blocking public DNS乗っ取り

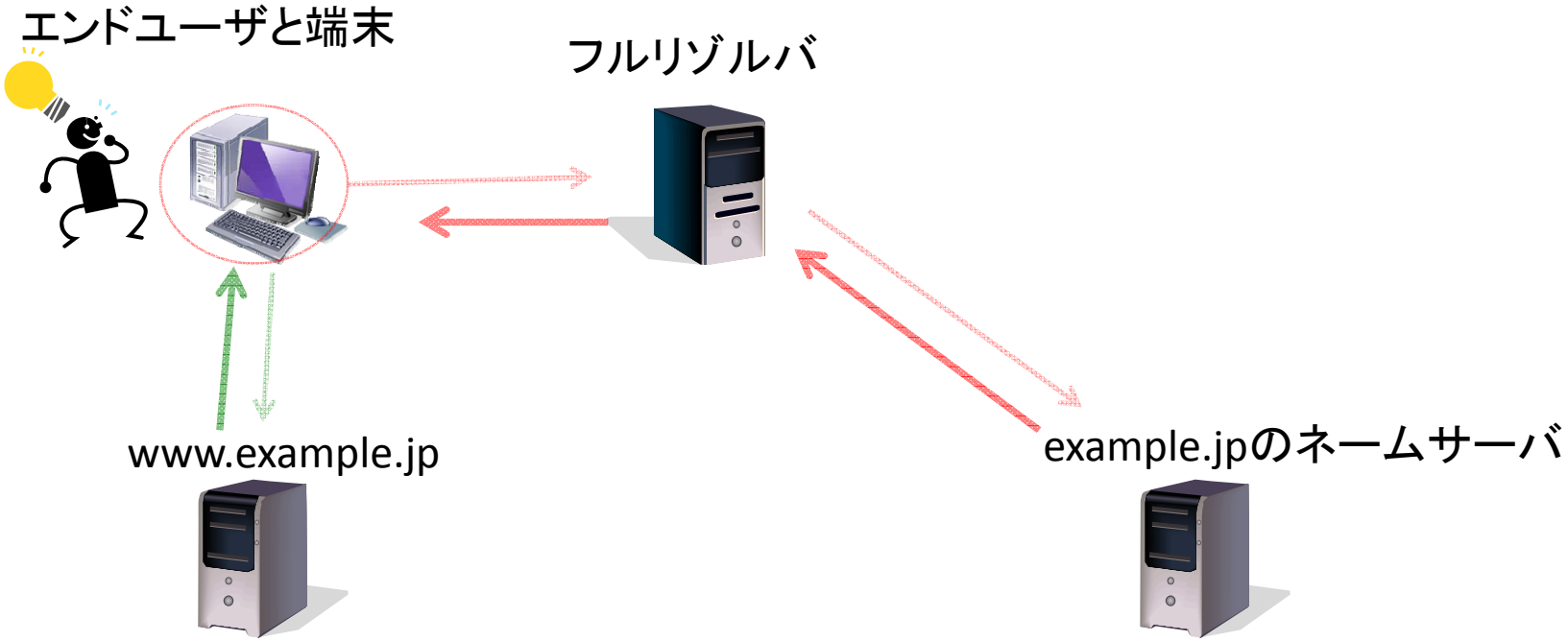
Matsuzaki ‘maz’ Yoshinobu

<maz@iij.ad.jp>

