public DNSとプライバシー

2020/01/23

JANOG45

山口崇徳@iij

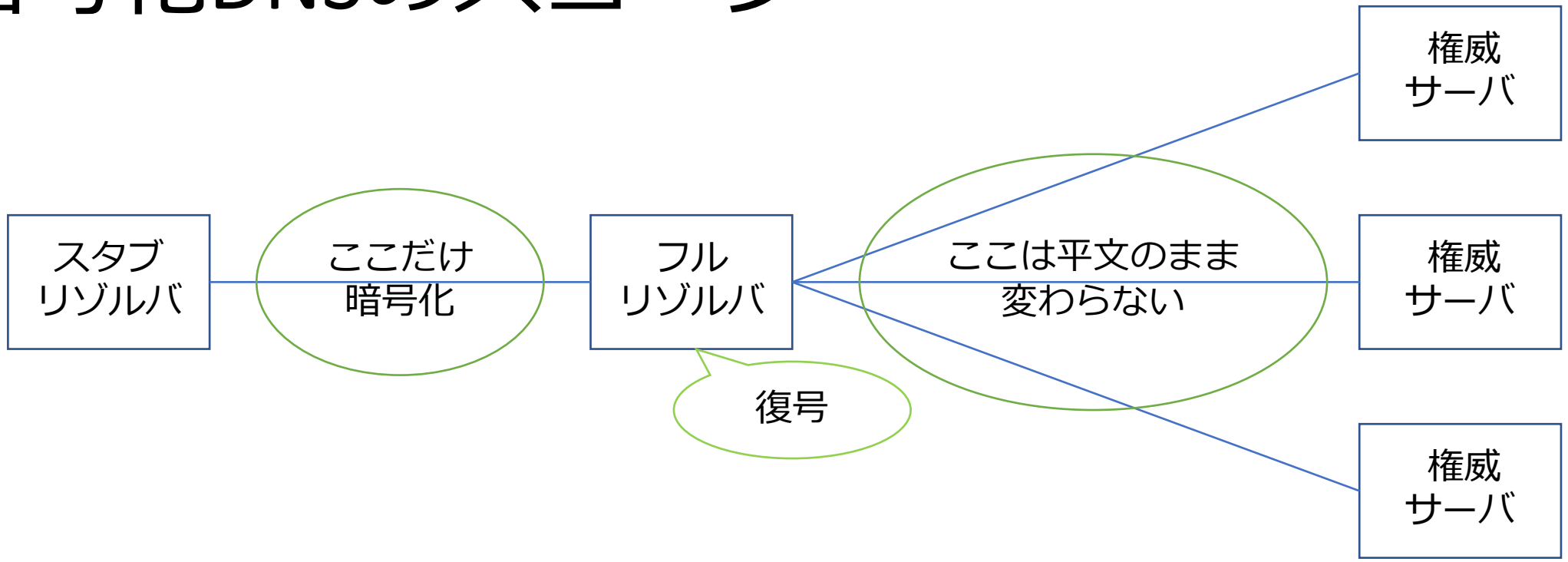
agenda

- 技術的なことや、そこから想定される懸念について(山口)
- それに対してどう考えるか、ISPの立場から(石田)
- public dnsサービス提供者、ブラウザ開発者の立場から(Kenji)
- ディスカッション

DNSとプライバシー

- 昔: DNSは公開情報
  - 盗聴されないことよりも改竄されないことを重視
  - 完全性の保証 ⇒ DNSSEC
- スノーデン事件(2013)
  - DNSに関しても広範に監視がおこなわれていたことが発覚
  - RFC7258 Pervasive Monitoring is an Attack
- 公開情報とはいえ、どんな情報を欲しがっているのかは個人のプライバシー
  - 「盗聴されないこと」も考慮しないといけないのでは?
  - 機密性の保証 ⇒ DNS over HTTPS (DoH) / DNS over TLS (DoT)

暗号化DNSのスコープ



- DoH/DoTはスタブ – フルリゾルバ間の機密性を保証する
  - (DNSSECなしなら)フルリゾルバの持つ情報が正しいという保証がない
  - 一般にTLSは完全性も保証するが、権威まで含めたDNSの系全体で考えればDoH/DoTに完全性があるとはいえない

