DNS blockingの仕組み

IIJ
Internet Initiative Japan

2018/11/29
Internet Week 2018
D3: DNS DAY

株式会社
インターネットイニシアティブ
島村 充
<simamura@iij.ad.jp>

Ongoing Innovation

about me

- 2006年 IIJ 新卒入社

  以降、メールサービスの設計・構築・運用12年

- 2010年～ 回線サービス向けフルサービスリゾルバの運用
- 2015年～ 権威DNSサービスの運用
- DNSOPS.jp所属。IW2017, 2018プログラム委員。脱BINDエヴァンジェリスト(自称)

アジェンダ

- ブロッキングとは
- (ブロッキングと法律)
- ブロッキングの手法
- DNSブロッキング回避の禁止

はじめに

- 今年度初頭から、海賊版サイトに対する対策案で「ブロッキング」をしろ、という論調が盛り上がりました。
- そもそも「ブロッキング」とは…？

> *block*
> *An obstacle to the normal progress or functioning of something.*
> Oxford Dictionaries

- 「正常な進展や何かの機能を妨げる」
  →「Webの正常な閲覧を妨げる」

フィルタリング or ブロッキング？

- ユーザー(or保護者)の…
  - 同意がある → 「フィルタリング」
  - 同意がない → 「ブロッキング」

  と区別する場合が多いように思われる

時間が足りないので、法制度に関しては省略します。

配布資料には記載しているので、そちらをご覧ください。

なぜブロッキングをしてはいけのか

配布資料のみ

- 通信の秘密
- 日本国憲法 第二十一条

> 第二十一条
> 集会、結社及び言論、出版その他一切の表現の自由は、これを保障する。
> ○２　検閲は、これをしてはならない。通信の秘密は、これを侵してはならない。

- 電気通信事業法 第四条

> （秘密の保護）
> 第四条
> 電気通信事業者の取扱中に係る通信の秘密は、侵してはならない。
> ２ 電気通信事業に従事する者は、在職中電気通信事業者の取扱中に係る通信に関して知り得た他人の秘密を守らなければならない。その職を退いた後においても、同様とする。

通信の秘密の侵害の3類型

配布資料のみ

通信当事者以外の第三者が…

- 知得
  - 積極的に通信内容を知ろうとすること
- 漏洩
  - 通信内容を他者の知りうる状態にすること
- 窃用
  - 通信当事者の意思に反して自己または他人の利益のために利用すること

違法性阻却事由

配布資料のみ

- 違法行為であっても以下の場合は違法性が否定される
  - 正当行為(法令行為・正当業務行為)
    - 警官による逮捕での身柄の拘束 (法令行為)
    - 外科医による手術で体をメスを入れる
    - IPパケットのルーティングのためにIPヘッダを見る
  - 正当防衛
    - ひったくりに物を取られたため、取り返そうとぶん殴って怪我をさせた

違法性阻却事由

配布資料のみ

- 緊急避難
  - 車に轢かれそうになって、花壇に飛び込んだら花を折ってしまった

緊急避難

配布資料のみ

- 緊急避難が成立するには3つの要件をすべて満たす必要がある
  - 現在の危難
  - 補充性
  - 法益均衡

緊急避難

配布資料のみ

- 現在の危機
  - 自己又は他人の生命、身体、自由又は財産に対して、今今、法益の侵害が生じていること (過去の事項で今今でないものはNG)
- 補充性
  - やむをえずにした行為であること

