Keep my privacy:
DNS over HTTPS over CGN, public NAT64
(or IPv6 transition technologies, Open HTTP proxies)

Kazunori Fujiwara, JPRS
fujiwara@jprs.co.jp

OARC 35, 2021/5/6

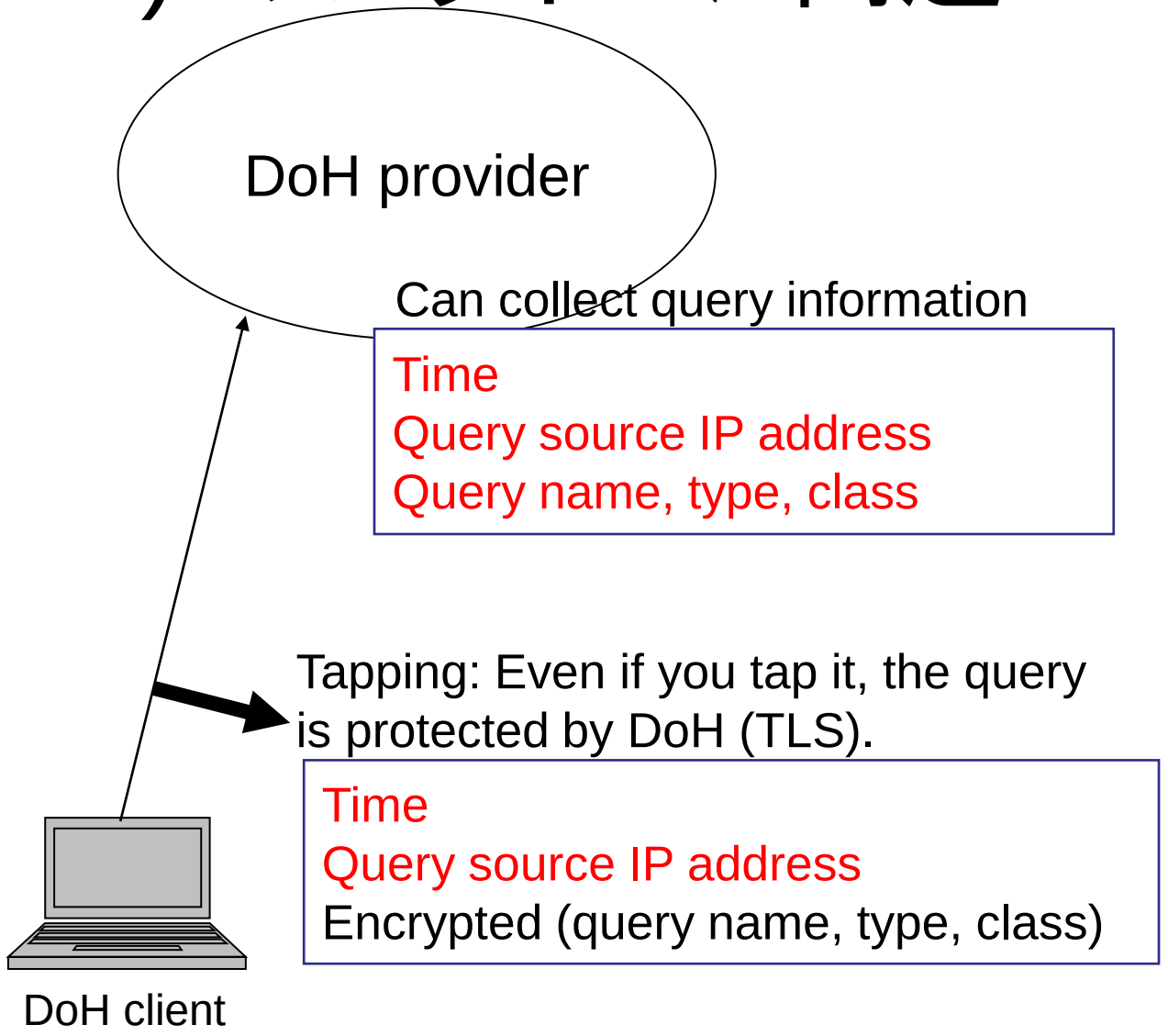
dnsops.jp, 2021/6/25

Copyright © 2021 Japan Registry Services Co., Ltd.

DNS over HTTPS (DoH) のプライバシ問題

- Sensitive data in DNS queries
  - Time
  - Query source IP address
  - DNS query (name, type, class)
- DoH hides DNS query (name, class, type) by encryption
- Privacy issues
  - query source IP address is not protected
  - DoH providers can collect the whole data

- **<u>How can I hide my IP address from DoH providers ?</u>**



Copyright © 2021 Japan Registry Services Co., Ltd.

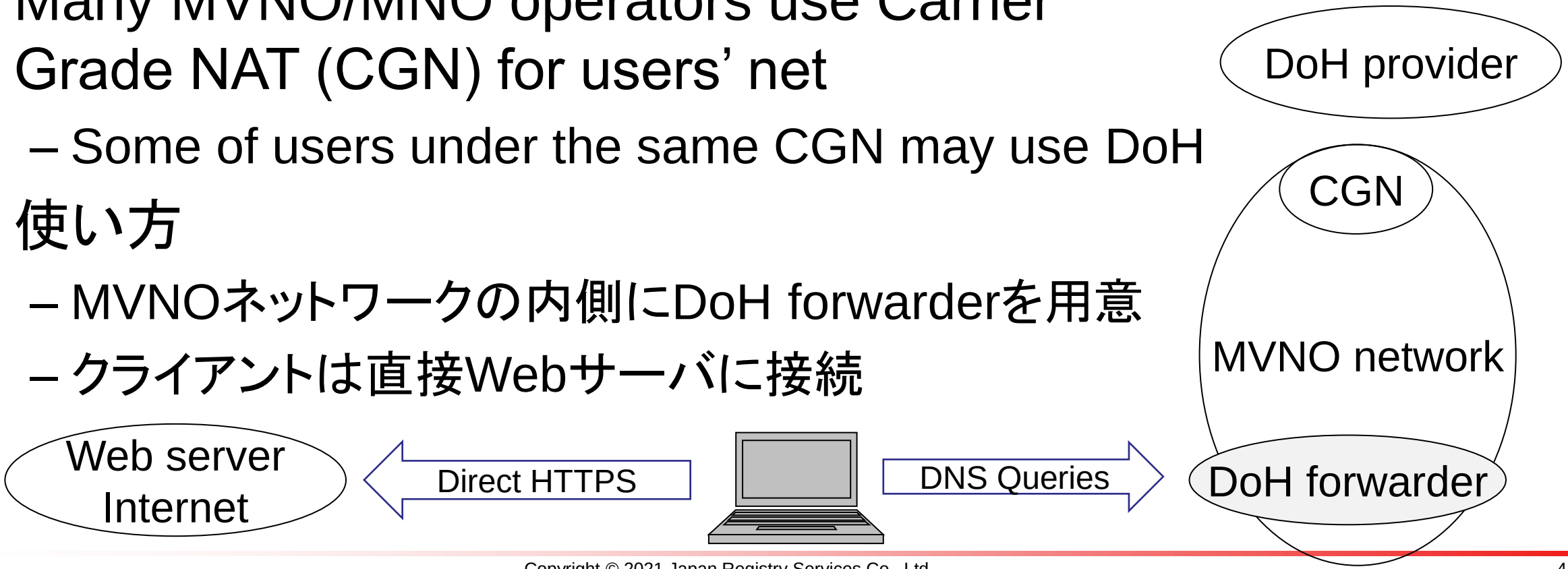
How to hide query source IP address ?