DNSSEC vs DoH/DoT

- DNSSEC = DNS SECurity extensions
  - 一言でいうと、「電子署名つき DNS」
  - 暗号化しない = 機密性なし
- スコープが異なる
  - DNSSEC ⇒ 完全性の保証、否認防止
  - DoH/DoT ⇒ 機密性の保証
- DNSSEC が守るもの ≠ DoH/DoT が守るもの
  - DoH/DoT があるから DNSSEC なんかいらない、とはならない(vice versa)

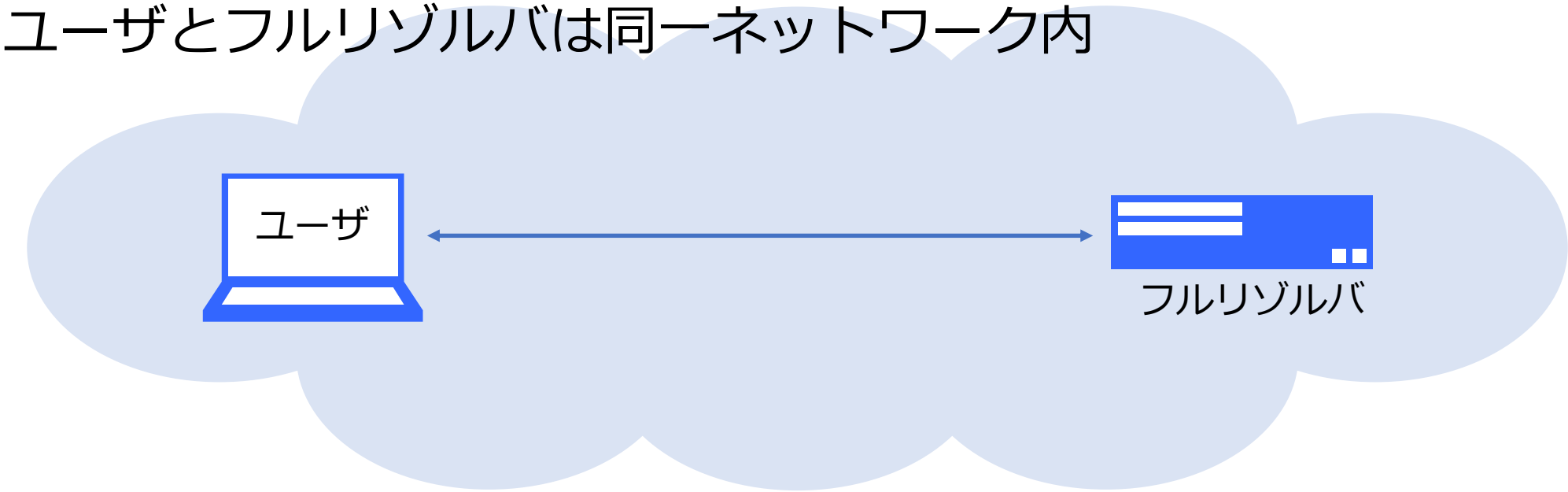
主なpublic DNS

	サービス開始	備考
Google Public DNS (8.8.8.8)	2009/12	EDNS Client Subnet対応
Quad9 (9.9.9.9)	2017/11	
CloudFlare (1.1.1.1)	2018/04	
IIJ Public DNS (public.dns.iij.jp)	2019/05	平文非対応

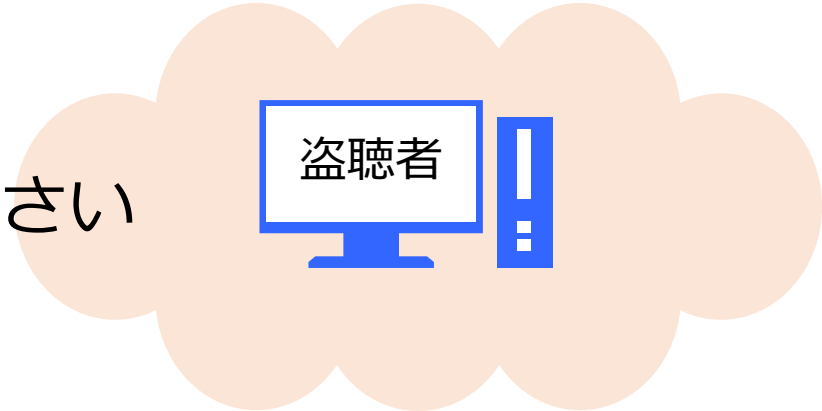
- 表中のサービスはいずれも DoH/DoT/DNSSEC 対応
- 他にOpenDNS、 CleanBrowsing、 Quad 101 (TWNIC)、 NextDNS など

