

**君のキャッシュDNSサーバが出すクエリ
を君は本当に理解しているか？**

**あ、でもそのうちそうなっちゃうかも？
～QNAME Minimisation の話～**

ENOG34@柏崎

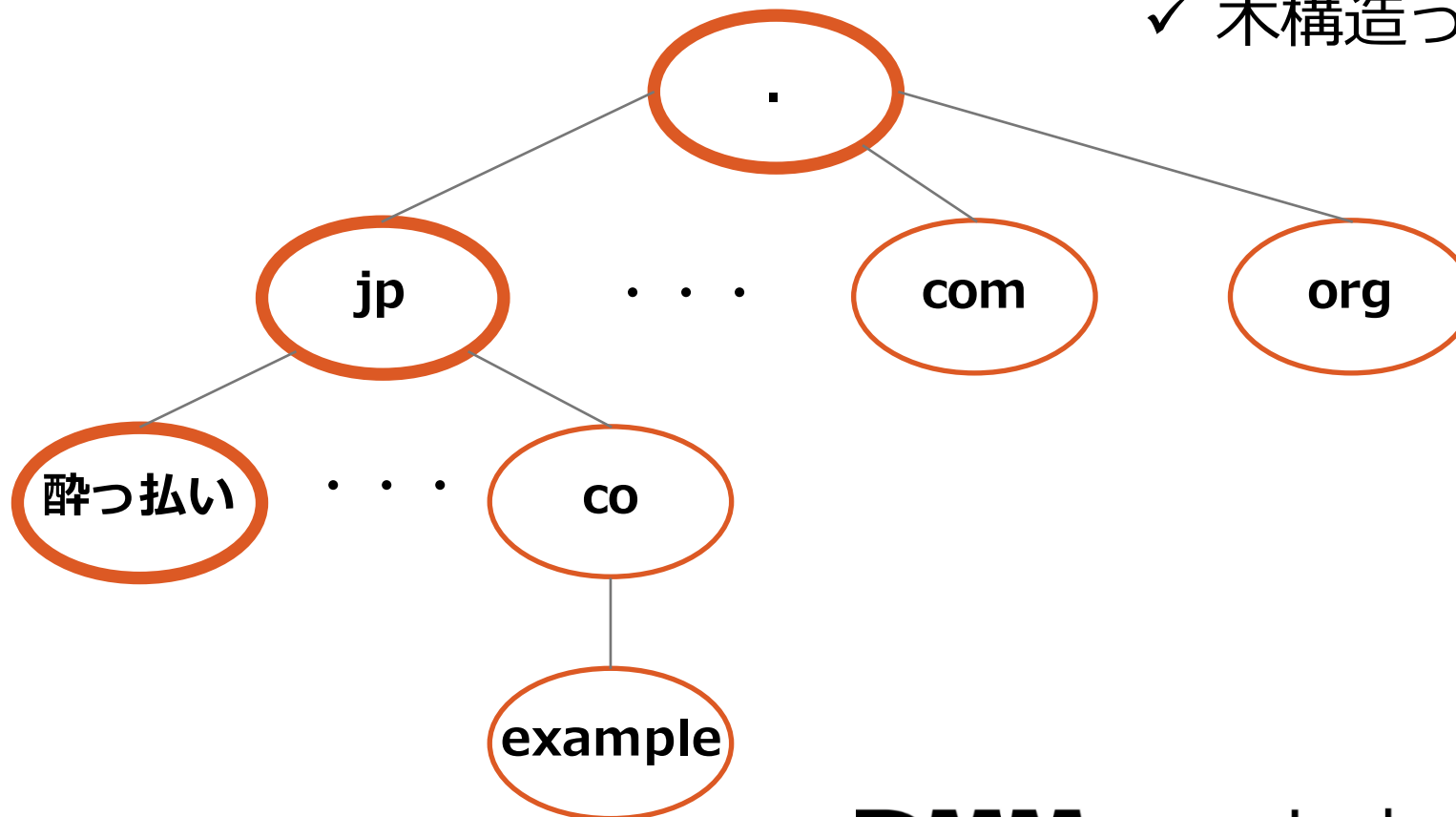
2015年9月4日

DMM.comラボ 高嶋隆一

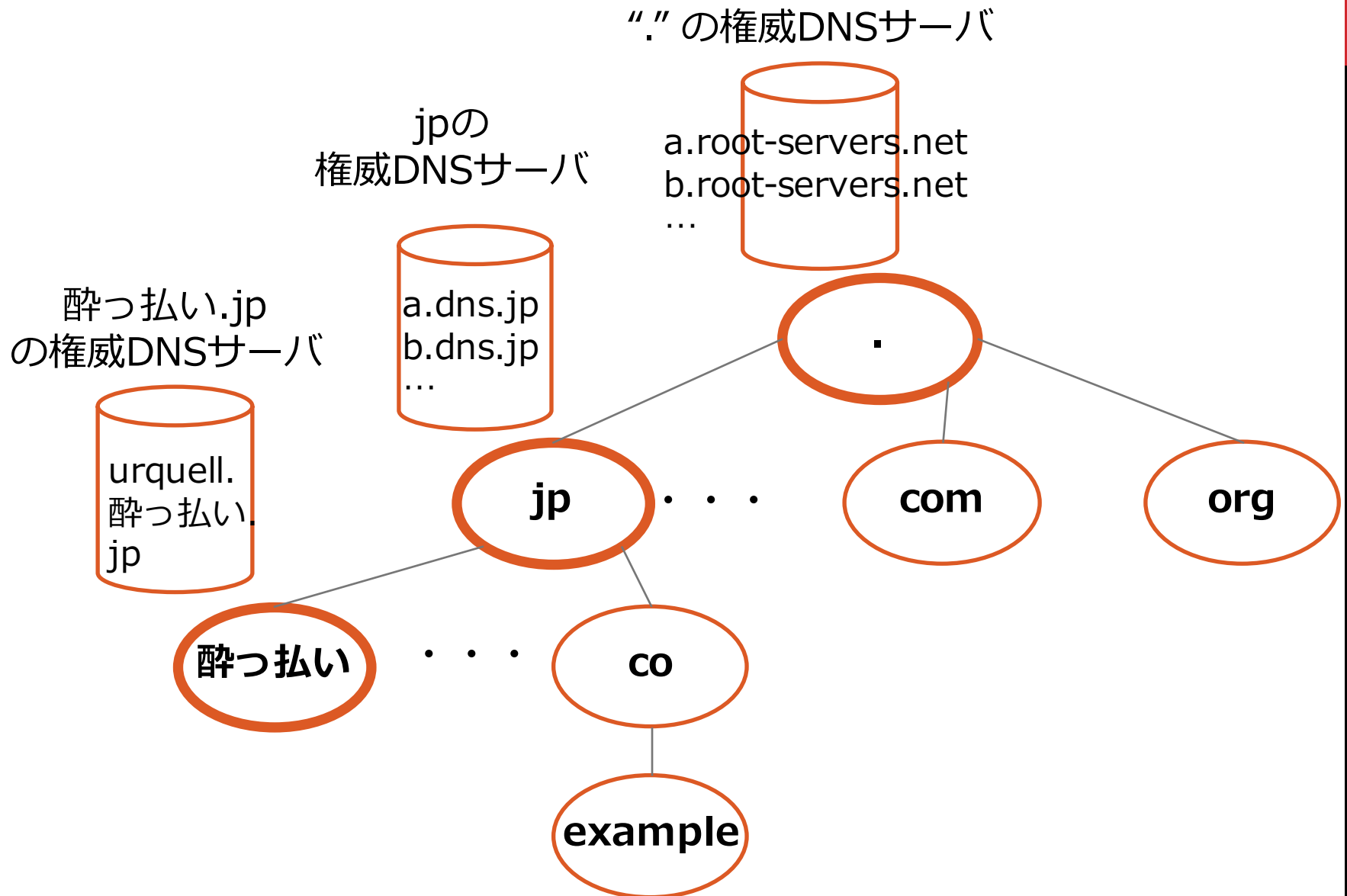
おさらい. ドメイン名は階層構造を持つ

酔っ払い . JP .

