

# DNSブロッキング/フィルタリングの 法的解釈と実施状況

# おことわり

- 法律の話をしてしますが、話者は法律の専門家ではありません
- DNSの話はほとんどありません

# アジェンダ

- DNSブロッキング/フィルタリングと通信の秘密
- ISPにおける運用
  - NTTコムさん
  - IIJ

# アジェンダ

- DNSブロッキング/フィルタリングと通信の秘密
- ISPにおける運用
  - NTTコムさん
  - IIJ

# ブロッキングとフィルタリング

- 技術的にはどちらも同じ
  - 特定サイトへのアクセスをISP設備で遮断すること
- 技術的でない部分で異なる
  - ブロッキング: 無条件に実施
    - ブロッキングされたくない人のための代替手段は用意されない
  - フィルタリング: ユーザの同意を得た上で実施
    - フィルタリングされたくない人(同意しない人)のための代替手段が用意される

# ユーザのアクセスをISPで遮断するには

1. ユーザがどのサイトにアクセスしようとしているか調べる
2. そのサイトが制限対象リストに含まれているか調べる
3. 制限リストにあればアクセスを遮断する
4. 制限リストになければアクセスさせる

・アクセス試行のたびに上記プロセスがおこなわれる

・制限対象サイトにアクセスする場合(3)だけでなく、制限対象外のサイトにアクセスする場合(4)でも、1のアクセス先検査はおこなわれている

# 通信の秘密

- 憲法

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

(検閲の禁止)

第三条 電気通信事業者の取扱中に係る通信は、検閲してはならない。

(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。

# 通信の秘密とは

- ざっくり言うと、「電話をかけたり手紙を出したりインターネットを使ったりするときに、当事者以外の人にそれを知られない」権利
  - コミュニケーションにおける**プライバシーの保証**
- 国家権力や通信事業者は個人の通信の秘密に不当に介入しない
  - 結果として、通信の公共性、信頼性の向上、自由な情報流通といった**社会的利益の保護**といった側面も持つ
- 対象は通信の中身だけでなく、外形的事実も含む
  - **いつ、誰と、どんな、そもそも通信したのかしなかったのか、**などもるもる
- 人間が直接見るだけでなく、機械的に処理する場合も保護される

