

資料更新：2019/01/25

# 運用の視点から (ISP) ZEROから考えるインターネット運用とブロッキング

2019年1月25日  
JANOG43@Yamanashi

株式会社QTnet  
技術本部 サービスオペレーションセンター

末松慶文 (yo\_suematsu at qtnet.co.jp)

# 自己紹介

- 末松慶文(すえまつ よしぶみ)
- 株式会社QTnet ,DNSOPS.JP幹事
  - DNSを含むサーバ関連の構築と運用/保守などを十数年くらい。
- DNSの耐障害性強化に向けてJPRSと共同研究を開始 (2015年7月13日)
  - JPRS: JPRSが新gTLD「.jprs」でDNSの耐障害性強化に向けてISPとの共同研究を開始 <http://jprs.co.jp/press/2015/150713.html>
  - QTNet: JPRSとの共同研究について <https://www.qtnet.co.jp/info/2016/20160118.html>
- JPRSおよび電力系通信事業者8社が共同研究の成果を公開
  - [https://www.qtnet.co.jp/info/2017/20171031\\_1.html](https://www.qtnet.co.jp/info/2017/20171031_1.html)
  - <https://tldlabs.jprs/acts/s001/>
- APRICOT 2017 TLD Anycast DNS servers to ISPs (JPRS, QTnet)
  - <https://2017.apricot.net/program/schedule/#/day/9/network-operations-2>

どのような局面においても名前解決を継続的に提供し続けたい！

- おことわり

法律の専門家ではありません。

個人の見解であり、所属する組織の見解を示すものではありません。

# ブロッキングとフィルタリング

## ■ ブロッキングとは

ユーザがウェブサイト等を閲覧しようとする場合に、当該ユーザにインターネットアクセスを提供するISP等が、ユーザの同意を得ることなく、ユーザがアクセスしようとするウェブサイト等のホスト名、IPアドレス ないしURLを検知し、そのアクセスを遮断する措置をいう。

ブロッキングの法律問題

[https://www.kantei.go.jp/jp/singi/titeki2/tyousakai/kensho\\_hyoka\\_kikaku/2018/contents/dai3/siryou3.pdf](https://www.kantei.go.jp/jp/singi/titeki2/tyousakai/kensho_hyoka_kikaku/2018/contents/dai3/siryou3.pdf)

