DNS Summer Day 2019

Encrypted DNS:
ISPから見たDoT/DoHの話

株式会社コミュニティネットワークセンター

ニコライ ボヤジエフ

2019年6月

Agenda

1. 自己紹介、会社紹介
2. 「Encrypted DNS」って何のこと?
3. DoHは何が違う？なぜ気にする必要あるの？
4. ISPから見た「集中型DoH」の課題
5. まとめ

自己紹介

名前：　ニコライ ボヤジエフ

出身：　ブルガリア 《България》 IDN ccTLD: **бг** (xn--90ae)

在日ブルガリア人：
<300人

所属：　株式会社コミュニティネットワークセンター (CNCI)
技術本部　サーバグループ

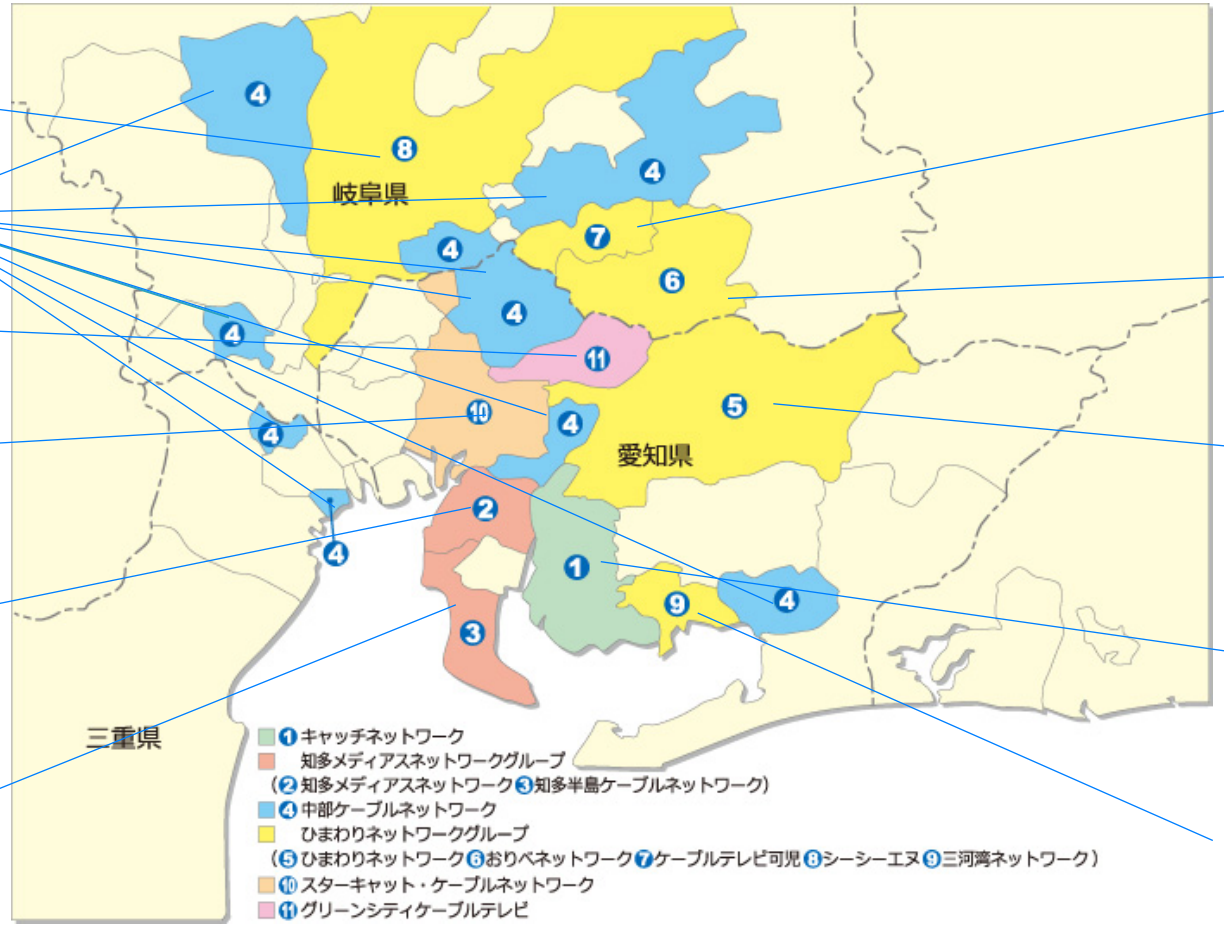
担当：　メール、DNS、ストレージ、ネットワーク、仮想化 etc. etc.
サーバインフラの企画・構築・運用やってます
複数の帽子をかぶってます

会社紹介

- **株式会社コミュニティネットワークセンター（CNCI）**
- **愛知/岐阜/三重で活動するケーブルテレビMSO**
  MSO：Multiple Systems Operator (統括運営会社)
- **グループ　ケーブルテレビ局11局**

サービスエリア

CCN
CCNet
Green City
star cat
medias
TAC TRY AND CREATE CCNC

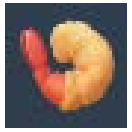


CTK
Oribe
ひまわり
KATCH
三河湾ネットワーク

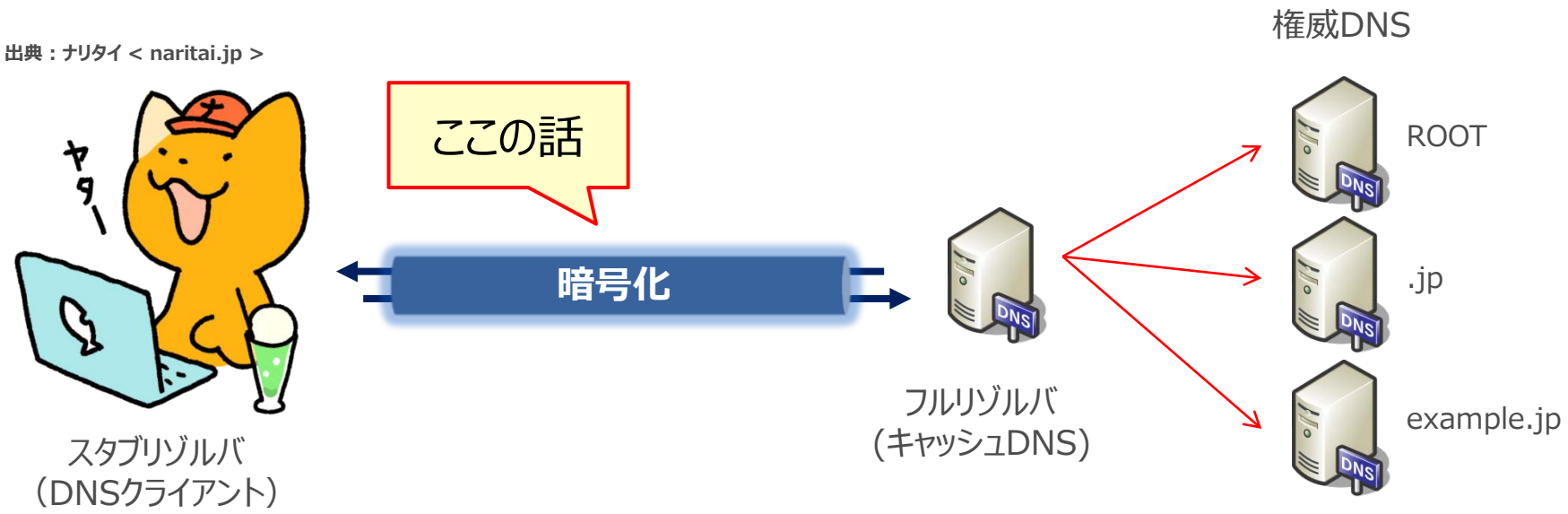
約150万世帯にテレビ || ネット || 電話サービスをご提供中

CNCI/AS9354

peering.cnci.nagoya

:ebifurya: 