最初に

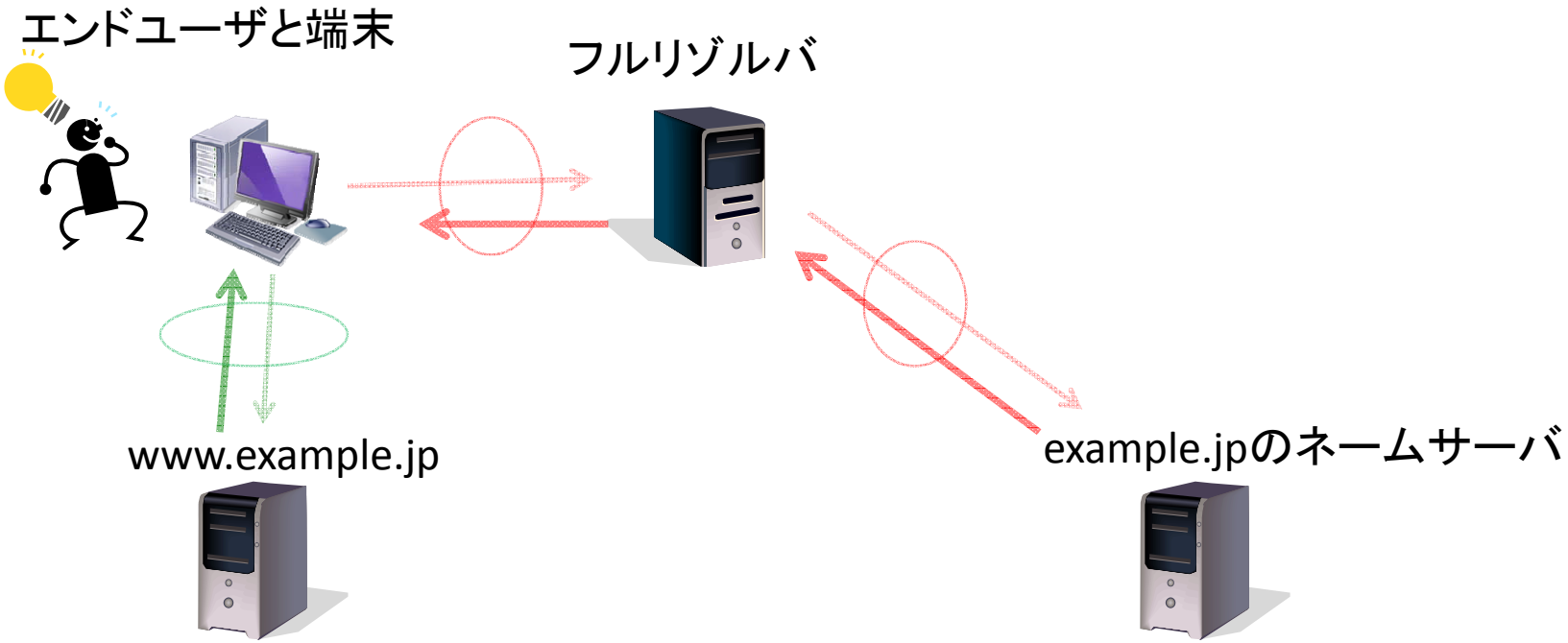
- 良いとも悪いとも、
- やれともやるなとも、
- そんな話はここではしません。
- ただ、世界にはこんな事もあるよというお話