# 何をすると侵害なのか

- 知得

- 通信の秘密を積極的に知ろうとすること

- 窃用

- 通信の秘密を利用すること

- 漏洩

- 通信の秘密を他人が知り得る状態に置くこと

- 上記のいずれかを通信当事者の意思に反して実施すると通信の秘密の侵害

# ユーザのアクセスをISPで遮断するには

1. ユーザがどのサイトにアクセスしようとしているか調べる

2. そのサイトが制限対象リストに含まれているか調べる

知得

3. 制限リストにあればアクセスを遮断する

4. 制限リストになければアクセスさせる

窃用

・アクセス試行のたびに上記プロセスがおこなわれる

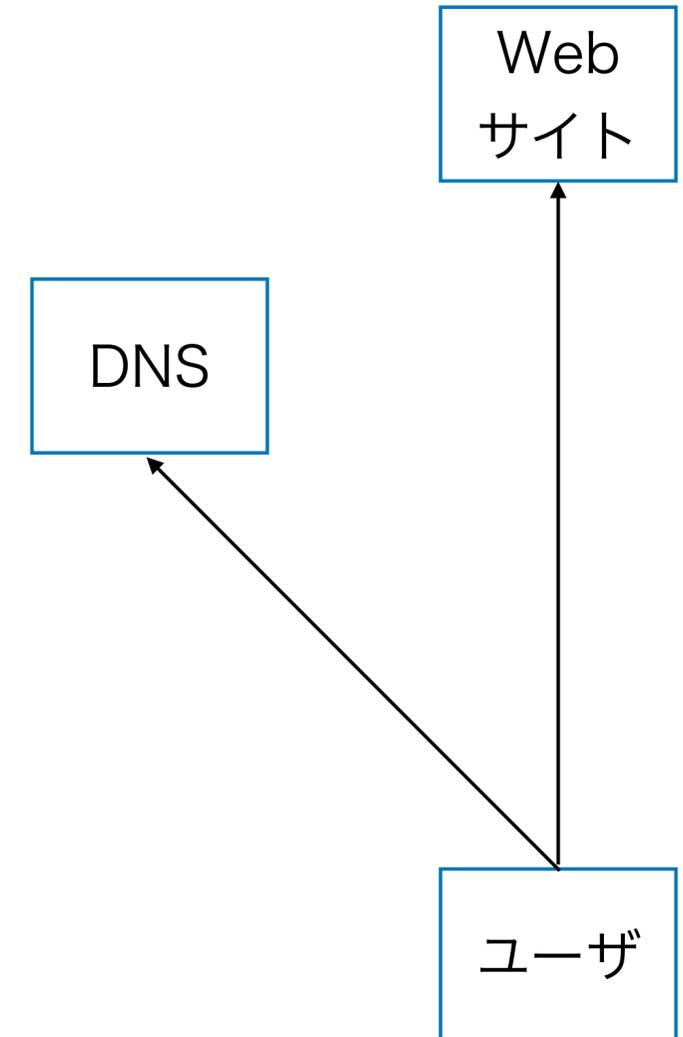
・制限対象サイトにアクセスする場合(3)だけでなく、制限対象外のサイトにアクセスする場合(4)でも、1のアクセス先検査はおこなわれている

# 誰の秘密を侵害するのか

- よくある誤解: ブロッキング対象サイトにアクセスする人の通信の秘密
  - 「そんなサイトにアクセスするのならブロッキングされてもしかたない」
  - 「自分はそんなサイトにアクセスしないから関係ない」
- 正しい理解: **すべての利用者**の通信の秘密
  - 特定サイトをブロッキングするためには、そのサイト以外も含めたすべてのアクセスを監視(知得)し、ブロッキング対象かどうかを判断する必要がある
  - ブロッキング対象サイトを一切閲覧することのない人の通信の秘密も、一方的に侵害することになる

# DNSと通信の秘密

- ユーザとDNS(フルリゾルバ)の間の通信において、フルリゾルバは通信当事者であるから、フルリゾルバがDNSクエリをどのように扱っても「通信当事者の意思」であり、通信の秘密の侵害にはならない
- ↑のような考え方は成立しない、というのが通説
- **名前解決は通信を成立させるために必要かつ分離不可分のもの**であり、DNSへの問い合わせだけを取り出して通信の秘密を侵害しない、というのは妥当な解釈ではない



# つまり、

- DNSフルリゾルバは通信の当事者ではない
  - あくまでユーザとユーザが通信しようとしている相手(Webサイト)の二者が当事者
- 通信当事者ではないのに、ユーザがどこにアクセスしようとしているかの情報を「知得」している
- フルリゾルバはふつーに名前解決するだけでも通信の秘密を侵害する
  - ブロッキング、フィルタリングの有無に関係なく
  - ルータなども同様

# ブロッキングとフィルタリング

- 技術的にはどちらも同じ

- 特定サイトへのアクセスをISP設備で遮断すること

- 技術的でない部分で異なる

- ブロッキング: 無条件に実施

- ブロッキングされたくない人のための代替手段は用意されない

- フィルタリング: ユーザの同意を得た上で実施

- フィルタリングされたくない人のための代替手段が用意される

通信当事者の意思に関係なく実施  
= 通信の秘密を侵害する  
→それならなぜブロッキングできるのか?