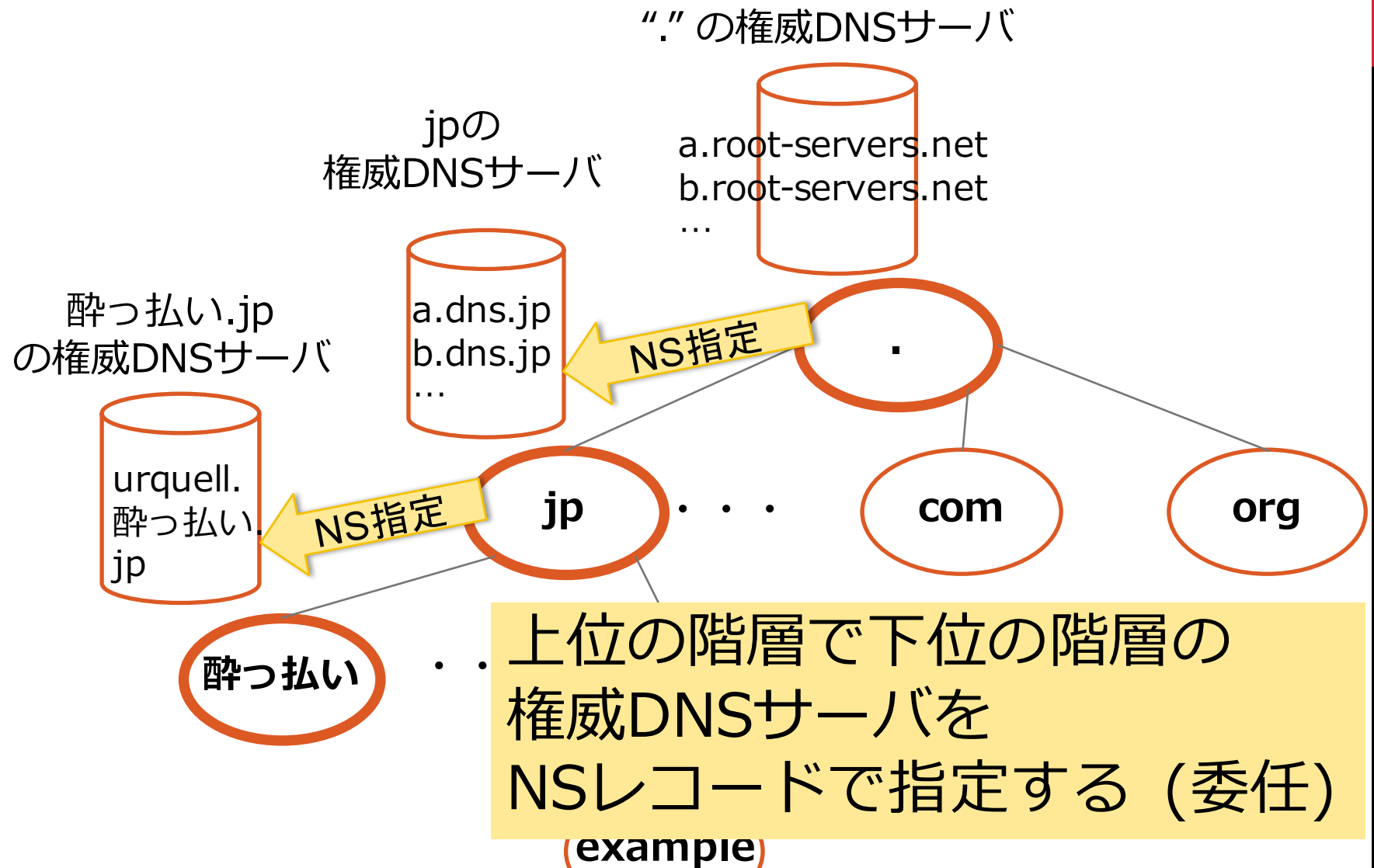
✓ 木構造っぽい



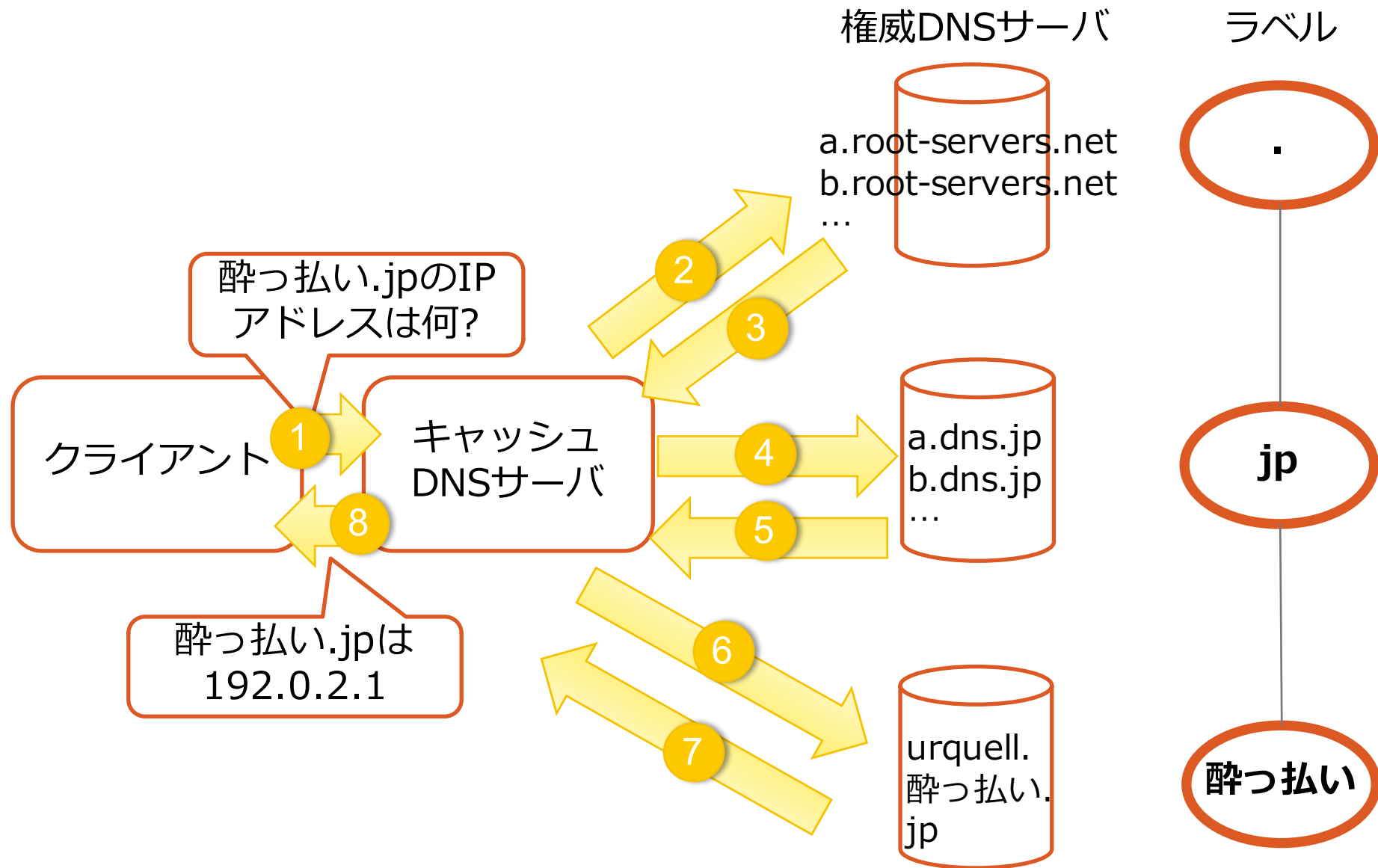
おさらい. 権威DNSサーバがいてデータを保管



おさらい. 権威DNSサーバがいてデータを保管