＝他に採るべき、より侵害性の少ない手段がないこと

緊急避難

配布資料のみ

- 法益均衡
  - 避難行為から生じた害が避けようとした害の程度を超えなかったこと

＝ 権利の侵害の度合いの比較

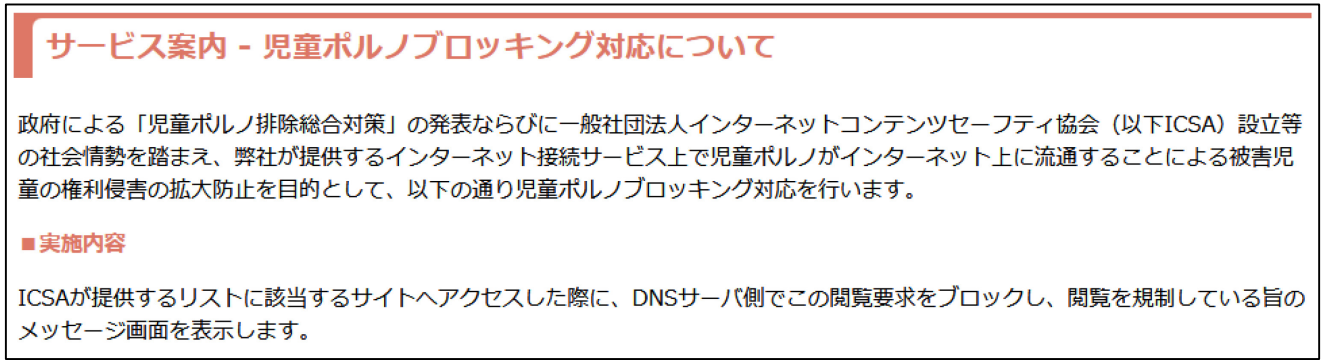
3行 4行で

- 電気通信事業者は通信の秘密を侵害すると罰せられる
- 違法行為であっても、違法性阻却事由が認められれば罪に問われない
  - 正当行為・正当防衛・緊急避難
- 緊急避難の3要件:

  現在の危機・補充性・法益均衡

すでにされているブロッキング

- 実はブロッキングはすでに行われている
- 児童ポルノブロッキング



サービス案内 - 児童ポルノブロッキング対応について

政府による「児童ポルノ排除総合対策」の発表ならびに一般社団法人インターネットコンテンツセーフティ協会（以下ICSA）設立等の社会情勢を踏まえ、弊社が提供するインターネット接続サービス上で児童ポルノがインターネット上に流通することによる被害児童の権利侵害の拡大防止を目的として、以下の通り児童ポルノブロッキング対応を行います。

■実施内容

ICSAが提供するリストに該当するサイトへアクセスした際に、DNSサーバ側でこの閲覧要求をブロックし、閲覧を規制している旨のメッセージ画面を表示します。

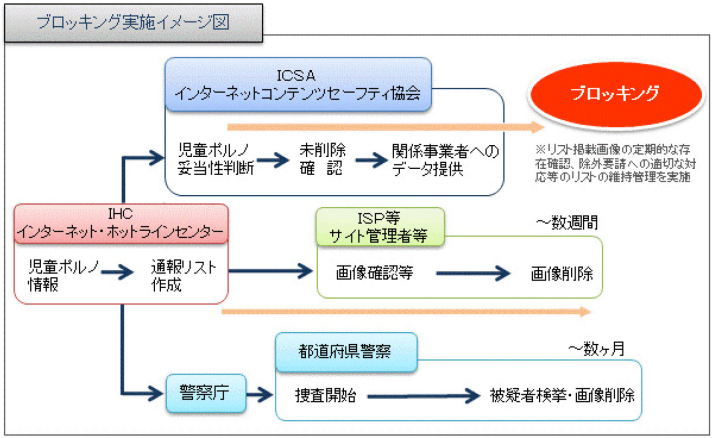
すでにされているブロッキング

- 実はブロッキングはすでに行われている
- 児童ポルノブロッキング

■実施イメージ

インターネット上の児童ポルノブロックは以下のような仕組みで運用されます。

出典：一般社団法人インターネットコンテンツセーフティ協会（新しいウインドウを開きます）
関連団体：インターネットホットラインセンター（新しいウインドウを開きます）



すでにされているブロッキング

このサイトは、児童への著しい権利侵害である児童ポルノを掲載しているサイトと判定され*1、児童ポルノアドレスリスト*2に掲載されているためブロックされました。

詳細につきましては、下記サイトにてご確認ください。

一般社団法人インターネットコンテンツセーフティ協会
(http://www.netsafety.or.jp/blocking/index.html)

