RITSUMEIKAN

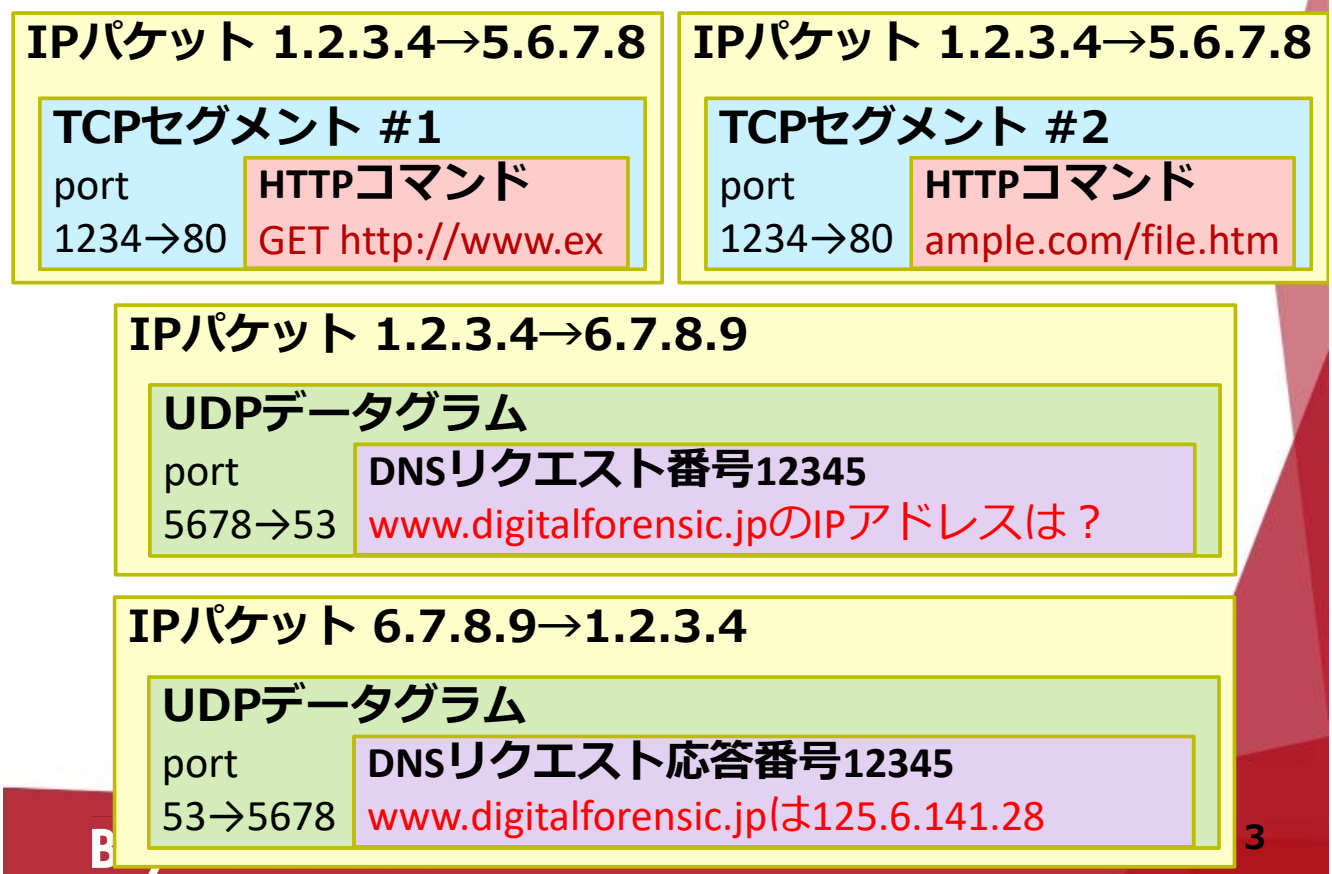
ＩＤＦ第１５期第１回「法務・監査」分科会

Ｗｅｂサイトのブロッキングにおける技術的・運用上の課題

立命館大学情報理工学部
上原哲太郎

IP→TCP・UDP→HTTP・DNS

- IPパケットはEthernetフレームなどを用いて
  「相手の計算機にデータを届ける」ためのもの
  ヘッダには送信側と受信側のIPアドレスが載る
- TCP/UDPはIPパケットを用いて
  「計算機内のプログラムにデータを届ける」もの
  TCPは双方向通信・データ長無制限・到達保証
  UDPは片方向通信・データ長制限あり・到達無保証
  いずれもヘッダには送受信双方のポート番号が載る
- SSL/TLSはTCPを暗号化するもの（以下TLS）
- HTTPはTCPを用いてWebのデータを送受信するもの
  - ブラウザからHTTPコマンドを送信　受信されるのがHTMLなど
  - TLSを用いて暗号化可能
- DNSはUDPを用いて
  ホスト名→IPアドレス変換などを行うもの
  - 暗号化はDNS over TLSなど別の規格があるが普及はこれから