※ユーザの同意を得て行う場合はフィルタリングと呼ぶことが多い

## ■ 様々なブロッキング、フィルタリング

- ・ 海賊版サイトブロッキング
- ・ 児童ポルノブロッキング
- ・ 子供向け、コンテンツフィルタリング

# ブロッキングの手法とその特徴

## ■ ISP視点でのブロッキングの手法

### ・ DNSブロッキング

- 今回はこちらの話

### ・ DPIによるブロッキング

- 高精度にブロッキング可?、装置が高価

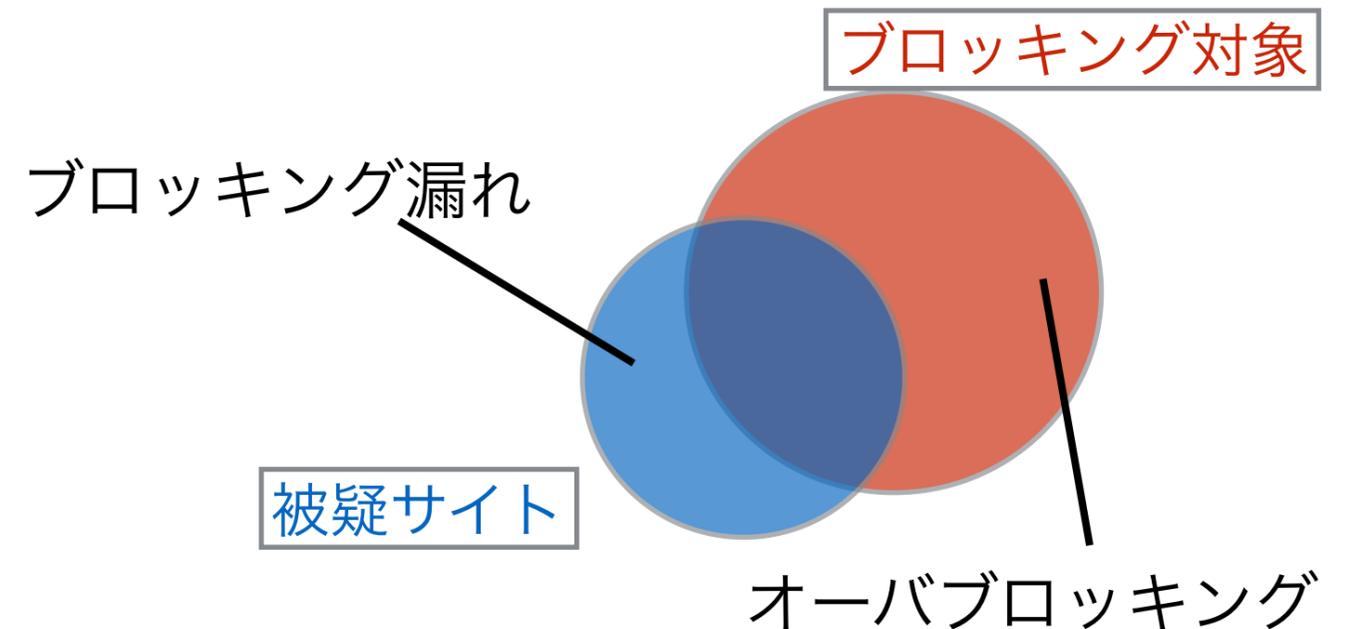