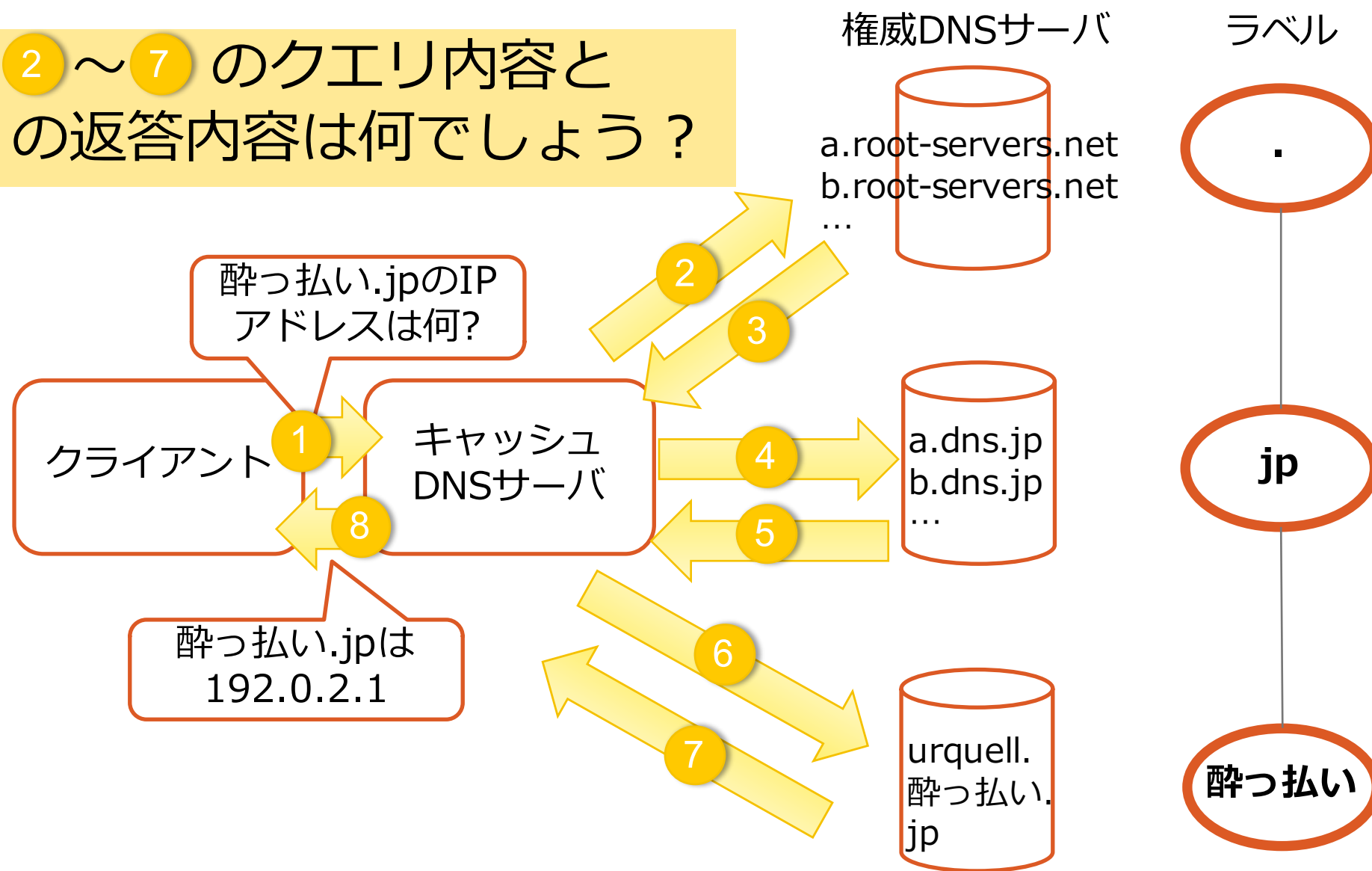


おさらい. キャッシュDNSサーバが "." の権威DNSサーバから順番に名前検索

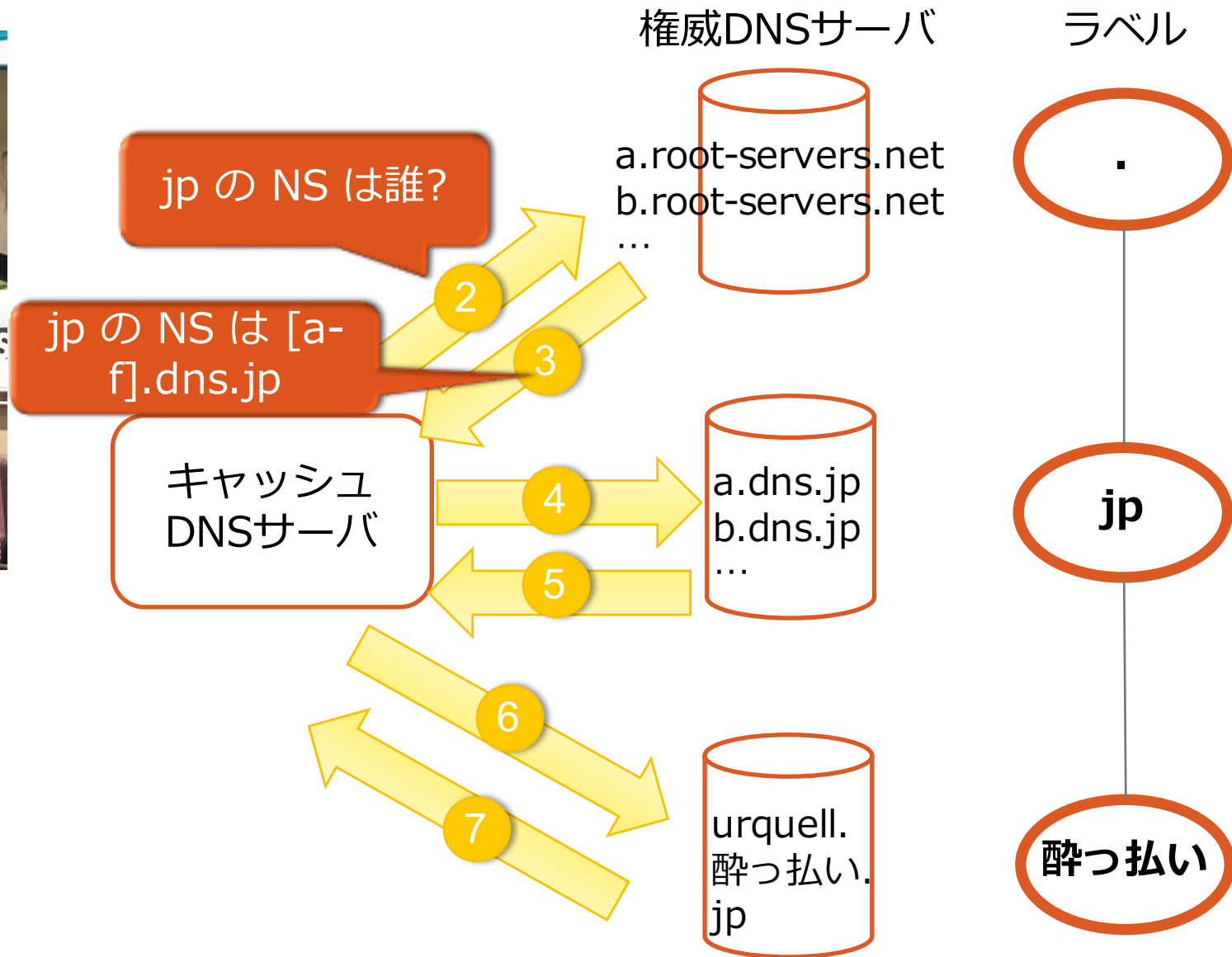
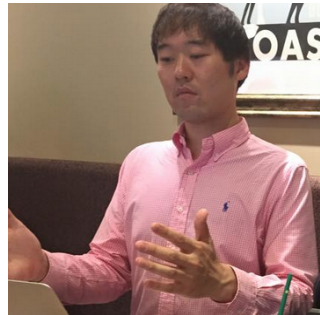