HTTPというのはどういうものか

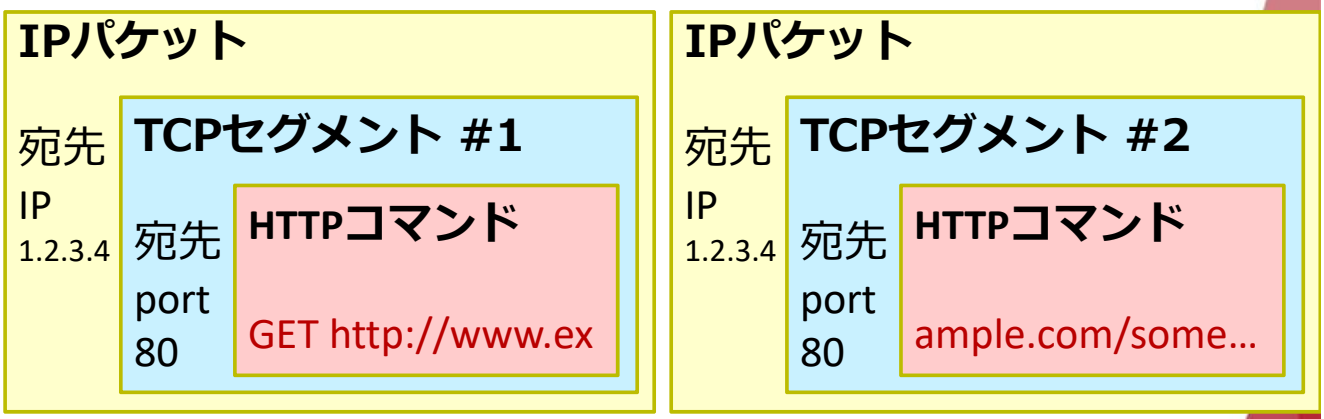
http://www.example.com/somewhere/file.html

ホスト名　ファイルパス名

- Webブラウザがこれを受け取ると…
  - DNSを使ってホスト名からWebサーバのIPアドレスを得る
  - そのIPアドレスに向けて TCP port 80でTCP接続
  - そのTCP接続を用いてHTTPプロトコルのGETコマンドでURLをWebサーバに伝えファイルを取得
  - そのファイルがHTMLである場合には、埋め込まれた画像等についても同様にURLに従いHTTPでファイルを取得
  - それを組み立てて（レンダリング）Webページを表示
- Proxyがある場合にはブラウザはURLをProxyに投げファイル取得手続きの代行を依頼
- httpsの場合にはTCP portが443になりTCP接続はTLSで暗号化
- このどこかを妨害すればブロッキングが成立