ISPのフルリゾルバ

- ユーザとフルリゾルバは同一ネットワーク内

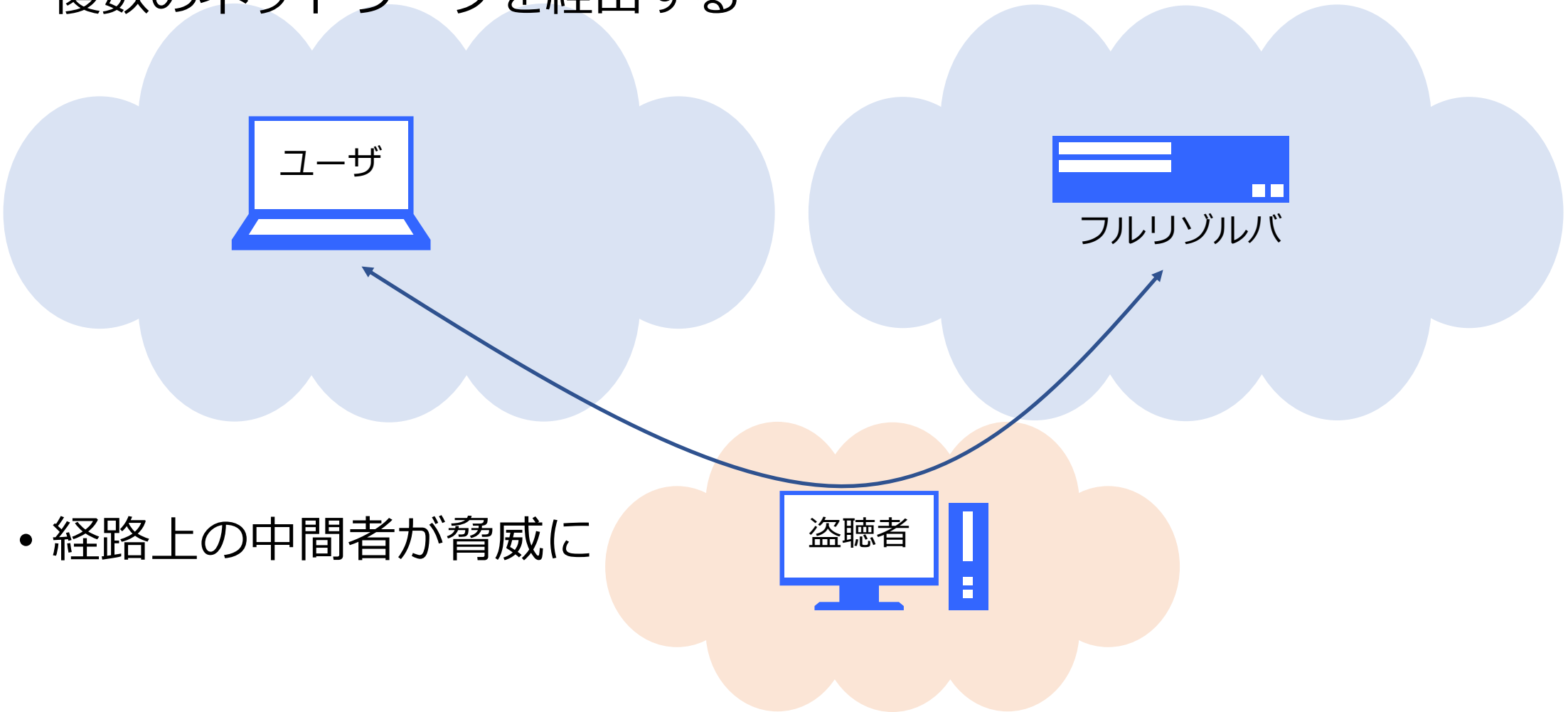


- 中間者攻撃は困難
- 平文でも盗聴の危険は小さい



public DNS

- 複数のネットワークを経由する



- 経路上の中間者が脅威に

平文DNSは危険なのか?