DNSと通信と



- エンドユーザが www.example.jp へアクセスしようとすると、大抵DNSでの名前解決が発生して、得られた宛先に通信が発生

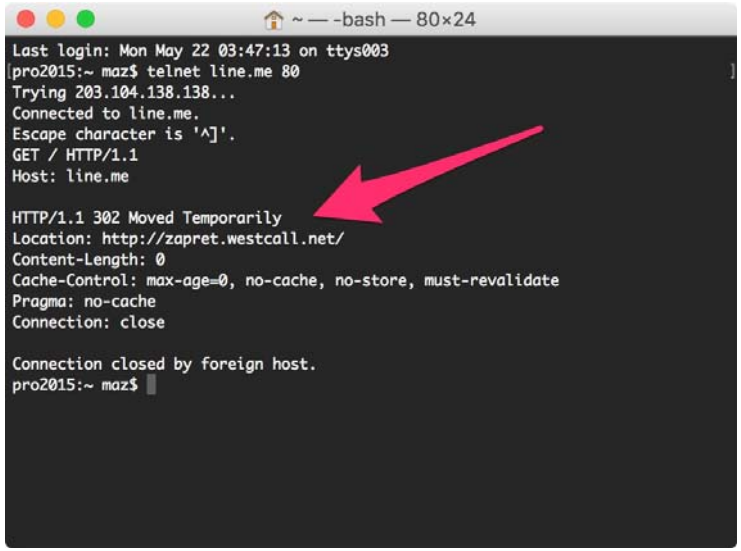
制限したい時

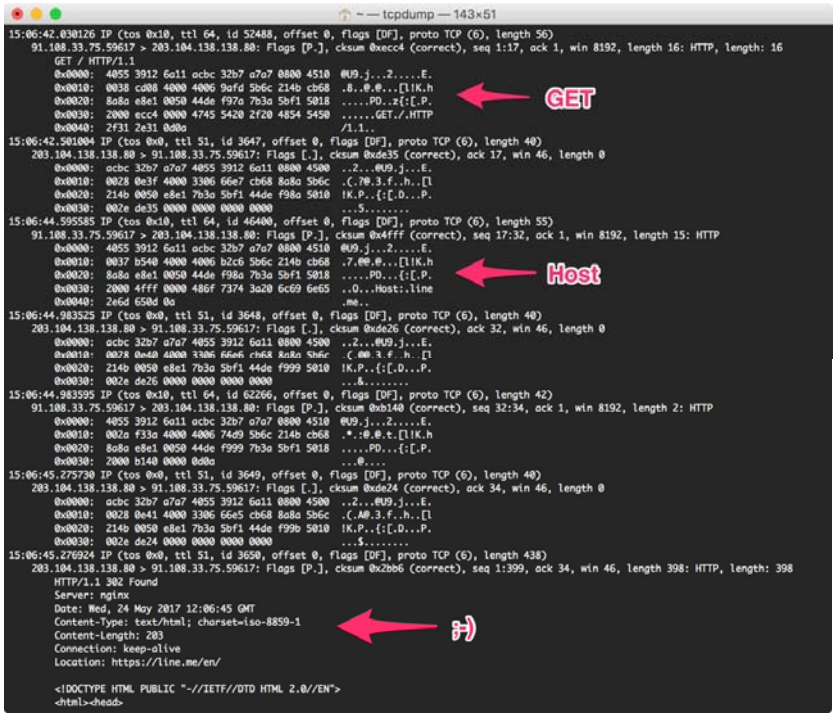


- このどこかで阻止できれば、通信を制限できる

httpで制限実装しようとすると

- 通信経路上で頑張らないといけない
  - エンドユーザのtcp通信を見ないといけない
- やってる所もある





httpsも考えなきゃいけない

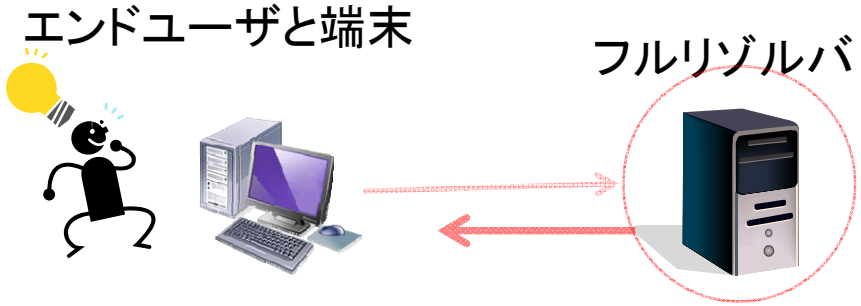
- TLSだと中が見えない
  - 偽の証明書で頑張る
  - セッション開始時に渡すホスト名情報で頑張る
- 何にせよ、tcpを細かく見ないといけないので実装が大変
  - 性能も課題
- どうせホスト名情報でブロックするならDNSでやったほうが簡単でお手軽じゃない！

DNSで制限

- 特定のQNAMEへの応答を制御して実装
  - 対応箇所が少ない
  - エンドユーザの全通信は見なくて良い
  - だいたいUDP使ってるから、実装が素直
  - QNAME単位でフィルタしてしまう
- 見たことがある適用箇所は概ね二箇所
  1. フルリゾルバで実装して制御
  2. 外向けDNS問い合わせを監視して制御

1. フルリゾルバで実装

- ISPの運用するフルリゾルバで指定のQNAMEの応答を上書きする
  - 日本でも児ポ対応などで実装されてますね
- リストを更新する手順さえ確立すれば、比較的網羅的かつお手軽に通信を制限できる
  - フルリゾルバはPPP/DHCPとかで自動配布