通信当事者の意思に反しない  
= 通信の秘密を侵害しない

# 違法性の阻却

- 通常であれば違法になることでも違法にならないような事情
  - 正当行為(刑法35条)
  - 正当防衛(刑法36条)
  - 緊急避難(刑法37条)
- 違法性阻却事由に該当する場合でも「通信の秘密を侵害しない」ではなく、「**侵害だが違法ではない**」であることに注意

# 正当行為

(正当行為)

第三十五条 法令又は正当な業務による行為は、罰しない。

- 刃物で他人の体を切ったら傷害罪だが、医師が手術でおこなうのなら正当行為
- ルータやMTAによる宛先の知得や、DNSの名前解決、課金のための通信履歴利用、その他ネットワークの安定運用に必要な行為は正当行為に該当
  - フルリゾルバの(通常の)名前解決は通秘の侵害だが、正当行為により違法性が阻却
  - ブロッキングしなくてもネットワークの安定運用は可能 → ブロッキングは正当行為ではない

# 正当防衛

(正当防衛)

第三十六条 急迫不正の侵害に対して、自己又は他人の権利を防衛するため、やむを得ずにした行為は、罰しない。

2 防衛の程度を超えた行為は、情状により、その刑を減輕し、又は免除することができる。

- 防衛行為の対象は侵害者でなければならない
- ユーザが「急迫不正の侵害」をしたわけではない
- ブロッキングで正当防衛は成立しない

# 緊急避難(1)

(緊急避難)

第三十七条 自己又は他人の生命、身体、自由又は財産に対する現在の危難を避けるため、<sup>(1)</sup>やむを得ずにした行為は、<sup>(2)</sup>これによって生じた害が避けようとした害の程度を超えなかった場合に限り、罰しない。

ただし、その程度を超えた行為は、情状により、その刑を減輕し、又は免除することができる。

2 前項の規定は、業務上特別の義務がある者には、適用しない。

1. 危難の現在性
2. 行為の補充性
3. 法益の権衡

# 緊急避難(2)

- ・危険の現在性

- ・ 危険: 違法行為にかぎらない(自然現象なども含む)
- ・ 現在性: 「過去そうだったから」 「将来そうなりそうだから」ではなく、「今まさに」

- ・行為の補充性

- ・ 危険を避けるための侵害性のより少ない手段が他に存在しないこと

- ・法益権衡

- ・ 避難行為から生じた害が、避けようとした害の程度を越えないこと

# アクセスを合法的に遮断する方法

- **通信当事者の意思に反しないことを確認する** → フィルタリング
  - 通信の秘密を侵害しない
- **緊急避難に該当するもの**に対してのみ遮断する → ブロッキング
  - 侵害だが違法ではない
  - どんなものが緊急避難に該当するかは個別に議論・検討が必要
- あくまでISPで実施する場合の話
  - 企業内ネットワークにおけるブロッキングはまた事情が異なる

# 通信当事者の意思の確認

- 個別同意(オプトイン)
  - 明示的な同意のある場合にのみフィルタリングする
- 包括同意(オプトアウト)
  - 明示的な不同意がなければ、同意ありとみなしてフィルタリングする
- 原則として包括同意ではなく個別同意が必要
  - 通信の秘密という重大な事項にかかわるため、その意味を正確に理解した上での同意が求められ、「約款に記載しただけ」のようなものでは通常は有効な同意とはみなされない

