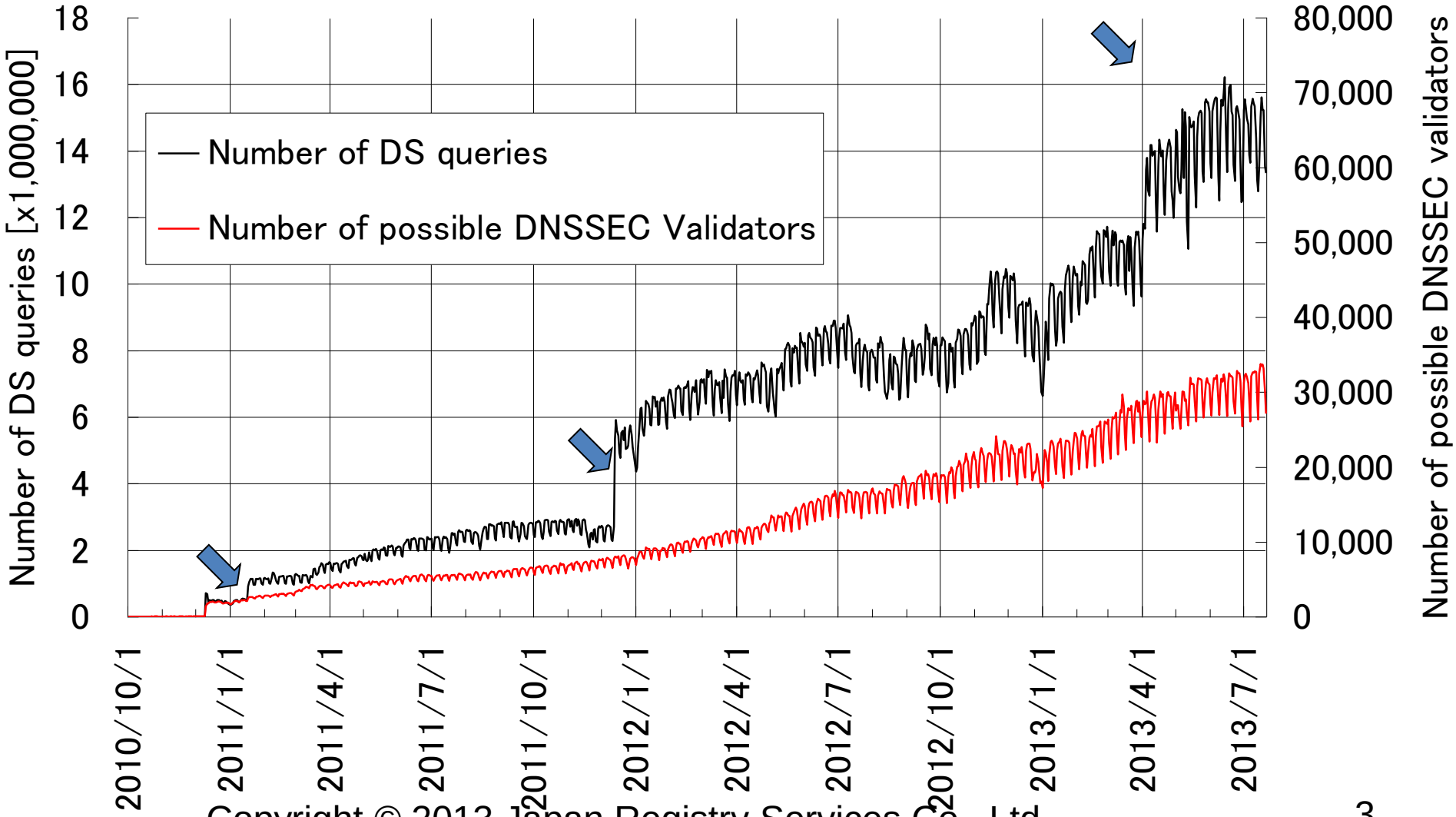
draft-fujiwara-dnsop-ds-query-increase-01
Side effect of DNSSEC
an increase of DS queries