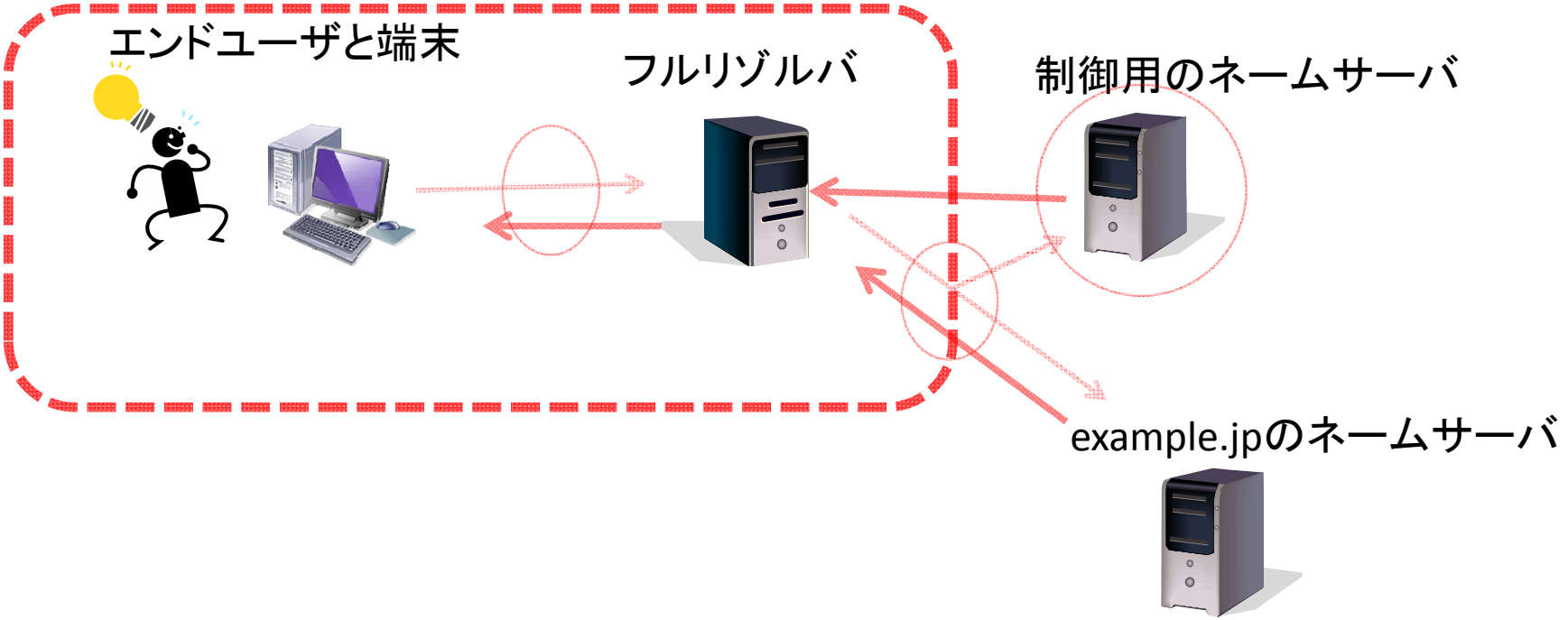
しかし抜けがある

- Public DNSサービスの拡大
  - 名前解決用のフルリゾルバサービス
  - 無償で利用可能
- 利用者が手動でこれらを端末に設定すると、ブロッキングが迂回されてしまう