「Encrypted DNS」って何のこと？



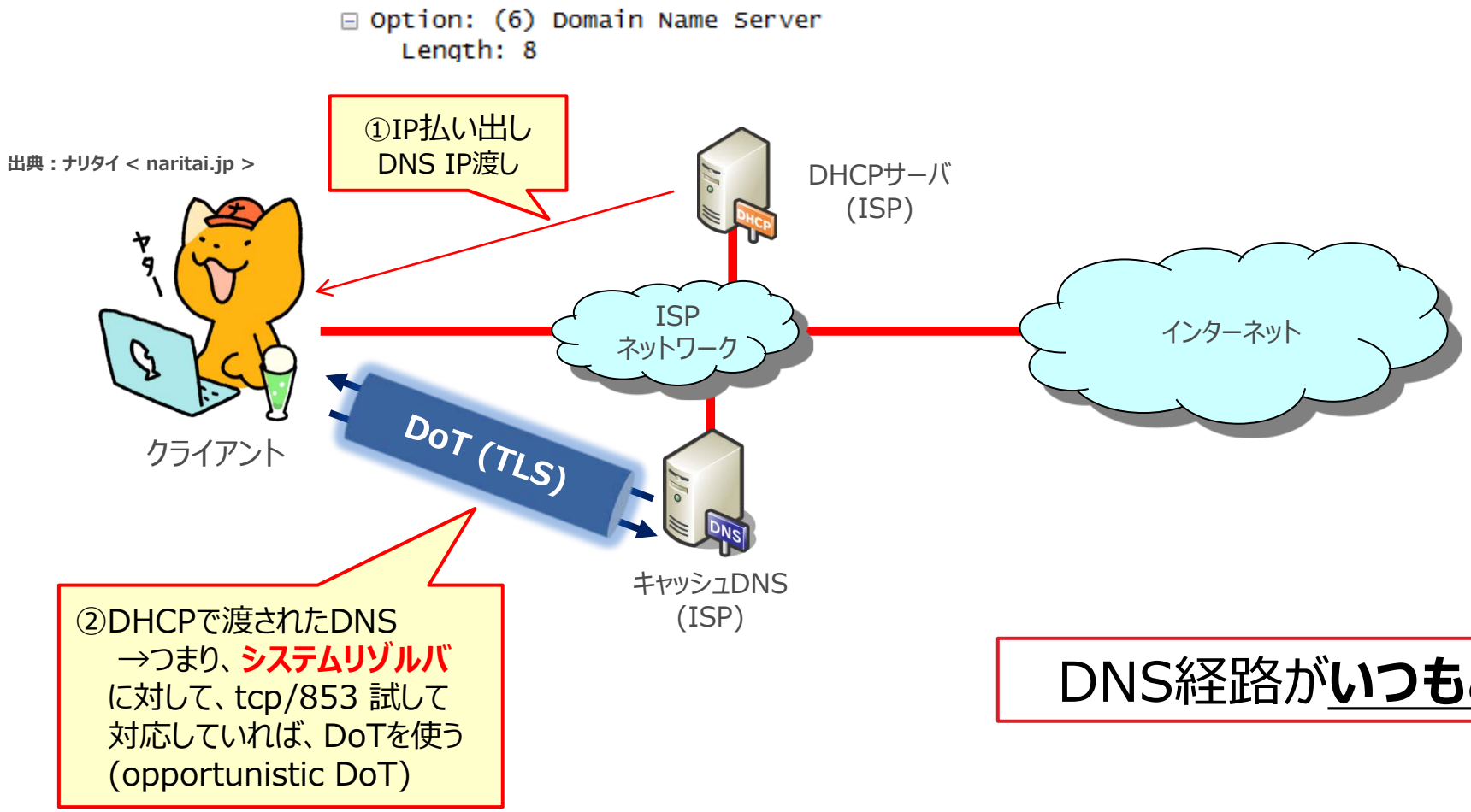
- スタブリゾルバとフルリゾルバ間の**DNS経路を暗号化する**仕組み
- **DoT**: DNS-over-TLS （RFC7858, May 2016）
- **DoH**: DNS-over-HTTPS （RFC8484, Oct 2018）

※その他の実装：DNScrypt (IETF外)、DNS-over-QUIC (draft)、DNS-over-DTLS (RFC8094)

DNS-over-TLS (DoT)

- RFC7858 (May 2016)
- IANA port **853/tcp** (※853/udp は DTLS/RFC8094)
- TLSセッションの中に**通常DNSメッセージ** (RFC1035)
- **opportunistic** (日和見) モードの実装が多い
  - 853/tcp 試して、NGだったら通常DNSへダウングレード (**STARTTLS的な動きはない**)
- strict (証明書検証) モードも定義されている (RFC8310参照)
  - サーバ名必要、手動設定、PKIX と DANE をサポート
- 基本的にシステム設定のリゾルバに接続する
  - **DNS経路が変わらないので分かりやすい**

DoT のイメージ (例)

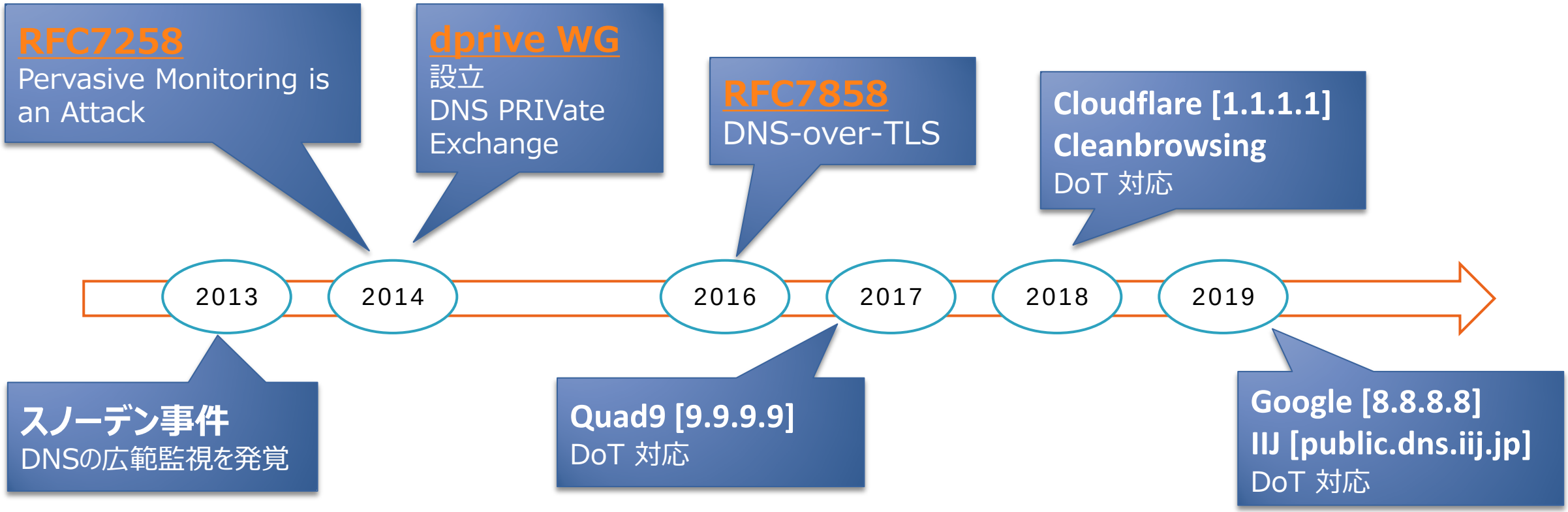


DNS経路が**いつもと同じ**

DoT を cli で試す

```
$ kdig -d @103.2.57.5 +tls-ca +tls-host=public.dns.iij.jp _dmarc.cnci.nagoya txt
;; DEBUG: Querying for owner(_dmarc.cnci.nagoya.), class(1), type(16), server(103.2.57.5), port(853), protocol(TCP)
;; DEBUG: TLS, imported 151 system certificates
;; DEBUG: TLS, received certificate hierarchy:
;; DEBUG:  #1, C=JP,ST=Tokyo,L=Chiyoda-ku,O=Internet Initiative Japan Inc.,CN=*.dns.iij.jp
;; DEBUG:      SHA-256 PIN: IG4Bkj0wTXzg0BDvaES1fCqgPya4hpA9AxaRWI90lss=
;; DEBUG:  #2, C=BE,O=GlobalSign nv-sa,CN=GlobalSign Organization Validation CA - SHA256 - G2
;; DEBUG:      SHA-256 PIN: IQBnNBEiFuhj+8x6X8XLgh01V9Ic5/V3IRQLNFFc7v4=
;; DEBUG: TLS, skipping certificate PIN check
;; DEBUG: TLS, The certificate is trusted.
;; TLS session (TLS1.2)-(ECDHE-ECDSA-SECP256R1)-(AES-128-GCM)
;; ->>HEADER<<- opcode: QUERY; status: NOERROR; id: 39153
;; Flags: qr rd ra; QUERY: 1; ANSWER: 1; AUTHORITY: 0; ADDITIONAL: 1

;; EDNS PSEUDOSECTION:
;; Version: 0; flags: ; UDP size: 1220 B; ext-rcode: NOERROR

;; QUESTION SECTION:
;; _dmarc.cnci.nagoya.          IN      TXT

;; ANSWER SECTION:
_dmarc.cnci.nagoya.     15      IN      TXT     "v=DMARC1; p=none; adkim=s; aspf=s"

;; Received 93 B
;; Time 2019-06-25 21:34:48 JST
;; From 103.2.57.5@853(TCP) in 12.5 ms
```