ここで質問です

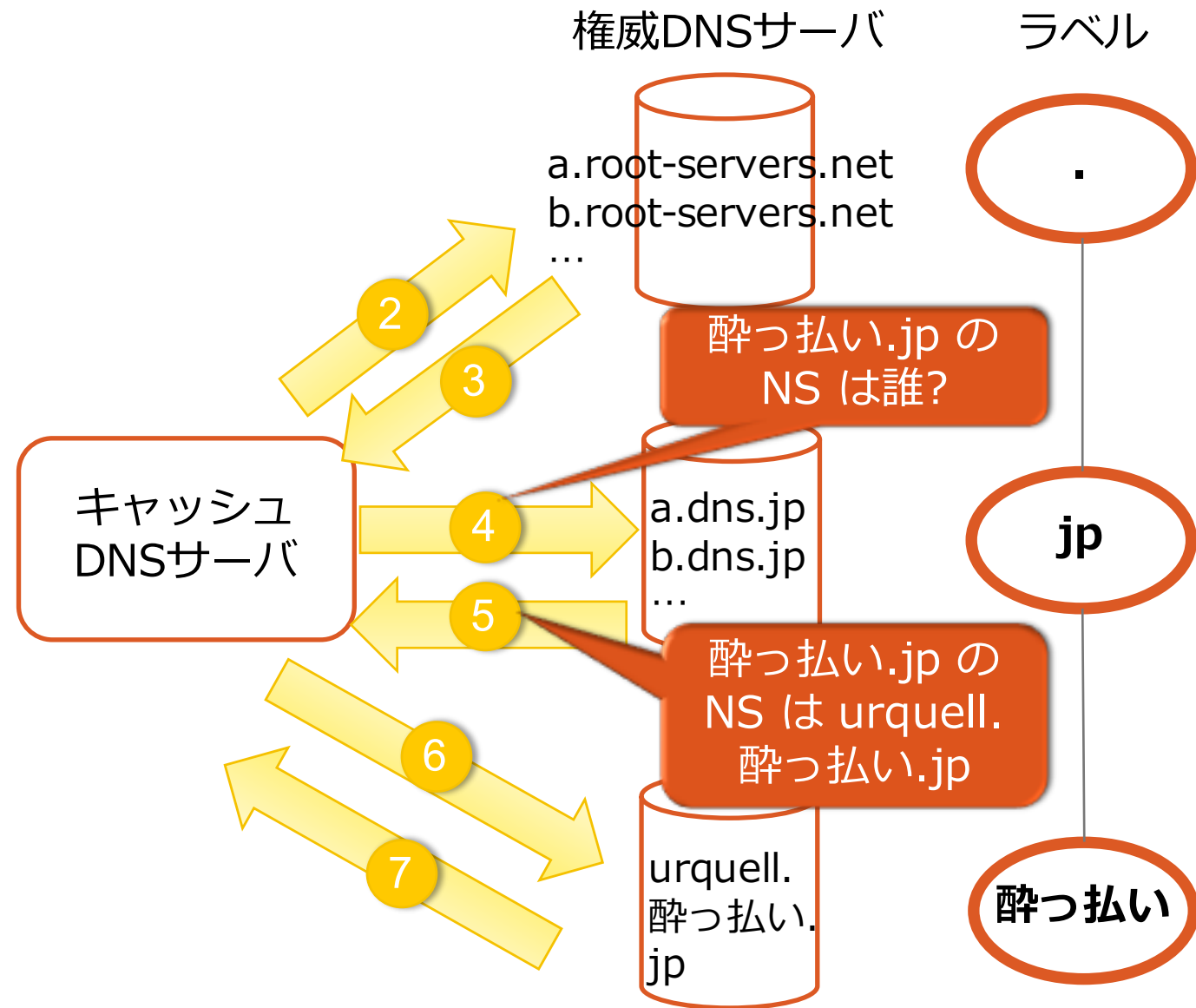
②～⑦ のクエリ内容との返答内容は何でしょう？



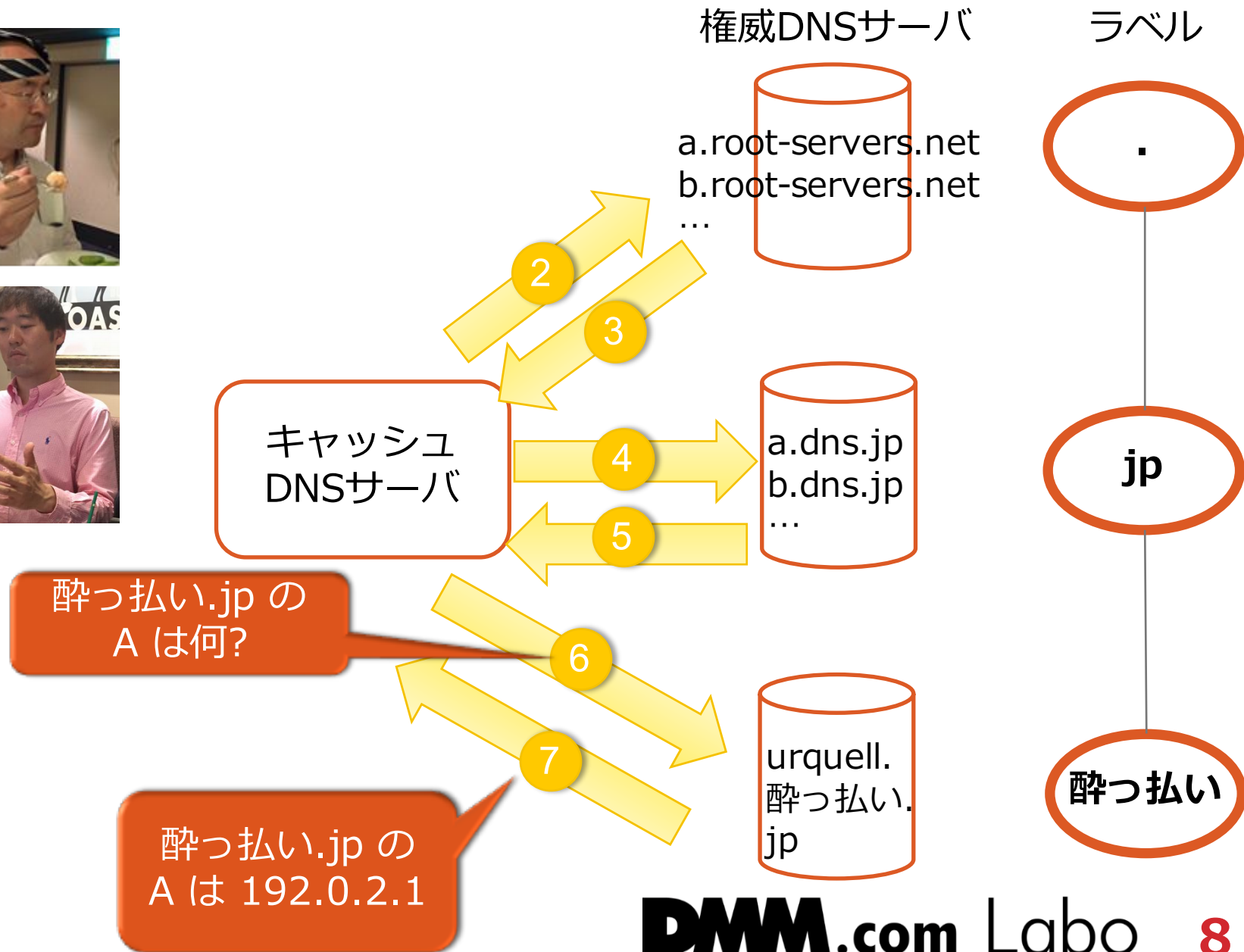
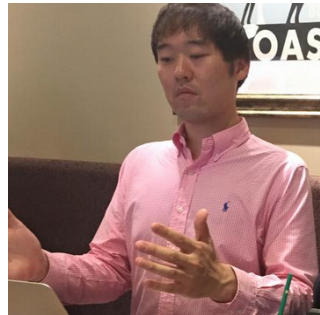
よくある回答



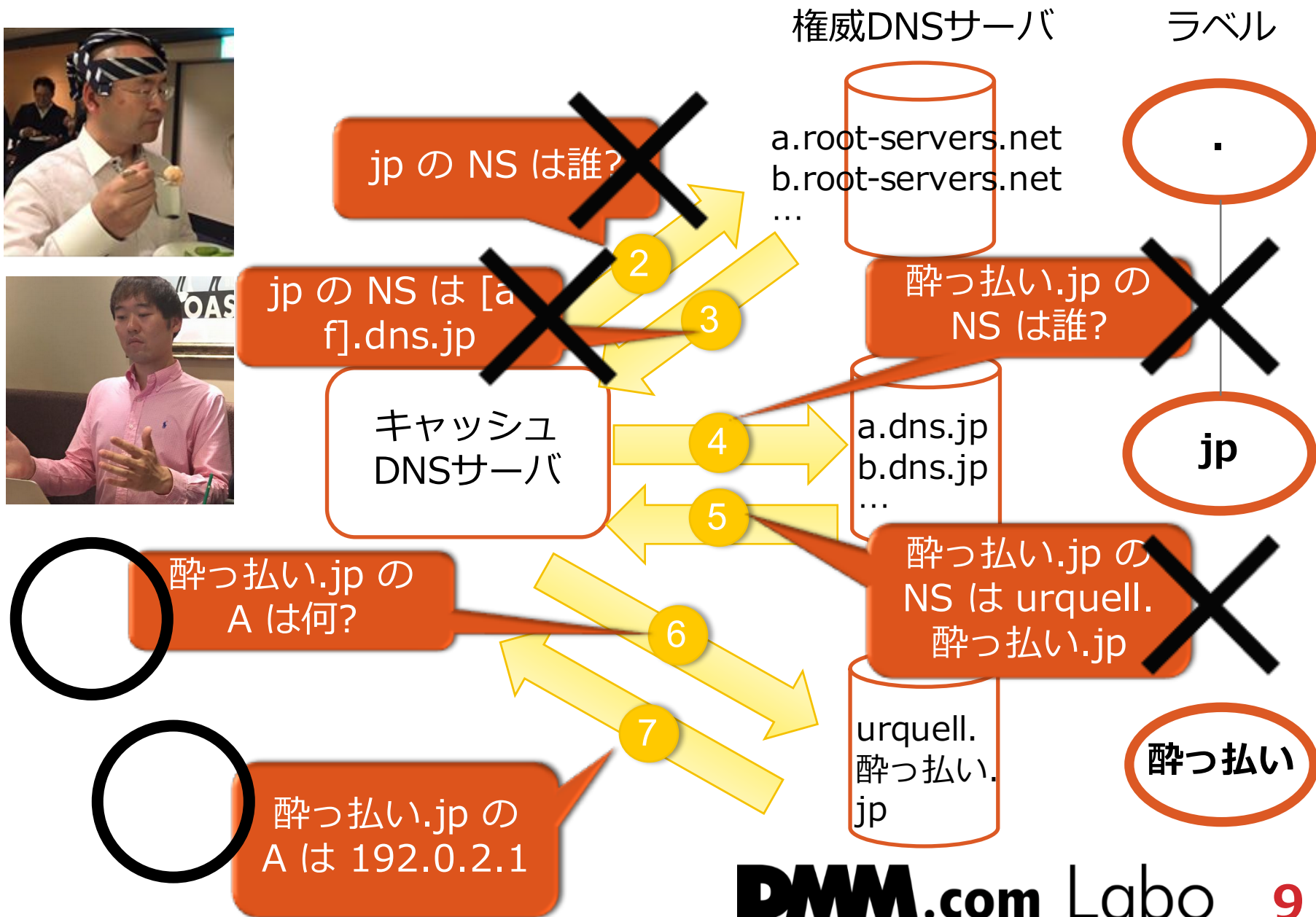
よくある回答



よくある回答



答え合わせ



答え合わせ



正解

No. ▼	Source	Destination	Protocol	Info
1	133.242.136.218.v6.sakura.ne.jp	i.root-servers.net	DNS	Standard query 0xd3ce NS <Root>
2	133.242.136.218.v6.sakura.ne.jp	i.root-servers.net	DNS	Standard query 0xab7c A XN--N8J1C913R6J1B.JP
3	i.root-servers.net	133.242.136.218.v6.sakura.ne.jp	DNS	Standard query response 0xab7c
4	i.root-servers.net	133.242.136.218.v6.sakura.ne.jp	DNS	Standard query response 0xd3ce NS c.root-servers.net NS
5	xavier.hanya-n.org	a.dns.JP	DNS	Standard query 0x73d5 A XN--N8J1C913R6J1B.JP
6	a.dns.JP	xavier.hanya-n.org	DNS	Standard query response 0x73d5
7	xavier.hanya-n.org	urquell.xn--n8j1c913r6j1b.jp	DNS	Standard query 0xf689 A XN--N8J1C913R6J1B.JP
8	urquell.xn--n8j1c913r6j1b.jp	xavier.hanya-n.org	DNS	Standard query response 0xf689 A 49.212.140.172 RRSIG