- 既存の提案もquery source IP addressを隠そうとしていた
  - Tor's DNS … Tor networkが必要
  - Oblivious DNS (DoH) … ODoHプロバイダが必要
- Simpler solutions to hide (1人でもできる軽いものが欲しい)
  - 木の葉を隠すなら森の中/
  - query source IP addresses を以下のものを使って隠せそう
    - IPv4 NAT (CGN, NAT64, IPv6 transition technologies)
    - Open HTTP Proxy (or Tor HTTPS)
- さらに、web serverへの接続は別のIP addressを使える
  - 直接接続する

Copyright © 2021 Japan Registry Services Co., Ltd.

Idea: DoH over CGN

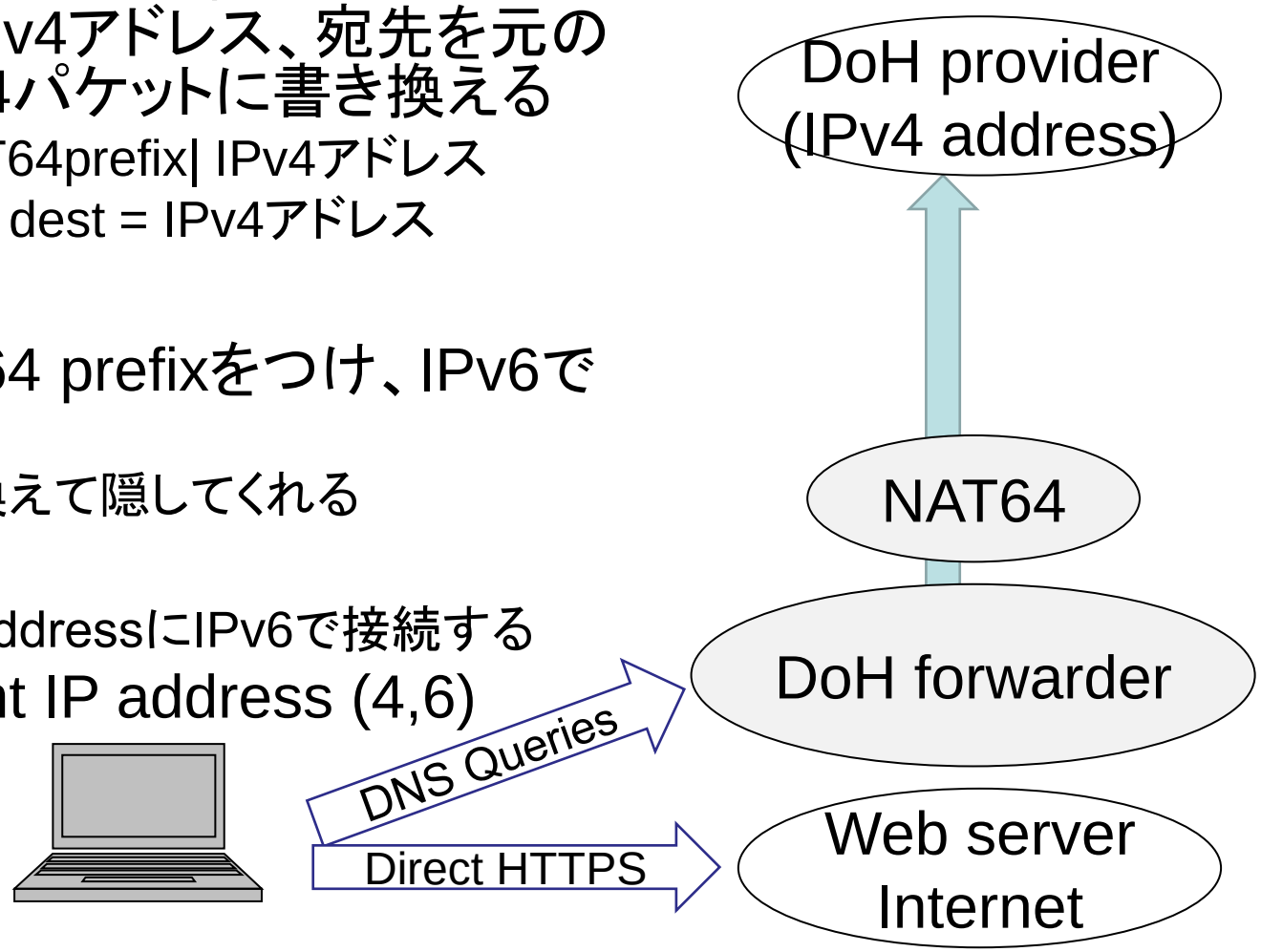
- 安いMVNO SIMを使い、CGNを使って隠す
  - 月100MBのプランなら190円
- Many MVNO/MNO operators use Carrier Grade NAT (CGN) for users' net
  - Some of users under the same CGN may use DoH
- 使い方
  - MVNOネットワークの内側にDoH forwarderを用意
  - クライアントは直接Webサーバに接続



Copyright © 2021 Japan Registry Services Co., Ltd.

Idea: DoH over NAT64

- Public NAT64 services: see https://nat64.xyz/
  - NAT64では、NAT64 prefix + IPv4アドレス行きのIPv6パケットを、送信元をNAT64の共有IPv4アドレス、宛先を元の宛先の中のIPv4アドレスとしたIPv4パケットに書き換える
    - IPv6: source=送信元IPv6, dest=NAT64prefix| IPv4アドレス
    - IPv4: source=NAT64共有v4アドレス, dest = IPv4アドレス
- 使い方
  - DoHサーバのIPv4アドレスにNAT64 prefixをつけ、IPv6でDoHサーバに接続する
    - NAT64が送信元IPv6アドレスを書き換えて隠してくれる
  - 特殊な DoH forwarder が必要
    - NAT64 prefix + DoH server's IPv4 addressにIPv6で接続する
  - Access web servers from different IP address (4,6)
  - もうすこし秘密にしたいなら
    - 複数の NAT64 services/prefixes
    - 複数の DoH providers



Copyright © 2021 Japan Registry Services Co., Ltd.