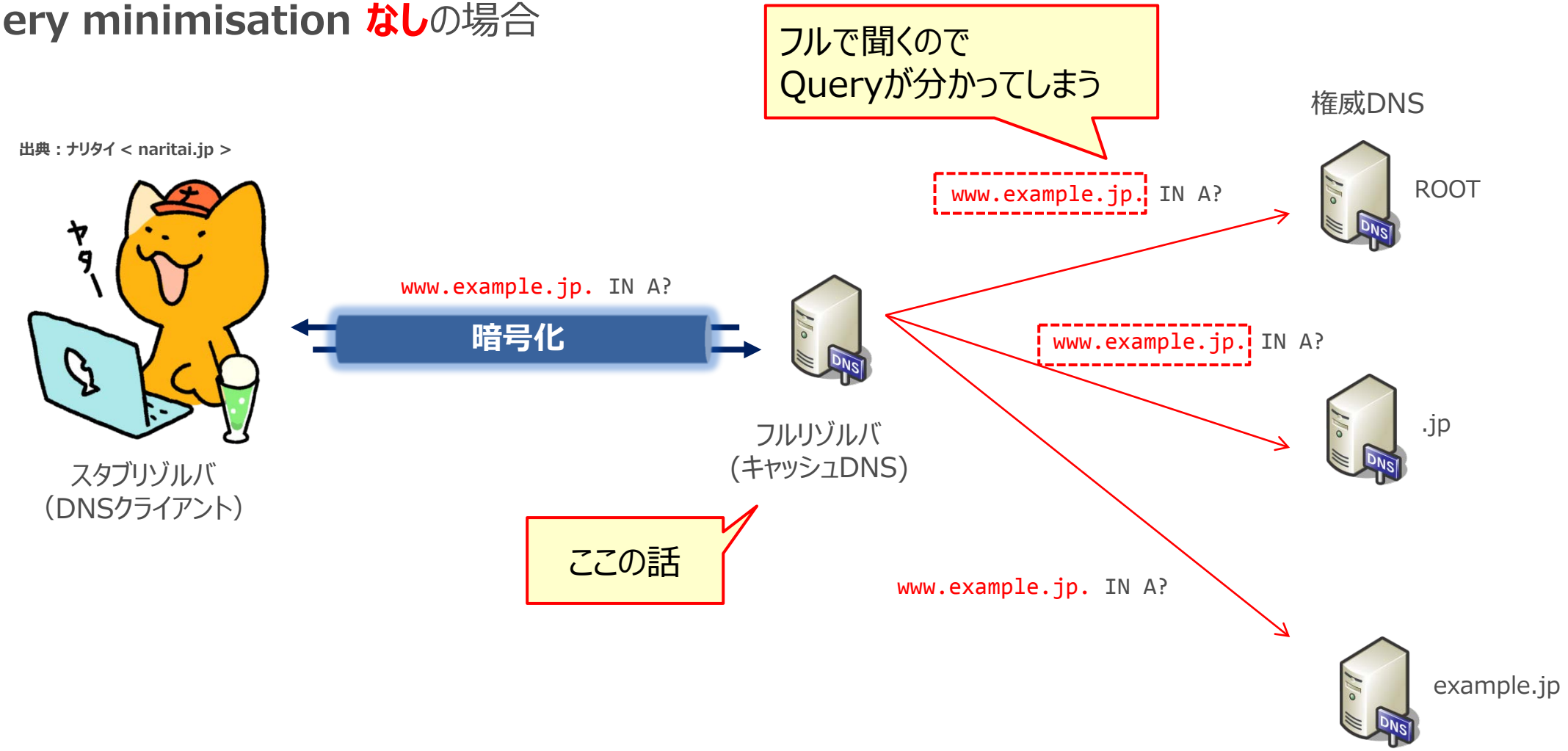
DNS-over-TLS (DoT) 標準化の話



- **DNS Privacy Considerations** (RFC7626) → dprive WG
- **Query minimisation** (RFC7816) → DNSOP WG
- **EDNS(0) padding option** (RFC7830, RFC8467) → dprive WG

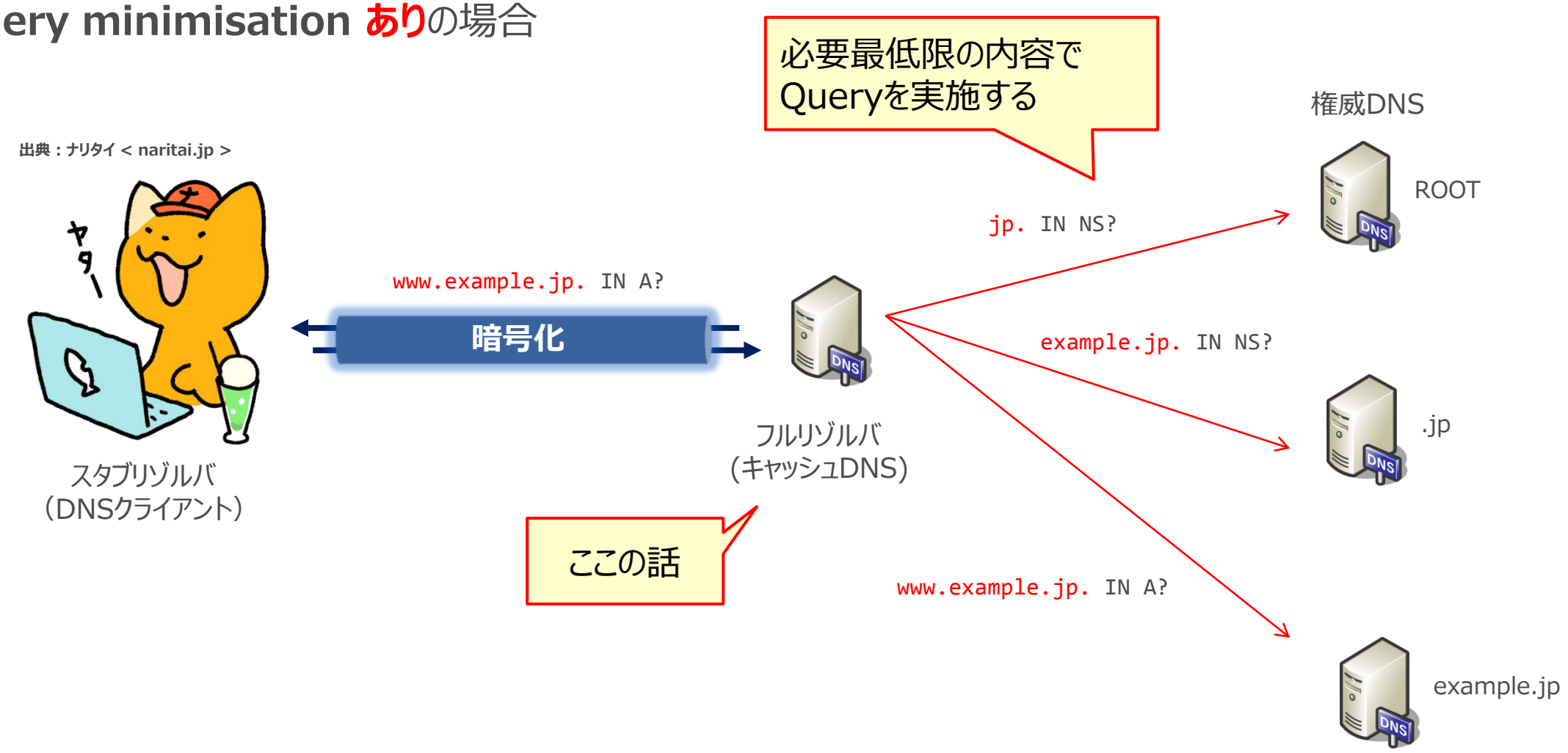
(補足) Query minimisation (RFC7816)

- Query minimisation **なし**の場合



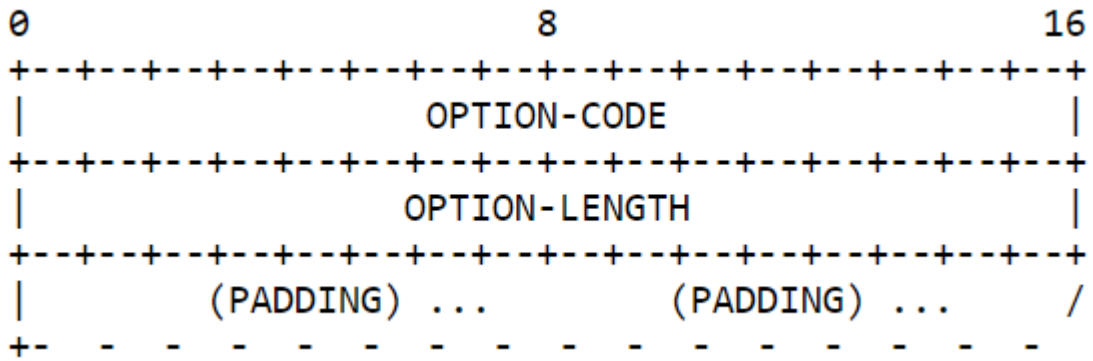
(補足) Query minimisation (RFC7816)