### ・ IPアドレスによるブロッキング

- バーチャルホスト利用の場合、オーバブロッキングの可能性大

## ■ その他のブロッキング手法

### ・ 検索エンジンからの除外

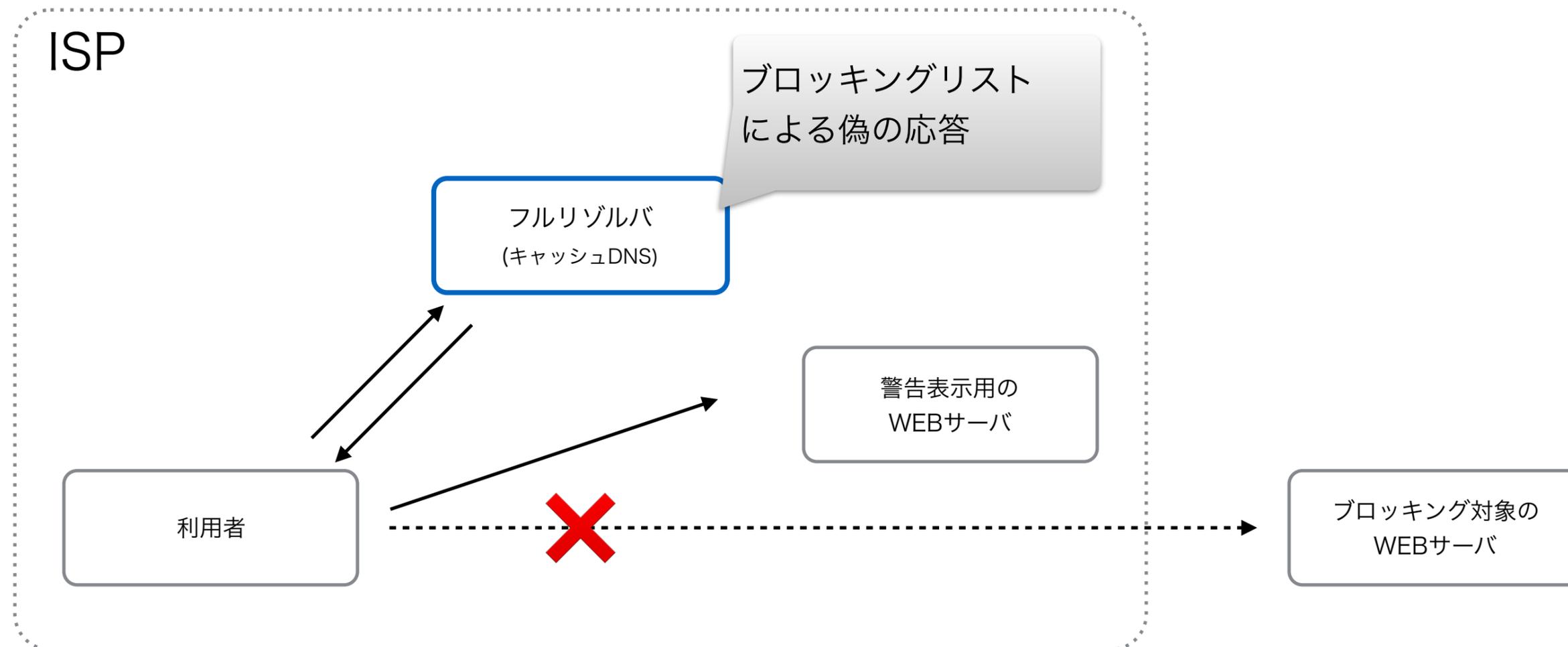
- 検索エンジン経由ではなく、URLを指定すればアクセス可能



# DNSブロッキング

## ■ DNSブロッキングとは

### ・動作概要



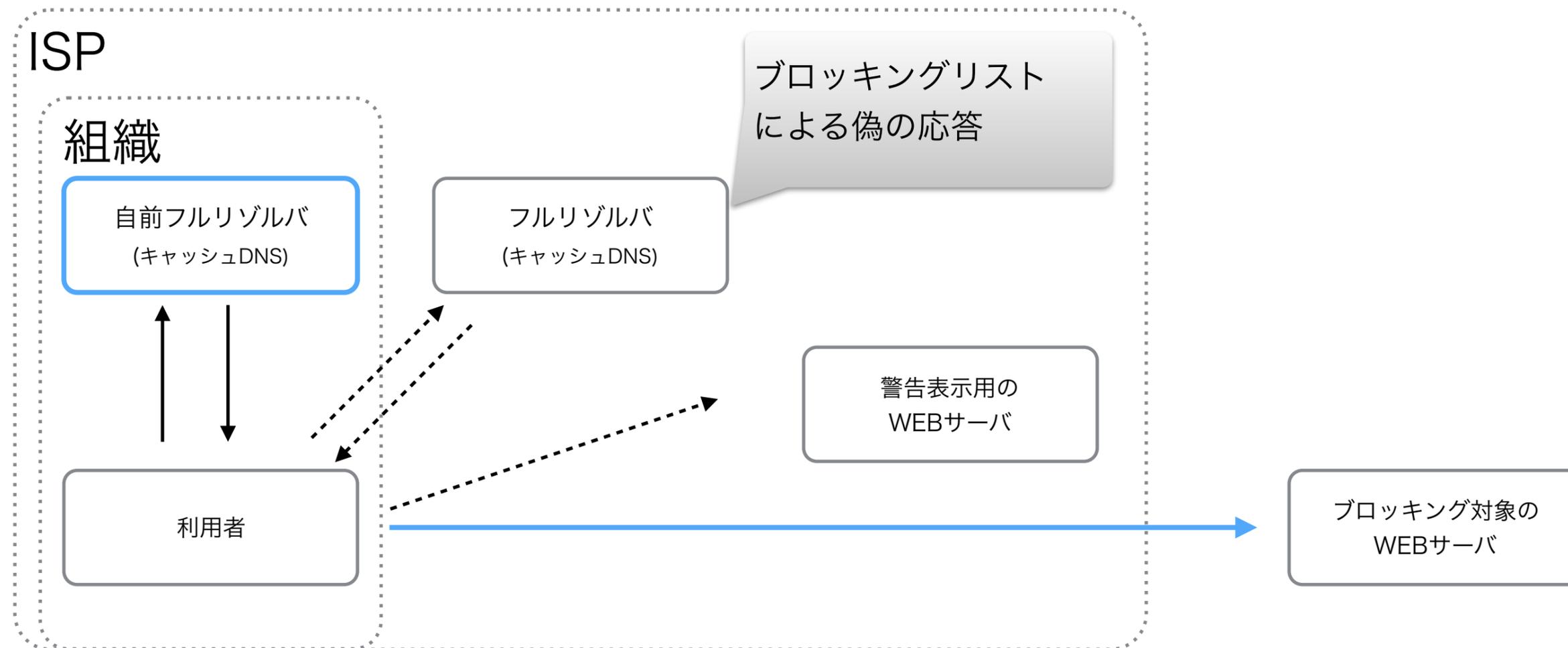
### ・実装について

- 児童ポルノブロッキングと同様の方法でいけそう。
- ブロッキングリストを取得/反映させる仕組みも

