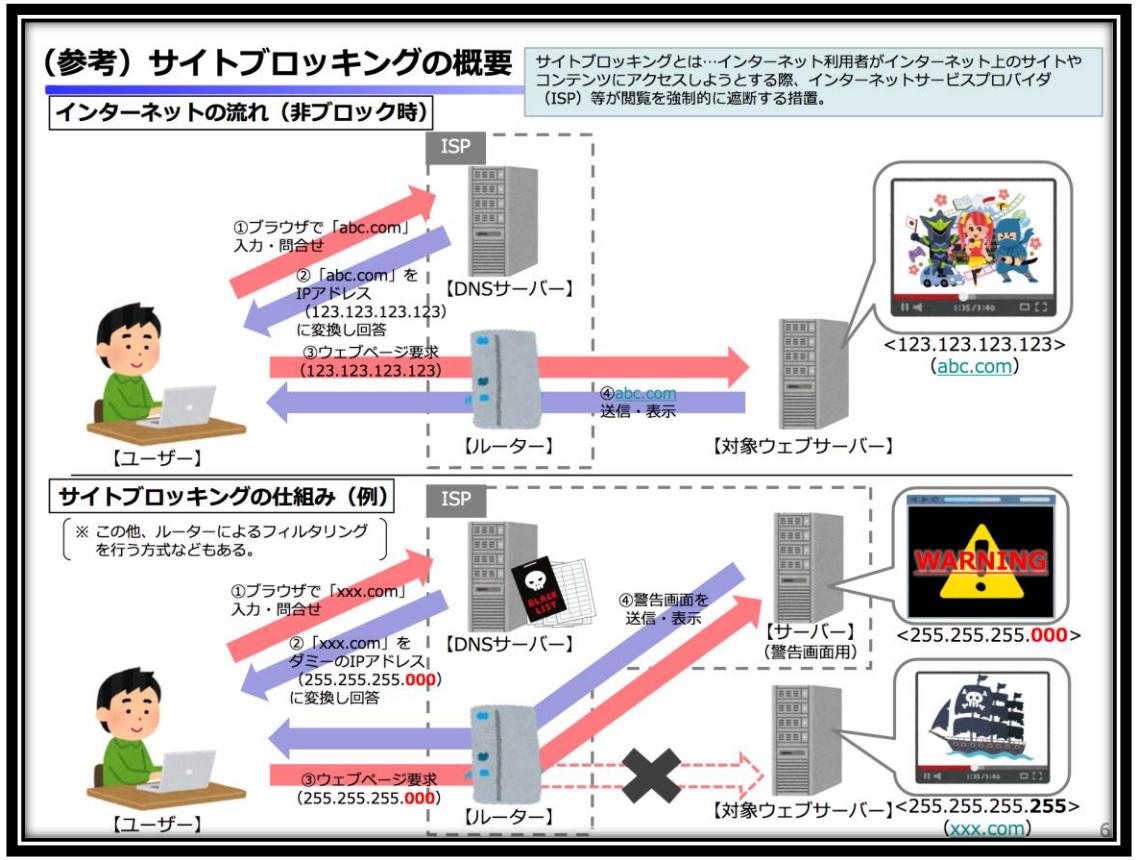
DNSブロッキングについて考える

2018/06/27

石田慶樹
山本功司
日本DNSオペレーターズグループ

DNSブロッキング

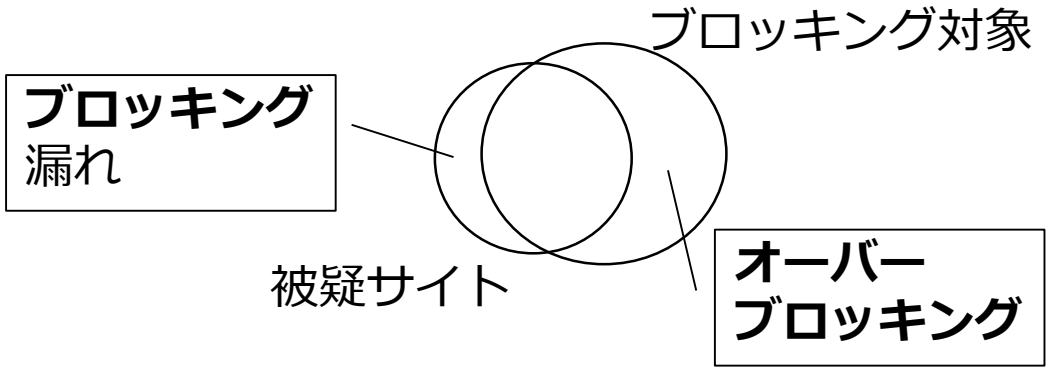


- DNSフルリゾルバにおいてあるドメイン名に対する問い合わせに対して正しくない返答を返す
- (国内の)ISPのすべてのDNSフルリゾルバにおいて実装されることを想定
- DNSフルリゾルバに来る問い合わせを「すべて」確認する必要がある⇒通信の秘密の侵害
- インターネットとしてはDNSにおける完全性(Integrity)を損なう挙動
- 通信の秘密の侵害および完全性を失うことと、それによって守られるものの重要度の比較

https://www.kantei.go.jp/jp/singi/titeki2/tyousakai/kensho_hyoka_kikaku/2018/contents/dai3/siryou1.pdf

DNSブロッキングの課題

- ISPの運用に関わる課題
  - ブロッキング対象
    - オーバーブロッキング
    - ブロッキング漏れ
  - ブロッキングリストの更新
  - ブロッキングした際のユーザ
    通知／カスタマ対応



DNSブロッキングの回避方法

- ブロッキングの抜け穴
  - 自前DNSフルリゾルバの利用
  - Public DNSの利用

- 自前フルリゾルバの利用
  - ノートPCやRaspherry Pi 程度のマシンで十分
  - オープンリソルバにならないように注意

- Public DNSの利用
  - Google, Cloudflare, Quad9 といった**「グローバルプラットフォーマー」**
  - 新たにNIR（TWNIC)も参入
  - 日本でサービスするためにはブロッキングへの参加を求める？