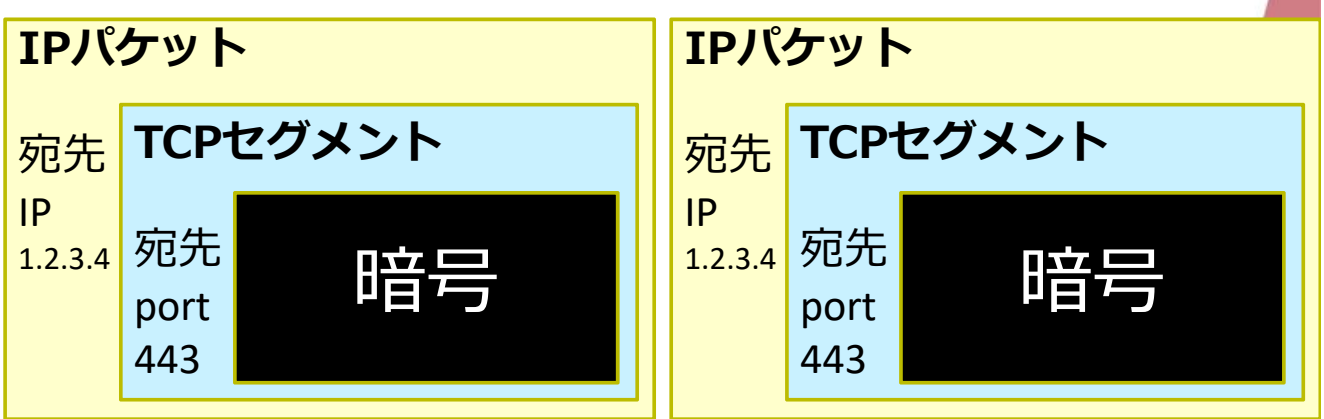
WebサーバのIPアドレスは分かる
URLは暗号化され分からない

HTTPリクエストを含むパケットのイメージ



- IPパケット・TCPセグメントの行き先はIPパケット単位で制御可
- HTTPは複数のIPパケットを集めないと中身がわからない
  - この仕事は通常ISPが運用している機器では出来ない（要DPI機器）
  - 技術的困難→運用コストがバカ高い　費用負担どうするの？？

HTTPSリクエストを含むパケットのイメージ

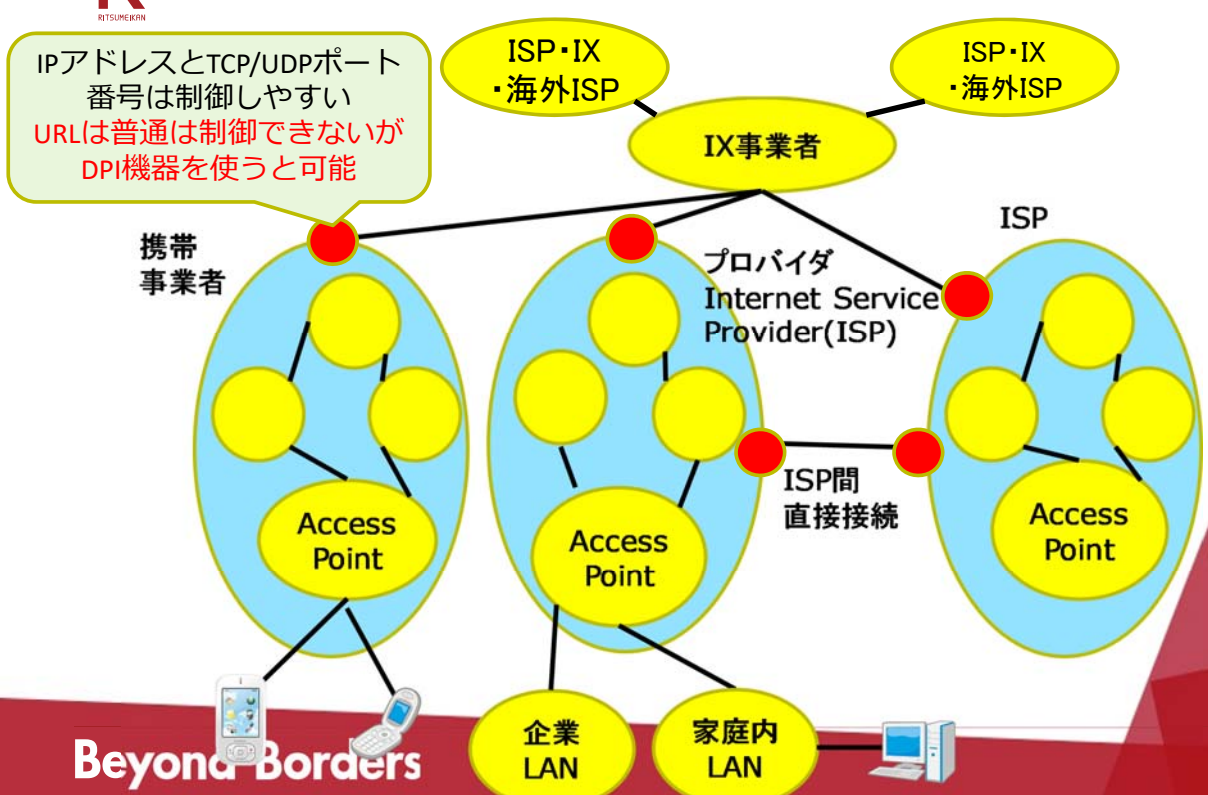


- IPパケット・TCPセグメントはIPパケット単位で制御可
- TCPセグメントのヘッダより内側は解読不能
  - なのでHTTPSを含む場合はURLによる制御はできない
  - ただ前段階のDNSのリクエストは暗号化されてない