どのような形でリストが配布されるのかわかりませんが・・・

# DNSブロッキングの実効性について

- 自前フルリゾルバとDNSブロッキングの関係

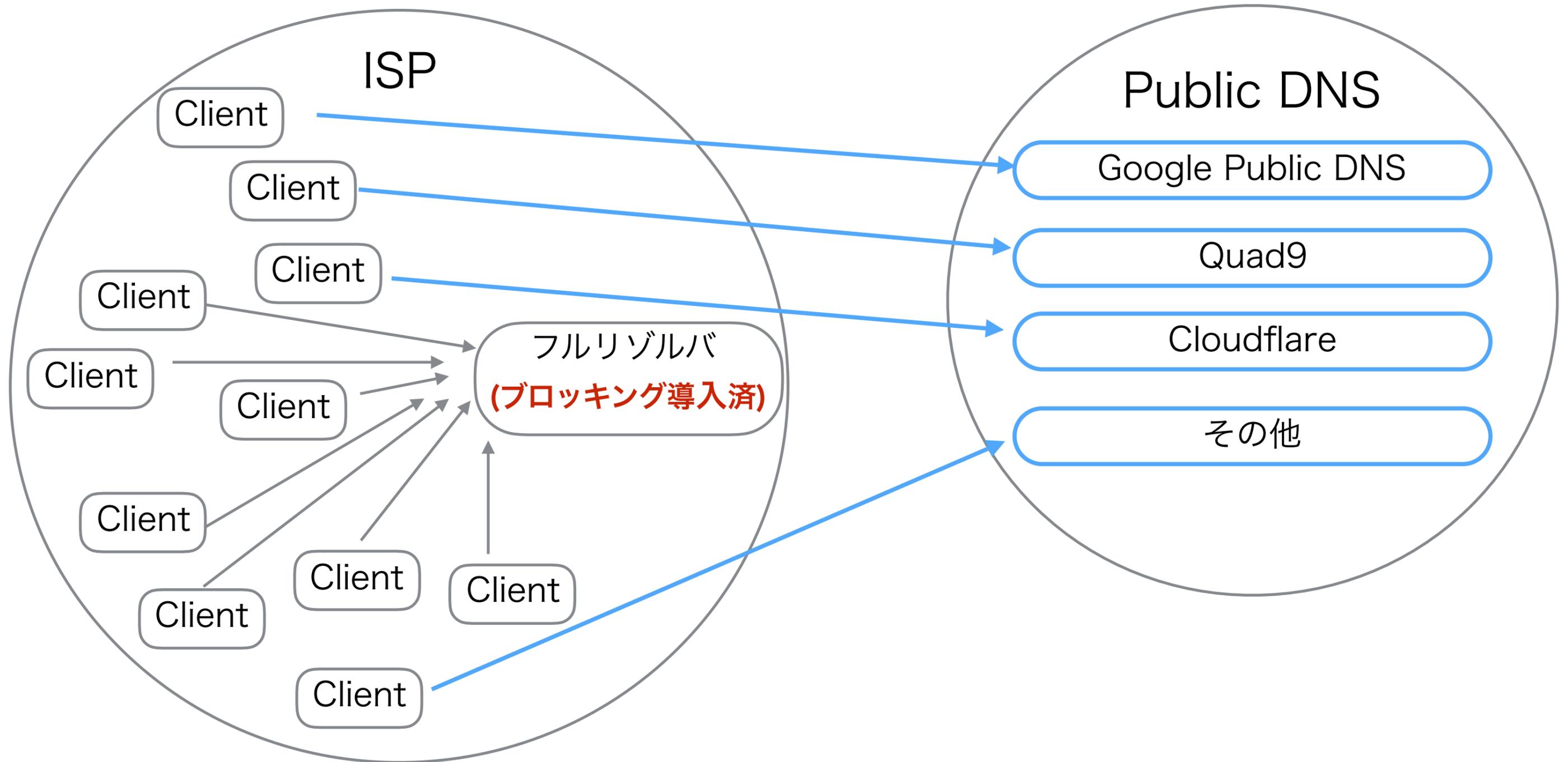


自前のフルリゾルバ利用者はDNSブロッキングの影響を受けない

・つまり抜け道になりうる。

# DNSブロッキングの実効性について

- Public DNSとDNSブロッキングの関係

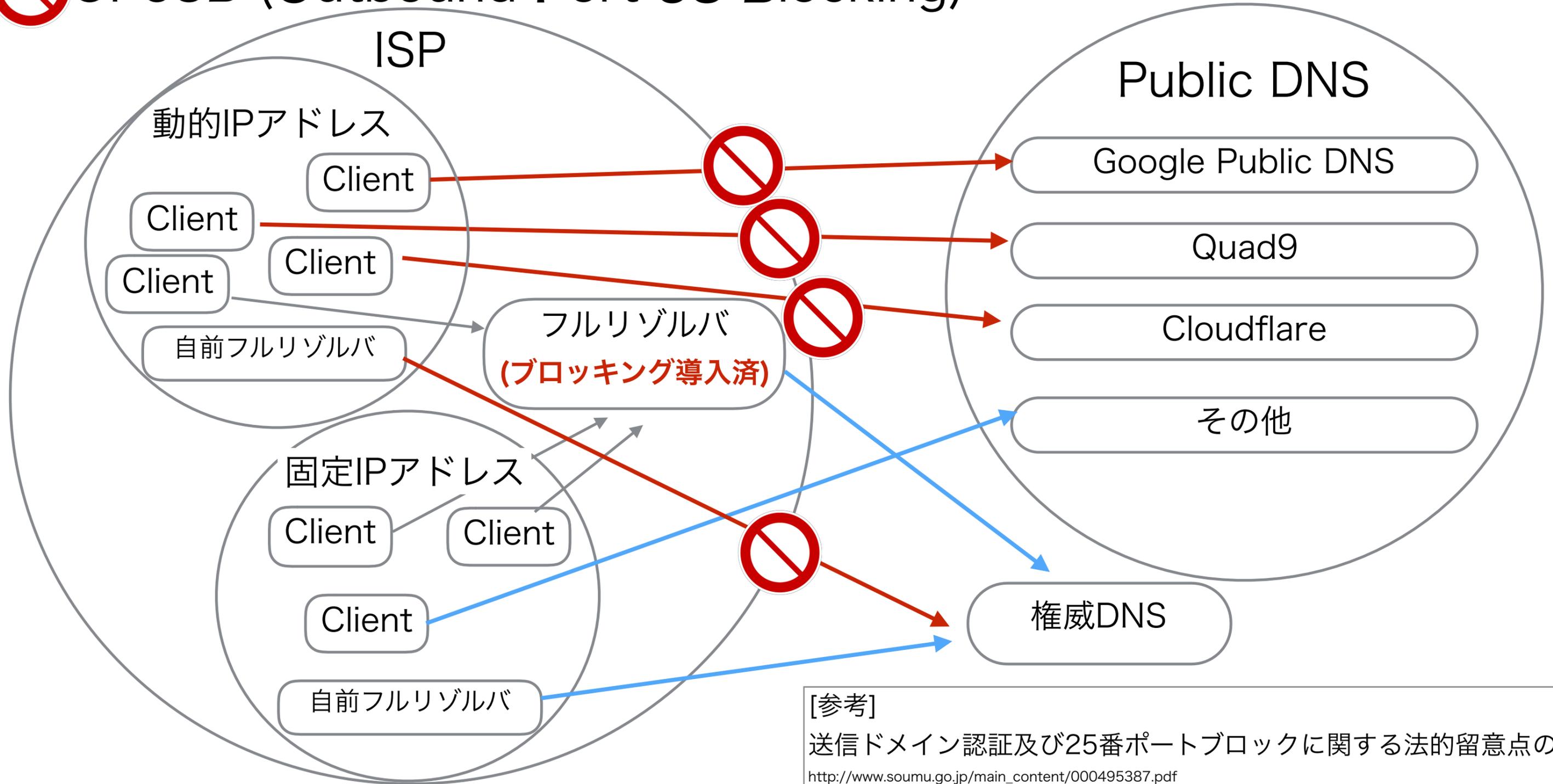


Public DNSの利用はDNSブロッキングの抜け道に...