イタチごっこの始まり

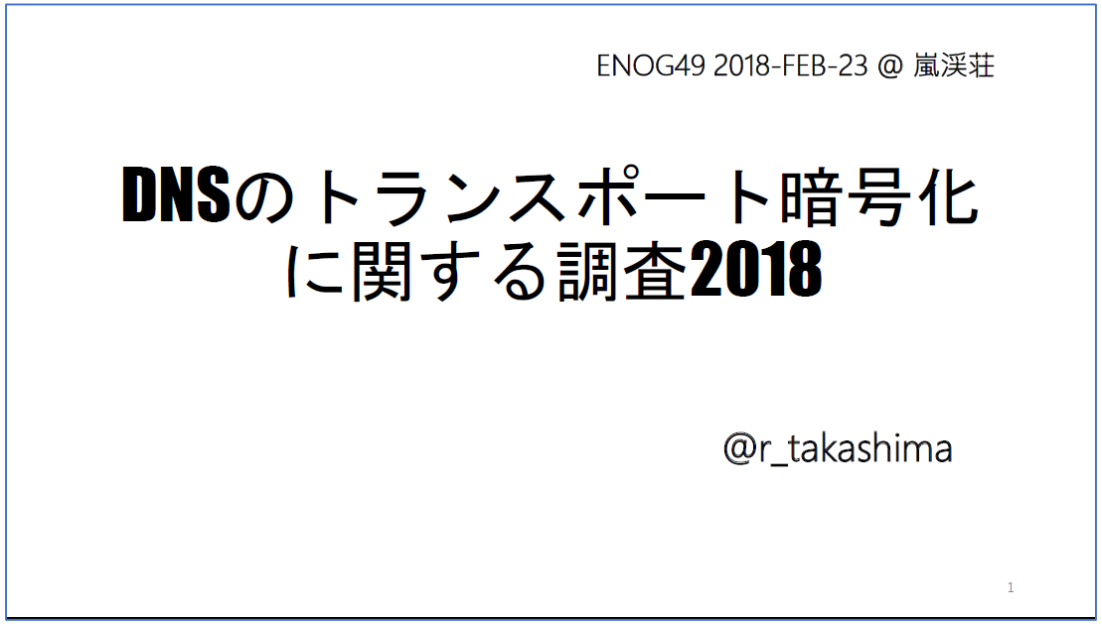
- 抜け道を塞ぐためOP53B
  - 際限なく広がる通信の秘密の侵害

- OP53BやってもDNS over HTTPSやDNS over TLSという技術も実用化されている
  - 提供者はGoogleやCloudflare

- そもそもISPがDNSを運用を続けるという前提がゆらぎつつある
  - Public DNSの利用やDNS/CDN事業者へのアウトソースがまもなく始まる

DNS over TLS/HTTPS

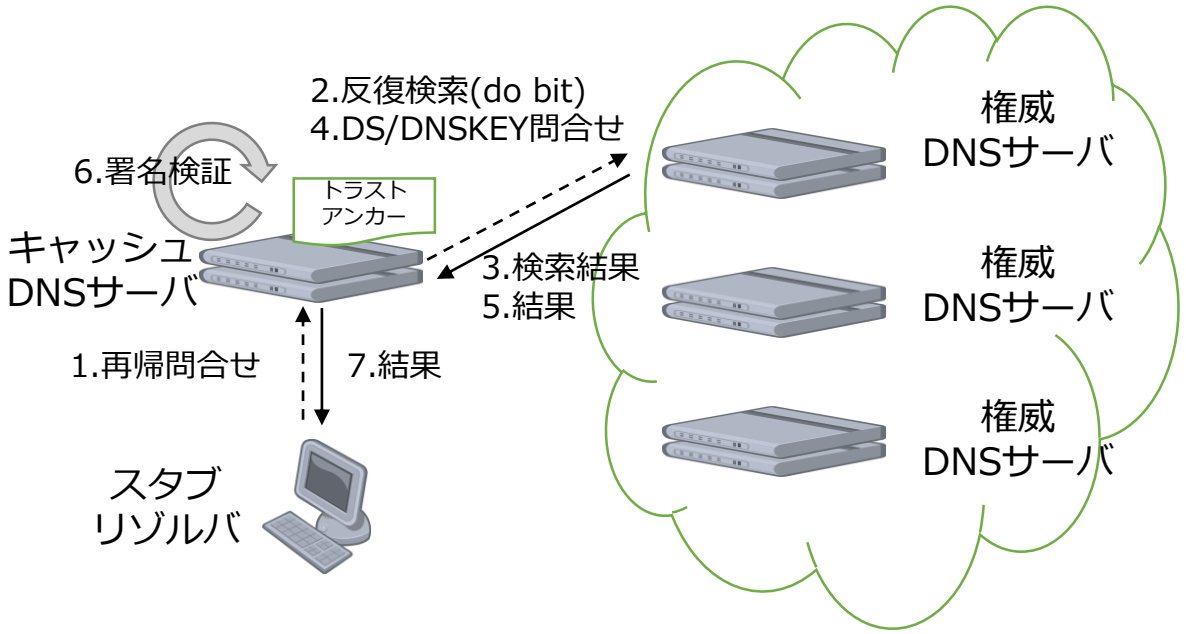
- DNSをUDP/TCPのPort 53ではなく、TLSやHTTPSでQuery/Responseを行う技術
- OP53Bやると逃げ込まれる可能性大
- すでにGoogleやCloudflareが提供中
- ChromeやAndroidに組み込まれないと良いなあ



https://www.slideshare.net/ryuichitakashima3/dns-privacy-of-transport-layer

DNSブロッキングとDNSSEC

- DNSSEC
  - DNSの完全性を守るためのもの
  - 可用性を犠牲にしている



- DNSSECの検証をDNSフルリゾルバで行っている場合にブロッキングされた場合の挙動は実装依存
- 原理的にはDNSブロッキングのための偽情報の挿入は対象サイトがDNSSECで署名されていれば検出可能
- 結果として対象サイトには接続不可なためブロッキングそのものは成功
- ただし警告表示用サイトには接続されない

DNSブロッキングの前にドメイン名は？

- 海賊版サイトが使っているドメイン名って不可侵なのか？
  - gTLDとccTLDで対応が異なる(はず)
- 申告先は？
  - レジストリ
  - レジストラ
  - ICANN(gTLDの場合)
  - 国(ccTLDの場合)
- 漫画村(.orgドメイン)
  - 元は日本？
- MioMio(.tvドメイン)
  - 元は中国
  - レジストラへの削除要請
  - アクセス不能となったが1日で復活
- Anitube(.seドメイン)
  - 元はブラジル

DNSブロッキングの問題点

- 通信の秘密の侵害
  - エンドユーザが接続しようとするサイトへのDNSの問い合わせが「すべて」知徳される
- インターネットの完全性の蹂躙
  - インターネットの仲介者によって「否応なく」情報のブロックもしくは書き換えが行われる

保護されるものと、喪失するものの、バランス