- Query minimisation **あり**の場合



(補足) EDNS(0) padding option

- EDNS Option Code 12 (000c)



- DNSクエリが暗号化されていても、**パケットサイズからパターン分析、ユーザ推測可能**
- PADDINGにダミーデータ (0) を入れることによって、推測防止

https://www.afnic.fr/medias/documents/JCSA/2017/5.JCSA17-DNS-over-TLS-experiments.pdf

DoT実装状況：クライアント (1)

Mode		Stub						Caching forwarder/proxy			
Software		ldns (drill)	digit	getdns (Stubby)	BIND (dig)	Go DNS	Knot (kdig)	Unbound	BIND	Knot Res	dndist
General	Send ECS with SOURCE PREFIX-LENGTH value of 0			✓	✓		✓				
TCP/TLS Features	TCP fast open[(b)]		✓	✓				✓			✓
	Connection reuse (Q/R, Q/R, Q/R)		✓	✓	✓	✓	✓		✓	✓	✓
	Pipelining of queries(Q,Q,Q,R,R,R)	n/a	✓	✓	✓	✓	✓		✓	✓	✓
	Process OOOR (Q1,Q2,R2,R1)	n/a	✓	✓	✓				✓	✓	✓
	EDNS0 Keepalive[(c)]			✓	✓				(f)		
TLS Features	TLS encryption (Port 853)		✓	✓		✓	✓	✓		✓	
	TLS authentication			✓			✓	✓		✓	
	EDNS0 Padding		✓	✓	✓		✓		✓		
	TLS DNSSEC Chain Extension[(h)]										

https://dnsprivacy.org/wiki/display/DP/DNS+Privacy+Implementation+Status

DoT実装状況：クライアント (2)

Android	- Android 9 “Pie” 以降 – “opportunistic” DoT ネイティブ ※ - Quad9 Connect アプリ (by Quad9) - Tenta VPN ブラウザ
iOS	- 1.1.1.1 アプリ (by Cloudflare) - Stubby iOS アプリ (※開発中)
ルータ	- OpenWRT - AsusWRT-Merlin - Turris
その他	- systemd (Linux) – opportunistic DoT ネイティブ

https://dnsprivacy.org/wiki/display/DP/DNS+Privacy+Clients#DNSPrivacyClients-Operatingsystems

※Android実装詳細
https://drive.google.com/open?id=0B7vYCtlP8e6KQ3RIYm40ZElzVHZJY0duYkZ4VUs4aFFGVzNF

DoT実装状況：サーバ (1)

Mode		Load Balancer	Recursive					Auth		
Software		dnsdist	Unbound	BIND	Knot Res	CoreDNS[e]	Tenta[e]	NSD	BIND	Knot Auth
General	QNAME minimisation	n/a	✓	✓	✓					
TCP/TLS Features	TCP fast open[b]	✓	✓	✓	✓				✓	✓
	Process Pipelined queries	✓	✓	✓	✓			✓	✓	✓
	Provide OOOR	(g)	✓	✓	✓			n/a	n/a	n/a
	EDNS0 Keepalive[c]		✓	✓	✓				✓	
TLS Features	TLS encryption (Port 853)	✓	✓	(d)	✓	✓	✓			
	Provide TLS auth credentials	✓	✓	(d)	✓	✓	✓			
	EDNS0 Padding (basic)			✓	✓				✓	
	TLS DNSSEC Chain Extension[h]									

https://dnsprivacy.org/wiki/display/DP/DNS+Privacy+Implementation+Status

↓ここも参照
https://doh.defaultroutes.de/implementations.html

DoH実装状況：サーバ (2) Public DNS

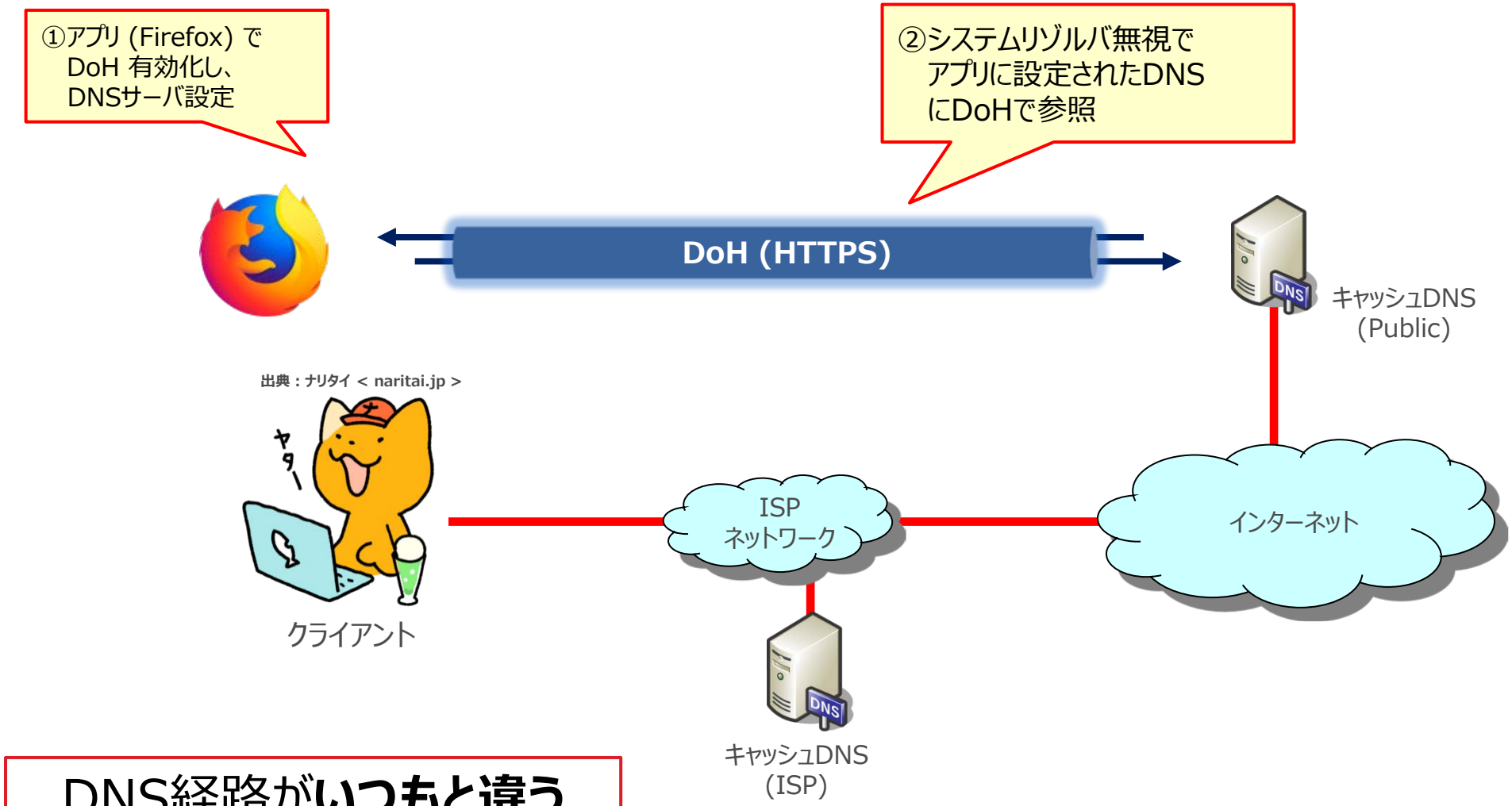
プロバイダ	Cloudflare	Google	Quad9 (IBM/PCH/GCA)	Cleanbrowsing	IIJ
IP/FQDN	1.1.1.1	8.8.8.8	9.9.9.9	185.228.168.168 185.228.169.168	public.dns.iij.jp
所在地	米国	米国	米国	米国	日本
平文DNS	○	○	○	○	×
DoT/DoH	DoT DoH	DoT DoH ~~(実験)~~※	DoT DoH	DoT DoH	DoT (実験) DoH (実験)
フィルタリング	×	×	○	○	○ (※ICSAのみ)
DNSSEC	○	○	○	○	○
Qname minimisation	○	×	×	×	○
EDNS0 Client Subnet (ECS)	×	○	×	×	×

※ 2019/6/26 正式発表
https://security.googleblog.com/2019/06/google-public-dns-over-https-doh.html

DNS-over-HTTPS (DoH)