(注1) 133.242...v6.sakura.ne.jp, xavier.hanya-n.org

はキャッシュDNSサーバの IPv4, IPv6アドレス

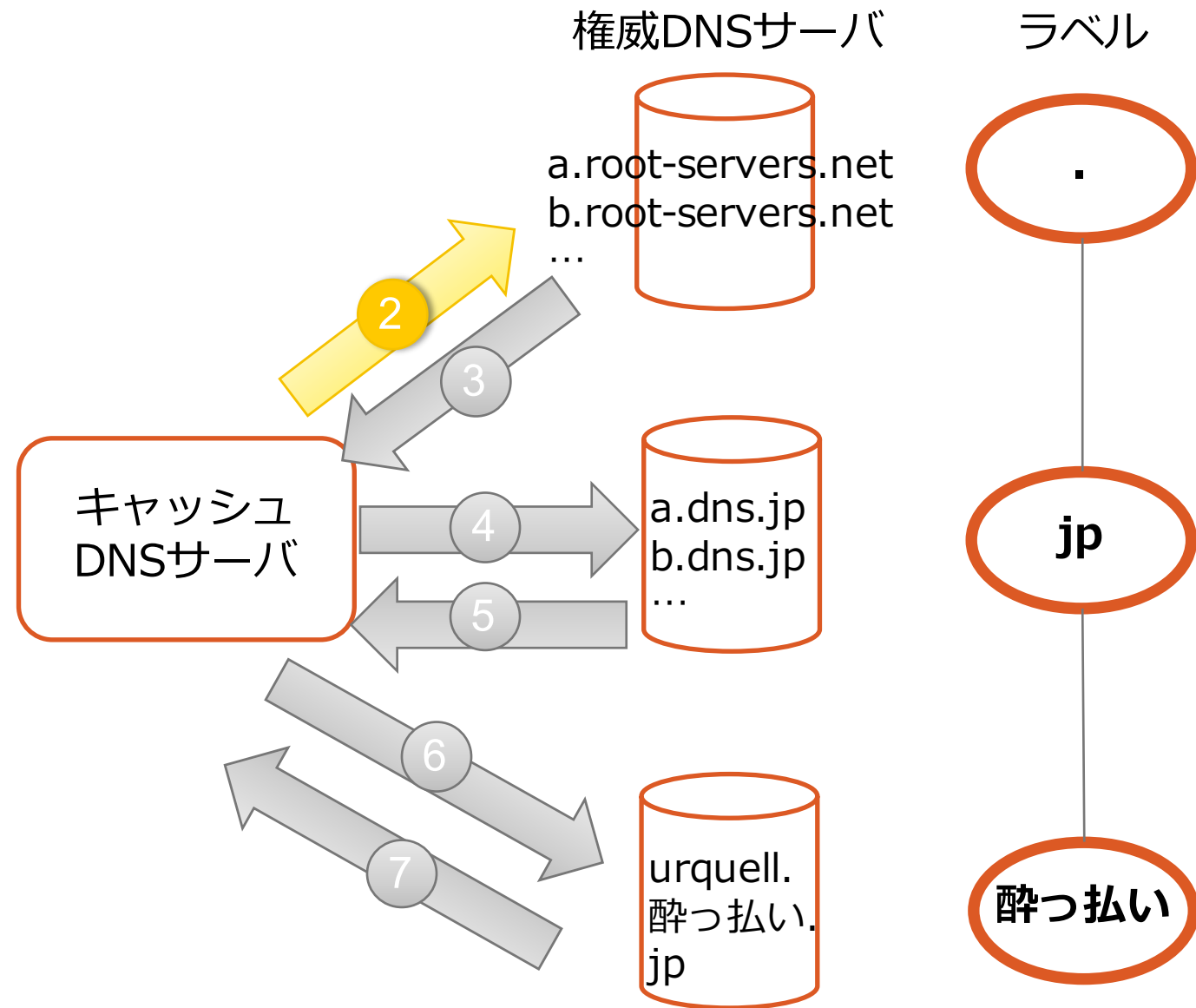
(注2) ハードコードされたroot DNSのhint情報から

真のroot DNSの一覧を得るためのクエリ

(プライミングと呼ばれ、BIND9やUnboundなどに実装)

(注3) BIND9 はルートサーバに何らかのクエリを送る際にも
プライミングと同様のクエリを送る模様

正解

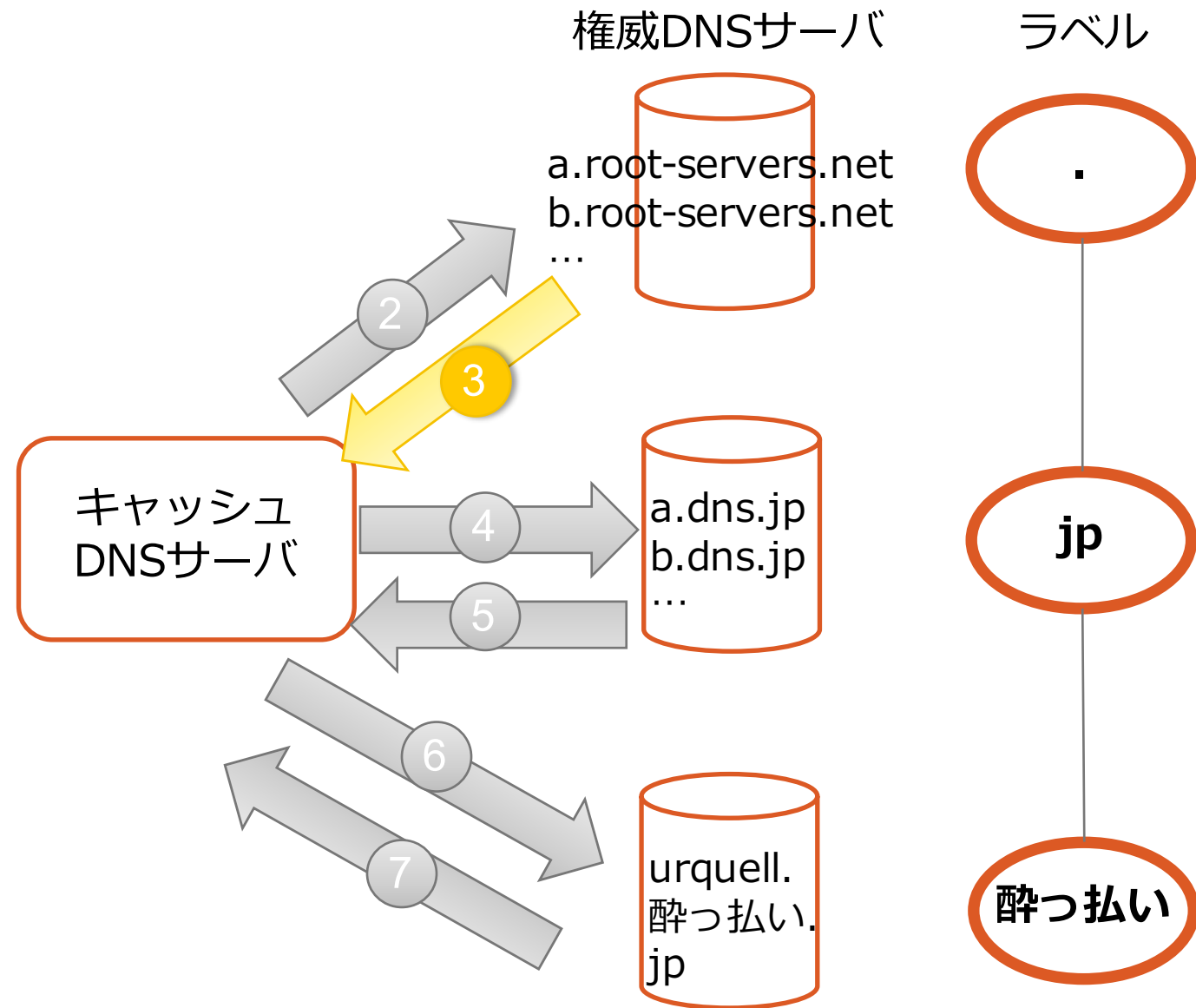


正解

```
Internet Protocol Version 6, Src: 133.242.136.218.v6.sakura.ne.jp  
(2401:2500:102:1201:133:242:136:218), Dst: i.root-servers.net (2001:7fe::53)  
User Datagram Protocol, Src Port: 18648 (18648), Dst Port: 53 (53)  
Domain Name System (query)  
  Transaction ID: 0xab7c  
  Flags: 0x0010 Standard query  
  ~~snip~~  
  Questions: 1  
  Answer RRs: 0  
  Authority RRs: 0  
  Additional RRs: 1  
  Queries  
    XN--N8J1C913R6J1B.JP: type A, class IN  
      Name: XN--N8J1C913R6J1B.JP  
      [Name Length: 20]  
      [Label Count: 2]  
      Type: A (Host Address) (1)  
      Class: IN (0x0001)  
  Additional records  
    <Root>: type OPT  
    ~~snip DO bit (DNSSEC ok) ~~
```

クライアントから問い合わせされた
内容を聞いている

正解



正解

Internet Protocol Version 6, Src: i.root-servers.net (2001:7fe::53), Dst:
133.242.136.218.v6.sakura.ne.jp (2401:2500:102:1201:133:242:136:218)
User Datagram Protocol, Src Port: 53 (53), Dst Port: 18648 (18648)
Domain Name System (response)

[Request In: 2]

[Time: 0.020326000 seconds]

Transaction ID: 0xab7c

Flags: 0x8010 Standard query response, No error

~~snip~~

Questions: 1

Answer RRs: 0

Authority RRs: 10

Additional RRs: 14

Queries

XN--N8J1C913R6J1B.JP: type A, class IN

Name: XN--N8J1C913R6J1B.JP

[Name Length: 20]

[Label Count: 2]

Type: A (Host Address) (1)

Class: IN (0x0001)