経路的に吸い込めばいける

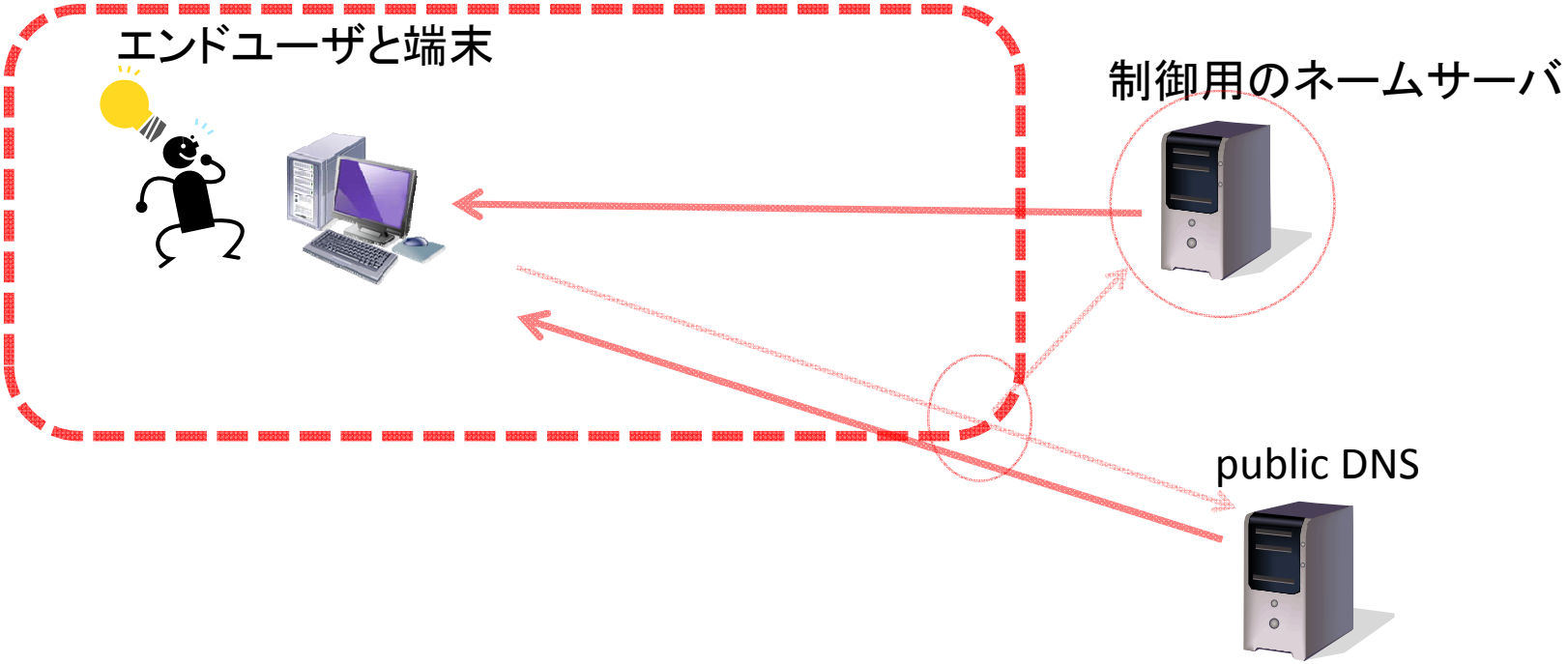
- フルリゾルバとしては同様のサービス
  - 誰でもサービス可能
  - サーバ認証などは存在しない
- 既存のフルリゾルバにIPアドレスを追加設定して、そこにパケットを運ぶだけでも良い
  - 戻りのパケットの送信元IPアドレスだけ気をつければ良い
  - anycast ネームサーバ作るときとほぼ一緒