- RFC8484 (Oct 2018)
- **HTTPS プロトコル上**に DNS を載せた仕組み (**平文へフォールバックなし**)
- Wire-Format : application/dns-message (RFC1035) (or JSON or…)
- **GET** or **POST**
  - DNS応答関係なしに、HTTPS接続正常であれば 200 OK が返る
- **URIテンプレート**設定必須 (**システムリゾルバ使わず、個別に設定が必要**)
  - 例：https://public.dns.iij.jp/dns-query
  - URIのホスト名を初回のみ名前解決するDNSリゾルバ設定が必要 (bootstrap IP)
- HTTP/2、(HTTP/3) の高速化工夫そのまま使える
  - 多重化、再送制御、HPACK、server-push (!)、0-RTT、QUIC

DoH のイメージ (例)



DNS経路が**いつもと違う**

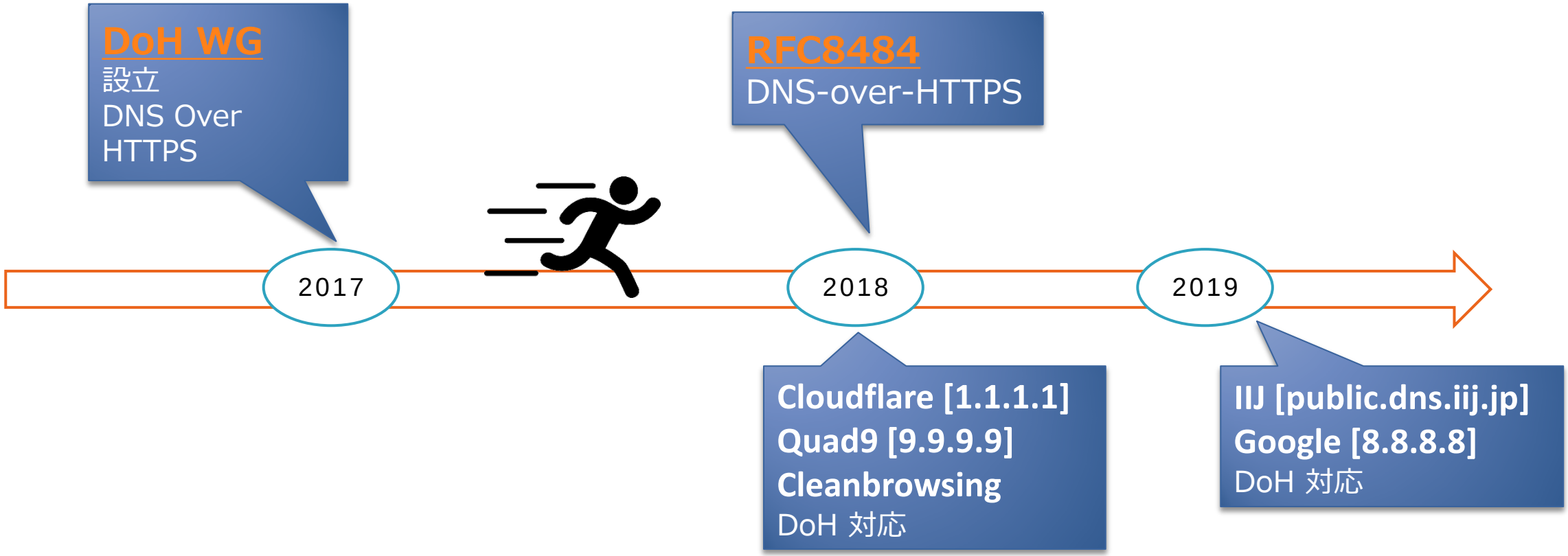
DoH を cli で試す – GET

```
$ ./dnsbase64.py _dmarc.cnci.nagoya TXT
H0cBAAABAAAAAAAABl9kbWFyYwRjbmNpBm5hZ295YQAAEAAB

$ curl -H 'accept: application/dns-message' -v 'https://public.dns.iij.jp/dns-
query?dns=H0cBAAABAAAAAAAABl9kbWFyYwRjbmNpBm5hZ295YQAAEAAB' | ./dnsbase64.py
* Connected to public.dns.iij.jp (2001:300::5) port 443 (#0)
> GET /dns-query?dns=H0cBAAABAAAAAAAABl9kbWFyYwRjbmNpBm5hZ295YQAAEAAB HTTP/1.1
> User-Agent: curl/7.29.0
> Host: public.dns.iij.jp
> accept: application/dns-message
>
< HTTP/1.1 200 OK
< Server: nginx
< Date: Thu, 27 Jun 2019 07:19:10 GMT
< Content-Type: application/dns-message
< Content-Length: 82
< Connection: close
< Cache-Control: 15
< Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
<

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 8007
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
;; QUESTION SECTION:
;_dmarc.cnci.nagoya.            IN      TXT
;; ANSWER SECTION:
_dmarc.cnci.nagoya.     15      IN      TXT     "v=DMARC1; p=none; adkim=s; aspf=s"
```

DoH を cli で試す – POST

```
$ ./dnsbytes.py _dmarc.cnci.nagoya TXT | curl -v -H 'Content-Type:application/dns-message'
'https://public.dns.iij.jp/dns-query' -X POST --data-binary @- | ./dnsbytes.py
* Connected to public.dns.iij.jp (2001:300::6) port 443 (#0)
> POST /dns-query HTTP/1.1
> User-Agent: curl/7.29.0
> Host: public.dns.iij.jp
> Accept: */*
> Content-Type:application/dns-message
> Content-Length: 36
>
* upload completely sent off: 36 out of 36 bytes
< HTTP/1.1 200 OK
< Server: nginx
< Date: Thu, 27 Jun 2019 07:28:48 GMT
< Content-Type: application/dns-message
< Content-Length: 82
< Connection: close
< Cache-Control: 2
< Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
<
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 29096
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
;; QUESTION SECTION:
;_dmarc.cnci.nagoya.            IN      TXT
;; ANSWER SECTION:
_dmarc.cnci.nagoya.     2       IN      TXT     "v=DMARC1; p=none; adkim=s; aspf=s"
```

DNS-over-HTTPS (DoH) 標準化の話



- 「**Web系人間**」(ブラウザ屋さん、CDN屋さん) により**超高速標準化**
- **Representing DNS Messages in JSON** (RFC8427) → WGなし
- **resolverless-dns@ietf.org** → server-push などでDNS情報を得る

DoH実装状況：クライアント (1)

Name	Version	Comments
Firefox	62	temporary docs
Bromite	67.0.3396.88	How to enable DoH
curl	7.62.0	See DOH-implementation
OkHttp	3.11	See Providers
curl-doh	n/a	basic stand-alone DoH client that uses curl
Chrome	66	https://bugs.chromium.org/p/chromium/issues/detail?id=799753

https://github.com/curl/curl/wiki/DNS-over-HTTPS#supported-in-browsers-and-clients

DoH実装状況：クライアント (2)

Android	- Intra アプリ (by Google) ※DoHサーバ設定可能
iOS	- 1.1.1.1 アプリ (by Cloudflare)
その他	- cloudflared プロキシ (by Cloudflare) - dnscrypt-proxy

https://dnsprivacy.org/wiki/display/DP/DNS+Privacy+Clients#DNSPrivacyClients-DOH

DoH実装状況：サーバ (1)

Mode	Load Balancer	Recursive		
Software	dnsdist	Unbound	BIND	Knot Res
DoH support	WIP			Experimental Implementation released in 4.0.0

https://dnsprivacy.org/wiki/display/DP/DNS+Privacy+Implementation+Status

↓ここも参照
https://doh.defaultroutes.de/implementations.html

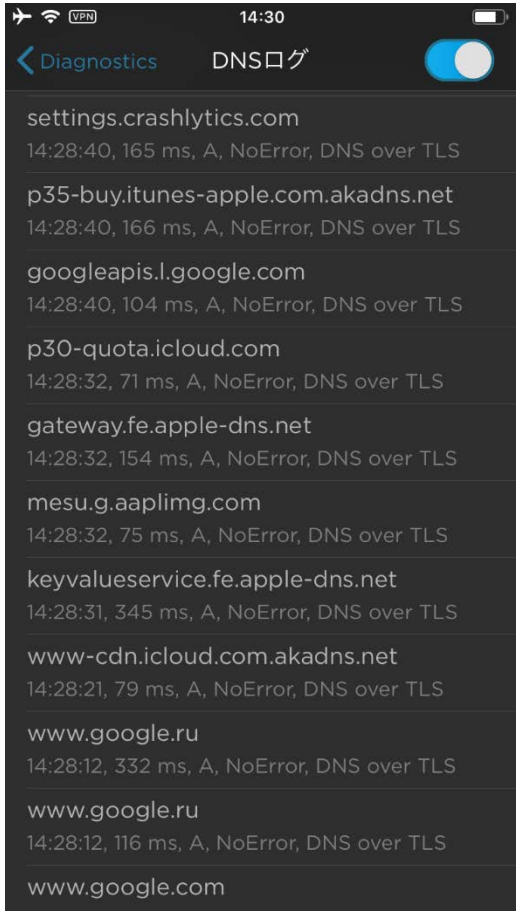
DoH実装状況：サーバ (2) Public DNS (再)