ブロッキングの手法は主に3つ

- IPアドレスブロッキング
  - ISPの出入り口で特定のIPアドレス向きのパケットを遮断または別のIPアドレスに書き換えて誘導
    - 実はWi-FiのWeb認証はこの手法
- DNSブロッキング
  - ISPがDNS応答を書き換えてニセのIPアドレスを返す
    - ISPが管理するDNSサーバで書き換える
    - DNSパケットを横取りしてニセの応答にして返す（UDPの場合）
- URLブロッキング
  - ISPのDPI機器でURLを読んだ上で特定のパターンのセグメントを落とす

ISPはIPアドレスとポート番号は制御できるがURLは普通は制御できない！



ところでDNSはどうなってるのか

- DNSサーバ（resolver）は通常ISPがそれぞれ所有しており その管理下にある
  - 通常各端末は自動設定により接続ISPのDNSを利用する
- なので「特定のホスト名に対して ウソのIPアドレスを返す」というDNSサーバを立てるのは比較的容易
  ∴DNSによるブロッキングが ISPにとっては比較的コスト低
  URLのうちホスト部だけなら制御可能

設定すればISP外のDNSサーバ利用可能（Public DNSなど）

Public DNSとは

- 広く誰にでも利用できるようにしたDNSサーバ
- Google Public DNS
  - サーバIPアドレス 8.8.8.8 / 8.8.4.4
  - アラブの春の際には大きな力
  - （おそらく）統計情報を収集するために運営
- APNIC/CloudFlair Public DNS
  - サーバIPアドレス1.1.1.1 / 1.0.0.1
  - ユーザのIPアドレスを保存しないとしているのが売り
- 他にCisco Open DNSなど

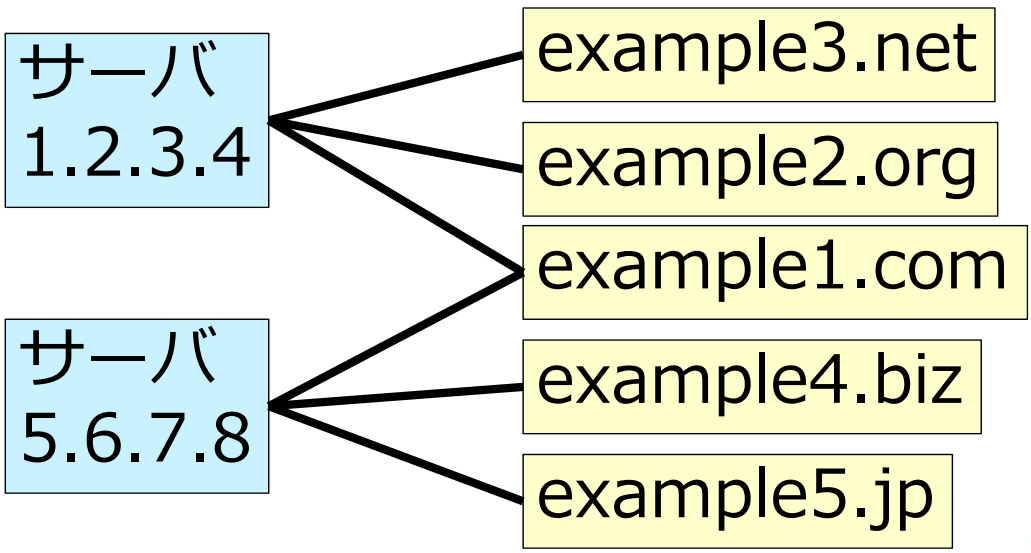
ISPがブロッキングを目的として自DNSの利用を強制することは可能か？

- 技術的には「今なら」可能
  - DNS over HTTPSが普及するまで限定の話（Androidが標準装備する予定で急速に普及しそう）
- 具体的にはOP53Bという技術
  - SPAM対策のOP25Bで実績はある
- ただし制度的には相当困難と思われる