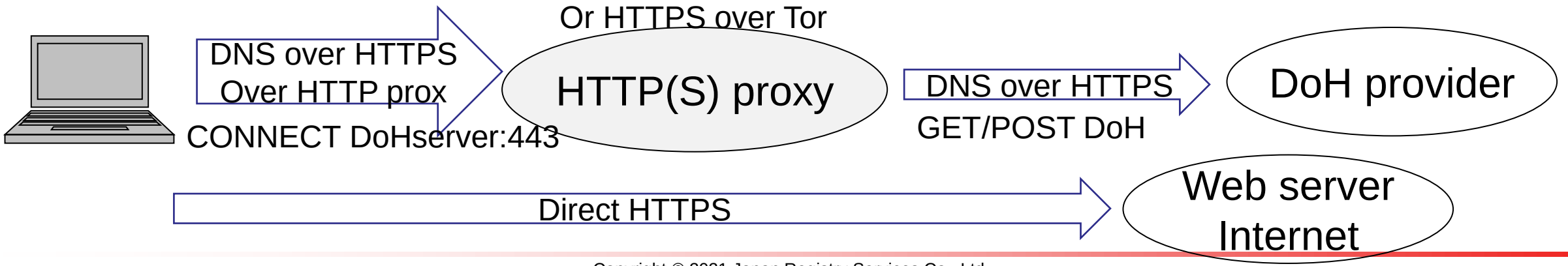
Idea: DoH over IPv6 transition technology

- IPv4 over IPv6 services (DS-Lite, MAP-E)
  - In many cases, multiple subscribers share one IPv4 address
  - When multiple users use DoH under the shared IPv4 address, DoH providers can know one global IPv4 address only
- Use scenario
  - Disable IPv6 at a client
  - Or, prepare DoH forwarder that connects to DoH server via IPv4 only
- Problem
  - It is weak because source IP address of DoH and web access are the same
  - Disabling IPv6 goes against IPv6 transition

Copyright © 2021 Japan Registry Services Co., Ltd.

Idea: DoH over (open) HTTP proxies

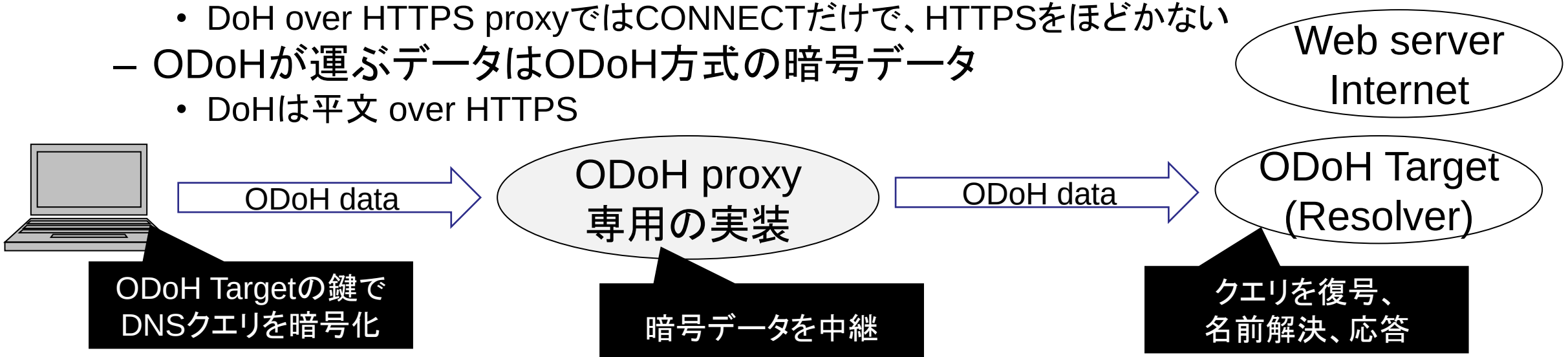
- 理由
  - ProxyはDoHの中身を知ることができない
  - DoH provider は、接続元IPアドレスを知りようがない
- 使い方
  - DoHクエリをHTTP proxy経由で送る
  - Webサーバへは直接接続する
  - 特殊なDoH forwarderが必要: proxy経由できるもの
- 問題: Open Proxyを使う時は、利用許諾をとれない (串ってやつ)
- 提案
  - DoH over Tor
  - だれか、DoHサーバにしか繋げられないOpen Proxy serviceを提供してください



Copyright © 2021 Japan Registry Services Co., Ltd.

Oblivious DoH

- Oblivios DoH (ODoH)
  - ODoHクライアントは、ODoH Targetの鍵でDNSクエリを暗号化、HTTPSでODoH proxyに接続
  - ODoH proxyはHTTPSをほどいて暗号化されたDNSクエリを取り出し、HTTPSでODoH Targetに接続して送信
  - ODoH Targetはクエリを復号して名前解決し、暗号化して返す
- DoHや、DoH over HTTP PROXYとの違い
  - ODoHでは、TLSが2本あり、proxyが一度終端する
    - DoH over HTTPS proxyではCONNECTだけで、HTTPSをほどかない
  - ODoHが運ぶデータはODoH方式の暗号データ
    - DoHは平文 over HTTPS



Copyright © 2021 Japan Registry Services Co., Ltd.

Tool: 自分の IPv4 address をDNSで知る

- Akamai provides "whoami.akamai.net"
  - Example: dig +short A whoami.akamai.net
  - It returns resolver's IP address in use
- We can use the service to know my IP address
  - First, dig akamai.net ns
    - returns akamai.net name server addresses
  - Next, "dig @(akamai.net IPv4 server address) whoami.akamai.net A
    - returns my IPv4 address
  - dig @(akamai.net IPv6 server address) whoami.akamai.net AAAA
    - returns my IPv6 address

Copyright © 2021 Japan Registry Services Co., Ltd.