DNSのブロッキングに実効性は・・・  
ある？/ない？

# 抜け道を塞ぐために (OP53B)

## OP53B (Outbound Port 53 Blocking)

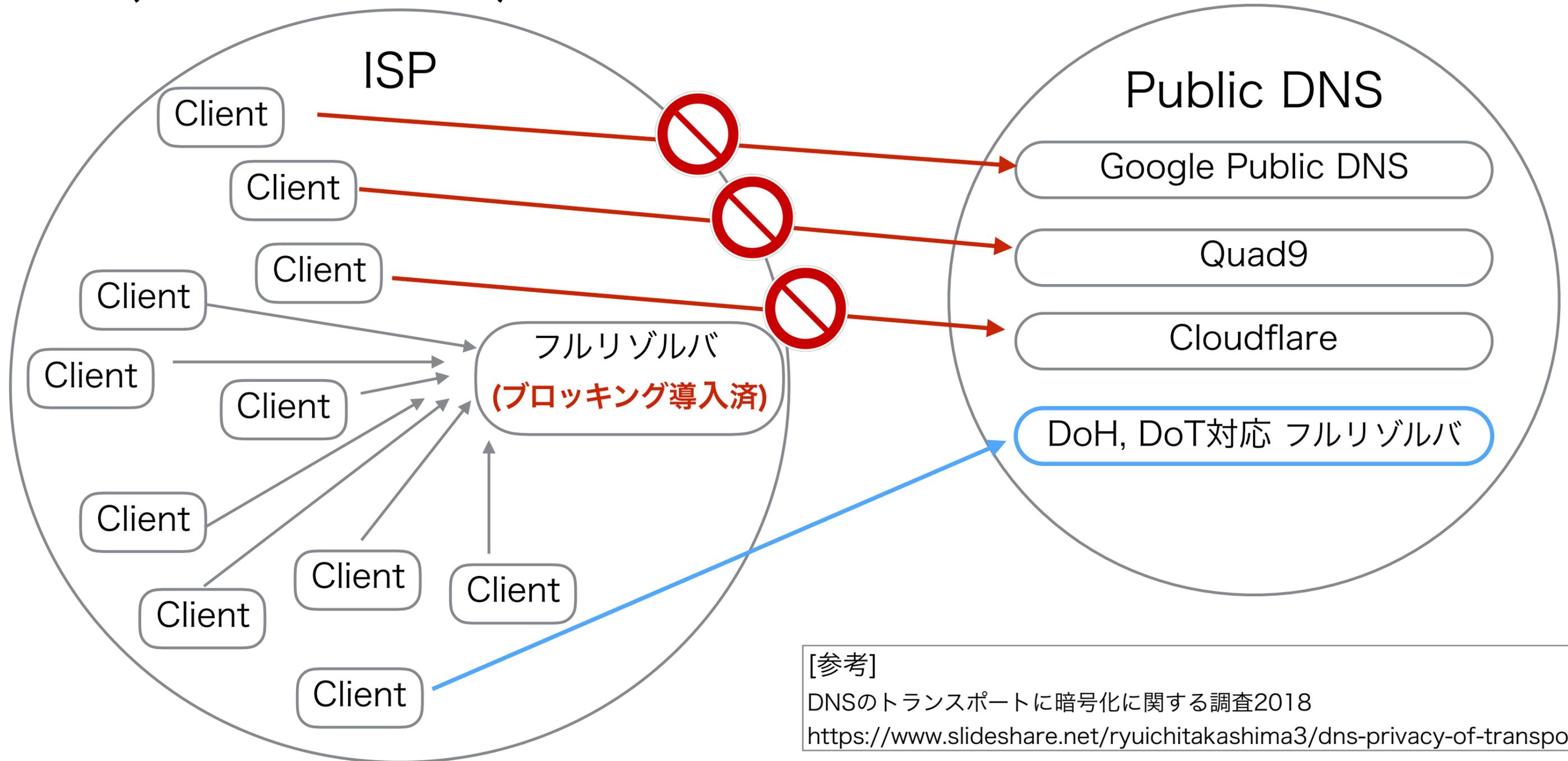


法的な問題は？

# OP53Bの回避(DoH, DoT)

- DoH (DNS over HTTPS)
- DoT (DNS over TLS)

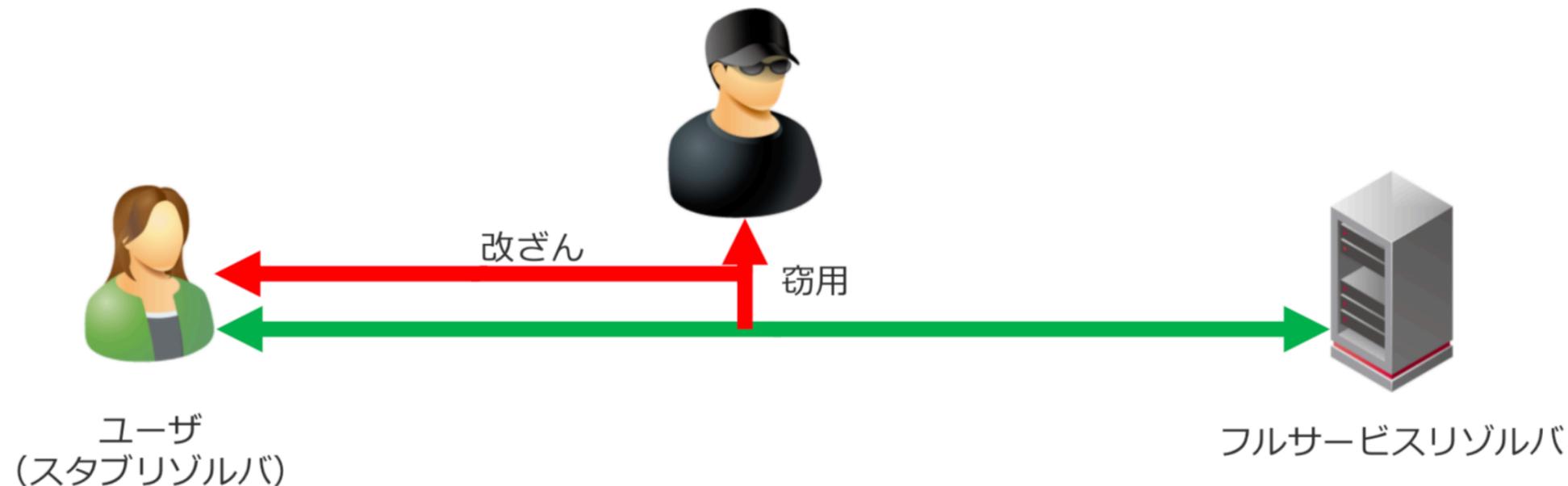
 OP53B



[参考]  
 DNSのトランスポートに暗号化に関する調査2018  
<https://www.slideshare.net/ryuichitakashima3/dns-privacy-of-transport-layer>

なぜ暗号化するようになったのか

スタブリゾルバとフルリゾルバ間をMITMしてクエリーの窃用や改ざんが行われていることがあります。特に海外では国家ぐるみで行われることもあります。これらの問題を**プライバシー侵害**の問題と捉え、DNSの通信を暗号化することで、これらを守ろうとしています。