- ISPで自動設定されるフルリゾルバを使うのであれば、従来の平文DNSでも盗聴の危険は小さい
  - ISPのネットワークに入る手前で盗聴される可能性はある
    - ユーザ宅内のwifi区間など
- public DNSを使うのであれば、平文DNSは安全ではない
  - 対応していれば、DoH/DoTを推奨
- 公衆wifiで自動設定されるフルリゾルバは?
  - うーん……?

https://twitter.com/bgpstream/status/1193995948281737216

DoH/DoTのユースケース

- 自動設定されるフルリゾルバが信頼できないとき、かわりに public DNSを利用する
  - 公衆wifiとかホテルの客室インターネットとか
  - フルリゾルバが意に反するブロッキングをやってるとか
- public DNSへの途中経路での中間者攻撃を回避 → DoH/DoT
  - ISPのフルリゾルバがほとんど対応していない現時点では、DoH/DoTはほぼpublic DNS専用プロトコル

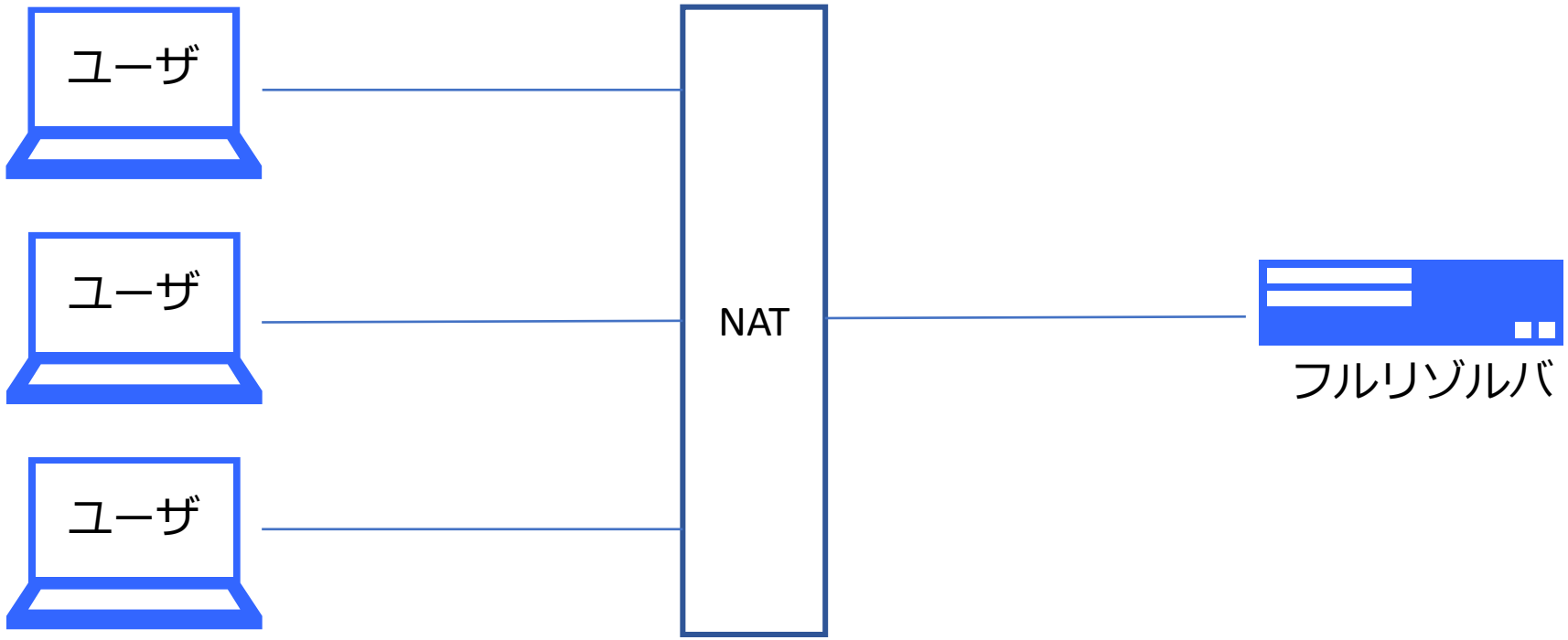
ISPでもDoH/DoTやればいいんじゃないの?