※1　児童ポルノ流通防止対策専門委員会が承認した基準に基づき、一般社団法人インターネットコンテンツセーフティ協会が判定しました。

※2　お客様ご契約の接続サービスにおいては、一般社団法人インターネットコンテンツセーフティ協会の作成した児童ポルノアドレスリストが利用されています。

児童ポルノブロッキングの場合

https://www.good-net.jp/blocking/relation/relation_2-2

- 違法性阻却事由：緊急避難
  - 現在の危難
    → 誰でも画像を見ることができ、拡散しつつある
  - 補充性
    → サイバーパトロールによる摘発などをした上で、なお画像が残っている

児童ポルノブロッキングの場合

- 法益均衡

→ 児童の人権侵害(しかも、未来永劫残りうる) vs 通信の秘密の侵害

海賊版サイトブロッキングでは？

- 現在の危難: 満たす…かな?
  - サイトが稼働していれば
- 補充性: 他に採るべき手段を尽くしたか？
- 法益均衡: 著作権・財産権侵害(金銭で被害を回復しうる)vs通信の秘密の侵害

ブロッキングの手法

- ブロッキングにはいろいろなやり方がある
  - HTTPリクエストを検査
    - DPI (Deep Packet Inspection)
  - HTTPS(TLS)リクエストのSNI部を検査
    - 金盾が最近(2018年8月)対応したらしい
  - SSL証明書(のCommon Name?)を検査
    - 金盾が2017年9月に対応したらしい

ブロッキングの手法

- dst IPアドレスで遮断する
- DNSで名前解決できない(or関係のないIPアドレスを返す)ようにする

採用手法

- 児童ポルノブロッキングで採用されているのはDNSブロッキングが多い
  - HTTPリクエスト検査やDNSとHTTPのハイブリッドのISPも

DNSブロッキング(手法)のメリット

- メリット
  - HTTPリクエストの検査と比べて…
    - 処理が軽い
      - HTTPの全パケットをチェックするのはとてもコストが高い
    - 追加設備が少なくて済む
      - 処理コストが高いので台数が多くなる
      - カスタマーエッジ、もしくはIX箇所全てに検査装置を配置する必要がある