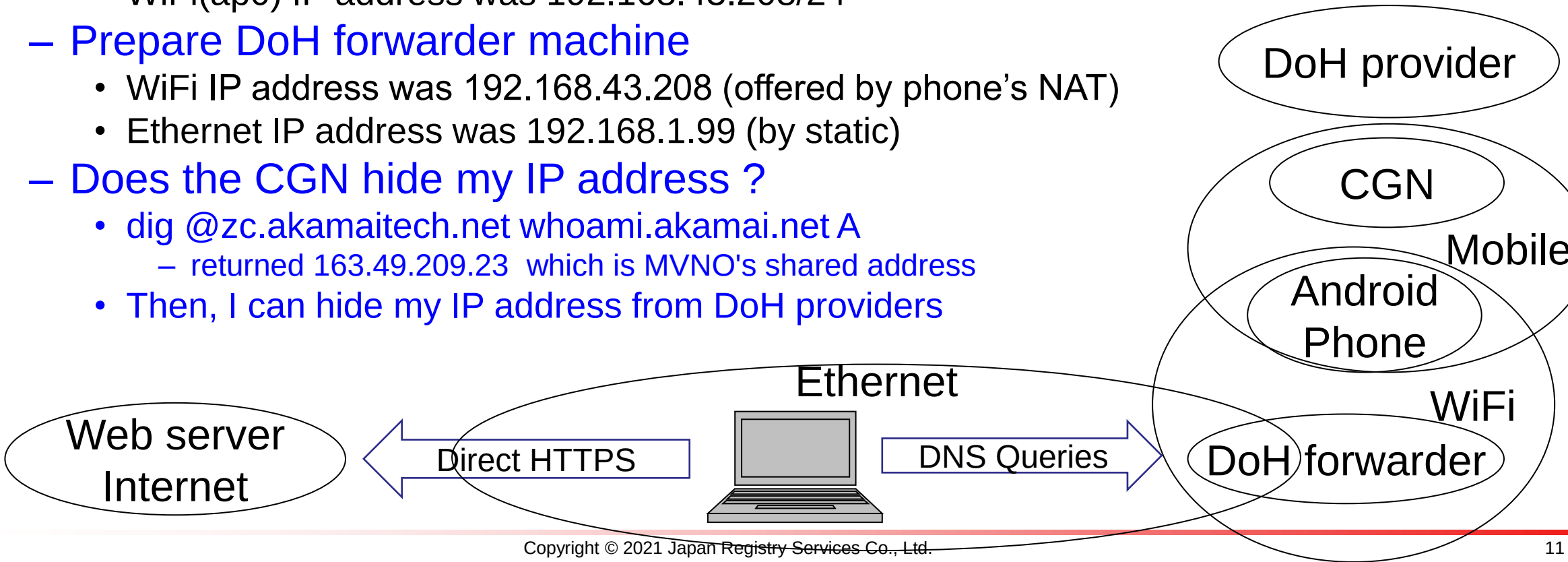
Tools: DoH forwarder

- doh-forwarder
  - https://github.com/kpadron/doh-forwarder
  - Receives queries from clients via port 53 UDP, TCP
  - Forwards queries to a DoH server
- fujiwara's DNS Forwarder: I made my own DNS forwarder
  - Written in perl (depends on Net::DNS and IO::Socket::SSL)
  - Receiveing queries from clients via UDP, TCP, (DoT), DoH
  - Forwarding queries to a server via UDP, TCP, (DoT), DoH, DoH over HTTP Proxy
  - Each TCP (DoT, DoH) connection is closed on every query
  - NAT64 is supported
  - Limited functions: No ACLs, No performance, ...
  - Usage: DNSforwarder.pl -u UDP_listen -t TCP_listen -U UDP_server -H DoH_URL -N NAT64 prefix

Copyright © 2021 Japan Registry Services Co., Ltd.

Evaluation of DoH over CGN (1)

- Environment
  - MVNO: Excite mobile (https://bb.excite.co.jp/exmb/sim/)
  - Android phone as WiFi/NAT router (WiFi Tethering)
    - Outgoing(ccmni1) IP address was 100.73.209.188 (RFC 6598 Shared Address Space)
    - WiFi(ap0) IP address was 192.168.43.208/24
  - Prepare DoH forwarder machine
    - WiFi IP address was 192.168.43.208 (offered by phone's NAT)
    - Ethernet IP address was 192.168.1.99 (by static)
  - Does the CGN hide my IP address ?
    - dig @zc.akamaitech.net whoami.akamai.net A
      - returned 163.49.209.23 which is MVNO's shared address
    - Then, I can hide my IP address from DoH providers

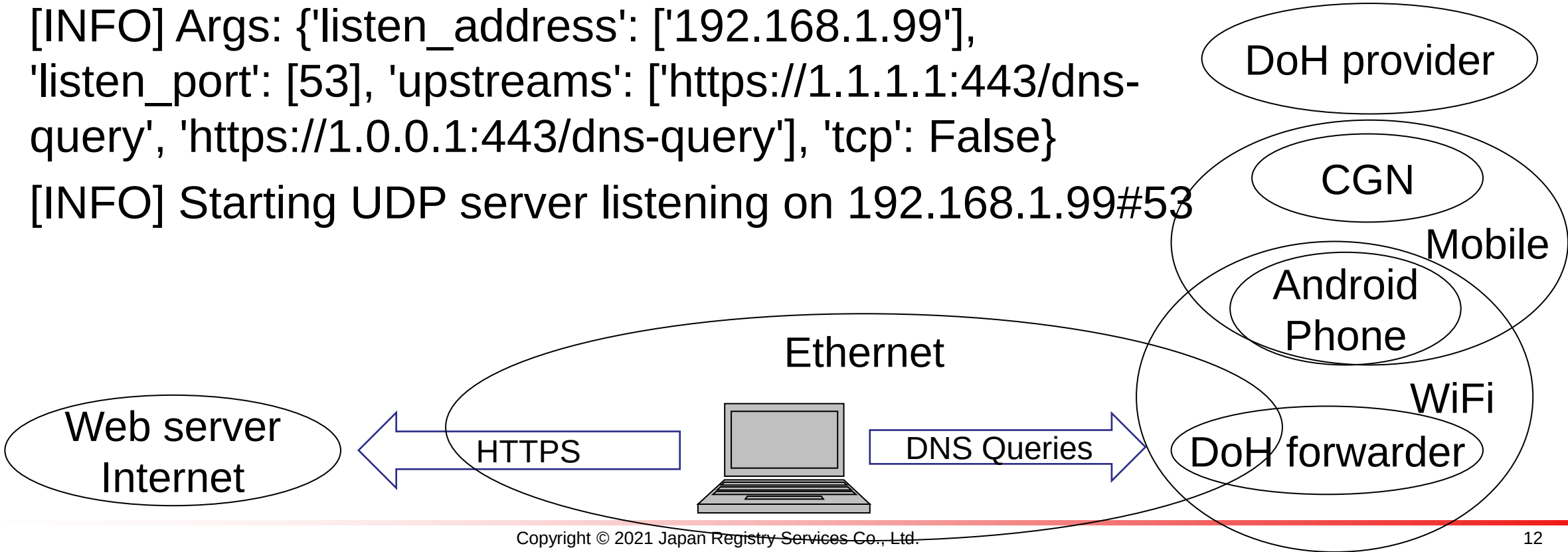


Copyright © 2021 Japan Registry Services Co., Ltd.

Evaluation of DoH over CGN (2)

- Run doh-forwarder at DoH forwarder machine

```
# python3.7 doh-forwarder.py  -l 192.168.1.99 -p 53
[INFO] Starting DNS over HTTPS forwarder
[INFO] Args: {'listen_address': ['192.168.1.99'], 'listen_port': [53], 'upstreams': ['https://1.1.1.1:443/dns-query', 'https://1.0.0.1:443/dns-query'], 'tcp': False}
[INFO] Starting UDP server listening on 192.168.1.99#53
```



Copyright © 2021 Japan Registry Services Co., Ltd.