2. 外向けDNS問い合わせを監視



- 外向けのUDP/53を制御用のネームサーバにも転送し、制限対象だった場合にはそこから即座に応答

public DNSを使っていても

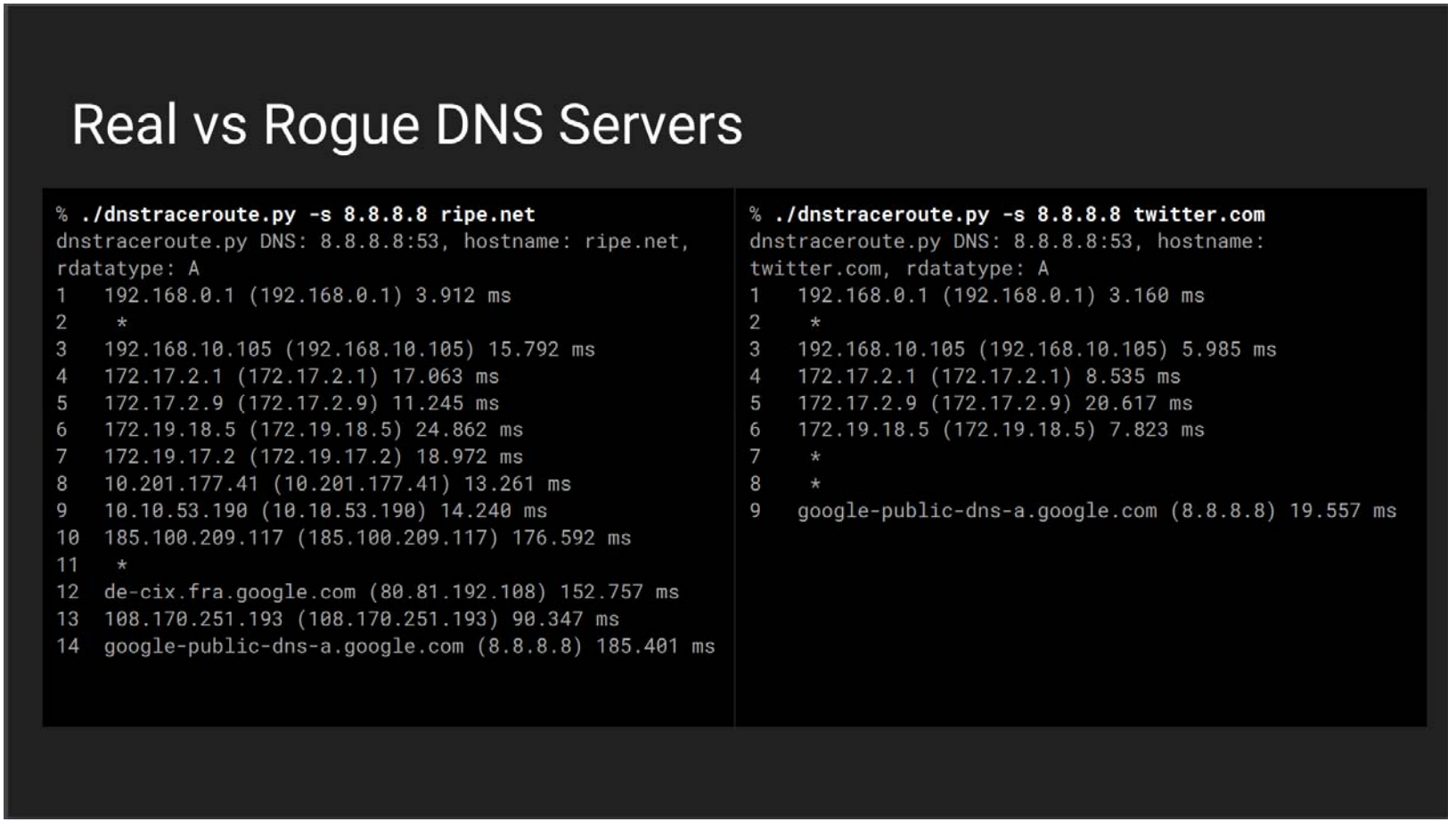


- 外部のフルリゾルバを使っていても同様の手段でブロッキング可能

実装の考察

- 制限対象のQNAMEが来た時に反応すれば良い
- 本物のネームサーバより早く応答する必要
  - パケットを監視する近傍に制御用のネームサーバを設置しておけば、だいたい大丈夫
- ‘外’との境界が増えると増設しないといけない
- ‘内’の名前解決にはあまり影響しない
  - 制限対象のネームサーバは常に外にあるモデル