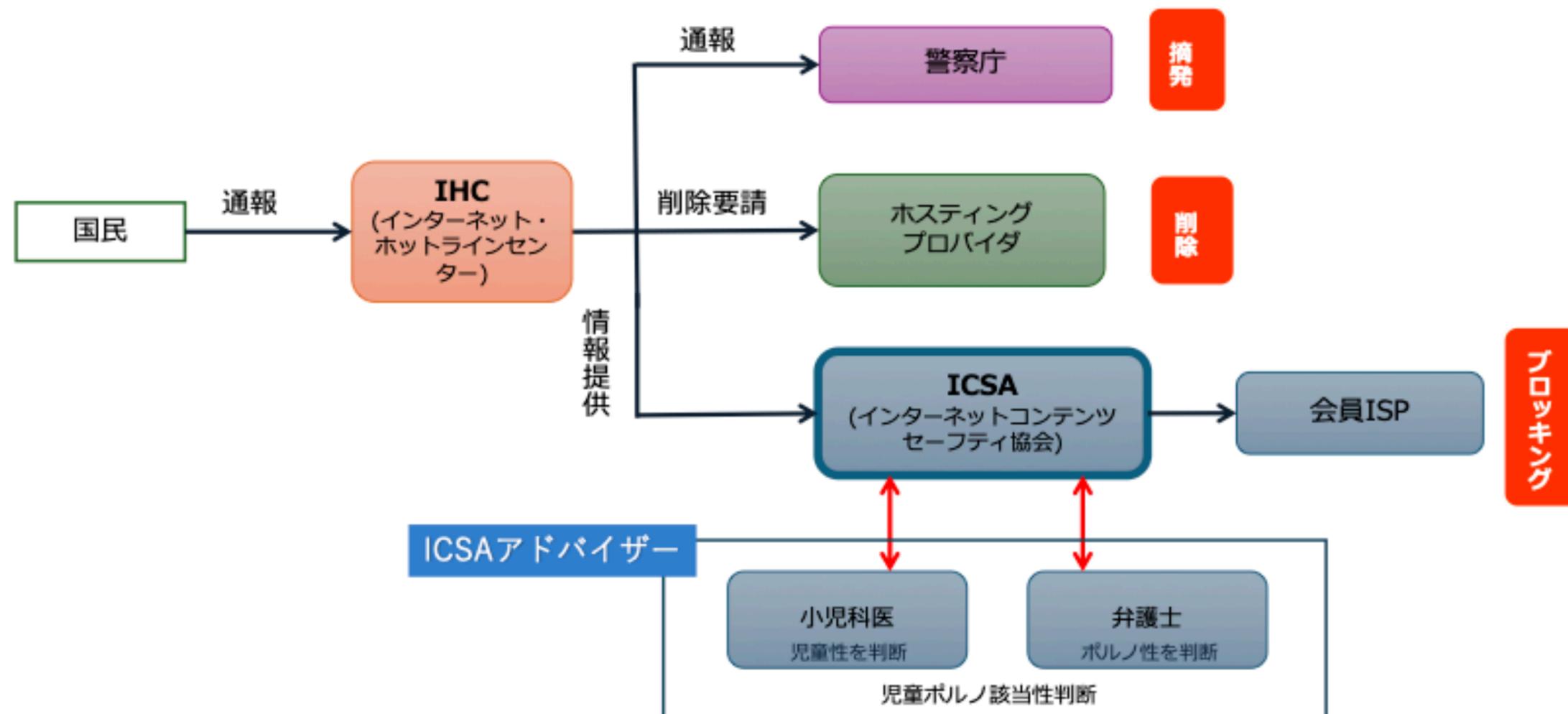
# 児童ポルノブロッキング(1)

- ・現時点で、ブロッキングできる(=緊急避難に該当する)と法的整理されているのは、児童ポルノのみ
  - ・ 危難の現在性(児童からの性的搾取・虐待の画像が現実には流通していること)
  - ・ 補充性(サーバ管理者が海外にいたり不明の場合など、検挙や削除の容易性・実効性が認められない場合)
  - ・ 法益権衡(通信の秘密による利益を上回るほど著しく児童の権利を侵害するものに限る)
- ・児童ポルノならなんでも、ではなく、警察による検挙が容易と見込まれるものや、侵害の程度が比較的低いと考えられるものは対象外

# 児童ポルノブロッキング(2)



## ブロッキング実施までの流れ



インターネットホットラインセンターに寄せられた通報の中で「児童ポルノ」と思われるものがICSAに情報提供される。その後、ICSAでは基準に則り、ブロック対象を選定。その際にICSAでは判断に迷うものをアドバイザーに判断を依頼。