Kazunori Fujiwara
<fujiwara@jprs.co.jp>

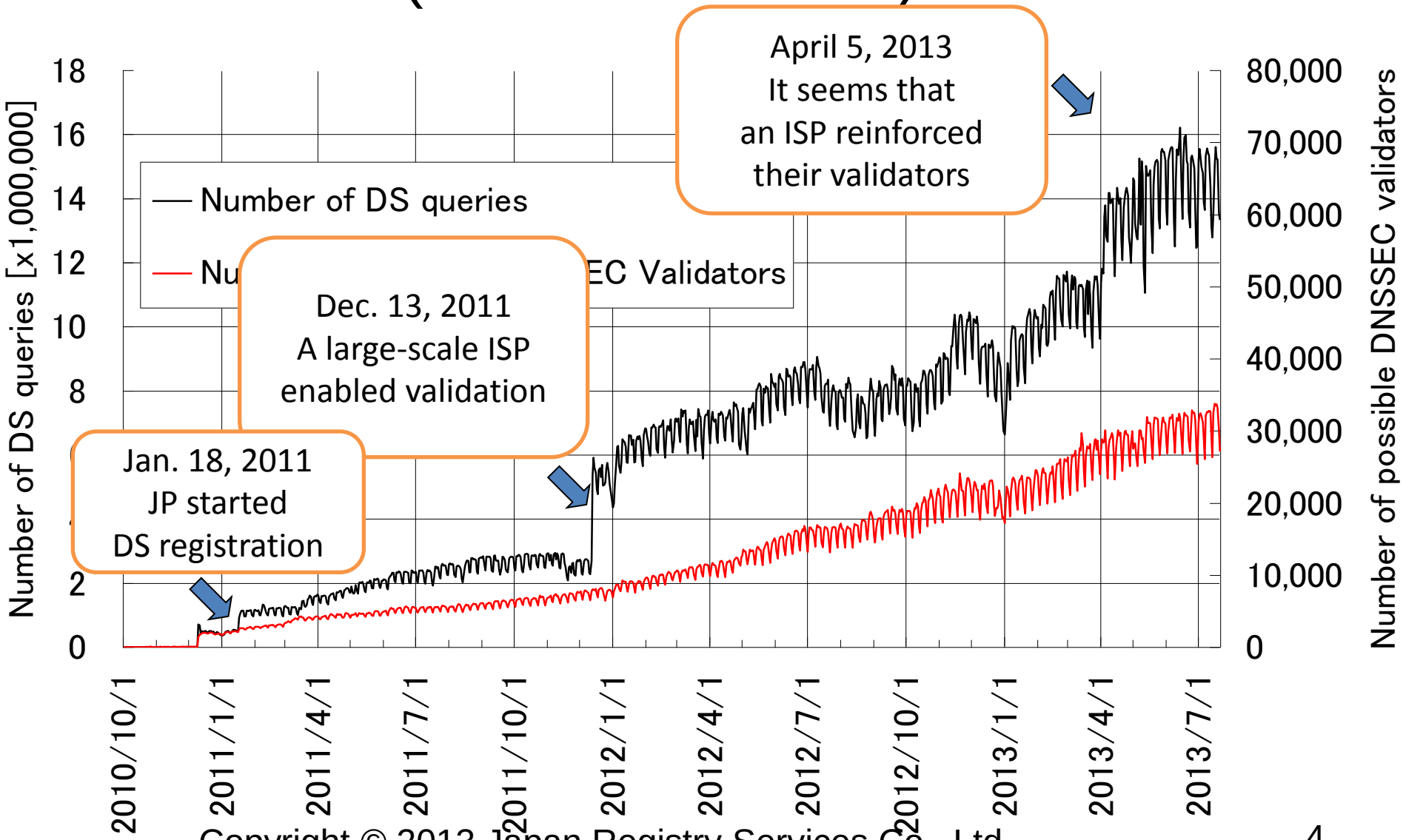
Ratio of DS queries seen at JP 2 of 7 servers, 24 hours data



Number of DS queries
(2 of 7 JP servers)



Number of DS queries
(2 of 7 JP servers)



A part of query log for a popular name from one IP address, 2 of 7 JP servers

30-Apr-2013 00:19:00.126 google.co.jp IN DS
30-Apr-2013 00:49:00.093 google.co.jp IN DS
30-Apr-2013 01:34:00.369 google.co.jp IN DS
30-Apr-2013 01:49:00.242 google.co.jp IN DS
30-Apr-2013 02:19:01.047 google.co.jp IN DS
30-Apr-2013 02:28:35.867 id.google.co.jp IN AAAA
30-Apr-2013 02:34:01.736 google.co.jp IN DS
30-Apr-2013 03:19:05.265 google.co.jp IN DS
30-Apr-2013 03:34:06.405 google.co.jp IN DS
30-Apr-2013 03:49:08.541 google.co.jp IN DS
30-Apr-2013 04:34:09.628 google.co.jp IN DS
30-Apr-2013 05:04:09.216 google.co.jp IN DS
30-Apr-2013 05:19:09.723 google.co.jp IN DS

One IP address sends many same (google.co.jp) DS queries.