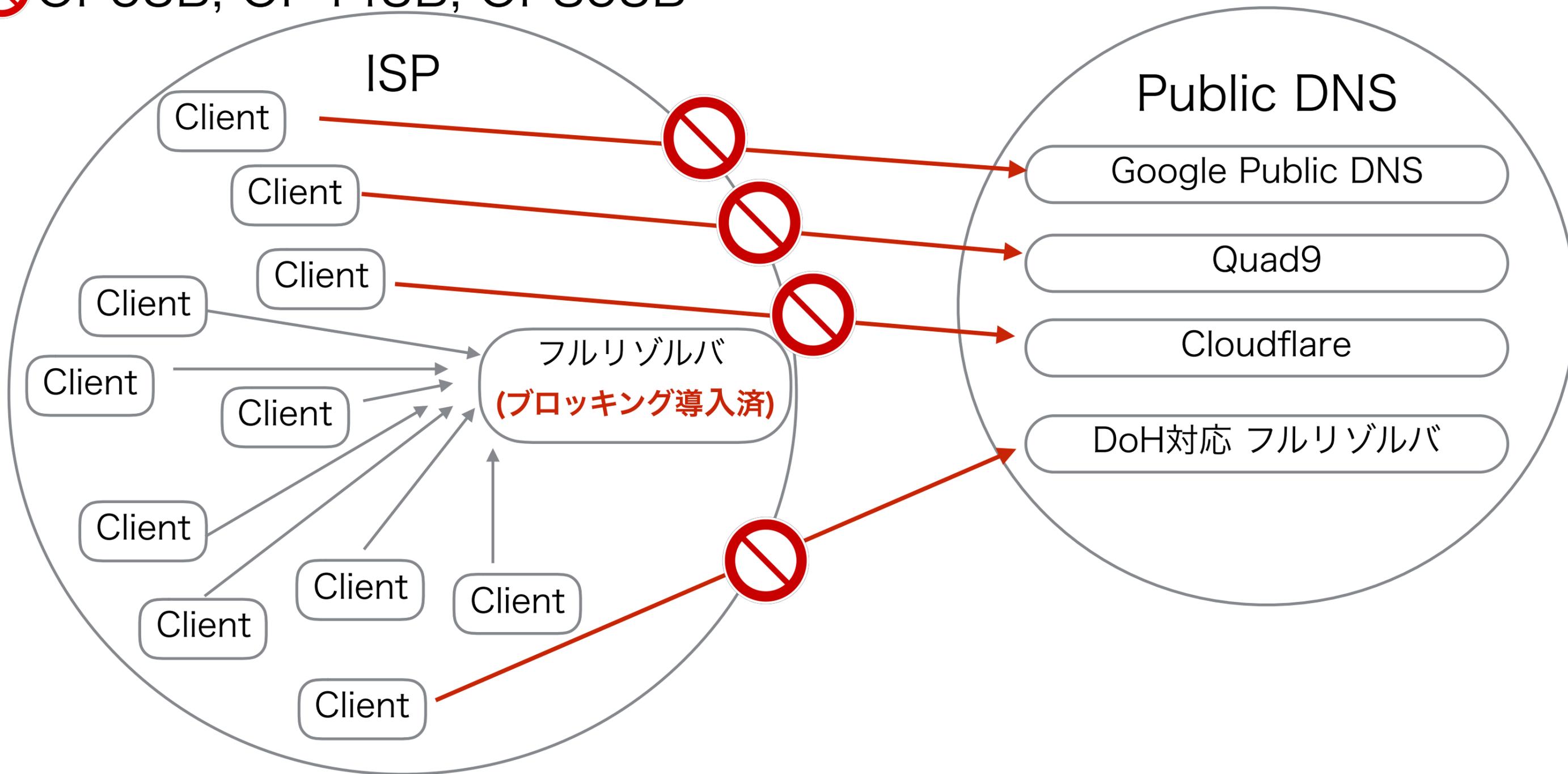
QUNOG12 DNS暗号化(IIJ 其田)

[https://www.kantei.go.jp/jp/singi/titeki2/tyousakai/kensho\\_hyoka\\_kikaku/2018/contents/dai3/siryous3.pdf](https://www.kantei.go.jp/jp/singi/titeki2/tyousakai/kensho_hyoka_kikaku/2018/contents/dai3/siryous3.pdf)