RIPE75での発表事例

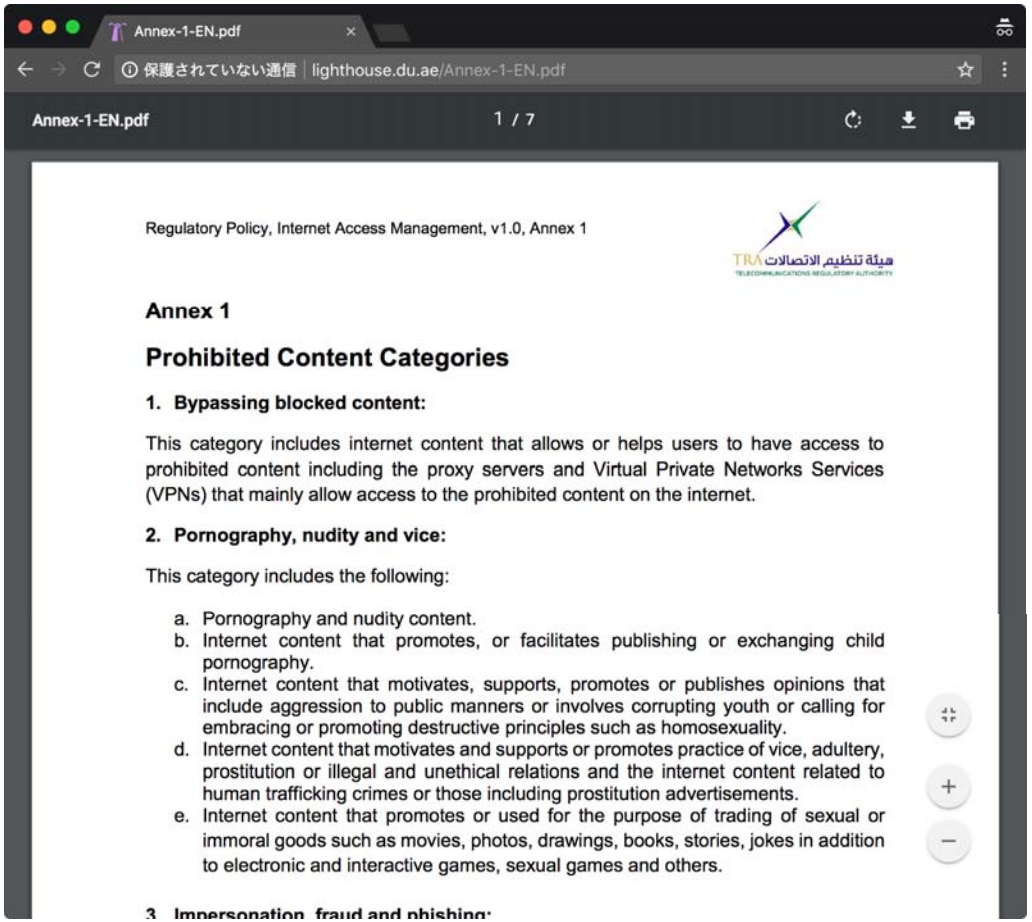


https://ripe75.ripe.net/presentations/20-A-curious-case-of-broken-DNS-responses-RIPE-75.pdf

体験可能だが推奨しない

- そんな地域でサービスしているPublic DNSを使えば、DNS blockingの様子を体験できる
  - ただし、推奨しません
- とある実装ではblocking対象のQNAME問い合わせにランダムなIPアドレスを応答
  - 端末が世界のランダムな宛先にアクセスを試みることになる

ポリシー事例


Annex-1-EN.pdf
保護されていない通信 | lighthouse.du.ae/Annex-1-EN.pdf
Annex-1-EN.pdf
1 / 7
Regulatory Policy, Internet Access Management, v1.0, Annex 1
هيئة تنظيم الاتصالات TRA
Annex 1
Prohibited Content Categories
1. Bypassing blocked content:
This category includes internet content that allows or helps users to have access to prohibited content including the proxy servers and Virtual Private Networks Services (VPNs) that mainly allow access to the prohibited content on the internet.
2. Pornography, nudity and vice:
This category includes the following:
a. Pornography and nudity content.
b. Internet content that promotes, or facilitates publishing or exchanging child pornography.
c. Internet content that motivates, supports, promotes or publishes opinions that include aggression to public manners or involves corrupting youth or calling for embracing or promoting destructive principles such as homosexuality.
d. Internet content that motivates and supports or promotes practice of vice, adultery, prostitution or illegal and unethical relations and the internet content related to human trafficking crimes or those including prostitution advertisements.
e. Internet content that promotes or used for the purpose of trading of sexual or immoral goods such as movies, photos, drawings, books, stories, jokes in addition to electronic and interactive games, sexual games and others.
3. Impersonation, fraud and phishing:

ポリシー事例（続き

17. Prohibited Top level Domains

This category includes top-level domains on the internet allocated for purposes that violate the laws of the UAE regardless of website content falling under them. e.g. top-level domains for pornographic material .xxx and others.

恐らく彼らが守りたいもの

- 社会体制
  - 社会制度
  - 価値観
  - 倫理
- 産業
  - 新興市場
- 情報
  - 個人情報
  - 動静