Minimal time interval is 15 minutes, it is the same as JP NCACHE TTL

Reason of DS queries increase

- JP NCACHE TTL is 900, RR TTL is 86400
- Most of JP domain names are not signed
  - DS nonexistence (NSEC3) is cached only 900 sec
- Assume there is a popular query name
  - 1 or more queries per NCACHE TTL period
  - Its RR TTL is smaller than NCACHE TTL
  - It is not signed

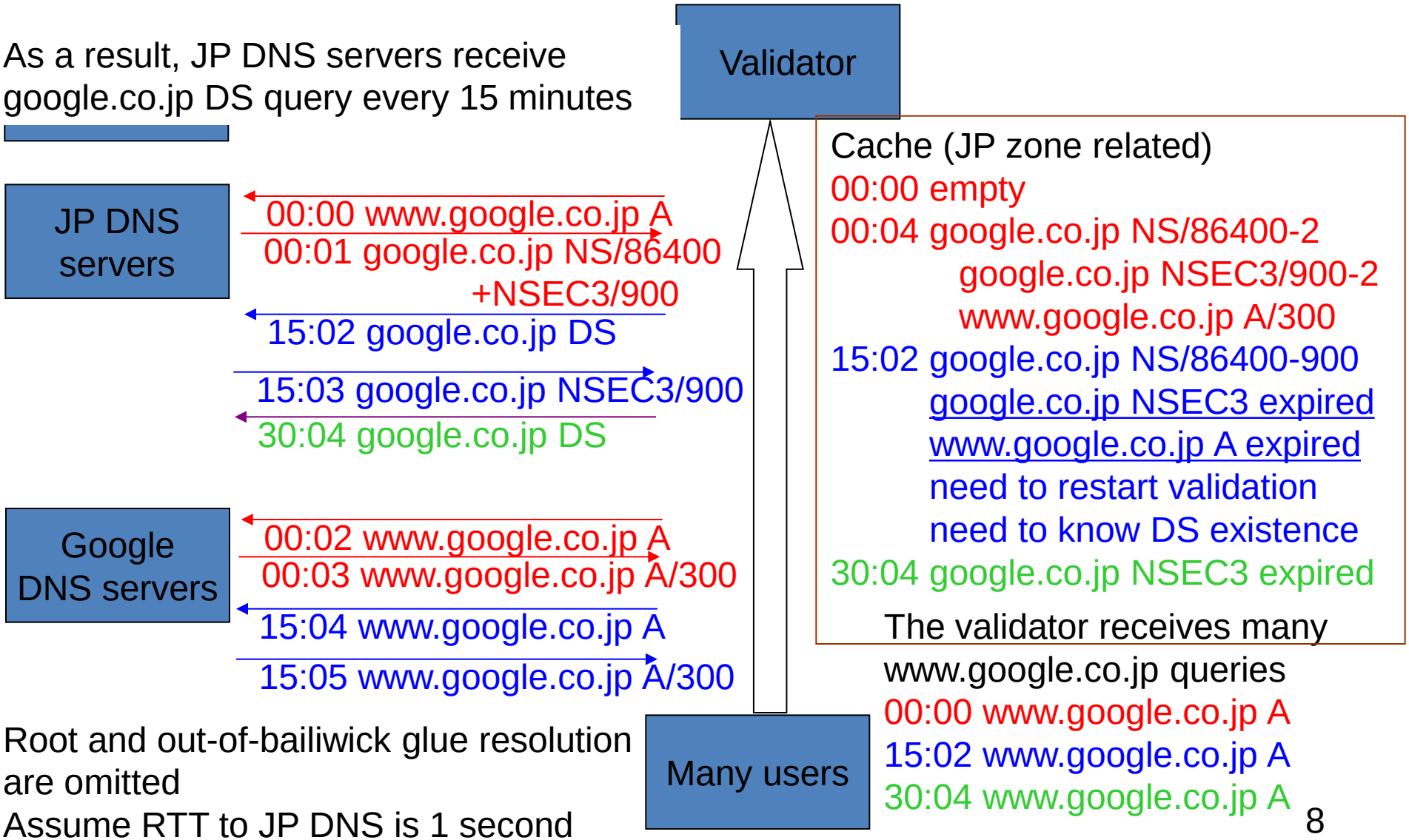
Reason of DS queries increase (2)