プロバイダ	Cloudflare	Google	Quad9 (IBM/PCH/GCA)	Cleanbrowsing	IIJ
IP/FQDN	1.1.1.1	8.8.8.8	9.9.9.9	185.228.168.168 185.228.169.168	public.dns.iij.jp
所在地	米国	米国	米国	米国	日本
平文DNS	○	○	○	○	×
DoT/DoH	DoT DoH	DoT DoH ~~(実験)~~※	DoT DoH	DoT DoH	DoT (実験) DoH (実験)
フィルタリング	×	×	○	○	○ (※ICSAのみ)
DNSSEC	○	○	○	○	○
Qname minimisation	○	×	×	×	○
EDNS0 Client Subnet (ECS)	×	○	×	×	×

※ 2019/6/26 正式発表
https://security.googleblog.com/2019/06/google-public-dns-over-https-doh.html

DoT/DoH 使ってみてどうだった

- Case 1: 海外出張中に、iPhone に 1.1.1.1 アプリを入れてみた



DoT/DoH 使ってみてどうだった

- Case 1: 海外出張中に、iPhone に 1.1.1.1 アプリを入れてみた
  - VPNアイコンに違和感 

  - アプリのデザインがいい
  - 普通に使えた (→**DoT/DoH両方とも遅延が気になることなかった**)
  - Captive Portal 検知して、待ってくれる
  - **ハンガリーのホテルWi-Fiで使えなかった** (1.1.1.1 ブラックリスト?)

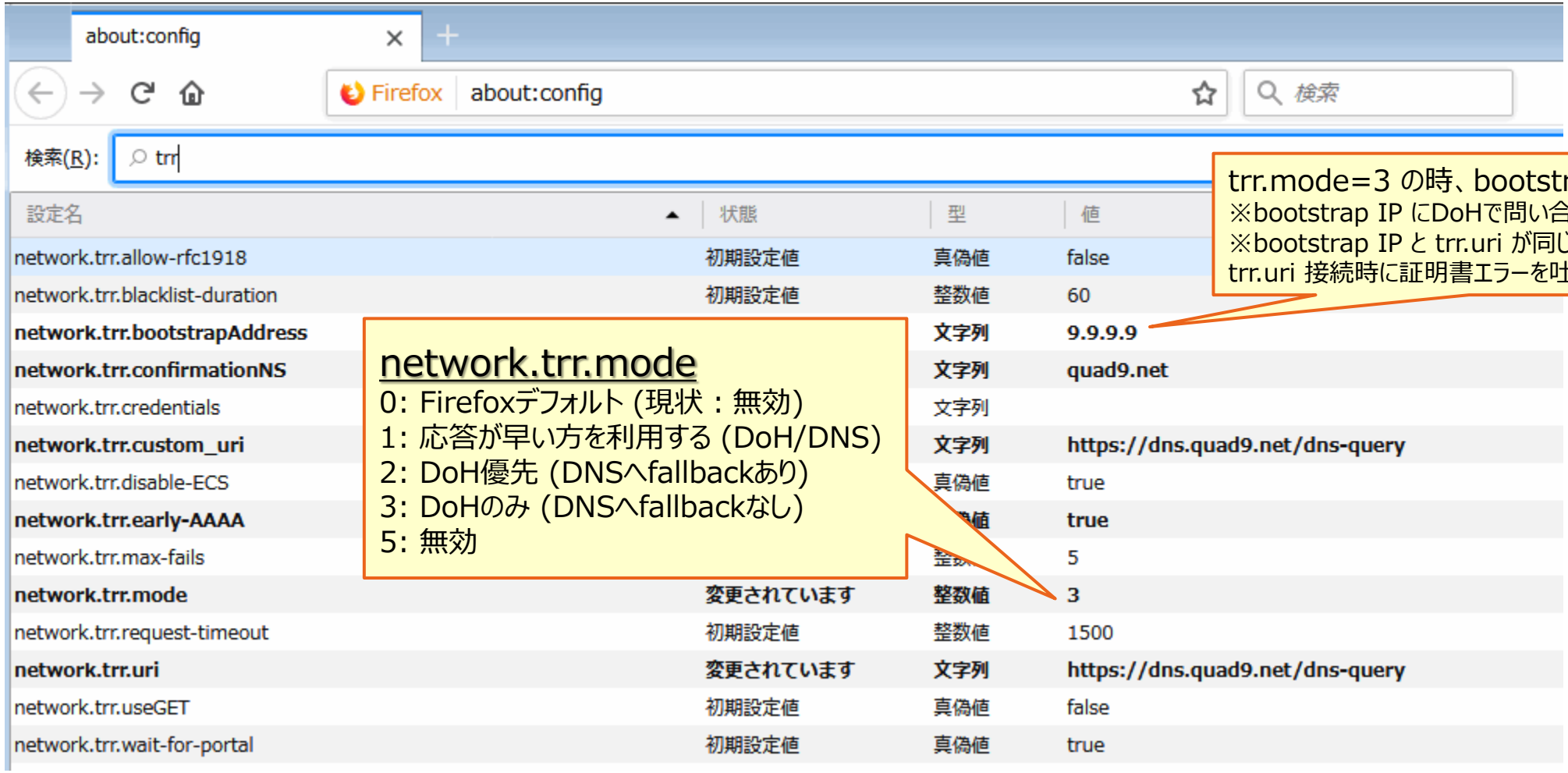
DoT/DoH 使ってみてどうだった

- Case 2: Firefox 67 で DoH を使ってみた

チェック入れるだけでON!

DoT/DoH 使ってみてどうだった

- Case 2: Firefox 67 で DoH を使ってみた



DoT/DoH 使ってみてどうだった

- Case 2: Firefox 67 で DoH を使ってみた
  - trr.mode=2 (DNSへfallbackあり) は普通に使えた
  - trr.mode=3 (DNSへfallbackなし) は時々おかしい
    - 名前解決エラーでページそもそもロードしない (F5で更新すればOK)
    - 外部コンテンツが多いサイト、部品がロード失敗 (タイミング?)
  - trr.mode=3 で社内ローカルゾーンが参照できない (当たり前)
  - 速いとは感じなかった

DoT/DoH 使ってみてどうだった

- Case 3: Firefox 67 DoH で亀が踊らない事件
  - **(1回目) trr.mode=3 で http://www.kame.net/ を開いた**

亀踊らない
じゃん！

about:networking#dns

www.kame.net	ipv4	true	2001:200:dff:fff1:216:3eff:feb1:44d7 203.178.141.194	43032
detectportal.firefox.com	ipv4	true	23.62.109.81 23.62.109.64 2600:1413:1::6011:b473 2600:1413:1::6011:b489	47
push.services.mozilla.com	ipv4	true	52.11.213.147	47
www.wide.ad.jp	ipv4	true	2001:200:dff:fff1:216:3eff:fe4b:651c 203.178.137.58	132
www.kame.net	ipv4	true	203.178.141.194	43032

・応答２つある！
・「IPv4」になってるから
踊らない？

DoT/DoH 使ってみてどうだった

- Case 3: Firefox 67 DoH で亀が踊らない事件
  - **(2回目) trr.mode=3, trr.early-AAAA=1 で http://www.kame.net/ を開いた**

亀踊らない
じゃん！

about:networking#dns

www.kame.net	ipv4	true	2001:200:dff:fff1:216:3eff:feb1:44d7 203.178.141.194	43032
detectportal.firefox.com	ipv4	true	23.62.109.81 23.62.109.64 2600:1413:1::6011:b473 2600:1413:1::6011:b489	47
push.services.mozilla.com	ipv4	true	52.11.213.147	47
www.wide.ad.jp	ipv4	true	2001:200:dff:fff1:216:3eff:fe4b:651c 203.178.137.58	132
www.kame.net	ipv4	true	203.178.141.194	43032

同じ結果
(IPv4)

DoT/DoH 使ってみてどうだった

- Case 3: Firefox 67 DoH で亀が踊らない事件
  - **(3回目) DoHなし (チェックなし) で http://www.kame.net/ を開いた**

亀踊っとる！

※PDFだと、踊らない (ご了承ください)

about:networking#dns

ホスト名	系統	TRR	アドレス	期限 (秒)
push.services.mozilla.com	ipv4	false	52.11.213.147	48
www.kame.net	ipv6	false	2001:200:dff:fff1:216:3eff:feb1:44d7	86393
www.netbsd.org	ipv4	false	2001:470:a085:999::80 199.233.217.205	59
www.kame.net	ipv4	false	2001:200:dff:fff1:216:3eff:feb1:44d7 203.178.141.194	86393