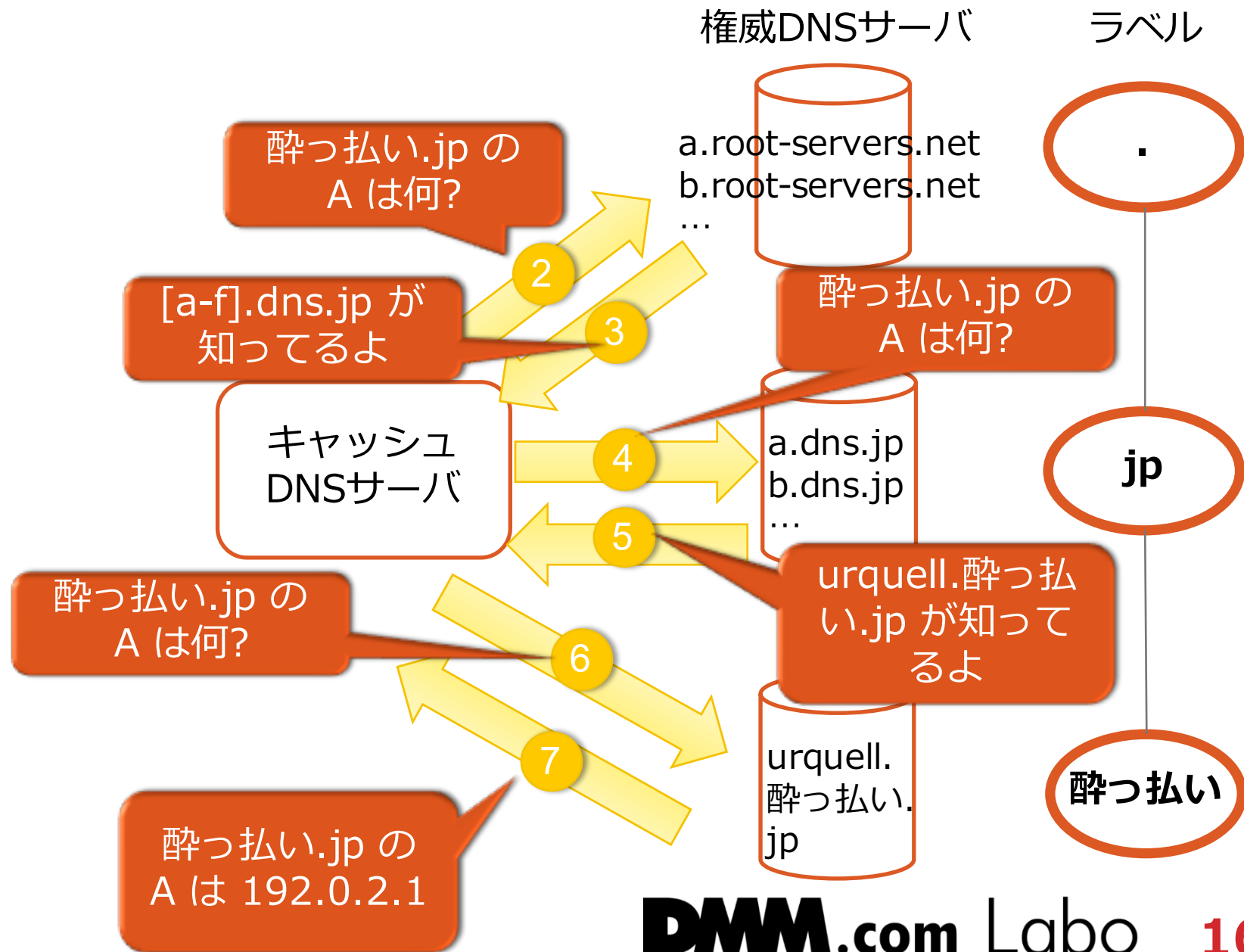
**Answer section ではなく、
Authority section に
NS を返してる!**

Authoritative nameservers

JP: type NS, class IN, ns b.dns.JP

~~snip 以下、jpの権威サーバとDS, RRSIGの列挙 ~~

正解



正解

- ✓ キャッシュDNSサーバは常にクライアントから問い合わせされた内容のクエリを送り続ける
- ✓ 権威DNSサーバは
 - 自分のドメイン名の階層に含まれる
 - 自分が直接対応するデータを持っていない
 - 自分のドメイン名の下位の階層の権威DNSサーバ（NSレコード）が設定されている（委任されている）場合は、Authority Section にそれらを入れて返す

だがしかし!

何か変わるか
もしんない！

QNAME Minimisation

Domain Name System Operations (dnsop) Working Group

Internet-Draft

Intended status: Experimental

Expires: February 2, 2016

|S. Bortzmeyer

AFNIC

August 1, 2015

DNS query name minimisation to improve privacy
draft-ietf-dnsop-qname-minimisation-05

Abstract

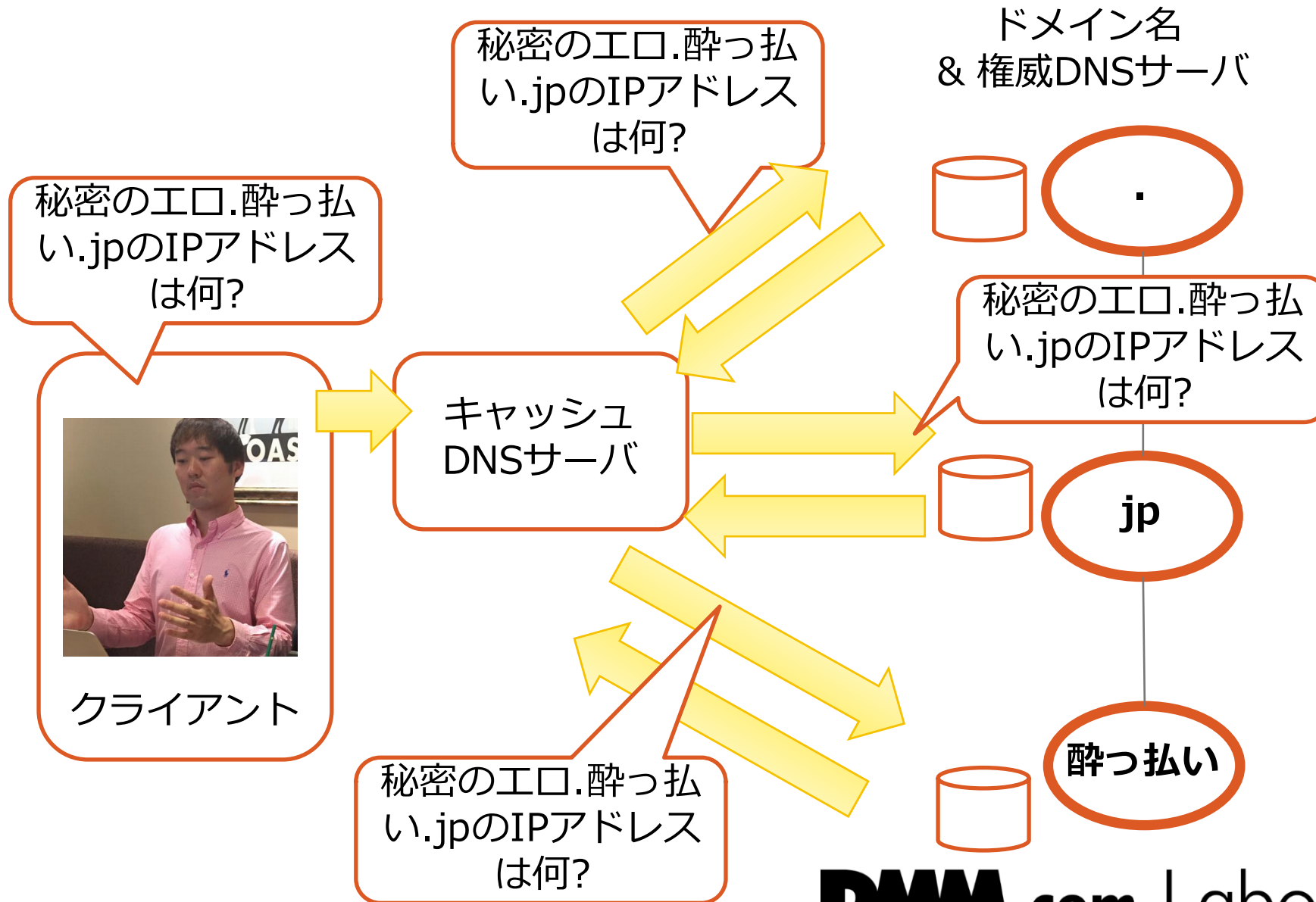
This document describes one of the techniques that could be used to improve DNS privacy (see [[I-D.ietf-dprive-problem-statement](#)]), a technique called "QNAME minimisation", where the DNS resolver no longer sends the full original QNAME to the upstream name server.

QNAME Minimisation

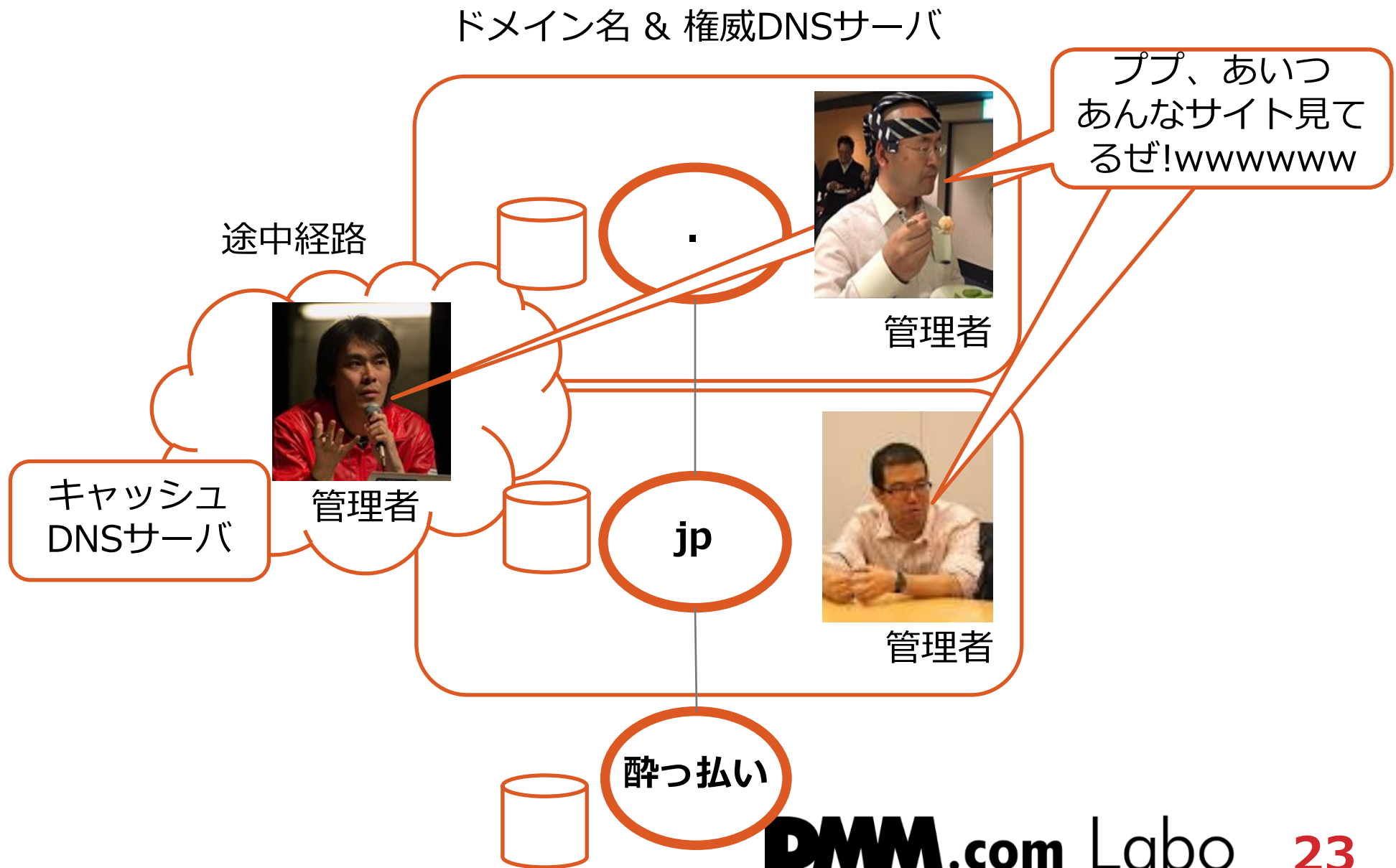
□ 従来の手法の問題点

- キャッシュDNSサーバ常にクライアントから要求された最終的に必要な DNS クエリを送り続ける
- 上位の権威DNSサーバ程、クライアントが何をしているのかわかっちゃう!
- 権威DNSサーバへの通信経路の人も覗き見できちゃう!