    ⇔ DNSサーバーはそこまで台数が多くない
    - HTTPSなサイトでもブロックできる

DNSブロッキング(手法)のメリット

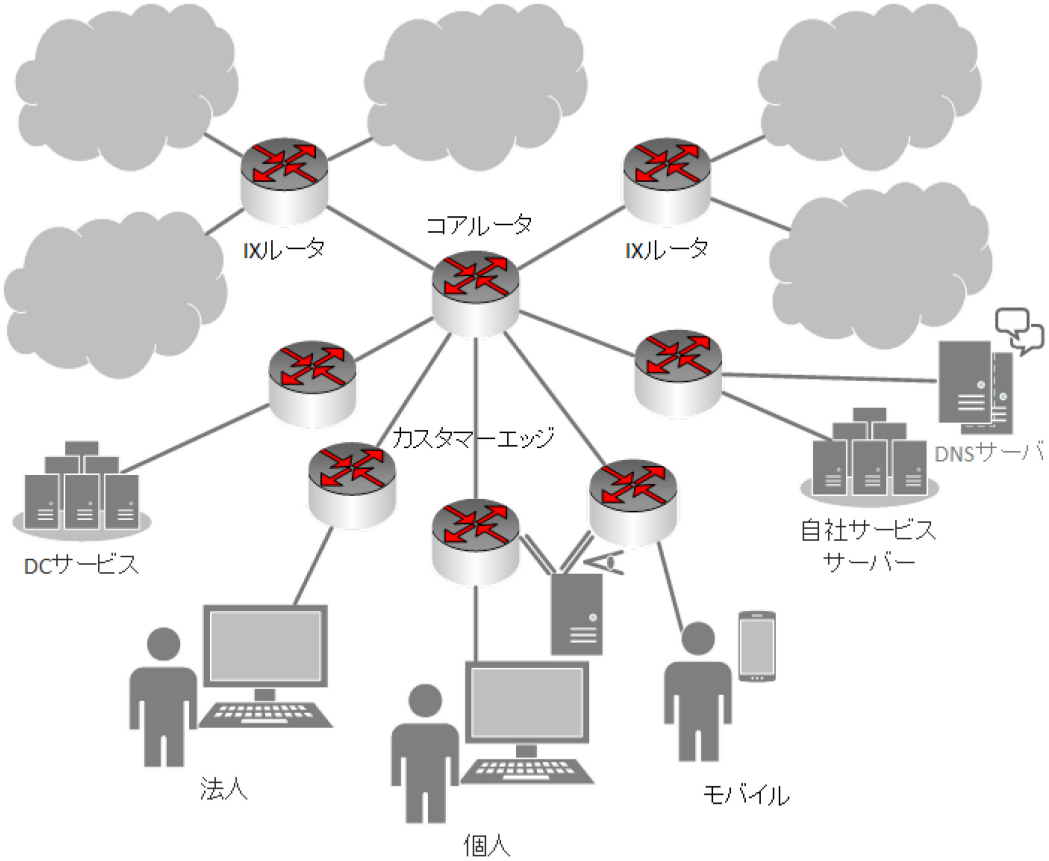
- IPアドレス検査に比べて…
  - ブロック対象の変更頻度が少ない(と思われる)
  - 対象を絞りやすい
    - ブロック対象がCDNを使っていたら…