海賊版サイトブロッキングの回避を目的とした技術ではない

# 抜け道を塞ぐために (OP53B, OP853B, OP443B)

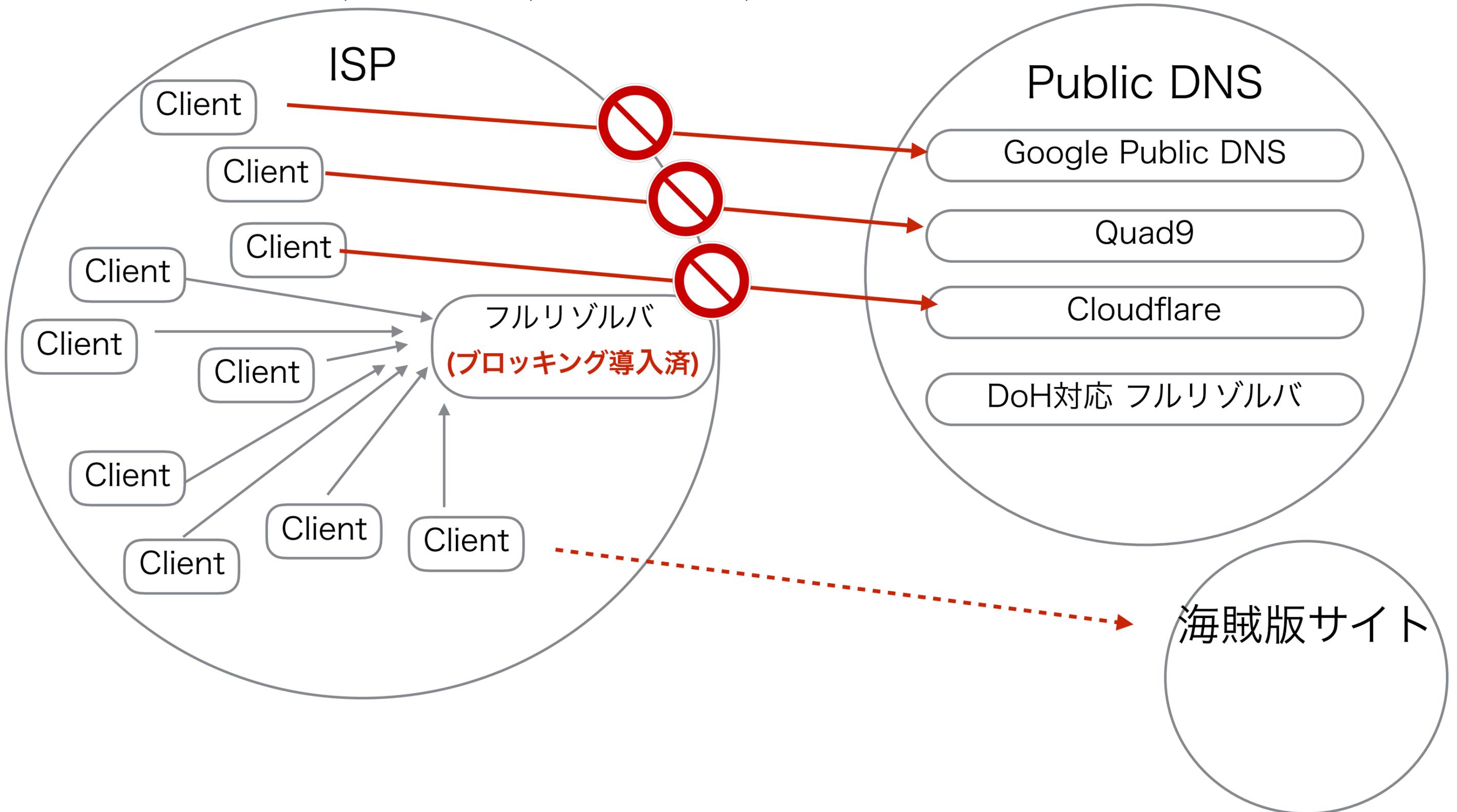
- ❌ OP53B, OP443B, OP853B



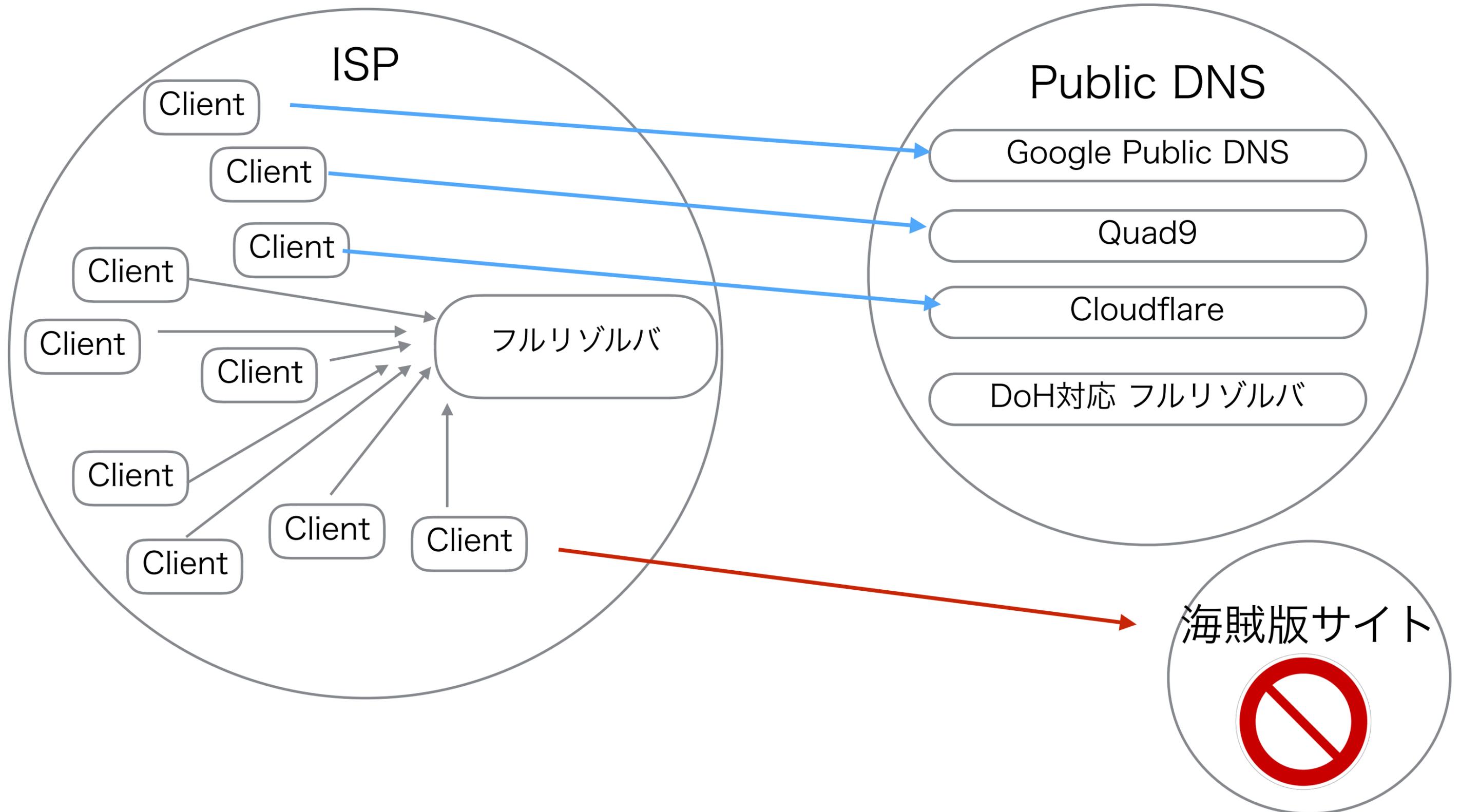
いたちごっこ、ブロッキングの連鎖

# ISP側でブロッキングせずとも . . .

- DNSブロッキング, OP53B, OP443B, OP853B

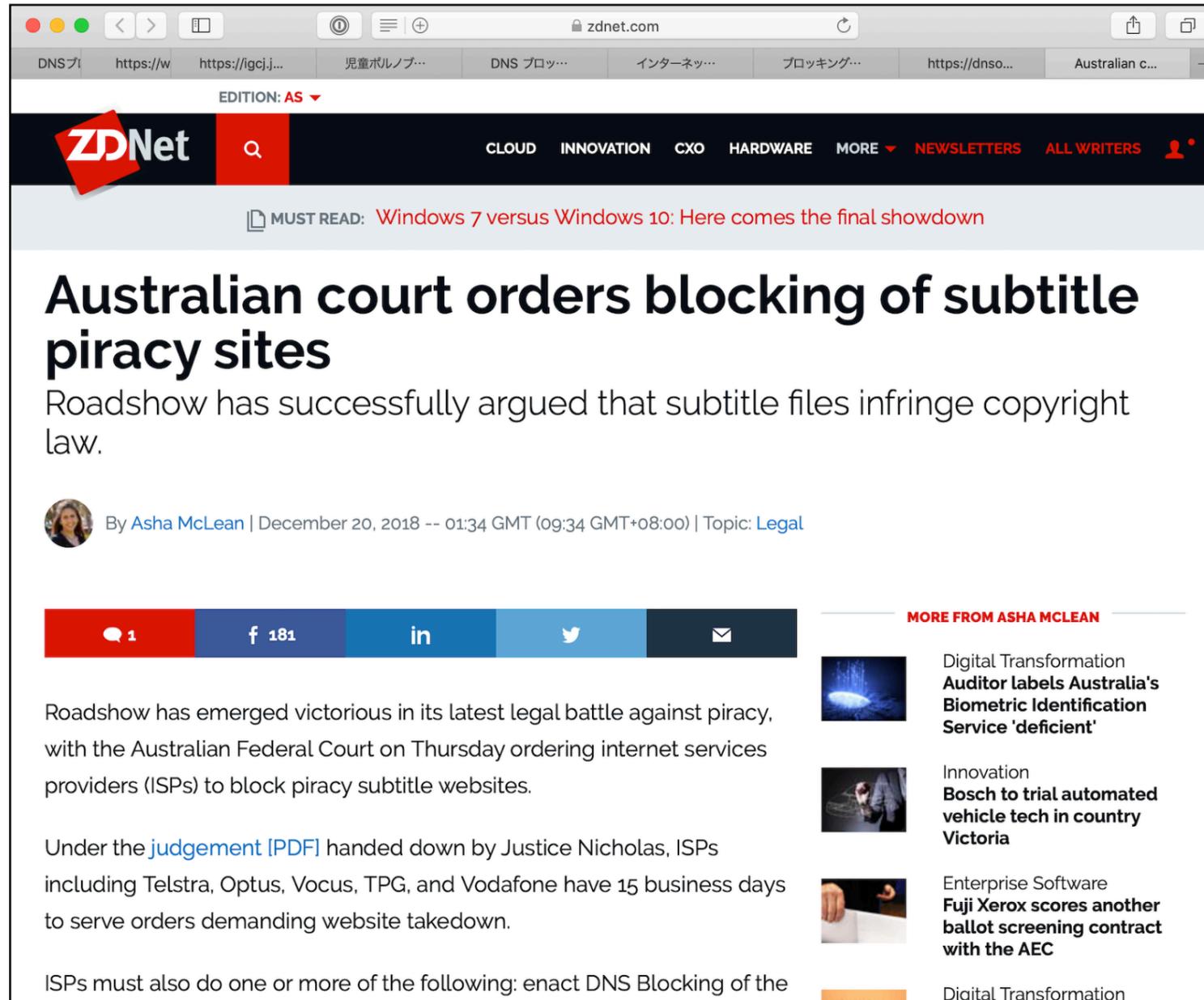


# ISP側でブロッキングせずとも . . .



# 海外では・・・

## ■ オーストラリアでの実例



- ・ 裁判所がISPにブロッキングを命じる判決
  - ・ 原告にブロッキングに関わる費用を負担せよと命令(1ドメイン名あたり50AUドル)
- 約3900円  
岡田さん補足・・・あれば。

# ディスカッション

- ISPの運用に関わる課題
  - ・ 設備・運用コスト(リストの更新/オーバブロック/カスタマー対応)
  - ・ 訴訟リスク(通信の秘密の侵害)
  - ・ オペレータ(個人)が刑事罰に問われる可能性 (未遂も・・・)
  
- その他の課題
  - ・ 検閲にあたらないか
    - 対象サイトの選定も民間主導でされるべきでは?
  - ・ インターネットの完全性、中立性、柔軟性
  - ・ 域外適用