- IIJは提供開始しましたがそれはそれとして…
  - https://www.iij.ad.jp/news/pressrelease/2020/0116-2.html

- 現状ではDoH/DoTにauto configurationの仕組みが存在しない
  - ISPがDoH/DoTに対応しても、ユーザが使うための設定を配布できない
  - 情報が少ないローカルISPと世界的超大手のpublic DNS、どちらを使うにしても手動設定が必要で、どちらも無料なら、後者の方が選ばれやすい(だろう)

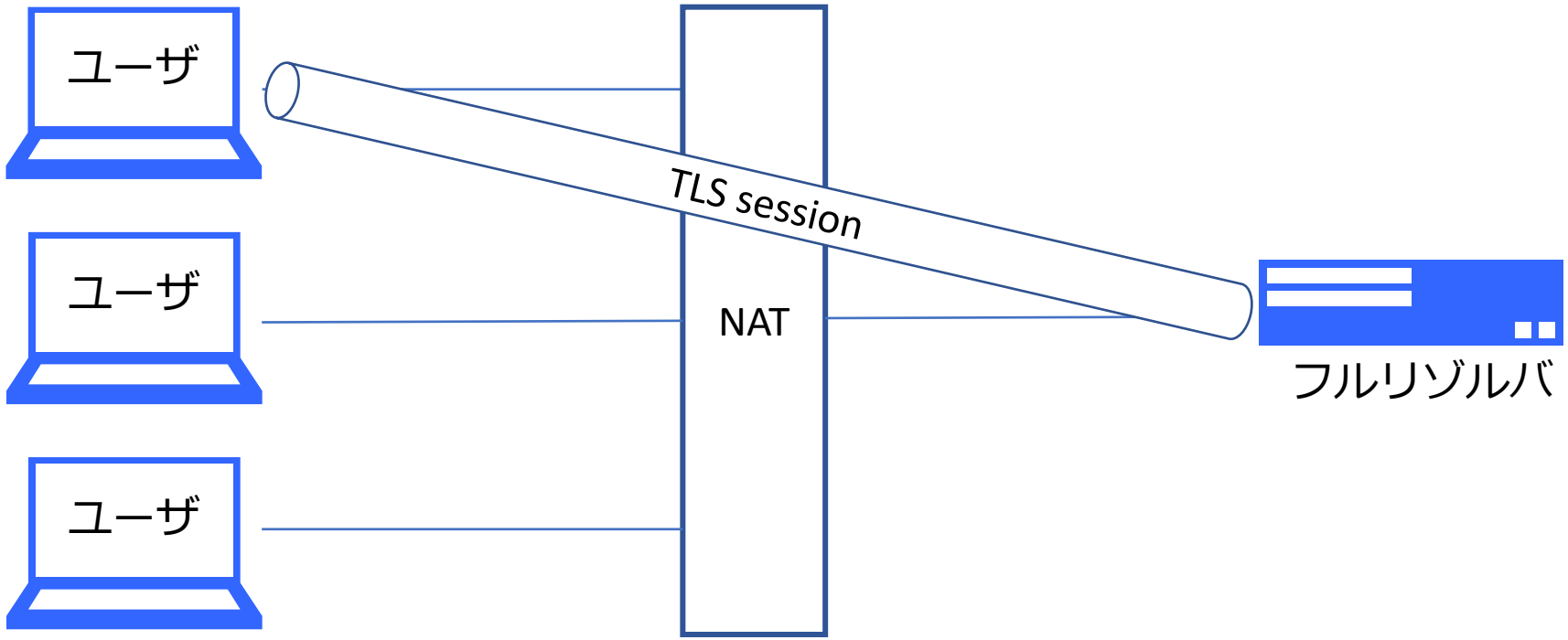
従来のDNSでユーザトラッキング

- ユーザを区別できる情報はIPアドレスだけ
  - NATの向こう側にいるユーザを区別できない



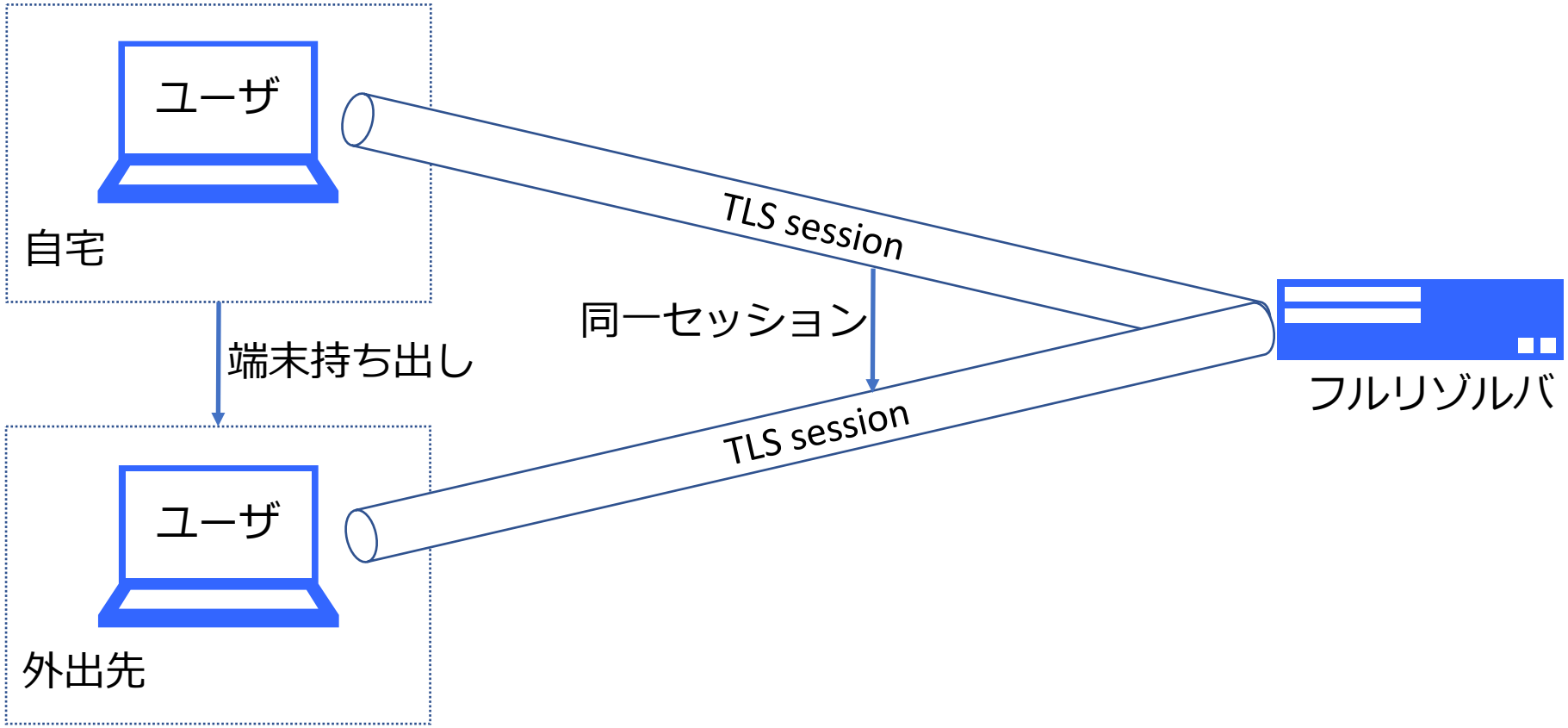
DoH/DoTでユーザトラッキング (1)

- TLSはセッションを持つ
  - NATの向こう側にいるユーザを区別できる



DoH/DoTでユーザトラッキング (2)

- TLSは終了したセッションを再開できる(resumption)
  - IPアドレスが変わってもTLSセッションからユーザの紐づけが可能



DoH/DoTでユーザトラッキング (3)

- DoHではHTTPヘッダから利用環境やユーザの情報を推測できる
  - user-agent: ブラウザ情報
  - accept-language: 言語
- クライアントはcookieを送るべきではない(SHOULD NOT)とされている(RFC8484)
  - が、MUST NOTではない
- フルリゾルバの得られるユーザに関する情報は、平文より暗号化した方がむしろ増える

そもそもフルリゾルバは信頼できるのか?