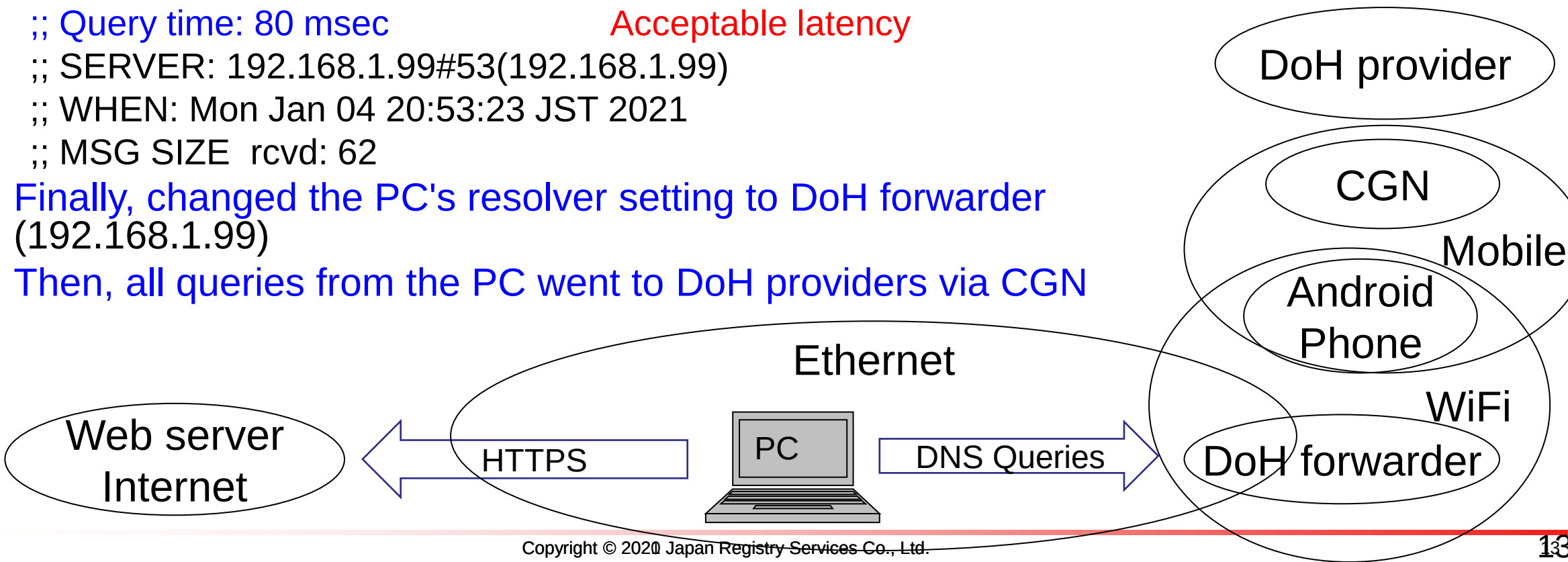
Evaluation of DoH over CGN (3)

- Checked responses from DoH forwarder
  - Client: dig @DoHforwarder whoami.akamai.net

```
;whoami.akamai.net.          IN     A
;; ANSWER SECTION:
whoami.akamai.net.     26     IN     A      162.158.117.105
;; Query time: 80 msec                    Acceptable latency
;; SERVER: 192.168.1.99#53(192.168.1.99)
;; WHEN: Mon Jan 04 20:53:23 JST 2021
;; MSG SIZE  rcvd: 62
```

Cloudflare's IP address

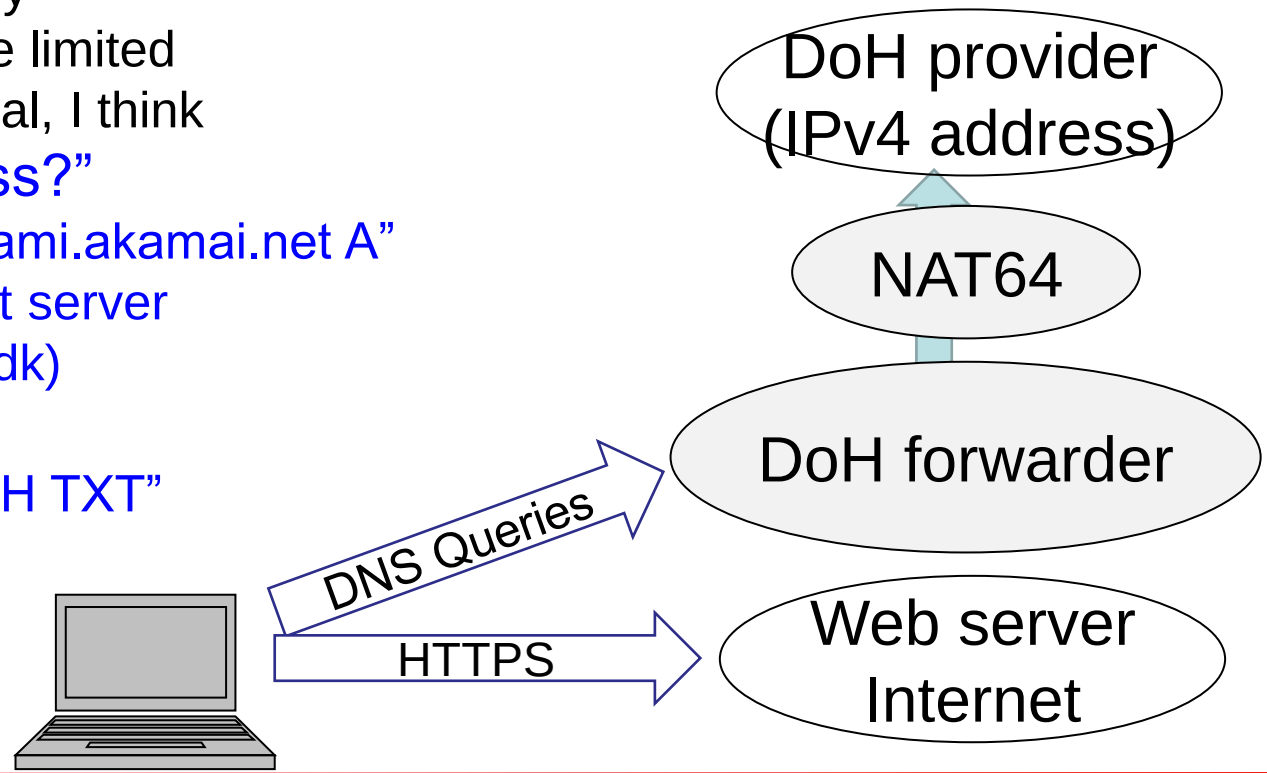
- Finally, changed the PC's resolver setting to DoH forwarder (192.168.1.99)
- Then, all queries from the PC went to DoH providers via CGN



Copyright © 2021 Japan Registry Services Co., Ltd.