サーバのIPアドレスで止められる？

- IPアドレスとWebサーバホスト名は一対一対応でない
  - Virtual Hostingにより多数のHost名が1つのサーバに
  - 1つのホスト名に負荷分散を目的として多数のIPアドレスを付けることがある
    - それを大規模に請け負うのがConent Devilery Network (CDN)
- よってホスト名やIPアドレスで止める場合はオーバーブロッキングや漏れが起きえる

ホスト名とIPアドレスの複雑なカンケイ



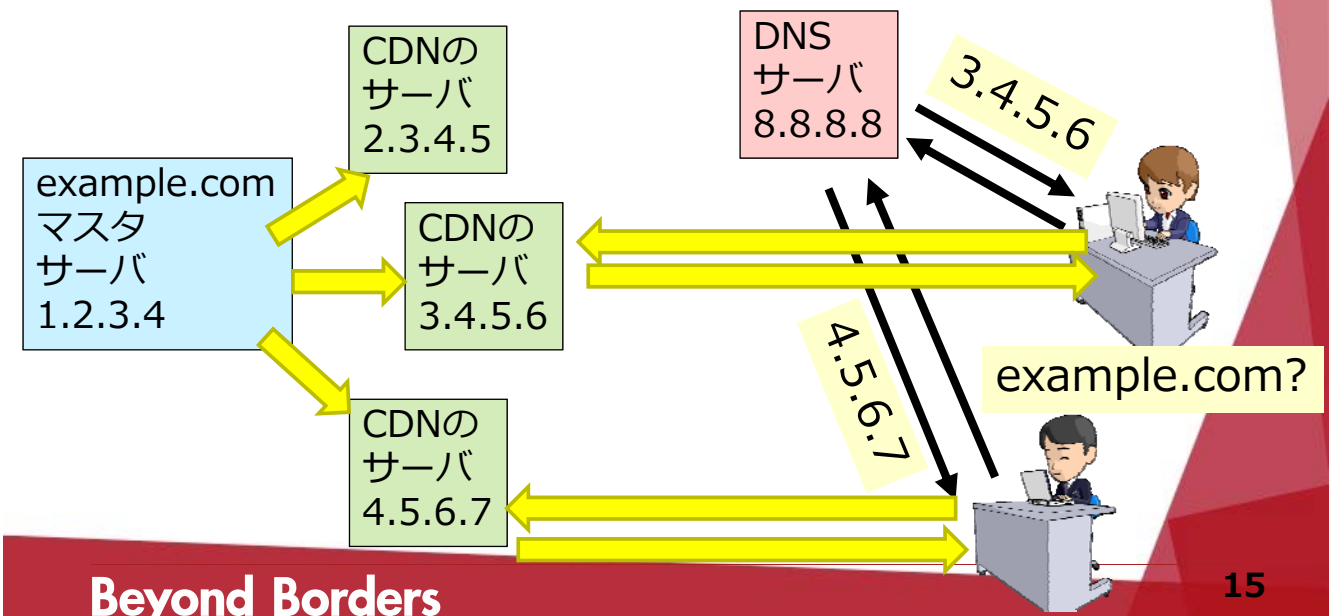
オーバーブロッキング問題・ブロッキング漏れ問題

**http://www.example.com/pirates/*
を止めるために
www.example.com をDNSで止めると…
http://www.example.com/honest/*
も止まってしまう（というか全部止まる）
IPアドレスベースで止める場合には
www.example.comのIPアドレスが
1.2.3.4, 5.6.7.8 等多数になれば
全部止めるのは大変で漏れが出る
（しかもどんどん増えるかも・変えるかも）
IPアドレス1.2.3.4を止めれば
www.example2.net www.example3.orgも止まる**

比較的運用コストの低いはずのIPアドレス/ホスト名ブロッキングも実運用は簡単ではない

Contents Delivery Network (CDN)

- コンテンツのコピーを世界中のサーバにばらまき、近いサーバに誘導するサービス



URLベースのブロッキングは本当に大変

- http://www.example.com/pirates/と http://www.example.com/honest/ を区別にするにはURLベースブロッキングが必要
- そもそもIPパケットを複数集めてHTTPメッセージを組み立ててから通すか止めるか考える必要
  - Deep Packet Inspection (DPI)
- 特別な機器が必要な上大変処理が重く現在の高速なインターネットでは技術的に困難で運用負荷が高い実現しても高価な機器が多数必要