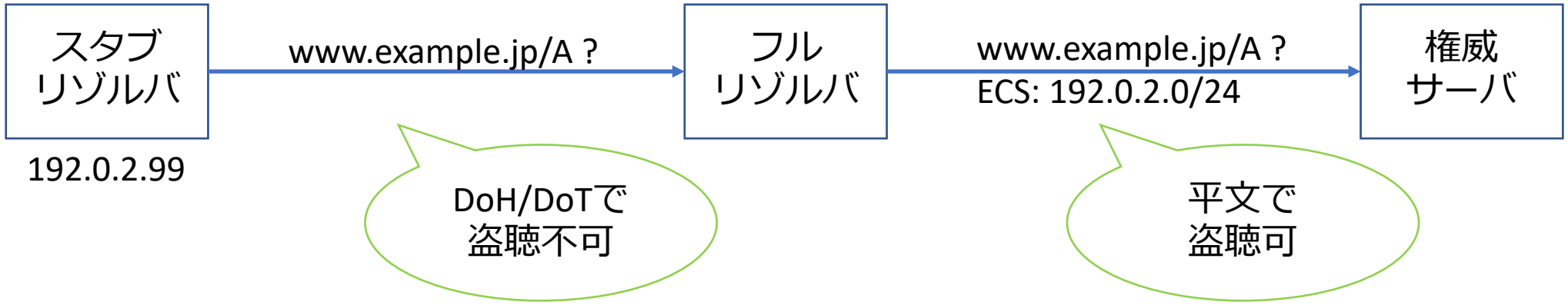
- DoH/DoTでもキャッシュされた情報の正しさは担保できない
  - 担保するにはDNSSECが必要だがほとんど使われていない
- ○○○や×××なことをしちゃうようなフルリゾルバとか
  - 応答を勝手に書き換えるとか
  - クエリ情報を広告屋や国家権力に提供するとか
  - 法的・道徳的・商慣習的な制限はともかく、技術的には可能
- DoH/DoTを使えば○○○や×××ができなくなる、わけではない
  - 暗号化は中間者攻撃対策だが、フルリゾルバは中間者ではない
  - フルリゾルバ自身が○○○や×××することには無力

public DNSがやってる○○○や×××

- Google
  - EDNS Client Subnet で権威サーバにクライアントのIPアドレスを通知
    - 平文なので第三者から盗聴されうる
- Quad9
  - マルウェア配布ドメインのブロッキング
  - ブロッキングに必要な情報収集のために外部ベンダーにクエリ情報を提供
- IIJ
  - 児童ポルノブロッキング
- Cloudflare
  - とくになし

EDNS Client Subnet

- CDN事業者がユーザに最も近いエッジノードからコンテンツを配信できるようにするためのDNS拡張(RFC7871)
  - フルリゾルバから権威サーバへのクエリにクライアントのIPアドレス(を/24程度に丸めたもの)を拡張情報として追加
  - 権威サーバはそれを参考に適切な配信サーバを応答する
  - 参考: https://www.janog.gr.jp/meeting/janog38/program/edns.html



public DNSとプライバシー (1)

- 暗号化DNSにより経路上の監視者による盗聴の危険が減る
  - 権力による監視・検閲からの回避
  - マルウェアにとっても活動が隠蔽されて都合がいい

- フルリゾルバはすべてのクエリを知ることができる
  - 暗号化されていても復号できる
  - 暗号化されていると平文DNSよりかえってユーザの情報を入手しやすい
  - 暗号化されていても応答の書き換えやクエリの別用途への利用は(やろうと思えば)可能

public DNSとプライバシー (2)

- 膨大なプライバシーがpublic DNS事業者の手元に
  - DoH/DoTは現状ではほぼpublic DNS専用プロトコル
  - DoH/DoTの普及 ≒ public DNSへの集中化・寡占化

- public DNSに集積されたプライバシーは捨てられるのか活用されるのか? 漏洩の懸念は?
  - ほとんどのpublic DNSは日本の事業者ではない
  - 日本では法制度上できないことでも、海外ではできる(かもしれない)
  - プライバシーポリシーを信じるしかない?