QNAME Minimisation



QNAME Minimisation

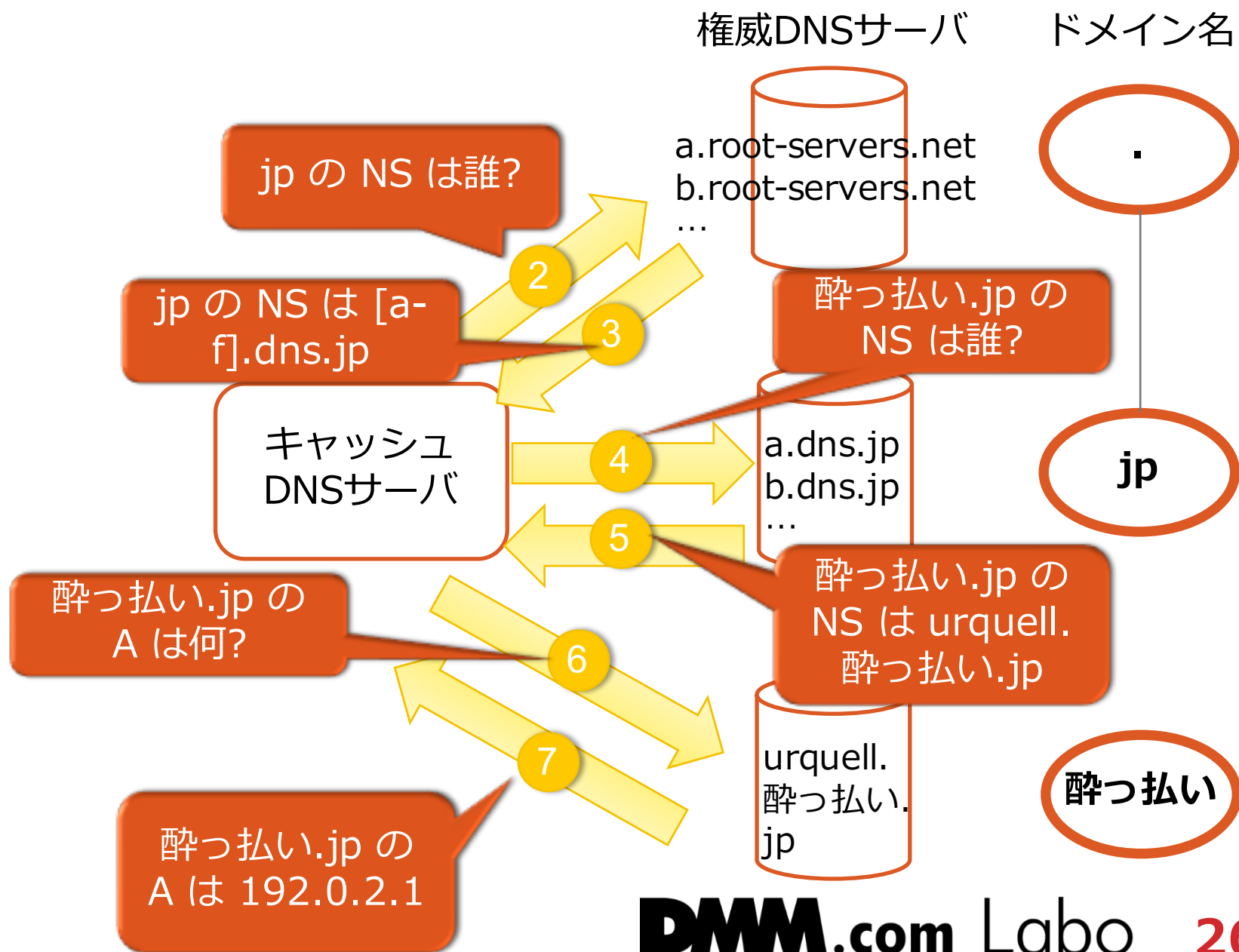


よくない！

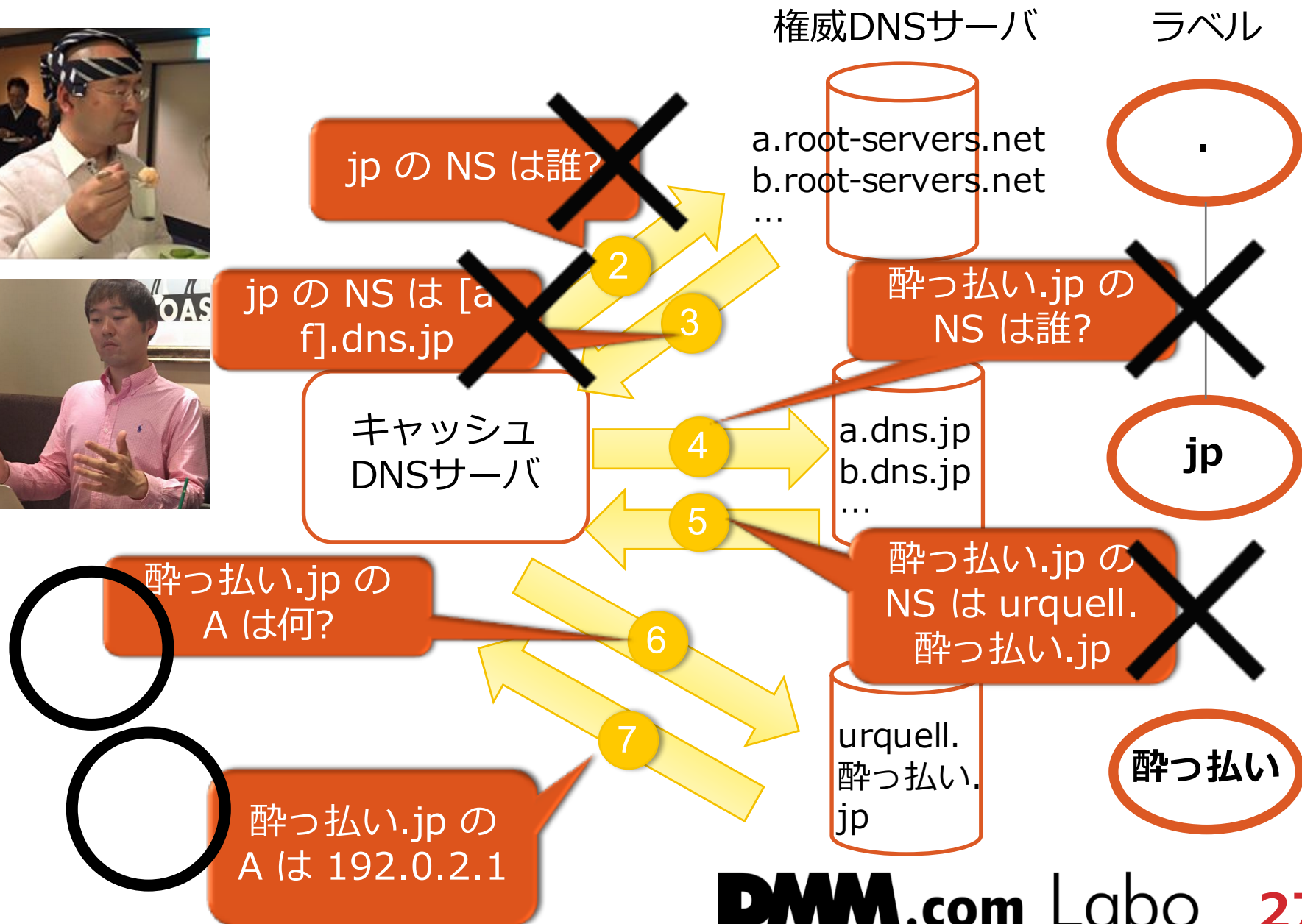
QNAME Minimisation の提案内容

- 権威DNSサーバには、それから1階層下の NS を聞く様にする

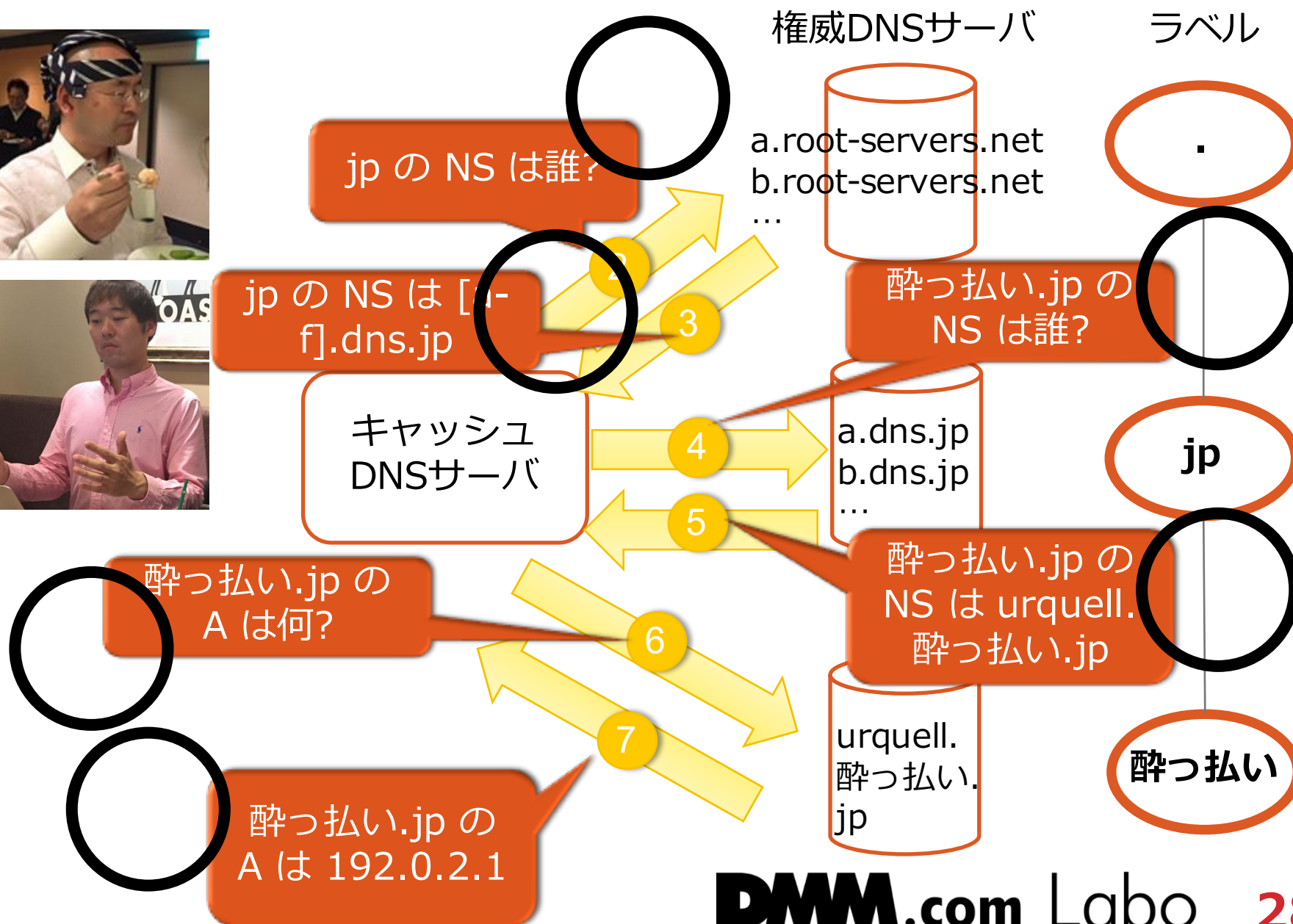
これだ!



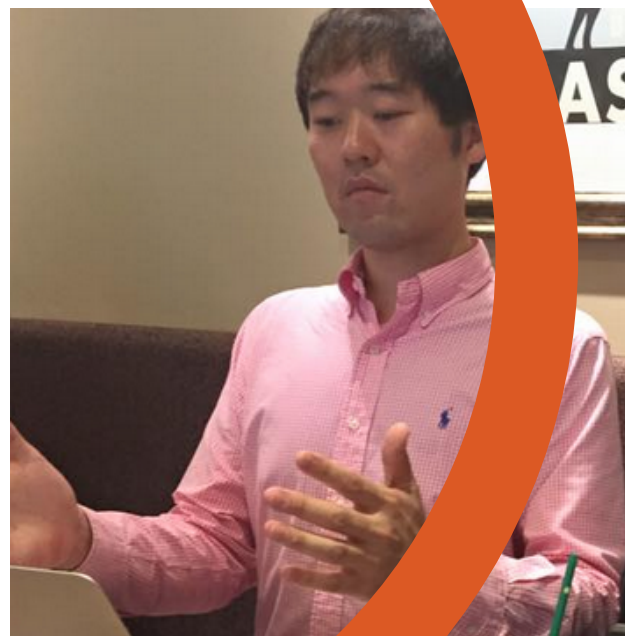
これが



こうなる



よかったね!



QNAME Minimisation のいいところ

□ 既存の仕組みと互換性がある

- 仮にすぐ下の階層に NS がなくて、2階層より下のドメイン名が定義されてても NO DATA が返ってくるだけなので、更に1個したのNSを聞くというのができる
- というか、最終的に知りたい名前を聞くというやり方自体、伝統的にそうしているがそういう決まりではないらしい

Under current practice, when a resolver receives the query "What is the AAAA record for www.example.com?", it sends to the root (assuming a cold resolver, whose cache is empty) the very same question. Sending the full QNAME to the authoritative name server is a tradition, not a protocol requirement. This tradition