# 児童ポルノブロッキング(3)

## ・児ポ防止法でISPの努力義務に

(インターネットの利用に係る事業者の努力)

### 第十六条の三

インターネットを利用した不特定の者に対する情報の発信又はその情報の閲覧等のために必要な電気通信役務（電気通信事業法（昭和五十九年法律第八十六号）第二条第三号に規定する電気通信役務をいう。）を提供する事業者は、児童ポルノの所持、提供等の行為による被害がインターネットを通じて容易に拡大し、これにより一旦国内外に児童ポルノが拡散した場合においてはその廃棄、削除等による児童の権利回復は著しく困難になることに鑑み、捜査機関への協力、当該事業者が有する管理権限に基づき児童ポルノに係る情報の送信を防止する措置その他インターネットを利用したこれらの行為の防止に資するための措置を講ずるよう努めるものとする。

# 漫画村事件

- 2018年 政府がISPに対してマンガ海賊版サイトのブロッキングを要請
  - 現在の危難(悪質な海賊版サイトが現在も閲覧可能)、補充性(海外にあって検挙が容易でない)、法益権衡(通信の秘密を侵害するデメリットを超えない)
  - …を「満たす場合には」緊急避難として違法性が阻却される、とした
  - が、ブロッキング対象に挙げられたサイトが実際にそれを「満たしている」かどうか政府で検討した形跡は見られなかった
- 要請に応じるとしたNTTコムに対して差し止め訴訟が提起
  - 控訴審(2019)で裁判所が通秘侵害に該当する可能性ありと言及(あくまで「可能性」のみで判断はしていない)

# アジェンダ

- DNSブロッキング/フィルタリングと通信の秘密
- ISPにおける運用
  - NTTコムさん
  - IIJ

# IJのブロッキング運用(1)

- 児童ポルノブロッキングのみ
- ICOSAが生成したブロッキング対象リストの取得からサーバへの反映まですべて自動化し、人間は一切かかわらない
  - リストの性質上、運用に携わる人間もできるだけ中身を見たくない
  - リストの妥当性はこちらでは一切判断しない
    - ICOSAが適切に判断しているという前提
    - ブロッキング対象を恣意的に追加/削除するような仕組みもない
    - もし誤掲載などがあってもそのままブロッキングされることになる

# IIJのブロッキング運用(2)

- ブロッキング対象サイトにアクセスする場合、名前解決を失敗させるのではなく、偽のAレコードを返してブロック対象になったことを示す専用のWebサイトにアクセスさせる
  - いまはHTTPS化によってほとんど機能してないですが…
- 児ポブロッキングの目的はあくまで児童の権利保護であり、誰がアクセスしようとしたのか調査することではない
  - 正常運用のためにログは取得しているが、ブロッキングされたユーザーの特定につながる情報(IPアドレスなど)は記録しない

# DNSブロッキングの回避

- フィルタリングは、同意しない人のために代替手段(フィルタリングしないフルリゾルバ)が提供される
- ブロッキングは全ユーザが対象なので代替手段は提供されない
- が、ブロッキングしないpublic DNSを利用することで回避は可能
  - IJ Public DNSはブロッキングするので回避先としては利用できない
- これを制限すること(OP53B)はまた別途通信の秘密の侵害に関する議論が必要
  - OP25Bは正当行為と解釈されるが、OP53Bは事情が異なり、おそらく認められない
  - 仮にOP53Bを実施してもDoH/DoTで回避可能

# IJのフィルタリング運用(1)

- マルウェアフィルタリング
  - botnetのC&Cサーバの名前解決を失敗させる
  - マルウェアが設置されているサイト、ではない
- 同意しないユーザーのために、フィルタリングしないフルリゾルバも提供
  - モバイル: ユーザーの申告により自動設定されるDNSサーバが変更
  - それ以外: 同意しない場合、フルリゾルバのIPアドレスを手動で変更
  - いずれも、デフォルトはフィルタリングあり(オプトアウト、包括同意)