- Therefore,
  - Validating process starts for every NCACHE TTL period or more
  - The validator need to know DS nonexistence
- As a result, the validator sends
  - one non-DS query per a day
  - 95 (86400/900-1) DS queries per a day
  - It increases queries 96 times

- DNSSEC protocol and parameter issue

The "www.google.co.jp" case

As a result, JP DNS servers receive google.co.jp DS query every 15 minutes



Root and out-of-bailiwick glue resolution are omitted

Assume RTT to JP DNS is 1 second

Evaluation on existing implementations (BIND 9 and Unbound)

- Sending periodic queries to test validators
  - dig @validator QNAME A, every 5 minutes
  - Tested QNAMEs:
    - unsigned JP domain names
    - signed JP domain names (jprs.co.jp, jprs.jp)
    - unsigned com, net, org domain names
- Results
  - Both BIND 9 and Unbound validator send
  - DS queries of unsigned delegations to TLD DNS servers every 15 or 20 minutes
  - Depends on DS existence and RR TTL of qname/type
  - Other queries depend on their own TTL

Possible situations in the future

- When large-scale ISPs enable DNSSEC validation,

  their validators start sending periodic DS queries of popular and unsigned delegations
  - As you have seen before, this happened already

- Therefore, JP DNS servers would receive very large amount of DS queries in the future
  - Magnification factor is 96 (86400/900)
  - Pessimistically, queries to JP DNS servers would increase 96 times
  - And almost of them are DS

Possibly affected domains

- Delegation centric zones, signed, smaller NCACHE TTL
- Domain names (TTL / NCACHE) magnification
  - Most of gTLDs 86400 / 900 96 times
  - 172800 / 900 192 times
  - jp: 86400 / 900 96 times
  - root 86400 / (10800) 8 times
    - root is not affected because most of popular TLDs have signed
  - 193.in-addr.arpa 172800 / 3600 48 times

- Causion: RFC 2308 recommends the maximum value in the negative cache with 1 hour to 3 hours.

No good countermeasures

1. Accept all DS queries and reinforce infrastructures
2. Change DNS/DNSSEC protocol
3. Sign all domain names (so that DS will exist)
   - Possible ? TLD cannot control
4. Lengthen RR TTL of popular names
   - TLD cannot control
5. Lengthen NCACHE TTL 900 to 10800
   - Newly registered domain names become usable soon
   - Magnification factor changes 96 to 8
6. Add dummy DS to popular unsigned delegations
   - Dummy DS TTL value is controllable
   - Need new digest type and deep considerations
   - Is it allowed that TLDs add dummy DS RRs without registrants' consent?

Do you have other ideas ?

RFC 4035 Section 5.2

If the validator does not support any of the algorithms listed in an authenticated DS RRset, then the resolver has no supported authentication path leading from the parent to the child. The resolver should treat this case as it would the case of an authenticated NSEC RRset proving that no DS RRset exists, as described above.

Dummy DS Proposal

- Define new digest type
- The digest type claims unsigned delegation
- Add dummy DS for popular unsigned delegations

- Existing DNSSEC validators do not support newly defined digest type and they should treat the delegations as unsigned
  - I'm afraid that the child zones do not have DNSKEY RRs and validators allow or not (RFC 4035 does not describe well)

BIND 9 and Unbound ignore dummy DS RRs

- A delegation which has dummy DS RR
  - test.dnslab.jp. IN DS 0 0 255 FFFFFFFF
    - Key tag 0, Algorithm 0, Digest type 255
  - test.dnslab.jp. zone is not signed
    - It contains “*.test.dnslab.jp A”
- "www.test.dnslab.jp A" queries
  - Both BIND 9 and Unbound validators resolve well

Please comment

- Do you have many DS queries to unsigned delegations ?

- Do you have good idea ?