      → 丸ごとブロックor全くブロックできない

DNSブロッキング(手法)のデメリット

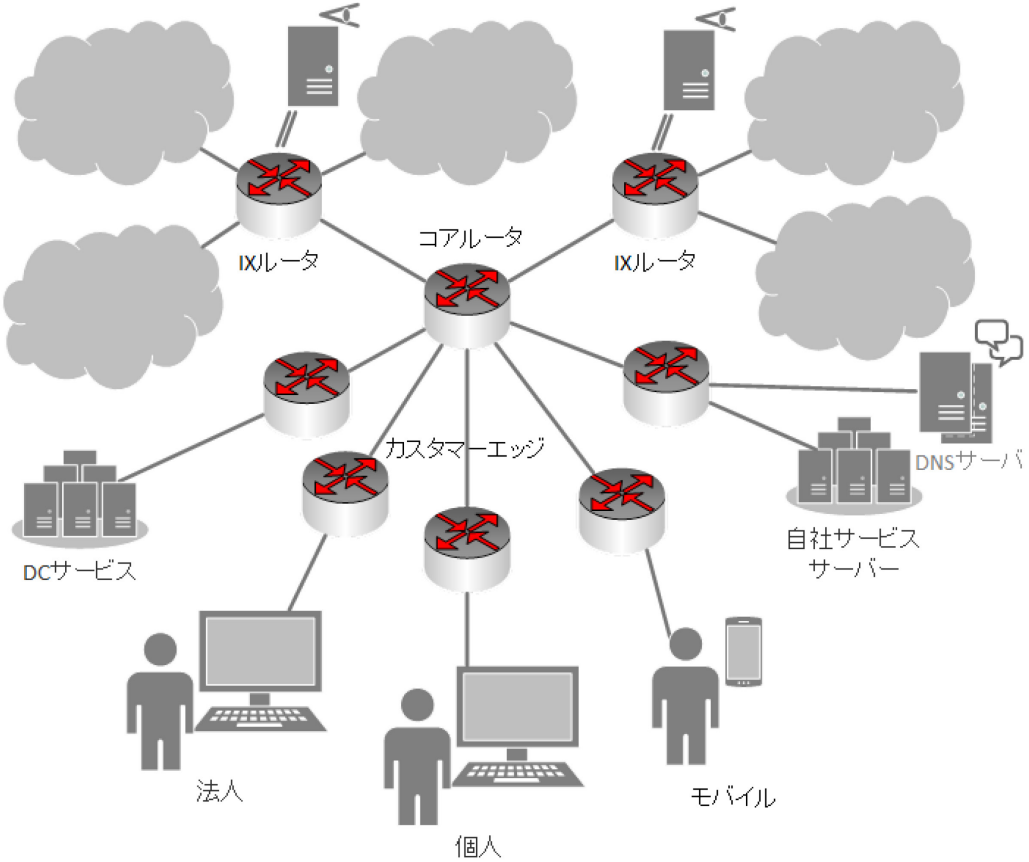
- デメリット
  - ブロッキング回避が簡単
    - 自前/ISP外のDNSサーバーを使えば良い
  - ホスト名しか検査できない
    - オーバーブロッキング(F/P)の危険
    - すり抜け(F/N)の恐れ