# IIJのフィルタリング運用(2)

- 第三者がリストを作成していた児ポブロッキングとは異なり、マルウェアフィルタリングはリストの作成もIIJがおこなう
  - リスト作成とフルリゾルバ運用は社内の別部署
  - DNS運用側では、児ポ同様にリストに恣意的な判断を加えずそのままサーバに反映
- C&Cサーバの検知のため、一部顧客からDNS以外の通信ログを収集して分析
  - こちらは包括同意ではなく、個別同意を得た顧客からのみ
- フィルタリングの実施状況について定期的にレポートを公表
  - <https://www.ij.ad.jp/sec-statement/>

# 包括同意によるフィルタリング(1)

- フィルタリングは原則として個別同意で実施すべきだが、IIJのマルウェアフィルタリングは包括同意で実施
  - 適切な条件を満たせば包括同意であっても有効な同意があるといえるとの解釈
    - 総務省「電気通信事業者におけるサイバー攻撃への適正な対処の在り方に関する研究会第三次とりまとめ」
      - [https://www.soumu.go.jp/main\\_content/000575399.pdf](https://www.soumu.go.jp/main_content/000575399.pdf)
    - JAIPAほか5団体「電気通信事業者におけるサイバー攻撃等への対処と通信の秘密に関するガイドライン第6版」
      - [https://www.jaipa.or.jp/other/mtcs/guideline\\_v6.pdf](https://www.jaipa.or.jp/other/mtcs/guideline_v6.pdf)

# 包括同意によるフィルタリング(2)

- ・サイバー攻撃と通信の秘密に関するガイドライン第6版 pp.33-34
  - a 自身が利用する端末が C&C サーバと通信している場合には当該通信が遮断されるサービスが提供されており、かつこれを希望しない者は検知等の対象にならない。
  - b 保存された情報が他の用途では利用されず、目的達成後速やかに削除される。
  - c 照合、記録及び分析を希望しない者(オプトアウトした者)の利益が侵害されないような態勢を整える。具体的な対応の例については、第二次とりまとめP13参照。
  - d 利用者が、一旦契約約款等に同意した後も、随時、同意内容を変更(設定変更)できるようにする。
  - e 同意内容の変更の有無にかかわらず、その他の提供条件が同一である契約内容とする。
  - f 本件対策の内容とともに、照合、記録及び分析を望まない利用者は随時同意内容を変更(設定変更)できること及びその方法につき利用者に相応の周知を図る。具体的には、契約締結時に書面等を用いて明確に説明する他、既契約者に対しては、ウェブサイトへの掲載に加えて、電子メールや郵便等によって周知すること等が考えられる。

# まとめ

- DNSによるコンテンツブロッキングとフィルタリングについて、主に通信の秘密の観点から説明してみました
  - 今回の話のスコープからははずれるが、これ以外にもDoS/DDoSへの対処、迷惑メールの取り扱いその他さまざまな場面で通信の秘密との関係が議論されている
    - [https://www.jaipa.or.jp/other/mtcs/guideline\\_v6.pdf](https://www.jaipa.or.jp/other/mtcs/guideline_v6.pdf)
  - あくまでISP業界による自主解釈・自主基準であり、裁判所がその解釈を認めるかどうかは不透明
- ISPはユーザの通信の秘密に容易にアクセスできる立場であり、そのためかなり慎重な取り扱いをしている

# 参考

- 安心ネットづくり促進協議会 児童ポルノ対策作業部会
  - 法的問題検討サブワーキンググループ報告書
    - <https://www.good-net.jp/files/original/201711012219018083684.pdf>
  - ブロッキングを実施するプロバイダが利用者に対して負う民事責任について
    - <https://www.good-net.jp/files/original/201711012219018948254.pdf>
- IJmio meeting 23 DNSフィルタリングをなぜ行うのか
  - <https://www.slideshare.net/slideshow/ijmio-meeting-23-dns/140576610>