「IPv6」になっているから踊る！

DoT/DoH 使ってみてどうだった

- Case 3: Firefox 67 DoH で亀が踊らない事件
  - **(10回目) trr.mode=3 で http://www.kame.net/ を開いた**

亀踊っとる！

※PDFだと、踊らない (ご了承ください)

about:networking#dns

www.kame.net	ipv4	true	203.178.141.194 2001:200:dff:fff1:216:3eff:feb1:44d7	33380
www.momonga.org	ipv4	true	219.75.141.175	7149
github.com	ipv4	true	13.114.40.48	9
www.ipv6forum.com	ipv4	true	158.64.50.42	1750
www.openbsd.org	ipv4	true	129.128.5.194	
www.kame.net	ipv6	true	2001:200:dff:fff1:216:3eff:feb1:44d7	33380

「IPv6」になっているから踊る！

DoT/DoH 使ってみてどうだった

- Case 3: Firefox 67 DoH で亀が踊らない事件
  - ➢ もうちょっとトラブルシュートしたかったけど、こんな感じ↓

Source	Destination	Protocol	Length	Info
192.168.	9.9.9.9	TLSv1.2	571	Client Hello
9.9.9.9	192.168.	TCP	60	443→60858 [ACK] Seq=1 Ack=518 Win=30464 Len=0
9.9.9.9	192.168.	TLSv1.2	1514	Server Hello
9.9.9.9	192.168.	TLSv1.2	1514	Certificate
9.9.9.9	192.168.	TLSv1.2	78	Server Key Exchange
192.168.	9.9.9.9	TCP	54	60858→443 [ACK] Seq=518 Ack=2945 Win=65700 Len=0
192.168.	9.9.9.9	TLSv1.2	240	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
192.168.	9.9.9.9	TLSv1.2	223	Application Data
192.168.	9.9.9.9	TLSv1.2	269	Application Data
192.168.	9.9.9.9	TLSv1.2	130	Application Data
9.9.9.9	192.168.	TCP	60	443→60858 [ACK] Seq=2945 Ack=1088 Win=33536 Len=0
9.9.9.9	192.168.	TLSv1.2	232	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
9.9.9.9	192.168.	TLSv1.2	108	Application Data
9.9.9.9	192.168.	TLSv1.2	88	Application Data
9.9.9.9	192.168.	TLSv1.2	84	Application Data
192.168.	9.9.9.9	TCP	54	60858→443 [ACK] Seq=1164 Ack=3241 Win=65404 Len=0
192.168.	9.9.9.9	TLSv1.2	84	Application Data
9.9.9.9	192.168.	TLSv1.2	88	Application Data
9.9.9.9	192.168.	TLSv1.2	435	Application Data
9.9.9.9	192.168.	TLSv1.2	226	Application Data
192.168.	9.9.9.9	TCP	54	60858→443 [ACK] Seq=1194 Ack=3828 Win=64816 Len=0
9.9.9.9	192.168.	TCP	60	443→60858 [ACK] Seq=3828 Ack=1194 Win=33536 Len=0
192.168.	9.9.9.9	TLSv1.2	114	Application Data

  - ➢ 本気になったら、こういう方法もある？（やらなかった）

Importing Master Key Secrets into Wireshark
https://developer.mozilla.org/en-US/docs/Mozilla/Projects/NSS/Key_Log_Format
https://wiki.wireshark.org/TLS?action=show&redirect=SSL

DoT と DoH の違い

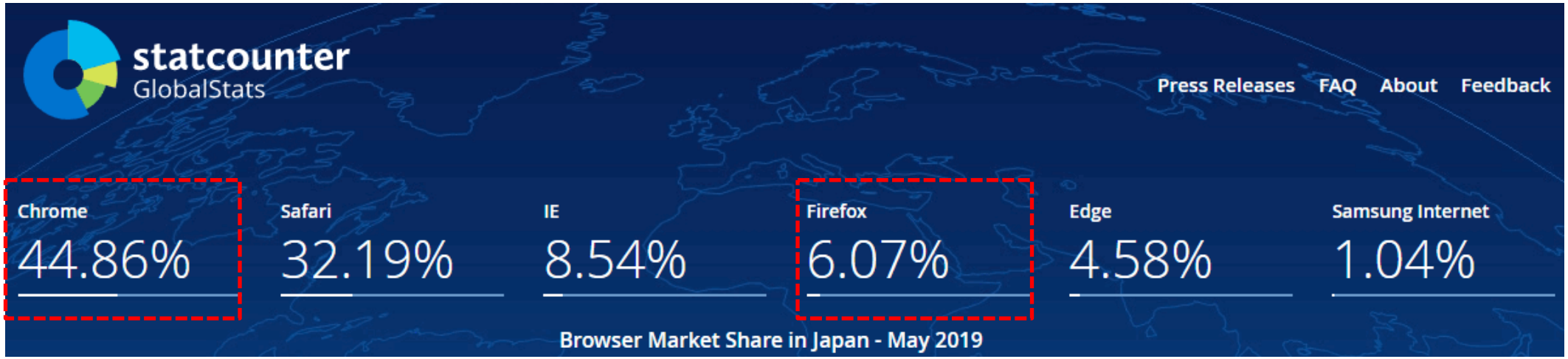
※現時点の実装

比較項目	DNS-over-TLS (DoT)	DNS-over-HTTPS (DoH)
DNSリゾルバ設定	システム	**ユーザ／アプリ毎**
通信の識別・検知	可能 (tcp/853)	**不可能**
“opportunistic” 動作	あり	なし
平文ダウングレード	あり	なし
多重化・再送制御	なし	あり (HTTP/2+)
server-push	なし	あり (HTTP/2+)
自動設定の仕組み	なし	**なし**

- 現時点のDoHは、**ネットワークオペレータがコントロールでない**、Public DNSを使わざるをえない**集中型DoH**の実装である。

集中型DoHはなぜ気にする必要あるの？

http://gs.statcounter.com/browser-market-share/all/japan



- シェア 50% 以上のブラウザがやろうとしてるから

Centralized DNS over HTTPS (DoH) Implementation Issues and Risks (draft) より
https://tools.ietf.org/html/draft-livingood-doh-implementation-risks-issues-03

> To illustrate the potential for rapid Centralized DoH, if just two organizations, Google and Mozilla, were to implement Centralized DoH in Android, Chrome, and Firefox, then global adoption of DoH could occur rapidly and represent the majority of DNS queries on the Internet.

GoogleとMozillaがデフォルト化したら、「集中型」DoHの採用が急速化し、**世界中のDNSクエリの大半がDoHになる恐れがある**

MozillaとGoogleのスタンス

https://mailarchive.ietf.org/arch/msg/doh/JhFPKoyGU2JqKmUk3GEe5yjuSHI

"Provide our users with meaningful choice and control, e.g. allow end users/admins to control and configure the feature, whether they want to use a custom DoH server or just keep on using their regular DNS[...].There are no plans to force any specific resolver without user consent / opt-in.[...]We are considering a first milestone where Chrome would do an automatic upgrade to DoH when a user's existing resolver is capable of it"

・**デフォルト化予定なし**
・管理者コントロールも考慮
・現行リゾルバがDoH対応していれば、DoHへ自動アップグレードする
→opportunistic DoH?

https://mailarchive.ietf.org/arch/msg/doh/po6GCAJ52BAKuyL-dZiU91v6hLw

・**デフォルト化予定あり（一部の地域）**
・ユーザへ告知、無効化オプションを提供

"we may have DoH/TRR on by default in some regions and not others[...].The user will be informed that we have enabled use of a TRR and have the opportunity to turn it off at that time"