    もっとも、HTTPSならSNIやCNを検査しても同じことだし、IPアドレス検査も同じ話

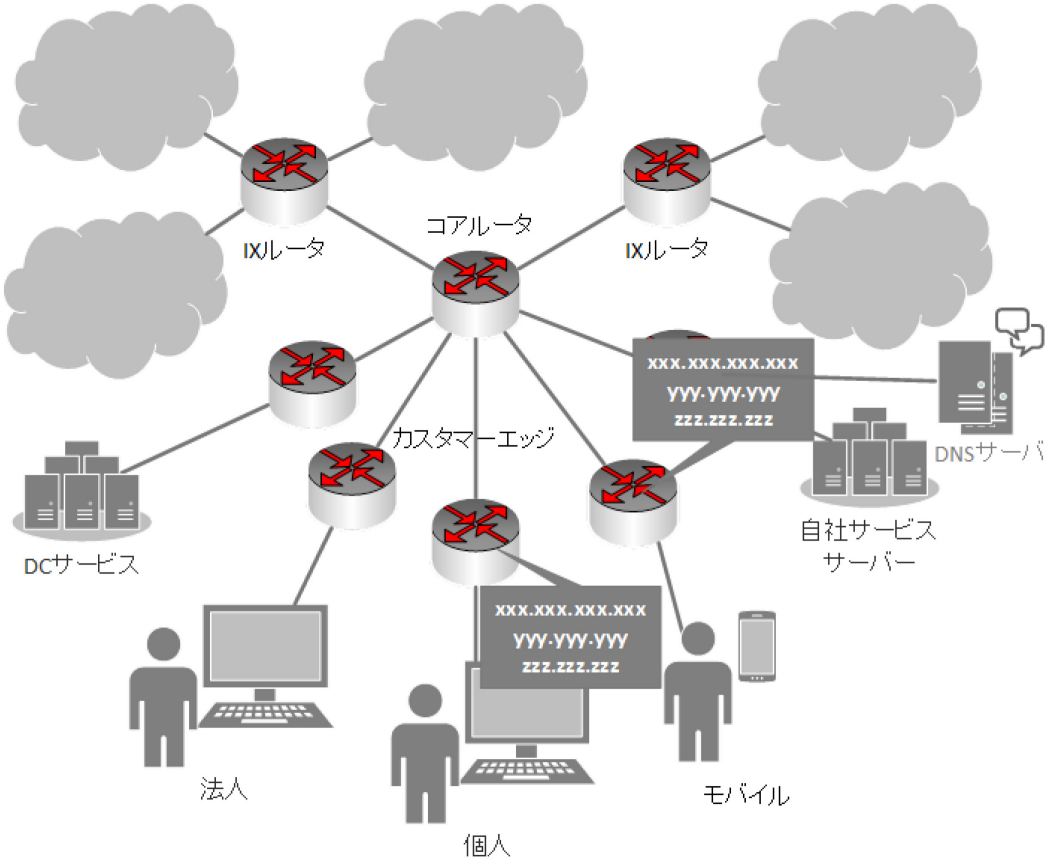
カスタマーエッジルータでDPI



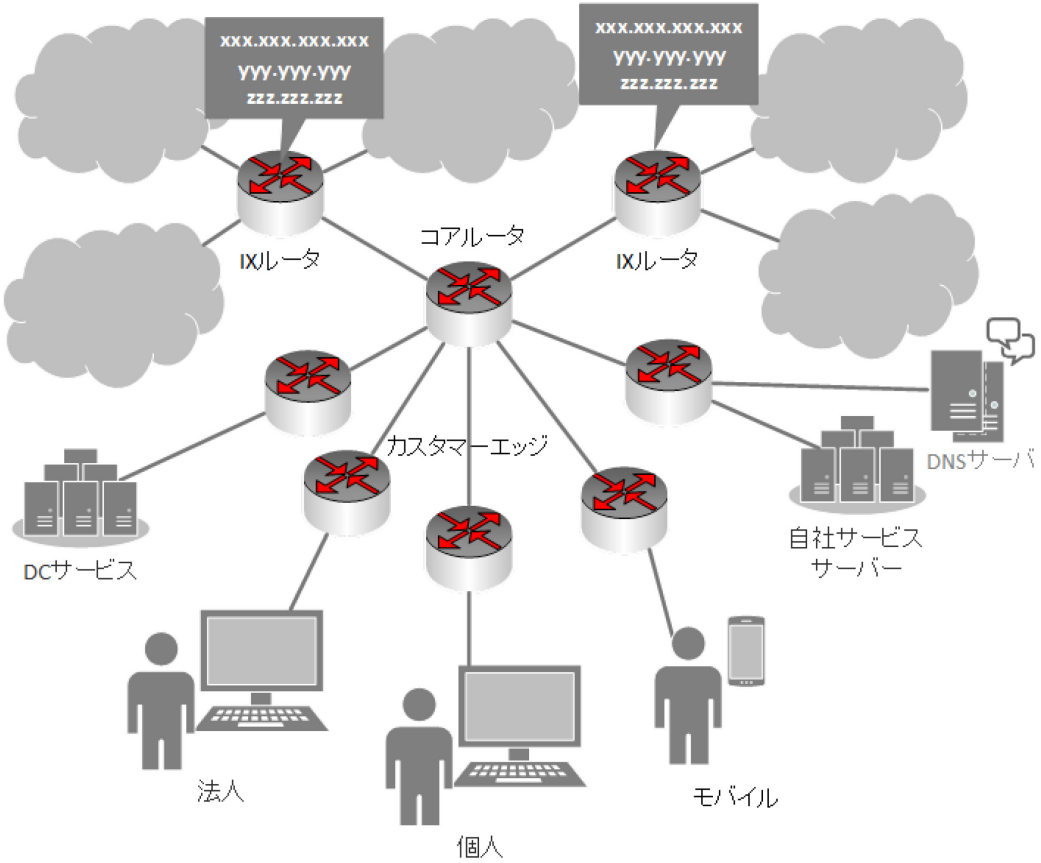
IXルータでDPI



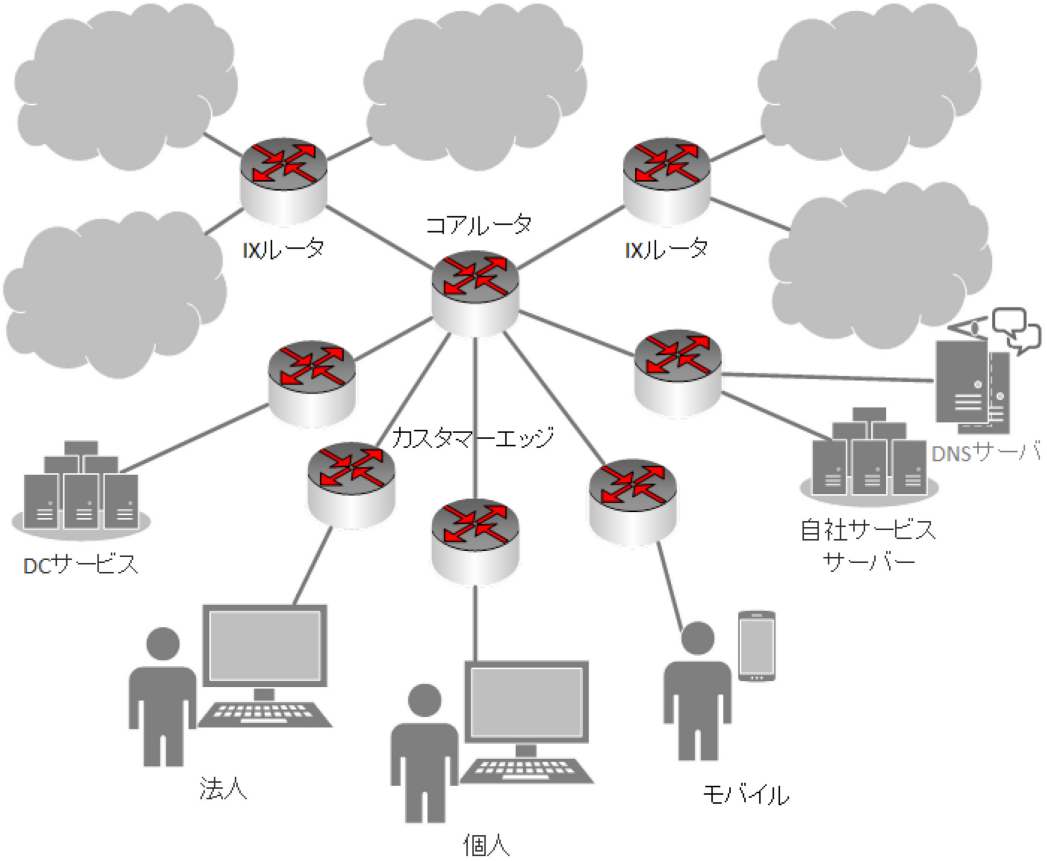
CEルータでIPアドレスフィルタ



IXルータでIPアドレス



DNSサーバで二セ応答を返す



DNSブロッキング回避の禁止？

カドカワ社長 川上量生氏曰く

採用されるサイトブロッキングの手法については児童ポルノ同様にDNSブロッキングであるということを前提とする。その場合、(略)一般ユーザーがDNSサーバーを変更する、という技術的には一般ユーザーでも簡単にとれる回避手段が存在する。これは迷惑メール対策として導入されているOP25Bの設定をポート番号を変更するだけであり、プロバイダにとって実現は容易である。

https://www.kantei.go.jp/jp/singi/titeki2/tyousakai/kensho_hyoka_kikaku/2018/kaizoku/dai5/siryou10.pdf

OP25Bとは

- Outbound Port 25 Blocking
  - ウイルスに感染したユーザー・迷惑メール送信業者などから、spamの発信を防ぐために、自社MSA以外へのdst port 25の通信を遮断する