抜け穴いっぱいという話

- DNSブロッキングに対しては…
  - 提供者はホスト名ころころ変えられたら逃げられる
  - 利用者はPublic DNS等の利用で逃げられる
- IPアドレスブロッキングに対しては…
  - 提供者はサーバを変えたら容易に逃げられる
  - 利用者は海外のOpen Proxyや Tor等Overlay Networkの利用によって逃げられる
- DPI利用のURLブロッキングに対しては…
  - 提供者はHTTPS等の暗号化によって逃げられる
  - 利用者は海外のOpen Proxyや Tor等Overlay Networkの利用によって逃げられる

日本国憲法第21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

- 電気通信事業者とは「電気通信設備を用いて他人の通信を媒介し、その他電気通信設備を他人の通信の用に供する」者

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。

電気通信事業法の罰則

第百七十九条　電気通信事業者の取扱中に係る通信（第百六十四条第三項に規定する通信を含む。）の秘密を侵した者は、二年以下の懲役又は百万円以下の罰金に処する。
２　電気通信事業に従事する者が前項の行為をしたときは、三年以下の懲役又は二百万円以下の罰金に処する。
３　前二項の未遂罪は、罰する。

有線電気通信法

第九条　有線電気通信（電気通信事業法第四条第一項又は第百六十四条第三項の通信たるものを除く。）の秘密は、侵してはならない。

第十四条　第九条の規定に違反して有線電気通信の秘密を侵した者は、二年以下の懲役又は五十万円以下の罰金に処する。

2　有線電気通信の業務に従事する者が前項の行為をしたときは、三年以下の懲役又は百万円以下の罰金に処する。

3　前二項の未遂罪は、罰する。

4　前三項の罪は、刑法（明治四十年法律第四十五号）第四条の二の例に従う。

電波法

第五十九条　何人も法律に別段の定めがある場合を除くほか、特定の相手方に対して行われる無線通信（電気通信事業法第四条第一項又は第百六十四条第三項の通信であるものを除く。第百九条並びに第百九条の二第二項及び第三項において同じ。）を傍受してその存在若しくは内容を漏らし、又はこれを窃用してはならない。

第百九条　無線局の取扱中に係る無線通信の秘密を漏らし、又は窃用した者は、一年以下の懲役又は五十万円以下の罰金に処する。

2　無線通信の業務に従事する者がその業務に関し知り得た前項の秘密を漏らし、又は窃用したときは、二年以下の懲役又は百万円以下の罰金に処する。

第百九条の二　暗号通信を傍受した者又は暗号通信を媒介する者であつて当該暗号通信を受信したものが、当該暗号通信の秘密を漏らし、又は窃用する目的で、その内容を復元したときは、一年以下の懲役又は五十万円以下の罰金に処する。

2　無線通信の業務に従事する者が、前項の罪を犯したとき（その業務に関し暗号通信を傍受し、又は受信した場合に限る。）は、二年以下の懲役又は百万円以下の罰金に処する。

3　前二項において「暗号通信」とは、通信の当事者（当該通信を媒介する者であつて、その内容を復元する権限を有するものを含む。）以外の者がその内容を復元できないようにするための措置が行われた無線通信をいう。

4　第一項及び第二項の未遂罪は、罰する。

5　第一項、第二項及び前項の罪は、刑法第四条の二の例に従う。

では通信の秘密とは何か

- 通信の内容
- 通信の存在
  - 通信の構成要素
    （通信当事者の住所、氏名、通信日時、
    発信場所等）
  - 通信の存在の事実の有無

つまりIPによる通信ほぼ全てが該当

よってDNSブロッキングは電気通信事業法違反

- DNSへの問い合わせの「内容」「存否」は
  もちろん通信の秘密
  - なのでそれを通信そのもの「以外」に使う行為は
    「正当業務行為」を除きアウトのはず
- もちろんHTTPアクセスとDNSは一連なので
  ブロッキングそのものは電気通信事業法違反

- 許される場合
  - 通信当事者（＝利用者）の許諾がある場合
  - 緊急避難にあたる場合

なぜ児童ポルノはブロッキングOK?
漫画村はダメ？

- 児童ポルノのブロッキングは緊急避難という整理
  - 被写体となった児童に対する人権侵害が継続
  - 流通が続く限り回復不可能な被害が続く

- 何故マンガ村ブロッキングは問題なのか？
  - 財産権である著作権の保護は緊急避難の対象ではないはず
  - 他に方法がないというのは本当か？