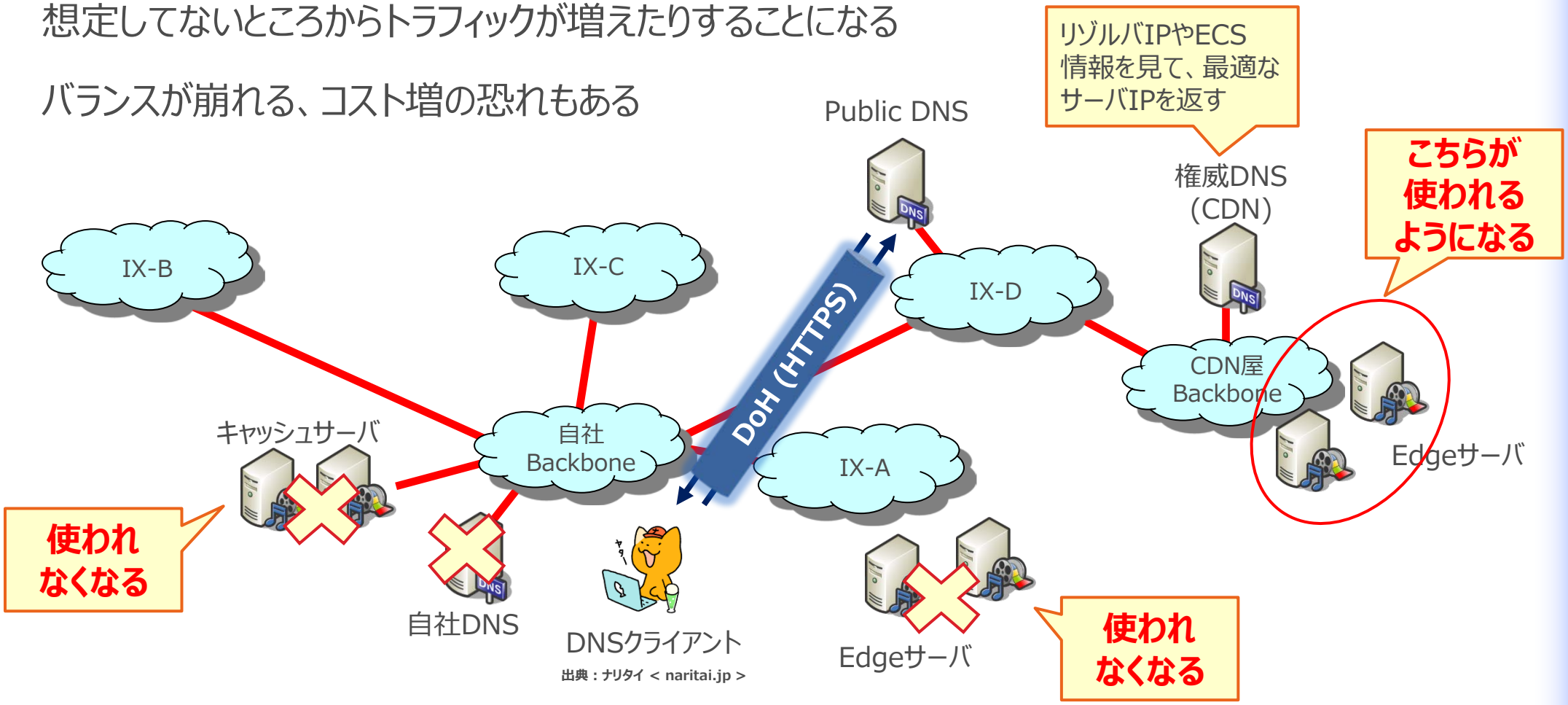
まだ、大丈夫かな… “Sky is not falling” (yet)?

集中型DoHの課題（ISP編）（1）

- **① サポート対応できなくなる**
  - DNS通信見えなくなっているので、トラブルシュートできない、対応できない
  - お客様に「Cloudflareが・・・」説明できない、自分達のせいにされてしまう、辛い
- **② サービスレベル低下の恐れがある**
  - 障害起きても、何もわからない、何も手が打てない
  - リモートDNSまでの経路で影響受ける可能性がある
- **③ フィルタリングが変わる**
  - 児童ポルノブロッキングができなくなる
  - 海外は「通信の秘密」がない、どのフィルタリングされるか不明

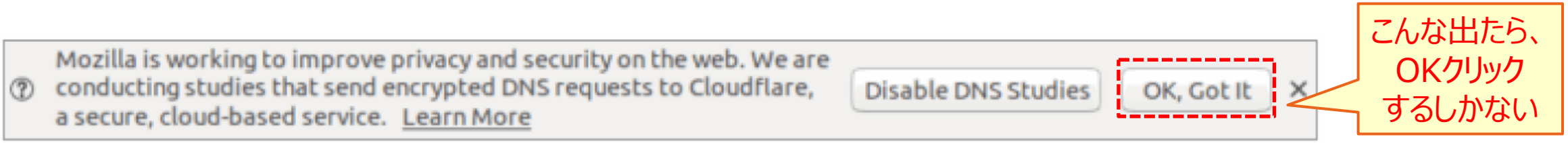
集中型DoHの課題（ISP編）(2)

- **④ ネットワーク経路設計が狂ってしまう（主にCDN関連）**
  - 想定してないところからトラフィックが増えたりすることになる
  - バランスが崩れる、コスト増の恐れもある



集中型DoHの課題（ISP編）(3)

- **⑤ ユーザセキュリティレベルの低下**
  - セキュリティソフトがDNS通信で行動パターン分析できなくなるので、検知率低下の恐れがある
  - DoHを使った高度なボットネットが普及し、踏み台にされてしまう
- **⑥ メリットを感じない**
  - 政府やプロバイダーへの信頼度が違う、文化の違いがある、日本ユーザにとってのメリットは？
  - ブラウザ屋さんがやるから、対応しないといけないけど、ISPとしてもメリット感じない
- **⑦ 自社ユーザがだまされるのが気にいらない**



※MozillaのDoH実証実験の時に表示されたメッセージ

集中型DoHの課題 (一般編) (1)

- **① エンタプライズネットワークへの影響**
  - ローカル (split-horizon) DNS、 .local/.home.arpa、DNS64 が動かない
  - プライベートネットワーク内のフィルタリングができなくなる
- **② プライバシー保護の有効性が怪しい**
  - WebRTC、ヘルパプログラムなどがシステムリゾルバ使ってしまうので、完全ではない
  - 命をかけてプライバシー保護ツールほしい者は、VPN/Tor/Psiphon既に使っている
  - パブリックDNS本当に信頼できるか → データ集中
- **③ DNSセキュリティ対策として不完全**
  - フルリゾルバまではいいけど、フルリゾルバ上位は通常通り (キャッシュ汚染、フラグメント攻撃など)
  - 秘密性はいいけど、完全性の保証できない (→完全性はDNSSECが必要)

集中型DoHの課題 (一般編) (2)

- **④ プロバイダ集中による課題 (“DNS-over-Cloud”)**
  - 攻撃しやすくなる、スケールが難しい、「分散インターネット」の概念に違反している
  - ROOT改ざんの可能性 (気にいらないTLDを消す、勝手にTLD増やす、など) 、ネット中立性
  - HTTPだと、ユーザ識別につながる情報が多い (cookie、ヘッダ、ヘッダ順番など)
  - データ悪用の恐れ (米国なので・・・)、HTTPだとユーザ識別につながる情報が多い
- **⑤ 更なるプライバシー侵害につながる**
  - ある国では、TLS MITM が必須になる、政府DNS利用が必須になる恐れがある
  - 政府による暗号化攻撃が行われる恐れがある

集中型DoHの課題 (一般編) (3)

- **⑥ サイバーセキュリティ研究への影響**
  - Passive DNS が使えなくなり、分析が難しくなる
  - セキュリティソフトの検知率低下につながってしまう恐れがある
- **⑦ BOT! Exfiltration! Abuse!**
  - C&C (C2) over DoH (PoCが既に公開されている)
  - HTTPヘッダ悪用でドメインフロンティング (Hostヘッダの悪用で別サーバへリダイレクト)

https://blog.redteam.pl/2019/04/dns-based-threat-hunting-and-doh.html
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/doh-dns-over-https-poses-possible-risks-to-enterprises/
https://github.com/SpiderLabs/DoHC2
https://sensepost.com/blog/2018/waiting-for-godoh/
https://blog.netlab.360.com/an-analysis-of-godlua-backdoor-en/

まとめ

- Encrypted DNS は素晴らしい概念
- DNS-over-TLS (DoT) ：わかりやすい、今後実装検討したい
- DNS-over-HTTPS (DoH) ：プロトコル的にいいが、現在の実装で課題が多い
- DoH出来たばかりだが、勢いと反論がすごいので、今後ウォッチしたい

Acknowledgements

- BBSec/安藤様：　DoH議論のお話ありがとうございました
- iij/やまぐち様：https://speakerdeck.com/yamaya/https　勉強になりました
- Joe St.Sauver, Barry Greene, Stephen Farrell: discussions at M3AAWG
- DNS Privacy Project: https://dnsprivacy.org/wiki/
- 神谷健太さん：DoHテスト用wrapperスクリプト、亀ちゃんGIF、ありがとう！

（おまけ）JPAAWGについて

https://www.jpaawg.org/

「Japan Anti-Abuse Working Group」発足！

- 2018年11月に1回目のGeneral Meetingを実施
- 大規模な General Meeting は 1回/年程度開催
- 検討テーマ毎に Sub Working Group を構成，これらについての会合は定期的に開催
- 東京圏以外での中規模なイベントも要望に応じて開催したい
- xSP、ESP、ベンダ、政府機関、アカデミック、セキュリティ関連団体等、**幅広く会員募集**
- 最新のアビューズとセキュリティ課題を取り上げて議論し、日本の環境にあったBCPを今後公開していきたい