Evaluation of DoH over NAT64 (1)

- Choose one NAT64 prefix from https://nat64.xyz/
  - Provider: Kasper Dupont
  - Location: The Netherlands / Amsterdam
  - NAT64 prefix: 2a00:1098:2b::/96
  - Agree and follow the terms of service: https://nat64.net/tos
    - No Abuse: It is an experiment / temporary
    - No flood: DNS queries from a person are limited
    - No illegal access: DoH server is not illegal, I think
  - “Does the NAT64 hide my IPv6 address?”
    - “dig @2a00:1098:2b::23.74.25.192 whoami.akamai.net A”
      NAT64 prefix + IPv4 of akamai.net server
      returned 46.235.231.114 (nat64.dyndns.dk)
  - Which node answered from NAT64 ?
    - “dig @2a00:1098:2b::1.1.1.1 id.server CH TXT”
      returned TXT “AMS“
      ;; Query time: 238 msec
      (from Japan)



Copyright © 2021 Japan Registry Services Co., Ltd.

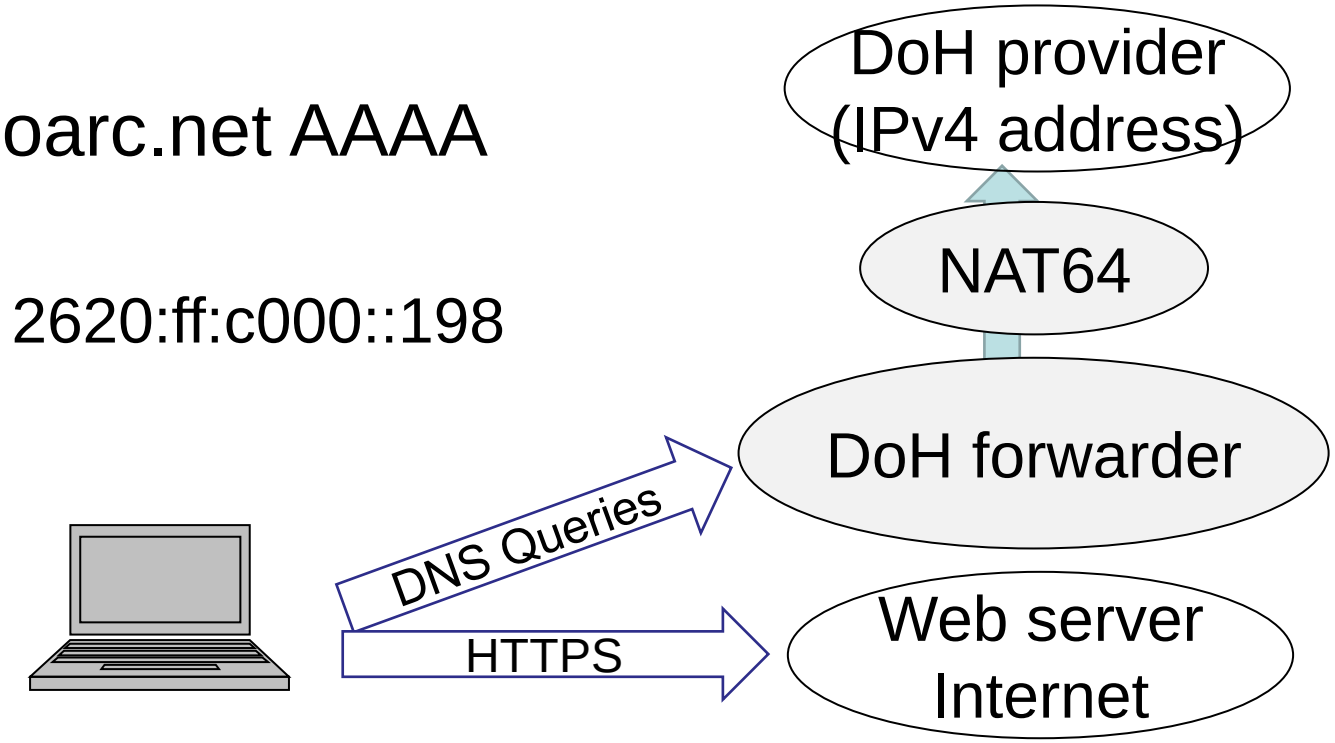
Evaluation of DoH over NAT64 (2)

- Start special DoH forwarder
  - perl DNSforwarder.pl -u 203.178.129.11/53 -U 8.8.8.8 -H https://cloudflare-dns.com/dns-query -N 2a00:1098:2b::
  - DoH forwarder's listen address is 203.178.129.11 port 53
    - DoH server address is https://cloudflare-dns.com/dns-query
    - to resolve "cloudflare-dns.com", the proxy uses 8.8.8.8 resolver
      → cloudflare-dns.com IN A 104.16.249.249
    - NAT64 address is 2a00:1098:2b::
      - DNSforwarder.pl rewrites DoH server's IP address to NAT64 prefix + IPv4 address 2a00:1098:2b::104.16.249.249 at connect

Copyright © 2021 Japan Registry Services Co., Ltd.

Evaluation of DoH over NAT64 (3)