OP25B実施の「制約」

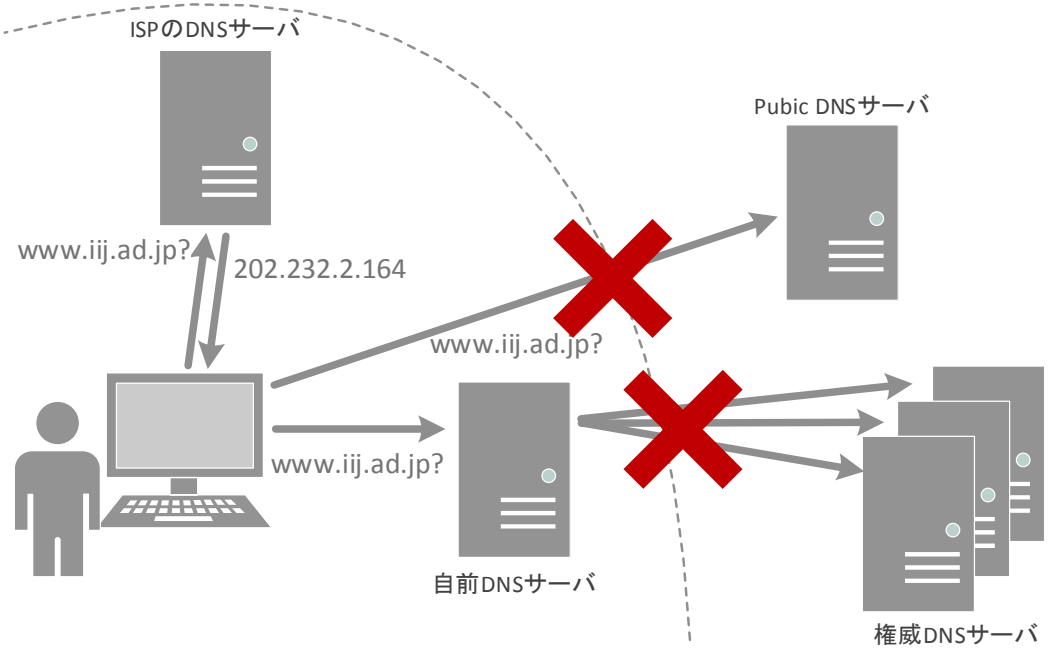
- 動的IPアドレスのユーザーのみに適用可能
  - 動的IPアドレスユーザーはクレームが入った時に、契約者を特定するのが大変なため
- submission portの準備
  - 自ISP外のMSAを利用してのメール送信は、port 587やport 465を利用可能

OP53B?

- Outbound Port ***53*** Blocking
  - 自ISP網外へのdst port ***53***の通信を遮断
  - DNSの通信はstub → full resolver, full resolver → AUTHともにdst port 53
  - dst port 53の通信を遮断することで、自ISP網外のfull resolverを使えず、自前でfull resolverを建てたとしても、AUTHにたどり着けず、名前解決ができない

OP53B?

- ISPのfull resolverの利用を強制することでブロッキング回避をさせない



OP53Bは違法性阻却事由を満たすのか？

- OP25Bは違法性阻却事由: 正当行為

① ISPの提供するメールサーバを利用した大量送信が行われていないこと、
② ISPの提供するメールサーバを経由しない動的IPアドレスからの大量送信が行われていること、
③ 必要な限度で実施され、かつ通信の秘密を侵害しない形での代替手段がないこと
が認められる場合には、OP25Bは正当業務行為と認められ、違法性が阻却されると考えることができる。

http://www.soumu.go.jp/main_content/000499986.pdf

“常時ブロックすること” は緊急避難たり得ず、
正当行為として認められる必要がある

Appendix:実際のDNSサーバの設定方法参考資料

- 安心ネットづくり促進協議会

  「DNS ブロッキングによる児童ポルノ対策ガイドライン」

  https://www.good-net.jp/files/original/20171101221901854677 6.pdf

- Internet Week 2011 DNS DAY

  「キャッシュDNSサーバとフィルタリングの実例」

  https://www.nic.ad.jp/ja/materials/iw/2011/proceedings/d1/d1-07.pdf

Appendix: 法制度をもっと詳しく

- IIJmio meeting 20
  「インターネットと通信の秘密」
  https://www.slideshare.net/IIJ_techlog/iijmio-meeting-20
- 『情報セキュリティ対策における「通信の秘密」について』
  https://www.jaipa.or.jp/event/oki_ict2014/140703_hiramatsu.pdf
- 「受信側における送信ドメイン認証技術導入に関する法的な留意点」
  http://www.soumu.go.jp/main_content/000499986.pdf

Ongoing Innovation

IIJ Internet Initiative Japan

Any Questions?