QNAME Minimisation のいいところ

□ Negative Cache 効率の向上

(例) A.example、B.example、C.exampleを
順に問い合わせた場合

❖ 従来の方法:

- ルートサーバへの問い合わせが毎回発生

❖ QNAME minimisation:

- A.exampleの時にだけ問い合わせが発生
 - ✓ exampleのNSを問い合わせるため、NS（委任）が存在しないことがわかる
 - ✓ B.example、C.exampleに対する問い合わせが発生しない

まとめ +1

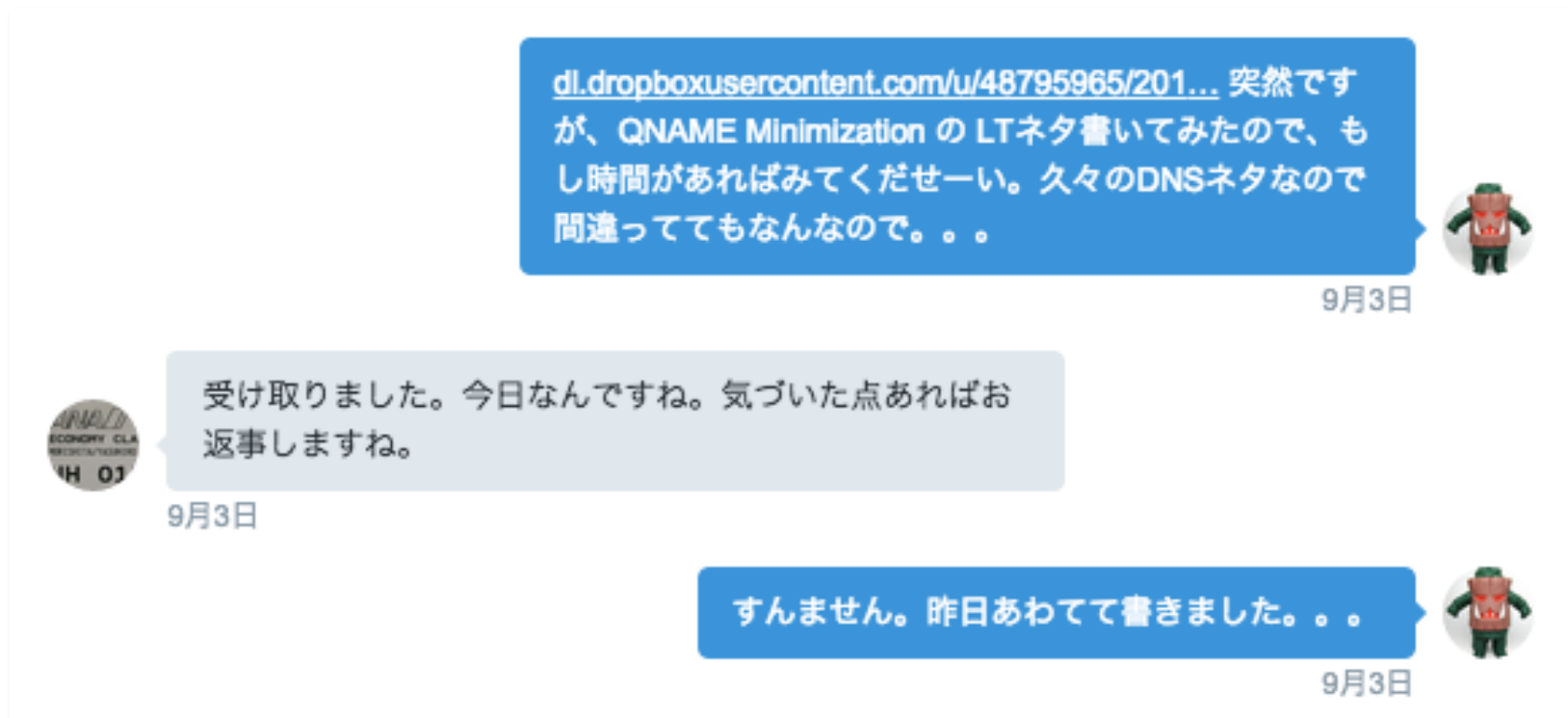
- 今の実装では、キャッシュDNSサーバは最終的に知りたいクエリを root から最終的にデータを持っている権威DNSサーバまで繰り返し聞き続ける
- QNAME Minimisation では root から1階層ずつ NS を検索する様なアプローチをとり、プライバシー対策になると同時に、クエリ/応答のパケット数の削減も実現できる

+1

- 現在の状況:
IETF dnsop WGで合意済、
Experimental RFCとなる予定

Special Thanks to: 重複の Orange の人

- 当日朝に内容チェックお願いしたにも関わらずありがとうございます。



Thank you!