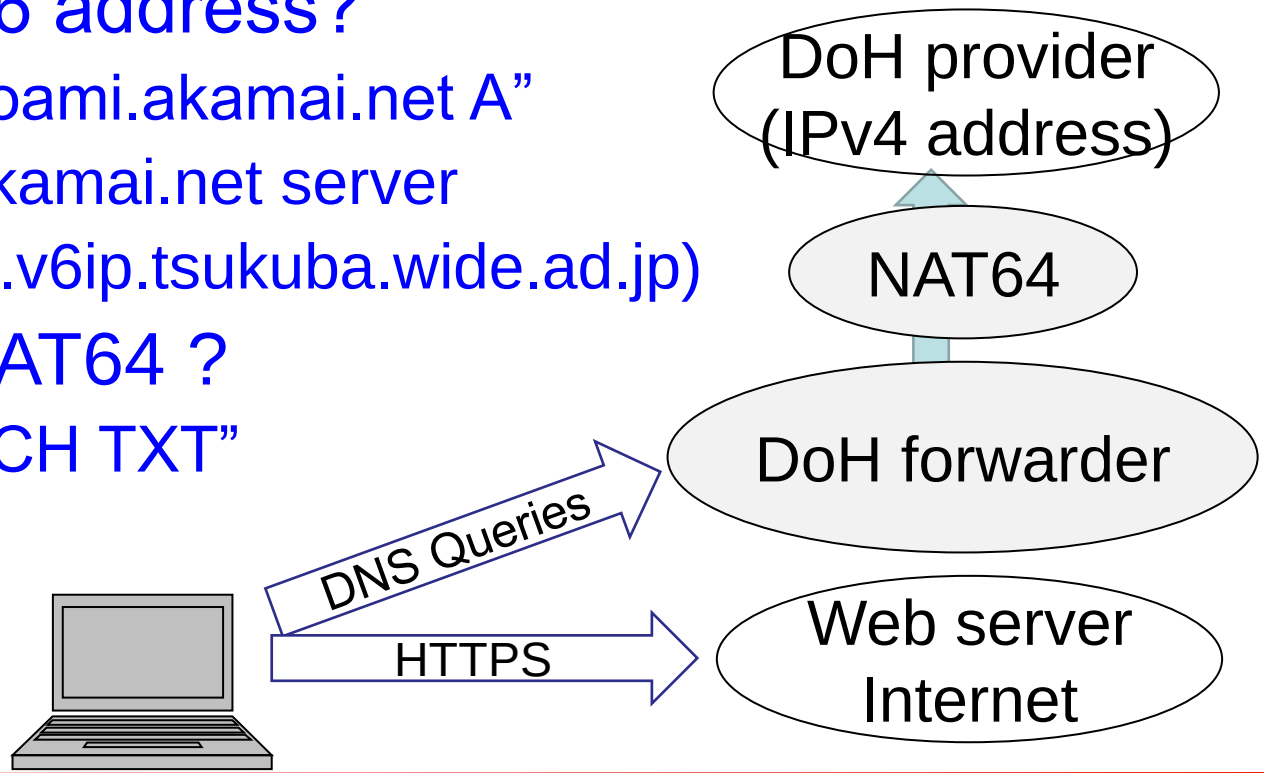
- dig @DoHforwarder id.server CH TXT
  - ;; ANSWER SECTION:
  - id.server. 1 CH TXT "AMS"
    Cloudflare's AMS node
  - ;; Query time: 955 msec
- dig @DoHforwarder www.dns-oarc.net AAAA
  - ;; ANSWER SECTION:
  - www.dns-oarc.net. 120 IN AAAA 2620:ff:c000::198
  - ;; Query time: 1035 msec



Copyright © 2021 Japan Registry Services Co., Ltd.

Evaluation of DoH over NAT64 (4)

- WIDE InternetではNAT64が提供されているみたいなので使ってみた
  - 64:ff9b::/96 (RFC 6052 Well-Known Prefix, 普通はAS内のみ)
  - “Does the NAT64 hide my IPv6 address?”
    - “dig @64:ff9b::23.74.25.192 whoami.akamai.net A”
      NAT64 prefix + IPv4 of akamai.net server
      returned 203.178.132.88 (nat64.v6ip.tsukuba.wide.ad.jp)
  - Which node answered from NAT64 ?
    - “dig @64:ff9b::1.1.1.1 id.server CH TXT”
      returned TXT “NRT“
      ;; Query time: 13 msec
      (from Japan)



Copyright © 2021 Japan Registry Services Co., Ltd.

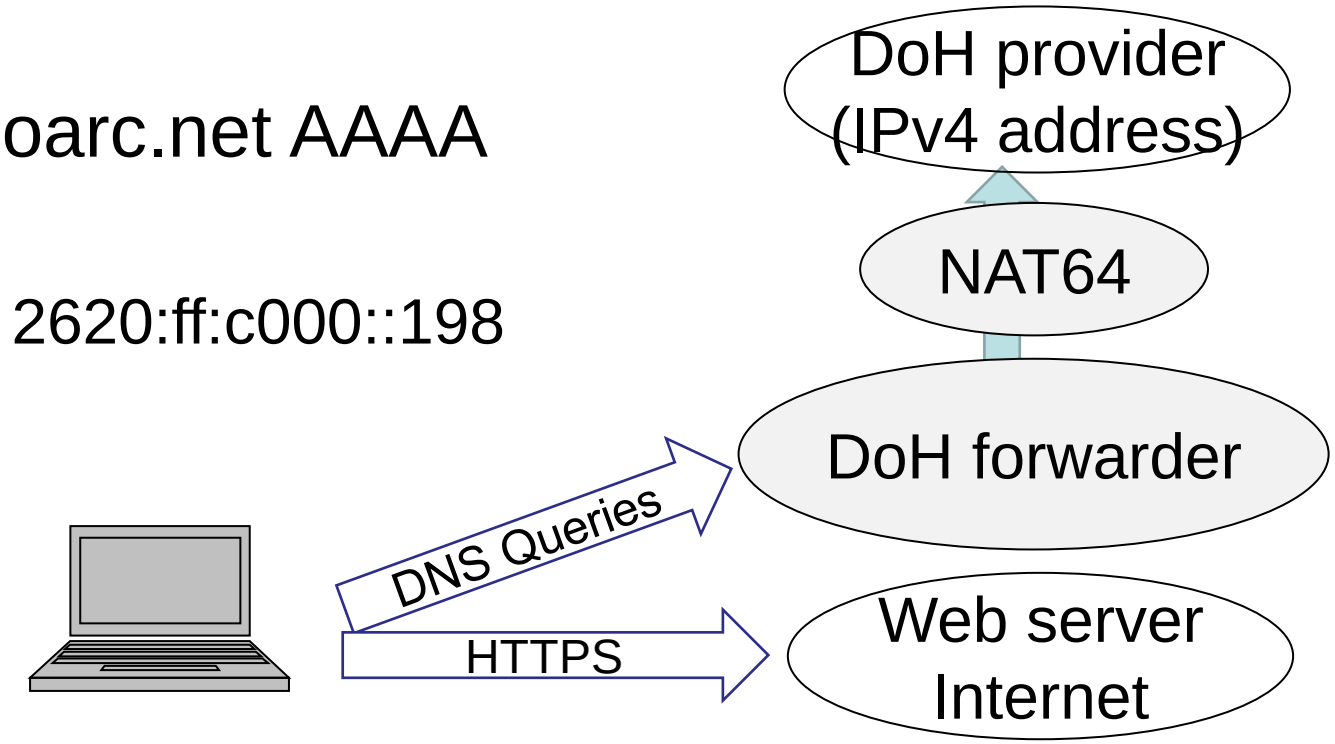
Evaluation of DoH over NAT64 (5)

- Start special DoH forwarder
  - perl DNSforwarder.pl -u 203.178.129.11/53 -U 8.8.8.8 -H https://cloudflare-dns.com/dns-query -N 64:ff9b::
  - DoH forwarder's listen address is 203.178.129.11 port 53
    - DoH server address is https://cloudflare-dns.com/dns-query
    - to resolve "cloudflare-dns.com", the proxy uses 8.8.8.8 resolver
      → cloudflare-dns.com IN A 104.16.249.249
    - NAT64 address is 64:ff9b::
      - DNSforwarder.pl rewrites DoH server's IP address to NAT64 prefix + IPv4 address 64:ff9b::104.16.249.249 at connect

Copyright © 2021 Japan Registry Services Co., Ltd.

Evaluation of DoH over NAT64 (6)

- dig @DoHforwarder id.server CH TXT
  - ;; ANSWER SECTION:
  - id.server. 1 CH TXT “NRT"
    Cloudflare's NRT node
  - ;; Query time: 155 msec
- dig @DoHforwarder www.dns-oarc.net AAAA
  - ;; ANSWER SECTION:
  - www.dns-oarc.net. 120 IN AAAA 2620:ff:c000::198
  - ;; Query time: 110 msec
  - これぐらいの遅延なら使える



Copyright © 2021 Japan Registry Services Co., Ltd.

Evaluation of DoH over HTTP Proxy

- Open Proxies使うのは微妙なので、いくつかのDoHのみ接続できるsquidを動かす
  - acl doh dstdomain dns.google
  - acl doh dstdomain cloudflare-dns.com
  - acl doh dstdomain doh.opendns.com
  - acl doh dstdomain dns.quad9.net
  - acl doh dstdomain public.dns.iij.jp
  - http_access allow doh CONNECT SSL_ports all
  - http_access deny all
- 今回は自宅で動かしたものを使用 / 都内

Copyright © 2021 Japan Registry Services Co., Ltd.

Evaluation of DoH over HTTP proxy (1)

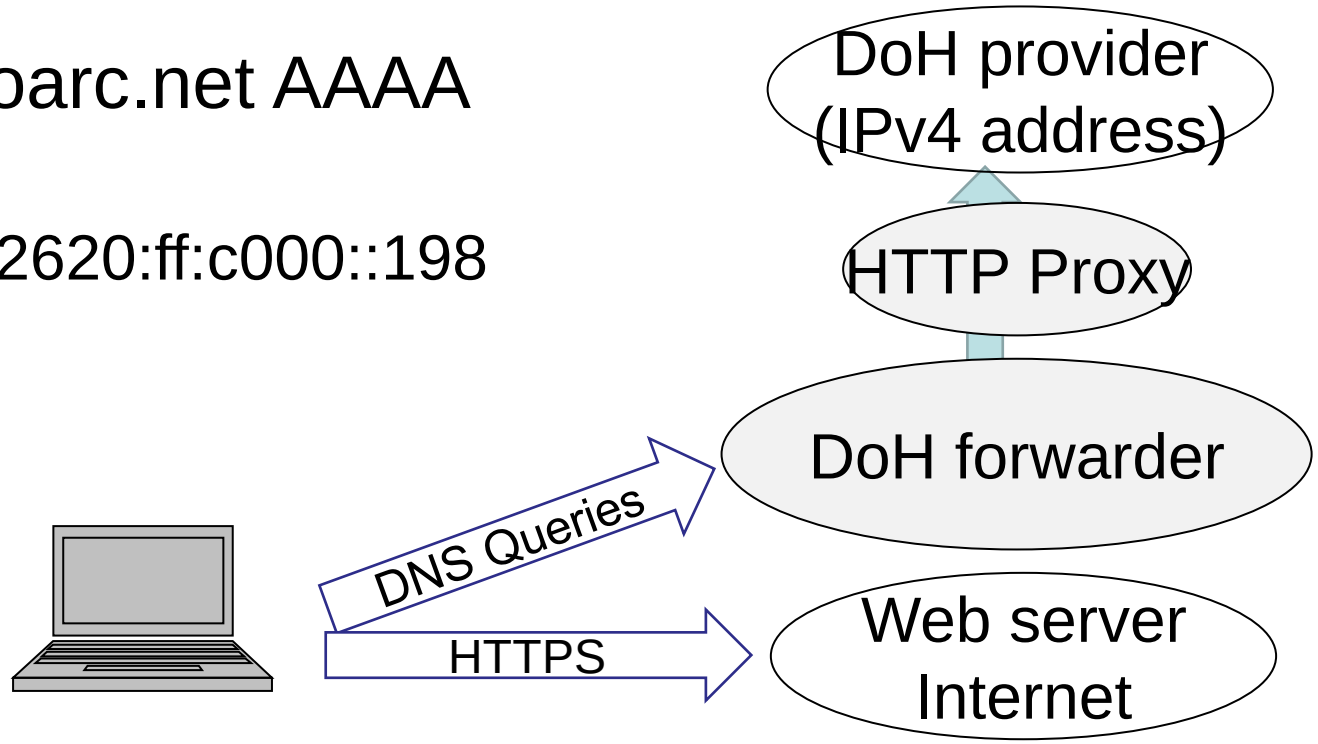
- Start special DoH forwarder
  - perl DNSforwarder.pl -u 203.178.129.11/53 -H https://cloudflare-dns.com/dns-query -P proxyaddr/port
  - DoH forwarder's listen address is 203.178.129.11 port 53
    - DoH server address is https://cloudflare-dns.com/dns-query
    - cloudflare-dns.com:443への接続に、HTTP Proxyを使用

Copyright © 2021 Japan Registry Services Co., Ltd.

Evaluation of DoH over HTTP proxy (2)

- dig @DoHforwarder id.server CH TXT
  - ;; ANSWER SECTION:
  - id.server. 1 CH TXT “NRT"
    Cloudflare’s Tokyo node
  - ;; Query time: 171 msec
- dig @DoHforwarder www.dns-oarc.net AAAA
  - ;; ANSWER SECTION:
  - www.dns-oarc.net. 120 IN AAAA 2620:ff:c000::198
  - ;; Query time: 173 msec

  - 都内のproxyでも、遅延大きめだが
  - これぐらいの遅延なら使える



Copyright © 2021 Japan Registry Services Co., Ltd.

DoH over CGN/NAT64/proxyの問題点

- CDNの経路制御を無効化
- DoH providers can track by using TLS session information
  - TLS pinning とかの最適化すると足がつく可能性あり
  - 毎回TLSを切ってつなぎなおす
- Public NAT64 services are located in Europe only
  - High latency (1 second !) from Japan
    - because UDP RTT is 238ms
  - 手元のISPがNAT64を提供していれば使用可能
    - だけどISPの情報まではDoHプロバイダにばれる

Copyright © 2021 Japan Registry Services Co., Ltd.

Conclusion

- DoH providers は、query source IP addresses と DNS queries を知ることができる
  - Privacy情報: だれ(IPアドレス)が、いつ、何を問い合わせたか
- privacyを守るには既存のツールで source IP address を隠せばいい
  - DoH over CGN with low priced MVNO SIM: 金かかるけど使える
  - DoH over NAT64: European region と WIDE Internet では使える
  - DoH over open HTTP(S) proxies (or Tor): 動くけど、
    - だれか複数のDoHサーバにつなげられるsquidを提供してください
- Any questions and suggestions ?

Copyright © 2021 Japan Registry Services Co., Ltd.